

Aci APIC GUI HTTPS証明書の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[コンフィギュレーション](#)

[ステップ1:CA認証局ルート証明書または中間証明書のインポート](#)

[ステップ2: キーリングの作成](#)

[ステップ3: 秘密キーとCSRの生成](#)

[ステップ4: CSRを取得してCA組織に送信する](#)

[手順5:Web上の署名証明書の更新](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、カスタムSSLおよび自己署名SSL証明書の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- デジタル署名とデジタル証明書
- 認証局(CA)組織による証明書の発行プロセス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Application Policy Infrastructure Controller (APIC)
- ブラウザ
- 5.2(8e)を実行するACI

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。

設定

デバイスが初期化されると、自己署名証明書がHTTPSのSSL証明書として使用されます。自己署名証明書は、1000日間有効です。

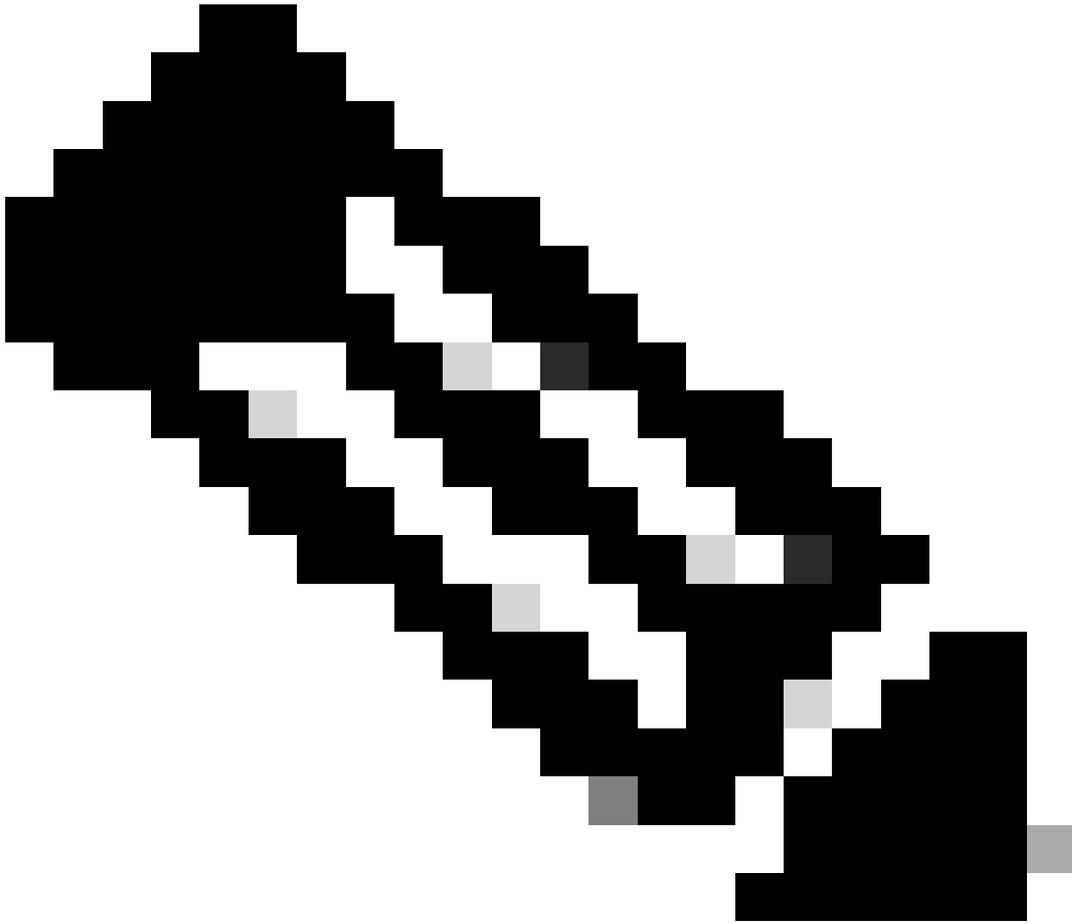
デフォルトでは、自己署名証明書の有効期限の1カ月前にデバイスが自動的に更新され、新しい自己署名証明書が生成されます。

コンフィギュレーション

デバイスが自己署名証明書を使用している。APIC GUIにアクセスすると、ブラウザは証明書が信頼できないことを示すプロンプトを表示します。この問題を解決するために、このドキュメントでは、信頼できるCA認証局を使用して証明書に署名します。



ステップ 1： CA認証局ルート証明書または中間証明書のインポート



注:CAルート証明書を使用して直接署名する場合は、CAルート証明書をインポートするだけです。ただし、署名に中間証明書を使用している場合は、完全な証明書チェーン（ルート証明書と信頼されていない中間証明書）をインポートする必要があります。

メニューバーで、Admin > AAA > Security > Public Key Management > Certificate Authoritiesに移動します。

System Tenants Fabric Virtual Networking **Admin** Operations Apps Integrations

AAA Schedulers | Firmware | External Data Collectors | Config Rollbacks | Import/Export

AAA

- Quick Start
- Authentication
- Security**
- Users

User Management - Security

Management Settings Security Domains Roles RBAC Rules **Public Key Management**

Key Rings **Certificate Authorities** JWT Keys

Name	Description	FP	N	
ACI_Root		[Cert 0] d7:29:6e:1c:60:26:4...	1	Delete
Cisco_AD_CA		[Cert 0] 57:1a:80:28:12:9a:5f...	1	

Create Certificate Authority

User Management - Security

Create Certificate Authority

Name: ⓘ

Description: optional

Certificate Chain:

Cancel Submit

名前：必須。

命名規則に従って内容を作成します。_を含めることはできますが、次のような特殊文字を英語に含めることはできません。

.,:;'":|+*/= `~!@#% ^&() およびスペース文字。

説明：オプション。

認定チェーン：必須。

信頼できるCAルート証明書とCA中間証明書を入力します。



注：各証明書は、固定フォーマットに準拠している必要があります。

```
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN  
CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE---  
-- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----
```

Submitボタンをクリックします。

ステップ 2：キーリングの作成

メニューバーで、Admin > AAA > Security > Public Key Management > Key Ringsに移動します。

The screenshot shows the Cisco APIC Admin console. The top navigation bar includes 'System', 'Tenants', 'Fabric', 'Virtual Networking', 'Admin', 'Operations', 'Apps', and 'Integrations'. The 'Admin' tab is active. On the left, the 'AAA' menu is expanded to 'Security'. The main content area is titled 'User Management - Security' and has several tabs: 'Management Settings', 'Security Domains', 'Roles', 'RBAC Rules', 'Public Key Management', 'Key Rings', 'Certificate Authorities', and 'JWT Keys'. The 'Public Key Management' tab is selected, and the 'Key Rings' sub-tab is also selected. Below the tabs is a table of key rings. The table has columns for 'Name', 'Description', 'Admin State', 'Trust Point', and 'Modulus'. There are two rows: 'ACL_Wildcard' and 'default'. A 'Create Key Ring' button is highlighted in red in the top right corner of the table area.

Name	Description	Admin State	Trust Point	Modulus
ACL_Wildcard		Completed	ACL_Root	MOD 2048
default	Default self-signed S...	Completed		MOD 2048

The 'Create Key Ring' dialog box is shown. It has a close button in the top right corner. The 'Name' field is required (indicated by a red exclamation mark) and is empty. The 'Description' field is optional and contains the text 'optional'. The 'Certificate' field is a large text area and is empty. The 'Modulus' field has four radio buttons: 'MOD 512', 'MOD 1024', 'MOD 1536', and 'MOD 2048'. The 'MOD 2048' button is selected. The 'Certificate Authority' field is a dropdown menu with 'select an option' selected. The 'Private Key' field is a large text area and is empty. Below the 'Private Key' field, there is a note: 'If you want to use an externally generated private key, please provide it here'. At the bottom right, there are 'Cancel' and 'Submit' buttons. The 'Submit' button is disabled.

名前：必須（名前を入力してください）。

証明書：キーリングを介してCisco APICを使用して証明書署名要求(CSR)を生成する場合は、コンテンツを追加しないでください。または、Cisco APICの外部で秘密キーとCSRを生成することで、前の手順でCAによって署名された証明書がすでに存在する場合は、署名付き証明書のコンテンツを追加します。

モジュラス：必須（キーの強度を確認するにはオプションボタンをクリックします）。

認証局：必須。ドロップダウンリストから、以前に作成した認証局を選択します。

秘密キー：キーリングをCisco APICを使用してCSRを生成する場合は、コンテンツを追加しないでください。または、入力した署名付き証明書のCSRの生成に使用する秘密キーを追加します。



注：システム生成の秘密キーとCSRを使用せず、カスタムの秘密キーと証明書を使用する場合は、名前、証明書、認証局、秘密キーの4つの項目を入力するだけです。送信後に実行する必要があるのは、最後のステップであるステップ5だけです。

Submitボタンをクリックします。

ステップ 3：秘密キーとCSRの生成

メニューバーで、Admin > AAA > Security > Public Key Management > Key Ringsに移動します。

System Tenants Fabric Virtual Networking **Admin** Operations Apps Integrations

AAA Schedulers Firmware External Data Collectors Config Rollbacks Import/Export

AAA

- Quick Start
- Authentication
- Security**
- Users

User Management - Security

Management Settings Security Domains Roles RBAC Rules **Public Key Management**

Key Rings Certificate Authorities JWT Keys

Name	Description	Admin State	Trust Point	Modulus
default	Default self-signed SSL Certi...	Completed		MOD 2048
Cisco_test		Started	Cisco	MOD 2048
Cisco_SSL		Completed	Cisco	MOD 2048
ACI_Wildcard_C		Started	ACI_Root_Copy	MOD 2048
ACI_Wildcard		Completed	ACI_Root	MOD 2048

Context menu for Cisco_test:

- Delete
- Create Certificate Request**
- Save as ...
- Post ...
- Share
- Open In Object Store Browser

Create Certificate Request

Subject:

Alternate Subject Name:
Eg:- DNS:server1.example.com,DNS:server2.example.com

Locality:

State:

Country:

Organization Name:

Organization Unit Name:

Email:

Password:

Confirm Password:

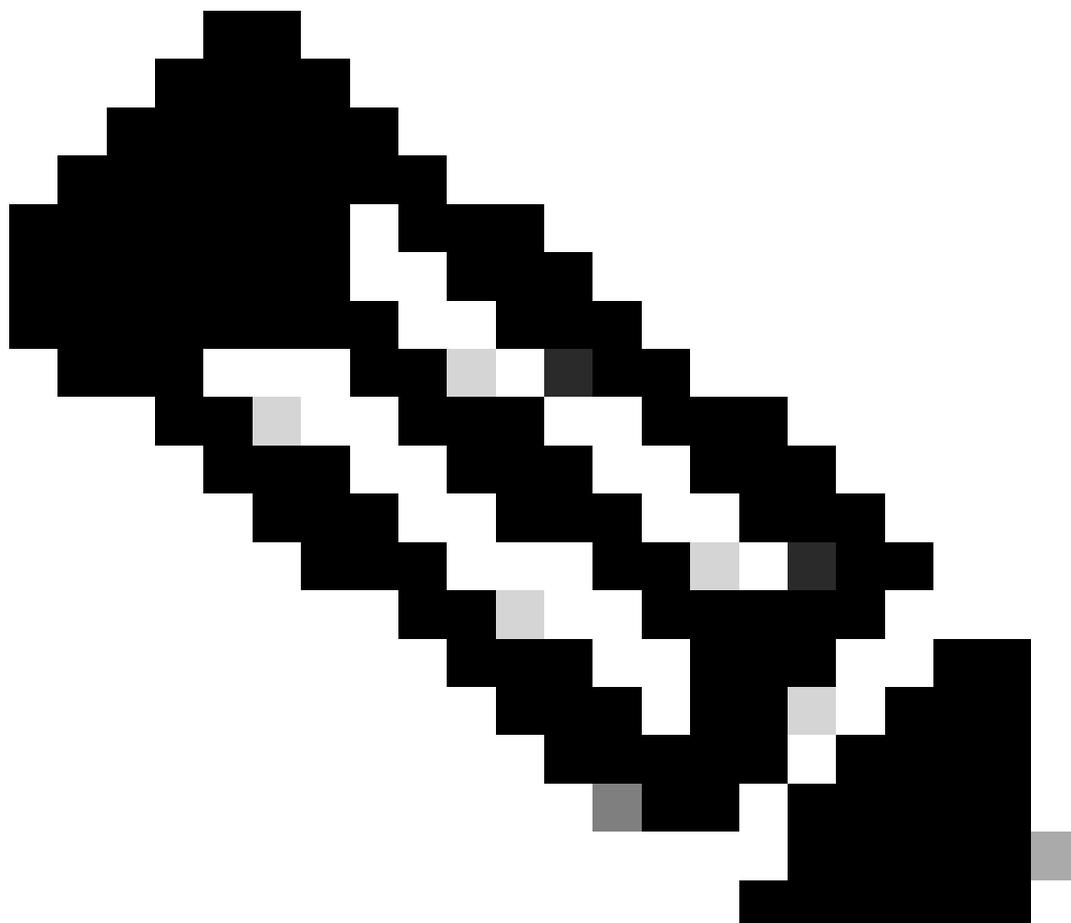
Cancel Submit

Subject:必須。CSRの共通名(CN)を入力します。

ワイルドカードを使用してCisco APICの完全修飾ドメイン名(FQDN)を入力できますが、最新の証明書ではFQDNがSANフィールドに必要であるため、一般的に、証明書の識別可能な名前を入力し、すべてのCisco APICのFQDNを代替サブジェクト名(SAN - Subject Alternative Name)フィールドに入力することをお勧めします。

代替サブジェクト名：必須です。すべてのCisco APICのFQDNを入力します
(DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.comやDNS:*example.comなど)。

SANでIPアドレスを一致させる場合は、Cisco APICのIPアドレスをIP:192.168.1.1の形式で入力します
。



注：このフィールドでは、ドメインネームサーバ(DNS)名、IPv4アドレス、またはその両方を組み合わせて使用できます。IPv6アドレスはサポートされていません。

証明書を発行するために適用するCA組織の要件に従って、残りのフィールドに入力します。

Submitボタンをクリックします。

ステップ 4：CSRを取得してCA組織に送信する

メニューバーで、Admin > AAA > Security > Public Key Management > Key Ringsに移動します。

作成したキーリングの名前をダブルクリックして、Requestオプションを探します。リクエスト

の内容はCSRです。

Key Ring - Cisco_test

Policy | Faults | History

Alternate Subject Names separated by commas

Locality:

State:

Country:

Organization Name:

Organization Unit Name:

Email:

Password:

Confirm Password:

Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICVDCCATwCAQAwDzENMAsGA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcXg/fHdKpbKBQAqKfCkRI
XJ44LGLfc076G00xcTsMwDDM8NZrdNT0Ky1Ewaz+8VoI3zbc55VmuV/0uXvJ1RP
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQqc+tjAeZH
1Bj0LxTa2Y22MaJ4G+GXoI6vP/WB3lKh4fnfgioKReqQRi2kQmZRITVJ/bVMljw
q80mvcSudBuzjK0ndm8EwW6yd8Uz43ZU0gj5mDahWk8oBJPxxA0IRBsoXyWwTGRY
AmValt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGCEAwEAAMA0GCSqG5Ib3DQEB
```

Show Usage | Close | Submit

要求のすべての内容をコピーして、CAに送信します。

CAは秘密キーを使用して、CSRの署名検証を実行します。

CAから署名付き証明書を取得すると、証明書が証明書にコピーされます。

Key Ring - Cisco_Test

Policy | Faults | History

Name: Cisco_Test

Admin State: Started

Description: optional

Certificate:

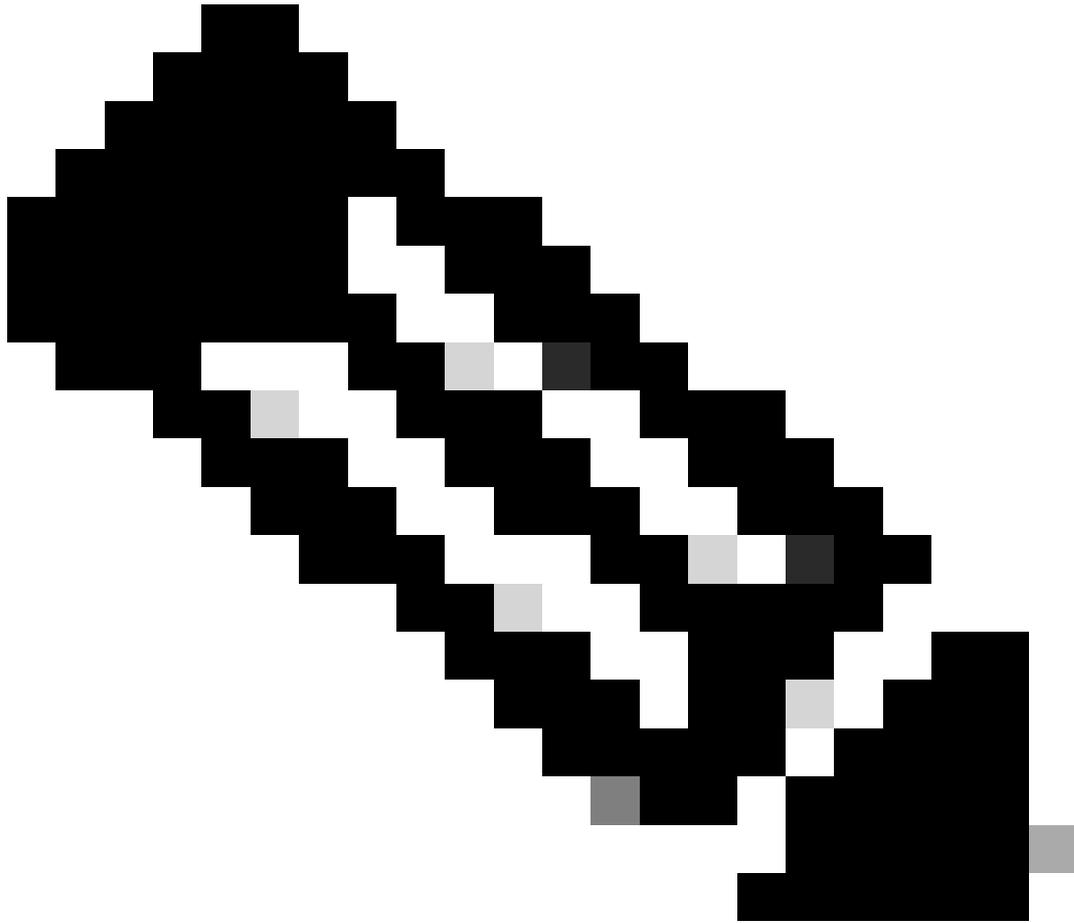
```
-----BEGIN CERTIFICATE-----
MIIDSzCCApuGAWIBAgIBAjANBgkqhkiG9w0BAQsFADBMYQswCQYDVQQGEwJVUzEL
MAKGA1UECAwCQ0EEXFTATBgNVBACMDERlZmF1bH0gQ2l0eTEwMDUyMDE5MDE5
Y28gQUNJIFRlYW0xMDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5
MjgwNDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5
Q2l0eTEwMDUyMDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5MDE5
LWFwaWwMxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALJA5N1wzE7WmBLK35pTd06FwH3M2ZmIeCDw6SktDTqaMHHqDkYek0UgG0dyRrDP
```

Modulus: MOD 512 | MOD 1024 | MOD 1536 | MOD 2048

Certificate Authority: Cisco_ACI_Team

Private Key:

Show Usage | Close | Submit



注：各証明書は、固定フォーマットに準拠している必要があります。

-----BEGIN CERTIFICATE----- CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

Submitボタンをクリックします。

ステップ 5： Web上の署名証明書の更新

メニューバーで、Fabric > Fabric Policies > Policies > Pod > Management Access > Defaultに移動します。

The screenshot shows the APIC GUI configuration for 'Management Access - default'. The 'Admin KeyRing' dropdown menu is highlighted with a red box, showing 'Cisco_Test' selected. The 'Submit' button is visible at the bottom right.

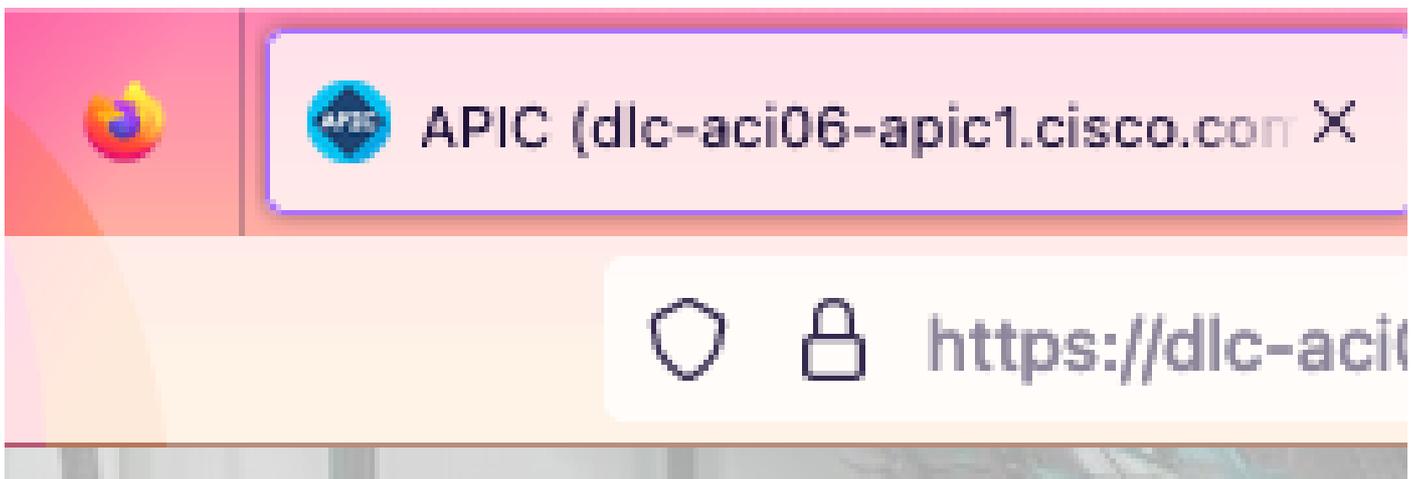
Admin KeyRing ドロップダウンリストで、目的のKeyRingを選択します。

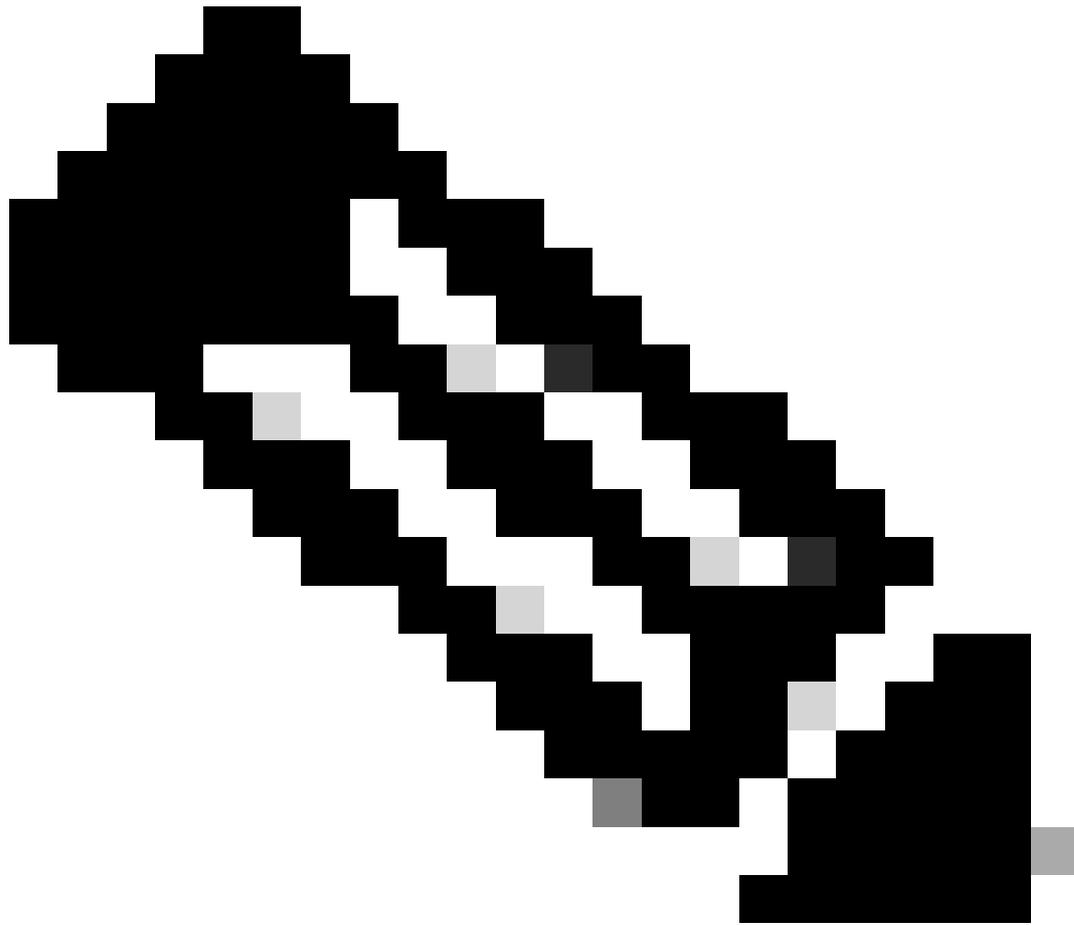
Submit ボタンをクリックします。

「submit」をクリックした後、証明書の理由によりエラーが発生します。新しい証明書で更新します。

確認

APIC GUI にアクセスした後、APIC は CA 署名付き証明書を使用して通信します。ブラウザで証明書情報を表示して確認します。

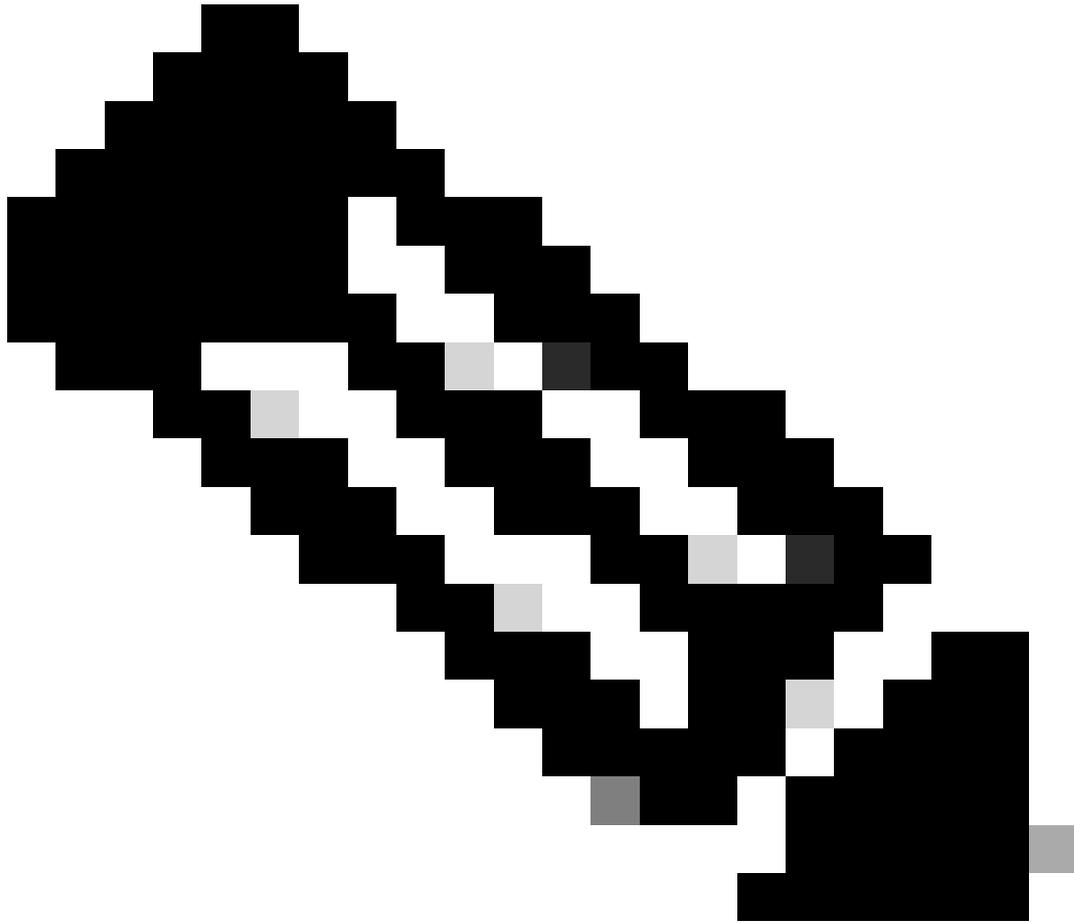




注：異なるブラウザでHTTPS証明書を表示する方法は、完全に同じではありません。特定の методについては、ブラウザのユーザガイドを参照してください。

トラブルシューティング

APIC GUIがuntrustedであることを示すプロンプトがブラウザに引き続き表示される場合は、GUIの証明書がキーリングで送信されたものと一致するかどうかをブラウザで確認します。コンピュータまたはブラウザで証明書を発行したCAルート証明書を信頼する必要があります。



注：この証明書を信頼するには、Google Chromeブラウザで証明書のSANを確認する必要があります。

自己署名証明書を使用するAPICでは、まれに証明書の有効期限に関する警告が表示されることがあります。

キーリングで証明書を見つけ、証明書解析ツールを使用して証明書を解析し、ブラウザで使用されている証明書と比較します。

キーリング内の証明書が更新された場合は、新しい管理アクセスポリシーを作成して適用します。

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory | **Fabric Policies** | Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies**
 - Pod
 - Date and Time
 - SNMP
 - Management Access
 - Create Management Access Policy**
 - Switch

Pod - Management Access

Name	HTTP			HTTPS		SSH State	SSH State
	HTTP State	HTTP Port	HTTP Redirect	HTTPS State	HTTPS Port		
default	enabled	80	disabled	enabled	443	enabled	

System Tenants **Fabric** Virtual Networking Admin Operations Apps Integrations

Inventory | **Fabric Policies** | Access Policies

Policies

- Quick Start
- Pods**
 - Policy Groups**
 - default**
 - Profiles
 - Switches
 - Modules
 - Interfaces
 - Policies
 - Pod
 - Date and Time
 - SNMP
 - Management Access
 - New
 - default
 - Switch
 - Interface
 - Global
 - Monitoring
 - Troubleshooting

Pod Policy Group - default

Policy Faults History

Properties

Date Time Policy: default

Resolved Date Time Policy: default

ISIS Policy: select a value

Resolved ISIS Policy: default

COOP Group Policy: select a value

Resolved COOP Group Policy: default

BGP Route Reflector Policy: select a value

Resolved BGP Route Reflector Policy: default

Management Access Policy: select a value

Resolved Management Access Policy: New

SNMP Policy: fabric

Resolved SNMP Policy: default

MACsec Policy: fabric

Resolved MACsec Policy: fabric

Create Management Access Policy

Show Usage Reset Submit

キーリングの証明書が自動的に更新されない場合は、Cisco TACに連絡してサポートを依頼してください。

関連情報

- [Cisco APICセキュリティ設定ガイド、リリース5.2\(x\)](#)
- [シスコのテクニカルサポートとダウンロード](#)

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。