Configurer le certificat du serveur UCS sur CIMC

Table des matières

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 lâ€™heure CIMC est définie sur lâ€™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 lâ€™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

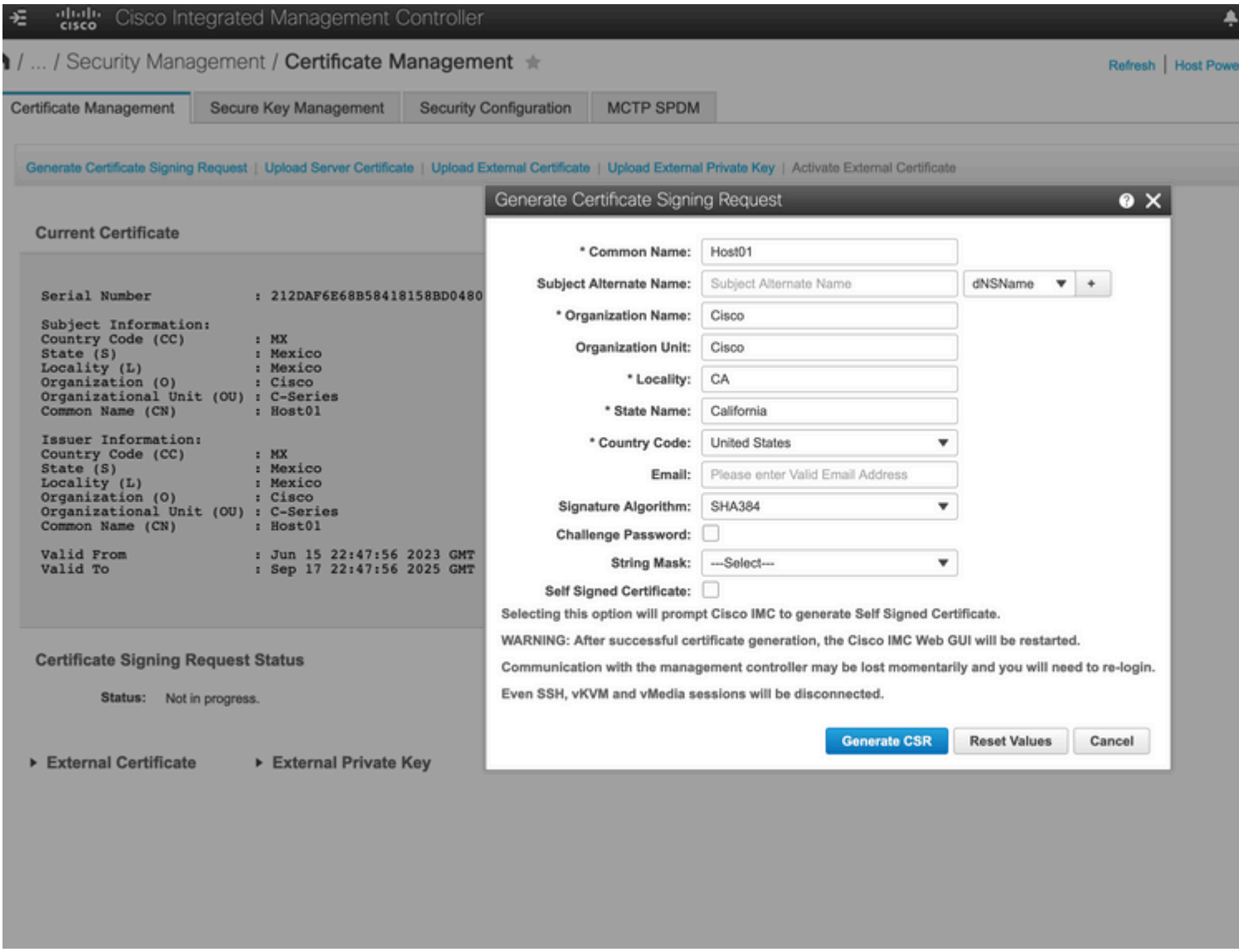
Étape 1.	Générez le CSR à partir du CIMC.
Étape 2.	Envoyez le fichier CSR à une autorité de certification pour signer le certificat. Si votre entreprise génère ses propres certificats auto-signés, vous pouvez utiliser le fichier CSR pour générer un certificat auto-signé.
Étape 3.	Téléchargez le nouveau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



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 dâ€™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 lâ€™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>

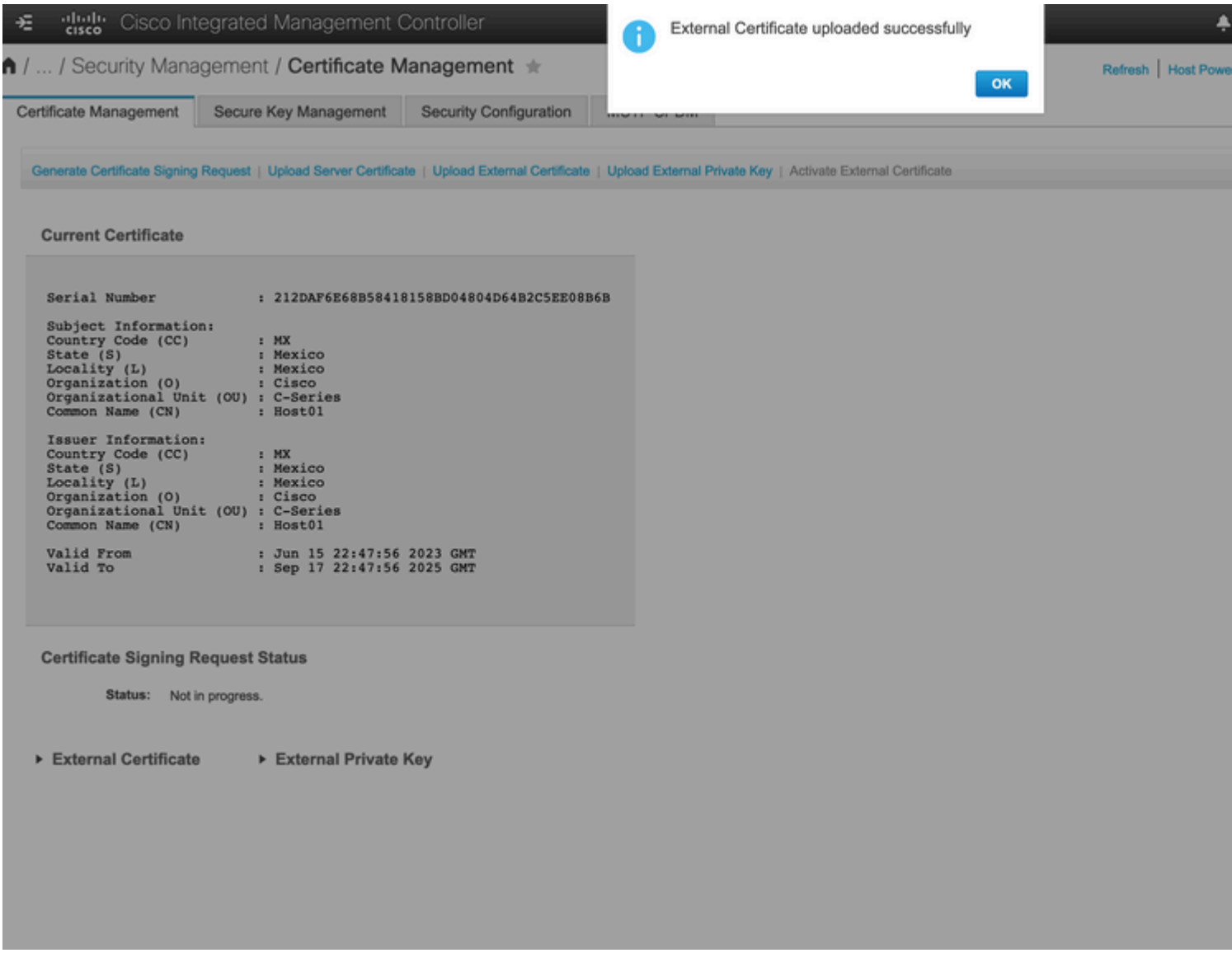
```
[root@redhat ~]#
openssl x509 -in server.crt -purpose

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-----
MIIDFzCCAoCgAwIBAgIBATANBgkqhkiG9w0BAQsFADBoMQswCQYDVQQGEwJVUzET
MBEGA1UECAwKQ2FsaWZvcm5pYTETMBEGA1UEBwwKQ2FsaWZvcm5pYTEOMAwGA1UE
CgwFQ2lzY28xDjAMBgNVBAsMBUNpc2NvMQ8wDQYDVQQDDAZIb3N0MDEwHhcNMjMw
NjI3MjI0NDE1WhcNMjQwNjI2MjI0NDE1WjBgMQswCQYDVQQGEwJVUzETMBEGA1UE
CAwKQ2FsaWZvcm5pYTELMAkGA1UEBwwCQ0ExDjAMBgNVBAoMBUNpc2NvMQ4wDAYD
VQQLDAVDaXNjbzEPMA0GA1UEAwwGSG9zdDAxMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAuhJ5OVOO4MZNV3dgQwOMns9sgzZwjJS8LvOtHt+GA4uzNf1Z
WKNyZbzD/yLoXiv8ZFgaWJbqEe2yijVzEcguZQTGFRkAWmDecKM9Fieob03B5FNt
pC8M9Dfb3YMkIx29abrZKFEIrYbabbG4gQyfzgOB6D9CK1WuoezsE7zH0oJX4Bcy
ISE0RsOd9bsXvxyLk2cauS/zvI9hvrWW9P/Og8nF3Y+PGtm/bnfodEnNWFWPLtvF
dGuG5/wBmmMbEb/GbrH9uVcy0z+3HReDcQ+kJde7PoFK3d6Z0dkh7Mmtjpvk5ucQ
NgzaeoCDL0Bn+Zl0800/eciSCsGIJKxYD/FYlQIDAQABo1UwUzARBglghkgBhvhC
AQEEBAMCBkAwHQYDVR0OBBYEFEJ2OTeuP27jyCJRiAKKfflNc0hbMB8GA1UdIwQY
MBaAFA4QR965FinE4GrhkiwRV62ziPj/MA0GCSqGSIb3DQEBCwUAA4GBAJuL/Bej
DxenfCt6pBA7O9GtkltWUS/rEtpQX190hdlahjwbfG/67MYIpIEbidL1BCw55dal
LI7sgu1dnItnIGsJIlL7h6IeFBu/coCvBtopOYUanaBJ1BgxBWhT2FAnmB9wIvYJ
5rMx95vWZXt3KGE8QlP+eGkmAHWA8M0yhwHa
-----END CERTIFICATE-----
[root@redhat ~]#
```

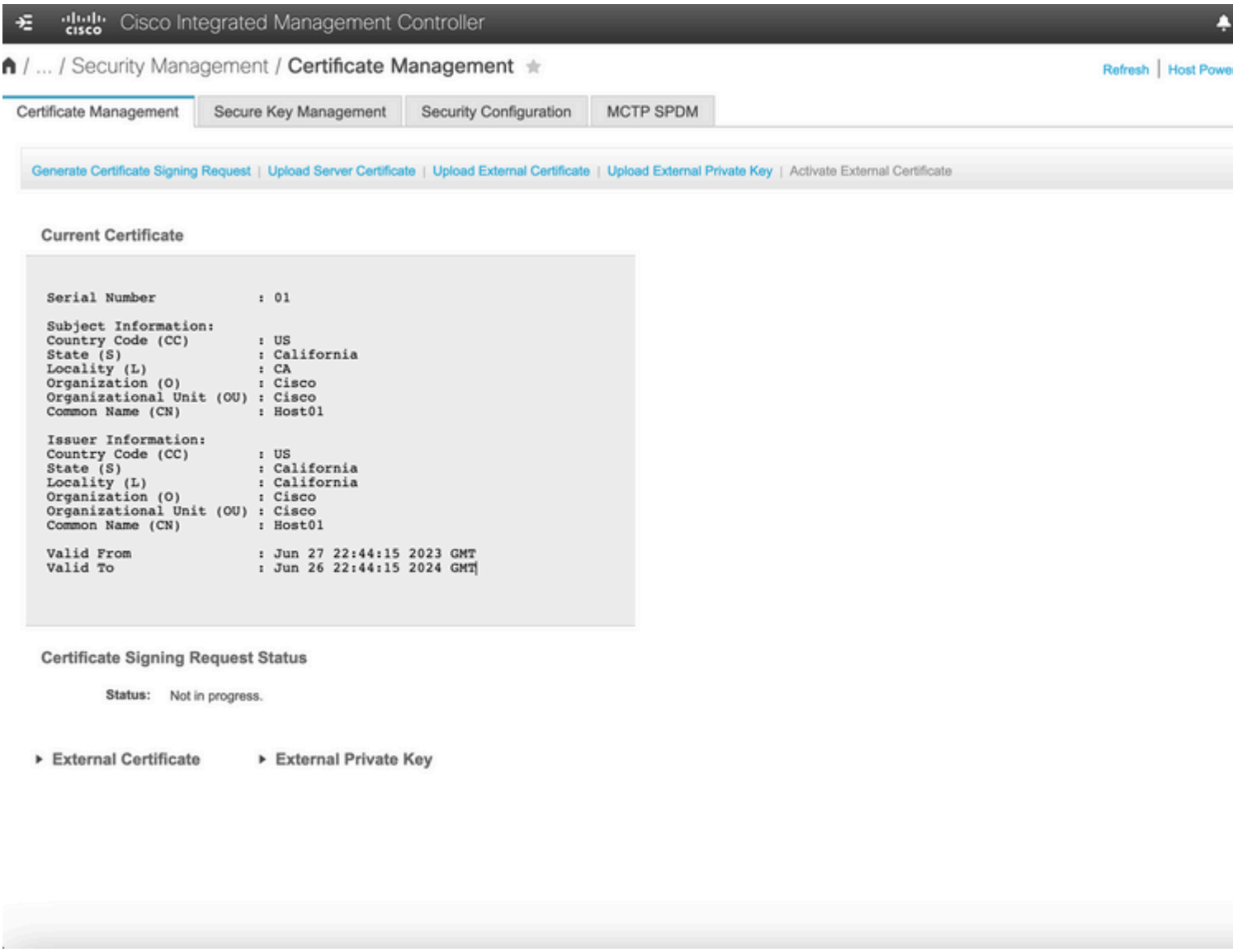
Étape 6. Téléchargez le certificat du serveur comme illustré dans l'image.



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.



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.