VMware Horizon Client for Chrome User Guide

MAR 2020

VMware Horizon Client for Chrome 5.4

vmware®

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

https://docs.vmware.com/

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

Contents

VMware Horizon Client for Chrome User Guide

This document, *VMware Horizon Client for Chrome User Guide*, explains how to use VMware Horizon® Client™ for Chrome 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 Chrome is already installed and configured on your client device. For information about installing and configuring Horizon Client for Chrome, see the *VMware Horizon Client for Chrome Installation and Setup Guide* document.

How Do I Log In?

1

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 Connect to a Remote Desktop or Published Application.

Connecting to Remote Desktops and Published Applications

2

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:

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 to log 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 you are using smart card authentication, see Smart Card Authentication Limitations.

Procedure

1 Log in to the Chromebook.

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

3 Open the VMware Horizon Client app.

4 If you are prompted to grant access to the Smart Card Connector, click **Allow**.

This prompt appears the first time you start Horizon Client if smart card authentication is configured on the Chromebook.

5 Connect to a server.

Option	Action
Connect to a new server	Click the plus sign (+), enter the name of the server as instructed by your system administrator, enter a description of the server (optional), and click **Connect**.
Connect to an existing server	Click the server shortcut.

Connections between Horizon Client and servers 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`.

6 If a smart card is required or optional, select the smart card certificate to use and enter your PIN.

7 If you are prompted for RSA SecurID or RADIUS authentication credentials, enter the credentials, and click **Login**.

The passcode might include both a PIN and the generated number on the token.

8 If you are prompted a second time for RSA SecurID or RADIUS authentication credentials, enter the next generated number on the token.

Do not enter your PIN, and do not enter the same generated number that entered previously. If necessary, wait until a new number is generated. If this step is required, it is required only when you mistype the first passcode or when configuration settings in the RSA server change.

9 If you are prompted for a user name and password, supply your Active Directory credentials.

a Enter a user name and password as instructed by your system administrator.

b Select a domain as instructed by your system administrator.

If you cannot select a domain, you must enter the user name in the format `username@domain` or `domain\username`.

c Tap **Login**.

10 (Optional) To mark a remote desktop or published application as a favorite, click the gray star inside the icon for the remote desktop or published application.

   The star icon turns from gray to yellow. The next time you log in, you can click the star icon in the upper-right part of the browser window to show only favorite items.

11 To connect to remote desktop or published application, click its icon in the desktop and application selector window.

12 If you are using smart card authentication, enter the smart card PIN again inside the remote session.

Results

If, soon after connecting to a remote desktop or published application, you are disconnected and see a prompt that asks you to click a link to accept the security certificate, select whether to trust the certificate. See Trust a Self-Signed Root Certificate.

If the time zone in the remote desktop or published application does not use the time zone set in the client device, set the time zone manually. See Setting the Time Zone.

What to do next

Horizon Client provides navigation aids to help you use remote desktops and published applications. For information, see Using Remote Desktops and Using Published Applications.

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:

- Server name to use for connecting to the server.
- An Unauthenticated Access user account to use for logging in anonymously.

Procedure

1 Click the **Settings** toolbar button in the upper-right corner of the server selection page and toggle the **Log in anonymously using Unathenticated Access** option to on.

2 Connect to a server, enter an Unauthenticated Access user account, and click **Login**.

   The application selection window appears.

3 Click the icon for the published application that you want to access.

Smart Card Authentication Limitations

With smart card authentication, you plug a smart card reader into the Chromebook, insert a smart card, and select a server in Horizon Client. During the authentication step, you enter a PIN instead of a user name and password. After you select a remote desktop or published application, all smart card commands and responses are redirected to the remote desktop or published application.

Smart card authentication has certain limitations when used with Horizon Client for Chrome.

- Single sign-on is not supported. When you connect to a remote desktop or published application, you must enter the smart card PIN again inside the remote session.
- After you use a smart card to authenticate to a server, you cannot switch to another authentication method, such as Active Directory authentication. To use a different authentication method the next time you connect to a server, you must log out of the Chrome OS or reboot the Chromebook.
- After you select a certificate and enter your PIN, the certificate you selected is cached on the Chromebook and is used the next time you connect to a server. To select a different certificate the next time you connect to a server, you must reboot the Chromebook.

Trust a Self-Signed Root Certificate

Sometimes, when connecting to a remote desktop or published application for the first time, the browser might prompt you to accept the self-signed certificate that the remote machine uses. You must trust the certificate before you can connect to the remote desktop or published application.

Chrome gives you the option to trust the self-signed certificate permanently. If you do not trust the certificate permanently, you must verify the certificate every time you restart your browser.

Procedure

1. If the browser presents an untrusted certificate warning, or a warning appears stating that your connection is not private, examine the certificate to verify that it matches the certificate that your company uses.

   You might need to contact your system administrator for assistance. For example, in Chrome, you might use the following procedure.

   a. Click the lock icon in the address bar.

   b. Click the **Certificate information** link.

   c. Verify that the certificate matches the certificate that your company uses.

      You might need to contact your system administrator for assistance.

2 Accept the security certificate.

   In Chrome, you can click the **Advanced** link on the browser page, and click **Proceed to *server-name* (unsafe)**.

Results

The remote desktop or published application starts.

Setting the Time Zone

The time zone that a remote desktop or published application uses is set to the time zone in your local system automatically.

When you use Horizon Client, if the time zone cannot be correctly determined due to certain daylight saving policies, you might need to set the time zone manually.

To set the correct time zone manually before you are connected to a remote desktop or published application, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window. Turn off the **Set Time Zone Automatically** option in the **Settings** window and select one of the time zones from the drop-down menu. The value you select is saved as your preferred time zone to use when connecting to a remote desktop or published application.

To set the correct time zone manually after you are connected to a remote desktop or published application, return to the desktop and application selector window and change the current time zone setting.

Manage Server Shortcuts

After you connect to a server, Horizon Client creates a server shortcut. You can edit and remove server shortcuts.

Horizon Client saves the server name or IP address in a shortcut, even if you mistype the server name or type the wrong IP address. You can delete or change this information by editing the server name or IP address. If you do not type a server description, the server name or IP address becomes the server description.

Procedure

1 Right-click the server shortcut.

   A context menu appears.

2 Use the context menu to delete the server shortcut or edit the server name or server description.

3 If you edited the server shortcut, click **Complete** to save your changes.

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.

Procedure

- Disconnect from a remote desktop.

Option	Description
From within the remote desktop	Point your mouse at the top of the remote desktop window until the menu bar appears and then click the **Disconnect** button. Alternatively, click the **X** (Close) button in the upper-right corner of the remote desktop window.
From the Session Management Center	Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window, open the Session Management Center, select the remote desktop session, and click **Disconnect**. You can also open the Session Management Center by right-clicking the remote desktop icon in the shelf and clicking **Session Management Center**.

- Log off from a remote desktop.

Option	Description
From within the remote desktop	Point your mouse at the top of the remote desktop window until the menu bar appears and then click the **Log out** button.
From the Session Management Center	Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window, open the Session Management Center, select the remote desktop session, and click **Log off**. You can also open the Session Management Center by right-clicking the remote desktop icon in the shelf and clicking **Session Management Center**.

- Close a published application.

Option	Description
From within the published application	Click the **X** (Close) button in the corner of the published application window.
From the shelf	Right-click the published application icon in the shelf and click **Close**.

- To log off from a server, click the **Log Out** button in the upper-right corner of the desktop and application selector window.

Using Remote Desktops and Published Applications

3

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:

Gestures

VMware has created user interaction aids to help you navigate conventional Windows user interface elements on a non-Windows device.

Clicking

As in other apps, you can tap your touchpad to click a user interface element. If the Chromebook has a touch screen, you can touch to click a user interface element. You can also use an external mouse.

Right-Clicking

The following options are available for right-clicking:

- Tap with two fingers on the touchpad.
- Hold down the Alt key on the keyboard and tap the touchpad with a single finger.
- Use an external mouse to right-click.
- If the Chromebook has a touch screen, tap with two fingers to right-click.

Scrolling and Scrollbars

The following options are available for vertical scrolling.

- Tap and hold with your thumb and then scroll down with one finger on the touchpad. You can also scroll with two fingers.
- Use an external mouse to scroll.
- If the Chromebook has a touch screen, tap with two fingers and then drag to scroll. The text under your fingers moves in the same direction as your fingers.

Zooming In and Out

Zooming in and out is not supported.

Window Resizing

To use the touchpad to resize a window, touch and hold one finger at the corner or side of the window and drag to resize.

If the Chromebook has an external mouse, place your cursor on the edge of the window and drag the border of the window to make it wider or narrower.

If the Chromebook has a touch screen, place one finger at the corner or side of the window and drag to resize.

Sound, Music, and Video

If sound is turned on for your device, you can play audio in a remote desktop.

Multiple Monitor Feature Limitation

Touch gestures are disabled when the multiple monitor feature is enabled. For more information, see Using Multiple Monitors.

Using Remote Desktops

You can use the top menu bar in a remote desktop window to perform common tasks in a remote desktop.

- To open the top menu bar in a remote desktop, move your mouse to the top of the remote desktop window until the top menu bar appears.
- To use the Ctrl+Alt+Delete keyboard shortcut inside a remote desktop, click **Send Ctrl+Alt +Delete to the to current work area** in the top menu bar.
- To enter full screen mode, click **Fullscreen** in the top menu bar. To exit full screen mode, click **Quit Fullscreen** in the top menu bar.
- To use the Esc key in a remote desktop when the remote desktop is in full screen mode, click **Send ESC** in the top menu bar.
- To disconnect from a remote desktop, click **Disconnect** in the top menu bar, or click the **X** (Close) button in the upper-right corner of the remote desktop window.
- To view information about Horizon Client, click **About** in the top menu bar.

To switch to another open remote desktop, click that remote desktop window. You can also browse through all the open remote desktops (including local and published applications) on the client device by pressing Alt+Tab. To focus on a selected remote desktop, release the Alt key.

For information about logging off from a remote desktop, see Log Off or Disconnect. For information about restarting a remote desktop, see Restart a Remote Desktop. For information about resetting a remote desktop, see Reset Remote Desktops or Published Applications.

Using Published Applications

Horizon Client provides navigation aids to help you use published applications.

- To maximize and minimize a published application, click the **Maximize** and **Minimize** buttons in the same way that you do in any application.
- To restore a minimized published application, click its shelf icon on the client device or select the published application session and click the **Restore** button in the Session Management Center window. In Kiosk mode, you must use the Session Management Center to restore a minimized published application. For more information, see Using Published Applications in Kiosk Mode.
- To reset a published application, see Reset Remote Desktops or Published Applications.

To switch to another open published application, click the published application window. You can also browse through all open published applications (including local applications and remote desktops) on the client device by pressing Alt+Tab. To focus on a selected published application, release the Alt key.

Using Published Applications in Kiosk Mode

When you are using published applications in Kiosk mode, you must use the Session Management Center to perform certain tasks.

- To open the Session Management Center window, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and click **Open** next to **Session Management Center**. If you have a remote desktop session open, you must close the remote desktop session before you can access the desktop and application selector window.
- To restore a minimized published application in Kiosk mode, select the published application session and click the **Restore** button in the Session Management Center window.
- To switch published applications in Kiosk mode, select the published application session and click the **Restore** button in the Session Management Center window.
- To close the Session Management Center window in Kiosk mode, click the close (**X**) button in the upper-right corner of the Session Management Center window.

Copying and Pasting Text and Images

By default, you can copy and paste plain text and HTML-format rich text from the client device to a remote desktop or published application.

You can also copy and paste plain text and HTML-format rich text from a remote desktop or published application to the client device if a Horizon administrator enables this feature.

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

When you copy and paste images and rich text, the following restrictions apply.

- If the clipboard source is a Google app, such as Google Docs, you can copy and paste images only when the client device can access the Google website.
- If you copy an image and rich text (or plain text) together from the client device, and the destination is an application that supports only rich text, such as WordPad, the image is discarded and only the text is copied and pasted. If the destination application supports HTML/XML-format rich text, such as Microsoft Word, this restriction does not apply.

You can copy a maximum of 1 MB of data from a remote desktop or published application to the client device. Plain text that exceeds this limit is truncated. Rich text is converted to plain text.

The clipboard can accommodate a maximum of 1 MB of data for all types of copy and paste operations. If the plain text and rich text data together use less than maximum clipboard size, the formatted text is pasted. Often the rich text cannot be truncated, so that if the text and formatting use more than the maximum clipboard size amount, the rich text is discarded, and plain text is pasted. If you are unable to paste all the formatted text you selected in one operation, you might need to copy and paste smaller amounts in each operation.

Transferring Files Between the Client and a Remote Desktop or Published Application

You can transfer files from the client device to a remote desktop or published application. You might also be able to transfer files from a remote desktop or published application to the client system.

To upload a file, drag the file from the client system to the remote desktop or published application window. When the upload is finished, the file appears in the `C:\Users\`*`username`*`\Documents` folder.

To download a file, select the file in the remote desktop or published application by pressing Ctrl +C. After you confirm the file transfer, the file appears in the `Downloads` directory on the client device.

A Horizon administrator can configure the ability to allow, disallow, or allow in one direction only, the transfer of files. The default is to only transfer files from the client system to a remote desktop or published application.

This feature has the following limitations.

- You can download files up to 500 MB and upload files up to 2 GB.
- You cannot download or upload folders or files that have a size of zero.
- If a file transfer is in progress in a remote session and you open a connection to a second remote session, and if a security warning appears, if you ignore the warning and continue to connect to the second remote session the file transfer in the first session aborts.

Share Access to Local Folders and Drives with Client Drive Redirection

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

Shared drives can include mapped drives and USB storage devices.

The client drive redirection feature has the following limitations.

- Network recovery is not supported. You cannot use client drive redirection after network reconnection unless you disconnect the session and connect again.
- You can use the client drive redirection feature with only one remote session at a time. Multiple remote sessions are not supported.
- You cannot change properties for shared folders or files in the remote desktop.

Prerequisites

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

Procedure

1. Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and turn on the **Enable Folder Sharing** option in the Settings window.
2. To select a specific folder or drive to share, click **Select**, click **Add**, browse to and select the folder or drive, and click **OK**.

   You can add multiple folders and drives, but you can select only one item at a time. You can remove a folder or drive by clicking the **X** next to its name in the Folder Sharing dialog box.
3. To save the settings, click **OK**.

   The folder sharing settings apply to all remote desktops and published applications.

Results

In a remote desktop, a network location appears for each folder and drive that you shared. For example, if you shared a folder named `test1`, the `test1(Z:)` network location might appear in the remote desktop. A device also appears for each shared folder and drive. The device name format is *`folder`* `on Horizon`, for example, `test1 on Horizon`.

In a published application, you can select **File > Open** or **File > Save As**, if applicable, and navigate to the shared folder or drive.

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.

To use this feature, an administrator must enable the VMware Integrated Printing feature for the remote desktop or published application.

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.

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*). By default, 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 Multiple Monitors

You can use up to two monitors with remote desktops.

If you are not connected to a remote desktop, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and turn on the **Use Multi Monitors if there are two monitors** option in the **Settings** window. If you have two monitors and you connect to a remote desktop, the multiple-monitor feature is used. If you have only a single monitor, or more than two monitors, single-monitor mode is used. If you switch to another remote desktop, it opens in multiple-monitor mode and the previous remote desktop reverts back to single-monitor mode.

If you are already connected to a remote desktop, you can enable the multiple-monitor feature by turning on the **Use Multi Monitors if there are two monitors** option in the **Settings** window.

The multiple-monitor feature has the following limitations.

- It is not supported for published applications.
- It is not supported if Unified Desktop mode is enabled for the client device.

For information about how to disable Unified Desktop mode, see the Google Chrome documentation.

An administrator can disable the multiple-monitor feature.

Use Full-Screen Mode

You can display a remote desktop in full-screen mode.

Prerequisites

Connect to the remote desktop.

Procedure

- To display the remote desktop in full-screen mode, point to the top of the remote desktop window until the menu bar appears and click the **Fullscreen** button.
- To exit from full-screen mode, point to the top of the remote desktop window until the menu bar appears and click the **Quit fullscreen** button.

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.

If DPI synchronization is disabled, display scaling is used. The Display Scaling feature scales the remote desktop or published application appropriately.

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.

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

With the Real-Time Audio-Video feature, you can use the client machine'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, and it supports standard webcams, audio USB devices, and analog audio input.

The default video resolution is 320 x 240 pixels. The default Real-Time Audio-Video settings work well with most webcam and audio applications.

When a remote desktop or published application is connected to the client machine's webcam or microphone, before the remote desktop or published application can use to the webcam or microphone, Chrome asks for permission the first time. If you allow the device to be used, Chrome does not ask for permission again.

If Real-Time Audio-Video is being used in a remote desktop or published application session and you open a connection to a second remote desktop or published application, and if a security warning appears (for example, if a valid certificate was not installed), ignoring the warning and continuing to connect to the second remote desktop or published application causes Real-Time Audio-Video to stop working in the first session.

Select a Preferred Webcam or Microphone on a Chromebook

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

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.

Prerequisites

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

Procedure

1. Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and scroll down to the Real-Time Audio-Video settings.
2. From the **Preferred microphone** drop-down menu, select a preferred microphone.
3. From the **Preferred webcam** drop-down menu, select a preferred webcam.

Results

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

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. Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window, scroll down to the **Multi-Launch** setting, and click **Set**.

   Alternatively, if you previously started a remote desktop or published application, you can click the **Open Menu** button in the sidebar, click **Settings**, and scroll down to the **Multi-Launch** setting. If no published applications are available to use in multi-session mode, the **Multi-Launch** setting is dimmed.
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.

Shortcut Key Combinations

Some key combinations cannot be sent to a remote desktop or published application, regardless of the language that you use.

Chrome allows some key presses and key combinations to be sent to both the client system and the destination system. For other keys and key combinations, the input is processed only locally and is not sent to the destination system.

The following keys and keyboard combinations often do not work in remote desktops.

- Ctrl+T
- Ctrl+W
- Ctrl+N
- Command key
- Alt+Enter

- Ctrl+Alt+*any_key*

  Important To input Ctrl+Alt+Del, use the **Send Ctrl+Alt+Delete** toolbar button at the top of the sidebar.

- Caps Lock+*modifier_key* (such as Alt or Shift)
- Function keys on a Chromebook
- Windows key combinations

If you enable the Windows key for remote desktops, the following Windows key combinations work in remote desktops. To enable this key, click the **Open Settings Window** toolbar button in the sidebar and turn on **Enable Windows Key for Desktops**.

After you turn on the **Enable Windows Key for Desktops**, you must press Ctrl+Search to simulate pressing the Windows key.

These key combinations do not work for published applications. These key combinations do work for Windows Server 2012 R2 and Windows Server 2016 remote desktops and published desktops.

Some key combinations that work in remote desktops that have a Windows 8.x or Windows Server 2012 R2 operating system do not work in remote desktops that have a Windows 7 or Windows 10 operating system.

Table 3-1. Windows Key Shortcuts for Windows 10 Remote Desktops and Windows Server 2016 Remote Desktops

Keys	Action	Limitations
Win	Open or close Start.	
Win+A	Open Action center.	
Win+E	Open File Explorer.	
Win+G	Open game bar when a game is open.	
Win+H	Open the Share charm.	
Win+I	Open the Settings charm.	
Win+K	Open the Connection quick action.	
Win+M	Minimize all windows.	
Win+R	Open the Run dialog box.	
Win+S	Open Search.	
Win+X	Open the **Quick Link** menu.	
Win+, (comma)	Temporarily peek at the remote desktop.	
Win+Shift+M	Restore minimized windows on the remote desktop.	
Win+Enter	Open Narrator.	

Table 3-2. Windows Key Shortcuts for Windows 8.x and Windows Server 2012 R2 Remote Desktops

Keys	Action	Limitations
Win+F1	Open Windows Help and Support.	
Win	Show or hide the Start window.	
Win+B	Set focus on the notification area.	
Win+C	Open the Charms panel.	
Win+D	Show and hide the remote desktop.	
Win+E	Open File Explorer.	
Win+H	Open the Share charm.	
Win+I	Open the Settings charm.	
Win+K	Open the Devices charm.	
Win+M	Minimize all windows.	
Win+Q	To search everywhere or within the open app, if the app supports app search, open the Search charm.	
Win+R	Open the Run dialog box.	
Win+S	To search Windows and the Web, open the Search charm.	
Win+X	Open the **Quick Link** menu.	
Win+Z	Show the commands available in the app.	
Win+, (comma)	Temporarily show the remote desktop, as long as you continue pressing the keys.	Does not work on Windows 2012 R2 operating systems.
Win+Shift+M	Restore minimized windows on the remote desktop.	
Win+Home	Minimize all but the active remote desktop window (restores all windows when you press Win+Home a second time).	
Win+Enter	Open Narrator.	

Table 3-3. Windows Key Shortcuts for Windows 7 Remote Desktops

Keys	Action	Limitations
Win	Open or close the **Start** menu.	
Win+D	Show and hide the remote desktop.	
Win+M	Minimize all windows.	
Win+E	Open the `Computer` folder.	
Win+R	Open the Run dialog box.	
Win+Home	Minimize all but the active remote desktop window.	
Win+G	Cycle through running remote desktop gadgets.	
Win+U	Open the Ease of Access Center.	

Adjusting the Sound in Remote Desktops and Published Applications

By default, sound playback is enabled for remote desktops and published applications. A Horizon administrator can set a policy to disable sound playback. Some limitations apply to sound playback in remote desktops and published applications.

- To turn up the volume, use the sound control on the client system, not the sound control in the remote desktop.
- Occasionally, the sound might go out of sync with the video.
- In conditions of heavy network traffic, or if the browser is performing many tasks, sound quality might be reduced.

Troubleshooting Horizon Client 4

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

This chapter includes the following topics:

Restart a Remote Desktop

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

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

Procedure

- Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, open the Session Management Center, select the remote desktop session, and click **Restart**.

  You can also open the Session Management Center by right-clicking the remote desktop icon in the shelf and clicking **Session Management Center**.

  Note A remote desktop session does not appear in the Session Management Center unless you connect to and then disconnect from the remote desktop.

Results

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.

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 a published application quits the application without saving any unsaved data. You can reset all running published applications, or you can reset specific published application sessions.

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

Procedure

1. To reset all running published applications, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, scroll down to **Reset all your running applications**, and click **Reset**.
2. To reset a published application session, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, open the Session Management Center, select the **Remote Apps** button for the application session, and click **Terminate**.

   You can also open the Session Management Center by right-clicking the published application icon in the shelf and clicking **Session Management Center**.
3. To reset a remote desktop, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen, open the Session Management Center, select the remote desktop session, and click **Reset**.

   You can also open the Session Management Center by right-clicking the published application icon in the shelf and clicking **Session Management Center**.

Results

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

What to do next

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

Uninstall Horizon Client for Chrome

To uninstall the VMware Horizon Client for Chrome app, you remove it in the same way that you remove other Chromebook apps.

Procedure

1. Log in to the Chromebook.
2. Right-click the VMware Horizon Client app and select **Uninstall**.

What to do next

To reinstall the VMware Horizon Client for Chrome app, see the *VMware Horizon Client for Chrome Installation and Setup Guide* document.

Enable Log Collection

When you enable log collection, Horizon Client collects log information that can help VMware troubleshoot problems with Horizon Client.

You cannot enable log collection after you connect to a remote desktop or published application.

Prerequisites

Connect to a server.

Procedure

1. Click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window.
2. To enable log collection, turn on the **Enable Collect Log** option in the **Settings** window and select the **Basic**, **Debug**, or **Trace** log level.

   The path to the log file appears under the **Enable Collect Log** option in the **Settings** window.
3. To change the log file path, click the default path, browse to and select a folder in which to save the log file, and click **Save**.

   The new path appears under the **Enable Collect Log** option in the **Settings** window.
4. To close the **Settings** window, click **Close**.

Results

Horizon Client collects and saves logging information continuously until you quit Horizon Client.