VMware View Installation

View 5.1
View Manager 5.1
View Composer 3.0

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-000730-00

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 Installation

VMware View Installation explains how to install the VMware® View™ server and client components.

Intended Audience

This information is intended for anyone who wants to install VMware View. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

System Requirements for Server Components

1

Hosts that run VMware View server components must meet specific hardware and software requirements.

This chapter includes the following topics:

View Connection Server Requirements

View Connection Server acts as a broker for client connections by authenticating and then directing incoming user requests to the appropriate View desktop. View Connection Server has specific hardware, operating system, installation, and supporting software requirements.

- Hardware Requirements for View Connection Server on page 8

  You must install all View Connection Server installation types, including standard, replica, and security server installations, on a dedicated physical or virtual machine that meets specific hardware requirements.

- Supported Operating Systems for View Connection Server on page 8

  You must install View Connection Server on a Windows Server 2008 R2 operating system.

- Virtualization Software Requirements for View Connection Server on page 8

  View Connection Server requires certain versions of VMware virtualization software.

- Network Requirements for Replicated View Connection Server Instances on page 8

  If you install replicated View Connection Server instances, configure the instances in the same location and connect them over a high-performance LAN.

Hardware Requirements for View Connection Server

You must install all View Connection Server installation types, including standard, replica, and security server installations, on a dedicated physical or virtual machine that meets specific hardware requirements.

Table 1-1. View Connection Server Hardware Requirements

Hardware Component	Required	Recommended
Processor	Pentium IV 2.0GHz processor or higher	4 CPUs
Networking	One or more 10/100Mbps network interface cards (NICs)	1Gbps NICs
Memory Windows Server 2008 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more View desktops

These requirements also apply to replica and security server View Connection Server instances that you install for high availability or external access.

IMPORTANT The physical or virtual machine that hosts View Connection Server must use a static IP address.

Supported Operating Systems for View Connection Server

You must install View Connection Server on a Windows Server 2008 R2 operating system.

The following operating systems support all View Connection Server installation types, including standard, replica, and security server installations.

Table 1-2. Operating System Support for View Connection Server

Operating System	Version	Edition
Windows Server 2008 R2	64-bit	Standard Enterprise
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise

Virtualization Software Requirements for View Connection Server

View Connection Server requires certain versions of VMware virtualization software.

- If you are using vSphere, you must use one of the following supported versions:
  - vSphere 4.0 Update 4 or later
  - vSphere 4.1 Update 2 or later
  - vSphere 5.0 Update 1 or later
- Both ESX and ESXi hosts are supported.

For details about which versions of VMware View are compatible with which versions of vCenter Server and ESX/ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Network Requirements for Replicated View Connection Server Instances

If you install replicated View Connection Server instances, configure the instances in the same location and connect them over a high-performance LAN.

Do not use a WAN to connect replicated View Connection Server instances.

Even a high-performance WAN with low average latency and high throughput might have periods when the network cannot deliver the performance characteristics that are needed for View Connection Server instances to maintain consistency.

If the View LDAP configurations on View Connection Server instances become inconsistent, users might not be able to access their desktops. A user might be denied access when connecting to a View Connection Server instance with an out-of-date configuration.

View Administrator Requirements

Administrators use View Administrator to configure View Connection Server, deploy and manage desktops, control user authentication, initiate and examine system events, and carry out analytical activities. Client systems that run View Administrator must meet certain requirements.

View Administrator is a Web-based application that is installed when you install View Connection Server. You can access and use View Administrator with the following Web browsers:

- Internet Explorer 8
- Internet Explorer 9
- Firefox 6
- Firefox 7

To use View Administrator with your Web browser, you must install Adobe Flash Player 10 or later. Your client system must have access to the internet to allow Adobe Flash Player to be installed.

The computer on which you launch View Administrator must trust the root and intermediate certificates of the server that hosts View Connection Server. The supported browsers already contain certificates for all of the well-known certificate authorities (CAs). If your certificates come from a CA that is not well known, you must follow the instructions in the *VMware View Installation* document about importing root and intermediate certificates.

To display text properly, View Administrator requires Microsoft-specific fonts. If your Web browser runs on a non-Windows operating system such as Linux, UNIX, or Mac OS, make sure that Microsoft-specific fonts are installed on your computer.

Currently, the Microsoft Web site does not distribute Microsoft fonts, but you can download them from independent Web sites.

View Composer Requirements

View Manager uses View Composer to deploy multiple linked-clone desktops from a single centralized base image. View Composer has specific installation and storage requirements.

- Supported Operating Systems for View Composer on page 10

  View Composer supports 64-bit operating systems with specific requirements and limitations. You can install View Composer on the same physical or virtual machine as vCenter Server or on a separate server.

- Hardware Requirements for Standalone View Composer on page 10

  With View 5.1 and later releases, View Composer is no longer required to be installed on the same physical or virtual machine as vCenter Server. If you install View Composer on a separate server, you must use a dedicated physical or virtual machine that meets specific hardware requirements.

- Database Requirements for View Composer on page 10

  View Composer requires an SQL database to store data. The View Composer database must reside on, or be available to, the View Composer server host.

Supported Operating Systems for View Composer

View Composer supports 64-bit operating systems with specific requirements and limitations. You can install View Composer on the same physical or virtual machine as vCenter Server or on a separate server.

Table 1-3. Operating System Support for View Composer

Operating System	Version	Edition
Windows Server 2008 R2	64-bit	Standard Enterprise
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise

If you plan to install View Composer on a different physical or virtual machine than vCenter Server, see "Hardware Requirements for Standalone View Composer," on page 10.

Hardware Requirements for Standalone View Composer

With View 5.1 and later releases, View Composer is no longer required to be installed on the same physical or virtual machine as vCenter Server. If you install View Composer on a separate server, you must use a dedicated physical or virtual machine that meets specific hardware requirements.

A standalone View Composer installation works with vCenter Server installed on a Windows Server computer and with the Linux-based vCenter Server Appliance. VMware recommends having a one-to-one mapping between each View Composer service and vCenter Server instance.

Table 1-4. View Composer Hardware Requirements

Hardware Component	Required	Recommended
Processor	1.4 GHz 64-bit processor or faster and 2 CPUs Intel Itanium 2 processor for Itanium-based systems	2GHz or faster and 4 CPUs
Networking	One or more 10/100Mbps network interface cards (NICs)	1Gbps NICs
Memory	4GB RAM or higher	8GB RAM or higher for deployments of 50 or more View desktops
Disk space	40GB	60GB

IMPORTANT The physical or virtual machine that hosts View Composer must use a static IP address.

Database Requirements for View Composer

View Composer requires an SQL database to store data. The View Composer database must reside on, or be available to, the View Composer server host.

If a database server already exists for vCenter Server, View Composer can use that existing database server if it is a version listed in Table 1-5. For example, View Composer can use the Microsoft SQL Server 2005 or 2008 Express instance provided with vCenter Server. If a database server does not already exist, you must install one.

View Composer supports a subset of the database servers that vCenter Server supports. If you are already using vCenter Server with a database server that is not supported by View Composer, continue to use that database server for vCenter Server and install a separate database server to use for View Composer and View Manager database events.

IMPORTANT If you create the View Composer database on the same SQL Server instance as vCenter Server, do not overwrite the vCenter Server database.

Table 1-5 lists the supported database servers and versions. For a complete list of database versions supported with vCenter Server, see the *VMware vSphere Compatibility Matrixes* on the VMware vSphere documentation Web site.

Table 1-5. Supported Database Servers for View Composer

Database	vCenter Server 5.0 U1 and later	vCenter Server 4.1 U2 and later	vCenter Server 4.0 U4 and later
Microsoft SQL Server 2005 (SP4), Standard, Enterprise, and Datacenter (32- and 64-bit)	Yes	Yes	Yes
Microsoft SQL Server 2008 Express (R2) (64-bit)	Yes	No	No
Microsoft SQL Server 2008 (SP2), Standard, Enterprise, and Datacenter (32- and 64-bit)	Yes	Yes	Yes
Microsoft SQL Server 2008 (R2), Standard and Enterprise (32- and 64-bit)	Yes	Yes	Yes
Oracle 10g Release 2, Standard, Standard ONE, and Enterprise [10.2.0.4] (32- and 64-bit)	Yes	Yes	Yes
Oracle 11g Release 2, Standard, Standard ONE, and Enterprise [11.2.0.1] with Patch 5 (32- and 64-bit)	Yes	Yes	Yes

NOTE If you use an Oracle 11g R2 database, you must install Oracle 11.2.0.1 Patch 5. This patch requirement applies to both 32-bit and 64-bit versions.

View Transfer Server Requirements

View Transfer Server is an optional View Manager component that supports check in, check out, and replication of desktops that run in local mode. View Transfer Server has specific installation, operating system, and storage requirements.

- Installation and Upgrade Requirements for View Transfer Server on page 12

  You must install View Transfer Server as a Windows application in a virtual machine that meets specific requirements.

- Supported Operating Systems for View Transfer Server on page 12

  You must install View Transfer Server on a supported operating system with at least the minimum required amount of RAM.

- Storage Requirements for View Transfer Server on page 12

  View Transfer Server transfers static content to and from the Transfer Server repository and dynamic content between local desktops and remote desktops in the datacenter. View Transfer Server has specific storage requirements.

Installation and Upgrade Requirements for View Transfer Server

You must install View Transfer Server as a Windows application in a virtual machine that meets specific requirements.

The virtual machine that hosts View Transfer Server must meet several requirements regarding network connectivity:

- It must be managed by the same vCenter Server instance as the local desktops that it will manage.
- It does not have to be part of a domain.
- It must use a static IP address.

The View Transfer Server software cannot coexist on the same virtual machine with any other View Manager software component, including View Connection Server.

Do not manually add or remove PCI devices on the virtual machine that hosts View Transfer Server. If you add or remove PCI devices, View might be unable to discover hot-added devices, which might cause data transfer operations to fail.

You can install multiple View Transfer Server instances for high availability and scalability.

Supported Operating Systems for View Transfer Server

You must install View Transfer Server on a supported operating system with at least the minimum required amount of RAM.

Table 1-6. Operating System Support for View Transfer Server

Operating System	Version	Edition	Minimum RAM
Windows Server 2008 R2	64-bit	Standard Enterprise	4GB
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise	4GB

IMPORTANT Configure two virtual CPUs for virtual machines that host View Transfer Server.

Storage Requirements for View Transfer Server

View Transfer Server transfers static content to and from the Transfer Server repository and dynamic content between local desktops and remote desktops in the datacenter. View Transfer Server has specific storage requirements.

- The disk drive on which you configure the Transfer Server repository must have enough space to store your static image files. Image files are View Composer base images.
- View Transfer Server must have access to the datastores that store the desktop disks to be transferred. The datastores must be accessible from the ESX/ESXi host where the View Transfer Server virtual machine is running.
- The recommended maximum number of concurrent disk transfers that View Transfer Server can support is 20.

During a transfer operation, a local desktop's virtual disk is mounted on View Transfer Server. The View Transfer Server virtual machine has four SCSI controllers. This configuration allows multiple disks to be attached to the virtual machine at one time.

- Because local desktops can contain sensitive user data, make sure data is encrypted during its transit over the network.

  In View Administrator, you can configure data-transfer security options on each View Connection Server instance. To configure these options in View Administrator, click **View Configuration > Servers**, select a View Connection Server instance, and click **Edit**.

- When View Transfer Server is added to View Manager, its Distributed Resource Scheduler (DRS) automation policy is set to Manual, which effectively disables DRS.

  To migrate a View Transfer Server instance to another ESX host or datastore, you must place the instance in maintenance mode before you begin the migration.

  When View Transfer Server is removed from View Manager, the DRS automation policy is reset to the value it had before View Transfer Server was added to View Manager.

System Requirements for Client Components

2

Systems running View client components must meet certain hardware and software requirements.

This chapter includes the following topics:

Supported Operating Systems for View Agent

The View Agent component assists with session management, single sign-on, and device redirection. You must install View Agent on all virtual machines, physical systems, and terminal servers that will be managed by View Manager.

Table 2-1. View Agent Operating System Support

Guest Operating System	Version	Edition	Service Pack
Windows 7	64-bit and 32-bit	Enterprise and Professional	None and SP1
Windows Vista	32-bit	Business and Enterprise	SP1 and SP2
Windows XP	32-bit	Professional	SP3
Windows 2008 R2 Terminal Server	64-bit	Standard	SP1
Windows 2008 Terminal Server	64-bit	Standard	SP2

To use the View Persona Management setup option with View Agent, you must install View Agent on Windows 7, Windows Vista, or Windows XP virtual machines. This option does not operate on physical computers or Microsoft Terminal Servers.

You can install the standalone version of View Persona Management on physical computers. See "Supported Operating Systems for Standalone View Persona Management," on page 16.

IMPORTANT If you use Windows 7 in a virtual machine, the host must be ESX/ESXi 4.0 Update 4 or later, ESX/ESXi 4.1 Update 2 or later, or ESXi 5.0 Update 1 or later.

Supported Operating Systems for Standalone View Persona Management

The standalone View Persona Management software provides persona management for standalone physical computers and virtual machines that do not have View Agent 5.*x* installed. When users log in, their profiles are downloaded dynamically from a remote profile repository to their standalone systems.

NOTE To configure View Persona Management for View desktops, install View Agent with the **View Persona Management** setup option. The standalone View Persona Management software is intended for non-View systems only.

Table 2-2 lists the operating systems supported for the standalone View Persona Management software.

Table 2-2. Operating System Support for Standalone View Persona Management

Guest Operating System	Version	Edition	Service Pack
Windows 7	64-bit and 32-bit	Enterprise and Professional	None and SP1
Windows Vista	32-bit	Business and Enterprise	SP1 and SP2
Windows XP	32-bit	Professional	SP3

The standalone View Persona Management software is not supported on Microsoft Terminal Services or Microsoft Remote Desktop Services.

Supported Operating Systems for Windows-Based View Client and View Client with Local Mode

Users run View Client to connect to their View desktops. You must install View Client or View Client with Local Mode on a supported operating system.

Table 2-3 lists the Microsoft Windows operating systems supported for View Client. For information about operating systems supported by other View Clients, such as View Client for the Mac and View Client for iPad, see the documents that pertain to the specific client. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Table 2-3. View Client Operating System Support for Windows-Based Clients

Operating System	Version	Edition	Service Pack
Windows 7	32-bit and 64-bit	Home, Enterprise, Professional, and Ultimate	None and SP1
Windows XP	32-bit	Home and Professional	SP3
Windows Vista	32-bit	Home, Business, Enterprise, and Ultimate	SP2

IMPORTANT View Client with Local Mode is supported only on Windows systems and only on physical computers. In addition, to use this feature, your VMware license must include View Client with Local Mode.

View Client with Local Mode is the fully supported feature that in earlier releases was an experimental feature called View Client with Offline Desktop.

NOTE VMware partners offer thin client devices for VMware View deployments. The features and Linux operating systems that are available for each thin client device are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin client devices, see the *Thin Client Compatibility Guide*, available on the VMware Web site.

Hardware Requirements for Local Mode Desktops

When you check out a View desktop to run on your local computer, the hardware on the client computer must support both the local system and the virtual machine that now runs on it.

PC Hardware

Table 2-4 describes the hardware requirements for various View desktop operating systems.

Table 2-4. Processor Requirements

Client Computer Requirement	Description
PC	x86 64-compatible LAHF/SAHF support in long mode
Number of CPUs	Multiprocessor systems are supported
CPU speed	For a Windows XP local desktop, 1.3GHz or faster; 1.6GHz recommended For a Windows 7 desktop, 1.3GHz or faster; for Aero effects, 2.0GHz or faster
Intel processors	Pentium 4, Pentium M (with PAE), Core, Core 2, Core i3, Core i5, and Core i7 processors For Windows 7 Aero: Intel Dual Core
AMD processors	Athlon, Athlon MP, Athlon XP, Athlon 64, Athlon X2, Duron, Opteron, Turion X2, Turion 64, Sempron, Phenom, and Phenom II The AMD CPU must have segment-limit support in long mode. For Windows 7 Aero: Althon 4200+ and above
64-bit operating systems on View desktops	Intel Pentium 4 and Core 2, and Core i7 processors with EM64T and Intel Virtualization Technology The Intel CPU must have VT-x support enabled in the host system BIOS. The BIOS settings that must be enabled for VT-x support vary depending on the system vendor. See the VMware knowledge base article at http://kb.vmware.com/kb/1003944 for information about how to determine if VT-x support is enabled. Most AMD64 processors (except the earliest revision C Opteron processors)
GPU for Windows 7 Aero	nVidia GeForce 8800GT and above ATI Radeon HD 2600 and above

Although the operating system on the client computer can be 32-bit or 64-bit, the hardware must be 64-bit compatible and must have the Intel or AMD virtualization assist technologies enabled to run a View desktop with a 64-bit operating system. If these requirements are met, you should be able to run a View desktop with a 64-bit operating system on a client that has either a 32-bit or 64-bit operating system.

Disk Space

If you use a default setup for the operating system in the View desktop, the actual disk space needs are approximately the same as those for installing and running the operating system and applications on a physical computer.

For example, Microsoft recommends 16GB of hard disk space for a machine that runs a 32-bit Windows 7 operating system. If you configure a 16GB virtual hard disk for a 32-bit Windows 7 virtual machine, only the amount of disk space actually used is downloaded when you check out the local desktop. For a desktop that is allocated 16GB, the actual download size might be 7GB.

After the desktop is downloaded, the amount of disk space used can grow to 16GB if you configured a 16GB hard disk. Because a snapshot is taken during replication, an additional equivalent amount of disk space is required. For example, if 7GB of disk space is currently being used for the local desktop, the snapshot consumes an additional 7GB on the client computer.

IDE and SCSI hard drives are supported.

Memory

You need enough memory to run the host operating system on the client computer, plus the memory required for the View desktop's operating system and for applications on the client computer and the View desktop. VMware recommends that you have 2GB and above for Windows XP and Windows Vista, and 3GB and above for Windows 7. For more information on memory requirements, see your guest operating system and application documentation.

The total amount of memory you can assign to all virtual machines running on a single computer is limited only by the amount of RAM on the computer. The maximum amount of memory for each View desktop on 64-bit computers it is 32GB.

Display

A 32-bit display adapter is recommended. 3D benchmarks, such as 3DMark '06, might not render correctly or at all when running Windows Vista or Windows 7 virtual machines on some graphics hardware.

View Client with Local Mode supports DirecX9c, which becomes enabled automatically on client systems with capable GPUs. DirecX9c includes 3D capabilities such as Google Earth with 3D building turned on, Windows 7 Aero effects, and some 3D games.

To play video at 720p or higher requires a multiprocessor system.

For CPU and GPU requirements to support Windows 7 Aero, see Table 2-4.

Client Browser Requirements for View Portal

From a client system, you can open a browser and browse to a View Connection Server instance. The Web page that appears is called View Portal, and it contains links for downloading the installer file for View Client.

To use View Portal, you must have one of the following Web browsers:

- Internet Explorer 8
- Internet Explorer 9
- Firefox 6
- Firefox 7

- Safari 5 (on a Mac)

Remote Display Protocol and Software Support

Remote display protocols and software provide access to the desktops of remote computers over a network connection. View Client supports the Microsoft Remote Desktop Protocol (RDP) and PCoIP from VMware.

- VMware View with PCoIP on page 19

  PCoIP provides an optimized desktop experience for the delivery of the entire desktop environment, including applications, images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP can compensate for an increase in latency or a reduction in bandwidth, to ensure that end users can remain productive regardless of network conditions.

- Microsoft RDP on page 21

  Remote Desktop Protocol is the same multichannel protocol many people already use to access their work computer from their home computer. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data.

- Requirements for Using Multimedia Redirection (MMR) on page 21

  Multimedia redirection (MMR) delivers the multimedia stream directly to client computers by using a virtual channel.

VMware View with PCoIP

PCoIP provides an optimized desktop experience for the delivery of the entire desktop environment, including applications, images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP can compensate for an increase in latency or a reduction in bandwidth, to ensure that end users can remain productive regardless of network conditions.

PCoIP is supported as the display protocol for View desktops with virtual machines and with physical machines that contain Teradici host cards.

PCoIP Features

Key features of PCoIP include the following:

- For users outside the corporate firewall, you can use this protocol with your company's virtual private network or with View security servers.
- Advanced Encryption Standard (AES) 128-bit encryption is supported and is turned on by default.
- Connections to Windows desktops with the View Agent operating system versions listed in "Supported Operating Systems for View Agent," on page 15 are supported.
- Connections from all types of View clients. For more information, go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.
- MMR redirection is supported for Windows XP and Vista clients. MMR redirection is not supported for Windows 7 View Clients and is not supported on Windows 7 View desktops.
- USB redirection is supported.
- Audio redirection with dynamic audio quality adjustment for LAN and WAN is supported.
- Optimization controls for reducing bandwidth usage on the LAN and WAN.
- Multiple monitors are supported. You can use up to four monitors and adjust the resolution for each monitor separately, with a resolution of up to 2560x1600 per display. Pivot display and autofit are also supported.

  When the 3D feature is enabled, up to 2 monitors are supported with a resolution of up to 1920x1200.

- 32-bit color is supported for virtual displays.
- ClearType fonts are supported.
- Copy and paste of text and images between a local Windows client system and the desktop is supported, up to 1MB. Supported file formats include text, images, and RTF (Rich Text Format). You cannot copy and paste system objects such as folders and files between systems.

Video Quality

480p-formatted video — You can play video at 480p or lower at native resolutions when the View desktop has a single virtual CPU. If the operating system is Windows 7 and you want to play the video in high-definition Flash or in full screen mode, the desktop requires a dual virtual CPU.

720p-formatted video — You can play video at 720p at native resolutions if the View desktop has a dual virtual CPU. Performance might be affected if you play videos at 720p in high definition or in full screen mode.

1080p-formatted video — If the View desktop has a dual virtual CPU, you can play 1080p formatted video, although the media player might need to be adjusted to a smaller window size.

3D — If you plan to use 3D applications such as Windows Aero themes or Google Earth, the Windows 7 View desktop must have virtual hardware version 8, available with vSphere 5 and later. You must also turn on the pool setting called **Windows 7 3D Rendering**. Up to 2 monitors are supported, and the maximum screen resolution is 1920 x 1200.

This non-hardware accelerated graphics feature enables you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical graphics processing unit (GPU).

Recommended Guest Operating System Settings

Recommended guest operating system settings include the following settings:

- For Windows XP desktops: 768MB RAM or more and a single CPU
- For Windows 7 desktops: 1GB of RAM and a dual CPU

Desktop Client Hardware Requirements

Client hardware requirements include the following:

- x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.
- ARM processor with NEON (preferred) or WMMX2 extensions, with a 1Ghz or higher processor speed.
- Available RAM above system requirements to support various monitor setups. Use the following formula as a general guide:

  ```
  20MB + (24 * (# monitors) * (monitor width) * (monitor height))
  ```

  As a rough guide, you can use the following calculations:

  ```
  1 monitor: 1600 x 1200: 64MB
  2 monitors: 1600 x 1200: 128MB
  3 monitors: 1600 x 1200: 256MB
  ```

NOTE For mobile client hardware requirements, go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Microsoft RDP

Remote Desktop Protocol is the same multichannel protocol many people already use to access their work computer from their home computer. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data.

Microsoft RDP provides the following features:

- With RDP 6, you can use multiple monitors in span mode. RDP 7 has true multiple monitor support, for up to 16 monitors.
- You can copy and paste text and system objects such as folders and files between the local system and the View desktop.
- RDP supports 32-bit color.
- RDP supports 128-bit encryption.
- You can use this protocol for making secure, encrypted connections to a View security server in the corporate DMZ.

Following are RDP-related requirements and considerations for different Windows operating systems and features.

- For Windows XP and Windows XP Embedded systems, you should use Microsoft RDC 6.x.
- Windows Vista comes with RDC 6.x installed, though RDC 7 is recommended.
- Windows 7 comes with RDC 7 installed. Windows 7 SP1 comes with RDC 7.1 installed.
- You must have RDC 6.0 or later to use multiple monitors.
- For Windows XP desktop virtual machines, you must install the RDP patches listed in Microsoft Knowledge Base (KB) articles 323497 and 884020. If you do not install the RDP patches, a `Windows Sockets failed error` message might appear on the client.
- The View Agent installer configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389. If you change the RDP port number, you must change the associated firewall rules.

You can download RDC versions from the Microsoft Web site.

Desktop Client Hardware Requirements

Client hardware requirements include the following:

- x86-based processor with SSE2 extensions, with a 800MHz or higher processor speed.
- ARM processor with NEON (preferred) or WMMX2 extensions, with a 600MHz or higher processor speed.
- 128MB RAM.

NOTE Mobile clients, such as iPad and Android, use only the PCoIP display protocol.

Requirements for Using Multimedia Redirection (MMR)

Multimedia redirection (MMR) delivers the multimedia stream directly to client computers by using a virtual channel.

With MMR, the multimedia stream is processed, that is, encoded and decoded, on the client system. Local hardware formats and plays media content, thereby offloading the demand on the ESX/ESXi host.

View Client and View Client with Local Mode support MMR on the following operating systems:

- Windows XP

- Windows XP Embedded
- Windows Vista

The MMR feature supports the media file formats that the client system supports, since local decoders must exist on the client. File formats include MPEG2-1, MPEG-2, MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3; and WAV, among others.

Use Windows Media Player 10 or later, and install it on both the local computer, or client access device, and the View desktop.

You must add the MMR port as an exception to your firewall software. The default port for MMR is 9427.

NOTE The View Client video display hardware must have overlay support for MMR to work correctly.

Windows 7 clients and Windows 7 View desktops do not support MMR. For Windows 7 clients agents, use Windows media redirection, included with RDP 7.

Adobe Flash Requirements

You can reduce the amount of bandwidth used by Adobe Flash content that runs in View desktop sessions. This reduction can improve the overall browsing experience and make other applications running in the desktop more responsive.

Adobe Flash bandwidth reduction is available for Internet Explorer sessions on Microsoft Windows only, and for Adobe Flash versions 9 and 10 only. To make use of Adobe Flash bandwidth reduction settings, Adobe Flash must not be running in full screen mode.

Smart Card Authentication Requirements

Client systems that use a smart card for user authentication must meet certain requirements.

Each client system that uses a smart card for user authentication must have the following software and hardware:

- View Client
- A Windows-compatible smart card reader
- Smart card middleware
- Product-specific application drivers

You must also install product-specific application drivers on the View desktops.

View supports smart cards and smart card readers that use a PKCS#11 or Microsoft CryptoAPI provider. You can optionally install the ActivIdentity ActivClient software suite, which provides tools for interacting with smart cards.

Users that authenticate with smart cards must have a smart card or USB smart card token, and each smart card must contain a user certificate.

To install certificates on a smart card, you must set up a computer to act as an enrollment station. This computer must have the authority to issue smart card certificates for users, and it must be a member of the domain you are issuing certificates for.

IMPORTANT When you enroll a smart card, you can choose the key size of the resulting certificate. To use smart cards with local desktops, you must select a 1024-bit or 2048-bit key size during smart card enrollment. Certificates with 512-bit keys are not supported.

The Microsoft TechNet Web site includes detailed information on planning and implementing smart card authentication for Windows systems.

See "Prepare Active Directory for Smart Card Authentication," on page 28 for information on tasks you might need to perform in Active Directory when you implement smart card authentication with View.

Smart card authentication is not supported by all View Clients. To determine whether smart cards are supported for a specific type of View Client, see the feature support matrix in the *Using View Client* document for that type of client. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Preparing Active Directory 3

View uses your existing Microsoft Active Directory infrastructure for user authentication and management. You must perform certain tasks to prepare Active Directory for use with View.

View supports the following versions of Active Directory:

- Windows 2003 Active Directory
- Windows 2008 Active Directory

This chapter includes the following topics:

Configuring Domains and Trust Relationships

You must join each View Connection Server host to an Active Directory domain. The host must not be a domain controller. You place View desktops in the same domain as the View Connection Server host or in a domain that has a two-way trust relationship with the View Connection Server host's domain.

You can entitle users and groups in the View Connection host's domain to View desktops and pools. You can also select users and groups from the View Connection Server host's domain to be administrators in View Administrator. To entitle or select users and groups from a different domain, you must establish a two-way trust relationship between that domain and the View Connection Server host's domain.

Users are authenticated against Active Directory for the View Connection Server host's domain and against any additional user domains with which a trust agreement exists.

NOTE Because security servers do not access any authentication repositories, including Active Directory, they do not need to reside in an Active Directory domain.

Trust Relationships and Domain Filtering

To determine which domains it can access, a View Connection Server instance traverses trust relationships beginning with its own domain.

For a small, well-connected set of domains, View Connection Server can quickly determine the full list of domains, but the time that it takes increases as the number of domains increases or as the connectivity between the domains decreases. The list might also include domains that you would prefer not to offer to users when they log in to their View desktops.

You can use the `vdmadmin` command to configure domain filtering to limit the domains that a View Connection Server instance searches and that it displays to users. See the *VMware View Administration* document for more information.

Creating an OU for View Desktops

You should create an organizational unit (OU) specifically for your View desktops. An OU is a subdivision in Active Directory that contains users, groups, computers, or other OUs.

To prevent group policy settings from being applied to other Windows servers or workstations in the same domain as your desktops, you can create a GPO for your View group policies and link it to the OU that contains your View desktops. You can also delegate control of the OU to subordinate groups, such as server operators or individual users.

If you use View Composer, you should create a separate Active Directory container for linked-clone desktops that is based on the OU for your View desktops. View administrators that have OU administrator privileges in Active Directory can provision linked-clone desktops without domain administrator privileges. If you change administrator credentials in Active Directory, you must also update the credential information in View Composer.

Creating OUs and Groups for Kiosk Mode Client Accounts

A client in kiosk mode is a thin client or a locked-down PC that runs View Client to connect to a View Connection Server instance and launch a remote desktop session. If you configure clients in kiosk mode, you should create dedicated OUs and groups in Active Directory for kiosk mode client accounts.

Creating dedicated OUs and groups for kiosk mode client accounts partitions client systems against unwarranted intrusion and simplifies client configuration and administration.

See the *VMware View Administration* document for more information.

Creating Groups for View Users

You should create groups for different types of View users in Active Directory. For example, you can create a group called VMware View Users for your View desktop users and another group called VMware View Administrators for users that will administer View desktops.

Creating a User Account for vCenter Server

You must create a user account in Active Directory to use with vCenter Server. You specify this user account when you add a vCenter Server instance in View Administrator.

The user account must be in the same domain as your View Connection Server host or in a trusted domain. If you use View Composer, you must add the user account to the local Administrators group on the vCenter Server computer.

You must give the user account privileges to perform certain operations in vCenter Server. If you use View Composer, you must give the user account additional privileges. See "Configuring User Accounts for vCenter Server and View Composer," on page 85 for information on configuring these privileges.

Create a User Account for View Composer

If you use View Composer, you must 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.

To ensure security, you should create a separate user account to use with View Composer. By creating a separate account, you can guarantee that it does not have additional privileges that are defined for another purpose. You can give the account the minimum privileges that it needs to create and remove computer objects in a specified Active Directory container. For example, the View Composer account does not require domain administrator privileges.

Procedure

1 In Active Directory, create a user account in the same domain as your View Connection Server host or in a trusted domain.

2 Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

   The following list shows all the required permissions for the user account, including permissions that are assigned by default:

   - List Contents
   - Read All Properties
   - Write All Properties
   - Read Permissions
   - Create Computer Objects
   - Delete Computer Objects

3 Make sure that the user account's permissions apply to the Active Directory container and to all child objects of the container.

What to do next

Specify the account in View Administrator when you configure View Composer for vCenter Server and when you configure and deploy linked-clone desktop pools.

Configure the Restricted Groups Policy

To be able to log in to a View desktop, users must belong to the local Remote Desktop Users group of the View desktop. You can use the Restricted Groups policy in Active Directory to add users or groups to the local Remote Desktop Users group of every View desktop that is joined to your domain.

The Restricted Groups policy sets the local group membership of computers in the domain to match the membership list settings defined in the Restricted Groups policy. The members of your View desktop users group are always added to the local Remote Desktop Users group of every View desktop that is joined to your domain. When adding new users, you need only add them to your View desktop users group.

Prerequisites

Create a group for View desktop users in your domain in Active Directory.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings**.

3 Right-click **Restricted Groups**, select **Add Group**, and add the Remote Desktop Users group.

4 Right-click the new restricted Remote Desktop Users group and add your View desktop users group to the group membership list.

5 Click **OK** to save your changes.

Using View Group Policy Administrative Template Files

View includes several component-specific group policy administrative (ADM) template files.

During View Connection Server installation, the View ADM template files are installed in the *install_directory*\VMware\VMware View\Server\Extras\GroupPolicyFiles directory on your View Connection Server host. You must copy these files to a directory on your Active Directory server.

You can optimize and secure View desktops by adding the policy settings in these files to a new or existing GPO in Active Directory and then linking that GPO to the OU that contains your View desktops.

See the *VMware View Administration* document for information on using View group policy settings.

Prepare Active Directory for Smart Card Authentication

You might need to perform certain tasks in Active Directory when you implement smart card authentication.

- Add UPNs for Smart Card Users on page 29

  Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users that use smart cards to authenticate in View must have a valid UPN.

- Add the Root Certificate to Trusted Root Certification Authorities on page 29

  If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

- Add an Intermediate Certificate to Intermediate Certification Authorities on page 30

  If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

- Add the Root Certificate to the Enterprise NTAuth Store on page 30

  If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Add UPNs for Smart Card Users

Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users that use smart cards to authenticate in View must have a valid UPN.

If the domain a smart card user resides in is different from the domain that your root certificate was issued from, you must set the user's UPN to the Subject Alternative Name (SAN) contained in the root certificate of the trusted CA. If your root certificate was issued from a server in the smart card user's current domain, you do not need to modify the user's UPN.

NOTE You might need to set the UPN for built-in Active Directory accounts, even if the certificate is issued from the same domain. Built-in accounts, including Administrator, do not have a UPN set by default.

Prerequisites

- Obtain the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.
- If the ADSI Edit utility is not present on your Active Directory server, download and install the appropriate Windows Support Tools from the Microsoft Web site.

Procedure

1 On your Active Directory server, start the ADSI Edit utility.

2 In the left pane, expand the domain the user is located in and double-click `CN=Users`.

3 In the right pane, right-click the user and then click **Properties**.

4 Double-click the `userPrincipalName` attribute and type the SAN value of the trusted CA certificate.

5 Click **OK** to save the attribute setting.

Add the Root Certificate to Trusted Root Certification Authorities

If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings\Public Key**.

3 Right-click **Trusted Root Certification Authorities** and select **Import**.

4 Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.

5 Close the Group Policy window.

All of the systems in the domain now have a copy of the root certificate in their trusted root store.

What to do next

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See "Add an Intermediate Certificate to Intermediate Certification Authorities," on page 30.

Add an Intermediate Certificate to Intermediate Certification Authorities

If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open the policy for **Windows Settings\Security Settings\Public Key**.

3 Right-click **Intermediate Certification Authorities** and select **Import**.

4 Follow the prompts in the wizard to import the intermediate certificate (for example, `intermediateCA.cer`) and click **OK**.

5 Close the Group Policy window.

All of the systems in the domain now have a copy of the intermediate certificate in their intermediate certification authority store.

Add the Root Certificate to the Enterprise NTAuth Store

If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

- On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAuth store.

  For example: **`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

The CA is now trusted to issue certificates of this type.

4 Installing View Composer

To use View Composer, you create a View Composer database, install the View Composer service, and optimize your View infrastructure to support View Composer. You can install the View Composer service on the same host as vCenter Server or on a separate host.

View Composer is an optional feature. Install View Composer if you intend to deploy linked-clone desktop pools.

You must have a license to install and use the View Composer feature.

This chapter includes the following topics:

Prepare a View Composer Database

You must create a database and data source name (DSN) to store View Composer data.

The View Composer service does not include a database. If a database instance does not exist in your network environment, you must install one. After you install a database instance, you add the View Composer database to the instance.

You can add the View Composer database to the instance on which the vCenter Server database is located. You can configure the database locally, or remotely, on a network-connected Linux, UNIX, or Windows Server computer.

The View Composer database stores information about connections and components that are used by View Composer:

- vCenter Server connections
- Active Directory connections
- Linked-clone desktops that are deployed by View Composer
- Replicas that are created by View Composer

Each instance of the View Composer service must have its own View Composer database. Multiple View Composer services cannot share a View Composer database.

For a list of supported database versions, see "Database Requirements for View Composer," on page 10.

To add a View Composer database to an installed database instance, choose one of these procedures.

- Create a SQL Server Database for View Composer on page 32

  View Composer can store linked-clone desktop information in a SQL Server database. You create a View Composer database by adding it to SQL Server and configuring an ODBC data source for it.

- Create an Oracle Database for View Composer on page 34

  View Composer can store linked-clone desktop information in an Oracle 11g or 10g database. You create a View Composer database by adding it to an existing Oracle instance and configuring an ODBC data source for it. You can add a new View Composer database by using the Oracle Database Configuration Assistant or by running a SQL statement.

Create a SQL Server Database for View Composer

View Composer can store linked-clone desktop information in a SQL Server database. You create a View Composer database by adding it to SQL Server and configuring an ODBC data source for it.

Add a View Composer Database to SQL Server

You can add a new View Composer database to an existing Microsoft SQL Server instance to store linked-clone data for View Composer.

If the database resides locally, on the system on which View Composer will be installed, you can use the Integrated Windows Authentication security model. If the database resides on a remote system, you cannot use this method of authentication.

Prerequisites

- Verify that a supported version of SQL Server is installed on the computer on which you will install View Composer or in your network environment. For details, see "Database Requirements for View Composer," on page 10.
- Verify that you use SQL Server Management Studio or SQL Server Management Studio Express to create and administer the data source. You can download and install SQL Server Management Studio Express from the following Web site.

  http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

Procedure

1. On the View Composer computer, select **Start > All Programs > Microsoft SQL Server 2008** or **Microsoft SQL Server 2005**.
2. Select **SQL Server Management Studio Express** and connect to the existing SQL Server instance for vSphere Management.
3. In the Object Explorer panel, right-click the Databases entry and select **New Database**.
4. In the New Database dialog box, type a name in the Database name text box.

   For example: **`viewComposer`**
5. Click **OK**.

   SQL Server Management Studio Express adds your database to the Databases entry in the Object Explorer panel.
6. Exit Microsoft SQL Server Management Studio Express.

What to do next

Follow the instructions in "Add an ODBC Data Source to SQL Server," on page 33.

Add an ODBC Data Source to SQL Server

After you add a View Composer database to SQL Server, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

When you configure an ODBC DSN for View Composer, secure the underlying database connection to an appropriate level for your environment. For information about securing database connections, see the SQL Server documentation.

If the underlying database connection uses SSL encryption, we recommend that you configure your database servers with SSL certificates signed by a trusted CA. If you use self-signed certificates, your database connections might be susceptible to man-in-the-middle attacks.

Prerequisites

Complete the steps described in "Add a View Composer Database to SQL Server," on page 32.

Procedure

1 On the computer on which View Composer will be installed, select **Start > Administrative Tools > Data Source (ODBC)**.

2 Select the **System DSN** tab.

3 Click **Add** and select **SQL Native Client** from the list.

4 Click **Finish**.

5 In the Create a New Data Source to SQL Server setup wizard, type a name and description of the View Composer database.

For example: **`ViewComposer`**

6 In the Server text box, type the SQL Server database name.

Use the form *host_name**server_name*, where *host_name* is the name of the computer and *server_name* is the SQL Server instance.

For example: **`VCHOST1\VIM_SQLEXP`**

7 Click **Next**.

8 Make sure that the **Connect to SQL Server to obtain default settings for the additional configuration options** check box is selected and select an authentication option.

Option	Description
Windows NT authentication	Select this option if you are using a local instance of SQL Server. This option is also known as trusted authentication. Windows NT authentication is supported only if SQL Server is running on the local computer.
SQL Server authentication	Select this option if you are using a remote instance of SQL Server. Windows NT authentication is not supported on remote SQL Server.

9 Click **Next**.

10 Select the **Change the default database to** check box and select the name of the View Composer database from the list.

For example: **`ViewComposer`**

11 If the SQL Server connection is configured with SSL enabled, navigate to the Microsoft SQL Server DSN Configuration page and select **Use strong encryption for data**.

12 Finish and close the Microsoft ODBC Data Source Administrator wizard.

What to do next

Install the new View Composer service. See "Install the View Composer Service," on page 37.

Create an Oracle Database for View Composer

View Composer can store linked-clone desktop information in an Oracle 11g or 10g database. You create a View Composer database by adding it to an existing Oracle instance and configuring an ODBC data source for it. You can add a new View Composer database by using the Oracle Database Configuration Assistant or by running a SQL statement.

- Add a View Composer Database to Oracle 11g or 10g on page 34

  You can use the Oracle Database Configuration Assistant to add a new View Composer database to an existing Oracle 11g or 10g instance.

- Use a SQL Statement to Add a View Composer Database to an Oracle Instance on page 35

  The View Composer database must have certain table spaces and privileges. You can use a SQL statement to create the View Composer database in an Oracle 11g or 10g database instance.

- Configure an Oracle Database User for View Composer on page 35

  By default, the database user that runs the View Composer database has Oracle system administrator permissions. To restrict the security permissions for the user that runs the View Composer database, you must configure an Oracle database user with specific permissions.

- Add an ODBC Data Source to Oracle 11g or 10g on page 36

  After you add a View Composer database to an Oracle 11g or 10g instance, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

Add a View Composer Database to Oracle 11g or 10g

You can use the Oracle Database Configuration Assistant to add a new View Composer database to an existing Oracle 11g or 10g instance.

Prerequisites

Verify that a supported version of Oracle 11g or 10g is installed on the local or remote computer. See "Database Requirements for View Composer," on page 10.

Procedure

1 Start the **Database Configuration Assistant** on the computer on which you are adding the View Composer database.

Database Version	Action
Oracle 11g	Select **Start > All Programs > Oracle-OraDb11g_home > Configuration and Migration Tools > Database Configuration Assistant**.
Oracle 10g	Select **Start > All Programs > Oracle-OraDb10g_home > Configuration and Migration Tools > Database Configuration Assistant**.

2 On the Operations page, select **Create a database**.

3 On the Database Templates page, select the **General Purpose or Transaction Processing** template.

4 On the Database Identification page, type a Global Database Name and an Oracle System Identifier (SID) prefix.

  For simplicity, use the same value for both items.

5 On the Management Options page, click **Next** to accept the default settings.

6 On the Database Credentials page, select **Use the Same Administrative Passwords for All Accounts** and type a password.

7 On the remaining configuration pages, click **Next** to accept the default settings.

8 On the Creation Options page, verify that **Create Database** is selected and click **Finish**.

9 On the Confirmation page, review the options and click **OK**.

The configuration tool creates the database.

10 On the Database Creation Complete page, click **OK**.

What to do next

Follow the instructions in "Add an ODBC Data Source to Oracle 11g or 10g," on page 36.

Use a SQL Statement to Add a View Composer Database to an Oracle Instance

The View Composer database must have certain table spaces and privileges. You can use a SQL statement to create the View Composer database in an Oracle 11g or 10g database instance.

When you create the database, you can customize the location of the data and log files.

Prerequisites

Verify that a supported version of Oracle 11g or 10g is installed on the local or remote computer. For details, see "Database Requirements for View Composer," on page 10.

Procedure

1 Log in to a SQL*Plus session with the system account.

2 Run the following SQL statement to create the database.

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

In this example, `VCMP` is the sample name of the View Composer database and `vcmp01.dbf` is the name of the database file.

For a Windows installation, use Windows conventions in the directory path to the `vcmp01.dbf` file.

What to do next

If you want to run the View Composer database with specific security permissions, follow the instructions in "Configure an Oracle Database User for View Composer," on page 35.

Follow the instructions in "Add an ODBC Data Source to Oracle 11g or 10g," on page 36

Configure an Oracle Database User for View Composer

By default, the database user that runs the View Composer database has Oracle system administrator permissions. To restrict the security permissions for the user that runs the View Composer database, you must configure an Oracle database user with specific permissions.

Prerequisites

Verify that a View Composer database was created in an Oracle 11g or 10g instance.

Procedure

1 Log in to a SQL*Plus session with the system account.

2 Run the following SQL command to create a View Composer database user with the correct permissions.

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
   grant connect to VCMPADMIN;
   grant resource to VCMPADMIN;
   grant create view to VCMPADMIN;
   grant create sequence to VCMPADMIN;
   grant create table to VCMPADMIN;
   grant create materialized view to VCMPADMIN;
   grant execute on dbms_lock to VCMPADMIN;
   grant execute on dbms_job to VCMPADMIN;
   grant unlimited tablespace to VCMPADMIN;
```

In this example, the user name is `VCMPADMIN` and the View Composer database name is `VCMP`.

By default the `resource` role has the `create procedure`, `create table`, and `create sequence` privileges assigned. If the `resource` role does not have these privileges, explicitly grant them to the View Composer database user.

Add an ODBC Data Source to Oracle 11g or 10g

After you add a View Composer database to an Oracle 11g or 10g instance, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

When you configure an ODBC DSN for View Composer, secure the underlying database connection to an appropriate level for your environment. For information about securing database connections, see the Oracle database documentation.

If the underlying database connection uses SSL encryption, we recommend that you configure your database servers with SSL certificates signed by a trusted CA. If you use self-signed certificates, your database connections might be susceptible to man-in-the-middle attacks.

Prerequisites

Verify that you completed the steps described in "Add a View Composer Database to Oracle 11g or 10g," on page 34 or "Use a SQL Statement to Add a View Composer Database to an Oracle Instance," on page 35.

Procedure

1 On the View Composer database computer, select **Start > Administrative Tools > Data Source (ODBC)**.

2 From the Microsoft ODBC Data Source Administrator wizard, select the **System DSN** tab.

3 Click **Add** and select the appropriate Oracle driver from the list.

For example: **`OraDb11g_home`**

4 Click **Finish**.

5 In the Oracle ODBC Driver Configuration dialog box, type a DSN to use with View Composer, a description of the data source, and a user ID to connect to the database.

If you configured an Oracle database user ID with specific security permissions, specify this user ID.

NOTE You use the DSN when you install the View Composer service.

6 Specify a **TNS Service Name** by selecting the Global Database Name from the drop-down menu.

The Oracle Database Configuration Assistant specifies the Global Database Name.

7 To verify the data source, click **Test Connection** and click **OK**.

What to do next

Install the new View Composer service. See "Install the View Composer Service," on page 37.

Configuring an SSL Certificate for View Composer

By default, a self-signed certificate is installed with View Composer. You can use the default certificate for testing purposes, but for production use you should replace it with a certificate that is signed by a Certificate Authority (CA).

You can configure a certificate before or after you install View Composer. In View 5.1 and later releases, you configure a certificate by importing it into the Windows local computer certificate store on the Windows Server computer where View Composer is, or will be, installed.

- If you import a CA-signed certificate before you install View Composer, you can select the signed certificate during the View Composer installation. This approach eliminates the manual task of replacing the default certificate after the installation.
- If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate after you install View Composer, you must import the new certificate and run the `SviConfig ReplaceCertificate` utility to bind your new certificate to the port used by View Composer.

For details about configuring SSL certificates and using the `SviConfig ReplaceCertificate` utility, see Configuring SSL Certificates for View Servers.

If you install vCenter Server and View Composer on the same Windows Server computer, they can use the same SSL certificate, but you must configure the certificate separately for each component.

Install the View Composer Service

To use View Composer, you must install the View Composer service. View Manager uses View Composer to create and deploy linked-clone desktops in vCenter Server.

You can install the View Composer service on the Windows Server computer on which vCenter Server is installed or on a separate Windows Server computer. A standalone View Composer installation works with vCenter Server installed on a Windows Server computer and with the Linux-based vCenter Server Appliance.

The View Composer software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a replica server, security server, View Connection Server, View Agent, View Client, or View Transfer Server.

Prerequisites

- Verify that your installation satisfies the View Composer requirements described in "View Composer Requirements," on page 9.
- Verify that you have a license to install and use View Composer.
- Verify that you have the DSN, domain administrator user name, and password that you provided in the ODBC Data Source Administrator wizard. You enter this information when you install the View Composer service.
- If you plan to configure an SSL certificate signed by a CA for View Composer during the installation, verify that your certificate is imported in the Windows local computer certificate store. See Configuring SSL Certificates for View Servers.
- Verify that no applications that run on the View Composer computer use Windows SSL libraries that require SSL version 2 (SSLv2) provided through the Microsoft Secure Channel (Schannel) security package. The View Composer installer disables SSLv2 on the Microsoft Schannel. Applications such as Tomcat, which uses Java SSL, or Apache, which uses OpenSSL, are not affected by this constraint.

- To run the View Composer installer, you must be a domain user with Administrator privileges on the system.

Procedure

1 Download the VMware View Composer installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

The installer filename is `VMware-viewcomposer-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number. This installer file installs the View Composer service on 64-bit Windows Server operating systems.

2 To start the View Composer installation program, right-click the installer file and select **Run as administrator**.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Type the DSN for the View Composer database that you provided in the Microsoft or Oracle ODBC Data Source Administrator wizard.

For example: **`VMware View Composer`**

NOTE If you did not configure a DSN for the View Composer database, click **ODBC DSN Setup** to configure a name now.

6 Type the domain administrator user name and password that you provided in the ODBC Data Source Administrator wizard.

If you configured an Oracle database user with specific security permissions, specify this user name.

7 Type a port number or accept the default value.

View Connection Server uses this port to communicate with the View Composer service.

8 Provide an SSL certificate.

Option	Action
Create default SSL certificate	Select this radio button to create a default SSL certificate for the View Composer service. After the installation, you can replace the default certificate with an SSL certificate signed by a CA.
Use an existing SSL certificate	Select this radio button if you installed a signed SSL certificate that you want to use for the View Composer service. Select an SSL certificate from the list.

9 Click **Install** and **Finish** to complete the View Composer service installation.

The VMware View Composer service starts.

View Composer uses the cryptographic cipher suites that are provided by the Windows Server operating system. You should follow your organization's guidelines for managing cipher suites on Windows Server systems. If your organization does not provide guidelines, VMware recommends that you disable weak cryptographic cipher suites on the View Composer server to enhance the security of your View environment. For information about managing cryptographic cipher suites, see your Microsoft documentation.

Configuring Your Infrastructure for View Composer

You can take advantage of features in vSphere, vCenter Server, Active Directory, and other components of your infrastructure to optimize the performance, availability, and reliability of View Composer.

Configuring the vSphere Environment for View Composer

To support View Composer, you should follow certain best practices when you install and configure vCenter Server, ESX/ESXi, and other vSphere components.

These best practices let View Composer work efficiently in the vSphere environment.

- After you create the path and folder information for linked-clone virtual machines, do not change the information in vCenter Server. Instead, use View Administrator to change the folder information.

  If you change this information in vCenter Server, View Manager cannot successfully look up the virtual machines in vCenter Server.
- Make sure that the vSwitch settings on the ESX/ESXi host are configured with enough ports to support the total number of virtual NICs that are configured on the linked-clone virtual machines that run on the ESX/ESXi host.
- When you deploy linked-clone desktops in a resource pool, make sure that your vSphere environment has enough CPU and memory to host the number of desktops that you require. Use vSphere Client to monitor CPU and memory usage in resource pools.
- A cluster that is used for View Composer linked clones can contain more than eight ESX/ESXi hosts, but you must store the replica disks on NFS datastores. On VMFS datastores, you can store replica disks only with clusters that contain at most eight ESX/ESXi hosts.
- Use vSphere DRS. DRS efficiently distributes linked-clone virtual machines among your hosts.

NOTE Storage vMotion is not supported for linked-clone desktops.

Additional Best Practices for View Composer

To make sure that View Composer works efficiently, check that your dynamic name service (DNS) operates correctly, and run antivirus software scans at staggered times.

By making sure that DNS resolution operates correctly, you can overcome intermittent issues caused by DNS errors. The View Composer service relies on dynamic name resolution to communicate with other computers. To test DNS operation, ping the Active Directory and View Connection Server computers by name.

If you stagger the run times for your antivirus software, performance of the linked-clone desktops is not affected. If the antivirus software runs in all linked clones at the same time, excessive I/O operations per second (IOPS) occur in your storage subsystem. This excessive activity can affect performance of the linked-clone desktops.

Installing View Connection Server 5

To use View Connection Server, you install the software on supported computers, configure the required components, and, optionally, optimize the components.

This chapter includes the following topics:

Installing the View Connection Server Software

Depending on the performance, availability, and security needs of your View deployment, you can install a single instance of View Connection Server, replicated instances of View Connection Server, and security servers. You must install at least one instance of View Connection Server.

When you install View Connection Server, you select a type of installation.

Standard installation	Generates a View Connection Server instance with a new View LDAP configuration.
Replica installation	Generates a View Connection Server instance with a View LDAP configuration that is copied from an existing instance.
Security server installation	Generates a View Connection Server instance that adds an additional layer of security between the Internet and your internal network.

Installation Prerequisites for View Connection Server

Before you install View Connection Server, you must verify that your installation environment satisfies specific prerequisites.

- View Connection Server requires a valid license key for View Manager. The following license keys are available:
  - View Manager
  - View Manager with View Composer and Local Mode
- You must join the View Connection Server host to an Active Directory domain. View Connection Server supports the following versions of Active Directory:
  - Windows 2003 Active Directory
  - Windows 2008 Active Directory

  The View Connection Server host must not be a domain controller.

  NOTE View Connection Server does not make, nor does it require, any schema or configuration updates to Active Directory.
- Do not install View Connection Server on systems that have the Windows Terminal Server role installed. You must remove the Windows Terminal Server role from any system on which you install View Connection Server.
- Do not install View Connection Server on a system that performs any other functions or roles. For example, do not use the same system to host vCenter Server.
- The system on which you install View Connection Server must have a static IP address.
- To run the View Connection Server installer, you must use a domain user account with Administrator privileges on the system.
- When you install View Connection Server, you authorize a View Administrators account. You can specify the local Administrators group or a domain user or group account. View assigns full View Administration rights, including the right to install replicated View Connection Server instances, to this account only. If you specify a domain user or group, you must create the account in Active Directory before you run the installer.

Install View Connection Server with a New Configuration

To install View Connection Server as a single server or as the first instance in a group of replicated View Connection Server instances, you use the standard installation option.

When you select the standard installation option, the installation creates a new, local View LDAP configuration. The installation loads the schema definitions, Directory Information Tree (DIT) definition, and ACLs and initializes the data.

After installation, you manage most View LDAP configuration data by using View Administrator. View Connection Server automatically maintains some View LDAP entries.

The View Connection Server software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a replica server, security server, View Composer, View Agent, View Client, or View Transfer Server.

When you install View Connection Server with a new configuration, you can participate in a customer experience improvement program. VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. No data that identifies your organization is collected. You can choose not to participate by deselecting this option during the installation. If you change your mind about

participating after the installation, you can either join or withdraw from the program by editing the Product Licensing and Usage page in View Administrator. To review the list of fields from which data is collected, including the fields that are made anonymous, see "Information Collected by the Customer Experience Improvement Program" in the *VMware View Administration* document.

Prerequisites

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install View Connection Server.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 42.
- If you intend to authorize a domain user or group as the View Administrators account, verify that you created the domain account in Active Directory.
- Prepare a data recovery password. When you back up View Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup View configuration, you must provide the data recovery password. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.

  IMPORTANT You will need the data recovery password to keep View operating and avoid downtime in a Business Continuity and Disaster Recovery (BCDR) scenario. You can provide a password reminder with the password when you install View Connection Server.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 58.
- If you plan to pair a security server with this View Connection Server instance, verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- If your network topology includes a back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 59.

Procedure

1. Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

   The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2. To start the View Connection Server installation program, double-click the installer file.
3. Accept the VMware license terms.
4. Accept or change the destination folder.
5. Select the **View Standard Server** installation option.
6. Type a data recovery password and, optionally, a password reminder.

7 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

8 Authorize a View Administrators account.

Only members of this account can log in to View Administrator, exercise full View administration rights, and install replicated View Connection Server instances and other View servers.

Option	Description
Authorize the local Administrators group	Allows users in the local Administrators group to administer View.
Authorize a specific domain user or domain group	Allows the specified domain user or group to administer View.

9 If you specified a domain View Administrators account, and you are running the installer as a local administrator or another user without access to the domain account, provide credentials to log in to the domain with an authorized user name and password.

Use *domain name**user name* or user principal name (UPN) format. UPN format can be *user@domain.com*.

10 Choose whether to participate in the customer experience improvement program.

If you participate, you can optionally select the type, size, and location of your organization.

11 Complete the installation wizard to finish installing View Connection Server.

12 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The VMware View services are installed on the Windows Server computer:

- VMware View Connection Server
- VMware View Framework Component
- VMware View Message Bus Component
- VMware View Script Host
- VMware View Security Gateway Component
- VMware View PCoIP Secure Gateway
- VMware View Web Component
- VMware VDMDS, which provides View LDAP directory services

For information about these services, see the *VMware View Administration* document.

What to do next

Configure SSL server certificates for View Connection Server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 71.

Perform initial configuration on View Connection Server. See Chapter 8, "Configuring View for the First Time," on page 85.

If you plan to include replicated View Connection Server instances and security servers in your deployment, you must install each server instance by running the View Connection Server installer file.

If you are reinstalling View Connection Server on a Windows Server 2008 operating system and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install View Connection Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to perform a standard installation of View Connection Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

With silent installation, you can efficiently deploy View components in a large enterprise.

Prerequisites

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install View Connection Server.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 42.
- If you intend to authorize a domain user or group as the View Administrators account, verify that you created the domain account in Active Directory.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 58.
- If you plan to pair a security server with this View Connection Server instance, verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- If your network topology includes a back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 59.
- Verify that the Windows computer on which you install View Connection Server has version 2.0 or later of the MSI runtime engine. For details, see the Microsoft Web site.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 59.
- Familiarize yourself with the silent installation properties available with a standard installation of View Connection Server. See "Silent Installation Properties for a View Connection Server Standard Installation," on page 46.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

  The installer filename is `VMware-viewconnectionserver-x86_64-`*`y.y.y`*`-`*`xxxxxx`*`.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

IMPORTANT When you perform a silent installation, the full command line, including the data recovery password, is logged in the installer's `vminst.log` file. After the installation is complete, either delete this log file or change the data recovery password by using View Administrator.

4 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The VMware View services are installed on the Windows Server computer. For details, see "Install View Connection Server with a New Configuration," on page 42.

What to do next

Configure SSL server certificates for View Connection Server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 71.

If you are configuring View for the first time, perform initial configuration on View Connection Server. See Chapter 8, "Configuring View for the First Time," on page 85.

Silent Installation Properties for a View Connection Server Standard Installation

You can include specific View Connection Server properties when you perform a silent installation from the command line. You must use a *PROPERTY=value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 5-1. MSI Properties for Silently Installing View Connection Server in a Standard Installation

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path.	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation For example, to perform a standard installation, define `VDM_SERVER_INSTANCE_TYPE=1`	1
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1`	1
VDM_INITIAL_ADMIN_SID	The SID of the initial View Administrators user or group that is authorized with full administration rights in View. The default value is the SID of the local Administrators group on the View Connection Server computer. You can specify a SID of a domain user or group account.	`S-1-5-32-544`

Table 5-1. MSI Properties for Silently Installing View Connection Server in a Standard Installation (Continued)

MSI Property	Description	Default Value
VDM_SERVER_RECOVERY_PWD	The data recovery password. If a data recovery password is not set in View LDAP, this property is mandatory. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.	None
VDM_SERVER_RECOVERY_PWD_REMINDER	The data recovery password reminder. This property is optional.	None

Install a Replicated Instance of View Connection Server

To provide high availability and load balancing, you can install one or more additional instances of View Connection Server that replicate an existing View Connection Server instance. After a replica installation, the existing and newly installed instances of View Connection Server are identical.

When you install a replicated instance, View Manager copies the View LDAP configuration data from the existing View Connection Server instance.

After the installation, the View Manager software maintains identical View LDAP configuration data on all View Connection Server instances in the replicated group. When a change is made on one instance, the updated information is copied to the other instances.

If a replicated instance fails, the other instances in the group continue to operate. When the failed instance resumes activity, its configuration is updated with the changes that took place during the outage.

NOTE Replication functionality is provided by View LDAP, which uses the same replication technology as Active Directory.

The replica server software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a security server, View Connection Server, View Composer, View Agent, View Client, or View Transfer Server.

Prerequisites

- Verify that at least one View Connection Server instance is installed and configured on the network.
- To install the replicated instance, you must log in as a user with the View Administrators role. You specify the account or group with the View Administrators role when you install the first instance of View Connection Server. The role can be assigned to the local Administrators group or a domain user or group. See "Install View Connection Server with a New Configuration," on page 42.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have View Administrator privileges on the Windows Server computer where the existing instance is installed.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Verify that the computers on which you install replicated View Connection Server instances are connected over a high-performance LAN. See "Network Requirements for Replicated View Connection Server Instances," on page 8.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 42.
- If you install a replicated View Connection Server instance that is View 5.1 or later, and the existing View Connection Server instance you are replicating is View 5.0.*x* or earlier, prepare a data recovery password. See "Install View Connection Server with a New Configuration," on page 42.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 58.
- If you plan to pair a security server with this View Connection Server instance, verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- If your network topology includes a back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 59.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2 To start the View Connection Server installation program, double-click the installer file.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Select the **View Replica Server** installation option.

6 Enter the host name or IP address of the existing View Connection Server instance you are replicating.

7 Type a data recovery password and, optionally, a password reminder.

You are prompted for a data recovery password only if the existing View Connection Server instance you are replicating is View 5.0.*x* or earlier.

8 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

9 Complete the installation wizard to finish installing the replicated instance.

10 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The VMware View services are installed on the Windows Server computer:

- VMware View Connection Server
- VMware View Framework Component
- VMware View Message Bus Component
- VMware View Script Host
- VMware View Security Gateway Component
- VMware View PCoIP Secure Gateway

- VMware View Web Component
- VMware VDMDS, which provides View LDAP directory services

For information about these services, see the *VMware View Administration* document.

What to do next

Configure an SSL server certificate for the View Connection Server instance. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 71.

You do not have to perform an initial View configuration on a replicated instance of View Connection Server. The replicated instance inherits its configuration from the existing View Connection Server instance.

However, you might have to configure client connection settings for this View Connection Server instance, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 97 and Sizing Windows Server Settings to Support Your Deployment.

If you are reinstalling View Connection Server on a Windows Server 2008 operating system and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install a Replicated Instance of View Connection Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install a replicated instance of View Connection Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

With silent installation, you can efficiently deploy View components in a large enterprise.

Prerequisites

- Verify that at least one View Connection Server instance is installed and configured on the network.
- To install the replicated instance, you must log in as a user with credentials to access the View Administrators account. You specify the View Administrators account when you install the first instance of View Connection Server. The account can be the local Administrators group or a domain user or group account. See "Install View Connection Server with a New Configuration," on page 42.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have View Administrator privileges on the Windows Server computer where the existing instance is installed.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Verify that the computers on which you install replicated View Connection Server instances are connected over a high-performance LAN. See "Network Requirements for Replicated View Connection Server Instances," on page 8.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 42.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 58.
- If you plan to pair a security server with this View Connection Server instance, verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- If your network topology includes a back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 59.

- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 59.
- Familiarize yourself with the silent installation properties available with a replica installation of View Connection Server. See "Silent Installation Properties for a Replicated Instance of View Connection Server," on page 51.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

   The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

   For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"`

   If you install a replicated View Connection Server instance that is View 5.1 or later, and the existing View Connection Server instance you are replicating is View 5.0.*x* or earlier, you must specify a data recovery password, and you can add a password reminder. For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

   IMPORTANT When you perform a silent installation, the full command line, including the data recovery password, is logged in the installer's `vminst.log` file. After the installation is complete, either delete this log file or change the data recovery password by using View Administrator.

4 Check for new patches on the Windows Server computer and run Windows Update as needed.

   Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The VMware View services are installed on the Windows Server computer. For details, see "Install a Replicated Instance of View Connection Server," on page 47.

What to do next

Configure an SSL server certificate for the View Connection Server instance. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 71.

You do not have to perform an initial View configuration on a replicated instance of View Connection Server. The replicated instance inherits its configuration from the existing View Connection Server instance.

However, you might have to configure client connection settings for this View Connection Server instance, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 97 and Sizing Windows Server Settings to Support Your Deployment.

Silent Installation Properties for a Replicated Instance of View Connection Server

You can include specific properties when you silently install a replicated View Connection Server instance from the command line. You must use a *PROPERTY=value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 5-2. MSI Properties for Silently installing a Replicated Instance of View Connection Server

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation To install a replicated instance, define `VDM_SERVER_INSTANCE_TYPE=2` This MSI property is required when installing a replica.	1
ADAM_PRIMARY_NAME	The host name or IP address of the existing View Connection Server instance you are replicating. For example: `ADAM_PRIMARY_NAME=cs1.companydomain.com` This MSI property is required.	None
ADAM_PRIMARY_PORT	The View LDAP port of the existing View Connection Server instance you are replicating. For example: `ADAM_PRIMARY_PORT=cs1.companydomain.com` This MSI property is optional.	None
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1` This MSI property is optional.	1
VDM_SERVER_RECOVERY_PWD	The data recovery password. If a data recovery password is not set in View LDAP, this property is mandatory. **NOTE** The data recover password is not set in View LDAP if the standard View Connection Server instance you are replicating is View 5.0 or earlier. If the View Connection Server instance you are replicating is View 5.1 or later, you do not have to provide this property. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.	None
VDM_SERVER_RECOVERY_PWD_REMINDER	The data recovery password reminder. This property is optional.	None

Configure a Security Server Pairing Password

Before you can install a security server, you must configure a security server pairing password. The View Connection Server installation program prompts you for this password during the installation process.

The security server pairing password is a one-time password that permits a security server to be paired with a View Connection Server instance. The password becomes invalid after you provide it to the View Connection Server installation program.

NOTE You cannot pair an older version of security server with the current version of View Connection Server. If you configure a pairing password on the current version of View Connecton Server and try to install an older version of security server, the pairing password will be invalid.

Procedure

1 In View Administrator, select **View Configuration > Servers**.

2 In the View Servers pane, select the View Connection Server instance to pair with the security server.

3 From the **More Commands** drop-down menu, select **Specify Security Server Pairing Password**.

4 Type the password in the Pairing password and Confirm password text boxes and specify a password timeout value.

You must use the password within the specified timeout period.

5 Click **OK** to configure the password.

What to do next

Install a security server. See "Install a Security Server," on page 52.

IMPORTANT If you do not provide the security server pairing password to the View Connection Server installation program within the password timeout period, the password becomes invalid and you must configure a new password.

Install a Security Server

A security server is an instance of View Connection Server that adds an additional layer of security between the Internet and your internal network. You can install one or more security servers to be connected to a View Connection Server instance.

The security server software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a replica server, View Connection Server, View Composer, View Agent, View Client, or View Transfer Server.

Prerequisites

- Determine the type of topology to use. For example, determine which load balancing solution to use. Decide if the View Connection Server instances that are paired with security servers will be dedicated to users of the external network. For information, see the *VMware View Architecture Planning* document.

  IMPORTANT If you use a load balancer, you must have static IP addresses for the load balancer and each security server. For example, if you use a load balancer with two security servers, you need 3 static IP addresses.

- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.

- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 42.
- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running View Connection Server 4.6 or later. You cannot pair a View 4.6 or later security server with an older version of View Connection Server.
- Verify that the View Connection Server instance to be paired with the security server is accessible to the computer on which you plan to install the security server.
- Configure a security server pairing password. See "Configure a Security Server Pairing Password," on page 52.
- Familiarize yourself with the format of external URLs. See "Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections," on page 98.
- Verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for a security server. See "Firewall Rules for View Connection Server," on page 58.
- If your network topology includes a back-end firewall between the security server and View Connection Server, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 59.
- If you are upgrading or reinstalling the security server, verify that the existing IPsec rules for the security server were removed. See "Prepare to Upgrade or Reinstall a Security Server," on page 57.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2 To start the View Connection Server installation program, double-click the installer file.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Select the **View Security Server** installation option.

6 Type the fully qualified domain name or IP address of the View Connection Server instance to pair with the security server in the **Server** text box.

The security server forwards network traffic to this View Connection Server instance.

7 Type the security server pairing password in the Password text box.

If the password has expired, you can use View Administrator to configure a new password and type the new password in the installation program.

8 In the **External URL** text box, type the external URL of the security server for View Clients that use the RDP or PCoIP display protocols.

The URL must contain the protocol, client-resolvable security server name, and port number. Tunnel clients that run outside of your network use this URL to connect to the security server.

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

9 In the **PCoIP External URL** text box, type the external URL of the security server for View Clients that use the PCoIP display protocol.

Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach the security server. You can type into the text box only if a PCoIP Secure Gateway is installed on the security server.

10 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

11 Complete the installation wizard to finish installing the security server.

The security server services are installed on the Windows Server computer:

- VMware View Security Server
- VMware View Framework Component
- VMware View Security Gateway Component
- VMware View PCoIP Secure Gateway

For information about these services, see *VMware View Administration*.

The security server appears in the Security Servers pane in View Administrator.

NOTE If the installation is cancelled or aborted, you might have to remove IPsec rules for the security server before you can begin the installation again. Take this step even if you already removed IPsec rules prior to reinstalling or upgrading security server. For instructions on removing IPsec rules, see "Prepare to Upgrade or Reinstall a Security Server," on page 57.

What to do next

Configure an SSL server certificate for the security server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 71.

You might have to configure client connection settings for the security server, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 97 and Sizing Windows Server Settings to Support Your Deployment.

If you are reinstalling the security server on a Windows Server 2008 operating system and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install a Security Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install a security server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

With silent installation, you can efficiently deploy View components in a large enterprise.

Prerequisites

- Determine the type of topology to use. For example, determine which load balancing solution to use. Decide if the View Connection Server instances that are paired with security servers will be dedicated to users of the external network. For information, see the *VMware View Architecture Planning* document.

  IMPORTANT If you use a load balancer, you must have static IP addresses for the load balancer and each security server. For example, if you use a load balancer with two security servers, you need 3 static IP addresses.

- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 42.
- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running View Connection Server 4.6 or later. You cannot pair a View 4.6 or later security server with an older version of View Connection Server.
- Verify that the View Connection Server instance to be paired with the security server is accessible to the computer on which you plan to install the security server.
- Configure a security server pairing password. See "Configure a Security Server Pairing Password," on page 52.
- Familiarize yourself with the format of external URLs. See "Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections," on page 98.
- Verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for a security server. See "Firewall Rules for View Connection Server," on page 58.
- If your network topology includes a back-end firewall between the security server and View Connection Server, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 59.
- If you are upgrading or reinstalling the security server, verify that the existing IPsec rules for the security server were removed. See "Prepare to Upgrade or Reinstall a Security Server," on page 57.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 59.
- Familiarize yourself with the silent installation properties available with a security server. See "Silent Installation Properties for a Security Server," on page 56.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

  The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3 VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172 VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_PWD=secret"`

The VMware View services are installed on the Windows Server computer. For details, see "Install a Security Server," on page 52.

NOTE If the installation is cancelled or aborted, you might have to remove IPsec rules for the security server before you can begin the installation again. Take this step even if you already removed IPsec rules prior to reinstalling or upgrading security server. For instructions on removing IPsec rules, see "Prepare to Upgrade or Reinstall a Security Server," on page 57.

What to do next

Configure an SSL server certificate for the security server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 71.

You might have to configure client connection settings for the security server, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 97 and Sizing Windows Server Settings to Support Your Deployment.

Silent Installation Properties for a Security Server

You can include specific properties when you silently install a security server from the command line. You must use a *PROPERTY=value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 5-3. MSI Properties for Silently Installing a Security Server

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation To install a security server, define `VDM_SERVER_INSTANCE_TYPE=3` This MSI property is required when installing a security server.	1
VDM_SERVER_NAME	The host name or IP address of the existing View Connection Server instance to pair with the security server. For example: `VDM_SERVER_NAME=cs1.internaldomain.com` This MSI property is required.	None
VDM_SERVER_SS_EXTURL	The external URL of the security server. The URL must contain the protocol, externally resolvable security server name, and port number For example: `VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443` This MSI property is required.	None

Table 5-3. MSI Properties for Silently Installing a Security Server (Continued)

MSI Property	Description	Default Value
VDM_SERVER_SS_PWD	The security server pairing password. For example: `VDM_SERVER_SS_PWD=secret` This MSI property is required.	None
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1` This MSI property is optional.	1
VDM_SERVER_SS_PCOIP_IP ADDR	The PCoIP Secure Gateway external IP address. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: `VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40` This property is required if you plan to use the PCoIP Secure Gateway component.	None
VDM_SERVER_SS_PCOIP_T CPPORT	The PCoIP Secure Gateway external TCP port number. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: `VDM_SERVER_SS_PCOIP_TCPPORT=4172` This property is required if you plan to use the PCoIP Secure Gateway component.	None
VDM_SERVER_SS_PCOIP_U DPPORT	The PCoIP Secure Gateway external UDP port number. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: `VDM_SERVER_SS_PCOIP_UDPPORT=4172` This property is required if you plan to use the PCoIP Secure Gateway component.	None

Prepare to Upgrade or Reinstall a Security Server

Before you can upgrade or reinstall a View 5.1 security server instance, you must remove the current IPsec rules that govern communication between the security server and its paired View Connection Server instance. If you do not take this step, the upgrade or reinstallation fails.

IMPORTANT This task pertains to View 5.1 and later security servers. If does not apply to View 5.0.x and earlier security servers.

By default, communication between a security server and its paired View Connection Server instance is governed by IPsec rules. When you upgrade or reinstall the security server and pair it again with the View Connection Server instance, a new set of IPsec rules must be established. If the existing IPsec rules are not removed before you upgrade or reinstall, the pairing fails.

You must take this step when you upgrade or reinstall a security server and are using IPsec to protect communication between the security server and View Connection Server.

You can configure an initial security server pairing without using IPsec rules. Before you install the security server, you can open View Administrator and deselect the Global Setting, **Use IPSec for Security Server Connections**, which is enabled by default. If IPsec rules are not in effect, you do not have to remove them before you upgrade or reinstall.

NOTE You do not have to remove a security server from View before you upgrade or reinstall the security server. Take this step only if you intend to remove security server permanently from the View environment.

Before View 5.1, you could remove security server in View Administrator or with the `vdmadmin -S` command. In View 5.1 and later releases, you can only use `vdmadmin -S`. See "Removing the Entry for a View Connection Server Instance or Security Server Using the -S Option" in the *VMware View Administration* document.

CAUTION If you remove the IPsec rules for an active security server, all communication with the security server is lost until you upgrade or reinstall the security server.

Procedure

1 In View Administrator, click **View Configuration > Servers**.

2 In the Security Servers tab, click **More Commands > Prepare for Upgrade or Reinstallation**.

If you disabled IPsec rules before you installed the security server, this setting is inactive. In this case, you do not have to remove IPsec rules before you reinstall or upgrade.

3 Click **OK**.

The IPsec rules are removed and the **Prepare for Upgrade or Reinstallation** setting becomes inactive, indicating that you can reinstall or upgrade the security server.

What to do next

Upgrade or reinstall security server.

Firewall Rules for View Connection Server

Certain ports must be opened on the firewall for View Connection Server instances and security servers.

When you install View Connection Server, the installation program can optionally configure the required Windows firewall rules for you.

Table 5-4. Ports Opened During View Connection Server Installation

Protocol	Ports	View Connection Server Instance Type
JMS	TCP 4001 in	Standard and replica
JMSIR	TCP 4100 in	Standard and replica
AJP13	TCP 8009 in	Standard and replica
HTTP	TCP 80 in	Standard, replica, and security server
HTTPS	TCP 443 in	Standard, replica, and security server
PCoIP	TCP 4172 in; UDP 4172 both directions	Standard, replica, and security server

Configuring a Back-End Firewall to Support IPsec

If your network topology includes a back-end firewall between security servers and View Connection Server instances, you must configure certain protocols and ports on the firewall to support IPsec. Without proper configuration, data sent between a security server and View Connection Server instance will fail to pass through the firewall.

By default, IPsec rules govern the connections between security servers and View Connection Server instances. To support IPsec, the View Connection Server installer can configure Windows firewall rules on the Windows Server hosts where View servers are installed. For a back-end firewall, you must configure the rules yourself.

NOTE It is highly recommended that you use IPsec. As an alternative, you can disable the View Administrator global setting, **Use IPsec for Security Server Connections**.

The following rules must allow bidirectional traffic. You might have to specify separate rules for inbound and outbound traffic on your firewall.

Different rules apply to firewalls that use network address translation (NAT) and those that do not use NAT.

Table 5-5. Non-NAT Firewall Requirements to Support IPsec Rules

Source	Protocol	Port	Destination	Notes
Security server	ISAKMP	UDP 500	View Connection Server	Security servers use UDP port 500 to negotiate IPsec security.
Security server	ESP	N/A	View Connection Server	ESP protocol encapsulates IPsec encrypted traffic. You do not have to specify a port for ESP as part of the rule. If necessary, you can specify source and destination IP addresses to reduce the scope of the rule.

The following rules apply to firewalls that use NAT.

Table 5-6. NAT Firewall Requirements to Support IPsec Rules

Source	Protocol	Port	Destination	Notes
Security server	ISAKMP	UDP 500	View Connection Server	Security servers use UDP port 500 to initiate IPsec security negotiation.
Security server	NAT-T ISAKMP	UDP 4500	View Connection Server	Security servers use UDP port 4500 to traverse NATs and negotiate IPsec security.

Microsoft Windows Installer Command-Line Options

To install View components silently, you must use Microsoft Windows Installer (MSI) command-line options and properties. The View component installers are MSI programs and use standard MSI features. You can also use MSI command-line options to uninstall View components silently.

For details about MSI, see the Microsoft Web site. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library Web site and search for MSI command-line options. To see MSI command-line usage, you can open a command prompt on the View component computer and type `msiexec /?`.

To run a View component installer silently, you begin by disabling the bootstrap program that extracts the installer into a temporary directory and starts an interactive installation.

Table 5-7 shows the command-line options that control the installer's bootstrap program.

Table 5-7. Command-Line Options for a View Component's Bootstrap Program

Option	Description
`/s`	Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs. For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` The `/s` option is required to run a silent installation. In the examples, *xxxxxx* is the build number and *y.y.y* is the version number.
`/v"`*`MSI_command_line_options`*`"`	Instructs the installer to pass the double-quote-enclosed string that you enter at the command line as a set of options for MSI to interpret. You must enclose your command-line entries between double quotes. Place a double quote after the `/v` and at the end of the command line. For example: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"`*`command_line_options`*`"` To instruct the MSI installer to interpret a string that contains spaces, enclose the string in two sets of double quotes. For example, you might want to install the View component in an installation path name that contains spaces. For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"`*`command_line_options`*` INSTALLDIR=""d:\abc\my folder"""` In this example, the MSI installer passes on the installation-directory path and does not attempt to interpret the string as two command-line options. Note the final double quote that encloses the entire command line. The `/v"`*`command_line_options`*`"` option is required to run a silent installation.

You control the remainder of a silent installation by passing command-line options and MSI property values to the MSI installer, `msiexec.exe`. The MSI installer includes the View component's installation code. The installer uses the values and options that you enter in the command line to interpret installation choices and setup options that are specific to the View component.

Table 5-8 shows the command-line options and MSI property values that are passed to the MSI installer.

Table 5-8. MSI Command-Line Options and MSI Properties

MSI Option or Property	Description
`/qn`	Instructs the MSI installer not to display the installer wizard pages. For example, you might want to install View Agent silently and use only default setup options and features: `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"` In the examples, *xxxxxx* is the build number and *y.y.y* is the version number. Alternatively, you can use the `/qb` option to display the wizard pages in a noninteractive, automated installation. As the installation proceeds, the wizard pages are displayed, but you cannot respond to them. The `/qn` or `/qb` option is required to run a silent installation.
`INSTALLDIR`	Specifies an alternative installation path for the View component. Use the format *`INSTALLDIR=path`* to specify an installation path. You can ignore this MSI property if you want to install the View component in the default path. This MSI property is optional.

Table 5-8. MSI Command-Line Options and MSI Properties (Continued)

MSI Option or Property	Description
ADDLOCAL	Determines the component-specific features to install. In an interactive installation, the View installer displays custom setup options to select. The MSI property, ADDLOCAL, lets you specify these setup options on the command line. To install all available custom setup options, enter ADDLOCAL=ALL. For example: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" If you do not use the MSI property, ADDLOCAL, the default setup options are installed. To specify individual setup options, enter a comma-separated list of setup option names. Do not use spaces between names. Use the format *ADDLOCAL=value,value,value...*. For example, you might want to install View Agent in a guest operating system with the View Composer Agent and PCoIP features: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" NOTE The Core feature is required in View Agent. This MSI property is optional.
REBOOT	You can use the REBOOT=ReallySuppress option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.
/l*v *log_file*	Writes logging information into the specified log file with verbose output. For example: /l*v ""%TEMP%\vmmsi.log"" This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The /l*v option is optional.

Uninstalling View Products Silently by Using MSI Command-Line Options

You can uninstall View components by using Microsoft Windows Installer (MSI) command-line options.

Syntax

```
msiexec.exe
/qb
/x
product_code
```

Options

The /qb option displays the uninstall progress bar. To suppress displaying the uninstall progress bar, replace the /qb option with the /qn option.

The /x option uninstalls the View component.

The *product_code* string identifies the View component product files to the MSI uninstaller. You can find the *product_code* string by searching for ProductCode in the %TEMP%\vmmsi.log file that is created during the installation.

For information about MSI command-line options, see "Microsoft Windows Installer Command-Line Options," on page 59.

Examples

Uninstall a View Connection Server instance.

```
msiexec.exe /qb /x {D6184123-57B7-26E2-809B-090435A8C16A}
```

Installing View Transfer Server 6

View Transfer Server transfers data between local desktops and the datacenter during check in, check out, and replication. To install View Transfer Server, you install the software on a Windows Server virtual machine, add View Transfer Server to your View Manager deployment, and configure the Transfer Server repository.

You must install and configure View Transfer Server if you deploy View Client with Local Mode on client computers.

You must have a license to install View Transfer Server and use local desktops.

1 Install View Transfer Server on page 63

View Transfer Server downloads system-image files, synchronizes data between local desktops and the corresponding remote desktops in the datacenter, and transfers data when users check in and check out local desktops. You install View Transfer Server in a virtual machine that runs Windows Server.

2 Add View Transfer Server to View Manager on page 65

View Transfer Server works with View Connection Server to transfer files and data between local desktops and the datacenter. Before View Transfer Server can perform these tasks, you must add it to your View Manager deployment.

3 Configure the Transfer Server Repository on page 66

The Transfer Server repository stores View Composer base images for linked-clone desktops that run in local mode. To give View Transfer Server access to the Transfer Server repository, you must configure it in View Manager. If you do not use View Composer linked clones in local mode, you do not have to configure a Transfer Server repository.

4 Firewall Rules for View Transfer Server on page 67

Certain incoming TCP ports must be opened on the firewall for View Transfer Server instances.

5 Installing View Transfer Server Silently on page 67

You can install View Transfer Server silently by typing the installer filename and installation options at the command line. With silent installation, you can efficiently deploy View components in a large enterprise.

Install View Transfer Server

View Transfer Server downloads system-image files, synchronizes data between local desktops and the corresponding remote desktops in the datacenter, and transfers data when users check in and check out local desktops. You install View Transfer Server in a virtual machine that runs Windows Server.

At runtime, View Transfer Server is deployed to an Apache Web Server. When you install View Transfer Server, the installer configures Apache Web Server as a service on the virtual machine. The Apache service uses ports 80 and 443.

Prerequisites

- Verify that you have local administrator privileges on the Windows Server on which you will install View Transfer Server.
- Verify that your installation satisfies the View Transfer Server requirements described in "View Transfer Server Requirements," on page 11.
- Verify that you did not manually add or remove PCI devices on the virtual machine on which you plan to install View Transfer Server. If you add or remove PCI devices, View might be unable to discover hot-added devices, which might cause data transfer operations to fail.
- Verify that you have a license to install View Transfer Server and use local desktops.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Transfer Server," on page 67.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2 To start the installation program, double-click the installer file.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Select **View Transfer Server**.

6 Configure the Apache Web Server to which View Transfer Server is deployed.

You can accept the default values for the network domain, Apache Server name, and administrator's email address that are provided by the installer.

7 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually.

8 Complete the installation program to install View Transfer Server.

The VMware View Transfer Server, View Transfer Server Control Service, and VMware View Framework Component services are installed and started on the virtual machine.

What to do next

In View Administrator, add View Transfer Server to your View Manager deployment.

Add View Transfer Server to View Manager

View Transfer Server works with View Connection Server to transfer files and data between local desktops and the datacenter. Before View Transfer Server can perform these tasks, you must add it to your View Manager deployment.

You can add multiple View Transfer Server instances to View Manager. The View Transfer Server instances access one common Transfer Server repository. They share the transfer workload for the local desktops that are managed by a View Connection Server instance or by a group of replicated View Connection Server instances.

NOTE When View Transfer Server is added to View Manager, its Distributed Resource Scheduler (DRS) automation policy is set to Manual, which effectively disables DRS.

Prerequisites

- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that vCenter Server is added to View Manager. The **View Configuration > Servers** page in View Administrator displays vCenter Server instances that are added to View Manager.
- If View Transfer Server is version 5.1 or later, and you plan to use linked-clone desktops in local mode, verify that all replicated View Connection Server instances in the View configuration are version 5.1 or later. If an earlier version of View Connection Server sends a request to publish a base image to the Transfer Server repository, View Transfer Server cannot perform the publish operation.

Procedure

1 In View Administrator, click **View Configuration > Servers**.

2 Click the Transfer Servers tab and click **Add**.

3 In the Add Transfer Server wizard, select the vCenter Server instance that manages the View Transfer Server virtual machine and click **Next**.

4 Select the virtual machine where View Transfer Server is installed and click **Finish**.

View Connection Server reconfigures the virtual machine with four SCSI controllers. The multiple SCSI controllers allow View Transfer Server to perform an increased number of disk transfers concurrently.

In View Administrator, the View Transfer Server instance appears in the Transfer Servers panel. If no Transfer Server repository is configured, the View Transfer Server status changes from **Pending** to **No Transfer Server Repository Configured**. If a Transfer Server repository is configured, the status changes from **Pending** to **Initializing Transfer Server Repository** to **Ready**.

This process can take several minutes. You can click the refresh button in View Administrator to check the current status.

When the View Transfer Server instance is added to View Manager, the Apache service is started on the View Transfer Server virtual machine.

CAUTION If your View Transfer Server virtual machine is an earlier version than hardware version 7, you must configure the static IP address on the View Transfer Server virtual machine after you add View Transfer Server to View Manager.

When multiple SCSI controllers are added to the View Transfer Server virtual machine, Windows removes the static IP address and reconfigures the virtual machine to use DHCP. After the virtual machine restarts, you must re-enter the static IP address in the virtual machine.

Configure the Transfer Server Repository

The Transfer Server repository stores View Composer base images for linked-clone desktops that run in local mode. To give View Transfer Server access to the Transfer Server repository, you must configure it in View Manager. If you do not use View Composer linked clones in local mode, you do not have to configure a Transfer Server repository.

If View Transfer Server is configured in View Manager before you configure the Transfer Server repository, View Transfer Server validates the location of the Transfer Server repository during the configuration.

If you plan to add multiple View Transfer Server instances to this View Manager deployment, configure the Transfer Server repository on a network share. Other View Transfer Server instances cannot access a Transfer Server repository that is configured on a local drive on one View Transfer Server instance.

Make sure that the Transfer Server repository is large enough to store your View Composer-generated base images. A base image can be several gigabytes in size.

If you configure a remote Transfer Server repository on a network share, you must provide a user ID with credentials to access the network share. As a best practice, to enhance the security of access to the Transfer Server repository, make sure that you restrict network access for the repository to View administrators.

Prerequisites

- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that View Transfer Server is added to View Manager. See "Add View Transfer Server to View Manager," on page 65.

NOTE Adding View Transfer Server to View Manager before you configure the Transfer Server repository is a best practice, not a requirement.

Procedure

1 Configure a path and folder for the Transfer Server repository.

The Transfer Server repository can be on a local drive or a network share.

Option	Action
Local Transfer Server repository	On the virtual machine where View Transfer Server is installed, create a path and folder for the Transfer Server repository. For example: `C:\TransferRepository\`
Remote Transfer Server repository	Configure a UNC path for the network share. For example: `\\server.domain.com\TransferRepository\` All View Transfer Server instances that you add to this View Manager deployment must have network access to the shared drive.

2 In View Administrator, click **View Configuration > Servers**.

3 Put all View Transfer Server instances into maintenance mode.

a In the Transfer Servers panel, select a View Transfer Server instance.

b Click **Enter Maintenance Mode** and click **OK**.

The View Transfer Server status changes to **Maintenance mode**.

c Repeat Step 3a and Step 3b for each instance.

When all View Transfer Server instances are in maintenance mode, current transfer operations are stopped.

4 In the General panel on the Transfer Server repository page, click **Edit**.

5 Type the Transfer Server repository location and other information.

Option	Description
Network share	■ **Path**. Type the UNC path that you configured. ■ **User name**. Type the user ID of an administrator with credentials to access the network share. ■ **Password**. Type the administrator password. ■ **Domain**. Type the domain name of the network share in NetBIOS format. Do not use the `.com` suffix.
Local filesystem	Type the path that you configured on the local View Transfer Server virtual machine.

6 Click **OK**.

If the repository network path or local drive is incorrect, the Edit Transfer Server Repository dialog displays an error message and does not let you configure the location. You must type a valid location.

7 On the **View Configuration > Servers** page, select the View Transfer Server instance and click **Exit Maintenance Mode**.

The View Transfer Server status changes to **Ready**.

Firewall Rules for View Transfer Server

Certain incoming TCP ports must be opened on the firewall for View Transfer Server instances.

The installation program can optionally configure the required Windows firewall rules for you.

Table 6-1 lists the incoming TCP ports that must be opened on the firewall for View Transfer Server instances.

Table 6-1. TCP Ports for View Transfer Server Instances

Protocol	Ports
HTTP	80
HTTPS	443

Installing View Transfer Server Silently

You can install View Transfer Server silently by typing the installer filename and installation options at the command line. With silent installation, you can efficiently deploy View components in a large enterprise.

Set Group Policies to Allow Silent Installation of View Transfer Server

Before you can install View Transfer Server silently, you must configure Microsoft Windows group policies to allow installation with elevated privileges.

You must set Windows Installer group policies for computers and for users on the local computer.

Prerequisites

Verify that you have local administrator privileges on the Windows Server computer on which you will install View Transfer Server.

Procedure

1 Log in to the Windows Server computer and click **Start > Run**.

2 Type **`gpedit.msc`** and click **OK**.

3 In the Group Policy Object Editor, click **Local Computer Policy > Computer Configuration**.

4 Expand **Administrative Templates**, expand **Windows Components**, open the **Windows Installer** folder, and double-click **Always install with elevated privileges**.

5 In the **Always Install with Elevated Privileges Properties** window, click **Enabled** and click **OK**.

6 In the left pane, click **User Configuration**.

7 Expand **Administrative Templates**, expand **Windows Components**, open the **Windows Installer** folder, and double-click **Always install with elevated privileges**.

8 In the **Always Install with Elevated Privileges Properties** window, click **Enabled** and click **OK**.

What to do next

Install View Transfer Server silently.

Install View Transfer Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install View Transfer Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

Prerequisites

- Verify that you have local administrator privileges on the Windows Server on which you will install View Transfer Server.
- Verify that your installation satisfies the View Transfer Server requirements described in "View Transfer Server Requirements," on page 11.
- Verify that you have a license to install View Transfer Server and use local desktops.
- Verify that the virtual machine on which you install View Transfer Server has version 2.0 or later of the MSI runtime engine. For details, see the Microsoft Web site.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 59.
- Familiarize yourself with the silent installation properties available with View Transfer Server. See "Silent Installation Properties for View Transfer Server," on page 69.
- Verify that the Windows Installer group policies that are required for silent installation are configured on the Windows Server computer. See "Set Group Policies to Allow Silent Installation of View Transfer Server," on page 67.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

The installer filename is `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number.

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=4"`

The VMware View Transfer Server, View Transfer Server Control Service, and VMware View Framework Component services are installed and started on the virtual machine.

What to do next

In View Administrator, add View Transfer Server to your View Manager deployment.

Silent Installation Properties for View Transfer Server

You can include specific properties when you silently install a View Transfer Server from the command line. You must use a *PROPERTY=value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 6-2. MSI Properties for Silently Installing View Transfer Server

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation To install a View Transfer Server, define `VDM_SERVER_INSTANCE_TYPE=4` This MSI property is optional for a standard installation. It is required for all other types of installation.	1
SERVERDOMAIN	The network domain of the virtual machine on which you install View Transfer Server. This value corresponds to the Apache Web Server network domain that is configured during an interactive installation. For example: `SERVERDOMAIN=companydomain.com` If you specify a custom Apache Web Server domain with the MSI property, `SERVERDOMAIN`, you also must specify custom `SERVERNAME` and `SERVERADMIN` properties. This MSI property is optional.	None
SERVERNAME	The host name of the virtual machine on which you install View Transfer Server. This value corresponds to the Apache Web Server host name that is configured during an interactive installation. For example: `SERVERNAME=ts1.companydomain.com` If you specify a custom Apache Web Server host name with the MSI property, `SERVERNAME`, you also must specify custom `SERVERDOMAIN` and `SERVERADMIN` properties. This MSI property is optional.	None
SERVERADMIN	The email address of the administrator of Apache Web Server that is configured with View Transfer Server. For example: `SERVERADMIN=admin@companydomain.com` If you specify a custom Apache Web Server administrator with the MSI property, `SERVERADMIN`, you also must specify custom `SERVERDOMAIN` and `SERVERNAME` properties. This MSI property is optional.	None
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1` This MSI property is optional.	1

Configuring SSL Certificates for View Servers

7

VMware strongly recommends that you configure SSL certificates for authentication of View Connection Server instances, security servers, and View Composer service instances.

A default SSL server certificate is generated when you install View Connection Server instances, security servers, or View Composer instances. You can use the default certificate for testing purposes.

IMPORTANT Replace the default certificate as soon as possible. The default certificate is not signed by a Certificate Authority (CA). Use of certificates that are not signed by a CA can allow untrusted parties to intercept traffic by masquerading as your server.

This chapter includes the following topics:

Understanding SSL Certificates for View Servers

You must follow certain guidelines for configuring SSL certificates for View servers and related components.

View Connection Server and Security Server

SSL is required for View Client connections to View. Client-facing View Connection Server instances, security servers, and intermediate servers that terminate SSL connections require SSL server certificates.

By default, when you install View Connection Server or security server, the installation generates a self-signed certificate for the View server. However, the installation uses an existing certificate in the following cases:

- If a valid certificate with a Friendly name of `vdm` already exists in the Windows Certificate Store

- If you upgrade to View 5.1 or later from an earlier release, and a valid keystore file is configured on the Windows Server computer. The installation extracts the keys and certificates and imports them into the Windows Certificate Store.

vCenter Server and View Composer

Before you add vCenter Server and View Composer to View Manager in a production environment, make sure that vCenter Server and View Composer use certificates that are signed by a CA.

For information about replacing the default certificate for vCenter Server, see the *vSphere Examples and Scenarios* document.

If you install vCenter Server and View Composer on the same Windows Server host, they can use the same SSL certificate, but you must configure the certificate separately for each component.

View Transfer Server

You do not have to configure SSL certificates for View Transfer Server if you are installing View 5.1 or later.

A default, self-signed certificate is installed with View Transfer Server that View Connection Server uses to handle secondary connections to View Clients. See "View Transfer Server and SSL Certificates," on page 82.

Additional Guidelines

For general information about requesting and using SSL certificates that are signed by a CA, see "Benefits of Using SSL Certificates Signed by a CA," on page 83.

When View Clients connect to a View Connection Server instance or security server, they are presented with the View server's SSL server certificate and any intermediate certificates in the trust chain. To trust the server certificate, the client systems must have installed the root certificate of the signing CA.

When View Connection Server communicates with vCenter Server and View Composer, View Connection Server is presented with SSL server certificates and intermediate certificates from these servers. To trust the vCenter Server and View Composer servers, the View Connection Server computer must have installed the root certificate of the signing CA.

Overview of Tasks for Setting Up SSL Certificates

To set up SSL server certificates for View servers, you must perform several high-level tasks.

The procedures for carrying out these tasks are described in the topics that follow this overview.

1 Determine if you need to obtain a new signed SSL certificate from a CA.

  If your organization already has a valid SSL server certificate, you can use that certificate to replace the default SSL server certificate provided with View Connection Server, security server, or View Composer. To use an existing certificate, you also need the accompanying private key.

Starting Place	Action
Your organization provided you with a valid SSL server certificate.	Go directly to step 2.
You do not have an SSL server certificate.	Obtain a signed SSL server certificate from a CA.

2 Import the SSL certificate into the Windows local computer certificate store on the View server host.

3 For View Connection Server instances and security servers, modify the certificate Friendly name to **vdm**.

  Assign the Friendly name **vdm** to only one certificate on each View server host.

4 On View Connection Server computers, if the root certificate is not trusted by the Windows Server host, import the root certificate into the Windows local computer certificate store.

   Take this step for View Connection Server instances only. You do not have to import the root certificate to View Composer, vCenter Server, or security server hosts.

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

   To simplify client configuration, import the entire certificate chain into the Windows local computer certificate store. If intermediate certificates are missing from the View server, they must be configured for View Clients and computers that launch View Administrator.

6 For View Composer instances, take one of these steps:

   - If you import the certificate into the Windows local computer certificate store before you install View Composer, you can select your certificate during the View Composer installation.
   - If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate after you install View Composer, run the `SviConfig ReplaceCertificate` utility to bind the new certificate to the port used by View Composer.

7 If your CA is not well known, configure View Clients to trust the root and intermediate certificates.

   Also ensure that the computers on which you launch View Administrator trust the root and intermediate certificates.

8 Determine whether to reconfigure certificate revocation checking.

   View Connection Server performs certificate revocation checking on View servers, View Composer, and vCenter Server. Most certificates signed by a CA include certificate revocation information. If your CA does not include this information, you can configure the server not to check certificates for revocation.

Obtaining a Signed SSL Certificate from a CA

If your organization does not provide you with an SSL server certificate, you must request a new certificate that is signed by a CA.

You can use several methods to obtain a new signed certificate. For example, you can use Microsoft Internet Information Services (IIS) Manager to request an SSL server certificate from a CA. For testing purposes, you can obtain a free temporary certificate based on an untrusted root from many CAs.

When you generate a certificate request on a computer, make sure that a private key is generated also. When you obtain the SSL server certificate and import it into the Windows local computer certificate store, there must be an accompanying private key that corresponds to the certificate.

IMPORTANT Do not create certificates for View servers using a certificate template that is compatible only with a Windows Server 2008 enterprise CA or later.

For general information about obtaining certificates, consult the Microsoft online help available with the Certificate Snap-in to MMC. If the Certificate Snap-in is not yet installed on your computer, see "Add the Certificate Snap-In to MMC," on page 75.

Obtain a Signed Certificate from a Windows Domain or Enterprise CA

To obtain a signed certificate from a Windows Domain or Enterprise CA, you can use the Windows Certificate Enrollment wizard in the Windows Certificate Store.

This method of requesting a certificate is appropriate if communications between computers remain within your internal domain. For example, obtaining a signed certificate from a Windows Domain CA might be appropriate for server-to-server communications.

If your View Clients connect to View servers from an external network, request SSL server certificates that are signed by a trusted, third-party CA.

Prerequisites

- Determine the fully qualified domain name (FQDN) that client computers use to connect to the host.
- Verify that the Certificate snap-in was added to MMC. See "Add the Certificate Snap-In to MMC," on page 75.
- Verify that you have the appropriate credentials to request a certificate that can be issued to a computer or service.

Procedure

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

2 From the **Action** menu, go to **All Tasks > Request New Certificate** to display the Certificate Enrollment wizard.

3 Select a Certificate Enrollment Policy.

4 Select the types of certificates that you want to request and click **Enroll**.

5 Click **Finish**.

The new signed certificate is added to the **Personal > Certificates** folder in the Windows Certificate Store.

What to do next

- Verify that the server certificate and certificate chain were imported into the Windows Certificate Store.
- For a View Connection Server instance or security server, modify the certificate friendly name to **`vdm`**. See "Modify the Certificate Friendly Name," on page 76.
- For a View Composer server, bind the new certificate to the port that used by View Composer. See "Bind a New SSL Certificate to the Port Used by View Composer," on page 78.

Configure View Connection Server, Security Server, or View Composer to Use a New SSL Certificate

To configure a View Connection Server instance, security server, or View Composer instance to use an SSL certificate, you must import the server certificate and the entire certificate chain into the Windows local computer certificate store on the View Connection Server, security server, or View Composer host.

IMPORTANT To configure View Connection Server or security server to use a certificate, you must change the certificate Friendly name to **`vdm`**. Also, the certificate must have an accompanying private key.

If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate after you install View Composer, you must run the `SviConfig ReplaceCertificate` utility to bind the new certificate to the port used by View Composer.

Procedure

1 Add the Certificate Snap-In to MMC on page 75

Before you can add certificates to the Windows Certificate Store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the Windows Server host on which the View server is installed.

2 Import a Signed Server Certificate into a Windows Certificate Store on page 75

You must import the SSL server certificate into the Windows local computer certificate store on the Windows Server host on which the View Connection Server instance, security server, or View Composer service is installed.

3 Modify the Certificate Friendly Name on page 76

To configure a View Connection Server instance or security server to recognize and use an SSL certificate, you must modify the certificate Friendly name to `vdm`.

4 Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store on page 77

If the Windows Server host on which View Connection Server is installed does not trust the root certificate for the signed SSL server certificate, you must import the root certificate into the Windows local computer certificate store. In addition, if the View Connection Server host does not trust the root certificates of the SSL server certificates configured for security server, View Composer, and vCenter Server hosts, you also must import those root certificates.

5 Bind a New SSL Certificate to the Port Used by View Composer on page 78

If you configure a new SSL certificate after you install View Composer, you must run the `SviConfig ReplaceCertificate` utility to replace the certificate that is bound to the port used by View Composer. This utility unbinds the existing certificate and binds the new certificate to the port.

Add the Certificate Snap-In to MMC

Before you can add certificates to the Windows Certificate Store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the Windows Server host on which the View server is installed.

Prerequisites

Verify that the MMC and Certificate snap-in are available on the Windows Server computer on which the View server is installed.

Procedure

1 On the Windows Server computer, click **Start** and type **`mmc.exe`**.

2 In the MMC window, go to **File > Add/Remove Snap-in**.

3 In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.

4 In the Certificates snap-in window, select **Computer account**, click **Next**, select **Local computer**, and click **Finish**.

5 In the Add or Remove snap-in window, click **OK**.

What to do next

Import the SSL server certificate into the Windows Certificate Store.

Import a Signed Server Certificate into a Windows Certificate Store

You must import the SSL server certificate into the Windows local computer certificate store on the Windows Server host on which the View Connection Server instance, security server, or View Composer service is installed.

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

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

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

NOTE If you off-load SSL connections to an intermediate server, you must import the same SSL server certificate onto both the intermediate server and the off-loaded View server. For details, see "Off-load SSL Connections to Intermediate Servers" in the *VMware View Administration* document.

Prerequisites

Verify that the Certificate snap-in was added to MMC. See "Add the Certificate Snap-In to MMC," on page 75.

Procedure

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

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

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

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

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

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

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

7 Select **Include all extendable properties**.

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

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

9 Verify that the new certificate contains a private key.

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

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

What to do next

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

Modify the Certificate Friendly Name

To configure a View Connection Server instance or security server to recognize and use an SSL certificate, you must modify the certificate Friendly name to `vdm`.

You do not have to modify the Friendly name of SSL certificates that are used by View Composer.

Prerequisites

Verify that the server certificate is imported into the **Certificates (Local Computer) > Personal > Certificates** folder in the Windows Certificate Store. See "Import a Signed Server Certificate into a Windows Certificate Store," on page 75.

Procedure

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

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

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

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

What to do next

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

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

Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store

If the Windows Server host on which View Connection Server is installed does not trust the root certificate for the signed SSL server certificate, you must import the root certificate into the Windows local computer certificate store. In addition, if the View Connection Server host does not trust the root certificates of the SSL server certificates configured for security server, View Composer, and vCenter Server hosts, you also must import those root certificates.

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

NOTE You do not have to import the root certificate into View Composer, vCenter Server, or security server hosts.

If a server certificate is signed by an intermediate CA, you also must import each intermediate certificate in the certificate chain. To simplify client configuration, import the entire intermediate chain to security server, View Composer, and vCenter Server hosts as well as View Connection Server hosts. If intermediate certificates are missing from a View Connection Server or security server host, they must be configured for View Clients and computers that launch View Administrator. If intermediate certificates are missing from a View Composer or vCenter Server host, they must be configured for each View Connection Server instance.

If you already verified that the entire certificate chain is imported into the Windows local computer certificate store, you can skip this task.

Procedure

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

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

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

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

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

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

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

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

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

7 Restart the View Connection Server service, Security Server service, View Composer service, or vCenter Server service to make your changes take effect.

Bind a New SSL Certificate to the Port Used by View Composer

If you configure a new SSL certificate after you install View Composer, you must run the `SviConfig ReplaceCertificate` utility to replace the certificate that is bound to the port used by View Composer. This utility unbinds the existing certificate and binds the new certificate to the port.

If you install the new certificate on the Windows Server computer before you install View Composer, you do not have to run the `SviConfig ReplaceCertificate` utility. When you run the View Composer installer, you can select a certificate signed by a CA instead of the default, self-signed certificate. During the installation, the selected certificate is bound to the port used by View Composer.

If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate, you must use the `SviConfig ReplaceCertificate` utility.

Prerequisites

Verify that the new certificate was imported into the Windows local computer certificate store on the Windows Server computer on which View Composer is installed.

Procedure

1 Stop the View Composer service.

2 Open a command prompt on the Windows Server host where View Composer is installed.

3 Type the `SviConfig ReplaceCertificate` command.

   For example:

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

   where `–delete` is a required parameter that operates on the certificate that is being replaced. You must specify either `–delete=true` to delete the old certificate from the Windows local computer certificate store or `–delete=false` to keep the old certificate in the Windows certificate store.

   The utility displays a numbered list of SSL certificates that are available in the Windows local computer certificate store.

4 To select a certificate, type the number of a certificate and press Enter.

5 Restart the View Composer service to make your changes take effect.

Example: SviConfig ReplaceCertificate

The following example replaces the certificate that is bound to the View Composer port:

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

Configure View Clients to Trust Root and Intermediate Certificates

If a View server certificate is signed by a CA that is not trusted by View Client computers and client computers that access View Administrator, you can configure all Windows client systems in a domain to trust the root and intermediate certificates. To do so, you must add the public key for the root certificate to the Trusted Root Certification Authorities group policy in Active Directory and add the root certificate to the Enterprise NTAuth store.

For example, you might have to take these steps if your organization uses an internal certificate service.

You do not have to take these steps if the Windows domain controller acts as the root CA, or if your certificates are signed by a well known CA. For well known CAs, the operating system venders preinstall the root certificate on client systems.

If your View server certificates are signed by a little-known intermediate CA, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

For View Clients that run on other operating systems and devices, see the following instructions for distributing root and intermediate certificates that users can install:

- For View Client for Mac OS X, see "Configure View Client for Mac OS X to Trust Root and Intermediate Certificates," on page 80.
- For View Client for iPad, see "Configure View Client for iPad to Trust Root and Intermediate Certificates," on page 80.
- For View Client for Android, see documentation on the Google Web site, such as the *Android 3.0 User's Guide*
- For View Client for Linux, see the Ubuntu documentation

Procedure

1 On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAuth store.

For example: **`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

2 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

3 Expand the **Computer Configuration** section and go to **Windows Settings > Security Settings > Public Key Policies**.

4 Import the certificate.

Option	Description
Root certificate	a Right-click **Trusted Root Certification Authorities** and select **Import**. b Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.
Intermediate certificate	a Right-click **Intermediate Certification Authorities** and select **Import**. b Follow the prompts in the wizard to import the intermediate certificate (for example, `intermediateCA.cer`) and click **OK**.

5 Close the Group Policy window.

All systems in the domain now have certificate information in their trusted root certificate stores and intermediate certificate stores that allows them to trust the root and intermediate certificates.

Configure View Client for Mac OS X to Trust Root and Intermediate Certificates

If a View server certificate is signed by a CA that is not trusted by computers that run View Client for Mac OS X, you can configure these computers to trust the root and intermediate certificates. You must distribute the root certificate and all intermediate certificates in the trust chain to the client computers.

Procedure

1 Deliver the root certificate and intermediate certificates to the computer that is running View Client for Mac OS X.

2 Open the root certificate on the Mac OS X computer.

The certificate displays the following message: `Do you want your computer to trust certificates signed by` *`CA name`* `from now on?`

3 Click **Always Trust**

4 Type the user password.

5 Repeat steps 2 through 4 for all intermediate certificates in the trust chain.

Configure View Client for iPad to Trust Root and Intermediate Certificates

If a View server certificate is signed by a CA that is not trusted by iPads that run View Client for iPad, you can configure the iPads to trust the root and intermediate certificates. You must distribute the root certificate and all intermediate certificates in the trust chain to the iPads.

Procedure

1 Send the root certificate and intermediate certificates as email attachments to the iPad.

2 Open the email attachment for the root certificate and select **Install**.

The certificate displays the following message:

`Unverifiable Profile. The authenticity of` *`Certificate name`* `cannot be verified. Installing this profile will change settings on your iPad.`

`Root Certificate. Installing the certificate` *`Certificate name`* `will add it to the list of trusted certificates on your iPad.`

3 Select **Install** again.

4 Repeat steps 2 and 3 for all intermediate certificates in the trust chain.

Configuring Certificate Revocation Checking on Server Certificates

Each View Connection Server instance performs certificate revocation checking on its own certificate and on those of the security servers paired to it. Each instance also checks the certificates of vCenter and View Composer servers whenever it establishes a connection to them. By default, all certificates in the chain are checked except the root certificate. You can, however, change this default.

View supports various means of certificate revocation checking, such as certificate revocation lists (CRLs) and the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate.

With CRLs, the list of revoked certificates is downloaded from a certificate distribution point (DP) that is often specified in the certificate. The View server periodically goes to the CRL DP URL specified in the certificate, downloads the list, and checks it to determine whether the server certificate has been revoked. With OCSP, the View server sends a request to an OCSP responder to determine the revocation status of the certificate.

When you obtain a server certificate from a third-party certificate authority (CA), the certificate includes one or more means by which its revocation status can be determined, including, for example, a CRL DP URL or the URL for an OCSP responder. If you have your own CA and generate a certificate but do not include revocation information in the certificate, the certificate revocation check fails. An example of revocation information for such a certificate could include, for example, a URL to a Web-based CRL DP on a server where you host a CRL.

If you have your own CA but do not or cannot include certificate revocation information in your certificate, you can choose not to check certificates for revocation or to check only certain certificates in a chain. On the View server, with the Windows Registry Editor, you can create the string (REG_SZ) value **CertificateRevocationCheckType**, under `HKLM\Software\VMware, Inc.\VMware VDM\Security`, and set this value to one of the following data values.

Value	Description
1	Do not perform certificate revocation checking.
2	Check only the server certificate. Do not check any other certificates in the chain.
3	Check all certificates in the chain.
4	(Default) Check all certificates except the root certificate.

If this registry value is not set, or if the value set is not valid (that is, if the value is not 1, 2, 3, or 4), all certificates are checked except the root certificate. Set this registry value on each View server on which you intend to modify revocation checking. You do not have to restart the system after you set this value.

Configuring Certificate Checking in View Client for Windows

You can use a security-related group policy setting in the View Client Configuration ADM template file (`vdm_client.adm`) to configure SSL server certificate checking in the Windows-based View Client.

Certificate checking occurs for SSL connections between View Connection Server and View Client. Certificate verification includes all the following checks:

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

- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects the View client to a server with a certificate that does not match the host name the user entered. A mismatch can also occur if the user enters an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA.

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

When you first set up a View environment, a default self-signed certificate is used. By default,**Warn But Allow**is the certificate verification mode. In this mode, when either of the following server certificate issues occurs, a warning is displayed, but the user can choose to continue on and ignore the warning:

- A self-signed certificate is provided by the View server. 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.

You can change the default certificate verification mode. You can set the mode to **No Security**, so that no certificate checking is done, or you can set the mode to **Full Security**, so that users are not allowed to connect to the server if any one of the checks fails. You can also allow end users to set the mode for themselves.

Use the `Certificate verification mode` group policy setting in the Client Configuration ADM template file to change the verification mode. When this group policy setting is configured, the setting is locked in View Client. Users can view the selected verification mode in View Client, but cannot configure the setting. When this group policy setting is not configured or disabled, View Client users can select a verification mode.

ADM template files for View components are installed in the *`install_directory`*`\VMware\VMware View\Server\Extras\GroupPolicyFiles` directory on your View Connection Server host. For information about using these templates to control GPO settings, see the *VMware View Administration* document.

View Transfer Server and SSL Certificates

You do not have to configure SSL certificates for View Transfer Server if you are installing View 5.1 or later.

A default, self-signed certificate is installed with View Transfer Server that View Connection Server uses to handle secondary connections to View clients.

When you add View Transfer Server to View, View Connection Server establishes a trust relationship with View Transfer Server. Communications between View Connection Server and View Transfer Server use Java Message Service (JMS). Messages containing sensitive data are encrypted.

When a View client requests a data transfer operation, which requires connecting to View Transfer Server, View Connection Server sends the thumbprint of the View Transfer Server certificate to the client. When the client connects to the Apache server that is associated with View Transfer Server, View Client verifies that the thumbprint passed from View Connection Server matches the certificate thumbprint on the Apache server.

Replacing the default certificate for View Transfer Server with a certificate that is signed by a CA would not significantly affect the secure communications between View Transfer Server, View Connection Server, and View clients.

In View 5.0.*x* and earlier versions, you did have to configure an SSL certificate for View Transfer Server.

If you are upgrading from View 5.0.*x* or earlier to View 5.1 or later, and you want to continue to use a certificate that is signed by a CA on the upgraded version of View Transfer Server, you must back up the certificate, upgrade View Transfer Server, and configure the signed certificate for the new View Transfer Server version.

If you configured a self-signed certificate for the old View Transfer Server, or you do not intend to use an existing CA-signed certificate on the upgraded server, you do not have to configure a certificate again. During the upgrade, a valid, self-signed certificate is installed with View Transfer Server.

For more information, see the *VMware View Upgrades* document.

Setting View Administrator to Trust a vCenter Server or View Composer Certificate

In the View Administrator dashboard, you can configure View to trust a vCenter Server or View Composer certificate that is untrusted.

VMware strongly recommends that you configure vCenter Server and View Composer to use SSL certificates that are signed by a CA. Alternatively, you can accept the thumbprint of the default certificate for vCenter Server or View Composer.

Benefits of Using SSL Certificates Signed by a CA

A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate, and thin client devices can connect without requiring additional configuration.

You can request an SSL server certificate that is specific to a Web domain such as `www.mycorp.com`, or you can request a wildcard SSL server certificate that can be used throughout a domain such as `*.mycorp.com`. To simplify administration, you might choose to request a wildcard certificate if you need to install the certificate on multiple servers or in different subdomains. Typically, domain-specific certificates are used in secure installations, and CAs usually guarantee more protection against losses for domain-specific certificates than for wildcard certificates. If you use a wildcard certificate, you must ensure that the private key is transferrable between servers.

When you replace the default certificate with your own certificate, clients use your certificate to authenticate the server. If your certificate is signed by a CA, the certificate for the CA itself is typically embedded in the browser or is located in a trusted database that the client can access. After a client accepts the certificate, it responds by sending a secret key, which is encrypted with the public key contained in the certificate. The secret key is used to encrypt traffic between the client and the server.

Configuring View for the First Time

8

After you install the View server software and configure SSL certificates for the servers, you must take a few additional steps to set up a working View environment.

You configure user accounts for vCenter Server and View Composer, install a View license key, add vCenter Server and View Composer to your View environment, configure the PCoIP Secure Gateway and secure tunnel, and, optionally, size Windows Server settings to support your View environment.

This chapter includes the following topics:

Configuring User Accounts for vCenter Server and View Composer

To use vCenter Server with View Manager, you must configure a user account with permission to perform operations in vCenter Server. To use View Composer, you must give this vCenter Server user additional privileges. To manage desktops that are used in local mode, you must give this user privileges in addition to those that are required for View Manager and View Composer.

You also must create a domain user for View Composer in Active Directory. See "Create a User Account for View Composer," on page 27.

Where to Use the vCenter Server User and Domain User for View Composer

After you create and configure these two user accounts, you specify the user names in View Administrator.

- You specify a vCenter Server user when you add vCenter Server to View Manager.
- You specify a domain user for View Composer when you configure View Composer for vCenter Server.
- You specify the domain user for View Composer when you create linked-clone pools.

Configure a vCenter Server User for View Manager, View Composer, and Local Mode

To configure a user account that gives View Manager permission to operate in vCenter Server, you must assign a role with appropriate privileges to that user. To use the View Composer service in vCenter Server, you must give the user account additional privileges. To manage desktops that are used in local mode, you must give the user account privileges that include View Manager, View Composer, and local mode privileges.

To support View Composer, you also must make this user a local system administrator on the vCenter Server computer.

Prerequisites

- In Active Directory, create a user in the View Connection Server domain or a trusted domain. See "Creating a User Account for vCenter Server," on page 26.
- Familiarize yourself with the privileges that are required for the user account. See "View Manager Privileges Required for the vCenter Server User," on page 87.
- If you use View Composer, familiarize yourself with the additional required privileges. See "View Composer Privileges Required for the vCenter Server User," on page 88.
- If you manage local desktops, familiarize yourself with the additional required privileges. See "Local Mode Privileges Required for the vCenter Server User," on page 88.

Procedure

1 In vCenter Server, prepare a role with the required privileges for the user.

   - You can use the predefined Administrator role in vCenter Server. This role can perform all operations in vCenter Server.
   - If you use View Composer, you can create a limited role with the minimum privileges needed by View Manager and View Composer to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`View Composer Administrator`**, and select privileges for the role.

     This role must have all the privileges that both View Manager and View Composer need to operate in vCenter Server.
   - If you manage local desktops, you can create a limited role with the minimum privileges needed by View Manager, View Composer, and the local mode feature to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`Local Mode Administrator`**, and select privileges for the role.

     This role must have all the privileges that View Manager, View Composer, and the local mode feature need to operate in vCenter Server.
   - If you use View Manager without View Composer and do not manage local desktops, you can create an even more limited role with the minimum privileges needed by View Manager to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`View Manager Administrator`**, and select privileges for the role.

2 In vSphere Client, right-click the vCenter Server at the top level of the inventory, click **Add Permission**, and add the vCenter Server user.

   NOTE You must define the vCenter Server user at the vCenter Server level.

3 From the drop-down menu, select the Administrator role, or the View Composer or View Manager role that you created, and assign it to the vCenter Server user.

4 If you use View Composer, on the vCenter Server computer, add the vCenter Server user account as a member of the local system Administrators group.

View Composer requires that the vCenter Server user is a system administrator on the vCenter Server computer.

What to do next

In View Administrator, when you add vCenter Server to View Manager, specify the vCenter Server user. See "Add vCenter Server Instances to View Manager," on page 90.

View Manager Privileges Required for the vCenter Server User

The vCenter Server user must have sufficient privileges to enable View Manager to operate in vCenter Server. Create a View Manager role for the vCenter Server user with the required privileges.

Table 8-1. View Manager Privileges

Privilege Group	Privileges to Enable
Folder	**Create Folder** **Delete Folder**
Virtual Machine	In **Configuration**: ■ **Add or remove device** ■ **Advanced** ■ **Modify device settings** In **Interaction**: ■ **Power Off** ■ **Power On** ■ **Reset** ■ **Suspend** In **Inventory**: ■ **Create new** ■ **Remove** In **Provisioning**: ■ **Customize** ■ **Deploy template** ■ **Read customization specifications**
Resource	**Assign virtual machine to resource pool**
Global	The following privilege is required to implement ESXi host caching in View. If you do not use host caching, the vCenter Server user does not need this privilege. **Act as vCenter Server**

View Composer Privileges Required for the vCenter Server User

To support View Composer, the vCenter Server user must have privileges in addition to those required to support View Manager. Create a View Composer role for the vCenter Server user with the View Manager privileges and these additional privileges.

Table 8-2. View Composer Privileges

Privilege Group	Privileges to Enable
Datastore	**Allocate space** **Browse datastore** **Low level file operations**
Virtual machine	**Inventory** (all) **Configuration** (all) **State** (all) In **Provisioning**: ■ **Clone virtual machine** ■ **Allow disk access**
Resource	**Assign virtual machine to resource pool**
Global	**Enable methods** **Disable methods** **System tag** The following privilege is required to implement ESXi host caching in View. If you do not use host caching, the vCenter Server user does not need this privilege. **Act as vCenter Server**
Network	(all)

Local Mode Privileges Required for the vCenter Server User

To manage desktops that are used in local mode, the vCenter Server user must have privileges in addition to those required to support View Manager and View Composer. Create a Local Mode Administrator role for the vCenter Server user that combines the View Manager privileges, View Composer privileges, and local mode privileges.

Table 8-3. Local Mode Privileges

Privilege Group	Privileges to Enable
Global	**Set custom attribute**
Host	In **Configuration**: **System management**

Configuring View Connection Server for the First Time

After you install View Connection Server, you must install a product license, add vCenter Servers and View Composer services to View Manager. You can also choose to configure ESXi hosts to cache virtual machine disk data.

If you install security servers, they are added to View Manager and appear in View Administrator automatically.

View Administrator and View Connection Server

View Administrator provides a management interface for View Manager.

Depending on your View deployment, you use one or more View Administrator interfaces.

- Use one View Administrator interface to manage the View components that are associated with a single, standalone View Connection Server instance or a group of replicated View Connection Server instances.

  You can use the IP address of any replicated instance to log in to View Administrator.

- You must use a separate View Administrator interface to manage the View components for each single, standalone View Connection Server instance and each group of replicated View Connection Server instances.

You also use View Administrator to manage security servers and View Transfer Server instances associated with View Connection Server.

- Each security server is associated with one View Connection Server instance.
- Each View Transfer Server instance can communicate with any View Connection Server instance in a group of replicated instances.

Log In to View Administrator

To perform initial configuration tasks, you must log in to View Administrator.

Prerequisites

Verify that you are using a Web browser supported by View Administrator. See "View Administrator Requirements," on page 9.

Procedure

1 Open your Web browser and enter the following URL, where *server* is the host name of the View Connection Server instance.

```
https://server/admin
```

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

Your access to View Administrator depends on the type of certificate that is configured on the View Connection Server computer.

Option	Description
You configured a certificate signed by a CA for View Connection Server.	When you first connect, your Web browser displays View Administrator.
The default, self-signed certificate supplied with View Connection Server is configured.	When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. Click **Ignore** to continue using the current SSL certificate.

2 Log in as a user with credentials to access the View Administrators account.

You specify the View Administrators account when you install a standalone View Connection Server instance or the first View Connection Server instance in a replicated group. The View Administrators account can be the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer or a domain user or group account.

After you log in to View Administrator, you can use **View Configuration > Administrators** to change the list of users and groups that have the View Administrators role.

Install the View Connection Server License Key

Before you can use View Connection Server, you must enter the product license key.

The first time you log in, View Administrator displays the Product Licensing and Usage page.

After you install the license key, View Administrator displays the dashboard page when you log in.

You do not have to configure a license key when you install a replicated View Connection Server instance or a security server. Replicated instances and security servers use the common license key stored in the View LDAP configuration.

NOTE View Connection Server requires a valid license key for View 5.0. As of the release of VMware View 4.0, the VMware View license key is a 25-character key.

Procedure

1 If the View Configuration view is not displayed, click **View Configuration** in the left navigation pane.

2 Click **Product Licensing and Usage**.

3 On the Product Licensing table, click **Edit License** and enter the View Manager license serial number.

4 Click **OK**.

5 Verify the license expiration date.

Add vCenter Server Instances to View Manager

You must configure View Manager to connect to the vCenter Server instances in your View deployment. vCenter Server creates and manages the virtual machines that View Manager uses as desktop sources.

If you run vCenter Server instances in a Linked Mode group, you must add each vCenter Server instance to View Manager separately.

View Manager connects to the vCenter Server instance using a secure channel (SSL).

Prerequisites

- Install the View Connection Server product license key.
- Prepare a vCenter Server user with permission to perform the operations in vCenter Server that are necessary to support View Manager. To use View Composer, you must give the user additional privileges. To manage desktops that are used in local mode, you must give the user privileges in addition to those that are required for View Manager and View Composer.

  See "Configure a vCenter Server User for View Manager, View Composer, and Local Mode," on page 86.
- Verify that an SSL server certificate is installed on the vCenter Server host. In a production environment, install a valid SSL certificate that is signed by a trusted Certificate Authority (CA).

  In a testing environment, you can use the default certificate that is installed with vCenter Server, but you must accept the certificate thumbprint when you add vCenter Server to View.

- Verify that all View Connection Server instances in the replicated group trust the root CA certificate for the server certificate that is installed on the vCenter Server host. Check if the root CA certificate is in the **Trusted Root Certification Authorities > Certificates** folder in the Windows local computer certificate stores on the View Connection Server hosts. If it is not, import the root CA certificate into the Windows local computer certificate stores.

  See "Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store" in the *VMware View Installation* document.

- Familiarize yourself with the settings that determine the maximum operations limits for vCenter Server and View Composer. See "Concurrent Operations Limits for vCenter Server and View Composer," on page 95 and "Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms," on page 95.

Procedure

1 In View Administrator, click **View Configuration > Servers**.

2 In the vCenter Servers tab, click **Add**.

3 In the vCenter Server Settings server address text box, type the fully qualified domain name (FQDN) of the vCenter Server instance.

  The FQDN includes the host name and domain name. For example, in the FQDN ***myserverhost.companydomain.com***, ***myserverhost*** is the host name and ***companydomain.com*** is the domain.

  NOTE If you enter a server by using a DNS name or URL, View Manager does not perform a DNS lookup to verify whether an administrator previously added this server to View Manager by using its IP address. A conflict arises if you add a vCenter Server with both its DNS name and its IP address.

4 Type the name of the vCenter Server user.

5 Type the vCenter Server user password.

6 (Optional) Type a description for this vCenter Server instance.

7 Type the TCP port number.

  The default port is 443.

8 Under Advanced Settings, set the concurrent operations limits for vCenter Server and View Composer operations.

9 Click **Next** to display the View Composer Settings page.

What to do next

Configure View Composer settings.

- If the vCenter Server instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Settings page.

- If the vCenter Server instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See "Accept the Thumbprint of a Default SSL Certificate," on page 96.

If View Manager uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

Configure View Composer Settings

To use View Composer, you must configure settings that allow View Manager to connect to the View Composer service. View Composer can be installed on its own separate host or on the same host as vCenter Server.

There must be a one-to-one mapping between each View Composer service and vCenter Server instance. A View Composer service can operate with only one vCenter Server instance. A vCenter Server instance can be associated with only one View Composer service.

Prerequisites

- Your Active Directory administrator must create a domain user with permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. To manage the linked-clone machine accounts in Active Directory, the domain user must have **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions.

  See "Create a User Account for View Composer," on page 27.

- Verify that you configured View Manager to connect to vCenter Server. To do so, you must complete the vCenter Server Information page in the Add vCenter Server wizard. See "Add vCenter Server Instances to View Manager," on page 90.
- Verify that this View Composer service is not already configured to connect to a different vCenter Server instance.

Procedure

1 In View Administrator, complete the vCenter Server Information page in the Add vCenter Server wizard.

   a Click **View Configuration > Servers**.

   b In the vCenter Servers tab, click **Add** and provide the vCenter Server settings.

2 On the View Composer Settings page, if you are not using View Composer, select **Do not use View Composer**.

   If you select **Do not use View Composer**, the other View Composer settings become inactive. When you click **Next**, the Add vCenter Server wizard displays the Host Cache Settings page. The View Composer Domains page is not displayed.

3 If you are using View Composer, select the location of the View Composer host.

Option	Description
View Composer is installed on the same host as vCenter Server.	a Select **View Composer co-installed with the vCenter Server**. b Make sure that the port number is the same as the port that you specified when you installed the View Composer service on vCenter Server. The default port number is 18443.
View Composer is installed on its own separate host.	a Select **Standalone View Composer Server**. b In the View Composer server address text box, type the fully qualified domain name (FQDN) of the View Composer host. c Type the name of the View Composer user. d Type the password of the View Composer user. e Make sure that the port number is the same as the port that you specified when you installed the View Composer service. The default port number is 18443.

4 Click **Next** to display the View Composer Domains page.

What to do next

Configure View Composer domains.

- If the View Composer instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Domains page.
- If the View Composer instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See "Accept the Thumbprint of a Default SSL Certificate," on page 96.

Configure View Composer Domains

You must configure an Active Directory domain in which View Composer deploys linked-clone desktops. You can configure multiple domains for View Composer. After you first add vCenter Server and View Composer settings to View, you can add more View Composer domains by editing the vCenter Server instance in View Administrator.

Prerequisites

In View Administrator, verify that you completed the vCenter Server Information and View Composer Settings pages in the Add vCenter Server wizard.

Procedure

1 On the View Composer Domains page, click **Add** to add the domain user for View Composer account information.

2 Type the domain name of the Active Directory domain.

For example: **`domain.com`**

3 Type the domain user name, including the domain name.

For example: **`domain.com\admin`**

4 Type the account password.

5 Click **OK**.

6 To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.

7 Click **Next** to display the Host Cache Settings page.

What to do next

Configure host cache settings for View.

Configure View Storage Accelerator (Host Caching) for vCenter Server

In vSphere 5.0 and later, you can configure ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. Host caching improves View performance during I/O storms, which can take place when many desktops start up or run anti-virus scans at once. Instead of reading the entire OS from the storage system over and over, a host can read common data blocks from cache.

By reducing the number of IOPS during boot storms, host caching lowers the demand on the storage array, which lets you use less storage I/O bandwidth to support your View deployment.

You enable caching on your ESXi hosts by using the View interface to vCenter Server.

To enable this feature, you also must configure host caching for individual desktop pools. Host caching is not active for a pool until you explicitly enable it. You can enable host caching when you create or edit a pool. You can disable host caching by editing an existing pool.

You can enable host caching on pools that contain linked clones and pools that contain full virtual machines.

Host caching is also supported with local mode. Users can check out desktops in pools that are enabled for host caching. Host caching is disabled while a desktop is checked out and reenabled after the desktop is checked in.

View Composer Array Integration is not supported in pools that are enabled for host caching. View Composer Array Integration uses vStorage APIs for Array Integration (VAAI) native NFS snapshot technology to clone virtual machines.

Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.0 or later.

  In an ESXi cluster, verify that all the hosts are version 5.0 or later.

- Verify that the vCenter Server user was assigned the **Global > Act as vCenter Server** privilege in vCenter Server. See the topics in the *VMware View Installation* documentation that describe View Manager and View Composer privileges required for the vCenter Server user.

Procedure

1 In View Administrator, complete the Add vCenter Server wizard pages that precede the Host Cache Settings page.

   a Select **View Configuration > Servers**.

   b In the vCenter Servers tab, click **Add**.

   c Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.

2 On the Host Cache Settings page, select the **Enable host caching for View** check box.

3 Specify a default host cache size.

   The default cache size applies to all ESXi hosts that are managed by this vCenter Server instance.

   The default value is 1,024MB. The cache size must be between 100MB and 2,048MB.

4 To specify a different cache size for an individual ESXi host, select an ESXi host and click **Edit cache size**.

   a In the Host cache dialog box, check **Override default host cache size**.

   b Type a **Host cache size** value between 100MB and 2,048MB and click **OK**.

5 On the Host Cache Settings page, click **Next**.

6 Click **Finish** to add vCenter Server, View Composer, and Host Cache Settings to View.

What to do next

To configure the PCoIP Secure Gateway, secure tunnel, and external URLs for client connections, see "Configuring View Client Connections," on page 97.

To complete host cache settings in View, configure host caching for desktop pools. See "Configure Host Caching for Desktop Pools" in the *VMware View Administration* document.

Concurrent Operations Limits for vCenter Server and View Composer

When you add vCenter Server to View or edit the vCenter Server settings, you can configure several options that set the maximum number of concurrent operations that are performed by vCenter Server and View Composer.

You configure these options in the Advanced Settings panel on the vCenter Server Information page.

Table 8-4. Concurrent Operations Limits for vCenter Server and View Composer

Setting	Description
Max concurrent vCenter provisioning operations	Determines the maximum number of concurrent requests that View Manager can make to provision and delete full virtual machines in this vCenter Server instance. The default value is 20. This setting applies to full virtual machines only.
Max concurrent power operations	Determines the maximum number of concurrent power operations (startup, shutdown, suspend, and so on) that can take place on virtual machines managed by View Manager in this vCenter Server instance. The default value is 50. For guidelines for calculating a value for this setting, see "Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms," on page 95. This setting applies to full virtual machines and linked clones.
Max concurrent View Composer maintenance operations	Determines the maximum number of concurrent View Composer refresh, recompose, and rebalance operations that can take place on linked clones managed by this View Composer instance. The default value is 12. Desktops that have active sessions must be logged off before a maintenance operation can begin. If you force users to log off as soon as a maintenance operation begins, the maximum number of concurrent operations on desktops that require logoffs is half the configured value. For example, if you configure this setting as 24 and force users to log off, the maximum number of concurrent operations on desktops that require logoffs is 12. This setting applies to linked clones only.
Max concurrent View Composer provisioning operations	Determines the maximum number of concurrent creation and deletion operations that can take place on linked clones managed by this View Composer instance. The default value is 8. This setting applies to linked clones only.

Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms

The **Max concurrent power operations** setting governs the maximum number of concurrent power operations that can occur on View desktop virtual machines in a vCenter Server instance. Starting in View 5.0, this limit is set to 50 by default. You can change this value to support peak power-on rates when many users log on to their desktops at the same time.

As a best practice, you can conduct a pilot phase to determine the correct value for this setting. For planning guidelines, see "Architecture Design Elements and Planning Guidelines" in the *VMware View Architecture Planning* document.

The required number of concurrent power operations is based on the peak rate at which desktops are powered on and the amount of time it takes for the desktop to power on, boot, and become available for connection. In general, the recommended power operations limit is the total time it takes for the desktop to start multiplied by the peak power-on rate.

For example, the average desktop takes two to three minutes to start. Therefore, the concurrent power operations limit should be 3 times the peak power-on rate. The default setting of 50 is expected to support a peak power-on rate of 16 desktops per minute.

View waits a maximum of five minutes for a desktop to start. If the start time takes longer, other errors are likely to occur. To be conservative, you can set a concurrent power operations limit of 5 times the peak power-on rate. With a conservative approach, the default setting of 50 supports a peak power-on rate of 10 desktops per minute.

Logons, and therefore desktop power on operations, typically occur in a normally distributed manner over a certain time window. You can approximate the peak power-on rate by assuming that it occurs in the middle of the time window, during which about 40% of the power-on operations occur in 1/6th of the time window. For example, if users log on between 8:00 AM and 9:00 AM, the time window is one hour, and 40% of the logons occur in the 10 minutes between 8:25 AM and 8:35 AM. If there are 2,000 users, 20% of whom have their desktops powered off, then 40% of the 400 desktop power-on operations occur in those 10 minutes. The peak power-on rate is 16 desktops per minute.

Accept the Thumbprint of a Default SSL Certificate

When you add vCenter Server and View Composer instances to View, you must ensure that the SSL certificates that are used for the vCenter Server and View Composer instances are valid and trusted by View Connection Server. If the default certificates that are installed with vCenter Server and View Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or View Composer instance is configured with a certificate that is signed by a CA, and the root certificate is trusted by View Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but View Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

NOTE If you install vCenter Server and View Composer on the same Windows Server host, they can use the same SSL certificate, but you must configure the certificate separately for each component.

For details about configuring SSL certificates, see Configuring SSL Certificates for View Servers.

You first add vCenter Server and View Composer to View in the Add vCenter Server wizard in View Administrator. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server and View Composer to View.

After these servers are added to View, you can reconfigure them in the Edit vCenter Server dialog.

NOTE You also must accept a certificate thumbprint when you upgrade from an earlier View release to View 5.1 or later, and a vCenter Server or View Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

On the View Administrator dashboard, the vCenter Server or View Composer icon turns red and an Invalid Certificate Detected dialog box appears. You must click **Verify** and follow the procedure shown here.

Procedure

1 When View Administrator displays an Invalid Certificate Detected dialog box, click **View Certificate**.

2 Examine the certificate thumbprint in the Certificate Information window.

3 Examine the certificate thumbprint that was configured for the vCenter Server or View Composer instance.

   a On the vCenter Server or View Composer host, start the MMC snap-in and open the Windows Certificate Store.

   b Navigate to the vCenter Server or View Composer certificate.

   c Click the Certificate Details tab to display the certificate thumbprint.

4 Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server or View Composer instance.

5 Determine whether to accept the certificate thumbprint.

Option	Description
The thumbprints match.	Click **Accept** to use the default certificate.
The thumbprints do not match.	Click **Reject**. Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server or View Composer.

Configuring View Client Connections

View clients communicate with a View Connection Server or security server host over secure connections.

The initial View Client connection, which is used for user authentication and View desktop selection, is created over HTTPS when a user provides a domain name to View Client. If firewall and load balancing software are configured correctly in your network environment, this request reaches the View Connection Server or security server host. With this connection, users are authenticated and a desktop is selected, but users have not yet connected to View desktops.

When users connect to View desktops, by default View Client makes a second connection to the View Connection Server or security server host. This connection is called the tunnel connection because it provides a secure tunnel for carrying RDP and other data over HTTPS.

When users connect to View desktops with the PCoIP display protocol, View Client can make a further connection to the PCoIP Secure Gateway on the View Connection Server or security server host. The PCoIP Secure Gateway ensures that only authenticated users can communicate with View desktops over PCoIP.

When the secure tunnel or PCoIP Secure Gateway is disabled, View desktop sessions are established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server or security server host. This type of connection is called a direct connection.

Desktop sessions that use direct connections remain connected even if View Connection Server is no longer running.

Typically, to provide secure connections for external clients that connect to a security server or View Connection Server host over a WAN, you enable both the secure tunnel and the PCoIP Secure Gateway. You can disable the secure tunnel and the PCoIP Secure Gateway to allow internal, LAN-connected clients to establish direct connections to View desktops.

Certain View Client endpoints, such as thin clients, do not support the tunnel connection and use direct connections for RDP data, but do support the PCoIP Secure Gateway for PCoIP data.

SSL is required for all client connections to View Connection Server and security server hosts.

Configure the PCoIP Secure Gateway and Secure Tunnel Connections

You use View Administrator to configure the use of the secure tunnel and PCoIP Secure Gateway. These components ensure that only authenticated users can communicate with View desktops.

Clients that use the PCoIP display protocol can use the PCoIP Secure Gateway. Clients that use the RDP display protocol can use the secure tunnel.

IMPORTANT A typical network configuration that provides secure connections for external clients includes a security server. To enable or disable the secure tunnel and PCoIP Secure Gateway on a security server, you must edit the View Connection Server instance that is paired with the security server.

In a network configuration in which external clients connect directly to a View Connection Server host, you enable or disable the secure tunnel and PCoIP Secure Gateway by editing that View Connection Server instance in View Administrator.

Prerequisites

- If you intend to enable the PCoIP Secure Gateway, verify that the View Connection Server instance and paired security server are View 4.6 or later.
- If you pair a security server to a View Connection Server instance on which you already enabled the PCoIP Secure Gateway, verify that the security server is View 4.6 or later.

Procedure

1 In View Administrator, select **View Configuration > Servers**.

2 In the View Connection Servers panel, select a View Connection Server instance and click **Edit**.

3 Configure use of the secure tunnel.

Option	Description
Disable the secure tunnel	Deselect **Use secure tunnel connection to desktop**.
Enable the secure tunnel	Select **Use secure tunnel connection to desktop**.

The secure tunnel is enabled by default.

4 Configure use of the PCoIP Secure Gateway.

Option	Description
Enable the PCoIP Secure Gateway	Select **Use PCoIP Secure Gateway for PCoIP connections to desktop**
Disable the PCoIP secure Gateway	Deselect **Use PCoIP Secure Gateway for PCoIP connections to desktop**

The PCoIP Secure Gateway is disabled by default.

5 Click **OK** to save your changes.

Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections

To use the secure tunnel, a client system must have access to an IP address, or a fully qualified domain name (FQDN) that it can resolve to an IP address, that allows the client to reach a View Connection Server or security server host. To use the PCoIP Secure Gateway, a client system must have access to an IP address that allows the client to reach a View Connection Server or security server host.

Using Tunnel Connections From External Locations

By default, a View Connection Server or security server host can be contacted only by tunnel clients that reside within the same network and are therefore able to locate the requested host.

Many organizations require that users can connect from an external location by using a specific IP address or client-resolvable domain name, and a specific port. This information might or might not resemble the actual address and port number of the View Connection Server or security server host. The information is provided to a client system in the form of a URL. For example:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

To use addresses like these in View Manager, you must configure the View Connection Server or security server host to return an external URL instead of the host's FQDN.

Configuring External URLs

You configure two external URLs. One URL allows client systems to make tunnel connections. The other allows client systems that use PCoIP to make secure connections through the PCoIP Secure Gateway. You must specify the PCoIP external URL as an IP address, which allows client systems to connect from an external location.

If your network configuration includes security servers, provide external URLs for the security servers. External URLs are not required on the View Connection Server instances that are paired with the security servers.

The process of configuring the external URLs is different for View Connection Server instances and security servers.

- For a View Connection Server instance, you set the external URLs by editing View Connection Server settings in View Administrator.
- For a security server, you set the external URLs when you run the View Connection Server installation program. You can use View Administrator to modify an external URL for a security server.

Set the External URLs for a View Connection Server Instance

You use View Administrator to configure the external URLs for a View Connection Server instance.

Both the secure tunnel external URL and PCoIP external URL must be the addresses that client systems use to reach this View Connection Server instance. For example, do not specify the secure tunnel external URL for this instance and the PCoIP external URL for a paired security server.

Procedure

1 In View Administrator, click **View Configuration > Servers**.

2 In the View Connection Servers panel, select a View Connection Server instance and click **Edit**.

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

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

For example: **`https://view.example.com:443`**

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

---

4 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach this View Connection Server host. You can type into the text box only if a PCoIP Secure Gateway is installed on the View Connection Server instance.

5 Click **OK**.

Modify the External URLs for a Security Server

You use View Administrator to modify the external URLs for a security server.

You initially configure the external URLs for a security server in the View Connection Server installation program.

Both the secure tunnel external URL and PCoIP external URL must be the addresses that client systems use to reach this security server. For example, do not specify the secure tunnel external URL for this security server and the PCoIP external URL for a paired View Connection Server instance.

Prerequisites

Verify that the version of the security server is View Connection Server 4.6 or later.

Procedure

1 In View Administrator, select **View Configuration > Servers**.

2 In the Security Servers panel, select the security server and click **Edit**.

The **Edit** button is unavailable if the security server is not upgraded to View Connection Server 4.6 or later.

3 Type the Secure Tunnel external URL in the **External URL** text box.

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

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

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

---

4 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach this security server. You can type into the text box only if a PCoIP Secure Gateway is installed on the security server.

5 Click **OK** to save your changes.

View Administrator sends the updated external URLs to the security server. You do not need to restart the security server service for the changes to take effect.

Sizing Windows Server Settings to Support Your Deployment

To support a large deployment of View Manager desktops, you can configure the Windows Server computers on which you install View Connection Server. On each computer, you can size the Windows page-file.

On 64-bit Windows Server 2008 computers, the ephemeral ports, TCB hash table, and Java Virtual Machine settings are sized by default. These adjustments ensure that the computers have adequate resources to run correctly with the expected user load.

By default, the system can create a maximum of approximately 16,000 ephemeral ports that run concurrently on Windows Server 2008. 16,000 ephemeral ports can support more than 2,000 concurrent client connections, the maximum supported number for a View Connection Server instance.

On Windows Server 2008 computers, you do not need to increase the maximum size of the TCB hash table. Windows Server 2008 fully tunes this value by default.

For hardware and memory requirements for View Connection Server, see "Hardware Requirements for View Connection Server," on page 8.

For hardware and memory recommendations for using View Connection Server in a large View deployment, see "View Connection Server Maximums and Virtual Machine Configuration" in *VMware View Architecture Planning*.

Sizing the Java Virtual Machine

The View Connection Server installer sizes the Java Virtual Machine (JVM) heap memory on View Connection Server computers to support a large number of concurrent View desktop sessions.

On a 64-bit Windows Server computer with at least 10GB of memory, the installer configures a JVM heap size of 2GB for the View Secure Gateway Server component. This configuration supports approximately 2,000 concurrent tunnel sessions, the maximum number that View Connection Server can support. There is no benefit in increasing the JVM heap size on a 64-bit computer with 10GB of memory.

NOTE On a 64-bit View Connection Server computer, 10GB of memory is recommended for deployments of 50 or more View desktops. Configure less than 10GB of memory for small, proof-of-concept deployments only.

If a 64-bit computer has less than 10GB of memory, the installer configures a JVM heap size of 512MB for the View Secure Gateway Server component. If the computer has the required minimum of 4GB of memory, this configuration supports approximately 500 concurrent tunnel sessions. This configuration is more than adequate to support small, proof-of-concept deployments.

If you increase a 64-bit computer's memory to 10GB to support a larger deployment, View Connection Server does not increase the JVM heap size. To adust the JVM heap size to the recommended value, reinstall View Connection Server.

IMPORTANT Do not change the JVM heap size on 64-bit Windows Server computers. Changing this value might make View Connection Server behavior unstable. On 64-bit computers, the View Connection Server installer sets the JVM heap size to accord with the physical memory. If you change the physical memory on a 64-bit View Connection Server computer, reinstall View Connection Server to reset the JVM heap size.

Configure the System Page-File Settings

You can optimize the virtual memory on the Windows Server computers on which your View Connection Server instances are installed by changing the system page-file settings.

When Windows Server is installed, Windows calculates an initial and maximum page-file size based on the physical memory installed on the computer. These default settings remain fixed even after you restart the computer.

If the Windows Server computer is a virtual machine, you can change the memory size through vCenter Server. However, if Windows uses the default setting, the system page-file size does not adjust to the new memory size.

Procedure

1 On the Windows Server computer on which View Connection Server is installed, navigate to the Virtual Memory dialog box.

   By default, **Custom size** is selected. An initial and maximum page-file size appear.

2 Click **System managed size**.

Windows continually recalculates the system page-file size based on current memory use and available memory.

Creating an Event Database

9

You create an event database to record information about View Manager events. If you do not configure an event database, you must look in the log file to get information about events, and the log file contains very limited information.

This chapter includes the following topics:

Add a Database and Database User for View Events

You create an event database by adding it to an existing database server. You can then use enterprise reporting software to analyze the events in the database.

The database server for the event database can reside on a View Connection Server host itself or on a dedicated server. Alternatively, you can use a suitable existing database server, such as a server that hosts a View Composer database.

NOTE You do not need to create an ODBC data source for this database.

Prerequisites

- Verify that you have a supported Microsoft SQL Server or Oracle database server on a system that a View Connection Server instance has access to. For a list of supported database versions, see "Database Requirements for View Composer," on page 10.
- Verify that you have the required database privileges to create a database and user on the database server.
- If you are not familiar with the procedure to create databases on Microsoft SQL Server database servers, review the steps in "Add a View Composer Database to SQL Server," on page 32.
- If you are not familiar with the procedure to create databases on Oracle database servers, review the steps in "Add a View Composer Database to Oracle 11g or 10g," on page 34.

Procedure

1 Add a new database to the server and give it a descriptive name such as ViewEvents.

2 Add a user for this database that has permission to create tables, views, and, in the case of Oracle, triggers and sequences, as well as permission to read from and write to these objects.

For a Microsoft SQL Server database, do not use the Integrated Windows Authentication security model method of authentication. Be sure to use the SQL Server Authentication method of authentication.

The database is created, but the schema is not installed until you configure the database in View Administrator.

What to do next

Follow the instructions in "Configure the Event Database," on page 104.

Prepare an SQL Server Database for Event Reporting

Before you can use View Administrator to configure an event database on Microsoft SQL Server, you must configure the correct TCP/IP properties and verify that the server uses SQL Server Authentication.

Prerequisites

- Create an SQL Server database for event reporting. See "Add a Database and Database User for View Events," on page 103.
- Verify that you have the required database privileges to configure the database.
- Verify that the database server uses the SQL Server Authentication method of authentication. Do not use Windows Authentication.

Procedure

1 Open SQL Server Configuration Manager and expand **SQL Server*YYYY*Network Configuration**.

2 Select **Protocols for*server_name***.

3 In the list of protocols, right-click **TCP/IP** and select **Properties.**

4 Set the **Enabled** property to **Yes.**

5 Verify that a port is assigned or, if necessary, assign one.

For information on the static and dynamic ports and how to assign them, see the online help for the SQL Server Configuration manager.

6 Verify that this port is not blocked by a firewall.

What to do next

Use View Administrator to connect the database to View Connection Server. Follow the instructions in "Configure the Event Database," on page 104.

Configure the Event Database

The event database stores information about View events as records in a database rather than in a log file.

You configure an event database after installing a View Connection Server instance. You need to configure only one host in a View Connection Server group. The remaining hosts in the group are configured automatically.

NOTE The security of the database connection between the View Connection Server instance and an external database is the responsibility of the administrator, although event traffic is limited to information about the health of the View environment. If you want to take extra precautions, you can secure this channel through IPSec or other means, or you can deploy the database locally on the View Connection Server computer.

You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *VMware View Integration* document.

You can also generate View events in `Syslog` format so that the event data can be accessible to third-party analytics software. You use the `vdmadmin` command with the `–I` option to record View event messages in `Syslog` format in event log files. See "Generating View Event Log Messages in Syslog Format Using the -I Option" in the *VMware View Administration* document.

Prerequisites

You need the following information to configure an event database:

- The DNS name or IP address of the database server.
- The type of database server: Microsoft SQL Server or Oracle.
- The port number that is used to access the database server. The default is 1521 for Oracle and 1433 for SQL Server. For SQL Server, if the database server is a named instance or if you use SQL Server Express, you might need to determine the port number. See the Microsoft KB article about connecting to a named instance of SQL Server, at http://support.microsoft.com/kb/265808.
- The name of the event database that you created on the database server. See "Add a Database and Database User for View Events," on page 103.
- The username and password of the user you created for this database. See "Add a Database and Database User for View Events," on page 103.

  Use SQL Server Authentication for this user. Do not use the Integrated Windows Authentication security model method of authentication.
- A prefix for the tables in the event database, for example, VE_. The prefix enables the database to be shared among View installations.

  NOTE You must enter characters that are valid for the database software you are using. The syntax of the prefix is not checked when you complete the dialog box. If you enter characters that are not valid for the database software you are using, an error occurs when View Connection Server attempts to connect to the database server. The log file indicates all errors, including this error and any others returned from the database server if the database name is invalid.

Procedure

1 In View Administrator, select **View Configuration > Event Configuration**.

2 In the **Event Database** section, click **Edit**, enter the information in the fields provided, and click **OK**.

3 (Optional) In the Event Settings window, click **Edit**, change the length of time to show events and the number of days to classify events as new, and click **OK**.

  These settings pertain to the length of time the events are listed in the View Administrator interface. After this time, the events are only available in the historical database tables.

  The Database Configuration window displays the current configuration of the event database.

4 Select **Monitoring > Events** to verify that the connection to the event database is successful.

  If the connection is unsuccessful, and error message appears. If you are using SQL Express or if you are using a named instance of SQL Server, you might need to determine the correct port number, as mentioned in the prerequisites.

In the View Administrator Dashboard, the System Component Status displays the event database server under the Reporting Database heading.

Installing and Starting View Client 10

You can obtain the Windows-based View Client installer either from the VMware Web site or from View Portal, a Web access page provided by View Connection Server. You can set various startup options for end users after View Client is installed.

For information about installing and using other View Clients, such as View Client for the Mac and View Client for iPad, see the documents that pertain to the specific client. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

This chapter includes the following topics:

Preparing View Connection Server for View Client

Administrators must perform specific tasks to enable end users to connect to View desktops.

Before end users can connect to View Connection Server or a security server and access a View desktop, you must configure certain pool settings and security settings:

- If you are using a security server, as VMware recommends, verify that you are using View Connection Server 4.6.1 and View Security Server 4.6.1 or later. See the *VMware View Installation* documentation for View 4.6 or later.
- If you plan to use a secure connection for client devices and if the secure connection is configured with a DNS host name for View Connection Server or a security server, verify that the client device can resolve this DNS name.

  To enable or disable the secure tunnel, in View Administrator, go to the Edit View Connection Server Settings dialog box and use the check box called **Use secure tunnel connection to desktop**.
- Verify that a virtual desktop pool has been created and that the user account you plan to use is entitled to access this View desktop. See the topics about creating desktop pools in the *VMware View Administration* documentation.

- To use two-factor authentication with View Client, such as RSA SecurID or RADIUS authentication, you must enable this feature on View Connection Server. RADIUS authentication is available with View 5.1 or later View Connection Server. For more information, see the topics about two-factor authentication in the *VMware View Administration* documentation.

Install the Windows-Based View Client or View Client with Local Mode

End users open View Client to connect to their virtual desktops from a physical machine. You can run a Windows-based installer file to install all components of View Client.

View Client with Local Mode lets end users download a copy of their virtual desktop to their local computer. End users can then use the virtual desktop even when they do not have a network connection. Latency is minimized and performance is enhanced.

View Client with Local Mode is the fully supported feature that in earlier releases was an experimental feature called View Client with Offline Desktop.

This procedure describes installing View Client by using an interactive installation wizard. If instead you would like to use the command-line, silent installation feature of the Microsoft Windows Installer (MSI), see "Install View Client Silently," on page 116.

Prerequisites

- Verify that the client system uses a supported operating system. See "Supported Operating Systems for Windows-Based View Client and View Client with Local Mode," on page 16.
- Verify that you can log in as an administrator on the client system.
- Verify that View Agent is not installed.
- Local mode prerequisites:
  - Verify that your license includes View Client with Local Mode.
  - Verify that none of the following products is installed: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Prerequisites for USB redirection:
  - Determine whether the person who uses the client device is allowed to access locally connected USB devices from a virtual desktop. If not, you can either deselect the **USB Redirection** component that the wizard presents or install the component but disable it using GPOs.

    VMware recommends that you always install the **USB Redirection** component and use GPOs to control USB access. This way, if you later want to enable USB redirection for a client, you will not need to re-install View Client. For information, see the topic "View Client Configuration ADM Template Settings" in the chapter about configuring policies in the *VMware View Administration* document.
  - If you plan to install the **USB Redirection** component, verify that the Windows Automatic Update feature is not turned off on the client computer.
- Determine whether to use the feature that lets end users log in to View Client and their virtual desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the View Connection Server instance and ultimately to the virtual desktop. Some client operating systems do not support this feature.
- If you do not want to require end users to supply the fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the FQDN so that you can supply it during installation.

Procedure

1 Log in to the client system as a user with administrator privileges.

2 On the client system, download the View Client installer file from the VMware product page at http://www.vmware.com/products/.

Select the appropriate installer file, where *xxxxxx* is the build number and *y.y.y* is the version number.

Option	Action
View Client on 64-bit operating systems	Select `VMware-viewclient-x86_64-y.y.y-xxxxxx.exe` for View Client. Select `VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe` for View Client with Local mode.
View Client on 32-bit operating systems	Select `VMware-viewclient-y.y.y-xxxxxx.exe` for View Client. Select `VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe` for View Client with Local Mode.

3 To start the View Client installation program, double-click the installer file.

4 Follow the prompts to install the components you want.

The VMware View Client service is installed on the Windows client computer. The service name for View Client is `wsnm.exe`. The service names for the USB components are `vmware-usbarbitrator.exe` and `vmware-view-usbd.exe`.

What to do next

Start the View Client and verify that you can log in to the correct virtual desktop. See "Log In to a View Desktop," on page 111 or "Install View Client by Using View Portal," on page 109.

Install View Client by Using View Portal

An expedient way of downloading and installing the View Client or View Client with Local Mode application is to open a browser and browse to the View Portal Web page. You can use View Portal to download the full View Client installer for both Windows and Mac client computers.

As an alternative to browsing to a VMware Download page to download View Client, you can browse to a View Connection Server URL. You can also configure settings so that the links on View Portal point to a different location than the VMware Download page.

Prerequisites

- If the links on View Portal must point to a different location than the VMware Downloads page, see "Configure the View Client Download Links Displayed in View Portal," on page 110.
- Verify that you have the URL for the View Connection Server instance.
- Verify that you can log in as an administrator on the client system.
- Verify that a virtual desktop has been created and that the user account you plan to use is entitled to access this desktop.
- Verify that the client system uses a supported operating system. See "Supported Operating Systems for Windows-Based View Client and View Client with Local Mode," on page 16.
- Verify that View Agent is not installed.
- Local mode prerequisites:
  - Verify that your license includes View Client with Local Mode.
  - Verify that none of the following products is installed: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.

- Prerequisites for USB redirection:
  - Determine whether the person who uses the client device is allowed to access locally connected USB devices from a virtual desktop. If not, you can either deselect the **USB Redirection** component that the wizard presents or install the component but disable it using GPOs.

    VMware recommends that you always install the **USB Redirection** component and use GPOs to control USB access. This way, if you later want to enable USB redirection for a client, you will not need to re-install View Client. For information, see the topic "View Client Configuration ADM Template Settings" in the chapter about configuring policies in the *VMware View Administration* document.
  - If you plan to install the **USB Redirection** component, verify that the Windows Automatic Update feature is not turned off on the client computer.

Procedure

1 Log in to the client system as a user with administrator privileges.

2 Open a browser and enter the URL of the View Connection Server instance that provides access to the virtual desktop.

  In the URL, be sure to use `https` rather than `http`.

3 Click the appropriate link for the type of operating system you have (32-bit or 64-bit) and the type of View Client to install (with or without Local Mode).

4 When prompted, save the installer file to your client system.

5 To start the View Client installation program, double-click the installer file.

6 Follow the prompts to install the components you want.

What to do next

Connect to the View desktop. See "Log In to a View Desktop," on page 111.

Configure the View Client Download Links Displayed in View Portal

By default, when you open a browser and enter the URL of a View Connection Server instance, the View Portal page that appears contains links to the VMware Download site for downloading View Client. You can change the default.

The default View Client links on View Portal ensure that you are directed to the latest compatible View Client installers. In some cases, however, you might want to have the links point to an internal Web server, or you might want to make specific client versions available on your own View Connection Server. You can reconfigure the page to point to a different URL.

Prerequisites

- Download the installer files for the types of View Client you want to use in your environment. The URL to the View Clients download page is https://www.vmware.com/go/viewclients.
- Determine which HTTP server will host the installer files. The files can reside on a View Connection Server instance or on another HTTP server.

Procedure

1 On the HTTP server where the installer files will reside, create a folder for the installer files.

  For example, to place the files in a `downloads` folder on the View Connection Server host, in the default installation directory, use the following path:

  ```
  C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
  ```

The links to the files would then use URLs with the format `https://server-name/downloads/client-installer-file-name`. For example, a server with the name `view.mycompany.com` would use the following URL for View Client for Windows: `https://view.mycompany.com/downloads/VMware-viewclient.exe`. In this example, the folder named `downloads` is located in the `webapps` root folder.

2 Copy the View Client installer files into the folder.

If the folder resides on View Connection Server, you can replace any files in this folder without having to restart the VMware View Connection Server service.

3 On the View Connection Server machine, copy the `portal-links.properties` file and the `portal.properties` file located in *install-path*`\Server\Extras\PortalExamples`.

4 Create a `portal` folder the directory `C:\ProgramData\VMware\VDM`, and copy the `portal-links.properties` and `portal.properties` files into the `portal` folder.

5 Edit `C:\ProgramData\VMware\VDM\portal\portal-links.properties` file to point to the new location of the installer files.

You can edit the lines in this file and add to them if you need to create more links. You can also delete lines.

The following examples show properties for creating two links for View Client for Windows and two links for View Client for Linux:

```
link.win=https://server-name/downloads/VMware-viewclient-x86_64-y.y.y-XXXX.exe#win
link.win.1=https://server-name/downloads/VMware-viewclient-y.y.y-XXXX.exe#win
link.linux=https://server-name/downloads/VMware-viewclient-x86_64-y.y.y-XXXX.rpm#linux
link.linux.1=https://server-name/downloads/VMware-viewclient-y.y.y-XXXX.tar.gz#linux
```

In this example, *y.y.y-XXXX* indicates the version and build number. The `win` text at the end of the line indicates that this link should appear in the browser if the client has a Windows operating system. Use `win` for Windows, `linux` for Linux, and `mac` for Mac OS X.

6 Edit `C:\ProgramData\VMware\VDM\portal\portal.properties` file to specify the text to display for the links.

These lines appear in the section of the file called `# keys based on key names in portal-links.properties`.

The following example shows the text that corresponds to the links specified for `link.win` and `link.win.1`:

```
text.win=View Client for Windows 32 bit Client users
text.win.1=View Client for Windows 64 bit Client users
```

7 Restart the VMware View Connection Server service.

When end users enter the URL for View Connection Server, they see links with the text you specified. The links point to the locations you specified.

Log In to a View Desktop

Before you have end users access their virtual desktops, test that you can log in to a virtual desktop from a client device. You can start View Client from the **Start** menu or a desktop shortcut on the client system.

In environments where a network connection is available, the user session is authenticated by View Connection Server.

Prerequisites

- Obtain the credentials you need to log in, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).

- Obtain the domain name for logging in.
- Perform the administrative tasks described in "Preparing View Connection Server for View Client," on page 107.
- If you are outside the corporate network and are not using a security server to access the virtual desktop, verify that your client device is set up to use a VPN connection and turn that connection on.

  IMPORTANT VMware recommends using a security server rather than a VPN.

- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the virtual desktop. You also need the port number if the port is not 443.
- If you plan to use the RDP display protocol to connect to a View desktop, verify that the AllowDirectRDP View Agent group policy setting is enabled.
- If your administrator has allowed it, you can configure the certificate checking mode for the SSL certificate presented by View Connection Server.

  To determine which mode to use, see "Configuring Certificate Checking in View Client for Windows," on page 81.

Procedure

1 Double-click the **VMware View Client** desktop shortcut or click **Start > Programs > VMware > VMware View Client**.

2 In the **Connection Server** drop-down menu, enter the host name of View Connection Server or a security server.

3 Verify that the other optional settings in the dialog box appear as you configured them.

Option	Description
Log in as current user	This check box is displayed or hidden according to the global setting in View Administrator. Do not select this check box if you plan to check out the View desktop for use in local mode.
Port	If you leave this field blank, the default port 443 is used.
Autoconnect	If you select this check box, the next time you start View Client, the **Connection Server** field is disabled and you are connected to the server specified when you selected the **Autoconnect** check box. To deselect this check box, cancel the next dialog box that appears and click **Options** to display and change this setting.
Configure SSL	If your View administrator has allowed it, you can set the certificate checking mode by clicking this link, as mentioned in the prerequisites to this procedure.

4 Click **Connect**.

You might see a message that you must confirm before the login dialog box appears.

5 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the user name and passcode and click **Continue**.

6 Enter the credentials of a user who is entitled to use at least one desktop pool, select the domain, and click **Login**.

If you type the user name using the format **`user@domain`**, the name is treated as a user principal name (UPN) because of the @ sign, and the domain drop-down menu is disabled.

For information about creating desktop pools and entitling users to pools, see *VMware View Administration* document.

7 In the list of desktops that appears, select a desktop.

   a (Optional) In the **Display** drop-down menu, select the window size for displaying the View desktop.

      The display setting is retained as the default the next time you open the desktop.

   b (Optional) To select a display protocol, click the down-arrow next to a desktop in the list, click **Display Protocol**, and select the protocol.

      This choice is available only if your View administrator has enabled it. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content on the LAN or across the WAN.

      NOTE If you are using smart card credentials to log in and you want to switch protocols, you must log off and log on again.

      The protocol setting is retained as the default the next time you open the desktop.

8 Click **Connect**.

   You are connected to the desktop.

After you are connected, the client window appears.

If authentication to View Connection Server fails or if View Client cannot connect to a desktop, perform the following tasks:

- Determine whether View Connection Server is configured not to use SSL. View Client requires SSL connections. Check whether the global setting in View Administrator for the **Use SSL for client connections** check box is deselected. If so, you must either select the check box, so that SSL is used, or set up your environment so that clients can connect to an HTTPS enabled load balancer or other intermediate device that is configured to make an HTTP connection to View Connection Server.
- Verify that the security certificate for View Connection Server is working properly. If it is not, in View Administrator, you might also see that the View Agent on desktops is unreachable and the Transfer Server status shows that it is not ready. These are symptoms of additional connection problems caused by certificate problems.
- Verify that the tags set on the View Connection Server instance allow connections from this user. See the *VMware View Administration* document.
- Verify that the user is entitled to access this desktop. See the *VMware View Administration* document.
- If you are using the RDP display protocol to connect to a View desktop, verify that the client computer allows remote desktop connections.

What to do next

- Configure startup options.

  If you do not want to require end users to provide the host name of View Connection Server, or if you want to configure other startup options, use the View Client command-line options to create a desktop shortcut.

  See the *VMware View Administration* document.

- Check out a desktop that can be used in local mode.

  End users can determine if a desktop is eligible for checkout by clicking the down-arrow next to the desktop in the list provided by View Client with Local Mode. If the desktop can be used in local mode, the **Check out** option appears in the context menu. Only the user who checks out the desktop can access it, even if a group is entitled to access the desktop.

Set Printing Preferences for the Virtual Printer Feature on Windows Clients

The virtual printing feature lets end users use local or network printers from a View desktop without requiring that additional print drivers be installed in the View desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on.

After a printer is added on the local Windows computer, View adds that printer to the list of available printers on the View desktop. No further configuration is required. Users who have administrator privileges can still install printer drivers on the View desktop without creating a conflict with the virtual printer component.

IMPORTANT This feature is not available for the following types of printers:

- USB printers that are using the USB redirection feature to connect to a virtual USB port in the View desktop

  You must disconnect the USB printer from the View desktop in order to use the virtual printing feature with it.

- The Windows feature for printing to a file

  Selecting the **Print to file** check box in a Print dialog box does not work. Using a printer driver that creates a file does work. For example, you can use a PDF writer to print to a PDF file.

Prerequisites

Verify that the Virtual Printing component of View Agent is installed on the View desktop. In the View desktop file system, the drivers are located in `C:\Program Files\Common Files\VMware\Drivers\Virtual Printer`.

Installing View Agent is one of the tasks required for preparing a virtual machine to be used as a View desktop. For more information, see the *VMware View Administration* document.

Procedure

1 In the View desktop, click **Start > Settings > Printers and Faxes**.

2 In the Printers and Faxes window, right-click any of the locally available printers and select **Properties**.

  On Windows 7 desktops, you might see only the default printer, even though other printers are available. To see the other printers, right-click the default printer and point to **Printer properties**.

  In the View desktop, virtual printers appear as *<printer_name>#:<number>*.

3 In the Print Properties window, click the **ThinPrint Device Setup** tab and specify which settings to use.

4 On the **General** tab, click **Printing Preferences** and edit the page and color settings.

5 On the **Advanced** tab, set preferences for double-sided printing and portrait (long edge) or landscape (short edge) printing.

6 To preview each printout on the host, enable **Preview on client before printing.**

  From this preview, you can use any printer with all its available properties.

7 On the **Adjustment** tab, review the settings for automatic print adjustment.

  VMware recommends that you retain the default settings.

8 Click **OK**.

Using USB Printers

In a View environment, virtual printers and redirected USB printers can work together without conflict.

A USB printer is a printer that is attached to a USB port on the local client system. To send print jobs to a USB printer, you can either use the USB redirection feature or use the virtual printing feature. USB printing can sometimes be faster than virtual printing, depending on network conditions.

- You can use the USB redirection feature to attach a USB printer to a virtual USB port in the View desktop as long as the required drivers are also installed on the View desktop.

  If you use this redirection feature the printer is no longer attached to the physical USB port on the client and this is why the USB printer does not appear in the list of local printers that the virtual printing feature displays. This also means that you can print to the USB printer from the View desktop but not from the local client machine.

  In the View desktop, USB printers appear as <*printer_name*>.

- On Windows clients, you can alternatively use the virtual printing feature to send print jobs to a USB printer. If you use the virtual printing feature you can print to the USB printer from both the View desktop and the local client, and you do not need to install print drivers on the View desktop.

Installing View Client Silently

You can install View Client silently by typing the installer filename and installation options at the command line. With silent installation, you can efficiently deploy View components in a large enterprise.

Set Group Policies to Allow Silent Installation of View Client with Local Mode

Before you can install View Client with Local Mode silently, you must configure Microsoft Windows group policies to allow installation with elevated privileges.

You do not have to set these group policies to install View Client silently. These policies are required only for View Client with Local Mode.

You must set Windows Installer group policies for computers and for users on the client computer.

Prerequisites

Verify that you have administrator privileges on the Windows client computer on which you will install View Client with Local Mode.

Procedure

1 Log in to the client computer and click **Start > Run**.

2 Type **`gpedit.msc`** and click **OK**.

3 In the Group Policy Object Editor, click **Local Computer Policy > Computer Configuration**.

4 Expand **Administrative Templates**, expand **Windows Components**, open the **Windows Installer** folder, and double-click **Always install with elevated privileges**.

5 In the **Always Install with Elevated Privileges Properties** window, click **Enabled** and click **OK**.

6 In the left pane, click **User Configuration**.

7 Expand **Administrative Templates**, expand **Windows Components**, open the **Windows Installer** folder, and double-click **Always install with elevated privileges**.

8 In the **Always Install with Elevated Privileges Properties** window, click **Enabled** and click **OK**.

What to do next

Install View Client with Local Mode silently.

Install View Client Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install View Client or View Client with Local Mode on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

Prerequisites

- Verify that the client system uses a supported operating system. See "Supported Operating Systems for Windows-Based View Client and View Client with Local Mode," on page 16.
- Verify that you can log in as an administrator on the client system.
- Verify that View Agent is not installed.
- Local mode prerequisites:
  - Verify that the Windows Installer group policies that are required for silent installation are configured on the client computer. See "Set Group Policies to Allow Silent Installation of View Client with Local Mode," on page 115.
  - Verify that your license includes View Client with Local Mode.
  - Verify that none of the following products is installed: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Determine whether to use the feature that lets end users log in to View Client and their virtual desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the View Connection Server instance and ultimately to the virtual desktop. Some client operating systems do not support this feature.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 59.
- Familiarize yourself with the silent installation (MSI) properties available with View Client. See "Silent Installation Properties for View Client," on page 117.
- Determine whether to allow end users to access locally connected USB devices from their virtual desktops. If not, set the MSI property, `ADDLOCAL`, to the list of features of interest and omit the USB feature. For details, see "Silent Installation Properties for View Client," on page 117.
- If you do not want to require end users to supply the fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the FQDN so that you can supply it during installation.

Procedure

1 On the client system, download the View Client installer file from the VMware product page at http://www.vmware.com/products/.

Select the appropriate installer file, where *xxxxxx* is the build number and *y.y.y* is the version number.

Option	Action
View Client on 64-bit operating systems	Select `VMware-viewclient-x86_64-y.y.y-xxxxxx.exe` for View Client. Select `VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe` for View Client with Local mode.
View Client on 32-bit operating systems	Select `VMware-viewclient-y.y.y-xxxxxx.exe` for View Client. Select `VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe` for View Client with Local Mode.

2 Open a command prompt on the Windows client computer.

3 Type the installation command on one line.

This example installs View Client with single sign-on and USB redirection features. A default View Connection Server instance is configured for View Client users: `VMware-viewclient-y.y.y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress VDM_SERVER=cs1.companydomain.com ADDLOCAL=Core,TSSO,USB"`

This example installs View Client with Local Mode: `VMware-viewclientwithlocal-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,MVDI"`

NOTE The `Core` feature is mandatory.

The VMware View Client service is installed on the Windows client computer.

What to do next

Start the View Client and verify that you can log in to the correct virtual desktop. See "Log In to a View Desktop," on page 111 or "Install View Client by Using View Portal," on page 109.

Silent Installation Properties for View Client

You can include specific properties when you silently install View Client from the command line. You must use a *PROPERTY=value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 10-1 shows the View Client silent installation properties that you can use at the command-line.

Table 10-1. MSI Properties for Silently Installing View Client

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Client software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles%\VMware\VMware View\Client`
VDM_SERVER	The fully qualified domain name (FQDN) of the View Connection Server instance to which View Client users connect by default. When you configure this property, View Client users do not have to supply this FQDN. For example: `VDM_SERVER=cs1.companydomain.com` This MSI property is optional.	None

Table 10-1. MSI Properties for Silently Installing View Client (Continued)

MSI Property	Description	Default Value
DESKTOP_SHORTCUT	Configures a desktop shortcut icon for View Client. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.	1
QUICKLAUNCH_SHORTCUT	Configures a shortcut icon on the quick-launch tray for View Client. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.	1
STARTMENU_SHORTCUT	Configures a shortcut for View Client in the Start menu. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.	1

In a silent installation command, you can use the MSI property, `ADDLOCAL=`, to specify features that the View Client installer configures. Each silent-installation feature corresponds to a setup option that you can select during an interactive installation.

Table 10-2 shows the View Client features you can type at the command line and the corresponding interactive-installation options.

Table 10-2. View Client Silent Installation Features and Interactive Custom Setup Options

Silent Installation Feature	Custom Setup Option in an Interactive Installation
Core If you specify individual features with the MSI property, `ADDLOCAL=`, you must include **`Core`**. If you specify `ADDLOCAL=ALL`, all View Client and View Client with Local Mode features, including Core, are installed.	None. During an interactive installation, the core View Client functions are installed by default.
MVDI Use this feature when you install View Client with Local Mode and specify individual features with `ADDLOCAL=`. If you specify `ADDLOCAL=ALL`, all View Client with Local Mode features, including MVDI, are installed.	None. When you install View Client with Local Mode interactively, the MVDI functions are installed by default. When you install View Client interactively, the MVDI functions are not available.
ThinPrint	Virtual Printing
TSSO	Single Sign-on (SSO)
USB	USB Redirection

Index

W