Configurer le certificat HTTPS de l'interface graphique ACI APIC

Table des matières

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

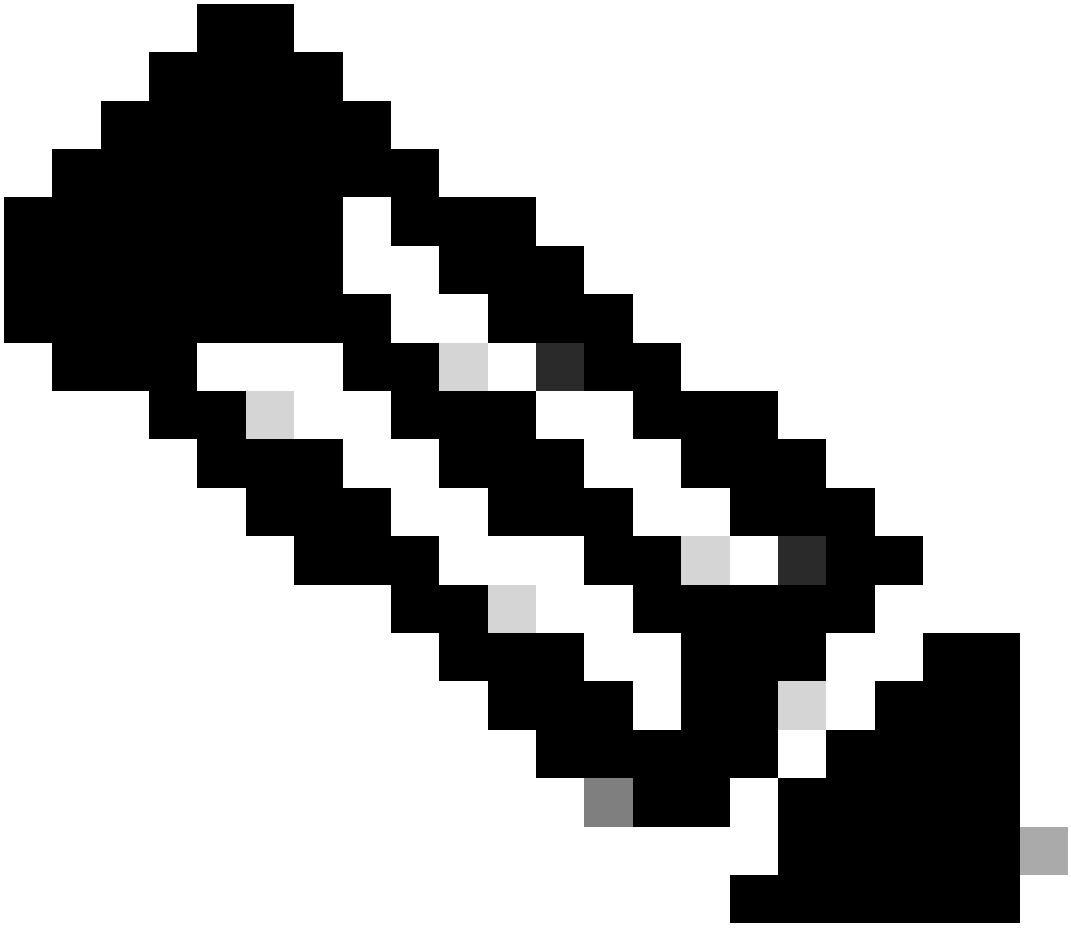
Une fois le périphérique initialisé, il utilise le certificat auto-signé comme certificat SSL pour HTTPS. Le certificat auto-signé est valide pendant 1 000 jours.

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

Configurations

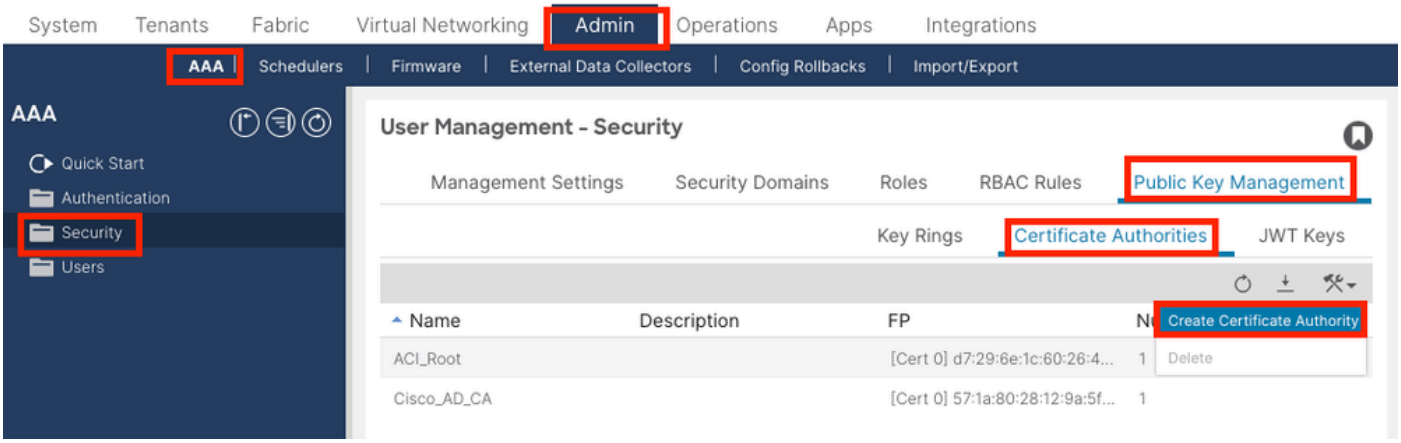
Le périphérique utilise un certificat auto-signé. Lorsque vous accédez à l'interface graphique utilisateur du contrôleur APIC, le navigateur vous demande si le certificat n'est pas digne de confiance. Afin de résoudre ce problème, ce document utilise une autorité de certification approuvée afin de signer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

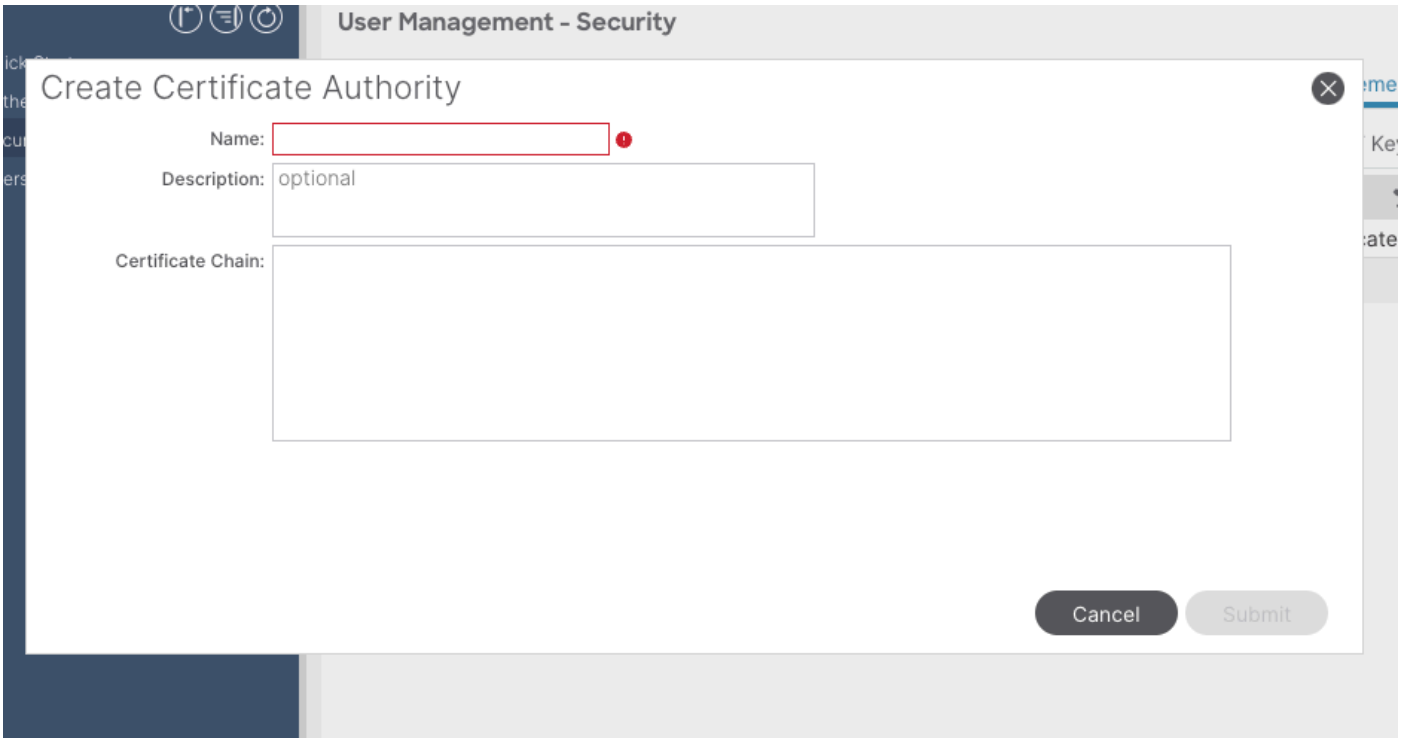
Étape 1. Importer le certificat racine de l'autorité de certification ou le certificat intermédiaire



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.





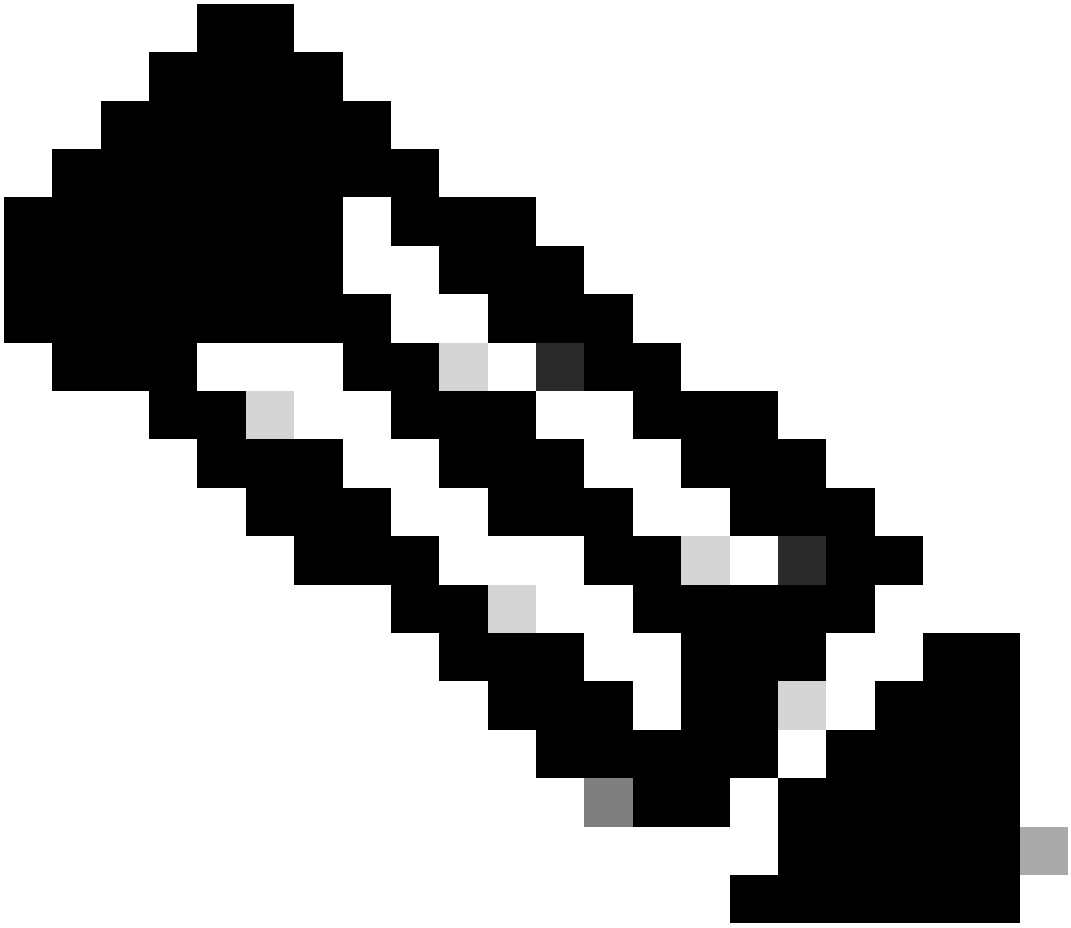
Nom : **obligatoire**.

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.



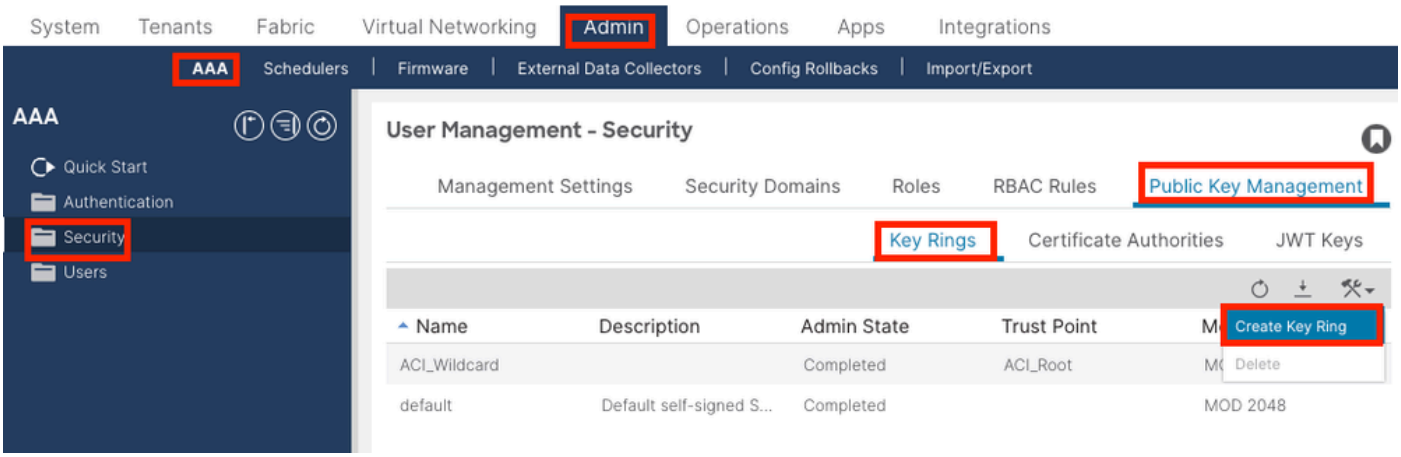
Remarque : chaque certificat doit être conforme à un format fixe.

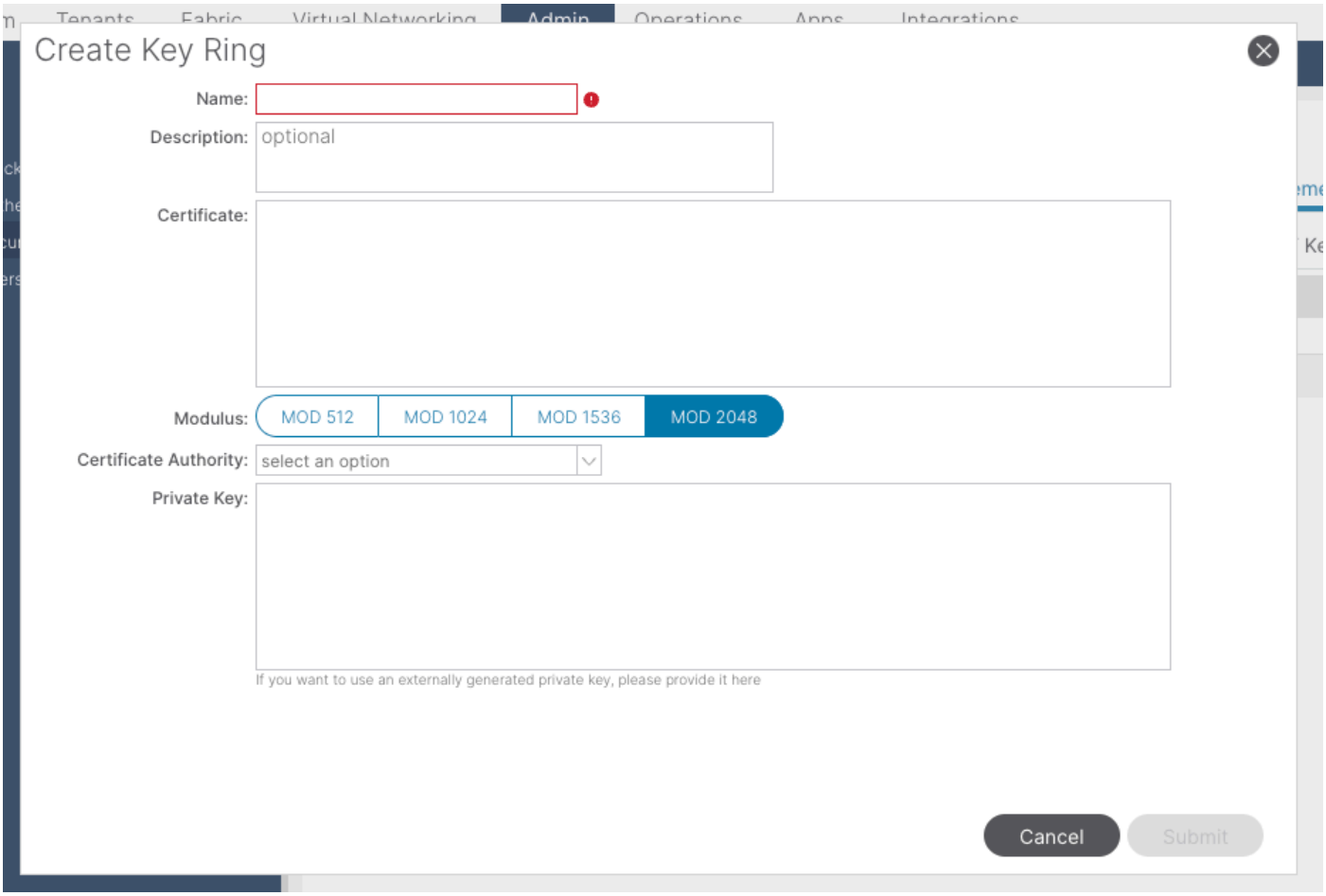
-----BEGIN CERTIFICATE----- INTER-CA-2 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- INTER-CA-1 CERTIFICATE CONTENT HERE -----END CERTIFICATE----- -----BEGIN CERTIFICATE----- ROOT-CA CERTIFICATE CONTENT HERE -----END CERTIFICATE-----

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.





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

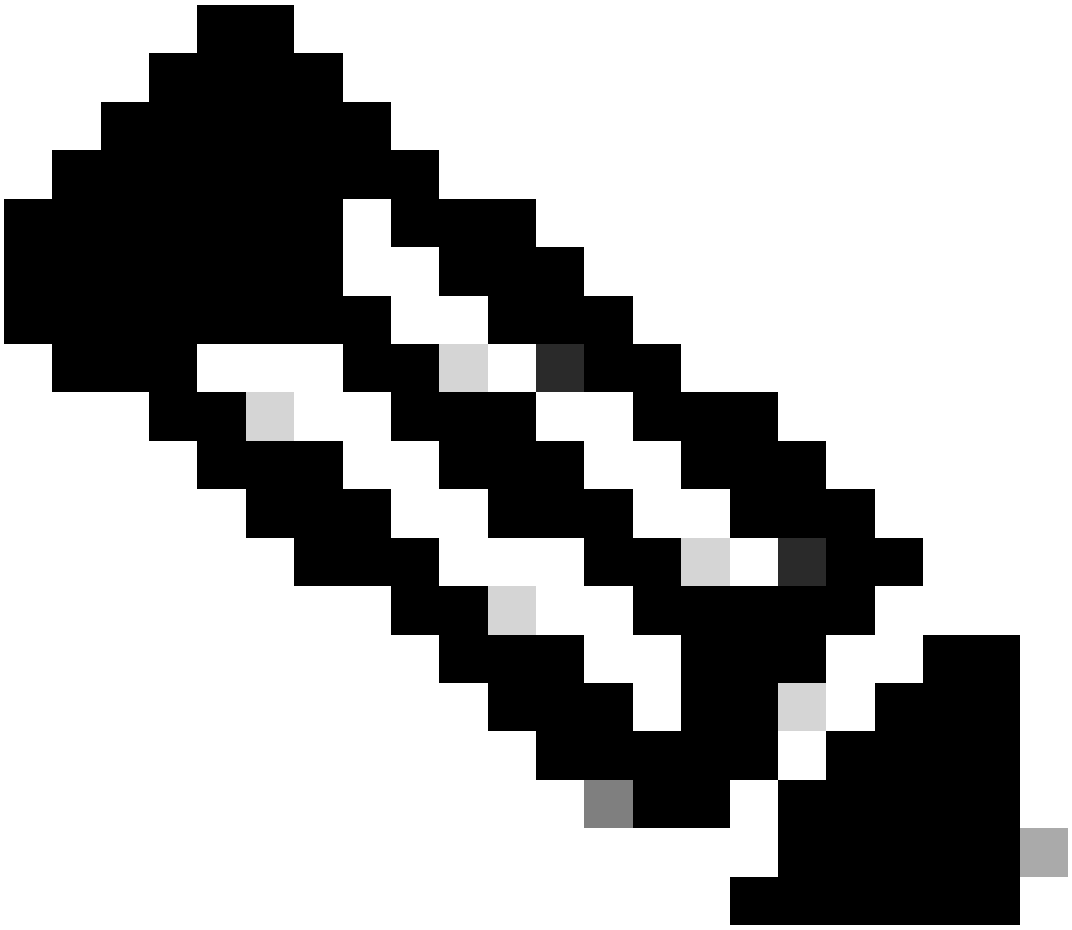
Certificat **: n'ajoutez** aucun contenu si vous générez une demande de signature de certificat (CSR) à l'aide du contrôleur APIC Cisco via l'anneau de clés. Vous pouvez également ajouter le contenu du certificat signé si vous en avez déjà un signé par l'autorité de certification à partir des étapes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

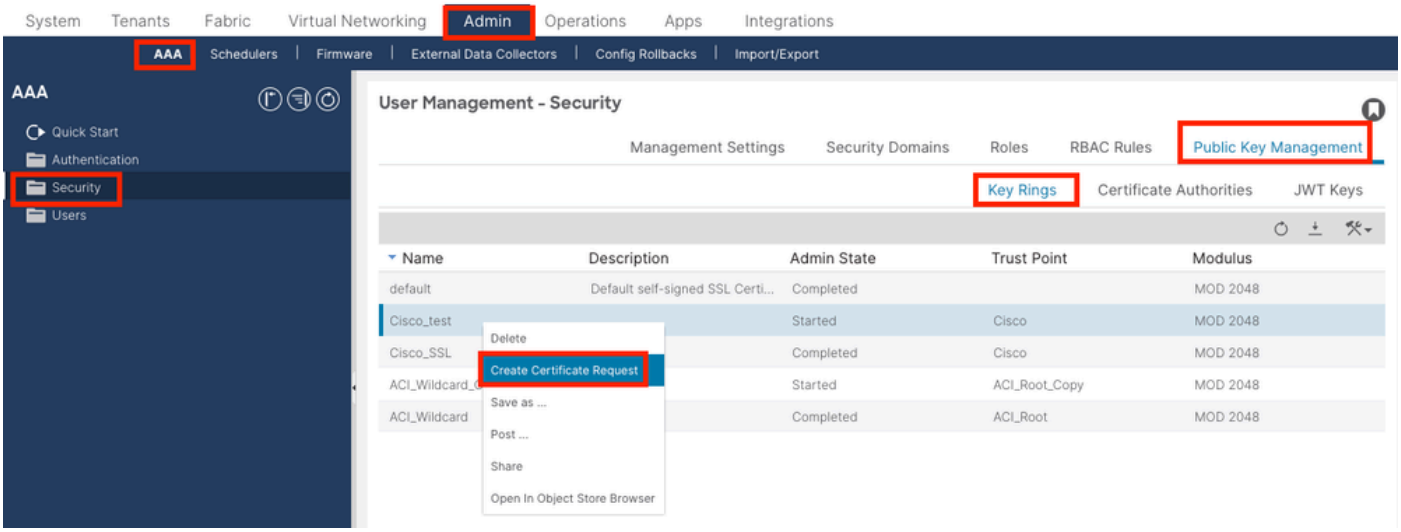


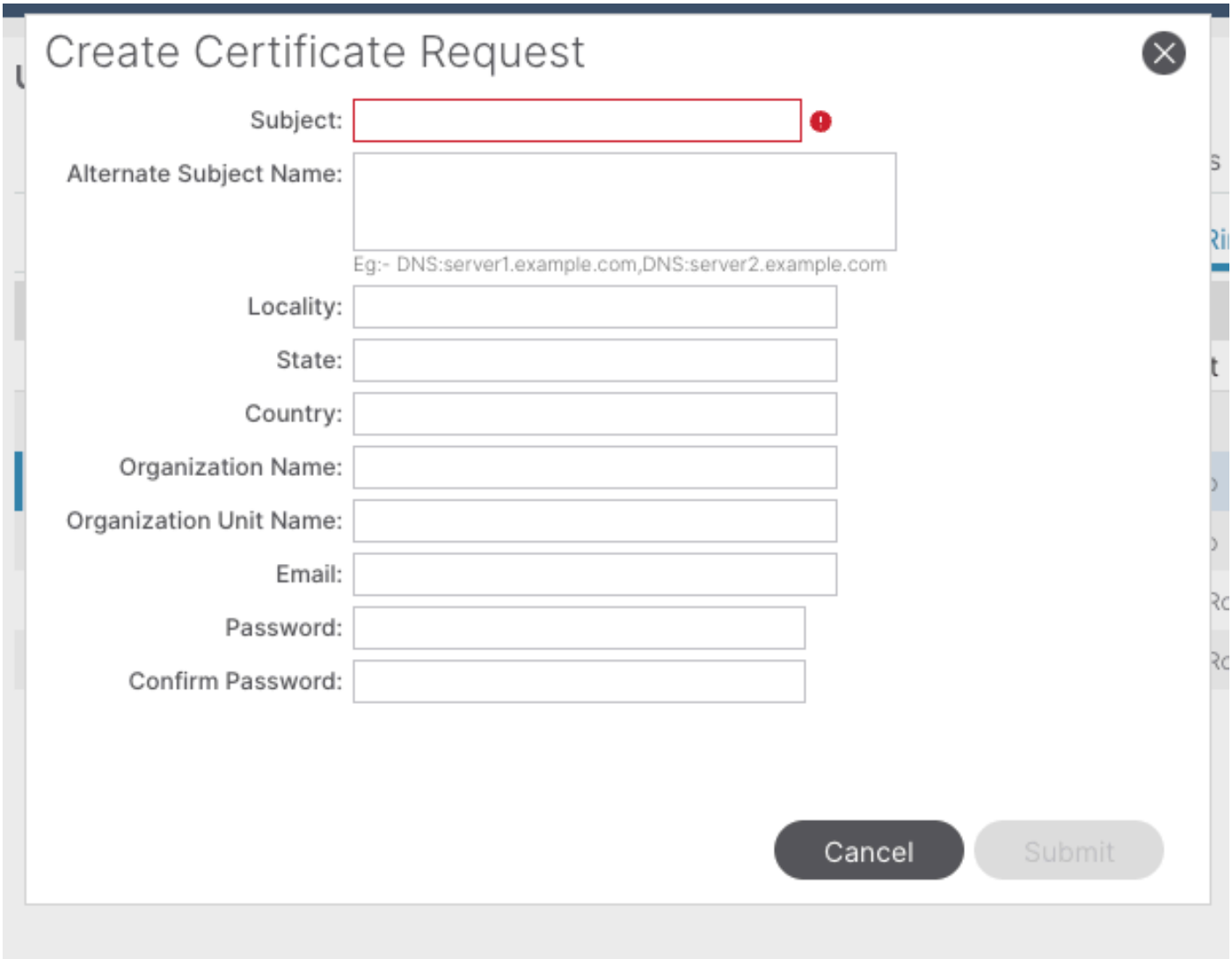
> **Remarque** : si vous ne souhaitez pas utiliser la clé privée et le CSR générés par le système et utiliser une clé privée et un certificat personnalisés, il vous suffit de remplir quatre éléments : Nom, Certificat, Autorité de certification et Clé privée. Après l'envoi, vous n'avez qu'à effectuer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



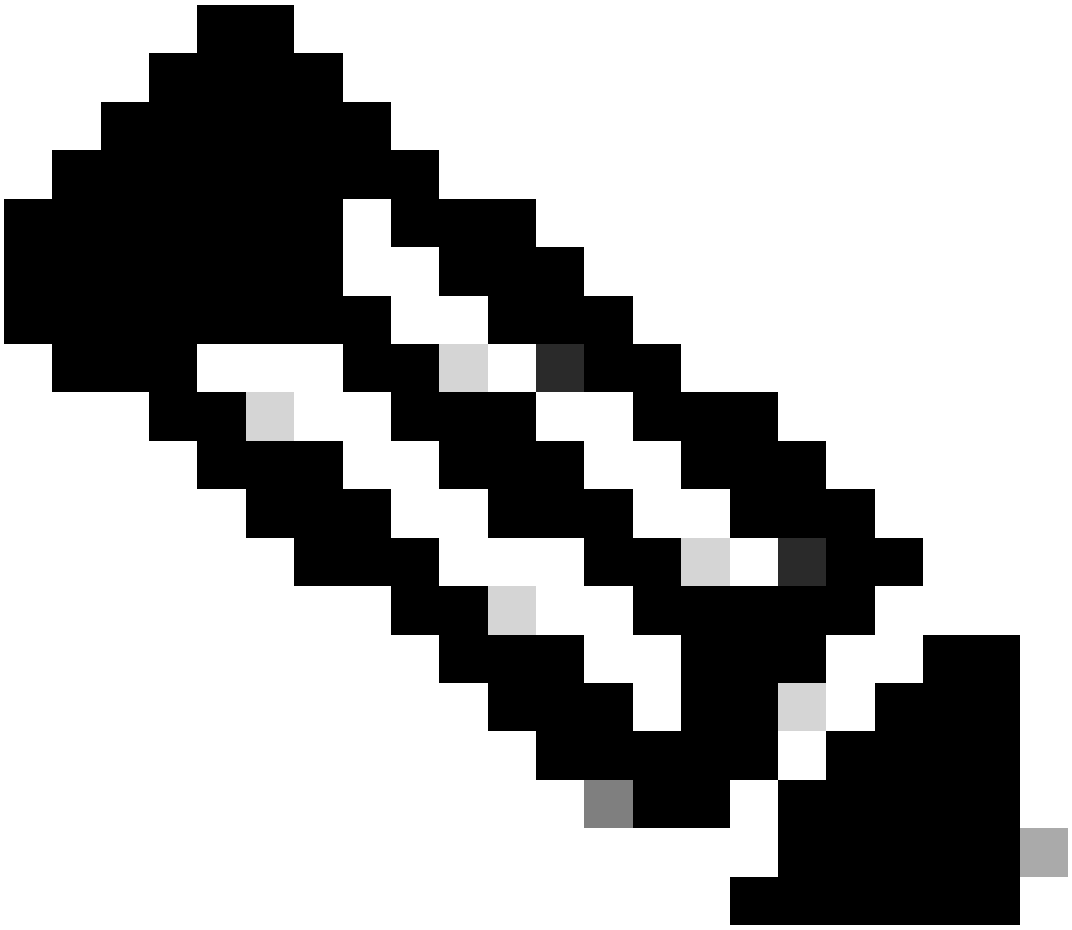


Objet : **obligatoire**. Saisissez le nom commun (CN) du CSR.

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.

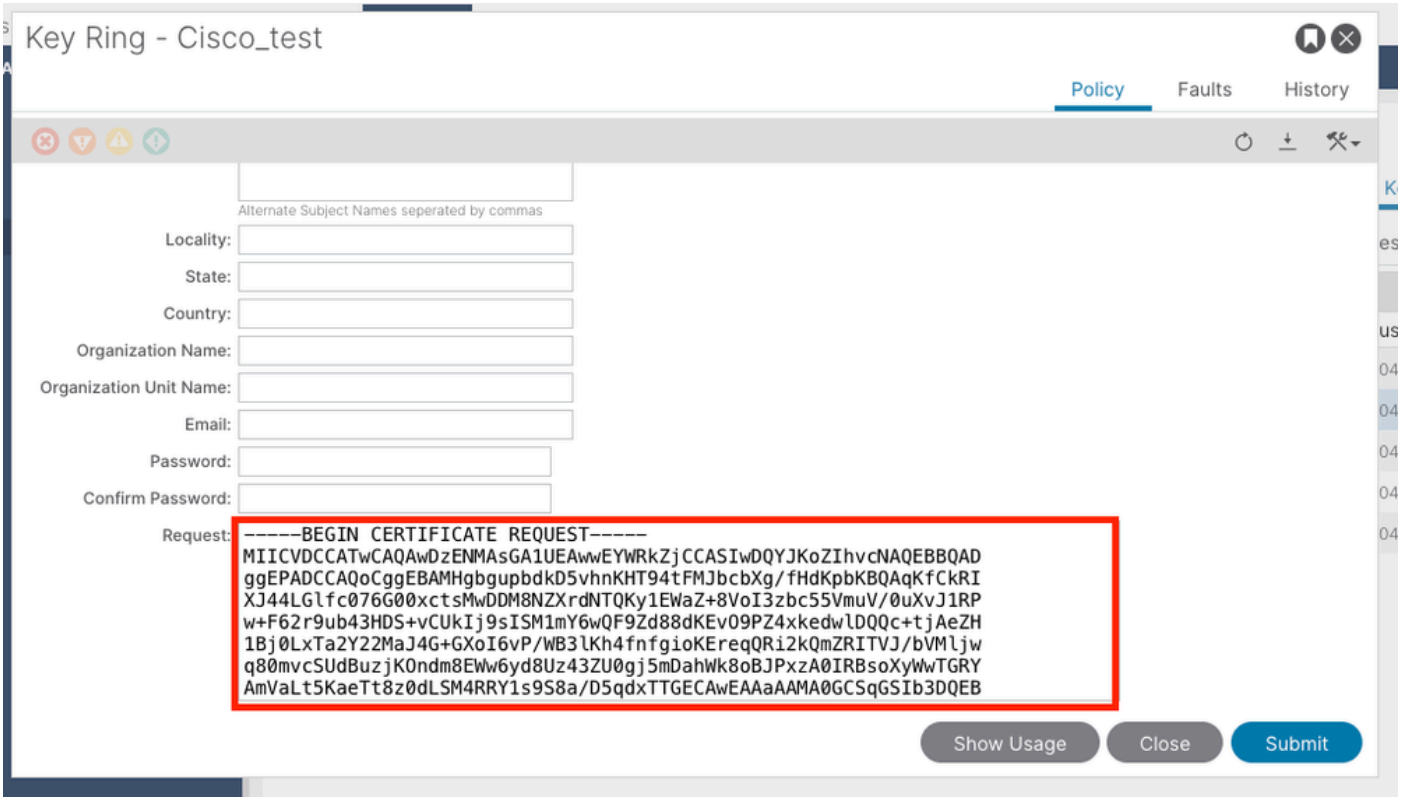
Remplissez les champs restants en fonction des exigences de l'organisme de certification que vous demandez afin de délivrer le certificat.

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.

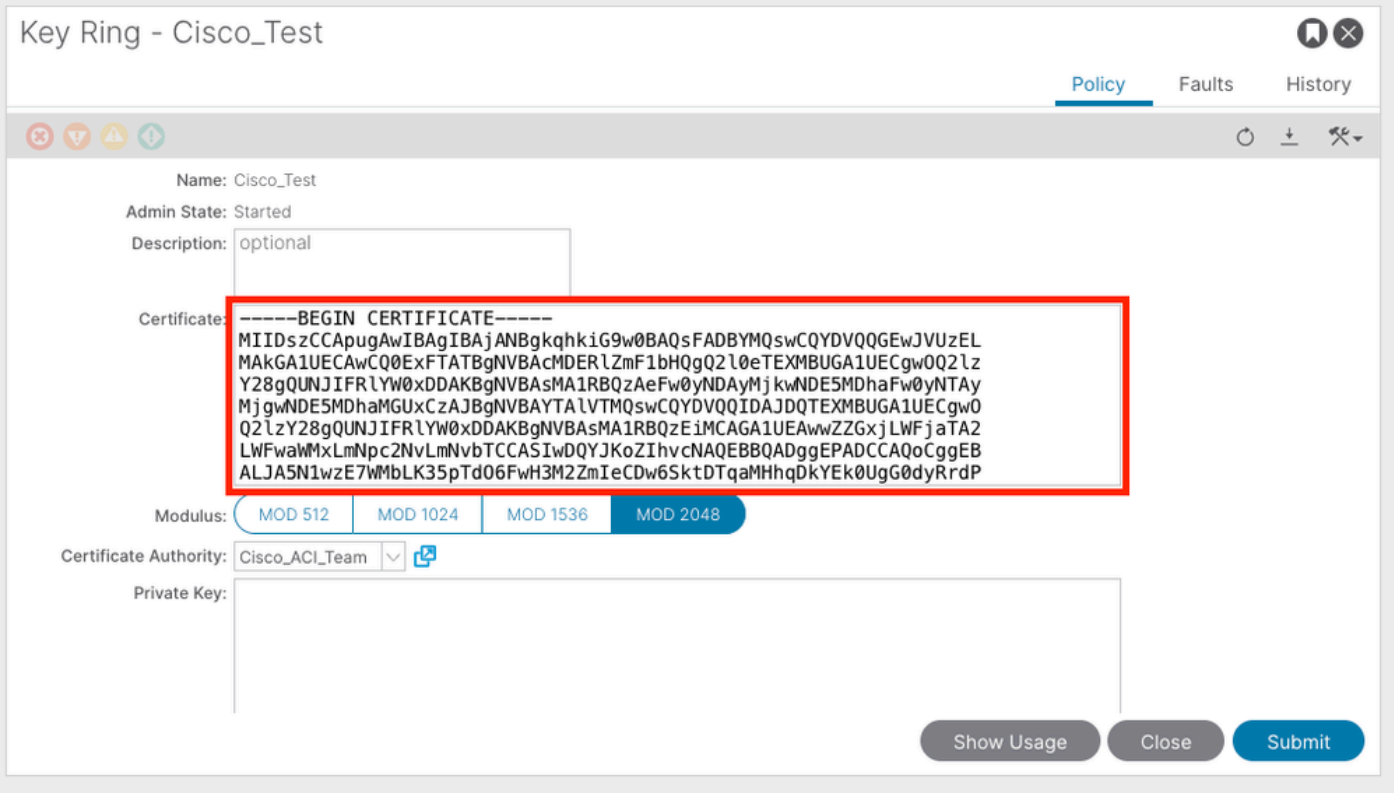
Double-cliquez sur le nom de votre **Key Ring** de création et recherchez l'option **Request**. Le contenu de la demande est le CSR.

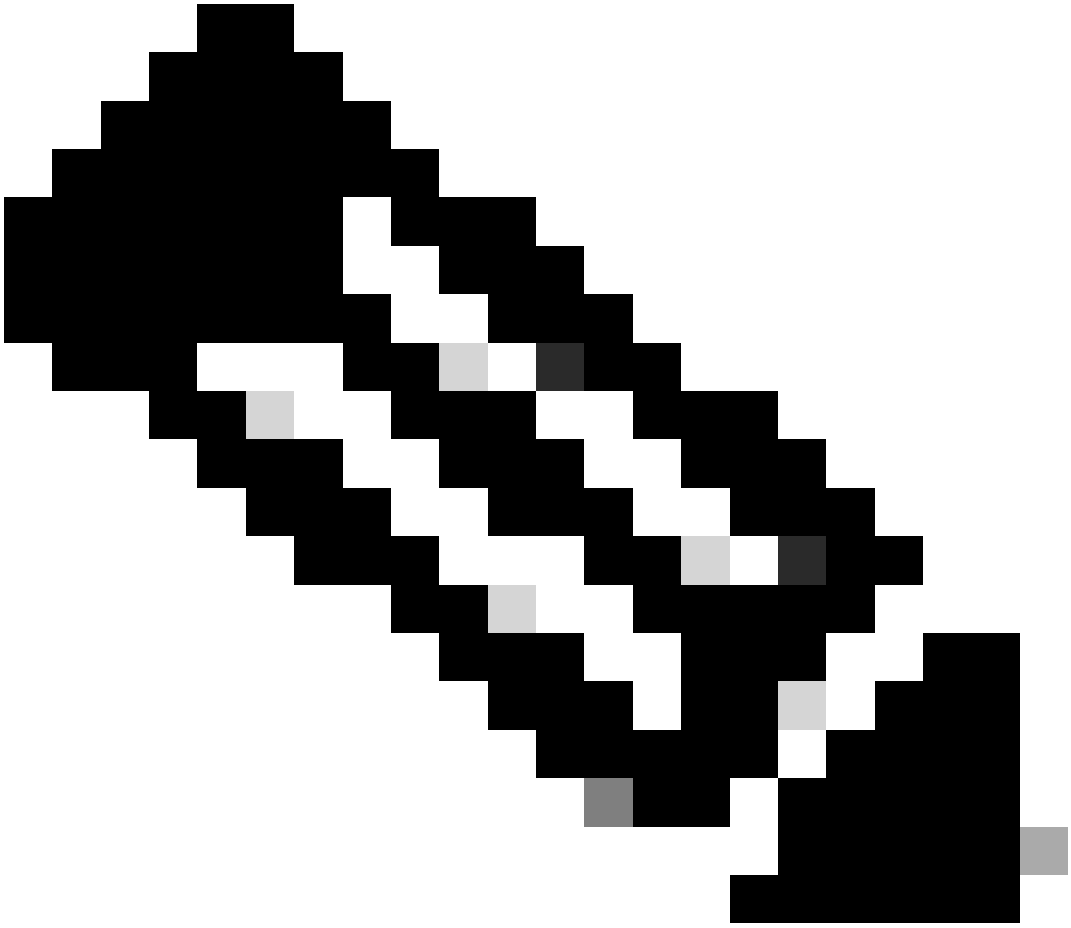


Copiez tout le contenu de la demande et envoyez-la à votre autorité de certification.

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.


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



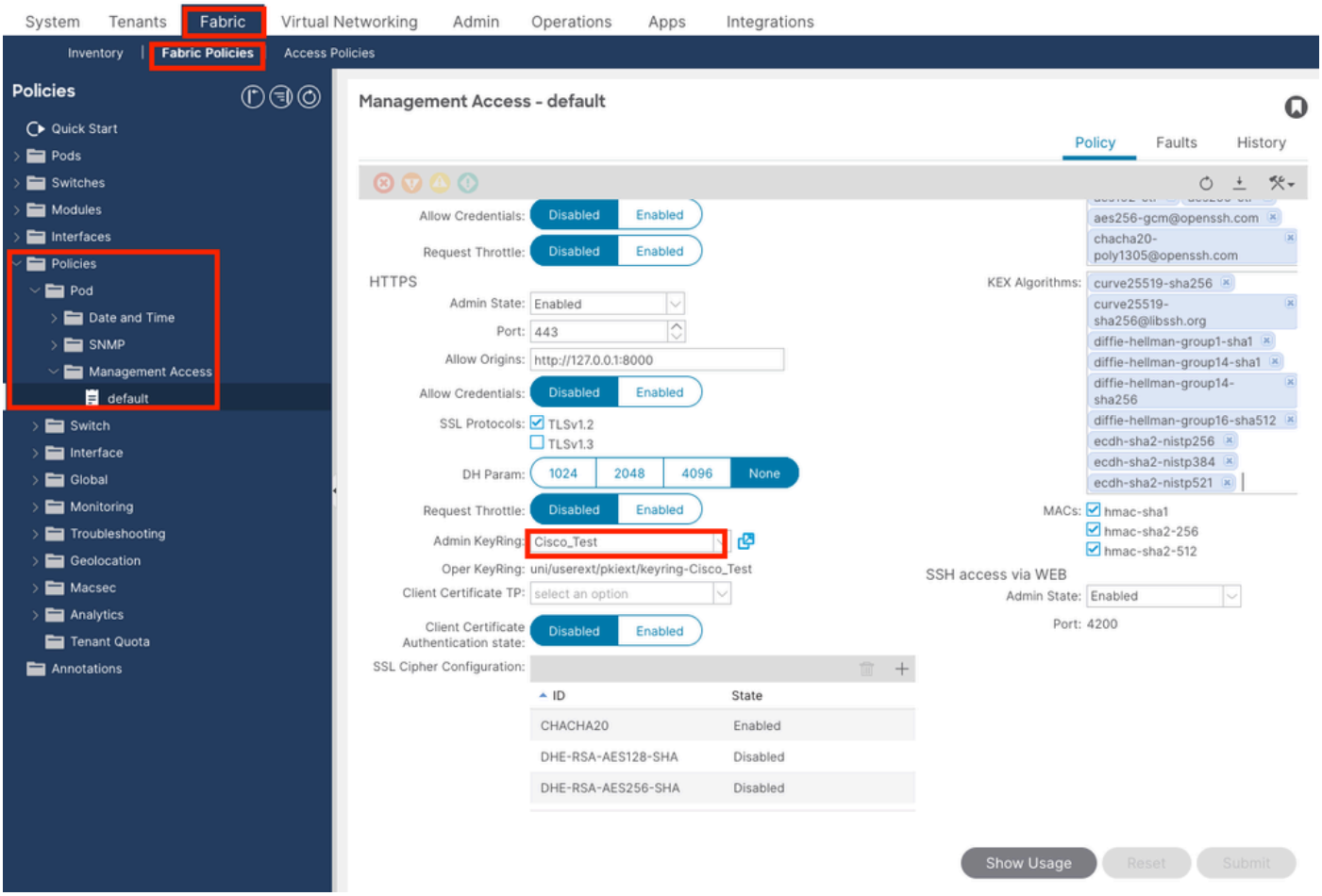
Remarque : chaque certificat doit être conforme à un format fixe.

-----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.



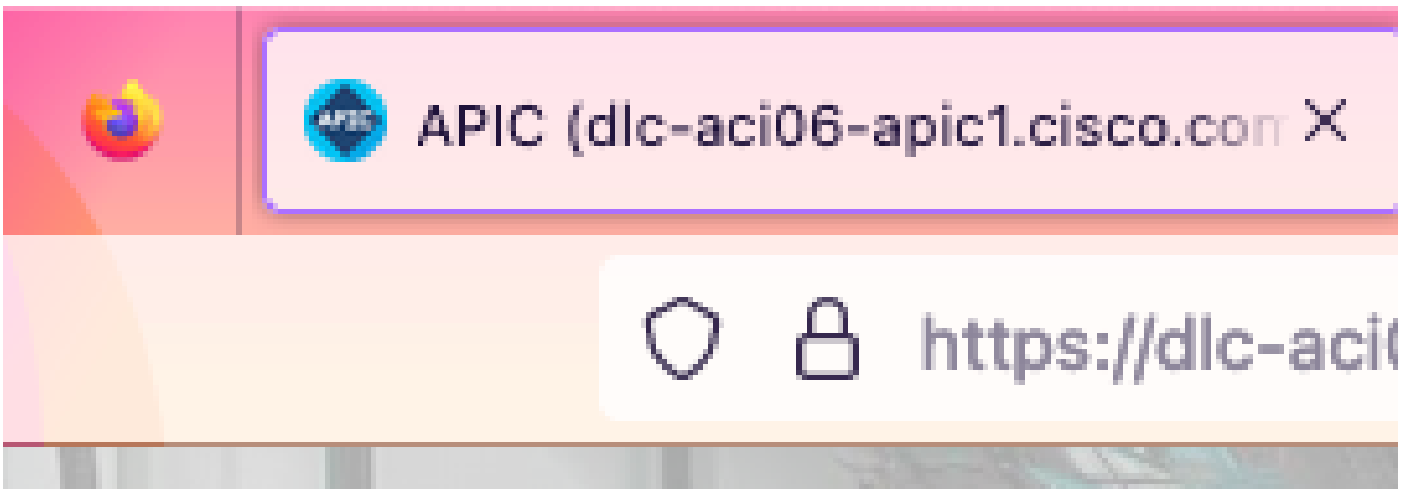
dans la liste déroulante **Admin KeyRing**, sélectionnez le KeyRing souhaité.

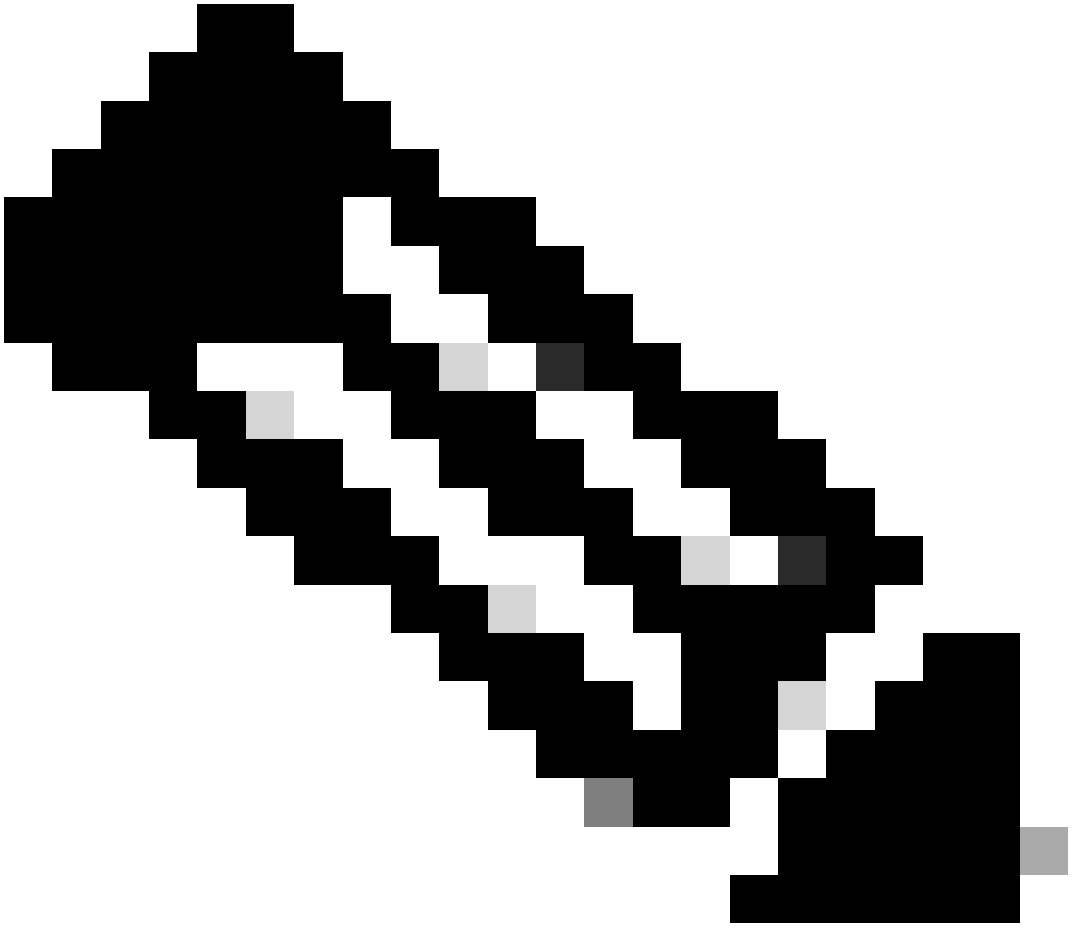
Cliquez sur le bouton **Envoyer**.

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.

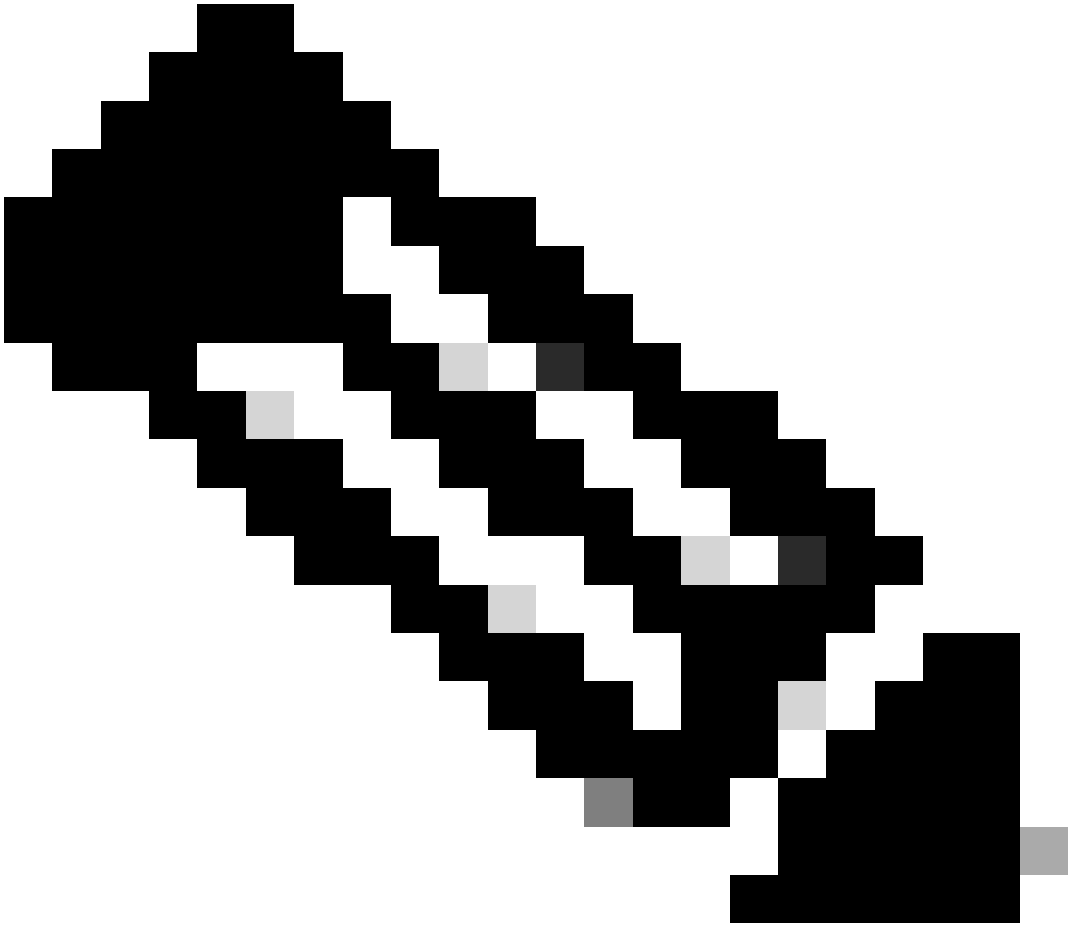




Remarque : les méthodes d'affichage des certificats HTTPS dans différents navigateurs ne sont pas exactement les mêmes. Pour connaître les méthodes spécifiques, reportez-vous au guide de l'utilisateur de votre navigateur.

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.

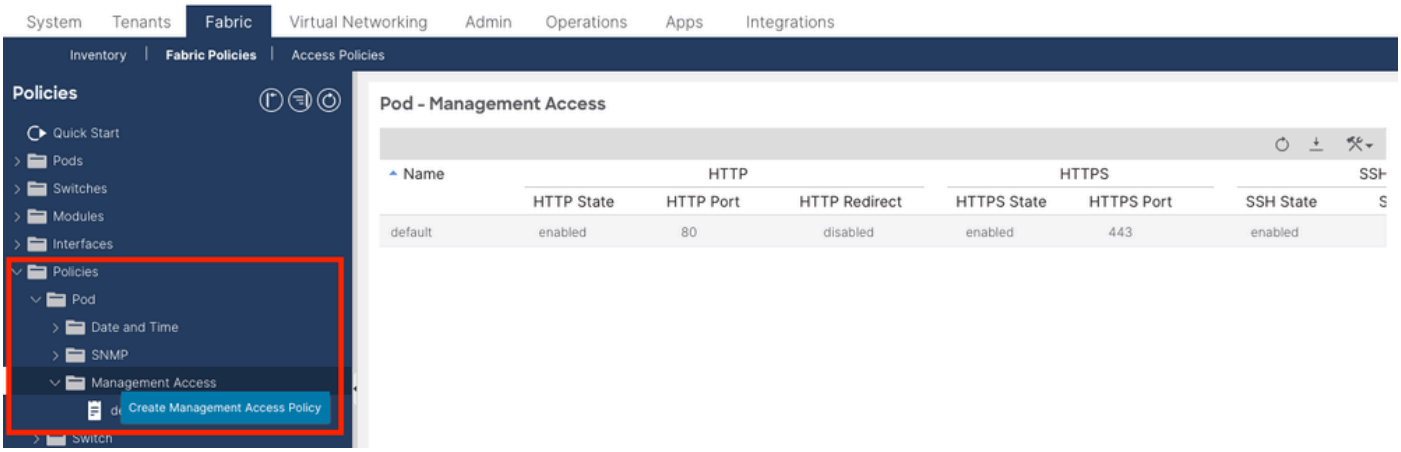


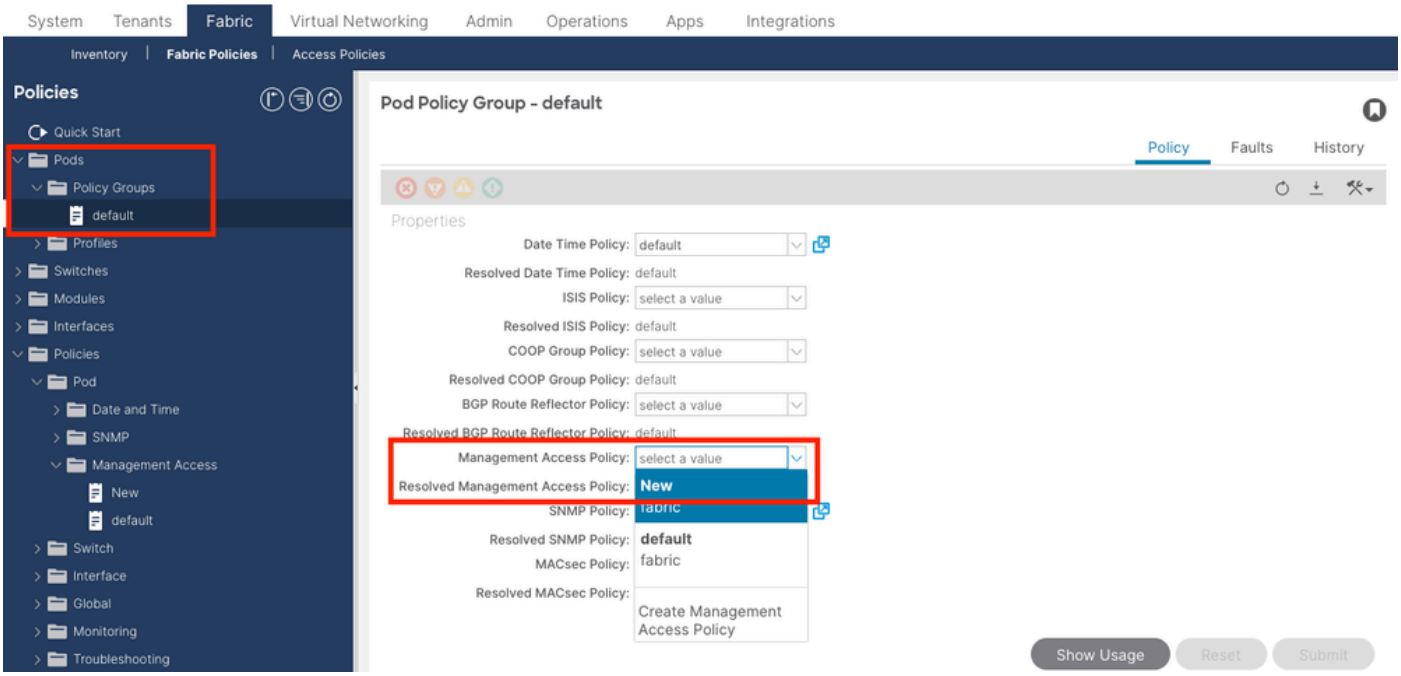
Remarque : le navigateur Google Chrome doit vérifier le **SAN** du certificat afin de faire confiance à ce certificat.

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.





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.