Generieren Sie das Standardzertifikat im Intersight-verwalteten Modus neu.

Inhalt

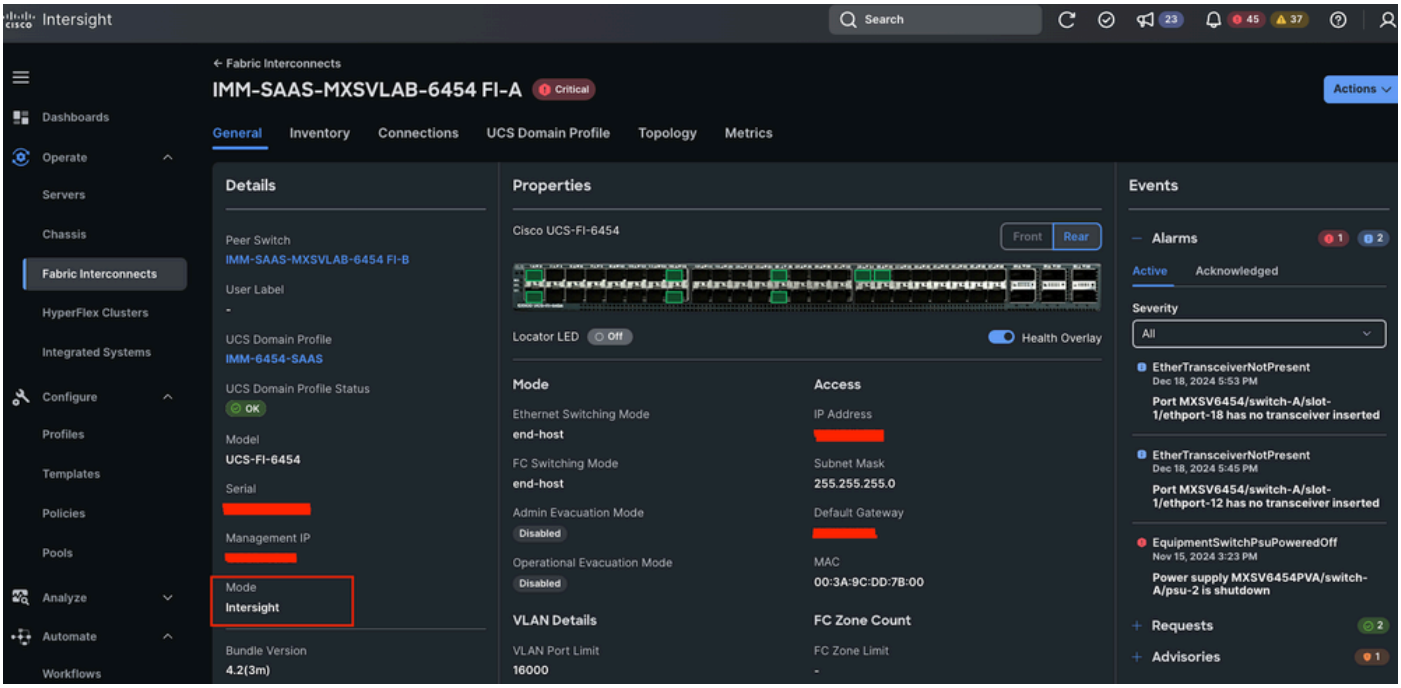
Einleitung

Dieses Dokument beschreibt den Prozess zur Verlängerung eines Fabric Interconnect selbst-signierten Zertifikats in Intersight-Umgebungen (SAAS oder Appliance).

Voraussetzungen

Anforderungen

UCS-Domäne im Intersight-Managed-Modus



Verwendete Komponenten

- Fabric Interconnect 6454
- Version: 4,2 (3 m)

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.

Selbstsigniertes Zertifikat generieren

Cisco empfiehlt, CA-signierte Zertifikate für den Zugriff auf die Appliance zu verwenden, da moderne Browser den Zugriff einschränken können, wenn selbstsignierte Zertifikate verwendet werden. Mit der Intersight Virtual Appliance können Sie ein selbstsigniertes Zertifikat generieren, um dessen Gültigkeit zu verlängern, wenn das von Cisco bereitgestellte Zertifikat abläuft.

Beim Generieren eines neuen selbstsignierten Zertifikats wird das vorhandene SSL-Zertifikat ersetzt, wodurch Sie sich möglicherweise von der aktuellen Browsersitzung abmelden. Wenn Sie nicht abgemeldet sind, aktualisieren Sie Ihren Browser, um das neue Zertifikat anzuwenden. Um die Aktualisierung zu bestätigen, klicken Sie auf das Sperr- oder Warnsymbol neben der URL in der Adressleiste Ihres Browsers. Nach der Aktualisierung gelangen Sie auf die Seite Einstellungen > Zertifikate, ohne sich erneut anmelden zu müssen.

Die Benutzeroberfläche der Gerätekonsole verwendet ein selbstsigniertes Zertifikat, für das der Common Name (CN) als Switch festgelegt ist. Dieses Zertifikat wird beim ersten Einschalten und Konfigurieren des Fabric Interconnects (FI) generiert. Das selbstsignierte Zertifikat ist 365 Tage gültig, d. h. dass alle FIs, die über ein Jahr laufen, abgelaufen sind.

Einige Kunden verwenden automatisierte Überwachungstools, um die IP-Adresse oder den Hostnamen des Geräts über HTTPS zu streichen und das Ablaufdatum des Zertifikats zu validieren. Nach Ablauf des Zertifikats können diese Tools Alarme auslösen, sodass Überwachungs- und Sicherheitsteams das Zertifikat als potenzielles Problem kennzeichnen.

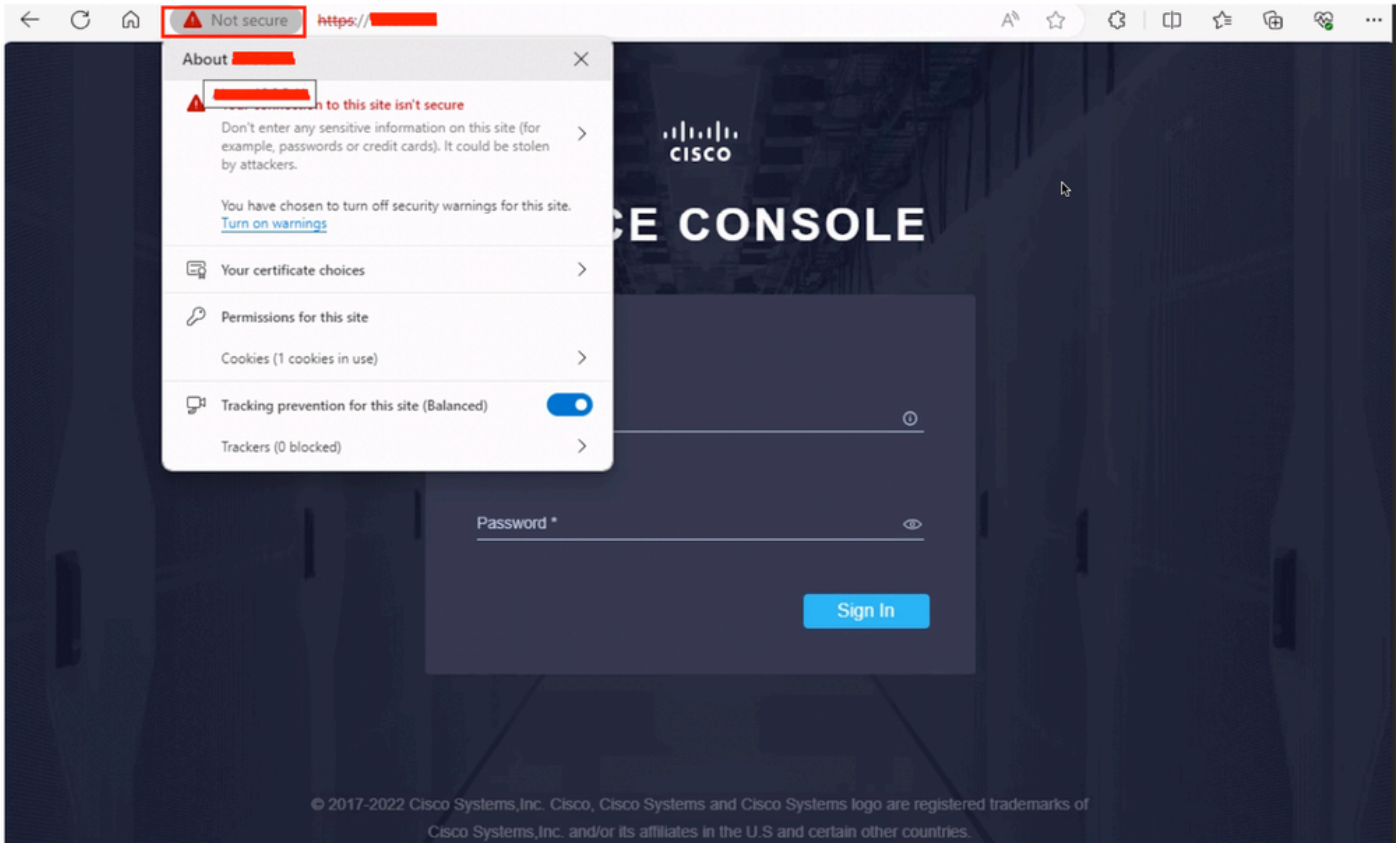
Da es sich um ein selbstsigniertes Zertifikat handelt, zeigen Webbrowser zudem eine Warnung "Nicht sicher" an. Diese Warnung kann auch angezeigt werden, wenn das Zertifikat abgelaufen ist, was weitere Sicherheitsbedenken hervorrufen kann.

Um diese Probleme zu vermeiden, wird empfohlen, das Zertifikat proaktiv zu erneuern oder zu ersetzen.

Problem/Symptom

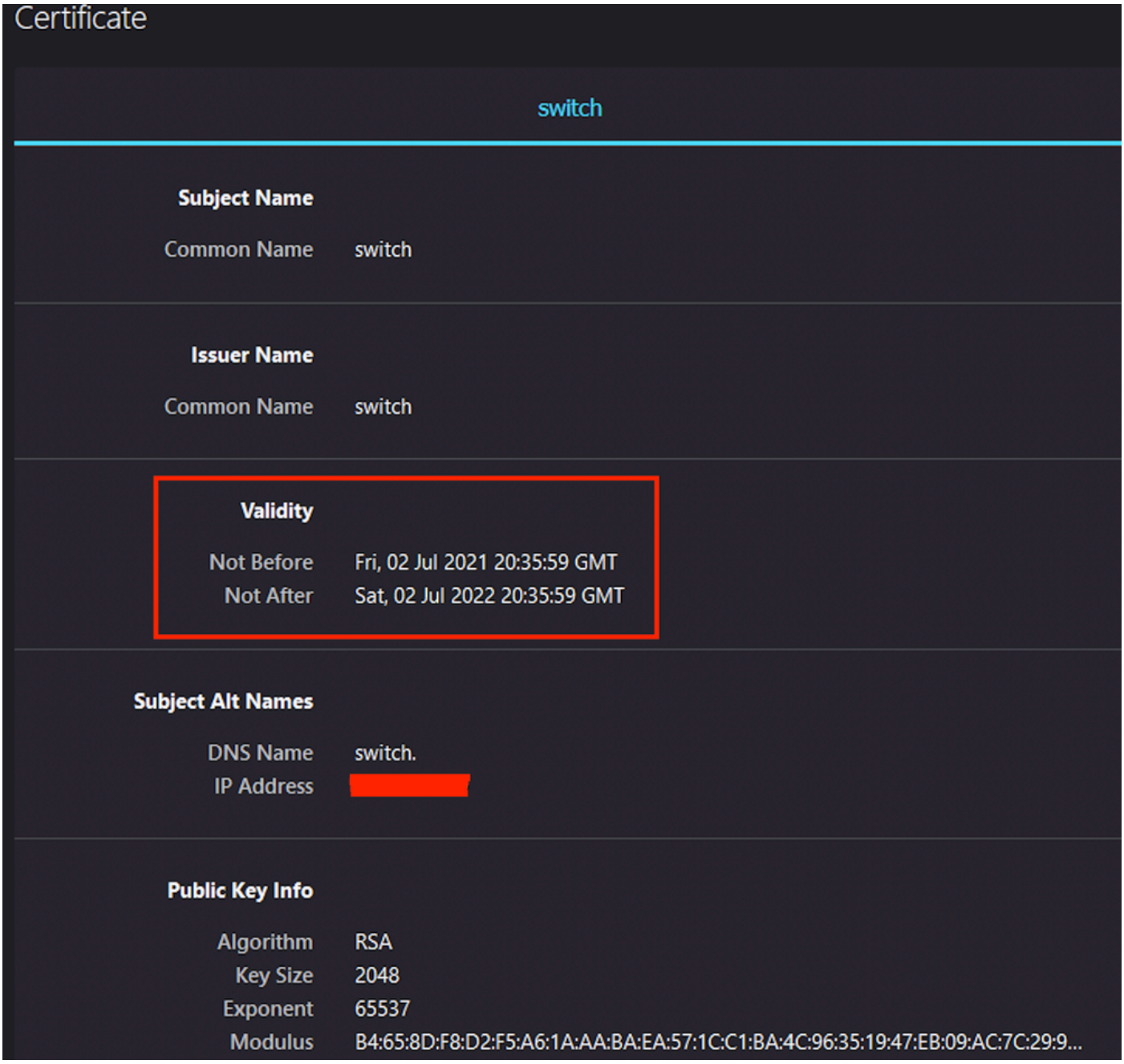
Wenn Sie auf die Gerätekonsole zugreifen, wird die Site als nicht sicher erkannt.

Anmerkung: Für den Zugriff auf die Gerätekonsole benötigen Sie die IP-Adresse des Fabric Interconnects.



Zertifikatfehler

Wenn Sie auf die Zertifikatinformationen klicken, wird das Ablaufdatum der Zertifizierung angezeigt.



Ablaufdatum des Zertifikats

Zertifikat neu generieren

Um das Standardzertifikat in Intersight zu erneuern, müssen Sie die Gerätekonsole neu starten oder den Fabric Interconnect neu starten (nicht empfohlen).

Führen Sie die folgenden Schritte aus, um das Standardzertifikat in Intersight manuell neu zu generieren:

1. Öffnen Sie eine SSH-Sitzung mit der IP-Adresse eines Fabric Interconnects.
2. Führen Sie den folgenden Befehl aus:

```
UCS# generate-self-signed-certificate
```

Wenn das Zertifikat erfolgreich generiert wurde, wird Folgendes angezeigt:

```
hostname is IMM-FI6454
Successfully generated the self-signed-certificates
Successfully restarted the web-server
```

Verwenden Sie den folgenden Befehl, um das tatsächliche Zertifikat zu überprüfen und seine Änderung zu bestätigen:

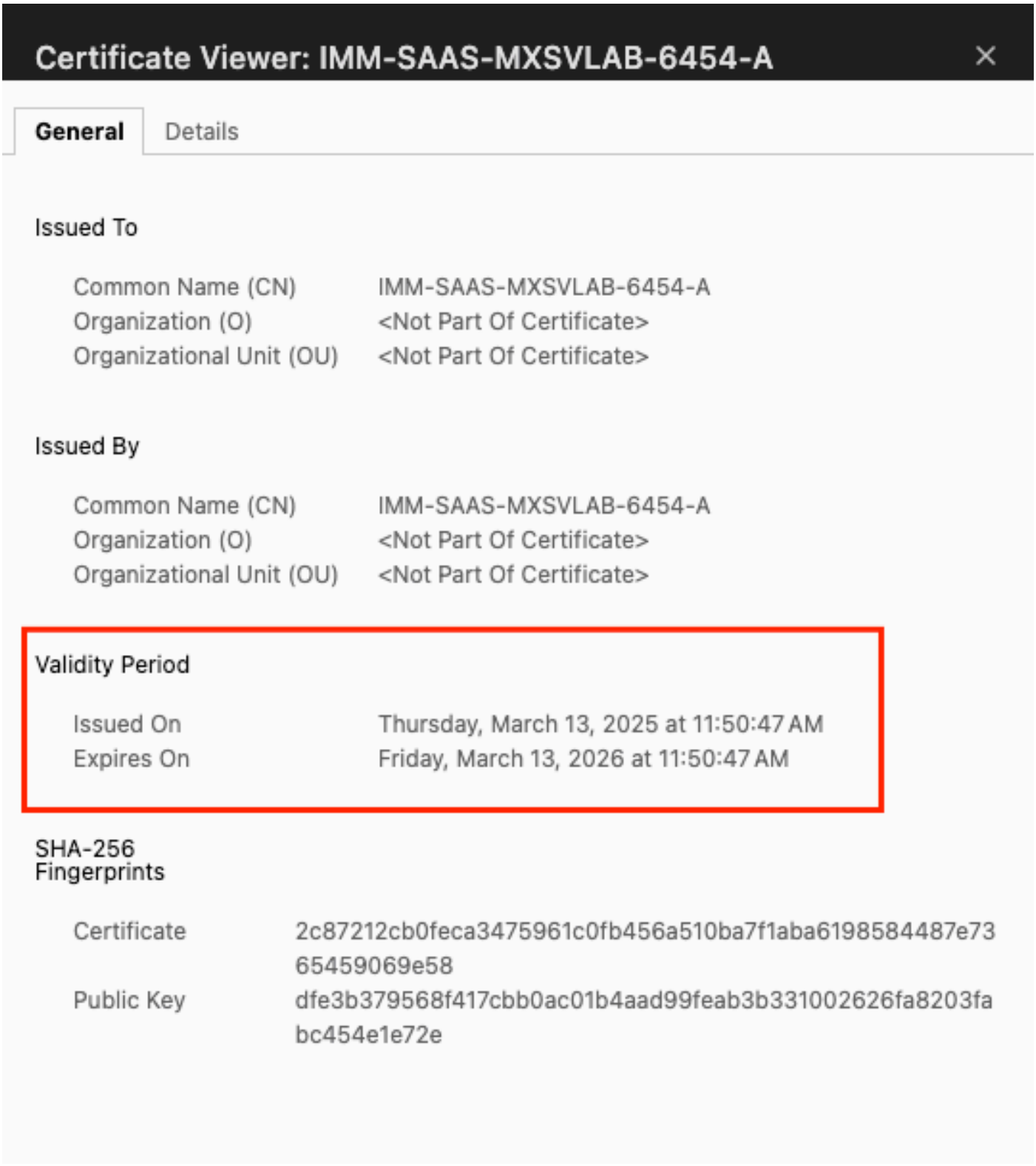
```
UCS# show self-signed-certificate
```

Beispiel:

```
-----BEGIN CERTIFICATE-----
MIIC+DCCAeCgAwIBAgICBnowDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAxMXSU1N
LVNBQVMtTVhTVkxBQiO2NDU0LUEwHhcNMjUwMzEyMjI1MTM4WhcNMjYwMzEyMjI1
MTM4WjAiMSAwHgYDVQQDExdJTU0tU0FBUy1NWFNWTEFCLTY0NTQtQTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK+Q9oAU2rHxtV5stg9vfCeKQ+9+n5Ke
oz6IKOeEDufeRcBYepaJlEhffvdLp/uOh/NnyphT4mVLiJxh6dTTIhW58G8LaGNV
hIRtNAX984eLCs1nSG3o3tzJ3+e5t04G6klAcj43HiKY+oRCEs+oiUsQlYpBjHoy
FGxMT8wpnNMIg59mKVTuUeC4r6ACnyy1CRNp8qD8Rf4lIBU/jTI/jPdzE2//9rAo
G85qhZ46vIOdLu1jv/ySszQkATFA15KHFETnyTkptdlJH8mcO33edJ1Xq9plebMp
dtn18zj+2qxQq8ErZ6doFdkOuyuq3N6QOdbfdefKKuiFvkCGv4GwRG8CAwEAAaM4
MDYwDgYDVR0PAQH/BAQDAgKkMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA8GA1UdEQQI
MAaHBH8AAAEwDQYJKoZIhvcNAQELBQADggEBAFn+v4ehwLFi/mcHWA4ld03JBkvI
RIlbFPHjOykzmAN8E1XoJlLciCxA3gHUzPP6lT+2VpeAXAoWzIlgUlm2GwPzZbCQ
nz2v7NpGHchaXAEi756IMmCm2IJ2jOuS9p9v3AAX3gLUp43SeCQN+C2nNOcZgmZr
/K1CoNkIUXdVI8nxEDCMFPezL1SXdNa2c4AB699teolCNc65tnnNDjsxkLkL7bTx
P5euETVi5CizQQpjcZzXEMHv3XdvXtkzyAATjRmvUS8lxyXxiisMjMl7f8zXkLnG
n7ZKR746BXgXufmSOzITtbpvgI9+6PnauoWOh3EH7rGmJyZnn5L62/oaoy4=
-----END CERTIFICATE-----
```

Anmerkung: Wenn Sie das Zertifikat vor der Verlängerung prüfen, stellen Sie sicher, dass es nach der Verlängerung geändert wird.

Schließlich sollte das Zertifikat wie folgt aussehen:



Zertifikatsvalidierung

Zugehörige Informationen

[Zertifikate in Intersight Virtual Appliance](#)

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.