VMware Horizon HTML Access Installation and Setup Guide

Modified on 29 MAY 2018
VMware Horizon HTML Access 4.8
VMware Horizon 7 7.5

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

VMware Horizon HTML Access Installation and Setup Guide

This guide, *VMware Horizon HTML Access Installation and Setup Guide*, describes how to install, configure, and use the VMware Horizon® HTML Access™ software to connect to virtual desktops without having to install any software on a client system.

The information in this document includes system requirements and instructions for installing HTML Access software on a VMware Horizon 7 server and on a remote desktop virtual machine so that end users can use a Web browser to access remote desktops.

Important This information is intended for administrators who already have some experience using Horizon 7 and VMware vSphere. If you are a novice user of Horizon 7, you might occasionally need to refer to the step-by-step instructions for basic procedures in the *Horizon 7 Installation* documentation and the *Horizon 7 Administration* documentation.

Setup and Installation

1

Setting up a Horizon 7 deployment for HTML Access involves installing HTML Access on View Connection Server, opening the required ports, and installing the HTML Access component in the remote desktop virtual machine.

End users can then access their remote desktops by opening a supported browser and entering the URL for View Connection Server.

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 Horizon 7 deployment must meet certain software requirements.

Note Starting with version 7.0, View Agent is renamed Horizon Agent.

Browser on client systems

Browser	Version
Chrome	65, 66
Chrome on Android device	65 or later
Internet Explorer	11
Safari	11
Safari on mobile device	iOS 10, iOS 11
Firefox	59, 60
Microsoft Edge	41, 42

Note

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

Client operating systems

Operating System	Version
Windows	7 SP1 (32-bit and 64-bit)
Windows	8.x (32-bit and 64-bit)
Windows	10 (32-bit and 64-bit)
Mac OS X	10.12.x (Sierra)
macOS	10.13.x (High Sierra)
iOS	10, 11
Chrome OS	28.x and later
Android	7, 8

Remote desktops	HTML Access requires Horizon Agent 7.0 or later, and supports all the desktop operating systems that Horizon 7.0 supports. For more information, see the topic "Supported Operating Systems for Horizon Agent" in version 7.0 or later of *View Installation*.
Pool settings	HTML Access requires the following pool settings, in Horizon Administrator: ■ 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 Screen Resolution. ■ The **HTML Access** setting must be enabled. Configuration instructions are provided in Prepare Desktops, Pools, and Farms.
Connection Server	Connection Server with the HTML Access option must be installed on the server. When you install the HTML Access component, the **VMware Horizon View Connection Server (Blast-In)** rule is enabled in the Windows Firewall, so that the firewall is automatically configured to allow inbound traffic to TCP port 8443.
Security Server	The same version as Connection Server must be installed on the security server. If client systems connect from outside the corporate firewall, use a security server. With a security server, client systems do not require a VPN connection. **Note** A single security server can support up to 800 simultaneous connections to Web clients.
Third-party firewalls	Add rules to allow the following traffic: ■ Servers (including security servers, Connection Server instances, and replica servers): inbound traffic to TCP port 8443. ■ Remote desktop virtual machines: inbound traffic (from servers) to TCP port 22443.
Display protocol for Horizon	VMware Blast When you use a Web browser to access a remote desktop, the VMware Blast protocol is used rather than PCoIP or Microsoft RDP. VMware Blast uses HTTPS (HTTP over SSL/TLS).

Preparing Connection Server and Security Servers

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

You can use Unified Access Gateway appliances, rather than security servers, for secure external access. For more information, see the *Deploying and Configuring Unified Access Gateway* document.

Following is a check list of the tasks that a Horizon administrator must perform to use HTML Access.

1 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 7 Installation* document.

   To verify that the HTML Access component is installed, you can open the Windows Uninstall a Program applet and look for **VMware Horizon 7 HTML Access** in the list.

2 If you use security servers, install Security Server. The version of Security Server must match the version of Connection Server. For installation instructions, see the *Horizon 7 Installation* document.

3 Verify that each Connection Server instance or security server 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 7 Installation* document.

4 To use two-factor authentication, such as RSA SecurID or RADIUS authentication, verify that this feature is enabled on Connection Server. For more information, see the topics about two-factor authentication in the *Horizon 7 Administration* document.

   Important If you enable the **Hide domain list in client user interface** settings and select two-factor authentication (RSA SecureID or RADIUS) for the Connection Server instance, do not enforce Windows user name matching. Enforcing Windows user name matching prevents users from entering domain information in the user name text box and login always fails. For more information, see the topics about two-factor authentication in the *Horizon 7 Administration* document.

5 If you use third-party firewalls, configure rules to allow inbound traffic to TCP port 8443 for all security servers and 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.

6 To provide unauthenticated access to published applications, enable this feature in Connection Server. For more information, see the *Horizon 7 Administration* document.

After the servers are installed, the **Blast Secure Gateway** setting is enabled on the applicable Connection Server instances and security servers in Horizon Administrator. Also, the **Blast External URL** setting is configured to use the Blast Secure Gateway on the applicable Connection Server instances and security servers. 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 or security server host. For more information, see "Set the External URLs for a Connection Server Instance," in the *Horizon 7 Installation* document.

Note You can use HTML Access with VMware Workspace ONE to allow users to connect to their desktops from an HTML5 browser. 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 7 Administration* document.

Firewall Rules for Client Web Browser Access

To allow client Web browsers to make connections to security servers, 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 or security server, 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	Security server or Connection Server instance	TCP 443	To make the initial connection, the Web browser on a client device connects to a security server or 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 security server or Connection Server instance to allow this second connection to take place.

Table 1-1. Firewall Rules for Client Browser Access (Continued)

Source	Default Source Port	Protocol	Target	Default Target Port	Notes
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 Horizon 7 to Remove Credentials from Cache

You can configure Horizon 7 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.

Note 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.

Prerequisites

This feature requires Horizon 7 version 7.0.2 or later.

Procedure

1. In Horizon Administrator, select **View Configuration > Global Settings** and click **Edit** in the General pane.
2. Select the **Clean up credential when tab closed for HTML Access** check box.
3. To save your changes, click **OK**.

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

Prepare Desktops, Pools, and Farms

Before end users can access a remote desktop or published application, a Horizon administrator must configure certain pool and farm settings and install Horizon Agent on desktop virtual machines and RDS hosts in the data center.

The HTML Access client is a good alternative when Horizon Client software is not installed on the client system.

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

Prerequisites

- Verify that the Horizon components meet the system requirements for HTML Access. See System Requirements for HTML Access.
- Verify that the HTML Access component is installed with Connection Server on the host or hosts and that the Windows firewalls on Connection Server instances and any security servers allow inbound traffic on TCP port 8443. See Preparing Connection Server and Security Servers.
- If you use third-party firewalls, configure a rule to allow inbound traffic from Horizon servers to TCP port 22443 on desktop virtual machines and RDS hosts in the data center. See Firewall Rules for Client Web Browser Access.
- Verify that the virtual machine you plan to use as a desktop source, or the RDS host that hosts published desktops and applications, has a supported operating system and VMware Tools installed. See System Requirements for HTML Access.
- Become familiar with the procedures for creating pools and farms and entitling users. See the *Setting Up Virtual Desktops in Horizon 7* and *Setting Up Published Desktops and Applications in Horizon 7* documents.
- To verify that the remote desktop or published application is accessible to end users, install Horizon Client for Windows on a client system. You can use Horizon Client for Windows to test the connection before you attempt to connect from a Web browser. For installation instructions, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.
- Verify that you have one of the supported browsers for accessing a remote desktop or published application. See System Requirements for HTML Access.

Procedure

1. For published desktops and applications, use Horizon Administrator to create or edit the farm and enable the **Allow HTML Access to desktops and applications on this farm** option in the farm settings.

2. For virtual desktop pools, use Horizon Administrator to create or edit the desktop pool so that the pool can be used with HTML Access.
   a. Enable the **HTML Access** in the Desktop Pool settings.
   b. In the pool settings, verify that the **Max resolution of any one monitor** setting is **1920x1200** or higher.
3. After the pools are created, recomposed, or upgraded to use Horizon Agent with the **Allow HTML Access to desktops and applications on this farm** or **HTML Access** option, use Horizon Client for Windows to connect to a remote desktop or published application.

   With this step, before you attempt to use HTML Access, you verify that the pool is working correctly.
4. Open a supported browser and enter a URL that points to your Connection Server instance.

   For example:

   ```
   https://horizon.mycompany.com
   ```

   You must include **`https`** in the URL.
5. On the Web page that appears, click **VMware Horizon HTML Access** and log in as you do with Horizon Client for Windows.
6. On the desktop and application selection page that appears, click an icon to connect.

You can now access a remote desktop or published application from a Web browser.

What to do next

For added security, if your security policies require that the HTML Access Agent on the remote desktop uses a TLS certificate from a certificate authority, see Configure HTML Access Agents to Use New TLS Certificates.

Requirements for the Session Collaboration Feature

With the Session Collaboration feature, users can invite other users to join an existing Windows 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 4.7 or later for Windows, Mac, or Linux installed on the client system, or must use HTML Access 4.7 or later.
Windows remote desktops	■ Horizon Agent 7.4 or later must be installed in the virtual desktop, or on the RDS host for published 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 7* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon 7* 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 7* document. The Session Collaboration feature does not support Linux remote desktop sessions or published application sessions.
Connection Server	The Session Collaboration feature requires that the Connection Server instance uses an Enterprise license.
Display protocols	VMware Blast

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 desktops, 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.

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 SSL 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. which is described at https://www.openssl.org/docs/manmaster/man1/ciphers.html.

Procedure

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

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 Restart the VMware Blast service to make your changes take effect.

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

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's 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 need to install SSL certificates that are signed by a Certificate Authority (CA) instead of the default SSL certificates that are generated by the View Connection Server or the HTML Access Agent.

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

Using a CA-Signed Certificate with Unified Access Gateway

If you use a Unified Access Gateway appliance instead of a Connection Server or security server, 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 or security server, users can still connect by clicking the `Proceed to ip-address (unsafe)` link.

For information about installing and configuring certificates for Horizon 7, see the *Horizon 7 Installation* document. For information about configuring HTML Access agents to use TLS certificates, see Configure HTML Access Agents to Use New TLS Certificates.

Upgrading the HTML Access Software

For most versions of HTML Access, upgrading involves simply upgrading Connection Servers and View Agent.

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

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

Note To check whether the HTML Access component is installed, you can 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 the Uninstall a Program applet provided by the Windows Control Panel.
2. Select **VMware Horizon 7 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

Disallow inbound traffic to TCP port 8443 on the Windows Firewall of any paired security servers. If applicable, on third-party firewalls, change the rules to disallow inbound traffic to TCP port 8443 for all paired security servers and the Connection Server instance.

Data Collected by VMware

If your company participates in the customer experience improvement program, VMware collects data from certain client fields. Fields containing sensitive information are made anonymous.

VMware collects data on the clients to prioritize hardware and software compatibility. If a Horizon administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment to improve VMware's response to customer requirements. No data that identifies your organization is collected. Client information is sent first to Connection Server and then on to VMware, along with data from servers, desktop pools, and remote desktops.

To participate in the VMware customer experience improvement program, the administrator who installs Connection Server can opt in while running the Connection Server installation wizard, or an administrator can set an option in Horizon Administrator after the installation.

Table 1-2. Client Data Collected for the Customer Experience Improvement Program

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	4.8.0-*build_number*
Client binary architecture	`<client-arch>`	No	Examples include the following values: ■ browser ■ arm

Table 1-2. Client Data Collected for the Customer Experience Improvement Program (Continued)

Description	Field name	Is This Field Made Anonymous?	Example Value
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

Configuring HTML Access for End Users

2

You can change the appearance of 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 this Web page to show or hide the icon for downloading Horizon Client or the icon for connecting to a remote desktop through HTML Access. You can also configure other links on this page.

By default, the web portal page shows both an icon for downloading and installing the native Horizon Client, and an icon for connecting through HTML Access. The download link used is determined from the default values defined in the `portal-links-html-access.properties` file.

In some cases, however, you might want to have the links 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 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 used to determine 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` folder. If this file is missing during the HTML Access session, the download link will direct 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://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

You can make installer links for specific client operating systems in either the portal-links-html-access.properties or oslinks.properties file. For example, if you browse to the portal page from a Mac OS X system, the link for the native Mac OS X installer appears. For Windows or Linux clients, you can make separate links for 32-bit and 64-bit installers.

Important If you upgraded from View Connection Server 5.x or an earlier release and did not have the HTML Access component installed, and if you previously edited the portal page to point to your own server for downloading Horizon Client, those customizations might be hidden after you install Connection Server 6.0 or later. With Horizon 6 or later, the HTML Access component is automatically installed during an upgrade of Connection Server.

If you already installed the HTML Access component separately for Horizon 7 5.x, any customizations you made to the Web page are preserved. If you did not have the HTML Access component installed, any customizations you had made are hidden. The customizations for earlier releases reside in the `portal-links.properties` file, which is no longer used.

Procedure

1 On the Connection Server host, open the `portal-links-html-access.properties` file with a text editor.

The location of this file is *`CommonAppDataFolder`*`\VMware\VDM\portal\portal-links-html-access.properties`. For Windows Server 2008 operating systems, the *CommonAppDataFolder* directory is `C:\ProgramData`. To display the `C:\ProgramData` folder in Windows Explorer, you must use the Folder Options dialog box to show hidden folders.

If the `portal-links-html-access.properties` file does not exist and the `oslinks.properties` file does, 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.

Note Customizations for Horizon 7 5.x and earlier releases resided in the `portal-links.properties` file, which is located in the same *`CommonAppDataFolder`*`\VMware\VDM\portal\` directory as the `portal-links-html-access.properties` file.

2 Edit the configuration properties to set them appropriately.

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 Web site. To disable an icon, which removes the icon from the Web page, set the property to `false`.

Note The `oslinks.properties` file can only be used to configure the links to the specific installer files. It does not support the other options listed below.

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, but you can use relative 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 Connection Server, 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`
	■ Mac OS X 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`

Option	Property Setting
	■ Chrome OS installer: `link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-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 Web site. The Help link appears at the bottom of the login page.

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

This location must correspond to the URLs you specified in the `portal-links-html-access.properties` file or 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 could 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

Using uniform resource identifiers (URIs), you can create a Web page or an email with links that end users click to launch the HTML Access Web client, connect to View Connection Server, and launch a specific desktop or application with specific configuration options.

You can simplify the process of connecting to a remote desktop or application by creating Web or email links for end users. You create these links by constructing URIs that provide some or all of the following information, so that your end users do not need to supply it:

- View Connection Server address
- Port number for View Connection Server
- Active Directory user name
- RADIUS or RSA SecurID user name, if different from Active Directory user name
- Domain name
- Desktop or application display name
- Actions including browse, reset, log off, and start session

Syntax for Creating URIs for HTML Access

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

URI Specification

Use the following syntax to create URIs for launching HTML Access Web clients:

```
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 is displayed.
- 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 the HTML Access Web client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the *Using VMware Horizon Client* 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 desktops and applications hosted on the specified server. You are not required to specify a desktop or application when using this action.
`start-session`	Starts the specified desktop or application. If no action query is provided and the desktop or application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified 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 an application.
`logoff`	Logs the user out of the guest operating system in the remote desktop. This action is not valid for an application.
`restart`	Shuts down and restarts the primary desktop after the user confirms the restart operation request. This action is not valid for an application.

applicationId

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

args

Specifies command-line arguments to add to remote application launch. 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 desktop display name. The display name is the name specified in View Administrator when the desktop pool was created. If the display name has a space in it, 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 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 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. The HTML Access Web client is launched and an anonymous user account is displayed. 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`**

Examples of URIs

You can create hypertext links or buttons with a URI and include these links in email or on a Web page. Your end users can click these links to, for example, open a particular remote desktop or application with the startup options you specify.

URI Syntax Examples

Each URI example 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
```

The HTML Access Web client is launched 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
```

The HTML Access Web client is launched 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
```

The HTML Access Web client is launched 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
```

The HTML Access Web client is launched 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 desktop whose display name is displayed as **Primary Desktop**, and the user is logged in to the guest operating system.

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

The HTML Access Web client is launched 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 is launched.

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

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for Connection Server. (The default port is 443.) Because a desktop identifier is provided, the desktop is launched 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 an application and a desktop. When you specify both an application and a desktop, only the desktop is launched.

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

The HTML Access Web client is launched 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 the 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 launch 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 launch 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 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
```

The HTML Access Web client is launched 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 the Horizon administrator has allowed end users to restart their machines.

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

The HTML Access Web client is launched 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 says, **Test Link**, and a button that says, **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 7* document.

Using a Remote Desktop or Application

3

The client provides a navigation sidebar with toolbar buttons so that you can easily disconnect from a remote desktop or application or use a button click to send the equivalent of the Ctrl+Alt+Delete key combination.

This chapter includes the following topics:

Feature Support Matrix

When you access a remote desktop or application from the browser-based HTML Access client, some features are not available.

Feature Support for Single-User Virtual Machine Desktops

Table 3-1. Features Supported Through HTML Access

Feature	Windows 7 Desktop	Windows 8.x Desktop	Windows 10 Desktop	Windows Server 2008 R2 Desktop	Windows Server 2012 R2 Desktop	Windows Server 2016 Desktop
RSA SecurID or RADIUS	X	X	X	X	X	X
Single sign-on	X	X	X	X	X	X
RDP display protocol						
PCoIP display protocol						
VMware Blast display protocol	X	X	X	X	X	X
USB redirection						
Real-Time Audio-Video (RTAV)	X	X	X	X	X	X
Wyse MMR						
Windows Media MMR						
Virtual printing						
Location-based printing	X	X	X	X	X	X
Smart cards						
Multiple monitors	X	X	X	X	X	X

For descriptions of these features and their limitations, see the *Horizon 7 Architecture Planning* document.

Feature Support for Session-Based Desktops and Hosted Applications on RDS Hosts

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

Note The following table contains rows only for the features that are available from RDS hosts if you use HTML Access. Additional features are available if you use natively installed Horizon Client, such as Horizon Client for Windows.

Table 3-2. Features Supported for HTML Access to RDS Hosts with View Agent 6.1.1 or Later, or Horizon Agent 7.0 or Later, Installed

Feature	Windows Server 2008 R2 RDS Host	Windows Server 2012 or 2012 R2 RDS Host	Windows Server 2016
RSA SecurID or RADIUS	X	X	Horizon Agent 7.0.2 and later
Single sign-on	X	X	Horizon Agent 7.0.2 and later
VMware Blast display protocol	X	X	Horizon Agent 7.0.2 and later
Location-based printing	X (virtual machine only)	X (virtual machine only)	Horizon Agent 7.0.2 and later (virtual machine only)
Real-Time Audio-Video (RTAV)	Horizon Agent 7.0.2 and later	Horizon Agent 7.0.2 and later	Horizon Agent 7.0.3 and later
Multiple monitors (for session-based desktops only)	X	X	X

For information about which editions of each guest operating system are supported, or which service packs, see "Supported Operating Systems for Horizon Agent" in the *View Installation* document.

Internationalization

The user interface and documentation are available in English, Japanese, French, German, Simplified Chinese, Traditional Chinese, Korean, and Spanish.

For information about which language packs you must use in the client system, browser, and remote desktop, see International Keyboards.

Connect to a Remote Desktop or Application

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

Prerequisites

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

Procedure

1. Open a browser and enter the URL for the Connection Server instance.

   In the URL, use **`https`** and use the fully qualified domain name; for example: `https://horizon.company.com`.

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

The VMware Horizon Web portal appears. By default, this page shows both an icon for downloading and installing the native Horizon Client and an icon for connecting through HTML Access.

2 (Optional) Select the **Click here to skip this screen and always use HTML Access** check box.

Your selection is stored in the local storage for the browser you are currently using. The next time you enter the URL for the Connection Server instance using the same browser type and same client machine, you will be taken directly to the Login screen. If you use a different browser type on the same client machine or if you use the same type of browser on a different client machine, the VMware Horizon Web portal appears. Clear your browser's cache if you want the VMware Horizon Web Portal to appear.

3 Click the **VMware Horizon HTML Access** icon.

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

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

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 entered previously. If necessary, wait until a new number is generated.

If this step is required, it is required only when you mistype the first passcode or when configuration settings in the RSA server change.

6 In the Login dialog box, enter your login credentials.

a In the Username text box, enter your valid Active Directory user name in either *username*, *domain**username*, or *username*@*domain* format.

If the Domain text box is disabled, you must use either the *domain**username* or *username*@*domain* format.

b Enter your password.

c (Optional) If the Domain text box is enabled, select a domain name, if it is not already correctly populated.

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

7 (Optional) If you have to set the time zone that is used in the remote desktop or application manually, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector screen. Turn off the **Set Time Zone Automatically** option and select one of the time zones from the drop-down menu. See Setting the Time Zone.

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

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

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

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

What to do next

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

Trust a Self-Signed Root Certificate

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

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

Procedure

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

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

   a Click the lock icon in the address bar.

   b Click the **Certificate information** link.

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

      You might need to contact your system administrator for assistance.

2 Accept the security certificate.

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

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

a Click the **Show Certificate** button when the untrusted certificate dialog box appears.

b Select the **Always Trust** check box and click **Continue**.

c When prompted, provide your password and click **Update Settings**.

The remote desktop or published application starts.

Connect to a Server in Workspace ONE Mode

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

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

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

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

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

Use Unauthenticated Access to Connect to Published Applications

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

Prerequisites

- Perform the administrative tasks described in Preparing Connection Server and Security Servers.
- Set up Unauthenticated Access users on the Connection Server instance. For information, see "Providing Unauthenticated Access for Published Applications" in the *Horizon 7 Administration* document.

Procedure

1. To connect to the Connection Server instance on which you have unauthenticated access to published applications, open a browser and use one of the following URI syntaxes.

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

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

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

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

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

   The application selection window appears.

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

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

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

Shortcut Key Combinations

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

Web browsers allow some key presses and key combinations to be sent to both the client system and the destination system. For other keys and key combinations, the input is processed only locally and is not sent to the destination system. The key combinations that work on your system depend on the browser software, the client operating system, and the language settings.

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

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

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

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

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

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

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

These key combinations do not work for published applications. These key combinations do work for Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016 remote desktops and published desktops.

Some key combinations that work in remote desktops that have a Windows 8.x or Windows Server 2012 R2 operating system do not work in remote desktops that have a Windows 7, Windows Server 2008 R2, or Windows 10 operating system.

Table 3-3. 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.	

Table 3-3. Windows Key Shortcuts for Windows 10 Remote Desktops and Windows Server 2016 Remote Desktops (Continued)

Keys	Action	Limitations
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+Shift+M	Restore minimized windows on the remote desktop.	Does not work in Safari.
Win+Alt+Num	Open the remote desktop and open the jump list for the app pinned to the taskbar in the position indicated by the number.	Does not work on a Chromebook.
Win+Enter	Open Narrator.	

Table 3-4. Windows Key Shortcuts for Windows 8.x and Windows Server 2012 R2 Remote Desktops

Keys	Action	Limitations
Win+F1	Open Windows Help and Support.	Does not work in Safari.
Win	Show or hide the Start window.	
Win+B	Set focus on the notification area.	
Win+C	Open the Charms panel.	
Win+D	Show and hide the remote desktop.	Does not work in Safari. Press Command-D on a Mac.
Win+E	Open File Explorer.	
Win+H	Open the Share charm.	
Win+I	Open the Settings charm.	
Win+K	Open the Devices charm.	
Win+M	Minimize all windows.	
Win+Q	To search everywhere or within the open app, if the app supports app search, open the Search charm.	
Win+R	Open the Run dialog box.	
Win+S	To search Windows and the Web, open the Search charm.	
Win+X	Open the **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.

Table 3-4. Windows Key Shortcuts for Windows 8.x and Windows Server 2012 R2 Remote Desktops (Continued)

Keys	Action	Limitations
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.	

Table 3-5. Windows Key Shortcuts for Windows 7 and Windows Server 2008 R2 Remote Desktops

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

Table 3-5. Windows Key Shortcuts for Windows 7 and Windows Server 2008 R2 Remote Desktops (Continued)

Keys	Action	Limitations
Win+G	Cycle through running remote desktop gadgets.	
Win+U	Open the Ease of Access Center.	

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 3-6. 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

Screen Resolution

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

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

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

- The software-accelerated graphics feature, available with vSphere 5.0 or later, allows you to use 3D applications such as Windows Aero themes or Google Earth. This features requires 64MB to 128MB of VRAM.
- The shared hardware-accelerated graphics feature (vSGA), available with vSphere 5.1 or later, allows you to use 3D applications for design, modeling, and multimedia. This feature requires 64MB to 512MB of VRAM. The default is 96MB.
- The dedicated hardware-accelerated graphics feature (vDGA), 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 64MB to 512MB of VRAM. The default is 96MB.

When 3D rendering is enabled, the maximum number of monitors is 1 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 you need for the VMware Blast display protocol is similar to estimating how much VRAM is required for the PCoIP display protocol. For guidelines, see the section "RAM Sizing for Specific Monitor Configurations When Using PCoIP" of the topic "Estimating Memory Requirements for Virtual Desktops," in the *Horizon 7 Architecture Planning* document.

Allowing H.264 Decoding

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

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

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

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

Setting the Time Zone

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

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

To set the correct time zone information to use before you connect to a remote desktop or published application manually, click the **Settings** toolbar button in the upper-right corner of the desktop and application selector window. Turn off the **Set Time Zone Automatically** option in the **Settings** window and select one of the time zones from the drop-down menu.

The value you selected is saved as your preferred time zone to use when connecting to a remote desktop or published application.

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

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

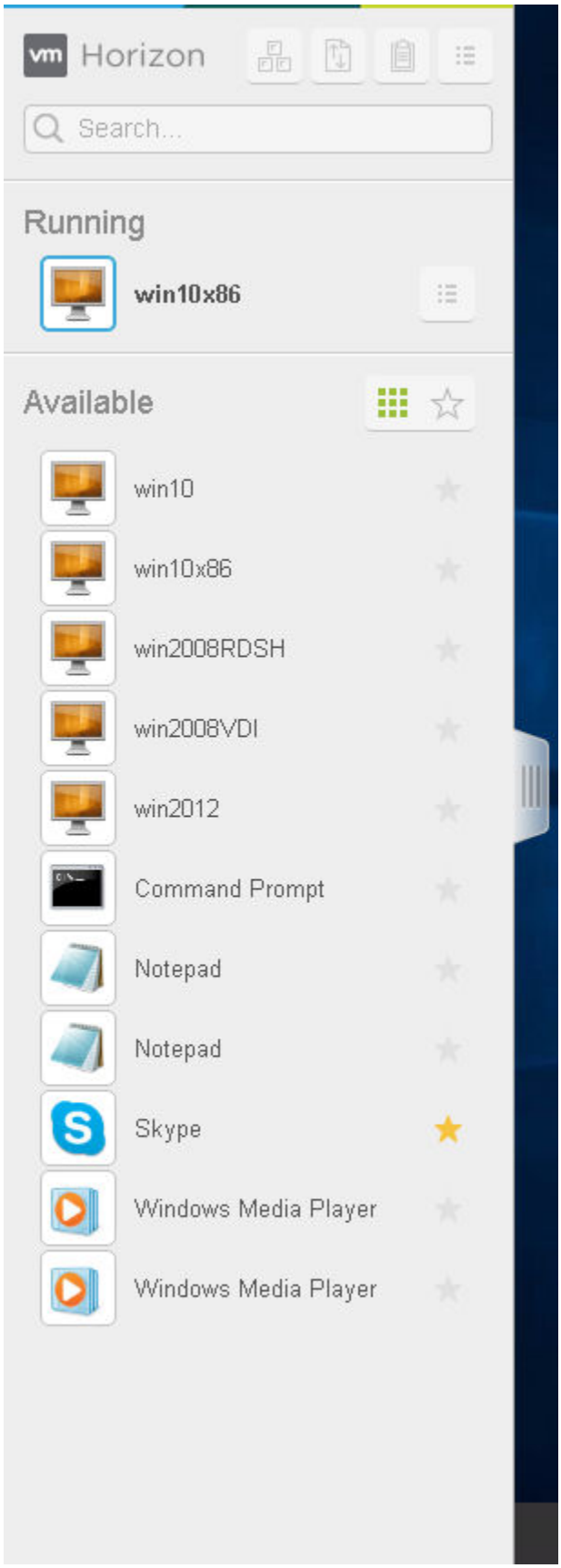
Note When you use the Chrome browser on an Android device, if the **Set Time Zone Automatically** option is set to **`true`** and you change the Android system's time zone, the new time zone is not synchronized with the remote desktop automatically. This problem is a Chrome limitation on the Android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

Using the Sidebar

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

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

Figure 3-1. Sidebar That Appears When You Start a Remote Desktop or Published Application



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

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

You can perform many actions from the sidebar.

Table 3-7. Sidebar Actions

Action	Procedure
Show the sidebar	When a published application or remote desktop is open, click the sidebar tab. When the sidebar is open, you can still perform actions in the published application or remote desktop window.
Hide the sidebar	Click the sidebar tab.
Start a published application or remote desktop	Click the name of a published application or remote desktop in the **Available** list in the sidebar. Remote desktops are listed first.
Search for a published application or remote desktop	■ Click in the **Search** box and begin typing the name of the published application or remote desktop. ■ To start a published application or remote desktop, click its name in the search results. ■ To return to the home view of the sidebar, tap the **X** in the search box.
Create a list of favorite published applications and remote desktops	Click the gray star next to the name of the remote desktop or published application in the **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 published applications or remote desktops	Click the published application or remote desktop name in the **Running** list in the sidebar.
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 3-7. 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**.
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.
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.

Use Multiple Monitors

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

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

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

Procedure

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

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

6 Drag the Display Selector window so that it appears in the other monitor display that you want to use.

   The message in the Display Selector browser window changes and a gray rectangular icon is added.

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

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

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

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

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

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

Using DPI Synchronization

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

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

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

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

Following are tips for using the DPI Synchronization feature.

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

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

Sound

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

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

The following limitations apply to sound playback in remote desktops and published applications.

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

Copying and Pasting Text

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

A Horizon administrator can configure the ability to copy and paste by using group policies that pertain to View Agent or Horizon Agent in remote desktops. For more information, see HTML Access Group Policy Settings. A Horizon administrator can also use group policies 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 the HTML Access client. For information about using group policies to filter clipboard formats, see the *Configuring Remote Desktop Features in Horizon 7* document.

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

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

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

Use the Copy and Paste Feature

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

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

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

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

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

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

Prerequisites

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

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

Procedure

- To copy the text from your client system to the remote desktop or application:
  a. Copy the text in the local client application.
  b. In your browser, click the HTML Access sidebar tab to open the sidebar, and click **Copy & Paste** at the top of the sidebar.

     The Copy & Paste window appears. If previously copied text already appears in the window, that text is replaced when you paste in the newly copied text.
  c. To paste the text into the Copy & Paste window, Press Ctrl+V (or Command-V on Macs).

     The following message appears briefly: `"Remote Clipboard Synced."`
  d. Click in the remote application where you want to past the text and press Ctrl+V.

     The text is pasted into the remote application.
- To copy the text from your remote desktop or application to your client system:
  a. Copy the text in your remote application.
  b. In your browser, click the HTML Access sidebar tab to open the sidebar, and click **Copy & Paste** at the top of the sidebar.

     The Copy & Paste window appears with the text already pasted in it. The following message appears briefly: `"Remote Clipboard Synced."`
  c. To copy the text again, click in the Copy & Paste window and press Ctrl+C (or Command-C on Macs).

     The text is not selected when you do this action, and you cannot select the text. The following message appears briefly: `"Copied from Clipboard Panel."`
  d. On your client system, click where you want to paste the text and press Ctrl+V.

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

Transferring Files Between the Client and a Remote Desktop

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

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

The Horizon administrator can configure the ability to allow, disallow, or allow in one direction only, the transfer of files by modifying the **Configure file transfer** group policy setting for the VMware Blast protocol. The default is upload only. If the **Disabled both upload and download** value is selected in the **Configure file transfer** group policy setting for the VMware Blast protocol, the **File Transfer** button is

disabled. If **Enabled file upload only** value is selected, only the **Upload** tab is displayed in the **Transfer Files** dialog window. If **Enabled file download only** value is selected, only the **Download** tab is displayed in the **Transfer Files** dialog window. For more information, see HTML Access Group Policy Settings.

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

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

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

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

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

Download Files from a Desktop to the Client

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

Procedure

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

   The **Transfer Files** window opens.
2. Click **Download**.
3. Select one or more files on the remote desktop.
4. Press Ctrl+c to start the download.
5. After the download is complete, click the download icon to save the files on the client machine.

Upload Files from the Client to a Desktop

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

Procedure

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

   The **Transfer Files** window opens.
2. Click **Upload**.
3. Drag and drop files into the **Transfer Files** window or click **Choose Files** to select files.

   The selected files are uploaded to the `My Documents` folder.

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

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

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

Real-Time Audio-Video is supported only in Chrome, Microsoft Edge, and Firefox. The default video resolution is 320 x 240. The default Real-Time Audio-Video settings work well with most webcam and audio applications.

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 7* 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.

Using the Session Collaboration Feature

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

Invite a User to Join a Remote Desktop Session

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

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

The Session Collaboration feature has the following limitations.

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

Prerequisites

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

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 Requirements for the Session Collaboration Feature.

For information about enabling the Session Collaboration feature for desktop pools, see the *Setting Up Virtual Desktops in Horizon 7* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon 7* document. For information about using group policy settings to configure the Session Collaboration feature, see the *Configuring Remote Desktop Features in Horizon 7* document.

Procedure

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

   You must use the VMware Blast display protocol.

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

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

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

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

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

4 Select an invitation method.

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

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

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

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

What to do next

Manage the collaborative session in the VMware Horizon Collaboration dialog box. See Manage a Collaborative Session.

Manage a Collaborative Session

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

Prerequisites

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

Procedure

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

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

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

Option	Action
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. You can also end the collaborative session by clicking the VMware Horizon Session Collaboration icon on the desktop and clicking the **Stop** button.

Join a Collaborative Session

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

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

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.

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

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

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

Prerequisites

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

Procedure

1 Click the link in the collaboration invitation.

  Horizon Client opens on the client system.

2 Enter your credentials to log in to Horizon Client.

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

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

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

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.

Reset a Remote Desktop or Published Applications

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

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

Resetting published applications quits the applications without saving any unsaved data. All open published applications are closed, even applications that come from different RDS server farms.

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 7* or *Setting Up Published Desktops and Applications in Horizon 7* 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`.

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

What to do next

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

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 7* or *Setting Up Published Desktops and Applications in Horizon 7* document.

Prerequisites

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

Procedure

- Use the **Restart** command.

Option	Action
From the sidebar	When connected to a remote desktop, click the **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`.

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

What to do next

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

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