

# VMware Horizon HTML Access User Guide

Modified on 29 MAY 2018

VMware Horizon HTML Access 4.8



vmware®

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

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

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2013–2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

<b>1</b>	<b>VMware Horizon HTML Access User Guide</b>	<b>4</b>
<b>2</b>	<b>How Do I Log In?</b>	<b>5</b>
<b>3</b>	<b>Connecting to Remote Desktops and Published Applications</b>	<b>6</b>
	Connect to a Remote Desktop or Application	6
	Trust a Self-Signed Root Certificate	7
	Use Unauthenticated Access to Connect to Published Applications	8
	Log Off or Disconnect	9
<b>4</b>	<b>Using Remote Desktops and Published Applications</b>	<b>11</b>
	Shortcut Key Combinations	11
	Allowing H.264 Decoding	15
	Setting the Time Zone	15
	Using the Sidebar	16
	Copying and Pasting Text	19
	Use the Copy and Paste Feature	19
	Transferring Files Between the Client and a Remote Desktop	21
	Download Files from a Desktop to the Client	21
	Upload Files from the Client to a Desktop	22
	Using DPI Synchronization	22
	Using the Session Collaboration Feature	23
	Invite a User to Join a Remote Desktop Session	23
	Manage a Collaborative Session	25
	Join a Collaborative Session	25
<b>5</b>	<b>Using External Devices</b>	<b>27</b>
	International Keyboards	27
	Screen Resolution	28
	Use Multiple Monitors	28
	Sound	29
	Using the Real-Time Audio-Video Feature for Webcams and Microphones	29
<b>6</b>	<b>Troubleshooting Horizon Client</b>	<b>31</b>
	Restart a Remote Desktop	31
	Reset a Remote Desktop or Published Applications	32
	Connect to a Server in Workspace ONE Mode	33

# VMware Horizon HTML Access User Guide

1

This document, *VMware Horizon HTML Access User Guide*, explains how to use VMware Horizon® HTML Access™ to connect to and use remote desktops and applications without having to install any software on your client system.

Use HTML Access to access your remote desktops or applications when you are using a client device that does not or cannot have Horizon Client software installed on its operating system. The Horizon Client software offers more features and better performance.

The following Web browsers are supported for HTML Access 4.8:

- Chrome 65 and 66
- Chrome 65 or later for Android device
- Internet Explorer 11
- Safari 11
- Safari on mobile device iOS 10 and iOS 11
- Firefox 59 and 60
- Microsoft Edge 41 and 42

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

## How Do I Log In?

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 automatically connects to the correct server and selects the correct domain for you.

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

When you are ready to log in and get started, see [Connect to a Remote Desktop or Application](#).

# 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:

- [Connect to a Remote Desktop or Application](#)
- [Trust a Self-Signed Root Certificate](#)
- [Use Unauthenticated Access to Connect to Published Applications](#)
- [Log Off or Disconnect](#)

## Connect to a Remote Desktop or Application

Use your Active Directory credentials to connect to the remote desktops and applications that you are authorized to use.

### Prerequisites

- Obtain login credentials, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication user name and passcode.
- Obtain the NETBIOS domain name for logging in. For example, you might use `mycompany` rather than `mycompany.com`.

### Procedure

- 1 In the Login dialog box, if you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode, and click **Login**.

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

- 2 If you are prompted a second time for RSA SecurID credentials 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 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.

- 3 In the Login dialog box, enter your login credentials.
  - a In the Username text box, enter your valid Active Directory user name in either *username*, *domain\username*, or *username@domain* format.

If the Domain text box is disabled, you must use either the *domain\username* or *username@domain* format.
  - b Enter your password.
  - c (Optional) If the Domain text box is enabled, select a domain name, if it is not already correctly populated.

---

**Note** To cancel the login process, click **Cancel** before the login process finishes.

---

- 4 (Optional) On the desktop and application selection screen, before you select the item you want to access, to mark a remote desktop or application as a favorite, click the gray star inside the icon for the desktop or 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 display only favorites.

- 5 Click the icon for the remote desktop or application that you want to access.

The remote desktop or application is displayed in your browser. A navigation sidebar is also available. You can click the tab at the left side of the browser window to display the sidebar. You can use the sidebar to access other remote desktops or applications, display the Settings window, copy and paste text, and more.

#### What to do next

If, soon after connecting to a desktop or application, you get disconnected and see a prompt asking you to click a link to accept the security certificate, you can select whether to trust the certificate. See [Trust a Self-Signed Root Certificate](#).

## Trust a Self-Signed Root Certificate

Sometimes, when connecting to a remote desktop or 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.

Most browsers give you the option to trust the self-signed certificate permanently. If you do trust the certificate permanently, you must verify the certificate every time you restart your browser. If you are using a Safari browser, you must trust the security certificate permanently to establish the connection.

**Procedure**

- 1 If the browser presents an untrusted certificate warning, or a warning 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.

Each browser has its own browser-specific prompts for accepting or always trusting a certificate. For example, in a Chrome browser, you can click the **Advanced** link on the browser page, and click **Proceed to server-name (unsafe)**.

In a Safari browser, use the following procedure to trust the certificate permanently.

- a Click the **Show Certificate** button when the untrusted certificate dialog box appears.
- b Select the **Always Trust** check box and click **Continue**.
- c When prompted, provide your password and click **Update Settings**.

The remote desktop or published application starts.

## Use Unauthenticated Access to Connect to Published Applications

A Horizon administrator can use the Unauthenticated Access feature to create Unauthenticated Access users and entitle those users to published applications on a Connection Server instance. Unauthenticated Access users can log in to the server anonymously to connect to their 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 To connect to the Connection Server instance on which you have unauthenticated access to published applications, open a browser and use one of the following URI syntaxes.
  - `https://authority-part?unauthenticatedAccessEnabled=true`



- `https://authority-part?unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_account`

*authority-part* specifies the server address and, optionally, a non-default port number. Server names must conform to a DNS syntax. To specify a port number, use the following syntax: *server-address:port-number*. *anonymous\_account* is the Unauthenticated Access user account created for logging in anonymously.

Connections to Connection Server always use TLS. The default port for TLS connections is 443. If Connection Server is not configured to use the default port, use the format shown in this example: **horizon.company.com:1443**.

- 2 (Optional) If you did not specify the `unauthenticatedAccessAccount` query, select an Unauthenticated Access user account from the **User account** drop-down menu, if necessary, and click **Submit**.

If only one Unauthenticated Access user account is available, the user account is selected by default.

The application selection window appears.

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

The published application appears in your browser. A navigation sidebar is also available. You can click the tab at the left side of the browser to show the sidebar. You can use the sidebar to access other published applications, show the **Settings** window, copy and paste text, and more.

---

**Note** You cannot reconnect to unauthenticated application sessions. When you disconnect from the client, the RDS host logs off the local user session automatically.

---

## 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

- Log out of the server and disconnect from (but do not log out from) the remote desktop or quit the published application.

Option	Action
From the desktop and application selector window, before connecting to a remote desktop or published application	Click the <b>Log Out</b> toolbar button in the upper-right corner of the window.
From the sidebar when connected to a remote desktop or published application	Click the <b>Log out</b> toolbar button at the top of the sidebar.

- Close a published application.

Option	Action
From within the published application	Quit the published application in the usual manner, for example, click the <b>X</b> (Close) button in the corner of the published application window.
From the sidebar	Click the <b>X</b> next to the published application name in the <b>Running</b> list in the sidebar.

- Log off or disconnect from a remote desktop.

Option	Action
From within the remote desktop	To log off, use the Windows <b>Start</b> menu to log off.
From the sidebar	<p>To log off and disconnect, click the <b>Open Menu</b> toolbar button next to the remote desktop name in the <b>Running</b> list in the sidebar and select <b>Log Off</b>. Files that are open on the remote desktop are closed without being saved first.</p> <p>To disconnect without logging off, click the <b>Open Menu</b> toolbar button next to the remote desktop name in the <b>Running</b> list and select <b>Close</b>.</p> <p><b>Note</b> A Horizon administrator can configure the remote desktop to log off automatically when disconnected. In that case, any open applications in the remote desktop are closed.</p>

# 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:

- [Shortcut Key Combinations](#)
- [Allowing H.264 Decoding](#)
- [Setting the Time Zone](#)
- [Using the Sidebar](#)
- [Copying and Pasting Text](#)
- [Transferring Files Between the Client and a Remote Desktop](#)
- [Using DPI Synchronization](#)
- [Using the Session Collaboration Feature](#)

## Shortcut Key Combinations

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

Web browsers allow 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 key combinations that work on your system depend on the browser software, the client operating system, and the language settings.

---

**Note** If you are using a Mac, you can map the Command key to the Windows Ctrl key when you use the key combinations to select, copy, and paste text. To enable this feature, click the **Open Settings Window** toolbar button in the sidebar and turn on **Enable Command-A, Command-C, Command-V, and Command-X**. This option appears in the **Settings** window only if you are using a Mac client 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 do 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**.

---

**Important** After you turn on **Enable Windows Key for Desktops**, you must press Ctrl+Win (on Windows systems), Ctrl+Command (on Macs), or Ctrl+Search (on Chromebooks) to simulate pressing the Windows key.

---

These key combinations do not work for published applications. These key combinations do work for Windows Server 2008 R2, 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, Windows Server 2008 R2, or Windows 10 operating system.

**Table 4-1. 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 <b>Quick Link</b> menu.	

**Table 4-1. Windows Key Shortcuts for Windows 10 Remote Desktops and Windows Server 2016 Remote Desktops (Continued)**

Keys	Action	Limitations
Win+, (comma)	Temporarily peek at the remote desktop.	
Win+Pause	Display the System Properties dialog box.	There is no Pause key on Chromebooks or Macs.
Win+Shift+M	Restore minimized windows on the remote desktop.	Does not work in Safari.
Win+Alt+Num	Open the remote desktop and open the jump list for the app pinned to the taskbar in the position indicated by the number.	Does not work on a Chromebook.
Win+Enter	Open Narrator.	

**Table 4-2. Windows Key Shortcuts for Windows 8.x and Windows Server 2012 R2 Remote Desktops**

Keys	Action	Limitations
Win+F1	Open Windows Help and Support.	Does not work in Safari.
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.	Does not work in Safari. Press Command-D on a Mac.
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 <b>Quick Link</b> 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+Pause	Display the System Properties dialog box.	Chromebooks and Macs do not have a Pause key .
Win+Shift+M	Restore minimized windows on the remote desktop.	Does not work in Safari. Press Command-D on a Mac.
Win+Alt+Num	Open the remote desktop and open the jump list for the app pinned to the taskbar in the position indicated by the number.	Does not work on a Chromebook.
Win+Up Arrow	Maximize the window.	Does not work on a Chromebook.

**Table 4-2. Windows Key Shortcuts for Windows 8.x and Windows Server 2012 R2 Remote Desktops (Continued)**

Keys	Action	Limitations
Win+Down Arrow	Remove current app from the screen or minimize the remote desktop window.	Does not work on a Chromebook.
Win+Left Arrow	Maximize the app or remote desktop window to the left side of the screen.	Does not work on a Chromebook.
Win+Right Arrow	Maximize the app or remote desktop window to the right side of the screen.	Does not work on a Chromebook.
Win+Home	Minimize all but the active remote desktop window (restores all windows when you press Win+Home a second time).	Does not work in Safari browsers.
Win+Shift+Up Arrow	Stretch the remote desktop window to the top and bottom of the screen.	Does not work on a Chromebook.
Win+Shift+Down Arrow	Restore the remote desktop window vertically, while maintaining width, after pressing Win+Shift+Up to stretch the window, or minimize active remote desktop window.	Does not work on a Chromebook.
Win+Enter	Open Narrator.	

**Table 4-3. Windows Key Shortcuts for Windows 7 and Windows Server 2008 R2 Remote Desktops**

Keys	Action	Limitations
Win	Open or close the <b>Start</b> menu.	
Win+Pause	Show the System Properties dialog box.	Chromebooks and Macs do not have a Pause key.
Win+D	Show and hide the remote desktop.	Does not work in Safari. Press Command-D on a Mac.
Win+M	Minimize all windows.	
Win+E	Open the Computer folder.	
Win+R	Open the Run dialog box.	
Win+Up Arrow	Maximize the window.	Does not work on a Chromebook.
Win+Down Arrow	Minimize the window.	Does not work on a Chromebook.
Win+Left Arrow	Maximize the app or remote desktop window to the left side of the window.	Does not work on a Chromebook.
Win+Right Arrow	Maximize the app or remote desktop window to the right side of the window.	Does not work on a Chromebook.
Win+Home	Minimize all but the active remote desktop window.	Does not work in Safari.
Win+Shift+Up Arrow	Stretch the remote desktop window to the top and bottom of the screen.	Does not work on a Chromebook.
Win+G	Cycle through running remote desktop gadgets.	
Win+U	Open the Ease of Access Center.	

## Allowing H.264 Decoding

When you use a Chrome browser, you can allow H.264 decoding in the client for remote desktop and published application sessions.

When you allow H.264 decoding, the HTML Access client uses H.264 decoding if the agent supports H.264 encoding. If the agent does not support H.264 encoding, the HTML Access client uses JPEG/PNG decoding.

If you are connected to a remote desktop or published application, you can allow H.264 decoding by turning on the **Allow H.264 decoding** option in the **Settings** window, which is available from the sidebar. You must disconnect and reconnect to the remote desktop or published application for the new setting to take effect.

If you are not connected to a remote desktop or published application, you can click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window and turn on the **Allow H.264 decoding** option in the **Settings** window. The new setting takes effect for any sessions that are connected after you change the setting.

## 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 the HTML Access 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 information to use before you connect to a remote desktop or published application manually, 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 selected is saved as your preferred time zone to use when connecting to a remote desktop or published application.

If you are already connected to a remote desktop or published application, return to the desktop and application selector window to change the current time zone setting.

The **Set Time Zone Automatically** option is not available from the **Settings** window that is accessible from the sidebar.

---

**Note** When you use the Chrome browser on an Android device, if the **Set Time Zone Automatically** option is set to **true** and you change the Android system's time zone, the new time zone is not synchronized with the remote desktop automatically. This problem is a Chrome limitation on the Android system. You must restart the Android device and the Chrome browser to synchronize the selected time zone.

---

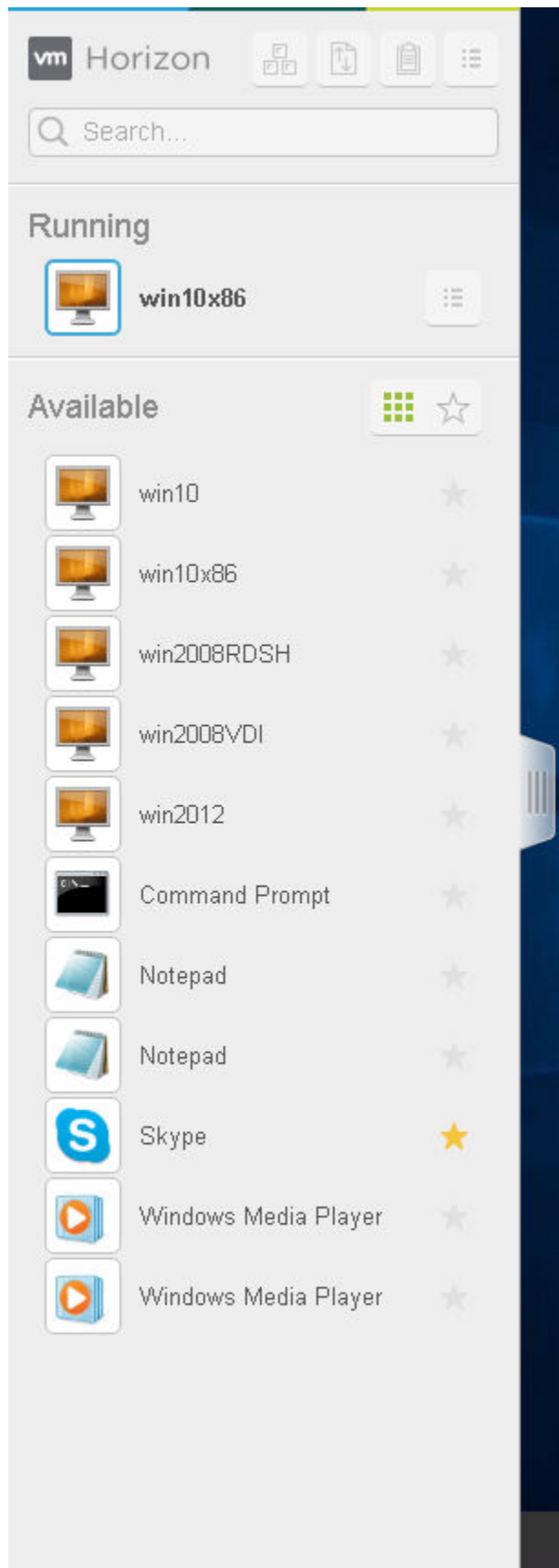
## Using the Sidebar

After you connect to a remote desktop or published application, you can use the sidebar to start other remote desktops and published applications, switch between running remote desktops and published applications, and perform other actions.

The sidebar appears on the left side of the remote desktop or published application window. To show or hide the sidebar, click the sidebar tab. You can also slide the tab up and down.



**Figure 4-1. Sidebar That Appears When You Start a Remote Desktop or Published Application**



To see the list of the documents opened by a running published application, click the expander arrow next to the published application in the **Running** list.

**Note** If you have two documents open from the same, but separate, published applications hosted on two different servers, the published application appears twice in the **Running** list in the sidebar.

You can perform many actions from the sidebar.

**Table 4-4. Sidebar Actions**

Action	Procedure
Show the sidebar	When a published application or remote desktop is open, click the sidebar tab. When the sidebar is open, you can still perform actions in the published application or remote desktop window.
Hide the sidebar	Click the sidebar tab.
Start a published application or remote desktop	Click the name of a published application or remote desktop in the <b>Available</b> list in the sidebar. Remote desktops are listed first.
Search for a published application or remote desktop	<ul style="list-style-type: none"> <li>Click in the <b>Search</b> box and begin typing the name of the published application or remote desktop.</li> <li>To start a published application or remote desktop, click its name in the search results.</li> <li>To return to the home view of the sidebar, tap the <b>X</b> in the search box.</li> </ul>
Create a list of favorite published applications and remote desktops	Click the gray star next to the name of the remote desktop or published application in the <b>Available</b> list in the sidebar. You can then click the <b>Show Favorites</b> toolbar button (star icon) next to <b>Available</b> to show a list of only favorites.
Switch between published applications or remote desktops	Click the published application or remote desktop name in the <b>Running</b> list in the sidebar.
Close a running remote desktop	<p>Click the <b>Open Menu</b> button next to the remote desktop name in the <b>Running</b> list in the sidebar and select an action.</p> <ul style="list-style-type: none"> <li>Select <b>Close</b> to disconnect from the remote desktop without logging off from its operating system. A Horizon administrator can configure a remote desktop to log off automatically when disconnected. In that case, unsaved changes in open applications are lost.</li> <li>Select <b>Log off</b> to log off from the operating system and disconnect from the remote desktop. Any unsaved changes in open applications are lost.</li> </ul>
Close a running published application	<p>Click the <b>X</b> next to the file name under the published application name in the <b>Running</b> list in the sidebar. Click the <b>X</b> next to the published application name to quit the published application and close all open files for that published application.</p> <p>You are prompted to save changes made to the files.</p>
Reset a remote desktop	Click the <b>Open Menu</b> button next to the remote desktop name in the <b>Running</b> list in the sidebar and select <b>Reset</b> . Any files that are open on the remote desktop are closed without being saved first. You can reset a remote desktop only if a Horizon administrator has enabled this feature.
Restart a remote desktop	Click the <b>Open Menu</b> button next to the remote desktop name in the <b>Running</b> list in the sidebar and select <b>Restart</b> . 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 this feature.

**Table 4-4. Sidebar Actions (Continued)**

Action	Procedure
Reset all running published applications	Click the <b>Open Menu</b> toolbar button at the top of the sidebar, click <b>Settings</b> , and click <b>Reset all your running applications</b> . All unsaved changes are lost.
Use key combinations that include the Windows key	Click the <b>Open Menu</b> toolbar button at the top of the sidebar, click <b>Settings</b> , and turn on <b>Enable Windows Key for Desktops</b> . For more information, see <a href="#">Shortcut Key Combinations</a> .
Send Ctrl+Alt+Del to current work area	Click the <b>Send Ctrl+Alt+Del</b> toolbar button at the top of the sidebar.
Disconnect from a server	Click the <b>Open Menu</b> toolbar button at the top of the sidebar and click <b>Log out</b> .
Allow H.264 decoding	(Chrome only) Click the <b>Open Menu</b> toolbar button at the top of the sidebar, click <b>Settings</b> , and turn on <b>Allow H.264 decoding</b> . For more information, see <a href="#">Allowing H.264 Decoding</a> .
Show help topics	Click the <b>Open Menu</b> toolbar button at the top of the sidebar, click <b>Settings</b> , and click <b>Help</b> . You can also click the Horizon logo at the top of the sidebar and click <b>Help</b> .
Show the About VMware Horizon Client dialog box	Click the <b>Open Menu</b> toolbar button or the Horizon logo at the top of the sidebar and click <b>About</b> . You can also click the Horizon logo at the top of the sidebar.

## Copying and Pasting Text

You can copy text to and from remote desktops and published applications. 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.

You can copy up to 1 MB of text, including any Unicode non-ASCII characters. You can copy text from the client system to a remote desktop or published application, or the reverse, but the pasted text is plain text.

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

**Note** The copy and paste feature is not supported in iOS Safari or Android devices.

## Use the Copy and Paste Feature

To copy and paste text, you must use the **Copy & Paste** button at the top of the sidebar.

This procedure describes how to use the Copy & Paste window to copy a text from your local client system to a remote application or how to copy a text from a remote application to your local client system. If, however, you are copying and pasting text between remote applications and desktops, you can simply copy and paste as you normally would, and there is no need to use the Copy & Paste window.

The Copy & Paste window, which you can open from the button at the top of the HTML Access sidebar, is required only for synchronizing the Clipboard on your local system with the Clipboard in the remote machine.

The text in the Copy & Paste window displays one of the following messages to indicate in which direction the user can copy and paste content.

- Use this panel to copy & paste content between your local client and remote desktop/application.
- Use the panel to copy & paste content from your local client to remote desktop/application.
- Use the panel to copy & paste content from your remote desktop/application to local client.

---

**Note** The default clipboard redirection group policy setting allows you to copy from client systems and paste into the remote desktop or application only. The policy setting must be enabled in both directions to be able to copy from your remote desktop or application to your client system. Contact your Horizon administrator for assistance.

---

### Prerequisites

If you are using a Mac, verify that you have enabled the setting for mapping the Command key to the Windows Ctrl key when using the key combinations to select, copy, and paste text. Click the **Open Settings Window** toolbar button in the sidebar and turn on **Enable Command-A, Command-C, Command-V, and Command-X**. (This option appears in the Settings window only if you are using a Mac.)

### Procedure

- To copy the text from your client system to the remote desktop or application:
  - a Copy the text in the local client application.
  - b In your browser, click the HTML Access sidebar tab to open the sidebar, and click **Copy & Paste** at the top of the sidebar.  
  
The Copy & Paste window appears. If previously copied text already appears in the window, that text is replaced when you paste in the newly copied text.
  - c To paste the text into the Copy & Paste window, Press Ctrl+V (or Command-V on Macs).  
  
The following message appears briefly: "Remote Clipboard Synced."
  - d Click in the remote application where you want to past the text and press Ctrl+V.  
  
The text is pasted into the remote application.
- To copy the text from your remote desktop or application to your client system:
  - a Copy the text in your remote application.
  - b In your browser, click the HTML Access sidebar tab to open the sidebar, and click **Copy & Paste** at the top of the sidebar.  
  
The Copy & Paste window appears with the text already pasted in it. The following message appears briefly: "Remote Clipboard Synced."

- c To copy the text again, click in the Copy & Paste window and press Ctrl+C (or Command-C on Macs).

The text is not selected when you do this action, and you cannot select the text. The following message appears briefly: "Copied from Clipboard Panel."

- d On your client system, click where you want to paste the text and press Ctrl+V.

The text is pasted into the application on your client system.

## Transferring Files Between the Client and a Remote Desktop

With the file transfer feature, you can transfer (upload and download) files between the client and a remote desktop. File transfer to or from published applications is not supported.

---

**Note** This feature is not available for use with remote Linux desktops, Android devices, or remote application sessions.

---

The Horizon administrator can configure the ability to allow, disallow, or allow in one direction only, the transfer of files. The default is upload only.

You can download a file up to 500 MB in size, and upload a file up to 2 GB in size. For 32-bit Internet Explorer 11, downloading a file larger than 300 MB might not work. To resolve the issue, run Internet Explorer 11 in 64-bit mode.

You cannot download or upload folders, or files that have a size of zero.

Safari on iOS and Safari 8 do not support upload or download. Safari 9 or later do not support download.

If file transfer is in progress in a desktop session and the user opens a connection to a second desktop, and if a security warning is displayed (this can happen if no valid certificate was installed, for example), ignoring the warning and continuing to connect to the second desktop will cause the file transfer in the first desktop session to abort. This is expected behavior.

---

**Note** The ability to download is affected by the group policy setting for clipboard redirection. If clipboard redirection is disabled from the server to the client, then file download is also disabled.

---

## Download Files from a Desktop to the Client

With Horizon Client you can download files from a remote desktop to the client machine.

### Procedure

- 1 Click the file transfer icon at the top of the sidebar.

The **Transfer Files** window opens.

- 2 Click **Download**.

- 3 Select one or more files on the remote desktop.

- 4 Press Ctrl+c to start the download.
- 5 After the download is complete, click the download icon to save the files on the client machine.

## Upload Files from the Client to a Desktop

With Horizon Client you can upload files from the client machine to a remote desktop.

### Procedure

- 1 Click the file transfer icon at the top of the sidebar.  
The **Transfer Files** window opens.
- 2 Click **Upload**.
- 3 Drag and drop files into the **Transfer Files** window or click **Choose Files** to select files.

The selected files are uploaded to the My Documents folder.

With Internet Explorer 11 and Chrome on ChromeBook, if you drag and drop folders, files of zero size, or files larger than 2 GB, you get an error message as expected. After you dismiss the error message, you can no longer drag and drop files that can be transferred.

## Using DPI Synchronization

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

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

The DPI Synchronization feature is enabled when the High Resolution Mode setting is disabled in the Settings window. Beginning with HTML Access version 4.5, if an administrator disables the **DPI Synchronization** agent group policy setting, the DPI Synchronization feature can be disabled, but the Display Scaling feature cannot be disabled. You must log out and log in again to make any configuration changes take effect. For information about the **DPI Synchronization** group policy setting, see the *Configuring Remote Desktop Features in Horizon 7* document.

The DPI Synchronization feature requires Windows 7 or later for single-session desktops, Windows Server 2008 R2 or later for published desktops and published applications on RDS hosts, Horizon Agent 7.0.2 or later, and HTML Access version 4.4 or later.

Following are tips for using the DPI Synchronization feature.

- If you change the DPI setting on the client system, you must log out and log in again to make Horizon Client aware of the new DPI setting on the client system. This requirement applies even if the client system is running Windows 10.

- If you start a remote session on a client system that has a DPI setting of more than 100 percent, and then use the same session on another client system that has a different DPI setting of more than 100 percent, you must log out and log back in to the remote session on the second client system to make DPI synchronization work on the second client system.
- Although Windows 10 and Windows 8.x systems support different DPI settings on different monitors, the DPI Synchronization feature uses the DPI value that is set on the client system's monitor in which the Web browser used for launching the HTML Access client session is located. HTML Access does not support different DPI settings in different monitors.
- If you want to sync up with another monitor with a different DPI setting, you must log out of the remote desktop or published application, drag the Web browser used for launching the HTML Access client session to the other monitor, 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.

## Using the Session Collaboration Feature

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

### Invite a User to Join a Remote Desktop Session

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

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

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

The Session Collaboration feature has the following limitations.

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

## Prerequisites

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

## Procedure

- 1 Connect to a remote desktop for which the session collaboration feature is enabled.

You must use the VMware Blast display protocol.

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



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

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

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

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

- 4 Select an invitation method.

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

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

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

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



## What to do next

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

## Manage a Collaborative Session

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

### Prerequisites

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

### Procedure

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

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

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

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

## Join a Collaborative Session

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

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

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

- Real-Time Audio-Video (RTAV)
- Location-based printing

- Clipboard redirection

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

### Prerequisites

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

### Procedure

- 1 Click the link in the collaboration invitation.

Horizon Client opens on the client system.

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

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

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

# Using External Devices

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

This chapter includes the following topics:

- [International Keyboards](#)
- [Screen Resolution](#)
- [Use Multiple Monitors](#)
- [Sound](#)
- [Using the Real-Time Audio-Video Feature for Webcams and Microphones](#)

## International Keyboards

When using non-English keyboards and locales, you must use certain settings in your client system, browser, and remote desktop. Some languages require you to use an IME (input method editor) on the remote desktop.

With the correct local settings and input methods installed, you can input characters for the following languages: English, Japanese, French, German, simplified Chinese, traditional Chinese, Korean, and Spanish.

**Table 5-1. Required Input Language Settings**

Language	Input Language on the Local Client System	IME Required on the Local Client System?	Browser and Input Language on the Remote Desktop	IME Required on the Remote Desktop?
English	English	No	English	No
French	French	No	French	No
German	German	No	German	No
Chinese (Simplified)	Chinese (Simplified)	English Input Mode	Chinese (Simplified)	Yes
Chinese (Traditional)	Chinese (Traditional)	English Input Mode	Chinese (Traditional)	Yes
Japanese	Japanese	English Input Mode	Japanese	Yes
Korean	Korean	English Input Mode	Korean	Yes
Spanish	Spanish	No	Spanish	No

## Screen Resolution

If the Horizon Administrator configures a remote desktop with the correct amount of video RAM, the Web client can resize a remote desktop to match the size of the browser window. The default configuration is 36MB of video RAM, which is comfortably more than minimum requirement of 16MB if you are not using 3D applications.

If you use a browser or Chrome device that has a high pixel density resolution, such as a Macbook with Retina Display or a Google Chromebook Pixel, you can set the remote desktop or application to use that resolution. Turn on the **High Resolution Mode** option in the Settings window, which is available from the sidebar. (This option only appears in the Settings window if you are using a high-resolution display or a normal display that uses a scale that is greater than 100 percent.)

## Use Multiple Monitors

By using a Chrome browser (version 55 or later), you can use multiple monitors in HTML Access Web client to display a remote desktop window.

You can add up to one additional monitor to your primary monitor to display the current remote desktop window to which you are connected. For example, if you have three monitors, you can specify that the remote desktop window appears on only two of those monitors. Adjacent monitors must be selected for the multiple-monitor setup. The monitors can be positioned side by side or stacked vertically.

Beginning with HTML Access Web client 4. 5, the per device DPI synchronization is applied when the multiple-monitor feature is enabled. If you are using two monitors that have different DPI settings, the DPI settings on the HTML Access agent are set to the same DPI setting value used by the monitor of the client machine that was used to start the HTML Access Web client session.

### Procedure

- 1 Start Horizon Client and log in to a server.
- 2 In the desktop and application selection window, click the icon for the remote desktop that you want to access.
- 3 To display the sidebar, click the sidebar tab.
- 4 Click the **Open Menu** toolbar button at the top of the sidebar, select **Display Settings**.
- 5 In the Display Settings dialog box, click **Add Display**.

---

**Note** If the Display Selector browser window does not appear, add your Horizon server's FQDN address into the Pop-up exceptions section of your browser's **Content settings** window.

---

- 6 Drag the Display Selector window so that it appears in the other monitor display that you want to use. The message in the Display Selector browser window changes and a gray rectangular icon is added.

- 7 In the Display Selector browser window, click the **+** monitor icon to confirm that you want to use the current monitor display.

The `Waiting for other displays` message appears on the current monitor display and the gray monitor icon in the Display settings window in your primary display changes to a green color.

- 8 Click **OK** in the Display Settings window when you are done adding the monitor displays that you want to use for the session.

The Display Settings window is dismissed, the `Waiting for other displays` message is cleared in the non-primary monitor display and displays the remote desktop window.

- 9 To exit the multiple displays mode, press Esc and click **Yes** in the **Exit the multiple displays mode** dialog box to confirm.

---

**Note** Each time you have to use the Esc key in the remote desktop, open the sidebar tab, click the **Open Menu** toolbar button at the top of the sidebar, and select **Send ESC**.

---

## Sound

You can play sound in remote desktops and published applications, but some limitations apply.

By default, sound playback is enabled for remote desktops and published applications, but a Horizon administrator can set a policy to disable sound playback.

The following 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. Some browsers work better than others in this regard.

## 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.

Real-Time Audio-Video is supported only in Chrome, Microsoft Edge, and Firefox. The default video resolution is 320 x 240. 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 the webcam or microphone, the browser might ask for permission. Different browsers behave differently.

- Microsoft Edge asks for permission every time. You cannot change this behavior. For more information, see <https://blogs.windows.com/msedgedev/2015/05/13/announcing-media-capture-functionality-in-microsoft-edge>.
- Firefox asks for permission every time. You can change this behavior. For more information, see <https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more?redirectlocale=en-US&redirectslug=how-do-i-manage-website-permissions>.
- Chrome asks for permission the first time. If you allow the device to be used, Chrome does not ask for permission again.

When a remote desktop is connected to the client machine's webcam or microphone, an icon for each device appears at the top of the sidebar. A red question mark appears over the device icon in the sidebar to indicate the permission request. If you allow a device to be used, the red question mark disappears. If you reject a permission request, the device icon disappears.

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.

# Troubleshooting Horizon Client

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](#)
- [Reset a Remote Desktop or Published Applications](#)
- [Connect 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.

### Prerequisites

Obtain login credentials, such as an Active Directory user name and password, RSA SecurID user name and password, or RADIUS authentication user name and password.

### Procedure

- ◆ Use the **Restart** command.

Option	Action
From the sidebar	When connected to a remote desktop, click the <b>Open Menu</b> toolbar button next to the remote desktop name in the <b>Running</b> list in the sidebar and select <b>Restart</b> .
Using a URI	To restart a desktop, use the URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&amp;action=restart</code> .

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

### What to do next

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

If restarting the remote desktop does not solve the problem, you might need to reset the remote desktop. See [Reset a Remote Desktop or Published Applications](#).

## Reset a Remote Desktop or Published Applications

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

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

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

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

### Procedure

- ◆ Use the **Reset** command.

Option	Action
<b>Reset published applications from the application selector window</b>	From the desktop and application selector window, before connecting to a remote desktop or published application, to reset all running published applications, click the <b>Settings</b> toolbar button in the upper-right corner of the screen, and click <b>Reset</b> .
<b>Reset a remote desktop from the sidebar</b>	When connected to a remote desktop, click the <b>Open Menu</b> toolbar button next to the desktop name in the <b>Running</b> list in the sidebar and select <b>Reset</b> .
<b>Reset published applications from the sidebar</b>	To reset all running applications, click the <b>Open Settings Window</b> toolbar button at the top of the sidebar, and click <b>Reset</b> .
<b>Reset a remote desktop using an URI</b>	To reset a remote desktop, use the URI <code>https://ConnectionServerFQDN?desktopId=desktop_name&amp;action=reset</code> .

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.



## Connect to a Server in Workspace ONE Mode

Beginning with Horizon 7 version 7.2, a Horizon administrator can enable the Workspace ONE mode on a Connection Server instance.

When the Workspace ONE mode is enabled, you can connect to the server only through Workspace ONE Web Portal. You are redirected to the Workspace ONE Web Portal when you try to connect to the server through HTML Access. After you connect to the server through Workspace ONE Web Portal, you can start remote desktops and published applications only through Workspace ONE Web Portal.

The sidebar does not display all the entitlements when the Workspace ONE mode is enabled. It displays only the currently running desktop and published applications.

You might encounter the following problems when the Workspace ONE mode is enabled.

- You cannot connect to the server through HTML Access. You might not reach the server, or you might see a message that states that the server expects to receive your login credentials from another application or server.
- After you start a remote desktop or published application through Workspace ONE Web Portal, you cannot see or start your remote desktops or published applications in HTML Access.