

VMware Horizon Client for Windows User Guide

04 JAN 2018

VMware Horizon Client for Windows 4.7



vmware®

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

<https://docs.vmware.com/>

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

docfeedback@vmware.com

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

Copyright © 2008–2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 VMware Horizon Client for Windows User Guide 5**
- 2 How Do I Log In? 6**
- 3 Connecting to Remote Desktops and Applications 7**
 - Setting the Certificate Checking Mode in Horizon Client 7
 - Connect to a Remote Desktop or Published Application 8
 - Use Unauthenticated Access to Connect to Published Applications 10
 - Log Off or Disconnect 11
 - Reconnecting to a Desktop or Published Application 13
 - Hide the VMware Horizon Client Window 13
 - Create a Desktop or Application Shortcut on the Client Desktop or Start Menu 14
 - Using Start Menu Shortcuts That the Server Creates 14
- 4 Using Remote Desktops and Applications 16**
 - Keyboard Shortcuts 16
 - Copying and Pasting Text and Images 19
 - Share Access to Local Folders and Drives with Client Drive Redirection 20
 - Switch Remote Desktops or Published Applications 22
 - Printing from a Remote Desktop or Published Application 22
 - Using Published Applications 24
 - Clicking URL Links That Open Outside of Horizon Client 27
 - Tips for Using the Desktop and Application Selector 27
 - Control Adobe Flash Display 28
 - Resizing the Remote Desktop Window 28
 - Use Display Scaling 29
 - Using DPI Synchronization 29
 - Using the Session Collaboration Feature 31
- 5 Using External Devices 35**
 - Monitors and Screen Resolution 35
 - Supported Multiple Monitor Configurations 36
 - Use USB Redirection to Connect USB Devices 38
 - Using Scanners 41
 - Using the Real-Time Audio-Video Feature for Webcams and Microphones 42
 - Using Serial Port Redirection 44
 - Using the Relative Mouse Feature for CAD and 3D Applications 46

6	Update Horizon Client Online	47
7	Troubleshooting Horizon Client	48
	Restart a Remote Desktop	48
	Reset a Remote Desktop or Published Applications	49
	Repair Horizon Client for Windows	49
	Uninstall Horizon Client for Windows	50
	Problems with Keyboard Input	50
	What to Do If Horizon Client Exits Unexpectedly	51
	Connecting to a Server in Workspace ONE Mode	51

VMware Horizon Client for Windows User Guide



This document, *VMware Horizon Client for Windows User Guide*, explains how to use VMware Horizon[®] Client[™] for Windows to connect to and use remote desktops and applications.

For information about the software installed on your remote desktops, contact your system administrator.

This document assumes that Horizon Client for Windows is already installed and configured on your client system. For information about installing and configuring Horizon Client for Windows, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

How Do I Log In?

Before you can log in and connect to a remote desktop or application, a system administrator at your company must set up your user account. If your system administrator has not set up your user account, you cannot use Horizon Client or HTML Access.

If Horizon Client prompts you for a server name and domain name, your system administrator must tell you the server name to type and domain to select. At some companies, Horizon Client automatically connects to the correct server and selects the correct domain for you.

If you do not know your user name or password or how to reset your password, contact the system administrator at your company.

When you are ready to log in and get started, see [Chapter 3 Connecting to Remote Desktops and Applications](#).

Connecting to Remote Desktops and Applications

3

You can use Horizon Client to connect to remote desktops and applications.

This chapter includes the following topics:

- [Setting the Certificate Checking Mode in Horizon Client](#)
- [Connect to a Remote Desktop or Published Application](#)
- [Use Unauthenticated Access to Connect to Published Applications](#)
- [Log Off or Disconnect](#)
- [Reconnecting to a Desktop or Published Application](#)
- [Hide the VMware Horizon Client Window](#)
- [Create a Desktop or Application Shortcut on the Client Desktop or Start Menu](#)
- [Using Start Menu Shortcuts That the Server Creates](#)

Setting the Certificate Checking Mode in Horizon Client

You can determine whether client connections are rejected if any or some server certificate checks fail by configuring a setting in Horizon Client.

Note At some companies, an administrator might set the default certificate verification mode and prevent end users from changing it in Horizon Client.

Certificate checking occurs for SSL connections between the 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.

To set the certificate checking mode, start Horizon Client and select **Configure SSL** in the **Options** menu on the Horizon Client menu bar. You have three choices:

- **Never connect to untrusted servers.** 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 server that uses a self-signed certificate.

Connect to a Remote Desktop or Published Application

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

If your system administrator instructs you to configure the certificate checking mode, see [Setting the Certificate Checking Mode in Horizon Client](#).

Prerequisites

Obtain the following information from your system administrator:

- Instructions about whether to turn on a VPN (virtual private network) connection.
- Server name to use for connecting to the server.
- If the port is not 443, the port number to use for connecting to the server.
- Credentials to log in, such as an Active Directory user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).
- Domain name for logging in.

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 log in as the currently logged-in Windows domain user, click the **Options** button on the menu bar and select **Log in as current user**.

This setting is available only if the **Log in as current user** feature is installed on the client system.

- 4 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 a server, and click **Connect**.

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

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

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

- 6 In the login dialog box, enter your user name and password, select a domain, and click **Login**.

If you selected **Log in as current user** in the **Options** menu and you are authorized to log in to the server, you are not prompted to enter a user name and password.

If you enter the user name as *username@domain*, it is treated as a user principal name (UPN) because of the at-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*.

- 7 If you are prompted to install applications or desktops to the **Start** menu, click **Yes** or **No**.

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

- 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 the Horizon administrator has allowed it, you can use the Connect Via list to select the display protocol. To use VMware Blast, Horizon Agent 7.0 or later must be installed.
Display layout	Use the Display list to select a window size or to use multiple monitors.

- 9 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.

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

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.

What to do next

If you connected to a remote desktop and you want to connect to this remote desktop each time you log in, select **Autoconnect to this Desktop** from the **Options** menu in the desktop.

Use Unauthenticated Access to Connect to Published Applications

A Horizon administrator can use the Unauthenticated Access feature to create Unauthenticated Access users and entitle those users to published applications. Unauthenticated Access users can log in to the server anonymously to connect to their published applications.

An administrator might preselect the **Log in anonymously using Unauthenticated Access** setting and log you in with a specific Unauthenticated Access user account.

Prerequisites

Obtain the following information from your system administrator:

- Instructions about whether to turn on a VPN (virtual private network) connection.
- Name of server on which you have unauthenticated access to published applications.
- If the port is not 443, the port number to use for connecting to the server.
- An Unauthenticated Access user account to use for logging in anonymously, if necessary.
- Instructions about whether to select **Log in anonymously using Unauthenticated Access** in Horizon Client.

If your system administrator instructs you to configure the certificate checking mode, see [Setting the Certificate Checking Mode in Horizon Client](#).

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 system 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 Connect to the server on which you have unauthenticated access to published applications.

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

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

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

- 5 When the **Login** dialog box appears, select a user account from the **User account** drop-down menu, if necessary.

If only one user account is available, the drop-down menu is disabled and the user account is already selected.

- 6 (Optional) If the **Always use this account** check box is available, select it to bypass the Login dialog box the next time you connect to the server.

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

- 7 Click **Login** to log in to the server.

The application selection window appears.

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

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 published 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: <ul style="list-style-type: none"> ■ 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 A Horizon administrator can configure remote desktops to automatically log off when they are disconnected. In that case, any open programs in the remote 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 published 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: <ul style="list-style-type: none"> ■ 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 authentication credentials.
- b Right-click the desktop icon and select **Logoff**.

Reconnecting to a Desktop or Published Application

For security purposes, a Horizon administrator can set timeouts that log you off of a server after a certain number of hours and that lock a published application after a certain number of minutes of inactivity.

If you have not used a published application for a certain amount of time, you receive a warning prompt 30 seconds before the application is automatically locked. If you do not respond, the application is locked. By default, the timeout occurs after 15 minutes of inactivity, but your Horizon administrator can change the time period. For example, if you have one or more applications open and you walk away from your computer, the application windows might no longer be open when you return an hour later. Instead you might see a dialog box that prompts you to click **OK** so that the application windows appear again.

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

On a Chromebook or an Android device in DeX desktop mode, if you navigate to the desktop and application selector window and one or more previous application sessions are disconnected, Horizon Client prompts you to reconnect to the previous application sessions. You can click **Reconnect to applications** to open the previous application sessions, or click **Not now** to dismiss the message. You can also select a check box to not show the message again.

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 An administrator can configure whether the window is always hidden after a remote desktop or application opens.

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**.

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

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

Procedure

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

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

What to do next

You can rename, delete, or perform any action on a shortcut that you can perform on shortcuts for locally installed applications. 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.

Using Start Menu Shortcuts That the Server Creates

In Horizon 7 version 7.3 and later, a Horizon administrator can configure Start menu shortcuts for remote desktops and applications.

If you are entitled to remote desktops or applications that have shortcuts, Horizon Client places the shortcuts in the Start menu on the client system when you connect to the server.

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

The first time you connect to the server, Horizon Client might prompt you to install the shortcuts, or the shortcuts might be installed automatically, depending on how your system administrator has configured this feature.

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

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

You can remove server-created shortcuts from the Start menu by deleting the server from the Horizon Client server selection window or by uninstalling Horizon Client.

Configure Start Menu Shortcut Update Behavior

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

Prerequisites

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

Procedure

- 1 Open the Settings dialog box and select **Shortcuts**.

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

- 2 Select or deselect the **Automatically update list of application and desktop shortcuts** check box.
- 3 Click **OK** to save your changes.

Using Remote Desktops and Applications

4

You can use Horizon Client to connect to remote desktops and applications. Horizon Client includes additional features to aid navigation.

This chapter includes the following topics:

- [Keyboard Shortcuts](#)
- [Copying and Pasting Text and Images](#)
- [Share Access to Local Folders and Drives with Client Drive Redirection](#)
- [Switch Remote Desktops or Published Applications](#)
- [Printing from a Remote Desktop or Published Application](#)
- [Using Published Applications](#)
- [Clicking URL Links That Open Outside of Horizon Client](#)
- [Tips for Using the Desktop and Application Selector](#)
- [Control Adobe Flash Display](#)
- [Resizing the Remote Desktop Window](#)
- [Use Display Scaling](#)
- [Using DPI Synchronization](#)
- [Using the Session Collaboration Feature](#)

Keyboard Shortcuts

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

Common Keyboard Shortcuts

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

Table 4-1. 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 selection 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.

Server Selection Window Key Combinations

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

Table 4-2. Server Selection Key Combinations

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
Configure SSL command	Alt+O+O
Hide selector after launching an item command	Alt+O+I

Remote Desktop and Application Selector Keyboard Shortcuts

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

Table 4-3. Remote Desktop and Application Selector Keyboard Shortcuts

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

Table 4-3. Remote Desktop and Application Selector Keyboard Shortcuts (Continued)

Menu Command or Action	Key Combination
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 Shortcuts

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

Table 4-4. Desktop Window Shortcuts

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 box	Alt+O+F
Toggle Enable display scaling	Alt+O+N
Switch to Other Desktop command	Alt+O+S

Table 4-4. Desktop Window Shortcuts (Continued)

Menu Command or Action	Key Combination
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

Copying and Pasting Text and Images

By default, you can copy and paste text from the local 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 the 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 the client system to a remote desktop or application, or only from a remote desktop or application to the client system, or both, or neither.

If you are connected to a Horizon 7 version 7.0 or earlier server, the clipboard can accommodate 1 MB of data for copy and paste operations. If you are connected to a Horizon 7 version 7.0.1 or later server, the clipboard memory size is configurable for both the server and the client. When a PCoIP or VMware Blast session is established, the server sends its clipboard memory size to the client. 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 the local client computer.

Share Access to Local Folders and Drives with Client Drive Redirection

You can use Horizon Client to share folders and drives on the local client system with remote desktops and applications. This feature is called client drive redirection.

Drives can include mapped drives and USB storage devices. Mapped drives can have UNC (Universal Naming Convention) paths.

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

You do not need to be connected to a remote desktop or application to configure client drive redirection settings. The settings apply to all 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 published applications directly from the local file system. When you right-click a local file, the **Open with** menu also lists the available published applications. You can also set files to be opened automatically with published 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 published 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 or later servers and agents.

Prerequisites

To share folders and drives with a remote desktop or application, a Horizon administrator must have enabled the client drive redirection feature.

An administrator can hide the client drive redirection feature in Horizon Client.

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	<p>Click the Add button, browse to and select the folder or drive to share, and click OK.</p> <p>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.</p>
Stop sharing a specific folder or drive	<p>Select the folder or drive in the Folder list and click the Remove button.</p>
Permit remote desktops and applications access to files in your local user directory	<p>Select the Share your local files <i>user-name</i> check box.</p>
Share USB storage devices with remote desktops and applications	<p>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.</p> <p>Note USB storage devices already connected to a remote desktop or application with the USB redirection feature are not shared.</p> <p>If this check box is deselected, you can use the USB redirection feature to connect USB storage devices to remote desktops and applications.</p>
Turn on the ability to open a local file with a published application from the local file system	<p>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 published application.</p> <p>You can also change the properties of the file so that all files with that file extension are opened with the published application by default, such as when you double-click the file. For example, you can right-click a file, select Properties, and click Change to select the published application to open files of that type.</p> <p>Your administrator can disable this feature.</p>
Do not show the Sharing dialog box when you connect to a remote desktop or application	<p>Select the Do not show dialog when connecting to a desktop or application check box.</p> <p>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.</p>

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 **This PC** folder, or open Windows Explorer and look in the **Computer** folder, depending on the Windows operating system version.

- From within a published application, if applicable, select **File > Open** or **File > Save As** and navigate to the folder or drive.

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

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

A redirected folder can have two entrances, such as **Z on JSMITH-W03** and **jsmith (Z:)**, and both entrances can appear at the same time. If all the volume labels (from A: through Z:) are already in use, the redirected folder has only one entrance, such as **Z on JSMITH-W03**.

Switch Remote Desktops or Published Applications

If you are connected to a remote desktop, you can switch to another desktop. You can also connect to published 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	<p>Perform one of the following actions:</p> <ul style="list-style-type: none"> ▪ 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 published 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 the other desktop or application. That desktop or application opens in a new window so that you have multiple windows open, and you can switch between them.
Choose a different desktop or application on a different server	<p>Perform either of the following actions:</p> <ul style="list-style-type: none"> ▪ 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.

Printing from a Remote Desktop or Published Application

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

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

With the virtual printing feature, you can use local or network printers from a remote desktop without having to install additional print drivers in the remote desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and other settings.

After a printer is added on the local client computer, Horizon Client adds that printer to the list of available printers on the remote desktop. No further configuration is required. If you have administrator privileges, you 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 applies to remote desktops that have 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.

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 is now available in the remote desktop.

Using USB Printers

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

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

- You can use the USB redirection feature to attach a USB printer to a virtual USB port in the remote desktop 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 [Use USB Redirection to Connect USB Devices](#).

- 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.

Using Published Applications

Published applications look and feel like applications that are installed on the local client PC or laptop.

Follow these tips when using published applications.

- You can minimize and maximize a published application through the application. When a published application is minimized, it appears in the taskbar of your client system. You can also minimize and maximize the published application by clicking its icon in the taskbar.
- You can quit a published application through the application or by right-clicking its icon in the taskbar.
- You can press Alt+Tab to switch between open published applications.

- If a published application creates a Windows System Tray item, that item also appears in the system tray on 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 published applications are listed as VMware Horizon Client - *application name*.

Saving Documents in a Published Application

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

Contact your system administrator to find out where documents created in published applications are saved in your environment.

Configure Published Application Reconnection Behavior

Running published applications might remain open when Horizon Client disconnects from a server. You can configure how running published applications behave when Horizon Client reconnects to the server.

An administrator can disable the published application reconnection behavior settings in Horizon Client.

Procedure

- 1 In the desktop and application selector window of Horizon Client, right-click a published 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 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 Horizon Client connects to the server.

Use a Local IME with Published Applications

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

You can also use hot keys and icons in the notification area (system tray) of the local client system to switch to a different IME. No IME is required to be installed in the server that hosts the published application.

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

By default the feature is disabled. 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.
- Verify that the input language on the local client system matches the language used in the IME.

Procedure

- 1 In the desktop and application selector window of Horizon Client, right-click a published 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 published application icon, select Settings , and click Reset . Using this option, if you have any remote desktops open, they are not disconnected. All the published 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**).

Clicking URL Links That Open Outside of Horizon Client

A Horizon administrator can configure URL links that you click inside a remote desktop or application to open in the default browser on the local 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.

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

A Horizon administrator might set up the URL Content Redirection feature for security purposes. For example, if you are 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 published application. An administrator can configure which application opens the link.

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

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

Tips for Using the Desktop and Application Selector

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

Control Adobe Flash Display

A 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.

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 display protocol 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.

Use Display Scaling

Users that have poor eyesight or high-resolution screens, such as a 4K monitors, generally have scaling enabled by setting the DPI (Dots Per Inch) on the client machine to greater than 100 percent. With the Display Scaling feature, remote desktops and applications support the client machine's scaling setting and appear normal-sized rather than very small.

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

Note An administrator can hide the display scaling setting.

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 DPI setting in a remote session matches the client machine's DPI setting. When you start a new remote session, Horizon Agent sets the DPI value in the session 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. A Horizon administrator can disable the DPI synchronization feature.

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

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

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

- Windows Server 2012 R2
- Windows Server 2016

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.
- 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.

Using the Session Collaboration Feature

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

Invite a User to Join a Remote Desktop Session

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

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

A Horizon administrator can disable the email and IM invitation methods, change the maximum number of collaborators, and disable the Session Collaboration feature. For information about how the Session Collaboration feature behaves at your company, contact your system administrator.

The Session Collaboration feature has the following limitations.

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

Prerequisites

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

Procedure

- 1 Connect to a remote desktop for which the session collaboration feature is enabled.
You must use the VMware Blast display protocol.

- In the system tray in the remote desktop, click the VMware Horizon Collaboration icon, for example,



The collaboration icon looks different depending on the Windows operating system version.

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

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

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

- Select an invitation method.

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

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

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

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

What to do next

Manage the collaborative session in the VMware Horizon Collaboration dialog box. See [Manage a Collaborative Session](#).

Manage a Collaborative Session

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

Prerequisites

Start a collaborative session. See [Invite a User to Join a Remote Desktop Session](#).

Procedure

- 1 In the remote desktop, click the VMware Horizon Collaboration icon in the system tray, or double-click the VMware Horizon Collaboration icon on the desktop.

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

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

Option	Action
Revoke an invitation or remove a collaborator	Click Remove in the Status column.
Hand off control to a session collaborator	<p>After the session collaborator joins the session, toggle the switch in the Control column to On.</p> <p>To resume control of the session, double-click or press any key. The session collaborator can also give back control by toggling the switch in the Control column to Off, or by clicking the Give Back Control button.</p>
Add a collaborator	Click Add Collaborators .
End the collaborative session	<p>Click End Collaboration. All active collaborators are disconnected.</p> <p>You can also end the collaborative session by clicking the VMware Horizon Session Collaboration icon on the desktop and clicking the Stop button.</p>

Join a Collaborative Session

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

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

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

- USB redirection
- Real-Time Audio-Video (RTAV)
- Multimedia redirection
- Client drive redirection
- Smart card redirection
- Virtual printing
- Microsoft Lync redirection
- File redirection and Keep in Dock functionality

- Clipboard redirection

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

Prerequisites

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

Procedure

- 1 Click the link in the collaboration invitation.

Horizon Client opens on the client system.

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

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

- 3 To return mouse and keyboard control to the session owner, click the VMware Horizon Session Collaboration icon in the system tray and toggle the switch in the Control column to **Off**, or click the **Give Back Control** button.
- 4 To leave the collaborative session, click **Options > Disconnect**.

Using External Devices

You can use external keyboards, external displays, microphones, and other external devices with remote desktops and applications in Horizon Client.

This chapter includes the following topics:

- [Monitors and Screen Resolution](#)
- [Supported Multiple Monitor Configurations](#)
- [Use USB Redirection to Connect USB Devices](#)
- [Using Scanners](#)
- [Using the Real-Time Audio-Video Feature for Webcams and Microphones](#)
- [Using Serial Port Redirection](#)
- [Using the Relative Mouse Feature for CAD and 3D Applications](#)

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.

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 published applications.

Prerequisites

Verify that you are using the 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.

Supported Multiple Monitor Configurations

Horizon Client supports the following multiple monitor configurations.

- If you use two monitors, the monitors are not required to be in the same mode. For example, if you are using a laptop connected to an external monitor, the external monitor can be in portrait mode or landscape mode.
- Monitors can be placed side by side, stacked two by two, or vertically stacked only if you are using two monitors and the total height is less than 4096 pixels.
- To use the selective multiple-monitor feature, you must use the VMware Blast display protocol or the PCoIP display protocol. For more information, see [Select Specific Monitors in a Multiple-Monitor Setup](#).
- To use the 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 desktop pools in Horizon 7 version 7.1 or earlier, the maximum number of monitors that you can use to display a remote desktop is two, with a resolution of up to 2560 X 1600.
- With the VMware Blast display protocol or the PCoIP display protocol, a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows version.

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

Hardware Version	Windows Version	Number of 4K Displays Supported
11	7 (3D rendering feature enabled)	1
11	8, 8.x, 10	1

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 published 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 the client system appear under Display settings. The display topology matches the display settings on the 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 changes color. 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 feature is not supported for published 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 USB Redirection to Connect USB Devices

You can use locally attached USB devices, such as thumb flash drives, cameras, and printers, from a remote desktop or a published application. 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 menus in Horizon Client. You use these menus 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. 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 drives and USB CD-ROM drives, are not supported in published desktops and applications.

Using USB devices with remote desktops and published applications 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](#).
- 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. See [Using the Real-Time Audio-Video Feature for Webcams and Microphones](#).
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle. Audio input and output devices work well with the Real-Time Audio-Video feature. You do not need to use USB redirection for those devices.
- You cannot format a redirected USB drive in a published desktop on an RDS host unless you connect as an administrator user.
- The published application auto-connect at startup and auto-connect when inserted features do not work with global application entitlements.

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

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

Prerequisites

- To use USB devices with a remote desktop or published application, a Horizon administrator must enable the USB redirection feature.
- 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 the 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 published application.
 - a Connect the USB device to the local client system.
 - b Start Horizon Client and connect to the published application.
 - c Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window and click **USB Devices**.
 - d In the right pane, select the USB device, click **Connect**, select the published application, and click **OK**.

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

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

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

- g Click **OK** to close the Settings dialog box.
- h When you are finished using the published application, open the Settings dialog box again, select **USB Devices**, and select **Disconnect**.

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

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

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

- a Before you plug in the USB device, start Horizon Client and connect to the remote desktop.
- b From the VMware Horizon Client menu bar, select **Connect USB Device > Automatically Connect when Inserted**.
- c Plug in the USB device.

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

- Configure Horizon Client to connect USB devices automatically to a remote desktop when Horizon Client starts.
 - a From the VMware Horizon Client menu bar, select **Connect USB Device > Automatically Connect at Startup**.
 - b Plug in the USB device and restart Horizon Client.

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

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

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

Using Scanners

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

Scanner redirection supports standard scanning devices that are compatible with the TWAIN and WIA (Windows Image Acquisition) formats. Although you must have the scanner device drivers installed on the local client system, you do not need to install the scanner device drivers on the remote desktop operating system where the agent is installed.

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

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

When scanning data is redirected to a remote desktop or 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 published applications, the system tray icon is redirected to the local client computer.

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

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

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

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

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

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

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

With the Real-Time Audio-Video feature, you can use the local client system's webcam or microphone on a 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.

When You Can Use a Webcam

If a Horizon administrator has configured the Real-Time Audio-Video feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, a webcam that is built-in or connected to the local client computer can be used on a remote 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 the 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 is not necessary.

If the webcam is currently being used by the local client 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 the local client 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 more than one webcam is connected to the local client computer, you can configure a preferred webcam to use on remote desktops.

Select a Preferred Webcam or Microphone on a Windows Client System

With the Real-Time Audio-Video feature, if multiple webcams or microphones are connected to the local client system, only one of the devices is used on the 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 the local client system.

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

Using Serial Port Redirection

With serial port redirection, you 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 display protocol or the PCoIP display protocol, serial port redirection works on the remote desktop without further configuration. For example, COM1 on the local client system is redirected as COM1 on the remote desktop. COM2 is redirected as COM2, 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 local 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 an 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 VMware Blast 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 reconnect 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.

Using the Relative Mouse Feature for CAD and 3D Applications

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

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

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

Update Horizon Client Online

You can update Horizon Client online.

An administrator can disable the online update feature by modifying a group policy setting. You can also disable the online update feature by setting the `AUTO_UPDATE_ENABLED` property to 0 if you install Horizon Client from the command line. For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

Prerequisites

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

Procedure

- 1 Log in to the client system as an administrator.
- 2 In Horizon Client, click **Software Updates**.

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

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

Horizon Client indicates whether an update is available.

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

- 4 If an update is available, click **Download and Install** to begin the update process.
- 5 After Horizon Client downloads the update, click **OK** to install the update.

The Horizon Client interactive installation wizard opens.

Troubleshooting Horizon Client

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:

- [Restart a Remote Desktop](#)
- [Reset a Remote Desktop or Published Applications](#)
- [Repair Horizon Client for Windows](#)
- [Uninstall Horizon Client for Windows](#)
- [Problems with Keyboard Input](#)
- [What to Do If Horizon Client Exits Unexpectedly](#)
- [Connecting to a Server in Workspace ONE Mode](#)

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.

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 Published Applications](#).

Reset a Remote Desktop or Published Applications

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

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

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

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 selector window	Right-click the desktop icon and select Reset Desktop .

- 2 To reset published applications, use the **Reset** button in the desktop and application selector window.
 - a Click the **Settings** button (gear icon) in the menu bar.
 - b Select **Applications** in the left pane, click the **Reset** button in the right pane, and click **OK**.

When you reset a remote desktop, the operating system in the remote desktop reboots and Horizon Client disconnects and logs off from the desktop. When you reset published 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 published 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 procedure 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. For installation instructions, see the *Using VMware Horizon Client for Windows* document.

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.

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.

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

Solution

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