Using VMware Horizon Client for Windows

Horizon Client 4.5

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

EN-002510-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Using VMware Horizon Client for Windows

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

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

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 datacenter operations.

System Requirements and Setup for Windows-Based Clients

1

Systems running 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 Connection Server. Ensure that your Internet Explorer settings are accurate and that you can access the Connection Server URL through Internet Explorer.

This chapter includes the following topics:

System Requirements for Windows Clients

You can install Horizon Client for Windows on PCs or 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.

Model

All x86 or x86-64 Windows devices

Memory

At least 1GB of RAM

Operating systems

The following operating systems are supported:

OS	Version	Service Pack or Servicing Option	Supported Editions
Windows 10	32- or 64-bit	Current Branch (CB) version 1703 (Creators Update) Current Branch (CB) version 1607 (Anniversary Update) Current Branch for Business (CBB) version 1607 (Anniversary Update) Long-Term Servicing Branch (LTSB) version 1607 (Anniversary Update)	Home, Pro, Enterprise, and IoT Core
Windows 8 or 8.1	32- or 64-bit	None or Update 2	Pro, Enterprise, and Industry Embedded
Windows 7	32- 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," on page 82.

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

Latest maintenance release of View 6.x and later releases.

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

Note Clients can also connect to the Unified Access Gateway appliance, which is available with Horizon 6 version 6.2 and later releases.

Display protocols

VMware Blast, PCoIP, and RDP

Hardware Requirements for PCoIP and VMware Blast

- x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.

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

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

  As a rough guide, you can use the following calculations:

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

Hardware Requirements for RDP

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

Software Requirements for 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 Real-Time Audio-Video

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

Remote desktops

The desktops must have View Agent 5.2 or later, or Horizon Agent 7.0 or later, installed. For View Agent 5.2 desktops, the desktops must also have the corresponding Remote Experience Agent installed. For example, if View Agent 5.2 is installed, you must also install the Remote Experience Agent from View 5.2 Feature Pack 2. See the *View Feature Pack Installation and*

Administration document. If you have View Agent 6.0 or later, or Horizon Agent 7.0 or later, no feature pack is required. To use Real-Time Audio-Video with published desktops and applications, you must have Horizon Agent 7.0.2 or later.

Horizon Client computer or client access device

- Real-Time Audio-Video is supported on all operating systems that run Horizon Client for Windows. For details, see "System Requirements for Windows Clients," on page 10.
- The webcam and audio device drivers must be installed, and the webcam and audio device must be operable, on the client computer. To support Real-Time Audio-Video, you do not have to install the device drivers on the desktop operating system where the agent is installed.

Display protocols

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

System Requirements for Scanner Redirection

You can scan information into your remote desktops and applications with scanners that are connected to your local client system. To use this feature, your remote desktops, applications, and client computers must meet certain system requirements.

Remote desktops

The 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 on single-user virtual machines and on RDS hosts, and for information about configuring scanner redirection in remote desktops and applications, see "Configure Scanner Redirection" in *Configuring Remote Desktop Features in Horizon 7*.

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 this feature, 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

The 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, on the parent or template virtual machines. This setup option is deselected by default.

The following guest operating systems are supported on 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 configured as a desktop
- Windows Server 2012 R2 configured as a desktop
- Windows Server 2016 configured as a desktop

This feature is not currently supported for Windows Server RDS hosts.

Serial port device drivers do not have to be installed on the desktop operating system where the agent is installed.

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

Horizon Client computer or client access device

- Serial port redirection is supported on Windows 7, Windows 8.x client systems, and Windows 10.
- Any required serial port device drivers must be installed, and the serial port must be operable, on the client computer. You do not need to install the device drivers on the remote desktop operating system where the agent is installed.

Display protocols

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

VMware Horizon serial port redirection is not supported in RDP desktop sessions.

System Requirements for Multimedia Redirection (MMR)

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

Remote desktops

- Single-user desktops must have View Agent 6.0.2 or later, or Horizon Agent 7.0 or later, installed.
- Session-based 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 for the remote desktop or application, see the topics about Windows Media Multimedia Redirection in *Configuring Remote Desktop Features in Horizon 7*.
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 are supported on Windows Media Player are supported. 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

With Flash Redirection, if you use Internet Explorer 9, 10, or 11, Flash content is sent to the client system. The client system plays the media content, which reduces the load on the ESXi host.

Remote desktop	■ Horizon Agent 7.0 or later must be installed in a single-user (VDI) remote desktop, with the Flash Redirection option. The Flash Redirection 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 *Setting Up Virtual Desktops in Horizon 7* document. ■ Flash Redirection is supported on Windows 7, Windows 8, Windows 8.1, and Windows 10 single-user remote 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	■ 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 protocol for the remote session	VMware Blast, PCoIP

Requirements for Using Flash URL Redirection

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

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

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

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

- 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 Horizon documentation.

System Requirements for Microsoft Lync with Horizon Client

You 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. Customers 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 datacenter server to the client endpoint, and encodes all media into Lync-optimized audio and video codecs. 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

- Client operating system: Windows 7 SP1, Windows 8.x, or Windows 10.

- Virtual machine (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- or 64-bit Windows 7 SP1, Windows 8.x, Windows 10, or 64-bit Windows Server 2008 R2 SP1 For Microsoft RDS hosts: Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2
View Agent 6.0 or 6.1	32- or 64-bit Windows 7 SP1, Windows 8.x, or 64-bit Windows Server 2008 R2 SP1
View Agent 5.3	32- or 64-bit Windows 7 SP1

Client system software

- 32-bit version of Microsoft Lync VDI Plug-in

  Important The 64-bit version of Microsoft Office must not be installed on the client machine. The 32-bit Microsoft Lync VDI plugin that is required 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 5.3 or later, or Horizon Agent 7.0 or later
- Microsoft Lync 2013 Client

  With the View 5.3 or later agent, the Lync 2013 client bit-level is not required to match the bit-level of the virtual machine operating system.

- 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 5.3 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: 1.5GHz or faster CPU and a minimum of 2GB of RAM for the Microsoft Lync 2013 Plug-in

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

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 application (client-to-agent redirection), or from a remote desktop or application to the client machine (agent-to-client redirection).

For example, you can click a link in the native Microsoft Word application on the client and the link opens in the remote Internet Explorer application, or you 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.

The supported browsers in which you can type or click a URL and have that URL redirected are Internet Explorer 9, 10, and 11.

Note This feature does not work for links clicked from inside Windows 10 universal apps, including the Microsoft Edge Browser.

To use client-to-agent redirection, 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," on page 27.

To use agent-to-client redirection, a Horizon administrator must enable URL Content Redirection during Horizon Agent installation. For information, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* documents.

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

Requirements for Using Skype for Business with Horizon Client

You can run Skype for Business inside a virtual desktop without negatively affecting the virtual infrastructure and overloading the network. All media processing takes place on the Windows client machine, instead of in the virtual desktop, during Skype audio and video calls.

To use this feature, you must install the Virtualization Pack for Skype for Business feature on the client machine during Horizon Client for Windows installation. For information, see Chapter 2, "Installing Horizon Client for Windows," on page 25.

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

For complete requirements, see the *Configuring Remote Desktop Features in Horizon 7* document.

Smart Card Authentication Requirements

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

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

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

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

Horizon 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.

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.

To install certificates on a smart card, you 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 you are issuing certificates for.

Important When you enroll a smart card, you can choose 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 during smart card enrollment. Certificates with 512-bit keys are not supported.

The Microsoft TechNet Web site includes detailed information on planning and implementing smart card authentication for Windows systems.

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

- For information about configuring Connection Server to support smart card use, see the *View Administration* document.

  You must add all applicable Certificate Authority (CA) certificates for all trusted user certificates to a server truststore file on the Connection Server host or security server host. These certificates include root certificates and must include intermediate certificates if the user's smart card certificate was issued by an intermediate certificate authority.

- For information about tasks you might need to perform in Active Directory to implement smart card authentication, see the *View Administration* document.

Enabling the Username Hint Field 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** field during smart card sign-in.

To make the **Username hint** field appear on the Horizon Client login dialog box, you must enable the smart card user name hints feature for the Connection Server instance in Horizon Administrator. 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 *View Administration* document.

If your environment uses an 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.

Note Horizon Client still supports single-account smart card certificates when the smart card user name hints feature is enabled.

Device Authentication Requirements

You can set up certificate authentication for client devices.

This feature has the following requirements:

- Unified Access Gateway 2.6 or later.
- Horizon 7 version 7.0 or later.
- A certificate installed on the client device that Unified Access Gateway will accept.

Supported Desktop Operating Systems

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

For a list of the supported Windows guest operating systems, see the *View Installation* document.

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

Preparing Connection Server for Horizon Client

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

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

- If you plan to use Unified Access Gateway, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring Unified Access Gateway* document. Unified Access Gateway appliances fulfill the same role that was previously played by only security servers.
- If you are using a security server, verify that you are using the latest maintenance releases of Connection Server 5.3.x and Security Server 5.3.x or later releases. For more information, see the *View Installation* document.
- If you plan to use a secure tunnel connection for client devices and if the secure connection is configured with a DNS host name for Connection Server or a security server, verify that the client device can resolve this DNS name.

  To enable or disable the secure tunnel, in Horizon Administrator, go to the Edit Horizon Connection Server Settings dialog box and use the check box called **Use secure tunnel connection to desktop**.
- Verify that a desktop or application pool has been created and that the user account that you plan to use is entitled to access the pool. For information, see the *Setting Up Virtual Desktops in Horizon 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

  Important If end users have a high-resolution display and will use the High Resolution Mode client setting while viewing their remote desktops in full screen mode, you must allocate sufficient VRAM 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 you need, see the *View Architecture Planning* document.
- To use two-factor authentication with Horizon Client, such as RSA SecurID or RADIUS authentication, you must enable this feature on Connection Server. For more information, see the topics about two-factor authentication in the *View Administration* document.
- 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 in Horizon Administrator. These global settings are available in Horizon 7 version 7.1 and later. For information about configuring global settings, see the *View 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 will prevent users from being able to enter domain information in the user name text box and login will always fail. For more information, see the topics about two-factor authentication in the *View Administration* document.

- To provide users unauthenticated access to published applications in Horizon Client, you must enable this feature in Connection Server. For more information, see the topics about unauthenticated access in the *View Administration* document.

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

When 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 *View Administration* document.

Configure VMware Blast Options

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

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 cannot change the network condition option after you log in to a server. You can configure H.264 decoding before or after you log in to a server.

Prerequisites

This feature requires Horizon Agent 7.0 or later.

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**. You cannot change the network condition option after you log in to a server.

2 Configure the decoding and network condition options.

Option	Action
H.264	Configure this option, before or after connecting to Connection Server, to allow H.264 decoding in Horizon Client. When this option is selected (the default setting), Horizon Client uses H. 264 decoding if the agent supports H.264 software or hardware encoding. If the agent does not support H.264 software or hardware encoding, Horizon Client uses JPG/PNG decoding. Deselect this option to use JPG/PNG decoding.
Select your network condition for the best experience	You can only configure this option before connecting to Connection Server. Select one of the following network condition options: ■ **Excellent** - Horizon Client uses only TCP networking. This option is ideal for a LAN environment. ■ **Typical (default)** - Horizon Client works in mixed mode. In mixed mode, Horizon Client uses TCP networking when connecting to the server and uses Blast Extreme Adaptive Transport (BEAT) if the agent and Blast Security Gateway (if enabled) support BEAT connectivity. This option is the default setting. ■ **Poor** - Horizon Client uses only BEAT networking if the BEAT Tunnel Server is enabled on the server, otherwise it switches to mixed mode. **Note** In Horizon 7 version 7.1 and earlier, Connection Server and Security Server instances do not support the BEAT Tunnel Server. Unified Access Gateway 2.9 and later supports the BEAT Tunnel Server. Blast Security Gateway for Connection Server and Security Server instances do not support BEAT networking.

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

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

Using Internet Explorer Proxy Settings

Horizon Client automatically 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 fields. Fields containing sensitive information are made anonymous.

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

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

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

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 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
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

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 family	No	Examples include the following: ■ Security ■ Human Interface Device ■ Imaging
USB device usage count	No	(Number of times the device was shared)

Installing Horizon Client for Windows 2

You can obtain the Windows-based Horizon Client installer either from the VMware Web site 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.

Important Installing Horizon Client with FIPS-compliant cryptography is supported only for client systems that have Windows 7 SP1 or later operating systems.

For more information about FIPS support, which is available with Horizon 6 version 6.2 or later, see the *View 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.

Install Horizon Client for Windows

End users open Horizon Client to connect to their remote desktops and remote applications from a client system. 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," on page 27. To install the URL Content Redirection feature, you must run the installer from the command line.

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

Prerequisites

- Verify that the client system uses a supported operating system. See "System Requirements for Windows Clients," on page 10.
- 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 before you run the Horizon Client installer. See "Enabling FIPS Mode in the Windows Client Operating System," on page 25.
- If you plan to install the **USB Redirection** component, do the following:
  - 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," on page 43.
  - 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 product 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 installs the USB Redirection and Log in as current user features.
Custom installation	Click **Customize Installation** and select the features to install. You must select this option to specify a non-default installation location, use the IPv6 Internet protocol, configure a default Connection Server instance, configure the default login behavior, enable FIPS-compliant cryptography, install the 32-bit Core Remote Experience component on a 64-bit machine, or install the Virtualization Pack for Skype for Business feature. FIPS-compliant cryptography custom installation options are available in the installer only if FIPS mode is enabled on the client operating system. Follow these guidelines when selecting custom features: ■ Do not select the **IPv6** option unless all of the components in your Horizon environment use the IPv6 Internet protocol. Certain features are not available in an IPv6 environment. For more information, see the *View Installation* document. ■ 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. You cannot install the Virtualization Pack for Skype for Business feature if you select this feature.

Certain features require you to restart the client system.

The installer installs certain 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 application. See "Connect to a Remote Desktop or Application," on page 67.

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.

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	The 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	Specifies the IP (network protocol) version that Horizon Client components use for communication. The possible values are IPv4 and IPv6.	IPv4
VDM_FIPS_ENABLED	Specifies 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," on page 25.	0
VDM_SERVER	The 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 When 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 in a silent installation. 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 /silent 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

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

Property	Description	Default
INSTALL_SFB	Specifies whether to install the VMware Virtualization Pack for Skype for Business feature. 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).	0
URL_FILTERING_ENABLED	Specifies whether to install the URL Content Redirection feature. 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

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 Clients," on page 10.
- 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 before you run the Horizon Client installer. See "Enabling FIPS Mode in the Windows Client Operating System," on page 25.
- 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," on page 27.
- Become familiar with the Horizon Client installation properties. See "Installation Properties for Horizon Client," on page 28.
- 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," on page 28.
- 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 product 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 certain Windows services, including VMware Horizon Client (`horizon_client_service`) and VMware USB Arbitration Service (`VMUSBArbService`).

Example: 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," on page 31.

Start Horizon Client and verify that you can log in to the correct remote desktop or application. See "Connect to a Remote Desktop or Application," on page 67.

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," on page 27.

Procedure

1 Log in to the client machine.

2 Navigate to the `%PROGRAMFILES%\VMware\VMware Horizon View Client\` directory and verify that the `vmware-url-protocol-launch-helper.exe` and the `vmware-url-filtering-plugin.dll` files are installed in that directory.

3 Verify that the VMware Horizon View URL Filtering Plugin add-on is installed and enabled in Internet Explorer on the client machine.

Upgrade Horizon Client Online

You can upgrade Horizon Client online if the online upgrade feature is enabled. This feature is disabled by default.

You can enable this feature by modifying the group policy settings `Enable Horizon Client online update` and `URL for Horizon Client online update`. For more information, see "General Settings for Client GPOs," on page 52.

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 as an administrator.

2 In Horizon Client, click **Software Updates** from one of two screens.

Horizon Client Screen	Action
Before you connect to a Connection Server	Click **Options > Software Updates**.
After you connect to a Connection Server	Click **Help > Software Updates**

3 Click **Check for Updates**.

4 Click **Download and Install**.

Configuring Horizon Client for End Users

3

Configuring Horizon Client for end users can involve configuring URIs to start Horizon Client, configuring the certificate verification mode, setting advanced TLS/SSL options, and using group policy ADMX template files to configure custom settings.

This chapter includes the following topics:

Common Configuration Settings

Horizon Client provides several configuration mechanisms to simplify the login and 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
Connection 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
Desktop display name	URI, Group Policy, Command Line
Window size	URI, Group Policy, Command Line
Display protocol	URI, Command Line
Configuring certificate checking	Group Policy, Windows Registry
Configuring SSL protocols and cryptographic algorithms	Group Policy, Windows Registry

Using URIs to Configure Horizon Client

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

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

- Connection Server address
- Port number for Connection Server
- Active Directory user name
- RADIUS or RSA SecurID user name, if different from the Active Directory user name
- Domain name
- Desktop or 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.

Note You can use URIs to start Horizon Client only if the client software is already installed on client computers.

Syntax for Creating vmware-view URIs

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

URI Specification

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

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

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

authority-part Specifies the server address and, optionally, a user name, a non-default port number, or both. 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

Specifies the desktop or application. Use the desktop display name or application display name. This name is the one specified in Horizon Administrator when the desktop or application pool was created. If the display name has a space in it, use the **`%20`** encoding mechanism to represent the space.

query-part

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

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

Supported Queries

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

action

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

Value	Description
`browse`	Displays a list of available desktops and applications hosted on the specified server. You are not required to specify a desktop or application when using this action.
`start-session`	Opens the specified desktop or application. If no action query is provided and the desktop or application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified desktop or remote application. Unsaved data is lost. Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC.
`restart`	Shuts down and restarts the specified desktop. Restarting a remote desktop is the equivalent of 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 an application, the action is ignored or the end user sees the warning message "Invalid URI action."

args

Specifies command-line arguments to add to remote application launch. 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 remote 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 virtual desktop when you plug in the device. This query is implicitly set if you specify the `unattended` query. To use this query, you must set the `action` query to **start-session** or else not have an `action` query. Valid values are **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 desktop. This query is implicitly set if you specify the `unattended` query. To use this query, you must set the `action` query to **start-session** or else not have an `action` query. Valid values are **true** and **false**. An example of the syntax is **connectUSBOnStartup=true**.

desktopLayout

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

Table 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 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 remote application. You must use 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, the Windows user name is used. 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, however, 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 desktop and 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	Sets the account to use if the Unauthenticated Access feature is enabled. 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 create hypertext links or buttons with the `vmware-view` URI scheme and include these links in email or on a Web page. Your end users can click these links to, for example, open a particular remote desktop with the startup options you specify.

URI Syntax Examples

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

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

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

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

---

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

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for Connection Server. (The default port is 443.) Because a desktop identifier is provided, the desktop 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 box, the **User name** text box is populated with the name **fred**. The user must supply the domain name and password. After a successful login, the client connects to the desktop whose display name is displayed as **Finance Desktop**, and the user is logged in to the guest operating system. The connection uses the PCoIP display protocol.

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

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

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

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

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

Horizon Client 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 box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client displays a dialog box that prompts the user to confirm the reset operation for Primary Desktop.

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

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

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

Note This action is available only if a Horizon administrator has enabled the desktop restart feature for the 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://`

This URI starts Horizon Client if it is not running, or brings Horizon Client to the foreground if it is running.

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

Launches My Notepad++ on server 10.10.10.10 and passes the argument `My new file.txt` in the application launch 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`

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

NOTE Applications can differ in the way they use command line arguments. For example, if you pass the argument `a.txt b.txt` to Wordpad, Wordpad will open 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 is launched 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 a hypertext link that says, **Test Link**, and a button that says, **TestButton**.

```
<html>
<body>

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

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

</body>
</html>
```

Configuring Certificate Checking for End Users

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

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

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

For details about the types of verification checks performed, see "Setting the Certificate Checking Mode for Horizon Client," on page 40.

Use the Horizon Client Configuration ADMX template file (`vdm_client.admx`) to set the verification mode. All ADMX files that provide group policy settings are available in a `.zip` file named `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 GPO bundle from the VMware Horizon download site at http://www.vmware.com/go/downloadview. For information about using this template to control GPO settings, see "Using the Group Policy Template to Configure VMware Horizon Client for Windows," on page 42.

Note 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 SSL connection. For more information about this setting, see"Security Settings for Client GPOs," on page 45.

If you do not want to configure the certificate verification 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 `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 release, configuring this setting using the Windows registry might not be supported. A GPO setting must be used.

Setting the Certificate Checking Mode for Horizon Client

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

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

- 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.

Note 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 *View Installation* document.

When you use Horizon Client to log in to a desktop, if your administrator has allowed it, you can click **Configure SSL** to set the certificate checking mode. You have three choices:

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

  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 the certificate checking mode is set to **Warn**, you can still connect to a Connection Server instance that uses a self-signed certificate.

If an administrator later installs a security certificate from a trusted certificate authority, so that 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 configured your company's client systems to use a specific cipher via GPO, such as by configuring SSL Cipher Suite Order group policy settings, you must now use a Horizon Client group policy security setting included in the ADMX template file. See "Security Settings for Client GPOs," on page 45. You can alternatively use the `SSLCipherList` registry setting on the client. See "Using the Windows Registry to Configure Horizon Client," on page 65.

Configuring Advanced TLS/SSL Options

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

These security options are also used to encrypt the USB channel.

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

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 desktops. Be aware of the security risk if you choose to 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/SSL 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. Otherwise, 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 GPO, see the setting called "Configures SSL protocols and cryptographic algorithms," in "Security Settings for Client GPOs," on page 45. For information about using the SSLCipherList setting in the Windows Registry, see "Using the Windows Registry to Configure Horizon Client," on page 65.

Configure Application Reconnection Behavior

When you disconnect from a server, running applications might remain open. You can configure how running applications behave when you reconnect to the server.

A Horizon administrator can disable the application reconnection behavior settings in Horizon Client from the command line or by setting 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 Usage," on page 61, or the **Disconnected application session resumption behavior** group policy setting in "Scripting Definition Settings for Client GPOs," on page 43.

Procedure

1 In the desktop and application selector window of Horizon Client, right-click a remote application and select **Settings**.

2 In the Remote Applications pane that appears, select an application reconnection behavior setting.

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

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

The setting takes effect the next time you connect to the server.

Using the Group Policy Template to Configure VMware Horizon Client for Windows

VMware Horizon Client includes a group policy ADMX template file that you can use to configure VMware Horizon Client. You can optimize and secure remote desktop 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, as well as RDP connection settings. User Configuration policies override equivalent Computer Configuration policies.

Horizon applies policies at desktop startup and when users log in.

The Horizon Client Configuration ADMX template file (`vdm_client.admx`), and all ADMX files that provide group policy settings, are available in a `.zip` file named `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 the files from the VMware Horizon download site at http://www.vmware.com/go/downloadview. You must copy these files 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 policies for many of the same settings used when you run Horizon Client from the command line, including desktop size, name, and domain name, among others.

The following table describes the scripting definition settings in the VMware Horizon Client Configuration ADMX template file. The 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 are 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`	Automatically connects to the desktop if it is the only one entitled for the user. This setting spares the user from having to select the desktop from a list that contains only one desktop.
`Connect all USB devices to the desktop on launch`	Determines whether all of the available USB devices on the client system are connected to the desktop when the desktop is launched. **Note** This setting does not apply to published applications.
`Connect all USB devices to the desktop when they are plugged in`	Determines whether USB devices are connected to the desktop when they are plugged in to the client system. **Note** This setting does not apply to published applications.
`DesktopLayout`	Specifies the layout of the Horizon Client window that a user sees when logging 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 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.

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

Setting	Description
`Locked Guest Size`	Specifies the screen resolution of the remote desktop if the display is used on one monitor. That is, this setting does not work if you set the remote desktop display to All Monitors. After you enable the 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 and does not apply to RDP 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 2 monitors are supported at a resolution of up to 1920x1200. ■ If 3D is not enabled, up to 4 monitors are supported at a resolution of up to 2560x1600. In practice, this client-side setting will be 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 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, it is recommended that you 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`.
`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 policy. If the login fails because of incorrect login information, the user is not notified and the Horizon Client process is terminated.
`Disconnected application session resumption behavior`	Determines how running 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 application reconnection behavior on the Settings page in Horizon Client. When this setting is disabled, end users can configure application reconnection behavior in Horizon Client. This setting is disabled by default.

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

Setting	Description
`Enable Unauthenticated Access to the server`	Determines whether users are required to enter credentials to access their applications when using 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 may 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 applications. The **Log in anonymously using Unauthenticated Access** setting in Horizon Client is hidden and deselected. When this setting is not configured (the default), users can enable Unauthenticated Access in Horizon Client. 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. When this setting is not configured, users can choose an account. This setting is not configured by default.

Security Settings for Client GPOs

Security settings include options regarding security certificate, 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, the User Configuration setting overrides the equivalent Computer Configuration setting. These settings are 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 is performed by Horizon Client. You can select one of these modes: ■ `No Security`. Horizon does not perform certificate checking. ■ `Warn But Allow`. A self-signed certificate is provided by Horizon. In this case, it is acceptable if the certificate name does not match the Connection Server name provided by the user in Horizon Client. If any other certificate error condition occurs, Horizon displays an error dialog and prevents the user from connecting to Connection Server. `Warn But Allow` is the default value. ■ `Full Security`. If any type of certificate error occurs, the user cannot connect to Connection Server. Horizon 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 SSL configuration dialog box informs users that the administrator has locked the setting. When this setting is not configured or disabled, Horizon Client users can select a certificate verification mode. To allow a server to perform checking 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 SSL 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 release, configuring this setting using the Windows registry might not be supported. A GPO 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 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 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 lets users connect to recent Connection Server instances and remote desktops. If Horizon Client is shared, you might not want users to see the names of recent desktops. You can disable the jump list by disabling this setting. This setting is enabled by default. The equivalent Windows Registry value is `EnableJumplist`.
`Enable SSL encrypted framework channel`	X	X	Determines whether SSL is enabled for View 5.0 and earlier desktops. Before View 5.0, the data sent over port TCP 32111 to the desktop was not encrypted. ■ **Enable**: Enables SSL, but allows fallback to the previous unencrypted connection if the remote desktop does not have SSL support. For example, View 5.0 and earlier desktops do not have SSL support. **Enable** is the default setting. ■ **Disable**: Disables SSL. This setting is not recommended but might be useful for debugging or if the channel is not being tunneled and could potentially then be optimized by a WAN accelerator product. ■ **Enforce**: Enables SSL, and refuses to connect to desktops with no SSL support . The equivalent Windows Registry value is `EnableTicketSSLAuth`.

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

Setting	Computer	User	Description
`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 SSL connection. The cipher list consists of one or more cipher strings separated by colons. **Note** 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**. That means that TLS v1, TLS v1.1 and TLS v1.2 are enabled. (SSL v2.0 and v3.0 are removed.) Cipher suites use 128- or 256-bit AES, remove anonymous DH algorithms, and then sort the current cipher list in order of encryption algorithm key length. Reference link for the configuration: 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. The equivalent Windows Registry value is `EnableSmartCardSSO`.
`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 set group policies for options such as redirection of such things as 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 are 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 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
`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 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 cursor 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.

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

Setting	Description
`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.
`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 is managed by the USB Redirection component of the agent.
`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. If this setting is not configured, key combinations are applied locally.
`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 will not be able to 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

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 are 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 should be prevented from passing through client information in a nested session. When enabled, if Horizon Client is running inside of a Horizon session, it will send the actual physical client information instead of the VM device information. This setting applies to the following pieces of 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	(View 5.2 and later releases only) Enables the relative mouse when using the PCoIP display protocol. Relative mouse mode improves mouse behavior for certain graphics applications and games. If the remote desktop does not support relative mouse then this setting will not be 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.

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

Setting	Computer	User	Description
`Enable Horizon Client online update`	X		Enables the online upgrade feature. This setting is disabled by default.
`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.
`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 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 remote 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. If this setting is not configured, the default value is Disabled. This setting is not configured 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 remote 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.
`Put icon cache in user's Local profile folder`	X		Specifies whether Horizon Client places its icon cache files in the user's `Local` folder instead of in the previously used `Roaming` folder. When this setting is set to Enabled, Horizon Client places its icon cache files in the user's `Local` folder. When you first start Horizon Client, it moves any existing cache files from the `Roaming` folder to the `Local` folder and places new cache files in the `Local` folder. Enabling this policy can help improve the response time of remote applications when roaming profiles are used by avoiding syncing cache files. If this setting is not configured, the default value is Disabled. This setting is not configured 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," on page 72. If this setting is not configured, the default value is Disabled. This setting is not configured by default.
`Redirect smart card readers in Local Mode`	X		Local Mode is not supported in this release.
`Delay the start of replications when starting Horizon Client with Local Mode`	X		Local Mode is not supported in this release.
`Default Exit Behavior For Local Mode Desktops`		X	Local Mode is not supported in this release.

USB Settings for Client GPOs

You can define USB policy settings for both the agent and Horizon Client for Windows. On connection, Horizon Client downloads the USB policy settings from the agent and uses them in conjunction with the Horizon Client USB policy settings to decide which devices it will allow to be available for redirection from the host machine.

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

For a description of how Horizon applies the policies for splitting composite USB devices, see the topics about using policies to control USB redirection, in 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.

The following table describes each policy setting for filtering USB devices in the Horizon Client Configuration ADMX template file. The settings apply at computer level. Horizon Client preferentially reads the settings from the GPO at computer level, and otherwise from the registry at `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. For a description of how Horizon applies the policies for filtering USB devices, see the topics about configuring filter policy settings for USB redirection, in 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 is 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 is 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 boot time (also known as hid-bootable devices) to be redirected. The default value is undefined, which equates to **`true`**. This setting is 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 is 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
`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 is 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 is 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 is 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 is 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 is in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.
`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 is 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 should be 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 is 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 is 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
`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 is 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 is in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`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 is 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`	Includes devices with specified vendor and product IDs that can be redirected. The format of the setting is `vid-`*xxx1*`_pid-`*yyy2*`[;vid-`*xxx2*`_pid-`*yyy2*`]...` You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: **`vid-0561_pid-554c`** The default value is undefined. This setting is in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

PCoIP Client Session Variables ADMX Template Settings

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

The ADMX files are available in a bundled `.zip` file named `VMware-Horizon-Extras-Bundle-`*x.x.x*`-`*yyyyyyy*`.zip`, which you can download from the VMware download site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the bundled `.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 not configured or when it is disabled, PCoIP uses a default client image cache size of 250MB. 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 250MB.
`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 not configured or disabled, the default event log verbosity level is 2. 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. Checking 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 will be overridden if both AES-128-GCM encryption and AES-256-GCM encryption are disabled. If the `Configure SSL Connections` setting is disabled or not configured, both the Salsa20-256round12 and AES-128-GCM algorithms are available for negotiation by this endpoint. 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.
`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 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. The UDP port range value determines how many additional ports to try if the base port is not available. 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.

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

Setting	Description
`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, taking into consideration 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 4Mbit/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 or not configured on an endpoint, the endpoint imposes no bandwidth constraints. When this setting is configured, the setting is used as the endpoint's maximum bandwidth constraint in kilobits per second. The default value when this setting is not configured 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 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 supported by both sides). 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 transport session priority value is negotiated by the PCoIP agent and client. 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. When this setting is not configured, audio is enabled by default.

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

Setting	Description
`Configure the PCoIP session bandwidth floor`	Specifies a lower limit, in kilobits per second, for the bandwidth that is reserved by the PCoIP session. 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 or not configured, no minimum bandwidth is reserved. 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.
`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 is not affected by this setting. 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 SSL connections to satisfy Security Tools`	Specifies how SSL 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 or not configured, 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.
`Configure SSL protocols`	Configures the OpenSSL protocol to restrict the use of certain protocols before establishing an encrypted SSL 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 negotation rule is followed.
`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 or not configured, the default event log cleanup by time in days setting is 7. The log file cleanup is performed once at session startup. Any change to the setting is be applied until the next session.
`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 or not configured, the default event log cleanup by size in MB setting is 100.

Running Horizon Client from the Command Line

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

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

Horizon Client Command Usage

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 your system.

- On 32-bit systems, the path is `C:\Program Files\VMware\VMware Horizon View Client\`.
- On 64-bit systems, the path is `C:\Program Files (x86)\VMware\VMware Horizon View Client\`.

For your convenience, add this path to your *PATH* environment variable.

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 application as it would appear in the desktop and application selection window. This is the display name that was specified for the application pool in the pool creation wizard.
`-appProtocol` *protocol*	Specifies the remote application display protocol to use, if available. The display protocol can be Blast or PCoIP.
`-appSessionReconnectionBehavior` *argument*	Specifies the application reconnection behavior setting. ■ `always` implements **Reconnect automatically to open applications** ■ `never` implements **Do not ask to reconnect and do not automatically reconnect** ■ `ask` implements **Ask to reconnect to open applications** When you use this option, the application reconnection settings are disabled on the Settings page in Horizon Client.
`-args` *argument*	Specifies command-line arguments to add to remote application launch. 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 to the desktop that are currently connected to the host. This option is implicitly set if you specify the `-unattended` option. The default is `false`.
`-connectUSBOnInsert`	When set to `true`, connects a USB device to the foreground desktop when you plug in the device. This option is implicitly set if you specify the `-unattended` option. The default is `false`.

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

Option	Description
`–desktopLayout` *window_size*	Specifies how to display the window for the desktop: **`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 desktop as it would appear in the desktop and application selection window. This 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 desktop is run in kiosk mode. For kiosk mode, the connection is made to the first desktop in the list of entitled desktops.
`–desktopProtocol` *protocol*	Specifies the display protocol to use as it would appear in the desktop and application selection window. The display protocol can be Blast, PCoIP, or RDP.
`–domainName` *domain_name*	Specifies the NETBIOS domain that the end user uses to log in to Horizon Client. For example, you would 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," on page 64.
`–h`	Shows help options.
`–hideClientAfterLaunchSession`	When set to `true`, hides the remote desktop and application selector window and the **Show VMware Horizon Client** menu after launching a remote session. When set to `false`, shows the remote desktop and application selector window and the **Show VMware Horizon Client** menu after launching 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 can use the 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 Connection Server instance and ultimately to the remote desktop. The default is `false`.
`–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.
`–noVMwareAddins`	Prevents loading of VMware-specific virtual channels such virtual printing.

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

Option	Description
`–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. You do not need to specify this option for clients in kiosk mode if you generate the password automatically. For improved security, it is recommended that you 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 Connection Server instance.
`–shutdown`	Shuts down all desktops and applications and relevant UI components.
`–singleAutoConnect`	Specifies that if the user is entitled to only one remote desktop or application, after the user authenticates to the server, the desktop or application is automatically connected and the user is logged in. This setting spares the user from having to select the desktop or application from a list that contains only one item.
`–smartCardPIN` *PIN*	Specifies the PIN when an end user inserts a smart card to login.
`–usernameHint` *user_name*	Specifies the account name to use as the username hint.
`–standalone`	Supported for backwards compatibility purposes. This is the default behavior for this client. Specifying `–standalone` is not necessary. Launches a second instance of the Horizon Client that can connect to the same or a different Connection Server instance. For multiple desktop connections to the same server or to a different server, using the secure tunnel is supported. **Note** The second desktop connection might not have access to 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.
`–unattended`	Runs Horizon Client in a noninteractive mode that is suitable for clients in kiosk mode. You must also specify: ■ 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`

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

Option	Description
`–unauthenticatedAccessEnabled`	Specifies Unauthenticated Access behavior: ■ `true` enables Unauthenticated Access. The client may fall back to another authentication method if Unauthenticated Access is not available. The **Log in anonymously using Unauthenticated Access** setting is visible, disabled, and selected in Horizon Client. ■ `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.

`–useExisting`	Enables you to launch multiple remote desktops and applications from a single Horizon Client session.
	When you specify this option, Horizon Client determines whether a session with the same username, domain, and server URL already exists and, if it does, reuses that session instead of creating a new session.
	For example, in the following command, user-1 launches 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 launches the Paint application with the same username, 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. You do not need to specify this option for clients in kiosk mode if you generate the account name from the MAC address of the client device.

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 in 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 whose account name is based on its 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 the 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 release, the Windows registry settings described in this section might not be supported. GPO settings must be used.

Table 3-12 shows 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, whereas the `HKEY_LOCAL_MACHINE` settings, described in the next table, are computer-wide settings and pertain to all local users and all domain users in a Windows domain environment who have permission to log in to the computer.

Table 3-12. Horizon Client Registry Settings for Credentials

Registry Setting	Description
`Password`	Specifies the default password.
`UserName`	Specifies the default user name.

Table 3-13 shows the registry settings for Horizon Client that do not include login credentials. The location of these settings 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\`

Table 3-13. Horizon Client Registry Settings

Registry Setting	Description
`DomainName`	Specifies the default NETBIOS domain name. For example, you would use `mycompany` rather than `mycompany.com`.
`EnableShade`	Specifies 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**.
`ServerURL`	Specifies the default Connection Server instance by its URL, IP address, or FQDN.
`EnableSoftKeypad`	If set to **`true`** and a Horizon Client window has focus, then physical keyboard, onscreen keyboard, mouse, and handwriting pad events are sent to the remote desktop or remote application, even if the mouse or onscreen keyboard is outside of 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:

- 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`	Specifies the certificate checking mode. ■ **`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 SSL connection. The cipher list consists of one or more cipher strings separated by colons. **Note** 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 means that TLSv.1, TLSv1.1, and TLSv1.2 are enabled. (SSL v2.0 and v3.0 are removed.) Cipher suites use 128- or 256-bit AES, remove anonymous DH algorithms, and then sort the current cipher list in order of encryption algorithm key length. Reference link for the configuration: http://www.openssl.org/docs/apps/ciphers.html

Managing Remote Desktop and Application Connections

4

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

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

This chapter includes the following topics:

Connect to a Remote Desktop or Application

After logging in to a server, you can connect to the remote desktops and applications that you are authorized to use.

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

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

The **Log in as current user** feature is available even if Horizon Client is installed on a remote desktop.

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," on page 19.
- If you are outside the corporate network and are not using a security server to access the remote desktop or application, verify that your client device is set up to use a VPN connection and turn on that connection.

  IMPORTANT In most cases, use a security server rather than a VPN.

- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or application. 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.
- If your administrator has allowed it, configure the certificate checking mode for the SSL certificate presented by Connection Server. To determine which mode to use, see "Setting the Certificate Checking Mode for Horizon Client," on page 40.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Double-click the **VMware Horizon Client** desktop shortcut or click **Start > Programs > VMware Horizon Client**.
3. (Optional) To set the certificate checking mode, click the **Options** button in the menu bar and select **Configure SSL**.

   You can configure this setting only if your administrator has allowed it.
4. (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 if the **Log in as current user** feature is installed on your client system.
5. Double-click the **+ Add Server** button if no servers have yet been added, or click the **+ New Server** button in the menu bar and enter the name of Connection Server or a security server, and click **Connect**.

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

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

   NOTE After a successful connection is made, an icon for this server is saved to the Horizon Client home window. The next time you use Horizon Client to connect to this server, you can double-click the icon, or, if you use only this one server, you can right-click the icon for the server and select **Autoconnect to this Server** from the context menu.
6. If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Continue**.
7. Enter the credentials of a user who is entitled to use at least one desktop or application pool, select the domain, and click **Login**.

   If you enter the user name using the format **`username@domain`**, the name is treated as a user principal name (UPN) because of the @ sign, 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`***.

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

Option	Description
Display protocol	If your administrator has allowed it, you can use the **Connect Via** list to select the display protocol. VMware Blast requires Horizon Agent 7.0 or later.
Display layout	Use the **Display** list to select a window size or to use multiple monitors.

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

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

10 To connect to a remote desktop or application, either double-click its icon or right-click the icon and select **Launch** from the context menu.

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

After you are connected, the remote desktop or application window appears. If you are entitled to more than one desktop or application, the desktop and application selector window also remains open, so that you can connect to multiple items at the same time.

From the Sharing dialog box, you can allow or deny access to files on your local system. For more information, see "Share Access to Local Folders and Drives," on page 72.

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

- Determine whether Connection Server is configured not to use SSL. The client software requires SSL connections. Check whether the global setting in Horizon Administrator for the **Use SSL for client connections** check box is deselected. If so, you must either select the check box, so that SSL is used, or set up your environment so that clients can connect to an HTTPS enabled load balancer or other intermediate device that is configured to make an HTTP connection to Connection Server.
- Verify that the security certificate for Connection Server is working properly. If it is not, in Horizon Administrator, you might also see that the agent on desktops is unreachable. These symptoms indicate additional connection problems caused by certificate problems.
- Verify that the tags set on the Connection Server instance allow connections from this user. See the *View Administration* document.
- Verify that the user is entitled to access this desktop or 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 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 Connection Server instance, or if you want to configure other startup settings, use a command-line option to create a desktop shortcut. See "Running Horizon Client from the Command Line," on page 61.

Use Unauthenticated Access to Connect to Remote Applications

An administrator can use the Unauthenticated Access feature to create Unauthenticated Access users and entitle those users to remote applications on a Connection Server instance. Unauthenticated Access users can log in to the server anonymously to connect to their remote applications.

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. An 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," on page 19.
- Set up Unauthenticated Access users on the Connection Server instance. For information, see "Providing Unauthenticated Access for Published Applications" in the *View 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 remote application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.
- If your administrator has allowed it, configure the certificate checking mode for the SSL certificate presented by Connection Server. To determine which mode to use, see "Setting the Certificate Checking Mode for Horizon Client," on page 40.
- (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," on page 43.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Double-click the **VMware Horizon Client** desktop shortcut or click **Start > Programs > VMware Horizon Client**.
3. If instructed to do so by your administrator, click the **Options** button in the menu bar and select **Log in anonymously using Unauthenticated Access**.

   Depending on how your client system is configured, this setting might already be selected.
4. (Optional) To set the certificate checking mode, click the **Options** button in the menu bar and select **Configure SSL**.

   You can configure this setting only if your administrator has allowed it.
5. Connect to the server on which you have unauthenticated access to remote 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 Connection Server always use SSL. The default port for SSL connections is 443. If Connection Server is not configured to use the default port, use the format shown in this example: **`view.company.com:1443`**.

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

6 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 already selected.

7 (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**.

8 Click **Login** to log in to the server.

The application selection window appears.

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

Tips for Using the Desktop and Application Selector

For your convenience, you can reorganize or reduce the number of icons on the Horizon Client desktop and application selector screen.

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

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

  If more than one item matches the letters you typed, you can press F4 to go to the next item that matches. When you get to the last item, you can press F4 to go back to the first item that matches.

- Mark an icon as a favorite by right-clicking the icon and selecting **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.

- While in the Favorites view, select an icon and drag it to change the ordering of the icons. When you are not in the Favorites view, by default desktop icons are listed first, in alphabetical order, followed by application icons, also listed in alphabetical order. But you can drag and drop icons to reposition them while in the Favorites view.

  The ordering of icons is saved on the server you are using, either when you disconnect from the server or when you launch an application or desktop. If you do not manually disconnect from the server or launch an item, your changes will not be saved.

- Create a shortcut so that you can access the remote desktop or application from your own local desktop and avoid the selector window altogether. Right click the icon and select **Create Shortcut** from the context menu.

- Right click the remote desktop or application icon and select **Add to Start Menu** from the context menu so that you can access the remote desktop or application from your own local Start menu and avoid the selector window altogether.

NOTE If you are using a Windows 7 or later client system, after you have connected to a server, desktop, or application, you can open Horizon Client and right-click the Horizon Client icon in the Windows taskbar to select that recently used server, desktop, or application. 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

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

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

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

You can also turn on the ability to open local files with remote applications directly from the local file system. When you right-click a local file, the **Open with** menu also lists the available remote applications. You can also set files to be opened automatically with remote applications when you double-click the file. When you enable 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 one of the remote applications available from the server, you can right-click a `.docx` file on your local file system and open the file with the remote MS Word application. This feature requires Horizon 6.2 servers and agents.

An administrator 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 Table 3-7.

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

Prerequisites

To share folders and drives with a remote desktop or application, you must enable the client drive redirection feature. This task includes installing View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, and enabling the agent **Client Drive Redirection** option. It can also include setting policies to control client drive redirection behavior. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

Procedure

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

Option	Description
From the desktop and application selection window	Right-click a desktop or application icon, select **Settings**, and select **Sharing** in the left panel of the window that appears.
From the Sharing dialog box that appears when you connect to a desktop or application	Click the **Settings > Sharing** link in the dialog box.
From within a desktop OS	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 applications	Click the **Add** button, browse to and select the folder or drive to share, and click **OK**. **NOTE** You cannot share a folder on a USB device if the device is already connected to a remote desktop or application with the USB redirection feature. Also, do not turn on the USB redirection feature that automatically connects USB devices 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 will be connected using the USB redirection feature rather than 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.
Permit remote desktops and 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 applications	Select the **Allow access to removable storage** check box. The client drive redirection feature automatically shares all USB storage devices inserted in your client system and all FireWire and Thunderbolt-connected external drives. You do not need to select a specific device to share. **NOTE** USB storage devices already connected to a remote desktop or 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 applications.
Turn on the ability to open a local file with a remote 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 with a remote application. You can also change the properties of the file so that all files with that file extension are opened with the remote 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 remote application to open files of that type. Your administrator can disable this feature.
Do not show the Sharing dialog box when you connect to a remote desktop or application	Select the **Do not show dialog when connecting to a desktop or application** check box. If this check box is deselected, the Sharing dialog box appears the first time you connect to a desktop or application after you connect to a server. For example, if you log in to a server and connect to a desktop, you see the Sharing dialog box. If you then connect to another desktop or application, you do not see the dialog box again. To see the dialog box again, you must disconnect from the server and then log in again.

What to do next

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

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

Hide the VMware Horizon Client Window

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

You can also set a preference that always hides the VMware Horizon Client window after a remote desktop or application opens.

NOTE Administrators can use a group policy setting to configure whether the window is always hidden after a remote desktop or application opens.

For more information, see "General Settings for Client GPOs," on page 52.

Procedure

- To hide the VMware Horizon Client window after you open a remote desktop or application, click the **Close** button in the corner of the VMware Horizon Client window.
- To set a preference that always hides the VMware Horizon Client window after a remote desktop or 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 **Show 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 Desktop or Application

For security purposes, administrators set timeouts that log you off of a server after a certain number of hours and that lock a remote application after a certain number of minutes of inactivity.

With the View 6.0 remote applications feature, if you have not used a remote application for a certain amount of time, then 30 seconds before the application is automatically locked, you receive a warning prompt. If you do not respond, the application is locked. By default the timeout occurs after 15 minutes of inactivity, but your administrator can change the time period.

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

The server timeout period is typically set for a certain number of hours of inactivity. By default, if you have Horizon Client open and connected to a particular server for more than 10 hours, you will be required to log in again. This timeout applies regardless of whether you are connected to a remote application or a remote desktop.

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

Create a Desktop or Application Shortcut on Your Client Desktop or Start Menu

You can create a shortcut for a remote desktop or application. The shortcut appears on your client desktop, just like shortcuts for locally installed applications. You can also create a Start menu item that appears in the Programs list.

Procedure

1 Start Horizon Client and log in to the server.

2 In the desktop and application selection window, right-click an application or desktop and select **Create Shortcut** or **Add to Start Menu** from the context menu that appears.

Depending on the command you selected, a shortcut item is created on your client desktop or in the Start menu of your client system.

What to do next

You can rename, delete, or perform any action on this shortcut that you can perform on shortcuts for locally installed applications. When you use the shortcut, if you are not already logged in to the server, you are prompted to log in before the remote desktop or application window opens.

Switch Desktops or Applications

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

Procedure

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

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

Log Off or Disconnect

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

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

Note The Windows key combination Ctrl+Alt+Del is not supported in remote desktops. To use the equivalent of pressing Ctrl+Alt+Del, click the **Send Ctrl+Alt+Delete** button in the menu bar. Alternatively, in most cases, 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 desktop window. ■ Select **Options > Disconnect** from the menu bar in the desktop window.
From the desktop and application selector window	The desktop and application selector window is open if you are entitled to multiple desktops or applications on the server. In the upper-left corner of the desktop selector window, click the **Disconnect from this server** icon and click **Yes** in the warning box.

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

- Log off and disconnect from a remote desktop.

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

- Disconnect from a remote application.

Option	Action
Disconnect from the application but not the server	Quit the application in the usual manner, for example, click the **Close** button in the corner of the application window.
Disconnect from the application and the server	Perform one of the following actions: ■ In the upper-left corner of the application selector window, click the **Disconnect from this server** icon and click **Yes** in the warning box. ■ Right-click the Horizon Client icon in the system tray and select **Quit**.
Close the application selector window but leave the application running	Clicking the **Close** button only closes the application selector window.

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

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

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

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

Working in a Remote Desktop or Application 5

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

This chapter includes the following topics:

Feature Support Matrix for Windows Clients

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

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

Table 5-1. Remote Desktop Features Supported on Windows-Based Horizon Client Systems

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 desktops require View Agent 6.2 or later, or Horizon Agent 7.0 or later. Windows Server 2012 R2 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 desktops. View Agent 6.0.2 is the last View release that supports these guest operating systems. Customers who have an extended support agreement with Microsoft for Windows XP and Vista, and an extended support agreement with VMware for these guest operating systems, can deploy the View Agent 6.0.2 version of their Windows XP and Vista desktops with View Connection Server 6.1.

For information about which editions of each client operating system are supported, or which service packs, see "System Requirements for Windows Clients," on page 10.

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 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 (for desktop clients)	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 (USB storage devices only)		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 (for desktop clients)	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)
Multiple monitors (for desktop clients)	X	X	Horizon Agent 7.0.2 and later
Unity Touch (for mobile and Chrome OS clients)	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, or which service packs, see the *View 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 View Agent 6.0.2 or later. To use the Windows Media MMR feature with RDS 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 View 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, RDS desktops (on virtual machine RDS hosts), and remote applications	Requires Horizon 6.0.1 with View 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 View 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 on RDS hosts, 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.

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

You can use remote applications only if you are connected to Connection Server 6.0 or later. For information about which operating systems are supported for the RDS host, which provides published applications and published desktops, see the *View Installation* document.

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

Feature Support for Linux Desktops

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

Nested mode is sometimes used for zero clients or thin clients, where, when the end user logs in to the zero client, Horizon Client automatically starts and logs the user in to a remote desktop. From this remote desktop, the user launches hosted applications.

In this setup, the remote desktop is either a single-user virtual machine desktop or a desktop provided by an RDS host. In either case, to provide hosted applications, the Horizon Client software must be installed in the remote desktop. This setup is called nested mode because the client connects to a desktop that also has the client installed.

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
- Windows 10 Enterprise, version 1607

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

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 Remote Applications

When using non-English keyboards and locales, you can use an IME (input method editor) installed in your local system to send non-English characters to a remote hosted application.

You can also use hot keys and icons in the notification area (system tray) of your local system to switch to a different IME. No IME is required to be installed in the remote RDS host.

When this feature is turned on, the local IME is used. If an IME is installed and configured on the RDS host where the remote application is installed, that remote IME is ignored.

By default the feature is turned off. Whenever you change the setting to turn the feature on or off, you must disconnect from the server and log in again before the change can take effect.

Prerequisites

- Verify that one or more IMEs are installed in the client system.
- Make sure that the input language on your local client system matches the language used in your IME.

  The input language on the RDS host is not applicable.
- Verify that the remote desktop has View Agent 6.0.2, or Horizon Agent 7.0 or later, installed.

Procedure

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

3 Restart the session by using one of the following options:

Option	Description
Log off of the server	Disconnect from the server and then log in to the server again and connect to the application again. You can resume your applications, which were disconnected but not closed, as were any remote desktops.
Reset the applications	Right-click a remote application icon, select **Settings**, and click **Reset**. Using this option, if you have any remote desktops open, they are not disconnected. All the remote applications are closed, however, and you must start them again.

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

4 Use the local IME as you would with any locally installed applications.

The language designation and an icon for the IME appear in the notification area (system tray) of your 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, will still 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 (available by going to **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 your client system so that if a Horizon Client window has focus, then physical keyboard, onscreen keyboard, mouse, and handwriting pad events are sent to the remote desktop or remote application, even if the mouse or onscreen keyboard is outside of the Horizon Client window.

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 displays the screen resolution in the lower-right corner of the window.

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

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

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 application in full resolution.

The All Monitors display mode displays a remote desktop window on multiple monitors. The remote desktop window appears on all monitors by default. You can use the selective multiple-monitor feature to display a remote desktop window on a subset of your monitors.

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

If you have Horizon Client use all monitors, if you maximize an application window, the window expands to the full screen of only the monitor that contains it.

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," on page 86.
- To use the 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.
- If you use instant clone desktops pools, 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

The remote desktop must have View Agent 6.2 or later, or Horizon Agent 7.0 or later, installed. For 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

You can use the selective multiple-monitor feature to 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. By default, a remote desktop window appears on all monitors in a multiple-monitor setup.

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.

This feature is not supported for remote applications.

Procedure

1 Start Horizon Client and log in to a server.

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

3 Select **PCoIP** or **VMware Blast** from the **Connect Via** drop-down menu.

4 Select **All Monitors** from the **Display** drop-down menu.

Thumbnails of the monitors that are currently connected to your client system appear under Display settings. The display topology matches the display settings on your client system.

5 Click a thumbnail to select or deselect a monitor on which to display the remote desktop window.

When you select a monitor, its thumbnail turns green. A warning message appears if you violate a display selection rule.

6 Click **Apply** to save your changes.

7 Click **OK** to close the dialog box.

8 Connect to the remote desktop.

Your changes are applied immediately when you connect to the remote desktop. Your changes are saved in the Horizon Client 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 preference is not supported for remote applications.

Procedure

1 Start Horizon Client and log in to a server.

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

3 Select **PCoIP** or **VMware Blast** from the **Connect Via** drop-down menu.

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

If you select **Custom**, you can select a specific window size.

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

Your changes take effect immediately after you click **Apply**.

6 Click **OK** to close the dialog box.

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 is opened and centered in the monitor and uses the window size you selected for the display mode, not a size that you might have created by dragging the window to resize it.

Use Display Scaling

A user who has a high-resolution screen such as a 4K monitor, or who has poor eyesight, generally has scaling enabled by setting the DPI (Dots Per Inch) on the client machine to greater than 100 percent. With the Display Scaling feature, the remote desktop or application supports the client machine's scaling setting, and the remote desktop or application appears normal-sized instead of very small.

Horizon Client saves the display scaling setting for each remote desktop separately. For remote applications, the display scaling setting applies to all remote 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 machine.

An administrator 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, an administrator must disable the **DPI Synchronization** group policy setting. For more information, see "Using DPI Synchronization," on page 88.

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 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**.

Procedure

1 Start Horizon Client and connect to a server.

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

3 Select the **Allow display scaling** check box.

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

5 Click **OK** to close the dialog box.

Using DPI Synchronization

The DPI Synchronization feature ensures that the remote desktop's DPI setting matches the client machine's DPI setting for new remote sessions. When you start a new session, Horizon Agent sets the DPI value in the remote desktop to match the DPI value of the client machine.

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 application appropriately.

The DPI Synchronization feature is enabled by default. An administrator can disable the DPI Synchronization feature by disabling the Horizon Agent **DPI Synchronization** group policy setting. You must log out and log in again to make the configuration change take effect. For more information, 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 machine), and display scaling stops working after the DPI settings match.

For single-session virtual machine 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 published 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 machine, you must log out and log in again to make Horizon Client aware of the new DPI setting on the client machine. This requirement applies even if the client machine is running Windows 10.
- If you start a remote session on a client machine that has a DPI setting of more than 100 percent, and then use the same session on another client machine that has a different DPI setting of more than 100 percent, you must log out and log back in to the session on the second client machine to make DPI synchronization work on the second client machine.
- Although Windows 10 and Windows 8.x machines support different DPI settings on different monitors, the DPI Synchronization feature uses only the DPI value that is set on the client machine's primary monitor. All monitors in the remote desktop also use the same DPI setting as the client machine's primary monitor. Horizon Client does not support different DPI settings in different monitors.

- If an 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 automatically 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 application to make the DPI settings match between the client system and remote desktop or application.
- For Windows 10 client machines, right-click on your 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 While a Desktop Window Is Open

You can change display modes, such as from All Monitors mode to Fullscreen mode, without having to disconnect from a remote desktop.

This feature is not supported for remote applications.

Prerequisites

Verify that you are using VMware Blast display protocol or the PCoIP display protocol.

Procedure

1 On the client system, in the notification area (system tray), right-click the **Horizon Client** icon and select the option to open the Settings window.

Note You can also open the Settings window from the application and desktop selection window.

2 Select the remote desktop and select a display option.

Connect USB Devices

You can use locally attached USB devices, such as thumb flash drives, cameras, and printers, from a remote desktop. This feature is called USB redirection.

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

Note With View Agent 6.1 or later, or Horizon Agent 7.0 or later, you can also redirect locally connected USB thumb flash drives and hard disks for use in published desktops and applications on RDS hosts. Other types of USB devices, including other types of storage devices, such as security storage drives and USB CD-ROM, are not supported in published desktops and applications. With Horizon Agent 7.0.2 or later, published desktops and applications can 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 drivers and USB CD-ROM drives, are not supported in published desktops and applications.

Using USB devices with remote desktops has the following 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 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 your 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," on page 99.
- Webcams are not supported for USB redirection using the **Connect USB Device** menu. To use a webcam or audio input device, you must use the Real-Time Audio-Video feature. This feature is available when used with View 5.2 Feature Pack 2 or a later release. See "Using the Real-Time Audio-Video Feature for Webcams and Microphones," on page 93.
- 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. If you have the Real-Time Audio-Video feature, included with View 5.2 Feature Pack 2 or a later release, audio input and output devices work well using that feature, and you do not need to use USB redirection for those devices.

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

Note Do not redirect USB devices such as USB Ethernet devices and touch screen devices to the remote desktop. If you redirect a USB Ethernet device, your client system loses network connectivity. If you redirect a touch screen device, the remote desktop receives touch input but not keyboard input. If you have set your virtual desktop to autoconnect USB devices, you can configure a policy to exclude specific devices.

Important This procedure tells how to use a VMware Horizon Client menu item to configure autoconnecting USB devices to a remote desktop. You can also configure autoconnecting by using the Horizon Client command-line interface or by creating a group policy.

For more information about the command-line interface, see "Running Horizon Client from the Command Line," on page 61. For more information about creating group policies, see the *Configuring Remote Desktop Features in Horizon 7* document.

Prerequisites

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

  This task includes installing the **USB Redirection** component of the agent, and can include setting policies regarding USB redirection. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.
- When Horizon Client was installed, the **USB Redirection** component must have been installed. If you did not include this component in the installation, uninstall the client and run the installer again to include the **USB Redirection** component.

Procedure

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

  The device is manually redirected from the local system to the remote desktop.
- Connect the USB device to a remote hosted application.
  a In the desktop and application selector window, open the remote application.

    The name of the application is the name that your administrator has configured for the application.
  b In the desktop and application selector window, right-click the application icon and select **Settings**.
  c In the left pane, select **USB Devices**.
  d In the right pane, select the USB device and click **Connect**.
  e Select the application, and click **OK**.

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

    You can now use the USB device with the remote application. After you close the application, the USB device is not released right away.
  f When you are finished using the application, to release the USB device so that you can access it from your local system, in the desktop and application selector window, open the Settings window again, select **USB Devices**, and select **Disconnect**.
- Configure Horizon Client to connect USB devices automatically to the remote desktop when 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 a remote desktop.
  b From the VMware Horizon Client menu bar, select **Connect USB Device > Autoconnect USB Devices 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 the remote desktop when Horizon Client starts.
  a From the VMware Horizon Client menu bar, select **Connect USB Device > Autoconnect USB Devices at Startup**.
  b Plug in the USB device and restart Horizon Client.

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

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

If the USB device does not appear in the desktop 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.

Configure Clients to Reconnect When USB Devices Restart

If you do not configure Horizon Client to automatically connect USB devices 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 will connect 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 automatically restarted 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.

If you use the **Automatically Connect When Inserted** option in Horizon Client, all devices that you plug in to the client system get 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 get automatically 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 Use a text editor to open the `config.ini` file on the client.

OS Version	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"
```

Here, *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.deviceN` device properties in order, starting from 0. For example, if the line `usb.quirks.device0` is followed by a line with `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 will succeed because the device will restart and connect 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 your local computer's webcam or microphone on your remote desktop. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications, and supports standard webcams, audio USB devices, and analog audio input.

For information about setting up the Real-Time Audio-Video feature and configuring the frame rate and image resolution in a remote desktop, see the *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. This test application is available as a VMware fling, and therefore no technical support is available for it.

When You Can Use Your 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, a webcam that is built-in or connected to your local computer can be used on your desktop. You can use the webcam in conferencing applications such as Skype, Webex, or Google Hangouts.

During the setup of an application such as Skype, Webex, or Google Hangouts on your remote desktop, you can choose input and output devices from menus in the application. For virtual machine desktops, you can choose VMware Virtual Microphone and VMware Virtual Webcam. For published desktops, you can choose Remote Audio Device and VMware Virtual Webcam.

With many applications, however, this feature will just work, and selecting an input device will not be necessary.

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

Important If you are using a USB webcam, do not connect it from the **Connect USB Device** menu in Horizon Client. To do so routes the device through USB redirection, and the performance will be unusable for video chat.

If you have more than one webcam connected to your local computer, you can configure a preferred webcam to use on your remote desktop.

Select a Preferred Webcam or Microphone on a Windows Client System

With the Real-Time Audio-Video feature, if you have multiple webcams or microphones on your client system, only one of them is used on your remote desktop or application. To specify which webcam or microphone is preferred, you can configure Real-Time Audio-Video settings in Horizon Client.

The preferred webcam or microphone is used on the remote desktop or application if it is available, and if not, 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. To do so routes the device through USB redirection, so that the device cannot use the Real-Time Audio-Video feature.

Prerequisites

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

Procedure

1 Open the Settings dialog box and select **Real-Time Audio-Video** in the left pane.

  You can open the Settings dialog box by clicking the **Settings** (gear) icon in the upper right corner of the desktop and application screen, or by right-clicking a desktop or application icon and selecting **Settings**.

2 Select the preferred webcam from the **Preferred webcam** drop-down menu and the preferred microphone from the **Preferred microphone** drop-down menu.

  The drop-down menus show the available webcams and microphones on the client system.

3 Click **OK** or **Apply** to save your changes.

The next time you start a remote desktop or application, the preferred webcam and microphone that you selected are redirected to the remote desktop or application.

Copying and Pasting Text and Images

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

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

If you use the VMware Blast display protocol or the PCoIP display protocol, a Horizon administrator can set this feature so that copy and paste operations are allowed only from your client system to a remote desktop or application, or only from a remote desktop or application to your client system, or both, or neither.

Horizon administrators configure the ability to copy and paste by configuring group policy settings that pertain to Horizon Agent. Depending on the Horizon server and agent version, administrators 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.

In Horizon 7 version 7.0 and earlier and Horizon Client 4.0 and earlier, the clipboard can accommodate 1 MB of data for copy and paste operations. 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.

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.

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

Configuring the Client Clipboard Memory Size

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

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

To set the 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 Remote Applications

Remote applications look and feel like applications that are installed on your client PC or laptop.

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

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

Saving Documents in a Remote Application

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

Administrators can use an ADMX template file to set a group policy that specifies where documents are saved. This policy is called **Set Remote Desktop Services User Home Directory**. For more information, see the *Configuring Remote Desktop Features in Horizon 7* document.

Printing from a Remote Desktop or Application

From a remote desktop, you can print to a virtual printer or to a USB printer that is attached to your client computer. Virtual printing and USB printing work together without conflict.

You can use the virtual printing feature with the following types of remote desktops and applications:

- Remote desktops that run Windows Server operating systems
- Session-based desktops (on virtual machine RDS hosts)
- Remote hosted applications

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

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

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

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

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

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

- The Windows feature for printing to a file

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

This procedure is written for a remote desktop that has a Windows 7 or Windows 8.x (Desktop) operating system. The procedure is similar but not exactly the same for Windows Server 2008 and Windows Server 2012.

Prerequisites

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

To use virtual printing, the Horizon administrator must enable the virtual printing feature for the remote desktop. This task includes enabling the **Virtual Printing** setup option in the agent installer, and can include setting policies regarding virtual printing behavior. For more information, see the *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.

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 will now be available in the remote desktop.

Using USB Printers

In a Horizon environment, virtual printers and redirected USB printers can work together without conflict.

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 either use the USB redirection feature or use the virtual printing feature. USB printing can sometimes be faster than virtual printing, depending on network conditions.

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

  If you use this redirection feature the printer is no longer logically attached to the physical USB port on the client and this is why the USB printer does not appear in the list of local printers on the local client machine. This also means that you can print to the USB printer from the remote desktop but not 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 "Connect USB Devices," on page 89.

- On some clients, 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, and you do not need to install print drivers on the remote desktop.

Control Adobe Flash Display

The Horizon administrator can set Adobe Flash content to display in your remote desktop at a level designed to conserve computing resources. In some cases, 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 your Horizon administrator specifies.

Adobe Flash display control is available for Internet Explorer sessions on Windows only, and for Adobe Flash versions 9 and 10 only. 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 your 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.

Display quality is improved as long as the cursor remains in the Adobe Flash content.

3 To retain the improvement in quality, double-click inside the Adobe Flash content.

Clicking URL Links That Open Outside of Horizon Client

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

An administrator can also configure URL links that you click inside a browser or application on your client system to open in a remote desktop or application. In this scenario, if Horizon Client is not already open, it starts and prompts you to log in.

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

The first time you start Horizon Client and connect to a server on which the URL Content Redirection feature is configured, Horizon Client prompts you to open the VMware Horizon URL Filter application when you click a link for redirection. Click **Open** to allow URL content redirection.

Depending on how the URL Content Redirection feature is configured, Horizon Client might display an alert message that asks you to change your default Web browser to VMware Horizon URL Filter. If you see this prompt, click the **Use "VMware Horizon URL Filter"** button to allow VMware Horizon URL Filter to become the default browser. This prompt appears only once unless you change your default browser after clicking **Use "VMware Horizon URL Filter"**.

Horizon Client might also display an alert message that asks you to select an application when you click a URL. If you see this prompt, you can click **Choose Application** to search for an application on your client system, or click **Search App Store** to search for and install a new application. If you click **Cancel**, the URL is not opened.

Each company configures its own URL redirection policies. If you have questions about how the URL Content Redirection feature behaves at your company, contact a system administrator.

Using the Relative Mouse Feature for CAD and 3D Applications

If you use the Blast Extreme display protocol or the PCoIP display protocol when using CAD or 3D applications in a View 5.2 or later 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. To use this feature, select **Options > Enable Relative Mouse** from the Horizon Client menu bar.

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.

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

Important This feature requires a View 5.2 or later desktop, and you must turn on 3D rendering for the desktop pool. For more 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.

Using Scanners

You can scan information into your remote desktops and applications with scanners that are connected to your 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 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 Blast Extreme display protocol or the PCoIP display protocol, a scanner connected to your local system can be used in a remote desktop or application.

Important If you are using a scanner, do not connect it from the **Connect USB Device** menu in Horizon Client. To do so routes the device through USB redirection, and the performance will be unusable.

When scanning data is redirected to a remote desktop or 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 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 RDS 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 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. Also, this icon does not appear on Mac or Linux client systems because the feature is not supported on those systems.

- 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 you configure 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 your 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 this feature, users can redirect locally connected, serial (COM) ports such as built-in RS232 ports or USB-to-serial adapters. Devices such as printers, bar code readers, and other serial devices can be connected to these ports and used in the remote desktops.

If a Horizon administrator has configured the serial port redirection feature, and if you use the VMware Blast Extreme or the PCoIP display protocol, serial port redirection works on your 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, unless the COM port is already in use. If so the COM port is mapped to avoid conflicts. For example, if COM1 and COM2 already exist on the remote desktop, COM1 on the client is mapped to COM3 by default.

Although you must have any required device drivers installed on the client system, you do not need to install the device drivers on the remote desktop operating system where the agent is installed. 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. To do so routes the device through USB redirection, and bypasses the serial port redirection functionality.

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, and customize the mapped COM ports.

  When you click the serial port icon, the **Serial COM Redirection for VMware Horizon** context menu appears.

  Note If the items in the context menu are grayed out, it means that the administrator has locked the configuration. Also note that the icon appears only if you use the required versions of the agent and Horizon Client for Windows, and you must connect over Blast Extreme or PCoIP. The icon does not appear if you connect to a remote desktop from a Mac, Linux, or mobile client.

- In the context menu, the port items are listed using the following format, 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 used on the local client system. The second port, which is COM3 in this example, is the port used in the virtual desktop.
- Right-click a COM port to select the **Port Properties** command.

  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 (that is, ignore the data-set-ready signal), which is required for some modems and other devices.

  You can also change the port number used in the remote desktop. For example, if the COM1 port on the client 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 already 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 ESXi host and also from the client system.

- Make sure you connect to a mapped COM port before you attempt to launch an application that requires access to this port. For example, right-click a COM port and select **Connect** to use the port in the remote desktop. When you launch 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. Be sure to use the same settings in the Windows Device Manager on your client system. Note that 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, launch an application that opens the serial port, and then disconnect and resonnect the desktop session, the auto-connect feature does not work. You also cannot connect using the serial port's system tray icon's menu option. In most cases, the application can no longer use the serial port. This is expected behavior. You must terminate the application, disconnect the desktop session and reconnect again to resolve the problem.

Keyboard Shortcuts

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

Shortcuts That Work the Same Way in Horizon Client as in All Applications

Table 5-4. Common Keyboard Shortcuts

Action	Key or Key Combination
Click the highlighted button in a dialog box.	Press Enter.
Invoke the context menu.	Press Shift+F10.
Click the **Cancel** button in a dialog box.	Press ESC.
Navigate between items in the server section window or the desktop and applications selection window.	Use an arrow key to move in the direction of the arrow. Press Tab to move to the right. Press Shift+Tab to move to the left.
Delete an item from the server section window or the desktop and applications selection window.	Press Delete.
In Windows 8.x, navigate between the Start screen and the desktop screen	Press the Windows key.

Horizon Client Window (Server Selection List) Shortcuts

Table 5-5. Key Combinations Specific to the Window Where You Specify Which Server to Connect To

Menu Command or Action	Key Combination
Open the help system in a browser window	Alt+O+H, Ctrl+H
New Server command	Alt+N
Display the Support Information window	Alt+O+S
Display the About Horizon Client window	Alt+O+V

Table 5-5. Key Combinations Specific to the Window Where You Specify Which Server to Connect To (Continued)

Menu Command or Action	Key Combination
Configure SSL command	Alt+O+O
Hide selector after launching an item command	Alt+O+I

Remote Desktop and Application Selector Shortcuts

Table 5-6. Keys and Key Combinations to Use in the Desktop and Application Selection Window

Menu Command or Action	Key Combination
Open the help system in a browser window	Alt+O+H, Ctrl+H
Display **Options** menu	Alt+O
Display the Support Information window	Alt+O+S
Display 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 application or 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 favorite designation	Shift+F10+F
Display **Settings** menu	Alt+S, or Shift+F10+S
Launch the selected item	Enter, or Shift+F10+L
Pin a shortcut for the remote desktop or application to the client system's Start menu (for Windows 7 and earlier) or the Start screen (for Windows 8.x)	Shift+F10+A
Display 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 desktop shortcut for the selected item	Shift+F10+C
Add the selected item to your Start menu or Start screen	Shift+F10+A
Reset the selected desktop (if your administrator allows you to reset)	Shift+F10+R
Refresh the desktop and application list	F5

Desktop Window (with a PCoIP or VMware Blast Extreme Session) Shortcuts

These shortcuts work if you first press Ctrl+Alt or click on the Horizon Client menu bar, rather than inside the remote desktop operating system, before you press the keys.

Table 5-7. Key Combinations for PCoIP and VMware Blast Sessions

Menu Command or Action	Key Combination
Release the mouse cursor so that it is no longer inside the remote desktop operating system	Ctrl+Alt
Display Options menu	Alt+O
Display the Support Information window	Alt+O+M
Display the About Horizon Client window	Alt+O+V
Invoke the Share Folders Settings dialog	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 the desktop, or by reinstalling the VMware Horizon Client application.

This chapter includes the following topics:

Problems with Keyboard Input

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

Problem

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

Cause

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

Solution

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

Connecting to a Server in Workspace ONE Mode

If you cannot connect to a server directly through Horizon Client, or if your desktop and application entitlements are not visible in Horizon Client, Workspace ONE mode might be enabled on the server.

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 desktop or 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 desktop or application through Workspace ONE and Horizon Client starts, you cannot see or open other entitled remote desktops or applications in Horizon Client.

Cause

Beginning with Horizon 7 version 7.2, an 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 applications.

What to Do If Horizon Client Exits Unexpectedly

Horizon Client might exit even if you do not close it.

Problem

Horizon Client might exit unexpectedly. Depending on your Connection Server configuration, you might see a message such as `There is no secure connection to the View Connection Server`. In some cases, no message is displayed.

Cause

This problem occurs when the connection to Connection Server is lost.

Solution

- Restart Horizon Client. You can connect successfully as soon as Connection Server is running again. If you continue to have connection problems, contact your Horizon administrator.

Restart a Remote Desktop

You might need to restart a remote desktop if the desktop operating system stops responding. Restarting a remote desktop is the equivalent of the Windows operating system restart command. The 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 desktop restart feature for the 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.

Procedure

- Use the **Restart Desktop** command.

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

Horizon Client prompts you to confirm the restart action.

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

What to do next

Wait an appropriate amount of time for system startup 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 Remote Applications," on page 107.

Reset a Remote Desktop or Remote 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 remote applications quits all open applications.

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

Resetting remote applications is the equivalent of quitting the applications without saving any unsaved data. All open remote 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 desktop reset feature for the 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 desktop OS	Select **Options > Reset Desktop** from the menu bar.
From the desktop and application selection window	Right-click the desktop icon and select **Reset Desktop**.

2 To reset remote applications, use the **Reset** button in the desktop and application selection 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 reboots and Horizon Client disconnects and logs off from the desktop. When you reset remote applications, the applications quit.

What to do next

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

Repair Horizon Client for Windows

You can sometimes resolve problems with Horizon Client by repairing the Horizon Client application.

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

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

Uninstall Horizon Client for Windows

You might need to uninstall and reinstall Horizon Client if repairing Horizon Client does not solve the problem.

This procedures shows you how to uninstall Horizon Client if 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, or run the Horizon Client installer with the `/uninstall` installation command from the command line, and click **Remove**.
- To uninstall Horizon Client silently, run the Horizon Client installer with the `/silent` and `/uninstall` installation commands from the command line.

  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,” on page 25.

Index

W