Rigenera il certificato predefinito in modalità Intersight Managed

Sommario

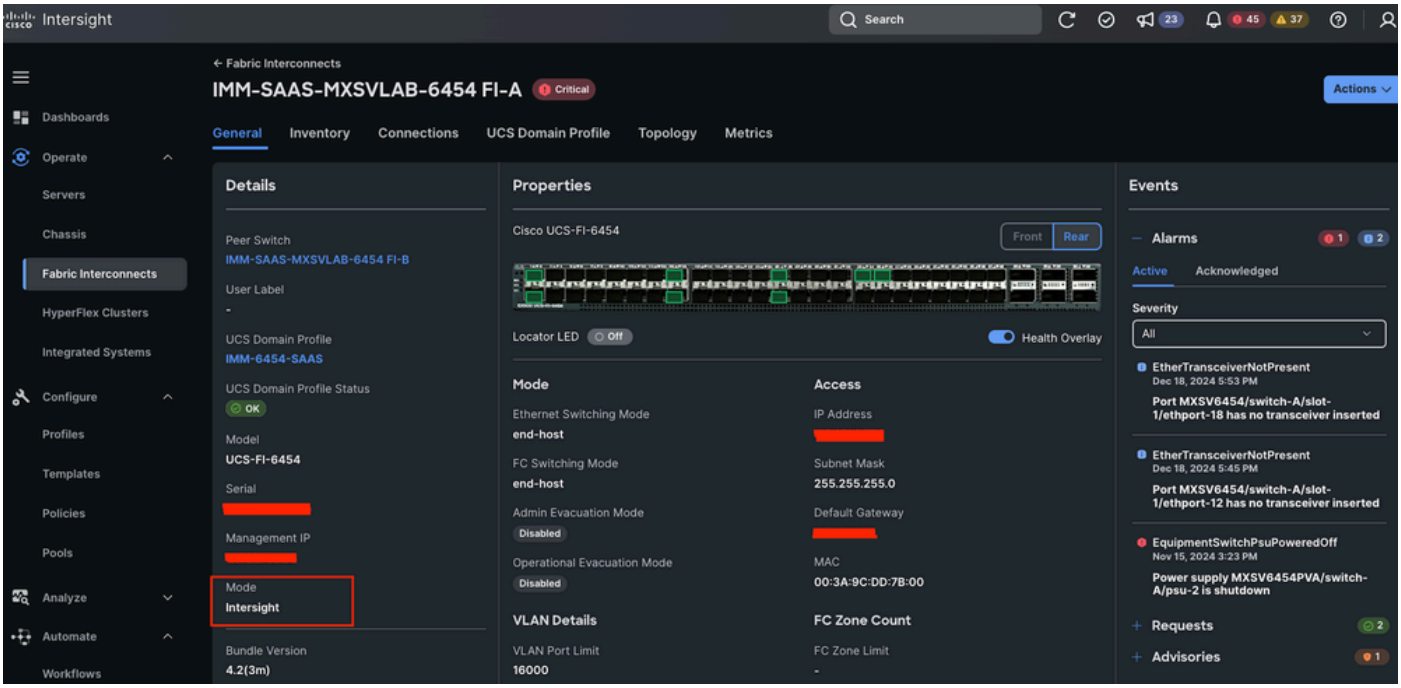
Introduzione

In questo documento viene descritto il processo di rinnovo di un certificato autofirmato Fabric Interconnect in ambienti Intersight (ASA o appliance).

Prerequisiti

Requisiti

Dominio UCS in modalità Intersight Managed.



Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Genera certificato autofirmato

Cisco consiglia di utilizzare certificati firmati dall'autorità di certificazione per accedere all'accessorio, in quanto i browser moderni possono limitare l'accesso se vengono utilizzati certificati autofirmati. Intersight Virtual Appliance consente di generare un certificato autofirmato per estenderne la validità se il certificato fornito da Cisco scade.

Durante la generazione di un nuovo certificato autofirmato, il certificato SSL esistente viene sostituito e l'utente viene potenzialmente disconnesso dalla sessione corrente del browser. Se non si è disconnessi, aggiornare il browser per applicare il nuovo certificato. Per confermare l'aggiornamento, fare clic sull'icona lock (Blocco) o warning (Avviso) accanto all'URL nella barra degli indirizzi del browser. Dopo l'aggiornamento, viene visualizzata la pagina Impostazioni > Certificati senza dover eseguire di nuovo l'accesso.

Nell'interfaccia utente della console del dispositivo viene utilizzato un certificato autofirmato con il nome comune impostato su switch. Questo certificato viene generato la prima volta che l'interconnessione fabric (FI) viene accesa e configurata. Il certificato autofirmato è valido per 365 giorni, il che significa che qualsiasi FI in esecuzione da oltre un anno ha un certificato scaduto.

Alcuni clienti utilizzano strumenti di monitoraggio automatizzato per eseguire lo scraping dell'IP o del nome host del dispositivo su HTTPS e convalidare la data di scadenza del certificato. Quando il certificato scade, questi strumenti possono attivare allarmi, portando i team di sicurezza e di osservabilità a contrassegnarlo come un potenziale problema.

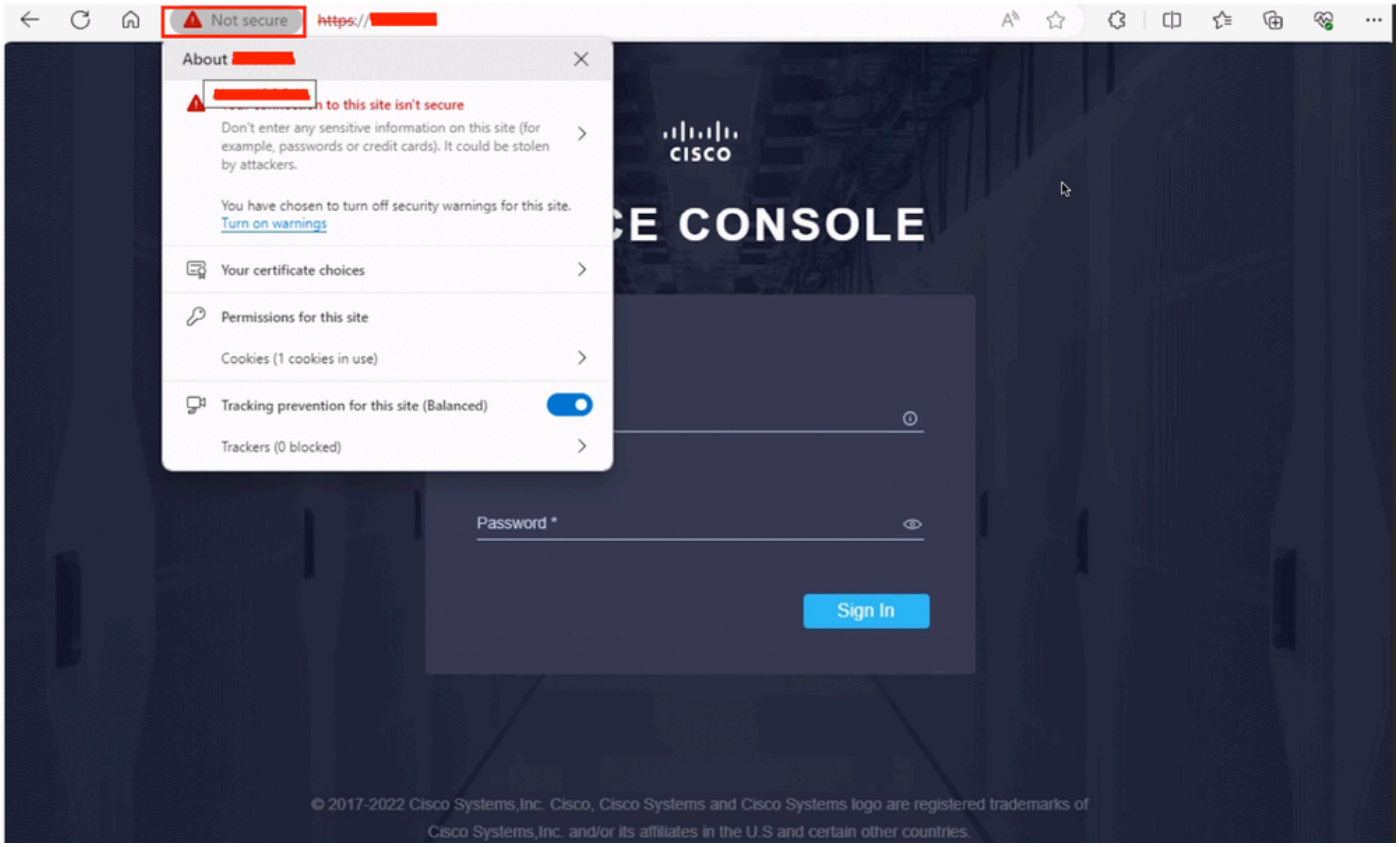
Inoltre, poiché il certificato è autofirmato, nei browser Web viene visualizzato un avviso di protezione da protezione. È possibile che questo avviso venga visualizzato anche se il certificato è scaduto, con potenziali problemi di protezione.

Per evitare questi problemi, si consiglia di rinnovare o sostituire il certificato in modo proattivo.

Problema/Sintomo

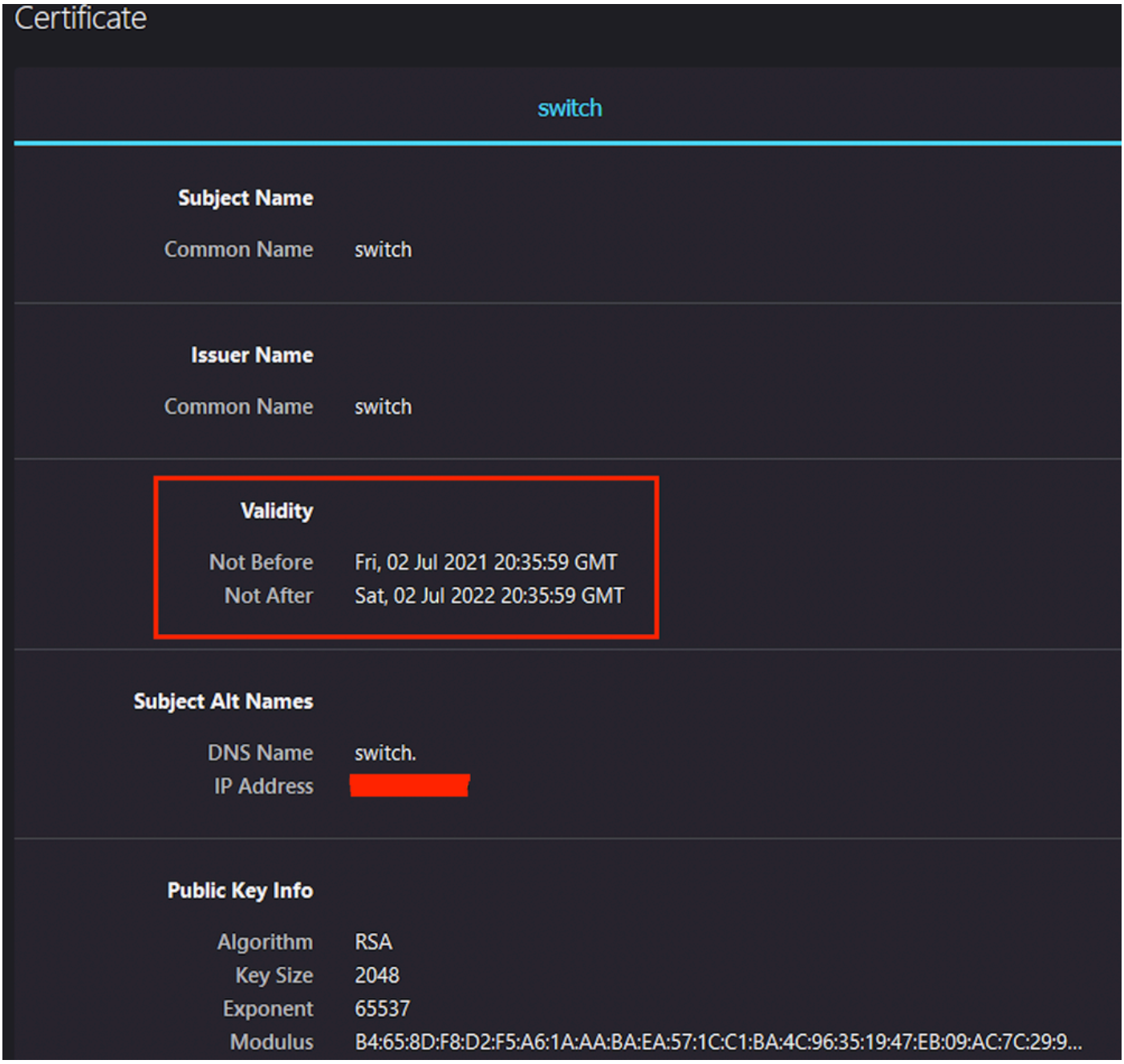
Quando si accede alla console del dispositivo, il sito non è protetto.

Nota: Per l'accesso alla console del dispositivo, è necessario l'indirizzo IP dell'interconnessione fabric.



Errore certificato

Quando si fa clic sulle informazioni del certificato, viene visualizzata la data di scadenza della certificazione.



Data di scadenza certificato

Rigenera il certificato

Per rinnovare il certificato predefinito in Intersight, è necessario riavviare la console del dispositivo o l'interconnessione del fabric (scelta non consigliata).

Per rigenerare manualmente il certificato predefinito in Intersight, attenersi alla procedura descritta di seguito.

1. Aprire una sessione SSH usando l'indirizzo IP di un'interconnessione fabric.
2. Eseguire il comando:

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

Se il certificato è stato generato correttamente, verrà visualizzato quanto segue:

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

Per verificare il certificato effettivo e confermarne la modifica, utilizzare questo comando:

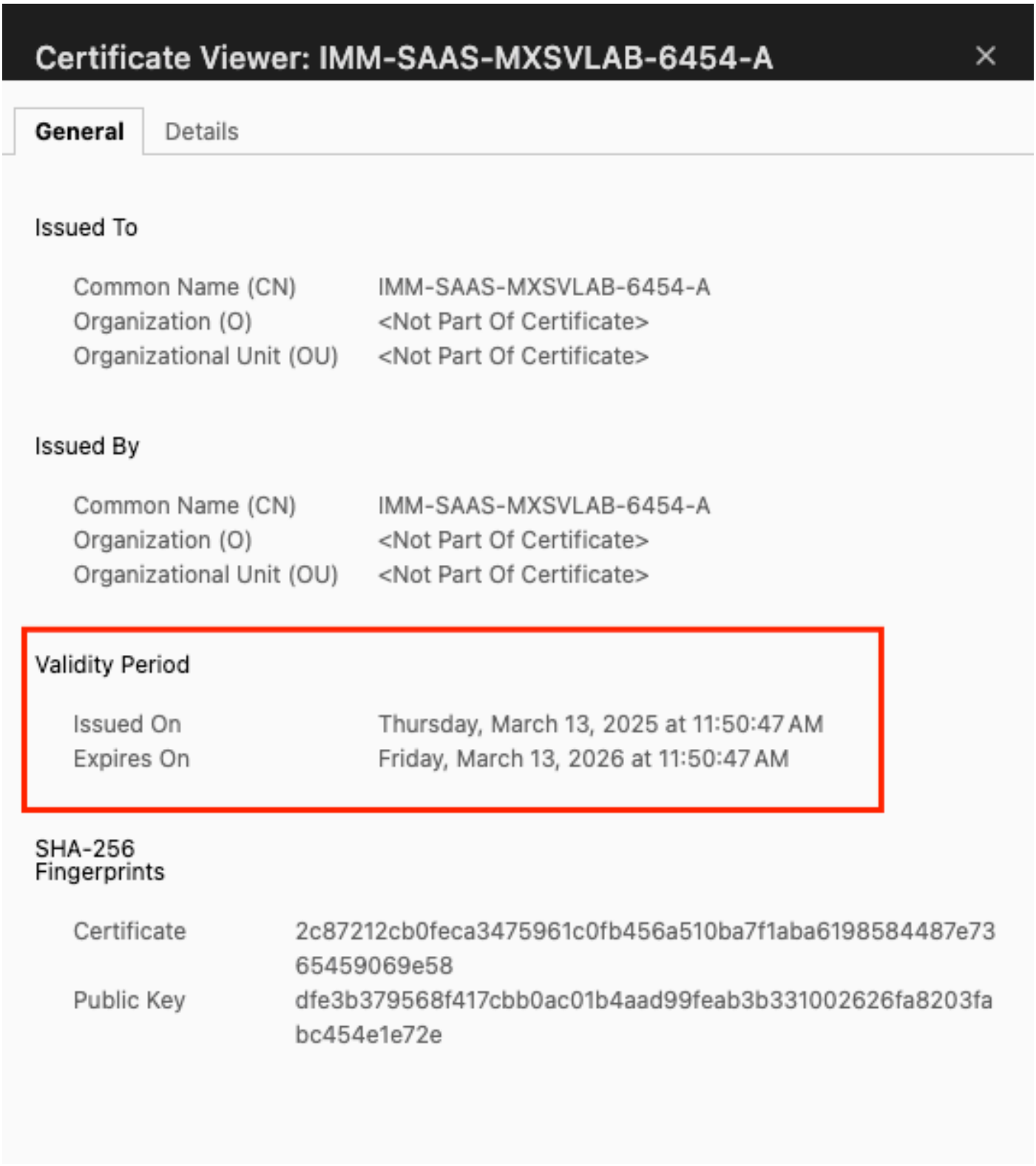
```
UCS# show self-signed-certificate
```

Output di esempio:

```
-----BEGIN CERTIFICATE-----
MIIC+DCCAeCgAwIBAgICBnowDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAxMXSU1N
LVNBQVMtTVhTVkxBQiO2NDU0LUEwHhcNMjUwMzEyMjI1MTM4WhcNMjYwMzEyMjI1
MTM4WjAiMSAwHgYDVQQDExdJTU0tU0FBUy1NWFNWTEFCLTY0NTQtQTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK+Q9oAU2rHxtV5stg9vfCeKQ+9+n5Ke
oz6IKOeEDufeRcBYepaJlEhffvdLp/uOh/NnyphT4mVLiJxh6dTTIhW58G8LaGNV
hIRtNAX984eLCs1nSG3o3tzJ3+e5tO4G6klAcj43HiKY+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-----
```

Nota: Se si controlla il certificato prima del rinnovo, assicurarsi che venga modificato dopo il processo di rinnovo.

Il certificato dovrebbe infine avere il seguente aspetto:



Convalida certificato

Informazioni correlate

[Certificati in Intersight Virtual Appliance](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).