Regenere el Certificado Predeterminado en el Modo Administrado de Intersight

Contenido

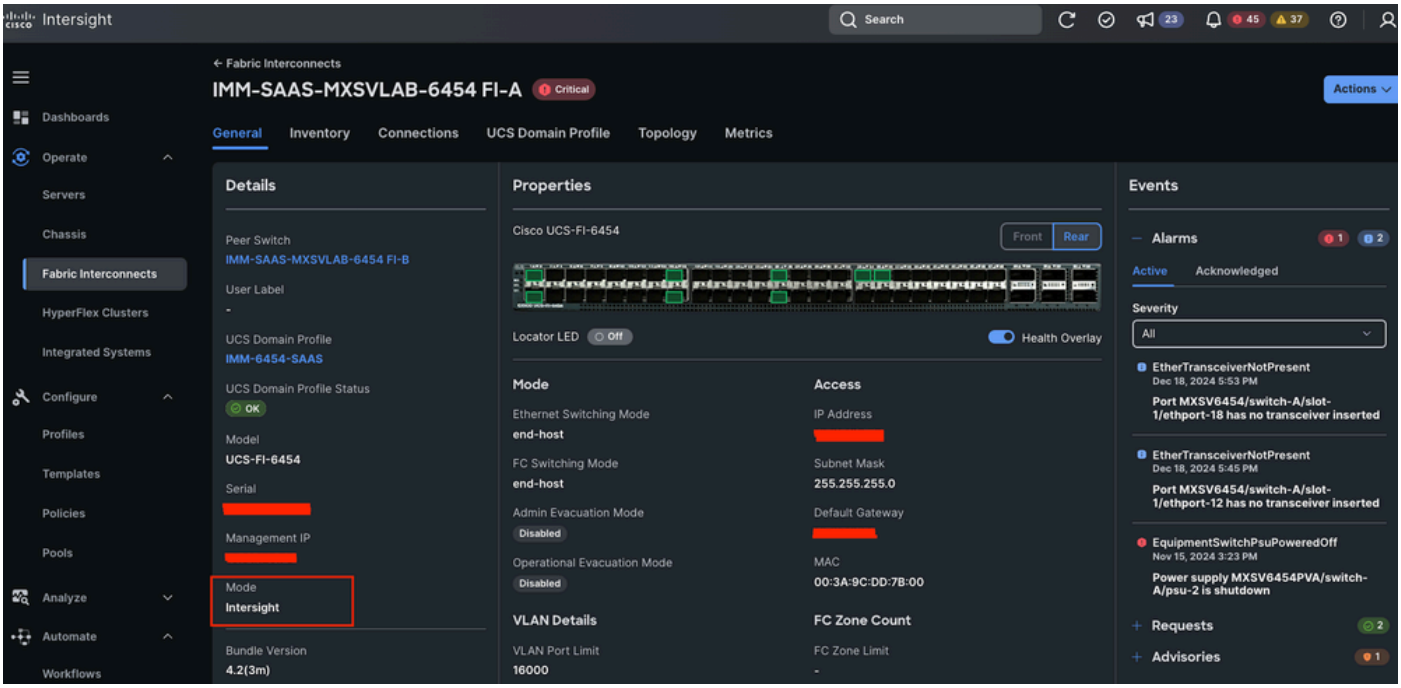
Introducción

Este documento describe el proceso para renovar un certificado autofirmado de Fabric Interconnect en entornos Intersight (SAAS o dispositivo).

Prerequisites

Requirements

Dominio UCS en el modo de gestión de información privilegiada.



Componentes Utilizados

- Fabric Interconnect 6454
- Versión: 4.2(3 m)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Generar certificado de firma automática

Cisco recomienda utilizar certificados firmados por CA para acceder al dispositivo, ya que los exploradores modernos pueden restringir el acceso si se utilizan certificados autofirmados. El dispositivo virtual Intersight permite generar un certificado autofirmado para ampliar su validez si caduca el certificado proporcionado por Cisco.

Al generar un nuevo certificado autofirmado, se reemplaza el certificado SSL existente, lo que puede cerrar la sesión actual del explorador. Si no ha cerrado la sesión, actualice el explorador para aplicar el nuevo certificado. Para confirmar la actualización, haga clic en el icono de bloqueo o advertencia situado junto a la URL en la barra de direcciones del navegador. Después de actualizar, se le dirigirá a la página Settings > Certificates sin necesidad de volver a iniciar sesión.

La interfaz de usuario de la consola del dispositivo (IU) utiliza un certificado autofirmado con el nombre común (CN) establecido en conmutador. Este certificado se genera la primera vez que se enciende y configura Fabric Interconnect (FI). El certificado autofirmado es válido durante 365 días, lo que significa que cualquier FI que se ejecute durante más de un año tiene un certificado caducado.

Algunos clientes utilizan herramientas de supervisión automatizadas para rastrear la IP o el nombre de host del dispositivo a través de HTTPS y validar la fecha de caducidad del certificado. Cuando caduca el certificado, estas herramientas pueden activar alarmas, lo que puede llevar a que los equipos de seguridad y observación marquen el certificado como un problema potencial.

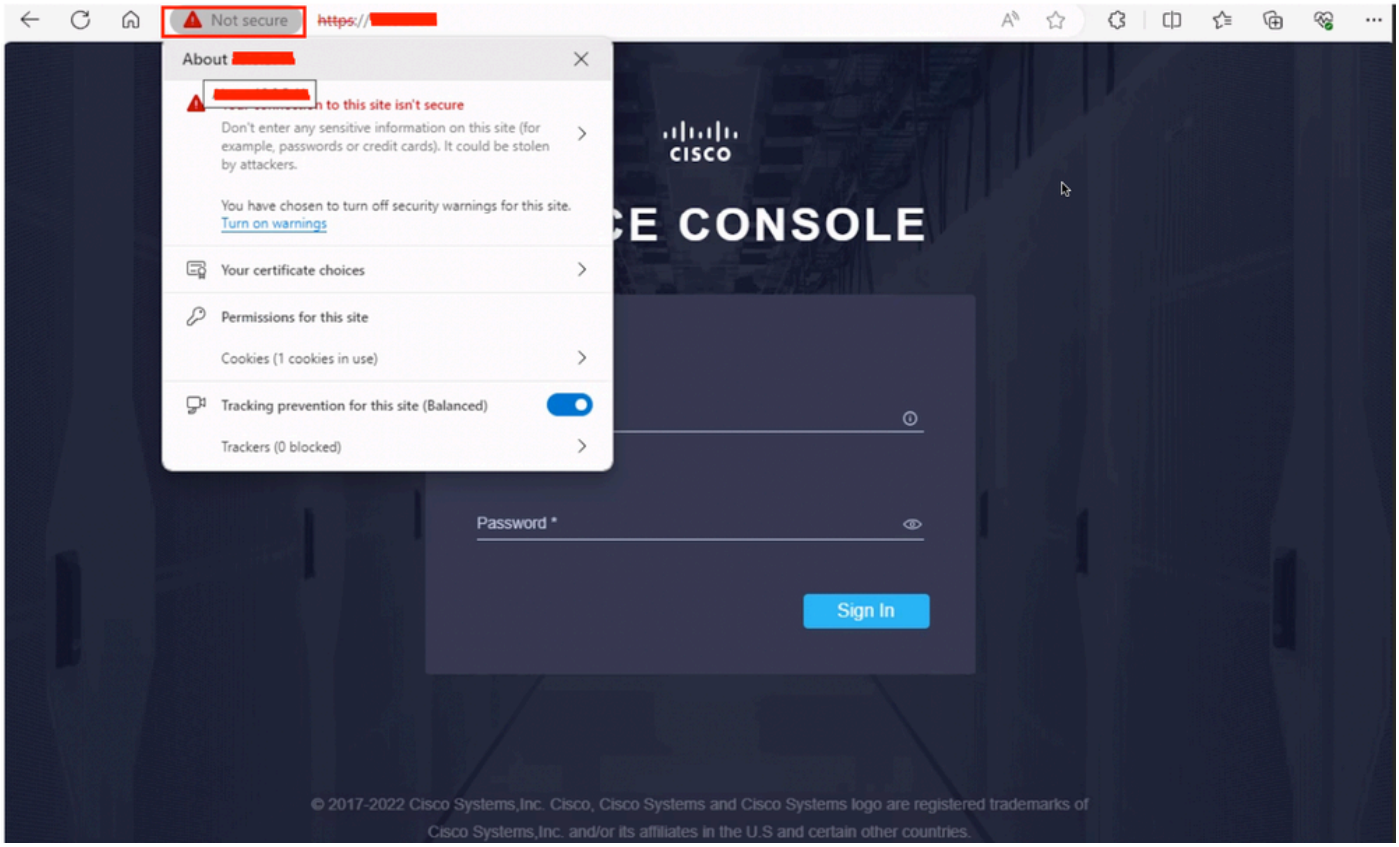
Además, como el certificado está autofirmado, los exploradores web muestran una advertencia de No seguro. Esta advertencia también puede aparecer si el certificado ha caducado, lo que puede causar más problemas de seguridad.

Para evitar estos problemas, se recomienda renovar o reemplazar el certificado de forma proactiva.

Problema/síntoma

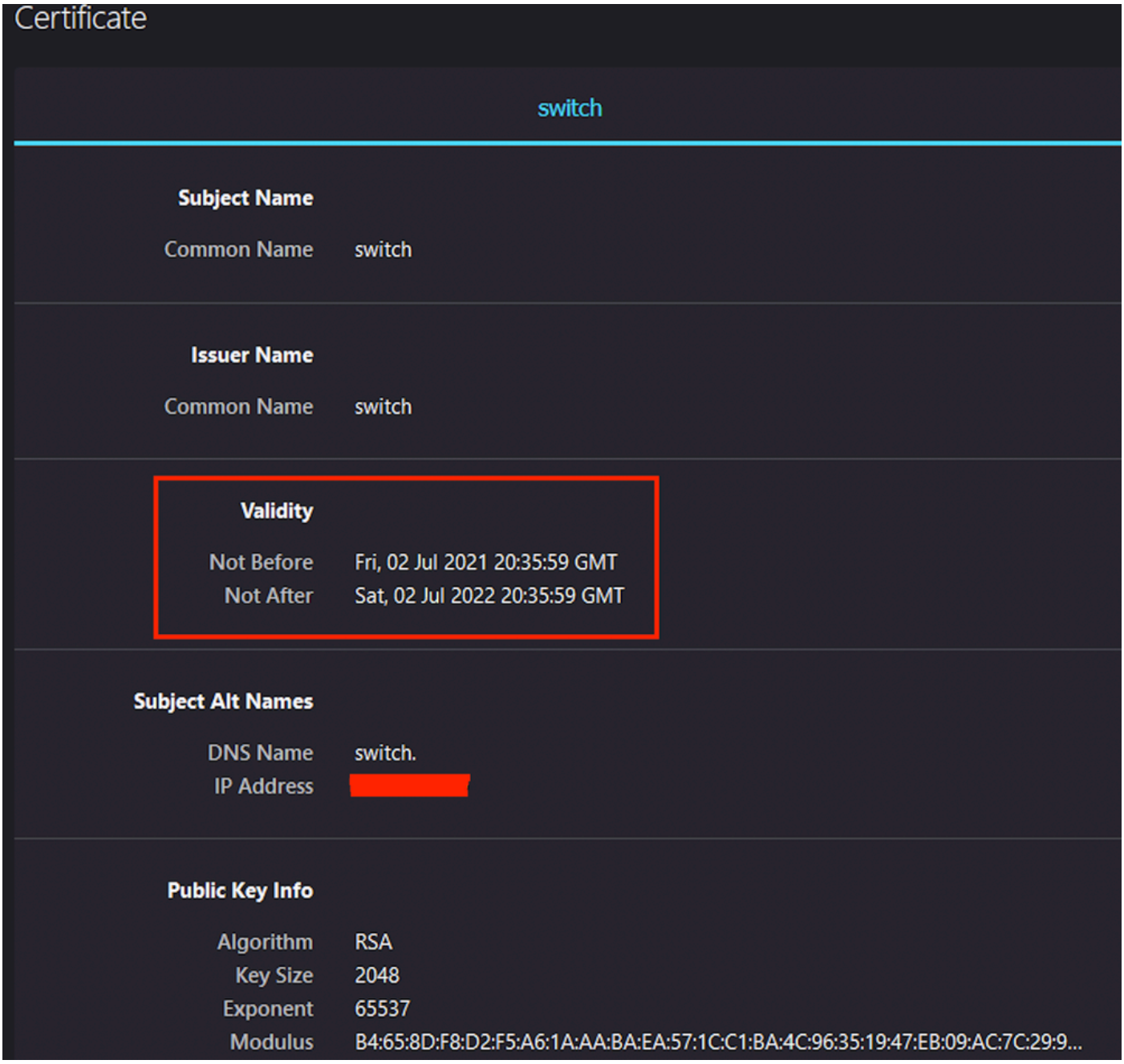
Verá que el sitio no es seguro cuando acceda a la consola del dispositivo.

Nota: Para acceder a la consola del dispositivo, necesita la dirección IP del Fabric Interconnect.



Error de certificado

Al hacer clic en la información del certificado, verá la fecha de caducidad de la certificación.



Fecha de vencimiento del certificado

Regenere el certificado

Para renovar el certificado predeterminado en Intersight, debe reiniciar la consola del dispositivo o Fabric Interconnect (no recomendado).

Utilice estos pasos para regenerar manualmente el certificado predeterminado en Intersight:

1. Abra una sesión SSH utilizando la dirección IP de un Fabric Interconnect.
2. Ejecute el comando :

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

Si el certificado se ha generado correctamente, verá:

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

Para comprobar el certificado real y confirmar que ha cambiado, utilice este comando:

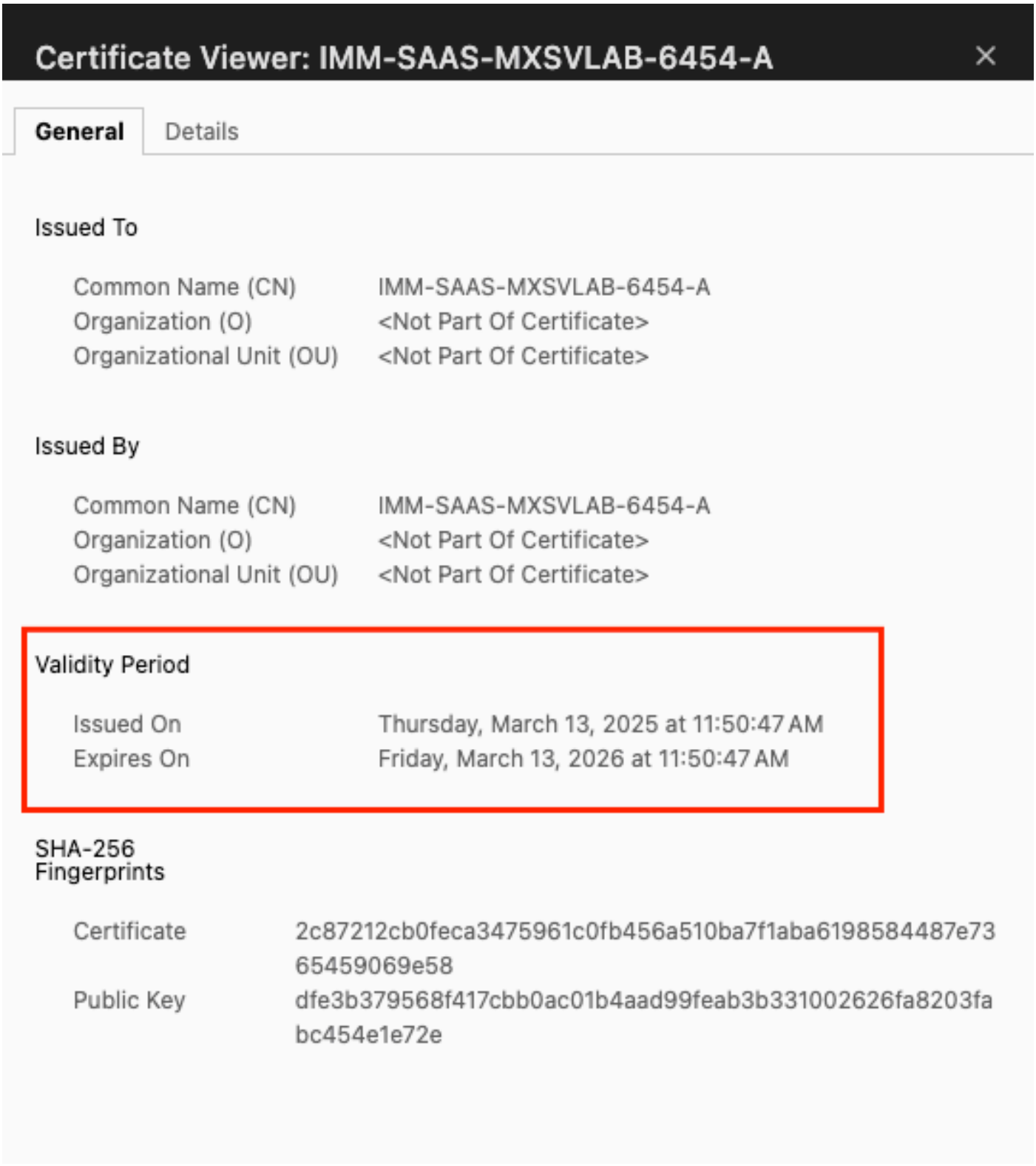
```
UCS# show self-signed-certificate
```

Ejemplo de salida:

```
-----BEGIN CERTIFICATE-----
MIIC+DCCAeCgAwIBAgICBnowDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAxMXSU1N
LVNBQVMtTVhTVkxBQi02NDU0LUEwHhcNMjUwMzEyMjI1MTM4WhcNMjYwMzEyMjI1
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-----
```

Nota: Si comprueba el certificado antes de la renovación, asegúrese de que cambia después del proceso de renovación.

Por último, el certificado debe tener el siguiente aspecto:



Validación de certificados

Información Relacionada

[Certificados en el dispositivo virtual Intersight]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).