VMware View Installation

View 5.0
View Manager 5.0
View Composer 2.7

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

VMware View Installation 5

1 System Requirements for Server Components 7
   View Connection Server Requirements 7
   View Administrator Requirements 9
   View Composer Requirements 9
   View Transfer Server Requirements 11

2 System Requirements for Client Components 13
   Supported Operating Systems for View Agent 13
   Supported Operating Systems for Windows-Based View Client and View Client with Local Mode 14
   Hardware Requirements for Local Mode Desktops 14
   Client Browser Requirements for View Portal 16
   Remote Display Protocol and Software Support 16
   Adobe Flash Requirements 19
   Smart Card Authentication Requirements 20

3 Preparing Active Directory 21
   Configuring Domains and Trust Relationships 21
   Creating an OU for View Desktops 22
   Creating OUs and Groups for Kiosk Mode Client Accounts 22
   Creating Groups for View Users 22
   Creating a User Account for vCenter Server 22
   Create a User Account for View Composer 23
   Configure the Restricted Groups Policy 23
   Using View Group Policy Administrative Template Files 24
   Prepare Active Directory for Smart Card Authentication 24

4 Installing View Composer 27
   Prepare a View Composer Database 27
   Install the View Composer Service 32
   Configuring Your Infrastructure for View Composer 34

5 Installing View Connection Server 35
   Installing the View Connection Server Software 35
   Configuring User Accounts for vCenter Server and View Composer 49
   Configuring View Connection Server for the First Time 52
   Configuring View Client Connections 56
   Sizing Windows Server Settings to Support Your Deployment 59
6 Installing View Transfer Server 67
   Install View Transfer Server 67
   Add View Transfer Server to View Manager 69
   Configure the Transfer Server Repository 70
   Firewall Rules for View Transfer Server 71
   Installing View Transfer Server Silently 71

7 Configuring SSL Certificates for View Servers 75
   Configuring SSL Certificates for View Connection Server and Security Server 76
   Configuring SSL Certificates for View Transfer Server 83
   Configuring Certificate Checking in View Client for Windows 87
   Appendix: Additional SSL Configuration Tasks 88

8 Creating an Event Database 91
   Add a Database and Database User for View Events 91
   Prepare an SQL Server Database for Event Reporting 92
   Configure the Event Database 92

9 Installing and Starting View Client 95
   Install the Windows-Based View Client or View Client with Local Mode 95
   Start the Windows-Based View Client or View Client with Local Mode 96
   Install View Client by Using View Portal 98
   Set Printing Preferences for the Virtual Printer Feature on Windows Clients 99
   Using USB Printers 100
   Installing View Client Silently 101

Index 105
VMware View Installation

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

**Intended Audience**

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

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

This chapter includes the following topics:

- “View Connection Server Requirements,” on page 7
- “View Administrator Requirements,” on page 9
- “View Composer Requirements,” on page 9
- “View Transfer Server Requirements,” on page 11

**View Connection Server Requirements**

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

- Hardware Requirements for View Connection Server on page 7
  You must install View Connection Server on a dedicated physical or virtual machine that meets specific hardware requirements.

- Supported Operating Systems for View Connection Server on page 8
  You must install View Connection Server on a supported operating system.

- Virtualization Software Requirements for View Connection Server on page 8
  View Connection Server requires VMware virtualization software to function properly.

- Network Requirements for Replicated View Connection Server Instances on page 9
  If you install replicated View Connection Server instances, configure the instances in the same location and connect them over a high-performance LAN.

**Hardware Requirements for View Connection Server**

You must install View Connection Server on a dedicated physical or virtual machine that meets specific hardware requirements.

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

<table>
<thead>
<tr>
<th>Hardware Component</th>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Pentium IV 2.0GHz processor or higher</td>
<td>4 CPUs</td>
</tr>
<tr>
<td>Networking</td>
<td>One or more 10/100Mbps network interface cards (NICs)</td>
<td>1Gbps NICs</td>
</tr>
</tbody>
</table>
Table 1-1. View Connection Server Hardware Requirements (Continued)

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

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 supported operating system.

Table 1-2 lists the operating systems supported for View Connection Server.

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

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Edition</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server</td>
<td>64-bit</td>
<td>Standard</td>
<td>None or SP1</td>
</tr>
<tr>
<td>Windows Server</td>
<td>32-bit</td>
<td>Standard</td>
<td>SP2</td>
</tr>
</tbody>
</table>

### Operating System Requirement for the PCoIP Secure Gateway

Although you can install a security server on a Windows Server 2003 physical or virtual machine, if you want to use the PCoIP Secure Gateway component, the operating system must be 64-bit Windows Server 2008 R2. The PCoIP Secure Gateway component enables View Clients that use the PCoIP display protocol to use a security server rather than a VPN from outside the corporate firewall.

You can pair a security server that runs on a 64-bit Windows Server 2008 R2 host with a Connection Server instance that runs on Windows Server 2003 or 2003 R2. Clients can still use the PCoIP Secure Gateway with this pair.

**IMPORTANT** If you use a load balancer in front of multiple security servers, make sure all security servers use the same operating system.

### Virtualization Software Requirements for View Connection Server

View Connection Server requires VMware virtualization software to function properly.

- If you are using vSphere, you must use one of the following supported versions:
  - vSphere 4.0 Update 3 or later
  - vSphere 4.1 Update 1 or later
  - vSphere 5.0 or later
Both ESX and ESXi hosts are supported.

Network Requirements for Replicated View Connection Server Instances

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

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

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

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

View Administrator Requirements

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

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

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Firefox 3.0
- Firefox 3.5

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.

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

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

View Composer Requirements

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

- **Supported Operating Systems for View Composer** on page 10
  View Composer supports 64-bit operating systems with specific requirements and limitations. You must install View Composer on the same physical computer or virtual machine as vCenter Server.

- **Database Requirements for View Composer** on page 10
  View Composer requires an SQL database to store data. The View Composer database must reside on, or be available to, the vCenter Server computer.
Supported Operating Systems for View Composer

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

Table 1-3 lists the operating systems supported for View Composer.

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

<table>
<thead>
<tr>
<th>vCenter Server Version</th>
<th>Operating System</th>
<th>Edition</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0 Update 3 and later</td>
<td>Windows Server 2008 R2</td>
<td>Standard or Enterprise</td>
<td>None or SP1</td>
</tr>
<tr>
<td>4.1 Update 1 and later</td>
<td>Windows Server 2008 R2</td>
<td>Standard or Enterprise</td>
<td>None or SP1</td>
</tr>
<tr>
<td>5.0 and later</td>
<td>Windows Server 2008 R2</td>
<td>Standard or Enterprise</td>
<td>None or SP1</td>
</tr>
</tbody>
</table>

Database Requirements for View Composer

View Composer requires an SQL database to store data. The View Composer database must reside on, or be available to, the vCenter Server computer.

If a database server already exists for vCenter Server, View Composer can use that existing database server if it is a version listed in Table 1-4. For example, View Composer can use the Microsoft SQL Server 2005 or 2008 Express instance provided with vCenter Server. If a database server does not already exist, you must install one.

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

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

Table 1-4 lists the supported database servers and versions. For a complete list of database versions supported with vCenter Server, see the VMware vSphere Compatibility Matrixes on the VMware vSphere documentation Web site.

Table 1-4. Supported Database Servers for View Composer

<table>
<thead>
<tr>
<th>Database</th>
<th>vCenter Server 5.0 and later</th>
<th>vCenter Server 4.1 U1 and later</th>
<th>vCenter Server 4.0 U3 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server 2005 Express</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft SQL Server 2005 SP3 and later, Standard and Enterprise (32- and 64-bit)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2 Express</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 1-4. Supported Database Servers for View Composer (Continued)

<table>
<thead>
<tr>
<th>Database</th>
<th>vCenter Server 5.0 and later</th>
<th>vCenter Server 4.1 U1 and later</th>
<th>vCenter Server 4.0 U3 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server 2008 SP1 and later, Standard and Enterprise (32- and 64-bit)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Oracle 10g Release 2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Oracle 11g Release 2, with Oracle 11.2.0.1 Patch 5</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

**View Transfer Server Requirements**

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

- **Installation Requirements for View Transfer Server** on page 11
  You must install View Transfer Server as a Windows application in a virtual machine that meets specific requirements.

- **Supported Operating Systems for View Transfer Server** on page 12
  You must install View Transfer Server on a supported operating system with at least the minimum required amount of RAM.

- **Storage Requirements for View Transfer Server** on page 12
  View Transfer Server transfers static content to and from the Transfer Server repository and dynamic content between local desktops and remote desktops in the datacenter. View Transfer Server has specific storage requirements.

**Installation Requirements for View Transfer Server**

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

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

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

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

On Windows Server 2008 virtual machines, the LSI Logic SAS controller is selected by default. You must change this selection to an LSI Logic Parallel controller before you install the operating system.
The View Transfer Server software cannot coexist on the same virtual machine with any other View Manager software component, including View Connection Server.

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

**Supported Operating Systems for View Transfer Server**

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

**Table 1-5. Operating System Support for View Transfer Server**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2</td>
<td>64-bit</td>
<td>Standard</td>
<td>None or SP1</td>
<td>4GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003 R2</td>
<td>32-bit</td>
<td>Standard</td>
<td>SP2</td>
<td>2GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enterprise</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**Storage Requirements for View Transfer Server**

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

- The disk drive on which you configure the Transfer Server repository must have enough space to store your static image files. Image files are View Composer base images.

- View Transfer Server must have access to the datastores that store the desktop disks to be transferred. The datastores must be accessible from the ESX/ESXi host where the View Transfer Server virtual machine is running.

- The recommended maximum number of concurrent disk transfers that View Transfer Server can support is 20.

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

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

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

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

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

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

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

View Client on Windows systems uses Microsoft Internet Explorer Internet settings, including proxy settings, when connecting to View Connection Server. Ensure that your Internet Explorer settings are accurate and that you can access the View Connection Server URL through Internet Explorer. You can use Internet Explorer 7, 8, or 9.

This chapter includes the following topics:
- “Supported Operating Systems for View Agent,” on page 13
- “Supported Operating Systems for Windows-Based View Client and View Client with Local Mode,” on page 14
- “Hardware Requirements for Local Mode Desktops,” on page 14
- “Client Browser Requirements for View Portal,” on page 16
- “Remote Display Protocol and Software Support,” on page 16
- “Adobe Flash Requirements,” on page 19
- “Smart Card Authentication Requirements,” on page 20

Supported Operating Systems for View Agent

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

Table 2-1 lists the operating systems supported for View Agent.

Table 2-1. View Agent Operating System Support

<table>
<thead>
<tr>
<th>Guest Operating System</th>
<th>Version</th>
<th>Edition</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>64-bit and 32-bit</td>
<td>Enterprise and Professional</td>
<td>None and SP1</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>32-bit</td>
<td>Business and Enterprise</td>
<td>SP1 and SP2</td>
</tr>
<tr>
<td>Windows XP</td>
<td>32-bit</td>
<td>Professional</td>
<td>SP3</td>
</tr>
<tr>
<td>Windows 2008 R2 Terminal Server</td>
<td>64-bit</td>
<td>Standard</td>
<td>None and SP1</td>
</tr>
<tr>
<td>Windows 2008 Terminal Server</td>
<td>64-bit</td>
<td>Standard</td>
<td>SP2</td>
</tr>
<tr>
<td>Windows 2003 R2 Terminal Server</td>
<td>32-bit</td>
<td>Standard</td>
<td>SP2</td>
</tr>
<tr>
<td>Windows 2003 Terminal Server</td>
<td>32-bit</td>
<td>Standard</td>
<td>SP2</td>
</tr>
</tbody>
</table>
To use the View Persona Management feature, you must install View Agent on Windows 7, Windows Vista, or Windows XP virtual machines. View Persona Management does not operate on physical computers or Microsoft Terminal Servers.

**IMPORTANT** If you use Windows 7 in a virtual machine, the host must be ESX/ESXi 4.0 Update 3 or later, ESX/ESXi 4.1 Update 1 or later, or ESXi 5.0 or later.

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

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

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Edition</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7</td>
<td>32-bit and 64-bit</td>
<td>Home, Enterprise, Professional, and Ultimate</td>
<td>None and SP1</td>
</tr>
<tr>
<td>Windows XP</td>
<td>32-bit</td>
<td>Home and Professional</td>
<td>SP3</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>32-bit</td>
<td>Home, Business, Enterprise, and Ultimate</td>
<td>SP 1 and SP2</td>
</tr>
</tbody>
</table>

**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.

#### Virtual Hardware

Checking out a View desktop that uses virtual hardware version 8 is not supported. If you use vSphere 5 to create virtual machines that will be sources for local mode desktops, be sure to create virtual machines that use virtual hardware version 7.

#### PC Hardware

Table 2-3 describes the hardware requirements for various View desktop operating systems.
Table 2-3. Processor Requirements

<table>
<thead>
<tr>
<th>Client Computer Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC</td>
<td>Standard x86 or x86 64-compatible</td>
</tr>
<tr>
<td>Number of CPUs</td>
<td>Multiprocessor systems are supported</td>
</tr>
<tr>
<td>CPU speed</td>
<td>For a Windows XP local desktop, 1.3GHz or faster; 1.6 1GHz recommended For a Windows 7 desktop, 1.3GHz or faster; for Aero effects, 2.0GHz or faster</td>
</tr>
<tr>
<td>Intel processors</td>
<td>Pentium 4, Pentium M (with PAE), Core, Core 2, Core i3, Core i5, and Core i7 processors For Windows 7 Aero: Intel Dual Core</td>
</tr>
<tr>
<td>AMD processors</td>
<td>Athlon, Athlon MP, Athlon XP, Athlon 64, Athlon X2, Duron, Opteron, Turion X2, Turion 64, Sempron, Phenom, and Phenom II For Windows 7 Aero: Althon 4200+ and above</td>
</tr>
<tr>
<td>64-bit operating systems</td>
<td>Intel Pentium 4 and Core 2, and Core i7 processors with EM64T and Intel Virtualization Technology Most AMD64 processors (except the earliest revision C Opteron processors)</td>
</tr>
<tr>
<td>GPU for Windows 7 Aero</td>
<td>nVidia GeForce 8800GT and above ATI Radeon HD 2600 and above</td>
</tr>
</tbody>
</table>

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 32-bit client computers is 8GB and on 64-bit computers it is 32GB.
Display

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

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

For CPU and GPU requirements to support Windows 7 Aero, see Table 2-3.

Client Browser Requirements for View Portal

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

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

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Firefox 3.0
- Firefox 3.5

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

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

Remote Display Protocol and Software Support

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

- **VMware View with PCoIP on page 17**
  
  PCoIP provides an optimized desktop experience for the delivery of the entire desktop environment, including applications, images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP can compensate for an increase in latency or a reduction in bandwidth, to ensure that end users can remain productive regardless of network conditions.

- **Microsoft RDP on page 18**
  
  Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.

- **Multimedia Redirection (MMR) on page 19**
  
  Multimedia redirection (MMR) delivers the multimedia stream directly to client computers by using a virtual channel.
VMware View with PCoIP

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

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

PCoIP Features

Key features of PCoIP include the following:

- For users outside the corporate firewall, you can use this protocol with your company’s virtual private network or with View security servers.
- Connections to Windows desktops with the View Agent operating system versions listed in “Supported Operating Systems for View Agent,” on page 13 are supported.
- Connections from Windows clients with the View Client operating system versions listed in “Supported Operating Systems for Windows-Based View Client and View Client with Local Mode,” on page 14 are supported.
- MMR redirection is supported for Windows XP and Vista clients. MMR redirection is not supported for Windows 7 View Clients and is not supported on Windows 7 View desktops.
- USB redirection is supported.
- Audio redirection with dynamic audio quality adjustment for LAN and WAN is supported.
- Multiple monitors are supported. You can use up to four monitors and adjust the resolution for each monitor separately, with a resolution of up to 2560x1600 per display. Pivot display and autofit are also supported.
  
  When 3D feature is enabled, up to 2 monitors are supported with a resolution of up to 1920x1200.
- 32-bit color is supported for virtual displays.
- ClearType fonts are supported.
- Copy and paste of text and images between the local system and the desktop is supported, up to 1MB. Supported file formats include text, images, and RTF (Rich Text Format). You cannot copy and paste system objects such as folders and files between systems.

Video Quality

480p-formatted video

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

720p-formatted video

You can play video at 720p at native resolutions if the View desktop has a dual virtual CPU. Performance might be affected if you play videos at 720p in high definition or in full screen mode.
1080p-formatted video

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

3D

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

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

**Recommended Guest Operating System Settings**

Recommended guest operating system settings include the following settings:

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

**Client Hardware Requirements**

Client hardware requirements include the following:

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

  \[20MB + (24 \times \#\text{monitors}) \times (\text{monitor width}) \times (\text{monitor height})\]

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

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

**Microsoft RDP**

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

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

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

You can download RDC versions from the Microsoft Web site.

**Client Hardware Requirements**

Client hardware requirements include the following:

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

**Multimedia Redirection (MMR)**

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

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

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

- Windows XP
- Windows XP Embedded
- Windows Vista

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

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

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

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

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

**Adobe Flash Requirements**

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

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

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

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

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

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

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

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

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

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

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

See “Prepare Active Directory for Smart Card Authentication,” on page 24 for information on tasks you might need to perform in Active Directory when you implement smart card authentication with View.

Smart card authentication is not supported by View Client for Mac or View Administrator. See the *VMware View Architecture Planning* document for complete information on smart card support.
Preparing Active Directory

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

View supports the following versions of Active Directory:

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

This chapter includes the following topics:

- “Configuring Domains and Trust Relationships,” on page 21
- “Creating an OU for View desktops,” on page 22
- “Creating OUs and Groups for Kiosk Mode Client Accounts,” on page 22
- “Creating Groups for View Users,” on page 22
- “Creating a User Account for vCenter Server,” on page 22
- “Create a User Account for View Composer,” on page 23
- “Configure the Restricted Groups Policy,” on page 23
- “Using View Group Policy Administrative Template Files,” on page 24
- “Prepare Active Directory for Smart Card Authentication,” on page 24

Configuring Domains and Trust Relationships

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

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

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

**Note**  Because security servers do not access any authentication repositories, including Active Directory, they do not need to reside in an Active Directory domain.
Trust Relationships and Domain Filtering

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

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

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

Creating an OU for View Desktops

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

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

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

Creating OUs and Groups for Kiosk Mode Client Accounts

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

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

See the VMware View Administration document for more information.

Creating Groups for View Users

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

Creating a User Account for vCenter Server

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

The user account must be in the same domain as your View Connection Server host or in a trusted domain. If you use View Composer, you must add the user account to the local Administrators group on the vCenter Server computer.
You must give the user account privileges to perform certain operations in vCenter Server. If you use View Composer, you must give the user account additional privileges. See “Configuring User Accounts for vCenter Server and View Composer,” on page 49 for information on configuring these privileges.

Create a User Account for View Composer

If you use View Composer, you must create a user account in Active Directory to use with View Composer. View Composer requires this account to join linked-clone desktops to your Active Directory domain.

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

Procedure

1. In Active Directory, create a user account in the same domain as your View Connection Server host or in a trusted domain.
2. Add the Create Computer Objects, Delete Computer Objects, and Write All Properties permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

   The following list shows all the required permissions for the user account, including permissions that are assigned by default:
   - List Contents
   - Read All Properties
   - Write All Properties
   - Read Permissions
   - Create Computer Objects
   - Delete Computer Objects
3. Make sure that the user account's permissions apply to the Active Directory container and to all child objects of the container.

What to do next

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

Configure the Restricted Groups Policy

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

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

Prerequisites

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

2. Right-click your domain and select Properties.
3. On the Group Policy tab, click Open to open the Group Policy Management plug-in.
4. Right-click Default Domain Policy and click Edit.
5. Expand the Computer Configuration section and open Windows Settings\Security Settings.
6. Right-click Restricted Groups, select Add Group, and add the Remote Desktop Users group.
7. Right-click the new restricted Remote Desktop Users group and add your View desktop users group to the group membership list.
8. Click OK to save your changes.

Using View Group Policy Administrative Template Files

View includes several component-specific group policy administrative (ADM) template files. During View Connection Server installation, the View ADM template files are installed in the install_directory\VMware\VMware View\Server\Extras\GroupPolicyFiles directory on your View Connection Server host. You must copy these files to a directory on your Active Directory server.

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

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

Prepare Active Directory for Smart Card Authentication

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

- **Add UPNs for Smart Card Users** on page 25
  Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users that use smart cards to authenticate in View must have a valid UPN.

- **Add the Root Certificate to Trusted Root Certification Authorities** on page 25
  If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

- **Add an Intermediate Certificate to Intermediate Certification Authorities** on page 26
  If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

- **Add the Root Certificate to the Enterprise NTAuth Store** on page 26
  If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.
Add UPNs for Smart Card Users

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

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

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

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

**Procedure**
1. On your Active Directory server, start the ADSI Edit utility.
2. In the left pane, expand the domain the user is located in and double-click CN=Users.
3. In the right pane, right-click the user and then click **Properties**.
4. Double-click the **userPrincipalName** attribute and type the SAN value of the trusted CA certificate.
5. Click **OK** to save the attribute setting.

Add the Root Certificate to Trusted Root Certification Authorities

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

**Procedure**
1. On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click your domain and click **Properties**.
3. On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in.
4. Right-click **Default Domain Policy** and click **Edit**.
5. Expand the **Computer Configuration** section and open **Windows Settings\Security Settings\Public Key**.
6. Right-click **Trusted Root Certification Authorities** and select **Import**.
7. Follow the prompts in the wizard to import the root certificate (for example, rootCA.cer) and click **OK**.
8. Close the Group Policy window.

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

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See “Add an Intermediate Certificate to Intermediate Certification Authorities,” on page 26.

Add an Intermediate Certificate to Intermediate Certification Authorities

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

Procedure

2. Right-click your domain and click Properties.
3. On the Group Policy tab, click Open to open the Group Policy Management plug-in.
4. Right-click Default Domain Policy, and click Edit.
5. Expand the Computer Configuration section and open Windows Settings\Security Settings\Public Key.
6. Right-click Intermediate Certification Authorities and select Import.
7. Follow the prompts in the wizard to import the intermediate certificate (for example, intermediateCA.cer) and click OK.
8. Close the Group Policy window.

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

Add the Root Certificate to the Enterprise NTAuth Store

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

Procedure

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

For example: certutil -dspublish -f path_to_root_CA_cert NTAuthCA

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

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

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

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

This chapter includes the following topics:

- “Prepare a View Composer Database,” on page 27
- “Install the View Composer Service,” on page 32
- “Configuring Your Infrastructure for View Composer,” on page 34

Prepare a View Composer Database

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

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

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

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

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

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

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

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

- Create a SQL Server Database for View Composer on page 28

  View Composer can store linked-clone desktop information in a SQL Server database. You create a View Composer database by adding it to SQL Server and configuring an ODBC data source for it.
Create an Oracle Database for View Composer on page 29

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

Create a SQL Server Database for View Composer

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

Add a View Composer Database to SQL Server

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

If the database resides on the same system as vCenter Server, you can use the Integrated Windows Authentication security model. If the database resides on a remote system, you cannot use this method of authentication.

Prerequisites

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

Procedure

1. On the vCenter Server computer, select Start > All Programs > Microsoft SQL Server 2008 or Microsoft SQL Server 2005.
2. Select SQL Server Management Studio Express and connect to the existing SQL Server instance for vSphere Management.
3. In the Object Explorer panel, right-click the Databases entry and select New Database.
4. In the New Database dialog box, type a name in the Database name text box.
   For example: viewComposer
5. Click OK.
   SQL Server Management Studio Express adds your database to the Databases entry in the Object Explorer panel.

What to do next

Follow the instructions in “Add an ODBC Data Source to SQL Server,” on page 28.

Add an ODBC Data Source to SQL Server

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

These instructions assume that you are configuring the ODBC data source on Windows Server 2003 SP2.
Prerequisites

Complete the steps described in “Add a View Composer Database to SQL Server,” on page 28.

Procedure

1. On the vCenter Server computer, select Start > Administrative Tools > Data Source (ODBC).
2. Select the System DSN tab.
3. Click Add and select SQL Native Client from the list.
4. Click Finish.
5. In the Create a New Data Source to SQL Server setup wizard, type a name and description of the View Composer database.
   For example: ViewComposer
6. In the Server text box, type the SQL Server database name.
   Use the form host_name\server_name, where host_name is the name of the computer and server_name is the SQL Server instance.
   For example: VCHOST1\SQLEXP_VIM
7. Click Next.
8. Make sure that the Connect to SQL Server to obtain default settings for the additional configuration options check box is selected and select an authentication option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows NT authentication</td>
<td>Select this option if you are using a local instance of SQL Server. This option is also known as trusted authentication. Windows NT authentication is supported only if SQL Server is running on the vCenter Server computer.</td>
</tr>
<tr>
<td>SQL Server authentication</td>
<td>Select this option if you are using a remote instance of SQL Server. Windows NT authentication is not supported on remote SQL Server.</td>
</tr>
</tbody>
</table>
9. Click Next.
10. Select the Change the default database to check box and select the name of the View Composer database from the list.
    For example: ViewComposer
11. Finish and close the Microsoft ODBC Data Source Administrator wizard.

What to do next

Install the new View Composer service on the vCenter Server computer. See “Install the View Composer Service,” on page 32.

Create an Oracle Database for View Composer

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

- Add a View Composer Database to Oracle 11g or 10g on page 30
  You can use the Oracle Database Configuration Assistant to add a new View Composer database to an existing Oracle 11g or 10g instance.
Use a SQL Statement to Add a View Composer Database to an Oracle Instance on page 31
The View Composer database must have certain table spaces and privileges. You can use a SQL statement to create the View Composer database in an Oracle 11g or 10g database instance.

Configure an Oracle Database User for View Composer on page 31
By default, the database user that runs the View Composer database has Oracle system administrator permissions. To restrict the security permissions for the user that runs the View Composer database, you must configure an Oracle database user with specific permissions.

Add an ODBC Data Source to Oracle 11g or 10g on page 32
After you add a View Composer database to an Oracle 11g or 10g instance, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

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

Prerequisites
Verify that a supported version of Oracle 11g or 10g is installed on the vCenter Server computer. See “Database Requirements for View Composer,” on page 10.

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

<table>
<thead>
<tr>
<th>Database Version</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 11g</td>
<td>Select Start &gt; All Programs &gt; Oracle-OraDb11g_home &gt; Configuration and Migration Tools &gt; Database Configuration Assistant.</td>
</tr>
<tr>
<td>Oracle 10g</td>
<td>Select Start &gt; All Programs &gt; Oracle-OraDb10g_home &gt; Configuration and Migration Tools &gt; Database Configuration Assistant.</td>
</tr>
</tbody>
</table>

2. On the Operations page, select Create a database.
3. On the Database Templates page, select the General Purpose or Transaction Processing template.
4. On the Database Identification page, type a Global Database Name and an Oracle System Identifier (SID) prefix.
   For simplicity, use the same value for both items.
5. On the Management Options page, click Next to accept the default settings.
6. On the Database Credentials page, select Use the Same Administrative Passwords for All Accounts and type a password.
7. On the remaining configuration pages, click Next to accept the default settings.
8. On the Creation Options page, verify that Create Database is selected and click Finish.
9. On the Confirmation page, review the options and click OK.
   The configuration tool creates the database.
10. On the Database Creation Complete page, click OK.

What to do next
Follow the instructions in “Add an ODBC Data Source to Oracle 11g or 10g,” on page 32.
Use a SQL Statement to Add a View Composer Database to an Oracle Instance

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

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

**Prerequisites**

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

**Procedure**

1. Log in to a SQL*Plus session with the system account.
2. Run the following SQL statement to create the database.

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

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

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

**What to do next**

If you want to run the View Composer database with specific security permissions, follow the instructions in “Configure an Oracle Database User for View Composer,” on page 31.

Follow the instructions in “Add an ODBC Data Source to Oracle 11g or 10g,” on page 32.

**Configure an Oracle Database User for View Composer**

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

**Prerequisites**

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

**Procedure**

1. Log in to a SQL*Plus session with the system account.
2. Run the following SQL command to create a View Composer database user with the correct permissions.

   ```sql
   CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE "VCMP"
   ACCOUNT UNLOCK;
   grant connect to VCMPADMIN;
   grant resource to VCMPADMIN;
   grant create view to VCMPADMIN;
   grant create sequence to VCMPADMIN;
   grant create table to VCMPADMIN;
   ```
grant create materialized view to VCMPADMIN;
grant execute on dbms_lock to VCMPADMIN;
grant execute on dbms_job to VCMPADMIN;
grant unlimited tablespace to VCMPADMIN;

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

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

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

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

These instructions assume that you are configuring the ODBC data source on Windows Server 2003 SP2.

**Prerequisites**

Verify that you completed the steps described in “Add a View Composer Database to Oracle 11g or 10g,” on page 30 or “Use a SQL Statement to Add a View Composer Database to an Oracle Instance,” on page 31.

**Procedure**

1. On the vCenter Server computer, select **Start > Administrative Tools > Data Source (ODBC)**.
2. From the Microsoft ODBC Data Source Administrator wizard, select the **System DSN** tab.
3. Click **Add** and select the appropriate Oracle driver from the list.
   
   For example: **OraDb11g_home**
4. Click **Finish**.
5. In the Oracle ODBC Driver Configuration dialog box, type a DSN to use with View Composer, a description of the data source, and a user ID to connect to the database.
   
   If you configured an Oracle database user ID with specific security permissions, specify this user ID.

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

6. Specify a **TNS Service Name** by selecting the Global Database Name from the drop-down menu.
   
   The Oracle Database Configuration Assistant specifies the Global Database Name.

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

**What to do next**

Install the new View Composer service on the vCenter Server computer. See “Install the View Composer Service,” on page 32.

**Install the View Composer Service**

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

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

**Prerequisites**

- Verify that your installation satisfies the View Composer requirements described in “View Composer Requirements,” on page 9.
- Verify that you have a license to install and use View Composer.
- In vCenter Server, create a resource pool on the ESX host or cluster on which you want to store linked-clone desktops.
- If Windows firewall is running on the computer on which View Composer is installed, make sure that the port the View Composer service uses to communicate with View Connection Server is accessible. You can add this port to the exception list or deactivate the local firewall service. You specify this port when you install the View Composer service.
- If Windows firewall is running on the computer on which View Composer is installed, make sure that the VMware Universal File Access (UFA) service is not blocked. You can add the UFA service to the exception list or deactivate the local firewall service.
- Verify that you have the DSN, domain administrator user name, and password that you provided in the ODBC Data Source Administrator wizard. You enter this information when you install the View Composer service.

**Procedure**


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

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

   On Windows Server 2008 computers, you might have to right-click the installer file and select Run As Administrator.

3. Accept the VMware license terms.

4. Accept or change the destination folder.

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

   For example: **VMware View Composer**

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

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

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

7. Type a port number or accept the default value.

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

8. Provide an SSL certificate.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create default SSL certificate</strong></td>
<td>Click this radio button to create a default SSL certificate for the View Composer service.</td>
</tr>
<tr>
<td><strong>Use an existing SSL certificate</strong></td>
<td>Click this radio button if you have an SSL certificate you want to use for the View Composer service. Select an SSL certificate from the list.</td>
</tr>
</tbody>
</table>

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

   The VMware View Composer service starts on the vCenter Server computer.
Configuring Your Infrastructure for View Composer

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

Configuring the vSphere Environment for View Composer

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

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

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

  If you change this information in vCenter Server, View Manager cannot successfully look up the virtual machines in vCenter Server.

- Make sure that the vSwitch settings on the ESX host are configured with enough ports to support the total number of virtual NICs that are configured on the linked-clone virtual machines that run on the ESX host.

- When you deploy linked-clone desktops in a resource pool, make sure that your vSphere environment has enough CPU and memory to host the number of desktops that you require. Use vSphere Client to monitor CPU and memory usage in resource pools.

- Use vSphere DRS. DRS efficiently distributes linked-clone virtual machines among your hosts.

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

Additional Best Practices for View Composer

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

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

If you stagger the run times for your antivirus software, performance of the linked-clone desktops is not affected. If the antivirus software runs in all linked clones at the same time, excessive I/O operations per second (IOPS) occur in your storage subsystem. This excessive activity can affect performance of the linked-clone desktops.
To use View Connection Server, you install the software on supported computers, configure the required components, and, optionally, optimize the components.

This chapter includes the following topics:

- “Installing the View Connection Server Software,” on page 35
- “Configuring User Accounts for vCenter Server and View Composer,” on page 49
- “Configuring View Connection Server for the First Time,” on page 52
- “Configuring View Client Connections,” on page 56
- “Sizing Windows Server Settings to Support Your Deployment,” on page 59

**Installing the View Connection Server Software**

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

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

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

**Installation Prerequisites for View Connection Server**

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

View Connection Server requires a valid license key for View Manager. The following license keys are available:

- View Manager
- View Manager with View Composer and Local Mode

You must join the View Connection Server host to an Active Directory domain. View Connection Server supports the following versions of Active Directory:

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

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

Note View Connection Server does not make, nor does it require, any schema or configuration updates to Active Directory.

Do not install View Connection Server on systems that have the Windows Terminal Server role installed. You must remove the Windows Terminal Server role from any system on which you install View Connection Server.

Do not install View Connection Server on a system that performs any other functions or roles. For example, do not use the same system to host vCenter Server.

The system on which you install View Connection Server must have a static IP address.

To run the View Connection Server installer, you must use a domain user account with Administrator privileges on the system.

Install View Connection Server with a New Configuration

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

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

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

Prerequisites

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install View Connection Server.
- Verify that your installation satisfies the requirements described in “View Connection Server Requirements,” on page 7.
- Prepare your environment for the installation. See “Installation Prerequisites for View Connection Server,” on page 35.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See “Firewall Rules for View Connection Server,” on page 39.

Procedure


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

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

3. Accept the VMware license terms.

4. Accept or change the destination folder.

5. Select the View Standard Server installation option.

6. Accept the Microsoft Software Supplemental License Agreement for Microsoft Active Directory Application Mode (ADAM).
If you install View Connection Server on Windows Server 2008, choose how to configure the Windows Firewall service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Windows Firewall automatically</td>
<td>Let the installer configure Windows Firewall to allow the required network connections.</td>
</tr>
<tr>
<td>Do not configure Windows Firewall</td>
<td>Configure the Windows firewall rules manually.</td>
</tr>
</tbody>
</table>

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

Complete the installation wizard to finish installing View Connection Server.

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

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

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

**What to do next**

Perform initial configuration on View Connection Server.

Configure SSL server certificates for View Connection Server. See “Configuring SSL Certificates for View Connection Server and Security Server,” on page 76.

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

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

**Install View Connection Server Silently**

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

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

**Prerequisites**

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install View Connection Server.

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

- Prepare your environment for the installation. See “Installation Prerequisites for View Connection Server,” on page 35.
- Verify that the Windows computer on which you install View Connection Server has version 2.0 or later of the MSI runtime engine. For details, see the Microsoft Web site.

- Familiarize yourself with the MSI installer command-line options. See “Microsoft Windows Installer Command-Line Options,” on page 47.

- Familiarize yourself with the silent installation properties available with a standard installation of View Connection Server. See “Silent Installation Properties for a View Connection Server Standard Installation,” on page 38.

**Procedure**


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

2. Open a command prompt on the Windows Server computer.

3. Type the installation command on one line.

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

   The VMware View services are installed on the Windows Server computer. For details, see “Install View Connection Server with a New Configuration,” on page 36.

**Silent Installation Properties for a View Connection Server Standard Installation**

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

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The path and folder in which the View Connection Server software is installed.</td>
<td><code>%ProgramFiles%\VMware\VMware View\Server</code></td>
</tr>
<tr>
<td></td>
<td>For example: <code>INSTALLDIR=&quot;D:abc\my folder&quot;</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path.</td>
<td></td>
</tr>
<tr>
<td>VDM_SERVER_INSTANCE_TYPE</td>
<td>The type of View server installation:</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1. Standard installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Replica installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Security server installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. View Transfer Server installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For example, to perform a standard installation, define <code>VDM_SERVER_INSTANCE_TYPE=1</code></td>
<td></td>
</tr>
<tr>
<td>FWCHOICE</td>
<td>The MSI property that determines whether to configure a firewall for the View Connection Server instance.</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>A value of 1 configures a firewall. A value of 2 does not configure a firewall.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For example: <code>FWCHOICE=1</code></td>
<td></td>
</tr>
</tbody>
</table>
Firewall Rules for View Connection Server

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

When you install View Connection Server on Windows Server 2008, the installation program can optionally configure the required Windows firewall rules for you. When you install View Connection Server on Windows Server 2003 R2, you must configure the required Windows firewall rules manually.

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Ports</th>
<th>View Connection Server Instance Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>JMS</td>
<td>TCP 4001 in</td>
<td>Standard and replica</td>
</tr>
<tr>
<td>JMSIR</td>
<td>TCP 4100 in</td>
<td>Standard and replica</td>
</tr>
<tr>
<td>AJP13</td>
<td>TCP 8009 in</td>
<td>Standard and replica</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP 80 in</td>
<td>Standard, replica, and security server</td>
</tr>
<tr>
<td>HTTPS</td>
<td>TCP 443 in</td>
<td>Standard, replica, and security server</td>
</tr>
<tr>
<td>PcoIP</td>
<td>TCP 4172 in;</td>
<td>Standard, replica, and security server</td>
</tr>
<tr>
<td></td>
<td>UDP 4172 both directions</td>
<td></td>
</tr>
</tbody>
</table>

Install a Replicated Instance of View Connection Server

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

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

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

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

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

Prerequisites

- Verify that at least one View Connection Server instance is installed and configured on the network.
- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you plan to install the replicated instance.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have View Administrator privileges on the Windows Server computer where the existing instance is installed.
- Verify that your installation satisfies the requirements described in “View Connection Server Requirements,” on page 7.
- Verify that the computers on which you install replicated View Connection Server instances are connected over a high-performance LAN. See “Network Requirements for Replicated View Connection Server Instances,” on page 9.
Prepare your environment for the installation. See “Installation Prerequisites for View Connection Server,” on page 35.

Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See “Firewall Rules for View Connection Server,” on page 39.

Procedure

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

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

3. Accept the VMware license terms.

4. Accept or change the destination folder.

5. Select the View Replica Server installation option.

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

7. Accept the Microsoft Software Supplemental License Agreement for Microsoft Active Directory Application Mode (ADAM).

8. If you install View Connection Server on Windows Server 2008, choose how to configure the Windows Firewall service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Windows Firewall</td>
<td>Let the installer configure Windows Firewall to allow the required network connections.</td>
</tr>
<tr>
<td>automatically</td>
<td></td>
</tr>
<tr>
<td>Do not configure Windows Firewall</td>
<td>Configure the Windows firewall rules manually.</td>
</tr>
</tbody>
</table>

   If you install View Connection Server on Windows Server 2003 R2, you must configure the required Windows firewall rules manually.

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

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

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

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

What to do next

You do not have to perform initial configuration on a replicated instance of View Connection Server. The replicated instance inherits its configuration from the existing View Connection Server instance.
Configure SSL server certificates for View Connection Server. See “Configuring SSL Certificates for View Connection Server and Security Server,” on page 76.

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

**Install a Replicated Instance of View Connection Server Silently**

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

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

**Prerequisites**

- Verify that at least one View Connection Server instance is installed and configured on the network.
- To install the replicated instance, you must log in as a user with credentials to access the View Administrators account. You specify the View Administrators account when you install the first instance of View Connection Server. The account can be the local Administrators group or a domain user or group account. See “Install View Connection Server with a New Configuration,” on page 36.
- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you plan to install the replicated instance.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have View Administrator privileges on the Windows Server computer where the existing instance is installed.
- Verify that your installation satisfies the requirements described in “View Connection Server Requirements,” on page 7.
- Verify that the computers on which you install replicated View Connection Server instances are connected over a high-performance LAN. See “Network Requirements for Replicated View Connection Server Instances,” on page 9.
- Prepare your environment for the installation. See “Installation Prerequisites for View Connection Server,” on page 35.
- Familiarize yourself with the MSI installer command-line options. See “Microsoft Windows Installer Command-Line Options,” on page 47.
- Familiarize yourself with the silent installation properties available with a replica installation of View Connection Server. See “Silent Installation Properties for a Replicated Instance of View Connection Server,” on page 42.

**Procedure**


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

2. Open a command prompt on the Windows Server computer.

3. Type the installation command on one line.

   For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com"`
The VMware View services are installed on the Windows Server computer. For details, see “Install a Replicated Instance of View Connection Server,” on page 39.

**Silent Installation Properties for a Replicated Instance of View Connection Server**

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

**Table 5-3. MSI Properties for Silently installing a Replicated Instance of View Connection Server**

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The path and folder in which the View Connection Server software is installed.</td>
<td>%ProgramFiles%\VMware\VMware View\Server</td>
</tr>
<tr>
<td>ADAM_PRIMARY_NAME</td>
<td>The host name or IP address of the existing View Connection Server instance you are replicating.</td>
<td>None</td>
</tr>
<tr>
<td>ADAM_PRIMARY_PORT</td>
<td>The View LDAP port of the existing View Connection Server instance you are replicating.</td>
<td>None</td>
</tr>
<tr>
<td>FWCHOICE</td>
<td>The MSI property that determines whether to configure a firewall for the View Connection Server instance.</td>
<td>1</td>
</tr>
</tbody>
</table>

**Configure a Security Server Pairing Password**

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

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

**Procedure**

1. In View Administrator, select **View Configuration > Servers**.
2. In the View Servers pane, select the View Connection Server instance to pair with the security server.
3. From the **More Commands** drop-down menu, select **Specify Security Server Pairing Password**.
4 Type the password in the Pairing password and Confirm password text boxes and specify a password timeout value.

You must use the password within the specified timeout period.

5 Click OK to configure the password.

What to do next

Install a security server. See “Install a Security Server,” on page 43.

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

Install a Security Server

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

Prerequisites

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

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

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

- Prepare your environment for the installation. See “Installation Prerequisites for View Connection Server,” on page 35.

- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running View Connection Server 4.6 or later. You cannot pair a View 4.6 or later security server with an older version of View Connection Server.

- Verify that the View Connection Server instance to be paired with the security server is accessible to the computer on which you plan to install the security server.

- Configure a security server pairing password. See “Configure a Security Server Pairing Password,” on page 42.

- Familiarize yourself with the format of external URLs. See “Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections,” on page 57.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for a security server. See “Firewall Rules for View Connection Server,” on page 39.

Procedure


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

2 To start the View Connection Server installation program, double-click the installer file.
3 Accept the VMware license terms.

4 Accept or change the destination folder.

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

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

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

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

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

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

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

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

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

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

   For example: 100.200.300.400:4172

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

10 If you install the security server on Windows Server 2008, choose how to configure the Windows Firewall service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Windows Firewall automatically</strong></td>
<td>Let the installer configure Windows Firewall to allow the required network connections.</td>
</tr>
<tr>
<td><strong>Do not configure Windows Firewall</strong></td>
<td>Configure the Windows firewall rules manually.</td>
</tr>
</tbody>
</table>

   If you install the security server on Windows Server 2003 R2, you must configure the required Windows firewall rules manually.

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

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

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

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

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

**What to do next**

Configure SSL server certificates for the security server. See “Configuring SSL Certificates for View Connection Server and Security Server,” on page 76.
If you are reinstalling the security server on a Windows Server 2008 operating system and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

**Install a Security Server Silently**

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

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

**Prerequisites**

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

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

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

- Prepare your environment for the installation. See “Installation Prerequisites for View Connection Server,” on page 35.

- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running View Connection Server 4.6 or later. You cannot pair a View 4.6 or later security server with an older version of View Connection Server.

- Verify that the View Connection Server instance to be paired with the security server is accessible to the computer on which you plan to install the security server.

- Configure a security server pairing password. See “Configure a Security Server Pairing Password,” on page 42.

- Familiarize yourself with the format of external URLs. See “Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections,” on page 57.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for a security server. See “Firewall Rules for View Connection Server,” on page 39.

- Familiarize yourself with the MSI installer command-line options. See “Microsoft Windows Installer Command-Line Options,” on page 47.

- Familiarize yourself with the silent installation properties available with a security server. See “Silent Installation Properties for a Security Server,” on page 46.

**Procedure**


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

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


The VMware View services are installed on the Windows Server computer. For details, see “Install a Security Server,” on page 43.

### Silent Installation Properties for a Security Server

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

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The path and folder in which the View Connection Server software is installed. For example: <code>INSTALLDIR=&quot;D:\abc\my folder&quot;</code></td>
<td><code>%ProgramFiles%\VMware\VMware View\Server</code></td>
</tr>
<tr>
<td>VDM_SERVER_INSTANCE_TYPE</td>
<td>The type of View server installation:</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1. Standard installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Replica installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Security server installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. View Transfer Server installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To install a security server, define <code>VDM_SERVER_INSTANCE_TYPE=3</code></td>
<td>This MSI property is required when installing a security server.</td>
</tr>
<tr>
<td>VDM_SERVER_NAME</td>
<td>The host name or IP address of the existing View Connection Server instance to pair with the security server. For example: <code>VDM_SERVER_NAME=cs1.internaldomain.com</code></td>
<td>None</td>
</tr>
<tr>
<td>VDM_SERVER_SS_EXTURL</td>
<td>The external URL of the security server. The URL must contain the protocol, externally resolvable security server name, and port number For example: <code>VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443</code></td>
<td>None</td>
</tr>
<tr>
<td>VDM_SERVER_SS_PWD</td>
<td>The security server pairing password. For example: <code>VDM_SERVER_SS_PWD=secret</code></td>
<td>None</td>
</tr>
<tr>
<td>FWCHOICE</td>
<td>The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: <code>FWCHOICE=1</code></td>
<td>1</td>
</tr>
<tr>
<td>VDM_SERVER_SS_PCOIP_IP_ADDR</td>
<td>The PCoIP Secure Gateway external IP address. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: <code>VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40</code></td>
<td>None</td>
</tr>
</tbody>
</table>
Table 5-4. MSI Properties for Silently Installing a Security Server (Continued)

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDM_SERVER_SS_PCOIP_TCPPORT</td>
<td>The PCoIP Secure Gateway external TCP port number. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: VDM_SERVER_SS_PCOIP_TCPPORT=4172 This property is required if you plan to use the PCoIP Secure Gateway component.</td>
<td>None</td>
</tr>
<tr>
<td>VDM_SERVER_SS_PCOIP_UDPPORT</td>
<td>The PCoIP Secure Gateway external UDP port number. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: VDM_SERVER_SS_PCOIP_UDPPORT=4172 This property is required if you plan to use the PCoIP Secure Gateway component.</td>
<td>None</td>
</tr>
</tbody>
</table>

Microsoft Windows Installer Command-Line Options

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

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

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

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

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

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

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

Table 5-6 shows the command-line options and MSI property values that are passed to the MSI installer.
### Table 5-6. MSI Command-Line Options and MSI Properties

<table>
<thead>
<tr>
<th>MSI Option or Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/qn</td>
<td>Instructs the MSI installer not to display the installer wizard pages. For example, you might want to install View Agent silently and use only default setup options and features: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn&quot;</code> In the examples, <code>xxxxxx</code> is the build number and <code>y.y.y</code> is the version number. Alternatively, you can use the /qb option to display the wizard pages in a noninteractive, automated installation. As the installation proceeds, the wizard pages are displayed, but you cannot respond to them. The /qn or /qb option is required to run a silent installation.</td>
</tr>
<tr>
<td>INSTALLDIR</td>
<td>Specifies an alternative installation path for the View component. Use the format <code>INSTALLDIR=path</code> to specify an installation path. You can ignore this MSI property if you want to install the View component in the default path. This MSI property is optional.</td>
</tr>
<tr>
<td>ADDLOCAL</td>
<td>Determines the component-specific features to install. In an interactive installation, the View installer displays custom setup options to select. The MSI property, ADDLOCAL, lets you specify these setup options on the command line. To install all available custom setup options, enter <code>ADDLOCAL=ALL</code>. For example: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn ADDLOCAL=ALL&quot;</code> If you do not use the MSI property, ADDLOCAL, the default setup options are installed. To specify individual setup options, enter a comma-separated list of setup option names. Do not use spaces between names. Use the format <code>ADDLOCAL=value,value,value,...</code>. For example, you might want to install View Agent in a guest operating system with the View Composer Agent and PCoIP features: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn ADDLOCAL=Core,SVIAgent,PCoIP&quot;</code> Note: The Core feature is required in View Agent. This MSI property is optional.</td>
</tr>
<tr>
<td>REBOOT</td>
<td>You can use the REBOOT=ReallySuppress option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.</td>
</tr>
<tr>
<td>/l*v log_file</td>
<td>Writes logging information into the specified log file with verbose output. For example: <code>/l*v &quot;%TEMP%\vmmsi.log&quot;</code> This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The /l*v option is optional.</td>
</tr>
</tbody>
</table>

### Uninstalling View Products Silently by Using MSI Command-Line Options

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

**Syntax**

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

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

The /x option uninstalls the View component.

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

For information about MSI command-line options, see “Microsoft Windows Installer Command-Line Options,” on page 47.

Examples

Uninstall a View Connection Server instance.

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

Configuring User Accounts for vCenter Server and View Composer

To use vCenter Server with View Manager, you must configure a user account with permission to perform operations in vCenter Server. To use View Composer, you must give this vCenter Server user additional privileges. To manage desktops that are used in local mode, you must give this user privileges in addition to those that are required for View Manager and View Composer.

You also must create a domain user for View Composer in Active Directory. See “Create a User Account for View Composer,” on page 23.

Where to Use the vCenter Server User and Domain User for View Composer

After you create and configure these two user accounts, you specify the user names in View Administrator.

- You specify a vCenter Server user when you add vCenter Server to View Manager.
- You specify a domain user for View Composer when you configure View Composer for vCenter Server.
- You specify the domain user for View Composer when you create linked-clone pools.

Configure a vCenter Server User for View Manager, View Composer, and Local Mode

To configure a user account that gives View Manager permission to operate in vCenter Server, you must assign a role with appropriate privileges to that user. To use the View Composer service in vCenter Server, you must give the user account additional privileges. To manage desktops that are used in local mode, you must give the user account privileges that include View Manager, View Composer, and local mode privileges.

To support View Composer, you also must make this user a local system administrator on the vCenter Server computer.

Prerequisites

- In Active Directory, create a user in the View Connection Server domain or a trusted domain. See “Creating a User Account for vCenter Server,” on page 22.
- Familiarize yourself with the privileges that are required for the user account. See “View Manager Privileges Required for the vCenter Server User,” on page 51.
- If you use View Composer, familiarize yourself with the additional required privileges. See “View Composer Privileges Required for the vCenter Server User,” on page 51.
If you manage local desktops, familiarize yourself with the additional required privileges. See “Local Mode Privileges Required for the vCenter Server User,” on page 52.

**Procedure**

1. In vCenter Server, prepare a role with the required privileges for the user.
   - You can use the predefined Administrator role in vCenter Server. This role can perform all operations in vCenter Server.
   - If you use View Composer, you can create a limited role with the minimum privileges needed by View Manager and View Composer to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **View Composer Administrator**, and select privileges for the role.

     This role must have all the privileges that both View Manager and View Composer need to operate in vCenter Server.

   - If you manage local desktops, you can create a limited role with the minimum privileges needed by View Manager, View Composer, and the local mode feature to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **Local Mode Administrator**, and select privileges for the role.

     This role must have all the privileges that View Manager, View Composer, and the local mode feature need to operate in vCenter Server.

   - If you use View Manager without View Composer and do not manage local desktops, you can create an even more limited role with the minimum privileges needed by View Manager to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **View Manager Administrator**, and select privileges for the role.

2. In vSphere Client, right-click the vCenter Server at the top level of the inventory, click **Add Permission**, and add the vCenter Server user.

   **NOTE** You must define the vCenter Server user at the vCenter Server level.

3. From the drop-down menu, select the Administrator role, or the View Composer or View Manager role that you created, and assign it to the vCenter Server user.

4. If you use View Composer, on the vCenter Server computer, add the vCenter Server user account as a member of the local system Administrators group.

   View Composer requires that the vCenter Server user is a system administrator on the vCenter Server computer.

**What to do next**

In View Administrator, when you add vCenter Server to View Manager, specify the vCenter Server user. See “Add vCenter Server Instances to View Manager,” on page 53.
View Manager Privileges Required for the vCenter Server User

The vCenter Server user must have sufficient privileges to enable View Manager to operate in vCenter Server. Create a View Manager role for the vCenter Server user with the required privileges.

Table 5-7. View Manager Privileges

<table>
<thead>
<tr>
<th>Privilege Group</th>
<th>Privileges to Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Create Folder</td>
</tr>
<tr>
<td></td>
<td>Delete Folder</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>In Configuration:</td>
</tr>
<tr>
<td></td>
<td>■ Add or remove device</td>
</tr>
<tr>
<td></td>
<td>■ Advanced</td>
</tr>
<tr>
<td></td>
<td>■ Modify device settings</td>
</tr>
<tr>
<td></td>
<td>In Interaction:</td>
</tr>
<tr>
<td></td>
<td>■ Power Off</td>
</tr>
<tr>
<td></td>
<td>■ Power On</td>
</tr>
<tr>
<td></td>
<td>■ Reset</td>
</tr>
<tr>
<td></td>
<td>■ Suspend</td>
</tr>
<tr>
<td></td>
<td>In Inventory:</td>
</tr>
<tr>
<td></td>
<td>■ Create new</td>
</tr>
<tr>
<td></td>
<td>■ Remove</td>
</tr>
<tr>
<td></td>
<td>In Provisioning:</td>
</tr>
<tr>
<td></td>
<td>■ Customize</td>
</tr>
<tr>
<td></td>
<td>■ Deploy template</td>
</tr>
<tr>
<td></td>
<td>■ Read customization specifications</td>
</tr>
<tr>
<td>Resource</td>
<td>Assign virtual machine to resource pool</td>
</tr>
</tbody>
</table>

View Composer Privileges Required for the vCenter Server User

To support View Composer, the vCenter Server user must have privileges in addition to those required to support View Manager. Create a View Composer role for the vCenter Server user with the View Manager privileges and these additional privileges.

Table 5-8. View Composer Privileges

<table>
<thead>
<tr>
<th>Privilege Group</th>
<th>Privileges to Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore</td>
<td>Allocate space</td>
</tr>
<tr>
<td></td>
<td>Browse datastore</td>
</tr>
<tr>
<td></td>
<td>Low level file operations</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>Inventory (all)</td>
</tr>
<tr>
<td></td>
<td>Configuration (all)</td>
</tr>
<tr>
<td></td>
<td>State (all)</td>
</tr>
<tr>
<td></td>
<td>In Provisioning:</td>
</tr>
<tr>
<td></td>
<td>■ Clone virtual machine</td>
</tr>
<tr>
<td></td>
<td>■ Allow disk access</td>
</tr>
<tr>
<td>Resource</td>
<td>Assign virtual machine to resource pool</td>
</tr>
<tr>
<td>Global</td>
<td>Enable methods</td>
</tr>
<tr>
<td></td>
<td>Disable methods</td>
</tr>
<tr>
<td></td>
<td>System tag</td>
</tr>
<tr>
<td>Network</td>
<td>(all)</td>
</tr>
</tbody>
</table>
Local Mode Privileges Required for the vCenter Server User

To manage desktops that are used in local mode, the vCenter Server user must have privileges in addition to those required to support View Manager and View Composer. Create a Local Mode Administrator role for the vCenter Server user that combines the View Manager privileges, View Composer privileges, and local mode privileges.

<table>
<thead>
<tr>
<th>Privilege Group</th>
<th>Privileges to Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Set custom attribute</td>
</tr>
<tr>
<td>Host</td>
<td>In Configuration:</td>
</tr>
<tr>
<td></td>
<td>System management</td>
</tr>
</tbody>
</table>

Configuring View Connection Server for the First Time

After you install View Connection Server, you must install a product license, add vCenter Servers and View Composer services to View Manager, add security servers if you use them, and set external URLs for client desktops that run outside your network.

View Administrator and View Connection Server

View Administrator provides a management interface for View Manager.

Depending on your View deployment, you use one or more View Administrator interfaces.

- Use one View Administrator interface to manage the View components that are associated with a single, standalone View Connection Server instance or a group of replicated View Connection Server instances.
- You can use the IP address of any replicated instance to log in to View Administrator.
- You must use a separate View Administrator interface to manage the View components for each single, standalone View Connection Server instance and each group of replicated View Connection Server instances.

You also use View Administrator to manage security servers and View Transfer Server instances associated with View Connection Server.

- Each security server is associated with one View Connection Server instance.
- Each View Transfer Server instance can communicate with any View Connection Server instance in a group of replicated instances.

Log In to View Administrator

To perform initial configuration tasks, you must log in to View Administrator.

Prerequisites

Verify that you are using a Web browser supported by View Administrator. See “View Administrator Requirements,” on page 9.
Procedure

1. Open your Web browser and enter the following URL, where `server` is the host name or IP address of the View Connection Server instance.

   `https://server/admin`

   You access View Administrator by using a secure (SSL) connection. When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. This response is expected behavior because the default certificate supplied with View Connection Server is self-signed.

2. Click **Ignore** to continue using the current SSL certificate.

3. Log in using administrator credentials on the View Connection Server computer.

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

   After you log in to View Administrator, you can use **View Configuration > Administrators** to change the list of users and groups that have the View Administrators role.

**Install the View Connection Server License Key**

Before you can use View Connection Server, you must enter the product license key.

The first time you log in, View Administrator displays the Product Licensing and Usage page.

After you install the license key, View Administrator displays the dashboard page when you log in.

You do not have to configure a license key when you install a replicated View Connection Server instance or a security server. Replicated instances and security servers use the common license key stored in the View LDAP configuration.

**Note** View Connection Server requires a valid license key for View 5.0. As of the release of VMware View 4.0, the VMware View license key is a 25-character key.

Procedure

1. If the View Configuration view is not displayed, click **View Configuration** in the left navigation pane.

2. Click **Product Licensing and Usage**.

3. On the Product Licensing table, click **Edit License** and enter the View Manager license serial number.

4. Click **OK**.

5. Verify the license expiration date.

**Add vCenter Server Instances to View Manager**

You must configure View Manager to connect to the vCenter Server instances in your View deployment. vCenter Server creates and manages the virtual machines that View Manager uses as desktop sources.

If you run vCenter Server instances in a Linked Mode group, you must add each vCenter Server instance to View Manager separately.

**Prerequisites**

- Install the View Connection Server product license key.
- Prepare a vCenter Server user with permission to perform the operations in vCenter Server that are necessary to support View Manager. To use View Composer, you must give the user additional privileges. To manage desktops that are used in local mode, you must give the user privileges in addition to those that are required for View Manager and View Composer.
If you plan to have View Connection Server connect to the vCenter Server instance using a secure channel (SSL), install a server SSL certificate on the vCenter Server host.

**Procedure**

1. In View Administrator, click **View Configuration > Servers**.
2. In the vCenter Servers panel, click **Add**.
3. In the server address text box, type the fully qualified domain name (FQDN) or IP address of the vCenter Server instance.
   
   The FQDN includes the host name and domain name. For example, in the FQDN `myserverhost.companydomain.com`, `myserverhost` is the host name and `companydomain.com` is the domain.

   **Note**: If you enter a server by using a DNS name or URL, View Manager does not perform a DNS lookup to verify whether an administrator previously added this server to View Manager by using its IP address. A conflict arises if you add a vCenter Server with both its DNS name and its IP address.

4. Type the name of the vCenter Server user.
5. Type the vCenter Server user password.
6. (Optional) Type a description for this vCenter Server instance.
7. To connect to the vCenter Server instance using a secure channel (SSL), make sure that **Connect using SSL** is selected. SSL connection is the default setting.
8. Type the TCP port number.
   
   The default port is 443.
9. (Optional) Click **Advanced** to configure the maximum concurrent pool operations in vCenter Server.
   
   a. Set the maximum number of concurrent provisioning operations.
   
   This setting determines the largest number of concurrent requests that View Manager can make to provision full virtual machines in this vCenter Server instance. The default value is eight. This setting does not control linked-clone provisioning.
   
   b. Set the maximum number of concurrent power operations.
   
   This setting determines the largest number of power operations (startup, shutdown, suspend, and so on) that can take place simultaneously on virtual machines managed by View Manager in this vCenter Server instance. The default value is five. This setting controls power operations for full virtual machines and linked clones.
10. Choose whether to configure View Composer.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>You are not using View Composer</td>
<td>Click OK.</td>
</tr>
<tr>
<td>You are using View Composer</td>
<td>Configure the View Composer settings.</td>
</tr>
</tbody>
</table>

**What to do next**

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

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

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

**Prerequisites**

- Your Active Directory administrator must create a domain user with permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. To manage the linked-clone machine accounts in Active Directory, the domain user must have **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions.

  See “Create a User Account for View Composer,” on page 23.

- You must configure View Manager to connect to vCenter Server. See “Add vCenter Server Instances to View Manager,” on page 53.

**Procedure**

1. In View Administrator, open the Edit vCenter Server dialog box.
   a. Click **View Configuration > Servers**.
   b. In the vCenter Servers panel, select the vCenter Server entry.
   c. Click **Edit**.

2. Select **Enable View Composer** and make sure that the port number is the same as the port that you specified when you installed the View Composer service on vCenter Server.

   View Manager verifies that the View Composer service is running on vCenter Server.

3. Click **Add** to add the domain user for View Composer account information.
   a. Type the domain name of the Active Directory domain.
      For example: `domain.com`
   b. Type the domain user name, including the domain name.
      For example: `domain.com\admin`
   c. Type the account password.
   d. Click **OK**.
   e. To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.

4. Click **OK** to close the Edit vCenter Server dialog box.

**What to do next**

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

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

The initial View Client connection, which is used for user authentication and View desktop selection, is created over HTTPS when a user provides a domain name or IP address to View Client. If firewall and load balancing software are configured correctly in your network environment, this request reaches the View Connection Server or security server host. With this connection, users are authenticated and a desktop is selected, but users have not yet connected to View desktops.

When users connect to View desktops, by default View Client makes a second connection to the View Connection Server or security server host. This connection is called the tunnel connection because it provides a secure tunnel for carrying RDP and other data over HTTPS.

When users connect to View desktops with the PCoIP display protocol, View Client can make a further connection to the PCoIP Secure Gateway on the View Connection Server or security server host. The PCoIP Secure Gateway ensures that only authenticated users can communicate with View desktops over PCoIP.

When the secure tunnel or PCoIP Secure Gateway is disabled, View desktop sessions are established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server or security server host. This type of connection is called a direct connection.

Typically, to provide secure connections for external clients that connect to a security server or View Connection Server host over a WAN, you enable both the secure tunnel and the PCoIP Secure Gateway. You can disable the secure tunnel and the PCoIP Secure Gateway to allow internal, LAN-connected clients to establish direct connections to View desktops.

Certain View Client endpoints, such as thin clients, do not support the tunnel connection and use direct connections for RDP data, but do support the PCoIP Secure Gateway for PCoIP data.

SSL for client connections is enabled by default. You can disable SSL so that initial and tunnel connections take place over HTTP, not HTTPS. Disabling SSL might be acceptable for internal, LAN-connected clients where communications are protected by a firewall. See “Configure SSL for Client Connections,” on page 82.

Configure the PCoIP Secure Gateway and Secure Tunnel Connections

You use View Administrator to configure the use of the secure tunnel and PCoIP Secure Gateway. These components ensure that only authenticated users can communicate with View desktops.

Clients that use the PCoIP display protocol can use the PCoIP Secure Gateway. Clients that use the RDP display protocol can use the secure tunnel.

**IMPORTANT** A typical network configuration that provides secure connections for external clients includes a security server. To enable or disable the secure tunnel and PCoIP Secure Gateway on a security server, you must edit the View Connection Server instance that is paired with the security server.

In a network configuration in which external clients connect directly to a View Connection Server host, you enable or disable the secure tunnel and PCoIP Secure Gateway by editing that View Connection Server instance in View Administrator.

**Prerequisites**

- If you intend to enable the PCoIP Secure Gateway, verify that the View Connection Server instance and paired security server are View 4.6 or later.
- If you pair a security server to a View Connection Server instance on which you already enabled the PCoIP Secure Gateway, verify that the security server is View 4.6 or later.

**Procedure**

1. In View Administrator, select **View Configuration > Servers**.
2 In the View Connection Servers panel, select a View Connection Server instance and click Edit.

3 Configure use of the secure tunnel.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable the secure tunnel</td>
<td>Deselect Use secure tunnel connection to desktop.</td>
</tr>
<tr>
<td>Enable the secure tunnel</td>
<td>Select Use secure tunnel connection to desktop.</td>
</tr>
</tbody>
</table>

The secure tunnel is enabled by default.

4 Configure use of the PCoIP Secure Gateway.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the PCoIP Secure Gateway</td>
<td>Select Use PCoIP Secure Gateway for PCoIP connections to desktop</td>
</tr>
<tr>
<td>Disable the PCoIP Secure Gateway</td>
<td>Deselect Use PCoIP Secure Gateway for PCoIP connections to desktop</td>
</tr>
</tbody>
</table>

The PCoIP Secure Gateway is disabled by default.

5 Click OK to save your changes.

### Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections

To use the secure tunnel, a client system must have access to an IP address, or a fully qualified domain name (FQDN) that it can resolve to an IP address, that allows the client to reach a View Connection Server or security server host. To use the PCoIP Secure Gateway, a client system must have access to an IP address that allows the client to reach a View Connection Server or security server host.

### Using Tunnel Connections From External Locations

By default, a View Connection Server or security server host can be contacted only by tunnel clients that reside within the same network and are therefore able to locate the requested host.

Many organizations require that users can connect from an external location by using a specific IP address or client-resolvable domain name, and a specific port. This information might or might not resemble the actual address and port number of the View Connection Server or security server host. The information is provided to a client system in the form of a URL. For example:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://100.200.300.400:443`

To use addresses like these in View Manager, you must configure the View Connection Server or security server host to return an external URL instead of the host's FQDN.

### Configuring External URLs

You configure two external URLs. One URL allows client systems to make tunnel connections. The other allows client systems that use PCoIP to make secure connections through the PCoIP Secure Gateway. You must specify the PCoIP external URL as an IP address, which allows client systems to connect from an external location.

If your network configuration includes security servers, provide external URLs for the security servers. External URLs are not required on the View Connection Server instances that are paired with the security servers.
The process of configuring the external URLs is different for View Connection Server instances and security servers.

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

Set the External URLs for a View Connection Server Instance

You use View Administrator to configure the external URLs for a View Connection Server instance.

Both the secure tunnel external URL and PCoIP external URL must be the addresses that client systems use to reach this View Connection Server instance. For example, do not specify the secure tunnel external URL for this instance and the PCoIP external URL for a paired security server.

**Procedure**

1. In View Administrator, click **View Configuration > Servers**.
2. In the View Connection Servers panel, select a View Connection Server instance and click **Edit**.
3. Type the secure tunnel external URL in the **External URL** text box.
   The URL must contain the protocol, client-resolvable host name or IP address, and port number.
   For example: `https://view.example.com:443`
4. Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.
   Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.
   For example: `100.200.300.400:4172`
   The URL must contain the IP address and port number that a client system can use to reach this View Connection Server host. You can type into the text box only if a PCoIP Secure Gateway is installed on the View Connection Server instance.
5. Click **OK**.

Modify the External URLs for a Security Server

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

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

Both the secure tunnel external URL and PCoIP external URL must be the addresses that client systems use to reach this security server. For example, do not specify the secure tunnel external URL for this security server and the PCoIP external URL for a paired View Connection Server instance.

**Prerequisites**

Verify that the version of the security server is View Connection Server 4.6 or later.

**Procedure**

1. In View Administrator, select **View Configuration > Servers**.
2. In the Security Servers panel, select the security server and click **Edit**.
   The **Edit** button is unavailable if the security server is not upgraded to View Connection Server 4.6 or later.
3 Type the Secure Tunnel external URL in the **External URL** text box.

The URL must contain the protocol, client-resolvable security server host name or IP address, and port number.

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

4 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

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

For example: 100.200.300.400:4172

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

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

View Administrator sends the updated external URLs to the security server. You do not need to restart the security server service for the changes to take effect.

---

**Sizing Windows Server Settings to Support Your Deployment**

To support a large deployment of View Manager desktops, you can configure the Windows Server computers on which you install View Connection Server. On each computer, you can size the ephemeral ports, TCB hash table, Java Virtual Machine settings, and Windows page-file. These adjustments ensure that the computers have adequate resources to run correctly with the expected user load.

For hardware and memory requirements for View Connection Server, see “**Hardware Requirements for View Connection Server,**” on page 7.

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

**Ephemeral Ports**

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

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

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

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

**Calculate the Number of Ephemeral Ports**

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

**Procedure**

1. Use the following formula.

   \[ \text{Number of ephemeral ports} = \left( \frac{5 \times \text{clients}}{\text{servers}} \right) + 10 \]
Where

clients  Projected number of concurrent client connections

servers  Number of View Connection Server instances in the replicated group

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

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

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Sample Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projected number of concurrent client connections</td>
<td>3,000</td>
</tr>
<tr>
<td>Number of View Connection Server instances in the replicated group</td>
<td>3</td>
</tr>
</tbody>
</table>

\[
\frac{5 \times \text{clients}}{\text{servers}} + 10 = \text{number of ephemeral ports on each View Connection Server}
\]

\[
\frac{5 \times 3,000}{3} + 10 = 5,010
\]

**What to do next**

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

**Increase the Number of Ephemeral Ports**

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

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

**Prerequisites**

Calculate the number of ephemeral ports to configure on the Windows Server computer. See “Calculate the Number of Ephemeral Ports,” on page 59.

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

**Procedure**

1. On the Windows Server computer, start the Windows Registry Editor.
   a. Select Start > Command Prompt.
   b. At the command prompt, type `regedit`.
2. In the registry, locate the correct subkey and click Parameters.
   
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

3. Click Edit > New and add the registry entry.
   
   Value Name: MaxUserPort
   Value Type: DWORD
   Value Data: 1024 + calculated number of ephemeral ports
   Valid Range: 5000-65534 (decimal)

4. Exit the Windows Registry Editor.
5 Restart the Windows Server computer.

**Increasing the Size of the TCB Hash Table**

The transmission control block (TCB) holds information about TCP connections that are made between View Connection Server clients and their desktop sources. To support a large View desktop deployment on Windows Server 2003 computers, you can increase the size of the TCB hash table.

On Windows Server 2008 computers, you do not need to increase the maximum size of the TCB hash table. Windows Server 2008 fully tunes this value by default.

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

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

By default, Windows Server 2003 configures the number of hash table rows based on the number of CPUs in the Windows Server computer.

<table>
<thead>
<tr>
<th>Number of CPUs</th>
<th>Maximum Number of TCB Hash Table Rows</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>128</td>
</tr>
<tr>
<td>2</td>
<td>512</td>
</tr>
<tr>
<td>4</td>
<td>2,048</td>
</tr>
<tr>
<td>8</td>
<td>8,192</td>
</tr>
</tbody>
</table>

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

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

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

**Procedure**

- Use the following formula.

  \[
  \text{Number of hash table rows on each View Connection Server instance} = \left( \frac{5 \times \text{clients}}{\text{servers}} \right) + \text{desktops} + 20
  \]

  Where

  - `clients`: Projected number of concurrent client connections
  - `servers`: Number of View Connection Server instances in the replicated group
  - `desktops`: Number of View desktop sources in your deployment

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

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

For each View Connection Server instance, the result is 11,020, as shown in Table 5-12.
Table 5-12. Example of Calculating the Size of the TCB Hash Table on Each View Connection Server

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Sample Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projected number of concurrent client desktop connections</td>
<td>3,000</td>
</tr>
<tr>
<td>Number of View Connection Server instances</td>
<td>3</td>
</tr>
<tr>
<td>Number of View desktop sources</td>
<td>6,000</td>
</tr>
</tbody>
</table>

\[
\frac{(5 \times \text{clients})}{\text{servers}} + \text{desks} + 20 = \text{number of TCB hash table rows on each server}
\]

(\(5 \times 3,000\)) \div 3 + 6,000 + 20 = 11,020

What to do next

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

Calculate the Size of the TCB Hash Table for Security Servers

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

Procedure

- Use the following formula.

\[
\text{Number of hash table rows} = \left( \frac{5 \times \text{clients}}{\text{security servers}} \right) + 10
\]

Where

- **clients**: Projected number of concurrent client connections
- **security servers**: Number of security servers

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

For example, you might have 3,000 concurrent client connections and two security servers in your deployment. For each security server, the result is 7,510, as shown in Table 5-13.

Table 5-13. Example of Calculating the Size of the TCB Hash Table on Each Security Server

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>Sample Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projected number of concurrent client desktop connections</td>
<td>3,000</td>
</tr>
<tr>
<td>Number of security servers</td>
<td>2</td>
</tr>
</tbody>
</table>

\[
\frac{(5 \times \text{clients})}{\text{security servers}} + 10 = \text{number of TCB hash table rows on each security server}
\]

(5\times3,000) \div 2 + 10 = 7,510

What to do next

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

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

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

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

1. On the Windows Server computer, start the Windows Registry Editor
   a. Select Start > Command Prompt.
   b. At the command prompt, type `regedit`.

2. In the registry, locate the subkey and click Parameters.
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

3. Click Edit > New and add the following registry entry.
   - Value Name: MaxHashTableSize
   - Value Type: DWORD
   - Value data: calculated hash table size
   - Valid Range: 64–65536 (decimal)

4. Exit the Windows Registry Editor.

5. Restart the Windows Server computer.

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

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

**Table 5-14. Configuration Parameters**

<table>
<thead>
<tr>
<th>Configuration Parameters</th>
<th>Fill in Your Site's Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projected number of concurrent client connections</td>
<td></td>
</tr>
<tr>
<td>Number of View Connection Server instances</td>
<td></td>
</tr>
<tr>
<td>Number of security servers</td>
<td></td>
</tr>
<tr>
<td>Number of View desktop sources</td>
<td></td>
</tr>
</tbody>
</table>

**Table 5-15. Number of Ephemeral Ports**

<table>
<thead>
<tr>
<th>Number of Ephemeral Ports</th>
<th>Fill in Your Site's Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>((5 \times \text{clients}) / \text{servers} + 10) = number of ephemeral ports on each View Connection Server instance</td>
<td></td>
</tr>
</tbody>
</table>

**Table 5-16. TCB Hash Table Size for View Connection Servers**

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

**Table 5-17. TCB Hash Table Size for Security Servers**

<table>
<thead>
<tr>
<th>Hash Table Size for Security Servers</th>
<th>Fill in Your Site's Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>((5 \times \text{clients}) / \text{security servers} + 10) = Number of hash table rows on each security server</td>
<td></td>
</tr>
</tbody>
</table>
**Sizing the Java Virtual Machine**

The View Connection Server installer sizes the Java Virtual Machine (JVM) heap memory on View Connection Server computers to support a large number of concurrent View desktop sessions. However, when View Connection Server runs on a 32-bit Windows Server computer, the View Secure Gateway Server component is configured with a limited JVM heap size. To size your deployment adequately, you can increase the JVM heap size on 32-bit computers.

On a 64-bit Windows Server computer with at least 10GB of memory, the installer configures a JVM heap size of 2GB for the View Secure Gateway Server component. This configuration supports approximately 2,000 concurrent tunnel sessions, the maximum number that View Connection Server can support. There is no benefit in increasing the JVM heap size on a 64-bit computer with 10GB of memory.

**NOTE** On a 64-bit View Connection Server computer, 10GB of memory is recommended for deployments of 50 or more View desktops. Configure less than 10GB of memory for small, proof-of-concept deployments only.

If a 64-bit computer has less than 10GB of memory, the installer configures a JVM heap size of 512MB for the View Secure Gateway Server component. If the computer has the required minimum of 4GB of memory, this configuration supports approximately 500 concurrent tunnel sessions. This configuration is more than adequate to support small, proof-of-concept deployments.

If you increase a 64-bit computer’s memory to 10GB to support a larger deployment, View Connection Server does not increase the JVM heap size. To adjust the JVM heap size to the recommended value, reinstall View Connection Server.

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

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

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

**IMPORTANT** Do not change the JVM heap size on 64-bit Windows Server computers. Changing this value might make View Connection Server behavior unstable. On 64-bit computers, the View Connection Server installer sets the JVM heap size to accord with the physical memory. If you change the physical memory on a 64-bit View Connection Server computer, reinstall View Connection Server to reset the JVM heap size.

On a 32-bit computer, if you increase the JVM heap size and reinstall or upgrade the View Connection Server software, you must increase the JVM heap size again. This value is reset each time the View Connection Server software is reinstalled or upgraded.

**Procedure**

1. On the Windows Server computer, start the Windows Registry Editor.
   a. Select Start > Command Prompt.
   b. At the command prompt, type `regedit`.
2. In the registry, locate the subkey and click **JvmOptions**.

   ```plaintext
   HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wsnm\tunnelService\Params
   ```
3 Click Edit > Modify.

A Windows dialog box displays an entry like the following one.

-Xms128m -Xmx512m -Xss96k -Xrs -XX:+UseConcMarkSweepGC

4 Edit the -Xmx parameter to have the value -Xmx1024m.

The dialog box displays the following entry.

-Xms128m -Xmx1024m -Xss96k -Xrs -XX:+UseConcMarkSweepGC

5 Click OK and exit the Registry Editor.

6 Restart the Windows Server computer.

Configure the System Page-File Settings

You can optimize the virtual memory on the Windows Server computers on which your View Connection Server instances are installed by changing the system page-file settings.

When Windows Server is installed, Windows calculates an initial and maximum page-file size based on the physical memory installed on the computer. These default settings remain fixed even after you restart the computer.

If the Windows Server computer is a virtual machine, you can change the memory size through vCenter Server. However, if Windows uses the default setting, the system page-file size does not adjust to the new memory size.

Procedure

1 On the Windows Server computer on which View Connection Server is installed, navigate to the Virtual Memory dialog box.

   By default, Custom size is selected. An initial and maximum page-file size appear.

2 Click System managed size.

Windows continually recalculates the system page-file size based on current memory use and available memory.
Installing View Transfer Server

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

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

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

1 Install View Transfer Server on page 67
   View Transfer Server downloads system-image files, synchronizes data between local desktops and the corresponding remote desktops in the datacenter, and transfers data when users check in and check out local desktops. You install View Transfer Server in a virtual machine that runs Windows Server.

2 Add View Transfer Server to View Manager on page 69
   View Transfer Server works with View Connection Server to transfer files and data between local desktops and the datacenter. Before View Transfer Server can perform these tasks, you must add it to your View Manager deployment.

3 Configure the Transfer Server Repository on page 70
   The Transfer Server repository stores View Composer base images for linked-clone desktops that run in local mode. To give View Transfer Server access to the Transfer Server repository, you must configure it in View Manager. If you do not use View Composer linked clones in local mode, you do not have to configure a Transfer Server repository.

4 Firewall Rules for View Transfer Server on page 71
   Certain incoming TCP ports must be opened on the firewall for View Transfer Server instances.

5 Installing View Transfer Server Silently on page 71
   You can install View Transfer Server silently by typing the installer filename and installation options at the command line. With silent installation, you can efficiently deploy View components in a large enterprise.

Install View Transfer Server

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

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

- Verify that you have local administrator privileges on the Windows Server on which you will install View Transfer Server.
- Verify that your installation satisfies the View Transfer Server requirements described in “View Transfer Server Requirements,” on page 11.
- Verify that you have a license to install View Transfer Server and use local desktops.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See “Firewall Rules for View Transfer Server,” on page 71.

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

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

Procedure

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

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

3. Accept the VMware license terms.

4. Accept or change the destination folder.

5. Select View Transfer Server.

6. Configure the Apache Web Server to which View Transfer Server is deployed.
   
   You can accept the default values for the network domain, Apache Server name, and administrator’s email address that are provided by the installer.

7. If you install View Transfer Server on Windows Server 2008, choose how to configure the Windows Firewall service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Windows Firewall automatically</td>
<td>Let the installer configure Windows Firewall to allow the required network connections.</td>
</tr>
<tr>
<td>Do not configure Windows Firewall</td>
<td>Configure the Windows firewall rules manually.</td>
</tr>
</tbody>
</table>

   If you install View Transfer Server on Windows Server 2003 R2, you must configure the required Windows firewall rules manually.

8. Complete the installation program to install View Transfer Server.

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

What to do next

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

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

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

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

**Prerequisites**
- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that vCenter Server is added to View Manager. The View Configuration > Servers page in View Administrator displays vCenter Server instances that are added to View Manager.

**Procedure**
1. In View Administrator, click View Configuration > Servers.
2. In the Transfer Servers panel, click Add.
3. In the Add Transfer Server wizard, select the vCenter Server instance that manages the View Transfer Server virtual machine and click Next.
4. Select the virtual machine where View Transfer Server is installed and click Finish.

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

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

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

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

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

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

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

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

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

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

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

**Prerequisites**

- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that View Transfer Server is added to View Manager. See “Add View Transfer Server to View Manager,” on page 69.

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

**Procedure**

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

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

   **Option** | **Action**
   --- | ---
   **Local Transfer Server repository** | On the virtual machine where View Transfer Server is installed, create a path and folder for the Transfer Server repository. For example: `C:\TransferRepository\`
   **Remote Transfer Server repository** | Configure a UNC path for the network share. For example: `\server.domain.com\TransferRepository\`

   All View Transfer Server instances that you add to this View Manager deployment must have network access to the shared drive.

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

3. Put all View Transfer Server instances into maintenance mode.
   a. In the Transfer Servers panel, select a View Transfer Server instance.
   b. Click **Enter Maintenance Mode** and click **OK**.
      The View Transfer Server status changes to **Maintenance mode**.
   c. Repeat Step 3a and Step 3b for each instance.

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

4. In the Transfer Servers panel, next to Transfer Server repository, click **None Configured**.
5. In the General panel on the Transfer Server repository page, click Edit.

6. Type the Transfer Server repository location and other information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Share</td>
<td>- Path. Type the UNC path that you configured.</td>
</tr>
<tr>
<td></td>
<td>- Username. Type the user ID of an administrator with credentials to access the network share.</td>
</tr>
<tr>
<td></td>
<td>- Password. Type the administrator password.</td>
</tr>
<tr>
<td></td>
<td>- Domain. Type the domain name of the network share in NetBIOS format. Do not use the .com suffix.</td>
</tr>
<tr>
<td>Local File System</td>
<td>Type the path that you configured on the local View Transfer Server virtual machine.</td>
</tr>
</tbody>
</table>

7. Click OK.

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

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

The View Transfer Server status changes to Ready.

**Firewall Rules for View Transfer Server**

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

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

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

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

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
</tr>
</tbody>
</table>

**Installing View Transfer Server Silently**

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

**Set Group Policies to Allow Silent Installation of View Transfer Server**

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

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

**Prerequisites**

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

1. Log in to the Windows Server computer and click Start > Run.
2. Type `gpedit.msc` and click OK.
3. In the Group Policy Object Editor, click Local Computer Policy > Computer Configuration.
4. Expand Administrative Templates, open the Windows Installer folder, and double-click Always install with elevated privileges.
5. In the Always Install with Elevated Privileges Properties window, click Enabled and click OK.
6. In the left pane, click User Configuration.
7. Expand Administrative Templates, open the Windows Installer folder, and double-click Always install with elevated privileges.
8. In the Always Install with Elevated Privileges Properties window, click Enabled and click OK.

What to do next

Install View Transfer Server silently.

Install View Transfer Server Silently

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

Prerequisites

- Verify that you have local administrator privileges on the Windows Server on which you will install View Transfer Server.
- Verify that your installation satisfies the View Transfer Server requirements described in “View Transfer Server Requirements,” on page 11.
- Verify that you have a license to install View Transfer Server and use local desktops.
- Verify that the virtual machine on which you install View Transfer Server has version 2.0 or later of the MSI runtime engine. For details, see the Microsoft Web site.
- Familiarize yourself with the MSI installer command-line options. See “Microsoft Windows Installer Command-Line Options,” on page 47.
- Familiarize yourself with the silent installation properties available with View Transfer Server. See “Silent Installation Properties for View Transfer Server,” on page 73.
- Verify that the Windows Installer group policies that are required for silent installation are configured on the Windows Server computer. See “Set Group Policies to Allow Silent Installation of View Transfer Server,” on page 71.

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

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

1. Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer. The installer filename is VMware-viewconnectionserver-y.y.y-xxxxxx.exe or VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe, where xxxxx is the build number and y.y.y is the version number.

2. Open a command prompt on the Windows Server computer.

3. Type the installation command on one line.

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

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

What to do next

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

Silent Installation Properties for View Transfer Server

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

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

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The path and folder in which the View Connection Server software is installed.  For example: INSTALLDIR=&quot;&quot;D:\abc\my folder&quot;&quot;</td>
<td>%ProgramFiles%\VMware\VMware View\Server</td>
</tr>
<tr>
<td></td>
<td>The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.</td>
<td></td>
</tr>
<tr>
<td>VDM_SERVER_INSTANCE_TYPE</td>
<td>The type of View server installation:</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1. Standard installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Replica installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Security server installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. View Transfer Server installation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To install a View Transfer Server, define VDM_SERVER_INSTANCE_TYPE=4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This MSI property is optional for a standard installation. It is required for all other types of installation.</td>
<td></td>
</tr>
<tr>
<td>SERVERDOMAIN</td>
<td>The network domain of the virtual machine on which you install View Transfer Server. This value corresponds to the Apache Web Server network domain that is configured during an interactive installation. For example: SERVERDOMAIN=companydomain.com</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>If you specify a custom Apache Web Server domain with the MSI property, SERVERDOMAIN, you also must specify custom SERVERNAME and SERVERADMIN properties. This MSI property is optional.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 6-2. MSI Properties for Silently Installing View Transfer Server (Continued)

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVERNAME</td>
<td>The host name of the virtual machine on which you install View Transfer Server. This value corresponds to the Apache Web Server host name that is configured during an interactive installation. For example: SERVERNAME=ts1.companydomain.com If you specify a custom Apache Web Server host name with the MSI property, SERVERNAME, you also must specify custom SERVERDOMAIN and SERVERADMIN properties. This MSI property is optional.</td>
<td>None</td>
</tr>
<tr>
<td>SERVERADMIN</td>
<td>The email address of the administrator of Apache Web Server that is configured with View Transfer Server. For example: SERVERADMIN=<a href="mailto:admin@companydomain.com">admin@companydomain.com</a> If you specify a custom Apache Web Server administrator with the MSI property, SERVERADMIN, you also must specify custom SERVERDOMAIN and SERVERNAME properties. This MSI property is optional.</td>
<td>None</td>
</tr>
<tr>
<td>FWCHOICE</td>
<td>The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: FWCHOICE=1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>This MSI property is optional.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring SSL Certificates for View Servers

You can configure SSL certificates for authentication of View Connection Server instances, security servers, and View Transfer Server instances.

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

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

View Connection Server instances, security servers, load balancers, and View Transfer Server instances require an SSL server certificate if they receive SSL connections.

- If you enable SSL for client connections, client-facing View Connection Server instances, security servers, and load balancers that terminate SSL connections require an SSL server certificate.
- If you enable the secure tunnel on a View Connection Server instance or security server, you must install an SSL server certificate on that server. Even if you use a load balancer to terminate SSL connections, View Client makes a second HTTPS connection to the View Connection Server or security server host on which you enabled the secure tunnel.
- If you enable SSL for local mode operations and desktop provisioning, View Transfer Server instances require an SSL server certificate.
- If you configure smart card authentication in VMware View, client-facing View Connection Server instances and security servers require a root CA certificate in addition to an SSL server certificate.

You can request an SSL server certificate that is specific to a web domain such as `www.mycorp.com`, or you can request a wildcard SSL server certificate that can be used throughout a domain such as `*.mycorp.com`. To simplify administration, you might choose to request a wildcard certificate if you need to install the certificate on multiple servers or in different subdomains. It is more usual to use domain-specific certificates in secure installations, and CAs usually guarantee more protection against losses for domain-specific certificates than for wildcard certificates. If you use a wildcard certificate, you need to ensure that the private key is transferrable between servers.

When you replace the default certificate with your own certificate, clients use your certificate to authenticate the server. If your certificate is signed by a CA, the certificate for the CA itself is typically embedded in the browser or is located in a trusted database that the client can access. After a client accepts the certificate, it responds by sending a secret key, which is encrypted with the public key contained in the certificate. The secret key is used to encrypt traffic between the client and the server.

You follow different procedures to configure certificates for use with View Connection Server and security server than you do for View Transfer Server. In addition, you can configure different levels of SSL security checking in View Client for Windows.
This chapter includes the following topics:

- “Configuring SSL Certificates for View Connection Server and Security Server,” on page 76
- “Configuring SSL Certificates for View Transfer Server,” on page 83
- “Configuring Certificate Checking in View Client for Windows,” on page 87
- “Appendix: Additional SSL Configuration Tasks,” on page 88

### Configuring SSL Certificates for View Connection Server and Security Server

You can configure SSL server certificates for View Connection Server instances and security servers.

You perform the following tasks to configure an SSL server certificate for View Connection Server or security server:

1. **Add the keytool utility to your system path on the View Connection Server instance or security server.**
   
   You use the keytool utility to create keystore files, generate certificate requests, import certificates into keystores, and add private keys to keystores. See “Add keytool to the System Path,” on page 89.

2. **Determine whether you need to obtain a new signed SSL server certificate from a CA. If you already have a valid SSL certificate, determine your configuration path.**
   
   **Starting Place** | **Action**
   --- | ---
   Your organization provided you with a valid SSL server certificate. | Determine the configuration path to take, depending on your SSL certificate format. See “Use an Existing SSL Certificate and Private Key,” on page 76.

   You do not have an SSL server certificate. | Obtain a signed SSL server certificate from a CA. See “Creating a New SSL Certificate,” on page 78.

3. **Configure View Connection Server or security server to use the SSL server certificate.** See “Configure a View Connection Server Instance or Security Server to Use a New Certificate,” on page 81.

4. **Configure settings in View Administrator to use SSL for client connections.** See “Configure SSL for Client Connections,” on page 82.

### Use an Existing SSL Certificate and Private Key

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

To use an existing certificate, you also need the accompanying private key. The PKCS#12 file format, formerly called PFX file format, includes both the server certificate and the private key. The PKCS#12 file type can have a .pfx or .p12 extension.

**Table 7-1** shows the configuration path to take when you start with a particular SSL certificate format.

**Table 7-1. SSL Certificate Formats and Configuration Path**

<table>
<thead>
<tr>
<th>If you have this SSL certificate format...</th>
<th>Take these steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKCS#12 signed by a root CA</td>
<td>If a PKCS#12 file contains a server certificate that is signed by a root CA and not an intermediate CA, you can use your existing PKCS#12 file when you configure your View Connection Server instance or security server to use the certificate. See “Configure a View Connection Server Instance or Security Server to Use a New Certificate,” on page 81.</td>
</tr>
<tr>
<td>PKCS#12 signed by an intermediate CA</td>
<td>If a PKCS#12 file contains a server certificate that is signed by an intermediate CA rather than by a root CA, you must import the PKCS#12 keystore into a JKS keystore. See “Convert a PKCS#12 File to JKS Format,” on page 78.</td>
</tr>
</tbody>
</table>
### Table 7-1. SSL Certificate Formats and Configuration Path (Continued)

<table>
<thead>
<tr>
<th>If you have this SSL certificate format...</th>
<th>Take these steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKCS#12 - You are not sure which type of CA has signed your certificate.</td>
<td>If you are not sure whether your PKCS#12 file is signed by a root CA or intermediate CA, see “Determine the Type of CA Signature on Your PKCS#12 Certificate,” on page 77.</td>
</tr>
<tr>
<td>PEM</td>
<td>If your organization provides you with an SSL certificate in PEM format, the certificate must be exported to PKCS#12 format. A certificate in PEM format might have an extension such as .crt or .pem. Consult with the provider of your certificate for advice on exporting the certificate to PKCS#12 format.</td>
</tr>
<tr>
<td>JKS</td>
<td>If your organization provides you with a Java keystore (JKS) file, you can use the existing JKS file when you configure your View Connection Server instance or security server to use the certificate. A JKS file might have an extension such as .jks. See “Configure a View Connection Server Instance or Security Server to Use a New Certificate,” on page 81.</td>
</tr>
</tbody>
</table>

### Determine the Type of CA Signature on Your PKCS#12 Certificate

If you are not sure whether your PKCS#12 file is signed by a root CA or intermediate CA, you can determine the signature type by using the `certutil` utility.

**Procedure**

1. Navigate to the directory that contains the PKCS#12 keystore file.
   - For example: `abc.p12`

2. Run the `certutil` command.
   - For example: `certutil abc.p12`

3. At the Windows prompt, type your PFX password.
   - The utility displays information about the PKCS#12 keystore file, including summaries of all certificates in the trust chain.

4. Look for the lines describing the **Signature**, **Root Certificate**, and **Intermediate Certificate**.
   - For example, a self-signed certificate might display the following lines:
     - Signature matches Public Key
     - Root Certificate: Subject matches Issuer

**What to do next**

If your PKCS#12 file contains a server certificate that is signed by a root CA and not an intermediate CA, you can use your existing PKCS#12 file when you configure your View Connection Server instance or security server to use the certificate. See “Configure a View Connection Server Instance or Security Server to Use a New Certificate,” on page 81.

If a PKCS#12 file contains a server certificate that is signed by an intermediate CA rather than by a root CA, you must import the PKCS#12 keystore into a JKS keystore. See “Convert a PKCS#12 File to JKS Format,” on page 78.
Convert a PKCS#12 File to JKS Format

If you already have a PKCS#12 keystore file and a server certificate that is signed by an intermediate CA rather than a root CA, you must convert the PKCS#12 keystore to JKS format before you can use it with View.

Procedure

1. Create the JKS keystore and add the intermediate certificate and root certificate to the keystore.

   To avoid seeing errors from keytool, you must add the intermediate certificate to the keystore before you can add the server certificate.
   
   a. Save the intermediate certificate as `intermediateCA.p7` in the directory that contains the keystore file.
   
   b. If your View Connection Server instance or security server does not trust the root certificate, save the root certificate as `rootCA.p7` in the keystore file directory and import the root certificate into the keystore file.

      For example:
      
      ```
      keytool -importcert -keystore keys.jks -storepass secret -alias rootCA -file rootCA.p7
      ```
   
   c. Import the intermediate certificate into the keystore file.

      For example:
      
      ```
      keytool -importcert -keystore keys.jks -storepass secret -trustcacerts -alias intermediateCA -file intermediateCA.p7
      ```

2. Add the server certificate and private key from the PKCS#12 file to the JKS keystore.

   For example:
   
   ```
   keytool -importkeystore -destkeystore keys.jks -deststorepass secret -srckeystore keys.p12 -srctype PKCS12 -srcstoretype PKCS12 -srcstorepass clydenw
   ```

   The `keytool` utility creates the JKS keystore if it does not already exist.

What to do next

Configure your View Connection Server instance or security server to use the certificate. See “Configure a View Connection Server Instance or Security Server to Use a New Certificate,” on page 81.

Creating a New SSL Certificate

You can use a self-signed certificate or a certificate signed by a CA to replace the default SSL server certificate that is provided with View Connection Server.

A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate, and thin client devices can connect without requiring additional configuration. If your clients need to determine the origin and integrity of the data they receive, you should obtain a CA-signed certificate rather than use a self-signed certificate.

1. Obtain a Signed Certificate from a CA for Use with a View Connection Server Instance or Security Server on page 79

   To obtain a signed certificate from a CA, you must use `keytool` to generate a keystore file and a certificate signing request (CSR) file. For testing purposes, you can obtain a free temporary certificate based on an untrusted root from many CAs.

2. Import a Root Certificate into a Keystore File on page 80

   If your View Connection Server instance or security server does not trust the root certificate for the server certificate that you have obtained from a CA, use `keytool` to import the certificate into your keystore file before you add the server certificate.
3 **Import an Intermediate Certificate into a Keystore File** on page 80
   If your server certificate is signed by an intermediate CA rather than by a root CA, you must add the intermediate certificate to the keystore before you add the server certificate.

4 **Import a Signed Server Certificate into a Keystore File** on page 81
   If you obtained a signed server certificate from a CA, use `keytool` to import the certificate into your keystore file.

**Obtain a Signed Certificate from a CA for Use with a View Connection Server Instance or Security Server**

To obtain a signed certificate from a CA, you must use `keytool` to generate a keystore file and a certificate signing request (CSR) file. For testing purposes, you can obtain a free temporary certificate based on an untrusted root from many CAs.

**Prerequisites**

Determine the fully qualified domain name (FQDN) that client computers use to connect to the host.

**Procedure**

1. Open a command prompt and use `keytool` to create a keystore file. For example:
   ```bash
   keytool -genkeypair -keyalg "RSA" -keysize 2048 -keystore keys.jks -storepass secret
   ```
   If you are going to import an intermediate certificate into the keystore file, you must specify a Java keystore file such as `keys.jks`.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Connection Server instance</td>
<td>Type the FQDN of the View Connection Server host if you have one View Connection Server instance. Type the FQDN of the load balancer host if you use load balancing.</td>
</tr>
<tr>
<td>Security server</td>
<td>Type the FQDN of the security server host.</td>
</tr>
</tbody>
</table>

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

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

3. Use `keytool` to create a CSR file with a name such as `certificate.csr`.
   For example: `keytool -certreq -file certificate.csr -keystore keys.jks -storepass secret`
   `keytool` creates the CSR file in the same directory as the keystore file.

4. Send the CSR file to the CA in accordance with the CA's enrollment process and request a certificate.
   After conducting some checks on your company, the CA signs your request, encrypts it with a private key, and sends you a validated certificate.

**What to do next**

If your View Connection Server instance or security server does not trust the root certificate for your server certificate, import the root certificate into your keystore file before you import the server certificate. See “Import a Root Certificate into a Keystore File,” on page 80.

If your server certificate is signed by an intermediate CA, import the intermediate certificate into your keystore file. See “Import an Intermediate Certificate into a Keystore File,” on page 80.
If you downloaded a server certificate, import it into your keystore file. See “Import a Signed Server Certificate into a Keystore File,” on page 81.

**Import a Root Certificate into a Keystore File**

If your View Connection Server instance or security server does not trust the root certificate for the server certificate that you have obtained from a CA, use keytool to import the certificate into your keystore file before you add the server certificate.

**Procedure**

1. Save the root certificate as `rootCA.p7` in the directory that contains your keystore file.
2. Open a command prompt and use keytool to import the root certificate into the keystore file.

   For example:
   
   ```
   keytool -importcert -keystore keys.jks -storepass secret -alias rootCA -file rootCA.p7
   ```

**What to do next**

If your server certificate is signed by an intermediate CA, import the intermediate certificate into your keystore file. See “Import an Intermediate Certificate into a Keystore File,” on page 80.

If your server certificate is signed by a root CA, import the certificate into your keystore file. See “Import a Signed Server Certificate into a Keystore File,” on page 81.

**Import an Intermediate Certificate into a Keystore File**

If your server certificate is signed by an intermediate CA rather than by a root CA, you must add the intermediate certificate to the keystore before you add the server certificate.

**Prerequisites**

Request and obtain an intermediate certificate from the intermediate CA.

**Procedure**

1. Save the intermediate certificate as `intermediateCA.p7` in the directory that contains the keystore file.
2. Import the intermediate certificate into the keystore file.

   For example:
   
   ```
   keytool -importcert -keystore keys.jks -storepass secret -trustcacerts -alias intermediateCA -file intermediateCA.p7
   ```

**What to do next**

If you downloaded a server certificate, import it into your keystore file. See “Import a Signed Server Certificate into a Keystore File,” on page 81.
Import a Signed Server Certificate into a Keystore File

If you obtained a signed server certificate from a CA, use keytool to import the certificate into your keystore file.

Procedure

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

   For example:
   ```plaintext
   -----BEGIN PKCS7-----
   MIIF+AYJKoZIhvcNAQcCoIIF6TCCBeUCAQExADALBgk
   LDCCApgAwIBAgIQThpY7Dsv1n1HeMgMjMR2PzANBgk
   i7oVx7J1/LCB1Fmx6NyK1ZK5mObgvd2dlnsAP+nnS
   EhCspik5pbtdo18jUubV6z1kQ71CrRQtbi/WtqpxE
   -----END PKCS7-----
   ```

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

   For example:
   ```plaintext
   keytool -importcert -keystore keys.jks -storepass secret -keyalg "RSA" -trustcacerts -file certificate.p7
   ```

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

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

What to do next

Configure your View Connection Server instance or security server to use the certificate. See “Configure a View Connection Server Instance or Security Server to Use a New Certificate,” on page 81.

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

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

Prerequisites

Obtain an existing PKCS#12 file, export an existing Microsoft IIS SSL server certificate, or create a new SSL server certificate.

Procedure

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

   For example: `install_directory\VMware\VMware View\Server\sslgateway\conf\keystore_file`

   `keystore_file` is the name of the keystore file.

   For example, your keystore file might be `keys.jks` if you imported your certificate with the keytool utility.

   Your keystore file might be `keys.pfx` if you have an existing PKCS#12 file or you exported an existing Microsoft IIS SSL server certificate.
2 Add the keyfile, keypass, and storetype properties to the locked.properties file in the SSL gateway configuration directory on the View Connection Server or security server host.

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

a Set the keyfile property to the name of your keystore file.
   
   For example: keyfile=keys.jks or keyfile=keys.pfx

b Set the keypass property to the password for your keystore file.
   
   For example: keypass=MY_PASS

c Set the storetype property to match the type of the keystore file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKCS#12 or PFX file</td>
<td>Set the value of storetype to pkcs12: storetype=pkcs12</td>
</tr>
<tr>
<td>Java keystore file</td>
<td>Set the value of storetype to jks: storetype=jks</td>
</tr>
<tr>
<td></td>
<td>You must specify the storetype property for a Java keystore file.</td>
</tr>
</tbody>
</table>

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

**What to do next**

In View Administrator, configure settings to use SSL for client connections. See “Configure SSL for Client Connections,” on page 82.

If your SSL certificates are signed by a CA that is not well known, install the root certificate (if not already present) and intermediate certificate in Active Directory. See “Add SSL Certificates in Active Directory,” on page 88.

**Configure SSL for Client Connections**

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

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

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

SSL is enabled by default for client connections.

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

**Important** If you disable or enable SSL for client connections, all existing client connections are terminated. Choose a time to restart the View Connection Server service that is least disruptive to the desktop users.

**Procedure**

1 In View Administrator, select View Configuration > Global Settings and click Edit.
2 To configure SSL for client connections, select or deselect Require SSL for client connections and View Administrator.
3 Click OK to save your changes.
4 Restart the View Connection Server service to make your changes take effect.
   In a replicated group, you must restart the service on each View Connection Server instance and on each paired security server.

5 Reconfigure any firewalls and load balancers to permit client connections using the new SSL configuration.
   See the VMware View Architecture Planning document for more information.

## Configuring SSL Certificates for View Transfer Server

If you enable SSL for local mode operations and local desktop provisioning, View Transfer Server instances require an SSL server certificate. You must replace the default certificate that is generated when you install View Transfer Server.

You can replace the default certificate with a certificate that is signed by a CA or, for testing purposes, you can generate and use a self-signed certificate.

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

You perform the following tasks to configure an SSL server certificate for View Transfer Server:

1 Add the openssl utility to your system path.
   You use the openssl utility to create and manage certificates for View Transfer Server. See “Add openssl to the System Path,” on page 89.

2 Determine your certificate configuration path.

<table>
<thead>
<tr>
<th>Starting Place</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>You do not have an SSL server certificate.</td>
<td>Obtain a signed SSL server certificate from a CA. See “Obtain a Signed Certificate from a CA for Use with a View Transfer Server Instance,” on page 84. Alternatively, for testing purposes, you can generate and use a self-signed certificate. See “Generate a Self-Signed Certificate for View Transfer Server,” on page 85.</td>
</tr>
<tr>
<td>Your organization provided you with a valid SSL server certificate in PKCS#12 format.</td>
<td>You must export the private key and server certificate into PEM format. See “Prepare an Existing Certificate in PKCS#12 Format for Use with View Transfer Server,” on page 84.</td>
</tr>
<tr>
<td>Your organization provided you with a valid SSL server certificate in PKCS#7 format and a separate private key.</td>
<td>You can use the certificate to replace the default SSL server certificate provided with View Transfer Server. See “Configure a View Transfer Server Instance to Use a Certificate,” on page 85.</td>
</tr>
</tbody>
</table>

**NOTE** A certificate that is used with View Transfer Server must be in PEM format. If your certificate is not in PEM format, you must export the certificate into PEM format.

3 Configure View Transfer Server to use the SSL server certificate. See “Configure a View Transfer Server Instance to Use a Certificate,” on page 85.

4 Configure settings in View Administrator to use SSL for local mode provisioning and other local mode operations. See “Configure SSL for View Transfer Server Communications,” on page 87.
Prepare an Existing Certificate in PKCS#12 Format for Use with View Transfer Server

An SSL certificate that is used with a View Transfer Server instance must be in PEM format. If you have an existing certificate in PKCS#12 format, you can use `openssl` to export the private key and server certificate in PEM format.

If you have an existing server certificate in PKCS#7 format and a separate private key, you can go directly to the procedure described in “Configure a View Transfer Server Instance to Use a Certificate,” on page 85.

Prerequisites

Verify that `openssl` was added to the system Path variable on your host. See “Add openssl to the System Path,” on page 89.

Procedure

1. On the View Transfer Server system, open a command prompt and use `openssl` to export the private key from your .p12 or .pfx certificate file.

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

2. Remove the pass phrase from the private key and save it to the file `server.key`.

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

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

3. Export the server certificate from your certificate file and save it to the file `server.crt`.

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

What to do next

Configure your View Transfer Server instance to use the certificate. See “Configure a View Transfer Server Instance to Use a Certificate,” on page 85.

Obtain a Signed Certificate from a CA for Use with a View Transfer Server Instance

To obtain a signed certificate from a CA, you must use `openssl` to generate a private key file and a certificate signing request (CSR) file. For testing purposes, you can obtain a free temporary certificate based on an untrusted root from many CAs.

Prerequisites

Determine the fully qualified domain name (FQDN) that client computers use to connect to the host.

Procedure

1. Open a command prompt and use `openssl` to create a private key file and a CSR file.

   For example: `openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr`

2. When `openssl` prompts you for a common name, type the fully qualified domain name (FQDN) that client computers use to connect to the View Transfer Server host.

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

   `openssl` creates the private key file and the CSR file in the current directory.
3 Send the CSR file to the CA in accordance with the CA’s enrollment process and request a certificate in PEM format. After conducting some checks on your company, the CA signs your request, encrypts it with a private key, and sends you a validated certificate.

4 If necessary, convert your certificate to PEM format. Some CAs provide certificates in a format other than PEM. If you download this type of certificate, you must convert it to PEM format.

   For example: `openssl x509 -inform der -in certificate.cer -out certificate.pem`

**What to do next**

Configure the View Transfer Server instance to use the SSL server certificate. See “Configure a View Transfer Server Instance to Use a Certificate,” on page 85.

### Generate a Self-Signed Certificate for View Transfer Server

You must replace the default SSL server certificate that is provided when you install a View Transfer Server instance. For testing purposes, you can generate and use a self-signed certificate to replace the default certificate.

You use the `openssl` utility to generate SSL certificates for View Transfer Server.

**Prerequisites**

Add `openssl` to the system Path variable on your host. See “Add openssl to the System Path,” on page 89.

**Procedure**

1 On the View Transfer Server computer, generate the private certificate key.
   
   For example: `openssl genrsa -des3 -out server-with-pass.key -passout password 2048`

2 Remove the pass phrase from the private key and save it to the file `server.key`.
   This step prevents Apache from prompting you for your pass phrase each time Apache is restarted.

   For example: `openssl rsa -in server-with-pass.key -passin password -out server.key`

3 Generate the self-signed server certificate.

   For example: `openssl req -new -x509 -days 3650 -key server.key -out server.crt`

**What to do next**

Configure the View Transfer Server instance to use the SSL server certificate. See “Configure a View Transfer Server Instance to Use a Certificate,” on page 85.

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

To configure a View Transfer Server instance to use an SSL server certificate, you must copy your certificate and private key files to the View Transfer Server host. You can use an SSL server certificate that is signed by a CA, or you can generate a self-signed certificate.

The Apache server on the View Transfer Server instance requires Base64 encoded DER (PEM) certificates. Certificate files and key files must have the extensions `.crt` and `.key` respectively.

When you install View Transfer Server, the installer generates the default certificate file, `server.crt`, and private key file, `server.key`. In the following procedure, make sure that you replace these files in the View Transfer Server certificate directory or configure the Apache configuration file to specify the names of your own certificate and private key files.
If your SSL server certificate is signed by an intermediate CA, you must add the intermediate certificate to the View Transfer Server certificate directory and configure the Apache configuration file to specify the name of the intermediate certificate.

**Prerequisites**

- Add openssl to the system Path variable on your host. See “Add openssl to the System Path,” on page 89.
- If you obtained a server certificate from a CA, or your organization provided a server certificate, verify that your certificate is in PEM format.
- If your certificate files and key files are in a PKCS#12 keystore file, see “Prepare an Existing Certificate in PKCS#12 Format for Use with View Transfer Server,” on page 84.
- If you use an intermediate CA, obtain an intermediate certificate in PEM format.

**Procedure**

1. Stop the View Transfer Server service.
2. Copy the server certificate, intermediate certificate (if any), and private key files to the directory `install_directory\VMware\VMware View\Server\http\conf` on the View Transfer Server host.
3. If you have not already taken this step, remove the pass phrase from the private key. This step prevents Apache from prompting you for your pass phrase each time it is restarted. For example: `openssl rsa -in server-with-pass.key -passin password -out server.key`
4. Edit the entries for `SSLCertificateFile` and `SSLCertificateKeyFile` in the Apache configuration file `mod_vprov.conf` to specify the names of the server certificate and private key files. For example:
   ```
   SSLCertificateFile server.crt
   SSLCertificateKeyFile server.key
   ```
5. If you copied an intermediate certificate file to the View Transfer Server host, add an entry for the `SSLCertificateChainFile` directive to `mod_vprov.conf`. For example:
   ```
   SSLCertificateChainFile intermediateCA.crt
   ```
6. Restart the View Transfer Server service to make your changes take effect.
7. Verify that the certificate is configured correctly by using your Web browser to navigate to the View Transfer Server host address. For example: `https://transfer_server_host_address`.

**What to do next**

In View Administrator, configure settings to use SSL for local mode provisioning and other local mode operations. See “Configure SSL for View Transfer Server Communications,” on page 87.

If your SSL certificates are signed by a CA that is not well known, install the root certificate (if not already present) and intermediate certificate in Active Directory. See “Add SSL Certificates in Active Directory,” on page 88.
Configure SSL for View Transfer Server Communications

To configure whether SSL is used for communications and data transfers between client computers that host local desktops and View Transfer Server, you set View Connection Server settings in View Administrator. The SSL settings for View Transfer Server communications and data transfers are specific to a single View Connection Server instance. You might want to enable SSL on an instance that services users that connect from the Internet, but disable it on an instance that is dedicated to internal users.

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

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

Procedure

1. In View Administrator, select View Configuration > Servers.
2. Select the View Connection Server instance and click Edit.
3. To configure SSL for communications and data transfers between client computers that host local desktops and View Transfer Server, select or deselect Use SSL for Local Mode operations. These operations include checking in and checking out desktops and replicating data from client computers to the datacenter.
4. To configure SSL for transfers of View Composer base-image files from the Transfer Server repository to client computers that host local desktops, select or deselect Use SSL when provisioning desktops in Local Mode.
5. Click OK to save your changes.

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

Configuring Certificate Checking in View Client for Windows

You can use a security-related group policy setting in the View Client Configuration ADM template file (vdm_client.adm) to configure SSL server certificate checking in the Windows-based View Client. Certificate checking occurs if you configure View Connection Server to require SSL connections for client connections or for connections to View Administrator. Certificate verification includes all the following checks:

- Has the certificate been revoked? Is it possible to determine whether the certificate has been revoked?
- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur is if a load balancer redirects the View client to a server with a certificate that does not match the host name the user entered. Another reason a mismatch can occur is if the user enters an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA.

To pass this check, the certificate's chain of trust must be rooted in the device’s local certificate store.
When you first set up a View environment, a default self-signed certificate is used. By default, the certificate verification mode that is used is Warn But Allow. In this mode, when either of the following server certificate issues occurs, a warning is displayed, but the user can choose to continue on and ignore the warning:

- A self-signed certificate is provided by the View server. In this case, it is acceptable if the certificate name does not match the View Connection Server name provided by the user in View Client.
- A verifiable certificate that was configured in your deployment has expired or is not yet valid.

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

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

**Appendix: Additional SSL Configuration Tasks**

When you configure SSL certificates for View servers, you might need to perform certain additional tasks.

**Add SSL Certificates in Active Directory**

For CAs that are not well known, you must add the root CA certificate and intermediate certificate in Active Directory. These steps allow the root CA certificate to be installed in your client systems’ Trusted Root stores. For example, you might need to take these steps if your organization uses an internal certificate service.

If your SSL server certificates are signed by a well known CA, you do not have to add certificates in Active Directory. For well known CAs, the operating system vendors preinstall the root certificate on client systems.

Specifically, if you use a little-known CA to provide SSL server certificates, you must add the root certificate to the Enterprise NTAuth store and the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

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

**Procedure**

1. On your Active Directory server, use the certutil command to publish the certificate to the Enterprise NTAuth store.
   
   For example: `certutil -dspublish -f path_to_root_CA_cert NTAuthCA`

2. On your Active Directory server, select Start > All Programs > Administrative Tools > Active Directory Users and Computers.

3. Right-click your domain and click Properties.

4. On the Group Policy tab, click Open to open the Group Policy Management plug-in.

5. Right-click Default Domain Policy and click Edit.

6. Expand the Computer Configuration section and open Windows Settings\Security Settings\Public Key.
7  Import the certificate.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Root certificate     | a Right-click Trusted Root Certification Authorities and select Import.  
b Follow the prompts in the wizard to import the root certificate (for example, rootCA.cer) and click OK. |
| Intermediate certificate | a Right-click Intermediate Certification Authorities and select Import.  
b Follow the prompts in the wizard to import the intermediate certificate (for example, intermediateCA.cer) and click OK. |

8  Close the Group Policy window.

All of the systems in the domain now have a copy of the root certificate in their Trusted Root stores and, if appropriate, a copy of the intermediate certificate in their Intermediate Certification Authority stores.

### Add keytool to the System Path

keytool is a key and certificate management utility. You must add the path to this utility to the system environment Path variable so that you can run the utility from any directory on your host.

You use the keytool utility to create keystores, generate certificate requests, import certificates into keystores, and add private keys to keystores.

**Procedure**

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

2  Click **OK** until the Windows System Properties dialog box closes.

### Add openssl to the System Path

You use the openssl utility export certificates and create and export private keys for use with View Transfer Server. You must add the path to openssl to the system environment Path variable so that you can run the utilities from any directory on your host.

**Procedure**

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

2  Click **OK** until the Windows System Properties dialog box closes.
Creating an Event Database

You create an event database to record information about View Manager events. If you do not configure an event database, you must look in the log file to get information about events, and the log file contains very limited information.

This chapter includes the following topics:

- “Add a Database and Database User for View Events,” on page 91
- “Prepare an SQL Server Database for Event Reporting,” on page 92
- “Configure the Event Database,” on page 92

Add a Database and Database User for View Events

You create an event database by adding it to an existing database server. You can then use enterprise reporting software to analyze the events in the database.

The database server for the event database can reside on a View Connection Server host itself or on a dedicated server. Alternatively, you can use a suitable existing database server, such as a server that hosts a View Composer database.

Note：You do not need to create an ODBC data source for this database.

Prerequisites

- Verify that you have a supported Microsoft SQL Server or Oracle database server on a system that a View Connection Server instance has access to. For a list of supported database versions, see “Database Requirements for View Composer,” on page 10.
- Verify that you have the required database privileges to create a database and user on the database server.
- If you are not familiar with the procedure to create databases on Microsoft SQL Server database servers, review the steps in “Add a View Composer Database to SQL Server,” on page 28.
- If you are not familiar with the procedure to create databases on Oracle database servers, review the steps in “Add a View Composer Database to Oracle 11g or 10g,” on page 30.

Procedure

1. Add a new database to the server and give it a descriptive name such as ViewEvents.
2 Add a user for this database that has permission to create tables, views, and, in the case of Oracle, triggers and sequences, as well as permission to read from and write to these objects.

For a Microsoft SQL Server database, do not use the Integrated Windows Authentication security model method of authentication. Be sure to use the SQL Server Authentication method of authentication.

The database is created, but the schema is not installed until you configure the database in View Administrator.

What to do next
Follow the instructions in “Configure the Event Database,” on page 92.

Prepare an SQL Server Database for Event Reporting
Before you can use View Administrator to configure an event database on Microsoft SQL Server, you must configure the correct TCP/IP properties and verify that the server uses SQL Server Authentication.

Prerequisites
- Create an SQL Server database for event reporting. See “Add a Database and Database User for View Events,” on page 91.
- Verify that you have the required database privileges to configure the database.
- Verify that the database server uses the SQL Server Authentication method of authentication. Do not use Windows Authentication.

Procedure
1 Open SQL Server Configuration Manager and expand SQL Server YYYY Network Configuration.
2 Select Protocols for server_name.
3 In the list of protocols, right-click TCP/IP and select Properties.
4 Set the Enabled property to Yes.
5 Verify that a port is assigned or, if necessary, assign one.
   For information on the static and dynamic ports and how to assign them, see the online help for the SQL Server Configuration manager.
6 Verify that this port is not blocked by a firewall.

What to do next
Use View Administrator to connect the database to View Connection Server. Follow the instructions in “Configure the Event Database,” on page 92.

Configure the Event Database
The event database stores information about View events as records in a database rather than in a log file.

You configure an event database after installing a View Connection Server instance. You need to configure only one host in a View Connection Server group. The remaining hosts in the group are configured automatically.

You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the VMware View Integration document.

Prerequisites
You need the following information to configure an event database:
- The DNS name or IP address of the database server.
- The type of database server: Microsoft SQL Server or Oracle.
- The port number that is used to access the database server. The default is 1521 for Oracle and 1433 for SQL Server. For SQL Server, if the database server is a named instance or if you use SQL Server Express, you might need to determine the port number. See the Microsoft KB article about connecting to a named instance of SQL Server, at http://support.microsoft.com/kb/265808.
- The name of the event database that you created on the database server. See “Add a Database and Database User for View Events,” on page 91.
- The username and password of the user you created for this database. See “Add a Database and Database User for View Events,” on page 91.

  Use SQL Server Authentication for this user. Do not use the Integrated Windows Authentication security model method of authentication.
- A prefix for the tables in the event database, for example, VE_. The prefix enables the database to be shared among View installations.

  **Note**  You must enter characters that are valid for the database software you are using. The syntax of the prefix is not checked when you complete the dialog box. If you enter characters that are not valid for the database software you are using, an error occurs when View Connection Server attempts to connect to the database server. The log file indicates all errors, including this error and any others returned from the database server if the database name is invalid.

**Procedure**

1. In View Administrator, select **View Configuration > Event Configuration**.
2. In the **Event Database** section, click **Edit**, enter the information in the fields provided, and click **OK**.
3. (Optional) In the Event Settings window, click **Edit**, change the length of time to show events and the number of days to classify events as new, and click **OK**.

   These settings pertain to the length of time the events are listed in the View Administrator interface. After this time, the events are only available in the historical database tables.

   The Database Configuration window displays the current configuration of the event database.
4. Select **Monitoring > Events** to verify that the connection to the event database is successful.

   If the connection is unsuccessful, and error message appears. If you are using SQL Express or if you are using a named instance of SQL Server, you might need to determine the correct port number, as mentioned in the prerequisites.

   In the View Administrator Dashboard, the System Component Status displays the event database server under the Reporting Database heading.
You can obtain the Windows-based View Client installer either from the VMware Web site or from View Portal, a Web access page provided by View Connection Server. You can set various startup options for end users after View Client is installed.

For information about installing and using other View Clients, such as View Client for the Mac and View Client for iPad, see the documents that pertain to the specific client. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

This chapter includes the following topics:
- “Install the Windows-Based View Client or View Client with Local Mode,” on page 95
- “Start the Windows-Based View Client or View Client with Local Mode,” on page 96
- “Install View Client by Using View Portal,” on page 98
- “Set Printing Preferences for the Virtual Printer Feature on Windows Clients,” on page 99
- “Using USB Printers,” on page 100
- “Installing View Client Silently,” on page 101

Install the Windows-Based View Client or View Client with Local Mode

End users open View Client to connect to their virtual desktops from a physical machine. You can run a Windows-based installer file to install all components of View Client.

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

View Client with Local Mode lets end users download a copy of their virtual desktop to their local computer. End users can then use the virtual desktop even when they do not have a network connection. Latency is minimized and performance is enhanced.

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

Prerequisites
- Verify that you can log in as an administrator on the client system.
- Verify that the client system uses a supported operating system. See “Supported Operating Systems for Windows-Based View Client and View Client with Local Mode,” on page 14.
- Verify that View Agent is not installed.
If you plan to install View Client with Local Mode, verify that your license includes View Client with Local Mode.

If you plan to install View Client with Local Mode, verify that none of the following products is installed: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.

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

If you plan to install the USB Redirection component, verify that the Windows Automatic Update feature is not turned off on the client computer.

Determine whether to use the feature that lets end users log in to View Client and their virtual desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the View Connection Server instance and ultimately to the virtual desktop. Some client operating systems do not support this feature.

If you do not want to require end users to supply the IP address or fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the IP address or FQDN so that you can supply it during installation.

**Procedure**

1. Log in to the client system as a user with administrator privileges.


   Select the appropriate installer file, where $xxxx$ is the build number and $y.y.y$ is the version number.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Client on 64-bit operating systems</td>
<td>Select VMware-viewclient-x86_64-y.y.y-xxxxxx.exe for View Client.</td>
</tr>
<tr>
<td></td>
<td>Select VMware-viewclientwithlocalmode-x86_64-y.y.y-xxxxxx.exe for View Client with Local mode.</td>
</tr>
<tr>
<td>View Client on 32-bit operating systems</td>
<td>Select VMware-viewclient-y.y.y-xxxxxx.exe for View Client.</td>
</tr>
<tr>
<td></td>
<td>Select VMware-viewclientwithlocalmode-y.y.y-xxxxxx.exe for View Client with Local Mode.</td>
</tr>
</tbody>
</table>

3. To start the View Client installation program, double-click the installer file.

4. Follow the prompts to install the components you want.

   The VMware View Client service is installed on the Windows client computer. The service name for View Client is wsnm.exe. The service name for the USB component is wsnm_usbctrl.exe.

**What to do next**

Start the View Client and verify that you can log in to the correct virtual desktop. See “Start the Windows-Based View Client or View Client with Local Mode,” on page 96 or “Install View Client by Using View Portal,” on page 98.

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

Before you have end users access their virtual desktops, test that you can log in to a virtual desktop from a client device. You can start View Client from the Start menu or a desktop shortcut on the client system.

In environments where a network connection is available, the user session is authenticated by View Connection Server.
Prerequisites

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

Procedure

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in as current user</td>
<td>This check box is displayed or hidden according to the global setting in View Administrator. Do not select this check box if you plan to check out the View desktop for use in local mode.</td>
</tr>
<tr>
<td>Use secure connection (SSL)</td>
<td>If this check box is selected, you must also select the global setting called Use SSL for client connections in View Administrator.</td>
</tr>
<tr>
<td>Port</td>
<td>If you use a secure connection, the default port is 443.</td>
</tr>
<tr>
<td>Autoconnect</td>
<td>If you select this check box, the next time you start View Client, the Connection Server field is disabled and you are connected to the server specified when you selected the Autoconnect check box. To deselect this check box, cancel the next dialog box that appears and click Options to display and change this setting.</td>
</tr>
</tbody>
</table>

4. Click Connect.
5. Enter the credentials of a user who is entitled to use at least one desktop pool, select the domain, and click Login.
   If you type the user name using the format user@domain, the name is treated as a user principal name (UPN) because of the @ sign, and the domain drop-down menu is disabled.
   For information about creating desktop pools and entitling users to pools, see VMware View Administration document.
6. (Optional) In the Display drop-down menu, select the window size for displaying the View desktop.
7. (Optional) To select a display protocol, click the down-arrow next to a desktop in the list, click Display Protocol, and select the protocol.
   This choice is available only if your View administrator has enabled it.
8. Select a desktop from the list of desktop pools and click Connect.

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

After you are connected, the client window appears.
If authentication to View Connection Server fails or if View Client cannot connect to a desktop, perform the following tasks:

- Verify that the View Client setting for using secure (SSL) connections matches the global setting in View Administrator. For example, if the check box for secure connections is deselected on the client, the check box must also be deselected in View Administrator.

- Verify that the security certificate for View Connection Server is working properly. If it is not, in View Administrator, you might also see that the View Agent on desktops is unreachable and the Transfer Server status shows that it is not ready. These are symptoms of additional connection problems caused by certificate problems.

- Verify that the tags set on the View Connection Server instance allow connections from this user. See the VMware View Administration document.

- Verify that the user is entitled to access this desktop. See the VMware View Administration document.

- Verify that the client computer allows remote desktop connections.

**What to do next**

- Configure startup options.
  
  If you do not want to require end users to provide the host name or IP address of View Connection Server, or if you want to configure other startup options, use the View Client command-line options to create a desktop shortcut. See the VMware View Administration document.

- Check out a desktop that can be used in local mode.

  End users can determine if a desktop is eligible for checkout by clicking the down-arrow next to the desktop in the list provided by View Client with Local Mode. If the desktop can be used in local mode, the Check out option appears in the context menu. Only the user who checks out the desktop can access it, even if a group is entitled to access the desktop.

**Install View Client by Using View Portal**

An expedient way of installing the View Client or View Client with Local Mode application is to open a browser and browse to the View Portal Web page. You can use View Portal to download the full View Client installer for both Windows and Mac client computers.

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

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

**Prerequisites**

- Verify that you have the URL for the View Connection Server instance.

- Verify that you can log in as an administrator on the client system.

- Verify that a virtual desktop has been created and that the user account you plan to use is entitled to access this desktop.

- Verify that the client system uses a supported operating system. See “Supported Operating Systems for Windows-Based View Client and View Client with Local Mode,” on page 14.

- Verify that View Agent is not installed.

- If you plan to install View Client with Local Mode, verify that your license includes View Client with Local Mode.
If you plan to install View Client with Local Mode, verify that none of the following products is installed: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.

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

If you plan to install the USB Redirection component, verify that the Windows Automatic Update feature is not turned off on the client computer.

**Procedure**

1. Log in to the client system as a user with administrator privileges.
2. Open a browser and enter the URL of the View Connection Server instance that provides access to the virtual desktop.
   
   Internet Explorer can determine whether an upgrade is available, whereas Firefox and Safari cannot. Also, in the list of installers, Internet Explorer lists 32-bit installers if the client has a 32-bit system and lists 64-bit installers if the client has a 64-bit system, whereas Firefox lists both 32-bit and 64-bit installers.
3. Follow the prompts on the Web page.
   
   If the version available from View Connection Server is newer than that installed on the client device, you can choose to upgrade. If the version is the same as that on the client device, View Portal starts the View Client installed on the client computer.
   
   If you have an older version of View Client and a smart card is required for client connections, an Internet Explorer browser prompts you to insert your smart card before View Portal checks the version of your existing View Client.
4. If Internet Explorer prompts you to insert a smart card, either insert the card or click Cancel.
   
   Inserting a smart card and Cancel have the same effect.

**What to do next**

Connect to the View desktop. See “Start the Windows-Based View Client or View Client with Local Mode,” on page 96.

**Set Printing Preferences for the Virtual Printer Feature on Windows Clients**

The virtual printing feature lets end users use local or network printers from a View desktop without requiring that additional print drivers be installed in the View desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on.

After a printer is added on the local Windows computer, View adds that printer to the list of available printers on the View desktop. No further configuration is required. Users who have administrator privileges can still install printer drivers on the View desktop without creating a conflict with the virtual printer component.

**IMPORTANT** This feature is not available for the following types of printers:

- USB printers that are using the USB redirection feature to connect to a virtual USB port in the View desktop
  
  You must disconnect the USB printer from the View desktop in order to use the virtual printing feature with it.

- The Windows feature for printing to a file
  
  Selecting the Print to file check box in a Print dialog box does not work. Using a printer driver that creates a file does work. For example, you can use a PDF writer to print to a PDF file.
Prerequisites

Verify that the Virtual Printing component of View Agent is installed on the View desktop. In the View desktop file system, the drivers are located in C:\Program Files\Common Files\VMware\Drivers\Virtual Printer.

Installing View Agent is one of the tasks required for preparing a virtual machine to be used as a View desktop. For more information, see the *VMware View Administration* document.

Procedure

1. In the View desktop, click **Start > Settings > Printers and Faxes**.
2. In the Printers and Faxes window, right-click any of the locally available printers and select **Properties**.
   - On Windows 7 desktops, you might see only the default printer, even though other printers are available. To see the other printers, right-click the default printer and point to **Printer properties**.
3. In the Print Properties window, click the **ThinPrint Device Setup** tab and specify which settings to use.
4. On the **General** tab, click **Printing Preferences** and edit the page and color settings.
5. On the **Advanced** tab, set preferences for double-sided printing and portrait (long edge) or landscape (short edge) printing.
6. To preview each printout on the host, enable **Preview on client before printing**. From this preview, you can use any printer with all its available properties.
7. On the **Adjustment** tab, review the settings for automatic print adjustment. VMware recommend that you retain the default settings.
8. Click **OK**.

Using USB Printers

In a View environment, virtual printers and redirected USB printers can work together without conflict.

A USB printer is a printer that is attached to a USB port on the local client system. To send print jobs to a USB printer, you can either use the USB redirection feature or use the virtual printing feature.

- You can use the USB redirection feature to attach a USB printer to a virtual USB port in the View desktop as long as the required drivers are also installed on the View desktop.
  - If you use this redirection feature the printer is no longer attached to the physical USB port on the client and this is why the USB printer does not appear in the list of local printers that the virtual printing feature displays. This also means that you can print to the USB printer from the View desktop but not from the local client machine.

- On Windows clients, you can alternatively use the virtual printing feature to send print jobs to a USB printer. If you use the virtual printing feature you can print to the USB printer from both the View desktop and the local client, and you do not need to install print drivers on the View desktop.
Installing View Client Silently

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

Set Group Policies to Allow Silent Installation of View Client with Local Mode

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

You do not have to set these group policies to install View Client silently. These policies are required only for View Client with Local Mode.

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

Prerequisites

Verify that you have administrator privileges on the Windows client computer on which you will install View Client with Local Mode.

Procedure

1. Log in to the client computer and click \Start > Run.\n2. Type `gpedit.msc` and click OK.
3. In the Group Policy Object Editor, click `Local Computer Policy > Computer Configuration`.
4. Expand `Administrative Templates`, open the `Windows Installer` folder, and double-click `Always install with elevated privileges`.
5. In the `Always Install with Elevated Privileges Properties` window, click `Enabled` and click OK.
6. In the left pane, click `User Configuration`.
7. Expand `Administrative Templates`, open the `Windows Installer` folder, and double-click `Always install with elevated privileges`.
8. In the `Always Install with Elevated Privileges Properties` window, click `Enabled` and click OK.

What to do next

Install View Client with Local Mode silently.

Install View Client Silently

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

Prerequisites

- Verify that you can log in as an administrator on the client system.
- Verify that the client system uses a supported operating system. See “Supported Operating Systems for Windows-Based View Client and View Client with Local Mode,” on page 14.
- If you plan to install View Client with Local Mode, verify that your license includes View Client with Local Mode.
- If you plan to install View Client with Local Mode, verify that none of the following products is installed: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
Determine whether to use the feature that lets end users log in to View Client and their virtual desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the View Connection Server instance and ultimately to the virtual desktop. Some client operating systems do not support this feature.

If you do not want to require end users to supply the IP address or fully qualified domain name (FQDN) of the View Connection Server instance that hosts their virtual machine, determine the IP address or FQDN so that you can supply it during installation.

Familiarize yourself with the MSI installer command-line options. See “Microsoft Windows Installer Command-Line Options,” on page 47.

Familiarize yourself with the silent installation (MSI) properties available with View Client. See “Silent Installation Properties for View Client,” on page 103.

Determine whether to allow end users to access locally connected USB devices from their virtual desktops. If not, set the MSI property, ADDLOCAL, to the list of features of interest and omit the USB feature. For details, see “Silent Installation Properties for View Client,” on page 103.

If you install View Client with Local Mode, verify that the Windows Installer group policies that are required for silent installation are configured on the client computer. See “Set Group Policies to Allow Silent Installation of View Client with Local Mode,” on page 101.

**Procedure**

1. On the client system, download the View Client installer file from the VMware product page at http://www.vmware.com/products/.

   Select the appropriate installer file, where `xxxxxx` is the build number and `y.y.y` is the version number.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Client on 64-bit operating systems</strong></td>
<td>Select VMware-viewclient-x86_64-y.y-y-xxxxxx.exe for View Client. Select VMware-viewclientwithlocalmode-x86_64-y.y-y-xxxxxx.exe for View Client with Local mode.</td>
</tr>
<tr>
<td><strong>View Client on 32-bit operating systems</strong></td>
<td>Select VMware-viewclient-y.y-y-xxxxxx.exe for View Client. Select VMware-viewclientwithlocalmode-y.y-y-xxxxxx.exe for View Client with Local mode.</td>
</tr>
</tbody>
</table>

2. Open a command prompt on the Windows client computer.

3. Type the installation command on one line.

   This example installs View Client with single sign-on and USB redirection features. A default View Connection Server instance is configured for View Client users: `VMware-viewclient-y.y-y-xxxxxx.exe /s /v"/qn REBOOT=ReallySuppress VDM_SERVER=cs1.companydomain.com ADDLOCAL=Core,MVDI"`

   This example installs View Client with Local Mode: `VMware-viewclientwithlocalmode-y.y-y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,MVDI"`

   **NOTE** The Core feature is mandatory.

The VMware View Client service is installed on the Windows client computer.

**What to do next**

Start the View Client and verify that you can log in to the correct virtual desktop. See “Start the Windows-Based View Client or View Client with Local Mode,” on page 96 or “Install View Client by Using View Portal,” on page 98.
Silent Installation Properties for View Client

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

Table 9-1 shows the View Client silent installation properties that you can use at the command-line.

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The path and folder in which the View Client software is installed. For example: <code>INSTALLDIR=&quot;D:\abc\my folder&quot;</code></td>
<td>%ProgramFiles%\VMware\VMware View\Client</td>
</tr>
<tr>
<td>VDM_SERVER</td>
<td>The fully qualified domain name (FQDN) or IP address of the View Connection Server instance to which View Client users connect by default. When you configure this property, View Client users do not have to supply this FQDN or IP address. For example: <code>VDM_SERVER=cs1.companydomain.com</code></td>
<td>None</td>
</tr>
<tr>
<td>DESKTOP_SHORTCUT</td>
<td>Configures a desktop shortcut icon for View Client. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.</td>
<td>1</td>
</tr>
<tr>
<td>QUICKLAUNCH_SHORTCUT</td>
<td>Configures a shortcut icon on the quick-launch tray for View Client. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.</td>
<td>1</td>
</tr>
<tr>
<td>STARTMENU_SHORTCUT</td>
<td>Configures a shortcut for View Client in the Start menu. A value of 1 installs the shortcut. A value of 0 does not install the shortcut. This MSI property is optional.</td>
<td>1</td>
</tr>
</tbody>
</table>

In a silent installation command, you can use the MSI property, `ADDLOCAL=`, to specify features that the View Client installer configures. Each silent-installation feature corresponds to a setup option that you can select during an interactive installation.

Table 9-2 shows the View Client features you can type at the command line and the corresponding interactive-installation options.

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

<table>
<thead>
<tr>
<th>A</th>
<th>Active Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configuring domains and trust relationships</td>
</tr>
<tr>
<td></td>
<td>preparing for smart card authentication</td>
</tr>
<tr>
<td></td>
<td>preparing for SSL certificate configuration</td>
</tr>
<tr>
<td></td>
<td>preparing for use with View</td>
</tr>
<tr>
<td>Active Directory groups</td>
<td>creating for kiosk mode client accounts</td>
</tr>
<tr>
<td></td>
<td>creating for View users and administrators</td>
</tr>
<tr>
<td>ADM template files</td>
<td>24</td>
</tr>
<tr>
<td>Adobe Flash requirements</td>
<td>19</td>
</tr>
<tr>
<td>antivirus software, View Composer</td>
<td>34</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
<th>browser requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9, 16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>certificate signing requests, See CSRs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>certificates</td>
</tr>
<tr>
<td></td>
<td>additional tasks</td>
</tr>
<tr>
<td></td>
<td>checking in View Client</td>
</tr>
<tr>
<td></td>
<td>configuring View Connection Server to use</td>
</tr>
<tr>
<td></td>
<td>configuring View Transfer Server to use</td>
</tr>
<tr>
<td></td>
<td>creating new</td>
</tr>
<tr>
<td></td>
<td>exporting to PEM format</td>
</tr>
<tr>
<td></td>
<td>for View Connection Server</td>
</tr>
<tr>
<td></td>
<td>for View Transfer Server</td>
</tr>
<tr>
<td></td>
<td>importing to a keystore file</td>
</tr>
<tr>
<td></td>
<td>obtaining signatures</td>
</tr>
<tr>
<td></td>
<td>replacing the default</td>
</tr>
<tr>
<td></td>
<td>requirements</td>
</tr>
<tr>
<td></td>
<td>self-signed for View Transfer Server</td>
</tr>
<tr>
<td></td>
<td>using an existing certificate</td>
</tr>
<tr>
<td></td>
<td>certutil, identifying the type of CA signature</td>
</tr>
<tr>
<td></td>
<td>certutil command</td>
</tr>
<tr>
<td></td>
<td>client software requirements</td>
</tr>
<tr>
<td></td>
<td>CPU requirements, local mode desktops</td>
</tr>
<tr>
<td></td>
<td>CSRs, creating</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
<th>databases</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>creating for View Composer</td>
</tr>
<tr>
<td></td>
<td>View events</td>
</tr>
<tr>
<td></td>
<td>default certificate, replacing</td>
</tr>
<tr>
<td></td>
<td>direct connections, configuring</td>
</tr>
<tr>
<td></td>
<td>display requirements, local mode desktops</td>
</tr>
<tr>
<td></td>
<td>DNS resolution, View Composer</td>
</tr>
<tr>
<td></td>
<td>documentation feedback, how to provide</td>
</tr>
<tr>
<td></td>
<td>domain filtering</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E</th>
<th>Enterprise NTAuth store, adding root certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ephemeral ports</td>
</tr>
<tr>
<td></td>
<td>calculating</td>
</tr>
<tr>
<td></td>
<td>how View Manager uses</td>
</tr>
<tr>
<td></td>
<td>increasing on a Windows Server computer</td>
</tr>
<tr>
<td></td>
<td>ESX hosts, View Composer</td>
</tr>
<tr>
<td></td>
<td>event database</td>
</tr>
<tr>
<td></td>
<td>creating for View</td>
</tr>
<tr>
<td></td>
<td>SQL Server configuration</td>
</tr>
<tr>
<td></td>
<td>external URLs</td>
</tr>
<tr>
<td></td>
<td>configuring for a View Connection Server instance</td>
</tr>
<tr>
<td></td>
<td>modifying for a security server</td>
</tr>
<tr>
<td></td>
<td>purpose and format</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>F</th>
<th>Firefox, supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>firewall rules</td>
</tr>
<tr>
<td></td>
<td>View Connection Server</td>
</tr>
<tr>
<td></td>
<td>View Transfer Server</td>
</tr>
<tr>
<td></td>
<td>firewalls, configuring</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>G</th>
<th>glossary, where to find</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GPOs, linking to a View desktop OU</td>
</tr>
<tr>
<td></td>
<td>Group Policy Objects, See GPOs</td>
</tr>
<tr>
<td></td>
<td>GroupPolicyFiles directory</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>H</th>
<th>hardware requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>local mode desktops</td>
</tr>
<tr>
<td></td>
<td>PCoIP</td>
</tr>
<tr>
<td></td>
<td>smart card authentication</td>
</tr>
<tr>
<td></td>
<td>View Connection Server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>I</th>
<th>intermediate certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>adding to intermediate certification authorities</td>
</tr>
<tr>
<td></td>
<td>importing to a keystore file</td>
</tr>
<tr>
<td></td>
<td>Intermediate Certification Authorities policy</td>
</tr>
</tbody>
</table>
Internet Explorer, supported versions 9, 16

J
JKS keystores, converting from PKCS#12 78
JVM heap size
  default 64
  increasing 64

K
keyfile property 81
keypass property 81
keytool utility
  adding to the system path 89
  creating a CSR 79
kiosk mode, Active Directory preparation 22

L
license key, View Connection Server 53
local desktop configuration
  adding a View Transfer Server instance 67, 69
  creating a vCenter Server user 49
  hardware requirements 14
  privileges for vCenter Server user 52
locked.properties file 81
Log in as current user feature 96

M
media file formats, supported 19
memory requirements, local mode desktops 14
Microsoft IIS SSL server certificates, using existing 76
Microsoft SQL Server databases 10
Microsoft Windows Installer
  command-line options for silent installation 47
  MSI properties for View Transfer Server 73
  properties for replicated View Connection Server 42
  properties for security server 46
  properties for View Client 103
  properties for View Connection Server 38
uninstalling View Components silently 48
multimedia redirection (MMR) 19

O
ODBC
  connecting to Oracle 11g or 10g 32
  connecting to SQL Server 28
  openssl, converting to PEM format 84
  openssl utility
    adding to the system path 89
    configuring a certificate for View Transfer Server 85
    creating a CSR 84

Oracle 10g, creating a View Composer database with a script 31
Oracle 10g database
  adding an ODBC data source 32
  adding for View Composer 29, 30
  configuring a database user 31
Oracle 11g, creating a View Composer database with a script 31
Oracle 11g database
  adding an ODBC data source 32
  adding for View Composer 29, 30
  configuring a database user 31
Oracle databases 10
organizational units, See OUs
OUs
  creating for kiosk mode client accounts 22
  creating for View desktops 22

P
page-file size, View Connection Server 65
PCoIP, hardware requirements 17
PCoIP Secure Gateway 8
PEM format, exporting from PKCS#12 format 84
PKCS #7 certificate, using with View Transfer Server 84
PKCS#12 file, exporting to PEM format 84
PKCS#12 keystores
  converting to JKS format 78
  determining the type of CA signature 77
  policies
    Intermediate Certification Authorities 26
    Restricted Groups 23
    Trusted Root Certification Authorities 25
printers, setting up 99
professional services 5

R
RDP 18
remote display protocols
  PCoIP 17
  RDP 18
replicated instances
  installing 39
  installing silently 41
  network requirements 9
silent installation properties 42
Restricted Groups policy, configuring 23
root certificates
  adding to the Enterprise NTAuth store 26, 88
  adding to trusted roots 25, 88
  importing to a keystore file 80

S
security servers
  calculating TCB hash table size 62
configuring a pairing password 42
configuring an external URL 57
configuring to use a certificate 81
installer file 43
installing silently 45
modifying an external URL 58
operating system requirements 8
silent installation properties 46
silent installation
  group policies to allow installation 71, 101
  replicated instances 41
security servers 45
View Client 101
View Client with Local Mode 101
View Connection Server 37
View Transfer Server 71, 72
sizing Windows Server settings
  calculating ephemeral ports 59
  calculation worksheets 63
  increasing ephemeral ports 59, 60
  increasing the JVM heap size 64
  increasing the TCB hash table size 62
smart card authentication
  Active Directory preparation 24
requirements 20
  UPNs for smart card users 25
software requirements, server components 7
SQL Server database
  adding an ODBC data source 28
  adding for View Composer 28
  preparing for event database 92
SQL Server databases 10
SQL Server Management Studio Express, installing 28
SSL
  configuring for client connections 82
  configuring for View Transfer Server communications 87
SSL certificates, See certificates
storetype property 81
streaming multimedia 19
support, online and telephone 5
system page file size, Windows Server 65

T
TCB hash table
  how View uses 61
  increasing size for non-security servers 61
  increasing size for security servers 62
  increasing size on a Windows Server computer 62
TCP ports
  View Connection Server 39
  View Transfer Server 71
technical support and education 5
ThinPrint setup 99
Transfer Server repository, configuring 70
  transmission control block
    how View uses 61
    increasing size for non-security servers 61
    increasing size for security servers 62
trust relationships, configuring for View Connection Server 21
Trusted Root Certification Authorities policy 25, 88

U
uninstalling View components 48
UPNs
  smart card users 25
  View Client 96
  View Client with Local Mode 96
USB printers 100
user accounts
  requirements 49
  vCenter Server 22, 49
  View Composer 23, 49
userPrincipalName attribute 25

V
vCenter Server
  configuring for View Composer 34
  creating a user for local mode 49
  installing the View Composer service 32
  user accounts 22, 49
  vCenter Server instances, adding in View Administrator 53
  vCenter Server user
    local mode privileges 52
    vCenter Server privileges 51
  View Composer privileges 51
  View Administrator
    logging in 52
    overview 52
    requirements 9
View Agent, installation requirements 13
View Client
  installation overview 95
  installing on a Windows PC or laptop 95
  installing silently on a Windows PC or laptop 101
  silent installation properties 103
  starting 95, 96
  supported operating systems 14
  using View Portal to install 98
View Client with Local Mode
  group policies for silent installation 101
  supported operating systems 14
  View clients, configuring connections 56
View components, command-line options for silent installation 47
View Composer, database requirements 10
View Composer configuration
creating a user account 23
creating a vCenter Server user 22, 49
privileges for the vCenter Server user 51
settings in View Administrator 55
View Composer database
ODBC data source for Oracle 11g or 10g 32
ODBC data source for SQL Server 28
Oracle 11g and 10g 29, 30
requirements 27
SQL Server 28
View Composer infrastructure
configuring vSphere 34
optimizing 34
testing DNS resolution 34
View Composer installation
installer file 32
overview 27
requirements overview 9
View Composer upgrade
compatibility with vCenter Server versions 10
operating system requirements 10
requirements overview 9
View Connection Server
certificate authentication 76
hardware requirements 7
View Connection Server configuration
client connections 56
event database 91, 92
external URL 57, 58
first time 52
overview 35
replacing the default certificate 75
server certificate 81
sizing Windows Server settings 59
system page file size 65
trust relationships 21
View Connection Server installation
installation types 35
network configuration 9
overview 35
prerequisites 35
product license key 53
replicated instances 39
requirements overview 7
security servers 43
silent 37
silent installation properties 38
single server 36
supported operating systems 8
virtualization software requirements 8
View desktops, configuring direct connections 56
View Portal, browser requirements 16
View Secure Gateway Server component, increasing the JVM heap size 64
View Transfer Server, certificate authentication 83
View Transfer Server configuration adding an instance 69
Transfer Server repository 70
View Transfer Server installation
group policies for silent installation 71
installer file 67
overview 67
requirements overview 11
silent 71, 72
silent installation properties 73
storage requirements 12
supported operating systems 12
virtual machine requirements 11
virtual printing feature 99
vSphere, configuring for View Composer 34

W
Web browser requirements 9, 16
Windows 7 requirements, local mode desktops 14
Windows computers, installing View Client 95
Windows Server, system page file size 65
worksheets, calculating ephemeral ports and TCB has table size 63
Wyse MMR 19