Configuration de l'inscription de certificat avec le protocole ACME sur la défense pare-feu sécurisée gérée par FMC

Introduction

Ce document décrit le processus d'inscription d'un certificat TLS (Transport Layer Security) via le protocole ACME (Automated Certificate Management Environment) sur la plate-forme Secure Firewall Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Processus d'inscription manuelle des certificats et principes fondamentaux du protocole SSL (Secure Sockets Layer).
- Concepts d’authentification de base pour les VPN d’accès à distance.
- Expérience des autorités de certification (AC).

Composants utilisés

- Cisco FTDv version 10.0.0-35.
- Cisco FMC version 10.0.0-35.
- Serveur d'autorité de certification (CA) qui prend en charge le protocole ACME.

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.

Exigences et limitations

Les conditions et contraintes actuelles pour l'inscription d'ACME sur Secure Firewall FTD sont les suivantes :

- Pris en charge sur FTD et FMC versions 10.0.0 et ultérieures.
- ACME ne permet pas l'émission de certificats génériques ; chaque demande de certificat doit spécifier un nom de domaine précis.
- Chaque point de confiance inscrit via ACME est limité à une seule interface, de sorte que les certificats obtenus via ACME ne peuvent pas être partagés entre plusieurs interfaces.
- Les paires de clés sont générées automatiquement et sont uniques pour chaque certificat inscrit via ACME, ce qui empêche la réutilisation des clés et renforce la sécurité.

Considérations de rétrogradation

Lors de la mise à niveau vers une version FTD de pare-feu sécurisé qui ne prend pas en charge l'inscription ACME (version 7.7 ou antérieure) :

- Toutes les configurations de point de confiance liées à ACME introduites dans la version 10.0.0 ou ultérieure sont perdues.
- Les certificats inscrits via ACME sont toujours accessibles ; cependant, leurs clés privées se dissocient après le premier enregistrement et redémarrent après la rétrogradation.

Si une rétrogradation est nécessaire, utilisez la solution de contournement recommandée :

- Avant la rétrogradation, exportez les certificats ACME au format PKCS12.
- Avant de rétrograder, supprimez la configuration du point de confiance ACME.
- Après la rétrogradation, importez le certificat PKCS12. Le point de confiance importé reste valide jusqu'à l'expiration du certificat émis par ACME.

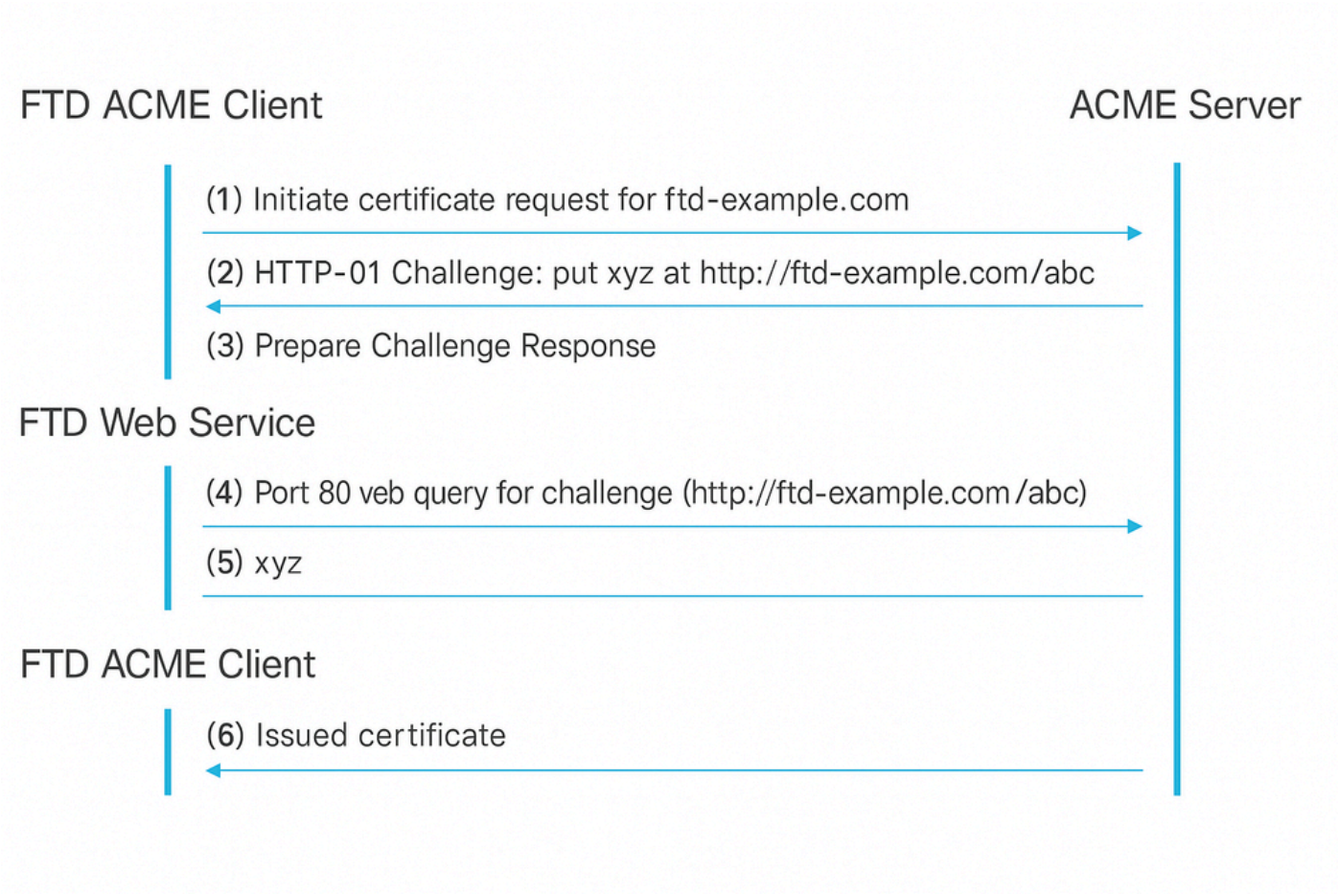
Informations générales

Le protocole ACME vise à simplifier la gestion des certificats TLS pour les administrateurs réseau. Grâce à ACME, les administrateurs peuvent automatiser les tâches d’acquisition et de renouvellement des certificats TLS. Cette automatisation est particulièrement utile lorsque vous travaillez avec des autorités de certification (CA) telles que Let's Encrypt, qui fournissent des certificats gratuits, automatisés et accessibles au public via le protocole ACME.ACME facilite l'émission de certificats de validation de domaine (DV). Ces certificats vérifient que le demandeur de certificat a le contrôle sur les domaines spécifiés. La validation s'effectue généralement par le biais d'un processus de demande de confirmation basé sur HTTP, dans lequel le demandeur place un fichier désigné sur son serveur Web. L'autorité de certification accède ensuite à ce fichier via le serveur HTTP du domaine pour confirmer le contrôle du domaine. La réussite de ce défi

permet à l’autorité de certification d’émettre le certificat DV.

Le processus d'inscription comprend les étapes suivantes :

1. Lancer la demande de certificat : Le client envoie une demande de certificat au serveur ACME, en spécifiant le ou les domaines pour lesquels le certificat est nécessaire.
2. Réception de la demande HTTP-01 : Le serveur ACME répond par une demande HTTP-01 contenant un jeton unique que le client doit utiliser pour prouver la propriété du domaine.
3. Préparer la réponse au défi :
    1. Le client génère une autorisation de clé en combinant le jeton du serveur ACME avec sa clé de compte.
    2. Le client configure son serveur Web pour servir cette autorisation de clé à un chemin d'URL spécifique.
4. Le serveur ACME relève le défi : Le serveur ACME effectue une requête HTTP GET vers l'URL fournie pour obtenir l'autorisation de clé.
5. Le serveur ACME vérifie la propriété : Le serveur compare l'autorisation de clé récupérée à la valeur attendue pour vérifier le contrôle du client sur le domaine.
6. Émettre le certificat : Une fois la validation réussie, le serveur ACME émet le certificat SSL/TLS au client.



Flux d'authentification HTTP-01 d'inscription ACME.

Les principaux avantages de l'utilisation du protocole ACME pour l'inscription de certificats TLS sur Secure Firewall FTD sont les suivants :

- Automatisation de la gestion des certificats : ACME simplifie le processus d'obtention et de maintenance des certificats de domaine TLS pour les interfaces TLS FTD Secure Firewall, réduisant ainsi considérablement les tâches administratives manuelles.
- Renouvellement automatique des certificats : Avec les points de confiance compatibles ACME, les certificats sont automatiquement renouvelés à l'approche de l'expiration, ce qui réduit le besoin d'une intervention administrative continue.
- Assurance de sécurité continue : Cette automatisation garantit que les certificats restent valides sans interruption, ce qui évite les expirations de certificats inattendues et garantit la sécurité des communications.

Ensemble, ces avantages améliorent l'efficacité opérationnelle et la sécurité des déploiements Secure Firewall FTD.

Configurer

Configuration des prérequis

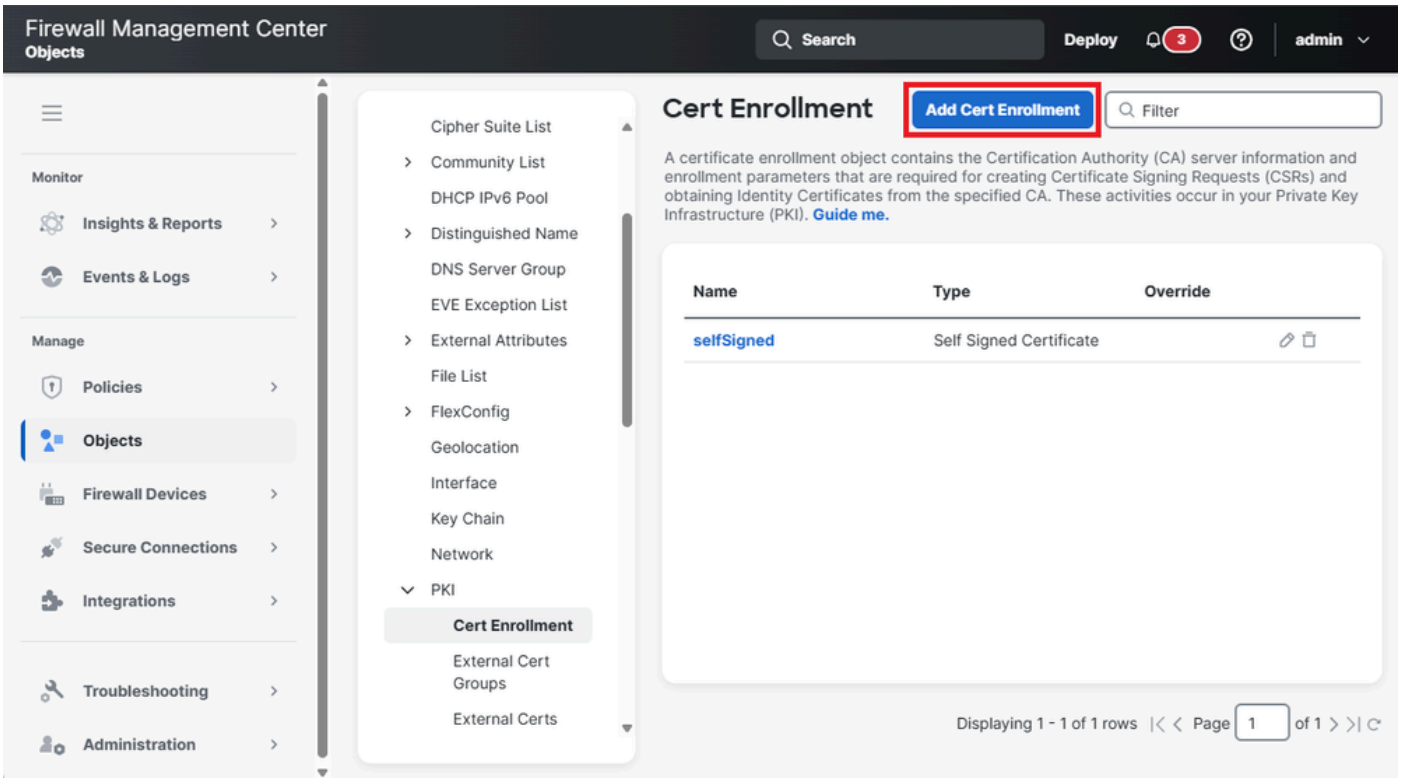
Avant de lancer le processus d'inscription ACME, assurez-vous que les conditions suivantes sont remplies :

1. Nom de domaine résoluble : le nom de domaine pour lequel vous demandez un certificat doit pouvoir être résolu par le serveur ACME. Cela garantit que le serveur peut vérifier la propriété du domaine.
2. Pare-feu sécurisé Accès au serveur ACME : le pare-feu sécurisé doit être en mesure d'accéder au serveur ACME via l'une de ses interfaces. Cet accès n'a pas besoin d'être via l'interface pour laquelle le certificat est demandé.
3. Disponibilité du port TCP 80 : autorise le port TCP 80 du serveur AC ACME vers l'interface qui correspond au nom de domaine. Cette opération est nécessaire pendant le processus d'échange ACME pour effectuer le défi HTTP-01.

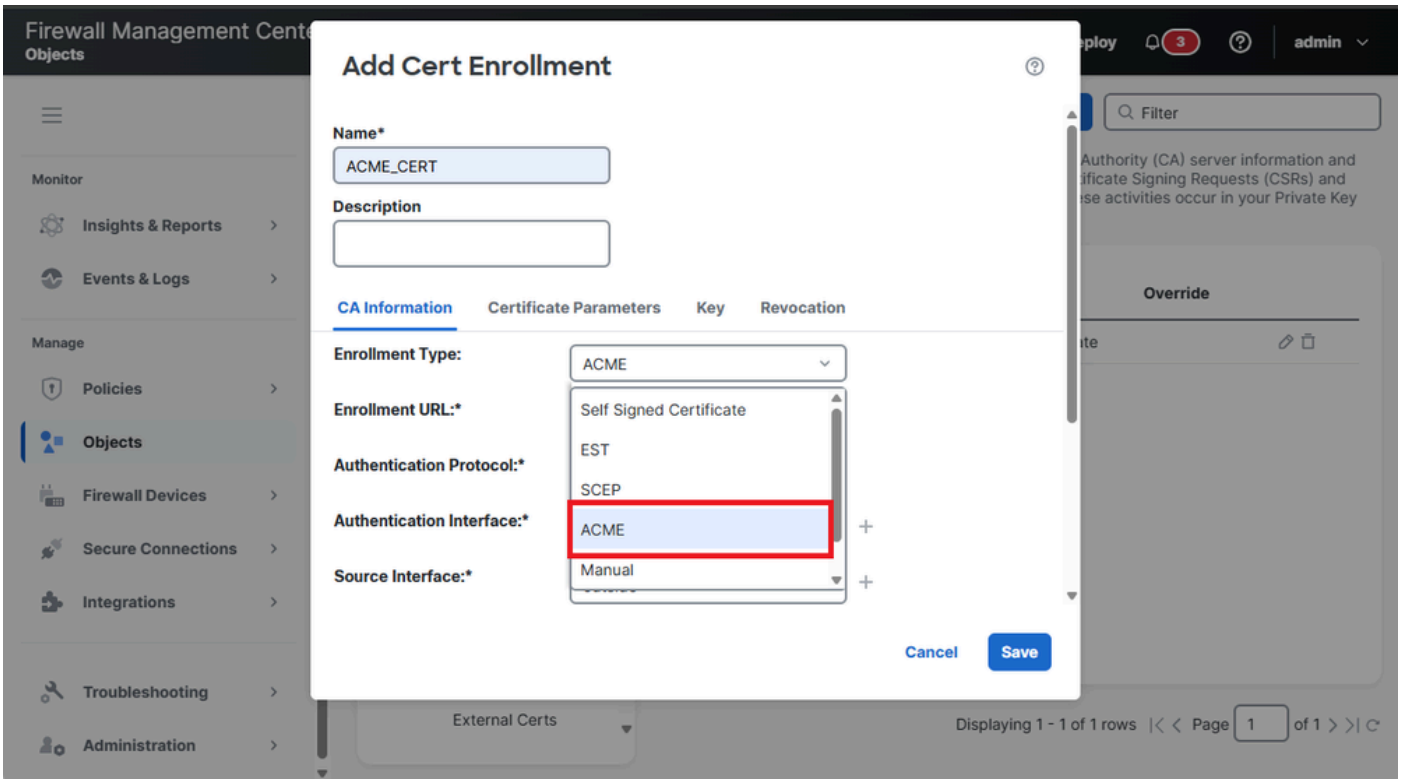
Remarque : Pendant la période où le port 80 est ouvert, seules les données de défi ACME sont accessibles.

Création d'objet Inscription de certificat ACME

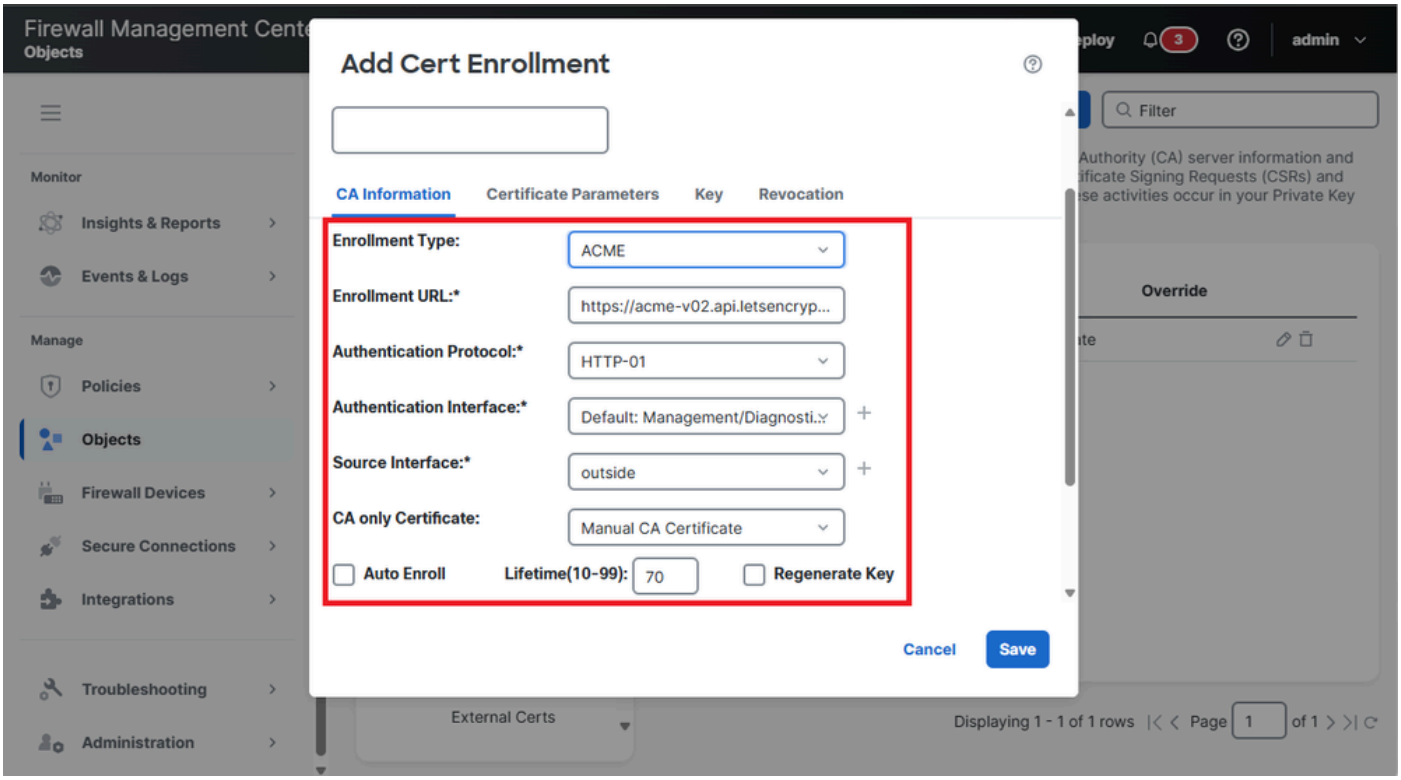
1. Accédez à Objets > ICP > Inscription de certificat et cliquez sur Ajouter inscription de certificat pour commencer le processus de configuration.



2. L'option d'inscription ACME est répertoriée dans le menu déroulant avec d'autres méthodes d'inscription. Sélectionnez ACME dans la liste déroulante Enrollment Type pour continuer.



3. Les options de configuration des paramètres de certificat s'affichent, renseignez les champs avec les informations appropriées.



- URL d'inscription : Il s'agit de l'adresse du serveur ACME (telle que Let's Encrypt) utilisée pour demander et récupérer des certificats.
- Protocole d'authentification : Indique la méthode utilisée pour vérifier la propriété du

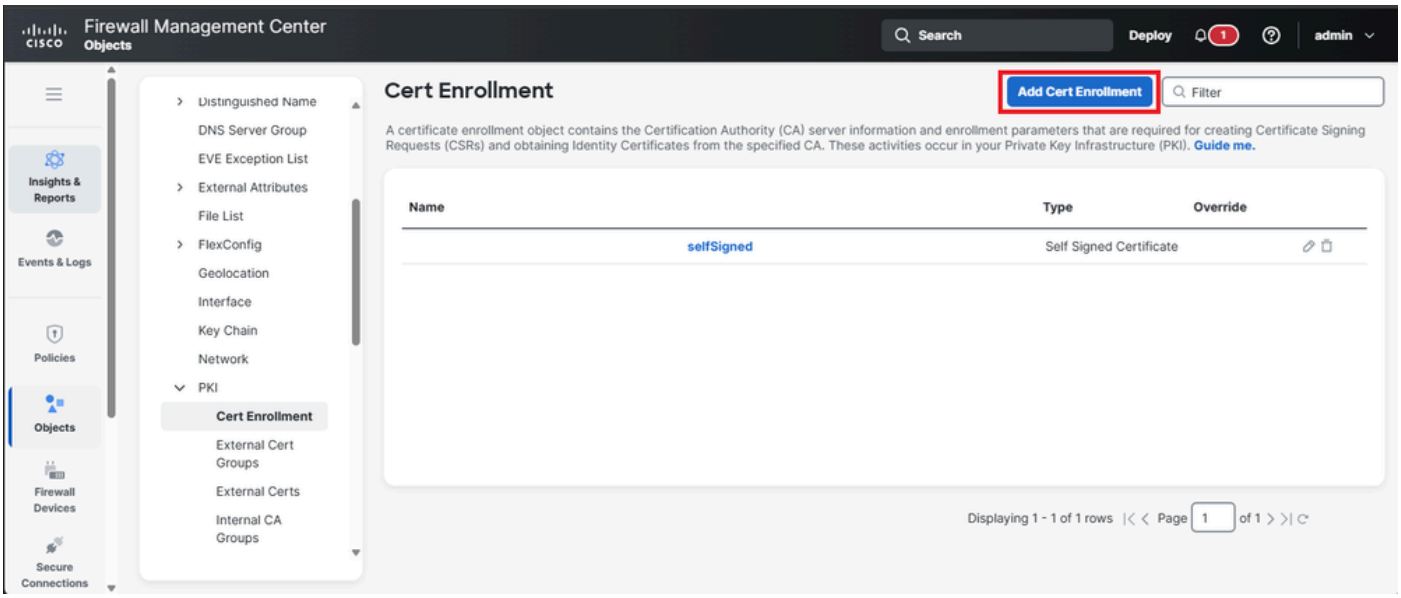
domaine. Le protocole pris en charge pour les défis ACME est HTTP-01.

- Interface d'authentification : Interface réseau sur le périphérique FTD qui reçoit le défi HTTP-01 du serveur ACME.
- Certificat CA uniquement : Vous devez choisir un certificat d'une autorité de certification (CA) pour faire confiance au serveur ACME.

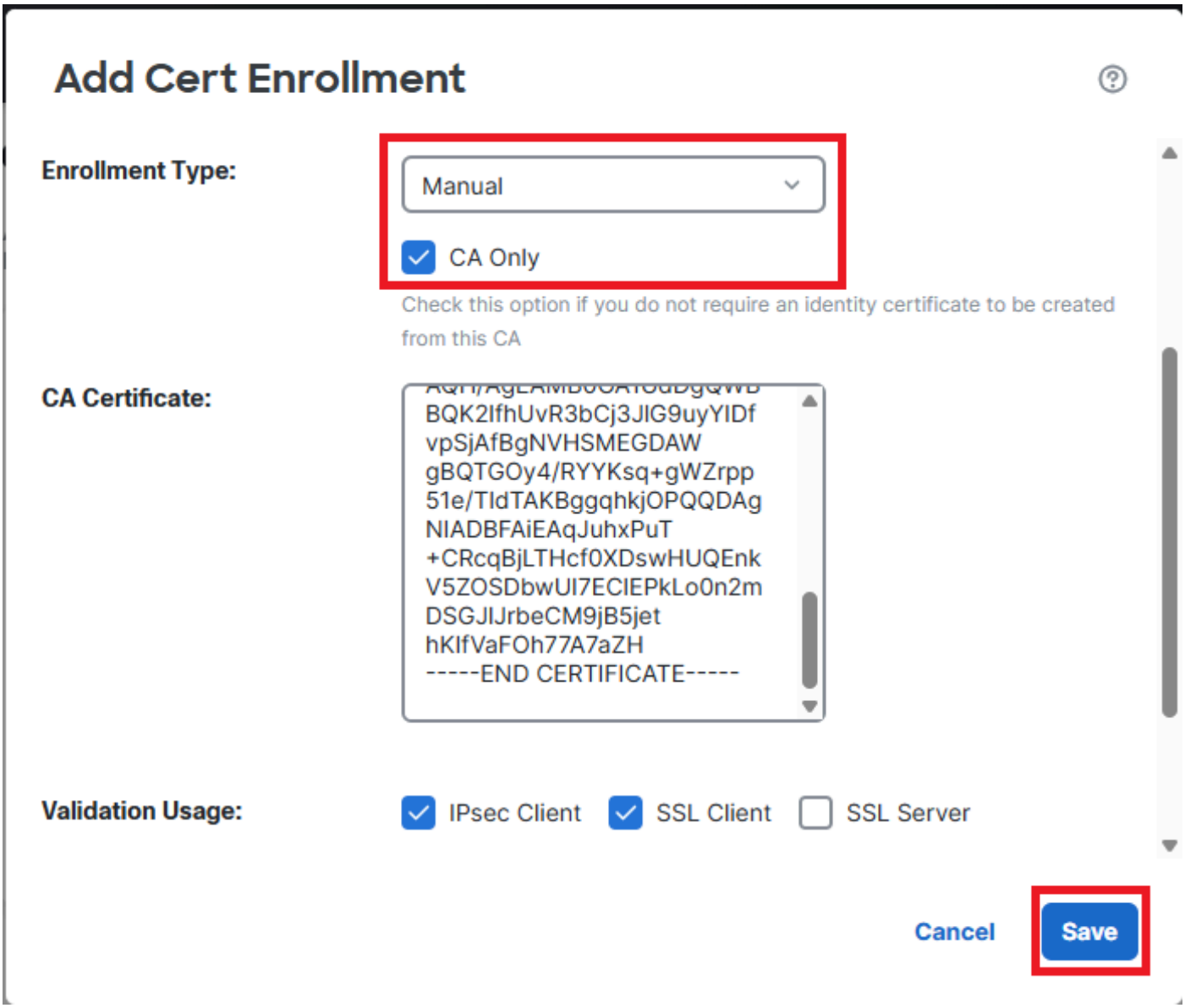
Remarque : Par défaut, il pointe vers l'URL du service public Let's Encrypt : https://acme-v02.api.letsencrypt.org/directory.

---

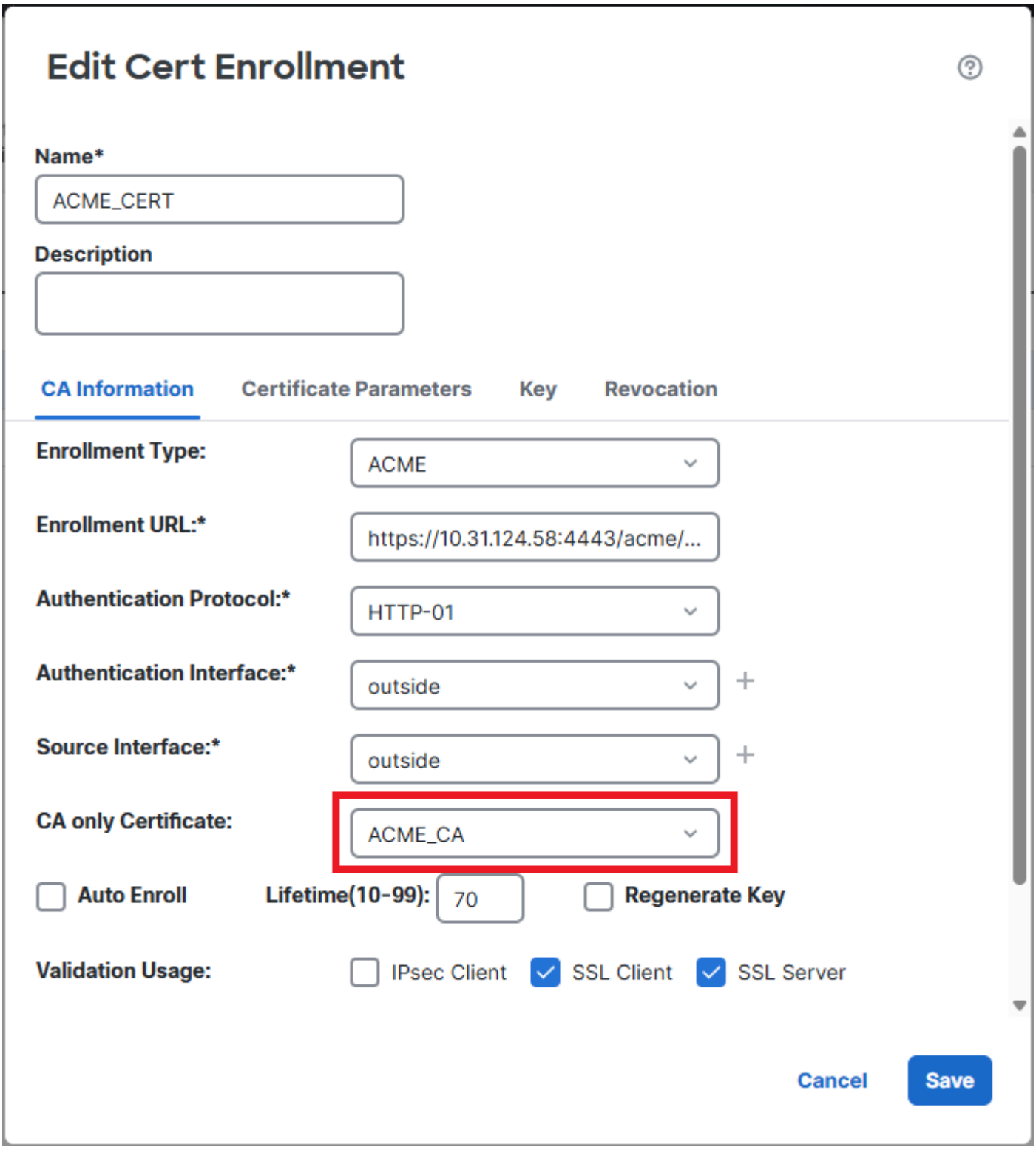
4. Si vous utilisez un serveur ACME qui n'est pas bien connu, vous devez ajouter le certificat CA du serveur ACME. Accédez à Objets > Inscription de certificat et cliquez sur le bouton Ajouter une inscription de certificat.



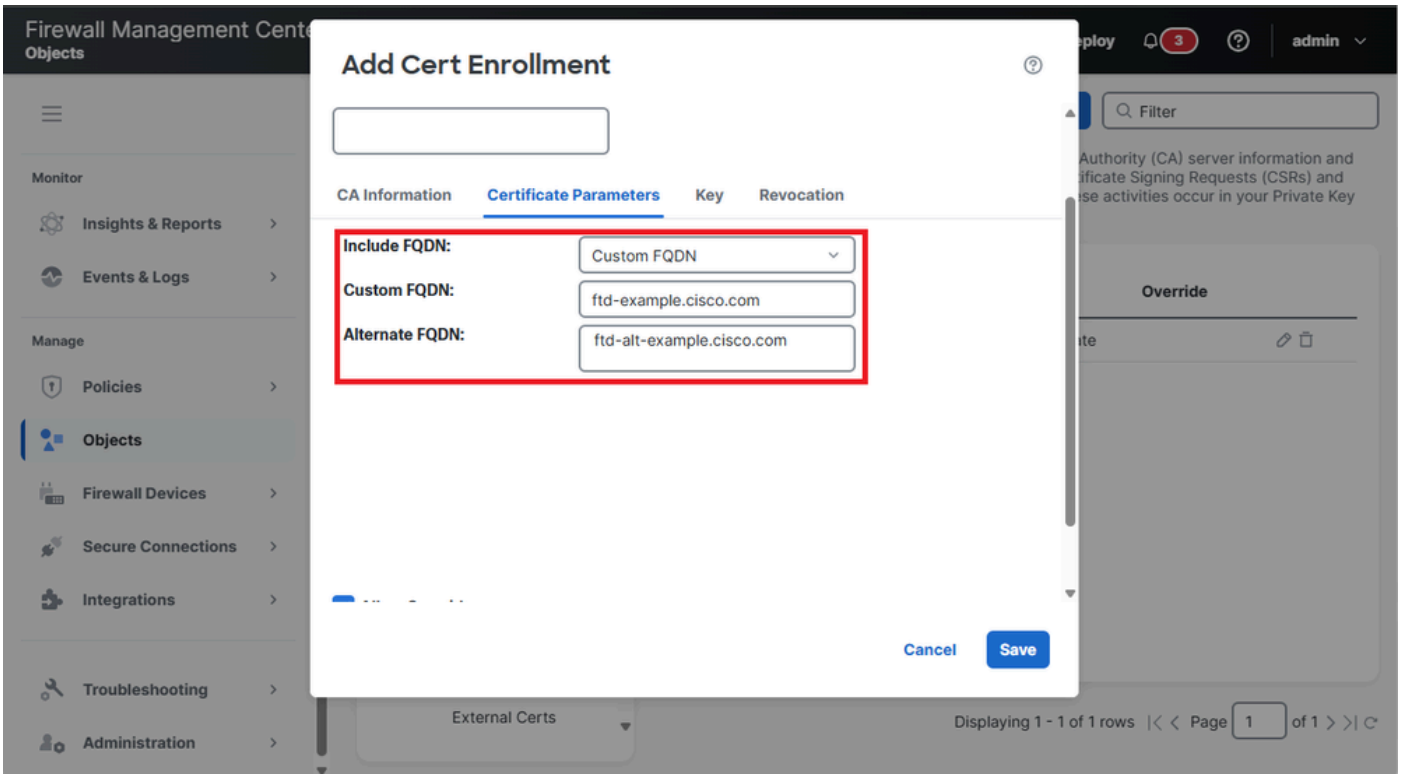
- Nommez le point de confiance et sélectionnez le type d'inscription Manuel. Cochez ensuite l'option CA Only. Enfin, collez le certificat CA du serveur ACME et cliquez sur Save.



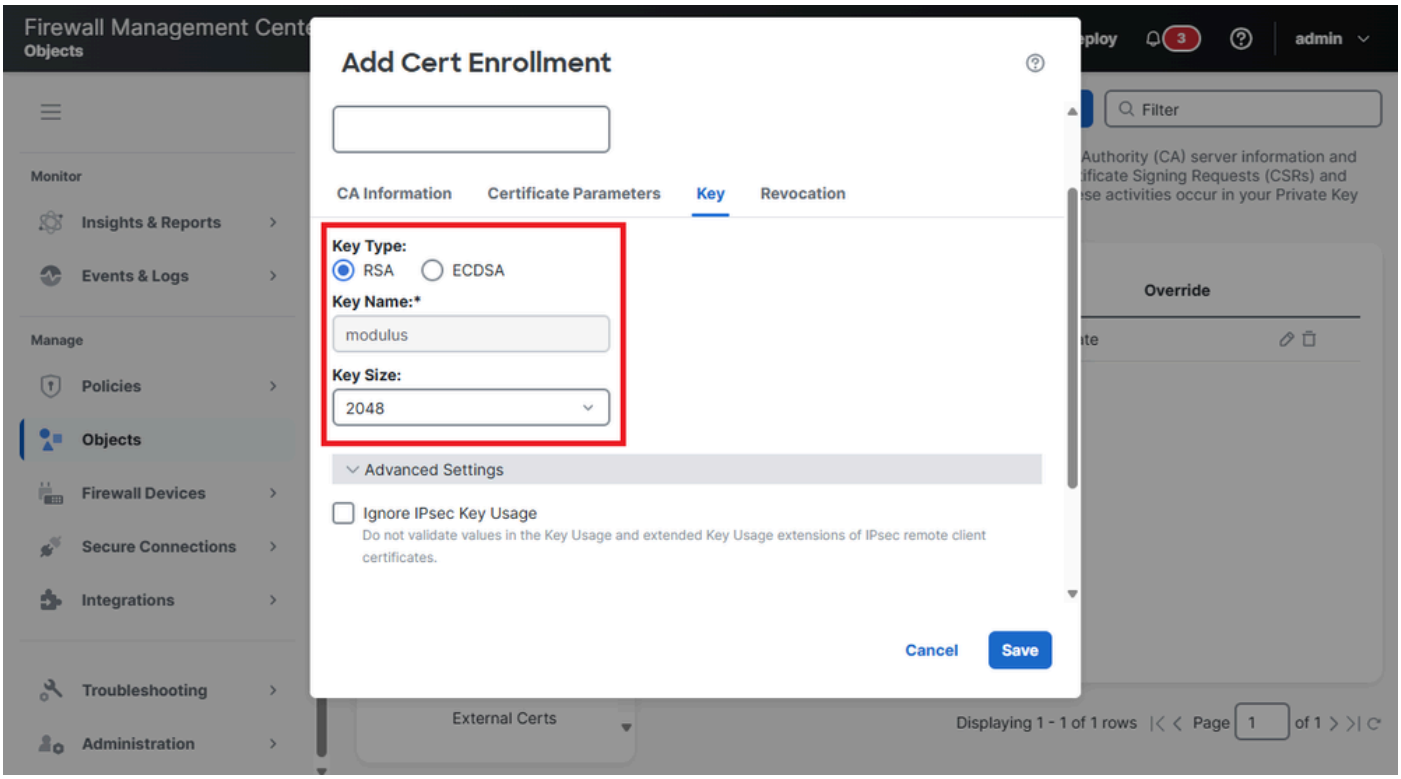
- Enfin, sélectionnez le point de confiance du serveur AC ACME dans la section Certificat CA uniquement.



5. Accédez à Paramètres du certificat, sélectionnez l'option Nom de domaine complet personnalisé dans la zone Inclure le nom de domaine complet, et renseignez les champs Nom de domaine complet personnalisé et Nom de domaine complet de remplacement avec le nom de domaine complet principal et tous les autres noms de domaine à inclure dans le certificat.



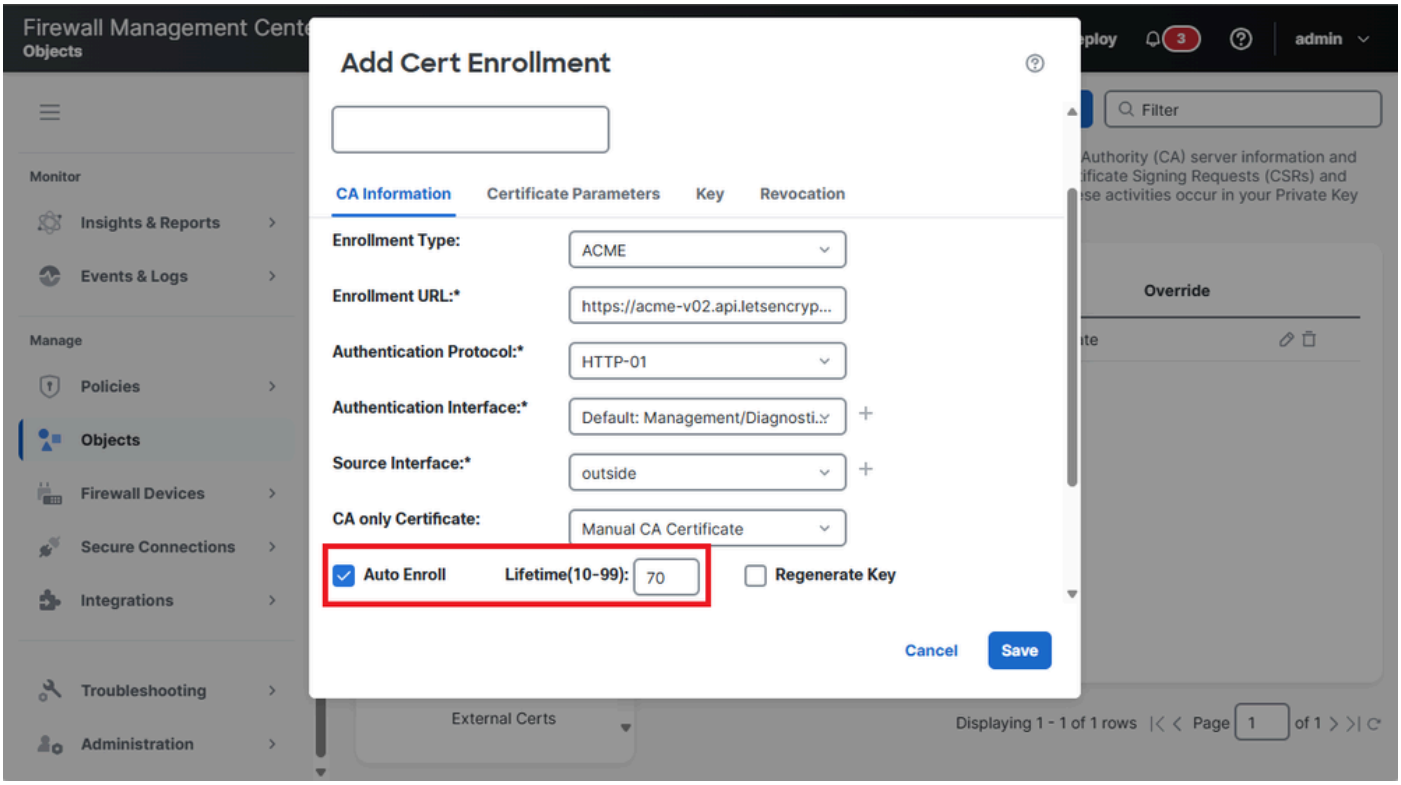
6. Accédez à Key pour modifier les paramètres Key Type et Key Size.



7. (Facultatif) Activez l'inscription automatique pour le certificat d'identité.

Cochez la case Inscription automatique et spécifiez le pourcentage de la durée de vie de l'inscription automatique.

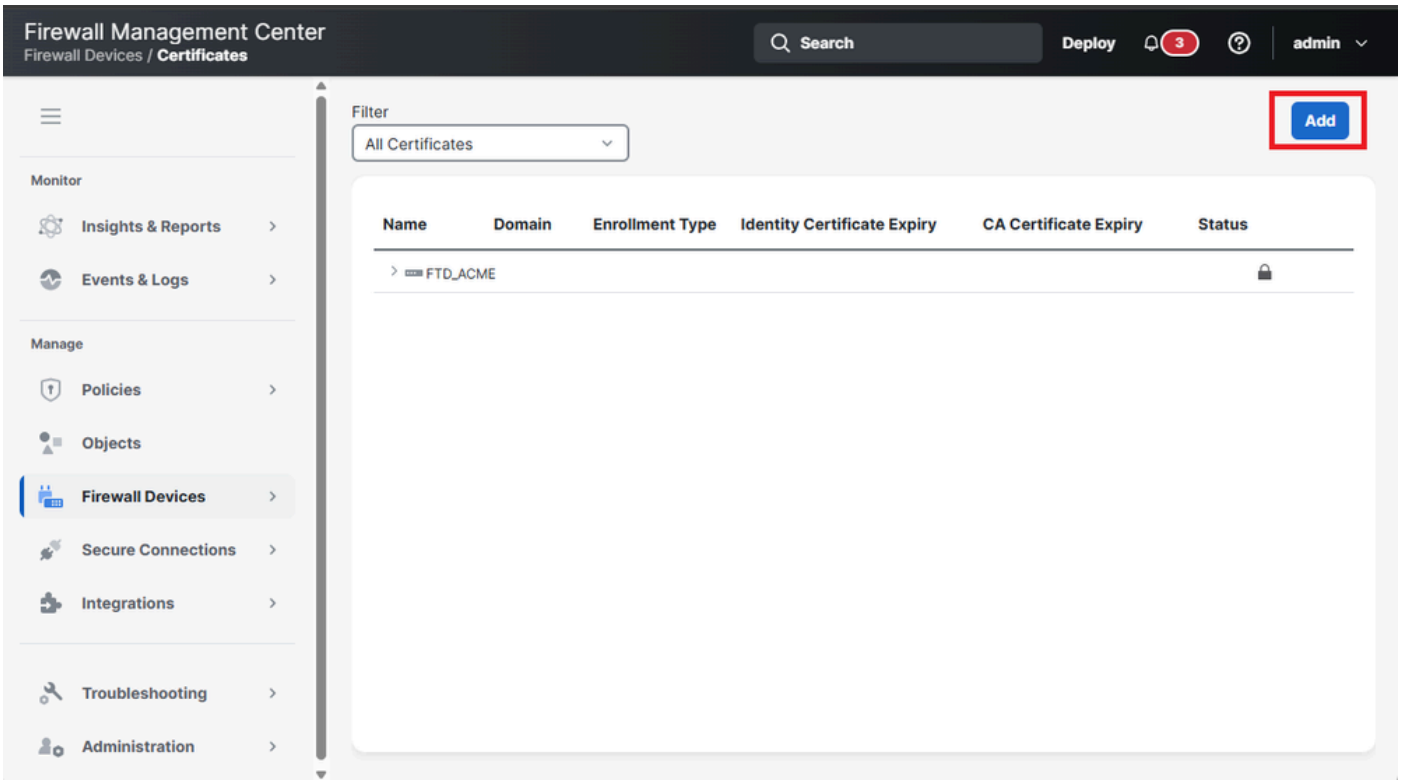
Cette fonctionnalité garantit que le certificat est renouvelé automatiquement avant son expiration. Le pourcentage détermine combien de temps avant l'expiration du certificat le processus de renouvellement commence. Par exemple, si la valeur est 80 %, le processus de renouvellement commence lorsque le certificat a atteint 80 % de sa période de validité.



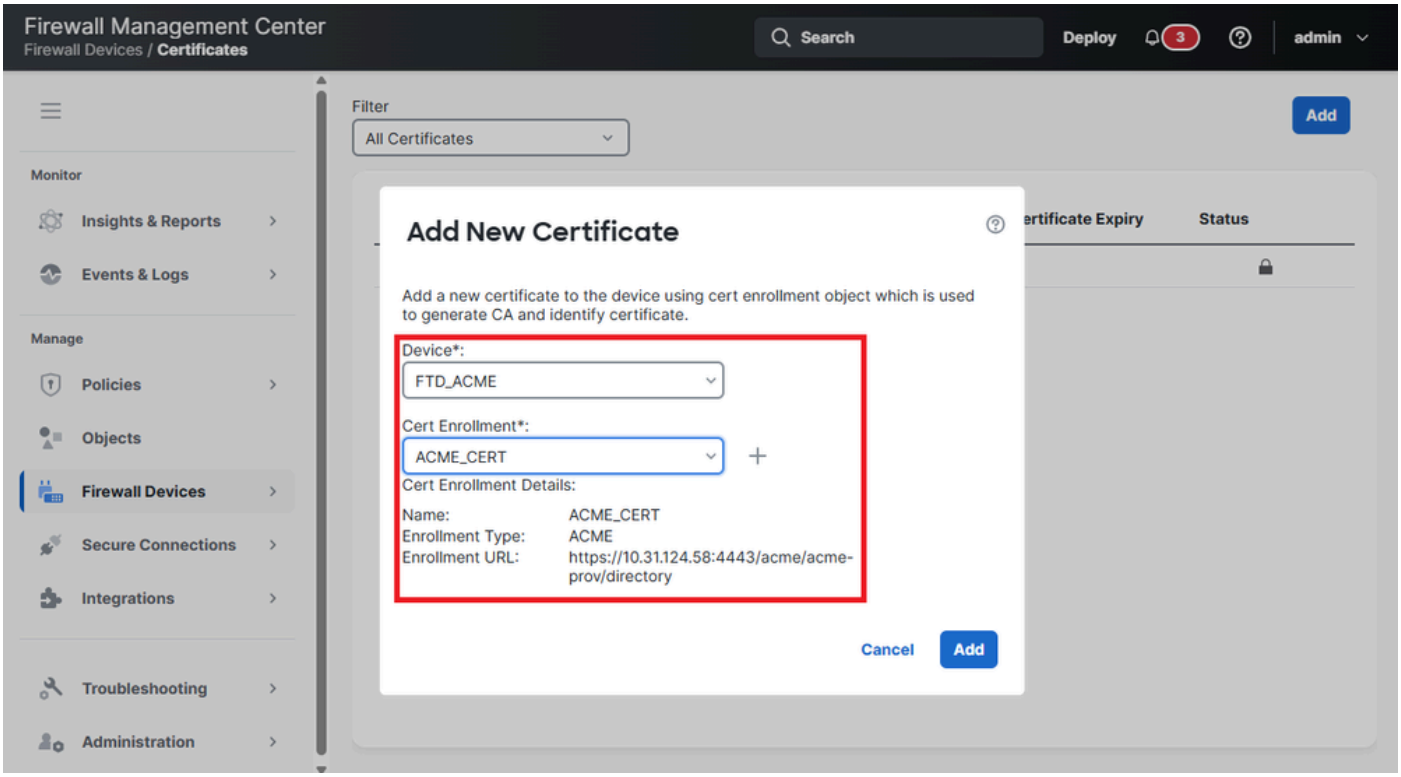
8. Cliquez sur Enregistrer.

Inscription de certificat ACME sur le périphérique

1.Accédez à Firewall Devices > Certificates et cliquez sur le bouton Add pour inscrire un nouveau certificat.

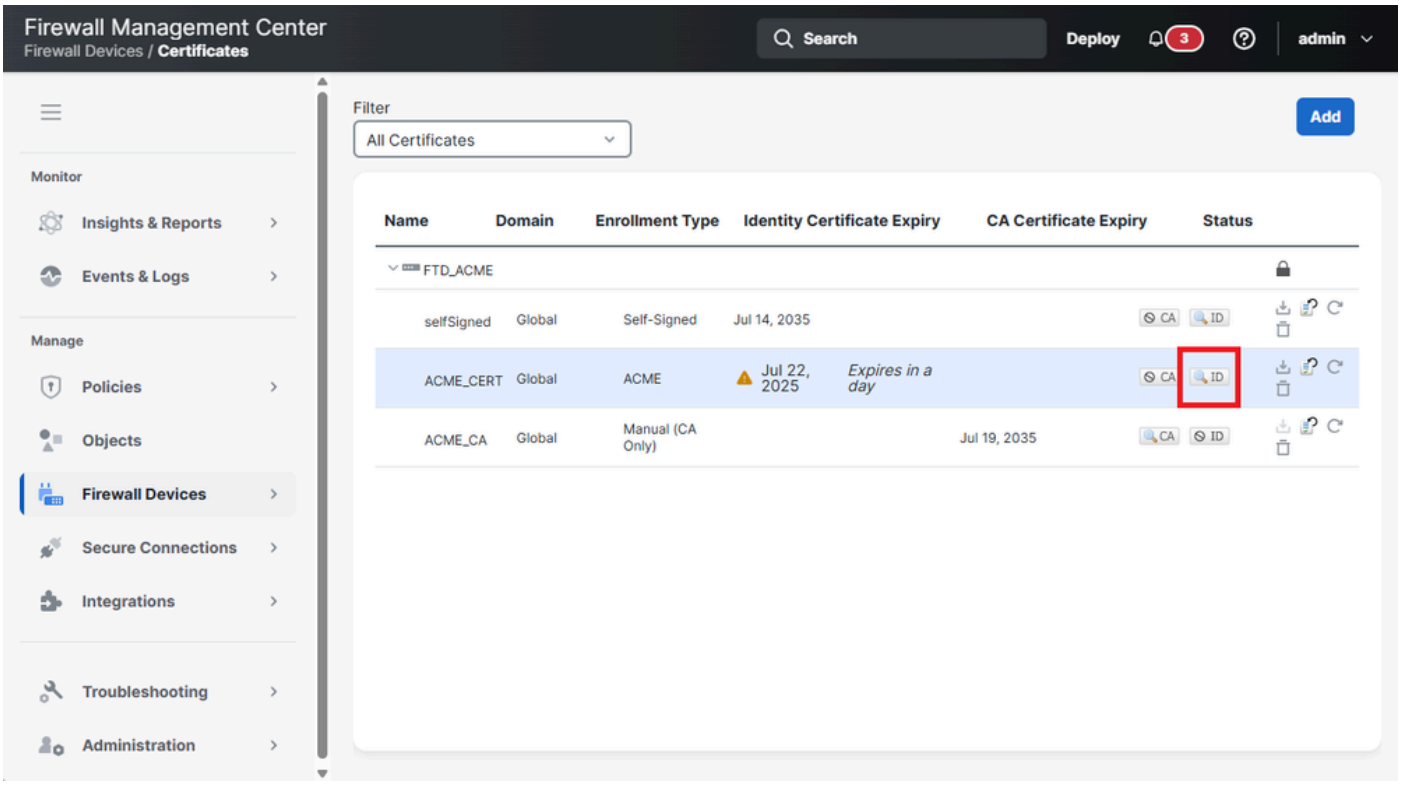


2. Sélectionnez le périphérique FTD dans la liste déroulante Périphérique et l'objet de certificat précédemment créé dans Inscription de certificat.

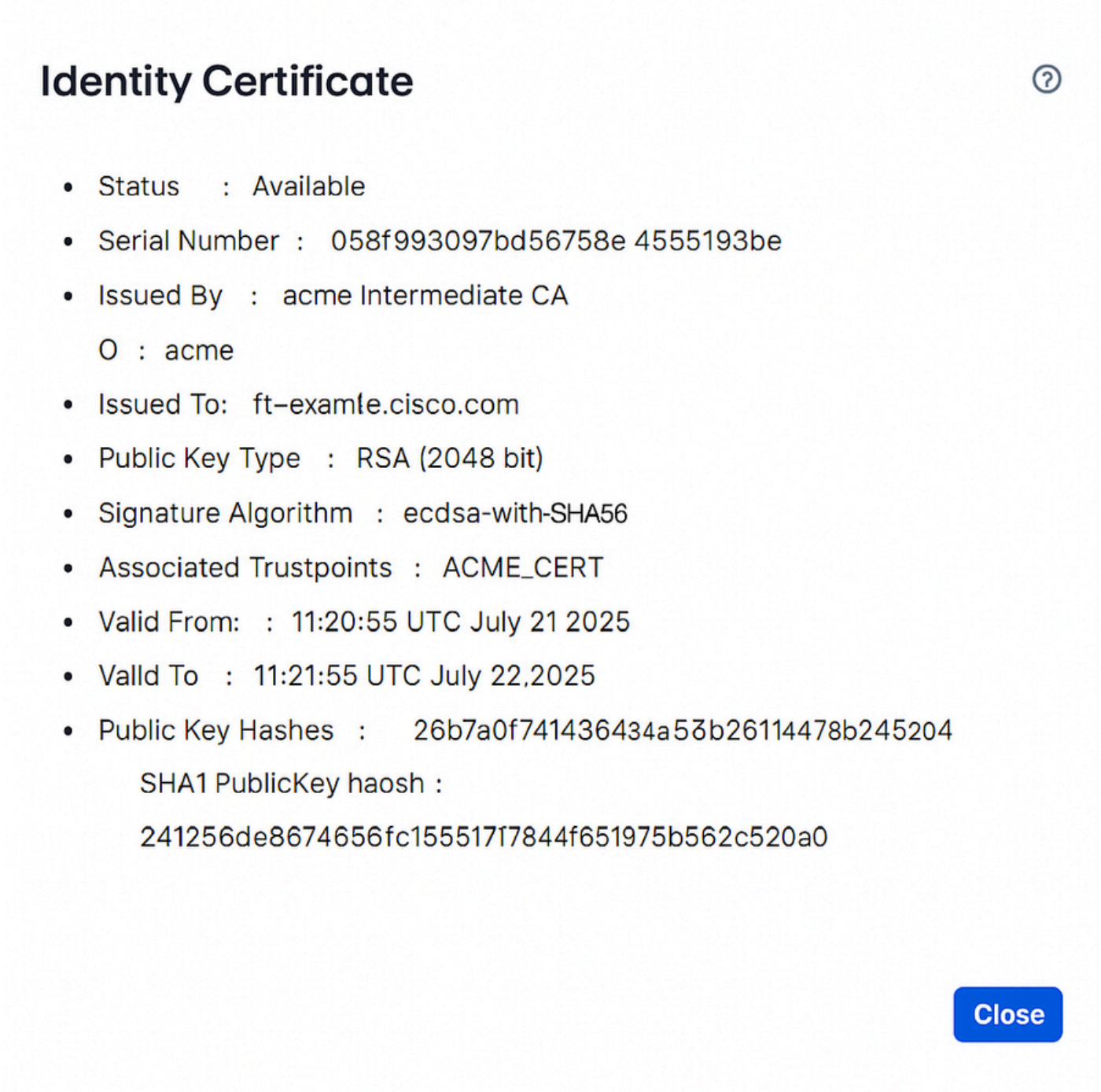


3. Cliquez sur Ajouter.

4. Une fois le déploiement terminé, la colonne d'état affiche le bouton ID certificate.



5. Validez les informations de certificat d'ID en cliquant sur le bouton ID.



Vérifier

Afficher le certificat installé dans FTD

Confirmez que le certificat est inscrit à l'aide de la commande.show crypto ca certificates <Nom du point de confiance>.

<#root>

```
firepower#
```

show crypto ca certificates

ACME_CERT

```
Certificate
Status: Available
Certificate Serial Number: 058f993097bd56758e44554194a953be
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=acme Intermediate CA
O=acme
Subject Name:
CN=ftd-example.cisco.com
Validity Date:
start date: 11:20:55 UTC Jul 21 2025
end date: 11:21:55 UTC Jul 22 2025
Storage: immediate
Associated Trustpoints: ACME_CERT
Public Key Hashes:
SHA1 PublicKey hash: 26b7a0f7414364a45b246114478bb74f432520c4
SHA1 PublicKeyInfo hash: 24125d6e8674566c1551784f651975b562c520a
```

Événements Syslog

De nouveaux syslogs sont disponibles dans le FTD Secure Firewall pour capturer les événements liés à l'inscription de certificat à l'aide du protocole ACME :

- 717067: Fournit des informations sur le démarrage de l'inscription de certificat ACME.

```
%FTD-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.
```

- 717068: Fournit des informations sur la réussite de l'inscription du certificat ACME.

```
%FTD-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069: Fournit des informations sur les échecs d'inscription ACME.

```
%FTD-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070: Fournit des informations relatives à la paire de clés pour l'inscription ou le renouvellement de certificat.

```
%FTD-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

Dépannage

Si l'inscription d'un certificat ACME échoue, envisagez les étapes suivantes pour identifier et résoudre le problème :

- Vérifier la connectivité au serveur :Vérifiez que le pare-feu sécurisé dispose d'une connectivité réseau au serveur ACME. Vérifiez qu'aucun problème réseau ou règle de pare-feu ne bloque la communication.
- Assurez-vous que le nom de domaine du pare-feu sécurisé peut être résolu : Assurez-vous que le nom de domaine configuré sur le FTD du pare-feu sécurisé peut être résolu par le serveur ACME. Cette vérification est essentielle pour que le serveur puisse valider la requête.
- Confirm Domain Ownership : vérifiez que tous les noms de domaine spécifiés dans le point de confiance appartiennent au FTD Secure Firewall. Cela garantit que le serveur ACME peut valider la propriété du domaine.

Dépannage des commandes

Pour plus d'informations, collectez le résultat des commandes debug suivantes :

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

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.