

15

VMware Horizon View Feature Pack 1

This chapter discusses VMware Horizon View Feature Pack 1, an add-on to the View platform that enables support for client access to View desktops over HTML5, and the touchscreen-optimized Unity Touch interface for mobile devices.

In this chapter, we will learn:

- What features does Feature Pack 1 enable?
- Where and how do you install Feature Pack 1?
- How do you install the Remote Experience Agent on desktops?
- What are the current limitations when using the View HTML client?
- What browsers are supported for the View HTML client?
- How do you enable access over HTML for desktops?
- How do you connect to desktops using HTML?
- How does the Unity Touch interface work?
- How do you customize the Unity Touch interface?
- How do you use the Feature Pack 1 group policy templates to customize the View HTML client settings?

Introducing View Feature Pack 1

The VMware Horizon View Feature Pack 1 is a free add-on to the View platform that enables support for two additional features:

- **View HTML Client:** Access View desktops using just a supported HTML5-compliant web browser; no additional software is required.
- **Unity Touch Interface:** This is a touchscreen-optimized customizable interface for the View desktop. The interface is available when using the View client on the Google Android or Apple iOS platforms.

This chapter contains information about how to install, enable, and use both of these new features.

Installing View Feature Pack 1

The HTML Access component of View is installed on each of the View Connection Servers. The software should not, and cannot, be installed on the View Security Servers. The software is delivered as a single EXE file, named in a format similar to `VMware-Horizon-View-HTML-Access_x64-x.x.x-yyyyyy.exe`. The following steps outline the installation process:

1. Double-click on the Horizon View HTML Access installer EXE file to launch the installer.
2. In the **Welcome to the VMware Horizon View HTML Access Setup Wizard** window, click on **Next**.
3. Review the VMware End User License Agreement, select the **I accept the terms in the license agreement** radio button, and click on **Next**.
4. Select the installation directory and click on **Next**.
5. Click on the **Install** button to begin the installation.
6. Once the installation has completed, click on the **Finish** button.

The installer will adjust the Windows Firewall rules as necessary to support access to desktops over HTML. This includes enabling access to TCP port 8443 inbound. If you are using a third-party firewall program on your View Connection Server, you must create this rule manually. Repeat this process on the remaining View Connection Servers.

The following additional tasks will need to be completed to enable View HTML Client access:

- If using View Security Servers, enable the Blast-in firewall rules on them, as described in the next section of this chapter.
- Enable and configure the **Blast Secure Gateway** setting on the View Connection and Security Servers. The setting is enabled and configured by default during the installation of the Connection Server software but can also be configured post-installation. The setting is configured in the **General** tab of the **Settings** window of each of the servers in the View Manager Admin console, in **View Configuration | Servers | Connection Servers** or **View Configuration | Servers | Security Servers**.
 - For the Connection Server, the secure gateway setting will use the internal FQDN of the Connection Server in the format `https://FQDN:8443`, as shown in the following screenshot:



- For the Security Server, the secure gateway setting will use the external FQDN of the Security Server in the format `https://FQDN:8443`, as shown in the following screenshot:

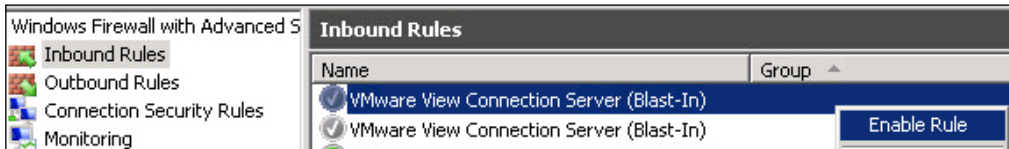


Enabling the Blast-in firewall rules

View Security Servers do not require any additional software in order to support HTML clients but they do require that two Windows Firewall rules be enabled. These rules were created when the View Security Software was installed; by default, however, they are not enabled. The following steps outline how to enable the Windows Firewall rules:

1. Log in to the View Security Server.
2. Open the Windows Firewall with Advanced Security console found in the **Administrative Tools** folder of the Windows Start menu.

3. Select the **Inbound Rules** list from the left column of the console.
4. Enable the two rules named **VMware View Connection Server (Blast-in)** by right-clicking on them and selecting **Enable Rule**. The rules are shown in the following screenshot:




5. Log out from the View Security Server.

These rules enable access to the Security Server on TCP port 8443 inbound. If you are using a third-party firewall program on your View Security Server, you must create this rule manually. Repeat this process on the remaining View Security Servers.

Installing the Remote Experience Agent

The View Remote Experience Agent is installed on the virtual desktop master image and enables support for HTML client connections and the Unity Touch interface. The software is delivered as a single EXE file, named in a format similar to `VMware-Horizon-View-5.2-Remote-Experience-Agent-x.x-yyyyyyy.exe`.

 At the time of publication, the View Remote Experience Agent only supports HTML client connections for Windows XP SP3 (32-bit), Windows Vista (32-bit), and Windows 7 (32-bit or 64-bit). Windows 8 (32-bit or 64-bit) is currently supported for Unity Touch only.

The View Agent must be installed prior to installing the Remote Experience Agent, or you will not be able to install it. The Remote Experience Agent also requires that the Windows Firewall service be enabled, even if the firewall itself is disabled. If the firewall service was disabled as part of your desktop optimization process, you will need to enable it to install the Remote Experience Agent. The installer will not complete unless the firewall service is enabled. The following steps outline the installation process:

1. Double-click on the VMware Remote Experience Agent installer EXE file to launch the installer.
2. Review the End User License Agreement and click on the **Accept** button.

3. By default, both components of the agent will be installed, which includes the HTML Access and Unity Touch components. If a specific component is not required, click on the drive icon to the left of the component name and select **This feature will not be available**. Once you have made any necessary changes, click on the **Install** button.
4. Once the installation is complete, click on the **Finish** button.

The virtual desktop master image is now ready to be deployed. Repeat this process as required on other master images.

View HTML Client Access

The View HTML Client Access component enables View clients to connect to their desktops using nothing more than a supported HTML5-compliant web browser. While View HTML clients do not yet have access to all of the same features as clients that use the full View client, this new feature provides organizations with additional options for providing client access. This section will outline the current limitations of View HTML clients, what browsers are supported, how to enable HTML access for a desktop pool, and how to use the View HTML client.

Limitations of HTML Client Access

A single View Security Server can support up to 100 simultaneous HTML client connections. At the time of publication, VMware has not yet revealed how many connections a single View Connection Server can support, although there is a limit of 256 simultaneous HTML connections for the entire View Pod. Consult the VMware document *Using VMware Horizon View HTML Access* (<http://www.vmware.com/pdf/horizon-view/horizon-view-html-access-document.pdf>) for updated information about the number of connections supported.

When accessing a desktop using the View HTML client, a number of features are not yet supported. These include:

- Sound.
- Clipboard support for pasting from the client session into the View desktop is not supported. Pasting within the client session is supported.
- The mouse pointer within the desktop will not change appearance in response to the action being performed. The action will still work but the mouse pointer will not update.

- Specific keyboard combinations will not work under certain circumstances. The results will vary based on the client browser software, client operating system, and language settings. The key combinations include:
 - *Ctrl + T*, *Ctrl + W*, and *Ctrl + N* commands
 - Windows and Command keys
 - *Alt + Enter* and *Caps Lock + modifier key* (*Alt*, *Shift*, and so on) commands
 - *Ctrl + Alt + any key* (*Ctrl + Alt + Delete* will take the user to the desktop using the client drop-down menu located in the upper-right corner of the client window)
- RDP or PCoIP display protocols.
- Access to USB devices on the client.
- Wyse MMR redirection.
- ThinPrint Virtual or location-based printing.
- Smart cards.
- Multiple monitors.
- Local Mode desktops.

RSA SecurID, RADIUS, and Single Sign-On authentication features are all supported when using the HTML client.

The following languages are supported when using the HTML client:

- English, French, and German are all supported. The locale on the client system should be set to the locale being used.
- Chinese (Simplified), Chinese (Traditional), Japanese, and Korean are all supported, assuming the appropriate input method editor (IME) has been installed in the virtual desktop. The locale on the client system should be set to **US International**.

Support for specific features and languages is likely to change as View is updated. Consult with the latest VMware Horizon View documentation (http://www.vmware.com/support/pubs/view_pubs.html) for up-to-date information about what is supported.

Supported HTML client web browsers

View HTML Access currently supports the following web browsers. Consult the VMware document *Using VMware Horizon View HTML Access* (<http://www.vmware.com/pdf/horizon-view/horizon-view-html-access-document.pdf>) for an updated list.

- Apple Safari 5.1.7 or later
- Firefox 16 or later
- Google Chrome 22 or later
- Internet Explorer 9 or later

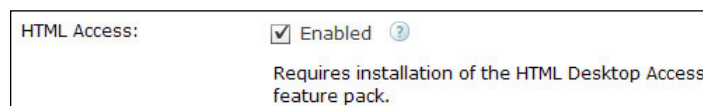
Enabling HTML access for the desktop pool

A View desktop pool does not allow HTML clients by default. This option can be enabled when the desktop pool is created, or after it has already been deployed. The following steps outline how to update an existing pool to allow HTML clients:

1. Log in to the View Manager Admin console.
2. Open the **Inventory - Pools** page to browse the existing desktop pools.
3. Highlight the desktop pool you wish to edit and click on the **Edit** button, as shown in the following screenshot. This will open the **Edit** window for the pool.



4. In the **Edit** window, select the **Pool Settings** tab. This is the same window that is displayed during the pool-creation process. Click on the **Enabled** checkbox next to **HTML Access** to allow HTML clients for desktops in the pool. The option is shown in the following screenshot:



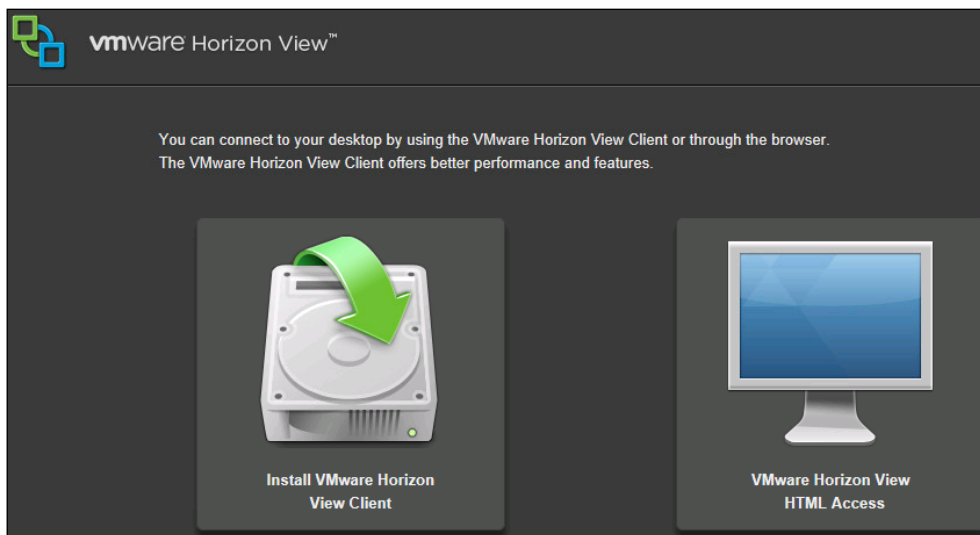
5. Verify that the **Max resolution of any one monitor** setting is set to at least **1920x1200** or higher. This is required to ensure that the desktop has the required minimum amount of video RAM (16 MB).
6. Click on **OK** to save the changes and close the **Edit** window and return to the View Manager Admin console.

Repeat the process for each pool that requires support for HTML clients.

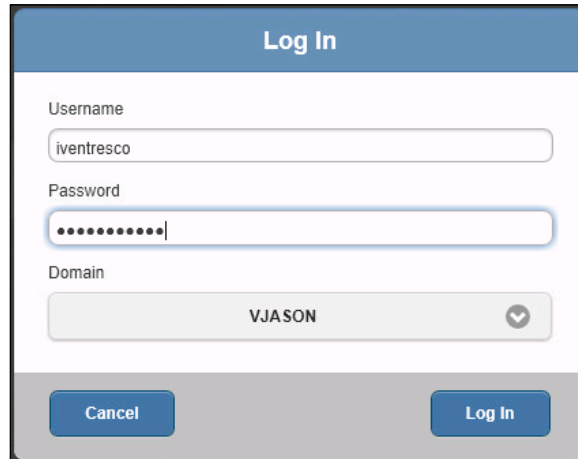
Accessing View desktops using the HTML client

Once all of the necessary steps have been completed to enable support for View HTML clients, the View Connection and Security Servers homepages will be updated with a new homepage. The following steps show the updated page and how to use it to establish a HTML client connection.

1. Using a supported web browser, browse to the homepage of either your View Security or Connection Server.
2. Click on **VMware Horizon View HTML Access** as shown in the following screenshot:



3. Log in with a username that is entitled to an HTML access-enabled desktop pool. The **Log in** screen is shown in the following screenshot:

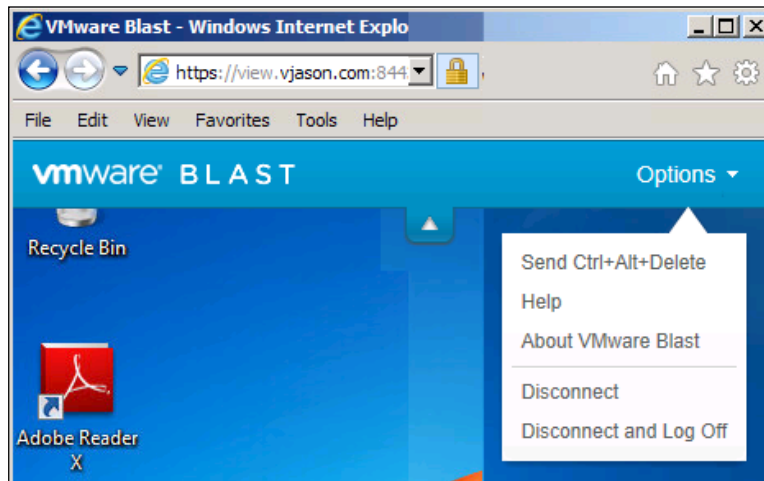


The screenshot shows a "Log In" dialog box with a blue header. It contains three input fields: "Username" with the text "iventresco", "Password" with masked characters ".....", and "Domain" with a dropdown menu showing "VJASON". At the bottom, there are two buttons: "Cancel" and "Log In".

4. Click on the desired desktop pool, as shown in the following screenshot:



5. If the pool has SSO enabled, the desktop should automatically be logged in. If not, you will need to log in again using the same credentials. The following screenshot shows a completed login and has the VMware Blast bar extended and **Options** window opened. Similar to the full View client, the window allows you to perform a number of different tasks including disconnecting or sending a *Ctrl + Alt + Delete* command to the desktop. The VMware Blast bar can be hidden by clicking on the up arrow button shown in the center of the bar.



The session can be closed by using the **Disconnect** or **Disconnect and Log Off** option in the **Options** menu. If you simply close the web browser, the session will be disconnected but your user account will remain logged in to the desktop.

The View Unity Touch interface

The View Remote Experience Agent includes an additional component: the View Unity Touch interface. The Unity Touch interface is designed for View clients who use a touchscreen interface as their primary means of interacting with their View desktop; it provides a much more efficient means of navigating the Windows desktop UI. The interface loads automatically when the desktop detects a connection from a tablet or other mobile device running the View client.

An overview of Unity Touch

The Unity Touch interface greatly reduces the need to use the desktop UI to perform tasks. It accomplishes this by presenting the user with a customizable touch-optimized interface that can be used as the primary means of interacting with the desktop. The following screenshot shows the Unity Touch interface; to open or close it, you simply swipe the tab left or right.

In the following screenshot, the tab is shown on the right side of the interface window below the **Recycle Bin**. This tab can be moved up or down by clicking on it and dragging it to a new location.



The Unity Touch interface is not designed to be left open and must be closed when not in use. You will not be able to interact with the Windows desktop session while the interface is open. The Unity Touch interface includes the following features:

- The **All Programs Unity Touch** menu allows View clients to navigate the contents of the desktop Windows Start menu
- The **My Files Unity Touch** menu allows View clients to browse the folders contained within their desktop Windows user profile
- The **Search** field allows View clients to search desktop applications and files; it supports both Google Android and Apple iOS voice dictation as an additional method for entering search terms
- The **Running Applications Unity Touch** menu allows View clients to quickly switch between running applications

Customizing Unity Touch

The interface can be customized to show frequently used applications or files. The preceding screenshot shows an interface that has already been customized with **Favorite Applications** and **Favorite Documents**. The following process outlines how to customize the favorites:

1. In the Unity Touch interface, click on either **Favorite Applications** or **Favorite Documents** to reveal the **Manage** button shown in the following screenshot. In this example, we will customize the application list.



2. Click on the **Manage** button to open the selection window shown in the following screenshot:



Any favorites that were already added will be displayed first under **Favorites**. To remove any existing favorites, simply click on the radio button to the right of the name. When selecting applications to add, all available applications will be displayed in alphabetical order underneath **Available Applications**. Click on the same radio button to add these applications for the **Favorites** list. When selecting documents, you have to select from documents that reside within your Windows user profile using the same process.

The View Feature Pack 1 group policy template

View Feature Pack 1 includes a group policy template that can be used to control four different configuration items related to View HTML clients. The template file is named `Blast-enUS.adm` and is located in the `\Program Files\VMware\VMware Blast\Tools\Group Policy` folder on any desktop that has the Remote Experience agent installed. The policies are all computer policies and should be applied to the virtual desktop computer objects or directly to the virtual desktop master image before it is deployed.

Screen Blanking

Screen Blanking instructs View to blank the display of the remote virtual machine when a View client is connected over HTML. By default the display is blanked, which is the same as configuring the group policy setting as **Enabled**. When set to **Disabled**, the display will not be blanked.

Session Garbage Collection

Session Garbage Collection is a memory management technique used to free up Connection Server memory when a View HTML client disconnects. The policy settings allow you to customize how old a disconnected client session must be in seconds before garbage collection is performed and how often the garbage collection runs in milliseconds. It is recommended you leave this setting at the default unless instructed to change it by VMware support.

Image Quality

The Image Quality group policy settings control the quality of the View HTML client display based on how often it changes. The low profile is used by those sections of the View client display that are updating frequently, while the high profile is used by those that are updating on a less frequent basis.

- By default, the **Low JPEG Quality** setting is set to **40** and the **Low JPEG Chroma Subsampling** setting is set to **4:1:0** (lowest)
- By default, the **High JPEG Quality** setting is set to **85** and the **High JPEG Chroma Subsampling** setting is set to **4:4:4** (highest)

The higher the quality and JPEG chroma subsampling values, the more bandwidth each View HTML client will require. The JPEG chroma subsampling policy value is changed using a drop-down menu, while the JPEG quality value is changed by providing a new numeric value.

HTTPS Service

The HTTPS Service policy setting allows you to change the port number used by the Blast Agent service. The default port number is 22443; to change the port, enable the policy setting and provide a value in the Secured (HTTPS) port field.

Summary

In this chapter, we learned about what additional features of View are enabled when you install Feature Pack 1, which include View HTML Client access and the Unity Touch interface. Additionally, we discussed the limitations of HTML client access compared to the full View software-based client.

We also discussed how to install and configure Feature Pack 1 and the Remote Experience Agent, and how to enable View HTML Client access. We then went through how to use and customize the View HTML Client and the Unity Touch interface.

