

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](#)

[手順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。

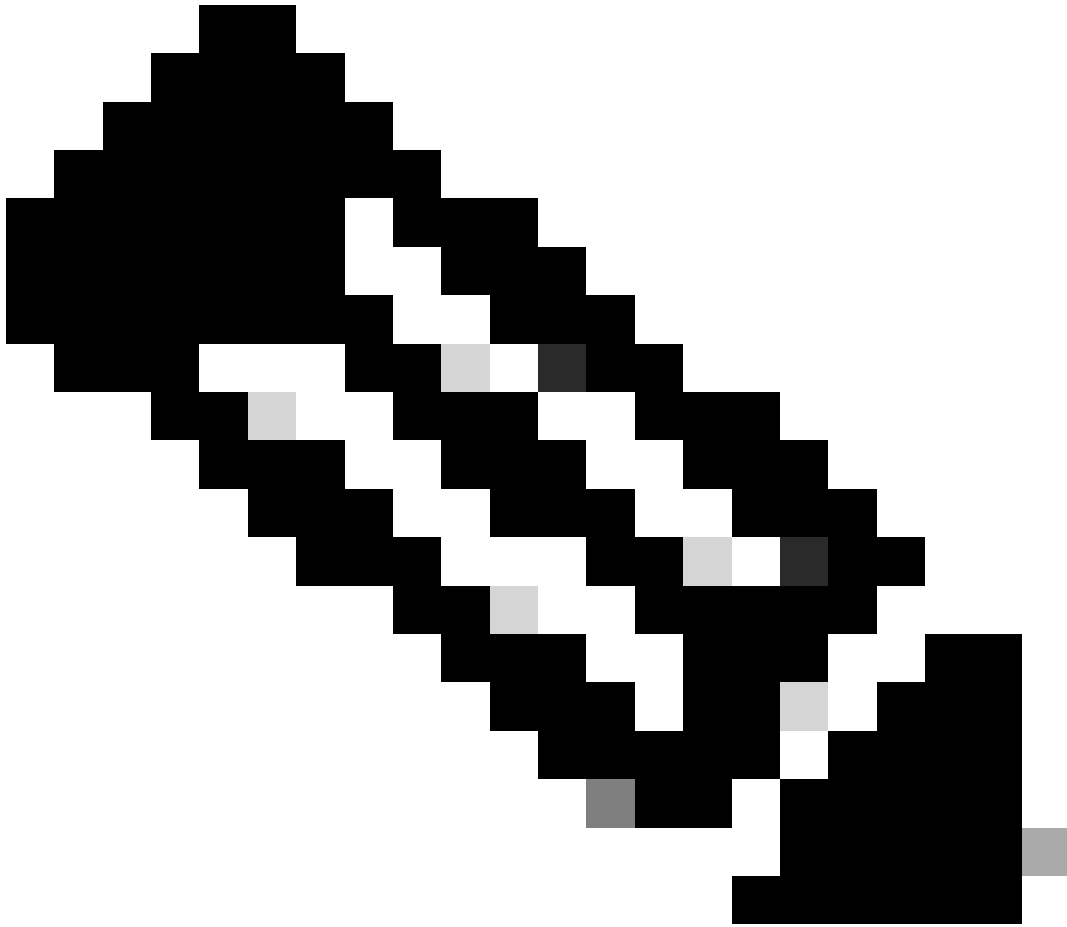
デフォルトでは、自己署名証明書の有効期限の1カ月前にデバイスが自動的に更新され、新しい自己署名証明書が生成されます。

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：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。

The screenshot shows the Cisco ACI management console interface. The top navigation bar includes System, Tenants, Fabric, Virtual Networking, Admin, Operations, Apps, and Integrations. The Admin menu is expanded, showing AAA, Schedulers, Firmware, External Data Collectors, Config Rollbacks, and Import/Export. The AAA menu is further expanded to show Authentication, Security, and Users. The Security menu is selected, and the Public Key Management page is displayed. The Public Key Management page has tabs for Management Settings, Security Domains, Roles, RBAC Rules, Public Key Management, Key Rings, Certificate Authorities, and JWT Keys. The Certificate Authorities tab is selected, showing a table with columns for Name, Description, FP, and N. The table contains two entries: ACI_Root and Cisco_AD_CA. A 'Create Certificate Authority' button is visible in the bottom right corner of the table.

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

User Management - Security

Create Certificate Authority

Name: !

Description: optional

Certificate Chain:

Cancel Submit

名前：必須。

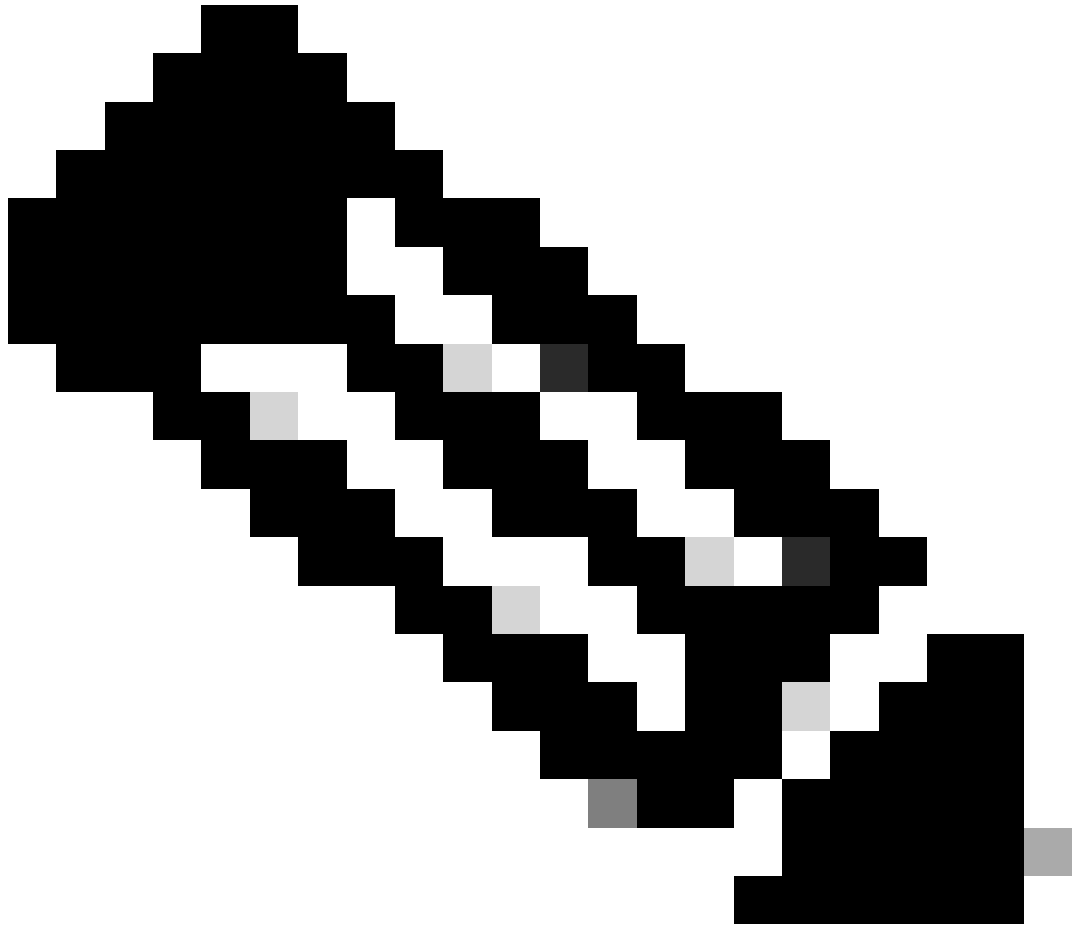
命名規則に従って内容を作成します。_を使用できますが、次のような特殊文字は使用できません。

, . ; ' " : | + * / = ` ~ ! @ # \$ % ^ & () 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。

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 selected. On the left sidebar, the 'AAA' menu is expanded, showing 'Quick Start', 'Authentication', 'Security', and 'Users'. The 'Security' option is highlighted. The main content area is titled 'User Management - Security' and contains sub-tabs for Management Settings, Security Domains, Roles, RBAC Rules, Public Key Management, Certificate Authorities, and JWT Keys. The 'Public Key Management' tab is active, and the 'Key Rings' sub-tab is selected. Below the sub-tabs is a table with columns: Name, Description, Admin State, Trust Point, and Modulus. The table contains two entries: 'ACI_Wildcard' and 'default'. A 'Create Key Ring' button is visible in the top right corner of the table area.

The 'Create Key Ring' dialog box is shown. It has a close button (X) in the top right corner. The fields are: Name (required, with a red error icon), Description (optional), Certificate (text area), Modulus (radio buttons for MOD 512, MOD 1024, MOD 1536, and MOD 2048), Certificate Authority (dropdown menu), and Private Key (text area). A note at the bottom of the Private Key field reads: 'If you want to use an externally generated private key, please provide it here'. At the bottom right, there are 'Cancel' and 'Submit' buttons.

名前：必須 (名前を入力してください)。

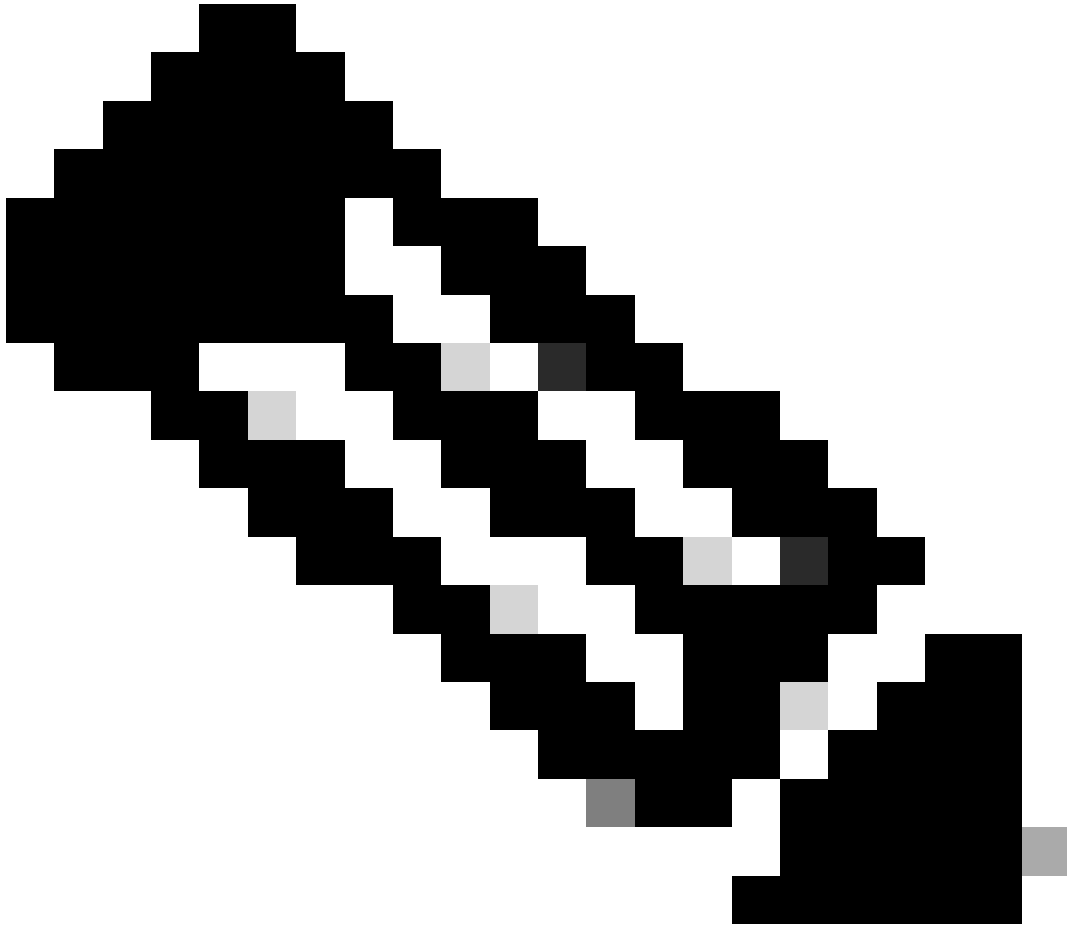
証明書：キーリングを介してCisco APICを使用して証明書署名要求(CSR)を生成する場合は、コンテンツを追加しないでください。または、秘密キーとCSRをCisco APICの外部で生成することで、前の手順でCAによって署名された証明書をすでに持っている場合は、署名付き証明書のコンテンツを追加します。

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。

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 Cert...	Completed		MOD 2048
Cisco_test		Started	Cisco	MOD 2048
Cisco_SSL		Completed	Cisco	MOD 2048
ACI_Wildcard_0		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

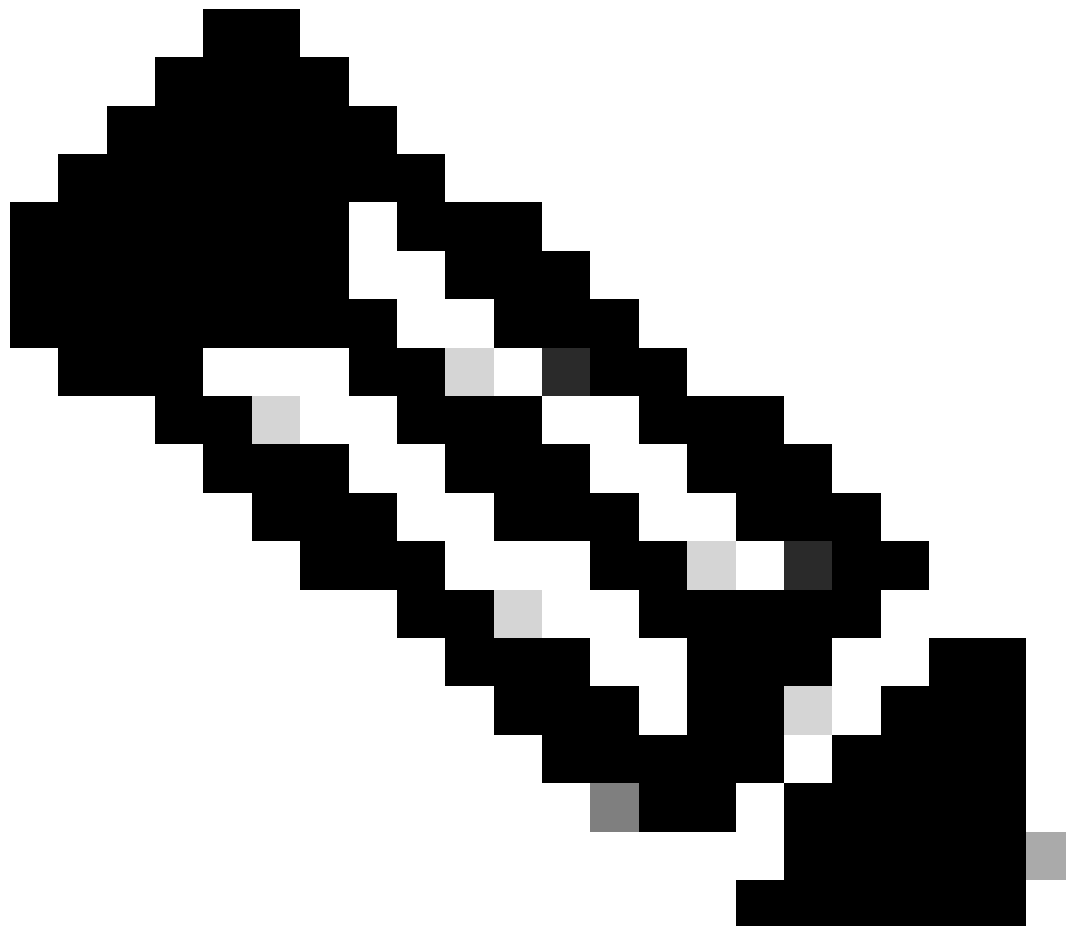
件名：必須。CSRの共通名(CN)を入力します。

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。

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-----
MIICVDCCAQAwDzENMAAGA1UEAwEYWRkZjCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcbXg/fHdKpbKBQAgKfCKRI
XJ44LGLfc076G00xctSMwDDM8NZXrdNTQKy1EwaZ+8VoI3zbc55VmuV/0uXvJ1RP
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQc+tjAeZH
1Bj0LxTa2Y22MaJ4G+GXoI6vP/WB3lKh4fnfgioKEreqQR12kQmZRITVJ/bVMljw
q80mvcSUDBuzjK0ndm8EWw6yd8Uz43ZU0gj5mDahWk8oBJPxzA0IRBsoXyWwTGRY
AmVaLt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECAwEAAMA0GCSqGSIb3DQEB
```

Show Usage Close Submit

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。



Name: Cisco_Test

Admin State: Started

Description: optional

Certificate: -----BEGIN CERTIFICATE-----
MIIDszCCApugAwIBAgIBAgjANBgqhkiG9w0BAQsFADBYMQswCQYDVQGEwJVUzEL
MAKGA1UECAwCQ0EFTATBgNVBACMDERlZmF1bHQgQ2l0eTEEXMBUGA1UECgw0Q2Lz
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDYyMjE5MDU5MDhaFw0yNTAy
MjE5MDU5MDhaMGUxCzAJBgNVBAYTAlVMTQswCQYDVQQLIDQTEEXMBUGA1UECgw0
Q2LzY28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFlaTA2
LWFwawMxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALJA5N1wzE7WmBk35pTd06FwH3M2ZmIeCDw6SktDTqaMHhqDkYEK0UgG0dyRrdP

Modulus: MOD 512 MOD 1024 MOD 1536 MOD 2048

Certificate Authority: Cisco_ACL_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。

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
 - default**
 - Switch
 - Interface
 - Global
 - Monitoring
 - Troubleshooting
 - Geolocation
 - Macsec
 - Analytics
 - Tenant Quota
 - Annotations

Management Access - default

Policy Faults History

Allow Credentials: Disabled Enabled

Request Throttle: Disabled Enabled

HTTPS

Admin State:

Port:

Allow Origins:

Allow Credentials: Disabled Enabled

SSL Protocols: TLSv1.2 TLSv1.3

DH Param:

Request Throttle: Disabled Enabled

Admin KeyRing:

Oper KeyRing: uni/userext/pkiext/keyring-Cisco_Test

Client Certificate TP:

Client Certificate Authentication state: Disabled Enabled

SSH access via WEB

Admin State:

Port:

MACs: hmac-sha1 hmac-sha2-256 hmac-sha2-512

KEX Algorithms:

SSL Cipher Configuration:

ID	State
CHACHA20	Enabled
DHE-RSA-AES128-SHA	Disabled
DHE-RSA-AES256-SHA	Disabled

Show Usage Reset Submit

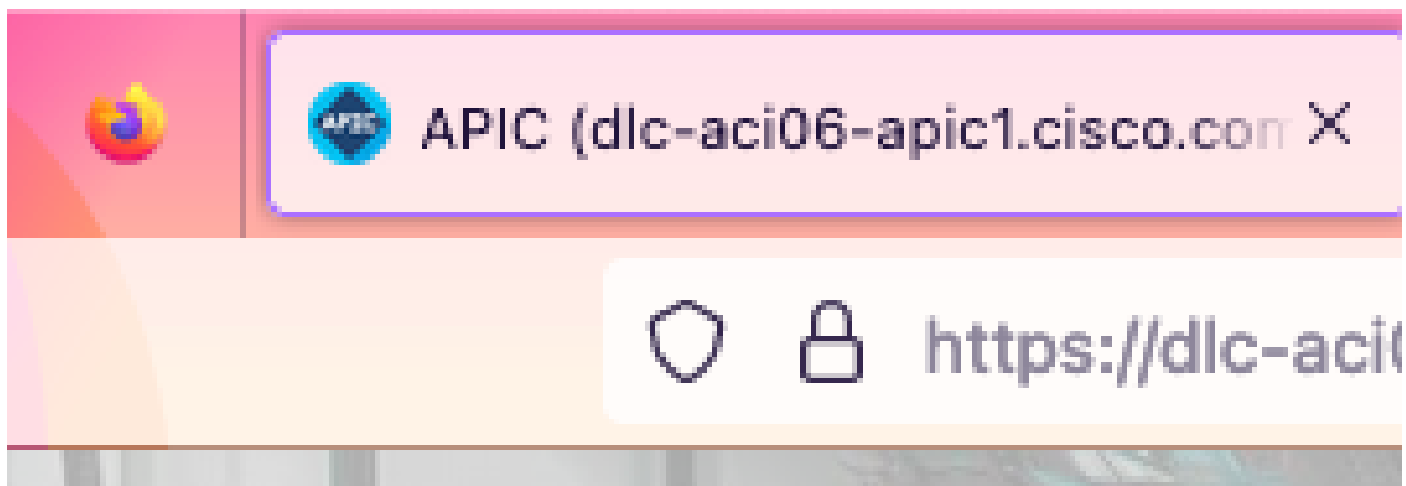
Admin KeyRing ドロップダウンリストから、目的のKeyRingを選択します。

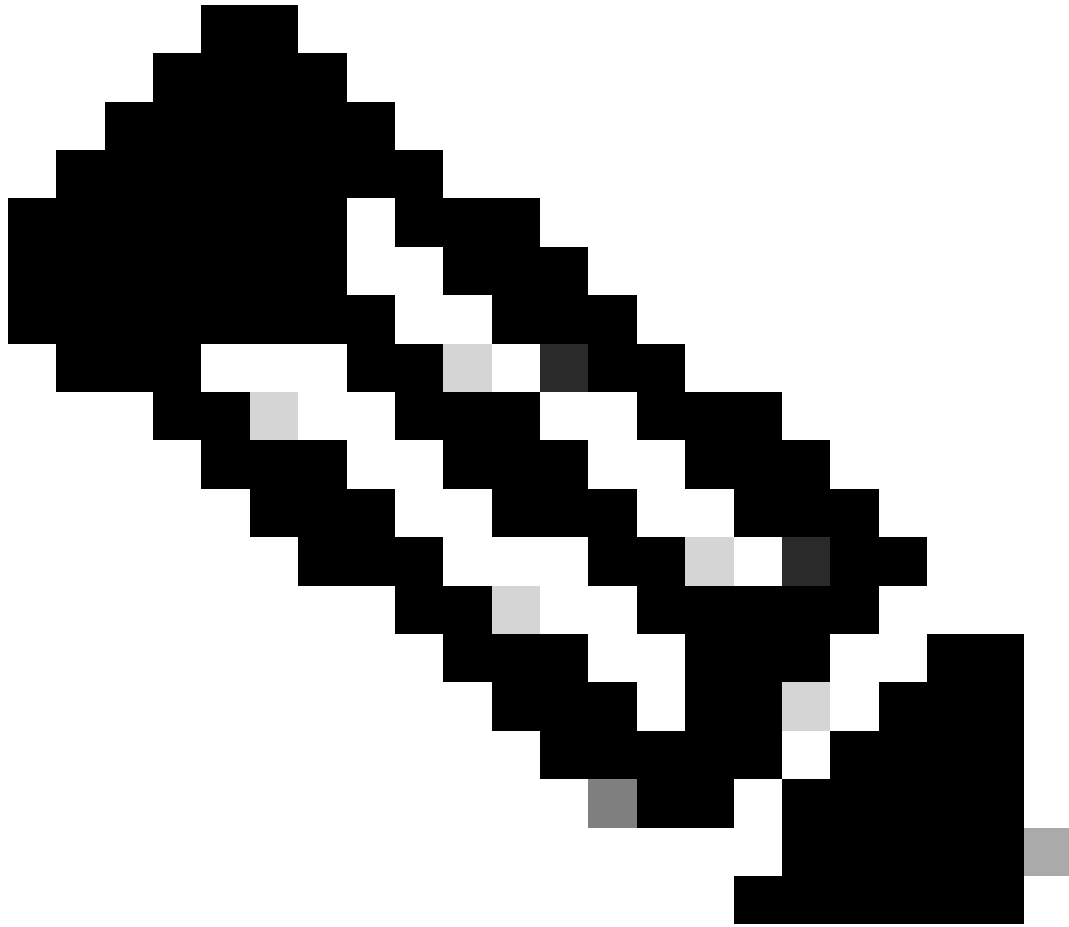
Submitボタンをクリックします。

「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。

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。