VMware View Security

View 5.0
View Manager 5.0
View Composer 2.7

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-000575-00

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

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

Contents

VMware View Security

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

- Required system and database login accounts.
- Configuration options and settings that have security implications.
- Resources that must be protected, such as security-relevant configuration files and passwords, and the recommended access controls for secure operation.
- Location of log files and their purpose.
- External interfaces, ports, and services that must be open or enabled for the correct operation of VMware View.

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of VMware View. This reference guide should be used in conjunction with the *VMware View Hardening Guide* and other VMware View documentation.

VMware 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.

- VMware View Accounts on page 8

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

- VMware View Security Settings on page 9

  VMware 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.

- VMware View Resources on page 17

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

- VMware View Log Files on page 17

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

- VMware View TCP and UDP Ports on page 19

  View uses TCP and UDP ports for network access between its components. You might have to reconfigure a firewall to allow access on the appropriate ports.

- Services on a View Connection Server Host on page 23

  The operation of View Manager depends on several services that run on a View Connection Server host. If you want to adjust the operation of these services, you must first familiarize yourself with them.

- Services on a Security Server on page 24

  The operation of View Manager depends on several services that run on a security server. If you want to adjust the operation of these services, you must first familiarize yourself with them.

- Services on a View Transfer Server Host on page 24

  Transfer operations for local desktops depend on services that run on a View Transfer Server host. If you want to adjust the operation of these services, you must first familiarize yourself with them.

VMware View Accounts

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

Table 1. VMware View System Accounts

VMware View Component	Required Accounts
View Client	Configure user accounts in Active Directory for the users who have access to View desktops. The user accounts must be members of the Remote Desktop Users group, but the accounts do not require View administrator privileges.
View Client with Local Mode	Configure user accounts in Active Directory for the users who have access to View desktops in local mode. The user accounts do not require View administrator privileges. As a standard best practice for desktops, make sure that a unique password is created for the local Administrator account on each View desktop that you plan to use in local mode.
vCenter Server	Configure a user account in Active Directory with permission to perform the operations in vCenter Server that are necessary to support View Manager. For information about the required privileges, see the *VMware View Installation* document.
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. 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. For information about the required privileges, see the *VMware View Installation* document.
View Connection Server, Security Server, or View Transfer Server	Initially, all users who are members of the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer are allowed to log in to View Administrator. In View Administrator, you can use **View Configuration > Administrators** to change the list of View administrators. See the *VMware View Administration* document for information about the privileges that are required.

Table 2. VMware View Database Accounts

VMware 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. For information about setting up a View Composer database, see the *VMware 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. For information about setting up a View Composer database, see the *VMware 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.

VMware View Security Settings

VMware 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 3. Security-Related Global Settings

Setting	Description
Disable Single Sign-on for Local Mode operations	Determines if single sign-on is enabled when users log in to their local desktops. This setting is disabled by default.
Enable automatic status updates	Determines if View Manager regularly updates the global status pane and the dashboard in View Administrator. If you enable this setting, idle sessions do not time out for any user who is logged into View Administrator. This setting is disabled by default.
Message security mode	Determines if signing and verification of the JMS messages passed between View Manager components takes place. If set to **Disabled**, message security mode is disabled. If set to **Enabled**, View components reject unsigned messages. If set to **Mixed**, message security mode is enabled, but not enforced for View components that predate View Manager 3.0. The default setting is **Disabled**.
Reauthenticate secure tunnel connections after network interruption	Determines if user credentials must be reauthenticated after a network interruption when View clients use secure tunnel connections to View desktops. This setting is enabled by default.
Require SSL for client connections and View Administrator	Determines if a secure SSL communication channel is used between View Connection Server and View desktop clients and between View Connection Server and clients that access View Administrator. This setting is enabled by default.
Session timeout	Determines how long a user can keep a session open after logging in to View Connection Server. The default is 600 minutes.

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

Security-Related Server Settings in View Administrator

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

Table 4. Security-Related Server Settings

Setting	Description
Connect using SSL	If enabled, View communicates with a vCenter Server using SSL encryption. This setting is enabled by default.
Use PCoIP Secure Gateway for PCoIP connections to desktop	If enabled, View Client makes a further secure connection to the View Connection Server or security server host when users connect to a View desktop with the PCoIP display protocol. If disabled, the desktop session is established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server or security server host. This setting is disabled by default.
Use secure tunnel connection to desktop	If enabled, View Client makes a further HTTPS connection to the View Connection Server or security server host when users connect to a View desktop. If disabled, the desktop session is established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server or security server host. This setting is enabled by default.
Use secure tunnel connection for Local Mode operations	If enabled, local desktops use tunneled communications. Network traffic is routed through View Connection Server or a security server if one is configured. If disabled, data transfers take place directly between local desktops and the corresponding remote desktops in the datacenter. This setting is disabled by default.
Use SSL for Local Mode operations	If enabled, communications and data transfers between client computers and the datacenter use SSL encryption. These operations include checking in and checking out desktops and replicating data from client computers to the datacenter, but do not include transfers of View Composer base images. This setting is disabled by default.
Use SSL when provisioning desktops in Local Mode	If enabled, transfers of View Composer base-image files from the Transfer Server repository to client computers use SSL encryption. This setting is disabled by default.

For more information about these settings and their security implications, see the *VMware 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\Policies\VMware, Inc.\VMware VDM\Agent\Configuration`.

Table 5. Security-Related Settings in the View Agent Configuration Template

Setting	Registry Value Name	Description
AllowDirectRDP	AllowDirectRDP	Determines whether non-View clients can connect directly to View desktops with RDP. When this setting is disabled, View Agent permits only View-managed connections through View Client. IMPORTANT For View to operate correctly, the Windows Terminal Services service must be running on the guest operating system of each desktop. You can use this setting to prevent users from making direct RDP connections to their desktops. This setting is enabled by default.
AllowSingleSignon	AllowSingleSignon	Determines whether single sign-on (SSO) is used to connect users to View desktops. When this setting is enabled, users are required to enter only their credentials when connecting with View Client. When it is disabled, users must reauthenticate when the remote connection is made. This setting is enabled by default.
CommandsToRunOnConnect	CommandsToRunOnConnect	Specifies a list of commands or command scripts to be run when a session is connected for the first time. No list is specified by default.
CommandsToRunOnReconnect	CommandsToRunOnReconnect	Specifies a list of commands or command scripts to be run when a session is reconnected after a disconnect. No list is specified by default.
ConnectionTicketTimeout	VdmConnectionTicketTimeout	Specifies the amount of time in seconds that the View connection ticket is valid. If this setting is not configured, the default timeout period is 120 seconds.
CredentialFilterExceptions	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.

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

Security Settings in the View Client Configuration Template

Security-related settings are provided in the ADM template file for View 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 `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\Security`.

Table 6. Security Settings in the View Client Configuration Template

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

Table 6. Security Settings in the View Client Configuration Template (Continued)

Setting	Registry Value Name	Description

Certificate verification mode	CertCheckMode	Configures the level of certificate checking that is performed by View Client. You can select one of these modes:
		■ 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:
		  ■ 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 View Client.
		  ■ A verifiable certificate that was configured in your deployment has expired or is not yet valid.
		If any other certificate error condition occurs, View displays an error dialog and prevents the user from connecting to View Connection Server.
		Warn But Allow is the default value.
		■ Full Security. If any type of certificate error occurs, the user cannot connect to View Connection Server. View displays certificate errors to the user.
		To allow View Client to perform any type of certificate checking, you must select the **Require SSL for client connections and View Administrator** Global Setting in View Administrator.
		When this group policy setting is configured, users can view the selected certificate verification mode in View Client but cannot configure the setting. The SSL configuration dialog box informs users that the administrator has locked the setting.
		When this setting is not configured or disabled, View Client users can configure SSL and select a certificate verification mode.
		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 the following registry key on the client computer:
		HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security
		Use the following values in the registry key:
		■ **0** implements No Security.
		■ **1** implements Warn But Allow.
		■ **2** implements Full Security.
		If you configure both the group policy setting and the CertCheckMode setting in the registry key, the group policy setting takes precedence over the registry key value.

Table 6. Security Settings in the View Client Configuration Template (Continued)

Setting	Registry Value Name	Description
Default value of the 'Log in as current user' checkbox	LogInAsCurrentUse	Specifies the default value of the **Log in as current user** check box on the View Client connection dialog box. This setting overrides the default value specified during View Client installation. If a user runs View Client from the command line and specifies the `logInAsCurrentUser` option, that value overrides this setting. 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 View desktop. When the check box is deselected, users must provide identity and credential information multiple times before they can access a View desktop. A User Configuration setting is available in addition to the Computer Configuration setting. These settings are disabled by default.
Display option to Log in as current user	LogInAsCurrentUser_Display	Determines whether the **Log in as current user** check box is visible on the View Client connection dialog box. 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 View Client connection dialog box. 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`. A User Configuration setting is available in addition to the Computer Configuration setting. These settings are enabled by default.
Enable jump list integration	EnableJumplist	Determines whether a jump list appears in the View Client icon on the taskbar of Windows 7 and later systems. The jump list lets users connect to recent View Connection Server instances and View desktops. If View 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. This setting is enabled by default.
Enable Single Sign-On for smart card authentication	EnableSmartCardSSO	Determines whether single sign-on is enabled for smart card authentication. When single sign-on is enabled, View Client stores the encrypted smart card PIN in temporary memory before submitting it to View Connection Server. When single sign-on is disabled, View Client does not display a custom PIN dialog. This setting is disabled by default.
Ignore bad SSL certificate date received from the server	IgnoreCertDateInvalid	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. This setting is enabled by default. This setting applies to View 4.6 and earlier releases only.

Table 6. Security Settings in the View Client Configuration Template (Continued)

Setting	Registry Value Name	Description
Ignore certificate revocation problems	IgnoreRevocation	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. This setting applies to View 4.6 and earlier releases only.
Ignore incorrect SSL certificate common name (host name field)	IgnoreCertCnInvalid	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. This setting is disabled by default. This setting applies to View 4.6 and earlier releases only.
Ignore incorrect usage problems	IgnoreWrongUsage	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. This setting is disabled by default. This setting applies to View 4.6 and earlier releases only.
Ignore unknown certificate authority problems	IgnoreUnknownCa	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. This setting is disabled by default. This setting applies to View 4.6 and earlier releases only.

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

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

Security-related settings are provided in the Scripting Definitions section of the ADM template file for View 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 are stored in the registry on the host machine under `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client`.

Table 7. Security-Related Settings in the Scripting Definitions Section

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

For more information about these settings and their security implications, see the *VMware View Administration* 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 8. Security-Related Settings in View LDAP

Name-value pair	Attribute	Description
cs-allowunencryptedstartsession	`pae-NameValuePair`	Allows static key protection to be used for single-sign on to desktops that are not in a trusted domain where Security Support Provider Interface (SSPI) negotiation is supported. Static key protection is known to be relatively insecure compared to SSPI. If set to **0**, static key protection is not allowed. This setting is suitable if all the desktops are in trusted domains. If SSPI negotiation fails, the session does not start. If set to **1**, static key protection can be used if SSPI negotiation fails. This setting is suitable if some desktops are not in trusted domains. The default setting is **1**.
	`pae-OVDIKeyCipher`	Specifies the encryption key cipher that View Connection Server uses to encrypt the virtual disk (`.vmdk`) file when users check in and check out a local desktop. You can set the encryption key cipher value to **AES-128**, **AES-192** or**AES-256**. The default value is **AES-128**.
	`pae-SSOCredentialCacheTimeout`	Sets the single sign-on (SSO) timeout limit in minutes after which a user's SSO credentials are no longer valid. The default value is **15**. A value of **-1** means that no SSO timeout limit is set. A value of **0** disables SSO.

VMware View Resources

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

Table 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) *<Drive Letter>*:\Documents and Settings\All Users\Application Data\VMWare\VDM\backups (Windows Server 2003)	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	*%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs *<Drive Letter>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs	Protected by access control.
web.xml (Tomcat configuration file)	*install_directory*\VMware View\Server\broker\web apps\ROOT\Web INF	Protected by access control.

Table 10. View Transfer Server Resources

Resource	Location	Protection
httpd.conf (Apache configuration file)	*install_directory*\VMware\VMware View\Server\httpd\conf	Can be protected by access control. Ensure that this file is secured against access by any user other than View administrators.
Log files	*<Drive Letter>*:\ProgramData\VMware\VDM\logs (Windows Server 2008 R2) *%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs (Windows Server 2003 and Windows Server 2003 R2) *<Drive Letter>*:\Program Files\Apache Group\Apache2\logs (Apache server)	Protected by access control.

VMware View Log Files

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

NOTE VMware 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 *VMware View Installation* and *VMware View Integration* documents.

Table 11. VMware View Log Files

VMware View Component	File Path and Other Information
All components (installation logs)	*%TEMP%*\vminst.log_*date_timestamp* *%TEMP%*\vmmsi.log_*date_timestamp*
View Agent	Windows XP guest OS: *<Drive Letter>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs Windows Vista and Windows 7 guest OS: *<Drive Letter>*:\ProgramData\VMware\VDM\logs If a User Data Disk (UDD) is configured, *<Drive Letter>* might correspond to the UDD. The logs for PCoIP are named pcoip_agent*.log and pcoip_server*.log.
View Applications	View Event Database configured on an SQL Server or Oracle database server. Windows Application Event logs. Disabled by default.
View Client with Local Mode	Windows XP host OS: C:\Documents and Settings*%username%*\Local Settings\Application Data\VMware\VDM\Logs\ Windows Vista and Windows 7 host OS: C:\Users*%username%*\AppData\VMware\VDM\Logs\
View Composer	*%system_drive%*\Windows\Temp\vmware-viewcomposer-ga-new.log on the linked-clone desktop. 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.
View Connection Server or Security Server	*%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs*.txt on the server. *<Drive Letter>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs*.txt on the server. The log directory is configurable in the log configuration settings of the View Common Configuration ADM template file (vdm_common.adm). 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. Windows System Event logs.
View Transfer Server	Windows Server 2008 R2: *<Drive Letter>*:\ProgramData\VMware\VDM\logs*.txt Windows Server 2003 and Windows Server 2003 R2: *%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs*.txt Apache Server: *<Drive Letter>*:\Program Files\Apache Group\Apache2\logs\error.log

VMware View TCP and UDP Ports

View uses TCP and UDP ports for network access between its components. You might have to reconfigure a firewall to allow access on the appropriate ports.

Table 12. TCP and UDP Ports Used by View, Excluding Local Mode

Source	Port	Target	Port	Protocol	Description
Security server	4172	View Agent 4.5 or earlier	50002 (can be changed by group policy)	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.
Security server	4172	View Agent 4.6 or later	4172	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.
Security server	4172	View Client 4.5 or earlier	50002 (cannot be changed)	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.
Security server	4172	View Client 4.6 or later	4172	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.
Security server	*	View Connection Server	4001	TCP	JMS traffic.
Security server	*	View Connection Server	8009	TCP	AJP13-forwarded Web traffic.
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 4.5 or earlier	50002 (can be changed by group policy)	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is used.
Security server	*	View desktop 4.6 or later	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is used.
View Agent 4.5 or earlier	50002 (can be changed by group policy)	View Client 4.5 or earlier	50002 (cannot be changed)	UDP	PCoIP (AES-128-GCM or SALSA20) if PCoIP Secure Gateway is not used.
View Agent 4.5 or earlier	50002 (can be changed by group policy)	View Client 4.6 or later	4172	UDP	PCoIP (AES-128-GCM or SALSA20) if PCoIP Secure Gateway is not used.
View Agent 4.6 or later	4172	View Client 4.5 or earlier	50002 (cannot be changed)	UDP	PCoIP (AES-128-GCM or SALSA20) if PCoIP Secure Gateway is not used.
View Agent 4.6 or later	4172	View Client 4.6 or later	4172	UDP	PCoIP (AES-128-GCM or SALSA20) if PCoIP Secure Gateway is not used.
View Agent 4.5 or earlier	50002 (can be changed by group policy)	View Connection Server or security server	4172	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.
View Agent 4.6 or later	4172	View Connection Server or security server	4172	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.

Table 12. TCP and UDP Ports Used by View, Excluding Local Mode (Continued)

Source	Port	Target	Port	Protocol	Description
View Client	*	View Connection Server or security server	80	TCP	HTTP access if SSL is disabled for client connections.
View Client	*	View Connection Server or security server	443	TCP	HTTPS access if SSL is enabled for client connections.
View Client	*	View Connection Server or security server	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is used.
View Client	*	View desktop	3389	TCP	Microsoft RDP traffic to View desktops if direct connections are used instead of tunnel connections.
View Client	*	View desktop	9427	TCP	Wyse MMR redirection if direct connections are used instead of tunnel connections.
View Client	*	View desktop	32111	TCP	USB redirection if direct connections are used instead of tunnel connections.
View Client 4.5 or earlier	*	View Agent 4.5 or earlier	50002 (can be changed by group policy)	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is not used.
View Client 4.5 or earlier	50002 (cannot be changed)	View Agent 4.5 or earlier	50002 (can be changed by group policy)	UDP	PCoIP (AES-28-GCM or SALSA20) if PCoIP Secure Gateway is not used.
View Client 4.5 or earlier	*	View Agent 4.6 or later	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is not used.
View Client 4.5 or earlier	50002 (cannot be changed)	View Agent 4.6 or later	4172	UDP	PCoIP (AES-28-GCM or SALSA20) if PCoIP Secure Gateway is not used.
View Client 4.5 or earlier	50002 (cannot be changed)	View Connection Server or security server	4172	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.
View Client 4.6 or later	*	View Agent 4.5 or earlier	50002 (can be changed by group policy)	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is not used.
View Client 4.6 or later	4172	View Agent 4.5 or earlier	50002 (can be changed by group policy)	UDP	PCoIP (AES-28-GCM or SALSA20) if PCoIP Secure Gateway is not used.
View Client 4.6 or later	*	View Agent 4.6 or later	4172	TCP	PCoIP (HTTPS) if PCoIP Secure Gateway is not used.
View Client 4.6 or later	4172	View Agent 4.6 or later	4172	UDP	PCoIP (AES-28-GCM or SALSA20) if PCoIP Secure Gateway is not used.

Table 12. TCP and UDP Ports Used by View, Excluding Local Mode (Continued)

Source	Port	Target	Port	Protocol	Description
View Client 4.6 or later	4172	View Connection Server or security server	4172	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway is used.
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	4172	View Agent 4.5 or earlier	50002 (can be changed by group policy)	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway via the View Connection Server is used.
View Connection Server	4172	View Agent 4.6 or later	4172	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway via the View Connection Server is used.
View Connection Server	4172	View Client 4.5 or earlier	50002 (cannot be changed)	UDP	PCoIP (AES-128-GCM only) if PCoIP Secure Gateway via the View Connection Server is used.
View Connection Server	4172	View Client 4.6 or later	4172	UDP	PCoIP (AES-128-GCM only) 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 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.

Table 12. TCP and UDP Ports Used by View, Excluding Local Mode (Continued)

Source	Port	Target	Port	Protocol	Description
View desktop	*	View Connection Server instances	4001	TCP	JMS 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.

The Local Mode feature requires you to open an additional number of ports for its correct operation.

Table 13. TCP and UDP Ports Used by Local Mode

Source	Port	Target	Port	Protocol	Description
Security server	*	View Transfer Server	80	TCP	View desktop download and data replication if tunnel connections are used and SSL is disabled for local mode operations.
Security server	*	View Transfer Server	443	TCP	View desktop download and data replication if tunnel connections are used and SSL is enabled for local mode operations.
View Client with Local Mode	*	View Transfer Server	80	TCP	View desktop download and data replication if direct connections are used instead of tunnel connections, and SSL is disabled for local mode operations.
View Client with Local Mode	*	View Transfer Server	443	TCP	View desktop download and data replication if direct connections are used instead of tunnel connections, and SSL is enabled for local mode operations.
View Connection Server	*	ESX host	902	TCP	Used when checking out local desktops.
View Connection Server	*	View Transfer Server	80	TCP	View desktop download and data replication if tunnel connections via the View Connection Server are used and SSL is disabled for local mode operations.

Table 13. TCP and UDP Ports Used by Local Mode (Continued)

Source	Port	Target	Port	Protocol	Description
View Connection Server	*	View Transfer Server	443	TCP	View desktop download and data replication if tunnel connections via the View Connection Server are used and SSL is enabled for local mode operations.
View Connection Server	*	View Transfer Server	4001	TCP	JMS traffic to support local mode.
View Transfer Server	*	ESX host	902	TCP	Publishing View Composer packages for local mode.

Services on a View Connection Server Host

The operation of View Manager depends on several services that run on a View Connection Server host. If you want to adjust the operation of these services, you must first familiarize yourself with them.

Table 14. View Connection Server Host Services

Service Name	Startup Type	Description
VMware View Connection Server	Automatic	Provides connection broker services. This service must be running for the correct operation of View Manager. 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 View Script Host service.
VMware View Framework Component	Manual	Provides event logging, security, and COM+ framework services for View Manager. This service must be running for the correct operation of View Manager.
VMware View Message Bus Component	Manual	Provides messaging services between View Manager components. This service must be running for the correct operation of View Manager.
VMware 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 View Script Host	Automatic (if enabled)	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 View Security Gateway Component	Manual	Provides secure tunnel services for View Manager. This service must be running for the correct operation of View Manager.
VMware View Web Component	Manual	Provides web services for View Manager. This service must be running for the correct operation of View Manager.
VMwareVDMDS	Automatic	Provides LDAP directory services for View Manager. This service must be running for the correct operation of View Manager. This service must also be running during upgrades of VMware View to ensure that existing data is migrated correctly.

Services on a Security Server

The operation of View Manager depends on several services that run on a security server. If you want to adjust the operation of these services, you must first familiarize yourself with them.

Table 15. Security Server Services

Service Name	Startup Type	Description
VMware View Security Server	Automatic	Provides security server services. This service must be running for the correct operation of a security server. If you start or stop this service, it also starts or stops the Framework and Security Gateway services.
VMware View Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must be running for the correct operation of a security server.
VMware View PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to a security server through the PCoIP Secure Gateway.
VMware View Security Gateway Component	Manual	Provides secure tunnel services. This service must be running for the correct operation of a security server.

Services on a View Transfer Server Host

Transfer operations for local desktops depend on services that run on a View Transfer Server host. If you want to adjust the operation of these services, you must first familiarize yourself with them.

All of the services that are installed with View Transfer Server must be running for the correct operation of local desktops in View Manager.

Table 16. View Transfer Server Host Services

Service Name	Startup Type	Description
VMware View Transfer Server	Automatic	Provides services that coordinate the View Transfer Server related services. If you start or stop this service, it also starts or stops the View Transfer Server Control Service and Framework service.
VMware View Transfer Server Control Service	Manual	Provides management capabilities for View Transfer Server and handles communication with View Connection Server.
VMware View Framework Component	Manual	Provides event logging, security, and COM+ framework services for View Manager.
Apache2.2 service	Automatic	Provides data-transfer capabilities for client computers that run View desktops in local mode. The Apache2.2 service is started when you add View Transfer Server to View Manager.

Index