Horizon Client and Agent Security

Horizon Client 2106, Horizon Agent 2106

VMware Horizon 2106

vmware®

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

https://docs.vmware.com/

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

Contents

Horizon Client and Agent Security

This guide describes the security features of VMware Horizon® Client™ and Horizon Agent. It is a companion guide to the *Horizon Security* document.

Horizon Client is the client software that end users run on their client devices to connect to remote desktops and published applications. Horizon Agent is the agent software that runs in virtual desktops, and on Microsoft RDS hosts that provide published desktops and published applications.

The information in this document is intended for IT decision makers, architects, administrators, and others who must understand the security components of VMware Horizon.

External Ports

1

Depending on which features you want to use, certain ports must be opened to enable the client and agent software to communicate.

This chapter includes the following topics:

Understanding Communications Protocols

VMware Horizon components use several different protocols to exchange messages.

The following table lists the default ports that each protocol uses. You can change the port numbers. For example, you might need to change the port numbers to comply with organization policies, or to avoid contention.

Table 1-1. Default Ports

Protocol	Port
JMS	TCP port 4001 TCP port 4002
HTTP	TCP port 80
HTTPS	TCP port 443
MMR/CDR	TCP port 9427 The following features use this port. ■ Windows multimedia redirection ■ Client drive redirection ■ Microsoft Teams optimization ■ HTML multimedia redirection ■ VMware printer redirection ■ USB redirection
RDP	TCP port 3389

Table 1-1. Default Ports (continued)

Protocol	Port
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 Horizon Agent

To open the default network ports, the Horizon Agent installer optionally configures Windows firewall rules on virtual desktops and RDS hosts.

The Horizon Agent installer configures 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 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 the firewall rules to allow access on the updated port. For more information, see the *Horizon Installation* document.

On RDS hosts, the Windows firewall rules for Horizon Agent show a block of 256 contiguous UDP ports as open for inbound traffic. This block of ports is for VMware Blast internal use in 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. For more information, see Microsoft Knowledge Base (KB) article 875357.

The following table lists the TCP and UDP ports that are opened during Horizon Agent installation. Ports are incoming unless otherwise noted.

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

Protocol	Ports
RDP	TCP port 3389
USB redirection and time zone synchronization	TCP port 32111

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

Protocol	Ports
Multimedia redirection (MMR) and client drive redirection (CDR)	TCP port 9427 The following features use this port: ■ Windows multimedia redirection ■ Client drive redirection ■ Microsoft Teams optimization ■ HTML multimedia redirection ■ VMware printer redirection ■ USB redirection
PCoIP	For RDS hosts, PCoIP uses TCP port 4172 and UDP port 4172 (bidirectional). For virtual desktops, PCoIP uses port numbers selected from a configurable range. By default, PCoIP uses TCP ports 4172 to 4173 and UDP ports 4172 to 4182. The firewall rules do not specify port numbers. Instead, they dynamically follow the ports opened by each PCoIP server. The selected port numbers are communicated to the client through the Connection Server instance.
VMware Blast	TCP port 22443 UDP port 22443 (bidirectional) **Note** UDP is not used on Linux desktops.
HTML Access	TCP port 22443
XDMCP	UDP 177 **Note** This port is opened for XDMCP access only on 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 on Linux desktops running Ubuntu 18.04. Firewall rules block all external host access to this port.

TCP and UDP Ports for Clients and Agents

Horizon Agent and Horizon Client use TCP and UDP ports for network access between each other and certain server components.

Table 1-3. TCP and UDP Ports That Horizon Agent Uses

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	Horizon Agent	3389	TCP	Microsoft RDP traffic to remote desktops when direct connections are used instead of tunnel connections.
Horizon Client	*	Horizon Agent	9427	TCP	Windows multimedia redirection, client drive redirection, Microsoft Teams optimization, HTML5 multimedia redirection, VMware printer redirection, and USB redirection when direct connections are used instead of tunnel connections. **Note** Not needed for client drive redirection when using VMware Blast.
Horizon Client	*	Horizon Agent	32111	TCP	USB redirection and time zone synchronization when direct connections are used instead of tunnel connections.
Horizon Client	*	Horizon Agent	4172	TCP and UDP	PCoIP when 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 when direct connections are used instead of tunnel connections. **Note** UDP is not used on Linux desktops.
Browser	*	Horizon Agent	22443	TCP	HTML Access when direct connections are used instead of tunnel connections.
Connection Server or Unified Access Gateway appliance	*	Horizon Agent	3389	TCP	Microsoft RDP traffic to remote desktops when tunnel connections are used.
Connection Server or Unified Access Gateway appliance	*	Horizon Agent	9427	TCP	Windows multimedia redirection, client drive redirection, Microsoft Teams optimization, HTML5 multimedia redirection, VMware printer redirection, and USB redirection when tunnel connections are used.
Connection Server or Unified Access Gateway appliance	*	Horizon Agent	32111	TCP	USB redirection and time zone synchronization when tunnel connections are used.
Connection Server or Unified Access Gateway appliance	55000	Horizon Agent	4172	UDP	PCoIP (not SALSA20) when PCoIP Secure Gateway is used.
Connection Server or Unified Access Gateway appliance	*	Horizon Agent	4172	TCP	PCoIP when PCoIP Secure Gateway is used.

Table 1-3. TCP and UDP Ports That Horizon Agent Uses (continued)

Source	Port	Target	Port	Protocol	Description
Connection Server or Unified Access Gateway appliance	*	Horizon Agent	22443	TCP and UDP	VMware Blast when Blast Secure Gateway is used. **Note** UDP is not used on Linux desktops.
Connection Server or Unified Access Gateway appliance	*	Horizon Agent	22443	TCP	HTML Access when Blast Secure Gateway is used.
Horizon Agent	*	Connection Server	4001, 4002	TCP	JMS SSL traffic.
Horizon Agent	4172	Horizon Client	*	UDP	PCoIP when PCoIP Secure Gateway is not used. **Note** Because the target port varies, see the note below this table.
Horizon Agent	4172	Connection Server or Unified Access Gateway appliance	55000	UDP	PCoIP (not SALSA20) when 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 uses port 50003. If port 50003 is in use, the agent uses 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 That Horizon Client Uses

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	Connection Server or Unified Access Gateway appliance	443	TCP	HTTPS for logging in to VMware Horizon. This port is also used for tunneling when tunnel connections are used. **Note** Horizon Client supports UDP port 443.
Horizon Client	*	Unified Access Gateway appliance	443	UDP	HTTPS for logging into VMware Horizon when Blast Secure Gateway is used and UDP Tunnel Server is enabled. This port is also used for tunneling when tunnel connections are used.
Unified Access Gateway appliance	443	Horizon Client	*	UDP	HTTPS for logging into VMware Horizon when Blast Secure Gateway is used and UDP Tunnel Server is enabled. This port is also used for tunneling when tunnel connections are used.
Horizon Client	*	Horizon Agent	22443	TCP	HTML Access and VMware Blast when Blast Secure Gateway is not used.

Table 1-4. TCP and UDP Ports That Horizon Client Uses (continued)

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	Horizon Agent	22443	UDP	VMware Blast when Blast Secure Gateway is not used. **Note** Not used when connecting to Linux desktops.
Horizon Agent	22443	Horizon Client	*	UDP	VMware Blast when Blast Secure Gateway is not used. **Note** Not used when connecting to Linux desktops.
Horizon Client	*	Horizon Agent	3389	TCP	Microsoft RDP traffic to remote desktops if direct connections are used instead of tunnel connections.
Horizon Client	*	Horizon Agent	9427	TCP	Windows multimedia redirection, client drive redirection, Microsoft Teams optimization, HTML5 multimedia redirection, VMware printer redirection, and USB redirection when direct connections are used instead of tunnel connections. **Note** Not needed for client drive redirection when using VMware Blast.
Horizon Client	*	Horizon Agent	32111	TCP	USB redirection and time zone synchronization when direct connections are used instead of tunnel connections.
Horizon Client	*	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 or Unified Access Gateway appliance	4172	TCP and UDP	PCoIP (not SALSA20) when PCoIP Secure Gateway is used. **Note** Because the source port varies, see the note below this table.
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.
Connection Server or Unified Access Gateway appliance	4172	Horizon Client	*	UDP	PCoIP (not SALSA20) when PCoIP Secure Gateway is used. **Note** Because the target port varies, see the note below this table.
Horizon Client	*	Connection Server or Unified Access Gateway appliance	8443	TCP	HTML Access and VMware Blast when Blast Secure Gateway is used.

Table 1-4. TCP and UDP Ports That Horizon Client Uses (continued)

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	Connection Server or Unified Access Gateway appliance	8443	UDP	VMware Blast when Blast Secure Gateway is used. **Note** Not used when connecting to a Linux desktop.
Connection Server or Unified Access Gateway appliance	8443	Horizon Client	*	UDP	VMware Blast when 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 selects port 50003, and if port 50003 is in use, the client selects 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

The Horizon Client and Horizon Agent installers install several components.

This chapter includes the following topics:

Horizon Agent Services on Windows Machines

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

Table 2-1. Horizon Agent Services

Service Name	Startup Type	Description
VMware Blast	Automatic	Provides services for HTML Access and for using the VMware Blast display protocol for connecting with native clients.
VMware Horizon View Agent	Automatic	Provides services for Horizon Agent.
VMware Horizon View Script Host	Disabled	Supports the running of start session scripts, if any, that 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	Supports the scanner redirection and the serial port redirection features by providing monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Agent	Automatic	Provides services for the scanner redirection feature.
VMware Serial Com Redirection Agent Service	Automatic	Provides services for the serial port redirection feature.

Table 2-1. Horizon Agent Services (continued)

Service Name	Startup Type	Description
VMware Snapshot Provider	Manual	Provides services for virtual machine snapshots, which are used for cloning.
VMware Tools	Automatic	Supports the synchronization of objects between the host and guest operating systems, which enhances the performance of virtual machine guest operating systems and improves the management of virtual machines.

Horizon Client Services on Windows Clients

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	Supports the scanner redirection and serial port redirection features by providing monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Client Service	Automatic	Provides services for the scanner redirection feature.
VMware Serial Com Client Service	Automatic	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.

Daemons in Non-Windows Clients and Linux Desktops

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

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

Horizon Client 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** If you click the **Register and start the service(s) after installation** check box during installation, these daemons start automatically. These processes run as root.
Mac client	None
iOS client	None

Table 2-3. Services, Processes, and Daemons by Horizon Client Type (continued)

Horizon Client Type	Service, Process, or Daemon
Android client	None. Horizon Client runs in one Android process.
Linux desktop	■ `StandaloneAgent`, which runs with root privileges and starts when the Linux system is up and running. `StandaloneAgent` communicates with Connection Server to perform remote desktop session management. It sets up, tears down the session, updating the remote desktop status to the broker in Connection Server. ■ `VMwareBlastServer`, which `StandaloneAgent` starts when it receives a `StartSession` request from Connection Server. The `VMwareBlastServer` daemon runs with `vmwblast` privilege. `vmwblast` is a system account that is created when the Linux agent is installed. 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

You must secure certain resources. 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.

- Configure client systems 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. Configuration File Locations by Client Type

Client Type	File Location
Linux client	When the Linux client starts, it processes configuration settings from the following directories 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 Linux client uses the value from the last file or command-line option that it reads.
Windows client	User settings that might include some private information are in the following file: `C:\Users\`*`user-name`*`\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt`
Mac client	When the Mac client starts, it generates the following configuration files: ■ `$HOME/Library/Preferences/com.vmware.horizon.plist` ■ `$HOME/Library/Preferences/com.vmware.vmrc.plist` ■ `$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist` ■ `/Library/Preferences/com.vmware.horizon.plist`
iOS client	Security-related settings appear in the user interface rather than in configuration files.
Android client	Security-related settings appear in the user interface rather than in configuration files.
Horizon Agent (remote desktop with Windows operating system)	Security-related settings appear only in the Windows Registry.
Linux desktop	You can use a text editor to open the following configuration file and specify TLS-related settings: `/etc/vmware/viewagent-custom.conf`

Accounts

Client users must have accounts in Active Directory.

Horizon Client User Accounts

In Active Directory, configure user accounts for users that need to access remote desktops and published applications. If you plan to use the RDP protocol, the user accounts must be members of the Remote Desktop Users group.

As a general rule, do not make end users Horizon administrators. If a Horizon administrator must verify the user experience, create and entitle a separate test account. On remote desktops, do not make end users members of privileged groups, such as Administrators. These users can modify locked-down configuration files and the Windows Registry.

System Accounts Created During Installation

Horizon Client does not create service user accounts on any type of client. For the services that Horizon Client for Windows creates, the login ID is Local System.

On Mac clients, users must grant Local Admin access to start the USB service the first time that Horizon Client starts. After the service starts for the first time, the standard user has execution access. Similarly, on a Linux client, if a user clicks the **Register and start the service(s) after installation** check box during installation, the `vmware-usbarbitrator` and `vmware-view-used` daemons start automatically. These processes run as root.

Horizon Agent does not create any service user accounts on Windows desktops. On Linux desktops, it creates a system account called `vmwblast`. 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. To access these settings for remote desktops and Windows clients, you can use group policy objects or Windows registry settings.

For configuration settings related to log collection, see the *Horizon Administration* document. 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. Administrators can also configure whether end users can control whether client connections are rejected if server certificate checks fail.

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

- End users can choose the verification mode.
- (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 select whether 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. A mismatch can also occur 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 that the client environment sends 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.

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 Horizon Agent Configuration Templates

The ADM and ADMX template files for Horizon Agent, `vdm_agent.adm` and `vdm_agent.admx`, contain security-related settings for Horizon Agent. Unless otherwise noted, these files include only Computer Configuration settings.

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

Table 4-1. Horizon Agent Security-Related Settings

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. Horizon Agent Security-Related Settings (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 *Configuring Remote Desktop Features in Horizon* document.

Setting Options in Configuration Files on a Linux Desktop

For Linux desktops, you can configure certain options by adding entries to the `/etc/vmware/config` file or the `/etc/vmware/viewagent-custom.conf` file.

During Horizon Agent installation, 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`. All the configuration options are listed and documented in the configuration files. To set an option, 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 to make the changes take effect.

Configuration Options in /etc/vmware/config

The VMware BlastServer and BlastProxy processes, along with their related plug-ins and processes, use the `/etc/vmware/config` configuration file.

Note The following table includes descriptions of each agent-enforced policy setting for USB devices in the Horizon Agent configuration file. Horizon Agent uses these settings to decide whether a USB device can be forwarded to the host machine. Horizon Agent also passes these 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
appScanner	`error`, `warn`, `info`, or `debug`	`info`	Use this option to specify the reported in the appScanner l records activity related to re sessions. Valid values range detailed "error" level to the m "debug" level. The appScanner log is locate `vmware-root/vmware-appSca` where <pid> is the ID of the process.
BlastProxy.log.logLevel	`error`, `warn`, `info`, `verbose`, `debug`, or `trace`	`info`	Use this option to specify the reported in the BlastProxy lo values range from the least d level to the most detailed "tr The BlastProxy log is located `root/vmware-BlastProxy-<p` <pid> is the ID of the BlastPr
BlastProxy.UdpEnabled	`true` or `false`	`true`	Use this option to specify wh forwards UDP requests throu 22443 to Horizon Agent. `true` forwarding. `false` deactivates forwarding.
cdrserver.cacheEnable	`true` or `false`	`true`	Set this option to enable or d write caching feature from th 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 redirection shared folder loca default `/home/`*`user`*`/tsclien` custom directory. For example, if the user `test` the client drive redirection sh at `/mnt/test/tsclient` inste `test/tsclient`, the user can **`cdrserver.customizedShare mnt/`**. **Note** For this option to take specified folder must exist ar with the correct user permiss
cdrserver.forcedByAdmin	`true` or `false`	`false`	Set this option to control whe can share additional folders t specified with the `cdrserver.` option.
cdrserver.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log `vmware-CDRserver.log` file.
cdrserver.permissions	`R`	`RW`	Use this option to apply addi permissions that Horizon Age folders shared by Horizon Cli ■ If the folder shared by Ho `read` and `write` permissio **`cdrserver.permissions=`** Agent has only `read` acce ■ If the folder shared by Ho only `read` permissions an **`cdrserver.permissions=`** Agent still has only `read` Horizon Agent cannot ch only attribute set by Hori Horizon Agent can only r access rights. Typical uses are as follows: ■ **`cdrserver.permissions=`** ■ **`#cdrserver.permissions`** comment it out or delete
cdrserver.sharedFolders	*`file_path1`*`,R;`*`file-path2`*`,;` *`file_path3`*`,R; ...`	undefined	Specify one or more file path that the client can share with desktop. For example: ■ For a Windows client: **`C:\spreadsheets,;D:\eb`** ■ For a non-Windows client: **`/tmp/spreadsheet ebooks,;/home/finance,`**

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

Option	Value/Format	Default	Description
Clipboard.Direction	`0`, `1`, `2`, or `3`	`2`	Use this option to specify the redirection policy. Valid value ■ 0 - Deactivate clipboard ■ 1 - Enable clipboard redir directions. ■ 2 - Enable clipboard redir client to the remote desk ■ 3 - Enable clipboard redir remote desktop to the cli
collaboration.enableControlPassing	`true` or `false`	`true`	Set this option to permit or re collaborators from having co desktop. To specify a read-o session, set this option to **fa**
collaboration.enableEmail	`true` or `false`	`true`	Set this option to enable or d sending of collaboration invit an installed email application option is disabled, you canno invite collaborators, even if a application is installed.
collaboration.logLevel	`error`, `info`, or `debug`	`info`	Use this option to set the log the collaboration session. If t `debug`, all calls made to `collab` the contents of the `collabor`
collaboration.maxCollabors	An integer less than or equal to 20	5	Specifies the maximum numb collaborators that you can in session.
collaboration.serverUrl	[URL]	undefined	Specifies the server URLs to collaboration invitations.
Desktop.displayNumberMax	An integer	`159`	Specifies the upper limit of th Window System display num to user sessions. This feature on SLED/SLES desktops. To restrict the allocation to a number, set `Desktop.displayN` `Desktop.displayNumberMin` to t **Note** If you specify a range of the display numbers 0 thro might occur with X server. Us workaround described in VM Base (KB) article 81704.

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

Option	Value/Format	Default	Description
Desktop.displayNumberMin	An integer	`100`	Specifies the lower limit of th Window System display num to user sessions. This feature on SLED/SLES desktops. To restrict the allocation to a number, set `Desktop.displayN` `Desktop.displayNumberMin` to t **Note** If you specify a range of the display numbers 0 thro might occur with X server. Us workaround described in VM Base (KB) article 81704.
mksVNCServer.useUInputButtonMapping	`true` or `false`	`false`	Set this option to enable the handed mouse on Ubuntu or do not need to set this optio which provides native suppo handed mouse.
mksvhan.clipboardSize	An integer	1024	Use this option to specify the maximum size to copy and p
rdeSvc.allowDisplayScaling	`true` or `false`	`false`	Set this option to enable or d scaling, which changes the si and navigation elements.
rdeSvc.blockedWindows	List of semicolon-separated paths to application executables	N/A	Use this option to block spec from starting as a remote ap Specify the path to each app executable and use semicolo entries in the list. For exampl **`rdeSvc.blockedWindows=/us gnome-terminal-server;`**
rdeSvc.enableOptimizedResize	`true` or `false`	`true`	Set this option to enable or d optimized window resizing fo application sessions in Horizo Windows. When this option i Windows client users can res application windows without screen artifacts.
RemoteDisplay.allowAudio	`true` or `false`	`true`	Set this option to enable or d out.
RemoteDisplay.allowH264	`true` or `false`	`true`	Set this option to enable or d encoding.
RemoteDisplay.allowH264YUV444	`true` or `false`	`true`	Set this option to enable or d YUV 4:4:4 encoding with Hig if the client supports it.
RemoteDisplay.allowHEVC	`true` or `false`	`true`	Set this option to enable or d Efficiency Video Coding (HEV

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

Option	Value/Format	Default	Description
RemoteDisplay.allowHEVCYUV444	`true` or `false`	`true`	Set this option to enable or d YUV 4:4:4 with High Color Ac client supports it.
RemoteDisplay.allowVMWKeyEvent2Unicode	`true` or `false`	`true`	Set this option to allow or no Agent to process Unicode ev representing keyboard input When this option is enabled, send Unicode values represe input to the remote desktop. not support Unicode input na Agent first converts the Unic KeyCodes and then sends th the operating system to disp appropriate Unicode charact When this option is disabled, does not handle any Unicode from clients.
RemoteDisplay.buildToPNG	`true` or `false`	`false`	Graphic applications, especia design applications, require p rendering of images in the cli Linux desktop. You can confi lossless PNG mode for image playback that are generated desktop and rendered on the This feature uses additional b between the client and the E Enabling this option deactiva encoding.
RemoteDisplay.enableNetworkContinuity	`true` or `false`	`true`	Set this option to enable or d Network Continuity feature in for Linux.
RemoteDisplay.enableNetworkIntelligence	`true` or `false`	`true`	Set this option to enable or d Network Intelligence feature for Linux.
RemoteDisplay.enableStats	`true` or `false`	`false`	Enables or deactivates the V display protocol statistics in r bandwidth, FPS, RTT, and so
RemoteDisplay.enableUDP	`true` or `false`	`true`	Set this option to enable or d protocol support in Horizon A
RemoteDisplay.maxBandwidthKbps	An integer	1000000	Specifies the maximum band per second (kbps) for a VMw session. The bandwidth inclu audio, virtual channel, and VM control traffic. Valid value mu Gbps (4096000).

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

Option	Value/Format	Default	Description
RemoteDisplay.minBandwidthKbps	An integer	256	Specifies the minimum bandw per second (kbps) for a VMw session. The bandwidth inclu audio, virtual channel, and VI control traffic.
RemoteDisplay.maxFPS	An integer	30	Specifies the maximum rate c updates. Use this setting to r average bandwidth that user value must be between 3 and is 30 updates per second.
RemoteDisplay.maxQualityJPEG	available range of values: 1–100	90	Specifies the image quality o display for JPEG/PNG encod quality settings are for areas that are more static, resulting image quality.
RemoteDisplay.midQualityJPEG	available range of values: 1–100	35	Specifies the image quality o display for JPEG/PNG encod the medium-quality settings display.
RemoteDisplay.minQualityJPEG	available range of values: 1–100	25	Specifies the image quality o display for JPEG/PNG encod quality settings are for areas that change often, for examp scrolling occurs.
RemoteDisplay.qpmaxH264	available range of values: 0–51	36	Use this option to set the H2 quantization parameter, whic best image quality for the re configured to use H.264 or H Set the value to greater than RemoteDisplay.qpminH264.
RemoteDisplay.qpminH264	available range of values: 0–51	10	Use this option to set the H2 quantization parameter, whic lowest image quality for the configured to use H.264 or H Set the value to less than the RemoteDisplay.qpmaxH264.
UsbRedirPlugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log Redirection plug-in.
UsbRedirServer.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log Redirection server.
vdpservice.log.logLevel	`fatal error`, `warn`, `info`, `debug`, or `trace`	`info`	Use this option to set the log `vdpservice`.
viewusb.AllowAudioIn	**`{m|o}:{true|false}`**	undefined, which equates to `true`	Use this option to allow or di input devices to be redirecte **`o:false`**

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

Option	Value/Format	Default	Description
viewusb.AllowAudioOut	**{m|o}:{true|false}**	undefined, which equates to `false`	Set this option to allow or dis of audio output devices.
viewusb.AllowAutoDeviceSplitting	**{m|o}:{true|false}**	undefined, which equates to `false`	Set this option to allow or dis automatic splitting of compo Example: **m:true**
viewusb.AllowDevDescFailsafe	**{m|o}:{true|false}**	undefined, which equates to `false`	Set this option to allow or dis be redirected even if Horizon get the configuration or devi To allow a device even if it fa configuration or device descr in the Include filters, such as or **IncludePath**.
viewusb.AllowHIDBootable	**{m|o}:{true|false}**	undefined, which equates to `true`	Use this option to allow or di redirection of input devices c keyboards or mice that are a time, also known as HID-boot
viewusb.AllowKeyboardMouse	**{m|o}:{true|false}**	undefined, which equates to `false`	Use this option to allow or di redirection of keyboards with pointing devices (such as a m or touch pad).
viewusb.AllowSmartcard	**{m|o}:{true|false}**	undefined, which equates to `false`	Set this option to allow or dis devices to be redirected.
viewusb.AllowVideo	**{m|o}:{true|false}**	undefined, which equates to `true`	Use this option to allow or di devices to be redirected.
viewusb.DisableRemoteConfig	**{m|o}:{true|false}**	undefined, which equates to `false`	Set this option to deactivate of Horizon Agent settings wh USB device filtering.
viewusb.ExcludeAllDevices	**{true|false}**	undefined, which equates to `false`	Use this option to exclude or devices from being redirecte you can use other policy sett specific devices or families o redirected. If set to **false**, yo policy settings to prevent spe families of devices from bein you set the value of **Exclude true** on Horizon Agent, and t passed to Horizon Client, the setting overrides the Horizon

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

Option	Value/Format	Default	Description
viewusb.ExcludeFamily	`{m|o}:family_name_1[;family_name_2;...]`	undefined	Use this option to exclude fa from being redirected. For ex `m:bluetooth;smart-card` If you have enabled automat splitting, Horizon examines th of each interface of a compo to decide which interfaces m If you have deactivated auto splitting, Horizon examines th of the whole composite USB **Note** Mice and keyboards a redirection by default and do excluded with this setting.
viewusb.ExcludePath	`{m|o}:bus-x1[/y1].../ port-z1[;bus-x2[/y2].../port-z2;...]`	undefined	Use this option to exclude de specified hub or port paths fr redirected. You must specify numbers in hexadecimal. You wildcard character in paths. For example:`m:bus-1/2/3_port-02;bus-1/1/1/4_port-ff`
viewusb.ExcludeVidPid	`{m|o}:vid-xxx1_ pid-yyy1[;vid-xxx2_pid-yyy2;..]`	undefined	Set this option to exclude de specified vendor and produc redirected. You must specify hexadecimal. You can use th character (*) in place of indiv ID. For example: `o:vid-0781_pid- ****;vid-`
viewusb.IncludeFamily	`{m|o}:family_name_1[;family_name_2]...`	undefined	Set this option to include fam that can be redirected. For example: `o:storage; sm`
viewusb.IncludePath	`{m|o}:bus-x1[/y1].../ port-z1[;bus-x2[/y2].../portz2;...]`	undefined	Use this option to include de hub or port paths that can be must specify bus and port nu hexadecimal. You cannot use character in paths. For example: `m:bus-1/2_port- 02;bus-1/`
viewusb.IncludeVidPid	`{m|o}:vid-xxx1_ pid-yyy1[;vid-xxx2_pid-yyy2;...]`	undefined	Set this option to include dev specified Vendor and Produc redirected. You must specify hexadecimal. You can use th character (*) in place of indiv ID. For example: `o:vid-***_pid-0001;vid-05`

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 specified composite USB dev by Vendor and Product IDs. setting is **vid-*xxx1*_pid-*yyy1*[;vid-*xx* *yyy2*;...]**. You must specify hexadecimal. You can use th character (*) in place of indiv ID. Example: **m:vid-0f0f_pid-5**
viewusb.SplitVidPid	**{m|o}: vid-*xxxx*_pid-*yyyy*([exintf:*zz*[;exintf:*ww*]])[;...]**	undefined	Set this option to treat the co composite USB device specif and Product IDs as separate format of the setting is **vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*]** You can use the **exintf** keyw components from redirection their interface number. You n numbers in hexadecimal, and numbers in decimal including zero. You can use the wildca place of individual digits in ar Example: **o:vid-0f0f_pid-***(exintf-01);vid-0781_p 01;exintf:02)** **Note** VMware Horizon does components that you have n excluded automatically. You filter policy such as **Include** to include those components
VMWPkcs11Plugin.log.enable	`true` or `false`	`false`	Set this option to enable or d logging mode for the True SS
VMWPkcs11Plugin.log.logLevel	`error`, `warn`, `info`, `debug`, `trace`, or `verbose`	`info`	Use this option to set the log True SSO feature.
VVC.RTAV.Enable	`true` or `false`	`true`	Set this option to enable/disa
VVC.ScRedir.Enable	`true` or `false`	`true`	Set this option to enable/dea card redirection.
VVC.logLevel	`fatal error`, `warn`, `info`, `debug`, or `trace`	`info`	Use this option to set the log proxy node.

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 deactivate the client drive redirection feature.
CollaborationEnable	`true` or `false`	`true`	Use this option to enable or deactivate the Session Collaboration feature on Linux desktops.
DPISyncEnable	`true` or `false`	`true`	Set this option to enable or deactivate the DPI Synchronization feature, which ensures that the DPI setting in the remote desktop matches the client system's DPI setting.
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.
HelpDeskEnable	`true` or `false`	`true`	Set this option to enable or deactivate 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 deactivated, 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.
MaxSessionsBuffer	An integer between 1 and the value specified for **Max Sessions Per RDS Host** in the farm configuration wizard.	`5`	When configuring farms and multi-session desktop pools, use this option to specify the number of pre-launched desktops per host machine.

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

Option	Value	Default	Description
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`
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 by the OpenSSL standard. To find information about the OpenSSL-defined format, type these keywords into an Internet search engine: **`openssl cipher string`**.
SSLProtocols	A text string	TLSv1_1:TLSv1_2	Use this option to specify the security protocols. The supported protocols are TLSv1.1 and TLSv1.2.

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

Option	Value	Default	Description
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 desktop, the option takes effect regardless if the SSO feature is enabled or not. If this option is specified in a RHEL/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.x desktops. VMware Horizon supports only the Gnome desktop environment on RHEL/CentOS 8.x desktops.
SSOEnable	`true` or `false`	`true`	Set this option to enable/deactivate 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 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 to connect to Horizon Agent for Linux. You must specify the value in the CIDR IP address format. For example, Subnet=123.456.7.8/24.
DEMEnable	`true` or `false`	`false`	Set this option to enable or deactivate smart policies created in Dynamic Environment Manager. If the option is set to enable, and the condition in a smart policy is met, then the policy is enforced.
DEMNetworkPath	A text string		This option must be set to the same network path that is set in the Dynamic Environment Manager Console. The path must be in the format similar to `//10.111.22.333/view/LinuxAgent/DEMConfig`. The network path must correspond to a public, shared folder which does not require user name and password credentials for access.

Note The VMwareBlastServer process uses the SSLCiphers, SSLProtocols, and SSLCipherServerPreference security options. 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

The ADM and ADMX template files for VMware Blast, `vdm_blast.adm` and `vdm_blast.admx`, contain group policy settings for HTML Access. The VMware Blast display protocol is the only display protocol that HTML Access uses.

The VMware Blast group policy settings are described in the *Configuring Remote Desktop Features in Horizon* document.

Security Settings in the Horizon Client Configuration Templates

The ADM and ADMX template files for Horizon Client, `vdm_client.adm` and `vdm_client.admx`, contain security-related settings. These settings appear in the Security and Scripting Definitions sections in the Group Policy Management Editor. Unless otherwise noted, these files include only Computer Configuration settings. If a User Configuration setting is available, and you define a value for it, it overrides the equivalent Computer Configuration setting.

For information about these settings and their security implications, see "Security Settings for Client GPOs" in the *VMware Horizon Client for Windows Installation and Setup Guide* document.

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.

Using the Legacy Microsoft CryptoAPI Standard

By default Horizon uses the Microsoft Cryptography API: Next Generation (CNG) standard. If you have a use case requiring use of the legacy CryptoAPI standard, you can do so.

To revert to the legacy CryptoAPI standard, change the `HKLM\Software\VMware, Inc.\VMware VDM \Agent\Configuration\UseCryptoAPI` registry key value to `true`.

Configuring Security Protocols and Cipher Suites

5

You can configure the security protocols and cipher suites that are accepted and proposed between 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 table lists the protocols and cipher suites that are enabled by default for Horizon Client. In Horizon Client 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 Horizon Agent). RC4 is not supported.

Table 5-1. Security Protocols and Cipher Suites Enabled by Default in Horizon Client

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_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) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Configuring Security Protocols and Cipher Suites for Specific Client Types

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

Change the security protocols in Horizon Client only if your Connection Server instance does not support the current settings. If you configure a security protocol for Horizon Client that is not enabled on the Connection Server instance to which the client connects, a TLS error occurs and the connection fails.

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

- On Windows clients, you can use either a group policy setting or a Windows Registry setting.
- On Linux clients, you can use either configuration file properties or command-line options.
- On Mac clients, you can use a preference setting in Horizon Client.
- On iOS and Android clients, you can use the advanced SSL options setting in Horizon Client.

For more information, see the Horizon Client documentation.

Disable Weak Ciphers in SSL/TLS

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

Procedure

1. To edit the GPO on the Active Directory server, select **Start > Administrative Tools > Group Policy Management**, right-click the GPO, and select **Edit**.
2. In the Group Policy Management Editor, navigate to **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_GCM_SHA256,
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
   ```

   The cipher suites appear 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.

   Note In FIPS mode, list GCM cipher suites only.

6 Exit the Group Policy Management Editor.

7 To make the new group policy take effect, restart the Horizon Agent machines.

Configure Security Protocols and Cipher Suites for HTML Access Agent

You can configure the cipher suites and security protocols that the HTML Access Agent uses. You can also specify the configurations in a group policy object (GPO).

By default, the HTML Access Agent uses only 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 the HTML Access Agent accepts. For example, setting `SslProtocolLow=tls_1.1` and `SslProtocolHigh=tls_1.2` causes the HTML Access Agent to accept TLS 1.1 and TLS 1.2. The default settings are `SslProtocolLow=tls_1.2` and `SslProtocolHigh=tls_1.2`, and therefore by default the HTML Access Agent accepts only TLS 1.2.

You must use the proper cipher list format when specifying the list of ciphers. To see the cipher list format, you can search for **`openssl cipher string`** in a web browser. The following cipher list is the default:

```
ECDHE+AESGCM
```

Procedure

1 Start the Windows Registry Editor.

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

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

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

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

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 VMware Blast Windows service.

Results

To revert to using the default cipher list, delete the `SslCiphers` registry value and restart the Windows service VMware Blast. Do not delete the data part of the value. If you delete the data part of the value, the HTML Access Agent treats 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.

Note The default protocols and cipher suites might change in accordance with evolving best practices for network security.

Configure Proposal Policies on Remote Desktops

To control the security of Message Bus connections to Connection Server, you can configure the proposal policies on remote desktops that run Windows.

Prerequisites

To avoid a connection failure, configure Connection Server to accept the same policies.

Procedure

1. On the remote desktop, start the Windows Registry Editor.
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
   ```

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 must 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
   ```

Applying Security Patches

6

Patch releases might include installer files for Connection Server, Horizon Agent, and Horizon Client. 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 VMware Horizon components, in the following order:

1 Connection Server

2 Horizon Agent

3 Horizon Client

For information about upgrading Connection Server and Horizon Agent, see the *Horizon Upgrades* document.

For information about upgrading Horizon Client, see the Horizon Client documentation.