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:

```
Domain Name [localdom]:
```

Step 2 Enter the domain name and press **`Enter`**.

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

The following information is displayed:

```
How many days is self-signed certificate valid for [ Choose value which is greater than 5 years and
 less than 15 years ]? [1825]:
```

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 5 years (1825 days) and 15 years (5475 days).

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) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My 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 []:
```

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 Widgits 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 or self-signed certificate using the **Importing CA/Self-Signed Certificate** option.

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

The following information is displayed:

```
Domain Name [localdom]:
```

Step 2 Enter the domain name 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 CA/self-signed certificate [/opt/certs/localdom.pem]:
```

Step 3 Enter the path to the CA signed certificate or self-signed certificate, 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

```
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.

Do you want to import the certificate file:///opt/certs/localdom.pem into WebProxy for secured access
 to VM console through VNC [y/n]?:
```

Step 6 Enter **y** and press **Enter** to import the certificate file into WebProxy for secured access to the VM console through VNC.

The following information is displayed:

```
Certificate file:///opt/certs/localdom.pem imported to WebProxy succesfully.
Press return to continue ...
```