



Provisioning Self-Sign Certificates

The Secure Socket Layer (SSL) protocol secures the network communication and allows data to be encrypted before transmission and provides security. Many application servers and Web servers support the use of keystores for SSL configuration.

This appendix also includes information on how to select the RSA Key Manager.

This appendix includes the following sections:

- [Configuring SSL for Cisco SME, page C-1](#)
- [Generating and Installing Self-Signed Certificates, page C-5](#)
- [Editing SSL Settings in Cisco Fabric Manager Web Client, page C-6](#)

Configuring SSL for Cisco SME

A certificate is an electronic document that you use to identify a server, a company, or some other entity and to associate that identity with a public key.

Certificate authority (CA) are entities that validate identities and issue certificates. The certificate that the CA issues binds a particular public key to the name of the entity that the certificate identifies (such as the name of a server or device). Only the public key that the certificate certifies works with the corresponding private key that is possessed by the entity that the certificate identifies. Certificates help prevent the use of fake public keys for impersonation.

You must install a third-party tool such as the OpenSSL application to generate a certificate request. In Windows, by default, openssl.exe is located at c:\openssl\bin.

Before configuring the SSL, consider the following:

- Ensure that the time in all the switches, Fabric Manager server and the system running the OpenSSL commands, are all synchronized.
- Provide different identities for the CA certificate and KMC certificate.
- Only JRE1.6 JAVA keytool is supported for importing PKCS12 certificates to Java Keystores (JKS) files.

This section describes the following topics:

- [Creating CA Certificates, page C-2](#)
- [Generating KMC Certificate, page C-4](#)

Send documentation comments to mdsfeedback-doc@cisco.com

```
AQABMA0GCSqGSIb3DQEBBAUAA4GBAKR3WAAF/9zMb2u9A42I2cB2G51ucSzndc4P
+O4sYZF5pBt7UpyAs1GKAqivGXVq2FJ2JetX78Fqy7jYcZanWm0tck0/G1dSfr/X
1CFXUuVed9de02yqxARSEx8mX4ifqzYHERHdbi+vDAaMzkUEvHWthOuUZ7fvpoNH
+xhRAuBo
----END CERTIFICATE----
```

- Step 11** Repeat steps 2 through 9 for all the switches managed by a Fabric Manager server. Ensure that the same trustpoint is used for all the switches in this Fabric Manager server.
-

Generating KMC Certificate

To generate the KMC server certificate, follow these steps:

- Step 1** Generate KMC certificate by entering the following commands in the OpenSSL application:
- ```
OpenSSL> genrsa -out sme_kmc_server.key 1024
OpenSSL> req -new -key sme_kmc_server.key -out sme_kmc_server.csr -config openssl.conf
OpenSSL> x509 -req -days 365 -in sme_kmc_server.csr -CA cacert.pem -CAkey privkey.pem
-CACreateserial -out sme_kmc_server.cert
OpenSSL> pkcs12 -export -in sme_kmc_server.cert -inkey sme_kmc_server.key -out
sme_kmc_server.p12
```

**Note**

Access the openssl.config file from the following location:

```
C:\Program Files\GnuWin32\share
```

---

- Step 2** Import this PKCS12 keystore to Java Keystores using JAVA keytool (JRE 1.6).
- ```
"C:\Program Files\Java\jre1.6.0_02\bin\keytool.exe" -importkeystore -srckeystore
sme_kmc_server.p12 -srcstoretype PKCS12 -destkeystore sme_kmc_server.jks -deststoretype JKS
```

**Note**

Remember the password as it needs to be updated in the properties file.

- Step 3** Import the CA certificate to Java Keystores using JAVA keytool (JRE 1.6).
- ```
"C:\Program Files\Java\jre1.6.0_02\bin\keytool.exe" -importcert -file cacert.pem -keystore
sme_kmc_trust.jks -storetype JKS
```

- Step 4** Place these keystore files in mds9000/conf/cert directory.

- Step 5** Modify the KMC SSL settings in the Key Manager Settings in Fabric Manager Web Client.

- Step 6** Restart the Fabric Manager server.

**Note**

You can also use sme\_kmc\_server.p12 as KMC server certificate and cacert.pem as KMC trust certificate instead of using Java keystores created in Step 3 and 4.

---

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)*

## Generating and Installing Self-Signed Certificates

To configure SSL when KMC is not integrated with Fabric Manager server, follow these steps:

**Step 1** Create the required certificates by using the following commands:

```
switch:./createSmeCerts.tcl
Usage: ./createSmeCerts.tcl [r] [k] [s] [a] [h]
r Generate Root CA certificate
k Generate KMC server certificate
s Generate Switch certificate and configure switch trust point
a Generate all certificates and configure switch
h Print this usage screen
Usage: ./createSmeCerts.tcl [r] [k] [s] [a] [h]
r Generate Root CA certificate
k Generate KMC server certificate
s Generate Switch certificate and configure switch trust point
a Generate all certificates and configure switch
h Print this usage screen

switch:./createSmeCerts.tcl a
Dir to store certificates [] :.
Openssl path [/usr/bin] :
RootCA CN [RootCA] :SMECA
Trust Pass Phrase [nbv123] :nbv123
Certificate Validity days [365] :1024
Trust point name [sme_ca] :
Generating CA certificate ...

Generated CA certificate /users/filename1/SSL script/./cacert.pem

Create switch certificate and configure trustpoint ...

Switch IP [] :switchname
username [] :admin
password [] :
Created certificate and configured trustpoint for switch: ips-hac4

Do you want to configure another switch? (y/n) [n] :n
Generating KMC certificate ...

KMC Common Name [] :KMC
Generated KMC certificate: /users/filename1/SSL script/./sme_KMC_server.p12

switch:./createSmeCerts.tcl k
Dir where RootCA certificate is stored [] :.
Reading properties from /users/filename1/SSL script/./sme_cert.properties
Generating KMC certificate ...

KMC Common Name [] :FM
Generated KMC certificate: /users/filename1/SSL script/./sme_FM_server.p12

switch:ls
cacert.pem openssl_FM.conf sme_FM_server.cert sme_KMC_server.csr
cacert.srl openssl_KMC.conf sme_FM_server.csr sme_KMC_server.key
createSmeCerts.tcl* privkey.pem sme_FM_server.key sme_KMC_server.p12
createSmeCerts.tcl.orig* README* sme_FM_server.p12 sw_ips.csr
openssl.conf sme_cert.properties sme_KMC_server.cert sw_ips.pem
switch:
```

**Step 2** Use JAVA keytool (JRE 1.6) to generate Java keystores.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

```
"C:\Program Files\Java\jre1.6.0_02\bin\keytool.exe" -importkeystore -srckeystore
sme_KMC_server.p12 -srcstoretype PKCS12 -destkeystore sme_kmc_server.jks -deststoretype
JKS
```

```
"C:\Program Files\Java\jre1.6.0_02\bin\keytool.exe" -importkeystore -srckeystore
sme_FM_server.p12 -srcstoretype PKCS12 -destkeystore sme_fm_server.jks -deststoretype JKS
```

```
"C:\Program Files\Java\jre1.6.0_02\bin\keytool.exe" -importcert -file cacert.pem -keystore
sme_kmc_trust.jks -storetype JKS
```

```
"C:\Program Files\Java\jre1.6.0_02\bin\keytool.exe" -importcert -file cacert.pem -keystore
fmtrust.jks -storetype JKS
```

**Step 3** Run the following commands for the Fabric Manager server:

```
Copy sme_fm_server.jks to <FMINSTALL>/jboss/server/default/conf/fmserver.jks
Copy fmtrust.jks to <FMINSTALL>/jboss/server/default/conf/fmtrust.jks
```

```
Go to <FMInstall>/bin
Run ./Encrypter.sh ssl
```

```
Edit <FMInstall>/conf/server.properties; set useSSL=true
```

**Step 4** Run the following commands for KMC (whether KMC is standalone or integrated with Fabric Manager server):

```
Copy sme_kmc_server.jks to <FMINSTALL>/conf/cert/sme_kmc_server.jks
Copy sme_kmc_trust.jks to <FMINSTALL>/conf/cert/sme_kmc_trust.jks
```

```
Copy sme_kmc_server.jks to <FMINSTALL>/jboss/server/default/conf/fmserver.jks
Copy fmtrust.jks to <FMINSTALL>/jboss/server/default/conf/fmtrust.jks
```

```
Go to <FMInstall>/bin
Run ./Encrypter.sh ssl
```

```
Edit <FMInstall>/conf/server.properties; set useSSL=true
```

```
Go to Key Manager settings tab in SME tab on web client. In KMC SSL settings select
sme_kmc_trust.jks as KMC trust and sme_kmc_server.jks as KMC server certificate
```

## Editing SSL Settings in Cisco Fabric Manager Web Client

You can edit the SSL settings if you chose the Cisco Key Manager.

To edit the SSL settings in the Cisco SME wizard, follow these steps:

**Step 1** Log into the Fabric Manager.

**Step 2** Click the SME tab and select the Key Manager Settings. The Key Manager Settings window displays.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Step 3** Click **Edit SSL Settings**.

**Step 4** In the KMC SSL settings area, select the SME KMC Trust certificate from the drop-down menu. This is the switch root certificate.



---

**Note** You must copy the acerts to the /mds9000/conf/cert directory. Certificates in the conf/cert directory are listed in the drop-down menus.

---

**Step 5** From the drop-down menu, select the SME KMC Server certificate.  
The keystore files that are stored in the KMC directory are listed in the drop-down menu.

**Step 6** Enter the server certificate password. Confirm the password.

**Step 7** Click **Submit SSL Settings** to apply the changes, or click **Cancel**. Save the settings.  
To change the SSL settings again, click **Edit SSL Settings**.

---



---

**Note** After editing the SSL settings, restart the Fabric Manager Server.

---

If On is selected in the Transport Settings during cluster creation, then SSL is enabled on KMC with the following results:

- New clusters are created. If Off is selected, cluster creation fails.
- Previously created clusters are updated by enabling SSL with trustpoint on the switches. KMC server connection state remains as none until the cluster is updated.

For more information, refer to [Selecting Transport Settings, page 4-10](#).

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***