# Replacing Default vCenter 5.1 and ESXi Certificates

vCenter Server 5.1
ESXi 5.1

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

EN-000980-05

vmware®

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



**VMware, Inc.**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

# Replacing Default vCenter Certificates

Replacing default SSL certificates for vCenter components with CA-signed SSL certificates helps ensure security. When you install vCenter components such as vCenter Single Sign-On and the vSphere Web Client, the installer generates SSL certificates for each service by default. vCenter Single Sign-On uses the certificates for SSL handshakes and to authenticate solution users. The default certificates are not signed by a commercial certificate authority (CA).

vCenter services that interact with vCenter Single Sign-On and the Lookup Service include the Inventory Service, vCenter Server, and the vSphere Web Client. Each of these services has an identity which is used to create x509 certificates. To help you protect your vCenter components, you can replace default certificates with certificates signed by a certificate authority. There are two ways to replace certificates.

- (Recommended) Use the Certificate Update Automation Tool to replace SSL certificates for vCenter components installed on Windows operating systems. The automation tool helps you plan the process of replacing certificates and guides you through the steps.
- Replace SSL certificates manually.

**NOTE** You must use the manual process to update certificates for third-party components such as load balancers.

## vCenter and ESXi SSL Certificate Requirements

VMware products use standard X.509 version 3 (X.509v3) certificates to encrypt session information sent over Secure Socket Layer (SSL) protocol connections between components.

For example, communications between a vCenter Server system and each ESXi host that it manages are encrypted. Some features, such as vSphere Fault Tolerance, require the certificate verification provided by SSL. The client verifies the authenticity of the certificate presented during the SSL handshake phase, before encryption, which protects against man-in-the-middle attacks.

The vSphere environment requires certificates in several places, as shown in the following list.

- STS certificate - used by Single Sign-On to encrypt the SAML token
- SSO certificates - used by solutions to register themselves to Single Sign-On
- SSL certificates - used for secure communication between clients and the vCenter Server and vSphere Web Client
- Host Certificates - used for communication between vCenter Servers and ESXi hosts.

Each vCenter Server system component, shown in the following list, must have a unique certificate.

- vCenter Inventory Service
- vCenter Single Sign-On

- vCenter Update Manager
- vCenter Orchestrator
- vCenter Server
- vSphere Web Client
- vCenter Log Browser

When you replace default vCenter and ESXi certificates, the certificates you obtain for your servers must be signed and conform to the Privacy Enhanced Mail (PEM) key format. PEM is a key format that stores data in a Base-64 encoded Distinguished Encoding Rules (DER) format.

The key used to sign certificates must be a standard RSA key with an encryption length that ranges from 1024 to 2048 bits (the recommended length).

Certificates signed by a commercial certificate authority, such as Entrust or VeriSign, are pre-trusted on the Windows operating system. However, if you replace a certificate with one signed by your own local root CA, or if you plan to continue using a default certificate, you must pre-trust the certificate by importing it into the local certificate store for each vSphere Client instance.

You must pre-trust all certificates that are signed by your own local root CA, unless you pre-trust the parent certificate, the root CA's own certificate. You must also pre-trust any valid default certificates that you will continue to use on vCenter Server.

# Managing ESXi and vCenter Server SSL Certificates

Certificate Authority (CA) assigned SSL certificates for vSphere are required within many organizations to maintain proper security for regulatory requirements.

For Windows operating systems, use the Certificate Update Automation Tool to simplify the process of updating SSL Certificates.

#### Prerequisites

Each vSphere component requires a unique certificate. Before you begin creating, installing, and replacing SSL certificates, be sure that your vSphere environment meets the following criteria.

- vSphere 5.1.0a or later
- All components for which you are managing certificates are installed
- OpenSSL 0.9.8 (required)

  The tasks in this document assume that you installed OpenSSL in the default directory (`C:\OpenSSL-Win32`). If you installed OpenSSL in a different directory, adjust the paths as needed.

# About the Certificate Update Automation Tool for vCenter

The SSL Certificate Update Automation Tool is a command-line utility that automates self- or CA-signed SSL certificate renewal for vCenter components on Windows operating systems. Updating certificates using the manual process is complex and can introduce errors in your configuration.

## Supported Platforms

The SSL Certificate Update Automation Tool is only available to machines running the Windows operating systems. The tool has been tested and verified on the following operating systems.

- Windows 2003 R2 SP2
- Windows 2008 R2 SP2

### Prerequisites

To run the SSL Certificate Automation Tool, you must have:

- Administrative privileges on the server(s) you are running the tool on. Although non administrator users can download and launch the tool, all operations will fail without the proper permissions.
- Access to each server that has a vSphere components for which the SSL certificate will be updated.
- All vCenter components which will have their certificates updated have already been installed and are running.
- The new certificates already exist and you know the location of the new certificates. For increased security, generate each certificate and private key on the machine where it will be used. The new SSL certificate for each vSphere component must have a unique base DN.

## Replace vCenter Certificates Using the Automation Tool

Use the SSL Certificate Update Automation Tool to replace self-signed or CA-signed SSL certificates for vSphere components on Windows operating systems.

While it is possible to manually replace SSL certificates, the process is complex and prone to mistakes. Whenever possible, use the Automation Tool, which provides step-by-step guidance.

vCenter services that interact with vCenter Single Sign-On and the Lookup Service include the Inventory Service, vCenter Server, and the vSphere Web Client. Each of these services has an identity which is used to create x509 certificates.

#### Prerequisites

Obtain SSL certificates as described in the VMware Knowledge Base article Generating certificates for use with the VMware SSL Certificate Automation Tool (2044696).

#### Procedure

- Follow the steps in the VMware Knowledge Base article Deploying and Using the SSL Certificate Automation Tool (2041600).

## Replace vCenter Certificates Manually

If you are unable to replace vCenter certificates using the automation tool, it is possible to update certificates manually. The SSL Certificate Update Automation Tool is the preferred way to update your SSL certificates.

vCenter services that interact with vCenter Single Sign-On and the Lookup Service include the Inventory Service, vCenter Server, and the vSphere Web Client. Each of these services has an identity which is used to create x509 certificates.

#### Prerequisites

Obtain SSL certificates as described in the VMware Knowledge Base article Creating certificate requests and certificates for vCenter Server 5.1 components (2037432).

#### Procedure

- Follow the steps in the VMware Knowledge Base article Implementing CA signed SSL certificates with vSphere 5.1 (2034833).

# About SSL Certificates on ESXi

Replace default certificates on ESXi with those signed by an internal certificate authority or public key infrastructure (PKI) service. Alternatively, purchase a certificate from a trusted commercial security authority.

**NOTE** Use commercially signed certificates for systems that are exposed to the Internet.

When you replace default server certificates in a production environment, deploy new certificates in stages, rather than all at the same time. Make sure that you understand the process as it applies to your environment before you replace certificates.

Ensure that your environment has the required software installed before you begin replacing default ESXi certificates.

- Microsoft CA (2000 or higher), with Web Server template
- Microsoft Visual C++ 2008 Redistributable Package (x86) installed on the system where you will generate the certificate-signing request
- OpenSSL 0.98r or higher installed on the system where you will generate the certificate-signing request
- Putty or other SSH client
- WinSCP or other SFTP/SCP client
- vCenter Server 5.1
- ESXi 5.1

# Replace ESXi Certificates Manually

Replacing default certificates on ESXi hosts is a manual process.

### Prerequisites

Obtain SSL certificates as described in the VMware Knowledge Base article Creating certificate requests and certificates for vCenter Server 5.1 components (2037432).

### Procedure

- Follow the steps in the VMware Knowledge Base article Configuring CA-signed certificates for ESXi 5.x hosts (2015499).

# Replace SSL Certificates on vCenter Server Appliance

Replacing CA-signed SSL certificates on vCenter Server Appliance is a manual process. You cannot use the automation tool to update certificates on the appliance.

To replace CA signed SSL certificates on a vCenter Server Appliance, see the VMware Knowledge Base article Configuring certificates signed by a Certificate Authority (CA) for vCenter Server Appliance 5.1 (2036744).

# Replace vCenter Server Heartbeat Certificates

If you have a problem with the current certificate, or if your corporate security policy requires doing so, you can replace default vCenter ServerHeartbeat certificates.

### Prerequisites

- Install OpenSSL on the system where you will replace the certificate.
- Obtain the certificate files `rui.crt`, `rui.key`, and `rui.pfx`.

### Procedure

1 Download the `SSLImport.jar` utility from the VMware Knowledge Base article Replacing SSL Certificates for vCenter Server Heartbeat 6.x (KB 2013041).

2 Follow the steps in the knowledge base article to replace the certificate.

## Update the Certificate Trust Store for vCenter Server Components

Before you can install the certificate for vCenter Server components, you must have a trust store for the CA signed certificates, including the root and intermediary certification authorities.

A trust store is a directory of trusted X.509 certificates.

---

**NOTE** If you are running vCenter Server in a virtual machine, take a snapshot before starting this process to ensure that you can revert to it if necessary. Delete the snapshot after the process is complete.

---

### Prerequisites

- Verify that trusted certificates are kept in separate files, with one certificate for each file.
- Verify that certificates are in X.509 PEM format.
- Verify that certificates have names in the form *hash*.0 or have symbolic links to the files using that form.

  *hash* is the hashed certificate subject name. See the OpenSSL documentation for the x.509 utility.
- Certificates are either self-signed CA root certificates or intermediate certificates whose chain is included in the root certificate.

### Procedure

1 Log in to the vCenter Single Sign-On Server.

  In this example, the files are located in `C:\certs`.

2 Copy the root certificate from the certification authority to the VMware SSL directory.

  For example, copy the `C:\certs\Root64.cer` file to `C:\ProgramData\VMware\SSL\`. This certificate is the root certificate for the certification authority which is being used.

3 Rename the `current ca_certificates.crt` to `ca_certificates.bak`, and then rename `Root64.cer` to `ca_certificates.crt`.

4 Type the following command to compute the hash.

  ```
  openssl x509 –subject_hash –noout –in c:\certs\Root64.cer
  ```

  The valid hash is returned.

5 Create a file named *`hash`*`.0` using the hash returned in the previous step.

  The content of the file should contain the certificate in which hash is used for the name of the file.

  ---

  **IMPORTANT** The hash must be created with OpenSSL v0.9.8, as this is the version which vCenter uses. If created with another version the hash might not be correct.

  ---

6 Repeat this task for other intermediary Certificate Authorities.

  If there are intermediate certificate authorities, there will be a file for each intermediate authority with the content of the intermediate certificate in the file. If you are using intermediate certificate authorities, you also need to append each certificate authority to the ca_certificates.crt file. To do this run the following command:

```
more intermediateCA.cer >> ca_certificates.crt
```

where *intermediateCA* is the certificate for the intermediate CA. Repeat this step for each intermediate CA that is in the certificate chain.

The certificates are updated in the trust store.

# Troubleshooting vCenter Server Certificates

These topics describe some of the issues you might encounter when you work with vCenter and ESXi certificates.

## New vCenter Server Certificate Does Not Appear to Load

After you replace default vCenter Server certificates, the new certificates might not appear to load.

### Problem

When you install new vCenter Server certificates, you might not see the new certificate.

### Cause

Existing open connections to vCenter Server are not forcibly closed and might still use the old certificate.

### Solution

To force all connections to use the new certificate, use one of the following methods.

- Restart the network stack or network interfaces on the server.
- Restart the vCenter Server service.

## vCenter Server Cannot Connect to Managed Hosts

After you replace default vCenter Server certificates and restart the system, vCenter Server might not be able to connect to managed hosts.

### Problem

vCenter Server cannot connect to managed hosts after server certificates are replaced and the system is restarted.

### Solution

Log into the host as the root user and reconnect the host to vCenter Server.

## vCenter Server Cannot Connect to the Database

After you replace default vCenter Server certificates, you might be unable to connect to the vCenter Server database.

### Problem

vCenter Server is unable to connect to the vCenter Server database after you replace default vCenter Server certificates, and management web services do not start.

### Cause

The database password must be updated in its encrypted form.

### Solution

Update the database password by running the following command: `vpxd -P pwd`.

## Cannot Configure vSphere HA When Using Custom SSL Certificates

After you install custom SSL certificates, attempts to enable vSphere High Availability (HA) fail.

### Problem

When you attempt to enable vSphere HA on a host with custom SSL certificates installed, the following error message appears: `vSphere HA cannot be configured on this host because its SSL thumbprint has not been verified.`

### Cause

When you add a host to vCenter Server, and vCenter Server already trusts the host's SSL certificate, `VPX_HOST.EXPECTED_SSL_THUMBPRINT` is not populated in the vCenter Server database. vSphere HA obtains the host's SSL thumbprint from this field in the database. Without the thumbprint, you cannot enable vSphere HA.

### Solution

1 In the vSphere Client, disconnect the host that has custom SSL certificates installed.

2 Reconnect the host to vCenter Server.

3 Accept the host's SSL certificate.

4 Enable vSphere HA on the host.

## Unexpected Behavior Occurs When You Change the rui.pfx Password

The default password for the PFX file rui.pfx is **`testpassword`**. If you change this password, you must also change the default keystorePass parameter in the Tomcat configuration file.

### Problem

Unexpected behavior might occur if the rui.pfx password does not match the keystorePass parameter. For example, you receive the error message `Unable to connect to the remote server` when you attempt to enable the vCenter Server Service Status plug-in or Tomcat is not listening on TCP port 8443 as expected.

### Cause

The default password for PFX files is **`testpassword`**. It is not necessary or recommended to change this password. However, if your organization requires that you change the default password, you must update the corresponding Tomcat the configuration file.

### Solution

1 Stop all vCenter Server services.

2 Browse to the Tomcat configuration files and open `server.xml` in a text editor.

The default location is `Program Files\VMware\Infrastructure\tomcat\conf\server.xml`.

3 Locate the line containing the following text: `Connector port="8443"`

4 Update the `keystorePass` parameter to match the rui.pfx certificate password.

You cannot leave this parameter empty. The default is testpassword.

5 Restart all vCenter Server services.

## SSL Certificate Update Errors with Single Sign-On

When you are updating an SSL certificate for vSphere components, the update might fail.

### Problem

During an SSL certificate update, vCenter Server fails to start or you are unable to log in to vCenter Server.

### Cause

After changing the vCenter Single Sign-On SSL certificate, the new system did not add the certificate to the vCenter trust store. The certificate is not valid for this update.

### Solution

- If you are unable to log in to vCenter Server after the SSL certificate update, restart vCenter Server.
- Verify that you are not attempting to update with the same SSL certificate that resides on another vCenter Server system pointing to the same vCenter Single Sign-On server. SSL certificates must be unique. Generate a new certificate with a unique distinguished name (DN) and repeat the update process.
- Verify that the X.509 SSL certificate is valid and not corrupt or expired. Provide a valid SSL certificate if needed. If vCenter Server cannot read the certificate, it might be corrupt.
- Verify that the SSL certificate key/certificate pair match. If they do not match, provide a valid key/certificate pair.
- If the error `SSL Exception: Verification parameters (certificate signature failure)` appears in the vCenter Server logs, add the certificate to the trust store. See "Update the Certificate Trust Store for vCenter Server Components," on page 9.