

# Configurer le certificat du serveur UCS sur CIMC

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Générer CSR](#)

[Créer un certificat auto-signé](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment générer une demande de signature de certificat (CSR) pour obtenir un nouveau certificat.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Vous devez vous connecter en tant qu'utilisateur avec des privilèges d'administrateur pour configurer les certificats.
- Assurez-vous que l'heure CIMC est définie sur l'heure actuelle.

### Composants utilisés

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

- CIMC 1.0 ou version ultérieure
- Openssl

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.

## Informations générales

Le certificat peut être téléchargé sur le contrôleur de gestion intégré Cisco (CIMC) afin de remplacer le certificat de serveur actuel. Le certificat du serveur peut être signé par une autorité de certification publique, telle que Verisign, ou par votre propre autorité de certification. La longueur de clé de certificat générée est de 2 048 bits.

## Configurer

Étape 1.	Générez le CSR à partir du CIMC.
Étape 2.	Envoyez le fichier CSR à une autorité de certification pour signer le certificat. Si votre entreprise génère ses propres certificats auto-signés, vous pouvez utiliser le fichier CSR pour générer un certificat auto-signé.
Étape 3.	Téléchargez le nouveau certificat sur le CIMC.

---

**Remarque** : le certificat téléchargé doit être créé à partir d'un CSR généré par le CIMC. Ne téléchargez pas un certificat qui n'a pas été créé par cette méthode.

---

## Générer CSR

Accédez à l'onglet **Admin** > **Security Management** > **Certificate Management** > **Generate Certificate Signing Request** (CSR) et remplissez les détails marqués d'un \*.

Reportez-vous également au guide [Generating a Certificate Signing Request](#).

The screenshot displays the Cisco IMC web interface. The main page is titled 'Certificate Management' and includes navigation tabs for 'Secure Key Management', 'Security Configuration', and 'MCTP SPDM'. A modal dialog box titled 'Generate Certificate Signing Request' is open, showing the following configuration details:

- Current Certificate:** Serial Number: 212DAF6E68B58418158BD0480. Subject Information: Country Code (CC): MX, State (S): Mexico, Locality (L): Mexico, Organization (O): Cisco, Organizational Unit (OU): C-Series, Common Name (CN): Host01. Issuer Information: Country Code (CC): MX, State (S): Mexico, Locality (L): Mexico, Organization (O): Cisco, Organizational Unit (OU): C-Series, Common Name (CN): Host01. Valid From: Jun 15 22:47:56 2023 GMT, Valid To: Sep 17 22:47:56 2025 GMT.
- Certificate Signing Request Status:** Status: Not in progress.
- Generate CSR Dialog:**
  - \* Common Name: Host01
  - Subject Alternate Name: Subject Alternate Name (dropdown: dNSName)
  - \* Organization Name: Cisco
  - Organization Unit: Cisco
  - \* Locality: CA
  - \* State Name: California
  - \* Country Code: United States
  - Email: Please enter Valid Email Address
  - Signature Algorithm: SHA384
  - Challenge Password:
  - String Mask: ---Select---
  - Self Signed Certificate:

Warnings in the dialog include: 'Selecting this option will prompt Cisco IMC to generate Self Signed Certificate.' and 'WARNING: After successful certificate generation, the Cisco IMC Web GUI will be restarted. Communication with the management controller may be lost momentarily and you will need to re-login. Even SSH, vKVM and vMedia sessions will be disconnected.' Buttons for 'Generate CSR', 'Reset Values', and 'Cancel' are visible at the bottom of the dialog.

**Attention :** utilisez l'autre nom du sujet pour spécifier des noms d'hôtes supplémentaires pour ce serveur. Si vous ne configurez pas dNSName ou si vous l'excluez du certificat téléchargé, les navigateurs risquent de bloquer l'accès à l'interface Cisco IMC.

Que faire ensuite ?

Effectuez les tâches suivantes :

- Si vous ne souhaitez pas obtenir un certificat auprès d'une autorité de certification publique et si votre organisation n'exploite pas sa propre autorité de certification, vous pouvez autoriser CIMC à générer en interne un certificat auto-signé à partir du CSR et à le télécharger immédiatement sur le serveur. **Cochez** la case **Certificat auto-signé** pour effectuer cette tâche.
- Si votre organisation utilise ses propres certificats auto-signés, copiez le résultat de la commande depuis -----BEGIN ...à END CERTIFICATE REQUEST----- et à coller dans un fichier nommé csr.txt. Entrez le fichier CSR sur votre serveur de certificats pour générer un certificat auto-signé.
- Si vous obtenez un certificat d'une autorité de certification publique, copiez le résultat de la commande à partir de -----BEGIN ... à END CERTIFICATE REQUEST----- et à coller dans un fichier nommé csr.txt. Envoyez le fichier CSR à l'autorité de certification pour obtenir un certificat signé. Assurez-vous que le certificat est de type Server.

---

**Remarque** : une fois le certificat correctement généré, l'interface utilisateur graphique Web de Cisco IMC est redémarrée. La communication avec le contrôleur de gestion peut être momentanément perdue et une nouvelle connexion est requise.

---

Si vous n'avez pas utilisé la première option, dans laquelle CIMC génère et télécharge en interne un certificat auto-signé, vous devez créer un nouveau certificat auto-signé et le télécharger vers CIMC.

## Créer un certificat auto-signé

Comme alternative à une autorité de certification publique et à la signature d'un certificat de serveur, utilisez votre propre autorité de certification et signez vos propres certificats. Cette section présente les commandes permettant de créer une autorité de certification et de générer un certificat de serveur avec le certificat de serveur OpenSSL. Pour plus d'informations sur OpenSSL, consultez [OpenSSL](#).

Étape 1. Générez une clé privée RSA comme illustré dans l'image.

```
<#root>
```

```
[root@redhat ~]#
```

```
openssl genrsa -out ca.key 1024
```

Étape 2. Générez un nouveau certificat auto-signé comme illustré dans l'image.

```
<#root>
```

```
[root@redhat ~]#
```

```
openssl req -new -x509 -days 1095 -key ca.key -out ca.crt
```

```
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) [XX]:
```

```
us
```

```
State or Province Name (full name) []:
```

```
California
```

```
Locality Name (eg, city) [Default City]:
```

```
California
```

```
Organization Name (eg, company) [Default Company Ltd]:
```

```
Cisco
```

Organizational Unit Name (eg, section) []:

Cisco

Common Name (eg, your name or your server's hostname) []:

Host01

Email Address []:

[root@redhat ~]#

Étape 3. Assurez-vous que le type de certificat est « server », comme indiqué dans l'image.

<#root>

[root@redhat ~]#

```
echo "nsCertType = server" > openssl.conf
```

Étape 4. Demande à l'autorité de certification d'utiliser votre fichier CSR pour générer un certificat de serveur, comme indiqué dans l'image.

<#root>

[root@redhat ~]#

```
openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
```

Étape 5. Vérifiez si le certificat généré est de type Serveur, comme illustré dans l'image.

<#root>

[root@redhat ~]#

```
openssl x509 -in server.crt -purpose
```

Certificate purposes:

SSL client : No

SSL client CA : No

SSL server :

Yes

SSL server CA : No

Netscape SSL server : Yes

Netscape SSL server CA : No

S/MIME signing : No

S/MIME signing CA : No

S/MIME encryption : No

```
S/MIME encryption CA : No
CRL signing : Yes
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No
-----BEGIN CERTIFICATE-----
MIIDFzCCAoCgAwIBAgIBATANBgkqhkiG9w0BAQsFAADBoMQswCQYDVQGEwJVUzET
MBEGA1UECAwKQ2FsaWZvcml5YUETMBEGA1UEBwwKQ2FsaWZvcml5YTEOMAwwGA1UE
CgwFQ2l2Y28xZDpAMBgNVBAsMBUNpc2NvMQ8wDQYDVQQDDAIZb3N0MDEwHhcNMjMw
NjI0NDUwMDEwMjI0NDUwMDEwMjI0NDUwMDEwMjI0NDUwMDEwMjI0NDUwMDEwMjI0NDUw
CAwKQ2FsaWZvcml5YUETMBEGA1UEBwwKQ2FsaWZvcml5YUETMBEGA1UEBwwKQ2FsaWZvcml5
VQQLDAVDAxNjZEPMA0GA1UEAwwGSG9zdDAXMIIBIjANBgkqhkiG9w0BAQEFAAOCC
AQ8AMIIBCgKCAQEAuhJ50V004MZNv3dgQw0Mns9sgzZwjJS8Lv0tHt+GA4uzNf1Z
WKNyZbzD/yLoXiv8ZFgaWJbqEe2yijVzEcguZQTGFRkAWmDecKM9Fieob03B5Fnt
pC8M9Dfb3YmKix29abrZKFEIrybabbG4gQyFzG0B6D9CK1WuoEzsE7zH0oJX4Bcy
ISE0Rs0d9bsXvxyLk2cauS/zvI9hvrWW9P/Og8nF3Y+PGtm/bnfodEnNFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcy0z+3HReDcQ+kJde7PoFK3d6Z0dkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Zl0800/eciSCsGIJKxYD/FYlQIDAQABo1UwUzARBglghkgBhvhC
AQEEBAMCBkAwHQYDVR00BBYEFJ20TeuP27jyCJRiAKKff1Nc0hbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBCwUAA4GBAJuL/Bej
DxenfCt6pBA709GtKltWUS/rEtpQX190hdlahjwbfG/67MYIpIEbidL1BCw55da1
LI7sgu1dnItNIGsJI1L7h6IEfBu/coCvBtop0YUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZxt3KGE8Q1P+eGkmAHWA8M0yhWHa
-----END CERTIFICATE-----
[root@redhat ~]#
```

Étape 6. Téléchargez le certificat du serveur comme illustré dans l'image.

Cisco Integrated Management Controller

External Certificate uploaded successfully

OK

Refresh | Host Power

Certificate Management | Secure Key Management | Security Configuration

Generate Certificate Signing Request | Upload Server Certificate | Upload External Certificate | Upload External Private Key | Activate External Certificate

### Current Certificate

```
Serial Number          : 212DAF6E68B58418158BD04804D64B2C5EE08B6B
Subject Information:
Country Code (CC)     : MX
State (S)             : Mexico
Locality (L)         : Mexico
Organization (O)      : Cisco
Organizational Unit (OU) : C-Series
Common Name (CN)     : Host01
Issuer Information:
Country Code (CC)     : MX
State (S)             : Mexico
Locality (L)         : Mexico
Organization (O)      : Cisco
Organizational Unit (OU) : C-Series
Common Name (CN)     : Host01
Valid From            : Jun 15 22:47:56 2023 GMT
Valid To              : Sep 17 22:47:56 2025 GMT
```

### Certificate Signing Request Status

Status: Not in progress.

▶ External Certificate    ▶ External Private Key

## Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Accédez à **Admin > Certificate Management** et vérifiez le certificat actuel comme indiqué dans l'image.

Certificate Management

Secure Key Management

Security Configuration

MCTP SPDM

[Generate Certificate Signing Request](#) | [Upload Server Certificate](#) | [Upload External Certificate](#) | [Upload External Private Key](#) | [Activate External Certificate](#)

## Current Certificate

```
Serial Number           : 01
Subject Information:
Country Code (CC)      : US
State (S)              : California
Locality (L)          : CA
Organization (O)       : Cisco
Organizational Unit (OU) : Cisco
Common Name (CN)      : Host01

Issuer Information:
Country Code (CC)      : US
State (S)              : California
Locality (L)          : California
Organization (O)       : Cisco
Organizational Unit (OU) : Cisco
Common Name (CN)      : Host01

Valid From              : Jun 27 22:44:15 2023 GMT
Valid To                : Jun 26 22:44:15 2024 GMT
```

## Certificate Signing Request Status

Status: Not in progress.

[External Certificate](#)[External Private Key](#)

## Dépannage

Aucune information spécifique n'est actuellement disponible pour dépanner cette configuration.

## Informations connexes

- [ID de bogue Cisco CSCup26248](#) - Impossible de télécharger le certificat SSL de l'autorité de certification tierce vers CIMC 2.0.(1a)
- [Assistance et documentation techniques - Cisco Systems](#)



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.