Managing Certificates

This chapter contains the following sections:

Managing SSL Certificates

This section describes how to generate a Self-Signed certificate and Certificate Signing Request (CSR) that can be used to obtain SSL certificates from a Certificate Authority such as VeriSign, Digicert, and so on It also provides instructions to import the generated Self-Signed certificate or CA certificate in Cisco UCS Director.

Generating Self-Signed Certificates and Certificate Signing Requests

When you generate a self-signed certificate, a new self-signed certificate in PEM format and a Certificate Signing Request (CSR) file are created in the `/opt/certs/` directory. When generating a self-signed certificate, clicking enter will select the default option. For example, if you do not specify a domain name, the shell admin by default chooses the domain name of the appliance that is configured.

You can generate a self-signed certificate and a CSR using the **Generate Self-Signed Certificate and Certificate Signing Request** option.

Step 1 From the Cisco UCS Director Shell menu, choose the **Generate Self-Signed Certificate and Certificate Signing Request** and press **Enter**.

The following information is displayed:

```
Do you want to use the domain localdom [y/n]?
```

Step 2 Enter **y** and press **Enter**.

By default the shell menu selects the domain name of the local appliance that is configured.

The following information is displayed:

```
Enter number of days the generated certificate will be valid for.
It should be between 1825 days (5 years) and 5475 days (15 years).
Enter number of days the certificate will be valid:
```

Step 3   Enter the number of days that you want the self-signed certificate to be valid for and press **Enter**. It is recommened to enter the number of days between 1825 days (5 years) and 5475 days (15 years).

The following information is displayed:

```
Generating a 2048 bit RSA private key
writing new private key to '/opt/certs/localdom.key'
------
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
------
Country Name (2 letter code) [xx]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
```

Step 4   Enter the country name, state or province name, locality name, organization name, organizational unit name, common name, and email address, and press **Enter**.

The following information is displayed:

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Step 5   (Optional) Enter a challenge password and an optional company name, and press **Enter**.

The following information is displayed:

```
Writing new CSR (Certificate Signing Request) to /opt/certs/localdom.csr.
Use the CSR to obtain a certificate in PEM format from a CA (Certificate Authority).
Signature ok
subject=/C=AU/ST=Some-State/O=Internet Pty Ltd
Getting Private key
Writing new self-signed certificate in PEM format to /opt/certs/localdom.pem.
Press return to continue ...
```

Importing Certification Authority or Self-Signed Certificates

You can either import the generated self-signed certificate or import a certificate generated by another system or third party by copying .pem and .key (private key) files to the `/opt/certs/` directory. The shell admin will automatically discover the .pem and .key files for the given domain in the `/opt/certs/` directory. The .pem file provided is exported into PKCS12 format, and then converted to JKS format. The JKS file can be imported into Tomcat.

You can import a CA signed certificate, self-signed certificate, or a certificate bundle (with multiple certificates, if it involves multiple signing authority) using the **Import CA/Self-Signed Certificate** option.

Note   Before importing a root chain CA certificate using the Shell menu, you must combine the primary, intermediate, and root certificates into a single .pem file.

Step 1   From the Cisco UCS Director Shell menu, choose the **Import CA/Self-Signed Certificate** option and press **Enter**.

The following information is displayed:

```
Do you want to use the domain localdom [y/n]?
```

Step 2   Enter **y** and press **Enter**.

By default the shell menu selects the domain name of the local appliance that is configured.

The following information is displayed:

```
Enter the path for the CA/self-signed certificate (PEM) for localdom (e.g.,
/root/Downloads/localdom.pem):
```

Step 3   Enter the path to the CA signed certificate, self-signed certificate, or a certificate bundle (with multiple certificates, if it involves multiple signing authority), and press **Enter**.

The following information is displayed:

```
Enter private key [/opt/certs/localdom.key]:
```

Step 4   Enter the path to the private key and press **Enter**.

The following information is displayed:

```
Enter keystore password:
```

Step 5   Enter the Java KeyStore (JKS) password and press **Enter**.

Information similar to the following is displayed

```
Verifying /opt/certs/localdom.pem ...

The certificate /opt/certs/localdom.pem is valid.

Exporting /opt/certs/localdom.pem to PKCS12 format....

Converting PKCS12 to JKS format...
```

```
Importing /opt/certs/keystore.jks into tomcat for secured access to UCSD UI using HTTPS.

Certificate /opt/certs/keystore.jks imported to tomcat succesfully.

Press return to continue ...
```