# ACI APIC GUI HTTPS証明書の設定

## 内容



## 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

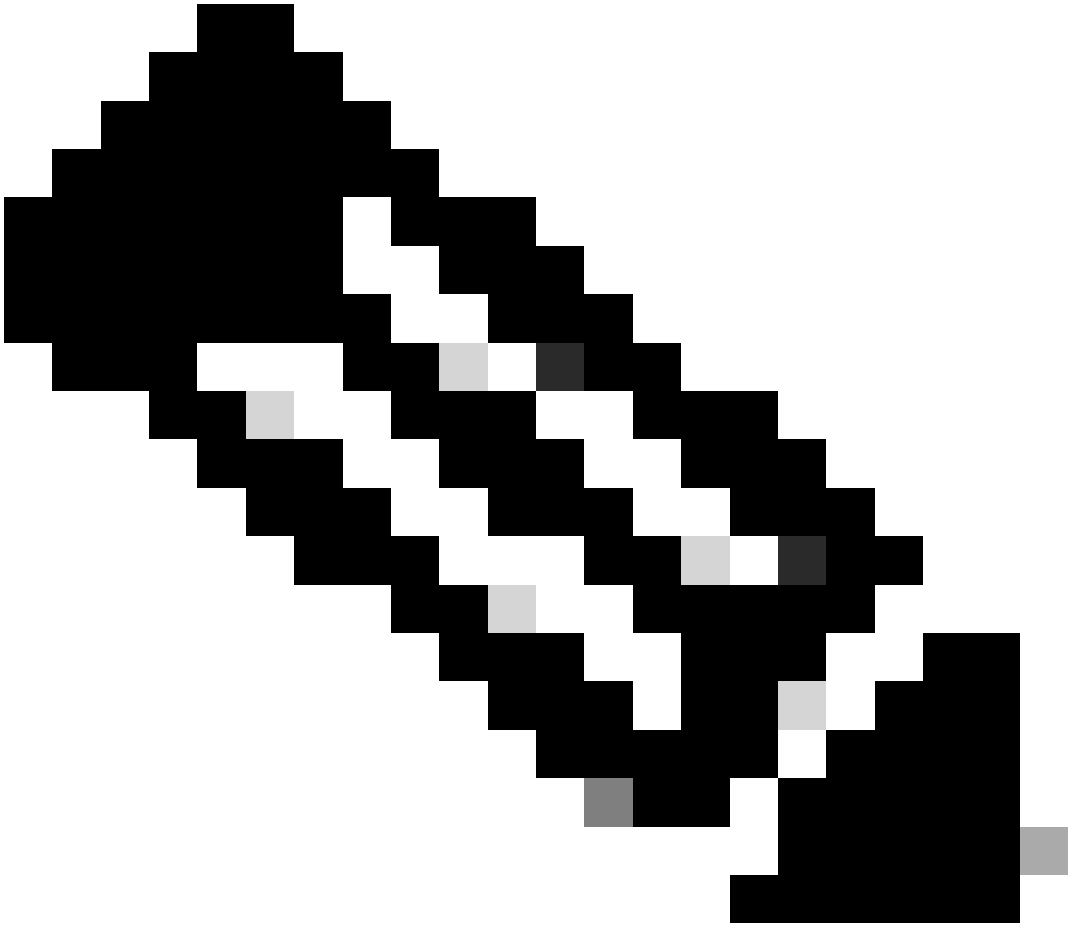
デバイスが初期化されると、自己署名証明書がHTTPSのSSL証明書として使用されます。自己署名証明書は、1000日間有効です。

デフォルトでは、自己署名証明書の有効期限の1ヵ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

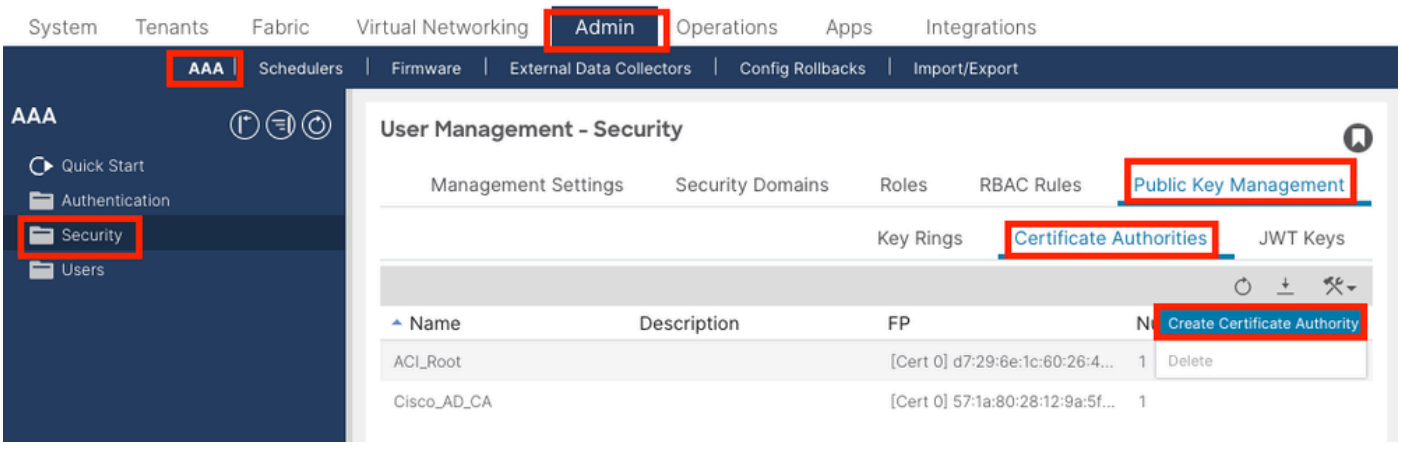
デバイスが自己署名証明書を使用している。APIC GUIにアクセスすると、ブラウザは証明書が信頼できないことを示すプロンプトを表示します。この問題を解決するために、このドキュメントでは、信頼できるCA認証局を使用して証明書に署名します。

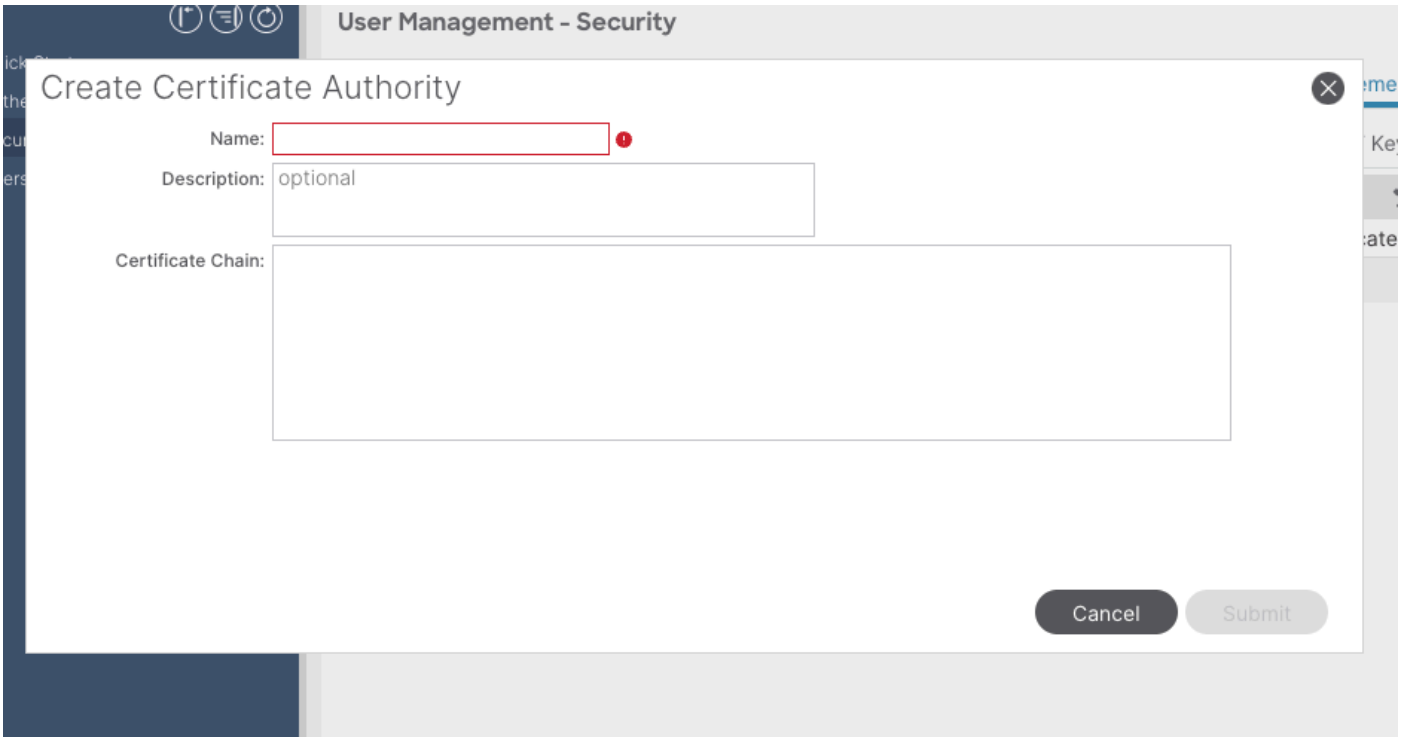

ステップ 1： CA認証局ルート証明書または中間証明書のインポート



注：直接署名にCAルート証明書を使用している場合は、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。





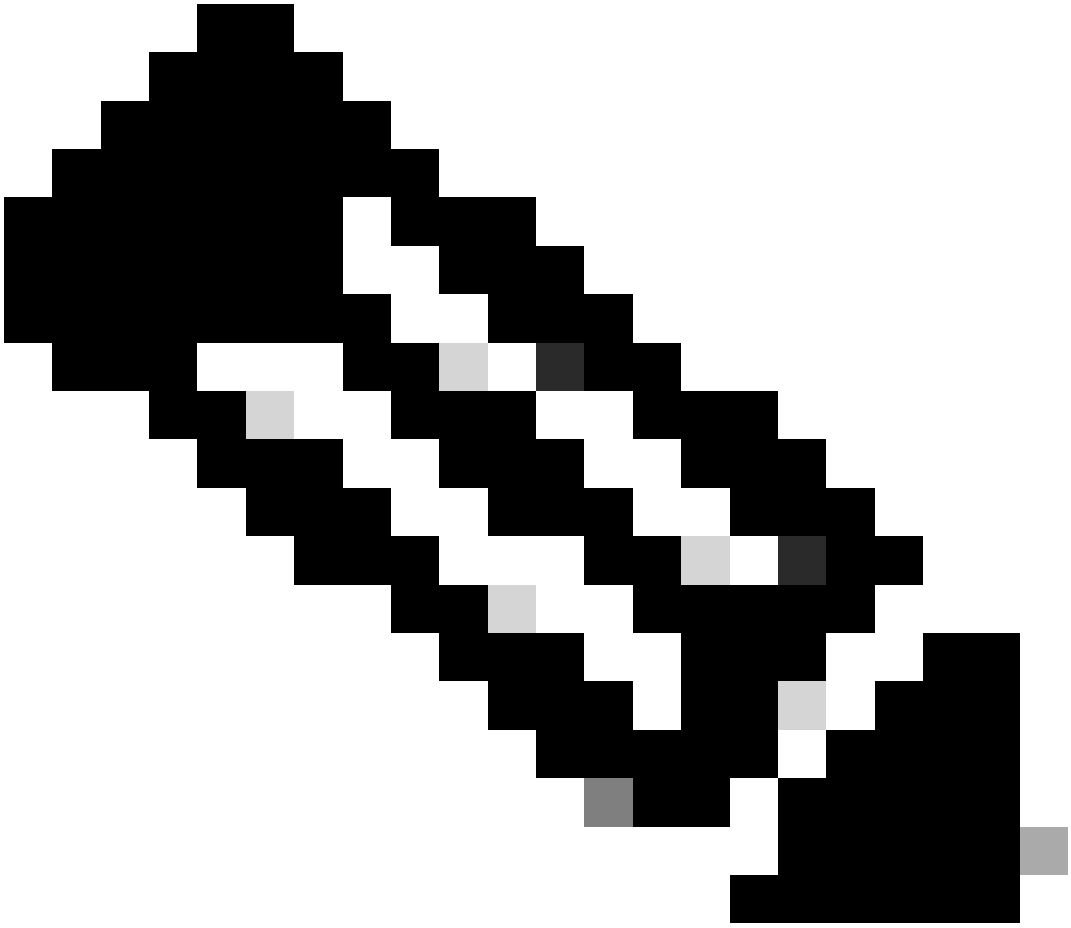

名前：**必須。**

命名規則に従って内容を作成します。_を使用できますが、次のような特殊文字は使用できません。
, . ; ' " : | + * / = ` ~ ! @ # $ % ^ & ( ) およびスペース文字を含む必要があります。

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。



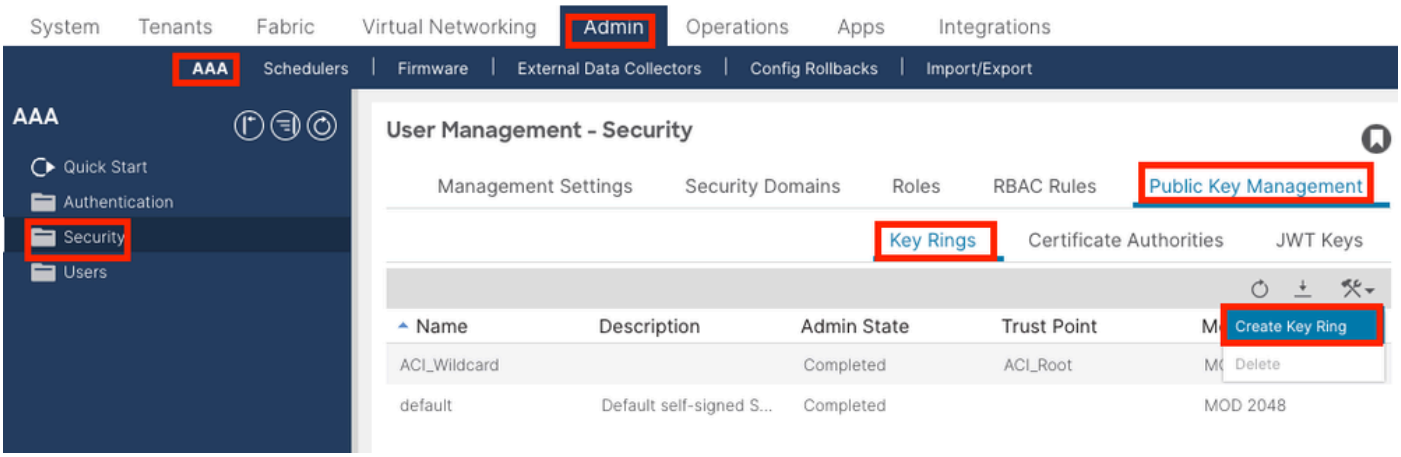
**注**：各証明書は、固定フォーマットに準拠している必要があります。

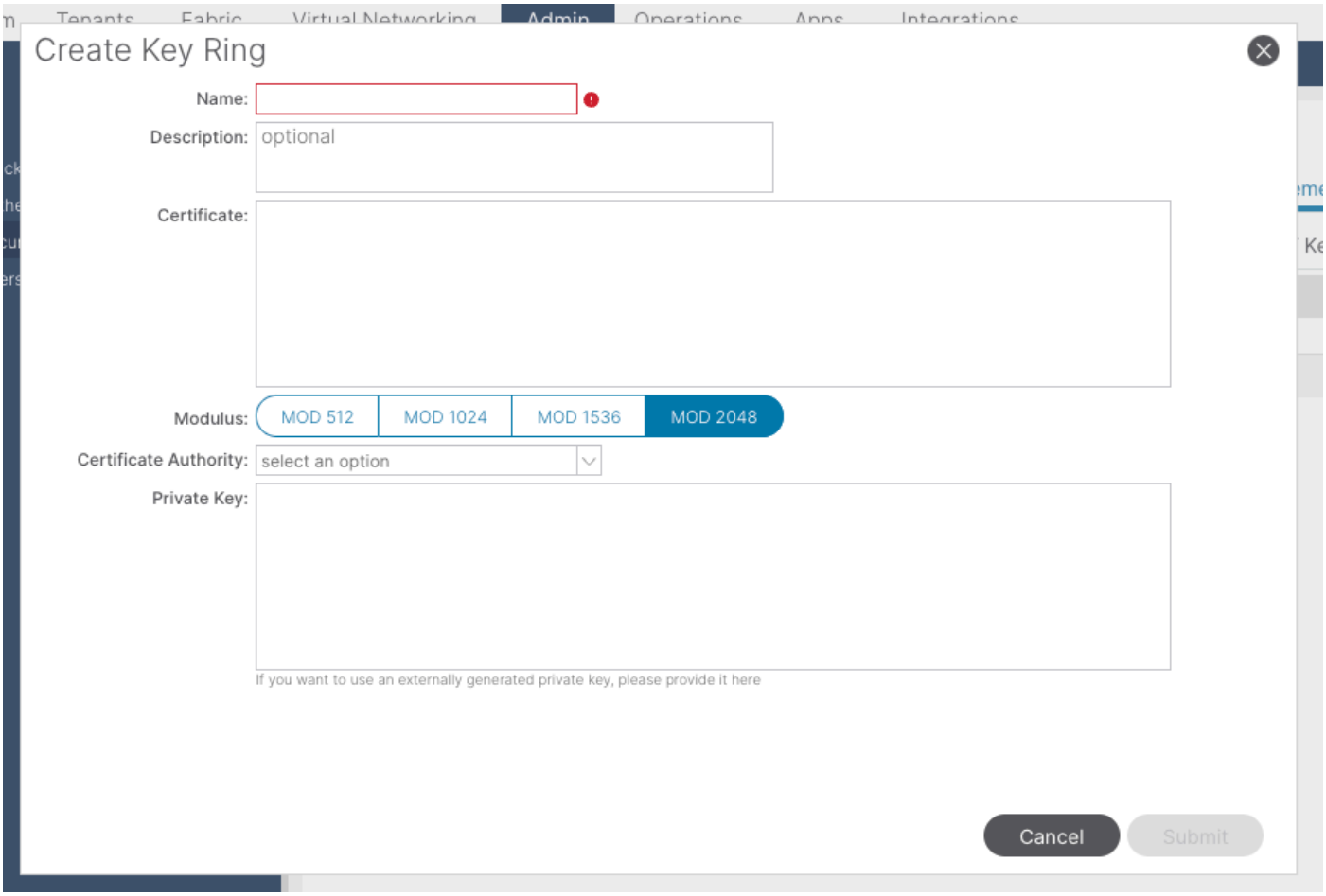
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

**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。




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、秘密キーとCSRをCisco APICの外部で生成することで、前の手順でCAによって署名された証明書をすでに持っている場合は、署名付き証明書の内容を追加します。

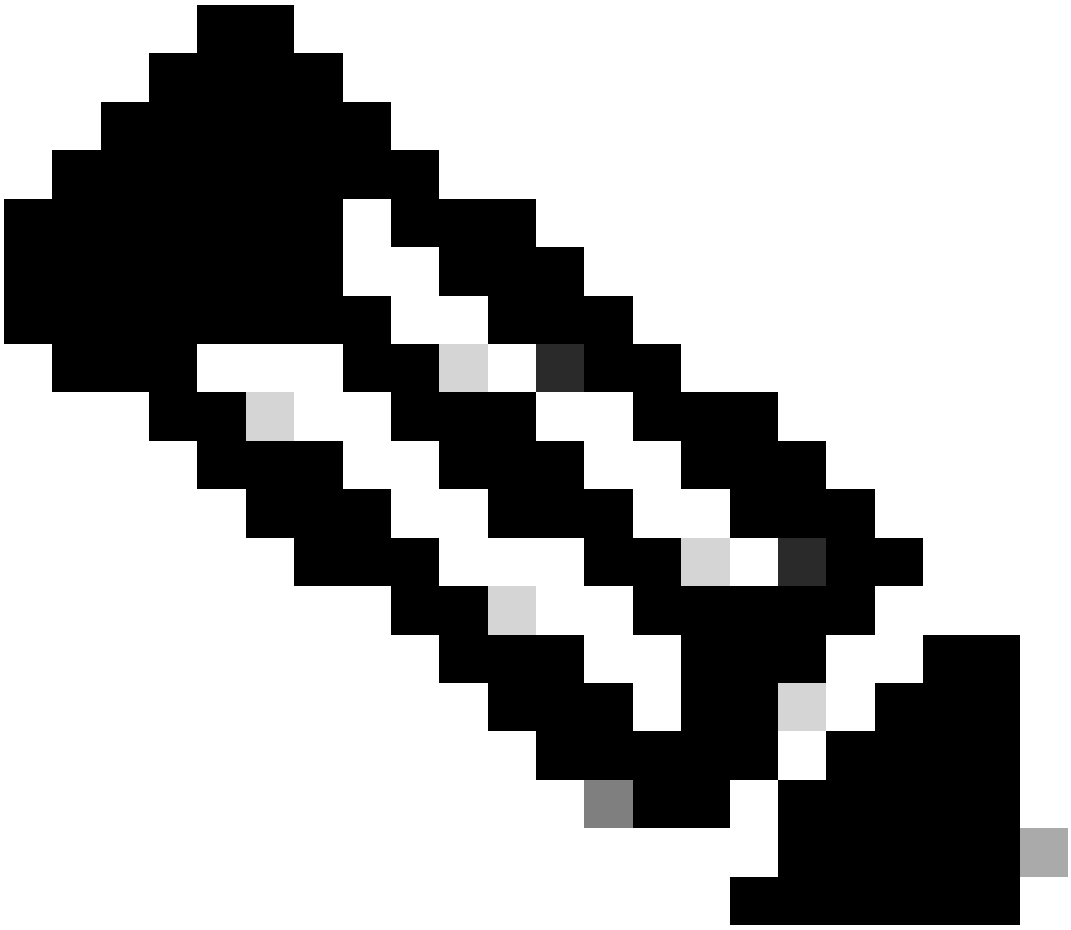
モジュラス：**必須**（目的のキー強度のオプションボタンをクリックします）。

認証局：**必須**。ドロップダウンリストから、先ほど作成した認証局を選択します。

秘密キー：キーリングを介して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。

---



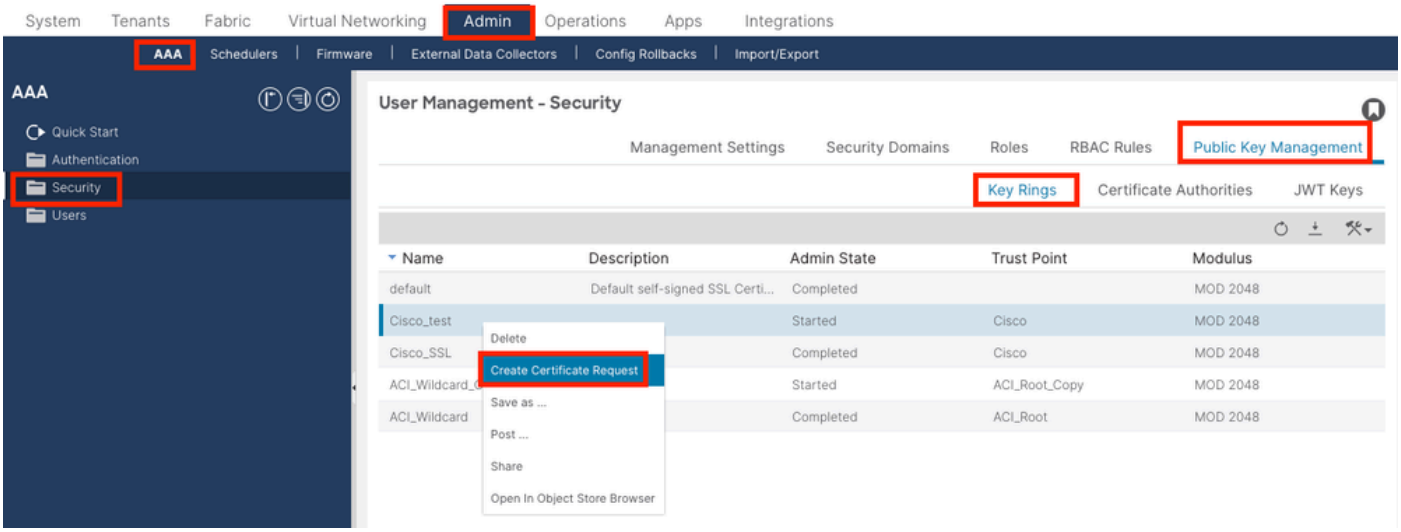
**注**：システム生成の秘密キーとCSRを使用せず、カスタムの秘密キーと証明書を使用する場合は、名前、証明書、認証局、秘密キーの4つの項目を入力するだけです。 送信後に実行する必要があるのは、最後のステップであるステップ5だけです。

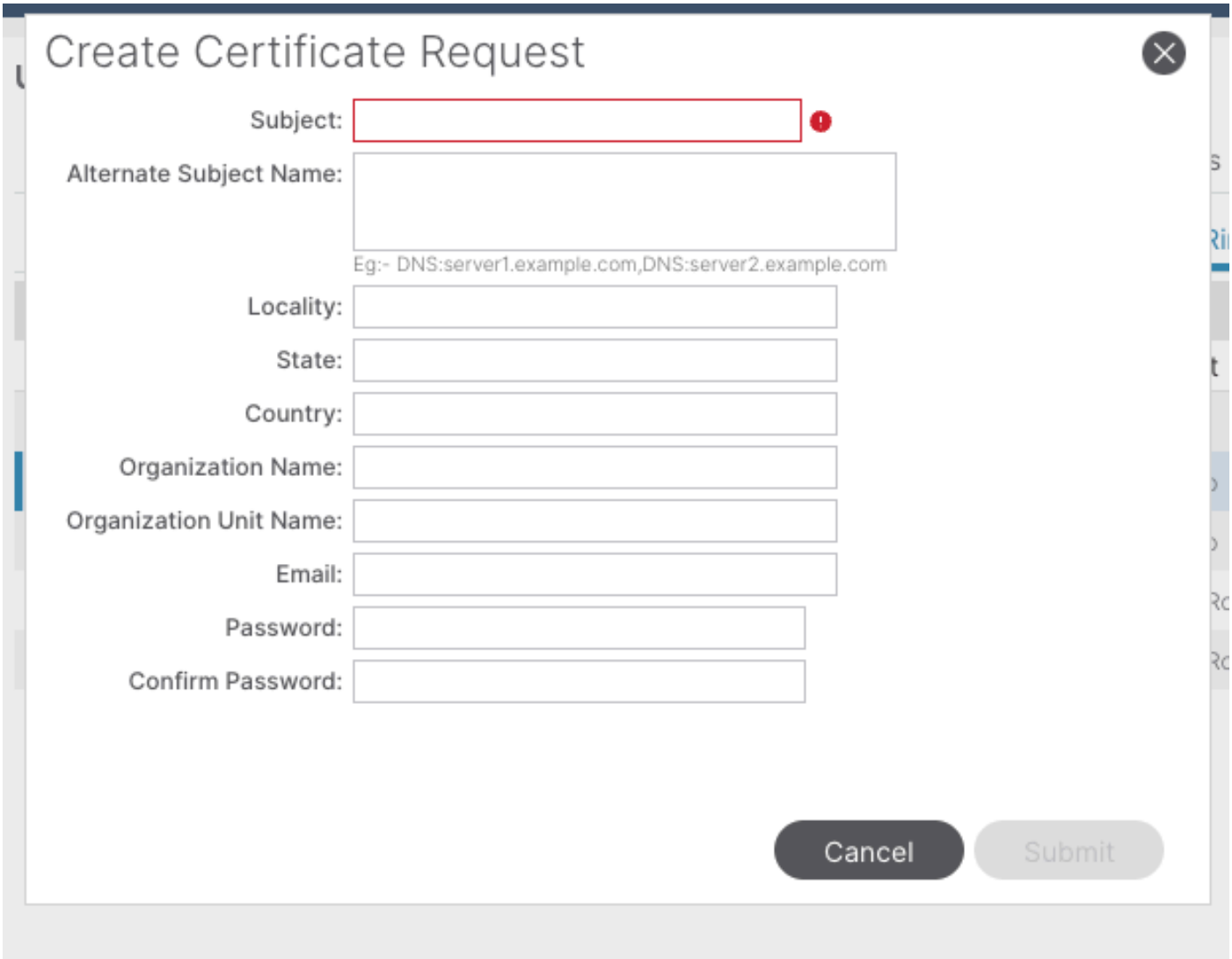
---

**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。




件名：**必須。**CSRの共通名(CN)を入力します。

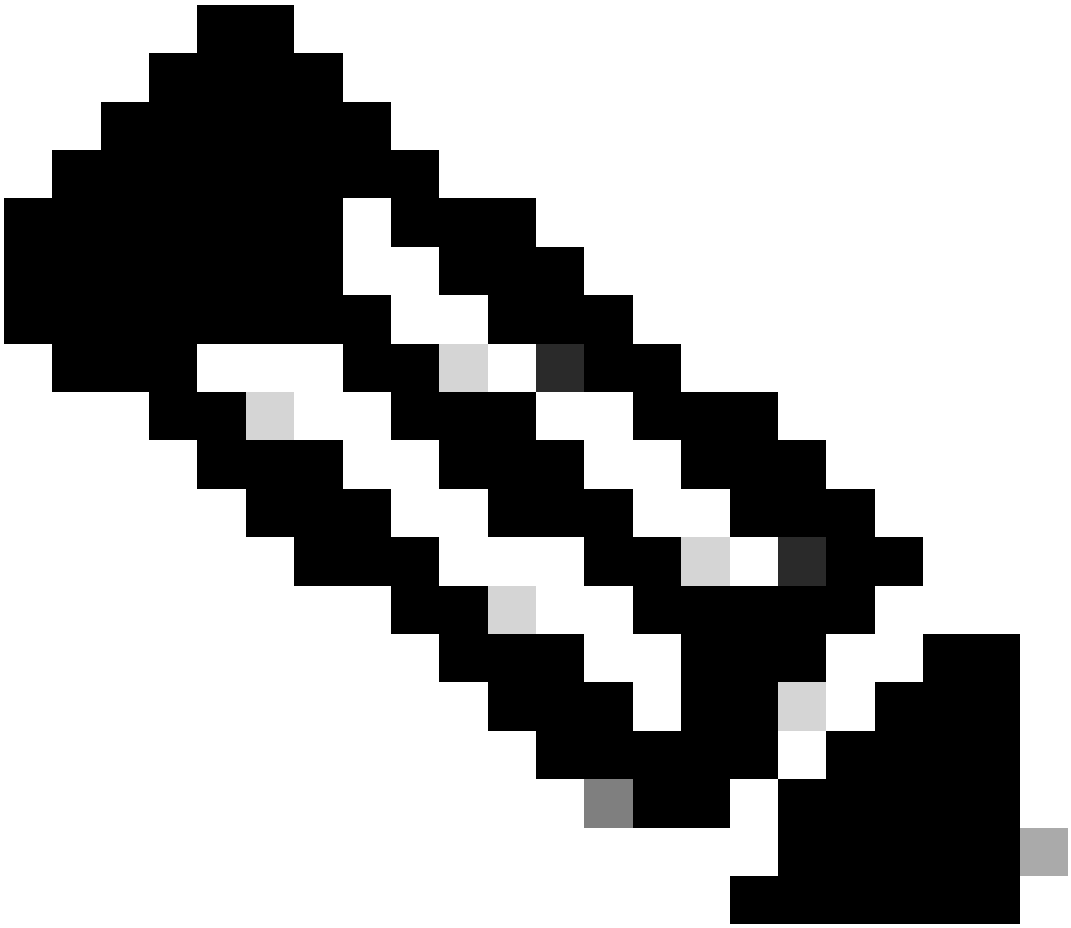
ワイルドカードを使用してCisco APICの完全修飾ドメイン名(FQDN)を入力できますが、最新の証明書では一般的に、証明書の識別可能な名前を入力し、すべてのCisco APICのFQDNを代替サブジェクト名（SAN – サブジェクト代替名）フィールドに入力することをお勧めします。これは、最近のブラウザの多くがSANフィールドにFQDNを想定しているためです。

代替サブジェクト名：**必須。** 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をIPアドレスに一致させる場合は、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、またはその両方の組み合わせを使用できます。IPv6アドレスはサポートされていません。

---

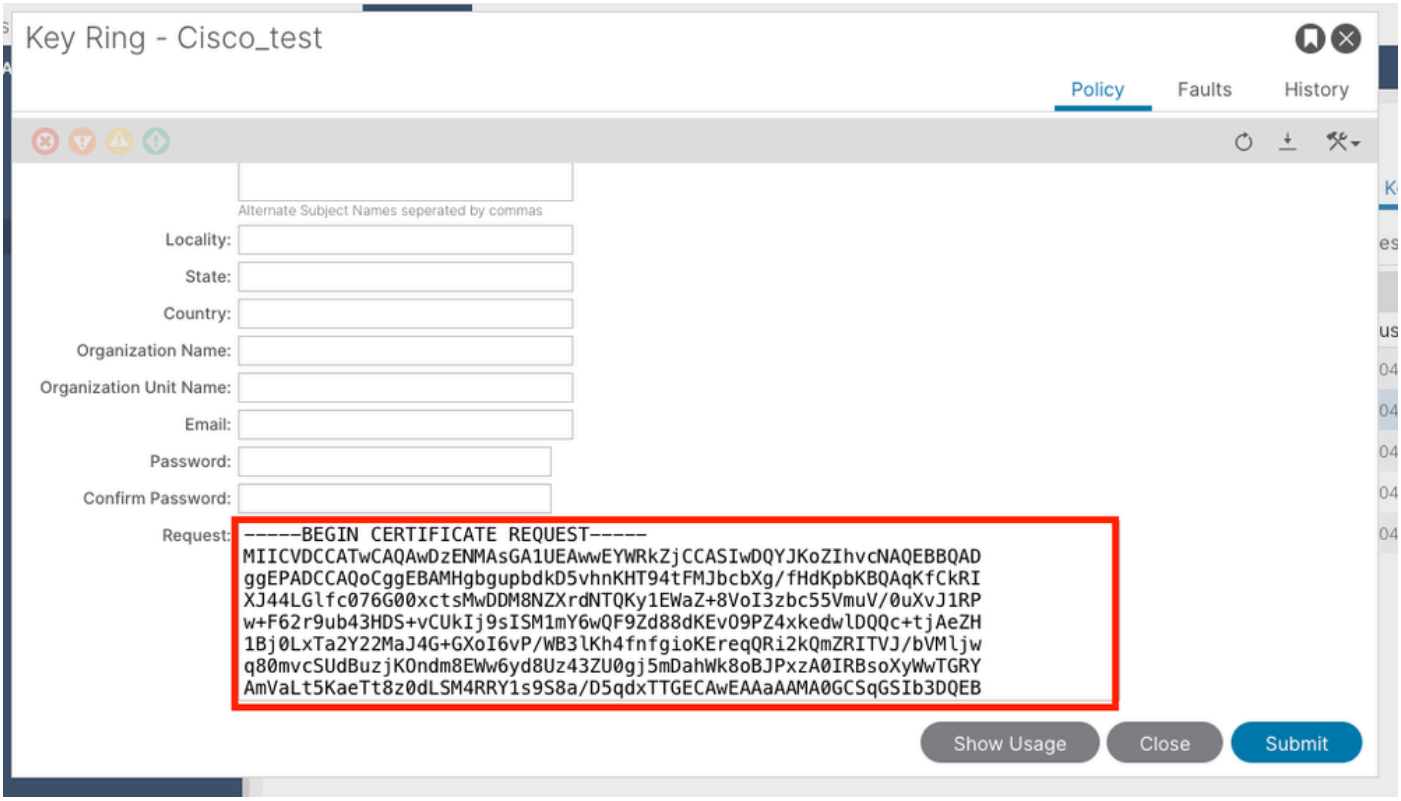
証明書を発行するために適用するCA組織の要件に従って、残りのフィールドに入力します。

**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。

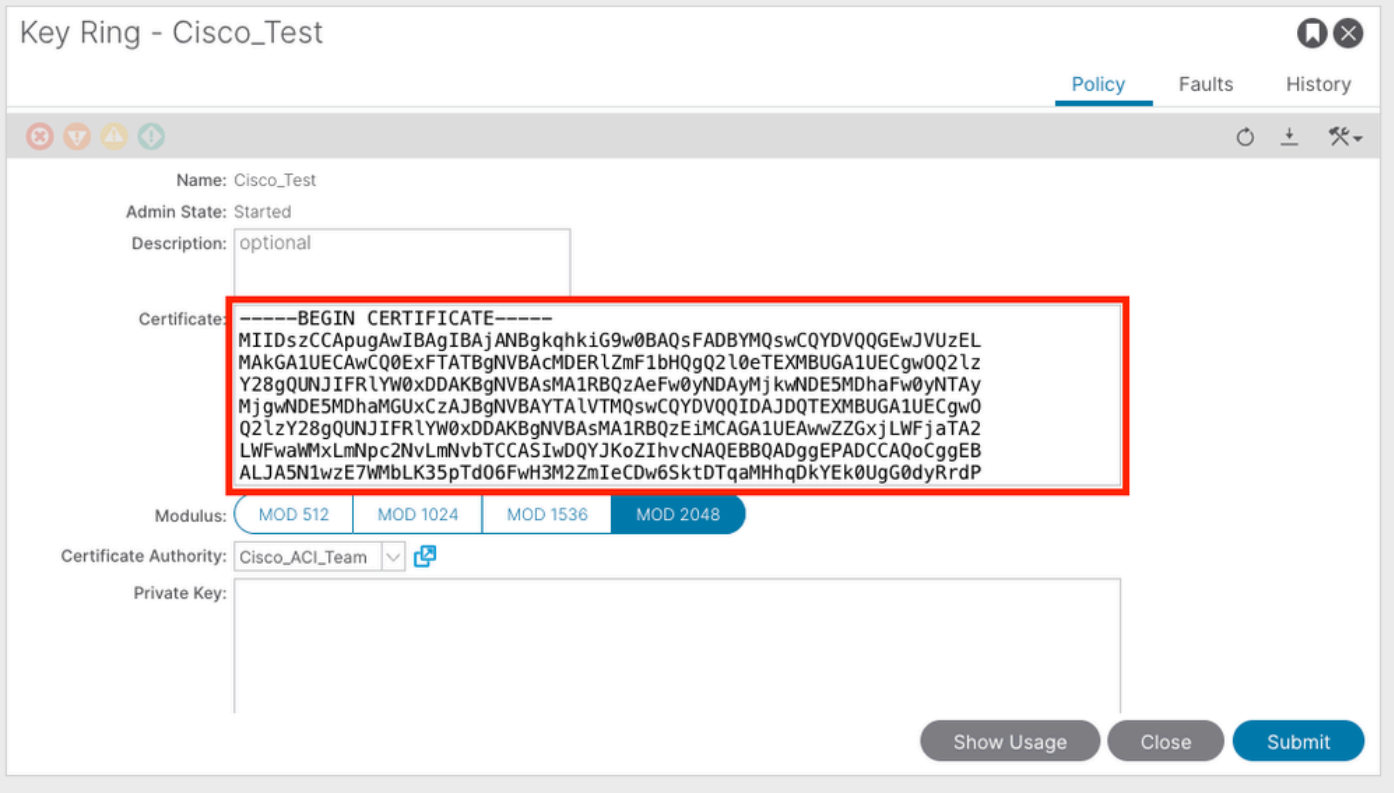
作成したキーリング名をダブルクリックして、**Request**オプションを探します。 リクエストの内容はCSRです。

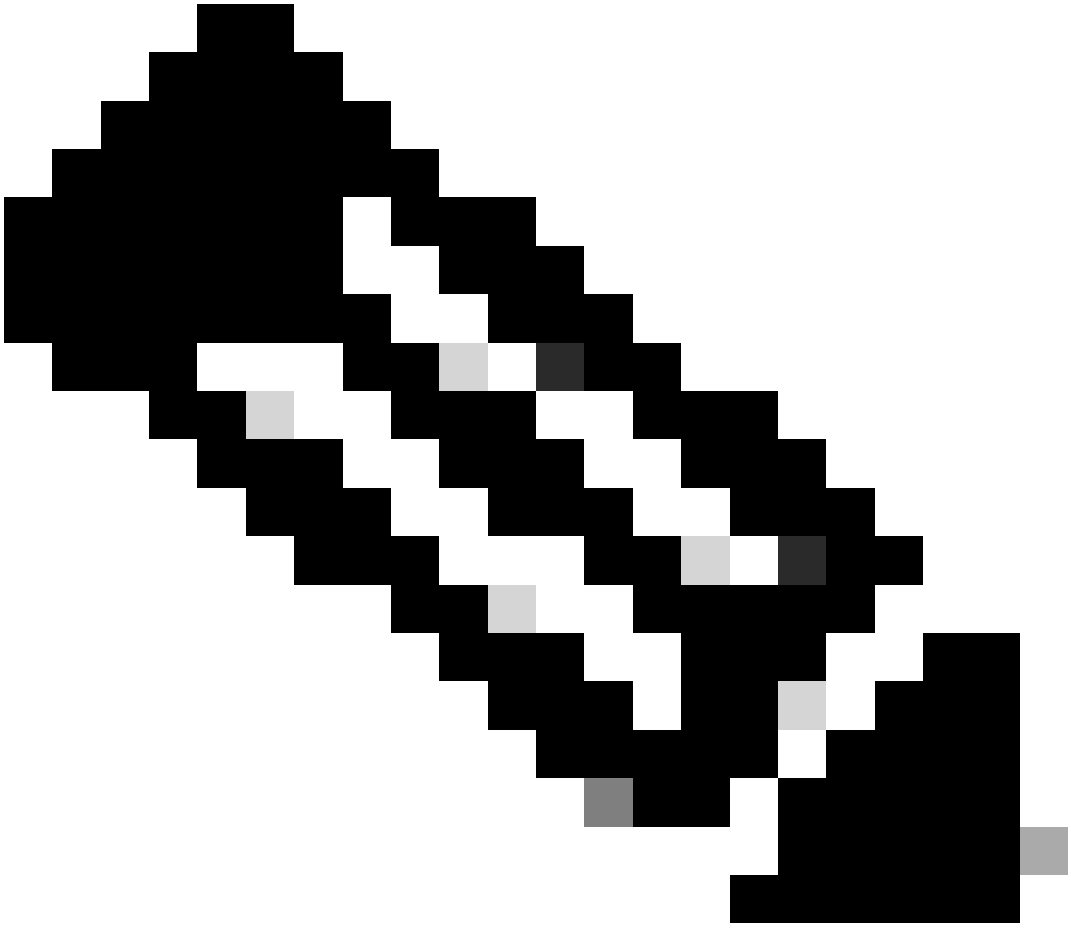



要求のすべての内容をコピーし、CAに送信します。

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-----
MIIDszCCApugAwIBAgIBAjANBgkqhkiG9w0BAQsFADBYMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExFTATBgNVBAcMDERlZmF1bHQgQ2l0eTEXMBUGA1UECgwOQ2lz
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDAyMjkwNDE5MDhaFw0yNTAy
MjgwNDE5MDhaMGUxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJDQTEXMBUGA1UECgwO
Q2lzY28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFjaTA2
LWFwaWMxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALJA5N1wzE7WMbLK35pTdO6FwH3M2ZmIeCDw6SktDTqaMHhqDkYEk0UgG0dyRrdP
Modulus:
MOD 512
MOD 1024
MOD 1536
MOD 2048
Certificate Authority: Cisco_ACI_Team
Private Key:
Show Usage
Close
Submit



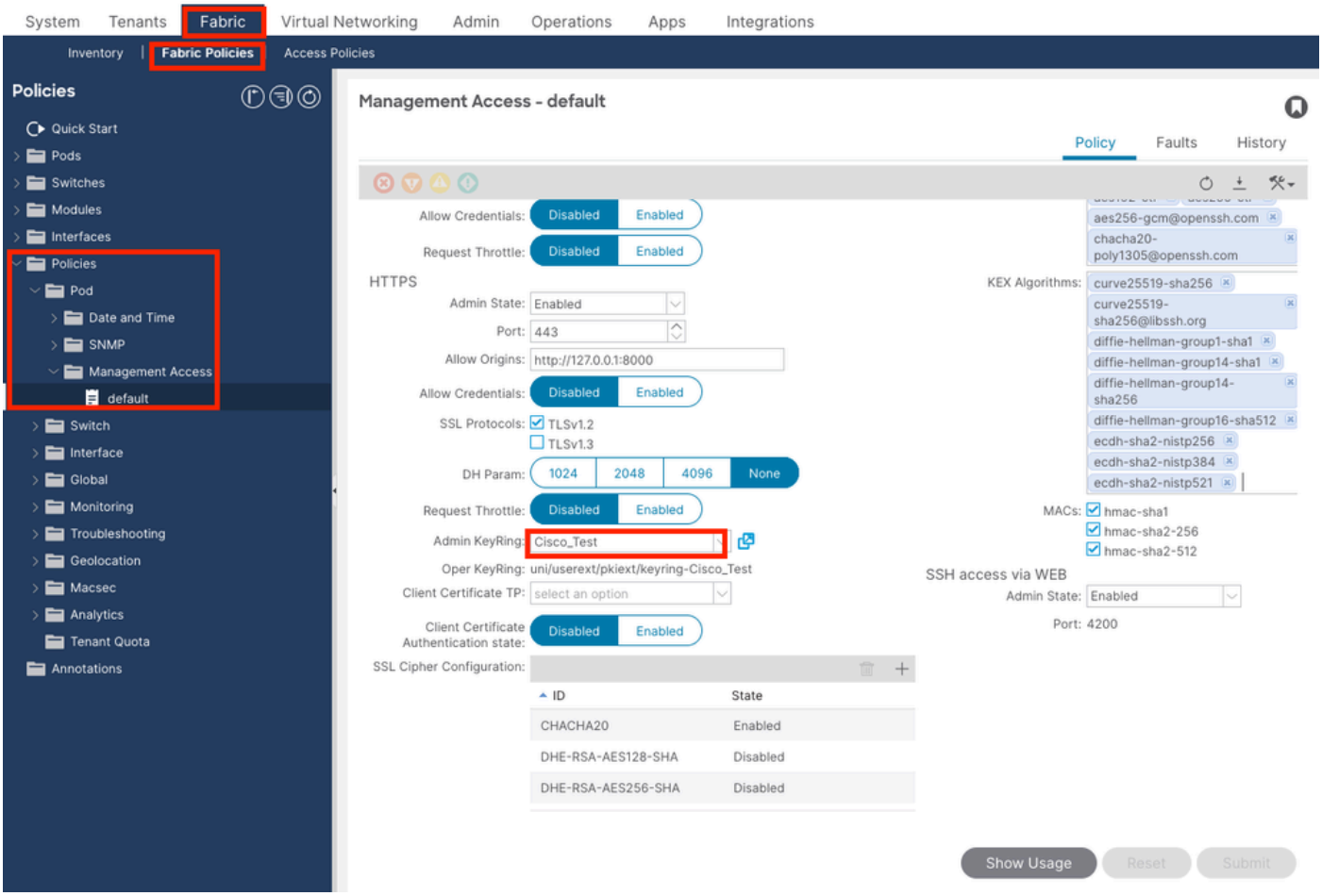
**注**：各証明書は、固定フォーマットに準拠している必要があります。

-----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上で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。



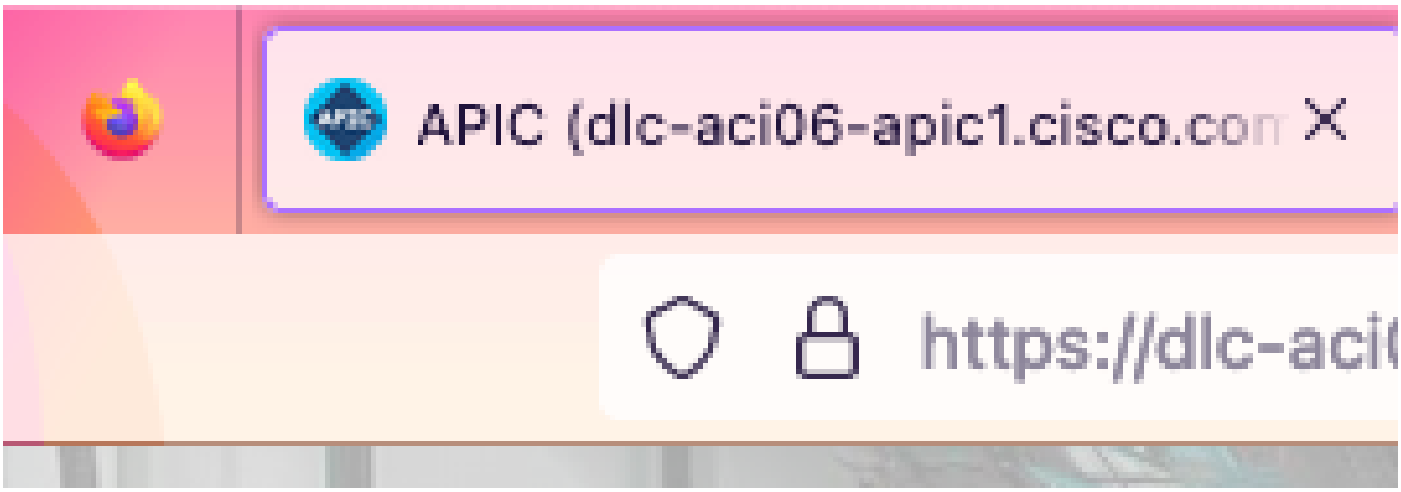

**Admin KeyRing**ドロップダウンリストから、目的のKeyRingを選択します。

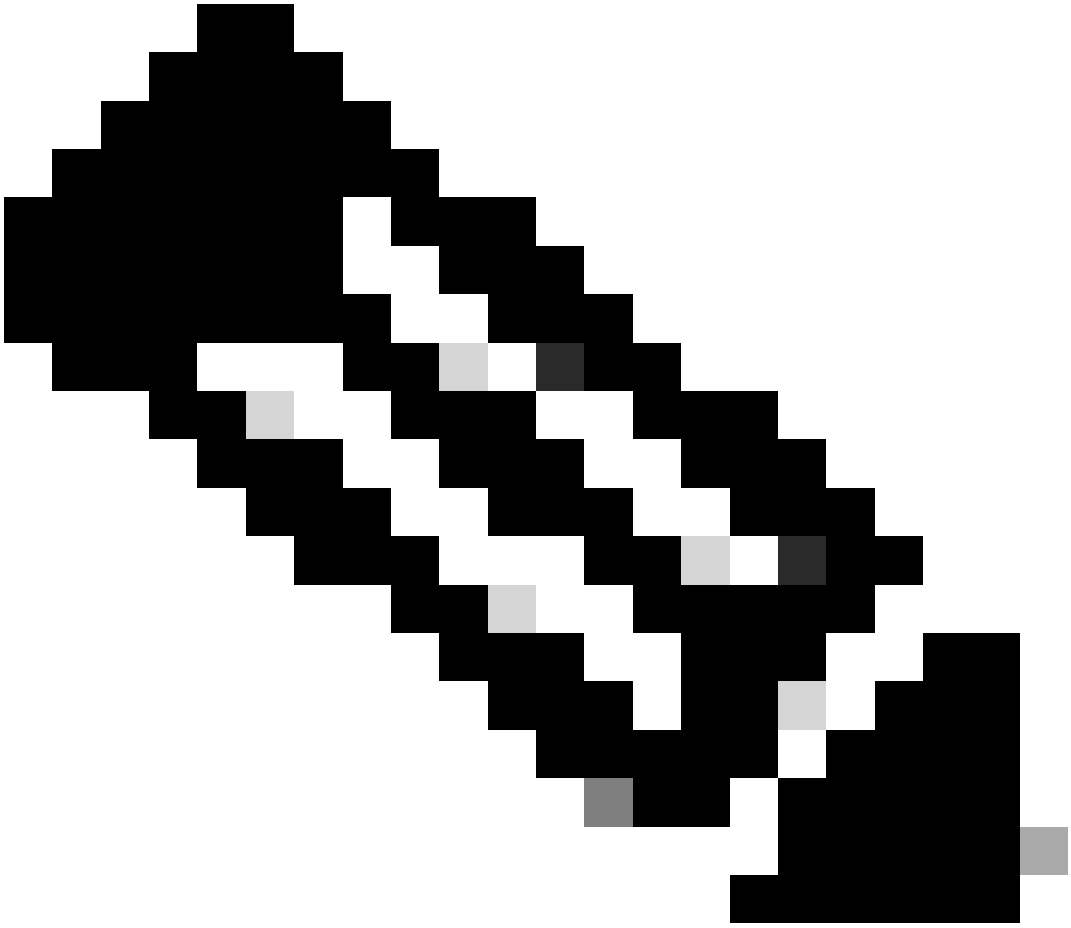
**Submit**ボタンをクリックします。

「submit」をクリックした後、証明書の理由による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。



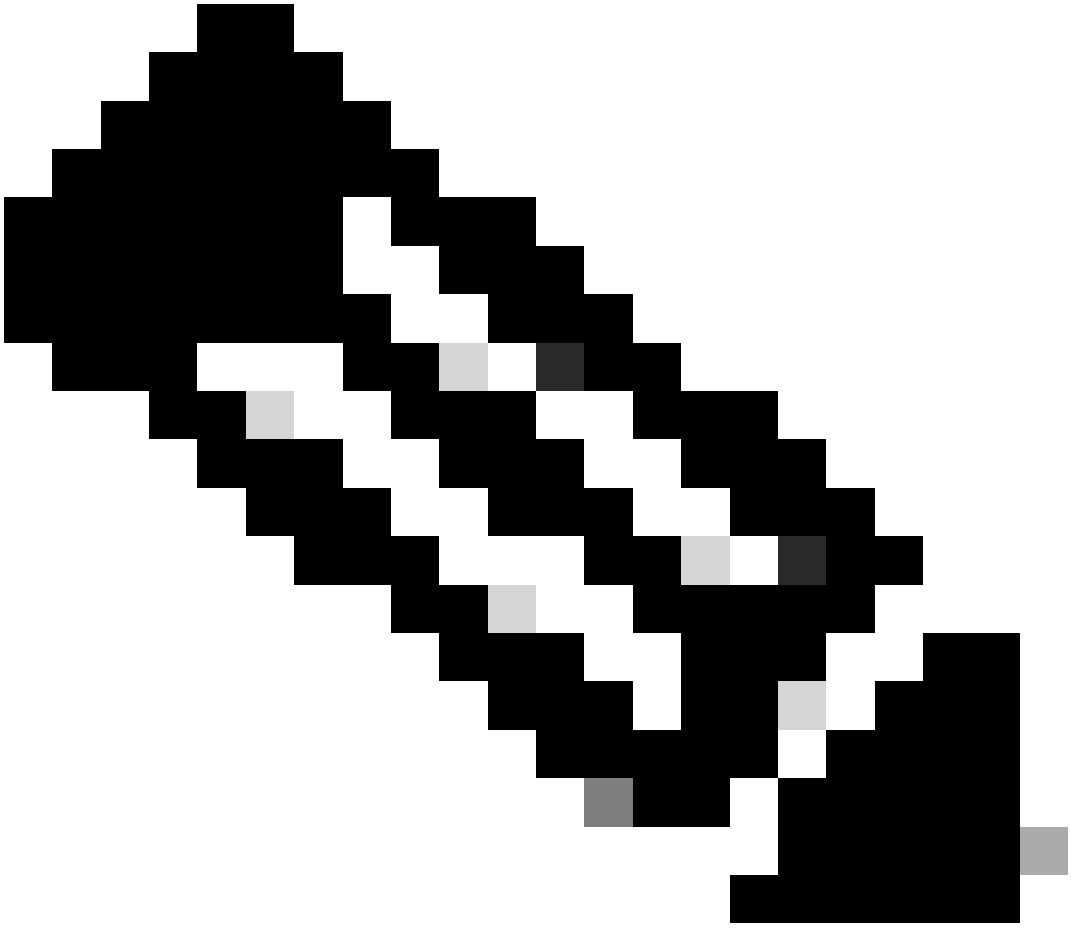


**注**：異なるブラウザでHTTPS証明書を表示する方法は、完全に同じではありません。特定の方法については、ブラウザのユーザガイドを参照してください。

---

トラブルシュート

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証明書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。



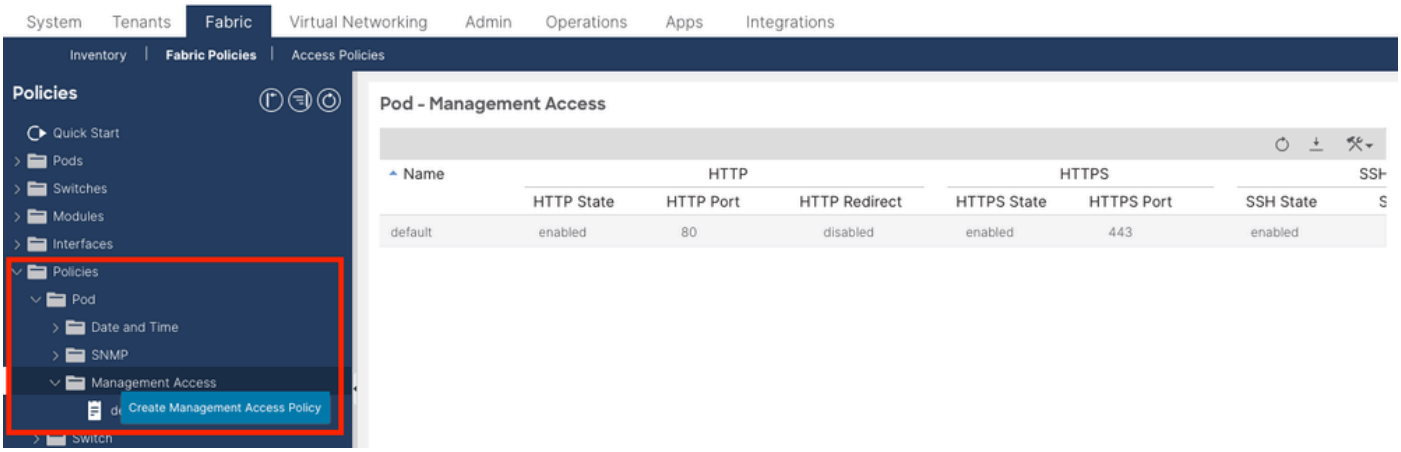
**注**：この証明書を信頼するには、Google Chromeブラウザが証明書の**SAN**を確認する必要があります。

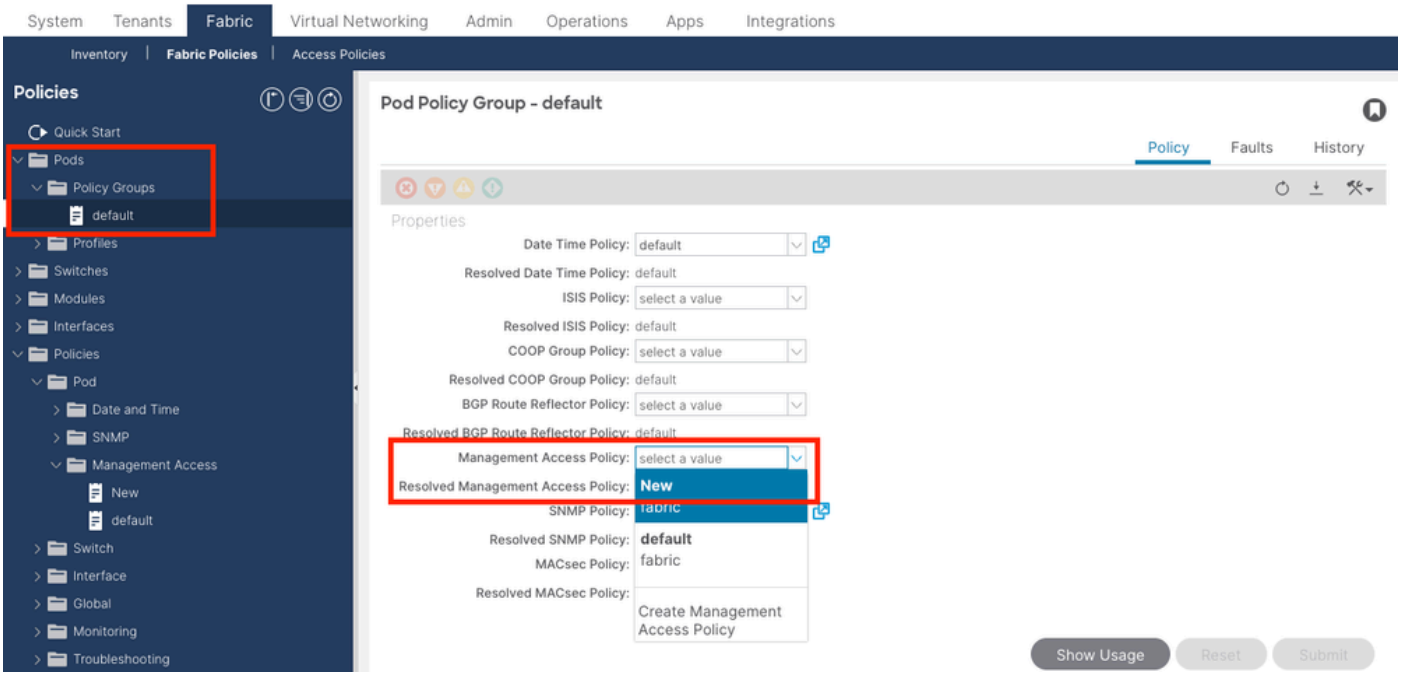
---

自己署名証明書を使用するAPICでは、まれに証明書の期限切れ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。




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。