

# Configuring Remote Desktop Features in Horizon

VMware Horizon 2106

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

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

<b>1</b>	<b>Configuring Remote Desktop Features in Horizon</b>	<b>8</b>
<b>2</b>	<b>Configuring Remote Desktop Features</b>	<b>9</b>
	Configuring Unity Touch	10
	System Requirements for Unity Touch	10
	Configure Favorite Applications Displayed by Unity Touch	10
	Configuring HTML5 Multimedia Redirection	13
	System Requirements for HTML5 Multimedia Redirection	13
	Install and Configure HTML5 Multimedia Redirection	14
	Install the VMware Horizon HTML5 Redirection Extension for Google Chrome	16
	Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge	18
	Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge (Chromium)	18
	HTML5 Multimedia Redirection Limitations	20
	Configuring Browser Redirection	21
	System Requirements for Browser Redirection	21
	Install and Configure Browser Redirection	22
	Install the VMware Horizon Browser Redirection Extension for Chrome	26
	Install the VMware Horizon Browser Redirection Extension for Edge (Chromium)	28
	Browser Redirection Limitations	29
	Configuring Geolocation Redirection	30
	System Requirements for Geolocation Redirection	30
	Install and Configure Geolocation Redirection	31
	Enable the VMware Horizon Geolocation Redirection Plugin for Internet Explorer	33
	Install the VMware Horizon Geolocation Redirection Extension for Chrome	34
	Install the VMware Horizon Geolocation Redirection Extension for Microsoft Edge (Chromium)	35
	Geolocation Redirection Limitations	37
	Configuring Real-Time Audio-Video	37
	Configuration Choices for Real-Time Audio-Video	38
	System Requirements for Real-Time Audio-Video	38
	Ensuring That Real-Time Audio-Video Is Used Instead of USB Redirection	39
	Selecting Preferred Webcams and Microphones	40
	Configuring Real-Time Audio-Video Group Policy Settings	40
	Real-Time Audio-Video Bandwidth	44
	Configuring Microsoft Teams with Real-Time Audio-Video	44
	Configuring Media Optimization for Microsoft Teams	45
	Configuring Scanner Redirection	50

- System Requirements for Scanner Redirection 51
- User Operation of Scanner Redirection 52
- Configuring Scanner Redirection Group Policy Settings 53
- Configuring Serial Port Redirection 54
  - System Requirements for Serial Port Redirection 55
  - User Operation of Serial Port Redirection 57
  - Guidelines for Configuring Serial Port Redirection 58
  - Configuring Serial Port Redirection Group Policy Settings 59
  - Configure USB to Serial Adapters 60
- Managing Access to Windows Media Multimedia Redirection (MMR) 61
  - Enabling Multimedia Redirection in Horizon 61
  - System Requirements for Windows Media MMR 62
  - Use Windows Media MMR Based on Network Latency 62
- Managing Access to Client Drive Redirection 63
  - Using Client Drive Redirection in a Unified Access Gateway Implementation 64
  - Use Group Policy to Disable Client Drive Redirection 64
  - Use Group Policy to Configure Drive Letter Behavior 65
  - Use Registry Settings to Configure Client Drive Redirection 66
- Configuring the Drag and Drop Feature 68
- Configuring the Clipboard Redirection Feature 68
  - Restricting Clipboard Formats for Copy and Paste Operations 69
- Configuring Simple Device Orientation (SDO) Sensor Redirection 70
- Configuring Pen Redirection 71
- Configuring a Digital Watermark 72
- Configuring Session Collaboration 72
- Configuring VMware Virtualization Pack for Skype for Business 74
  - Collect Logs to Troubleshoot Skype for Business 78
- Configuring VMware Integrated Printing 79
- Setting Up Location-Based Printing 82
  - Install the Location-Based Printing User Interface 82
  - Configure Location-Based Printing 83
  - Location-Based Printing Translation Table Syntax 85
- Configuring Windows Registry Settings for Cursor Event Handling 87

### **3** Configuring URL Content Redirection 88

- Understanding URL Content Redirection 88
- Using URL Content Redirection in a Cloud Pod Architecture Environment 89
- System Requirements for URL Content Redirection 89
- Configuring Agent-to-Client Redirection 91
  - Installing Horizon Agent with the URL Content Redirection Feature Enabled 92
  - Add the URL Content Redirection ADMX Template to a GPO 92

- URL Content Redirection Group Policy Settings 93
- Syntax for URL Content Redirection Rules 96
- Regular Expression Rules That URL Content Redirection Supports 97
- Agent-to-Client Redirection Group Policy Example 99
- Configuring Client-to-Agent Redirection 100
  - Using the vdmutil Command-Line Utility on a Connection Server Instance 101
  - Syntax for the --agentURLPattern Option 103
  - Create a Local URL Content Redirection Setting 103
  - Create a Global URL Content Redirection Setting 105
  - Assign a URL Content Redirection Setting to a User or Group 107
  - Installing Horizon Client for Windows with the URL Content Redirection Feature Enabled 108
  - Test a URL Content Redirection Setting 109
  - Managing URL Content Redirection Settings 111
  - Using Group Policy Settings to Configure Client-to-Agent Redirection 112
- Installing Browser Extensions for URL Content Redirection 112
  - Install and Enable the URL Content Redirection Helper Extension for Chrome on Windows 113
  - Install the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on Windows 114
  - Enable the URL Content Redirection Helper for Chrome on a Mac 115
  - Install and Enable the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on a Mac 115
  - Install and Enable the VMware Horizon URL Redirection Extension for Firefox on Linux 116
  - Install and Enable the VMware Horizon URL Content Redirection Helper for Chrome on Linux 117
  - Using Internet Explorer (IE) Mode in Microsoft Edge (Chromium) with URL Content Redirection 118
- URL Content Redirection Limitations 119
- Unsupported URL Content Redirection Features 120

## **4 Using USB Devices with Remote Desktops and Applications 122**

- Limitations Regarding USB Device Types 123
- USB Redirection Recommendations 124
- Overview of Setting Up USB Redirection 124
- Configuring USB Redirection for Google Chrome, Microsoft Edge, and HTML Access Clients 126
- Configuring Fingerprint Scanner and Microscope Redirection 126
- Configuring Card Reader Redirection 127
- Configuring Microsoft Xbox One Controller Redirection 128
- Network Traffic and USB Redirection 128
  - Enabling the USB Over Session Enhancement SDK Feature 129
- Automatic Connections to USB Devices 129
- Deploying USB Devices in a Secure VMware Horizon Environment 130

- Disabling USB Redirection for All Types of Devices 131
- Disabling USB Redirection for Specific Devices 132
- Using Log Files for Troubleshooting and to Determine USB Device IDs 133
- Using Policies to Control USB Redirection 134
  - Configuring Device Splitting Policy Settings for Composite USB Devices 135
  - Configuring Filter Policy Settings for USB Devices 137
- USB Device Families 141
- USB Settings in the Horizon Agent Configuration ADMX Template 142
- Troubleshooting USB Redirection Problems 147

## 5 Configuring Policies for Desktop and Application Pools 149

- Setting Policies in Horizon Console 149
  - Horizon Policies 150
  - Configure Global Policy Settings 151
- Using Smart Policies 151
  - Requirements for Smart Policies 151
  - Installing Dynamic Environment Manager 152
  - Configuring Dynamic Environment Manager 152
  - Horizon Smart Policy Settings 153
  - Bandwidth Profile Reference 153
  - Adding Conditions to Horizon Smart Policy Definitions 154
  - Create a Horizon Smart Policy in Dynamic Environment Manager 157
- Using Active Directory Group Policies 158
  - Creating an OU for Remote Desktops 159
  - Enabling Loopback Processing for Remote Desktops 159
- Using Horizon Group Policy Administrative Template Files 159
- Horizon ADMX Template Files 160
- Add the ADMX Template Files to Active Directory 161
- VMware View Agent Configuration ADMX Template Settings 162
  - Client System Information Sent to Remote Desktops 187
  - Running Commands on Horizon Desktops 193
- Client Drive Redirection Policy Settings 193
- VMware HTML5 Feature Policy Settings 195
- VMware Virtualization Pack for Skype for Business Policy Settings 200
- VMware Integrated Printing Policy Settings 202
- PCoIP Policy Settings 205
  - PCoIP General Settings 206
  - PCoIP Bandwidth Settings 215
  - PCoIP Keyboard Settings 218
  - PCoIP Build-to-Lossless Feature 219
- VMware Blast Policy Settings 220

- Enabling Lossless Compression for VMware Blast 223
- Managing Special Unity Windows 223
- Active Directory Group Policy Example 225
  - Create an OU for Horizon Machines 225
  - Create GPOs for Horizon Group Policies 226
  - Add a Horizon ADMX Template File to a GPO 227
  - Enable Loopback Processing for Remote Desktops 227
- 6 Setting Desktop Policies with Start Session Scripts 229**
  - Obtaining Input Data for a Start Session Script 229
  - Best Practices for Using Start Session Scripts 229
  - Preparing a Horizon Desktop to Use a Start Session Script 230
    - Enable the VMware Horizon View Script Host Service 231
    - Add Windows Registry Entries for a Start Session Script 231
  - Sample Start Session Scripts 233
- 7 Examining PCoIP Session Statistics with WMI 235**
  - Using PCoIP Session Statistics 235
  - General PCoIP Session Statistics 236
  - PCoIP Audio Statistics 237
  - PCoIP Imaging Statistics 238
  - PCoIP Network Statistics 239
  - PCoIP USB Statistics 240
  - Examples of Using PowerShell cmdlets to Examine PCoIP Statistics 241

# Configuring Remote Desktop Features in Horizon

# 1

*Configuring Remote Desktop Features in Horizon* describes how to configure remote desktop features that are installed with Horizon Agent on virtual 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 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 VMware Horizon releases. You can configure these features to enhance the remote desktop experience for your end users.

These features include HTML Access, Unity Touch, HTML5 Multimedia Redirection, Geolocation Redirection, Real-Time Audio-Video, Windows Media Multimedia Redirection (MMR), USB Redirection, Scanner Redirection, Serial Port Redirection, Fingerprint Scanner Redirection, Session Collaboration, Skype for Business, and URL Content Redirection.

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 chapter includes the following topics:

- [Configuring Unity Touch](#)
- [Configuring HTML5 Multimedia Redirection](#)
- [Configuring Browser Redirection](#)
- [Configuring Geolocation Redirection](#)
- [Configuring Real-Time Audio-Video](#)
- [Configuring Microsoft Teams with Real-Time Audio-Video](#)
- [Configuring Media Optimization for Microsoft Teams](#)
- [Configuring Scanner Redirection](#)
- [Configuring Serial Port Redirection](#)
- [Managing Access to Windows Media Multimedia Redirection \(MMR\)](#)
- [Managing Access to Client Drive Redirection](#)
- [Configuring the Drag and Drop Feature](#)
- [Configuring the Clipboard Redirection Feature](#)
- [Configuring Simple Device Orientation \(SDO\) Sensor Redirection](#)

- [Configuring Pen Redirection](#)
- [Configuring a Digital Watermark](#)
- [Configuring Session Collaboration](#)
- [Configuring VMware Virtualization Pack for Skype for Business](#)
- [Configuring VMware Integrated Printing](#)
- [Setting Up Location-Based Printing](#)
- [Configuring Windows Registry Settings for Cursor Event Handling](#)

## 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`).

For information about the end user features provided by Unity Touch, see the Horizon Client documentation for iOS and Android devices.

## 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.

### Remote desktop

- Install the Unity Touch feature in Horizon Agent. For information, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.
- Supported operating systems include Windows 10 64-bit, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019.

### Horizon Client software

- Unity Touch is supported in Horizon Client for iOS and Horizon Client for Android.
- For the supported operating system versions, see the Horizon Client documentation for iOS and for Android devices.

## Configure Favorite Applications Displayed by Unity Touch

With the Unity Touch feature, tablet and smart phone users can quickly navigate to a remote 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 remote 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-Horizon-Agent-x86-YYMM-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-Horizon-Agent-x86-YYMM-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-Horizon-Agent-x86-YYMM-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 HTML5 Multimedia Redirection

With HTML5 Multimedia Redirection, when an end user uses a HTML5 Multimedia Redirection-supported browser in a remote desktop, 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

- The HTML5 Multimedia Redirection group policy settings must be configured on the Active Directory server. See [Install and Configure HTML5 Multimedia Redirection](#).
- The Google Chrome, Microsoft Edge, or Microsoft Edge (Chromium) browser must be installed.

- The VMware Horizon HTML5 Multimedia Redirection extension must be installed in the browser. See [Install the VMware Horizon HTML5 Redirection Extension for Google Chrome](#), [Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge](#), or [Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge \(Chromium\)](#).

### Client system

- For Windows client systems, Horizon Client for Windows must be installed with the Support for HTML5 Multimedia Redirection and Browser Redirection 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.
- For Linux client systems, Horizon Client for Linux 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 Linux Installation and Setup Guide*

### Display protocol for the remote session

- PCoIP
- VMware Blast

### TCP port

HTML5 Multimedia Redirection uses port 9427.

## 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 the Google Chrome, Microsoft Edge, or Microsoft Edge (Chromium) 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](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 VMware View 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 Google Chrome, Microsoft Edge, or Microsoft Edge (Chromium) browser on the remote desktop.
- 2 On your Active Directory server, open the Group Policy Management Editor.
- 3 Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features** folder.
- 4 Open the **Enable VMware HTML5 Features** setting, select **Enabled**, and click **OK**.
- 5 Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware HTML5 Multimedia Redirection** folder.
- 6 Open the **Enable VMware HTML5 Multimedia Redirection** setting, select **Enabled**, and click **OK**.
- 7 To enable the HTML5 Multimedia Redirection feature for the Google Chrome browser, perform these steps.
  - a Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware HTML5 Multimedia Redirection** folder.
  - b Open the **Enable Chrome Browser for VMware HTML5 Multimedia Redirection**, select **Enabled**, and click **OK**.
- 8 To enable the HTML5 Multimedia Redirection feature for the Microsoft Edge browser, perform these steps.
  - a Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware HTML5 Multimedia Redirection** folder.
  - b Open the **Enable legacy version of Microsoft Edge Browser for VMware HTML5 Multimedia Redirection** setting, select **Enabled**, and click **OK**.

- c Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features** folder.
  - d Open the **Disable Automatically Detect Intranet** setting, select **Enabled**, and click **OK**.
- 9 To enable the HTML5 Multimedia Redirection feature for the Microsoft Edge (Chromium) browser, perform these steps.
- a Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware HTML5 Multimedia Redirection** folder.
  - b Open the **Enable Microsoft Edge (Chromium) Browser for VMware HTML5 Multimedia Redirection** setting, select **Enabled**, and click **OK**.
- 10 Specify which websites can use the HTML5 Multimedia Redirection feature.
- a Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware HTML5 Multimedia Redirection** folder.
  - b Open the **Enable URL list for VMware HTML5 Multimedia Redirection** setting and select **Enabled**.
  - c 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.
  - d Click **OK** to save the URL list and then click **OK** to save the policy setting.

#### What to do next

Install the VMware Horizon HTML5 Redirection Extension in the browser on the remote desktop. See [Install the VMware Horizon HTML5 Redirection Extension for Google Chrome](#), [Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge](#), or [Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge \(Chromium\)](#).

## Install the VMware Horizon HTML5 Redirection Extension for Google Chrome

To use the HTML5 Multimedia Redirection feature with the Google Chrome browser, you must install the VMware Horizon HTML5 Redirection extension on the remote desktop. You can install the extension from the Chrome Web Store. Alternatively, you can install the extension silently, without user interaction, by using group policy.

To apply the Google 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](#).
- If you plan to use group policy, verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server and make sure that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.

## Procedure

- 1 To install the extension from the Chrome Web Store, perform these steps.
  - a Connect to the remote desktop.
  - b In the Chrome browser, download and install <https://chrome.google.com/webstore/detail/vmware-horizon-html5-redi/ljmaegmnepbjgkghdfkgegbckolmcok> from the Chrome Web Store.
- 2 To install the extension silently, perform these steps to download and install the ADMX and ADML files.
  - a Download the Google Chrome `policy_templates.zip` file from [https://dl.google.com/dl/edgedl/chrome/policy/policy\\_templates.zip](https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip).
  - b 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.
  - c Copy the `chrome.admx` file to the `%systemroot%\PolicyDefinitions` folder on your Active Directory server.
  - d 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 To configure the Chrome group policy, perform these steps.
  - a On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > Google Chrome > Extensions** folder.
  - b Open the **Configure the list of force-installed apps and extensions** policy setting and click **Enabled**.
  - c Click **Show** and enter `ljmaegmnepbjgkghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx` in the Value column.
  - d Click **OK** to save the extension ID/update URL and click **OK** to save the policy setting.

- 4 Verify that the HTML5 Multimedia Redirection extension is installed on the remote desktop.
  - a Connect to the remote desktop and start the Google Chrome browser.
  - b Type **chrome://extensions** in the Google Chrome address bar.

**VMware Horizon HTML5 Redirection Extension** appears in the Extensions list.

## Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge

To use the HTML5 Multimedia Redirection feature with the Microsoft Edge browser, you must install the VMware Horizon HTML5 Redirection Extension for Edge extension from Microsoft Store on the remote desktop.

For information about installing the extension for the Microsoft Edge (Chromium) browser, see [Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge \(Chromium\)](#).

### Prerequisites

Configure the HTML5 Multimedia Redirection feature. See [Install and Configure HTML5 Multimedia Redirection](#).

### Procedure

- 1 Connect to the remote desktop.
- 2 In the Microsoft Edge browser, download and install the **VMware Horizon HTML5 Redirection Extension for Edge** extension from Microsoft Store.

### Results

After you install the extension, the **VMware HTML5 Multimedia Redirection** icon appears in the upper-right corner of the Microsoft Edge browser window. When the HTML5 Multimedia Redirection feature is working, the letters REDR appear over the icon.

## Install the VMware Horizon HTML5 Redirection Extension for Microsoft Edge (Chromium)

To use the HTML5 Multimedia Redirection feature with the Microsoft Edge (Chromium) browser, you must install the VMware Horizon HTML5 Redirection extension on the remote desktop. You can install the extension from the Chrome Web Store. Alternatively, you can install the extension silently, without user interaction, by using Microsoft Edge policy.

### Prerequisites

- Configure the HTML5 Multimedia Redirection feature. See [Install and Configure HTML5 Multimedia Redirection](#).
- Verify that the Microsoft Edge (Chromium) browser allows extensions from other stores. For information about how to configure this feature, see the Microsoft documentation.

- If you plan to configure Microsoft Edge (Chromium) policy, verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server and make sure that the MMC and the Group Policy Object Editor snap-in are available.

For the most up-to-date information about Microsoft Edge (Chromium) features and policy, see the Microsoft documentation.

### Procedure

- 1 To install the extension from the Chrome Web Store, perform these steps.
  - a Connect to the remote desktop.
  - b In the Microsoft Edge (Chromium) browser, download and install <https://chrome.google.com/webstore/detail/vmware-horizon-html5-redi/ljmaegmnepbgjekghdfkgegbckolmcok> from the Chrome Web Store.
- 2 To install the extension silently, perform these steps to download and install the Microsoft Edge ADMX and ADML files.
  - a Download the MicrosoftEdgePolicyTemplates.cab file from <https://www.microsoft.com/en-us/edge/business/download>.
  - b Unzip the MicrosoftEdgePolicyTemplates.cab file and copy the msedge.admx and msedge.adml files to your Active Directory server.
 

After extracting the MicrosoftEdgePolicyTemplates.cab file, the msedge.admx file is in the \windows\admx folder and the msedge.adml file is in the \windows\admx\language folder.
  - c Copy the msedge.admx file to the %systemroot%\PolicyDefinitions folder on your Active Directory server.
  - d Copy the msedge.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 msedge.adml file to the %systemroot%\PolicyDefinitions\en\_us subfolder on your Active Directory server.
- 3 To configure Microsoft Edge policy, perform these steps.
  - a On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Extensions** folder.
  - b Open the **Control which extensions are installed silently** policy setting and click **Enable**.
  - c Click **Show** and enter **ljmaegmnepbgjekghdfkgegbckolmcok;https://clients2.google.com/service/update2/crx** in the **Value** column.

- 4 Verify that the HTML5 Multimedia Redirection extension is installed on the remote desktop.
  - a Connect to the remote desktop and start the Microsoft Edge (Chromium) browser.
  - b Enter **edge://extensions** in the address bar.

**VMware Horizon HTML5 Redirection Extension** appears in the Extensions list.

## Results

After you install the extension, the **VMware HTML5 Multimedia Redirection** icon appears in the upper-right corner of the Microsoft Edge (Chromium) browser window. When the HTML5 Multimedia Redirection feature is working, the letters REDR appear over the icon.

## HTML5 Multimedia Redirection Limitations

The HTML5 Multimedia Redirection feature has certain limitations.

- HTML5 Multimedia Redirection does not support 360 videos. The HTML5 Multimedia Redirection extension icon is marked with the REDR badge, even though the video is not supported.
- The HTML5 Multimedia Redirection feature cannot redirect HTML multimedia content from `http://huffingtonpost.com`. The HTML5 Multimedia Redirection feature can redirect HTML5 multimedia content from `http://www.yahoo.com`, but you might see a Page Unresponsive message.
- If you include the URL of a Microsoft Edge trusted site in the list of websites in the **Enable URL list for VMware HTML5 Multimedia Redirection** group policy setting, HTML5 Multimedia Redirection does not work for that URL. You can avoid this limitation by making the host less secure by running the command **CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge\_8wekyb3d8bbwe"**.
- With the Microsoft Edge browser, the HTML5 Multimedia Redirection feature cannot redirect HTML multimedia content from websites that use the m3u8 video format, such as `ted.com`.
- When the **Scanner Redirection** setup option is enabled in Horizon Agent in a remote desktop, the VMware Horizon HTML5 Redirection Extension for Edge extension sometimes crashes after the Microsoft Edge browser is launched in the remote desktop. This problem typically occurs in large-monitor environments and under stress.
- If a user plays an HTML5 video that uses a static video URL in a remote desktop, their client machine does not have access to the static URL and the playback falls back to the remote desktop.
- Bullet comments in video are not supported when using the HTML5 Multimedia Redirection feature.
- The Horizon Client relative mouse feature is not supported.
- You cannot use **Mute site** (Chrome browser) or **Mute tab** (Edge browser) to mute redirected video content.

- To use HTML5 Multimedia Redirection from Chrome on a Linux client system, open at most one Chrome browser published by an RDS host. HTML5 Multimedia Redirection does not work properly if you open an additional Chrome browser published by another RDS host.
- If you encounter slow performance when playing redirected multimedia content on a Linux client system that uses lower-capacity thin client hardware, you can optimize the system performance as described here. Add the entry `disableGPU.html5mmr=true` to one of the following three configuration files. The configuration files are processed in the listed order:
  - a `/usr/lib/vmware/config`
  - b `/etc/vmware/config`
  - c `~/.vmware/config`
- IE mode for Microsoft Edge (Chromium) is not supported with this feature. Websites that are enabled for IE mode can be opened in the Microsoft Edge (Chromium) browser with IE mode, but HTML5 Multimedia Redirection content is not redirected to Horizon Client by the HTML5 Multimedia Redirection extension for Microsoft Edge (Chromium).

## Configuring Browser Redirection

With Browser Redirection, when an end user uses a Browser Redirection-supported browser in a remote desktop, the website is rendered on the client system instead of the agent system, and it is displayed over the remote browser's viewport. The viewport is the portion of the browser window that displays the content of a web page.

## System Requirements for Browser Redirection

The remote desktops and client systems on which you install the agent and client software must meet certain requirements to support the Browser Redirection feature.

### Remote desktops

- The VMware Browser Redirection group policy settings must be configured on the Active Directory server.
- The Chrome browser or Microsoft Edge (Chromium) browser must be installed.
- The VMware Horizon Browser Redirection extension must be installed in the browser.

### Client system

Only Windows client systems are supported.

Horizon Client for Windows must be installed with the Support for HTML5 Multimedia Redirection and Browser Redirection 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.

### Display protocol for the remote session

- PCoIP
- VMware Blast

## Install and Configure Browser Redirection

Installing and configuring the Browser Redirection feature involves installing the Google Chrome or Microsoft Edge (Chromium) browser, enabling the Browser Redirection feature on the agent machine, and specifying the URLs for redirection.

Optionally, you can specify the URLs that users can navigate to from redirected URLs and customize fallback behavior for white list violations. You can also configure client-side group policy settings for microphone and camera use, certificate error handling, and browser cache storage.

To enable Browser Redirection and specify the URLs for redirection, you must configure agent-side group policy settings on your Active Directory server. Compile a list of the URLs for websites that can be redirected and, optionally, for the websites that users can navigate to from redirected URLs. Include the **http://** or **https://** prefix in the URLs. You can use match patterns in the URLs. For example, to redirect all Yahoo content, enter **https://www.yahoo.com/\***. For more information, see [https://developer.chrome.com/extensions/match\\_patterns](https://developer.chrome.com/extensions/match_patterns).

### 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 VMware View 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. If you plan to configure any of the optional client-side group policy settings, also add the Horizon Client Configuration ADMX template file (`vdm_client.admx`). For installation instructions, see [Add the ADMX Template Files to Active Directory](#).
- Compile a list of URLs for websites that can use the Browser Redirection feature.

### Procedure

- 1 Install the Google Chrome or Microsoft Edge (Chromium) browser on the remote desktop.
- 2 On your Active Directory server, open the Group Policy Management Editor.
- 3 Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features** folder.
- 4 Open the **Enable VMware HTML5 Features** setting, select **Enabled**, and click **OK**.

- 5 Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware Browser Redirection** folder.
- 6 Open the **Enable VMware Browser Redirection** setting, select **Enabled**, and click **OK**.
- 7 To enable the Browser Redirection feature for the Google Chrome browser, perform these steps.
  - a Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware Browser Redirection** folder
  - b Open the **Enable VMware Browser Redirection for Chrome Browser**, select **Enabled**, and click **OK**.
- 8 To enable the Browser Redirection feature for the Microsoft Edge (Chromium) browser, perform these steps.
  - a Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware Browser Redirection** folder
  - b Open the **Enable VMware Browser Redirection feature for Microsoft Edge (Chromium) Browser**, select **Enabled**, and click **OK**.
- 9 Specify the URLs for the Browser Redirection feature.

Users can visit these URLs by entering them in either the Chrome address bar or the custom address bar. Users can also visit these URLs by navigating to them starting from another URL in the list, or from any agent-side rendered page. Only the URLs that you specify are redirected. No URLs are added by default.

  - a Open the **Enable URL list for VMware Browser Redirection** setting and select **Enabled**.
  - b Click **Show**, enter the URLs in the Value name column, and click **OK**.

Leave the Value column blank.
  - c To save the policy setting, click **OK**.

## 10 (Optional) Configure one or more of the optional agent-side group policy settings.

The following table describes the optional agent-side group policy settings.

Option	Description
<b>Enable Navigation URL list for VMware Browser Redirection</b>	<p>You can use this setting to specify the URLs that a user is allowed to navigate to from a URL specified in the <b>Enable URL list for VMware Browser Redirection</b> list, either by entering the URL directly in the custom address bar, or by navigating to the URL starting from a URL specified in the list.</p> <p>Users cannot visit these URLs directly by entering them into the Chrome address bar or by navigating to them from an agent-side rendered page.</p> <p>To specify the URLs, click <b>Show</b>, enter the URLs in the Value name column, and click <b>OK</b>. Leave the Value column blank.</p>
<b>Enable automatic fallback after a whitelist violation</b>	<p>When you enable this setting, if a user navigates to a URL that is not specified in one of the Browser Redirection white lists, either by entering it in the custom address bar or by navigating to it starting from a URL in either white list, redirection stops for that tab and the URL is fetched and displayed on the agent instead.</p> <p><b>Note</b> If a user attempts to navigate to a URL that is not specified in the <b>Enable URL list for VMware Browser Redirection</b> setting, the tab always falls back to fetching and rendering the URL on the agent, regardless of whether this setting is enabled.</p>
<b>Show a page with error information before automatic fallback</b>	<p>When you enable this setting, and a white list violation occurs, a page appears that shows a five-second count down. After five seconds have elapsed, the tab falls back to fetching and rendering the URL that caused the violation on the agent. If this setting is disabled, the five-second warning page does not appear. This setting takes effect only if the <b>Enable automatic fallback after a whitelist violation</b> setting is also enabled.</p>

## 11 (Optional) To configure one or more of the optional client-side group policy settings, navigate to the **Computer Configuration > Policies > Administrative Templates > VMware Horizon Client Configuration > VMware Browser Redirection** folder.

The following table describes the client-side group policy settings.

Option	Description
<b>Enable WebRTC camera and microphone access for browser redirection</b>	<p>When you enable this setting, redirected pages that use WebRTC have access to the client system's camera and microphone. This setting is enabled by default.</p>
<b>Ignore certificate errors for browser redirection</b>	<p>When you enable this setting, certificate errors that occur in a redirected page are ignored and browsing proceeds. This setting is disabled by default.</p>
<b>Enable cache for browser redirection</b>	<p>When you enable this setting, the browsing history, including cookies, is stored on the client system. This setting is enabled by default.</p> <p><b>Note</b> Disabling this setting does not clear the cache. If you disable and then re-enable this setting, the cache is reused.</p>



**Example**

https://play.google.com and https://news.google.com have a common sign-in page, https://accounts.google.com.

In following example, https://play.google.com/\* and https://accounts.google.com/\* are included in **Enable URL list for VMware Browser Redirection**. The following table describes the behavior that occurs in this scenario.

<p>A user visits https://play.google.com</p>	<ul style="list-style-type: none"> <li>■ https://play.google.com is redirected to the client machine.</li> <li>■ When the user signs in, https://accounts.google.com opens on the client machine and the user authenticates on the client machine.</li> <li>■ After successful authentication, the website redirects back to https://play.google.com on the client machine and the user is logged in correctly.</li> </ul>
<p>A user visits https://news.google.com</p>	<ul style="list-style-type: none"> <li>■ https://news.google.com is rendered on the agent machine.</li> <li>■ When the user signs in, https://accounts.google.com is redirected to the client machine and the user authenticates on the client machine.</li> <li>■ After successful authentication, the user is not logged in correctly because https://news.google.com is rendered on the agent machine, but authentication occurred on the client machine.</li> </ul>
<p>A user opens https://accounts.google.com directly in the address bar</p>	<p>https://accounts.google.com is redirected to the client machine.</p>

In the next example, https://play.google.com/\* is included in **Enable URL list for VMware Browser Redirection** and https://accounts.google.com/\* is included in **Enable Navigation URL list for VMware Browser Redirection**. The following table describes the behavior that occurs in this scenario.

<p>A user visits <a href="https://play.google.com">https://play.google.com</a></p>	<ul style="list-style-type: none"> <li>■ <a href="https://play.google.com">https://play.google.com</a> is redirected to the client machine.</li> <li>■ When the user signs in, <a href="https://accounts.google.com">https://accounts.google.com</a> opens on the client machine and the user authenticates on the client machine.</li> <li>■ After successful authentication, the website redirects back to <a href="https://play.google.com">https://play.google.com</a> on the client machine and the user is logged in correctly.</li> </ul>
<p>A user visits <a href="https://news.google.com">https://news.google.com</a></p>	<ul style="list-style-type: none"> <li>■ <a href="https://news.google.com">https://news.google.com</a> is rendered on the agent machine.</li> <li>■ When the user signs in, <a href="https://accounts.google.com">https://accounts.google.com</a> is rendered on the agent machine and the user authenticates on the agent machine.</li> <li>■ After successful authentication, the website redirects back to <a href="https://news.google.com">https://news.google.com</a> on the agent machine and the user is logged in correctly.</li> </ul>
<p>A user opens <a href="https://accounts.google.com">https://accounts.google.com</a> directly in the address bar</p>	<p><a href="https://accounts.google.com">https://accounts.google.com</a> is rendered on the agent machine.</p>

**What to do next**

[Install the VMware Horizon Browser Redirection Extension for Chrome .](#)

## Install the VMware Horizon Browser Redirection Extension for Chrome

To use the Browser Redirection feature with the Chrome browser, you must install the VMware Horizon Browser Redirection extension on the remote desktop. You can install the extension from the Chrome Web Store. Alternatively, you can install the extension silently, without user interaction, by using group policy.

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 Browser Redirection feature. See [Install and Configure Browser Redirection](#).
- If you plan to use group policy, verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server and make sure that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.

## Procedure

- 1 To install the extension from the Chrome Web Store, perform these steps.
  - a Connect to remote desktop.
  - b In the Chrome browser, download and install <https://chrome.google.com/webstore/detail/vmware-horizon-browser-re/demgbalbngngkkgjcofhdiipjblblob?hl> from the Chrome Web Store.
  
- 2 To install the extension silently, perform these steps to download and install the ADMX and ADML files.
  - a Download the Google Chrome `policy_templates.zip` file from [https://dl.google.com/dl/edgedl/chrome/policy/policy\\_templates.zip](https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip).
  - b 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.
  - c Copy the `chrome.admx` file to the `%systemroot%\PolicyDefinitions` folder on your Active Directory server.
  - d 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 To configure Chrome group policy, perform these steps.
  - a On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > Google Chrome > Extensions** folder.
  - b Click **Show** and type `demgbalbngngkkgjcofhdiipjblblob;https://clients2.google.com/service/update2/crx` in the Value column.
  - c Open the **Configure the list of force-installed apps and extensions** policy setting and click **Enabled**.
  - d Click **OK** to save the extension ID/update URL and then click **OK** to save the policy setting.
  
- 4 Verify that the VMware Horizon Browser 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 Browser Redirection** appears in the Extensions list.

## Install the VMware Horizon Browser Redirection Extension for Edge (Chromium)

To use the Browser Redirection feature with the Microsoft Edge (Chromium) browser, you must install the VMware Horizon Browser Redirection extension on the remote desktop. You can install the extension from the Chrome Web Store. Alternatively, you can install the extension silently, without user interaction, by using Microsoft Edge policy.

### Prerequisites

- Configure the Browser Redirection feature. See [Install and Configure Browser Redirection](#).
- Verify that the Microsoft Edge (Chromium) browser allows extensions from other stores. For information about how to configure this feature, see the Microsoft documentation.
- If you plan to configure Microsoft Edge (Chromium) policy, verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server and make sure that the MMC and the Group Policy Object Editor snap-in are available.

For the most up-to-date information about Microsoft Edge (Chromium) features and policy, see the Microsoft documentation.

### Procedure

- 1 To install the extension from the Chrome Web Store, perform these steps.
  - a Connect to the remote desktop.
  - b In the Microsoft Edge (Chromium) browser, download and install <https://chrome.google.com/webstore/detail/vmware-horizon-browser-re/demgbalbngngkgjcofhdiipjblblob?hl> from the Chrome Web Store.
- 2 To install the extension silently, perform these steps to download and install the Microsoft Edge ADMX and ADML files.
  - a Download the `MicrosoftEdgePolicyTemplates.cab` file from <https://www.microsoft.com/en-us/edge/business/download>.
  - b Unzip the `MicrosoftEdgePolicyTemplates.cab` file and copy the `msedge.admx` and `msedge.adml` files to your Active Directory server.

After extracting the `MicrosoftEdgePolicyTemplates.cab` file, the `msedge.admx` file is in the `\windows\admx` folder and the `msedge.adml` file is in the `\windows\admx\language` folder.
  - c Copy the `msedge.admx` file to the `%systemroot%\PolicyDefinitions` folder on your Active Directory server.
  - d Copy the `msedge.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 `msedge.adml` file to the `%systemroot%\PolicyDefinitions\en_us` subfolder on your Active Directory server.

- 3 To configure Microsoft Edge policy, perform these steps.
  - a On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Extensions** folder.
  - b Open the **Control which extensions are installed silently** policy setting and click **Enable**.
  - c Click **Show** and enter **demgbalbngngkkgjcofhdiipjblblob;https://clients2.google.com/service/update2/crx** in the **Value** column.
- 4 Verify that the Browser Redirection extension is installed on the remote desktop.
  - a Connect to the remote desktop and start the Microsoft Edge (Chromium) browser.
  - b Enter **edge://extensions** in the address bar.

**VMware Horizon Browser Redirection** appears in the Installed extensions list.

## Browser Redirection Limitations

The Browser Redirection feature has certain limitations.

- The Browser Redirection feature is supported only with Windows clients.
- Only the VMware Blast and PCoIP display protocols are supported with the Browser Redirection feature. The RDP protocol is not supported.
- The Browser Redirection feature does not work with the following other VMware Horizon redirection features:
  - URL Content Redirection.
  - If the VMware Horizon Browser Redirection extension and the HTML5 Multimedia Redirection extension are both installed, and group policy settings are configured correctly for both features, only Browser Redirection works.
  - Geolocation Redirection. If both features are configured, Browser Redirection takes precedence.
- The Browser Redirection feature does not work if you start the browser by using a run command, such as **chrome url**, click a URL inside an editor, or drag a bookmark item from the **Bookmarks** menu to the remote desktop and double-click the shortcut icon.
- Protocols other than http and https, such as mailto, are not supported with the Browser Redirection feature.
- When using the Browser Redirection feature, you might encounter the following browser-related limitations.
  - Pop-up windows always open in a new tab.
  - Permissions-related pop-up windows do not appear.
  - You cannot drag a link on the redirected viewport to the address bar.

- You cannot download a file or save an image.
- You cannot save passwords for websites that require authentication.
- To close a tab, shift focus to the tab on the browser. Pressing Alt+F4, Ctrl+F4, or Ctrl+W while the focus is on the viewport can result in unexpected behavior.
- Clearing browser data, including cookies, has no effect.
- Sometimes, you cannot go back or forward to the previous page.
- Screen sharing is not supported with the Browser Redirection feature.
- Google account sign is not supported with the Browser Redirection feature. If you use a Google account to sign in with the Browser Redirection feature, "The browser or app may not be secure" error occurs. The Browser Redirection feature uses the Chromium Embedded Framework (CEF), and Google blocks all sign-ins to Google accounts from embedded browser frameworks.
- IE mode for Microsoft Edge (Chromium) is not supported with this feature. Websites that are enabled for IE mode can be opened in the Microsoft Edge (Chromium) browser with IE mode, but content is not redirected to Horizon Client by the Browser Redirection extension for Microsoft Edge (Chromium).

## Configuring Geolocation Redirection

With the Geolocation Redirection feature, remote desktops and published applications can use the client device's geolocation information.

### System Requirements for Geolocation Redirection

Horizon Agent and Horizon Client, and the virtual desktop or RDS host and client machine on which you install the agent and client software, must meet certain requirements to support the Geolocation Redirection feature.

#### Virtual desktop or RDS host

- The Windows **Location service** setting must be **On** in **Settings > Privacy > Location**.
- The Geolocation Redirection feature supports the following remote desktop applications.

Application	Platform
Google Chrome (latest version)	All virtual desktops or RDS hosts
Internet Explorer 11	All virtual desktops or RDS hosts
Microsoft Edge (Chromium)	All virtual desktops or RDS hosts
Microsoft Edge, Maps, Weather, and other Win32 and UWP apps	Windows 10

The **Location** permission setting, if any, must be enabled individually in each supported browser.

- Horizon Agent must be installed with the Geolocation 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* and *Setting Up Published Desktops and Applications in Horizon* documents.
- The VMware Geolocation Redirection group policy settings must be configured on the Active Directory server. See [Install and Configure Geolocation Redirection](#).
- For Internet Explorer 11, the VMware Horizon Geolocation Redirection IE Plugin must be enabled for RDS hosts. See [Enable the VMware Horizon Geolocation Redirection Plugin for Internet Explorer](#). You do not need to enable the VMware Horizon Geolocation Redirection IE plugin for Windows 10 virtual desktops. Internet Explorer is supported on Windows 10 virtual desktops with the VMware Geolocation Redirection driver.
- For Chrome and Microsoft Edge (Chromium), the VMware Horizon Geolocation Redirection Chrome extension must be installed on the remote desktop. See [Install the VMware Horizon Geolocation Redirection Extension for Chrome](#) and [Install the VMware Horizon Geolocation Redirection Extension for Microsoft Edge \(Chromium\)](#).

### Client system

- Install Horizon Client for Windows on a Windows client system. Non-Windows clients are not supported. For information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.
- Share the client system's location information by configuring the **Geolocation** settings in Horizon Client for Windows.
- For Windows 10 client systems, the Windows **Location service** setting must be **On** in **Settings > Privacy > Location** for Horizon to access your location.

### Display protocol for the remote session

- PCoIP
- VMware Blast

## Install and Configure Geolocation Redirection

Redirecting geolocation information from the client device to remote desktops or published applications requires enabling the Geolocation Redirection feature on the agent machine, configuring group policy settings on your Active Directory server, and specifying which websites use this feature.

To enable the Geolocation Redirection feature and specify which websites use this feature, you must configure group policy settings on your Active Directory server. You must compile a list of URLs for websites that can use the redirected geolocation information. Include the `http://` or `https://` prefix in the URLs. You can use match patterns in the URLs.

For example, specify `https://www.google.com/maps*` or `https://mycurrentlocation.net/*`. For more information, see [https://developer.chrome.com/extensions/match\\_patterns](https://developer.chrome.com/extensions/match_patterns).

## Prerequisites

- Install Horizon Client on the client system and install Horizon Agent in the virtual desktop or RDS host with the Geolocation Redirection feature enabled. For required versions, setup options, and complete system requirements, see [System Requirements for Geolocation 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 Group Policy Object Editor snap-in are available on your Active Directory server.
- Add the VMware View Agent Configuration ADMX template file (`vdm_agent.admx`) to a GPO that is linked to the OU for the virtual desktop or RDS host. For installation instructions, see [Add the ADMX Template Files to Active Directory](#).
- Compile a list of URLs for websites that can use the redirected geolocation information.
- Install a supported browser on the agent machine. See [System Requirements for Geolocation Redirection](#).

## Procedure

- 1 On your Active Directory server, open the Group Policy Management Editor.
- 2 Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features** folder.
- 3 Open the **Disable Automatically Detect Intranet** setting, select **Enabled**, and click **OK**.
- 4 Open the **Enable VMware HTML5 Features** setting, select **Enabled**, and click **OK**.
- 5 Navigate to the **Computer Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware Geolocation Redirection** folder.
- 6 Open the **Enable VMware Geolocation Redirection** setting and select **Enabled**.
- 7 Open the **Enable URL List for VMware Geolocation Redirection** setting, select **Enabled**, and specify which websites can use the Geolocation Redirection feature.

The VMware Horizon Geolocation Redirection extension uses this website list in all RDS host and virtual desktop environments. The VMware Horizon Geolocation Redirection IE plugin uses this website list in RDS host and Windows 7 virtual desktop environments.

- a Click **Show** and enter the URLs that you compiled in the **Value name** column.

Only the URLs that you specify can use the redirected geolocation information. No URLs are added by default. Leave the Value column blank.

- b Click **OK** to save the URL list and then click **OK** to save the policy setting.



- 8 Open the **Set the minimum distance for which to report location updates** setting, select **Enabled**, and specify the minimum distance (in meters), between a location update in the client and the last update reported to the agent. for which the new location must be updated.  
By default, the minimum distance is 75 meters.
- 9 To use the Geolocation Redirection feature with the Google Chrome browser, open the **Enable VMware Geolocation Redirection for Chrome Browser** setting and select **Enabled**
- 10 To use the Geolocation Redirection feature with the Microsoft Edge (Chromium) browser, open the **Enable VMware Geolocation Redirection for Microsoft Edge (Chromium)** setting and select **Enabled**.

#### What to do next

If you installed Internet Explorer on an RDS host agent machine, you must also enable the VMware Horizon Geolocation Redirection IE plugin. For information, see [Enable the VMware Horizon Geolocation Redirection Plugin for Internet Explorer](#).

---

**Note** Internet Explorer is supported on Windows 10 virtual desktops with the VMware Geolocation Redirection driver. You do not need to enable the VMware Horizon Geolocation Redirection IE plugin for Windows 10 virtual desktops.

---

To use the Geolocation Redirection feature in Google Chrome on a remote desktop, see [Install the VMware Horizon Geolocation Redirection Extension for Chrome](#). To use the Geolocation Redirection feature in Microsoft Edge (Chromium) on a remote desktop, see [Install the VMware Horizon Geolocation Redirection Extension for Microsoft Edge \(Chromium\)](#).

## Enable the VMware Horizon Geolocation Redirection Plugin for Internet Explorer

To use the Geolocation Redirection feature with Internet Explorer on a published desktop , you must enable the VMware Horizon Geolocation Redirection IE Plugin on the RDS host.

Internet Explorer is supported on Windows 10 virtual desktops with the VMware Geolocation Redirection driver. You do not need to enable the VMware Horizon Geolocation Redirection IE plugin for Windows 10 virtual desktops.

#### Prerequisites

- Configure the Geolocation Redirection feature. See [Install and Configure Geolocation Redirection](#).
- Verify that **Enhanced Protection Mode** is turned off in Internet Explorer 11. The plugin does not work with this feature.
- For Windows Server operating systems, verify that **Internet Explorer Enhanced Security Configuration** is turned off. The plugin does not work with this feature.

### Procedure

- 1 On the RDS host where the Geolocation Redirection feature is enabled, open Internet Explorer 11.
- 2 Click the **Tools** icon in the upper-right corner of the browser window and select **Manage add-ons**.
- 3 Scroll down to the VMware, Inc. section, select **VMware Horizon Geolocation Redirection IE Plugin**, and click **Enable**.
- 4 Restart Internet Explorer 11.

## Install the VMware Horizon Geolocation Redirection Extension for Chrome

To use the Geolocation Redirection feature with the Chrome browser, you must install the VMware Horizon Geolocation Redirection Chrome extension on the remote desktop. Alternatively, you can install the extension silently, without user interaction, by using group policy.

To apply the Google 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 Geolocation Redirection feature. See [Install and Configure Geolocation Redirection](#).
- If you plan to configure group policy, verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server and make sure that the MMC and the Group Policy Object Editor snap-in are available.

### Procedure

- 1 To install the extension from the Chrome Web Store, perform these steps.
  - a Connect to the remote desktop.
  - b In the Chrome browser, download and install <https://chrome.google.com/webstore/detail/vmware-horizon-geolocatio/Indponbebpocehnoibfgdfeiegeaokcf> from the Chrome Web Store.

- 2 To install the extension silently, perform these steps to download and install the ADMX and ADML files.
  - a On your Active Directory server, download the [https://dl.google.com/dl/edgedl/chrome/policy/policy\\_templates.zip](https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip) file.
  - b Unzip the `chrome.admx` file and copy it to `%systemroot%\PolicyDefinitions` folder on the your Active Directory server.
  - c Unzip the `chrome.adml` language resource file and copy it to the appropriate language subfolder in the `%systemroot%\PolicyDefinitions\` folder 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 To configure Chrome group policy, perform these steps.
  - a On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > Google Chrome > Extensions** folder.
  - b Open the **Configure the list of force-installed apps and extensions** group policy setting and click **Enabled**.
  - c Click **Show**, type `1ndponbebpocehno1fgdfeiegeaokcf;https://clients2.google.com/service/update2/crx` in the **Value** text box, and click **OK**.
  - d To save your changes, click **OK**.
- 4 To verify that the VMware Horizon Geolocation Redirection extension is installed on the remote desktop, perform the following steps.
  - a Connect to the remote desktop and start Chrome.
  - b Type `chrome://extensions` in the Chrome address bar.
  - c Verify that VMware Horizon Geolocation Redirection appears in the Extensions list.

## Install the VMware Horizon Geolocation Redirection Extension for Microsoft Edge (Chromium)

To use the Geolocation Feature feature with the Microsoft Edge (Chromium) browser, you must install the VMware Horizon Geolocation Redirection extension on the remote desktop. You can install the extension from the Chrome Web Store. Alternatively, you can install the extension silently, without user interaction, by using Microsoft Edge policy.

Microsoft Edge (Chromium) is supported on Windows 10 virtual desktops with the VMware Geolocation Redirection driver. You do not need to install the VMware Horizon Geolocation Redirection extension on Windows 10 virtual desktops.

## Prerequisites

- Configure the Geolocation Redirection feature. See [Install and Configure Geolocation Redirection](#).
- Verify that the Microsoft Edge (Chromium) browser allows extensions from other stores. For information about how to configure this feature, see the Microsoft documentation.
- If you plan to configure Microsoft Edge policy, verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server and make sure that the MMC and the Group Policy Object Editor snap-in are available.

For the most up-to-date information about Microsoft Edge features and policy, see the Microsoft documentation.

## Procedure

- 1 To install the extension from the Chrome Web Store, perform these steps.
  - a Connect to the remote desktop.
  - b In the Microsoft Edge (Chromium) browser, download and install <https://chrome.google.com/webstore/detail/vmware-horizon-geolocationpnbepoehnoblfgdfeiegeaokcf> from the Chrome Web Store.
- 2 To install the extension silently, perform these steps to download and install the Microsoft Edge ADMX and ADML files.
  - a Download the MicrosoftEdgePolicyTemplates.cab file from <https://www.microsoft.com/en-us/edge/business/download>.
  - b Unzip the MicrosoftEdgePolicyTemplates.cab file and copy the msedge.admx and msedge.adml files to your Active Directory server.
 

After extracting the MicrosoftEdgePolicyTemplates.cab file, the msedge.admx file is in the \windows\admx folder and the msedge.adml file is in the \windows\admx\language folder.
  - c Copy the msedge.admx file to the %systemroot%\PolicyDefinitions folder on your Active Directory server.
  - d Copy the msedge.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 msedge.adml file to the %systemroot%\PolicyDefinitions\en\_us subfolder on your Active Directory server.

- 3 To configure Microsoft Edge policy, perform these steps.
  - a On your Active Directory server, open the Group Policy Management Editor and navigate to the **Computer Configuration > Policies > Administrative Templates > Microsoft Edge > Extensions** folder.
  - b Open the **Control which extensions are installed silently** policy setting and click **Enable**.
  - c Click **Show** and enter `1ndponbebpocehnoblfgdfeiegeaokcf;https://clients2.google.com/service/update2/crx` in the **Value** column.
- 4 Verify that the VMware Horizon Geolocation Redirection extension is installed on the remote desktop.
  - a Connect to the remote desktop and start the Microsoft Edge (Chromium) browser.
  - b Enter `edge://extensions` in the address bar.

**VMware Horizon Geolocation Redirection Extension** appears in the Extensions list.

## Geolocation Redirection Limitations

The Geolocation Redirection feature has certain limitations.

IE mode for Microsoft Edge (Chromium) is supported, but with the following conditions.

- On an RDS host, geolocation information can be redirected, but only when the geolocation IE add-on is enabled.
- On a Windows 10 virtual desktop, geolocation information can be redirected regardless of whether the geolocation IE add-on is enabled.

## Configuring Real-Time Audio-Video

Real-Time Audio-Video allows Horizon users to run Skype, Webex, Google Hangouts, Microsoft Teams, and other online conferencing applications in their remote sessions. With Real-Time Audio-Video, webcam and audio devices that are connected locally to the client system are redirected to the remote sessions. This feature redirects video and audio data 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.

During the setup of an application such as Skype, Webex, Google Hangouts, or Microsoft Teams, users can choose input and output devices from menus in the application.

- For virtual desktops, Real-Time Audio-Video can redirect more than one audio and video device. The names of redirected devices in the virtual desktop are the actual device names, but with (VDI) appended, for example, C670i FHD Webcam (VDI).

- For published desktops and published applications, Real-Time Audio-Video can redirect only one audio device and only one video device. The device names are Remote Audio Device and VMware Virtual Webcam in remote sessions.

The VMware Virtual Webcam uses a kernel-mode webcam driver that provides enhanced compatibility with browser-based video applications and other third-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 drivers for the audio and webcam devices must be installed on the 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 remote sessions 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. An ADMX template file enables you to install Real-Time Audio-Video group policy settings on your Active Directory server 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 might need to configure preferred webcams and audio input devices to be redirected. 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 session, 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 session.

## System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard webcam, USB audio, and analog audio devices. The feature also works with standard conferencing applications. To support Real-Time Audio-Video, your Horizon deployment must meet certain software and hardware requirements.

### Virtual desktops

When using Microsoft Teams with Real-Time Audio-Video, virtual desktops must have a minimum of 4 vCPUs and 4 GB of RAM.

### Horizon Client software

Horizon Client for Windows, Linux, Mac, iOS, or Android.

### Horizon Client computer or client access device

- All operating systems that run Horizon Client for Windows, Mac, iOS, and Android.
- All operating systems that run Horizon Client for Linux on x64 devices. This feature is not supported on ARM processors.
- 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. You do not need to install the device drivers on the machine where the agent is installed.

### Display protocols

- PCoIP
- VMware Blast

## 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 microphone that Real-Time Audio-Video redirects to the remote desktop or published application. These devices can be built in or connected to the client computer.

Real-Time Audio-Video redirects the preferred webcam if it is available. If the preferred webcam is not available, Real-Time Audio-Video uses the first webcam that is provided by system enumeration.

### Windows client computer

For a published desktop or published application, you select a preferred webcam or microphone by configuring Real-Time Audio-Video settings in the Horizon Client Settings dialog box.

For a virtual desktop, the Real-Time Audio-Video feature can redirect more than one webcam and microphone to a virtual desktop and you do not select a preferred webcam or microphone.

For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

### Mac client computer

You specify a preferred webcam or microphone by using the Mac defaults system. For more information, see the *VMware Horizon Client for Mac Installation and Setup Guide* document.

### Linux client computer

You 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. For more information, see the *VMware Horizon Client for Linux Installation and Setup Guide* document.

## 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 remote 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 remote 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 VMware Horizon 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 download, which includes the GPO Bundle.

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

- 2 Unzip the `VMware-Horizon-Extras-Bundle-YYYY-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	<p>When you enable this setting, the Real-Time Audio-Video feature is disabled.</p> <p>When this setting is not configured or disabled, Real-Time Audio-Video is enabled.</p> <p>This setting is in the <b>VMware View Agent Configuration &gt; View RTAV Configuration</b> folder in the Group Policy Management Editor.</p>
Sample Rate – Recording Audio Device sample rate	<p>Enable this setting to set the recording audio device sample rate for RDS hosts and published applications. Values range from 8000 to 48000 Hz. This setting is not configured by default. Reboot the system for this setting to take effect.</p> <p><b>Important</b> Do not change this GPO setting when a session is connected.</p>
Max frames per second	<p>This setting is located in the <b>VMware View Agent Configuration &gt; View RTAV Configuration &gt; View RTAV Microphone Settings</b> folder in the Group Policy Management Editor.</p> <p>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.</p> <p>The minimum value is one frame per second. The maximum value is 25 frames per second.</p> <p>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.</p> <p>By default, client webcams have a frame rate of 15 frames per second. If no setting is configured on the client system and the <b>Max frames per second</b> setting is not configured or disabled, the webcam captures 15 frames per second.</p> <p>This setting is located in the <b>VMware View Agent Configuration &gt; View RTAV Configuration &gt; View RTAV Webcam Settings</b> folder in the Group Policy Management Editor.</p>
Resolution – Max image width in pixels	<p>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.</p> <p>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.</p> <p>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.</p> <p>This setting is located in the <b>VMware View Agent Configuration &gt; View RTAV Configuration &gt; View RTAV Webcam Settings</b> folder in the Group Policy Management Editor.</p>
Resolution – Max image height in pixels	<p>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.</p> <p>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.</p> <p>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.</p> <p>This setting is located in the <b>VMware View Agent Configuration &gt; View RTAV Configuration &gt; View RTAV Webcam Settings</b> folder in the Group Policy Management Editor.</p>
Resolution – Default image resolution width in pixels	<p>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.</p> <p>When this setting is not configured or disabled, the default image width is 320 pixels.</p> <p>This setting is located in the <b>VMware View Agent Configuration &gt; View RTAV Configuration &gt; View RTAV Webcam Settings</b> folder in the Group Policy Management Editor.</p>

Group Policy Setting	Description
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. This setting is located in the <b>VMware View Agent Configuration &gt; View RTAV Configuration &gt; View RTAV Webcam Settings</b> 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 2-1. Sample Bandwidth Results for Sending Real-Time Audio-Video Data from Horizon Client to Horizon Agent](#) measure the bandwidth that Real-Time Audio-Video uses in a Horizon 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 2-1. 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 Microsoft Teams with Real-Time Audio-Video

With Real-Time Audio-Video, users can run Microsoft Teams in their remote sessions.

Webcam and audio devices that are connected locally to the client system are redirected to the remote sessions, and use a significantly lower bandwidth than by using USB redirection.

When you launch the Microsoft Teams application inside a remote desktop, you select VMware virtual input and output devices from menus in the application. The VMware virtual devices redirect the audio and video devices that are connected to the client machine.

- For virtual desktops, Real-Time Audio-Video can redirect more than one audio and video device. The names of redirected devices in the virtual desktop are the actual device names, but with (VDI) appended, for example, C670i FHD Webcam (VDI).
- For published desktops and published applications, Real-Time Audio-Video can redirect only one audio device and only one video device. The device names are Remote Audio Device and VMware Virtual Webcam in remote sessions.

To use Real-Time Audio-Video with Microsoft Teams, you must install the audio and webcam device drivers on your Horizon Client systems.

After you install Horizon Agent with Real-Time Audio-Video, Microsoft Teams works on your remote sessions without any further configuration. See [Configuring Real-Time Audio-Video](#).

## Recommendations for Using Microsoft Teams with Real-Time Audio-Video

To use Microsoft Teams with Real-Time Audio-Video, follow these recommendations:

- Microsoft Teams with Real-Time Audio-Video is supported on Horizon Agent 7.9 and later on Windows, Linux, and Mac clients.
- Microsoft Teams with Real-Time Audio-Video requires a minimum 4 vCPU, 4 GB RAM configuration, with a maximum video resolution of 640 x 480 pixels. Additional vCPUs and memory configurations deliver a superior experience.
- The default video resolution for Real-Time Audio-Video is 320 x 240 pixels. You can change the resolution by changing the setting in the **VMware View Agent Configuration > View RTAV Configuration** folder in the Group Policy Management Editor.

## Configuring Media Optimization for Microsoft Teams

The Media Optimization for Microsoft Teams redirects audio calls, video calls, and viewing desktop shares for a seamless experience between the client system and the remote session without negatively affecting the virtual infrastructure and overloading the network. Microsoft Teams media processing takes place on the client machine instead of in the virtual desktop and does not rely on Real-Time Audio-Video (RTAV).

### Media Optimization for Microsoft Teams Features

Media Optimization for Microsoft Teams offers the following features:

- Accepting and making audio and video calls
- Multiparty audio and video conferencing
- Transfer, forward, mute, hold, and resume a call
- PSTN calls via dial pad
- Desktop screen sharing
- Multi monitor screen sharing and screen picker for screen sharing
- Volume control from the remote desktop
- Active speaker identification

In addition, Microsoft has enabled the following features. Contact Microsoft for any issues with these Microsoft Teams features:

- Gallery View (2x2)
- Large Gallery (7x7)
- Together Mode
- Call Queue
- Live Webinar (optimized)
- Call Quality Dashboard

For other Microsoft Teams features supported with VDI, see the Microsoft documentation [Meetings and live events](#).

**Note** If Microsoft Teams is optimized on a virtual desktop and you encounter generic issues or certain features missing, check the Microsoft Teams web client for the same behavior. Media Optimization for Microsoft Teams on virtual desktops is based on Microsoft Teams web client that leverages WebRTC technology. If you see the same behavior on the web client, contact Microsoft for assistance.

## Media Optimization for Microsoft Teams System Requirements

The Media Optimization for Microsoft Teams supports these configurations.

**Table 2-2. Media Optimization for Microsoft Teams System Requirements**

System	Requirements
Microsoft Server	Microsoft 365
Microsoft Teams Client (Optimized)	<ul style="list-style-type: none"> <li>■ Microsoft Teams Desktop Client x64</li> <li>■ Microsoft Teams Desktop Client x86</li> </ul> <p>See the Microsoft documentation for installation instructions.</p> <p><b>Note</b> Microsoft Teams web client is not supported with Teams Optimization Pack. Web browser media offload is supported with Browser Redirection. See <a href="#">Configuring Browser Redirection</a> for supported browsers and clients. Consult Microsoft documentation for supported browsers for Microsoft Teams web client.</p>
Virtual desktop operating systems	Minimum requirement is 2 vCPU for operating systems supported for Horizon Agent.

Table 2-2. Media Optimization for Microsoft Teams System Requirements (continued)

System	Requirements
Client machine operating systems	<p>Windows: Media Optimization for Microsoft Teams supports the same Windows operating systems as those supported by Horizon Client. Minimum hardware requirement is 2.4 GHz dual core.</p> <p>Mac: Media Optimization for Microsoft Teams supports the same Mac operating systems as those supported by Horizon Client. Media Optimization for Microsoft Teams with Mac client is not supported with versions prior to Horizon Client 2103.</p> <p>Linux: Media Optimization for Microsoft Teams supports the same Linux operating systems as those supported by Horizon Client. Media Optimization for Microsoft Teams with Linux client is not supported with versions prior to Horizon Client 2106.</p> <p><b>Note</b> For Linux clients, to support the German, French, and Spanish (DE/FR/ES) locales in optimization mode, you must update to Horizon Client for Linux 2106.1. For more information, see <a href="#">VMware Horizon Client for Linux 2106.1 Release Notes</a>.</p>
Deployments	<p>On premise and cloud:</p> <ul style="list-style-type: none"> <li>■ VDI</li> <li>■ Non-persistent desktops</li> <li>■ RDS published desktop deployments</li> <li>■ RDS published application deployments (not supported with versions prior to Horizon Client 2012 or Horizon Client 5.5)</li> </ul> <p>Cloud: Windows 10 Enterprise multi-session and all deployment types for Horizon Cloud Services on Azure.</p>
Display Protocols	VMware Blast and PCoIP (no RDP)
TCP Port	9427
Network	IPv4
Microphones and Webcams	Same devices that are qualified to work with Microsoft Teams
Audio codecs	<p>For details, see <a href="https://developer.mozilla.org/en-US/docs/Web/Media/Formats/WebRTC_codecs">https://developer.mozilla.org/en-US/docs/Web/Media/Formats/WebRTC_codecs</a>.</p> <ul style="list-style-type: none"> <li>■ SILK</li> <li>■ Opus</li> <li>■ G.722</li> </ul>
Video codecs	<p>For details, see <a href="https://developer.mozilla.org/en-US/docs/Web/Media/Formats/WebRTC_codecs">https://developer.mozilla.org/en-US/docs/Web/Media/Formats/WebRTC_codecs</a>.</p> <ul style="list-style-type: none"> <li>■ AVC/H.264</li> <li>■ VP8</li> <li>■ VP9</li> </ul>
Media Feature Pack	<p>Must be installed on the remote desktop for Windows 10 N and KN versions. You can install Media Feature from the Microsoft download page: <a href="https://www.microsoft.com/en-us/download/details.aspx?id=48231">https://www.microsoft.com/en-us/download/details.aspx?id=48231</a>.</p>

## Installing and Configuring Media Optimization for Microsoft Teams

The Media Optimization for Microsoft Teams feature is installed by default with Horizon Client for Windows when using the interactive installation wizard. For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide*.

The Media Optimization for Microsoft Teams feature is installed by default with Horizon Client for Mac and Horizon Client for Linux.

Horizon Agent must be installed before you install Microsoft Teams. If you install Microsoft Teams before installing Horizon Agent, delete the %APPDATA%\Microsoft\Teams folder and relaunch Microsoft Teams.

The Media Optimization for Microsoft Teams group policy setting must be enabled to use the feature. See VMware WebRTC Redirection Features in [VMware HTML5 Feature Policy Settings](#).

See the Microsoft documentation [Teams for Virtualized Desktop Infrastructure](#) for installation, setup, and deployment requirements, guidelines on persistent and non-persistent desktops, and limitations of using Microsoft Teams in a remote desktop.

Microsoft updates their Teams recommended version periodically. Check Microsoft for updates and install the latest recommended version to access new features without updating Horizon Client or Horizon Agent.

For additional information about installing and configuring Media Optimization for Microsoft Teams, see the TechZone article [Microsoft Teams Optimization with VMware Horizon](#).

---

**Note** Media optimization for Microsoft Teams is not supported in Horizon Agent 7.12 or earlier and Horizon Client versions 5.4.3, 5.4.2, 5.4.1, 5.4, and 5.3 or earlier due to UX issues. These UX issues have been fixed in the latest release of Horizon Agent and Horizon Client.

---

## Media Optimization for Microsoft Teams Limitations

Media Optimization for Microsoft Teams has the following limitations. Contact Microsoft for Microsoft limitations.

Limitation	Comments
In optimized mode, screensharing is not supported on Mac Client or Linux Client if Microsoft Teams is published as an application.	VMware limitation
Volume control from remote desktop is not supported on Linux clients. To change the volume during the call, change the volume of the Linux client.	VMware limitation
Media Optimization on Linux and Mac clients does not support proxy configuration.	VMware limitation
HID buttons to answer and end calls are not supported.	VMware limitation
Outgoing application window sharing is not supported.	VMware limitation
Virtual backgrounds are not supported.	Microsoft and VMware limitation



Limitation	Comments
Desktop screen sharing give or take control is not supported.	Microsoft limitation
Pop out chat, call, or meeting window.	Microsoft limitation. As of Horizon Client version 2106 release, pop out chat, call or meeting window is not supported by Microsoft for VDI.
The camera light stays on if the user puts the video call on hold (but video will not be sent).	Microsoft limitation
During a video call, when a remote desktop user starts a desktop share, the user's video automatically turns off. After ending the desktop share, the remote desktop user can click the video button to turn the video back on.	Microsoft limitation
When minimizing a Microsoft Teams video call window, the small Microsoft Teams window in the lower right corner will not show an active video.	Microsoft limitation
Microsoft Teams running in fallback mode on an RDSH machine cannot access the remote machine's microphone and speaker.	See the KB article <a href="https://kb.vmware.com/s/article/84205">https://kb.vmware.com/s/article/84205</a> for a workaround.
Test call	Microsoft limitation
VDI participants cannot create breakout rooms but can join only.	Microsoft limitation
E911 and location-based routing are not supported.	VMware limitation
Live Events is not optimized, but supported as an attendee. Producer and presenter roles are not supported for a VDI user.	Microsoft limitation
Media bypass for direct routing is not supported.	Microsoft limitation
Live caption in meetings is not supported.	Microsoft and VMware limitation
1080p video is not supported.	Microsoft limitation
Zoom in and out function in Microsoft Teams is not supported.	Microsoft limitation
Microsoft starts meetings with a lower resolution and gradually increases the resolution based on network conditions, such as bandwidth of meeting participants and video window size.	Microsoft limitation
Quality of Service (QoS) in Microsoft Teams is not supported.	VMware limitation
3x3 video gallery is not supported.	Microsoft limitation

For a list of other Microsoft Teams limitations on VDI, see the Microsoft documentation [Meetings and live events](#).

## Pairing Modes for a Session

A user can check if Microsoft Teams is running in optimized mode, fallback mode, or natively in the virtual desktop (no optimization). On the top right corner of the Microsoft Teams interface, click the user icon and navigate to **About->Version** to see a banner under the user icon describing the Microsoft Teams version and pairing modes:

- **Optimized:** If the banner shows **VMware Media Optimized**, then Microsoft Teams is running in the optimized mode. In this mode, the **Enable Media Optimization for Microsoft Teams** GPO is enabled, Microsoft Teams is running in the virtual desktop, and audio and video is offloaded to the client machine.
- **Fallback:** If the banner shows **VMware Media Not Connected**, then Microsoft Teams is running in fallback mode. In this mode, the **Enable Media Optimization for Microsoft Teams** GPO is enabled and Microsoft Teams has tried to start in Optimized mode, but the Horizon Client being used does not support Microsoft Teams optimization. RTAV is used and audio and video from Microsoft Teams is not offloaded to the client machine. Fallback mode has the same limitations as Optimized mode. When you make a call in fallback mode, you see a warning sign on the call:  
  
**Your device does not support VMware optimization. Audio and video quality may be reduced. Talk to your IT admin.**
- **No optimization:** If the banner does not show **VMware** text in the message, the **Enable Media Optimization for Microsoft Teams** GPO is not enabled. RTAV is used and audio and video from Microsoft Teams is not offloaded to the client machine.

## Configuring Scanner Redirection

By using scanner redirection, end 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 supports standard scanning and imaging devices that are compatible with the TWAIN and WIA formats, and SANE on Linux clients.

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.

To ensure the optimal host consolidation, make sure that the Scanner Redirection setup option is only selected for those users who need it. (By default, the Scanner Redirection option is not selected when you install Horizon Agent.) For users who need the Scanner Redirection feature, configure a separate desktop pool and select the setup option only in that pool.

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 on your Active Directory server 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 VMware Horizon deployment must meet certain software and hardware requirements.

### Remote desktop or published application

You must install Horizon Agent with the Scanner Redirection setup option enabled on the virtual desktop or RDS host for published desktops and published applications. The Horizon Agent Scanner Redirection setup option is deselected by default.

This feature is supported on the following virtual desktops and RDS hosts.

- 64-bit Windows 10 1903
- Windows Server 2012 R2 configured as a desktop or RDS host
- Windows Server 2016 configured as a desktop with Desktop Experience installed
- Windows Server 2016 configured as RDS host
- Windows Server 2019 configured as a desktop or RDS host

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 for Windows

### Horizon Client computer or client access device

The scanner device drivers must be installed and the scanner must be operable on the client computer.

The following client operating systems are supported.

- 32-bit or 64-bit Windows 10
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

## Scanning device standard

TWAIN or WIA

## Display protocol

PCoIP


VMware Blast

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 (  ) is added to the desktop. On published 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 appears. 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 [Configuring 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 the **Force the TWAIN Scanning Properties 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 **Force the TWAIN Scanning Properties dialog** option.

---

**Note** If you run two published 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 published applications that run on different farms. In that case, you must open each icon to see which scanner redirection menu controls which published application.

---

For end-user instructions for operating redirected scanners, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

## Configuring Scanner Redirection Group Policy Settings

You can configure group policy settings that control the behavior of scanner redirection on your remote 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 [VMware View Agent Configuration ADMX Template Settings](#).

### Procedure

- 1 Download the VMware Horizon 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 download, which includes the GPO Bundle.

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

- 2 Unzip the VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyyy.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.

## 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 and published applications.

After you install Horizon Agent and set up the serial port redirection feature, the feature can work on your remote desktops and published applications 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 connects to the remote desktop or published application. 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 machines. See [Configuring Serial Port Redirection Group Policy Settings](#).

In VMware Horizon version 2103 and later, you can run a console utility `vmwsprrdctl.exe` on Horizon Agent to see a list of redirected COM ports. For every virtual COM port on the agent where the source port (remote COM port) on the client is created from a USB device, the utility provides the following information:

- Hardware ID
  - USB device VID (Vendor ID)
  - USB device PID (Product ID)
  - USB device Rev (Product Revision)
- COM port device description as it appears in Device Manager

For all ports, the utility provides the following additional information:

- Source COM port number on the client side
- COM port redirection status

The utility on Horizon Agent is in `C:\Program Files\Common Files\VMware\SerialPortRedirection\Agent\vmwsprrdctl.exe`.

For command line usage help for the utility, launch a desktop session in Horizon Client, and type:

```
# cd "C:\Program Files\Common Files\VMware\SerialPortRedirection\Agent\" (If the path is in the agent OS PATH environment variable, skip this step.)
```

```
# vmwsprrdctl.exe -h
```

This utility is supported on remote desktops and nested mode sessions on Windows and Linux client systems.

When a redirected COM port is opened and in use on a remote desktop or published application, 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 or published application.

## System Requirements for Serial Port Redirection

With the serial port redirection 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 and

published applications. To support serial port redirection, your VMware Horizon deployment must meet certain software and hardware requirements.

### **Virtual desktops**

Horizon Agent must be installed with the Serial Port Redirection setup option selected. This setup option is deselected by default.

The following operating systems are supported on virtual desktops.

- 64-bit Windows 10
- Windows Server 2016
- Windows Server 2019

Serial port device drivers do not need to be installed in the virtual desktop.

### **Published desktops and published applications**

RDS hosts must have Horizon Agent installed with the Serial Port Redirection setup option selected. This setup option is deselected by default.

The following operating systems are supported for published desktops and published applications.

- Windows Server 2016
- Windows Server 2019

Serial port device drivers do not need to be installed in the RDS host.

Serial port redirection is available with full desktops and not supported on published applications on RDS hosts.

### **Horizon Client computer or client access device**

For Horizon Client for Windows, serial port redirection is supported on Windows 10 client systems. Any required serial port device drivers must be installed and the serial port must be operable.

### **Display protocols**


- PCoIP
- VMware Blast

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 third-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 (COMn)**.

When the COM port is connected, you can open the port in a third-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 menu.

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 *VMware Horizon Client for Windows Installation and Setup Guide* 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 third-party applications in your organization.

For information about the group policy settings, see [VMware View Agent Configuration ADMX Template Settings](#).

- If your users run the same third-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 various third-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 third-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 third-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 in your remote sessions. 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 in remote 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 in remote sessions and client systems.

These policy settings affect your remote sessions, not the client systems where the physical COM port devices are connected. To configure these settings for remote desktops and published applications, 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 virtual desktops or RDS hosts. The group policy settings have no effect if serial port redirection is not installed. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.
- 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 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.
- Become familiar with the serial port redirection group policy settings. See [VMware View Agent Configuration ADMX Template Settings](#).

#### Procedure

- 1 Download the VMware Horizon 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 download, which includes the GPO Bundle.

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

- 2 Unzip the VMware-Horizon-Extras-Bundle-*YYYY-x.x.x-yyyyyyyyy*.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**.

## Configure USB to Serial Adapters

You can configure USB to Serial adapters that use a Prolific chipset to be redirected to remote sessions 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 virtual machine desktop or RDS host.

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 virtual machine desktops or RDS hosts. The group policy settings have no effect if serial port redirection is not installed. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.
- Verify that the Serial Port Redirection ADMX template file is added in Active Directory.
- Become familiar with the **Serial2USBModeChangeEnabled** item in the **PortSettings** group policy setting. See [VMware View Agent Configuration ADMX Template Settings](#).

### Procedure

- 1 On the Active Directory server, open the Group Policy Management Object Editor.
- 2 Navigate to the **Computer Configuration > Policies > 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 Management Object Editor.

#### Results

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

## Managing Access to Windows Media Multimedia Redirection (MMR)

VMware Horizon provides the Windows Media MMR feature for virtual desktops that run on single-user machines and for published desktops on RDS hosts. MMR is not available on published applications on RDS hosts.

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

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 on a secure network.

By default, the global policy **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, see [Horizon Policies](#).

## System Requirements for Windows Media MMR

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

### Remote desktop

- This feature is supported on virtual desktops and RDS hosts for published desktops.
- The following guest operating systems are supported.
  - 64-bit Windows 10. Windows Media Player is supported. The default player TV & Movies is not supported.
  - Windows Server 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.

### Horizon Client software

Horizon Client for Windows.

### Horizon Client computer or client access device

The clients must run a 64-bit or 32-bit Windows 10 operating system.

### Supported media formats

Media formats that Windows Media Player supports, for example: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3; WAV.

MP3 is not supported when using MMS and RTSP.

---

**Note** DRM-protected content is not redirected through Windows Media MMR.

---

### Horizon policies

In Horizon Console, set the **Multimedia redirection (MMR)** policy to **Allow**. The default value is **Deny**.

### Back-end firewall

If your VMware Horizon 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.

## 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 and published desktops.

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.

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
<b>64-bit Windows Media Player</b>	<ul style="list-style-type: none"> <li>■ For a 64-bit desktop, use the registry key: HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr</li> </ul>
<b>32-bit Windows Media Player</b>	<ul style="list-style-type: none"> <li>■ For a 32-bit desktop, use the registry key: HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr</li> <li>■ For a 64-bit desktop, use the registry key: HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr</li> </ul>

- 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 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.

If you deselect the **Client Drive Redirection** custom setup option, the following features do not work.

- Dragging and dropping files and folders between clients and remote desktops and published applications.
- Dragging and dropping file content (for example, Outlook attachments and ZIP file items) between remote desktops and published applications.
- Copying files and folders between clients and remote desktops and published applications.
- Opening local files with published applications from a remote desktop that does not have the client drive redirection feature.

When client drive redirection is installed, you can drag and drop and copy and paste files and folders between client systems and remote desktops and published applications. See [Configuring the Drag and Drop Feature](#) and [Configuring the Clipboard Redirection Feature](#).

## Using Client Drive Redirection in a Unified Access Gateway Implementation

If your Horizon 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.

## 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 `vdm_agent_cdr.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 Group Policy to Configure Drive Letter Behavior

You can use agent group policy settings to configure drive letter behavior for drives that are redirected with the client drive redirection feature.

When drive letter mapping is configured, the folders configured in the client drive redirection share list are not redirected. This limitation applies only to Horizon Client for Windows. For information about sharing local files and drives in Horizon Client for Windows, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

#### 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 VMware Horizon Client Drive Redirection ADMX template file (`vdm_agent_cdr.admx`) 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 > Administrative Templates > VMware View Agent Configuration > VMware Horizon Client Drive Redirection**.
- 2 To configure whether to display a drive letter for redirected drives, configure the **Display redirected device with drive letter** group policy setting.

This setting is enabled by default.

- To specify how long to wait, in milliseconds, for Windows Explorer to initialize and display a drive letter for redirected drives, configure the **Timeout for drive letter configuration** group policy setting.

When this setting is disabled or not configured, the default value is 5000 milliseconds.

- To set the drive letter mapping mode, configure the **Configure drive letter mapping mode** group policy setting.

You can select one of the following options.

Option	Description
<b>One to one mapping</b>	Maps the drive letter on the client machine to the same drive letter on the agent machine. For example, drive X on the client machine is mapped to drive X on the agent machine.
<b>Defined mapping</b>	Maps drive letters on the client machine to certain drive letters on the agent machine according to a mapping table that is defined in the <b>Define drive letter mapping table</b> group policy setting.

- To map driver letters, configure the **Define drive letter mapping table** group policy setting.

You click **Show** to define a drive letter mapping table. The **Value name** column specifies the drive letter on the client machine and corresponding **Value** column specifies the drive letter to use on the agent machine.

## 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.

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 or Read 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
```

To prevent read access, set the `permissions` value to any string that begins with `w`.

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

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.

---

## Configuring the Drag and Drop Feature

Users can drag and drop data between client systems and remote desktops and published applications.

### Client Requirements for Drag and Drop

- Only Windows client and Mac client systems are supported. Other types of client systems are not supported.
- To drag and drop files and folders, the client drive redirection feature must be enabled in Horizon Client for Windows.

For information about using the drag and drop feature on a Windows client, see the *VMware Horizon Client for Windows Installation and Setup Guide* document. For information about using the drag and drop feature on a Mac client, see the *VMware Horizon Client for Mac Installation and Setup Guide* document.

### Agent Requirements for Drag and Drop

To use the drag and drop feature with files, folders, and file content, you must enable the **Client Drive Redirection** option when you install Horizon Agent.

### Using Group Policy Settings to Configure Drag and Drop

You can configure the drag and drop direction, the allowed drag and drop formats, and the drag and drop size limit by editing group policy settings in the ADMX template file `vdm_agent_dnd.admx`. The Drag and Drop settings are in the **VMware View Agent Configuration > Drag and Drop** folder in the Group Policy Management Editor. See [VMware View Agent Configuration ADMX Template Settings](#).

### Using Dynamic Environment Manager to Configure Drag and Drop

With Dynamic Environment Manager 9.8 or later, you can use Smart Policies to configure drag and drop behavior, including disabling the entire drag and drop feature. See [Horizon Smart Policy Settings](#).

## Configuring the Clipboard Redirection Feature

Users can copy and paste data between client systems and remote desktops and published applications.

### Client Requirements for Clipboard Redirection

- To copy and paste files and folders, only Windows client systems are supported. Other types of client systems are not supported.
- To copy and paste files and folders, the client drive redirection feature must be enabled in Horizon Client for Windows.

For information about copying and pasting files and folders on a Windows client, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

## Agent Requirements for Clipboard Redirection

To use the copy and paste feature with files, folders, and file content, you must enable the **Client Drive Redirection** option when you install Horizon Agent.

## Using Group Policy Settings to Configure Clipboard Redirection

You can configure the copy and paste direction, the allowed copy and paste formats, and the copy and paste size limit by editing group policy settings in the ADMX template file `vdm_agent_clipboard.admx`. The Clipboard Redirection settings are in the **VMware View Agent Configuration > Clipboard Redirection** folder in the Group Policy Management Editor. See [VMware View Agent Configuration ADMX Template Settings](#).

## Using Dynamic Environment Manager to Configure Clipboard Redirection

With Dynamic Environment Manager 9.8 or later, you can use Smart Policies to configure copy and paste behavior, including disabling the entire clipboard redirection feature. See [Horizon Smart Policy Settings](#).

## Restricting Clipboard Formats for Copy and Paste Operations

You can configure group policy settings to control which clipboard formats are permitted when users copy and paste data during PCoIP and VMware Blast sessions. This feature is useful if you need to restrict copy and paste operations for security reasons.

You can configure clipboard format restrictions based on the direction of the copy and paste operation. For example, you can configure one set of policies for data copied from client systems to remote desktops, and another set of policies for data copied from remote desktops to client systems.

The group policy settings for filtering clipboard redirection formats are in the ADMX template file `vdm_agent_clipboard.admx`. You can edit the settings in **VMware View Agent Configuration > Clipboard Redirection > Configure clipboard redirection formats** in the Group Policy Management Editor. See [VMware View Agent Configuration ADMX Template Settings](#).

## Clipboard Format Filtering Examples

The following examples show how you can use group policy settings to filter clipboard formats during copy and paste operations.

- To filter out images for non-Microsoft Office applications, such as Wordpad, when users copy data from their client systems to remote desktops, enable the `Filter images out of the incoming clipboard data` group policy setting.

- To filter out images for both non-Microsoft Office applications and Microsoft Office applications when users copy data from their client systems to remote desktops, enable the Filter Microsoft Chart and Smart Art data out of the incoming clipboard data and the Filter images out of the incoming clipboard data group policy settings. The Filter Microsoft Chart and Smart Art data out of the incoming clipboard data group policy setting filters out Microsoft Office Chart and Smart Art data, which can include images.
- To filter out only Microsoft Office Chart and Smart Art data when users copy data from their client system to remote desktops, enable only the Filter Microsoft Chart and Smart Art data out of the incoming clipboard data group policy setting.
- To filter out Microsoft Word-related text formatting when users copy data from their client systems to remote desktops and from remote desktops to their client systems, enable the incoming group policy settings Filter Microsoft Text Effects data out of the incoming clipboard data and Filter Rich Text Format data out of the incoming clipboard data, and the outgoing group policy settings Filter Microsoft Text Effects data out of the outgoing clipboard data and Filter Rich Text Format data out of the outgoing clipboard data.
- To filter out images for Microsoft Word when users copy data from their client systems to remote desktops and from remote desktops to their client systems, enable the incoming group policy setting Filter Rich Text Format data out of the incoming clipboard data and the outgoing group policy setting Filter Rich Text Format data out of the outgoing clipboard data. The images in Microsoft Word are stored in compound RTF format.

## Configuring Simple Device Orientation (SDO) Sensor Redirection

The Simple Device Orientation (SDO) Sensor Redirection feature can sense changes in the screen orientation of a client device and accordingly display a different view on the device.

SDO Sensor Redirection integrates with your software application on Horizon Agent. If your application uses SimpleOrientationSensor class <https://docs.microsoft.com/en-us/uwp/api/windows.devices.sensors.simpleorientationsensor>, the application can display content based on the current quadrant orientation of the client device.

### System Requirements for SDO Sensor Redirection

These devices are supported:

Table 2-3. Devices that Support SDO Sensor Redirection

Device	Client OS	Windows OS Servers	Protocols
Surface Book	Windows 10 1709	Windows 10 1709 (64-bit, 32-bit)	PCoIP, Blast
Surface Pro	Windows 10 1709	Windows 10 1709 (64-bit, 32-bit)	PCoIP, Blast

For Horizon Agent operating systems, only Windows 10 64-bit is supported.

## Installing SDO Sensor

SDO Sensor Redirection is a custom setup option in the Horizon Agent installer. It is not selected by default. You must select SDO Sensor Redirection to install it. For silent installation properties for SDO Sensor Redirection, see the *Setting Up Virtual Desktops in Horizon* document.

Sensor Service on the local system must be enabled for the SDO driver to function. SDO sensor must be enabled on the client device.

## Logs

Horizon Client logs for SDO sensor redirection are recorded in rdeSvc log file %TEMP%\vmware-%USERNAME%\vmware-rdeSvc-x-xxxxx.log.

Horizon Agent logs for SDO sensor redirection are recorded in rdeSvc log file C:\Windows\Temp\vmware-SYSTEM\*\vmware-rdeSvc-x-xxxx.log.

## Configuring Pen Redirection

As an extension of the mouse and touch functionality, you can use an integrated pen on a Windows tablet, such as a Microsoft Surface Book 2.

Pen input includes pointing, pressure to create varying thickness of lines, tilt, rotation, and erasing. You can sign on a PDF with Microsoft Edge or draw on OneNote or another ink-based application in LAN and WAN environments. The pen functionality is enabled by default if your system supports the pen.

## System Requirements for Pen Redirection

System	Requirements
Device	Surface Book 2 and its integrated pen
Client machine operating system	Windows 10
Agent machine operating system	Windows 10 1809 or later
Software	Windows Ink workspace applications Sketchpad, Screen Sketch Windows Ink-based applications OneNote, Edge
Display protocol	Blast

## Configuring a Digital Watermark

You can create a unique digital watermark as a solution for authenticity, content integrity, and ownership protection of your intellectual property. A watermark shows traceable information that can deter people from stealing potential data.

### Watermark Features and Limitations

The watermark can be displayed on the following remote sessions:

- Published applications and applications running on a desktop pool
- Virtual desktops and RDS hosts
- Nested mode
- Multiple monitors
- Primary session in a collaborative session

The watermark feature has the following limitations:

- RDP protocol is not supported.
- HTML5 multimedia redirection is not supported.
- Recorded sessions in Zoom or Webex applications do not include the watermark.
- Screen capture applications and the Print Screen key operated from within the remote desktop do not include the watermark. However, screen capture applications and the Print Screen key operated from the client system do include the watermark.
- Windows remote assistance does not show the watermark.
- If you use an old client version with the latest agent version, the watermark shows on the agent side, but some remote desktop redirection features such as Skype and Microsoft Teams do not function.
- If you use the latest client version with an old agent version, the watermark does not display.
- A shadow session in a collaborative session cannot show the watermark.

### Using Group Policy Settings to Configure Watermark

You can configure watermark features, such as the text content, layout, rotation, and opacity, by editing the group policy settings. See [VMware View Agent Configuration ADMX Template Settings](#). Changes take effect at the subsequent login.

## Configuring Session Collaboration

With the Session Collaboration feature, users can invite other users to join an existing Windows or Linux remote desktop session.



## System Requirements for Session Collaboration

To support the Session Collaboration feature, your VMware Horizon deployment must meet certain requirements.

Component	Requirements
Client system	Session owners and collaborators must have Horizon Client for Windows, Mac, or Linux installed on the client system, or must use HTML Access.
Windows remote desktops	Horizon Agent must be installed in the virtual desktop, or on the RDS host for published applications. The Session Collaboration feature must be enabled at the desktop pool or farm level. For information about enabling the Session Collaboration feature for desktop pools, see the <i>Setting Up Virtual Desktops in Horizon</i> document. For information about enabling the Session Collaboration feature for a farm, see the <i>Setting Up Published Desktops and Applications in Horizon</i> document.
Linux remote desktops	For Linux remote desktop requirements, see the <i>Setting Up Linux Desktops in Horizon</i> document.
Connection Server	The Connection Server instance uses an Enterprise license.
Display protocol	VMware Blast

For information about how to use the Session Collaboration feature, see the Horizon Client documentation.

## Configuring Session Collaboration Group Policy Settings

Use the Collaboration group policy settings in the VMware View Agent Configuration ADMX template file (`vdm_agent.admx`) to configure session collaboration. See [VMware View Agent Configuration ADMX Template Settings](#).

## Session Collaboration Feature Limitations

Users cannot use the following remote desktop features in a collaborative session.

- USB redirection
- Real-Time Audio-Video (RTAV)
- Multimedia redirection
- Client drive redirection
- Smart card redirection
- Microsoft Lync redirection
- File redirection and Keep in Dock functionality
- Clipboard redirection

Users cannot change the remote desktop resolution in a collaborative session.

Users cannot have multiple collaboration sessions on the same client machine.

## Configuring VMware Virtualization Pack for 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 a Skype audio and video call.

### VMware Virtualization Pack for Skype for Business Features

VMware Virtualization Pack for Skype for Business offers the following features:

- Execute calls and conferences using a HTTPS proxy server
- Response groups
- Microsoft Office Integration: start a Skype for Business call from Word, Outlook, SharePoint, and so on
- Quality-of-Experience allows Skype for Business clients to report call metrics to the Skype for Business server to generate reports
- Manage calls on behalf of someone else as a delegate
- Active speaker identification
- Call via X (home, work, and so on)
- Control the volume from the remote desktop
- 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
- Skype for Business online meeting
- Meet Now conferencing
- Whiteboarding and screensharing

## System Requirements for VMware Virtualization Pack for Skype for Business

VMware Virtualization Pack for Skype for Business supports these configurations.

**Table 2-4. VMware Virtualization Pack for Skype for Business System Requirements**

System	Requirements
Microsoft Server	Lync Server 2013, Skype for Business Server 2015, Skype for Business Server 2019, Office365  For Skype for Business on-premises server deployments, Skype for Business Edge Server is needed for communication with external users.
Microsoft Client	VMware strongly recommends that you use the latest Skype for Business client updates. <ul style="list-style-type: none"> <li>■ Skype for Business 2015 client: 15.0.4933.100 or later</li> <li>■ Skype for Business 2016 as part of Office 365 Plus: 16.0.7571.2072 or later</li> <li>■ Skype for Business 2016 as part of Office 2016: 16.0.4561.1000 or later</li> </ul> <p><b>Note</b> Skype for Business Basic 2015 or 2016 clients are not supported.</p>
Virtual desktop operating systems	Minimum 2 vCPU
Client machine operating systems	Minimum hardware 2.4 GHz dual core VMware Virtualization Pack for Skype for Business supports the same Windows, Mac, and Linux operating systems as those supported by Horizon Client.
Deployments	<ul style="list-style-type: none"> <li>■ VDI (on premise and cloud)</li> <li>■ Persistent and non-persistent desktops</li> <li>■ RDS deployments (published desktops and applications)</li> </ul>
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 <a href="https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/ports-and-protocols">https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/ports-and-protocols</a> . See also <a href="https://kb.vmware.com/s/article/52558">https://kb.vmware.com/s/article/52558</a> .
Microphones and Webcams	The same devices that are qualified to work with Skype for Business. See webcams listed in <a href="https://docs.microsoft.com/en-us/SkypeForBusiness/certification/devices-usb-devices">https://docs.microsoft.com/en-us/SkypeForBusiness/certification/devices-usb-devices</a> .

**Table 2-4. VMware Virtualization Pack for Skype for Business System Requirements (continued)**

System	Requirements
Audio and video codecs	The same as the audio and video codecs used by the native Skype for Business client. See <a href="https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/network-requirements">https://docs.microsoft.com/en-us/skypeforbusiness/plan-your-deployment/network-requirements/network-requirements</a> .
Compatible Peer Skype for Business Clients (non-VDI)	<ul style="list-style-type: none"> <li>■ Skype for Business 2016 client with latest updates</li> <li>■ Skype for Business 2015 client with latest updates</li> <li>■ Lync 2013 client with latest updates</li> <li>■ Lync 2010 client (audio calls only)</li> </ul>
Media Feature Pack	Must be installed on the remote desktop for Windows 10 N and KN versions. You can install Media Feature from <a href="https://www.microsoft.com/en-us/download/details.aspx?id=48231">https://www.microsoft.com/en-us/download/details.aspx?id=48231</a> .

## Installing VMware Virtualization Pack for Skype for Business

To use Skype for Business, you must install VMware Virtualization Pack for Skype for Business on the client machine. VMware Virtualization Pack for Skype for Business software is installed by default as part of the Horizon Client for Windows, Horizon Client for Linux, and Horizon Client for Mac installers. For Horizon Client installation information, see the installation and setup guide for the Horizon Client version.

A Horizon administrator must install VMware Virtualization Pack for Skype for Business on the virtual desktop during Horizon Agent installation. For Horizon Agent installation information, see the *Setting Up Virtual Desktops in Horizon* document.

VMware 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

To check if VMware Virtualization Pack for Skype for Business is installed on the virtual machine, check these registry keys:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\Lync\VdiMediaProvider – GUID(REG\_SZ)
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\Lync\VdiMediaProvider – GUID(REG\_SZ)

## Pairing Modes for a Session

Lync.exe loads VMware Virtualization Pack for Skype for Business plugin on startup. The plugin checks for a valid session and writes the pairing mode state in the registry. To query pairing modes, verify that Lync.exe is running in the processes list, then check HKEY\_CURRENT\_USER\Software\VMware, Inc.\VMWMMAPLugin – PairingMode(REG\_SZ).

Valid pairing modes include:

- Optimized: a valid session
- Fallback: no valid session

- Optimized (version-mismatch)
- Fallback (version-mismatch)
- Connecting
- Disconnected
- Undefined

When Lync.exe exits, the plugin deletes the pairing mode value from the registry.

Users do not need administrator privileges to check the pairing mode. Multiple users logged in on remote desktops can find each user's pairing mode in the HKCU hive.

## Configuring VMware Virtualization Pack for Skype for Business Group Policy Settings

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

## VMware Virtualization Pack for Skype for Business Limitations

VMware Virtualization Pack for Skype for Business has the following limitations:

- Socks and http proxy servers are not supported.
- The VMware Virtualization Pack for Skype for Business solution does not support interoperability with third-party multiparty conferencing units, such as Pexip.
- Gallery view is not currently supported.
- You cannot record calls.
- Media Bypass is not supported. For details, see <https://kb.vmware.com/s/article/56977>.
- The double-hop scenario, such as Horizon Agent nested with Horizon Client, is not supported.
- Skype for Business VDI optimized solution is not compatible for inter-operability with Lync 2010 clients.
- 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.
- Using Microsoft Teams 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 want the camera to update dynamically, use the Skype for Business 2016 Click-to-Run installer version 16.0.11001.20097 or later.
- 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.

## Collect Logs to Troubleshoot Skype for Business

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

### Procedure

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

### Results

A folder named `vdm-sdct` containing zipped log files appears on the desktop and includes these directories, which contain logs for VMware 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>\MMAPLogin`

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

## Configuring VMware Integrated Printing

With VMware Integrated Printing, users can print from a remote desktop to any local or network printer available on their client computer. VMware Integrated Printing works with Windows, Mac, Linux, and mobile client devices. It also works with browser-based clients.

VMware Integrated Printing supports client printer redirection, location-based printing, and persistent print settings.

### Client Printer Redirection

With Client Printer Redirection, users can print from a remote desktop to any local or network printer available on their client computer. For printers redirected from a Windows client to a remote desktop, VMware Integrated Printing supports the following types of printer drivers on the remote desktop.

- Native Printer Driver (NPD). On the remote desktop, you must install the same printer driver as the driver for the client printer. NPD supports only v3 printers.
- Universal Printer Driver (UPD). You do not need to install any driver on the remote desktop.

By default, VMware Integrated Printing displays the session user name on the client side print queue. This way, the end user can monitor the print job and see who initiated the print job.

By default, if you install the native driver on the Horizon Agent computer, NPD is used. Otherwise, UPD is used. You can select the printer driver type to use on a remote desktop by configuring a group policy setting.

To determine which printer driver type is used in a remote desktop, go to **Control Panel > Hardware and Sound > Devices and Printers**, right-click the virtual printer, and select **Printer Properties** from the context menu. On the **General** tab, if **Model** is VMware Universal EMF driver, UPD is used. Otherwise, NPD is used.

### Location-Based Printing

The location-based printing feature maps printers that are physically near client systems to remote desktops. For information, see [Setting Up Location-Based Printing](#).

### Nested Mode Redirection

In a nested mode setup, you can redirect local printers installed on the first and second layers to the remote desktop or published application on the third layer. Depending on the group policy setting and whether native print drivers are installed, redirected printers on the third layer might use UPD or NPD.

## Static Printer Names

Redirected printers retain their names across sessions with the suffix `vdi` so that users do not need to remap the printer manually when they connect to another session. The static printer name is supported only on single-user machines, and is not supported on Windows Server with VDI mode.

## Persistent Print Settings

Printer settings for redirected client printers, including NPD and UPD, or location-based printers, are retained after a user logs out or disconnects from the remote desktop. For example, a user might set a redirected client printer or location-based printer to use black and white mode. After the user logs out and logs in to the remote desktop again, the previous print setting is persistent.

Persistent print setting can be disabled by configuring a group policy setting.

## Universal Printer Driver Print Settings

VMware Integrated Printing provides the following print settings for redirected UPD printers from Windows clients.

- **Orientation:** select portrait or landscape orientation of the paper. The staple and punch finishing options depend on the orientation of the paper.
- **Print on Both Sides:** select duplex (double-sided) printing for duplex-capable printers.
- **Multiple Pages per Sheet:** to print multiple document pages onto one physical page, select the number of pages to print onto one physical page, and select the layout of the pages.
- **Paper source:** select the name of the input paper tray.
- **Paper size:** select the paper size:
  - Standard paper sizes: paper sizes that are commonly supported by most printers, such as A4, letter, and legal.
  - Vendor-defined paper sizes (also called nonstandard paper sizes): paper sizes that are defined by a printer vendor.
  - User-defined paper sizes (also called customized paper sizes): paper sizes that are defined by system administrators.
- **DPI:** specify the printer resolution.
- **Color:** specify whether a color printer prints color or monochrome.
- **Print and Preview:** select **print directly** or **print preview**:
  - With **print directly**, you can select **with opening preference dialog**, which opens the client printer preferences before printing, so that you can change print settings.
  - With **print preview**, the **with opening preference dialog** option is not available.
- **Number of copies:** specify the number of copies.



- **Print as Image:** print each page as an image.
- **Compression:** specify how the images in the printed document are to be compressed.
- **Finishing:** specify staple and punch options for specified printers.

You can define default settings for UPD printers by enabling the group policy setting **Default settings for UPD printers**. See [VMware Integrated Printing Policy Settings](#).

By default, you cannot set the media type on a UPD printer. To change the media type on a UPD printer, enable the **Disable Printer Property Persistence** group policy setting and change the media type setting of the client printer to the desired setting. For information about the **Disable Printer Property Persistence** group policy setting, see [VMware Integrated Printing Policy Settings](#).

## Native Printer Driver Finishing Options

These redirected native printers support a finishing option when the specific hardware is connected to the printers.

Printer	Finishing option	Requirements on the client-side local printer
FX ApeosPort-IV C5575 PCL 6	staple, booklet	<p>Verify that the finishing hardware device is connected to the printer.</p> <p>Update printer information with bi-directional communication in printer properties.</p> <p>Enable the finishing options in printer preferences.</p>
Ricoh MP C5003	staple, punch	<p>Manually add the finisher according to its device setting to enable the finishing option, which is then available in printer preferences.</p>

## Installing VMware Integrated Printing Redirection

VMware Integrated Printing is a custom setup option in the Horizon Agent installer. It is not selected by default. You must select VMware Integrated Printing to install it.

To install this feature on a virtual machine, see the *Setting Up Virtual Desktops in Horizon* document. To install this feature on an RDS host, see the *Setting Up Published Desktops and Applications in Horizon* document.

VMware Integrated Printing uses TCP port 9427.

## Configuring VMware Integrated Printing Group Policy Settings

To customize VMware Integrated Printing, including disabling location-based printing, disabling print setting persistence, selecting the printer driver for a redirected client printer, and disabling printing to non-desktop clients, use the group policy settings in the VMware Integrated Printing ADMX template file (`printerRedirection.admx`). See [VMware Integrated Printing Policy Settings](#).

## Setting Up Location-Based Printing

The location-based printing feature maps printers that are physically near client systems to remote desktops. Location-based printing enables 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.

Location-based printing works with Windows, Mac, Linux, and mobile client devices. It also works with browser-based clients. Location-based printing is supported on the following remote desktops and applications.

- Remote desktops that are deployed on single-user machines, including Windows desktop and Windows Server machines.
- Published desktops and published applications that are deployed on RDS hosts, where the RDS hosts are virtual machines or physical machines.

To use location-based printing, you must install the VMware Integrated Printing setup option in Horizon Agent, install the correct printer drivers on the remote desktop, and define translation rules for each location-based 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, VMware Horizon compares the client system to the translation rules. If the client system meets all the translation rules, VMware Horizon maps the printer to the remote desktop during the user's session.

You can disable location-based printing by enabling the **Disable LBP** group policy setting. For more information, see [VMware Integrated Printing Policy Settings](#).

### Install the Location-Based Printing User Interface

Before you can configure location-based printing, you must install the location-based printing user interface. The location-based printing user interface is distributed as a dynamic linked library (DLL) named `vmware-print-lbpsettingui.dll`. You install the DLL file as an MMC snap-in by running `InstallUtil.exe`.

#### Prerequisites

Sometimes, the operating system treats the `vmware-print-lbpsettingui.dll` file as an insecure binary file and blocks the DLL from loading. To unblock the file, right-click the filename, select **Properties**, click the **General** tab, and click **Unblock** in the Security section.

## Procedure

- 1 Download the VMware Horizon GPO bundle ZIP file from the VMware download site at <https://my.vmware.com/web/vmware/downloads> to your Active Directory server.

Under Desktop & End-User Computing, select the VMware Horizon download, which includes the GPO Bundle. The file is named `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyyy.zip`, where `YYMM` is the marketing version, `x.x.x` is the internal version, and `yyyyyyyyy` is the build number.

- 2 Extract the `vmware-print-lbpsettingui.dll` file from the ZIP file.

- 3 Open a command prompt with administrator privileges.

For example, click **Start**, type **command**, right-click **Command Prompt**, and select **Run as administrator**.

- 4 At the command prompt, run `InstallUtil.exe` to install the `vmware-print-lbpsettingui.dll` file.

For example:

```
installutil.exe C:\vmware-print-lbpsettingui.dll
```

`InstallUtil.exe` is usually in the `Microsoft.NET` directory, for example, `C:\Windows\Microsoft.NET\Framework64\v4.0.30319`.

- 5 To verify that the location-based printing user interface is installed, open the Group Policy Management Editor and navigate to **Computer Configuration > Software Settings**.

The **LBP Setting UI** group policy setting appears under **Software Settings** in the left navigation pane.

## What to do next

Configure the **LBP Setting UI** group policy setting. See [Configure Location-Based Printing](#).

## Configure Location-Based Printing

To set up location-based printing, you configure the **LBP Setting UI** group policy setting. The group policy setting is a name translation table that maps printers to remote desktops. 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, VMware Horizon 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, VMware Horizon 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. A group consists of multiple users and a user can belong to many groups. Depending on the group type, you can nest groups and grant access to resources.

You can specify one translation rule, or a combination of several translation rules, for a specific printer.

If you defined translation rules in a previous VMware Horizon release, and those rules are in an XML file, you can import the XML file into the **LBP Setting UI** group policy setting.

The information used to map the printer to the remote desktop is stored in the LBPSettingData registry entry on the remote desktop under HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\PrintRedir.

### Prerequisites

- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Install the vmware-print-lbpsettingui.dll file on your Active Directory server. See [Install the Location-Based Printing User Interface](#).
- Become familiar with the name translation table syntax. See [Location-Based Printing Translation Table Syntax](#).
- Create a GPO for the location-based group policy setting and link it to the OU that contains your remote desktops. See [Create GPOs for Horizon Group Policies](#) for an example of how to create GPOs for Horizon group policies.
- Because print jobs are sent directly from the remote desktop to the printer, verify that the required printer drivers are installed on your remote desktops.

### Procedure

- 1 On your Active Directory server, open the Group Policy Management Editor.
- 2 Expand **Computer Configuration**, open the **Software Settings** folder, and select **LBP Setting UI**.

Computer-specific policies apply to all remote desktops, regardless of who connects to the remote desktop.

- 3 In the Policy pane, double-click **Configure AutoConnect**.
- 4 Select **Enabled** to enable the group policy setting.

---

**Note** 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 remote desktops and define their associated translation rules.

Alternatively, if you have an existing configuration in an XML file, click the **Import configuration from existing file data** button to import the XML file.

6 To save your changes, click **OK**.

## Location-Based Printing Translation Table Syntax

**LBP Setting UI** is a name translation table that identifies printers and defines associated translation rules. Location-based printing maps local printers to remote desktops.

**Table 2-5. Translation Table Columns and Values**

Column	Description
Default	Indicates whether the printer is the default printer. By default, this value is not selected.
IP Range	<p>A translation rule that specifies a range of IP addresses for client systems.</p> <p>To specify IP addresses in a specific range, use the following notation: <b><i>ip_address–ip_address</i></b></p> <p>For example: <b>10.112.116.0–10.112.119.255</b></p> <p>To specify all of the IP addresses in a specific subnet, use the following notation: <b><i>ip_address/subnet_mask_bits</i></b></p> <p>For example: <b>10.112.4.0/22</b></p> <p>This notation specifies the usable IPv4 addresses from 10.112.4.1 to 10.112.7.254.</p> <p>Type an asterisk (the default value) to match any IP address.</p> <p><b>Important</b> In an IPv6 mixed-mode environment, add two IP address ranges for one printer (one range for IPv4 addresses and another range for IPv6 addresses) to ensure that the printer appears in remote sessions regardless of which protocol Horizon Client uses to connect.</p>
Client Name	<p>A translation rule that specifies a computer name. The maximum length is 1024 characters.</p> <p>For example: <b>Mary's Computer</b></p> <p>Type an asterisk to match any computer name.</p>
Mac Address	<p>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:</p> <ul style="list-style-type: none"> <li>■ Windows clients use hyphens: <b>01–23–45–67–89–ab</b></li> <li>■ Linux clients use colons: <b>01:23:45:67:89:ab</b></li> </ul> <p>Type an asterisk to match any MAC address.</p>

Table 2-5. Translation Table Columns and Values (continued)

Column	Description
User/Group	<p>A translation rule that specifies a user or group name.</p> <p>To specify a particular user or group, use the following notation:  <code>\\domain\user_or_group</code></p> <p>Examples for a user: <code>\\mydomain\Mary</code> and <code>Mary</code></p> <p>Example for a group: <code>\\localdomain\Sales</code></p> <p>A user can belong to many groups and groups consist of multiple users. Location-based printing supports the group types that Microsoft supports in the domain.</p> <p>The fully qualified domain name (FQDN) is not supported notation for the domain name. Type an asterisk to match any user or group name.</p>
Printer Name	<p>The name of the printer when it is mapped to the remote desktop.</p> <p>For example: <code>PRINTER-2-CLR</code></p> <p>The mapped name does not have to match the printer name on the client system.</p> <p>The printer must be local to the client device. Mapping a network printer in a UNC path is not supported.</p>
Printer Driver	<p>The name of the driver that the printer uses.</p> <p>For example: <code>HP Color LaserJet 4700 PS</code></p> <p><b>Important</b> Because print jobs are sent directly from the remote desktop to the printer, the printer driver must be installed on the remote desktop.</p>
IP Port	<p>For network printers, the IP address of the printer prepended with <code>IP_</code>. The default port is 9100.</p> <p>You can specify a non-default port by appending the port number to the IP address.</p> <p>For example, for IPv4: <code>IP_10.114.24.1:9104</code></p> <p>For example, for IPv6: <code>IP_1:1:1:1::1:PORT_9100</code></p>

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.

**Note** Location-based printing policies that use the MAC Address or client name are not supported if you use HTML Access to connect to remote desktops.

The following table shows an example of two translation table rows.

Table 2-6. Location-Based Printing Group Policy Setting Example

IP Range	Client Name	Mac Address	User/ Group	Printer Name	Printer Driver	IP 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.

## Configuring Windows Registry Settings for Cursor Event Handling

You can optimize cursor event handling by configuring Windows registry settings located in `\\HKLM\SOFTWARE\VMware Inc.\VMware Blast\Config` on the agent system.

These Windows registry settings on the agent machine allow you to configure coalescing mouse movement events allowed and low-latency channel use.

Setting	Type	Description
MouseMoveEventsCoalescingEnabled	REG_SZ	Determines whether coalescing mouse movement events is enabled or not. Values are 1 or 0. The default value is 1 (true).
ReflectCursorPositionEnabled	REG_SZ	Determines whether the low-latency channel is used for cursor updates. Values are 1 or 0. The default value is 1 (true).

You can also configure cursor event handling on the client machine. The settings on both the client and agent must match for the feature to be enabled. For information on the client-side settings, see the *VMware Horizon Client for Windows Installation and Setup Guide*, *VMware Horizon Client for Mac Installation and Setup Guide*, and *VMware Horizon Client for Linux Installation and Setup Guide*.

You can also configure a group policy setting for cursor warping. See [VMware Blast Policy Settings](#).

# 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 published application. You can redirect URLs that users type in the browser address bar or in an application.

This chapter includes the following topics:

- [Understanding URL Content Redirection](#)
- [Using URL Content Redirection in a Cloud Pod Architecture Environment](#)
- [System Requirements for URL Content Redirection](#)
- [Configuring Agent-to-Client Redirection](#)
- [Configuring Client-to-Agent Redirection](#)
- [Installing Browser Extensions for URL Content Redirection](#)
- [URL Content Redirection Limitations](#)
- [Unsupported URL Content Redirection Features](#)

## Understanding URL Content Redirection

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

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

You might want to set up the URL Content Redirection feature for security purposes. For example, if an end user clicks a link in their client browser that points to a URL outside your company network, that link might be opened more securely in a published application. With client-to-agent redirection, you can designate a certain published application to open the link from the client.

### **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.

For the list of browsers that support agent-to-client redirection, see the “Web browsers for Windows agents” section under [System Requirements for URL Content Redirection](#).

### **Client-to-agent redirection**

With client-to-agent redirection, Horizon Client opens a remote desktop or published 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 published application, the link is opened by the specified published application. The end user must be entitled to the desktop or application pool.

For the list of browsers that support client-to-agent redirection, see the sections for platform-specific clients under [System Requirements for URL Content Redirection](#).

You can redirect some URLs from a remote desktop or published application to a client, and redirect other URLs from a client to a remote desktop or published application. You can redirect any number of protocols, including HTTP, HTTPS, mailto, and callto. The callto protocol is not supported for redirection with the Chrome browser. You can also specify which applications are supported for the protocol in the URL.

## **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* document.

## **System 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.

### **Web browsers for Windows agents**

The following browsers are supported on Windows agents.

- Internet Explorer 11
- Chrome 60.0.3112.101 and later (Official Build), 64-bit or 32-bit
- Microsoft Edge (Chromium) 80.0.361.48 and later (Official Build), 64-bit or 32-bit

### Web browsers for Windows clients

The following browsers are supported on Windows clients.

- Internet Explorer 11
- Chrome 60.0.3112.101 and later (Official Build), 64-bit or 32-bit
- Microsoft Edge (Chromium) 80.0.361.48 and later (Official Build), 64-bit or 32-bit

### Web browsers for Mac clients

The following browsers are supported on Mac clients.

- Chrome 60.0.3112.101 and later (Official Build), 64-bit or 32-bit
- Microsoft Edge (Chromium) 87.0.664.60 and later (Official build)

### Web browsers for Linux clients

The following browsers are supported on Linux clients.

- Firefox 70.0 and later
- Chrome 87.0.4280.88 and later (Official Build), 64-bit

### Web browser extensions

You must install the VMware Horizon URL Content Redirection extension to use most supported browsers with URL Content Redirection. You do not need to install an extension for Internet Explorer. For installation instructions, see [Installing Browser Extensions for URL Content Redirection](#).

---

**Note** You must install the browser extensions before you enable URL Content Redirection in Horizon Agent or Horizon Client. If you do not, the JSON file does not load and URL Content Redirection does not work.

If you change a URL Content Redirection rule, the extension might remember the previous data cache. You must refresh the extension, either by restarting the browser or closing and reopening the extension, so that the new rule can take effect immediately.

---

### Windows clients

Install Horizon Client for Windows.

To use client-to-agent redirection, you must enable the URL Content Redirection feature during Horizon Client for Windows installation. See [Installing Horizon Client for Windows with](#)

the [URL Content Redirection Feature Enabled](#). You do not need to enable the URL Content Redirection feature in Horizon Client for Windows to use agent-to-client redirection.

### Mac clients

Install Horizon Client for Mac. Horizon Client for Mac adds support for client-to-agent redirection by default. No extra installation steps are required.

### Linux clients

Install Horizon Client for Linux. Horizon Client for Linux adds support for client-to-agent redirection by default. No extra installation steps are required.

### Virtual desktops and RDS hosts

To use agent-to-client redirection, install Horizon Agent with the URL Content Redirection feature enabled. See [Installing Horizon Agent with the URL Content Redirection Feature Enabled](#).

### Display protocols

- VMware Blast
- PCoIP

## 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 in the order shown.

- 1 Install the extensions for the browsers that you intend to use on the Windows agent machine.

Browser	Instructions
Chrome	<a href="#">Install and Enable the URL Content Redirection Helper Extension for Chrome on Windows</a>
Microsoft Edge (Chromium)	<a href="#">Install the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on Windows</a>

**Note** For Internet Explorer, VMware Horizon View URL Filtering Plugin is installed by default with Horizon Agent. See [Installing Horizon Agent with the URL Content Redirection Feature Enabled](#).

- 2 Enable the URL Content Redirection feature in Horizon Agent. See [Installing Horizon Agent with the URL Content Redirection Feature Enabled](#).
- 3 Apply the URL Content Redirection group policy settings to your remote desktops and published applications. See [Add the URL Content Redirection ADMX Template to a GPO](#).

- 4 Configure group policy settings to indicate, for each protocol, how Horizon Agent should redirect the URL. See [URL Content Redirection Group Policy Settings](#).

## Installing Horizon Agent with the URL Content Redirection Feature Enabled

To use URL content redirection from a remote desktop or published application to a client (agent-to-client 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-Horizon-Agent-x86-YYMM-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. If you are using the URL Content Redirection feature with Internet Explorer, also verify that the VMware Horizon View URL Filtering Plugin Internet Explorer add-on is enabled.

## 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 published application (client-to-agent redirection).

To apply the URL Content Redirection group policy settings to your remote desktops and published applications, add the ADMX template file to GPOs on your Active Directory server. For rules regarding URL links clicked in a remote desktop or published 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 `vmutil` command-line utility. Because macOS does not support GPOs, you must use `vmutil` 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 Enabled](#).
- 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 VMware Horizon 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 download, which includes the GPO Bundle.

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

- 2 Unzip the `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyyy.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. See [URL Content Redirection Group Policy Settings](#).

## URL Content Redirection Group Policy Settings

The URL Content Redirection template file (`urlRedirection.admx`) contains group policy settings that enable you to create rules for agent-to-client and client-to-agent redirection. The template file contains both Computer Configuration and User Configuration policies. All 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	Computer	User	Properties
IE Policy: Automatically enable URL Redirection plugin	X		Determines whether newly installed Internet Explorer plug-ins are automatically activated. This setting is not configured by default.
IE Policy: Prevent users from changing URL Redirection plugin loading behavior	X		Determines whether users can disable the URL Content Redirection feature. This setting is not configured by default.

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

Setting	Computer	User	Properties
Url Redirection Enabled	X		<p>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.</p> <p>This setting is not configured by default.</p>
Url Redirection IP Rules Enabled	X		<p>When this setting is enabled, you can enter a specific IP address or IP address range in <b>Client Rules</b> or <b>Agent Rules</b>. For more information, see <a href="#">IP Address and IP Address Range Filtering</a>.</p> <p>This setting is disabled by default.</p> <p><b>Note</b> This feature is supported only with Internet Explorer and IPv4.</p>
Url Redirection Protocol '...'	X		<p>Use this setting for any protocol other than HTTP and HTTPS, such as email or callto.</p> <p>The options are the same as for Url Redirection Protocol 'http' and Url Redirection Protocol 'https'.</p> <p>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.</p> <p>This setting is not configured by default.</p>
Url Redirection whitelist configuration	X		<p>Specifies the applications that the URL Content Redirection feature supports on Windows for the protocol in the URL. The following applications are supported by default:</p> <ul style="list-style-type: none"> <li>■ Internet Explorer (iexplore.exe)</li> <li>■ Chrome (chrome.exe)</li> <li>■ Firefox (firefox.exe)</li> <li>■ Microsoft Outlook (outlook.exe)</li> <li>■ Skype for Business (lync.exe)</li> <li>■ Skype (skype.exe)</li> <li>■ Windows Media Player (vmpayer.exe)</li> </ul> <p>You can modify the list of supported applications on Windows by configuring this group policy setting. For example, if you enter the following executable files in the <b>Whitelist</b> text box, URL Content Redirection supports only Chrome, Microsoft Outlook, and Skype:</p> <ul style="list-style-type: none"> <li>■ chrome.exe</li> <li>■ outlook.exe</li> <li>■ skype.exe</li> </ul> <p>This setting is not configured by default.</p>

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

Setting	Computer	User	Properties
Url Redirection Protocol 'http'	X		<p>For all URLs that use the HTTP protocol, specifies the URLs that should be redirected. This setting has the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Broker Hostname</b> - IP address or fully qualified name of the Connection Server host to use when redirecting URLs to a remote desktop or application.</li> <li>■ <b>Remote Item</b> - display name of the remote desktop or application pool that can handle the URLs specified in <b>Agent Rules</b>.</li> <li>■ <b>Client Rules</b> - the URLs that should be redirected to the client. For example, if you set <b>Client Rules</b> to <b>.*mycompany.com</b>, all URLs that include the text <b>mycompany.com</b> are redirected to the Windows-based client and are opened in the default browser on the client.</li> <li>■ <b>Agent Rules</b> - the URLs that should be redirected to the remote desktop or application specified in <b>Remote Item</b>. For example, if you set <b>Agent Rules</b> to <b>.*mycompany.com</b>, all URLs that include the text <b>mycompany.com</b> are redirected to the remote desktop or application.</li> </ul> <p>You can enter regular expressions in <b>Client Rules</b> and <b>Agent Rules</b>. If the <b>Url Redirection IP Rules Enabled</b> setting is enabled, you can also enter a specific IP address or IP address range. For complete syntax information, see <a href="#">Syntax for URL Content Redirection Rules</a>.</p> <p>When you create agent rules, you must also use the <b>Broker Hostname</b> option to specify the IP address or fully qualified domain name of the Connection Server host, and the <b>Remote Item</b> option to specify the display name of the desktop or application pool.</p> <p>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 <b>mycompany.com</b>, and that site redirects from HTTP to HTTPS automatically, the URL Content Redirection feature works 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.</p> <p>This setting is enabled by default.</p>

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

Setting	Computer	User	Properties
Url Redirection Protocol 'https'	X		<p>For all URLs that use the HTTPS protocol, specifies the URLs that should be redirected.</p> <p>The options are the same as for Url Redirection Protocol 'http'.</p> <p>This setting is not configured by default.</p>
Install the Chrome extension that is required in the URL content redirection feature.		X	<p>If this setting is enabled, the Chrome extension that the URL Content Redirection feature requires is installed silently and automatically. This installation also includes granting the necessary permissions. Reversing this installation requires administrative privileges.</p> <p>If this setting is disabled or is not configured, the Chrome extension that the URL Content Redirection feature requires is not installed, and URL content redirection does not work in the Chrome browser, even if redirection is set, unless the extension is installed from the Chrome Web Store manually.</p> <p>This setting is not configured by default.</p>

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.

The preferred method for configuring client-to-agent redirection is to use the `vdmutil` command-line utility instead of group policy settings.

## Syntax for URL Content Redirection Rules

When you use URL Content Redirection group policy settings, you must specify which URLs to open on the client (**Client Rules** option) or in a remote desktop or published application (**Agent Rules** option).

### URLs

You can enter URLs in **Client Rules** and **Agent Rules**. You can use wildcards (\*) to specify a URL pattern that matches multiple URLs. You must add an escape character (\) before a period to specify a period in a rule entry. For example, if you specify `".*\\.net"`, `xxx.net` is redirected, but `http://intranet` is not redirected.

The following table shows examples of rule entries that include URLs.



Rule Entry	Description
.*	Specifies that all URLs are redirected. If you use this setting for agent rules ( <b>Agent Rules</b> option), all URLs are opened in the specified remote desktop or published application. If you use this setting for client rules ( <b>Client Rules</b> option), all URLs are redirected to the client.
.*\acme\.com;.*\example\.com	Specifies that all URLs that include the text <b>.acme.com</b> or <b>.example.com</b> are redirected. Use semicolons to separate multiple entries. Spaces are not allowed between entries.
.*\acme\.com/software	Specifies that all URLs that include the text <b>.acme.com</b> and the subdirectory <b>/software</b> are redirected. For example, <code>http://www.acme.com/software</code> is redirected. Also, <code>http://www.acme.com/software/consumer</code> is redirected.
[space or leave empty]	Specifies that no URLs are redirected. For example, leaving the <b>Client Rules</b> option empty specifies that no URLs are redirected to the client.

## Regular Expressions

You can enter regular expressions in **Client Rules** and **Agent Rules**. For syntax information, see [Regular Expression Rules That URL Content Redirection Supports](#).

## IP Address and IP Address Range Filtering

If you enable the Url Redirection IP Rules Enabled group policy setting, you can enter a specific IP address or IP address range in **Client Rules** and **Agent Rules**.

For example, if you enable Url Redirection IP Rules Enabled and enter

"**.\*\mycompany\.com;22.22.22.22;10.10.1.2–10.10.12.20**", the following URLs and IP addresses are redirected.

- All URLs that include `.mycompany.com`
- IP address `22.22.22.22`
- All IP addresses in the range `10.10.1.2` through `10.10.12.20`
- All URLs that resolve into IP address `22.22.22.22`
- All URLs that resolve into the IP address range `10.10.1.2` through `10.10.12.20`

If you enter both a URL and an IP address or IP address range, the URL rule has the higher priority. If the URL is matched, redirection occurs directly by using the URL. If the URL is not matched, Horizon performs a DNS query and then does the IP address or IP address range filtering.

This feature is supported only with Internet Explorer and IPv4. It is disabled by default.

## Regular Expression Rules That URL Content Redirection Supports

You can enter a regular expression in **Client Rules** and **Agent Rules**. A regular expression is an object that describes a pattern of characters. Regular expressions perform pattern-matching and search-and-replace functions on text.

URL Content Redirection supports the following regular expression rules.

Rule	Detail
Brackets	[ ], [^ ], ( ), (?:), (?=)
\+metacharacter or metacharacter	'\w', '\W', '\d', '\D', '\b', '\B'
Quantifiers	+, *, ?, {x}, {x,y}, {x,}
Alternation	

For detailed information about regular expressions, see [https://en.wikipedia.org/wiki/Regular\\_expression](https://en.wikipedia.org/wiki/Regular_expression).

The following table contains examples of regular expression rules that URL Content Redirection supports.

Rule Entry	Examples of Matching URLs and IP Addresses
.*\.net	www.hello.net, www.inter.net, train.word.net, test.train.net, and train.chromeie.net.com.cn.
.*\.sth\.ctirial	example.sth.ctirial, www.google.sth.ctirial, and www.google.com/test.sth.ctirial/editpage.action.
.*administra	www.administra.com, www.askadministra-tor.net, and google.akmkda.eae/administra.cn.
.*a{4}custom\.com	world.banada.cn/aaaacustom.com, www.aaaacustom.com, and exple.aaaacustom.com.net/nodepad.action.
.*a{2,3}custom\.com	world.banada.aacustom.com, www.aacustom.com, and exple.aacustom.com.net/nodepad.action.
.*train[abc]\.net	hello.traina.net, hello.trainb.net, example.trainc.net.com, and www.testtraina.net.com/edit.
.*train[^abc]\.net	hello.traind.net, hello.traine.net, example.train2.net.com, and www.testtrain3.net.com/edit.
.*a+c*tra\.net	www.actra.net.com. aactra.net.cn, atra.net.www.train, and aaccetra.network.
.*example(test)?\.cn	www.example.cn, www.exampletest.cn, example.cn/editpage, and exampletest.cn/editpage.
sac(=?sprt)	helloworld.sacsprt.net, examplesacsprt.com/text, and www.sacsprtexam.com.
sac(?!sprt)	helloworld.sacspra.net, examplesacbprrt.com/text, and www.sacexam.com.
10\.1\.1\.1[0-5]	10.1.1.10 through 10.1.1.15.
10\.1\.(1 2)\.1[0-5]	10.1.1.10 through 10.1.1.15 and 10.1.2.10 to 10.1.2.15.
10\. [2-4]\.19\.12	10.2.19.12, 10.3.19.12, and 10.4.19.12.
10\. [^2-4]\.19\.12	10.6.19.12, 10.1.19.12, 10.5.19.12, and 10.7.19.12.

Rule Entry	Examples of Matching URLs and IP Addresses
<code>a(\w)cd(\d)345a\.com</code>	<code>www.abccd2345a.com.net</code> and <code>train.adc2cd1345a.com/edit.action</code> .
<code>abc(\W)cd(\D)345a\.com</code>	<code>google.abc+cda345a.com</code> and <code>test.train.net/abc&amp;cda345a.com</code> .
<code>((25[0-5] 2[0-4][0-9] [01]?[0-9]?[0-9])\.){3}(25[0-5] 2[0-4][0-9] [01]?[0-9]?[0-9])</code>	All IPv4 addresses.
<code>.*example(test)? \.cn;10\.1\.1\.1[0-5];a(\w)cd(\d)345a\.com</code>	<code>www.example.cn</code> , <code>example.cn/editpage</code> , <code>10.1.1.10</code> to <code>10.1.1.15</code> , <code>www.abccd2345a.com.net</code> , and <code>train.adc2cd1345a.com/edit.action</code> .

## 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 watch videos in a remote desktop or published application, for example, you might redirect those URLs to the client machine so that no extra load is put on the data center. For employees that work outside the company network, you might want all URLs that point to external locations outside the company network to open on an employee's own client machine for security purposes.

For example, you can configure rules so that any URLs that do not point to the company network are redirected to open on the client machine. In this example, you might use the following settings, which include regular expressions:

- For **Agent Rules**: `.*.mycompany.com`

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

- For **Client Rules**: `.*`

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 published application or remote desktop, the client rules are checked first.
- 2 If the URL matches a client rule, the agent rules are checked next.
- 3 If a conflict exists between the agent and client rules, the link opens locally. In this example, the URL opens on the agent machine.
- 4 If no conflicts exist, the URL is redirected to the client.

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

## Configuring Client-to-Agent Redirection

With client-to-agent redirection, Horizon Client opens a remote desktop or published 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 published application is opened, the published application processes the URL.

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

- 1 Install the browser extensions for the clients and browsers that you intend to use with the URL Content Redirection feature.

Client	Browser	Instructions
Linux	Firefox	<a href="#">Install and Enable the VMware Horizon URL Redirection Extension for Firefox on Linux</a>
Linux	Chrome	<a href="#">Install and Enable the VMware Horizon URL Content Redirection Helper for Chrome on Linux</a>
Windows	Chrome	<a href="#">Install and Enable the URL Content Redirection Helper Extension for Chrome on Windows</a>
Windows	Microsoft Edge (Chromium)	<a href="#">Install the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on Windows</a>
Mac	Chrome	<a href="#">Enable the URL Content Redirection Helper for Chrome on a Mac</a>
Mac	Microsoft Edge (Chromium)	<a href="#">Install and Enable the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on a Mac</a>

**Note** For Internet Explorer, VMware Horizon View URL Filtering Plugin is installed by default with Horizon Client. See [Installing Horizon Client for Windows with the URL Content Redirection Feature Enabled](#).

- 2 Install the URL Content Redirection feature on the client machine.
  - a For Windows clients, install Horizon Client for Windows with the URL Content Redirection feature enabled. See [Installing Horizon Client for Windows with the URL Content Redirection Feature Enabled](#).
  - b For Mac and Linux clients, install Horizon Client. The URL Content Redirection feature is enabled by default when you install Horizon Client for Mac and Horizon Client for Linux. No additional steps are required to enable the URL Content Redirection feature on these clients.
- 3 Use the `vdmutil` command-line utility on a Connection Server instance 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](#).

- 4 Use the `vdmutil` command-line utility on a Connection Server instance 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](#).
- 5 Verify the URL content redirection setting. See [Test a URL Content Redirection Setting](#).

---

**Important** 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 and Linux clients, you must use `vdmutil` to configure client-to-agent redirection. Because macOS and Linux do not support GPOs, you cannot use group policy settings to configure client-to-agent configuration if you have Mac or Linux clients.

---

## Using the `vdmutil` Command-Line Utility on a Connection Server Instance

You can use the `vdmutil` command-line interface on a Connection Server instance 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 Console to assign the Administrators role to a user. For more information, see the *Horizon 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 <b>domain\username</b> 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.

**Table 3-3. vdmutil Command Options for URL Content Redirection (continued)**

Option	Description
<code>--removeUserURLSetting</code>	Removes a user assignment from a URL content redirection setting.
<code>--updateURLSetting</code>	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`.

## Syntax for the `--agentURLPattern` Option

When you use the `vdmutil` command on a Connection Server instance to create a URL Content Redirection setting, you type a quoted string that specifies the URL, or URLs, that should be opened on the remote desktop or published application in the `--agentURLPattern` option.

The quoted string contains a regular expression and must include the protocol prefix. You can use wildcards to specify a URL pattern that matches multiple URLs.

The following table describes some sample URL patterns.

Agent URL Pattern	Description
<code>".*"</code>	All client URLs are redirected to the remote desktop or published application.
<code>"http://google.*"</code>	All client URLs that include the text <b>google</b> are redirected to the remote desktop or published application.
<code>"http://acme.com/software"</code>	All client URLs that include the text <b>acme.com</b> and the subdirectory <b>/software</b> are redirected to the remote desktop or published application. For example, <code>http://www.acme.com/software</code> is redirected. Also, <code>http://www.acme.com/software/consumer</code> is redirected.

## 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 published 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. The callto protocol is not supported for redirection with the Chrome browser.

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 redirects from HTTP to HTTPS automatically, the URL Content Redirection feature works 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.

VMware recommends that you do not create more than one setting for URL content redirection.

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 `vdmutl` command-line interface options and requirements and verify that you have sufficient privileges to run the `vdmutl` command. See [Using the `vdmutl` Command-Line Utility on a Connection Server Instance](#).
- Become familiar with the syntax for URLs in URL content redirection settings. See [Syntax for the `--agentURLPattern` Option](#).

## Procedure

- 1 Log in to the Connection Server instance.
- 2 Run the `vdmutl` command with the `--createURLSetting` option to create the URL content redirection setting.

```
vdmutl --createURLSetting --urlSettingName url-filtering --urlRedirectionScope LOCAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

Option	Description
<code>--urlSettingName</code>	Unique name for the URL content redirection setting. The name must be <b>url-filtering</b> .
<code>--urlRedirectionScope</code>	Scope of the URL content redirection setting. Specify LOCAL to make the setting visible only in the local pod.
<code>--description</code>	Description of the URL content redirection setting. The description can contain between 1 and 1024 characters.
<code>--urlScheme</code>	Protocol to which the URL content redirection setting applies, for example, http, https, mailto, or callto.
<code>--entitledApplication</code>	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.
<code>--entitledDesktop</code>	Display name of a local desktop pool to use to open the specified URLs, for example, Win10. For RDS desktop pools, use the <code>--entitledApplication</code> option.
<code>--agentURLPattern</code>	A quoted string that specifies the URL that should be opened on the remote desktop or published application.

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

```
vdmutl --updateURLSetting --urlSettingName url-filtering --urlRedirectionScope LOCAL
[--description value][--urlScheme value][--entitledApplication value | --entitledDesktop value]
[--agentURLPattern value]
```

The options are the same as for the `vdmutl` 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 published 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. The callto protocol is not supported for redirection with the Chrome browser.

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 redirects from HTTP to HTTPS automatically, the URL Content Redirection feature works 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* document.

VMware recommends that you do not create more than one setting for URL content redirection. 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 `vdmutil` command. See [Using the `vdmutil` Command-Line Utility on a Connection Server Instance](#).
- Become familiar with the syntax for URLs in URL content redirection settings. See [Syntax for the `--agentURLPattern` Option](#).

### 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 url-filtering --urlRedirectionScope GLOBAL
[--description value] [--urlScheme value] [--entitledApplication value | --entitledDesktop
value] [--agentURLPattern value]
```

Option	Description
<code>--urlSettingName</code>	Unique name for the URL content redirection setting. The name must be <b>url-filtering</b> .
<code>--urlRedirectionScope</code>	Scope of the URL content redirection setting. Specify GLOBAL to make the setting visible across the pod federation.
<code>--description</code>	Description of the URL content redirection setting. The description can contain between 1 and 1024 characters.
<code>--urlScheme</code>	Protocol to which the URL content redirection setting applies, for example, http, https, mailto, or callto.
<code>--entitledApplication</code>	Display name of a global application entitlement to use to open the specified URLs.
<code>--entitledDesktop</code>	Display name of a global desktop entitlement to use to open the specified URLs, for example, GE-1.
<code>--agentURLPattern</code>	A quoted string that specifies the URL that should be opened on the remote desktop or published 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 url-filtering --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 `url-filtering` that redirects all client URLs that include the text `http://google.*` to the global application entitlement called `GAE1`.

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

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

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

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

```
vdmutil --updateURLSetting --urlSettingName url-filtering --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 on a Connection Server Instance](#).

## Procedure

- ◆ To assign a URL Content Redirection setting to a user, on the Connection Server instance, run the `vdmutil` command with the `--addUserURLSetting` option.

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

Option	Description
<code>--urlSettingName</code>	Name of the URL content redirection setting to assign. It must be <b>url-filtering</b> .
<code>--userName</code>	Name of the Active Directory user in <code>domain\username</code> 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
<code>--urlSettingName</code>	Name of the URL Content Redirection setting to assign. It must be <b>url-filtering</b> .
<code>--groupName</code>	Name of the Active Directory group in <code>domain\group</code> 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](#).

## Installing Horizon Client for Windows with the URL Content Redirection Feature Enabled

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

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-YYMM-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

To verify that the URL Content Redirection feature is enabled, 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. If you are using the URL Content Redirection feature with Internet Explorer, also verify that the VMware Horizon View URL Filtering Plugin Internet Explorer add-on is installed.

## 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 `vdmutil` command. See [Using the vdmutil Command-Line Utility on a Connection Server Instance](#).

### 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, perform the following steps.
  - a 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.
  - b 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.
- 4 On a Mac client, perform the following steps.
  - a Open Horizon Client and connect to the Connection Server instance.
  - b In a third-party application such as Notes, click URLs that match the URL patterns configured in the setting and verify that the URLs are redirected as expected.
  - c Verify that the JSON file is created.

**Note** The JSON file is created when the VMware URL Content Redirection Helper extension is installed.

Browser	Path
Chrome	~/Library/Application Support/Google/Chrome/Default/Extensions/lfidjngibpklhhijphdmbmedchiolgk/version/data.json
Edge	~/Library/Application Support/Microsoft Edge/Default/Extensions/lfidjngibpklhhijphdmbmedchiolgk/version/data.json

- 5 On a Linux client, perform the following steps.
  - a Open Horizon Client and connect to the Connection Server instance.
  - b Verify that the JSON file is created for the third-party application and browser.

**Note** The JSON file is created when the VMware URL Content Redirection helper extension is installed.

Component	Path
Third-party application	~/.vmware/broker-url-config.json
Chrome	~/.config/google-chrome/Default/Extensions/lfidjngibpklhhijphdmbmedchiolgk/version/data.json
Firefox	~/.mozilla/managed-storage/url_redirection@vmware.com.json

## 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 on a Connection Server Instance](#).

### 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 published application (client-to-agent redirection).

---

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

---

To create a rule for client-to-agent redirection, you use the **Remote Item** option to specify the display name of a desktop or application pool and the **Agent Rules** option to specify the URLs that should be redirected to the remote desktop or published application. You must also use the **Broker Hostname** 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 published 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 published application. In this case, you might set the **Agent Rules** option to `.*.mycompany.com`.

For URL Content Redirection template file installation instructions, group policy setting descriptions, and **Agent Rules** option syntax, see [Configuring Agent-to-Client Redirection](#).

## Installing Browser Extensions for URL Content Redirection

You must install the VMware Horizon URL Content Redirection extension to use most supported browsers with URL Content Redirection. You do not need to install an extension for Internet



Explorer. You must install the browser extensions before you enable URL Content Redirection in Horizon Agent or Horizon Client.

## Install and Enable the URL Content Redirection Helper Extension for Chrome on Windows

To use the Chrome browser with the URL Content Redirection feature on a Windows client or Windows agent machine, you must install and enable the VMware Horizon URL Content Redirection Helper extension for Chrome.

You can install and enable the VMware Horizon URL Content Redirection Helper extension by enabling a URL Content Redirection group policy setting.

This procedure describes how to apply the URL Content Redirection group policy setting to GPOs on your Active Directory server. For Windows client machines, the GPO must be linked to the OU that contains your Windows client computers. For remote desktops and applications, the GPO must be linked to the OU that contains your virtual desktops and RDS hosts.

If you do not use group policy to install and enable the VMware Horizon URL Content Redirection Helper extension, you must install the extension manually from the Chrome Web Store.

### Prerequisites

- Install the Chrome browser. For supported versions, see [System Requirements for URL Content 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 URL Content Redirection ADMX Template file to your Active Directory server. See [Add the URL Content Redirection ADMX Template to a GPO](#).

### Procedure

- 1 To apply the URL Content Redirection group policy setting to GPOs on your Active Directory server, perform the following steps.
  - a On your Active Directory server, open the Group Policy Management Editor and navigate to the **User Configuration > Policies > Administrative Templates > VMware Horizon URL Redirection** folder.
  - b Open the **Install the Chrome extension that is required in the URL content redirection feature** setting, select **Enabled**, and click **OK**.

- c Start Chrome on the Windows machine.

The VMware Horizon URL Content Redirection Helper extension is installed silently.

- d To verify that the Chrome extension is installed, type **chrome://extensions** in the Chrome browser.

**VMware Horizon URL Content Redirection Helper** appears in the Extensions list and the **Enabled** check box is selected.

- 2 To install the extension manually from the Chrome Web Store, perform the following steps.
  - a In the Chrome browser, go to the Chrome Web Store.
  - b Search for **VMware Horizon URL Content Redirection Helper**.
  - c Select **VMware Horizon URL Content Redirection Helper** and click **Add to Chrome**.

### Results

The first time a URL is redirected from the Chrome browser on the client, the user is prompted to open the URL in Horizon Client. The user must click **Open URL:VMware Hori...lient Protocol**, or URL redirection does not occur. If the user selects the **Remember my choice for URL:VMware Hori...lient Protocol links** check box (recommended), this prompt does not appear again.

## Install the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on Windows

To use the Microsoft Edge (Chromium) browser with the URL Content Redirection feature on a Windows client or Windows agent machine, you must install the VMware Horizon URL Content Redirection Helper extension in the Microsoft Edge (Chromium) browser.

You install the VMware Horizon URL Content Redirection Helper extension from the Chrome Web Store.

### Prerequisites

Install the Microsoft Edge (Chromium) browser on the Windows client machine. For supported versions, see [System Requirements for URL Content Redirection](#).

### Procedure

- 1 In the Microsoft Edge (Chromium) browser, enter <https://chrome.google.com/webstore/detail/vmware-horizon-url-content-redirection-helper/lfidjngibpklhijphdmbmedchiiolgk>.
- 2 Click the **Add extensions from other stores** button at the top of the browser window and click **Allow**.
- 3 Click **Add to Chrome**.
- 4 When you are prompted to add the extension to Microsoft Edge (Chromium), click **Add extension**.

- 5 To verify that the extension is installed, click the **Settings and more (...)** icon in the upper-right corner of the browser window and select **Extensions**.

VMware Horizon URL Content Redirection Helper appears in the Installed extensions list.

#### Results

The first time a URL is redirected from the Microsoft Edge (Chromium) browser on the client, the user is prompted to open the URL in Horizon Client. The user must click **Open URL:VMware Hori...lient Protocol**, or URL redirection does not occur.

## Enable the URL Content Redirection Helper for Chrome on a Mac

To use the Chrome browser with the URL Content Redirection feature on a Mac client, you must enable the VMware Horizon URL Content Redirection Helper extension for Chrome.

#### Prerequisites

Install the Chrome browser on the Mac client. For the supported versions, see [System Requirements for URL Content Redirection](#).

#### Procedure

- 1 In the Chrome browser, go to the Chrome Web Store.
- 2 Search for **VMware Horizon URL Content Redirection Helper**.
- 3 Select **VMware Horizon URL Content Redirection Helper** and click **Add to Chrome**.
- 4 To verify that the Chrome extension is installed, type **chrome://extensions** in the Chrome browser.

**VMware Horizon URL Content Redirection Helper** appears in the Extensions list and the **Enabled** check box is selected.

#### Results

The first time a URL is redirected from the Chrome browser on the Mac client, the user is prompted to open the URL in Horizon Client. The user must click **Open VMware Horizon Client**, or URL redirection does not occur. If the user selects the **Remember my choice for VMware Horizon Client links** check box (recommended), this prompt does not appear again.

## Install and Enable the URL Content Redirection Helper Extension for Microsoft Edge (Chromium) on a Mac

To use the Microsoft Edge (Chromium) browser with the URL Content Redirection feature on a Mac client, you must install the VMware Horizon URL Content Redirection Helper extension in the Microsoft Edge (Chromium) browser.

You install the VMware Horizon URL Content Redirection Helper extension from the Chrome Web Store.

### Prerequisites

Install the Microsoft Edge (Chromium) browser on the Mac client. For supported versions, see [System Requirements for URL Content Redirection](#).

### Procedure

- 1 In the Microsoft Edge (Chromium) browser, enter <https://chrome.google.com/webstore/detail/vmware-horizon-url-content-redirector/lfidjngibpkllhijphdmbmedchiioigk>.
- 2 Click the **Add extensions from other stores** button at the top of the browser window and click **Allow**.
- 3 Click **Add to Chrome**.
- 4 When you are prompted to add the extension to Microsoft Edge (Chromium), click **Add extension**.
- 5 To verify that the extension is installed, click the **Settings and more (...)** icon in the upper-right corner of the browser window and select **Extensions**.

VMware Horizon URL Content Redirection Helper appears in the Installed extensions list.

### Results

When you start Horizon Client and connect to a Connection Server instance on which the URL Content Redirection settings have been configured, Horizon Client downloads the necessary URL Content Redirection configurations to the Mac client. Restart the Microsoft Edge (Chromium) browser on the Mac client.

## Install and Enable the VMware Horizon URL Redirection Extension for Firefox on Linux

To use the Firefox browser for client-to-agent URL content redirection from a Linux client, you must install and enable the VMware Horizon URL Redirection Extension for Firefox.

You can use the Firefox Add-ons Manager to find the installer for the VMware Horizon URL Redirection Extension.

### Prerequisites

- Install the Firefox browser on the Linux client system. For the supported browser versions, see [System Requirements for URL Content Redirection](#).
- Install Horizon Client for Linux on the Linux client system. For instructions, see the *VMware Horizon Client for Linux Installation and Setup Guide* document.
- Configure URL Content Redirection settings on the Connection Server instance. See [Configuring Client-to-Agent Redirection](#).

## Procedure

- 1 Start Firefox on the Linux system.

Starting the browser creates a profile folder on the client system that is required to support the URL Content Redirection feature.

- 2 From the Firefox menu, select **Add-ons**.

- 3 In the **Add-ons Manager** page, type **vmware** into the search text box to locate the VMware Horizon URL Redirection Extension.

- 4 Select the VMware Horizon URL Redirection Extension, and follow the prompts to add this extension to Firefox.

- 5 To verify that the Firefox extension is installed, return to the **Add-ons Manager** page and click **Extensions**. Verify that the extension appears under the **Enabled** list.

- 6 Start Horizon Client on the Linux system and connect to a Connection Server instance on which URL Content Redirection settings have been configured.

Horizon Client downloads the necessary URL Content Redirection configurations to the Linux system.

- 7 Restart Firefox.

## What to do next

The first time a URL is redirected from the Firefox browser on the Linux client, the user is prompted to open the URL in Horizon Client. The user must specify Horizon Client as the application for opening the URL and click **Open link**, or URL redirection does not occur. If the user selects the option to remember this choice and always allow links to be opened with Horizon Client (recommended), this prompt does not appear again.

## Install and Enable the VMware Horizon URL Content Redirection Helper for Chrome on Linux

To use the Chrome browser for client-to-agent URL content redirection from a Linux client, you must install and enable the VMware Horizon URL Content Redirection Helper extension for Chrome.

You can use the Chrome extensions page to find the installer for the VMware Horizon URL Content Redirection Helper.

## Prerequisites

- Install the Chrome browser on the Linux client system. For the supported browser versions, see [System Requirements for URL Content Redirection](#).
- Install Horizon Client for Linux on the Linux client system. For instructions, see the *VMware Horizon Client for Linux Installation and Setup Guide* document.

- Configure URL Content Redirection settings on the Connection Server instance. See [Configuring Client-to-Agent Redirection](#).

#### Procedure

- 1 Start the Chrome browser on the Linux system and navigate to the extensions page.
- 2 On the extensions page, search for the VMware Horizon URL Content Redirection Helper.
- 3 Select the VMware Horizon URL Content Redirection Helper, and follow the prompts to add this extension to Chrome.
- 4 To confirm that the extension is installed and enabled, return to the extensions page. Verify that the VMware Horizon URL Content Redirection Helper appears on the page and that its enablement toggle is set to the on position.
- 5 Start Horizon Client on the Linux system and connect to a Connection Server instance on which URL Content Redirection settings have been configured.

Horizon Client downloads the necessary URL Content Redirection configurations to the Linux system.

- 6 Restart Chrome.

## Using Internet Explorer (IE) Mode in Microsoft Edge (Chromium) with URL Content Redirection

You can use Internet Explorer (IE) mode with the URL Content Redirection feature in Microsoft Edge (Chromium). This feature is supported for agent-to-Windows client and Windows client-to-agent URL content redirection.

There are two independent switches for the Internet Explorer and Microsoft Edge (Chromium) browsers.

- VMware Horizon View URL Filtering Plugin is installed for supporting the URL Content Redirection feature for the Internet Explorer browser. This plug-in is installed when you install Horizon Client for Windows or Horizon Agent with the URL Content Redirection feature enabled. See [Installing Horizon Client for Windows with the URL Content Redirection Feature Enabled](#) and [Installing Horizon Agent with the URL Content Redirection Feature Enabled](#). IE mode in Microsoft Edge (Chromium) uses the Internet Explorer browser's VMware Horizon View URL Filtering Plugin for URL content redirection.
- You install the URL Content Redirection extension for the Microsoft Edge (Chromium) browser from the related web store. See [Install the URL Content Redirection Helper Extension for Microsoft Edge \(Chromium\) on Windows](#).

To use the URL Content Redirection feature in IE mode in the address bar in the Microsoft Edge (Chromium) browser, enable the VMware Horizon View URL Filtering Plugin in **Manage add-ons** in the Internet Explorer browser. The IP Rules and Regular Expressions modes are both supported. For more information, see [Syntax for URL Content Redirection Rules](#). The Microsoft Edge (Chromium) extension (see [Install the URL Content Redirection Helper Extension for Microsoft Edge \(Chromium\) on Windows](#)) is optional for this use case, but is required for other URLs that are not set under rules for IE Mode.

To use the URL Content Redirection feature in the Microsoft Edge (Chromium) browser address bar (not IE mode), enable the VMware Horizon URL Content Redirection Helper extension in the Microsoft Edge (Chromium) browser. Disable the IE plugin if you do not want to use IE mode. Regular Expressions mode is supported.

For feature limitations, see [URL Content Redirection Limitations](#).

## 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.
- If you do not install the browser extensions for URL Content Redirection before you enable the URL Content Redirection feature in Horizon Agent or Horizon Client, the JSON file does not load and the URL Content Redirection feature does not work.
- Roaming profiles are not supported with the URL Content Redirection feature in the Windows agent or Windows client.

- To support published Chrome and Microsoft Edge (Chromium) browsers in an RDS host, the URL Content Redirection browser extension must use a helper process that is started by Windows Explorer (`explorer.exe`). If the helper process is not started, URL Content Redirection does not work in Chrome and Microsoft Edge (Chromium). URL Content Redirection is supported if the published application is the Internet Explorer browser or a non-browser application, such as WordPad or Word.
- If you disable the IE browser URL Plugin, enable the Microsoft Edge (Chromium) browser URL Content Redirection extension, and input a URL in the IE mode of the Microsoft Edge (Chromium) address bar, Microsoft Edge (Chromium) stops responding. Make sure that the IE browser plugin is enabled if you want to use IE mode.
- If you enable the IE browser URL Plugin and the Microsoft Edge (Chromium) browser URL Content Redirection extension and input a URL in the Microsoft Edge (Chromium) browser address bar (not in IE mode), the URL is redirected twice.

## 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, Groove 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.

# 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 virtual desktop. This feature is called USB redirection. A virtual desktop can accommodate up to 255 USB devices.

You can also redirect certain locally connected USB devices for use in published desktops and applications. For information about the specific types of devices that are supported, see [Limitations Regarding USB Device Types](#).

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 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 the types of USB devices to which end users are allowed to connect. 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 certain types of clients. To find out whether this feature is supported on a particular client, see the feature support matrix included in the Horizon Client installation and setup document for that client.

---

**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 VMware Horizon Environment](#).

---

This chapter includes the following topics:

- [Limitations Regarding USB Device Types](#)

- [USB Redirection Recommendations](#)
- [Overview of Setting Up USB Redirection](#)
- [Configuring USB Redirection for Google Chrome, Microsoft Edge, and HTML Access Clients](#)
- [Configuring Fingerprint Scanner and Microscope Redirection](#)
- [Configuring Card Reader Redirection](#)
- [Configuring Microsoft Xbox One Controller Redirection](#)
- [Network Traffic and USB Redirection](#)
- [Automatic Connections to USB Devices](#)
- [Deploying USB Devices in a Secure VMware Horizon Environment](#)
- [Using Log Files for Troubleshooting and to Determine USB Device IDs](#)
- [Using Policies to Control USB Redirection](#)
- [Troubleshooting USB Redirection Problems](#)

## Limitations Regarding USB Device Types

Although VMware Horizon does not explicitly prevent any devices from working with the USB redirection feature, 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.

### USB 3.0 Device Limitations

You can plug USB 3.0 devices into USB 3.0 ports on the client machine. USB 3.0 devices are supported only with a single stream. Because multiple stream support is not implemented, 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 remote session, due to network latency.

### USB Redirection with Virtual Desktops

The following types of USB 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 and scanners 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.

## USB Redirection with Published Desktops and Applications

You can redirect locally connected USB thumb flash drives and hard disks for use in published desktops and applications. Published desktops and applications can also support more generic USB devices, including TOPAZ Signature Pad, Olympus Dictation Foot pedal, and Wacom signature pad. Other types of USB devices, including security storage drives and USB CD-ROM drives, are not supported in published desktops and applications.

## USB Redirection Recommendations

You can use recommended solutions to USB redirection for some types of USB devices.

Instead of using USB redirection, use these redirection features that provide better performance and user experience:

- For scanners, use scanner redirection. See [Configuring Scanner Redirection](#).
- For printers, use printer redirection. See [Configuring VMware Integrated Printing](#).
- For smart card readers, use smart card redirection. See the *Horizon Administration* document.
- For serial port devices, use serial port redirection. See [Configuring Serial Port Redirection](#).
- Use client drive redirection for file sharing instead of USB redirection for USB disks and massive storage devices. See [Managing Access to Client Drive Redirection](#).

## 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 Horizon 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. To find out whether this feature is supported on a particular type of client, see the feature support matrix included in the installation and setup document for the specific type of client device.

---

**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 VMware Horizon 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, 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 Horizon Administrator.

In Horizon 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 clients, you can configure group policies. For Mac clients, you use a command-line command. For more information, see the installation and setup 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.

## Configuring USB Redirection for Google Chrome, Microsoft Edge, and HTML Access Clients

To use the USB redirection feature with Horizon Client for Google Chrome, Microsoft Edge (Chromium) browser, and HTML Access clients, you must perform some additional steps.

- 1 Install the USB Redirection component in Horizon Agent. See [Overview of Setting Up USB Redirection](#).
- 2 Set the `UsbVirtualChannelEnabled` registry key to true on the agent machine. See [Enabling the USB Over Session Enhancement SDK Feature](#).
- 3 Using the administrator account, install the USB device driver on the agent machine.

For information about configuring USB redirection for Linux remote desktops, see "VHCI Driver for USB Redirection" in the *Setting Up Linux Desktops in Horizon* document.

For information about using USB redirection in Horizon Client for Google Chrome, Microsoft Edge (Chromium), or HTML Access, see the client's user guide or installation and setup guide.

## Configuring Fingerprint Scanner and Microscope Redirection

You can redirect biometric devices, specifically fingerprint scanners, that are plugged into a USB port on a Windows client system, to virtual desktops. You can also redirect Dino-Lite USB microscopes from a Windows, Mac, or Linux client system to virtual desktops.

### Configuring Fingerprint Scanner Redirection

To redirect these fingerprint scanners, you need a minimum of 200 Mbps network bandwidth on the remote agent desktop.

These fingerprint scanning devices are supported:

**Table 4-1. Supported Fingerprint Scanners**

Device	Client OS	Windows OS Servers	Protocols
U.are.U 5160 Fingerprint Reader	Windows 10 1809 64-bit	Windows 10 1809 64-bit Windows 10 1903 64-bit	PCoIP, Blast
U.are.U 5300 Fingerprint Reader	Windows 10 1809 64-bit	Windows 10 1809 64-bit Windows 10 1903 64-bit	PCoIP, Blast

### Configuring Microscope Redirection

To redirect USB microscope devices, you must meet these network requirements:

Table 4-2. Network Requirements for Microscope Redirection

Network Requirement	For Client-to-Agent Data Transfer	For Agent-to-Client Data Transfer
Bandwidth	At least 400 Mbps	At least 20 Mbps
Delay	1 ms or less	2 ms or less
Loss	0.005% or less	0.005% or less

Windows and Mac client systems allow USB redirection of supported microscopes by default.

Linux client systems exclude microscopes from USB redirection by default. To use redirection, you must allow the microscope device by setting the **viewusb.IncludeVidPid** property. See the "Setting USB Configuration Properties" topic in *VMware Horizon Client for Linux Installation and Setup Guide*.

To optimize performance, configure the microscope settings as follows:

- Set the resolution to **640 x 480**.
- Set **Video Encoder** to **MJPEG**.
- Reduce or turn off the auto-exposure setting.

These USB microscope devices are supported:

Table 4-3. Supported USB Microscopes

Device	Client OS	Windows OS Remote Agent Desktop	Protocols
Dino-Lite Premier AM4113ZT	Windows Mac Linux (kernel version 3.3-rc1 or later)	Windows 10	PCoIP, Blast

## Configuring Card Reader Redirection

You can redirect card readers that are plugged into a USB port over PCoIP virtual channel on a Windows client system to virtual desktops.

These card readers are supported:

Table 4-4. Supported Card Readers

Device	Client OS	Windows OS Servers	Protocol
Sony FeliCa RC-S320	Windows 10 1809 64-bit	Windows 10 1809 64-bit Windows 10 1903 64-bit	PCoIP
Sony PaSoRi RC-S380	Windows 10 1809 64-bit	Windows 10 1809 64-bit Windows 10 1903 64-bit	PCoIP

## Configure USB over PCoIP Virtual Channel

To configure USB over PCoIP virtual channel using UDP port 4172, modify the registry in Horizon Agent:

- 1 Set the registry HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration\UsbVirtualChannelEnabled (REG\_SZ) to true.
- 2 Set the registry HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware UsbRedirection\sideChannelType (REG\_SZ) to pcoip.
- 3 Reboot the Horizon Agent VM.

To check the configuration is in effect:

- 1 Connect the Horizon Agent desktop with PCoIP protocol.
- 2 Check the Horizon Client log from "C:\Users\\AppData\Local\Temp\vmware-  
<username>\vmware-UsbRedirectionClient-xxxx.log". If the configuration is in effect, you can find the "RPCManager::OnChannelDataObjectStateChanged(): Requesting virtual side channel" in this file.

## Configuring Microsoft Xbox One Controller Redirection

You can redirect Microsoft Xbox One controllers that are plugged into a USB port on a Windows client system to virtual desktops.

To redirect these tested Xbox One controllers, verify the setting **Connect USB Device > Automatically Connect When inserted** is enabled in the VMware Horizon Client menu bar in the remote desktop.

Device	Client and Agent OS	Limitations
Xbox controller vid_045e&pid_02ea Xbox controller vid_045e&pid_0b00	Windows 10 v21H1 x64	After you disable redirection of the device from the agent USB menu, place the cursor outside the virtual desktop window. Otherwise, the device will be redirected to the desktop automatically again.
Xbox controller vid_045e&pid_0b12	Windows 10 v21H1 x64	When you launch the Horizon desktop, place the cursor on the virtual desktop window, then plug in the device into the client machine's USB port.  After disabling redirection of the device from the agent, the device might not work in the client machine. Unplug the device from the client machine's USB port and plug it in again.

## Network Traffic and USB Redirection

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.



USB redirection works independently of the display protocol and USB traffic usually uses TCP port 32111.

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 *Horizon 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](#).

## 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 connection that the display protocol uses, or it might use a dedicated TCP 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) 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 side channel uses 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.

## 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.

On Windows clients, the USB autoconnect features, including URI queries, command-line options, and group policy settings, apply to published applications in addition to remote desktops.

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, 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. Sometimes 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 or application:

- 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 or application receives touch input, but not keyboard input.

If you have set the remote desktop or application 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. For instructions, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

## Deploying USB Devices in a Secure VMware Horizon 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 VMware Horizon deployment against this security vulnerability.

By disabling USB redirection, you can prevent any USB devices from being redirected to your users' remote desktops and applications. Alternatively, you can disable redirection of specific USB devices, allowing users to have access only to specific devices on their remote 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 VMware Horizon 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 Console, 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 published desktop and application pools. You cannot set this policy for individual published desktop or application pools.

- In Horizon Console, 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 4-5. 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
<b>false</b> or not defined (include all USB devices)	<b>false</b> or not defined (include all USB devices)	Include all USB devices
<b>false</b> (include all USB devices)	<b>true</b> (exclude all USB devices)	Exclude all USB devices
<b>true</b> (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 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 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 *VMware Horizon Client for Mac Installation and Setup Guide* 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 4-6. 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.

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. These USB redirection policy settings apply to published desktops and applications as well as to remote desktops that run on single-user machines.

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 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 4-7. 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	<b>false</b> (automatic splitting disabled)	Automatic splitting disabled
Allow – Default Client Setting	<b>true</b> (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 disables automatic splitting, and excludes any audio-output, keyboard, mouse, or smart-card components of a composite USB device from redirection.

Horizon 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 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 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 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 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 4-8. Splitting Modifiers for Device-Splitting Policy Settings on Horizon Agent](#) 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 4-8. Splitting Modifiers for Device-Splitting Policy Settings on Horizon Agent**

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

[Table 4-9. Examples of Applying Splitting Modifiers to Device-Splitting Policy Settings](#) 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 4-9. 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
<code>m:vid-XXXX_pid-XXXX</code>	<code>vid-YYYY_pid-YYYY</code>	<code>vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code>
<code>o:vid-XXXX_pid-XXXX</code>	<code>vid-YYYY_pid-YYYY</code>	<code>vid-XXXX_pid-XXXX</code>



Table 4-9. Examples of Applying Splitting Modifiers to Device-Splitting Policy Settings (continued)

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-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, set 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 applies any device splitting policy settings before it applies the filter policy settings. If you have split a composite USB device, Horizon 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 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 4-10. Filter Modifiers for Agent-Enforceable Settings**

Modifier	Description
<b>m</b> (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 <code>Exclude All Devices</code> setting. If the <code>Exclude All Devices</code> policy is set on the agent side, the policy overrides the client setting.
<b>o</b> (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 4-11. Filter Modifiers for Client-Interpreted Settings**

Modifier	Description
Default ( <b>d</b> 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 ( <b>o</b> 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 4-12. 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 ( <b>d:false</b> in the registry setting)	<b>true</b> (Allow)	<b>true</b> (Allow)
Disable – Override Client Setting ( <b>o:false</b> in the registry setting)	<b>true</b> (Allow)	<b>false</b> (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 Include a device by Vendor/Product ID
- 2 Include a device by USB family
- 3 Exclude a device by Vendor/Product ID
- 4 Exclude a device by USB family
- 5 Exclude 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 USB device family when you create USB filtering rules for Horizon Client or Horizon Agent.

---

**Note** Some devices do not report a device family.

---

Table 4-13. 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 startup 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.
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 4-14. 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 <b>false</b> .
Exclude Automatically Connection Device Family	Excludes a family of devices from being automatically forwarded. The format of the setting is <code>{m o}:&lt;family-name&gt;[;...]</code> Set the merge ( <b>m</b> ) modifier for the client setting to merge with the agent setting or the override ( <b>o</b> ) modifier for the agent setting to override the client setting. For example: <b>o:storage;hid</b>
Exclude Automatically Connection Vid/Pid Device	Excludes a device with specified vendor and product IDs from being automatically forwarded. The format of the setting is <code>{m o}:&lt;vid-&lt;xxxx&gt;_pid-&lt;xxxx *&gt;&gt;[;...]</code> Set the merge ( <b>m</b> ) modifier for the client setting to merge with the agent setting or the override ( <b>o</b> ) modifier for the agent setting to override the client setting. For example: <b>m:vid-0781_pid-554c;vid-0781_pid-9999</b>

Table 4-14. Horizon Agent Configuration Template: Device-Splitting Settings (continued)

Setting	Properties
Exclude Vid/Pid Device from Split Property: SplitExcludeVidPid	<p>Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is {mlo}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</p> <p>You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID.</p> <p>For example: <b>o:vid-0781_pid-55**</b></p> <p>The default value is undefined.</p>
Split Vid/Pid Device Property: SplitVidPid	<p>Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is {mlo}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])</p> <p>or</p> <p>{mlo}:vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww])</p> <p>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.</p> <p>For example: <b>o:vid-0781_pid-554c(exintf:01;exintf:02)</b></p> <hr/> <p><b>Note</b> Horizon does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as <b>Include Vid/Pid Device</b> to include those components.</p> <hr/> <p>The default value is undefined.</p>

## 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 applies the policies for filtering USB devices, see [Configuring Filter Policy Settings for USB Devices](#).



**Table 4-15. Horizon Agent Configuration Template: Agent-Enforced Settings**

Setting	Properties
Exclude All Devices Property: ExcludeAllDevices	<p>Excludes all USB devices from being forwarded. If set to <b>true</b>, you can use other policy settings to allow specific devices or families of devices to be forwarded. If set to <b>false</b>, you can use other policy settings to prevent specific devices or families of devices from being forwarded.</p> <p>If set to <b>true</b> 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.</p> <p>The default value is undefined, which equates to <b>false</b>.</p>
Exclude Device Family Property: ExcludeFamily	<p>Excludes families of devices from being forwarded. The format of the setting is {m o}:family_name_1[;family_name_2]...</p> <p>For example: <b>o:bluetooth;smart-card</b></p> <p>If you have enabled automatic device splitting, Horizon 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 examines the device family of the whole composite USB device.</p> <p>The default value is undefined.</p>
Exclude Vid/Pid Device Property: ExcludeVidPid	<p>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]...</p> <p>You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID.</p> <p>For example: <b>m:vid-0781_pid-****;vid-0561_pid-554c</b></p> <p>The default value is undefined.</p>
Include Device Family Property: IncludeFamily	<p>Includes families of devices that can be forwarded. The format of the setting is {m o}:family_name_1[;family_name_2]...</p> <p>For example: <b>m:storage</b></p> <p>The default value is undefined.</p>
Include HID Optimization Vid/Pid Device Property: HidOptIncludeVidPid	<p>Includes devices with specified vendor and product IDs that can be optimized. The format of the setting is vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]...</p> <p>You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID.</p> <p>For example: <b>vid-056a_pid-0302;vid-046d_pid-c628</b></p> <p>The default value is undefined.</p>
Include Vid/Pid Device Property: IncludeVidPid	<p>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]...</p> <p>You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID.</p> <p>For example: <b>o:vid-0561_pid-554c</b></p> <p>The default value is undefined.</p>

## 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 4-16. 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 <b>true</b> .
Allow Audio Output Devices Property: AllowAudioOut	Allows audio output devices to be forwarded. The default value is undefined, which equates to <b>false</b> .
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 <b>true</b> .
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 <b>false</b> .
Allow Smart Cards Property: AllowSmartcard	Allows smart-card devices to be forwarded. The default value is undefined, which equates to <b>false</b> .
Allow Video Devices Property: AllowVideo	Allows video devices to be forwarded. The default value is undefined, which equates to <b>true</b> .

Table 4-16. Horizon Agent Configuration Template: Client-Interpreted Settings (continued)

Setting	Properties
Exclude Automatically Connection Device Family	<p>Excludes families of devices from being forwarded automatically.</p> <p>Use the following syntax:</p> <pre>{m o}:family-name[;...]</pre> <p>m specifies that the client setting is merged with the agent setting. o specifies that the agent setting overrides the client setting.</p> <p>For example:</p> <pre>o:storage;hid</pre>
Exclude Automatically Connection Vid/Pid Device	<p>Excludes devices that have specific vendor and product IDs from being forwarded automatically.</p> <p>Use the following syntax:</p> <pre>{m o}:vid-xxxx_pid-xxxx *[*;...]</pre> <p>m specifies that the client setting is merged with the agent setting. o specifies that the agent setting overrides the client setting.</p> <p>For example:</p> <pre>m:vid-0781_pid-554c;vid-0781_pid-9999</pre>

## Troubleshooting USB Redirection Problems

Various problems can arise with USB redirection in Horizon.

### Problem

USB has its limitations. For more information, see [Limitations Regarding USB Device Types](#). Scanner redirection, Real-Time AudioVideo, serial port redirection, and client drive redirection help to bypass these limitations for most use cases. VMware recommends using an alternate technology, when available, as USB redirection for audio, scanners, and so on, can be unreliable due to network latency.

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

### Cause

USB redirection can fail to function correctly or as expected for the following reasons:

- Verify the virtual operating system is supported. See *Requirements and Considerations for Horizon Agent* in the *Horizon Upgrades* document.

**Note** For server operating systems deployed as RDSH servers, there are limitations with supported devices. Storage drives and a limited set of lightweight device types are supported. For example, CDROM devices are not supported.

- 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](#).
- By default, Horizon Client for Windows does not allow you to select keyboard, mouse, smartcard, and audio-out devices for redirection. See [Configuring Filter Policy Settings for USB Devices](#).
- 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.
- 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 and might be suited to client drive redirection.
- USB flash cards formatted with the FAT32 file system are slow to load. See the Knowledge Base article [Redirecting a USB flash drive might take several minutes](#).
- 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 Console.
- Missing or disabled USB redirection drivers on the guest.

#### Solution

- ◆ If available, use VMware Blast or 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 Console, 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](#).
- ◆ 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 chapter includes the following topics:

- [Setting Policies in Horizon Console](#)
- [Using Smart Policies](#)
- [Using Active Directory Group Policies](#)
- [Using Horizon Group Policy Administrative Template Files](#)
- [Horizon ADMX Template Files](#)
- [Add the ADMX Template Files to Active Directory](#)
- [VMware View Agent Configuration ADMX Template Settings](#)
- [Client Drive Redirection Policy Settings](#)
- [VMware HTML5 Feature Policy Settings](#)
- [VMware Virtualization Pack for Skype for Business Policy Settings](#)
- [VMware Integrated Printing Policy Settings](#)
- [PCoIP Policy Settings](#)
- [VMware Blast Policy Settings](#)
- [Managing Special Unity Windows](#)
- [Active Directory Group Policy Example](#)

## Setting Policies in Horizon Console

You use Horizon Console 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 published desktop and application pools. You cannot set user-level policies or pool-level policies for published desktop and application pools.

---

## Horizon Policies

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

The following table describes each Horizon policy setting.

**Table 5-1. Horizon Policies**

Policy	Description
Multimedia redirection (MMR)	<p>Determines whether MMR is enabled for client systems.</p> <p>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.</p> <p>The default value is <b>Deny</b>.</p> <p>If client systems have insufficient resources to handle local multimedia decoding, leave the setting as <b>Deny</b>.</p> <p>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.</p>
USB Access	<p>Determines whether remote desktops can use USB devices connected to the client system.</p> <p>The default value is <b>Allow</b>. To prevent the use of external devices for security reasons, change the setting to <b>Deny</b>.</p>
PCoIP hardware acceleration	<p>Determines whether to enable hardware acceleration of the PCoIP display protocol and specifies the acceleration priority that is assigned to the PCoIP user session.</p> <p>This setting has an effect only if a PCoIP hardware acceleration device is present on the physical computer that hosts the remote desktop.</p> <p>The default value is <b>Allow</b> at <b>Medium</b> priority.</p>

## 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 Policies](#).

### Procedure

- 1 In Horizon Console, select **Settings > Global Policies**.
- 2 Click **Edit policies**.
- 3 Click **OK** to save your changes.

## Using Smart Policies

You can use Smart Policies for user environment settings in a published desktop or application and also for computer environment settings that apply during computer boot or session reconnection.

You can create policies for user environment settings that control a range of behaviors. Horizon Smart Policies for user environment settings are applied during login and can be refreshed during reconnect of a session. To reapply Horizon Smart Policies when a user reconnects to a session, you can configure a triggered task.

You can create policies for computer environment settings that Dynamic Environment Manager applies while end users' computers boot. Horizon Smart Policies for computer environment settings are applied during computer boot and can be refreshed during the reconnection of a session.

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.

For information about using Smart Policies to control the behavior of features on a remote Linux desktop, see *Setting Up Linux Desktops in Horizon*.

## Requirements for Smart Policies

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

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

## Installing Dynamic Environment Manager

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

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

For an RDS desktop pool, you install Dynamic Environment Manager on the RDS host that provides the published desktop sessions.

For Dynamic Environment Manager system requirements and complete installation instructions, see the *Installing and Configuring VMware Dynamic Environment Manager* document.

## Configuring Dynamic Environment Manager

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

To configure Dynamic Environment Manager, follow the configuration instructions in the *VMware Dynamic Environment Manager Administration Guide*. The following configuration steps supplement the information in that document.

To configure Dynamic Environment Manager, follow the configuration instructions in the *VMware Dynamic Environment Manager Administration Guide*.

- When configuring the VMware DEM FlexEngine client component on remote desktops, create FlexEngine logon and logoff scripts. For multiple sessions, such as a RDSH desktop and RDSH application or a multiple RDSH application session for the same user on the same RDSH host, use the **-HorizonViewMultiSession -r** parameter for the logon script. For the logoff script, use the **-HorizonViewMultiSession -s** parameter.

---

**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`.



- To ensure that Horizon Smart Policy settings are refreshed when users reconnect to desktop sessions, use the Dynamic 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 features in Dynamic Environment Manager by creating a Horizon smart policy.

You can create policies for user environment settings that control a range of behaviors. Horizon Smart Policies for user environment settings are applied during login and can be refreshed during reconnect of a session. To reapply Horizon Smart Policies when a user reconnects to a session, you can configure a triggered task. See the complete list of policies in the topic "Configure Horizon Smart Policies for User Environment Settings" in the *VMware Dynamic Environment Manager Administration Guide*.

You can create policies for computer environment settings that Dynamic Environment Manager applies while end users' computers boot. Horizon Smart Policies for computer environment settings are applied during computer boot and can be refreshed during the reconnection of a session. See the complete list of policies in the topic "Configure Horizon Smart Policies for Computer Environment Settings" in the *VMware Dynamic Environment Manager Administration Guide*.

In general, Horizon smart policy settings that you configure for remote features in Dynamic 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 5-2. Bandwidth Profiles

Bandwidth Profile	Max Session BW (Kbps)	Min Session BW (Kbps)	Enable Build-to-Lossless (BTL)	Max Initial Image Quality	Min Image Quality	Max FPS	Max Audio BW (Kbps)	Image Quality Performance
High-speed LAN	900000	64	Yes	100	50	60	1600	50
LAN	900000	64	Yes	90	50	30	1600	50
Dedicated WAN	900000	64	No	80	40	30	500	50
Broadband WAN	5000	64	No	70	40	20	500	50

Table 5-2. Bandwidth Profiles (continued)

Bandwidth Profile	Max Session BW (Kbps)	Min Session BW (Kbps)	Enable Build-to-Lossless (BTL)	Max Initial Image Quality	Min Image Quality	Max FPS	Max Audio BW (Kbps)	Image Quality Performance
Low-speed WAN	2000	64	No	70	30	15	200	25
Extremely low-speed connection	1000	64	No	70	30	10	90	0

## Adding Conditions to Horizon Smart Policy Definitions

When you define a Horizon Smart Policy in Dynamic 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 Dynamic Environment Manager Management Console, see the *VMware Dynamic Environment Manager Administration 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 5-3. Predefined Properties for the Horizon Client Property Condition](#) 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 5-3. Predefined Properties for the Horizon Client Property Condition

Property	Corresponding Registry Key	Description
<b>Client location</b>	ViewClient_Broker_GatewayLocation	<p>Specifies the location of the user's client system. Valid values are as follows:</p> <ul style="list-style-type: none"> <li>■ Internal - the policy takes effect only if a user connects to the remote desktop from inside the corporate network</li> <li>■ External - the policy takes effect only if a user connects to the remote desktop from outside the corporate network</li> </ul> <p>For information about setting the gateway location for a Connection Server or security server host, see <a href="#">Configure the Gateway Location for a Horizon Connection Server or Security Server Host</a>.</p> <p>For information about setting the gateway location for an Access Point appliance, see the <i>Deploying and Configuring VMware Unified Access Gateway</i> document.</p>
<b>Launch tag(s)</b>	ViewClient_Launch_Matched_Tags	<p>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.</p> <p>For information about assigning tags to Connection Server instances and desktop pools, see your Setting Up document.</p>
<b>Pool name</b>	ViewClient_Launch_ID	<p>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.</p> <p><b>Note</b> 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.</p>

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 Dynamic 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 *VMware Dynamic Environment Manager Administration Guide* document.

## Configure the Gateway Location for a Horizon Connection Server or Security Server Host

By default, Horizon Connection Server instances set the gateway location to Internal and security servers set the gateway location to External. You can change the default gateway location by setting the `gatewayLocation` property in the `locked.properties` file.

The gateway location determines the value of the `ViewClient_Broker_GatewayLocation` registry key in a remote desktop. You can use this value with Smart Policies to create a policy that takes effect only if a user connects to a remote desktop from inside or outside your corporate network. For more information, see [Using Smart Policies](#).

### Procedure

- 1 Create or edit the `locked.properties` file in the TLS/SSL gateway configuration folder on the Horizon Connection Server or security server host.

For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

The properties in the `locked.properties` file are case sensitive.

- 2 Add the following line to the `locked.properties` file:

```
gatewayLocation=value
```

*value* can be either `External` or `Internal`. `External` indicates that the gateway is available for users outside the corporate network. `Internal` indicates that the gateway is available only for users inside the corporate network.

For example: `gatewayLocation=External`

- 3 Save the `locked.properties` file.
- 4 Restart the VMware Horizon Connection Server service or the VMware Horizon Security Server service to make your changes take effect.

## Create a Horizon Smart Policy in Dynamic Environment Manager

You use the Dynamic Environment Manager Management Console to create a Horizon smart policy in Dynamic 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 Dynamic Environment Manager. See [Installing Dynamic Environment Manager](#) and [Configuring Dynamic 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](#).

You can create policies for user environment settings that control a range of behaviors. Horizon Smart Policies for user environment settings are applied during login and can be refreshed during reconnect of a session. To reapply Horizon Smart Policies when a user reconnects to a session, you can configure a triggered task.

You can create policies for computer environment settings that Dynamic Environment Manager applies while end users' computers boot. Horizon Smart Policies for computer environment settings are applied during computer boot and can be refreshed during the reconnection of a session.

For complete information about using the Dynamic Environment Manager Management Console, see the *VMware Dynamic Environment Manager Administration Guide* document.

### Procedure

- 1 In the Dynamic Environment Manager Management Console, select the **User Environment** to create a policy for user environment settings or the **Computer Environment** tab to create a policy for computer environment settings.

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

- 2 Select **Horizon Smart Policies** and click **Create** to create a new smart policy.

- 3 Select the **Settings** tab and define the smart policy settings.
  - a In the General Settings section, enter a name for the smart policy in the **Name** text box.  
For example, if the smart policy affects 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.

### Results

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

Dynamic 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 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 components at a domain-wide level to control various areas of the Horizon 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 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 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. You might need to implement a different approach.

---

## Using Horizon Group Policy Administrative Template Files

Horizon 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 are available in VMware–Horizon–Extras–Bundle–YYMM–x.x.x–yyyyyyyyy.zip, where YYMM is the marketing version, x.x.x is the internal version and yyyyyyyy is the build number. You can download the file from the VMware Downloads site at <https://my.vmware.com/web/vmware/downloads>. Under Desktop & End-User Computing, select the VMware Horizon download, which includes the GPO Bundle containing the ZIP file.

The Horizon 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 ADMX Template Files

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

The ADMX files are available in `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyyy.zip`, which you can download from the VMware Downloads site at <https://my.vmware.com/web/vmware/downloads>. Under Desktop & End-User Computing, select the VMware Horizon download, which includes the GPO Bundle containing the ZIP file.

**Table 5-4. Horizon ADMX Template Files**

Template Name	Template File	Description
VMware Blast	<code>vdm_blast.admx</code>	Contains policy settings related to the VMware Blast display protocol. See <a href="#">VMware Blast Policy Settings</a> .
VMware View Agent Configuration	<code>vdm_agent.admx</code>	Contains policy settings related to the authentication and environmental components of Horizon Agent.
Clipboard Redirection	<code>vdm_agent_clipboard.admx</code>	Contains policy settings related to clipboard redirection.
Drag and Drop	<code>vdm_agent_dnd.admx</code>	Contains policy settings related to drag and drop redirection.
VMware Horizon Client Configuration	<code>vdm_client.admx</code>	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 <i>VMware Horizon Client for Windows Installation and Setup Guide</i> document.
VMware Horizon URL Redirection	<code>urlRedirection.admx</code>	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 <a href="#">Chapter 3 Configuring URL Content Redirection</a> and see the <i>VMware Horizon Client for Windows Installation and Setup Guide</i> document.
VMware View Server Configuration	<code>vdm_server.admx</code>	Contains policy settings related to Connection Server. See the <i>Horizon Administration</i> document.



Table 5-4. Horizon ADMX Template Files (continued)

Template Name	Template File	Description
VMware View Common Configuration	vdm_common.admx	Contains policy settings that are common to all Horizon components. See the <i>Horizon Administration</i> 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 <i>VMware Horizon Client for Windows Installation and Setup Guide</i> document.
VMware Integrated Printing	printerRedirection.admx	Contains policy settings related to the VMware Integrated Printing feature.
View RTAV Configuration	vdm_agent_rtav.admx	Contains policy settings related to webcams that are used with the Real-Time Audio-Video feature. See <a href="#">Real-Time Audio-Video Group Policy Settings</a> .
Scanner Redirection	vdm_agent_scanner.admx	Contains policy settings related to scanning devices that are redirected for use in published desktops and applications.
Serial COM	vdm_agent_serialport.admx	Contains policy settings related to serial (COM) ports that are redirected for use in virtual desktops.
VMware Horizon Printer Redirection	vdm_agent_printing.admx	Contains policy settings related to filtering redirected printers.
View Agent Direct-Connection	view_agent_direct_connection.admx	Contains policy settings related to the View Agent Direct-Connection Plug-In. See the <i>View Agent Direct-Connection Plug-In Administration</i> document.
VMware Horizon Performance Tracker	vdm_agent_perfTracker.admx	Contains policy settings related to the VMware Horizon Performance Tracker feature.
VMware Horizon Client Drive Redirection	vdm_agent_cdr.admx	Contains policy settings related to the client drive redirection feature. See <a href="#">Use Group Policy to Configure Drive Letter Behavior</a> .

## Add the ADMX Template Files to Active Directory

You can add the policy settings for specific remote desktop features in the Horizon 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 ADMX Template Files](#).
- Verify that the Group Policy Management feature is available on your Active Directory server.

## Procedure

- 1 Download the VMware Horizon 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 download, which includes the GPO Bundle.

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

- 2 Unzip the `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyyy.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 VMware–Horizon–Extras–Bundle–YYMM–x.x.x–yyyyyyyyy.zip, which you can download from the VMware Downloads site at <https://my.vmware.com/web/vmware/downloads>. Under Desktop & End-User Computing, select the VMware Horizon download, which includes the GPO Bundle containing the ZIP file.

The following tables describe policy settings in the VMware View Agent Configuration ADMX template file. The template contains both Computer Configuration and User Configuration settings. The User Configuration setting overrides the equivalent Computer Configuration setting.

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

## Agent Configuration

Agent configuration settings are in the **VMware View Agent Configuration > Agent Configuration** folder in the Group Policy Management Editor.

Table 5-5. Agent Configuration Policy Settings

Setting	Computer	User	Properties
AllowDirectRDP	X		<p>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.</p> <p>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.</p> <p>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.</p> <hr/> <p><b>Important</b> 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.</p> <hr/> <p>This setting is enabled by default.</p>
AllowSingleSignon	X		<p>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.</p> <p>This setting is enabled by default.</p>

Table 5-5. Agent Configuration Policy Settings (continued)

Filter Microsoft Chart and Smart Art			
Setting	Computer	User	Properties
Audio option for single session Windows 10 physical Remote Desktop machine	X		<p>Specifies the audio device to use on a Horizon Windows 10 physical machine hosting the remote desktop session. When enabled, select from the following options:</p> <ul style="list-style-type: none"> <li>■ Use audio device attached to the Horizon Client endpoint. This is the default setting.</li> <li>■ Use audio device attached to Horizon Windows 10 physical remote desktop endpoint.</li> </ul> <p>This setting is not configured by default.</p>
CommandsToRunOnConnect	X		<p>Specifies a list of commands or command scripts to be run when a session is connected for the first time.</p> <p>See <a href="#">Running Commands on Horizon Desktops</a> for more information.</p>
CommandsToRunOnDisconnect	X		<p>Specifies a list of commands or command scripts to be run when a session is disconnected.</p> <p>See <a href="#">Running Commands on Horizon Desktops</a> for more information.</p>
CommandsToRunOnReconnect	X		<p>Specifies a list of commands or command scripts to be run when a session is reconnected after a disconnect.</p> <p>See <a href="#">Running Commands on Horizon Desktops</a> for more information.</p>
ConnectionTicketTimeout	X		<p>Specifies the amount of time in seconds that the Horizon connection ticket is valid.</p> <p>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.</p>
CredentialFilterExceptions	X		<p>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.</p>
Disable Time Zone Synchronization	X	X	<p>Determines whether the time zone of the remote desktop is synchronized with the time zone of the connected client. An enabled setting applies only if the <code>Disable time zone forwarding</code> setting of the Horizon Client Configuration policy is not set to disabled.</p> <p>This setting is disabled by default.</p>

Table 5-5. Agent Configuration Policy Settings (continued)

Filter Microsoft Chart and Smart Art			
Setting	Computer	User	Properties
Disconnect Session Time Limit (VDI)	X		<p>Specifies the amount of time after which a disconnected desktop session logs out automatically.</p> <ul style="list-style-type: none"> <li>■ <b>Never:</b> disconnected sessions on this machine never log out.</li> <li>■ <b>Immediately:</b> disconnected sessions log out immediately.</li> </ul> <p>You can also configure the time limit in the <b>Automatically logoff after disconnect</b> desktop pool setting in Horizon Console. If you configure this setting in both places, the group policy setting takes precedence.</p> <p>For example, selecting <b>Never</b> prevents a disconnected session on this machine from ever logging out, regardless of the setting in Horizon Console.</p>
DPI Synchronization	X	X	<p>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.</p> <p>For a list of the supported guest operating systems, see the "Using DPI Synchronization" topic in the <i>VMware Horizon Client for Windows Installation and Setup Guide</i> document.</p> <p>This setting is enabled by default.</p>
DPI Synchronization Per Monitor	X	X	<p>Adjusts the DPI setting in multiple monitors during a remote session.</p> <p>When this setting is enabled, the DPI setting in all monitors changes to match the client per-monitor DPI setting during a remote session. If the DPI setting is customized, the customized DPI setting is matched. The <b>Allow Display Scaling</b> option is dimmed in Horizon Client.</p> <p>When this setting is disabled, users must log out and reconnect to the remote desktop to make DPI setting changes take effect in all monitors.</p> <p>For a list of the supported guest operating systems, see the "Using DPI Synchronization" topic in the <i>VMware Horizon Client for Windows Installation and Setup Guide</i> document.</p> <p>This setting is enabled by default.</p>

Table 5-5. Agent Configuration Policy Settings (continued)

Filter Microsoft Chart and Smart Art			
Setting	Computer	User	Properties
Enable Battery State Redirection	X		<p>Determines whether battery state redirection is enabled. This feature is supported with Windows and Linux client systems.</p> <p>When this setting is enabled, information about the Windows or Linux client system's battery is redirected to a Windows remote desktop. The battery icon in the system tray on the remote desktop indicates the battery charge percentage. If the battery charge is less than or equal to 10 percent, a message pops up stating that the battery is low.</p> <p>This setting is enabled by default.</p>
Enable multi-media acceleration	X		<p>Determines whether multimedia redirection (MMR) is enabled on the remote desktop.</p> <p>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 decoded directly on the client, where it is played. You can disable MMR if the client has insufficient resources to handle local multimedia decoding.</p> <p>This setting is enabled by default.</p>
Enable Unauthenticated Access	X		<p>Enables or disables the unauthenticated access feature. When this setting is enabled, unauthenticated access users can access published applications from Horizon Client without requiring Active Directory credentials. When this setting is disabled, unauthenticated access users cannot access published applications from Horizon Client without requiring Active Directory credentials. You must reboot the RDS host for this setting to take effect.</p> <p>This setting is enabled by default.</p>
Force MMR to use software overlay	X		<p>MMR tries to use the hardware overlay to play back video for better performance. When working with multiple displays, the hardware overlay exists on only one of the displays, either the primary display or the display where WMP started. If a user drags WMP 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.</p> <p>This setting is enabled by default.</p>
Idle Time Until Disconnect (VDI)	X		<p>Specifies the amount of time after which a remote desktop session disconnects because of user inactivity. If disabled, not configured, or enabled with the <b>Never</b> setting, the remote desktop sessions are never disconnected.</p> <p>If the desktop pool or machine is configured to log out automatically after a disconnect, that setting is honored.</p>

**Table 5-5. Agent Configuration Policy Settings (continued)**

<b>Filter Microsoft Chart and Smart Art</b>			
<b>Setting</b>	<b>Computer</b>	<b>User</b>	<b>Properties</b>
Prewarm Session Time Limit	X		Specifies the amount of time after which a prewarm session logs out automatically. This setting is not configured by default.
RDS Connection Time Until Disconnect	X		Specifies the maximum amount of time that a Remote Desktop Services session can be active before it is disconnected automatically. Timeout values range from Never to one week. Selecting <b>Never</b> will never disconnect Remote Desktop Services sessions on this machine.
RDS Disconnected Time Until Logoff	X		Specifies the amount of time after which a disconnected Remote Desktop Services session logs off automatically. Timeout values range from Never to one week. Selecting <b>Never</b> will never log off disconnected Remote Desktop Services sessions on this machine.
RDS End Session When Time Limit Reached	X		Specifies whether to end or disconnect a Remote Desktop Services session that has timed out. If this setting is enabled, the Remote Desktop Services session is ended (user is logged off and the session is deleted from the server) after the time limit for active or idle sessions have been reached. By default, Remote Desktop Services sessions are disconnected after reaching their time limits.
RDS Idle Time Until Disconnect	X		Specifies the amount of time after which an idle Remote Desktop Services session disconnects automatically. Timeout values range from Never to one week. Selecting <b>Never</b> will never disconnect Remote Desktop Services sessions on this machine.

Table 5-5. Agent Configuration Policy Settings (continued)

Filter Microsoft Chart and Smart Art			
Setting	Computer	User	Properties
Screen-capture Blocking	X		<p>Determines whether users can take screenshots of their virtual desktop or published application from their end point.</p> <p>If enabled, users are blocked from taking screenshots of the virtual desktop or virtual applications from their Windows or macOS devices.</p> <p>The default is disabled, allowing users to take screenshots from their devices.</p> <p>This feature is supported on Horizon Agent 2106 and later. This setting can only be enforced on the Horizon Client for Windows and Horizon Client for Mac 2106 and later.</p> <p>On Horizon Client for Windows, this feature supports Multimedia Redirection, WebRTC, VMware Virtualization for Skype for Business, and HTML5 Multimedia Redirection. Native applications, such as Zoom and Microsoft Teams, block remote desktop or seamless window content sharing.</p> <p>You can configure this setting for the machine or per user. If you disable SSO on the agent, you must configure this setting for the machine, not per user. If both machine and user are configured, the GPO setting for the user takes effect.</p> <p>If you want to prevent a user from connecting to the agent using clients that do not support screen capture blocking, limit the session connection. See <i>Global Client Restriction Settings for Client Sessions</i> in the <i>Horizon Administration</i> document.</p> <p>Limitations:</p> <ul style="list-style-type: none"> <li>■ Double hop is not supported for Horizon Client for Windows.</li> <li>■ Native applications such as Zoom and Microsoft Teams might not share content of the remote desktop or published application that enables this feature.</li> <li>■ Optimized VDI Zoom or WebEx as virtual applications might not work as expected if this feature is enabled.</li> <li>■ VMware WebRTC/Media Optimization for Microsoft Teams plugin displays black content when this feature is enabled.</li> </ul>
ShowDiskActivityIcon	X		This setting is not supported in this release.



Table 5-5. Agent Configuration Policy Settings (continued)

Filter Microsoft Chart and Smart Art			
Setting	Computer	User	Properties
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 enabled by default.
Toggle Display Settings Control	X		Determines whether to disable the <b>Settings</b> tab in the <b>Display</b> control panel when a client session uses the PCoIP display protocol. This setting is enabled by default.

**Note** The `Connect using DNS Name` setting was removed in the Horizon 6 version 6.1 release. You can set the Horizon 8 LDAP attribute, **pae-PreferDNS**, to tell 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 *Horizon Installation* document.

## Agent Security

The Agent Security setting is in the **VMware View Agent Configuration > Agent Security** folder in the Group Policy Management Editor.

Table 5-6. Agent Security Policy Setting

Setting	Computer	User	Properties
Accept SSL encrypted framework channel		X	<p>Enables the TLS encrypted framework channel. You can specify one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Disable</b> - Disable TLS.</li> <li>■ <b>Enable</b> - Enable TLS. Allow legacy clients to connect without TLS.</li> <li>■ <b>Enforce</b> - Enable TLS. Refuse legacy client connections.</li> </ul> <p>This setting is enabled by default.</p>

## Clipboard Redirection

Policy settings for Clipboard Redirection are in the ADMX template file `vdm_agent_clipboard.admx`. The Clipboard Redirection settings are in the **VMware View Agent Configuration > Clipboard Redirection** folder in the Group Policy Management Editor.

Table 5-7. Clipboard Redirection Policy Settings

Setting	Computer	User	Description
Clipboard memory size on server	X	X	<p>Specifies the server clipboard memory size value in bytes or kilobytes, as selected. If it is not configured, the memory size is in kilobytes.</p> <p>The client also has a value for the clipboard memory size, which is always in kilobytes. 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.</p> <p>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.</p> <p><b>Note</b> To transfer larger amounts of data, use the client drive redirection feature.</p>
Configure clipboard audit	X	X	<p>Specifies whether the clipboard audit feature is enabled on the agent machine. When this setting is enabled, the options are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Disabled in both directions.</b> Information about clipboard data is not recorded.</li> <li>■ <b>Enabled client to server only.</b> Information about clipboard data that is copied from the client machine to the agent machine is recorded in an event log on the agent machine.</li> <li>■ <b>Enabled in both directions.</b> Information about clipboard data that is copied from the client machine to the agent machine, and from the agent machine to the client machine, is recorded in an event log on the agent machine.</li> <li>■ <b>Enabled server to client only.</b> Information about clipboard data that is copied from the agent machine to the client machine is recorded in an event log on the agent machine.</li> </ul> <p>When this setting is disabled or not configured, the default value is <b>Disabled in both directions</b>.</p> <p>You can use the Windows event viewer on the agent machine to view the event log. The log name is VMware Horizon RX Audit. To view the event log in a centralized location, you can configure VMware Log Insight or Windows Event Collector.</p> <p><b>Note</b> Only the Windows client supports agent machine to client machine clipboard auditing.</p>

Table 5-7. Clipboard Redirection Policy Settings (continued)

Setting	Computer	User	Description
Configure clipboard redirection	X	X	<p>Determines the direction in which clipboard redirection is allowed. You can select one of the following values:</p> <ul style="list-style-type: none"> <li>■ <b>Enabled client to agent only</b></li> <li>■ <b>Disabled in both directions</b></li> <li>■ <b>Enabled in both directions</b></li> <li>■ <b>Enabled agent to client only</b></li> </ul> <p>Clipboard redirection is implemented as a virtual channel. If virtual channels are disabled, clipboard redirection does not function.</p> <p>This setting applies only to Horizon Agent.</p> <p>When this setting is disabled or not configured, the default value is <b>Enabled client to agent only</b>.</p>

Table 5-7. Clipboard Redirection Policy Settings (continued)

Setting	Computer	User	Description
Configure clipboard redirection formats	X	X	<p data-bbox="821 294 1423 357">Determines whether a filter is enabled or disabled on the agent machine for each data format.</p> <ul style="list-style-type: none"> <li data-bbox="821 367 1423 588"> <p data-bbox="821 367 1423 388">■ <b>Filter files folders from incoming clipboard data:</b> Specifies whether selected files or folders can be copied to the clipboard from the client machine to the agent machine. If enabled, copying files and folders from the client machine is blocked. If disabled, copying and pasting files and folders from the client machine is allowed.</p> </li> <li data-bbox="821 598 1423 819"> <p data-bbox="821 598 1423 619">■ <b>Filter files and folders from outgoing clipboard data:</b> Specifies whether selected files or folders can be copied to the clipboard from the agent machine to the client machine. If enabled, copying files and folders from the agent machine is blocked. If disabled, copying and pasting files and folders from the agent machine is allowed.</p> </li> <li data-bbox="821 829 1423 1008"> <p data-bbox="821 829 1423 850">■ <b>Filter text out of the incoming clipboard data:</b> Specifies whether textual data is filtered out of the clipboard data coming from the client machine to the agent machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</p> </li> <li data-bbox="821 1018 1423 1197"> <p data-bbox="821 1018 1423 1039">■ <b>Filter text out of the outgoing clipboard data:</b> Specifies whether textual data is filtered out of the clipboard data sent from the agent machine to the client machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</p> </li> <li data-bbox="821 1207 1423 1386"> <p data-bbox="821 1207 1423 1228">■ <b>Filter Rich Text Format data out of the incoming clipboard data:</b> Specifies whether Rich Text Format data is filtered out of the clipboard data coming from the client machine to the agent machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</p> </li> <li data-bbox="821 1396 1423 1575"> <p data-bbox="821 1396 1423 1417">■ <b>Filter Rich Text Format data out of the outgoing clipboard data:</b> Specifies whether Rich Text Format data is filtered out of the clipboard data sent from the agent machine to the client machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</p> </li> <li data-bbox="821 1585 1423 1789"> <p data-bbox="821 1585 1423 1606">■ <b>Filter images out of the incoming clipboard data:</b> Specifies whether image data is filtered out of the clipboard data coming from the client machine to the agent machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</p> </li> </ul>

Table 5-7. Clipboard Redirection Policy Settings (continued)

Setting	Computer	User	Description
			<ul style="list-style-type: none"> <li>■ <b>Filter images out of the outgoing clipboard data:</b> Specifies whether image data is filtered out of the clipboard data sent from the agent machine to the client machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</li> <li>■ <b>Filter Microsoft Office text data out of the incoming clipboard data:</b> Specifies whether Microsoft Office text format data (BIFF12 format) is filtered out of the clipboard data coming from the client machine to the agent machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</li> <li>■ <b>Filter Microsoft Office text data out of the outgoing clipboard data:</b> Specifies whether Microsoft Office text format data (BIFF12 format) is filtered out of the clipboard data sent from the agent machine to the client machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</li> <li>■ <b>Filter Microsoft Chart and Smart Art data out of the incoming clipboard data:</b> Specifies whether Microsoft Office Chart and Smart Art data (Art::GVML ClipFormat) is filtered out of the clipboard data sent from the client machine to the agent machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</li> <li>■ <b>Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data:</b> Specifies whether Microsoft Office Chart and Smart Art data (Art::GVML ClipFormat) is filtered out of the clipboard data sent from the agent machine to the client machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</li> <li>■ <b>Filter Microsoft Text Effects data out of the incoming clipboard data:</b> Specifies whether Microsoft Office text effects data (HTML Format) is filtered out of the clipboard data coming from the client machine to the agent machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</li> <li>■ <b>Filter Microsoft Text Effects data out of the outgoing clipboard data:</b> Specifies whether Microsoft Office text effects data (HTML Format) is filtered out of the clipboard data sent from the agent machine to the client machine. When this setting is enabled, the data is filtered out. When this setting is disabled, the data is allowed.</li> </ul>

Table 5-7. Clipboard Redirection Policy Settings (continued)

Setting	Computer	User	Description
			<p>When the setting is not configured or disabled, the filters for clipboard redirection are disabled for all formats.</p> <p>This setting not configured by default.</p>
Configure file transfer	X		<p>Configures how the file transfer feature works between the remote desktop and HTML Access. Valid values are as follows.</p> <p>This setting applies only to remote desktops.</p> <ul style="list-style-type: none"> <li>■ <b>Disabled both upload and download</b></li> <li>■ <b>Enabled both upload and download</b></li> <li>■ <b>Enabled file upload only.</b> Users can upload files from the client system to the remote desktop.</li> <li>■ <b>Enabled file download only.</b> Users can download files from the remote desktop to the client system.</li> </ul> <p>When this setting is disabled or not configured, the default value is <b>Enabled file upload only</b>.</p>
Whether block clipboard redirection to client side when client doesn't support audit	X	X	<p>Specifies whether to block clipboard redirection to clients that do not support the clipboard audit feature.</p> <p>When this setting is enabled, you must select one of the following values.</p> <ul style="list-style-type: none"> <li>■ <b>Block</b> blocks agent-to-client clipboard redirection if the clipboard audit feature is supported on the agent machine, but is not supported on the client machine.</li> <li>■ <b>Passthrough</b> allows agent-to-client clipboard redirection if the clipboard audit feature is supported on the agent machine, but is not supported on the client machine.</li> </ul> <p>When this setting is disabled or not configured, the default value is <b>Block</b>.</p> <p>You must enable the <code>Configure clipboard audit</code> group policy setting for this setting to take effect.</p>

## Collaboration

Collaboration settings are in the **VMware View Agent Configuration > Collaboration** folder in the Group Policy Management Editor.

Table 5-8. Collaboration Policy Settings

Setting	Description
Allow control passing to collaborators	When enabled, users can pass input control to other collaborators during collaboration. When disabled, the toggle switch does not appear in the collaboration window. This setting is enabled by default.
Allow inviting collaborators by e-mail	When enabled, you can send collaboration invitations by using an installed email application. When disabled, you cannot use email to invite collaborators, even if an email application is installed. This setting is enabled by default.
Allow inviting collaborators by IM	When enabled, you can send collaboration invitations by using an installed Instant Message (IM) application. When disabled, you cannot use IM to invite collaborators, even if an IM application is installed. This setting is enabled by default.
Include Outlook-formatted URL in clipboard text	When this setting is enabled, a Microsoft Outlook-formatted invitation URL is included in the clipboard invitation text. Enable this setting if you expect end users to paste clipboard invitation text into an email message. This setting is disabled by default.
Separator used for multiple e-mail addresses in mailto: links	Configures the separator used for multiple email addresses in mailto: links to allow better compatibility with various email clients. When not configured, the default value is a semicolon without a space to separate email addresses.  If your default email client does not allow a semicolon as a separator, try other combinations, such as a comma plus one space or semicolon plus one space.
Server URLs to include in invitation message	Sets the server URLs to include in collaboration invitations. If this setting is not configured, a default URL is used, but it might be incorrect in all but the simplest deployments.
Turn off collaboration	When enabled, the Session Collaboration feature is turned off. When disabled or not configured, you can control the feature at the farm or desktop pool level. This setting takes effect after you reboot the Horizon Agent machines.
Maximum number of invited collaborators	Specifies the maximum number of collaborators that you can invite to join a session. The default maximum is 5. The limit is 20.

## Drag and Drop

Policy settings for Drag and Drop are in the ADMX template file `vdm_agent_dnd.admx`. The Drag and Drop settings are in the **VMware View Agent Configuration > Drag and Drop** folder in the Group Policy Management Editor.

Table 5-9. Drag and Drop Policy Settings

Setting	Description
Configure drag and drop direction	<p>Specifies the direction in which drag and drop is allowed. When enabled, the options are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Disabled in both directions</b></li> <li>■ <b>Enabled client to agent only.</b> Allows drag and drop only from the client system to the agent.</li> <li>■ <b>Enabled agent to client only.</b> Allows drag and drop only from the agent to the client system.</li> <li>■ <b>Enabled in both directions</b></li> </ul> <p>When this setting is disabled or not configured, the default value is <b>Enabled client to agent only.</b></p> <p>This setting applies to the agent only.</p>
Configure drag and drop formats	<p>Determines which drag and drop direction (<b>Disabled in both directions, Enabled agent to client only, Enabled client to agent only, or Enabled in both directions</b>) is allowed for each data format. When this setting is enabled, the options are as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Option for file format</b></li> <li>■ <b>Option for text format</b></li> <li>■ <b>Option for Rich Text format</b></li> <li>■ <b>Option for Image format</b></li> <li>■ <b>Option for HTML format</b></li> <li>■ <b>Option for File Content format</b></li> </ul> <p>When this setting is disabled or not configured, the default value for all formats is <b>Enabled in both directions.</b></p> <p>This setting applies to the agent only.</p>
Configure drag and drop size threshold	<p>Determines the size limit for dragging common data types other than files and folders.</p> <p>When this setting is enabled, select the unit of the drag data size from the <b>Choose the unit of the drag and drop size</b> drop-down menu. You can select <b>Bytes, Kilobytes, or Megabytes.</b> Select or enter the drag data size in the <b>Drag and drop size threshold</b> text box. The effective data range for each unit is as follows:</p> <ul style="list-style-type: none"> <li>■ <b>Bytes:</b> 1 through 1023</li> <li>■ <b>Kilobytes:</b> 1 through 1023</li> <li>■ <b>Megabytes:</b> 1 through 16 (the maximum data size to drag and drop is 16 megabytes)</li> </ul> <p>When this setting is disabled or not configured, a default threshold of 1 megabyte is set.</p> <p>This setting applies only to the agent.</p>

## Performance Tracker

Policy settings for Performance Tracker are in the ADMX template file `vdm_agent_perfTracker.admx`. Performance Tracker settings are in the **VMware View Agent Configuration > Performance Tracker** folder in the Group Policy Management Editor.



Table 5-10. Performance Tracker Policy Settings

Setting	Description
Enable Horizon Performance Tracker auto start in remote desktop connection	When enabled, Horizon Performance Tracker starts automatically when a user logs on to a remote desktop connection. To clear this preference GPO setting, select <b>Disable</b> .
Enable Horizon Performance Tracker auto start in remote application connection	When enabled, Horizon Performance Tracker starts automatically when a user logs on to a remote application connection. To clear this preference GPO setting, select <b>Disable</b> .
Performance Tracker basic setting	When enabled, you can set the frequency in seconds at which Horizon Performance Tracker collects data.

## Scanner Redirection

Policy settings for Scanner Redirection are in the ADMX template file `vdm_agent_scanner.admx`. Scanner Redirection settings are in the **VMware View Agent Configuration > Scanner Redirection** folder in the Group Policy Management Editor.

Table 5-11. Scanner Redirection Group Policy Settings

Setting	Computer	User	Description
BandwidthLimit		X	Specifies the maximum allowed bandwidth, in kilobytes per second, for transferring scanned data to a user session. If you specify 0 or no value, the bandwidth is unlimited.
Compression		X	Specifies the image compression rate to use during the image transfer to a remote desktop or published application. You can select one of the following compression modes: <ul style="list-style-type: none"> <li>■ <b>Disable</b> – Image compression is disabled.</li> <li>■ <b>Lossless</b> – Lossless (zlib) compression is used without loss of image quality.</li> <li>■ <b>JPEG</b> – JPEG compression is used with loss of quality. You select the level of image quality from the <b>JPEG compression quality</b> drop-down menu. JPEG compression quality must be a value between 0 and 100.</li> </ul> When you enable this setting, the selected compression mode is set for all users affected by this policy. Users can change the <b>Compression</b> 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.
Default Color Mode			When this setting is enabled, you can configure the default color mode: black and white, grayscale, or color. This setting is supported on Windows XP Professional or Windows Server 2003 or later.

**Table 5-11. Scanner Redirection Group Policy Settings (continued)**

Setting	Computer	User	Description
Default Duplex			<p>When this setting is enabled, you can configure the default scanning mode: simplex or duplex. In duplex mode, the scanning application must support duplex scanning and request two pages from the scanner. This setting is supported on Windows XP Professional or Windows Server 2003 or later.</p>
Default Scanner	X	X	<p>Provides centralized management of scanner autoselection. You select scanner autoselection options separately for TWAIN and WIA scanners. You can select one of the following autoselection options:</p> <ul style="list-style-type: none"> <li>■ <b>None.</b> Do not select scanners automatically.</li> <li>■ <b>Autoselect</b> Automatically select the locally connected scanner.</li> <li>■ <b>Last used</b> Automatically select the last-used scanner.</li> <li>■ <b>Specified</b> Select the scanner name that you type in the <b>Specified scanner</b> text box.</li> </ul> <p>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 <b>Default Scanner</b> option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>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 <b>Default Scanner</b> option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>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.</p> <p>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.</p>
Disable functionality	X		<p>Disables the scanner redirection feature.</p> <p>When you enable this setting, scanners cannot be redirected and do not appear in the scanner menu on users' desktops and applications.</p> <p>When you disable this setting or do not configure it, scanner redirection works and scanners appear in the scanner menu.</p>
Force the TWAIN Scanning Properties dialog		X	<p>When this setting is enabled, the TWAIN Scanning Properties dialog box is always displayed, even if a scanning application does not display the scanning dialog box.</p>

Table 5-11. Scanner Redirection Group Policy Settings (continued)

Setting	Computer	User	Description
Hide Webcam	X	X	<p>Prevents webcams from appearing in the scanner selection menu in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>By default, webcams can be redirected to desktops and applications. Users can select webcams and use them as virtual scanners to capture images.</p> <p>When you enable this setting as a Computer Configuration policy, webcams are hidden from all users of the affected computers. Users cannot change the <b>Hide Webcam</b> option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>When you enable this setting as a User Configuration policy, webcams are hidden from all affected users. However, users can change the <b>Hide Webcam</b> option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>When you enable this setting in both Computer Configuration and User Configuration, the <b>Hide Webcam</b> setting in Computer Configuration overrides the corresponding policy setting in User Configuration for all users of the affected computers.</p> <p>When you disable this setting or do not configure it in either policy configuration, the <b>Hide Webcam</b> 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.</p>
Lock config	X		<p>Locks the scanner redirection user interface and prevents users from changing configuration options on their desktops and applications.</p> <p>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.</p> <p>When you disable this setting or do not configure it, users can configure the options in the VMware Horizon Scanner Redirection Preferences dialog box.</p>
TWAIN Scanner Properties dialog location		X	<p>Specifies where the TWAIN Scanning Properties dialog box appears. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Agent</b> – the VMware Scanner Properties dialog box appears on the agent side.</li> <li>■ <b>Client</b> – the native vendor scanner TWAIN dialog box appears on the client side. (This option is not supported for the Linux client.)</li> </ul>

## Serial COM

Policy settings for Serial COM are in the ADMX template file `vdm_agent_serialport.admx`. Serial COM settings are in the **VMware View Agent Configuration > Serial COM** folder in the Group Policy Management Editor.

Table 5-12. Serial COM Policy Settings

Setting	Com puter	U ser	Description
PortSettings1	X	X	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>■ The <b>Source port number</b> setting specifies the number of the physical COM port that is connected to the client system.</li> <li>■ The <b>Destination virtual port number</b> setting specifies the number of the redirected virtual COM port on the remote desktop.</li> <li>■ The <b>Autoconnect</b> setting automatically connects the COM port to the redirected COM port at the start of each desktop session.</li> <li>■ With the <b>IgnoreDSR</b> setting, the redirected COM port device ignores the Data Set Ready (DSR) signal.</li> <li>■ The <b>Pause before close port (in milliseconds)</b> setting specifies the time to wait (in milliseconds) after a user closes the redirected port and before the port is actually closed. Certain USBs to Serial adapters require to this delay to preserve transmitted data. This setting is intended for troubleshooting purposes.</li> <li>■ The <b>Serial2USBModeChangeEnabled</b> setting resolves problems 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 cannot receive data.</li> <li>■ The <b>Disable errors in wait mask</b> setting disables the error value in the COM port mask. This troubleshooting setting is required for certain applications. For more information, see the Microsoft documentation for the <code>WaitCommEvent</code> function at <a href="http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx</a>.</li> <li>■ The <b>HandleBtDisappear</b> setting supports BlueTooth COM port behavior. This setting is intended for troubleshooting purposes.</li> <li>■ The <b>UsbToComTroubleShooting</b> setting resolves some issues that apply to USB to Serial port adapters. This setting is intended for troubleshooting purposes.</li> <li>■ The <b>Permanent</b> setting keeps the redirected COM port status in the remote session even if the client disconnects.</li> </ul>
PortSettings2			
PortSettings3			
PortSettings4			
PortSettings5			

Table 5-12. Serial COM Policy Settings (continued)

Setting	Com puter	User	Description
Bandwidth limit	X		<p>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 on to the remote desktop, and they cannot ignore the DSR signal. These properties are controlled by the group policy setting.</p> <hr/> <p><b>Note</b> 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.</p> <hr/> <p>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 <b>Serial COM Redirection for VMware Horizon</b> menu options are active and available to users.</p> <p>These settings are in the <b>VMware View Agent Configuration &gt; Serial COM &gt; PortSettings</b> folder in the Group Policy Management Editor.</p> <hr/> <p>Sets a limit on the data transfer speed, in kilobytes per second, between the redirected serial port and client systems.</p> <p>When you enable this setting, you can set a value in the <b>Bandwidth limit (in kilobytes per second)</b> box that determines the maximum data transfer speed between the redirected serial port and the client. A value of 0 disables the bandwidth limit.</p> <p>When this setting is disabled, no bandwidth limit is set.</p> <p>When this setting is not configured, local program settings on the remote desktop determine whether a bandwidth limit is set.</p> <p>This setting is in the <b>VMware View Agent Configuration &gt; Serial COM</b> folder in the Group Policy Management Editor.</p>
COM Port Isolation Mode	X		<p>Specifies the isolation mode for COM ports. When you enable this setting, you can select one of the following isolation modes:</p> <ul style="list-style-type: none"> <li>■ <b>Full Isolation</b> – virtual serial ports are visible and accessible only within user sessions. COM port names can have the same names in different user sessions. System services, such as <code>spoolsvr.exe</code>, cannot access isolated serial ports in this mode.</li> <li>■ <b>Isolation Disabled</b> – virtual serial ports are visible globally. Any port can be accessed from any session. Because ports cannot have the same name in different user sessions, port names must be unique for each user. System services, such as <code>spoolsvr.exe</code>, can access any serial port.</li> </ul> <p>If this setting is not configured, serial port redirection operates in <b>Full Isolation</b> mode.</p>

Table 5-12. Serial COM Policy Settings (continued)

Setting	Com puter	U ser	Description
Connect all ports automatically	X		<p>When you enable this setting, all COM ports are connected automatically, even if no individual group policy settings are enabled. If individual group policy settings are configured for specific ports, the individual group policy settings are used.</p> <p>If this setting is disabled or not configured, the auto-connect functionality is determined by the individual port group policy settings or the local program settings.</p> <p>This setting is not configured by default.</p>
Disable functionality	X		<p>Disables the serial port redirection feature.</p> <p>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.</p> <p>When this setting is disabled, serial port redirection works, the serial port tool tray icon is displayed, and COM ports appear in the <b>Serial COM Redirection for VMware Horizon</b> menu.</p> <p>When this setting is not configured, settings that are local to the remote desktop determine whether serial port redirection is disabled or enabled.</p> <p>This setting is in the <b>VMware View Agent Configuration &gt; Serial COM</b> folder in the Group Policy Management Editor.</p>
Local settings priority	X	X	<p>Gives priority to the settings that are configured on the remote desktop.</p> <p>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.</p> <p>When this setting is disabled or not configured, group policy settings take precedence over the settings that are configured on the remote desktop.</p> <p>This setting is in the <b>VMware View Agent Configuration &gt; Serial COM</b> folder in the Group Policy Management Editor.</p>
Lock configuration	X	X	<p>Locks the serial port redirection user interface and prevents users from changing configuration options on the remote desktop.</p> <p>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 <b>Serial COM Redirection for VMware Horizon</b> menu, but the options are inactive and cannot be changed.</p> <p>When this setting is disabled, users can configure the options in the <b>Serial COM Redirection for VMware Horizon</b> menu.</p> <p>When this setting is not configured, local program settings on the remote desktop determine whether users can configure the COM port redirection settings.</p> <p>This setting is in the <b>VMware View Agent Configuration &gt; Serial COM</b> folder in the Group Policy Management Editor.</p>

## Smart Card Redirection Settings

Smart card redirection settings are in the **VMware View Agent Configuration > Smartcard Redirection > Local Reader Access** folder in the Group Policy Management Editor.

Table 5-13. Smart Card Redirection Policy Settings

Setting	Computer	User	Properties
Allow applications access to Local Smart Card readers	X		<p>If enabled, applications can access all local smart card readers even when the smart card redirection feature is installed. When enabled, the desktop is monitored for the presence of a local reader and when detected, the smart card redirection switches off, allowing access to the local readers. The redirection remains off until the next time the user connects to the session. When local access is enabled, applications can no longer access remote readers present on the client.</p> <p>This setting does not apply to RDP or to RDS hosts when the Remote Desktop Services role is enabled.</p> <p>This setting is disabled by default.</p>
Local Reader Name	X		<p>Specifies the name of a local reader to monitor to enable local access. By default, the reader must have a card inserted to enable local access. You can disable this requirement by using the Require an inserted Smart Card setting.</p> <p>This setting is enabled by default.</p>
Require an inserted Smart Card	X		<p>If enabled, local reader access is enabled if the local reader has a card inserted. If disabled, local access is enabled as long as a local reader is detected.</p> <p>This setting is enabled by default.</p>

## True SSO Configuration Settings

True SSO configuration settings are in the **VMware View Agent Configuration > True SSO Configuration** folder in the Group Policy Management Editor. See the *Horizon Administration* document.

## Unity Touch and Hosted Apps Settings

Unity Touch and Hosted Apps settings are in the **VMware View Agent Configuration > Unity Touch and Hosted Apps** folder in the Group Policy Management Editor.

Table 5-14. Unity Touch and Hosted Apps Policy Settings

Setting	Computer	User	Properties
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 windows that are smaller than 2x2 pixels, or that are located offscreen, are not sent to the client.  This setting is disabled by default.
Enable UWP support on RDSH platforms	X		When enabled, Universal Windows Platform (UWP) applications can run on Windows 10 virtual desktop (WVD) hosts on Horizon Cloud Service on Azure. When disabled, the application status shows as unavailable in Horizon Agent and the user cannot access the application. Restart the agent VM for this setting to take effect.  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 published applications in Horizon Client and allows mobile device users to access applications in the Unity Touch sidebar.  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 published applications.  This setting is enabled by default.
Enable user profile customization for Hosted Apps	X	X	Specifies whether to customize the user profile when published applications are used. If this setting is enabled, a user profile is generated, the Windows theme is customized, and startup applications are registered.  This setting is disabled by default.
Limit usage of Windows hooks	X		Disables most hooks when published 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 disabled by default, which means that all preferred hooks are used.
Only launch new instances of Hosted Apps if arguments are different	X		This policy controls the behavior when a published application starts, but an existing instance of the application is already running inside a disconnected protocol session. When disabled, the existing instance of the application activates. When enabled, the inside existing instance of the application activates only if the command-line parameters match.  This setting is disabled by default.



Table 5-14. Unity Touch and Hosted Apps Policy Settings (continued)

Setting	Computer	User	Properties
Redirect legal notice messages as a window	X		<p>When enabled, this policy redirects legal notices to a custom-sized window in Horizon Client. Specify the width and height of the window in pixels. For high DPI monitors, the sizes will be multiplied based on the DPI. This functionality is only supported for published applications.</p> <p>Restart the RDSH server and Horizon Client for the setting to take effect.</p> <p>This setting is disabled by default.</p>
Unity Filter rule list	X		<p>Specifies filter rules for unity windows when using published applications. Horizon Agent uses these rules to support custom applications. For information about creating filter rules, see <a href="#">Managing Special Unity Windows</a>.</p> <p>This setting is not configured by default.</p>

## View Agent Direct-Connection Configuration

Policy settings for View Agent Direct-Connection Configuration are in the ADMX template file `vdm_agent_direct_connection.admx`. View Agent Direct-Connection configuration settings are in the **VMware View Agent Configuration > View Agent Direct-Connection Configuration** folder in the Group Policy Management Editor. See the *View Agent Direct-Connection Plug-In Administration* document.

## Real-Time Audio-Video Configuration

Policy settings for Real-Time Audio-Video Configuration are in the ADMX template file `vdm_agent_rtav.admx`. RTAV configuration settings are in the **VMware View Agent Configuration > View RTAV Configuration** folder in the Group Policy Management Editor. See [Real-Time Audio-Video Group Policy Settings](#).

## USB Configuration

USB Configuration settings are in the **VMware View Agent Configuration > View USB Configuration** folder in the Group Policy Management Editor. See [Using Policies to Control USB Redirection](#).

## VMware AppTap Configuration

The VMware AppTap configuration setting is in the **VMware View Agent Configuration > VMware AppTap Configuration** folder in the Group Policy Management Editor.

Table 5-15. VMware AppTap Configuration Setting

Setting	Computer	User	Properties
Processes to ignore when detecting empty application sessions	X		Specifies the list of processes to ignore when detecting empty application sessions. You can specify either a process filename or a full path. Values are not case-sensitive. Do not use environment variables in paths. UNC network paths are allowed, example: \\vmware\temp\app.exe. This setting is not configured by default.

## Client Drive Redirection

Policy settings for Client Drive Redirection are in the ADMX template file `vdm_agent_cdr.admx`. Client Drive Redirection settings are in the **VMware View Agent Configuration > VMware Horizon Client Drive Redirection** folder in the Group Policy Management Editor. See [Client Drive Redirection Policy Settings](#).

## VMware HTML5 Features

VMware HTML5 features consist of Browser Redirection, Geolocation Redirection, HTML5 Multimedia Redirection, and WebRTC Redirection. Policy settings for these features are in the **VMware View Agent Configuration > VMware HTML5 Features** folder in the Group Policy Management Editor. See [VMware HTML5 Feature Policy Settings](#).

## VMware Integrated Printing

Policy settings for VMware Integrated Printing are in the ADMX template file `printerRedirection.admx`. VMware Integrated Printing settings are in the **VMware View Agent Configuration > VMware Integrated Printing** folder in the Group Policy Management Editor. See [VMware Integrated Printing Policy Settings](#).

## VMware Virtualization Pack for Skype for Business

VMware Virtualization Pack for Skype for Business settings are in the **VMware View Agent Configuration > VMware Virtualization Pack for Skype for Business** folder in the Group Policy Management Editor. See [VMware Virtualization Pack for Skype for Business Policy Settings](#).

## Watermark Configuration

The watermark configuration setting is in the **User Configuration** folder, located in **User Configuration > Policies > Administrative Templates > VMware View Agent Configuration > Watermark** folder in the Group Policy Management Editor.

Table 5-16. Watermark Configuration Setting

Setting	Computer	User	Properties
Watermark Configuration		X	<p>Enable this setting to configure a watermark to appear on your virtual desktop. Enter information you want to display as the watermark in <b>Text</b>. Options are:</p> <pre style="background-color: #f0f0f0; padding: 5px;"> %ViewClient_IP_Address% %ViewClient_Broker_UserName% %ViewClient_Broker_DomainName% %COMPUTERNAME% %USERDOMAIN% %USERNAME% %ViewClient_ConnectTime%</pre> <p>The character limit is 256 characters and 1024 characters after expansion.</p> <p><b>Image Layout:</b> the watermark layout on the screen, which is divided into nine squares:</p> <ul style="list-style-type: none"> <li>■ <b>Tile:</b> watermark is positioned in all 9 squares. This layout is always used for application sessions.</li> <li>■ <b>Multiple:</b> watermark is positioned in the center and four corner squares. If the watermark size exceeds the box size, it is scaled to maintain the aspect ratio.</li> <li>■ <b>Center:</b> watermark is positioned in the center square.</li> </ul> <p><b>Text Rotation:</b> a specific angle for the watermark text.</p> <p><b>Opacity:</b> the transparency level of the text. The range is 0 through 255. The default value is 255.</p> <p><b>Margin:</b> the space around the watermark for the Tile layout. If the watermark is scaled, the margin is also scaled.</p> <p>This setting is not configured by default.</p>

## 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** Client system information is passed to the second-hop desktop on the initial protocol connection. 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 5-17. Client System Information](#) 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.

**Note** The entries in the table appear in the registry only if they are configured.

**Table 5-17. Client System Information**

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
<code>ViewClient_IP_Address</code>	The IP address of the client system.	Yes	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
<code>ViewClient_MAC_Address</code>	The MAC address of the client system.	Yes	VDI (single-user machine) RDS	Windows, Linux, Mac, Android
<code>ViewClient_Machine_Name</code>	The machine name of the client system.	Yes	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
<code>ViewClient_Machine_Domain</code>	The domain of the client system.	Yes	VDI (single-user machine) RDS	Windows
<code>ViewClient_LoggedOn_Username</code>	The user name that was used to log in to the client system.		VDI (single-user machine) RDS	Windows, Linux, Mac

Table 5-17. Client System Information (continued)

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
ViewClient_LoggedOn_Domainname	The domain name that was used to log in to the client system.		VDI (single-user machine) RDS	Windows 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
ViewClient_Broker_DNS_Name	The DNS name of the Connection Server instance.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_URL	The URL of the Connection Server instance as specified by the client or the previous gateway.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
Broker_Tags	Restrict pools to be brokered by certain Connection Servers only.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
Broker_Pool_tags	Restrict pools to be brokered by certain Connection Servers only.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Gateway_Host	The value of the Host header in the request presented to the gateway.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Gateway_IP_Address	The IP address of the gateway.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.

Table 5-17. Client System Information (continued)

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
ViewClient_Broker_Gateway_Location	Whether the gateway is handling internal or external connections.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Gateway_Type	If this is a Horizon-aware gateway, a code indicating its type.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Tunnel_Enabled	The status of the tunnel connection for the Connection Server instance, which can be either true (enabled) or false (disabled).		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Tunnel_URL	The URL of the Connection Server tunnel connection, if the tunnel connection is enabled.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Remote_IP_Address	The IP address of the client system that is seen by the Connection Server instance.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Request_Path	All IP addresses, beginning with the public IP address of the client system that is seen by the Connection Server instance.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_TZID	The Olson time zone ID.  To disable time zone synchronization, enable the Horizon Agent <code>Disable Time Zone Synchronization</code> group policy setting.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS

Table 5-17. Client System Information (continued)

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
ViewClient_Windows_Timezone	The GMT standard time. To disable time zone synchronization, enable the Horizon Agent <code>Disable Time Zone Synchronization</code> group policy setting.		VDI (single-user machine) RDS	Windows
ViewClient_Broker_DomainName	Domain name used to authenticate to Connection Server.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Username	Username used to authenticate to Connection Server.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Client_ID	Specifies the Unique Client <code>HardwareId</code> used as a link to the license key.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Displays.Number	Specifies the number of monitors being used on the client.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Displays.Topology	Specifies the arrangement, resolution, and dimensions of displays on the client.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
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_Session Type	Specifies the session type. The type can be desktop or application.		VDI (single-user machine) RDS	Value is sent directly from Connection Server, not gathered by Horizon Client.
ViewClient_Mouse.Identifier	Specifies the type of mouse.		VDI (single-user machine) RDS	Windows

Table 5-17. Client System Information (continued)

Registry Key	Description	Supports Nested Mode	Supported Desktops	Supported Client Systems
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
ViewClient_Language	Specifies the operating system language.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Launch_Matched_Tags	Specifies one or more tags.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Launch_ID	Specifies the desktop or application pool unique ID.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Broker_Farm_ID	Specifies the farm ID of the desktop or application pool on an RDS host.		RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Client_Version	Specifies Horizon client version, in format {x.y.z}-{build_number}		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Keyboard.Subtype	Specifies the keyboard subtype, a vendor-specific value		VDI (single-user machine) RDS	Windows, Linux, Mac
ViewClient_Displays.TopologyV2	Extended Displays.Topology to include Monitor DPI value as the last element.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Displays.SystemDpi	Specifies the client OS system DPI.		VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS

**Note** The definitions of `ViewClient_LoggedOn_Username` and `ViewClient_LoggedOn_Domainname` in [Table 5-17. Client System Information](#) apply to Horizon Client for Windows.



## 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.

## Client Drive Redirection Policy Settings

The VMware Horizon Client Drive Redirection ADMX template file (`vdm_agent_cdr.admx`) contains policy settings related to the client drive redirection feature.

Client Drive Redirection settings are in the **VMware View Agent Configuration > VMware Horizon Client Drive Redirection** folder in the Group Policy Management Editor.

Table 5-18. Client Drive Redirection Settings

Setting	Computer	User	Properties
Configure drive letter mapping mode	X		<p>Specifies the drive letter mapping mode. When this setting is enabled, you can select one of the following modes:</p> <ul style="list-style-type: none"> <li>■ <b>One to one mapping</b>, which maps the drive letter on the client machine to the same drive letter on the agent machine. For example, drive X on the client machine is mapped to drive X on the agent machine.</li> <li>■ <b>Defined mapping</b>, which maps drive letters on the client machine to certain drive letters on the agent machine according to a mapping table that is defined in the <b>Define drive letter mapping table</b> group policy setting.</li> </ul> <p>If a drive letter conflict occurs, for example, if a drive letter to be mapped is already in use on the agent machine, the first available drive letter from Z to A is used. If no drive letter is available, a drive letter is not assigned.</p> <p>This setting is valid only when the <b>Display redirected device with drive letter</b> group policy setting is not disabled.</p>
Define drive letter mapping table	X		<p>When this setting is enabled, you can click <b>Show</b> and define a drive letter mapping table. In the <b>Value name</b> column, enter the drive letter on the client machine. In the corresponding <b>Value</b> column, enter the drive letter to use on the agent machine.</p> <p>This setting is valid only when you select <b>Defined mapping</b> in the <b>Configure drive letter mapping mode</b> group policy setting.</p>
Display redirected device with drive letter	X		<p>Determines whether to display a drive letter for drives that are redirected with the client drive redirection feature.</p> <p>This setting is enabled by default.</p>
Timeout for drive letter initialization	X		<p>Specifies how long to wait, in milliseconds, for Windows Explorer to initialize and display a drive letter for drives that are redirected with the client drive redirection feature.</p> <p>When this setting is disabled or not configured, the default value is 5000 milliseconds.</p>

## Policy Settings for Filtering Client Devices

Device filtering settings for Client Drive Redirection are in the **VMware View Agent Configuration > VMware Horizon Client Drive Redirection > Device Filtering** folder in the Group Policy Management Editor.

The device filtering feature works only for Horizon Client for Windows, Mac, and Linux. When these device filtering policies are set, client drive redirection is disabled for other clients, including Horizon Client for Android and iOS.

Table 5-19. Device Filtering Settings

Setting	Computer	User	Properties
Exclude Vid/Pid Device	X		<p>Excludes devices that have a specified vendor and product ID from being redirected with the client drive redirection feature.</p> <p>You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. Use a semicolon to separate multiple devices. For example:</p> <pre>vid-0781_pid-554c;vid-0781_pid-****</pre> <p>The default value is undefined (no devices are excluded).</p> <p>This setting takes precedence over the <b>Include Vid/Pid Device</b> setting.</p> <hr/> <p><b>Note</b> To disable client drive redirection for all devices, you can specify <code>vid-****_pid-****</code>.</p>
Include Vid/Pid Device	X		<p>Specifies devices that have a specified vendor and product ID that can be redirected with the client drive redirection feature.</p> <p>You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. Use a semicolon to separate multiple devices. For example:</p> <pre>vid-054C_pid-0099;vid-8888_pid-****</pre> <p>The default value is undefined (all devices are included).</p>

## VMware HTML5 Feature Policy Settings

The VMware View Agent Configuration ADMX template file (`vdm_agent.admx`) contains policy settings related to the VMware HTML5 features.

### General VMware HTML5 Feature Settings

General VMware HTML5 feature settings are in the Group Policy Management Editor in the **Computer Configuration > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features** folder.

Table 5-20. General VMware HTML5 Feature Settings

Setting	Description
Enable VMware HTML5 Features	Enables the VMware HTML5 features. You must enable this setting to use the VMware HTML5 Multimedia Redirection, Geolocation Redirection, or Browser Redirection feature. This setting takes effect at the next logon.
Disable Automatically Detect Intranet	<p>When the policy is enabled, the intranet settings "Include all local (intranet) sites not listed in other zones" and "Include all sites that bypass the proxy server" are disabled during the next logon.</p> <p>When this policy is disabled, no changes are made to the IE Local intranet zone.</p> <p><b>Important</b> You must enable this setting if you enable the Edge browser for the HTML5 Multimedia Redirection feature or enable the Geolocation Redirection feature.</p>

## VMware HTML5 Multimedia Redirection Feature Settings

VMware HTML5 Multimedia Redirection feature settings are in the Group Policy Management Editor in the **Computer Configuration > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware HTML5 Multimedia Redirection** folder.

Table 5-21. VMware HTML5 Multimedia Redirection Policy Settings

Setting	Description
Enable VMware HTML5 Multimedia Redirection	Enables the VMware HTML5 Multimedia Redirection feature. This setting takes effect at the next logon.
Enable URL list for VMware HTML5 Multimedia Redirection	<p>Specifies which websites use the HTML5 Multimedia Redirection feature.</p> <p>Enter the list of URLs for the websites that can redirect HTML5 multimedia content in the Value name column. Include the <code>http://</code> or <code>https://</code> prefix in the URLs. You can use match patterns in the URLs.</p> <p>For example, to redirect all videos on YouTube, enter <code>https://www.youtube.com/*</code>. To redirect all videos on Vimeo, enter <code>https://www.vimeo.com/*</code>.</p> <p>Leave the Value column blank.</p>
Enable Chrome Browser for VMware HTML5 Multimedia Redirection	Enables the HTML5 Multimedia Redirection feature for the Google Chrome browser. This policy is used only when the VMware HTML5 Multimedia Redirection feature is enabled. If this policy is not configured, the default value is the same as the value of the Enable VMware HTML5 Multimedia Redirection setting.

Table 5-21. VMware HTML5 Multimedia Redirection Policy Settings (continued)

Setting	Description
Enable legacy version of Microsoft Edge Browser for VMware HTML5 Multimedia Redirection	Enables the HTML5 Multimedia Redirection feature for the legacy Microsoft Edge browser. This policy is used only when the VMware HTML5 Multimedia Redirection feature is enabled. If this policy is not configured, the default value is the same as the value of the Enable VMware HTML5 Multimedia Redirection setting.
Enable Microsoft Edge (Chromium) Browser for VMware HTML5 Multimedia Redirection	Enables the HTML5 Multimedia Redirection feature for the Microsoft Edge (Chromium) browser. This policy is used only when the VMware HTML5 Multimedia Redirection feature is enabled. If this policy is not configured, the default value is the same as the value of the Enable VMware HTML5 Multimedia Redirection setting.

## VMware Geolocation Redirection Feature Settings

VMware Geolocation Redirection feature settings are in the Group Policy Management Editor in the **Computer Configuration > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware Geolocation Redirection** folder.

Table 5-22. VMware Geolocation Redirection Settings

Setting	Description
Enable URL list for VMware Geolocation Redirection	Specifies which websites use the Geolocation Redirection feature.  Enter the list of URLs for the websites that can redirect geolocation information in the Value name column. Include the <code>http://</code> or <code>https://</code> prefix in the URLs. You can use match patterns in the URLs.  For example, to specify all YouTube videos, enter <code>https://www.youtube.com/*</code> . To specify all Vimeo videos, enter <code>https://www.vimeo.com/*</code> .  Leave the Value column blank.
Enable VMware Geolocation Redirection	Enables the Geolocation Redirection feature. This setting takes effect at the next logon.
Enable VMware Geolocation Redirection for Chrome Browser	Enables the Geolocation Redirection feature for the Google Chrome browser. This setting takes effect the next time a user logs in.
Enable VMware Geolocation Redirection for Microsoft Edge (Chromium) Browser	Enables the Geolocation Redirection feature for the Microsoft Edge (Chromium) browser. This setting takes effect the next time a user logs in.
Set the minimum distance for which to report location updates	Specifies the minimum distance, in meters, between a location update in the client and the last update reported to the agent for which the new location must be reported to the agent.  By default, the minimum distance used is 75 meters.

## VMware Browser Redirection Feature Settings

VMware Browser Redirection feature settings are in the Group Policy Management Editor in the **Computer Configuration > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware Browser Redirection** folder.

Table 5-23. VMware Browser Redirection Settings

Setting	Description
Enable VMware Browser Redirection	Enables the Browser Redirection feature.
Enable URL list for VMware Browser Redirection	<p>Specifies all the URLs for the Browser Redirection feature. Users can visit these URLs by entering them in either the Chrome address bar or the custom address bar. Users can also visit these URLs by navigating to them starting from another URL in the list, or from any agent-side rendered page.</p> <p>Enter the URLs in the Value name column. Include the <code>http://</code> or <code>https://</code> prefix in the URLs. You can use match patterns in the URLs. Match patterns must follow <a href="https://developer.chrome.com/extensions/match_patterns">https://developer.chrome.com/extensions/match_patterns</a>.</p> <p>For example, to specify all YouTube content, enter <code>https://www.youtube.com/*</code>.</p> <p>Leave the Value column blank.</p>
Enable Navigation URL list for VMware Browser Redirection	<p>Specifies the URLs that a user is allowed to navigate to from a URL specified in the <b>Enable URL list for VMware Browser Redirection</b> white list., either by entering the URL directly in the custom address bar, or by navigating to the URL starting from a URL in the white list.</p> <p>Users cannot visit these URLs directly by typing them into the Chrome address bar or by navigating to them from an agent-side rendered page.</p> <p>Enter the list of URLs in the Value name column. Include the <code>http://</code> or <code>https://</code> prefix in the URLs. You can use match patterns in the URLs. Match patterns must follow <a href="https://developer.chrome.com/extensions/match_patterns">https://developer.chrome.com/extensions/match_patterns</a>.</p> <p>For example, to specify all YouTube content, enter <code>https://www.youtube.com/*</code>.</p> <p>Leave the Value column blank.</p>

Table 5-23. VMware Browser Redirection Settings (continued)

Setting	Description
Enable automatic fallback after a whitelist violation	<p>When this setting is enabled, if a user navigates to a URL that is not specified in one of the Browser Redirection white lists, either by entering it in the custom address bar or by navigating to it starting from a URL in either white list, redirection stops for that tab and the URL is fetched and displayed on the agent instead.</p> <p><b>Note</b> If a user attempts to navigate to a URL that is not specified in the <b>Enable URL list for VMware Browser Redirection</b> setting, the tab always falls back to fetching and rendering the URL on the agent, regardless of whether this setting is enabled.</p>
Show a page with error information before automatic fallback	<p>When this setting is enabled, and a white list violation occurs, a page appears that shows a five-second count down. After five seconds have elapsed, the tab falls back to fetching and rendering the URL that caused the violation on the agent. If this setting is disabled, the five-second warning page does not appear.</p> <p>This setting takes effect only if the <b>Enable automatic fallback after a whitelist violation</b> setting is also enabled.</p>
Enable VMware Browser Redirection for Chrome Browser	Enables the Browser Redirection feature for the Google Chrome browser. This setting takes effect the next time a user logs in.
Enable VMware Browser Redirection feature for Microsoft Edge (Chromium) Browser	Enables the Browser Redirection feature for the Microsoft Edge (Chromium) browser. This setting takes effect the next time a user logs in.

## VMware WebRTC Redirection Features Settings

General VMware HTML5 feature settings are in the Group Policy Management Editor in the **Computer Configuration > Administrative Templates > VMware View Agent Configuration > VMware HTML5 Features > VMware WebRTC Redirection Features** folder.

Table 5-24. VMware WebRTC Redirection Features Settings

Setting	Description
Configure CPU overuse threshold	If CPU usage is above the default threshold of 85, the sent video resolution is reduced, which will lower client CPU usage. Enable this policy with a value less than 85 to reduce client CPU during video calls. To use the default threshold of 85, disable or do not configure this policy. If you do not want to detect CPU overuse, enable this policy with a value of 0. This setting takes effect at the next logon.
Enable Media Optimization for Microsoft Teams	This policy enables Media Optimization for Microsoft Teams. If the policy is not configured, it is disabled. You must enable this policy to apply Media Optimization for Microsoft Teams.
Enable sharing the client desktop screen while remoting the Microsoft Teams application in application sharing mode	When you enable Microsoft Teams screen share feature in a published application, the screen share feature will share the client desktop screen instead of the remote desktop screen. Disable the policy to disable the screen share feature in application sharing mode. If the policy is enabled or not configured, the screen share can share the client desktop screen.
Enable software acoustic echo cancellation for Media Optimization for Microsoft Teams	This policy enables or disables acoustic echo cancellation in the software irrespective of acoustic echo cancellation availability in the hardware.  If the policy is not configured, acoustic echo cancellation is enabled in the software whenever it is not available in the hardware.

## 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 5-25. Virtualization Pack for Skype for Business Policy Settings**

Setting	Description
Disable extended filter for acoustic echo cancellation in VMware Virtualization Pack for Skype for Business	Enabled by default, the extended filter for acoustic echo cancellation provides better echo and feedback cancellation and is particularly effective in scenarios when Horizon Client system's microphone and speaker are close in proximity to each other. Enable this policy if you do not want VMware Virtualization Pack for Skype for Business to use this filter.
EnableDetectProxySettings	Enable this policy to reduce delays when the Horizon Client system is required to use a proxy server. When enabled, Virtualization Pack for Skype for Business checks for proxy settings on the Horizon Client system, and uses those settings for media traffic. If proxy settings are not present on the Horizon Client system, Virtualization Pack for Skype for Business uses direct connection.
Force Skype for Business in non-optimized mode	<p>You can force Skype for Business to run in the non-optimized mode for Horizon Client connections by automatically detecting external connections that are determined when Horizon Client connects to an external gateway.</p> <p>In this scenario, the environment variables ViewClient_Broker_GatewayType is present and ViewClient_Broker_GatewayLocation is set to external.</p> <p>If you check the box to automatically detect external connections, Virtualization Pack for Skype for Business reverts to fallback mode if the connection is determined to be external.</p> <p>You can also force Skype for Business to run in the non-optimized mode for Horizon Client connections by setting the name of environment variable that will be present at connection time on the machine where Horizon Agent is installed. If the variable name is set, Virtualization Pack for Skype for Business reverts to fallback mode.</p> <p>For example, if the environment variable ViewClient_F5_APM is set on the Remote Desktop Agent machine when the Horizon Client machine connects from outside the network using F5 load balancer, and you want to force non-optimized mode, set this value to ViewClient_F5_APM.</p> <p>This policy is not configured by default.</p>
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.
Suppress minor version mismatch warning	The notification area displays a warning if the Virtualization Pack for Skype for Business does not have the same minor API version on the Horizon Client system and on the Horizon desktop. When this policy is enabled, this warning will be suppressed. Note that when there is a minor API version mismatch, Skype for Business calls will be optimized, but the Virtualization Pack might not have the latest functionality.

## VMware Integrated Printing Policy Settings

The VMware Integrated Printing ADMX template file (printerRedirection.admx) contains policy settings related to the VMware Integrated Printing feature.

These settings are in the Group Policy Management Editor in the **Computer Configuration > Administrative Templates > VMware Integrated Printing** folder and also in **User Configuration > Policies > Administrative Templates > VMware View Agent Configuration > VMware Integrated Printing** folder. If the User Configuration setting is enabled, it overrides the equivalent Computer Configuration setting. If the User Configuration setting is not enabled, the Computer Configuration settings is used.

Table 5-26. VMware Integrated Printing Policy Settings

Setting	Description
Default settings for UPD printers	<p>When this setting is enabled, you can define the following default settings for UPD printers.</p> <ul style="list-style-type: none"> <li>■ Duplex: None, Flip on Long Edge, or Flip on Short Edge</li> <li>■ Color: Black/White or Color</li> <li>■ Compression Level: Lossless, High Quality, Optimized, No Image</li> </ul> <p>When a client printer supports Duplex printing, the default Duplex print setting will be used as the initial Duplex print setting of the UPD printer. If a client printer supports Duplex printing and the checkbox <b>Always use default duplex setting</b> is selected, the redirected UPD printer will always use the default Duplex print setting as the Duplex print setting and user cannot change the Duplex print setting.</p> <p>If a client printer does not support the Duplex print setting, the default Duplex print setting and <b>Always use default duplex setting</b> setting will be ignored by the redirected UPD printer.</p> <p>Color print setting is similar. If a client printer does not support the Color print setting, the default Color print setting and <b>Always use default color setting</b> setting will be ignored by the redirected UPD printer.</p> <p>For example, a client printer supports Color printing but does not support Duplex printing. When defining the default Duplex setting to Flip On Long Edge and defining Color setting to Color, the initial setting of the redirected UPD printer is Simplex and Color.</p> <p>For each print setting, selecting or deselecting a checkbox determines whether or not a user can change the default print setting.</p> <p>When this setting is disabled or not configured, default settings are not enabled for UPD printers.</p> <p>This setting is not configured by default.</p>
Disable LBP	<p>Specifies whether location-based printing is enabled. When this setting is enabled, location-based printing is disabled. When this setting is disabled or not configured, location-based printing is enabled.</p>
Disable Printer Property Persistence	<p>Determines whether printer properties are persistent. When this setting is enabled, printer properties are not persistent between the client local printer and the redirected printer. When this setting is disabled or not configured, printer properties are persistent between the client local printer and the redirected printer.</p> <p>This setting is not configured by default.</p>

Table 5-26. VMware Integrated Printing Policy Settings (continued)

Setting	Description
Disable printer redirection for non-desktop client	<p>Determines whether VMware Integrated Printing is supported for non-desktop client endpoints.</p> <p>When this setting is enabled, VMware Integrated Printing is not supported for non-desktop client endpoints. When this setting is not configured or disabled, VMware Integrated Printing is supported for non-desktop client endpoints.</p> <p>This setting is not configured by default.</p>
Do not change default printer	<p>Determines whether VMware Integrated Printing changes the default printer in remote sessions.</p> <p>By default, if any location-based printer is configured as the default printer, that printer is set as the default printer in remote sessions. If no location-based printer is configured to be the default printer, the default client printer is set as the default printer in remote sessions and overwrites any printer selected in the VM image. You can use this setting to override this behavior.</p> <p>If you enable this setting, VMware Integrated Printing does not change the default printer in remote sessions.</p> <p>If you disable or do not configure this setting, VMware Integrated Printing changes the default printer in remote sessions. This is the default behavior.</p> <p>This setting is not configured by default.</p>
Do not redirect client printer(s)	<p>Determines whether client printers are redirected.</p> <p>When this setting is enabled, no client printers are redirected. When this setting is disabled or not configured, all client printers are redirected.</p> <p>This setting is not configured by default.</p> <p>Changes to this setting do not take effect until the user disconnects and reconnects to the remote desktop.</p>
Limit Tx Rate (KBps)	<p>Limits the transmission rate in kilobytes per second (KBps) of all print jobs. The minimum allowed Tx rate is 200KBps. The maximum allowed Tx rate is 4000KBps. When this setting is not configured, disabled, or set to a Tx rate greater than the maximum (4000KBps), the Tx rate is not limited.</p> <p>This setting is not configured by default.</p>
Print Preview Setting	<p>Configures the print preview behavior.</p> <p><b>Disable Print Choice</b> determines whether the print target is enabled. When this setting is selected, users cannot select the print target. When this setting is deselected or not configured, users can select the print target, which can be print preview or print directly. It is not configured by default.</p> <p><b>Print Target Default Choices</b> specifies the default print target. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Print directly:</b> the default print option in the print user interface is to print directly.</li> <li>■ <b>Print preview:</b> the default print option in the print user interface is print preview.</li> </ul>

Table 5-26. VMware Integrated Printing Policy Settings (continued)

Setting	Description
Printer Driver Selection	<p data-bbox="644 275 1412 333">Specifies the printer driver to use for redirected client printers. When this setting is enabled, the options are as follows:</p> <ul data-bbox="644 346 1412 640" style="list-style-type: none"> <li data-bbox="644 346 1412 405">■ <b>Always Use NPD</b> uses the native printer driver for the redirected printer.</li> <li data-bbox="644 415 1412 474">■ <b>Always Use UPD</b> uses the universal printer driver for the redirected printer</li> <li data-bbox="644 485 1412 543">■ <b>Use NPD First, then UPD</b> uses the native printer driver first and, if the native printer does not exist, uses the universal printer driver.</li> <li data-bbox="644 554 1412 640">■ <b>Use UPD First, then NPD</b> uses the universal printer driver first and, if the universal printer driver does not exist, uses the native printer driver.</li> </ul> <p data-bbox="644 653 1412 709">When this setting is disabled or not configured, the default value is <b>Use NPD First, then UPD</b> .</p>

Table 5-26. VMware Integrated Printing Policy Settings (continued)

Setting	Description
Printer Name Schema	<p>Determines the printer naming convention when you use VMware Integrated Printing.</p> <p>When this setting is enabled, you can change the printer name schema used for virtual desktops, published desktops, and published applications. The printer name schema must be in the format "%P (*)", where * represents the configurable part of the printer name. You can specify the following variables:</p> <ul style="list-style-type: none"> <li>■ %S: session ID</li> <li>■ %C: client machine name</li> </ul> <p>If this setting is enabled, but the printer name schema is empty or invalid, the default printer name schema is used.</p> <p>When this setting is not configured or disabled, virtual desktops use the printer name schema "%P (vdi)". Published desktops and published applications use the printer name schema "%P (v%S)".</p> <p>This setting is not configured by default.</p>
Specify a filter in redirecting client printers	<p>Specifies a rule that filters client printers from printer redirection. When this setting is enabled, you can type a filtering rule in the <b>Printer Filter</b> text box. The filtering rule is a regular expression that specifies the printers that are not redirected (a deny list). Any printer that does not match the printers in the filtering rule is redirected.</p> <p>The following attributes, operators, and wild cards are supported in the filtering rule:</p> <ul style="list-style-type: none"> <li>■ Attributes: DriverName, VendorName, and PrinterName</li> <li>■ Operators: AND, OR, and NOT</li> <li>■ Wild cards: * and ?</li> </ul> <p>Following are examples of filtering rules.</p> <pre>(DriverName="DrName1" OR VendorName="VeName1") AND NOT PrinterName="PrNa.?e" PrinterName=".*HP.*" OR PrinterName=".*EPSON.*" AND DriverName="PDF" PrinterName!=".*PDFCreator.*"</pre> <p><b>Note</b> The filtering rule is not case sensitive. To use an exact match, use a regular expression such as "^HP\$" rather than "HP".</p> <p>By default, the filtering rule is empty, which means that all client printers are redirected.</p>

## PCoIP Policy Settings

The PCoIP ADMX template file (`pcoip.admx`) contains policy settings related to the PCoIP display protocol. 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 VMware–Horizon–Extras–Bundle–YYMM–x.x.x–yyyyyyyyy.zip, which you can download from the VMware Downloads site at <https://my.vmware.com/web/vmware/downloads>. Under Desktop & End-User Computing, select the VMware Horizon download, which includes the GPO Bundle containing the 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 5-27. PCoIP General Policy Settings

Setting	Description
Configure PCoIP event log cleanup by size in MB	<p>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 <math>m</math>, log files larger than <math>m</math> MB are automatically and silently deleted. A setting of 0 indicates that no file cleanup by size takes place.</p> <p>When this policy is disabled or not configured, the default event log cleanup by size is 100 MB.</p> <p>The log file cleanup is performed once at session startup. A change to the setting is not applied until the next session.</p>
Configure PCoIP event log cleanup by time in days	<p>Enables the configuration of the PCoIP event log cleanup by time in days.</p> <p>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 <math>n</math>, log files older than <math>n</math> days are automatically and silently deleted. A setting of 0 indicates that no file cleanup by time takes place.</p> <p>When this policy is disabled or not configured, the default event log cleanup is 7 days.</p> <p>The log file cleanup is performed once at session startup. A change to the setting is not applied until the next session.</p>
Configure PCoIP event log verbosity	<p>Sets the PCoIP event log verbosity. The values range from 0 (least verbose) to 3 (most verbose).</p> <p>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.</p> <p>When this setting is modified during an active PCoIP session, the new setting takes effect immediately.</p>

Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Configure PCoIP image quality levels	<p>Controls how PCoIP renders images during periods of network congestion. The <b>Minimum Image Quality</b>, <b>Maximum Initial Image Quality</b>, and <b>Maximum Frame Rate</b> values interoperate to provide fine control in network-bandwidth constrained environments.</p> <p>Use the <b>Minimum Image Quality</b> 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.</p> <p>Use the <b>Maximum Initial Image Quality</b> 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.</p> <p>The <b>Minimum Image Quality</b> value cannot exceed the <b>Maximum Initial Image Quality</b> value.</p> <p>Use the <b>Maximum Frame Rate</b> 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.</p> <p>These image quality values apply to the soft host only and have no effect on a soft client.</p> <p>When this setting is disabled or not configured, the default values are used.</p> <p>When this setting is modified during an active PCoIP session, the new setting takes effect immediately.</p>



Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Configure frame rate vs image quality preference	<p>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.</p> <p>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.</p> <p>This setting could work with the <code>Configure PCoIP image quality levels GPO</code>, which determines the max initial image quality level and min image quality level. While the <code>Frame rate and image quality preference</code> can adjust the image quality level for each frame, it cannot exceed the max/min quality level threshold configured by <code>Configure PCoIP image quality levels GPO</code>.</p> <p>When this policy is changed during run time, it could take effect immediately.</p>
Configure PCoIP session encryption algorithms	<p>Controls the encryption algorithms advertised by the PCoIP endpoint during session negotiation.</p> <p>Checking one of the check boxes disables the associated encryption algorithm. You must enable at least one algorithm.</p> <p>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 <b>Disable AES-128-GCM encryption</b> value is always overridden so that AES-128-GCM encryption is enabled.</p> <p>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.</p> <p>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.</p>

Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Configure PCoIP USB allowed and unallowed device rules	<p>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.</p> <p>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.</p> <p>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.</p> <p>The format of a combination VID/PID rule is <b>1xxxxyyyy</b>, where <b>xxxx</b> is the VID in hexadecimal format and <b>yyyy</b> is the PID in hexadecimal format. For example, the rule to authorize or block a device with VID <b>0x1a2b</b> and PID <b>0x3c4d</b> is <b>11a2b3c4d</b>.</p> <p>For class rules, use one of the following formats:</p> <p><b>Allow all USB devices</b></p> <p>Format: <b>23XXXXXX</b></p> <p>Example: <b>23XXXXXX</b></p> <p><b>Allow USB devices with a specific class ID</b></p> <p>Format: <b>22classXXXX</b></p> <p>Example: <b>22aaXXXX</b></p> <p><b>Allow a specific subclass</b></p> <p>Format: <b>21class-subclassXX</b></p> <p>Example: <b>21aabbXX</b></p> <p><b>Allow a specific protocol</b></p> <p>Format: <b>20class-subclass-protocol</b></p> <p>Example: <b>20aabbcc</b></p> <p>For example, the USB authorization string to allow USB HID (mouse and keyboard) devices (class ID 0x03) and webcams (class ID 0x0e) is <b>2203XXXX 220eXXXX</b>. The USB unauthorization string to disallow USB Mass Storage devices (class ID 0x08) is <b>2208XXXX</b>.</p> <p>An empty USB authorization string means that no USB devices are authorized. An empty USB unauthorization string means that no USB devices are banned.</p> <p>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.</p> <p>By default, all devices are allowed and none are disallowed.</p>

Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Configure PCoIP virtual channels	<p>Specifies the virtual channels that can and cannot operate over PCoIP sessions.</p> <p>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.</p> <p>You can specify a maximum of 15 virtual channels for use in PCoIP sessions.</p> <p>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 <b>mksvchan vdp_vdpvcbridge</b>.</p> <p>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 <b>awk\ ward\channel</b>.</p> <p>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.</p> <p>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.</p> <p>By default, all virtual channels are enabled.</p>
Configure the PCoIP transport header	<p>Configures the PCoIP transport header and sets the transport session priority.</p> <p>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.</p> <p>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.</p> <p>When the Configure the PCoIP transport header setting is enabled, the following transport session priorities are available:</p> <ul style="list-style-type: none"> <li>■ <b>High</b></li> <li>■ <b>Medium</b> (default value)</li> <li>■ <b>Low</b></li> <li>■ <b>Undefined</b></li> </ul> <p>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 <b>Undefined Priority</b> is specified, the session uses the default value, <b>Medium</b> priority.</p>

Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Configure the TCP port to which the PCoIP host binds and listens	<p>Specifies the TCP agent port bound to by software PCoIP hosts.</p> <p>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.</p> <p>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.</p> <p>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, <code>The Display protocol for this desktop is currently not available. Please contact your system administrator.</code></p> <p>This setting applies to Horizon Agent only.</p> <p>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.</p> <p>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.</p> <p><b>Important</b> 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.</p>

Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Configure the UDP port to which the PCoIP host binds and listens	<p>Specifies the UDP agent port bound to by software PCoIP hosts.</p> <p>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.</p> <p>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, <i>The Display protocol for this desktop is currently not available. Please contact your system administrator.</i></p> <p>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.</p> <p>This setting applies to Horizon Agent only.</p> <p>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.</p> <p>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.</p> <p><b>Important</b> 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.</p>
Enable access to a PCoIP session from a vSphere console	<p>Determines whether to allow a vSphere Client console to display an active PCoIP session and send input to the desktop.</p> <p>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.</p> <p>This setting applies to Horizon Agent only.</p> <p>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.</p> <p>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.</p>
Enable/disable audio in the PCoIP session	<p>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.</p>

Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Enable/disable microphone noise and DC offset filter in PCoIP session	<p>Determines whether to enable the microphone noise and DC offset filter for microphone input during PCoIP sessions.</p> <p>This setting applies to Horizon Agent and Teradici audio driver only.</p> <p>When this setting is not configured, the Teradici audio driver uses the microphone noise and DC offset filter by default.</p>
Turn on PCoIP user default input language synchronization	<p>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.</p> <p>This setting applies to Horizon Agent only.</p>
Configure SSL Connections to satisfy Security Tools	<p>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:</p> <ol style="list-style-type: none"> <li>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.</li> <li>2 Store the certificate for the Certificate Authority that signed it in the Trusted Root certificate store.</li> <li>3 Disable connections to VMware View 5.1 and earlier.</li> <li>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.</li> </ol> <p>The resulting PCoIP Server will satisfy Security Tools such as port scanners.</p>

Table 5-27. PCoIP General Policy Settings (continued)

Setting	Description
Configure SSL Protocols	<p>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.</p> <p>The default value is: "TLS1.1:TLS1.2"</p> <p>This means that both TLS v1.1 and TLS v1.2 are enabled (SSL v2.0, SSLv3.0 and TLS v1.0 are disabled).</p> <p>This setting applies to both Horizon Agent and Horizon Client.</p> <p>If it is set on both sides, the OpenSSL protocol negotiation rule will be followed.</p>
Configure SSL cipher list	<p>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.</p> <p>The default value is ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH.</p> <p>If this setting is configured, the <b>Enforce AES-256 or stronger ciphers for SSL connection negotiation</b> check box in the <b>Configure SSL connections to satisfy Security Tools</b> setting is ignored.</p> <p>This setting must be applied to both the PCoIP server and the PCoIP client.</p>

## 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 5-28. Horizon PCoIP Session Bandwidth Variables

Setting	Description
Configure the maximum PCoIP session bandwidth	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The default value when this setting is not configured is 900000 kilobits per second.</p> <p>This setting applies to Horizon Agent and the client. If the two endpoints have different settings, the lower value is used.</p>
Configure the PCoIP session bandwidth floor	<p>Specifies a lower limit, in kilobits per second, for the bandwidth that is reserved by the PCoIP session.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>This setting applies to Horizon Agent and the client, but the setting only affects the endpoint on which it is configured.</p> <p>When this setting is modified during an active PCoIP session, the change takes effect immediately.</p>



**Table 5-28. Horizon PCoIP Session Bandwidth Variables (continued)**

<b>Setting</b>	<b>Description</b>
Configure the PCoIP session MTU	<p>Specifies the Maximum Transmission Unit (MTU) size for UDP packets for a PCoIP session.</p> <p>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.</p> <p>The maximum MTU size is 1500 bytes. The minimum MTU size is 500 bytes. The default value is 1300 bytes.</p> <p>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.</p> <p>This setting applies to Horizon Agent and the client. If the two endpoints have different MTU size settings, the lowest size is used.</p> <p>If this setting is disabled or not configured, the client uses the default value in the negotiation with Horizon Agent.</p>

Table 5-28. Horizon PCoIP Session Bandwidth Variables (continued)

Setting	Description
Configure the PCoIP session audio bandwidth limit	<p>Specifies the maximum bandwidth that can be used for audio (sound playback) in a PCoIP session.</p> <p>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.</p> <p>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.</p> <p>This setting applies to Horizon Agent only. You must enable audio on both endpoints before this setting has any effect.</p> <p>In addition, this setting has no effect on USB audio.</p> <p>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.</p> <p>This setting applies to View 4.6 and later. It has no effect on earlier versions of View.</p> <p>When this setting is modified during an active PCoIP session, the change takes effect immediately.</p>
Turn off Build-to-Lossless feature	<p>Specifies whether to turn the build-to-lossless feature of the PCoIP protocol off or on. This feature is turned off by default.</p> <p>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.</p> <p>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.</p> <p>When this setting is modified during an active PCoIP session, the change takes effect immediately.</p> <p>For more information about the PCoIP build-to-lossless feature, see <a href="#">PCoIP Build-to-Lossless Feature</a>.</p>

## 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 5-29. Horizon PCoIP Session Variables for the Keyboard**

Setting	Description
Disable sending CAD when users press Ctrl+Alt+Del	<p>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.</p> <p>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.</p> <p>This setting applies to Horizon Agent only and has no effect on a client.</p> <p>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.</p>
Use alternate key for sending Secure Attention Sequence	<p>Specifies an alternate key, instead of the Insert key, for sending a Secure Attention Sequence (SAS).</p> <p>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.</p> <p>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+<i>Alternate Key</i> sequence to send a Ctrl+Alt+Del SAS to the PCoIP desktop.</p> <p>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.</p> <p>When this setting is disabled or not configured, the Ctrl+Alt+Ins key sequence is used as the SAS.</p> <p>This setting applies to Horizon Agent only and has no effect on a client.</p>

## 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 1Mbps, 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 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 Client platforms.

**Table 5-30. VMware Blast Policy Settings**

Setting	Description
Audio playback	Specifies whether audio playback is enabled for remote desktops. This setting is to enable audio playback.
Blast Codec Quality	The minimum and maximum values of the Quantization Parameter (QP) control the image quality of the remoted display when using Blast Codec compression. The QP values range [1-8] and roughly map to the JPEG quality value in the range [20-88]. This quantization applies to non-text regions and has no bearing on text compression.  The maximum QP is mapped to the low JPEG quality configuration and a value of zero for maximum QP results in overriding the configuration by the low JPEG quality configuration.  The minimum QP is mapped to the high JPEG quality configuration and a value of zero for minimum QP results in overriding the configuration by the high JPEG quality configuration.
Cookie Cleanup Interval	Determines how often, in milliseconds, cookies associated with inactive sessions are deleted. The default is 100 ms.
Cursor warping	When this setting is enabled, the cursor warping feature is enabled. When enabled and the mouse is in absolute mode, the remote agent detects sudden cursor movements and reflects them to the client by moving the local cursor. If this setting is not enabled, sudden cursor movements in the remote agent will be ignored by the client. This setting is disabled by default.

Table 5-30. VMware Blast Policy Settings (continued)

Setting	Description
DSCP Marking	<p>When enabled or not configured, this setting allows Differentiated Services Code Point (DSCP) values to be established in outgoing Blast network traffic, as specified by the various individual settings for each network hop. When disabled, DSCP values are not established in Blast network traffic.</p> <p>When enabled, you can set a numeric value in the range 0-63 for the following network connections:</p> <ul style="list-style-type: none"> <li>■ DSCP from Agent, TCP/IPv4</li> <li>■ DSCP from Agent, TCP/IPv6</li> <li>■ DSCP from Agent, UDP/IPv4</li> <li>■ DSCP from Agent, UDP/IPv6</li> <li>■ DSCP from BSG to Client, TCP/IPv4</li> <li>■ DSCP from BSG to Client, TCP/IPv6</li> <li>■ DSCP from BSG to Client, UDP/IPv4</li> <li>■ DSCP from BSG to Client, UDP/IPv6</li> <li>■ DSCP from BSG to Agent, TCP/IPv4</li> <li>■ DSCP from BSG to Agent, TCP/IPv6</li> <li>■ DSCP from BSG to Agent, UDP/IPv4</li> <li>■ DSCP from BSG to Agent, UDP/IPv6</li> <li>■ DSCP from Client, TCP/IPv4</li> <li>■ DSCP from Client, TCP/IPv6</li> <li>■ DSCP from Client, UDP/IPv4</li> <li>■ DSCP from Client, UDP/IPv6</li> </ul>
H264	Specifies whether to use H.264 encoding or JPEG/PNG encoding. The default is to use H.264 encoding.
H264 High Color Accuracy	<p>Increases color accuracy when using H.264 encoding by using the YUV 4:4:4 colorspace instead of 4:2:0.</p> <p>This setting might result in degraded performance at very high resolutions or with multiple monitors.</p>
H.264 Quality	<p>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:</p> <ul style="list-style-type: none"> <li>■ <b>H264maxQP</b> (available range of values: 0-51, default: 36)</li> <li>■ <b>H264minQP</b> (available range of values: 0-51, default: 10)</li> </ul> <p>For the best image quality, set the quantization parameter (QP) values to within +5 or -5 of the available range of values. These parameters determine the amount of data that is discarded, so a lower value results in higher image quality.</p>
HEVC High Color Accuracy	Enable this setting to request increased color accuracy by using the YUV 4:4:4 colorspace instead of 4:2:0 with HEVC encoding. The client requires hardware HEVC 4:4:4 support for this policy to take effect. This setting is enabled by default.
HEVC	Enable or do not configure this setting to allow HEVC encoding for remoting the desktop. Disable this setting to use H.264 or JPEG/PNG for encoding.

Table 5-30. VMware Blast Policy Settings (continued)

Setting	Description
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.
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: <ul style="list-style-type: none"> <li>■ <b>Low JPEG Quality</b> (available range of values: 10 - 100, default: 25)</li> <li>■ <b>Mid JPEG Quality</b> (available range of values: 10- 100, default: 35)</li> <li>■ <b>High JPEG Quality</b> (available range of values: 10 - 100, default: 90)</li> </ul>
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.
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.
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.
Max Session Bandwidth kbit/s Megapixel Slope	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.
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.
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.
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.
UDP Protocol	Specifies whether to use the UDP or the TCP protocol. The default is to use the UDP protocol. The setting takes effect when a user performs a session login-logout on the Horizon Agent machine on which the registry key exists. This setting does not apply to HTML Access, which always uses the TCP protocol.

## 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](#).

---

## Managing Special Unity Windows

You can use the **Unity Filter rule list** agent group policy setting to filter out unity windows, or map unity windows to a specific type, when using published applications. This feature is useful if you have a window display problem, such as a window that has a black background, or a drop-down window that is not sized correctly.

The **Unity Filter rule list** group policy setting is provided in the VMware View Agent Configuration ADMX template file (`vdm_agent.admx`), which is bundled in the `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyy.zip` file. For installation instructions, see [Add the ADMX Template Files to Active Directory](#).

When you enable the **Unity Filter rule list** group policy setting, you click **Show** and type a filtering rule in the **Value** text box. A filtering rule is composed of characteristics and actions. If you specify the map action, you must also include a type. The following table lists the characteristics, actions, and types that you can use in filtering rules.

**Table 5-31. Unity Filter Rule Characteristics, Actions, and Types**

Characteristics	Actions	Types
classname, company, product, major, minor, build, revision, style	block, map	normal, panel, dialog, tooltip, splash, toolbar, dock, desktop, widget, combobox, startscreen, sidepanel, taskbar, metrofullscreen, metroocked

The Windows class name is usually the preferred characteristic, for example, `classname=CustomClassName`. To further refine the filtering of windows with similar class names, you can use the `style` characteristic which lets you apply rules based on Microsoft window styles. The `company`, `product`, `major`, `minor`, `build`, and `revision` characteristics are provided in case you must limit rules to a specific product. You can find the values for these characteristics in the **Properties** window of an executable file.

The following rules apply to characteristic values:

- With the exception of `classname` and `style`, the values for these characteristics must be an exact case-sensitive match, including any special characters. If you provide multiple characteristics, all the values must match for the rule to apply to the window.
- The `classname` characteristic supports regular expression (regex) matches.
- In addition to exact case-sensitive matches, the `style` characteristic supports the " | " OR operator.

To specify an action, you type `action=value`, for example, `action=block`. The `block` action tells Horizon Agent not to show the window on the client. Use the `block` action when a window appears too large or interferes with normal window focus behavior on the client.

The `map` action, for example, `action=map`, tells Horizon Agent to treat the window as a certain hard-coded type. To specify the type, you must include `type=value` in the rule, for example, `type=normal`. Because determining if a window is mapped to the wrong type is difficult, mapping a window to a type is necessary only if VMware Support instructs you to do so.

## Filtering Rule Examples

The following filtering rule blocks all windows that have the class name `MyClassName`.

```
classname=MyClassName;action=block
```

The following filtering rule blocks all windows from the product named `MyProduct`.

```
product=MyProduct;action=block
```

The following filtering rule maps a custom class to the combo box type.

```
classname=MyClassName;action=map;type=combobox
```



The following filtering rule uses regex matching to block all classes containing the prefix HwndWrapper in their name, such as HwndWrapper1, HwndWrapper123, and HwndWrapper[Sod.exe;;1cc83874-f028-4d07-af82-3213d1ce7815].

```
classname=HwndWrapper.*;action=block
```

The following filtering rule blocks all windows with a style of either WS\_MINIMIZEBOX or WS\_MAXIMIZEBOX.

```
style=WS_MINIMIZEBOX | WS_MAXIMIZEBOX;action=block
```

---

**Note** The **Unity Filter rule list** group policy setting has a lower priority than filtering rules that are specified in a file in the %ProgramData%\VMware\RdeServer\Unity Filters directory on the RDS host.

---

## Active Directory Group Policy Example

One way to implement Active Directory group policies in Horizon 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 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 environment is different, you might need to perform different steps to meet your organization's specific needs.

---

### Create an OU for Horizon 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 machines. You might create one OU for your entire Horizon 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 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 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 machine in the right panel and select **Move**.
- c Select the OU and click **OK**.

The Horizon machine appears in the right pane when you select the OU.

**What to do next**

Create GPOs for Horizon group policies.

## Create GPOs for Horizon Group Policies

Create GPOs to contain group policies for Horizon components and location-based printing and link them to the OU for your Horizon machines.

**Prerequisites**

- Create an OU for your Horizon 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 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 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 machines and click **OK**.

The Horizon 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 ADMX Template File to a GPO

To apply Horizon component group policy settings to your desktops and applications, add their ADMX template files to GPOs.

### Prerequisites

- Create GPOs for the Horizon component group policy settings and link them to the OU that contains your Horizon 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 VMware Horizon 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 download, which includes the GPO Bundle.

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

- 2 Unzip the `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyyy.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 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 component group policy settings and link them to the OU that contains your Horizon 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 **Configure user Group Policy loopback processing mode**.
- 5 Select **Enabled** and then select a loopback processing mode from the **Mode** drop-down menu.

Option	Action
<b>Merge</b>	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.
<b>Replace</b>	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.

# Setting Desktop Policies with Start Session Scripts

# 6

With start session scripts, you can configure specific Horizon desktop settings before a desktop session starts based on information received from Horizon Client and Horizon Connection Server.

For example, you can use a start session script to configure desktop policies based on client device and user location instead of setting up multiple desktop pools that have different desktop policies. A start session script can enable mapped drives, clipboard redirection, and other desktop features for a user who has an IP address in your organization's internal domain, but disallow these features for a user who has an IP address in an external domain.

This chapter includes the following topics:

- [Obtaining Input Data for a Start Session Script](#)
- [Best Practices for Using Start Session Scripts](#)
- [Preparing a Horizon Desktop to Use a Start Session Script](#)
- [Sample Start Session Scripts](#)

## Obtaining Input Data for a Start Session Script

Start session scripts cannot run interactively. A start session script runs in an environment created by Horizon and must obtain its input data from that environment.

Start session scripts gather input data from environment variables on the client computer. Start session environment variables have the prefix `VDM_StartSession_`. For example, the start session environment variable that contains the client system's IP address is `VDM_StartSession_IP_Address`. You must ensure that a start session script validates the existence of any environment variable that it uses.

For a list of variables similar to start session environment variables, see [Client System Information Sent to Remote Desktops](#).

## Best Practices for Using Start Session Scripts

Follow these best practices when using start session scripts.

## When to Use Start Session Scripts

Use start session scripts only if you need to configure desktop policies before a session starts.

As a best practice, use the Horizon Agent `CommandsToRunOnConnect` and `CommandsToRunOnReconnect` group policy settings to run command scripts after a desktop session is connected or reconnected. Running scripts within a desktop session, rather than using start session scripts, satisfies most use cases.

For more information, see [Running Commands on Horizon Desktops](#).

## Managing Start Session Timeouts

Make sure your start session scripts run quickly.

If you set the `WaitScriptsOnStartSession` value in the Windows registry, your start session script must finish running before Horizon Agent can respond to the `StartSession` message that Horizon Connection Server sends. A long-running script is likely to cause the `StartSession` request to time out.

If a timeout occurs and the pool uses floating assignments, Connection Server tries to connect the user to another virtual machine. If a timeout occurs and no virtual machine is available, Connection Server rejects the user's connection request.

As a best practice, set a hard timeout for the script host operation so that a specific error can be returned if a script runs too long.

## Making Start Session Scripts Accessible

The path where you configure your start session scripts must be accessible only to the SYSTEM account and to local administrators. Set the ACL for the base key to be accessible to these accounts only.

As a best practice, place start session scripts in the `View_Agent_install_path\scripts` directory, for example:

```
%ProgramFiles%\VMware\VMware View\Agent\scripts\sample.vbs
```

By default, this directory is accessible only by the SYSTEM and administrator accounts.

## Preparing a Horizon Desktop to Use a Start Session Script

To prepare a Horizon desktop to use a start session script, you must enable the VMware Horizon View Script Host service and add entries in the Windows registry.

You must configure all Horizon desktops that need to run start session scripts. Horizon does not provide a mechanism to propagate registry changes, VMware Horizon View Script Host service configuration changes, and start session scripts to multiple Horizon desktop virtual machines.

## Enable the VMware Horizon View Script Host Service

You must enable the VMware Horizon View Script Host service on each Horizon desktop virtual machine where you want Horizon to run a start session script. The VMware Horizon View Script Host service is disabled by default.

When you configure the VMware Horizon View Script Host service, you can optionally specify the user account under which the start session script runs. Start session scripts run in the context of the VMware Horizon View Script Host service. By default, the VMware View Host Script service is configured to run as the SYSTEM user.

---

**Important** Start session scripts are run outside a desktop user session and not by the desktop user account. Information is sent directly from the client computer within a script running as the SYSTEM user.

---

### Procedure

- 1 Log in to the Horizon desktop virtual machine.
- 2 At the command prompt, type `services.msc` to start the Windows Services tool.
- 3 In the details pane, right-click the VMware Horizon View Script Host service entry and select **Properties**.
- 4 On the **General** tab, select **Automatic** from the **Startup type** drop-down menu.
- 5 (Optional) If you do not want the local System account to run the start session script, select the **Log On** tab, select **This account**, and type the user name and password of the account to run the start session script.
- 6 Click **OK** and exit the Windows Services tool.

## Add Windows Registry Entries for a Start Session Script

You must add Windows registry entries on each Horizon desktop virtual machine where you want Horizon to run a start session script.

### Prerequisites

- Verify that the path where you configured your start session scripts is accessible only to the SYSTEM account and local administrators. For more information, see [Best Practices for Using Start Session Scripts](#).
- Make sure your start session scripts run quickly. If you set the `WaitScriptsOnStartSession` value in the Windows registry, your start session script must finish running before Horizon Agent can respond to the `StartSession` message that Horizon Connection Server sends. For more information, see [Best Practices for Using Start Session Scripts](#).

### Procedure

- 1 Log in to the Horizon desktop virtual machine.
- 2 At the command prompt, type `regedit` to start the Windows Registry Editor.

**3** In the registry, navigate to HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents.

**4** Add the path to the start session script to the registry.

a In the navigation area, right-click ScriptEvents, select **New > Key**, and create a key named StartSession.

b In the navigation area, right-click StartSession, select **New > String Value**, and create a string value that identifies the start session script to run, for example, SampleScript.

To run more than one start session script, create a string value entry for each script under the StartSession key. You cannot specify the order in which these scripts run. If the scripts must run in a particular order, invoke them from a single control script.

c In the topic area, right-click the entry for the new string value and select **Modify**.

d In the **Value data** text box, type the command line that invokes the start session script and click **OK**.

Type the full path of the start session script and any files that it requires.

**5** Add and enable a start session value in the registry.

a Navigate to HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration.

b (Optional) If the Configuration key does not exist, right-click **Agent**, select **New > Key**, and create the key.

c In the navigation area, right-click Configuration, select **New > DWORD (32 bit) Value**, and type RunScriptsOnStartSession.

d In the topic area, right-click the entry for the new DWORD value and select **Modify**.

e In the **Value data** text box, type 1 to enable start session scripting and click **OK**.

You can type 0 to disable this feature. The default value is 0.

f (Optional) To delay the StartSession response by Horizon Agent, add a second DWORD value to the Configuration key called WaitScriptsOnStartSession.

A WaitScriptsOnStartSession data value of 1 causes Horizon Agent to delay sending a StartSession response and fail if the scripts do not complete. A value of 0 means that Horizon Agent does not wait for the scripts to complete or check script exit codes before sending the StartSession response. The default value is 0.



- 6 Set a registry value to specify timeout values in seconds rather than minutes to prevent scripts from timing out.

Setting this timeout value in seconds enables you to configure the VMware View Script Host service timeout value in seconds. For example, if you set the VMware View Script Host service timeout to 30 seconds, you can ensure that a start session script either finishes running or times out before a Connection Server timeout occurs.

- a Navigate to HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents.
  - b Add a DWORD value called TimeoutsInMinutes.
  - c Set a data value of 0.
- 7 (Optional) To enable the VMware View Script Host service to time out the start session script, set a timeout value.
    - a Navigate to HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents\StartSession.
    - b In the topic area, right-click the Default (@) key and select **Modify**.
    - c In the **Value data** text box, type the timeout value and click **OK**.
 

A value of 0 means that no timeout is set.
  - 8 Exit the Registry Editor and restart the system.

## Sample Start Session Scripts

These sample start session scripts illustrate how to write environment variables to a file, test the timeout functionality, and test a non-zero exit code.

The following sample Visual Basic script writes all the environment variables provided to the script into a file. You can use this sample script to see example data in your own environment. You might save this script as C:\sample.vbs.

```
Option Explicit
Dim WshShell, FSO, outFile, strOutputFile, objUserEnv, strEnv

strOutputFile = "c:\setvars.txt"

Set FSO = CreateObject("Scripting.FileSystemObject")
Set outFile = FSO.CreateTextFile(strOutputFile, TRUE)
outFile.WriteLine("Script was called at (" & Now & ")")

Set WshShell = CreateObject( "WScript.Shell" )
Set objUserEnv = WshShell.Environment("PROCESS")
For Each strEnv In objUserEnv
outFile.WriteLine(strEnv)
Next

outFile.Close
```

The following sample script tests the timeout functionality.

```
Option Explicit  
WScript.Sleep 60000
```

The following sample script tests a non-zero exit code.

```
Option Explicit  
WScript.Quit 2
```

# Examining PCoIP Session Statistics with WMI

# 7

You can use Windows Management Instrumentation (WMI) to examine performance statistics for a PCoIP session by using any of the supported programming interfaces, including C#, C++, PowerShell, VBScript, VB .NET, and Windows Management Instrumentation Command-line (WMIC).

You can also use the Microsoft WMI Code Creator tool to generate VBScript, C#, and VB .NET code that accesses the PCoIP performance counters. For more information about WMI, WMIC, and the WMI Code Creator tool, go to <http://technet.microsoft.com/en-us/library/bb742610.aspx>.

This chapter includes the following topics:

- [Using PCoIP Session Statistics](#)
- [General PCoIP Session Statistics](#)
- [PCoIP Audio Statistics](#)
- [PCoIP Imaging Statistics](#)
- [PCoIP Network Statistics](#)
- [PCoIP USB Statistics](#)
- [Examples of Using PowerShell cmdlets to Examine PCoIP Statistics](#)

## Using PCoIP Session Statistics

The WMI namespace for the PCoIP session statistics is `root\CIMV2`. The names of the statistics are suffixed with (Server) or (Client), according to whether the statistic is recorded on the PCoIP server or PCoIP client.

You can use Windows Performance Monitor (PerfMon) with the counters to calculate averages over a specified sampling period. You must have administrator privileges to access the performance counters remotely.

All statistics are reset to 0 when a PCoIP session is closed. If the WMI `SessionDurationSeconds` property is a non-zero value and stays constant, the PCoIP server was forcefully ended or crashed. If the `SessionDurationSeconds` property changes from a non-zero value to 0, the PCoIP session is closed.

To avoid a division-by-zero error, verify that the denominator in the expressions for calculating bandwidth or packet-loss percentage does not evaluate to zero.

USB statistics are recorded for zero clients, but not for thin clients or software clients.

## General PCoIP Session Statistics

The WMI class name for PCoIP general session statistics is `Win32_PerfRawData_TeradiciPerf_PCoIPSessionGeneralStatistics`.

Table 7-1. General Session Statistics

WMI Property Name	Description
BytesReceived	Total number of bytes of PCoIP data that have been received since the PCoIP session started.
BytesSent	Total number of bytes of PCoIP data that have been transmitted since the PCoIP session started.
PacketsReceived	Total number of packets that have been received successfully since the PCoIP session started. Not all packets are the same size.
PacketsSent	Total number of packets that have been transmitted since the PCoIP session started. Not all packets are the same size.
RXPacketsLost	Total number of received packets that have been lost since the PCoIP session started.
SessionDurationSeconds	Total number of seconds that the PCoIP Session has been open.
TXPacketsLost	Total number of transmitted packets that have been lost since the PCoIP session started.

### Calculating Bandwidth for Received PCoIP Data

To calculate the bandwidth in kilobits per second for received PCoIP data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{BytesReceived}[t_2] - \text{BytesReceived}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

### Calculating Bandwidth for Transmitted PCoIP Data

To calculate the bandwidth in kilobits per second for transmitted PCoIP data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{BytesSent}[t_2] - \text{BytesSent}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

### Calculating Packet Loss for Received PCoIP Data

To calculate the percentage of received packets that are lost, use the following formula.

$$100 / (1 + ((\text{PacketsReceived}[t_2] - \text{PacketsReceived}[t_1]) / (\text{RXPacketsLost}[t_2] - \text{RXPacketsLost}[t_1])))$$

## Calculating Packet Loss for Transmitted PCoIP Data

To calculate the percentage of transmitted packets that are lost, use the following formula.

$$100 * (\text{TXPacketsLost}[t2] - \text{TXPacketsLost}[t1]) / (\text{PacketsSent}[t2] - \text{PacketsSent}[t1])$$

## PCoIP Audio Statistics

The WMI class name for PCoIP audio statistics is `Win32_PerfRawData_TeradiciPerf_PCoIPSessionAudioStatistics`.

**Note** Audio statistics do not include audio data that is carried within USB data.

Table 7-2. PCoIP Audio Statistics

WMI Property Name	Description
AudioBytesReceived	Total number of bytes of audio data that have been received since the PCoIP session started.
AudioBytesSent	Total number of bytes of audio data that have been sent since the PCoIP session started.
AudioRXBwKbitPersec	Bandwidth for ingoing audio packets averaged over the sampling period, in seconds.
AudioTXBwKbitPersec	Bandwidth for outgoing audio packets averaged over the sampling period, in seconds.
AudioTXBWLimitKbitPersec	Transmission bandwidth limit in kilobits per second for outgoing audio packets. The limit is defined by a GPO setting.

## Calculating Bandwidth for Received Audio Data

To calculate the bandwidth in kilobits per second for received audio data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{AudioBytesReceived}[t2] - \text{AudioBytesReceived}[t1]) * 8 / (1024 * (t2 - t1))$$

Do not use `AudioRXBwKbitPersec` for this calculation.

## Calculating Bandwidth for Transmitted Audio Data

To calculate the bandwidth in kilobits per second for transmitted audio data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{AudioBytesSent}[t2] - \text{AudioBytesSent}[t1]) * 8 / (1024 * (t2 - t1))$$

Do not use `AudioTXBwKbitPersec` for this calculation.

## PCoIP Imaging Statistics

The WMI class name for PCoIP imaging statistics is `Win32_PerfRawData_TeradiciPerf_PCoIPSessionImagingStatistics`.

Table 7-3. PCoIP Imaging Statistics

WMI Property Name	Description
<code>ImagingBytesReceived</code>	Total number of bytes of imaging data that have been received since the PCoIP session started.
<code>ImagingBytesSent</code>	Total number of bytes of imaging data that have been transmitted since the PCoIP session started.
<code>ImagingDecoderCapabilitykbitPersec</code>	Estimated processing capability of the imaging decoder in kilobits per second. This statistic is updated once per second.
<code>ImagingEncodedFramesPersec</code>	Number of imaging frames that were encoded over a one-second sampling period.
<code>ImagingActiveMinimumQuality</code>	Lowest encoded quality value on a scale from 0 to 100. This statistic is updated once per second. This counter does not correspond to the GPO setting for minimum quality.
<code>ImagingRXBkbitPersec</code>	Bandwidth for incoming imaging packets averaged over the sampling period, in seconds.
<code>ImagingTXBkbitPersec</code>	Bandwidth for outgoing imaging packets averaged over the sampling period, in seconds.

### Calculating Bandwidth for Received Imaging Data

To calculate the bandwidth in kilobits per second for received imaging data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{ImagingBytesReceived}[t_2] - \text{ImagingBytesReceived}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Do not use `ImagingRXBkbitPersec` for the calculation.

### Calculating Bandwidth for Transmitted Imaging Data

To calculate the bandwidth in kilobits per second for transmitted imaging data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{ImagingBytesSent}[t_2] - \text{ImagingBytesSent}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Do not use `ImagingTXBkbitPersec` for the calculation.

## PCoIP Network Statistics

The WMI class name for PCoIP network statistics is `Win32_PerfRawData_TeradiciPerf_PCoIPSessionNetworkStatistics`.

**Table 7-4. PCoIP Network Statistics**

WMI Property Name	Description
RoundTripLatencymms	Round trip latency in milliseconds between the PCoIP server and the PCoIP client.
RXBWkbitPersec	Overall bandwidth for incoming PCoIP packets averaged over the sampling period, in seconds.
RXBWPeakkbitPersec	Peak bandwidth in kilobits per second for incoming PCoIP packets over a one-second sampling period.
RXPacketLossPercent	Percentage of received packets lost during a sampling period.
TXBWkbitPersec	Overall bandwidth for outgoing PCoIP packets averaged over the sampling period, in seconds.
TXBWActiveLimitkbitPersec	Estimated available network bandwidth in kilobits per second. This statistic is updated once per second.
TXBWLimitkbitPersec	Transmission bandwidth limit in kilobits per second for outgoing packets. The limit is the minimum of the following values. <ul style="list-style-type: none"> <li>■ GPO bandwidth limit for the PCoIP client</li> <li>■ GPO bandwidth limit for the PCoIP server</li> <li>■ Bandwidth limit for the local network connection</li> <li>■ Negotiated bandwidth limit for the Zero Client firmware based on encryption limits</li> </ul>
TXPacketLossPercent	Percentage of transmitted packets lost during a sampling period.

### Calculating Bandwidth for Received Network Data

To calculate the bandwidth in kilobits per second for received data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{BytesReceived}[t_2] - \text{BytesReceived}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Do not use `RXBWkbitPersec` for the calculation.

### Calculating Bandwidth for Transmitted Network Data

To calculate the bandwidth in kilobits per second for transmitted data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{BytesSent}[t_2] - \text{BytesSent}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Do not use TXBWkbitPersec for the calculation.

## Calculating Packet Loss for Received Network Data

To calculate the packet loss in percentage for received data over the time interval from time t1 to time t2, use the following formula.

```
PacketsReceived during interval = (PacketsReceived[t2]-PacketsReceived[t1])
```

```
RXPacketsLost during interval = (RXPacketsLost[t2]-RXPacketsLost[t1])
```

```
RXPacketsLost % = RXPacketsLost during interval /  
(RXPacketsLost during interval + PacketsReceived during interval) * 100
```

Do not use RXPacketLostPercent or RXPacketLostPercent\_Base for the calculation.

## Calculating Packet Loss for Transmitted Network Data

To calculate the packet loss in percentage for transmitted data over the time interval from time t1 to time t2, use the following formula.

```
PacketsSent during interval = (PacketsSent[t2]-PacketsSent[t1])
```

```
TXPacketsLost during interval = (TXPacketsLost[t2]-TXPacketsLost[t1])
```

```
TXPacketsLost % = TXPacketsLost during interval /  
(TXPacketsLost during interval + PacketsSent during interval) * 100
```

Do not use TXPacketLostPercent or TXPacketLostPercent\_Base for the calculation.

Use this formula to prevent the packet loss percent from becoming greater than 100 percent.

This calculation is required because PacketsLost and PacketsSent are asynchronous.

## PCoIP USB Statistics

The WMI class name for PCoIP USB statistics is Win32\_PerfRawData\_TeradiciPerf\_PCoIPSessionUSBStatistics.

Table 7-5. PCoIP USB Statistics

WMI Property Name	Description
USBBytesReceived	Total number of bytes of USB data that have been received since the PCoIP session started.
USBBytesSent	Total number of bytes of USB data that have been transmitted since the PCoIP session started.
USBRXBWkbitPersec	Bandwidth for incoming USB packets averaged over the sampling period, in seconds.
USBTXBWkbitPersec	Bandwidth for outgoing USB packets averaged over the sampling period, in seconds.



## Calculating Bandwidth for Received USB Data

To calculate the bandwidth in kilobits per second for received USB data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{USBBytesReceived}[t_2] - \text{USBBytesReceived}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Do not use `USBRXBkbitPersec` for the calculation.

## Calculating Bandwidth for Transmitted USB Data

To calculate the bandwidth in kilobits per second for transmitted USB data over the time interval from time  $t_1$  to time  $t_2$ , use the following formula.

$$(\text{USBBytesSent}[t_2] - \text{USBBytesSent}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Do not use `USBTXBkbitPersec` for the calculation.

## Examples of Using PowerShell cmdlets to Examine PCoIP Statistics

You can use PowerShell cmdlets to examine PCoIP statistics.

In the following example, the `Get-WmiObject` cmdlet retrieves the PCoIP network statistics for the client `cm-02`.

```
Get-WmiObject -namespace "root\cimv2" -computername cm-02 -class
Win32_PerfRawData_TeradiciPerf_PCoIPSessionNetworkStatistics
```

In the following example, the `Get-WmiObject` cmdlet retrieves the PCoIP general session statistics for desktop `dt-03` if any transmitted packets have been lost.

```
Get-WmiObject -namespace "root\cimv2" -computername desktop-03 -query "select * from
Win32_PerfRawData_TeradiciPerf_PCoIPSessionGeneralStatistics where TXPacketsLost > 0"
```