VMware Horizon Client for Windows User Guide

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

Contents

VMware Horizon Client for Windows User Guide

<div align="right">1</div>

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 published applications.

Horizon Client communicates with a server, which acts as a broker between the client device and remote desktops and published applications. You enter credentials into Horizon Client, the server authenticates your credentials, and then the server finds the remote desktops and published applications that you are entitled to use.

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?

2

Before you can log in and connect to a remote desktop or published 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 the domain to select. At some companies, Horizon Client connects to the correct server and selects the correct domain automatically.

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 Published Applications.

Connecting to Remote Desktops and Published Applications

3

Horizon Client makes it easy to work on remote desktops and published applications from your local client device, giving you on-the-go access from any location.

This chapter includes the following topics:

Set the Certificate Checking Mode

Server certificate checking occurs for connections between Horizon Client and a server. A certificate is a digital form of identification, similar to a passport or a driver's license. Your system administrator might ask you to set the certificate checking mode in Horizon Client to make sure that you can successfully connect to a server.

At some companies, an administrator might set the certificate checking mode and prevent you from changing it in Horizon Client.

Procedure

1 Start Horizon Client.

2 Click the **Options** menu on the Horizon Client menu bar and select **Configure SSL**.

3 Select the certificate checking mode.

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

4 (Optional) If your environment includes an SSL proxy server, select the **Allow connection via an SSL Proxy** check box.

This setting allows certificate checking for remote desktop and published application connections through an SSL proxy server. You cannot enable this setting if you select **Do not verify server identity certificates**.

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

What to do next

If you receive a certificate error after setting the certificate checking mode, contact your system administrator.

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.

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 for logging in, such as an Active Directory user name and password, RSA SecurID user name and passcode, RADIUS authentication credentials, or smart card personal identification number (PIN).

- Domain name for logging in.

If your system administrator instructs you to configure the certificate checking mode, see Set the Certificate Checking Mode.

Procedure

1   If a VPN connection is required, turn on the VPN.

2   Start Horizon Client.

3   (Optional) To log in as the currently logged-in Windows domain user, click the **Options** button in the upper-right corner of the menu bar and select **Log in as current user**.

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

4   Connect to a server.

Option	Action
Connect to a new server	Double-click the **+ Add Server** button, or click **New Server** on the menu bar, enter the name of a server as instructed by your system administrator, and click **Connect**.
Connect to an existing server	Double-click the server icon, or right-click the server icon and select **Connect**.

Connections between Horizon Client and the server always use TLS. The default port for TLS connections is 443. If the server is not configured to use the default port, use the format *servername*:*port*, for 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 credentials and click **Continue**.

6   In the login dialog box, enter your user name and password and select a domain, as instructed by your system administrator, 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*, Horizon Client treats it as a user principal name (UPN) and the **Domain** drop-down menu is disabled.

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

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

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

8 (Optional) To configure display settings for a remote desktop, right-click the remote desktop icon and select **Settings**.

Option	Action
Select a display protocol	If a Horizon administrator has allowed it, use the **Connect Via** drop-down menu to select the display protocol.
Select a display layout	Use the **Display** drop-down menu to select a window size or to use multiple monitors.

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

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

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

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

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

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

What to do next

(Optional) To connect to the same remote desktop each time you log in, select **Autoconnect to This Desktop** from the **Options** menu on the menu bar in the remote desktop window.

Use Unauthenticated Access to Connect to Published Applications

If you have an Unauthenticated Access user account, you can log in to a server anonymously and connect to your published applications.

Prerequisites

Obtain the following information from your system administrator:

▪ Instructions about whether to turn on a VPN (virtual private network) connection.

▪ Name of the 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, if necessary.

- Instructions about whether to select **Log in anonymously using Unauthenticated Access** in Horizon Client. A Horizon administrator might preselect this setting and log you in with a specific Unauthenticated Access user account.

If your system administrator instructs you to configure the certificate checking mode, see Set the Certificate Checking Mode.

Procedure

1 If a VPN connection is required, turn on the VPN.

2 Start 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 the client system is configured, this setting might be preselected.

4 Connect to the server on which you have unauthenticated access.

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 as instructed by your system administrator, and click **Connect**.
Connect to an existing server	Double-click the server icon on the Horizon Client home window.

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

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

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

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

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

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

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

The application selector window appears.

8 To start a published application, double-click the published application icon.

Log Off or Disconnect

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

You can log off from a remote desktop even if you do not have the remote desktop open. This feature has the same result as sending Ctrl+Alt+Del to the remote desktop and then clicking **Log Off**.

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

Procedure

◆ Disconnect from a remote desktop without logging off.

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

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

◆ Log off and disconnect from a remote desktop.

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

◆ Disconnect from a published application.

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

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

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

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

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

Disconnecting From a Server

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

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

Reconnecting to a Remote Desktop or Published Application

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

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

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

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

Configure the Autoconnect Feature for a Remote Desktop

You can configure a server to open a particular remote desktop automatically when you connect to that server. You cannot configure a server to open a published application automatically.

Prerequisites

Obtain credentials for connecting to the server, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).

Procedure

1   Start Horizon Client and log in to the server.

2   In the desktop and application selector window, right-click the remote desktop and select
    Autoconnect to this desktop.

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

4   To exit from the dialog box, click **OK**.

5   Disconnect from the server.

6   Reconnect to the server.

    Horizon Client launches the remote desktop automatically.

7   (Optional) If you need to disable the autoconnect feature for the remote desktop, click the **Options**
    drop-down menu in the menu bar in the remote desktop and deselect the **Autoconnect to This
    Desktop** option.

Hide the VMware Horizon Client Window

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

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

Procedure

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

◆   To configure a setting that always hides the VMware Horizon Client window after a remote desktop or
    published application opens, before you connect to a server, click the **Options** button in the menu bar
    and select **Hide the selector after launching an item**.

◆   To show the VMware Horizon Client window after it has been hidden, right-click the VMware Horizon
    Client icon in the system tray and select **VMware Horizon Client**, or, if you are logged in to a remote
    desktop, click the **Options** button in the menu bar and select **Switch to Other Desktop**.

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

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

Procedure

1   Start Horizon Client and log in to the server.

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

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

What to do next

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

Using Shortcuts Created by the Server

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

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

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

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 the Horizon 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 remote desktop or published application opens.

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

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

Configure Start Menu Shortcut Updates

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

Prerequisites

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

Procedure

1 Start Horizon Client and connect to a server.

2 Open the Settings dialog box and select **Shortcuts**.

   ■ Click the **Settings** (gear) icon in the upper right corner of the desktop and application selector window.

   ■ Right-click a remote desktop or published application icon and select **Settings**.

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

Using Remote Desktops and Published Applications

4

Horizon Client includes additional features to help you use remote desktops and published applications on your local client device.

This chapter includes the following topics:

- Keyboard Shortcuts

- Configure Lock Key Synchronization

- Share Access to Local Folders and Drives with Client Drive Redirection

- Copying and Pasting Text and Images

- Dragging and Dropping

- Share Location Information

- Tips for Using Published Applications

- Using the URL Content Redirection Feature

- Control Adobe Flash Display

- Resizing the Remote Desktop Window

- Sharing Remote Desktop Sessions

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.
Open the context menu	Press Shift+F10.
Click the **Cancel** button in a dialog box	Press ESC.

Table 4-1. Common Keyboard Shortcuts (continued)

Action	Key or Key Combination
Navigate between items in the server selection window or the desktop and application selector window	Use an arrow key to move in the direction of the arrow. To move to the right, press Tab. To move to the left, press Shift+Tab.
Delete an item from the server selection window or the desktop and application selector window	Press Delete.
In Windows 8.x, navigate between the **Start** window and the remote desktop window	Press the Windows key.

Server Selection Window Key Combinations

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

Table 4-2. Server Selection Key Combinations

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

Desktop and Application Selector Keyboard Shortcuts

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

Table 4-3. Desktop and Application Selector Keyboard Shortcuts

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

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

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

Desktop Window Shortcuts

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

Table 4-4. Remote Desktop Window Shortcuts

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

Table 4-4. Remote Desktop Window Shortcuts (continued)

Menu Command or Action	Key Combination
Disconnect and Log Off command	Alt+O+L
Connect USB Device command	Alt+U

Configure Lock Key Synchronization

You can configure Horizon Client to synchronize the toggle states of the Num Lock, Scroll Lock, and Caps Lock keys from the client system to a remote desktop.

If an administrator has enabled or disabled lock key synchronization, you cannot configure lock key synchronization in Horizon Client.

Procedure

1   Start Horizon Client and connect to a server.

2   Open the Settings dialog box for the remote desktop.

   ■   Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.

   ■   Right-click the remote desktop in the desktop and application selection window and select **Settings**.

3   To enable the lock key synchronization feature, select the **Automatically synchronize the keypad, scroll and cap lock keys** check box and click **OK**.

Share Access to Local Folders and Drives with Client Drive Redirection

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

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

The maximum length of a shared folder name is 117 characters.

The client drive redirection feature does not support sharing Microsoft OneDrive, Google Drive, and enterprise file storage.

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

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

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

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

Prerequisites

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

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

Procedure

1   Open the Settings dialog box and display the Sharing panel.

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

2   Configure the client drive redirection settings.

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

Option	Action
Share USB storage devices with remote desktops and published applications	Select the **Allow access to removable storage** check box. The client drive redirection feature shares all USB storage devices inserted in your client system and all FireWire and Thunderbolt-connected external drives automatically. Selecting a specific device to share is not necessary.
	Note USB storage devices already connected to a remote desktop or published application with the USB redirection feature are not shared.
	If this check box is deselected, you can use the USB redirection feature to connect USB storage devices to remote desktops and published applications.
Turn on the ability to open a local file with a published application from the local file system	Select the **Open local files in hosted applications** check box. With this option, you can right-click a file in your local file system and select to open the file in a published application.
	You can also change the properties of the file so that all files with that file extension are opened with the published application by default, such as when you double-click the file. For example, you can right-click a file, select **Properties**, and click **Change** to select the published application to open files of that type.
	A Horizon administrator can disable this feature.
Do not show the Sharing dialog box when you connect to a remote desktop or published application	Select the **Do not show dialog when connecting to a desktop or application** check box.
	If this check box is deselected, the Sharing dialog box appears the first time you connect to a remote desktop or published application. For example, if you log in to a server and connect to a remote desktop, you see the Sharing dialog box. If you then connect to another remote desktop or published application, you do not see the dialog box. To see the dialog box again, you must disconnect from the server and log in again.

What to do next

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

- In a Windows remote desktop, open File Explorer and look in the **This PC** folder, or open Windows Explorer and look in the **Computer** folder, depending on the Windows operating system version.

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

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

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

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

Copying and Pasting Text and Images

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

The following data formats are supported.

- CF_BITMAP

- CF_DIB

- CF_HDROP (file type)

- CF_UNICODETEXT

- Biff12

- Art::GVML ClipFormat

- HTML Format

- RTF (Rich Text Format)

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

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

The copy and paste feature has the following limitations.

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

- If you are copying formatted text, some of the data is text and some of the data is formatting information. If you copy a large amount of formatted text or text and an image, when you attempt to paste the text and image, you might see some or all the plain text, but no formatting or image. This problem occurs because the three types of data are sometimes stored separately. For example, depending on the type of document, images might be stored as images or as RTF data.

- If the text and RTF data together use less than the 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 the plain text is pasted.

- If you are unable to paste all the formatted text and images that you selected in one operation, you might need to copy and paste smaller amounts in each operation.

Dragging and Dropping

The drag and drop feature works differently depending on how a Horizon administrator configures the feature.

For example, you might be able to drag and drop files, folders, text, rich text, and images between the client system and remote desktops and published applications, or you might be able to drag and drop only files and folders between the client system and remote desktops and published applications.

Dragging Text and Images

Depending on how a Horizon administrator has configured the drag and drop feature, you might be able to drag text, images, and other data formats between the client system and an open application in a remote desktop or a published application. For example, you might be able to drag text from a browser on the client system and drop it into the WordPad application in a remote desktop.

The following data formats are supported.

- HTML Format
- Rich Text Format (RTF)
- CF_BITMAP
- CF_DIB
- CF_UNICODETEXT
- FileGroupDescriptorW
- FileGroupDescriptor
- FileContents

By default, you can drag up to 1 MB of data, and you can drag only from the client system to a remote desktop or published application. A Horizon administrator can configure the maximum data size and drag and drop direction.

Dragging Files and Folders

Depending on how a Horizon administrator has configured the drag and drop feature, you might be able to drag and drop files and folders between the Windows client system and remote desktops and published applications. You can drag and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation.

If you drag a file or folder between the client system and a remote desktop, the file or folder appears in the file system on the target system. If you drag a file and drop it into an open application, such as Notepad, the text appears in the application. If you drag a file into a new email message, the file becomes an attachment to the email message.

By default, dragging and dropping from the client system to remote desktops and published applications is enabled, and dragging and dropping from remote desktops and published applications to the client system is disabled. A Horizon administrator can configure the drag and drop direction.

Tips for Using the Drag and Drop Feature

When using the drag and drop feature, follow these tips.

Note   Depending on how a Horizon administrator configures the drag and drop feature, some tips might not apply to your environment.

- You must use the VMware Blast or PCoIP display protocol.

- If the relative mouse feature is enabled (**Options > Enable Relative Mouse**), you can drag and drop only from the client system to a virtual desktop.

- When a drag and drop operation is in progress, you cannot start a new drag and drop operation until after the first drag and drop operation has finished.

- When dragging and dropping, you must use the primary mouse button (by default the left button). Using the secondary mouse button (by default the right button), and pressing Ctrl+Shift+Alt plus the primary mouse button, are not supported.

- You cannot drag and drop between remote desktops.

- You cannot drag and drop between published applications.

- If you drag and drop a file or folder between the client system and a remote desktop, the file or folder appears in the file system on the target system. If you drag a file and drop it into an open application, such as Notepad, the text appears in the application. If you drag a file into a new email message, the file becomes an attachment to the email message.

- You can drag and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation.

- By default, dragging and dropping from the client system to remote desktops and published applications is enabled, and dragging and dropping from remote desktops and published applications to the client system is disabled.

- If you are dragging formatted text, some of the data is text and some of the data is formatting information. If you drag a large amount of formatted text, or text and an image, when you attempt to drop the text and image, you might see some or all the plain text, but no formatting or image. This problem occurs because the three types of data are sometimes stored separately. For example, depending on the type of document, images might be stored as images or as RTF data.

- If you are dragging both plain text and RTF data, and the total data size is less than the drag and drop size threshold, the formatted text is copied. Because RTF data cannot be truncated, if the total data size is greater than the drag and drop size threshold, the RTF data is discarded and only the plain text (or part of the plain text) is copied.

- If you are unable to drag all the formatted text and images in one operation, you might need to drag smaller amounts in each operation.

- When you drag a file from the client system and drop it into a published application, you cannot click **Save as** to copy the file back to a different file on the client system. You can click **Save** to copy the file back to the same file on the client system.

- If you drag a file from the client system to an application in a remote desktop, the file is copied to the remote desktop and you can only edit the copy of the file.

- In a 64-bit Windows machine, if you are unable to drag from Horizon Client to a local 64-bit application, try using the 32-bit version of the local application.

- If the target local application fails to accept the dragged object, try dragging the object to the local file system and then dragging it to the target local application from local file system.

- A built-in timeout mechanism exists for fault tolerance.

Share Location Information

When the Geolocation Redirection feature is enabled for a remote desktop or published application, you can share the client system's location information with the remote desktop or published application.

To share the client system's location information, you must configure a setting in Horizon Client.

Prerequisites

A Horizon administrator must configure the Geolocation Redirection feature for the remote desktop or published application.

Procedure

1   Connect to a server.

2   Open the **Settings** dialog box and select **Geolocation** in the left pane.

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

   - Right-click a remote desktop or published application in the desktop and application selector window and select **Settings**.

3   Configure the geolocation settings.

Option	Action
Share the client system's location information with remote desktops and published applications	Select the **Share your location** check box.
Do not show the Geolocation dialog box when you connect to a remote desktop or published application	Select the **Do not show dialog when connecting a desktop or application** check box. The Geolocation dialog box asks you whether you want to share location information with a remote desktop or published application. If this check box is deselected, the Geolocation dialog box appears the first time you connect to a remote desktop or published application. For example, if you log in to a server and connect to a remote desktop, you see the Geolocation dialog box. If you then connect to another remote desktop or published application, you do not see the dialog box again. To see the dialog box again, you must disconnect from the server and log in again.

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

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

Tips for Using Published Applications

Published applications look and feel like applications that are installed on the local client system. When using published applications, follow these tips.

- You can minimize and maximize a published application through the published application. When a published application is minimized, it appears in the taskbar of the client system. You can also minimize and maximize the published application by clicking its icon in the taskbar.

- You can quit a published application through the published application or by right-clicking its icon in the taskbar.

- You can press Alt+Tab to switch between open published applications.

- If a published application creates a Windows System Tray item, that item also appears in the system tray on the client system. By default, the system tray icons appear only to show notifications. You can customize this behavior in the same way that you customize natively installed applications.

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

Reconnect to Published Applications After Disconnecting

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

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

Procedure

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

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

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

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

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

Use Multiple Sessions of a Published Application from Different Client Devices

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

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

The multi-session mode feature has the following limitations.

■ Multi-session mode does not work for applications that do not support multiple instances, such as Skype for Business.

■ If the application session is disconnected while you are using a published application in multi-session mode, you are logged off automatically and any unsaved data is lost.

Prerequisites

A Horizon administrator must enable multi-session mode for the published application. You cannot enable or change the multi-session mode for a published application unless a Horizon administrator allows it.

Procedure

1 Connect to a server.

2 Open the Settings dialog box and select **Multi-Launch** in the left pane.

■ Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window.

■ Right-click a remote desktop or published application in the desktop and application selection window and select **Settings**.

If no published applications are available to use in multi-session mode, the **Multi-Launch** setting does not appear.

3 Select the published applications that you want to use in multi-session mode and click **OK**.

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

Use a Local IME with Published Applications

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

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

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

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

Prerequisites

- Verify that one or more IMEs are installed in the client system.

- Verify that the input language on the local client system matches the language used in the IME.

Procedure

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

2   In the Remote Applications pane, select the **Extend the local IME to hosted applications** check box and click **OK**.

3   Restart the session.

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

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

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

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

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

Using the URL Content Redirection Feature

A Horizon administrator can configure URL links that you click inside a remote desktop or published application to open in the default browser on the local client system. The URL link might be to a Web

page, a phone number, an email address, or another type of link. This feature is called URL Content Redirection.

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

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

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

Using URL Content Redirection with Chrome

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

Control Adobe Flash Display

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

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

Procedure

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

    Depending on how the Horizon administrator configured Adobe Flash settings, you might notice dropped frames or low playback quality.

2   Move the mouse pointer into the Adobe Flash content while it is playing.

    If the pointer remains in the Adobe Flash content, display quality is improved.

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

Resizing the Remote Desktop Window

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

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

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

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

Sharing Remote Desktop Sessions

With the Session Collaboration feature, you can invite other users to join an existing remote desktop session. A remote desktop session that is shared in this way is called a collaborative session. The user that shares a session with another user is called the session owner, and the user that joins a shared session is called a session collaborator.

A Horizon administrator must enable the Session Collaboration feature.

For information about how the Session Collaboration feature behaves at your company, contact your system administrator.

Invite a User to Join a Remote Desktop Session

With the Session Collaboration feature, you can invite users to join a remote desktop session by sending collaboration invitations by email, in an instant message (Windows remote desktops only), or by copying a link to the clipboard and forwarding the link to users.

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 change the maximum number of users that you can invite.

The Session Collaboration feature has the following limitations.

- If you have multiple monitors, only the primary monitor is shown to session collaborators.

- You must select the VMware Blast display protocol when you create a remote desktop session to share. The Session Collaboration feature does not support PCoIP or RDP sessions.

- Anonymous collaboration is not supported. Session collaborators must be identifiable through Horizon-supported authentication mechanisms.

- Session collaborators must have Horizon Client 4.7 or later for Windows, Mac, or Linux installed, or they must use HTML Access 4.7 or later.

- If a session collaborator has an unsupported version of Horizon Client, an error message appears when the user clicks a collaboration link.

- You cannot use the Session Collaboration feature to share published application sessions.

Prerequisites

- The Session Collaboration feature must be enabled and configured.

- To use the email invitation method, an email application must be installed.

- To use the IM invitation method for a Windows remote desktop, Skype for Business must be installed and configured.

Procedure

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

    You must use the VMware Blast display protocol.

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

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

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

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

4 Select an invitation method.

    Not all invitation methods might be available.

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

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

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

What to do next

Manage the remote desktop session in the VMware Horizon Collaboration dialog box. See Manage a Shared Remote Desktop Session.

Manage a Shared Remote Desktop Session

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

A Horizon administrator can configure a remote desktop to prevent the hand off of control to a session collaborator.

Prerequisites

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

Procedure

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

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

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

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

Join a Remote Desktop Session

With the Session Collaboration feature, you can click the link in a collaboration invitation to join a remote desktop session. 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 session in the remote desktop and application selector window.

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

When you join a remote desktop session with the Session Collaboration feature, you cannot use the following features in the remote desktop session.

- USB redirection

- Real-Time Audio-Video (RTAV)

- Multimedia redirection

- Client drive redirection

- Smart card redirection

- Virtual Printing

- VMware Integrated Printing

- Microsoft Lync redirection

- File redirection and Keep in Dock functionality

- Clipboard redirection

You also cannot change the remote desktop resolution in the remote desktop session.

Prerequisites

To join a remote desktop session with the Session Collaboration feature, you must have Horizon Client 4.7 for Windows, Mac, or Linux installed on the client system, or you must use HTML Access 4.7 or later.

Procedure

1   Click the link in the collaboration invitation.

    Horizon Client opens on the client system.

2   Enter your credentials to log in to Horizon Client.

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

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

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

Using External Devices

5

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

This chapter includes the following topics:

- Monitors and Screen Resolution

- Use USB Redirection to Connect USB Devices

- Printing From a Remote Desktop or Published Application

- Using Scanners

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

- Using Serial Port Redirection

- Improve Mouse Performance in a Remote Desktop

Monitors and Screen Resolution

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

Supported Multiple Monitor Configurations

Horizon Client supports the following multiple monitor configurations.

- Horizon 7 version 7.8 adds support for six monitors at 2560 X 1600 resolution with virtual desktops that are running Windows 10 version 1703 or later. Updated Windows display specifications require Windows 10 version 1803 or later for six monitor support on Horizon 7 version 7.9 and later.

- With instant clone desktop pools, the maximum number of monitors is four at 4K resolution.

- 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 two or more 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.

- With Hardware Version 13 or earlier, 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 to Display a Remote Desktop and Select Specific Monitors to Display Published Applications.

- To use the vSGA 3D rendering feature, you must use the VMware Blast display protocol or the PCoIP display protocol. You can use up to two monitors, with a resolution of up to 1920 X 1200. For a resolution of 4K (3840 X 2160), only one monitor is supported.

- For vGPU or other GPU passthrough modes, the vendor hardware and drivers determine the number of monitors and maximum resolution. For more information, see the *NVIDIA GRID Virtual GPU User Guide*, or go to the vendor website.

- If you are using five or more monitors, and you connect to a remote session with VMware Blast, if you use the same user credentials to connect to the session with PCoIP from a different device (without logging off the original session), the initial connection to the new session fails.

- With the VMware Blast display protocol or the PCoIP display protocol, a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows version.

Hardware Version	Windows Version	Number of 4K Displays Supported
10 (ESXi 5.5.x compatible)	7, 8, 8.x, 10	1
11 (ESXi 6.0 compatible)	7 (3D rendering feature disabled and Windows Aero disabled)	3
11	7 (3D rendering feature enabled)	1
11	8, 8.x, 10	1
13 or 14	7, 8, 8.x, 10 (3D rendering feature enabled)	1
13 or 14	7, 8, 8.x, 10	4

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 the Microsoft RDP display protocol, you must have Microsoft Remote Desktop Connection (RDC) 6.0 or later installed in the remote desktop.

Select Specific Monitors to Display a Remote Desktop

If you have multiple monitors, you can select the monitors on which to display a remote desktop window. For example, if you have three monitors, you can specify that the remote desktop window appears on only two of those monitors.

Depending on how a Horizon administrator has configured the remote desktop, you might be able to select between four and six adjacent monitors.

Prerequisites

You must have two or more monitors.

Procedure

1   Start Horizon Client and connect to a server.

2   Open the Settings dialog box for the remote desktop.

- Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.

- Right-click the remote desktop in the desktop and application selection window and select **Settings**.

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

The **Connect Via** drop-down menu appears only if a Horizon administrator has enabled it.

4   From the **Display** drop-down menu, select **All Monitors**.

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

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

When you select a monitor, its thumbnail changes color. If you violate a display selection rule, a warning message appears.

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

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

8   Connect to the remote desktop.

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

Select Specific Monitors to Display Published Applications

If you have three or more monitors, you can select the monitors on which to display published application windows. For example, if you have three monitors, you can specify that published application windows appear on only two of those monitors.

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.

Prerequisites

You must have three or more monitors.

Procedure

1   Start Horizon Client and connect to a server.

2   Open the Settings dialog box for published applications.

▪   Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select **Applications**.

▪   Right-click a published application in the desktop and application selection window and select **Settings**.

3   Under Display settings, select or deselect a monitor on which to display the published application window.

When you select a monitor, its thumbnail changes color. If you violate a display selection rule, a warning message appears.

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

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

Display a Remote Desktop on a Single Monitor in a Multiple-Monitor Setup

If you have two more monitors, but you want a remote desktop window to appear on only one monitor, you can configure the remote desktop window to open on a single monitor.

Prerequisites

You must have two or more monitors.

Procedure

1   Start Horizon Client and connect to a server.

2   Open the Settings dialog box for the remote desktop.

▪   Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.

▪   Right-click the remote desktop in the desktop and application selection window and select **Settings**.

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

The **Connect Via** drop-down menu appears only if a Horizon administrator has enabled it.

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

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

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

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

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

Change the Display Mode for a Remote Desktop

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

Procedure

1   Start Horizon Client and connect to a server.

2   Open the Settings dialog box for the remote desktop.

- Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.

- Right-click the remote desktop in the desktop and application selection window and select **Settings**.

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

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

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

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

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

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

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

Use Display Scaling

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

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

Note   An administrator can hide or preconfigure 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 is in effect, scaling is based on the DPI setting of the primary monitor.

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

Procedure

1   Start Horizon Client and connect to a server.

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

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

    If an administrator has preconfigured display scaling, the check box is dimmed. If an administrator has hidden the display scaling setting, the check box does not appear.

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

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

Using DPI Synchronization

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

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 system), and display scaling stops working after the DPI settings match.

Following are tips for using the DPI Synchronization feature.

- If you change the DPI setting on the client system, but the DPI setting does not change in the remote desktop, you might need to log out and log in again to make Horizon Client aware of the new DPI setting on the client system.

- If you start a remote session on a client system that has a DPI setting of more than 100 percent, and then use the same session on another client system that has a different DPI setting of more than 100 percent, you might need to log out and log back in to the remote session on the second client system to make DPI synchronization work on the second client system.

- Although Windows 10 and Windows 8.x systems support different DPI settings on different monitors, the DPI Synchronization feature uses only the DPI value that is set on the client system's primary monitor. All monitors in the remote desktop also use the same DPI setting as the client system's primary monitor. Horizon Client does not support different DPI settings in different monitors.

- When you connect a laptop that supports different DPI settings on different monitors to an external monitor, and you set the external monitor to be the primary monitor, Windows changes the primary monitor and primary monitor DPI setting every time you detach or reattach the external monitor. In this situation, you must log out and log back in to the client system to make Horizon Client aware of the primary monitor change, and you must log out and log back in to the remote desktop or published application to make the DPI settings match between the client system and remote desktop or published application.

- For Windows 10 client systems, right-click on the desktop, select **Display Settings > Advanced display settings > Advanced sizing of text and other items**, click the **set a custom scaling level** link, and then log out and log in again to make the new DPI setting take effect.

Customize the Display Resolution and Display Scaling for a Remote Desktop

You can use Horizon Client to customize the display resolution and display scaling for a remote desktop. The display resolution determines the clarity of the text and images. At higher resolutions, such as 1600 x 1200 pixels, items appear sharper. Display scaling, which is represented as a percentage, increases or decreases the size of text, icons, and navigation elements.

By default, custom display resolution and display scaling settings are stored only on the local client system. An administrator can configure the local client system so that these settings are stored on the server and are always applied, regardless of the client system that you use to log in to the remote desktop.

This feature has the following limitations and considerations.

■ Customizing the display resolution and scaling for a remote desktop is not supported in multiple-monitor mode.

■ If you select a custom resolution that is higher or lower than the client resolution, Horizon Client resizes the remote desktop window to fit the client window.

■ If you customize the display resolution during a remote desktop session, your changes take effect immediately. If you customize display scaling during a remote desktop session, you must log out and log back in to make your changes take effect.

Procedure

1   Start Horizon Client and connect to a server.

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

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

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

5   To customize the display resolution, select a resolution from the **Resolution** drop-down menu.

If you select **Automatic** (the default setting), Horizon Client fits the remote desktop to the client window size. If the remote desktop does not support the display resolution that you select, it uses the default setting.

6   To customize display scaling, select a scaling size from the **Scaling** drop-down menu.

If you select **Automatic** (the default setting), Horizon Client synchronizes the client system's display scaling to the remote desktop.

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

Use USB Redirection to Connect USB Devices

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

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

The types of USB devices that you can redirect depend on how a Horizon administrator has configured the remote desktop or published application.

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

Prerequisites

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

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

■ Become familiar with USB Redirection Limitations.

Procedure

◆ Manually connect the USB device to a remote desktop.

    a   Connect the USB device to the local client system.

    b   From the VMware Horizon Client menu bar in the remote desktop, click **Connect USB Device**.

    c   Select the USB device.

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

◆ Connect the USB device to a published application.

    a   Connect the USB device to the local client system.

    b   Start Horizon Client and connect to the published application.

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

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

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

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

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

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

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

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

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

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

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

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

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

c   Plug in the USB device.

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

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

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

b   Plug in the USB device and restart Horizon Client.

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

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

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

What to do next

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

USB Redirection Limitations

The USB redirection feature has certain limitations.

■   When you access a USB device from a menu in Horizon Client and use the device in a remote desktop, you cannot access the device on the local computer.

■   USB devices that do not appear in the menu, but are available in a remote desktop, include human interface devices such as keyboards and pointing devices. The remote desktop and the local computer use these devices at the same time. Interaction with these devices can sometimes be slow because of network latency.

■   Large USB disk drives can take several minutes to appear in the remote desktop.

■   Some USB devices require specific drivers. If a required driver is not already installed on a remote desktop, you might be prompted to install it when you connect the USB device to the remote desktop.

- If you plan to attach USB devices that use MTP drivers, such as Android-based Samsung smart phones and tablets, configure Horizon Client so that it automatically connects USB devices to the remote desktop. Otherwise, if you try to manually redirect the USB device by using a menu item, the device is not redirected unless you unplug the device and then plug it in again.

- Do not connect to scanners by using the **Connect USB Device** menu. To use a scanner device, use the scanner redirection feature, if available. See Using Scanners.

- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle. Audio input and output devices work well with the Real-Time Audio-Video feature. You do not need to use USB redirection for those devices.

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

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

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

Printing From a Remote Desktop or Published Application

You can print to a network printer or a locally attached printer from a remote desktop or published application.

You can use the Virtual Printing feature or the VMware Integrated Printing feature, depending on which feature is enabled in Horizon Agent.

Set Printing Preferences for the Virtual Printing Feature

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

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

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

- USB printers that use the USB redirection feature to connect to a virtual USB port in the remote desktop.

  You must disconnect the USB printer from the remote desktop to use the Virtual Printing feature with it.

- The Windows feature for printing to a file.

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

Prerequisites

To use Virtual Printing, a Horizon administrator must enable the Virtual Printing feature for the remote desktop.

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

Procedure

1   In the Windows remote desktop, go to **Control Panel > Hardware and Sound > Devices and Printers**.

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

    In a remote desktop, each virtual printer might appear as *<printer_name>*, *<printer_name>(s<session_ID>)*, or *<printer_name>#:<number>*.

3   On the **General** tab, click **Preferences**.

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

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

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

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

    b   Select the printer and click **Print server properties** at the top of the screen.

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

    This form is now available in the remote desktop.

Set Printing Preferences for the VMware Integrated Printing Feature

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

Prerequisites

To use VMware Integrated Printing, a Horizon administrator must enable the VMware Integrated Printing feature for the remote desktop.

To determine whether the VMware Integrated Printing feature is installed in a remote desktop, verify that the `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` and `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` files exist in the remote desktop file system.

This feature requires Horizon Agent 7.7 or later.

Procedure

1   In the Windows remote desktop, go to **Control Panel > Hardware and Sound > Devices and Printers**.

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

    In a single-user virtual machine desktop, each virtual printer appears as *<printer_name>*(*vdi*). In a published desktop or published application, each virtual printer appears as *<printer_name>*(*v<session_ID>*).

3   On the **General** tab, click **Preferences**.

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

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

Using USB Printers

A USB printer is a printer that is attached to a USB port on the local client system. You can send print jobs to a USB printer attached to the local client system from a remote desktop.

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

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

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

- You can alternatively use the Virtual Printing feature or the VMware Integrated Printing feature to send print jobs to a USB printer. You can print to the USB printer from both the remote desktop and the client system, and you do not need to install printer drivers in the remote desktop.

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

Using Scanners

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

Scanner redirection supports standard scanning devices that are compatible with the TWAIN and WIA (Windows Image Acquisition) formats. You must install the scanner device drivers on the local client system. You do not need to install the scanner device drivers on a remote desktop.

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 client system can be used in a remote desktop or published application.

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

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

A Horizon administrator can configure group policy settings to control the options that available in the VMware Horizon Scanner Redirection Preferences dialog box.

Note   If a Horizon administrator configures scanner redirection to use a specific scanner and that scanner is not available, scanner redirection does not work.

Tips for Using the Scanner Redirection Feature

- To change scanner redirection settings, click the scanner icon ( ) in the system tray or notification area of the remote desktop. In a published application, the system tray icon is redirected to the local client computer.

  Note   You do not need to use the menu that appears when you click the scanner icon. Scanner redirection works without any further configuration. If the menu does not list any scanners, an incompatible scanner is connected to the local client system. If the scanner icon does not appear, the scanner redirection feature is either disabled or not installed on the remote desktop. The scanner icon also does not appear on local client systems that do not support this feature.

- If you want the TWAIN Scanning Properties dialog box to appear even if a scanning application does not display the scanning dialog box, click the **Preferences** option in the scanner icon menu and select the **Force the TWAIN Scanning Properties dialog** check box.

- To display the actual scanner names rather than VMware Virtual *nnn* scanner, click the **Preferences** option in the scanner icon menu and select the **Use vendor defined names for TWAIN scanners** check box.

- To select options to control image compression or determine how to select the default scanner, click the **Preferences** option in the scanner icon menu and select the **Compression** or **Defaults** tab.

- If you plan to use the Real-Time Audio-Video feature to redirect webcams as recommended by VMware, click the **Preferences** option in the scanner icon menu and select the **Hide webcam type imaging devices** check box.

- Most TWAIN scanners display a scanner settings dialog box by default, but some do not. For those scanners that do not display settings options, you can use the **Preferences** option in the scanner icon menu and select the **Always show Scanner Settings dialog** option.

- To display the TWAIN Scanner Properties dialog box on the remote desktop, click the **Preferences** option in the scanner icon menu and select the **Agent (VMware Scanning Properties dialog)** check box. To display the TWAIN Scanner Properties dialog box on the local client system, select the **Client (Native Scanning Properties dialog, if supported)** check box.

  Note In the agent-side TWAIN Scanner Properties dialog box, some less-common options might not be included. To use these less-common options, select the **Client (Native Scanning Properties dialog, if supported)** check box.

- Scanning too large an image or scanning at too high a resolution might not work. In this case, you might see the scanning progress indicator freeze, or the scanner application might exit unexpectedly. If you minimize the remote desktop, an error message might appear on the local client system, notifying you that the resolution is set too high. To resolve this issue, reduce the resolution or crop the image to a smaller size and scan again.

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

With the Real-Time Audio-Video feature, you can use the local client system's webcam or microphone in a remote desktop or published application. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications. It supports standard webcams, audio USB devices, and analog audio input.

When You Can Use a Webcam with the Real-Time Audio-Video Feature

If a Horizon administrator has configured the Real-Time Audio-Video feature, you can use a webcam that is built in or connected to the client computer in a remote desktop or published application. You can use the webcam in conferencing applications such as Skype, Webex, or Google Hangouts.

During the setup of an application such as Skype, Webex, or Google Hangouts on a remote desktop, you can select input and output devices from menus in the application.

For remote desktops, a redirected webcam might be named VMware Virtual Webcam in the application, or it might have the actual device name with (VDI) appended, for example, C670i FHD Webcam (VDI), depending on whether multiple webcams are supported. In published applications, a redirected webcam is always named VMware Virtual Webcam in remote sessions.

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

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

Important   If you use a USB webcam, do not connect it from the **Connect USB Device** menu in Horizon Client. Doing so routes the device through USB redirection and the performance is not usable for video chat.

With a remote desktop, if more than one webcam is connected to the client computer, you might need to configure a preferred webcam, depending on how a Horizon administrator has configured the remote desktop. With a published application, you can use only one webcam in remote sessions, and you must configure a preferred webcam.

For more information, see Select a Preferred Webcam or Microphone on a Windows Client System.

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 client system, you can specify which webcam or microphone is preferred by configuring Real-Time Audio-Video settings in Horizon Client.

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

With the Real-Time Audio-Video feature, video devices, audio input devices, and audio output devices work without requiring the use of USB redirection, and the amount of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

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

Prerequisites

- Ask your Horizon administrator if you need to configure a preferred webcam or microphone. Some remote desktops support multiple devices with the Real-Time Audio-Video feature and you do not need to configure a preferred webcam or microphone.

- Verify that a USB webcam or USB microphone, or other type of microphone, is installed and operational on the client system.

- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for the remote desktop or published application.

- Connect to a server.

Procedure

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

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

- Right-click a remote desktop or published application in the desktop and application selector window and select **Settings**.

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

The menu shows the available webcams on the client system.

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

The menu shows the available microphones on the client system.

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

Using Multiple Devices with the Real-Time Audio-Video Feature

If more than one webcam or microphone is connected to the client computer, and the remote desktop supports multiple device redirection with the Real-Time Audio-Video feature, you can use all the webcams and microphones connected to the client computer in the remote desktop.

Whether you can use more than one webcam or microphone with the Real-Time Audio-Video feature depends on how a Horizon administrator has configured the remote desktop.

Following are tips for using more than one webcam or microphone with the Real-Time Audio-Video feature.

- When you connect to a remote desktop, the Real-Time Audio-Video feature redirects all webcams and microphones currently connected to the client computer. The remote desktop decides which webcam and microphone is the default device. You do not need to configure a preferred webcam or microphone in Horizon Client.

- If you disconnect a webcam or microphone from the client computer, and the device is not being used in an application in the remote desktop, the Real-Time Audio-Video feature deletes the device in the remote desktop immediately. If the device is being used by an application in the remote desktop, the Real-Time Audio-Video feature deletes the device after the application releases it.

- The display name of a redirected device is the actual device name, but with (VDI) appended, for example, C670i FHD Webcam (VDI).

- You can use multiple redirected devices simultaneously in a remote desktop.

Using Serial Port Redirection

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

If a Horizon administrator has configured the serial port redirection feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, serial port redirection works in the remote desktop without further configuration. For example, COM1 on the local client system is redirected as COM1 on the remote desktop. COM2 is redirected as COM2. If the COM port is already in use, it is mapped to avoid conflicts. For example, if COM1 and COM2 exist on the remote desktop, COM1 on the client system is mapped to COM3 by default.

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

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

Tips for Using the Serial Port Redirection Feature

- Click the serial port icon (🖫) in the system tray or notification area of the remote desktop to connect, disconnect, or customize the mapped COM ports.

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

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

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

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

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

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

   When a redirected COM port is opened and in use on a remote desktop, you cannot access the port on the local computer. Conversely, when a COM port is in use on the local computer, you cannot access the port on the remote desktop.

- In the remote desktop, you can use the Windows Device Manager **Port Settings** tab to set the default Baud rate for a particular COM port. Use the same settings in the Windows Device Manager on the client system. The settings from this tab are used only if the application does not specify the port settings.

- Before you can disconnect the COM port, you must close the port in the application or close the application. You can then select the **Disconnect** command to disconnect and make the physical COM port available for use on the client computer.

- If you configure a serial port to connect automatically, start an application that opens the serial port, and then disconnect and reconnect the remote desktop session, the auto-connect feature does not work. You also cannot connect by using the serial port's system tray icon's menu option. In most cases, the application can no longer use the serial port. You must stop the application, disconnect the remote desktop session, and reconnect again to resolve the problem.

Improve Mouse Performance in a Remote Desktop

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

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

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

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

Prerequisites

A Horizon administrator must turn on 3D rendering for the remote desktop.

Procedure

1   Start Horizon Client and log in to the server.

2   Right-click the remote desktop and select **VMware Blast** or **PCoIP**.

3   Connect to the remote desktop.

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

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

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

Update Horizon Client Online

<div style="text-align: right; font-size: large;">6</div>

You can update Horizon Client online.

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.

- Verify that the online update feature is enabled.

Procedure

1   Log in to the client system as an administrator.

2   Start Horizon Client and click **Software Updates**.

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

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

   Horizon Client indicates whether an update is available.

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

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

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

   The Horizon Client interactive installation wizard opens.

Troubleshooting Horizon Client

7

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

This chapter includes the following topics:

- Restart a Remote Desktop
- Reset Remote Desktops or Published Applications
- Repair Horizon Client for Windows
- Uninstall Horizon Client for Windows
- Problems with Keyboard Input
- What to Do If Horizon Client Quits Unexpectedly
- Connecting to a Server in Workspace ONE Mode

Restart a Remote Desktop

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

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

Procedure

◆ Use the **Restart Desktop** command.

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

Horizon Client prompts you to confirm the restart action.

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

What to do next

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

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

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

Resetting published applications quits all open applications.

Resetting published applications quits the applications without saving any unsaved data. All open published applications are closed.

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

Procedure

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

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

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

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

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

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

What to do next

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

Repair Horizon Client for Windows

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

Prerequisites

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

- Verify that you have the Horizon Client installer. You cannot repair Horizon Client if you do not have the installer.

Procedure

◆ To repair Horizon Client interactively, perform one of the following tasks.

- Double-click the Horizon Client installer and click **Repair**.

- Run the Horizon Client installer from the command line and enter the `/repair` command.

    For example, at the command prompt, type the following command:

    ```
    VMware-Horizon-Client-y.y.y-xxxxxx.exe /repair
    ```

    y.y.y is the version number and *xxxxxx* is the build number.

◆ To repair Horizon Client silently, run the Horizon Client installer from the command line and enter the `/silent` and `/repair` commands.

    For example, at the command line, type the following command:

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

    y.y.y is the version number and *xxxxxx* is the build number.

Uninstall Horizon Client for Windows

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

This procedures shows you how to uninstall Horizon Client when you have the Horizon Client installer.

If you do not have the Horizon Client installer, you can uninstall Horizon Client in the same way that you uninstall other applications on your Windows system. For example, on a Windows 10 system, you can use the Windows operating system uninstall or change a program feature (**Control Panel > Programs and Features > Uninstall or change a program**).

Prerequisites

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

Procedure

◆ To uninstall Horizon Client interactively, perform one of the following tasks.

- Double-click the Horizon Client installer and click **Remove**.

- Run the Horizon Client installer from the command line and enter the `/uninstall` command.

For example, at the command prompt, type the following command:

```
VMware-Horizon-Client-y.y.y-xxxxxx.exe /uninstall
```

y.y.y is the version number and *xxxxxx* is the build number.

◆ To uninstall Horizon Client silently, run the Horizon Client installer from the command line and enter the `/silent` and `/uninstall` commands.

For example, at the command prompt, type the following command:

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

y.y.y is the version number and *xxxxxx* is the build number.

What to do next

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

Problems with Keyboard Input

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

Problem

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

Cause

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

Solution

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

What to Do If Horizon Client Quits Unexpectedly

Horizon Client quits even if you do not close it.

Problem

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

Cause

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

Solution

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

Connecting to a Server in Workspace ONE Mode

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

Problem

■ When you try to connect to the server directly through Horizon Client, Horizon Client redirects you to the Workspace ONE portal.

■ When you open a remote desktop or published application through a URI or shortcut, or when you open a local file through file association, the request redirects you to the Workspace ONE portal for authentication.

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

Cause

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

Solution

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