



Securing VMware® View™ Communication Channels with SSL Certificates

TECHNICAL WHITE PAPER

Table of Contents

About VMware View	3
Changes in VMware View 5.1.....	3
SSL Authentication Mechanism.....	4
X.509 Certificate Validation Flow	4
X.509 Certificate Configuration on Different Components and Integration with VMware View.....	6
X.509 Certificate, Issued by Trusted Certification Authority, Configuration on Secure Gateway Components	6
X.509 Certificate, Issued by Trusted Certification Authority, Configuration on View Composer.....	6
X.509 Certificate, Issued by Trusted Certification Authority, Configuration on vCenter Server.....	6
Revocation Checking.....	7
Other Revocation Check Settings.....	7
Certificate Types and Their Use in VMware View.....	8
Events and Logs to Troubleshoot	8
Common Misconfigurations	8
Self-Signed Certificate Configured on a Connection Server / Security Server.....	9
Trusted CA-Signed Certificate Configured on a Connection Server / Security Server	9
Trusted CA-Signed Certificate Configured on a Connection Server / Security Server Expires.....	9
Trusted CA-Signed Certificate Configured on a Connection Server / Security Server About to Expire.....	9
Trusted CA-Signed Certificate Configured on a Connection Server / Security Server Revoked.....	9
About the Authors.....	10
Acknowledgements	10

About VMware View

VMware® View™ is a best-in-class enterprise desktop virtualization platform. The VMware View solution separates the personal desktop environment from the physical system by moving desktops to a datacenter, from which the users can access the desktops using a client-server computing model. VMware View incorporates a rich set of features required for any enterprise deployment by providing a robust platform for hosting virtual desktops from VMware vSphere™. Additional capabilities such as distributed infrastructure services and virtual desktop failover and recovery make it an ideal solution for desktop virtualization.

VMware View consists of various components such as Connection Server, Security Server, View Composer, and vCenter™ Server. Communication between each of these components is established in a secure manner. The communication channel is secured using a Secure Socket Layer (SSL) encryption mechanism. This paper provides a technical overview of these features, in addition to the specific configurations required in an ideal implementation. Overall, this paper covers:

- A brief discussion of SSL authentication
- X.509 certificate validation flow on Secure Gateway components
- X.509 certificate configuration in different View components and SSL integration with VMware View
- Basic troubleshooting

Changes in VMware View 5.1

VMware View 5.1 has many new features and enhancements. This paper focuses on enhancements to HTTP communication between different View components. In VMware View 5.0, VMware supported JKS and PKCS12 file-based certificate stores for configuring certificates on View components. From View 5.1 onward, VMware View instead uses the Windows Certificate Store. This change allows better integration with mainstream certificate management processes. When upgrading to View 5.1, existing JKS and PKCS12 certificate stores are automatically migrated to the Windows Certificate Store. Refer to the [VMware View 5.1 Readme](#) documentation for detailed information.

The use of SSL is now mandated for HTTP communication between View components. Although a trust-on-first-use mechanism is included, it is a best practice to place valid certificates signed by a trusted Certificate Authority (CA) on all View components. In View 5.1, the View Administrator dashboard shows the certificate's present health status in the appropriate components.

Figure 1 depicts the use of Secure SSL Communication between different VMware View components. In the case of vCenter Server and View Composer, Administrators are given the option to accept the existing self-signed or invalid certificates after verifying the identity of the certificate from the View Administrator UI.

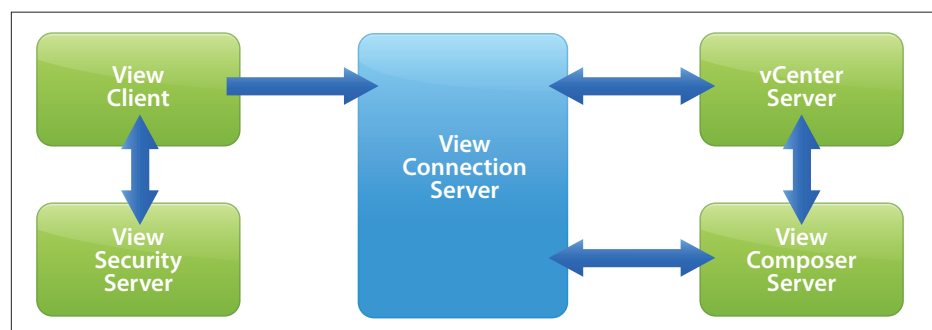


Figure 1: Channels Protected by SSL in VMware View

SSL Authentication Mechanism

SSL authentication is primarily based on the Transport Layer Security (TLS) protocol. The main goal of TLS is to provide privacy and data integrity between two communicating applications. The TLS Handshake Protocol authenticates the server with the client and, optionally, the client with the server. TLS also negotiates an encryption algorithm and cryptographic keys before the application protocol (server and client) transmits or receives its first byte of data. The Handshake Protocol creates a secure channel by:

- Authenticating peers (client or server) using asymmetric (public-private) keys
- Agreeing upon cryptographic protocols to be used, such as 3DES, RSA
- Negotiating a shared secret

Once the handshake is completed between peers, the peers start to communicate in a secured fashion using the negotiated encryption algorithm and cryptographic keys, which negate any eavesdropping and man-in-the-middle attacks.

Detailed information about the SSL Authentication Mechanism can be found in [The TLS Protocol: Version 1.0](#) and [The Transport Layer Security \(TLS\) Protocol: Version 1.2](#).

X.509 Certificate Validation Flow

This section describes the validation flow of x.509 certificates, the standard form of public key certificates. These are configured on the Connection Server, Security Server, View Composer and vCenter Server. The certificate health of each of these components is displayed in the View Administrator dashboard, as shown in Figure 2.

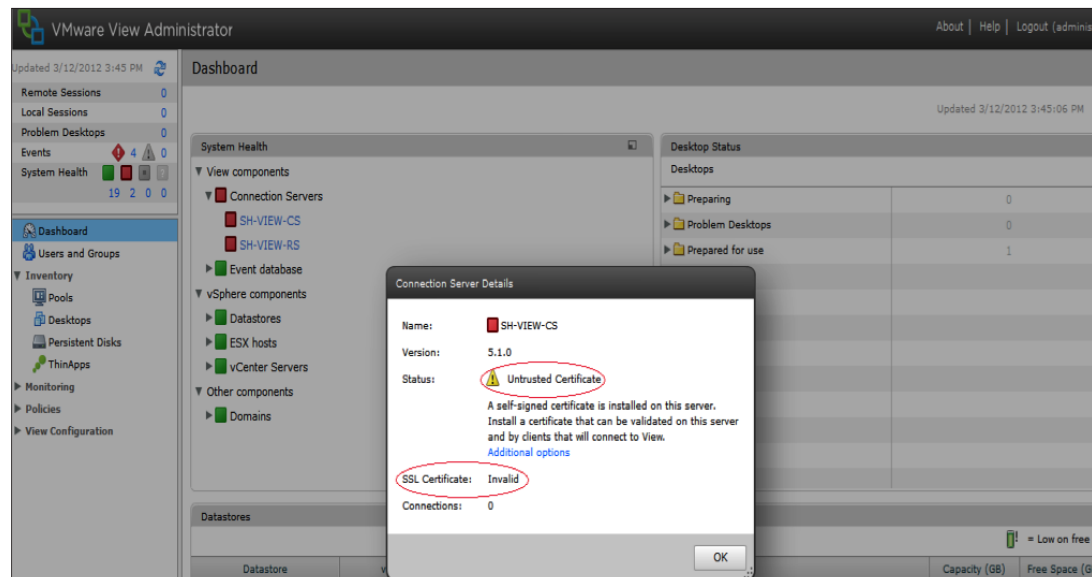


Figure 2: View Administrator Showing the Certificate Health of a Secure Gateway Component

A default certificate is generated for each of these components. It is a best practice to replace these certificates with certificates issued by a trusted CA. Configuring certificates in each of these components is discussed later in the [X.509 Certificate Configuration](#) section.

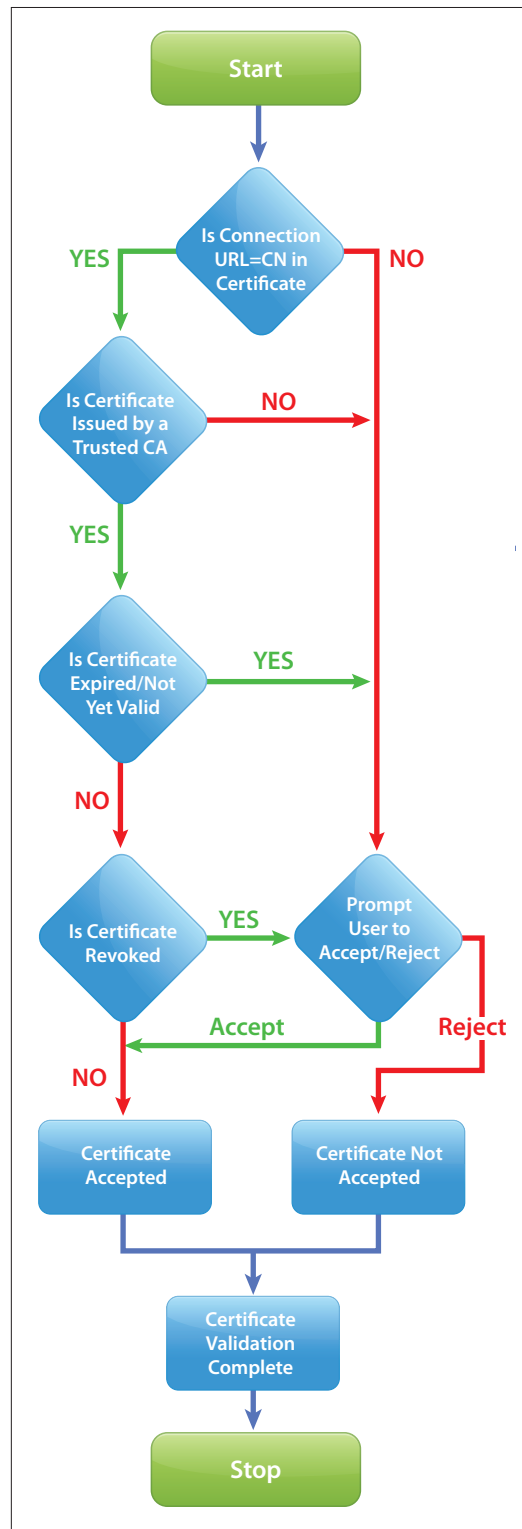


Figure 3: Flow of Certificate Validation in VMware View Components

Each Connection Server validates the certificate of the other components connected to it. The flow chart in Figure 3 depicts the flow of certificate validation in VMware View. The validation consists of the following checks:

- Hostname match** – The Connection Server checks that the server name portion of the connection URL (in the case of a Security Server, the configured External URL) matches one of the subject names in the presented certificate. If there is a mismatch, the status of the appropriate component displays as *Server's Certificate does not match the URL* in the View Administrator dashboard.
- Certificate issuer's verification** – The Connection Server verifies the authenticity of the certificate issuer and verifies that the issuer's certificate is trusted.
- Certificate Expired/Not Yet Valid** – The validity of the certificate in the certificate chain is checked by verifying if the current date and time fall within the validity period of the issued certificate. If they do not, an appropriate status for the component—either *Certificate Expired* or *Certificate Not Yet Valid*—is shown in the View Administrator Dashboard.
- Certificate revocation checking** – VMware View supports Revocation Checking, a technique to ensure that the certificate issuer has not withdrawn the certificate for some reason. View performs revocation checking using both CRLs (Certificate Revocation Lists) and OCSRs (Online Certificate Status Protocols). The CRL distribution point / OCSR responder address specified in the certificate is used for revocation checking. If the certificate is found to be revoked or if the Certificate Distribution Point (CDP) is not accessible, the status of the appropriate component in View Administrator displays as *Revocation status cannot be checked*.

Note: The revocation check happens for the whole chain except the root. This means that all the certificates present in the chain up to the root certificate are checked for revocation. The root certificate is excluded because active management of the root certificate store should ensure that only current, unrevoked certificates will be trusted. If you do not feel confident that the root certificate store is fully up to date, it is advisable to extend the scope of revocation checking to include root certificates. If any of the certificates fails the revocation check, the status of the appropriate component in the View Administrator displays as *Server Certificate has been revoked*.

X.509 Certificate Configuration on Different Components and Integration with VMware View

X.509 Certificate, Issued by Trusted Certification Authority, Configuration on Secure Gateway Components

During installation of the VMware View Connection Server and Security Server, a default certificate is generated and configured. It is recommended that you replace this default certificate with a certificate issued by a trusted Certificate Authority (CA).

The complete procedure for configuring x.509 certificates on Secure Gateway components is specified in the *Configuring SSL Certificates for View Servers* section of the [VMware View 5.1 Installation guide](#).

Note: In cases where the Secure Gateway components are being upgraded and the previous version was configured with valid certificates signed by a trusted CA, those certificates will be automatically migrated to the Windows Certificate Store at the time of installation.

X.509 Certificate, Issued by Trusted Certification Authority, Configuration on View Composer

During installation of VMware View Composer, a default certificate is generated and configured. It is recommended that you replace this default certificate with a certificate issued by a trusted Certificate Authority (CA).

Note: If you already have a certificate issued by a trusted CA, you can point the Composer installer to the certificate at the time of installation. Detailed steps for configuring an x.509 certificate on View Composer are specified in the *Install the View Composer Service* section of the [VMware View 5.1 Installation guide](#). If the composer needs to be configured with certificates after installation, please follow the steps specified in the *Configuring an SSL Certificate for View Composer* section of the [VMware View 5.1 Installation guide](#).

X.509 Certificate, Issued by Trusted Certification Authority, Configuration on vCenter Server

During installation of VMware vCenter Server, a default certificate is generated and configured. It is recommended that you replace this default certificate with a certificate issued by a trusted Certificate Authority (CA).

For the complete procedure for replacing default certificates with valid certificates signed by a trusted CA, refer to the [vCenter Server documentation](#).

Revocation Checking

VMware View 5.1 supports revocation checking of SSL certificates. This can be configured in the registry or by setting GPO policy.

To configure revocation check types, edit the following registry settings or set a GPO policy on the Connection Servers:

Add a string type registry key ***CertificateRevocationCheckType*** to ***Software\Policies\VMware, inc.\VMware VDM\Security***.

The following revocation check types are supported by VMware View 5.1.

- None – Set ***CertificateRevocationCheckType*** = **1**. No revocation checking is done if this option is set.
- EndCertificateOnly – Set ***CertificateRevocationCheckType*** = **2**. Revocation checking is done only for the end certificate in the chain.
- WholeChain – Set ***CertificateRevocationCheckType*** = **3**. A complete path is built for the certificate, and a revocation check is done for all certificates in the path.
- WholeChainButRoot – Set ***CertificateRevocationCheckType*** = **4**. A complete path is built for the certificate, and a revocation check is done for all certificates in the path except for the Root CA certificate (default value).

Note: As per [RFC 4158](#), the options EndCertificateOnly = 2, WholeChain = 3, and WholeChainButRoot = 4 yield the same revocation check results.

Other Revocation Check Settings

Additional revocation check setting supported by VMware View 5.1 include:

Software\Policies\VMware, inc.\VMware VDM\Security\ CertificateRevocationCheckCacheOnly.

“False” (default) – Disable caching revocation responses.

“True” – Enable caching revocation responses.

Software\Policies\VMware, inc.\VMware VDM\Security\ CertificateRevocationCheckTimeOut.

Cumulative timeout across all revocation check intervals in milliseconds. If not set, default is set to ‘0’, which means Microsoft defaults are used.

Please visit Microsoft-TechNet for detailed information on [Certificate Status Checking](#).

Certificate Types and Their Use in VMware View

View supports different types of certificates to fulfill the various deployment scenarios at customer sites. The certificates can be classified into single-server name certificates and multiple-server name certificates.

A single-server name certificate contains a single URL that identifies the server for which the certificate is issued. This type of certificate is used when a connection broker is accessed only from within the internal network or only from the external network, i.e., the server has a single Fully Qualified Domain Name.

Multiple-server name certificates are used in environments where the View Connection Server is accessed from both internal and external networks. Such configuration requires a connection server to have multiple Fully Qualified Domain Names, e.g., one for the internal network and one for the external network.

Multiple-server name certificates support more than one SAN (Subject Alternative Name) per single certificate. This type of certificate is also used if SSL offloaders are placed between View clients and the connection server, and when a tunneled connection with the Security server is enabled.

A wildcard certificate is a certificate issued to all the servers in an organization's domain. The Fully Qualified Domain Name in a wildcard certificate would typically follow the format ***.organization.com**. A wildcard certificate is less secure than a SAN certificate since, if one server or subdomain is compromised, the entire environment is exposed.

Events and Logs to Troubleshoot

This section discusses the View Connection Server logs and events you can examine for troubleshooting. The section also covers scenarios where corrupted certificates have been configured, certificates are missing Friendly Name, and where the private key of the certificate is not marked as Exportable.

Note: View Connection server logs can be found under `<DriveLetter>:\ProgramData\Application Data\VMware\VDM\logs`.

Common Misconfigurations

The following log lines indicate that the private key is not marked as Exportable.

```
KeyVault CryptExportKey get size FAILED, error=<Error code in Hex> (Key not
valid for use in specified state.)
```

The following log lines could indicate that the External URL does not match the Common Name of the certificate.

```
Server's certificate does not match the URL
```

If the server name part of a secure gateway's External URL does not match any of the subject names in the certificate, then the Certificate Health is reported as invalid.

The Log line

```
ATTR_SG_URL","type":"STRING","stringValue":"https://<FQDN>:443
```

defines the Secure Gateway External URL.

Self-Signed Certificate Configured on a Connection Server / Security Server

The log line

```
"ATTR_SG_CERTDEFAULT","type":"STRING","stringValue":"true"
```

indicates that this secure gateway instance is configured with a self-signed certificate.

The logs also contain the following lines

```
ATTR_SG_CERTVALID","type":"STRING","stringValue":"false" and ATTR_SG_CERTINVALID_REASON","type":"STRING","stringValue":"NOT_TRUSTED",
```

which indicate that the certificate is not valid, and that the certificate cannot be trusted because it is not issued by a trusted CA. In addition, the event "Certificate is invalid for Secure Gateway at address <NetBIOS name>" is raised in View Administrator as a warning for View administrators.

Trusted CA-Signed Certificate Configured on a Connection Server / Security Server

The log line

```
"ATTR_SG_CERTDEFAULT","type":"STRING","stringValue":"false"
```

indicates that this secure gateway instance is not configured with a self-signed certificate. The logs also contain the line "ATTR_SG_CERTVALID","type":"STRING","stringValue":"true", meaning that the configured certificate is valid.

Trusted CA-Signed Certificate Configured on a Connection Server / Security Server Expires

The log line

```
"ATTR_SG_CERTVALID","type":"STRING","stringValue":"false"
```

indicates that the configured certificate is invalid. The log line

```
"ATTR_SG_CERTINVALID_REASON","type":"STRING","stringValue":"EXPIRED"
```

indicates the reason for invalidating the configured certificate. In this case, it states that the certificate has expired. In addition, the event "Certificate is invalid for Secure Gateway at address <NetBIOS name>" is raised in View Administrator as a warning for View administrators.

Trusted CA-Signed Certificate Configured on a Connection Server / Security Server About to Expire

The only difference from the above section is that the log line

```
"ATTR_SG_CERTABOUTTOEXPIRE","type":"STRING","stringValue":"true"
```

indicates that the configured certificate is about to expire. All other log lines in this case are similar to the scenario where the configured certificate is valid. VMware View Administrator also raises an event warning that the configured certificate will expire within <Configured Number of Days>.

Trusted CA-Signed Certificate Configured on a Connection Server / Security Server Revoked

The log line

```
"ATTR_SG_CERTVALID","type":"STRING","stringValue":"false"
```

indicates that the configured certificate is invalid. The log line

```
"ATTR_SG_CERTINVALID_REASON","type":"STRING","stringValue":"REVOKED"
```

indicates the reason for invalidating the configured certificate. In this case, it states that the certificate has been revoked. In addition, the event "Certificate is invalid for Secure Gateway at address <NetBIOS name>" is raised in View Administrator as a warning for View administrators.

About the Authors

Suhas Hariharan is a member of the Technical Staff at VMware. Currently, he is part of the View-Management Quality Engineering team in Bangalore. He has a Master of Technology in Computer Science and Engineering from Manipal University.

Noble Peter is a member of Technical Staff at VMware. Currently, he is part of the View-Management Quality Engineering team in Bangalore. He has an MSc in Digital Design and Embedded Systems from Manipal University.

Acknowledgements

Many thanks to Paul Green, Senior Member of Technical Staff (View Development Team) and Fred Schimscheimer, Senior Technical Marketing Engineering Manager, for their thorough technical review of this white paper.

