

Intersight マネージドモードでのデフォルト証明書の再生成

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[自己署名証明書の生成](#)

[問題/症状](#)

[証明書の再生成](#)

[関連情報](#)

はじめに

このドキュメントでは、Intersight環境（SAASまたはアプライアンス）でファブリックインターコネクト(FI)自己署名証明書を更新するプロセスについて説明します。

前提条件

要件

Intersight マネージドモードのUCSドメイン。

The screenshot displays the Cisco Intersight web interface for a Fabric Interconnect (FI-A). The interface is organized into three main columns: Details, Properties, and Events.

- Details:** Shows the UCS Domain Profile as 'IMM-6454-SAAS' and the Mode as 'Intersight' (highlighted with a red box). Other details include Peer Switch, User Label, and UCS Domain Profile Status.
- Properties:** Displays the Cisco UCS-FI-6454 model and various configuration options. The Mode is set to 'end-host'. The Access section shows IP Address, Subnet Mask, Default Gateway, MAC, and FC Zone Count.
- Events:** Lists alarms and events, including 'EtherTransceiverNotPresent' and 'EquipmentSwitchPsuPoweredOff'.

使用するコンポーネント

- ファブリックインターコネクト6454
- バージョン：4.2(3m)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

自己署名証明書の生成

現在のブラウザでは自己署名証明書が使用されている場合にアクセスが制限されるため、アプライアンスへのアクセスにはCA署名証明書を使用することをお勧めします。Intersight仮想アプライアンスを使用すると、自己署名証明書を生成して、シスコが提供する証明書の有効期限が切れた場合に有効な証明書を延長できます。

新しい自己署名証明書を生成すると、既存のSSL証明書が置き換えられ、現在のブラウザセッションからログアウトされる可能性があります。ログアウトしていない場合は、ブラウザを更新して、新しい証明書を適用します。更新を確認するには、ブラウザのアドレスバーのURLの横にあるロックまたは警告アイコンをクリックします。更新すると、再度ログインしなくても、Settings > Certificatesの順にページが表示されます。

デバイスコンソールユーザインターフェイス(UI)は、共通名(CN)がswitchに設定された自己署名証明書を使用します。この証明書は、ファブリックインターコネクト(FI)の電源を初めてオンにして設定したときに生成されます。自己署名証明書は365日間有効です。これは、1年以上にわたって実行されているFIの証明書が期限切れであることを意味します。

一部のお客様は、自動化された監視ツールを使用して、HTTPS経由でデバイスのIPまたはホスト名を取得し、証明書の有効期限を検証します。証明書の有効期限が切れると、これらのツールによってアラームがトリガーされ、可観測性チームとセキュリティチームによって潜在的な問題としてフラグが付けられます。

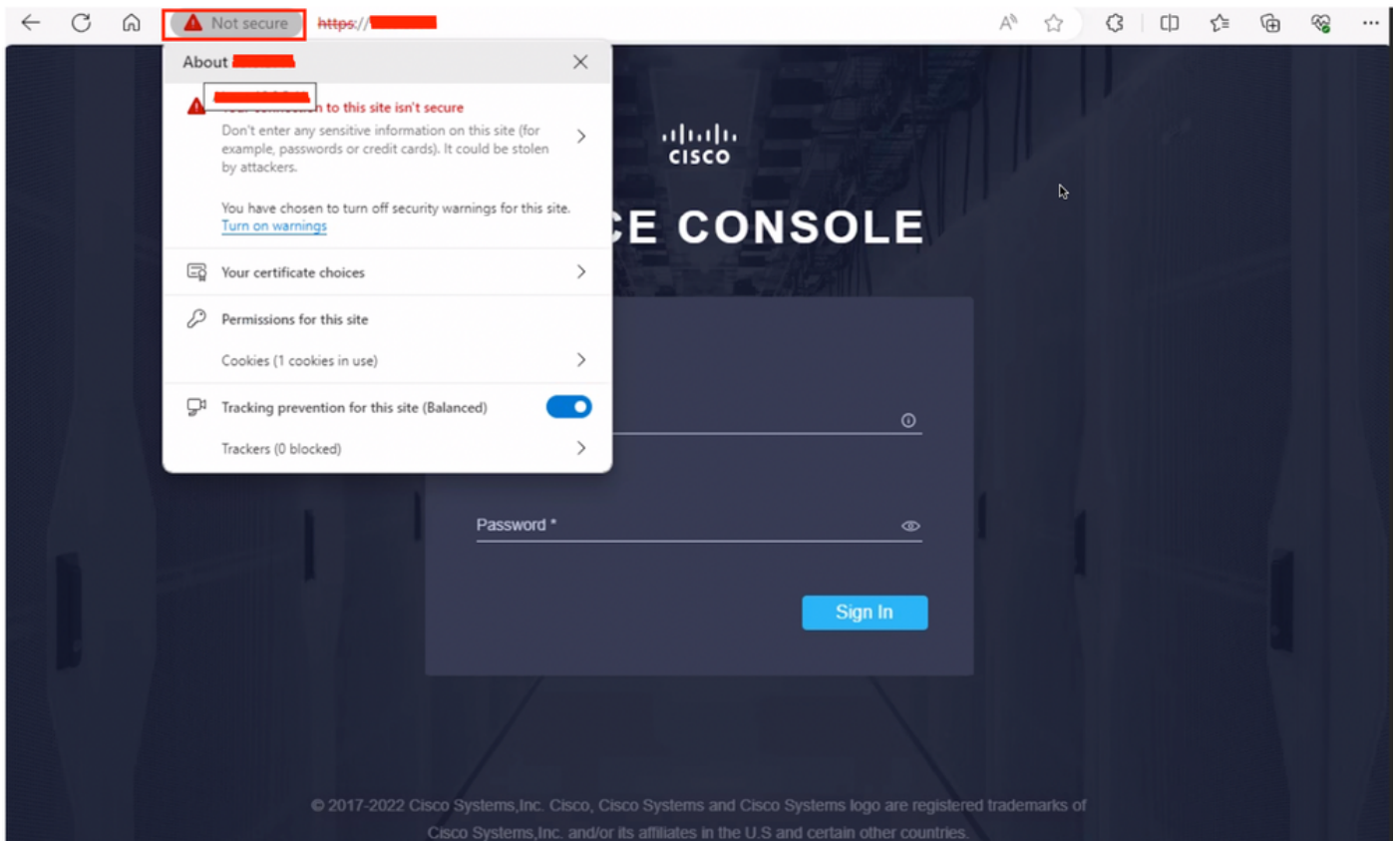
また、証明書は自己署名されているため、WebブラウザにはNot Secure警告が表示されます。この警告は、証明書の有効期限が切れている場合にも表示され、セキュリティ上の問題がさらに発生する可能性があります。

これらの問題を防ぐために、証明書を予防的に更新または置き換えることをお勧めします。

問題/症状

デバイスコンソールにアクセスすると、このサイトは安全ではないことがわかります。

 注：デバイスコンソールにアクセスするには、Fabric InterconnectのIPアドレスが必要です



証明書エラー

証明書情報をクリックすると、証明書の有効期限が表示されます。

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...

証明書の有効期限

証明書の再生成

Intersightでデフォルトの証明書を更新するには、デバイスコンソールを再起動するか、ファブリックインターコネクト（推奨されません）を再起動する必要があります。

Intersightでデフォルトの証明書を手動で再生成するには、次の手順を実行します。

1. 1つのFabric InterconnectのIPアドレスを使用してSSHセッションを開きます。
2. 次のコマンドを実行します：

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

証明書が正常に生成されると、次のように表示されます。

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

実際の証明書を確認し、変更されたことを確認するには、次のコマンドを使用します。

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

出力例：

```
-----BEGIN CERTIFICATE-----
MIIC+DCCAeCgAwIBAgICBnowDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAxMXSU1N
LVNBQVMTTVhTVkxwBQI02NDU0LUeWHhcNMjUwMzEyMjI1MTM4WhcNMjYwMzEyMjI1
MTM4WjAiMSAwHgYDVQQDExdJTU0tU0FBUEy1NWFWTEFCLTY0NTQtQTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBBAK+Q9oAU2rHxtV5stg9vfCeKQ+9+n5Ke
oz6IKOeEDufeRcBYepaJlEhffvdLp/u0h/NnyphT4mVLiJxh6dTTIhW58G8LaGNV
hIRtNAX984eLCs1nSG3o3tzJ3+e5t04G6klAcj43HiKY+oRCEs+oiUsQlYpBjHoy
FGxMT8wpmNMIg59mKVtuUeC4r6ACnyy1CRNp8qD8Rf4lIBU/jTI/jPdzE2//9rAo
G85qhZ46vI0dLu1jv/ySszQkATFA15KHFETnyTkptd1JH8mc033edJ1Xq9p1ebMp
dtn18zj+2qxQq8ErZ6doFdkOuyuq3N6Q0dbfdefKKuiFvkCGv4GwRG8CAwEAAAM4
MDYwDgYDVROPAQH/BAQDAgKkMBMGA1UdJQQMAoGCCsGAQUFBwMBMA8GA1UdEQQI
MAAHBH8AAAAEwDQYJKoZIhvcNAQELBQADggEBAFn+v4ehwLFi/mcHWA4ld03JBkvI
RI1bFPHj0ykmAN8E1XoJlLciCxA3gHUzPP6lT+2VpeAXAoWzIlgUlm2GwPzZbCQ
nz2v7NpGHchaXAEi756IMmCm2IJ2jOuS9p9v3AAX3gLUp43SeCQN+C2nN0cZgmZr
/K1CoNkIUXdVI8nxEDCMFPezL1SXdNa2c4AB699teo1CNc65tnnNDjsxkLkL7bTx
P5euETVi5CizQQpjczZxEMHv3XdvXtkzyAATjRmvUS8lxyXxiisMjM17f8zXkLnG
n7ZKR746BXgXufmS0zITtbpvgI9+6PnauoW0h3EH7rGmJyZnn5L62/oaoy4=
-----END CERTIFICATE-----
```

 注：更新前に証明書を確認する場合は、更新プロセス後に証明書が変更されていることを確認してください。

最後に、証明書は次のようになります。

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	2c87212cb0fec3475961c0fb456a510ba7f1aba6198584487e7365459069e58
Public Key	dfe3b379568f417cbb0ac01b4aad99feab3b331002626fa8203fab454e1e72e

証明書の検証

関連情報

[Intersight仮想アプライアンスの証明書](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。