

Horizon Client and View Agent Security

Horizon Client 3.x and View Agent 6.2.x

VMware Horizon 6 6.2

vmware[®]

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

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

Contents

Horizon Client and View Agent Security	5
1 External Ports	7
Understanding View Communications Protocols	7
Firewall Rules for View Agent	8
TCP and UDP Ports Used by Clients and View Agent	8
2 Installed Services, Daemons, and Processes	11
Services Installed by the View Agent Installer on Windows Machines	11
Services Installed on the Windows Client	12
Daemons Installed in Other Clients and the Linux Desktop	12
3 Resources to Secure	15
Implementing Best Practices to Secure Client Systems	15
Configuration File Locations	15
Accounts	16
4 Security Settings for the Client and Agent	17
Configuring Certificate Checking	17
Security-Related Settings in the View Agent Configuration Template	18
Setting Options in Configuration Files on a Linux Desktop	19
HTML Access Group Policy Settings	21
Security Settings in the Horizon Client Configuration Templates	21
5 Configuring Security Protocols and Cipher Suites	27
Default Policies for Security Protocols and Cipher Suites	27
Configuring Security Protocols and Cipher Suites for Specific Client Types	29
Disable Weak Ciphers in SSL/TLS	30
Configure Security Protocols and Cipher Suites for HTML Access Agent	30
Configure Proposal Policies on View Desktops	31
6 Client and Agent Log File Locations	33
Horizon Client for Windows Logs	33
Horizon Client for Mac OS X Logs	35
Horizon Client for Linux Logs	36
Horizon Client Logs on Mobile Devices	37
View Agent Logs from Windows Machines	37
Linux Desktop Logs	38

7	Applying Security Patches	41
	Apply a Patch for View Agent	41
	Apply a Patch for Horizon Client	42
	Index	43

Horizon Client and View Agent Security

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

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

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

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Horizon 6, including Horizon Client and View Agent.

VMware Technical Publications Glossary

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

External Ports

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

This chapter includes the following topics:

- [“Understanding View Communications Protocols,”](#) on page 7
- [“Firewall Rules for View Agent,”](#) on page 8
- [“TCP and UDP Ports Used by Clients and View Agent,”](#) on page 8

Understanding View Communications Protocols

View components exchange messages by using several different protocols.

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

Table 1-1. Default Ports

Protocol	Port
JMS	TCP port 4001 TCP port 4002
HTTP	TCP port 80
HTTPS	TCP port 443
MMR/CDR	For multimedia redirection and client drive redirection, TCP port 9427
RDP	TCP port 3389
PCoIP	Any TCP port from Horizon Client to port 4172 of the remote desktop or application. PCoIP also uses UDP port 50002 from Horizon Client (or UDP port 55000 from the PCoIP Secure Gateway) to port 4172 of the remote desktop or application.
USB redirection	TCP port 32111. This port is also used for time zone synchronization.
HTML Access	For the HTML Access Gateway on connection servers and security servers, TCP Port 8443 For View Agent connections, TCP Port 22443

Firewall Rules for View Agent

The View Agent installation program opens certain TCP ports on the firewall. Ports are incoming unless otherwise noted.

Table 1-2. TCP Ports Opened During View Agent Installation

Protocol	Ports
RDP	3389
USB redirection	32111 (This port is also used for time zone synchronization.)
MMR (multimedia redirection) and CDR (client drive redirection)	9427
PCoIP	4172 (TCP and UDP)
HTML Access	22443

The View Agent installation program 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 change the RDP port number after installation, you must change the associated firewall rules.

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

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

TCP and UDP Ports Used by Clients and View Agent

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

During installation in Windows clients and remote desktops and RDS hosts, the installer can optionally configure Windows firewall rules to open the ports that are used by default. If you change a default port after installation, you must manually reconfigure Windows firewall rules to allow access on the updated port. See "Replacing Default Ports for View Services" in the *View Installation* document.

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

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	View Agent	3389	TCP	Microsoft RDP traffic to View desktops if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent	9427	TCP	Windows Media MMR redirection and client drive redirection, if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent	32111	TCP	USB redirection and time zone synchronization if direct connections are used instead of tunnel connections.
Horizon Client	*	View 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.
Browser	*	View Agent	22443	TCP	HTML Access if direct connections are used instead of tunnel connections.

Table 1-3. TCP and UDP Ports Used by View Agent (Continued)

Source	Port	Target	Port	Protocol	Description
Security server, View Connection Server, or Access Point appliance	*	View Agent	3389	TCP	Microsoft RDP traffic to View desktops when tunnel connections are used.
Security server, View Connection Server, or Access Point appliance	*	View Agent	9427	TCP	Windows Media MMR redirection and client drive redirection when tunnel connections are used.
Security server, View Connection Server, or Access Point appliance	*	View Agent	32111	TCP	USB redirection and time zone synchronization when tunnel connections are used.
Security server, View Connection Server, or Access Point appliance	55000	View Agent	4172	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.
Security server, View Connection Server, or Access Point appliance	*	View Agent	4172	TCP	PCoIP if PCoIP Secure Gateway is used.
Security server, View Connection Server, or Access Point appliance	*	View Agent	22443	TCP	HTML Access if Blast Secure Gateway is used.
View Agent	*	View Connection Server	4001, 4002	TCP	JMS SSL traffic.
View Agent	4172	Horizon Client	*	UDP	PCoIP, if PCoIP Secure Gateway is not used. NOTE Because the target port varies, see the note below this table.
View Agent	4172	View Connection Server, security server, or Access Point appliance	55000	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used.

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

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

Source	Port	Target	Port	Protocol	Description
Horizon Client	*	View Connection Server, security server, or Access Point appliance	443	TCP	HTTPS for logging in to View. (This port is also used for tunnelling when tunnel connections are used.)
Horizon Client	*	View Agent	3389	TCP	Microsoft RDP traffic to View desktops if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent	9427	TCP	Windows Media MMR redirection and client drive redirection, if direct connections are used instead of tunnel connections.
Horizon Client	*	View Agent	32111	TCP	USB redirection and time zone synchronization if direct connections are used instead of tunnel connections.
Horizon Client	*	View 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	*	View Connection Server, security server, or Access Point 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.
View Agent	4172	Horizon Client	*	UDP	PCoIP if PCoIP Secure Gateway is not used. NOTE Because the target port varies, see the note below this table.
Security server, View Connection Server, or Access Point appliance	4172	Horizon Client	*	UDP	PCoIP (not SALSA20) if PCoIP Secure Gateway is used. NOTE Because the target port varies, see the note below this table.

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.

Installed Services, Daemons, and Processes

2

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

This chapter includes the following topics:

- [“Services Installed by the View Agent Installer on Windows Machines,”](#) on page 11
- [“Services Installed on the Windows Client,”](#) on page 12
- [“Daemons Installed in Other Clients and the Linux Desktop,”](#) on page 12

Services Installed by the View Agent Installer on Windows Machines

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

Table 2-1. View Agent Services

Service Name	Startup Type	Description
VMware Blast	Automatic	Provides services for HTML Access.
VMware Horizon View Agent	Automatic	Provides services for View Agent.
VMware Horizon View Composer Guest Agent Server	Automatic	Provides services if this virtual machine is part of a View Composer linked-clone desktop pool.
VMware Horizon View Persona Management	Automatic if the feature is enabled; otherwise Disabled	Provides services for the VMware Persona Management feature.
VMware Horizon View Script Host	Disabled	Provides support for running start session scripts, if any, to configure desktop security policies before a desktop session begins. Policies are based on the client device and the user's location.
VMware Netlink Supervisor Service	Automatic	To support the scanner redirection feature and the serial port redirection feature, provides monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Client Service	Automatic	(View Agent 6.0.2 and later) Provides services for the scanner redirection feature.
VMware Serial Com Client Service	Automatic	(View Agent 6.1.1 and later) Provides services for the serial port redirection feature.
VMware Snapshot Provider	Manual	Provides services for virtual machine snapshots, which are used for cloning.

Table 2-1. View Agent Services (Continued)

Service Name	Startup Type	Description
VMware Tools	Automatic	Provides support for synchronizing objects between the host and guest operating systems, which enhances the performance of the virtual machines guest operating system and improves management of the virtual machine.
VMware USB Arbitration Service	Automatic	Enumerates the various USB devices connected to the client and determines which devices to connect to the client and which to connect to the remote desktop.
VMware View USB	Automatic	Provides services for the USB redirection feature.

Services Installed on the Windows Client

The operation of Horizon Client depends on several Windows services.

Table 2-2. Horizon Client Services

Service Name	Startup Type	Description
VMware Horizon Client	Automatic	Provides Horizon Client services.
VMware Netlink Supervisor Service	Automatic	To support the scanner redirection feature and the serial port redirection feature, provides monitoring services for transferring information between kernel and user space processes.
VMware Scanner Redirection Client Service	Automatic	(Horizon Client 3.2 and later) Provides services for the scanner redirection feature.
VMware Serial Com Client Service	Automatic	(Horizon Client 3.4 and later) Provides services for the serial port redirection feature.
VMware USB Arbitration Service	Automatic	Enumerates the various USB devices connected to the client and determines which devices to connect to the client and which to connect to the remote desktop.
VMware View USB	Automatic	Provides services for the USB redirection feature.

Daemons Installed in Other Clients and the Linux Desktop

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

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

Type	Service, Process, or Daemon
Linux client	<ul style="list-style-type: none"> ■ <code>vmware-usbarbitrator</code>, 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. ■ <code>vmware-view-used</code>, which provides services for the USB redirection feature. <p>NOTE These daemons start automatically if you click the Register and start the service(s) after installation check box during installation. These processes run as root.</p>
Mac client	Horizon Client does not create any daemons.
Chrome client	Horizon Client runs in one Android process. Horizon Client does not create any daemons.
iOS client	Horizon Client does not create any daemons.
Android client	Horizon Client runs in one Android process. Horizon Client does not create any daemons.

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

Type	Service, Process, or Daemon
Windows Store client	Horizon Client does not create or trigger any system services.
Linux desktop	<ul style="list-style-type: none"> <li data-bbox="453 327 1422 432">■ <code>StandaloneAgent</code>, which runs with root privileges and is started when the Linux system is up and running. <code>StandaloneAgent</code> communicate with View Connection Server to perform remote desktop session management (sets up tears down the session, updating the remote desktop status to the broker in View Connection Server). <li data-bbox="453 443 1422 573">■ <code>VMwareBlastServer</code>, which is started by <code>StandaloneAgent</code> when a <code>StartSession</code> request is received from View Connection Server. The <code>VMwareBlastServer</code> daemon runs with <code>vmwblast</code> (a system account created when Linux Agent is installed.) privilege. It communicates with <code>StandaloneAgent</code> through an internal <code>MKSControl</code> channel and communicates with Horizon Client by using the Blast protocol.

Resources to Secure

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

This chapter includes the following topics:

- [“Implementing Best Practices to Secure Client Systems,”](#) on page 15
- [“Configuration File Locations,”](#) on page 15
- [“Accounts,”](#) on page 16

Implementing Best Practices to Secure Client Systems

You should implement best practices to secure client systems.

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

Configuration File Locations

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

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

Type	Directory Path
Linux client	<p>When Horizon Client starts up, configuration settings are processed from various locations in the following order:</p> <ol style="list-style-type: none"> 1 /etc/vmware/view-default-config 2 ~/.vmware/view-preferences 3 /etc/vmware/view-mandatory-config <p>If a setting is defined in multiple locations, the value that is used is the value from the last file or command-line option read.</p>
Windows client	<p>The user settings that might include some private information are located in the following file:</p> <p>C:\Users\user-name\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt</p>

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

Type	Directory Path
Mac client	Some configuration files generated after Mac client startup. <ul style="list-style-type: none"> ■ \$HOME/Library/Preferences/com.vmware.horizon.plist ■ \$HOME/Library/Preferences/com.vmware.vmc.plist ■ \$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist ■ /Library/Preferences/com.vmware.horizon.plist
Chrome client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
iOS client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
Android client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
Windows Store client	Security-related settings appear in the user interface rather than in configuration files. No configuration files are visible to any users.
View Agent (remote desktop with Windows operating system)	Security-related settings appear in the Windows Registry only.
Linux desktop	You can use a text editor to open the following configuration file and specify SSL-related settings. /etc/vmware/viewagent-custom.conf

Accounts

Client users must have accounts in Active Directory.

Horizon Client User Accounts

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

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

System Accounts Created During Installation

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

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

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

Security Settings for the Client and Agent

4

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

For configuration settings related to log collection, see [Chapter 6, “Client and Agent Log File Locations,”](#) on page 33. For configuration settings related to security protocols and cipher suites, see [Chapter 5, “Configuring Security Protocols and Cipher Suites,”](#) on page 27.

This chapter includes the following topics:

- [“Configuring Certificate Checking,”](#) on page 17
- [“Security-Related Settings in the View Agent Configuration Template,”](#) on page 18
- [“Setting Options in Configuration Files on a Linux Desktop,”](#) on page 19
- [“HTML Access Group Policy Settings,”](#) on page 21
- [“Security Settings in the Horizon Client Configuration Templates,”](#) on page 21

Configuring Certificate Checking

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

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

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

Certificate verification includes the following checks:

- Has the certificate been revoked?
- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?

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

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

For information about how to configure certificate checking on a specific type of client, see the *Using VMware Horizon Client* document for the specific type of client. The documents are available from the Horizon Clients documentation page at

https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html. These documents also contain information about using self-signed certificates.

Security-Related Settings in the View Agent Configuration Template

Security-related settings are provided in the ADM template file for View Agent (`vdm_agent.adm`). Unless noted otherwise, the settings include only a Computer Configuration setting.

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

Table 4-1. Security-Related Settings in the View Agent Configuration Template

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

Table 4-1. Security-Related Settings in the View Agent Configuration Template (Continued)

Setting	Description
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 <code>CommandsToRunOnReconnect</code> .
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 <code>CommandsToRunOnDisconnect</code> .
ConnectionTicketTimeout	Specifies the amount of time in seconds that the View connection ticket is valid. Horizon Client devices use a connection ticket for verification and single sign-on when connecting to View Agent. For security reasons, a connection ticket is valid for a limited amount of time. When a user connects to a View 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 <code>VdmConnectionTicketTimeout</code> .
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 <code>CredentialFilterExceptions</code> .

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

Setting Options in Configuration Files on a Linux Desktop

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

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

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

Configuration Options in `/etc/vmware/config`

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

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

Option	Value	Default	Description
VVC.ScRedir.Enable	TRUE or FALSE	TRUE	Set this option to disable smart card redirection.
Clipboard.Direction	0, 1, 2, or 3	2	This option determines the clipboard redirectopn policy. <ul style="list-style-type: none"> ■ 0 - Disable clipboard redirection. ■ 1 - Enable clipboard redirection in both directions. ■ 2 - Enable clipboard redirection from client to remote desktop only. ■ 3 - Enable clipboard redirection from remote desktop to client only.

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

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

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

Option	Value	Default	Description
SSOEnable	TRUE or FALSE	TRUE	Set this option to disable single sign-on (SSO).
SSOUserFormat	A text string	[username]	Use this option to specify the format of the login name for single sign-on. The default is the user name only. Set this option if the domain name is also required. Typically the login name is the domain name plus a special character followed by the user name. If the special character is the backslash, you must escape it with another backslash. Examples of login name formats: <ul style="list-style-type: none"> ■ SSOUserFormat=[domain] \ [username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
StartBlastServerTimeout	An integer	20	This option determines the amount of time, in seconds, that the VMwareBlastServer process has for initialization. If the process is not ready within this timeout value, the user's login will fail.
SSLCiphers	A text string	!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH	Use this option to specify the list of ciphers. You must use the format that is defined in https://www.openssl.org/docs/manmaster/apps/ciphers.html .
SSLProtocols	A text string	TLSv1_1:TLSv1_2	Use this option to specify the security protocols. The supported protocols are TLSv1.0, TLSv1.1, and TLSv1.2.
SSLCipherServerPreference	TRUE or FALSE	TRUE	Use this option to enable or disable the option <code>SSL_OP_CIPHER_SERVER_PREFERENCE</code> . For more information, see https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html .

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

HTML Access Group Policy Settings

The HTML Access ADM Template file, `vdm-blast.adm`, contains group policy settings that you can apply to your remote desktops. After the template file is imported into Active Directory, the HTML Access group policy settings are contained in the VMware Blast folder in the Group Policy Editor.

Table 4-4. HTML Access Group Policy Settings

Setting	Description
Screen Blanking	<p>Controls whether the remote virtual machine can be seen from outside of View during an HTML Access session. For example, an administrator might use vSphere Web Client to open a console on the virtual machine while a user is connected to the desktop through HTML Access.</p> <p>When this setting is enabled or not configured, and someone attempts to access the remote virtual machine from outside of View while an HTML Access session is active, the remote virtual machine displays a blank screen.</p>
Session Garbage Collection	<p>Controls the garbage collection of abandoned remoting sessions. When this setting is enabled, you can configure the garbage collection interval and threshold.</p> <p>The interval controls how often the garbage collector runs. You set the interval in milliseconds.</p> <p>The threshold determines how much time must pass after a session is abandoned before it becomes a candidate for deletion. You set the threshold in seconds.</p>
Configure clipboard redirection	<p>Determines the direction in which clipboard redirection is allowed. Only text can be copied and pasted. You can select one of these values:</p> <ul style="list-style-type: none"> ■ Enabled client to server only (That is, allow copy and paste only from the client system to the remote desktop.) ■ Disabled in both directions ■ Enabled in both directions ■ Enabled server to client only (That is, allow copy and paste only from the remote desktop to the client system.) <p>This setting applies to View Agent only.</p> <p>When this setting is disabled or not configured, the default value is Enabled client to server only.</p>
HTTP Service	<p>Allows you to change the secured (HTTPS) TCP port for the Blast Agent service. The default port is 22443.</p> <p>Enable this setting to change the port number. If you change this setting, you must also update settings on the firewall of the affected remote desktops (where View Agent is installed).</p>

Security Settings in the Horizon Client Configuration Templates

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

Security Settings are stored in the registry on the host machine under one of the following paths:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- For 64-bit Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

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

Setting	Description
Allow command line credentials (Computer Configuration setting)	<p>Determines whether user credentials can be provided with Horizon Client command line options. If this setting is disabled, the <code>smartCardPIN</code> and <code>password</code> options are not available when users run Horizon Client from the command line.</p> <p>This setting is enabled by default.</p> <p>The equivalent Windows Registry value is <code>AllowCmdLineCredentials</code>.</p>
Servers Trusted For Delegation (Computer Configuration setting)	<p>Specifies the View Connection Server instances that accept the user identity and credential information that is passed when a user selects the Log in as current user check box. If you do not specify any View Connection Server instances, all View Connection Server instances accept this information.</p> <p>To add a View Connection Server instance, use one of the following formats:</p> <ul style="list-style-type: none"> ■ <code>domain\system\$</code> ■ <code>system\$@domain.com</code> ■ The Service Principal Name (SPN) of the View Connection Server service. <p>The equivalent Windows Registry value is <code>BrokersTrustedForDelegation</code>.</p>
Certificate verification mode (Computer Configuration setting)	<p>Configures the level of certificate checking that is performed by Horizon Client. You can select one of these modes:</p> <ul style="list-style-type: none"> ■ No Security. View does not perform certificate checking. ■ Warn But Allow. When the following server certificate issues occur, a warning is displayed, but the user can continue to connect to View Connection Server: <ul style="list-style-type: none"> ■ A self-signed certificate is provided by View. In this case, it is acceptable if the certificate name does not match the View Connection Server name provided by the user in Horizon Client. ■ A verifiable certificate that was configured in your deployment has expired or is not yet valid. <p>If any other certificate error condition occurs, View displays an error dialog and prevents the user from connecting to View Connection Server.</p> <p>Warn But Allow is the default value.</p> <ul style="list-style-type: none"> ■ Full Security. If any type of certificate error occurs, the user cannot connect to View Connection Server. View displays certificate errors to the user. <p>When this group policy setting is configured, users can view the selected certificate verification mode in Horizon Client but cannot configure the setting. The SSL configuration dialog box informs users that the administrator has locked the setting.</p> <p>When this setting is not configured or disabled, Horizon Client users can select a certificate verification mode.</p> <p>For Windows clients, if you do not want to configure this setting as a group policy, you can also enable certificate verification by adding the <code>CertCheckMode</code> value name to one of the following registry keys on the client computer:</p> <ul style="list-style-type: none"> ■ For 32-bit Windows: <code>HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security</code> ■ For 64-bit Windows: <code>HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security</code> <p>Use the following values in the registry key:</p> <ul style="list-style-type: none"> ■ 0 implements No Security. ■ 1 implements Warn But Allow. ■ 2 implements Full Security. <p>If you configure both the group policy setting and the <code>CertCheckMode</code> setting in the Windows Registry key, the group policy setting takes precedence over the registry key value.</p>

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

Setting	Description
Default value of the 'Log in as current user' checkbox (Computer and User Configuration setting)	<p>Specifies the default value of the Log in as current user check box on the Horizon Client connection dialog box.</p> <p>This setting overrides the default value specified during Horizon Client installation.</p> <p>If a user runs Horizon Client from the command line and specifies the <code>LogInAsCurrentUser</code> option, that value overrides this setting.</p> <p>When the Log in as current user check box is selected, the identity and credential information that the user provided when logging in to the client system is passed to the View Connection Server instance and ultimately to the remote desktop. When the check box is deselected, users must provide identity and credential information multiple times before they can access a remote desktop.</p> <p>This setting is disabled by default.</p> <p>The equivalent Windows Registry value is <code>LogInAsCurrentUser</code>.</p>
Display option to Log in as current user (Computer and User Configuration setting)	<p>Determines whether the Log in as current user check box is visible on the Horizon Client connection dialog box.</p> <p>When the check box is visible, users can select or deselect it and override its default value. When the check box is hidden, users cannot override its default value from the Horizon Client connection dialog box.</p> <p>You can specify the default value for the Log in as current user check box by using the policy setting <code>Default value of the 'Log in as current user' checkbox</code>.</p> <p>This setting is enabled by default.</p> <p>The equivalent Windows Registry value is <code>LogInAsCurrentUser_Display</code>.</p>
Enable jump list integration (Computer Configuration setting)	<p>Determines whether a jump list appears in the Horizon Client icon on the taskbar of Windows 7 and later systems. The jump list lets users connect to recent View Connection Server instances and remote desktops.</p> <p>If Horizon Client is shared, you might not want users to see the names of recent desktops. You can disable the jump list by disabling this setting.</p> <p>This setting is enabled by default.</p> <p>The equivalent Windows Registry value is <code>EnableJumpList</code>.</p>
Enable SSL encrypted framework channel (Computer and User Configuration setting)	<p>Determines whether SSL is enabled for View 5.0 and earlier desktops. Before View 5.0, the data sent over port TCP 32111 to the desktop was not encrypted.</p> <ul style="list-style-type: none"> ■ Enable: Enables SSL, but allows fallback to the previous unencrypted connection if the remote desktop does not have SSL support. For example, View 5.0 and earlier desktops do not have SSL support. Enable is the default setting. ■ Disable: Disables SSL. This setting is not recommended but might be useful for debugging or if the channel is not being tunneled and could potentially then be optimized by a WAN accelerator product. ■ Enforce: Enables SSL, and refuses to connect to desktops with no SSL support. <p>The equivalent Windows Registry value is <code>EnableTicketSSLAUTH</code>.</p>

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

Setting	Description
Configures SSL protocols and cryptographic algorithms (Computer and User Configuration setting)	Configures the cipher list to restrict the use of certain cryptographic algorithms and protocols before establishing an encrypted SSL connection. The cipher list consists of one or more cipher strings separated by colons. NOTE All cipher strings are case-sensitive. <ul style="list-style-type: none"> ■ If this feature is enabled, the default value for Horizon Client 3.5 is TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ The default value for Horizon Client 3.3 and 3.4 is TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. ■ The value for Horizon Client 3.2 and earlier is SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. That means that in Horizon Client 3.5, TLS v1.0, TLS v1.1, and TLS v1.2 are enabled. (SSL v2.0 and v3.0 are disabled.) In Horizon Client 3.3 and 3.4, TLS v1.0 and TLS v1.1 are enabled. (SSL v2.0 and v3.0, and TLS v1.2 are disabled.) In Horizon Client 3.2 and earlier, SSL v3.0 is also enabled. (SSL v2.0 and TLS v1.2 are disabled.) Cipher suites use 128- or 256-bit AES, remove anonymous DH algorithms, and then sort the current cipher list in order of encryption algorithm key length. Reference link for the configuration: http://www.openssl.org/docs/apps/ciphers.html The equivalent Windows Registry value is <code>SSLCipherList</code> .
Enable Single Sign-On for smart card authentication (Computer Configuration setting)	Determines whether single sign-on is enabled for smart card authentication. When single sign-on is enabled, Horizon Client stores the encrypted smart card PIN in temporary memory before submitting it to View Connection Server. When single sign-on is disabled, Horizon Client does not display a custom PIN dialog. The equivalent Windows Registry value is <code>EnableSmartCardSSO</code> .
Ignore bad SSL certificate date received from the server (Computer Configuration setting)	(View 4.6 and earlier releases only) Determines whether errors that are associated with invalid server certificate dates are ignored. These errors occur when a server sends a certificate with a date that has passed. The equivalent Windows Registry value is <code>IgnoreCertDateInvalid</code> .
Ignore certificate revocation problems (Computer Configuration setting)	(View 4.6 and earlier releases only) Determines whether errors that are associated with a revoked server certificate are ignored. These errors occur when the server sends a certificate that has been revoked and when the client cannot verify a certificate's revocation status. This setting is disabled by default. The equivalent Windows Registry value is <code>IgnoreRevocation</code> .
Ignore incorrect SSL certificate common name (host name field) (Computer Configuration setting)	(View 4.6 and earlier releases only) Determines whether errors that are associated with incorrect server certificate common names are ignored. These errors occur when the common name on the certificate does not match the hostname of the server that sends it. The equivalent Windows Registry value is <code>IgnoreCertCnInvalid</code> .
Ignore incorrect usage problems (Computer Configuration setting)	(View 4.6 and earlier releases only) Determines whether errors that are associated with incorrect usage of a server certificate are ignored. These errors occur when the server sends a certificate that is intended for a purpose other than verifying the identity of the sender and encrypting server communications. The equivalent Windows Registry value is <code>IgnoreWrongUsage</code> .
Ignore unknown certificate authority problems (Computer Configuration setting)	(View 4.6 and earlier releases only) Determines whether errors that are associated with an unknown Certificate Authority (CA) on the server certificate are ignored. These errors occur when the server sends a certificate that is signed by an untrusted third-party CA. The equivalent Windows Registry value is <code>IgnoreUnknownCa</code> .

Settings for Scripting Definitions for USB devices are stored in the registry on the host machine under one of the following paths:

- For 32-bit Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\USB
- For 64-bit Windows: HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\USB

Settings for Scripting Definitions for the password are stored in the registry on the host machine under HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\USB.

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

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

For more information about these settings and their security implications, see the *Using VMware Horizon Client for Windows* document.

Configuring Security Protocols and Cipher Suites

5

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

This chapter includes the following topics:

- [“Default Policies for Security Protocols and Cipher Suites,”](#) on page 27
- [“Configuring Security Protocols and Cipher Suites for Specific Client Types,”](#) on page 29
- [“Disable Weak Ciphers in SSL/TLS,”](#) on page 30
- [“Configure Security Protocols and Cipher Suites for HTML Access Agent,”](#) on page 30
- [“Configure Proposal Policies on View Desktops,”](#) on page 31

Default Policies for Security Protocols and Cipher Suites

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

The following tables list the protocols and cipher suites that are enabled by default for Horizon Client 3.x on Windows, Linux, Mac OS X, iOS, Android, and Chrome client systems. In Horizon Client 3.1 (and later) for Windows, Linux, and Mac OS X, these cipher suites and protocols are also used to encrypt the USB channel (communication between the USB service daemon and View Agent). The USB service daemon adds RC4 (:RC4-SHA: +RC4) to the end of the cipher control string when it connects to a remote desktop.

Horizon Client 3.5

Table 5-1. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 3.5

Default Security Protocols	Default Cipher Suites
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

IMPORTANT Although TLS 1.0 is enabled by default, VMware recommends disabling TLS 1.0 where possible. In future releases TLS 1.0 will be disabled by default.

Horizon Client 3.3 and 3.4

Table 5-2. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 3.3 and 3.4

Default Security Protocols	Default Cipher Suites
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

NOTE TLS 1.2 is also supported, though not enabled by default. To enable TLS 1.2, follow the instructions in [VMware KB 2121183](#), after which the cipher suites listed in [Table 5-1](#) are supported.

Horizon Client 3.0, 3.1, and 3.2

Table 5-3. Security Protocols and Cipher Suites Enabled by Default on Horizon Client 3.0, 3.1, and 3.2

Default Security Protocols	Default Cipher Suites
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 ■ SSL 3.0 (enabled on Windows clients only) 	<ul style="list-style-type: none"> ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022) ■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f) ■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

NOTE TLS 1.2 is also supported, though not enabled by default. To enable TLS 1.2, follow the instructions in [VMware KB 2121183](#), after which the cipher suites listed in [Table 5-1](#) are supported.

Configuring Security Protocols and Cipher Suites for Specific Client Types

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

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

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

- On Windows client systems, you can use either a group policy setting or a Windows Registry setting. For information, see *Using Horizon Client for Windows*.
- On Linux client systems, you can use either configuration file properties or command-line options. For information, see *Using Horizon Client for Linux*.
- On Mac OS X client systems, you can use a Preference setting in Horizon Client. For information, see *Using Horizon Client for Mac OS X*.
- On iOS, Android, and Chrome client systems, you can use an Advanced SSL Options setting in the Horizon Client settings. For information, see the applicable document: *Using Horizon Client for iOS*, *Using Horizon Client for Android*, or *Using Horizon Client for Chrome*.

The documents are available from the Horizon Clients documentation page at https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html.

Disable Weak Ciphers in SSL/TLS

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

Procedure

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

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

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

- 6 Exit the Group Policy Management Editor.
- 7 Restart the View Agent machines for the new group policy to take effect.

Configure Security Protocols and Cipher Suites for HTML Access Agent

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

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

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

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

Procedure

- 1 Start the Windows Registry Editor.
- 2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` registry key.
- 3 Add two new string (REG_SZ) values, `SslProtocolLow` and `SslProtocolHigh`, to specify the range of protocols.

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

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

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

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

- 5 Restart the Windows service VMware Blast.

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

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

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

Configure Proposal Policies on View Desktops

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

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

Procedure

- 1 Start the Windows Registry Editor on the View desktop.
- 2 Navigate to the `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration` registry key.
- 3 Add a new String (REG_SZ) value, `ClientSSLSecureProtocols`.

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

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

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

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

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

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

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

Client and Agent Log File Locations

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

This chapter includes the following topics:

- [“Horizon Client for Windows Logs,”](#) on page 33
- [“Horizon Client for Mac OS X Logs,”](#) on page 35
- [“Horizon Client for Linux Logs,”](#) on page 36
- [“Horizon Client Logs on Mobile Devices,”](#) on page 37
- [“View Agent Logs from Windows Machines,”](#) on page 37
- [“Linux Desktop Logs,”](#) on page 38

Horizon Client for Windows Logs

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

Log Location

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

Table 6-1. Horizon Client for Windows Log Files

Type of Logs	Directory Path	File Name
Installation	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
PCoIP client From the vmware-remotemks.exe process	C:\Users\%username%\AppData\Local\Temp	pcoip_client_YYYY_MM_DD_XXXXXX.txt NOTE You can use a GPO to configure the log level, from 0 to 3 (most verbose). Use the View PCoIP Client Session Variables ADM template file (pcoip.adm). The setting is called Configure PCoIP event log verbosity .
Horizon Client UI From the vmware-view.exe process	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt NOTE You can use a GPO to configure the log location. Use the View Common Configuration ADM template file (vdm_common.adm).

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

Type of Logs	Directory Path	File Name
Horizon Client logs From the vmware-view.exe process	C:\Users\%username%\AppData\Local\Temp\vmware-username-XXXXXX	vmware-crtbora-XXXXXX.log
Message framework	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	log-YYYY-MM-DD-XXXXXX.txt debug-YYYY-MM-DD-XXXXXX.txt
Remote MKS (mouse-keyboard-screen) logs From the vmware-remotemks.exe process	C:\Users\%username%\AppData\Local\Temp\vmware-username	ViewMP-Client-XXXXXX.log vmware-mks-XXXXXX.log vmware-rdeSvc-XXXXXX.log vmware-vvaClient-XXXXXX.log
Tsdr client From the vmware-remotemks.exe process	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsdr-Client-XXXXXX.log
Tsmmr client From the vmware-remotemks.exe process	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsmmr-Client-XXXXXX.log
VdpService client From the vmware-remotemks.exe process	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-vdpServiceClient-XXXXXX.log
WSNM service From the wsnm.exe process	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-XXXXXX.txt NOTE You can use a GPO to configure the log location. Use the View Common Configuration ADM template file (vdm_common.adm).
USB redirection From the vmware-view-usbd.exe process	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-XXXXXX.txt NOTE You can use a GPO to configure the log location. Use the View Common Configuration ADM template file (vdm_common.adm).
Serial port redirection From the vmwsprdpwks.exe process	C:\ProgramData\VMware\VDM\Logs	Serial*.txt Netlink*.txt
Scanner redirection From the ftscanmgr.exe process	C:\ProgramData\VMware\VDM\Logs	Scanner*.txt Netlink*.txt

Log Configuration

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

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

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

```
support.bat loglevels
```

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

Collecting a Log Bundle

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

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

Horizon Client for Mac OS X Logs

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

Log Location

Table 6-2. Horizon Client for Mac OS X Log Files

Type of Logs	Directory Path	File Name
Horizon Client UI	~/Library/Logs/VMware Horizon Client	
PCoIP client	~/Library/Logs/VMware Horizon Client	
Real-Time Audio-Video	~/Library/Logs/VMware	vmware-RTAV-pid.log
USB redirection	~/Library/Logs/VMware	
VChan	~/Library/Logs/VMware Horizon Client	
Remote MKS (mouse-keyboard-screen) logs	~/Library/Logs/VMware	
Crtbora	~/Library/Logs/VMware	

Log Configuration

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

Table 6-3. plist Keys for Log File Collection

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

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

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

Horizon Client for Linux Logs

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

Log Location

Table 6-4. Horizon Client for Linux Log Files

Type of Logs	Directory Path	File Name
Installation	/tmp/vmware-root/	.vmware-installer-pid.log vmware-vmis-pid.log
Horizon Client UI	/tmp/vmware-username/	vmware-horizon-client-pid.log
PCoIP client	/tmp/teradici-username/	pcoip_client_YYYY_MM_DD_XXXXXX.log
Real-Time Audio-Video	/tmp/vmware-username/	vmware-RTAV-pid.log
USB redirection	/tmp/vmware-root/	vmware-usbarb-pid.log vmware-view-usbd-pid.log
VChan	/tmp/vmware-username/	VChan-Client.log NOTE This log is created when you enable RDPVCBridge logs by setting "export VMW_RDPVC_BRIDGE_LOG_ENABLED=1".
Remote MKS (mouse-keyboard-screen) logs	/tmp/vmware-username/	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
VdpService client	/tmp/vmware-username/	vmware-vdpServiceClient-pid.log
Tsdr client	/tmp/vmware-username/	vmware-ViewTsdr-Client-pid.log

Log Configuration

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

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

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

Collecting a Log Bundle

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

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

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

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

Horizon Client Logs on Mobile Devices

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

iOS Client Logs

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

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

Android Client Logs

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

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

Chrome Client Logs

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

Windows Store Client Logs

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

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

View Agent Logs from Windows Machines

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

Log Location

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

Table 6-5. Horizon Client for Windows Log Files

Type of Logs	Directory Path	File Name
Installation	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
View Agent	<Drive Letter>:\ProgramData\VMware\VDM\logs	pcoip_agent_YYYY_MM_DD_XXXXXX.txt pcoip_agent_YYYY_MM_DD_XXXXXX.txt vmware-vdpServiceServer-XXXXXX.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-XXXXXX.txt NOTE You can use a GPO to configure the log location. Use the View Common Configuration ADM template file (vdm_common.adm).

Log Configuration

There are several methods for configuring logging options.

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

Collecting a Log Bundle

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

Linux Desktop Logs

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

Log Location

Table 6-6. Linux Desktop Log Files

Type of Logs	Directory Path
Installation	/tmp/vmware-root
View Agent	/var/log/vmware
View Agent	/usr/lib/vmware/viewagent/viewagent-debug.log

Log Configuration

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

Collecting a Log Bundle

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

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

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

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

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

Applying Security Patches

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

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

- 1 View Composer
- 2 View Connection Server
- 3 View Agent
- 4 Horizon Client

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

This chapter includes the following topics:

- [“Apply a Patch for View Agent,”](#) on page 41
- [“Apply a Patch for Horizon Client,”](#) on page 42

Apply a Patch for View Agent

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

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

Prerequisites

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

Procedure

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

Your contact at VMware will provide instructions for this download.

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

Step-by-step instructions for running the View Agent installer appear in *Setting Up Desktop and Application Pools in View*.

NOTE With Horizon 6 version 6.2 and later releases, you are no longer required to uninstall the previous version before installing the patch.

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

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

Apply a Patch for Horizon Client

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

Procedure

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

Your contact at VMware will provide instructions for this download. Or you can go to the client download page at <http://www.vmware.com/go/viewclients>. As mentioned previously, for some clients, you might get the patch release from an app store.
- 2 If the client device is a Mac or Linux desktop or laptop, remove the current version of the client software from your device.

Use the customary device-specific method for removing applications.

NOTE With Horizon Client for Windows 3.5 and later releases, you are no longer required to uninstall the previous version before installing the patch on Windows clients.

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

If you got the patch from the Apple App Store or Google Play, the app is usually installed when you download it, and you do not need to run an installer.
- 4 Verify that you can log in to the patched desktop pools with the newly patched Horizon Client.

Index

A

- accounts **16**
- ADM template files, HTML Access **21**
- Android client logs **37**

C

- certificates, ignoring problems **17**
- cipher suites, configuring for HTML Access Agents **30**
- client systems, best practices for securing **15**
- communication protocols, understanding **7**
- configuration files **15**
- configuration options
 - audio out **19**
 - clipboard redirection **19**
 - left-handed mouse **19**
 - lossless PNG mode **19**
 - single sign-on (SSO) **19**
- configuration file locations **15**

D

- daemons installed **11**
- daemons installed by the client installer **12**
- desktops, configuring proposal policies **31**

F

- firewall settings **8**
- firewall rules, View Agent **7, 8**

G

- glossary **5**
- GPOs related to security **17**

H

- Horizon Client, applying patches for **42**
- Horizon Client configuration template security settings **21**
- HTML Access Agent, configuring cipher suites **30**

I

- installed components **11**
- intended audience **5**
- iOS client logs **37**

J

- JMS protocol **7**

L

- Linux client logs **36**
- Linux desktop logs **38**
- log files **33**
- logs
 - Linux client **36**
 - Linux desktop **38**
 - Mac OS X client **35**
 - mobile clients **37**
 - View Agent **37**
 - Windows client **33**

M

- Mac OS X client logs **35**

P

- patch releases **41**

S

- security protocols **27, 29**
- security settings **17**
- server certificate verification **17**
- services installed **11**
- SSL certificates, verifying **17**

T

- TCP ports, View Agent **7, 8**

U

- UDP ports **8**

V

- verification modes for certificate checking **17**
- View Agent logs **37**
- View Agent, applying patches for **41**
- View Agent configuration template security settings **18**

W

- weak ciphers in SSL/TLS, disabling **30**
- Windows client logs **33**

Windows services
 associated with Horizon Client **12**
 associated with View Agent **11**
Windows Store client logs **37**