

Using VMware Horizon View HTML Access

November 2013
Horizon View

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-001116-02

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

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

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

Contents

Using VMware Horizon View HTML Access	5
Setup and Installation	5
System Requirements for HTML Access	5
Preparing View Connection Server and Security Servers for HTML Access	7
Prepare View Desktops and Pools for HTML Access	8
Upgrading the HTML Access Software	10
Uninstall HTML Access from View Connection Server	10
Horizon View Data Collected by VMware	11
Configuring HTML Access for End Users	12
Configure the HTML Access Page for End Users	12
Configure HTML Access Group Policy Settings	13
HTML Access Group Policy Settings	15
Using a View Desktop	16
Feature Support Matrix	16
Internationalization	17
Product Limitations	17
Keyboards and Monitors	17
Sound	19
Copying and Pasting Text	19
Log Off or Disconnect from a Desktop	20
Reset a Desktop	21
Index	23

Using VMware Horizon View HTML Access

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

This information is intended for administrators who need to set up a Horizon View deployment that includes HTML Access. The information is written for experienced system administrators who are familiar with virtual machine technology and datacenter operations.

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

Setup and Installation

Setting up a Horizon View deployment for HTML Access involves installing HTML Access on View Connection Server, opening the required ports, and installing the Remote Experience Agent in the View desktop.

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

System Requirements for HTML Access

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

Browser on client system

The following Web browsers are supported:

- Chrome 28 or later
- Internet Explorer 9 or later
- Safari 6 or later
- Mobile Safari on iOS devices running iOS 6 or later
- Firefox 21 or later

Client operating systems

- Windows XP SP3 (32-bit)

- Windows 7 SP1 or no SP (32- or 64-bit)
- Windows 8 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)
- iPad with iOS 6.0 or later (therefore, iPad 1 is not supported)
- Chrome OS 28.x or later

View desktop

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

- Operating systems: Windows XP SP3 (32-bit), Windows Vista (32-bit), Windows 7 (32- or 64-bit), or Windows Server 2008 R2.

In addition, HTML Access is available on Windows 8 (32- or 64-bit) or Windows 8.1 (32- or 64-bit) as a Tech Preview. You can try out HTML Access on a Windows 8 or Windows 8.1 desktop, but no support is provided.

- View Agent 5.3

Installation instructions are provided in the *VMware Horizon View Administration* document.

- Remote Experience Agent

Installation instructions are provided in the *VMware Horizon View Feature Pack Installation and Administration* document.

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 View desktop has at least 17.58MB of video RAM.

If you plan to use 3D applications, see [“Keyboards and Monitors,”](#) on page 17.

- The **HTML Access** setting must be enabled.

Configuration instructions are provided in [“Prepare View Desktops and Pools for HTML Access,”](#) on page 8.

View Connection Server

The following software must be installed on the server that hosts View Connection Server:

- View Connection Server 5.3

Installation instructions are provided in the *VMware Horizon View Installation* document.

- HTML Access

Installation instructions are provided in the *VMware Horizon View Feature Pack Installation and Administration* document.

When you install HTML Access, the firewall is automatically configured to allow inbound traffic to TCP port 8443.

Security Server

The Windows Firewall service or other software firewall must be configured to allow inbound traffic to TCP port 8443.

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 350 simultaneous connections to Web clients.

Third-party firewalls

Add rules to allow the following traffic:

- View servers (including security servers, View Connection Server instances, and replica servers): inbound traffic to TCP port 8443.
- View desktops: inbound traffic (from View servers) to TCP port 22443.

Display protocol for Horizon View

Blast

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

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

Preparing View Connection Server and Security Servers for HTML Access

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

Before end users can connect to View Connection Server or a security server and access a View desktop, you must install software on View Connection Server and open the required port on any paired security servers.

Following is a check list of the tasks you must perform:

- 1 Verify that you are using View Connection Server 5.3 and, if you use a security server, verify that the version is View Security Server 5.3.

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

- 2 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 *VMware Horizon View Installation* documentation.

- 3 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 *VMware Horizon View Administration* documentation.

- 4 On the View Connection Server host or hosts in a replicated group, download the VMware Horizon View HTML Access installer from the VMware Horizon View Downloads page, and run the installer.

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

- 5 On any paired security servers, configure the Windows firewall to allow inbound traffic on TCP port 8443.

This port is automatically opened on View Connection Server instances when you run the HTML Access installer, but on security servers, you must open the port manually.

- 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 View desktops in the datacenter.

- 7 Use View Administrator to enable the **Blast Secure Gateway** setting on the applicable View Connection Server instances and security servers.

For details about editing View Connection Server settings and security server settings, see the *VMware Horizon View Administration* documentation.

- 8 Use View Administrator to configure the **Blast External URL** setting to use for the Blast Secure Gateway on the applicable View Connection Server instances and security servers.

The URL must contain the HTTPS protocol, client-resolvable host name, and port number, for example: `https://myserver.example.com:8443`

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.

- 9 To customize the links that end users see when they go to the Web page for accessing a View desktop, see [“Configure the HTML Access Page for End Users,”](#) on page 12.

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

Prepare View Desktops and Pools for HTML Access

Before end users can access a View desktop from a browser, administrators must configure certain pool settings and install HTML Access software on View desktops in the datacenter.

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

NOTE The Horizon View Client software offers more features and better performance than the HTML Access client. For example, with the Horizon View Client software, sound is available when you watch videos. With the HTML Access client, sound is not yet available.

Prerequisites

- Verify that your vSphere infrastructure and Horizon View components meet the system requirements for HTML Access. See “[System Requirements for HTML Access](#),” on page 5.
- Verify that the HTML Access software is installed on the View Connection Server 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 7.

- 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, in the following order: a supported operating system, VMware Tools, and View Agent 5.3. For a list of the supported operating systems, see “[System Requirements for HTML Access](#),” on page 5.
- Familiarize yourself with the procedures for creating desktop pools and entitling users to desktops. See the topics about creating desktop pools in the *VMware Horizon View Administration* documentation.
- To verify that the View desktop is accessible to end users, verify that you have View Client software installed on a client system. You will test the connection by using the View Client software before attempting to connect from a browser.

For View Client installation instructions, go to the View 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 View desktop. See “[System Requirements for HTML Access](#),” on page 5.

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, go to the VMware Horizon View Downloads page and download and install the Remote Experience Agent software.

The HTML Access component of this agent is required for HTML Access. The 32-bit installer is named `VMware-Horizon-View-5.3-Remote-Experience-Agent-y.y-xxxxxxx.exe`. The 64-bit installer is named `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxxx.exe`.

In these file names, *y.y* is the version number of the feature pack, and *xxxxxxx* is the build number. Running this installer also opens TCP port 22443 in the Windows firewall for the desktop virtual machine.

- 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 Pool wizard.

All types of pools support HTML Access.

- 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 View 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-view.mycompany.com`

Be sure to use **https** in the URL.

- 8 On the Web page that appears, click **VMware Horizon View HTML Access** and log in as you would with the View Client software.
- 9 On the View Client home screen that appears, click a desktop icon.

You can now access a View desktop from a Web browser when you are using a client device that does not or cannot have Horizon View 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 View desktop uses an SSL certificate from a certificate authority, see the topic about configuring the Blast agent to use a new SSL certificate, in the *VMware Horizon View Feature Pack Installation and Administration* document.

Upgrading the HTML Access Software

Install the current HTML Access release to obtain the latest updates and improvements.

Before you can install the HTML Access software that is provided with the Horizon View 5.3 Feature Pack 1 release, you must upgrade your View Connection Server instances to Horizon View 5.3.

To upgrade, you run the latest version of the HTML Access software on the View Connection Server instances in a replicated group.

To complete the upgrade of HTML Access, you also must run the latest version of the Remote Experience Agent installer on the applicable parent virtual machines or virtual machine templates for your desktop pools.

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 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.

Horizon View Data Collected by VMware

If your company participates in the customer experience improvement program, VMware collects data from certain View 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. View Client information is sent first to View Connection Server and then on to VMware, along with data from View servers, desktop pools, and View 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. Data Collected from HTML Access Clients for the Customer Experience Improvement Program

Description	Field name	Is This Field Made Anonymous?	Example Value
Company that produced the HTML Access application	<client-vendor>	No	VMware
Product name	<client-product>	No	VMware Horizon View HTML Access
Client product version	<client-version>	No	2.2.0-build_number
Client binary architecture	<client-arch>	No	browser
Native architecture of the browser	<browser-arch>	No	Examples include the following values: <ul style="list-style-type: none"> ■ Win32 ■ Win64 ■ MacIntel ■ iPad
Browser user agent string	<browser-user-agent>	No	Examples include the following values: <ul style="list-style-type: none"> ■ Mozilla/5.0 (Windows NT 6.1; WOW64) ■ AppleWebKit/536.11 (KHTML, like Gecko) ■ Chrome/20.0.1132.57 ■ Safari/536.11
Browser's internal version string	<browser-version>	No	Examples include the following values: <ul style="list-style-type: none"> ■ 6.0 (for Safari), ■ 21.0 (for Firefox)
Browser's core implementation	<browser-core>		Examples include the following values: <ul style="list-style-type: none"> ■ 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

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.

Configure the HTML Access Page for End Users

You can configure this Web page to show or hide the icon for downloading Horizon View Client or the icon for connecting to a View 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 View 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.

If you use HTML Access 2.2 or later, you can make installer links for specific client operating systems. For example, if you browse to the portal page from a Windows system, the link for the native Windows installer appears. You cannot, however, make separate links for 32-bit and 64-bit installers.

IMPORTANT If you previously edited the portal page to point to your own server for downloading Horizon View Client, those customizations are hidden when you install HTML Access. You can, however, customize the page after installing HTML Access.

Any customizations you make to the HTML Access Web page are preserved when you upgrade HTML Access. If you uninstall HTML Access, any customizations you made to the portal page before you installed HTML Access are reinstated.

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.

- 2 Set the configuration properties 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, set the property to `false`.

Option	Property Setting
Disable the icon for connecting through HTML Access	<code>enable.webclient =false</code>
Disable the icon for downloading Horizon View Client	<code>enable.download=false</code>

Option	Property Setting
Change the URL of the Web page for downloading Horizon View Client	link.download=https://url-of-web-server Use this property if you plan to create your own Web page.
Create links for specific installers (Available if you have HTML Access 2.2 or later)	The following examples show full URLs, but you can use relative URLs if you place the installer files in the <code>downloads</code> directory, which is under the <code>C:\Program Files\VMware\VMware View\Server\broker\webapps\</code> directory on View Connection Server, as described in the next step. <ul style="list-style-type: none"> ■ link.win=https://server/downloads/VMware-Horizon-View-Client.exe ■ link.linux=https://server/downloads/VMware-Horizon-View-Client.tar.gz ■ link.mac=https://server/downloads/VMware-Horizon-View-Client.dmg ■ link.ios=https://server/downloads/VMware-Horizon-View-Client-iPhoneOS.zip ■ link.android=https://server/downloads/VMware-Horizon-View-Client-AndroidOS.apk ■ link.unknown=https://server/downloads/Horizon-View-Client.zip

- 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` 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`.

- 4 Restart the VMware View Web Component service.

Configure HTML Access Group Policy Settings

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

Prerequisites

- Verify that the Remote Experience Agent is installed on your Horizon View desktops. The HTML Access component of this agent is required for HTML Access.
- 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 View desktops. For general information about setting up Horizon View group policy settings in Active Directory, see "Configuring Policies" in the *VMware Horizon View Administration* document.
- 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 15.

Procedure

- 1 In vSphere Web Client or vSphere Client, open a console on a View desktop virtual machine on which you installed the Remote Experience Agent.

The HTML Access ADM Template file is installed when you install the agent.

- 2 Copy the HTML Access ADM Template file, `Blast-enUS.adm`, from the `install_directory\VMware\VMware Blast\Tools\Group Policy` directory on the View desktop to your Active Directory server.

The default installation directory is `C:\Program Files`.

- 3 On the Active Directory server, edit the GPO.

Option	Description
Windows 2008	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> a Select Start > All Programs > Administrative Tools > Active Directory Users and Computers. b Right-click the OU that contains your View 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 Horizon View 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 Horizon View 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. HTML Access Group Policy Settings

Setting	Description
Screen Blanking	<p>Controls whether the remote virtual machine can be seen from outside of Horizon 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.</p> <p>When this setting is enabled or not configured, and someone attempts to access the remote virtual machine from outside of Horizon View while an HTML Access session is active, the remote virtual machine displays a blank screen.</p> <p>When this setting is disabled, under the preceding conditions, the remote virtual machine displays the active Horizon View desktop session to the second remote accessor.</p>
Session Garbage Collection	<p>Controls the garbage collection of abandoned remoting sessions. When this setting is enabled, you can configure the garbage collection interval and threshold.</p> <p>The interval controls how often the garbage collector runs. You set the interval in milliseconds.</p> <p>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.</p>
Audio playback	<p>Controls whether audio playback is allowed on the View desktop. By default, this setting is enabled.</p>
Image Quality	<p>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.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> ■ 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. HTML Access Group Policy Settings (Continued)

Setting	Description
Configure clipboard redirection	<p>Determines the direction in which clipboard redirection is allowed. Only text can be copied and pasted. You can select one of these values:</p> <ul style="list-style-type: none"> ■ Enabled client to server only (That is, allow copy and paste only from the client system to the View desktop.) ■ Disabled in both directions ■ Enabled in both directions ■ Enabled server to client only (That is, allow copy and paste only from the View desktop to the client system.) <p>This setting applies to View Agent only.</p> <p>When this setting is disabled or not configured, the default value is Enabled client to server only.</p>
HTTPS Service	<p>Allows you to change the secured (HTTPS) TCP port for the Blast Agent service. The default port is 22443.</p> <p>Enable this setting to change the port number.</p>

Using a View Desktop

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

Feature Support Matrix

When you access a View desktop from a Web browser, some features are not available.

Table 3. Features Supported Through HTML Access

Feature	Windows 7 View Desktop	Windows XP View Desktop	Windows Vista View Desktop	Windows Server 2008 R2 Desktop
RSA SecurID or RADIUS	X	X	X	X
Single sign-on	X	X	X	X
RDP display protocol				
PCoIP display protocol				
USB access				
Real-time audio-video (RTAV)				
Wyse MMR				
Windows 7 MMR				
Virtual printing				
Location-based printing				
Smart cards				
Multiple monitors				
Local mode				

For descriptions of these features and their limitations, see the *VMware Horizon View Architecture Planning* 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 View desktop, see [“Keyboards and Monitors,”](#) on page 17.

Product Limitations

Although the Web client provided by VMware Horizon View HTML Access allows you to access a View desktop without having to install any software, features are limited.

The following features, which are supported with the native Horizon View Client, might have some limitations when you use the Web client provided by HTML Access.

- Internet Explorer 9 does not support many of the HTML5 features proved with the HTML Access 2.2 release. The features that are not supported by Internet Explorer 9 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 View 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.

- Keyboard modifier keys and special keys

Some keys and key combinations do not work in a View desktop. For more information, and for information about using international keyboards, see [“Keyboards and Monitors,”](#) on page 17.

Keyboards and Monitors

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

Keyboard Limitations

Regardless of the language used, some key combinations cannot be sent to the to a View desktop when you use HTML Access. 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

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 4. Required Locale Settings

Language	Locale on the Local Client System	Browser and Local on the Remote View Desktop	IME Required on the Remote View Desktop?
English	English	English	No
French	French	French	No
German	German	German	No
Chinese (Simplified)	US International	Chinese (Simplified)	Yes
Chinese (Traditional)	US International	Chinese (Traditional)	Yes
Japanese	US International	Japanese	Yes
Korean	US International	Korean	Yes

Screen Resolution

If the View desktop has been configured with the correct amount of video RAM, the Web client can resize a View 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.

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

- The software-accelerated graphics feature, available with View 5.0 or later, allows you to use 3D applications such as Windows Aero themes or Google Earth. This feature requires 64MB (the default) to 128MB of VRAM.
- The hardware-accelerated graphics feature (vSGA), available with Horizon View 5.2 or later and 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 2 and the maximum resolution is 1920 x 1200. Estimating the amount of vRAM you need for HTML Access 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 *VMware Horizon View Architecture Planning* document.

If you have HTML Access 2.2 and use a browser that has a high pixel density resolution, such as a Macbook with Retina Display or a Google Chromebook Pixel, you can set the View 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 2.2 also provides a **Toggle Full Screen** command from the drop-down menu.

Sound

If you use VMware Horizon View HTML Access 2.2 or later and use a browser that supports WebSockets, you can play sound in your View desktop, but some limitations apply.

By default, sound playback is enabled for View desktops, 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 View 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

By default, you can copy and paste text from your client system to a remote View desktop. If your administrator enables the feature, you can also copy and paste text from a View desktop to your client system or between two View desktops. Some restrictions apply.

If you use VMware Horizon View HTML Access 2.2 and use a browser that supports WebSockets, your View administrator can set this feature so that copy and paste operations are allowed only from your client system to a View desktop, or only from a View desktop 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 in View desktops. For more information, see the topic about View PCoIP general session variables in the *VMware Horizon View Administration* document, in the chapter about configuring policies.

You can copy plain text or formatted text, including any 110n characters, from View Client to a View 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 View 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 15.
- You must be using HTML Access 2.2 or later.
- You must use a browser that supports WebSockets. Browsers that do not support this technology, such as Internet Explorer 9, do not display the **Paste Text** and **Get Copied Text** menu commands.

Procedure

- To copy text from your client system to the View desktop opened in your browser:
 - a Copy the text on your client system.
 - b Inside your View 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 View desktop to your client system:
 - a Copy the text in your View desktop.
 - b Inside your View 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 your browser does not support WebSockets or that your View administrator has not configured your setup to allow you to copy text from the View 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 from a Desktop

If you disconnect from a View desktop without logging off, applications remain open.

Even if you do not have a View desktop open, you can log off of the View 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 View 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 Horizon View server as well as disconnect 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 browser, next to the user name.
From the HTML Access Web page that displays View desktop icons	Click the Log Out button in the upper-right corner of the browser, next to the user name.

- Disconnect without logging off.

Option	Action
Also quit View Client	Close the browser tab.
Choose a different View 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 View desktop.
Choose a View 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 off when disconnected. In that case, any open programs in your desktop are stopped.

- Log off and disconnect from a desktop by selecting **Log Off** from the **Start** menu inside the desktop operating system.
- Log off of a View desktop from the HTML Access Web page that displays icons of View desktops.
 - Click the **Log Off** button under the desktop icon.
 - If prompted, supply credentials for accessing the View desktop.

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

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 View 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 View 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 HTML Access Web page that displays View desktop icons	Click the Reset button under the desktop icon.

The operating system in the View desktop is rebooted. View Client disconnects from the desktop.

What to do next

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

Index

A

ADM template files, HTML Access 15

B

Blast Agent 8

C

configuration settings 12

copy text 19

copying text 19

Ctrl+Alt+Delete 20

customer experience program, desktop pool data 11

D

desktop

log off from 20

reset 21

disconnecting from a View desktop 20

F

feature limitations 17

feature support matrix 16

G

group policies, configuring for HTML Access 13

H

Horizon View HTML Access 5

HTML Access

configuring group policies 13

installing View Client on 5

upgrading 10

HTML Access page 12

HTML Access Web client 5

I

IME (input method editor) 17

installation 5

K

keyboards 17

L

limitations 17

log off 20

M

monitors 17

P

paste text 19

pasting text 19

R

reset desktop 21

S

screen resolution 17

security servers 7

Send Ctrl+Alt+Del menu command 20

setup 5

sound playback 19

system requirements, for HTML Access 5

T

text, copying 19

U

uninstall HTML Access 10

V

video RAM 17

View Client, disconnect from a desktop 20

View Portal 12

View Connection Server 7

View desktop 16

W

Web client, system requirements for HTML Access 5

