

# VMware View Upgrades

View 5.1

View Manager 5.1

View Composer 3.0

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

EN-000733-00

**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 © 2009–2012 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

VMware View Upgrades	5
<b>1</b> VMware View Component Compatibility Matrix	7
<b>2</b> VMware View Upgrade Overview	9
<b>3</b> System Requirements for Upgrades	11
View Connection Server Requirements	11
Hardware Requirements for View Connection Server	11
Supported Operating Systems for View Connection Server	12
Upgrade Requirements for View Connection Server	12
Virtualization Software Requirements for View Connection Server	13
View Composer Requirements	13
Supported Operating Systems for View Composer	13
Hardware Requirements for Standalone View Composer	14
Database Requirements for View Composer	14
Upgrade Requirements for View Composer	15
View Transfer Server Requirements	16
Installation and Upgrade Requirements for View Transfer Server	16
Supported Operating Systems for View Transfer Server	16
View Administrator Requirements	16
Supported Operating Systems for Windows-Based View Client and View Client with Local Mode	17
Hardware Requirements for Local Mode Desktops	17
Client Browser Requirements for View Portal	19
Supported Operating Systems for View Agent	19
<b>4</b> Preparing for a VMware View Upgrade	21
Preparing View Connection Server for an Upgrade	21
Prepare to Upgrade or Reinstall a Security Server	22
Preparing vCenter Server and View Composer for an Upgrade	23
<b>5</b> Upgrading VMware View Server Components	25
Upgrade View Connection Servers in a Replicated Group	25
Accept the Thumbprint of a Default SSL Certificate	27
Upgrade to View Connection Server 5.1 on a Different Machine	28
Create a Replicated Group After Reverting View Connection Server to a Snapshot	29
Upgrade View Security Server	30
Upgrade View Composer	31
Manually Upgrading the View Composer Database	32
Migrate View Composer to Another Computer	35
Upgrade vCenter Server	40

	Upgrade View Transfer Server	41
	Upgrade to View Transfer Server 5.1 on a Different Machine	42
<b>6</b>	<b>Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines</b>	<b>45</b>
<b>7</b>	<b>Upgrading VMware View Desktops and Clients</b>	<b>47</b>
	Upgrade View Agent	47
	Upgrade View Composer Desktop Pools	49
	Upgrade View Clients	50
	Upgrade View Local Mode Clients	51
<b>8</b>	<b>Applying VMware View Patches</b>	<b>53</b>
	Apply a Patch for View Connection Server	53
	Apply a Patch for View Composer	54
	Apply a Patch for View Agent	55
	Apply a Patch for View Clients	56
<b>9</b>	<b>Upgrading vSphere Components Separately in a VMware View Environment</b>	<b>57</b>
	Index	59

# VMware View Upgrades

---

*VMware View Upgrades* provides instructions for upgrading from VMware® View™ 4.6.x or 5.0.x to View 5.1. You can also use this guide when you upgrade to View 5.1 maintenance and patch releases.

If you are also upgrading your version of vSphere, this guide tells you which steps of that upgrade to do at various stages of the VMware View upgrade.

For VMware View 5.1 patch releases, see [Chapter 8, “Applying VMware View Patches,”](#) on page 53.

## Intended Audience

This guide is intended for anyone who needs to upgrade to View 5.1. The information in this guide is written for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.



# VMware View Component Compatibility Matrix

# 1

Because large enterprises must often perform phased upgrades, VMware View components are designed to be somewhat forward and backward compatible, at least during upgrades.

View Connection Server compatibility with View Agents is limited to interoperability during a View Connection Server upgrade. You must upgrade View Agents as soon as possible to match the version of the View Connection Server that manages them.

The following tables list the components of VMware View and show whether they are compatible with other components whose version is different. For information about compatibility with VMware Infrastructure and vSphere, see [“Virtualization Software Requirements for View Connection Server,”](#) on page 13.

**Table 1-1.** Compatibility Matrix for VMware View 5.1 and 5.0.x Components

	Connection Server 5.0.x	Security Server 5.0.x (PCoIP and RDP)	View Composer 2.7	View Agent 5.0.x	View Client (Windows) 5.0.x	View Transfer Server 5.0.x	View Client with Local Mode 5.0.x
Connection Server 5.1	Only during upgrade	Only if paired before upgrade	No	Only during upgrade	Yes	No	Yes
Security Server 5.1 (PCoIP and RDP)	No	N/A	No	Only during upgrade	Yes	No	Yes
View Composer 3.0	Only during upgrade	Only during upgrade	N/A	Only during upgrade	N/A	N/A	N/A
View Agent 5.1	No	No	No	N/A	Only during upgrade	Yes	Yes
View Client (Windows) 5.1	5.0.1 Connection Server only	Yes	Yes	Yes	N/A	Yes	N/A
View Transfer Server 5.1	No	N/A	N/A	Yes	N/A	N/A	Yes
View Client with Local Mode 5.1	5.0.1 Connection Server only	Yes	Yes	Yes	N/A	Yes	N/A

Although View Client 5.1 can work with View Connection Server 5.0.0, the View 5.1 security enhancements and certificate checking are available only with View Connection Server 5.0.1 and 5.1.

**Table 1-2.** Compatibility Matrix for VMware View 5.1 and 4.6.x Components

	Connection Server 4.6.x	Security Server 4.6.x (PCoIP and RDP)	View Composer 2.6	View Agent 4.6.x	View Client (Windows) 4.6.x	View Transfer Server 4.6.x	View Client with Local Mode 4.6.x
Connection Server 5.1	Only during upgrade	Only if paired before upgrade	No	Only during upgrade	5.0.1 client only	No	5.0.1 client only
Security Server 5.1 (PCoIP and RDP)	No	N/A	No	Only during upgrade	5.0.1 client only	No	5.0.1 client only
View Composer 3.0	Only during upgrade	Only during upgrade	N/A	Only during upgrade	N/A	N/A	N/A
View Agent 5.1	No	No	No	N/A	Only during upgrade	Yes	Yes
View Client (Windows) 5.1	4.6.1 Connection Server only	4.6.1 security server only	Yes	Yes	N/A	Yes	N/A
View Transfer Server 5.1	No	N/A	N/A	Yes	N/A	N/A	Yes
View Client with Local Mode 5.1	4.6.1 Connection Server only	4.6.1 security server only	Yes	Yes	N/A	Yes	N/A



**CAUTION** During an upgrade to View 5.1, View does not support View Composer provisioning and maintenance operations, local mode operations, or View Transfer Server publish operations. Operations such as provisioning and recomposing linked-clone desktops, checking out or checking in desktops, and publishing View Composer base images are not supported during the transitional period when any View servers are still running the earlier version. You can successfully perform these operations only when all instances of View Connection Server, View Composer, and View Transfer Server have been upgraded to View 5.1.

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



# VMware View Upgrade Overview

---

Upgrading an enterprise VMware View deployment involves several high-level tasks. Upgrading is a multistage process in which procedures must be performed in a particular order.

During an upgrade to View 5.1, View does not support View Composer provisioning and maintenance operations, local mode operations, or View Transfer Server publish operations. Operations such as provisioning and recomposing linked-clone desktops, checking out or checking in desktops, and publishing View Composer base images are not supported during the transitional period when any View servers are still running the earlier version. You can successfully perform these operations only when all instances of View Connection Server, View Composer, and View Transfer Server have been upgraded to View 5.1.

You must complete the upgrade process in a specific order. Order is also important within each upgrade stage.

---

**NOTE** This overview relates to upgrades for major, minor, and maintenance releases. For information about patches, see [Chapter 8, “Applying VMware View Patches,”](#) on page 53.

---

How many of the following tasks you need to complete depends on which components of VMware View you use in your deployment.

- 1 On the physical or virtual machines that host View Connection Server instances, make backups and record various configuration and system settings. See [“Preparing View Connection Server for an Upgrade,”](#) on page 21.
- 2 On the physical or virtual machines that host View Composer and vCenter Server, make backups and temporarily halt certain scheduled tasks. See [“Preparing vCenter Server and View Composer for an Upgrade,”](#) on page 23.

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

- 3 If you use View 5.1 security servers, perform the tasks in [“Prepare to Upgrade or Reinstall a Security Server,”](#) on page 22.
- 4 Upgrade View Connection Server on the existing host or migrate to a new machine. See [“Upgrade View Connection Servers in a Replicated Group,”](#) on page 25.

---

**IMPORTANT** After you upgrade a View Connection Server instance to View 5.1, you cannot downgrade that instance to an earlier version. After you upgrade all View Connection Server instances in a replicated group, you cannot add another instance that runs an earlier version of View.

---

- 5 If you use View security servers, upgrade to 5.1, see [“Upgrade View Security Server,”](#) on page 30.
- 6 Upgrade View Composer on an existing Windows Server 2008 host or, if you are running View Composer 2.6 on Windows Server 2003, migrate to a new machine. See [“Upgrade View Composer,”](#) on page 31.

- 7 If you are also upgrading vSphere components, upgrade vCenter Server. See [“Upgrade vCenter Server,”](#) on page 40.
- 8 For the View Client with Local Mode component, upgrade or install and configure one or more View Transfer Server instances. See the *VMware View 5.1 Installation* document or, for upgrades, see [“Upgrade View Transfer Server,”](#) on page 41.  
  
This server transfers data that end users need to check out and run View desktops locally on their client systems.
- 9 If you are also upgrading vSphere, upgrade the ESXi hosts and virtual machines. See [Chapter 6, “Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines,”](#) on page 45.
- 10 Upgrade the VMware View software that runs on the physical or virtual machines that are used as desktop sources, as full-clone desktops in a pool, and as individual desktops in a manual pool. See [“Upgrade View Agent,”](#) on page 47.
- 11 Use the newly upgraded virtual desktop sources to create upgraded pools of View desktops. See [“Upgrade View Composer Desktop Pools,”](#) on page 49.
- 12 Upgrade the VMware View software that runs on end users' client devices. See [“Upgrade View Clients,”](#) on page 50 and [“Upgrade View Local Mode Clients,”](#) on page 51.

Because certain commands can simultaneously upgrade more than one stage, VMware recommends that you thoroughly understand the irreversible changes at each stage before you upgrade your production environments.

## System Requirements for Upgrades

Hosts and virtual machines in a VMware View deployment must meet specific hardware and operating system requirements.

This chapter includes the following topics:

- [“View Connection Server Requirements,”](#) on page 11
- [“View Composer Requirements,”](#) on page 13
- [“View Transfer Server Requirements,”](#) on page 16
- [“View Administrator Requirements,”](#) on page 16
- [“Supported Operating Systems for Windows-Based View Client and View Client with Local Mode,”](#) on page 17
- [“Hardware Requirements for Local Mode Desktops,”](#) on page 17
- [“Client Browser Requirements for View Portal,”](#) on page 19
- [“Supported Operating Systems for View Agent,”](#) on page 19

### 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

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

**Table 3-1.** View Connection Server Hardware Requirements

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

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

---

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

---

## Supported Operating Systems for View Connection Server

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

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

**Table 3-2.** Operating System Support for View Connection Server

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

## Upgrade Requirements for View Connection Server

The View Connection Server upgrade process has specific requirements and limitations.

- View Connection Server requires a valid license key for View 5.1.
- The domain user account that you use to install the new version of View Connection Server must have administrative privileges on the View Connection Server host. The View Connection Server administrator must have administrative credentials for vCenter Server.
- With View Connection Server 5.0 and later releases, when you run the installer, you authorize a View Administrators account. You can specify the local Administrators group or a domain user or group account. View assigns full View Administration rights, including the right to install replicated View Connection Server instances, to this account only. If you specify a domain user or group, you must create the account in Active Directory before you run the installer.
- With View 5.1, when you back up View Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup View configuration, you must provide the data recovery password. The password must contain between 1 and 128 characters.

## Security-Related Requirements

- View Connection Server requires an SSL certificate that is signed by a CA (certificate authority) and that your clients can validate. To improve the security of VMware View deployments, VMware is deprecating support for View Client authentication and brokering over a non-secured HTTP connection. In the past, you could use the default self-signed certificate that is generated in the absence of a CA-signed certificate. With View 5.1, you must replace the default self-signed certificate as soon as possible. Self-signed certificates are shown as invalid in View Administrator.

Also, as a security enhancement, updated View clients expect information about the server's certificate to be communicated as part of the XML handshake between client and server. Often updated clients do not trust self-signed certificates. For complete information about security certificate requirements, see "Configuring SSL Certificates for View Servers" in the *VMware View Installation* guide.

---

**NOTE** If your original View servers already have SSL certificates signed by a CA, during the upgrade, View imports your existing CA-signed certificate into the Windows Server certificate store.

---

- Certificates for vCenter Server, View Composer, and View servers must include certificate revocation lists (CRLs). For more information, see "Configuring Certificate Revocation Checking on Server Certificates" in the *VMware View Installation* guide.
- If you plan to pair a security server with this View Connection Server instance, verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- If your network topology includes a firewall between a security server and a View Connection Server instance, you must configure the firewall to support IPsec. See the *VMware View Installation* document.

If you plan to perform fresh installations of View Connection Server instances on additional physical or virtual machines, see the complete list of installation requirements in the *VMware View Installation* document.

## Virtualization Software Requirements for View Connection Server

View Connection Server requires certain versions of VMware virtualization software.

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

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

## 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

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

**Table 3-3.** Operating System Support for View Composer

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

If you plan to install View Composer on a different physical or virtual machine than vCenter Server, see "Hardware Requirements for Standalone View Composer," on page 14.

## Hardware Requirements for Standalone View Composer

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

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

**Table 3-4.** View Composer Hardware Requirements

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

---

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

---

## Database Requirements for View Composer

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

If a database server already exists for vCenter Server, View Composer can use that existing database server if it is a version listed in [Table 3-5](#). For example, View Composer can use the Microsoft SQL Server 2005 or 2008 Express instance provided with vCenter Server. If a database server does not already exist, you must install one.

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

---

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

---

[Table 3-5](#) 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 3-5.** Supported Database Servers for View Composer

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

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

## Upgrade Requirements for View Composer

The View Composer upgrade process has specific requirements and limitations.

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

### Security-Related Requirements

- View Composer requires an SSL certificate that is signed by a CA (certificate authority). If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate after you install View Composer, you must import the new certificate and run the `SviConfig ReplaceCertificate` utility to bind your new certificate to the port used by View Composer.

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

For complete information about security certificate requirements, see "Configuring SSL Certificates for View Servers" in the *VMware View Installation* guide.

- Certificates for vCenter Server, View Composer, and View servers must include certificate revocation lists (CRLs). For more information, see "Configuring Certificate Revocation Checking on Server Certificates" in the *VMware View Installation* guide.
- Verify that no applications that run on the View Composer computer use Windows SSL libraries that require SSL version 2 (SSLv2) provided through the Microsoft Secure Channel (Schannel) security package. The View Composer installer disables SSLv2 on the Microsoft Schannel. Applications such as Tomcat, which uses Java SSL, or Apache, which uses OpenSSL, are not affected by this constraint.
- To enhance the security of View Composer, disable the weak cryptographic cipher suites on the Windows Server computer on which the View Composer service is installed. See "Disable Weak Cryptographic Cipher Suites on the View Composer Server" in the *VMware View Installation* guide.

## View Transfer Server Requirements

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

### Installation and Upgrade Requirements for View Transfer Server

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

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

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

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

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

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

For information about storage requirements, see the *VMware View Installation* document.

### Supported Operating Systems for View Transfer Server

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

**Table 3-6.** Operating System Support for View Transfer Server

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

---

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

---

## View Administrator Requirements

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

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

- Internet Explorer 8
- Internet Explorer 9
- Firefox 6



- Firefox 7

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

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

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

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

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

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

Table 3-7 lists the Microsoft Windows operating systems supported for View Client. For information about operating systems supported by other View Clients, such as View Client for the Mac and View Client for iPad, see the documents that pertain to the specific client. Go to [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html).

**Table 3-7.** View Client Operating System Support for Windows-Based Clients

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

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

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

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

## Hardware Requirements for Local Mode Desktops

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

### PC Hardware

Table 3-8 describes the hardware requirements for various View desktop operating systems.

**Table 3-8.** Processor Requirements

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

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

## Disk Space

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

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

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

IDE and SCSI hard drives are supported.

## Memory

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

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

## Display

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

View Client with Local Mode supports DirectX9c, which becomes enabled automatically on client systems with capable GPUs. DirectX9c includes 3D capabilities such as Google Earth with 3D building turned on, Windows 7 Aero effects, and some 3D games.

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

For CPU and GPU requirements to support Windows 7 Aero, see [Table 3-8](#).

## Client Browser Requirements for View Portal

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

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

- Internet Explorer 8
- Internet Explorer 9
- Firefox 6
- Firefox 7
- Safari 5 (on a Mac)

## 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 3-9.** View Agent Operating System Support

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

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



# Preparing for a VMware View Upgrade

---

Before you start the upgrade process, you must review system requirements for the new version, back up databases, take snapshots of virtual machines that host server components, and document configuration settings.

This chapter includes the following topics:

- [“Preparing View Connection Server for an Upgrade,”](#) on page 21
- [“Prepare to Upgrade or Reinstall a Security Server,”](#) on page 22
- [“Preparing vCenter Server and View Composer for an Upgrade,”](#) on page 23

## Preparing View Connection Server for an Upgrade

Before you upgrade View Connection Server or before you upgrade any of the vSphere components that View Connection Server relies on, you must perform several tasks to ensure that these upgrades are successful.

- Verify that the virtual or physical machine on which the current View Connection Server instance is installed meets the system requirements for View 5.1.

See [“View Connection Server Requirements,”](#) on page 11.

- If View Connection Server is installed in a virtual machine, take a snapshot of the virtual machine. If you have a replicated group of View Connection Server instances, take a snapshot of only one View Connection Server instance.

For instructions on taking snapshots, see the vSphere Client online help. If you ever need to revert to this snapshot and if you have other View Connection Server instances in a replicated group, you must uninstall those instances before you revert the master to the snapshot. After you revert, you can reinstall the replicated instances and point to the instance you reverted.

You can label the snapshot Upgrade Preparation Phase.

- Open View Administrator and document all the global settings and settings for desktops and pools: Pools section and Desktops section in the Inventory tree, and the Global Settings section in the View Configuration tree.

For example, take a screen shot of the applicable settings. If you have multiple instances of View Connection Server in a replicated group, you need only document the settings for one instance.

- Use the `vdmexport.exe` utility to back up the LDAP database.

For instructions, see the administration guide for your current version of the *VMware View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need only export the data from one instance.

- Document the IP address and system name of the machine on which View Connection Server is installed.

- Determine if your company has written any batch files or scripts that run against the View database on the View Connection Server instance, and if so, document their names and locations.
- If you use load balancers for View Connection Server, document the configuration settings for the load balancers.

## Prepare to Upgrade or Reinstall a Security Server

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

---

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

---

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

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

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

---

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

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

---



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

---

### Procedure

- 1 In View Administrator, click **View Configuration > Servers**.
- 2 In the Security Servers tab, click **More Commands > Prepare for Upgrade or Reinstallation**.  
If you disabled IPsec rules before you installed the security server, this setting is inactive. In this case, you do not have to remove IPsec rules before you reinstall or upgrade.
- 3 Click **OK**.

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

## Preparing vCenter Server and View Composer for an Upgrade

Because vCenter Server and View Composer are often installed on the same virtual or physical machine, some preparation tasks apply to both.

### Preparing for Upgrades That Include vSphere

If you are upgrading vCenter Server in addition to upgrading to VMware View 5.1 with View Composer 3.0, you must consult the *vSphere Upgrade Guide* and perform the following tasks in the following order:

- 1 Verify that the virtual or physical machine meets the system requirements for the version of vCenter Server that you want to upgrade to.  
  
For example, vCenter Server 5.0 and later versions require two CPUs and must run on a 64-bit operating system. Because View Composer 2.6 was supported on 32-bit operating systems, upgrading might mean that you must upgrade vCenter Server and View Composer to a different machine.
- 2 Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that vCenter Server is unavailable. For information about replacing the default certificate for vCenter Server, see the *vSphere Examples and Scenarios* document.
- 3 If vCenter Server is installed in a virtual machine, take a snapshot of the virtual machine.  
  
For instructions on taking snapshots, see the vSphere Client online help.
- 4 If the computer name is longer than 15 characters, shorten the name to 15 or fewer characters.
- 5 Back up the vCenter Server database and the View Composer database.  
  
For instructions on performing a database backup, see the documentation from your database vendor.
- 6 Verify that the database server is compatible with the version of vCenter Server you plan to use.  
  
For example, if the database server is Oracle 9i, you must upgrade.
- 7 Verify that the database is compatible with View Composer 3.0.  
  
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.
- 8 Make a copy of the folder that contains SSL certificates.  
  
This folder is located at %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.
- 9 Document the IP address and system name of the machine on which vCenter Server is installed.
- 10 For all linked-clone desktop pools, disable provisioning of new virtual machines.  
  
Because View Composer might be upgraded during a different maintenance window than its desktop pools, provisioning must be postponed until both components are upgraded.
- 11 If any desktop pools are set to refresh the OS disk on logoff, edit the **Desktop/Pools** settings for that pool and set **Refresh OS disk on logoff** to **Never**.  
  
This setting prevents an error from occurring when the newly upgraded View Composer attempts to refresh a desktop that has not yet been upgraded to View Agent 5.1.
- 12 If any desktop pools are scheduled to do a refresh or recompose operation, cancel these tasks.

## Preparing for Upgrades of View Composer Only

If you are upgrading only View Composer and are not upgrading VirtualCenter Server, you must perform the following tasks:

- 1 Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that vCenter Server is unavailable. For information about replacing the default certificate for vCenter Server, see the *vSphere Examples and Scenarios* document.
- 2 If View Composer is installed in a virtual machine, take a snapshot of the virtual machine.  
For instructions on taking snapshots, see the vSphere Client online help.
- 3 Back up the vCenter Server database and the View Composer database.  
For instructions on performing a database backup, see the documentation from your database vendor.
- 4 Verify that the database is compatible with View Composer 3.0.  
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.
- 5 Make a copy of the folder that contains SSL certificates.  
This folder is located at %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.
- 6 Document the IP address and system name of the machine on which vCenter Server is installed.
- 7 For all linked-clone desktop pools, disable provisioning of new virtual machines.  
Because View Composer might be upgraded during a different maintenance window than its desktop pools, provisioning must be postponed until both components are upgraded.
- 8 If any desktop pools are set to refresh the OS disk on logoff, edit the **Desktop/Pools** settings for that pool and set **Refresh OS disk on logoff** to **Never**.  
This setting prevents an error from occurring when the newly upgraded View Composer attempts to refresh a desktop that has not yet been upgraded to View Agent 5.1.
- 9 If any desktop pools are scheduled to do a refresh or recompose operation, cancel these tasks.



# Upgrading VMware View Server Components

---

# 5

The server components that you must upgrade include View Connection Server, replicated servers, and security servers. Depending on the optional components you use, you might also need to upgrade View Composer. If you plan to use View Client with Local Mode, you must also install or upgrade a View Transfer Server instance.

During an upgrade to View 5.1, View does not support View Composer provisioning and maintenance operations, local mode operations, or View Transfer Server publish operations. Operations such as provisioning and recomposing linked-clone desktops, checking out or checking in desktops, and publishing View Composer base images are not supported during the transitional period when any View servers are still running the earlier version. You can successfully perform these operations only when all instances of View Connection Server, View Composer, and View Transfer Server have been upgraded to View 5.1.

For VMware View 5.1 patch releases, see [Chapter 8, “Applying VMware View Patches,”](#) on page 53.

This chapter includes the following topics:

- [“Upgrade View Connection Servers in a Replicated Group,”](#) on page 25
- [“Upgrade View Security Server,”](#) on page 30
- [“Upgrade View Composer,”](#) on page 31
- [“Upgrade vCenter Server,”](#) on page 40
- [“Upgrade View Transfer Server,”](#) on page 41

## Upgrade View Connection Servers in a Replicated Group

If you spread the upgrade tasks across multiple maintenance windows, you can verify success or discover issues at each phase of the process. VMware recommends upgrading all server components during the first maintenance window, starting with View Connection Server instances.

To use the new features of VMware View 5.1, you must upgrade to VMware View 5.1. For a list of the new features included in View 5.1, see the release notes.

---

**NOTE** This procedure describes an in-place upgrade. To migrate to a different machine, see [“Upgrade to View Connection Server 5.1 on a Different Machine,”](#) on page 28.

---

### Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. The amount of time the upgrade takes depends on the number of View Connection Server instances in the group. Budget 15 minutes to half an hour for each instance.

- Familiarize yourself with the security-related requirements of VMware View 5.1, and verify that these requirements are met. See “[Upgrade Requirements for View Connection Server](#),” on page 12. You might need to obtain and install a CA-signed SSL server certificate that includes certificate revocation information, verify that Windows Firewall with Advanced Security is set to on, and configure any back-end firewalls to support IPsec.
- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that vCenter Server is unavailable.
- Complete the tasks listed in “[Preparing View Connection Server for an Upgrade](#),” on page 21.
- Verify that you have a VMware View license for the new version.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- If you are unfamiliar with the `vdmexport.exe` utility, print the instructions for using it from the *VMware View Administration* document for your current version of VMware View. You will use this utility to back up the View LDAP database as part of the upgrade procedure.
- If you use security servers, familiarize yourself with the instructions on running the installer to create a security server that uses the new security server pairing mechanism. See the *VMware View Installation* document for your current version of VMware View.
- If you do not remember the location of the GPO templates on View Connection Server, see the section about Group Policy Objects in the *VMware View Administration* document for your current version of VMware View. You must copy these templates as part of the upgrade procedure.

You do not need to make any changes to the configuration of existing load balancers.

### Procedure

- 1 Stop the service called VMware View Connection Server service on all View Connection Server instances in the group.  
  
Do not stop the VMwareVDMDS service. The VMwareVDMDS service must be running so that the View LDAP database can be upgraded.
- 2 On the host of one of the View Connection Server instances in the group, run the installer for the VMware View 5.1 Connection Server.  
  
The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.  
  
The View LDAP is also upgraded.
- 3 Verify that the VMware View Connection Server service restarts after the installer wizard closes.
- 4 Verify that you can log in to View Connection Server, and click **About** in View Administrator to verify that the new version is being used.
- 5 Go to **View Configuration > Product Licensing and Usage**, click **Edit License**, enter the View Manager license key, and click **OK**.
- 6 Verify that you can log in to a View desktop.
- 7 Stop the View Connection Server service again.

- 8 Repeat [Step 1](#) through [Step 7](#) to upgrade each View Connection Server instance in the group.

---

**IMPORTANT** If you do not upgrade all View Connection Server instances in a replicated group, the health indicators in the View Administrator dashboard might show that one or more instances are in an error state. This situation arises because different versions supply different kinds of data. The solution is to upgrade all instances in the replicated group.

---

- 9 After all servers in the group are upgraded, start the View Connection Server service on all of them.

- 10 Use the `vdmexport.exe` utility to back up the newly upgraded View LDAP database.

If you have multiple instances of View Connection Server in a replicated group, you need only export the data from one instance.

- 11 On one of the upgraded View Connection Server instances, copy the GPO templates and load them into Active Directory.

- 12 Log in to View Administrator and examine the dashboard to verify that the vCenter Server icon is green.

If the vCenter Server icon is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

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

---

**IMPORTANT** After you upgrade View Connection Server, the View Composer icon will be red. After you upgrade to View Composer 3.0, you will be able to add View Composer using View Administrator 5.1. The View Composer icon will then appear green again.

---

### What to do next

To use a default or self-signed certificate from vCenter Server or View Composer, see "[Accept the Thumbprint of a Default SSL Certificate](#)," on page 27.

If the upgrade fails on one or more of the View Connection Server instances, see "[Create a Replicated Group After Reverting View Connection Server to a Snapshot](#)," on page 29.

If the upgrade is successful, upgrade the other View server components. If you use security servers, see "[Upgrade View Security Server](#)," on page 30.

If you ever reinstall 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.

## Accept the Thumbprint of a Default SSL Certificate

When you add vCenter Server and View Composer instances to View, you must ensure that the SSL certificates that are used for the vCenter Server and View Composer instances are valid and trusted by View Connection Server. If the default certificates that are installed with vCenter Server and View Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or View Composer instance is configured with a certificate that is signed by a CA, and the root certificate is trusted by View Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but View Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

---

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

---

For details about configuring SSL certificates, see "Configuring SSL Certificates for View Servers" in the *VMware View Installation* document.

You first add vCenter Server and View Composer to View in the Add vCenter Server wizard in View Administrator. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server and View Composer to View.

After these servers are added to View, you can reconfigure them in the Edit vCenter Server dialog.

---

**NOTE** You also must accept a certificate thumbprint when you upgrade from an earlier View release to View 5.1 or later, and a vCenter Server or View Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

On the View Administrator dashboard, the vCenter Server or View Composer icon turns red and an Invalid Certificate Detected dialog box appears. You must click **Verify** and follow the procedure shown here.

---

### Procedure

- 1 When View Administrator displays an Invalid Certificate Detected dialog box, click **View Certificate**.
- 2 Examine the certificate thumbprint in the Certificate Information window.
- 3 Examine the certificate thumbprint that was configured for the vCenter Server or View Composer instance.
  - a On the vCenter Server or View Composer host, start the MMC snap-in and open the Windows Certificate Store.
  - b Navigate to the vCenter Server or View Composer certificate.
  - c Click the Certificate Details tab to display the certificate thumbprint.
- 4 Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server or View Composer instance.
- 5 Determine whether to accept the certificate thumbprint.

Option	Description
<b>The thumbprints match.</b>	Click <b>Accept</b> to use the default certificate.
<b>The thumbprints do not match.</b>	Click <b>Reject</b> . Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server or View Composer.

## Upgrade to View Connection Server 5.1 on a Different Machine

As part of your upgrade, you can migrate View Connection Server to a new machine. For example, if you have View 4.6.x Connection Server on a 32-bit Windows 2003 Server machine, you can migrate to a 64-bit Windows 2008 Server machine.

### Prerequisites

- Upgrade at least one existing View Connection Server instance to View 5.1. See "[Upgrade View Connection Servers in a Replicated Group](#)," on page 25. During this upgrade, your existing View LDAP will be upgraded.

- Verify that the new physical or virtual machine meets the system requirements for installing View Connection Server. See [“Supported Operating Systems for View Connection Server,”](#) on page 12 and [“Hardware Requirements for View Connection Server,”](#) on page 11.
- Familiarize yourself with the security-related requirements of VMware View 5.1, and verify that these requirements are met. See [“Upgrade Requirements for View Connection Server,”](#) on page 12.
- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Verify that you have a domain user account with administrative privileges on the host you will use to run the installer.
- Familiarize yourself with the procedure for installing a replicated instance. See the *VMware View Installation* document. You install a replicated instance as part of this procedure.

You do not need to make any changes to the configuration of existing load balancers.

### Procedure

- 1 Verify that an upgraded instance of View Connection Server is running and is accessible to the new machine where you plan to install View Connection Server.

When you install View Connection Server on the new host, you will point to this existing instance.

- 2 On the new machine, install a replicated instance of View Connection Server.

The View LDAP on the new instance will replicate that of the upgraded source instance.

- 3 If applicable, uninstall View Connection Server from the old host by using the Windows **Add/Remove Programs** utility.
- 4 In View Administrator, go to **View Configuration > Servers > Connection Servers** tab and determine whether the View Connection Server instance that was uninstalled still appears in the list.
- 5 If the uninstalled View Connection Server instance still appears in the list, use a `vdadmin` command to remove it.

```
vdadmin.exe -S -s server_name -r
```

In this example, `server_name` is the host name or IP address of the View Connection Server host. For more information about the `vdadmin` command-line tool, see the *VMware View Administration* document.

A new instance of View Connection Server is added to a group and an old instance is removed.

### What to do next

Upgrade the other View server components. If you use View Composer, see [“Upgrade View Composer,”](#) on page 31. If you use VMware View with Local Mode, see [“Upgrade View Transfer Server,”](#) on page 41.

If you ever reinstall 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.

## Create a Replicated Group After Reverting View Connection Server to a Snapshot

If an upgrade fails, or if for some other reason, you must revert a virtual machine that hosts View Connection Server to a snapshot, you must uninstall the other View Connection Server instances in the group and recreate the replicated group.

If you revert one View Connection Server virtual machine to a snapshot, the View LDAP objects in the database of that virtual machine are no longer consistent with the View LDAP objects in the databases of the other replicated instances. After you revert to a snapshot, the following event is logged in the Windows Event log, in the VMwareVDMDS Event log (Event ID 2103): The Active Directory Lightweight Directory Services database has been restored using an unsupported restoration procedure. The reverted virtual machine stops replicating its View LDAP.

If you find it necessary to revert to a snapshot, you must uninstall other View Connection Server instances and uninstall the View LDAP on those virtual machines and then reinstall replica instances.

### Prerequisites

Determine which View Connection Server instance is to be the new standard, or master, View Connection Server. This Connection Server has the desired View configuration data.

### Procedure

- 1 On all View Connection Server instances except the one chosen to be the new standard View Connection Server instance, uninstall View Connection Server and the View LDAP instance.  
The View LDAP instance is called AD LDS Instance VMwareVDMDS.
- 2 On the virtual machine that hosts the standard, or master, View Connection Server instance, open a command prompt and enter the following command to ensure that replication is not disabled.  

```
repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL -DISABLE_INBOUND_REPL
```
- 3 On the virtual machines that are to host the replica View Connection Server instances, run the View Connection Server installer, select the **View Replica Server** installation option, and specify the host name or IP address of the standard View Connection Server instance.

The replicated group of View Connection Server instances is recreated and their View LDAP objects are consistent.

## Upgrade View Security Server

After you upgrade View Connection Server, you can upgrade the security servers that are paired with it.

### Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Verify that you have upgraded View Connection Server. For instructions, see [“Upgrade View Connection Servers in a Replicated Group,”](#) on page 25.
- Verify that the virtual or physical machine on which the current View Connection Server instance is installed meets the system requirements for View 5.1.  
See [“View Connection Server Requirements,”](#) on page 11.
- Familiarize yourself with the security-related requirements of VMware View 5.1, and verify that these requirements are met. See [“Upgrade Requirements for View Connection Server,”](#) on page 12. You might need to obtain and install a CA-signed SSL server certificate that includes certificate revocation information, verify that Windows Firewall with Advanced Security is set to on, and configure any back-end firewalls to support IPsec.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- If you have not configured a security server pairing password, use View Administrator 5.1 to do so. The installation program might prompt you for this password during installation. See the topic called [“Configure a Security Server Pairing Password”](#) in the *VMware View 5.1 Installation* document.
- If you are upgrading a View 5.1 security server, such as for a maintenance release, remove existing IPsec rules for the security server. See [“Prepare to Upgrade or Reinstall a Security Server,”](#) on page 22.

You do not need to make any changes to the configuration of existing load balancers.

## Procedure

- 1 Stop the service called VMware View Connection Server service.
- 2 Run the installer for the VMware View 5.1 Connection Server.  
The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.
- 3 Verify that the VMware View Connection Server service restarts after the installer wizard closes.
- 4 Log in to View Administrator, select the security server in the Dashboard, and verify that the security server is now at version 5.1.
- 5 Verify that you can log in to a View desktop.
- 6 In View Administrator, go to **View Configuration > Servers > Security Servers** tab and remove any duplicate security servers from the list.

The new automated security server pairing mechanism can produce duplicate entries in the **Security Servers** list if the full system name does not match the name that was assigned when the security server was originally created.

## What to do next

Upgrade the other View server components, such as View Composer, vCenter Server, and View Transfer Server, if you use any of these components. See [Chapter 5, “Upgrading VMware View Server Components,”](#) on page 25.

If you have finished upgrading View server components, at your next maintenance window, continue with the VMware View upgrade.

- If you are also upgrading vSphere components, see [Chapter 6, “Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines,”](#) on page 45.
- If you upgrading only View components, see [“Upgrade View Agent,”](#) on page 47.

## Upgrade View Composer

For View 5.1, during the first maintenance window, upgrade View Composer. Operations such as provisioning and recomposing linked-clone desktops and publishing View Composer base images are not supported until all View servers are upgraded to View 5.1.

---

**IMPORTANT** If your current version of View Composer is installed on a computer with a Windows Server 2003 operating system, see the procedure called "Manually Migrate View Composer to the New Machine" in the *VMware View 4.6 Upgrades* document. After you migrate View Composer 2.6 to a system with a Windows Server 2008 R2 operating system, you can perform an in-place upgrade to View Composer 3.0.

To migrate View Composer 3.0 to a different physical or virtual machine, see [“Migrate View Composer to Another Computer,”](#) on page 35.

---

## Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Complete the tasks listed in [“Preparing for Upgrades of View Composer Only,”](#) on page 24.
- Verify that the server on which View Composer is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if View Composer does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator.

- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- Determine whether to let the installer wizard upgrade the View Composer database. You can choose to run the SviConfig command-line utility after the wizard finishes to upgrade the database manually and to create a log of the upgrade.

### Procedure

- 1 On the virtual or physical machines where View Composer is installed, download and run the installer for View Composer 3.0, which is the version included with VMware View 5.1.

You can download the installer from the VMware Web site.

Step-by-step instructions for running the installer appear in the *VMware View Installation* document.

- 2 Specify whether you do want the wizard to upgrade the database.

If a dialog box appears with the message "Database upgrade completed with warnings" you can click **OK** and safely ignore the message.

- 3 When the wizard prompts you for the View Composer port number, verify that the port number is set to 18443.

You will use this port number when you use View Administrator to add View Composer. After you upgrade View Connection Server, the View Composer icon is red in the View Administrator Dashboard until you upgrade to View Composer 3.0 and configure View Composer settings.

### What to do next

Log in to View Administrator and add View Composer. See the procedure called "Configure View Composer Settings," in the *VMware View 5.1 Installation* document.

## Manually Upgrading the View Composer Database

Rather than letting the View Composer installer upgrade the database when a schema update is required, you can manually upgrade the database. You can use the SviConfig utility when you must observe the upgrade process more closely or when upgrade tasks must be distributed to IT administrators with different responsibilities.

When you upgrade View Composer to a version with an updated database schema, an installer prompt asks if you want the wizard to upgrade the database. If you choose not to use the installer wizard, you must use the SviConfig utility to upgrade the database and migrate the existing data.

Using the SviConfig command-line utility has the following advantages:

- This utility returns result codes and creates a log of the database upgrade to simplify troubleshooting if the upgrade fails.
- You can separate the upgrade tasks. A vSphere or View Manager administrator can run the View Composer installer to upgrade the software. A database administrator (DBA) can use SviConfig to upgrade the View Composer database.
- The software upgrade and the database upgrade can occur during different maintenance windows. For example, your site might run database-maintenance operations on weekends only, whereas software-maintenance tasks can occur during the week.



## Run SviConfig to Manually Upgrade the Database

With the SviConfig command-line utility, you can upgrade the View Composer database separately from the View Composer software. This utility also creates a log file to simplify troubleshooting if the upgrade fails.

---

**IMPORTANT** Only experienced View Composer administrators should use the SviConfig utility. This utility is intended to resolve issues relating to the View Composer service.

---

### Prerequisites

- Back up the View Composer database. For instructions, see the documentation for your database server.
- Verify that you know the database source name (DSN) for the View Composer database.
- Verify that you know the user name and password for the database administrator account for this database.

### Procedure

- 1 On the vCenter Server virtual or physical machine, open a Windows command prompt and navigate to the SviConfig executable file.

The file is located with the View Composer application. The default path is C:\Program Files (86)\VMware\VMware View Composer\sviconfig.exe.

- 2 Enter the command to stop the VMware View Composer service.

```
net stop svid
```

- 3 Run the SviConfig `databaseupgrade` command.

```
sviconfig -operation=databaseupgrade
          -DsnName=target_DSN
          -Username=database_administrator_username
```

For example:

```
sviconfig -operation=databaseupgrade -dsname=LinkedClone
          -username=Admin
```

- 4 When prompted, supply the password.

A successful operation displays output that shows the upgrade steps.

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

- 5 Enter the command to start the VMware View Composer service.

```
net start svid
```

A complete log of the upgrade process is created and placed in C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log.

## What to do next

If the database upgrade fails, see [“Troubleshooting a View Composer Database Upgrade Failure,”](#) on page 34.

If the result code is any number other than 0, which means success, see [“Result Codes for a Manual Database Schema Update,”](#) on page 34.

## Result Codes for a Manual Database Schema Update

When you manually upgrade the View Composer database, the `sviconfig databaseupgrade` command displays a result code.

[Table 5-1](#) shows the `sviconfig databaseupgrade` result codes.

**Table 5-1.** Result Codes for the `databaseupgrade` Command

Code	Description
0	The operation ended successfully.
1	The supplied DSN could not be found.
2	Invalid database administrator credentials were provided.
3	The driver for the database is not supported.
4	An unexpected problem arose and the command failed to complete.
14	Another application is using the View Composer service. Shut down the service before executing the command.
15	A problem arose during the restore process. Details are provided in the onscreen log output.
17	Unable to upgrade the database data.
18	Unable to connect to the database server.

## Troubleshooting a View Composer Database Upgrade Failure

When you upgrade the View Composer service with the View Composer installer or run the `SviConfig databaseupgrade` command, the operation might fail to upgrade the View Composer database.

### Problem

The `SviConfig databaseupgrade` operation displays error code 17, or the View Composer installer displays a warning message.

```
Database upgrade completed with warnings
```

### Cause

The database-upgrade software contacts vCenter Server to get additional data about desktops. The database upgrade might fail if the desktops are not available, the ESX host is not running, or vCenter Server is not available.

### Solution

- 1 See the View Composer `SviConfig` log file for more information.

The default location of this file is `C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log`. The upgrade script logs a message for each failure.

- 2 Examine the log records to identify the desktops that failed to upgrade.

Option	Action
<b>The desktop exists but is unavailable.</b>	Make the desktop available again. Depending on the cause of the failure, you might have to restart the ESX host or vCenter Server, or take another action.
<b>The desktop does not exist.</b>	Ignore the log message. <b>NOTE</b> A deleted desktop might appear to exist in View Manager if an administrator deletes the desktop virtual machine directly in vSphere.

- 3 Run the `SviConfig databaseupgrade` command again.

## Migrate View Composer to Another Computer

In some situations, you might need to migrate a View Composer service to a new Windows Server computer. For example, you might migrate View Composer and vCenter Server to a new ESXi host or cluster to expand your View deployment. In addition, View Composer and vCenter Server do not have to be installed on the same Windows Server computer.

You can migrate View Composer from the vCenter Server computer to a standalone computer or from a standalone computer to the vCenter Server computer.

---

**IMPORTANT** These topics pertain to migrating View Composer 3.0 to another computer. You must upgrade from View Composer 2.6 or 2.7 to View Composer 3.0 before you perform these tasks.

If your current version of View Composer is installed on a computer that does not meet the system requirements for View Composer 3.0, you cannot use these procedures. For example, if you have View Composer 2.6, which is included with View 4.6, installed on a Windows Server 2003 operating system, see the procedure called "Manually Migrate View Composer to the New Machine" in the *VMware View 4.6 Upgrades* document. After you migrate View Composer 2.6 to a system with a Windows Server 2008 R2 operating system, you can perform an in-place upgrade to View Composer 3.0.

---

- [Guidelines for Migrating View Composer](#) on page 36  
The steps you take to migrate the View Composer service depend on whether you intend to preserve existing linked-clone desktops.
- [Migrate View Composer with an Existing Database](#) on page 36  
When you migrate View Composer to another computer, if you intend to preserve your current linked-clone desktops, the new View Composer service must continue to use the existing View Composer database.
- [Migrate View Composer Without Linked-Clone Desktops](#) on page 38  
If the current View Composer service does not manage any linked-clone desktops, you can migrate View Composer to a new computer without migrating the RSA keys to the new computer. The migrated View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.
- [Prepare a Microsoft .NET Framework for Migrating RSA Keys](#) on page 39  
To use an existing View Composer database, you must migrate the RSA key container between computers. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.
- [Migrate the RSA Key Container to the New View Composer Service](#) on page 39  
To use an existing View Composer database, you must migrate the RSA key container from the source computer on which the existing View Composer service resides to the computer on which you want to install the new View Composer service.

## Guidelines for Migrating View Composer

The steps you take to migrate the View Composer service depend on whether you intend to preserve existing linked-clone desktops.

To preserve the linked-clone desktops in your deployment, the View Composer service that you install on the new computer must continue to use the existing View Composer database. The View Composer database contains data that is required to create, provision, maintain, and delete the linked clones.

When you migrate the View Composer service, you can also migrate the View Composer database to a new computer.

Whether or not you migrate the View Composer database, the database must be configured on an available computer in the same domain as the new computer on which you install the View Composer service, or on a trusted domain.

View Composer creates RSA key pairs to encrypt and decrypt authentication information stored in the View Composer database. To make this data source compatible with the new View Composer service, you must migrate the RSA key container that was created by the original View Composer service. You must import the RSA key container to the computer on which you install the new service.

If the current View Composer service does not manage any linked-clone desktops, you can migrate the service without using the existing View Composer database. You do not have to migrate the RSA keys, whether or not you use the existing database.

---

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

---

## Migrate View Composer with an Existing Database

When you migrate View Composer to another computer, if you intend to preserve your current linked-clone desktops, the new View Composer service must continue to use the existing View Composer database.

Follow the steps in this procedure when you migrate View Composer in any of the following directions:

- From a vCenter Server computer to a standalone computer
- From a standalone computer to a vCenter Server computer
- From a standalone computer to another standalone computer
- From a vCenter Server computer to another vCenter Server computer

When you migrate the View Composer service, you can also migrate the View Composer database to a new location. For example, you might need to migrate the View Composer database if the current database is located on a vCenter Server computer that you are migrating as well.

When you install the View Composer service on the new computer, you must configure the service to connect to the View Composer database.

### Prerequisites

- Familiarize yourself with the View Composer migration requirements. See [“Guidelines for Migrating View Composer,”](#) on page 36.
- Familiarize yourself with the steps for migrating the RSA key container to the new View Composer Service. See [“Prepare a Microsoft .NET Framework for Migrating RSA Keys,”](#) on page 39 and [“Migrate the RSA Key Container to the New View Composer Service,”](#) on page 39.
- Familiarize yourself with installing the View Composer service. See “Installing View Composer” in the *VMware View Installation* document.

- Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the *VMware View Installation* document.
- Familiarize yourself with configuring View Composer in View Administrator. See the topics about configuring View Composer settings and View Composer domains in the *VMware View Administration* document.

### Procedure

- 1 Disable virtual machine provisioning in the vCenter Server instance that is associated with the View Composer service.
  - a In View Administrator, click **View Configuration > Servers**.
  - b In the vCenter Server tab, select the vCenter Server instance and click **Disable provisioning**.

- 2 (Optional) Migrate the View Composer database to a new location.

If you need to take this step, consult your database administrator for migration instructions.

- 3 Uninstall the View Composer service from the current computer.
- 4 (Optional) Migrate the RSA key container to the new computer.
- 5 Install the View Composer service on the new computer.

During the installation, specify the DSN of the database that was used by the original View Composer service. Also specify the domain administrator user name and password that were provided for the ODBC data source for that database.

If you migrated the database, the DSN and data source information must point to the new location of the database. Whether or not you migrated the database, the new View Composer service must have access to the original database information about the linked clones.

- 6 Configure an SSL server certificate for View Composer on the new computer.

You can copy the certificate that was installed for View Composer on the original computer or install a new certificate.

- 7 In View Administrator, configure the new View Composer settings.

- a In View Administrator, click **View Configuration > Servers**, select the vCenter Server instance that is associated with this View Composer service, and click **Edit**.
- b In the View Composer tab, provide the new View Composer settings.

If you are installing View Composer with vCenter Server on the new computer, select **View Composer co-installed with the vCenter Server**.

If you are installing View Composer on a standalone computer, select **Standalone View Composer Server** and provide the FQDN of the View Composer computer and the user name and password of the View Composer user.

- c In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.
- d Click **OK**.

## Migrate View Composer Without Linked-Clone Desktops

If the current View Composer service does not manage any linked-clone desktops, you can migrate View Composer to a new computer without migrating the RSA keys to the new computer. The migrated View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

### Prerequisites

- Familiarize yourself with installing the View Composer service. See "Installing View Composer" in the *VMware View Installation* document.
- Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the *VMware View Installation* document.
- Familiarize yourself with the steps for removing View Composer from View Manager. See topic about removing View Composer from View Manager in the *VMware View Administration* document.

Before you can remove View Composer, verify that it no longer manages any linked-clone desktops. If any linked clones remain, you must delete them.

- Familiarize yourself with configuring View Composer in View Administrator. See the topics about configuring View Composer settings and View Composer domains in the *VMware View Administration* document.

### Procedure

- 1 In View Administrator, remove View Composer from View Manager.
  - a In the Edit vCenter Server dialog, make sure that **Do not use View Composer** is selected.
  - b In the Edit vCenter Server dialog, click **OK**.
- 2 Uninstall the View Composer service from the current computer.
- 3 Install the View Composer service on the new computer.
 

During the installation, configure View Composer to connect to the DSN of the original or new View Composer database.
- 4 Configure an SSL server certificate for View Composer on the new computer.
 

You can copy the certificate that was installed for View Composer on the original computer or install a new certificate.
- 5 In View Administrator, configure the new View Composer settings.
  - a In View Administrator, click **View Configuration > Servers**, select the vCenter Server instance that is associated with this View Composer service, and click **Edit**.
  - b In the View Composer Server Settings pane, click **Edit**.
  - c Provide the new View Composer settings.
 

If you are installing View Composer with vCenter Server on the new computer, select **View Composer co-installed with the vCenter Server**.

If you are installing View Composer on a standalone computer, select **Standalone View Composer Server** and provide the FQDN of the View Composer computer and the user name and password of the View Composer user.
  - d In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.
  - e Click **OK**.

## Prepare a Microsoft .NET Framework for Migrating RSA Keys

To use an existing View Composer database, you must migrate the RSA key container between computers. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

### Prerequisites

Download the .NET Framework and read about the ASP.NET IIS registration tool from the following locations:

- <http://www.microsoft.com/net>
- [http://msdn.microsoft.com/library/k6h9cz8h\(VS.80\).aspx](http://msdn.microsoft.com/library/k6h9cz8h(VS.80).aspx)

### Procedure

- 1 Install the .NET Framework on the computer on which the View Composer service associated with the existing database is installed.
- 2 Install the .NET Framework on the destination computer on which you want to install the new View Composer service.

### What to do next

Migrate the RSA key container to the destination computer. See “[Migrate the RSA Key Container to the New View Composer Service](#),” on page 39.

## Migrate the RSA Key Container to the New View Composer Service

To use an existing View Composer database, you must migrate the RSA key container from the source computer on which the existing View Composer service resides to the computer on which you want to install the new View Composer service.

You must perform this procedure before you install the new View Composer service.

### Prerequisites

Verify that the Microsoft .NET Framework and the ASP.NET IIS registration tool are installed on the source and destination computers. See “[Prepare a Microsoft .NET Framework for Migrating RSA Keys](#),” on page 39.

### Procedure

- 1 On the source computer on which the existing View Composer service resides, open a command prompt and navigate to the %windir%\Microsoft.NET\Framework\v2.0.xxxx directory.
- 2 Type the `aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri`

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

The ASP.NET IIS registration tool exports the RSA public-private key pair from the SviKeyContainer container to the keys.xml file and saves the file locally.

- 3 Copy the keys.xml file to the destination computer on which you want to install the new View Composer service.
- 4 On the destination computer, open a command prompt and navigate to the %windir%\Microsoft.NET\Framework\v2.0.xxxx directory.
- 5 Type the `aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp`

```
aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp
```

where *path* is the path to the exported file.

The `-exp` option creates an exportable key pair. If a future migration is required, the keys can be exported from this computer and imported to another computer. If you previously migrated the keys to this computer without using the `-exp` option, you can import the keys again using the `-exp` option so that you can export the keys in the future.

The registration tool imports the key pair data into the local key container.

### What to do next

Install the new View Composer service on the destination computer. Provide the DSN and ODBC data source information that allows View Composer to connect to the same database information that was used by the original View Composer service. For installation instructions, see "Installing View Composer" in the *VMware View Installation* document.

Complete the steps to migrate View Composer to a new computer and use the same database. See "[Migrate View Composer with an Existing Database](#)," on page 36.

## Upgrade vCenter Server

Perform a vCenter Server upgrade as part of the same maintenance window during which you upgrade other View server components. Before you upgrade vCenter Server, you must back up some View data. After the upgrade, if View Composer is running on the same server, you must restart the View Composer service.

### Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. For information about how much time is required, see the *vSphere Upgrade Guide*.
- Back up the vCenter Server database and the View Composer database.
- Back up the View LDAP database from a View Connection Server instance by using the `vdlexport.exe` utility.

For instructions, see the *VMware View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need to export the data from only one instance.

- Perform the tasks listed in "[Preparing for Upgrades That Include vSphere](#)," on page 23.
- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that vCenter Server is unavailable.
- Complete the prerequisites listed in the *vSphere Upgrade Guide*, using the version of the guide that corresponds to the version of vSphere that you plan to upgrade to.

### Procedure

- 1 Upgrade vCenter Server as described in the *vSphere Upgrade Guide*.
- 2 If View Composer is installed on the same host, restart the View Composer service.
- 3 Log in to View Administrator and examine the dashboard to verify that the vCenter Server and View Composer icons are green.

If either of these icons is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

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



### What to do next

To use a default or self-signed certificate from vCenter Server or View Composer, see [“Accept the Thumbprint of a Default SSL Certificate,”](#) on page 27.

If you use VMware View with Local Mode, see [“Upgrade View Transfer Server,”](#) on page 41.

If you have finished upgrading View server components, at your next maintenance window, continue with the VMware View upgrade.

- If you are also upgrading vSphere components, see [Chapter 6, “Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines,”](#) on page 45.
- If you are upgrading only View components, see [“Upgrade View Agent,”](#) on page 47.

## Upgrade View Transfer Server

The View Transfer Server component was added in View 4.5. View Transfer Server is an optional View Manager component that supports check in, check out, and replication of desktops that run in local mode.

After you upgrade all replicated View Connection Server instances to version 5.1, you can upgrade View Transfer Server. View Connection Server 5.1 is not compatible with earlier versions of View Transfer Server, and View Transfer Server 5.1 is not compatible with earlier versions of View Connection Server. If an earlier version of View Connection Server tried to send a publish request to a View 5.1 Transfer Server, the publish operation would fail. Similarly, if a View 5.1 Connection Server sent a publish request to an earlier version of View Transfer Server, the publish operation would fail.

---

**NOTE** This procedure describes an in-place upgrade. To migrate to a different machine, see [“Upgrade to View Transfer Server 5.1 on a Different Machine,”](#) on page 42.

---

### Prerequisites

- Verify that View Connection Server has been upgraded to version 5.1 and View Composer has been upgraded to version 3.0. See [Chapter 5, “Upgrading VMware View Server Components,”](#) on page 25. If only one of these components is upgraded to version 5.1, end users will not be able to check out View desktops if the desktops are based on linked clones.
- Verify that you have local administrator privileges on the Windows Server that you will use to run the installer and perform the upgrade.
- Verify that the virtual machine on which the current View Transfer Server instance is installed meets the system requirements for View 5.1.

See [“Supported Operating Systems for View Transfer Server,”](#) on page 16.

- If the View Transfer Server instance uses a local file system for its Transfer Server Repository, back up the Transfer Server Repository directory.
- If you are using an SSL server certificate that is signed by a certificate authority (CA), and you want to continue using the certificate after the upgrade, back up the certificate. The certificate is located in the following directory: `install_directory\VMware\VMware View\Server\httpd\conf`.

---

**IMPORTANT** With View 5.1 and later versions, having a CA-signed server certificate for View Transfer Server is not necessary. Instead you can use the default self-signed certificate that gets installed during the upgrade. Security enhancements have been made so that using a CA-signed certificate does not offer significantly more security than using the default self-signed certificate.

---

## Procedure

- 1 Put the View Transfer Server into maintenance mode.
  - a In View Administrator, go to **View Configuration > Servers > Transfer Servers** tab, select the View Transfer Server, and click **Enter Maintenance Mode**.
  - b Wait until the status changes to Maintenance.
 

The status remains in Maintenance Pending until all active transfers are complete.
- 2 On the virtual machine that hosts the View Transfer Server instance, run the installer for the VMware View 5.1 Transfer Server.
 

The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.
- 3 Verify that the VMware View Transfer Server service restarts after the installer wizard closes.
- 4 In View Administrator, go to **View Configuration > Servers > Transfer Servers** tab, select the View Transfer Server, and click **Exit Maintenance Mode**.

## What to do next

If you are using an SSL server certificate that is signed by a certificate authority (CA) and you want to continue to use that certificate on the upgraded version of View Transfer Server, you must configure the signed certificate for the new View Transfer Server version. See the section called "Configuring Certificate Authentication for View Transfer Server" in the previous version, version 5.0, of the *VMware View Installation* document. Note that with View 5.1 and later versions, having a CA-signed server certificate for View Transfer Server is not necessary and so the procedure is not included in the 5.1 version of the document.

If you have finished upgrading View server components, at your next maintenance window, continue with the VMware View upgrade.

- If you are also upgrading vSphere components, see [Chapter 6, "Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines,"](#) on page 45.
- If you upgrading only View components, see ["Upgrade View Agent,"](#) on page 47.

## Upgrade to View Transfer Server 5.1 on a Different Machine

As part of your upgrade, you can migrate View Transfer Server to a new machine. For example, you might want to move View Transfer Server from a 32-bit Windows 2003 Server machine to a 64-bit Windows 2008 Server machine.

### Prerequisites

- Verify that the new virtual machine meets the system requirements for installing View Transfer Server. See ["View Transfer Server Requirements,"](#) on page 16.
- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Verify that you have local administrator privileges on the Windows Server that you will use to run the installer.
- If the original View Transfer Server instance used a network share for its Transfer Server Repository, document the path to the directory on the network share.

In View Administrator, go to **View Configuration > Servers > Transfer Servers** tab.

- Familiarize yourself with the procedure for installing and configuring View Transfer Server. See the *VMware View Installation* document.

- If the original View Transfer Server instance used a local file system for its Transfer Server Repository, familiarize yourself with the instructions for migrating the Transfer Server Repository to a new location. See the *VMware View Administration* document.

### Procedure

- 1 On the new virtual machine, install View Transfer Server.
- 2 In View Administrator, add the new View Transfer Server instance.  
Go to **View Configuration > Servers > Transfer Servers** tab.
- 3 If you have a Transfer Server Repository located on a network share, verify that this new View Transfer Server can access the Transfer Server Repository on the network share.
- 4 If you have a Transfer Server Repository located on the local file system of the original View Transfer Server, migrate the repository to a new location.
- 5 In View Administrator, remove the original View Transfer Server instance.
- 6 If applicable, uninstall View Transfer Server from the old host by using the Windows **Add/Remove Programs** utility.

### What to do next

If you have finished upgrading View server components, at your next maintenance window, continue with the VMware View upgrade.

- If you are also upgrading vSphere components, see [Chapter 6, “Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines,”](#) on page 45.
- If you are upgrading only View components, see [“Upgrade View Agent,”](#) on page 47.



# Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines

---

# 6

Upgrading ESX/ESXi hosts and virtual machines is the most time-consuming aspect of this middle phase of a VMware View upgrade.

This procedure provides an overview of the tasks you must perform during the second and subsequent maintenance windows. To complete some of these tasks, you might need step-by-step instructions found in the *vSphere Upgrade Guide* and the *VMware View Administrator's Guide*.

## Prerequisites

- Complete the procedure described in [“Upgrade View Connection Servers in a Replicated Group,”](#) on page 25.
- Perform the ESX/ESXi upgrade preparation tasks listed in the *vSphere Upgrade Guide*.

## Procedure

- 1 Upgrade ESX/ESXi hosts, cluster by cluster.

For instructions, see the *vSphere Upgrade Guide*. If you have many clusters, this step could take several maintenance windows to complete. Upgrading ESX/ESXi hosts might include the following tasks:

- a Use VMotion to move the virtual machines off of the ESX/ESXi host.
- b Put the host into maintenance mode.
- c Perform the upgrade.
- d Use VMotion to move the virtual machines back onto the host.
- e Perform post-upgrade tasks for ESXi hosts.

Every host must be a member of a cluster, as mentioned in the prerequisites.

- 2 If an upgraded host does not reconnect itself to vCenter, use vSphere Client to reconnect the host to the vCenter Server.
- 3 If you use View Composer, after all ESX/ESXi hosts are upgraded, on the vCenter Server host, restart the View Composer service.

- 4 (Optional) Upgrade VMware Tools on all parent virtual machines, virtual machine templates, and virtual machines that host View server components such as View Connection Server instances.

- a Plan for down time, as described in the *vSphere Upgrade Guide*.
- b Update VMware Tools, and upgrade the virtual machine hardware for virtual machines that will be used as sources for View desktops.

To use the Windows 7 3D rendering feature, available with View 5.0 and later, you must upgrade the virtual machine hardware to version 8.

If you use vSphere Update Manager, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *vSphere Upgrade Guide*.

- 5 (Optional) If you use full-clone desktops, on each virtual machine, upgrade VMware Tools and the virtual hardware for virtual machines that will be used as sources for View desktops.

To use the Windows 7 3D rendering feature, available with View 5.0 and later, you must upgrade the virtual machine hardware to version 8.

If you use vSphere Update Manager, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *vSphere Upgrade Guide*.

#### **What to do next**

Upgrade View Agent. See [“Upgrade View Agent,”](#) on page 47.

# Upgrading VMware View Desktops and Clients

# 7

The View desktop and client components that you can upgrade include View Client for any of the supported desktop and mobile client platforms, thin clients provided by VMware partners, and the View Agent, which runs inside the operating systems of View desktops.

This chapter includes the following topics:

- [“Upgrade View Agent,”](#) on page 47
- [“Upgrade View Composer Desktop Pools,”](#) on page 49
- [“Upgrade View Clients,”](#) on page 50
- [“Upgrade View Local Mode Clients,”](#) on page 51

## Upgrade View Agent

The strategy for upgrading View Agent depends on the type of desktop source.

This procedure provides an overview of the tasks you must perform to upgrade from View Agent 4.6.x or 5.0.x to View Agent 5.1 in virtual machines used as desktop sources. To complete some of these tasks, you might need the step-by-step instructions found in the vSphere Client online help or in the *VMware View Administration* document, available by clicking the **Help** button in View Administrator.

---

**NOTE** If you are upgrading from View 4.0.x or 4.5.x, you must upgrade to View 5.0.x before upgrading to View 5.1. For instructions, see version 5.0 of the *VMware View Upgrades* document.

---

### Prerequisites

- Verify that at least one View Connection Server instance in the replicated group has been upgraded to View 5.1. View Connection Server must be upgraded to version 5.1 so that the secure JMS pairing mechanism can work with View Agent 5.1.
- For local mode desktops, verify that View Composer and View Transfer Server have been upgraded to version 5.1. See [Chapter 5, “Upgrading VMware View Server Components,”](#) on page 25. If only one of these components is upgraded to version 5.1, you will not be able to check out View desktops if the desktops are based on linked clones.
- If you are upgrading ESX/ESXi hosts and virtual machines, complete the procedure described in [Chapter 6, “Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines,”](#) on page 45.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.

## Procedure

- 1 If you use View Composer, upgrade the View Agent on a parent virtual machine and create a desktop pool for testing purposes.
  - a Download and run the View 5.1 View Agent installer on a parent virtual machine.  
You can download the installer from the VMware Web site.
  - b Create a small linked-clone desktop pool from this virtual machine.
  - c Test a virtual desktop from the desktop pool to verify that all the usage scenarios function properly.  
For example, create a desktop pool that contains one virtual desktop, and verify that you can use View Client to log in to that desktop.  
Step-by-step instructions for running the View Agent installer and creating desktop pools appear in the *VMware View Administration* document, available by clicking the **Help** button in View Administrator.
- 2 On the other parent virtual machines and virtual machine templates, download and run the installer for View Agent 5.1.  
Step-by-step instructions for running the View Agent installer and creating desktop pools appear in the *VMware View Administration* document, available by clicking the **Help** button in View Administrator.
- 3 If you use View Composer, take a snapshot of each upgraded parent virtual machine that you use to create linked-clone desktop pools.  
You use the new snapshot for recomposing all the virtual machines in the pool.  
For instructions on taking snapshots, see the vSphere Client online help.
- 4 If you use full-clone desktops or other virtual machines that you added as individual desktops or as part of a manual pool, upgrade View Agent by using whatever third-party tools you usually use for software upgrades.
- 5 For automated and manual Windows 7 pools that are not linked-clone pools, to use the Windows 7 3D rendering feature available with View 5.0 and later, edit the pool and power the virtual machine desktops off and on.
  - a Configure the following pool settings:
    - Set the pool to use the PCoIP display protocol.
    - Set **Allow users to choose protocol** to **No**.
    - Turn on the **Windows 7 3D Rendering** feature.
  - b Power off each virtual machine and power it on again.  
Restarting a virtual machine, rather than powering off and on, does not cause the setting to take effect.
- 6 If you use Windows Terminal Servers or physical or blade PCs as desktop sources, download and run the installer for View Agent 5.1 on these physical machines.  
You can download the installer from the VMware Web site.
- 7 Use a View Client that has not been upgraded to verify that you can log in to the upgraded View 5.1 desktop sources with your old View Client software.

## What to do next

If you use View Composer desktop pools, recompose or recreate the pools. See [“Upgrade View Composer Desktop Pools,”](#) on page 49.

Upgrade View Clients. See [“Upgrade View Clients,”](#) on page 50 and [“Upgrade View Local Mode Clients,”](#) on page 51.



## Upgrade View Composer Desktop Pools

Part of the final phase of a VMware View upgrade includes upgrading View Composer desktop pools.

Upgrading pools that were created with View Composer requires that you use a snapshot taken after upgrading View Agent on the parent virtual machine.

---

**NOTE** If you are also upgrading the virtual hardware version, such as upgrading to virtual hardware version 8 or later, included with vSphere 5 or later, the snapshot of the upgraded parent virtual machine is used to upgrade the virtual hardware version of the rest of the virtual machines in the linked-clone pool.

Upgrading in this way, from one virtual hardware version (or compatibility level) to a higher version, is supported. You cannot, however, recompose linked clones to a lower hardware version than their current version. For example, you cannot recompose hardware version 8 clones to a parent virtual machine that is hardware version 7.

---

### Prerequisites

- Complete the procedure described in [“Upgrade View Connection Servers in a Replicated Group,”](#) on page 25.
- Complete the procedure described in [“Upgrade View Composer,”](#) on page 31.
- If you are upgrading pools of desktops that will be checked out and run in local mode, complete the procedure described in [“Upgrade View Transfer Server,”](#) on page 41.
- If you are also upgrading ESX/ESXi hosts and virtual machines, complete the procedure described in [Chapter 6, “Upgrade ESX/ESXi 4.0.x, 4.1.x, or 5.0.x Hosts and Their Virtual Machines,”](#) on page 45.

To use the 3D rendering feature available with View 5.0 and later, you must upgrade the virtual hardware version to 8 or later in Windows 7 virtual machines.

- Complete the procedure described in [“Upgrade View Agent,”](#) on page 47 for upgrading the agent in the parent virtual machine.
- Plan maintenance windows carefully so that recreating and recomposing desktop pools will not overwhelm the storage array and ESX/ESXi hosts.

### Procedure

- 1 If you disabled provisioning of new virtual machines in preparation for the upgrade, enable provisioning again.
- 2 For pools composed of Windows 7 desktops, to use the Windows 7 3D rendering feature available with View 5.0 and later, edit the pool to configure the following settings:
  - Set the pool to use the PCoIP display protocol.
  - Set **Allow users to choose protocol** to **No**.
  - Turn on the **Windows 7 3D Rendering** feature.

This feature is available for Windows 7 desktops that use virtual hardware version 8 or later, available with vSphere 5 or later.

- 3 Use the snapshot you created after upgrading the parent virtual machine to recompose desktop pools.
- 4 If you changed the **Refresh OS disk on logoff** setting for a pool to **Never** in preparation for the upgrade, change the setting back to reflect the appropriate refresh policy.
- 5 If you canceled any refresh or recompose operations for any desktop pools, schedule the tasks again.

## What to do next

Upgrade View Clients. See “[Upgrade View Clients](#),” on page 50 and “[Upgrade View Local Mode Clients](#),” on page 51.

## Upgrade View Clients

The final phase of a VMware View upgrade includes upgrading View Clients and upgrading the firmware on thin client devices if you use them.

This procedure provides instructions for upgrading View clients that use remote desktops. If you are upgrading client systems that use View Client with Local Mode, see “[Upgrade View Local Mode Clients](#),” on page 51.

---

**IMPORTANT** Upgrading involves running the View Client 5.1 installer without first removing older versions of View Client. Upgrading is supported for View Client 4.6.x and 5.0.x. If your end users have older versions of View Client, instruct them to remove the View Client software before downloading and running the View Client 5.1 installer.

---

### Prerequisites

- Complete the procedures for upgrading the server components, which can include View Connection Server, View Transfer Server, and View Composer. See [Chapter 5, “Upgrading VMware View Server Components,”](#) on page 25.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- For Windows-based View Clients, verify that client systems have a supported operating system and, if you plan to use the PCoIP display protocol, verify that clients meet the additional hardware requirements. See “[Supported Operating Systems for Windows-Based View Client and View Client with Local Mode](#),” on page 17.

### Procedure

- 1 Have end users upgrade to the latest version of View Client.

Option	Action
<b>View Client</b>	Download and send the View Client installers to your end users or post them on a Web site and ask end users to download the installer and run it. You can download the installers from the VMware Web site at <a href="https://www.vmware.com/go/viewclients">https://www.vmware.com/go/viewclients</a> . For mobile View clients, you can alternatively instruct your end users to get the latest version of View Client from the Apple App Store or Google Play.
<b>View Portal</b>	End users can open a browser and browse to a View Connection Server instance. The Web page that appears is called View Portal, and it contains links for downloading the installer file for View Client. <b>NOTE</b> The default links in View Portal point to the VMware Clients download site. You can change the default links to point elsewhere. See the topic called “Configure the View Client Download Links Displayed in View Portal” in the <i>VMware View 5.1 Installation</i> document. If their existing View Clients require smart cards and end users use Internet Explorer to connect to View Portal, they might be prompted to insert a smart card before View Portal checks the client version. End users can either insert their smart card or click <b>Cancel</b> . The result is the same. View Portal checks the version and prompts end users to download the new client installer.
<b>Thin client</b>	Upgrade the thin client firmware and install the new View Client on end users’ client devices. Thin clients and zero clients are provided by VMware partners.

- 2 Have end users verify that they can log in and connect to their View desktops.

**What to do next**

If your end users have View Client with Local Mode, upgrade these clients. See [“Upgrade View Local Mode Clients,”](#) on page 51.

**Upgrade View Local Mode Clients**

Upgrading View Client with Local Mode is very similar to upgrading View Client for Windows. You run the new installer on the client system.

---

**IMPORTANT** This procedure provides instructions for upgrading from View 4.6.x or 5.0.x Client with Local Mode. If your end users have View Client with Local Mode 4.0.x or 4.5.x, instruct them to check in their View desktops and then ask them to remove the View Client for Local Mode software from their client systems. After their View desktops are upgraded to View 5.1 in the datacenter, they can perform a fresh installation of View Client for Local Mode 5.1 and check out their upgraded View desktops.

---

**Prerequisites**

- Verify that View Connection Server, View Composer, and View Transfer Server have all been upgraded to version 5.1. See [Chapter 5, “Upgrading VMware View Server Components,”](#) on page 25. If only one or two of these components are upgraded to version 5.1, you will not be able to check out View desktops if the desktops are based on linked clones.
- Verify that you have either a local user account with administrative privileges or a domain user account with administrative privileges on client systems that you will use to run the installer and perform the upgrade.
- Verify that client computers have a supported operating system and can accommodate the View desktop that end users plan to download and run locally. See [“Supported Operating Systems for Windows-Based View Client and View Client with Local Mode,”](#) on page 17 and [“Hardware Requirements for Local Mode Desktops,”](#) on page 17.
- Determine a strategy for upgrading the View Agent software installed in the local desktop operating system. One strategy is to instruct end users to check in their local desktops so that you can upgrade View Agent on the virtual machine in the datacenter. Another strategy is to upgrade View Agent inside the local View desktop on the client system. You can use whatever third-party tools you usually use for software upgrades.

**Procedure**

- 1 If applicable, have end users check in their local desktops.
  - If you plan to upgrade View Agent on the virtual machine in the datacenter, have end users check in their local mode desktops.
  - If the end user occasionally switches back and forth between system locales that use unicode and non-unicode characters, have the user check in the View desktop before upgrading View Client.
- 2 On the client system, run the View 5.1 Client with Local Mode installer.

If end users have the required administrative privileges on their computers, you have several options for providing end users with the installer:

- Download the installer from the VMware Web site and send it to your end users. Go to the following URL: <https://www.vmware.com/go/viewclients>.
- Post the installer on a company Web site and ask end users to download it.

- Give end users the URL for View Portal and have them download the installer from View Portal.

---

**NOTE** The default links in View Portal point to the VMware Clients download site. You can change the default links to point elsewhere. See the topic called "Configure the View Client Download Links Displayed in View Portal" in the *VMware View 5.1 Installation* document.

---

- 3 Have end users verify that they can log in and connect to their local View desktops.

### **What to do next**

If end users checked in their local mode desktops so that the View Agent software could be upgraded in the datacenter, when the View Agent upgrade is complete, instruct end users to check out their newly upgraded View desktops to their local systems.

If the View Agent software inside the local desktops is not yet upgraded to View Agent 5.1, upgrade View Agent, either in the datacenter virtual machine or on the local client system.

# Applying VMware View Patches

---

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

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

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

This chapter includes the following topics:

- [“Apply a Patch for View Connection Server,”](#) on page 53
- [“Apply a Patch for View Composer,”](#) on page 54
- [“Apply a Patch for View Agent,”](#) on page 55
- [“Apply a Patch for View Clients,”](#) on page 56

## Apply a Patch for View Connection Server

Applying a patch involves uninstalling the current version and then installing the patch version.

### Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. The amount of time required depends on the number of View Connection Server instances in the group. Budget 15 minutes to half an hour for each instance.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the patch installer.

### Procedure

- 1 If View Connection Server is installed in a virtual machine, take a snapshot of the virtual machine.  
For instructions on taking snapshots, see the vSphere Client online help.
- 2 Stop the service called `VMware View Connection Server service` on all View Connection Server instances in the group.

View LDAP database corruption can occur if you upgrade a View Connection Server instance while other instances in the same group are running. Do not stop the `VMwareVDMDS` service.

- 3 On one of the View Connection Server instances in a replicated group, download the installer file for the patch version of VMware View Connection Server.  
Your contact at VMware will provide instructions for this download.
- 4 Use the Windows **Add/Remove Programs** utility to remove your previously installed View Connection Server, but do not remove **Adam Instance VMwareVDMDS**.
- 5 Run the installer that you downloaded for the patch release of VMware View Connection Server.  
For information about running the installer, see the *VMware View Installation* document.
- 6 Follow the installation wizard prompts and click **OK** when asked to continue the installation with the existing ADAM instance.
- 7 Verify that the VMware View Connection Server service restarts after the installer wizard closes.
- 8 Stop the View Connection Server service again.
- 9 Repeat [Step 3](#) through [Step 8](#) for the other View Connection Server instances in the replicated group.
- 10 After all servers in the group are upgraded, start the View Connection Server service on all of them.
- 11 Repeat this process for View security servers.

#### What to do next

If applying the patch fails on one or more of the View Connection Server instances, see [“Create a Replicated Group After Reverting View Connection Server to a Snapshot,”](#) on page 29.

Apply the patch to View Composer or View Agent, as applicable.

## Apply a Patch for View Composer

Applying a patch involves uninstalling the current version and then installing the patch version. Not all patch releases include patches for View Composer.

#### Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance of View Composer.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the patch installer.
- If View Composer is installed in a virtual machine, take a snapshot of the virtual machine.  
For instructions on taking snapshots, see the vSphere Client online help.
- Back up the vCenter Server database and the View Composer database.  
For instructions on performing a database backup, see the documentation from your database vendor.
- For all linked-clone desktop pools, disable provisioning of new virtual machines.
- If any desktop pools are scheduled to do a refresh or recompose operation, cancel these tasks.

#### Procedure

- 1 On the virtual machine that hosts View Composer, download the installer file for the patch version of VMware View Composer.  
Your contact at VMware will provide instructions for this download.
- 2 Use the Windows **Add/Remove Programs** utility to remove your previously installed View Composer.
- 3 Run the installer that you downloaded for the patch release of VMware View Composer.

- 4 Verify that the VMware View Composer service restarts after the installer wizard closes.
- 5 If applicable, apply the patch for View Agent on a parent virtual machine and create a desktop pool for testing purposes.
  - a Use the Windows **Add/Remove Programs** utility to remove your previously installed View Agent.
  - b Download and run the VMware View Agent patch installer on a parent virtual machine.  
Your contact at VMware will provide instructions for this download.
  - c Create a small linked-clone desktop pool from this virtual machine.
  - d Test a virtual desktop from the desktop pool to verify that all the usage scenarios function properly.  
For example, create a desktop pool that contains one virtual desktop, and verify that you can use View Client to log in to that desktop.  
  
Step-by-step instructions for running the View Agent installer and creating desktop pools appear in the *VMware View Administration* document, available by clicking the **Help** button in View Administrator.
  - e Verify that virtual desktops from the test desktop pool work as expected.

#### What to do next

Apply the patch to View Agent, if applicable.

## Apply a Patch for View Agent

Applying a patch involves uninstalling the current version and then installing the patch version.

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

#### Prerequisites

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

#### Procedure

- 1 On all parent virtual machines, virtual machines used for full-clone templates, full clones in a pool, and manually added individual virtual machines, download the installer file for the patch version of VMware View Agent.  
  
Your contact at VMware will provide instructions for this download.
- 2 Use the Windows **Add/Remove Programs** utility to remove the previously installed View Agent.
- 3 Run the installer that you downloaded for the patch release of the VMware View Agent.  
  
Step-by-step instructions for running the View Agent installer appear in the *VMware View Administration* document.
- 4 If you disabled provisioning of new virtual machines in preparation for applying a patch to View Composer, enable provisioning again.
- 5 For parent virtual machines that will be used to create linked-clone desktop pools, take a snapshot of the virtual machine.  
  
For instructions on taking snapshots, see the vSphere Client online help.
- 6 For linked-clone desktop pools, use the snapshot you created to recompose the desktop pools.
- 7 Verify that you can log in to the patched View desktop pools with View Client.

- 8 If you canceled any refresh or recompose operations for any linked-clone desktop pools, schedule the tasks again.

**What to do next**

Apply the patch to one or more View clients, as applicable.

## Apply a Patch for View Clients

Applying a patch involves uninstalling the current version and then installing the patch version.

**Procedure**

- 1 On each client system, download the installer file for the patch version of VMware View Client.  
Your contact at VMware will provide instructions for this download. For some View clients, you might get the patch release from the Android Market or the Apple App Store.
- 2 Remove the current version of the VMware View client from your device.  
Use the customary device-specific method for removing applications.
- 3 If applicable, run the installer that you downloaded for the patch release of the View Client.  
If you got the patch from the Apple App Store or the Android Market, the app is usually installed when you download it, and you do not need to run an installer.
- 4 Verify that you can log in to the patched View desktop pools with the newly patched View Client.



# Upgrading vSphere Components Separately in a VMware View Environment

---

# 9

If you upgrade vSphere components separately from VMware View components, you must back up some View data and reinstall some View software.

Instead of performing an integrated upgrade of VMware View and vSphere components, you can choose to first upgrade all View components and then upgrade vSphere components, or the reverse. You might also upgrade only vSphere components when a new version or update of vSphere is released.

When you upgrade vSphere components separately from View components, you must perform the following additional tasks:

- 1 Before you upgrade vCenter Server, back up the vCenter Server database and the View Composer database.
- 2 Before you upgrade vCenter Server, back up the View LDAP database from a View Connection Server instance by using the `vdmexport.exe` utility.

For instructions, see the *VMware View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need to export the data from only one instance.

- 3 If you use View Composer, after you upgrade all ESX/ESXi hosts that are managed by a particular vCenter Server instance, restart the View Composer service on that host.
- 4 After you upgrade VMware Tools in virtual machines that are used as View desktops, reinstall View Agent.

Reinstalling View Agent guarantees that the drivers in the virtual machine remain compatible with the other View components.

Step-by-step instructions for running the View Agent installer appear in the *VMware View Administration* document.



# Index

## A

ASP.NET IIS registration tool, RSA key container **39**

## B

backward compatibility **7**

blade PCs **47**

browser requirements **16, 19**

## C

certificates, accept the thumbprint **27**

cluster upgrades **45**

compatibility matrix for View components **7**

CPU requirements, local mode desktops **17**

## D

database backups **23**

database compatibility **23**

database upgrade

sviconfig does not succeed **34**

View Composer sviconfig **32, 33**

databaseupgrade, result codes **34**

desktop pool management, upgrading pools **49**

desktop pool upgrade, full clone and linked-clone pools **47**

desktops, local **51**

display requirements, local mode desktops **17**

## E

ESX host upgrade procedure **45**

## F

Firefox, supported versions **16, 19**

firmware upgrades for thin clients **47, 50**

forward compatibility **7**

## G

GPO templates **25**

## H

hardware requirements

local mode desktops **17**

View Composer, standalone **14**

View Connection Server **11**

## I

Internet Explorer, supported versions **16, 19**

## L

LDAP **21**

LDAP upgrade **25**

license requirements **12, 15**

linked-clone desktop management, upgrade procedure **47**

load balancers **21**

local desktop configuration, hardware requirements **17**

local desktop upgrade **51**

## M

maintenance window **25**

memory requirements, local mode desktops **17**

Microsoft SQL Server databases **14**

migrating

View Composer to another computer **35**

View Composer with an existing database **36**

View Composer without linked clones **38**

## N

NET Framework, migrating RSA key container **39**

nonpersistent desktop pools **49**

## O

Oracle databases **14**

## P

patch releases **25, 53**

PCoIP Secure Gateway **12**

persistent desktop pools **49**

physical PCs **47**

port change for View Composer **31**

## R

result codes, databaseupgrade operation **34**

RSA key container

migrating to View Composer **39**

using NET Framework **39**

**S**

- security servers
  - operating system requirements **12**
  - prepare to upgrade or reinstall **22**
  - remove IPsec rules **22**
  - upgrading **25, 30**
- services
  - VMware View Connection Server **25, 30**
  - VMwareVDMDS **25, 30**
- SQL Server databases **14**
- SSL, accept a certificate thumbprint **27**
- SSL certificate backups **23**
- sviconfig utility **32–34**
- system requirements for VMware View upgrades **11**

**T**

- Technical Support, VMware **5**
- thin clients **47, 50**
- thumbprint, accept for a default certificate **27**

**U**

- upgrade check list **9**
- upgrade preparation
  - vCenter Server **23**
  - View Composer **23**
  - View Connection Server **21**
  - VMware View components **21**
- utilities
  - sviconfig **32–34**
  - vdadmin.exe **28**
  - vdlexport.exe **21, 25**

**V**

- vCenter Server, upgrade preparation tasks **57**
- vCenter Server upgrade, upgrade preparation tasks **23**
- vdadmin.exe utility **28**
- vdlexport.exe utility **21, 25**
- View Administrator, requirements **16**
- View Agent
  - applying patches for **55**
  - installation requirements **19**
  - upgrade procedure **47, 57**
- View Client
  - applying patches for **56**
  - supported operating systems **17**
  - upgrade **47, 50**
  - upgrading **51**
- View Client with Local Mode, supported operating systems **17**
- View Composer
  - applying patches for **54**

hardware requirements for standalone View Composer **14**

sviconfig database upgrade **32**

upgrade requirements **15**

vSphere mode **45**

View Composer database, requirements **14**

View Composer installation, requirements overview **13**

View Composer maintenance

guidelines for migrating **36**

migrating an RSA key container **39**

migrating View Composer to another computer **35**

migrating with the existing database **36**

View Composer upgrade

compatibility with vCenter Server versions **13**

database upgrade does not complete **34**

operating system requirements **13**

port change **31**

requirements overview **13**

sviconfig database upgrade **33**

upgrade preparation tasks **23**

upgrade procedure **31, 40**

View Connection Server

applying patches for **53**

hardware requirements **11**

migrating to a new machine **28**

revert to a snapshot **29**

upgrade preparation tasks **21**

upgrade procedure **25**

upgrade requirements **12**

View Connection Server installation

requirements overview **11**

supported operating systems **12**

virtualization software requirements **13**

View LDAP **21**

View LDAP upgrade **25**

View Portal, browser requirements **19**

View Transfer Server

migrating to a new machine **42**

upgrade procedure **42**

View Transfer Server installation

requirements overview **16**

supported operating systems **16**

virtual machine requirements **16**

View Transfer Server upgrade, upgrade

procedure **41**

virtual hardware upgrade procedure **45**

virtual machines, upgrading **45**

VirtualCenter upgrade procedure **31, 40**

VMotion **45**

VMware Infrastructure 3 **5**

VMware Tools, upgrade procedure **45, 57**

VMwareVDMDS service **25, 30**

vSphere, upgrading components separately **57**  
vSphere mode for View Composer **45**  
vSphere Update Manager **45**

## **W**

Web browser requirements **16, 19**  
Windows 7 requirements, local mode  
  desktops **17**  
Windows Terminal Servers **47**

