VMware Horizon HTML Access Installation and Setup Guide

VMware Horizon HTML Access 2106

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 HTML Access Installation and Setup Guide

This guide describes how to install, configure, and use the VMware Horizon® HTML Access™ software to connect to remote desktops and published applications. HTML Access is a good alternative when Horizon Client software is not installed on the client system.

Note Horizon Client offers more features and better performance than HTML Access. For example, with HTML Access, some key combinations do not work in the remote desktop, but these key combinations do work with Horizon Client.

This document includes system requirements and instructions for installing HTML Access software on a Connection Server instance and on a virtual desktop or Microsoft Remote Desktop Services (RDS) host.

This information is intended for administrators who are familiar with VMware Horizon and VMware vSphere. If you are a novice user, you might need to refer to the step-by-step instructions for basic procedures in the *Horizon Installation* and *Horizon Administration* documents

Setup and Installation

1

Setting up a VMware Horizon deployment for HTML Access involves installing the HTML Access component in Connection Server and allowing inbound traffic on certain TCP ports.

End users access their remote desktops and published applications by opening a supported browser and entering the URL for a server. When an end user connects to a server, the VMware Horizon Web portal page appears. You can configure the appearance of the VMware Horizon Web Portal page, and you can set group policies to control image quality, the ports used, and other settings.

This chapter includes the following topics:

System Requirements for HTML Access

With HTML Access, the client system does not require any software other than a supported browser. The VMware Horizon deployment must meet certain software requirements.

Browsers on the client system

Browser	Version
Chrome	90, 91
Internet Explorer	11
Safari	13, 14
Firefox	88, 89
Microsoft Edge	44, 90, 91
Note Supported only on Windows clients.	
VMware Workspace ONE Web	The latest version in the Apple App Store (iOS devices) or Google Play Store (Android devices).

Note

- On an Android device, Chrome does not support the Windows key, multiple monitors, copy and paste to the system, file transfer, printing, H.264 decoding, credential cleanup, and an external mouse. The Del, Ctrl+A, Ctrl+C, Ctrl+V, Ctrl+X, Ctrl+Y, Ctrl+Z key combinations do not work on the software keyboard.
- On a mobile device, Safari does not support an external mouse, the Windows key, multiple monitors, copy and paste to the system, file transfer, printing, H.264 decoding, credential cleanup, and Real-Time Audio-Video.

Client operating systems

Operating System	Version
Windows	10 (32-bit and 64-bit)
macOS	11 (Big Sur) 10.15.x (Catalina) 10.14.x (Mojave) 10.13.x (High Sierra)
iOS	10 or later
Android	7 or later

Remote desktops

HTML Access supports all the desktop operating systems that Horizon Agent supports.

Pool settings

HTML Access requires certain pool settings.

- The **Max resolution of any one monitor** setting must be **1920x1200** or higher so that the remote desktop has at least 17.63 MB of video RAM.
- If you use 3D applications, or if end users use a MacBook with Retina Display or a Google Chromebook Pixel, see Setting the Screen Resolution.

Connection Server

Install the HTML Access component in Connection Server. For more information, see Preparing Connection Server.

Third-party firewalls

Add rules to allow the following traffic:

- For servers, allow inbound traffic to TCP port 8443.
- For virtual desktop machines, allow inbound traffic (from servers) to TCP port 22443.

When you install the HTML Access component in Connection Server, the **VMware Horizon View Connection Server (Blast-In)** rule is enabled in the Windows Firewall. This rule configures the firewall to allow inbound traffic to TCP port 8443 automatically.

Display protocols

VMware Blast

When you use a web browser to access a remote desktop, the VMware Blast display protocol is used rather than PCoIP or Microsoft RDP. VMware Blast uses HTTPS (HTTP over SSL/TLS).

Preparing Connection Server

Before end users can connect to a server and access a remote desktop or published application, a Horizon administrator must install and configure Connection Server.

Install the HTML Access Component in Connection Server

Install Connection Server with the **Install HTML Access** setting selected on the server, or servers, that comprise a Connection Server replicated group. This setting installs the HTML Access component. This setting is selected in the installer by default. For more information, see the *Horizon Installation* document.

Configure the Blast External URL

After the servers are installed, the **Blast Secure Gateway** setting is enabled on the applicable Connection Server instances in Horizon Console. Also, the **Blast External URL** setting is configured to use the Blast Secure Gateway on the applicable Connection Server instances.

By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach the Connection Server host.

For more information, see "Set the External URLs for Horizon Connection Server Instances," in the *Horizon Installation* document.

Configure Firewall Rules

If you use third-party firewalls, configure rules to allow inbound traffic to TCP port 8443 for all Connection Server hosts in a replicated group, and configure a rule to allow inbound traffic (from servers) to TCP port 22443 on remote desktop virtual machines and RDS hosts in the data center.

For more information, see Firewall Rules for Client Web Browser Access.

Configure User Authentication

Use the following check list when setting up user authentication.

- Verify that each Connection Server instance has a TLS certificate that can be fully verified by using the host name that you enter in the web browser. For more information, see the *Horizon Installation* document.
- To use two-factor authentication, such as RSA SecurID or RADIUS authentication, verify that this feature is enabled on Connection Server. You can customize the labels on the RADIUS authentication login page. You can configure two-factor authentication to occur after a remote session times out. For more information, see the topics about two-factor authentication in the *Horizon Administration* document.
- To hide the **Domain** drop-down menu in HTML Access, enable the **Hide domain list in client user interface** global setting. This setting is enabled by default. For more information, see the *Horizon Administration* document.
- To send the domain list to HTML Access, enable the **Send domain list** global setting. This setting is disabled by default. For more information, see the *Horizon Administration* document.
- To provide unauthenticated access to published applications, enable this feature in Connection Server. For more information, see the *Horizon Administration* document.

The following table shows how the **Send domain list** and **Hide domain list in client user interface** global settings determine how users can log in to the server from HTML Access.

Send domain list setting	Hide domain list in client user interface setting	How users log in
Disabled (default)	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ *domain\username* ■ *username@domain.com*
Disabled (default)	Disabled	If a default domain is configured on the client, the default domain appears in the **Domain** drop-down menu. If the client does not know a default domain, `*DefaultDomain*` appears in the **Domain** drop-down menu. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ *domain\username* ■ *username@domain.com*
Enabled	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ *domain\username* ■ *username@domain.com*
Enabled	Disabled	Users can enter a user name in the **User name** text box and then select a domain from the **Domain** drop-down menu. Alternatively, users can enter one of the following values in the **User name** text box. ■ *domain\username* ■ *username@domain.com*

Use HTML Access with VMware Workspace ONE

You can optionally use HTML Access with VMware Workspace ONE. For information about installing Workspace ONE and configuring it for use with Connection Server, see the Workspace ONE documentation.

For information about pairing Connection Server with a SAML Authentication server, see the *Horizon Administration* document.

Firewall Rules for Client Web Browser Access

To allow client web browsers to make connections to Connection Server instances, remote desktops, and published applications, your firewalls must allow inbound traffic on certain TCP ports.

HTML Access connections must use HTTPS. HTTP connections are not allowed.

By default, when you install a Connection Server instance, the **VMware Horizon View Connection Server (Blast-In)** rule is enabled in the Windows Firewall and the firewall is configured to allow inbound traffic to TCP port 8443.

Table 1-1. Firewall Rules for Client Browser Access

Source	Default Source Port	Protocol	Target	Default Target Port	Notes
Client web browser	TCP Any	HTTPS	Connection Server instance	TCP 443	To make the initial connection, the web browser on a client device connects to a Connection Server instance on TCP port 443.
Client web browser	TCP Any	HTTPS	Blast Secure Gateway	TCP 8443	After the initial connection is made, the web browser on a client device connects to the Blast Secure Gateway on TCP port 8443. The Blast Secure Gateway must be enabled on a Connection Server instance to allow this second connection to take place.
Blast Secure Gateway	TCP Any	HTTPS	HTML Access Agent	TCP 22443	If the Blast Secure Gateway is enabled, after the user selects a remote desktop or published application, the Blast Secure Gateway connects to the HTML Access Agent on TCP port 22443 on the remote desktop virtual machine or RDS host. This agent component is included when you install Horizon Agent.
Client web browser	TCP Any	HTTPS	HTML Access Agent	TCP 22443	If the Blast Secure Gateway is not enabled, after the user selects a remote desktop or published application, the web browser on a client device makes a direct connection to the HTML Access Agent on TCP port 22443 on the remote desktop virtual machine or RDS host. This agent component is included when you install Horizon Agent.

Configure VMware Horizon to Remove Credentials From Cache

You can configure VMware Horizon to remove a user's credentials from cache when a user closes a tab that connects to a remote desktop or published application, or closes a tab that connects to the desktop and application selection window.

When this feature is disabled (the default setting), the credentials remain in cache.

When you enable this feature, the credentials are also removed from cache when a user refreshes the desktop and application selection page or the remote session page, or runs a URI command in the tab that contains the remote session. If the server presents a self-signed certificate, the credentials are removed from cache after a user starts a remote desktop or published application and accepts the certificate when the security warning appears.

Enabling this feature also affects how HTML Access behaves when it is launched from Workspace ONE. For more information, see the Workspace ONE documentation.

Procedure

1 In Horizon Console, select **Settings > Global Settings**, click the **General Settings** tab, and click **Edit**.

2 Select the **Clean Up Credential When Tab Closed for HTML Access** check box.

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

Results

Your changes take effect immediately. You do not need to restart Connection Server.

System Requirements for the Session Collaboration Feature

With the Session Collaboration feature, users can invite other users to join an existing remote desktop session. To support the Session Collaboration feature, your Horizon deployment must meet certain requirements.

Session collaborators

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

Windows remote desktops

The Session Collaboration feature must be enabled at the desktop pool or farm level. For information about enabling the Session Collaboration feature for desktop pools, see the *Setting Up Virtual Desktops in Horizon* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon* document.

You can use Horizon Agent group policy settings to configure the Session Collaboration feature. For information, see the *Configuring Remote Desktop Features in Horizon* document.

Linux remote desktops

For Linux remote desktop requirements, see the *Setting Up Linux Desktops in Horizon* document.

Connection Server

The Session Collaboration feature requires that the Connection Server instance uses an Enterprise license.

Display protocols

VMware Blast

The Session Collaboration feature does not support published application sessions.

Configure HTML Access Agents to Use New TLS Certificates

To comply with industry or security regulations, you can replace the default TLS certificates that the HTML Access Agent generates with certificates that a Certificate Authority (CA) signs.

When you install the HTML Access Agent on a remote desktop, the HTML Access Agent service creates default self-signed certificates. The service presents the default certificates to browsers that use HTML Access.

Note In the guest operating system on the desktop virtual machine, this service is called the VMware Blast service.

To replace the default certificates with signed certificates that you obtain from a CA, you must import a certificate into the Windows local computer certificate store on each remote desktop. You must also set a registry value that allows the HTML Access Agent to use the new certificate.

If you replace the default HTML Access Agent certificates with CA-signed certificates, configure a unique certificate on each remote desktop. Do not configure a CA-signed certificate on a parent virtual machine or template that you use to create a desktop pool. That approach results in hundreds or thousands of remote desktops that have identical certificates.

Procedure

1 Add the Certificate Snap-In to MMC on a Remote Desktop

   Before you can add certificates to the Windows local computer certificate store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the remote desktops where the HTML Access Agent is installed.

2 Import a Certificate for the HTML Access Agent into the Windows Certificate Store

   To replace a default HTML Access Agent certificate with a CA-signed certificate, you must import the CA-signed certificate into the Windows local computer certificate store. Perform this procedure on each remote desktop where the HTML Access Agent is installed.

3 Import Root and Intermediate Certificates for the HTML Access Agent

   If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

4 Set the Certificate Thumbprint in the Windows Registry

   To allow the HTML Access Agent to use a CA-signed certificate that was imported into the Windows certificate store, you must configure the certificate thumbprint in a Windows registry key. You must take this step on each remote desktop on which you replace the default certificate with a CA-signed certificate.

Add the Certificate Snap-In to MMC on a Remote Desktop

Before you can add certificates to the Windows local computer certificate store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the remote desktops where the HTML Access Agent is installed.

Prerequisites

Verify that the MMC and Certificate snap-in are available on the Windows guest operating system where the HTML Access Agent is installed.

Procedure

1. On the remote desktop, click **Start** and type **`mmc.exe`**.
2. In the **MMC** window, go to **File > Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** window, select **Certificates** and click **Add**.
4. In the **Certificates snap-in** window, select **Computer account**, click **Next**, select **Local computer**, and click **Finish**.
5. In the **Add or Remove snap-in** window, click **OK**.

What to do next

Import the SSL certificate into the Windows local computer certificate store. See Import a Certificate for the HTML Access Agent into the Windows Certificate Store.

Import a Certificate for the HTML Access Agent into the Windows Certificate Store

To replace a default HTML Access Agent certificate with a CA-signed certificate, you must import the CA-signed certificate into the Windows local computer certificate store. Perform this procedure on each remote desktop where the HTML Access Agent is installed.

Prerequisites

- Verify that the HTML Access Agent is installed on the remote desktop.
- Verify that the CA-signed certificate was copied to the remote desktop.
- Verify that the Certificate snap-in was added to MMC. See Add the Certificate Snap-In to MMC on a Remote Desktop.

Procedure

1. In the MMC window on the remote desktop, expand the **Certificates (Local Computer)** node and select the **Personal** folder.
2. In the Actions pane, go to **More Actions > All Tasks > Import**.
3. In the **Certificate Import** wizard, click **Next** and browse to the location where the certificate is stored.
4. Select the certificate file and click **Open**.

   To display your certificate file type, you can select its file format from the **File name** drop-down menu.
5. Type the password for the private key that is included in the certificate file.

6 Select **Mark this key as exportable**.

7 Select **Include all extendable properties**.

8 Click **Next** and click **Finish**.

The new certificate appears in the **Certificates (Local Computer) > Personal > Certificates** folder.

9 Verify that the new certificate contains a private key.

a In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.

b In the General tab of the Certificate Information dialog box, verify that the following statement appears: `You have a private key that corresponds to this certificate`.

What to do next

If necessary, import the root certificate and intermediate certificates into the Windows certificate store. See Import Root and Intermediate Certificates for the HTML Access Agent.

Configure the appropriate registry key with the certificate thumbprint. See Set the Certificate Thumbprint in the Windows Registry.

Import Root and Intermediate Certificates for the HTML Access Agent

If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

Procedure

1 In the MMC console on the remote desktop, expand the **Certificates (Local Computer)** node and go to the **Trusted Root Certification Authorities > Certificates** folder.

- If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip this procedure.
- If your root certificate is not in this folder, proceed to step 2.

2 Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

3 In the **Certificate Import** wizard, click **Next** and browse to the location where the root CA certificate is stored.

4 Select the root CA certificate file and click **Open**.

5 Click **Next**, click **Next**, and click **Finish**.

6 If an intermediate CA signed your server certificate, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

   a Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

   b Repeat steps 3 through 6 for each intermediate certificate that must be imported.

What to do next

Configure the appropriate registry key with the certificate thumbprint. See Set the Certificate Thumbprint in the Windows Registry.

Set the Certificate Thumbprint in the Windows Registry

To allow the HTML Access Agent to use a CA-signed certificate that was imported into the Windows certificate store, you must configure the certificate thumbprint in a Windows registry key. You must take this step on each remote desktop on which you replace the default certificate with a CA-signed certificate.

Prerequisites

Verify that the CA-signed certificate is imported into the Windows certificate store. See Import a Certificate for the HTML Access Agent into the Windows Certificate Store.

Procedure

1 In the MMC window on the remote desktop where the HTML Access Agent is installed, navigate to the **Certificates (Local Computer) > Personal > Certificates** folder.

2 Double-click the CA-signed certificate that you imported into the Windows certificate store.

3 In the Certificates dialog box, click the Details tab, scroll down, and select the **Thumbprint** icon.

4 Copy the selected thumbprint to a text file.

   For example: `31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e`

   Note When you copy the thumbprint, do not to include the leading space. If you inadvertently paste the leading space with the thumbprint into the registry key (in Step 7), the certificate might not be configured successfully. This problem can occur even though the leading space is not displayed in the registry value text box.

5 Start the Windows Registry Editor on the desktop where the HTML Access Agent is installed.

6 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` registry key.

7 Modify the `SslHash` value and paste the certificate thumbprint into the text box.

8 Reboot Windows.

Results

When a user connects to a remote desktop through HTML Access, the HTML Access Agent presents the CA-signed certificate to the user's browser.

Configure HTML Access Agents to Use Specific Cipher Suites

You can configure the HTML Access Agent to use specific cipher suites instead of the default set of ciphers.

By default, the HTML Access Agent requires incoming TLS connections to use encryption based on certain ciphers that provide strong protection against network eavesdropping and forgery. You can configure an alternative list of ciphers for the HTML Access Agent to use. The set of acceptable ciphers is expressed in the OpenSSL format. To see the cipher list format, you can search for **`openssl cipher string`** in a web browser.

Procedure

1. On the desktop where the HTML Access Agent is installed, start the Windows Registry Editor.
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` registry key.
3. Add a new String (REG_SZ) value, `SslCiphers`, and paste the cipher list in the OpenSSL format into the text box.
4. To make your changes take effect, restart the VMware Blast service.

   In the Windows guest operating system, the service for the HTML Access Agent is called VMware Blast.

Results

To revert to using the default cipher list, delete the `SslCiphers` value and restart the VMware Blast service. Do not simply delete the data part of the value because the HTML Access Agent will then treat all ciphers as unacceptable, in accordance with the OpenSSL cipher list format definition.

When the HTML Access Agent starts, it writes the cipher definition in the VMware Blast service's log file. You can discover the current default cipher list by inspecting the logs when the VMware Blast service starts with no `SslCiphers` value configured in the Windows Registry.

The HTML Access Agent default cipher definition might change from one release to the next to provide improved security.

Configuring iOS to Use CA-Signed Certificates

To use HTML Access on iOS devices, you must install TLS certificates that are signed by a Certificate Authority (CA). You cannot use the default TLS certificates that Connection Server or the HTML Access Agent generate.

For information, see "Configure Horizon Client for iOS to Trust Root and Intermediate Certificates" in the *Horizon Installation* document.

Using a CA-Signed Certificate with Unified Access Gateway

If you use a Unified Access Gateway appliance, you must install a CA-signed certificate that has a Subject Alternative Name (SAN) configured.

If you use a CA-signed certificate that does not have a SAN configured, or a self-signed certificate, users receive a "Your connection is not private" error and cannot connect with HTML Access.

Note If you use a Connection Server instance, users can still connect by clicking the `Proceed to` *`ip-address`* `(unsafe)` link.

For information about installing and configuring certificates, see the *Horizon Installation* document. For information about configuring HTML Access agents to use TLS certificates, see Configure HTML Access Agents to Use New TLS Certificates.

Configuring Autoplay in Safari

When using HTML Access in Safari, users might see the `Click to enable audio` dialog box when they start a remote desktop or published application for the first time, or when they refresh the browser while using a remote desktop or published application. If users click **OK** in this dialog box, audio plays normally.

You can prevent this dialog box from appearing by configuring the autoplay policy in the browser. For example, for Safari on a Mac, select **Safari > Settings for This Website**, move the mouse to the right of **Auto-Play**, click the drop-down menu, and select **Allow All Auto-Play**.

Upgrading HTML Access

Upgrading HTML Access involves upgrading Connection Server and Horizon Agent.

When you upgrade HTML Access, make sure that the corresponding version of Connection Server is installed on all the instances in a replicated group.

When you upgrade Connection Server, HTML Access is installed or upgraded automatically.

To verify that the HTML Access component is installed, open the Uninstall a Program applet in the Windows operating system and look for HTML Access in the list.

Uninstall the HTML Access Component from Connection Server

You can remove the HTML Access component by using the same method that you use to remove other Windows software.

Procedure

1. On the Connection Server instance where HTML Access is installed, open **Uninstall a program** in the Windows Control Panel.
2. Select **VMware Horizon HTML Access** and click **Uninstall**.
3. (Optional) In the Windows Firewall for the host, verify that TCP port 8443 no longer allows inbound traffic.

What to do next

On third-party firewalls, if applicable, change the rules to disallow inbound traffic to TCP port 8443 for the Connection Server instance.

Configure Horizon Client Data Sharing

If a Horizon administrator has opted to participate in the VMware Customer Experience Improvement Program (CEIP), VMware collects and receives anonymous data from client systems through Connection Server. You can configure whether to share this client data with Connection Server.

For information about configuring Horizon to join the CEIP, see the *Horizon Administration* document.

Data sharing is enabled by default in HTML Access. You cannot change the data sharing setting after you connect to a server.

A Horizon administrator can disable data sharing in HTML Access for all users and prevent users from changing the data sharing setting in HTML Access. For more information, see Disabling Data Sharing for all HTML Access Users.

Table 1-2. Client Data Collected for the CEIP

Description	Field name	Is This Field Made Anonymous?	Example Value
Company that produced the application	`<client_vendor>`	No	VMware
Product name	`<client_product>`	No	VMware Horizon HTML Access
Client product version	`<client_version>`	No	2012-8.1.0-xxxxxxxx

Table 1-2. Client Data Collected for the CEIP (continued)

Description	Field name	Is This Field Made Anonymous?	Example Value
Client binary architecture	<client_arch>	No	Examples include the following values: ■ browser ■ arm
Native architecture of the browser	<browser_arch>	No	Examples include the following values: ■ Win32 ■ Win64 ■ MacIntel ■ iPad ■ Linux armv81 (for Android Chrome support)
Browser user agent string	<browser_user_agent>	No	Examples include the following values: ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/703.00 (KHTML, like Gecko) ■ Chrome/3.0.1750 ■ Safari/703.00 ■ Edge/13.10586
Browser's internal version string	<browser_version>	No	Examples include the following values: ■ 7.0.3 (for Safari), ■ 44.0 (for Firefox) ■ 13.10586 (for Edge)
Browser's core implementation	<browser_core>	No	Examples include the following values: ■ Chrome ■ Safari ■ Firefox ■ Internet Explorer ■ Edge
Whether the browser is running on a handheld device	<browser_is_handheld>	No	true

Procedure

1 Click **Settings** (gear icon) on the VMware Horizon Web Portal page.

2 Toggle the **Allow data sharing** option to on or off.

Disabling Data Sharing for all HTML Access Users

A Horizon administrator can disable data sharing for all HTML Access users, and prevent users from changing the **Allow data sharing** option in HTML Access, by adding the following setting to the `C:\Program Files\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\classes\portal-version.properties` file on the Connection Server instance.

```
CEIP.disabled=true
```

When this setting is set to `true`, **Settings** (gear icon) does not appear on the VMware Horizon Web Portal page.

Note This setting has no affect on Horizon Client. For information about disabling data sharing in Horizon Client, see the installation and setup guide for the Horizon Client platform.

Configuring HTML Access for End Users

2

You can change the appearance of the VMware Horizon Web Portal page, which is the web page that end users see when they enter the URL for HTML Access. You can also set group policies that control the image quality, the ports used, and other settings.

This chapter includes the following topics:

Configure the VMware Horizon Web Portal Page for End Users

You can configure the VMware Horizon Web Portal page to show or hide the icon for downloading Horizon Client, the icon for connecting to a remote desktop through HTML Access, and other links.

By default, the VMware Horizon Web Portal page shows both an icon for downloading and installing Horizon Client and an icon for connecting through HTML Access. The default values defined in the `portal-links-html-access.properties` file determine the download link that appears on the VMware Horizon Web Portal page.

Sometimes, you might want the links on the VMware Horizon Web Portal page to point to an internal web server, or you might want to make specific client versions available on your own server. You can reconfigure the VMware Horizon Web Portal page to point to a different download URL by modifying the contents of the `portal-links-html-access.properties` file. If that file is unavailable or is empty, and the `oslinks.properties` file exists, the `oslinks.properties` file is determines the link value for the installer file.

The `oslinks.properties` file is installed in the *`installation-directory`*`\VMware\VMware View\Server\broker\webapps\portal\WEB-INF` directory. If this file is missing during the HTML Access session, the download link directs users to `https://www.vmware.com/go/viewclients` by default. The file contains the following default values.

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

You can define installer links for specific client operating systems in the `portal-links-html-access.properties` file or the `oslinks.properties` file. For example, if you browse to the VMware Horizon Web Portal page from a macOS system, the link for the Horizon Client for Mac installer appears. For Linux clients, you can make separate links for 32-bit and 64-bit installers. For Chrome clients, you can substitute the link to Horizon Client for Chrome in the Chrome Web Store (https://chrome.google.com/webstore/detail/vmware-horizon-client-for/ppkfnjlimknmjoaemnpidmdlfchhehel).

Procedure

1. On the Connection Server host, use a text editor to open the `portal-links-html-access.properties` file *`CommonAppDataFolder`*`\VMware\VDM\portal\portal-links-html-access.properties` directory.

   The *CommonAppDataFolder* directory is usually in the `C:\ProgramData` directory. To show the `C:\ProgramData` folder in Windows Explorer, use the Folder Options dialog box to show hidden folders.

   If the `portal-links-html-access.properties` file does not exist, but the `oslinks.properties` file does exist, open the *<installation-directory>*`\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` file to modify the URLs to use for downloading specific installer files.

2 Edit the configuration properties.

By default, both the installer icon and the HTML Access icon are enabled and a link points to the client download page on the VMware website. To disable an icon, which removes the icon from the web page, set the property to `false`.

Note The `oslinks.properties` file can be used only to configure the links to the specific installer files.

Option	Property Setting
Disable HTML Access	`enable.webclient=false` If this option is set to false, but the `enable.download` option is set to true, the user is taken to a web page for downloading the native Horizon Client installer. If both options are set to false, the user sees the following message: `"Contact your local administrator for instructions on accessing this Connection Server."`
Disable downloading Horizon Client	`enable.download=false` If this option is set to false, but the `enable.webclient` option is set to true, the user is taken to the HTML Access login web page. If both options are set to false, the user sees the following message: `"Contact your local administrator for instructions on accessing this Connection Server."`
Change the URL of the Web page for downloading Horizon Client	`link.download=https://`*`url-of-web-server`* Use this property if you plan to create your own web page.

Option	Property Setting

Create links for specific installers	The following examples show full URLs. If you place the installer files in the `downloads` directory, which is under the `C:\Program Files\VMware\VMware View\Server\broker\webapps\` directory on the Connection Server host, you can use relative URLs as described in the next step.
	■ General link to download installer:
	`link.download=https://server/downloads`
	■ 32-bit Windows installer:
	`link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe`
	■ 64-bit Windows installer:
	`link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe`
	■ Windows Phone installer:
	`link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx`
	■ 32-bit Linux installer:
	`link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle`
	■ 64-bit Linux installer:
	`link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle`
	■ macOS installer:
	`link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg`
	■ iOS installer:
	`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa`
	■ Android installer:
	`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk`

Change the URL for the Help link in the login page	`link.help` By default, this link points to a help system hosted on the VMware website. The Help link appears at the bottom of the login page.

3 To have users download installers from a location other than the VMware website, place the installer files on the HTTP server where the installer files reside.

   This location must correspond to the URLs that you specified in the `portal-links-html-access.properties` file or in the `oslinks.properties` file from the previous step. For example, to place the files in a `downloads` directory on the Connection Server host, use the following path.

   ```
   C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
   ```

   The links to the installer files can then use relative URLs with the format `/downloads/`*`client-installer-file-name`*.

4 Restart the Horizon Web Component service.

Using URIs to Configure HTML Access Web Clients

You can use uniform resource identifiers (URIs) to create web or email links for end users. End users can click these links to start HTML Access, connect to a server, and start a remote desktop or published application with specific configuration options.

You create these links by constructing URIs that provide some or all the following information so that end users do not need to supply it.

- Server address
- Port number for the server
- Active Directory user name
- RADIUS or RSA SecurID user name, if different from the Active Directory user name
- Domain name
- Remote desktop or published application display name
- Actions, including browse, reset, log out, and start session

URI Specification

Syntax includes a path part to specify the server, and, optionally, a query to specify a user, remote desktop or published application, and actions or configuration options.

Use the following syntax to create URIs for starting HTML Access:

```
https://authority-part[/?query-part]
```

authority-part

Specifies the server address and, optionally, a non-default port number. Server names must conform to DNS syntax.

To specify a port number, use the following syntax:

```
server-address:port-number
```

query-part

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

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

Observe the following guidelines when creating the query-part:

- If you do not use at least one of the supported queries, the default VMware Horizon Web portal page appears.
- In the query part, some special characters are not supported, and you must use the URL encoding format for them, as follows: For the pound symbol (#) use **%23**, for the percent sign (%) use **%25**, for the ampersand (&) use **%26**, for the at sign (@) use **%40**, and for the backslash (\) use **%5C**.

  For more information about URL encoding, go to http://www.w3schools.com/tags/ref_urlencode.asp.
- In the query part, non-ASCII characters must first be encoded according to UTF-8 [STD63], and then each octet of the corresponding UTF-8 sequence must be percent-encoded to be represented as URI characters.

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

Supported Queries

This topic lists the queries that are supported for HTML Access. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the installation and setup document for each type of client system.

action

Table 2-1. Values That Can Be Used With the action Query

Value	Description
`browse`	Displays a list of available remote desktops and published applications hosted on the specified server. You are not required to specify a remote desktop or published application when you use this action.
`start-session`	Starts the specified remote desktop or published application. If no action query is provided and the remote desktop or published application name is provided, `start-session` is the default action.

Table 2-1. Values That Can Be Used With the action Query (continued)

Value	Description
`reset`	Shuts down and restarts the specified remote desktop. Unsaved data is lost. Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC. This action is not valid for a published application.
`logoff`	Logs the user out of the guest operating system in the remote desktop. This action is not valid for a published application.
`restart`	Shuts down and restarts the primary remote desktop after the user confirms the restart operation request. This action is not valid for a published application.

applicationId

The published application display name. The display name is the name specified in Horizon Console when the application pool was created. If the display name contains a space, the browser uses **`%20`** to represent the space.

args

Specifies command-line arguments to add when starting a published application. Use the syntax `args=`*value*, where *value* is a string. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**
- For a double quotation mark ("), use **`%22`**

For example, to specify the filename `"My new file.txt"` for the Notepad++ application, use **`%22My%20new%20file.txt%22`**.

desktopId

The remote desktop display name. The display name is the name specified in Horizon Console when the desktop pool was created. If the display name contains a space, the browser uses **`%20`** to represent the space.

domainName

The NETBIOS domain name associated with the user who is connecting to the remote desktop or published application. For example, use `mycompany` rather than `mycompany.com`.

tokenUserName

The RSA or RADIUS user name. Use this query only if the RSA or RADIUS user name is different from the Active Directory user name. If you do not specify this query and RSA or RADIUS authentication is required, the Windows user name is used.

userName

The Active Directory user who is connecting to the remote desktop or published application. The user name can be in one of the following formats:

- *userName*
- *domainName%5CuserName*
- user principal name (UPN), that is, *userName@domainName*

unauthenticatedAccessEnabled

If this option is set to **true**, the Unauthenticated Access feature is enabled by default. HTML Access starts and an anonymous user account appears. An example of the syntax is **unauthenticatedAccessEnabled=true**.

unauthenticatedAccessAccount

Sets the account to use if the Unauthenticated Access feature is enabled. If Unauthenticated Access is disabled, then this query is ignored. An example of the syntax using the **anonymous1** user account is **unauthenticatedAccessAccount=anonymous1**

URI Syntax Examples

Each of the following URI examples is followed by a description of what the end user sees after clicking the URI link. Queries are not case-sensitive, for example, you can use **domainName** or **domainname**.

1 `https://horizon.mycompany.com/?domainName=finance&userName=fred`

HTML Access starts and connects to the `horizon.mycompany.com` server. In the login box, the **User name** text box is populated with the name **fred**, and the **Domain** text box is populated with **finance**. The user must supply only a password.

2 `https://horizon.mycompany.com/?userName=finance%5Cfred`

HTML Access starts and connects to the `horizon.mycompany.com` server. In the login box, the **User name** text box is populated with the name **finance\fred**. The user must supply only a password.

3 `https://horizon.mycompany.com/?userName=fred@finance`

HTML Access starts and connects to the `horizon.mycompany.com` server. In the login box, the **User name** text box is populated with the name **fred@finance**. The user must supply only a password.

4 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

HTML Access starts and connects to the `horizon.mycompany.com` server. The login box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the display name **Primary Desktop** and the user is logged in to the guest operating system.

5 `https://horizon.mycompany.com/?applicationId=Notepad&action=start-session`

HTML Access starts and connects to the `horizon.mycompany.com` server. The login box prompts the user for a user name, domain name, and password. After a successful login, the Notepad application starts.

6 `https://horizon.mycompany.com:7555/?desktopId=Primary%20Desktop`

This URI has the same effect as the previous example, except that it uses the non-default port 7555 for the server. The default port is 443. Because a remote desktop identifier is provided, the remote desktop starts even though the `start-session` action is not included in the URI.

7 `https://horizon.mycompany.com/?applicationId=Primary%20Application&desktopId=Primary%20Desktop`

This URI specifies both a published application and a remote desktop. When you specify both a published application and a remote desktop, only the remote desktop starts.

8 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=reset`

HTML Access starts and connects to the `horizon.mycompany.com` server. The login box prompts the user for a user name, domain name, and password. After a successful login, the client displays a dialog box that prompts the user to confirm the reset operation for Primary Desktop.

Note This action is available only if a Horizon administrator has allowed end users to reset their machines.

9 `https://horizon.mycompany.com/?My%20Notepad++?args=%22My%20new%20file.txt%22`

Opens My Notepad++ on server `horizon.mycompany.com` and passes the argument `My new file.txt` in the application start command. The filename is enclosed in double quotes because it contains spaces.

10 `https://horizon.mycompany.com/?Notepad++%2012?args=a.txt%20b.txt`

Opens Notepad++ 12 on server `horizon.mycompany.com` and passes the argument `a.text b.txt` in the application start command. Because the argument is not enclosed in double quotes, a space separates the filenames and the two files are opened separately in Notepad++.

Note Applications can differ in the way that they use command-line arguments. For example, if you pass the argument `a.txt b.txt` to WordPad, WordPad opens only one file, `a.txt`.

11 `https://horizon.mycompany.com/?desktopId=Primary%20Desktop&action=restart`

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

Note This action is available only if a Horizon administrator has allowed end users to restart their machines.

12
```
https://horizon.mycompany.com/?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous_user1
```

HTML Access starts and connects to the `horizon.mycompany.com` server using the **`anonymous_user1`** account.

HTML Code Examples

You can use URIs to make hypertext links and buttons to include in emails or on web pages. The following examples show how to use the URI from the first URI example to code a hypertext link that reads **Test Link** and a button that reads **TestButton**.

```
<html>
<body>

<a href="https://horizon.mycompany.com/?domainName=finance&userName=fred">Test Link</a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'https://horizon.mycompany.com/?domainName=finance&userName=fred'"></form> <br>

</body>
</html>
```

HTML Access Group Policy Settings

HTML Access uses the VMware Blast protocol. You configure group policies for HTML Access by configuring group policies for the VMware Blast protocol.

For more information, see "Configuring Policies for Desktop and Application Pools" and "VMware Blast Policy Settings" in the *Configuring Remote Desktop Features in Horizon* document.

Managing Remote Desktop and Published Application Connections

3

End users can connect to a server and use remote desktops and published applications. For troubleshooting purposes, end users can reset remote desktops and published applications.

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 login credentials, such as an Active Directory user name and password, RSA SecurID user name and passcode, or RADIUS authentication credentials.
- Obtain the NETBIOS domain name for logging in. For example, you might use `mycompany` rather than `mycompany.com`.
- If you are outside the corporate network and require a VPN connection to access remote desktops and published applications, verify that the client device is set up to use a VPN connection and turn on that connection.
- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or published application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.

Procedure

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

2 Open a browser and type the server name in the navigation bar.

Type **`https`** and use the fully qualified domain name (FQDN) of the server, for example, `https://view.company.com`.

Server connections 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 **`view.company.com:1443`**.

3 When the VMware Horizon Web Portal page appears, select one of the following options.

The following table lists all the possible options. The options that are available to you depend on the server that you connect to and how your environment is configured.

Option	Description
Launch Native Client	(Unified Access Gateway only) Starts Horizon Client.
Browser Access	(Unified Access Gateway only) Starts HTML Access.
VMware Horizon HTML Access	Starts HTML Access.
Install VMware Horizon Client	Opens the VMware Horizon Clients download page, where you can download the Horizon Client installer for your client system. **Note** This option might appear as a link instead of an option.

Optionally, you can select a check box to save your selection and skip the VMware Horizon Web Portal page the next time you enter the server name in the same browser type on the same client system. If you change your mind later, you can use the **Restore default landing page** setting on the HTML Access Settings page to display the VMware Horizon Web Portal page.

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

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

5 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 that you entered previously. If necessary, wait until a new number is generated. This step is required only when you mistype the first passcode or when configuration settings in the RSA server change.

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

   a Enter the user name and password of a user who is entitled to use at least one desktop or application pool.

   b (Optional) Select a domain.

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

   c Log in.

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

   The remote desktop or published application opens in the browser window. To open the sidebar, click the tab on the left side of the browser window. From the sidebar, you can open other remote desktops or published applications, configure settings, copy and paste text, and perform other tasks.

8 (Optional) To mark a remote desktop or published application as a favorite, in the desktop and application selector window, 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 your favorite items.

What to do next

If you are disconnected after connecting to a remote desktop or published application, and a prompt appears asking 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, you can set the time zone manually. See Setting the Time Zone.

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.

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 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.

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

   In Safari, 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**.

Results

The remote desktop or published application starts.

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

- Perform the administrative tasks described in Preparing Connection Server.
- Set up Unauthenticated Access users on the Connection Server instance. For information, see "Providing Unauthenticated Access for Published Applications" in the *Horizon Administration* document.

Procedure

1 To connect to the server on which you have unauthenticated access, open a browser and enter a Uniform Resource Identifier (URI).

Use one of the following URI syntaxes.

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

authority-part is the server address and, optionally, a non-default port number. If you need to specify a port number, enter *server-address:port-number*.

anonymous_account is the Unauthenticated Access user account.

Connections 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: **`horizon.company.com:1443`**.

2 (Optional) If you did not specify an Unauthenticated Access user account in the URI, 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, that 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 on the left side of the browser window 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, you are logged off the local user session automatically.

Connect to a Server in Workspace ONE Mode

A Horizon administrator can enable Workspace ONE mode on a Connection Server instance.

When Workspace ONE mode is enabled, you can connect to the server only through the 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 the Workspace ONE Web Portal, you can start remote desktops and published applications only through the Workspace ONE Web Portal.

When Workspace ONE mode is enabled, the sidebar does not show all the remote desktops and published applications that you are entitled to use. Instead, it shows only the currently running remote desktops and published applications.

You might encounter the following problems when 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 the Workspace ONE Web Portal, you cannot see or start the remote desktop or published application in HTML Access.

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 HTML Access, 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.

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 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.

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.

H.264 is an industry standard for video compression, which is the process of converting digital video into a format that takes up less capacity when it is stored or transmitted.

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

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 **Log Out** toolbar button in the upper-right corner of the window.
From the sidebar when connected to a remote desktop or published application	Click the **Log out** 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 **X** (Close) button in the corner of the published application window.
From the sidebar	Click the **X** next to the published application name in the **Running** 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 **Start** menu to log off.
From the sidebar	To log off and disconnect, click the **Open Menu** toolbar button next to the remote desktop name in the **Running** list in the sidebar and select **Log Off**. Files that are open on the remote desktop are closed without being saved first. To disconnect without logging off, click the **Open Menu** toolbar button next to the remote desktop name in the **Running** list and select **Close**. **Note** 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.

Using a Remote Desktop or Published Application

4

HTML Access provides a familiar, personalized desktop and application environment. After you connect to a remote desktop or published application, you can use a navigation sidebar to start other remote desktops and published applications, switch between running remote desktops and published applications, and perform other actions.

You can copy and paste text and transfer files from the client device to remote desktops and published applications, print from locally attached printers in remote desktops and published applications, use the client machine's webcam and microphone in remote desktops and published applications, and share your remote desktop sessions with other users.

This chapter includes the following topics:

Feature Support Matrix

When planning which features to make available to your end users, use the following information to determine which guest operating systems support the feature when they use HTML Access. Additional features are available if end users use a natively installed Horizon Client application, such as Horizon Client for Windows.

Table 4-1. Features Supported for HTML Access to Windows Virtual Desktops

Feature	Windows 10 Desktop	Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 Desktops
RSA SecurID or RADIUS	X	X
Single sign-on	X	X
RDP display protocol		
PCoIP display protocol		
VMware Blast display protocol	X	X
USB redirection	X	X
Real-Time Audio-Video (RTAV)	X	X
Windows Media MMR		
VMware Integrated Printing	X	Windows Server 2016/2019 only
Location-based printing	X	X
Smart cards		
Multiple monitors	X	X

Feature Support for Published Desktops on RDS Hosts

RDS hosts are server computers that have Windows Remote Desktop Services and Horizon Agent installed. Multiple users can have remote desktop sessions on an RDS host simultaneously. An RDS host can be either a physical machine or a virtual machine.

Table 4-2. Features Supported for HTML Access to RDS Hosts

Feature	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019
RSA SecurID or RADIUS	X	X	X
Single sign-on	X	X	X
VMware Blast display protocol	X	X	X

Table 4-2. Features Supported for HTML Access to RDS Hosts (continued)

Feature	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019
VMware Integrated Printing		X	X
Location-based printing	X	X	X
Real-Time Audio-Video (RTAV)	X	X	X
Multiple monitors (for session-based desktops only)	X	X	X

For information about which editions of each guest operating system are supported, see the *Horizon Installation* document.

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.

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

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

Table 4-3. Sidebar Actions

Action	Procedure
Show the sidebar	When a remote desktop or published application is open, click the sidebar tab. When the sidebar is open, you can still perform actions in the remote desktop or published application window.
Hide the sidebar	Click the sidebar tab.
Start a remote desktop or published application	Click the name of a remote desktop or published application in the **Available** list in the sidebar. Remote desktops are listed first.
Search for a remote desktop or published application	■ Click in the **Search** box and begin typing the name of the remote desktop or published application. ■ To start a remote desktop or published application, click its name in the search results. ■ To return to the home view of the sidebar, tap the **X** in the search box.

Table 4-3. Sidebar Actions (continued)

Action	Procedure
Create a list of favorite remote desktops or published applications	Click the gray star next to the name of the remote desktop or published application in the **Available** list in the sidebar. You can then click the **Show Favorites** toolbar button (star icon) next to **Available** to show a list of only favorites.
Switch between remote desktops or published applications	Click the remote desktop or published application name in the **Running** list in the sidebar.
Enable multi-session mode for published applications	Click the **Open Menu** button in the sidebar, click **Settings**, and scroll down to the **Multi-Launch** setting. For more information, see Use Multiple Sessions of a Published Application From Different Client Devices.
Open the Copy & Paste panel	Click the **Copy & Paste** button at the top of the sidebar. Use this button for copying text to and from applications on your local client system. For more information, see Copying and Pasting Text. On iOS Safari, this button is not available because the copy and paste feature is not supported.
Open the File Transfer window	To download files from, or upload files to, a remote desktop or published application, click the **File Transfer** button at the top of the sidebar. For more information, see Download Files From a Remote Desktop or Published Application to the Client System and Upload Files From the Client System to a Remote Desktop or Published Application.
Enable Command-A, Command-C, Command-V, and Command-X	This option appears in the **Settings** window only if you are using a Mac. Click the **Open Menu** toolbar button at the top of the sidebar and then click **Settings**. When this feature is enabled, The Command key on the Mac is mapped to the Ctrl key on the remote Windows desktop or application. For example, pressing Command-A on a Mac keyboard is the same as pressing Ctrl+A on the remote Windows desktop or application.
Close a running remote desktop	Click the **Open Menu** button next to the remote desktop name in the **Running** list in the sidebar and select an action. ■ Select **Close** 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. ■ Select **Log off** to log off from the operating system and disconnect from the remote desktop. Any unsaved changes in open applications are lost.
Close a running published application	Click the **X** next to the file name under the published application name in the **Running** list in the sidebar. Click the **X** next to the published application name to quit the published application and close all open files for that published application. You are prompted to save changes made to the files.
Reset a remote desktop	Click the **Open Menu** button next to the remote desktop name in the **Running** list in the sidebar and select **Reset**. 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 **Open Menu** button next to the remote desktop name in the **Running** list in the sidebar and select **Restart**. 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 4-3. Sidebar Actions (continued)

Action	Procedure
Reset all running published applications	Click the **Open Menu** toolbar button at the top of the sidebar, click **Settings**, and click **Reset all your running applications**. All unsaved changes are lost.
Use key combinations that include the Windows key	Click the **Open Menu** toolbar button at the top of the sidebar, click **Settings**, and turn on **Enable Windows Key for Desktops**. For more information, see Shortcut Key Combinations.
Send Ctrl+Alt+Del to current work area	Click the **Send Ctrl+Alt+Del** toolbar button at the top of the sidebar.
Disconnect from a server	Click the **Open Menu** toolbar button at the top of the sidebar and click **Log out**.
Use high-resolution mode on machines that have a high-resolution display, such as Retina Macbook Pro	Click the **Open Menu** toolbar button at the top of the sidebar, click **Settings**, and turn on **High Resolution Mode**.
Allow H.264 decoding	(Chrome only) Click the **Open Menu** toolbar button at the top of the sidebar, click **Settings**, and turn on **Allow H.264 decoding**. For more information, see Allowing H.264 Decoding.
Use multiple monitors	(Chrome version 55 or later only) Click the **Open Menu** toolbar button at the top of the sidebar and select **Display Settings**. For more information, see Use Multiple Monitors
Call out or close the soft keyboard	(iOS Safari only) Click the keyboard icon at the top of the sidebar. You can also call out or dismiss the soft keyboard by tapping the screen with three fingers.
Show help topics	Click the **Open Menu** toolbar button at the top of the sidebar, click **Settings**, and click **Help**. You can also click the Horizon logo at the top of the sidebar and click **Help**.
Show the About VMware Horizon Client dialog box	Click the **Open Menu** toolbar button or the Horizon logo at the top of the sidebar and click **About**. You can also click the Horizon logo at the top of the sidebar.
Display a remote desktop or published application in full-screen mode	Click the **Open Menu** toolbar button at the top of the sidebar and click **Fullscreen**.
Exit from full-screen mode	Click the **Open Menu** toolbar button at the top of the sidebar and click **Quit fullscreen**.
Send Esc to a remote desktop or published application when in full-screen mode	Click the **Open Menu** toolbar button at the top of the sidebar and click **Send ESC**.
Redirect USB devices	Click the **Open Menu** toolbar button at the top of the sidebar and click **USB**. For more information, see Use USB Devices in a Remote Desktop.

Monitors and Screen Resolution

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

Use Multiple Monitors

You can use multiple monitors to display a remote desktop window.

Prerequisites

- You must use HTML Access in a Chrome or Chromium-based Edge browser. In Chrome, Chromecast must be enabled.
- You must have two or more monitors.

Procedure

1. Start HTML Access and log in to a server.
2. To enable the multiple-monitor feature, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window, turn on the **Use Multi Monitors if there are two monitors** option in the **Settings** window, and click **Close**.
3. In the desktop and application selector window, click the icon for the remote desktop that you want to use.
4. When the remote desktop prompts you to grant permission to use full screen for all screens, click **OK**.

   A pop-up menu appears that lists the available external displays.
5. From the pop-up menu, select a display to use.
6. When the remote desktop prompts you to grant permission to use full screen for all screens again, click **OK**.
7. To exit from multiple-monitor mode, press the Esc key. In a Chrome or Chromium Edge browser, press and hold the Esc. key.
8. In the **Exit the multiple displays mode** dialog box, click **Yes**.

Setting the Screen Resolution

HTML Access can resize the remote desktop to match the size of the browser window. To use this feature, a Horizon administrator must configure the remote desktop to have the correct amount of video RAM (VRAM). The default VRAM configuration is 36 MB. If you are not using 3D applications, the minimum VRAM requirement is 16 MB.

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 published application to use that resolution. Turn on the **High Resolution Mode** option in the **Settings** window, which is available from the sidebar. This option appears in the **Settings** window only if you are using a high-resolution display or a normal display that uses a scale that is greater than 100 percent.

The High Resolution Mode feature cannot change the resolution for an active remote session. You must log out and log in again to make the feature take effect.

To use the 3D rendering feature, you must allocate sufficient VRAM for each remote desktop.

- With the software-accelerated graphics feature, you can use 3D applications, such as Windows Aero themes or Google Earth. This feature requires from 64 MB to 128 MB of VRAM.
- The shared hardware-accelerated graphics feature (vSGA), which is available with vSphere 5.1 or later, enables you to use 3D applications for design, modeling, and multimedia. This feature requires from 64 MB to 512 MB of VRAM. The default is 96 MB.
- The dedicated hardware-accelerated graphics feature (vDGA), which is available with vSphere 5.5 or later, dedicates a single physical GPU (graphical processing unit on an ESXi host to a single virtual machine. Use this feature if you require high-end hardware-accelerated workstation graphics. This feature requires from 64 MB to 512 MB of VRAM. The default is 96 MB.

When 3D rendering is enabled, the maximum number of monitors is one and the maximum resolution is 3840 x 2160.

Similarly, if you use a browser on a device that has a high pixel density resolution, such as a MacBook with Retina Display or a Google Chromebook Pixel, you must allocate sufficient VRAM for each remote desktop.

Important Estimating the amount of VRAM that you need for the VMware Blast display protocol is similar to estimating how much VRAM is required for the PCoIP display protocol.

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.

Like the Display Scaling feature, the DPI Synchronization feature can improve the readability of text and icons on high-DPI displays. Unlike the Display Scaling feature, which increases the size of fonts and images and can make them blurry, the DPI Synchronization feature increases the size of fonts and images, keeping them sharp. For this reason, the DPI Synchronization feature is generally preferred for an optimal user experience.

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

The **DPI Synchronization** agent group policy setting determines whether the DPI Synchronization feature is enabled. The feature is enabled by default.

Behavior of DPI Synchronization

The default DPI synchronization behavior depends on the Horizon Agent version that is installed in the agent machine.

Beginning with Horizon Agent 2012, the client's per-monitor DPI setting is synchronized to the agent and changes take effect immediately during a remote session by default. This feature is controlled by the DPI Synchronization Per Monitor agent group policy setting. The DPI Synchronization Per Monitor feature is supported by default for virtual desktops and physical desktops. It is not supported for published desktops.

With earlier Horizon Agent versions, the client supports synchronization only to the system DPI setting. DPI Synchronization happens during the initial connection, and Display Scaling works in case of reconnection, if necessary. When DPI Synchronization works and the client system's DPI setting matches the remote desktop's DPI setting, Display Scaling cannot take effect, even if you select the Allow Display Scaling option in the user interface. Windows does not allow users to change the system-level DPI setting for the current user session, and DPI synchronization occurs only when they log in and start a remote session. If users change the DPI setting during a remote session, they must log out and log in again to make the remote desktop's DPI setting match the client system's new DPI setting.

The agent DPI setting is located in the Windows registry at `Computer\HKEY_CURRENT_USER\Control Panel\Desktop: logPixels`.

Note The system DPI setting might not be the same as the main monitor's DPI setting. For example, if you close the main monitor and the system switches to an external display that has a different DPI setting than the main monitor, the system DPI setting is still the same as the DPI setting of the previously closed main monitor.

This version of the client does not support the DPI Synchronization Per Connection agent group policy setting, which is provided with Horizon Agent versions 7.8 through 2006.

For more information about the DPI synchronization group policy settings, see the *Configuring Remote Desktop Features in Horizon* document for your Horizon Agent version.

Supported Guest Operating Systems for Virtual Desktops

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

- 32-bit or 64-bit Windows 7
- 32-bit or 64-bit Windows 8.x
- 32-bit or 64-bit Windows 10
- Windows Server 2008 R2 configured as a desktop
- Windows Server 2012 R2 configured as a desktop
- Windows Server 2016 configured as a desktop
- Windows Server 2019 configured as a desktop

Note For Windows server machines that are configured as a desktop, the DPI Synchronization Per Monitor feature is not supported.

Supported RDS Hosts for Published Desktops and Published Applications

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

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note For RDS hosts, the DPI Synchronization Per Monitor feature is not supported. This limitation does not apply to published applications that run on desktop pools with the VM Hosted Applications feature.

Tips for Using the DPI Synchronization Feature with HTML Access

Following are tips for using the DPI Synchronization feature.

- Although Windows 10 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.
- To sync up with another monitor that has 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.
- If you want to set the resolution manually, you might be able to enable the **High Resolution Mode** setting. For information, see Setting the Screen Resolution.

Use Full-Screen Mode

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

You cannot use full-screen mode in the following situations.

- You are using multiple monitors.
- The browser is in full-screen mode or is maximized by dragging the mouse.
- You are using Safari.

Prerequisites

Connect to the remote desktop or published application.

Procedure

- To display the remote desktop or published application in full-screen mode, click the **Open Menu** button at the top of the sidebar and click **Fullscreen**.

- To exit from full-screen mode, click the **Open Menu** button at the top of the sidebar and click **Quit fullscreen**.

  Alternatively, press the Esc key. In a Chrome or Chromium Edge browser, press and hold the Esc key.

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 pixels. The default Real-Time Audio-Video settings work well with most webcam and audio applications.

Note Browsers on iOS do not support Real-Time Audio-Video.

For information about changing the Real-Time Audio-Video settings, see "Configuring Real-Time Audio-Video Group Policy Settings" in the *Configuring Remote Desktop Features in Horizon* document.

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, 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.

Sharing Remote Desktop Sessions

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

A Horizon administrator must enable the Session Collaboration feature.

For Windows desktops, this task includes enabling the Session Collaboration feature at the desktop pool or farm level. It can also include using group policies to configure Session Collaboration features, such as the available invitation methods. For complete requirements, see System Requirements for the Session Collaboration Feature.

For information about enabling the Session Collaboration feature for Windows desktops, see the *Setting Up Virtual Desktops in Horizon* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon* document. For information about using group policy settings to configure the Session Collaboration feature, see the *Configuring Remote Desktop Features in Horizon* document.

For information about enabling the Session Collaboration feature for Linux desktops, see the *Setting Up Linux Desktops in Horizon* document.

Invite a User to Join a Remote Desktop Session

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

You can invite only users that belong to a domain that the server allows for authentication. You can invite up to five users by default. A Horizon administrator can change the maximum number of users that you can invite.

The Session Collaboration feature has the following limitations.

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

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

Prerequisites

- The Session Collaboration feature must be enabled and configured.
- To use the email invitation method, an email application must be installed.
- To use the IM invitation method for a Windows remote desktop, Skype for Business must be installed and configured.

Procedure

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

   You must use the VMware Blast display protocol.

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

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

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

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

4. Select an invitation method.

   Not all invitation methods might be available.

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

Results

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

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

What to do next

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

Manage a Shared Remote Desktop Session

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

A Horizon administrator can prevent the hand off of control to a session collaborator. For Windows remote desktops, see the **Allow control passing to collaborators** group policy setting in the *Configuring Remote Desktop Features in Horizon* document. For Linux remote desktops, see the `collaboration.enableControlPassing` parameter in the *Setting Up Linux Desktops in Horizon* document.

Prerequisites

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

Procedure

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

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

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

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

Join a Remote Desktop Session

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

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

Note In a Cloud Pod Architecture environment, you cannot join a collaborative session by logging in to the server unless you log in to the session owner's pod.

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

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

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

Prerequisites

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

Procedure

1. Click the link in the collaboration invitation.

   HTML Access opens on the client system.

2. Enter your credentials to log in to HTML Access.

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

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

4. To leave the collaborative session, click **Close** from the sidebar.

Copying and Pasting Text

You can copy and paste plain text and HTML-format rich text between the client device and 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.

A Horizon administrator can configure the ability to copy and paste by using group policy settings that pertain to Horizon Agent for remote desktops and published applications. For more information, see HTML Access Group Policy Settings.

If you use HTML Access in an Internet Explorer (IE), Microsoft Edge 44, or Safari browser, you must click the Clipboard icon on the sidebar and use the **Copy & Paste** window to copy and paste text. See Use the Copy and Paste Window.

If you use HTML Access in a Chrome, Microsoft Edge 81 or later, or Firefox browser, a tool tip appears when you point to the Clipboard icon on the sidebar. The tool tip explains whether the clipboard feature is available. After you allow access to the clipboard, copying and pasting from the client system to a remote desktop or published application, and conversely, is the same as copying and pasting between applications on the same system. For example, you can press Ctrl+C to copy text and press Ctrl+V to paste text. When you copy and paste rich text, the following restrictions apply.

- Image copy and paste is not supported.
- If you copy rich text from the client device and the destination is the WordPad application, only the plain text is copied and pasted.
- A Horizon administrator can use group policy settings to restrict clipboard formats during copy and paste operations. Because HTML Access supports transferring only text in the clipboard, only the text filters work with HTML Access. For information about clipboard format filter policy settings, see the *Configuring Remote Desktop Features in Horizon* document.

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 the maximum clipboard size amount, 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.

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 Window

When you use HTML Access in an Internet Explorer (IE), Microsoft Edge 44, or Safari browser, you must use the **Copy & Paste** window to copy and paste text.

This procedure describes how to use the **Copy & Paste** window to copy text on the local client system to an application in a remote desktop or to a published application, and how to copy text from an application in a remote desktop or published application to the client system.

If you are copying and pasting text between published applications, or between remote desktops, you can copy and paste as you normally do. You do not need to use the **Copy & Paste** window.

The text in the **Copy & Paste** window shows one of the following messages to indicate in which direction you 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 only from the client system and paste into a remote desktop or published application. To be able to copy from a remote desktop or published application to the client system, the group policy setting must be enabled in both directions.

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**. If you are using a Mac, this option appears only in the **Settings** window.

A Horizon administrator must leave the default policy in effect, which allows users to copy from client systems and paste into remote desktops and published applications, or configure another policy that allows copying and pasting. For more information, see HTML Access Group Policy Settings.

Procedure

- To copy text from the client system to an application in a remote desktop, or from the client system to a published application, perform these steps.
  a. Copy the text in the local client application.
  b. In HTML Access, open the sidebar and click the Clipboard icon 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 on a Windows system or Command-V on a Mac.

The following message appears briefly: `"Remote Clipboard Synced."`

d Click in the application where you want to past the text and press Ctrl+V.

The text is pasted into the application.

- To copy text from an application in a remote desktop to the client system, or from a published application to the client system, perform these steps.

a Copy the text in the application.

b In HTML Access, open the sidebar and click the Clipboard icon at the top of the sidebar.

The **Copy & Paste** window appears and shows the pasted text. The following message appears briefly: `"Remote Clipboard Synced."`

c To copy the text again, click in the **Copy & Paste** window and press Ctrl+C on a Windows system or Command-C on a Mac.

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

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

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

With the file transfer feature, you can transfer files between the client system and a remote desktop or published application.

A Horizon administrator can configure the ability to allow, disallow, or allow in one direction only, the transfer of files by modifying the **Configure file transfer** group policy setting for VMware Blast. This group policy setting has the following values.

- If the **Disabled both upload and download** value is selected, the **File Transfer** button is disabled.
- If the **Enabled file upload only** value is selected (the default setting), only the **Upload** tab appears in the **Transfer Files** window.
- If the **Enabled file download only** value is selected, only the **Download** tab appears in the **Transfer Files** window.

If the **Configure clipboard redirection** group policy setting is disabled from the server to the client, file download is also disabled.

For more information about these group policy settings, see the *Configuring Remote Desktop Features in Horizon* document.

This feature has the following limitations.

- You can download files up to 500 MB and upload files up to 2 GB.
- 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 and later do not support download.
- 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.
- If you upload a file with Internet Explorer 11, or with Chrome on a Chromebook, if you drag and drop folders, files of zero size, or files that are larger than 2 GB, you receive an error message as expected. After you dismiss the error message, you can no longer drag and drop files that can be transferred.
- You cannot use this feature with Linux remote desktops or Android devices.

Download Files From a Remote Desktop or Published Application to the Client System

You can download files from a remote desktop or published application to the client system.

A Horizon administrator can disable this feature. For more information, see Transferring Files Between the Client and a Remote Desktop or Published Application.

Procedure

1. Connect to the remote desktop or published application.
2. To open the sidebar, click the sidebar tab.
3. Click the file transfer icon at the top of the sidebar.

   The **Transfer Files** window appears.
4. Click **Download** in the **Transfer Files** window.
5. Select one or more files to download.
6. To begin the file transfer, press Ctrl+c.

   The files appear on the **Download** tab in the **Transfer Files** window.
7. To download the files to the client system, click the download icon (the down arrow).

   The files appear in the `Downloads` folder on the client system.

Upload Files From the Client System to a Remote Desktop or Published Application

You can upload files from the client system to a remote desktop or published application.

A Horizon administrator can disable this feature. For more information, see Transferring Files Between the Client and a Remote Desktop or Published Application.

Procedure

1. Connect to the remote desktop or published application.
2. To open the sidebar, click the sidebar tab.
3. Click the file transfer icon at the top of the sidebar.

   The **Transfer Files** window appears.
4. To upload files, drag and drop the files to the **Upload** tab in the **Transfer Files** window, or click **Choose Files** on the **Upload** tab and select the files to upload.

   The uploaded files appear in the `Documents` folder.

Use USB Devices in a Remote Desktop

With the USB Redirection feature, you can use some locally attached USB devices in a remote desktop. You can redirect multiple USB devices to a remote desktop. You cannot redirect USB devices to published desktops and published applications.

Because of Chrome browser limitations, many USB devices cannot be redirected to a remote desktop. For this release, VMware tested the following USB devices. Additional devices might be supported. If a USB device is not supported, Horizon Client returns an error message when you try to redirect the device.

- Samsung C43x Print Series
- HP LaserJet P2055d
- HP Deskjet 3525
- AmbirScanPro 490i

Prerequisites

- You must use Chrome 87 or later or Chromium-based Microsoft Edge 87 or later.
- A Horizon administrator must configure the USB redirection feature for the remote desktop.

For information about configuring the USB redirection feature for remote desktops, see "Configuring USB Redirection for Chrome and HTML Access Clients" in the *Configuring Remote Desktop Features in Horizon* document.

Procedure

1. Connect the USB device to the local system.
2. Start HTML Access and connect to the remote desktop.
3. To open the sidebar, click the sidebar tab.
4. Click the **Open Menu** button at the top of the sidebar and click **USB**.
5. Click **Add Device**.
6. Select the USB device from the list and click **Connect**.

   If the device is supported, it is redirected to the remote desktop and is available for use in the session. If the device is not supported, an error message appears.
7. (Optional) Click **Add Device** again to redirect another USB device.
8. To release a USB device from the remote desktop, click **Release**.

Printing From a Remote Desktop or Published Application

With the VMware Integrated Printing feature, you can print to a network printer or a locally attached printer from a remote desktop or published application.

To use this feature, Horizon Agent must be installed on the virtual machine or RDS host with the VMware Integrated Printing option enabled. For more information, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

A Horizon administrator can disable the VMware Integrated Printing feature by using the **Disable printer redirection for non-desktop client** group policy setting. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

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.

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>*) by default.

Beginning with Horizon Agent 7.12, you can use group policy to modify the printer naming convention for client printers that are redirected. For information, see the *Configuring Remote Desktop Features in Horizon* document for your Horizon Agent version.

Prerequisites

To use VMware Integrated Printing, a Horizon administrator must install the VMware Integrated Printing feature in the remote desktop. This task involves enabling the **VMware Integrated Printing** option in the Horizon Agent installer. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document. For information about configuring the VMware Integrated Printing feature, see the *Configuring Remote Desktop Features in Horizon* document.

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.
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**.

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 application pool. Users cannot modify the multi-session mode for a published application unless a Horizon administrator allows it. See *Setting Up Published Desktops and Applications in Horizon*.

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.

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. Some browsers work better than others in this regard.

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 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), Ctrl+Command (on Mac), or Ctrl+Search (on Chromebook) 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 Server 2012 R2 operating system do not work in remote desktops that have a Windows 10 operating system.

Table 4-4. 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+Pause	Display the System Properties dialog box.	There is no Pause key on Chromebooks or Macs.
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 4-5. Windows Key Shortcuts for 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.	

Table 4-5. Windows Key Shortcuts for Windows Server 2012 R2 Remote Desktops (continued)

Keys	Action	Limitations
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+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.
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.	

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 4-6. 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

Troubleshooting

5

You can solve most HTML Access problems by restarting or resetting remote desktops or published applications.

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.

For information about enabling the desktop restart feature, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Procedure

- Use the **Restart** command.

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

Results

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

What to do next

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

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

Reset Remote Desktops or Published Applications

You might need to reset a remote desktop if the desktop operating system stops responding and restarting the remote desktop does not solve the problem.

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

Resetting published applications quits all open applications.

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

For information about enabling the desktop reset feature, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Procedure

- Use the **Reset** command.

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

Results

When you reset a remote desktop, the operating system in the remote desktop restarts and the 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.