**Procedure**

To generate a self-signed SSL certificate using the OpenSSL, complete the following steps:

1. Write down the Common Name (CN) for your SSL Certificate. The CN is the fully qualified name for the system that uses the certificate. If you are using Dynamic DNS, your CN should have a wild-card, for example: \*.api.com. Otherwise, use the hostname or IP address set in your Gateway Cluster (for example. 192.16.183.131 or dp1.acme.com).
2. Run the following OpenSSL command to generate your private key and public certificate. Answer the questions and enter the Common Name when prompted.

openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem

1. Review the created certificate:

openssl x509 -text -noout -in certificate.pem

1. Combine your key and certificate in a PKCS#12 (P12) bundle:

openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12

1. Validate your P2 file.

openssl pkcs12 -in certificate.p12 -noout -info

1. In the navigation section of the Cloud Management Console, click the SSL Profiles icon . The SSL Profiles page opens.
2. In the SSL Profiles page, click + SSL Profile.
3. In the Name text field, enter the name of the new SSL Profile.
4. In the Present Certificate section, click Select File, then browse for and select certificate.p12.

**Note**

* + Your P12 file must contain the private key, the public certificate from the Certificate Authority and all intermediate certificates used for signing.
  + Your P12 file can contain a maximum of 10 intermediate certificates.

1. In the **Password** text field, enter the password for the certificate file.