Using HTML Access

VMware Horizon HTML Access 4.0
VMware Horizon HTML Access 3.5
VMware Horizon HTML Access 3.4

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

Using HTML Access

This guide, *Using HTML Access*, provides information about installing and using the HTML Access feature of VMware Horizon™ 7 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 View server and in a remote desktop virtual machine so that end users can use a Web browser to access remote desktops.

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

Setup and Installation 1

Setting up a View 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 View deployment must meet certain software requirements.

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

Browser on client systems

- HTML Access 4.0 supports the following browsers.

Browser	Version
Chrome	47, 48
Internet Explorer	11
Safari	8, 9
Safari on mobile device	iOS 8, iOS 9

Browser	Version
Firefox	43, 44
Microsoft Edge	20, 25

- HTML Access 3.5 supports the following browsers.

Browser	Version
Chrome	43, 44
Internet Explorer	10, 11
Safari	7, 8 (Mobile Safari is not supported.)
Firefox	38, 39
Microsoft Edge	20

- HTML Access 3.4 supports the following browsers.

Browser	Version
Chrome	41, 42, 43
Internet Explorer	10, 11
Safari	7, 8 (Mobile Safari is not supported.)
Firefox	36, 37, 38

Client operating systems

- HTML Access 4.0 supports the following operating systems.

Operating System	Version
Windows	7 SP1 (32- and 64-bit)
Windows	8.x (32- and 64-bit)
Windows	10 (32- and 64-bit)
Mac OS X	10.10.x (Yosemite)
Mac OS X	10.11 (El Capitan)
iOS	8
iOS	9
Chrome OS	28.x and later

- HTML Access 3.5 supports the following operating systems.

Operating System	Version
Windows	7 SP1 (32- and 64-bit)
Windows	8.x (32- and 64-bit)
Windows	10 (32- and 64-bit)
Mac OS X	10.9.x (Mavericks)
Max OS X	10.10.x (Yosemite)
Chrome OS	28.x and later

- HTML Access 3.4 supports the following operating systems.

Operating System	Version
Windows	7 SP1 (32- and 64-bit)
Windows	8 (32- and 64-bit)
Mac OS X	10.9.x (Mavericks)
Max OS X	10.10.x (Yosemite)
Chrome OS	28.x and later

Note For HTML Access 3.5 and earlier, iOS devices such as phones and tablets are not supported. VMware recommends that you instead use Horizon Client for iOS. If you must support HTML Access on these devices, do not install HTML Access 3.x. Instead use HTML Access 2.6, which is the default version installed with View Connection Server 6.1.1.

Remote desktops

- HTML Access 4.0 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 View Agent" in version 7.0 of *View Installation*.
- HTML Access 3.5 requires View Agent 6.1 or later, and supports all the desktop operating systems that View 6.2 supports. For more information, see the topic "Supported Operating Systems for View Agent" in version 6.2 of *View Installation*.
- HTML Access 3.4 requires View Agent 6.1.1, and supports all the desktop operating systems that View 6.1 supports. For more information, see the topic "Supported Operating Systems for View Agent" in version 6.1 of *View Installation*.

Pool settings

HTML Access requires the following pool settings, in View 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 plan to use 3D applications or if end users will use a Macbook with Retina Display or a Google Chromebook Pixel, see "Screen Resolution," on page 38.
- The **HTML Access** setting must be enabled.

Configuration instructions are provided in "Prepare Desktops, Pools, and Farms for HTML Access," on page 12.

View Connection Server

View Connection Server with the HTML Access option must be installed on the server.

HTML Access 3.5 requires View Connection Server 6.2. When you install View Connection Server 6.2, you must select the **Install HTML Access** option.

HTML Access 3.4 requires View Connection Server 6.1.1. After you install or upgrade to View Connection Server 6.1.1 and verify that your remote desktops and RDS hosts are running View Agent 6.1.1, you must run a separate HTML Access installer on View Connection Server instances.

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

View Security Server: The same version as View Connection Server must be installed on the security server.

If client systems connect from outside the corporate firewall, VMware recommends that you use a security server. With a security server, client systems will 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, View 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 View

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 View Connection Server and Security Servers for HTML Access

Administrators must perform specific tasks so that end users can connect to remote desktops using a Web browser.

Before end users can connect to View Connection Server or a security server and access a remote desktop, you must install View Connection Server with the HTML Access component and install security servers.

Important For some versions of HTML Access, if you accidentally install View Connection Server without the HTML Access option and then later decide that you do want the HTML Access component, you must uninstall View Connection Server and then run the installer again with the HTML Access option selected. When you uninstall View Connection Server, do not uninstall the View LDAP configuration, called the AD LDS Instance VMwareVDMDS instance.

For other versions of HTML Access, you use a separate installer for HTML Access and so do not need to reinstall View Connection Server.

Table 1-1. Installer Requirements for HTML Access Versions

HTML Access Version	View Connection Server Version	Install Requirements
4.0	7.0	No separate HTML Access installer
3.5	6.2	No separate HTML Access installer
3.4	6.1.1	Separate installer
2.6	6.1, 6.1.1	No separate HTML Access installer

Following is a check list of the tasks you must perform in order to use HTML Access:

1 Install View Connection Server with the HTML Access option on the server or servers that will compose a View Connection Server replicated group.

By default, the HTML Access component is already selected in the installer. For installation instructions, see the *View Installation* documentation.

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 View HTML Access in the list.

2 For HTML Access 3.4 only, download the HTML Access Web Portal installer onto your View Connection Server instances and run the installer. For other versions, this step is not necessary because HTML Access is automatically installed in step 1.

The HTML Access 3.4 installer is available from the Horizon 6 version 6.1.1 download page (http://www.vmware.com/go/downloadview). The installer is named `VMware-Horizon-View-HTML-Access_X64-3.4.0-xxxxxx.exe`, where *xxxxxx* is the build number.

Note If you are performing an upgrade rather than a new installation, you must upgrade View Agent before you perform this step. Follow the steps in "Upgrading the HTML Access Software," on page 18.

3 If you use security servers, install View Security Server.

For installation instructions, see the *View Installation* documentation.

Important The version of View Security Server must match the version of View Connection Server.

4 Verify that each View Connection Server instance or security server has a security certificate that can be fully verified by using the host name that you enter in the browser.

For more information, see the *View Installation* documentation.

5 To use two-factor authentication, such as RSA SecurID or RADIUS authentication, verify that this feature is enabled on View Connection Server.

For more information, see the topics about two-factor authentication in the *View Administration* documentation.

6 If you use third-party firewalls, configure rules to allow inbound traffic to TCP port 8443 for all security servers and View Connection Server hosts in a replicated group, and configure a rule to allow inbound traffic (from View servers) to TCP port 22443 on remote desktops in the datacenter. For more information, see "Firewall Rules for HTML Access," on page 12.

After the servers are installed, if you look in View Administrator, you will see that the **Blast Secure Gateway** setting is enabled on the applicable View Connection Server instances and security servers. Also, the **Blast External URL** setting is automatically configured to use for the Blast Secure Gateway on the applicable View 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 this View Connection Server host or security server host. For more information, see "Set the External URLs for a View Connection Server Instance," in the *View Installation* documentation.

Note You can use HTML Access in conjunction with VMware Workspace Portal to allow users to connect to their desktops from an HTML5 browser. For information about installing Workspace Portal and configuring it for use with View Connection Server, see the Workspace Portal documentation. For information about pairing View Connection Server with a SAML Authentication server, see the *View Administration* documentation.

Firewall Rules for HTML Access

To allow client Web browsers to use HTML Access to make connections to security servers, View Connection Server instances, and remote desktops, 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 View Connection Server instance or security server, 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.

Table 1-2. Firewall Rules for HTML Access

Source	Default Source Port	Protocol	Target	Default Target Port	Notes
Client Web browser	TCP Any	HTTPS	Security server or View Connection Server instance	TCP 443	To make the initial connection to View, the Web browser on a client device connects to a security server or View Connection Server instance on TCP port 443.
Client Web browser	TCP Any	HTTPS	Blast Secure Gateway	TCP 8443	After the initial connection to View 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 View Connection Server instance to allow this second connection to take place.
Blast Secure Gateway	TCP Any	HTTPS	HTML Access agent	TCP 22443	If the Blast Secure Gateway is enabled, after the user selects a remote desktop, the Blast Secure Gateway connects to the HTML Access agent on TCP port 22443 on the desktop. This agent component is included when you install View 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 View desktop, the Web browser on a client device makes a direct connection to the HTML Access agent on TCP port 22443 on the desktop. This agent component is included when you install View Agent.

Prepare Desktops, Pools, and Farms for HTML Access

Before end users can access a remote desktop or application, administrators must configure certain pool and farm settings and install View Agent on remote 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 your vSphere infrastructure and View components meet the system requirements for HTML Access.

  See "System Requirements for HTML Access," on page 7.

- Verify that the HTML Access component is installed with View Connection Server on the host or hosts and that the Windows firewalls on View Connection Server instances and any security servers allow inbound traffic on TCP port 8443.

  See "Preparing View Connection Server and Security Servers for HTML Access," on page 10.

- If you use third-party firewalls, configure a rule to allow inbound traffic from View servers to TCP port 22443 on View desktops in the data center.
- Verify that the virtual machine you plan to use as a desktop source or RDS host has the following software installed: a supported operating system and VMware Tools.

  For a list of the supported operating systems, see "System Requirements for HTML Access," on page 7.

- Familiarize yourself with the procedures for creating pools and farms and entitling users. See the topics about creating pools and farms in *Setting Up Desktops and Applications in View*.
- To verify that the remote desktop or application is accessible to end users, verify that you have Horizon Client software installed on a client system. You will test the connection by using the Horizon Client software before attempting to connect from a browser.

  For Horizon Client installation instructions, see the Horizon Client documentation site at https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

- Verify that you have one of the supported browsers for accessing a remote desktop. See "System Requirements for HTML Access," on page 7.

Procedure

1. Install View Agent with the **HTML Access** option on all parent virtual machines for linked-clone pools, virtual machine templates for full clone pools, virtual machines for manual pools, and RDS hosts for desktop and hosted application pools.
2. For RDS desktops and applications, use View 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.
3. For single-session desktop pools, use View 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.

      The **HTML Access** setting does not appear in the Add Desktop Pool wizard when you create RDS desktop pools. Instead, you enable the **Allow HTML Access to desktops and applications on this farm** option when creating or editing the farm of RDS hosts.

   b. In the pool settings, verify that the **Max resolution of any one monitor** setting is **1920x1200** or higher.
4. After the pools are created, recomposed, or upgraded to use View Agent with the **HTML Access** option, use Horizon Client to log in to a desktop or application.

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

   For example:

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

   Be sure to use **`https`** in the URL.
6. On the Web page that appears, click **VMware Horizon HTML Access** and log in as you would with the Horizon Client software.
7. On the desktop and application selection page that appears, click an icon to connect.

You can now access a remote desktop or application from a Web browser when you are using a client device that does not or cannot have Horizon Client software installed in its operating system.

What to do next

For added security, if your security policies require that the Blast agent on the remote desktop uses an SSL certificate from a certificate authority, see "Configure HTML Access Agents to Use New SSL Certificates," on page 14.

Configure HTML Access Agents to Use New SSL Certificates

To comply with industry or security regulations, you can replace the default SSL certificates that are generated by the HTML Access Agent with certificates that are signed by a Certificate Authority (CA).

When you install the HTML Access Agent on View desktops, the HTML Access Agent service creates default, self-signed certificates. The service presents the default certificates to browsers that use HTML Access to connect to View.

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 View desktop. You must also set a registry value on each desktop that allows the HTML Access Agent to use the new certificate.

If you replace the default HTML Access Agent certificates with CA-signed certificates, VMware recommends that you configure a unique certificate on each 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 would result in hundreds or thousands of desktops with identical certificates.

Procedure

1 Add the Certificate Snap-In to MMC on a View Desktop on page 15

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 View desktops where the HTML Access Agent is installed.

2 Import a Certificate for the HTML Access Agent into the Windows Certificate Store on page 15

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 desktop where the HTML Access Agent is installed.

3 Import Root and Intermediate Certificates for the HTML Access Agent on page 16

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 on page 17

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 desktop on which you replace the default certificate with a CA-signed certificate.

Add the Certificate Snap-In to MMC on a View 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 View 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 View 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," on page 15.

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 desktop where the HTML Access Agent is installed.

Prerequisites

- Verify that the HTML Access Agent is installed on the View desktop.
- Verify that the CA-signed certificate was copied to the desktop.
- Verify that the Certificate snap-in was added to MMC. See "Add the Certificate Snap-In to MMC on a View Desktop," on page 15.

Procedure

1 In the MMC window on the View 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," on page 16.

Configure the appropriate registry key with the certificate thumbprint. See "Set the Certificate Thumbprint in the Windows Registry," on page 17.

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 View 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 your server certificate was signed by an intermediate CA, 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," on page 17.

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 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," on page 15.

Procedure

1. In the MMC window on the View 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. 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.

When a user connects to a 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/apps/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.

Upgrading the HTML Access Software

For most versions of HTML Access, upgrading involves simply upgrading Connection Servers and View Agent. For HTML Access 3.4, you must also install HTML Access separately on the Connection Servers..

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.

Table 1-3. Installer Requirements for HTML Access Versions

HTML Access Version	View Connection Server Version	Install Requirements
4.0	7.0	No separate HTML Access installer
3.5	6.2	No separate HTML Access installer
3.4	6.1.1	Separate installer
2.6	6.1, 6.1.1	No separate HTML Access installer

For HTML Access that do not have a separate installer, when you upgrade Connection Server, HTML Access is automatically installed or upgraded. You do not need to install HTML Access separately.

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.

Upgrading to HTML Access 3.4

Upgrading to HTML Access 3.4 requires that you install HTML Access on the Connection Servers separately. Following is a check list of the tasks you must perform:

1 Upgrade to View Connection Server 6.1.1 with the HTML Access option on the server or servers that compose a View Connection Server replicated group.

   By default, the HTML Access component is already selected in the installer.

   When you install View Connection Server 6.1.1 interactively, the version of HTML Access that is installed is HTML Access 2.6. At this stage, you cannot use remote (hosted) applications with HTML Access. Users can continue to use HTML Access 2.6 to connect to desktops running View Agent 6.1.

2 If you use security servers, upgrade to View Security Server 6.1.1.

The version of View Security Server must match the version of View Connection Server.

3 Upgrade to View Agent 6.1.1 on all RDS hosts and VDI machines, including parent and template virtual machines and the virtual machines in your desktop pools.

With this step, you upgrade View Agent before you upgrade HTML Access on your View Connection Server instances. If you upgraded HTML Access on your servers first, your end users would not be able to connect to older View Agent desktops (version 6.1 or earlier) from their Web clients.

Note The View Agent installer now includes the HTML Access agent component that had been included in the Remote Experience Agent for releases prior to Horizon 6.0 (with View). The Remote Experience Agent was part of the Horizon View Feature Pack. To upgrade features that were installed with the Remote Experience Agent, you can simply run the View Agent installer. This installer removes the Remote Experience Agent before performing the upgrade. If, for some reason, you decide to manually remove the Remote Experience Agent, be sure to do so before you run the installer for the new version of View Agent.

4 From the Horizon 6 version 6.1.1 download page (http://www.vmware.com/go/downloadview), download the HTML Access Web Portal installer onto your View Connection Server instances and run the installer.

The installer is named `VMware-Horizon-View-HTML-Access_X64-3.4.0-xxxxxx.exe`, where *xxxxxx* is the build number.

Important For HTML Access 3.4, whenever you upgrade View Connection Server, you must run the HTML Access installer after the View Connection Server upgrade. For example, after you upgrade View Connection Server to a new patch or maintenance release, the HTML Access Web Portal page might not display the HTML Access icon. If no new version of HTML Access is available, use the Uninstall a Program feature of Windows to uninstall HTML Access and then reinstall the same version.

Uninstall HTML Access from View Connection Server

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

Procedure

1 On the View Connection Server hosts where HTML Access is installed, open the Uninstall a Program applet provided by the Windows Control Panel.

2 Select the HTML Access program and click **Uninstall**.

HTML Access Version	HTML Access Program Name
4.0	VMware Horizon 7 HTML Access
3.5	VMware Horizon 6 HTML Access
3.4	VMware Horizon View HTML Access

3 (Optional) In the Windows Firewall for that 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 this View Connection Server host.

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 View 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 View 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 View Connection Server can opt in while running the View Connection Server installation wizard, or an administrator can set an option in View Administrator after the installation.

Table 1-4. 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	4.0.0-*build_number*
Client binary architecture	`<client-arch>`	No	Examples include the following values: ■ browser ■ arm
Native architecture of the browser	`<browser-arch>`	No	Examples include the following values: ■ Win32 ■ Win64 ■ MacIntel ■ iPad
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)

Table 1-4. Client Data Collected for the Customer Experience Improvement Program (Continued)

Description	Field name	Is This Field Made Anonymous ?	Example Value
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 portal page shows both an icon for downloading and installing the native Horizon Client and an icon for connecting through HTML Access. In some cases, however, you might want to have the links point to an internal Web server, or you might want to make specific client versions available on your own server. You can reconfigure the page to point to a different URL.

You can make installer links for specific client operating systems. 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 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 View Connection Server 6.0 or later. With Horizon 6 or later, the HTML Access component is automatically installed during an upgrade of View Connection Server.

If you already installed the HTML Access component separately for View 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 View 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.

Note Customizations for View 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`.

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 View Connection Server, as described in the next step.
	■ 32-bit Windows installer:
	`link.win32=https://server/downloads/VMware-Horizon-Client.exe`
	■ 64-bit Windows installer:
	`link.win64=https://server/downloads/VMware-Horizon-Client.exe`
	■ Linux installer:
	`link.linux=https://server/downloads/VMware-Horizon-Client.tar.gz`
	■ Mac OS X installer:
	`link.mac=https://server/downloads/VMware-Horizon-Client.dmg`
	■ iOS installer:
	`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS.zip`
	■ Android installer:
	`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS.apk`
	■ Installer for an unknown OS (for example, you could use this property for the Chrome client installer):
	`link.unknown=https://server/downloads/VMware-Horizon-Client-AndroidOS-arm-ARC.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 from the previous step. For example, to place the files in a `downloads` directory on the View 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 View 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 with specific configuration options.

You can simplify the process of connecting to a remote desktop 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 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 the user, desktop, and desktop 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 desktop 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* guide for each type of client system.

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

userName The Active Directory user who is connecting to the remote desktop.

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.

desktopId The desktop display name. This name is the one specified in View Administrator when the desktop pool was created. If the display name has a space in it, the browser will automatically use **`%20`** to represent the space.

action

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

Value	Description
`browse`	Displays a list of available desktops hosted on the specified server. You are not required to specify a desktop when using this action.
`start-session`	Launches the specified desktop. If no action query is provided and the desktop name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified desktopn. Unsaved data is lost. Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC.
`logoff`	Logs the user out of the guest operating system in the remote desktop.

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, launch 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. Note that queries are not case-sensitive. For example, you can use **`domainName`** or **`domainname`**.

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

The HTML Access Web client is launched and connects to the `view.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://view.mycompany.com/?desktopId=Primary%20Desktop&action=start-session`

The HTML Access Web client is launched and connects to the `view.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.

3 `https://view.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 View 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.

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

The HTML Access Web client is launched and connects to the `view.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 View administrator has allowed end users to reset their machines.

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

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

</body>
</html>
```

Configure Group Policy Settings for HTML Access

You can configure group policy settings for HTML Access by adding the group policy template file `vdm_blast.adm` to the domain policy. This template is for the VMware Blast display protocol, which is the only display protocol that HTML Access uses.

Before HTML Access 4.0 and Horizon 7.0, only HTML Access uses the VMware Blast display protocol. Starting with HTML Access 4.0 and Horizon 7.0, VMware Blast is available to all Horizon Clients.

For HTML Access 4.0 and Horizon 7.0, you configure VMware Blast group policy settings for HTML Access and all other Horizon Clients. For more information, see "Configuring Policies for Desktop and Application Pools" and "VMware Blast Policy Settings" in the *Setting Up Desktop and Application Pools in View* document.

If you have HTML Access 3.5 or earlier and Horizon 6.2.x or earlier, use the following procedure to configure group policy settings for HTML Access.

Prerequisites

- Familiarize yourself with the information about setting up View group policy settings in Active Directory. See "Configuring Policies for Desktop and Application Pools" in *Setting Up Desktops and Applications in View*.
- Familiarize yourself with the HTML Access group policy settings. See "Group Policy Settings for HTML Access," on page 29.

Procedure

1 Download the View GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

The file is named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.

2 Copy the file to your Active Directory server and unzip the file.

The HTML Access GPOs are included in the `vdm_blast.adm` template file.

3 On the Active Directory server, edit the GPO.

a Select **Start > Administrative Tools > Group Policy Management**.

b Expand your domain, right-click the GPO that you created for the group policy settings, and select **Edit**.

The Group Policy Object Editor window appears.

4 In the Group Policy Object Editor, right-click **Administrative Templates** under **Computer Configuration** and then select **Add/Remove Templates**.

5 Click **Add**, browse to the `vdm-blast.adm` file, and click **Open**.

6 Click **Close** to apply the policy settings in the template file to the GPO.

The VMware Blast folder appears in the left pane under **Administrative Templates > Classic Administrative Templates**.

7 Configure the HTML Access group policy settings.

8 Make sure your policy settings are applied to the remote desktops.

a Run the `gpupdate.exe` command on the desktops.

b Restart the desktops.

Group Policy Settings for HTML Access

Group policy settings for HTML Access are specified in the template file `vdm_blast.adm`. This template is for the VMware Blast display protocol, which is the only display protocol that HTML Access uses.

For HTML Access 4.0 and Horizon 7.0, the VMware Blast group policy settings are described in "VMware Blast Policy Settings" in the *Setting Up Desktop and Application Pools in View* document.

If you have HTML Access 3.5 or earlier and Horizon 6.2.x or earlier, the following table describes group policy settings that apply to HTML Access. Note that starting with Horizon 7.0, more VMware Blast group policy settings are available.

Table 2-2. Group Policy Settings for HTML Access 3.5 and Earlier

Setting	Description
Screen Blanking	Controls whether the remote virtual machine can be seen from outside of View during an HTML Access session. For example, an administrator might use vSphere Web Client to open a console on the virtual machine while a user is connected to the desktop through HTML Access. When this setting is enabled or not configured, and someone attempts to access the remote virtual machine from outside of View while an HTML Access session is active, the remote virtual machine displays a blank screen. When this setting is disabled, under the preceding conditions, the remote virtual machine displays the active View desktop session to the second remote accessor.
Session Garbage Collection	Controls the garbage collection of abandoned remoting sessions. When this setting is enabled, you can configure the garbage collection interval and threshold. The interval controls how often the garbage collector runs. You set the interval in milliseconds. The threshold determines how much time must pass after a session is abandoned before it becomes a candidate for deletion. You set the threshold in seconds.
Audio playback	Controls whether audio playback is allowed on the remote desktop. By default, this setting is enabled.
Image Quality	Controls the image quality of the remote display. There are three image quality profiles, low, medium, and high. The encoder tries to use the best quality level possible, given the constraints of available bandwidth, recent frame-rate, and the size of the region that has recently changed in the current frame. The encoder keeps track of which regions of the client screen are currently low- or medium-quality and incrementally improves those areas to high quality. When this setting is enabled, you can separately change the low-, medium-, and high-quality JPEG settings to different values. The actual JPEG quality levels used at low, medium, and high settings are individually configurable as numbers between 0 and 100. Chroma subsampling is enabled according to the JPEG quality level chosen. Whenever JPEG quality set to 80 or higher, chroma-subsampling is turned off and the ratio is set to the highest available value, YUV-4:4:4. For JPEG quality set to 79 or below, the ratio is set to YUV-4:2:0. ■ **Low JPEG Quality**. By default, this value is 25. You can also set the low JPEG chroma subsampling to various ratios. By default, the low ratio is set to the lowest available value, 4:1:0. ■ **Mid JPEG Quality**. By default, this value is 35. You can also set the low JPEG chroma subsampling to various ratios. By default, the low ratio is set to the lowest available value, 4:2:0. ■ **High JPEG Quality**. By default, this value is 90.You can also set the high JPEG chroma subsampling to various ratios. By default, the low ratio is set to the highest available value, 4:4:4.
Configure clipboard redirection	Determines the direction in which clipboard redirection is allowed. Only text can be copied and pasted. You can select one of these values: ■ **Enabled client to server only** (That is, allow copy and paste only from the client system to the remote desktop.) ■ **Disabled in both directions** ■ **Enabled in both directions** ■ **Enabled server to client only** (That is, allow copy and paste only from the remote desktop to the client system.) This setting applies to View Agent or Horizon Agent only. When this setting is disabled or not configured, the default value is **Enabled client to server only**.
HTTP Service	Allows you to change the secured (HTTPS) TCP port for the Blast Agent service. The default port is 22443. Enable this setting to change the port number. If you change this setting, you must also update settings on the firewall of the affected remote desktops (where View Agent or Horizon Agent is installed).

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
RSA SecurID or RADIUS	X	X	X	X	X
Single sign-on	X	X	X	X	X
RDP display protocol					
PCoIP display protocol					
VMware Blast display protocol	X	X	X	X	X

Table 3-1. Features Supported Through HTML Access (Continued)

Feature	Windows 7 Desktop	Windows 8.x Desktop	Windows 10 Desktop	Windows Server 2008 R2 Desktop	Windows Server 2012 R2 Desktop
USB redirection					
Real-time audio-video (RTAV)					
Wyse MMR					
Windows Media MMR					
Virtual printing					
Location-based printing	X	X	X	X	X
Smart cards					
Multiple monitors					

For descriptions of these features and their limitations, see the *View 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.

The following table describes which features 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 Installed

Feature	Windows Server 2008 R2 RDS Host on a Physical Machine	Windows Server 2008 R2 RDS Host on a Virtual Machine	Windows Server 2012 or 2012 R2 RDS Host on a Physical Machine	Windows Server 2012 or 2012 R2 RDS Host on a Virtual Machine
RSA SecurID or RADIUS	X (HTML Access 4.0 only)	X	X (HTML Access 4.0 only)	X
Single sign-on	X (HTML Access 4.0 only)	X	X (HTML Access 4.0 only)	X
VMware Blast display protocol	X (HTML Access 4.0 only)	X	X (HTML Access 4.0 only)	X
Virtual printing				
Location-based printing		X		X
Multiple monitors				

Note For HTML Access 3.5 and earlier, the RDS host must be a virtual machine. Starting with HTML Access 4.0, it can also be a physical machine.

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

Internationalization

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

For information about which language packs you must use in the client system, browser, and remote desktop, see "International Keyboards," on page 38.

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 the credentials that you need to log in, such as 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 would use `mycompany` rather than `mycompany.com`.

Procedure

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

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

Connections to View Connection Server always use SSL. The default port for SSL connections is 443. If View Connection Server is not configured to use the default port, use the format shown in this example: **`view.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 Click the **VMware Horizon HTML Access** icon.

3 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.

4 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.

5 In the Login dialog box, enter your Active Directory user name and password, select a domain name, and click **Login**.

6 (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.

7 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," on page 34.

Trust a Self-Signed Root Certificate

In some cases, when connecting to a remote desktop or application for the first time, you might be prompted by the browser to accept the self-signed certificate used by the remote machine. You must trust the certificate before the connection can be made to the remote desktop or application.

Most browsers will give you the option to permanently trust the self-signed certificate. If you do not choose to permanently trust the certificate, you must verify the certificate every time you restart your browser. If you are using a Safari browser, you must permanently trust the security certificate in order to establish the connection.

Procedure

1 If your 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 is used by your company.

You might need to contact your View administrator for assistance. For example, in a Chrome browser, 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 is used by your company.

You might need to contact your View 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 permanently trust the certificate.

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 application is launched.

Shortcut Key Combinations

Regardless of the language used, some key combinations cannot be sent to the to a remote desktop or application.

Web browsers allow some key presses and key combinations to be sent to both the client 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 using the key combinations to select, copy, and paste text. To enable this feature, you can 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 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 located at the top of the sidebar.

- Caps Lock+*modifier_key* (such as Alt or Shift)
- Function keys, if you are using a Chromebook
- Windows key combinations

The following Windows key combinations do work in remote desktops if you enable the Windows key for desktops. To enable this key, you can 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 remote applications provided by RDS hosts. They do work as listed for Windows Server 2008 R2 and Windows Server 2012 R2 single-user desktops and session-based desktops provided by an RDS host.

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

Table 3-3. Windows Key Shortcuts for Windows 10 Remote Desktops

Keys	Action	Limitations
Win	Open or close Start.	
Win+A	Open Action center.	
Win+E	Open File Explorer.	

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

Keys	Action	Limitations
Win+G	Open game bar when a game is open.	
Win+H	Open the Share charm.	
Win+I	Open the Settings charm.	
Win+K	Open the Connection quick action.	
Win+M	Minimize all windows.	
Win+R	Open the Run dialog box.	
Win+S	Open Search.	
Win+X	Open the **Quick Link** menu.	
Win+, (comma)	Temporarily peek at the 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 desktop.	Does not work in Safari browsers.
Win+Alt+Num	Open the 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 browsers.
Win	Show or hide the Start screen.	
Win+B	Set focus on the notification area.	
Win+C	Open the Charms panel.	
Win+D	Display and hide the desktop.	Does not work in Safari browsers. Workaround: Press Command-D on Macs.
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	Open the Search charm to search everywhere or within the open app, if the app supports app search.	
Win+R	Open the Run dialog box.	
Win+S	Open the Search charm to search Windows and the Web.	
Win+X	Open the **Quick Link** menu.	
Win+Z	Show the commands available in the app.	
Win+, (comma)	Temporarily display the desktop, as long as you continue pressing the keys.	**Note** Does not work on Windows 2012 R2 operating systems.
Win+Pause	Display the System Properties dialog box.	There is no Pause key on Chromebooks or Macs.

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

Keys	Action	Limitations
Win+Shift+M	Restore minimized windows on the desktop.	Does not work in Safari browsers. Workaround: Press Command-D on Macs.
Win+Alt+Num	Open the 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 desktop window.	Does not work on a Chromebook.
Win+Left Arrow	Maximize the app or desktop window to the left side of the screen.	Does not work on a Chromebook.
Win+Right Arrow	Maximize the app or desktop window to the right side of the screen.	Does not work on a Chromebook.
Win+Home	Minimize all but the active 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 desktop window to the top and bottom of the screen.	Does not work on a Chromebook.
Win+Shift+Down Arrow	Restore the desktop window vertically, while maintaining width, after pressing Win+Shift+Up to stretch the window, or minimize active 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	Display the System Properties dialog box.	There is no Pause key on Chromebooks or Macs.
Win+D	Display and hide the desktop.	Does not work in Safari browsers. Workaround: Press Command-D on Macs.
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 desktop window to the left side of the screen.	Does not work on a Chromebook.
Win+Right Arrow	Maximize the app or desktop window to the right side of the screen.	Does not work on a Chromebook.
Win+Home	Minimize all but the active desktop window.	Does not work in Safari browsers.
Win+Shift+Up Arrow	Stretch the desktop window to the top and bottom of the screen.	Does not work on a Chromebook.
Win+G	Cycle through running 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, and Korean.

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

Screen Resolution

If the View 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 appears in the Settings window only if you are using a high-resolution display.)

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.

With Horizon Client 3.4, when 3D rendering is enabled, the maximum number of monitors is 1 and the maximum resolution is 1920 x 1200.

With Horizon Client 3.5 and 4.0, 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.

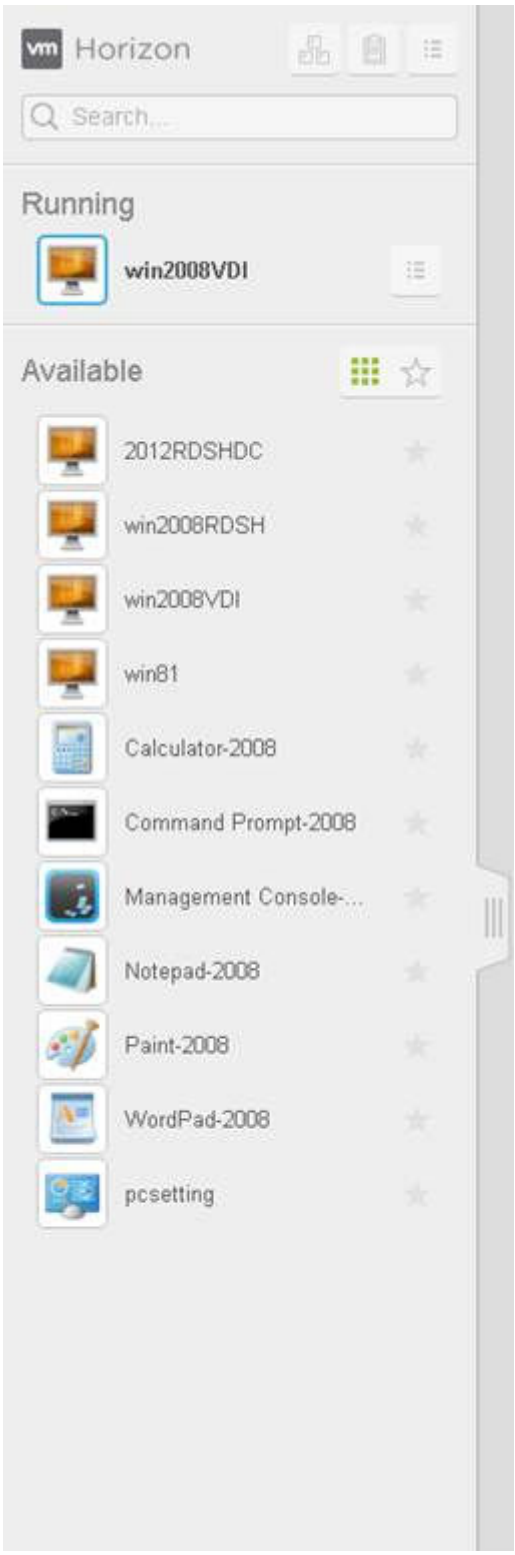
Important Estimating the amount of VRAM you need for the VMware Blast display protocol is similar to estimating how much VRAM is required for the PCoIP display protocol. For guidelines, see the section "RAM Sizing for Specific Monitor Configurations When Using PCoIP" of the topic "Estimating Memory Requirements for Virtual Desktops," in the *View Architecture Planning* document.

Using the Sidebar

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

When you access a remote application or desktop, the sidebar appears on the left side of the screen. Click the sidebar tab to display or hide the sidebar. You can also slide the tab up and down.

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



Click the expander arrow next to a running application to see the list of documents opened from that application. Note, however, that if you have, for example, two Excel documents open from separate Excel programs hosted on two different servers, the Excel application will be listed twice in **Running** list in the sidebar.

From the sidebar, you can perform several actions.

Table 3-7. Sidebar Actions

Action	Procedure
Show the sidebar	When you have a remote application or desktop open, click the sidebar tab. When the sidebar is open, you can still perform actions in the application or desktop window.
Hide the sidebar	Click the sidebar tab.
Launch a remote application or desktop	Click the name of an application or desktop under **Available** in the sidebar. The desktops are listed first.
Search for a remote application or desktop	■ Click in the **Search** box and begin typing the name of the application or desktop. ■ To launch an application or desktop, click the name of the application or desktop 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 applications and desktops	Click the gray star next to the name of the desktop or application in the **Available** list in the sidebar. You can then click the **Show Favorites** toolbar button (star icon) next to **Available** to display a list of only favorites.
Switch between applications or desktops	Click the application file name or desktop name in the **Running** list in the sidebar.
Open Copy & Paste panel	Click the **Copy & Paste** button at the top of the sidebar. Use this button for copying text to and from applications on your local client system. For more information, see "Copying and Pasting Text," on page 42. On iOS Safari, this button is not available because the copy and paste feature is not supported.
Enable Command-A, Command-C, Command-V, and Command-X	This option appears in the Settings window only if you are using a Mac. Click the **Open Menu** toolbar button at the top of the sidebar and then click **Settings**. When this feature is enabled, The Command key on the Mac is mapped to the Ctrl key on the remote Windows desktop or application. For example, pressing Command-A on a Mac keyboard will have the effect of pressing Ctrl+A on the remote Windows desktop or application.
Close a running desktop	Click the **Open Menu** button next to the desktop name in the **Running** list in the sidebar and select the action you want: ■ Select **Close** to disconnect from the desktop without logging off from its operating system. Note, however, that your View administrator can configure your desktop to automatically log off when disconnected. In that case, unsaved changes in open applications will be lost. ■ Select **Log off** to log off from the operating system and disconnect from the desktop. Any unsaved changes in open applications will be lost.
Close a running application	Click the **X** next to the file name under the application name in the **Running** list in the sidebar. Click the **X** next to the application name to quit the application and close all open files for that application. You are prompted to save changes made to the files.
Reset a desktop	Click the **Open Menu** button next to the desktop name in the **Running** list in the sidebar and select **Reset**. Any files that are open on the remote desktop will be closed without being saved first. You can reset a desktop only if your administrator has enabled this feature.
Reset all running applications	Click the **Open Menu** toolbar button at the top of the sidebar, click **Settings**, and click **Reset**. 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," on page 35.
Send Ctrl+Alt+Del to current work area	Click the **Send Ctrl+Alt+Del** toolbar button at the top of the sidebar.
Disconnect from the server	Click the **Open Menu** toolbar button at the top of the sidebar, or else click the Horizon logo at the top of the sidebar, and click **Log off**.

Table 3-7. Sidebar Actions (Continued)

Action	Procedure
Use high-resolution mode on machines with a high-resolution display (such as Retina Macbook Pro)	Click the **Open Menu** toolbar button at the top of the sidebar, click **Settings**, and turn on **High Resolution Mode**. (This option appears in the Settings window only if you are using a high-resolution display.)
Call out or dismiss the soft keyboard	(iOS Safari only) Click the keyboard icon at the top of the sidebar. You can also call out or dismiss the soft keyboard by tapping the screen with three fingers.
Display help topics	Click the **Open Menu** toolbar button at the top of the sidebar, or else click the Horizon logo at the top of the sidebar, and click **Help**.
Display the About VMware Horizon box	Click the **Open Menu** toolbar button at the top of the sidebar, or else click the Horizon logo at the top of the sidebar, and click **About**.

Sound

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

By default, sound playback is enabled for remote desktops and applications, although your View administrator can set a policy to disable sound playback.

Take into account the following guidelines:

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

Copying and Pasting Text

It is possible to copy text to and from remote desktops and applications. Your View administrator can set this feature so that copy and paste operations are allowed only from your client system to a remote desktop or application, or only from a remote desktop or application to your client system, or both, or neither.

Administrators configure the ability to copy and paste by using group policy objects (GPOs) that pertain to View Agent or Horizon Agent in remote desktops. For more information, see "Group Policy Settings for HTML Access," on page 29.

You can copy up to 1MB of text, including any Unicode non-ASCII characters. You can copy text from your client system to a remote desktop or 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 your client computer.

Note The copy and paste feature is not supported on iOS Safari.

Use the Copy and Paste Feature

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

This procedure describes how to use the Copy & Paste window to copy text from your local client system to a remote application or how to copy 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.

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 View 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 else the administrator must configure another policy that allows copying and pasting. For more information, see "Group Policy Settings for HTML Access," on page 29.

Procedure

- To copy text from your client system to the remote desktop or application:
  a. Copy the text in 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 will be replaced when you paste in the newly copied text.

     Note If copying is disabled, a message appears at the bottom of the Copy & Paste window.
  c. Press Ctrl+V (or Command-V on Macs) to paste the text into the Copy & Paste window.

     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 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."`

     Note If copying is disabled, a message appears at the bottom of the Copy & Paste window.
  c. Click in the Copy & Paste window and press Ctrl+C (or Command-C on Macs) to copy again.

     The text will not be 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.

Log Off or Disconnect

With some configurations, if you disconnect from a remote desktop without logging off, applications in the desktop can remain open. You can also disconnect from a server and leave remote applications running.

Procedure

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

Option	Action
From the desktop and application selector screen, before connecting to a remote desktop or application	Click the **Log Out** toolbar button in the upper-right corner of the screen.
From the sidebar when connected to a remote desktop or application	Click the **Log off from VMware Horizon** toolbar button at the top of the sidebar.

- Close a remote application.

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

- Log off or disconnect from a remote desktop.

Option	Action
From within the desktop OS	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 desktop name in the **Running** list in the sidebar and select **Log Off**. Files that are open on the remote desktop will be closed without being saved first. To disconnect without logging off, click the **Open Menu** toolbar button next to the desktop name in the **Running** list and select **Close**. **Note** Your View administrator can configure your desktop to automatically log off when disconnected. In that case, any open applications in your desktop are closed.
Using an URI	To log off, use the URI `https://`*`ConnectionServerFQDN`*`?desktopId=`*`desktop_name`*`&action=logoff`.

Reset a Remote Desktop or Application

You might need to reset a desktop or application if the application or desktop operating system stops responding. Resetting a remote desktop shuts down and restarts the desktop. Resetting your remote applications quits the applications. Unsaved data is lost.

Resetting a remote desktop is the equivalent of pressing the Reset button on a physical PC to force the PC to restart. Any files that are open on the remote desktop will be closed without being saved first.

Resetting applications is the equivalent of quitting all remote applications without saving any unsaved data. All open applications are closed, even if the applications come from different RDS server farms.

You can reset a remote desktop only if your administrator has enabled this feature.

Procedure

- Use the **Reset** command.

Option	Action
Reset applications from the application selector screen	From the desktop and application selector screen, before connecting to a remote desktop or application, to reset all running applications, click the **Settings** toolbar button in the upper-right corner of the screen, anc click **Reset**.
Reset a 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 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 desktop using an URI	To reset a desktop, use the URI `https://`*`ConnectionServerFQDN`*`?desktopId=`*`desktop_name`*`&action=reset`.

For a remote desktop, the operating system in the remote desktop is rebooted. The client disconnects from the desktop. For remote applications, the applications are quit.

What to do next

Wait an appropriate amount of time for system startup before attempting to connect to the remote desktop.

Index

V

W