Horizon Security

VMware Horizon 2209

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

https://docs.vmware.com/

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

Contents

Horizon Security

1

Horizon Security contains information about the security features 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.

This chapter includes the following topics:

- Horizon System Security
- Horizon Client and Agent Security
- Scenarios for Setting Up TLS Certificates for Horizon 8

Horizon System Security

This section 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.

VMware Horizon Accounts, Resources, and Log Files

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.

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 and Upgrade* document.
Connection broker	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 the 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 the connection broker	A Microsoft SQL Server, Oracle, or PostgreSQL database stores Horizon event data. You create an administrative account for the database that the Horizon consoler 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. Connection Broker 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.

Table 1-3. Connection Broker Resources (continued)

Resource	Location	Protection
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. In VMware Horizon 8 deployments, VMware recommends that you configure and use the event database to monitor VMware Horizon. For more information, see the *Horizon Installation and Upgrade* 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 an application with elevated administrator privileges. Right-click the application 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 (VMware Horizon 8 only)	The Horizon Event Database configured on a Microsoft SQL Server, Oracle database server, or PostgreSQL database server. Windows Application Event logs. Disabled by default.

Table 1-4. VMware Horizon Log Files (continued)

Horizon Component	File Path and Other Information
Connection Server (VMware Horizon 8 only)	`<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

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

Security-Related Global Settings for VMware Horizon 8

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 the Horizon console.

Table 1-5. 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. In VMware Horizon 8 environments: - When you install Connection Server, you provide a data recovery password. After installation, you can change this password in the 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 broker 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 1-5. 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 console session continues before the session times out. **Important** Setting the console session timeout to a high number of minutes increases the risk of unauthorized use of the console. Use caution when you allow an idle session to persist a long time. By default, the 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 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 broker instances. See "Off-load TLS Connections to Intermediate Servers" in the *Horizon Administration* document.

Change the Data Recovery Password for VMware Horizon 8

You provide a data recovery password when you install Connection Server. After installation, you can change this password in the 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 the console, select **Settings > Global Settings**.

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

3 Enter and re-enter 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 in VMware Horizon 8

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 1-6. 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 the connection broker 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. JMS access control is also enabled so that desktops and connection broker instances can only send and receive JMS messages on certain topics.
Enhanced	SSL is used for all JMS connections. Messages are not signed or encrypted individually because all are protected by the channel. This brings significant performance benefits. Certificates are auto-managed. For more information see Certificate Thumbprint Verification and Automatic Certificate Generation. **Note** There is an LDAP setting that you can enable to block **Enhanced** mode from being selected.

Note Some JMS messages are encrypted because they carry sensitive information such as user credentials. If you do not use Enhanced mode, you can also use IPSec to encrypt all JMS messages between connection broker instances.

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 the message security mode for an upgraded VMware Horizon environment from **Enabled** to **Enhanced** or from **Enhanced** to **Enabled**, you must first upgrade all connection broker instances and VMware Horizon desktops. After you change the setting, the new setting takes place in stages.

1 You must manually restart the VMware Horizon Message Bus Component service on all connection broker hosts in the pod, or restart the connection broker instances.

2 After the services are restarted, the connection broker instances reconfigure the message security mode on all desktops, changing the mode to your new setting.

3 To monitor the progress in the console, go to **Settings > Global Settings**.

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

   Alternatively, you can use the `vdmutil` command-line utility to monitor progress. See Using the vdmutil Utility to Configure the JMS Message Security Mode for VMware Horizon 8.

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 for VMware Horizon 8

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 *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 1-7. 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 activated by using the `--verbose` option, the `vdmutil` command writes output to standard output, in US English.

Table 1-8. 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.

Table 1-8. vdmutil Command Options (continued)

Option	Description
`--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.
`--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.
`--refreshDesktopCertificates`	Refresh certificates for all machines in the specified desktop in the local pod.
`--setMsgSecMode`	Sets the message security mode for the local pod.
`--verbose`	Activates 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 the Horizon Console

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

Table 1-9. 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 broker 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 broker 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 broker 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 broker 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 the connection broker. If not enabled, clients using a Blast Extreme session and Web browsers make direct connections to VMware Horizon desktops, bypassing the connection broker. 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

This topic describes security-related settings in LDAP that cannot be modified using APIs, the administration console, or provided command-line tools. Security-related settings are provided in Horizon LDAP under the object path `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`. If you have full administrative privileges, you can use an LDAP editor such as the ADSI Edit utility to change the value of these settings on a connection broker instance. The change propagates automatically to all other connection broker instances in a cluster.

Security-Related Settings in Horizon LDAP

Attribute	Description
`pae-AgentLogCollectionDisabled`	This setting can be used to prevent downloading of DCT archives from Horizon Agents, using either APIs or the administration console. Log collection is still possible from Connection Servers in VMware Horizon 8 environments. Set to 1 to deactivate agent log collection.
`pae-DisallowEnhancedSecurityMode`	This setting can be used to prevent the use of Enhanced message security. Use this if you want to disable automatic certificate management. Once this is set to 1, the Horizon environment begins the transition to Enabled message security mode automatically. Setting this attribute back to 0 or removing it allows Enhanced message security to be chosen once more, but does not trigger an automatic transition.
`pae-enableDbSSL`	If you configure an Event Database, the connection is not protected by TLS by default. Set this attribute to 1 to enable TLS on the connection.
`pae-managedCertificateAdvanceRollOver`	For Certificate Thumbprint Verification and Automatic Certificate Generation, this attribute can be set to force certificates to be renewed before they expire. Specify the number of days in advance of the expiry date that this should be done. The maximum period is 90 days. If not specified, this setting defaults to 0 days, and so roll-over happens at expiry.

Attribute	Description
`pae-MsgSecOptions`	This is a multi-valued attribute where each value is itself a name-value pair (for example, `course=fish`). **Warning** When adding or modifying a name-value pair, be very careful not to remove other values. Currently the only name-value pair that can be set is `keysize`. This specifies the length of the DSA message signing key. If not specified, it defaults to 512 bits. - If message security is Enabled or Mixed, every message is signed. Increasing the key length affects performance and scalability. - If message security is Enhanced, few messages are signed and VMware recommends a key length of 2048 bits. - If you selected FIPS compatibility when installing Horizon, keysize is already set to 2048. The key length can be changed immediately after the first connection broker instance is installed and before additional servers and desktops are created. After this, it must not be changed.
`pae-noManagedCertificate`	This setting can be used to disable automatic certificate management. When this is set to 1, certificates are no longer renewed automatically and self-signed certificates in the certificate stores are ignored. All certificates must be CA signed and admin-managed. This setting is not compatible with Enhanced message security. Before setting to 1, you must switch message security to Enabled. If you selected FIPS compatibility when installing Horizon, the "vdm" certificate must be CA signed but others need not be, unless this is set to 1. All Connection Servers in a CPA configuration should have the root certificate that was used to generate the Enrollment client certificate (vdm.ec) of other PODs.
`pae-SSLCertificateSignatureAlgorithm`	This specifies the certificate signature algorithm to use for auto-managed certificates. If not specified, it defaults to `rsa_pkcs1_sha384`. For more examples see Default Global Policies for Security Protocols and Cipher Suites.

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 the Horizon console. These security settings determine how Horizon Client can log in to the connection broker.

- To allow the connection broker 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 broker 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 the 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/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***

Send domain list setting	Hide domain list in client user interface setting	How users log in
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

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.

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 and Upgrade* 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 1-10. TCP and UDP Ports Used by VMware Horizon

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

Table 1-10. TCP and UDP Ports Used by VMware Horizon (continued)

Source	Port	Target	Port	Protocol	Description
Connection broker or Unified Access Gateway appliance	*	Horizon Agent	3389	TCP	Microsoft RDP traffic to VMware Horizon desktops when tunnel connections are used.
Connection broker 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 broker or Unified Access Gateway appliance	*	Horizon Agent	32111	TCP	USB redirection and time zone synchronization when tunnel connections are used.
Connection broker or Unified Access Gateway appliance	*	Horizon Agent	4172	TCP	PCoIP if PCoIP Secure Gateway is used.
Connection broker or Unified Access Gateway appliance	*	Horizon Agent	22443	TCP	VMware Blast Extreme if Blast Secure Gateway is used.
Connection broker 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 following this table.
Horizon Agent	4172	Connection broker 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 1-10. TCP and UDP Ports Used by VMware Horizon (continued)

Source	Port	Target	Port	Protocol	Description
Horizon Agent (unmanaged)	*	Connection broker instance	389	TCP	AD LDS access during unmanaged agent installation. **Note** For other uses of this port, see the note following this table.
Horizon Client	*	Connection broker 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 broker or Unified Access Gateway appliance	443	TCP	HTTPS for logging in to VMware Horizon. (This port is also used for tunneling when tunnel connections are used.)
Horizon Client	*	Connection broker 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 following this table.
Horizon Client	*	Horizon Agent	22443	TCP and UDP	VMware Blast
Horizon Client	*	Connection broker 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 broker	*	Connection broker	48080	TCP	For internal communication between Connection broker components.
Connection broker	*	vCenter Server	80	TCP	SOAP messages if TLS is disabled for access to vCenter Servers.

Table 1-10. TCP and UDP Ports Used by VMware Horizon (continued)

Source	Port	Target	Port	Protocol	Description
Connection broker	*	vCenter Server	443	TCP	SOAP messages if TLS is enabled for access to vCenter Servers.
Connection broker	*	Connection broker	4100	TCP	JMS inter-router traffic.
Connection broker	*	Connection broker	4101	TCP	JMS TLS inter-router traffic.
Connection broker	*	Connection broker	8472	TCP	For inter-pod communication in Cloud Pod Architecture.
Connection broker	*	Connection broker	22389	TCP	For global LDAP replication in Cloud Pod Architecture.
Connection broker	*	Connection broker	22636	TCP	For secure global LDAP replication in Cloud Pod Architecture.
Connection broker	*	Connection broker	32111	TCP	Key sharing traffic.
Connection broker	*	Certificate Authority	*	HTTP, HTTPS	CRL or OCSP queries
Unified Access Gateway appliance	*	Connection broker or load balancer	443	TCP	HTTPS access. Unified Access Gateway appliances connect on TCP port 443 to communicate with a Connection broker instance or load balancer in front of multiple connection broker 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 brokers 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 broker 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 the 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 the 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 and Upgrade* 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 and Upgrade* 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 the connection broker and the virtual desktop or published application for a certificate login associated with the TrueSSO solution.

Table 1-11. 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	Connection broker	TCP 443	HTTPS	Launch Horizon Client.
Connection broker	VMware Identity Manager appliance	TCP 443	HTTPS	Connection broker performs SAML resolve against VMware Identity Manager. VMware Identity Manager validates artifact and returns assertion.
Connection broker	Horizon Enrollment Server	TCP 32111		Use the Enrollment Server.

Table 1-11. TrueSSO Ports Used by VMware Horizon (continued)

Source	Target	Port	Protocol	Description
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	Connection broker	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 in to the Windows desktop or application and a remote session is initiated on Horizon Client.

Services on a Connection Server Host in a VMware Horizon 8 Environment

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

Table 1-12. 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.
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.

Table 1-12. Horizon Connection Server Host Services (continued)

Service Name	Startup Type	Description
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

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 brokers, and also between Horizon Agents and connection broker 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 broker instances or Horizon Agents.

The initial certificate thumbprints and setup message signing keys are provided in different ways. On connection brokers, certificate thumbprints are stored in LDAP, so that Horizon Agents can communicate with any connection broker, and all connection brokers 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 broker 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 broker remembers the cryptographic hash of the certificate for subsequent unattended acceptance using thumbprint verification.

Configuring Security Protocols and Cipher Suites on Connection Server for VMware Horizon 8

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 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.

Default Global Policies for Security Protocols and Cipher Suites

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

Security-related settings are provided in Horizon LDAP under the object path `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`.

Table 1-13. Default Global Acceptance Policy

Default Security Protocols	Default Cipher Suites	Default Signature Schemes
■ 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 ■ TLS_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_RSA_WITH_AES_256_CBC_SHA256	■ rsa_pss_rsae_sha512 ■ rsa_pss_rsae_sha384 ■ rsa_pss_rsae_sha256 ■ rsa_pss_pss_sha512 ■ rsa_pss_pss_sha384 ■ rsa_pss_pss_sha256 ■ rsa_pkcs1_sha512 ■ rsa_pkcs1_sha384 ■ rsa_pkcs1_sha256 ■ rsa_pkcs1_sha1 ■ ecdsa_secp521r1_sha512 ■ ecdsa_secp384r1_sha384 ■ ecdsa_secp256r1_sha256

Table 1-14. Default Global Proposal Policy

Default Security Protocols	Default Cipher Suites	Default Signature Schemes
■ 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	■ rsa_pss_rsae_sha512 ■ rsa_pss_rsae_sha384 ■ rsa_pss_rsae_sha256 ■ rsa_pss_pss_sha512 ■ rsa_pss_pss_sha384 ■ rsa_pss_pss_sha256 ■ rsa_pkcs1_sha512 ■ rsa_pkcs1_sha384 ■ rsa_pkcs1_sha256 ■ rsa_pkcs1_sha1

Table 1-15. Default Global Common Policy

Default Named Groups
■ secp384r1 ■ secp256r1 ■ secp521r1 ■ ffdhe2048 ■ ffdhe3072 ■ ffdhe4096 ■ ffdhe6144 ■ ffdhe8192

Note 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. Security-related settings are provided in Horizon LDAP under the object path `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`.

Global Acceptance Policies

Attribute	Description
`pae-ServerSSLSecureProtocols`	Lists security protocols. You must order the list by placing the latest protocol first. For example: `pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1`
`pae-ServerSSLCipherSuites`	Lists 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`
`pae-ServerSSLHonorClientOrder`	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`
`pae-SSLServerSignatureSchemes`	Lists certificate signature schemes. This example shows an abbreviated list: `pae-SSLServerSignatureSchemes = \LIST:rsa_pss_rsae_sha256,rsa_pkcs1_sha512,rsa_pkcs1_sha1`

Global Proposal Policies

Attribute	Description
`pae-ClientSSLSecureProtocols`	Lists security protocols. You must order the list by placing the latest protocol first: `pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1`
`pae-ClientSSLCipherSuites`	Lists 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`
`pae-SSLClientSignatureSchemes`	Lists certificate signature schemes. This example shows an abbreviated list: `pae-SSLClientSignatureSchemes = \LIST:rsa_pss_rsae_sha256,rsa_pkcs1_sha512,rsa_pkcs1_sha1`

Global Common Policies

Attribute	Description
`pae-SSLNamedGroups`	Lists named groups (elliptic curves and Diffie-Hellman groups), both proposed and accepted. This example shows an abbreviated list: `pae-SSLNamedGroups = \LIST:secp384r1,secp256r1,ffdhe2048`

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.

Note The `pae-ServerSSLSecureProtocols` and `pae-ClientSSLSecureProtocols` do not exist until you create them yourself.

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, enter the distinguished name **`DC=vdi, DC=vmware, DC=int`**.

4 In the **Select or type a domain or server** text box, select or enter **`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 enter 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 required 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.

Note It is not recommended that you make any changes to the values in the `SOFTWARE\VMware, Inc.\VMware VDM\Security` registry key. The values in this key are set using LDAP settings on the Connection Server and should not be edited in the Registry. For more information, see Global Acceptance and Proposal Policies Defined in Horizon LDAP.

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 new String (REG_SZ) values as described below.

String (REG_SZ) Value	Description
`ClientSSLSecureProtocols`	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`
`ClientSSLCipherSuites`	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.

Disabled Protocols and Ciphers

In VMware Horizon, the following protocols and ciphers are disabled by default:

- SSLv3

  For more information, see http://tools.ietf.org/html/rfc7568.

- TLSv1 and TLSv1.1

  For more information, see https://datatracker.ietf.org/doc/html/rfc8996 and https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf.

- RC4

  For more information, see http://tools.ietf.org/html/rfc7465.

DHE Cipher Suites

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 more information, see http://kb.vmware.com/kb/2121183.

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 Horizon Agent Direct-Connection Plug-In 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 and Upgrade* 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.

SHA-1

In FIPS mode, certificate verification will fail with "Certificates do not conform to algorithm constraints" if a certificate is signed using SHA-1. This applies to any certificate in the chain, including the root certificate. For more information about why this signature algorithm is deprecated, see https://cabforum.org/wp-content/uploads/BRv1.2.5.pdf.

Replace failing certificates if possible. If this cannot be done, SHA-1 signatures can be re-enabled by making an LDAP edit. Navigate to **CN=Common,OU=Global,OU=Properties,DC=vdi,DC=vmware,DC=int**. Modify attribute **pae-SSLClientSignatureSchemes** by adding **rsa_pkcs1_sha1** to the list of comma-separated values. Save the modified attribute and then restart the Connection Server service on each Connection Server in the cluster, one at a time.

No Forward Secrecy (PFS)

For more information, see https://datatracker.ietf.org/doc/html/rfc7525. Cipher suites specifying key exchange algorithms that do not exhibit forward secrecy (PFS) are disabled by default. For instructions on how to enable these cipher suites, see the other sections of this topic.

Re-enabling Protocols

Although the protocols listed above have been deprecated for good reasons, you might have a use case where you need to re-enable one or more of them. If so, you can enable protocols by following the procedure below.

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

Also see the section "Enable TLSv1 on vCenter Connections from Connection Server" in the *Horizon Installation and Upgrade* document.

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

```
TLS_RSA_WITH_RC4_128_SHA
```

Configuring Security Protocols and Cipher Suites for Blast Secure Gateway

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

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 broker 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

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

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 broker 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

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

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

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

Disabling USB Redirection for All Types of Devices

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

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

- When you install Horizon Agent on a desktop image or RDS host, deselect the **USB redirection** setup option. (The option is deselected by default.) This approach prevents access to USB devices on all remote desktops and applications that are deployed from the desktop image or RDS host.
- In the 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 the 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 1-16. 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 *Horizon Remote Desktop Features and GPOs*.

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.

Table 1-17. Exclude Options

Option	Description
`ExcludeAllDevices`	Excludes all devices from being redirected.
`ExcludeDeviceFamily`	Prevents specific device families from being redirected. For example, you can block all video, audio, and mass storage devices: `ExcludeDeviceFamily   o:video;audio;storage`

Table 1-17. Exclude Options (continued)

Option	Description
ExcludeVidPid	Prevents devices with specified vendor and product IDs from being redirected. The format of the setting is:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2]...` You must specify the VID or PID with a hexadecimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: vid-0781_pid-****_rel-0100;vid-7081_pid-5591_rel-0100
ExcludeVidPidRel	Prevents devices with specified vendor ID, product ID, and release number from being redirected. The format of the setting is:vid-xxx1_pid-yyy1_rel-zzz1[;vid-xxx2_pid-yyy2_rel-zzz2]...` You must specify the VID or PID with a hexadecimal and specify REL with a binary-coded decimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: vid-0781_pid-****_rel-0100;vid-7081_pid-5591_rel-0100

Table 1-18. Include Options

Option	Description
IncludeAllDevices	All devices are redirected.
IncludeDeviceFamily	All device families are redirected.
IncludeVidPid	Devices with specified vendor and product IDs are redirected. The format of the setting is `vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2]...` You must specify the VID or PID with a hexadecimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: vid-0781_pid-****_rel-0100;vid-7081_pid-5591_rel-0100
IncludeVidPidRel	Devices with specified vendor ID, product ID, and release number are redirected. The format of the setting is `vid-xxx1_pid-yyy1_rel-zzz1[;vid-xxx2_pid-yyy2_rel-zzz2]...` You must specify the VID or PID with a hexadecimal and specify REL with a binary-coded decimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: vid-0781_pid-****_rel-0100;vid-7081_pid-5591_rel-0100

By default, Horizon 8 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 USB access to any Horizon 8 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 *Horizon Remote Desktop Features and GPOs*.

Device Filtering Examples

- Block a single device:

  ```
  ExcludeVidPidRel o:vid-0781_pid-5591_rel-0100
  ```

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

- Block all devices with the same vendor and product ID except one with a specific release number:

  ```
  ExcludeVidPid o:vid-0781_pid-5591IncludeVidPidRel o:vid-0781_pid-5591_rel-0100
  ```

- Include all devices with the same vendor and product ID except one with a specific release number:

  ```
  IncludeVidPid o:vid-0781_pid-5591ExcludeVidPidRel o:vid-0781_pid-5591_rel-0100
  ```

Using Device Filtering Options

You can use device filtering options in one of the following ways:

- Registry key:

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Agent\USB
  ```

- Group Policy Object

  ```
  Local Computer Policy\Computer Configuration\Administrative
  Templates\VMware View Agent Configuration\View USB Configuration
  ```

HTTP Protection Measures on Connection Servers for VMware Horizon 8

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

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 click-jacking, is enabled by default. You can disable it by adding the entry `x-frame-options=OFF` to the file `locked.properties`. For information about adding 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.

Example:

```
hstsFlags.1=includeSubDomains
```

```
hstsFlags.2=preload
```

Note These properties are not set by default because they can affect URLs outside of Horizon 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 1-19. CORS Properties

Property	Value Type	Primary 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 1-19. CORS Properties (continued)

Property	Value Type	Primary 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 1-19. CORS Properties (continued)

Property	Value Type	Primary 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 1-20. CSP Properties

Property	Value Type	Primary 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 https://lumos.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 1-21. 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
`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 recognized 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 and a primary 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 primary value and a service-specific value are specified, then the service-specific value applies to the named service, and the primary value applies to all other services. The sole exception is the special value "OFF". If the primary 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

Horizon Client and Agent Security

This section describes the security features of VMware Horizon® Client™ and Horizon Agent.

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

External Ports

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

Understanding Communications Protocols

VMware Horizon components use several different protocols to exchange messages.

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

Table 1-22. Default Ports

Protocol	Port
JMS	TCP port 4001 TCP port 4002
HTTP	TCP port 80
HTTPS	TCP port 443
MMR/CDR	TCP port 9427 The following features use this port. ■ Windows multimedia redirection ■ Client drive redirection ■ Microsoft Teams optimization ■ HTML multimedia redirection ■ VMware printer redirection ■ USB redirection
RDP	TCP port 3389
PCoIP	TCP port 4172 UDP ports 4172, 50002, 55000
USB redirection	TCP port 32111. This port is also used for time zone synchronization.

Table 1-22. Default Ports (continued)

Protocol	Port
VMware Blast Extreme	TCP ports 8443, 22443 UDP ports 443, 8443, 22443
HTML Access	TCP ports 8443, 22443

Firewall Rules for Horizon Agent

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

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

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

If you change the RDP port number after installation, you must change the associated firewall rules. If you change a default port after installation, you must manually reconfigure the firewall rules to allow access on the updated port. For more information, see the *Horizon Installation and Upgrade* document.

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

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

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

Table 1-23. TCP and UDP Ports Opened During Horizon Agent Installation

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

Table 1-23. TCP and UDP Ports Opened During Horizon Agent Installation (continued)

Protocol	Ports
Multimedia redirection (MMR) and client drive redirection (CDR)	TCP port 9427 The following features use this port: ■ Windows multimedia redirection ■ Client drive redirection ■ Microsoft Teams optimization ■ HTML multimedia redirection ■ VMware printer redirection ■ USB redirection
PCoIP	For RDS hosts, PCoIP uses TCP port 4172 and UDP port 4172 (bidirectional). For virtual desktops, PCoIP uses port numbers selected from a configurable range. By default, PCoIP uses TCP ports 4172 to 4173 and UDP ports 4172 to 4182. The firewall rules do not specify port numbers. Instead, they dynamically follow the ports opened by each PCoIP server. The selected port numbers are communicated to the client through the connection broker instance.
VMware Blast	TCP port 22443 UDP port 22443 (bidirectional) **Note** UDP is not used on Linux desktops.
HTML Access	TCP port 22443
XDMCP	UDP 177 **Note** This port is opened for XDMCP access only on Linux desktops running Ubuntu 18.04. Firewall rules block all external host access to this port.
X11	TCP 6100 **Note** This port is opened for XServer access only on Linux desktops running Ubuntu 18.04. Firewall rules block all external host access to this port.

TCP and UDP Ports for Clients and Agents

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

Table 1-24. TCP and UDP Ports That Horizon Agent Uses

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

Table 1-24. TCP and UDP Ports That Horizon Agent Uses (continued)

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

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

Table 1-25. TCP and UDP Ports That Horizon Client Uses

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

Table 1-25. TCP and UDP Ports That Horizon Client Uses (continued)

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

Table 1-25. TCP and UDP Ports That Horizon Client Uses (continued)

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	Connection Server or Unified Access Gateway appliance	8443	UDP	VMware Blast when Blast Secure Gateway is used. **Note** Not used when connecting to a Linux desktop.
Connection Server or Unified Access Gateway appliance	8443	Horizon Client	*	UDP	VMware Blast when Blast Secure Gateway is used. **Note** Not used when connecting to a Linux desktop.

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

Installed Services, Daemons, and Processes

The Horizon Client and Horizon Agent installers install several components.

Horizon Agent Services on Windows Machines

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

Table 1-26. Horizon Agent Services

Service Name	Startup Type	Description
VMware Blast	Automatic	Provides services for HTML Access and for using the VMware Blast display protocol for connecting with native clients.
VMware Horizon View Agent	Automatic	Provides services for Horizon Agent.
VMware Horizon View Script Host	Disabled	Supports the running of start session scripts, if any, that configure desktop security policies before a desktop session begins. Policies are based on the client device and the user's location.
VMware Netlink Supervisor Service	Automatic	Supports the scanner redirection and the serial port redirection features by providing monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Agent	Automatic	Provides services for the scanner redirection feature.
VMware Serial Com Redirection Agent Service	Automatic	Provides services for the serial port redirection feature.

Table 1-26. Horizon Agent Services (continued)

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

Horizon Client Services on Windows Clients

The operation of Horizon Client depends on several Windows services.

Table 1-27. Horizon Client Services

Service Name	Startup Type	Description
VMware Horizon Client	Automatic	Provides Horizon Client services.
VMware Netlink Supervisor Service	Automatic	Supports the scanner redirection and serial port redirection features by providing monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Client Service	Automatic	Provides services for the scanner redirection feature.
VMware Serial Com Client Service	Automatic	Provides services for the serial port redirection feature.
VMware USB Arbitration Service	Automatic	Enumerates the various USB devices connected to the client and determines which devices to connect to the client and which to connect to the remote desktop.

Daemons in Non-Windows Clients and Linux Desktops

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

Table 1-28. Services, Processes, and Daemons by Horizon Client Type

Horizon Client Type	Service, Process, or Daemon
Linux client	■ `vmware-usbarbitrator`, which numerates the various USB devices connected to the client and determines which devices to connect to the client and which to connect to the remote desktop. ■ `vmware-view-used`, which provides services for the USB redirection feature. **Note** If you click the **Register and start the service(s) after installation** check box during installation, these daemons start automatically. These processes run as root.
Mac client	None
iOS client	None

Table 1-28. Services, Processes, and Daemons by Horizon Client Type (continued)

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

Resources to Secure

You must secure certain resources. These resources include relevant configuration files, passwords, and access controls.

Implementing Best Practices to Secure Client Systems

Implement these best practices to secure client systems.

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

Configuration File Locations

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

Table 1-29. Configuration File Locations by Client Type

Client Type	File Location
Linux client	When the Linux client starts, it processes configuration settings from the following directories in the following order: 1 `/etc/vmware/view-default-config` 2 `~/.vmware/view-preferences` 3 `/etc/vmware/view-mandatory-config` If a setting is defined in multiple locations, the Linux client uses the value from the last file or command-line option that it reads.
Windows client	User settings that might include some private information are in the following file: `C:\Users\`*`user-name`*`\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt`
Mac client	When the Mac client starts, it generates the following configuration files: ■ `$HOME/Library/Preferences/com.vmware.horizon.plist` ■ `$HOME/Library/Preferences/com.vmware.vmrc.plist` ■ `$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist` ■ `/Library/Preferences/com.vmware.horizon.plist`
iOS client	Security-related settings appear in the user interface rather than in configuration files.
Android client	Security-related settings appear in the user interface rather than in configuration files.
Horizon Agent (remote desktop with Windows operating system)	Security-related settings appear only in the Windows Registry.
Linux desktop	You can use a text editor to open the following configuration file and specify TLS-related settings: `/etc/vmware/viewagent-custom.conf`

Accounts

Client users must have accounts in Active Directory.

Horizon Client User Accounts

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

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

System Accounts Created During Installation

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

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

Horizon Agent does not create any service user accounts on Windows desktops. On Linux desktops, it creates a system account called `vmwblast`. On Linux desktops, the `StandaloneAgent` daemon runs with root privileges and the `VmwareBlastServer` daemon runs with `vmwblast` privileges.

Security Settings for the Client and Agent

Several client and agent settings are available for adjusting the security of the configuration. To access these settings for remote desktops and Windows clients, you can use group policy objects or Windows registry settings.

For configuration settings related to log collection, see the *Horizon Administration* document. For configuration settings related to security protocols and cipher suites, see Configuring Security Protocols and Cipher Suites.

For configuration settings related to the Linux Client, see the *Horizon Client for Linux Guide*.

Configuring Certificate Checking

Administrators can configure the certificate verification mode. Administrators can also configure whether end users can control whether client connections are rejected if server certificate checks fail.

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

- End users can choose the verification mode.
- (No verification) No certificate checks are performed.
- (Warn) End users are warned if a self-signed certificate is being presented by the server. Users can select whether to allow this type of connection.
- (Full security) Full verification is performed and connections that do not pass full verification are rejected.

Certificate verification includes the following checks:

- Has the certificate been revoked?
- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?

- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects Horizon Client to a server that has a certificate that does not match the host name entered in Horizon Client. A mismatch can also occur if you enter an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA. To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

If you use an SSL proxy server to inspect traffic that the client environment sends to the Internet, you can enable certificate checking for secondary connections through an SSL proxy server. You can also configure VMware Blast connections to use a proxy server.

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

Security-Related Settings in the Horizon Agent Configuration Templates

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

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

Table 1-30. Horizon Agent Security-Related Settings

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

Table 1-30. Horizon Agent Security-Related Settings (continued)

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

For more information about these settings and their security implications, see the *Horizon Remote Desktop Features and GPOs* document.

Group Policy Settings for HTML Access

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

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

Security Settings in the Horizon Client Configuration Templates

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

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

Configuring the Horizon Client Certificate Verification Mode

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

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

Use one of the following values in the registry key:

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

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

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

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

Configuring Local Security Authority Protection

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

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

Using the Legacy Microsoft CryptoAPI Standard

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

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

Configuring Security Protocols and Cipher Suites

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

Default Policies for Security Protocols and Cipher Suites

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

The following table lists the protocols and cipher suites that are enabled by default for Horizon Client. In Horizon Client for Windows, Linux, and Mac, these cipher suites and protocols are also used to encrypt the USB channel (communication between the USB service daemon and Horizon Agent). RC4 is not supported.

Table 1-31. Security Protocols and Cipher Suites Enabled by Default in Horizon Client

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

Configuring Security Protocols and Cipher Suites for Specific Client Types

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

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

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

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

For more information, see the Horizon Client documentation.

Disable Weak Ciphers in SSL/TLS

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

Procedure

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

   ```
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
   ```

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

   Note In FIPS mode, list GCM cipher suites only.

6. Exit the Group Policy Management Editor.
7. To make the new group policy take effect, restart the Horizon Agent machines.

Configure Security Protocols and Cipher Suites for HTML Access Agent

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

By default, the HTML Access Agent uses only TLS 1.0, TLS 1.1, and TLS 1.2. Older protocols such as SSLv3 and earlier are never allowed. Two registry values, `SslProtocolLow` and `SslProtocolHigh`, determine the range of protocols that the HTML Access Agent accepts. For example, setting `SslProtocolLow=tls_1.1` and `SslProtocolHigh=tls_1.2` causes the HTML Access Agent to accept TLS 1.1 and TLS 1.2. The default settings are `SslProtocolLow=tls_1.2` and `SslProtocolHigh=tls_1.2`, and therefore by default the HTML Access Agent accepts only TLS 1.2.

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

```
ECDHE+AESGCM
```

Procedure

1 Start the Windows Registry Editor.

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

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

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

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

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

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

5 Restart the VMware Blast Windows service.

Results

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

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

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

Configure Proposal Policies on Remote Desktops

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

Note It is not recommended that you make any changes to the values in the `SOFTWARE\VMware, Inc.\VMware VDM\Security` registry key. The values in this key are set using LDAP settings on the Connection Server and should not be edited in the Registry. For more information, see Global Acceptance and Proposal Policies Defined in Horizon LDAP.

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 new String (REG_SZ) values as described below.

String (REG_SZ) Value	Description
`ClientSSLSecureProtocols`	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`
`ClientSSLCipherSuites`	Set the value to a list of cipher suites in the format `\LIST:`*`cipher_suite_1`*`,`*`cipher_suite_2`*`,....` The list must be in order of preference, with the most preferred cipher suite first. For example: `\LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA`

Applying Security Patches

Patch releases might include installer files for Connection Server, Horizon Agent, and Horizon Client. The patch components that you must apply depend on the bug fixes that your deployment requires.

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

1 Connection Server

2 Horizon Agent

3 Horizon Client

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

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

Scenarios for Setting Up TLS Certificates for Horizon 8

This section provides examples of setting up TLS certificates for use by Horizon 8 servers. The first scenario shows you how to obtain signed TLS certificates from a Certificate Authority and ensure that the certificates are in a format that can be used by Horizon 8 servers. The second scenario shows you how to configure Horizon 8 servers to off-load TLS connections to an intermediate server.

Obtaining TLS Certificates from a Certificate Authority

VMware strongly recommends that you configure TLS certificates that are signed by a valid Certificate Authority (CA) for use by Horizon Connection Server instances.

Default TLS certificates are generated when you install Connection Server. Although you can use the default, self-signed certificates for testing purposes, replace them as soon as possible. The default certificates are not signed by a CA. Use of certificates that are not signed by a CA can allow untrusted parties to intercept traffic by masquerading as your server.

In a Horizon 8 environment, replace the default certificate that is installed with vCenter Server with a certificate that is signed by a CA. You can use `openTLS` to perform this task for vCenter Server. For details, see "Replacing vCenter Server Certificates" on the VMware Technical Papers site at http://www.vmware.com/resources/techresources/.

Determining If This Scenario Applies to You

You configure certificates for Horizon 8 by importing the certificates into the Windows local computer certificate store on the Horizon 8 server host.

Before you can import a certificate, you must generate a Certificate Signing Request (CSR) and obtain a valid, signed certificate from a CA. If the CSR is not generated according to the example procedure described in this scenario, the resulting certificate and its private key must be available in a PKCS#12 (formerly called PFX) format file.

There are many ways to obtain TLS certificates from a CA. This scenario shows how to use the Microsoft `certreq` utility to generate a CSR and make a certificate available to a Horizon 8 server. You can use another method if you are familiar with the required tools and they are installed on your server.

Use this scenario to solve the following problems:

- You do not have TLS certificates that are signed by a CA, and you do not know how to obtain them
- You have valid, signed TLS certificates, but they are not in PKCS#12 (PFX) format

If your organization provides you with TLS certificates that are signed by a CA, you can use these certificates. Your organization can use a valid internal CA or a third-party, commercial CA. If your certificates are not in PKCS#12 format, you must convert them. See Convert a Certificate File to PKCS#12 Format.

When you have a signed certificate in the proper format, you can import it into the Windows certificate store and configure a Horizon 8 server to use it. See Set Up an Imported Certificate for a Horizon 8 Server.

Selecting the Correct Certificate Type

You can use various types of TLS certificates with Horizon 8. Selecting the correct certificate type for your deployment is critical. Different certificate types vary in cost, depending on the number of servers on which they can be used.

Follow VMware security recommendations by using fully qualified domain names (FQDNs) for your certificates, no matter which type you select. Do not use a simple server name or IP address, even for communications within your internal domain.

Single Server Name Certificate

You can generate a certificate with a subject name for a specific server. For example: `dept.company.com`.

This type of certificate is useful if, for example, only one Connection Server instance needs a certificate.

When you submit a certificate signing request to a CA, you provide the server name that will be associated with the certificate. Be sure that the Horizon 8 server can resolve the server name you provide so that it matches the name associated with the certificate.

Subject Alternative Names

A Subject Alternative Name (SAN) is an attribute that can be added to a certificate when it is being issued. You use this attribute to add subject names (URLs) to a certificate so that it can validate more than one server.

For example, a certificate might be issued for a server with the host name `dept.company.com`. You intend the certificate to be used by external users connecting to Horizon 8 through Connection Server. Before the certificate is issued, you can add the SAN `dept-int.company.com` to the certificate to allow the certificate to be used on Connection Server instances behind a load balancer when tunneling is enabled.

Wildcard Certificate

A wildcard certificate is generated so that it can be used for multiple services. For example: `*.company.com`.

A wildcard is useful if many servers need a certificate. If other applications in your environment in addition to Horizon 8 need TLS certificates, you can use a wildcard certificate for those servers, too. However, if you use a wildcard certificate that is shared with other services, the security of the VMware Horizon product also depends on the security of those other services.

Note You can use a wildcard certificate only on a single level of domain. For example, a wildcard certificate with the subject name `*.company.com` can be used for the subdomain `dept.company.com` but not `dept.it.company.com`.

Generating a Certificate Signing Request and Obtaining a Certificate with Microsoft Certreq

To make a certificate available to a Horizon 8 server, you must create a configuration file, generate a certificate signing request (CSR) from the configuration file, and send the signing request to a CA. When the CA returns the certificate, you must import the signed certificate into the Windows local computer certificate store on the Horizon 8 server host, where it joins the previously generated private key.

A CSR can be generated in several ways, depending on how the certificate itself will be generated.

Procedure

1 Create a CSR Configuration File

   The Microsoft `certreq` utility uses a configuration file to generate a CSR. You must create a configuration file before you can generate the request. Create the file and generate the CSR on the Windows Server computer that hosts the Horizon 8 server that will use the certificate.

2 Generate a CSR and Request a Signed Certificate from a CA

   Using the completed configuration file, you can generate a CSR by running the `certreq` utility. You send the request to a third-party CA, which returns a signed certificate.

3 Verify That the CSR and Its Private Key Are Stored in the Windows Certificate Store

   If you use the `certreq` utility to generate a CSR, the utility also generates an associated private key. The utility stores the CSR and private key in the Windows local computer certificate store on the computer on which you generated the CSR. You can confirm that the CSR and private key are properly stored by using the Microsoft Management Console (MMC) Certificate snap-in.

4 Import a Signed Certificate by Using Certreq

   When you have a signed certificate from a CA, you can import the certificate into the Windows local computer certificate store on the Horizon 8 server host.

5 Set Up an Imported Certificate for a Horizon 8 Server

After you import a server certificate into the Windows local computer certificate store, you must take additional steps to allow a Horizon 8 server to use the certificate.

Create a CSR Configuration File

The Microsoft `certreq` utility uses a configuration file to generate a CSR. You must create a configuration file before you can generate the request. Create the file and generate the CSR on the Windows Server computer that hosts the Horizon 8 server that will use the certificate.

Prerequisites

Gather the information required to fill out the configuration file. You must know the FQDN of the Horizon 8 server and the organizational unit, organization, city, state, and country to complete the Subject name.

Procedure

1 Open a text editor and paste the following text, including the beginning and ending tags, into the file.

```
;----------------- request.inf -----------------

[Version]

Signature="$Windows NT$"

[NewRequest]

Subject = "CN=View_Server_FQDN, OU=Organizational_Unit, O=Organization, L=City, S=State,
C=Country"
; Replace View_Server_FQDN with the FQDN of the Horizon server.
; Replace the remaining Subject attributes.
KeySpec = 1
KeyLength = 2048
; KeyLength is usually chosen from 2048, 3072, or 4096. A KeyLength
; of 1024 is also supported, but it is not recommended.
HashAlgorithm = SHA256
; Algorithms earlier than SHA-2 are insufficiently secure and are not recommended.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]
```

```
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

;-----------------------------------------------
```

If an extra CR/LF character is added to the `Subject =` line when you copy and paste the text, delete the CR/LF character.

2 Update the `Subject` attributes with appropriate values for your Horizon 8 server and deployment.

   For example: `CN=dept.company.com`

   To comply with VMware security recommendations, use the fully qualified domain name (FQDN) that client devices use to connect to the host. Do not use a simple server name or IP address, even for communications within your internal domain.

   Some CAs do not allow you to use abbreviations for the state attribute.

3 (Optional) Update the `Keylength` attribute.

   The default value, 2048, is adequate unless you specifically need a different `KeyLength` size. Many CAs require a minimum value of 2048. Larger key sizes are more secure but have a greater impact on performance.

   A `KeyLength` of 1024 is also supported, although the National Institute of Standards and Technology (NIST) recommends against keys of this size, as computers continue to become more powerful and can potentially crack stronger encryption.

   Important Do not generate a `KeyLength` value under 1024. Horizon Client for Windows will not validate a certificate on a Horizon 8 server that was generated with a `KeyLength` under 1024, and the Horizon Client devices will fail to connect to Horizon 8. Certificate validations that are performed by Connection Server will also fail, resulting in the affected Horizon 8 servers showing as red in the console dashboard.

4 Save the file as `request.inf`.

What to do next

Generate a CSR from the configuration file.

Generate a CSR and Request a Signed Certificate from a CA

Using the completed configuration file, you can generate a CSR by running the `certreq` utility. You send the request to a third-party CA, which returns a signed certificate.

Prerequisites

- Verify that you completed a CSR configuration file. See Create a CSR Configuration File.
- Perform the `certreq` operation described in this procedure on the computer where the CSR configuration file is located.

Procedure

1 Open a command prompt by right-clicking on **Command Prompt** in the **Start** menu and selecting **Run as administrator**.

2 Navigate to the directory where you saved the `request.inf` file.

   For example: **`cd c:\certificates`**

3 Generate the CSR file.

   For example: **`certreq -new request.inf certreq.txt`**

4 Use the contents of the CSR file to submit a certificate request to the CA in accordance with the CA's enrollment process.

   a When you submit the request to a CA, the CA prompts you to select the type of server on which you will install the certificate. Since Horizon 8 uses the Microsoft Certificates MMC to manage certificates, select a certificate for a server type of Microsoft, Microsoft IIS 7, or something similar. The CA should produce a certificate in the format needed to work with Horizon 8.

   b If you request a single server name certificate, use a name that Horizon Client devices can resolve into an IP address for this Horizon 8 server. The name that computers use to connect to the Horizon 8 server should match the name associated with the certificate.

   Note The CA might require that you copy and paste the contents of the CSR file (such as `certreq.txt`) into a Web form. Using a text editor, you can copy the contents of the CSR file. Be sure to include the beginning and ending tags. For example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAsICAQAwazEWMBQGA1UEBhMNVW5pdGVkIFN0YXRlczELMAkGA1UECAwC
Q0ExEjAQBgNVBAcMCVBhbG8gQWx0bzEKMAgGA1UECgwBTzELMAkGA1UECwwCT1Ux
FzAVBgNVBAMMDm15LmNvbXBhbnkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
. . .
. . .
L9nPYX76jeu5rwQfXLivSCea6nZiIOZYw8Dbn8dgwAqpJdzBbrwuM1TuSnx6bAK8
S52Tv0GxW58jUTtxFV+Roz8TE8wZDFB51jx+FmLs
-----END NEW CERTIFICATE REQUEST-----
```

   After conducting some checks on your company, the CA creates a server certificate based on the information in the CSR, signs it with its private key, and sends you the certificate.

   The CA also sends you a root CA certificate and, if applicable, an intermediate CA certificate.

5 Rename the certificate text file to `cert.cer`.

   Make sure that the file is located on the Horizon 8 server on which the certificate request was generated.

6 Rename the root CA and intermediate CA certificate files to `root.cer` and `intermediate.cer`.

   Make sure that the files are located on the Horizon 8 server on which the certificate request was generated.

   Note These certificates do not have to be in PKCS#12 (PFX) format when you use the `certreq` utility to import the certificates into the Windows local computer certificate store. PKCS#12 (PFX) format is required when you use the Certificate Import wizard to import certificates into the Windows certificate store.

What to do next

Verify that the CSR file and its private key were stored in the Windows local computer certificate store.

Verify That the CSR and Its Private Key Are Stored in the Windows Certificate Store

If you use the `certreq` utility to generate a CSR, the utility also generates an associated private key. The utility stores the CSR and private key in the Windows local computer certificate store on the computer on which you generated the CSR. You can confirm that the CSR and private key are properly stored by using the Microsoft Management Console (MMC) Certificate snap-in.

The private key must later be joined with the signed certificate to enable the certificate to be properly imported and used by a Horizon 8 server.

Prerequisites

- Verify that you generated a CSR by using the `certreq` utility and requested a signed certificate from a CA. See Generate a CSR and Request a Signed Certificate from a CA.
- Familiarize yourself with the procedure for adding a Certificate snap-in to the Microsoft Management Console (MMC). See "Add the Certificate Snap-in to MMC" in the chapter, "Configuring TLS Certificates for Horizon 8 Servers," in the *Horizon Installation and Upgrade* document.

Procedure

1 On the Windows Server computer, add the Certificate snap-in to MMC.

2 In the MMC window on the Windows Server computer, expand the **Certificates (Local Computer)** node and select the **Certificate Enrollment Request** folder.

3 Expand the **Certificate Enrollment Request** folder and select the **Certificates** folder.

4 Verify that the certificate entry is displayed in the **Certificates** folder.

   The **Issued To** and **Issued By** fields must show the domain name that you entered in the **`subject:CN`** field of the `request.inf` file that was used to generate the CSR.

5 Verify that the certificate contains a private key by taking one of the following steps:

   - Verify that a yellow key appears on the certificate icon.

  - Double-click the certificate and verify that the following statement appears in the Certificate Information dialog box: `You have a private key that corresponds to this certificate.`.

What to do next

Import the certificate into the Windows local computer certificate store.

Import a Signed Certificate by Using Certreq

When you have a signed certificate from a CA, you can import the certificate into the Windows local computer certificate store on the Horizon 8 server host.

If you used the `certreq` utility to generate a CSR, the certificate private key is local to the server on which you generated the CSR. To work correctly, the certificate must be combined with the private key. Use the `certreq` command shown in this procedure to ensure that the certificate and private key are properly combined and imported into the Windows certificate store.

If you use another method to obtain a signed certificate from a CA, you can use the Certificate Import wizard in the Microsoft Management Console (MMC) Snap-in to import a certificate into the Windows certificate store. This method is described in "Configuring TLS Certificates for Horizon 8 Servers" in the *Horizon Installation and Upgrade* document.

Prerequisites

- Verify that you received a signed certificate from a CA. See Generate a CSR and Request a Signed Certificate from a CA.
- Perform the `certreq` operation described in this procedure on the computer on which you generated a CSR and stored the signed certificate.

Procedure

1. Open a command prompt by right-clicking on **Command Prompt** in the **Start** menu and selecting **Run as administrator**.
2. Navigate to the directory where you saved the signed certificate file such as `cert.cer`.

   For example: **`cd c:\certificates`**
3. Import the signed certificate by running the `certreq -accept` command.

   For example: **`certreq -accept cert.cer`**

Results

The certificate is imported into the Windows local computer certificate store.

What to do next

Configure the imported certificate to be used by a Horizon 8 server. See Set Up an Imported Certificate for a Horizon 8 Server.

Set Up an Imported Certificate for a Horizon 8 Server

After you import a server certificate into the Windows local computer certificate store, you must take additional steps to allow a Horizon 8 server to use the certificate.

Procedure

1. Verify that the server certificate was imported successfully.
2. Change the certificate Friendly name to **`vdm`**.

   `vdm` must be lower case. Any other certificates with the Friendly name **`vdm`** must be renamed, or you must remove the Friendly name from those certificates.
3. Install the root CA certificate and intermediate CA certificate in the Windows certificate store.
4. Restart the Connection Server service to allow the service to start using the new certificates.
5. If you use HTML Access, restart the Blast Secure Gateway service.

Results

To perform the tasks in this procedure, see the following topics:

- Modify the Certificate Friendly Name
- Import the Root and Intermediate Certificates into the Windows Certificate Store

For more information, see "Configure Connection Server to Use a New TLS Certificate" in the *Horizon Installation and Upgrade* document.

Note The *Horizon Installation and Upgrade* topic "Import a Signed Server Certificate into a Windows Certificate Store" is not listed here because you already imported the server certificate by using the `certreq` utility. You should not use the Certificate Import wizard in the MMC Snap-in to import the server certificate again.

However, you can use the Certificate Import wizard to import the root CA certificate and intermediate CA certificate into the Windows certificate store.

Off-loading TLS Connections to Intermediate Servers

You can set up intermediate servers between your Horizon 8 servers and Horizon Client devices to perform tasks such as load balancing and off-loading TLS connections. Horizon Client devices connect over HTTPS to the intermediate servers, which pass on the connections to the external-facing Connection Server instances.

To off-load TLS connections to an intermediate server, you must complete a few key tasks:

- Import the TLS certificate that is used by the intermediate server to your external-facing Horizon 8 servers.
- Set the External URLs on your external-facing Horizon 8 servers to match the URL that clients can use to connect to the intermediate server.
- Allow HTTP connections between the intermediate server and the Horizon 8 servers.

Import TLS Off-loading Servers' Certificates to Horizon 8 Servers

If you off-load TLS connections to an intermediate server, you must import the intermediate server's certificate onto the Connection Server instances that connect to the intermediate server. The same TLS server certificate must reside on both the off-loading intermediate server and each off-loaded Horizon 8 server that connects to the intermediate server.

If you have a mixed network environment with some intermediate servers and some external-facing Connection Server instances, the intermediate server and any Connection Server instances that connect to it must have the same TLS certificate.

If the intermediate server's certificate is not installed on the Connection Server instance, clients cannot validate their connections to Horizon 8. In this situation, the certificate thumbprint sent by the Horizon 8 server does not match the certificate on the intermediate server to which Horizon Client connects.

Do not confuse load balancing with TLS off-loading. The preceding requirement applies to any device that is configured to provide TLS off-loading, including some types of load balancers. However, pure load balancing does not require copying of certificates between devices.

Procedure

1 Download an TLS Certificate from the Intermediate Server

   You must download the CA-signed TLS certificate that is installed on the intermediate server so that it can be imported into the external-facing Horizon 8 servers.

2 Download a Private Key from the Intermediate Server

   You must download the private key that is associated with the TLS certificate on the intermediate server. The private key must be imported with the certificate into the Horizon 8 servers.

3 Convert a Certificate File to PKCS#12 Format

   If you obtained a certificate and its private key in PEM or another format, you must convert it to PKCS#12 (PFX) format before you can import the certificate into a Windows certificate store on a Horizon 8 server. PKCS#12 (PFX) format is required if you use the Certificate Import wizard in the Windows certificate store.

4 Import a Signed Server Certificate into a Windows Certificate Store

   You must import the TLS server certificate into the Windows local computer certificate store on the Windows Server host on which Connection Server is installed.

5 Modify the Certificate Friendly Name

   To configure a Connection Server instance to recognize and use an TLS certificate, you must modify the certificate Friendly name to `vdm`.

6 Import the Root and Intermediate Certificates into the Windows Certificate Store

   You must import the root certificate and any intermediate certificates in the certificate chain into the Windows local computer certificate store.

Download an TLS Certificate from the Intermediate Server

You must download the CA-signed TLS certificate that is installed on the intermediate server so that it can be imported into the external-facing Horizon 8 servers.

Procedure

1 Connect to the intermediate server and find the TLS certificates that are presented to clients sending HTTPS requests.

2 Find and download the TLS certificate that is used for Horizon 8.

Example: Download an TLS Certificate from an F5 BIG-IP LTM System

This example uses F5 BIG-IP Local Traffic Manager (LTM) as an intermediate server. The example is intended to give you a general idea of how you might download a certificate from your own intermediate server.

Important These steps are specific to F5 BIG-IP LTM and may not apply to new releases or other F5 products. The steps do not apply to other vendors' intermediate servers.

Before you start, verify that the F5 BIG-IP LTM system is deployed with Horizon 8. Check that you completed the tasks in the F5 deployment guide, *Deploying the BIG-IP LTM System with VMware View*, located at http://www.f5.com/pdf/deployment-guides/f5-vmware-view-dg.pdf.

1 Connect to the F5 BIG-IP LTM configuration utility.

2 On the Main tab of the navigation pane, expand **Local Traffic** and click **SSL certificates**.

  The utility displays a list of certificates that are installed on the system.

3 In the Name column, click the name of the certificate that is used for Horizon 8.

4 At the bottom of the screen, click **Export**.

  The utility displays the existing TLS certificate in the **Certificate Text** box.

5 From the **Certificate File** setting, click **Download** ***file_ name***.

  The TLS certificate is downloaded as a CRT file.

Download a Private Key from the Intermediate Server

You must download the private key that is associated with the TLS certificate on the intermediate server. The private key must be imported with the certificate into the Horizon 8 servers.

Procedure

1 Connect to the intermediate server and find the TLS certificates that are presented to clients sending HTTPS requests.

2 Find the certificate that is used for Horizon 8 and download its private key.

Example: Download a Private Key from a F5 BIG-IP LTM System

This example uses F5 BIG-IP Local Traffic Manager (LTM) as an intermediate server. The example is intended to give you a general idea of how you might download a private key from your own intermediate server.

Important These steps are specific to F5 BIG-IP LTM and may not apply to new releases or other F5 products. The steps do not apply to other vendors' intermediate servers.

Before you start, verify that you are connected to the F5 BIG-IP LTM configuration utility.

1. On the Main tab of the navigation pane, expand **Local Traffic** and click **SSL certificates**.

   The utility displays a list of certificates installed on the system.

2. In the Name column, click the name of the certificate that is used for Horizon 8.

3. On the menu bar, click **Key**.

4. At the bottom of the screen, click **Export**.

   The utility displays the existing private key in the **Key Text** box.

5. From the Key File setting, click **Download** ***file_ name.***.

   The private key is downloaded as a KEY file.

Convert a Certificate File to PKCS#12 Format

If you obtained a certificate and its private key in PEM or another format, you must convert it to PKCS#12 (PFX) format before you can import the certificate into a Windows certificate store on a Horizon 8 server. PKCS#12 (PFX) format is required if you use the Certificate Import wizard in the Windows certificate store.

You might obtain certificate files in one of these ways:

- You obtain a certificate keystore file from a CA.
- You download a certificate and its private key from an intermediate server that is set up in your Horizon 8 deployment.
- Your organization provides you with certificate files.

Certificate files come in various formats. For example, PEM format is often used in a Linux environment. Your files might have a certificate file, key file, and CSR file with the following extensions:

```
server.crt
server.csr
server.key
```

The CRT file contains the SSL certificate that was returned by the CA. The CSR file is the original certificate signing request file and is not needed. The KEY file contains the private key.

Prerequisites

- Verify that OpenSSL is installed on the system. You can download `openssl` from `http://www.openssl.org`.
- Verify that the root certificate of the SSL certificate that was returned by the CA is also available on the system.

Procedure

1 Copy the CRT and KEY files to the OpenSSL installation directory.

For example: `cd c:\OpenSSL-Win32\bin`

2 Open a Windows command prompt and, if necessary, navigate to the OpenSSL installation directory.

3 Generate a PKCS#12 (PFX) keystore file from the certificate file and your private key.

For example: `openssl pkcs12 -export -out server.p12 -inkey server.key -in server.crt -certfile CACert.crt`

In this example, `CACert.crt` is the name of the root certificate that was returned by the certificate authority.

The Windows certificate store also accepts a keystore that is generated with a PFX extension. For example: `-out server.pfx`

4 Type an export password to protect the PKCS#12 (PFX) file.

Import a Signed Server Certificate into a Windows Certificate Store

You must import the TLS server certificate into the Windows local computer certificate store on the Windows Server host on which Connection Server is installed.

Depending on your certificate file format, the entire certificate chain that is contained in the keystore file might be imported into the Windows local computer certificate store. For example, the server certificate, intermediate certificate, and root certificate might be imported.

For other types of certificate files, only the server certificate is imported into the Windows local computer certificate store. In this case, you must take separate steps to import the root certificate and any intermediate certificates in the certificate chain.

For more information about certificates, consult the Microsoft online help available with the Certificate snap-in to MMC.

Prerequisites

Procedure

1 In the MMC window on the Windows Server host, expand the **Certificates (Local Computer)** node and select the **Personal** folder.

2 In the Actions pane, go to **More Actions > All Tasks > Import**.

3 In the **Certificate Import** wizard, click **Next** and browse to the location where the certificate is stored.

4 Select the certificate file and click **Open**.

   To display your certificate file type, you can select its file format from the **File name** drop-down menu.

5 Type the password for the private key that is included in the certificate file.

6 Select **Mark this key as exportable**.

7 Select **Include all extended properties**.

8 Click **Next** and click **Finish**.

   The new certificate appears in the **Certificates (Local Computer) > Personal > Certificates** folder.

9 Verify that the new certificate contains a private key.

   a In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.

   b In the General tab of the Certificate Information dialog box, verify that the following statement appears: `You have a private key that corresponds to this certificate`.

What to do next

Modify the certificate Friendly name to **`vdm`**.

Modify the Certificate Friendly Name

To configure a Connection Server instance to recognize and use an TLS certificate, you must modify the certificate Friendly name to `vdm`.

Prerequisites

Verify that the server certificate is imported into the **Certificates (Local Computer) > Personal > Certificates** folder in the Windows Certificate Store. See Import a Signed Server Certificate into a Windows Certificate Store.

Procedure

1 In the MMC window on the Windows Server host, expand the **Certificates (Local Computer)** node and select the **Personal > Certificates** folder.

2 Right-click the certificate that is issued to the VMware Horizon 8 server host and click **Properties**.

3 On the General tab, delete the **Friendly name** text and type **`vdm`**.

4 Click **Apply** and click **OK**.

5 Verify that no other server certificates in the **Personal > Certificates** folder have a Friendly name of `vdm`.

   a Locate any other server certificate, right-click the certificate, and click **Properties**.

   b If the certificate has a Friendly name of `vdm`, delete the name, click **Apply**, and click **OK**.

What to do next

Import the root certificate and intermediate certificates into the Windows local computer certificate store.

After all certificates in the chain are imported, you must restart the Connection Server service to make your changes take effect.

Import the Root and Intermediate Certificates into the Windows Certificate Store

You must import the root certificate and any intermediate certificates in the certificate chain into the Windows local computer certificate store.

If the TLS server certificate that you imported from the intermediate server is signed by a root CA that is known and trusted by the Connection Server host, and there are no intermediate certificates in your certificate chains, you can skip this task. Commonly used Certificate Authorities are likely to be trusted by the host.

Procedure

1 In the MMC console on the Windows Server host, expand the **Certificates (Local Computer)** node and go to the **Trusted Root Certification Authorities > Certificates** folder.

   - If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip to step 7.
   - If your root certificate is in this folder, and there are intermediate certificates in your certificate chain, skip to step 6.
   - If your root certificate is not in this folder, proceed to step 2.

2 Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

3 In the **Certificate Import** wizard, click **Next** and browse to the location where the root CA certificate is stored.

4 Select the root CA certificate file and click **Open**.

5 Click **Next**, click **Next**, and click **Finish**.

6 If your server certificate was signed by an intermediate CA, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

   a Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

   b Repeat steps 3 through 6 for each intermediate certificate that must be imported.

7 If you use HTML Access, restart the Blast Secure Gateway service.

Set Horizon 8 Server External URLs to Point Clients to TLS Off-loading Servers

If TLS is off-loaded to an intermediate server and Horizon Client devices use the secure tunnel to connect to Horizon 8, you must set the secure tunnel external URL to an address that clients can use to access the intermediate server.

You configure the external URL settings on the Connection Server instance that connects to the intermediate server.

If you have a mixed network environment with some intermediate servers and some external-facing Connection Server instances, External URLs are required for any Connection Server instances that connect to the intermediate server.

Note You cannot off-load TLS connections from a PCoIP Secure Gateway (PSG) or Blast Secure Gateway. The PCoIP external URL and Blast Secure Gateway external URL must allow clients to connect to the computer that hosts the PSG and Blast Secure Gateway. Do not reset the PCoIP external URL and Blast external URL to point to the intermediate server unless you plan to require TLS connections between the intermediate server and the Horizon 8 server.

Set the External URLs for a Connection Server Instance

You use Horizon Console to configure the external URLs for a Connection Server instance.

Prerequisites

Verify that the secure tunnel connections are enabled on the Connection Server instance.

Procedure

1 In Horizon Console, click **Settings > Servers**.

2 Select **Connection Servers**, select a Connection Server instance, and click **Edit**.

3 Type the secure tunnel external URL in the **External URL** text box.

The URL must contain the protocol, client-resolvable host name and port number.

For example: `https://myserver.example.com:443`

Note You can use the IP address if you have to access a Connection Server instance when the host name is not resolvable. However, the host that you contact will not match the TLS certificate that is configured for the Connection Server instance, resulting in blocked access or access with reduced security.

4 Verify that all addresses in this dialog allow client systems to reach this Connection Server instance.

5 Click **OK**.

Allow HTTP Connections From Intermediate Servers

When TLS is off-loaded to an intermediate server, you can configure Connection Server instances to allow HTTP connections from the client-facing, intermediate devices. The intermediate devices must accept HTTPS for Horizon Client connections.

To allow HTTP connections between Horizon 8 servers and intermediate devices, you must configure the `locked.properties` file on each Connection Server instance on which HTTP connections are allowed.

Even when HTTP connections between Horizon 8 servers and intermediate devices are allowed, you cannot disable TLS in Horizon 8. Horizon 8 servers continue to accept HTTPS connections as well as HTTP connections.

Note If your Horizon 8 clients use smart card authentication, the clients must make HTTPS connections directly to Connection Server. TLS off-loading is not supported with smart card authentication.

Procedure

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

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

2 To configure the Horizon 8 server's protocol, add the `serverProtocol` property and set it to `http`.

   The value `http` must be typed in lower case.

3 (Optional) Add properties to configure a non-default HTTP listening port and a network interface on the Horizon 8 server.

   - To change the HTTP listening port from 80, set `serverPortNonTLS` to another port number to which the intermediate device is configured to connect.
   - If the Horizon 8 server has more than one network interface, and you intend the server to listen for HTTP connections on only one interface, set `serverHostNonTLS` to the IP address of that network interface.

4 Save the `locked.properties` file.

5 Restart the Connection Server service to make your changes take effect.

Example: locked.properties file

This file allows non-TLS HTTP connections to a Horizon 8 server. The IP address of the Horizon 8 server's client-facing network interface is 10.20.30.40. The server uses the default port 80 to listen for HTTP connections. The value `http` must be lower case.

```
serverProtocol=http
serverHostNonTLS=10.20.30.40
```