

Intersight Managed Mode에서 기본 인증서 재생성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[자체 서명 인증서 생성](#)

[문제/증상](#)

[인증서 다시 생성](#)

[관련 정보](#)

소개

이 문서에서는 Intersight 환경(SAAS 또는 어플라이언스)에서 Fabric Interconnect 자체 서명 인증서를 갱신하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Intersight Managed Mode의 UCS 도메인

The screenshot displays the Intersight web interface for a Fabric Interconnect (IMM-SAAS-MXSVLAB-6454 FI-A) in Managed Mode. The interface 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:** Displays the IP Address, Subnet Mask (255.255.255.0), Default Gateway, MAC (00:3A:9C:DD:7B:00), and FC Zone Count.
- VLAN Details:** Shows the VLAN Port Limit (16000).
- Events:** Displays a list of alarms and requests. The 'Alarms' section shows two active alarms: 'EtherTransceiverNotPresent' (Dec 18, 2024 5:53 PM) and 'EquipmentSwitchPsuPoweredOff' (Nov 15, 2024 3:23 PM). The 'Requests' section shows two requests: 'Port MXSV6454/switch-A/slot-1/ethport-18 has no transceiver inserted' and 'Power supply MXSV6454PVA/switch-A/psu-2 is shutdown'.

사용되는 구성 요소

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

자체 서명 인증서 생성

최신 브라우저는 자체 서명 인증서를 사용하는 경우 액세스를 제한할 수 있으므로 CA 서명 인증서를 사용하여 어플라이언스에 액세스하는 것이 좋습니다. Intersight Virtual Appliance에서는 Cisco에서 제공한 인증서가 만료될 경우 유효성을 연장하기 위해 자체 서명 인증서를 생성할 수 있습니다.

새 자체 서명 인증서를 생성할 때 기존 SSL 인증서가 교체되어 현재 브라우저 세션에서 로그아웃될 수 있습니다. 로그아웃하지 않은 경우 브라우저를 새로 고쳐 새 인증서를 적용합니다. 업데이트를 확인하려면 브라우저의 주소 표시줄에서 URL 옆에 있는 잠금 또는 경고 아이콘을 클릭합니다. 새로 고치면 다시 로그인하지 않고 Settings(설정) > Certificates(인증서) 페이지로 이동합니다.

장치 콘솔 사용자 인터페이스(UI)에서는 CN(Common Name)이 전환으로 설정된 자체 서명 인증서를 사용합니다. 이 인증서는 FI(Fabric Interconnect)의 전원을 처음 켜고 구성할 때 생성됩니다. 자체 서명 인증서는 365일 동안 유효하며, 이는 1년 이상 실행 중인 모든 FI에 만료된 인증서가 있음을 의미합니다.

일부 고객은 자동화된 모니터링 툴을 사용하여 HTTPS를 통해 디바이스의 IP 또는 호스트 이름을 폐기하고 인증서의 만료 날짜를 확인합니다. 인증서가 만료되면 이러한 툴은 경보를 트리거하여 관찰력 및 보안 팀이 잠재적 문제로 플래그 지정할 수 있습니다.

또한 인증서가 자체 서명되어 있기 때문에 웹 브라우저에서는 Not Secure 경고가 표시되지 않습니다. 이 경고는 인증서가 만료되어 추가 보안 문제가 발생할 수 있는 경우에도 나타납니다.

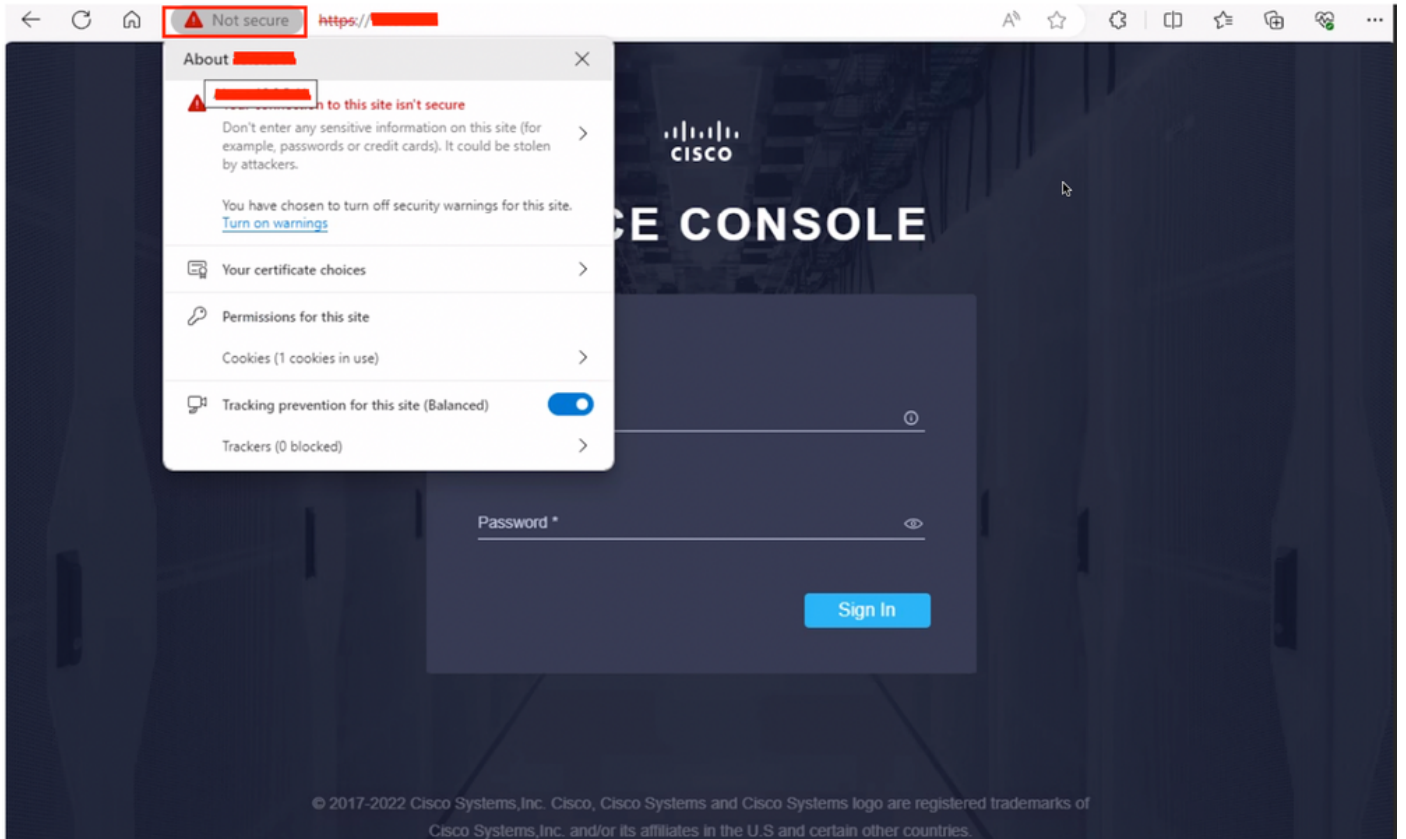
이러한 문제를 방지하려면 인증서를 사전에 갱신하거나 교체하는 것이 좋습니다.

문제/증상

디바이스 콘솔에 액세스할 때 사이트가 안전하지 않음을 알 수 있습니다.



참고: 디바이스 콘솔 액세스의 경우 Fabric Interconnect의 IP 주소가 필요합니다.



인증서 오류

인증서 정보를 클릭하면 인증서 만료 날짜가 표시됩니다.

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...

인증서 만료 날짜

인증서 다시 생성

Intersight에서 기본 인증서를 갱신하려면 디바이스 콘솔을 다시 시작하거나 Fabric Interconnect를 재부팅해야 합니다(권장하지 않음).

Intersight에서 기본 인증서를 수동으로 재생성하려면 다음 단계를 수행합니다.

1. 하나의 패브릭 인터커넥트의 IP 주소를 사용하여 SSH 세션을 엽니다.
2. 다음 명령을 실행합니다.

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

인증서가 성공적으로 생성되면 다음을 볼 수 있습니다.

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

실제 인증서를 확인하고 변경되었는지 확인하려면 다음 명령을 사용합니다.

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

출력 예:

```
-----BEGIN CERTIFICATE-----
MIIC+DCCAeCgAwIBAgICBnowDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAxMXSU1N
LVNBQVMtTVhTVkxkYzBQI02NDU0LUeWHhcNMjUwMzEyMjI1MTM4WhcNMjUwMzEyMjI1
MTM4WjAiMSAwHgYDVoQDExdJTU0tU0FBuY1NWFWTEFCLTY0NTQ0TCCASiWdQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAK+Q9oAU2rHxtV5stg9vfCeKQ+9+n5Ke
oz6IKOeEDufeRcBYepaJlEhffvdLp/u0h/NnyphT4mVLiJxh6dTTIhW58G8LaGNV
hIRtNAX984eLCs1nSG3o3tzJ3+e5t04G6klAcj43HiKY+oRCes+oiUsQlYpBjHoy
FGxMT8wpmNMIg59mKVtuUeC4r6ACnyy1CRNp8qD8Rf4lIBU/jTI/jPdzE2//9rAo
G85qhZ46vI0dLu1jv/ySszQkATFA15KHFETnyTkptd1JH8mc033edJ1Xq9p1ebMp
dtn18zj+2qxQq8ErZ6doFdk0uyyq3N6Q0dbfdefKKuiFvkCGv4GwRG8CAwEAAAM4
MDYwDgYDVROPAQH/BAQDAgKkMBMGA1UdJQQMAoGCCsGAQUFBwMBMA8GA1UdEQQI
MAaHBH8AAAAEwDQYJKoZIhvcNAQELBQADggEBAFn+v4ehwLFi/mcHWA41d03JBkvI
RI1bFPHj0ykmAN8E1XoJlLciCxA3gHuZPP61T+2VpeAXAoWzIlgU1m2GwPzZbCQ
nz2v7NpGHchaXAEi756IMmCm2IJ2jOuS9p9v3AAX3gLUp43SeCQN+C2nN0cZgmZr
/K1CoNkIUXdVI8nxEDCMFPeZL1SXdNa2c4AB699teo1CNc65tnnNDjsxkLkL7bTx
P5euETVi5CizQQpjczZxEMHv3XdvXtkzyAATjRmvUS8lxyXxiisMjM17f8zXkLnG
n7ZKR746BXgXufmS0zITtbpvgI9+6PnauoW0h3EH7rGmJyZnn5L62/oaoy4=
-----END CERTIFICATE-----
```



참고: 갱신 전에 인증서를 확인하는 경우 갱신 프로세스 후에 변경되는지 확인합니다.

마지막으로, 인증서는 다음과 같이 표시되어야 합니다.

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

인증서 검증

관련 정보

[Intersight Virtual Appliance의 인증서](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.