Using HTML Access

March 2015

VMware Horizon 6

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001116-06

vmware®

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

http://www.vmware.com/support/

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™ with View™ 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.

Browser on client system

The following Web browsers are supported.

	Chrome	Internet Explorer	Safari	Mobile Safari	Firefox
HTML Access 2.6	38 and 39	10 and 11	6.2, 7, and 8	iOS 7 or later	33
HTML Access 2.5	35, 36, and 37	9 (limited support), 10, and 11	6.1.3 and 7	iOS 7 or later	30 and 31
HTML Access 2.4	33 and 34	9 (limited support), 10, and 11	6.1.3 and 7	iOS 7 or later	28 and 29

Client operating systems

- Windows XP SP3 (32-bit)
- Windows 7 SP1 or no SP (32- or 64-bit)
- Windows 8.x Desktop (32- or 64-bit)

- Windows Vista SP1 or SP2 (32-bit)
- Mac OS X Snow Leopard (10.6.8)
- Mac OS X Lion (10.7)
- Mac OS X Mountain Lion (10.8)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- iPad with iOS 7.0 or later (therefore, iPad 1 is not supported)
- Chrome OS 28.*x* or later

Remote desktop

The following software must be installed in the virtual machine that the end user will access:

- Operating systems for single-user View desktops: If you have View Agent 6.0.x, Windows XP SP3 (32-bit) and Windows Vista (32-bit) are supported. If you have View Agent 6.0.x or later, Windows 7 (32- or 64-bit), and Windows Server 2008 R2 are also supported. If you have View Agent 6.0.1 or later, Windows 8 (32- or 64-bit) and Windows 8.1 (32- or 64-bit) remote desktops are also supported. If you have View Agent 6.1 or later, Windows Server 2012 R2 is also supported.
- Operating systems for session-based View desktops on RDS hosts: If you have View Agent 6.0.2 or later, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 are supported.
- View Agent: HTML Access 2.6 requires View Agent 6.1 or View Agent 6.0.2. HTML Access 2.5 requires View Agent 6.0.1. HTML Access 2.4 requires View Agent 6.0.

  Installation instructions are provided in the *Setting Up Desktops and Applications in View*.

IMPORTANT The remote desktop must be a virtual machine. Although you can install View Agent on a physical machine, the Blast protocol used with HTML Access cannot access a physical machine. View Agent must be installed on a virtual machine.

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 17.63MB 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 35.
- The **HTML Access** setting must be enabled.

Configuration instructions are provided in "Prepare Remote Desktops and Pools," on page 12.

View Connection Server

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

- HTML Access 2.6 requires View Connection Server 6.1 or View Connection Server 6.0.x. If you have View Connection Server 6.0.x, you must also run the separate HTML Access installer on the server.

- HTML Access 2.5 requires View Connection Server 6.0.1. With this version of View Connection Server, HTML Access 2.5 is built in.
- HTML Access 2.4 requires View Connection Server 6.0. With this version of View Connection Server, HTML Access 2.4 is built in.

By default, the HTML Access component is already selected in the View Connection Server installer. Installation instructions are provided in the *View Installation* document.

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

Blast

When you use a Web browser to access a remote desktop, the Blast protocol is used rather than PCoIP or Microsoft RDP. 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
2.6	6.1	No separate installer
2.6	6.0.x	Separate HTML Access installer
2.5	6.0.x	No separate installer
2.4	6.0	No separate 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 If a separate HTML Access installer is required, on the View Connection Server host or hosts in a replicated group, download the HTML Access installer from the View Downloads page, and run the installer.

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

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 11.

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.

Table 1-2. Firewall Rules for HTML 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, 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 Remote Desktops and Pools

Before end users can access a remote desktop, administrators must configure certain pool settings and install View Agent on remote desktop virtual machines 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 datacenter.

- Verify that the virtual machine you plan to use as a desktop source 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 desktop pools and entitling users to desktops. See the topics about creating desktop pools in *Setting Up Desktops and Applications in View*.

- To verify that the remote desktop 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 On the parent virtual machine you plan to use as a source for a linked-clone pool, or on the virtual machine template that you plan to use for a full-clone pool, install View Agent.

The View Agent software includes an HTML Access component.

2 If you are creating a linked-clone pool, use vSphere Client to take a snapshot of the parent virtual machine.

3 Use View Administrator to create a pool from this virtual machine, and enable the **HTML Access** setting when completing the Add Desktop Pool wizard.

HTML Access is supported for virtual machine desktop pools and, if you have HTML Access 2.6, session-based desktop pools on RDS hosts. Remote, hosted applications on RDS hosts are not supported.

4 In the pool settings, verify that the **Max resolution of any one monitor** setting is **1920x1200** or higher.

5 Entitle users to this pool.

6 Use Horizon Client to log in to a desktop from this pool.

With this step, before you attempt to use HTML Access, you verify that the pool is working correctly.

7 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.

8 On the Web page that appears, click **VMware Horizon HTML Access** and log in as you would with the Horizon Client software.

9 On the desktop selection page that appears, click a desktop icon.

You can now access a remote desktop 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 13.

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 Horizon View Desktop on page 14

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 16

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 Horizon 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 Horizon View Desktop," on page 14.

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 16.

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 16.

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.

Upgrading the HTML Access Software

Install the latest version of HTML Access to obtain the latest updates and improvements.

To upgrade to the latest version of HTML Access, you must verify that the latest version of View Connection Server is installed on all the instances in a replicated group.

For some releases of HTML Access, a separate HTML Access installer is required because no corresponding maintenance release of View Connection Server is released. The following table shows which versions of HTML Access require a separate installer.

Table 1-3. Installer Requirements for HTML Access Versions

HTML Access Version	View Connection Server Version	Install Requirements
2.6	6.1	No separate installer
2.6	6.0.x	Separate HTML Access installer
2.5	6.0.x	No separate installer
2.4	6.0	No separate installer

To complete the upgrade of HTML Access, you also must run the View Agent installer on the applicable parent virtual machines or virtual machine templates for your desktop pools. The version of View Agent should correspond to the version of View Connection Server.

IMPORTANT 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.

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 **VMware Horizon View HTML Access** and click **Uninstall**.

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	2.6.0-*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

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

Description	Field name	Is This Field Made Anonymous ?	Example Value
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
Browser's internal version string	<browser_version>	No	Examples include the following values: ■ 7.0.3 (for Safari), ■ 29.0 (for Firefox)
Browser's core implementation	<browser_core>	No	Examples include the following values: ■ Chrome ■ Safari ■ Firefox ■ MSIE (for Internet Explorer)
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`

Change the URL for the Help link in the login screen and desktop selector screen	`link.help` By default, this link points to a help system hosted on the VMware Web site. The Help link appears in the upper-right corner of the screen. For the HTML Access login screen and the desktop selector screen, the Help link is a question mark icon.

3 (Optional) Change the URL for the Help link in the Horizon Client toolbar.

After you are logged in to a desktop, the Help link is a **Help** command in the drop-down menu on the right end of the client. To change the URL for this link, edit the `HELP_URL_VIEW` property in the appropriate file in the appropriate folder.

Option	Description
For HTML Access 2.6	On the View Connection Server host, the file is located in: *ViewConnectionServer-InstallDir*`\webapps\portal\desktop\locale\`
For HTML Access 2.4 and 2.5	On the remote desktop operating system (where View Agent is installed), the file is located in: `C:\Program Files\VMware\VMware Blast\web\locale\`

For example, if you are using English, edit the `HELP_URL_VIEW` property in the `en.json` file.

4 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` folder 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`*.

5 Restart the View Web Component service.

Enable Desktops from RDS Hosts

With HTML Access 2.6, administrators can configure View Connection Server to allow a Microsoft RDS (Remote Desktop Sessions) host to provide remote session-based desktops.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version. If you use a Windows Server 2012 RDS host, you might need to install the AD DS & LDS Tools from the Remote Server Administration Tools (RSAT) in **Add Roles & Features**.

Procedure

1 Start the ADSI Edit utility on your View Connection Server host.

2 In the Connection Settings dialog box, select or connect to **DC=vdi,DC=vmware,DC=int**.

3 In the Computer pane, select or type **`localhost:389`** or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.

For example: **`localhost:389`** or **`mycomputer.mydomain.com:389`**

4 If the pool has already been created, find the name of the pool under the object **OU=Applications**, and add **BLAST** in the **pae-ServerProtocolLevel** attribute.

5 Find the name of the farm under the object **OU=Server Groups**, and add **BLAST** in the **pae-ServerProtocolLevel** attribute.

The farm items now appear in the HTML Access Web client.

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]`

IMPORTANT When coding the HTML hyperlinks or buttons that contain the URI, do not use `target='_Blank'` in the link. This code is used to open a new browser window, but causes problems in Internet Explorer 9, 10, and 11 browsers. If you use this code in an `href`, then if the user selects the **Disconnect** menu item, after the desktop is disconnected, the client immediately attempts to reconnect. Also the user name and domain name are not set.

---

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 domain associated with the user who is connecting to the remote desktop.

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 desktop. 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 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>
```

NOTE Do not use `target='_Blank'` in the link, as, for example, in the following code:

```
<a href="https://view.mycompany.com?desktopId=Primary%20Desktop&action=start-session"
target="_Blank">Test Link</a>
```

`target='_Blank'` is used to open a new browser window, but causes problems in Internet Explorer 9,10, and 11 browsers. If you use this code in an `href`, then if the user selects the **Disconnect** menu item, after the desktop is disconnected, the client immediately attempts to reconnect. Also the user name and domain name are not set.

Configure HTML Access Group Policy Settings

You can configure group policy settings that control the behavior of HTML Access on your remote desktops. To apply these settings, add the HTML Access ADM template file to group policy objects (GPOs) in Active Directory.

Prerequisites

- Verify that View Agent 6.0 or later is installed on your remote desktops. View Agent 6.0 or later includes an HTML Access component. For previous releases, you were required to install a Remote Experience Agent in order to get the HTML Access component.
- Verify that Active Directory GPOs are created for the HTML Access group policy settings. The GPOs must be linked to the OU that contains your remote desktops. For general information about setting up View group policy settings in Active Directory, see "Configuring Policies" in *Setting Up Desktops and Applications in View*.

- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Familiarize yourself with the HTML Access group policy settings. See "HTML Access Group Policy Settings," on page 29.

Procedure

1 Download the View GPO Bundle `.zip` file from the VMware Horizon 6 download site at http://www.vmware.com/go/downloadview.

The file is named `VMware-Horizon-View-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 `Blast-enUS.adm` ADM Template file.

3 On the Active Directory server, edit the GPO.

Option	Description
Windows 2008 or 2012	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**.
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click the OU that contains your remote desktops and select **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d In the right pane, 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 `Blast-enUS.adm` file, and click **Open**.

6 Click **Close** to apply the policy settings in the ADM 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.

HTML Access Group Policy Settings

The HTML Access ADM Template file, `Blast-enUS.adm`, contains group policy settings that you can apply to your remote desktops. After the template file is imported into Active Directory, the HTML Access group policy settings are contained in the `VMware Blast` folder in the Group Policy Editor.

Table 2-2. HTML Access Group Policy Settings

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.

Table 2-2. HTML Access Group Policy Settings (Continued)

Setting	Description
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 only. For single-user remote desktops, when this setting is disabled or not configured, the default value is **Enabled client to server only**. For session-based remote desktops on RDS hosts (available with HTML Access 2.6), when this setting is disabled or not configured, the default value is **Disabled in both directions**.
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 is installed).

Using a Remote Desktop 3

The client provides a drop-down toolbar and menu so that you can easily disconnect from a remote desktop or use a menu-command equivalent of the Ctrl+Alt+Delete key combination.

This chapter includes the following topics:

Feature Support Matrix

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

Table 3-1. Features Supported Through HTML Access

Feature	Windows 8.x Remote Desktop	Windows 7 Remote Desktop	Windows XP Remote Desktop	Windows Vista Remote Desktop	Windows Server 2008 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					
Blast protocol	X	X	X	X	X
USB access					
Real-time audio-video (RTAV)					

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

Feature	Windows 8.x Remote Desktop	Windows 7 Remote Desktop	Windows XP Remote Desktop	Windows Vista Remote Desktop	Windows Server 2008 R2 Desktop
Wyse MMR					
Windows 7 MMR					
Virtual printing					
Location-based printing					
Smart cards					
Multiple monitors					

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

Feature Support for Session-Based Desktops on RDS Hosts

RDS hosts are server computers that have Windows Remote Desktop Services and View Agent installed. Multiple users can have desktop sessions on an RDS host simultaneously.

If you have HTML Access 2.6, you can also access remote session-based desktops on a Microsoft RDS (Remote Desktop Sessions) host. 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 RDS Hosts with View Agent 6.0.2 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 RDS Host on a Physical Machine	Windows Server 2012 RDS Host on a Virtual Machine
RSA SecurID or RADIUS	X	X	X	X
Single sign-on	X	X	X	X
Blast protocol	X	X	X	X
Virtual printing				
Location-based printing				
Multiple monitors				

For information about which editions of each guest operating system are supported, or which service packs, see the "Supported Operating Systems for View Agent" topic in the View 6.x installation documentation.

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 35.

Connect to a Remote Desktop

Use your Active Directory credentials to connect to the remote desktops 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 domain name for logging in.

Procedure

1. If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Log In**.

   The passcode might include both a PIN and the generated number on the token.
2. If you are prompted a second time for RSA SecurID credentials or RADIUS authentication credentials, enter the next generated number on the token.

   Do not enter your PIN and do not enter the same generated number entered previously. If necessary, wait until a new number is generated.

   If this step is required, it is required only when you mistype the first passcode or when configuration settings in the RSA server change.
3. In the Log In dialog box, enter your Active Directory user name, password, and domain name, and click **Sign In**.
4. If you are entitled to more than one remote desktop, click the icon for the remote desktop that you want to access.

   The remote desktop is displayed in your browser.

What to do next

If you are using a Safari browser and soon after connecting to the desktop, 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 33.

Trust a Self-Signed Root Certificate

In some cases, if you are using a Safari browser, soon after connecting to a remote desktop, you get disconnected and a Desktop Disconnected dialog box appears. You can use the browser to accept the self-signed security certificate and connect to the remote desktop again.

This issue can occur when the Blast Secure Gateway is not being used.

Procedure

1. Click the **Click here to accept the security certificate** link in the Desktop Disconnected dialog box.
2. Click the **Show Certificate** button in the next prompt that appears.
3. In the Blast pane that appears, click to expand the **Trust** drop-down list.
4. In the **When using this certificate** drop-down list, select **Always Trust**, and click **Continue**.
5. When prompted, provide your password and click **Update Settings**.
6. In the desktop selector window, click the remote desktop.

You are connected and logged in to the remote desktop again.

Product Limitations

The Web client provided by HTML Access has product limitations with regard to sound playback and keyboards.

- Audio playback is not supported for Windows XP and Windows Vista remote desktops.
- Internet Explorer 9 is not supported with HTML Access 2.6. For HTML Access 2.4 and 2.5, Internet Explorer 9 is supported, but that version of the browser does not support many of the HTML5 features provided with HTML Access. The features that are not supported by Internet Explorer 9 (even with HTML Access 2.4 or 2.5) include audio playback, clipboard redirection, mouse cursor changes, and full-screen mode, among others.
- If you use an Internet Explorer browser or a browser on handheld devices such as iPads and Android tablets, the mouse pointer types do not change dynamically based on the location of the pointer.

  Some of the unavailable types are the busy cursor, the drag cursor, and the resize cursor. For example, on Internet Explorer browsers and mobile device browsers, when you move the mouse pointer over a link on a Web page in a remote desktop, the mouse pointer does not change to a hand icon. If you move the mouse pointer to the edge of a window, the pointer does not change to resizing arrows. If you are editing text, the pointer does not change to a cursor. You can still perform the actions, but the pointer remains a pointer.
- Some modifier keys, special keys, and key combinations do not work in a remote desktop. For more information, and for information about using international keyboards, see "Keyboard Limitations," on page 34 and "International Keyboards," on page 35.

Keyboard Limitations

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

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.

The following keys and keyboard combinations often do not work:

- Ctrl+T
- Ctrl+W
- Ctrl+N
- Windows key
- Command key
- Alt+Enter
- Ctrl+Alt+*any_key*
- Caps Lock+*modifier_key* (such as Alt or Shift)
- Function keys, if you are using a Chromebook

IMPORTANT To input Ctrl+Alt+Del, use the **Send Ctrl+Alt+Delete** from the drop-down menu located at the right end of the client menu bar.

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 3-3. 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 remote desktop has been configured with the correct amount of video RAM, the client can resize a remote desktop to match the size of the client 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.

IMPORTANT To use the 3D rendering feature, you must allocate sufficient VRAM for each Windows 7 or later 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.

When 3D rendering is enabled, the maximum number of monitors is 1 and the maximum resolution is 1920 x 1200. Estimating the amount of vRAM you need for the Blast 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.

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 to use that resolution. Select the **Toggle High Resolution Mode** command from the drop-down menu located at the right end of the client menu bar. To display this menu bar, click the down-arrow on the tab at the top-center of the window.

HTML Access also provides a **Toggle Full Screen** command from the drop-down menu.

IMPORTANT To use High Resolution mode in Full Screen mode, you must allocate sufficient VRAM for each Windows 7 or later remote desktop. Estimating the amount of vRAM you need for the Blast 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.

Sound

If you use a Chrome device or a browser that supports WebSockets, you can play sound in your remote desktop, but some limitations apply.

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

Take into account the following guidelines:

- Audio playback is not supported for Windows XP and Windows Vista remote desktops.
- To turn up the volume, use the sound control on your 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 a lot of tasks (I/O), sound quality might be reduced. Some browsers work better than others in this regard.

Copying and Pasting Text

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 only from a remote desktop to your client system, or both, or neither. Some restrictions apply.

This feature is available if you use a Chrome device or a browser that supports WebSockets.

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

You can copy plain text or formatted text, including any non-ASCII characters, from Horizon Client to a remote desktop, or the reverse, but the pasted text is plain text. You can copy and paste up to 5,000 characters.

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.

Use the Copy and Paste Feature

To copy and paste text, you must use the **Paste Text** and **Get Copied Text** commands from the drop-down menu located at the right end of the client menu bar.

Prerequisites

- The View administrator must either leave the default policy in effect, which allows users to copy from client systems and paste into their remote virtual desktop, or else the administrator must configure another policy that allows copying and pasting. For more information, see "HTML Access Group Policy Settings," on page 29.
- You must use a Chrome device or a browser that supports WebSockets. Browsers that do not support this technology do not display the **Paste Text** and **Get Copied Text** menu commands.

Procedure

- To copy text from your client system to the remote desktop:
  a Copy the text on your client system.
  b Inside your remote desktop, click the down-arrow on the tab at the top-center of the window to display the menu bar.
  c Select **Paste Text** from the drop-down menu located at the right end of the client menu bar.
  d Paste the text into the dialog box that appears.
  e Position your mouse cursor in the application where you want to paste the text.
  f Click **Paste** in the Paste dialog box and then close the box.

  The text is pasted into the application.
- To copy text from your remote desktop to your client system:
  a Copy the text in your remote desktop.
  b Inside your remote desktop, click the down-arrow on the tab at the top-center of the window to display the menu bar.
  c Select **Get Copied Text** from the drop-down menu located at the right end of the client menu bar.

  If you do not see the **Get Copied Text** command in the drop-down menu, it means either that you are using a browser that does not support WebSockets or that your View administrator has not configured your setup to allow you to copy text from the remote desktop to your client system, as mentioned in the prerequisites to this procedure.
  d In the Get Copied Text dialog box, select and copy the text again.

  The text is now copied to your Clipboard.
  e On your client system, paste the text as you normally would.

Log Off or Disconnect

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

Even if you do not have a remote desktop open, you can log off of the remote desktop operating system. Using this feature has the same result as sending Ctrl+Alt+Del to the desktop and then clicking **Log Off**.

NOTE The Windows key combination Ctrl+Alt+Del is not supported in remote desktops. To use the equivalent of pressing Ctrl+Alt+Del, select **Send Ctrl+Alt+Del** from the drop-down menu located at the right end of the client menu bar. To display the menu bar, click the down-arrow on the tab at the top-center of the window.

Procedure

- Log out from the View server and disconnect (but do not log out) from the desktop.

Option	Action
From within the desktop OS	Select **Disconnect** from the drop-down menu located at the right end of the client menu bar, and then click the **Log Out** button in the upper-right corner of the screen.
From the desktop selector screen	Click the **Log Out** button in the upper-right corner of the screen.

- Log off of and disconnect from a desktop by selecting **Log off** from the **Start** menu inside the desktop operating system.

- Disconnect without logging out.

Option	Action
Also quit the client	Close the browser tab.
Choose a different remote desktop on the same server	Select **Disconnect** from the drop-down menu located at the right end of the client menu bar, and then select a different remote desktop.
Choose a remote desktop on a different server	Select **Disconnect** from the drop-down menu, and then enter the URL of the other server in your browser.

NOTE Your View administrator can configure your desktop to automatically log out when disconnected. In that case, any open programs in your desktop are stopped.

- Log off of the desktop operating system when you do not have a remote desktop open.

  If you use this procedure, files that are open on the remote desktop will be closed without being saved first.

  a On the desktop selector screen, click the **Log Off** button on the desktop icon.

  b If prompted, supply credentials for accessing the remote desktop.

Reset a Desktop

You might need to reset a desktop if the desktop operating system stops responding. Resetting shuts down and restarts the desktop. 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.

You can reset the desktop only if your View administrator has enabled this feature.

Procedure

- Use the **Reset** command.

Option	Action
From within the desktop OS	Select **Disconnect** from the drop-down menu located at the right end of the client menu bar, and then click the **Reset** button under the desktop icon.
From the desktop selector screen	Click the **Reset** button under the desktop icon.

The operating system in the remote desktop is rebooted. The client disconnects from the desktop.

What to do next

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

Index

V

W