# VMware Horizon View Feature Pack Installation and Administration

Horizon View 5.3

Horizon View Feature Pack 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-001301-01

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

# VMware Horizon View Feature Pack Installation and Administration

The *VMware Horizon View Feature Pack Installation and Administration Guide* provides information about installing and configuring the VMware® Horizon View™ Feature Pack components.

The information in this document includes system requirements and instructions for installing the Remote Experience Agent on Horizon View desktops and the HTML Access installer on View Connection Server instances. Post-installation configuration tasks are also described.

## Intended Audience

This document is intended for administrators who install and configure the Feature Pack in a Horizon View deployment. The information is written for experienced system administrators who are familiar with virtual machine technology and datacenter operations. If you are a novice user of Horizon View, you might need to refer to the step-by-step instructions for basic procedures in the *VMware Horizon View Installation* and *VMware Horizon View Administration* documents.

## VMware Horizon View Feature Pack Components

The VMware Horizon View Feature Pack includes two installers that deliver the Feature Pack components in a Horizon View environment. The Remote Experience Agent installer configures the components on Horizon View desktops. The HTML Access installer configures View Connection Server to provide access to desktops through HTML Access.

### Remote Experience Agent installer

The Remote Experience Agent installs Feature Pack components on Horizon View desktops, enhancing the remote desktop experience provided by View Agent 5.3. This program installs the following components:

- HTML Access Agent
- Flash URL Redirection
- Real-Time Audio-Video
- Unity Touch
- Windows 7 Multimedia Redirection (MMR)

The Feature Pack components allow users to take advantage of several new desktop features.

**HTML Access Agent**

The HTML Access Agent allows users to connect to Horizon View desktops by using HTML Access. The HTML Access Agent must be running on a desktop to enable HTML Access on that desktop.

Therefore, to use HTML Access, you must install the Remote Experience Agent with the HTML Access feature.

**Flash URL Redirection**

Flash URL Redirection intercepts and redirects a ShockWave Flash (SWF) file from the remote desktop to the client endpoint. Without this feature, multicast or unicast video data is streamed from an Adobe Media Server to the virtual desktops running on ESXi hosts. The data is then resent in individual PCoIP sessions from each virtual desktop to each client endpoint.

Flash URL Redirection allows Flash content from Adobe Media Server to stream directly to the client endpoints and bypass the virtual desktop infrastructure. The Flash content is then displayed using the clients' local Flash media players.

Streaming Flash content directly from the Adobe Media Server to the client endpoints lowers the load on the datacenter ESXi host, removes the extra routing through the datacenter, and reduces the bandwidth required to simultaneously stream Flash content to multiple client endpoints.

**Real-Time Audio-Video**

Real-Time Audio-Video allows Horizon View users to run Skype, Webex, Google Hangouts, and other online conferencing applications on their virtual desktops. With Real-Time Audio-Video, webcam and audio devices that are connected locally to the client system are redirected to the remote desktop. This feature redirects video and audio data to the desktop with a significantly lower bandwidth than can be achieved by using USB redirection.

Real-Time Audio-Video is compatible with standard conferencing applications and supports standard webcams, audio USB devices, and analog audio input.

This feature installs the VMware Virtual Webcam and VMware Virtual Microphone on the desktop operating system. When a conferencing application is launched, it displays and uses these VMware virtual devices, which handle the audio-video redirection from the locally-connected devices on the client. The VMware Virtual Microphone also appears in the Device Manager on the desktop operating system.

The drivers for the audio and webcam devices must be installed on your Horizon View Client systems to enable the redirection.

Real-Time Audio-Video is not supported on local mode desktops.

This feature provides an ADM Template file that lets you install Real-Time Audio-Video group policy settings on Active Directory or on individual desktops. With these settings, you can change the webcam's default maximum frame rate and image resolution, and you can disable or enable the feature altogether.

**Unity Touch**

With Unity Touch, tablet and smart phone users can easily browse, search, and open Windows applications and files, choose favorite applications and files, and switch between running applications, all without using the Start menu or Taskbar. The VMware Horizon View Client documents for iOS and Android devices provide more information about end user features provided by Unity Touch.

**Windows 7 Multimedia Redirection (MMR)**

This feature extends MMR to Windows 7 desktops and clients.

MMR delivers the multimedia stream directly to client computers. With MMR, the multimedia stream is processed, that is, decoded, on the client system. The client system plays the media content, thereby offloading the demand on the ESXi host.

### HTML Access installer

This installer configures View Connection Server instances to allow users to select HTML Access to connect to desktops. After you run the HTML Access installer, the View Portal displays an HTML Access icon in addition to the View Client icon.

You must run this installer if you want to use HTML Access to connect to desktops in a Horizon View deployment. Running this installer is also required if your users go through Horizon Workspace and select HTML Access to connect to desktops.

## Setup and Installation

To set up the Horizon View Feature Pack, you install the Remote Experience Agent on Horizon View desktops and the HTML Access installer on View Connection Server instances.

### System Requirements for the Horizon View Feature Pack

Horizon View desktops and View Connection Server instances must meet certain software requirements to support the Feature Pack components.

**View Connection Server**

View Connection Server 5.3

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

**Horizon 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-bit or 64-bit), Windows 8 (32-bit or 64-bit), Windows 8.1 (32-bit or 64-bit), or Windows Server 2008 R2

  **NOTE** Certain individual Feature Pack components are supported on only some of the supported desktop operating systems. See Table 1.

- View Agent 5.3

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

Table 1 shows the desktop operating systems on which each Feature Pack component is supported.

**Table 1.** Horizon View Desktop Operating System Support for Individual Feature Pack Components

| Feature Pack Component | Windows XP SP3 (32-bit) | Windows Vista (32-bit) | Windows 7 (32-bit or 64-bit) | Windows 8 or Windows 8.1 (32-bit or 64-bit) | Windows Server 2008 R2 |
|---|---|---|---|---|---|
| HTML Access Agent | Yes | Yes | Yes | Yes (Tech Preview) | Yes |
| Flash URL Redirection | No | No | Yes | No | No |
| Real-Time Audio-Video | Yes | Yes | Yes | Yes | Yes |
| Unity Touch | Yes | Yes | Yes | Yes | Yes |
| Windows 7 MMR | No | No | Yes | No | No |

The supported Feature Pack components are installed by default when you run the Remote Experience Agent installer. You can choose not to install a component by deselecting it during the installation.

To support individual Feature Pack components, your Horizon View deployment must meet additional software and hardware requirements.

## 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.

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

Configuration instructions are provided in the topic "Prepare View Desktops and Pools for HTML Access," in the *Using VMware Horizon View HTML Access* document.

**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 "Install HTML Access Software on View Connection Server," on page 20.

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.

## System Requirements for Flash URL Redirection

To support Flash URL Redirection, your Horizon View deployment must meet certain software and hardware requirements.

**Flash media player and ShockWave Flash (SWF)**

You must integrate an appropriate Flash media player such as Strobe Media Playback into your Web site. To stream multicast content, you can use `multicastplayer.swf` or `StrobeMediaPlayback.swf` in your Web pages. To stream live unicast content, you must use `StrobeMediaPlayback.swf`. You can also use `StrobeMediaPlayback.swf` for other supported features such as RTMP streaming and HTTP dynamic streaming.

**Horizon View desktop**

- The desktops must run Windows 7 64-bit or 32-bit operating systems.
- The desktops must have View Agent 5.3 installed.
- Supported desktop browsers include Internet Explorer 8, 9, and 10, Chrome 29.*x*, and Firefox 20.*x*.

**Horizon View Client software**

The following Horizon View Client releases support multicast and unicast:

- Horizon View Client 2.2 for Linux or a later release
- Horizon View Client 2.2 for Windows or a later release

The following Horizon View Client releases support multicast only (they do not support unicast):

- Horizon View Client 2.0 or 2.1 for Linux
- Horizon View Client 5.4 for Windows

**View Client computer or client access device**

- Flash URL Redirection is supported on all operating systems that run Horizon View Client for Linux on x86 Thin client devices. This feature is not supported on ARM processors.
- Flash URL Redirection is supported on all operating systems that run Horizon View Client for Windows. For details, see the *Using VMware Horizon View Client for Windows* document.
- On Windows client devices, you must install Adobe Flash Player 10.1 or later for Internet Explorer.
- On Linux Thin client devices, you must install the `libexpat.so.0` and `libflashplayer.so` files. See "Set Up Client Devices for Flash URL Redirection," on page 31.

**Note** With Flash URL Redirection, the multicast or unicast stream is redirected to client devices that might be outside your organization's firewall. Your clients must have access to the Adobe Web server that hosts the ShockWave Flash (SWF) file that initiates the multicast or unicast streaming. If needed, configure your firewall to open the appropriate ports to allow client devices to access this server.

## System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard webcam, USB audio, and analog audio devices, and with standard conferencing applications like Skype, WebEx, and Google Hangouts. To support Real-Time Audio-Video, your Horizon View deployment must meet certain software and hardware requirements.

| | |
|---|---|
| **Horizon View desktop** | The desktops must have View Agent 5.3 installed. Real-Time Audio-Video is supported on all Windows guest operating systems that support View Agent 5.3. |
| **Horizon View Client software** | Horizon View Client 5.4 for Windows<br>Horizon View Client 2.2 for Windows or a later release<br>**Note** Horizon View Client 2.2 for Windows is a later release than Horizon View Client 5.4 for Windows. The release number for Windows is now consistent with the Horizon View Client releases on other operating systems and devices.<br>Horizon View Client 2.2 for Linux or a later release. Note that this feature is available only with the version of Horizon View Client for Linux provided by third-party vendors. |
| **View Client computer or client access device** | ■ Real-Time Audio-Video is supported on all operating systems that run Horizon View Client for Windows. For details, see the *Using VMware Horizon View Client for Windows* document.<br>■ Real-Time Audio-Video is supported on all operating systems that run Horizon View Client for Linux on x86 devices. This feature is not supported on ARM processors. For details, see the *Using VMware Horizon View Client for Linux* document.<br>■ The webcam and audio device drivers must be installed, and the webcam and audio device must be operable, on the client computer. To support Real-Time Audio-Video, you do not have to install the device drivers on the desktop operating system where View Agent is installed. |
| **Display protocol for Horizon View** | PCoIP<br>Real-Time Audio-Video is not supported in RDP desktop sessions. |

## System Requirements for Unity Touch

Horizon View Client software and the mobile devices on which you install Horizon View Client must meet certain version requirements to support Unity Touch.

| | |
|---|---|
| **Horizon View Client software** | Unity Touch is supported on the following Horizon View Client versions:<br>■ Horizon View Client 2.0 for iOS or later<br>■ Horizon View Client 2.0 for Android or later |
| **Mobile device operating systems** | Unity Touch is supported on the following mobile device operating systems:<br>■ iOS 5.0 and later |

| | |
|---|---|
| | ■ Android 3 (Honeycomb), Android 4 (Ice Cream Sandwich), and Android 4.1 and 4.2 (Jelly Bean) |
| **Horizon View desktop** | To support Unity Touch, the following software must be installed in the virtual machine that the end user will access:<br>■ Operating systems: Windows XP SP3 (32-bit), Windows Vista (32-bit), Windows 7 (32-bit or 64-bit), Windows 8 (32-bit or 64-bit), Windows 8.1 (32-bit or 64-bit), or Windows Server 2008 R2<br>■ View Agent 5.3<br>Installation instructions are provided in the *VMware Horizon View Administration* document. |

## System Requirements for Windows 7 Multimedia Redirection

To support Windows 7 Multimedia Redirection (MMR), your Horizon View deployment must meet certain software and hardware requirements.

| | |
|---|---|
| **Horizon View desktop** | ■ The desktops must run 64-bit or 32-bit Windows 7 operating systems.<br>■ **3D Rendering** must be enabled on the desktop pool.<br>■ The desktop virtual machines must be virtual hardware version 8 or later.<br>■ Users must play videos on Windows Media Player 12 or later. |
| **Horizon View Client software** | Horizon View Client 2.2 for Windows or a later release |
| **View Client computer or client access device** | ■ The clients must run 64-bit or 32-bit Windows 7 or Windows 8 operating systems.<br>■ The clients must have DirectX Video Acceleration (DXVA)-compatible video cards that can decode the selected videos.<br>■ Windows Media Player 12 or later must be installed on the clients to allow redirection to the local hardware. |
| **Supported media formats** | Media formats must comply with the H.264 video compression standard. The M4V, MP4, and MOV file formats are supported. Your virtual desktops must use one of these file formats, and local decoders for these formats must exist on the client systems. |
| **View policies** | In View Administrator, verify that the **Multimedia redirection (MMR)** policy is set to **Allow**, which is the default value. |
| **Back-end firewall** | If your Horizon View deployment includes a back-end firewall between your DMZ-based security servers and your internal network, verify that the back-end firewall allows traffic to port 9427 on your desktops. |

For a comparison of the Windows 7 Multimedia Redirection (MMR) component and the Wyse MMR component, which operates on Windows XP and Windows Vista desktops, see "Multimedia Redirection Support on Desktop Operating Systems," on page 13.

### Multimedia Redirection Support on Desktop Operating Systems

Windows 7 Multimedia Redirection (MMR) is a feature pack component that is installed with the Remote Experience Agent. The Wyse MMR component is installed with View Agent and operates on Windows XP and Windows Vista desktops. Windows 7 MMR has somewhat different characteristics and requirements than the Wyse MMR component.

**Table 2.** Horizon View Desktop Operating System Support for Multimedia Redirection

| Desktop Operating System | Desktop Virtual Machine Requirements | Supported Media Formats | Supported Clients | Audio Redirection |
|---|---|---|---|---|
| Windows XP, Windows Vista | Windows Media Player 10 or later must be installed. | Many formats are supported. For example:<br>MPEG2-1; MPEG2; MPEG-4 Part 2;WMV 7, 8, and 9; WMA; AVI; ACE; MPT3; WAV | Windows XP, Windows Vista, Windows 7<br>Windows Media Player 10 or later must be installed. | The audio stream is redirected to the client system. |
| Windows 7 | The desktops must be virtual hardware version 8 or later.<br>**3D Rendering** must be enabled.<br>Windows Media Player 12 or later must be installed. | H.264 compression standard in M4V, MP4, or MOV format. | Windows 7, Windows 8<br>The clients must have DirectX Video Acceleration (DXVA)-compatible video cards that can decode the selected videos.<br>Windows Media Player 12 or later must be installed. | The audio stream is not redirected. Audio is delivered over PCoIP from the remote desktop to the client system. |
| Windows 8 | Not supported | Not supported | Not supported | Not supported |

For more information about MMR system requirements on Horizon View clients, see the *Using VMware Horizon View Client for Windows* document.

## Installing and Deploying the Remote Experience Agent on Horizon View Desktops

Run the Remote Experience Agent installer to install the Feature Pack components on Horizon View desktops. You can use the interactive Remote Experience Agent installer or run the installer silently from the command line.

If you intend to create a new desktop pool, install the Remote Experience Agent on a parent virtual machine. Take a snapshot or make a template from the virtual machine and create the desktop pool.

If you intend to install the Feature Pack components on an existing desktop pool, the approach you take depends on the type of desktop pool. For example, for a linked-clone pool with floating assignments, you can run the Remote Experience Agent installer on the parent virtual machine and recompose the linked clones. For a full-clone pool or a pool that you do not recompose, you can install the Remote Experience Agent silently on the desktops. You might use your own script or a software distribution tool to perform the distributed installation.

## Upgrading the Remote Experience Agent

If an earlier release of the Remote Experience Agent is installed on your desktops, install the current release to obtain the latest versions of the Feature Pack components.

Before you can install the Remote Experience Agent that is provided with Horizon View 5.3 Feature Pack 1, you must install View Agent 5.3 on your desktops. Installing View Agent 5.3 removes any earlier release of the Remote Experience Agent and its associated Feature Pack components. You can then install the current release of the Remote Experience Agent, which performs a fresh installation of the Feature Pack components.

## Install the Remote Experience Agent Interactively

Install the Remote Experience Agent to configure the Feature Pack components on Horizon View desktops.

The HTML Access Agent component is required for HTML Access. For information about setting up Horizon View desktops and pools for HTML Access, see "Prepare View Desktops and Pools for HTML Access" in the *Using VMware Horizon View HTML Access* document, located on the VMware Horizon View Clients Documentation page.

**Important** Do not install or uninstall the Remote Experience Agent from within a View desktop session that was established through View Client or HTML Access. Run the installer directly on the virtual machine. For example, you can open a console on the virtual machine in vSphere Web Client or vSphere Client.

### Prerequisites

- Verify that View Agent 5.3 is installed on the virtual machine.
- Verify that you have administrative rights on the virtual machine.
- Verify that the Windows Firewall service is running on the virtual machine. If the Windows Firewall service is not started and running, the Remote Experience Agent installation cannot be completed.
- Familiarize yourself with the features that can be installed by the Remote Experience Agent. See "Remote Experience Agent Installation Options," on page 15.
- Verify that you have access to the Remote Experience Agent installer file on the VMware product page at http://www.vmware.com/products/.

### Procedure

1 Download the Remote Experience Agent installer file from the VMware product page.

Select the appropriate installer file, where *y.y* is the Feature Pack version number and *xxxxxx* is the build number.

| Option | Description |
|---|---|
| **32-bit installer** | `VMware-Horizon-View-5.3-Remote-Experience-Agent-`*`y.y`*`-`*`xxxxxx`*`.exe` |
| **64-bit installer** | `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-`*`y.y`*`-`*`xxxxxx`*`.exe` |

2 Double-click the installer file to start the Remote Experience Agent installation program.

3 Accept the VMware End User License Agreement.

4 Select your installation options.

Use the drop-down menu for an individual feature to select or deselect that feature for installation.

5 Click **Install**.

When the installation is completed, the installer displays the following message: `Setup has successfully installed VMware Horizon View 5.3 Remote Experience Agent`.

6 Click **Finish**.

When the HTML Access Agent is installed on the virtual machine, TCP port 22443 is opened on the Windows firewall. See "Firewall Rules for HTML Access," on page 22.

### What to do next

If you installed the Remote Experience Agent on a parent virtual machine, create a snapshot or make a template and create a Horizon View desktop pool, or recompose an existing pool.

## Remote Experience Agent Installation Options

When you install the Remote Experience Agent on a virtual machine, you can select installation options.

| Option | Description |
|---|---|
| HTML Access | Allows users to connect to Horizon View desktops by using HTML Access. The HTML Access Agent must be installed on Horizon View desktops to allow users to make connections with HTML Access.<br>This feature is installed by default. |
| Flash URL Redirection | Redirects Flash URL multicast or unicast streaming data from virtual desktops to client devices. This feature allows videos to be streamed directly from a multicast or unicast Web source to the client hardware and displayed to users on the client's local Flash media player.<br>This feature is installed by default. |
| Real-Time Audio-Video | Redirects webcam and audio devices that are connected to the client system so that they can be used on the remote desktop.<br>This feature is installed by default. |
| Unity Touch | Provides tablet and smart phone users a convenient sidebar they can touch to browse, search, open, and close Windows applications and files, and switch between running applications.<br>This feature is installed by default. |
| Win7 Multimedia Redirection | Extends multimedia redirection to Windows 7 desktops and clients. This feature delivers a multimedia stream directly to the client computer, allowing the multimedia stream to be processed on the client hardware instead of the remote ESXi host.<br>This feature is installed by default. |

## Install the Remote Experience Agent Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install the Remote Experience Agent on several Windows virtual machines. In a silent installation, you use the command line and do not have to respond to wizard prompts.

The Remote Experience Agent installer configures the Feature Pack components on Horizon View desktops.

**Important** Do not install or uninstall the Remote Experience Agent from within a View desktop session that was established through View Client or HTML Access. Run the installation command directly on the virtual machine. For example, you can open a console on the virtual machine in vSphere Web Client or vSphere Client.

### Prerequisites

- Verify that View Agent 5.3 is installed on the virtual machine.
- Verify that you have administrative rights on the virtual machine.
- Verify that the Windows Firewall service is running on the virtual machine. If the Windows Firewall service is not started and running, the Remote Experience Agent installation cannot be completed.

- Verify that you have access to the Remote Experience Agent installer file on the VMware product page at http://www.vmware.com/products/.
- Familiarize yourself with the silent installation properties available with the Remote Experience Agent. See "Silent Installation Properties for the Remote Experience Agent," on page 16.
- Familiarize yourself with the MSI installer command-line options. See "MSI Command-Line Options for the Remote Experience Agent Installer," on page 17.

### Procedure

1 Download the Remote Experience Agent installer file from the VMware product page.

Select the appropriate installer file, where *y.y* is the Feature Pack version number and *xxxxxx* is the build number.

| Option | Description |
|---|---|
| **32-bit installer** | `VMware-Horizon-View-5.3-Remote-Experience-Agent-`*`y.y-xxxxxx`*`.exe` |
| **64-bit installer** | `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-`*`y.y-xxxxxx`*`.exe` |

2 Open a Windows command prompt on the virtual machine.

3 Type the installation command on one line.

This example installs the Remote Experience Agent on a virtual machine. The installer configures all the Remote Experience Agent installation options and writes logs to the file `install.log`.

```
VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn /l*v
""C:\myfolder\install.log"""
```

**Note** The preceding example installs all publicly available features. To install selected features, use the `ADDLOCAL=` option and list the silent installation properties in a comma-separated list. For example: `ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR`. The `Core` property is required when you use `ADDLOCAL=` to specify selected features.

When the HTML Access Agent is installed on the virtual machine, TCP port 22443 is opened on the Windows firewall. See "Firewall Rules for HTML Access," on page 22.

### What to do next

If you installed the Remote Experience Agent on a parent virtual machine, create a snapshot or make a template and create a Horizon View desktop pool, or recompose an existing pool.

## Silent Installation Properties for the Remote Experience Agent

In a silent installation command, you can use the MSI property, `ADDLOCAL=`, to specify Feature Pack components that the Remote Experience Agent installer configures. Each silent installation feature corresponds to an installation option that you can select or deselect during an interactive installation.

For more information about these features, see "Remote Experience Agent Installation Options," on page 15.

**Table 3.** Remote Experience Agent Silent Installation Features and Interactive Installation Options

| Silent Installation Feature | Installation Option in an Interactive Installation |
|---|---|
| HTMLAccess | HTML Access Agent |
| FlashURLRedirection | Flash URL Redirection |
| RTAV | Real-Time Audio-Video |

**Table 3.** Remote Experience Agent Silent Installation Features and Interactive Installation Options (Continued)

| Silent Installation Feature | Installation Option in an Interactive Installation |
|---|---|
| UnityTouch | Unity Touch |
| MMR | Win7 Multimedia Redirection (MMR) |

## MSI Command-Line Options for the Remote Experience Agent Installer

To install the Remote Experience Agent silently, you must use Microsoft Windows Installer (MSI) command-line options and properties. The installer is an MSI program and uses standard MSI features.

For details about MSI, see the Microsoft Web site. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library Web site and search for MSI command-line options. To see MSI command-line usage, you can open a command prompt on the virtual machine where you are performing the installation and type `msiexec /?`.

**NOTE** The `INSTALLDIR` option is not available with the Remote Experience Agent installer. You cannot change the installation directory.

To run an installer silently, you begin by silencing the bootstrap program that extracts the installer into a temporary directory and starts an interactive installation.

At the command line, you must enter command-line options that control the installer's bootstrap program.

**Table 4.** Command-Line Options for an Installer's Bootstrap Program

| Option | Description |
|---|---|
| `/s` | Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs.<br>For example: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s`<br>The `/s` option is required to run a silent installation. |
| `/v"`*`MSI_command_line_options`*`"` | Instructs the installer to pass the double-quote-enclosed string that you enter at the command line as a set of options for MSI to interpret. You must enclose your command-line entries between double quotes. Place a double quote after the `/v` and at the end of the command line.<br>For example: `VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"`*`command_line_options`*`"`<br>The `/v"`*`command_line_options`*`"` option is required to run a silent installation. |

You control the remainder of a silent installation by passing command-line options and MSI property values to the MSI installer, `msiexec.exe`. The MSI installer uses the values and options that you enter in the command line to interpret installation options that are specific to the Remote Experience Agent installer.

**Table 5.** MSI Command-Line Options and MSI Properties

| MSI Option or Property | Description |
|---|---|
| /qn | Instructs the MSI installer not to display the installer wizard pages.<br>For example, you might want to install the Remote Experience Agent silently and use only default setup options and features:<br>`VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn"`<br>Alternatively, you can use the /qb option to display the wizard pages in a noninteractive, automated installation. As the installation proceeds, the wizard pages are displayed, but you cannot respond to them.<br>The /qn or /qb option is required to run a silent installation. |
| /x | Uninstalls the Remote Experience Agent. For example:<br>`VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qb /x"`<br>For instructions for uninstalling the Remote Experience Agent and returning the Horizon View desktop to a pre-installation state, see "Uninstall the Remote Experience Agent," on page 19. |
| UNITY_DEFAULT_APPS | Specifies a default list of default favorite applications that are displayed in the Unity Touch sidebar on a mobile device. This property was created to support the Unity Touch component. It is not a general MSI property.<br>For information about configuring a default list of favorite applications and about the syntax and format to use with this property, see "Configure Favorite Applications Displayed by Unity Touch," on page 26.<br>The UNITY_DEFAULT_APPS property is optional. |
| ADDLOCAL | Determines the component-specific features to install. In an interactive installation, the installer displays installation options to select. The ADDLOCAL property lets you specify these options on the command line.<br>If you do not use the ADDLOCAL property, the default options are installed.<br>To specify individual installation options, enter a comma-separated list of option names. Do not use spaces between names. Use the format ADDLOCAL=*value*,*value*,*value*.... The option names are case-sensitive. For a list of available installation options, see "Silent Installation Properties for the Remote Experience Agent," on page 16.<br>The following example installs the HTML Access Agent, Unity Touch, Flash URL Redirection, and Real-Time Audio-Video:<br>`VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR"`<br>The Core component is required when you use the ADDLOCAL property to specify installation options.<br>The ADDLOCAL property is optional. |
| REBOOT | You can use the REBOOT=ReallySuppress option to allow system configuration tasks to complete before the system reboots.<br>This MSI property is optional. |

**Table 5.** MSI Command-Line Options and MSI Properties (Continued)

| MSI Option or Property | Description |
|---|---|
| REMOVE | Removes the specified Feature Pack components (installation options) that were installed by the Remote Experience Agent installer.<br>To remove individual installation options, enter a comma-separated list of option names. Do not use spaces between names. Use the format REMOVE=*value*,*value*,*value*.... The option names are case-sensitive. For a list of available installation options, see "Silent Installation Properties for the Remote Experience Agent," on page 16.<br>The following example removes the HTML Access Agent, Unity Touch, Flash URL Redirection, and Real-Time Audio-Video:<br>VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-*y.y-xxxxxx*.exe /s /v"/qn REMOVE=HTMLAccess,UnityTouch,FlashURLRedirection,RTAV,MMR"<br>The REMOVE property is optional. |
| /l*v *log_file* | Writes logging information into the specified log file with verbose output.<br>For example: /l*v ""%TEMP%\vmmsi.log""<br>This example generates a detailed log file that is similar to the log generated during an interactive installation.<br>You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations.<br>The /l*v option is optional. |

## Uninstall the Remote Experience Agent

You can remove the Remote Experience Agent from Horizon View desktops by using the same method you use to remove other Windows software.

The Remote Experience Agent affects certain files that are installed with View Agent 5.3. When you uninstall the Remote Experience Agent, to return your View Agent virtual machine to its pre-installation state, you must either uninstall and reinstall View Agent or repair View Agent.

### Procedure

1 On the virtual machines where the Remote Experience Agent is installed, open the Uninstall a Program applet provided by the Windows Control Panel.

2 Select **VMware Horizon View 5.3 Remote Experience Agent** and click **Uninstall**.

3 Either uninstall and reinstall or repair View Agent.

| Option | Description |
|---|---|
| **Uninstall and reinstall** | a In the Windows Uninstall a Program applet, select **VMware View Agent** and click **Uninstall**.<br>b Launch the VMware View Agent 5.3 installation file to reinstall the software. |
| **Repair** | Launch the VMware View Agent 5.3 installation file and select the **Repair** option. |

4 (Optional) In the Windows Firewall on the virtual machine, verify that TCP port 22443 no longer allows inbound traffic.

### What to do next

If applicable, change the rules in your organization's firewalls to disallow inbound traffic to TCP port 22443 on the desktop virtual machine.

# Installing HTML Access Software on View Connection Server

The HTML Access installer configures the View Portal page on View Connection Server to allow users to select HTML Access when they connect to their desktops. Run the installer on a View Connection Server instance and on all the instances in a replicated group.

By default, when a users opens a browser and enters the URL of a View Connection Server instance, the View Portal page that appears contains links to the VMware Download site for downloading View Client.

After you run the HTML Access installer, the View Portal page displays an HTML Access icon in addition to the View Client icon, allowing users to connect to their desktops through HTML Access. Users do not have to install View Client to connect to their desktops.

You can customize the View Portal page if you want to disable the icon for downloading View Client, disable the icon for connecting through HTML Access, or change the URL of the Web page for downloading View Client. See "Configure the HTML Access Page for End Users" in the *Using VMware Horizon View HTML Access* document, located on the VMware Horizon View Clients Documentation page.

---

**Important** If you previously edited the View Portal page that came with Horizon View or the HTML Access Portal page that came with Horizon View 5.2 Feature Pack 1, those customizations will be lost when you upgrade to a newer version of HTML Access. You can customize the page again after you upgrade. If you previously edited the HTML Access Portal page that came with Horizon View 5.2 Feature Pack 2 or later, your customizations are preserved.

---

For an overview of setting up View Connection Server for HTML Access, see "Preparing View Connection Server and Security Servers for HTML Access" in the *Using VMware Horizon View HTML Access* document, located on the VMware Horizon View Clients Documentation page.

## 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. See "Upgrading the Remote Experience Agent," on page 14.

## Install HTML Access Software on View Connection Server

To configure the View Portal page to display the HTML Access icon for end users, run the HTML Access installer on the View Connection Server instance or instances in a replicated group.

### Prerequisites

- Verify that View Connection Server is Horizon View 5.3.
- Verify that you have access to the HTML Access installer file on the VMware product page at http://www.vmware.com/products/.

### Procedure

1 Download the HTML Access installer file from the VMware product page.

  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.

2 Double-click the installer file to start the HTML Access installation program.

3 Accept the VMware End User License Agreement.

4 Accept or change the installation folder.

5 Click **Install**.

6 Click **Finish**.

### What to do next

Make sure that the port that is used by HTML Access to allow connections to security servers is opened on the Windows firewall. See "Open the Port Used by HTML Access on Security Servers," on page 21.

You can modify the View Portal page by hiding either the View Client icon or HTML Access icon from users. See "Configure the HTML Access Page for End Users" in the *Using VMware Horizon View HTML Access* document, located on the VMware Horizon View Clients Documentation page.

## Open the Port Used by HTML Access on Security Servers

When you install View Connection Server or security server, the View server installer creates the Windows Firewall rule for the port that is used by HTML Access for client connections, but the installer leaves the rule disabled until it is actually needed. When you later install HTML Access on a View Connection Server instance, the HTML Access installer automatically enables the rule to allow communication to that port. However, on security servers, you must manually enable the rule in the Windows Firewall to allow communication to the port.

By default, HTML Access uses TCP port 8443 for client connections to the Blast Secure Gateway.

### Procedure

- To open the port used by HTML Access on a View Connection Server computer, install HTML Access on that computer.

  The HTML Access installer enables the **VMware View Connection Server (Blast-In)** rule in the Windows Firewall.

- To open the port for HTML Access on a security server, manually enable the **VMware View Connection Server (Blast-In)** rule in the Windows Firewall.

## 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.

### 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 Horizon View desktops, your firewalls must allow inbound traffic on certain TCP ports.

HTML Access connections must use HTTPS. HTTP connections are not allowed.

To ensure that the Windows firewall on security servers is configured to allow traffic to the TCP port used by HTML Access, see "Open the Port Used by HTML Access on Security Servers," on page 21.

**Table 6.** 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 Horizon 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 Horizon 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.<br>**Note** The Blast Secure Gateway is installed with View Connection Server in Horizon View 5.2 and later releases. |
| Blast Secure Gateway | TCP Any | HTTPS | HTML Access Agent | TCP 22443 | If the Blast Secure Gateway is enabled, after the user selects a Horizon View desktop, the Blast Secure Gateway connects to the HTML Access Agent on TCP port 22443 on the desktop. |
| Client Web browser | TCP Any | HTTPS | HTML Access Agent | TCP 22443 | If the Blast Secure Gateway is not enabled, after the user selects a Horizon 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. |

## 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 Horizon 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 Horizon 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 Horizon 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 23

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 Horizon 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 23

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 24

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 25

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 Horizon 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 Horizon 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 23.

## 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 Horizon 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 23.

### Procedure

1 In the MMC window on the Horizon 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 24.

Configure the appropriate registry key with the certificate thumbprint. See "Set the Certificate Thumbprint in the Windows Registry," on page 25.

## 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 Horizon 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 25.

## 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 23.

### Procedure

1 In the MMC window on the Horizon View desktop where the HTML Access Agent is installed, navigate to the **Certificates (Local Computer) > Personal > Certificates** folder.

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

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

4 Copy the selected thumbprint to a text file.

   For example: `31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e`

   **Note** When you copy the thumbprint, do not to include the leading space. If you inadvertently paste the leading space with the thumbprint into the registry key (in Step 7), the certificate might not be configured successfully. This problem can occur even though the leading space is not displayed in the registry value text box.

5 Start the Windows Registry Editor on the desktop where the HTML Access Agent is installed.

6 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` registry key.

7 Modify the `SslHash` value and paste the certificate thumbprint into the text box.

8 Restart the VMware Blast service to make your changes take effect.

   In the Windows guest operating system, the service for the HTML Access Agent is called VMware Blast.

When a user connects to a desktop through HTML Access, the HTML Access Agent presents the CA-signed certificate to the user's browser.

# Configure Security Protocols and Cipher Suites for HTML Access Agent

Starting with Feature Pack 5 (FP5), you can configure the security protocols and cipher suites that HTML Access Agent uses by editing the Windows registry. You can also specify the configurations in a group policy object (GPO).

By default, the FP5 HTML Access Agent uses only TLS 1.0, TLS 1.1, and TLS 1.2. The protocols that are allowed are, from low to high, TLS 1.0, TLS 1.1, and TLS 1.2. Older protocols such as SSLv3 and earlier are never allowed. Two registry values, `SslProtocolLow` and `SslProtocolHigh`, determine the range of protocols that HTML Access Agent will accept. For example, setting `SslProtocolLow=tls_1.0` and `SslProtocolHigh=tls_1.2` will cause the HTML Access Agent to accept TLS 1.0, TLS 1.1, and TLS 1.2. The default settings are `SslProtocolLow=tls_1.0` and `SslProtocolHigh=tls_1.2`.

You must specify the list of ciphers using the format that is defined in http://openssl.org/docs/manmaster/apps/ciphers.html, under the section CIPHER LIST FORMAT. The following cipher list is the default:

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

**Procedure**

1 Start the Windows Registry Editor.

2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` registry key.

3 Add two new string (REG_SZ) values, `SslProtocolLow` and `SslProtocolHigh`, to specify the range of protocols.

   The data for the registry values must be `tls_1.0`, `tls_1.1`, or `tls_1.2`. To enable only one protocol, specify the same protocol for both registry values. If any of the two registry values does not exist or if its data is not set to one of the three protocols, the default protocols will be used.

4 Add a new string (REG_SZ) value, `SslCiphers`, to specify a list of cipher suites.

   Type or paste the list of cipher suites in the data field of the registry value. For example,

   ```
   ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
   ```

5 Restart the Windows service VMware Blast.

To revert to using the default cipher list, delete the `SslCiphers` registry value and restart the Windows service VMware Blast. Do not simply delete the data part of the value because the HTML Access Agent will then treat all ciphers as unacceptable, in accordance with the OpenSSL cipher list format definition.

When the HTML Access Agent starts, it writes the protocol and cipher information to its log file. You can examine the log file to determine the values that are in force.

The default protocols and cipher suites might change in the future in accordance with VMware's evolving best practices for network security.

# Configure Unity Touch

You can configure a default list of favorite applications that appear in the Unity Touch sidebar, and you can disable or enable the Unity Touch feature after it is installed.

## Configure Favorite Applications Displayed by Unity Touch

With the Unity Touch feature, tablet and smart phone users can quickly navigate to a Horizon View desktop application or file from a Unity Touch sidebar. Although end users can specify which favorite applications appear in the sidebar, for added convenience, administrators can configure a default list of favorite applications.

If you use floating desktop pools, the favorite applications and favorite files that end users specify will be lost when they disconnect from a desktop unless you enable roaming user profiles in Active Directory.

The default list of favorite applications list remains in effect when an end user first connects to a desktop that is enabled with Unity Touch. However, if the user configures his or her own favorite application list, the default list is ignored. The user's favorite application list stays in the user's roaming profile and is available when the user connects to different desktops in a floating or persistent pool.

If you create a default list of favorite applications and one or more of the applications are not installed in the Horizon View desktop operating system, or the paths to these applications are not found in the Start menu, the applications do not appear in the list of favorites. You can use this behavior to set up one master default list of favorite applications that can be applied to multiple virtual machine images with different sets of installed applications.

For example, if Microsoft Office 2010 and Microsoft Visio are installed on one virtual machine, and Windows Powershell and VMware vSphere Client are installed on a second virtual machine, you can create one list that includes all four applications. Only the installed applications appear as default favorite applications on each respective desktop.

You can use different methods to specify a default list of favorite applications:

- Add a value to the Windows registry on the desktop virtual machines
- Create an administrative installation package from the Remote Experience Agent installer and distribute the package to the virtual machines
- Run the Remote Experience Agent installer from the command line on the virtual machines

---

**Note** Unity Touch assumes that shortcuts to applications are located in the Programs folder in the **Start** menu. If any shortcut is located outside of the Programs folder, attach the prefix **`Programs`** to the shortcut path. For example, `Windows Update.lnk` is located in the `ProgramData\Microsoft\Windows\Start Menu` folder. To publish this shortcut as a default favorite application, add the prefix **`Programs`** to the shortcut path. For example: `"Programs/Windows Update.lnk"`.

---

### Prerequisites

- Verify that the Remote Experience Agent is installed on the virtual machine.
- Verify that you have administrative rights on the virtual machine. For this procedure, you might need to edit a registry setting.
- If you have floating desktop pools, use Active Directory to set up roaming user profiles. Follow the instructions provided by Microsoft.

  Users of floating pool desktops will be able to see their list of favorite applications and favorite files every time they log in.

### Procedure

- (Optional) Create a default list of favorite applications by adding a value to the Windows registry.
  a. Open `regedit` and navigate to the `HKLM\Software\VMware, Inc.\VMware Unity` registry setting.

     On a 64-bit virtual machine, navigate to the `HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity` directory.
  b. Create a string value called `FavAppList`.
  c. Specify the default favorite applications.

     Use the following format to specify the shortcut paths to the applications that are used in the Start menu.

     *path-to-app-1*|*path-to-app-2*|*path-to-app-3*|…

     For example:

     ```
     Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere
     Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010
     Language Preferences.lnk
     ```

- (Optional) Create a default list of favorite applications by creating an administrative installation package from the Remote Experience Agent installer.
  a. From the command line, use the following format to create the administrative installation package.

     ```
     VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /a /v"/qn
     TARGETDIR=""a network share to store the admin install package""
     UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the
     registry"""
     ```

     For example:

     ```
     VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /a /v"/qn
     TARGETDIR=""\\foo-installer-share\ViewFeaturePack\""
     UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|
     Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows
     PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|
     Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft
     Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|
     Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|"""
     ```
  b. Distribute the administrative installation package from the network share to the desktop virtual machines by using a standard Microsoft Windows Installer (MSI) deployment method that is employed in your organization.

- (Optional) Create a default list of favorite applications by running the Remote Experience Agent installer on a command line directly on a virtual machine.

  Use the following format.

  ```
  VMware-Horizon-View-5.3-Remote-Experience-Agent-x64-y.y-xxxxxx.exe /s /v"/qn
  UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry"""
  ```

  **Note** The preceding command combines installing the Remote Experience Agent with specifying the default list of favorite applications. You do not have to install the Remote Experience Agent before you run this command.

### What to do next

If you performed this task directly on a virtual machine (by editing the Windows registry or installing the Remote Experience Agent from the command line), you must deploy the newly configured virtual machine. You can create a snapshot or make a template and create a Horizon View desktop pool, or recompose an existing pool. Or you can create an Active Directory group policy to deploy the new configuration.

## Disable or Enable Unity Touch

When you install the Remote Experience Agent, the Unity Touch installation option is selected by default and the feature is enabled. You can disable or reenable the Unity Touch feature on selected virtual desktops by setting a value on a Windows registry key on those desktops.

You can use the registry to enable Unity Touch only if Unity Touch was installed by the Remote Experience Agent installer and then disabled through the registry. If Unity Touch was never installed, that is, if the option was deselected when you installed the Remote Experience Agent, and you then set the registry value to enable Unity Touch, certain Unity Touch functions will not work correctly.

### Procedure

1 Start the Windows Registry Editor on the virtual desktop.

2 Navigate to the Windows registry key that controls Unity Touch.

| Option | Description |
|---|---|
| **Windows 7 64-bit** | `HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware Unity\enabled = value` |
| **Windows 7 32-bit** | `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware Unity\enabled = value` |

3 Set the value to disable or enable Unity Touch.

| Option | Value |
|---|---|
| **Disabled** | `0` |
| **Enabled** | `1` |

By default, the value is set to `1`.

# Configure Flash URL Redirection for Multicast or Unicast Streaming

Customers can now use Adobe Media Server and multicast or unicast to deliver live video events in a virtual desktop infrastructure (VDI) environment. To deliver multicast or unicast live video streams within a VDI environment, the media stream should be sent directly from the media source to the endpoints, bypassing the virtual desktops. The Flash URL Redirection feature supports this capability by intercepting and redirecting the ShockWave Flash (SWF) file from the virtual desktop to the client endpoint.

The Flash URL redirection feature uses a JavaScript that is embedded inside an HTML Web page by the Web page administrator. Whenever a virtual desktop user clicks on the designated URL link from within a Web page, the JavaScript intercepts and redirects the SWF file from the virtual desktop session to the client endpoint. The endpoint then opens a local Flash Projector outside of the virtual desktop session and plays the media stream locally.

To configure Flash URL Redirection, you must set up your HTML Web page and your client devices.

### Procedure

1 Verify that the Flash URL Redirection Feature Is Installed on page 30

Before you use this feature, verify that the Remote Experience Agent with the Flash URL Redirection option is installed and running on your virtual desktops.

2 Set Up the Web Pages That Provide Multicast or Unicast Streams on page 30

To allow Flash URL redirection to take place, you must embed a JavaScript command in the MIME HTML (MHTML) Web pages that provide links to the multicast or unicast streams. Users display these Web pages in the browsers on their virtual desktops to access the video streams.

3 Set Up Client Devices for Flash URL Redirection on page 31

The Flash URL Redirection feature redirects the SWF file from virtual desktops to client devices. To allow these client devices to play Flash videos from a multicast or unicast stream, you must verify that the appropriate Adobe Flash Player is installed on the client devices. The clients also must have IP connectivity to the media source.

4 Disable or Enable Flash URL Redirection on page 31

When you install the Remote Experience Agent and select the Flash URL Redirection installation option, this feature is enabled. You can disable or reenable the Flash URL Redirection feature on selected virtual desktops by setting a value on a Windows registry key on those desktops.

## Verify that the Flash URL Redirection Feature Is Installed

Before you use this feature, verify that the Remote Experience Agent with the Flash URL Redirection option is installed and running on your virtual desktops.

The Flash URL Redirection feature must be present on every desktop where you intend to support multicast or unicast redirection. For Remote Experience Agent installation instructions, see "Installing and Deploying the Remote Experience Agent on Horizon View Desktops," on page 13.

### Procedure

1 Start a virtual desktop session that uses PCoIP.

2 Open the Task Manager.

3 Verify that the `ViewMPServer.exe` process is running on the desktop.

## Set Up the Web Pages That Provide Multicast or Unicast Streams

To allow Flash URL redirection to take place, you must embed a JavaScript command in the MIME HTML (MHTML) Web pages that provide links to the multicast or unicast streams. Users display these Web pages in the browsers on their virtual desktops to access the video streams.

In addition, you can customize the English error message that is displayed to end users when a problem occurs with Flash URL redirection. Take this optional step if you want to display a localized error message to your end users. You must embed the `var vmwareScriptErroMessage` configuration, together with your localized text string, in the MHTML Web page.

### Prerequisites

Verify that the `swfobject.js` library is imported in the MHTML Web page.

### Procedure

1 Embed the `viewmp.js` JavaScript command in the MHTML Web page.

For example: `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

2 (Optional) Customize the Flash URL redirection error message that is sent to end users.

For example: `"var vmwareScriptErroMessage=`*`localized error message`*`"`

3 Make sure to embed the `viewmp.js` JavaScript command, and optionally customize the Flash URL redirection error message, before the ShockWave Flash (SWF) file is imported into the MHTML Web page.

When a user displays the Web page in a virtual desktop, the `viewmp.js` JavaScript command invokes the Flash URL Redirection mechanism on the virtual desktop, which redirects the SWF file from the desktop to the hosting client device.

## Set Up Client Devices for Flash URL Redirection

The Flash URL Redirection feature redirects the SWF file from virtual desktops to client devices. To allow these client devices to play Flash videos from a multicast or unicast stream, you must verify that the appropriate Adobe Flash Player is installed on the client devices. The clients also must have IP connectivity to the media source.

**Note** With Flash URL Redirection, the multicast or unicast stream is redirected to client devices that might be outside your organization's firewall. Your clients must have access to the Adobe Web server that hosts the SWF file that initiates the multicast or unicast streaming. If needed, configure your firewall to open the appropriate ports to allow client devices to access this server.

### Procedure

- Install Adobe Flash Player on your client devices.

| Operating System | Action |
|---|---|
| **Windows** | Install Adobe Flash Player 10.1 or later for Internet Explorer. |
| **Linux** | a Install the `libexpat.so.0` file, or verify that this file is already installed.<br>Ensure that the file is installed in the `/usr/lib` or `/usr/local/lib` directory.<br>b Install the `libflashplayer.so` file, or verify that this file is already installed.<br>Ensure that the file is installed in the appropriate Flash plug-in directory for your Linux operating system.<br>c Install the `wget` program, or verify that the program file is already installed. |

## Disable or Enable Flash URL Redirection

When you install the Remote Experience Agent and select the Flash URL Redirection installation option, this feature is enabled. You can disable or reenable the Flash URL Redirection feature on selected virtual desktops by setting a value on a Windows registry key on those desktops.

### Procedure

1 Start the Windows Registry Editor on the virtual desktop.

2 Navigate to the Windows registry key that controls Flash URL Redirection.

| Option | Description |
|---|---|
| **Windows 7 64-bit** | `HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = value` |
| **Windows 7 32-bit** | `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = value` |

3 Set the value to disable or enable Flash URL Redirection.

| Option | Value |
|---|---|
| **Disabled** | `0` |
| **Enabled** | `1` |

By default, the value is set to `1`.

# Configure Real-Time Audio-Video

After you install Real-Time Audio-Video, the feature works on your Horizon View desktops without any further configuration. The default values for the webcam frame rate and image resolution are recommended for most standard devices and applications.

You can configure group policy settings to change these default values to adapt to particular applications, webcams, or environments. See "Configuring Real-Time Audio-Video Group Policy Settings," on page 38.

If users have multiple webcams and audio input devices built in or connected to their client computers, you can configure preferred webcams and audio input devices that will be redirected to their desktops. See "Selecting Preferred Webcams and Microphones," on page 33.

**NOTE** You can select a preferred audio device, but no other audio configuration options are available.

When webcam images and audio input are redirected to a remote desktop, you cannot access the webcam and audio devices on the local computer. Conversely, when these devices are in use on the local computer, you cannot access them on the remote desktop.

Real-Time Audio-Video is not supported on local mode desktops.

For information about supported applications, see the VMware knowledge base article, *Guidelines for Using Real-Time Audio-Video with 3rd-Party Applications on Horizon View Desktops*, at http://kb.vmware.com/kb/2053754.

## Ensuring That Real-Time Audio-Video Is Used Instead of USB Redirection

Real-Time Audio-Video supports webcam and audio input redirection for use in conferencing applications. The USB redirection feature that can be installed with View Agent does not support webcam redirection. If you redirect audio input devices through USB redirection, the audio stream does not synchronize properly with video during Real-Time Audio-Video sessions, and you lose the benefit of reducing the demand on network bandwidth. You can take steps to ensure that webcams and audio input devices are redirected to your desktops through Real-Time Audio-Video, not USB redirection.

If your desktops are configured with USB redirection, end users can connect and display their locally connected USB devices by selecting the **Connect USB Device** option in the VMware Horizon View Client menu bar.

If an end user selects a USB device from the **Connect USB Device** list, that device becomes unusable for video or audio conferencing. For example, if a user makes a Skype call, the video image might not appear or the audio stream might be degraded. If an end user selects a device during a conferencing session, the webcam or audio redirection is disrupted.

To hide these devices from end users and prevent potential disruptions, you can configure USB redirection group policy settings to disable the display of webcams and audio input devices in VMware Horizon View Client.

In particular, you can create USB redirection filtering rules for Horizon View Agent and specify the `audio-in` and `video` Device Family Names to be disabled. For information about setting group policies and specifying filtering rules for USB redirection, see "Using Policies to Control USB Redirection" in the *VMware Horizon View Administration* document.

**Caution** If you do not set up USB redirection filtering rules to disable the USB device families, inform your end users that they cannot select webcam or audio devices from the **Connect USB Device** list in the VMware Horizon View Client menu bar.

## Selecting Preferred Webcams and Microphones

If a client computer has more than one webcam and microphone, you can configure a preferred webcam and default microphone that Real-Time Audio-Video will redirect to the desktop. These devices can be built in or connected to the local client computer.

On a Windows client computer, you select a preferred webcam by setting a registry key value. On a Linux client computer, you can specify a preferred webcam or microphone by editing a configuration file. Real-Time Audio-Video redirects the preferred webcam if it is available. If not, Real-Time Audio-Video uses the first webcam that is provided by system enumeration.

To select a default microphone, you can configure the Sound control in the Windows or Linux operating system on the client computer.

### Select a Preferred Webcam on a Windows Client System

With the Real-Time Audio-Video feature, if you have multiple webcams on your client system, only one of them is used on your View desktop. To specify which webcam is preferred, you can set a registry key value.

The preferred webcam is used on the View desktop if it is available, and if not, another webcam is used.

#### Prerequisites

- Verify that you have a USB webcam installed and operational on your client system.
- Verify that you are using the PCoIP display protocol for your View desktop.

#### Procedure

1 Attach the webcam you want to use.

2 Start a call and then stop a call.

This process creates a log file.

3 Open the debug log file with a text editor.

| Operating System | Log File Location |
|---|---|
| **Windows XP** | `C:\Documents and Settings\username\Local Settings\Application Data\VMware\VDM\Logs\debug-20YY-MM-DD-XXXXXX.txt` |
| **Windows 7 or Windows 8** | `C:\Users\%username%\AppData\Local\VMware\VDM\Logs\debug-20YY-MM-DD-XXXXXX.txt` |

The format of the log file is `debug-20YY-MM-DD-XXXXXX.txt` , where 20*YY* is the year, *MM* is the month, *DD* is the day, and *XXXXXX* is a number.

4 Search the log file for `[ViewMMDevRedir] VideoInputBase::LogDevEnum` to find the log file entries that reference the attached webcams.

Here is an excerpt from the log file identifying the Microsoft Lifecam HD-5000 webcam:

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum – 2 Device(s) found

[ViewMMDevRedir] VideoInputBase::LogDevEnum – Index=0 Name=Integrated Webcam
UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000   SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#

[ViewMMDevRedir] VideoInputBase::LogDevEnum – Index=1 Name=Microsoft LifeCam HD–5000
UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000  SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

5 Copy the user ID of the preferred webcam.

For example, copy `vid_045e&pid_076d&mi_00#8&11811f49&0&0000` to set the Microsoft LifeCam HD-5000 as the default webcam.

6 Start the Registry Editor (`regedit.exe`) and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV`.

7 Paste the ID portion of the string into the REG_SZ value, **srcWCamId**.

For example, paste `vid_045e&pid_076d&mi_00#8&11811f49&0&0000` into **srcWCamId**.

8 Save your changes and exit the registry.

9 Start a new call.

## Select a Preferred Webcam or Microphone on a Linux Client System

With the Real-Time Audio-Video feature, if you have multiple webcams and microphones on your client system, only one webcam and one microphone can be used on your View desktop. To specify which webcam and microphone are preferred, you can edit a configuration file.

The preferred webcam or microphone is used on the View desktop if it is available, and if not, another webcam or microphone is used.

With the Real-Time Audio-Video feature, webcams, audio input devices, and audio output devices work without requiring the use of USB redirection, and the amount network bandwidth required is greatly reduced. Analog audio input devices are also supported.

To set the properties in the `/etc/vmware/config` file and specify a preferred device, you must determine the device ID.

- For webcams, you set the `rtav.srcWCamId` property to the value of the webcam description found in the log file, as described in the procedure that follows.
- For audio devices, you set the `rtav.srcAudioInId` property to the value of the Pulse Audio `device.description` field.

  To find the value of this field you can search the log file, as described in the procedure that follows.

### Prerequisites

Depending on whether you are configuring a preferred webcam, preferred microphone, or both, perform the appropriate prerequisite tasks:

- Verify that you have a USB webcam installed and operational on your client system.
- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the PCoIP display protocol for your View desktop.

### Procedure

1 Launch the client, and start a webcam or microphone application to trigger an enumeration of camera devices or audio devices to the client log.

   a Attach the webcam or audio device you want to use.

   b Use the command `vmware-view` to start View Client.

   c Start a call and then stop the call.

      This process creates a log file.

2 Find log entries for the webcam or microphone.

a Open the debug log file with a text editor.

The log file with real-time audio-video log messages is located at `/tmp/vmware-<username>/vmware-mks-<pid>.log`. The client log is located at `/tmp/vmware-<username>/vmware-view-<pid>.log`.

b Search the log file to find the log file entries that reference the attached webcams and microphones.

The following example shows an extract of the webcam selection:

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:
0819)   UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1-3/1-3.4/1-3.4.5   SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=Microsoft® LifeCam HD-6000 for Notebooks   UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6   SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

The following example shows an extract of the audio device selection, and the current audio level for each:

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering
enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of
Microsoft LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
```

Warnings are shown if any of the source audio levels for the selected device do not meet the PulseAudio criteria if the source is not set to 100% (0dB), or if the selected source device is muted, as follows:

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0:  67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

3 Copy the description of the device and use it to set the appropriate property in the `/etc/vmware/config` file.

   For a webcam example, copy `Microsoft® LifeCam HD-6000 for Notebooks` to specify the Microsoft webcam as the preferred webcam and set the property as follows:

   ```
   rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
   ```

   For this example you could also set the property to `rtav.srcWCamId="Microsoft"`.

   For an audio device example, copy `Logitech USB Headset Analog Mono` to specify the Logitech headset as the preferred audio device and set the property as follows:

   ```
   rtav.srcAudioInId="Logitech USB Headset Analog Monoo"
   ```

4 Save your changes and close the `/etc/vmware/config` configuration file.

5 Start a new call.

## Select a Default Microphone on a Windows Client System

If you have multiple microphones on your client system, only one of them is used on your View desktop. To specify which microphone is the default, you can use the Sound control on your client system.

With the Real-Time Audio-Video feature, audio input devices and audio output devices work without requiring the use of USB redirection, and the amount network bandwidth required is greatly reduced. Analog audio input devices are also supported.

---

**Important** If you are using a USB microphone, do not connect it from the **Connect USB Device** menu in Horizon View Client. To do so routes the device through USB redirection so that the device cannot use the Real-Time Audio-Video feature.

---

### Prerequisites

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the PCoIP display protocol for your View desktop.

### Procedure

1 If you are currently on a call, stop the call.

2 Right-click the speaker icon in your system tray and select **Recording devices**.

   You can alternatively open the Sound control from the Control Panel and click the **Recording** tab.

3 In the **Recording** tab of the Sound dialog box, right-click the microphone you prefer to use.

4 Select **Set as Default Device** and click **OK**.

5 Start a new call from your View desktop.

## Select a Default Microphone on a Linux Client System

If you have multiple microphones on your client system, only one of them is used on your View desktop. To specify which microphone is the default, you can use the Sound control on your client system.

With the Real-Time Audio-Video feature, audio input devices and audio output devices work without requiring the use of USB redirection, and the amount network bandwidth required is greatly reduced. Analog audio input devices are also supported.

This procedure describes choosing a default microphone from the user interface of the client system. Administrators can also configure a preferred microphone by editing a configuration file. See "Select a Preferred Webcam or Microphone on a Linux Client System," on page 34.

### Prerequisites

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the PCoIP display protocol for your View desktop.

### Procedure

1 In the Ubuntu graphical user interface, select **System > Preferences > Sound**.

You can alternatively click the **Sound** icon on the right side of the toolbar at the top of the screen.

2 Click the **Input** tab in the Sound Preferences dialog box.

3 Select the preferred device and click **Close**.

## Configuring Real-Time Audio-Video Group Policy Settings

You can configure group policy settings that control the behavior of Real-Time Audio-Video (RTAV) on your Horizon View desktops. These settings determine a virtual webcam's maximum frame rate and image resolution. The settings allow you to manage the maximum bandwidth that any one user can consume. An additional setting disables or enables the RTAV feature.

You do not have to configure these policy settings. Real-Time Audio-Video works with the frame rate and image resolution that are set for the webcam on client systems. The default settings are recommended for most webcam and audio applications.

For examples of bandwidth use during Real-Time Audio-Video, see "Real-Time Audio-Video Bandwidth," on page 40.

These policy settings affect your Horizon View desktops, not the client systems to which the physical devices are connected. To configure these settings on your desktops, add the RTAV Group Policy Administrative Template (ADM) file in Active Directory.

For information about configuring settings on client systems, see the VMware knowledge base article, *Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients*, at http://kb.vmware.com/kb/2053644.

### Add the RTAV ADM Template in Active Directory and Configure the Settings

Horizon View provides an RTAV ADM file, `vdm_agent_rtav.adm`, on the VMware product download page. You can add the policy settings in this ADM file to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

For your convenience, the RTAV ADM file is bundled in a zip file with all the other Horizon View ADM files.

The RTAV ADM file is new in this Feature Pack release. The other ADM files are the same versions as those that are installed with Horizon View 5.3 on View Connection Server in the *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles` directory. You do not have to reinstall the other ADM files if you already added them to Active Directory when you installed or upgraded to Horizon View 5.3.

#### Prerequisites

- Verify that the Remote Experience Agent with the RTAV option is installed on your desktops. The settings have no effect if RTAV is not installed. See "Installing and Deploying the Remote Experience Agent on Horizon View Desktops," on page 13.

- Verify that Active Directory GPOs are created for the RTAV group policy settings. The GPOs must be linked to the OU that contains your 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 RTAV group policy settings. See "Real-Time Audio-Video Group Policy Settings," on page 39.

**Procedure**

1 Download the bundled Horizon View ADM zip file from the VMware product download page.

The zip file is named `VMware-Horizon-View-GPO-Bundle-y.y.y-xxxxxx.zip`, where *y.y.y.* is the version and *xxxxxx* is the build number.

2 Unzip the file and copy the RTAV ADM file, `vdm_agent_rtav.adm`, to your Active Directory server.

3 On the Active Directory server, edit the GPO by selecting **Start > Administrative Tools > Group Policy Management**, right-clicking the GPO, and selecting **Edit**.

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

5 Click **Add**, browse to the `vdm_agent_rtav.adm` file, and click **Open**.

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

The settings are located in the **Computer Configuration > Administrative Templates > Classic Administrative Templates > VMware View Agent Configuration > View RTAV Configuration** folder.

7 Configure the RTAV group policy settings.

## Real-Time Audio-Video Group Policy Settings

The Real-Time Audio-Video (RTAV) group policy settings control the virtual webcam's maximum frame rate and maximum image resolution. An additional setting lets you disable or enable the RTAV feature. These policy settings affect Horizon View desktops, not the client systems where the physical devices are connected.

If you do not configure the RTAV group policy settings, RTAV uses the values that are set on the client systems. On client systems, the default webcam frame rate is 15 frames per second. The default webcam image resolution is 320x240 pixels.

The RTAV group policy settings determine the maximum values that can be used. The frame rate and resolution that are set on client systems are absolute values. For example, if you configure the RTAV settings for maximum image resolution to 640x480 pixels, the webcam displays any resolution that is set on the client up to 640x480 pixels. If you set the image resolution on the client to a value higher than 640x480 pixels, the client resolution is capped at 640x480 pixels.

Not all configurations can achieve the maximum group policy settings of 1920x1080 resolution at 25 frames per second. The maximum frame rate that your configuration can achieve for a given resolution depends upon the webcam being used, the client system hardware, the View Agent virtual hardware, and the available bandwidth.

| Group Policy Setting | Description |
|---|---|
| Disable RTAV | When you enable this setting, the Real-Time Audio-Video feature is disabled.<br>When this setting is not configured or disabled, Real-Time Audio-Video is enabled.<br>This setting is located in the **View RTAV Configuration** folder. |
| Max frames per second | Determines the maximum rate per second at which the webcam can capture frames. You can use this setting to limit the webcam frame rate in low-bandwidth network environments.<br>The minimum value is one frame per second. The maximum value is 25 frames per second.<br>When this setting is not configured or disabled, no maximum frame rate is set. Real-Time Audio-Video uses the frame rate that is selected for the webcam on the client system.<br>By default, client webcams have a frame rate of 15 frames per second. If no setting is configured on the client system and the **Max frames per second** setting is not configured or disabled, the webcam captures 15 frames per second.<br>This setting is located in the **View RTAV Configuration > View RTAV Webcam Settings** folder. |
| Resolution - Max image width in pixels | Determines the maximum width, in pixels, of image frames that are captured by the webcam. By setting a low maximum image width, you can lower the resolution of captured frames, which can improve the imaging experience in low-bandwidth network environments.<br>When this setting is not configured or disabled, a maximum image width is not set. RTAV uses the image width that is set on the client system. The default width of a webcam image on a client system is 320 pixels.<br>The maximum limit for any webcam image is 1920x1080 pixels. If you configure this setting with a value that is higher than 1920 pixels, the effective maximum image width is 1920 pixels.<br>This setting is located in the **View RTAV Configuration > View RTAV Webcam Settings** folder. |
| Resolution - Max image height in pixels | Determines the maximum height, in pixels, of image frames that are captured by the webcam. By setting a low maximum image height, you can lower the resolution of captured frames, which can improve the imaging experience in low-bandwidth network environments.<br>When this setting is not configured or disabled, a maximum image height is not set. RTAV uses the image height that is set on the client system. The default height of a webcam image on a client system is 240 pixels.<br>The maximum limit for any webcam image is 1920x1080 pixels. If you configure this setting with a value that is higher than 1080 pixels, the effective maximum image height is 1080 pixels.<br>This setting is located in the **View RTAV Configuration > View RTAV Webcam Settings** folder. |

## Real-Time Audio-Video Bandwidth

Real-Time Audio-Video bandwidth varies according to the webcam's image resolution and frame rate, and the image and audio data being captured.

The sample tests shown in Table 7 measure the bandwidth that Real-Time Audio-Video uses in a Horizon View environment with standard webcam and audio input devices. The tests measure the bandwidth to send both video and audio data from Horizon View Client to Horizon View Agent. The total bandwidth that is required to run a desktop session from View Client might be higher than these numbers. In these tests, the webcam captures images at 15 frames per second for each image resolution.

**Table 7.** Sample Bandwidth Results for Sending Real-Time Audio-Video Data from Horizon View Client to Horizon View Agent

| Image Resolution (Width x Height) | Bandwidth Used (Kbps) |
|---|---|
| 160 x 120 | 225 |
| 320 x 240 | 320 |
| 640 x 480 | 600 |

# Manage Access to Windows 7 Multimedia Redirection

You can take steps to ensure that Windows 7 Multimedia Redirection (MMR) is accessible only to View Client systems that have appropriate resources and that are connected to Horizon View on a secure network.

MMR data is sent across the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.

You might want to disable MMR if client systems have insufficient resources to handle local multimedia decoding or if you want to restrict access to MMR only to client systems on a secure network. You can configure a policy in View Administrator, **Multimedia redirection (MMR)**, that lets you disable or enable MMR for client systems. You can set the policy globally, for specific desktop pools, or for specific users. The policy is enabled by default. The policy affects MMR for Windows 7, Windows XP, and Windows Vista desktops. For details, see "Configuring Policies" in the *VMware Horizon View Administration* document.

## Ensure That Clients Can Initiate Windows 7 MMR

Windows 7 MMR uses a handshake between the Horizon View Client system and the desktop to validate requests for multimedia redirection. Under certain network conditions, this handshake can take too long to complete, which causes MMR not to be initiated. To ensure that Windows 7 MMR can be initiated, you can configure a Windows registry key on the desktop to increase the time allowed for the validation handshake to complete.

The Windows registry key controls the handshake Time to Live (TTL) value and is set in milliseconds. The key is in REG_DWORD (hex) format. The default value is 5000 milliseconds (five seconds).

Before you deploy Windows 7 MMR to your Horizon View users, test a few client systems to check if the default time allowed to complete the handshake is adequate in your environment. If your network conditions require a longer handshake than five seconds, increase the TTL value.

### Procedure

1 Start the Windows Registry Editor on the virtual desktop.

2 Navigate to the Windows registry key that controls the MMR validation handshake.

| Option | Description |
|---|---|
| **Windows 7 64-bit** | `HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware VDPService\handshakeTTL` |
| **Windows 7 32-bit** | `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware VDPService\handshakeTTL` |

3 Increase the `handshakeTTL` value to a number that is greater than 5000.

4 Restart Windows Media Player on the desktop to allow the updated value to take effect.

# Index

## S



## T



## U



## V



## W