Configuring Remote Desktop Features in Horizon 7

Modified for Horizon 7 7.3.2
VMware Horizon 7 7.3

vmware®

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

https://docs.vmware.com/

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

Configuring Remote Desktop Features in Horizon 7

1

Configuring Remote Desktop Features in Horizon 7 describes how to configure remote desktop features that are installed with Horizon Agent on virtual machine desktops or on an RDS host. You can also configure policies to control the behavior of desktop and application pools, machines, and users.

Intended Audience

This information is intended for anyone who wants to configure remote desktop features or policies on virtual machine desktops or RDS hosts. The information is written for Windows system administrators who are familiar with virtual machine technology and data center operations.

Configuring Remote Desktop Features

2

Certain remote desktop features that are installed with Horizon Agent can be updated in Feature Pack Update releases as well as in core Horizon 7 releases. You can configure these features to enhance the remote desktop experience for your end users.

These features include HTML Access, Unity Touch, Flash URL Redirection, HTML5 Multimedia Redirection, Real-Time Audio-Video, Windows Media Multimedia Redirection (MMR), USB Redirection, Scanner Redirection, Serial Port Redirection, and URL Content Redirection.

For information about HTML Access, see the *VMware Horizon HTML Access Installation and Setup Guide* document. For information about USB Redirection, see Chapter 4 Using USB Devices with Remote Desktops and Applications. For information about URL Content Redirection, see Chapter 3 Configuring URL Content Redirection.

This section includes the following topics:

Configuring 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. You can configure a default list of favorite applications that appear in the Unity Touch sidebar.

You can disable or enable the Unity Touch feature after Horizon Agent is installed by configuring the **Enable Unity Touch** group policy setting in the Horizon Agent Configuration ADMX template file (`vdm_agent.admx`).

The VMware Horizon Client documents for iOS, Android, and Chrome OS devices provide more information about the end user features provided by Unity Touch.

System Requirements for Unity Touch

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

Horizon 7 desktop

To support Unity Touch, the following software must be installed in the virtual machine that the end user will access:

- You install the Unity Touch feature by installing View Agent 6.0 or later. See "Install View Agent on a Virtual Machine" in the *Setting Up Virtual Desktops in Horizon 7* document.
- Operating systems: Windows 7 (32-bit or 64-bit), Windows 8 (32-bit or 64-bit), Windows 8.1 (32-bit or 64-bit), Windows Server 2008 R2, or Windows Server 2012 R2, Windows 10 (32-bit or 64-bit)

Horizon Client software

Unity Touch is supported on the following Horizon Client versions:

- Horizon Client for iOS
- Horizon Client for Android
- Horizon Client for Chrome OS

Configure Favorite Applications Displayed by Unity Touch

With the Unity Touch feature, tablet and smart phone users can quickly navigate to a Horizon 7 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-assignment 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 machines in a floating or dedicated pool.

If you create a default list of favorite applications and one or more of the applications are not installed in the Horizon 7 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 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 virtual machines in the desktop pool
- Create an administrative installation package from the Horizon Agent installer and distribute the package to the virtual machines
- Run the Horizon 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 Horizon 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-assignment desktop pools, use Active Directory to set up roaming user profiles. Follow the instructions provided by Microsoft.

  Users of floating-assignment desktop pools 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 Horizon Agent installer.
  a. From the command line, use the following format to create the administrative installation package.

     ```
     VMware-viewagent-x86_64-y.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-viewagent-x86_x64-y.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 Horizon Agent installer on a command line directly on a virtual machine.

  Use the following format.

  ```
  VMware-viewagent-x86_x64-y.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 Horizon Agent with specifying the default list of favorite applications. You do not have to install Horizon 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 Horizon 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 desktop pool, or recompose an existing pool. Or you can create an Active Directory group policy to deploy the new configuration.

Configuring 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 remote desktops. The Flash URL Redirection feature supports this capability by intercepting and redirecting the ShockWave Flash (SWF) file from the remote desktop to the client endpoint.

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.

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

  To support Flash URL Redirection, your Horizon 7 deployment must meet certain software and hardware requirements.

2 Verify that the Flash URL Redirection Feature Is Installed

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

3 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 remote desktops to access the video streams.

4 Set Up Client Devices for Flash URL Redirection

The Flash URL Redirection feature redirects the SWF file from remote 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.

5 Disable or Enable Flash URL Redirection

Flash URL Redirection is enabled when you perform a silent installation of Horizon Agent with the `VDM_FLASH_URL_REDIRECTION=1` property. You can disable or reenable the Flash URL Redirection feature on selected remote desktops by setting a value on a Windows registry key on those virtual machines.

System Requirements for Flash URL Redirection

To support Flash URL Redirection, your Horizon 7 deployment must meet certain software and hardware requirements.

Horizon 7 desktop

- You install Flash URL Redirection by typing the `VDM_FLASH_URL_REDIRECTION` property on the command line during a silent installation of View Agent 6.0 or later. See "Silent Installation Properties for Horizon Agent" in the *Setting Up Virtual Desktops in Horizon 7* document.
- The desktops must run Windows 7 64-bit or 32-bit operating systems.
- Supported desktop browsers include Internet Explorer 8, 9, and 10, Chrome 29.*x*, and Firefox 20.*x*.

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 Client software

The following Horizon Client releases support multicast and unicast:

- Horizon Client 2.2 for Linux or a later release

- Horizon Client 2.2 for Windows or a later release

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

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

Horizon Client computer or client access device

- Flash URL Redirection is supported on all operating systems that run Horizon 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 Client for Windows. For details, see the *Using VMware Horizon 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.

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.

Verify that the Flash URL Redirection Feature Is Installed

Before you use this feature, verify that the Flash URL Redirection feature 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 Horizon Agent installation instructions, see "Silent Installation Properties for Horizon Agent" in the *Setting Up Virtual Desktops in Horizon 7* document.

Procedure

1. Start a remote 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 remote 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 remote desktop, the `viewmp.js` JavaScript command invokes the Flash URL Redirection mechanism on the remote 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 remote 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. Ensure that the file is installed in the `/usr/lib` or `/usr/local/lib` directory. b Install the `libflashplayer.so` file, or verify that this file is already installed. Ensure that the file is installed in the appropriate Flash plug-in directory for your Linux operating system. c Install the `wget` program, or verify that the program file is already installed.

Disable or Enable Flash URL Redirection

Flash URL Redirection is enabled when you perform a silent installation of Horizon Agent with the `VDM_FLASH_URL_REDIRECTION=1` property. You can disable or reenable the Flash URL Redirection feature on selected remote desktops by setting a value on a Windows registry key on those virtual machines.

Procedure

1. Start the Windows Registry Editor on the virtual machine.
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`.

Configuring Flash Redirection

With Flash Redirection, if an end user uses Internet Explorer 9, 10, or 11, Flash content is sent to the client system, which reduces the load on the ESXi host. The client system plays the media content in a Flash container window by using the Flash Player ActiveX version.

Although the name of this feature is similar to the feature called Flash URL Redirection, there are important differences, as described in the following table.

Table 2-1. Comparison of the Flash Redirection Feature and Flash URL Redirection

Item of Differentiation	Flash Redirection	Flash URL Redirection
Horizon Client types that support this feature	Windows client only	Windows client and Linux client
Display protocol	PCoIP and VMware Blast.	PCoIP
Browsers	Internet Explorer 9, 10, or 11 for the remote desktop	All browsers that are currently supported on Horizon Client and Horizon Agent
Configuration mechanism	Use a Horizon Agent group policy setting to specify a white list or black list of websites that use or do not use Flash Redirection	To embed the required JavaScript, modify the source code on the web page.

Feature Limitations

The Flash Redirection feature has the following limitations:

- Clicking a URL link inside the Flash Player window opens a browser on the client rather than in the remote desktop (agent side).
- Some websites do not work with Flash Redirection on some browser versions. For example, vimeo.com does not work if you use Internet Explorer 11.
- Flash and Java scripting might not work as expected.
- The Horizon Client window might freeze while playing Flash content, although you can set a Windows Registry key to work around this issue.

  On a 32-bit client, set `HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` value to "FALSE" and on a 64-bit client, set `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` to "FALSE".
- YouTube no longer supports Flash media.
- Flash Redirection does not work for redbox.com.
- The Flash context menu (activated by a right click) is disabled.
- If Horizon Client 4.1 connects to a remote desktop with PCoIP, Flash Redirection fails. Horizon Client either plays the Flash content in the remote desktop's native player, or the user sees a white screen.

System Requirements for Flash Redirection

Horizon Agent and Horizon Client, and the remote desktops and client systems on which you install the agent and client software, must meet certain requirements to support the Flash Redirection feature.

Remote desktop

- Horizon Agent 7.0 or later must be installed in a virtual desktop with the Flash Redirection custom setup option selected. The Flash Redirection custom setup option is not selected by default. See the topics about installing Horizon Agent in the *Setting Up Virtual Desktops in Horizon 7* document.

	■ The appropriate group policy settings must be configured. See Install and Configure Flash Redirection. ■ Flash Redirection is supported on Windows 7, Windows 8, Windows 8.1, and Windows 10 virtual desktops. ■ Internet Explorer 9, 10, or 11 must be installed with the corresponding Flash ActiveX plug-in. ■ After installation, the VMware View FlashMMR Server add-on must be enabled in Internet Explorer.
Horizon Client computer or client access device	■ Horizon Client 4.0 or later must be installed. The Flash Redirection option is enabled by default. See the topic about installing Horizon Client in the *VMware Horizon Client for Windows Installation and Setup Guide* document. ■ Flash Redirection is supported on Windows 7, Windows 8, Windows 8.1, and Windows 10. ■ The Flash ActiveX plug-in must be installed and enabled
Display protocols for the remote session	■ PCoIP ■ VMware Blast (requires Horizon Agent 7.0 or later)

Install and Configure Flash Redirection

Redirecting Flash content from a remote desktop to a Flash Player window on the local client system requires installing the Flash Redirection feature and Internet Explorer on the remote desktop and the client system and specifying which websites use this feature.

To enable this feature and specify which websites use this feature, you configure group policy settings. Alternatively, you can use Windows Registry settings on the remote desktop to configure a white list of websites to use for Flash Redirection. See Use Windows Registry Settings to Configure Flash Redirection.

Prerequisites

- Install Horizon Client on the client system and install Horizon Agent on the remote desktop with the Flash Redirection feature enabled. For required versions, setup options, and complete system requirements, see System Requirements for Flash Redirection.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Add the Horizon Agent Configuration ADMX template file `vdm_agent.admx` file to the OU for the remote desktop. For installation instructions, see Add the ADMX Template Files to Active Directory.

- Compile a list of the websites that can (a white list) or cannot (a black list) redirect Flash content.
- Verify that Flash ActiveX is installed and works properly. To verify the installation, run Internet Explorer and go to https://helpx.adobe.com/flash-player.html.

Procedure

1. On the client system, install the ActiveX version of Flash Player (rather than the NPAPI version), if necessary.

   Flash Player is installed by default in Internet Explorer 10 and 11. For Internet Explorer 9, you might need to go to https://get.adobe.com/flashplayer/ to download and install Flash Player.

2. On the remote desktop, perform the following installation steps.

   a. Install Internet Explorer 9, 10, or 11.

   b. Install the ActiveX version of Flash Player (rather than the NPAPI version), if necessary.

      Flash Player is installed by default in Internet Explorer 10 and 11. For Internet Explorer 9, you might need to go to https://get.adobe.com/flashplayer/ to download and install Flash Player.

3. On the remote desktop, in Internet Explorer, select **Tools > Manage add-ons** from the menu bar and verify that **VMware View FlashMMR Server** is listed and enabled.

4. On the Active Directory server, open the Group Policy Management Editor and configure the Flash Redirection policy settings in the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware FlashMMR** folder.

Setting	Description
Enable Flash multi-media redirection	Specifies whether Flash Redirection (FlashMMR) is enabled on the remote desktop (agent-side). When enabled, this feature forwards Flash multi-media data from the designated URLs through a TCP channel to the client, and invokes the local Flash Player on the client system. This feature greatly reduces demand on the agent-side CPU and network bandwidth.
Minimum rect size to enable FlashMMR	Specifies the minimum width and height, in pixels, of the rectangle in which the Flash content is played. For example, **`400,300`** specifies a width of 400 pixels and a height of 300 pixels. Flash Redirection is used only if the Flash content is equal to or greater than the values specified in this policy. If this GPO is not configured, the default value used is **`320,200`**.

5. On the Active Directory server, open the Group Policy Management Editor and configure the Flash Redirection policy settings in the **User Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware FlashMMR** folder.

   a. To define a list of host URLs to use with Flash redirection, open the **Definiton for FlashMMR url list usage** setting and select **Enabled**.

   b. In the **Definition for FlashMMR url list usage** drop-down menu, select **Enable white list** or **Enable black list**, and click **OK**.

      By default, a white list is enabled.

c To add the list of host URLs that use or do not use Flash Redirection, open the **Hosts Url list to enable FlashMMR** setting and select **Enabled**.

d Click **Show** and enter the complete URLs that you compiled for the white list or black list in the Value Name column.

Include the `http://` or `https://` prefix in the URL. You can use regular expressions. For example, you can specify `https://*.google.com` and `http://www.cnn.com/*`.

In the Value column, you can optionally specify `requireIECompatibility=true`, `appMode=0`, or both. Use a comma to separate the two strings.

By default, external interface support is enabled when Flash Redirection runs and can degrade performance. In certain situations, setting `appMode=0` can improve performance and result in a better user experience.

e Click **OK** to save the URL list, and click **OK** again to save the policy setting.

6 On the remote desktop, open a command prompt and navigate to the `%Program Files%\Common Files\VMware\Remote Experience` directory.

7 To add the white list or black list to Internet Explorer, run the `cscript mergeflashmmrwhitelist.vbs` command.

8 Restart Internet Explorer.

The sites set with the `requireIECompatibility=true` parameter are added to Internet Explorer's compatibility view. To verify the sites in compatibility view, select **Tools > Compatibility View Settings** from the menu bar.

The sites are also added to Internet Explorer's list of trusted sites. To verify the trusted sites, select **Tools > Internet Options** from the Internet Explorer menu bar and click **Sites** and on the **Security** tab.

Use Windows Registry Settings to Configure Flash Redirection

If you are a domain user who does not have Administrator privileges on the Active Directory server, you can alternatively configure Flash Redirection by setting the appropriate values in Windows Registry keys on the remote desktop.

You can use this procedure as an alternative to using group policy settings to configure Flash Redirection.

Prerequisites

- To ensure that only the URLs specified in the list can redirect Flash content, compile a white list of websites. You cannot use the Windows registry settings to enable a black list. To enable a black list, use the group policy settings for Flash Redirection.
- Verify that Horizon Agent 7.0 or later, Flash Player, and Internet Explorer 9, 10, or 11 are installed in the remote desktop. See System Requirements for Flash Redirection.
- Verify that Horizon Client 4.0 or later and Flash Player ActiveX version are installed in the client system.

Procedure

1. Use Horizon Client to access the remote desktop.
2. Open the Windows Registry Editor (`regedit.exe`) on the remote desktop, navigate to the `HKLM\Software\VMware, Inc.\VMware FlashMMR` folder, and set **FlashRedirection** to `1`.

   Note This setting enables the Flash Redirection feature. If this setting is disabled (set to 0) in `HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR`, Flash Redirection is disabled domain-wide and requires a domain administrator to enable it.

3. Navigate to the `HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR` folder.

   If this folder does not exist, create it.
4. In the `VMware FlashMMR` folder, create a subkey named **UrlWhiteList**.
5. Right-click the **UrlWhiteList** key, select **New > String Value**, and enter the URL of a website that uses Flash Redirection for the name.

   You can use regular expressions. For example, you can specify **`https://*.google.com`**. Leave the **Data** value empty.
6. (Optional) In the data field of the new registry value, add the data **`requireIECompatibility=true`**, **`appMode=0`**, or both.

   Use a comma to separate the two strings. By default, external interface support is enabled when Flash Redirection runs and can degrade performance. In certain situations, setting **`appMode=0`** can improve performance, and setting **`appMode=1`** can result in a better user experience.
7. To add additional URLs, repeat the previous step and then close the Registry Editor.
8. On the remote desktop, open a command prompt and navigate to the `%Program Files%\Common Files\VMware\Remote Experience` directory.
9. To add the white list to Internet Explorer, run the `cscript mergeflashmmrwhitelist.vbs` command.
10. Restart Internet Explorer.

    The sites set that have the parameter **`requireIECompatibility=true`** are added to Internet Explorer's compatibility view. To verify the sites in compatibility view, select **Tools > Compatibility View Settings** from the menu bar.

    The sites are also added to Internet Explorer's list of trusted sites. To verify the trusted sites, select **Tools > Internet Options** from the Internet Explorer menu bar and click **Sites** on the **Security** tab.

Configuring HTML5 Multimedia Redirection

With HTML5 Multimedia Redirection, if an end user uses the Chrome browser, HTML5 multimedia content is sent to the client system, which reduces the load on the ESXi host. The client system plays the multimedia content and the user has a better audio and video experience.

System Requirements for HTML5 Multimedia Redirection

Horizon Agent and Horizon Client, and the remote desktops and client systems on which you install the agent and client software, must meet certain requirements to support the HTML5 Multimedia Redirection feature.

Remote desktop	■ Virtual desktops must have Horizon Agent 7.3 or later installed with the HTML5 Multimedia Redirection custom setup option selected. This option is not selected by default. See the topics about installing Horizon Agent in the *Setting Up Virtual Desktops in Horizon 7* document. ■ RDS hosts for published desktops must have Horizon Agent 7.3 or later installed with the HTML5 Multimedia Redirection custom setup option selected. This option is not selected by default. See the topics about installing Horizon Agent in the *Setting Up Published Desktops and Applications in Horizon 7* document. ■ The HTML5 Multimedia Redirection group policy settings must be configured on the Active Directory server. See Install and Configure HTML5 Multimedia Redirection. ■ The Chrome browser must be installed. ■ The VMware Horizon HTML5 Multimedia Redirection extension must be installed in the Chrome browser. See Force Install the VMware Horizon HTML5 Redirection Extension.
Client system	■ Horizon Client 4.6 or later must be installed with the HTML5 Multimedia Redirection Support custom setup option selected. This option is selected by default. See the topics about installing Horizon Client in the *VMware Horizon Client for Windows Installation and Setup Guide* document. Non-Windows client systems are not supported.
Display protocol for the remote session	■ PCoIP ■ VMware Blast

Install and Configure HTML5 Multimedia Redirection

Redirecting HTML5 multimedia content from a remote desktop to the local client system requires installing the HTML5 Multimedia Redirection feature and Chrome browser on the remote desktop, enabling the HTML5 Multimedia Redirection feature, and specifying which websites use this feature.

To enable HTML5 Multimedia Redirection and specify which websites use this feature, you configure group policy settings on your Active Directory server. You must compile a list of URLs for the websites that can redirect HTML5 multimedia content. Include the `http://` or `https://` prefix in the URLs. You can use match patterns in the URLs. For example, to redirect all videos on YouTube, specify `https://www.youtube.com/*`. To redirect all videos on Vimeo, specify `https://www.vimeo.com/*`. For more information, see https://developer.chrome.com/extensions/match_patterns.

Prerequisites

- Install Horizon Client on the client system and install Horizon Agent on the remote desktop with the HTML5 Multimedia Redirection feature enabled. For required versions, setup options, and complete system requirements, see System Requirements for HTML5 Multimedia Redirection.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Add the Horizon Agent Configuration ADMX template file `vdm_agent.admx` to a GPO that is linked to the OU for the virtual desktop or to the RDS host for the published desktop. For installation instructions, see Add the ADMX Template Files to Active Directory.
- Compile a list of URLs for websites that can redirect HTML5 multimedia content.

Procedure

1. Install the Chrome browser on the remote desktop.
2. On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Multimedia Redirection** folder.
3. Open the **Enable VMware HTML5 Multimedia Redirection** setting, select **Enabled**, and click **OK**.
4. Open the **Enable URL list for VMware HTML5 Multimedia Redirection** setting and select **Enabled**.
5. Click **Show** and enter the URLs that you compiled in the Value name column.

   Only the URLs that you specify can redirect HTML5 multimedia content. No URLs are added by default. Leave the Value column blank.
6. Click **OK** to save the URL list and then click **OK** to save the policy setting.

What to do next

Force install the VMware Horizon HTML5 Redirection Extension in the Chrome browser on the remote desktop. See Force Install the VMware Horizon HTML5 Redirection Extension.

Force Install the VMware Horizon HTML5 Redirection Extension

To use the HTML5 Multimedia Redirection feature, you must force install the VMware Horizon HTML5 Redirection extension on the remote desktop. You force install the extension by configuring a Google Chrome group policy setting on your Active Directory server.

To apply the Chrome group policy setting to the remote desktop, you must add the ADMX template file to a GPO on your Active Directory server. For a virtual desktop, the GPO must be linked to the OU that contains the virtual desktop. For a published desktop, the GPO must be linked to the OU that contains the RDS host.

Prerequisites

- Configure the HTML5 Multimedia Redirection feature. See Install and Configure HTML5 Multimedia Redirection.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.

Procedure

1. Download the Google Chrome `policy_templates.zip` file from https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip.
2. Unzip the `policy_templates.zip` file and copy the `chrome.admx` and `chrome.adml` files to your Active Directory Server.

   The `chrome.admx` file is in the `\windows\admx` folder and the `chrome.adml` file is in the `\windows\admx\`*`language`* folder in the `policy_templates.zip` file.

   a. Copy the `chrome.admx` file to the `%systemroot%\PolicyDefinitions` folder on your Active Directory server.

   b. Copy the `chrome.adml` language resource file to the appropriate language subfolder in `%systemroot%\PolicyDefinitions` on your Active Directory server.

      For example, copy the `en_us` version of the `chrome.adml` file to the `%systemroot%\PolicyDefinitions\en_us` subfolder on your Active Directory server.
3. On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > Google Chrome > Extensions** folder.
4. Open the **Configure the list of force-installed apps and extensions** policy setting and click **Enabled**.

5 Click **Show** and type **`ljmaegmnepbgjekghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx`** in the Value column.

6 Click **OK** to save the extension ID/update URL and then click **OK** to save the policy setting.

7 Verify that the HTML5 Multimedia Redirection extension is installed on the remote desktop.

   a Connect to the remote desktop and start Chrome.

   b Type **`chrome://extensions`** in the Chrome address bar.

   VMware Horizon HTML5 Redirection Extension appears in the Extensions list.

Configuring Real-Time Audio-Video

Real-Time Audio-Video allows Horizon 7 users to run Skype, Webex, Google Hangouts, and other online conferencing applications on their remote 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 browser-based video 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. The VMware Virtual Webcam uses a kernel-mode webcam driver that provides enhanced compatibility with browser-based video applications and other 3rd-party conferencing software.

When a conferencing or video 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 Webcam and Microphone appear in the Device Manager on the desktop operating system.

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

Configuration Choices for Real-Time Audio-Video

After you install Horizon Agent with Real-Time Audio-Video, the feature works on your Horizon 7 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. You can also set a policy to disable or enable the feature altogether. An ADMX template file aloows you to install Real-Time Audio-Video group policy settings on Active Directory or on individual desktops. See Configuring Real-Time Audio-Video Group Policy Settings.

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.

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.

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.

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 deployment must meet certain software and hardware requirements.

Remote desktops	You install the Real-Time Audio-Video feature by installing View Agent 6.0 or later, or Horizon Agent 7.0 or later. To use this feature with published desktops and applications, you must install Horizon Agent 7.0.2 or later. See your Setting Up document for information on installing Horizon Agent.
Horizon Client software	Horizon Client 2.2 for Windows or a later release Horizon Client 2.2 for Linux or a later release. For Horizon Client for Linux 3.1 or earlier, this feature is available only with the version of Horizon Client for Linux provided by third-party vendors. For Horizon Client for Linux 3.2 and later, this feature is also available with the version of the client available from VMware. Horizon Client 2.3 for Mac or a later release Horizon Client 4.0 for iOS or a later release. Horizon Client 4.0 for Android or a later release.
Horizon Client computer or client access device	■ All operating systems that run Horizon Client for Windows. ■ All operating systems that run Horizon Client for Linux on x86 devices. This feature is not supported on ARM processors. ■ Mac OS X Mountain Lion (10.8) and later. It is disabled on all earlier Mac OS X operating systems. ■ All operating systems that run Horizon Client for iOS. ■ All operating systems than run Horizon Client for Android.

	■ For information about supported client operating systems, see the Horizon Client installation and setup document for the appropriate system or device. ■ 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 need to install the device drivers on the remote desktop operating system where the agent is installed.
Display protocols	■ PCoIP ■ VMware Blast (requires Horizon Agent 7.0 or later)

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 Horizon 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 Windows client menu bar or the **Desktop > USB** menu in the Mac client. Linux clients block USB redirection of audio and video devices by default and do not provide the USB device options to end users.

If an end user selects a USB device from the **Connect USB Device** or **Desktop > USB** 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 Client.

In particular, you can create USB redirection filtering rules for Horizon 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.

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** or **Desktop > USB** list in the VMware Horizon 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 that has Horizon Client for Windows 4.2 or later installed, you can select a preferred webcam or microphone by configuring Real-Time Audio-Video settings in the Horizon Client Settings dialog box. With earlier Horizon Client versions, you modify registry settings to select a preferred webcam and use the Sound control in the Windows operating system to select a default microphone.

On a Mac client computer, you can specify a preferred webcam or microphone by using the Mac defaults system.

On a Linux client computer, you can specify a preferred webcam by editing a configuration file. To select a default microphone, you can configure the Sound control in the Linux operating system on the client computer.

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.

Select a Preferred Webcam or Microphone on a Windows Client System

With the Real-Time Audio-Video feature, if multiple webcams or microphones are connected to the local client system, only one of the devices is used on the remote desktop or application. To specify which webcam or microphone is preferred, you can configure Real-Time Audio-Video settings in Horizon Client.

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

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

Note If you are using a USB webcam or microphone, do not connect it from the **Connect USB Device** menu in Horizon 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 webcam, or USB microphone or other type of microphone, installed and operational on the local client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for the remote desktop or application.
- Connect to a server.

Procedure

1. Open the **Settings** dialog box and select **Real-Time Audio-Video** in the left pane.

   You can open the **Settings** dialog box by clicking the **Settings** (gear) icon in the upper right corner of the desktop and application screen, or by right-clicking a desktop or application icon and selecting **Settings**.

2. Select the preferred webcam from the **Preferred webcam** drop-down menu and the preferred microphone from the **Preferred microphone** drop-down menu.

   The drop-down menus show the available webcams and microphones on the client system.

3. Click **OK** or **Apply** to save your changes.

The next time you start a remote desktop or application, the preferred webcam and microphone that you selected are redirected to the remote desktop or application.

Select a Default Microphone on a Mac Client System

If you have multiple microphones on the client system, only one microphone is used on the remote desktop. You can use System Preferences on the client system to specify which microphone is the default microphone on the remote desktop.

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 of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

This procedure describes how to choose a microphone from the user interface of the client system. Administrators can also configure a preferred microphone by using the Mac defaults system. See Configure a Preferred Webcam or Microphone on a Mac Client System.

Important If you are using a USB microphone, do not connect it from the **Connection > USB** menu in Horizon Client. To do so routes the device through USB redirection and 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 the client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for the remote desktop.

Procedure

1. On the client system, select **Apple menu > System Preferences** and click **Sound**.
2. Open the Input pane of Sound preferences.
3. Select the microphone that you prefer to use.

The next time that you connect to a remote desktop and start a call, the desktop uses the default microphone that you selected on the client system.

Configuring Real-Time Audio-Video on a Mac Client

You can configure Real-Time Audio-Video settings at the command line by using the Mac defaults system. With the defaults system, you can read, write, and delete Mac user defaults by using Terminal (`/Applications/Utilities/Terminal.app`).

Mac defaults belong to domains. Domains typically correspond to individual applications. The domain for the Real-Time Audio-Video feature is com.vmware.rtav.

Syntax for Configuring Real-Time Audio-Video

You can use the following commands to configure the Real-Time Audio-Video feature.

Table 2-2. Command Syntax for Real-Time Audio-Video Configuration

Command	Description
`defaults write com.vmware.rtav scrWCamId "`*webcam-userid*`"`	Sets the preferred webcam to use on remote desktops. When this value is not set, the webcam is selected automatically by system enumeration. You can specify any webcam connected to (or built into) the client system.
`defaults write com.vmware.rtav srcAudioInId "`*audio-device-userid*`"`	Sets the preferred microphone (audio-in device) to use on remote desktops. When this value is not set, remote desktops use the default recording device set on the client system. You can specify any microphone connected to (or built into) the client system.
`defaults write com.vmware.rtav srcWCamFrameWidth` *pixels*	Sets the image width. The value defaults to a hardcoded value of 320 pixels. You can change the image width to any pixel value.
`defaults write com.vmware.rtav srcWCamFrameHeight` *pixels*	Sets the image height. The value defaults to a hardcoded value of 240 pixels. You can change the image height to any pixel value.
`defaults write com.vmware.rtav srcWCamFrameRate` *fps*	Sets the frame rate. The value defaults to 15 fps. You can change the frame rate to any value.
`defaults write com.vmware.rtav LogLevel "`*level*`"`	Sets the logging level for the Real-Time Audio-Video log file (`~/Library/Logs/VMware/vmware-RTAV-`*pid*`.log`). You can set the logging level to trace or debug.
`defaults write com.vmware.rtav IsDisabled` *value*	Determines whether Real-Time Audio-Video is enabled or disabled. Real-Time Audio-Video is enabled by default. (This value is not in effect.) To disable Real-Time Audio-Video on the client, set the value to true.
`defaults read com.vmware.rtav`	Displays Real-Time Audio-Video configuration settings.
`defaults delete com.vmware.rtav` *setting*	Deletes a Real-Time Audio-Video configuration setting, for example: `defaults delete com.vmware.rtav srcWCamFrameWidth`

Note You can adjust frame rates from 1 fps up to a maximum of 25 fps and resolution up to a maximum of 1920x1080. A high resolution at a fast frame rate might not be supported on all devices or in all environments.

Configure a Preferred Webcam or Microphone on a Mac Client System

With the Real-Time Audio-Video feature, if you have multiple webcams or microphones on the client system, only one webcam and one microphone can be used on the remote desktop. You specify which webcam and microphone are preferred at the command line by using the Mac defaults system.

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

In most environments, there is no need to configure a preferred microphone or webcam. If you do not set a preferred microphone, remote desktops use the default audio device set in the client system's System Preferences. See Select a Default Microphone on a Mac Client System. If you do not configure a preferred webcam, the remote desktop selects the webcam by enumeration.

Prerequisites

- If you are configuring a preferred USB webcam, verify that the webcam is installed and operational on the client system.
- If you are configuring a preferred USB microphone or other type of microphone, verify that the microphone is installed and operational on the client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for the remote desktop.

Procedure

1. On the Mac client system, start a webcam or microphone application to trigger an enumeration of camera devices or audio devices to the Real-Time Audio-Video log file.
   a. Attach the webcam or audio device.
   b. In the **Applications** folder, double-click **VMware Horizon Client** to start Horizon Client.
   c. Start a call and then stop the call.

2 Find log entries for the webcam or microphone in the Real-Time Audio-Video log file.

   a In a text editor, open the Real-Time Audio-Video log file.

      The Real-Time Audio-Video log file is named `~/Library/Logs/VMware/vmware-RTAV-pid.log`, where *pid* is the process ID of the current session.

   b Search the Real-Time Audio-Video log file for entries that identify the attached webcams or microphones.

   The following example shows how webcam entries might appear in the Real-Time Audio-Video log file:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() - 1
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-in)#0xfa20000005ac8509
SystemId=0xfa20000005ac8509
```

   The following example shows how microphone entries might appear in the Real-Time Audio-Video log file:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - 2
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Microphone   UserId=Built-in Microphone#AppleHDAEngineInput:1B,0,1,0:1
SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255   Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

3 Find the webcam or microphone that you prefer in the Real-Time Audio-Video log file and make a note of its user ID.

   The user ID appears after the string UserId= in the log file. For example, the user ID of the internal face time camera is FaceTime HD Camera (Built-in) and the user ID of the internal microphone is Built-in Microphone.

4 In Terminal (`/Applications/Utilities/Terminal.app`), use the `defaults write` command to set the preferred webcam or microphone.

Option	Action
Set the preferred webcam	Type **`defaults write com.vmware.rtav srcWCamId "`*`webcam-userid`*`"`**, where *webcam-userid* is the user ID of the preferred webcam, which you obtained from the Real-Time Audio-Video log file. For example: `defaults write com.vmware.rtav srcWCamId "HD Webcam C525"`
Set the preferred microphone	Type **`defaults write com.vmware.rtav srcAudioInId "`*`audio-device-userid`*`"`**, where *audio-device-userid* is the user ID of the preferred microphone, which you obtained from the Real-Time Audio-Video log file. For example: `defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"`

5 (Optional) Use the `defaults read` command to verify your changes to the Real-Time Audio-Video feature.

For example: **`defaults read com.vmware.rtav`**

The command lists all of the Real-Time Audio-Video settings.

The next time you connect to a remote desktop and start a new call, the desktop uses the preferred webcam or microphone that you configured, if it is available. If the preferred webcam or microphone is not available, the remote desktop can use another available webcam or microphone.

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 Horizon 7 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 of 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.

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 VMware Blast display protocol or the PCoIP display protocol for your remote 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**.

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 Horizon 7 desktop. To specify which webcam and microphone are preferred, you can edit a configuration file.

The preferred webcam or microphone is used on the remote 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 values of certain fields. You can search the log file for the values of these fields.

- For webcams, you set the `rtav.srcWCamId` property to the value of the `UserId` field for the webcam and the `rtav.srcWCamName` property to the value of the `Name` field for the webcam.

  The `rtav.srcWCamName` property has a higher priority than the `rtav.srcWCamId` property. Both properties should specify the same webcam. If the properties specify different webcams, the webcam specified by `rtav.srcWCamName` is used, if it exists. If it does not exist, the webcam specified by `rtav.srcWCamId` is used. If both webcams are not found, the default webcam is used.
- For audio devices, you set the `rtav.srcAudioInId` property to the value of the Pulse Audio `device.description` field.

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 VMware Blast display protocol or the PCoIP display protocol for your remote 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 Horizon 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-RTAV-<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` and `Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6` to specify the Microsoft webcam as the preferred webcam and set the properties as follows:

```
rtav.srcWCamName = “Microsoft® LifeCam HD-6000 for Notebooks”
rtav.srcWCamId = “Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1-3/1-3.6”
```

For this example, you could also set the `rtav.srcWCamId` property to `"Microsoft"`. The `rtav.srcWCamId` property supports both partial and exact matches. The `rtav.srcWCamName` property supports only an exact match.

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 Mono"
```

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

5 Log off of the desktop session and start a new session.

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 7 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.

These policy settings affect your Horizon 7 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 (ADMX) 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 ADMX Template in Active Directory and Configure the Settings

You can add the policy settings in the RTAV ADMX file (`vdm_agent_rtav.admx`), to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

Prerequisites

- Verify that the RTAV setup option is installed on your virtual machine desktops and RDS hosts. This setup option is installed by default but can be deselected during installation. The settings have no effect if RTAV is not installed. See your Setting Up document for information on installing Horizon Agent.
- Verify that Active Directory GPOs are created for the RTAV group policy settings. The GPOs must be linked to the OU that contains your virtual machine desktops or RDS hosts. See Active Directory Group Policy Example.
- 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.

Procedure

1. Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

   The file is named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADMX files that provide group policy settings for Horizon 7 are available in this file.

2. Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the ADMX files to your Active Directory server.

   a. Copy the `vdm_agent_rtav.admx` file and the `en-US` folder to the `C:\Windows\PolicyDefinitions` folder on your Active Directory server.

   b. (Optional) Copy the language resource file (`vdm_agent_rtav.adml`) to the appropriate subfolder in `C:\Windows\PolicyDefinitions\` on your Active Directory server.

3. On the Active Directory server, open the Group Policy Management Editor and enter the path to the template file in the editor.

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

What to do next

Configure the 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 remote 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 resolution 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 Horizon Agent virtual hardware, and the available bandwidth.

The resolution group policy settings determine the default values that are used when resolution values are not set by the user.

Group Policy Setting	Description
`Disable RTAV`	When you enable this setting, the Real-Time Audio-Video feature is disabled. When this setting is not configured or disabled, Real-Time Audio-Video is enabled. This setting is in the **VMware View Agent Configuration > View RTAV Configuration** folder in the Group Policy Management Editor.
`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. The minimum value is one frame per second. The maximum value is 25 frames per second. 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. 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. This setting is located in the **VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings** folder in the Group Policy Management Editor.

Group Policy Setting	Description
`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. 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. 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. This setting is located in the **VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings** folder in the Group Policy Management Editor.
`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. 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. 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. This setting is located in the **VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings** folder in the Group Policy Management Editor.
`Resolution – Default image resolution width in pixels`	Determines the default resolution width, in pixels, of image frames that are captured by the webcam. This setting is used when no resolution value is defined by the user. When this setting is not configured or disabled, the default image width is 320 pixels. The value that is configured by this policy setting takes effect only if both View Agent 6.0 or later and Horizon Client 3.0 or later are used. For older versions of View Agent and Horizon Client, this policy setting has no effect, and the default image width is 320 pixels. This setting is located in the **VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings** folder in the Group Policy Management Editor.
`Resolution – Default image resolution height in pixels`	Determines the default resolution height, in pixels, of image frames that are captured by the webcam. This setting is used when no resolution value is defined by the user. When this setting is not configured or disabled, the default image height is 240 pixels. The value that is configured by this policy setting takes effect only if both View Agent 6.0 or later and Horizon Client 3.0 or later are used. For older versions of View Agent and Horizon Client, this policy setting has no effect, and the default image height is 240 pixels. This setting is located in the **VMware View Agent Configuration > View RTAV Configuration > View RTAV Webcam Settings** folder in the Group Policy Management Editor.

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 2-3 measure the bandwidth that Real-Time Audio-Video uses in a View environment with standard webcam and audio input devices. The tests measure the bandwidth to send both video and audio data from Horizon Client to Horizon Agent. The total bandwidth that is required to run a desktop session from Horizon Client might be higher than these numbers. In these tests, the webcam captures images at 15 frames per second for each image resolution.

Table 2-3. Sample Bandwidth Results for Sending Real-Time Audio-Video Data from Horizon Client to Horizon Agent

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

Configuring Scanner Redirection

By using scanner redirection, Horizon 7 users can scan information in their remote desktops and applications with scanning and imaging devices that are connected locally to their client computers. Scanner redirection is available in Horizon 6.0.2 and later releases.

Scanner redirection supports standard scanning and imaging devices that are compatible with the TWAIN and WIA formats.

After you install Horizon Agent with the Scanner Redirection setup option, the feature works on your remote desktops and applications without further configuration. You do not have to configure scanner-specific drivers on remote desktops or applications.

You can configure group policy settings to change default values to adapt to particular scanning and imaging applications or environments. You can also set a policy to disable or enable the feature altogether. With an ADMX template file, you can install scanner redirection group policy settings in Active Directory or on individual desktops. See Configuring Scanner Redirection Group Policy Settings.

When scanning data is redirected to a remote desktop or application, you cannot access the scanning or imaging device on the local computer. Conversely, when a device is in use on the local computer, you cannot access it on the remote desktop or application.

System Requirements for Scanner Redirection

To support scanner redirection, your Horizon 7 deployment must meet certain software and hardware requirements.

Horizon 7 remote desktop or application

This feature is supported on RDS desktops, RDS applications, and VDI desktops that are deployed on single-user virtual machines.

You must install View Agent 6.0.2 or later, and select the Scanner Redirection setup option, on the parent or template virtual machines or RDS hosts.

On Windows Desktop and Windows Server guest operating systems, the Horizon Agent Scanner Redirection setup option is deselected by default.

The following guest operating systems are supported on single-user virtual machines and, where noted, on RDS hosts:

- 32-bit or 64-bit Windows 7

	■ 32-bit or 64-bit Windows 8.*x* ■ 32-bit or 64-bit Windows 10 ■ Windows Server 2008 R2 configured as a desktop or RDS host ■ Windows Server 2012 R2 configured as a desktop or RDS host **Important** The Desktop Experience feature must be installed on Windows Server guest operating systems, whether they are configured as desktops or as RDS hosts. The scanner device drivers do not have to be installed on the desktop operating system where Horizon Agent is installed.
Horizon Client software	Horizon Client 3.2 for Windows or a later release
Horizon Client computer or client access device	Supported operating systems: ■ 32-bit or 64-bit Windows 7 ■ 32-bit or 64-bit Windows 8.*x* ■ 32-bit or 64-bit Windows 10 The scanner device drivers must be installed, and the scanner must be operable, on the client computer.
Scanning device standard	TWAIN or WIA
Display protocol for Horizon 7	PCoIP Scanner redirection is not supported in RDP desktop sessions.

User Operation of Scanner Redirection

With scanner redirection, users can operate physical scanners and imaging devices that are connected to their client computers as virtual devices that perform scanning operations in their remote desktops and applications.

Users can operate their virtual scanners in a way that closely parallels the way that they use the scanners on their locally connected client computers.

- After the Scanner Redirection option is installed with Horizon Agent, a scanner tool tray icon icon () is added to the desktop. On RDS applications, the tool tray icon is redirected to the local client computer.

  You do not have to use the scanner tool tray icon. Scanning redirection works without any further configuration. You can use the icon to configure options such as changing which device to use if more than one device is connected to the client computer.

- When you click the scanner icon, the Scanner Redirection for VMware Horizon menu is displayed. No scanners appear in the menu list if incompatible scanners are connected to the client computer.
- By default, scanning devices are autoselected. TWAIN and WIA scanners are selected separately. You can have one TWAIN scanner and one WIA scanner selected at the same time.
- If more than one locally connected scanner is configured, you can select a different scanner than the one that is selected by default.
- WIA scanners are displayed in the remote desktop's Device Manager menu, under **Imaging devices**. The WIA scanner is named **VMware Virtual WIA Scanner**.
- In the Scanner Redirection for VMware Horizon menu, you can click the **Preferences** option and select options such as hiding webcams from the scanner redirection menu and determining how to select the default scanner.

  You can also control these features by configuring scanner redirection group policy settings in Active Directory. See Scanner Redirection Group Policy Settings.
- When you operate a TWAIN scanner, the TWAIN Scanner Redirection for VMware Horizon menu provides additional options for selecting regions of an image, scanning in color, black and white, or grayscale, and choosing other common functions.
- To display the TWAIN user interface window for TWAIN scanning software that does not display the window by default, you can select an **Always show Scanner Settings dialog** option in the VMware Horizon Scanner Redirection Preferences dialog box.

  Note that most TWAIN scanning software displays the TWAIN user interface window by default. For this software, the window is always displayed, whether you select or deselect the **Always show Scanner Settings dialog** option.

Note If you run two RDS applications that are hosted on different farms, two scanner redirection tool tray icons appear on the client computer. Typically, only one scanner is connected to a client computer. In this case, both icons operate the same device, and it does not matter which icon you select. In some situations, you might have two locally connected scanners and run two RDS applications that run on different farms. In that case, you must open each icon to see which scanner redirection menu controls which RDS application.

For end-user instructions for operating redirected scanners, see the *Using VMware Horizon Client for Windows* document.

Configuring Scanner Redirection Group Policy Settings

You can configure group policy settings that control the behavior of scanner redirection on your Horizon 7 desktops and applications. With these policy settings, you can control centrally, from Active Directory, the options that are available in the VMware Horizon Scanner Redirection Preferences dialog box on users' desktops and applications.

You do not have to configure these policy settings. Scanner redirection works with the default settings that are configured for scanning devices on remote desktops and client systems.

These policy settings affect your remote desktops and applications, not the client systems where the physical scanners are connected. To configure these settings on your desktops and applications, add the Scanner Redirection Group Policy Administrative Template (ADMX) file in Active Directory.

Add the Scanner Redirection ADMX Templates in Active Directory

You can add the policy settings in the scanner redirection ADMX template file (`vdm_agent_scanner.admx`) to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

Prerequisites

- Verify that the Scanner Redirection setup option is installed on your virtual machine desktops or RDS hosts. The group policy settings have no effect if scanner redirection is not installed. See your Setting Up document for information on installing Horizon Agent.
- Verify that Active Directory GPOs are created for the scanner redirection group policy settings. The GPOs must be linked to the OU that contains your virtual desktops or RDS hosts. See Active Directory Group Policy Example.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Familiarize yourself with scanner redirection group policy settings. See Scanner Redirection Group Policy Settings.

Procedure

1. Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

   The file is named `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADMX files that provide group policy settings for Horizon 7 are available in this file.

2. Unzip the `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip` file and copy the ADMX files to your Active Directory server.

   a. Copy the `vdm_agent_scanner.admx` file and the `en-US` folder to the `C:\Windows\PolicyDefinitions` folder on your Active Directory server.

   b. (Optional) Copy the language resource file (`vdm_agent_scanner.adml`) to the appropriate subfolder in `C:\Windows\PolicyDefinitions\` on your Active Directory server.

3. On the Active Directory server, open the Group Policy Management Editor and enter the path to the template file in the editor.

   The settings are located in the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Scanner Redirection** folder.

Most settings are also added to the **User Configuration** folder, located in **User Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Scanner Redirection** folder.

What to do next

Configure the group policy settings.

Scanner Redirection Group Policy Settings

The scanner redirection group policy settings control the options that are available in the VMware Horizon Scanner Redirection Preferences dialog box on users' desktops and applications.

The scanner redirection ADMX template file contains both Computer Configuration and User Configuration policies. The User Configuration policies allow you to set different configurations for users of VDI desktops, RDS desktops, and RDS applications. Different User Configuration policies can take effect even when users' desktop sessions and applications are running on the same RDS hosts. All of the settings are in the **VMware Horizon Agent Configuration > Scanner Redirection** folder in the Group Policy Management Editor.

Group Policy Setting	Computer	User	Description
`Disable functionality`	X		Disables the scanner redirection feature. When you enable this setting, scanners cannot be redirected and do not appear in the scanner menu on users' desktops and applications. When you disable this setting or do not configure it, scanner redirection works and scanners appear in the scanner menu.
`Lock config`	X		Locks the scanner redirection user interface and prevents users from changing configuration options on their desktops and applications. When you enable this setting, users cannot configure the options that are available from the tray menu on their desktops and applications. Users can display the VMware Horizon Scanner Redirection Preferences dialog box, but the options are inactive and cannot be changed. When you disable this setting or do not configure it, users can configure the options in the VMware Horizon Scanner Redirection Preferences dialog box.
`Compression`		X	Sets the image compression rate during the image transfer to the remote desktop or application. You can choose from the following compression modes: ■ **Disable**. Image compression is disabled. ■ **Lossless**. Lossless (`zlib`) compression is used without loss of image quality. ■ **JPEG**. JPEG compression is used with loss of quality. You specify the level of image quality in the **JPEG compression quality** field. JPEG compression quality must be a value between 0 and 100. When you enable this setting, the selected compression mode is set for all users affected by this policy. However, users can change the **Compression** option in the VMware Horizon Scanner Redirection Preferences dialog box, overriding the policy setting. When you disable this policy setting or do not configure it, **JPEG** compression mode is used.

Group Policy Setting	Computer	User	Description
Hide Webcam	X	X	Prevents webcams from appearing in the scanner selection menu in the VMware Horizon Scanner Redirection Preferences dialog box. By default, webcams can be redirected to desktops and applications. Users can select webcams and use them as virtual scanners to capture images. When you enable this setting as a Computer Configuration policy, webcams are hidden from all users of the affected computers. Users cannot change the **Hide Webcam** option in the VMware Horizon Scanner Redirection Preferences dialog box. When you enable this setting as a User Configuration policy, webcams are hidden from all affected users. However, users can change the **Hide Webcam** option in the VMware Horizon Scanner Redirection Preferences dialog box. When you enable this setting in both Computer Configuration and User Configuration, the **Hide Webcam** setting in Computer Configuration overrides the corresponding policy setting in User Configuration for all users of the affected computers. When you disable this setting or do not configure it in either policy configuration, the **Hide Webcam** setting is determined by the corresponding policy setting (either User Configuration or Computer Configuration) or by user selection in the VMware Horizon Scanner Redirection Preferences dialog box.
Default Scanner	X	X	Provides centralized management of scanner autoselection. You select scanner autoselection options separately for TWAIN and WIA scanners. You can choose from the following autoselection options: ■ **None**. Do not select scanners automatically. ■ **Autoselect** Automatically select the locally connected scanner. ■ **Last used** Automatically select the last-used scanner. ■ **Specified** Select the scanner name that you type in the **Specified scanner** text box. When you enable this setting as a Computer Configuration policy, the setting determines the scanner autoselection mode for all users of the affected computers. Users cannot change the **Default Scanner** option in the VMware Horizon Scanner Redirection Preferences dialog box. When you enable this setting as a User Configuration policy, the setting determines the scanner autoselection mode for all affected users. However, users can change the **Default Scanner** option in the VMware Horizon Scanner Redirection Preferences dialog box. When you enable this setting in both Computer Configuration and User Configuration, the scanner autoselection mode in Computer Configuration overrides the corresponding policy setting in User Configuration for all users of the affected computers. When you disable this setting or do not configure it in either policy configuration, the scanner autoselection mode is determined by the corresponding policy setting (either User Configuration or Computer Configuration) or by user selection in the VMware Horizon Scanner Redirection Preferences dialog box.

Configuring Serial Port Redirection

With serial port redirection, users can redirect locally connected, serial (COM) ports such as built-in RS232 ports or USB to Serial adapters. Devices such as printers, bar code readers, and other serial devices can be connected to these ports and used in the remote desktops.

Serial port redirection is available in Horizon 6 version 6.1.1 and later releases with Horizon Client for Windows 3.4 and later releases.

After you install Horizon Agent and set up the serial port redirection feature, the feature can work on your remote desktops without further configuration. For example, COM1 on the local client system is redirected as COM1 on the remote desktop, and COM2 is redirected as COM2, unless a COM port already exists on the remote desktop. If so, the COM port is mapped to avoid conflicts. For example, if COM1 and COM2 already exist on the remote desktop, COM1 on the client is mapped to COM3 by default. You do not have to configure the COM ports or install device drivers on the remote desktops.

To make a redirected COM port active, a user selects the **Connect** option from the menu on the serial port tool tray icon during a desktop session. A user can also set a COM port device to connect automatically whenever the user logs in to the remote desktop. See User Operation of Serial Port Redirection.

You can configure group policy settings to change the default configuration. For example, you can lock the settings so that users cannot change the COM port mappings or properties. You can also set a policy to disable or enable the feature altogether. With an ADMX template file, you can install serial port redirection group policy settings in Active Directory or on individual desktops. See Configuring Serial Port Redirection Group Policy Settings.

When a redirected COM port is opened and in use on a remote desktop, you cannot access the port on the local computer. Conversely, when a COM port is in use on the local computer, you cannot access the port on the remote desktop.

System Requirements for Serial Port Redirection

With this feature, end users can redirect locally connected, serial (COM) ports, such as built-in RS232 ports or USB to Serial adapters, to their remote desktops. To support serial port redirection, your Horizon deployment must meet certain software and hardware requirements.

Remote desktops

The remote desktops must have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, installed with the Serial Port Redirection setup option, on the parent or template virtual machines. This setup option is deselected by default.

The following guest operating systems are supported on single-session virtual machines:

- 32-bit or 64-bit Windows 7
- 32-bit or 64-bit Windows 8.x
- 32-bit or 64-bit Windows 10
- Windows Server 2008 R2 configured as a desktop
- Windows Server 2012 R2 configured as a desktop
- Windows Server 2016 configured as a desktop

	This feature is not currently supported for Windows Server RDS hosts. Serial port device drivers do not have to be installed on the desktop operating system where the agent is installed.
Horizon Client computer or client access device	■ Serial port redirection is supported on Windows 7, Windows 8.x client systems, and Windows 10. ■ Any required serial port device drivers must be installed, and the serial port must be operable, on the client computer. You do not need to install the device drivers on the remote desktop operating system where the agent is installed.
Display protocols	■ PCoIP ■ VMware Blast (requires Horizon Agent 7.0 or later) VMware Horizon serial port redirection is not supported in RDP desktop sessions.

User Operation of Serial Port Redirection

Users can operate physical COM port devices that are connected to their client computers and use serial port virtualization to connect the devices to their remote desktops, where the devices are accessible to 3rd party applications.

- After the Serial Port Redirection option is installed with Horizon Agent, a serial port tool tray icon () is added to the remote desktop. For published applications, the icon is redirected to the local client computer.

  The icon appears only if you use the required versions of Horizon Agent and Horizon Client for Windows, and you connect over PCoIP. The icon does not appear if you connect to a remote desktop from a Mac, Linux, or mobile client.

  You can use the icon to configure options to connect, disconnect, and customize the mapped COM ports.
- When you click the serial port icon, the **Serial COM Redirection for VMware Horizon** menu appears.
- By default, the locally connected COM ports are mapped to corresponding COM ports on the remote desktop. For example: **COM1 mapped to COM3**. The mapped ports are not connected by default.
- To use a mapped COM port, you must manually select the **Connect** option in the **Serial COM Redirection for VMware Horizon** menu, or the **Autoconnect** option must be set during a previous desktop session or by configuring a group policy setting. **Autoconnect** configures a mapped port to connect automatically when a remote desktop session is started.
- When you select the **Connect** option, the redirected port is active. In the Device Manager in the guest operating system on the remote desktop, the redirected port is shown as **Serial Port Redirector for VMware Horizon (COM*n*)**.

When the COM port is connected, you can open the port in a 3rd-party application, which can exchange data with the COM port device that is connected to the client machine. While a port is open in an application, you cannot disconnect the port in the **Serial COM Redirection for VMware Horizon** menu.

Before you can disconnect the COM port, you must close the port in the application or close the application. You can then select the **Disconnect** option to disconnect the port and make the physical COM port available for use on the client machine.

- In the **Serial COM Redirection for VMware Horizon** menu, you can right-click a redirected port to select the **Port Properties** command.

  In the COM Properties dialog box, you can configure a port to connect automatically when a remote desktop session is started, ignore the Data Set Ready (DSR) signal, enable the port to be a permanent port, and map the local port on the client to a different COM port on the remote desktop by selecting a port in the **Custom port name** drop-down list.

  A remote desktop port might be shown as overlapped. For example, you might see **COM1 (Overlapped)**. In this case, the virtual machine is configured with a COM port in the virtual hardware on the ESXi host. You can use a redirected port even when it is mapped to an overlapped port on the virtual machine. The virtual machine receives serial data through the port from the ESXi host or from the client system.

- In the Device Manager in the guest operating system, you can use the **Properties > Port Settings** tab to configure settings for a redirected COM port. For example, you can set the default baud rate and data bits. However, the settings you configure in Device Manager are ignored if the application specifies the port settings.

For end-user instructions for operating redirected serial COM ports, see the *Using VMware Horizon Client for Windows* document.

Guidelines for Configuring Serial Port Redirection

Through the group policy settings, you can configure serial port redirection and control the extent to which users can customize redirected COM ports. Your choices depend on the user roles and 3rd-party applications in your organization.

For details about the group policy settings, see Serial Port Redirection Group Policy Settings.

- If your users run the same 3rd-party applications and COM port devices, make sure that the redirected ports are configured in the same way. For example, in a bank or retail store that uses point-of-sale devices, make sure that all COM port devices are connected to the same ports on the client endpoints, and all ports are mapped to the same redirected COM ports on the remote desktops.

  Set the **PortSettings** policy setting to map client ports to redirected ports. Select the **Autoconnect** item in **PortSettings** to ensure that the redirected ports are connected at the start of each desktop session. Enable the **Lock Configuration** policy setting to prevent users from changing the port mappings or customizing the port configurations. In this scenario, users never have to connect or disconnect manually and cannot accidentally make a redirected COM port inaccessible to a 3rd-party application.

- If your users are knowledge workers who use a variety of 3rd-party applications and might also use their COM ports locally on their client machines, make sure that users can connect and disconnect from the redirected COM ports.

  You might set the **PortSettings** policy setting if the default port mappings are incorrect. You might or might not set the **Autoconnect** item, depending on your users' requirements. Do not enable the **Lock Configuration** policy setting.
- Make sure that your 3rd-party applications open the COM port that is mapped to the remote desktop.
- Make sure that the baud rate that is in use for a device matches the baud rate that the 3rd-party application is attempting to use.
- You can redirect up to five COM ports from a client system to a remote desktop.

Configuring Serial Port Redirection Group Policy Settings

You can configure group policy settings that control the behavior of serial port redirection on your remote desktops. With these policy settings, you can control centrally, from Active Directory, the options that are available in the **Serial COM Redirection for VMware Horizon** menu on users' desktops.

You do not have to configure these policy settings. Serial port redirection works with the default settings that are configured for redirected COM ports on remote desktops and client systems.

These policy settings affect your remote desktops, not the client systems where the physical COM port devices are connected. To configure these settings on your desktops, add the Serial Port Redirection Group Policy Administrative Template (ADMX) file in Active Directory.

Add the Serial Port Redirection ADMX Template in Active Directory

You can add the policy settings in the Serial COM (serial port redirection) ADMX file (`vdm_agent_serialport.admx`), to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

Prerequisites

- Verify that the Serial Port Redirection setup option is installed on your desktops. The group policy settings have no effect if serial port redirection is not installed. See your Setting Up document for more information on installing the Horizon Agent.
- Verify that Active Directory GPOs are created for the serial port redirection group policy settings. The GPOs must be linked to the OU that contains your desktops. See Active Directory Group Policy Example.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Familiarize yourself with serial port redirection group policy settings. See Serial Port Redirection Group Policy Settings.

Procedure

1 Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

The file is named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADMX files that provide group policy settings for Horizon 7 are available in this file.

2 Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the ADMX files to your Active Directory server.

a Copy the `vdm_agent_serialport.admx` file and the `en-US` folder to the `C:\Windows\PolicyDefinitions` folder on your Active Directory server.

b (Optional) Copy the language resource file (`vdm_agent_serialport.adml`) to the appropriate subfolder in `C:\Windows\PolicyDefinitions\` on your Active Directory server.

3 On the Active Directory server, open the Group Policy Management Editor and enter the path to the template file in the editor.

The settings are located in the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Serial COM** folder.

Most settings are also added to the **User Configuration** folder, located in **User Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Serial COM**.

What to do next

Configure the group policy settings.

Serial Port Redirection Group Policy Settings

The serial port redirection group policy settings control the redirected COM port configuration, including the options that are available in the **Serial COM Redirection for VMware Horizon** menu on remote desktops.

The serial port redirection ADMX file contains both Computer Configuration and User Configuration policies. The User Configuration policies allow you to set different configurations for specified users of VDI desktops. Policy settings that are configured in Computer Configuration take precedence over the corresponding settings that are configured in User Configuration.

Group Policy Setting	Computer	User	Description
PortSettings1 PortSettings2 PortSettings3 PortSettings4 PortSettings5	X	X	The port settings determine the mapping between the COM port on the client system and the redirected COM port on the remote desktop and determines other settings that affect the redirected COM port. You configure each redirected COM port individually. Five port settings policy settings are available, allowing up to five COM ports to be mapped from the client to the remote desktop. Select one port settings policy setting for each COM port that you intend to configure. When you enable the port settings policy setting, you can configure the following items that affect the redirected COM port: ■ The **Source port number** setting specifies the number of the physical COM port that is connected to the client system. ■ The **Destination virtual port number** setting specifies the number of the redirected virtual COM port on the remote desktop. ■ The **Autoconnect** setting automatically connects the COM port to the redirected COM port at the start of each desktop session. ■ With the **IgnoreDSR** setting, the redirected COM port device ignores the Data Set Ready (DSR) signal. ■ The **Pause before close port (in milliseconds)** setting specifies the time to wait (in milliseconds) after a user closes the redirected port and before the port is actually closed. Certain USB to Serial adapters require this delay to ensure that transmitted data is preserved. This setting is intended for troubleshooting purposes. ■ The **Serial2USBModeChangeEnabled** setting resolves issues that apply to USB to Serial adapters that use the Prolific chipset, including the GlobalSat BU353 GPS adapter. If you do not enable this setting for Prolific chipset adapters, connected devices can transmit data but not receive data. ■ The **Disable errors in wait mask** setting disables the error value in the COM port mask. This troubleshooting setting is required for certain applications. For details, see the Microsoft documentation of the `WaitCommEvent` function at http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx. ■ The **HandleBtDisappear** setting supports BlueTooth COM port behavior. This setting is intended for troubleshooting purposes. ■ The **UsbToComTroubleShooting** setting resolves some issues that apply to USB to Serial port adapters. This setting is intended for troubleshooting purposes. ■ The **Permanent** setting keeps the redirected COM port status in the remote session even if the client disconnects. When you enable the port settings policy setting for a particular COM port, users can connect and disconnect the redirected port, but users cannot configure properties of the port on the remote desktop. For example, users cannot set the port to be redirected automatically when they log in to the desktop, and they cannot ignore the DSR signal. These properties are controlled by the group policy setting. **Note** A redirected COM port is connected and active only if the physical COM port is connected locally to the client system. If you map a COM port that does not exist on the client, the redirected port appears as inactive and not available in the tool tray menu on the remote desktop.

Group Policy Setting	Computer	User	Description
			When the port settings policy setting is disabled or not configured, the redirected COM port uses the settings that users configure on the remote desktop. The **Serial COM Redirection for VMware Horizon** menu options are active and available to users. These settings are in the **VMware View Agent Configuration > Serial COM > PortSettings** folder in the Group Policy Management Editor.
`Local settings priority`	X	X	Gives priority to the settings that are configured on the remote desktop. When you enable this policy, the serial port redirection settings that a user configures on the remote desktop take precedence over the group policy settings. A group policy setting takes effect only if a setting is not configured on the remote desktop. When this setting is disabled or not configured, group policy settings take precedence over the settings that are configured on the remote desktop. This setting is in the **VMware View Agent Configuration > Serial COM** folder in the Group Policy Management Editor.
`Disable functionality`	X		Disables the serial port redirection feature. When you enable this setting, COM ports are not redirected to the remote desktop. The serial port tool tray icon on the remote desktop is not displayed. When this setting is disabled, serial port redirection works, the serial port tool tray icon is displayed, and COM ports appear in the **Serial COM Redirection for VMware Horizon** menu. When this setting is not configured, settings that are local to the remote desktop determine whether serial port redirection is disabled or enabled. This setting is in the **VMware View Agent Configuration > Serial COM** folder in the Group Policy Management Editor.
`Lock configuration`	X	X	Locks the serial port redirection user interface and prevents users from changing configuration options on the remote desktop. When you enable this setting, users cannot configure the options that are available from the tool tray menu on their desktops. Users can display the **Serial COM Redirection for VMware Horizon** menu, but the options are inactive and cannot be changed. When this setting is disabled, users can configure the options in the **Serial COM Redirection for VMware Horizon** menu. When this setting is not configured, local program settings on the remote desktop determine whether users can configure the COM port redirection settings. This setting is in the **VMware View Agent Configuration > Serial COM** folder in the Group Policy Management Editor.
`Bandwidth limit`	X		Sets a limit on the data transfer speed, in kilobytes per second, between the redirected serial port and client systems. When you enable this setting, you can set a value in the **Bandwidth limit (in kilobytes per second)** box that determines the maximum data transfer speed between the redirected serial port and the client. A value of 0 disables the bandwidth limit. When this setting is disabled, no bandwidth limit is set. When this setting is not configured, local program settings on the remote desktop determine whether a bandwidth limit is set. This setting is in the **VMware View Agent Configuration > Serial COM** folder in the Group Policy Management Editor.

Configure USB to Serial Adapters

You can configure USB to Serial adapters that use a Prolific chipset to be redirected to remote desktops by the serial port redirection feature.

To ensure that data is transmitted properly on Prolific chipset adapters, you can enable a serial port redirection group policy setting in Active Directory or on an individual desktop virtual machine.

If you do not configure the group policy setting to resolve issues for Prolific chipset adapters, connected devices can transmit data but not receive data.

You do not have to configure a policy setting or registry key on client systems.

Prerequisites

- Verify that the Serial Port Redirection setup option is installed on your desktops. The group policy settings have no effect if serial port redirection is not installed. See your Setting Up document for more information on installing Horizon Agent.
- Verify that the Serial Port Redirection ADMX template file is added in Active Directory or on the desktop virtual machine.
- Familiarize yourself with the **Serial2USBModeChangeEnabled** item in the **PortSettings** group policy setting. See Serial Port Redirection Group Policy Settings.

Procedure

1. In Active Directory or on the virtual machine, open the Group Policy Object Editor.
2. Navigate to the **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware View Agent Configuration > Serial COM** folder.
3. Select the **PortSettings** folder.
4. Select and enable a **PortSettings** group policy setting.
5. Specify the source and destination COM port numbers to map the COM port.
6. Select the **Serial2USBModeChangeEnabled** check box.
7. Configure other items in the **PortSettings** policy setting as needed.
8. Click **OK** and close the Group Policy Object Editor.

USB to Serial adapters can be redirected to remote desktops, and can receive data successfully, when users start their next desktop sessions.

Managing Access to Windows Media Multimedia Redirection (MMR)

Horizon 7 provides the Windows Media MMR feature for VDI desktops that run on single-user machines and for RDS desktops.

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.

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.

If the secure tunnel is enabled, MMR connections between clients and the View Secure Gateway are secure, but connections from the View Secure Gateway to desktop machines are not encrypted. If the secure tunnel is disabled, MMR connections from clients to the desktop machines are not encrypted.

Enabling Multimedia Redirection in Horizon 7

You can take steps to ensure that MMR is accessible only to Horizon Client systems that have sufficient resources to handle local multimedia decoding and that are connected to Horizon 7 on a secure network.

By default, the global policy in View Administrator, **Multimedia redirection (MMR)** is set to **Deny**.

To use MMR, you must explicitly set this value to **Allow**.

To control access to MMR, you can enable or disable the **Multimedia redirection (MMR)** policy globally, for individual desktop pools, or for specific users.

For instructions for setting global policies in Horizon Administrator, see Horizon 7 Policies.

System Requirements for Windows Media MMR

To support Windows Media Multimedia Redirection (MMR), your Horizon 7 deployment must meet certain software and hardware requirements. Windows Media MMR is provided in Horizon 6.0.2 and later releases.

Horizon 7 remote desktop

- This feature is supported on virtual machine desktops that are deployed on single-user virtual machines and on RDS desktops.

  View Agent 6.1.1 or later is required to support this feature on RDS desktops.

  View Agent 6.0.2 or later is required to support this feature on single-user machines.

- The following guest operating systems are supported:
  - 64-bit or 32-bit Windows 10. Windows Media Player is supported. The default player TV & Movies is not supported.

	■ Windows Server 2016 is a Tech Preview feature. Windows Media Player is supported. The default player TV & Movies is not supported. ■ 64-bit or 32-bit Windows 7 SP1 Enterprise or Ultimate (single-user machine). Windows 7 Professional is not supported. ■ 64-bit or 32-bit Windows 8/8.1 Professional or Enterprise (single-user machine) ■ Windows Server 2008 R2 configured as an RDS host ■ Windows Server 2012 and 2012 R2 configured as an RDS host ■ **3D Rendering** can be enabled or disabled on the desktop pool. ■ Users must play videos on Windows Media Player 12 or later or in Internet Explorer 8 or later. To use Internet Explorer, you must disable Protected Mode. In the Internet Options dialog box, click the **Security** tab and deselect **Enable Protected Mode**.
Horizon Client software	Horizon Client 3.2 for Windows or a later release is required to support Windows Media MMR on single-user machines.
Horizon Client computer or client access device	■ The clients must run 64-bit or 32-bit Windows 7, Windows 8/8.1, or Windows 10 operating systems.
Supported media formats	Media formats that are supported on Windows Media Player are supported. For example: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3; WAV. **Note** DRM-protected content is not redirected through Windows Media MMR.
Horizon policies	In Horizon Administrator, set the **Multimedia redirection (MMR)** policy to **Allow**. The default value is **Deny**.
Back-end firewall	If your Horizon 7 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.

Determine Whether to Use Windows Media MMR Based on Network Latency

By default, Windows Media MMR adapts to network conditions on single-user desktops that run on Windows 8 or later and RDS desktops that run on Windows Server 2012 or 2012 R2 or later. If the network latency between Horizon Client and the remote desktop is 29 milliseconds or lower, the video is redirected with Windows Media MMR. If the network latency is 30 milliseconds or higher, the video is not redirected. Instead, it is rendered on the ESXi host and sent to the client over PCoIP.

This feature applies to Windows 8 or later single-user desktops and Windows Server 2012 or 2012 R2 or later RDS desktops. Users can run any supported client system, Windows 7 or Windows 8/8.1.

This feature does not apply to Windows 7 single-user desktops or Windows Server 2008 R2 RDS desktops. On these guest operating systems, Windows Media MMR always performs multimedia redirection, regardless of network latency.

You can override this feature, forcing Windows Media MMR to perform multimedia redirection regardless of the network latency, by configuring the `RedirectionPolicy` registry setting on the desktop.

Procedure

1 Start the Windows Registry Editor on the remote desktop.

2 Navigate to the Windows registry key that controls the redirection policy.

The registry key that you configure for a remote desktop depends on the bit version of the Windows Media Player.

Option	Description
64-bit Windows Media Player	■ For a 64-bit desktop, use the registry key: `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr`
32-bit Windows Media Player	■ For a 32-bit desktop, use the registry key: `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr` ■ For a 64-bit desktop, use the registry key: `HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr`

3 Set the `RedirectionPolicy` value to `always`.

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

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

Managing Access to Client Drive Redirection

When you deploy Horizon Client and Horizon Agent with client drive redirection, folders and files are sent across the network with encryption.

Client drive redirection connections between clients and the View Secure Gateway and connections from the View Secure Gateway to desktop machines are secure. If VMware Blast is enabled, files and folders are transferred across a virtual channel with encryption.

TCP connections on port 9427 are required to support client drive redirection. If your Horizon 7 deployment includes a back-end firewall between your DMZ-based security servers and your internal network, the back-end firewall must allow traffic to port 9427 on your remote desktops. If VMware Blast is enabled, TCP port 9427 is not required to be open because client drive redirection transfers data through the virtual channel.

The **Client Drive Redirection** custom setup option in the Horizon Agent installer is selected by default. As a best practice, enable the **Client Drive Redirection** custom setup option only in remote desktops where users require this feature.

With Horizon Client releases that are earlier than version 3.5, or Horizon Agent releases that are earlier than version 6.2, client drive redirection folders and files are sent across the network without encryption and might contain sensitive data, depending on the content being redirected. If the secure tunnel is enabled, client drive redirection connections between Horizon Client and the View Secure Gateway are secure, but connections from the View Secure Gateway to desktop machines are not encrypted. If the secure tunnel is disabled, client drive redirection connections from Horizon Client to the desktop machines are not encrypted. To ensure that this data cannot be monitored on the network, use client drive redirection only on a secure network with earlier client and agent releases.

Use Group Policy to Disable Client Drive Redirection

You can disable client drive redirection by configuring a group policy setting for your remote desktops on your Active Directory server.

The group policy setting overrides the local registry and Smart Policies settings that enable the client drive redirection feature.

Prerequisites

- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Add the Remote Desktop Services ADMX template file `vmware_rdsh_server.admx` file to a GPO that is linked to the OU for your virtual desktops or to the RDS host for your published desktops. For installation instructions, see Add the ADMX Template Files to Active Directory.

Procedure

1. On your Active Directory server, open the Group Policy Management Editor and navigate to **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection**.
2. Open the **Do not allow drive redirection** group policy setting, select **Enabled**, and click **OK**.

Use Registry Settings to Configure Client Drive Redirection

You can use Windows registry key settings to control client drive redirection behavior on a remote desktop. This feature requires Horizon Agent 7.0 or later and Horizon Client 4.0 or later.

The Windows registry settings that control client drive redirection behavior on a remote desktop are located in the following path:

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

You can use the Windows Registry Editor on the remote desktop to edit local registry settings.

Note Client drive redirection policies set with Smart Policies take precedence over local registry settings.

Disabling Client Drive Redirection

To disable client drive redirection, create a new string value named `disabled` and set its value to `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

The value is `false` (enabled) by default.

Preventing Write Access to Shared Folders

To prevent write access to all folders that are shared with the remote desktop, create a new string value named `permissions` and set its value to any string that begins with `r`, except for `rw`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

The value is `rw` (all shared folders are readable and writeable) by default.

Sharing Specific Folders

To share specific folders with the remote desktop, create a new key named `default shares` and create a new subkey for each folder to share with the remote desktop. For each subkey, create a new string value named `name` and set its value to the path of the folder to share. The following example shares the folders `C:\ebooks` and `C:\spreadsheets`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

If you set `name` to `*all`, all client drives are shared with the remote desktop. The `*all` setting is supported only on Windows client systems.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

To prevent the client from sharing additional folders (that is, folders that are not specified with the `default shares` key), create a string value named `ForcedByAdmin` and set its value to `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

When the value is `true`, the Sharing dialog box does not appear when users connect to the remote desktop in Horizon Client. The value is `false` (clients can share additional folders) by default.

The following example shares the folders `C:\ebooks` and `C:\spreadsheets`, makes both folders read-only, and prevents the client from sharing additional folders.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Note Do not use the `ForcedByAdmin` feature as a security feature or share control. A user can bypass the `ForcedByAdmin=true` setting by creating a link to an existing share that points to folders not specified with the `default shares` key.

Using Client Drive Redirection in a Unified Access Gateway Implementation

If your Horizon 7 implementation uses a Unified Access Gateway appliance instead of a security server, users use client drive redirection with the PCoIP display protocol, and the Horizon Client and Horizon Agent machines are on different networks, the UDP Tunnel Server must be enabled for the Unified Access Gateway appliance.

To enable the UDP Tunnel Server, in the Unified Access Gateway admin UI, set the **UDP Tunnel Server Enabled** setting to **Yes**.

If you do not enable the UDP Tunnel Server, users cannot use the client drive redirection feature with the PCoIP display protocol. Client drive redirection works with the VMware Blast display protocol, regardless of whether the UDP Tunnel Server is enabled.

For more information, see the Unified Access Gateway documentation.

Configure Skype for Business

You can make optimized audio and video calls with Skype for Business inside a virtual desktop without negatively affecting the virtual infrastructure and overloading the network.

All media processing takes place on the client machine instead of in the virtual desktop during Skype audio and video call.

VMware Horizon Virtualization Pack for Skype for Business

To use Skype for Business, you must have the VMware Horizon Virtualization Pack for Skype for Business on the client machine.

You can configure group policy settings to change the default configuration. See VMware Virtualization Pack for Skype for Business Policy Settings.

A Horizon administrator must install the VMware Horizon Virtualization Pack for Skype for Business on the virtual desktop during Horizon Agent installation. To install the Horizon Client for Windows, see the *Using VMware Horizon Client for Windows* document.

The VMware Horizon Virtualization Pack for Skype for Business contains these software modules:

- Horizon Media Proxy installed inside the virtual desktop.
- Horizon Media Provider installed on the client endpoint

Skype for Business Features

Skype for Business offers the following features:

- E911 calls
- Call park and pick up
- Join external meetings anonymously
- Redirect calls to mobile devices
- Call statistics
- Smart card authentication
- Point to point audio calls
- Point to point video calls
- PSTN calls via dial pad
- Transfer, forward, mute, hold, and resume a call
- HID commands
- Calls to PSTN through mediation server
- Remote connectivity and calls through Edge Server

- Music on hold
- Custom ringtones
- Voicemail integration
- USB phones
- Published applications support
- Forward Error Correction (FEC) with audio and video
- Multiparty audio or video conferencing
- Meet Now conferencing
- Whiteboarding and screensharing

System Requirements

This feature supports these configurations.

Table 2-4. Skype for Business System Requirements

System	Requirements
Microsoft Server	Lync Server 2013, Skype for Business Server 2015, Office365
Microsoft Client	VMware strongly recommends using the latest update Skype for Business 2015 client 15.0.4933.100 or later Skype for Business 2016 as part of Office 365 Plus: 16.0.7571.2072 or later Skype for Business 2016 as part of Office 2016: 16.0.4561.1000 or later
Virtual desktop operating systems	■ Windows 7 SP1 ■ Windows 8.1, ■ Windows 10 persistent and non-persistent desktops ■ Windows 2008 R2 SP1 desktops ■ Windows 2012 R2 desktops ■ Windows 2008 R2 SP1 RDSH desktops ■ Windows 2012 R2 RDSH desktops ■ Published Application Support

Table 2-4. Skype for Business System Requirements (Continued)

System	Requirements
Client machine operating systems	■ Windows 7 SP1 ■ Windows 8.1 ■ Windows 10 ■ WES7 ■ Windows 10 IoT ■ Ubuntu 14.04 32-bit ■ Ubuntu 14.04 64-bit ■ Ubuntu 16.04 64-bit ■ RHEL 6.9 32-bit ■ RHEL 6.9 64-bit ■ RHEL 7.3 64-bit ■ CentOS 6.x 32-bit ■ CentOS 6.x 64-bit ■ SLED 12 SP2 64-bit
Deployments	VDI only (on premise and Cloud), persistent and non-persistent desktops
Display protocols	VMware Blast and PCoIP
Network ports	The same ports as those used by the native Skype for Business client. See client ports in https://technet.microsoft.com/en-us/library/gg398833.aspx
Microphones and Webcams	The same devices that are qualified to work with Skype for Business. See webcams listed in https://technet.microsoft.com/en-us/office/dn947482.aspx
Audio and video codecs	The same as the audio and video codecs used by the native Skype for Business client. See https://technet.microsoft.com/en-us/library/gg425841.aspx?f=255&MSPPError=-2147217396
Media Feature Pack	Must be installed on the remote desktop for Windows 10 N and KN versions. You can install Media Feature from https://www.microsoft.com/en-us/download/details.aspx?id=48231

Limitations

Skype for Business has the following limitations:

- IPv6 is not supported. Only IPv4 deployments are supported.
- Response group call and call via X (home, work, etc.) are not supported
- Gallery view is not currently supported.
- You cannot record calls.
- Double-hop scenario such as Horizon Agent nested with Horizon Client is not supported.
- Using Lync or Skype for Business client on the client machine concurrently with optimized Skype for Business client in the remote desktop is not supported.

- The Lync 2013 client UI is not supported when connecting Skype 2015 client to a Lync 2013 server. An administrator can configure Skype client UI on the server: https://social.technet.microsoft.com/wiki/contents/articles/30282.switch-between-skype-for-business-and-lync-client-ui.aspx
- In the video preview window, if you want to preview a different camera than the one listed, select the device, then close the dialog, then re-open it to preview it.
- If you are connected to a private network when you install Skype for Business on the remote desktop, the installer adds inbound and outbound firewall rules for that network profile. When you log on to the remote desktop from a domain network and then use Skype for Business, you see a firewall exception. To fix the problem, manually add firewall exceptions for Skype for Business client in the firewall rules for all network profiles.
- The volume control option in the remote desktop operating system does not affect the volume level of an ongoing Skype call. Use the volume control in the Skype call or use the volume control on the client machine to make volume changes.

Collect Logs to Troubleshoot Skype for Business

To troubleshoot Skype for Business, collect logs from the Horizon Agent and the Windows Horizon Client.

Procedure

1. To collect Horizon logs, including the Media Proxy logs, from the Horizon Agent, log into a virtual machine where Horizon Agent is installed.
2. Open a command prompt, and run `C:\Program Files\VMware\VMware View\Agent\DCT\support.bat`
3. To collect Horizon logs, including the Media Provider logs, from the Horizon Client, log into a physical or a virtual machine where Horizon Client is installed.
4. Open a command prompt, and run:
   - 32-bit: `C:\Program Files\VMware\VMware Horizon View Client\DCT\support.bat`
   - 64-bit: `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat`

A folder vdm-sdct containing zipped log files appears on the desktop and will include these directories which contain logs for the VMware Horizon Virtualization Pack for Skype for Business:

- Client device: `%TEMP%\vmware-<username>\VMWMediaProvider`
- Virtual desktop:
  - `%TEMP%\vmware-<username>\VMWMediaProviderProxy`
  - `%TEMP%\vmware-<username>\VMWMediaProviderProxyLocal`
  - `%TEMP%\vmware-<username>\MMAPlugin`

The default log level is 7, where the log level size and crash dumps are small. You can increase the log level to 8 for maximum logs and full crash dumps. All settings are DWORD:

- Client: HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProvider/DebugLogging/LoggingPriority = 8
- Agent: HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxy/DebugLogging/LoggingPriority = 8
- Agent: HKEY_CURRENT_USER/SOFTWARE/VMware, Inc./VMWMediaProviderProxyLocal/DebugLogging/LoggingPriority = 8

Activate the BEAT Side Channel for USB or Client Drive Redirection

With the VMware Blast display protocol, you can configure the USB redirection and client drive redirection features to send side channel traffic over a Blast Extreme Adaptive Transport (BEAT) connection rather than through the VMware Virtual Channel (VVC) or TCP side channel.

The BEAT side channel enables you to consolidate network port requirements for USB redirection and client drive redirection. If your network allows VMware Blast session traffic, you do not need to open any additional UDP ports because the BEAT side channel shares a single UDP port with core (mouse, keyboard, and display) VMware Blast session traffic. By comparison, the TCP side channel, which does not share the TCP port used for session traffic, requires you to open another TCP port.

This feature is supported only with Horizon Client for Windows. Non-Windows clients are not supported in this release.

Procedure

1. To activate the BEAT side channel for the client drive redirection feature, perform these steps.
   a. Open the Windows Registry Editor (`regedit.exe`) on the agent machine.
   b. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware TSDR` and set the `sideChannelType` key to `beat`.
2. To active the BEAT side channel for the USB redirection feature, perform these steps.
   a. Open the Windows Registry Editor (`regedit.exe`) on the agent machine.
   b. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration` and set the `UsbVirtualChannelEnabled` key to `true`.
   c. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection`, set the `vchanSideChannelEnabled` key to `true`, and set the `sideChannelType` key to `beat`.
   d. Open the Windows Registry Editor (`regedit.exe`) on the client machine.
   e. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Client` and set the `EnableUsbVirtualChannelOnClient` key to `true`.

Configuring URL Content Redirection

3

With the URL Content Redirection feature, you can configure specific URLs to open on the client machine or in a remote desktop or application. You can redirect URLs that users type in the Internet Explorer address bar or in an application.

This section includes the following topics:

Understanding URL Content Redirection

The URL Content Redirection feature supports redirection from a remote desktop or application to a client, and from a client to a remote desktop or application.

Redirection from a remote desktop or application to a client is called agent-to-client redirection. Redirection from a client to a remote desktop or application is called client-to-agent redirection.

Agent-to-client redirection	With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL on the client machine.
Client-to-agent redirection	With client-to-agent redirection, Horizon Client opens a remote desktop or remote application that you specify to handle the URL. If the URL is redirected to a remote desktop, the link is opened in the default browser for the protocol on the desktop. If the URL is redirected to a remote application, the link is opened by the specified application. The end user must be entitled to the desktop or application pool.

You can redirect some URLs from a remote desktop or application to a client, and redirect other URLs from a client to a remote desktop or application. You can redirect any number of protocols, including HTTP, HTTPS, mailto, and callto.

Requirements for URL Content Redirection

To use the URL Content Redirection feature, your client machines, remote desktop machines, and RDS hosts must meet certain requirements.

Windows clients	Horizon Client 4.0 for Windows or later. To use client-to-agent redirection, you must enable the URL Content Redirection feature during Horizon Client for Windows installation. You do not need to enable the URL Content Redirection feature in Horizon Client for Windows to use agent-to-client redirection.
Mac clients	Horizon Client 4.2 for Mac or later. In Horizon Client 4.2 or 4.3 for Mac, URL Content Redirection is a Tech Preview feature and it supports only agent-to-client redirection. In Horizon Client 4.4 for Mac and later, URL Content Redirection is officially supported and it supports both agent-to-client and client-to-agent redirection.
Desktop virtual machines and RDS hosts	Horizon Agent 7.0 or later in remote desktop machines and RDS hosts that provide desktops and applications. You must enable the URL Content Redirection feature during Horizon Agent installation.
Web browsers	Internet Explorer 9,10, and 11
Display protocols	VMware Blast and PCoIP

Using URL Content Redirection in a Cloud Pod Architecture Environment

If you have a Cloud Pod Architecture environment, you can configure global URL content redirection settings in addition to local URL content redirection settings.

Unlike local URL content redirection settings, which are visible only in the local pod, global URL content redirection settings are visible across the pod federation. With global URL content redirection settings, you can redirect URL links in the client to global resources, such as global desktop entitlements and global application entitlements.

When a user uses Horizon Client to log in to a Connection Server instance in the pod federation, the Connection Server instance looks for all of the local and global URL content redirection settings assigned to the user. The local and global settings are merged and used whenever the user clicks a URL on the client machine.

For complete information about configuring and managing a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon 7* document.

Installing Horizon Agent with the URL Content Redirection Feature

To use URL content redirection from a remote desktop or application to a client (agent-to-client redirection), or from a client to a remote desktop or application (client-to-agent redirection), you must enable the URL Content Redirection feature when you install Horizon Agent.

Instead of double-clicking the installer file, start the Horizon Agent installation by running the following command in a command prompt window:

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Follow the prompts and complete the installation.

To verify that the URL Content Redirection feature is installed, make sure that the `vmware-url-protocol-launch-helper.exe` and `vmware-url-filtering-plugin.dll` files are in the `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection` directory. Also, verify that the VMware Horizon View URL Filtering Plugin Internet Explorer add-on is enabled.

Configuring Agent-to-Client Redirection

With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL.

To enable agent-to-client redirection, perform the following configuration tasks.

- Enable the URL Content Redirection feature in Horizon Agent. See Installing Horizon Agent with the URL Content Redirection Feature.
- Apply the URL Content Redirection group policy settings to your remote desktops and applications. See Add the URL Content Redirection ADMX Template to a GPO.
- Configure group policy settings to indicate, for each protocol, how Horizon Agent should redirect the URL. See URL Content Redirection Group Policy Settings.

Add the URL Content Redirection ADMX Template to a GPO

The URL Content Redirection ADMX template file, called `urlRedirection.admx`, contains settings that enable you to control whether a URL link is opened on the client (agent-to-client redirection) or in a remote desktop or application (client-to-agent redirection).

To apply the URL Content Redirection group policy settings to your remote desktops and applications, add the ADMX template file to GPOs on your Active Directory server. For rules regarding URL links clicked in a remote desktop or application, the GPOs must be linked to the OU that contains your virtual desktops and RDS hosts.

You can also apply the group policy settings to a GPO that is linked to the OU that contains your Windows client computers, but the preferred method for configuring client-to-agent redirection is to use the `vdmutil` command-line utility. Because macOS does not support GPOs, you must use `vmdutil` if you have Mac clients.

Prerequisites

- Verify that the URL Content Redirection feature is included when you install Horizon Agent. See Installing Horizon Agent with the URL Content Redirection Feature.
- Verify that Active Directory GPOs are created for the URL Content Redirection group policy settings.
- Verify that the MMC and the Group Policy Management Editor snap-in are available on your Active Directory server.

Procedure

1. Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

   The file is named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADMX files that provide group policy settings for Horizon 7 are available in this file.

2. Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the URL Content Redirection ADMX file to your Active Directory server.

   a. Copy the `urlRedirection.admx` file to the `C:\Windows\PolicyDefinitions` folder.

   b. Copy the `urlRedirection.adml` language resource file to the appropriate subfolder in `C:\Windows\PolicyDefinitions`.

      For example, for the EN locale, copy the `urlRedirection.adml` file to the `C:\Windows\PolicyDefinitions\en-US` folder.

3 On your Active Directory server, open the Group Policy Management Editor.

The URL Content Redirection group policy settings are installed in **Computer Configuration > Policies > Administrative Templates > VMware Horizon URL Redirection**.

What to do next

Configure the group policy settings.

URL Content Redirection Group Policy Settings

The URL Content Redirection template file contains group policy settings that enable you to create rules for agent-to-client and client-to-agent redirection. The template file contains only Computer Configuration settings. All of the settings are in the **VMware Horizon URL Redirection** folder in the Group Policy Management Editor.

The following table describes the group policy settings in the URL Content Redirection template file.

Table 3-1. URL Content Redirection Group Policy Settings

Setting	Properties
`IE Policy: Prevent users from changing URL Redirection plugin loading behavior`	Determines whether users can disable the URL Content Redirection feature. This setting is not configured by default.
`IE Policy: Automatically enable URL Redirection plugin`	Determines whether newly installed Internet Explorer plug-ins are automatically activated. This setting is not configured by default.
`Url Redirection Enabled`	Determines whether the URL Content Redirection feature is enabled. You can use this setting to disable the URL Content Redirection feature even if the feature has been installed in the client or agent. This setting is not configured by default.

Table 3-1. URL Content Redirection Group Policy Settings (Continued)

Setting	Properties
`Url Redirection Protocol 'http'`	For all URLs that use the HTTP protocol, specifies the URLs that should be redirected. This setting has the following options: ■ **brokerHostname** - IP address or fully qualified name of the Connection Server host to use when redirecting URLs to a remote desktop or application. ■ **remoteItem** - display name of the remote desktop or application pool that can handle the URLs specified in **agentRules**. ■ **clientRules** - the URLs that should be redirected to the client. For example, if you set **clientRules** to `.*.mycompany.com`, all URLs that include the text `mycompany.com` are redirected to the Windows-based client and are opened in the default browser on the client. ■ **agentRules** - the URLs that should be redirected to the remote desktop or application specified in **remoteItem**. For example, if you set **agentRules** to `.*.mycompany.com`, all URLs that include "mycompany.com" are redirected to the remote desktop or application. When you create agent rules, you must also use the **brokerHostname** option to specify the IP address or fully qualified domain name of the Connection Server host, and the **remoteItem** option to specify the display name of the desktop or application pool. **Note** The preferred method for configuring client rules is to use the `vdmutil` command-line utility. This setting is enabled by default.
`Url Redirection Protocol '[...]'`	Use this setting for any protocol other than HTTP, such as HTTPS, email, or callto. The options are the same as for `Url Redirection Protocol 'http'`. If you do not need to configure other protocols, you can delete or comment out this entry before adding the URL Content Redirection template file to Active Directory. As a best practice, configure the same redirection settings for the HTTP and HTTPS protocols. That way, if a user types a partial URL into Internet Explorer, such as `mycompany.com`, and that site automatically redirects from HTTP to HTTPS, the URL Content Redirection feature will work as expected. In this example, if you set a rule for HTTPS but do not set the same redirection setting for HTTP, the partial URL that the user types is not redirected. This setting is not configured by default.

For client-to-agent redirection, if you configure a protocol that does not have a default handler, after you configure a group policy setting for this protocol, you must start Horizon Client once before URLs that specify this protocol are redirected.

Syntax for Creating URL Content Redirection Rules

You can use regular expressions when you specify which URLs to open on the client or in a remote desktop or application. Use semicolons to separate multiple entries. Spaces are not allowed between entries.

The following table describes some sample entries.

Entry	Description
`.*`	Specifies that all URLs are redirected. If you use this setting for agent rules (**agentRules** option), all URLs are opened in the specified remote desktop or application. If you use this setting for client rules (**clientRules** option), all URLs are redirected to the client.
`.*.acme.com;.*.example.com`	Specifies that all URLs that include the text `.acme.com` or `example.com` are redirected.
[space or leave empty]	Specifies that no URLs are redirected. For example, leaving the **clientRules** option empty specifies that no URLs are redirected to the client.

Agent-to-Client Redirection Group Policy Example

You might want to use agent-to-client redirection to conserve resources or as an added security layer. If employees are working in a remote desktop or application and they want to watch videos, for example, you might redirect those URLs to the client machine so that no extra load is put on the data center. Or for security purposes, for employees working outside the company network, you might want all URLs that point to external locations outside the company network to be opened on an employee's own client machine.

You could, for example, configure rules so that any content that is not company-related, that is, any URLs that do not point to the company network, are redirected to open on the client machine. In this case you could use the following settings, which include regular expressions:

- For **agentRules**: `.*.mycompany.com`

  This rule redirects any URL that contains the text `mycompany.com` to be opened on the specified remote desktop or application (agent).

- For **clientRules**: `.*`

  This rule redirects all URLs to the client, to be opened with the default client browser.

The URL Content Redirection feature uses the following process to apply client and agent rules:

1. When a user clicks a link in a remote application or desktop, the client rules are checked first.
2. If the URL matches a client rule, the agent rules are checked next.
3. If there is a conflict between the agent rules and the client rules, the link is opened locally. In this case, the URL is opened on the agent machine.
4. If there is no conflict, the URL is redirected to the client.

   In the example, the client and agent rules conflict because URLs with `mycompany.com` are a subset of all URLs. Because of this conflict, URLs that include `mycompany.com` are opened locally. If you click a link that includes `mycompany.com` in the URL while in a remote desktop, the URL is opened on that remote desktop. If you click a link with `mycompany.com` in the URL in it from a client system, the URL is opened on the client.

Configuring Client-to-Agent Redirection

With client-to-agent redirection, Horizon Client opens a remote desktop or application to handle a URL link that a user clicks on the client. If a remote desktop is opened, the default application for the protocol in the URL processes the URL. If a remote application is opened, the application processes the URL.

To use client-to-agent redirection, perform the following configuration tasks.

- Enable the URL Content Redirection feature in Horizon Agent. See Installing Horizon Agent with the URL Content Redirection Feature.
- (Windows clients only) Enable the URL Content Redirection feature in Horizon Client for Windows. See Installing Horizon Client for Windows with the URL Content Redirection Feature.
- Use the `vdmutil` command-line utility to create a URL content redirection setting that indicates, for each protocol, how Horizon Client should redirect the URLs. See Create a Local URL Content Redirection Setting or Create a Global URL Content Redirection Setting.
- Use the `vdmutil` command-line utility to assign the URL content redirection setting to Active Directory users or groups. See Assign a URL Content Redirection Setting to a User or Group.
- Verify the URL content redirection setting. See Test a URL Content Redirection Setting.

Note You can use group policy settings to configure client-to-agent redirection rules, but using the `vdmutil` command-line utility is the preferred method. For information about using group policy settings, see Using Group Policy Settings to Configure Client-to-Agent Redirection. For Mac clients, you must use `vdmutil` to configure client-to-agent redirection. Because GPOs are not supported by macOS, you cannot use group policy settings to configure client-to-agent configuration if you have Mac clients.

Installing Horizon Client for Windows with the URL Content Redirection Feature

To use URL Content Redirection from a Windows client to a remote desktop or application (client-to-agent redirection), you must install Horizon Client for Windows with the URL Content Redirection feature.

To enable the URL Content Redirection feature, you must use the Horizon Client for Windows installer with a command-line option. Instead of double-clicking the installer file, start the installation by running the following command in a command prompt window:

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

To verify that the feature is installed, make sure that the `vmware-url-protocol-launch-helper.exe` and `vmware-url-filtering-plugin.dll` files are in the `%PROGRAMFILES%\VMware\VMware Horizon View Client` directory. Also, verify that the VMware Horizon View URL Filtering Plugin Internet Explorer add-on is installed.

Note Horizon Client 4.4 for Mac supports client-to-agent redirection by default. No extra installation steps are required. Horizon Client 4.2 and 4.3 for Mac do not support client-to-agent redirection.

Using the vdmutil Command-Line Utility

You can use the `vdmutil` command-line interface to create, assign, and manage URL content redirection settings for client-to-agent redirection.

Note You must use the `vdmutil` command to configure client-to-agent redirection for Mac clients. Because GPOs are not supported by macOS, you cannot use GPOs to configure client-to-agent configuration if you have Mac clients.

Command Usage

The syntax of the `vdmutil` command controls its operation from a Windows command prompt.

```
vdmutil command_option [additional_option argument] ...
```

The additional options that you can use depend on the command option.

By default, the path to the `vdmutil` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`. To avoid entering the path on the command line, add the path to your PATH environment variable.

Command Authentication

You must run the `vdmutil` command as a user who has the Administrators role.

You can use Horizon Administrator to assign the Administrators role to a user. For more information, see the *View Administration* document.

The `vdmutil` command includes options to specify the user name, domain, and password to use for authentication. You must use these authentication options with all `vdmutil` command options except for `--help` and `--verbose`.

Table 3-2. vdmutil Command Authentication Options

Option	Description
`--authAs`	User name of a Horizon administrator user to authenticate to the Connection Server instance. Do not use **`domain\username`** or user principal name (UPN) format.
`--authDomain`	Fully qualified domain name for the Horizon administrator user specified in the `--authAs` option.
`--authPassword`	Password for the Horizon administrator specified in the `--authAs` option. Typing **"*"** instead of a password causes the `vdmutil` command to prompt for the password and does not leave sensitive passwords in the command history on the command line.

For example, the following `vdmutil` command logs in the user mydomain\johndoe.

```
vdmutil --listURLSetting --authAs johndoe --authDomain mydomain --authPassword secret
```

Command Output

The `vdmutil` command returns 0 when an operation succeeds and a failure-specific non-zero code when an operation fails. The `vdmutil` command writes error messages to standard error. When an operation produces output, or when verbose logging is enabled by using the `--verbose` option, the `vdmutil` command writes output to standard output in US English.

Options for URL Content Redirection

You can use the following `vdmutil` command options to create, assign, and manage URL content redirection settings. All options are preceded by two dashes (--).

Table 3-3. vdmutil Command Options for URL Content Redirection

Option	Description
`--addGroupURLSetting`	Assigns a group to a particular URL content redirection setting.
`--addUserURLSetting`	Assigns a user to a particular URL content redirection setting.
`--createURLSetting`	Creates a URL content redirection setting.
`--deleteURLSetting`	Deletes a URL content redirection setting.
`--disableURLSetting`	Disables a URL content redirection setting.
`--enableURLSetting`	Enables a URL content redirection setting that was previously disabled with the `--disableURLSetting` option.
`--listURLSetting`	Lists all of the URL content redirection settings on the Connection Server instance.
`--readURLSetting`	Displays information about a URL content redirection setting.
`--removeGroupURLSetting`	Removes a group assignment from a URL content redirection setting.
`--removeUserURLSetting`	Removes a user assignment from a URL content redirection setting.
`--updateURLSetting`	Updates an existing URL content redirection setting.

You can display syntax information for all `vdmutil` options by typing **`vdmutil --help`**. To display detailed syntax information for a particular option, type **`vdmutil --`*`option`*` --help`**.

Create a Local URL Content Redirection Setting

You can create a local URL content redirection setting that redirects specific URLs to open on a remote desktop or application. A local URL content redirection setting is visible only in the local pod.

You can configure any number of protocols, including HTTP, HTTPS, mailto, and callto.

As a best practice, configure the same redirection settings for the HTTP and HTTPS protocols. That way, if a user types a partial URL into Internet Explorer, such as `mycompany.com`, and that site automatically redirects from HTTP to HTTPS, the URL Content Redirection feature will work as expected. In this example, if you set a rule for HTTPS but do not set the same redirection setting for HTTP, the partial URL that the user types is not redirected.

To create a global URL content redirection setting, which is visible across the pod federation, see Create a Global URL Content Redirection Setting.

Prerequisites

Become familiar with `vdmutil` command-line interface options and requirements and verify that you have sufficient privileges to run the the `vdmutil` command. See Using the vdmutil Command-Line Utility.

Procedure

1 Log in to the Connection Server instance.

2 Run the `vdmutil` command with the `--createURLSetting` option to create the URL content redirection setting.

```
vdmutil --createURLSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

Option	Description
--urlSettingName	Unique name for the URL content redirection setting. The name can contain between 1 and 64 characters.
--urlRedirectionScope	Scope of the URL content redirection setting. Specify LOCAL to make the setting visible only in the local pod.
--description	Description of the URL content redirection setting. The description can contain between 1 and 1024 characters.
--urlScheme	Protocol to which the URL content redirection setting applies, for example, http, https, mailto, or callto.
--entitledApplication	Display name of a local application pool to use to open the specified URLs, for example, `iexplore-2012`. You can also use this option to specify the display name of a local RDS desktop pool.
--entitledDesktop	Display name of a local desktop pool to use to open the specified URLs, for example, xx. For RDS desktop pools, use the `--entitledApplication` option.
--agentURLPattern	A quoted string that specifies the URL that should be opened on the remote desktop or application. You must include the protocol prefix. You can use wildcards to specify a URL pattern that matches multiple URLs. For example, if you type **"http://google.*"**, all URLs that include the text **google** are redirected to the remote desktop or application pool that you specified. If you type **.*** (dot star), all URLs are redirected to the remote desktop or application.

3 (Optional) Run the `vdmutil` command with the `--updateURLSetting` option to add more protocols, URLs, and local resources to the URL content redirection setting that you created.

```
vdmutil --updateURLSetting --urlSettingName value --urlRedirectionScope LOCAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop value] [--
agentURLPattern value]
```

The options are the same as for the `vdmutil` command with the `--createURLSetting` option.

Example: Creating a Local URL Content Redirection Setting

The following example creates a local URL content redirection setting called `url-filtering` that redirects all client URLs that include the text `http://google.*` to the application pool called `iexplore2012`.

```
VdmUtil --createURLSetting --urlSettingName url-filtering --urlScheme http
--entitledApplication iexplore2012 --agentURLPattern "http://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

The following example updates the `url-filtering` setting to also redirect all client URLs that contain the text `https://google.*` to the application pool called `iexplore2012`.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme https
--entitledApplication iexplore2012 --agentURLPattern "https://google.*"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

The following example updates the `url-filtering` setting to redirect all client URLs that contain the text `mailto://.*.mycompany.com` to the application pool called `Outlook2008`.

```
vdmutil --updateURLSetting --urlSettingName url-filtering --urlScheme mailto
--entitledApplication Outlook2008 --agentURLPattern "mailto://.*.mycompany.com"
--urlRedirectionScope LOCAL --authAs johndoe --authDomain mydomain --authPassword secret
```

What to do next

Assign the URL content redirection setting to a user or group. See Assign a URL Content Redirection Setting to a User or Group.

Create a Global URL Content Redirection Setting

If you have a Cloud Pod Architecture environment, you can create a global URL content redirection setting that redirects specific URLs to open on a remote desktop or application in any pod in the pod federation.

A global URL content redirection setting is visible across the pod federation. When you create a global URL content redirection setting, you can redirect URLs to global resources, such as global desktop entitlements and global application entitlements.

You can configure any number of protocols, including HTTP, HTTPS, mailto, and callto.

As a best practice, configure the same redirection settings for the HTTP and HTTPS protocols. That way, if a user types a partial URL into Internet Explorer, such as `mycompany.com`, and that site automatically redirects from HTTP to HTTPS, the URL Content Redirection feature will work as expected. In this example, if you set a rule for HTTPS but do not set the same redirection setting for HTTP, the partial URL that the user types is not redirected.

For complete information about configuring and managing a Cloud Pod Architecture environment, see the *Administering Cloud Pod Architecture in Horizon 7* document.

To create a local URL content redirection setting, see Create a Local URL Content Redirection Setting.

Prerequisites

Become familiar with `vdmutil` command-line interface options and requirements and verify that you have sufficient privileges to run the the `vdmutil` command. See Using the vdmutil Command-Line Utility.

Procedure

1 Log in to any Connection Server instance in the pod federation.

2 Run the `vdmutil` command with the `--createURLSetting` option to create the URL content redirection setting.

```
vdmutil --createURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

Option	Description
--urlSettingName	Unique name for the URL content redirection setting. The name can contain between 1 and 64 characters.
--urlRedirectionScope	Scope of the URL content redirection setting. Specify GLOBAL to make the setting visible across the pod federation.
--description	Description of the URL content redirection setting. The description can contain between 1 and 1024 characters.
--urlScheme	Protocol to which the URL content redirection setting applies, for example, http, https, mailto, or callto.
--entitledApplication	Display name of a global application entitlement to use to open the specified URLs.
--entitledDesktop	Display name of a global desktop entitlement to use to open the specified URLs, for example, GE-1.
--agentURLPattern	A quoted string that specifies the URL that should be opened on the remote desktop or application. You must include the protocol prefix. You can use wildcards to specify a URL pattern that matches multiple URLs. For example, if you type "http://google.*", all URLs that include the text google are redirected to the remote desktop or application. If you type .* (dot star), all URLs are redirected to the remote desktop or application.

3 (Optional) Run the `vdmutil` command with the `--updateURLSetting` option to add more protocols, URLs, and global resources to the URL content redirection setting that you created.

```
vdmutil --updateURLSetting --urlSettingName value --urlRedirectionScope GLOBAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

The options are the same as for the `vdmutil` command with the `--createURLSetting` option.

Example: Configuring a Global URL Content Redirection Setting

The following example creates a global URL content redirection setting called `Operations-Setting` that redirects all client URLs that include the text `http://google.*` to the global application entitlement called `GAE1`.

```
vdmutil --createURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme http --entitledApplication GAE1 --agentURLPattern "http://google.*" --authAs johndoe
--authDomain mydomain --authPassword secret
```

The following example updates the `Operations-Setting` setting to also redirect all URLs that contain the text `https://google.*` to the global application entitlement called `GAE1`.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme https --entitledApplication GAE1 --agentURLPattern "https://google.*" -authAs johndoe
--authDomain mydomain --authPassword secret
```

The following example updates the `Operations-Setting` setting to redirect all URLs that contain the text `"mailto://.*.mycompany.com"` to the global application entitlement called `GA2`.

```
vdmutil --updateURLSetting --urlSettingName Operations-Setting --urlRedirectionScope GLOBAL
--urlScheme mailto --entitledApplication GAE2 --agentURLPattern "mailto://.*.mycompany.com"
--authAs johndoe --authDomain mydomain --authPassword secret
```

What to do next

Assign the URL content redirection setting to a user or group. See Assign a URL Content Redirection Setting to a User or Group.

Assign a URL Content Redirection Setting to a User or Group

After you create a URL content redirection setting, you can assign it to an Active Directory user or group.

Prerequisites

Become familiar with `vdmutil` command-line interface options and requirements and verify that you have sufficient privileges to run the `vdmutil` command. See Using the vdmutil Command-Line Utility.

Procedure

- To assign a URL content redirection setting to a user, run the `vdmutil` command with the `--addUserURLSetting` option.

  ```
  vdmutil --addUserURLSetting --urlSettingName value --userName value
  ```

Option	Description
--urlSettingName	Name of the URL content redirection setting to assign.
--userName	Name of the Active Directory user in `domain\username` format.

- To assign a URL content redirection setting to a group, run the `vdmutil` command with the `--addGroupURLSetting` option.

```
vdmutil --addGroupURLSetting --urlSettingName value --groupName value
```

Option	Description
--urlSettingName	Name of the URL content redirection setting to assign.
--groupName	Name of the Active Directory group in `domain\group` format.

Example: Assigning a URL Content Redirection Setting

The following example assigns the URL content redirection setting called `url-filtering` to the user named `mydomain\janedoe`.

```
vdmutil --addUserURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --userName mydomain\janedoe
```

The following example assigns the URL content redirection setting called `url-filtering` to the group called `mydomain\usergroup`.

```
vdmutil --addGoupURLSetting --authAs johndoe --authDomain mydomain
--authPassword secret --urlSettingName url-filtering --groupName mydomain\usergroup
```

What to do next

Verify your URL content redirection settings. See Test a URL Content Redirection Setting.

Test a URL Content Redirection Setting

After you create and assign a URL content redirection setting, perform certain steps to verify that the setting is working properly.

Prerequisites

Become familiar with `vdmutil` command-line interface options and requirements and verify that you have sufficient privileges to run the the `vdmutil` command. See Using the vdmutil Command-Line Utility.

Procedure

1. Log in to the Connection Server instance.
2. Run the `vdmutil` command with the `--readURLSetting` option.

   For example:

```
vdmutil --readURLSetting --urlSettingName url-filtering --authAs johndoe
--authDomain mydomain --authPassword secret
```

The command displays detailed information about the URL content redirection setting. For example, the following command output for the `url-filtering` setting shows that HTTP and HTTPS URLs that contain the text `google.*` are redirected from the client to the local application pool named `iexplore2012`.

```
URL Redirection setting url-filtering
   Description                                    : null
   Enabled                                        : true
   Scope of URL Redirection Setting               : LOCAL
   URL Scheme And Local Resource handler pairs
      URL Scheme                                  : http
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
      URL Scheme                                  : https
      Handler type                                : APPLICATION
      Handler Resource name                       : iexplore2012
   AgentPatterns
        https://google.*
        http://google.*
   ClientPatterns
      No client patterns configured
```

3. On a Windows client machine, open Horizon Client, connect to the Connection Server instance, click URLs that match the URL patterns configured in the setting, and verify that the URLs are redirected as expected.
4. On the same Windows client machine, open the registry editor (`regedit`) and check the registry keys in the path `\Computer\HKEY_CURRENT_USER\Software\Vmware. Inc.\VMware VDM\URLRedirection\`.

   You should see a key for each protocol specified in the setting. You can click a protocol to see the rules associated with that protocol. For example, `agentRules` shows the URLs that are being redirected, `brokerHostName` shows the IP address or fully qualified host name of the Connection Server instance that is used when redirecting the URLs, and `remoteItem` shows the display name of the desktop or application pool that handles the redirected URLs.

Managing URL Content Redirection Settings

You can use `vdmutil` commands to manage your URL content redirection settings.

You must specify the `--authAs`, `--authDomain`, and `--authPassword` options with all commands. For more information, see Using the vdmutil Command-Line Utility.

Displaying Settings

Run the `vdmutil` command with the `--listURLSetting` option to list the names of all configured URL content redirection settings.

```
vdmutil --listURLSetting
```

Run the vdmutil command with the --readURLSetting to view detailed information about a particular URL content redirection setting.

```
vdmutil --readURLSetting --urlSettingName value
```

Deleting a Setting

Run the vdmutil command with the --deleteURLSetting option to delete a URL content redirection setting.

```
vdmutil --deleteURLSetting --urlSettingName value
```

Disabling and Enabling a Setting

Run the vdmutil command with the --disableURLSetting option to disable a URL content redirection setting.

```
vdmutil --disableURLSetting --urlSettingName value
```

Run the vdmutil with the --enableURLSetting option to enable a URL content redirection setting that was disabled.

```
vdmutil --enableURLSetting --urlSettingName value
```

Removing a User or Group From a Setting

Run the vdmutil command with the --removeUserURLSetting option to remove a user from a URL content redirection setting.

```
vdmutil --removeUserURLSetting --urlSettingName value --userName value
```

Run the vdmutil command with the --removeGroupURLSetting option to remove a group from a URL content redirection setting.

```
vdmutil --removeGroupURLSetting --urlSettingName value --userGroup value
```

Use the format domain\username or domain\groupname when specifying a user or group name.

Using Group Policy Settings to Configure Client-to-Agent Redirection

The URL Content Redirection ADMX template file (`urlRedirection.admx`) contains group policy settings that you can use to create rules that redirect URLs from the client to a remote desktop or application (client-to-agent redirection).

Note The preferred method for configuring client-to-agent redirection is to use the `vdmutil` command-line interface. Because GPOs are not supported by macOS, you cannot use GPOs to configure client-to-agent configuration if you have Mac clients.

To create a rule for client-to-agent redirection, you use the **remoteItem** option to specify the display name of a remote desktop or application pool and the **agentRules** option to specify the URLs that should be redirected to the remote desktop or application. You must also use the **brokerHostname** option to specify the IP address or fully qualified domain name of the Connection Server host to use when redirecting the URLs to a remote desktop or application.

For example, for security purposes you might want all HTTP URLs that point to the company network to be opened in a remote desktop or application. In this case, you might set the **agentRules** option to **`.*.mycompany.com`**.

For URL Content Redirection template file installation instructions, see Add the URL Content Redirection ADMX Template to a GPO.

URL Content Redirection Limitations

The behavior of the URL Content Redirection feature might have certain unexpected results.

- If the URL opens a country-specific page based on the locale, the source of the link determines the locale page that is opened. For example, if the remote desktop (agent source) resides in a data center in Japan and the user computer resides in the U.S., if the URL is redirected from the agent to the client machine, the page that opens on the U.S. client is the Japanese page.
- If users create favorites from Web pages, the favorites are created after redirection. For example, if a user clicks a link on the client machine and the URL is redirected to a remote desktop (agent), and the user creates a favorite for that page, the favorite is created on the agent. The next time the user opens the browser on the client machine, the user might expect to find the favorite on the client machine, but the favorite was stored on the remote desktop (agent source).
- Files that users download appear on the machine where the browser was used to open the URL, for example, when a user clicks a link on the client machine and the URL is redirected to a remote desktop. If the link downloaded a file, or if the link is for a Web page where the user downloads a file, the file is downloaded to the remote desktop rather than to the client machine.
- If you install Horizon Agent and Horizon Client on the same machine, you can enable URL Content Redirection in Horizon Agent or in Horizon Client, but not in both. On this machine, you can set up either client-to-agent redirection or agent-to-client redirection, but not both.

Unsupported URL Content Redirection Features

The URL Content Redirection feature does not work in certain circumstances.

Shortened URLs

Shortened URLs, such as `https://goo.gl/abc`, can be redirected based on filtering rules, but the filtering mechanism does not examine the original unshortened URL.

For example, if you have a rule that redirects URLs that contain `acme.com`, an original URL, such as `http://www.acme.com/some-really-long-path`, and a shortened URL of the original URL, such as `https://goo.gl/xyz`, the original URL is redirected, but the shortened URL is not redirected.

You can work around this limitation by creating rules to block or redirect URLs from the Web sites most often used for shortening URLs.

Embedded HTML Pages

Embedded HTML pages bypass URL redirection, for example, when a user goes to a URL that does not match a URL redirection rule. If a page contains an embedded HTML page (an iFrame or inline frame) that contains a URL that does match a redirection rule, the URL redirection rule does not work. The rule works only on the top-level URL.

Disabled Internet Explorer Plug-Ins

URL Content Redirection does not work in situations where Internet Explorer plug-ins are disabled, for example, when a user switches to InPrivate Browsing in Internet Explorer. People use private browsing so that Web pages and files downloaded from Web pages will not be logged in to the browsing and download history on their computer. This limitation occurs because the URL Redirection feature requires a certain Internet Explorer plug-in to be enabled, and private browsing disables these plug-ins.

You can work around this limitation by using the GPO setting to prevent users from disabling plug-ins. These settings include "Do not allow users to enable or disable add-ons" and "Automatically enable newly installed add-ons." In the Group Policy Management Editor, these settings are under **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer**.

To work around this limitation specifically for Internet Explorer, use the GPO setting to disable InPrivate mode. This setting is called "Turn off InPrivate Browsing." In the Group Policy Management Editor, these settings are under **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Privacy**.

These workarounds are best practices and can prevent issues with redirection that situations other than private browsing can cause.

Windows 10 Universal App Is the Default Handler for a Protocol

URL redirection does not work if a Windows 10 Universal app is the default handler for a protocol specified in a link. Universal applications are built on the Universal Windows Platform so that they can be downloaded to PCs, tablets, and phones, include the Microsoft Edge browser, Mail, Maps, Photos, Grove Music and others.

If you click a link for which one of these applications is the default handler, the URL is not redirected. For example, if a user clicks an email link in an application and the default email application is the Mail universal app, the URL specified in the link is not redirected.

You can work around this limitation by making a different application the default handler of the protocol of URLs that you want to redirect. For example, if Edge is the default browser, make Internet Explorer the default browser.

Secure Boot Enabled Machines

Machines that have secure boot enabled leave the URL Content Redirection feature disabled. URLs cannot be redirected from these machines. URLs can be redirected to these machines.

Using USB Devices with Remote Desktops and Applications

4

Administrators can configure the ability to use USB devices, such as thumb flash drives, cameras, VoIP (voice-over-IP) devices, and printers, from a remote desktop. This feature is called USB redirection, and it supports using the Blast Extreme, PCoIP, or Microsoft RDP display protocol. A remote desktop can accommodate up to 128 USB devices.

You can also redirect locally connected USB thumb flash drives and hard disks for use in RDS desktops and applications. Other types of USB devices, including other types of storage devices, are not supported in RDS desktops and applications.

When you use this feature in desktop pools that are deployed on single-user machines, most USB devices that are attached to the local client system become available in the remote desktop. You can even connect to and manage an iPad from a remote desktop. For example, you can sync your iPad with iTunes installed in your remote desktop. On some client devices, such as Windows and Mac computers, the USB devices are listed in a menu in Horizon Client. You use the menu to connect and disconnect the devices.

In most cases, you cannot use a USB device in your client system and in your remote desktop or application at the same time. Only a few types of USB devices can be shared between a remote desktop and the local computer. These devices include smart card readers and human interface devices such as keyboards and pointing devices.

Administrators can specify which types of USB devices end users are allowed to connect to. For composite devices that contain multiple types of devices, such as a video input device and a storage device, on some client systems, administrators can split the device so that one device (for example, the video input device) is allowed but the other device (for example, the storage device) is not.

The USB redirection feature is available only on some types of clients. To find out whether this feature is supported on a particular type of client, see the feature support matrix included in the "Using VMware Horizon Client" document for the specific type of desktop or mobile client device. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Important When you deploy the USB redirection feature, you can take steps to protect your organization from the security vulnerabilities that can affect USB devices. See Deploying USB Devices in a Secure Horizon 7 Environment.

This section includes the following topics:

Limitations Regarding USB Device Types

Although Horizon 7 does not explicitly prevent any devices from working in a remote desktop, due to factors such as network latency and bandwidth, some devices work better than others. By default, some devices are automatically filtered, or blocked, from being used.

In Horizon 6.0.1, together with Horizon Client 3.1 or later, you can plug USB 3.0 devices into USB 3.0 ports on the client machine, on Windows, Linux, and Mac clients. USB 3.0 devices are supported only with a single stream. Because multiple stream support is not implemented in this release, USB device performance is not enhanced. Some USB 3.0 devices that require a constant high throughput to function correctly might not work in a VDI session, due to network latency.

In earlier View releases, although super-speed USB 3.0 devices are not supported, USB 3.0 devices do often work when plugged into a USB 2.0 port on the client machine. However, there might be exceptions, depending on the type of USB chipset on the motherboard of the client system.

The following types of devices might not be suitable for USB redirection to a remote desktop that is deployed on a single-user machine:

- Due to the bandwidth requirements of webcams, which typically consume more than 60 Mbps of bandwidth, webcams are not supported through USB redirection. For webcams, you can use the Real-Time Audio-Video feature.
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle. If you have the Real-Time Audio-Video feature, audio input and output devices will work well using that feature, and you do not need to use USB redirection for those devices.
- USB CD/DVD burning is not supported.
- Performance of some USB devices varies greatly, depending on the network latency and reliability, especially over a WAN. For example, a single USB storage device read-request requires three round-trips between the client and the remote desktop. A read of a complete file might require multiple USB read operations, and the larger the latency, the longer the round-trip will take.

The file structure can be very large, depending on the format. Large USB disk drives can take several minutes to appear in the desktop. Formatting a USB device as NTFS rather than FAT helps to decrease the initial connection time. An unreliable network link causes retries, and performance is further reduced.

Similarly, USB CD/DVD readers, as well as scanners and touch devices such as signature tablets, do not work well over a latent network such as a WAN.

- The redirection of USB scanners depends on the state of the network, and scans might take longer than normal to complete.

You can redirect the following types of devices to a published desktop or application on an RDS host:

- USB thumb flash drives
- USB hard disks

Beginning with Horizon 7 version 7.0.2, you can redirect signature pads, dictation foot pedals, and some Wacom tablets to a published desktop or application. These devices are disabled by default in Horizon 7 version 7.0.2. To enable these devices, delete the Windows registry key settings `ExcludeAllDevices` and `IncludeFamily` from the following path: `HKLM\Software\Policies\VMware, Inc\VMware VDM\Agent\USB`. These devices are enabled by default in Horizon 7 version 7.0.3 and later.

You cannot redirect other types of USB devices, and other types of USB storage devices such as security storage drives and USB CD-ROM, to a published desktop or application.

Overview of Setting Up USB Redirection

To set up your deployment so that end users can connect removable devices, such as USB flash drives, cameras, and headsets, you must install certain components on both the remote desktop or RDS host and the client device, and you must verify that the global setting for USB devices is enabled in View Administrator.

This checklist includes both required and optional tasks for setting up USB redirection in your enterprise.

The USB redirection feature is available only on some types of clients, such as Windows, Mac, and partner-supplied Linux clients. To find out whether this feature is supported on a particular type of client, see the feature support matrix included in the "Using VMware Horizon Client" document for the specific type of client device. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Important When you deploy the USB redirection feature, you can take steps to protect your organization from the security vulnerabilities that can affect USB devices. For example, you can use group policy settings to disable USB redirection for some remote desktops and users, or to restrict which types of USB devices can be redirected. See Deploying USB Devices in a Secure Horizon 7 Environment.

1 When you run the Horizon Agent installation wizard on the remote desktop source or RDS host, be sure to include the USB Redirection component.

This component is deselected by default. You must select the component to install it.

2 When you run the VMware Horizon Client installation wizard on the client system, be sure to include the USB Redirection component.

   This component is included by default.

3 Verify that access to USB devices from a remote desktop or application is enabled in View Administrator.

   In View Administrator, go to **Policies > Global Policies** and verify that **USB access** is set to **Allow**.

4 (Optional) Configure Horizon Agent group policies to specify which types of devices are allowed to be redirected.

   See Using Policies to Control USB Redirection.

5 (Optional) Configure similar settings on the client device.

   You can also configure whether devices are automatically connected when Horizon Client connects to the remote desktop or application, or when the end user plugs in a USB device. The method of configuring USB settings on the client device depends on the type of device. For example, for Windows client endpoints, you can configure group policies, whereas for Mac endpoints, you use a command-line command. For instructions, see the "Using VMware Horizon Client" document for the specific type of client device.

6 Have end users connect to a remote desktop or application and plug their USB devices into the local client system.

   If the driver for the USB device is not already installed in the remote desktop or RDS host, the guest operating system detects the USB device and searches for a suitable driver, just as it would on a physical Windows computer.

Network Traffic and USB Redirection

USB redirection works independently of the display protocol and USB traffic usually uses TCP port 32111. Network traffic between a client system and a remote desktop or application can travel various routes, depending on whether the client system is inside the corporate network and how the administrator has chosen to set up security.

If the client system is inside the corporate network, so that a direct connection can be made between the client and remote desktop or application, USB traffic uses TCP port 32111.

If the client system is outside the corporate network, the client can connect through a Unified Access Gateway appliance or a security server in the DMZ. Unified Access Gateway appliances and security servers in the DMZ communicate with Connection Server instances inside the corporate firewall and provide an additional layer of security by shielding the Connection Server instances from the public-facing internet.

A Unified Access Gateway appliance (the preferred method) does not require opening additional ports on the firewall for USB traffic. A security server requires opening TCP port 32111 on the firewall for USB traffic. For complete security server port requirements, see "Firewall Rules for DMZ-Based Security Servers" in the *View Architecture Planning* document.

You can configure the USB over Session Enhancement SDK feature to avoid opening TCP port 32111. See Enabling the USB Over Session Enhancement SDK Feature.

Note If you are using a zero client, USB traffic is redirected using a PCoIP virtual channel, rather than through TCP port 32111. Data is encapsulated and encrypted by the PCoIP Secure Gateway using TCP/UDP port 4172. If you are using only zero clients, it is not necessary to open TCP port 32111.

Enabling the USB Over Session Enhancement SDK Feature

With the USB over Session Enhancement SDK feature you do not need to open TCP port 32111 for USB traffic. This feature is supported for both virtual desktops and published desktops on RDS hosts.

To enable the USB over Session Enhancement SDK feature, open the Windows Registry Editor (`regedit.exe`) on the remote desktop, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration`, and set the `UsbVirtualChannelEnabled` key to `true`.

When this feature is enabled, USB traffic might use the TCP or Blast Extreme Adaptive Transport (BEAT) connection that the display protocol uses, or it might use a dedicated TCP or BEAT connection. The connection that USB traffic uses depends on your configuration.

For example, with the VMware Blast display protocol, USB traffic might use the VMware Virtual Channel (VVC), the BEAT side channel, or the TCP side channel. With the PCoIP display protocol, USB traffic uses only the TCP side channel.

By default, the TCP side channel uses TCP port 9427. The VVC and the BEAT side channel use the same port as the VMware Blast display protocol.

USB counters displayed using PerfMon on Windows agents are valid if USB traffic is configured to use the VVC.

For information about using the BEAT side channel for USB traffic with VMware Blast, see Activate the BEAT Side Channel for USB or Client Drive Redirection.

Automatic Connections to USB Devices

On some client systems, administrators, end users, or both can configure automatic connections of USB devices to a remote desktop. Automatic connections can be made either when the user plugs a USB device in to the client system or when the client connects to the remote desktop.

Some devices, such as smart phones and tablets, require automatic connections because these devices are restarted, and therefore disconnected, during an upgrade. If these devices are not set to automatically reconnect to the remote desktop, during an upgrade, after the devices restart, they connect to the local client system instead.

Configuration properties for automatic USB connections that administrators set on the client, or that end users set by using a Horizon Client menu item, apply to all USB devices unless the devices are configured to be excluded from USB redirection. For example, in some client versions, webcams and microphones are excluded from USB redirection by default because these devices work better through

the Real-Time Audio-Video feature. In some cases, a USB device might not be excluded from redirection by default but might require administrators to explicitly exclude the device from redirection. For example, the following types of USB devices are not good candidates for USB redirection and must not be automatically connected to a remote desktop:

- USB Ethernet devices. If you redirect a USB Ethernet device, your client system might lose network connectivity if that device is the only Ethernet device.
- Touch screen devices. If you redirect a touch screen device, the remote desktop will receive touch input but not keyboard input.

If you have set the remote desktop to autoconnect USB devices, you can configure a policy to exclude specific devices such as touch screens and network devices. For more information, see Configuring Filter Policy Settings for USB Devices.

On Windows clients, as an alternative to using settings that automatically connect all but excluded devices, you can edit a configuration file on the client that sets Horizon Client to reconnect only a specific device or devices, such as smart phones and tablets, to the remote desktop. For instructions, see *Using VMware Horizon Client for Windows*.

Deploying USB Devices in a Secure Horizon 7 Environment

USB devices can be vulnerable to a security threat called BadUSB, in which the firmware on some USB devices can be hijacked and replaced with malware. For example, a device can be made to redirect network traffic or to emulate a keyboard and capture keystrokes. You can configure the USB redirection feature to protect your Horizon 7 deployment against this security vulnerability.

By disabling USB redirection, you can prevent any USB devices from being redirected to your users' Horizon 7 desktops and applications. Alternatively, you can disable redirection of specific USB devices, allowing users to have access only to specific devices on their desktops and applications.

The decision whether to take these steps depends on the security requirements in your organization. These steps are not mandatory. You can install USB redirection and leave the feature enabled for all USB devices in your Horizon 7 deployment. At a minimum, consider seriously the extent to which your organization should try to limit its exposure to this security vulnerability.

Disabling USB Redirection for All Types of Devices

Some highly secure environments require you to prevent all USB devices that users might have connected to their client devices from being redirected to their remote desktops and applications. You can disable USB redirection for all desktop pools, for specific desktop pools, or for specific users in a desktop pool.

Use any of the following strategies, as appropriate for your situation:

- When you install Horizon Agent on a desktop image or RDS host, deselect the **USB redirection** setup option. (The option is deselected by default.) This approach prevents access to USB devices on all remote desktops and applications that are deployed from the desktop image or RDS host.

- In Horizon Administrator, edit the **USB access** policy for a specific pool to either deny or allow access. With this approach, you do not have to change the desktop image and can control access to USB devices in specific desktop and application pools.

  Only the global **USB access** policy is available for RDS desktop and application pools. You cannot set this policy for individual RDS desktop or application pools.
- In View Administrator, after you set the policy at the desktop or application pool level, you can override the policy for a specific user in the pool by selecting the **User Overrides** setting and selecting a user.
- Set the `Exclude All Devices` policy to **`true`**, on the Horizon Agent side or on the client side, as appropriate.
- Use Smart Policies to create a policy that disables the **USB redirection** Horizon Policy setting. With this approach, you can disable USB redirection on a specific remote desktop if certain conditions are met. For example, you can configure a policy that disables USB redirection when users connect to a remote desktop from outside your corporate network.

If you set the `Exclude All Devices` policy to **`true`**, Horizon Client prevents all USB devices from being redirected. You can use other policy settings to allow specific devices or families of devices to be redirected. If you set the policy to **`false`**, Horizon Client allows all USB devices to be redirected except those that are blocked by other policy settings. You can set the policy on both Horizon Agent and Horizon Client. The following table shows how the `Exclude All Devices` policy that you can set for Horizon Agent and Horizon Client combine to produce an effective policy for the client computer. By default, all USB devices are allowed to be redirected unless otherwise blocked.

Table 4-1. Effect of Combining Exclude All Devices Policies

Exclude All Devices Policy on Horizon Agent	Exclude All Devices Policy on Horizon Client	Combined Effective Exclude All Devices Policy
`false` or not defined (include all USB devices)	**`false`** or not defined (include all USB devices)	Include all USB devices
`false` (include all USB devices)	**`true`** (exclude all USB devices)	Exclude all USB devices
`true` (exclude all USB devices)	Any or not defined	Exclude all USB devices

If you have set `Disable Remote Configuration Download` policy to **`true`**, the value of `Exclude All Devices` on Horizon Agent is not passed to Horizon Client, but Horizon Agent and Horizon Client enforce the local value of `Exclude All Devices`.

These policies are included in the Horizon Agent Configuration ADMX template file (`vdm_agent.admx`).

Disabling USB Redirection for Specific Devices

Some users might have to redirect specific locally-connected USB devices so that they can perform tasks on their remote desktops or applications. For example, a doctor might have to use a Dictaphone USB device to record patients' medical information. In these cases, you cannot disable access to all USB devices. You can use group policy settings to enable or disable USB redirection for specific devices.

Before you enable USB redirection for specific devices, make sure that you trust the physical devices that are connected to client machines in your enterprise. Be sure that you can trust your supply chain. If possible, keep track of a chain of custody for the USB devices.

In addition, educate your employees to ensure that they do not connect devices from unknown sources. If possible, restrict the devices in your environment to those that accept only signed firmware updates, are FIPS 140-2 Level 3-certified, and do not support any kind of field-updatable firmware. These types of USB devices are hard to source and, depending on your device requirements, might be impossible to find. These choices might not be practical, but they are worth considering.

Each USB device has its own vendor and product ID that identifies it to the computer. By configuring Horizon Agent Configuration group policy settings, you can set an include policy for known device types. With this approach, you remove the risk of allowing unknown devices to be inserted into your environment.

For example, you can prevent all devices except a known device vendor and product ID, `vid/pid=0123/abcd`, from being redirected to the remote desktop or application:

```
ExcludeAllDevices   Enabled

IncludeVidPid       o:vid-0123_pid-abcd
```

Note This example configuration provides protection, but a compromised device can report any vid/pid, so a possible attack could still occur.

By default, Horizon 7 blocks certain device families from being redirected to the remote desktop or application. For example, HID (human interface devices) and keyboards are blocked from appearing in the guest. Some released BadUSB code targets USB keyboard devices.

You can prevent specific device families from being redirected to the remote desktop or application. For example, you can block all video, audio, and mass storage devices:

```
ExcludeDeviceFamily   o:video;audio;storage
```

Conversely, you can create a whitelist by preventing all devices from being redirected but allowing a specific device family to be used. For example, you can block all devices except storage devices:

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

Another risk can arise when a remote user logs into a desktop or application and infects it. You can prevent USB access to any Horizon 7 connections that originate from outside the company firewall. The USB device can be used internally but not externally.

Be aware that if you block TCP port 32111 to disable external access to USB devices, time zone synchronization will not work because port 32111 is also used for time zone synchronization. For zero clients, the USB traffic is embedded inside a virtual channel on UDP port 4172. Because port 4172 is used for the display protocol as well as for USB redirection, you cannot block port 4172. If required, you can disable USB redirection on zero clients. For details, see the zero client product literature or contact the zero client vendor.

Setting policies to block certain device families or specific devices can help to mitigate the risk of being infected with BadUSB malware. These policies do not mitigate all risk, but they can be an effective part of an overall security strategy.

Using Log Files for Troubleshooting and to Determine USB Device IDs

Useful log files for USB are located on both the client system and the remote desktop operating system or RDS host. Use the log files in both locations for troubleshooting. To find product IDs for specific devices, use the client-side logs.

If you are trying to configure USB device splitting or filtering, or if you are trying to determine why a particular device does not appear in a Horizon Client menu, look in the client-side logs. Client logs are produced for the USB arbitrator and the Horizon View USB Service. Logging on Windows and Linux clients is enabled by default. On Mac clients, logging is disabled by default. To enable logging on Mac clients, see the *Using VMware Horizon Client for Mac* document.

When you configure policies for splitting and filtering out USB devices, some values you set require the VID (vendor ID) and PID (product ID) for the USB device. To find the VID and PID, you can search on the Internet for the product name combined with `vid` and `pid`. Alternatively, you can look in the client-side log file after you plug in the USB device to the local system when Horizon Client is running. The following table shows the default location of the log files.

Table 4-2. Log File Locations

Client or Agent	Path to Log Files
Windows client	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt` `C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log`
Horizon Agent	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt`
Mac client	`/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log` `/Library/Logs/VMware/vmware-usbarbitrator-xxxx.log`
Linux client	(Default location) `/tmp/vmware-root/vmware-view-usbd-*.log`

If a problem with the device occurs after the device is redirected to the remote desktop or application, examine both the client- and agent-side logs.

Using Policies to Control USB Redirection

You can configure USB policies for both the remote desktop or application (Horizon Agent) and Horizon Client. These policies specify whether the client device should split composite USB devices into separate components for redirection. You can split devices to restrict the types of USB devices that the client makes available for redirection, and to make Horizon Agent prevent certain USB devices from being forwarded from a client computer.

If you have older versions of Horizon Agent or Horizon Client installed, not all the features of the USB redirection policies are available. Table 4-3 shows how Horizon 7 applies the policies for different combinations of Horizon Agent and Horizon Client.

Table 4-3. Compatibility of USB Policy Settings

Horizon Agent Version	Horizon Client Version	Effect of USB Policy Settings on USB Redirection
5.1 or later	5.1 or later	USB policy settings are applicable to both Horizon Agent and Horizon Client. You can use Horizon Agent USB policy settings to block USB devices from being forwarded to a desktop. Horizon Agent can send device splitting and filtering policy settings to Horizon Client. You can use Horizon Client USB policy settings to prevent USB devices from being redirected from a client computer to a desktop. **Note** In View Agent 6.1 or later and Horizon Client 3.3 or later, these USB redirection policy settings apply to RDS desktops and applications as well as to remote desktops that run on single-user machines.
5.1 or later	5.0.x or earlier	USB policy settings apply only to Horizon Agent. You can use Horizon Agent USB policy settings to block USB devices from being forwarded to a desktop. You cannot use Horizon Client USB policy settings to control which devices can be redirected from a client computer to a desktop. Horizon Client cannot receive device splitting and filtering policy settings from Horizon Agent. Existing registry settings for USB redirection by Horizon Client remain valid.
5.0.x or earlier	5.1 or later	USB policy settings apply only to Horizon Client. You can use Horizon Client USB policy settings to prevent USB devices from being redirected from a client computer to a desktop. You cannot use Horizon Agent USB policy settings to block USB devices from being forwarded to a desktop. Horizon Agent cannot send device splitting and filtering policy settings to Horizon Client.
5.0.x or earlier	5.0.x or earlier	USB policy settings do not apply. Existing registry settings for USB redirection by Horizon Client remain valid.

If you upgrade Horizon Client, any existing registry settings for USB redirection, such as `HardwareIdFilters`, remain valid until you define USB policies for Horizon Client.

On client devices that do not support client-side USB policies, you can use the USB policies for Horizon Agent to control which USB devices are allowed to be forwarded from the client to a desktop or application.

Configuring Device Splitting Policy Settings for Composite USB Devices

Composite USB devices consist of a combination of two or more different devices, such as a video input device and a storage device or a microphone and a mouse device. If you want to allow one or more of the components to be available for redirection, you can split the composite device into its component interfaces, exclude certain interfaces from redirection and include others.

You can set a policy that automatically splits composite devices. If automatic device splitting does not work for a specific device, or if automatic splitting does not produce the results your application requires, you can split composite devices manually.

Automatic Device Splitting

If you enable automatic device splitting Horizon 7 attempts to split the functions, or devices, in a composite device according to the filter rules that are in effect. For example, a dictation microphone might be split automatically so that the mouse device remains local to the client, but the rest of the devices are forwarded to the remote desktop.

The following table shows how the value of the `Allow Auto Device Splitting` setting determines whether Horizon Client attempts to split composite USB devices automatically. By default, automatic splitting is disabled.

Table 4-4. Effect of Combining Disable Automatic Splitting Policies

Allow Auto Device Splitting Policy on Horizon Agent	Allow Auto Device Splitting Policy on Horizon Client	Combined Effective Allow Auto Device Splitting Policy
`Allow – Default Client Setting`	**`false`** (automatic splitting disabled)	Automatic splitting disabled
`Allow – Default Client Setting`	**`true`** (automatic splitting enabled)	Automatic splitting enabled
`Allow – Default Client Setting`	Not defined	Automatic splitting enabled
`Allow – Override Client Setting`	Any or not defined	Automatic splitting enabled
Not defined	Not defined	Automatic splitting disabled

Note These policies are included in the Horizon Agent Configuration ADMX template file. The ADMX template file is named (`vdm_agent.admx`).

By default, Horizon 7 disables automatic splitting, and excludes any audio-output, keyboard, mouse, or smart-card components of a composite USB device from redirection.

Horizon 7 applies the device splitting policy settings before it applies any filter policy settings. If you have enabled automatic splitting and do not explicitly exclude a composite USB device from being split by specifying its vendor and product IDs, Horizon 7 examines each interface of the composite USB device to decide which interfaces should be excluded or included according to the filter policy settings. If you have disabled automatic device splitting and do not explicitly specify the vendor and product IDs of a composite USB device that you want to split, Horizon 7 applies the filter policy settings to the entire device.

If you enable automatic splitting, you can use the `Exclude Vid/Pid Device From Split` policy to specify the composite USB devices that you want to exclude from splitting.

Manual Device Splitting

You can use the `Split Vid/Pid Device` policy to specify the vendor and product IDs of a composite USB device that you want to split. You can also specify the interfaces of the components of a composite USB device that you want to exclude from redirection. Horizon 7 does not apply any filter policy settings to components that you exclude in this way.

Important If you use the `Split Vid/Pid Device` policy, Horizon 7 does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as `Include Vid/Pid Device` to include those components.

Table 4-5 shows the modifiers that specify how Horizon Client handles a Horizon Agent device splitting policy setting if there is an equivalent device splitting policy setting for Horizon Client. These modifiers apply to all device-splitting policy settings.

Table 4-5. Splitting Modifiers for Device-Splitting Policy Settings on Horizon Agent

Modifier	Description
m (merge)	Horizon Client applies the Horizon Agent device splitting policy setting in addition to the Horizon Client device splitting policy setting.
o (override)	Horizon Client uses the Horizon Agent device splitting policy setting instead of the Horizon Client device splitting policy setting.

Table 4-6 shows examples of how Horizon Client processes the settings for `Exclude Device From Split by Vendor/Product ID` when you specify different splitting modifiers.

Table 4-6. Examples of Applying Splitting Modifiers to Device-Splitting Policy Settings

Exclude Device From Split by Vendor/Product ID on Horizon Agent	Exclude Device From Split by Vendor/Product ID on Horizon Client	Effective Exclude Device From Split by Vendor/Product ID Policy Setting Used by Horizon Client
`m:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX`
`m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`
`o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`	`vid-YYYY_pid-YYYY`	`vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY`

Horizon Agent does not apply the device splitting policy settings on its side of the connection.

Horizon Client evaluates the device splitting policy settings in the following order of precedence.

- `Exclude Vid/Pid Device From Split`
- `Split Vid/Pid Device`

A device splitting policy setting that excludes a device from being split takes precedence over any policy setting to split the device. If you define any interfaces or devices to be excluded from splitting, Horizon Client excludes the matching component devices from being available for redirection.

Examples of Setting Policies to Split Composite USB Devices

Set splitting policies for desktops to exclude devices with specific vendor and product IDs from redirection after automatic splitting and pass these policies to client computers:

- For Horizon Agent, set the `Allow Auto Device Splitting` policy to `Allow – Override Client Setting`.
- For Horizon Agent, se the `Exclude VidPid From Split` policy to **`o:vid-`*`xxx`*`_pid-`*`yyyy`***, where *xxx* and *yyyy* are the appropriate IDs.

Allow automatic device splitting for desktops and specify policies for splitting specific devices on client computers:

- For Horizon Agent, set the `Allow Auto Device Splitting` policy to `Allow – Override Client Setting`.
- For the client device, set the `Include Vid/Pid Device` filter policy to include the specific device that you want to split; for example, **`vid-0781_pid-554c`**.
- For the client device, set the `Split Vid/Pid Device` policy to **`vid-0781_pid-554c(exintf:00;exintf:01)`** for example, to split a specified composite USB device so that interface 00 and interface 01 are excluded from redirection.

Configuring Filter Policy Settings for USB Devices

Filter policy settings that you configure for Horizon Agent and Horizon Client establish which USB devices can be redirected from a client computer to a remote desktop or application. USB device filtering is often used by companies to disable the use of mass storage devices on remote desktops, or to block a specific type of device from being forwarded, such as a USB-to-Ethernet adapter that connects the client device to the remote desktop.

When you connect to a desktop or application, Horizon Client downloads the Horizon Agent USB policy settings and uses them in conjunction with the Horizon Client USB policy settings to decide which USB devices it will allow you to redirect from the client computer.

Horizon 7 applies any device splitting policy settings before it applies the filter policy settings. If you have split a composite USB device, Horizon 7 examines each of the device's interfaces to decide which should be excluded or included according to the filter policy settings. If you have not split a composite USB device, Horizon 7 applies the filter policy settings to the entire device.

The device splitting policies are included in the Horizon Agent Configuration ADMX template file (`vdm_agent.admx`).

Interaction of Agent-Enforced USB Settings

The following table shows the modifiers that specify how Horizon Client handles a Horizon Agent filter policy setting for an agent-enforceable setting if an equivalent filter policy setting exists for Horizon Client.

Table 4-7. Filter Modifiers for Agent-Enforceable Settings

Modifier	Description
`m` (merge)	Horizon Client applies the Horizon Agent filter policy setting in addition to the Horizon Client filter policy setting. In the case of Boolean, or true/false, settings, if the client policy is not set, the agent settings are used. If the client policy is set, the agent settings are ignored, except for the `Exclude All Devices` setting. If the `Exclude All Devices` policy is set on the agent side, the policy overrides the client setting.
`o` (override)	Horizon Client uses the Horizon Agent filter policy setting instead of the Horizon Client filter policy setting.

For example, the following policy on the agent side overrides any include rules on the client side, and only device VID-0911_PID-149a will have an include rule applied:

```
IncludeVidPid: o:VID-0911_PID-149a
```

You can also use asterisks as wildcard characters; for example: **`o:vid-0911_pid-****`**

Important If you configure the agent side without the **`o`** or **`m`** modifier, the configuration rule is considered invalid and will be ignored.

Interaction of Client-Interpreted USB Settings

The following table shows the modifiers that specify how Horizon Client handles a Horizon Agent filter policy setting for a client-interpreted setting.

Table 4-8. Filter Modifiers for Client-Interpreted Settings

Modifier	Description
`Default` (**`d`** in the registry setting)	If a Horizon Client filter policy setting does not exist, Horizon Client uses the Horizon Agent filter policy setting. If a Horizon Client filter policy setting exists, Horizon Client applies that policy setting and ignores the Horizon Agent filter policy setting.
`Override` (**`o`** in the registry setting)	Horizon Client uses the Horizon Agent filter policy setting instead of any equivalent Horizon Client filter policy setting.

Horizon Agent does not apply the filter policy settings for client-interpreted settings on its side of the connection.

The following table shows examples of how Horizon Client processes the settings for `Allow Smart Cards` when you specify different filter modifiers.

Table 4-9. Examples of Applying Filter Modifiers to Client-Interpreted Settings

Allow Smart Cards Setting on Horizon Agent	Allow Smart Cards Setting on Horizon Client	Effective Allow Smart Cards Policy Setting Used by Horizon Client
`Disable – Default Client Setting` (**`d:false`** in the registry setting)	**`true`** (Allow)	**`true`** (Allow)
`Disable – Override Client Setting` (**`o:false`** in the registry setting)	**`true`** (Allow)	**`false`** (Disable)

If you set the `Disable Remote Configuration Download` policy to **`true`**, Horizon Client ignores any filter policy settings that it receives from Horizon Agent.

Horizon Agent always applies the filter policy settings in agent-enforceable settings on its side of the connection even if you configure Horizon Client to use a different filter policy setting or disable Horizon Client from downloading filter policy settings from Horizon Agent. Horizon Client does not report that Horizon Agent is blocking a device from being forwarded.

Precedence of Settings

Horizon Client evaluates the filter policy settings according to an order of precedence. A filter policy setting that excludes a matching device from being redirected takes precedence over the equivalent filter policy setting that includes the device. If Horizon Client does not encounter a filter policy setting to exclude a device, Horizon Client allows the device to be redirected unless you have set the `Exclude All Devices` policy to **`true`**. However, if you have configured a filter policy setting on Horizon Agent to exclude the device, the desktop or application blocks any attempt to redirect the device to it.

Horizon Client evaluates the filter policy settings in order of precedence, taking into account the Horizon Client settings and the Horizon Agent settings together with the modifier values that you apply to the Horizon Agent settings. The following list shows the order of precedence, with item 1 having the highest precedence.

1 `Exclude Path`

2 `Include Path`

3 `Exclude Vid/Pid Device`

4 `Include Vid/Pid Device`

5 `Exclude Device Family`

6 `Include Device Family`

7 `Allow Audio Input Devices`, `Allow Audio Output Devices`, `Allow HIDBootable`, `Allow HID (Non Bootable and Not Mouse Keyboard)`, `Allow Keyboard and Mouse Devices`, `Allow Smart Cards`, and `Allow Video Devices`

8 Combined effective `Exclude All Devices` policy evaluated to exclude or include all USB devices

You can set `Exclude Path` and `Include Path` filter policy settings only for Horizon Client. The `Allow` filter policy settings that refer to separate device families have equal precedence.

If you configure a policy setting to exclude devices based on vendor and product ID values, Horizon Client excludes a device whose vendor and product ID values match this policy setting even though you might have configured an `Allow` policy setting for the family to which the device belongs.

The order of precedence for policy settings resolves conflicts between policy settings. If you configure `Allow Smart Cards` to allow the redirection of smart cards, any higher precedence exclusion policy setting overrides this policy. For example, you might have configured an `Exclude Vid/Pid Device` policy setting to exclude smart-card devices with matching path or vendor and product ID values, or you might have configured an `Exclude Device Family` policy setting that also excludes the `smart-card` device family entirely.

If you have configured any Horizon Agent filter policy settings, Horizon Agent evaluates and enforces the filter policy settings in the following order of precedence on the remote desktop or application, with item 1 having the highest precedence.

1 `Exclude Vid/Pid Device`

2 `Include Vid/Pid Device`

3 `Exclude Device Family`

4 `Include Device Family`

5 Agent-enforced `Exclude All Devices` policy set to exclude or include all USB devices

Horizon Agent enforces this limited set of filter policy settings on its side of the connection.

By defining filter policy settings for Horizon Agent, you can create a filtering policy for non-managed client computers. The feature also allows you to block devices from being forwarded from client computers, even if the filter policy settings for Horizon Client permit the redirection.

For example, if you configure a policy that permits Horizon Client to allow a device to be redirected, Horizon Agent blocks the device if you configure a policy for Horizon Agent to exclude the device.

Examples of Setting Policies to Filter USB Devices

The vendor IDs and product IDs used in these examples are examples only. For information about determining the vendor ID and product ID for a specify device, see Using Log Files for Troubleshooting and to Determine USB Device IDs.

- On the client, exclude a particular device from being redirected:

```
Exclude Vid/Pid Device:     Vid-0341_Pid-1a11
```

- Block all storage devices from being redirected to this desktop or application pool. Use an agent-side setting:

```
Exclude Device Family:      o:storage
```

- For all users in a desktop pool, block audio and video devices to ensure that these devices will always be available for the Real-Time Audio-Video feature. Use an agent-side setting::

  ```
  Exclude Device Family:      o:video;audio
  ```

  Note that another strategy would be to exclude specific devices by vendor and product ID.

- On the client, block all devices from being redirected except one particular device:

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd
  ```

- Exclude all devices made by a particular company because these devices cause problems for your end users. Use an agent-side setting:

  ```
  Exclude Vid/Pid Device:     o:Vid-0341_Pid-*
  ```

- On the client, include two specific devices but exclude all others:

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
  ```

USB Device Families

You can specify a family when you are creating USB filtering rules for Horizon Client, or View Agent or Horizon Agent.

Note Some devices do not report a device family.

Table 4-10. USB Device Families

Device Family Name	Description
audio	Any audio-input or audio-output device.
audio-in	Audio-input devices such as microphones.
audio-out	Audio-output devices such as loudspeakers and headphones.
bluetooth	Bluetooth-connected devices.
comm	Communications devices such as modems and wired networking adapters.
hid	Human interface devices excluding keyboards and pointing devices.
hid-bootable	Human interface devices that are available at boot time excluding keyboards and pointing devices.
imaging	Imaging devices such as scanners.
keyboard	Keyboard device.
mouse	Pointing device such as a mouse.
other	Family not specified.
pda	Personal digital assistants.

Table 4-10. USB Device Families (Continued)

Device Family Name	Description
physical	Force feedback devices such as force feedback joysticks.
printer	Printing devices.
security	Security devices such as fingerprint readers.
smart-card	Smart-card devices.
storage	Mass storage devices such as flash drives and external hard disk drives.
unknown	Family not known.
vendor	Devices with vendor-specific functions.
video	Video-input devices.
wireless	Wireless networking adapters.
wusb	Wireless USB devices.

USB Settings in the Horizon Agent Configuration ADMX Template

You can define USB policy settings for both Horizon Agent and Horizon Client. On connection, Horizon Client downloads the USB policy settings from Horizon Agent and uses them in conjunction with the Horizon Client USB policy settings to decide which devices it will allow to be available for redirection from the client computer.

The Horizon Agent Configuration ADMX template file contains policy settings related to the authentication and environmental components of Horizon Agent, including USB redirection. The ADMX template file is named (`vdm_agent.admx`). The settings apply at the computer level. Horizon Agent preferentially reads the settings from the GPO at the computer level, and otherwise from the registry at `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB`

Settings for Configuring USB Device Splitting

The following table describes each policy setting for splitting composite USB devices in the Horizon Agent Configuration ADMX template file. All of these settings are in the **VMware Horizon Agent Configuration > View USB Configuration > Client Downloadable only Settings** folder in the Group Policy Management Editor. Horizon Agent does not enforce these settings. Horizon Agent passes the settings to Horizon Client for interpretation and enforcement according to whether you specify the merge (`m`) or override (`o`) modifier. Horizon Client uses the settings to decide whether to split composite USB devices into their component devices, and whether to exclude the component devices from being available for redirection. For a description of how Horizon applies the policies for splitting composite USB devices, see Configuring Device Splitting Policy Settings for Composite USB Devices.

Table 4-11. Horizon Agent Configuration Template: Device-Splitting Settings

Setting	Properties
`Allow Auto Device Splitting` Property: `AllowAutoDeviceSplitting`	Allows the automatic splitting of composite USB devices. The default value is undefined, which equates to **`false`**.
`Exclude Vid/Pid Device from Split` Property: `SplitExcludeVidPid`	Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is {`m`|`o`}`:vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: **`o:vid-0781_pid-55**`** The default value is undefined.
`Split Vid/Pid Device` Property: `SplitVidPid`	Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is {`m`|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*]) or {`m`|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*]) You can use the `exintf` keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: **`o:vid-0781_pid-554c(exintf:01;exintf:02)`** **Note** Horizon 7 does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as `Include Vid/Pid Device` to include those components. The default value is undefined.

Horizon Agent -Enforced USB Settings

The following table describes each agent-enforced policy setting for USB in the Horizon Agent Configuration ADMX template file. All of these settings are in the **VMware Horizon Agent Configuration > View USB Configuration** folder in the Group Policy Management Editor. Horizon Agent uses the settings to decide if a USB device can be forwarded to the host machine. Horizon Agent also passes the settings to Horizon Client for interpretation and enforcement according to whether you specify the merge (`m`) or override (`o`) modifier. Horizon Client uses the settings to decide if a USB device is available for redirection. As Horizon Agent always enforces an agent-enforced policy setting that you specify, the effect might be to counteract the policy that you have set for Horizon Client. For a description of how Horizon 7 applies the policies for filtering USB devices, see Configuring Filter Policy Settings for USB Devices.

Table 4-12. Horizon Agent Configuration Template: Agent-Enforced Settings

Setting	Properties
`Exclude All Devices` Property: `ExcludeAllDevices`	Excludes all USB devices from being forwarded. If set to **`true`**, you can use other policy settings to allow specific devices or families of devices to be forwarded. If set to **`false`**, you can use other policy settings to prevent specific devices or families of devices from being forwarded. If set to **`true`** and passed to Horizon Client, this setting always overrides the setting on Horizon Client. You cannot use the merge (`m`) or override (`o`) modifier with this setting. The default value is undefined, which equates to **`false`**.
`Exclude Device Family` Property: `ExcludeFamily`	Excludes families of devices from being forwarded. The format of the setting is {`m`|`o`}`:`*`family_name_1`*[`;`*`family_name_2`*]... For example: **`o:bluetooth;smart-card`** If you have enabled automatic device splitting, Horizon 7 examines the device family of each interface of a composite USB device to decide which interfaces should be excluded. If you have disabled automatic device splitting, Horizon 7 examines the device family of the whole composite USB device. The default value is undefined.
`Exclude Vid/Pid Device` Property: `ExcludeVidPid`	Excludes devices with specified vendor and product IDs from being forwarded. The format of the setting is {`m`|`o`}`:vid-`*`xxx1`*`_pid-`*`yyy2`*[`;vid-`*`xxx2`*`_pid-`*`yyy2`*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: **`m:vid-0781_pid-****;vid-0561_pid-554c`** The default value is undefined.
`Include Device Family` Property: `IncludeFamily`	Includes families of devices that can be forwarded. The format of the setting is {`m`|`o`}`:`*`family_name_1`*[`;`*`family_name_2`*]... For example: **`m:storage`** The default value is undefined.
`Include Vid/Pid Device` Property: `IncludeVidPid`	Includes devices with specified vendor and product IDs that can be forwarded. The format of the setting is {`m`|`o`}`:vid-`*`xxx1`*`_pid-`*`yyy2`*[`;vid-`*`xxx2`*`_pid-`*`yyy2`*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: **`o:vid-0561_pid-554c`** The default value is undefined.

Client-Interpreted USB Settings

The following table describes each client-interpreted policy setting in the Horizon Agent Configuration ADMX template file. All of these settings are in the **VMware Horizon Agent Configuration > View USB Configuration > Client Downloadable only Settings** folder in the Group Policy Management Editor. Horizon Agent does not enforce these settings. Horizon Agent passes the settings to Horizon Client for interpretation and enforcement. Horizon Client uses the settings to decide if a USB device is available for redirection.

Table 4-13. Horizon Agent Configuration Template: Client-Interpreted Settings

Setting	Properties
`Allow Audio Input Devices` Property: `AllowAudioIn`	Allows audio input devices to be forwarded. The default value is undefined, which equates to **`true`**.
`Allow Audio Output Devices` Property: `AllowAudioOut`	Allows audio output devices to be forwarded. The default value is undefined, which equates to **`false`**.
`Allow HID-Bootable` Property: `AllowHIDBootable`	Allows input devices other than keyboards or mice that are available at boot time (also known as hid-bootable devices) to be forwarded. The default value is undefined, which equates to **`true`**.
`Allow Other Input Devices`	Allows input devices other than hid-bootable devices or keyboards with integrated pointing devices to be forwarded. The default value is undefined.
`Allow Keyboard and Mouse Devices` Property: `AllowKeyboardMouse`	Allows keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad) to be forwarded. The default value is undefined, which equates to **`false`**.
`Allow Smart Cards` Property: `AllowSmartcard`	Allows smart-card devices to be forwarded. The default value is undefined, which equates to **`false`**.
`Allow Video Devices` Property: `AllowVideo`	Allows video devices to be forwarded. The default value is undefined, which equates to **`true`**.

Troubleshooting USB Redirection Problems

Various problems can arise with USB redirection in Horizon Client.

Problem

USB redirection in Horizon Client fails to make local devices available on the remote desktop, or some devices do not appear to be available for redirection in Horizon Client.

Cause

The following are possible causes for USB redirection failing to function correctly or as expected.

- The device is a composite USB device and one of the devices it includes is blocked by default. For example, a dictation device that includes a mouse is blocked by default because mouse devices are blocked by default. To work around this problem, see "Configuring Device Splitting Policy Settings for Composite USB Devices" in the *Configuring Remote Desktop Features in Horizon 7* document.
- USB redirection is not supported on Windows Server 2008 RDS hosts that deploy remote desktops and applications. USB redirection is supported on Windows Server 2012 RDS hosts with View Agent 6.1 and later, but only for USB storage devices. USB redirection is supported on Windows Server 2008 R2 and Windows Server 2012 R2 systems that are used as single-user desktops.
- Only USB flash drives and hard disks are supported on RDS desktops and applications. You cannot redirect other types of USB devices, and other types of USB storage devices such as security storage drives and USB CD-ROM, to an RDS desktop or application.

- Webcams are not supported for redirection.
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle.
- USB redirection is not supported for boot devices. If you run Horizon Client on a Windows system that boots from a USB device, and you redirect this device to the remote desktop, the local operating system might become unresponsive or unusable. See http://kb.vmware.com/kb/1021409.
- By default, Horizon Client for Windows does not allow you to select keyboard, mouse, smart card and audio-out devices for redirection. See http://kb.vmware.com/kb/1011600.
- RDP does not support the redirection of USB HIDs for the console session, or of smart card readers. See http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center can prevent the redirection of USB devices for RDP sessions. See http://kb.vmware.com/kb/1019205.
- For some USB HIDs, you must configure the virtual machine to update the position of the mouse pointer. See http://kb.vmware.com/kb/1022076.
- Some audio devices might require changes to policy settings or to registry settings. See http://kb.vmware.com/kb/1023868.
- Network latency can cause slow device interaction or cause applications to appear frozen because they are designed to interact with local devices. Very large USB disk drives might take several minutes to appear in Windows Explorer.
- USB flash cards formatted with the FAT32 file system are slow to load. See http://kb.vmware.com/kb/1022836.
- A process or service on the local system opened the device before you connected to the remote desktop or application.
- A redirected USB device stops working if you reconnect a desktop or application session even if the desktop or application shows that the device is available.
- USB redirection is disabled in Horizon Administrator.
- Missing or disabled USB redirection drivers on the guest.

Solution

- If available, use PCoIP instead of RDP as the protocol.
- If a redirected device remains unavailable or stops working after a temporary disconnection, remove the device, plug it in again, and retry the redirection.
- In Horizon Administrator, go to **Policies > Global Policies**, and verify that USB access is set to **Allow** under View Policies.

- Examine the log on the guest for entries of class `ws_vhub`, and the log on the client for entries of class `vmware-view-usbd`.

  Entries with these classes are written to the logs if a user is not an administrator, or if the USB redirection drivers are not installed or are not working. For the location of these log files, see "Using Log Files for Troubleshooting and to Determine USB Device IDs" in the *Configuring Remote Desktop Features in Horizon 7* document.

- Open the Device Manager on the guest, expand Universal Serial Bus controllers, and reinstall the VMware View Virtual USB Host Controller and VMware View Virtual USB Hub drivers if these drivers are missing or re-enable them if they are disabled.

Configuring Policies for Desktop and Application Pools 5

You can configure policies to control the behavior of desktop and application pools, machines, and users. You use Horizon Administrator to set policies for client sessions. You can use Active Directory group policy settings to control the behavior of Horizon Agent, Horizon Client for Windows, and features that affect single-user machines, RDS hosts, PCoIP, or VMware Blast.

This section includes the following topics:

Setting Policies in Horizon Administrator

You use Horizon Administrator to configure policies for client sessions.

You can set these policies to affect specific users, specific desktop pools, or all client sessions users. Policies that affect specific users and desktop pools are called user-level policies and desktop pool-level policies. Policies that affect all sessions and users are called global policies.

User-level policies inherit settings from the equivalent desktop pool-level policy settings. Similarly, desktop pool-level policies inherit settings from the equivalent global policy settings. A desktop pool-level policy setting takes precedence over the equivalent global policy setting. A user-level policy setting takes precedence over the equivalent global and desktop pool-level policy settings.

Lower-level policy settings can be more or less restrictive than the equivalent higher-level settings. For example, you can set a global policy to **Deny** and the equivalent desktop pool-level policy to **Allow**, or vice versa.

Note Only global policies are available for RDS desktop and application pools. You cannot set user-level policies or pool-level policies for RDS desktop and application pools.

Configure Global Policy Settings

You can configure global policies to control the behavior of all client sessions users.

Prerequisites

Familiarize yourself with the policy descriptions. See Horizon 7 Policies.

Procedure

1. In Horizon Administrator, select **Policies > Global Policies**.
2. Click **Edit policies** in the **View Policies** pane.
3. Click **OK** to save your changes.

Configure Policies for Desktop Pools

You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See Horizon 7 Policies.

Procedure

1. In Horizon Administrator, select **Catalog > Desktop Pools**.
2. Double-click the ID of the desktop pool and click the **Policies** tab.

   The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
3. Click **Edit Policies** in the **View Policies** pane.
4. Click **OK** to save your changes.

Configure Policies for Users

You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop pool-level policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See Horizon 7 Policies.

Procedure

1. In Horizon Administrator, select **Catalog > Desktop Pools**.
2. Double-click the ID of the desktop pool and click the **Policies** tab.

   The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
3. Click **User Overrides** and then click **Add User**.
4. To find a user, click **Add**, type the name or description of the user, and then click **Find**.
5. Select one or more users from the list, click **OK**, and then click **Next**.

   The Add Individual Policy dialog box appears.
6. Configure the Horizon policies and click **Finish** to save your changes.

Horizon 7 Policies

You can configure Horizon 7 policies to affect all client sessions, or you can apply them to affect specific desktop pools or users.

Table 5-1 describes each Horizon 7 policy setting.

Table 5-1. Horizon Policies

Policy	Description
Multimedia redirection (MMR)	Determines whether MMR is enabled for client systems. MMR is a Windows Media Foundation filter that forwards multimedia data from specific codecs on remote desktops directly through a TCP socket to the client system. The data is then decoded directly on the client system, where it is played. The default value is **Deny**. If client systems have insufficient resources to handle local multimedia decoding, leave the setting as **Deny**. Multimedia Redirection (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.
USB Access	Determines whether remote desktops can use USB devices connected to the client system. The default value is **Allow**. To prevent the use of external devices for security reasons, change the setting to **Deny**.
PCoIP hardware acceleration	Determines whether to enable hardware acceleration of the PCoIP display protocol and specifies the acceleration priority that is assigned to the PCoIP user session. This setting has an effect only if a PCoIP hardware acceleration device is present on the physical computer that hosts the remote desktop. The default value is **Allow** at **Medium** priority.

Using Smart Policies

You can use Smart Policies to create policies that control the behavior of the USB redirection, virtual printing, clipboard redirection, client drive redirection, and PCoIP display protocol features on specific remote desktops. You can also use Smart Policies to create policies that control the behavior of published applications.

With Smart Policies, you can create policies that take effect only if certain conditions are met. For example, you can configure a policy that disables the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

Requirements for Smart Policies

To use Smart Policies, your Horizon 7 environment must meet certain requirements.

- You must install Horizon Agent 7.0 or later and VMware User Environment Manager 9.0 or later on the remote desktops that you want to manage with Smart Policies.
- Users must use Horizon Client 4.0 or later to connect to remote desktops that you manage with Smart Policies.

Installing User Environment Manager

To use Smart Policies to control the behavior of remote desktop features on a remote desktop, you must install User Environment Manager 9.0 or later on the remote desktop.

You can download the User Environment Manager installer from the VMware Downloads page. You must install the VMware UEM FlexEngine client component on each remote desktop that you want to manage with User Environment Manager. You can install the User Environment Manager Management Console component on any desktop from which you want to manage the User Environment Manager environment.

For a linked-clone pool, you install User Environment Manager in the parent virtual machine that you use as a base image for the linked clones. For an RDS desktop pool, you install User Environment Manager on the RDS host that provides the RDS desktop sessions.

For User Environment Manager system requirements and complete installation instructions, see the *User Environment Manager Administrator's Guide* document.

Configuring User Environment Manager

You must configure User Environment Manager before you can use it to create smart policies for remote desktop features.

To configure User Environment Manager, follow the configuration instructions in the *User Environment Manager Administrator's Guide*. The following configuration steps supplement the information in that document.

- When configuring the VMware UEM FlexEngine client component on remote desktops, create FlexEngine logon and logoff scripts. Use the **–HorizonViewMultiSession –r** parameter for the logon script and the **–HorizonViewMultiSession –s** parameter for the logoff script.

  Note Do not use logon scripts to start other applications on a remote desktop. Additional logon scripts can delay remote desktop logon for up to 10 minutes.

- Enable the user group policy setting `Run logon scripts synchronously` on remote desktops. This setting is located in the folder `User Configuration\Policies\Administrative Templates\System\Scripts`.
- Enable the computer group policy setting `Always wait for the network at computer startup and logon` on remote desktops. This setting is located in the folder `Computer Configuration\Administrative Template\System\Logon`.
- For Windows 8.1 remote desktops, disable the computer group policy setting `Configure Logon Script Delay`. This setting is located in the folder `Computer Configuration\Administrative Templates\System\Group Policy`.

- To ensure that Horizon Smart Policy settings are refreshed when users reconnect to desktop sessions, use the User Environment Manager Management Console to create a triggered task. Set the trigger to **Reconnect session**, set the action to **User Environment refresh**, and select **Horizon Smart Policies** for the refresh.

  Note If you create the triggered task while a user is logged in to the remote desktop, the user must log off from the desktop for the triggered task to take effect.

Horizon Smart Policy Settings

You control the behavior of remote desktop features in User Environment Manager by creating a Horizon smart policy.

Table 5-2 describes the settings that you can select when you define a Horizon smart policy in User Environment Manager.

Table 5-2. Horizon Smart Policy Settings

Setting	Description
USB redirection	Determines whether USB redirection is enabled on the remote desktop. The USB redirection feature allows users to use locally attached USB devices, such as thumb flash drives, cameras, and printers, from the remote desktop.
Printing	Determines whether virtual printing is enabled on the remote desktop. The virtual printing feature allows users to print to a virtual printer or a USB printer that is attached to the client computer from the remote desktop.
Clipboard	Determines the direction in which clipboard redirection is allowed. You can select one of these values: ■ **Disable**. Clipboard redirection is disabled in both directions. ■ **Allow all**. Clipboard redirection is enabled. Users can copy and paste from the client system to the remote desktop and from the remote desktop to the client system. ■ **Allow copy from client to agent**. Users can copy and paste only from the client system to the remote desktop. ■ **Allow copy from agent to client**. Users can copy and paste only from the remote desktop to the client system.
Client drive redirection	Determines whether client drive redirection is enabled on the remote desktop and if shared drives and folders are writeable. You can select one of these values: ■ **Disable**. Client drive redirection is disabled on the remote desktop. ■ **Allow all**. Client drives and folders are shared with the remote desktop and are readable and writeable. ■ **Read-only**. Client drives and folders are shared with the remote desktop and are readable, but not writeable. If you do not configure this setting, whether shared drives and folders are writeable depends on local registry settings. For more information, see Use Registry Settings to Configure Client Drive Redirection.
Bandwidth profile	Configures a bandwidth profile for PCoIP and Blast sessions on the remote desktop. You can select a predefined bandwidth profile, for example, **LAN**. Selecting a predefined bandwidth profile prevents the agent from attempting to transmit at a higher rate than the link capacity. If you select the default profile, the maximum bandwidth is 90000 kilobits per second. For more information, see Bandwidth Profile Reference.
HTML Access file transfer	Determines the transfer of HTML files between client and agent.

In general, Horizon smart policy settings that you configure for remote desktop features in User Environment Manager override any equivalent registry key and group policy settings.

Bandwidth Profile Reference

With Smart Policies, you can use the Bandwidth profile policy setting to configure a bandwidth profile for PCoIP or Blast sessions on remote desktops.

Table 5-3. Bandwidth Profiles

Bandwidth Profile	Max Session BW (Kbps)	Min Session BW (Kbps)	Enable BTL	Max Initial Image Quality	Min Image Quality	Max FPS	Max Audio BW (Kbps)	Image Quality Performance
High-speed LAN	900000	100	Yes	100	50	60	1600	50
LAN	900000	100	Yes	90	50	30	1600	50
Dedicated WAN	900000	100	No	80	40	30	500	50
Broadband WAN	5000	100	No	70	40	20	500	50
Low-speed WAN	2000	100	No	70	30	15	200	25
Extremely low-speed connection	1000	100	No	70	30	5	90	0

Adding Conditions to Horizon Smart Policy Definitions

When you define a Horizon Smart Policy in User Environment Manager, you can add conditions that must be met for the policy to take effect. For example, you can add a condition that disables the client drive redirection feature only if a user connects to the remote desktop from outside your corporate network.

You can add multiple conditions for the same remote desktop feature. For example, you can add one condition that enables local printing if a user is a member of the HR group and another condition that enables local printing if the remote desktop is in the Win7 pool.

For detailed information about adding and editing conditions in the User Environment Manager Management Console, see the *User Environment Manager Administrator's Guide*.

Using the Horizon Client Property Condition

When a user connects or reconnects to a remote desktop, Horizon Client gathers information about the client computer and Connection Server sends that information to the remote desktop. You can add the Horizon Client Property condition to a Horizon Policy definition to control when the policy takes effect based on the information that the remote desktop receives.

Note The Horizon Client Property condition is effective only if a user launches the remote desktop with the PCoIP display protocol or the VMware Blast display protocol. If a user launches the remote desktop with the RDP display protocol, the Horizon Client Property condition has no effect.

Table 5-4 describes the predefined properties that you can select from the **Properties** drop-down menu when you use the Horizon Client Property condition. Each predefined property corresponds to a `ViewClient_` registry key.

Table 5-4. Predefined Properties for the Horizon Client Property Condition

Property	Corresponding Registry Key	Description
Client location	`ViewClient_Broker_GatewayLocation`	Specifies the location of the user's client system. Valid values are as follows: ■ Internal - the policy takes effect only if a user connects to the remote desktop from inside the corporate network ■ External - the policy takes effect only if a user connects to the remote desktop from outside the corporate network For information about setting the gateway location for a Connection Server or security server host, see the *View Administration* document. For information about setting the gateway location for an Access Point appliance, see the *Deploying and Configuring Unified Access Gateway* document.
Launch tag(s)	`ViewClient_Launch_Matched_Tags`	Specifies one or more tags. Separate multiple tags with a comma or semicolon. The policy takes effect only if the tag that enabled the remote desktop or application launch to occur matches one of the specified tags. For information about assigning tags to Connection Server instances and desktop pools, see your Setting Up document.
Pool name	`ViewClient_Launch_ID`	Specifies a desktop or application pool ID. The policy takes effect only if the ID of the desktop or application pool the user selected when launching the remote desktop or application matches the specified desktop or application pool ID. For example, if the user selected the Win7 pool and this property is set to Win7, the policy takes effect. **Note** If more than one application pool is launched in the same RDS host session then the value is the ID of the first application that is launched from Horizon Client.

The **Properties** drop-down menu is also a text box, and you can manually enter any `ViewClient_` registry key in the text box. Do not include the `ViewClient_` prefix when you enter the registry key. For example, to specify `ViewClient_Broker_URL`, enter `Broker_URL`.

You can use the Windows Registry Editor (`regedit.exe`) on the remote desktop to view the `ViewClient_` registry keys. Horizon Client writes client computer information to the system registry path `HKEY_CURRENT_USER\Volatile Environment` on remote desktops that are deployed on single-user machines. For remote desktops that are deployed in RDS sessions, Horizon Client writes the client computer information to the system registry path `HKEY_CURRENT_USER\Volatile Environment\`*x*, where *x* is the session ID on the RDS host.

Using Other Conditions

The User Environment Manager Management Console provides many conditions. The following conditions can be especially useful when creating policies for remote desktop features.

Group Member	You can use this condition to configure the policy to take effect only if a user is a member of a specific group.
Remote Display Protocol	You can use this condition to configure the policy to take effect only if the user selects a particular display protocol. The condition settings include RDP, PCoIP, and Blast.
IP Address	You can use this condition to configure the policy that takes effect only if a user connects from inside or outside the corporate network. Use the condition settings to specify an internal IP address range or an external IP address range. **Note** You can also use the **Client location** property in the Horizon Client Property condition.

For descriptions of all the available conditions, see the *User Environment Manager Administrator's Guide* document.

Create a Horizon Smart Policy in User Environment Manager

You use the User Environment Manager Management Console to create a Horizon smart policy in User Environment Manager. When you define a Horizon smart policy, you can add conditions that must be met for the smart policy to take effect.

Prerequisites

- Install and configure User Environment Manager. See Installing User Environment Manager and Configuring User Environment Manager.
- Become familiar with the Horizon Smart Policy settings. See Horizon Smart Policy Settings.
- Become familiar with the conditions that you can add to Horizon Smart Policy definitions. See Adding Conditions to Horizon Smart Policy Definitions.

For complete information about using the User Environment Manager Management Console, see the *User Environment Manager Administrator's Guide* document.

Procedure

1. In the User Environment Manager Management Console, select the **User Environment** tab and click **Horizon Smart Policies** in the tree view.

   Existing Horizon smart policy definitions, if any, appear in the Horizon Smart Policies pane.

2 Right-click **Horizon Smart Policies** and select **Create Horizon Smart Policy definition** to create a new smart policy.

   The Horizon Smart Policy dialog box appears.

3 Select the **Settings** tab and define the smart policy settings.

   a In the General Settings section, type a name for the smart policy in the **Name** text box.

      For example, if the smart policy will affect the client drive redirection feature, you might name the smart policy CDR.

   b In the Horizon Smart Policy Settings section, select the remote desktop features and settings to include in the smart policy.

      You can select multiple remote desktop features.

4 (Optional) To add a condition to the smart policy, select the **Conditions** tab, click **Add**, and select a condition.

   You can add multiple conditions to a smart policy definition.

5 Click **Save** to save the smart policy.

User Environment Manager processes the Horizon smart policy each time a user connects or reconnects to the remote desktop.

User Environment Manager processes multiple smart policies in alphabetical order based on the smart policy name. Horizon smart policies appear in alphabetical order in the Horizon Smart Policies pane. If smart policies conflict, the last smart policy processed takes precedence. For example, if you have a smart policy named Sue that enables USB redirection for the user named Sue, and another smart policy named Pool that disables USB redirection for the desktop pool named Win7, the USB redirection feature is enabled when Sue connects to a remote desktop in the Win7 desktop pool.

Using Active Directory Group Policies

You can use Microsoft Windows Group Policy to optimize and secure remote desktops, control the behavior of Horizon 7 components, and to configure location-based printing.

Group Policy is a feature of Microsoft Windows operating systems that provides centralized management and configuration of computers and remote users in an Active Directory environment.

Group policy settings are contained in entities called group policy objects (GPOs). GPOs are associated with Active Directory objects. You can apply GPOs to Horizon 7 components at a domain-wide level to control various areas of the Horizon 7 environment. After they are applied, GPO settings are stored in the local Windows Registry of the specified component.

You use the Microsoft Windows Group Policy Object Editor to manage group policy settings. The Group Policy Object Editor is a Microsoft Management Console (MMC) snap-in. The MMC is part of the Microsoft Group Policy Management Console (GPMC). See the Microsoft TechNet Web site for information on installing and using the GPMC.

Creating an OU for Remote Desktops

Create an organizational unit (OU) in Active Directory specifically for your remote desktops.

To prevent group policy settings from being applied to other Windows servers or workstations in the same domain as your remote desktops, create a GPO for your Horizon 7 group policies and link it to the OU that contains your remote desktops.

See the Microsoft Active Directory documentation on the Microsoft TechNet Web site for information on creating OUs and GPOs.

Enabling Loopback Processing for Remote Desktops

By default, a user's policy settings come from the set of GPOs that are applied to the user object in Active Directory. However, in the Horizon 7 environment, GPOs apply to users based on the computer they log in to.

When you enable loopback processing, a consistent set of policies applies to all users that log in to a particular computer, regardless of their location in Active Directory.

See the Microsoft Active Directory documentation for information on enabling loopback processing.

Note Loopback processing is only one approach to handling GPOs in Horizon 7. You might need to implement a different approach.

Using Horizon 7 Group Policy Administrative Template Files

Horizon 7 provides several component-specific Group Policy Administrative ADMX template files. You can optimize and secure remote desktops and applications by adding the policy settings in the ADMX template files to a new or existing GPO in Active Directory.

All ADMX files that provide group policy settings for Horizon 7 are available in a bundled `.zip` file named `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. You can download the file from the VMware download site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the bundled `.zip` file.

The Horizon 7 ADMX template files contain both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to all remote desktops, regardless of who connects to the desktop.
- The User Configuration policies set policies that apply to all users, regardless of the remote desktop or application they connect to. User Configuration policies override equivalent Computer Configuration policies.

Microsoft Windows applies policies at desktop startup and when users log in.

Horizon 7 ADMX Template Files

The Horizon 7 ADMX template files provide group policy settings that allow you to control and optimize Horizon 7 components.

Table 5-5. Horizon ADMX Template Files

Template Name	Template File	Description
VMware View Agent Configuration	`vdm_agent.admx`	Contains policy settings related to the authentication and environmental components of Horizon Agent.
VMware Horizon Client Configuration	`vdm_client.admx`	Contains policy settings related to Horizon Client for Windows. Clients that connect from outside the Connection Server host domain are not affected by policies applied to Horizon Client. See the *VMware Horizon Client for Windows Installation and Setup Guide* document.
VMware Horizon URL Redirection	`urlRedirection.admx`	Contains policy settings related to the URL Content Redirection Feature. If you add this template to a GPO for a remote desktop pool or application pool, certain URL links clicked inside the remote desktops or app can be redirected to a Windows-based client and opened in a client-side browser. If you add this template to a client-side GPO, when a user clicks certain URL links in a Windows-based client system, the URL can be opened in a remote desktop or application. See Chapter 3 Configuring URL Content Redirection and see the *VMware Horizon Client for Windows Installation and Setup Guide* document.
VMware View Server Configuration	`vdm_server.admx`	Contains policy settings related to Connection Server. See the *View Administration* document.
VMware View Common Configuration	`vdm_common.admx`	Contains policy settings that are common to all Horizon components. See the *View Administration* document.
PCoIP Session Variables	`pcoip.admx`	Contains policy settings related to the PCoIP display protocol.
PCoIP Client Session Variables	`pcoip.client.admx`	Contains policy settings related to the PCoIP display protocol that affect Horizon Client for Windows. See the *VMware Horizon Client for Windows Installation and Setup Guide* document.
Persona Management	`ViewPM.admx`	Contains policy settings related to Horizon Persona Management. See the *Setting Up Virtual Desktops in Horizon 7* document.

Table 5-5. Horizon ADMX Template Files (Continued)

Template Name	Template File	Description
Remote Desktop Services	`vmware_rdsh_server.admx`	Contains policy settings related to Remote Desktop Services. See Using Remote Desktop Services Group Policies.
View RTAV Configuration	`vdm_agent_rtav.admx`	Contains policy settings related to webcams that are used with the Real-Time Audio-Video feature. See Real-Time Audio-Video Group Policy Settings.
Scanner Redirection	`vdm_agent_scanner.admx`	Contains policy settings related to scanning devices that are redirected for use in published desktops and applications. See Scanner Redirection Group Policy Settings.
Serial COM	`vdm_agent_serialport.admx`	Contains policy settings related to serial (COM) ports that are redirected for use in virtual desktops. See Serial Port Redirection Group Policy Settings.
VMware Horizon Printer Redirection	`vdm_agent_printing.admx`	Contains policy settings related to filtering redirected printers. See Filtering Printers for Virtual Printing.

Add the ADMX Template Files to Active Directory

You can add the policy settings for specific remote desktop features in the Horizon 7 ADMX files to group policy objects (GPOs) in Active Directory.

Prerequisites

- Verify that the setup option for the remote desktop feature you are applying the policy for is installed on your virtual machine desktops and RDS hosts. The group policy settings have no effect if the remote desktop feature is not installed. See your Setting Up document for information on installing Horizon Agent.
- Create GPOs for the remote desktop features that you want to apply the group policy settings to and link them to the OU that contains your virtual machine desktops or RDS hosts.
- Verify the name of the ADMX template file that you want to add to Active Directory. See Horizon 7 ADMX Template Files.
- Verify that the Group Policy Management feature is available on your Active Directory server.

Procedure

1 Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

  Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

The file is named VMware-Horizon-Extras-Bundle-*x.x.x*-*yyyyyyy*.zip, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADMX files that provide group policy settings for Horizon 7 are available in this file.

2 Unzip the VMware-Horizon-Extras-Bundle-*x.x.x*-*yyyyyyy*.zip file and copy the ADMX files to your Active Directory server.

   a Copy the .admx files and the en-US folder to the %systemroot%\PolicyDefinitions folder on your Active Directory server.

   b Copy the language resource (.adml) files to the appropriate subfolder in %systemroot%\PolicyDefinitions\ on your Active Directory server.

3 On the Active Directory server, open the Group Policy Management Editor and enter the path to the template files where they appear in the editor after installation.

What to do next

Configure the group policy settings.

VMware View Agent Configuration ADMX Template Settings

The VMware View Agent Configuration ADMX template file (vdm_agent.admx) contains policy settings related to the authentication and environmental components of Horizon Agent.

The ADMX files are available in a bundled .zip file named VMware-Horizon-Extras-Bundle-*x.x.x*-*yyyyyyy*.zip, which you can download from the VMware download site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the bundled .zip file.

The following table describes policy settings in the VMware View Agent Configuration ADMX template file other than those settings that are used with USB devices. The template contains both Computer Configuration and User Configuration settings. The User Configuration setting overrides the equivalent Computer Configuration setting.

Table 5-6. VMware View Agent Configuration Template Settings

Setting	Computer	User	Properties
`AllowDirectRDP`	X		Determines whether clients other than Horizon Client devices can connect directly to remote desktops with RDP. When this setting is disabled, the agent permits only Horizon-managed connections through Horizon Client. When connecting to a remote desktop from Horizon Client for Mac, do not disable the `AllowDirectRDP` setting. If this setting is disabled, the connection fails with an `Access is denied` error. By default, while a user is logged in to a remote desktop session, you can use RDP to connect to the virtual machine. The RDP connection terminates the remote desktop session, and the user's unsaved data and settings might be lost. The user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, disable the `AllowDirectRDP` setting. **Important** The Windows Remote Desktop Services service must be running on the guest operating system of each desktop. You can use this setting to prevent users from making direct RDP connections to their desktops. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is enabled by default.
`AllowSingleSignon`	X		Determines whether single sign-on (SSO) is used to connect users to desktops and applications. When this setting is enabled, users are required to enter their credentials only once, when they log in to the server. When this setting is disabled, users must reauthenticate when the remote connection is made. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is enabled by default.
`CommandsToRunOnConnect`	X		Specifies a list of commands or command scripts to be run when a session is connected for the first time. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. See Running Commands on Horizon Desktops for more information.
`CommandsToRunOnDisconnect`	X		Specifies a list of commands or command scripts to be run when a session is disconnected. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. See Running Commands on Horizon Desktops for more information.

Table 5-6. VMware View Agent Configuration Template Settings (Continued)

Setting	Computer	User	Properties
CommandsToRunOnReconnect	X		Specifies a list of commands or command scripts to be run when a session is reconnected after a disconnect. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. See Running Commands on Horizon Desktops for more information.
ConnectionTicketTimeout	X		Specifies the amount of time in seconds that the Horizon connection ticket is valid. Horizon Client devices use a connection ticket for verification and single sign-on when connecting to the agent. For security reasons, a connection ticket is valid for a limited amount of time. When a user connects to a remote desktop, authentication must take place within the connection ticket timeout period or the session times out. If this setting is not configured, the default timeout period is 900 seconds. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor.
CredentialFilterExceptions	X		Specifies the executable files that are not allowed to load the agent CredentialFilter. Filenames must not include a path or suffix. Use a semicolon to separate multiple filenames. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor.
Disable Time Zone Synchronization	X	X	Determines whether the time zone of the Horizon desktop is synchronized with the time zone of the connected client. An enabled setting applies only if the `Disable time zone forwarding` setting of the Horizon Client Configuration policy is not set to disabled. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is disabled by default.
DPI Synchronization	X	X	Adjusts the system-wide DPI setting for the remote session. When this setting is enabled or not configured, the system-wide DPI setting for the remote session is set to match the corresponding DPI setting on the client operating system. When this setting is disabled, the system-wide DPI setting for the remote session is never changed. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is not configured by default. **Note** This setting applies only to Windows clients on which Horizon Client 4.2 or later is installed.

Table 5-6. VMware View Agent Configuration Template Settings (Continued)

Setting	Computer	User	Properties
Enable multi-media acceleration	X		Determines whether multimedia redirection (MMR) is enabled on the remote desktop. MMR is a Windows Media Foundation filter that forwards multimedia data from specific codecs on the remote system directly through a TCP socket to the client. The data is then decoded directly on the client, where it is played. You can disable MMR if the client has insufficient resources to handle local multimedia decoding. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is enabled by default.
Force MMR to use software overlay	X		MMR tries to use the hardware overlay to play back video for better performance. When working with multiple displays, the hardware overlay exists only on one of the displays, either the primary display or the display where WMP was started. If WMP is dragged to another display, the video appears as a black rectangle. Use this option to force MMR to use a software overlay that works on all displays. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is not configured by default.
Single sign-on retry timeout	X		Specifies the time, in milliseconds, after which single sign-on is retried. Set the value to 0 to disable single sign-on retry. The default value is 5000 milliseconds. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is not configured by default.
ShowDiskActivityIcon	X		This setting is not supported in this release. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor.
Toggle Display Settings Control	X		Determines whether to disable the **Settings** tab in the **Display** control panel when a client session uses the PCoIP display protocol. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is enabled by default.

Table 5-6. VMware View Agent Configuration Template Settings (Continued)

Setting	Computer	User	Properties
UnAuthenticatedAccessEnabled			Enables or disables the unauthenticated access feature. When this setting is enabled, unauthenticated access users can access published applications from a Horizon Client without requiring AD credentials. When this setting is disabled, unauthenticated access users cannot access published applications from a Horizon Client without requiring AD credentials. You must reboot the RDS host for this setting to take effect. This setting is in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor. This setting is enabled by default.
Send updates for empty or offscreen windows	X		Specifies whether the client receives updates about empty or offscreen windows. When this setting is disabled, information about window that are smaller than 2x2 pixels, or that are located entirely offscreen, are not sent to the client. This setting is in the **VMware View Agent Configuration > Unity Touch and Hosted Apps** folder in the Group Policy Management Editor. This setting is disabled by default.
Enable Unity Touch	X		Determines whether the Unity Touch functionality is enabled on the remote desktop. Unity Touch supports the delivery of remote applications in Horizon and allows mobile device users to access applications in the Unity Touch sidebar. This setting is in the **VMware View Agent Configuration > Unity Touch and Hosted Apps** folder in the Group Policy Management Editor. This setting is enabled by default.
Enable system tray redirection for Hosted Apps	X		Determines whether system tray redirection is enabled while a user is running remote applications. This setting is in the **VMware View Agent Configuration > Unity Touch and Hosted Apps** folder in the Group Policy Management Editor. This setting is enabled by default.
Enable user profile customization for Hosted Apps	X	X	Specifies whether to customize the user profile when remote applications are used. If this setting is enabled, a user profile is generated, the Windows theme is customized, and startup applications are registered. This Computer Configuration setting is in the **VMware View Agent Configuration > Unity Touch and Hosted Apps** folder in the Group Policy Management Editor. The User Configuration setting is in the **VMware View Agent Configuration > Agent Security > Unity Touch and Hosted Apps** folder in the Group Policy Management Editor. This setting is disabled by default.

Table 5-6. VMware View Agent Configuration Template Settings (Continued)

Setting	Computer	User	Properties
Limit usage of Windows hooks	X		Disables most hooks when remote applications or Unity Touch are used. This setting is intended for applications that have compatibility issues when OS-level hooks are set. For example, enabling this setting disables the use of most Windows active accessibility and in-process hooks. This setting is in the **VMware View Agent Configuration > Unity Touch and Hosted Apps** folder in the Group Policy Management Editor. This setting is disabled by default, which means that all preferred hooks are used.
Accept SSL encrypted framework channel		X	Enables the SSL encrypted framework channel. The following options are available: ■ **Disable** - Disable SSL. ■ **Enable** - Enable SSL. Allow legacy clients to connect without SSL. ■ **Enforce** - Enable SSL. Refuse legacy client connections. This setting is in the **VMware View Agent Configuration > Agent Security** folder in the Group Policy Management Editor. This setting is not configured by default. The default value is **Enable**.
Default Proxy Server	X		Default Internet Explorer connection setting for the proxy server. Specifies the proxy server to use in Internet Options > Local Area Network (LAN) Settings. This setting is in the **VMware View Agent Configuration > VMware Client IP Transparency** folder in the Group Policy Management Editor. This setting is not enabled by default.
Enable	X		Enables VMware Client IP Transparency. Remote connections to Internet Explorer use the client's IP address instead of the IP address of the remote desktop machine. This setting takes effect at the next login. This setting is in the **VMware View Agent Configuration > VMware Client IP Transparency** folder in the Group Policy Management Editor. If the VMware Client IP Transparency custom setup option is selected in the Horizon Agent installer, this setting is enabled by default.
Default auto detect proxy	X		Default Internet Explorer connection setting. Turns on **Automatically detect settings** in Internet Options > Local Area Network (LAN) Settings. This setting is in the **VMware View Agent Configuration > VMware Client IP Transparency** folder in the Group Policy Management Editor. This setting is not enabled by default.

Table 5-6. VMware View Agent Configuration Template Settings (Continued)

Setting	Computer	User	Properties
`Set proxy for Java applet`	X		Sets the proxy for Java applets. The following options are available: ■ **Use client ip transparency for Java proxy** - directs a remote connection to use the client's IP address instead of the IP address of the remote desktop machine for Java applets. ■ **Use direct connection for Java proxy** - uses a direct connection to bypass the browser setting for Java applets. ■ **Use the default value for Java proxy** - restores the original Java proxy settings. This setting is in the **VMware View Agent Configuration > VMware Client IP Transparency** folder in the Group Policy Management Editor. This setting is not enabled by default.
`Enable flash multi-media redirection`	X		Specifies whether Flash Redirection is enabled on the agent. This setting is in the **VMware View Agent Configuration > VMware FlashMMR** folder in the Group Policy Management Editor.
`Minimum rect size to enable FlashMMR`	X		Specifies the minimum rect size to enable Flash Redirection. This setting is in the **VMware View Agent Configuration > VMware FlashMMR** folder in the Group Policy Management Editor. The default width is 320 pixels and the default height is 200 pixels.
`Definition for FlashMMR url list usage`		X	Defines the white list or black list rule that enables or disables URLs from using Flash Redirection. If you select **Enable white list** from the **Definition for FlashMMR url list usage** drop-down menu, only the URLs in the URL list are enabled to use Flash Redirection. If you select **Enable black list** from the **Definition for FlashMMR url list usage** drop-down menu, the URLs in the URL list are not able to use Flash Redirection. You specify the URL list in the `Hosts Url list to enable FlashMMR` group policy setting. This setting is in the **VMware View Agent Configuration > VMware FlashMMR** folder in the Group Policy Management Editor. This setting specifies a white list by default.
`Hosts Url list to enable FlashMMR`		X	Specifies the URL list that is enabled or disabled to use Flash Redirection based on the `Definition for FlashMMR url list usage` group policy setting. You must include **http://** or **https://**. You can use regular expressions. For example, you can specify **`https://*.google.com`** and **`http://www.cnn.com`**. This setting is in the **VMware View Agent Configuration > VMware FlashMMR** folder in the Group Policy Management Editor.

Note The `Connect using DNS Name` setting was removed in the Horizon 6 version 6.1 release. You can set the Horizon 7 LDAP attribute, **pae-PreferDNS**, to tell Horizon Connection Server to give preference to DNS names when sending the addresses of desktop machines and RDS hosts to clients and gateways. See "Give Preference to DNS Names When Horizon Connection Server Returns Address Information" in the *View Installation* document.

USB Settings for the Horizon Agent

See USB Settings in the Horizon Agent Configuration ADMX Template.

Client System Information Sent to Remote Desktops

When a user connects or reconnects to a remote desktop, Horizon Client gathers information about the client system and Connection Server sends that information to the remote desktop.

Horizon Agent writes the client computer information to the system registry path `HKCU\Volatile Environment` on remote desktops that are deployed on single-user machines. For remote desktops that are deployed in RDS sessions, Horizon Agent writes the client computer information to the system registry path `HKCU\Volatile Environment\`*x*, where *x* is the session ID, on the RDS host.

If Horizon Client is running inside of a remote desktop session, it sends the physical client information instead of the virtual machine information to the remote desktop. For example, if a user connects from their client system to a remote desktop, launches Horizon Client inside the remote desktop and connects to another remote desktop, the IP address of the physical client system is sent to the second remote desktop. This feature is referred to as nested mode or a double-hop scenario. Horizon Client sends `ViewClient_Nested_Passthrough`, which is set to 1, along with the client system information to indicate that it is sending nested mode information.

Note With Horizon Client 4.1, client system information is passed to the second-hop desktop on the initial protocol connection. With Horizon Client 4.2 and later, client system information is also updated if the first-hop protocol connection disconnects and reconnects.

You can add commands to the Horizon Agent `CommandsToRunOnConnect`, `CommandsToRunOnReconnect`, and `CommandsToRunOnDisconnect` group policy settings to run commands or command scripts that read this information from the system registry when users connect and reconnect to desktops. See Running Commands on Horizon Desktops for more information.

Table 5-7 describes the registry keys that contain client system information and lists the types of desktops and client systems that support them. If Yes appears in the **Supports Nested Mode** column, it indicates that physical client information (rather than virtual machine information) is sent to a second-hop desktop.

Table 5-7. Client System Information

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
ViewClient_IP_Address	The IP address of the client system.	Yes	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_MAC_Address	The MAC address of the client system.	Yes	VDI (single-user machine) RDS	Windows, Linux, Mac, Android
ViewClient_Machine_Name	The machine name of the client system.	Yes	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Machine_Domain	The domain of the client system.	Yes	VDI (single-user machine) RDS	Windows, Windows Store
ViewClient_LoggedOn_Username	The user name that was used to log in to the client system.		VDI (single-user machine) RDS	Windows, Linux, Mac
ViewClient_LoggedOn_Domainname	The domain name that was used to log in to the client system.		VDI (single-user machine) RDS	Windows, Windows Store For Linux and Mac clients, see ViewClient_Machine_Domain.ViewClient_LoggedOn_Domainname is not given by the Linux or Mac client because Linux and Mac accounts are not bound to Windows domains.
ViewClient_Type	The thin client name or operating system type of the client system.	Yes	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Broker_DNS_Name	The DNS name of the View Connection Server instance.		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Broker_URL	The URL of the View Connection Server instance.		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.

Table 5-7. Client System Information (Continued)

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
`ViewClient_Broker_Tunneled`	The status of the tunnel connection for the View Connection Server, which can be either `true` (enabled) or `false` (disabled).		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
`ViewClient_Broker_Tunnel_URL`	The URL of the View Connection Server tunnel connection, if the tunnel connection is enabled.		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
`ViewClient_Broker_Remote_IP_Address`	The IP address of the client system that is seen by the View Connection Server instance.		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
`ViewClient_TZID`	The Olson time zone ID. To disable time zone synchronization, enable the Horizon Agent `Disable Time Zone Synchronization` group policy setting.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
`ViewClient_Windows_Timezone`	The GMT standard time. To disable time zone synchronization, enable the Horizon Agent `Disable Time Zone Synchronization` group policy setting.		VDI (single-user machine) RDS	Windows, Windows Store
`ViewClient_Broker_DomainName`	Domain name used to authenticate to View Connection Server.		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
`ViewClient_Broker_UserName`	Username used to authenticate to View Connection Server.		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
`ViewClient_Client_ID`	Specifies the `Unique Client HardwareId` used as a link to the license key.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
`ViewClient_Displays.Number`	Specifies the number of monitors being used on the client.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store

Table 5-7. Client System Information (Continued)

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
ViewClient_Displays.Topology	Specifies the arrangement, resolution, and dimensions of displays on the client.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Keyboard.Type	Specifies the type of keyboard being used on the client. For example: Japanese, Korean.		VDI (single-user machine) RDS	Windows
ViewClient_Launch_SessionType	Specifies the session type. The type can be desktop or application.		VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Mouse.Identifier	Specifies the type of mouse.		VDI (single-user machine) RDS	Windows
ViewClient_Mouse.NumButtons	Specifies the number of buttons supported by the mouse.		VDI (single-user machine) RDS	Windows
ViewClient_Mouse.SampleRate	Specifies the rate, in reports per second, at which input from a PS/2 mouse is sampled.		VDI (single-user machine) RDS	Windows
ViewClient_Protocol	Specifies the protocol being used.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Language	Specifies the operating system language.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Launch_Matched_Tags	Specifies one or more tags.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Launch_ID	Specifies the desktop or application pool Unique ID.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Windows Store
ViewClient_Broker_Farm_ID	Specifies the Farm ID of the desktop or application pool on an RDS host.		RDS	Windows, Linux, Mac, Android, iOS, Windows Store

Note The definitions of `ViewClient_LoggedOn_Username` and `ViewClient_LoggedOn_Domainname` in Table 5-7 apply to Horizon Client 2.2 for Windows or later releases.

For Horizon Client 5.4 for Windows or earlier releases, `ViewClient_LoggedOn_Username` sends the user name that was entered in Horizon Client, and `ViewClient_LoggedOn_Domainname` sends the domain name that was entered in Horizon Client.

Horizon Client 2.2 for Windows is a later release than Horizon Client 5.4 for Windows. Starting with Horizon Client 2.2, the release numbers for Windows are consistent with the Horizon Client releases on other operating systems and devices.

Running Commands on Horizon Desktops

You can use the Horizon Agent `CommandsToRunOnConnect`, `CommandsToRunOnReconnect`, and `CommandsToRunOnDisconnect` group policy settings to run commands and command scripts on Horizon desktops when users connect, reconnect, and disconnect.

To run a command or a command script, add the command name or the file path of the script to the group policy setting's list of commands. For example:

```
date
```

```
C:\Scripts\myscript.cmd
```

To run scripts that require console access, prepend the `–C` or `–c` option followed by a space. For example:

```
–c C:\Scripts\Cli_clip.cmd
```

```
–C e:\procexp.exe
```

Supported file types include `.CMD`, `.BAT`, and `.EXE`. `.VBS` files will not run unless they are parsed with `cscript.exe` or `wscript.exe`. For example:

```
–C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

The total length of the string, including the `–C` or `–c` option, should not exceed 260 characters.

VMware Virtualization Pack for Skype for Business Policy Settings

The VMware View Agent Configuration ADMX template file (`vdm_agent.admx`) contains policy settings related to the VMware Virtualization Pack for Skype for Business.

These settings are in the Group Policy Management Editor in **Computer Configuration > Administrative Templates > VMware View Agent Configuration > VMware Virtualization Pack for Skype for Business** folder.

Table 5-8. Virtualization Pack for Skype for Business Policy Settings

Setting	Description
Show Icon	Displays the icon for Virtualization Pack for Skype for Business. This policy is enabled by default. The icon does not appear if the Show Icon policy for Virtualization Pack for Skype for Business is disabled. When it is disabled, you cannot view the call statistics or messages.
Show Messages	Displays messages for Virtualization Pack for Skype for Business. This policy is enabled by default. Messages do not appear if the Show Icon or Show Messages policies for Virtualization Pack for Skype for Business are disabled.

PCoIP Policy Settings

The PCoIP ADMX template file contains policy settings related to the PCoIP display protocol. The ADMX template file is named (`pcoip.admx`). You can configure settings to default values that can be overridden by an administrator, or you can configure settings to non-overridable values.

The ADMX files are available in a bundled `.zip` file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, which you can download from the VMware download site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the bundled `.zip` file.

The PCoIP Session Variables ADMX template file contains two subcategories:

Overridable Administrator Defaults — Specifies PCoIP policy setting default values. These settings can be overridden by an administrator. These settings write registry keys values to `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults`. All of these settings are in the **Computer Configuration > Policies > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults** folder in the Group Policy Management Editor.

Not Overridable Administrator Settings — Contains the same settings as Overridable Administrator Defaults, but these settings cannot be overridden by an administrator. These settings write registry key values to `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin`. All of these settings are in the **User Configuration > Policies > Administrative Templates > PCoIP Session Variables > Not Overridable Administrator Settings** folder in the Group Policy Management Editor.

The template contains both Computer Configuration and User Configuration settings.

Non-Policy Registry Keys

If a local machine setting needs to be applied and cannot be placed under `HKLM\Software\Policies\Teradici`, local machine settings can be placed in registry keys in `HKLM\Software\Teradici`. The same registry keys can be placed in `HKLM\Software\Teradici` as in `HKLM\Software\Policies\Teradici`. If the same registry key is present in both locations, the setting in `HKLM\Software\Policies\Teradici` overrides the local machine value.

PCoIP General Settings

The PCoIP ADMX template file contains group policy settings that configure general settings such as PCoIP image quality, USB devices, and network ports.

All of these settings are in the **Computer Configuration > Policies > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults** folder in the Group Policy Management Editor.

All of these settings are also in the **User Configuration > Policies > Administrative Templates > PCoIP Session Variables > Not Overridable Administrator Settings** folder in the Group Policy Management Editor.

Table 5-9. PCoIP General Policy Settings

Setting	Description
`Configure PCoIP event log cleanup by size in MB`	Enables the configuration of the PCoIP event log cleanup by size in MB. When this policy is configured, the setting controls how large a log file can grow before it is cleaned up. For a non-zero setting of *m*, log files larger than *m* MB are automatically and silently deleted. A setting of 0 indicates that no file cleanup by size takes place. When this policy is disabled or not configured, the default event log cleanup by size is 100 MB. The log file cleanup is performed once at session startup. A change to the setting is not applied until the next session.
`Configure PCoIP event log cleanup by time in days`	Enables the configuration of the PCoIP event log cleanup by time in days. When this policy is configured, the setting controls how many days can pass before the log file is cleaned up. For a non-zero setting of *n*, log files older than *n* days are automatically and silently deleted. A setting of 0 indicates that no file cleanup by time takes place. When this policy is disabled or not configured, the default event log cleanup is 7 days. The log file cleanup is performed once at session startup. A change to the setting is not applied until the next session.
`Configure PCoIP event log verbosity`	Sets the PCoIP event log verbosity. The values range from 0 (least verbose) to 3 (most verbose). When this setting is enabled, you can set the verbosity level from 0 to 3. When the setting is not configured or disabled, the default event log verbosity level is 2. When this setting is modified during an active PCoIP session, the new setting takes effect immediately.

Table 5-9. PCoIP General Policy Settings (Continued)

Setting	Description
`Configure PCoIP image quality levels`	Controls how PCoIP renders images during periods of network congestion. The **Minimum Image Quality**, **Maximum Initial Image Quality**, and **Maximum Frame Rate** values interoperate to provide fine control in network-bandwidth constrained environments. Use the **Minimum Image Quality** value to balance image quality and frame rate for limited-bandwidth scenarios. You can specify a value between 30 and 100. The default value is 40. A lower value allows higher frame-rates, but with a potentially lower quality display. A higher value provides higher image quality, but with potentially lower frame rates when network bandwidth is constrained. When network bandwidth is not constrained, PCoIP maintains maximum quality regardless of this value. Use the **Maximum Initial Image Quality** value to reduce the network bandwidth peaks required by PCoIP by limiting the initial quality of the changed regions of the display image. You can specify a value between 30 and 100. The default value is 80. A lower value reduces the image quality of content changes and decreases peak bandwidth requirements. A higher value increases the image quality of content changes and increases peak bandwidth requirements. Unchanged regions of the image progressively build to a lossless (perfect) quality regardless of this value. A value of 80 or lower best utilizes the available bandwidth. The **Minimum Image Quality** value cannot exceed the **Maximum Initial Image Quality** value. Use the **Maximum Frame Rate** value to manage the average bandwidth consumed per user by limiting the number of screen updates per second. You can specify a value between 1 and 120 frames per second. The default value is 30. A higher value can use more bandwidth but provides less jitter, which allows smoother transitions in changing images such as video. A lower value uses less bandwidth but results in more jitter. These image quality values apply to the soft host only and have no effect on a soft client. When this setting is disabled or not configured, the default values are used. When this setting is modified during an active PCoIP session, the new setting takes effect immediately.
`Configure frame rate vs image quality preference`	Configure the frame rate and image quality preference from 0 (highest frame rate) to 100 (highest image quality). If this policy is disabled or not configured, the default setting is 50. Higher value (max: 100) means you prefer high image quality even if frame rate is choppy. Lower value (min: 0) means you prefer a fluent experience with aggressive image quality. This setting could work with the `Configure PCoIP image quality levels` GPO, which determines the max initial image quality level and min image quality level. While the `Frame rate and image quality preference` can adjust the image quality level for each frame, it cannot exceed the max/min quality level threshold configured by `Configure PCoIP image quality levels` GPO. When this policy is changed during run time, it could take effect immediately.

Table 5-9. PCoIP General Policy Settings (Continued)

Setting	Description
`Configure PCoIP session encryption algorithms`	Controls the encryption algorithms advertised by the PCoIP endpoint during session negotiation. Checking one of the check boxes disables the associated encryption algorithm. You must enable at least one algorithm. This setting applies to both agent and client. The endpoints negotiate the actual session encryption algorithm that is used. If FIPS140-2 approved mode is enabled, the **Disable AES-128-GCM encryption** value is always overridden so that AES-128-GCM encryption is enabled. Supported encryption algorithms, in order of preference, are SALSA20/12-256, AES-GCM-128, and AES-GCM-256. By default, all supported encryption algorithms are available for negotiation by this endpoint. If both endpoints are configured to support all three algorithms and the connection does not use a Security Gateway (SG), the SALSA20 algorithm will be negotiated and used. However, if the connection uses an SG, SALSA20 is automatically disabled and AES128 will be negotiated and used. If either endpoint or the SG disables SALSA20 and either endpoint disables AES128, then AES256 will be negotiated and used.

Table 5-9. PCoIP General Policy Settings (Continued)

Setting	Description
`Configure PCoIP USB allowed and unallowed device rules`	Specifies the USB devices that are authorized and not authorized for PCoIP sessions that use a zero client that runs Teradici firmware. USB devices that are used in PCoIP sessions must appear in the USB authorization table. USB devices that appear in the USB unauthorization table cannot be used in PCoIP sessions. You can define a maximum of 10 USB authorization rules and a maximum of 10 USB unauthorization rules. Separate multiple rules with the vertical bar (|) character. Each rule can be a combination of a Vendor ID (VID) and a Product ID (PID), or a rule can describe a class of USB devices. A class rule can allow or disallow an entire device class, a single subclass, or a protocol within a subclass. The format of a combination VID/PID rule is **`1xxxxyyyy`**, where **`xxxx`** is the VID in hexadecimal format and **`yyyy`** is the PID in hexadecimal format. For example, the rule to authorize or block a device with VID **`0x1a2b`** and PID **`0x3c4d`** is **`11a2b3c4d`**. For class rules, use one of the following formats: **Allow all USB devices** — Format: **`23XXXXXX`**; Example: **`23XXXXXX`** **Allow USB devices with a specific class ID** — Format: **`22`*`class`*`XXXX`**; Example: **`22aa`**`XXXX` **Allow a specific subclass** — Format: **`21`*`class`*`–`*`subclass`*`XX`**; Example: **`21aabbXX`** **Allow a specific protocol** — Format: **`20`*`class`*`–`*`subclass`*`–`*`protocol`***; Example: **`20aabbcc`** For example, the USB authorization string to allow USB HID (mouse and keyboard) devices (class ID 0x03) and webcams (class ID 0x0e) is **`2203XXXX|220eXXXX`**. The USB unauthorization string to disallow USB Mass Storage devices (class ID 0x08) is **`2208XXXX`**. An empty USB authorization string means that no USB devices are authorized. An empty USB unauthorization string means that no USB devices are banned. This setting applies to Horizon Agent only and only when the remote desktop is in a session with a zero client that runs Teradici firmware. Device use is negotiated between the endpoints. By default, all devices are allowed and none are disallowed.

Table 5-9. PCoIP General Policy Settings (Continued)

Setting	Description
`Configure PCoIP virtual channels`	Specifies the virtual channels that can and cannot operate over PCoIP sessions. This setting also determines whether to disable clipboard processing on the PCoIP host. Virtual channels that are used in PCoIP sessions must appear on the virtual channel authorization list. Virtual channels that appear in the unauthorized virtual channel list cannot be used in PCoIP sessions. You can specify a maximum of 15 virtual channels for use in PCoIP sessions. Separate multiple channel names with the vertical bar (|) character. For example, the virtual channel authorization string to allow the mksvchan and vdp_rdpvcbridge virtual channels is **`mksvchan|vdp_vdpvcbridge`**. If a channel name contains the vertical bar or backslash (\) character, insert a backslash character before it. For example, type the channel name awk|ward\channel as **`awk\\|ward\\channel`**. When the authorized virtual channel list is empty, all virtual channels are disallowed. When the unauthorized virtual channel list is empty, all virtual channels are allowed. The virtual channels setting applies to both agent and client. Virtual channels must be enabled on both agent and client for virtual channels to be used. The virtual channels setting provides a separate check box that allows you to disable remote clipboard processing on the PCoIP host. This value applies to the agent only. By default, all virtual channels are enabled, including clipboard processing.
`Configure the PCoIP transport header`	Configures the PCoIP transport header and sets the transport session priority. The PCoIP transport header is a 32-bit header that is added to all PCoIP UDP packets (only if the transport header is enabled and supported by both sides). The PCoIP transport header allows network devices to make better prioritization/QoS decisions when dealing with network congestion. The transport header is enabled by default. The transport session priority determines the PCoIP session priority reported in the PCoIP transport header. Network devices make better prioritization/QoS decisions based on the specified transport session priority. When the `Configure the PCoIP transport header` setting is enabled, the following transport session priorities are available: ■ **High** ■ **Medium** (default value) ■ **Low** ■ **Undefined** The transport session priority value is negotiated by the PCoIP agent and client. If the PCoIP agent specifies a transport session priority value, the session uses the agent-specified session priority. If only the client has specified a transport session priority, the session uses the client-specified session priority. If neither agent nor client has specified a transport session priority, or **Undefined Priority** is specified, the session uses the default value, **Medium** priority.

Table 5-9. PCoIP General Policy Settings (Continued)

Setting	Description
Configure the TCP port to which the PCoIP host binds and listens	Specifies the TCP agent port bound to by software PCoIP hosts. The TCP port value specifies the base TCP port that the agent attempts to bind to. The TCP port range value determines how many additional ports to try if the base port is not available. The port range must be between 1 and 10. The range spans from the base port to the sum of the base port and port range. For example, if the base port is 4172 and the port range is 10, the range spans from 4172 to 4182. Do not set the size of the retry port range to 0. Setting this value to 0 causes a connection failure when users log in to the desktop with the PCoIP display protocol. Horizon Client returns the error message, The Display protocol for this desktop is currently not available. Please contact your system administrator. This setting applies to Horizon Agent only. On single-user machines, the default base TCP port is 4172 in View 4.5 and later. The default base port is 50002 in View 4.0.*x* and earlier. By default, the port range is 1. On RDS hosts, the default base TCP port is 4173. When PCoIP is used with RDS hosts, a separate PCoIP port is used for each user connection. The default port range that is set by the Remote Desktop Service is large enough to accommodate the expected maximum of concurrent user connections. **Important** As a best practice, do not use this policy setting to change the default port range on RDS hosts, or change the TCP port value from the default of 4173. Most important, do not set the TCP port value to 4172. Resetting this value to 4172 will adversely affect PCoIP performance in RDS sessions.

Table 5-9. PCoIP General Policy Settings (Continued)

Setting	Description
Configure the UDP port to which the PCoIP host binds and listens	Specifies the UDP agent port bound to by software PCoIP hosts. The UDP port value specifies the base UDP port that the agent attempts to bind to. The UDP port range value determines how many additional ports to try if the base port is not available. The port range must be between 1 and 10. Do not set the size of the retry port range to 0. Setting this value to 0 causes a connection failure when users log in to the desktop with the PCoIP display protocol. Horizon Client returns the error message, The Display protocol for this desktop is currently not available. Please contact your system administrator. The range spans from the base port to the sum of the base port and port range. For example, if the base port is 4172 and the port range is 10, the range spans from 4172 to 4182. This setting applies to Horizon Agent only. On single-user machines, the default base UDP port is 4172 for View 4.5 and later and 50002 for View 4.0.*x* and earlier. By default, the port range is 10. On RDS hosts, the default base UDP port is 4173. When PCoIP is used with RDS hosts, a separate PCoIP port is used for each user connection. The default port range that is set by the Remote Desktop Service is large enough to accommodate the expected maximum of concurrent user connections. **Important** As a best practice, do not use this policy setting to change the default port range on RDS hosts, or change the UDP port value from the default of 4173. Most important, do not set the UDP port value to 4172. Resetting this value to 4172 will adversely affect PCoIP performance in RDS sessions.
Enable access to a PCoIP session from a vSphere console	Determines whether to allow a vSphere Client console to display an active PCoIP session and send input to the desktop. By default, when a client is attached through PCoIP, the vSphere Client console screen is blank and the console cannot send input. The default setting ensures that a malicious user cannot view the user's desktop or provide input to the host locally when a PCoIP remote session is active. This setting applies to Horizon Agent only. When this setting is disabled or not configured, console access is not allowed. When this setting is enabled, the console displays the PCoIP session and console input is allowed. When this setting is enabled, the console can display a PCoIP session that is running on a Windows 7 system only when the Windows 7 virtual machine is hardware v8. Hardware v8 is available only on ESXi 5.0 and later. By contrast, console input to a Windows 7 system is allowed when the virtual machine is any hardware version.
Enable/disable audio in the PCoIP session	Determines whether audio is enabled in PCoIP sessions. Both endpoints must have audio enabled. When this setting is enabled, PCoIP audio is allowed. When it is disabled, PCoIP audio is disabled. When this setting is not configured, audio is enabled by default.

Table 5-9. PCoIP General Policy Settings (Continued)

Setting	Description
Enable/disable microphone noise and DC offset filter in PCoIP session	Determines whether to enable the microphone noise and DC offset filter for microphone input during PCoIP sessions. This setting applies to Horizon Agent and Teradici audio driver only. When this setting is not configured, the Teradici audio driver uses the microphone noise and DC offset filter by default.
Turn on PCoIP user default input language synchronization	Determines whether the default input language for the user in the PCoIP session is synchronized with the default input language of the PCoIP client endpoint. When this setting is enabled, synchronization is allowed. When this setting is disabled or not configured, synchronization is disallowed. This setting applies to Horizon Agent only.
Configure SSL Connections to satisfy Security Tools	Specifies how SSL session negotiation connections are established. In order to satisfy port scanners, enable this 'Configure SSL connections' setting and on Horizon Agent, complete the following tasks: 1 In Microsoft Management Console, store a correctly named and signed certificate into the Personal store for the Local Machine's computer account and mark it exportable. 2 Store the certificate for the Certificate Authority that signed it in the Trusted Root certificate store. 3 Disable connections to VMware View 5.1 and earlier. 4 Configure Horizon Agent to load certificates only from the Certificate Store. If the Personal store for the Local Machine is used, leave the certificate store names unchanged as "MY" and "ROOT" (without the quotes), unless a different store location was used in steps 1 and 2. The resulting PCoIP Server will satisfy Security Tools such as port scanners.
Configure SSL Protocols	Configures the OpenSSL protocol to restrict the use of certain protocols before establishing an encrypted SSL connection. The protocol list consists of one or more openssl protocol strings separated by colons. Note that all cipher strings are case insensitive. The default value is: 'TLS1.1:TLS1.2" This means that both TLS v1.1 and TLS v1.2 are enabled (SSL v2.0, SSLv3.0 and TLS v1.0 are disabled). This setting applies to both Horizon Agent and Horizon Client. If it is set on both sides, the OpenSSL protocol negotation rule will be followed.
Configure SSL cipher list	Configures an SSL cipher list to restrict the use of cipher suites before establishing an encrypted SSL connection. The list consists of one or more cipher suite strings separated by colons. All cipher suite strings are case insensitive. The default value is ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH. If this setting is configured, the **Enforce AES-256 or stronger ciphers for SSL connection negotiation** check box in the **Configure SSL connections to satisfy Security Tools** setting is ignored. This setting must be applied to both the PCoIP server and the PCoIP client.

PCoIP Clipboard Settings

The Horizon PCoIP ADMX template file contains group policy settings that configure clipboard settings for copy-and-paste operations.

All of these settings are in the **Computer Configuration > Policies > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults** folder in the Group Policy Management Editor.

All of these settings are also in the **User Configuration > Policies > Administrative Templates > PCoIP Session Variables > Not Overridable Administrator Settings** folder in the Group Policy Management Editor.

Table 5-10. PCoIP Clipboard Policy Settings

Setting	Description
`Configure clipboard memory size on server (in kilobytes)`	Specifies the server's clipboard memory size value, in kilobytes. The client also has a value for the clipboard memory size. After the session is set up, the server sends its clipboard memory size value to the client. The effective clipboard memory size value is the lesser of the client and server clipboard memory size values. You can specify a minimum value of 512 kilobytes and a maximum value of 16384 kilobytes. If you specify 0 or do not specify a value, the default server clipboard memory size is 1024 kilobytes. This setting applies only to version 7.0.1 or later and to Windows, Linux, and Mac clients on which Horizon Client 4.1 or later is installed. In earlier releases, the clipboard memory size is 1 MB. **Note** A large clipboard memory size can negatively affect performance, depending on your network. VMware recommends that you do not set the clipboard memory size to a value greater than 16 MB.
`Configure clipboard redirection`	Determines the direction in which clipboard redirection is allowed. You can select one of these values: ■ **Enabled client to agent only** (That is, allow copy and paste only from the client system to the remote desktop.) ■ **Disabled in both directions** ■ **Enabled in both directions** ■ **Enabled agent to client only** (That is, allow copy and paste only from the remote desktop to the client system.) Clipboard redirection is implemented as a virtual channel. If virtual channels are disabled, clipboard redirection does not function. This setting applies to Horizon Agent only. When this setting is disabled or not configured, the default value is **Enabled client to agent only**.
`Filter text out of the incoming clipboard data`	Specifies whether textual data is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.

Table 5-10. PCoIP Clipboard Policy Settings (Continued)

Setting	Description
Filter Rich Text Format data out of the incoming clipboard data	Specifies whether Rich Text Format data is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter images out of the incoming clipboard data	Specifies whether image data is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Office text data out of the incoming clipboard data	Specifies whether Microsoft Office text format data (BIFF12 format) is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	Specifies whether Microsoft Office Chart and Smart Art data (Art::GVML ClipFormat) is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Text Effects data out of the incoming clipboard data	Specifies whether Microsoft Office text effects data (HTML Format) is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter text out of the outgoing clipboard data	Specifies whether textual data is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Rich Text Format data out of the outgoing clipboard data	Specifies whether Rich Text Format data is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter images out of the outgoing clipboard data	Specifies whether image data is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Office text data out of the outgoing clipboard data	Specifies whether Microsoft Office text format data (BIFF12 format) is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.

Table 5-10. PCoIP Clipboard Policy Settings (Continued)

Setting	Description
`Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data`	Specifies whether Microsoft Office Chart and Smart Art data (Art::GVML ClipFormat) is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
`Filter Microsoft Text Effects data out of the outgoing clipboard data`	Specifies whether Microsoft Office text effects data (HTML Format) is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.

PCoIP Bandwidth Settings

The Horizon PCoIP ADMX template file contains group policy settings that configure PCoIP bandwidth characteristics.

All of these settings are in the **Computer Configuration > Policies > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults** folder in the Group Policy Management Editor.

All of these settings are also in the **User Configuration > Policies > Administrative Templates > PCoIP Session Variables > Not Overridable Administrator Settings** folder in the Group Policy Management Editor.

Table 5-11. Horizon PCoIP Session Bandwidth Variables

Setting	Description
`Configure the maximum PCoIP session bandwidth`	Specifies the maximum bandwidth, in kilobits per second, in a PCoIP session. The bandwidth includes all imaging, audio, virtual channel, USB, and control PCoIP traffic. Set this value to the overall capacity of the link to which your endpoint is connected, taking into consideration the number of expected concurrent PCoIP sessions. For example, with a single-user VDI configuration (a single PCoIP session) that connects through a 4Mbit/s Internet connection, set this value to 4Mbit, or 10% less than this value to leave some allowance for other network traffic. When you expect multiple concurrent PCoIP sessions to share a link, comprising either multiple VDI users or an RDS configuration, you might want to adjust the setting accordingly. However, lowering this value will restrict the maximum bandwidth for each active session. Setting this value prevents the agent from attempting to transmit at a higher rate than the link capacity, which would cause excessive packet loss and a poorer user experience. This value is symmetric. It forces the client and agent to use the lower of the two values that are set on the client and agent side. For example, setting a 4Mbit/s maximum bandwidth forces the agent to transmit at a lower rate, even though the setting is configured on the client. When this setting is disabled or not configured on an endpoint, the endpoint imposes no bandwidth constraints. When this setting is configured, the setting is used as the endpoint's maximum bandwidth constraint in kilobits per second. The default value when this setting is not configured is 900000 kilobits per second. This setting applies to Horizon Agent and the client. If the two endpoints have different settings, the lower value is used.
`Configure the PCoIP session bandwidth floor`	Specifies a lower limit, in kilobits per second, for the bandwidth that is reserved by the PCoIP session. This setting configures the minimum expected bandwidth transmission rate for the endpoint. When you use this setting to reserve bandwidth for an endpoint, the user does not have to wait for bandwidth to become available, which improves session responsiveness. Make sure that you do not over-subscribe the total reserved bandwidth for all endpoints. Make sure that the sum of bandwidth floors for all connections in your configuration does not exceed the network capability. The default value is 0, which means that no minimum bandwidth is reserved. When this setting is disabled or not configured, no minimum bandwidth is reserved. This setting applies to Horizon Agent and the client, but the setting only affects the endpoint on which it is configured. When this setting is modified during an active PCoIP session, the change takes effect immediately.

Table 5-11. Horizon PCoIP Session Bandwidth Variables (Continued)

Setting	Description
`Configure the PCoIP session MTU`	Specifies the Maximum Transmission Unit (MTU) size for UDP packets for a PCoIP session. The MTU size includes IP and UDP packet headers. TCP uses the standard MTU discovery mechanism to set MTU and is not affected by this setting. The maximum MTU size is 1500 bytes. The minimum MTU size is 500 bytes. The default value is 1300 bytes. Typically, you do not have to change the MTU size. Change this value if you have an unusual network setup that causes PCoIP packet fragmentation. This setting applies to Horizon Agent and the client. If the two endpoints have different MTU size settings, the lowest size is used. If this setting is disabled or not configured, the client uses the default value in the negotiation with Horizon Agent.

Table 5-11. Horizon PCoIP Session Bandwidth Variables (Continued)

Setting	Description
`Configure the PCoIP session audio bandwidth limit`	Specifies the maximum bandwidth that can be used for audio (sound playback) in a PCoIP session. The audio processing monitors the bandwidth used for audio. The processing selects the audio compression algorithm that provides the best audio possible, given the current bandwidth utilization. If a bandwidth limit is set, the processing reduces quality by changing the compression algorithm selection until the bandwidth limit is reached. If minimum quality audio cannot be provided within the bandwidth limit specified, audio is disabled. To allow for uncompressed high quality stereo audio, set this value to higher than 1600 kbit/s. A value of 450 kbit/s and higher allows for stereo, high-quality, compressed audio. A value between 50 kbit/s and 450 kbit/s results in audio that ranges between FM radio and phone call quality. A value below 50 kbit/s might result in no audio playback. This setting applies to Horizon Agent only. You must enable audio on both endpoints before this setting has any effect. In addition, this setting has no effect on USB audio. If this setting is disabled or not configured, a default audio bandwidth limit of 500 kilobits per second is configured to constrain the audio compression algorithm selected. If the setting is configured, the value is measured in kilobits per second, with a default audio bandwidth limit of 500 kilobits per second. This setting applies to View 4.6 and later. It has no effect on earlier versions of View. When this setting is modified during an active PCoIP session, the change takes effect immediately.
`Turn off Build-to-Lossless feature`	Specifies whether to turn the build-to-lossless feature of the PCoIP protocol off or on. This feature is turned off by default. If this setting is enabled or not configured, the build-to-lossless feature is turned off, and images and other desktop and application content are never built to a lossless state. In network environments with constrained bandwidth, turning off the build-to-lossless feature can provide bandwidth savings. If this setting is disabled, the build-to-lossless feature is turned on. Turning on the build-to-lossless feature is recommended in environments that require images and other desktop and application content to be built to a lossless state. When this setting is modified during an active PCoIP session, the change takes effect immediately. For more information about the PCoIP build-to-lossless feature, see PCoIP Build-to-Lossless Feature.

PCoIP Keyboard Settings

The View PCoIP ADMX template file contains group policy settings that configure PCoIP settings that affect the use of the keyboard.

All of these settings are in the **Computer Configuration > Policies > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults** folder in the Group Policy Management Editor.

All of these settings are also in the **User Configuration > Policies > Administrative Templates > PCoIP Session Variables > Not Overridable Administrator Settings** folder in the Group Policy Management Editor.

Table 5-12. Horizon PCoIP Session Variables for the Keyboard

Setting	Description
`Disable sending CAD when users press Ctrl+Alt+Del`	When this policy is enabled, users must press Ctrl+Alt+Insert instead of Ctrl +Alt+Del to send a Secure Attention Sequence (SAS) to the remote desktop during a PCoIP session. You might want to enable this setting if users become confused when they press Ctrl+Alt+Del to lock the client endpoint and an SAS is sent to both the host and the guest. This setting applies to Horizon Agent only and has no effect on a client. When this policy is not configured or is disabled, users can press Ctrl+Alt+Del or Ctrl+Alt+Insert to send an SAS to the remote desktop.
`Use alternate key for sending Secure Attention Sequence`	Specifies an alternate key, instead of the Insert key, for sending a Secure Attention Sequence (SAS). You can use this setting to preserve the Ctrl+Alt+Ins key sequence in virtual machines that are launched from inside a remote desktop during a PCoIP session. For example, a user can launch a vSphere Client from inside a PCoIP desktop and open a console on a virtual machine in vCenter Server. If the Ctrl+Alt+Ins sequence is used inside the guest operating system on the vCenter Server virtual machine, a Ctrl+Alt+Del SAS is sent to the virtual machine. This setting allows the Ctrl+Alt+*Alternate Key* sequence to send a Ctrl+Alt+Del SAS to the PCoIP desktop. When this setting is enabled, you must select an alternate key from a drop-down menu. You cannot enable the setting and leave the value unspecified. When this setting is disabled or not configured, the Ctrl+Alt+Ins key sequence is used as the SAS. This setting applies to Horizon Agent only and has no effect on a client.

PCoIP Build-to-Lossless Feature

You can configure the PCoIP display protocol to use an encoding approach called progressive build, or build-to-lossless, which works to provide the optimal overall user experience even under constrained network conditions. This feature is turned off by default.

The build-to-lossless feature provides a highly compressed initial image, called a lossy image, that is then progressively built to a full lossless state. A lossless state means that the image appears with the full fidelity intended.

On a LAN, PCoIP always displays text using lossless compression. If the build-to-lossless feature is turned on, and if available bandwidth per session drops below 1Mbs, PCoIP initially displays a lossy text image and rapidly builds the image to a lossless state. This approach allows the desktop to remain responsive and display the best possible image during varying network conditions, providing an optimal experience for users.

The build-to-lossless feature provides the following characteristics:

- Dynamically adjusts image quality
- Reduces image quality on congested networks
- Maintains responsiveness by reducing screen update latency
- Resumes maximum image quality when the network is no longer congested

You can turn on the build-to-lossless feature by disabling the `Turn off Build-to-Lossless feature` group policy setting. See PCoIP Bandwidth Settings.

VMware Blast Policy Settings

The VMware Blast group policy ADMX template file `vdm_blast.admx` contains policy settings for the VMware Blast display protocol. After the policy is applied, the settings are stored in the registry key `HKLM\Software\Policies\VMware, Inc.\VMware Blast\config`.

These settings apply to HTML Access and all Horizon Clients.

Table 5-13. VMware Blast Policy Settings

Setting	Description
`Max Session Bandwidth`	Specifies the maximum bandwidth, in kilobits per second (kbps), for a VMware Blast session. The bandwidth includes all imaging, audio, virtual channel, USB, and VMware Blast control traffic. The default is 1 Gbps.
`Min Session Bandwidth`	Specifies the minimum bandwidth, in kilobits per second (kbps), that is reserved for a VMware Blast session. The default is 256 kbps.
`Max Bandwidth Slope for the Kbps Per Megapixel`	Specifies the maximum bandwidth slope, in kilobits per second (kbps), that is reserved for a VMware Blast session. The minimum value is 100. The maximum value is 100000. The default value is 6200.
`Max Frame Rate`	Specifies the maximum rate of screen updates. Use this setting to manage the average bandwidth that users consume. The default is 30 updates per second.
`UDP Protocol`	Specifies whether to use the UDP or the TCP protocol. The default is to use the UDP protocol. This setting requires a reboot of the Horizon Agent machine on which the registry key exists. This setting does not apply to HTML Access, which always uses the TCP protocol.
`H264`	Specifies whether to use H.264 encoding or JPEG/PNG encoding. The default is to use H.264 encoding.
`PNG`	If you enable or do not configure this setting, PNG encoding is available for remote sessions. If you disable this setting, only JPEG encoding is used for encoding in JPEG/PNG mode. This policy does not apply when the H.264 encoder is active. This setting is not configured by default. This setting applies to 7.0.2 and later.
`Screen Blanking`	Specifies whether to have the desktop VM's console show the actual desktop that the user sees or to show a blank screen when the desktop has an active session. The default is to show a blank screen.
`Cookie Cleanup Interval`	Determines how often, in milliseconds, cookies associated with inactive sessions are deleted. The default is 100 ms.

Table 5-13. VMware Blast Policy Settings (Continued)

Setting	Description
Image Quality	Specifies the image quality of the remote display. You can specify two low-quality settings, two high-quality settings, and a mid-quality setting. The low-quality settings are for areas of the screen that change often, for example, when scrolling occurs. The high-quality settings are for areas of the screen that are more static, resulting in a better image quality. You can specify the following settings: ■ **Low JPEG Quality** (available range of values: 1 - 100, default: 25) ■ **Low JPEG Chroma Subsampling** (available range of values: 4:1:0 (lowest), 4:1:1, 4:2:0, 4:2:2, and 4:4:4 (highest), default: 4:1:0) ■ **Mid JPEG Quality** (available range of values: 1 - 100, default: 35) ■ **High JPEG Quality** (available range of values: 1 - 100, default: 90) ■ **High JPEG Chroma Subsampling** (available range of values: 4:1:0 (lowest), 4:1:1, 4:2:0, 4:2:2, and 4:4:4 (highest), default: 4:4:4)
H.264 Quality	Specifies the image quality for the remote display configured to use H.264 encoding. You can specify the minimum and maximum quantization values that determine how much an image is controlled for lossless compression. You can specify a minimum quantization value for the best image quality. You can specify a maximum quantization value for the lowest image quality. You can specify the following settings: ■ **H264maxQP** (available range of values: 0-51, default: 36) ■ **H264minQP** (available range of values: 0-51, default: 10) For the best image quality, set the quantization values to within +5 or -5 of the available range of values.
HTTP Service	Specifies the port that is used for secure communication (HTTPS) between the security server or Access Point appliance and a desktop. The firewall must be configured to have this port open. The default is 22443.
Audio playback	Specifies whether audio playback is enabled for remote desktops. This setting is to enable audio playback.
Configure clipboard redirection	Specifies the permissible behavior for clipboard redirection. The options are: ■ **Enabled in both directions** ■ **Disabled in both directions** ■ **Enabled client to server only** (Users can copy/paste from the client to the desktop only.) ■ **Enabled server to client only** (Users can copy/paste from the desktop to the client only.) The default is **Enabled client to server only**.
Clipboard memory size on server(in kilobytes)	Specifies the server's clipboard memory size value, in kilobytes. The client also has a value for the clipboard memory size. After the session is set up, the server sends its clipboard memory size value to the client. The effective clipboard memory size value is the lesser of the client and server clipboard memory size values. You can specify a minimum value of 512 kilobytes and a maximum value of 16384 kilobytes. If you specify 0 or do not specify a value, the default server clipboard memory size is 1024 kilobytes. This setting applies only to version 7.0.1 and later and to Windows, Linux, and Mac clients on which Horizon Client 4.1 or later is installed. In earlier releases, the clipboard memory size is 1 MB. **Note** A large clipboard memory size can negatively affect performance, depending on your network. VMware recommends that you do not set the clipboard memory size to a value greater than 16 MB.

Table 5-13. VMware Blast Policy Settings (Continued)

Setting	Description
Keyboard locale synchronization	Specifies whether to synchronize a client's keyboard locale list and default keyboard locale to the remote desktop or application. If this setting is enabled, synchronization occurs. This setting applies to Horizon Agent only. **Note** This feature is supported only for Horizon Client for Windows.
Configure file transfer	Specifies the permissible behavior for file transfer between a remote desktop and the HTML Access client. You can select one of the following values: ■ **Disabled both upload and download** ■ **Enabled both upload and download** ■ **Enabled file upload only** (Users can upload files from the client system to the remote desktop only.) ■ **Enabled file download only** (Users can download files from the remote desktop to the client system only.) The default is **Enabled file upload only**. This setting applies only to version 7.0.1 and later and to HTML Access 4.1 and later.
Filter text out of the incoming clipboard data	Specifies whether textual data is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Rich Text Format data out of the incoming clipboard data	Specifies whether Rich Text Format data is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter images out of the incoming clipboard data	Specifies whether image data is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Office text data out of the incoming clipboard data	Specifies whether Microsoft Office text format data (BIFF12 format) is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	Specifies whether Microsoft Office Chart and Smart Art data (Art::GVML ClipFormat) is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Text Effects data out of the incoming clipboard data	Specifies whether Microsoft Office text effects data (HTML Format) is filtered out of the clipboard data coming from the client to the agent. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter text out of the outgoing clipboard data	Specifies whether textual data is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.

Table 5-13. VMware Blast Policy Settings (Continued)

Setting	Description
Filter Rich Text Format data out of the outgoing clipboard data	Specifies whether Rich Text Format data is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter images out of the outgoing clipboard data	Specifies whether image data is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Office text data out of the outgoing clipboard data	Specifies whether Microsoft Office text format data (BIFF12 format) is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	Specifies whether Microsoft Office Chart and Smart Art data (Art::GVML ClipFormat) is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.
Filter Microsoft Text Effects data out of the outgoing clipboard data	Specifies whether Microsoft Office text effects data (HTML Format) is filtered out of the clipboard data sent from the agent to the client. When this setting is enabled and the check box is selected, the data is filtered out. When this setting is disabled or not configured, the data is allowed. This setting applies to version 7.0.2 and later.

Applying VMware Blast Policy Settings

If the following VMware Blast policies change during a client session, Horizon Client detects the change and immediately applies the new setting.

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

For all other VMware Blast policies, Microsoft GPO update rules apply. GPOs can be updated manually or by restarting the Horizon Agent machine. For more information, see the Microsoft documentation.

Enabling Lossless Compression for VMware Blast

You can enable the VMware Blast display protocol to use an encoding approach called progressive build, or build-to-lossless. This feature provides a highly compressed initial image, called a lossy image, that is then progressively built to a full lossless state. A lossless state means that the image appears with the full fidelity intended.

To enable lossless compression for VMware Blast, set the `EncoderBuildToPNG` key to `1` in the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` folder in the Windows registry on the agent machine. The default value is `0` (disabled), which means the codec does not build to PNG, which is a lossless format.

Configuration changes to the `EncoderBuildToPNG` key take place immediately.

Note Enabling lossless compression for VMware Blast causes an increase in bandwidth and CPU usage. VMware recommends that you use the PCoIP display protocol instead of VMware Blast if you require lossless compression. For information about configuring lossless compression for PCoIP, see PCoIP Build-to-Lossless Feature.

Using Remote Desktop Services Group Policies

You can use Remote Desktop Services group policies to control the configuration and performance of RDS hosts and RDS desktop and application sessions. Horizon 7 provides an ADMX file that contains the Microsoft RDS group policies that are supported in Horizon 7.

As a best practice, configure the group policies that are provided in the Horizon 7 ADMX file rather than the corresponding Microsoft group policies. The Horizon 7 group policies are certified to support your Horizon 7 deployment.

Add the Remote Desktop Services ADMX File to Active Directory

You can add the policy settings in the Remote Desktop Services ADMX file to group policy objects (GPOs) in Active Directory.

You can also install the Remote Desktop Services ADMX file on individual RDS hosts. On an individual RDS host, you use the Local Group Policy Editor (`gpedit.msc`) to edit group policy settings.

Prerequisites

- Create GPOs for the Remote Desktop Services group policy settings and link them to the OU that contains your RDS hosts.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Management snap-in are available on your Active Directory server.

Procedure

1 Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

The file is named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADMX files that provide group policy settings for Horizon 7 are available in this file.

2 Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the Remote Desktop Services ADMX and ADML files to your Active Directory server.

a Copy the `vmware_rdsh_server.admx` file to the `C:\Windows\PolicyDefinitions` folder on your Active Directory server.

b (Optional) Copy the `vmware_rdsh_server.adml` language resource file to the appropriate subfolder in `C:\Windows\PolicyDefinitions\` on your Active Directory server.

3 On the Active Directory server, open the Group Policy Management Editor.

The Remote Desktop Services group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host** folder.

Some Remote Desktop Services group policy settings are also installed in the **User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host** folder.

4 (Optional) Configure the group policy settings in the **Remote Desktop Services > Remote Desktop Session Host** folder.

RDS Application Compatibility Settings

The RDS Application Compatibility group policy settings control Windows installer compatibility, remote desktop IP virtualization, network adapter selection, and the use of the RDS host IP address.

Table 5-14. RDS Application Compatibility Group Policy Settings

Setting	Description
`Turn off Windows Installer RDS Compatibility`	This policy setting specifies whether Windows Installer RDS Compatibility runs on a per user basis for fully installed applications. Windows Installer allows one instance of the `msiexec` process to run at a time. By default, Windows Installer RDS Compatibility is turned on. If you enable this policy setting, Windows Installer RDS Compatibility is turned off, and only one instance of the `msiexec` process can run at a time. If you disable or do not configure this policy setting, Windows Installer RDS Compatibility is turned on, and multiple per user application installation requests are queued and handled by the `msiexec` process in the order in which they are received.

`Turn on Remote Desktop IP Virtualization`	This policy setting specifies whether Remote Desktop IP Virtualization is turned on.
	By default, Remote Desktop IP Virtualization is turned off.
	If you enable this policy setting, Remote Desktop IP Virtualization is turned on. You can select the mode in which this setting is applied. If you are using Per Program mode, you must enter a list of programs to use virtual IP addresses. List each program on a separate line (do not enter any blank lines between programs). For example:
	`explorer.exe`
	`mstsc.exe`
	If you disable or do not configure this policy setting, Remote Desktop IP Virtualization is turned off.

Table 5-14. RDS Application Compatibility Group Policy Settings (Continued)

Setting	Description
Select the network adapter to be used for Remote Desktop IP Virtualization	This policy setting specifies the IP address and network mask that corresponds to the network adapter used for virtual IP addresses. The IP address and network mask should be entered in Classless Inter-Domain Routing notation. For example: 192.0.2.96/24. If you enable this policy setting, the specified IP address and network mask are used to select the network adapter used for the virtual IP addresses. If you disable or do not configure this policy setting, Remote Desktop IP Virtualization is turned off. A network adapter must be configured for Remote Desktop IP Virtualization to work.
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	This policy setting specifies whether a session uses the IP address of the RDS host if a virtual IP address is not available. If you enable this policy setting, the IP address of the RDS host is not used if a virtual IP is not available. The session will not have network connectivity. If you disable or do not configure this policy setting, the IP address of the RDS host is used if a virtual IP is not available.

RDS Connections Settings

The RDS Connections group policy settings let users set policies for connections to sessions on RDS hosts.

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections** folder.

The Horizon 7 RDS group policy settings are also installed in the **User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections** folder.

Table 5-15. RDS Connections Group Policy Settings

Setting	Description
`Automatic reconnection`	Specifies whether to allow remote desktop connection clients to automatically reconnect to sessions on an RDS host if their network link is temporarily lost. By default, a maximum of twenty reconnection attempts are made at five second intervals. If you enable this policy setting, automatic reconnection is attempted for all clients running the remote desktop connection whenever their network connection is lost. If you disable this policy setting, automatic reconnection of clients is prohibited. If you do not configure this policy setting, automatic reconnection is not specified at the Group Policy level. However, users can configure automatic reconnection using the **Reconnect if connection is dropped** checkbox on the **Experience** tab in the remote desktop connection.
`Allow users to connect remotely using Remote Desktop Services`	This policy setting configures remote access to computers using Remote Desktop Services. If you enable this policy setting, users who are members of the Remote Desktop Users group on the target computer can connect remotely to the target computer using Remote Desktop Services. If you disable this policy setting, users cannot connect remotely to the target computer using Remote Desktop Services. The target computer will maintain any current connections, but will not accept any new incoming connections. If you do not configure this policy setting, Remote Desktop Services uses the Remote Desktop setting on the target computer to determine whether remote connection is allowed. This setting is found on the **Remote** tab in **System Properties**. By default, remote connection is not allowed. **Note** You can limit which clients are able to connect remotely using Remote Desktop Services by configuring the "Require user authentication for remote connections by using Network Level Authentication" policy setting located in the **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security** folder. You can limit the number of users who can connect simultaneously by configuring the Maximum Connections option on the **Network Adapter** tab in the Remote Desktop Session Host Configuration tool or by configuring the "Limit number of connections" policy setting located in the **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections** folder.

Table 5-15. RDS Connections Group Policy Settings (Continued)

Setting	Description
Deny logoff of an administrator logged in to the console session	This policy setting determines whether an administrator attempting to connect remotely to the console of a server can log off an administrator currently logged on to the console. This policy is useful when the currently connected administrator does not want to be logged off by another administrator. If the connected administrator is logged off, any data not previously saved is lost. If you enable this policy setting, logging off the connected administrator is not allowed. If you disable or do not configure this policy setting, logging off the connected administrator is allowed. **Note** The console session is also known as Session 0. Console access can be obtained by using the `/console` switch from Remote Desktop Connection in the computer field name or from the command line.
Configure keep-alive connection interval	This policy setting allows you to enter a keep-alive interval to ensure that the session state on the RDS host is consistent with the client state. After a client loses the connection to an RDS host, the session on the RDS host might remain active instead of changing to a disconnected state, even if the client is physically disconnected from the RDS host. If the client logs on to the same RDS host again, a new session might be established (if the RDS host is configured to allow multiple sessions), and the original session might still be active. If you enable this policy setting, you must enter a keep-alive interval. The keep-alive interval determines how often, in minutes, the server checks the session state. The range of values you can enter is 1 to 999,999. If you disable or do not configure this policy setting, a keep-alive interval is not set and the server will not check the session state.

Table 5-15. RDS Connections Group Policy Settings (Continued)

Setting	Description
`Limit number of connections`	Specifies whether Remote Desktop Services limits the number of simultaneous connections to the server. You can use this setting to restrict the number of Remote Desktop Services sessions that can be active on a server. If this number is exceeded, additional users who try to connect receive an error message that states the server is busy and to try again later. Restricting the number of sessions improves performance because fewer sessions are demanding system resources. By default, RDS hosts allow an unlimited number of Remote Desktop Services sessions, and Remote Desktop for Administration allows two Remote Desktop Services sessions. To use this setting, enter the number of connections you want to specify as the maximum for the server. To specify an unlimited number of connections, type 999999. If you enable this policy setting, the maximum number of connections is limited to the specified number consistent with the version of Windows and the mode of Remote Desktop Services running on the server. If you disable or do not configure this policy setting, limits to the number of connections are not enforced at the Group Policy level. **Note** This setting is designed to be used on RDS hosts, which are servers running the Windows operating system with Remote Desktop Session Host role service installed.
`Set rules for remote control of Remote Desktop Services user sessions`	Use this policy setting to specify the level of remote control permitted in a Remote Desktop Services session. You can use this policy setting to select one of two levels of remote control: View Session or Full Control. View Session permits the remote control user to watch a session. Full Control permits the administrator to interact with the session. Remote control can be established with or without the user's permission. If you enable this policy setting, administrators can remotely interact with a user's Remote Desktop Services session according to the specified rules. To set these rules, select the desired level of control and permission in the Options list. To disable remote control, select "No remote control allowed." If you disable or do not configure this policy setting, remote control rules are determined by the setting on the **Remote Control** tab in the Remote Desktop Session Host Configuration tool. By default, remote control users have full control of the session with the user's permission. **Note** This policy setting appears in both Computer Configuration and User Configuration. If both policy settings are configured, the Computer Configuration policy setting takes precedence.

Table 5-15. RDS Connections Group Policy Settings (Continued)

Setting	Description
Restrict Remote Desktop Services users to a single Remote Desktop Services session	Use this policy setting to restrict users to a single Remote Desktop Services session. If you enable this policy setting, users who log on remotely using Remote Desktop Services will be restricted to a single session (either active or disconnected) on that server. If the user leaves the session in a disconnected state, the user automatically reconnects to that session at next logon. If you disable this policy setting, users are allowed to make unlimited simultaneous remote connections using Remote Desktop Services. If you do not configure this policy setting, the "Restrict each user to one session" setting in the Remote Desktop Session Host Configuration tool will determine if users are restricted to a single Remote Desktop Services session.
Allow remote start of unlisted programs	Use this policy setting to specify whether remote users can start any program on the RDS host when they start a Remote Desktop Services session, or whether they can only start programs that are listed in the RemoteApp Programs list. You can control which programs on an RDS host can be started remotely by using the RemoteApp Manager tool to create a list of RemoteApp programs. By default, only programs in the RemoteApp Programs list can be started when a user starts a Remote Desktop Services session. If you enable this policy setting, remote users can start any program on the RDS host when they start a Remote Desktop Services session. For example, a remote user can start any program by specifying the program's executable path at connection time by using the Remote Desktop Connection client. If you disable or do not configure this policy setting, remote users can only start programs that are listed in the RemoteApp Programs list in RemoteApp Manager when they start a Remote Desktop Services session.
Turn off Fair Share CPU Scheduling	Fair Share CPU Scheduling dynamically distributes processor time across all Remote Desktop Services sessions on the same RDS host, based on the number of sessions and the demand for processor time within each session. If you enable this policy setting, Fair Share CPU Scheduling is turned off. If you disable or do not configure this policy setting, Fair Share CPU Scheduling is turned on.

RDS Device and Resource Redirection Settings

The RDS device and resource redirection group policy settings control access to devices and resources on a client computer in Remote Desktop Services sessions.

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection** folder.

The Horizon 7 RDS group policy settings are also installed in the **User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection** folder.

Table 5-16. RDS Device and Resource Redirection Group Policy Settings

Setting	Description
Allow audio and video playback redirection	Use this policy setting to specify whether users can redirect the remote computer's audio and video output in a Remote Desktop Services session. Users can specify where to play the remote computer's audio output by configuring the remote audio settings on the Local Resources tab in Remote Desktop Connection (RDC). Users can choose to play the remote audio on the remote computer or on the local computer. Users can also choose to not play the audio. Video playback can be configured by using the videoplayback setting in a Remote Desktop Protocol (.rdp) file. By default, video playback is enabled. By default, audio and video playback redirection is not allowed when connecting to a computer running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003. Audio and video playback redirection is allowed by default when connecting to a computer running Windows 7, Windows Vista, or Windows XP Professional. If you enable this policy setting, audio and video playback redirection is allowed. If you disable this policy setting, audio and video playback redirection is not allowed, even if audio playback redirection is specified in RDC or video playback is specified in the .rdp file. If you do not configure this policy setting, the Audio and video playback setting on the Client Settings tab in the Remote Desktop Session Host Configuration tool determines whether audio and video playback redirection is allowed.
Allow audio recording redirection	Use this policy setting to specify whether users can record audio to the remote computer in a Remote Desktop Services session. Users can specify whether to record audio to the remote computer by configuring the remote audio settings on the Local Resources tab in Remote Desktop Connection (RDC). Users can record audio by using an audio input device on the local computer, such as a built-in microphone. By default, audio recording redirection is not allowed when connecting to a computer running Windows Server 2008 R2. Audio recording redirection is allowed by default when connecting to a computer running Windows 7. If you enable this policy setting, audio recording redirection is allowed. If you disable this policy setting, audio recording redirection is not allowed, even if audio recording redirection is specified in RDC. If you do not configure this policy setting, the Audio recording setting on the Client Settings tab in the Remote Desktop Session Host Configuration tool determines whether audio recording redirection is allowed.

Table 5-16. RDS Device and Resource Redirection Group Policy Settings (Continued)

Setting	Description
Limit audio playback quality	Use this policy setting to limit the audio playback quality for a Remote Desktop Services session. Limiting the quality of audio playback can improve connection performance, particularly over slow links. If you enable this policy setting, you must select one of the following: High, Medium, or Dynamic. If you select High, the audio will be sent without any compression and with minimum latency. This requires a large amount of bandwidth. If you select Medium, the audio will be sent with some compression and with minimum latency as determined by the codec that is being used. If you select Dynamic, the audio will be sent with a level of compression that is determined by the bandwidth of the remote connection. The audio playback quality that you specify on the remote computer by using this policy setting is the maximum quality that can be used for a Remote Desktop Services session, regardless of the audio playback quality configured on the client computer. For example, if the audio playback quality configured on the client computer is higher than the audio playback quality configured on the remote computer, the lower level of audio playback quality will be used. Audio playback quality can be configured on the client computer by using the audioqualitymode setting in a Remote Desktop Protocol (.rdp) file. By default, audio playback quality is set to Dynamic.
Do not allow clipboard redirection	Specifies whether to prevent the sharing of clipboard contents (clipboard redirection) between a remote computer and a client computer during a Remote Desktop Services session. You can use this setting to prevent users from redirecting clipboard data to and from the remote computer and the local computer. By default, Remote Desktop Services allows clipboard redirection. If you enable this setting, users cannot redirect clipboard data. If you disable this setting, Remote Desktop Services always allows clipboard redirection. If you do not configure this setting, clipboard redirection is not specified at the Group Policy level. However, an administrator can still disable clipboard redirection using the Remote Desktop Session Host Configuration tool.

Table 5-16. RDS Device and Resource Redirection Group Policy Settings (Continued)

Setting	Description
Do not allow COM port redirection	Specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Remote Desktop Services session. You can use this setting to prevent users from redirecting data to COM port peripherals or mapping local COM ports while they are logged on to a Remote Desktop Services session. By default, Remote Desktop Services allows this COM port redirection. If you enable this setting, users cannot redirect server data to the local COM port. If you disable this setting, Remote Desktop Services always allows COM port redirection. If you do not configure this setting, COM port redirection is not specified at the Group Policy level. However, an administrator can still disable COM port redirection using the Remote Desktop Session Host Configuration tool.
Do not allow drive redirection	Specifies whether to prevent the mapping of client drives in a Remote Desktop Services session (drive redirection). By default, an RD Session Host server maps client drives automatically upon connection. Mapped drives appear in the session folder tree in Windows Explorer or Computer in the format <driveletter> on <computername>. You can use this setting to override this behavior. If you enable this setting, client drive redirection is not allowed in Remote Desktop Services sessions. If you disable this setting, client drive redirection is always allowed. If you do not configure this setting, client drive redirection is not specified at the Group Policy level. However, an administrator can still disable client drive redirection by using the Remote Desktop Session Host Configuration tool.
Do not allow LTP Port redirection	Specifies whether to prevent the redirection of data to client LPT ports during a Remote Desktop Services session. You can use this setting to prevent users from mapping local LPT ports and redirecting data from the remote computer to local LPT port peripherals. By default, Remote Desktop Services allows this LPT port redirection. If you enable this setting, users in a Remote Desktop Services session cannot redirect server data to the local LPT port. If you disable this setting, LPT port redirection is always allowed. If you do not configure this setting, LPT port redirection is not specified at the Group Policy level. However, an administrator can still disable local LPT port redirection using the Remote Desktop Session Host Configuration tool.

Table 5-16. RDS Device and Resource Redirection Group Policy Settings (Continued)

Setting	Description
Do not allow supported Plug and Play device redirection	Use this policy setting to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Remote Desktop Services session. By default, Remote Desktop Services allows redirection of supported Plug and Play devices. Users can use the "More" option on the Local Resources tab of Remote Desktop Connection to choose the supported Plug and Play devices to redirect to the remote computer. If you enable this policy setting, users cannot redirect their supported Plug and Play devices to the remote computer. If you disable this policy setting or do not configure this policy setting, users can redirect their supported Plug and Play devices to the remote computer. **Note** You can also disallow redirection of supported Plug and Play devices on the Client Settings tab in the Remote Desktop Session Host Configuration tool. You can disallow redirection of specific types of supported Plug and Play devices by using the policy settings in the **Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions** folder.
Do not allow smart card device redirection	Use this policy setting to control the redirection of smart card devices in a Remote Desktop Services session. If you enable this policy setting, Remote Desktop Services users cannot use a smart card to log on to a Remote Desktop Services session. If you disable or do not configure this policy setting, smart card device redirection is allowed. By default, Remote Desktop Services automatically redirects smart card devices on connection. **Note** The client computer must be running at least Microsoft Windows 2000 Server or at least Microsoft Windows XP Professional and the target server must be joined to a domain.
Allow time zone redirection	This policy setting determines whether the client computer redirects its time zone settings to the Remote Desktop Services session. If you enable this policy setting, clients that are capable of time zone redirection send their time zone information to the server. The server base time is then used to calculate the current session time (current session time = server base time + client time zone). If you disable or do not configure this policy setting, the client computer does not redirect its time zone information and the session time zone is the same as the server time zone.

RDS Licensing Settings

The RDS Licensing group policy settings control the order in which RDS license servers are located, whether problem notifications are displayed, and whether Per User or Per Device licensing is used for RDS Client Access Licenses (CALs).

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Licensing** folder.

Table 5-17. RDS Licensing Group Policy Settings

Setting	Description
`Use the specified Remote Desktop license servers`	This policy setting allows you to specify the order in which an RDS host server attempts to locate Remote Desktop license severs. If you enable this policy setting, an RDS host server first attempts to locate the license servers that you specify. If the specified license servers cannot be located, the RDS host server will attempt automatic license server discovery. In the automatic license server discovery process, an RDS host server in a Windows Server-based domain attempts to contact a license server in the following order: 1 License servers that are specified in the Remote Desktop Session Host Configuration tool. 2 License servers that are published in Active Directory Domain Services. 3 License servers that are installed on domain controllers in the same domain as the RDS host. If you disable or do not configure this policy setting, the RDS host uses the license server discovery mode specified in the Remote Desktop Session Host Configuration tool.
`Hide notifications about RD Licensing problems that affect the RD Session Host server`	This policy setting determines whether notifications are displayed on an RDS host when there are problems with RD Licensing that affect the RDS host. By default, notifications are displayed on an RDS host after you log on as a local administrator, if there are problems with RD Licensing that affect the RDS host. If applicable, a notification will also be displayed that notes the number of days until the licensing grace period for the RDS host will expire. If you enable this policy setting, these notifications will not be displayed on the RDS host. If you disable or do not configure this policy setting, these notifications will be displayed on the RDS host after you log on as a local administrator.
`Set the Remote Desktop licensing mode`	This policy setting allows you to specify the type of Remote Desktop Services client access license (RDS CAL) that is required to connect to this RDS host. You can use this policy setting to select one of two licensing modes: Per User or Per Device. Per User licensing mode requires that each user account connecting to this RDS host have an RDS Per User CAL. Per Device licensing mode requires that each device connecting to this RDS host have an RDS Per Device CAL. If you enable this policy setting, the licensing mode that you specify takes precedence over the licensing mode that is specified during the installation of Remote Desktop Session Host or specified in the Remote Desktop Session Host Configuration tool. If you disable or do not configure this policy setting, the licensing mode that is specified during the installation of Remote Desktop Session Host role service or specified in the Remote Desktop Session Host Configuration tool is used.

RDS Printer Redirection Settings

The RDS Printer Redirection group policy settings let users configure policies for printer redirection.

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Printer Redirection** folder.

The Horizon 7 RDS group policy settings are also installed in the **User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Printer Redirection** folder.

Table 5-18. RDS Printer Redirection Group Policy Settings

Setting	Description
`Do not set default client printer to be default printer in a session`	Use this policy setting to specify whether the client default printer is automatically set as the default printer in a session on an RDS host. By default, Remote Desktop Services automatically designates the client default printer as the default printer in a session on an RDS host. You can use this policy setting to override this behavior. If you enable this policy setting, the default printer is the printer specified on the remote computer. If you disable this policy setting, the RDS host automatically maps the client default printer and sets it as the default printer upon connection. If you do not configure this policy setting, the default printer is not specified at the Group Policy level. However, an administrator can configure the default printer for client sessions by using the Remote Desktop Session Host Configuration tool.
`Do not allow client printer redirection`	Use this policy setting to specify whether to prevent the mapping of client printers in Remote Desktop Services sessions. You can use this policy setting to prevent users from redirecting print jobs from the remote computer to a printer attached to their local (client) computer. By default, Remote Desktop Services allows this client printer mapping. If you enable this policy setting, users cannot redirect print jobs from the remote computer to a local client printer in Remote Desktop Services sessions. If you disable this policy setting, users can redirect print jobs with client printer mapping. If you do not configure this policy setting, client printer mapping is not specified at the Group Policy level. However, an administrator can still disable client printer mapping by using the Remote Desktop Session Host Configuration tool.

Table 5-18. RDS Printer Redirection Group Policy Settings (Continued)

Setting	Description
`Use Remote Desktop Easy Print printer driver first`	Use this policy setting to specify whether the Remote Desktop Easy Print printer driver is used first to install all client printers. If you enable or do not configure this policy setting, the RDS host first tries to use the Remote Desktop Easy Print printer driver to install all client printers. If for any reason the Remote Desktop Easy Print printer driver cannot be used, a printer driver on the RDS host that matches the client printer is used. If the RDS host does not have a printer driver that matches the client printer, the client printer is not available for the Remote Desktop session. If you disable this policy setting, the RDS host tries to find a suitable printer driver to install the client printer. If the RDS host does not have a printer driver that matches the client printer, the RDS host tries to use the Remote Desktop Easy Print driver to install the client printer. If for any reason the Remote Desktop Easy Print printer driver cannot be used, the client printer is not available for the Remote Desktop Services session. **Note** If the "Do not allow client printer redirection" policy setting is enabled, the "Use Remote Desktop Easy Print printer driver first" policy setting is ignored.

Table 5-18. RDS Printer Redirection Group Policy Settings (Continued)

Setting	Description
`Specify RD Session Host Server fallback printer driver behavior`	Use this policy setting to specify the RDS host fallback printer driver behavior. By default, the RDS host fallback printer driver is disabled. If the RDS host does not have a printer driver that matches the client's printer, no printer will be available for the Remote Desktop Services session. If you enable this policy setting, the fallback printer driver is enabled, and the default behavior is for the RDS host to find a suitable printer driver. If a printer driver is not found, the client's printer is not available. You can choose to change this default behavior. The available options are: ■ `Do nothing if one is not found`. If there is a printer driver mismatch, the RDS host will attempt to find a suitable driver. If one is not found, the client's printer is not available. This is the default behavior. ■ `Default to PCL if one is not found`. If no suitable printer driver can be found, default to the Printer Control Language (PCL) fallback printer driver. ■ `Default to PS if one is not found`. If no suitable printer driver can be found, default to the PostScript (PS) fallback printer driver. ■ `Show both PCL and PS if one is not found`. If no suitable driver can be found, show both PS and PCL-based fallback printer drivers. If you disable this policy setting, the RDS host fallback driver is disabled and the RDS host will not attempt to use the fallback printer driver. If you do not configure this policy setting, the fallback printer driver behavior is off by default. **Note** If the "Do not allow client printer redirection" setting is enabled, this policy setting is ignored and the fallback printer driver is disabled.
`Redirect only the default client printer`	Use this policy setting to specify whether the default client printer is the only printer redirected in Remote Desktop Services sessions. If you enable this policy setting, only the default client printer is redirected in Remote Desktop Services sessions. If you disable or do not configure this policy setting, all client printers are redirected in Remote Desktop Services sessions.

RDS Profiles Settings

The RDS Profiles group policy settings control roaming profile and home directory settings for Remote Desktop Services sessions.

Table 5-19. RDS Profiles Group Policy Settings

Setting	Description
`Limit the size of the entire roaming user profile cache`	This policy setting allows you to limit the size of the entire roaming user profile cache on the local drive. This policy setting only applies to a computer on which the Remote Desktop Session Host role service is installed. **Note** If you want to limit the size of an individual user profile, use the `Limit profile size` policy setting located in **User Configuration\Policies\Administrative Templates\System\User Profiles**. If you enable this policy setting, you must specify a monitoring interval (in minutes) and a maximum size (in gigabytes) for the entire roaming user profile cache. The monitoring interval determines how often the size of the entire roaming user profile cache is checked. When the size of the entire roaming user profile cache exceeds the maximum size that you have specified, the oldest (least recently used) roaming user profiles will be deleted until the size of the entire roaming user profile cache is less than the maximum size specified. If you disable or do not configure this policy setting, no restriction is placed on the size of the entire roaming user profile cache on the local drive. Note: This policy setting is ignored if the `Prevent Roaming Profile changes from propagating to the server` policy setting located in **Computer Configuration\Policies\Administrative Templates\System\User Profiles** is enabled.
`Set Remote Desktop Services User Home Directory`	Specifies whether Remote Desktop Services uses the specified network share or local directory path as the root of the user's home directory for a Remote Desktop Services session. To use this setting, select the location for the home directory (network or local) from the Location drop-down list. If you choose to place the directory on a network share, type the Home Dir Root Path in the form `\\Computername\Sharename`, and then select the drive letter to which you want the network share to be mapped. If you choose to keep the home directory on the local computer, type the Home Dir Root Path in the form `Drive:\Path`, without environment variables or ellipses. Do not specify a placeholder for user alias, because Remote Desktop Services automatically appends this at logon. **Note** The Drive Letter field is ignored if you choose to specify a local path. If you choose to specify a local path but then type the name of a network share in Home Dir Root Path, Remote Desktop Services places user home directories in the network location.

Table 5-19. RDS Profiles Group Policy Settings (Continued)

Setting	Description
	If the status is set to Enabled, Remote Desktop Services creates the user's home directory in the specified location on the local computer or the network. The home directory path for each user is the specified Home Dir Root Path and the user's alias. If the status is set to Disabled or Not Configured, the user's home directory is as specified at the server.

Table 5-19. RDS Profiles Group Policy Settings (Continued)

Setting	Description
`Use mandatory profiles on the RD Session Host server`	This policy setting allows you to specify whether Remote Desktop Services uses a mandatory profile for all users connecting remotely to the RDS host. If you enable this policy setting, Remote Desktop Services uses the path specified in the `Set path for Remote Desktop Services Roaming User Profile` policy setting as the root folder for the mandatory user profile. All users connecting remotely to the RDS host use the same user profile. If you disable or do not configure this policy setting, mandatory user profiles are not used by users connecting remotely to the RDS host. **Note** For this policy setting to take effect, you must also enable and configure the `Set path for Remote Desktop Services Roaming User Profile` policy setting.
`Set path for Remote Desktop Services Roaming User Profile`	This policy setting allows you to specify the network path that Remote Desktop Services uses for roaming user profiles. By default, Remote Desktop Services stores all user profiles locally on the RDS host. You can use this policy setting to specify a network share where user profiles can be centrally stored, allowing a user to access the same profile for sessions on all RDS host that are configured to use the network share for user profiles. If you enable this policy setting, Remote Desktop Services uses the specified path as the root directory for all user profiles. The profiles are contained in subfolders named for the account name of each user. To configure this policy setting, type the path to the network share in the form of `\\Computername\Sharename`. Do not specify a placeholder for the user account name, because Remote Desktop Services automatically adds this when the user logs on and the profile is created. If the specified network share does not exist, Remote Desktop Services displays an error message on the RDS host and will store the user profiles locally on the RDS host. If you disable or do not configure this policy setting, user profiles are stored locally on the RDS host. You can configure a user's profile path on the Remote Desktop Services Profile tab on the user's account Properties dialog box. Notes: 1 The roaming user profiles enabled by the policy setting apply only to Remote Desktop Services connections. A user might also have a Windows roaming user profile configured. The Remote Desktop Services roaming user profile always takes precedence in a Remote Desktop Services session. 2 To configure a mandatory Remote Desktop Services roaming user profile for all users connecting remotely to the RDS host, use this policy setting together with the `Use mandatory profiles on the RD Session Host server` policy setting located in **Computer Configuration\Administrative**

Table 5-19. RDS Profiles Group Policy Settings (Continued)

Setting	Description
	Templates\Windows Components\Remote Desktop Services\RD Session Host\Profiles. The path set in the `Set path for Remote Desktop Services Roaming User Profile` policy setting should contain the mandatory profile.

RDS Connection Server Settings

The RDS Connection Server group policy settings let users set policies for Connection Server.

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker** folder.

Table 5-20. RDS Connection Server Group Policy Settings

Setting	Description
`Join RD Connection Broker`	Use this policy setting to specify whether the RDS host should join a farm in Connection Server that is installed on an RDS host. Connection Server on an RDS host tracks user sessions and allows a user to reconnect to their existing session in a load-balanced RDS farm. To participate in Connection Server on an RDS host, the Remote Desktop Session Host role service must be installed on the RDS host. If the policy setting is enabled, the RDS host joins the farm that is specified in the "Configure RD Connection Broker Farm Name" setting. The farm exists on the Connection Server that is specified in the "Configure RD Connection Broker Server name" policy setting. If you disable this policy setting, the RDS host does not join a farm in Connection Server, and user session tracking is not performed. If the setting is disabled, you cannot use either the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider to join the RDS host to Connection Server. If the policy setting is not configured, the setting is not specified at the Group Policy level. In this case, you can configure the RDS host to join Connection Server on the RDS host by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. **Note** 1 f you enable this setting, you must also enable the "Configure RD Connection Broker Farm Name" and "Configure RD Connection Broker Server name" policy settings, or configure these settings by using either the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. 2 For Windows Server 2008, this policy setting is supported on at least Windows Server 2008 Standard.
`Configure RD Connection Broker farm name`	Use this policy setting to specify the name of a farm to join in the Connection Server for an RDS host. Connection Server uses the farm name to determine which RDS hosts are in the same RDS farm. Therefore, you must use the same farm name for all RDS hosts in the same load-balanced farm. The farm name does not have to correspond to a name in Active Directory Domain Services. If you specify a new farm name, a new farm is created in Connection Server for the RDS host. If you specify an existing farm name, the RDS host joins that farm in the Connection Server on the RDS host. If you enable this policy setting, you must specify the name of a farm in Connection Server for the RDS host.

Table 5-20. RDS Connection Server Group Policy Settings (Continued)

Setting	Description
	If you disable or do not configure this policy setting, the farm name is not specified by Group Policy. In this case, you can adjust the farm name by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. **Note** For Windows Server 2008, this policy setting is supported on at least Windows Server 2008 Standard. This setting is not effective unless both the "Join RD Connection Broker" and the "Configure RD Connection Broker server name" settings are enabled and configured by using Group Policy, the Remote Desktop Session Host Configuration tool, or the Terminal Services WMI provider.
`Use IP Address Redirection`	Use this policy setting to specify the redirection method to use when a client device reconnects to an existing Remote Desktop Services session in a load-balanced RDS farm. This setting applies to an RDS host that is configured to use the Connection Server on an RDS host and not to the Connection Server on a remote desktop. If you enable this policy setting, a Remote Desktop Services client queries the Connection Server on the RDS host and is redirected to an existing session by using the IP address of the RDS host where the session exists. To use this redirection method, client computers must be able to connect directly by IP address to the RDS host in the farm. If you disable this policy setting, the IP address of the RDS host is not sent to the client. Instead, the IP address is embedded in a token. When a client reconnects to the load balancer, the routing token is used to redirect the client to the existing session on the correct RDS host in the farm. Only disable this setting when your network load-balancing solution supports the use of RDS host Connection Server routing tokens and you do not want clients to directly connect by IP address to the RDS host in the load-balanced farm. If you do not configure this policy setting, the "Use IP address redirection" setting in the Remote Desktop Session Host Configuration tool is used. By default, this setting in the Remote Desktop Session Host Configuration tool is enabled. **Note** For Windows Server 2008, this policy setting is supported on at least Windows Server 2008 Standard.

Table 5-20. RDS Connection Server Group Policy Settings (Continued)

Setting	Description
`Configure RD Connection Broker Server name`	Use this policy setting to specify the Connection Server that the RDS host uses to track and redirect user sessions for a load-balanced RDS farm. The specified RDS host must be running the Connection Server service. All RDS hosts in a load-balanced farm should use the same Connection Server. If you enable this policy setting, you must specify the Connection Server for the RDS host, using either its host name, IP address, or fully qualified domain name. If you specify a name or IP address for the Connection Server that is not valid, an error message is logged in Event Viewer on the RDS host. If you disable or do not configure this policy setting, you can adjust the RDS host Connection Server name or IP address by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. **Note** ■ For Windows Server 2008, this policy setting is supported on Windows Server 2008 Standard. ■ This policy setting is not effective unless the "Join RD Connection Broker" policy setting is enabled or the RDS host is configured to join the Connection Server on the RDS host by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. ■ To be an active member of a Connection Server enabled session on an RDS farm, the computer account for each RDS host in the farm must be a member of the "Session Directory Computers" local group on the Connection Server for the RDS host.
`Use RD Connection Broker load balancing`	Use this policy setting to specify whether to use the load balancing feature in Connection Server on an RDS host to balance the load between servers in an RDS farm. If you enable this policy setting, Connection Server on an RDS host redirects users who do not have an existing session to the RDS host in the farm with the fewest sessions. Redirection behavior for users with existing sessions is not affected. If the server is configured to use Connection Server on an RDS host, users who have an existing session are redirected to the RDS host where their session exists. If you disable this policy setting, users who do not have an existing session log on to the first RDS host to which they connect. If you do not configure this policy setting, you can configure the RDS host to participate in Connection Server load balancing for the RDS host by using the Remote Desktop Session Host Configuration tool or the Terminal Services WMI provider. **Note** If you enable this policy setting, you must also enable the "Join RD Connection Broker", the "Configure RD Connection Broker farm name", and the "Configure RD Connection Broker server name" policy settings.

RDS Remote Session Environment Settings

The RDS Remote Session Environment group policy settings control configuration of the user interface in Remote Desktop Services sessions.

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment** folder.

The Horizon 7 RDS group policy settings are also installed in the **User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment** folder.

Table 5-21. RDS Remote Session Environment Group Policy Settings

Setting	Description
`Limit maximum color depth`	Use this policy setting to specify the maximum color resolution (color depth) for Remote Desktop Services connections. You can use this policy setting to set a limit on the color depth of any connection using RDP. Limiting the color depth can improve connection performance, particularly over slow links, and reduce server load. If you enable this policy setting, the color depth that you specify is the maximum color depth allowed for a user's connection over RDP. The actual color depth for the connection is determined by the color support available on the client computer. If you select "Client Compatible," the highest color depth supported by the client will be used. **Note** A color depth of 24 bit is only supported on Windows XP Professional and Windows Server 2003. If you disable or do not configure this policy setting, the color depth for connections is determined by the "Limit Maximum Color Depth" setting on the Client Settings tab in the Remote Desktop Session Host Configuration tool, unless a lower level is specified by the user at the time of connection.
`Enforce Removal of Remote Desktop Wallpaper`	Specifies whether desktop wallpaper is displayed to remote clients connecting via Remote Desktop Services. You can use this setting to enforce the removal of wallpaper during a Remote Desktop Services session. By default, Windows XP Professional displays wallpaper to remote clients connecting through Remote Desktop, depending on the client configuration. For more information, see the Experience tab in the Remote Desktop Connection options. By default, servers running Windows Server 2003 do not display wallpaper to Remote Desktop Services sessions. If you enable this setting, wallpaper never appears in a Remote Desktop Services session. If you disable this setting, wallpaper might appear in a Remote Desktop Services session, depending on the client configuration. If you do not configure this setting, the default behavior applies.

Table 5-21. RDS Remote Session Environment Group Policy Settings (Continued)

Setting	Description
Configure RemoteFX	Use this policy setting to control the availability of RemoteFX on both a Remote Desktop Virtualization Host (RD Virtualization host) and an RDS host. When deployed on an RD Virtualization host, RemoteFX delivers a rich user experience by rendering content on the server by using graphics processing units (GPUs) or hardware. By default, RemoteFX for RD Virtualization Host uses server-side GPUs or hardware to deliver a rich user experience over LAN connections and RDP 7.1. When deployed on an RDS host, RemoteFX delivers a rich user experience by using a hardware-accelerated compression scheme. If you enable this policy setting, RemoteFX will be used to deliver a rich user experience over LAN connections and RDP 7.1. If you disable this policy setting, RemoteFX will be disabled. If you do not configure this policy setting, the default behavior will be used. By default, RemoteFX for RD Virtualization host is enabled and RemoteFX for RDS host is disabled.
Limit maximum display resolution	Use this policy setting to specify the maximum display resolution that can be used by each monitor used to display a Remote Desktop Services session. Limiting the resolution used to display a remote session can improve connection performance, particularly over slow links, and reduce server load. If you enable this policy setting, you must specify a resolution width and height. The resolution specified will be the maximum resolution that can be used by each monitor used to display a Remote Desktop Services session. If you disable or do not configure this policy setting, the maximum resolution that can be used by each monitor to display a Remote Desktop Services session will be determined by the values specified on the Display Settings tab in the Remote Desktop Session Host Configuration tool.
Limit maximum number of monitors	Use this policy setting to limit the number of monitors that a user can use to display a Remote Desktop Services session. Limiting the number of monitors to display a Remote Desktop Services session can improve connection performance, particularly over slow links, and reduce server load. If you enable this policy setting, you can specify the number of monitors that can be used to display a Remote Desktop Services session. You can specify a number from 1 to 10. If you disable or do not configure this policy setting, the number of monitors that can be used to display a Remote Desktop Services session is determined by the value specified in the "Maximum number of monitors per session" box on the Display Settings tab in the Remote Desktop Session Host Configuration tool.

Table 5-21. RDS Remote Session Environment Group Policy Settings (Continued)

Setting	Description
Remove "Disconnect" option from Shut Down dialog	Use this policy setting to remove the "Disconnect" option from the Shut Down Windows dialog box in Remote Desktop Services sessions. You can use this policy setting to prevent users from using this familiar method to disconnect their client from an RDS host. If you enable this policy setting, "Disconnect" does not appear as an option in the drop-down list in the Shut Down Windows dialog box. If you disable or do not configure this policy setting, "Disconnect" is not removed from the list in the Shut Down Windows dialog box. **Note** This policy setting affects only the Shut Down Windows dialog box. It does not prevent users from using other methods to disconnect from a Remote Desktop Services session. This policy setting also does not prevent disconnected sessions at the server. You can control how long a disconnected session remains active on the server by configuring the "Set time limit for disconnected sessions" policy setting in the **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > RD Session Host > Session Time Limits** folder.
Optimize visual experience when using RemoteFX	Use this policy setting to specify the visual experience that remote users will have in Remote Desktop Connection (RDC) connections that use RemoteFX. You can use this policy to balance the network bandwidth usage with the type of graphics experience that is delivered. Depending on the requirements of your users, you can reduce network bandwidth usage by reducing the screen capture rate. You can also reduce network bandwidth usage by reducing the image quality (increasing the amount of image compression that is performed). If you have a higher than average bandwidth network, you can maximize the utilization of bandwidth by selecting the highest setting for screen capture rate and the highest setting for image quality. By default, Remote Desktop Connection sessions that use RemoteFX are optimized for a balanced experience over LAN conditions. If you disable or do not configure this policy setting, Remote Desktop Connection sessions that use RemoteFX will be the same as if the medium screen capture rate and the medium image compression settings were selected (the default behavior).

Table 5-21. RDS Remote Session Environment Group Policy Settings (Continued)

Setting	Description
Set compression algorithm for RDP data	Use this policy setting to specify which Remote Desktop Protocol (RDP) compression algorithm to use. By default, servers use an RDP compression algorithm that is based on the server's hardware configuration. If you enable this policy setting, you can specify which RDP compression algorithm to use. If you select the algorithm that is optimized to use less memory, this option is less memory-intensive, but uses more network bandwidth. If you select the algorithm that is optimized to use less network bandwidth, this option uses less network bandwidth, but is more memory-intensive. Additionally, a third option is available that balances memory usage and network bandwidth. You can also choose not to use an RDP compression algorithm. Choosing not to use an RDP compression algorithm will use more network bandwidth and is only recommended if you are using a hardware device that is designed to optimize network traffic. Even if you choose not to use an RDP compression algorithm, some graphics data will still be compressed. If you disable or do not configure this policy setting, the default RDP compression algorithm will be used.
Optimize visual experience for Remote Desktop Services sessions	Use this policy setting to specify the visual experience that remote users receive in Remote Desktop Services sessions. Remote sessions on the remote computer are then optimized to support this visual experience. By default, Remote Desktop Services sessions are optimized for rich multimedia, such as applications that use Silverlight or Windows Presentation Foundation. If you enable this policy setting, you must select the visual experience for which you want to optimize Remote Desktop Services sessions. You can select either Rich multimedia or Text. If you disable or do not configure this policy setting, Remote Desktop Services sessions are optimized for rich multimedia.

Table 5-21. RDS Remote Session Environment Group Policy Settings (Continued)

Setting	Description
Start a program on connection	Configures Remote Desktop Services to run a specified program automatically upon connection. You can use this setting to specify a program to run automatically when a user logs on to a remote computer. By default, Remote Desktop Services sessions provide access to the full Windows desktop, unless otherwise specified with this setting, by the server administrator, or by the user in configuring the client connection. Enabling this setting overrides the "Start Program" settings set by the server administrator or user. The Start menu and Windows Desktop are not displayed, and when the user exits the program the session is automatically logged off. To use this setting, in Program path and file name, type the fully qualified path and file name of the executable file to be run when the user logs on. If necessary, in Working Directory, type the fully qualified path to the starting directory for the program. If you leave Working Directory blank, the program runs with its default working directory. If the specified program path, file name, or working directory is not the name of a valid directory, the RDS host connection fails with an error message. If the status is set to Enabled, Remote Desktop Services sessions automatically run the specified program and use the specified Working Directory (or the program default directory, if Working Directory is not specified) as the working directory for the program. If the status is set to Disabled or Not Configured, Remote Desktop Services sessions start with the full desktop, unless the server administrator or user specify otherwise. For more information, see the "Run these programs at user logon: policy setting in the **Computer Configuration > Administrative Templates > System > Logon** folder. **Note** This setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides the User Configuration setting.

Table 5-21. RDS Remote Session Environment Group Policy Settings (Continued)

Setting	Description
`Always show desktop on connection`	This policy setting determines whether the desktop is always displayed after a client connects to a remote computer or an initial program can run. Use this setting to require that the desktop be displayed after a client connects to a remote computer, even if an initial program is already specified in the default user profile, Remote Desktop Connection, Remote Desktop Services client, or through Group Policy. If you enable this policy setting, the desktop is always displayed when a client connects to a remote computer. This policy setting overrides any initial program policy settings. If you disable or do not configure this policy setting, an initial program can be specified that runs on the remote computer after the client connects to the remote computer. If an initial program is not specified, the desktop is always displayed on the remote computer after the client connects to the remote computer. **Note** If this policy setting is enabled, then the "Start a program on connection" policy setting is ignored.
`Allow desktop composition for remote desktop sessions`	Use this policy setting to specify whether desktop composition is allowed for remote desktop sessions. This policy setting does not apply to RemoteApp sessions. Desktop composition provides the user interface elements of Windows Aero, such as translucent windows, for remote desktop sessions. Because Windows Aero requires additional system and bandwidth resources, allowing desktop composition for remote desktop sessions can reduce connection performance, particularly over slow links, and increase the load on the remote computer. If you enable this policy setting, desktop composition will be allowed for remote desktop sessions. On the client computer, you can configure desktop composition on the Experience tab in Remote Desktop Connection (RDC) or by using the "allow desktop composition" setting in a Remote Desktop Protocol (.rdp) file. In addition, the client computer must have the necessary hardware to support Windows Aero features. **Note** Additional configuration might be necessary on the remote computer to make Windows Aero features available for remote desktop sessions. For example, the Desktop Experience feature must be installed on the remote computer, and the maximum color depth on the remote computer must be set to 32 bits per pixel. Also, the Themes service must be started on the remote computer. If you disable or do not configure this policy setting, desktop composition is not allowed for remote desktop sessions, even if desktop composition is enabled in RDC or in the .rdp file.

Table 5-21. RDS Remote Session Environment Group Policy Settings (Continued)

Setting	Description
Do not allow font smoothing	Use this policy setting to specify whether font smoothing is allowed for remote connections. Font smoothing provides ClearType functionality for a remote connection. ClearType is a technology for displaying computer fonts so that they appear clear and smooth, especially when you are using an LCD monitor. Because font smoothing requires additional bandwidth resources, not allowing font smoothing for remote connections can improve connection performance, particularly over slow links. By default, font smoothing is allowed for remote connections. You can configure font smoothing on the Experience tab in Remote Desktop Connection (RDC) or by using the "allow font smoothing" setting in a Remote Desktop Protocol (.rdp) file. If you enable this policy setting, font smoothing will not be allowed for remote connections, even if font smoothing is enabled in RDC or in the .rdp file. If you disable or do not configure this policy setting, font smoothing is allowed for remote connections.
Remove Windows Security item from Start menu	Specifies whether to remove the Windows Security item from the Settings menu on Remote Desktop clients. You can use this setting to prevent inexperienced users from logging off from Remote Desktop Services inadvertently. If the status is set to Enabled, Windows Security does not appear in Settings on the Start menu. As a result, users must type a security attention sequence, such as CTRL+ALT+END, to open the Windows Security dialog box on the client computer. If the status is set to Disabled or Not Configured, Windows Security remains in the Settings menu.

RDS Security Settings

The RDS Security group policy setting controls whether to let local administrators customize permissions.

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security** folder.

Table 5-22. RDS Security Group Policy Settings

Setting	Description
`Server Authentication Certificate Template`	Use this policy setting to specify the name of the certificate template that determines which certificate is automatically selected to authenticate an RDS host. A certificate is needed to authenticate an RDS host when SSL (TLS 1.0) is used to secure communication between a client and an RDS host during RDP connections. If you enable this policy setting, you need to specify a certificate template name. Only certificates created by using the specified certificate template will be considered when a certificate to authenticate the RDS host is automatically selected. Automatic certificate selection only occurs when a specific certificate has not been selected. If no certificate can be found that was created with the specified certificate template, the RDS host will issue a certificate enrollment request and will use the current certificate until the request is completed. If more than one certificate is found that was created with the specified certificate template, the certificate that will expire latest and that matches the current name of the RDS host will be selected. If you disable or do not configure this policy setting, a self-signed certificate will be used by default to authenticate the RDS host. You can select a specific certificate to be used to authenticate the RDS host on the General tab of the Remote Desktop Session Host Configuration tool. **Note** If you select a specific certificate to be used to authenticate the RDS host, that certificate will take precedence over this policy setting.
`Set client connection encryption level`	Specifies whether to require the use of a specific encryption level to secure communications between clients and RDS hosts during Remote Desktop Protocol (RDP) connections. If you enable this setting, all communications between clients and RDS hosts during remote connections must use the encryption method specified in this setting. By default, the encryption level is set to High. The following encryption methods are available: ■ `High`. The High setting encrypts data sent from the client to the server and from the server to the client by using strong 128-bit encryption. Use this encryption level in environments that contain only 128-bit clients (for example, clients that run Remote Desktop Connection). Clients that do not support this encryption level cannot connect to RDS host servers. ■ `Client Compatible`. The Client Compatible setting encrypts data sent between the client and the server at the maximum key strength supported by the client. Use this encryption level in environments that include clients that do not support 128-bit encryption. ■ `Low`. The Low setting encrypts only data sent from the client to the server using 56-bit encryption.

Table 5-22. RDS Security Group Policy Settings (Continued)

Setting	Description
	If you disable or do not configure this setting, the encryption level to be used for remote connections to RDS host is not enforced through Group Policy. However, you can configure a required encryption level for these connections by using the Remote Desktop Session Host Configuration tool. **Important** FIPS compliance can be configured through the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" policy setting in the **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** folder or, through the "FIPS Compliant" setting in Remote Desktop Session Host Configuration. The FIPS Compliant setting encrypts and decrypts data sent from the client to the server and from the server to the client, with the Federal Information Processing Standard (FIPS) 140-1 encryption algorithms, using Microsoft cryptographic modules. Use this encryption level when communications between clients and RDS hosts require the highest level of encryption. If FIPS compliance is already enabled through the Group Policy "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" setting, that setting overrides the encryption level specified in this Group Policy setting or in the Remote Desktop Session Host Configuration tool.
`Always prompt for password upon connection`	Specifies whether Remote Desktop Services always prompts the client for a password upon connection. You can use this setting to enforce a password prompt for users logging on to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client. By default, Remote Desktop Services allows users to automatically log on by entering a password in the Remote Desktop Connection client. If you enable this setting, users cannot automatically log on to Remote Desktop Services by supplying their passwords in the Remote Desktop Connection client. They are prompted for a password to log on. If you disable this setting, users can always log on to Remote Desktop Services automatically by supplying their passwords in the Remote Desktop Connection client. If you do not configure this setting, automatic logon is not specified at the Group Policy level. However, an administrator can still enforce password prompting by using the Remote Desktop Session Host Configuration tool.

Table 5-22. RDS Security Group Policy Settings (Continued)

Setting	Description
`Require secure RPC communication`	Specifies whether an RDS host requires secure RPC communication with all clients or allows unsecured communication. You can use this setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. If you enable this setting, Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients. If you disable this setting, Remote Desktop Services always requests security for all RPC traffic. However, unsecured communication is allowed for RPC clients that do not respond to the request. If you do not configure this setting, unsecured communication is allowed. **Note** The RPC interface is used for administering and configuring Remote Desktop Services.
`Require use of specific security layer for remote (RDP) connections`	Specifies whether to require the use of a specific security layer to secure communications between clients and RDS hosts during Remote Desktop Protocol (RDP) connections. If you enable this setting, all communications between clients and RDS hosts during remote connections must use the security method specified in this setting. The following security methods are available: ■ `Negotiate`. The Negotiate method enforces the most secure method that is supported by the client. If Transport Layer Security (TLS) version 1.0 is supported, it is used to authenticate the RDS host. If TLS is not supported, native Remote Desktop Protocol (RDP) encryption is used to secure communications, but the RDS host is not authenticated. ■ `RDP`. The RDP method uses native RDP encryption to secure communications between the client and RDS host. If you select this setting, the RDS host is not authenticated. ■ `SSL (TLS 1.0)`. The SSL method requires the use of TLS 1.0 to authenticate the RDS host. If TLS is not supported, the connection fails. If you disable or do not configure this setting, the security method to use for remote connections to RDS hosts is not enforced through Group Policy. However, you can configure a required security method for these connections by using the Remote Desktop Session Host Configuration tool.

Table 5-22. RDS Security Group Policy Settings (Continued)

Setting	Description
`Require user authentication for remote connections by using Network`	Use this policy setting to specify whether to require user authentication for remote connections to the RDS host by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RDS host. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase "Network Level Authentication supported." If you disable or do not configure this policy setting, Network Level Authentication is not required for user authentication before allowing remote connections to the RDS host. You can specify that Network Level Authentication be required for user authentication by using Remote Desktop Session Host Configuration tool or the Remote tab in System Properties. **Important** Disabling or not configuring this policy setting provides less security because user authentication will occur later in the remote connection process.
`Do not allow local administrators to customize permissions`	Specifies whether to disable the administrator rights to customize security permissions in the Remote Desktop Session Host Configuration tool. You can use this setting to prevent administrators from making changes to the user groups on the Permissions tab in the Remote Desktop Session Host Configuration tool. By default, administrators are able to make such changes. If the status is set to Enabled, the Permissions tab in the Remote Desktop Session Host Configuration tool cannot be used to customize per-connection security descriptors or to change the default security descriptors for an existing group. All of the security descriptors are Read Only. If the status is set to Disabled or Not Configured, server administrators have full Read/Write privileges to the user security descriptors on the Permissions tab in the Remote Desktop Session Host Configuration tool. **Note** The preferred method of managing user access is by adding a user to the Remote Desktop Users group.

RDS Session Time Limits

The RDS Session Time Limits group policy settings let users set policies for time limits to sessions on RDS hosts.

The Horizon 7 RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits** folder.

The Horizon 7 RDS group policy settings are also installed in the **User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits** folder.

Table 5-23. RDS Session Time Limits Group Policy Settings

Setting	Description
`Set time limit for disconnected sessions`	Use this policy setting to configure a time limit for disconnected Remote Desktop Services sessions. You can use this policy setting to specify the maximum amount of time that a disconnected session is kept active on the server. By default, Remote Desktop Services allows users to disconnect from a Remote Desktop Services session without logging off and ending the session. When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server. If you enable this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select "Never". If you have a console session, disconnected session time limits do not apply. If you disable or do not configure this policy setting, disconnected sessions are maintained for an unlimited time. You can specify time limits for disconnected sessions on the Sessions tab in the Remote Desktop Session Host Configuration tool. **Note** This policy setting appears in both Computer Configuration and User Configuration. If both policy settings are configured, the Computer Configuration policy setting takes precedence.
`Set time limit for active but idle Remote Desktop Services sessions`	Use this policy setting to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected. If you enable this policy setting, you must select the desired time limit in the Idle session limit drop-down list. Remote Desktop Services will automatically disconnect active but idle sessions after the specified amount of time. The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. If you have a console session, idle session time limits do not apply. If you disable or do not configure this policy setting, Remote Desktop Services allows sessions to remain active but idle for an unlimited time. You can specify time limits for active but idle sessions on the Sessions tab in the Remote Desktop Session Host Configuration tool.

Table 5-23. RDS Session Time Limits Group Policy Settings (Continued)

Setting	Description
	If you want Remote Desktop Services to terminate-instead of disconnect-a session when the time limit is reached, you can configure the "Terminate session when time limits are reached" policy setting in the **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits** folder. **Note** This policy setting appears in both Computer Configuration and User Configuration. If both policy settings are configured, the Computer Configuration policy setting takes precedence.
`Set time limit for active Remote Desktop Services sessions`	Use this policy setting to specify the maximum amount of time that a Remote Desktop Services session can be active before it is automatically disconnected. If you enable this policy setting, you must select the desired time limit in the Active session limit drop-down list. Remote Desktop Services will automatically disconnect active sessions after the specified amount of time. The user receives a warning two minutes before the Remote Desktop Services session disconnects, which allows the user to save open files and close programs. If you have a console session, active session time limits do not apply. If you disable or do not configure this policy setting, Remote Desktop Services allows sessions to remain active for an unlimited time. You can specify time limits for active sessions on the Sessions tab in the Remote Desktop Session Host Configuration tool. If you want Remote Desktop Services to terminate-instead of disconnect-a session when the time limit is reached, you can configure the "Terminate session when time limits are reached" policy setting in the **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits** folder. **Note** This policy setting appears in both Computer Configuration and User Configuration. If both policy settings are configured, the Computer Configuration policy setting takes precedence.

Table 5-23. RDS Session Time Limits Group Policy Settings (Continued)

Setting	Description
Terminate session when time limits are reached	Specifies whether to terminate a timed-out Remote Desktop Services session instead of disconnecting it. You can use this setting to direct Remote Desktop Services to terminate a session (that is, the user is logged off and the session is deleted from the server) after time limits for active or idle sessions are reached. By default, Remote Desktop Services disconnects sessions that reach their time limits. Time limits are set locally by the server administrator or in Group Policy. See the "Set time limit for active Remote Desktop Services sessions" and "Set time limit for active but idle Remote Desktop Services sessions" settings. If you enable this setting, Remote Desktop Services terminates any session that reaches its time-out limit. If you disable this setting, Remote Desktop Services always disconnects a timed-out session, even if specified otherwise by the server administrator. If you do not configure this setting, Remote Desktop Services disconnects a timed-out session, unless specified otherwise in local settings. **Note** This setting only applies to time-out limits that are deliberately set in the Remote Desktop Session Host Configuration tool or Group Policy Management Console, and not to time-out events that occur due to connectivity or network conditions. Also note that this setting appears in both Computer Configuration and User Configuration. If both settings are configured, the Computer Configuration setting overrides.
Set time limit for logoff of RemoteApp sessions	Use this policy setting to specify how long a user's remote application session will remain in a disconnected state before the session is logged off from the RDS host. By default, if a user closes a remote application, the session is disconnected from the RDS host. If you enable this policy setting, when a user closes a remote application, the remote application session will remain in a disconnected state until the time limit that you specify is reached. When the time limit specified is reached, the remote application session will be logged off from the RDS host. If the user starts a remote application before the time limit is reached, the user will reconnect to the disconnected session on the RDS host. If you disable or do not configure this policy setting, when a user closes a remote application, the session will be disconnected from the RDS host. **Note** This policy setting appears in both Computer Configuration and User Configuration. If both policy settings are configured, the Computer Configuration policy setting takes precedence.

RDS Temporary Folders Settings

The RDS Connections group policy settings control the creation and deletion of temporary folders for Remote Desktop Services sessions.

Table 5-24. RDS Temporary Folders Group Policy Settings

Setting	Description
`Do not delete temp folder upon exit`	Specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. You can use this setting to maintain a user's session-specific temporary folders on a remote computer, even if the user logs off from a session. By default, Remote Desktop Services deletes a user's temporary folders when the user logs off. If the status is set to Enabled, users' per-session temporary folders are retained when the user logs off from a session. If the status is set to Disabled, temporary folders are deleted when a user logs off, even if the administrator specifies otherwise in the Remote Desktop Session Host Configuration tool. If the status is set to Not Configured, Remote Desktop Services deletes the temporary folders from the remote computer at logoff, unless specified otherwise by the server administrator. **Note** This setting only takes effect if per-session temporary folders are in use on the server. That is, if you enable the "Do not use temporary folders per session" setting, this setting has no effect.
`Do not use temporary folders per session`	This policy setting allows you to prevent Remote Desktop Services from creating session-specific temporary folders. You can use this policy setting to disable the creation of separate temporary folders on a remote computer for each session. By default, Remote Desktop Services creates a separate temporary folder for each active session that a user maintains on a remote computer. These temporary folders are created on the remote computer in a Temp folder under the user's profile folder and are named with the `sessionid`. If you enable this policy setting, per-session temporary folders are not created. Instead, a user's temporary files for all sessions on the remote computer are stored in a common Temp folder under the user's profile folder on the remote computer. If you disable this policy setting, per-session temporary folders are always created, even if you specify otherwise in the Remote Desktop Session Host Configuration tool. If you do not configure this policy setting, per-session temporary folders are created unless you specify otherwise in the Remote Desktop Session Host Configuration tool.

Filtering Printers for Virtual Printing

When the virtual printing feature is enabled, users can print to any printer available on their client systems from their remote desktops and applications. You can use the **Specify a filter in redirecting client printers** agent group policy setting to prevent the virtual printing feature from redirecting specific client printers to remote desktops and applications.

The **Specify a filter in redirecting client printers** group policy setting is provided in the VMware Horizon Printer Redirection ADMX template file (`vdm_agent_printing.admx`), which is bundled in the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` file. For installation instructions, see Add the ADMX Template Files to Active Directory.

When you enable the **Specify a filter in redirecting client printers** group policy setting, you must type a filtering rule in the **Registry value name: PrinterFilterString** text box. The filtering rule is a regular expression that specifies the printers that should not be redirected (a black list). Any printer that does not match the printers in the filtering rule is redirected. By default, the filtering rule is empty, which means that all client printers are redirected.

The following table lists the attributes, operators, and wildcards that you can use in filtering rules.

Table 5-25. Supported Attributes, Operators, and Wildcards for Filtering Rules

Attributes	Operators	Wildcards
DriverName, VendorName, and PrinterName	AND, OR, and NOT	* and ?

Following are several examples of filtering rules.

```
(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e"

PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF"

PrinterName!=".*PDFCreator.*"
```

You enable the virtual printing feature when you install Horizon Agent on a virtual desktop or RDS host. For installation instructions, see the *Setting Up Virtual Desktops in Horizon 7* and *Setting Up Published Desktops and Applications in Horizon 7* documents.

Setting Up Location-Based Printing

The location-based printing feature maps printers that are physically near client systems to remote desktops, enabling users to print to their local and network printers from their remote desktops.

Location-based printing allows IT organizations to map remote desktops to the printer that is closest to the endpoint client device. For example, as a doctor moves from room to room in a hospital, each time the doctor prints a document, the print job is sent to the nearest printer.

The location-based printing feature is available for Windows, Mac, Linux, and mobile client devices.

Location-based printing is supported on the following remote desktops and applications:

- Desktops that are deployed on single-user machines, including Windows Desktop and Windows Server machines
- Desktops that are deployed on RDS hosts, where the RDS hosts are virtual machines
- Published applications
- Published applications that are launched from Horizon Client inside remote desktops

To use the location-based printing feature, you must install the Virtual Printing setup option with Horizon Agent and install the correct printer drivers on the desktop.

You set up location-based printing by configuring the Active Directory group policy setting `AutoConnect Map Additional Printers for VMware View`, which is located in the Microsoft Group Policy Object Editor in the **Software Settings** folder under **Computer Configuration**.

Note `AutoConnect Map Additional Printers for VMware View` is a computer-specific policy. Computer-specific policies apply to all remote desktops, regardless of who connects to the desktop.

`AutoConnect Map Additional Printers for VMware View` is implemented as a name translation table. You use each row in the table to identify a specific printer and define a set of translation rules for that printer. The translation rules determine whether the printer is mapped to the remote desktop for a particular client system.

When a user connects to a remote desktop, Horizon 7 compares the client system to the translation rules associated with each printer in the table. If the client system meets all of the translation rules set for a printer, or if a printer has no associated translation rules, Horizon 7 maps the printer to the remote desktop during the user's session.

You can define translation rules based on the client system's IP address, name, and MAC address, and on the user's name and group. You can specify one translation rule, or a combination of several translation rules, for a specific printer.

The information used to map the printer to the remote desktop is stored in a registry entry on the remote desktop in `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`.

Printer Settings for Location-Based Printing

Printer settings for location-based printers are retained after a user logs out or disconnects from the desktop. For example, a user might set a location-based printer to use black and white mode. After the user logs out and logs in to the desktop again, the location-based printer continues to use black and white mode.

To save printer settings across sessions in a published application, the user must select a location-based printer from the application's print dialog box, right-click the selected printer, and select **Printing Preferences**. Printer settings are not saved if the user selects a printer and clicks the **Preferences** button in the application's print dialog box.

Persistent settings for location-based printers are not supported if the settings are saved in the printer driver's private space and not in the DEVMODE extended part of the printer driver, as recommended by Microsoft. To support persistent settings, deploy printers that have the settings saved in the DEVMODE part of the printer driver.

Register the Location-Based Printing Group Policy DLL File

Before you can configure the group policy setting for location-based printing, you must register the DLL file `TPVMGPoACmap.dll`.

The 32-bit and 64-bit versions of `TPVMGPoACmap.dll` are available in a bundled `.zip` file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. You can download the file from the VMware download site at http://www.vmware.com/go/downloadview.

Procedure

1. Copy the appropriate version of `TPVMGPoACmap.dll` to your Active Directory server or to the domain computer that you use to configure group policies.
2. Use the `regsvr32` utility to register the `TPVMGPoACmap.dll` file.

   For example: `regsvr32 "C:\TPVMGPoACmap.dll"`

What to do next

Configure the group policy setting for location-based printing.

Configure the Location-Based Printing Group Policy

To set up location-based printing, you configure the `AutoConnect Map Additional Printers for VMware View` group policy setting. The group policy setting is a name translation table that maps printers to Horizon desktops.

Prerequisites

- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server or on the domain computer that you use to configure group policies.
- Register the DLL file `TPVMGPoACmap.dll` on your Active Directory server or on the domain computer that you use to configure group policies. See Register the Location-Based Printing Group Policy DLL File.
- Familiarize yourself with syntax of the `AutoConnect Map Additional Printers for VMware View` group policy setting. See Location-Based Printing Group Policy Setting Syntax.
- Create a GPO for the location-based group policy setting and link it to the OU that contains your Horizon desktops. See Create GPOs for Horizon 7 Group Policies for an example of how to create GPOs for Horizon group policies.

- Verify that the Virtual Printing setup option was installed with Horizon Agent on your desktops. To verify, check if the TP AutoConnect Service and TP VC Gateway Service are installed in the desktop operating system.
- Because print jobs are sent directly from the Horizon desktop to the printer, verify that the required printer drivers are installed on your desktops.

Procedure

1 On the Active Directory server, edit the GPO.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click the OU that contains your Horizon desktops and select **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d In the right pane, right-click the GPO that you created for the location-based printing group policy setting and select **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click the GPO that you created for the location-based printing group policy setting and select **Edit**.

The **Group Policy Object Editor** window appears.

2 Expand **Computer Configuration**, open the **Software Settings** folder, and select **AutoConnect Map Additional Printers for VMware View**.

3 In the Policy pane, double-click **Configure AutoConnect Map Additional Printers**.

The **AutoConnect Map Additional Printers for VMware View** window appears.

4 Select **Enabled** to enable the group policy setting.

The translation table headings and buttons appear in the group policy window.

Important Clicking **Disabled** deletes all table entries. As a precaution, save your configuration so that you can import it later.

5 Add the printers that you want to map to Horizon desktops and define their associated translation rules.

6 Click **OK** to save your changes.

Location-Based Printing Group Policy Setting Syntax

You use the `AutoConnect Map Additional Printers for VMware View` group policy setting to map printers to remote desktops.

`AutoConnect Map Additional Printers for VMware View` is a name translation table that identifies printers and defines associated translation rules. Table 5-26 describes the syntax of the translation table.

Location-based printing maps local printers to remote desktops but does not support mapping network printers that are configured by using UNC paths.

Table 5-26. Translation Table Columns and Values

Column	Description
IP Range	A translation rule that specifies a range of IP addresses for client systems. To specify IP addresses in a specific range, use the following notation: ***ip_address*-*ip_address*** For example: **10.112.116.0-10.112.119.255** To specify all of the IP addresses in a specific subnet, use the following notation: *ip_address*/*subnet_mask_bits* For example: **10.112.4.0/22** This notation specifies the usable IPv4 addresses from 10.112.4.1 to 10.112.7.254. Type an asterisk to match any IP address.
Client Name	A translation rule that specifies a computer name. For example: **Mary's Computer** Type an asterisk to match any computer name.
Mac Address	A translation rule that specifies a MAC address. In the GPO editor, you must use the same format that the client system uses. For example: ■ Windows clients use hyphens: **01-23-45-67-89-ab** ■ Linux clients use colons: **01:23:45:67:89:ab** Type an asterisk to match any MAC address.
User/Group	A translation rule that specifies a user or group name. To specify a particular user or group, use the following notation: *domain**user_or_group* For example: **\\mydomain\Mary** The Fully Qualified Domain Name (FQDN) is not supported notation for the domain name. Type an asterisk to match any user or group name.
Printer Name	The name of the printer when it is mapped to the remote desktop. For example: **PRINTER-2-CLR** The mapped name does not have to match the printer name on the client system. The printer must be local to the client device. Mapping a network printer in a UNC path is not supported.
Printer Driver	The name of the driver that the printer uses. For example: **HP Color LaserJet 4700 PS** **Important** Because print jobs are sent directly from the desktop to the printer, the printer driver must be installed on the desktop.

Table 5-26. Translation Table Columns and Values (Continued)

Column	Description
IP Port/ThinPrint Port	For network printers, the IP address of the printer prepended with **IP_**. For example: **IP_10.114.24.1** The default port is 9100. You can specify a non-default port by appending the port number to the IP address. For example: **IP_10.114.24.1:9104**
Default	Indicates whether the printer is the default printer.

You use the buttons that appear above the column headings to add, delete, and move rows and save and import table entries. Each button has an equivalent keyboard shortcut. Mouse over each button to see a description of the button and its equivalent keyboard shortcut. For example, to insert a row at the end of the table, click the first table button or press Alt+A. Click the last two buttons to import and save table entries.

Table 5-27 shows an example of two translation table rows.

Table 5-27. Location-Based Printing Group Policy Setting Example

IP Range	Client Name	Mac Address	User/ Group	Printer Name	Printer Driver	IP Port/ThinPrint Port	Default
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10 .112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

The network printer specified in the first row will be mapped to a remote desktop for any client system because asterisks appear in all of the translation rule columns. The network printer specified in the second row will be mapped to a remote desktop only if the client system has an IP address in the range 10.112.116.140 through 10.112.116.145.

Active Directory Group Policy Example

One way to implement Active Directory group policies in Horizon 7 is to create an OU for the machines that deliver remote desktop sessions and link one or more GPOs to that OU. You can use these GPOs to apply group policy settings to your Horizon 7 machines.

You can link GPOs directly to a domain if the policy settings apply to all computers in the domain. As a best practice, however, most deployments should link GPOs to individual OUs to avoid policy processing on all computers in the domain.

You can configure policies on your Active Directory Server or on any computer in your domain. This example shows how to configure policies directly on your Active Directory server.

Note Because every Horizon 7 environment is different, you might need to perform different steps to meet your organization's specific needs.

Create an OU for Horizon 7 Machines

To apply group policies to the machines that deliver remote desktop sessions without affecting other Windows computers in the same Active Directory domain, create an OU specifically for your Horizon 7 machines. You might create one OU for your entire Horizon 7 deployment, or create separate OUs for virtual desktop machines and RDS hosts.

Procedure

1. On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the domain that contains your Horizon 7 machines and select **New > Organizational Unit**.
3. Type a name for the OU and click **OK**.

   The new OU appears in the left pane.
4. Add Horizon 7 machines to the new OU.
   a. Click **Computers** in the left pane.

      All the computer objects in the domain appear in the right pane.
   b. Right-click the name of the computer object that represents the Horizon 7 machine in the right panel and select **Move**.
   c. Select the OU and click **OK**.

      The Horizon 7 machine appears in the right pane when you select the OU.

What to do next

Create GPOs for Horizon 7 group policies.

Create GPOs for Horizon 7 Group Policies

Create GPOs to contain group policies for Horizon 7 components and location-based printing and link them to the OU for your Horizon 7 machines.

Prerequisites

- Create an OU for your Horizon 7 machines.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Management snap-in are available on your Active Directory server.

Procedure

1. On the Active Directory server, open the Group Policy Management Console.

2 Expand your domain, right-click the OU that contains your Horizon 7 machines, and select **Create a GPO in this domain, and Link it here**.

3 Type a name for the GPO and click **OK**.

The new GPO appears under the OU in the left pane.

4 (Optional) Apply the GPO to specific Horizon 7 machines in the OU.

a Select the GPO in the left pane.

b Select **Security Filtering > Add**.

c Type the computer names of the Horizon 7 machines and click **OK**.

The Horizon 7 machines appear in the Security Filtering pane. The settings in the GPO apply only to these machines.

What to do next

Add the Horizon ADMX templates to the GPO.

Add a Horizon 7 ADMX Template File to a GPO

To apply Horizon 7 component group policy settings to your desktops and applications, add their ADMX template files to GPOs.

Prerequisites

- Create GPOs for the Horizon 7 component group policy settings and link them to the OU that contains your Horizon 7 machines.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Management snap-in are available on your Active Directory server.

Procedure

1 Download the Horizon 7 GPO Bundle `.zip` file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Under Desktop & End-User Computing, select the VMware Horizon 7 download, which includes the GPO Bundle.

The file is named `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. All ADMX files that provide group policy settings for Horizon 7 are available in this file.

2 Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the ADMX files to your Active Directory server.

   a Copy the `.admx` files and the `en-US` folder to the `%systemroot%\PolicyDefinitions` folder on your Active Directory server.

   b Copy the language resource (`.adml`) files to the appropriate subfolder in `%systemroot%\PolicyDefinitions\` on your Active Directory server.

3 On the Active Directory server, open the Group Policy Management Editor and enter the path to the template files where they appear in the editor after installation.

What to do next

Configure the group policy settings and enable loopback processing for your Horizon 7 machines.

Enable Loopback Processing for Remote Desktops

To make User Configuration settings that usually apply to a computer apply to all of the users that log in to that computer, enable loopback processing.

Prerequisites

- Create GPOs for the Horizon 7 component group policy settings and link them to the OU that contains your Horizon 7 machines.
- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Management snap-in are available on your Active Directory server.

Procedure

1 On the Active Directory server, open the Group Policy Management Console.

2 Expand your domain, right-click the GPO that you created for the group policy settings, and select **Edit**.

3 In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates: Policy definitions > System > Group Policy**.

4 In the right pane, double-click **User Group Policy loopback processing mode**.

5 Select **Enabled** and then select a loopback processing mode from the **Mode** drop-down menu.

Option	Action
Merge	The user policy settings applied are the combination of those included in both the computer and user GPOs. Where conflicts exist, the computer GPOs take precedence.
Replace	The user policy is defined entirely from the GPOs associated with the computer. Any GPOs associated with the user are ignored.

6 Click **OK** to save your changes.