UCS Server-Zertifikat für CIMC konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine CSR-Anforderung (Certificate Signing Request) erstellen, um ein neues Zertifikat zu erhalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sie müssen sich als Benutzer mit Administratorberechtigungen anmelden, um Zertifikate zu konfigurieren.
- Stellen Sie sicher, dass die CIMC-Zeit auf die aktuelle Zeit eingestellt ist.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CIMC 1.0 oder spätere Version
- OpenSSL

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Zertifikat kann auf den Cisco Integrated Management Controller (CIMC) hochgeladen werden, um das aktuelle Serverzertifikat zu ersetzen. Das Serverzertifikat kann entweder von einer öffentlichen Zertifizierungsstelle (Certificate Authority, CA), z. B. Verisign, oder von Ihrer eigenen Zertifizierungsstelle signiert werden. Die generierte Zertifikatschlüssellänge beträgt 2048 Bit.

Konfigurieren

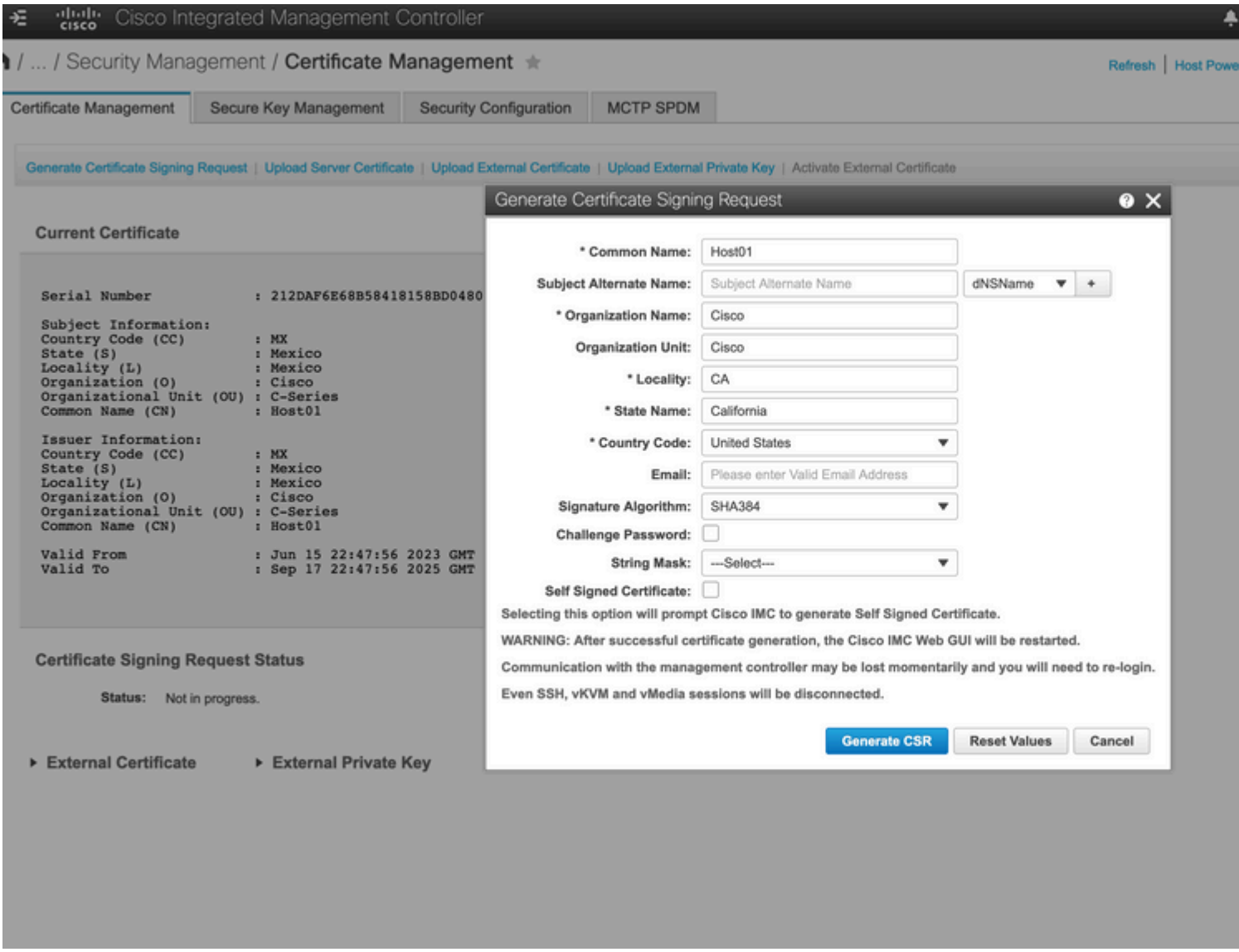
Schritt 1:	Erstellen Sie den CSR vom CIMC aus.
Schritt 2:	Senden Sie die CSR-Datei an eine Zertifizierungsstelle, um das Zertifikat zu signieren. Wenn Ihre Organisation ihre eigenen selbstsignierten Zertifikate generiert, können Sie die CSR-Datei verwenden, um ein selbstsigniertes Zertifikat zu generieren.
Schritt 3:	Laden Sie das neue Zertifikat in den CIMC hoch.

Hinweis: Das hochgeladene Zertifikat muss von einem vom CIMC generierten CSR erstellt werden. Laden Sie kein Zertifikat hoch, das nicht mit dieser Methode erstellt wurde.

CSR erstellen

Navigieren Sie zur Registerkarte **Admin** > **Security Management** > **Certificate Management** > **Generate Certificate Signing Request** (CSR), und füllen Sie die mit einem * gekennzeichneten Felder aus.

Weitere Informationen finden Sie im Leitfaden Generating a Certificate Signing Request.



Achtung: Verwenden Sie den *alternativen Antragstellernamen*, um zusätzliche Hostnamen für diesen Server anzugeben. Wenn dNSName nicht konfiguriert oder vom hochgeladenen Zertifikat ausgeschlossen wird, können Browser den Zugriff auf die Cisco IMC-Schnittstelle blockieren.

Nächste Schritte

Führen Sie folgende Aufgaben aus:

- Wenn Sie kein Zertifikat von einer öffentlichen Zertifizierungsstelle erhalten möchten und Ihre Organisation keine eigene Zertifizierungsstelle betreibt, können Sie CIMC erlauben, intern ein selbstsigniertes Zertifikat vom CSR zu generieren und es sofort auf den Server hochzuladen. **Aktivieren Sie** das Feld **Selbstsigniertes Zertifikat**, um diese Aufgabe auszuführen.

- Wenn Ihre Organisation eigene selbstsignierte Zertifikate verwendet, kopieren Sie die Befehlsausgabe von -----BEGIN ..., um CERTIFICATE REQUEST----- zu BEENDEN und in eine Datei namens csr.txt einzufügen. Geben Sie die CSR-Datei auf Ihrem Zertifikatserver ein, um ein selbstsigniertes Zertifikat zu generieren.

- Wenn Sie ein Zertifikat von einer öffentlichen Zertifizierungsstelle erhalten, kopieren Sie die Befehlsausgabe von -----BEGIN ... , um CERTIFICATE REQUEST----- zu BEENDEN und in eine Datei namens csr.txt einzufügen. Senden Sie die CSR-Datei an die Zertifizierungsstelle, um ein

signiertes Zertifikat zu erhalten. Stellen Sie sicher, dass das Zertifikat vom Typ Server ist.

Hinweis: Nach der erfolgreichen Zertifikatgenerierung wird die Cisco IMC Web-Benutzeroberfläche neu gestartet. Die Kommunikation mit dem Management-Controller kann vorübergehend unterbrochen werden, und eine erneute Anmeldung ist erforderlich.

Wenn Sie die erste Option, bei der CIMC intern ein selbstsigniertes Zertifikat generiert und hochlädt, nicht verwendet haben, müssen Sie ein neues selbstsigniertes Zertifikat erstellen und es in den CIMC hochladen.

Selbstsigniertes Zertifikat erstellen

Alternativ zu einer öffentlichen Zertifizierungsstelle und zum Signieren eines Serverzertifikats können Sie Ihre eigene Zertifizierungsstelle betreiben und Ihre eigenen Zertifikate signieren. In diesem Abschnitt werden Befehle zum Erstellen einer Zertifizierungsstelle und zum Generieren eines Serverzertifikats mit dem OpenSSL-Serverzertifikat angezeigt. Ausführliche Informationen zu OpenSSL finden Sie unter OpenSSL.

Schritt 1: Generieren Sie den privaten RSA-Schlüssel, wie im Bild gezeigt.

<#root>

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

openssl genrsa -out ca.key 1024

Schritt 2: Generieren Sie ein neues selbstsigniertes Zertifikat, wie im Bild dargestellt.

<#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 ~]#
```

Schritt 3: Stellen Sie sicher, dass es sich beim Zertifikatstyp um einen Server handelt, wie im Abbild dargestellt.

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

Schritt 4: Weist die Zertifizierungsstelle an, die CSR-Datei zum Generieren eines Serverzertifikats zu verwenden, wie im Abbild dargestellt.

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

Schritt 5: Überprüfen, ob das generierte Zertifikat vom Typ ist Server wie im Bild dargestellt.

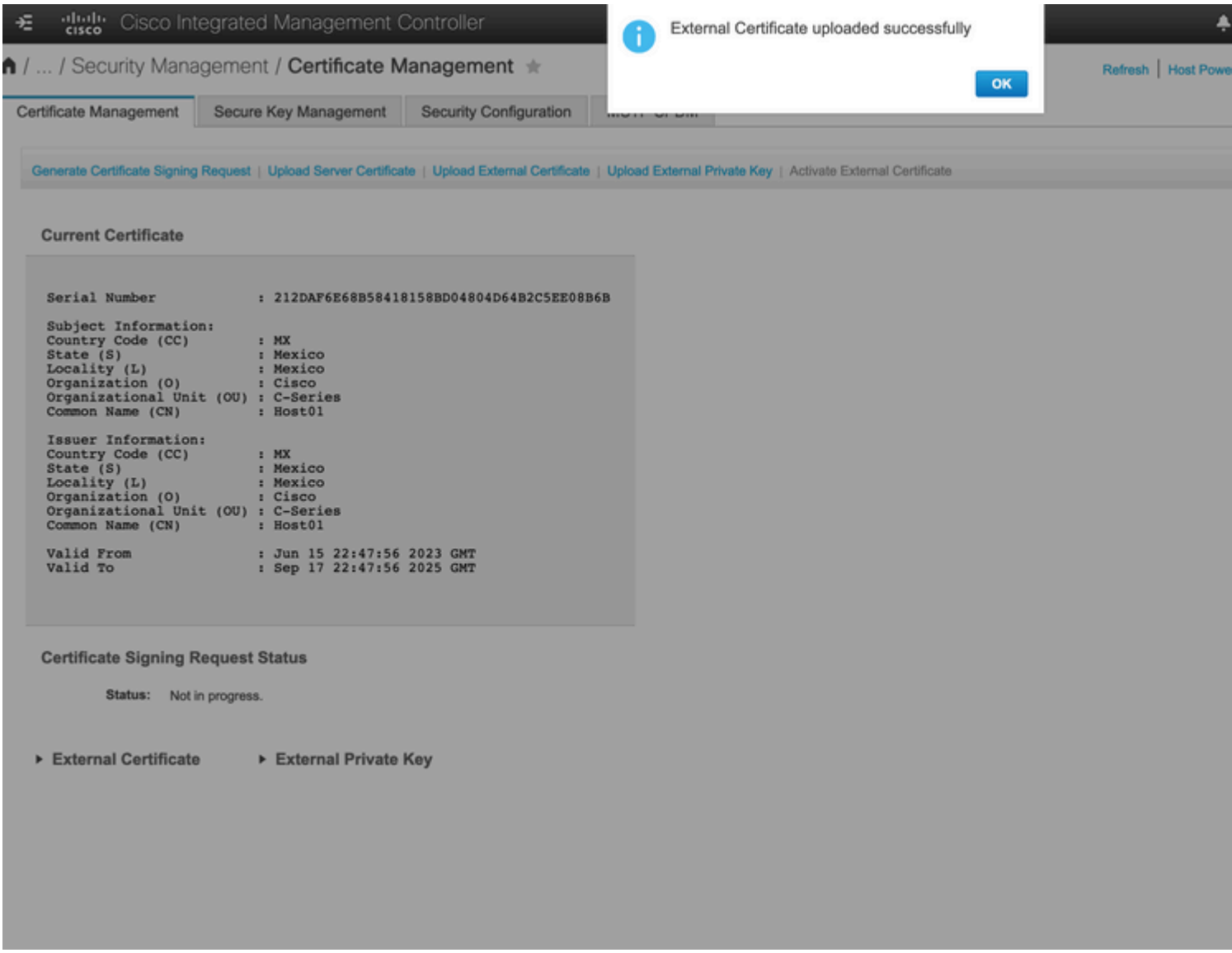
```
<#root>
[root@redhat ~]#
openssl x509 -in server.crt -purpose

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 ~]#
```

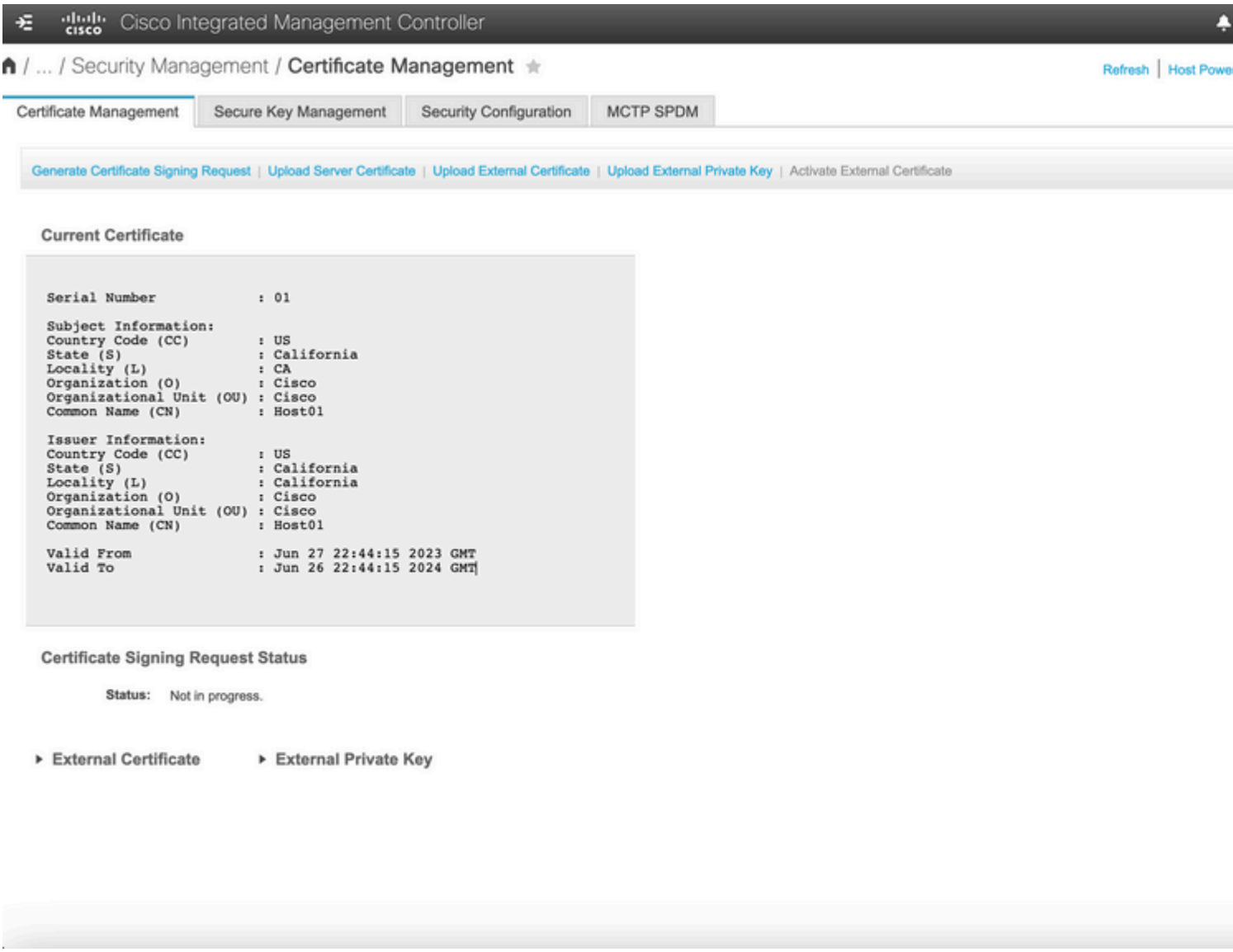
Schritt 6: Laden Sie das Serverzertifikat wie im Bild dargestellt hoch.



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Navigieren Sie zu **Admin > Certificate Management**, und überprüfen Sie das aktuelle Zertifikat wie im Bild dargestellt.



Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

- Cisco Bug-ID CSCup26248 - Das CA SSL-Zertifikat eines Drittanbieters kann nicht in CIMC 2.0 hochgeladen werden.(1a)
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.