UCS Server-certificaat configureren naar CIMC

Inhoud

Inleiding

Dit document beschrijft hoe u een aanvraag voor het ondertekenen van een certificaat (CSR) genereert om een nieuw certificaat te verkrijgen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- U moet inloggen als gebruiker met beheerdersrechten om certificaten te configureren.
- Zorg ervoor dat de CIMC-tijd is ingesteld op de huidige tijd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CIMC 1.0 of hoger
- OpenSSL

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het certificaat kan worden geüpload naar de Cisco Integrated Management Controller (CIMC) om het huidige servercertificaat te vervangen. Het servercertificaat kan worden ondertekend door een openbare certificeringsinstantie (CA), zoals Verisign, of door uw eigen certificeringsinstantie. De gegenereerde certificaatsleutellengte is 2048 bits.

Configureren

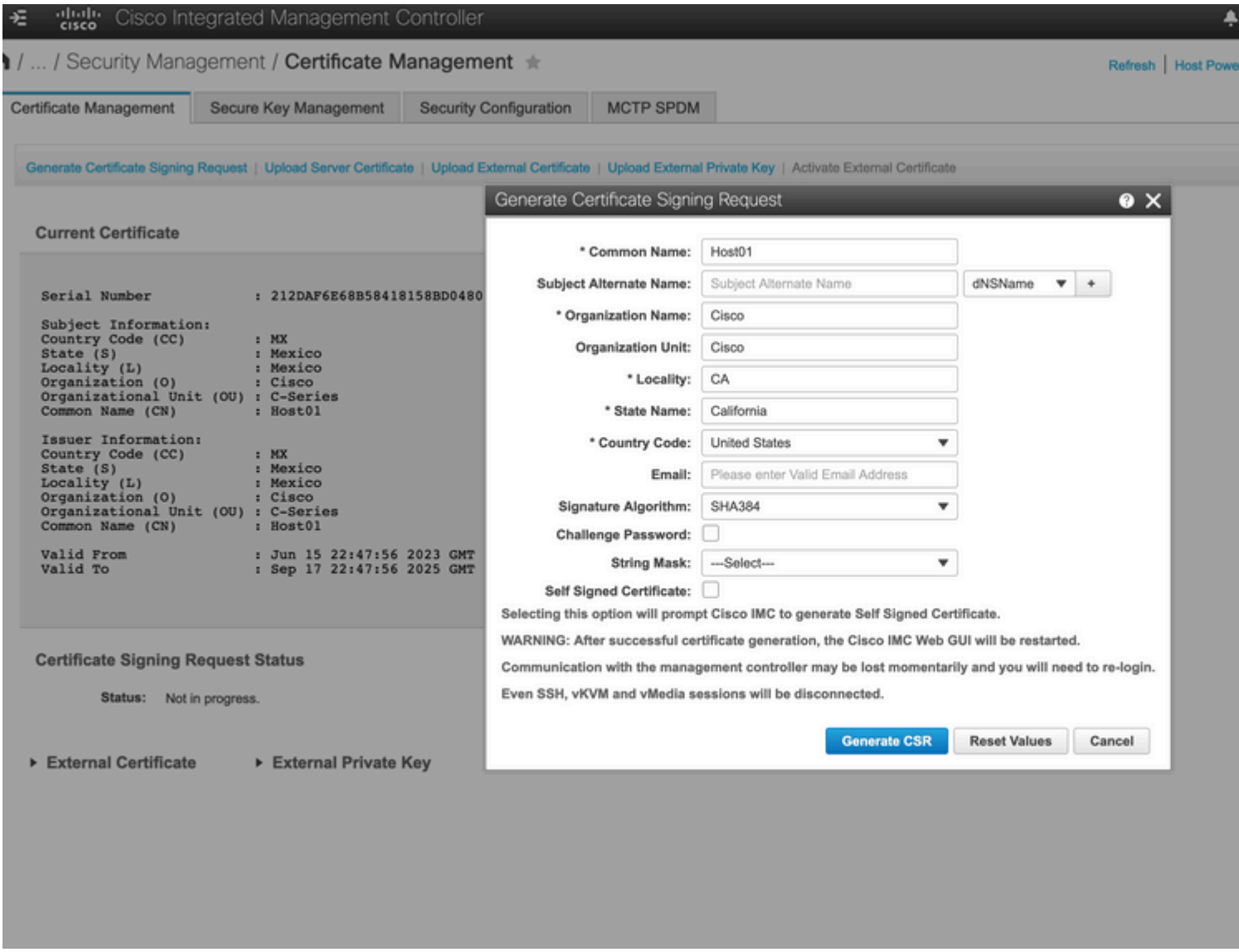
Stap 1.	Genereert de CSR via de CIMC.
Stap 2.	Leg het CSR-bestand voor aan een CA om het certificaat te ondertekenen. Als uw organisatie eigen zelfondertekende certificaten genereert, kunt u het CSR-bestand gebruiken om een zelfondertekend certificaat te genereren.
Stap 3.	Upload het nieuwe certificaat naar de CIMC.

Opmerking: het geüploade certificaat moet worden aangemaakt op basis van een CSR dat door de CIMC wordt gegenereerd. Upload geen certificaat dat niet met deze methode is gemaakt.

MVO genereren

Navigeer naar het tabblad **Beheerder** > **Beveiligingsbeheer** > **Certificaatbeheer** > **Certificaatondertekeningsaanvraag** (CSR) genereren en vul de gegevens in die zijn gemarkeerd met een *.

Raadpleeg ook de handleiding voor het genereren van een aanvraag voor certificaatondertekening.



Waarschuwing: gebruik de *alternatieve onderwerpnaam* om extra hostnamen voor deze server op te geven. Het niet configureren van NSName of het uitsluiten van het geüploade certificaat kan resulteren in browsers die de toegang tot de Cisco IMC-interface blokkeren.

Wat nu?

Voer de volgende taken uit:

- Als u geen certificaat van een openbare certificeringsinstantie wilt verkrijgen en uw organisatie geen eigen certificeringsinstantie beheert, kunt u CIMC toestaan intern een zelfondertekend certificaat van de CSR te genereren en het onmiddellijk naar de server te uploaden. **Controleer** het vakje **Zelfondertekend certificaat** om deze taak uit te voeren.
- Als uw organisatie zelf ondertekende certificaten gebruikt, kopieert u de opdrachtoutput van -----BEGIN ...om HET CERTIFICAAT AAN TE VRAGEN----- en te plakken op een bestand met de naam csr.txt. Voer het CSR-bestand in op uw certificaatserver om een zelfondertekend certificaat te genereren.
- Als u een certificaat verkrijgt van een openbare certificeringsinstantie, kopieert u de opdrachtoutput van -----BEGIN ... om HET CERTIFICAAT AAN TE VRAGEN----- en te plakken op een bestand met de naam csr.txt. Leg het MVO-bestand voor aan de certificeringsinstantie om een ondertekend

certificaat te verkrijgen. Zorg ervoor dat het certificaat van het type Server is.

Opmerking: na een succesvolle certificaatgeneratie wordt de Cisco IMC Web GUI opnieuw gestart. De communicatie met de managementcontroller kan tijdelijk verloren gaan en opnieuw inloggen is vereist.

Als u de eerste optie niet hebt gebruikt, waarin CIMC intern een zelf-ondertekend certificaat genereert en uploadt, moet u een nieuw zelf-ondertekend certificaat maken en uploaden naar de CIMC.

Zelfondertekend certificaat maken

Als alternatief voor een openbare CA en onderteken een servercertificaat, beheer uw eigen CA en onderteken uw eigen certificaten. Deze sectie toont opdrachten om een CA te maken en een servercertificaat te genereren met het OpenSSL-servercertificaat. Zie OpenSSL voor meer informatie over OpenSSL.

Stap 1. Genereert RSA private key zoals in de afbeelding.

<#root>

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

openssl genrsa -out ca.key 1024

Stap 2. Genereer nieuw zelfondertekend certificaat zoals in de afbeelding.

<#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 ~]#
```

Stap 3. Zorg ervoor dat het certificaattype een server is zoals in de afbeelding.

<#root>

```
[root@redhat ~]#
echo "nsCertType = server" > openssl.conf
```

Stap 4. Leidt de CA om uw CSR-bestand te gebruiken om een servercertificaat te genereren zoals in de afbeelding.

<#root>

```
[root@redhat ~]#
openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
```

Stap 5. Controleer of het gegenereerde certificaat van type is Server zoals in de afbeelding.

<#root>

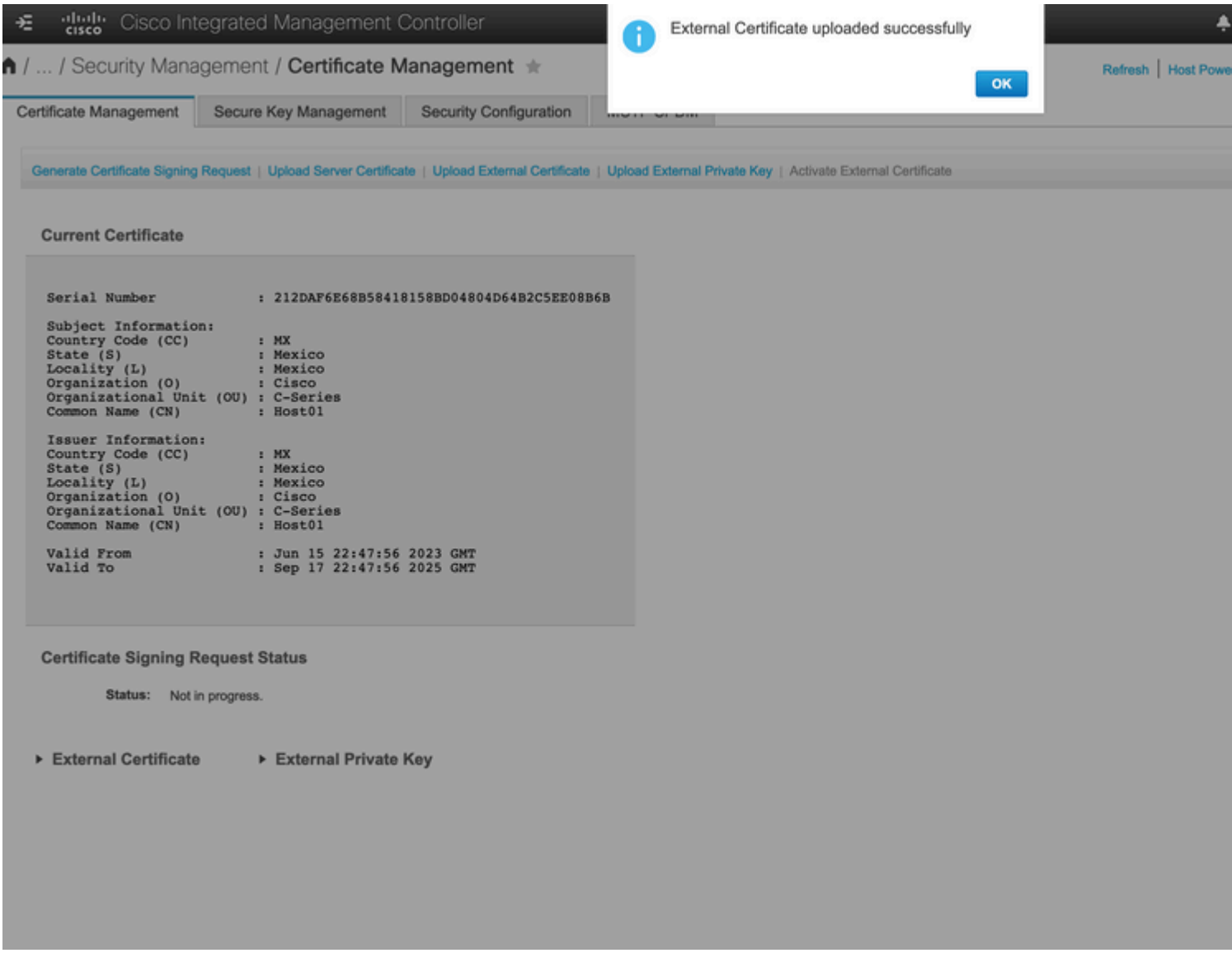
```
[root@redhat ~]#
openssl x509 -in server.crt -purpose

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 ~]#
```

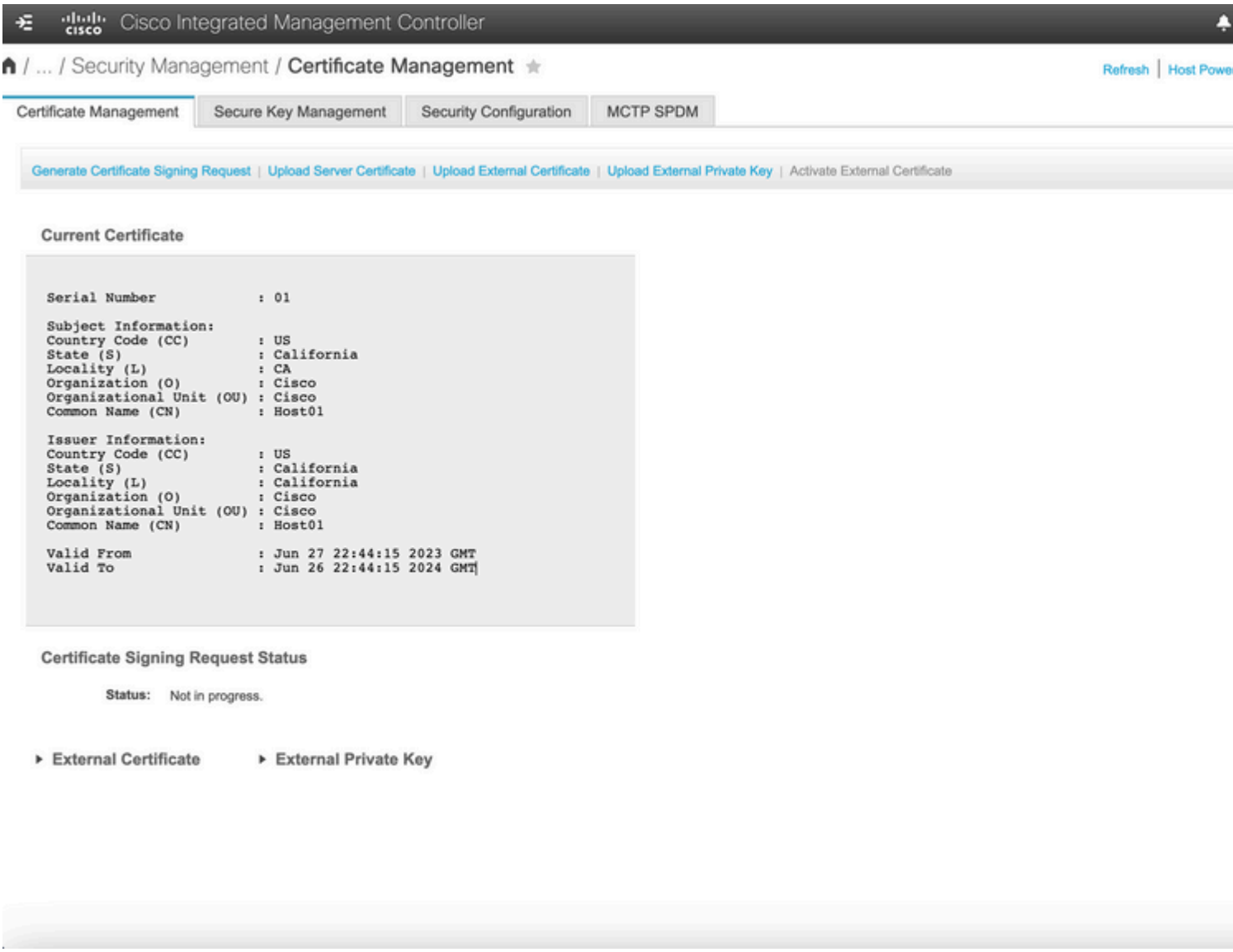
Stap 6. Servercertificaat uploaden zoals in de afbeelding.



Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Navigeer naar **Beheer > Certificaatbeheer** en controleer het huidige certificaat zoals in de afbeelding.



Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

Gerelateerde informatie

- Cisco bug-id CSCup26248 - CA SSL-certificaat van derden kan niet naar CIMC 2.0 worden geüpload.(1a)
- Technische ondersteuning en documentatie â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.