

# Configurer le certificat HTTPS de l'interface graphique ACI APIC

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Configurations](#)

[Étape 1. Importez le certificat racine de l'autorité de certification ou le certificat intermédiaire](#)

[Étape 2. Créer un anneau de clés](#)

[Étape 3. Génération d'une clé privée et d'un CSR](#)

[Étape 4. Obtenir le CSR et l'envoyer à l'organisation AC](#)

[Étape 5. Mise à jour du certificat de signature sur le Web](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit la configuration des certificats SSL personnalisés et auto-signés.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Signatures numériques et certificats numériques
- Processus d'émission de certificat par l'organisme d'autorité de certification

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur des infrastructures des politiques relatives aux applications (APIC)
- Navigateur
- ACI 5.2 (8e)

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

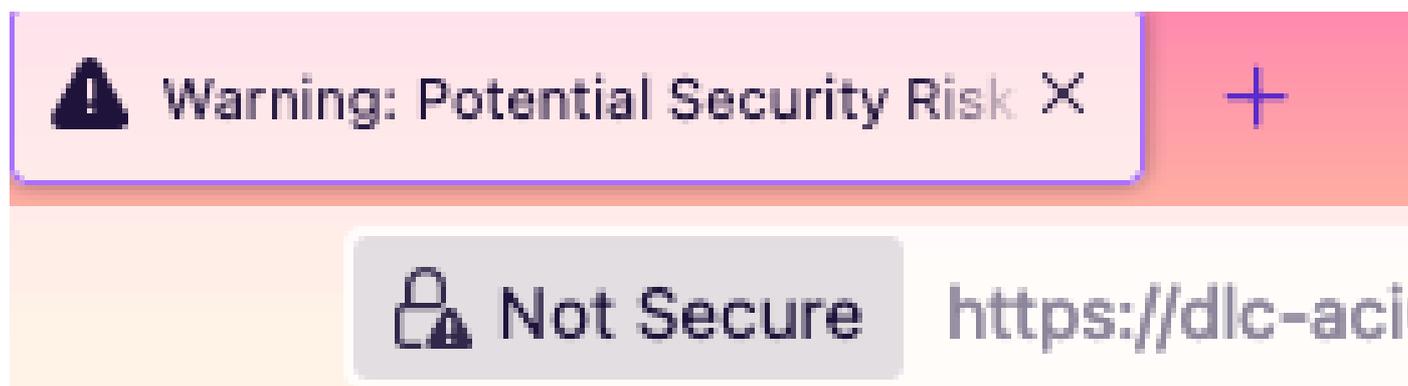
## Configurer

Une fois le périphérique initialisé, il utilise le certificat auto-signé comme certificat SSL pour HTTPS. Le certificat auto-signé est valide pendant 1 000 jours.

Par défaut, le périphérique renouvelle et génère automatiquement un nouveau certificat auto-signé un mois avant l'expiration du certificat auto-signé.

## Configurations

Le périphérique utilise un certificat auto-signé. Lorsque vous accédez à l'interface graphique utilisateur du contrôleur APIC, le navigateur vous demande si le certificat n'est pas digne de confiance. Afin de résoudre ce problème, ce document utilise une autorité de certification approuvée afin de signer le certificat.



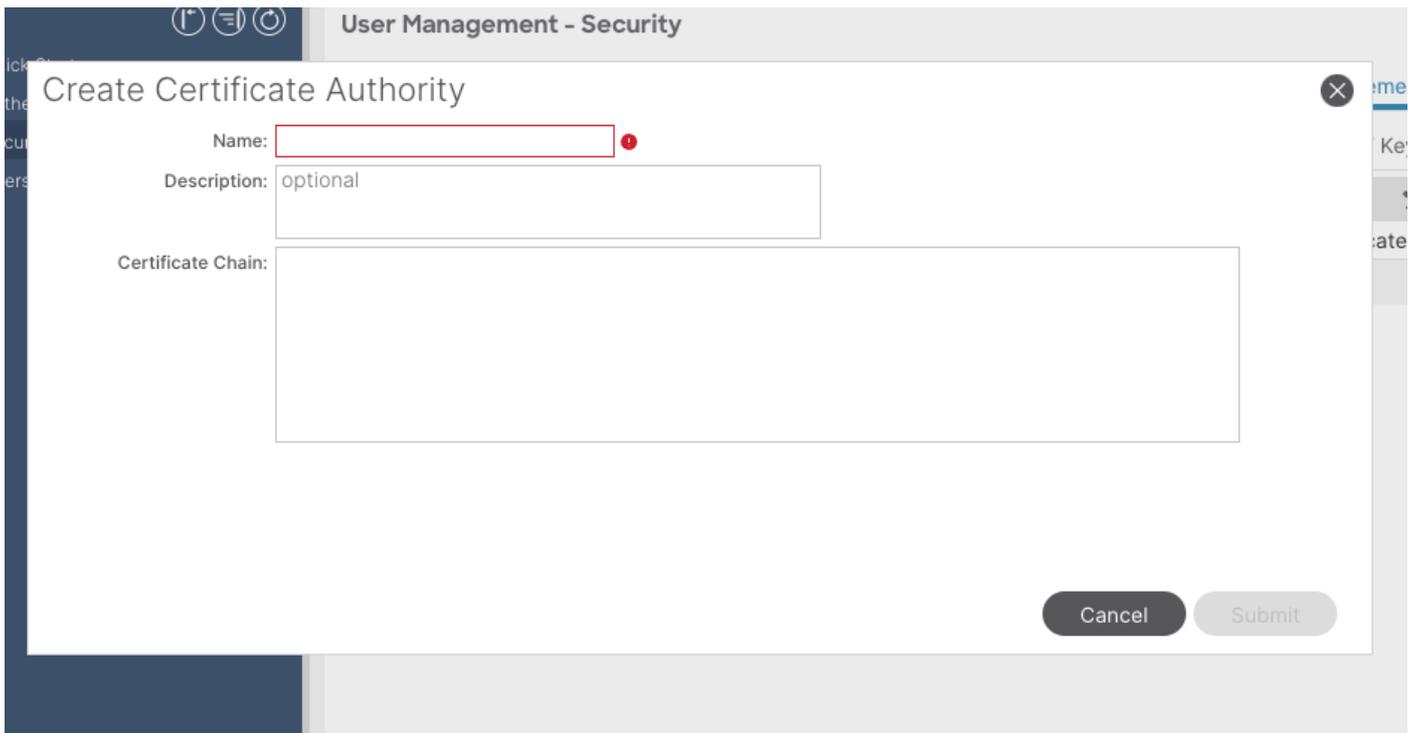
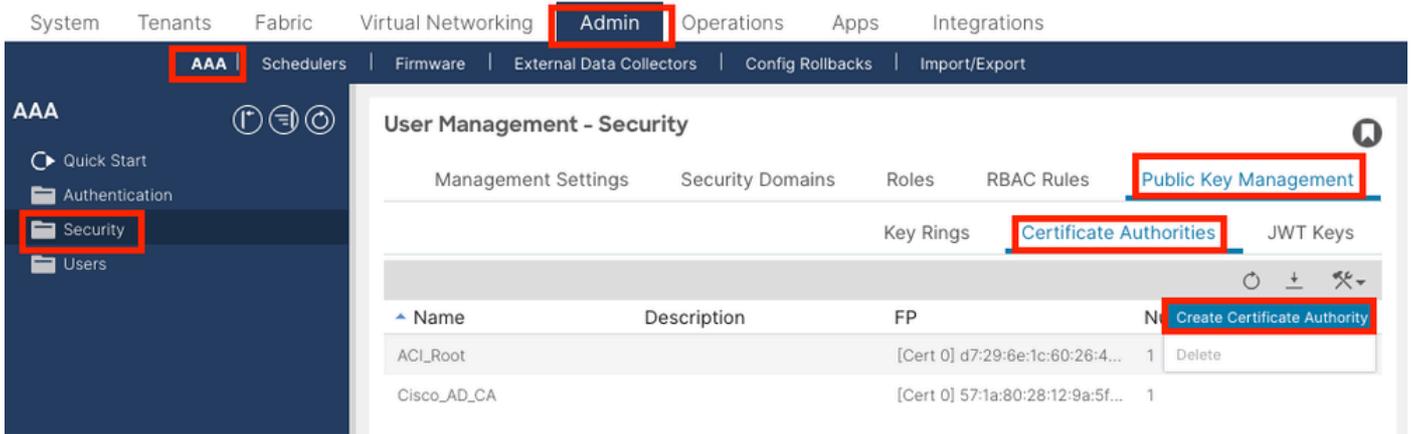
Étape 1. Importer le certificat racine de l'autorité de certification ou le certificat intermédiaire



Remarque : si vous utilisez le certificat racine de l'autorité de certification pour signer directement, vous pouvez simplement importer le certificat racine de l'autorité de certification. Mais si vous utilisez un certificat intermédiaire pour la signature, vous devez importer la chaîne de certificats complète, c'est-à-dire : le certificat racine et les certificats intermédiaires moins fiables.

---

Dans la barre de menus, accédez à [Admin > AAA > Security > Public Key Management > Certificate Authorities](#).



Nom : **obligatoire**.

Formuler le contenu en fonction de vos règles de nommage. Il peut contenir \_, mais pas de caractères anglais spéciaux, tels que : . , ; ' " : | + \* / = ` ~ ! @ # \$ % ^ & ( ) et des espaces.

Description : **Facultatif**.

Chaîne de certification : **obligatoire**.

Remplissez le certificat racine CA approuvé et le certificat intermédiaire CA.



**Remarque** : chaque certificat doit être conforme à un format fixe.

```
-----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-----
```

---

Cliquez sur le bouton **Envoyer**.

Étape 2. Créer un anneau de clés

Dans la barre de menus, accédez à Admin > AAA > Security > Public Key Management > Key Rings.

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. Below it, the 'AAA' section is expanded, showing 'Schedulers', 'Firmware', 'External Data Collectors', 'Config Rollbacks', and 'Import/Export'. The 'Security' folder is highlighted. The main content area is titled 'User Management - Security' and contains 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. A table lists existing key rings, and a 'Create Key Ring' button is visible in the top right corner of the table.

Name	Description	Admin State	Trust Point	M
ACI_Wildcard		Completed	ACI_Root	M Delete
default	Default self-signed S...	Completed		MOD 2048

The 'Create Key Ring' form is displayed. It includes the following fields and options:

- Name:** A required text input field with a red border and a red exclamation mark icon.
- Description:** A text input field with the value 'optional'.
- Certificate:** A large text area for pasting certificate content.
- Modulus:** A set of radio buttons with options: MOD 512, MOD 1024, MOD 1536, and MOD 2048. The MOD 2048 option is selected.
- Certificate Authority:** A dropdown menu with the text 'select an option'.
- Private Key:** A large text area for pasting private key content.

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.

Nom : **obligatoire** (saisissez un nom).

Certificat : **n'ajoutez** aucun contenu si vous générez une demande de signature de certificat (CSR) à l'aide du contrôleur APIC Cisco via l'anneau de clés. Vous pouvez également ajouter le contenu du certificat signé si vous en avez déjà un signé par l'autorité de certification à partir des étapes précédentes en générant une clé privée et un CSR en dehors du contrôleur APIC Cisco.

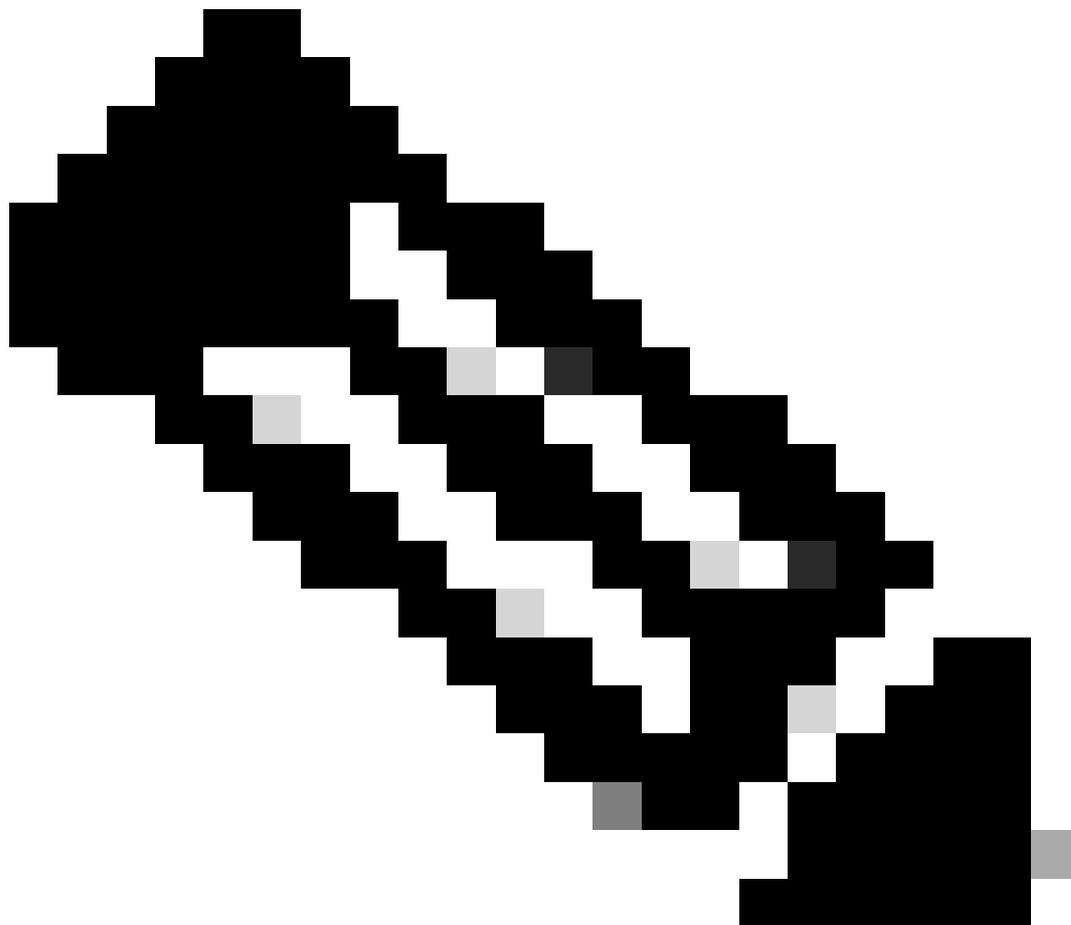
Module : **Obligatoire** (cliquez sur la case d'option correspondant à l'intensité de la touche souhaitée).

Autorité de certification : **obligatoire**. Dans la liste déroulante, sélectionnez l'autorité de certification que vous avez créée précédemment.

Clé privée : **n'ajoutez** aucun contenu si vous générez un CSR à l'aide du contrôleur APIC Cisco via le porte-clés. Vous pouvez également

ajouter la clé privée utilisée pour générer le CSR pour le certificat signé que vous avez entré.

---



**Remarque** : si vous ne souhaitez pas utiliser la clé privée et le CSR générés par le système et utiliser une clé privée et un certificat personnalisés, il vous suffit de remplir quatre éléments : Nom, Certificat, Autorité de certification et Clé privée. Après l'envoi, vous n'avez qu'à effectuer la dernière étape, l'étape 5.

---

Cliquez sur le bouton **Envoyer**.

Étape 3. Générer une clé privée et un CSR

Dans la barre de menus, accédez à Admin > AAA > Security > Public Key Management > Key Rings.

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_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

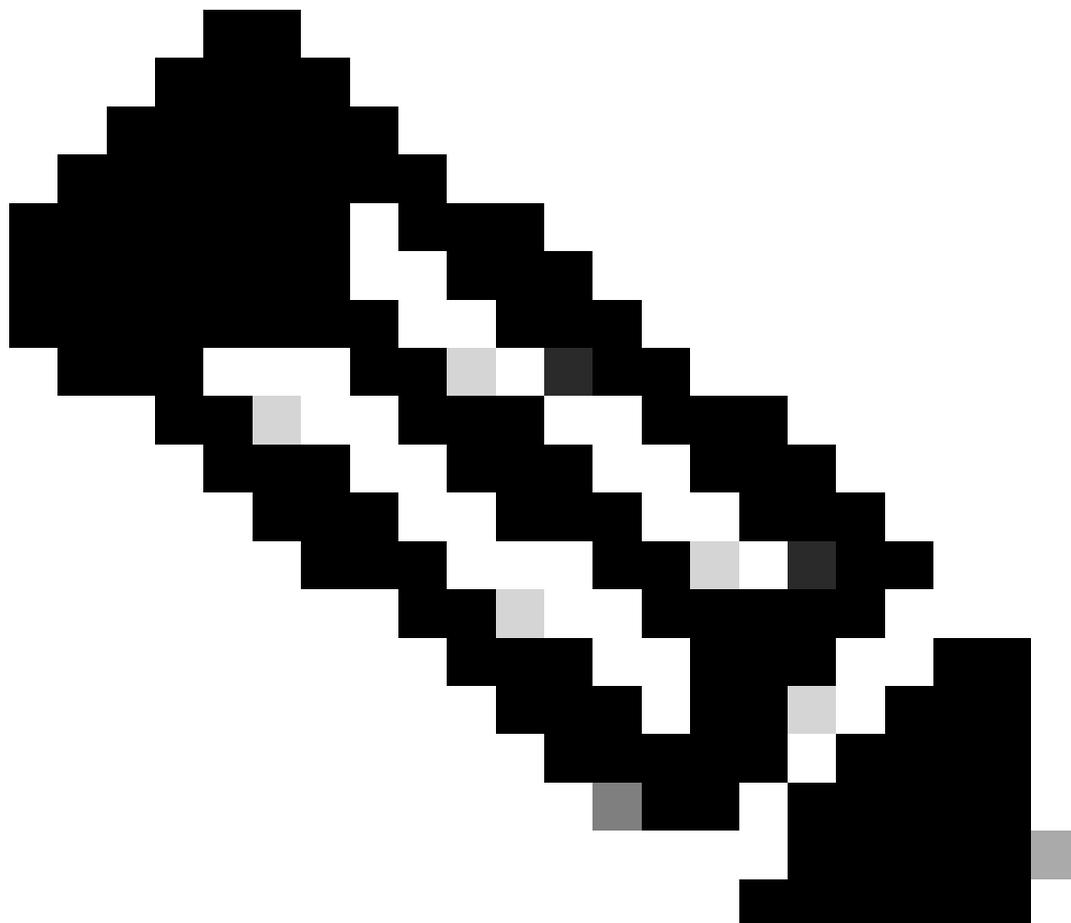
Objet : **obligatoire**. Saisissez le nom commun (CN) du CSR.

Vous pouvez entrer le nom de domaine complet (FQDN) des Cisco APIC en utilisant un caractère générique, mais dans un certificat moderne, il est généralement recommandé d'entrer un nom identifiable du certificat et d'entrer le FQDN de tous les Cisco APIC dans le champ Autre nom de sujet (également connu sous le nom alternatif de SAN - Sujet) parce que de nombreux navigateurs modernes attendent le FQDN dans le champ SAN.

Autre nom du sujet : **obligatoire**. Saisissez le nom de domaine complet de tous les APIC Cisco, tels que  
DNS:apic1.example.com,DNS:apic2.example.com,DNS:apic3.example.com ou DNS:\*example.com.

Si vous souhaitez que le SAN corresponde à une adresse IP, vous pouvez également entrer les adresses IP des cartes Cisco APIC au format  
suivant : IP:192.168.1.1.

---



**Remarque** : vous pouvez utiliser des noms DNS (Domain Name Server), des adresses IPv4 ou une combinaison des deux dans ce champ. Les adresses IPv6 ne sont pas prises en charge.

---

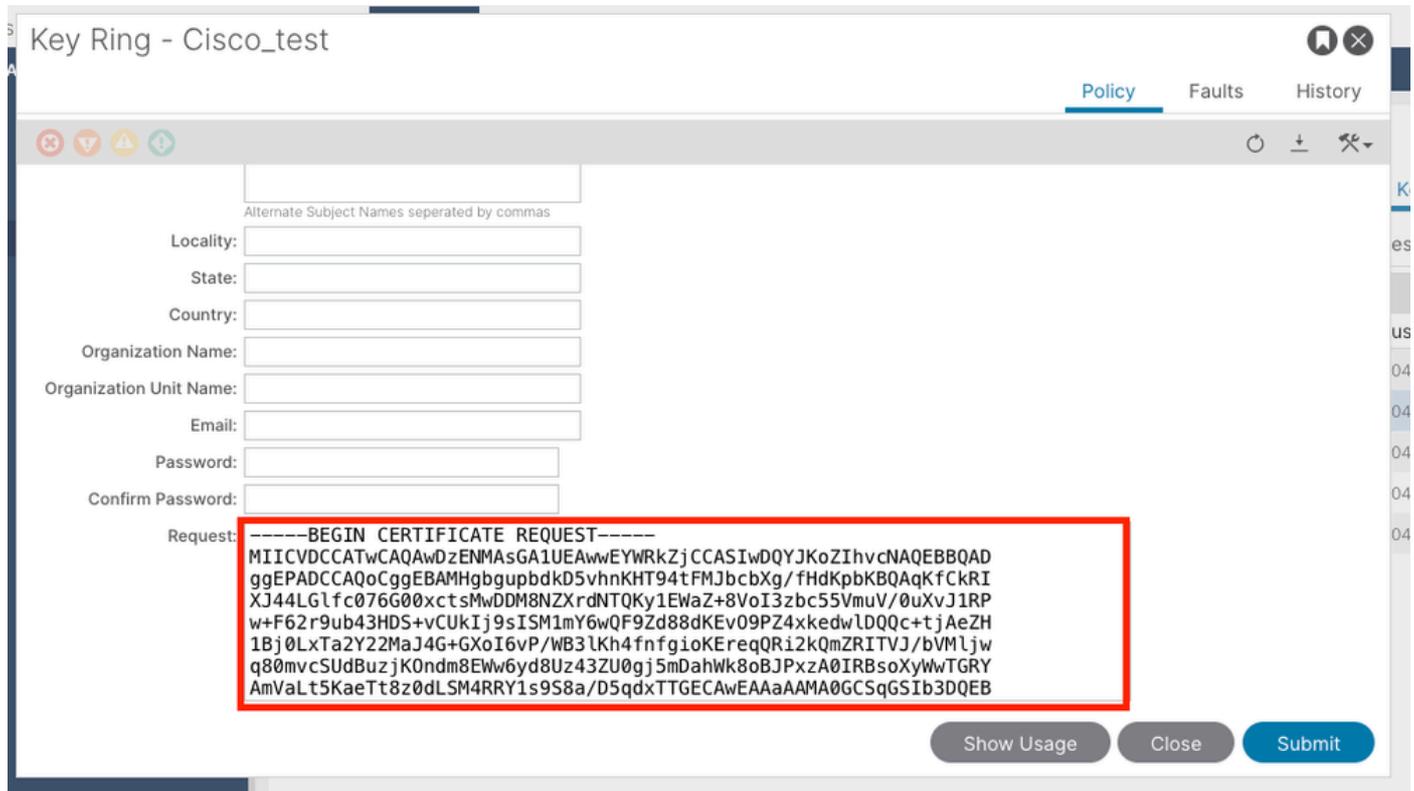
Remplissez les champs restants en fonction des exigences de l'organisme de certification que vous demandez afin de délivrer le certificat.

Cliquez sur le bouton **Envoyer**.

#### Étape 4. Obtenir le CSR et l'envoyer à l'organisation AC

Dans la barre de menus, accédez à Admin > AAA > Security > Public Key Management > Key Rings.

Double-cliquez sur le nom de votre **Key Ring** de création et recherchez l'option **Request**. Le contenu de la demande est le CSR.



The screenshot shows the 'Key Ring - Cisco\_test' configuration page. The 'Request' field is highlighted with a red box and contains the following text:

```
-----BEGIN CERTIFICATE REQUEST-----  
MIICVDCCATwCAQAwDzENMAsgA1UEAwEYWRkZjCCASiwDQYJKoZIhvcNAQEBBQAD  
ggEPADCCAQoCggEBAMHgbgubdkD5vhnKHT94tFMJbcbXg/fHdKpbKBQAgKfCKRI  
XJ44LGLfc076G00xctsmwDDM8NZXrdNTQKy1EwaZ+8VoI3zbc55VmuV/0uXvJ1RP  
w+F62r9ub43HDS+vCUkIj9sISM1mY6wQF9Zd88dKEv09PZ4xkedwLDQqc+tjAeZH  
1Bj0LxTa2Y22MaJ4G+GxoI6vP/WB3lKh4fnfgioKEreqQR12kQmZRITVJ/bVMljw  
q80mvcSUDBuzjK0ndm8EWw6yd8Uz43ZU0gj5mDahWk8oBJPxzA0IRBsoXyWwTGRY  
AmVaLt5KaeTt8z0dLSM4RRY1s9S8a/D5qdxTTGECAwEAAMA0GCSqGSIb3DQEBA
```

Copiez tout le contenu de la demande et envoyez-la à votre autorité de certification.

L'autorité de certification utilise sa clé privée afin d'effectuer la vérification de signature sur votre CSR.

Après avoir obtenu le certificat signé auprès de l'autorité de certification, elle copie le certificat dans le certificat.



Name: Cisco\_Test

Admin State: Started

Description: optional

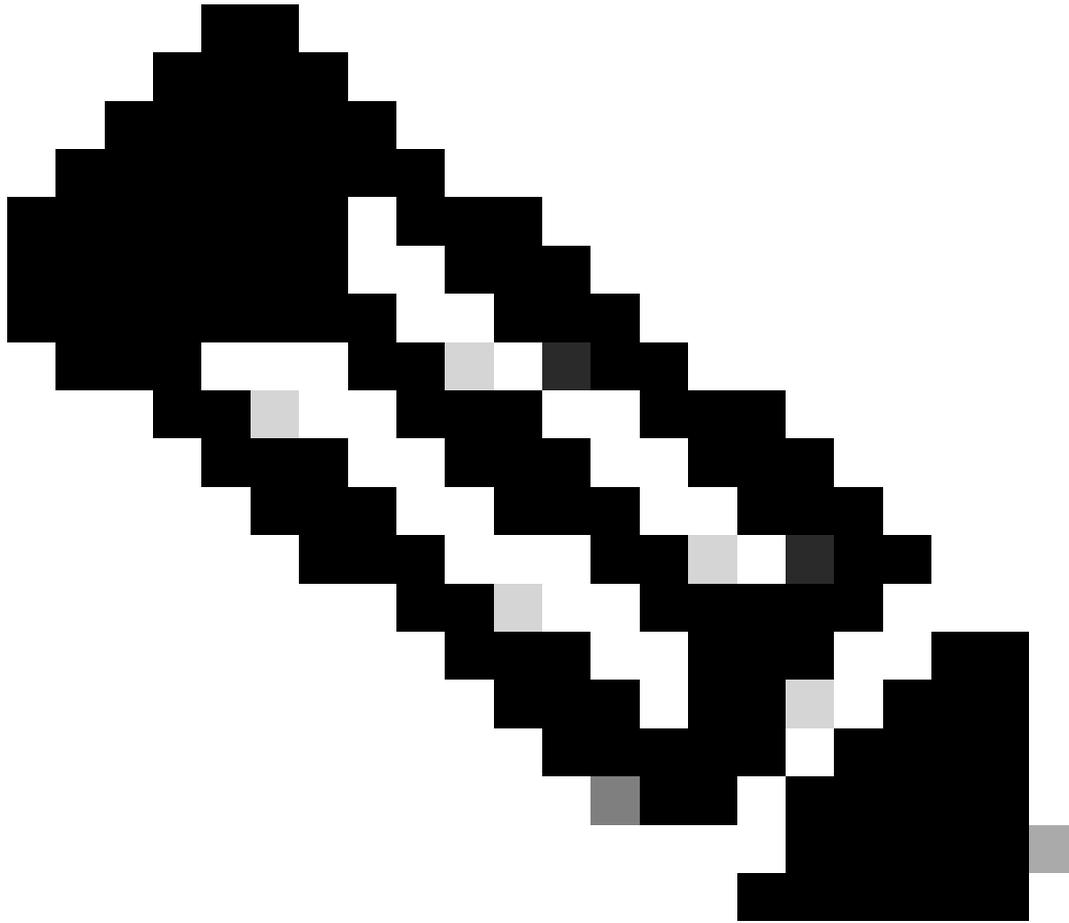
Certificate: -----BEGIN CERTIFICATE-----  
MIIDSzCCApugAwIBAgIBAgjANBgqhkiG9w0BAQsFADBYMQswCQYDVQGEwJVUzEL  
MAKGA1UECAwCQ0EFTATBgNVBACMDERlZmF1bHQgQ2l0eTEEXMBUGA1UECgw0Q2l2  
Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzAeFw0yNDYyMjE5MDU5MDhaFw0yNTAy  
MjE5MDU5MDhaMGUxCzAJBgNVBAYTAlVMTQswCQYDVQQLIDQTEEXMBUGA1UECgw0  
Q2l2Y28gQUNJIFRlYW0xDDAKBgNVBAsMA1RBQzEiMCAGA1UEAwwZZGxjLWFlaTA2  
LWFWaWxLmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB  
ALJA5N1wzE7WmBk35pTd06FwH3M2ZmIeCDw6SktDTqaMHhqDkYEK0UgG0dyRrdP

Modulus: MOD 512 MOD 1024 MOD 1536 MOD 2048

Certificate Authority: Cisco\_ACL\_Team

Private Key:

Show Usage Close Submit



**Remarque** : chaque certificat doit être conforme à un format fixe.

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

---

Cliquez sur le bouton **Envoyer**.

Étape 5. Mettre à jour le certificat de signature sur le Web

Dans la barre de menus, accédez à [Fabric](#) > [Fabric Policies](#) > [Policies](#) > [Pod](#) > [Management Access](#) > [Default](#).

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:

SSH Cipher Configuration:

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

Show Usage Reset Submit

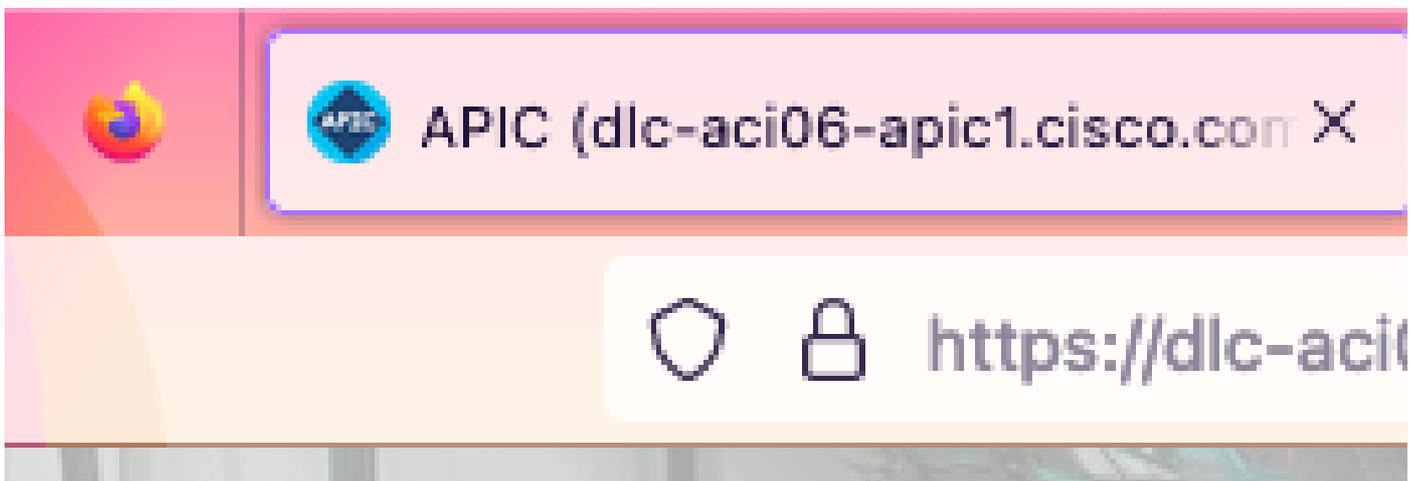
dans la liste déroulante **Admin KeyRing**, sélectionnez le KeyRing souhaité.

Cliquez sur le bouton **Envoyer**.

Après avoir cliqué sur Envoyer, une erreur se produit pour des raisons de certificat. Actualisez avec le nouveau certificat.

Vérifier

Après avoir accédé à l'interface utilisateur graphique du contrôleur APIC, ce dernier utilise le certificat signé par l'autorité de certification pour communiquer. Affichez les informations de certificat dans le navigateur afin de les vérifier.





**Remarque** : les méthodes d'affichage des certificats HTTPS dans différents navigateurs ne sont pas exactement les mêmes. Pour connaître les méthodes spécifiques, reportez-vous au guide de l'utilisateur de votre navigateur.

---

## Dépannage

Si le navigateur vous demande toujours si l'interface graphique du contrôleur APIC n'est pas approuvée, vérifiez dans le navigateur si le certificat de l'interface graphique est cohérent avec celui envoyé dans le porte-clés.

Vous devez faire confiance au **certificat racine CA** qui a émis le certificat sur votre ordinateur ou votre navigateur.



**Remarque** : le navigateur Google Chrome doit vérifier le **SAN** du certificat afin de faire confiance à ce certificat.

---

Dans les APIC qui utilisent des certificats auto-signés, des avertissements d'expiration de certificat peuvent apparaître dans de rares cas.

Recherchez le certificat dans Keyring, utilisez l'outil d'analyse de certificat afin d'analyser le certificat, et comparez-le avec le certificat utilisé dans le navigateur.

Si le certificat du porte-clés est renouvelé, créez une nouvelle stratégie d'accès à la gestion et appliquez-la.

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
- 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

Si le certificat de Keyring n'est pas renouvelé automatiquement, contactez le TAC Cisco pour obtenir de l'aide.

#### Informations connexes

- [Guide de configuration de la sécurité Cisco APIC, version 5.2\(x\)](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.