VMware Horizon Client for Windows Installation and Setup Guide

29 MAY 2018

VMware Horizon Client for Windows 4.8

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 Windows Installation and Setup Guide

This guide, *VMware Horizon Client for Windows Installation and Setup Guide*, describes how to install, configure, and use VMware Horizon® Client™ software on a Microsoft Windows client system.

This information is intended for administrators who need to set up a Horizon deployment that includes Microsoft Windows client systems, such as desktops and laptops. The information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

If you are an end user, see the *VMware Horizon Client for Windows User Guide* document on VMware Docs, or view the Horizon Client online help.

System Requirements and Setup for Windows-Based Clients

1

Systems that run Horizon Client components must meet certain hardware and software requirements.

Horizon Client on Windows systems uses Microsoft Internet Explorer Internet settings, including proxy settings, when connecting to a server. Ensure that your Internet Explorer settings are accurate and that you can access the server URL through Internet Explorer.

This chapter includes the following topics:

System Requirements for Windows Client Systems

You can install Horizon Client for Windows on PCs and laptops that use a supported Microsoft Windows operating system.

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

Models	All x86 or x86-64 Windows devices
Memory	At least 1 GB of RAM
Operating systems	Horizon Client supports the following operating systems.

OS	Version	Service Pack or Servicing Option	Supported Editions
Windows 10	32-bit or 64-bit	Version 1803 SAC (Spring Creators Update) Version 1709 SAC (Fall Creators Update) Version 1703 SAC (Creators Update) Version 1607 CB/CBB/LTSB (Anniversary Update) Version 1507 LTSB	Home, Pro, Pro for Workstations, Enterprise, and IoT Enterprise
Windows 8 or 8.1	32-bit or 64-bit	None or Update 2	Pro, Enterprise, and Industry Embedded
Windows 7	32-bit or 64-bit	SP1	Home, Enterprise, Professional, and Ultimate
Windows Server 2008 R2	64-bit	Latest update	Standard
Windows Server 2012 R2	64-bit	Latest update	Standard

Windows Server 2008 R2 and Windows Server 2012 R2 are supported for the purposes of running Horizon Client in nested mode. For more information, see Features Supported in Nested Mode.

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

Latest maintenance release of Horizon 6 version 6.x and later releases.

If client systems connect from outside the corporate firewall, use a security server or Unified Access Gateway appliance so that client systems do not require a VPN connection.

Display protocols

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

Hardware requirements for PCoIP and VMware Blast

- x86-based processor with SSE2 extensions, with an 800 MHz or faster processor speed.

- Available RAM above system requirements to support various monitor setups. Use the following formula as a general guide.

```
20MB + (24 * (# monitors) * (monitor width) * (monitor height))
```

In general, you can use the following calculations.

```
1 monitor: 1600 x 1200: 64MB
2 monitors: 1600 x 1200: 128MB
3 monitors: 1600 x 1200: 256MB
```

Hardware requirements for RDP

- x86-based processor with SSE2 extensions, with an 800 MHz or faster processor speed.
- 128 MB RAM.

Software requirements for RDP

- For Windows 7, use RDP 7.1 or 8.0. Windows 7 includes RDP 7. Windows 7 SP1 includes RDP 7.1.
- For Windows 8, use RDP 8.0. For Windows 8.1, use RDP 8.1.
- For Windows 10, use RDP 10.0.
- (Supported with View Agent 6.0.2 and earlier only) For Windows XP desktop virtual machines, you must install the RDP patches listed in Microsoft Knowledge Base (KB) articles 323497 and 884020. If you do not install the RDP patches, a `Windows Sockets failed error` message might appear on the client.
- The agent installer configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389. If you change the RDP port number, you must change the associated firewall rules.

You can download Remote Desktop Client versions from the Microsoft Download Center.

Video and graphics requirements

- Graphics card that supports Direct3D 11 Video.
- Latest video and graphics card drivers.
- For Windows 7 SP1, install the Platform update for Windows 7 SP1 and Windows Server 2008 R2 SP1. For information, go to https://support.microsoft.com/en-us/kb/2670838.

System Requirements for Horizon Client Features

Horizon Client features have specific hardware and software requirements.

Smart Card Authentication Requirements

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

Client Hardware and Software Requirements

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

  Horizon Client supports smart cards and smart card readers that use a PKCS#11 or Microsoft CryptoAPI provider. You can optionally install the ActivIdentity ActivClient software suite, which provides tools for interacting with smart cards.
- Product-specific application drivers

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

Smart Card Enrollment Requirements

To install certificates on a smart card, an administrator must set up a computer to act as an enrollment station. This computer must have the authority to issue smart card certificates for users, and it must be a member of the domain for which you are issuing certificates.

When you enroll a smart card, you can select the key size of the resulting certificate. To use smart cards with local desktops, you must select a 1024-bit or 2048-bit key size when you enroll the smart card. Certificates that have 512-bit keys are not supported.

The Microsoft TechNet website includes detailed information about planning and implementing smart card authentication for Windows systems.

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.

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 all operating systems that run Horizon Client for Windows. For information, see System Requirements for Windows Client Systems.

	■ 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 Scanner Redirection

End users can scan information into their remote desktops and published applications with scanners that are connected to their local client systems. To use this feature, the remote desktops, applications, and client computers must meet certain system requirements.

Remote desktops	Remote desktops must have View Agent 6.0.2 or later, or Horizon Agent 7.0 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 and published applications, see "Configure Scanner Redirection" in the *Configuring Remote Desktop Features in Horizon 7* document.
Horizon Client computer or client access device	■ Scanner redirection is supported on Windows 7, Windows 8/8.1, and Windows 10. ■ The 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	TWAIN or WIA
Display protocols	■ PCoIP ■ VMware Blast (requires Horizon Agent 7.0 or later) Scanner redirection is not supported in RDP desktop sessions.

System Requirements for Serial Port Redirection

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

Remote desktops

Remote desktops must have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, installed with the Serial Port Redirection setup option selected. This setup option is deselected by default.

The following operating systems are supported on virtual desktops (single-session virtual machines).

- 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
- Windows Server 2012 R2
- Windows Server 2016

This feature is not currently supported for published desktops or published applications on Windows Server RDS hosts.

Serial port device drivers do not need to be installed in the virtual desktop.

Horizon Client computer or client access device

Serial port redirection is supported on Windows 7, Windows 8.x, and Windows 10 client systems. 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 Windows 3.4 and later releases.

Display protocols

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

Serial port redirection is not supported in RDP desktop sessions.

For information about configuring serial port redirection, see "Configuring Serial Port Redirection" in the *Configuring Remote Desktop Features in Horizon 7* document.

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	32-bit or 64-bit Windows 7, Windows 8.x, or Windows 10.
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.

System Requirements for Flash Redirection

Horizon Agent and Horizon Client, and the remote desktops and client systems on which you install the agent and client software, must meet certain requirements to support the Flash Redirection feature.

With Flash Redirection, if an end user uses Internet Explorer 9, 10, or 11, Flash content is sent to the client system, which reduces the load on the ESXi host. The client system plays the media content in a Flash container window by using the Flash Player ActiveX version.

Remote desktop	■ Horizon Agent 7.0 or later must be installed in a virtual desktop with the Flash Redirection custom setup option selected. The Flash Redirection custom setup option is not selected by default. See the topics about installing Horizon Agent in the *Setting Up Virtual Desktops in Horizon 7* document. ■ The appropriate group policy settings must be configured. See the topics about configuring Flash Redirection in the *Configuring Remote Desktop Features in Horizon 7* document. ■ Flash Redirection is supported on Windows 7, Windows 8, Windows 8.1, and Windows 10 virtual desktops. ■ Internet Explorer 9, 10, or 11 must be installed with the corresponding Flash ActiveX plug-in.

	■ After installation, the VMware View FlashMMR Server add-on must be enabled in Internet Explorer.
Horizon Client computer or client access device	■ Horizon Client must be installed with the Flash Redirection option enabled. The Flash Redirection option is enabled by default. ■ Flash Redirection is supported on Windows 7, Windows 8, Windows 8.1, and Windows 10. ■ The Flash ActiveX plug-in must be installed and enabled
Display protocols for the remote session	■ PCoIP ■ VMware Blast (requires Horizon Agent 7.0 or later)

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.

- 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 Adobe Flash Player 10.1 or later for Internet Explorer (which uses ActiveX).

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 URL Content Redirection

With the URL Content Redirection feature, URL content can be redirected from the client machine to a remote desktop or published application (client-to-agent redirection), or from a remote desktop or published application to the client machine (agent-to-client redirection).

For example, an end user can click a link in the native Microsoft Word application on the client and the link opens in the remote Internet Explorer application, or an end user can click a link in the remote Internet Explorer application and the link opens in a native browser on the client machine. Any number of protocols can be configured for redirection, including HTTP, mailto, and callto.

Note The callto protocol is not supported for URL content redirection with the Chrome browser.

Web browsers	You can type or click a URL in the following browsers and have that URL redirected. ■ Internet Explorer 9, 10, and 11 ■ 64-bit or 32-bit Chrome 60.0.3112.101, Official Build (requires Horizon 7 version 7.4 or later) URL Content Redirection does not work for links clicked from inside Windows 10 universal apps, including the Microsoft Edge Browser.
Client system	You must enable URL Content Redirection when you install Horizon Client. You must install Horizon Client from the command line to enable URL Content Redirection. For information, see Installing Horizon Client From the Command Line. To use URL Content Redirection with the Chrome browser, a Horizon administrator must install and enable the VMware Horizon URL Content Redirection Helper extension for Chrome. You can also install the extension manually from the Chrome Web Store. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document for Horizon 7 version 7.4 or later. The first time a URL is redirected from the Chrome browser, you are prompted to open the URL in Horizon Client. You must click **Open URL:VMware Hori...lient Protocol** for URL content redirection to occur. If you select the **Remember my choice for URL:VMware Hori...lient Protocol links** check box, this prompt does not appear again.
Remote desktop or published application	A Horizon administrator must enable URL Content Redirection when Horizon Agent is installed. For information, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* documents. To use URL Content Redirection with the Chrome browser, a Horizon administrator must install and enable the VMware Horizon URL Content Redirection Helper extension on the Windows agent machine. For information, see the *Configuring Remote Desktop Features in Horizon 7* document for Horizon 7 version 7.4 or later.

A Horizon administrator must also configure settings that specify how Horizon Client redirects URL content from the client to a remote desktop or published application, or how Horizon Agent redirects URL content from a remote desktop or published application to the client. For complete information, see the "Configuring URL Content Redirection" topic in the *Configuring Remote Desktop Features in Horizon 7* document.

System Requirements for HTML5 Multimedia Redirection

Horizon Agent and Horizon Client, and the remote desktops and client systems on which you install the agent and client software, must meet certain requirements to support the HTML5 Multimedia Redirection feature.

With HTML5 Multimedia Redirection, if an end user uses the Google Chrome or Microsoft Edge browser, HTML5 multimedia content is sent to the client system. The client system plays the multimedia content, which reduces the load on the ESXi host, and the end user has a better audio and video experience.

Remote desktop	■ Virtual desktops must have Horizon Agent 7.3.2 or later for Chrome, or Horizon Agent 7.5 or later for Edge, installed with the HTML5 Multimedia Redirection custom setup option selected. This option is not selected by default. See the topics about installing Horizon Agent in the *Setting Up Virtual Desktops in Horizon 7* document. ■ RDS hosts for published desktops must have Horizon Agent 7.3.2 or later installed with the HTML5 Multimedia Redirection custom setup option selected. This option is not selected by default. See the topics about installing Horizon Agent in the *Setting Up Published Desktops and Applications in Horizon 7* document. ■ The HTML5 Multimedia Redirection group policy settings must be configured on the Active Directory server. See the topics about configuring HTML5 Multimedia Redirection in the *Configuring Remote Desktop Features in Horizon 7* document. ■ The Chrome or Edge browser must be installed. ■ The VMware Horizon HTML5 Multimedia Redirection extension must be installed in the Chrome or Edge browser. See the topics about configuring HTML5 Multimedia Redirection in the *Configuring Remote Desktop Features in Horizon 7* document.
Client system	■ The HTML5 Multimedia Redirection Support custom setup option must be selected when you install Horizon Client. This option is selected by default.
Display protocol for the remote session	■ PCoIP ■ VMware Blast

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 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. The Session Collaboration feature does not support Linux remote desktop sessions or published application sessions.
Connection Server	The Session Collaboration feature requires that the Connection Server instance uses an Enterprise license.
Display protocols	VMware Blast

Requirements for Using Fingerprint Scanner Redirection

With the device bridge feature, you can redirect biometric devices, specifically fingerprint scanners, that are plugged into a USB port on the Windows client system to virtual desktops, published desktops, and published applications.

To use fingerprint scanner redirection, you must obtain the Smartchip Biometric Authentication System (BAS) third-party software and install it on both the Windows client system and on the Horizon Agent system. You must also install the Device Bridge BAS Plugin feature when you install Horizon Agent.

For more information, see "Configuring Fingerprint Scanner Redirection" in the *Configuring Remote Desktop Features in Horizon 7* document for Horizon 7 version 7.4 or later.

Requirements for Using Microsoft Lync with Horizon Client

End users can use a Microsoft Lync 2013 client on remote desktops to participate in Unified Communications (UC) VoIP (voice over IP) and video chat calls with Lync certified USB audio and video devices. A dedicated IP phone is no longer required.

This architecture requires the installation of a Microsoft Lync 2013 client on the remote desktop and a Microsoft Lync VDI plug-in on the client endpoint. End users can use the Microsoft Lync 2013 client for presence, instant messaging, Web conferencing, and Microsoft Office functionality.

Whenever a Lync VoIP or video chat call occurs, the Lync VDI plug-in offloads all the media processing from the data center server to the client endpoint, and encodes all media into audio and video codecs that are optimized for Lync. This optimized architecture is highly scalable, results in lower network bandwidth used, and provides point-to-point media delivery with support for high-quality real-time VoIP and video. For more information, see the white paper about Horizon 6 and Microsoft Lync 2013, at http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf.

Note Recording audio is not yet supported. This integration is supported only with the PCoIP display protocol.

This feature has the following requirements.

Operating system

- The client operating system must support the Microsoft Lync VDI Plug-in. For 32-bit client operating system requirements, see https://www.microsoft.com/en-us/download/details.aspx?id=35457. For 64-bit client operating system requirements, see https://www.microsoft.com/en-us/download/details.aspx?id=35454.

  Note Windows 10 clients are not supported. For Windows 10 clients, you can use the Skype for Business feature instead of Microsoft Lync. For more information, see Requirements for Using Skype for Business with Horizon Client.

- The remote desktop (agent) operating system depends on the agent version.

Version	Guest Operating System
View Agent 6.2 or later, or Horizon Agent 7.0 or later	32-bit or 64-bit Windows 7 SP1, Windows 8.x, Windows 10, or 64-bit Windows Server 2008 R2 SP1, Windows Server 2012 R2 For Microsoft RDS hosts, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2
View Agent 6.0 or 6.1	32-bit or 64-bit Windows 7 SP1, Windows 8.x, or 64-bit Windows Server 2008 R2 SP1, Windows Server 2012 R2

Client system software

- 32-bit or 64-bit version of Microsoft Lync VDI Plug-in. Install the 32-bit plug-in if you install the 32-bit version of Horizon Client. Install the 64-bit plug-in if you install the 64-bit version of Horizon Client.

  Important If you install the 32-bit Microsoft Lync VDI Plug-in, the 64-bit version of Microsoft Office must not be installed on the client machine. The 32-bit Microsoft Lync VDI Plug-in is not compatible with 64-bit Microsoft Office 2013.

- Security certificate generated during Microsoft Lync Server 2013 deployment must be imported into the Trusted Root Certificate Authorities directory.

Remote desktop (agent) software

- View Agent 6.0 or later, or Horizon Agent 7.0 or later
- Microsoft Lync 2013 Client
- Security certificate generated during Microsoft Lync Server 2013 deployment must be imported into the Trusted Root Certificate Authorities directory

Required servers

- A server running Connection Server 6.0 or later
- A server running Microsoft Lync Server 2013
- A vSphere infrastructure to host the virtual machines

  The vCenter Server and ESXi hosts must be running vSphere 5.0 or later.

Hardware

- Hardware that supports each of the required software components previously listed
- Client endpoint: 1.5 GHz or faster CPU and a minimum of 2 GB of RAM for the Microsoft Lync 2013 Plug-in

Note For troubleshooting information, see VMware KB 2063769 and VMware KB 2053732.

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 Virtualization Pack for Skype for Business feature on the client machine when Horizon Client for Windows is installed. For information, see Chapter 2 Installing Horizon Client for Windows.

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.

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.
- If end users have a high-resolution display and use the High Resolution Mode client setting while viewing their remote desktops in full screen mode, verify that sufficient vRAM is allocated for each Windows 7 or later remote desktop. The amount of vRAM depends on the number of monitors configured for end users and on the display resolution. To estimate the amount of vRAM, see the *Horizon 7 Architecture Planning* document.

User Authentication

- To use two-factor authentication, such as RSA SecurID or RADIUS authentication, with Horizon Client, you must enable the two-factor authentication feature in Connection Server. For more information, see the topics about two-factor authentication in the *Horizon 7 Administration* document.
- To hide security information in Horizon Client, including server URL information and the **Domain** drop-down menu, enable the **Hide server information in client user interface** and **Hide domain list in client user interface** settings for the Connection Server instance. These global settings are available in Horizon 7 version 7.1 and later. For information about configuring global settings, see the *Horizon 7 Administration* document.

  To authenticate when the **Domain** drop-down menu is hidden, users must provide domain information by entering their user name in the format ***domain**username*** or ***username*@*domain*** in the **User name** text box.

  Important If you enable the **Hide server information in client user interface** and **Hide domain list in client user interface** settings and select two-factor authentication (RSA SecureID or RADIUS) for the Connection Server instance, do not enforce Windows user name matching. Enforcing Windows user name matching prevents users from entering domain information in the user name text box and login always fails. For more information, see the topics about two-factor authentication in the *Horizon 7 Administration* document.

- 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.

Clearing the Last User Name Used to Log In to a Server

When end users log in to a Connection Server instance for which the **Hide domain list in client user interface** global setting is enabled, the **Domain** drop-down menu is hidden in Horizon Client and users provide domain information in the Horizon Client **User name** text box. For example, users must enter their user name in the format ***domain**username*** or ***username*@*domain***.

On a Windows client system, a registry key determines whether the last user name is saved and displayed in the **User name** text box the next time a user logs in to the server. To prevent the last user name from being displayed in the **User name** text box and exposing domain information, you must set the value of the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` registry key to 1 on the Windows client system.

For information about hiding security information in Horizon Client, including the **Domain** drop-down menu and server URL information, see the topics about global settings in the *Horizon 7 Administration* document.

Configure VMware Blast Options

You can configure H.264 decoding for remote desktop and published application sessions that use the VMware Blast display protocol.

You can also allow increased color fidelity when H.264 decoding is allowed.

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. If a resolution for H.264 is not supported, Horizon Client uses JPEG/PNG instead.

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

Note In previous 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 use increased color fidelity when H.264 decoding is allowed, Horizon Agent 7.4 or later must be installed.

Procedure

1 Click the **Options** button in the menu bar and select **Configure VMware Blast**.

  If you are logged in to a server, you can click the **Settings** (gear) icon and select **VMware Blast**.

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

   When this option is selected (the default setting), Horizon Client uses H.264 decoding if the agent supports H.264 software or hardware encoding. If the agent does not support H.264 software or hardware encoding, Horizon Client uses JPG/PNG decoding. When this option is deselected, Horizon Client uses JPG/PNG decoding.

3 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 uses high color accuracy, but only if the agent supports high color accuracy. Selecting this option might reduce battery life and performance. This feature is disabled by default.

4 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.

Using Internet Explorer Proxy Settings

Horizon Client uses proxy settings configured in Internet Explorer.

Bypassing Proxy Settings

Horizon Client uses the Internet Explorer proxy bypass settings to bypass HTTPS connections to a Connection Server host, security server, or Unified Access Gateway appliance.

If the secure tunnel is enabled on the Connection Server host, security server, or Unified Access Gateway appliance, you must use the `Tunnel proxy bypass address list` group policy setting in the Horizon Client Configuration ADM or ADMX template file to specify a list of addresses to bypass the tunnel connection. The proxy server is not used for these addresses. Use a semicolon (;) to separate multiple entries. This group policy setting creates the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

You cannot use this group policy setting for direct connections. If applying the group policy setting does not work as expected, try bypassing the proxy for local addresses. For more information, see https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/.

Proxy Fail Over

Horizon Client supports proxy fail over with the **Use automatic configuration script** setting under **Automatic configuration** in **Internet Options > Connections > LAN settings** in Internet Explorer. To use this setting, you must create an automatic configuration script that returns multiple proxy servers.

Horizon Client Data Collected by VMware

If your company participates in the customer experience improvement program, VMware collects data from certain Horizon Client text boxes. Text boxes that contain sensitive information are anonymous.

VMware collects data on client systems to prioritize hardware and software compatibility. If your company's 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, with data from Connection Server, desktop pools, and remote desktops.

Although 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 any personally identifiable information.

The Horizon administrator that installs Connection Server can select whether to participate in the VMware customer experience improvement program when installing Connection Server, or can set an option in Horizon Administrator after the installation.

Table 1-1. 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

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

Description	Is This Field Made Anonymous?	Example Value
Host operating system	No	Examples include the following: ■ Windows 8.1 ■ Windows 7, 64-bit Service Pack 1 (Build 7601) ■ iPhone OS 5.1.1 (9B206) ■ Ubuntu 12.04.4 LTS ■ Mac OS X 10.8.5 (12F45)
Host operating system kernel	No	Examples include the following: ■ Windows 6.1.7601 SP1 ■ Darwin Kernel Version 11.0.0: Sun Apr 8 21:52:26 PDT 2012; root:xnu-1878.11.10~1/RELEASE_ARM_S5L8945X ■ Darwin 11.4.2 ■ Linux 2.6.32-44-generic #98-Ubuntu SMP Mon Sep 24 17:27:10 UTC 2012 ■ unknown (for Windows Store)
Host operating system architecture	No	Examples include the following: ■ x86_64 ■ i386 ■ armv71 ■ ARM
Host system model	No	Examples include the following: ■ Dell Inc. OptiPlex 960 ■ iPad3,3 ■ MacBookPro8,2 ■ Dell Inc. Precision Workstation T3400 (A04 03/21/2008)
Host system CPU	No	Examples include the following: ■ Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GH ■ Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GH ■ unknown (for iPad)
Number of cores in the host system's processor	No	For example: 4
MB of memory on the host system	No	Examples include the following: ■ 4096 ■ unknown (for Windows Store)
Number of USB devices connected	No	2 (USB device redirection is supported only for Linux, Windows, and Mac clients.)
Maximum concurrent USB device connections	No	2

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

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

Installing Horizon Client for Windows

2

You can obtain the Windows-based Horizon Client installer from the VMware website, or from a Web access page provided by Connection Server. You can set various startup options for end users after Horizon Client is installed.

This chapter includes the following topics:

Enabling FIPS Mode in the Windows Client Operating System

If you plan to install Horizon Client with Federal Information Processing Standard (FIPS) compliant cryptography, you must enable FIPS mode in the client operating system before you run the Horizon Client installer.

When FIPS mode is enabled in the client operating system, applications use only cryptographic algorithms that are FIPS-140 compliant and in compliance with FIPS-approved modes of operation. You can enable FIPS mode by enabling a specific security setting, either in the Local Security Policy or as part of Group Policy, or by editing a Windows Registry key.

FIPS compliance is available with Horizon 6 version 6.2 and later. For more information, see the *Horizon 7 Installation* document.

Setting the FIPS Configuration Property

To enable FIPS mode in the client operating system, you can use a Windows group policy setting or a Windows Registry setting for the client computer.

- To use the group policy setting, open the Group Policy Editor, navigate to `Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options`, and enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting.
- To use the Windows Registry, go to `HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` and set **Enabled** to 1.

For more information about FIPS mode, go to https://support.microsoft.com/en-us/kb/811833.

Important If you do not enable FIPS mode before running the Horizon Client installer, the installer option to use FIPS-compliant cryptography does not appear during a custom installation. FIPS-compliant cryptography is not enabled during a typical installation. If you install Horizon Client without the FIPS-compliant cryptography option and you later decide to use the option, you must uninstall the client, enable FIPS mode in the client operating system, and run the Horizon Client installer again.

Enabling Automatic Internet Protocol Selection

When you perform a custom installation of Horizon Client, you can enable the automatic selection of the Internet protocol. With automatic selection, Horizon Client checks the current network and connects over IPv4 or IPv6 automatically.

When automatic selection is enabled, the following features are supported with Horizon 7 version 7.5 or later, and Unified Access Gateway 3.3 or later, with the VMware Blast display protocol.

- Log in as current user
- Audio-out
- Customer Experience Improvement Program data collection
- Virtual printing and location-based printing
- HTML5 Multimedia Redirection
- VMware video
- USB redirection

Install Horizon Client for Windows

You can run a Windows-based installer file to install all Horizon Client components.

This procedure describes how to install Horizon Client by using an interactive installation wizard. To install Horizon Client from the command line, see Installing Horizon Client From the Command Line. To install the URL Content Redirection feature, you must run the installer from the command line.

Note If a remote desktop is running View Agent 6.0 or later, or Horizon Agent 7.0 or later, you can install Horizon Client in the remote desktop virtual machine. Companies might use this installation strategy when their end users access published applications from Windows thin-client devices.

Prerequisites

- Verify that the client system uses a supported operating system. See System Requirements for Windows Client Systems.
- Verify that you have the URL for a download page that contains the Horizon Client installer. This URL might be the VMware Downloads page at http://www.vmware.com/go/viewclients, or it might be the URL for a Connection Server instance.
- Verify that you can log in as an administrator on the client system.
- Verify that the domain controllers have the latest patches, enough free disk space, and can communicate with each other. Otherwise, when you run the installer on a Windows 8.1 system, the installer can take an unusual amount of time to finish. This problem occurs if the machine's domain controller, or another domain controller in its hierarchy, is unresponsive or unreachable.
- If you plan to install Horizon Client with FIPS-compliant cryptography, enable FIPS mode in the client operating system. See Enabling FIPS Mode in the Windows Client Operating System.
- If you plan to select the IPv6 protocol or automatic Internet protocol selection, see the *Horizon 7 Installation* document for information about features that are not available in an IPv6 environment.
- If you plan to enable automatic Internet protocol selection, see Enabling Automatic Internet Protocol Selection for information about the supported features.
- If you plan to install the **USB Redirection** component, perform the following tasks:
  - Determine whether the person who uses the client device is allowed to access locally connected USB devices from a remote desktop. If access is not permitted, either do not install the **USB Redirection** component, or install the component and disable it by using a group policy setting. If you use group policy to disable USB redirection, you do not need to reinstall Horizon Client if you later decide to enable USB redirection for a client. For more information, see Scripting Definition Settings for Client GPOs.
  - Verify that the Windows Automatic Update feature is not turned off on the client computer.
- Decide whether to use the feature that allows end users to log in to Horizon Client and their remote desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the Connection Server instance and ultimately to the remote desktop. Some client operating systems do not support this feature.
- If you do not want to require end users to supply the fully qualified domain name (FQDN) of the Connection Server instance, determine the FQDN so that you can supply it during installation.

Procedure

1. Log in to the client system as an administrator.
2. Navigate to the VMware Downloads page at http://www.vmware.com/go/viewclients.
3. Download the installer file, for example, `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

   xxxxxx is the build number and *y.y.y* is the version number.
4. Double-click the installer file to begin the installation.
5. Select an installation type and follow the prompts.

Option	Action
Typical installation	Click **Agree & Install**. The installer configures the client to use the IPv4 Internet protocol and installs the USB Redirection, Log in as current user, Virtualization Pack for Skype for Business, and HTML5 Multimedia Redirection Support features.
Custom installation	Click **Customize Installation** and select the features to install. You must select this option to specify the following features: ■ Specify a non-default installation location. ■ Use the IPv6 Internet protocol, ■ Enable automatic selection of the Internet protocol. Horizon Client checks the current network and connects over IPv4 or IPv6 automatically. ■ Configure a default Connection Server instance. ■ Configure the default login behavior. ■ Enable FIPS-compliant cryptography. FIPS-compliant cryptography custom installation options are available in the installer only if FIPS mode is enabled on the client operating system. ■ Install the 32-bit Core Remote Experience component on a 64-bit machine **Note** Select the **32-bit Core Remote Experience on a 64-bit machine** feature if the 64-bit client machine does not have 64-bit plug-ins for the product. If you select this feature, you cannot install the Virtualization Pack for Skype for Business feature.

Some features require you to restart the client system.

The installer installs Windows services, including VMware Horizon Client (`horizon_client_service`) and VMware USB Arbitration Service (`VMUSBArbService`).

What to do next

Start Horizon Client and verify that you can log in to the correct remote desktop or published application. See Connect to a Remote Desktop or Published Application.

Installing Horizon Client From the Command Line

You can install Horizon Client by typing the installer filename, installation commands, and installation properties at the command line.

When you install Horizon Client from the command line, you can perform a silent installation. With a silent installation, you can efficiently deploy Horizon Client in a large enterprise.

Installation Commands for Horizon Client

When you install Horizon Client from the command line, you can specify certain installation commands.

The following table describes the Horizon Client installation commands.

Table 2-1. Horizon Client Installation Commands

Command	Description
`/?` or `/help`	Lists the Horizon Client installation commands and properties.
`/silent`	Installs Horizon Client silently. You do not need to respond to wizard prompts.
`/install`	Installs Horizon Client interactively. You must respond to wizard prompts.
`/uninstall`	Uninstalls Horizon Client.
`/repair`	Repairs Horizon Client.
`/norestart`	Suppresses all restarts and restart prompts during the installation process.
`/x /extract`	Extracts the installer packages into the `%TEMP%` directory.
`/l` or `/log`	Specifies a folder and a naming pattern for installation log files. For example, if you specify the following command, the Horizon Client installer creates log files that have the prefix `Test` in the folder named `C:\Temp`. `/log "C:\Temp\Test"`

Installation Properties for Horizon Client

When you install Horizon Client from the command line, you can specify certain installation properties.

The following table describes the Horizon Client installation properties.

Table 2-2. Horizon Client Installation Properties

Property	Description	Default
INSTALLDIR	Path and folder in which Horizon Client is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of double quotes that enclose the path enable the installer to interpret the space as a valid part of the path.	`%ProgramFiles %VMware\VMware Horizon View Client`
VDM_IP_PROTOCOL_USAGE	IP (Internet Protocol) version that Horizon Client components use for communication. Valid values are as follows: ■ IPv4 ■ IPv6 ■ Dual If you specify Dual, Horizon Client checks the current network and connects over IPv4 or IPv6 automatically.	IPv4
VDM_FIPS_ENABLED	Determines whether to install Horizon Client with FIPS-compliant cryptography. A value of 1 installs Horizon Client with FIPS-compliant cryptography. A value of 0 installs Horizon Client without FIPs-compliant cryptography. **Note** Before you set this property to 1, you must enable FIPS mode in the Windows client operating system. See Enabling FIPS Mode in the Windows Client Operating System.	0
VDM_SERVER	Fully qualified domain name (FQDN) of the Connection Server instance to which Horizon Client users connect by default. For example: `VDM_Server=cs1.companydomain.com` If you configure this property, Horizon Client users do not need to supply this FQDN.	None
LOGINASCURRENTUSER_DISPLAY	Determines whether **Log in as current user** appears in the **Options** menu on the Horizon Client menu bar. Valid values are 1 (enabled) or 0 (disabled).	1

Table 2-2. Horizon Client Installation Properties (Continued)

Property	Description	Default
LOGINASCURRENTUSER_DEFAULT	Determines whether **Log in as current user** is selected by default in the **Options** menu on the Horizon Client menu bar. Valid values are 1 (enabled) and 0 (disabled). When log in as current user is the default login behavior, the identity and credential information that users provide when they log in to the client system is passed to the Connection Server instance and ultimately to the remote desktop. When log in as current user is not the default login behavior, users must provide identity and credential information multiple times before they can access a remote desktop or application.	0
ADDLOCAL	Specifies the features to install. Valid values are as follows: ■ ALL - Installs all available features, except for URL Content Redirection. ■ TSSO - Installs the Log in as Current User feature. ■ USB - Installs the USB Redirection feature. To specify individual features, enter a comma-separated list of feature names. Do not use spaces between names. For example, to install Horizon Client with the USB Redirection feature, but without the Log in as Current User feature, type the following command: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe ADDLOCAL=USB	None
INSTALL_32BITRMKS	On a 64-bit client machine, specifies whether to install the 32-bit Core Remote Experience component. A value of 1 installs the 32-bit Core Remote Experience component. A value of 0 installs the 64-bit Core Remote Experience component. Install the 32-bit Core Remote Experience component if the 64-bit client machine does not have 64-bit plug-ins for the product. This property is not valid on a 32-bit client machine.	0
INSTALL_SFB	Determines whether the VMware Virtualization Pack for Skype for Business feature is installed. A value of 1 installs the feature. A value of 0 does not install the feature. This feature is not compatible with the 32-bit Core Remote Experience Component (INSTALL_32BITRMKS=1).	1

Table 2-2. Horizon Client Installation Properties (Continued)

Property	Description	Default
INSTALL_HTML5MMR	Determines whether the HTML5 Multimedia Redirection feature is installed. A value of 1 installs the feature. A value of 0 does not install the feature.	1
REMOVE	Specifies the features not to install. Valid values are as follows: ■ ThinPrint - Does not install the virtual printing feature. ■ Scanner - Does not install the scanner redirection feature. ■ FolderRedirection - Does not install the folder redirection feature. ■ SerialPort - Does not install the serial port redirection feature. To specify multiple features, enter a comma-separated list of feature names. Do not use spaces between names. For example, the following command does not install the virtual printing and scanner redirection features: VMware-Horizon-Client-*y.y.y-xxxxxx*.exe REMOVE=ThinPrint,Scanner	None
DESKTOP_SHORTCUT	Determines whether to create a desktop shortcut for Horizon Client. A value of 0 does not create a desktop shortcut. A value of 1 creates a desktop shortcut.	1
STARTMENU_SHORTCUT	Determines whether to create a Start menu shortcut for Horizon Client. A value of 0 does not create a Start menu shortcut. A value of 1 creates a Start menu shortcut.	1

Table 2-2. Horizon Client Installation Properties (Continued)

Property	Description	Default
URL_FILTERING_ENABLED	Determines whether the URL Content Redirection feature is installed. A value of 1 installs the feature. A value of 0 does not install the feature. When you set this property to 1 in an interactive installation, the **URL Content Redirection** check box appears under Additional features on the custom installation dialog box and is selected by default. The check box does not appear unless you set this property to 1. **Note** The ADDLOCAL=ALL property does not include the URL Content Redirection feature.	0
AUTO_UPDATE_ENABLED	Determines whether the online update feature is enabled. A value of 1 enables the feature. A value of 0 disables the feature. For more information, see Update Horizon Client Online.	1

Install Horizon Client from the Command Line

You can install Horizon Client from the command line by typing the installer filename and specifying installation commands and properties. You can install Horizon Client silently from the command line.

Prerequisites

- Verify that the client system uses a supported operating system. See System Requirements for Windows Client Systems.
- Verify that you can log in as an administrator on the client system.
- Verify that the domain controllers have the latest patches, enough free disk space, and can communicate with each other. Otherwise, when you run the installer on a Windows 8.1 system, the installer can take an unusual amount of time to finish. This problem occurs if the machine's domain controller, or another domain controller in its hierarchy, is unresponsive or unreachable.
- If you plan to install Horizon Client with FIPS-compliant cryptography, enable FIPS mode in the client operating system. See Enabling FIPS Mode in the Windows Client Operating System.
- Decide whether to use the feature that allows end users to log in to Horizon Client and their remote desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the Connection Server instance and ultimately to the remote desktop. Some client operating systems do not support this feature.
- Become familiar with the Horizon Client installation commands. See Installation Commands for Horizon Client.
- Become familiar with the Horizon Client installation properties. See Installation Properties for Horizon Client.

- Determine whether to allow end users to access locally connected USB devices from their remote desktops. If not, set the ADDLOCAL installation property to the list of features and omit the USB feature. For more information, see Installation Properties for Horizon Client.
- If you do not want to require end users to supply the fully qualified domain name (FQDN) of the Connection Server instance, determine the FQDN so that you can supply it during installation.

Procedure

1. Log in to the client system as an administrator.
2. Navigate to the VMware Downloads page at http://www.vmware.com/go/viewclients.
3. Download the Horizon Client installer file, for example, `VMware-Horizon-Client-y.y.y-xxxxxx.exe`.

   xxxxxx is the build number and *y.y.y* is the version number.
4. Open a command prompt on the Windows client computer.
5. Type the installer filename, installation commands, and installation properties on one line.

   `VMware-Horizon-Client-y.y.y-xxxxxx.exe [commands] [properties]`

The installer installs Horizon Client according to the installation commands and properties that you specify. If you specify the `/silent` installation command, the wizard prompts do not appear.

The installer installs Windows services, including VMware Horizon Client (`horizon_client_service`) and VMware USB Arbitration Service (`VMUSBArbService`).

Example: Sample Installation Commands

The following command installs Horizon Client interactively and enables the URL Content Redirection feature.

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

The following command installs Horizon Client silently and suppresses all restarts and restart prompts during the installation process.

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /norestart
```

What to do next

If you enabled the URL Content Redirection feature when you installed Horizon Client, verify that the feature is installed. See Verify URL Content Redirection Installation.

Start Horizon Client and verify that you can log in to the correct remote desktop or published application. See Connect to a Remote Desktop or Published Application.

Verify URL Content Redirection Installation

If you enabled the URL Content Redirection feature when you installed Horizon Client, verify that the feature was installed.

Prerequisites

Specify the `URL_FILTERING_ENABLED=1` installation property when you install Horizon Client. See Installing Horizon Client From the Command Line.

Procedure

1. Log in to the client machine.
2. Verify that the `vmware-url-protocol-launch-helper.exe` and `vmware-url-filtering-plugin.dll` files are installed in the `%PROGRAMFILES%\VMware\VMware Horizon View Client\` directory.
3. Verify that the VMware Horizon View URL Filtering Plugin add-on is installed and enabled in Internet Explorer.

Update Horizon Client Online

You can update Horizon Client online.

You can disable the online update feature by modifying the `Enable Horizon Client online update` group policy setting. You can specify an alternate URL from which to retrieve updates by modifying the `URL for Horizon Client online update` group policy setting. For more information, see General Settings for Client GPOs.

You can also disable the online update feature by setting the `AUTO_UPDATE_ENABLED` property to 0 when you install Horizon Client from the command line. For more information, see Installation Properties for Horizon Client.

Prerequisites

- Save your work before you update Horizon Client. The update might initiate a system reboot.
- Verify that you can log in as an administrator on the client system.

Procedure

1. Log in to the client system as an administrator.
2. Start Horizon Client and click **Software Updates**.

Option	Action
Before you connect to a server	Click **Options > Software Updates**.
After you connect to a server	Click **Help > Software Updates**.

3 To check for available updates, click **Check for Updates**.

   Horizon Client indicates whether an update is available.

   If the **Enable update notifications** check box is selected (the default), Horizon Client detects available updates. To indicate that a new Horizon Client version is available, a red dot appears on the **Options** menu (before you connect to a server) or on the **Help** button (after you connect to a server). You can disable automatic update detection by deselecting this check box.

4 To begin the update process if an update is available, click **Download and Install**.

5 To install the update after Horizon Client downloads the update, click **OK**.

   The Horizon Client interactive installation wizard opens.

Configuring Horizon Client for End Users

3

Configuring Horizon Client for end users can involve configuring URIs to start Horizon Client, configuring the certificate checking mode, setting advanced TLS options, and using group policies to configure custom settings.

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 3-1. Common Configuration Settings

Setting	Mechanisms for Configuring
Server address	URI, Group Policy, Command Line, Windows Registry
Active Directory user name	URI, Group Policy, Command Line, Windows Registry
Domain name	URI, Group Policy, Command Line, Windows Registry
Remote desktop display name	URI, Group Policy, Command Line
Window size	URI, Group Policy, Command Line
Display protocol	URI, Command Line

Table 3-1. Common Configuration Settings (Continued)

Setting	Mechanisms for Configuring
Configuring certificate checking	Group Policy, Windows Registry
Configuring TLS protocols and cryptographic algorithms	Group Policy, Windows Registry

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
- RADIUS or RSA SecurID user name, if different from the 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
- Options for redirecting USB devices

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

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 3-2. 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.
`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`**.

connectUSBOnInsert Connects a USB device to the foreground remote desktop or published application when you plug in the device. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnInsert=true`**.

connectUSBOnStartup Redirects all USB devices that are currently connected to the client system to the remote desktop or published application. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnStartup=true`**.

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 3-3. 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`.

filePath Specifies the path to the file on the local system that you want to open with the published application. You must specify the full path, including the drive letter. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**

For example, to represent file path `C:\test file.txt`, use **`C%3A%5Ctest%20file.txt`**.

tokenUserName	Specifies the RSA or RADIUS user name. Use this query only if the RSA or RADIUS user name is different from the Active Directory user name. If you do not specify this query and RSA or RADIUS authentication is required, Horizon Client uses the Windows user name. The syntax is **tokenUserName=*name***.
unattended	Creates a server connection to a remote desktop in kiosk mode. If you use this query, do not specify user information if you generated the account name from the MAC address of the client device. If you created custom account names in ADAM, such as names that begin with "custom-", you must specify the account information.
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**.
unauthenticatedAccess Enabled	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 hidden from the user interface and disabled. An example of the syntax is **unauthenticatedAccessEnabled=true**.
unauthenticatedAccess Account	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.

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://view.mycompany.com/Primary%20Desktop?action=start-session&connectUSBOnStartup=true
```

This URI has the same effect as the first example, and all USB devices connected to the client system are redirected to the remote desktop.

10
```
vmware-view://
```

If Horizon Client is not running, it starts. If Horizon Client is already running, it comes to the foreground.

11
```
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. Spaces and double quotes use percent escaping. The filename is enclosed in double quotes because it contains spaces.

You can also type this command at the Windows command-line prompt by using the following syntax:

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

In this example, double quotes are escaped by using the characters \".

12
```
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`.

13
```
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>
```

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:

- Has the certificate been revoked?
- 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.

For information about distributing a self-signed root certificate to all Windows client systems in a domain, see "Add the Root Certificate to Trusted Root Certification Authorities" in the *Horizon 7 Installation* document.

To set the certificate checking mode, start Horizon Client and select **Configure SSL** in the **Options** menu on the Horizon Client 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.

  You can also receive a warning if the certificate has expired.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

If an administrator later installs a security certificate from a trusted certificate authority and all certificate checks pass when you connect, this trusted connection is remembered for that specific server. In the future, if that server ever presents a self-signed certificate again, the connection fails. After a particular server presents a fully verifiable certificate, it must always do so.

Important If you previously used group policy to configure your company's client systems to use a specific cipher, such as by configuring SSL Cipher Suite Order group policy settings, you must now use a Horizon Client group policy security setting. See Security Settings for Client GPOs. Alternatively, you can use the `SSLCipherList` registry setting on the client system. See Using the Windows Registry to Configure Horizon Client.

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.

You can use the Horizon Client Configuration ADMX template file (`vdm_client.admx`) to set the certificate checking mode. All ADMX files that provide group policy settings are available in `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. You can download this ZIP file from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. For information about using this template to control group policy settings, see Using Group Policy Settings to Configure Horizon Client.

You can also use the Horizon Client Configuration ADMX template file to restrict the use of certain cryptographic algorithms and protocols before establishing an encrypted TLS connection. For more information, see Security Settings for Client GPOs.

If you do not want to configure the certificate checking mode as a group policy, you can enable certificate checking by adding the `CertCheckMode` value name to one of the following registry keys on the client computer:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- For 64-bit Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

Use the following values in the registry key:

- **`0`** implements `Do not verify server identity certificates`.
- **`1`** implements `Warn before connecting to untrusted servers`.
- **`2`** implements `Never connect to untrusted servers`.

If you configure both the group policy setting and the `CertCheckMode` setting in the registry key, the group policy setting takes precedence over the registry key value.

Note In a future Horizon Client version, using the Windows registry to configure this setting might not be supported and group policy settings must be used.

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 security options are also used to encrypt the USB channel.

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

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

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 a group policy setting or a Windows Registry setting to change the default ciphers and protocols. For information about using a group policy setting, see the **Configures SSL protocols and cryptographic algorithms** setting in Security Settings for Client GPOs. For information about using the SSLCipherList setting in the Windows Registry, see Using the Windows Registry to Configure Horizon Client.

Configure Published Application Reconnection Behavior

Running published applications can remain open after you disconnect for a server in Horizon Client. You can configure how running published applications behave when you reconnect to the server in Horizon Client.

You can disable the published application reconnection behavior settings in Horizon Client, either from the command line, or by configuring a group policy setting. The group policy setting takes precedence over the command-line setting. For more information, see the `–appSessionReconnectionBehavior` option in Horizon Client Command Use, or the **Disconnected application session resumption behavior** group policy setting in Scripting Definition Settings for Client GPOs.

Procedure

1. In the Horizon Client desktop and application selector window, right-click a published application and select **Settings**.
2. In the Remote Applications pane, select an application reconnection behavior setting.

Option	Description
Ask to reconnect to open published applications	Horizon Client notifies you that you have one or more published applications running when you reconnect to the server. You can click **Reconnect to applications** to reopen the published application windows, or **Not Now** not to reopen the published application windows.
Reconnect automatically to open published applications	Windows for running published applications reopen when you reconnect to the server.
Do not ask to reconnect and do not automatically reconnect	Horizon Client does not prompt you to reopen running published applications, and running published application windows do not reopen when you reconnect to the server.

3. To save your changes, click **OK**.

The setting takes effect the next time Horizon Client connects to the server.

Using Group Policy Settings to Configure Horizon Client

Horizon Client includes a group policy ADMX template file that you can use to configure Horizon Client features and behavior. You can optimize and secure remote desktop and published application connections by adding the policy settings in the ADMX template file to a new or existing GPO in Active Directory.

The template file contains both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to Horizon Client, regardless of who is running the client on the host.
- The User Configuration policies set Horizon Client policies that apply to all users who are running Horizon Client, and to RDP connection settings. User Configuration policies override equivalent Computer Configuration policies.

Horizon Client applies policies when remote desktops and published applications start and when users log in.

The Horizon Client Configuration ADMX template file (`vdm_client.admx`), and all ADMX template files that provide group policy settings, are available in `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. You can download this ZIP file from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. You must copy the file to your Active Directory server and use the Group Policy Management Editor to add the administrative templates. For instructions, see the *Configuring Remote Desktop Features in Horizon 7* document.

Scripting Definition Settings for Client GPOs

You can set group policies for many of the same settings that you can configure when you run Horizon Client from the command line, including the remote desktop window size, login user name, and login domain name.

The following table describes the scripting definition settings in the VMware Horizon Client Configuration ADMX template file. This template file provides a Computer Configuration and a User Configuration version of each scripting definition setting. The User Configuration setting overrides the equivalent Computer Configuration setting. The settings appear in the **VMware Horizon Client Configuration > Scripting definitions** folder in Group Policy Management Editor.

Table 3-4. VMware Horizon Client Configuration Template: Scripting Definitions

Setting	Description
`Automatically connect if only one launch item is entitled`	If a user is entitled to only one remote desktop, connect the user to that remote desktop. This setting prevents the user from having to select a remote desktop from a list that contains only one remote desktop.
`Connect all USB devices to the desktop or remote application on launch`	Determines whether all the available USB devices on the client system are connected to the remote desktop or published application when the remote desktop or published application starts.

Table 3-4. VMware Horizon Client Configuration Template: Scripting Definitions (Continued)

Setting	Description
`Connect USB devices to the desktop or remote application when they are plugged in`	Determines whether USB devices are connected to the remote desktop or published application when the devices are plugged in to the client system.
`DesktopLayout`	Specifies the layout of the Horizon Client window that users see when they log into a remote desktop. The layout choices are as follows: ■ `Full Screen` ■ `Multimonitor` ■ `Window – Large` ■ `Window – Small` This setting is available only when the `DesktopName to select setting` is also set.
`DesktopName to select`	Specifies the default remote desktop that Horizon Client uses during login.
`Disable 3rd-party Terminal Services plugins`	Determines whether Horizon Client checks third-party Terminal Services plugins that are installed as normal RDP plugins. If you do not configure this setting, Horizon Client checks third-party plugins by default. This setting does not affect Horizon-specific plugins, such as USB redirection.
`Locked Guest Size`	If the display is used on one monitor, specifies the screen resolution of the remote desktop. This setting does not work if you set the remote desktop display to All Monitors. After you enable this setting, remote desktop autofit functionality is disabled. The minimum screen size is 640x480. The maximum screen size is 4096x4096. This setting applies only to PCoIP connections. **Important** As a best practice, do not set the resolution higher than the maximum resolution supported for the remote desktop, which is set in Horizon Administrator. ■ If 3D is enabled, up to two monitors are supported at a resolution of up to 1920x1200. ■ If 3D is not enabled, up to four monitors are supported at a resolution of up to 2560x1600. In practice, this client-side setting is ignored if it is set to a higher resolution than is possible, given operating system version, amount of vRAM, and color depth of the remote desktop. For example, if the resolution for the remote desktop is set to 1920x1200 in Horizon Administrator, the resolution shown on the client might not be higher than 1920x1200, depending on the capabilities of the remote desktop.
`Logon DomainName`	Specifies the NetBIOS domain that Horizon Client uses during login.
`Logon Password`	Specifies the password that Horizon Client uses during login. The password is stored in plain text by Active Directory. For improved security, do not specify this setting. Users can enter the password interactively.
`Logon UserName`	Specifies the password that Horizon Client uses during login. The password is stored in plain text by Active Directory.
`Server URL`	Specifies the URL that Horizon Client uses during login, for example, `https://view1.example.com`.

Table 3-4. VMware Horizon Client Configuration Template: Scripting Definitions (Continued)

Setting	Description
`Suppress error messages (when fully scripted only)`	Determines whether Horizon Client error messages are hidden during login. This setting applies only when the login process is fully scripted, for example, when all the required login information is prepopulated through group policy. If the login fails because of incorrect login information, users are not notified and the Horizon Client process is terminated.
`Disconnected application session resumption behavior`	Determines how running published applications behave when users reconnect to a server. The choices are as follows: ■ Ask to reconnect to open applications ■ Reconnect automatically to open applications ■ Do not ask and do not automatically reconnect When this setting is enabled, end users cannot configure the published application reconnection behavior in Horizon Client. When this setting is disabled, end users can configure published application reconnection behavior in Horizon Client. This setting is disabled by default.
`Enable Unauthenticated Access to the server`	Determines whether users are required to enter credentials to access their published applications when they use Horizon Client. When this setting is enabled, the **Log in anonymously using Unauthenticated Access** setting in Horizon Client is visible, disabled, and selected. The client can fall back to another authentication method if Unauthenticated Access is not available. When this setting is disabled, users are always required to enter their credentials to log in and access their published applications. The **Log in anonymously using Unauthenticated Access** setting in Horizon Client is hidden and deselected. Users can enable Unauthenticated Access in Horizon Client by default. The **Log in anonymously using Unauthenticated Access** setting is visible, enabled, and deselected.
`Account to use for Unauthenticated Access`	Specifies the Unauthenticated Access user account that Horizon Client uses to log in anonymously to the server if the `Enable Unauthenticated Access to the server` group policy setting is enabled, or if a user enables Unauthenticated Access by selecting **Log in anonymously using Unauthenticated Access** in Horizon Client. If Unauthenticated Access is not used for a specific connection to a server, this setting is ignored. Users can select an account by default.

Security Settings for Client GPOs

Security settings include group policies for certificates, login credentials, and the single sign-on feature.

The following table describes the security settings in the Horizon Client Configuration ADMX template file. This table shows whether the settings include both Computer Configuration and User Configuration settings, or only Computer Configuration settings. For the security settings that include both types of settings, the User Configuration setting overrides the equivalent Computer Configuration setting. These settings appear in the **VMware Horizon Client Configuration > Security Settings** folder in the Group Policy Management Editor.

Table 3-5. Horizon Client Configuration Template: Security Settings

Setting	Computer	User	Description
`Allow command line credentials`	X		Determines whether user credentials can be provided with Horizon Client command-line options. If this setting is disabled, the `smartCardPIN` and `password` options are not available when users run Horizon Client from the command line. This setting is enabled by default. The equivalent Windows Registry value is `AllowCmdLineCredentials`.
`Servers Trusted For Delegation`	X		Specifies the Connection Server instances that accept the user identity and credential information that is passed when a user selects **Log in as current user** in the **Options** menu on the Horizon Client menu bar. If you do not specify any Connection Server instances, all Connection Server instances accept this information. To add a Connection Server instance, use one of the following formats: ■ **`domain\system$`** ■ **`system$@domain.com`** ■ The Service Principal Name (SPN) of the Connection Server service. The equivalent Windows Registry value is `BrokersTrustedForDelegation`.

Table 3-5. Horizon Client Configuration Template: Security Settings (Continued)

Setting	Computer	User	Description
Certificate verification mode	X		Configures the level of certificate checking that Horizon Client performs. You can select one of these modes: ■ No Security. No certificate checking occurs. ■ Warn But Allow. If a certificate check fails because the server uses a self-signed certificate, users see a warning, which they can ignore. For self-signed certificates, the certificate name is not required to match the server name that users enter in Horizon Client. If any other certificate error condition occurs, Horizon Client shows an error and prevents users from connecting to the server. Warn But Allow is the default value. ■ Full Security. If any type of certificate error occurs, users cannot connect to the server. Horizon Client displays certificate errors to the user. When this group policy setting is configured, users can view the selected certificate verification mode in Horizon Client, but cannot configure the setting. The certificate checking mode dialog box informs users that an administrator has locked the setting. When this setting is disabled, Horizon Client users can select a certificate checking mode. This setting is disabled by default. To allow a server to perform selecting of certificates provided by Horizon Client, the client must make HTTPS connections to the Connection Server or security server host. Certificate checking is not supported if you off-load TLS to an intermediate device that makes HTTP connections to the Connection Server or security server host. If you do not want to configure this setting as a group policy, you can also enable certificate verification by adding the CertCheckMode value name to one of the following registry keys on the client computer: ■ For 32-bit Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security ■ For 64-bit Windows: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security Use the following values in the registry key: ■ **0** implements No Security. ■ **1** implements Warn But Allow. ■ **2** implements Full Security. If you configure both the group policy setting and the CertCheckMode setting in the Windows Registry key, the group policy setting takes precedence over the registry key value. **Note** In a future Horizon Client release, using the Windows registry to configure this setting might not be supported and the group policy setting must be used.

Table 3-5. Horizon Client Configuration Template: Security Settings (Continued)

Setting	Computer	User	Description
`Default value of the 'Log in as current user' checkbox`	X	X	Specifies the default value of **Log in as current user** in the **Options** menu on the Horizon Client menu bar. This setting overrides the default value specified during Horizon Client installation. If a user runs Horizon Client from the command line and specifies the `logInAsCurrentUser` option, that value overrides this setting. When **Log in as current user** is selected in the **Options** menu, the identity and credential information that the user provided when logging in to the client system is passed to the Connection Server instance and ultimately to the remote desktop or published application. When **Log in as current user** is deselected, users must provide identity and credential information multiple times before they can access a remote desktop or published application. This setting is disabled by default. The equivalent Windows Registry value is `LogInAsCurrentUser`.
`Display option to Log in as current user`	X	X	Determines whether **Log in as current user** is visible in the **Options** menu on the Horizon Client menu bar. When **Log in as current user** is visible, users can select or deselect it and override its default value. When **Log in as current user** is hidden, users cannot override its default value from the Horizon Client **Options** menu. You can specify the default value for **Log in as current user** by using the policy setting `Default value of the 'Log in as current user' checkbox`. This setting is enabled by default. The equivalent Windows Registry value is `LogInAsCurrentUser_Display`.
`Enable jump list integration`	X		Determines whether a jump list appears in the Horizon Client icon on the taskbar of Windows 7 and later systems. The jump list enables users to connect to recent servers, remote desktops, and published applications. If Horizon Client is shared, you might not want users to see the names of recent desktops and published applications. You can disable the jump list by disabling this setting. This setting is enabled by default. The equivalent Windows Registry value is `EnableJumplist`.

Table 3-5. Horizon Client Configuration Template: Security Settings (Continued)

Setting	Computer	User	Description
Enable SSL encrypted framework channel	X	X	Determines whether TLS is enabled for View 5.0 and earlier remote desktops. Before View 5.0, the data sent over port TCP 32111 to the remote desktop was not encrypted. ■ **Enable**: Enables TLS, but allows fallback to the previous unencrypted connection if the remote desktop does not have TLS support. For example, View 5.0 and earlier remote desktops do not have TLS support. **Enable** is the default setting. ■ **Disable**: Disables TLS. This setting might be useful for debugging, or if the channel is not being tunneled and might potentially be optimized by a WAN accelerator product. ■ **Enforce**: Enables TLS and refuses to connect to remote desktops that do not have TLS support . The equivalent Windows Registry value is `EnableTicketSSLAuth`.
Configures SSL protocols and cryptographic algorithms	X	X	Configures the cipher list to restrict the use of certain cryptographic algorithms and protocols before establishing an encrypted TLS connection. The cipher list consists of one or more cipher strings separated by colons. The cipher string is case-sensitive. The default value is **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** This cipher string means that TLS v1, TLS v1.1, and TLS v1.2 are enabled and SSL v2.0 and v3.0 are removed. Cipher suites use 128-bit or 256-bit AES, remove anonymous DH algorithms, and sort the current cipher list in order of encryption algorithm key length. For more information, see http://www.openssl.org/docs/apps/ciphers.html. The equivalent Windows Registry value is `SSLCipherList`.
Enable Single Sign-On for smart card authentication	X		Determines whether single sign-on is enabled for smart card authentication. When single sign-on is enabled, Horizon Client stores the encrypted smart card PIN in temporary memory before submitting it to Connection Server. When single sign-on is disabled, Horizon Client does not display a custom PIN dialog box. The equivalent Windows Registry value is `EnableSmartCardSSO`.

Table 3-5. Horizon Client Configuration Template: Security Settings (Continued)

Setting	Computer	User	Description
`Ignore certificate revocation problems`	X	X	Determines whether errors associated with a revoked server certificate are ignored. These errors occur when the certificate that the server sends has been revoked or the client cannot verify the certificate's revocation status. This setting is disabled by default.
`Unlock remote sessions when the client machine is unlocked`	X	X	Determines whether the Recursive Unlock feature is enabled. The Recursive Unlock feature unlocks all remote sessions after the client machine has been unlocked. This feature applies only after a user logs in to the server with the Log in as current user feature. This setting is enabled by default.

RDP Settings for Client GPOs

You can configure group policy settings for options such as the redirection of audio, printers, ports, and other devices when you use the Microsoft RDP display protocol.

The following table describes the Remote Desktop Protocol (RDP) settings in the Horizon Client Configuration ADMX template file. All RDP settings are User Configuration settings. The settings appear in the **VMware Horizon Client Configuration > RDP Settings** folder in the Group Policy Management Editor.

Table 3-6. Horizon Client Configuration Administrative Template: RDP Settings

Setting	Description
`Audio redirection`	Determines whether audio information played on the remote desktop is redirected. Select one of the following settings: ■ **Disable Audio**: Audio is disabled. ■ **Play in VM (needed for VoIP USB Support)**: Audio plays within the remote desktop. This setting requires a shared USB audio device to provide sound on the client. ■ **Redirect to client**: Audio is redirected to the client. This setting is the default mode. This setting applies only to RDP audio. Audio that is redirected through MMR plays in the client.
`Enable audio capture redirection`	Determines whether the default audio input device is redirected from the client to the remote session. When this setting is enabled, the audio recording device on the client appears in the remote desktop and can record audio input. The default setting is disabled.
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps`	Specifies the size of the bitmap cache, in kilobytes or megabytes, to use for specific bits per pixel (bpp) bitmap color settings. Separate versions of this setting are provided for the following unit and bpp combinations: ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp

Table 3-6. Horizon Client Configuration Administrative Template: RDP Settings (Continued)

Setting	Description
In-memory bitmap cache size in KB for 8bpp bitmaps	Specifies the size, in kilobytes, of the RAM bitmap cache to use for the 8-bits-per-pixel color setting. If ScaleBitmapCachesByBPP is true (the default), this cache size is multiplied by the bytes per pixel to determine the actual RAM cache size. When this setting is enabled, enter a size in kilobytes.
Bitmap caching/cache persistence active	Determines whether persistent bitmap caching is used (active). Persistent bitmap caching can improve performance, but it requires additional disk space.
Color depth	Specifies the color depth of the remote desktop. Select one of the available settings: ■ 8 bit ■ 15 bit ■ 16 bit ■ 24 bit ■ 32 bit For 24-bit Windows XP systems, you must enable the Limit Maximum Color Depth policy in **Computer Configuration > Administrative Templates > Windows Components > Terminal Services** and set it to 24 bits.
Cursor shadow	Determines whether a shadow appears under the pointer on the remote desktop.
Desktop background	Determines whether the desktop background appears when clients connect to a remote desktop.
Desktop composition	(Windows Vista or later) Determines whether desktop composition is enabled on the remote desktop. When desktop composition is enabled, individual windows no longer draw directly to the screen or primary display device as they did in previous versions of Microsoft Windows. Instead, drawing is redirected to off-screen surfaces in video memory, which are then rendered into a desktop image and presented on the display.
Enable compression	Determines whether RDP data is compressed. This setting is enabled by default.
Enable RDP Auto-Reconnect	Determines whether the RDP client component attempts to reconnect to a remote desktop after an RDP protocol connection failure. This setting has no effect if the **Use secure tunnel connection to desktop** option is enabled in Horizon Administrator. This setting is disabled by default.
Font smoothing	(Windows Vista or later) Determines whether anti-aliasing is applied to the fonts on the remote desktop.
Menu and window animation	Determines whether animation for menus and windows is enabled when clients connect to a remote desktop.
Redirect clipboard	Determines whether the local clipboard information is redirected when clients connect to the remote desktop.
Redirect drives	Determines whether local disk drives are redirected when clients connect to the remote desktop. By default, local drives are redirected. Enabling this setting, or leaving it unconfigured, allows data on the redirected drive on the remote desktop to be copied to the drive on the client computer. Disable this setting if allowing data to pass from the remote desktop to users' client computers represents a potential security risk in your deployment. Another approach is to disable folder redirection in the remote desktop virtual machine by enabling the Microsoft Windows group policy setting, `Do not allow drive redirection`. The `Redirect drives` setting applies to RDP only.

Table 3-6. Horizon Client Configuration Administrative Template: RDP Settings (Continued)

Setting	Description
`Redirect printers`	Determines whether local printers are redirected when clients connect to the remote desktop.
`Redirect serial ports`	Determines whether local COM ports are redirected when clients connect to the remote desktop.
`Redirect smart cards`	Determines whether local smart cards are redirected when clients connect to the remote desktop. **Note** This setting applies to both RDP and PCoIP connections.
`Redirect supported plug-and-play devices`	Determines whether local plug-and-play and point-of-sale devices are redirected when clients connect to the remote desktop. This behavior is different from the redirection that the USB Redirection component of the agent manages.
`Shadow bitmaps`	Determines whether bitmaps are shadowed. This setting has no effect in full-screen mode.
`Show contents of window while dragging`	Determines whether the folder contents appear when users drag a folder to a new location.
`Themes`	Determines whether themes appear when clients connect to a remote desktop.
`Windows key combination redirection`	Determines where Windows key combinations are applied. This setting lets you send key combinations to the remote virtual machine or apply key combinations locally. Key combinations are applied locally by default.
`Enable Credential Security Service Provider`	Specifies whether the remote desktop connection uses Network Level Authentication (NLA). In Windows Vista, remote desktop connections require NLA by default. If the guest operating system requires NLA for remote desktop connections, you must enable this setting or Horizon Client might not connect to the remote desktop. In addition to enabling this setting, you must also verify that the following conditions are met: ■ Both the client and guest operating systems support NLA. ■ Direct client connections are enabled for the Connection Server instance. Tunneled connections are not supported with NLA.

General Settings for Client GPOs

General settings include proxy options, time zone forwarding, multimedia acceleration, and other display settings.

General Settings

The following table describes the general settings in the Horizon Client Configuration ADMX template file. General settings include both Computer Configuration and User Configuration settings. The User Configuration setting overrides the equivalent Computer Configuration setting. The settings appear in the **VMware Horizon Client Configuration** folder in the Group Policy Management Editor.

Table 3-7. Horizon Client Configuration Template: General Settings

Setting	Computer	User	Description
Always on top		X	Determines whether the Horizon Client window is always the topmost window. Enabling this setting prevents the Windows taskbar from obscuring a full-screen Horizon Client window. This setting is disabled by default.
Default value of the "Hide the selector after launching an item" check box	X	X	Sets whether the **Hide the selector after launching an item** check box is selected by default. This setting is disabled by default.
Disable time zone forwarding	X		Determines whether time zone synchronization between the remote desktop and the connected client is disabled.
Disable toast notifications	X	X	Determines whether to disable toast notifications from Horizon Client. Enable this setting if you do not want the user to see toast notifications in the corner of the screen. **Note** If you enable this setting, the user does not see a five-minute warning when the Session Timeout function is active.
Disallow passing through client information in a nested session	X		Specifies whether Horizon Client is prevented from passing through client information in a nested session. When enabled, if Horizon Client is running inside a remote session, it sends the actual physical client information instead of the virtual machine device information. This setting applies to the following client information: device name and domain, client type, IP address, and MAC address. This setting is disabled by default, which means passing through client information in a nested session is allowed.
Don't check monitor alignment on spanning		X	By default, the client desktop does not span multiple monitors if the screens do not form an exact rectangle when they are combined. Enable this setting to override the default. This setting is disabled by default.
Enable multi-media acceleration		X	Determines whether multimedia redirection (MMR) is enabled on the client. MMR does not work correctly if the Horizon Client video display hardware does not have overlay support.
Enable relative mouse	X	X	Enables the relative mouse when using the PCoIP display protocol. Relative mouse mode improves the mouse behavior for certain graphics applications and games. If the remote desktop does not support the relative mouse, this setting is not used. This setting is disabled by default.
Enable the shade		X	Determines whether the shade menu bar at the top of the Horizon Client window is visible. This setting is enabled by default. **Note** The shade menu bar is disabled by default for kiosk mode.
Enable Horizon Client online update	X		Enables the online update feature. This setting is enabled by default. **Note** You can also disable the online update feature by setting the `AUTO_UPDATE_ENABLED` property to 0 when you install Horizon Client from the command line. For more information, see Installation Properties for Horizon Client.

Table 3-7. Horizon Client Configuration Template: General Settings (Continued)

Setting	Computer	User	Description
Tunnel proxy bypass address list	X		Specifies a list of tunnel addresses. The proxy server is not used for these addresses. Use a semicolon (;) to separate multiple entries.
URL for Horizon Client online help	X		Specifies an alternate URL from which Horizon Client can retrieve help pages. This setting is intended for use in environments that cannot retrieve the remotely hosted help system because they do not have Internet access.
URL for Horizon Client online update	X		Specifies an alternate URL from which Horizon Client can retrieve updates. This setting is intended for use in an environment that defines its own private/personal update center. If it is not enabled, the VMware official update server is used.
Pin the shade		X	Determines whether the pin on the shade at the top of the Horizon Client window is enabled and auto-hiding of the menu bar does not occur. This setting has no effect if the shade is disabled. This setting is enabled by default.
Disable desktop disconnect messages	X	X	Specifies whether messages that are normally shown upon remote desktop disconnection should be disabled. These messages are shown by default.
Disable sharing files and folders		X	Specifies whether client drive redirection functionality is available in Horizon Client. When this setting is set to Enabled, all client drive redirection functionality is disabled in Horizon Client, including the ability to open local files with published applications. In addition, the following elements are hidden in the Horizon Client user interface: ■ Sharing panel in the Settings dialog box. ■ **Share Folders** item in the **Option** menu in a remote desktop. ■ **Sharing** item for Horizon Client in the system tray. ■ Sharing dialog box that appears the first time you connect to a remote desktop or application after you connect to a server. When this setting is set to Disabled, the client drive redirection feature is fully functional. This setting is disabled by default.
Always hide the remote floating language (IME) bar for Hosted Apps	X	X	Forces the floating language bar off for application sessions. When this setting is enabled, the floating language bar is never shown in a published application session, regardless of whether the local IME feature is enabled. When this setting is disabled, the floating language bar is shown only if the local IME feature is disabled. This setting is disabled by default.

Table 3-7. Horizon Client Configuration Template: General Settings (Continued)

Setting	Computer	User	Description
Disable opening local files in hosted applications		X	Specifies whether Horizon Client registers local handlers for the file extensions that hosted applications support. When this setting is set to Enabled, Horizon Client does not register any file extension handlers and does not allow the user to override the setting. When this setting is set to Disabled, Horizon Client always registers file extension handlers. By default, file extension handlers are registered, but users can disable the feature in the Horizon Client user interface by using the **Turn on the ability to open a local file with a remote application from the local file system** setting on the Sharing panel in the Settings dialog box. For more information, see Share Access to Local Folders and Drives with Client Drive Redirection. This setting is disabled by default.
Automatically install shortcuts when configured on the Horizon server		X	When published application and remote desktop shortcuts are configured on a Connection Server instance, this setting specifies how and whether the shortcuts are installed on client machines when users connect to the server. When this setting is set to Enabled, shortcuts are installed on client machines. Users are not prompted to install the shortcuts. When this setting is set to Disabled, shortcuts are never installed on client machines. Users are not prompted to install the shortcuts. Users are prompted to install the shortcuts by default.
Block multiple Horizon Client instances per Windows session	X		Prevents a user from starting multiple Horizon Client instances during a Windows session. When this setting is set to Enabled, Horizon Client runs in single-instance mode and a user cannot start multiple Horizon Client instances in a Windows session. When this setting is set to Disabled, a user can start multiple Horizon Client instances in a Windows session. This setting is disabled by default.
Display only smart card certificates during login	X		Specifies whether to list all certificates from user and system stores, or to show only smart card certificates. When this setting is set to Enabled, the certificate selection dialog box shows only smart card certificates. When this setting is set to Disabled, all types of certificates are listed in the certificate selection dialog box. This setting is disabled by default.

USB Settings for Client GPOs

You can define USB policy settings for Horizon Agent and Horizon Client. On connection, Horizon Client downloads the USB policy settings from Horizon Agent and uses those settings, together with the Horizon Client USB policy settings, to determine which devices are available for redirection from the host machine.

Policy Settings for Splitting Composite USB Devices

The following table describes each policy setting for splitting composite USB devices in the Horizon Client Configuration ADMX template file. The settings apply at the computer level. The settings from the GPO at the computer level take precedence over the registry at `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. The settings appear in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

For more information about using policies to control USB redirection, see the *Configuring Remote Desktop Features in Horizon 7* document.

Table 3-8. Horizon Client Configuration Template: USB Splitting Settings

Setting	Properties
`Allow Auto Device Splitting`	Allow the automatic splitting of composite USB devices. The default value is undefined, which equates to **`false`**.
`Exclude Vid/Pid Device From Split`	Excludes a composite USB device specified by vendor and product IDs from splitting. 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-55**`** The default value is undefined.
`Split Vid/Pid Device`	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** Horizon 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.

Policy Settings for Filtering USB Devices

The following table describes the policy settings in the Horizon Client Configuration ADMX template file for filtering USB devices. The settings apply at the computer level. The settings from the GPO at the computer level take precedence over the registry at `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`.

For more information about configuring filter policy settings for USB redirection, see the *Configuring Remote Desktop Features in Horizon 7* document.

Table 3-9. Horizon Client Configuration Template: USB Filtering Settings

Setting	Properties
`Allow Audio Input Devices`	Allows audio input devices to be redirected. The default value is undefined, which equates to **`true`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Audio Output Devices`	Allows audio output devices to be redirected. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow HID-Bootable`	Allows input devices other than keyboards or mice that are available at startup time (also known as hid-bootable devices) to be redirected. The default value is undefined, which equates to **`true`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Device Descriptor Failsafe Behavior`	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`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.
`Allow Other Input Devices`	Allows input devices other than hid-bootable devices or keyboards with integrated pointing devices to be redirected. The default value is undefined, which equates to **`true`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Keyboard and Mouse Devices`	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`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Smart Cards`	Allows smart-card devices to be redirected. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Video Devices`	Allows video devices to be redirected. The default value is undefined, which equates to **`true`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Disable Remote Configuration`	Disables the use of agent settings when performing USB device filtering. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.

Table 3-9. Horizon Client Configuration Template: USB Filtering Settings (Continued)

Setting	Properties
`Exclude All Devices`	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 the agent, and this setting is passed to Horizon Client, the agent setting overrides the Horizon Client setting. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Exclude Device Family`	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, Horizon examines the device family of each interface of a composite USB device to decide which interfaces are excluded. If you have disabled automatic device splitting, Horizon examines the device family of the whole composite USB device. The default value is undefined. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Exclude Vid/Pid Device`	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. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Exclude Path`	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. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.
`Include Device Family`	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. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

Table 3-9. Horizon Client Configuration Template: USB Filtering Settings (Continued)

Setting	Properties
`Include Path`	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. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.
`Include Vid/Pid Device`	Specifies USB devices that have a specified vendor and product ID 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. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

Considerations for Nested Sessions

In a nested mode or double-hop scenario, a user connects from the physical client system to a remote desktop, starts Horizon Client inside the remote desktop (the nested session), and connects to another remote desktop. To make the device work as expected in the nested session, you must configure the USB policy settings in the same way on both the physical client machine and in the nested session.

PCoIP Client Session Variables ADMX Template Settings

The PCoIP Client Session Variables ADMX template file (`pcoip.client.admx`) contains policy settings related to the PCoIP display protocol. You can configure computer default values that an administrator can override, or you can configure user settings that an administrator cannot override. The settings that can be overridden appear in the **PCoIP Client Session Variables > Overridable Administrator Defaults** folder in the Group Policy Management Editor. The settings that cannot be overridden appear in the **PCoIP Client Session Variables > Not Overridable Settings** folder in the Group Policy Management Editor.

The ADMX files are available in `VMware-Horizon-Extras-Bundle-`*x.x.x-yyyyyyy*`.zip`, which you can download from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the ZIP file.

Table 3-10. PCoIP Client Session Variables

Setting	Description
`Configure PCoIP client image cache size policy`	Controls the size of the PCoIP client image cache. The client uses image caching to store portions of the display that were previously transmitted. Image caching reduces the amount of data that is retransmitted. When this setting is disabled, PCoIP uses a default client image cache size of 250 MB. When you enable this setting, you can configure a client image cache size from a minimum of 50 MB to a maximum of 300 MB. The default value is 250 MB. This setting is disabled by default.
`Configure PCoIP event log cleanup by size in MB`	Enables the configuration of the PCoIP event log cleanup by size in MB. When this setting is configured, it controls the log file cleanup by size in MB. For example, for a non-zero setting of *m*, log files larger than *m* MB are silently deleted. A setting of 0 indicates no file cleanup by size. When this setting is disabled, the default event log cleanup by size in MB setting is 100. This setting is disabled by default.
`Configure PCoIP event log cleanup by time in days`	Enables the configuration of the PCoIP event log cleanup by time in days. When this setting is configured, it controls the log file cleanup by time in days. For example, for a non-zero setting of *n*, log files older than *n* days are silently deleted. A setting of 0 indicates no file cleanup by time. When this policy is disabled, the default event log cleanup by time in days setting is 7. This setting is disabled by default. The log file cleanup is performed once, when the session starts. Any change to the setting is not applied until the next session.
`Configure PCoIP event log verbosity`	Sets the PCoIP event log verbosity. The values range from 0 (least verbose) to 3 (most verbose). When this setting is enabled, you can set the verbosity level from 0 to 3. When the setting is disabled, the default event log verbosity level is 2. This setting is disabled by default. When this setting is modified during an active PCoIP session, the new setting takes effect immediately.
`Configure PCoIP session encryption algorithms`	Controls the encryption algorithms advertised by the PCoIP endpoint during session negotiation. Selecting one of the check boxes disables the associated encryption algorithm. You must enable at least one algorithm. This setting applies to both agent and client. The endpoints negotiate the actual session encryption algorithm that is used. If FIPS140-2 approved mode is enabled, the **Disable AES-128-GCM encryption** value is overridden if both AES-128-GCM encryption and AES-256-GCM encryption are disabled. If the `Configure SSL Connections` setting is disabled, both the Salsa20-256round12 and AES-128-GCM algorithms are available for negotiation by this endpoint. This setting is disabled by default. Supported encryption algorithms, in order of preference, are SALSA20/12-256, AES-GCM-128, and AES-GCM-256. By default, all supported encryption algorithms are available for negotiation by this endpoint.

Table 3-10. PCoIP Client Session Variables (Continued)

Setting	Description
`Configure PCoIP virtual channels`	Specifies the virtual channels that can and cannot operate over PCoIP sessions. This setting also determines whether to disable clipboard processing on the PCoIP host. Virtual channels that are used in PCoIP sessions must appear on the virtual channel authorization list. Virtual channels that appear in the unauthorized virtual channel list cannot be used in PCoIP sessions. You can specify a maximum of 15 virtual channels for use in PCoIP sessions. Separate multiple channel names with the vertical bar (|) character. For example, the virtual channel authorization string to allow the mksvchan and vdp_rdpvcbridge virtual channels is **`mksvchan|vdp_rdpvcbridge`**. If a channel name contains the vertical bar or backslash (\) character, insert a backslash character before it. For example, type the channel name awk|ward\channel as **`awk|ward\\channel`**. When the authorized virtual channel list is empty, all virtual channels are disallowed. When the unauthorized virtual channel list is empty, all virtual channels are allowed. The virtual channels setting applies to both agent and client. Virtual channels must be enabled on both agent and client for virtual channels to be used. The virtual channels setting provides a separate check box that allows you to disable remote clipboard processing on the PCoIP host. This value applies to the agent only. By default, all virtual channels are enabled, including clipboard processing.
`Configure SSL cipher list`	Configures a TLS/SSL cipher list to restrict the use of cipher suites before establishing an encrypted TLS/SSL connection. The list consists of one or more cipher suite strings separated by colons. All cipher suite strings are case insensitive. The default value is ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH. If this setting is configured, the **Enforce AES-256 or stronger ciphers for SSL connection negotiation** check box in the `Configure SSL connections to satisfy Security Tools` setting is ignored. This setting must be applied to both the PCoIP server and the PCoIP client.
`Configure SSL connections to satisfy Security Tools`	Specifies how TLS session negotiation connections are established. To satisfy security tools, such as port scanners, enable this setting and do the following: 1 Store the certificate for the Certificate Authority that signed any Server certificate to be used with PCoIP in the Trusted Root certificate store. 2 Configure the agent to load certificates only from the Certificate Store. If the Personal store for the Local Machine is used, leave the CA Certificate store name unchanged with the value ROOT, unless a different store location was used in step 1. If this setting is disabled, the AES-128 cipher suite is not available and the endpoint uses Certification Authority certificates from the machine account's MY store and Certification Authority certificates from the ROOT store. This setting is disabled by default.
`Configure SSL protocols`	Configures the OpenSSL protocol to restrict the use of certain protocols before establishing an encrypted TLS connection. The protocol list consists of one or more OpenSSL protocol strings separated by colons. All cipher strings are case insensitive. The default value is `TLS1.1:TLS1.2`, which means that TLS v1.1 and TLS v1.2 are enabled and SSL v2.0, SSLv3.0, and TLS v1.0 are disabled. If this setting is set in both the client and the agent, the OpenSSL protocol negotiation rule is followed.

Table 3-10. PCoIP Client Session Variables (Continued)

Setting	Description
`Configure the Client PCoIP UDP port`	Specifies the UDP client port that is used by software PCoIP clients. The UDP port value specifies the base UDP port to use. If the base port is not available, the UDP port range value determines how many additional ports to try. The range spans from the base port to the sum of the base port and port range. For example, if the base port is 50002 and the port range is 64, the range spans from 50002 to 50066. This setting applies to the client only. By default, the base port is 50002 and the port range is 64.
`Configure the maximum PCoIP session bandwidth`	Specifies the maximum bandwidth, in kilobits per second, in a PCoIP session. The bandwidth includes all imaging, audio, virtual channel, USB, and control PCoIP traffic. Set this value to the overall capacity of the link to which your endpoint is connected, considering the number of expected concurrent PCoIP sessions. For example, with a single-user VDI configuration (a single PCoIP session) that connects through a 4Mbit/s Internet connection, set this value to 4Mbit, or 10% less than this value to leave some allowance for other network traffic. When you expect multiple concurrent PCoIP sessions to share a link, comprising either multiple VDI users or an RDS configuration, you might want to adjust the setting accordingly. However, lowering this value will restrict the maximum bandwidth for each active session. Setting this value prevents the agent from attempting to transmit at a higher rate than the link capacity, which would cause excessive packet loss and a poorer user experience. This value is symmetric. It forces the client and agent to use the lower of the two values that are set on the client and agent side. For example, setting a 4 Mbit/s maximum bandwidth forces the agent to transmit at a lower rate, even though the setting is configured on the client. When this setting is disabled on an endpoint, the endpoint imposes no bandwidth constraints. When this setting is enabled, the setting is used as the endpoint's maximum bandwidth constraint in kilobits per second. The default value is 900000 kilobits per second. This setting applies to the agent and the client. If the two endpoints have different settings, the lower value is used.
`Configure the PCoIP session bandwidth floor`	Specifies a lower limit, in kilobits per second, for the bandwidth that the PCoIP session reserves. This setting configures the minimum expected bandwidth transmission rate for the endpoint. When you use this setting to reserve bandwidth for an endpoint, the user does not have to wait for bandwidth to become available, which improves session responsiveness. Make sure that you do not over-subscribe the total reserved bandwidth for all endpoints. Make sure that the sum of bandwidth floors for all connections in your configuration does not exceed the network capability. The default value is 0, which means that no minimum bandwidth is reserved. When this setting is disabled, no minimum bandwidth is reserved. This setting is disabled by default. This setting applies to the agent and the client, but the setting only affects the endpoint on which it is configured. When this setting is modified during an active PCoIP session, the change takes effect immediately.

Table 3-10. PCoIP Client Session Variables (Continued)

Setting	Description
`Configure the PCoIP session MTU`	Specifies the Maximum Transmission Unit (MTU) size for UDP packets for a PCoIP session. The MTU size includes IP and UDP packet headers. TCP uses the standard MTU discovery mechanism to set MTU and this setting does not affect it. The maximum MTU size is 1500 bytes. The minimum MTU size is 500 bytes. The default value is 1300 bytes. Typically, you do not have to change the MTU size. Change this value if you have an unusual network setup that causes PCoIP packet fragmentation. This setting applies to the agent and the client. If the two endpoints have different MTU size settings, the lowest size is used. If this setting is disabled or not configured, the client uses the default value in the negotiation with the agent.
`Configure the PCoIP transport header`	Configures the PCoIP transport header and sets the transport session priority. The PCoIP transport header is a 32-bit header that is added to all PCoIP UDP packets (only if the transport header is enabled and both side support it). The PCoIP transport header allows network devices to make better prioritization/QoS decisions when dealing with network congestion. The transport header is enabled by default. The transport session priority determines the PCoIP session priority reported in the PCoIP transport header. Network devices make better prioritization/QoS decisions based on the specified transport session priority. When the `Configure the PCoIP transport header` setting is enabled, the following transport session priorities are available: ■ **High** ■ **Medium** (default value) ■ **Low** ■ **Undefined** The PCoIP agent and client negotiate the transport session priority value. If the PCoIP agent specifies a transport session priority value, the session uses the agent-specified session priority. If only the client has specified a transport session priority, the session uses the client-specified session priority. If neither agent nor client has specified a transport session priority, or **Undefined Priority** is specified, the session uses the default value, **Medium** priority.
`Enable/disable audio in the PCoIP session`	Determines whether audio is enabled in PCoIP sessions. Both endpoints must have audio enabled. When this setting is enabled, PCoIP audio is allowed. When it is disabled, PCoIP audio is disabled. Audio is enabled by default.

Running Horizon Client from the Command Line

You can run Horizon Client from the command line or from scripts. You might want to run Horizon Client from the command line if you are implementing a kiosk-based application that grants end users access to remote desktop applications.

To run Horizon Client from the command line, you use the `vmware-view.exe` command. The `vmware-view.exe` command includes options that you can specify to change the behavior of Horizon Client.

Horizon Client Command Use

The syntax of the `vmware-view` command controls the operation of Horizon Client.

Use the following form of the `vmware-view` command from a Windows command prompt.

```
vmware-view [command_line_option [argument]] ...
```

The default path to the `vmware-view` command executable file depends on the client system. You can add this path to the *PATH* environment variable on the client system.

- 32-bit systems: `C:\Program Files\VMware\VMware Horizon View Client\`
- 64-bit systems: `C:\Program Files (x86)\VMware\VMware Horizon View Client\`

The following table shows the command-line options that you can use with the `vmware-view` command.

Table 3-11. Horizon Client Command-Line Options

Option	Description
`/?`	Displays the list of command options.
`-appName` *application_name*	Specifies the name of the published application as it appears in the desktop and application selection window. The name is the display name that was specified for the application pool in the pool creation wizard.
`-appProtocol` *protocol*	Specifies the published application display protocol to use, if available. The valid protocols are as follows: ■ **`VMware Blast`** ■ **`PCoIP`**
`-appSessionReconnectionBehavior` *argument*	Specifies the published application reconnection behavior setting. The valid arguments are as follows: **`always`** Implements the **Reconnect automatically to open applications** setting. **`never`** Implements the **Do not ask to reconnect and do not automatically reconnect** setting. **`ask`** Implements **Ask to reconnect to open applications** setting. When you use this option, the published application reconnection settings are disabled in Horizon Client.
`-args` *argument*	Specifies command-line arguments to add when a published application starts. For example: `vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""`
`-connectUSBOnStartup`	When set to `true`, redirects all USB devices that are connected to the host to the remote desktop or published application. This option is implicitly set if you specify the `-unattended` option for a remote desktop. The default is `false`.
`-connectUSBOnInsert`	When set to `true`, connects a USB device to the foreground remote desktop or published application when you plug in the device. This option is implicitly set if you specify the `-unattended` option for a remote desktop. The default is `false`.

Table 3-11. Horizon Client Command-Line Options (Continued)

Option	Description
`–desktopLayout` *window_size*	Specifies how to display the remote desktop window. The valid window size values are as follows: **`fullscreen`** Full-screen display. **`multimonitor`** Multiple-monitor display. **`windowLarge`** Large window. **`windowSmall`** Small window. **`length X width`** Custom size, for example, 800 X 600.
`–desktopName` *desktop_name*	Specifies the name of the remote desktop as it appears in the desktop and application selection window. The name is the display name that was specified for the pool in the pool creation wizard. **Important** Do not specify this option for clients in kiosk mode. This option has no effect when in the remote desktop runs in kiosk mode. For kiosk mode, the connection is made to the first remote desktop in the list of entitled remote desktops.
`–desktopProtocol` *protocol*	Specifies the display protocol to use as it appears in the desktop and application selection window. The valid display protocols are as follows: ■ **`Blast`** ■ **`PCoIP`** ■ **`RDP`**
`–domainName` *domain_name*	Specifies the NETBIOS domain that the end user uses to log in to Horizon Client. For example, use `mycompany` rather than `mycompany.com`.
`–file` *file_path*	Specifies the path of a configuration file that contains additional command options and arguments. See Horizon Client Configuration File.
`–h`	Shows help options.
`–hideClientAfterLaunchSession`	When set to `true`, hides the desktop and application selector window and the **Show VMware Horizon Client** menu after starting a remote session. When set to `false`, shows the desktop and application selector window and the **Show VMware Horizon Client** menu after starting a remote session. The default is `true`.
`–languageId` *Locale_ID*	Provides localization support for different languages in Horizon Client. If a resource library is available, specify the Locale ID (LCID) to use. For US English, enter the value 0x409.

`–listMonitors`	Lists index values and display layout information for the connected monitors. For example:
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (–900, –410, 0, 1190)`
	You use these index values in the `–monitors` option.

`–logInAsCurrentUser`	When set to `true`, uses the credential information that the end user provides when logging in to the client system to log in to the server and ultimately to the remote desktop. The default is `false`.

Table 3-11. Horizon Client Command-Line Options (Continued)

Option	Description
`–monitors "n[,n,n,n]"`	Specifies monitors to use in a multiple-monitor setup, where *n* is the index value of a monitor. You can use the `–listMonitors` option to determine the index values of the connected monitors. You can specify up to four index values, separated by commas. For example: `–monitors "1,2"` This option has no effect unless `–desktopLayout` is set to `multimonitor`.
`–nonInteractive`	Suppresses error message boxes when starting Horizon Client from a script. This option is implicitly set if you specify the `–unattended` option. **Note** If you log in to a server in non-interactive mode, you are not prompted to install **Start** menu shortcuts (if available), and shortcuts are installed by default.
`–noVMwareAddins`	Prevents loading of VMware-specific virtual channels, such virtual printing.
`–password` *password*	Specifies the password that the end user uses to log in to Horizon Client. The password is processed in plain text by the command console or any scripting tool. If you generate the password automatically, you do not need to specify this option for clients in kiosk mode. For improved security, do not specify this option. Users can enter the password interactively.
`–printEnvironmentInfo`	Displays the IP address, MAC address, and machine name of the client device.
`–serverURL` *connection_server*	Specifies the URL, IP address, or FQDN of the server.
`–shutdown`	Shuts down all remote desktops and published applications and relevant user interface components.
`–singleAutoConnect`	If the user is entitled to only one remote desktop or published application, connects to that remote desktop or published application after the user authenticates to the server. This setting saves the user from selecting a remote desktop or published application from a list that contains only one item.
`–smartCardPIN` *PIN*	Specifies the PIN when an end user inserts a smart card to log in.
`–usernameHint` *user_name*	Specifies the account name to use as the user name hint.
`–standalone`	Starts a second instance of Horizon Client that can connect to the same or a different server. This option is supported for backwards compatibility. Specifying `–standalone` is not necessary as it is the default behavior for the client. For multiple remote desktop connections to the same or a different server, using the secure tunnel is supported. **Note** The second remote desktop connection might not have access to the local hardware, such as USB devices, smart, cards, printers, and multiple monitors.
`–supportText` *file_name*	Specifies the full path of a text file. The content of the file is displayed in the Support Information dialog box.

Table 3-11. Horizon Client Command-Line Options (Continued)

Option	Description
`–unattended`	Starts Horizon Client in a noninteractive mode that is suitable for clients in kiosk mode. You must also specify the following information: ■ The account name of the client, if you did not generate the account name from the MAC address of the client device. The name must begin with the string “custom-”, or an alternate prefix that you have configured in ADAM. ■ The password of the client, if you did not generate a password automatically when you set up the account for the client. The `–unattended` option implicitly sets the `–nonInteractive`, `–connectUSBOnStartup`, `–connectUSBOnInsert` , and `–desktopLayout multimonitor`options.
`–unauthenticatedAccessAccount`	Specifies an Unauthenticated Access user account to use to log in anonymously to the server when Unauthenticated Access is enabled. If Unauthenticated Access is not enabled, this option is ignored. For example: `vmware–view.exe –serverURL ag–broker.agwork.com –unauthenticatedAccessEnabled true –unauthenticatedAccessAccount anonymous1`
`–unauthenticatedAccessEnabled`	When set to `true`, enables Unauthenticated Access. If Unauthenticated Access is not available, the client can fall back to another authentication method. The **Log in anonymously using Unauthenticated Access** setting is visible, disabled, and selected in Horizon Client. When set to `false`, requires you to enter your credentials to log in and access your applications. The **Log in anonymously using Unauthenticated Access** setting is hidden and deselected in Horizon Client. If you do not specify this option, you can enable Unauthenticated Access in Horizon Client. The **Log in anonymously using Unauthenticated Access** setting is visible, enabled, and deselected.

Table 3-11. Horizon Client Command-Line Options (Continued)

Option	Description

`–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 user name, domain, and server URL exists and, if it does, reuses that session instead of creating a session.
	For example, in the following command, user-1 starts the Calculator application and a new session is created.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Calculator –serverURL view.mycompany.com –useExisting`
	In the next command, user1 starts the Paint application with the same user name, domain, and server URL, and the same session is used.
	`vmware–view.exe –userName user–1 –password secret –domainName domain –appName Paint –serverURL view.mycompany.com –useExisting`

`–userName` *user_name*	Specifies the account name that the end user uses to log in to Horizon Client. If you generate the account name from the MAC address of the client device, you do not need to specify this option for clients in kiosk mode.

You can specify all options by Active Directory group policies, except for `–file`, `–languageId`, `–printEnvironmentInfo`, `–smartCardPIN`, and `–unattended`.

Note Group policy settings take precedence over settings that you specify from the command line.

Horizon Client Configuration File

You can read command-line options for Horizon Client from a configuration file.

You can specify the path of the configuration file as an argument to the `–file` *file_path* option of the `vmware–view` command. The file must be a Unicode (UTF-16) or ASCII text file.

Example: Example of a Configuration File for a Noninteractive Application

The following example shows the contents of a configuration file for a noninteractive application.

```
–serverURL https://view.yourcompany.com
–userName autouser
–password auto123
–domainName companydomain
–desktopName autodesktop
–nonInteractive
```

Example: Example of a Configuration File for a Client in Kiosk Mode

The following example shows a client in kiosk mode where the account name is based on the client's MAC address. The client has an automatically generated password.

```
–serverURL 145.124.24.100
–unattended
```

Using the Windows Registry to Configure Horizon Client

You can define default settings for Horizon Client in the Windows Registry instead of specifying these settings on the command line. Group policy settings take precedence over Windows Registry settings, and Windows Registry settings take precedence over the command line.

Note In a future version of Horizon Client, Windows registry settings might not be supported and group policy settings must be used.

The following table lists the registry settings for logging in to Horizon Client. These settings are located under `HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\` in the registry. This location is specific to a particular user. The `HKEY_LOCAL_MACHINE` settings, which are described in the next table, are computer-wide settings and pertain to all local users and all domain users that have permission to log in to the computer in a Windows domain environment.

Table 3-12. Horizon Client Registry Settings for Credentials

Registry Setting	Description
`Password`	Default password.
`UserName`	Default user name.

The following table lists the registry settings for Horizon Client that do not include login credentials. The location of these settings depends on the type of system as follows:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- For 64-bit Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Table 3-13. Horizon Client Registry Settings

Registry Setting	Description
`DomainName`	Default NETBIOS domain name. For example, you might use `mycompany` rather than `mycompany.com`.
`EnableShade`	Determines whether the menu bar (shade) at the top of the Horizon Client window is enabled. The menu bar is enabled by default, except for clients in kiosk mode. A value of **`false`** disables the menu bar. **Note** This setting is applicable only when you have the display layout set to **All Monitors** or **Fullscreen**.

Table 3-13. Horizon Client Registry Settings (Continued)

Registry Setting	Description
ServerURL	URL, IP address, or FQDN of the default Connection Server instance.
EnableSoftKeypad	If set to **true** and a Horizon Client window has focus, the physical keyboard, onscreen keyboard, mouse, and handwriting pad events are sent to the remote desktop or published application, even if the mouse or onscreen keyboard is outside the Horizon Client window. The default is **false**.

The following table shows security settings that you can add. The location of these settings depends on the type of system as follows:

- For 32-bit Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security
- For 64-bit Windows: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security

Table 3-14. Security Settings

Registry Setting	Description and Valid Values
CertCheckMode	Certificate checking mode. Valid values are as follows: ■ **0** implements Do not verify server identity certificates. ■ **1** implements Warn before connecting to untrusted servers. ■ **2** implements Never connect to untrusted servers.
SSLCipherList	Configures the cipher list to restrict the use of certain cryptographic algorithms and protocols before establishing an encrypted TLS connection. The cipher list consists of one or more cipher strings separated by colons. All cipher strings are case-sensitive. The default value is **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. This value means that TLSv.1, TLSv1.1, and TLSv1.2 are enabled and SSL v2.0 and SSL v3.0 are removed. Cipher suites use 128-bit or 256-bit AES, remove anonymous DH algorithms, and sort the current cipher list in order of encryption algorithm key length. For reference information about the configuration, see http://www.openssl.org/docs/apps/ciphers.html .

Managing Remote Desktop and Published Application Connections

4

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

To connect to a remote desktop or published application, you must provide the name of a server and supply credentials for your user account.

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

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.
- Configure the certificate checking mode for the certificate presented by the server. To determine which mode to use, see Setting the Certificate Checking Mode in Horizon Client.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Start Horizon Client.
3. (Optional) To log in as the currently logged-in Windows domain user, click the **Options** button on the menu bar and select **Log in as current user**.

   This setting is available only if the **Log in as current user** feature is installed on the client system.
4. Connect to a server.

Option	Action
Connect to a new server	Double-click the **+ Add Server** button, or click the **+ New Server** button in the menu bar, enter the name of a server, and click **Connect**.
Connect to an existing server	Double-click the server icon, or right-click the server icon and select **Connect**.

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

   You might see a message that you must confirm before the login dialog box appears.
5. If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Continue**.

6 Enter the credentials of a user who is entitled to use at least one remote desktop or published application, select the domain, and click **Login**.

   If you enter the user name as **username@domain**, Horizon Client treats it as a user principal name (UPN) and the **Domain** drop-down menu is disabled.

   If the **Domain** drop-down menu is hidden, you must enter the user name as ***username@domain*** or ***domain\username***.

7 If Horizon Client prompts you to install published applications or remote desktops to the Windows **Start** menu, click **Yes** or **No**.

   This prompt can appear the first time you connect to a server on which shortcuts have been configured for published applications or remote desktops. If you click **Yes**, **Start** menu shortcuts are installed on the client system for those published applications or remote desktops, if you are entitled to use them. If you click **No**, **Start** menu shortcuts are not installed.

   A Horizon administrator can configure the **Automatically install shortcuts when configured on the Horizon server** group policy setting to prompt end users to install shortcuts (the default), install shortcuts automatically, or never install shortcuts.

8 (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.

9 To connect to a remote desktop or published application, double-click the remote desktop or published application icon.

   If you are connecting to a published desktop, and if the published desktop is already set to use a different display protocol, you cannot connect immediately. Horizon Client prompts you to use the set protocol or to log off so that Horizon Client can connect with a different display protocol.

After you are connected, the remote desktop or published application opens.

If you are entitled to more than one remote desktop or published application on the server, the desktop and application selector window remains open so that you can connect to multiple remote desktops and published applications.

If the client drive redirection feature is enabled, the Sharing dialog box appears and you can allow or deny access to files on the local file system. For more information, see Share Access to Local Folders and Drives with Client Drive Redirection.

The first time you connect to a server, Horizon Client saves a shortcut to the server on the Horizon Client home window. You can double-click this server shortcut the next time you need to connect to the server.

If authentication to the server fails, or if the client cannot connect to the remote desktop or published application, perform the following tasks:

- Verify that the certificate for the server is working properly. If it is not, in Horizon Administrator, you might also see that the agent on remnote 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 remote desktop or published application. See the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.
- If you are using the RDP display protocol to connect to a remote desktop, verify that the remote desktop operating system allows remote desktop connections.

What to do next

Configure startup settings. If you do not want to require end users to provide the host name of the server, or if you want to configure other startup settings, use a command-line option to create a remote desktop shortcut. See Running Horizon Client from the Command Line.

Use Unauthenticated Access to Connect to Published Applications

A Horizon administrator can create Unauthenticated Access users and entitle those users to published applications on a particular server. Unauthenticated Access users can log in to a server anonymously to connect to their published applications.

Before you have end users access a published application with the Unauthenticated Access feature, test that you can connect to the published application from a client device. You might need to specify a server and supply credentials for your user account.

By default, users select the **Log in anonymously using Unauthenticated Access** setting from the **Options** menu and select a user account to log in anonymously. A Horizon administrator can configure group policy settings to preselect the **Log in anonymously using Unauthenticated Access** setting and log in users with a specific Unauthenticated Access user account.

Prerequisites

- Perform the administrative tasks described in Preparing Connection Server for Horizon Client.
- Set up Unauthenticated Access users on the Connection Server instance. For information, see "Providing Unauthenticated Access for Published Applications" in the *Horizon 7 Administration* document.
- If you are outside the corporate network, verify that your 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 published application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.
- Configure the certificate checking mode for the certificate presented by the server in Horizon Client. To determine which mode to use, see Setting the Certificate Checking Mode in Horizon Client.
- (Optional) Configure the **Account to use for Unauthenticated Access** and **Log in anonymously using Unauthenticated Access** group policy settings to change the default Unauthenticated Access behavior. For information, see Scripting Definition Settings for Client GPOs.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Start Horizon Client.
3. Click the **Options** button in the menu bar and select **Log in anonymously using Unauthenticated Access**.

   Depending on how the client system is configured, this setting might be preselected.
4. Connect to the server on which you have unauthenticated access to published applications.

Option	Action
Connect to a new server	Double-click the **+ Add Server** button or click the **+ New Server** button in the menu bar, enter the name of the server, and click **Connect**.
Connect to an existing server	Double-click the server icon on the Horizon Client home window.

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

   You might see a message that you must confirm before the Login dialog box appears.
5. When the Login dialog box appears, select a user account from the **User account** drop-down menu, if necessary.

   If only one user account is available, the drop-down menu is disabled and the user account is preselected.
6. (Optional) If the **Always use this account** check box is available, select it to bypass the Login dialog box the next time you connect to the server.

   To deselect this setting before you connect to the server the next time, right-click the server icon on the Horizon Client home window and select **Forget the saved Unauthenticated Access account**.
7. Click **Login** to log in to the server.

   The application selector window appears.
8. To start a published application, double-click the published application icon.

Tips for Using the Desktop and Application Selector

You can reorganize or reduce the number of icons on the Horizon Client desktop and application selector window.

After you connect to a particular server, a window appears that includes icons for all the remote desktops and published applications that you are entitled to use. Try the following suggestions to open your most frequently used remote desktops and published applications.

- Type the first few letters of the name. For example, if you have icons for Paint, PowerPoint, and Publisher, you can type **pa** to select the Paint published application.

  If more than one item matches the letters that you type, you can press F4 to go to the next matching item. When you get to the last item, you can press F4 to go back to the first matching item.
- To mark an icon as a favorite, right-click the icon and select **Mark as Favorite** from the context menu. After you select favorites, click the **Show Favorites View** button (star icon) to remove all the icons that are not favorites.
- To change the order of icons while in the Favorites view, select an icon and drag it to a new location. When you are not in the Favorites view, remote desktop icons are listed first, followed by published application icons, and the icons are in alphabetical order. To reposition the icons, drag them to new locations.

  Horizon Client saves the new icon order on the server when you disconnect from the server and when you open a published application or remote desktop. If you do not manually disconnect from the server or open a published application or remote desktop, your changes are not saved.
- To open the remote desktop or published application from the client system and avoid the selector window, create a shortcut by right-clicking the icon and selecting **Create Shortcut** from the context menu.
- To open the remote desktop or published application from your own local Start menu and avoid the selector window, right-click the remote desktop or published application icon and select **Add to Start Menu** from the context menu.

Note If you are using a Windows 7 or later client system, you can open Horizon Client and right-click the Horizon Client icon in the Windows taskbar to select recently used servers, remote desktops, and published applications. Up to 10 items appear in the list. To remove an item, right-click it and select **Remove from this list**.

If you right-click the Horizon Client icon in the taskbar and do not see a jump list, right-click the taskbar, select **Properties**, and click the **Start Menu** tab. In the Privacy section, select the **Store and display recently opened items in the Start menu and the taskbar** check box, and click **OK**.

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. Mapped drives can have UNC (Universal Naming Convention) paths.

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.

You can also turn on the ability to open local files in published applications directly from the local file system. With this feature, the **Open with** menu on the client system lists the available published applications when you right-click a local file.

You can also set files to be opened automatically in published applications when you double-click the file. With this feature, all files on your local file system that have certain file extensions are registered with the server that you are logged in to. For example, if Microsoft Word is a published application on the server, you can right-click a `.docx` file on your local file system and open the file with the Microsoft Word published application.

This feature requires Horizon 6 version 6.2 or later servers and agents.

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 to control the client drive redirection behavior. Support for UNC paths requires Horizon Agent 7.3 or later. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

You can hide the client drive redirection feature in Horizon Client by enabling a group policy setting. For more information, see **Disable sharing files and folders** in General Settings for Client GPOs.

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 and display the Sharing panel.

Option	Description
From the desktop and application selector window	Right-click a remote desktop or published application icon, select **Settings**, and select **Sharing** in the left panel of the window that appears.
From the Sharing dialog box that appears when you connect to a remote desktop or published application	Click the **Settings > Sharing** link in the dialog box.
From within a remote desktop	Select **Options > Share Folders** from the menu bar.

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. Also, do not turn on the USB redirection feature that connects USB devices automatically at startup or when the device is inserted. If you do so, the next time you start Horizon Client or plug in the USB device, the device connects with the USB redirection feature instead of with the client drive redirection feature.
Stop sharing a specific folder or drive	Select the folder or drive in the Folder list and click the **Remove** button.
Give remote desktops and published applications access to files in your local user directory	Select the **Share your local files *user-name*** 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.

Option	Action
Turn on the ability to open a local file with a published application from the local file system	Select the **Open local files in hosted applications** check box. With this option, you can right-click a file in your local file system and select to open the file in a published application. You can also change the properties of the file so that all files with that file extension are opened with the published application by default, such as when you double-click the file. For example, you can right-click a file, select **Properties**, and click **Change** to select the published application to open files of that type. A Horizon administrator can disable this feature.
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:

- ***name* on *MACHINE-NAME***. For example, **jsmith on JSMITH-W03**.
- ***N* on *MACHINE-NAME***. For example, **Z on JSMITH-W03**.
- ***name* (*N*:)**. For example, **jsmith (Z:)**.

A redirected folder can have two entrances, such as **Z on JSMITH-W03** and **jsmith (Z:)**, 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, such as **Z on JSMITH-W03**.

Hide the VMware Horizon Client Window

You can hide the VMware Horizon Client window after you open a remote desktop or published application.

You can use a group policy setting to configure whether the window is always hidden after a remote desktop or published application opens. For more information, see General Settings for Client GPOs.

Procedure

- To hide the VMware Horizon Client window after you open a remote desktop or published application, click the **Close** button in the corner of the VMware Horizon Client window.

- To configure a setting that always hides the VMware Horizon Client window after a remote desktop or published application opens, before you connect to a server, click the **Options** button in the menu bar and select **Hide the selector after launching an item**.
- To show the VMware Horizon Client window after it has been hidden, right-click the VMware Horizon Client icon in the system tray and select **VMware Horizon Client**, or, if you are logged in to a remote desktop, click the **Options** button in the menu bar and select **Switch to Other Desktop**.

Reconnecting to a Remote Desktop or Published Application

For security purposes, a Horizon administrator can set timeouts that log you off a server and lock a published application after some period of inactivity.

By default, you must log in again if you have Horizon Client open and are connected to a particular server for more than 10 hours. This timeout applies to both remote desktop and published application connections.

You receive a warning prompt 30 seconds before a published application is locked automatically. If you do not respond, the published application is locked. By default, the timeout occurs after 15 minutes of inactivity, but a Horizon administrator can change the timeout period.

For example, if you have one or more published applications open and you walk away from your computer, the published application windows might no longer be open when you return an hour later. Instead, you might see a dialog box that prompts you to click **OK** so that the published application windows appear again.

To configure these timeout settings in Horizon Administrator, go to **Global Settings** and edit the general settings.

Create a Shortcut on the Windows Client Desktop or in the Start Menu

You can create a shortcut for a remote desktop or published application. The shortcut appears on the client system's desktop, just like shortcuts for locally installed applications. You can also create a Windows Start menu shortcut.

Procedure

1. Start Horizon Client and log in to the server.
2. In the desktop and application selector window, right-click a remote desktop or published application and select **Create Shortcut to Desktop** or **Add to Start Menu** from the context menu.

Depending on the command that you selected, Horizon Client creates a shortcut on the desktop or in the Windows Start menu on the client system.

What to do next

You can rename, delete, or perform any action on a shortcut that you can perform on shortcuts for locally installed applications. If you are not already logged in to the server when you use the shortcut, Horizon Client prompts you to log in before the remote desktop or published application opens.

Using Shortcuts Created by the Server

A Horizon administrator might configure Start menu or desktop shortcuts for certain remote desktops and published applications.

Start menu shortcuts are supported on Horizon 7 version 7.3 and later servers. Desktop shortcuts are supported on Horizon 7 version 7.5 and later servers.

If you are entitled to a remote desktop or published application that has shortcuts, Horizon Client places the shortcuts in the Start menu, on the desktop, or both, on the client system when you connect to the server.

For Start menu shortcuts, on Windows 7 systems, Horizon Client places shortcuts in the VMware Applications folder in the Start menu. On Windows 8 and Windows 10 systems, Horizon Client places shortcuts in the Apps list. If a Horizon administrator creates a category folder for a shortcut, the category folder appears under the VMware Applications folder or as a category in the Apps list.

You can use a group policy setting to configure whether Horizon Client installs shortcuts automatically, prompts end users before installing shortcuts, or never installs shortcuts. For more information, see the **Automatically install shortcuts when configured on the Horizon server** group policy setting in General Settings for Client GPOs.

If you are not already logged in to the server when you click a server-created shortcut, Horizon Client prompts you to log in before the remote desktop or published application opens.

If a Horizon administrator modifies remote desktop and published application shortcuts on the server, by default the shortcuts are updated on the client system the next time you connect to that server. You can change the default shortcut update behavior in Horizon Client. For more information, see Configure the Shortcut Update Behavior.

To remove server-created shortcuts from the client system, you can delete the server from the Horizon Client server selection window or uninstall Horizon Client.

Note Users are not prompted to install server-created shortcuts, and server-created shortcuts are not created, on clients in kiosk mode.

Configure the Shortcut Update Behavior

You can configure whether changes made to remote desktop and published application shortcuts on the server are applied to the client system when you connect to the server.

Prerequisites

You cannot change the shortcut update setting unless you have previously installed a shortcut from a server.

Procedure

1 Open the Settings dialog box in Horizon Client and select **Shortcuts**.

- Click the **Settings** (gear) icon in the upper right corner of the desktop and application selector window.
- Right-click a remote desktop or published application icon and select **Settings**.

2 Select or deselect the **Automatically update list of application and desktop shortcuts** check box.

3 To save your changes, click **OK**.

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 published application from the same server or from a different server.

Option	Action
Choose a different remote desktop or published application on the same server	Perform one of the following actions: ■ If you are logged in to a remote desktop select **Options > Switch to Other Desktop** from the Horizon Client menu bar, and select another remote desktop or a published application. ■ If you are logged in to a published application, right-click the **VMware Horizon Client** icon in the system tray, select **VMware Horizon Client** to display the desktop and application selector window, and double-click the icon for the other remote desktop or published application. ■ From the desktop and application selector window, double-click the icon for the other remote desktop or published application. That remote desktop or published application opens in a new window. You now have multiple windows open, and you can switch between them.
Choose a different remote desktop or published application on a different server	Perform one of the following actions: ■ To keep the current remote desktop or published application open and also connect to a remote desktop or published application on another server, start a new instance of Horizon Client and connect to the other remote desktop or published application. ■ To close the current remote desktop and connect to a remote desktop on another server, go to the desktop and application selector window, click the **Disconnect** icon in the upper-left corner of the window, and log off of the server. You are disconnected from the current server and any open remote desktop sessions, and you can now 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**.

Note The Windows key combination Ctrl+Alt+Del is not supported in remote desktops. Instead, click the **Send Ctrl+Alt+Delete** button in the menu bar. Alternatively, you can press Ctrl+Alt+Insert.

Procedure

- Disconnect from a remote desktop without logging off.

Option	Action
From the remote desktop window	Perform one of the following actions: ■ Click the **Close** button in the corner of the remote desktop window. ■ Select **Options > Disconnect** from the menu bar in the remote desktop window.
From the desktop and application selector window	In the upper-left corner of the desktop and application selector window, click the **Disconnect from this server** icon and click **OK** in the warning dialog box. If you are entitled to multiple remote desktops or published applications on the server, the desktop and application selector window is open.

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

- 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 **Options > Disconnect and Log Off**. If you use this procedure, files that are open on the remote desktop are closed without being saved first.

- Disconnect from a published application.

Option	Action
Disconnect from the published application but not the server	Quit the published application in the usual manner, for example, click the **Close** button in the corner of the application window.
Disconnect from the published application and the server	In the upper-left corner of the application selector window, click the **Disconnect from this server** icon and click **OK** in the warning dialog box.
Close the application selector window, but leave the published application running	Click the **Close** button. The application selector window closes.

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

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

  a Start Horizon Client, connect to the server that provides access to the remote desktop, and supply authentication credentials.

  b Right-click the remote desktop icon and select **Logoff**.

Disconnecting from a Server

After you have finished using a remote desktop or published application, you can disconnect from the server.

To disconnect from a server, click the **Disconnect from this server** icon in the upper-left corner of the Horizon Client window, or press Alt+D.

Working in a Remote Desktop or Published Application 5

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

This chapter includes the following topics:

Feature Support Matrix for Windows Clients

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

Table 5-1. 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 Desktop or Windows Server 2016 Desktop
USB redirection	Limited	Limited	X	X	X	X
Client drive redirection			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			X	X	X	X
VMware Blast display protocol			X	X	X	X
RDP display protocol	Limited	Limited	X	X	X	X
PCoIP display protocol	Limited	Limited	X	X	X	X
Persona Management	Limited	Limited	X	X		
Wyse MMR	Limited	Limited				
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

Windows 10 remote desktops require View Agent 6.2 or later, or Horizon Agent 7.0 or later. Windows Server 2012 R2 remote desktops require View Agent 6.1 or later, or Horizon Agent 7.0 or later.

Important View Agent 6.1 and later releases do not support Windows XP and Windows Vista remote desktops. View Agent 6.0.2 is the last View release that supports these guest operating systems. Customers that 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 remote desktops with Connection Server 6.1.

For information about which editions of each client operating system are supported, see System Requirements for Windows Client Systems.

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 5-2. 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 RDS Host	Windows Server 2016 RDS Host
RSA SecurID or RADIUS	X	X	Horizon Agent 7.0.2 and later
Smart card	View Agent 6.1 and later	View Agent 6.1 and later	Horizon Agent 7.0.2 and later
Single sign-on	X	X	Horizon Agent 7.0.2 and later
RDP display protocol	X	X	Horizon Agent 7.0.2 and later
PCoIP display protocol	X	X	Horizon Agent 7.0.2 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
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
Windows Media MMR	View Agent 6.1.1 and later	View Agent 6.1.1 and later	Horizon Agent 7.0.2 and later
USB redirection		View Agent 6.1 and later	Horizon Agent 7.0.2 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
Virtual printing	View Agent 6.0.1 and later (virtual machine only)	View Agent 6.0.1 and later (virtual machine only)	Horizon Agent 7.0.2 and later (virtual machine only)
Scanner redirection	View Agent 6.0.2 and later	View Agent 6.0.2 and later	Horizon Agent 7.0.2 and later
Location-based printing	View Agent 6.0.1 and later (virtual machine only)	View Agent 6.0.1 and later (virtual machine only)	Horizon Agent 7.0.2 and later (virtual machine only)

Table 5-2. 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 RDS Host	Windows Server 2016 RDS Host
Multiple monitors	X	X	Horizon Agent 7.0.2 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

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-based clients have the following restrictions.

Table 5-3. Requirements for Specific Features

Feature	Requirements
Windows Media MMR	Requires Horizon 7 Agent 6.0.2 or later. To use the Windows Media MMR feature with published desktops, you must have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later. If you use the VMware Blast display protocol, you must have Horizon Agent 7.0 or later.
Serial port redirection	Requires Horizon 7 Agent 6.1.1 or later. For Windows 10, requires View Agent 6.2 or later, or Horizon Agent 7.0 or later. If you use the VMware Blast display protocol, you must have Horizon Agent 7.0 or later.
Virtual printing and location-based printing for Windows Server 2008 R2 desktops, published desktops (on virtual machine RDS hosts), and published applications	Requires Horizon 6.0.1 or later. If you use the VMware Blast display protocol for this feature, you must have Horizon Agent 7.0 or later.
Scanner redirection	Requires Horizon 7 Agent 6.0.2 or later. Requires the PCoIP display protocol. For Windows 10, requires View Agent 6.2 or later, or Horizon Agent 7.0 or later. If you use the VMware Blast display protocol, you must have Horizon Agent 7.0 or later.
Client drive redirection	For single-user virtual machine desktops and published desktops, requires View Agent 6.1.1 or later, or Horizon Agent 7.0 or later. If you use the VMware Blast display protocol, you must have Horizon Agent 7.0 or later.

For descriptions of these features and their limitations, see the *Horizon 7 Architecture Planning* document.

Feature Support for Linux Desktops

If you have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, some Linux guest operating systems are supported.

For a list of supported Linux operating systems and information about supported features, see *Setting Up Horizon 6 for Linux Desktops* or *Setting Up Virtual Desktops in Horizon 7*.

Features Supported in Nested Mode

Sometimes nested mode is used for zero clients or thin clients. When an end user logs in to a zero client, Horizon Client starts automatically and connects to a remote desktop. The user starts published applications from this remote desktop session. The remote desktop can be a virtual desktop or a published desktop.

To provide published applications, Horizon Client must be installed in the remote desktop. This setup is called nested mode because Horizon Client connects to a remote desktop that also has Horizon Client installed.

The remote desktop where both Horizon Client and Horizon Agent are installed is called the first-level remote desktop. The machine where only Horizon Client is installed is called the host.

The following operating systems are supported when running Horizon Client in nested mode.

- Windows Server 2008 R2.
- Windows Server 2012 R2.
- Windows 7 Enterprise SP1.
- All Windows 10 operating system versions that Horizon Client supports. See System Requirements for Windows Client Systems.

The following features are supported when a user uses Horizon Client in nested mode.

- VMware Blast, PCoIP, and RDP display protocols
- Location-based printing
- Virtual printing
- Single sign-on (without smart card)
- Clipboard redirection
- URL Content Redirection
- Log in as current user
- USB redirection
- Open local files in published applications

The following features have certain limitations in nested mode.

- For the USB redirection feature to work in nested mode, the first-level remote desktop must be a virtual desktop. Published desktops are not supported.
- When opening local files in published applications in nested mode, you can open files from the first-level remote desktop in a second-level published application. You cannot open files on the host in a second-level published application.

Internationalization

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

Use a Local IME with Published Applications

If you use non-English keyboards and locales, you can use an IME (input method editor) that is installed in the local client system to send non-English characters to a published application.

You can use hot keys and icons in the notification area (system tray) of the local client system to switch to a different IME. You do not need to install an IME on the server that hosts the published application.

When this feature is enabled, the local IME is used. If an IME is installed and configured on the server that hosts the published application, that remote IME is ignored.

This feature is disabled by default. When you enable or disable this feature, you must disconnect from the server and log in again before the change takes effect.

Prerequisites

- Verify that one or more IMEs are installed in the client system.
- Verify that the input language on the local client system matches the language used in the IME.
- Verify that the remote desktop has View Agent 6.0.2, or Horizon Agent 7.0 or later, installed.

Procedure

1. In the Horizon Client desktop and application selector window, right-click a published application and select **Settings**.
2. In the Remote Applications pane, select the **Extend the local IME to hosted applications** check box and click **OK**.
3. Restart the session.

Option	Action
Log off of the server	Disconnect from the server, log in again, and reconnect to the published application. You can resume the published applications, which were disconnected but not closed, and any remote desktops.
Reset the applications	Right-click a published application icon, select **Settings**, and click **Reset**. When you use this option, any open remote desktops are not disconnected, but all published applications are closed and must be restarted.

   The setting takes effect only after you restart the session. The setting applies to all published applications on the server.

4. Use the local IME as you might use it with locally installed applications.

The language designation and an icon for the IME appear in the notification area (system tray) of the local client system. You can use hot keys to switch to a different language or IME. Key combinations that perform certain actions, such as CTRL+X for cutting text and Alt+Right Arrow for moving to a different tab, work correctly.

Note On Windows 7 and 8.x systems, you can specify hot keys for IMEs by using the **Text Services and Input Languages** dialog box, which is available at **Control Panel > Region and Language > Keyboards and Languages tab > Change Keyboards button > Text Services and Input Languages > Advanced Key Settings tab**).

Enabling Support for Onscreen Keyboards

You can configure the client system so that physical and onscreen keyboard, mouse, and handwriting pad events are sent to the remote desktop or published application, even when the mouse or onscreen keyboard is outside the Horizon Client window. The Horizon Client window must have focus.

This feature is especially useful if you are using an x86-based Windows tablet, such as a Windows Surface Pro. To use this feature, you must set the Windows Registry key `EnableSoftKeypad` to `true`. The location of this key depends on the type of system:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- For 64-bit Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\`

Resizing the Remote Desktop Window

If you drag a corner of the remote desktop window to resize it, a tooltip shows the screen resolution in the lower-right corner of the window.

If you are using the VMware Blast display protocol or the PCoIP display protocol, the tooltip changes to show different screen resolutions when you change the size of the remote desktop window. This information is useful if you must resize the remote desktop window to a specific resolution.

If a Horizon administrator has locked the guest size, or if you are using the RDP display protocol, you cannot change the resolution of the remote desktop window. In these cases, the resolution tooltip shows the initial resolution.

If you have multiple monitors, you can select the monitors on which to display a remote desktop window. For more information, see Select Specific Monitors in a Multiple-Monitor Setup. You can also configure the remote desktop window to open on a single monitor. For more information, see Use One Monitor in a Multiple-Monitor Setup.

Monitors and Screen Resolution

You can extend a remote desktop to multiple monitors. If you have a high-resolution monitor, you can see the remote desktop or published application in full resolution.

Supported Multiple Monitor Configurations

Horizon Client supports the following multiple monitor configurations.

- If you use two 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.
- Monitors can be placed side by side, stacked two by two, or vertically stacked only if you are using two monitors and the total height is less than 4096 pixels.
- To use the selective multiple-monitor feature, you must use the VMware Blast display protocol or the PCoIP display protocol. For more information, see Select Specific Monitors in a Multiple-Monitor Setup.
- To use the vSGA 3D rendering feature, you must use the VMware Blast display protocol or the PCoIP display protocol. You can use up to two monitors, with a resolution of up to 1920 X 1200. For a resolution of 4K (3840 X 2160), only one monitor is supported.
- For vGPU or other GPU passthrough modes, the vendor hardware and drivers determine the number of monitors and maximum resolution. For more information, see the *NVIDIA GRID Virtual GPU User Guide*, or go to the vendor website.
- If you use instant clone desktop pools in Horizon 7 version 7.1 or earlier, the maximum number of monitors that you can use to display a remote desktop is two, with a resolution of up to 2560 X 1600.
- 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	8, 8.x, 10	4

The remote desktop must have View Agent 6.2 or later, or Horizon Agent 7.0 or later, installed. 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. In this scenario, you can set the client machine's DPI to the proper setting and enable the DPI Synchronization feature to redirect the client machine's DPI setting to the remote desktop.

- If you use Microsoft RDP 7, the maximum number of monitors that you can use to display a remote desktop is 16.
- If you use Microsoft RDP display protocol, you must have Microsoft Remote Desktop Connection (RDC) 6.0 or later installed in the remote desktop.

Select Specific Monitors in a Multiple-Monitor Setup

With the selective multiple-monitor feature, you can select the monitors on which to display a remote desktop window. For example, if you have three monitors, you can specify that the remote desktop window appears on only two of those monitors. This feature is not supported for published applications.

You can select up to four adjacent monitors. The monitors can be side by side, stacked two by two, or stacked vertically. A maximum of two monitors can be stacked vertically.

Procedure

1. Start Horizon Client and log in to a server.
2. In the desktop and application selector window, right-click the remote desktop and select **Settings**.
3. From the **Connect Via** drop-down menu, select **PCoIP** or **VMware Blast**.

   The **Connect Via** drop-down menu appears only if a Horizon administrator has enabled it. To use VMware Blast, Horizon Agent 7.0 or later must be installed.
4. From the **Display** drop-down menu, select **All Monitors**.

   Thumbnails of the monitors that are currently connected to the client system appear under Display settings. The display topology matches the display settings on the client system.
5. To select or deselect a monitor on which to display the remote desktop window, click a thumbnail.

   When you select a monitor, its thumbnail changes color. If you violate a display selection rule, a warning message appears.
6. To save your changes, click **Apply**.
7. To close the dialog box, click **OK**.

8 Connect to the remote desktop.

Your changes are applied immediately when you connect to the remote desktop. Horizon Client saves display settings in a preferences file for the remote desktop after you exit from Horizon Client.

Use One Monitor in a Multiple-Monitor Setup

If you have multiple monitors but want a remote desktop window to appear on only one monitor, you can configure the remote desktop window to open on a single monitor. This feature is not supported for published applications.

Procedure

1 Start Horizon Client and log in to a server.

2 In the desktop and application selector window, right-click the remote desktop and select **Settings**.

3 From the **Connect Via** drop-down menu, select **PCoIP** or **VMware Blast**.

The **Connect Via** drop-down menu appears only if a Horizon administrator has enabled it. To use VMware Blast, Horizon Agent 7.0 or later must be installed.

4 From the **Display** drop-down menu, select **Window - Large**, **Window - Small**, or **Custom**.

Window - Large sets the window size to 1904 x 978 pixels. **Window - Small** sets the window size to 640 x 480 pixels. If you select **Custom**, you can select a specific window size.

5 To save your changes, click **Apply**.

6 To close the dialog box, click **OK**.

By default, the remote desktop window opens on the primary monitor. You can drag the remote desktop window to a non-primary monitor, and the next time you open the remote desktop, the remote desktop window appears on that same monitor. The window opens, is centered in the monitor, and uses the window size that you selected for the display mode, not a size that you might have created by dragging the window to resize it.

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. With the Display Scaling feature, remote desktops and published applications support the client machine's scaling setting and appear normal-sized rather than very small.

Horizon Client saves the display scaling setting for each remote desktop separately. For published applications, the display scaling setting applies to all published applications that are available to the currently logged-in user. The display scaling setting appears, even if the DPI setting is 100 percent on the client system.

You can hide the display scaling setting by enabling the Horizon Client **Locked Guest Size** group policy setting. Enabling the **Locked Guest Size** group policy setting does not disable the DPI Synchronization feature. To disable the DPI Synchronization feature, a Horizon administrator must disable the **DPI Synchronization** group policy setting. For more information, see Using DPI Synchronization.

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 primary monitor.

This procedure describes how to enable the Display Scaling feature before you connect to a remote desktop or application. You can enable the Display Scaling feature after you connect to a remote desktop by selecting **Options > Allow Display Scaling** from the Horizon Client menu bar.

Procedure

1. Start Horizon Client and connect to a server.
2. In the desktop and application selector window, right-click the remote desktop or published application and select **Settings**.
3. Select the **Allow display scaling** check box.
4. To save your changes, click **Apply**.
5. To close the dialog box, click **OK**.

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. When you start a new remote session, Horizon Agent sets the DPI value in the remote session to match the DPI value of the client system.

The DPI Synchronization feature cannot change the DPI setting for active remote sessions. If you reconnect to an existing remote session, the Display Scaling feature scales the remote desktop or published application appropriately.

The DPI Synchronization feature is enabled by default. A Horizon administrator can disable the DPI Synchronization feature by disabling the **DPI Synchronization** agent group policy setting. You must log out and log in again to make the configuration change take effect. For information about the **DPI Synchronization** group policy setting, see the *Configuring Remote Desktop Features in Horizon 7* document.

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.

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

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

- Windows Server 2012 R2
- Windows Server 2016

The DPI Synchronization feature requires Horizon Agent 7.0.2 or later and Horizon Client 4.2 or later.

Note The DPI Synchronization feature is not available if you use Horizon Client 4.2 with Horizon Agent 7.0 or 7.0.1, or Horizon Client 4.0 or 4.1 with Horizon Agent 7.0.2 or later. Only the Display Scaling feature is available in these scenarios.

Following are tips for using the DPI Synchronization feature.

- If you change the DPI setting on the client system, you must log out and log in again to make Horizon Client aware of the new DPI setting on the client system. This requirement applies even if the client system is running Windows 10.
- 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 must 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.
- Although Windows 10 and Windows 8.x systems support different DPI settings on different monitors, the DPI Synchronization feature uses only the DPI value that is set on the client system's primary monitor. All monitors in the remote desktop also use the same DPI setting as the client system's primary monitor. Horizon Client does not support different DPI settings in different monitors.
- 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.
- When you connect a laptop that supports different DPI settings on different monitors to an external monitor, and you set the external monitor to be the primary monitor, Windows changes the primary monitor and primary monitor DPI setting every time you detach or reattach the external monitor. In this situation, you must log out and log back in to the client system to make Horizon Client aware of the primary monitor change, and you must log out and log back in to the remote desktop or published application to make the DPI settings match between the client system and remote desktop or published application.
- For Windows 10 client systems, right-click on the desktop, select **Display Settings > Advanced display settings > Advanced sizing of text and other items**, click the **set a custom scaling level** link, and then log out and log in again to make the new DPI setting take effect.

Change the Display Mode for a Remote Desktop

You can change the display mode, such as from **All Monitors** mode to **Fullscreen** mode, before or after you connect to a remote desktop. This feature is not supported for published applications.

Procedure

1 Start Horizon Client and log in to a server.

2 Connect to the remote desktop, or right-click the remote desktop in the desktop and application selector window and select **Settings**.

3 From the **Display** drop-down menu, select the display mode.

Option	Description
All Monitors	Displays the remote desktop window on multiple monitors. The remote desktop window appears on all monitors by default.
Fullscreen	Makes the remote desktop window fill the screen.
Window - Large	Sets the remote desktop window size to 1904 x 978 pixels.
Window - Small	Sets the remote desktop window size to 640 x 480 pixels.
Custom	Displays a slider that you can use to configure a custom remote desktop window size.

4 To save your changes, click **Apply**.

5 To close the dialog box, click **OK**.

If you are connected to the remote desktop, your changes are applied immediately. If you are not connected to the remote desktop, your changes are applied when you connect to it. Horizon Client saves display settings in a preferences file for the remote desktop after you exit from Horizon Client.

If you use **All Monitors** mode and you click the **Minimize** button, if you then maximize the window, the window goes back to **All Monitors** mode. Similarly, if you use **Fullscreen** mode and minimize the window, if you then maximize the window, the window goes back to **Fullscreen** mode on one monitor.

Note If Horizon Client uses all monitors, and you maximize a published application window, the window expands to the full screen of only the monitor that contains it.

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 use these 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.

This procedure describes how to use Horizon Client to configure autoconnection of USB devices to a remote desktop or published application. You can also configure autoconnection by using the Horizon Client command-line interface, or by configuring a group policy.

For information about the command-line interface, see Running Horizon Client from the Command Line. For information about configuring group policies, see the *Configuring Remote Desktop Features in Horizon 7* document.

Prerequisites

- To use USB devices with a remote desktop or published application, a Horizon administrator must enable the USB redirection 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 USB Settings for Client GPOs.

- The USB Redirection component must be installed in Horizon Client. If you did not include this component in the installation, uninstall Horizon Client and run the installer again to include the USB Redirection component.

  For installation instructions, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

- Become familiar with USB Redirection Limitations.

Procedure

- Manually connect the USB device to a remote desktop.
  a Connect the USB device to the local client system.
  b From the VMware Horizon Client menu bar in the remote desktop, 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 Connect the USB device to the local client system.
  b Start Horizon Client and connect to the published application.

c Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window and click **USB Devices**.

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

Horizon Client connects the USB device to the published application that you selected. The USB device is also available to other applications in the same farm as the application that you selected.

e (Optional) To configure Horizon Client to connect the USB device automatically to the published application when the application is started, select the **Auto-connect at startup** check box.

f (Optional) To configure Horizon Client to connect the USB device automatically to the published application when you plug the device into the local system, select the **Auto-connect when inserted** check box.

The published application must be activated and in the foreground for this behavior to take effect.

g To close the Settings dialog box, click **OK**.

h When you are finished using the published application, open the Settings dialog box again, select **USB Devices**, and select **Disconnect**.

You must release the USB device so that you can access it from your local system.

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

  Use the autoconnect feature if you plan to connect devices that use MTP drivers, such as Android-based Samsung smart phones and tablets.

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

  b From the VMware Horizon Client menu bar in the remote desktop, select **Connect USB Device > Automatically Connect when Inserted**.

  c 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.

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

  a From the VMware Horizon Client menu bar in the remote desktop, select **Connect USB Device > Automatically Connect at Startup**.

  b Plug in the USB device and restart Horizon Client.

  USB devices that are connected to the local client system when you start Horizon Client are redirected to the remote desktop.

The USB device appears in the remote desktop or published application. A USB device might take up to 20 seconds to appear in the remote desktop or published application. The first time you connect the device to a remote desktop you might be prompted to install drivers.

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 View Agent 6.0.2 or later or Horizon Agent 7.0 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.

- The published application auto-connects at startup and auto-connects when inserted features do not work with global application entitlements.

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.

Configure Clients to Reconnect When USB Devices Restart

If you do not configure Horizon Client to connect USB devices automatically to your remote desktop, you can still configure Horizon Client to reconnect to specific devices that occasionally restart. Otherwise, when a device restarts during an upgrade, the device connects to the local system rather than to the remote desktop.

If you plan to attach a USB device such as a smart phone or tablet, which is restarted automatically during operating system upgrades, you can set Horizon Client to reconnect that specific device to the remote desktop. To perform this task, you edit a configuration file on the client system.

If you use the **Automatically Connect When Inserted** option in Horizon Client, all devices that you plug in to the client system are redirected to the remote desktop. If you do not want all devices to be connected, use the following procedure to configure Horizon Client so that only certain USB devices are reconnected.

Prerequisites

Determine the hexadecimal format of the vendor ID (VID) and product ID (PID) of the device. For instructions see the VMware KB article at http://kb.vmware.com/kb/1011600.

Procedure

1 On the client system, open the `config.ini` file in a text editor.

Operating System	File Path
Windows 7, 8.x, or Windows 10	`C:\ProgramData\VMware\VMware USB Arbitration Service\config.ini`
Windows XP	`C:\Documents and Settings\All Users\Application Data\VMware\VMware USB Arbitration Service\config.ini`

2 Set the `slow-reconnect` property for the specific device or devices.

```
usb.quirks.device0 = "vid:pid slow-reconnect"
```

vid:*pid* represent the vendor ID and product ID, in hexadecimal format, for the device. For example, the following lines set this property for two USB devices:

```
usb.quirks.device0 = "0x0529:0x0001 slow-reconnect"
usb.quirks.device1 = "0x0601:0x0009 slow-reconnect"
```

Specify the `usb.quirks.device`*N* device properties in order, starting from 0. For example, if the line `usb.quirks.device0` is followed by `usb.quirks.device2` rather than `usb.quirks.device1`, only the first line is read.

When devices such as smart phones and tablets undergo a firmware or operating system upgrade, the upgrade succeeds because the device restarts and connects to the remote desktop that manages it.

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.

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 you use a USB webcam, do not connect it from the **Connect USB Device** menu in Horizon Client. Doing so routes the device through USB redirection and 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 Preferred Webcam or Microphone on a Windows Client System

With the Real-Time Audio-Video feature, if multiple webcams or microphones are connected to the local client system, only one of the devices is used in the remote desktop or published application. To specify which webcam or microphone is preferred, you can configure Real-Time Audio-Video settings in Horizon Client.

If it is available, the preferred webcam or microphone is used in the remote desktop or published application. If the preferred webcam or microphone is not available, another webcam or microphone is used.

With the Real-Time Audio-Video feature, video devices, 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.

Note If you are using a USB webcam or microphone, do not connect it from the **Connect USB Device** menu in Horizon Client. Doing so routes the device through USB redirection and the device cannot use the Real-Time Audio-Video feature.

Prerequisites

- Verify that a USB webcam or USB microphone, or other type of microphone, is installed and operational on the local client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for the remote desktop or published application.
- Connect to a server.

Procedure

1. Open the **Settings** dialog box and select **Real-Time Audio-Video** in the left pane.
   - Click the **Settings** (gear) icon in the upper right corner of the desktop and application selector window.
   - Right-click a remote desktop or published application shortcut and selecting **Settings**.

2 To select a preferred webcam, select a webcam from the **Preferred webcam** drop-down menu.

   The menu shows the available webcams on the client system.

3 To select a preferred microphone, select a microphone from the **Preferred microphone** drop-down menu.

   The menu shows the available microphones on the client system.

4 To save you changes, click **OK** or **Apply**.

The next time you start a remote desktop or published application, the preferred webcam or microphone that you selected is redirected to the remote 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 (IM), 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, 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 Linux remote desktop sessions or published application sessions.

Prerequisites

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

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 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. For information about using group policy settings to configure the Session Collaboration feature, see the *Configuring Remote Desktop Features in Horizon 7* 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 looks different depending on the Windows 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. 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.

   The following invitation methods are available by default. A Horizon administrator can disable the email and IM invitation methods.

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	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 and joins the session, the session collaboration feature notifies you and a red dot appears on the VMware Horizon Collaboration icon in the system tray.

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.

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, or double-click the VMware Horizon Collaboration icon on the desktop.

   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 collaboration 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. You can also end the collaborative session by clicking the VMware Horizon Session Collaboration icon on the desktop and clicking the **Stop** button.

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
- Microsoft Lync redirection
- File redirection and Keep in Dock functionality
- 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 Session 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**.

Copying and Pasting

By default, you can copy and paste from the local client system to a remote desktop or published application. You can also copy and paste from a remote desktop or published application to the client system, or between two remote desktops or published applications, if a Horizon administrator enables these features.

Supported file formats include text, images, and RTF (Rich Text Format).

For example, to copy text on the client system, select the text and press Ctrl+C. To paste the text into a remote desktop, press Ctrl+V in the remote desktop.

If you use the VMware Blast display protocol or the PCoIP display protocol, 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.

A Horizon administrator configures the ability to copy and paste by setting agent group policies. Depending on the Horizon server and agent version, a Horizon administrator might also be able to use group policies to restrict clipboard formats during copy and paste operations, or use Smart Policies to control the copy and paste behavior in remote desktops. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

If you are connected to a Horizon 7 version 7.0 or earlier server, the clipboard can accommodate 1 MB of data for copy and paste operations. If you are connected to a Horizon 7 version 7.0.1 or later server, 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 system. The effective clipboard memory size is the lesser of the server and client clipboard memory size values.

The copy and paste feature has the following limitations.

- You cannot copy and paste files between a remote desktop and the file system on the local client computer.
- If you are copying formatted text, some of the data is text and some of the data is formatting information. If you copy a large amount of formatted text or text and an image, when you attempt to paste the text and image, you might see some or all the plain text but no formatting or image. The reason is that the three types of data is sometimes stored separately. For example, depending on the type of document you are copying from, images might be stored as images or as RTF data.
- If the text and RTF data together use less than maximum clipboard size, the formatted text is pasted. Often the RTF data cannot be truncated, so that if the text and formatting use more than the maximum clipboard size amount, the RTF data is discarded, and plain text is pasted.
- If you are unable to paste all the formatted text and images you selected in one operation, you might need to copy and paste smaller amounts in each operation.

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, modify the Windows registry value `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize`. The value type is REG_DWORD. The value is specified in KB. If you specify 0 or do not specify a value, the default client clipboard memory size is 8192 KB (8 MB).

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.

Using Published Applications

Published applications look and feel like applications that are installed on the local client system.

When using published applications, follow these tips.

- You can minimize and maximize a published application through the published application. When a published application is minimized, it appears in the taskbar of the client system. You can also minimize and maximize the published application by clicking its icon in the taskbar.
- You can quit a published application through the published application or by right-clicking its icon in the taskbar.
- You can press Alt+Tab to switch between open published applications.
- If a published application creates a Windows System Tray item, that item also appears in the system tray on the client system. By default, the system tray icons appear only to show notifications. You can customize this behavior in the same way that you customize natively installed applications.

  Note If you open the Control Panel to customize the notification area icons, the names of the icons for published applications are listed as VMware Horizon Client - *application name*.

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.

Printing from a Remote Desktop or Published Application

You can print to a virtual printer or a USB printer that is attached to the local client computer from a remote desktop or published application. Virtual printing and USB printing work together without conflict.

For information about the types of remote desktops that support virtual printing, see Feature Support Matrix for Windows Clients.

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

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.

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 printer 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.

This procedure applies to Windows 7 or Windows 8.x remote desktops. The procedure is similar, but not exactly the same, for other types of Windows remote desktops.

Prerequisites

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

To use virtual printing, a Horizon administrator must enable the virtual printing feature for 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 more information, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

Procedure

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

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

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

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

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

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

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

6 Click **OK**.

7 To use custom paper forms, define the forms on the client system.

   a Go to **Control Panel > Hardware and Sound > Devices and Printers**.

   b Select the printer and click **Print Server Properties** at the top of the screen.

   c On the **Forms** tab, specify the settings and click **Save Form**.

   This form is now available in the remote desktop.

Using USB Printers

A USB printer is a printer that is attached to a USB port on the local client system. To send print jobs to a USB printer, you can use the USB redirection feature or the virtual printing feature. Depending on network conditions, USB printing can sometimes be faster than virtual printing.

Virtual printers and redirected USB printers can work together without conflict.

- You can use the USB redirection feature to attach a USB printer to a virtual USB port in the remote desktop, but only if the required drivers are also installed on the remote desktop.

  If you use the USB redirection feature, the printer is no longer logically attached to the physical USB port on the client, and it does not appear in the list of local printers on the local client machine. You can print to the USB printer from the remote desktop, but you cannot print to the USB printer from the local client machine. In the remote desktop, redirected USB printers appear as *<printer_name>*.

  For information about how to connect a USB printer, see Use USB Redirection to Connect USB Devices.

- On some client systems, you can alternatively use the virtual printing feature to send print jobs to a USB printer. If you use the virtual printing feature, you can print to the USB printer from both the remote desktop and the local client system, and you do not need to install printer drivers in the remote desktop.

Control Adobe Flash Display

A Horizon administrator can set Adobe Flash content to display in a remote desktop at a level designed to conserve computing resources. Sometimes these settings can result in low playback quality. By moving the mouse pointer into the Adobe Flash content, you can override the Adobe Flash settings that the Horizon administrator specifies.

Adobe Flash display control is available for Internet Explorer sessions only on Windows, and only for Adobe Flash versions 9 and 10. To control Adobe Flash display quality, Adobe Flash must not be running in full screen mode.

Procedure

1. From Internet Explorer in the remote desktop, browse to the relevant Adobe Flash content and start it if necessary.

   Depending on how the Horizon administrator configured Adobe Flash settings, you might notice dropped frames or low playback quality.
2. Move the mouse pointer into the Adobe Flash content while it is playing.

   If the pointer remains in the Adobe Flash content, display quality is improved.
3. To retain the improvement in quality, double-click inside the Adobe Flash content.

Clicking URL Links That Open Outside of Horizon Client

A Horizon administrator can configure URL links that you click inside a remote desktop or published application to open in the default browser on the local client system. The URL link might be to a Web page, a phone number, an email address, or another type of link. This feature is called URL Content Redirection.

A Horizon administrator can also configure URL links that you click inside a browser or application on the local client system to open in a remote desktop or published application. If Horizon Client is not already open you click the URL link, it starts and prompts you to log in.

A Horizon administrator might set up the URL Content Redirection feature for security purposes. For example, if you are at work and click a link that points to a URL outside your company network, the link might be more safely opened in a published application. An administrator can configure which published application opens the link.

Using URL Content Redirection with Chrome

The first time a URL is redirected from the Chrome browser on the client, you are prompted to open the URL in Horizon Client. If you select the **Remember my choice for URL:VMware Hori...lient Protocol links** check box (recommended) and then click **Open URL:VMware Hori...lient Protocol**, this prompt does not appear again.

Enable the Relative Mouse Feature for a Remote Desktop

If you use the VMware Blast display protocol or the PCoIP display protocol when using CAD or 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.

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 **Options > Enable Relative Mouse** from the Horizon Client menu bar.

   The option is a toggle. To disable the relative mouse feature, select **Options > 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 Scanners

With the scanner redirection feature, you can scan information into remote desktops and published applications with scanners that are connected to the local client system. This feature redirects scanning data with a significantly lower bandwidth than can be achieved by using USB redirection.

Scanner redirection supports standard scanning devices that are compatible with the TWAIN and WIA (Windows Image Acquisition) formats. Although you must have the 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 or published application.

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 or published application, 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 or published application.

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. On published applications, the system tray icon is redirected to the local client computer.

  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 control image compression, 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 TWAIN scanners display the 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 Serial Port Redirection

With serial port redirection, you can redirect locally connected serial (COM) 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 remote desktops.

If a Horizon administrator has configured the serial port redirection feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, serial port redirection works in the remote desktop without further configuration. For example, COM1 on the local client system is redirected as COM1 on the remote desktop. COM2 is redirected as COM2. If the COM port is already in use, it is mapped to avoid conflicts. For example, if COM1 and COM2 exist on the remote desktop, COM1 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 remote 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 remote desktop to connect, disconnect, or customize the mapped COM 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.

- In the context menu, the port items are listed as ***port* mapped to *port***, for example, **COM1 mapped to COM3**. The first port, which is COM1 in this example, is the physical port or the USB-to-serial adapter on the local client system. The second port, which is COM3 in this example, is the port used in the remote desktop.

- To select the **Port Properties** command, right-click a COM port.

  In the COM Properties dialog box, you can configure a port to connect automatically when a remote 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 remote desktop uses. For example, if the COM1 port on the client system is mapped to COM3 in the remote desktop, but the application you are using requires COM1, you can change the port number to COM1. If COM1 exists in the remote desktop, you might see **COM1 (Overlapped)**. You can still use this overlapped port. The remote desktop can receive serial data through the port from the server and also from the client system.

- Connect to a mapped COM port before you attempt to start an application that requires access to the port. For example, right-click a COM port and select **Connect** to use the port in the remote desktop. When you start the application, the application opens the serial port.

  When a redirected COM port is opened and in use on a remote desktop, you cannot access the port on the local computer. Conversely, when a COM port is in use on the local computer, you cannot access the port on the remote desktop.
- In the remote desktop, you can use the Windows Device Manager **Port Settings** tab to set the default Baud rate for a particular COM port. Use the same settings in the Windows Device Manager on the client system. The settings from this tab are used only if the application does not specify the port settings.
- Before you can disconnect the COM port, you must close the port in the application or close the application. You can then select the **Disconnect** command to disconnect and make the physical COM port available for use on the client computer.
- If you configure a serial port to connect automatically, start an application that opens the serial port, and then disconnect and reconnect the remote desktop session, the auto-connect feature does not work. You also cannot connect by using the serial port's system tray icon's menu option. In most cases, the application can no longer use the serial port. You must stop the application, disconnect the remote desktop session, and reconnect again to resolve the problem.

Keyboard Shortcuts

You can use keyboard shortcuts for menu commands and common actions.

Common Keyboard Shortcuts

These keyboard shortcuts work the same way in Horizon Client as they do in all applications.

Table 5-4. Common Keyboard Shortcuts

Action	Key or Key Combination
Click the highlighted button in a dialog box	Press Enter.
Open the context menu	Press Shift+F10.
Click the **Cancel** button in a dialog box	Press ESC.
Navigate between items in the server selection window or the desktop and application selector window	Use an arrow key to move in the direction of the arrow. To move to the right, press Tab. To move to the left, press Shift +Tab.

Table 5-4. Common Keyboard Shortcuts (Continued)

Action	Key or Key Combination
Delete an item from the server selection window or the desktop and application selector window	Press Delete.
In Windows 8.x, navigate between the **Start** window and the remote desktop window	Press the Windows key.

Server Selection Window Key Combinations

You can use these key combinations in the server selection window in Horizon Client.

Table 5-5. Server Selection Key Combinations

Menu Command or Action	Key Combination
Open the online help in a browser window	Alt+O+H, Ctrl+H
New Server command	Alt+N
Open the **Support Information** window	Alt+O+S
Open the **About Horizon Client** window	Alt+O+V
Configure SSL command	Alt+O+O
Hide selector after launching an item command	Alt+O+I

Desktop and Application Selector Keyboard Shortcuts

You can use these keyboard shortcuts when you select remote desktops and published applications in Horizon Client.

Table 5-6. Desktop and Application Selector Keyboard Shortcuts

Menu Command or Action	Key Combination
Open the online help in a browser window	Alt+O+H, Ctrl+H
Open the **Options** menu	Alt+O
Open the **Support Information** window	Alt+O+S
Open the **About Horizon Client** window	Alt+O+V
Log off from the remote desktop	Shift+F10+O
Disconnect and log off from the server	Alt+D
Toggle between **Show Favorites** and **Show All**	Alt+F
While showing favorites, after typing the first few characters of the published application or remote desktop name, go to the next item that matches the search	F4
While showing favorites, go to the previous item that matches the search	Shift+F4
Mark as a favorite or remove a favorite designation	Shift+F10+F
Open the **Settings** menu	Alt+S, or Shift+F10+S

Table 5-6. Desktop and Application Selector Keyboard Shortcuts (Continued)

Menu Command or Action	Key Combination
Start the selected item	Enter, or Shift+F10+L
Pin a shortcut for the remote desktop or published application to the Start menu (for Windows 7 and earlier) or the Start window (for Windows 8.x and later) on the client system	Shift+F10+A
Open the **Display Settings** context menu for the selected remote desktop	Shift+F10+D
Use the PCoIP display protocol to connect to the selected remote desktop	Shift+F10+P
Use the RDP display protocol to connect to the selected remote desktop	Shift+F10+M
Create a remote desktop shortcut for the selected item	Shift+F10+C
Add the selected item to the Start menu or Start window	Shift+F10+A
Reset the selected remote desktop (if your administrator allows you to reset)	Shift+F10+R
Refresh the remote desktop and published application list	F5

Desktop Window Shortcuts

To use these shortcuts, you must press Ctrl+Alt or click the Horizon Client menu bar, rather than click inside the remote desktop, before you press the keys. These shortcuts work only when you use the VMware Blast display protocol or the PCoIP display protocol.

Table 5-7. Remote Desktop Window Shortcuts

Menu Command or Action	Key Combination
Release the mouse pointer so that it is no longer inside the remote desktop	Ctrl+Alt
Open **Options** menu	Alt+O
Open the **Support Information** window	Alt+O+M
Open the **About Horizon Client** window	Alt+O+V
Open the Share Folders Settings dialog box	Alt+O+F
Toggle **Enable display scaling**	Alt+O+N
Switch to Other Desktop command	Alt+O+S
Autoconnect to This Desktop command	Alt+O+A
Enable Relative Mouse command	Alt+O+E
Send Ctrl+Alt+Del command	Alt+O+C
Disconnect command	Alt+O+D
Disconnect and Log Off command	Alt+O+L
Connect USB Device command	Alt+U

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 Desktop** command.

Option	Action
From within the remote desktop	Select **Options > Restart Desktop** from the menu bar.
From the desktop selector window	Right-click the remote desktop icon and select **Restart Desktop**.

  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

1 To reset a remote desktop, use the **Reset Desktop** command.

Option	Action
From within the remote desktop	Select **Options > Reset Desktop** from the menu bar.
From the desktop and application selector window	Right-click the remote desktop icon and select **Reset Desktop**.

2 To reset published applications, use the **Reset** button in the desktop and application selector window.

   a Click the **Settings** button (gear icon) in the menu bar.

   b Select **Applications** in the left pane, click the **Reset** button in the right pane, and click **OK**.

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.

Repair Horizon Client for Windows

Sometimes you can resolve problems with Horizon Client by repairing Horizon Client.

Prerequisites

Verify that you can log in as an administrator on the client system.

Procedure

- To repair Horizon Client interactively, double-click the Horizon Client installer and click **Repair**, or run the Horizon Client installer with the `/repair` installation command from the command line.

  For example: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /repair`

- To repair Horizon Client silently, run the Horizon Client installer from the command line with the `/silent` and `/repair` installation commands.

  For example: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /repair`

Uninstall Horizon Client for Windows

If repairing Horizon Client does not solve the problem, you might need to uninstall and reinstall Horizon Client.

This procedures shows you how to uninstall Horizon Client when you have the Horizon Client installer. If you do not have the Horizon Client installer, you can uninstall Horizon Client in the same way that you uninstall other applications on your Windows system. For example, you can use the Windows operating system Add or Remove Programs feature to uninstall Horizon Client.

Prerequisites

Verify that you can log in as an administrator on the client system.

Procedure

- To uninstall Horizon Client interactively, double-click the Horizon Client installer and click **Remove**, or run the Horizon Client installer from the command line with the `/uninstall` installation command.

  For example: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /uninstall`

- To uninstall Horizon Client silently, run the Horizon Client installer from the command line with the `/silent` and `/uninstall` installation commands.

  For example: `VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /uninstall`

What to do next

Reinstall Horizon Client. See Chapter 2 Installing Horizon Client for Windows.

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.

What to Do If Horizon Client Quits Unexpectedly

Horizon Client quits even if you do not close it.

Problem

Horizon Client quits unexpectedly. Depending on the server configuration, you might see a message such as `There is no secure connection to the View Connection Server`. Sometimes a message does not appear.

Cause

This problem occurs when the connection to the server is lost.

Solution

- Restart Horizon Client. You can connect successfully when the server is running again. If you continue to have connection problems, contact your system administrator.

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 shortcut, or when you open a local file through file association, 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.