# Generate a CSR for Third-Party Certificate and Installation on CMX 10.6 Configuration Example

## Contents



## Introduction

This document describes how to generate a Certificate Signing Request (CSR) in order to obtain a third-party certificate and how to download a chained certificate to Cisco Connected Mobile Experiences (CMX).

Contributed by Andres Silva and Ram Krishnamoorthy, Cisco TAC Engineers.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Linux
- Public Key Infrastructure (PKI)
- Digital Certificates
- CMX

### Components Used

The information in this document is based on CMX version 10.6.1-47

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configure

---

Note: Please use CMX 10.6.2-57 or above when working with Certificates.

---

## Configurations

### Generate CSR

Step1. Access the Command Line Interface (CLI) of CMX using SSH, run the following command to generate a CSR and complete the information requested:

```
[cmxadmin@cmx-andressi]$ cmxctl config certs createcsr
Keytype is RSA, so generating RSA key with length 4096
Generating RSA private key, 4096 bit long modulus
............
...
e is 65537 (0x10001)
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 a 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) [AU]:MX
State or Province Name (full name) [Some-State]:Tlaxcala
Locality Name (eg, city) []:Tlaxcala
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:cmx-andressi
Email Address []:cmx@cisco.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:Cisco
The CSR is stored in : /opt/cmx/srv/certs/cmxservercsr.pem
The Private key is stored in: /opt/cmx/srv/certs/cmxserverkey.pem
```

The private key and the CSR are stored in **/opt/cmx/srv/certs/**

> **Note**: if using CMX 10.6.1, the SAN filed is automatically added to the CSR. If third-party CA is not able to sign the CSR due to the SAN field, remove the SAN string from the openssl**.conf** file on CMX. Refer to bug CSCvp39346 for more information.

Step 2. Get the CSR signed by a Third-Party Certificate Authority.

In order to get the certificate from CMX and send it to the Third-Party, run the **cat** command to open the CSR. You can copy and paste the output into a .txt file or change the extension based on

the requirements of the Third-Party.

```
[cmxadmin@cmx-andressi]$ cat /opt/cmx/srv/certs/cmxservercsr.pem
```

**Import signed certificate and Certificate Authority (CA) certificates to CMX**

> **Note**: In order to import and install the certificates on CMX the installation of root patch is required on CMX 10.6.1 and 10.6.2 due to bug CSCvr27467.

Step 1. Bundle private key with the signed certificate into a **.pem** file. Copy and paste them as follows:

```
-----BEGIN RSA PRIVATE KEY----- < Private Key
MIIEpAIBAAKCAQEA2gXgEo7ouyBfWwCktcYo8ABwFw3d0yG5rvZRHvS2b3FwFRw5
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE----- <  Signed certificate
MIIFEzCCAvugAwIBAgIBFzANBgkqhkiG9w0BAQsFADCBlDELMAkGA1UEBhMCVVMx
```

Step 2. Bundle the Intermediate and root CA certificates into a **.crt** file. Copy and paste them as follows:

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < Intermediate CA certificates
...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE----- < The root CA certificate
MIIGqjCCBJKgAwIBAgIJAPj9p1QMdTgoMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
...
-----END CERTIFICATE-----
```

Step 3. Transfer both files from Step 1 and 2 above to CMX.

Step 4. Access the CLI of CMX as root and clear the current certificates by running the following command:

```
[cmxadmin@cmx-andressi]$ cmxctl config certs clear
```

Step 5. Run the **cmxctl config certs importcacert** command to import CA certificate. Enter a password and repeat it for all the other password prompts.

```
[cmxadmin@cmx-andressi]# cmxctl config certs importcacert ca.crt
Importing CA certificate.....

Enter Export Password:
Verifying - Enter Export Password:
Enter Import Password:

No CRL URI found. Skipping CRL download.
Import CA Certificate successful
```

Step 6. To import server certificate and private key (combined into a single file), run the **cmxctl config certs importservercert** command. Select a password and repeat it for all the password prompts.

```
[cmxadmin@cmx-andressi]# cmxctl config certs importservercert key-cert.pem

Importing Server certificate.....
Successfully transferred the file
Enter Export Password: password
Verifying - Enter Export Password: password
Enter Import Password: password
Private key present in the file: /home/cmxadmin/key-cert.pem
Enter Import Password: password

No CRL URI found. Skipping CRL download.
Validation of server certificate is successful
Import Server Certificate successful
Restart CMX services for the changes to take effect.
Server certificate imported successfully.

To apply these certificate changes, CMX Services will be restarted now.
Please press Enter to continue.
```

Step 7. Press **Enter** to restart the Cisco CMX services.

### Installing Certificates in High Availability

- Certificates have to be installed separately on both the primary and secondary servers.
- If the servers are already paired, HA should be disabled first before proceeding with the certificate install.
- To clear any existing certificates on the primary, use "cmxctl config certs clear" command from the CLI
- Certificates to be installed on both the primary and Secondary should be from the same certificate authority.
- After the install of certificates, CMX services should be restarted and then paired for HA.

## Verify

To confirm the certificate got installed correctly, open the web interface of CMX and review the certificate in use.

## Troubleshoot

In case CMX fails to import the server certificate due to the SAN verification, something like this is logged:

```
Importing Server certificate.....

CRL successfully downloaded from http://<URL>.crl
This is new CRL. Adding to the CRL collection.
ERROR:Check for subjectAltName(SAN) failed for Server Certificate
ERROR: Validation is unsuccessful (err code = 3)
ERROR: Import Server Certificate unsuccessful
```

If the SAN field is not required, you can disable the SAN verification on CMX. To do so, refer to the

procedure on bug CSCvp39346