# View Security

VMware Horizon 6
Version 6.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001726-00

vmware®

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

http://www.vmware.com/support/

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 © 2015 VMware, Inc. All rights reserved. Copyright and trademark information.

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

# Contents

# View Security

*View Security* provides a concise reference to the security features of VMware Horizon 6™.

- 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 View.

## Intended Audience

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

# 1 View Security Reference

When you are configuring a secure View environment, you can change settings and make adjustments in several areas to protect your systems.

This chapter includes the following topics:



## View Accounts

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

**Table 1-1.** View System Accounts

| View 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 View 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 View.<br>For information about the required privileges, see the *View Installation* document. |

**Table 1-1.** View System Accounts (Continued)

| View Component | Required Accounts |
|---|---|
| View Composer | Create a user account in Active Directory to use with View Composer. View Composer requires this account to join linked-clone desktops to your Active Directory domain.<br>The user account should not be a View administrative account. Give the account the minimum privileges that it requires to create and remove computer objects in a specified Active Directory container. For example, the account does not require domain administrator privileges.<br>For information about the required privileges, see the *View Installation* document. |
| View Connection Server, or Security Server | When you install View, you can choose which members of the local Administrators group (`BUILTIN\Administrators`) are allowed to log in to View Administrator.<br>In View Administrator, you can use **View Configuration > Administrators** to change the list of View administrators.<br>See the *View Administration* document for information about the privileges that are required. |

**Table 1-2.** View Database Accounts

| View Component | Required Accounts |
|---|---|
| View Composer database | An SQL Server or Oracle database stores View Composer data. You create an administrative account for the database that you can associate with the View Composer user account.<br>For information about setting up a View Composer database, see the *View Installation* document. |
| Event database used by View Connection Server | An SQL Server or Oracle database stores View event data. You create an administrative account for the database that View Administrator can use to access the event data.<br>For information about setting up a View Composer database, see the *View Installation* document. |

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

- Configure View 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 separate accounts for access to the View Composer and event databases.

# View Security Settings

View includes several settings that you can use to adjust the security of the configuration. You can access the settings by using View Administrator, by editing group profiles, or by using the ADSI Edit utility, as appropriate.

## Security-Related Global Settings in View Administrator

Security-related global settings for client sessions and connections are accessible under **View Configuration > Global Settings** in View Administrator.

**Table 1-3.** Security-Related Global Settings

| Setting | Description |
|---|---|
| **Change data recovery password** | The password is required when you restore the View LDAP configuration from an encrypted backup.<br>When you install View Connection Server version 5.1 or later, you provide a data recovery password. After installation, you can change this password in View Administrator.<br>When you back up View Connection Server, the View 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 View components.<br>■ If set to **Disabled**, message security mode is disabled.<br>■ If set to **Enabled**, legacy message signing and verification of JMS messages takes place. View components reject unsigned messages. This mode supports a mix of SSL and plain JMS connections.<br>■ If set to **Enhanced**, SSL is used for all JMS connections, to encrypt all messages. Access control is also enabled to restrict the JMS topics that View components can send messages to and receive messages from.<br>■ If set to **Mixed**, message security mode is enabled, but not enforced for View components that predate View Manager 3.0.<br>The default setting is **Enhanced** for new installations. If you upgrade from a previous version, the setting used in the previous version is retained.<br>IMPORTANT VMware strongly recommends setting the message security mode to **Enhanced** after you upgrade all View Connection Server instances, security servers, and View 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:<br>■ **Waiting for Message Bus restart** is the first phase. This state is displayed until you manually restart either all View Connection Server instances in the pod or the VMware Horizon View Message Bus Component service on all View Connection Server hosts in the pod.<br>■ **Pending Enhanced** is the next state. After all View Message Bus Component services have been restarted, the system begins changing the message security mode to **Enhanced** for all desktops and security servers.<br>■ **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 View desktops and applications.<br>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 View desktops and applications because the network connection was temporarily interrupted.<br>This setting is enabled by default. |
| **Forcibly disconnect users** | Disconnects all desktops and applications after the specified number of minutes has passed since the user logged in to View. All desktops and applications will be disconnected at the same time regardless of when the user opened them.<br>The default is 600 minutes. |
| **For clients that support applications.**<br>**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**, View 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.<br>If set to **Never**, View never disconnects applications or discards SSO credentials due to user inactivity.<br>The default is **Never**. |

**Table 1-3.** Security-Related Global Settings (Continued)

| Setting | Description |
|---|---|
| **Other clients.**<br>**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 View, regardless of any user activity on the client device.<br>The default is **After 15 minutes**. |
| **Enable IPSec for Security Server pairing** | Determines whether to use Internet Protocol Security (IPSec) for connections between security servers and View Connection Server instances.<br>By default, IPSec for security server connections is enabled. |
| **View Administrator session timeout** | Determines how long an idle View Administrator session continues before the session times out.<br>IMPORTANT Setting the View Administrator session timeout to a high number of minutes increases the risk of unauthorized use of View Administrator. Use caution when you allow an idle session to persist a long time.<br>By default, the View Administrator session timeout is 30 minutes. You can set a session timeout from 1 to 4320 minutes. |

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

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

## Security-Related Server Settings in View Administrator

Security-related server settings are accessible under **View Configuration > Servers** in View Administrator.

**Table 1-4.** 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 View Connection Server or security server host when users connect to View desktops and applications with the PCoIP display protocol.<br>If this setting is disabled, the desktop or application session is established directly between the client and the View desktop or the Remote Desktop Services (RDS) host, bypassing the View Connection Server or security server host.<br>This setting is disabled by default. |
| **Use Secure Tunnel connection to machine** | Determines whether Horizon Client makes a further HTTPS connection to the View Connection Server or security server host when users connect to a View desktop or an application.<br>If this setting is disabled, the desktop or application session is established directly between the client and the View desktop or the Remote Desktop Services (RDS) host, bypassing the View Connection Server or security server host.<br>This setting is enabled by default. |
| **Use Blast Secure Gateway for HTML Access to machine** | Determines whether clients that use a Web browser to access desktops use Blast Secure Gateway to establish a secure tunnel to View Connection Server.<br>If not enabled, Web browsers make direct connections to View desktops, bypassing View Connection Server.<br>This setting is disabled by default. |

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

## 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 1-5.** Security-Related Settings in the View Agent Configuration Template

| Setting | Description |
|---|---|
| `AllowDirectRDP` | Determines whether non-Horizon Clients can connect directly to View desktops with RDP. When this setting is disabled, View Agent permits only View-managed connections through Horizon Client.<br>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 `AllowDirectRDP` setting.<br>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.<br>This setting is enabled by default.<br>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 only their credentials when connecting with Horizon Client. When it is disabled, users must reauthenticate when the remote connection is made.<br>This setting is enabled by default.<br>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.<br>No list is specified by default.<br>The equivalent Windows Registry value is `CommandsToRunOnConnect`. |
| `CommandsToRunOnReconnect` | Specifies a list of commands or command scripts to be run when a session is reconnected after a disconnect.<br>No list is specified by default.<br>The equivalent Windows Registry value is `CommandsToRunOnReconnect`. |
| `CommandsToRunOnDisconnect` | Specifies a list of commands or command scripts to be run when a session is disconnected.<br>No list is specified by default.<br>The equivalent Windows Registry value is `CommandsToRunOnDisconnect`. |
| `ConnectionTicketTimeout` | Specifies the amount of time in seconds that the View connection ticket is valid.<br>If this setting is not configured, the default timeout period is 120 seconds.<br>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.<br>No list is specified by default.<br>The equivalent Windows Registry value is `CredentialFilterExceptions`. |

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

## Security Settings in the Horizon Client Configuration Template

Security-related settings are provided in 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 1-6.** Horizon Client Configuration Template: Security Settings

| Setting | Description |
|---|---|
| `Allow command line credentials` (Computer Configuration setting) | Determines whether user credentials can be provided with Horizon Client command line options. If this setting is disabled, the `smartCardPIN` and `password` options are not available when users run Horizon Client from the command line.<br>This setting is enabled by default.<br>The equivalent Windows Registry value is `AllowCmdLineCredentials`. |
| `Servers Trusted For Delegation` (Computer Configuration setting) | 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.<br>To add a View Connection Server instance, use one of the following formats:<br>■ **`domain\system$`**<br>■ **`system$@domain.com`**<br>■ The Service Principal Name (SPN) of the View Connection Server service.<br>The equivalent Windows Registry value is `BrokersTrustedForDelegation`. |

**Table 1-6.** Horizon Client Configuration Template: Security Settings (Continued)

| Setting | Description |
|---|---|
| `Certificate verification mode` (Computer Configuration setting) | Configures the level of certificate checking that is performed by Horizon Client. You can select one of these modes:<br>■ `No Security`. View does not perform certificate checking.<br>■ `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:<br>  ■ 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.<br>  ■ A verifiable certificate that was configured in your deployment has expired or is not yet valid.<br>  If any other certificate error condition occurs, View displays an error dialog and prevents the user from connecting to View Connection Server.<br>  `Warn But Allow` is the default value.<br>■ `Full Security`. If any type of certificate error occurs, the user cannot connect to View Connection Server. View displays certificate errors to the user.<br>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.<br>When this setting is not configured or disabled, Horizon Client users can select a certificate verification mode.<br>To allow a View server to perform checking of certificates provided by Horizon Client, the client must make HTTPS connections to the View Connection Server or security server host. Certificate checking is not supported if you off-load SSL to an intermediate device that makes HTTP connections to the View Connection Server or security server host.<br>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 `CertCheckMode` value name to one of the following registry keys on the client computer:<br>■ For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`<br>■ For 64-bit Windows: `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`<br>Use the following values in the registry key:<br>■ **`0`** implements `No Security`.<br>■ **`1`** implements `Warn But Allow`.<br>■ **`2`** implements `Full Security`.<br>If you configure both the group policy setting and the `CertCheckMode` setting in the Windows Registry key, the group policy setting takes precedence over the registry key value. |
| `Default value of the 'Log in as current user' checkbox` (Computer and User Configuration setting) | Specifies the default value of the **Log in as current user** check box on theHorizon Client connection dialog box.<br>This setting overrides the default value specified during Horizon Client installation.<br>If a user runs Horizon Client from the command line and specifies the `logInAsCurrentUser` option, that value overrides this setting.<br>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.<br>This setting is disabled by default.<br>The equivalent Windows Registry value is `LogInAsCurrentUser`. |

**Table 1-6.** Horizon Client Configuration Template: Security Settings (Continued)

| Setting | Description |
|---|---|
| `Display option to Log in as current user` (Computer and User Configuration setting) | Determines whether the **Log in as current user** check box is visible on the Horizon Client connection dialog box.<br>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.<br>You can specify the default value for the **Log in as current user** check box by using the policy setting `Default value of the 'Log in as current user' checkbox`.<br>This setting is enabled by default.<br>The equivalent Windows Registry value is `LogInAsCurrentUser_Display`. |
| `Enable jump list integration` (Computer Configuration setting) | Determines whether a jump list appears in the Horizon Client icon on the taskbar of Windows 7 and later systems. The jump list lets users connect to recent View Connection Server instances and remote desktops.<br>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.<br>This setting is enabled by default.<br>The equivalent Windows Registry value is `EnableJumplist`. |
| `Enable SSL encrypted framework channel` (Computer and User Configuration setting) | 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.<br>■ **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.<br>■ **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.<br>■ **Enforce**: Enables SSL, and refuses to connect to desktops with no SSL support .<br>The equivalent Windows Registry value is `EnableTicketSSLAuth`. |
| `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.<br>**NOTE** All cipher strings are case-sensitive.<br>If this feature is enabled, the default value for Horizon Client 3.3 and later is **TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**. The value for Horizon Client 3.2 and earlier is **SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH**.<br>That means that In Horizon Client 3.3 and later, 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.)<br>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.<br>Reference link for the configuration:<br>http://www.openssl.org/docs/apps/ciphers.html<br>The equivalent Windows Registry value is `SSLCipherList`. |
| `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.<br>The equivalent Windows Registry value is `EnableSmartCardSSO`. |
| `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.<br>The equivalent Windows Registry value is `IgnoreCertDateInvalid`. |

**Table 1-6.** Horizon Client Configuration Template: Security Settings (Continued)

| Setting | Description |
|---|---|
| `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.<br>This setting is disabled by default.<br>The equivalent Windows Registry value is `IgnoreRevocation`. |
| `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.<br>The equivalent Windows Registry value is `IgnoreCertCnInvalid`. |
| `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.<br>The equivalent Windows Registry value is `IgnoreWrongUsage`. |
| `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.<br>The equivalent Windows Registry value is `IgnoreUnknownCa`. |

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

## Security-Related Settings in the Scripting Definitions Section of the Horizon Client Configuration Template

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

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 1-7.** 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.<br>This setting is disabled by default.<br>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.<br>This setting is disabled by default.<br>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.<br>This setting is undefined by default.<br>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.

## Security-Related Settings in View LDAP

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

**Table 1-8.** Security-Related Settings in View LDAP

| Name-value pair | Description |
|---|---|
| **cs-allowunencryptedstartsession** | The attribute is `pae-NameValuePair`.<br>This attribute controls whether a secure channel is required between a View Connection Server instance and a desktop when a remote user session is being started.<br>When View Agent 5.1 or later is installed on a desktop computer, this attribute has no effect and a secure channel is always required. When a View Agent older than View 5.1 is installed, a secure channel cannot be established if the desktop computer is not a member of a domain with a two-way trust to the domain of the View Connection Server instance. In this case, the attribute is important to determine whether a remote user session can be started without a secure channel.<br>In all cases, user credentials and authorization tickets are protected by a static key. A secure channel provides further assurance of confidentiality by using dynamic keys.<br>If set to **0**, a remote user session will not start if a secure channel cannot be established. This setting is suitable if all the desktops are in trusted domains or all desktops have View Agent 5.1 or later installed.<br>If set to **1**, a remote user session can be started even if a secure channel cannot be established. This setting is suitable if some desktops have older View Agents installed and are not in trusted domains.<br>The default setting is **1**. |

# View Resources

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

**Table 1-9.** View Connection Server and Security Server Resources

| Resource | Location | Protection |
|---|---|---|
| LDAP settings | Not applicable. | LDAP data is protected automatically as part of role-based access control. |
| LDAP backup files | *<Drive Letter>*:\Programdata\VMWare\VDM\backups (Windows Server 2008) | Protected by access control. |
| locked.properties (Certificate properties file) | *install_directory*\VMware\VMware View\Server\sslgateway\conf | Can be protected by access control. Ensure that this file is secured against access by any user other than View administrators. |
| Log files | See "View Log Files," on page 17 | Protected by access control. |
| web.xml (Tomcat configuration file) | *install_directory*\VMware View\Server\broker\web apps\ROOT\Web INF | Protected by access control. |

# View Log Files

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

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

**Table 1-10.** View Log Files

| View Component | File Path and Other Information |
|---|---|
| All components (installation logs) | *%TEMP%*\vminst.log_*date_timestamp*<br>*%TEMP%*\vmmsi.log_*date_timestamp* |
| View Agent | *<Drive Letter>*:\ProgramData\VMware\VDM\logs<br>To access View log files that are stored in *<Drive Letter>*:\ProgramData\VMware\VDM\logs, you must open the logs from a program with elevated administrator privileges. Right-click the program file and select **Run as administrator**.<br>If a User Data Disk (UDD) is configured, *<Drive Letter>* might correspond to the UDD.<br>The logs for PCoIP are named pcoip_agent*.log and pcoip_server*.log. |
| View Applications | View Event Database configured on an SQL Server or Oracle database server.<br>Windows Application Event logs. Disabled by default. |
| View Composer | *%system_drive%*\Windows\Temp\vmware-viewcomposer-ga-new.log on the linked-clone desktop.<br>The View Composer log contains information about the execution of QuickPrep and Sysprep scripts. The log records the start time and end time of script execution, and any output or error messages. |

**Table 1-10.** View Log Files (Continued)

| View Component | File Path and Other Information |
|---|---|
| View Connection Server or Security Server | *<Drive Letter>*:\ProgramData\VMware\VDM\logs.<br>The log directory is configurable in the log configuration settings of the View Common Configuration ADM template file (vdm_common.adm).<br>PCoIP Secure Gateway logs are written to files named SecurityGateway_*.log in the PCoIP Secure Gateway subdirectory of the log directory on a security server. |
| View Services | View Event Database configured on an SQL Server or Oracle database server.<br>Windows System Event logs. |

# View TCP and UDP Ports

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

During installation, View 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 View Services" in the *View Installation* document.

**Table 1-11.** TCP and UDP Ports Used by View

| Source | Port | Target | Port | Protocol | Description |
|---|---|---|---|---|---|
| Security server | 55000 | View Agent | 4172 | UDP | PCoIP (not SALSA20) if PCoIP Secure Gateway is used. |
| Security server | 4172 | Horizon Client | 50001 | UDP | PCoIP (not SALSA20) if PCoIP Secure Gateway is used. |
| Security server | 500 | View Connection Server | 500 | UDP | IPsec negotiation traffic. |
| Security server | * | View Connection Server | 4001 | TCP | JMS traffic. |
| Security server | * | View Connection Server | 4002 | TCP | JMS SSL traffic. |
| Security server | * | View Connection Server | 8009 | TCP | AJP13-forwarded Web traffic, if not using IPsec. |
| Security server | * | View Connection Server | * | ESP | AJP13-forwarded Web traffic, when using IPsec without NAT. |
| Security server | 4500 | View Connection Server | 4500 | UDP | AJP13-forwarded Web traffic, when using IPsec through a NAT device. |
| Security server | * | View desktop | 3389 | TCP | Microsoft RDP traffic to View desktops. |
| Security server | * | View desktop | 9427 | TCP | Wyse MMR redirection. |
| Security server | * | View desktop | 32111 | TCP | USB redirection. |
| Security server | * | View desktop | 4172 | TCP | PCoIP (HTTPS) if PCoIP Secure Gateway is used. |
| Security server | * | View desktop | 22443 | TCP | HTML Access. |
| View Agent | 4172 | Horizon Client | 50001 | UDP | PCoIP, if PCoIP Secure Gateway is not used. |
| View Agent | 4172 | View Connection Server or security server | 55000 | UDP | PCoIP (not SALSA20) if PCoIP Secure Gateway is used. |
| Horizon Client | * | View Connection Server or security server | 80 | TCP | SSL (HTTPS access) is enabled by default for client connections, but port 80 (HTTP access) can be used in certain cases. See "Notes and Caveats for TCP and UDP Ports Used by View," on page 20. |

**Table 1-11.** TCP and UDP Ports Used by View (Continued)

| Source | Port | Target | Port | Protocol | Description |
|---|---|---|---|---|---|
| Horizon Client | * | View security server | 443 | TCP | HTTPS access. Port 443 is enabled by default for client connections. Port 443 can be changed.<br>Connection attempts over HTTP to port 80 are redirected to port 443 by default, but port 80 can service client connections if SSL is off-loaded to an intermediate device. You can reconfigure the redirection rule if the HTTPS port was changed. See "Notes and Caveats for TCP and UDP Ports Used by View," on page 20. |
| Horizon Client | * | View Connection Server | 443 | TCP | HTTPS access. Port 443 is enabled by default for client connections. Port 443 can be changed.<br>Client connection attempts to port 80 are redirected to port 443 by default, but port 80 can service client connections if SSL is off-loaded to an intermediate device. Connection attempts to port 80 to reach View Administrator are not redirected. You must connect over HTTPS to reach View Administrator.<br>You can prevent HTTP redirection and force clients to use HTTPS. See "Notes and Caveats for TCP and UDP Ports Used by View," on page 20. |
| Horizon Client | * | View Connection Server or security server | 4172 | TCP | PCoIP (HTTPS) if PCoIP Secure Gateway is used. |
| Horizon Client | * | View desktop | 3389 | TCP | Microsoft RDP traffic to View desktops if direct connections are used instead of tunnel connections. |
| Horizon Client | * | View desktop | 9427 | TCP | Wyse MMR redirection if direct connections are used instead of tunnel connections. |
| Horizon Client | * | View desktop | 32111 | TCP | USB redirection if direct connections are used instead of tunnel connections. |
| Horizon Client | * | View Agent | 4172 | TCP | PCoIP (HTTPS) if PCoIP Secure Gateway is not used. |
| Horizon Client | 50001 | View Agent | 4172 | UDP | PCoIP, if PCoIP Secure Gateway is not used. |
| Horizon Client | 50001 | View Connection Server or security server | 4172 | UDP | PCoIP (not SALSA20) if PCoIP Secure Gateway is used. |
| Web Browser | * | Security server | 8443 | TCP | HTML Access. |
| View Connection Server | * | View Connection Server | 48080 | TCP | For internal communication between View Connection Server components. |
| View Connection Server | * | vCenter Server or View Composer | 80 | TCP | SOAP messages if SSL is disabled for access to vCenter Servers or View Composer. |
| View Connection Server | * | vCenter Server or View Composer | 443 | TCP | SOAP messages if SSL is enabled for access to vCenter Servers or View Composer. |
| View Connection Server | 55000 | View Agent | 4172 | UDP | PCoIP (not SALSA20) if PCoIP Secure Gateway via the View Connection Server is used. |
| View Connection Server | 4172 | Horizon Client | 50001 | UDP | PCoIP (not SALSA20) if PCoIP Secure Gateway via the View Connection Server is used. |
| View Connection Server | * | View Connection Server | 4100 | TCP | JMS inter-router traffic. |
| View Connection Server | * | View Connection Server | 4101 | TCP | JMS SSL inter-router traffic. |

**Table 1-11.** TCP and UDP Ports Used by View (Continued)

| Source | Port | Target | Port | Protocol | Description |
|---|---|---|---|---|---|
| View Connection Server | * | View desktop | 3389 | TCP | Microsoft RDP traffic to View desktops if tunnel connections via the View Connection Server are used. |
| View Connection Server | * | View desktop | 4172 | TCP | PCoIP (HTTPS) if PCoIP Secure Gateway via the View Connection Server is used. |
| View Connection Server | * | View desktop | 9427 | TCP | Wyse MMR redirection if tunnel connections via the View Connection Server are used. |
| View Connection Server | * | View desktop | 32111 | TCP | USB redirection if tunnel connections via the View Connection Server are used. |
| View Connection Server | * | View Connection Server | 8472 | TCP | For interpod communication in Cloud Pod Architecture. |
| View Connection Server | * | View Connection Server | 22389 | TCP | For global LDAP replication in Cloud Pod Architecture. |
| View Connection Server | * | View Connection Server | 22636 | TCP | For secure global LDAP replication in Cloud Pod Architecture. |
| View desktop | * | View Connection Server instances | 4001 | TCP | JMS traffic. |
| View desktop | * | View Connection Server instances | 4002 | TCP | JMS SSL traffic. |
| View Composer service | * | ESXi host | 902 | TCP | Used when View Composer customizes linked-clone disks, including View Composer internal disks and, if they are specified, persistent disks and system disposable disks. |

## Notes and Caveats for TCP and UDP Ports Used by View

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

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

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

**NOTE** The UDP port number that clients use for PCoIP may change. If port 50001 is in use, the client will pick 50002. If port 50002 is in use, the client will pick port 50003, and so on. You must configure firewall with ANY where 50001 is listed in the table.

# Services on a View Connection Server Host

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

**Table 1-12.** View Connection Server Host Services

| Service Name | Startup Type | Description |
|---|---|---|
| VMware Horizon View Blast Secure Gateway | Automatic | Provides secure HTML Access services. This service must be running if clients connect to View Connection Server through the HTML Access Secure Gateway. |
| VMware Horizon View 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 View Script Host service. |
| VMware Horizon View Framework Component | Manual | Provides event logging, security, and COM+ framework services. This service must always be running. |
| VMware Horizon View Message Bus Component | Manual | Provides messaging services between the View components. This service must always be running. |
| VMware Horizon View PCoIP Secure Gateway | Manual | Provides PCoIP Secure Gateway services. This service must be running if clients connect to View Connection Server through the PCoIP Secure Gateway. |
| VMware Horizon View 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 View Security Gateway Component | Manual | Provides common gateway services. This service must always be running. |
| VMware Horizon View Web Component | Manual | Provides web services. This service must always be running. |
| VMwareVDMDS | Automatic | Provides LDAP directory services. This service must always be running. During upgrades of View, this service ensures that existing data is migrated correctly. |

# Services on a Security Server

The operation of View depends on several services that run on a security server.

**Table 1-13.** Security Server Services

| Service Name | Startup Type | Description |
|---|---|---|
| VMware Horizon View Blast Secure Gateway | Automatic | Provides secure HTML Access services. This service must be running if clients connect to this security server through the HTML Access Secure Gateway. |
| VMware Horizon View Security Server | Automatic | Provides security server services. This service must always be running. If you start or stop this service, it also starts or stops the Framework and Security Gateway services. |
| VMware Horizon View Framework Component | Manual | Provides event logging, security, and COM+ framework services. This service must always be running. |

**Table 1-13.** Security Server Services (Continued)

| Service Name | Startup Type | Description |
|---|---|---|
| VMware Horizon View PCoIP Secure Gateway | Manual | Provides PCoIP Secure Gateway services. This service must be running if clients connect to this security server through the PCoIP Secure Gateway. |
| VMware Horizon View Security Gateway Component | Manual | Provides common gateway services. This service must always be running. |

# Configuring Security Protocols and Cipher Suites on a View Connection Server Instance or on a Security Server

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

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

The default policies and the procedures for configuring policies were changed in View 5.2. For information about earlier View releases, see VMware Knowledge Base article 1021466 at http://kb.vmware.com/kb/1021466.

## Default Global Policies for Security Protocols and Cipher Suites

Certain security protocols and cipher suites are provided by default in View 5.2 and later releases. By default, the global acceptance and proposal policies are very similar.

**Table 1-14.** Default Global Policies

| Default Security Protocols | Default Cipher Suites |
|---|---|
| ■ `TLS 1.1`<br>■ `TLS 1.0`<br>■ `SSLv2Hello` (acceptance policy only) | ■ `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`<br>■ `TLS_DHE_DSS_WITH_AES_128_CBC_SHA`<br>■ `TLS_DHE_RSA_WITH_AES_128_CBC_SHA`<br>■ `TLS_RSA_WITH_AES_128_CBC_SHA`<br>■ `SSL_RSA_WITH_RC4_128_SHA` |

You can change the default policies in the following ways:

- If all connecting clients support `TLS 1.1`, you can remove `TLS 1.0` and `SSLv2Hello` from the acceptance policy.
- You can add `TLS 1.2` to the acceptance and proposal policies, which will then be selected if the other end of the connection supports `TLS 1.2`.
- If all connecting clients support `AES` cipher suites, you can remove `SSL_RSA_WITH_RC4_128_SHA` from the acceptance policy.

## Updating JCE Policy Files to Support High-Strength Cipher Suites

You can add high-strength cipher suites for greater assurance, but first you must update the `local_policy.jar` and `US_export_policy.jar` policy files for JRE 7 on each View Connection Server instance and security server. You update these policy files by downloading the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7 from the Oracle Java SE Download site.

If you include high-strength cipher suites in the list and do not replace the policy files, you cannot restart the VMware Horizon View Connection Server service.

The policy files are located in the `C:\Program Files\VMware\VMware View\Server\jre\lib\security` directory.

For more information about downloading the JCE Unlimited Strength Jurisdiction Policy Files 7, see the Oracle Java SE Download site: http://www.oracle.com/technetwork/java/javase/downloads/index.html.

After you update the policy files, you must create backups of the files. If you upgrade the View Connection Server instance or security server, any changes that you have made to these files might be overwritten, and you might have to restore the files from the backup.

## Configuring Global Acceptance and Proposal Policies

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

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

### Global Acceptance and Proposal Policies Defined in View LDAP

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

#### Global Acceptance Polices

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

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

The following attribute lists the cipher suites. The order of the cipher suites is unimportant. This example shows an abbreviated list:

```
pae-ServerSSLCipherSuites = "\LIST:TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_
WITH_AES_128_CBC_SHA"
```

#### Global Proposal Policies

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

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

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

```
pae-ClientSSLCipherSuites = "\LIST:TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_
WITH_AES_128_CBC_SHA"
```

### Change the Global Acceptance and Proposal Policies

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

#### Prerequisites

- Familiarize yourself with the View LDAP attributes that define the acceptance and proposal policies. See "Global Acceptance and Proposal Policies Defined in View LDAP," on page 23.
- 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 View Connection Server computer.

2 In the console tree, select **Connect to**.

3 In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **`DC=vdi, DC=vmware, DC=int`**.

4 In the **Select or type a domain or server** text box, select or type **`localhost:389`** or the fully qualified domain name (FQDN) of the View 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 **OU=Common** in the right pane.

6 On the object **CN=Common, OU=Global, OU=Properties**, select each attribute that you want to change and type the new list of security protocols or cipher suites.

7 Restart the VMware Horizon View Connection Server service.

## Configure Acceptance Policies on Individual View Servers

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

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 SSL gateway configuration folder on the View Connection Server or security 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 View Connection Server service or VMware Horizon View Security Server service to make your changes take effect.

### Example: Default Acceptance Policies on an Individual Server

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

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

secureProtocols.1=TLSv1.1
secureProtocols.2=TLSv1
secureProtocols.3=SSLv2Hello

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

preferredSecureProtocol=TLSv1.1

# The order of the following list is unimportant:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.2=TLS_DHE_DSS_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_DHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.5=SSL_RSA_WITH_RC4_128_SHA
```

## Internet Engineering Task Force Standards

View Connection Server and security server comply 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.
- RFC 6797 HTTP Strict Transport Security (HSTS), also known as transport security, is enabled by default.
- RFC 7034 HTTP Header Field X-Frame-Options, also known as counter clickjacking, is disabled by default. You can enable it by adding the entry `x-frame-options=<options>` to the file `locked.properties`. For information on how to add properties to the file `locked.properties`, see "Configure Acceptance Policies on Individual View Servers," on page 24. The parameter `<options>` can have one of the following values, which are case-sensitive:
  - `OFF` - Disable counter clickjacking (default).
  - `DENY` - Do not use frames.
  - `SAMEORIGIN` - Do not use foreign frames.
  - `ALLOW-FROM <URL>` - Do not use foreign frames except <URL>, where <URL> specifies an additional trusted origin.

  For more information on RFC 7034, see http://tools.ietf.org/html/rfc7034.

  **NOTE** Counter clickjacking will prevent the proper operation of HTML Access when using a Blast Secure Gateway (BSG), which is why it is not enabled by default.

### Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) assures that compromise of an SSL session does not mean compromise of other SSL sessions that use the same server certificate. It is a property of cipher suites with DHE in their names. Of the five cipher suites we enable by default, three have this property. The downside of PFS is performance, so a balance needs to be struck.

View supports DHE-DSS, DHE-RSA, and ECDHE-RSA cipher suites. The first two can be enabled in conjunction with standard DSS or RSA certificates. ECDHE-RSA has better performance but requires an ECC certificate that is signed with an RSA key. Do not request from a CA an ECC certificate that is signed with an EC key because View cannot use this.

### SSLv3 Is Disabled in View

SSLv3 is excluded from the default list of supported security protocols in Horizon 6.0 with View and later releases. Starting in Horizon 6 version 6.1, the View components use JRE 7u75 or later releases, in which SSLv3 is deactivated in Java.

VMware strongly recommends that you do not use SSLv3 in your View environment. Security vulnerability CVE-2014-3566, known as the Poodle vulnerability, affects SSLv3. For details, see http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566.

If you absolutely require SSLv3 in your environment, you can reactivate it in Java. You do this by removing `SSLv3` from the `jdk.tls.disabledAlgorithms` property in the `C:\Program Files\VMware\VMware View\Server\jre\lib\security\java.security` file on each View Connection Server instance and security server.

## Deploying USB Devices in a Secure View 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 View deployment against this security vulnerability.

By disabling USB redirection, you can prevent any USB devices from being redirected to your users' View desktops and applications. Alternatively, you can disable redirection of specific USB devices, allowing users to have access only to specific devices on their 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 View 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 View 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 View Administrator, 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 RDS desktop and application pools. You cannot set this policy for individual RDS desktop or application pools.

- In View Administrator, 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 View Agent side or on the client side, as appropriate.

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 View Agent and Horizon Client. The following table shows how the `Exclude All Devices` policy that you can set for View 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 1-15.** Effect of Combining Exclude All Devices Policies

| Exclude All Devices Policy on View 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 View Agent is not passed to Horizon Client, but View Agent and Horizon Client enforce the local value of `Exclude All Devices`.

These policies are included in the View Agent Configuration ADM template file (`vdm_agent.adm`). For more information, see "USB Settings in the View Agent Configuration ADM Template" in the *Setting Up Desktop and Application Pools in View* document.

## 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 View Agent Configuration group policy settings, you can set an include policy for known device types. With this approach, you remove the risk of allowing unknown devices to be inserted into your environment.

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

```
ExcludeAllDevices   Enabled

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

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

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

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

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

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

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

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

To disable external access to USB devices, you can block TCP port 32111 from the security server to the remote desktops and applications. 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 View Agent Configuration ADM template file (`vdm_agent.adm`). For more information, see "USB Settings in the View Agent Configuration ADM Template" in the *Setting Up Desktop and Application Pools in View* document.

# Index