Horizon Client and Agent Security

Horizon Client 3.x/4.x/5.x and View Agent 6.2.x/Horizon Agent 7.x

DEC 2019

VMware Horizon 7 7.11

vmware®

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

Horizon Client and Agent Security

Horizon Client and Agent Security provides a concise reference to the security features of VMware Horizon® Client™ and Horizon Agent (for Horizon 7) or VMware View Agent® (for Horizon 6). This guide is a companion to the *Horizon 7 Security* guide, which is produced for every major and minor version of VMware Horizon™ 6 and Horizon 7. The *Horizon Client and Agent Security* guide is updated quarterly, with the quarterly releases of the client and agent software.

Horizon Client is the application that end users launch from their client devices in order to connect to a remote application or desktop. View Agent (for Horizon 6) or Horizon Agent (for Horizon 7) is the agent software that runs in the operating system of the remote desktop or Microsoft RDS host that provides remote applications. This guide includes the following information:

- Required system login accounts. Log-on ID of accounts created during system install/bootstrap and instructions on how to change defaults.
- Configuration options and settings that have security implications.
- Resources that must be protected, such as security-relevant configuration files and passwords, and the recommended access controls for secure operation.
- Location of log files and their purpose.
- Privileges assigned to service users.
- External interfaces, ports, and services that must be open or enabled for the correct operation of the client and agent.
- Information on how customers can obtain and apply the latest security update or patch.

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Horizon 6 or Horizon 7, including the client and agent.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

External Ports

1

For proper operation of the product, and depending on which features you want to use, various ports must be opened so that the clients and agent on remote desktops can communicate with each other.

This chapter includes the following topics:

Understanding Communications Protocols

Horizon 6 and Horizon 7 components exchange messages by using several different protocols.

Table 1-1. Default Ports lists the default ports that are used by each protocol. If necessary, to comply with organization policies or to avoid contention, you can change which port numbers are used.

Table 1-1. Default Ports

Protocol	Port
JMS	TCP port 4001 TCP port 4002
HTTP	TCP port 80
HTTPS	TCP port 443
MMR/CDR	For multimedia redirection and client drive redirection, TCP port 9427
RDP	TCP port 3389
PCoIP	TCP port 4172 UDP ports 4172, 50002, 55000
USB redirection	TCP port 32111. This port is also used for time zone synchronization.
VMware Blast Extreme	TCP ports 8443, 22443 UDP ports 443, 8443, 22443
HTML Access	TCP ports 8443, 22443

Firewall Rules for View Agent or Horizon Agent

The View Agent and Horizon Agent installers optionally configure Windows firewall rules on remote desktops and RDS hosts to open the default network ports. Ports are incoming unless otherwise noted.

The View Agent and Horizon Agent installers configure the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389.

If you instruct the View Agent or Horizon Agent installer not to enable Remote Desktop support, it does not open ports 3389 and 32111, and you must open these ports manually.

If you change the RDP port number after installation, you must change the associated firewall rules. If you change a default port after installation, you must manually reconfigure Windows firewall rules to allow access on the updated port. See "Replacing Default Ports for View Services" in the *Horizon 7 Installation* document.

Windows firewall rules for View Agent or Horizon Agent on RDS hosts show a block of 256 contiguous UDP ports as open for inbound traffic. This block of ports is for VMware Blast internal use in View Agent or Horizon Agent. A special Microsoft-signed driver on RDS hosts blocks inbound traffic to these ports from external sources. This driver causes the Windows firewall to treat the ports as closed.

If you use a virtual machine template as a desktop source, firewall exceptions carry over to deployed desktops only if the template is a member of the desktop domain. You can use Microsoft group policy settings to manage local firewall exceptions. See the Microsoft Knowledge Base (KB) article 875357 for more information.

Table 1-2. TCP and UDP Ports Opened During View Agent or Horizon Agent Installation

Protocol	Ports
RDP	TCP port 3389
USB redirection and time zone synchronization	TCP port 32111
MMR (multimedia redirection) and CDR (client drive redirection)	TCP port 9427
PCoIP	For RDS hosts, PCoIP uses the following port numbers: TCP port 4172 and UDP port 4172 (bidirectional). For desktops, PCoIP uses port numbers chosen from a configurable range. By default, TCP ports 4172 to 4173 and UDP ports 4172 to 4182. The firewall rules for these do not specify port numbers but dynamically follow the ports opened by each PCoIP Server. The chosen port numbers are communicated to the client via the Connection Server.
VMware Blast	TCP port 22443 UDP port 22443 (bidirectional) **Note** UDP is not used on Linux desktops.
HTML Access	TCP port 22443

Table 1-2. TCP and UDP Ports Opened During View Agent or Horizon Agent Installation (continued)

Protocol	Ports
XDMCP	UDP 177 **Note** This port is opened for XDMCP access only at Linux desktops running Ubuntu 18.04. Firewall rules block all external host access to this port.
X11	TCP 6100 **Note** This port is opened for XServer access only at Linux desktops running Ubuntu 18.04. Firewall rules block all external host access to this port.

TCP and UDP Ports Used by Clients and Agents

View Agent (for Horizon 6), Horizon Agent (for Horizon 7), and Horizon Client use TCP and UDP ports for network access between each other and various server components.

Table 1-3. TCP and UDP Ports Used by View Agent or Horizon Agent

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	Microsoft RDP traffic to remote desktops if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR redirection and client drive redirection, if direct connections are used instead of tunnel connections. **Note** Not needed for client drive redirection when using VMware Blast.
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	USB redirection and time zone synchronization if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP and UDP	PCoIP if PCoIP Secure Gateway is not used. **Note** Because the source port varies, see the note below this table.
Horizon Client	*	Horizon Agent	22443	TCP and UDP	VMware Blast if direct connections are used instead of tunnel connections. **Note** UDP is not used on Linux desktops.
Browser	*	View Agent/ Horizon Agent	22443	TCP	HTML Access if direct connections are used instead of tunnel connections.
Security server, Connection Server, or Unified Access Gateway appliance	*	View Agent/ Horizon Agent	3389	TCP	Microsoft RDP traffic to remote desktops when tunnel connections are used.

Table 1-3. TCP and UDP Ports Used by View Agent or Horizon Agent (continued)

Source	Port	Target	Port	Protocol	Description
Security server, Connection Server, or Unified Access Gateway appliance	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR redirection and client drive redirection when tunnel connections are used.
Security server, Connection Server, or Unified Access Gateway appliance	*	View Agent/ Horizon Agent	32111	TCP	USB redirection and time zone synchronization when tunnel connections are used.
Security server, Connection Server, or Unified Access Gateway appliance	55000	View Agent/ Horizon Agent	4172	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
Security server, Connection Server, or Unified Access Gateway appliance	*	View Agent/ Horizon Agent	4172	TCP	PCoIP if PCoIP Secure Gateway is used.
Security server, Connection Server, or Unified Access Gateway appliance	*	Horizon Agent	22443	TCP and UDP	VMware Blast if Blast Secure Gateway is used. **Note** UDP is not used on Linux desktops.
Security server, Connection Server, or Unified Access Gateway appliance	*	View Agent/ Horizon Agent	22443	TCP	HTML Access if Blast Secure Gateway is used.
View Agent/Horizon Agent	*	Connection Server	4001, 4002	TCP	JMS SSL traffic.
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP, if PCoIP Secure Gateway is not used. **Note** Because the target port varies, see the note below this table.
View Agent/Horizon Agent	4172	Connection Server, security server, or Unified Access Gateway appliance	55000	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.

Note The UDP port number that agents use for PCoIP might change. If port 50002 is in use, the agent will pick 50003. If port 50003 is in use, the agent will pick port 50004, and so on. You must configure firewalls with ANY where an asterisk (*) is listed in the table.

Table 1-4. TCP and UDP Ports Used by Horizon Client

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	Connection Server, security server, or Unified Access Gateway appliance	443	TCP	HTTPS for logging in to Horizon 6 or Horizon 7. (This port is also used for tunnelling when tunnel connections are used.) **Note** Horizon Client 4.4 and later supports UDP port 443 (see below).
Horizon Client 4.4 or later	*	Unified Access Gateway appliance 2.9 or later	443	UDP	HTTPS for logging into Horizon 6 or Horizon 7, if Blast Secure Gateway is used and UDP Tunnel Server is enabled. (This port is also used for tunnelling when tunnel connections are used.)
Unified Access Gateway appliance 2.9 or later	443	Horizon Client 4.4 or later	*	UDP	HTTPS for logging into Horizon 6 or Horizon 7, if Blast Secure Gateway is used and UDP Tunnel Server is enabled. (This port is also used for tunnelling when tunnel connections are used.)
Horizon Client	*	View Agent/ Horizon Agent	22443	TCP	HTML Access and VMware Blast if Blast Secure Gateway is not used.
Horizon Client	*	Horizon Agent	22443	UDP	VMware Blast if Blast Secure Gateway is not used. **Note** Not used when connecting to Linux desktops.
Horizon Agent	22443	Horizon Client	*	UDP	VMware Blast if Blast Secure Gateway is not used. **Note** Not used when connecting to Linux desktops.
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	Microsoft RDP traffic to remote desktops if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR redirection and client drive redirection, if direct connections are used instead of tunnel connections. **Note** Not needed for CDR when using VMware Blast.
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	USB redirection and time zone synchronization if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP and UDP	PCoIP if PCoIP Secure Gateway is not used. **Note** Because the source port varies, see the note below this table.
Horizon Client	*	Connection Server, security server, or Unified Access Gateway appliance	4172	TCP and UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used. **Note** Because the source port varies, see the note below this table.

Table 1-4. TCP and UDP Ports Used by Horizon Client (continued)

Source	Port	Target	Port	Protocol	Description
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP if PCoIP Secure Gateway is not used. **Note** Because the target port varies, see the note below this table.
Security server, View Connection Server, or Unified Access Gateway appliance	4172	Horizon Client	*	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used. **Note** Because the target port varies, see the note below this table.
Horizon Client	*	Connection Server, security server, or Unified Access Gateway appliance	8443	TCP	HTML Access and VMware Blast if Blast Secure Gateway is used.
Horizon Client	*	Connection Server, security server, or Unified Access Gateway appliance	8443	UDP	VMware Blast if Blast Secure Gateway is used. **Note** Not used when connecting to a Linux desktop.
View Connection Server, security server, or Unified Access Gateway appliance	8443	Horizon Client	*	UDP	VMware Blast if Blast Secure Gateway is used. **Note** Not used when connecting to a Linux desktop.

Note The UDP port number that clients use for PCoIP and VMware Blast might change. If port 50002 is in use, the client chooses 50003. If port 50003 is in use, the client chooses port 50004, and so on. You must configure firewalls with ANY where an asterisk (*) is listed in the table.

Installed Services, Daemons, and Processes

2

When you run the client or agent installer, several components are installed.

This chapter includes the following topics:

Services Installed by the View Agent or Horizon Agent Installer on Windows Machines

The operation of remote desktops and applications depends on several Windows services.

Table 2-1. View Agent (for Horizon 6) or Horizon Agent (for Horizon 7) Services

Service Name	Startup Type	Description
VMware Blast	Automatic	Provides services for HTML Access and for using the VMware Blast Extreme protocol for connecting with native clients.
VMware Horizon View Agent	Automatic	Provides services for View Agent/Horizon Agent.
VMware Horizon View Composer Guest Agent Server	Automatic	Provides services if this virtual machine is part of a View Composer linked-clone desktop pool.
VMware Horizon View Persona Management	Automatic if the feature is enabled; otherwise Disabled	Provides services for the VMware Persona Management feature.
VMware Horizon View Script Host	Disabled	Provides support for running start session scripts, if any, to configure desktop security policies before a desktop session begins. Policies are based on the client device and the user's location.
VMware Netlink Supervisor Service	Automatic	To support the scanner redirection feature and the serial port redirection feature, provides monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Client Service	Automatic	(View Agent 6.0.2 and later) Provides services for the scanner redirection feature.

Table 2-1. View Agent (for Horizon 6) or Horizon Agent (for Horizon 7) Services (continued)

Service Name	Startup Type	Description
VMware Serial Com Client Service	Automatic	(View Agent 6.1.1 and later) Provides services for the serial port redirection feature.
VMware Snapshot Provider	Manual	Provides services for virtual machine snapshots, which are used for cloning.
VMware Tools	Automatic	Provides support for synchronizing objects between the host and guest operating systems, which enhances the performance of the virtual machines guest operating system and improves management of the virtual machine.
VMware USB Arbitration Service	Automatic	Enumerates the various USB devices connected to the client and determines which devices to connect to the client and which to connect to the remote desktop.
VMware View USB	Automatic	Provides services for the USB redirection feature.

Services Installed on the Windows Client

The operation of Horizon Client depends on several Windows services.

Table 2-2. Horizon Client Services

Service Name	Startup Type	Description
VMware Horizon Client	Automatic	Provides Horizon Client services.
VMware Netlink Supervisor Service	Automatic	To support the scanner redirection feature and the serial port redirection feature, provides monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Client Service	Automatic	(Horizon Client 3.2 and later) Provides services for the scanner redirection feature.
VMware Serial Com Client Service	Automatic	(Horizon Client 3.4 and later) Provides services for the serial port redirection feature.
VMware USB Arbitration Service	Automatic	Enumerates the various USB devices connected to the client and determines which devices to connect to the client and which to connect to the remote desktop.
VMware View USB	Automatic	(Horizon Client 4.3 and earlier) Provides services for the USB redirection feature. **Note** In Horizon Client 4.4 and later, this service is removed and the USBD service is moved to the `vmware-remotemks.exe` process.

Daemons Installed in Other Clients and the Linux Desktop

For security purposes, it is important to know whether any daemons or processes are installed by Horizon Client.

Table 2-3. Services, Processes, or Daemons Installed by Horizon Client, by Client Type

Type	Service, Process, or Daemon
Linux client	■ `vmware-usbarbitrator`, which numerates the various USB devices connected to the client and determines which devices to connect to the client and which to connect to the remote desktop. ■ `vmware-view-used`, which provides services for the USB redirection feature. **Note** These daemons start automatically if you click the **Register and start the service(s) after installation** check box during installation. These processes run as root.
Mac client	Horizon Client does not create any daemons.
Chrome OS client	Horizon Client runs in one Android process. Horizon Client does not create any daemons.
iOS client	Horizon Client does not create any daemons.
Android client	Horizon Client runs in one Android process. Horizon Client does not create any daemons.
Windows 10 UWP client	Horizon Client does not create or trigger any system services.
Windows Store client	Horizon Client does not create or trigger any system services.
Linux desktop	■ `StandaloneAgent`, which runs with root privileges and is started when the Linux system is up and running. `StandaloneAgent` communicate with Connection Server to perform remote desktop session management (sets up, tears down the session, updating the remote desktop status to the broker in Connection Server). ■ `VMwareBlastServer`, which is started by `StandaloneAgent` when a `StartSession` request is received from Connection Server. The `VMwareBlastServer` daemon runs with `vmwblast` (a system account created when Linux Agent is installed.) privilege. It communicates with `StandaloneAgent` through an internal `MKSControl` channel and communicates with Horizon Client by using the VMware Blast display protocol.

Resources to Secure

3

These resources include relevant configuration files, passwords, and access controls.

This chapter includes the following topics:

Implementing Best Practices to Secure Client Systems

Implement these best practices to secure client systems.

- Make sure that client systems are configured to go to sleep after a period of inactivity and require users to enter a password before the computer awakens.
- Require users to enter a username and password when starting client systems. Do not configure client systems to allow automatic logins.
- For Mac client systems, consider setting different passwords for the Keychain and the user account. When the passwords are different, users are prompted before the system enters any passwords on their behalf. Also consider turning on FileVault protection.

Configuration File Locations

Resources that must be protected include security-relevant configuration files.

Table 3-1. Location of Configuration Files, by Client Type

Type	Directory Path
Linux client	When Horizon Client starts up, configuration settings are processed from various locations in the following order: 1 `/etc/vmware/view-default-config` 2 `~/.vmware/view-preferences` 3 `/etc/vmware/view-mandatory-config` If a setting is defined in multiple locations, the value that is used is the value from the last file or command-line option read.
Windows client	The user settings that might include some private information are located in the following file: `C:\Users\`*`user-name`*`\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt`
Mac client	Some configuration files generated after Mac client startup. ■ `$HOME/Library/Preferences/com.vmware.horizon.plist` ■ `$HOME/Library/Preferences/com.vmware.vmrc.plist` ■ `$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist` ■ `/Library/Preferences/com.vmware.horizon.plist`
Chrome OS client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
iOS client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
Android client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
Windows 10 UWP Client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
Windows Store client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
View Agent or Horizon Agent (remote desktop with Windows operating system)	Security-related settings appear in the Windows Registry only.
Linux desktop	You can use a text editor to open the following configuration file and specify SSL-related settings. `/etc/vmware/viewagent-custom.conf`

Accounts

Client users must have accounts in Active Directory.

Horizon Client User Accounts

Configure user accounts in Active Directory for the users who have access to remote desktops and applications. The user accounts must be members of the Remote Desktop Users group if you plan to use the RDP protocol.

End users should not normally be Horizon administrators. If a Horizon administrator needs to verify the user experience, create and entitle a separate test account. On the desktop, Horizon end users should not be members of privileged groups such as Administrators because they will then be able to modify locked down configuration files and the Windows Registry.

System Accounts Created During Installation

No service user accounts are created on any type of client by the Horizon Client application. For the services created by Horizon Client for Windows, the log-on ID is Local System.

On the Mac client, on the first startup, the user must grant Local Admin access to start the USB and virtual printing (ThinPrint) services. After these services are started for the first time, the standard user has execution access for them. Similarly, on the Linux client, the `vmware-usbarbitrator` and `vmware-view-used` daemons start automatically if you click the **Register and start the service(s) after installation** check box during installation. These processes run as root.

No service user accounts are created by View Agent or Horizon Agent on Windows desktops. On Linux desktops a system account, `vmwblast`, is created. On Linux desktops, the `StandaloneAgent` daemon runs with root privileges and the `VmwareBlastServer` daemon runs with `vmwblast` privileges.

Security Settings for the Client and Agent

4

Several client and agent settings are available for adjusting the security of the configuration. You can access the settings for the remote desktop and Windows clients by using group policy objects or by editing Windows registry settings.

For configuration settings related to log collection, see Chapter 6 Client and Agent Log File Locations. For configuration settings related to security protocols and cipher suites, see Chapter 5 Configuring Security Protocols and Cipher Suites.

This chapter includes the following topics:

Configuring Certificate Checking

Administrators can configure the certificate verification mode so that, for example, full verification is always performed. Administrators can also configure whether end users are allowed to choose whether client connections are rejected if any or some server certificate checks fail.

Certificate checking occurs for SSL/TLS connections between Connection Server instances and Horizon Client. Administrators can configure the verification mode to use one of the following strategies:

- End users are allowed to choose the verification mode. The rest of this list describes the three verification modes.
- (No verification) No certificate checks are performed.
- (Warn) End users are warned if a self-signed certificate is being presented by the server. Users can choose whether or not to allow this type of connection.

- (Full security) Full verification is performed and connections that do not pass full verification are rejected.

Certificate verification includes the following checks:

- Has the certificate been revoked?
- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects Horizon Client to a server that has a certificate that does not match the host name entered in Horizon Client. Another reason a mismatch can occur is if you enter an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA.

  To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

If you use an SSL proxy server to inspect traffic sent from the client environment to the Internet, you can enable certificate checking for secondary connections through an SSL proxy server. You can also configure VMware Blast connections to use a proxy server. These features are supported with Horizon Client 5.2 and later for Windows, Mac, and Linux.

For information about how to configure certificate checking and SSL proxy server use for a specific type of client, see the Horizon Client installation and setup document for that client. These documents also contain information about using self-signed certificates.

Security-Related Settings in the View Agent and Horizon Agent Configuration Templates

Security-related settings are provided in ADM and ADMX template files for View Agent and Horizon Agent. The ADM and ADMX template files are named `vdm_agent.adm` and `vdm_agent.admx`. Unless noted otherwise, the settings include only a Computer Configuration setting.

Security Settings are stored in the registry on the guest machine under `HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration`.

Table 4-1. Security-Related Settings in the View Agent (for Horizon 6) or Horizon Agent (for Horizon 7) Configuration Template

Setting	Description
`AllowDirectRDP`	Determines whether clients other than Horizon Client devices can connect directly to remote desktops with RDP. When this setting is disabled, the agent permits only Horizon-managed connections through Horizon Client. When connecting to a remote desktop from Horizon Client for Mac, do not disable the `AllowDirectRDP` setting. If this setting is disabled, the connection fails with an `Access is denied` error. By default, while a user is logged in to a remote desktop session, you can use RDP to connect to the virtual machine. The RDP connection terminates the remote desktop session, and the user's unsaved data and settings might be lost. The user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, disable the `AllowDirectRDP` setting. **Important** The Windows Remote Desktop Services service must be running on the guest operating system of each desktop. You can use this setting to prevent users from making direct RDP connections to their desktops. This setting is enabled by default. The equivalent Windows Registry value is `AllowDirectRDP`.
`AllowSingleSignon`	Determines whether single sign-on (SSO) is used to connect users to desktops and applications. When this setting is enabled, users are required to enter their credentials only once, when they log in to the server. When this setting is disabled, users must reauthenticate when the remote connection is made. This setting is enabled by default. The equivalent Windows Registry value is `AllowSingleSignon`.
`CommandsToRunOnConnect`	Specifies a list of commands or command scripts to be run when a session is connected for the first time. No list is specified by default. The equivalent Windows Registry value is `CommandsToRunOnConnect`.
`CommandsToRunOnDisconnect`	Specifies a list of commands or command scripts to be run when a session is disconnected. No list is specified by default. The equivalent Windows Registry value is `CommandsToRunOnReconnect`.
`CommandsToRunOnReconnect`	Specifies a list of commands or command scripts to be run when a session is reconnected after a disconnect. No list is specified by default. The equivalent Windows Registry value is `CommandsToRunOnDisconnect`.

Table 4-1. Security-Related Settings in the View Agent (for Horizon 6) or Horizon Agent (for Horizon 7) Configuration Template (continued)

Setting	Description
`ConnectionTicketTimeout`	Specifies the amount of time in seconds that the Horizon connection ticket is valid. Horizon Client devices use a connection ticket for verification and single sign-on when connecting to the agent. For security reasons, a connection ticket is valid for a limited amount of time. When a user connects to a remote desktop, authentication must take place within the connection ticket timeout period or the session times out. If this setting is not configured, the default timeout period is 900 seconds. The equivalent Windows Registry value is `VdmConnectionTicketTimeout`.
`CredentialFilterExceptions`	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. No list is specified by default. The equivalent Windows Registry value is `CredentialFilterExceptions`.

For more information about these settings and their security implications, see the *View Administration* document.

Setting Options in Configuration Files on a Linux Desktop

You can configure certain options by adding entries to the files `/etc/vmware/config` or `/etc/vmware/viewagent-custom.conf`.

During the installation of Horizon Agent, the installer copies two configuration template files, `config.template` and `viewagent-custom.conf.template`, to `/etc/vmware`. In addition, if `/etc/vmware/config` and `/etc/vmware/viewagent-custom.conf` do not exist, the installer copies `config.template` to `config` and `viewagent-custom.conf.template` to `viewagent-custom.conf`. In the template files, all the configuration options are listed and documented. To set an option, simply remove the comment and change the value as appropriate.

For example, the following line in `/etc/vmware/config` enables the build to lossless PNG mode.

```
RemoteDisplay.buildToPNG=TRUE
```

After you make configuration changes, reboot Linux for the changes to take effect.

Configuration Options in /etc/vmware/config

VMwareBlastServer and its related plug-ins use the configuration file `/etc/vmware/config`.

Note The following table includes description for each agent-enforced policy setting for USB in the Horizon Agent configuration file. Horizon Agent uses the settings to decide if a USB can be forwarded to the host machine. Horizon Agent also passes the settings to Horizon Client for interpretation and enforcement. The enforcement is based on whether you specify the merge **`(m)`** modifier to apply the Horizon Agent filter policy setting in addition to the Horizon Client filter policy setting, or override the **`(o)`** modifier to use the Horizon Agent filter policy setting instead of the Horizon Client filter policy setting.

Table 4-2. Configuration Options in `/etc/vmware/config`

Option	Value/Format	Default	Description
Clipboard.Direction	`0`, `1`, `2`, or `3`	`2`	Use this option to specify the clipboard redirection policy. Valid values are as follows: ■ 0 - Disable clipboard redirection. ■ 1 - Enable clipboard redirection in both directions. ■ 2 - Enable clipboard redirection from the client to the remote desktop only. ■ 3 - Enable clipboard redirection from the remote desktop to the client only.
RemoteDisplay.allowAudio	`true` or `false`	`true`	Set this option to enable/disable audio out.
RemoteDisplay.allowH264	`true` or `false`	`true`	Set this option to enable or disable H.264 encoding.
RemoteDisplay.buildToPNG	`true` or `false`	`false`	Graphic applications, especially graphic design applications, require pixel-exact rendering of images in the client display of a Linux desktop. You can configure the build to lossless PNG mode for images and video playback that are generated on a Linux desktop and rendered on the client device. This feature uses additional bandwidth between the client and the ESXi host. Enabling this option disables the H.264 encoding.
RemoteDisplay.enableNetworkContinuity	`true` or `false`	`true`	Set this option to enable or disable the Network Continuity feature in the Horizon Agent for Linux.
RemoteDisplay.enableNetworkIntelligence	`true` or `false`	`true`	Set this option to enable or disable the Network Intelligence feature in Horizon Agent for Linux.
RemoteDisplay.enableStats	`true` or `false`	`false`	Enables or disables the VMware Blast display protocol statistics in mks log, such as bandwidth, FPS, RTT, and so on.
RemoteDisplay.enableUDP	`true` or `false`	`true`	Set this option to enable or disable UDP protocol support in Horizon Agent for Linux.
RemoteDisplay.maxBandwidthKbps	An integer	1000000	Specifies the maximum bandwidth in kilobits per second (kbps) for a VMware Blast session. The bandwidth includes all imaging, audio, virtual channel, and VMware Blast control traffic. Valid value must be less than 4 Gbps (4096000).
RemoteDisplay.minBandwidthKbps	An integer	256	Specifies the minimum bandwidth in kilobits per second (kbps) for a VMware Blast session. The bandwidth includes all imaging, audio, virtual channel, and VMware Blast control traffic.
RemoteDisplay.maxFPS	An integer	30	Specifies the maximum rate of screen updates. Use this setting to manage the average bandwidth that users consume. Valid value must be between 3 and 60. The default is 30 updates per second.
RemoteDisplay.maxQualityJPEG	available range of values: 1–100	90	Specifies the image quality of the desktop display for JPEG/PNG encoding. The high-quality settings are for areas of the screen that are more static, resulting in a better image quality.

Table 4-2. Configuration Options in `/etc/vmware/config` (continued)

Option	Value/Format	Default	Description
RemoteDisplay.midQualityJPEG	available range of values: 1–100	35	Specifies the image quality of the desktop display for JPEG/PNG encoding. Use to set the medium-quality settings of the desktop display.
RemoteDisplay.minQualityJPEG	available range of values: 1–100	25	Specifies the image quality of the desktop display for JPEG/PNG encoding. The low-quality settings are for areas of the screen that change often, for example, when scrolling occurs.
RemoteDisplay.qpmaxH264	available range of values: 0–51	36	Use this option to set the H264minQP quantization parameter, which specifies the best image quality for the remote display configured to use H.264 encoding. Set the value to greater than the value set for RemoteDisplay.qpminH264.
RemoteDisplay.qpminH264	available range of values: 0–51	10	Use this option to set the H264maxQP quantization parameter, which specifies the lowest image quality for the remote display configured to use H.264 encoding. Set the value to less than the value set for RemoteDisplay.qpmaxH264.
UsbRedirPlugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the USB Redirection plugin.
UsbRedirServer.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the USB Redirection server.
VMWPkcs11Plugin.log.enable	`true` or `false`	`false`	Set this option to enable or disable the logging mode for the True SSO feature.
VMWPkcs11Plugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the True SSO feature.
VVC.RTAV.Enable	`true` or `false`	`true`	Set this option to enable/disable audio input.
VVC.ScRedir.Enable	`true` or `false`	`true`	Set this option to enable/disable smart card redirection.
VVC.logLevel	`fatal` `error`, `warn`, `info`, `debug`, or `trace`	`info`	Use this option to set the log level of the VVC proxy node.
cdrserver.cacheEnable	`true` or `false`	`true`	Set this option to enable or disable the write caching feature from the agent towards the client side.

Table 4-2. Configuration Options in `/etc/vmware/config` (continued)

Option	Value/Format	Default	Description
cdrserver.customizedSharedFolderPath	`folder_path`	`/home/`	Use this option to change the Client Drive Redirection (CDR) shared folder location from the default `/home/`*`user`*`/tsclient` directory to a custom directory. For example, if the user `test` wants to place the CDR shared folder at `/mnt/test/tsclient` instead of `/home/test/tsclient`, the user can specify **`cdrserver.customizedSharedFolderPath=/mnt/`**. **Note** In order for this option to take effect, the specified folder must exist and be configured with the correct user permissions.
cdrserver.forcedByAdmin	`true` or `false`	`false`	Set this option to control whether the client can share additional folders that are not specified with the `cdrserver.shareFolders` option.
cdrserver.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log level for the `vmware-CDRserver.log` file.
cdrserver.permissions	`R`	`RW`	Use this option to apply additional read/write permissions that Horizon Agent has on the folders shared by Horizon Client. For example: ■ If the folder shared by Horizon Client has `read` and `write` permissions and you set **`cdrserver.permissions=R`**, then Horizon Agent has only `read` access permissions. ■ If the folder shared by Horizon Client has only `read` permissions and you set **`cdrserver.permissions=RW`**, Horizon Agent still has only `read` access rights. Horizon Agent cannot change the `read` only attribute set by Horizon Client. Horizon Agent can only remove the write access rights. Typical uses are as follows: ■ **`cdrserver.permissions=R`** ■ **`#cdrserver.permissions=R`** (for example, comment it out or delete the entry)
cdrserver.sharedFolders	***`file_path1`*`,R;`*`file-path2`*`,;`*`file_path3`*`,R; ...`**	undefined	Specify one or more file paths to the folders that the client can share with the Linux desktop. For example: ■ For a Windows client: **`C:\spreadsheets,;D:\ebooks,R`** ■ For a non-Windows client: **`/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R`**
collaboration.logLevel	`error`, `info`, or `debug`	`info`	Use this option to set the log level used for the collaboration session. If the log level is `debug`, all calls made to `collabui` functions and the contents of the `collabor` list are logged.

Table 4-2. Configuration Options in `/etc/vmware/config` (continued)

Option	Value/Format	Default	Description
collaboration.maxCollabors	An integer less than 10	5	Specifies the maximum number of collaborators that you can invite to join a session.
collaboration.enableEmail	`true` or `false`	`true`	Set this option to enable or disable sending of collaboration invitations by using an installed email application. When this option is disabled, you cannot use email to invite collaborators, even if an email application is installed.
collaboration.serverUrl	[URL]	undefined	Specifies the server URLs to include in the collaboration invitations.
collaboration.enableControlPassing	`true` or `false`	`true`	Set this option to permit or restrict collaborators from having control of the Linux desktop. To specify a read-only collaboration session, set this option to **`false`**.
mksVNCServer.useUInputButtonMapping	`true` or `false`	`false`	Set this option to enable the support of a left-handed mouse on Ubuntu or RHEL 7.x. CentOS and RHEL 6.x support a left-handed mouse and you do not need to set this option.
mksvhan.clipboardSize	An integer	1024	Use this option to specify the clipboard maximum size to copy and paste.
vdpservice.log.logLevel	`fatal` `error`, `warn`, `info`, `debug`, or `trace`	`info`	Use this option to set the log level of the `vdpservice`.
viewusb.AllowAudioIn	**`{m|o}:{true|false}`**	undefined, which equates to `true`	Use this option to allow or disallow audio input devices to be redirected. Example: **`o:false`**
viewusb.AllowAudioOut	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to allow or disallow redirection of audio output devices.
viewusb.AllowAutoDeviceSplitting	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to allow or disallow the automatic splitting of composite USB devices. Example: **`m:true`**
viewusb.AllowDevDescFailsafe	**`{m|o}:{true|false}`**	undefined, which equates to `false`	Set this option to allow or disallow devices to be redirected even if Horizon Client fails to get the configuration or device descriptors. To allow a device even if it fails to get the configuration or device descriptors, include it in the Include filters, such as **`IncludeVidPid`** or **`IncludePath`**.
viewusb.AllowHIDBootable	**`{m|o}:{true|false}`**	undefined, which equates to `true`	Use this option to allow or disallow the redirection of input devices other than keyboards or mice that are available at boot time, also known as HID-bootable devices.

Table 4-2. Configuration Options in `/etc/vmware/config` (continued)

Option	Value/Format	Default	Description
viewusb.AllowKeyboardMouse	**{m|o}: {true|false}**	undefined, which equates to `false`	Use this option to allow or disallow the redirection of keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad).
viewusb.AllowSmartcard	**{m|o}: {true|false}**	undefined, which equates to `false`	Set this option to allow or disallow smart card devices to be redirected.
viewusb.AllowVideo	**{m|o}: {true|false}**	undefined, which equates to `true`	Use this option to allow or disallow video devices to be redirected.
viewusb.DisableRemoteConfig	**{m|o}: {true|false}**	undefined, which equates to `false`	Set this option to disable or enable the use of Horizon Agent settings when performing USB device filtering.
viewusb.ExcludeAllDevices	**{true|false}**	undefined, which equates to `false`	Use this option to exclude or include all USB devices from being redirected. If set to **true**, you can use other policy settings to allow specific devices or families of devices to be redirected. If set to **false**, you can use other policy settings to prevent specific devices or families of devices from being redirected. If you set the value of **ExcludeAllDevices** to **true** on Horizon Agent, and this setting is passed to Horizon Client, the Horizon Agent setting overrides the Horizon Client setting.
viewusb.ExcludeFamily	**{m|o}:*family_name_1*[;family_name_2;...]**	undefined	Use this option to exclude families of devices from being redirected. For example: **m:bluetooth;smart-card** If you have enabled automatic device splitting, Horizon examines the device family of each interface of a composite USB device to decide which interfaces must be excluded. If you have disabled automatic device splitting, Horizon examines the device family of the whole composite USB device. **Note** Mice and keyboards are excluded from redirection by default and do not need to be excluded with this setting.
viewusb.ExcludePath	**{m|o}:bus-*x1*[/*y1*].../ port-*z1*[;bus-*x2*[/*y2*].../port-*z2*;...]**	undefined	Use this option to exclude devices at specified hub or port paths from being redirected. You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example:**m:bus-1/2/3_port-02;bus-1/1/1/4_port-ff**

Table 4-2. Configuration Options in `/etc/vmware/config` (continued)

Option	Value/Format	Default	Description
viewusb.ExcludeVidPid	`{m|o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;..]`	undefined	Set this option to exclude devices with specified vendor and product IDs from being redirected. You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: `o:vid-0781_pid- ****;vid-0561_pid-554c`
viewusb.IncludeFamily	`{m|o}:family_name_1[;family_name_2]...`	undefined	Set this option to include families of devices that can be redirected. For example: `o:storage; smart-card`
viewusb.IncludePath	`{m|o}:bus-x1[/y1].../ port-z1[;bus-x2[/y2].../ portz2;...]`	undefined	Use this option to include devices at specified hub or port paths that can be redirected. You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: `m:bus-1/2_port- 02;bus-1/7/1/4_port-0`f
viewusb.IncludeVidPid	`{m|o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]`	undefined	Set this option to include devices with specified Vendor and Product IDs that can be redirected. You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: `o:vid-***_pid-0001;vid-0561_pid-554c`

Table 4-2. Configuration Options in `/etc/vmware/config` (continued)

Option	Value/Format	Default	Description
viewusb.SplitExcludeVidPid	**{m|o}:vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*;...]**	undefined	Use this option to exclude or include a specified composite USB device from splitting by Vendor and Product IDs . The format of the setting is **vid-*xxx1*_pid-*yyy1*[;vid-*xxx2*_pid-*yyy2*;...]**. You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. Example: **m:vid-0f0f_pid-55****
viewusb.SplitVidPid	**{m|o}: vid-*xxxx*_pid-*yyyy*([exintf:*zz*[;exintf:*ww*]])[;...]**	undefined	Set this option to treat the components of a composite USB device specified by Vendor and Product IDs as separate devices. The format of the setting is **vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*])**. You can use the **exintf** keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (*) in place of individual digits in an ID. Example: **o:vid-0f0f_pid-***(exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)** **Note** Horizon does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as **Include VidPid Device** to include those components.

Configuration Options in /etc/vmware/viewagent-custom.conf

Java Standalone Agent uses the configuration file `/etc/vmware/viewagent-custom.conf`.

Table 4-3. Configuration Options in `/etc/vmware/viewagent-custom.conf`

Option	Value	Default	Description
CDREnable	`true` or `false`	`true`	Use this option to enable or disable the Client Drive Redirection (CDR) feature.
CollaborationEnable	`true` or `false`	`true`	Use this option to enable or disable the Session Collaboration feature on Linux desktops.
EndpointVPNEnable	`true` or `false`	`false`	Set this option to specify if the client's physical network card IP address or the VPN IP address is to be used when evaluating the endpoint IP address against the range of endpoint IP addresses used in the Dynamic Environment Manager Console. If the option is set to `false`, the client's physical network card IP address is used. Otherwise, the VPN IP address is used.

Table 4-3. Configuration Options in `/etc/vmware/viewagent-custom.conf` (continued)

Option	Value	Default	Description
HelpDeskEnable	`true` or `false`	`true`	Set this option to enable or disable the Help Desk Tool feature.
KeyboardLayoutSync	`true` or `false`	`true`	Use this option to specify whether to synchronize a client's system locale list and current keyboard layout with Horizon Agent for Linux desktops. When this setting is enabled or not configured, synchronization is allowed. When this setting is disabled, synchronization is not allowed. This feature is supported only for Horizon Client for Windows, and only for the English, French, German, Japanese, Korean, Spanish, Simplified Chinese, and Traditional Chinese locales.
LogCnt	An integer	-1	Use this option to set the reserved log file count in `/tmp/vmware-root`. ■ -1 - keep all ■ 0 - delete all ■ > 0 - reserved log count.
NetbiosDomain	A text string, in all caps		When configuring True SSO, use this option to set the NetBIOS name of your organization's domain.
OfflineJoinDomain	`pbis` or `samba`	`pbis`	Use this option to set the instant-clone offline domain join. The available methods to perform an offline domain join are the PowerBroker Identity Services Open (PBISO) authentication and the Samba offline domain join. If this property has a value other than `pbis` or `samba`, the offline domain join is ignored.
RunOnceScript			Use this option to rejoin the cloned virtual machine to Active Directory. Set the `RunOnceScript` option after the host name has changed. The specified script is run only once after the first host name change. The script is run with the root permission when the agent service starts and the host name has been changed since the agent installation. For example, for the winbind solution, you must join the base virtual machine to Active Directory with winbind, and set this option to a script path. The script must contain the domain rejoin command `/usr/bin/net ads join -U <ADUserName>%<ADUserPassword>`. After VM Clone, the operating system customization changes the host name. When the agent service starts, the script is run to join the cloned virtual machine to Active Directory.
RunOnceScriptTimeout		120	Use this option to set the timeout time in seconds for the RunOnceScript option. For example, set `RunOnceScriptTimeout=120`

Table 4-3. Configuration Options in `/etc/vmware/viewagent-custom.conf` (continued)

Option	Value	Default	Description
SSLCiphers	A text string	!aNULL:kECDH +AESGCM:ECDH +AESGCM:RSA +AESGCM:kECDH +AES:ECDH+AES:RSA +AES	Use this option to specify the list of ciphers. You must use the format that is defined in https://www.openssl.org/docs/manmaster/man1/ciphers.html.
SSLProtocols	A text string	TLSv1_1:TLSv1_2	Use this option to specify the security protocols. The supported protocols are TLSv1.0, TLSv1.1, and TLSv1.2.
SSODesktopType	`UseGnomeClassic` or `UseGnomeFlashback` or `UseGnomeUbuntu` or `UseMATE` or `UseKdePlasma`	N/A	This option specifies the desktop environment to use, instead of the default desktop environment, when SSO is enabled. You must first ensure that the selected desktop environment is installed on your desktop before specifying to use it. After this option is set in an Ubuntu 16.04/18.04 desktop, the option takes effect regardless if the SSO feature is enabled or not. If this option is specified in a RHEL.x/CentOS 7.x desktop, the selected desktop environment is used only if SSO is enabled. **Note** This option is not supported on RHEL/CentOS 8.0 and RHEL/CentOS 6.x desktops. Horizon 7 only supports the Gnome desktop environment on RHEL/CentOS 8.0 desktops. See #unique_20/unique_20_Connect_42_section_F8FCD42564F3457A9491B067F9F65276 for more information on how to set up KDE as the default desktop environment when SSO is enabled on RHEL/CentOS 6.x desktops.
SSOEnable	`true` or `false`	`true`	Set this option to enable/disable single sign-on (SSO).
SSOUserFormat	A text string	[username]	Use this option to specify the format of the login name for single sign-on. The default is the user name only. Set this option if the domain name is also required. Typically, the login name is the domain name plus a special character followed by the user name. If the special character is the backslash, you must escape it with another backslash. Examples of login name formats are as follows: ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
Subnet	A value in CIDR IP address format	[subnet]	Set this option to a subnet which other machines can use to connect to the Horizon Agent for Linux. If there is more than one local IP address with different subnets, the local IP address in the configured subnet is used for connecting to the Horizon Agent for Linux. You must specify the value in the CIDR IP address format. For example, Subnet=123.456.7.8/24.

Table 4-3. Configuration Options in `/etc/vmware/viewagent-custom.conf` (continued)

Option	Value	Default	Description
UEMEnable	`true` or `false`	`false`	Set this option to enable or disable Dynamic Environment Manager smart policies. If the option is set to enable, and the condition in the Dynamic Environment Manager smart policy is met, then the policies are enforced.
UEMNetworkPath	A text string		This option must be set to the same network path that is set in User Environment Manager Console. The path must be in the format similar to `//10.111.22.333/view/LinuxAgent/UEMConfig`.

Note The three security options, SSLCiphers, SSLProtocols, and SSLCipherServerPreference are for the VMwareBlastServer process. When starting the VMwareBlastServer process, the Java Standalone Agent passes these options as parameters. When Blast Secure Gateway (BSG) is enabled, these options affect the connection between BSG and the Linux desktop. When BSG is disabled, these options affect the connection between the client and the Linux desktop.

Group Policy Settings for HTML Access

Group policy settings for HTML Access are specified in the ADM and ADMX template files named `vdm_blast.adm` and `vdm_blast.admx`. The templates are for the VMware Blast display protocol, which is the only display protocol that HTML Access uses.

For HTML Access 4.0 and later and Horizon 7 version 7.x, the VMware Blast group policy settings are described in "VMware Blast Policy Settings" in the *Configuring Remote Desktop Features in Horizon 7* document.

If you have HTML Access 3.5 or earlier and Horizon 6 version 6.2.x or earlier, the following table describes group policy settings that apply to HTML Access. In Horizon 7 version 7.x and later, more VMware Blast group policy settings are available.

Table 4-4. Group Policy Settings for HTML Access 3.5 or Earlier and Horizon 6 version 6.2.x or Earlier

Setting	Description
Screen Blanking	Controls whether the remote virtual machine can be seen from outside of Horizon 6 during an HTML Access session. For example, an administrator might use vSphere Web Client to open a console on the virtual machine while a user is connected to the desktop through HTML Access. When this setting is enabled or not configured, and someone attempts to access the remote virtual machine from outside of Horizon 6 while an HTML Access session is active, the remote virtual machine displays a blank screen.
Session Garbage Collection	Controls the garbage collection of abandoned remote sessions. When this setting is enabled, you can configure the garbage collection interval and threshold. The interval controls how often the garbage collector runs. You set the interval in milliseconds. The threshold determines how much time must pass after a session is abandoned before it becomes a candidate for deletion. You set the threshold in seconds.

Table 4-4. Group Policy Settings for HTML Access 3.5 or Earlier and Horizon 6 version 6.2.x or Earlier (continued)

Setting	Description
Configure clipboard redirection	Determines the direction in which clipboard redirection is allowed. Only text can be copied and pasted. You can select one of these values: ■ **Enabled client to server only** (That is, allow copy and paste only from the client system to the remote desktop.) ■ **Disabled in both directions** ■ **Enabled in both directions** ■ **Enabled server to client only** (That is, allow copy and paste only from the remote desktop to the client system.) This setting applies to View Agent or Horizon Agent only. When this setting is disabled or not configured, the default value is **Enabled client to server only**.
HTTP Service	Allows you to change the secured (HTTPS) TCP port for the Blast Agent service. The default port is 22443. Enable this setting to change the port number. If you change this setting, you must also update settings on the firewall of the affected remote desktops (where View Agent or Horizon Agent is installed).

Security Settings in the Horizon Client Configuration Templates

Security-related settings are provided in the Security section and the Scripting Definitions section of the ADM and ADMX template files for Horizon Client. The ADM template file is named `vdm_client.adm` and the ADMX template file is named `vdm_client.admx`. Except where noted, the settings include only a Computer Configuration setting. If a User Configuration setting is available and you define a value for it, it overrides the equivalent Computer Configuration setting.

The following table describes the settings in the Security section of the ADM and ADMX template files.

Table 4-5. Horizon Client Configuration Template: Security Settings

Setting	Description
`Allow command line credentials` (Computer Configuration setting)	Determines whether user credentials can be provided with Horizon Client command line options. If this setting is disabled, the `smartCardPIN` and `password` options are not available when users run Horizon Client from the command line. This setting is enabled by default. The equivalent Windows Registry value is `AllowCmdLineCredentials`.
`Servers Trusted For Delegation` (Computer Configuration setting)	Specifies the Connection Server instances that accept the user identity and credential information that is passed when a user selects the **Log in as current user** check box. If you do not specify any Connection Server instances, all Connection Server instances accept this information. To add a Connection Server instance, use one of the following formats: ■ **`domain\system$`** ■ **`system$@domain.com`** ■ The Service Principal Name (SPN) of the Connection Server service. The equivalent Windows Registry value is `BrokersTrustedForDelegation`.
`Certificate verification mode` (Computer Configuration setting)	Configures the level of certificate checking that is performed by Horizon Client. You can select one of these modes: ■ `No Security`. No certificate checking. ■ `Warn But Allow`. A warning appears if the Connection Server host presents a self-signed certificate, but the user can continue to connect to Connection Server. The certificate name does not need to match the Connection Server name provided by the user in Horizon Client. If any other certificate error condition occurs, an error dialog box appears and prevents the user from connecting to Connection Server. `Warn But Allow` is the default value. ■ `Full Security`. If any type of certificate error occurs, the user cannot connect to Connection Server. The user sees certificate errors. When this group policy setting is configured, users can view the selected certificate verification mode in Horizon Client, but they cannot configure the setting. The SSL configuration dialog box informs users that the administrator has locked the setting. When this setting is not configured or disabled, Horizon Client users can select a certificate verification mode. If you do not want to configure the certificate verification setting as a group policy, you can also enable certificate verification by modifying Windows registry settings.
`Default value of the 'Log in as current user' checkbox` (Computer and User Configuration setting)	Specifies the default value of the **Log in as current user** check box on theHorizon Client connection dialog box. This setting overrides the default value specified during Horizon Client installation. If a user runs Horizon Client from the command line and specifies the `logInAsCurrentUser` option, that value overrides this setting. When the **Log in as current user** check box is selected, the identity and credential information that the user provided when logging in to the client system is passed to the Connection Server instance and ultimately to the remote desktop. When the check box is deselected, users must provide identity and credential information multiple times before they can access a remote desktop. This setting is disabled by default. The equivalent Windows Registry value is `LogInAsCurrentUser`.

Table 4-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Description
`Display option to Log in as current user` (Computer and User Configuration setting)	Determines whether the **Log in as current user** check box is visible on the Horizon Client connection dialog box. When the check box is visible, users can select or deselect it and override its default value. When the check box is hidden, users cannot override its default value from the Horizon Client connection dialog box. You can specify the default value for the **Log in as current user** check box by using the policy setting `Default value of the 'Log in as current user' checkbox`. This setting is enabled by default. The equivalent Windows Registry value is `LogInAsCurrentUser_Display`.
`Enable jump list integration` (Computer Configuration setting)	Determines whether a jump list appears in the Horizon Client icon on the taskbar of Windows 7 and later systems. The jump list lets users connect to recent Connection Server instances and remote desktops. If Horizon Client is shared, you might not want users to see the names of recent desktops. You can disable the jump list by disabling this setting. This setting is enabled by default. The equivalent Windows Registry value is `EnableJumplist`.
`Enable SSL encrypted framework channel` (Computer and User Configuration setting)	Determines whether to enable the SSL encrypted framework channel. ■ **Enable**: Enables SSL, but allows fallback to the previous unencrypted connection if the remote desktop does not have SSL support. ■ **Disable**: Disables SSL. This setting is not recommended but might be useful for debugging or if the channel is not being tunneled and could potentially then be optimized by a WAN accelerator product. ■ **Enforce**: Enables SSL, and refuses to connect to desktops with no SSL support. The equivalent Windows Registry value is `EnableTicketSSLAuth`.

Table 4-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Description
`Configures SSL protocols and cryptographic algorithms` (Computer and User Configuration setting)	Configures the cipher list to restrict the use of certain cryptographic algorithms and protocols before establishing an encrypted SSL connection. The cipher list consists of one or more cipher strings separated by colons. **Note** All cipher strings are case-sensitive. ■ The default value for Horizon Client 4.10 and later is **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** ■ The default value for Horizon Client 4.2 and later is **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** ■ The default value for Horizon Client 4.0.1 and 4.1 is **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**. ■ The default value for Horizon Client 4.0 is **TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**. ■ The default value for Horizon Client 3.5 is **TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH**. ■ The default value for Horizon Client 3.3 and 3.4 is **TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**. ■ The value for Horizon Client 3.2 and earlier is **SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**. Beginning with Horizon Client 4.10, TLS v1.0 is permanently disabled, so it is no longer supported. In Horizon Client 4.0.1 through 4.9, TLS v1.0, TLS v1.1, and TLS v1.2 are enabled. (SSL v2.0 and v3.0 are removed.) You can disable TLS v1.0 if TLS v1.0 compatibility with the server is not required. In Horizon Client 4.0, TLS v1.1 and TLS v1.2 are enabled. (TLS v1.0 is disabled. SSL v2.0 and v3.0 are removed.) In Horizon Client 3.5, TLS v1.0, TLS v1.1, and TLS v1.2 are enabled. (SSL v2.0 and v3.0 are disabled.) In Horizon Client 3.3 and 3.4, TLS v1.0 and TLS v1.1 are enabled. (SSL v2.0 and v3.0, and TLS v1.2 are disabled.) In Horizon Client 3.2 and earlier, SSL v3.0 is also enabled. (SSL v2.0 and TLS v1.2 are disabled.) Cipher suites use 128- or 256-bit AES, remove anonymous DH algorithms, and then sort the current cipher list in order of encryption algorithm key length. Reference link for the configuration: http://www.openssl.org/docs/apps/ciphers.html The equivalent Windows Registry value is `SSLCipherList`. If you do not want to configure this setting as a group policy, you can also enable it by adding the `SSLCipherList` value name to one of the following registry keys on the client computer: ■ For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware VDM\Client\Security` ■ For 64-bit Windows: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware,Inc.\VMware VDM\Client\Security`
`Enable Single Sign-On for smart card authentication` (Computer Configuration setting)	Determines whether single sign-on is enabled for smart card authentication. When single sign-on is enabled, Horizon Client stores the encrypted smart card PIN in temporary memory before submitting it to Connection Server. When single sign-on is disabled, Horizon Client does not display a custom PIN dialog.

Table 4-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Description
	The equivalent Windows Registry value is `EnableSmartCardSSO`.

The following table describes the settings in the Scripting Definitions section of the ADM and ADMX template files.

Table 4-6. Security-Related Settings in the Scripting Definitions Section

Setting	Description
`Connect all USB devices to the desktop on launch`	Determines whether all of the available USB devices on the client system are connected to the desktop when the desktop is launched. This setting is disabled by default. The equivalent Windows Registry value is `connectUSBOnStartup`.
`Connect all USB devices to the desktop when they are plugged in`	Determines whether USB devices are connected to the desktop when they are plugged in to the client system. This setting is disabled by default. The equivalent Windows Registry value is `connectUSBOnInsert`.
`Logon Password`	Specifies the password that Horizon Client uses during login. The password is stored in plain text by Active Directory. This setting is undefined by default. The equivalent Windows Registry value is `Password`.

For more information about these settings and their security implications, see the Horizon Client for Windows documentation.

Configuring the Horizon Client Certificate Verification Mode

You can configure the Horizon Client certificate verification mode by adding the `CertCheckMode` value name to a registry key on the Windows client computer.

On 32-bit Windows systems, the registry key is `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`. On 64-bit Windows systems, the registry key is `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`.

Use one of the following values in the registry key:

- `0` - implements the **Do not verify server identity certificates** option.
- `1` - implements the **Warn before connecting to untrusted servers** option.
- `2` - implements the **Never connect to untrusted servers** option.

You can also configure the Horizon Client certificate verification mode by configuring the `Certificate verification mode` group policy setting. If you configure both the group policy setting and the `CertCheckMode` setting in the registry key, the group policy setting takes precedence over the registry key value.

When either the group policy setting or the registry setting is configured, users can view the selected certificate verification mode in Horizon Client, but they cannot configure the setting.

For information about configuring the `Certificate verification mode` group policy setting, see Security Settings in the Horizon Client Configuration Templates.

Configuring Local Security Authority Protection

Horizon Client and Horizon Agent support Local Security Authority (LSA) protection. LSA protection prevents users with unprotected credentials from reading memory and injecting code.

For more information about configuring LSA protection, read the Microsoft Windows Server documentation.

The following feature fails when LSA protection is configured for Horizon Client 4.4 and earlier:

- Log In As Current User

The following features fail when LSA protection is configured for Horizon Agent versions earlier than Horizon 7 version 7.2:

- Smart card authentication
- True SSO

Configuring Security Protocols and Cipher Suites

5

You can configure the security protocols and cipher suites that are accepted and proposed between Horizon Client, View Agent/Horizon Agent, and server components.

This chapter includes the following topics:

Default Policies for Security Protocols and Cipher Suites

Global acceptance and proposal policies enable certain security protocols and cipher suites by default.

The following tables list the protocols and cipher suites that are enabled by default for Horizon Client. In Horizon Client 3.1 and later for Windows, Linux, and Mac, these cipher suites and protocols are also used to encrypt the USB channel (communication between the USB service daemon and View Agent or Horizon Agent). For Horizon Client versions earlier than 4.0, the USB service daemon adds `RC4 ( :RC4-SHA: +RC4 )` to the end of the cipher control string when it connects to a remote desktop. RC4 is no longer added starting with Horizon Client 4.0.

Horizon Client 4.2 and Later

Table 5-1. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 4.2 and Later

Default Security Protocols	Default Cipher Suites
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0 **Note** Beginning with Horizon Client 4.10, TLS v1.0 is permanently disabled, so it is no longer supported.	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Table 5-1. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 4.2 and Later (continued)

Default Security Protocols	Default Cipher Suites
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Beginning with Horizon Client 4.10, TLS v1.0 is permanently disabled, so it is no longer supported.

In Horizon Client 4.2 through 4.9, TLS v1.0 is enabled by default to ensure that, by default, Horizon Client can connect to Horizon Cloud with Hosted Infrastructure servers. The default cipher string is !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. You can disable TLS v1.0 if TLS v1.0 compatibility with the server is not required.

Horizon Client 4.0.1 and 4.1

Table 5-2. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 4.0.1 and 4.1

Default Security Protocols	Default Cipher Suites
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Table 5-2. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 4.0.1 and 4.1 (continued)

Default Security Protocols	Default Cipher Suites
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

TLS 1.0 is enabled by default to ensure that, by default, Horizon Client can connect to Horizon Cloud with Hosted Infrastructure servers. The default cipher string is TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH +AES:ECDH+AES:RSA+AES:@STRENGTH. You can disable TLS 1.0 if TLS 1.0 compatibility with the server is not required.

Horizon Client 4.0

Table 5-3. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 4.0

Default Security Protocols	Default Cipher Suites
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Important TLS 1.0 is disabled by default. SSL 3.0 has been removed.

Horizon Client 3.5

Table 5-4. Security Protocols and Cipher Suites Enabled by Default onHorizon Client 3.5

Default Security Protocols	Default Cipher Suites
TLS 1.2	■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Horizon Client 3.3 and 3.4

Table 5-5. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 3.3 and 3.4

Default Security Protocols	Default Cipher Suites
■ TLS 1.1 ■ TLS 1.0	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Note TLS 1.2 is also supported, though not enabled by default. To enable TLS 1.2, follow the instructions in VMware KB 2121183, after which the cipher suites listed in Table 5-4. Security Protocols and Cipher Suites Enabled by Default onHorizon Client 3.5 are supported.

Horizon Client 3.0, 3.1, and 3.2

Table 5-6. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 3.0, 3.1, and 3.2

Default Security Protocols	Default Cipher Suites
■ TLS 1.1 ■ TLS 1.0 ■ SSL 3.0 (enabled on Windows clients only)	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022) ■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f) ■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Note TLS 1.2 is also supported, though not enabled by default. To enable TLS 1.2, follow the instructions in VMware KB 2121183, after which the cipher suites listed in Table 5-4. Security Protocols and Cipher Suites Enabled by Default onHorizon Client 3.5 are supported.

Configuring Security Protocols and Cipher Suites for Specific Client Types

Each type of client has its own method for configuring the protocols and cipher suites used.

You should change the security protocols in Horizon Client only if your View server does not support the current settings. If you configure a security protocol for Horizon Client that is not enabled on the View server to which the client connects, a TLS/SSL error occurs and the connection fails.

To change the protocols and ciphers from their default values, use the client-specific mechanism:

- On Windows client systems, you can use either a group policy setting or a Windows Registry setting.
- On Windows 10 UWP client systems, you can use the SSL Options setting in the Horizon Client options.
- On Linux client systems, you can use either configuration file properties or command-line options.
- On Mac client systems, you can use a Preference setting in Horizon Client.
- On iOS, Android, and Chrome OS client systems, you can use an Advanced SSL Options setting in the Horizon Client settings.

For more information, see the Horizon Client documentation.

Disable Weak Ciphers in SSL/TLS

To achieve greater security, you can configure the domain policy GPO (group policy object) to ensure that Windows-based machines running View Agent or Horizon Agent do not use weak ciphers when they communicate using the SSL/TLS protocol.

Procedure

1. On the Active Directory server, edit the GPO by selecting **Start > Administrative Tools > Group Policy Management**, right-clicking the GPO, and selecting **Edit**.
2. In the Group Policy Management Editor, navigate to the **Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings**.
3. Double-click **SSL Cipher Suite Order**.
4. In the SSL Cipher Suite Order window, click **Enabled**.
5. In the Options pane, replace the entire content of the SSL Cipher Suites text box with the following cipher list:

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
```

```
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

The cipher suites are listed above on separate lines for readability. When you paste the list into the text box, the cipher suites must be on one line with no spaces after the commas.

6 Exit the Group Policy Management Editor.

7 Restart the View Agent or Horizon Agent machines for the new group policy to take effect.

Configure Security Protocols and Cipher Suites for HTML Access Agent

Starting with View Agent 6.2, you can configure the cipher suites that HTML Access Agent uses by editing the Windows registry. Starting with View Agent 6.2.1, you can also configure the security protocols used. You can also specify the configurations in a group policy object (GPO).

With View Agent 6.2.1 and later releases, by default, the HTML Access Agent uses only TLS 1.1 and TLS 1.2. The protocols that are allowed are, from low to high, TLS 1.0, TLS 1.1, and TLS 1.2. Older protocols such as SSLv3 and earlier are never allowed. Two registry values, `SslProtocolLow` and `SslProtocolHigh`, determine the range of protocols that HTML Access Agent will accept. For example, setting `SslProtocolLow=tls_1.0` and `SslProtocolHigh=tls_1.2` will cause the HTML Access Agent to accept TLS 1.0, TLS 1.1, and TLS 1.2. The default settings are `SslProtocolLow=tls_1.1` and `SslProtocolHigh=tls_1.2`.

You must specify the list of ciphers using the format that is defined in https://www.openssl.org/docs/manmaster/man1/ciphers.html, under the section CIPHER LIST FORMAT. The following cipher list is the default:

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

Procedure

1 Start the Windows Registry Editor.

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

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

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

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

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

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

5 Restart the Windows service VMware Blast.

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

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

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

Configure Proposal Policies on Remote Desktops

You can control the security of Message Bus connections to Connection Server by configuring the proposal policies on remote desktops that run Windows.

Make sure that Connection Server is configured to accept the same policies to avoid a connection failure.

Procedure

1 Start the Windows Registry Editor on the remote desktop.

2 Navigate to the `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration` registry key.

3 Add a new String (REG_SZ) value, `ClientSSLSecureProtocols`.

4 Set the value to a list of cipher suites in the format **\LIST:*protocol_1*,*protocol_2*,...**.

   List the protocols with the latest protocol first. For example:

   ```
   \LIST:TLSv1.2,TLSv1.1,TLSv1
   ```

5 Add a new String (REG_SZ) value, `ClientSSLCipherSuites`.

6 Set the value to a list of cipher suites in the format **\LIST:*cipher_suite_1*,*cipher_suite_2*,...**.

   The list should be in order of preference, with the most preferred cipher suite first. For example:

   ```
   \LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
   ```

Client and Agent Log File Locations

6

The clients and the agent create log files that record the installation and operation of their components.

This chapter includes the following topics:

Horizon Client for Windows Logs

Log files can help troubleshoot issues with installation, display protocol, and various feature components. You can use group policy settings to configure the location, verbosity, and retention period of some log files.

Log Location

For the file names in the following table, *YYYY* represents the year, *MM* is the month, *DD* is the day, and *XXXXXX* is a number.

Table 6-1. Horizon Client for Windows Log Files

Type of Logs	Directory Path	File Name
Installation	`C:\Users\%username%\AppData\Local\Temp`	`vminst.log_XXXXXX_XXXXXX.txt` `vmmsi.log_XXXXXX_XXXXXX.txt`
PCoIP client From the `vmware-remotemks.exe` process	`C:\Users\%username%\AppData\Local\Temp`	`pcoip_client_YYYY_MM_DD_XXXXXX.txt` **Note** You can use a GPO to configure the log level, from 0 to 3 (most verbose). Use the View PCoIP Client Session Variables ADMX template file `pcoip.admx`. The setting is called **Configure PCoIP event log verbosity**.

Table 6-1. Horizon Client for Windows Log Files (continued)

Type of Logs	Directory Path	File Name
Horizon Client UI From the `vmware-view.exe` process	`C:\Users\%username%\AppData\Local\VMware\VDM\Logs`	`vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt` **Note** You can use a GPO to configure the log location. Use the View Common Configuration ADMX template file `vdm_common.admx`.
Horizon Client logs From the `vmware-view.exe` process	`C:\Users\%username%\AppData\Local\Temp\vmware-username-XXXXXX`	`vmware-crtbora-XXXXXX.log`
Message framework	`C:\Users\%username%\AppData\Local\VMware\VDM\Logs`	`log-YYYY-MM-DD-XXXXXX.txt` `debug-YYYY-MM-DD-XXXXXX.txt`

Remote MKS (mouse-keyboard-screen) logs
From the `vmware-remotemks.exe` process
	`C:\Users\%username%\AppData\Local\Temp\vmware-username`	`ViewMP-Client-XXXXXX.log`
		`vmware-mks-XXXXXX.log`
		`vmware-rdeSvc-XXXXXX.log`
		`vmware-vvaClient-XXXXXX.log`

Tsdr client From the `vmware-remotemks.exe` process	`C:\Users\%username%\AppData\Local\Temp\vmware-username`	`vmware-ViewTsdr-Client-XXXXXX.log`
Tsmmr client From the `vmware-remotemks.exe` process	`C:\Users\%username%\AppData\Local\Temp\vmware-username`	`vmware-ViewTsmmr-Client-XXXXXX.log`
VdpService client From the `vmware-remotemks.exe` process	`C:\Users\%username%\AppData\Local\Temp\vmware-username`	`vmware-vdpServiceClient-XXXXXX.log`
WSNM service From the `wsnm.exe` process	`C:\ProgramData\VMware\VDM\logs`	`debug-yyyy-mm-dd-XXXXXX.txt` **Note** You can use a GPO to configure the log location. Use the View Common Configuration ADMX template file `vdm_common.admx`.
USB redirection From the `vmware-view-usbd.exe` or `vmware-remotemks.exe` process	`C:\ProgramData\VMware\VDM\logs`	`debug-yyyy-mm-dd-XXXXXX.txt` In Horizon Client 4.4 and later, the `vmware-view-usbd.exe` process is removed and the USBD process is moved to the `vmware-remotemks.exe` process. **Note** You can use a GPO to configure the log location. Use the View Common Configuration ADMX template file `vdm_common.admx`.
Serial port redirection From the `vmwsprrdpwks.exe` process	`C:\ProgramData\VMware\VDM\Logs`	`Serial*.txt` `Netlink*.txt`
Scanner redirection From the `ftscanmgr.exe` process	`C:\ProgramData\VMware\VDM\Logs`	`Scanner*.txt` `Netlink*.txt`

Log Configuration

You can use group policy settings to make some configuration changes:

- For PCoIP client logs, you can configure the log level, from 0 to 3 (most verbose). Use the View PCoIP Client Session Variables ADMX template file `pcoip.admx`. The setting is called **Configure PCoIP event log verbosity**.
- For client UI logs, configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file `vdm_common.admx`.
- For USB redirection logs, configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file `vdm_common.admx`.
- For WSNM service logs, configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file `vdm_common.admx`.

You can also use a command-line command to set a verbosity level. Navigate to the `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` directory and enter the following command:

```
support.bat loglevels
```

A new command prompt window appears, and you are prompted to select a verbosity level.

Collecting a Log Bundle

You can use either the client UI or a command-line command to collect logs into a .zip file that you can send to VMware Technical Support.

- In the **Horizon Client** window, from the Options menu, select **Support Information**, and in the dialog box that appears, click **Collect Support Data**.
- From the command line, navigate to the `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` directory and enter the following command: `support.bat`.

Horizon Client for Mac Logs

Log files can help troubleshoot issues with installation, display protocol, and various feature components. You can create a configuration file to configure the verbosity level.

Log Location

Table 6-2. Horizon Client for Mac Log Files

Type of Logs	Directory Path	File Name
Horizon Client UI	`~/Library/Logs/VMware Horizon Client`	
PCoIP client	`~/Library/Logs/VMware Horizon Client`	
Real-Time Audio-Video	`~/Library/Logs/VMware`	`vmware-RTAV-pid.log`
USB redirection	`~/Library/Logs/VMware`	

Table 6-2. Horizon Client for Mac Log Files (continued)

Type of Logs	Directory Path	File Name
VChan	`~/Library/Logs/VMware Horizon Client`	
Remote MKS (mouse-keyboard-screen) logs	`~/Library/Logs/VMware`	
Crtbora	`~/Library/Logs/VMware`	

Log Configuration

In Horizon Client 3.1 and later, Horizon Client generates log files in the `~/Library/Logs/VMware Horizon Client` directory on the Mac client. Administrators can configure the maximum number of log files and the maximum number of days to keep log files by setting keys in the `/Library/Preferences/com.vmware.horizon.plist` file on a Mac client.

Table 6-3. plist Keys for Log File Collection

Key	Description
`MaxDebugLogs`	Maximum number of log files. The maximum value is 100.
`MaxDaysToKeepLogs`	Maximum number of days to keep log files. This value has no limit.

Files that do not match these criteria are deleted when you launch Horizon Client.

If the `MaxDebugLogs` or `MaxDaysToKeepLogs` keys are not set in the `com.vmware.horizon.plist` file, the default number of log files is 5 and the default number of days to keep log files is 7.

Horizon Client for Linux Logs

Log files can help troubleshoot issues with installation, display protocol, and various feature components. You can create a configuration file to configure the verbosity level.

Log Location

Table 6-4. Horizon Client for Linux Log Files

Type of Logs	Directory Path	File Name
Installation	`/tmp/vmware-root/`	`.vmware-installer-pid.log` `vmware-vmis-pid.log`
Horizon Client UI	`/tmp/vmware-`*`username`*`/`	`vmware-horizon-client-pid.log`
PCoIP client	`/tmp/teradici-`*`username`*`/`	`pcoip_client_`*`YYYY_MM_DD_XXXXXX`*`.log`
Real-Time Audio-Video	`/tmp/vmware-`*`username`*`/`	`vmware-RTAV-pid.log`
USB redirection	`/tmp/vmware-root/`	`vmware-usbarb-pid.log` `vmware-view-usbd-pid.log`

Table 6-4. Horizon Client for Linux Log Files (continued)

Type of Logs	Directory Path	File Name
VChan	/tmp/vmware-*username*/	VChan-Client.log **Note** This log is created when you enable RDPVCBridge logs by setting "export VMW_RDPVC_BRIDGE_LOG_ENABLED=1".
Remote MKS (mouse-keyboard-screen) logs	/tmp/vmware-*username*/	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
VdpService client	/tmp/vmware-*username*/	vmware-vdpServiceClient-pid.log
Tsdr client	/tmp/vmware-*username*/	vmware-ViewTsdr-Client-pid.log

Log Configuration

You can use a configuration property (`view.defaultLogLevel`) to set the verbosity level for client logs, from 0 (collect all events) to 6 (collect only fatal events).

For USB-specific logs, you can use the following command-line commands:

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

Collecting a Log Bundle

The log collector is located at `/usr/bin/vmware-view-log-collector` . To use the log collector, you must have execute permissions. You can set permissions from the Linux command line by entering the following command:

```
chmod +x /usr/bin/vmware-view-log-collector
```

You can run the log collector from a Linux command line by entering the following command:

`/usr/bin/vmware-view-log-collector`

Horizon Client Logs on Mobile Devices

On mobile devices, you might need to install a third-party program to navigate to the directory where log files are stored. Mobile clients have configuration settings for sending log bundles to VMware. Because logging can affect performance, you should enable logging only when you need to troubleshoot an issue.

iOS Client Logs

For iOS clients, the log files are in the `tmp` and `Documents` directories under *`User Programs`*`/Horizon/`. To navigate to these directories, you must first install a third-party app such as iFunbox.

You can enable logging by turning on the **Logging** setting in the Horizon Client settings. With this setting enabled, if the client exits unexpectedly or if you exit the client and then launch it again, the log files are merged and compressed into a single GZ file. You can then send the bundle to VMware through email. If your device is connected to a PC or Mac, you can also use iTunes to retrieve log files.

Android Client Logs

For Android clients, the log files are in the `Android/data/com.vmware.view.client.android/files/` directory. To navigate to this directory, you must first install a third-party app such as File Explorer or My Files.

By default, logs are created only after the application exits unexpectedly. You can change this default by turning on the **Enable Log** setting in the Horizon Client settings. To send a log bundle to VMware through email, you can use the **Send the log** setting in the General Settings of the client.

Chrome OS Client Logs

For Chrome OS clients, logs are available only through the JavaScript console.

Windows 10 UWP Client Logs

For Windows 10 UWP clients, logs are in the `C:\Windows\Users\`*`%username%`*`\AppData\Local\VMware\VDM\logs` directory.

You can enable logging by turning on the **Enable advanced logging** option in the Logging section of the Horizon Client options and then clicking the **Collect support information** button. You are prompted to select a folder for the logs, and you can zip the folder as you would any other folder.

Windows Store Client Logs

For Windows Store clients that have Horizon Client for Windows Store installed, rather than Horizon Client for Windows, the log files are in the directory `C:\Users\`*`%username%`*`\AppData\Local\Packages\VMwareInc.VMwareViewClient_23chmsjxv380w\LocalState\logs` directory.

You can enable logging by turning on the **Enable advanced logging** setting in the Horizon Client General Settings and then clicking the **Collect support information** button. You are prompted to select a folder for the logs, and you can zip the folder as you would any other folder.

Horizon Agent Logs from Windows Machines

Log files can help troubleshoot issues with installation, display protocol, and various feature components. You can use group policy settings to configure the location, verbosity, and retention period of some log files.

Log Location

For the file names in the following table, *YYYY* represents the year, *MM* is the month, *DD* is the day, and *XXXXXX* is a number.

Table 6-5. Horizon Client for Windows Log Files

Type of Logs	Directory Path	File Name
Installation	C:\Users\%*username*%\AppData\Local\Temp	vminst.log_*XXXXXX_XXXXXX*.txt vmmsi.log_*XXXXXX_XXXXXX*.txt
View Agent (for Horizon 6) or Horizon Agent (for Horizon 7)	*<Drive Letter>*:\ProgramData\VMware\VDM\logs	pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt pcoip_agent_*YYYY_MM_DD_XXXXXX*.txt vmware-vdpServiceServer-*XXXXXX*.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-*XXXXXX*.txt **Note** You can use a GPO to configure the log location. Use the View Common Configuration ADMX template file vdm_common.admx.

Log Configuration

There are several methods for configuring logging options.

- You can use group policy settings to configure the log location, verbosity, and retention policy. Use the View Common Configuration ADMX template file vdm_common.admx.
- You can use a command-line command to set a verbosity level. Navigate to the C:\Program Files\VMware\VMware View\Agent\DCT directory and enter the following command: support.bat loglevels. A new command prompt window appears, and you are prompted to select a verbosity level.
- You can use the vdmadmin command with the -A option to configure logging by View Agent or Horizon Agent. For instructions, see the *Horizon 7 Administration* document.

Collecting a Log Bundle

You can use a command-line command to collect logs into a .zip file that you can send to VMware Technical Support. From the command line, navigate to the C:\Program Files\VMware\VMware View\Agent\DCT directory and enter the following command: support.bat.

Linux Desktop Logs

Log files can help troubleshoot issues with installation, display protocol, and various feature components. You can create a configuration file to configure the verbosity level.

Log Location

Table 6-6. Linux Desktop Log Files

Type of Logs	Directory Path
Installation	`/tmp/vmware-root`
View Agent (for Horizon 6) or Horizon Agent (for Horizon 7)	`/var/log/vmware`
View Agent (for Horizon 6) or Horizon Agent (for Horizon 7)	`/usr/lib/vmware/viewagent/viewagent-debug.log`

Log Configuration

Edit the `/etc/vmware/config` file to configure logging.

Collecting a Log Bundle

You can create a Data Collection Tool (DCT) bundle that gathers the machine's configuration information and logs into a compressed tarball. Open a command prompt in the Linux desktop and run the `dct-debug.sh` script.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

The tarball is generated in the directory from which the script was executed (the current working directory). The file name includes the operating system, timestamp, and other information; for example: `ubuntu-12-vdm-sdct-20150201-0606-agent.tgz`

This command collects log files from the `/tmp/vmware-root` directory and the `/var/log/vmware` directory, and also collects the following system log and configuration files:

- `/var/log/messages*`
- `/var/log/syslog*`
- `/var/log/boot*.log`
- `/proc/cpuinfo`, `/proc/meminfo`, `/proc/vmstat`, `/proc/loadavg`
- `/var/log/audit/auth.log*`
- `/etc/hosts`
- `/etc/resolv.conf`
- `/etc/nsswitch.conf`
- `/var/log/Xorg*`
- `/etc/X11/xorg.conf`
- Core files in `/usr/lib/vmware/viewagent`
- Any crash files in `/var/crash/_usr_lib_vmware_viewagent*`

Applying Security Patches 7

Patch releases might include installer files for the following Horizon 6 or Horizon 7 components: View Composer, Connection Server, View Agent or Horizon Agent, and various clients. The patch components that you must apply depend on the bug fixes that your deployment requires.

Depending on which bug fixes you require, install the applicable Horizon 6 or Horizon 7 components, in the following order:

1 View Composer

2 Connection Server

3 View Agent (for Horizon 6) or Horizon Agent (for Horizon 7)

4 Horizon Client

For instructions about applying patches for the server components, see the *Horizon 7 Upgrades* document.

This chapter includes the following topics:

Apply a Patch for View Agent or Horizon Agent

Applying a patch involves downloading and running the installer for the patch version.

The following steps need to be performed on the parent virtual machine, for linked-clone desktop pools, or on each virtual machine desktop in a full-clone pool, or on individual desktop virtual machines for pools that contain only one virtual machine desktop.

Prerequisites

Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the patch installer.

Procedure

1. On all parent virtual machines, virtual machines used for full-clone templates, full clones in a pool, and manually added individual virtual machines, download the installer file for the patch version of View Agent (for Horizon 6) or Horizon Agent (for Horizon 7).

   Your contact at VMware will provide instructions for this download.

2. Run the installer that you downloaded for the patch release of View Agent or Horizon Agent.

   Note In Horizon 6 version 6.2 and later releases, you do not need to uninstall the previous version before you install the patch.

3. If you disabled provisioning of new virtual machines in preparation for applying a patch to View Composer, enable provisioning again.
4. For parent virtual machines that will be used to create linked-clone desktop pools, take a snapshot of the virtual machine.

   For information about taking snapshots, see the vSphere Client online help.

5. For linked-clone desktop pools, use the snapshot you created to recompose the desktop pools.
6. Verify that you can log in to the patched desktop pools with Horizon Client.
7. If you canceled any refresh or recompose operations for any linked-clone desktop pools, schedule the tasks again.

Apply a Patch for Horizon Client

On desktop client devices, applying a patch involves downloading and running the installer for the patch version. On mobile clients, applying a patch involves simply installing the update from the Web site that sells apps, such as Google Play, Windows Store, or the Apple App Store.

Procedure

1. On each client system, download the installer file for the patch version of Horizon Client.

   Your contact at VMware will provide instructions for this download. Or you can go to the client download page at http://www.vmware.com/go/viewclients. As mentioned previously, for some clients, you might get the patch release from an app store.

2. If the client device is a Mac or Linux desktop or laptop, remove the current version of the client software from your device.

   Use the customary device-specific method for removing applications.

   Note With Horizon Client 3.5 for Windows and later releases, you do not need to uninstall the previous version before you install the patch on Windows clients. With Horizon Client 4.1 for Windows and later releases, you can enable the Upgrade Horizon Client Online feature to upgrade Horizon Client online on Windows clients. With Horizon Client for Mac 4.4 and later, you can enable the Upgrade Horizon Client Online feature to upgrade Horizon Client online on Mac clients.

3 If applicable, run the installer that you downloaded for the patch release of the Horizon Client.

   If you got the patch from the Apple App Store or Google Play, the app is usually installed when you download it, and you do not need to run an installer.

4 Verify that you can log in to the patched desktop pools with the newly patched Horizon Client.