Horizon DaaS Platform 15.3.2
HTML Access Setup

This document describes the process for setting up HTML Access (Blast) for the Horizon DaaS Platform.

July 2015

vmware

Revision History

Date	Version	Description
07/31/2015	1.0	Initial release

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

Contents

This page intentionally left blank.

1 Overview

1.1 About Desktop Protocols

The VMware View Agent has a very small footprint (90Kb) and supports the full View Client capabilities: PCoIP, RDP, HTTPS, SSL, SSO, USB Redirection, printer support, and session management. The View Agent Connect Direct Plug-in supports two desktop connection protocols: PCoIP and HTML Access.

1.2 About HTML Access (Blast)

HTML Access (formerly known as Blast) enables access to a desktop via any HTML5 compliant web browser.

To use HTML Access:

- Each virtual desktop must have View Agent 6.1.1 and View Agent Direct Connect (VADC) Plug-in service installed and running.
- Virtual Desktops must be running the Horizon DaaS Agent 15.3.2.
- SSL certificate install automation must be configured as described under Automate SSL Installation below.

1.3 System Requirements

Browser on client system:

- Chrome 41, 42, and 43
- Internet Explorer 10 and 11
- Safari 7 and 8 (Mobile Safari is not supported for this release.)
- Firefox 36, 37, and 38

Client operating systems:

- Windows 7 SP1 (32- or 64-bit)
- Windows 8.x desktop (32- or 64-bit)
- Windows 10 desktop (32- or 64-bit)
- Mac OS X Mavericks (10.9)

- Mac OS X Yosemite (10.10)
- Chrome OS 28.x or later

1.4 HTML Access (Blast) Support for RDSH Applications

Launching RDSH applications is supported in HTML Access 3.4.

To enable this functionality:

1. In the Enterprise Center, select **configuration ► general**.
2. Select the check box under HTML Access for RDSH Remote Applications and click **Save**.
3. Click **OK** in the informational dialog box to confirm the action.

Note the following:

- Horizon View Agent 6.1.1 and the View Agent Direct-Connection (VADC) Plug-In 6.1.1 must be installed on the desktops.

  Note: When you enable HTML Access for RDSH applications in Enterprise Center as described below, users will no longer be able to connect to VMs running older versions of the View Agent via Blast.

- Access Point 2.0 remote access gateway must be deployed (confirm with your Service Provider).
- This functionality does not work for iOS or Android.

Note: Attempts to launch applications via HTML Access (Blast) fail with an error when the older version of the HTML Access client is still selected. To prevent this error, verify that the HTML Access for RDSH Remote Applications option is enabled and that the prerequisites have been met as described above.

2 Setup Procedure

2.1 Install Correct Browser

See list of supported browsers in System Requirements.

2.2 Prepare Desktops to Support Protocol

Before installing the software required to connect to desktops, complete the following pre-installation steps.

Procedure

1. Uninstall all software components related to all other protocols.

   Important: You must uninstall all software components related to all other protocols (e.g. HDX, RGS). If you do not uninstall these other protocol components, your template will be corrupted and you will no longer successfully boot into Windows. This warning does not apply to RDP; the presence of RDP components does not cause problems.

2. Update VMware Tools.
3. Make sure that port 443 is not being used by any other software.
4. Enable the Windows Firewall if not already enabled.
5. Make sure that the following ports are open to TCP and/or UDP traffic as indicated:

Port(s)	Source	Destination	TCP	UDP
4172	Access Point	VM	✓	✓
443	Tenant Appliance	VM	✓	
22443	Access Point	VM	✓	

2.3 Install DaaS Agent

Procedure

1. Copy the DaaS Agent executable file (VMware-DaaS-Agent-*x.x.x*.msi) to each VM.
2. Run the DaaS Agent executable file.

   Note: You must use the DaaS Agent 6.1.0 or higher for HTML Access (Blast) functionality.

2.4 Install VMware View Agent

There are three possible scenarios when installing the View Agent

- Install View Agent on Desktop (Windows7/8/XP)
- Install View agent on Windows Server 2008R2/2012 as Personal Desktop (Non-RDSH)

- Install View Agent on Windows Server 2008R2/2012 as RDSH Role

2.4.1 Install View Agent on Desktop (Windows7/8/XP)

Note: If there is an option for which Internet Protocol to use (IPv4 or IPv6), be sure that IPv4 is selected.

Procedure

1. Download VMware Horizon View Agent from VMware's website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.
2. Double-click the View Agent installation file (file name is: VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe). The Welcome window appears, click **Next**.
3. The **License Agreement** window appears. **Accept** the license agreement, click **Next**.
4. The **Desktop OS Configuration** window appears. Click **Next**.
5. The **Custom Setup** window appears. Customize the components that you want to install, and **choose the location** where you want to install the View Agent. Click **Next**.
6. The **Remote Desktop Protocol Configuration** page appears. Select **Enable the Remote desktop capability on this computer** and click **Next**.
7. The **Ready to Install the Program** page appears. Click **Install**.
8. The **Installing View Agent** page appears and shows the installation process.

   During installation, a window pops up asking "Would you like to install this device software?" Check **Always trust software from VMware, Inc.** and click **Install**.
9. The installation takes a few minutes to finish. When it finishes, the **Installer Completed** page appears. Click **Finish**.
10. The View Agent Installer Information window appears, requiring restart of the system. Select **Yes** to restart your virtual machine.

2.4.2 Install View agent on Windows Server 2008R2/2012 as Personal Desktop (Non-RDSH)

Note: If there is an option for which Internet Protocol to use (IPv4 or IPv6), be sure that IPv4 is selected.

Procedure

1. Download VMware Horizon View Agent from VMware's website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.
2. Double-click the View Agent installation file (file name is: VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe). The Welcome window appears, click **Next**.
3. The **License Agreement** window appears. **Accept** the license agreement, click **Next**.
4. The **Desktop OS Configuration** window appears. Select **Install View Agent in 'desktop mode'** and click **Next**.
5. The **Custom Setup** window appears. Customize the components that you want to install, and **choose the location** where you want to install the View Agent. Click **Next**.
6. The **Remote Desktop Protocol Configuration** page appears. Select **Enable the Remote desktop capability on this computer** and click **Next**.

7. The **Ready to Install the Program** page appears. Click **Install**.
8. The **Installing View Agent** page appears and shows the installation process.

   During installation, a window pops up asking "Would you like to install this device software?" Check **Always trust software from VMware, Inc.** and click **Install**.
9. The installation takes a few minutes to finish. When it finishes, the **Installer Completed** page appears. Click **Finish**.
10. The View Agent Installer Information window appears, requiring restart of the system. Select Yes to restart your virtual machine.

2.4.3 Install View Agent on Windows Server 2008R2/2012 as RDSH Role

Note: To install the View Agent in this scenario, you MUST run the command line install and cannot use the default "double click" GUI.

Note: If there is an option for which Internet Protocol to use (IPv4 or IPv6), be sure that IPv4 is selected.

Procedure

1. Download VMware Horizon View Agent from VMware's website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.
2. Run the following on the command line as an administrator user:

   `VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"`

   The **Welcome** window appears, click **Next**.
3. The **License Agreement** window appears. **Accept** the license agreement, click **Next**.
4. The **Custom Setup** window appears. Customize the components that you want to install, and **choose the location** where you want to install the View Agent. Click **Next**.
5. The **Remote Desktop Protocol Configuration** page appears. Select **Enable the Remote desktop capability on this computer** and click **Next**.
6. The **Ready to Install the Program** page appears. Click **Install**.
7. The **Installing View Agent** page appears and shows the installation process.

   During installation, a window pops up asking "Would you like to install this device software?" Check **Always trust software from VMware, Inc.** and click **Install**.
8. The installation takes a few minutes to finish. When it finishes, the **Installer Completed** page appears. Click **Finish**.
9. The View Agent Installer Information window appears, requiring restart of the system. Select Yes to restart your virtual machine.

2.5 Install VMware View Agent Direct Connect Plug-in

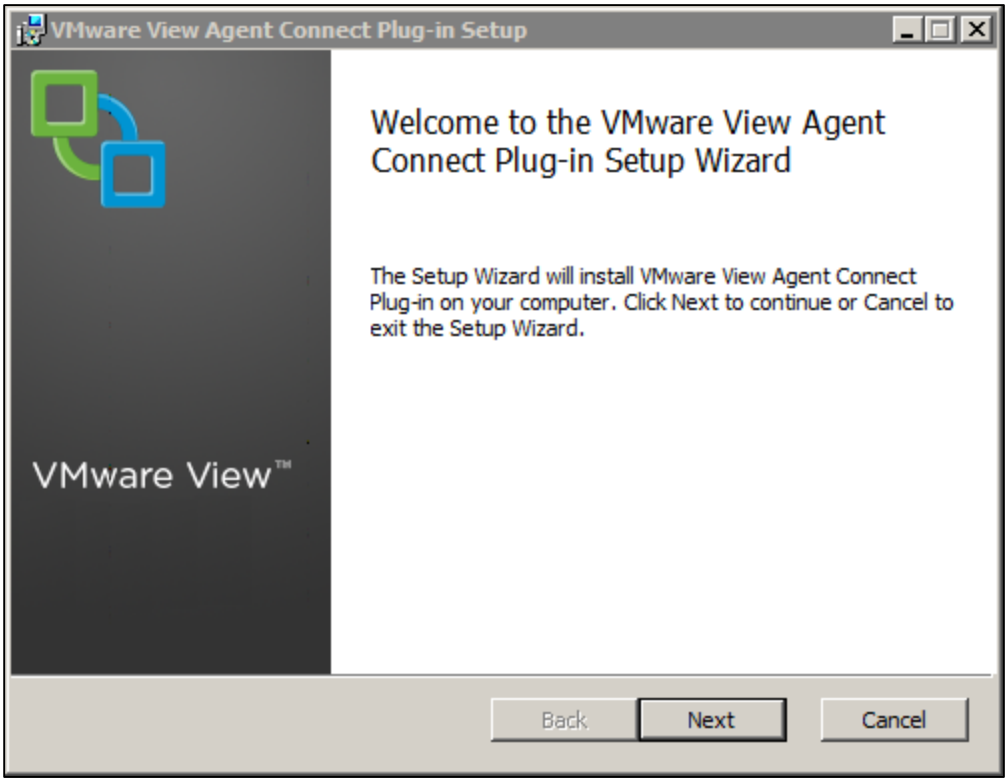
Procedure

1. Log in to the virtual machine as an administrator and launch the installer that is appropriate for your operating system.

Operating System	Installer
Windows 64-bit	VMware-viewagent-direct-connection-x86_64-x.y.z-nnnnnn.exe
Windows 32-bit	VMware-viewagent-direct-connection-x.y.z-nnnnnn.exe

   The installer confirms that the correct version of the Windows operating system and View Agent is installed.

2. Double click on the View Agent Direct Connect Plug-in executable to start the installation. The VMware Horizon View Agent Direct Connect Plug-In Setup Wizard launches:



3. Click **Next** and accept the terms of the license agreement.
4. Click **Next** and accept the default port settings.
5. Click **Next** and then click **Install** to begin the installation.
6. In the Windows Control Panel, verify that VMware View Agent Direct Connect appears in the list of installed programs (Control Panel\Programs\Programs and Features). If not, the installation did not complete properly and you will need to reinstall.

2.6 Add the HTML Access (Blast) Group Policy Settings to the Local Computer Policy Environment

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	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 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.

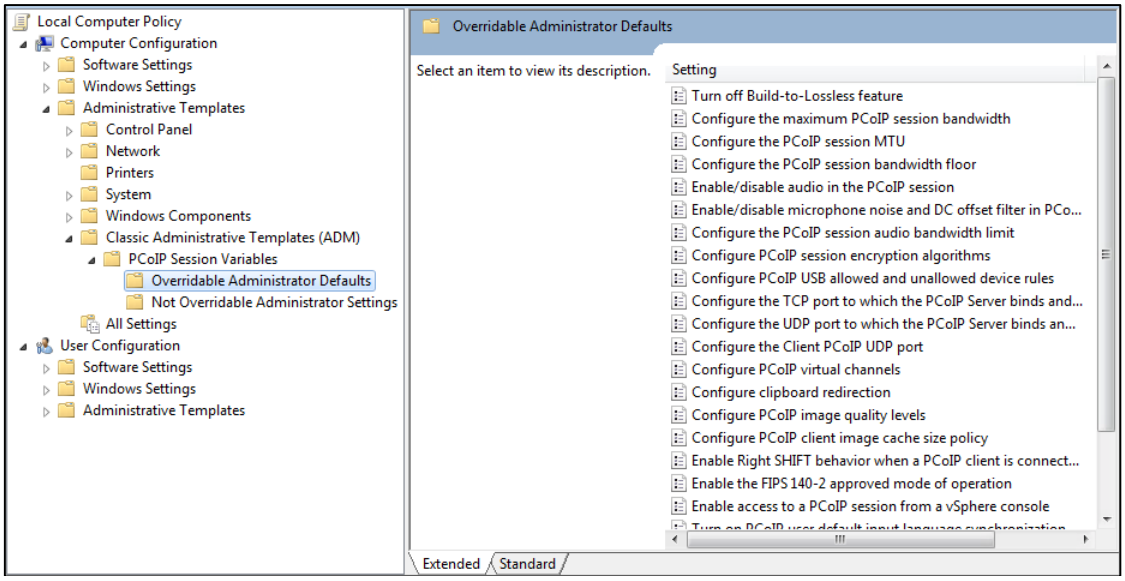
   The VMware HTML Access folder appears in the left pane under **Administrative Templates > Classic Administrative Templates**.

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.



2.7 Automate SSL Installation

The process described in this section is needed to facilitate internal access that is not via Access Point. If you do not have users requiring this type of access, you do not need to perform this procedure.

Note the following:

- **You must follow this process on the gold pattern before converting the VM as a gold pattern or reseal.**
- **You must repeat this process each time you open and re-seal a gold pattern.**

You can install the certificate using post sysprep script execution in order to avoid sysprep issues and duplicate certificate problems. You can also use your own own standard practice as well (for example, Active Directory GPO and scripts). Please read the Horizon View feature pack documentation for SSL certificate requirements.

Follow the steps below to configure post sysprep commands/scripts in the Horizon DaaS environment.

- Import certificate on test machine and note certificate thumbprint.
- Create post sysprep script/batch file on gold pattern image and copy certificate.
- Convert image to gold pattern or reseal.

2.7.1 Import Certificate and Record Certificate Thumbprint

Procedure

1. Add the certificate snap-in to MMC by performing the steps below.

   In order to add certificates to the Windows certificate store, you must first add the certificate snap-in to the Microsoft Management Console (MMC). Before you begin, verify that the MMC and certificate snap-in are available on the Windows guest operating system.

   a. On the desktop, click **Start** and type `mmc.exe`

   b. In the MMC window, select **File > Add/Remove Snap-in**.

c. In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.

d. In the Certificates snap-in window, select Computer account, click **Next**, select local computer, and click **Finish**.

e. In the Add or Remove snap-in window, click **OK**.

2. Import a certificate for the HTML Access Agent into the Windows Certificate Store by performing the steps below.

   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. Before you begin, verify that the HTML Access Agent is installed, the CA-signed certificate was copied to the desktop, and the certificate snap-in was added to MMC (see Step 1 above).

   a. In the MMC window, expand the Certificates (Local Computer) node and select the Personal folder.

   b. In the Actions pane, select **More Actions > All Tasks > Import**.

   c. In the Certificate Import wizard, click **Next** and browse to the location where the certificate is stored.

   d. 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.

   e. Type the password for the private key that is included in the certificate file.

   f. Select **Mark this key as exportable**.

   g. Select **Include all extendable properties**.

   h. Click **Next** and click **Finish**.

      The new certificate appears in the Certificates (Local Computer) > Personal > Certificates folder.

   i. Verify that the new certificate contains a private key.

      1) In the Certificates (Local Computer) > Personal > Certificates folder, double-click the new certificate.

      2) 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.

3. Import root and intermediate certificates for the HTML Access Agent

   If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

   a. In the MMC console, 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 b.

   b. Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

c. In the Certificate Import wizard, click **Next** and browse to the location where the root CA certificate is stored.

d. Select the root CA certificate file and click **Open**.

e. Click **Next**, click **Next**, and click **Finish**.

f. 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.

1) Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

2) Repeat steps c through f for each intermediate certificate that must be imported.

4. In the certificate MMC window, navigate to the Certificates (Local Computer) > Personal > Certificates folder.

5. Double-click the CA-signed certificate that you imported into the Windows certificate store.

6. In the Certificates dialog box, click the Details tab, scroll down, and select the Thumbprint icon.

7. 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.

2.7.2 Create Post Sysprep Script/Batch File on Gold Pattern Image and Copy Certificate

2.7.2.1 Windows 7 and Later

Use post build configuration script "SetupComplete.cmd "to import the SSL certificate and configure the VMware HTML Access registry.

http://technet.microsoft.com/en-us/library/dd744268%28v=ws.10%29.aspx

For example:

- Copy the SSL certificate file under C: drive. For this example, the "C:\desktone_ca_cert" file.
- Create a file SetupComplete.cmd under "%WINDIR%\Setup\Scripts\" folder. Create "Scripts" folder if it does not exist.
- Add following commands in SetupComplete.cmd file. The thumbprint value is what you copied in Step 1.
- Note that if you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in batch file.

```
CertUtil  -importPFX -f  -p "<password>" "C:\desktone_ca_cert.pfx"

        reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash"
/t REG_SZ /d "31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
```

```
del /F /Q "C:\desktone_ca_cert.pfx"

del /F /Q "%systemroot%\setup\scripts\SetupComplete.cmd"
```

- Save the SetupComplete.cmd file. You can test the SetupComplete.cmd file on test machine.

2.7.2.2 Windows XP

- Follow the Desktone post sysprep command execution approach to import the SSL certificate and configure the VMware HTML Access registry.
- Install the Administration Tools Pack for Windows XP as the CertUtil tool is not available with the OS install.

  http://www.microsoft.com/en-us/download/details.aspx?id=16770

  For example:

  - Copy the SSL certificate file under C: drive. For this example, the `C:\desktone_ca_cert.pfx` file.
  - Create a folder path `C:\Sysprep\i386\$OEM$\`
  - Now create `postprep-extra.bat` file under `C:\Sysprep\i386\$OEM$\` and add the following commands in the batch file. The thumbprint value is the one you recorded above after importing the certificate.
  - Note that if you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in the vbatch file.

    ```
    CertUtil  -importPFX -f  -p "<password>" "C:\desktone_ca_cert.pfx"

    del /F /Q "C:\desktone_ca_cert.pfx.pfx"

    reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t
    REG_SZ /d "31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
    ```

  - Save the postprep-extra.bat file. You do not need a command to delete the batch `postprep-extra.bat` file as sysprep deletes the `C:\Sysprep` folder after successful deployment.
  - You can test the `SetupComplete.cmd` file on the test machine.

2.7.3 Convert Image to Gold Pattern or Reseal

Procedure

1. Convert the image as a gold pattern or reseal, and create a pool.
2. Verify the HTML Access connection for the certificate, or check certificates and HTML Access registry on desktops.

Note: If the HTML Access (Blast) service generates the self-signed certificate even after you set the valid CA certificate as described above, then you can troubleshoot this issue by looking at the logs located here: %ProgramData%\VMWare\Vmware Blast\Blast-worker.txt

3 Troubleshoot Connection Problems

There are several configuration/setup problems that can result in an inability to launch a HTML Access (Blast) connection successfully:

- Browser is not HTML5 compliant. Check that the browser version is one cited in the requirements.
- Pop-up blocker enabled. The browser's pop-up blocker could prevent opening the new window for a HTML Access connection. Make sure that the user disables the pop-up blocker for the Desktop Portal.
- Windows firewall disabled. Make sure that the Windows Firewall is installed and running on the user's desktop. A disabled Windows Firewall will result in errors reported in the HTML Access logs.
- Certificate errors. If you receive an error that indicates a missing or non-matching certificate, review the instructions above under Import Certificate and Record Certificate Thumbprint and confirm that you have performed the necessary steps.

  Note: You must repeat this process each time you open and re-seal a gold pattern.

4 Known Limitations and Workarounds

- An SSL certificate warning will be displayed upon connecting to the desktop. This is because the SSL certificate process was not performed correctly on a tenant gold pattern.
- Changing resolution to 2560x1920 ends the HTML Access session. This happens due to lack of vRAM allocation. For more information see Estimating Memory Requirements for Virtual Desktops in the View documentation.
- If your client system uses a super high resolution monitor (such as 2560 x 1600), HTML Access fails to display the desktop.

  Workaround: Lower the resolution on your monitor and connect. The resolution on the client monitor must be less than 2560 x 1600 if the remote desktop resolution is 1920 x 1200.
- Sound playback quality is best on browsers that have Web Audio API support, such as Chrome, Safari, and Firefox 25. Browsers that do not have this support include Internet Explorer (up to and including Internet Explorer 11) and Firefox 24 and earlier.
- Black artifacts appear on the screen on ESXi 5.1 or 5.0 hosts. This is a known HTML Access issue when the desktop HW version is 9 (ESX 5.0/5.1) with 3D disabled and the Windows 7 basic theme is used. This is not an issue when Aero is turned on or when the VM uses HW version 10 (ESX 5.5).
- View Agent session timeout may occur before the Desktop Portal session timeout, resulting in "Authentication error" connecting to the desktop via HTML Access. The workaround for this this is to log out of Desktop Portal and log in again.

For additional known limitations, see Known Issues in the *HTML Access Release Notes*.