

Regenere el Certificado Predeterminado en el Modo Administrado de Intersight

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Generar certificado de firma automática](#)

[Problema/síntoma](#)

[Regenere el certificado](#)

[Información Relacionada](#)

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.

The screenshot displays the Cisco Intersight interface for a Fabric Interconnect (FI-A). The main content area is divided into several sections:

- Details:** Shows the Peer Switch (IMM-SAAS-MXSVLAB-6454 FI-B), User Label, UCS Domain Profile (IMM-6454-SAAS), and UCS Domain Profile Status (OK).
- Properties:** Displays the Cisco UCS-FI-6454 model, Locator LED (Off), and Health Overlay (On).
- Mode:** Shows the Ethernet Switching Mode (end-host), FC Switching Mode (end-host), Admin Evacuation Mode (Disabled), and Operational Evacuation Mode (Disabled).
- Access:** Lists IP Address, Subnet Mask (255.255.255.0), Default Gateway, and MAC (00:3A:9C:DD:7B:00).
- VLAN Details:** Shows the VLAN Port Limit (16000) and FC Zone Count.
- Events:** Displays a list of alarms, including 'EtherTransceiverNotPresent' (Dec 18, 2024 5:53 PM) and 'EquipmentSwitchPsuPoweredOff' (Nov 15, 2024 3:23 PM).

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.

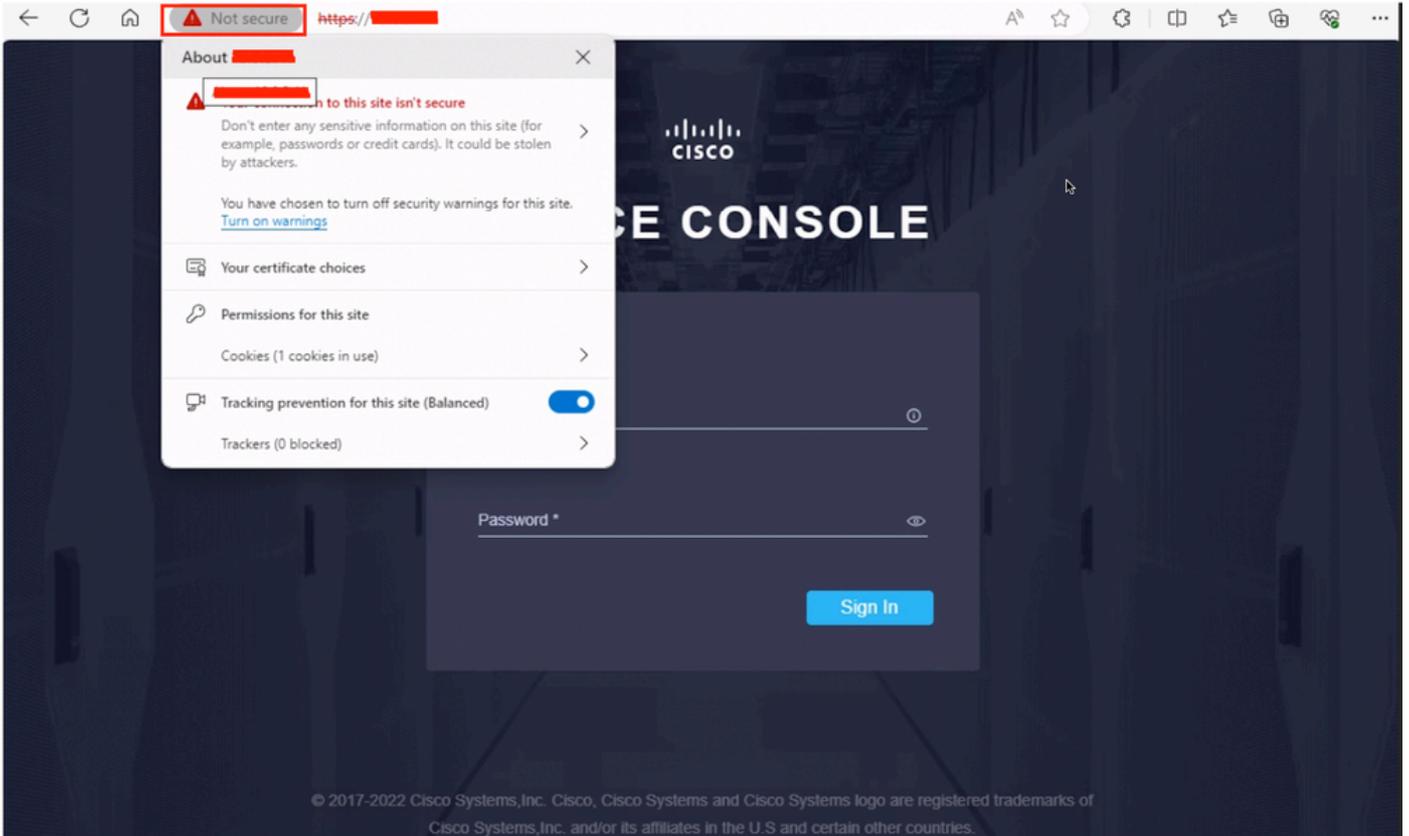
Además, como el certificado está autofirmado, los exploradores web muestran una advertencia de No seguro. Esta advertencia también puede aparecer si el certificado ha caducado, lo que puede causar más problemas de seguridad.

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.

Certificate

switch

Subject Name

Common Name switch

Issuer Name

Common Name switch

Validity

Not Before Fri, 02 Jul 2021 20:35:59 GMT
Not After Sat, 02 Jul 2022 20:35:59 GMT

Subject Alt Names

DNS Name switch.
IP Address [REDACTED]

Public Key Info

Algorithm RSA
Key Size 2048
Exponent 65537
Modulus B4:65:8D:F8:D2:F5:A6:1A:AA:BA:EA:57:1C:C1:BA:4C:96:35:19:47:EB:09:AC:7C:29:9...

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
LVNBQVMtTVhTVkxkYzQ1ODNDU0LUeW5hcnMjUwMzEyMjI1MTM4WhcNMjYwMzEyMjI1
MTM4WjAiMSAwHgYDVQDExdJTU0tU0FBYy1NWFWTEFCLTY0NTQtQTCCASiWdQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBBAK+Q9oAU2rHxtV5stg9vfCeKQ+9+n5Ke
oz6IKOeEDufeRcBYepaJlEhffvdLp/u0h/NnyphT4mVLiJxh6dTTIhW58G8LaGNV
hIRtNAX984eLCS1nSG3o3tzJ3+e5t04G6k1Acj43HiKY+oRCEs+oiUsQ1YpBjHoy
FGxMT8wpmNMIg59mKVtuUeC4r6ACnyy1CRNp8qD8Rf41IBU/jTI/jPdzE2//9rAo
G85qhZ46vI0dLu1jv/ySszQkATFA15KHFETnyTkptd1JH8mc033edJ1Xq9p1ebMp
dtn18zj+2qxQq8ErZ6doFdkOuyuq3N6Q0dbfdefKkuiFvkCGv4GwRG8CAwEAAAM4
MDYwDgYDVR0PAQH/BAQDAgKkMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA8GA1UdEQQI
MAAaHBH8AAAEdQYJKoZIhvcNAQELBQADggEBAFn+v4ehwLFi/mcHWA41d03JBkvI
RI1bFPHj0ykmAN8E1XoJ1LciCxA3gHUzPP61T+2VpeAXAoWzI1gU1m2GwPzZbCQ
nz2v7NpGHchaXAEi756IMmCm2IJ2jOuS9p9v3AAX3gLUp43SeCQN+C2nN0cZgmZr
/K1CoNkIUXdVI8nxEDCMFPezL1SXdNa2c4AB699teo1CNc65tnnNDjsxkLkL7bTx
P5euETVi5CizQQpjczZxEMHv3XdvXtkzyAATjRmvUS81xyXxiisMjM17f8zXkLnG
n7ZKR746BXgXufmS0zITtbpvgI9+6PnauoW0h3EH7rGmJyZnn5L62/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:

Certificate Viewer: IMM-SAAS-MXSVLAB-6454-A



General

Details

Issued To

Common Name (CN)	IMM-SAAS-MXSVLAB-6454-A
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	IMM-SAAS-MXSVLAB-6454-A
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Thursday, March 13, 2025 at 11:50:47 AM
Expires On	Friday, March 13, 2026 at 11:50:47 AM

SHA-256 Fingerprints

Certificate	2c87212cb0feca3475961c0fb456a510ba7f1aba6198584487e73 65459069e58
Public Key	dfe3b379568f417cbb0ac01b4aad99feab3b331002626fa8203fa bc454e1e72e

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).