VMware Horizon Client for Linux Installation and Setup Guide

14 MAR 2019

VMware Horizon Client for Linux 5.0

vmware®

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

https://docs.vmware.com/

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

VMware Horizon Client for Linux Installation and Setup Guide

This document, *VMware Horizon Client for Linux Installation and Setup Guide*, provides information about installing, configuring, and using VMware Horizon® Client™ software on a Linux client system.

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 Horizon 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 Horizon 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.

This chapter includes the following topics:

System Requirements for Linux Client Systems

The Linux device on which you install Horizon Client, and the peripherals it uses, must meet certain system configurations that have been tested and are officially supported by VMware.

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 Horizon 7 deployments. The vendor and model of the thin or zero client device, and the configuration that an enterprise chooses to use, determine the features available for each client device and the operating systems supported. For information about the vendors and models for these client devices, see the VMware Compatibility Guide, available on the VMware website.

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

i386, x86_64, ARM

Memory

At least 2 GB of RAM

Operating system

Horizon Client for Linux has been tested on the following operating systems for this release.

Operating System	Version
Ubuntu 32-bit	16.04
Ubuntu 64-bit	16.04, 18.04
Red Hat Enterprise Linux (RHEL) 32-bit	6.10
Red Hat Enterprise Linux (RHEL) 64-bit	6.10, 7.6

OpenSSL requirement

Horizon Client requires a specific version of OpenSSL. The correct version is automatically downloaded and installed.

Horizon Connection Server, Security Server, and View Agent or Horizon Agent

Latest maintenance release of Horizon 6.2.x and later releases

If client systems connect from outside the corporate firewall, it is good practice for you to use a security server. With a security server, client systems do not require a VPN connection.

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

Display protocol

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

	■ RDP
Screen resolution on the client system	Minimum: 1024 X 768 pixels

Hardware requirements for VMware Blast and PCoIP	■ x86- or x64-based processor with SSE2 extensions, with a 800 MHz or faster processor speed.
	■ Available RAM above system requirements to support various monitor setups. Use the following formula as a general guide:
	`20 MB + (24 * (# monitors) * (monitor width) * (monitor height))`
	As a rough guide, you can use the following calculations:
	`1 monitor: 1600 x 1200: 64 MB`
	`2 monitors: 1600 x 1200: 128 MB`
	`3 monitors: 1600 x 1200: 256 MB`

Hardware requirements for RDP	■ x86- or x64-based processor with SSE2 extensions, with a 800 MHz or faster processor speed. ■ 128 MB RAM.
Software requirements for Microsoft RDP	Use the latest `rdesktop` version available.
Software requirements for FreeRDP	If you plan to use an RDP connection to Horizon desktops and you 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.
Other software requirements	Horizon Client also has certain other software requirements, depending on the Linux distribution you use. 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. ■ `libudev.so.0` **Note** Beginning with Horizon Client 4.2, `libudev0` is required to run Horizon Client. By default, `libudev0` is not installed in some systems. ■ 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 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. The feature also works with standard conferencing applications, such as Skype, WebEx, and Google Hangouts. To support Real-Time Audio-Video, your Horizon deployment must meet certain software and hardware requirements.

Virtual desktops

Virtual desktops must have View Agent 6.0, or Horizon Agent 7.0 or later, installed.

Published desktops and applications

To use the Real-Time Audio-Video feature with published desktops and applications, Horizon Agent 7.0.2 or later must be installed on the RDS host.

Horizon Client computer or client access device

- Real-Time Audio-Video is supported on x86 and x64 devices. This feature is not supported on ARM processors. The client system must meet the following minimum hardware requirements.

Resolution	Frame Rate	CPU	Required Memory
320 x 240	15 FPS	2 core, 1800 MHz	105 MB
640 x 480	15 FPS	2 core, 2700 MHz	150 MB
1280 x 720	15 FPS	4 core, 3400 MHz	210 MB

- Horizon Client requires the following libraries:
  - `Video4Linux2`
  - `libv4l`
  - `Pulse Audio`

  The plug-in file (`/usr/lib/pcoip/vchan_plugins/libviewMMDevRedir.so`) 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. You do not need to install the device drivers on the machine where the agent is installed.
Display protocols	■ PCoIP ■ VMware Blast (requires Horizon Agent 7.0 or later)

System Requirements for Serial Port Redirection

With the serial port redirection feature, end users can redirect locally connected serial (/dev/ttyS) ports, such as built-in RS232 ports or USB-to-Serial adapters, to their published desktops. To support serial port redirection, your Horizon deployment must meet certain software and hardware requirements.

Published desktops on RDS hosts	The RDS host that hosts published desktops must have Horizon Agent 7.6 or later installed with the Serial Port Redirection setup option selected. This setup option is deselected by default. The following operating systems are supported for published desktops. ■ Windows Server 2012 R2 ■ Windows Server 2016 ■ Windows Server 2019 Serial port device drivers do not need to be installed in the RDS host.
Virtual desktops	Virtual desktops are not supported.
Horizon Client computer or client access device	The serial port redirection feature is supported on Linux systems that are supported for this release. Any required serial port device drivers must be installed and the serial port must be operable. Serial port redirection is available with Horizon Client for Linux 4.9 and later releases.
Nested sessions	The serial port redirection feature is supported in published applications that are started from Horizon Client inside published desktops (nested sessions). Horizon Client 4.10 or later must be installed in the published desktops. The serial port redirection feature has the following limitations when used in a nested session. ■ The number of concurrent users is limited. ■ Users must use matched client and agent versions, for example, Horizon Client 5.0 and Horizon Agent 7.8.
Display protocols	■ VMware Blast (requires Horizon Agent 7.0 or later)

- PCoIP (supported but not tested)

Serial port redirection is not supported in RDP desktop sessions.

System Requirements for Scanner Redirection

End users can scan information into remote desktops with scanners that are connected to their local client systems. They can control scanner settings by selecting options in the remote desktop interface. To use this feature, the remote desktops and client computers must meet certain system requirements.

Remote desktops	Remote desktops must have Horizon Agent 7.8 or later, installed with the Scanner Redirection setup option, on the parent or template virtual machines or RDS hosts. On Windows desktop and Windows Server guest operating systems, the Horizon Agent Scanner Redirection setup option is deselected by default. For information about which guest operating systems are supported for virtual desktops and RDS hosts, and for information about configuring scanner redirection in remote desktops, see "Configure Scanner Redirection" in the *Configuring Remote Desktop Features in Horizon 7* document.
Horizon Client computer or client access device	The client computer must be connected to a scanner compatible with the SANE scanner interface standard. The SANE scanner device drivers must be installed, and the scanner must be operable, on the client computer. You do not need to install the scanner device drivers on the remote desktop operating system where the agent is installed.
Scanning device standard	SANE
Display protocols	■ PCoIP ■ VMware Blast Scanner redirection is not supported in RDP desktop sessions.

System Requirements for Multimedia Redirection (MMR)

With multimedia redirection (MMR), the multimedia stream is decoded on the client system. The client system plays the media content so that the load on the ESXi host is reduced.

Remote desktops	■ Virtual desktops must have View Agent 6.0.2 or later, or Horizon Agent 7.0 or later, installed. ■ Published desktops must have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, installed on the RDS host.

For information about operating system requirements and other software requirements and configuration settings, see the topics about Windows Media Multimedia Redirection in the *Configuring Remote Desktop Features in Horizon 7* document.

Horizon Client computer or client access device

Because MMR offloads media processing from the server to the client, the client has the following minimum hardware requirements.

Processor:	Intel Pentium 4 or AMD Athlon dual-core
Processor speed:	1.5 GHz for common case, or 1.8 GHz for Full HD
Memory:	2-GB RAM
Video adapter:	Hardware accelerated

You must install one of the following libraries to avoid video playback issues:

- GStreamer core library and gstreamer-ffmpeg 0.10
- GStreamer core library and fluendo 0.10

On Dell Wyse thin clients, video playback might not work with the pre-installed fluendo library. To resolve the problem, contact Dell support to obtain the latest fluendo library.

Supported media formats

Media formats that Windows Media Player supports, for example: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3; WAV.

Note DRM-protected content is not redirected through Windows Media MMR.

GStreamer Framework

Set up the GStreamer environment such that the framework is composed of the graphics card, hardware acceleration API, and GStreamer plug-in that allow GStreamer to function properly. Table 1-1 lists the different possible setup combinations. To ensure the best possible environment, set up your GStreamer environment using the information in Table 1-1 for the NVIDIA and Intel graphic cards.

Table 1-1. GStreamer Framework Setup

Graphics Card (including Driver)	Hardware Accelerator API	GStreamer Plug-in
NVIDIA	VDPAU (`libvdpau.so`)	`vdpau`
Intel	VAAPI (`libvaapi.so`)	`gstreamer-vaapi`
--	OpenMax	`gst-omx`

Table 1-1. GStreamer Framework Setup (Continued)

Graphics Card (including Driver)	Hardware Accelerator API	GStreamer Plug-in
--	DCE	gstreamer-ducati
AMD	OVD/UVD	Unavailable

To get more detailed information, see https://gstreamer.freedesktop.org/documentation/tutorials/playback/hardware-accelerated-video-decoding.html.

MMR is not enabled by default. To enable it, you must set the configuration option `view.enableMMR`. For more information, see Horizon Client Configuration Settings and Command-Line Options.

Requirements for Using Flash URL Redirection

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

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

The Flash URL redirection feature is available only when the correct version of the agent software is installed. This feature is included in the agent software beginning with View Agent 6.0.

To use the Flash URL redirection feature, you must set up your Web page and the client devices. Client systems must meet the following software requirements.

- This feature is supported 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` application, or verify that the application 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 *Configuring Remote Desktop Features in Horizon 7* document.

Requirements for Using Skype for Business with Horizon Client

An end user can run Skype for Business inside a virtual desktop without negatively affecting the virtual infrastructure and overloading the network. During Skype audio and video calls, all media processing takes place on the client machine instead of in the virtual desktop.

To use this feature, you must install the VMware Virtualization Pack for Skype for Business feature on the client machine during the Horizon Client for Linux installation. For information, see Installation Options .

A Horizon administrator must also install the VMware Virtualization Pack for Skype for Business feature on the virtual desktop when Horizon Agent is installed. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon 7* document.

For complete requirements, see "Configure Skype for Business" in the *Configuring Remote Desktop Features in Horizon 7* document.

Requirements for the Session Collaboration Feature

With the Session Collaboration feature, users can invite other users to join an existing Windows remote desktop session. To support the Session Collaboration feature, your Horizon deployment must meet certain requirements.

Session collaborators

To join a collaborative session, a user must have Horizon Client 4.7 or later for Windows, Mac, or Linux installed on the client system, or must use HTML Access 4.7 or later.

Windows remote desktops

- Horizon Agent 7.4 or later must be installed in the Windows virtual desktop, or on the RDS host for published desktops.
- The Session Collaboration feature must be enabled at the desktop pool or farm level. For information about enabling the Session Collaboration feature for desktop pools, see the *Setting Up Virtual Desktops in Horizon 7* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon 7* document.

You can use Horizon Agent group policy settings to configure the Session Collaboration feature. For information, see the *Configuring Remote Desktop Features in Horizon 7* document.

Linux remote desktops

For Linux remote desktop requirements, see the *Setting Up Horizon 7 for Linux Desktops* document.

Connection Server	The Session Collaboration feature requires that the Connection Server instance uses an Enterprise license.
Display protocols	VMware Blast

The Session Collaboration feature does not support published application sessions.

Smart Card Authentication Requirements

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

Client Hardware and Software Requirements

PIV smart card authentication is not supported on RedHat 6.x systems.

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

- Horizon Client
- A compatible smart card reader
- Smart card reader driver
- Smart card driver
- PKCS#11 module

  Note It is suggested that you install the OpenSC PKCS#11 module for the PIV Smart Card.

- Product-specific application drivers

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

Remote Desktop and Published Application Software Requirements

A Horizon administrator must install product-specific application drivers on the virtual desktops or RDS host.

Enabling the User Name Hint Text Box in Horizon Client

In some environments, smart card users can use a single smart card certificate to authenticate to multiple user accounts. Users enter their user name in the **Username hint** text box when they sign in with a smart card.

To make the **Username hint** text box appear on the Horizon Client login dialog box, you must enable the smart card user name hints feature in Connection Server. The smart card user name hints feature is supported only with Horizon 7 version 7.0.2 and later servers and agents. For information about enabling the smart card user name hints feature, see the *Horizon 7 Administration* document.

If your environment uses a Unified Access Gateway appliance rather than a security server for secure external access, you must configure the Unified Access Gateway appliance to support the smart card user name hints feature. The smart card user name hints feature is supported only with Unified Access Gateway 2.7.2 and later. For information about enabling the smart card user name hints feature in Unified Access Gateway, see the *Deploying and Configuring Unified Access Gateway* document.

Horizon Client continues to support single-account smart card certificates even when the smart card user name hints feature is enabled.

Additional Smart Card Authentication Requirements

In addition to meeting the smart card requirements for Horizon Client systems, other Horizon components must meet certain configuration requirements to support smart cards.

Connection Server and security server hosts	An administrator must add all applicable Certificate Authority (CA) certificates for all trusted user certificates to a server truststore file on the Connection Server or security server host. These certificates include root certificates and, if an intermediate certificate authority issues the user's smart card certificate, must also include intermediate certificates. For information about configuring Connection Server to support smart card use, see the *Horizon 7 Administration* document.
Active Directory	For information about tasks that an administrator might need to perform in Active Directory to implement smart card authentication, see the *Horizon 7 Administration* document.

Configure Horizon Client for Smart Card Authentication

You must perform certain configuration steps to use a smart card in Horizon Client.

Prerequisites

- Install Horizon Client.
- (Optional) To make the **Username hint** field appear in the Horizon Client login dialog box, enable the smart card user name hints feature in Connection Server. For more information, see "Setting Up Smart Card Authentication" in the *Horizon 7 Administration* document.

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/lib64/pkcs11/opensc–pkcs11.so
                /usr/lib/vmware/view/pkcs11/libopenscpkcs11.so
```

Note Make sure that the symbolic link name to the `opensc–pkcs11` library begins with `lib`.

Supported Desktop Operating Systems

A Horizon administrator creates virtual machines that have a guest operating system and installs 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 *Horizon 7 Installation* document.

If you have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, some Linux guest operating systems are also supported. For information about system requirements, configuring Linux virtual machines, and a list of supported features, see the *Setting Up Horizon 6 for Linux Desktops* or *Setting Up Horizon 7 for Linux Desktops* document.

Preparing Connection Server for Horizon Client

Before end users can connect to a server and access a remote desktop or published application, a Horizon administrator must configure certain Connection Server settings.

Unified Access Gateway and Security Servers

- If your Horizon deployment includes a Unified Access Gateway appliance, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring Unified Access Gateway* document. Unified Access Gateway appliances perform the same role as security servers.
- If your Horizon deployment includes a security server, verify that you are using the latest maintenance releases of Connection Server 6.x and Security Server 6.x or later releases. For more information, see the installation document for your Horizon version.

Secure Tunnel Connection

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 a Connection Server instance or a security server, verify that the client device can resolve this DNS name.

Desktop and Application Pools

- 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 more information, see the *Setting Up Virtual Desktops in Horizon 7* and *Setting Up Published Desktops and Applications in Horizon 7* documents.

User Authentication

- To provide end users with unauthenticated access to published applications in Horizon Client, you must enable this feature in the Connection Server instance. For more information, see the topics about unauthenticated access in the *Horizon 7 Administration* document.
- To use two-factor authentication, such as RSA SecurID or RADIUS authentication, with Horizon Client, you must enable the two-factor authentication feature for the Connection Server instance. For more information, see the topics about two-factor authentication in the *Horizon 7 Administration* document.
- To hide the server URL in Horizon Client, enable the **Hide server information in client user interface** global setting. This setting is available in Horizon 7 version 7.1 and later. For more information, see the *Horizon 7 Administration* document.
- To hide the **Domain** drop-down menu in Horizon Client, enable the **Hide domain list in client user interface** global setting. This setting is available in Horizon 7 version 7.1 and later. Beginning with Horizon 7 version 7.8, it is enabled by default. For more information, see the *Horizon 7 Administration* document.
- To send the domain list to Horizon Client, enable the **Send domain list** global setting in Horizon Administrator. This setting is available in Horizon 7 verison 7.8 and later and is disabled by default. Earlier Horizon 7 versions send the domain list. For more information, see the *Horizon 7 Administration* document.

The following table shows how the **Send domain list** and **Hide domain list in client user interface** global settings determine how users can log in to the server.

Send domain list setting	Hide domain list in client user interface setting	How users log in
Disabled (default)	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain\username*** ■ ***username@domain.com***
Disabled (default)	Disabled	If a default domain is configured on the client, the default domain appears in the **Domain** drop-down menu. If the client does not know a default domain, `*DefaultDomain*` appears in the **Domain** drop-down menu. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain\username*** ■ ***username@domain.com***

Send domain list setting	Hide domain list in client user interface setting	How users log in
Enabled	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain\username*** ■ ***username@domain.com***
Enabled	Disabled	Users can enter a user name in the **User name** text box and then select a domain from the **Domain** drop-down menu. Alternatively, users can enter one of the following values in the **User name** text box. ■ ***domain\username*** ■ ***username@domain.com***

Installation Options

During the Horizon Client installation process, you are prompted to confirm whether to install optional components. The default is to install all components.

The following table provides a brief summary of each optional component.

Table 1-2. Horizon Client for Linux Installation Options

Option	Description
Seamless Window	With this feature, users can interact with an application that is running on a remote desktop as if it was a locally running application.
Multimedia Redirection (MMR)	Redirects multimedia stream from the desktop to the client machine, where the stream is processed. The component file is installed in `/usr/lib/vmware/view/vdpService/`.
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 Horizon Agent installer in the remote desktop. Smart card is supported on remote desktops that are deployed on single-user machines and RDS hosts. For smart card support on RDS hosts, you must have View Agent 6.1.1 or later. The component files are installed in `/usr/lib/pcoip/vchan_plugins/`.
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/`.
VMware Horizon(R) Virtualization Pack for Skype for Business	Lets users run Skype for Business inside a virtual desktop without negatively affecting the virtual infrastructure and overloading the network. All media processing takes place on the Linux client machine, instead of in the virtual desktop, during Skype audio and video calls. The component file is installed in `/usr/lib/vmware/mediaprovider`.

Table 1-2. Horizon Client for Linux Installation Options (Continued)

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops and applications. USB redirection is supported on remote desktops and applications that are deployed on single-user machines. The component files are installed in `/usr/lib/vmware/view/usb/`. If you allow the installer to register and start installed services after the installation completes, the USB arbitrator daemon, `vmware-USBArbitrator`, runs automatically. Otherwise, you can start the daemon manually by running the following command: `sudo /etc/init.d/vmware-USBArbitrator start` **Note** You can use group policy settings to disable USB redirection for specific users. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.
Scanner Redirection	Lets users scan data into remote desktops with SANE-compliant scanners connected to their local client system. Users do not have to install additional drivers on their remote desktops. If you allow the Horizon Client installer to register and start the installed services after the installation completes successfully, the scanner redirection daemon runs automatically. Otherwise, you can start the scanner redirection daemon manually by running the following command. `sudo /etc/init.d/ftscanhv start` Scanner redirection requires remote desktops to have Horizon Agent 7.8 or later, installed with the Scanner Redirection setup option, on the parent or template virtual machines or RDS hosts. In addition, this feature requires the PCoIP or VMware Blast display protocol. After the installation, you can configure group policy settings for this feature by following the instructions in "Configure Scanner Redirection" in the *Configuring Remote Desktop Features in Horizon 7* document.
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 allow the installer to register and start installed services after the installation, you do not need to configure this feature manually. Otherwise, you can configure and enable this feature by following the instructions in Enable the Virtual Printing Feature on a Linux Client. In Horizon 6.0.2 and later, virtual printing is supported on the following remote desktops and published applications: ■ Desktops that are deployed on single-user machines. ■ Desktops that are deployed on RDS hosts, where the RDS hosts are virtual machines. ■ Remote applications, which are provided by RDS hosts. ■ Remote applications that are launched from Horizon Client inside remote desktops (nested sessions).

Table 1-2. Horizon Client for Linux Installation Options (Continued)

Option	Description
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. The component files are installed in `/usr/lib/vmware/view/vdpService/`.
Serial Port Redirection	Lets end users redirect locally connected serial ports, such as built-in RS-232 ports (/dev/ttySxx) or USB-to-Serial adapters (/dev/ttyUSBxx), to their published desktops. If you allow the Horizon Client installer to register and start the installed services after the installation completes successfully, the serial port daemon runs automatically. Otherwise, you can start the serial port daemon manually by running the following command. `sudo /etc/init.d/ftsprhv start` To make a USB-to-Serial adapter device available for serial port redirection, deselect **Connect USB Device > Automatically Connect at Startup & Automatically Connect when inserted** and ensure that the USB-to-Serial adapter device is not selected under the **Connect USB Device** menu.

Install or Upgrade Horizon Client for Linux from VMware Product Downloads

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 starts a GUI wizard. You can also run the installer with the `--console` option to start the command-line wizard.

Prerequisites

- Verify that the client system runs a supported operating system. See System Requirements for Linux Client Systems.
- Become familiar with the installation options. See Installation Options.
- 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.
- Uninstall any earlier version of the Horizon Client software. See Uninstall Horizon Client for Linux.
- If you plan to use the command-line installer, become familiar with the Linux command-line installation options. See Command-Line Installation Options for the Linux Client.
- In a python2 environment on Ubuntu 16.04 x64 or x86, and Ubuntu 18.04 x64 distributions, run `sudo apt-get install python-gtk2` to install the `gtk2` library.

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`.

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 To finish the installation, follow the prompts.

Important 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 must manually start USB redirection services every time you reboot, and you do not need to enable the Virtual Printing feature manually.

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

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

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 Published Application.

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-serialportclient serialportEnable yes`	Installs the serial port redirection feature.
`--set-setting vmware-horizon-scannerclient scannerEnable yes`	Installs the scanner redirection feature.
`--set-setting vmware-horizon-virtual-printing tpEnable yes`	Installs the virtual printing feature.
`--set-setting vmware-horizon-tsdr tsdrEnable yes`	Installs the client drive redirection feature.
`--set-setting vmware-horizon-mmr mmrEnable yes`	Installs the multimedia redirection (MMR) feature.

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

Option	Description
`--set-setting vmware-horizon-media-provider mediaproviderEnable yes`	Installs the VMware Horizon Virtualization Pack for Skype for Business component.
`--stop-services`	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 basic text UI.
`VMWARE_EULAS_AGREED=yes`	Allows you to silently accept the product EULAs.
`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

--set-setting vmware-horizon-scannerclient scannerEnable yes

--set-setting vmware-horizon-serialportclient serialportEnable yes

--set-setting vmware-horizon-mmr mmrEnable yes

--set-setting vmware-horizon-media-provider mediaproviderEnable 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.

Configure VMware Blast Options

You can configure VMware Blast options for remote desktop and published application sessions that use the VMware Blast display protocol.

You can allow H.264 decoding. You can also allow increased color fidelity when H.264 decoding is allowed. This feature is not supported on ARM processors.

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 support 4K resolution for H.264.

H.264 decoding is supported on AMD, NVIDIA, and Intel GPUs. H.264 decoding requires that the graphics library OpenGL 3.2 or later is installed for AMD and NVIDIA GPUs.

If you plan to use H.264 decoding with a NVIDIA GPU, install VDPAU (Video Decode and Presentation API for UNIX). VDPAU is no longer included with the latest NVIDIA driver and must be installed separately.

To use H.264 with an Intel GPU, the Intel VA-API driver and the GLX VA-API libraries are required. Running the command `vainfo` shows the H.264 profiles. If the VA-API driver version is 1.2.x or earlier, you must add the entry `mks.enableGLBasicRenderer = TRUE` to `/etc/vmware/config`, `/usr/lib/vmware/config`, or `~/.vmware/config`. The configuration files are processed in the following order:

1 `/etc/vmware/config`

2 `/usr/lib/vmware/config`

3 `~/.vmware/config`

With Red Hat 7.x, Intel GPU, Intel driver version 1.2 or earlier, OpenGL 3.2, and H.264 enabled, you must add the following entries to one of the three configuration files to avoid display issues such as a black screen.

```
mks.enableGLRenderer=FALSE
mks.enableGLBasicRenderer=TRUE
```

You can configure H.264 decoding and high color accuracy before or after you connect to a server.

Note In earlier Horizon Client versions, you had to select a network condition option to provide the best user experience with VMware Blast. In this release, Horizon Client senses current network conditions and chooses one or more transports to provide the best user experience automatically.

Prerequisites

To use H.264 decoding, Horizon Agent 7.0 or later must be installed.

To allow increased color fidelity when H.264 decoding is allowed, Horizon Agent 7.4 or later must be installed.

Procedure

1 Start Horizon Client.

2 Select **File > Configure VMware Blast** from the menu bar.

3 To allow H.264 decoding in Horizon Client, select the **H.264** check box.

- When this option is selected (the default setting) and the client GPU has an H.264 hardware decoder, Horizon Client uses H.264 4.2.0 hardware decoding.
- If the client GPU does not have an H.264 hardware decoder and this option is selected, Horizon Client 4.8 or earlier uses JPG/PNG decoding.
- When this option is selected and if the client GPU does not have an H.264 hardware decoder and the increased color fidelity feature is not allowed, Horizon Client 4.9 or later uses H.264 4.2.0 software decoding.
- When this option is deselected, Horizon Client uses JPG/PNG decoding.

4 To allow increased color fidelity when H.264 decoding is allowed in Horizon Client, select the **High Color Accuracy** check box.

   When this option is selected, Horizon Client 4.9 or later uses H.264 4.4.4 software decoding, regardless of whether or not the client GPU has an H.264 hardware decoder. Selecting this option might reduce battery life and performance. This feature is disabled by default.

5 Click **OK** to save your changes.

Changes for H.264 take effect the next time a user connects to a remote desktop or published application and selects the VMware Blast display protocol. Your changes do not affect existing VMware Blast sessions.

Configure Horizon Client Data Sharing

If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects and receives anonymous data on client systems to prioritize hardware and software compatibility. You can configure whether to share information on your client system by enabling or disabling a setting in Horizon Client.

Horizon Client data sharing is enabled by default. The `view.enableDataSharing` configuration key is initially set to "TRUE" in the `~/.vmware/view-preferences` file. You must configure the data sharing setting before you connect to a server. The setting is applied to all servers. You cannot change the Horizon Client data sharing setting after you connect to a server.

Procedure

1 Start Horizon Client.

2 Select **File > Configure data sharing** from the menu bar.

3 Select or deselect the **Allow data sharing** check box.

4 Click **OK** to save your changes.

   Your preference is stored using the `view.enableDataSharing` configuration key in the `~/.vmware/view-preferences` configuration file.

Horizon Client Data Collected by VMware

If a Horizon administrator has opted to participate in the customer experience improvement program, and data sharing is enabled on the client system, VMware collects data about the client system.

VMware collects data about client systems to prioritize hardware and software compatibility. If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment to respond better to customer requirements. VMware does not collect data that identifies your organization. Horizon Client information is sent first to the Connection Server instance and then to VMware, along with data about Connection Server, desktop pools, and remote desktops.

The information is encrypted when it is in transit to the Connection Server instance. The information on the client system is logged unencrypted in a user-specific directory. The logs do not contain personally identifiable information.

A Horizon administrator can select whether to participate in the VMware customer experience improvement program when installing Connection Server or by setting an option in Horizon 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
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)

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

Description	Is This Field Made Anonymous?	Example Value
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 clients.)
Maximum concurrent USB device connections	No	2
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 use count	No	(Number of times the device was shared)

Configuring Horizon Client for End Users

2

Configuring Horizon Client for end users can involve constructing URIs, setting the certificate verification mode, modifying advanced TLS/SSL options, configuring specific keys and key combinations, setting display protocol options, and enabling FIPS Compatible mode.

This chapter includes the following topics:

Common Configuration Settings

Horizon Client provides several configuration mechanisms that simplify the login and remote desktop selection experience for end users, and 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
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
Remote 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

Table 2-1. Common Configuration Settings (Continued)

Setting	Mechanisms for Configuring
Configuring certificate checking	Configuration File Property
Configuring TLS protocols and cryptographic algorithms	Configuration File Property, Command Line

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`

Note You must create the `/etc/vmware/view-default-config` and `/etc/vmware/view-mandatory-config` files manually. The `~/.vmware/view-preferences` file is generated automatically after Horizon Client starts up.

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 cannot 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 2-2. 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 Horizon 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 Horizon 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 Horizon Administrator, which by default might be to disconnect after one minute.

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

Configuration Key	Command-Line Option	Description
`view.autoHideToolbar`	None	Specifies whether the toolbar is to be automatically hidden or pinned by default. Specify **"TRUE"** to automatically hide the toolbar. Default is "FALSE". This option can also be set by starting Horizon Client, selecting **File > Preferences** from the menu bar and then selecting the **Auto-hide toolbar** checkbox.
`view.BENITServerConnectionMode`	None	Sets the connection mode to use when connecting to the Horizon Connection Server instance. Use one of the following values: ■ **"T"** to force a TCP connection only. ■ **"U"** to force a UDP connection only. ■ **"4"** to force a connection using an IPv4 address. ■ **"T4"** to force a TCP connection only and use an IPv4 address. ■ **"U4"** to force a UDP connection only and use an IPv4 address. ■ **"bypass"** to use the legacy BEAT connection mode.
`view.BENITTcpConnectCount`	None	Use this value when connecting from an extremely high-loss network (greater than 20% packet loss). Set the default value to **12**. **Important** This option must always be used with the `view.BENITUdpSendCount` configuration key.
`view.BENITUdpSendCount`	None	Use this value when connecting from an extremely high-loss network (greater than 20% packet loss). Set the default value to **12**. **Important** This option must always be used with the `view.BENITTcpConnectCount` configuration key.
`view.defaultAppHeight`	None	Specifies the default height of the window for remote applications, in pixels. Use this property and `view.defaultAppWidth` when specifying a custom desktop size (`view.defaultAppSize` property is set to "5"). Default is "480".

Table 2-2. 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 and 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. The value specified is the name you can 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 Horizon desktop, in pixels. Use this property and view.defaultDesktopWidth when specifying a custom desktop size (view.defaultDesktopSize property is set to "5").

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

Configuration Key	Command-Line Option	Description

`view.defaultDesktopSize`	`--desktopSize=`	Sets the default size of the window for the Horizon 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"`

`view.defaultDesktopWidth`	None	Specifies the default width of the window for the Horizon desktop, in pixels. Use this property and `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.

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

Configuration Key	Command-Line Option	Description
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 if Horizon Connection Server accepts password authentication, adds the password to the **Password** field in the authentication dialog box. **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 **"BLAST"** or **"RDP"**. These values are case-sensitive. For example, if you enter **rdp**, the protocol used is the default. Default is the setting specified in Horizon 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.

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

Configuration Key	Command-Line Option	Description
view.enableDataSharing	None	Specifies whether Horizon Client is allowed to share anonymous data on your client system. Set the value to **"TRUE"** or **"FALSE"**. Default is "TRUE".
view.enableDisplayScaling	None	Specifies whether the display scaling feature is enabled for all remote desktops. Set the value to **"TRUE"** or **"FALSE"**. When this setting is set to **"FALSE"**, the display scaling feature is disabled for all remote desktops. If this setting is not configured or is set to **"TRUE"** (the default setting), display scaling is enabled for all remote desktops.
view.enableH264	None	Enables or disables H.264 decoding. Specify **"TRUE"** or **"FALSE"**. Default is "TRUE". See Configure VMware Blast Options for more information.
view.enableMMR	None	Enables or disables multimedia redirection (MMR). Specify **"TRUE"** or **"FALSE"**. Default is "FALSE".
view.enableRelativeMouse	None	Specifies whether to force enable or disable the Horizon Client relative mouse feature for the current remote desktop session. If you set the configuration key, specify **"1"** to force enable the feature and **"0"** to force disable it. Any other values are invalid and ignored. The specified value can not be edited during the current remote desktop session. If the remote desktop does not support the relative mouse, this setting is not used. If this setting is not configured (the default setting), end users can enable and disable the relative mouse feature using **Connection > Enable Relative Mouse** from the Horizon Client menu bar.
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 2-2. 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.monitors	--monitors= *numbered list*	Allows you to specify which adjacent monitors to use for Horizon Client. Use --allmonitors (or view.allMonitors) to specify that you want to use a 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" `` To help distinguish which physical monitor is associated with a monitor icon in the client UI, a rectangle is displayed at the top left corner of the physical monitor you had specified to use. The rectangle has the corresponding color and number that is used in the icon for the selected monitor.

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

Configuration Key	Command-Line Option	Description
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 out of, reset, or disconnect from a Horizon 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"`
view.once	--once	Specifies that you do not want Horizon Client to retry connecting if an error is occurring. 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"`

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

Configuration Key	Command-Line Option	Description
None	`-r`, `--redirect=`	(Available if you use the Microsoft RDP display protocol.) Specifies a local device that you want rdesktop to redirect to the Horizon 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 and any applicable patches. For more information, see Install and Configure FreeRDP.
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 them 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 Horizon 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 Horizon desktop. Default is "FALSE". This option has a higher priority than the setting in the `/etc/vmware/view-keycombos-config` file.

Table 2-2. 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 "PCoIP Keyboard Settings" in the "Configuring Policies for Desktop and Application Pools" chapter of the *Configuring Remote Desktop Features in Horizon 7* document. This option has a lower priority than the setting in the `/etc/vmware/view-keycombos-config` file.
`view.shareRemovableStorage`	None	When set to **"TRUE"**, enables the **Allow access to removable storage** option. Default is "TRUE".
`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 is "!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES".
`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 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 is "TLSv1.1:TLSv1.2".
`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".

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

Configuration Key	Command-Line Option	Description
view.UnauthenticatedAccessEnabled	--unauthenticatedAccessEnabled	When set to **"TRUE"**, the Unauthenticated Access feature is enabled by default. The **Log in anonymously using Unauthenticated Access** setting is visible in the user interface and is marked as selected. When set to **"FALSE"**, the Unauthenticated Access feature is disabled. The **Log in anonymously using Unauthenticated Access** setting is hidden and deselected. When set to **""**, the Unauthenticated Access feature is disabled, and the **Log in anonymously using Unauthenticated Access** setting is visible from the user interface and deselected. If you are setting the configuration key, specify **"TRUE"** or **"FALSE"**. Examples for using the command-line option: `--unauthenticatedAccessEnabled="TRUE"`
view.UnauthenticatedAccessAccount	--unauthenticatedAccessAccount	Specifies the account to use when `unauthenticatedAccessEnabled` is set to "TRUE". If the `unauthenticatedAccessEnabled` is set to **"FALSE"**, then this configuration is ignored. Example for using the command-line option with the **anonymous1** user account: `--unauthenticatedAccessAccount='anonymous1'`
view.usbAutoConnectAtStartup	--usbAutoConnectAtStartUp=	Automatically redirects USB devices to a Horizon desktop if the USB devices were inserted into the host system before the desktop is connected. This option does not apply to remote applications. Specify **"TRUE"** or **"FALSE"**. Default is **"TRUE"**.
view.usbAutoConnectOnInsert	--usbAutoConnectOnInsert=	Automatically redirects USB devices to a Horizon desktop when the USB devices are inserted into the host system after the desktop is connected. This option does not apply to remote applications. Specify **"TRUE"** or **"FALSE"**. Default is **"TRUE"**.

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

Configuration Key	Command-Line Option	Description
`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 and any applicable patches. For more information, see Install and Configure FreeRDP.

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

Configuration Key	Command-Line Option	Description

None	`--useExisting`	Enables you to start multiple remote desktops and published applications from a single Horizon Client session. When you specify this option, Horizon Client determines whether a session that has the same server URL exists and, if it does, uses that session instead of creating a new session.
		If there already exists a session with a different server URL, Horizon Client disconnects from the existing session and then creates a new session with the new server URL. If more than one such session exists, Horizon Client disconnects from the earliest session before creating the new session.
		In the following example, user1 starts the Calculator application and a new session is created.
		`vmware-view -serverURL view.mycompany.com -userName user1 -password 'secret' -domainName domain -appName Calculator`
		In the next example, user1 starts the Paint application with the same server URL, and the same session is used.
		`vmware-view -serverURL view.mycompany.com -userName user1 -password 'secret' -domainName domain -appName Paint --useExisting`
		In the next example, user1 starts the Calculator application with a different server URL. Horizon Client disconnects from the first session with **`view.mycompany.com`** and creates a new session with **`horizon.mycompany.com`**.
		`vmware-view -serverURL horizon.mycompany.com -userName user1 -password 'secret' -domainName domain -appName Calculator --useExisting`

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

Configuration Key	Command-Line Option	Description
None	`--enableNla`	(Applies if you are using FreeRDP for RDP connections.) Enables network-level authentication (NLA). You must use this option and the `--ignore-certificate` option. For more information, see Using FreeRDP for RDP Connections. NLA is turned off by default if you are using FreeRDP. You must have the correct version of FreeRDP installed and any applicable patches. For more information, see Install and Configure FreeRDP. **Note** The `rdesktop` program does not support NLA.
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=`	Specifies which options to use for USB redirection. See System Requirements for USB Redirection.
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 Horizon 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 Horizon Connection Server instance and perform several procedures documented in the chapter about kiosk mode in the *Horizon 7 Administration* document. After you set up kiosk mode, you can use the `vmware-view` command on a Linux client to connect to a Horizon desktop in kiosk mode.

To connect to Horizon 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 Horizon 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, 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 Horizon Connection Server instance and Horizon 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 Horizon 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 Horizon desktop, the user must acknowledge the message before being allowed to access the desktop. To avoid this issue, use Horizon Administrator to disable pre-login messages.

Using URIs to Configure Horizon Client

You can use uniform resource identifiers (URIs) to create Web page or email links that end users can click to start Horizon Client, connect to a server, or open a remote desktop or published application.

You create these links by constructing URIs that provide some or all the following information, so that your end users do not need to supply it.

- Server address

- Port number for the server
- Active Directory user name
- Domain name
- Remote desktop or published application display name
- Window size
- Actions including reset, log out, and start session
- Display protocol

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

To use URIs to start Horizon Client, Horizon Client must already be installed on client computers.

Syntax for Creating vmware-view URIs

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

URI Specification

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

Use the following syntax to create URIs to start Horizon Client.

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

The only required element is the URI scheme, `vmware-view`. Because the scheme name is case-sensitive for some versions of some client operating systems, type `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 Server address and, optionally, a user name, a non-default port number, or both. 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
```

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

Remote desktop or published application. Use the remote desktop display name or published application display name. This value is the name that is specified in Horizon Administrator when the desktop or application pool was created. If the display name contains a space, use the **`%20`** encoding mechanism to represent the space.

query-part

Configuration options to use, or the remote desktop or published application actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If the queries conflict, Horizon Client uses the last query in the list. Use the following syntax.

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

Supported Queries

The following queries 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 installation and setup guide for each type of client system for the list of supported queries.

action

Table 2-3. Values That Can Be Used with the action Query

Value	Description
`browse`	Displays a list of available remote desktops and published applications hosted on the specified server. You are not required to specify a remote desktop or published application when using this action.
`start-session`	Opens the specified remote desktop or published application. If no action query is provided and the remote desktop or published application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified remote desktop or published application. Unsaved data is lost. Resetting a remote desktop is the same as pressing the Reset button on a physical PC.

Table 2-3. Values That Can Be Used with the action Query (Continued)

Value	Description
`restart`	Shuts down and restarts the specified remote desktop. Restarting a remote desktop is the same as the Windows operating system restart command. The operating system usually prompts the user to save any unsaved data before it restarts.
`logoff`	Logs the user out of the guest operating system in the remote desktop. If you specify a published application, the action is ignored or the end user sees the warning message "Invalid URI action."

args

Specifies command-line arguments to add when the published application starts. Use the syntax `args=`*value*, where *value* is a string. Use percent encoding for the following characters:

- For a colon (:), use **%3A**
- For a back slash (\), use **%5C**
- For a space ( ), use **%20**
- For a double quotation mark ("), use **%22**

For example, to specify the filename "`My new file.txt`" for the Notepad ++ application, use **%22My%20new%20file.txt%22**.

appProtocol

For published applications, valid values are **PCOIP** and **BLAST**. For example, to specify PCoIP, use the syntax **appProtocol=PCOIP**.

desktopLayout

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

Table 2-4. Valid Values for the desktopLayout Query

Value	Description
`fullscreen`	Full screen on one monitor. This value 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**.

domainName

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

useExisting	If this option is set to **true**, only one Horizon Client instance can run. If users try to connect to a second server, they must log out of the first server, causing remote desktop and published application sessions to be disconnected. If this option is set to **false**, multiple Horizon Client instances can run and users can connect to multiple servers at the same time. The default is **true**. An example of the syntax is **useExisting=false**.
unauthenticatedAccessEnabled	If this option is set to **true**, the Unauthenticated Access feature is enabled by default. The **Log in anonymously using Unauthenticated Access** option is visible in the user interface and is selected. If this option is set to **false**, the Unauthenticated Access feature is disabled. The **Log in anonymously using Unauthenticated Access** setting is hidden and disabled. When this option is set to **""**, the Unauthenticated Access feature is disabled and the **Log in anonymously using Unauthenticated Access** setting is visible from the user interface and deselected. An example of the syntax is **unauthenticatedAccessEnabled=true**.
unauthenticatedAccessAccount	If the Unauthenticated Access feature is enabled, sets the account to use. If Unauthenticated Access is disabled, then this query is ignored. An example of the syntax using the **anonymous1** user account is **unauthenticatedAccessAccount=anonymous1**.

Examples of vmware-view URIs

You can use the `vmware-view` URI scheme to create hypertext links or buttons and include these links in email or on a Web page. For example, an end user can click a URI link to start a remote desktop with the startup options that 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 starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the display name `Primary Desktop`, and the user is logged in to the guest operating system.

Note In this example, the default display protocol and window size are used. The default display protocol is PCoIP and the default window size is full screen.

You can change the defaults. See Using the Horizon Client Command-Line Interface and Configuration Files.

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 the Connection Server instance. (The default port is 443.) Because a remote desktop identifier is provided, the remote desktop opens, 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 starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`. The user must supply the domain name and password. After a successful login, the client connects to the remote desktop that has the display name `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 starts and connects to the `view.mycompany.com` server. In the login dialog box, the user must supply the user name, domain name, and password. After a successful login, the client connects to the published application that has the display name `Calculator`. The connection uses the VMware Blast display protocol.

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

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `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 remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system.

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

Horizon Client starts 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 starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client shows a dialog box that prompts the user to confirm the reset operation for `Primary Desktop`.

Note This action is available only if a Horizon administrator has enabled the reset feature for the remote desktop.

8
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client shows a dialog box that prompts the user to confirm the restart operation for `Primary Desktop`.

Note This action is available only if a Horizon administrator has enabled the restart feature for the remote desktop.

9
```
vmware-view://
```

Horizon Client starts and the user is taken to the page for entering the address of a server.

10
```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

Starts My Notepad++ on server 10.10.10.10 and passes the argument `My new file.txt` in the published application start command. The filename is enclosed in double quotes because it contains spaces.

11
```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Starts Notepad++ 12 on server 10.10.10.10 and passes the argument `a.text b.txt` in the published application start command. Because the argument is not enclosed in quotes, a space separates the filenames and the two files are opened separately in Notepad++.

Note Published applications can differ in the way that they use command-line arguments. For example, if you pass the argument `a.txt b.txt` to WordPad, WordPad opens only one file, `a.txt`.

12
```
vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1
```

Horizon Client starts and connects to the `view.mycompany.com` server using the **`anonymous1`** user account. The Notepad application starts without prompting the user to provide login credentials.

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 the hypertext link labeled **Test Link** and a button labeled **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>
```

Configuring the Certificate Checking Mode for End Users

You can configure the certificate checking mode for end users. For example, you can configure that full verification is always performed. Certificate checking occurs for TLS connections between a server and Horizon Client.

You can configure one of the following certificate verification strategies for end users.

- End users are allowed to select the certificate checking mode in Horizon Client.
- (No verification) No certificate checks are performed.
- (Warn) If the server presents a self-signed certificate, end users are warned. Users can determine whether to allow this type of connection.
- (Full security) Full verification is performed and connections that do not pass full verification are rejected.

For information about the types of certificate checks that can be performed, see Setting the Certificate Checking Mode in Horizon Client.

To set the default certificate checking mode, set the `view.sslVerificationMode` key in the `/etc/vmware/view-mandatory-config` file on the Linux client to one of the following values.

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

To configure the certificate checking mode so that end users cannot change it, 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.

Configuring Advanced TLS Options

You can select the security protocols and cryptographic algorithms that are used to encrypt communications between Horizon Client and servers, and between Horizon Client and the agent in a 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-bit or 256-bit AES, remove anonymous DH algorithms, and then sort the current cipher list in order of encryption algorithm key length.

By default, TLS v1.1 and TLS v1.2 are enabled. SSL v2.0, SSL v3.0, and TLS v1.0 are not supported.

If you configure a security protocol for Horizon Client that is not enabled on the server to which the client connects, a TLS error occurs and the connection fails.

Important At least one of the protocols that you enable in Horizon Client must also be enabled on the remote desktop or 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 and look up the property and option names in the table in Horizon Client Configuration Settings and Command-Line Options.

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.

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.

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 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 the following patch commands:

```
cd /client-installation-directory/patches/FreeRDP-stable-1.1
patch -p1 < freerdp-1.1.0.patch
patch -p1 < freerdp-1.1.0-tls.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. The `freerdp-1.1.0-tls.patch` file enables the TLSv1.2 connection in `xfreerdp`. If you have installed the VMware Horizon Client for Linux, the `freerdp-1.1.0.patch` and `freerdp-1.1.0-tls.patch` files are located in the `/usr/share/doc/vmware-horizon-client/patches` directory. 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 if you use VMware Blast or PCoIP.

Enabling FIPS Compatible Mode

You can enable FIPS (Federal Information Processing Standard) Compatible mode so that the client uses FIPS-compliant cryptographic algorithms when communicating with remote desktops.

Note FIPS Compatible Mode means Horizon Client for Linux implements a cryptographic module that is designed for FIPS 140-2 compliance. This module was validated in operational environments listed in CMVP certificate #2839 and was ported to this platform. However, the CAVP and CMVP testing requirement to include the new operational environments in VMware's NIST CAVP and CMVP certificates remains to be completed on the product roadmap.

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

To enable FIPS Compatible 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 value that is less than the amount of available memory divided by 2, the value is rounded to the nearest multiple of 10. The minimum value is 50. Any value that is less than 50 is ignored.

If you specify a value that is larger than the available memory divided by 2, the value is set to the amount of available memory divided by 2 and 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 Published Application Connections

3

End users can use Horizon Client to connect to a server, log in to or off of remote desktops, and use published applications. For troubleshooting purposes, end users can also restart and reset remote desktops and reset published applications.

Depending on how you configure policies, end users might be able to perform many operations on their remote desktops and published applications.

This chapter includes the following topics:

Connect to a Remote Desktop or Published Application

After logging in to a server, you can connect to the remote desktops and published 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 Connection Server 6.0 or later.

Prerequisites

- Obtain login credentials, 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 might use `mycompany` rather than `mycompany.com`.
- Perform the administrative tasks described in Preparing Connection Server for Horizon Client.

- If you are outside the corporate network and require a VPN connection to access remote desktops and published applications, verify that the client device is set up to use a VPN connection and turn on that connection.
- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or published application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.
- 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. For information, see the *Configuring Remote Desktop Features in Horizon 7* document.

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. If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Login**.
3. If you are prompted for a user name and password, supply Active Directory credentials.
   a. Type the user name and password of a user who is entitled to use at least one desktop or application pool.

      If the **Domain** drop-down menu is disabled, you must type the user name as **`domain\username`** or **`username@domain.com`**.

   b. (Optional) Select a domain value from the **Domain** drop-down menu.

   c. Click **Login**.
4. If the desktop security indicator turns red and a warning message appears, respond to the prompt.

   Usually, this warning means that the 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.
5. (Optional) To configure display settings for a remote desktop, right-click the remote desktop icon and select **Settings**.

Option	Action
Select a display protocol	If a Horizon administrator has allowed it, use the **Connect Via** drop-down menu to select the display protocol. To use VMware Blast, Horizon Agent 7.0 or later must be installed.
Select a display layout	Use the **Display** drop-down menu to select a window size or to use multiple monitors.

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

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

7 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 set or have the system log you off 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:

- Verify that the security certificate for Connection Server is working properly. If it is not, in Horizon Administrator, you might also see that View Agent or Horizon Agent on desktops is unreachable. These symptoms indicate additional connection problems caused by certificate problems.
- Verify that the tags set on the Connection Server instance allow connections from this user. See the *Horizon 7 Administration* document.
- Verify that the user is entitled to access this desktop or application. See the *Setting Up Published Desktops and Applications in Horizon 7* or *Setting Up Virtual Desktops in Horizon 7* 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.

Connect to Published Applications Using Unauthenticated Access

You can connect to published applications using an unauthenticated access account with Horizon Client.

Before you have end users access their published applications using unauthenticated access, test that you can connect to the published applications from a client device using an unauthenticated access user account.

Prerequisites

- Verify that Horizon 7 version 7.1 or later Connection Server is configured for unauthenticated access.
- Verify that your unauthenticated access users are created in Horizon Administrator. If the default unauthenticated user is the only unauthenticated access user, the Horizon Client connects to the Connection Server with the default user.

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 In the Horizon Client home screen, select **File > Log in anonymously using Unauthenticated Access** from the menu bar, if it is not already selected.

3 Connect to the Connection Server that is configured for unauthenticated access.

- If the server that you need has not yet been added, double-click the **+ Add Server** button, or click the **New Server** button in the menu bar to add a new one. Then enter the name of the Connection Server or a security server, and click **Connect**.
- If the server that you need is displayed in the Horizon Client home screen, right-click the icon for the server and select **Connect** from the context menu.

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

4 In the Server Login dialog box, specify the unauthenticated access account to use.

a Select a user account from the drop-down menu of existing unauthenticated access accounts.

The default user account has `(default)` displayed next to it.

b (Optional) Click **Always use this account** if you want to bypass the Server Login dialog box the next time you connect to the server.

c Click **OK**.

The application selector window appears and displays the published applications that the unauthenticated access account is authorized to use.

Note If you had selected the **Always use this account** option during a previous unauthenticated access login session, you will not be prompted for the account to use for the current unauthenticated access session. To deselect this option, right-click the icon for the server in the Horizon Client home screen, and select **Forget the saved Unauthenticated Access account** from the context menu.

5 To start an application, double-click the application icon.

The application window appears.

6 Exit the application after you are done using it.

The Disconnect from Session dialog box appears asking if you want to disconnect from the server.

If the session timeout specified by your Horizon administrator is reached, the session is automatically disconnected from the server.

Share Access to Local Folders and Drives with Client Drive Redirection

With the client drive redirection feature, you can share folders and drives on the local client system with remote desktops and published applications.

Shared drives can include mapped drives and USB storage devices.

In a Windows remote desktop, shared folders and drives appear in the **This PC** folder or in the **Computer** folder, depending on the Windows operating system version. In a published application, such as Notepad, you can browse to and open a file in a shared folder or drive.

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`

The client drive redirection settings apply to all remote desktops and published applications.

Prerequisites

To share folders and drives with a remote desktop or published application, a Horizon administrator must enable the client drive redirection feature. This task involves 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 the client drive redirection behavior. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

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

Procedure

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

Option	Description
From the desktop and application selector window	Right-click a remote desktop or published 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 remote desktop or published application	Click **Allow** to share, or **Deny** to not share, your home directory.
From within a remote desktop	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 published applications	Click the **Add** button, browse to and select the folder or drive to share, and click **OK**.
	Note If a USB device is already connected to a remote desktop or published application with the USB redirection feature, you cannot share a folder on the USB device.
Stop sharing a specific folder or drive	Select the folder or drive in the Folder list and click the **Remove** button.

Option	Action
Give remote desktops and published applications access to files in your home directory	Select the **Share your home folder:** *home-directory* check box.
Share USB storage devices with remote desktops and published applications	Select the **Allow access to removable storage** check box. The client drive redirection feature shares all USB storage devices inserted in your client system and all FireWire and Thunderbolt-connected external drives automatically. Selecting a specific device to share is not necessary. **Note** USB storage devices already connected to a remote desktop or published application with the USB redirection feature are not shared. If this check box is deselected, you can use the USB redirection feature to connect USB storage devices to remote desktops and published applications.
Do not show the Sharing dialog box when you connect to a remote desktop or published 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 remote desktop or published application. For example, if you log in to a server and connect to a remote desktop, you see the Sharing dialog box. If you then connect to another remote desktop or published application, you do not see the dialog box. To see the dialog box again, you must disconnect from the server and log in again.

What to do next

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

- In a Windows remote desktop, open File Explorer and look in the **This PC** folder, or open Windows Explorer and look in the **Computer** folder, depending on the Windows operating system version.
- In a published application, select **File > Open** or **File > Save As** and navigate to the folder or drive.

The folders and drives that you selected for sharing might use one (or more) of the following naming conventions.

Naming Convention	Example
folder-name on *desktop-name*	jsmith on JSMITH-W03
folder-name (*drive-number*:)	jsmith (Z:)
folder-name on *desktoptop-name* (*drive-number*:)	jsmith on JSMITH-W03 (Z:)

For some Horizon Agent versions, a redirected folder can have two entrances, such as under **Devices and drives** and **Network locations** in Windows 10, and both entrances can appear at the same time. If all the volume labels (from A: through Z:) are already in use, the redirected folder has only one entrance.

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.

Setting the Certificate Checking Mode in Horizon Client

Server certificate checking occurs for connections between Horizon Client and a server. A certificate is a digital form of identification, similar to a passport or a driver's license.

End users can configure a setting in Horizon Client to determine whether Horizon Client connections are rejected if server certificate checking fails.

You can configure the default certificate checking mode and prevent end users from changing it in Horizon Client. For more information, see Configuring the Certificate Checking Mode for End Users.

Server certificate checking 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 information 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 information about importing a root certificate stored in this location, see "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, the 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 the server does not send a thumbprint, you see a warning that the connection is untrusted.

If a Horizon administrator has allowed it, you can set the certificate checking mode. To set the certificate checking mode, start Horizon Client and select **File > Preferences** from the menu bar. You have three choices:

- **Never connect to untrusted servers**. This setting means that you cannot connect to the server if any of the certificate checks fail. An error message lists the checks that failed.
- **Warn before connecting to untrusted servers**. This setting means that you can click **Continue** to ignore the warning if a certificate check fails because the server uses a self-signed certificate. For self-signed certificates, the certificate name is not required to match the server name that you entered in Horizon Client.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

Switch Remote Desktops or Published Applications

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

If you disconnect from a remote desktop without logging off, applications in the remote desktop might remain open. You can also disconnect from a server and leave published applications running.

You can log off from a remote desktop even if you do not have the remote desktop open. This feature has the same result as sending Ctrl+Alt+Del to the remote 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.
Select a different remote desktop on the same server	Select **Desktop > Disconnect** from the menu bar.
Select a remote desktop on a different server	Select **File > Disconnect from server** from the menu bar.

Note A Horizon administrator can configure remote desktops to log off automatically when they are disconnected. In that case, any open applications in the remote desktop are stopped.

- Log off and disconnect from a remote desktop.

Option	Action
From within the remote desktop	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 are 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 are closed without being saved first.

Using a Microsoft Windows Desktop or Application on a Linux System

4

Horizon Client for Linux provides a familiar, personalized desktop and application environment. End users can access USB and other devices connected to their local computer, send documents to any printer that their local computer can detect, authenticate with smart cards, and use multiple display monitors. .

This chapter includes the following topics:

Feature Support Matrix for Linux Clients

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.

Table 4-1. Features Supported for Windows Virtual Desktops

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 2008/2012 R2 or Windows Server 2016, or Windows Server 2019 Desktop
USB redirection	Limited	Limited	X	X	X	X
Real-Time Audio-Video (RTAV)	Limited	Limited	X	X	X	X
Scanner redirection		Limited	X	X	X	X
Serial port redirection						
RDP display protocol	Limited	Limited	X	X	X	X
PCoIP display protocol	Limited	Limited	X	X	X	X
VMware Blast display protocol			X	X	X	X
Persona Management						
Windows Media MMR			X	X	X	
Location-based printing	Limited	Limited	X	X	X	X
Virtual printing	Limited	Limited	X	X	X	X
Smart cards	Limited	Limited	X	X	X	X
RSA SecurID or RADIUS	Limited	Limited	X	X	X	X
Single sign-on	Limited	Limited	X	X	X	X
Multiple monitors	Limited	Limited	X	X	X	X
Client Drive Redirection			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. Windows Server 2016 desktops require Horizon Agent 7.0.2 or later.

VMware Blast requires 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 Horizon 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 Horizon Connection Server 6.1.

Feature Support for Published 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 remote 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.x and later.

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

Feature	Windows Server 2008 R2 RDS Host	Windows Server 2012 R2 RDS Host	Windows Server 2016 RDS Host	Windows Server 2019 RDS Host
RSA SecurID or RADIUS	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Smart card	View Agent 6.1 and later	View Agent 6.1 and later	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Single sign-on	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
RDP display protocol	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
PCoIP display protocol	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
VMware Blast display protocol	Horizon Agent 7.0 and later	Horizon Agent 7.0 and later	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
HTML Access	View Agent 6.0.2 and later (virtual machine only)	View Agent 6.0.2 and later (virtual machine only)	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Windows Media MMR	View Agent 6.1.1 and later	View Agent 6.1.1 and later	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
USB redirection		View Agent 6.1 and later	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Client drive redirection	View Agent 6.1.1 and later	View Agent 6.1.1 and later	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later

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

Feature	Windows Server 2008 R2 RDS Host	Windows Server 2012 R2 RDS Host	Windows Server 2016 RDS Host	Windows Server 2019 RDS Host
Virtual Printing	View Agent 6.0.1 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	View Agent 6.0.1 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.0.2 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.7 and later
Location-based printing	View Agent 6.0.1 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	View Agent 6.0.1 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.0.2 through Horizon Agent 7.6 (virtual machine only) Horizon Agent 7.7 and later (virtual machine and physical machine)	Horizon Agent 7.7 and later
Multiple monitors	X	X	Horizon Agent 7.0.2 and later	Horizon Agent 7.7 and later
Real-Time Audio-Video (RTAV)	Horizon Agent 7.0.2 and later	Horizon Agent 7.0.2 and later	Horizon Agent 7.0.3 and later	Horizon Agent 7.7 and later

For information about which editions of each guest operating system are supported, see the *Horizon 7 Installation* document.

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	Requires the VMware Blast or PCoIP display protocol, and View Agent 6.0.2 or later .
Virtual printing and location-based printing for Windows Server 2008 R2 desktops, RDS desktops (on virtual machine RDS hosts), and remote applications	■ For client software from third-party vendors, this feature requires Horizon 6.0.1 or later. ■ For Horizon Client from VMware, this feature requires View Agent 6.0.2 or later. Requires the VMware Blast or PCoIP display protocol.
USB redirection	Requires the VMware Blast or PCoIP display protocol, and View Agent 6.0.2 or later .
Smart cards	For single-user virtual machine desktops, this feature requires View Agent 6.0.2 or later. For session-based desktops provided by RDS hosts, this feature requires View Agent 6.1 or later.

Table 4-3. Requirements for Specific Features (Continued)

Feature	Requirements
Scanner redirection	Requires the VMware Blast or PCoIP display protocol and Horizon Agent 7.8 or later.
Client drive redirection	View Agent 6.1.1 or 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 host, which provides published applications and published desktops, see the *Horizon 7 Installation* document.

Note The vendor and model of each thin client device and the configuration that an enterprise chooses to use determine the features that are available for the device. 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 *Horizon 7 Planning* document.

Feature Support for Linux Desktops

Some Linux guest operating systems are supported if you have View Agent 6.1.1 or later. For a list of the latest supported Linux operating systems and information about supported features, see the *Setting Up Horizon 7 for Linux Desktops* document.

Internationalization

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

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 appears 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 appears 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 an 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 into the client system while Horizon Client is running, you must restart Horizon Client 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 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 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 and Windows Aero disabled)	3
11	7 (3D rendering feature enabled)	1
11	8, 8.x, 10	1
13 or 14	8, 8.x, 10	3
13 or 14	8, 8.x, 10 (3D rendering feature enabled)	1

  For the best performance, the virtual machine should have at least 2 GB of RAM and 2 vCPUs. This feature might require good network conditions, such as a bandwidth of 1000 Mbps 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

Generally, 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 Horizon 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 *Configuring Remote Desktop Features in Horizon 7* 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, it is a good practice to turn off the screen saver on a remote desktop and avoid specifying a sleep timer.

Use Display Scaling

Users that have poor eyesight or high-resolution screens, such as 4K monitors, generally have scaling enabled by setting the DPI (Dots Per Inch) on the client system to greater than 100 percent. The DPI setting controls the size of the text, apps, and icons. A lower DPI setting makes them appear smaller and a higher setting makes them appear bigger. With the Display Scaling feature, remote desktops support the client machine's scaling setting and appear normal-sized rather than very small.

Note The DPI Scaling feature is not supported on Raspberry Pi devices and does not work with published applications.

In a multiple-monitor setup, using display scaling does not affect the number of monitors and the maximum resolutions that Horizon Client supports. When display scaling is allowed and is in effect, scaling is based on the DPI setting of the system.

This procedure describes how to use one of the configuration files to enable or disable display scaling for all remote desktops.

Procedure

1. Open the `~/.vmware/view-preferences`, `/etc/vmware/view-default-config`, or `/etc/vmware/view-mandatory-config` configuration file in a text editor.
2. Set the `view.enableDisplayScaling` configuration key.

   Set the value to **`"TRUE"`** or **`"FALSE"`**. When this setting is set to **`"FALSE"`**, the display scaling feature is disabled for all remote desktops. If this setting is not configured or is set to **`"TRUE"`** (the default setting), display scaling is enabled for all remote desktops.
3. Save your changes and close the file.

Using DPI Synchronization

The DPI Synchronization feature ensures that the DPI setting in a remote desktop or published application matches the client system's DPI setting.

Note The DPI synchronization feature is not supported on Raspberry Pi devices.

When the DPI Synchronization feature and the Display Scaling feature are both enabled, only one feature takes effect at any given time. Display scaling occurs only when DPI synchronization has not yet taken effect (that is, before the DPI setting on the remote desktop matches the DPI setting on the client system), and display scaling stops working after the DPI settings match.

The **DPI Synchronization** agent group policy setting determines whether the DPI Synchronization feature is enabled. The feature is enabled by default. With DPI Synchronization, the DPI value in the remote session changes to match the DPI value of the client machine when you connect to a remote desktop or published application. The DPI Synchronization feature requires Horizon Agent 7.0.2 or later.

If the **DPI Synchronization Per Connection** agent group policy setting is enabled in addition to the **DPI Synchronization** group policy setting, DPI Synchronization is supported when you reconnect to a remote desktop. This feature is disabled by default. The DPI Synchronization Per Connection feature requires Horizon Agent 7.8 or later.

For more information about the **DPI Synchronization** and **DPI Synchronization Per Connection** group policy settings, see the *Configuring Remote Desktop Features in Horizon 7* document.

For virtual desktops, the DPI Synchronization feature is supported on the following guest operating systems:

- 32-bit or 64-bit Windows 7
- 32-bit or 64-bit Windows 8.x
- 32-bit or 64-bit Windows 10
- Windows Server 2008 R2 configured as a desktop
- Windows Server 2012 R2 configured as a desktop
- Windows Server 2016 configured as a desktop
- Windows Server 2019 configured as a desktop

For published desktops and published applications, the DPI Synchronization feature is supported on the following RDS hosts:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

For virtual desktops, the DPI Synchronization Per Connection feature is supported on the following guest operating systems:

- Windows 10 version 1607 and later
- Windows Server 2016 and later configured as a desktop

The DPI Synchronization Per Connection feature is not supported for published desktops or published applications.

Following are tips for using the DPI Synchronization feature.

- If you change the DPI setting on the client system, but the DPI setting does not change in the remote desktop, you might need to log out and log in again to make Horizon Client aware of the new DPI setting on the client system.
- If you start a remote session on a client system that has a DPI setting of more than 100 percent, and then use the same session on another client system that has a different DPI setting of more than 100 percent, you might need to log out and log back in to the remote session on the second client system to make DPI synchronization work on the second client system.
- If a Horizon administrator changes the **DPI Synchronization** group policy setting value for Horizon Agent, you must log out and log in again to make the new setting take effect.

Use USB Redirection to Connect USB Devices

With the USB redirection feature, you can use locally attached USB devices, such as thumb flash drives, in a remote desktop or published application.

When you use the USB redirection feature, most USB devices that are attached to the local client system become available from menus in Horizon Client. You can use the menus to connect and disconnect the devices.

With View Agent 6.1 and later, or Horizon Agent 7.0 and later, you can redirect locally connected USB thumb flash drives and hard disks for use in published desktops and applications. Beginning with Horizon Agent 7.0.2, published desktops and applications can also support more generic USB devices, including TOPAZ Signature Pad, Olympus Dictation Foot pedal, and Wacom signature pad. Other types of USB devices, including security storage drives and USB CD-ROM drives, are not supported in published desktops and applications.

You can connect USB devices to a remote desktop or published application either manually or automatically.

Important This procedure describes how to use Horizon Client to configure auto-connection of USB devices to a remote desktop or published application. You can also configure USB redirection by using a configuration file or by creating a group policy. For more information about using a configuration file, see Chapter 5 Configuring USB Redirection on the Client. For more information about creating group policies, see the *Setting Up Desktop and Application Pools in Horizon 7* document.

Prerequisites

- To use USB devices with a remote desktop or published application, a Horizon administrator must enable the USB feature.

  This task includes installing the USB Redirection component of Horizon Agent, and can include setting policies regarding USB redirection. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document and Setting USB Configuration Properties.
- The USB Redirection component must be installed in Horizon Client. If you did not include this component in the installation, uninstall the client and run the installer again to include the USB Redirection component.
- Become familiar with USB Redirection Limitations

Procedure

- Manually connect a USB device to a remote desktop.
  a Connect the USB device to your local client system.
  b From the Horizon Client menu bar, click **Connect USB Device**.
  c Select the USB device.

  The device is manually redirected from the local system to the remote desktop.

- Connect the USB device to a published application.
  a In the desktop and application selector window, open the remote application.

    The name of the application is the name that your administrator has configured for the application.

  b In the desktop and application selector window, right-click the application icon and select **Settings**.

  c In the left pane, select **USB Devices**.

  d In the right pane, select the USB device and click **Connect**.

  e Select the application, and click **OK**.

    Note The name of the application in the list comes from the application itself and might not match the application name that your administrator configured to appear in the desktop and application selector window.

    You can now use the USB device with the remote application. After you close the application, the USB device is not released right away.

  f When you are finished using the application, to release the USB device so that you can access it from your local system, in the desktop and application selector window, open the Settings window again, select **USB Devices**, and select **Disconnect**.

- Configure Horizon Client to connect USB devices automatically to the remote desktop when Horizon Client starts.

  This option is selected by default.

  a Before you plug in the USB device, start Horizon Client and connect to a remote desktop.

  b From the Horizon Client menu bar, click **Connect USB Device**.

  c Select **Automatically Connect at Startup**.

  d Plug in the USB device and restart Horizon Client.

  USB devices that you connect to your local system after you start Horizon Client are redirected to the remote desktop. USB devices that you connect to your local system after you start Horizon Client are redirected to the remote desktop.

- Configure Horizon Client to connect USB devices automatically to the remote desktop when you plug them in to the local system.

  Enable this option if you plan to connect devices that use MTP drivers, such as Android-based Samsung smart phones and tablets. This option is selected by default.

  a Before you plug in the USB device, start Horizon Client and connect to a remote desktop.

  b From the Horizon Client menu bar, click **Connect USB Device**.

c Select **Automatically Connect when Inserted**.

d Plug in the USB device.

USB devices that you connect to your local system after you start Horizon Client are redirected to the remote desktop.

You can also configure automatically connecting USB devices using the configuration file options `view.usbAutoConnectAtStartup` and `view.usbAutoConnectOnInsert` For more information, see Horizon Client Configuration Settings and Command-Line Options..

If the USB device does not appear in the remote desktop or published application after several minutes, disconnect and reconnect the device to the client computer.

What to do next

If you have problems with USB redirection, see the topic about troubleshooting USB redirection problems in the *Configuring Remote Desktop Features in Horizon 7* document.

USB Redirection Limitations

The USB redirection feature has certain limitations.

- When you access a USB device from a menu in Horizon Client and use the device in a remote desktop, you cannot access the device on the local computer.
- USB devices that do not appear in the menu, but are available in a remote desktop, include human interface devices such as keyboards and pointing devices. The remote desktop and the local computer use these devices at the same time. Interaction with these devices can sometimes be slow because of network latency.
- Large USB disk drives can take several minutes to appear in the remote desktop.
- Some USB devices require specific drivers. If a required driver is not already installed on a remote desktop, you might be prompted to install it when you connect the USB device to the remote desktop.
- If you plan to attach USB devices that use MTP drivers, such as Android-based Samsung smart phones and tablets, configure Horizon Client so that it automatically connects USB devices to the remote desktop. Otherwise, if you try to manually redirect the USB device by using a menu item, the device is not redirected unless you unplug the device and then plug it in again.
- Do not connect to scanners by using the **Connect USB Device** menu. To use a scanner device, use the scanner redirection feature. This feature is available for Horizon Client when used with Horizon Agent 7.8 or later. See Using Scanners.
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle. Audio input and output devices work well with the Real-Time Audio-Video feature. You do not need to use USB redirection for those devices.

- You cannot format a redirected USB drive in a published desktop unless you connect as an administrator user.

Note Do not redirect USB devices such as USB Ethernet devices and touch screen devices to a remote desktop or published application. If you redirect a USB Ethernet device, your client system loses network connectivity. If you redirect a touch screen device, the remote desktop or published application receives touch input but not keyboard input. If you have set the remote desktop or published application to autoconnect USB devices, you can configure a policy to exclude specific devices. See "Configuring Filter Policy Settings for USB Devices" in the *Configuring Remote Desktop Features in Horizon 7* document.

Using Scanners

With the scanner redirection feature, you can scan information into remote desktops with scanners that are connected to the local client system. You can control scanner settings by selecting options in the remote desktop interface. This feature redirects scanning data with a significantly lower bandwidth than can be achieved by using USB redirection.

Scanner redirection supports scanning devices that are compatible with the SANE interface standard. Although you must have the SANE scanner device drivers installed on the local client system, you do not need to install the scanner device drivers on the remote desktop operating system where the agent is installed.

If a Horizon administrator has configured the scanner redirection feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, a scanner connected to your local system can be used in a remote desktop.

Important Do not connect a scanner from the **Connect USB Device** menu in Horizon Client. The performance will be unusable.

When scanning data is redirected to a remote desktop, you cannot access the scanner on the local computer. Conversely, when a scanner is in use on the local computer, you cannot access it on the remote desktop.

Note When you connect a scanner to a USB port on the local computer, Horizon Client sends scanning data to the remote desktop through USB redirection by default. To send data through scanner redirection instead, configure a USB redirection policy to exclude your scanning device. For more information, see Setting USB Configuration Properties.

Tips for Using the Scanner Redirection Feature

- Click the scanner icon () in the system tray, or notification area, of the remote desktop to select a non-default scanner or to change configuration settings.

You do not have to use the menu that appears when you click this icon. Scanner redirection works without any further configuration. The icon menu allows you to configure options such as changing which device to use if more than one device is connected to the local client computer.

Note If the menu that appears does not list any scanners it means that an incompatible scanner is connected to the client computer. If the scanner icon is not present, it means that the scanner redirection feature is disabled or not installed on the remote desktop. The scanner icon also does not appear on client systems that do not support this feature.

- Click the **Preferences** option in the menu to select options to hide webcams from the scanner redirection menu and determine how to select the default scanner.

  You can select the option to hide webcams if you plan to use the Real-Time Audio-Video feature to redirect webcams, which is what VMware recommends. Use scanner redirection with webcams to take a photograph of yourself and scan it.

  Note If a Horizon administrator has configured scanner redirection to use a specific scanner and that scanner is not available, scanner redirection will not work.

- Although most scanners display a scanner settings dialog box by default, some do not. For those that do not display settings options, you can use the **Preferences** option in the scanner icon menu, and select **Always show Scanner Settings dialog** option.
- Scanning too large an image or scanning at too high a resolution might not work. In this case, you might see the scanning progress indicator freeze, or the scanner application might exit unexpectedly. If you minimize the remote desktop, an error message might appear on the local client system, notifying you that the resolution is set too high. To resolve this issue, reduce the resolution or crop the image to a smaller size and scan again.

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

With the Real-Time Audio-Video feature, you can use the local client system's webcam or microphone in a remote desktop or published application. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications. It 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 on the agent machine, see the *Configuring Remote Desktop Features in Horizon 7* document. 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. Because this test application is available as a VMware fling, technical support is not available.

Note This feature is available only with the version of Horizon Client for Linux provided by third-party vendors or with the Horizon Client software available from the VMware Product Downloads website.

When You Can Use a Webcam

If a Horizon administrator has configured the Real-Time Audio-Video feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, you can use a webcam that is built in or connected to the local client computer in a remote desktop or published application. 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 a remote desktop, you can select input and output devices from menus in the application. For virtual desktops, you can select VMware Virtual Microphone and VMware Virtual Webcam. For published desktops and applications, you can select Remote Audio Device and VMware Virtual Webcam.

For many applications, you do not need to select an input device.

When the local client computer uses the webcam, the remote session cannot use it at the same time. Also, when the remote session uses the webcam, the local client computer cannot use it at the same time.

Important If end users use USB webcams, do not configure the client to forward devices through USB redirection automatically. If the webcam connects through USB redirection, the performance is not usable for video chat.

If more than one webcam is connected to the local client computer, you can configure a preferred webcam to use in remote sessions.

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 remote 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.

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 remote desktop. To specify which webcam and microphone are preferred, you can edit a configuration file.

The preferred webcam or microphone is used on the remote 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 values of certain fields. You can search the log file for the values of these fields.

- For webcams, you set the `rtav.srcWCamId` property to the value of the `UserId` field for the webcam and the `rtav.srcWCamName` property to the value of the `Name` field for the webcam.

  The `rtav.srcWCamName` property has a higher priority than the `rtav.srcWCamId` property. Both properties should specify the same webcam. If the properties specify different webcams, the webcam specified by `rtav.srcWCamName` is used, if it exists. If it does not exist, the webcam specified by `rtav.srcWCamId` is used. If both webcams are not found, the default webcam is used.
- For audio devices, you set the `rtav.srcAudioInId` property to the value of the Pulse Audio `device.description` field.

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` and `Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6` to specify the Microsoft webcam as the preferred webcam and set the properties as follows:

```
rtav.srcWCamName = “Microsoft® LifeCam HD-6000 for Notebooks”
rtav.srcWCamId = “Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1-3/1-3.6”
```

For this example, you could also set the `rtav.srcWCamId` property to `"Microsoft"`. The `rtav.srcWCamId` property supports both partial and exact matches. The `rtav.srcWCamName` property supports only an exact match.

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.

Using the Session Collaboration Feature

You can use the Session Collaboration feature to invite other users to join an existing remote desktop session.

Invite a User to Join a Remote Desktop Session

When the Session Collaboration feature is enabled for a remote desktop, you can invite other users to join an existing remote desktop session.

By default, you can send Session Collaboration invitations by email, in an instant message (Windows remote desktops only), or by copying a link to the clipboard and forwarding the link to users. To use the email invitation method, an email application must be installed. To use the IM invitation method for a Windows remote desktop, Skype for Business must be installed and configured. You can invite only users that belong to a domain that the server allows for authentication. You can invite up to five users by default.

The Session Collaboration feature has the following limitations.

- If you have multiple monitors, only the primary monitor is shown to session collaborators.
- You must select the VMware Blast display protocol when you create a remote desktop session. The Session Collaboration feature does not support PCoIP or RDP sessions.
- H.264 hardware encoding is not supported. If the session owner is using hardware encoding and a collaborator joins the session, both fall back to software encoding.
- Anonymous collaboration is not supported. Session collaborators must be identifiable through Horizon-supported authentication mechanisms.
- Session collaborators must have Horizon Client 4.7 or later for Windows, Mac, or Linux installed, or they must use HTML Access 4.7 or later.
- If a session collaborator has an unsupported version of Horizon Client, an error message appears when the user clicks a collaboration link.
- You cannot use the Session Collaboration feature to share published application sessions.

Prerequisites

To invite users to join a remote desktop session, a Horizon administrator must enable the Session Collaboration feature.

For Windows desktops, this task includes enabling the Session Collaboration feature at the desktop pool or farm level. It can also include using group policies to configure Session Collaboration features, such as the available invitation methods. For complete requirements, see Requirements for the Session Collaboration Feature.

For information about enabling the Session Collaboration feature for Windows desktops, see the *Setting Up Virtual Desktops in Horizon 7* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon 7* document. For information about using group policy settings to configure the Session Collaboration feature, see the *Configuring Remote Desktop Features in Horizon 7* document.

For information about enabling the Session Collaboration feature for Linux desktops, see the *Setting Up Horizon 7 for Linux Desktops* document.

Procedure

1. Connect to a remote desktop for which the Session Collaboration feature is enabled.

   You must use the VMware Blast display protocol.

2. In the system tray in the remote desktop, click the **VMware Horizon Collaboration** icon, for example,  .

   The collaboration icon might look different, depending on the operating system version.

3 When the VMware Horizon Collaboration dialog box opens, enter the user name (for example, **`testuser`** or **`domain\testuser`**) or the email address of the user that you want to join the remote desktop session.

   The first time you enter the user name or email address of a particular user, you must click **Look up "*user*"**, enter a comma (,), or press the **Enter** key to validate the user. For Windows remote desktops, the Session Collaboration feature remembers the user the next time you enter the user's user name or email address.

   You can invite up to five users by default. A Horizon administrator can change the maximum number of users that you can invite.

4 Select an invitation method.

   Not all invitation methods might be available.

Option	Action
Email	Copies the collaboration invitation to the clipboard and opens a new email message in the default email application. An email application must be installed to use this invitation method.
IM	(Windows remote desktops only) Copies the collaboration invitation to the clipboard and opens a new window in Skype for Business. Press Ctrl+V to paste the link into the Skype for Business window. Skype for Business must be installed and configured to use this invitation method.
Copy Link	Copies the collaboration invitation to the clipboard. You must manually open another application, such as Notepad, and press Ctrl+V to paste the invitation.

After you send an invitation, the VMware Horizon Collaboration icon also appears on the desktop and the Session Collaboration user interface turns into a dashboard that shows the current state of the collaboration session and enables you to take certain actions.

When a session collaborator accepts your invitation to join a Windows remote desktop session, the Session Collaboration feature notifies you and a red dot appears on the VMware Horizon Collaboration icon in the system tray. When a session collaborator accepts your invitation to join a Linux remote desktop session, a notification appears in the primary session desktop.

What to do next

Manage the collaborative session in the VMware Horizon Collaboration dialog box. See Manage a Collaborative Session.

Manage a Collaborative Session

After you send a session collaboration invitation, the Session Collaboration user interface turns into a dashboard that shows the current state of the collaborative session and enables you to take certain actions.

A Horizon administrator can prevent the hand off of control to a session collaborator. For Windows remote desktops, see the **Allow control passing to collaborators** group policy setting in the *Configuring Remote Desktop Features in Horizon 7* document. For Linux remote desktops, see the `collaboration.enableControlPassing` parameter in the *Setting Up Horizon 7 for Linux Desktops* document.

Prerequisites

Start a collaborative session. See Invite a User to Join a Remote Desktop Session.

Procedure

1 In the remote desktop, click the **VMware Horizon Collaboration** icon in the system tray.

The names of all session collaborators appear in the Name column and their status appears in the Status column.

2 Use the VMware Horizon Session Collaboration dashboard to manage the collaborative session.

Option	Action
Revoke an invitation or remove a collaborator	Click **Remove** in the Status column.
Hand off control to a session collaborator	After the session collaborator joins the session, toggle the switch in the Control column to **On**. To resume control of the session, double-click or press any key. The session collaborator can also give back control by toggling the switch in the Control column to **Off**, or by clicking the **Give Back Control** button.
Add a collaborator	Click **Add Collaborators**.
End the collaborative session	Click **End Collaboration**. All active collaborators are disconnected. In Windows remote desktops, you can also end the collaborative session by clicking the **Stop** button next to the **VMware Horizon Session Collaboration** icon. The **Stop** button is not available in Linux remote desktops.

Join a Collaborative Session

To join a collaborative session, you can click the link in a collaboration invitation. The link might be in an email or instant message, or in a document that the session owner forwards to you. Alternatively, you can log in to the server and double-click the icon for the collaborative session in the remote desktop and application selector window.

This procedure describes how to join a collaborative session from a collaboration invitation.

Note In a Cloud Pod Architecture environment, you cannot join a collaborative session by logging in to the server unless you log in to the session owner's pod.

You cannot use the following remote desktop features in a collaborative session.

- USB redirection
- Real-Time Audio-Video (RTAV)

- Multimedia redirection
- Client drive redirection
- Smart card redirection
- Virtual printing
- Clipboard redirection

You cannot change the remote desktop resolution in a collaborative session.

Prerequisites

To join a collaborative session, you must have Horizon Client 4.7 for Windows, Mac, or Linux installed on the client system, or you must use HTML Access 4.7 or later.

Procedure

1. Click the link in the collaboration invitation.

   Horizon Client opens on the client system.

2. Enter your credentials to log in to Horizon Client.

   After you are successfully authenticated, the collaborative session begins and you can see the session owner's remote desktop. If the session owner transfers mouse and keyboard control to you, you can use the remote desktop.

3. To return mouse and keyboard control to the session owner, click the **VMware Horizon Collaboration** icon in the system tray and toggle the switch in the Control column to **Off**, or click the **Give Back Control** button.

4. To leave the collaborative session, click **Options > Disconnect**.

Enable Multi-Session Mode for Published Applications

When multi-session mode is enabled for a published application, you can use multiple sessions of the same published application when you log on to the server from different client devices.

For example, if you open a published application in multi-session mode on client A, and then open the same published application on client B, the published application remains open on client A and a new session of the published application opens on client B. By comparison, when multi-session mode is disabled (single-session mode), the published application session on client A disconnects and reconnects on client B.

The multi-session mode feature has the following limitations.

- Multi-session mode does not work for applications that do not support multiple instances, such as Skype for Business.
- If the application session is disconnected while you are using a published application in multi-session mode, you are logged off automatically and any unsaved data is lost.

Prerequisites

A Horizon administrator must enable multi-session mode for the application pool. Users cannot modify the multi-session mode for a published application unless a Horizon administrator allows it. See *Setting Up Published Desktops and Applications in Horizon 7*. This feature requires Horizon 7 version 7.7 or later.

Procedure

1. Connect to a server.
2. Click the **Settings** button (gear icon) in the upper-right corner of the desktop and application selector window and select **Multi-Launch**.

   If no published applications are available to use in multi-session mode, the **Multi-Launch** setting does not appear.
3. Select the published applications that you want to use in multi-session mode and click **OK**.

   If a Horizon administrator has enforced multi-session mode for a published application, you cannot change this setting.

Using the Seamless Window Feature

With the Seamless Window feature, you can interact with an application that is running on a remote desktop as if it was a locally running application.

Beginning with Horizon Client 4.9 for Linux, the Seamless Window feature is enabled by default and available for all supported Linux systems.

Saving Documents in a Published Application

With certain published 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.

A Horizon administrator can use the RDS Profiles group policy setting called **Set Remote Desktop Services User Home Directory** to specify where documents are saved. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

Set Printing Preferences for the Virtual Printing Feature

You can set printing preferences in a remote desktop for the Virtual Printing feature. With the Virtual Printing feature, you can use local or network printers from a remote desktop without having to install additional printer drivers 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 other settings.

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.

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, 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 client computer, Horizon Client adds that printer to the list of available printers in the remote desktop. No further configuration is required. If you have administrator privileges, you can install printer drivers on the remote desktop without creating a conflict with the Virtual Printing component.

Important This feature is not available for the following types of printers.

- USB printers that use 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 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.

Prerequisites

To use Virtual Printing, a Horizon administrator must enable the Virtual Printing feature in the remote desktop. This task involves enabling the **Virtual Printing** setup option in the agent installer, and can include setting policies that control virtual printing behavior. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document. For information about configuring policies, see the *Configuring Remote Desktop Features in Horizon 7* document.

To determine whether the Virtual Printing feature is installed in a remote desktop, verify that the `C:\Program Files\Common Files\ThinPrint` folder exists in the remote desktop file system.

Procedure

1. In the Windows remote desktop, go to **Control Panel > Hardware and Sound > Devices and Printers**.
2. In the **Devices and Printers** window, right-click the virtual printer and select **Printer properties** from the context menu.

   In a single-user virtual machine desktop, each virtual printer appears as *<printer_name>*. In a published desktop, if View Agent 6.2 or later or Horizon Agent 7.0 or later is installed, each virtual printer appears as *<printer_name>(s<session_ID>)*. If View Agent 6.1 or earlier is installed in the remote desktop, each virtual printer appears as *<printer_name>#:<number>*.
3. On the **General** tab, click **Preferences**.
4. In the Printing Preferences dialog box, select the different tabs and specify which settings to use.
5. To save your changes, click **OK**.

Copying and Pasting Text

You can copy and paste text to and from remote desktops and published applications. A Horizon administrator can configure this feature so that copy and paste operations are allowed only from the client system to a remote desktop or published application, or only from a remote desktop or published application to the client system, or both, or neither.

Copying and pasting from the client system (where Horizon Client is installed) to a remote desktop or published application, and conversely, is the same as copying and pasting between applications on the same system. For example, you can press Ctrl+C to copy text and press Ctrl+V to paste text.

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

A Horizon administrator can configure the ability to copy and paste by using group policy settings that pertain to View Agent or Horizon Agent in remote desktops. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

You can copy text from Horizon Client to a remote desktop or published 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 the client computer.

Configuring the Client Clipboard Memory Size

In Horizon 7 version 7.0.1 and later and Horizon Client 4.1 and later, the clipboard memory size is configurable for both the server and the client.

When a PCoIP or VMware Blast session is established, the server sends its clipboard memory size to the client. The effective clipboard memory size is the lesser of the server and client clipboard memory size values.

To set the client clipboard memory size, add the following parameter to any one of three configuration files: `~/.vmware/config`, `/usr/lib/vmware/config`, or `/etc/vmware/config`.

```
mksvchan.clipboardSize=value
```

value is the client clipboard memory size in kilobytes (KB). You can specify a maximum value of 16384 KB. If you specify 0 or do not specify a value, the default client clipboard memory size is 8192 KB (8 MB).

Horizon Client looks for the clipboard memory size in the configuration files in the following order and stops as soon as a non-zero value is found.

1. `~/.vmware/config`
2. `/usr/lib/vmware/config`
3. `/etc/vmware/config`

A large clipboard memory size can negatively affect performance, depending on your network. VMware recommends that you do not set the clipboard memory size to a value greater than 16 MB.

Logging Copy and Paste Activity

When you enable the clipboard audit feature, Horizon Agent records information about copy and paste activity in an event log on the agent machine. The clipboard audit feature is disabled by default.

To enable the clipboard audit feature, you must configure the **Configure clipboard audit** group policy setting for VMware Blast or PCoIP.

You can optionally configure the **Whether block clipboard redirection to client side when client doesn't support audit** group policy setting for VMware Blast or PCoIP to specify whether to block clipboard redirection to clients that do not support the clipboard audit feature.

For information about configuring these group policy settings, see the "VMware Blast Policy Settings" and "PCoIP Clipboard Settings" topics in the *Configuring Remote Desktop Features in Horizon 7* document.

This feature requires Horizon Agent 7.7 or later on the agent machine.

The event log where information about copy and paste activity is recorded is named VMware Horizon RX Audit. To view the event log on the agent machine, use the Windows event viewer. To view the event log from a centralized location, configure VMware Log Insight or Windows Event Collector. For information about Log Insight, go to https://docs.vmware.com/en/vRealize-Log-Insight/index.html. For information about Windows Event Collector, see the Microsoft documentation.

Enable the Relative Mouse Feature for a Remote Desktop

If you use the VMware Blast display protocol or the PCoIP display protocol when using 3D applications in a remote desktop, mouse performance improves when you enable the relative mouse feature.

In most circumstances, if you are using applications that do not require 3D rendering, Horizon Client transmits information about mouse pointer movements by using absolute coordinates. Using absolute coordinates, the client renders the mouse movements locally, which improves performance, especially if you are outside the corporate network.

For work that requires using graphics-intensive applications, such as AutoCAD, or for playing 3D video games, you can improve mouse performance by enabling the relative mouse feature, which uses relative, rather than absolute, coordinates.

The Horizon Client relative mouse feature is not enabled by default. You can use the `view.enableRelativeMouse` configuration key in the `~/.vmware/view-preferences` file to enable or disable Horizon Client relative mouse and prevent users from changing the setting in the Horizon Client user interface. You must configure the relative mouse setting before end users connect to a server. The setting is applied to the current desktop connection session. If the Horizon Client relative mouse setting is configured using the `~/.vmware/view-preferences` file, end users cannot change the setting after connecting to a server.

When the relative mouse feature is enabled, performance might be slow if you are outside the corporate network, on a WAN.

Prerequisites

A Horizon administrator must turn on 3D rendering for the desktop pool. For information about pool settings and the options available for 3D rendering, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

Procedure

1. Start Horizon Client and log in to the server.
2. Right-click the remote desktop and select **VMware Blast** or **PCoIP**.
3. Connect to the remote desktop.
4. Select **Connection > Enable Relative Mouse** from the Horizon Client menu bar.

   The option is a toggle. To disable the relative mouse feature, select **Connection > Enable Relative Mouse** again.

   Note If you use Horizon Client in windowed mode rather than full-screen mode and the relative mouse feature is enabled, you might not be able to move the mouse pointer to the Horizon Client menu options or move the pointer outside of the Horizon Client window. To resolve this situation, press Ctrl+Alt.

Using Serial Port Redirection

With serial port redirection, you can redirect locally connected serial (/dev/ttyS) ports, such as built-in RS232 ports and USB-to-serial adapters. Devices such as printers, bar code readers, and other serial devices can be connected to these ports and used in RDS-hosted desktops.

If a Horizon administrator has configured the serial port redirection feature, and if you use the VMware Blast display protocol, serial port redirection works in the RDS-hosted desktop without further configuration. For example, /dev/ttyS0 on the local client system is redirected as COM1 on the RDS-hosted desktop. Serial port /dev/ttyS1 is redirected as COM2. If the /dev/ttyS port is already in use, it is mapped to avoid conflicts. For example, if COM1 and COM2 exist on the RDS-hosted desktop, /dev/ttyS0 on the client system is mapped to COM3 by default.

You must have any required device drivers installed on the local client system, but you do not need to install the device drivers on the RDS-hosted desktop. For example, if you use a USB-to-serial adapter that requires specific device drivers to work on your local client system, you must install those drivers, but only on the client system.

Important If you are using a device that plugs in to a USB-to-serial adapter, do not connect the device from the **Connect USB Device** menu in Horizon Client. Doing so routes the device through USB redirection and bypasses the serial port redirection feature.

Tips for Using the Serial Port Redirection Feature

- Click the serial port icon ( ) in the system tray or notification area of the RDS-hosted desktop to connect, disconnect, or customize the mapped /dev/ttyS ports.

  When you click the serial port icon, the **Serial COM Redirection for VMware Horizon** context menu appears. If an administrator has locked the configuration, the items in the context menu are dimmed. The icon appears only if a Horizon administrator has configured the serial port redirection feature and all requirements are met. For more information, see System Requirements for Serial Port Redirection.

- In the context menu, the port items are listed as ***port* mapped to *port***, for example, **/dev/ttyS0 mapped to COM1**. The first port, which is /dev/ttyS0 in this example, is the physical port or the USB-to-serial adapter on the local client system. The second port, which is COM1 in this example, is the port used in the RDS-hosted desktop.

- To select the **Port Properties** command, right-click a /dev/ttyS port.

  In the COM Properties dialog box, you can configure a port to connect automatically when a RDS-hosted desktop session is started, or you can ignore DSR (data-set-ready signal), which is required for some modems and other devices.

  You can also change the port number that the RDS-hosted desktop uses. For example, if the /dev/ttyS0 port on the client system is mapped to COM3 in the RDS-hosted desktop, you can change the port number to COM1. If COM1 exists in the RDS-hosted desktop, you might see **COM1 (Overlapped)**. You can still use this overlapped port. The RDS-hosted desktop can receive serial data through the port from the server and also from the client system.

- Connect to a mapped COM port by selecting **Connect** to use the port in the RDS-hosted desktop.

  When a redirected COM port is opened and in use on a RDS-hosted desktop, you cannot access the port on the local computer. Conversely, when a /dev/ttyS port is in use on the local computer, you cannot access the port on the RDS-hosted desktop.

- You can then select the **Disconnect** command to disconnect and make the physical COM port available for use on the client computer.

Configuring USB Redirection on the Client

5

With the USB redirection feature, you can use a configuration file on the client system to specify which USB devices can be redirected to a remote desktop.

For example, you can 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, and specify whether Horizon Client should split composite USB devices into separate components for redirection.

This chapter includes the following topics:

System Requirements for USB Redirection

The USB redirection feature is available only with certain versions of the client software.

For the Horizon Client software provided by third-party vendors, the USB redirection feature 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 this document 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. 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.

For Horizon Client, the USB redirection feature 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

Horizon Client sends USB information to log files.

To specify the USBD log level, add the following parameter in one of the configuration files.

```
view-usbd.logLevel = "value"
```

Use one of the following values for *value*.

- **trace**
- **info**
- **debug**
- **error**

The configuration files are in the following locations and processed in the order listed:

1 `/etc/vmware/config`

2 `/usr/lib/vmware/config`

3 `~/.vmware/config`

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

1 Stop the USB arbitrator daemon.

```
sudo /etc/init.d/vmware-USBArbitrator stop
```

2 Restart the USB arbitrator daemon using the `verbose` option.

```
sudo /usr/lib/vmware/view/usb/vmware-usbarbitrator -verbose
```

The default USB arbitrator log file is located in `/var/log/vmware/vmware-usbarb-<pid>.log`, where *<pid>* is the process id for the USB arbitrator daemon.

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

```
sudo /usr/lib/vmware/view/usb/vmware-usbarbitrator -h
```

Setting USB Configuration Properties

You can set USB configuration properties in the `/etc/vmware/config`, `/usr/lib/vmware/config`, and `~/.vmware/config` configuration files.

Use the following syntax to set USB configuration properties in the configuration files.

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

With USB configuration properties, you can control whether certain types of devices are redirected. Filtering properties are also available to enable you to include or exclude certain types of devices. For Linux clients version 1.7 and later, and for Windows clients, properties for splitting composite devices are also provided.

Some property 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-<current_user>/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 When redirecting audio devices, make sure that the kernel version of your Ubuntu system is 3.2.0-27.43 or later. 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.

The following table describes the available USB configuration properties.

Table 5-1. 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.

Table 5-1. Configuration Properties for USB Redirection (Continued)

Policy Name and Property	Description
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 5-1. 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.

Table 5-1. Configuration Properties for USB Redirection (Continued)

Policy Name and Property	Description
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.

USB Redirection Examples

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

- 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.

- 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 *Horizon 7 Administration* document.

USB Device Families

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

Note Some devices do not report a device family.

Table 5-2. USB Device Families

Device Family Name	Description
`audio`	Any audio-input or audio-output device.
`audio-in`	Audio-input devices such as microphones.
`audio-out`	Audio-output devices such as loudspeakers and headphones.
`bluetooth`	Bluetooth-connected devices.
`comm`	Communications devices such as modems and wired networking adapters.
`hid`	Human interface devices excluding keyboards and pointing devices.
`hid-bootable`	Human interface devices that are available at startup 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.

Table 5-2. USB Device Families (Continued)

Device Family Name	Description
`video`	Video-input devices.
`wireless`	Wireless networking adapters.
`wusb`	Wireless USB devices.

Troubleshooting Horizon Client 6

You can solve most problems with Horizon Client by restarting or resetting remote desktops or published applications, or by reinstalling Horizon Client.

This chapter includes the following topics:

Restart a Remote Desktop

If the remote desktop operating system stops responding, you might need to restart a remote desktop. Restarting a remote desktop is similar to using the Windows operating system restart command. The remote desktop operating system usually prompts you to save any unsaved data before it restarts.

You can restart a remote desktop only if a Horizon administrator has enabled the restart feature for the remote desktop.

For information about enabling the desktop restart feature, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

Prerequisites

Obtain login credentials, such as a user name and password, RSA SecurID user name and password, RADIUS authentication user name and password, or smart card personal identification number (PIN).

Procedure

- Use the **Restart** command.

Option	Action
From within the desktop	Select **Connection > Restart Desktop** from the menu bar.
From the desktop selection window	Select the remote desktop and select **Connection > Restart Desktop** from the menu bar.

Horizon Client prompts you to confirm the restart action.

The operating system in the remote desktop restarts and Horizon Client disconnects and logs off from the remote desktop.

What to do next

Wait an appropriate amount of time for the system to restart before you attempt to reconnect to the remote desktop.

If restarting the remote desktop does not solve the problem, you might need to reset the remote desktop. See Reset a Remote Desktop or Published Applications.

Reset a Remote Desktop or Published Applications

You might need to reset a remote desktop if the desktop operating system stops responding and restarting the remote desktop does not solve the problem. Resetting published applications quits all open applications.

Resetting a remote desktop is the same as pressing the Reset button on a physical PC to force the PC to restart. Any files that are open on the remote desktop are closed and are not saved.

Resetting published applications quits the applications without saving any unsaved data. All open published applications are closed, even applications that come from different RDS server farms.

You can reset a remote desktop only if a Horizon administrator has enabled the reset feature for the remote desktop.

For information about enabling the desktop reset feature, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

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 published 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**.

  You can also use uniform resource identifiers (URIs) to reset a remote desktop or application. See Using URIs to Configure Horizon Client for information on the syntax and examples.

When you reset a remote desktop, the operating system in the remote desktop restarts and Horizon Client disconnects and logs off from the remote desktop. When you reset published applications, the published applications quit.

What to do next

Wait an appropriate amount of time for system to restart before attempting to reconnect to the remote desktop or published application.

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.

Problems with Keyboard Input

When you type in a remote desktop or published application, none of the keystrokes seem to work.

Problem

When you are connected to a remote desktop or published 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 keystroke logging software and blocks keystroke logging. This security feature is meant to protect the system against spyware that steals passwords and credit card numbers. This security software might block Horizon Client from sending keystrokes to the remote desktop or published application.

Solution

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

Connecting to a Server in Workspace ONE Mode

You cannot connect to a server directly through Horizon Client, or your remote desktop and published application entitlements are not visible in Horizon Client.

Problem

- When you try to connect to the server directly through Horizon Client, Horizon Client redirects you to the Workspace ONE portal.
- When you open a remote desktop or published application through a URI or command, the request redirects you to the Workspace ONE portal for authentication.
- After you open a remote desktop or published application through Workspace ONE and Horizon Client starts, you cannot see or open other entitled remote desktops or published applications in Horizon Client.

Cause

Beginning with Horizon 7 version 7.2, a Horizon administrator can enable Workspace ONE mode on a Connection Server instance. This behavior is normal when Workspace ONE mode is enabled on a Connection Server instance.

Solution

Use Workspace ONE to connect to a Workspace ONE enabled server and access your remote desktops and published applications.