Horizon Security

VMware Horizon 2106

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

https://docs.vmware.com/

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

Contents

VMware Horizon Security

Horizon Security provides a concise reference to the security features of VMware Horizon.

- Required system and database login accounts.
- 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.
- External interfaces, ports, and services that must be open or enabled for the correct operation of VMware Horizon.

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of VMware Horizon.

VMware Horizon Accounts, Resources, and Log Files

1

Having different accounts for specific components protects against giving individuals more access and permissions than they need. Knowing the locations of configuration files and other files with sensitive data aids in setting up security for various host systems.

This chapter includes the following topics:

VMware Horizon Accounts

You must set up system and database accounts to administer VMware Horizon components.

Table 1-1. VMware Horizon System Accounts

Horizon Component	Required Accounts
Horizon Client	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, but the accounts do not require Horizon administrator privileges.
vCenter Server	Configure a user account in Active Directory with permission to perform the operations in vCenter Server that are necessary to support VMware Horizon. For information about the required privileges, see the *Horizon Installation* document.
Connection Server	When you install VMware Horizon, you can specify a specific domain user, the local Administrators group, or a specific domain user group as Horizon administrators. We recommend creating a dedicated domain user group of Horizon administrators. The default is the currently logged in domain user. In Horizon Console, you can use **Settings > Administrators** to change the list of Horizon administrators. See the *Horizon Administration* document for information about the privileges that are required.

Table 1-2. Horizon Database Accounts

Horizon Component	Required Accounts
Event database used by Horizon Connection Server	A Microsoft SQL Server, Oracle, or PostgreSQL database stores Horizon event data. You create an administrative account for the database that Horizon Console can use to access the event data.

To reduce the risk of security vulnerabilities, take the following actions:

- Configure VMware Horizon databases on servers that are separate from other database servers that your organization uses.
- Do not allow a single user account to access multiple databases.
- Configure a separate account for access to the event database.

VMware Horizon Resources

VMware Horizon includes several configuration files and similar resources that must be protected.

Table 1-3. Horizon Connection Server Resources

Resource	Location	Protection
LDAP settings	Not applicable.	LDAP data is protected automatically as part of role-based access control.
LDAP backup files	`%ProgramData%\VMWare\VDM\backups`	Protected by access control.
`locked.properties` (secure gateway configuration file)	*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf`	Ensure that this file is secured against access by any user other than Horizon administrators.
`absg.properties` (Blast Secure Gateway configuration file)	*`install_directory`*`\VMware\VMware View\Server\appblastgateway`	Ensure that this file is secured against access by any user other than Horizon administrators.
Log files	See VMware Horizon Log Files	Protected by access control.
`web.xml` (Tomcat configuration file)	*`install_directory`*`\VMware View\Server\broker\web apps\ROOT\Web INF`	Protected by access control.

VMware Horizon Log Files

VMware Horizon creates log files that record the installation and operation of its components.

Note VMware Horizon log files are intended for use by VMware Support. VMware recommends that you configure and use the event database to monitor VMware Horizon. For more information, see the *Horizon Installation* and *Horizon Administration* documents.

Table 1-4. VMware Horizon Log Files

Horizon Component	File Path and Other Information
All components (installation logs)	*%TEMP%*\vminst.log_*date_timestamp* *%TEMP%*\vmmsi.log_*date_timestamp*
Horizon Agent	*<Drive Letter>*:\ProgramData\VMware\VDM\logs To access VMware Horizon log files that are stored in *<Drive Letter>*:\ProgramData\VMware\VDM\logs, you must open the logs from a program with elevated administrator privileges. Right-click the program file and select **Run as administrator**. If a User Data Disk (UDD) is configured, *<Drive Letter>* might correspond to the UDD. The logs for PCoIP are named pcoip_agent*.log and pcoip_server*.log.
Remote Desktop Features	You can set log levels and generate log files in a Data Collection Tool (DCT) bundle for remote desktop features on Windows Agent and Client, Mac Client, and Linux Client. Windows Agent: C:\Program Files\VMware\VMware View\Agent\DCT\support.bat Windows Client: C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat Mac Client: /Applications/VMware Horizon Client.app/Contents/Library/dct/HorizonCollector.sh Linux Client: /usr/bin/vmware-view-log-collector
Published Applications	The Horizon Event Database configured on a Microsoft SQL Server, Oracle database server, or PostgreSQL database server. Windows Application Event logs. Disabled by default.
Connection Server	*<Drive Letter>*:\ProgramData\VMware\log\ConnectionServer. **Note** This file path is a symbolic link that redirects to the actual location of the log files, which is *<Drive Letter>*:\ProgramData\VMware\VDM\logs. The log directory is configurable in the log configuration settings of the Common Configuration ADMX template file (vdm_common.admx) . PCoIP Secure Gateway logs are written to files named SecurityGateway_*.log in the PCoIP Secure Gateway subdirectory. Blast Secure Gateway logs are written to files named absg*.log in the Blast Secure Gateway subdirectory.
Horizon Services	Horizon Event Database configured on a Microsoft SQL Server, Oracle database server, or PostgreSQL database server. Windows System Event logs.

VMware Horizon Security Settings 2

VMware Horizon includes several settings that you can use to adjust the security of the configuration. You can access the settings by using Horizon Console or by using the ADSI Edit utility, as appropriate.

Note For information about security settings for Horizon Client and Horizon Agent, see the *Horizon Client and Agent Security* document.

This chapter includes the following topics:

Security-Related Global Settings in Horizon Console

Security-related global settings for client sessions and connections are accessible under **Settings > Global Settings > Security Settings** or under **Settings > Global Settings > General Settings** in Horizon Console.

Table 2-1. Security-Related Global Settings

Setting	Description
Change data recovery password	The password is required when you restore the Horizon LDAP configuration from an encrypted backup. When you install Connection Server, you provide a data recovery password. After installation, you can change this password in Horizon Console. When you back up Connection Server, the Horizon LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup with the `vdmimport` utility, you must provide the data recovery password. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.
Message security mode	Determines the security mechanism used when JMS messages are passed between VMware Horizon components. ■ If set to **Disabled**, message security mode is disabled. ■ If set to **Enabled**, legacy message signing and verification of JMS messages takes place. VMware Horizon components reject unsigned messages. This mode supports a mix of TLS and plain JMS connections. ■ If set to **Enhanced**, TLS is used for all JMS connections, to encrypt all messages. Access control is also enabled to restrict the JMS topics that VMware Horizon components can send messages to and receive messages from. ■ If set to **Mixed**, message security mode is enabled, but not enforced for VMware Horizon components. The default setting is **Enhanced** for new installations. If you upgrade from a previous version, the setting used in the previous version is retained. **Important** VMware strongly recommends setting the message security mode to **Enhanced** after you upgrade all Connection Server instances and VMware Horizon desktops to this release. The **Enhanced** setting provides many important security improvements and MQ (message queue) updates.
Enhanced Security Status (Read-only)	Read-only field that appears when **Message security mode** is changed from **Enabled** to **Enhanced**. Because the change is made in phases, this field shows the progress through the phases: ■ **Waiting for Message Bus restart** is the first phase. This state is displayed until you manually restart either all Connection Server instances in the pod or the VMware Horizon Message Bus Component service on all Connection Server hosts in the pod. ■ **Pending Enhanced** is the next state. After all Horizon Message Bus Component services have been restarted, the system begins changing the message security mode to **Enhanced** for all desktops. ■ **Enhanced** is the final state, indicating that all components are now using **Enhanced** message security mode.
Reauthenticate secure tunnel connections after network interruption	Determines if user credentials must be reauthenticated after a network interruption when Horizon Clients use secure tunnel connections to VMware Horizon desktops and applications. This setting offers increased security. For example, if a laptop is stolen and moved to a different network, the user cannot automatically gain access to the VMware Horizon desktops and applications because the network connection was temporarily interrupted. This setting is disabled by default.

Table 2-1. Security-Related Global Settings (continued)

Setting	Description
Forcibly disconnect users	Disconnects all desktops and applications after the specified number of minutes has passed since the user logged in to VMware Horizon. All desktops and applications will be disconnected at the same time regardless of when the user opened them. The default is 600 minutes.
For clients that support applications. **If the user stops using the keyboard and mouse, disconnect their applications and discard SSO credentials**	Protects application sessions when there is no keyboard or mouse activity on the client device. If set to **After ... minutes**, VMware Horizon disconnects all applications and discards SSO credentials after the specified number of minutes without user activity. Desktop sessions are disconnected. Users must log in again to reconnect to the applications that were disconnected or launch a new desktop or application. If set to **Never**, VMware Horizon never disconnects applications or discards SSO credentials due to user inactivity. The default is **Never**.
Other clients. **Discard SSO credentials**	Discards the SSO credentials after a certain time period. This setting is for clients that do not support application remoting. If set to **After ... minutes**, users must log in again to connect to a desktop after the specified number of minutes has passed since the user logged in to VMware Horizon, regardless of any user activity on the client device. The default is **After 15 minutes**.
View Administrator session timeout	Determines how long an idle Horizon Console session continues before the session times out. **Important** Setting the Horizon Console session timeout to a high number of minutes increases the risk of unauthorized use of Horizon Console. Use caution when you allow an idle session to persist a long time. By default, the Horizon Console session timeout is 30 minutes. You can set a session timeout from 1 to 4320 minutes.

Note TLS is required for all Horizon Client connections and Horizon Console connections to VMware Horizon. If your VMware Horizon deployment uses load balancers or other client-facing, intermediate servers, you can off-load TLS to them and then configure non-TLS connections on individual Connection Server instances. See "Off-load TLS Connections to Intermediate Servers" in the *Horizon Administration* document.

Change the Data Recovery Password

You provide a data recovery password when you install Connection Server. After installation, you can change this password in Horizon Console. The password is required when you restore the Horizon LDAP configuration from a backup.

When you back up Connection Server, the Horizon LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup VMware Horizon configuration, you must provide the data recovery password.

The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.

Procedure

1 In Horizon Console, select **Settings > Global Settings**.

2 On the **Security Settings** tab, click **Change data recovery password**.

3 Type and retype the new password.

4 (Optional) Type a password reminder.

Results

Note You can also change the data recovery password when you schedule your VMware Horizon configuration data to be backed up. See "Schedule Horizon Configuration Backups" in the *Horizon Administration* document.

What to do next

When you use the `vdmimport` utility to restore a backup VMware Horizon configuration, provide the new password.

Message Security Mode for Horizon Components

You can set the message security mode to specify the security mechanism used when JMS messages pass among VMware Horizon components.

The following table shows the options you can select to configure the message security mode. To set an option, select it from the **Message security mode** list on the **Security Settings** tab on the **Global Settings** page.

Table 2-2. Message Security Mode Options

Option	Description
Disabled	Message security mode is disabled.
Mixed	Message security mode is enabled but not enforced. You can use this mode to detect older components in your VMware Horizon environment. The log files generated by Connection Server contain references to these components. This setting is not recommended. Use this setting only to discover components that need to be upgraded.
Enabled	Message security mode is enabled, using a combination of message signing and encryption. JMS messages are rejected if the signature is missing or invalid, or if a message was modified after it was signed. Some JMS messages are encrypted because they carry sensitive information such as user credentials. If you use the **Enabled** setting, you can also use IPSec to encrypt all JMS messages between Connection Server instances, and between Connection Server instances and Unified Access Gateway appliances.
Enhanced	SSL is used for all JMS connections. JMS access control is also enabled so that desktops and Connection Server instances can only send and receive JMS messages on certain topics.

When you first install VMware Horizon on a system, the message security mode is set to **Enhanced**. If you upgrade VMware Horizon from a previous release, the message security mode remains unchanged from its existing setting.

Important If you plan to change an upgraded VMware Horizon environment from **Enabled** to **Enhanced**, you must first upgrade all Connection Server instances and VMware Horizon desktops. After you change the setting to **Enhanced**, the new setting takes place in stages.

1. You must manually restart the VMware Horizon Message Bus Component service on all Connection Server hosts in the pod, or restart the Connection Server instances.
2. After the services are restarted, the Connection Server instances reconfigure the message security mode on all desktops, changing the mode to **Enhanced**.
3. To monitor the progress in Horizon Console, go to **Settings > Global Settings**.

   On the **Security Settings** tab, the **Enhanced Security Status** item will show **Enhanced** when all components have made the transition to Enhanced mode.

   Alternatively, you can use the `vdmutil` command-line utility to monitor progress. See Using the vdmutil Utility to Configure the JMS Message Security Mode.

If you plan to change an active VMware Horizon environment from **Disabled** to **Enabled**, or from **Enabled** to **Disabled**, change to **Mixed** mode for a short time before you make the final change. For example, if your current mode is **Disabled**, change to **Mixed** mode for one day, then change to **Enabled**. In **Mixed** mode, signatures are attached to messages but not verified, which allows the change of message mode to propagate through the environment.

Using the vdmutil Utility to Configure the JMS Message Security Mode

You can use the `vdmutil` command-line interface to configure and manage the security mechanism used when JMS messages are passed between VMware Horizon components.

Syntax and Location of the Utility

The `vdmutil` command can perform the same operations as the `lmvutil` command that was included with earlier versions of VMware Horizon. In addition, the `vdmutil` command has options for determining the message security mode being used and monitoring the progress of changing all VMware Horizon components to Enhanced mode. Use the following form of the `vdmutil` command from a Windows command prompt.

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

The additional options that you can use depend on the command option. This topic focuses on the options for message security mode. For the other options, which relate to Cloud Pod Architecture, see the *Administering Cloud Pod Architecture in Horizon* document.

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

Authentication

You must run the command as a user who has the Administrators role. You can use Horizon Console to assign the Administrators role to a user. See "Configuring Role-Based Delegated Administration" in the *Horizon Administration* document.

The `vdmutil` command includes options to specify the user name, domain, and password to use for authentication.

Table 2-3. vdmutil Command Authentication Options

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

You must use the authentication options with all `vdmutil` command options except for `--help` and `--verbose`.

Options Specific to JMS Message Security Mode

The following table lists only the `vdmutil` command-line options that pertain to viewing, setting, or monitoring the JMS message security mode. For a list of the arguments you can use with a specific option, use the `--help` command-line option.

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

Table 2-4. vdmutil Command Options

Option	Description
`--activatePendingConnectionServerCertificates`	Activates a pending security certificate for a Connection Server instance in the local pod.
`--countPendingMsgSecStatus`	Counts the number of machines preventing a transition to or from Enhanced mode.
`--createPendingConnectionServerCertificates`	Creates a new pending security certificate for a Connection Server instance in the local pod.
`--getMsgSecLevel`	Gets the enhanced message security status for the local pod. This status pertains to the process of changing the JMS message security mode from **Enabled** to **Enhanced** for all the components in a VMware Horizon environment.
`--getMsgSecMode`	Gets the message security mode for the local pod.

Table 2-4. vdmutil Command Options (continued)

Option	Description
`--help`	Lists the `vdmutil` command options. You can also use `--help` on a particular command, such as `--setMsgSecMode --help`.
`--listMsgBusSecStatus`	Lists the message bus security status for all connection servers in the local pod.
`--listPendingMsgSecStatus`	List machines preventing a transition to or from Enhanced mode. Limited to 25 entries by default.
`--setMsgSecMode`	Sets the message security mode for the local pod.
`--verbose`	Enables verbose logging. You can add this option to any other option to obtain detailed command output. The `vdmutil` command writes to standard output.

Security-Related Server Settings in Horizon Console

Security-related server settings are accessible under **Settings > Servers** in Horizon Console.

Table 2-5. Security-Related Server Settings

Setting	Description
Use PCoIP Secure Gateway for PCoIP connections to machine	Determines whether Horizon Client makes a further secure connection to the Connection Server host when users connect to VMware Horizon desktops and applications with the PCoIP display protocol. If this setting is disabled, the desktop or application session is established directly between the client and the VMware Horizon desktop or the Remote Desktop Services (RDS) host, bypassing the Connection Server host. This setting is disabled by default.
Use Secure Tunnel connection to machine	Determines whether Horizon Client makes a further HTTPS connection to the Connection Server host when users connect to an VMware Horizon desktop or an application. If this setting is disabled, the desktop or application session is established directly between the client and the VMware Horizon desktop or the Remote Desktop Services (RDS) host, bypassing the Connection Server host. This setting is enabled by default.
Use Blast Secure Gateway for Blast connections to machine	Determines whether clients that use a Web browser or the Blast Extreme display protocol to access desktops use Blast Secure Gateway to establish a secure tunnel to Connection Server. If not enabled, clients using a Blast Extreme session and Web browsers make direct connections to VMware Horizon desktops, bypassing Connection Server. This setting is disabled by default.

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

Security-Related Settings in Horizon LDAP

Security-related settings are provided in Horizon LDAP under the object path `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`. You can use the ADSI Edit utility to change the value of these settings on a Connection Server instance. The change propagates automatically to all other Connection Server instances in a group.

Table 2-6. Security-Related Settings in Horizon LDAP

Name-value pair	Description
cs-allowunencryptedstartsession	The attribute is `pae-NameValuePair`. This attribute controls whether a secure channel is required between a Connection Server instance and a desktop when a remote user session is being started. When Horizon Agent, is installed on a desktop computer, this attribute has no effect and a secure channel is always required. In all cases, user credentials and authorization tickets are protected by a static key. A secure channel provides further assurance of confidentiality by using dynamic keys. If set to **0**, a remote user session will not start if a secure channel cannot be established. This setting is suitable if all the desktops are in trusted domains or all desktops have Horizon Agent installed. If set to **1**, a remote user session can be started even if a secure channel cannot be established. This setting is suitable if some desktops have older Horizon Agents installed and are not in trusted domains. The default setting is **1**.
keysize	The attribute is `pae-MSGSecOptions`. When the message security mode is set to **Enhanced**, TLS is used to secure JMS connections rather than using per-message encryption. In enhanced message security mode, validation applies to only one message type. For enhanced message mode, VMware recommends increasing the key size to 2048 bits. If you are not using enhanced message security mode, VMware recommends not changing the default from 512 bits because increasing the key size affects performance and scalability. If you want all keys to be 2048 bits, the DSA key size must be changed immediately after the first Connection Server instance is installed and before additional servers and desktops are created.

Security-Related Server Settings for User Authentication

Security-related server settings for user authentication are accessible under **Settings > Global Settings > Global Settings** or **Settings > Server** in Horizon Console. These security settings determine how Horizon Client can log in to the Connection Server.

- To allow the Connection Server instance to accept the user identity and credential information that is passed when users select **Log in as current user** in the **Options** menu in Horizon Client, enable the **Accept logon as current user** setting for the Connection Server instance. This setting is available for Horizon Client for Windows. For more information, see the *Horizon Administration* document.

- To hide the server URL in Horizon Client, enable the **Hide server information in client user interface** global setting. For more information, see "Global Settings for Client Sessions" in the *Horizon Administration* document.
- To hide the **Domain** drop-down menu in Horizon Client, enable the **Hide domain list in client user interface** global setting. For more information, see "Global Settings for Client Sessions" in the *Horizon Administration* document.
- To send the domain list to Horizon Client, enable the **Send domain list** global setting in Horizon Console. For more information, see "Global Settings for Client Sessions" in the *Horizon Administration* document.

Note Not all settings are applicable to all Horizon Clients. To see user authentication settings for a particular Horizon Client, see the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Providing Server Details

In order for the Logon as current user feature to work, VMware Horizon must provide the Connection Server's Server Principal Name (Windows identity) to connecting clients prior to user authentication.

This information is withheld by default but can be provided by enabling the **Accept logon as current user** setting in Horizon Console. This choice is made individually for each server. If not enabled for a given server, then users logging in to that server from Horizon Client for Windows are required to enter credentials, even if they have enabled the **Logon as current user** setting. When deciding whether to enable the **Accept logon as current user** setting for a server, consider whether connecting clients are on an internal network, and therefore somewhat under your control, or external network, and hence uncontrolled.

The **Hide server information in client user interface** setting affects the client's user interface only, it doesn't change what information the server provides to the client. This setting is disabled by default.

Providing Domain Information

The list of available user domains can be provided to connecting clients prior to user authentication, and if provided, the list can be displayed to users in a drop-down menu.

This information is withheld by default but can be provided by enabling the **Send domain list** global setting in Horizon Console.

It is safe to provide the domain list to clients if they connect to the environment through a Unified Access Gateway appliance that is configured to perform two-factor pre-authentication. The domain list is not sent to a client until pre-authentication is successful. For more information on configuring two-factor authentication for a Unified Access Gateway appliance, see the Unified Access Gateway documentation at https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

The **Hide domain list in client user interface** setting affects the client's user interface only, it doesn't change what information the server provides to the client. This setting is disabled by default.

When users log in to a server, and **Send domain list** is disabled, and **Hide domain list in client user interface** is enabled, the **Domain** drop-down menu in Horizon Client shows `*DefaultDomain*` and users might need to enter a domain, for example, username@domain, in the **User name** text box. If users do not enter the domain manually, and if more than one domain is configured, they might fail to log in to the server.

The following table shows how the **Send domain list** and **Hide domain list in client user interface** global settings determine how users can log in to the server.

Send domain list setting	Hide domain list in client user interface setting	How users log in
Disabled (default)	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain**username*** ■ ***username*@*domain.com***
Disabled (default)	Disabled	If a default domain is configured on the client, the default domain appears in the **Domain** drop-down menu. If the client does not know a default domain, `*DefaultDomain*` appears in the **Domain** drop-down menu. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain**username*** ■ ***username*@*domain.com***
Enabled	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain**username*** ■ ***username*@*domain.com***
Enabled	Disabled	Users can enter a user name in the **User name** text box and then select a domain from the **Domain** drop-down menu. Alternatively, users can enter one of the following values in the **User name** text box. ■ ***domain**username*** ■ ***username*@*domain.com***

Ports and Services

3

Certain UDP and TCP ports must be open so that VMware Horizon components can communicate with each other. Knowing which Windows services run on each type of VMware Horizon server helps identify services that do not belong on the server.

This chapter includes the following topics:

VMware Horizon TCP and UDP Ports

VMware Horizon uses TCP and UDP ports for network access between its components.

During installation, VMware Horizon can optionally configure Windows firewall rules to open the ports that are used by default. If you change the default ports after installation, you must manually reconfigure Windows firewall rules to allow access on the updated ports. See "Replacing Default Ports for VMware Horizon Services" in the *Horizon Installation* document.

For a list of ports that VMware Horizon uses for a certificate login associated with the TrueSSO solution, see VMware Horizon TrueSSO Ports.

Table 3-1. TCP and UDP Ports Used by VMware Horizon

Source	Port	Target	Port	Protocol	Description
Connection Server, or Unified Access Gateway appliance	55000	Horizon Agent	4172	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
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.

Table 3-1. TCP and UDP Ports Used by VMware Horizon (continued)

Source	Port	Target	Port	Protocol	Description
Connection Server, or Unified Access Gateway appliance	*	Horizon Agent	3389	TCP	Microsoft RDP traffic to VMware Horizon 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	*	Horizon Agent	4172	TCP	PCoIP if PCoIP Secure Gateway is used.
Connection Server, or Unified Access Gateway appliance	*	Horizon Agent	22443	TCP	VMware Blast Extreme if Blast Secure Gateway is used.
Connection Server, or Unified Access Gateway appliance	*	Horizon Agent	22443	TCP	HTML Access if Blast Secure Gateway is used.
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.
Horizon Agent	4172	Connection Server or Unified Access Gateway appliance	55000	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
Horizon Agent	4172	Unified Access Gateway appliance	*	UDP	PCoIP. VMware Horizon desktops and applications send PCoIP data back to an Unified Access Gateway appliance from UDP port 4172 . The destination UDP port will be the source port from the received UDP packets and so as this is reply data, it is normally unnecessary to add an explicit firewall rule for this.

Table 3-1. TCP and UDP Ports Used by VMware Horizon (continued)

Source	Port	Target	Port	Protocol	Description
Horizon Agent (unmanaged)	*	Connection server instance	389	TCP	AD LDS access during unmanaged agent installation. **Note** For other uses of this port, see the note below this table.
Horizon Client	*	Connection Server or Unified Access Gateway appliance	80	TCP	TLS (HTTPS access) is enabled by default for client connections, but port 80 (HTTP access) can be used in certain cases. See HTTP Redirection in VMware Horizon.
Horizon Client	*	Connection Server or Unified Access Gateway appliance	443	TCP	HTTPS for logging in to VMware Horizon. (This port is also used for tunnelling when tunnel connections are used.)
Horizon Client	*	Connection Server or Unified Access Gateway appliance	4172	TCP and UDP	PCoIP if PCoIP Secure Gateway is used.
Horizon Client	*	Horizon Agent	3389	TCP	Microsoft RDP traffic to VMware Horizon 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, if direct connections are used instead of tunnel connections.
Horizon Client	*	Horizon Agent	32111	TCP	USB redirection and time zone synchronization if 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	*	Horizon Agent	22443	TCP and UDP	VMware Blast
Horizon Client	*	Connection 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.
Web Browser	*	Unified Access Gateway appliance	8443	TCP	HTML Access.
Connection Server	*	Connection Server	48080	TCP	For internal communication between Connection Server components.
Connection Server	*	vCenter Server	80	TCP	SOAP messages if TLS is disabled for access to vCenter Servers.

Table 3-1. TCP and UDP Ports Used by VMware Horizon (continued)

Source	Port	Target	Port	Protocol	Description
Connection Server	*	vCenter Server	443	TCP	SOAP messages if TLS is enabled for access to vCenter Servers.
Connection Server	*	Connection Server	4100	TCP	JMS inter-router traffic.
Connection Server	*	Connection Server	4101	TCP	JMS TLS inter-router traffic.
Connection Server	*	Connection Server	8472	TCP	For interpod communication in Cloud Pod Architecture.
Connection Server	*	Connection Server	22389	TCP	For global LDAP replication in Cloud Pod Architecture.
Connection Server	*	Connection Server	22636	TCP	For secure global LDAP replication in Cloud Pod Architecture.
Connection Server	*	Connection Server	32111	TCP	Key sharing traffic.
Connection Server	*	Certificate Authority	*	HTTP, HTTPS	CRL or OCSP queries
Unified Access Gateway appliance	*	Connection Server or load balancer	443	TCP	HTTPS access. Unified Access Gateway appliances connect on TCP port 443 to communicate with a Connection Server instance or load balancer in front of multiple Connection Server instances.
Horizon Help Desk Tool	*	Horizon Agent	3389	TCP	Microsoft RDP traffic to Horizon desktops for Remote Assistance.

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

Note Microsoft Windows Server requires a dynamic range of ports to be open between all Connection Servers in the VMware Horizon environment. These ports are required by Microsoft Windows for the normal operation of Remote Procedure Call (RPC) and Active Directory replication. For more information about the dynamic range of ports, see the Microsoft Windows Server documentation.

Note On a Connection Server instance, port 389 is accessible for infrequent, ad hoc connections. It is accessed when installing an unmanaged agent as shown in the table, and also when using an LDAP editor to directly edit the database, and when issuing commands using a tool such as repadmin. A firewall rule is created for these purposes when AD LDS is installed, but it can be disabled if access to the port is not required.

Note VMware Blast Extreme Adaptive Transport reserves some ports starting from ephemeral port range 49152-65535, by default. See the Knowledge Base article 52558.

HTTP Redirection in VMware Horizon

Connection attempts over HTTP are silently redirected to HTTPS, except for connection attempts to Horizon Console. HTTP redirection is not needed with more recent Horizon clients because they default to HTTPS, but it is useful when your users connect with a Web browser, for example to download Horizon Client.

The problem with HTTP redirection is that it is a non-secure protocol. If a user does not form the habit of entering **`https://`** in the address bar, an attacker can compromise the Web browser, install malware, or steal credentials, even when the expected page is correctly displayed.

Note HTTP redirection for external connections can take place only if you configure your external firewall to allow inbound traffic to TCP port 80.

Connection attempts over HTTP to Horizon Console are not redirected. Instead, an error message is returned indicating that you must use HTTPS.

To prevent redirection for all HTTP connection attempts, see "Prevent HTTP Redirection for Client Connections to Connection Server" in the *Horizon Installation* document.

Connections to port 80 of a Connection Server instance can also take place if you off-load TLS client connections to an intermediate device. See "Off-load TLS Connections to Intermediate Servers" in the *Horizon Administration* document.

To allow HTTP redirection when the TLS port number was changed, see "Change the Port Number for HTTP Redirection to Connection Server" in the *Horizon Installation* document.

VMware Horizon TrueSSO Ports

VMware Horizon uses TrueSSO ports for the communications pathway (port and protocol) and security controls used for the certificate to pass between Horizon Connection Server and the virtual desktop or published application for a certificate login associated with the TrueSSO solution.

Table 3-2. TrueSSO Ports Used by VMware Horizon

Source	Target	Port	Protocol	Description
Horizon Client	VMware Identity Manager appliance	TCP 443	HTTPS	Launch VMware Horizon from VMware Identity Manager appliance which generates SAML assertion and artifact.
Horizon Client	Horizon Connection Server	TCP 443	HTTPS	Launch Horizon Client.
Horizon Connection Server	VMware Identity Manager appliance	TCP 443	HTTPS	Connection Server performs SAML resolve against VMware Identity Manager. VMware Identity Manager validates artifact and returns assertion.

Table 3-2. TrueSSO Ports Used by VMware Horizon (continued)

Source	Target	Port	Protocol	Description
Horizon Connection Server	Horizon Enrollment Server	TCP 32111		Use the Enrollment Server.
Enrollment Server	ADCS			Enrollment Server requests certificate from Microsoft Certificate Authority (CA) to generate a temporary, short-lived certificate. The enrollment service uses TCP 135 RPC for the initial communication with the CA, then a random port from 1024 - 5000 and 49152 -65535. See Certificate Services in https://support.microsoft.com/en-us/help/832017#method4. Enrollment Server also communicates with domain controllers, using all relevant ports to discover a DC and bind to and query the Active Directory. See https://support.microsoft.com/en-us/help/832017#method1 and https://support.microsoft.com/en-us/help/832017#method12.
Horizon Agent	Horizon Connection Server	TCP 4002	JMS over TLS	Horizon Agent requests and receives a certificate for logon.
Virtual desktop or published application	AD DC			Windows validates the authenticity of the certificate with Active Directory. See Microsoft documentation for a list of ports and protocols, as numerous ports might be required.
Horizon Client	Horizon Agent (protocol session)	TCP/UDP 22443	Blast	Log on to the Windows desktop or application and a remote session is initiated on Horizon Client.
Horizon Client	Horizon Agent (protocol session)	UDP 4172	PCoIP	Log on to the Windows desktop or application and a remote session is initiated on Horizon Client.

Services on a Connection Server Host

The operation of VMware Horizon depends on several services that run on a Connection Server host.

Table 3-3. Horizon Connection Server Host Services

Service Name	Startup Type	Description
VMware Horizon Blast Secure Gateway	Automatic	Provides secure HTML Access and Blast Extreme services. This service must be running if clients connect to Connection Server through the Blast Secure Gateway.
VMware Horizon Connection Server	Automatic	Provides connection broker services. This service must always be running. If you start or stop this service, it also starts or stops the Framework, Message Bus, Security Gateway, and Web services. This service does not start or stop the VMwareVDMDS service or the VMware Horizon Script Host service.

Table 3-3. Horizon Connection Server Host Services (continued)

Service Name	Startup Type	Description
VMware Horizon Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must always be running.
VMware Horizon Message Bus Component	Manual	Provides messaging services between the VMware Horizon components. This service must always be running.
VMware Horizon PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to Connection Server through the PCoIP Secure Gateway.
VMware Horizon Script Host	Disabled	Provides support for third-party scripts that run when you delete virtual machines. This service is disabled by default. You should enable this service if you want to run scripts.
VMware Horizon Security Gateway Component	Manual	Provides common gateway services. This service must always be running.
VMware Horizon Web Component	Manual	Provides web services. This service must always be running.
VMwareVDMDS	Automatic	Provides Horizon LDAP services. This service must always be running. During upgrades of VMware Horizon, this service ensures that existing data is migrated correctly.

Certificate Thumbprint Verification and Automatic Certificate Generation

4

VMware Horizon uses many Public-Key Certificates. Some of these certificates are verified using mechanisms that involve a trusted third party but such mechanisms do not always provide the required precision, speed, or flexibility. VMware Horizon uses an alternative mechanism known as thumbprint verification in several situations.

Rather than validating individual certificate fields or building a chain of trust, thumbprint verification treats the certificate as a token, matching the entire byte sequence (or a cryptographic hash of this) to a pre-shared byte sequence or hash. Typically, this is shared just-in-time over a separate trusted channel and means that the certificate presented by a service can be verified to be the exact certificate that was expected.

Horizon Message Bus communicates between Connection Servers, and also between Horizon Agents and Connection Server instances. Setup channels use per-message signatures and payload encryption, whereas main channels are protected using TLS with mutual authentication. When using TLS to protect a channel, authentication of both client and server involves TLS certificates and thumbprint validation. For Horizon Message Bus channels, the server is always a message router. It is possible for the client to be a message router too since this is how message routers share messages. However, clients are either Connection Server instances or Horizon Agents.

The initial certificate thumbprints and setup message signing keys are provided in different ways. On Connection Servers, certificate thumbprints are stored in LDAP, so that Horizon Agents can communicate with any Connection Server, and all Connection Servers can communicate with each other. Horizon Message Bus server and client certificates are automatically generated and exchanged on a periodic basis, and stale certificates are automatically deleted, so no manual intervention is necessary, or indeed possible. Certificates at each end of the main channels are auto-generated on a scheduled basis and exchanged over the setup channels. It is not possible to replace these certificates yourself. Expired certificates are removed automatically.

A similar mechanism applies to the inter-Pod communication.

Other communication channels can use customer-provided certificates but default to auto-generating certificates. These include Secure Tunnel, Enrollment Server, and vCenter connections, and display protocol and auxiliary channels. For more information on how to replace these certificates, see the *Horizon Administration* document. Default certificates are generated at install time and are not automatically renewed, except for PCoIP. If a PKI-generated certificate is not available for PCoIP to use, it auto-generates a new certificate at each startup. Thumbprint verification is used for most of these channels, even if a PKI-generated certificate is used.

Verification of vCenter certificates uses a combination of techniques. Connection Server instances always attempt to validate the received certificate using PKI. If this validation fails, then after reviewing the certificate the VMware Horizon administrator can allow the connection to proceed, and the Connection Server remembers the cryptographic hash of the certificate for subsequent unattended acceptance using thumbprint verification.

Configuring Security Protocols and Cipher Suites on a Connection Server Instance

5

You can configure the security protocols and cipher suites that are accepted by Connection Server. You can define a global acceptance policy that applies to all Connection Server instances in a replicated group, or you can define an acceptance policy for individual Connection Server instances.

You also can configure the security protocols and cipher suites that Connection Server instances propose when connecting to vCenter Server. You can define a global proposal policy that applies to all Connection Server instances in a replicated group. You cannot define individual instances to opt out of a global proposal policy.

Note The security settings for Connection Server do not apply to Blast Secure Gateway (BSG). You must configure security for BSG separately. See Chapter 6 Configuring Security Protocols and Cipher Suites for Blast Secure Gateway.

Oracle's Unlimited Strength Jurisdiction Policy files are included as standard, allowing 256-bit keys by default.

This chapter includes the following topics:

Default Global Policies for Security Protocols and Cipher Suites

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

Table 5-1. Default Global Acceptance Policy

Default Security Protocols	Default Cipher Suites
■ TLS 1.2	■ 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

Table 5-2. Default Global Proposal Policy

Default Security Protocols	Default Cipher Suites
■ TLS 1.2	■ 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

In FIPS mode, only GCM cipher suites are enabled.

Configuring Global Acceptance and Proposal Policies

Global acceptance and proposal policies are defined in Horizon LDAP attributes. These policies apply to all Connection Server instances. To change a global policy, you can edit Horizon LDAP on any Connection Server instance.

Each policy is a single-valued attribute in the following Horizon LDAP location: `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`

Global Acceptance and Proposal Policies Defined in Horizon LDAP

You can edit the Horizon LDAP attributes that define global acceptance and proposal policies.

Global Acceptance Policies

The following attribute lists security protocols. You must order the list by placing the latest protocol first:

```
pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

The following attribute lists the cipher suites. This example shows an abbreviated list:

```
pae-ServerSSLCipherSuites =
\LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

The following attribute controls the precedence of cipher suites. Normally, the server's ordering of cipher suites is unimportant and the client's ordering is used. To use the server's ordering of cipher suites instead, set the following attribute:

```
pae-ServerSSLHonorClientOrder = 0
```

Global Proposal Policies

The following attribute lists security protocols. You must order the list by placing the latest protocol first:

```
pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

The following attribute lists the cipher suites. This list should be in order of preference. Place the most preferred cipher suite first, the second-most preferred suite next, and so on. This example shows an abbreviated list:

```
pae-ClientSSLCipherSuites =
\LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Change the Global Acceptance and Proposal Policies

To change the global acceptance and proposal policies for security protocols and cipher suites, you use the ADSI Edit utility to edit Horizon LDAP attributes.

Prerequisites

- Familiarize yourself with the Horizon LDAP attributes that define the acceptance and proposal policies. See Global Acceptance and Proposal Policies Defined in Horizon LDAP.
- See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows Server operating system version.

Procedure

1. Start the ADSI Edit utility on your Connection Server computer.
2. In the console tree, select **Connect to**.
3. In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **`DC=vdi, DC=vmware, DC=int`**.
4. In the **Select or type a domain or server** text box, select or type **`localhost:389`** or the fully qualified domain name (FQDN) of the Connection Server computer followed by port 389.

   For example: **`localhost:389`** or **`mycomputer.mydomain.com:389`**
5. Expand the ADSI Edit tree, expand **OU=Properties**, select **OU=Global**, and select **CN=Common** in the right pane.
6. On the object **CN=Common, OU=Global, OU=Properties**, select each attribute that you want to change and type the new list of security protocols or cipher suites.
7. Restart the Windows service VMware Horizon Security Gateway Component on each Connection Server instance if you modified `pae-ServerSSLSecureProtocols`.

   You do not need to restart any service after modifying `pae-ClientSSLSecureProtocols`.

Configure Acceptance Policies on Individual Servers

To specify a local acceptance policy on an individual Connection Server instance , you must add properties to the `locked.properties` file. If the `locked.properties` file does not yet exist on the server, you must create it.

You add a `secureProtocols.`*`n`* entry for each security protocol that you want to configure. Use the following syntax: `secureProtocols.`*`n=security protocol`*.

You add an `enabledCipherSuite.`*`n`* entry for each cipher suite that you want to configure. Use the following syntax: `enabledCipherSuite.`*`n=cipher suite`*.

The variable *`n`* is an integer that you add sequentially (1, 2, 3) to each type of entry.

You add an `honorClientOrder` entry to control the precedence of cipher suites. Normally, the server's ordering of cipher suites is unimportant and the client's ordering is used. To use the server's ordering of cipher suites instead, use the following syntax:

```
honorClientOrder=false
```

Make sure that the entries in the `locked.properties` file have the correct syntax and the names of the cipher suites and security protocols are spelled correctly. Any errors in the file can cause the negotiation between the client and server to fail.

Procedure

1. Create or edit the `locked.properties` file in the TLS/SSL gateway configuration folder on the Connection Server computer.

   For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\`
2. Add `secureProtocols.`*`n`* and `enabledCipherSuite.`*`n`* entries, including the associated security protocols and cipher suites.
3. Save the `locked.properties` file.
4. Restart the VMware Horizon Connection Server service to make your changes take effect.

Example: Default Acceptance Policies on an Individual Server

The following example shows the entries in the `locked.properties` file that are needed to specify the default policies:

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:
```

```
enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.3=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
enabledCipherSuite.4=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

# Use the client's ordering of cipher suites (ignores the ordering given above):

honorClientOrder=true
```

Note In FIPS mode, only GCM cipher suites are enabled.

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
   ```

Older Protocols and Ciphers Disabled in VMware Horizon

Some older protocols and ciphers that are no longer considered secure are disabled in VMware Horizon by default. If required, you can enable them manually.

DHE Cipher Suites

For more information, see http://kb.vmware.com/kb/2121183. Cipher suites that are compatible with DSA certificates use Diffie-Hellman ephemeral keys, and these suites are no longer enabled by default, starting with Horizon 6 version 6.2.

For Connection Server instances and VMware Horizon desktops, you can enable these cipher suites by editing the Horizon LDAP database, `locked.properties` file, or registry, as described in this guide. See Change the Global Acceptance and Proposal Policies, Configure Acceptance Policies on Individual Servers, and Configure Proposal Policies on Remote Desktops. You can define a list of cipher suites that includes one or more of the following suites, in this order:

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (TLS 1.2 only, not FIPS)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (TLS 1.2 only, not FIPS)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (TLS 1.2 only)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (TLS 1.2 only)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

For View Agent Direct-Connection (VADC) machines, you can enable DHE cipher suites by adding the following to the list of ciphers when you follow the procedure "Disable Weak Ciphers in SSL/TLS for Horizon Agent Machines" in the *Horizon Installation* document.

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

Note It is not possible to enable support for ECDSA certificates. These certificates have never been supported.

SSLv3

In VMware Horizon, SSL version 3.0 has been removed.

RC4

For Connection Server instances and VMware Horizon desktops, you can enable RC4 on a Connection Server or a Horizon Agent machine by editing the configuration file `C:\Program Files\VMware\VMware View\Server\jre\conf\security\java.security`. At the end of the file is a multi-line entry called `jdk.tls.legacyAlgorithms`. Remove `RC4_128` and the comma that follows it from this entry and restart the Connection Server,or the Horizon Agent machine, as the case may be.

For View Agent Direct-Connection (VADC) machines, you can enable RC4 by adding the following to the list of ciphers when you follow the procedure "Disable Weak Ciphers in SSL/TLS Horizon Agent Machines" in the *Horizon Installation* document.

```
TLS_RSA_WITH_RC4_128_SHA
```

TLS 1.0

In VMware Horizon, TLS 1.0 is disabled by default.

For more information, see https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf and http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf. For instructions on how to enable TLS 1.0, see the sections "Enable TLSv1 on vCenter Connections from Connection Server" and the *Horizon Upgrades* document.

Configuring Security Protocols and Cipher Suites for Blast Secure Gateway

6

The security settings for Connection Server do not apply to Blast Secure Gateway (BSG). You must configure security for BSG separately.

This chapter includes the following topics:

- Configure Security Protocols and Cipher Suites for Blast Secure Gateway (BSG)

Configure Security Protocols and Cipher Suites for Blast Secure Gateway (BSG)

You can configure the security protocols and cipher suites that BSG's client-side listener accepts by editing the file `absg.properties`.

The protocols that are allowed are, from low to high, tls1.0, tls1.1, and tls1.2. Older protocols such as SSLv3 and earlier are never allowed. Two properties, `localHttpsProtocolLow` and `localHttpsProtocolHigh`, determine the range of protocols that the BSG listener will accept. For example, setting `localHttpsProtocolLow=tls1.0` and `localHttpsProtocolHigh=tls1.2` will cause the listener to accept tls1.0, tls1.1, and tls1.2. The default settings are `localHttpsProtocolLow=tls1.2` and `localHttpsProtocolHigh=tls1.2`, meaning that by default only TLS 1.2 is allowed. You can examine the BSG's `absg.log` file to discover the values that are in force for a specific BSG instance.

You must specify the list of ciphers using the format that is defined in OpenSSL. You can search for `openssl cipher string` in a web browser and see the cipher list format. The following cipher list is the default:

```
ECDHE+AESGCM
```

Note In FIPS mode, only GCM cipher suites are enabled (`ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256`).

Procedure

1 On the Connection Server instance, edit the file *`install_directory`*`\VMware\VMware View\Server\appblastgateway\absg.properties`.

  By default, the install directory is *%ProgramFiles%*.

2 Edit the properties `localHttpsProtocolLow` and `localHttpsProtocolHigh` to specify a range of protocols.

   For example,

   ```
   localHttpsProtocolLow=tls1.0
   localHttpsProtocolHigh=tls1.2
   ```

   To enable only one protocol, specify the same protocol for both `localHttpsProtocolLow` and `localHttpsProtocolHigh`.

3 Edit the `localHttpsCipherSpec` property to specify a list of cipher suites.

   For example,

   ```
   localHttpsCipherSpec=!aNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES
   ```

4 Restart the Windows service VMware Horizon Blast Secure Gateway.

Configuring Security Protocols and Cipher Suites for PCoIP Secure Gateway

7

The security settings for Connection Server do not apply to PCoIP Secure Gateway (PSG). You must configure security for PSG separately.

This chapter includes the following topics:

Configure Security Protocols and Cipher Suites for PCoIP Secure Gateway (PSG)

You can configure the security protocols and cipher suites that PSG's client-side listener accepts by editing the registry. If required, this task can also be performed on a RDS host.

The protocols that are allowed are, from low to high, tls1.0, tls1.1, and tls1.2. Older protocols such as SSLv3 and earlier are never allowed. The default setting is `tls1.2:tls1.1`.

Note In FIPS mode, only TLS 1.2 is enabled (tls1.2).

The following cipher list is the default:

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:@STRENGTH"
```

Note In FIPS mode, only GCM cipher suites are enabled (`ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256`).

Procedure

1. On the Connection Server instance or RDS host, open a registry editor and navigate to `HKLM\Software\Teradici\SecurityGateway`.
2. Add or edit the REG_SZ registry value `SSLProtocol` to specify a list of protocols.

   For example,

   ```
   tls1.2:tls1.1
   ```

3 Add or edit the REG_SZ registry value `SSLCipherList` to specify a list of cipher suites.

   For example,

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256
```

4 Add or edit the REG_SZ registry value `SSLDisableAES128` to filter cipher suites that negotiate a 128-bit AES encryption key. If not defined, the value defaults to **0**, meaning that the filter will not be applied. To exclude these cipher suites, turn on the filter by setting the registry value to **1**.

5 Add or edit the REG_SZ registry value `SSLDisableRSACipher` to filter cipher suites that use RSA for key exchange. If not defined, the value defaults to **1**, meaning that these cipher suites will be filtered from the list. If it is necessary to include them, turn off the filter by setting the registry value to **0**.

Deploying USB Devices in a Secure VMware Horizon Environment

8

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

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

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

This chapter includes the following topics:

Disabling USB Redirection for All Types of Devices

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

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

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

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

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

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

Table 8-1. Effect of Combining Exclude All Devices Policies

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

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

These policies are included in the Horizon Agent Configuration ADMX template file (`vdm_agent.admx`). For more information, see "USB Settings in the Horizon Agent Configuration ADMX Template" in *Configuring Remote Desktop Features in Horizon*.

Disabling USB Redirection for Specific Devices

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

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

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

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

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

```
ExcludeAllDevices   Enabled

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

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

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

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

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

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

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

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

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

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

These policies are included in the Horizon Agent Configuration ADMX template file (`vdm_agent.admx`). For more information, see *Configuring Remote Desktop Features in Horizon*.

HTTP Protection Measures on Connection Servers

9

employs certain measures to protect communication that uses the HTTP protocol.

This chapter includes the following topics:

Internet Engineering Task Force Standards

Connection Server complies with certain Internet Engineering Task Force (IETF) standards.

- RFC 5746 Transport Layer Security (TLS) – Renegotiation Indication Extension, also known as secure renegotiation, is enabled by default.

  Note Client-initiated renegotiation is disabled by default on Connection Servers. To enable, edit registry value `[HKLM\SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params]JvmOptions` and remove **`-Djdk.tls.rejectClientInitiatedRenegotiation=true`** from the string.

- RFC 6797 HTTP Strict Transport Security (HSTS), also known as transport security, is enabled by default. This setting cannot be disabled.
- RFC 7034 HTTP Header Field X-Frame-Options, also known as counter clickjacking, is enabled by default. You can disable it by adding the entry `x-frame-options=OFF` to the file `locked.properties`. For information on how to add properties to the file `locked.properties`, see Configure HTTP Protection Measures.

  Note In releases earlier than version 7.2, changing this option did not affect connections to HTML Access.

- RFC 6454 Origin Checking, which protects against cross-site request forging, is enabled by default. You can disable it by adding the entry `checkOrigin=false` to `locked.properties`. For more information, see Cross-Origin Resource Sharing.

  Note In earlier releases, this protection was disabled by default.

HTTP Strict Transport Security

The HTTP Strict Transport Security (HSTS) feature is a security policy mechanism that helps to protect against man-in-the-middle attacks by telling web browsers that they should use only HTTPS to connect.

The header is added to all HTTP responses on port 443, specifying a lifetime of one year. Optional properties can be set by adding multi-value property hstsFlags to the locked.properties file. The following values can be set.

Property	Value
includeSubDomains	Applies to all subdomains of this site.
preload	Hint to include this site in HSTS preload lists.

Note These properties are not set by default because they can affect non-Horizon URLs too. Do not set unless you understand the implications.

World Wide Web Consortium Standards

Connection Server complies with certain World Wide Web Consortium (W3) standards.

- Cross-Origin Resource Sharing (CORS) constrains client-side cross-origin requests. You can enable it by adding the entry `enableCORS=true` or disable it by adding the entry `enableCORS=false` to `locked.properties`.
- Content Security Policy (CSP), which mitigates a broad class of content injection vulnerabilities, is enabled by default. You can disable it by adding the entry `enableCSP=false` to `locked.properties`.

Cross-Origin Resource Sharing

The Cross-Origin Resource Sharing (CORS) feature regulates client-side cross-origin requests by providing policy statements to the client on demand and by checking requests for compliance with the policy. This feature can be configured and enabled if required.

Policies include the set of HTTP methods that can be accepted, where requests can originate, and which content types are valid. These policies vary according to the request URL, and can be reconfigured as needed by adding entries to the `locked.properties` file.

An ellipsis after a property name indicates that the property can accept a list.

Table 9-1. CORS Properties

Property	Value Type	Master Default	Other Defaults
`enableCORS`	`true` `false`	`true`	`n/a`
`acceptContentType...`	`http-content-type`	`application/x-www-form-urlencoded,application/xml,text/xml`	`admin`=application/json,application/text,application/x-www-form-urlencoded `portal`=application/json `rest`=application/json `sse`=application/json `view-vlsi-rest`=application/json

Table 9-1. CORS Properties (continued)

Property	Value Type	Master Default	Other Defaults
acceptHeader...	http-header-name	*	admin=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Cache-Control,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrftoken,DNT,Host,Origin,Referer,User-Agent broker=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,Gateway-Location,Gateway-Name,Gateway-Type,Host,Origin,Referer,User-Agent,X-CSRF-Token,X-EUC-Gateway,X-EUC-Health,X-Forwarded-For,X-Forwarded-Host,X-Forwarded-Proto portal=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,Host,Origin,Referer,User-Agent,X-CSRF-Token rest=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege view-vlsi=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege view-vlsi-rest=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege

Table 9-1. CORS Properties (continued)

Property	Value Type	Master Default	Other Defaults
exposeHeader...	http-header-name	*	n/a
filterHeaders	true false	true	n/a
checkOrigin	true false	true	n/a
checkReferer	true false	false	n/a
allowCredentials	true false	false	admin =true broker=true health=true misc =true portal=true rest=true saml=true sse=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET,HEAD,POST	health=GET,HEAD misc =GET,HEAD rest=GET,POST,PUT, PATCH,DELETE saml =GET,HEAD sse=GET,POST tunnel=GET,POST
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension...	chrome-extension-hash	ppkfnjlimknmjoaemnpidmdlfchhehel **Note** This value is the Chrome extension ID for Horizon Client for Chrome.	n/a

Following are examples of CORS properties in the `locked.properties` file.

```
enableCORS = true
allowPreflight = true
checkOrigin = true
```

```
checkOrigin-misc = false
allowMethod.1 = GET
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

Origin Checking

Origin checking is enabled by default. When it is enabled, a request is accepted only without an Origin, or with an Origin equal to the address that the External URL specifies, to the `balancedHost` address, to any `portalHost` address, to any `chromeExtension` hash, to `null`, or to `localhost`. If Origin is not one of these possibilities, an "Unexpected Origin" error is logged and a status of 404 is returned.

Note Some browsers do not provide an Origin header, or do not always provide one. Optionally, the Referer header in a request can be checked in the absence of an Origin header. The Referer header has one "r" in header name. To check the Referer header, add the following property to the `locked.properties` file:

```
checkReferer=true
```

If multiple Connection Server hosts are load balanced, you must specify the load balancer address by adding a `balancedHost` entry to the `locked.properties` file. Port 443 is assumed for this address.

If clients connect through a Unified Access Gateway appliance or another gateway, you must specify all the gateway addresses by adding `portalHost` entries to the `locked.properties` file. Port 443 is assumed for these addresses. You must also specify `portalHost` entries to provide access to a Connection Server host by a name that is different from the name that the External URL specifies.

Chrome extension clients set their initial Origin to their own identity. To allow connections to succeed, register the extension by adding a `chromeExtension` entry to the `locked.properties` file. For example:

```
chromeExtension.1=bpifadopbphhpkkcfohecfadckmpjmjd
```

Content Security Policy

The Content Security Policy (CSP) feature mitigates a broad class of content injection vulnerabilities, such as cross-site scripting (XSS), by providing policy directives to compliant browsers. This feature is enabled by default. You can reconfigure the policy directives by adding entries to `locked.properties`.

Table 9-2. CSP Properties

Property	Value Type	Master Default	Other Defaults
enableCSP	true false	true	n/a
content-security-policy	directives-list	default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data: ;frame-ancestors 'none'	admin=default-src 'self' https://feedback.esp.vmware.com; script-src https://feedback.esp.vmware.com 'unsafe-inline' 'unsafe-eval';style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:;frame-ancestors 'none' portal=default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self' blob:;connect-src 'self' wss:;frame-src 'self' blob:;child-src 'self' blob:;object-src 'self' blob:;frame-ancestors 'self' rest=default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:;frame-ancestors 'none'
x-content-type-options	OFF specification	nosniff	n/a
x-frame-options	OFF specification	deny	portal = sameorigin
x-xss-protection	OFF specification	1; mode=block	n/a

You can add CSP properties to the `locked.properties` file. Example CSP properties:

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;style-src 'self'
 'unsafe-inline';font-src 'self' data:
```

```
content-security-policy-newadmin = default-src 'self';script-src 'self' 'unsafe-inline'
'unsafe-eval' data:;style-src 'self'
 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:
content-security-policy-portal = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-
eval' data:;style-src 'self'
'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self'
blob:;connect-src 'self' wss:;frame-src
'self' blob:;child-src 'self' blob:;object-src 'self' blob:
x-content-type-options = nosniff
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

Other Protection Measures

Besides the Internet Engineering Task Force and W3 standards, VMware Horizon employs other measures to protect communication that uses the HTTP protocol.

Reducing MIME Type Security Risks

By default, VMware Horizon sends the header `x-content-type-options: nosniff` in its HTTP responses to help prevent attacks based on MIME-type confusion.

You can disable this feature by adding the following entry to the file `locked.properties`:

```
x-content-type-options=OFF
```

Mitigating Cross-Site Scripting Attacks

By default, VMware Horizon employs the XSS (cross-site scripting) Filter feature to mitigate cross-site scripting attacks by sending the header `x-xss-protection=1; mode=block` in its HTTP responses.

You can disable this feature by adding the following entry to the file `locked.properties`:

```
x-xss-protection=OFF
```

Content Type Checking

By default, VMware Horizon accepts requests with the following declared content types only:

- application/x-www-form-urlencoded
- application/xml
- text/xml

Note In earlier releases, this protection was disabled by default.

To restrict the content types that VMware Horizon accepts, add the following entry to the file `locked.properties`:

```
acceptContentType.1=content-type
```

For example:

```
acceptContentType.1=x-www-form-urlencoded
```

To accept another content type, add the entry `acceptContentType.2=content-type`, and so on

To accept requests with any declared content type, specify `acceptContentType=*`.

Client Behavior Monitoring

Connection Servers have finite resources available to handle requests from clients, and misbehaving clients can tie up those resources, preventing others from being serviced. Client behavior monitoring is a class of detections and mitigation that protect against bad behavior.

Handshake Monitoring

TLS handshakes on port 443 must complete within a configurable period, otherwise they will be forcibly terminated. By default, this period is 10 seconds. If smart card authentication is enabled, TLS handshakes on port 443 can complete within 100 seconds.

If required, you can adjust the time for TLS handshakes on port 443 by adding the following property to the `locked.properties` file:

```
handshakeLifetime = lifetime_in_seconds
```

For example:

```
handshakeLifetime = 20
```

Optionally, the client that is responsible for an over-running TLS handshake can be automatically added to a blacklist. See Client Blacklisting for more information.

Request Reception Monitoring

HTTP requests must be fully received within 30 seconds, otherwise the connection will be forcibly terminated.

Optionally, a client that takes longer than this to send a request can be automatically added to a blacklist. See Client Blacklisting for more information.

Request Counting

A single client is not expected to send more than 100 HTTP requests per minute, although by default no action is taken if this threshold is exceeded.

Optionally, a client that exceeds this threshold can be automatically added to a blacklist. See Client Blacklisting for more information.

If client blacklisting has been enabled, you may need to configure request counting thresholds.

You can adjust the maximum number of served HTTP requests per client by adding the following property to the `locked.properties` file:

```
requestTallyThreshold = max_served_requests_in_30_seconds
```

Example:

```
requestTallyThreshold = 100
```

You can adjust the maximum number of failed HTTP requests per client by adding the following property to the `locked.properties` file:

```
 tarPitGraceThreshold = max_failed_requests_in_30_seconds
```

Example:

```
 tarPitGraceThreshold = 5
```

Client Blacklisting

This type of protection is disabled by default because it can reduce performance and frustrate users if it is not correctly configured. Do not enable client blacklisting if using a gateway, such as a Unified Access Gateway appliance, which presents all client connections as the same IP address.

If enabled, connections from clients on the blacklist are delayed for a configurable period before processing. If many connections from the same client are being delayed at the same time, further connections from that client are refused, rather than delayed. This threshold is configurable.

You can enable this feature by adding the following property to the `locked.properties` file:

```
secureHandshakeDelay = delay_in_milliseconds
```

For example:

```
secureHandshakeDelay = 2000
```

To disable blacklisting of HTTPS connections, remove the `secureHandshakeDelay` entry or set it to 0.

When a TLS handshake over-run occurs, the client's IP address is added to the blacklist for a minimum period equal to the sum of `handshakeLifetime` and `secureHandshakeDelay`.

Using the values in the examples above, the IP address of a misbehaving client is blacklisted 22 seconds:

```
(20 * 1000) + 2000 = 22 seconds
```

The minimum period is extended each time a connection from the same IP address misbehaves. The IP address is removed from the blacklist after the minimum period has expired and after the last delayed connection from that IP address has been processed.

A TLS handshake over-run is not the only reason to blacklist a client. Other reasons include a series of abandoned connections, or a series of requests ending in error, such as multiple attempts to access non-existent URLs. These various triggers have differing minimum blacklist periods. To extend monitoring of these additional triggers to port 80, add the following entry to the `locked.properties` file:

```
insecureHandshakeDelay = delay_in_milliseconds
```

For example:

```
insecureHandshakeDelay = 1000
```

To disable blacklisting of HTTP connections, remove the `insecureHandshakeDelay` entry or set it to 0.

Behavior Monitoring Properties

Use these properties to monitor client behavior. These properties include properties for detections and mitigations that protect against bad behavior.

Table 9-3. Behavior Monitoring Properties

Property	Description	Default Value	Dynamic
`handshakeLifetime`	Maximum time for TLS handshake, in seconds.	10 or 100 (See Handshake Monitoring.)	No
`secureHandshakeDelay`	Delay before TLS handshake when blacklisting, in milliseconds.	0 (blacklisting OFF)	No
`insecureHandshakeDelay`	Delay before non-TLS handshake when blacklisting, in milliseconds.	0 (blacklisting OFF)	No
`requestTallyThreshold`	Served HTTP requests per 30-second period for client blacklisting.	50	No
`tarPitGraceThreshold`	Unserved HTTP requests per 30-second period for client blacklisting.	3	No
`secureBlacklist...`	List of IP addresses on port 443 to reject immediately when blacklisting.	n/a	Yes
`insecureBlacklist...`	List of IP addresses on port 80 to reject immediately when blacklisting.	n/a	Yes

Table 9-3. Behavior Monitoring Properties (continued)

Property	Description	Default Value	Dynamic
`secureWhitelist...`	List of IP addresses on port 443 to exclude from blacklisting.	n/a	Yes
`insecureWhitelist...`	List of IP addresses on port 80 to exclude from blacklisting.	n/a	Yes

Changes to dynamic entries take immediate effect, without a service restart.

User Agent Whitelisting

Set a whitelist to restrict user agents that can interact with VMware Horizon. By default, all user agents are accepted.

Note This is not strictly a security feature. User agent detection relies on the user-agent request header provided by the connecting client or browser, which can be spoofed. Some browsers allow the request header to be modified by the user.

A user agent is specified by its name and a minimum version. For example:

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

This means that only Google Chrome version 14 and later, and Safari version 5.1 and later are allowed to connect using HTML Access. All browsers can connect to other services.

You can enter the following recognised user agent names:

- Android
- Chrome
- Edge
- IE
- Firefox
- Opera
- Safari

Note Not all of these user agents are supported by VMware Horizon. These are examples.

Configure HTTP Protection Measures

To configure HTTP protection measures you must create or edit the `locked.properties` file in the gateway configuration folder on the Connection Server instance.

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

- Use the following syntax to configure a property in `locked.properties`:

```
myProperty = newValue
```

- The property name is always case-sensitive and the value might be case-sensitive. Whitespace around the = sign is optional.
- For CORS and CSP properties, it is possible to set service-specific values as well as a master value. For example, the admin service is responsible for handling Horizon Console requests, and a property can be set for this service without affecting other services by appending `-admin` after the property name.

```
myProperty-admin = newValueForAdmin
```

- If both a master value and a service-specific value are specified, then the service-specific value applies to the named service, and the master value applies to all other services. The sole exception to this is the special value "OFF". If the master value for a property is set to "OFF", then all service-specific values for this property are ignored.

  For example:

```
myProperty = OFF
myProperty-admin = newValueForAdmin    ; ignored
```

- Some properties can accept a list of values.

  To set a single value, enter the following property:

```
myProperty = newValue
myProperty-admin = newValueForAdmin
```

  To set multiple values for a property that accepts list values, you can specify each value on a separate line:

```
myProperty.1 = newValue1
myProperty.2 = newValue2
myProperty-admin.1 = newValueForAdmin1
myProperty-admin.2 = newValueForAdmin2
```

- To determine the correct service name to use when making a service-specific configuration, look in the debug logs for lines containing the following sequence:

```
(ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
```

  In this example, the service name is `admin`. You can use the following typical service names:

  - `newadmin` for Horizon Console
  - `broker` for Connection Server

- `docroot` for Local file serving
- `portal` for HTML Access
- `saml` for SAML communication (vIDM)
- `tunnel` for Secure Tunnel
- `view-vlsi` for View API
- `misc` for Other
- `rest` for REST API