VCP5-DT – Installation Guide Notes

Chapter 1 - System Requirements for Server Components

View Connection Server Requirements

Processor – P4 2.0 Ghz or higher | 4 CPUs
Networking – one or more 10\100 Mbps NICs | 1 Gbps NICs
RAM W2K8 64 – 4 GB | 10 GB Recommended (50 or more deployments)
RAM W2K3 32 R2 – 2 GB | 6 GB Recommended | Enable PAE

View CS – Use static IP
These requirements also apply to additional View Connection Server instances that you install for high availability or external access

Supported Operating Systems for View Connection Server
These operating systems support all View Connection Server installation types, including **standard, replicated, security-server,** and **transfer** Server installations
W2K8 R2 64 bit – Standard\Enterprise None or SP1
W2K3 R2 32 bit – Standard\Enterprise SP2

Virtualization Software Requirements for View Connection Server
-vSphere 4.0 Update 3 or later
-vSphere 4.1 Update 1 or later
-vSphere 5.0 or later

For replicated View CS instances, use **high-performance LAN** and do not use WAN

View Administrator Requirements - **IE 7, 8, 9 | Firefox 3.0 & 3.5**

View Composer Requirements
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

vCenter Server Version	Operating System	Edition	Service Pack
4.0 U3 and later	W2K8 R2	Std or Ent	None or SP1
4.1 U1 and later	W2K8 R2	Std or Ent	None or SP1
5.0 and later	W2K8 R2	Std or Ent	None or SP1

Database Requirements for View Composer

Database	vC 5.0 and later	vC 4.1 U1 and later	vC 4.0 U3 and later
MS SQL 2005 Exp Edition	No	Yes	Yes
MS SQL 2005 SP3 and later Std\Ent 32 and 64 bit	Yes	Yes	Yes
MS SQL 2008 R2 Express	Yes	No	No
MS SQL 2008 SP1 and later Std\Ent 32 and 64 bit	Yes	Yes	Yes
Oracle 10g R2	Yes	Yes	Yes
Oracle 11g R2 with Oracle 11.2.0.1 Patch 5	Yes	Yes	Yes

Sysprep is supported for linked clones only on vSphere 4.1 software. You cannot use Sysprep on vSphere 4.0 or VI 3.5 software

View Transfer Server Requirements
-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

You must configure the virtual machine that hosts View Transfer Server with an **LSI Logic Parallel SCSI controller**

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

Operating System	Version	Edition	Service Pack	Minimum RAM
W2K8 R2	64 bit	Std\Ent	None or SP1	4GB
W2K3 R2	32 bit	Std\Ent	SP2	2GB

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

Recommended maximum number of concurrent disk transfers that View Transfer Server can support is **20 – View 5.0 and 4.6**
Recommended maximum number of concurrent disk transfers that View Transfer Server can support is **60 – View 4.5 (Tested by VMware)**

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

Chapter 2 - System Requirements for Client Components

Supported Operating Systems for View Agent

Guest OS	Version	Edition	Service Pack
Windows 7	64 | 32	Ent\Prof	None or SP1
Windows Vista	32	Bus\Ent	SP1 & SP2
Windows XP	32	Prof	SP3
W2K8 R2 TS	64	Std	None or SP1
W2K8 TS	64	Std	SP2
W2K3 R2 TS	32	Std	SP2
W2K3 TS	32	Std	SP2

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
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 View Client and View Client with Local Mode

Windows 7	**64 | 32**	**H\E\P\U**	**None or SP1**
Windows Vista	**32**	**H\B\E\U**	**SP1 & SP2**
Windows XP	**32**	**H\P**	**SP3**

View Client with Local Mode is supported only on Windows systems and only on physical computers

*Checking out a View desktop that uses virtual hardware version 8 is **not supported**. In vSphere 5, create virtual machines that will be sources for local mode desktops with virtual hardware version 7

Local mode - The maximum amount of memory for each View desktop on 32-bit client computers is 8GB and on 64-bit computers it is 32GB
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

Remote Display Protocol and Software Support
PCoIP
For users outside the corporate firewall, you can use this protocol with your company's VPN or with View security servers
You can use up to four monitors and adjust the resolution for each monitor separately, with a resolution of up to 2560x1600 per monitor
(EQ) When 3D feature is enabled, up to 2 monitors are supported with a resolution of up to 1920x1200
For 3D applications such as Windows Aero themes or Google Earth, the Windows 7 View desktop must have virtual hardware version 8 from vSphere 5 and later.
*You must also turn on the pool setting called **Windows 7 3D Rendering**.

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

RDP
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

View Agent installer configures the local firewall rule for inbound RDP connections. Port **3389**

Client hardware requirement - **128MB RAM**

Multimedia Redirection (MMR)
View Client and View Client with Local Mode support MMR on the following operating systems: **Windows XP | Windows XP Embedded | Windows Vista**
For best quality, use Windows Media Player 10 or later. Port **9427**
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 - Adobe Flash bandwidth reduction is available for IE 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 - Smart cards with local desktops, you must select a 1024-bit or 2048-bit key size. Smart card authentication is **not** supported by View Client for Mac or View Administrator

Chapter 3 - Preparing Active Directory
View uses your existing Microsoft Active Directory infrastructure for user authentication and management. Supports W2K, W2K3, W2K8 AD's

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 - Use vdmadmin command with (-N)

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
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
Create dedicated OUs and groups in Active Directory for kiosk mode client accounts

Creating Groups for View Users
VMware View Users for your View desktop users and another group called VMware View Administrators is a good practice

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
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

Create a User Account for View Composer (D – Default)
*(D)List Contents | (D) Read All Properties | **Write All Properties** | (D) Read Permissions | **Create Computer Objects | Delete Computer Objects***

Configure the Restricted Groups Policy
*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

Using View Group Policy Administrative Template Files
View includes several component-specific group policy administrative (ADM) template files - \VMware\VMware View\Server\Extras\GroupPolicyFiles
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

Prepare Active Directory for Smart Card Authentication
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
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

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

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

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 – Use **certutil** command to publish the certificate to the Enterprise NTAuth Store

Chapter 4 – 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
*You must have a license to install and use the View Composer feature

Prepare a View Composer Database
View Composer service does not include a database by default. Must create one before installing View Composer
(EQ) View Composer database stores information about:
1. vCenter Server connections
2. Active Directory connections
3. Linked-clone desktops that are deployed by View Composer
4. Replicas that are created by View Composer

Each instance of the View Composer service must have its own View Composer database

Create a SQL Server Database for View Composer
Add an ODBC Data Source to SQL Server (System DSN)
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
-If the database resides on the same system as vCenter Server, you can use the **Integrated Windows Authentication security**
-If the database resides in a remote system, you can use the **SQL Server Authentication**

Create an Oracle Database for View Composer
View Composer can store linked-clone desktop information in an Oracle 11g, 10g, database
You can add a new View Composer database by using the Oracle Database Configuration Assistant or by running a SQL statement
Database Credentials page, select **Use the Same Administrative Passwords for All Accounts** and type a password
You can also use a SQL Statement to Add a View Composer Database to an Oracle Instance
Configure an Oracle Database User for View Composer - By default, the database user that runs the View Composer database has Oracle system administrator permissions
Add an ODBC Data Source to Oracle 11g or 10g (System DSN)

Install the View Composer Service
You install the View Composer service on the Windows Server computer on which vCenter Server is installed
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
Check the Firewall.
(EQ) On Windows Server 2008 computers, you might have to right-click the installer file and select **Run As Administrator**
*Create or use the default SSL certificate for the View Composer Service

Configuring Your Infrastructure for View Composer
Use vSphere DRS. DRS efficiently distributes linked-clone virtual machines among your hosts
Storage vMotion is not supported for linked-clone desktops
*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
*To test DNS operation, ping the Active Directory and View Connection Server computers by name

---

Chapter 5 - Installing View Connection Server
Installing the View Connection Server Software
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
*To install View Connection Server, you must use a domain user account with administrator privileges on the system

Install View Connection Server with a New Configuration
-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

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
MSI runtime engine 2.0 or later is required
/v"/qn VDM_SERVER_INSTANCE_TYPE=1"

Install a Replicated Instance of View Connection Server
(Required for silent installation) **ADAM_PRIMARY_NAME** - The host name or IP address of the existing View Connection Server instance you are replicating

Install a Security Server instance
To install a security server, you must configure a security server pairing password. The View CS installation program prompts you for this password during the installation process
(EQ) Security Server instance - An instance of View Connection Server that adds an additional layer of security between the Internet and your internal network
-VMware View Security Server
-VMware View Framework Component
-VMware View Security Gateway Component
-VMware View PCoIP Secure Gateway

External URL - type the external URL of the security server for View Clients that use the RDP or PCoIP display protocols - https://view.example.com:443
PCoIP External URL text box, type the external URL of the security server for View Clients that use the PCoIP display protocol - 100.200.300.400:4172

Configuring User Accounts for vCenter Server and View Composer
-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

*.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. vSphere Client -> **View Composer Administrator**
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 -> **Local Mode Administrator**
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 ->**View Manager Administrator**

Configuring View Connection Server for the First Time
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

Initially, all users who are members of the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer are allowed to log in to View Administrator.
After you log in to View Administrator, you can use **View Configuration > Administrators** to change the list of View Manager Administrators

*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
To add a vCenter Server, use its FQDN name. Ex: **vcenterserver.vdi.com**

Configure View Composer Settings for vCenter Server
*To add View Composer in View Manager, in user credentials when adding should be like this - **domain.com\admin**

Configure the PCoIP Secure Gateway and Secure Tunnel Connections
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
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
The **secure tunnel** is enabled by default
The **PCoIP Secure Gateway** is disabled by default

Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections
Secure Tunnel - https://view.example.com:443 **|** https://100.200.300.400:443
PCoIP Secure Gateway External URL - 100.200.300.400:4172
*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

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

Sizing Windows Server Settings to Support Your Deployment
Ephemeral Ports – W2K3 – 4000; W2K8 – 16000 ports Maximum
*.On 64-bit VCS, 10GB memory is recommended for 50 or more View desktops deployments

---

Chapter 6 – Installing View Transfer Server
You must install and configure View Transfer Server if you deploy View Client with Local Mode on client computers

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

Configure View Transfer Server with an LSI Logic Parallel SCSI controller
-VMware View Transfer Server,
-View Transfer Server Control Service,
-VMware View Framework Component services

Add View Transfer Server to View Manager
You can add multiple View Transfer Server instances to View Manager
When View Transfer Server is added to View Manager, its DRS automation policy is set to Manual, which effectively disables DRS
After you add View Transfer Server, View Connection Server reconfigures the virtual machine with four SCSI controllers
When the View Transfer Server instance is added to View Manager, the **Apache2.2 service** is started on the View Transfer Server virtual machine
The Apache service uses ports **80 and 443**

Configure the Transfer Server Repository
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
Restrict network access for the repository to View administrators

(EQ) Adding View Transfer Server to View Manager before you configure the Transfer Server repository is a best practice, not a requirement

Transfer Server repository
*Local Transfer Server repository - Ex: C:\TransferRepository\
*Remote Transfer Server repository - Ex: \\Ser.dom.com\TransferRepository\
Domain – do not use the .com suffix

Firewall Rules for View Transfer Server
HTTP – 80 **|** HTTPS – 443

Installing View Transfer Server Silently
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**
/v"/qn VDM_SERVER_INSTANCE_TYPE=4"

Chapter 7 - 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

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

*You can request an SSL server certificate that is specific to a web **domain** such as www.mycorp.com
*You can request a wildcard SSL server certificate that can be used **throughout a domain** such as *.mycorp.com
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
*You can configure different levels of SSL security checking in View Client for Windows

Configuring SSL Certificates for <u>View Connection Server and Security Server</u>
1. Add the **keytool** utility to your system path on the View Connection Server instance or security server
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

1. Use an Existing SSL Certificate and Private Key
To use an existing certificate, you also need the accompanying private key PKCS#12 file format, formerly called PFX file format, and includes both the server certificate and the private key (.pfx or .p12 extension)

*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

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 **(keytool)**

2. 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
*CA-signed certificate is better than Self-signed certificate. Self-signed can be used for **testing** purpose

Obtain a Signed Certificate from a CA for Use with a View Connection Server Instance or Security Server
You must use keytool to generate a **keystore file** and a **certificate signing request (CSR) file**
Determine the fully qualified domain name **(FQDN)** that client computers use to connect to the host
IMPORTANT: If you type your name, the certificate will be invalid (in certificates)

Import a Root Certificate into a Keystore File
*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

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

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

3. Configure a <u>View Connection Server Instance or Security Server to Use a New Certificate</u>
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
***Restart** the **View Connection Server service or Security Server service** to make your changes take effect

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
IMPORTANT: If you disable or enable SSL for client connections, all existing client connections are terminated
*Restart the **View Connection Server service** to make your changes take effect

Configuring SSL Certificates for <u>View Transfer Server</u>
If you enable SSL for local mode operations and local desktop provisioning, View Transfer Server instances require an SSL server certificate
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

1. Add the **openssl** utility to your system path - You use the **openssl** utility to create and manage certificates for **View Transfer Server**
2. Determine your certificate configuration path: Obtain new SSL, existing SSL in PKCS#12 format or existing SSL in PKCS#12 format and separate private key
NOTE: A certificate that is used with View Transfer Server must be in **PEM** format
3. Configure View Transfer Server to use the SSL server certificate
4. Configure settings in **View Administrator** to use SSL for local mode provisioning and other local mode operations

Prepare an Existing Certificate in PKCS#12 Format for Use with View Transfer Server - 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

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

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

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
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
*You must add the SSL server certificate to the View Transfer Server certificate directory and configure the Apache configuration file to specify the name of the new SSL server certificate
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\httpd\conf on the View Transfer Server host
3. 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
4. Restart the View Transfer Server service to make your changes take effect
5. 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

Configure SSL for View Transfer Server Communication
The SSL settings for View Transfer Server communications and data transfers are specific to a single View Connection Server instance
*SSL is disabled by default for View Transfer Server communications and data transfers

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**
Use the Client Configuration ADM template file to change the verification mode
Verification Modes: Warn but allow, No security, Full security

Additional SSL Configuration Tasks
When you configure SSL certificates for View servers, you might need to perform certain additional tasks
1. Add SSL Certificates in Active Directory (certutil)
For CAs that is not well known, you must add the root CA certificate and intermediate certificate in Active Directory

If you use a little-known CA to provide SSL server certificates:
1. Add the root certificate to the Enterprise NTAuth store
2. Trusted Root Certification Authorities group policy in Active Directory

If your SSL server certificates are signed by an little-known intermediate CA
1. Add the intermediate certificate to the Intermediate Certification Authorities group policy in AD

Chapter 8 - 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
1. Add a Database and Database User for View Events
You create an event database by adding it to an existing or new database server
*You do not need to create an ODBC data source for this database
*You should use the **SQL Server Authentication** method of authentication
Prepare an SQL Server Database for Event Reporting
*You must configure the correct TCP/IP properties and verify that the server uses SQL Server Authentication

Configure the Event Database
Microsoft SQL Server – Port **1433**
Oracle – Port **1521**
In the View Administrator Dashboard, the System Component Status displays the event database server under the Reporting Database heading

Chapter 9 - Installing and Starting View Client
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
Install the Windows-Based View Client or View Client with Local Mode
If you plan to install the **USB Redirection** component, verify that the Windows Automatic Update feature is not turned off on the client computer
VMware View Client service is installed on the Windows client computer
Service name for View Client is **wsnm.exe**
Service name for the USB component is **wsnm_usbctrl.exe**
Optional settings available in View Clients
1. Log in as current user
2. Use secure connection (SSL)
3. Port
4. Autoconnect

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

Set Printing Preferences for the Virtual Printer Feature on Windows Clients
After a printer is added on the local Windows computer, View adds that printer to the list of available printers on the View desktop
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. Ex: PDF writer to print to a PDF file
Verify that the Virtual Printing component of View Agent is installed on the View desktop. *C:\Program Files\Common Files\VMware\Drivers\Virtual Printer*

Installing View Client Silently
Set Group Policies to Allow Silent Installation of View Client with Local Mode
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

Use **ADDLOCAL** if you want to install specific features that the View Client installer configures. ADDLOCAL=ALL install all the features available in the View Client (Core – required if the ADDLOCAL is used)

Silent Installation Feature	Custom setup option in an Interactive Installation
Core (Required when ADDLOCAL is Used)	None (Core is installed by default)
MVDI (Client with Local mode)	None (Installed by default and not available)
ThinPrint	Virtual Printing
TSSO	Single Sign-on
USB	USB Redirection