# Procédure d'installation du certificat SSL CMX 10.5

## Table des matières


Introduction

Conditions préalables

- Exigences
- Composants utilisés

Préparation et sauvegarde

Configurer

Vérification des certificats

Installer les certificats sur CMX

Dépannage


## Introduction

Ce document décrit comment obtenir un certificat SSL gratuit et comment l'installer sur CMX

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Un nom de domaine qui peut être résolu en externe

- Compétences Linux de base

- Connaissances de base de l'ICP (infrastructure à clé publique)

### Composants utilisés

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CMX 10.5

## Préparation et sauvegarde

Le certificat Web se trouve dans le dossier suivant :

```
[root@cmxtry ssl]# pwd
/opt/haproxy/ssl
```

Sauvegardez l'ancien certificat et l'ancienne clé :

<#root>

```
[cmxadmin@cmxtry ssl]$cd /opt/haproxy/ssl/

[cmxadmin@cmxtry ssl]$su root
Password: (enter root password)

[root@cmxtry ssl]# mkdir ./oldcert
[root@cmxtry ssl]# mv host.* ./oldcert/

[root@cmxtry ssl]#

ls ./oldcert/
host.key  host.pem
```

Si vous n'êtes pas très familier avec Linux, les commandes peuvent être interprétées de la façon suivante :

```
[cmxadmin@cmxtry ssl]$cd /opt/haproxy/ssl/

[cmxadmin@cmxtry ssl]$su root
Password: (enter root password)

[root@cmxtry ssl]# mkdir /opt/haproxy/ssl/oldcert
[root@cmxtry ssl]# mv host.pem /opt/haproxy/ssl/oldcert/
[root@cmxtry ssl]# mv host.key /opt/haproxy/ssl/oldcert/

[root@cmxtry ssl]# ls /opt/haproxy/ssl/oldcert/
host.key  host.pem
```

# Configurer

Générez une clé privée :

```
openssl genrsa -out cmxtry.com.key 2048
```

<#root>

```
[root@cmxtry ssl]# openssl genrsa -out
```

**cmxtry.com.key**

```
 2048
Generating RSA private key, 2048 bit long modulus
............
..............
e is 65537 (0x10001)

[root@cmxtry ssl]# ls
```

**cmxtry.com.key**

```
  oldcert
```

Générez une demande de signature de certificat (CSR) à l'aide de la clé privée que vous avez générée à l'étape précédente.

<#root>

```
[root@cmxtry ssl]#
```

**openssl req -new -sha256 -key cmxtry.com.key -out cmxtry.com.csr**

```
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]:BE
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:DIEGEM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CMXTRY
Organizational Unit Name (eg, section) []:CMXTRY
Common Name (e.g. server FQDN or YOUR name) []:cmxtry.com
Email Address []:avitosin@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:CMXTRY


[root@cmxtry ssl]# ls
cmxtry.com.csr  cmxtry.com.key  oldcert
```

Affichez le CSR :

```
[root@cmxtry ssl]# cat cmxtry.com.csr
-----BEGIN CERTIFICATE REQUEST-----
```

```
MIIDZTCCAk0CAQAwgY0xCzAJBgNVBAYTAkJFMRMwEQYDVQQIDApTb21lLVN0YXRl
MQ8wDQYDVQQHDAZESUVHRU0xDzANBgNVBAoMBkNNWFRSWTEPMA0GA1UECwwGQ01Y
VFJZMRMwEQYDVQQDDApjbXh0cnkuY29tMSEwHwYJKoZIhvcNAQkBFhJhdml0b3Np
bkBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCkEIg0
AxV/3HxAxUu7UI/LxkTP+DZJvvuua1WgyQ+tlD4r1+k1Wv1eINCJqywglCKt9vVg
aiYp4JAKL28TV7rtSKqNFnWDMtTKoYRkYWI3L48r9Mu9Tt3zDCG09ygnQFi6SnmX
VmKx7Ct/wIkkBXfkq1nq4vqosCry8SToS1PThX/KSuwIF6w2aKj1Fbrw3eW4XJxc
5hoQFrSsquqmbi5IZWgH/zMZUZTdWYvFc/h50PCBJsAa9HTY0sgUe/nyjHdt+V/l
alNSh41jsrulhWiPzqbaPW/Fej9/5gtPG5LReWuS20ulAnso4tdcST1vVletoXJw
F58S8AqeVrcOV9SnAgMBAAGggZEwFQYJKoZIhvcNAQkCMQgMBkNNWFRSWTAXBgkq
hkiG9w0BCQcxCgwIQ2lzY28xMjMwXwYJKoZIhvcNAQkOMVIwUDAJBgNVHRMEAjAA
MBcGA1UdEQQQMA6CDF9fSE9TVE5BTUVfXzAdBgNVHSUEFjAUBggrBgEFBQcDAQYI
KwYBBQUHAwIwCwYDVR0PBAQDAgOoMA0GCSqGSIb3DQEBCwUAA4IBAQCBslfRzbiw
WBBBN74aWm6YwkO0YexpR2yCrQhcOsxWTujPVvzNP9WaDNxu1rw6o3iZclGi6D61
qFsKtchQhnclvOj7rNI8TInaxIorR2zMyOlF2vtJmvY4YQFso9qzmuaxkmttEMFU
Fj0bxKh6SpvxePh6+BDcwt+kQExK5aF3Q6cRIMyKBS2+I5J5eddJ0cdIqTfwZOGD
5dMDWqHGd7IZyrend8AMPZvNKm3Sbx11Uq+A/fa7f9JZEOO2Q9h3sl3hj3QIPU6s
w1Pyd66/OXO4yYIvMyjJ8xpJGigNWBOvQ+GLvK0ce441h2u2oIoPe60sDOYldL+X
JsnSbefiJ4Fe
-----END CERTIFICATE REQUEST-----
```

Copier le CSR (inclure les lignes « début de la demande de certificat » et « fin de la demande de certificat »).

Dans mon laboratoire, j'utilisais le certificat gratuit de Comodo (https://www.instantssl.com/)

Absorption

## **Free SSL Certificate** 90 days
## + **COMODO SSL TrustLogo** 90 days

### Step 1: Provide your CSR

You must generate a Certificate Signing Request (CSR) on your webserver. Click here for help generating your CSR. When you have created your CSR you may continue with the enrollment.

After you have generated a CSR using your server software **copy and paste** the CSR text using an **ASCII text editor** into the CSR box below. Your CSR should look something like this:

-----BEGIN CERTIFICATE REQUEST-----
MIIDUDCCArkCAQAwdTEWMBQGA1UEAxMNdGVzdC50ZXN0LmNvbTESMBAGA1UECxMJ
TWFya2V0aW5nMREwDwYDVQQKEwhUZXN0IE9yZzESMBAGA1UEBxMJVGVzdCBDaXR5
(more encoded data).....
Rq+blLr5X5iQdzyF1pLqP1Mck5Ve1eCz0R9/OekGSRno7ow4TVyxAF6J6ozDaw7e
GisfZw40VLT0/6IGvK2jX0i+t58RFQ8WYTOcTRlPnkG8B/uV
-----END CERTIFICATE REQUEST-----

| | |
|---|---|
| 1. Copy and paste your CSR into this box: | |
| 2. Select the server software used to generate the CSR: | Select from list: |
| 3. Select the subscription period for your certificate: | **90 days** |

Note: You will be licensed to use this Certificate on an unlimited number of servers.

| | |
|---|---|
| 4. COMODO Newsletter: | Opt in? |
| 5. Comodo HackerGuardian Free Scan: | Include Comodo HackerGuardian Free Scan? |

**Total Cost:** **$0.00**

Next >

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.