

# VMware View Installation Guide

View 4.5

View Manager 4.5

View Composer 2.5

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-000245-01

**vmware**<sup>®</sup>

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](mailto:docfeedback@vmware.com)

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

About This Book	5
<b>1 System Requirements for Server Components</b>	<b>7</b>
View Connection Server Requirements	7
View Administrator Requirements	9
View Composer Requirements	9
View Transfer Server Requirements	11
<b>2 System Requirements for Client Components</b>	<b>15</b>
Supported Operating Systems for View Agent	15
Supported Operating Systems for View Client and View Client with Local Mode	16
Hardware Requirements for Local Mode Desktops	16
Client Browser Requirements for View Portal	18
Remote Display Protocol and Software Support	18
Adobe Flash Requirements	21
Smart Card Authentication Requirements	21
<b>3 Preparing Active Directory</b>	<b>23</b>
Configuring Domains and Trust Relationships	23
Creating an OU for View Desktops	24
Creating OUs and Groups for Kiosk Mode Client Accounts	24
Creating Groups for View Users	24
Creating a User Account for vCenter Server	24
Create a User Account for View Composer	25
Configure the Restricted Groups Policy	25
Using View Group Policy Administrative Template Files	26
Prepare Active Directory for Smart Card Authentication	26
<b>4 Installing View Composer</b>	<b>29</b>
Prepare a View Composer Database	29
Install the View Composer Service	34
Configuring Your Infrastructure for View Composer	36
<b>5 Installing View Connection Server</b>	<b>37</b>
Installing the View Connection Server Software	37
Configuring User Accounts for vCenter Server and View Composer	51
Configuring View Connection Server for the First Time	54
Configuring View Client Connections	57
Sizing Windows Server Settings to Support Your Deployment	59

<b>6</b>	<b>Installing View Transfer Server</b>	<b>67</b>
	Install View Transfer Server	67
	Add View Transfer Server to View Manager	69
	Configure the Transfer Server Repository	70
	Firewall Rules for View Transfer Server	71
	Installing View Transfer Server Silently	71
<b>7</b>	<b>Configuring Certificate Authentication</b>	<b>75</b>
	Replacing the Default Certificate	75
	Add keytool and openssl to the System Path	76
	Export an Existing Microsoft IIS SSL Server Certificate	76
	Creating a New SSL Certificate	77
	Configure a View Connection Server Instance or Security Server to Use a New Certificate	80
	Configure a View Transfer Server Instance to Use a New Certificate	81
	Configure SSL for Client Connections	82
	Configure SSL for View Transfer Server Communications	82
	Using Group Policy to Configure Certificate Checking in View Client	83
<b>8</b>	<b>Creating an Event Database</b>	<b>85</b>
	Add a Database and Database User for View Events	85
	Prepare an SQL Server Database for Event Reporting	86
	Configure the Event Database	86
<b>9</b>	<b>Installing and Starting View Client</b>	<b>89</b>
	Install the Windows-Based View Client or View Client with Local Mode	89
	Start the Windows-Based View Client or View Client with Local Mode	90
	Install View Client by Using View Portal	92
	Install View Client on Mac OS X	93
	Start View Client on Mac OS X	94
	Set Printing Preferences for the Virtual Printer Feature	96
	Using USB Printers	97
	Installing View Client Silently	97
	<b>Index</b>	<b>101</b>

# About This Book

---

The *VMware View Installation Guide* explains how to install the VMware® View server and client components.

## Intended Audience

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

## VMware Technical Publications Glossary

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

## Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to [docfeedback@vmware.com](mailto:docfeedback@vmware.com).

## Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to <http://www.vmware.com/support/pubs>.

### Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to <http://www.vmware.com/support>.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to [http://www.vmware.com/support/phone\\_support.html](http://www.vmware.com/support/phone_support.html).

### Support Offerings

To find out how VMware support offerings can help meet your business needs, go to <http://www.vmware.com/support/services>.

### VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting

Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to <http://www.vmware.com/services>.

# 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,”](#) on page 7
- [“View Administrator Requirements,”](#) on page 9
- [“View Composer Requirements,”](#) on page 9
- [“View Transfer Server Requirements,”](#) on page 11

## 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 7  
You must install View Connection Server on a 32-bit or 64-bit 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 supported operating system.
- [Virtualization Software Requirements for View Connection Server](#) on page 8  
View Connection Server requires VMware virtualization software to function properly.
- [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 View Connection Server on a 32-bit or 64-bit 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	Dual processors
Networking	One or more 10/100Mbps network interface cards (NICs)	1Gbps NICs

**Table 1-1.** View Connection Server Hardware Requirements (Continued)

Hardware Component	Required	Recommended
Memory Windows Server 2008 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more View desktops
Memory Windows Server 2003 32-bit	2GB RAM or higher	6GB RAM for deployments of 50 or more View desktops, and enable Physical Address Extension (PAE) See the Microsoft KB article at <a href="http://support.microsoft.com/kb/283037">http://support.microsoft.com/kb/283037</a> .

These requirements also apply to additional 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 supported operating system.

[Table 1-2](#) lists the operating systems supported for View Connection Server.

These operating systems support all View Connection Server installation types, including standard, replicated, security-server, and View Transfer Server installations.

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

Operating System	Version	Edition	Service Pack
Windows Server 2008 R2	64-bit	Standard Enterprise	N/A
Windows Server 2003 R2	32-bit	Standard Enterprise	SP2
Windows Server 2003	32-bit	Standard Enterprise	SP2

**IMPORTANT** If you use a Windows Server 2003 operating system, enable Physical Address Extension (PAE). See the Microsoft KB article at <http://support.microsoft.com/kb/283037>.

## Virtualization Software Requirements for View Connection Server

View Connection Server requires VMware virtualization software to function properly.

- If you are using vSphere, you must have vSphere 4.0 Update 2 or vSphere 4.1.
- If you are using VMware Infrastructure, you must have VMware Infrastructure 3.5 Update 5 and VirtualCenter Server 2.5 Update 6.
- Both ESX and ESXi hosts are supported.

## 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 7
- Internet Explorer 8
- Firefox 3.0
- Firefox 3.5

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

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 and 32-bit operating systems with specific requirements and limitations. You must install View Composer on the same physical computer or virtual machine as vCenter Server.
- [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 vCenter Server computer.
- [Virtualization Software Requirements for View Composer Features](#) on page 11  
You must create linked-clone virtual machines on hosts that run ESX/ESXi 4 or later, and you must configure linked-clone pools in vSphere mode, to take advantage of several View Composer and vSphere features.

## Supported Operating Systems for View Composer

View Composer supports 64-bit and 32-bit operating systems with specific requirements and limitations. You must install View Composer on the same physical computer or virtual machine as vCenter Server.

### 64-Bit Operating Systems

Table 1-3 lists the 64-bit operating systems supported for View Composer. Standard and Enterprise editions are supported.

**Table 1-3.** 64-Bit Operating System Support for View Composer

vCenter Server Version	Operating System	Service Pack
4.1	Windows Server 2008 R2	N/A
4.1	Windows Server 2008	SP2
4.1	Windows Server 2003 R2	SP2
4.1	Windows Server 2003	SP2
4.0 Update 2	Windows Server 2008	SP2

### 32-Bit Operating Systems

Table 1-4 lists the 32-bit operating systems supported for View Composer. Standard and Enterprise editions are supported.

**Table 1-4.** 32-Bit Operating System Support for View Composer

vCenter Server Version	Operating System	Service Pack
4.0 Update 2	Windows Server 2003	SP2
2.5 Update 6	Windows Server 2003 R2	SP2
2.5 Update 6	Windows Server 2003	SP2

## 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 vCenter Server computer.

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 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 4.1	vCenter Server 4.0 U2	VC Server 2.5 U6
Microsoft SQL Server 2000 SP4 Standard	No	No	Yes
Microsoft SQL Server 2005 Express	Yes	Yes	Yes
Microsoft SQL Server 2005 SP3 Standard and Enterprise	Yes	Yes	Yes
Microsoft SQL Server 2008 SP1 Standard and Enterprise	Yes	Yes	No
Microsoft SQL Server 2008 SP1 Standard and Enterprise 64-bit	Yes	Yes	No
Oracle 9i Release 2	No	No	Yes
Oracle 10g Release 2	Yes	Yes	No
Oracle 11g Release 1	Yes	Yes	No

## Virtualization Software Requirements for View Composer Features

You must create linked-clone virtual machines on hosts that run ESX/ESXi 4 or later, and you must configure linked-clone pools in vSphere mode, to take advantage of several View Composer and vSphere features.

- Storing linked-clone virtual machines on local datastores
- Redirecting disposable data to separate, non-persistent disks
- Storing replicas and linked clones on separate datastores
- Creating pools from a parent virtual-machine snapshot that uses hardware version 7
- Using Sysprep customization specifications for linked-clone virtual machines.

In addition, Sysprep is supported for linked clones only on vSphere 4.1 software. You cannot use Sysprep on vSphere 4.0 or VMware Infrastructure 3.5 software.

## 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 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 the required amount of RAM.
- [Storage Requirements for View Transfer Server](#) on page 13  
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 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.



**CAUTION** You must configure the virtual machine that hosts View Transfer Server with an LSI Logic Parallel SCSI controller. You cannot use a SAS or VMware paravirtual controller.

On Windows Server 2008 virtual machines, the LSI Logic SAS controller is selected by default. You must change this selection to a BusLogic or LSI Logic controller before you install the operating system.

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

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 the required amount of RAM.

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

Operating System	Version	Edition	Service Pack	Minimum RAM
Windows Server 2008 R2	64-bit	Standard Enterprise	N/A	4GB
Windows Server 2003 R2	32-bit	Standard Enterprise	SP2	2GB
Windows Server 2003	32-bit	Standard Enterprise	SP2	2GB

**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 host where the View Transfer Server virtual machine is running.
- View Transfer Server can transfer a maximum of 60 disks concurrently.

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, each with 15 slots. This configuration allows 60 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.

View Client uses Microsoft Internet Explorer Internet settings, including proxy settings, when connecting to View Connection Server. Ensure that your Internet Explorer settings are accurate and that you can access the View Connection Server URL through Internet Explorer.

This chapter includes the following topics:

- [“Supported Operating Systems for View Agent,”](#) on page 15
- [“Supported Operating Systems for View Client and View Client with Local Mode,”](#) on page 16
- [“Hardware Requirements for Local Mode Desktops,”](#) on page 16
- [“Client Browser Requirements for View Portal,”](#) on page 18
- [“Remote Display Protocol and Software Support,”](#) on page 18
- [“Adobe Flash Requirements,”](#) on page 21
- [“Smart Card Authentication Requirements,”](#) on page 21

## 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](#) lists the operating systems supported for View Agent.

**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	N/A
Windows Vista	32-bit	Business and Enterprise	SP1 and SP2
Windows XP	32-bit	Professional	SP3
Windows 2008 R2 Terminal Server	64-bit	Standard	N/A
Windows 2008 Terminal Server	64-bit	Standard	SP2

**Table 2-1.** View Agent Operating System Support (Continued)

Guest Operating System	Version	Edition	Service Pack
Windows 2003 R2 Terminal Server	32-bit	Standard	SP2
Windows 2003 Terminal Server	32-bit	Standard	SP2

**IMPORTANT** If you use Windows 7 in a virtual machine, the virtual machine must be hosted on an ESX 4.0 or ESX 4.1 server. For ESX 4.0, the version must be ESX 4.0 Update 2 or higher. For ESX 4.1, the version must be ESX 4.1 or higher.

## Supported Operating Systems for 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 2-2 lists the operating systems supported for View Client.

**Table 2-2.** View Client Operating System Support

Operating System	Version	Edition	Service Pack
Windows 7	32-bit and 64-bit	Home, Enterprise, Professional, and Ultimate	N/A
Windows XP	32-bit	Home and Professional	SP3
Windows Vista	32-bit	Home, Business, Enterprise, and Ultimate	SP1 and SP2
Mac OS X Leopard 10.5	N/A	N/A	N/A
Mac OS X Snow Leopard 10.6	N/A	N/A	N/A

**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.

A Windows 7 or Windows Vista View desktop that is created on an ESX 3.5 host cannot produce 3D and Windows Aero effects. This limitation applies even when the desktop is checked out for local use on a Windows 7 or Windows Vista client computer. Windows Aero and 3D effects are available only if the View desktop is created using vSphere 4.x.

**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 2-3 describes the hardware requirements for various View desktop operating systems.

**Table 2-3.** Processor Requirements

Client Computer Requirement	Description
PC	Standard x86 or x86 64-compatible
Number of CPUs	Multiprocessor systems are supported
CPU speed	For a Windows XP local desktop, 1.3GHz or faster; 1.6 GHz recommended For a Windows 7 desktop, 1.6GHz or faster; for Aero effects, 2.2GHz 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 For Windows 7 Aero: Althon 4200+ and above
64-bit operating systems	Intel Pentium 4 and Core 2, and Core i7 processors with EM64T and Intel Virtualization Technology 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

## 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 spaced 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 32-bit client computers is 8GB and 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.

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

For CPU and GPU requirements to support Windows 7 Aero, see the table in [“PC Hardware,”](#) on page 16.

## Client Browser Requirements for View Portal

From a client system, you can browse to a View Connection Server instance and use View Portal to install a Mac-based View Client, a Windows-based View Client, or View Client with Local Mode. If you use Internet Explorer, View Portal indicates when a new version of View Client is available for download.

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

- Internet Explorer 7
- Internet Explorer 8
- Firefox 3.0
- Firefox 3.5

If you use Internet Explorer and you already have View Client installed, if the version available from View Connection Server is newer than that installed on the client device, you can choose to upgrade. If the version is the same as that on the client device, View Portal starts the View Client installed on the local system.

---

**NOTE** View Portal does not support Linux. A native client for Linux is available only through certified VMware partners.

---

## 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), PCoIP from VMware, and Hewlett-Packard Remote Graphics Software (RGS) display protocols.

- [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 20  
Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.
- [HP RGS Software](#) on page 20  
View Client supports connections to desktops using HP RGS when connecting to HP Blade PCs, HP Workstations, and HP Blade Workstations. VMware does not bundle or license HP RGS with View. You must contact HP to license a copy of HP RGS version 5.2.5 to use with View.
- [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:

- Remote connections using Virtual Private Networks (VPNs) are supported.
- 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 Windows clients with the View Client operating system versions listed in [“Supported Operating Systems for View Client and View Client with Local Mode,”](#) on page 16 are supported.
- 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.
- Adobe Flash bandwidth reduction is supported.
- Audio redirection with dynamic audio quality adjustment for LAN and WAN is supported.
- 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.
- 32-bit color is supported for virtual displays.
- ClearType fonts are supported.
- Text copy and paste between the local system and the desktop is supported, up to 64 kilobytes. 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.

### PCoIP Limitations

PCoIP has the following limitation: View clients that use PCoIP can connect to security servers, but PCoIP sessions with the desktop ignore the security server. PCoIP uses UDP for streaming audio and video, but security servers support only TCP.

## 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

## Client Hardware Requirements

Client hardware requirements include the following:

- 800MHz or higher processor speed.
- x86-based processor with SSE2 extensions.
- See the *VMware View Architecture Planning Guide* for information about RAM sizing for specific monitor configurations.

## Microsoft RDP

Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.

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

- For Windows XP and Windows XPe systems, you should use Microsoft RDC 6.x.
- Windows Vista comes with RDC 6.x installed.
- Windows 2000 supports RDC 5.0. It does not support RDC 6.x.
- 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 6.1 from the Microsoft Web site.

## HP RGS Software

View Client supports connections to desktops using HP RGS when connecting to HP Blade PCs, HP Workstations, and HP Blade Workstations. VMware does not bundle or license HP RGS with View. You must contact HP to license a copy of HP RGS version 5.2.5 to use with View.

HP RGS consists of a server-side component, called RGS Sender, and a client-side component, the RGS Receiver. Before you can configure View to use HP RGS, you must install HP RGS Sender in the remote desktop operating system and install HP RGS Receiver in the desktop. Do not install RGS USB on either the sender or receiver.

You must add the RGS Sender application or port as an exception to any firewall software. The default RGS port is 42966. See the HP RGS documentation on the HP Web site for information on installing and configuring HP RGS components.

HP RGS has the following limitations:

- Connections to virtual machines are not supported.
- Vista desktops are not supported.
- Tunnel connections are not supported. Only direct connections are supported.
- Smart cards are not supported.
- Multiple monitors are not supported.
- View Portal does not support RGS connections.
- Linux thin clients do not support RGS connections.

## Multimedia Redirection (MMR)

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

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, WMV, AVI, and WAV, among others.

For best quality, 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.

---

## 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 ActiveIdentity 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 cards 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 26 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 View Client for Mac or View Administrator. See the *VMware View Architecture Planning Guide* for complete information on smart card support.

## Preparing Active Directory

---

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 2000 Active Directory
- Windows 2003 Active Directory
- Windows 2008 Active Directory

This chapter includes the following topics:

- [“Configuring Domains and Trust Relationships,”](#) on page 23
- [“Creating an OU for View Desktops,”](#) on page 24
- [“Creating OUs and Groups for Kiosk Mode Client Accounts,”](#) on page 24
- [“Creating Groups for View Users,”](#) on page 24
- [“Creating a User Account for vCenter Server,”](#) on page 24
- [“Create a User Account for View Composer,”](#) on page 25
- [“Configure the Restricted Groups Policy,”](#) on page 25
- [“Using View Group Policy Administrative Template Files,”](#) on page 26
- [“Prepare Active Directory for Smart Card Authentication,”](#) on page 26

### 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 Administrator's Guide* 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.

See the *VMware View Administrator's Guide* for more information.

## Creating OUs and Groups for Kiosk Mode Client Accounts

A client in kiosk mode is a thin client or a lock-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 Administrator's Guide* 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 51 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 your Active Directory server, select **Start > Administrative Tools > Active Directory Users and Computers**.
- 2 Right-click your domain and select **Properties**.
- 3 On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in.
- 4 Right-click **Default Domain Policy** and click **Edit**.
- 5 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings**.
- 6 Right-click **Restricted Groups**, select **Add Group**, and add the Remote Desktop Users group.
- 7 Right-click the new restricted Remote Desktop Users group and add your View desktop users group to the group membership list.
- 8 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 Administrator's Guide* 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 27  
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 27  
If you use a 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 the Root Certificate to the Enterprise NTAAuth Store](#) on page 28  
If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAAuth 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 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 the 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 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 your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 Right-click your domain and click **Properties**.
- 3 On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in.
- 4 Right-click **Default Domain Policy**, and then click **Edit**.
- 5 Expand the **Computer Configuration** section and then open **Windows Settings\Security Settings\Public Key**.
- 6 Right-click **Trusted Root Certification Authorities** and select **Import**.
- 7 Follow the prompts in the wizard to import the certificate and click **OK**.
- 8 Close the Group Policy window.

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

## Add the Root Certificate to the Enterprise NTAAuth Store

If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAAuth 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 NTAAuth store.

For example: `certutil -dspublish -f path_to_root_CA_cert NTAAuthCA`

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

# Installing View Composer

---

To use View Composer, you create a View Composer database, install the View Composer service on the vCenter Server computer, and optimize your View infrastructure to support View Composer.

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,”](#) on page 29
- [“Install the View Composer Service,”](#) on page 34
- [“Configuring Your Infrastructure for View Composer,”](#) on page 36

## 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 on the vCenter Server computer or in your network environment, you must install one. After you install a database instance, you add the View Composer database to the instance.

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 30  
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 11g or 10g Database for View Composer](#) on page 32  
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 11g or 10g instance and configuring an ODBC data source for it.
- [Create an Oracle 9i Database for View Composer](#) on page 33  
View Composer can store linked-clone desktop information in an Oracle 9i database. You create a View Composer database by adding it to an existing Oracle 9i instance and configuring an ODBC data source for it.

## 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 on the same system as vCenter Server, 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 vCenter Server computer 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 vCenter Server 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 31.

## 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.

These instructions assume that you are configuring the ODBC data source on Windows Server 2003 SP1. Some steps are different if you configure the ODBC data source on Windows XP Professional SP2.

### Prerequisites

Complete the steps described in [“Add a View Composer Database to SQL Server,”](#) on page 30.

### Procedure

- 1 On the vCenter Server computer, 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\SQLEXP\_VIM**

- 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
<b>Windows NT authentication</b>	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 vCenter Server computer.
<b>SQL Server authentication</b>	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 Finish and close the Microsoft ODBC Data Source Administrator wizard.

### What to do next

Install the new View Composer service on the vCenter Server computer. See [“Install the View Composer Service,”](#) on page 34.

## Create an Oracle 11g or 10g 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 11g or 10g instance and configuring an ODBC data source for it.

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

You can add a new View Composer database to an existing Oracle 11g or 10g instance to store linked-clone data for View Composer.

#### Prerequisites

Verify that a supported version of Oracle 11g or 10g is installed on the vCenter Server computer. For details, see [“Database Requirements for View Composer,”](#) on page 10.

#### Procedure

- 1 On the vCenter Server computer, start the **Database Configuration Assistant**.

Database Version	Action
<b>Oracle 11g</b>	Select <b>Start &gt; All Programs &gt; Oracle-OraDb11g_home &gt; Configuration and Migration Tools &gt; Database Configuration Assistant</b> .
<b>Oracle 10g</b>	Select <b>Start &gt; All Programs &gt; Oracle-OraDb10g_home &gt; Configuration and Migration Tools &gt; Database Configuration Assistant</b> .

- 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 32.

### 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.

These instructions assume that you are configuring the ODBC data source on Windows Server 2003 SP1. Some steps are different if you configure the ODBC data source on Windows XP Professional SP2.

**Prerequisites**

Complete the steps described in [“Add a View Composer Database to Oracle 11g or 10g,”](#) on page 32.

**Procedure**

- 1 On the vCenter Server 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.

---

**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 on the vCenter Server computer. See [“Install the View Composer Service,”](#) on page 34.

**Create an Oracle 9i Database for View Composer**

View Composer can store linked-clone desktop information in an Oracle 9i database. You create a View Composer database by adding it to an existing Oracle 9i instance and configuring an ODBC data source for it.

**Add a View Composer Database to Oracle 9i**

You can add a new View Composer database to an existing Oracle 9i instance to store linked-clone data for View Composer.

**Prerequisites**

Verify that a supported version of Oracle 9i is installed on the vCenter Server computer. For details, see [“Database Requirements for View Composer,”](#) on page 10.

**Procedure**

- 1 On the vCenter Server computer, select **Start > All Programs > Oracle-OraHome92 > 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** 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 Database Connection Options page, select **Dedicated Server Mode**.
- 6 On the remaining configuration pages, click **Next** to accept the default settings.
- 7 On the Creation Options page, verify that **Create Database** is selected and click **Finish**.

- 8 On the Summary page, review the options and click **OK**.  
The configuration tool creates the database.
- 9 Set passwords for the SYS and SYSTEM administrator accounts.  
You use the SYSTEM account to set up the data-source connection.

### What to do next

Follow the instructions in [“Add an ODBC Data Source to Oracle 9i,”](#) on page 34.

## Add an ODBC Data Source to Oracle 9i

After you add a View Composer database to an Oracle 9i instance, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

These instructions assume that you are configuring the ODBC data source on Windows Server 2003 SP1. Some steps are different if you configure the ODBC data source on Windows XP Professional SP2.

### Prerequisites

Complete the steps described in [“Add a View Composer Database to Oracle 9i,”](#) on page 33.

### Procedure

- 1 On the vCenter Server 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: **Oracle in OraHome92**
- 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.

---

**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 on the vCenter Server computer. See [“Install the View Composer Service,”](#) on page 34.

## Install the View Composer Service

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

You install the View Composer service on the Windows Server computer on which vCenter Server is installed.

### 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.

- In vCenter Server, create a resource pool on the ESX host or cluster on which you want to store linked-clone desktops.
- If Windows firewall is running on the vCenter Server computer, make sure that the port the View Composer service uses to communicate with View Connection Server is accessible. You can add this port to the exception list or deactivate the local firewall service. You specify this port when you install the View Composer service.
- 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.

### 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 on which vCenter Server is installed.

The installer filename is `VMware-viewcomposer-xxxxxx.exe`, where `xxxxxx` is the build number. This installer file installs the View Composer service on 64-bit and 32-bit Windows Server operating systems.

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

On Windows Server 2008 computers, you might have to 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.
- 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
<b>Create default SSL certificate</b>	Click this radio button to create a default SSL certificate for the View Composer service.
<b>Use an existing SSL certificate</b>	Click this radio button if you have an SSL certificate 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 on the vCenter Server computer.

## 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, 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.

- If you create more than 120 virtual machines as linked-clone desktops, edit the vSwitch settings on the ESX host to increase the number of ports that are used for the virtual machines. By default, ESX is configured for 120 ports.
- 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 can contain at most eight ESX hosts. In a large View Composer environment, you might have to configure many eight-host clusters.
- 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

---

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,”](#) on page 37
- [“Configuring User Accounts for vCenter Server and View Composer,”](#) on page 51
- [“Configuring View Connection Server for the First Time,”](#) on page 54
- [“Configuring View Client Connections,”](#) on page 57
- [“Sizing Windows Server Settings to Support Your Deployment,”](#) on page 59

## 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.

<b>Standard installation</b>	Generates a View Connection Server instance with a new View LDAP configuration.
<b>Replica installation</b>	Generates a View Connection Server instance with a View LDAP configuration that is copied from an existing instance.
<b>Security server installation</b>	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 2000 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 install View Connection Server, you must use a domain user account with administrator privileges on the system.

## 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.

### 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 37.
- Familiarize yourself with the incoming TCP ports that must be opened on the Windows Firewall for View Connection Server instances. See “[Firewall Rules for View Connection Server](#),” on page 41.

### 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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build 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 Accept the Microsoft Software Supplemental License Agreement for Microsoft Active Directory Application Mode (ADAM).
- 7 If you install View Connection Server on Windows Server 2008, choose how to configure the Windows Firewall service.

Option	Action
<b>Configure Windows Firewall automatically</b>	Let the installer configure Windows Firewall to allow the required incoming TCP protocol connections.
<b>Do not configure Windows Firewall</b>	Configure the Windows firewall rules manually.

If you install View Connection Server on Windows Server 2003, you must configure the required Windows firewall rules manually.

- 8 Complete the installation wizard to finish installing View Connection Server.

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

For information about these services, see the *VMware View Administrator's Guide*.

### What to do next

Perform initial configuration on View Connection Server.

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 37.

- 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 48.
- 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 40.

**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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build number.

- 2 Open a command prompt on the Windows Server computer.
- 3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-4.5.x-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1"`

The VMware View services are installed on the Windows Server computer. For details, see [“Install View Connection Server with a New Configuration,”](#) on page 38.

**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: <code>INSTALLDIR=""D:\abc\my folder""</code> The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path.	%ProgramFiles %\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	The type of View Connection Server installation: <ul style="list-style-type: none"> <li>■ 1. Standard installation</li> <li>■ 2. Replica installation</li> <li>■ 3. Security server installation</li> <li>■ 4. View Transfer Server installation</li> </ul> For example, to perform a standard installation, define <code>VDM_SERVER_INSTANCE_TYPE=1</code>	1
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 sets a firewall. A value of 2 does not set a firewall. For example: <code>FWCHOICE=1</code>	1

## Firewall Rules for View Connection Server

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

When you install View Connection Server on Windows Server 2008, the installation program can optionally configure the required Windows firewall rules for you. When you install View Connection Server on Windows Server 2003, you must configure the required Windows firewall rules manually.

**Table 5-2.** TCP Ports Opened During View Connection Server Installation

Protocol	Ports	View Connection Server Instance Type
JMS	4001	Standard and replica
JMSIR	4100	Standard and replica
AJP13	8009	Standard and replica
HTTP	80	Standard, replica, and security server
HTTPS	443	Standard, replica, and security server

## 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.

---

### Prerequisites

- Verify that at least one View Connection Server instance is installed and configured on the network.
- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you plan to install the replicated instance.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have local 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 37.
- Familiarize yourself with the incoming TCP ports that must be opened on the Windows Firewall for View Connection Server instances. See “[Firewall Rules for View Connection Server](#),” on page 41.

### 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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build 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 Accept the Microsoft Software Supplemental License Agreement for Microsoft Active Directory Application Mode (ADAM).
- 8 If you install View Connection Server on Windows Server 2008, choose how to configure the Windows Firewall service.

Option	Action
<b>Configure Windows Firewall automatically</b>	Let the installer configure Windows Firewall to allow the required incoming TCP protocol connections.
<b>Do not configure Windows Firewall</b>	Configure the Windows firewall rules manually.

If you install View Connection Server on Windows Server 2003, you must configure the required Windows firewall rules manually.

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

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

For information about these services, see the *VMware View Administrator's Guide*.

### What to do next

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

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.

Repeat this procedure to install additional replicated instances.

## 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.
- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you plan to install the replicated instance.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have local 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 37.
- Familiarize yourself with the MSI installer command-line options. See [“Microsoft Windows Installer Command-Line Options,”](#) on page 48.
- 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 44.

### 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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build number.

- 2 Open a command prompt on the Windows Server computer.
- 3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-4.5.x-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com"`

The VMware View services are installed on the Windows Server computer. For details, see [“Install a Replicated Instance of View Connection Server,”](#) on page 41.

## 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 5-3.** 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: <code>INSTALLDIR=""D:\abc\my folder""</code> The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	%ProgramFiles %\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	The type of View Connection Server installation: <ul style="list-style-type: none"> <li>■ 1. Standard installation</li> <li>■ 2. Replica installation</li> <li>■ 3. Security server installation</li> <li>■ 4. View Transfer Server installation</li> </ul> To install a replicated instance, define <code>VDM_SERVER_INSTANCE_TYPE=2</code> This MSI property is optional for a standard installation. It is required for all other types of installation.	1
ADAM_PRIMARY_NAME	The host name or IP address of the existing View Connection Server instance you are replicating. For example: <code>ADAM_PRIMARY_NAME=cs1.companydomain.com</code> 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: <code>ADAM_PRIMARY_PORT=cs1.companydomain.com</code> 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 sets a firewall. A value of 2 does not set a firewall. For example: <code>FWCHOICE=1</code> This MSI property is optional.	1

## 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.

### 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 45.

---

**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.

### Prerequisites

- Review the requirements for installing and deploying a security server in the *VMware View Architecture Planning Guide*.
- 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 37.
- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running View Connection Server 4.5. You cannot pair a 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 44.
- Familiarize yourself with the format of external URLs. See [“Configuring External URLs for Tunnel Connections,”](#) on page 58.
- Verify that you can log in as a domain user with local administrator privileges on the Windows Server computer on which you plan to install the security server.
- Familiarize yourself with the incoming TCP ports that must be opened on the Windows Firewall for a security server. See [“Firewall Rules for View Connection Server,”](#) on page 41.

### 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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build 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 then type the new password in the installation program.

- 8 Type the external URL of the security server in the **External URL** text box.

The URL must contain the protocol, externally 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 If you install the security server on Windows Server 2008, choose how to configure the Windows Firewall service.

Option	Action
<b>Configure Windows Firewall automatically</b>	Let the installer configure Windows Firewall to allow the required incoming TCP protocol connections.
<b>Do not configure Windows Firewall</b>	Configure the Windows firewall rules manually.

If you install the security server on Windows Server 2003, you must configure the required Windows firewall rules manually.

- 10 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

For information about these services, see the *VMware View Administrator's Guide*.

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

### What to do next

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

- Review the requirements for installing and deploying a security server in the *VMware View Architecture Planning Guide*.
- 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 37.
- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running View Connection Server 4.5. You cannot pair a security server with an older version of View Connection Server.
- Configure a security server pairing password. See “[Configure a Security Server Pairing Password](#),” on page 44.
- Familiarize yourself with the format of external URLs. See “[Configuring External URLs for Tunnel Connections](#),” on page 58.
- Verify that you can log in as a domain user with local administrator privileges on the Windows Server computer on which you plan to install the security server.
- Familiarize yourself with the MSI installer command-line options. See “[Microsoft Windows Installer Command-Line Options](#),” on page 48.
- Familiarize yourself with the silent installation properties available with a security server. See “[Silent Installation Properties for a Security Server](#),” on page 48.

### 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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build number.

- 2 Open a command prompt on the Windows Server computer.
- 3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-4.5.x-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3 VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_SS_EXTURL=https://ss1.companydomain.com:443 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 45.

## 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 5-4.** 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: <code>INSTALLDIR=""D:\abc\my folder""</code> The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	%ProgramFiles %\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	The type of View Connection Server installation: <ul style="list-style-type: none"> <li>■ 1. Standard installation</li> <li>■ 2. Replica installation</li> <li>■ 3. Security server installation</li> <li>■ 4. View Transfer Server installation</li> </ul> To install a security server, define <code>VDM_SERVER_INSTANCE_TYPE=3</code> This MSI property is optional for a standard installation. It is required for all other types of installation.	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: <code>VDM_SERVER_NAME=cs1.companydomain.com</code> 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: <code>VDM_SERVER_SS_EXTURL=https://ss1.companydomain.com:443</code> This MSI property is required.	None
VDM_SERVER_SS_PWD	The security server pairing password. For example: <code>VDM_SERVER_SS_PWD=secret</code> 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 sets a firewall. A value of 2 does not set a firewall. For example: <code>FWCHOICE=1</code> This MSI property is optional.	1

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

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

Option	Description
/s	<p>Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs.</p> <p>For example: VMware-viewconnectionserver-4.5.x-xxxxxx.exe /s</p> <p>The /s option is required to run a silent installation.</p>
/v" MSI_command_line_options"	<p>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.</p> <p>For example: VMware-viewagent-4.5.x-xxxxxx.exe /s /v"command_line_options"</p> <p>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.</p> <p>For example: VMware-viewconnectionserver-4.5.x-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""</p> <p>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.</p> <p>The /v"command_line_options" option is required to run a silent installation.</p>

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 5-6](#) shows the command-line options and MSI property values that are passed to the MSI installer.

**Table 5-6.** MSI Command-Line Options and MSI Properties

MSI Option or Property	Description
/qn	<p>Instructs the MSI installer not to display the installer wizard pages.</p> <p>For example, you might want to install View Agent silently and use only default setup options and features:</p> <p>VMware-viewagent-4.5.x-xxxxxx.exe /s /v"/qn"</p> <p>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.</p> <p>The /qn or /qb option is required to run a silent installation.</p>
INSTALLDIR	<p>Specifies an alternative installation path for the View component.</p> <p>Use the format <i>INSTALLDIR=path</i> to specify an installation path. You can ignore this MSI property if you want to install the View component in the default path.</p> <p>This MSI property is optional.</p>

**Table 5-6.** MSI Command-Line Options and MSI Properties (Continued)

MSI Option or Property	Description
ADDLOCAL	<p>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.</p> <p>To install all available custom setup options, enter ADDLOCAL=ALL.</p> <p>For example: <code>VMware-viewagent-4.5.x-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</code></p> <p>If you do not use the MSI property, ADDLOCAL, the default setup options are installed.</p> <p>To specify individual setup options, enter a comma-separated list of setup option names. Do not use spaces between names. Use the format <code>ADDLOCAL=value,value,value...</code></p> <p>For example, you might want to install View Agent in a guest operating system with the View Composer Agent and PCoIP features:</p> <p><code>VMware-viewagent-4.5.x-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP"</code></p> <p><b>NOTE</b> The Core feature is required in View Agent.</p> <p>This MSI property is optional.</p>
<code>/l*v log_file</code>	<p>Writes logging information into the specified log file with verbose output.</p> <p>For example: <code>/l*v ""%TEMP%\vmmsi.log""</code></p> <p>This example generates a detailed log file that is similar to the log generated during an interactive installation.</p> <p>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.</p> <p>The <code>/l*v</code> option is optional.</p>

## 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 48.

### Examples

Uninstall a View Connection Server instance.

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

## 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 25.

### 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 24.
- Familiarize yourself with the privileges that are required for the user account. See [“View Manager Privileges Required for the vCenter Server User,”](#) on page 53.
- If you use View Composer, familiarize yourself with the additional required privileges. See [“View Composer Privileges Required for the vCenter Server User,”](#) on page 53.
- If you manage local desktops, familiarize yourself with the additional required privileges. See [“Local Mode Privileges Required for the vCenter Server User,”](#) on page 54.

## 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 **Administration > 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 **Administration > 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 **Administration > 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 datacenter or cluster that will host the View desktop virtual machines in your deployment, click **Add Permission**, and add the vCenter Server user.
- 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 55.

## 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 5-7.** View Manager Privileges

Privilege Group	Privileges to Enable
Folder	Create Folder Delete Folder
Virtual Machine	In Configuration: <ul style="list-style-type: none"> <li>■ Add or remove device</li> <li>■ Advanced</li> <li>■ Modify device settings</li> </ul> In Interaction: <ul style="list-style-type: none"> <li>■ Power Off</li> <li>■ Power On</li> <li>■ Reset</li> <li>■ Suspend</li> </ul> In Inventory: <ul style="list-style-type: none"> <li>■ Create new</li> <li>■ Remove</li> </ul> In Provisioning: <ul style="list-style-type: none"> <li>■ Customize</li> <li>■ Deploy template</li> <li>■ Read customization specifications</li> </ul>
Resource	Assign virtual machine to resource pool

## 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 5-8.** 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: <ul style="list-style-type: none"> <li>■ Clone virtual machine</li> <li>■ Allow disk access</li> </ul>
Resource	Assign virtual machine to resource pool
Global	Enable methods Disable methods System tag
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 5-9.** 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, add security servers if you use them, and set external URLs for client desktops that run outside your network.

### 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 View Connection Server is installed on a dedicated computer.
- 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 or IP address of the View Connection Server instance.

**https://*server*/admin**

You access View Administrator by using a secure (SSL) connection. 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. This response is expected behavior because the default certificate supplied with View Connection Server is self-signed.

- 2 Click **Ignore** to continue using the current SSL certificate.
- 3 Log in using administrator credentials on the View Connection Server computer.

Initially, all users who are members of the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer are allowed to log in to View Administrator.

After you log in to View Administrator, you can use **View Configuration > Administrators** to change the list of View Manager administrators.

## 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** You must use a View 4.x license key for View Connection Server 4.x. A license key provided with View 3.x or earlier does not work with the new license model introduced in View 4.x.

---

### 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.

### 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 51.

## Procedure

- 1 In View Administrator, click **View Configuration > Servers**.
- 2 In the vCenter Servers panel, click **Add**.
- 3 In the server address text box, type the fully qualified domain name (FQDN) or IP address 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 To connect to the vCenter Server instance using a secure channel (SSL), make sure that **Connect using SSL** is selected. SSL connection is the default setting.
- 8 Type the TCP port number.  
The default port is 443.
- 9 (Optional) Click **Advanced** to configure the maximum concurrent pool operations in vCenter Server.

- a Set the maximum number of concurrent provisioning operations.

This setting determines the largest number of concurrent requests that View Manager can make to provision full virtual machines in this vCenter Server instance. The default value is eight. This setting does not control linked-clone provisioning.

- b Set the maximum number of concurrent power operations.

This setting determines the largest number of power operations (startup, shutdown, suspend, and so on) that can take place simultaneously on full virtual machines managed by View Manager in this vCenter Server instance. The default value is five. This setting controls power operations for full virtual machines and linked clones.

- 10 Choose whether to configure View Composer.

Option	Action
<b>You are not using View Composer</b>	Click <b>OK</b> .
<b>You are using View Composer</b>	Configure the View Composer settings.

## What to do next

If this View Connection Server instance or group of replicated View Connection Server instances uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

## Configure View Composer Settings for vCenter Server

To use View Composer, you must configure View Manager with initial settings that match the settings for the View Composer service that is installed in vCenter Server. View Composer is a feature of View Manager, but its service operates directly on virtual machines in vCenter Server.

---

**NOTE** If you are not using View Composer, you can skip this task.

---

### 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 25.

- You must configure View Manager to connect to vCenter Server. See [“Add vCenter Server Instances to View Manager,”](#) on page 55.

### Procedure

- 1 In View Administrator, open the Edit vCenter Server dialog box.
  - a Click **View Configuration > Servers**.
  - b In the vCenter Servers panel, select the vCenter Server entry.
  - c Click **Edit**.
- 2 Select **Enable View Composer** and 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.  
View Manager verifies that the View Composer service is running on vCenter Server.
- 3 Click **Add** to add the domain user for View Composer account information.
  - a Type the domain name of the Active Directory domain.  
For example: **domain.com**
  - b Type the domain user name, including the domain name.  
For example: **domain.com\admin**
  - c Type the account password.
  - d Click **OK**.
  - e To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.
- 4 Click **OK** to close the Edit vCenter Server dialog box.

### What to do next

Repeat this procedure for each vCenter Server instance in which View Composer services are installed.

## Configuring View Client Connections

View clients communicate with a View Connection Server or security server host over secure HTTPS connections.

The initial View Client connection, which is used for user authentication and View desktop selection, is created when a user provides an IP address 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.

When users connect to a View desktop with the Microsoft RDP display protocol, View Client makes a second HTTPS 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 data.

When the tunnel connection 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.

Clients that use the PCoIP and HP RGS display protocols do not use the tunnel connection.

## Configure the Tunnel Connection

You use View Administrator to configure the tunnel connection.

Only clients that use the RDP display protocol can use the tunnel connection. Clients that use the PCoIP and HP RGS display protocols do not use the tunnel connection.

### 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**.
  - To configure a secure tunnel for carrying RDP data between View desktop virtual machines and the View Connection Server or security server host, select **Use secure tunnel connection to desktop**.
  - To bypass the View Connection Server or security server host and configure direct connections between client systems and View desktop virtual machines, deselect **Use secure tunnel connection to desktop**.
- 3 Click **OK** to save your changes.

## Configuring External URLs for Tunnel Connections

To use the tunnel connection, a client system must be able to resolve the fully qualified domain name (FQDN) of the View Connection Server or security server host. 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 an externally resolvable domain or subdomain name or IP address, or by reassigning specific ports on an existing address, to route client requests to the appropriate location (typically, a security server). For example:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`

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 a FQDN.

The process of configuring an external URL is different for View Connection Server instances and security servers.

- For a View Connection Server instance, you set an external URL by editing View Connection Server settings in View Administrator.
- For a security server, you set an external URL when you run the View Connection Server installation program. You can use View Administrator to modify the external URL for a security server.

## Set the External URL for a View Connection Server Instance

You use View Administrator to configure the external URL for a View Connection Server instance. Tunnel clients that run outside of your network must use an externally resolvable URL to connect to a View Connection Server instance.

For security servers, you configure the external URL in the View Connection Server installation program.

**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 external URL in the **External URL** text box.  
The URL must contain the protocol, externally resolvable host name, and port number.  
For example: `https://view.example.com:443`
- 4 Click **OK**.

**Modify the External URL for a Security Server**

You use View Administrator to modify the external URL for a security server.

You initially configure the external URL for a security server in the View Connection Server installation program.

**Prerequisites**

Verify that the security server is upgraded to View Connection Server 4.5.

**Procedure**

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 In the Security Servers pane, select the security server and click **Edit**.  
The **Edit** button is unavailable if the security server is not upgraded to View Connection Server 4.5.
- 3 Type the external URL in the **External URL** text box.  
The URL must contain the protocol, externally resolvable security server host name, and port number.  
For example: `https://view.example.com:443`
- 4 Click **OK** to save your changes.

View Administrator sends the updated external URL 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 ephemeral ports, TCB hash table, Java Virtual Machine settings, and Windows page-file. These adjustments ensure that the computers have adequate resources to run correctly with the expected user load.

For hardware and memory requirements for View Connection Server, see [“Hardware Requirements for View Connection Server,”](#) on page 7.

For hardware and memory recommendations for using View Connection Server in a large View deployment, see "Connection Server Virtual Machine Configuration and Maximums" in the *VMware View Architecture Planning Guide*.

## Ephemeral Ports

View Manager uses ephemeral ports to establish TCP connections between View Connection Server and the View desktops that it administers. To support a large View desktop deployment, you can increase the number of available ephemeral ports.

An ephemeral port is a short-lived endpoint that is created by the operating system when a program requests any available user port. The operating system selects the port number from a predefined range, typically between 1024 and 65535, and releases the port after the related TCP connection terminates.

By default, the system can create a maximum of approximately 4,000 ephemeral ports that run concurrently on Windows Server 2003 and approximately 16,000 on Windows Server 2008.

On 32-bit Windows Server 2003 computers, you should increase the number of available ephemeral ports if a View Connection Server instance is likely to use more than 800 concurrent client connections.

### Calculate the Number of Ephemeral Ports

You can calculate the number of ephemeral ports that are needed on each View Connection Server instance to support a large number of concurrent client connections.

#### Procedure

- ◆ Use the following formula.

$$\text{Number of ephemeral ports} = ( (5 \times \text{clients}) / \text{servers} ) + 10$$

Where

**clients**                                      Projected number of concurrent client connections

**servers**                                      Number of View Connection Server instances in the replicated group

#### Example: Calculating the Number of Ephemeral Ports

For example, you might plan a deployment managed by three View Connection Server instances. If you anticipate having 3,000 concurrent client connections, you would need 5,010 ephemeral ports, as shown in [Table 5-10](#).

**Table 5-10.** Example of Calculating the Number of Ephemeral Ports

Configuration Parameter	Sample Values
Projected number of concurrent client connections	3,000
Number of View Connection Server instances in the replicated group	3
$( (5 \times \text{clients}) / \text{servers} ) + 10 = \text{number of ephemeral ports on each View Connection Server}$	$(5 \times 3,000) / 3 + 10 = 5,010$

#### What to do next

Use the [“Worksheets for Calculating Ephemeral Ports and TCB Hash Table Size,”](#) on page 63 to fill in values for your deployment.

### Increase the Number of Ephemeral Ports

You can edit the Windows registry to increase the maximum number of ephemeral ports on a Windows Server computer on which View Connection Server runs.

Active Directory group policies can override registry entries. When possible, use a group policy to set the maximum number of ephemeral ports on View Connection Server.

### Prerequisites

Calculate the number of ephemeral ports to configure on the Windows Server computer. See [“Calculate the Number of Ephemeral Ports,”](#) on page 60.

Modify the Windows registry value only if the resulting number of ports is greater than 4,000 on Windows Server 2003 or greater than 16,000 on Windows Server 2008.

### Procedure

- 1 On the Windows Server computer, start the Windows Registry Editor.
  - a Select **Start > Command Prompt**.
  - b At the command prompt, type **regedit**.
- 2 In the registry, locate the correct subkey and click **Parameters**.  
 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- 3 Click **Edit > New** and add the registry entry.
 

Value Name: MaxUserPort  
 Value Type: DWORD  
 Value data: 1024 + *calculated number of ephemeral ports*  
 Valid Range: 5000–65534 (decimal)
- 4 Exit the Windows Registry Editor.
- 5 Restart the Windows Server computer.

## Increasing the Size of the TCB Hash Table

The transmission control block (TCB) holds information about TCP connections that are made between View Connection Server clients and their desktop sources. To support a large View desktop deployment, you can increase the size of the TCB hash table.

The TCB is a memory-resident data structure that contains socket numbers, the location of incoming and outgoing data buffers, bytes received or unacknowledged, and other information.

To retrieve this information quickly, Windows Server stores TCB data structures in a hash table.

By default, Windows Server configures the number of hash table rows based on the number of CPUs in the Windows Server computer.

You use two different formulas to calculate the TCB hash table size on View Connection Server instances and security servers.

### Calculate the Size of the TCB Hash Table for View Connection Server

To support a large number of View desktops, you can optimize the size of the TCB hash table on each View Connection Server instance. Calculate the size in rows.

#### Procedure

- ◆ Use the following formula.

$$\text{Number of hash table rows on each View Connection Server instance} = ( (5 \times \text{clients}) / \text{servers} ) + \text{desktops} + 20$$

Where

<b>clients</b>	Projected number of concurrent client connections
<b>servers</b>	Number of View Connection Server instances in the replicated group
<b>desktops</b>	Number of View desktop sources in your deployment

### Example: Calculating the Size of the TCB Hash Table on Each View Connection Server

For example, you might have 3,000 concurrent client connections, three View Connection Server instances, and 6,000 View desktop sources in your deployment.

For each View Connection Server instance, the result is 11,020, as shown in [Table 5-11](#).

**Table 5-11.** Example of Calculating the Size of the TCB Hash Table on Each View Connection Server

Configuration Parameter	Sample Values
Projected number of concurrent client desktop connections	3,000
Number of View Connection Server instances	3
Number of View desktop sources	6,000
$(5 \times \text{clients}) / \text{servers} + \text{desktops} + 20 = \text{number of TCB hash table rows on each server}$	$(5 \times 3,000) / 3 + 6,000 + 20 = 11,020$

### What to do next

Use the “[Worksheets for Calculating Ephemeral Ports and TCB Hash Table Size](#),” on page 63 to fill in values for your deployment.

### Calculate the Size of the TCB Hash Table for Security Servers

To support a large number of View desktops, you can optimize the size of the TCB hash table on each security server. Calculate the size in rows.

#### Procedure

- ◆ Use the following formula.

$$\text{Number of hash table rows} = (5 \times \text{clients}) / \text{security servers} + 10$$

Where

<b>clients</b>	Projected number of concurrent client connections
<b>security servers</b>	Number of security servers

### Example: Calculating the Size of the TCB Hash Table on Each Security Server

For example, you might have 3,000 concurrent client connections and two security servers in your deployment.

For each security server, the result is 7,510, as shown in [Table 5-12](#).

**Table 5-12.** Example of Calculating the Size of the TCB Hash Table on Each Security Server

Configuration Parameter	Sample Values
Projected number of concurrent client desktop connections	3,000
Number of security servers	2
$(5 \times \text{clients}) / \text{security servers} + 10 = \text{number of TCB hash table rows on each security server}$	$(5 \times 3,000) / 2 + 10 = 7,510$

**What to do next**

Use the “[Worksheets for Calculating Ephemeral Ports and TCB Hash Table Size](#),” on page 63 to fill in values for your deployment.

**Increase the Size of the TCB Hash Table on a Windows Server Computer**

Edit the Windows registry to increase the size of the TCB hash table on a Windows Server computer on which View Connection Server runs.

Active Directory group policies can override registry entries. When possible, use a group policy to set the size of the TCB hash table on View Connection Server.

**Procedure**

- 1 On the Windows Server computer, start the Windows Registry Editor
  - a Select **Start > Command Prompt**.
  - b At the command prompt, type **regedit**.
- 2 In the registry, locate the subkey and click **Parameters**.  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- 3 Click **Edit > New** and add the following registry entry.
 

Value Name: MaxHashTableSize  
 Value Type: DWORD  
 Value data: *calculated hash table size*  
 Valid Range: 64–65536 (decimal)
- 4 Exit the Windows Registry Editor.
- 5 Restart the Windows Server computer.

**Worksheets for Calculating Ephemeral Ports and TCB Hash Table Size**

Use these worksheets to calculate the number of ephemeral ports and the size of the TCB hash table on each View Connection Server instance and security server in your deployment.

**Table 5-13.** Configuration Parameters

Configuration Parameters	Fill in Your Site's Value
Projected number of concurrent client connections	
Number of View Connection Server instances	
Number of security servers	
Number of View desktop sources	

**Table 5-14.** Number of Ephemeral Ports

Number of Ephemeral Ports	Fill in Your Site's Value
$(5 \times \text{clients}) / \text{servers} + 10 =$ number of ephemeral ports on each View Connection Server instance	

**Table 5-15.** TCB Hash Table Size for View Connection Servers

Hash Table Size for View Connection Servers	Fill in Your Site's Value
$(5 \times \text{clients}) / \text{servers} + \text{desktops} + 20 =$ Number of hash table rows on each View Connection Server instance	

**Table 5-16.** TCB Hash Table Size for Security Servers

Hash Table Size for Security Servers	Fill in Your Site's Value
( 5 x clients ) / security servers ) + 10 = Number of hash table rows on each security server	

## 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. However, when View Connection Server runs on a 32-bit Windows Server computer, the View Secure Gateway Server component is configured with a limited JVM heap size. To size your deployment adequately, you can increase the JVM heap size on 32-bit computers.

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 adjust the JVM heap size to the recommended value, reinstall View Connection Server.

On a 32-bit Windows Server computer, the default JVM heap size is 512MB for the View Secure Gateway Server component. This JVM heap size can support approximately 750 concurrent tunnel sessions. To support more than 750 sessions, the computer must have at least 3GB of memory and the JVM heap size should be increased to 1GB. A JVM heap size of 1GB supports 1,500 concurrent tunnel sessions, the maximum number that View Connection Server can support on a 32-bit computer.

## Increase the JVM Heap Size on 32-Bit Windows Server Computers

You can edit the Windows registry to increase the JVM heap size on a 32-bit Windows Server computer on which View Connection Server is installed.

---

**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.

---

On a 32-bit computer, you must increase the JVM heap size each time you install or upgrade the View Connection Server software.

**Procedure**

- 1 On the Windows Server computer, start the Windows Registry Editor.
  - a Select **Start > Command Prompt**.
  - b At the command prompt, type **regedit**.
- 2 In the registry, locate the subkey and click **JvmOptions**.  
 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wsnm\tunnelService\Params
- 3 Click **Edit > Modify**.  
 A Windows dialog box displays an entry like the following one.  
 -Xms128m -Xmx512m -Xss96k -Xrs -XX:+UseConcMarkSweepGC  
 -Dsimple.http.poller=simple.http.GranularPoller  
 -Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
- 4 Edit the -Xmx parameter to have the value **-Xmx1024m**.  
 The dialog box displays the following entry.  
 -Xms128m -Xmx1024m -Xss96k -Xrs -XX:+UseConcMarkSweepGC  
 -Dsimple.http.poller=simple.http.GranularPoller  
 -Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
- 5 Click **OK** and exit the Registry Editor.
- 6 Restart the Windows Server computer.

**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.



# Installing View Transfer Server

---

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 67

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 69

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 70

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 71

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

5 [Installing View Transfer Server Silently](#) on page 71

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 have a license to install View Transfer Server and use local desktops.
- Familiarize yourself with the incoming TCP ports that must be opened on the Windows Firewall for View Connection Server instances. See “[Firewall Rules for View Transfer Server](#),” on page 71.



**CAUTION** Verify that the virtual machine that hosts View Transfer Server is configured with an LSI Logic Parallel SCSI controller. You cannot install View Transfer Server on a virtual machine with a SAS or VMware paravirtual controller.

On Windows Server 2008 virtual machines, the LSI Logic SAS controller is selected by default. You must change this selection to a BusLogic or LSI Logic controller before you install the operating system.

## Procedure

- 1 Download the VMware 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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build 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 If you install View Transfer Server on Windows Server 2008, choose how to configure the Windows Firewall service.

Option	Action
<b>Configure Windows Firewall automatically</b>	Let the installer configure Windows Firewall to allow the required incoming TCP protocol connections.
<b>Do not configure Windows Firewall</b>	Configure the Windows firewall rules manually.

If you install View Transfer Server on Windows Server 2003, you must configure the required 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.

### Procedure

- 1 In View Administrator, click **View Configuration > Servers**.
- 2 In the Transfer Servers panel, 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 shuts down the virtual machine, reconfigures it with four SCSI controllers, and restarts the virtual machine. 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 **Missing Transfer Server repository**. 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 Apache2.2 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 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 69.

---

**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
<b>Local Transfer Server repository</b>	On the virtual machine where View Transfer Server is installed, create a path and folder for the Transfer Server repository. For example: C:\TransferRepository\
<b>Remote Transfer Server repository</b>	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 Transfer Servers panel, next to Transfer Server repository, click **None Configured**.

- 5 In the General panel on the Transfer Server repository page, click **Edit**.
- 6 Type the Transfer Server repository location and other information.

Option	Description
<b>Network Share</b>	<ul style="list-style-type: none"> <li>■ <b>Path.</b> Type the UNC path that you configured.</li> <li>■ <b>Username.</b> Type the user ID of an administrator with credentials to access the network share.</li> <li>■ <b>Password.</b> Type the administrator password.</li> <li>■ <b>Domain.</b> Type the domain name of the network share in NetBIOS format. Do not use the .com suffix.</li> </ul>
<b>Local File System</b>	Type the path that you configured on the local View Transfer Server virtual machine.

- 7 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.

- 8 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.

When you install View Transfer Server on Windows Server 2008, the installation program can optionally configure the required Windows firewall rules for you.

When you install View Transfer Server on Windows Server 2003, you must configure the required Windows firewall rules manually.

[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**, 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**, 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 48.
- Familiarize yourself with the silent installation properties available with View Transfer Server. See [“Silent Installation Properties for View Transfer Server,”](#) on page 73.
- 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 71.



**CAUTION** Verify that the virtual machine that hosts View Transfer Server is configured with an LSI Logic Parallel SCSI controller. You cannot install View Transfer Server on a virtual machine with a SAS or VMware paravirtual controller.

On Windows Server 2008 virtual machines, the LSI Logic SAS controller is selected by default. You must change this selection to a BusLogic or LSI Logic controller before you install the operating system.

## Procedure

- 1 Download the VMware 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-4.5.x-xxxxxx.exe` or `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, where `xxxxxx` is the build number.

- 2 Open a command prompt on the Windows Server computer.
- 3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-4.5.x-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: <code>INSTALLDIR=""D:\abc\my folder""</code> The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	%ProgramFiles %\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	The type of View Connection Server installation: <ul style="list-style-type: none"> <li>■ 1. Standard installation</li> <li>■ 2. Replica installation</li> <li>■ 3. Security server installation</li> <li>■ 4. View Transfer Server installation</li> </ul> To install a View Transfer Server, define <code>VDM_SERVER_INSTANCE_TYPE=4</code> 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: <code>SERVERDOMAIN=companydomain.com</code> If you specify a custom Apache Web Server domain with the MSI property, <code>SERVERDOMAIN</code> , you also must specify custom <code>SERVERNAME</code> and <code>SERVERADMIN</code> properties. This MSI property is optional.	None

**Table 6-2.** MSI Properties for Silently Installing View Transfer Server (Continued)

MSI Property	Description	Default Value
SERVERNAME	<p>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.</p> <p>For example: SERVERNAME=ts1.companydomain.com</p> <p>If you specify a custom Apache Web Server host name with the MSI property, SERVERNAME, you also must specify custom SERVERDOMAIN and SERVERADMIN properties.</p> <p>This MSI property is optional.</p>	None
SERVERADMIN	<p>The email address of the administrator of Apache Web Server that is configured with View Transfer Server.</p> <p>For example: SERVERADMIN=admin@companydomain.com</p> <p>If you specify a custom Apache Web Server administrator with the MSI property, SERVERADMIN, you also must specify custom SERVERDOMAIN and SERVERNAME properties.</p> <p>This MSI property is optional.</p>	None
FWCHOICE	<p>The MSI property that determines whether to configure a firewall for the View Connection Server instance.</p> <p>A value of 1 sets a firewall. A value of 2 does not set a firewall.</p> <p>For example: FWCHOICE=1</p> <p>This MSI property is optional.</p>	1

# Configuring Certificate Authentication

---

# 7

You can configure certificate authentication for View Connection Server instances, security servers, and View Transfer Server instances.

This chapter includes the following topics:

- [“Replacing the Default Certificate,”](#) on page 75
- [“Add keytool and openssl to the System Path,”](#) on page 76
- [“Export an Existing Microsoft IIS SSL Server Certificate,”](#) on page 76
- [“Creating a New SSL Certificate,”](#) on page 77
- [“Configure a View Connection Server Instance or Security Server to Use a New Certificate,”](#) on page 80
- [“Configure a View Transfer Server Instance to Use a New Certificate,”](#) on page 81
- [“Configure SSL for Client Connections,”](#) on page 82
- [“Configure SSL for View Transfer Server Communications,”](#) on page 82
- [“Using Group Policy to Configure Certificate Checking in View Client,”](#) on page 83

## Replacing the Default Certificate

A default server SSL certificate is generated when you install View Connection Server. You can use the default certificate for testing purposes.

---

**IMPORTANT** You should replace the default certificate as soon as possible. The default certificate is not signed by a commercial Certificate Authority (CA). Use of noncertified certificates can allow untrusted parties to intercept traffic by masquerading as your server.

---

View Connection Server instances that receive direct connections from client systems require a server SSL certificate. If you use a security server as your client-facing system, only the security server that is paired with the View Connection Server instance requires a server SSL certificate. A server SSL certificate is also required if you configure View Connection Server to use smart card authentication.

View Transfer Server instances always require a server SSL certificate. Communications and data transfers between local computers and a View Transfer Server instance are encrypted if you enable SSL settings for local mode operations and desktop provisioning.

When you replace the default certificate with your own certificate, clients use the public key contained in your certificate to encrypt the data that they send to 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 server's public key. This key is used to encrypt traffic between the client and the server.

You use the `keytool` and `openssl` utilities to create and manage certificates for View.

## Add keytool and openssl to the System Path

`keytool` and `openssl` are key and certificate management utilities. You must add the paths to these utilities to the system environment Path variable so that you can run the utilities from any directory on your host.

### Procedure

- 1 On your View Connection Server or security server host, right-click **My Computer** and select **Properties**.
  - a On the **Advanced** tab, click **Environment Variables**.
  - b In the System variables group, select **Path** and click **Edit**.
  - c Type the path to the JRE directory in the **Variable Value** text box. Use a semicolon (;) to separate each entry from other entries in the text box.  
 For example: `install_directory\VMware\VMware View\Server\jre\bin`
- 2 On your View Transfer Server host, right-click **My Computer** and select **Properties**.
  - a On the **Advanced** tab, click **Environment Variables**.
  - b In the System variables group, select **Path** and click **Edit**.
  - c Type the paths to the JRE and Apache directories in the **Variable Value** text box. Use a semicolon (;) to separate each entry from other entries in the text box.  
 For example: `install_directory\VMware\VMware View\Server\httpd\bin;install_directory\VMware\VMware View\Server\jre\bin`
- 3 Click **OK** until the Windows System Properties dialog box closes.

## Export an Existing Microsoft IIS SSL Server Certificate

If your organization already has a valid server SSL certificate, you can use that certificate to replace the default server SSL certificate provided with View Connection Server.

To use an existing certificate, you need both the certificate and the accompanying private key. You must export the certificate from the IIS application server that hosts the Web site that uses the certificate. Windows provides visual tools to assist you.

### Procedure

- 1 On the IIS application server host, click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.  
 The Internet Information Services Manager appears.
- 2 To view the list of sites hosted by the server, expand the local computer entry and click **Web Sites**.
- 3 Right-click the Web site entry that contains the certificate you want to export and select **Properties**.
- 4 On the Directory Security tab, click **Server Certificate**.
- 5 When the Web Server Certificate wizard appears, click **Next**.

- 6 Select **Export the current certificate to a .pfx file** and click **Next**.
- 7 Specify a filename for the certificate file and click **Next**.
- 8 Type and confirm a password to be used to encrypt the information you want to export and click **Next**.  
The system displays summary information about the certificate you are about to export.
- 9 Verify the summary information and click **Next > Finish**.

#### What to do next

Configure your View Connection Server instance, security server, or View Transfer Server instance to use the certificate. See [“Configure a View Connection Server Instance or Security Server to Use a New Certificate,”](#) on page 80 or [“Configure a View Transfer Server Instance to Use a New Certificate,”](#) on page 81.

## Creating a New SSL Certificate

You can create a new certificate to replace the default server SSL certificate provided with View Connection Server. When you create a new certificate, you must decide whether it should be self-signed or signed by a CA.

Because self-signed certificates are not officially registered with a trusted CA, they are not guaranteed to be authentic. While adequate for data encryption between server and client, self-signed certificates do not provide reliable information about the location of the software application or the corporate entity responsible for its administration.

A CA is a trusted third party 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. If your clients need to determine the origin and integrity of the data they receive, you should obtain a CA-signed certificate.

- 1 [Generate a Keystore and Certificate](#) on page 77  
Whether you plan to use a self-signed certificate, or to obtain a signed certificate from a CA, you must use `keytool` to generate a keystore file and a self-signed certificate.
- 2 [Obtain a Signed Certificate from a CA](#) on page 78  
To obtain a signed certificate from a CA, you must create a CSR. For testing purposes, you can obtain a free temporary certificate based on an untrusted root from Thawte, VeriSign, or GlobalSign.
- 3 [Convert a PKCS#12 Certificate to PKCS#7 Format](#) on page 79  
If you obtained a certificate in PKCS#12 format, you must convert it to PKCS#7 format before importing it into your keystore file.
- 4 [Import a Signed Certificate into a Keystore File](#) on page 79  
If you obtained a signed certificate from a CA, or if you exported an existing Microsoft IIS SSL server certificate, use `keytool` to import the certificate into your keystore file.

## Generate a Keystore and Certificate

Whether you plan to use a self-signed certificate, or to obtain a signed certificate from a CA, you must use `keytool` to generate a keystore file and a self-signed certificate.

When you initially create a keystore file, the first certificate in the keystore file is a self-signed certificate. Later, if you obtain a signed certificate from a CA, you import the response from the CA into the keystore file and the self-signed certificate is replaced.

#### Prerequisites

Add `keytool` to the system path on your host. See [“Add keytool and openssl to the System Path,”](#) on page 76.

**Procedure**

- 1 Open a command prompt and use `keytool` to generate a keystore file.

For example: `keytool -genkey -keyalg "RSA" -keystore keys.p12 -storetype pkcs12 -validity 360`

- 2 When `keytool` prompts you for your first and last name, type the fully qualified domain name (FQDN) that client computers use to connect to the host.

Option	Action
<b>View Connection Server instance</b>	Type the FQDN of the View Connection Server host if you have one View Connection Server instance. Type the FQDN of the load balancer host if you use load balancing.
<b>Security server</b>	Type the FQDN of the security server host.
<b>View Transfer Server instance</b>	Type the FQDN of the View Transfer Server host.

---

**IMPORTANT** If you type your name, the certificate will be invalid.

---

- 3 After `keytool` creates the keystore file, back up the file.

The backup file is useful in case you ever need to rebuild the configuration for the host.

**What to do next**

To use the self-signed certificate contained in the keystore file, configure the View Connection Server instance, security server, or View Transfer Server instance to use the certificate. See [“Configure a View Connection Server Instance or Security Server to Use a New Certificate,”](#) on page 80 or [“Configure a View Transfer Server Instance to Use a New Certificate,”](#) on page 81.

To replace the self-signed certificate, obtain a signed certificate from a CA. See [“Obtain a Signed Certificate from a CA,”](#) on page 78.

**Obtain a Signed Certificate from a CA**

To obtain a signed certificate from a CA, you must create a CSR. For testing purposes, you can obtain a free temporary certificate based on an untrusted root from Thawte, VeriSign, or GlobalSign.

This procedure assumes that there is no more than one link in the chain between the server certificate and the root certificate. If you use a temporary certificate, there might be one or more intermediate certificates and you will need to follow a different procedure. See the instructions provided by the CA that generated the temporary certificate for more information.

**Prerequisites**

Create a keystore file and a self-signed certificate.

**Procedure**

- 1 Open a command prompt and use `keytool` to create a CSR.

For example:

```
keytool -certreq -keyalg "RSA" -file certificate.csr -keystore keys.p12 -storetype pkcs12 -storepass secret
```

`keytool` creates the CSR file in the current directory.

- 2 Send the CSR to the CA in accordance with the CA's enrollment process and request a certificate in PKCS#7 format.

Some CAs provide certificates only in PKCS#12 format. If you download this type of certificate, you must convert it to PKCS#7 format.

After conducting some checks on your company, the CA signs your request, encrypts it with a private key, and sends you a validated certificate.

**What to do next**

If you downloaded a certificate in PKCS#7 format, import it into your keystore file. See [“Import a Signed Certificate into a Keystore File,”](#) on page 79.

If you downloaded a certificate in PKCS#12 format, convert it to PKCS#7 format.

**Convert a PKCS#12 Certificate to PKCS#7 Format**

If you obtained a certificate in PKCS#12 format, you must convert it to PKCS#7 format before importing it into your keystore file.

**Procedure**

- 1 Right-click the certificate (.cer) file and select **Open With > Crypto Shell Extensions**.
- 2 On the **Details** tab, click **Copy to File**.  
The Certificate Export wizard appears.
- 3 Specify PKCS#7 format, include all certificates in the certification path, and then click **Next**.
- 4 Specify a filename and click **Next**.
- 5 Click **Finish** to export the file in PKCS#7 format.

---

**NOTE** Certificate files that are converted to PKCS#7 format have a .p7b extension.

---

**What to do next**

Import the PKCS#7 format certificate into your keystore file.

**Import a Signed Certificate into a Keystore File**

If you obtained a signed certificate from a CA, or if you exported an existing Microsoft IIS SSL server certificate, use keytool to import the certificate into your keystore file.

**Prerequisites**

If your certificate is in PKCS#12 format, convert it to PKCS#7 format.

## Procedure

- 1 Copy the text file that contains your certificate to the directory that contains your keystore file and save it as `certificate.p7`.

For example:

```
-----BEGIN PKCS7-----
MIIF+AYJKoZIhvcNAQcCoIIF6TCCBeUCAQEExADALBgk
LDCCApWgAwIBAgIQTpY7DsV1n1HeMGgMjMR2PzANBgk
i7coVx71/LCB0LFmx66NyKlZK5m0bgvd2dlnsAP+nnS
EhCsdpikSpbtdo18jUubV6z1kQ71CrRQtbi/WtdqxQE
-----END PKCS7-----
```

- 2 Open a command prompt and use `keytool` to import the certificate into your keystore file.

For example:

```
keytool -import -keystore keys.p12 -storetype pkcs12 -storepass secret -keyalg "RSA" -
trustcacerts -file certificate.p7
```

- 3 If you specified a temporary certificate, type **yes** when you receive the message `... is not trusted. Install reply anyway?`.

`keytool` generates this message because temporary certificates are not meant for production use.

## What to do next

Configure your View Connection Server instance, security server, or View Transfer Server instance to use the certificate. See [“Configure a View Connection Server Instance or Security Server to Use a New Certificate,”](#) on page 80 or [“Configure a View Transfer Server Instance to Use a New Certificate,”](#) on page 81.

# Configure a View Connection Server Instance or Security Server to Use a New Certificate

To configure a View Connection Server instance or security server to use a new server SSL certificate, you must set properties in the `locked.properties` file on the View Connection Server or security server host.

## Prerequisites

Create a self-signed certificate, export an existing Microsoft IIS SSL server certificate, or obtain a signed certificate from a CA.

**Procedure**

- 1 Copy the keystore file that contains your certificate to the SSL gateway configuration directory on the View Connection Server or security server host.

For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\keys.p12`

- 2 Add the `keyfile` and `keypass` properties to the `locked.properties` file in the SSL gateway configuration directory on the View Connection Server or security server host.

If the `locked.properties` file does not already exist, you must create it.

- a Set the `keyfile` property to the name of your keystore file.

If you exported an existing Microsoft IIS SSL server certificate, set `keyfile` to the name of your PFX file.

- b Set the `keypass` property to the password for your keystore file.

If you exported an existing Microsoft IIS SSL server certificate, set `keypass` to the password that you used when you exported the certificate.

For example:

```
keyfile=keys.p12
keypass=MY_PASS
```

- 3 Restart the View Connection Server service or Security Server service to make your changes take effect.

## Configure a View Transfer Server Instance to Use a New Certificate

To configure a View Transfer Server instance to use a new server SSL certificate, you must copy your certificate and private key files to the View Transfer Server host.

**Prerequisites**

- Add `openssl` to the system Path variable on your host. See [“Add keytool and openssl to the System Path,”](#) on page 76.
- Create a self-signed certificate, export an existing Microsoft IIS SSL server certificate, or obtain a signed certificate from a CA.

**Procedure**

- 1 Open a command prompt and use `openssl` to export the private key file from your PFX or P12 file.

For example: `openssl pkcs12 -in filename.pfx -nocerts -out key.pem`

- 2 Export the certificate file from your PFX or P12 file.

For example: `openssl pkcs12 -in filename.pfx -clcerts -nokeys -out server.crt`

- 3 Remove the pass phrase from the private key.

This step prevents Apache from prompting you for your pass phrase each time it is restarted.

For example: `openssl rsa -in key.pem -out server.key`

- 4 Stop the View Transfer Server service.
- 5 Copy the certificate and private key files to the directory `install_directory\VMware\VMware View\Server\httpd\conf` on the View Transfer Server host.
- 6 Rename the certificate file to `server.crt`.
- 7 Rename the private key file to `server.key`.

- 8 Restart the View Transfer Server service to make your changes take effect.
- 9 Verify that the certificate is configured correctly by using your Web browser to navigate to `https://transfer_server_host_address`.

## Configure SSL for Client Connections

To configure whether client connections use SSL when communicating with View Connection Server, you configure a global setting in View Administrator. The setting applies to View desktop clients and clients that run View Administrator.

Global settings affect all client sessions that are managed by a standalone View Connection Server instance or a group of replicated instances. They are not specific to a single View Connection Server instance.

If View Connection Server is configured for smart card authentication, SSL must be enabled for client connections.

SSL is enabled by default for client connections.

---

**NOTE** If you disable SSL for client connections, users must deselect the **Use secure connection (SSL)** check box in View Client before connecting to the View Connection Server host and administrators must type an HTTP URL to run View Administrator.

---

### Procedure

- 1 In View Administrator, select **View Configuration > Global Settings** and click **Edit**.
- 2 To configure SSL for client connections, select or deselect **Require SSL for client connections and View Administrator**.
- 3 Click **OK** to save your changes.
- 4 Restart the View Connection Server service to make your changes take effect.

In a group of replicated View Connection Server instances, you can restart the View Connection Server service on any instance in the group.

## Configure SSL for View Transfer Server Communications

To configure whether SSL is used for communications and data transfers between client computers that host local desktops and View Transfer Server, you set View Connection Server settings in View Administrator.

The SSL settings for View Transfer Server communications and data transfers are specific to a single View Connection Server instance. You might want to enable SSL on an instance that services users that connect from the Internet, but disable it on an instance that is dedicated to internal users.

SSL is disabled by default for View Transfer Server communications and data transfers.

---

**NOTE** These SSL settings do not affect local data, which is always encrypted.

---

### Procedure

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 Select the View Connection Server instance and click **Edit**.
- 3 To configure SSL for communications and data transfers between client computers that host local desktops and View Transfer Server, select or deselect **Use SSL for Local Mode operations**.

These operations include checking in and checking out desktops and replicating data from client computers to the datacenter.

- 4 To configure SSL for transfers of View Composer base-image files from the Transfer Server repository to client computers that host local desktops, select or deselect **Use SSL when provisioning desktops in Local Mode**.
- 5 Click **OK** to save your changes.

Your changes take effect immediately. You do not need to restart the View Transfer Server service.

## Using Group Policy to Configure Certificate Checking in View Client

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

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.

See the *VMware View Administrator's Guide* for information on using View Manager group policy settings.



# Creating an Event Database

---

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,”](#) on page 85
- [“Prepare an SQL Server Database for Event Reporting,”](#) on page 86
- [“Configure the Event Database,”](#) on page 86

## 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 30.
- 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 32.

**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 86.

## 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 85.
- 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 *YYY* 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 86.

## 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.

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 Guide*.

## 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 85.
- The username and password of the user you created for this database. See “[Add a Database and Database User for View Events](#),” on page 85.

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, an 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 Dashboard, the System Component Status displays the event database server under the Reporting Database heading.



# Installing and Starting View Client

---

You can obtain the 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.

This chapter includes the following topics:

- [“Install the Windows-Based View Client or View Client with Local Mode,”](#) on page 89
- [“Start the Windows-Based View Client or View Client with Local Mode,”](#) on page 90
- [“Install View Client by Using View Portal,”](#) on page 92
- [“Install View Client on Mac OS X,”](#) on page 93
- [“Start View Client on Mac OS X,”](#) on page 94
- [“Set Printing Preferences for the Virtual Printer Feature,”](#) on page 96
- [“Using USB Printers,”](#) on page 97
- [“Installing View Client Silently,”](#) on page 97

## 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.

In addition to accessing virtual desktops with View Client, end users can use View Client to configure some display options if the View administrator enables these options. For example, end users can optionally choose a display protocol or window size or use their current login credentials for View authentication.

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.

### Prerequisites

- Verify that you can log in as an administrator on the client system.
- Verify that the client system uses a supported operating system. See [“Supported Operating Systems for View Client and View Client with Local Mode,”](#) on page 16.
- Verify that View Agent is not installed.
- If you plan to install View Client with Local Mode, verify that your license includes View Client with Local Mode.

- If you plan to install 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 the person who uses the client device is allowed to access locally connected USB devices from a virtual desktop. If not, you must deselect the **USB Redirection** component that the wizard presents.
- 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 single-sign-on feature. This feature 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 IP address or fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the IP address or 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.

Option	Action
<b>View Client on 64-bit operating systems</b>	Select <code>VMware-viewclient-x86_64-4.5.x-xxxxxx.exe</code> for View Client. Select <code>VMware-viewclientwithlocalmode-x86_64-4.5.x-xxxxxx.exe</code> for View Client with Local mode.
<b>View Client on 32-bit operating systems</b>	Select <code>VMware-viewclient-4.5.x-xxxxxx.exe</code> for View Client. Select <code>VMware-viewclientwithlocalmode-4.5.x-xxxxxx.exe</code> 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 `wsm.exe`. The service name for the USB component is `wsm_usbctrl.exe`.

### What to do next

Start the View Client and verify that you can log in to the correct virtual desktop. See “[Start the Windows-Based View Client or View Client with Local Mode](#),” on page 90 or “[Install View Client by Using View Portal](#),” on page 92.

## Start the Windows-Based View Client or View Client with Local Mode

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

- Verify that View Client or View Client with Local Mode is installed on the client device.
- If you plan to use View Client with Local Mode, verify that your license includes View Client with Local Mode and verify that the View desktop meets the requirements for local mode. See the overview topic for setting up a local desktop deployment in the *VMware View Administrator's Guide*.
- Verify that a virtual desktop pool has been created and that the user account you plan to use is entitled to access this desktop. See the topics about creating desktop pools in the *VMware View Administrator's Guide*.
- Verify that you have the fully qualified domain name (FQDN) or IP address of the View Connection Server instance that provides access to the virtual desktop.

## Procedure

- 1 If View Client does not start automatically after installation, double-click the desktop shortcut or click **Start > Programs > VMware > VMware View Client**.
- 2 In the **Connection Server** drop-down menu, enter the host name or IP address of View Connection Server.
- 3 Verify that the other optional settings in the dialog box appear as you configured them.

Option	Description
<b>Log in as current user</b>	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.
<b>Use secure connection (SSL)</b>	If this check box is selected, you must also select the global setting called <b>Use SSL for client connections</b> in View Administrator.
<b>Port</b>	If you use a secure connection, the default port is 443.
<b>Autoconnect</b>	If you select this check box, the next time you start View Client, the <b>Connection Server</b> field is disabled and you are connected to the server specified when you selected the <b>Autoconnect</b> check box. To deselect this check box, cancel the next dialog box that appears and click <b>Options</b> to display and change this setting.

- 4 Click **Connect**.
- 5 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 Administrator's Guide*.

- 6 (Optional) In the **Display** drop-down menu, select the window size for displaying the View desktop.
- 7 (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.

- 8 Select a desktop from the list of desktop pools and click **Connect**.

View Client attempts to connect to a desktop in the specified pool.

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:

- Verify that the View Client setting for using secure (SSL) connections matches the global setting in View Administrator. For example, if the check box for secure connections is deselected on the client, the check box must also be deselected in View Administrator.
- 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 Administrator's Guide*.
- Verify that the user is entitled to access this desktop. See the *VMware View Administrator's Guide*.
- 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 or IP address 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 Administrator's Guide*.

- 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.

## Install View Client by Using View Portal

An expedient way of 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 of View 4.5, View Portal installs the full View Client for Windows, with or without Local Mode, and View Client for the Mac.

---

**NOTE** View Portal does not support Linux. A native client for Linux is available only through certified VMware partners.

---

### Prerequisites

- 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 View Client and View Client with Local Mode,”](#) on page 16.
- Verify that View Agent is not installed.
- If you plan to install View Client with Local Mode, verify that your license includes View Client with Local Mode.

- If you plan to install 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 the person who uses the client device is allowed to access locally connected USB devices from a virtual desktop. If not, you must deselect the **USB Redirection** component that the wizard presents.
- 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.

Internet Explorer can determine whether an upgrade is available, whereas Firefox and Safari cannot. Also, in the list of installers, Internet Explorer lists 32-bit installers if the client has a 32-bit system and lists 64-bit installers if the client has a 64-bit system, whereas Firefox lists both 32-bit and 64-bit installers.

- 3 Follow the prompts on the Web page.

If the version available from View Connection Server is newer than that installed on the client device, you can choose to upgrade. If the version is the same as that on the client device, View Portal starts the View Client installed on the client computer.

If you have an older version of View Client and a smart card is required for client connections, an Internet Explorer browser prompts you to insert your smart card before View Portal checks the version of your existing View Client.

- 4 If Internet Explorer prompts you to insert a smart card, either insert the card or click **Cancel**.

Inserting a smart card and **Cancel** have the same effect.

### What to do next

Connect to the View desktop. See [“Start the Windows-Based View Client or View Client with Local Mode,”](#) on page 90 or [“Start View Client on Mac OS X,”](#) on page 94.

## Install View Client on Mac OS X

End users open View Client to connect to virtual desktops from a Mac OS X physical machine. You install View Client on Mac OS X client systems from a disk image file.

### Prerequisites

- Verify that the client system uses a supported operating system. See [“Supported Operating Systems for View Client and View Client with Local Mode,”](#) on page 16.
- Verify that the Mac client system has Remote Desktop Connection version 2.0 or higher installed. The View Client disk image file includes a link to the Microsoft Remote Desktop Connection Client for Mac download page.

### Procedure

- 1 Log in to the client system.
- 2 On the client system, download the View Client disk image file from the VMware product page at <http://www.vmware.com/products/>.

Select the `VMware-View-Client-4.5.x-xxxxxx.dmg` disk image file, where `xxxxxx` is the build number.

- 3 Double-click the `.dmg` file to open it and click **Agree**.

The contents of the disk image appear in a VMware View Client Finder window.

- 4 Open a new Finder window and navigate to the Applications folder.
- 5 Drag the VMware View Client icon to the Applications folder.

If you are not logged in as an administrator user, you are prompted for an administrator user name and password.

You can now unmount the disk image.

### What to do next

Start View Client and verify that you can log in to the correct virtual desktop. See [“Start View Client on Mac OS X,”](#) on page 94.

## Start View Client on Mac OS X

Before you have end users access their virtual desktops, test that you can log in to a virtual desktop from the Mac client system.

In addition to accessing virtual desktops with View Client, end users can configure View Client settings. For example, end users can optionally choose a window size or use their current login credentials for View authentication.

### Prerequisites

- Verify that View Client is installed on the client system.
- Verify that a virtual desktop pool has been created and that the user account you plan to use is entitled to access this desktop. See the topics about creating desktop pools in the *VMware View Administrator's Guide*.
- Verify that you have the fully qualified domain name (FQDN) or IP address of the View Connection Server instance that provides access to the virtual desktop.
- Verify that the AllowDirectRDP View Agent group policy setting is enabled. This setting is enabled by default.

### Procedure

- 1 In the folder where you installed View Client (typically the Applications folder), double-click **VMware View Client**.
- 2 Select your View Connection Server from the **Address** drop-down menu, or enter the server host name or IP address.

- 3 (Optional) Choose options for how you connect to the selected server.

Option	Description
<b>Port</b>	Specify the port number, or leave blank to use the default port for View Connection Server.
<b>Use Secure Connection (SSL)</b>	Select to use a secure (SSL) connection to protect sensitive corporate information and ensure that all connections are completely encrypted. Your View administrator might have configured View Connection Server to always use a secure connection, even if you select a nonsecure connection.
<b>Always connect to this server at startup</b>	Select to connect directly to the current instance of View Connection Server when you start View Client. Select this option if you always connect to the same View Connection Server. If deselected, you must enter or select a View Connection Server when you start View Client.

You can also supply the port and SSL options by typing them into the address field directly. For a non-SSL connection, type `http://URL[:port number]`. For an SSL connection, type `https://URL[:port number]`.

- 4 Click **Continue**.

You are connected to View Connection Server and can now log in.

- 5 Enter your user name and password in the login dialog box.

If you type the user name as `user@domain`, it is treated as a user principal name (UPN) because of the at-sign (@), so the domain drop-down menu dims. Otherwise, you must also select a domain.

- 6 (Optional) Select **Remember this password in my keychain** to securely store your login credentials.

- 7 Click **Continue**.

If login is successful, the list of desktops that you are authorized to use appears.

- 8 Select a desktop from the list.

- 9 (Optional) Select an option from the **Display** drop-down menu.

Option	Description
<b>Full Screen</b>	Display the desktop over the complete monitor screen. If you select Full Screen and have multiple monitors, drag the desktop selection window to the monitor in which you want the desktop to appear.
<b>Large Window</b>	Display the desktop in a large window.
<b>Small Window</b>	Display the desktop in a small window.
<b>Custom</b>	Use the slider in the displayed dialog box to set the window size and click <b>Select</b> . The size you select is added to the <b>Display</b> drop-down menu.

Display settings are retained the next time you open the desktop.

- 10 Click **Continue**, or click the Action menu (with the Gear icon) and select **Connect**.

After you are connected, the client window appears. If View Client cannot connect to the desktop, perform the following tasks:

- Verify that the View Client setting for using secure (SSL) connections matches the global setting in View Administrator. For example, if the check box for secure connections is deselected on the client, the check box must also be deselected in View Administrator.
- 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.
- Verify that the tags set on the View Connection Server instance allow connections from this user. See the *VMware View Administrator's Guide*.

- Verify that the user is entitled to access this desktop. See the *VMware View Administrator's Guide*.
- Verify that the client computer allows remote desktop connections.

### What to do next

For instructions on using View Client, see the VMware View Client Help.

## Set Printing Preferences for the Virtual Printer Feature

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 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 Administrator's Guide*.

### 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**.
- 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 recommend 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.

- 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.

- 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**, 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**, 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 you can log in as an administrator on the client system.
- Verify that the client system uses a supported operating system. See [“Supported Operating Systems for View Client and View Client with Local Mode,”](#) on page 16.
- If you plan to install View Client with Local Mode, verify that your license includes View Client with Local Mode.
- If you plan to install 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 single-sign-on feature. This feature 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 IP address or fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the IP address or FQDN so that you can supply it during installation.
- Familiarize yourself with the MSI installer command-line options. See [“Microsoft Windows Installer Command-Line Options,”](#) on page 48.
- Familiarize yourself with the silent installation (MSI) properties available with View Client. See [“Silent Installation Properties for View Client,”](#) on page 99.
- 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 99.
- If you install View Client with Local Mode, 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 97.

## 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.

Option	Action
<b>View Client on 64-bit operating systems</b>	Select <code>VMware-viewclient-x86_64-4.5.x-xxxxxx.exe</code> for View Client. Select <code>VMware-viewclientwithlocalmode-x86_64-4.5.x-xxxxxx.exe</code> for View Client with Local mode.
<b>View Client on 32-bit operating systems</b>	Select <code>VMware-viewclient-4.5.x-xxxxxx.exe</code> for View Client. Select <code>VMware-viewclientwithlocalmode-4.5.x-xxxxxx.exe</code> 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-4.5.x-xxxxxx.exe /s /v"/qn VDM_SERVER=cs1.companydomain.com ADDLOCAL=Core,TSSO,USB"`

This example installs View Client with Local Mode: `VMware-viewclientwithlocal-4.5.x-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 [“Start the Windows-Based View Client or View Client with Local Mode,”](#) on page 90 or [“Install View Client by Using View Portal,”](#) on page 92.

## 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 9-1](#) shows the View Client silent installation properties that you can use at the command-line.

**Table 9-1.** 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: <code>INSTALLDIR=""D:\abc\my folder""</code> The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	%ProgramFiles %\VMware\VMware View\Client
VDM_SERVER	The fully qualified domain name (FQDN) or IP address 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 or IP address. For example: <code>VDM_SERVER=cs1.companydomain.com</code> This MSI property is optional.	None

**Table 9-1.** 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 9-2](#) shows the View Client features you can type at the command line and the corresponding interactive-installation options.

**Table 9-2.** View Client Silent Installation Features and Interactive Custom Setup Options

Silent Installation Feature	Custom Setup Option in an Interactive Installation
<p>Core</p> <p>If you specify individual features with the MSI property, <code>ADDLOCAL=</code>, you must include <b>Core</b>.</p> <p>If you specify <code>ADDLOCAL=ALL</code>, all View Client and View Client with Local Mode features, including Core, are installed.</p>	<p>None.</p> <p>During an interactive installation, the core View Client functions are installed by default.</p>
<p>MVDI</p> <p>Use this feature when you install View Client with Local Mode and specify individual features with <code>ADDLOCAL=</code>.</p> <p>If you specify <code>ADDLOCAL=ALL</code>, all View Client with Local Mode features, including MVDI, are installed.</p>	<p>None.</p> <p>When you install View Client with Local Mode interactively, the MVDI functions are installed by default.</p> <p>When you install View Client interactively, the MVDI functions are not available.</p>
ThinPrint	Virtual Printing
TSSO	Single Sign-on (SSO)
USB	USB Redirection

# Index

## A

- Active Directory
  - configuring domains and trust relationships **23**
  - preparing for smart card authentication **26**
  - preparing for use with View **23**
- Active Directory groups
  - creating for kiosk mode client accounts **24**
  - creating for View users and administrators **24**
- ADM template files **26**
- Adobe Flash requirements **21**
- antivirus software, View Composer **36**

## B

- browser requirements **9, 18**

## C

- certificate signing requests, *See* CSRs
- certificates
  - checking in View Client **83**
  - configuring View Connection Server to use **80**
  - configuring View Transfer Server to use **81**
  - converting to PKCS#7 format **79**
  - creating new **77**
  - importing to a keystore file **79**
  - obtaining signatures **78**
  - replacing the default **75**
  - requirements **75**
  - using keytool to generate **77**
- certutil command **28**
- client software requirements **15**
- CPU requirements, local mode desktops **16**
- CSRs, creating **78**

## D

- databases
  - creating for View Composer **29**
  - View events **85, 86**
- default certificate, replacing **75**
- direct connections, configuring **58**
- display requirements, local mode desktops **16**
- DNS resolution, View Composer **36**
- documentation feedback, how to provide **5**
- domain filtering **24**

## E

- Enterprise NTAAuth store, adding root certificates **28**
- ephemeral ports
  - calculating **60**
  - how View Manager uses **60**
  - increasing on a Windows Server computer **60**
- ESX hosts, View Composer **36**
- event database
  - creating for View **85, 86**
  - SQL Server configuration **86**
- external URLs
  - configuring for a View Connection Server instance **58**
  - modifying for a security server **59**
  - purpose and format **58**

## F

- Firefox, supported versions **9, 18**
- firewall rules
  - View Connection Server **41**
  - View Transfer Server **71**
- firewalls, configuring **38**

## G

- glossary, where to find **5**
- GPOs, linking to a View desktop OU **26**
- Group Policy Objects, *See* GPOs
- GroupPolicyFiles directory **26**

## H

- hardware requirements
  - local mode desktops **16**
  - PCoIP **19**
  - smart card authentication **21**
- HP RGS **20**

## I

- Internet Explorer, supported versions **9, 18**

## J

- JVM heap size
  - default **64**
  - increasing **64**

## K

- keychain **94**

- keyfile property **80**
- keypass property **80**
- keytool utility
  - adding to the system path **76**
  - creating a CSR **78**
  - generating a keystore file **77**
- kiosk mode, Active Directory preparation **24**

**L**

- license key, View Connection Server **55**
- local desktop configuration
  - adding a View Transfer Server instance **67, 69**
  - creating a vCenter Server user **51**
  - hardware requirements **16**
  - privileges for vCenter Server user **54**
- locked.properties file **80**
- Log in as current user feature **90**

**M**

- Mac OS X, installing View Client **93**
- media file formats, supported **21**
- memory requirements, local mode desktops **16**
- Microsoft IIS SSL server certificates, using existing **76**
- Microsoft Windows Installer
  - command-line options for silent installation **48**
  - MSI properties for View Transfer Server **73**
  - properties for replicated View Connection Server **44**
  - properties for security server **48**
  - properties for View Client **99**
  - properties for View Connection Server **40**
  - uninstalling View Components silently **50**
- multimedia redirection (MMR) **21**

**O**

- ODBC
  - connecting to Oracle 11g or 10g **32**
  - connecting to Oracle 9i **34**
  - connecting to SQL Server **31**
- openssl utility
  - adding to the system path **76**
  - configuring a certificate for View Transfer Server **81**
- Oracle 10g database
  - adding an ODBC data source **32**
  - adding for View Composer **32**
- Oracle 11g database
  - adding an ODBC data source **32**
  - adding for View Composer **32**
- Oracle 9i database
  - adding an ODBC data source **34**
  - adding for View Composer **33**
- organizational units, See OUs

- OS X, installing View Client **93**
- OUs
  - creating for kiosk mode client accounts **24**
  - creating for View desktops **24**

**P**

- page-file size, View Connection Server **65**
- PCoIP, hardware requirements **19**
- PKCS#12 format certificates **79**
- PKCS#7 format certificates **79**
- policies
  - Restricted Groups **25**
  - Trusted Root Certification Authorities **27**
- printers, setting up **96**
- professional services **5**

**R**

- RDP **20**
- remote display protocols
  - HP RGS **20**
  - PCoIP **19**
  - RDP **20**
- replicated instances
  - installing **41**
  - installing silently **43**
  - network requirements **8**
  - silent installation properties **44**
- Restricted Groups policy, configuring **25**
- RGS **20**
- root certificates
  - adding to the Enterprise NTAAuth store **28**
  - adding to trusted roots **27**

**S**

- security servers
  - calculating TCB hash table size **62**
  - configuring a pairing password **44**
  - configuring an external URL **58**
  - configuring to use a certificate **80**
  - installer file **45**
  - installing silently **46**
  - modifying an external URL **59**
  - silent installation properties **48**
- silent installation
  - group policies to allow installation **71, 97**
  - replicated instances **43**
  - security servers **46**
  - View Client **97, 98**
  - View Client with Local Mode **98**
  - View Connection Server **39**
  - View Transfer Server **71, 72**
- sizing Windows Server settings
  - calculating ephemeral ports **60**
  - calculation worksheets **63**

- increasing ephemeral ports **60**
- increasing the JVM heap size **64**
- increasing the TCB hash table size **63**
- smart card authentication
  - Active Directory preparation **26**
  - requirements **21**
  - UPNs for smart card users **27**
- software requirements, server components **7**
- SQL Server database
  - adding an ODBC data source **31**
  - adding for View Composer **30**
  - preparing for event database **86**
- SQL Server Management Studio Express, installing **30**
- SSL
  - configuring for client connections **82**
  - configuring for View Transfer Server communications **82**
- SSL certificates, *See* certificates
- streaming multimedia **21**
- support, online and telephone **5**
- Sysprep, requirements for View Composer **11**
- system page file size, Windows Server **65**

## T

- TCB hash table
  - how View uses **61**
  - increasing size for non-security servers **61**
  - increasing size for security servers **62**
  - increasing size on a Windows Server computer **63**
- TCP ports
  - View Connection Server **41**
  - View Transfer Server **71**
- technical support and education **5**
- ThinPrint setup **96**
- Transfer Server repository, configuring **70**
- transmission control block
  - how View uses **61**
  - increasing size for non-security servers **61**
  - increasing size for security servers **62**
- trust relationships, configuring for View Connection Server **23**
- Trusted Root Certification Authorities policy **27**

## U

- uninstalling View components **50**
- UPNs
  - smart card users **27**
  - View Client **90**
  - View Client on Mac OS X **94**
  - View Client with Local Mode **90**
- USB printers **97**
- user accounts
  - requirements **51**

- vCenter Server **24, 51**
- View Composer **25, 51**
- userPrincipalName attribute **27**

## V

- vCenter Server
  - adding instances to View Manager **55**
  - configuring for View Composer **36**
  - creating a user for local mode **51**
  - installing the View Composer service **34**
  - user accounts **24, 51**
- vCenter Server user
  - local mode privileges **54**
  - vCenter Server privileges **53**
  - View Composer privileges **53**
- View Administrator
  - logging in **54**
  - overview **54**
  - requirements **9**
- View Agent, installation requirements **15**
- View Client
  - installation overview **89**
  - installing on a Windows PC or laptop **89**
  - installing on Mac OS X **93**
  - installing silently on a Windows PC or laptop **97, 98**
  - silent installation properties **99**
  - starting **89, 90, 94**
  - supported operating systems **16**
  - using View Portal to install **92**
- View Client with Local Mode
  - group policies for silent installation **97**
  - supported operating systems **16**
- View clients, configuring connections **57**
- View components, command-line options for silent installation **48**
- View Composer configuration
  - creating a user account **25**
  - creating a vCenter Server user **24, 51**
  - privileges for the vCenter Server user **53**
  - settings in View Administrator **56**
- View Composer database
  - ODBC data source for Oracle 11g or 10g **32**
  - ODBC data source for Oracle 9i **34**
  - ODBC data source for SQL Server **31**
  - Oracle 11g and 10g **32**
  - Oracle 9i **33**
  - requirements **29**
  - SQL Server **30**
- View Composer infrastructure
  - configuring vSphere **36**
  - optimizing **36**
  - testing DNS resolution **36**
- View Composer installation
  - database requirements **10**

- installer file **34**
- operating system requirements **10**
- overview **29**
- requirements overview **9**
- virtualization software requirements **11**
- View Connection Server configuration
  - client connections **57**
  - event database **85, 86**
  - external URL **58**
  - first time **54**
  - overview **37**
  - replacing the default certificate **75**
  - server certificate **80**
  - sizing Windows Server settings **59**
  - system page file size **65**
  - trust relationships **23**
- View Connection Server installation
  - hardware requirements **7**
  - installation types **37**
  - network configuration **8**
  - overview **37**
  - prerequisites **37**
  - product license key **55**
  - replicated instances **41**
  - requirements overview **7**
  - security servers **45**
  - silent **39**
  - silent installation properties **40**
  - single server **38**
  - supported operating systems **8**
  - virtualization software requirements **8**
- View desktops, configuring direct connections **58**
- View Portal, browser requirements **18**
- View Secure Gateway Server component, increasing the JVM heap size **64**
- View Transfer Server configuration
  - adding an instance **69**
  - Transfer Server repository **70**
- View Transfer Server installation
  - group policies for silent installation **71**
  - installer file **67**
  - overview **67**
  - requirements overview **11**
  - silent **71, 72**
  - silent installation properties **73**
  - storage requirements **13**
  - supported operating systems **12**
  - virtual machine requirements **12**
- virtual printing feature **96**
- vSphere, configuring for View Composer **36**

## W

- Web browser requirements **9, 18**
- Windows 7 requirements, local mode desktops **16**
- Windows computers, installing View Client **89**
- Windows Server, system page file size **65**
- worksheets, calculating ephemeral ports and TCB has table size **63**
- Wyse MMR **21**