Configurer l'inscription de certificat avec le protocole ACME sur le pare-feu sécurisé

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Exigences et limitations
  - Considérations de rétrogradation
- Informations générales
- Configurer
  - Configuration des prérequis
  - Inscription ACME avec ASDM
  - Inscription ACME avec Secure Firewall ASA CLI
- Vérifier
  - Afficher le certificat installé dans ASA
  - Événements Syslog
- Dépannage
  - Dépannage des commandes
  - « Error Code
  - Motif
  - Cause possible ou correction
- Informations connexes

Introduction

Ce document décrit le processus d'inscription d'un certificat TLS (Transport Layer Security) à l'aide du protocole ACME (Automated Certificate Management Environment) sur Secure Firewall ASA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil de sécurité adaptatif Cisco Secure Firewall (ASA)
- Infrastructures à clé publique (PKI)

Composants utilisés

- Cisco ASAv version 9.23.1.
- Cisco ASDM version 7.23(1).
- 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 limitations actuelles pour l'inscription ACME sur Secure Firewall ASA sont les suivantes :

- Prise en charge sur ASA version 9.23.1 et ASDM 7.23.1 et ultérieures
- Non pris en charge dans plusieurs contextes
- ACME ne prend pas en charge la création de certificats génériques. Chaque demande de certificat doit spécifier un nom de domaine exact.
- Chaque point de confiance inscrit via ACME est limité à une seule interface, ce qui signifie que les certificats inscrits avec ACME ne peuvent pas être partagés entre plusieurs interfaces.
- Les paires de clés sont générées automatiquement et ne peuvent pas être partagées pour les certificats inscrits via ACME. Chaque certificat utilise une paire de clés unique, ce qui améliore la sécurité mais limite la réutilisation des clés.

Considérations de rétrogradation

Lors d'une mise à niveau vers une version qui ne prend pas en charge l'inscription ACME sur Secure Firewall ASA (9.22 et versions antérieures) :

- Toutes les configurations de point de confiance liées à ACME nouvelles à la version 9.23.x ou ultérieure sont perdues
- Tous les certificats inscrits via ACME restent accessibles, mais la clé privée est dissociée après le premier enregistrement et redémarrage post-rétrogradation

Si une rétrogradation est nécessaire, exécutez la procédure de contournement suivante recommandée :

1. Avant de procéder à la rétrogradation, assurez-vous d'exporter les certificats ACME au format PKCS12.
2. Avant de procéder à la rétrogradation, veillez à supprimer la configuration du point de confiance ACME.

3. Après la rétrogradation, importez le certificat PKCS12. Le point de confiance résultant est toujours valide jusqu'à l'expiration du certificat émis via ACME.

Informations générales

Le protocole ACME est conçu pour rationaliser la gestion des certificats TLS pour les administrateurs réseau. Grâce à ACME, les administrateurs peuvent automatiser les processus d'obtention et de renouvellement des certificats TLS. Cette automatisation est particulièrement utile lors de l'utilisation d'autorités de certification (CA) telles que Let's Encrypt, qui offrent des certificats gratuits, automatisés et ouverts à l'aide du protocole ACME.

ACME prend en charge l'émission de certificats de validation de domaine (DV). Ces certificats sont un type de certificat numérique qui confirme le contrôle du détenteur du certificat sur les domaines spécifiés. Le processus de validation des certificats DV est généralement effectué par le biais d'un mécanisme de demande de confirmation basé sur HTTP. Dans ce mécanisme, le demandeur place un fichier spécifique sur son serveur Web, que l'autorité de certification (AC) vérifie en accédant au fichier par le serveur HTTP du domaine. La réussite de ce défi démontre à l'autorité de certification que le demandeur a le contrôle sur le domaine, ce qui permet l'émission du certificat DV.

Le processus d'inscription est le suivant :

1. Lancer la demande de certificat : Le client demande un certificat au serveur ACME et spécifie le ou les domaines pour lesquels le certificat est requis.
2. Réception de la demande HTTP-01 : Le serveur ACME fournit une interrogation HTTP-01 avec un jeton unique que le client peut utiliser pour prouver le contrôle du domaine.
3. Préparer la réponse au défi :
    - Le client crée une autorisation de clé en combinant le jeton du serveur ACME avec sa clé de compte.
    - 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 envoie une requête HTTP GET à l'URL spécifiée pour récupérer l'autorisation de clé.
5. Le serveur ACME vérifie la propriété : Le serveur vérifie si l'autorisation de clé récupérée correspond à la valeur attendue pour confirmer le contrôle du client sur le domaine.
6. Émettre le certificat : Après validation réussie, le serveur ACME émet le certificat SSL/TLS au client.



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

Les avantages les plus pertinents de l'utilisation du protocole ACME pour inscrire des certificats TLS sont les suivants :

- ACME facilite l'acquisition et la maintenance des certificats de domaine TLS pour les interfaces TLS ASA de pare-feu sécurisé. Cette automatisation réduit considérablement les tâches manuelles et permet de maintenir les certificats à jour sans surveillance constante.
- Avec les points de confiance compatibles ACME, les certificats sont automatiquement renouvelés à l'expiration. Cette fonctionnalité réduit la nécessité d'une intervention administrative, garantissant une sécurité ininterrompue et empêchant l'expiration inattendue des certificats.

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. Accès sécurisé du pare-feu au serveur ACME : Le pare-feu sécurisé doit avoir la capacité 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.

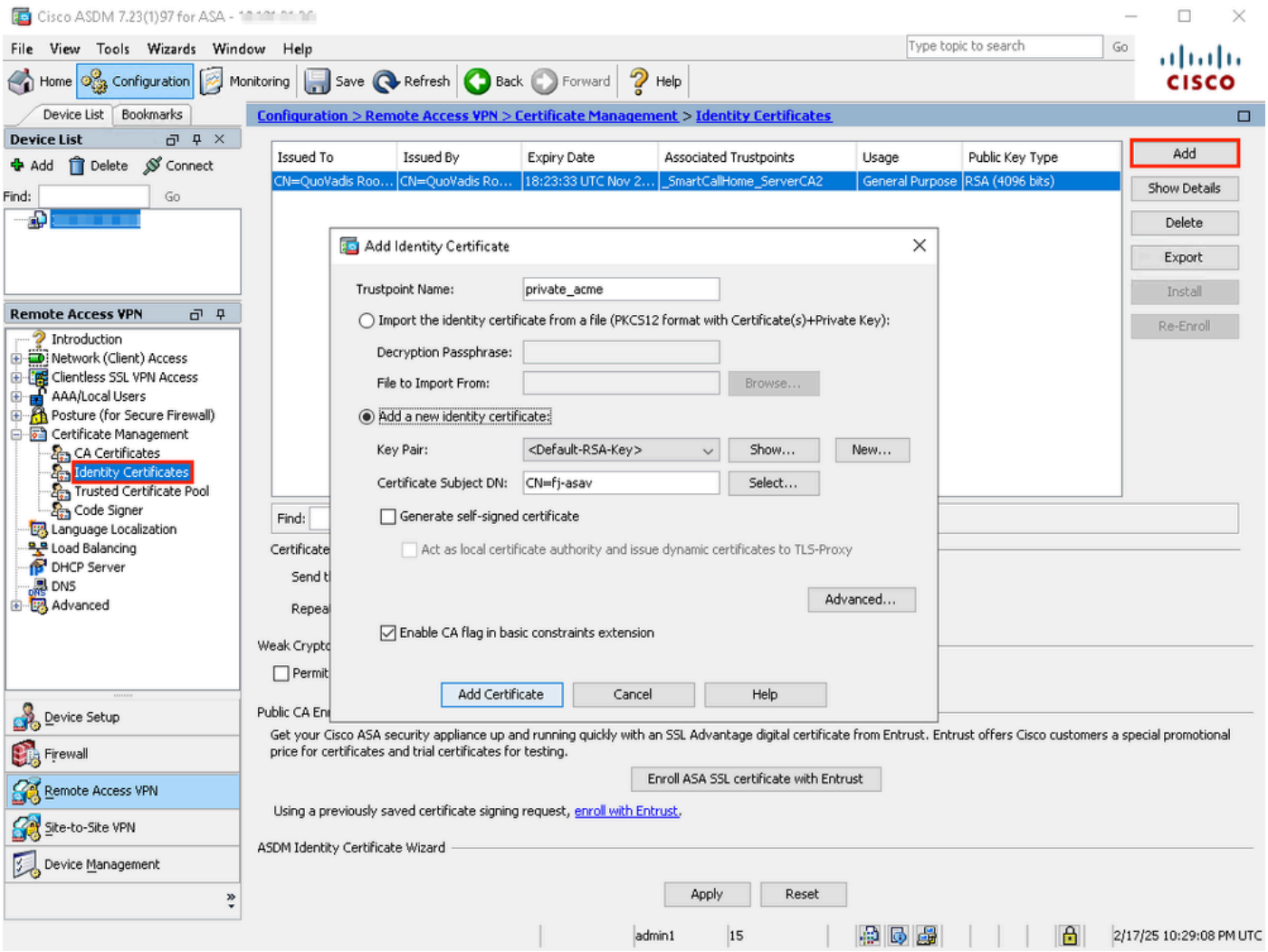
3. Disponibilité du port TCP 80 : Autorisez le port TCP 80 du serveur AC ACME vers l'interface qui correspond au nom de domaine. Cette opération est nécessaire pendant le processus d'échange ACME pour effectuer le défi HTTP-01.

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

Inscription ACME avec ASDM

1. Ajoutez un nouveau certificat d'identité.

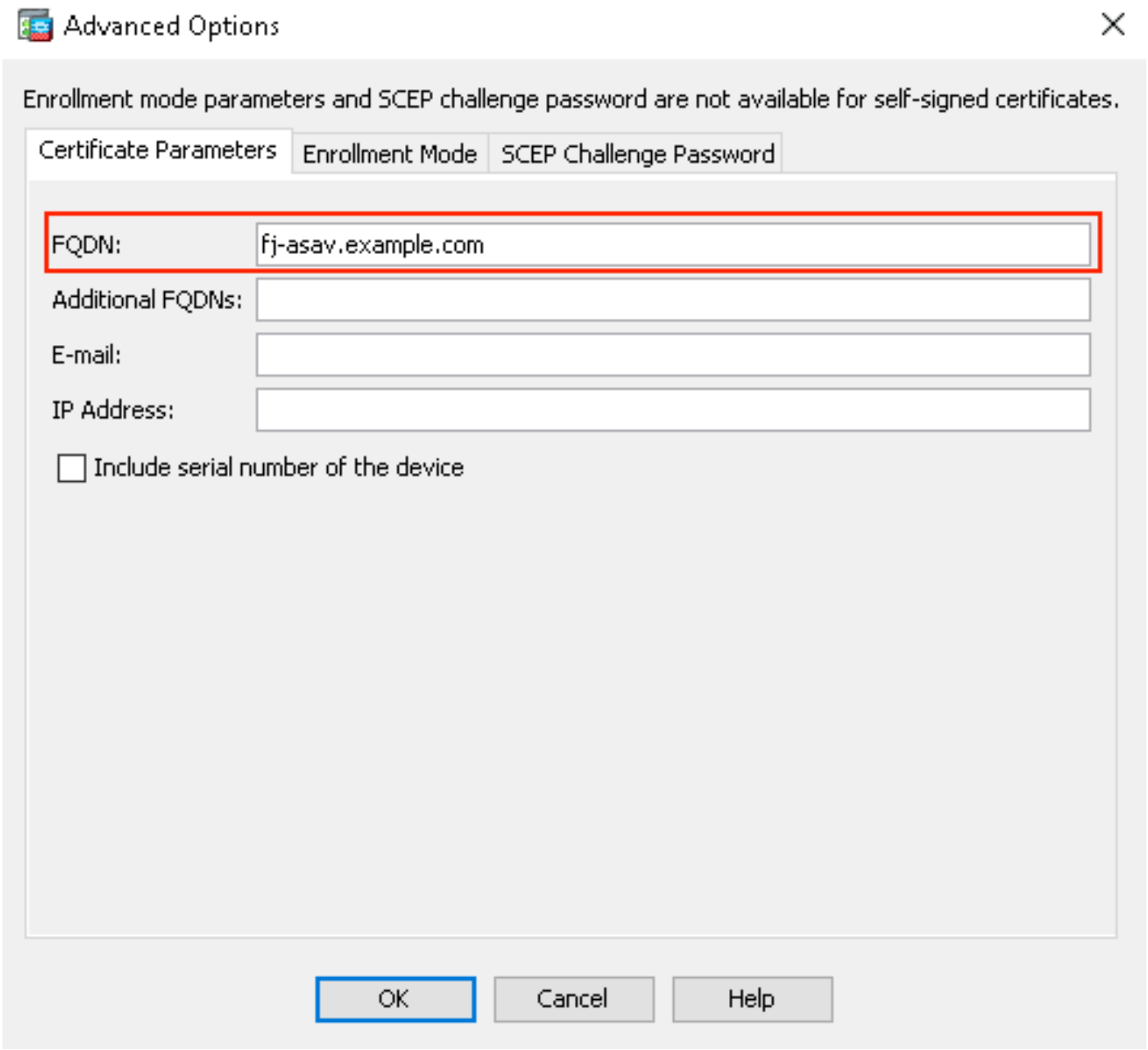
- Accédez à Configuration > Remote Access VPN > Certificate Management > Identity Certificates.
- Cliquez sur le bouton Add et sélectionnez Add a new identity certificate.



Inscription ACME Certificat d'identité ASDM.

2. Spécifiez le nom de domaine complet du certificat d'identité.

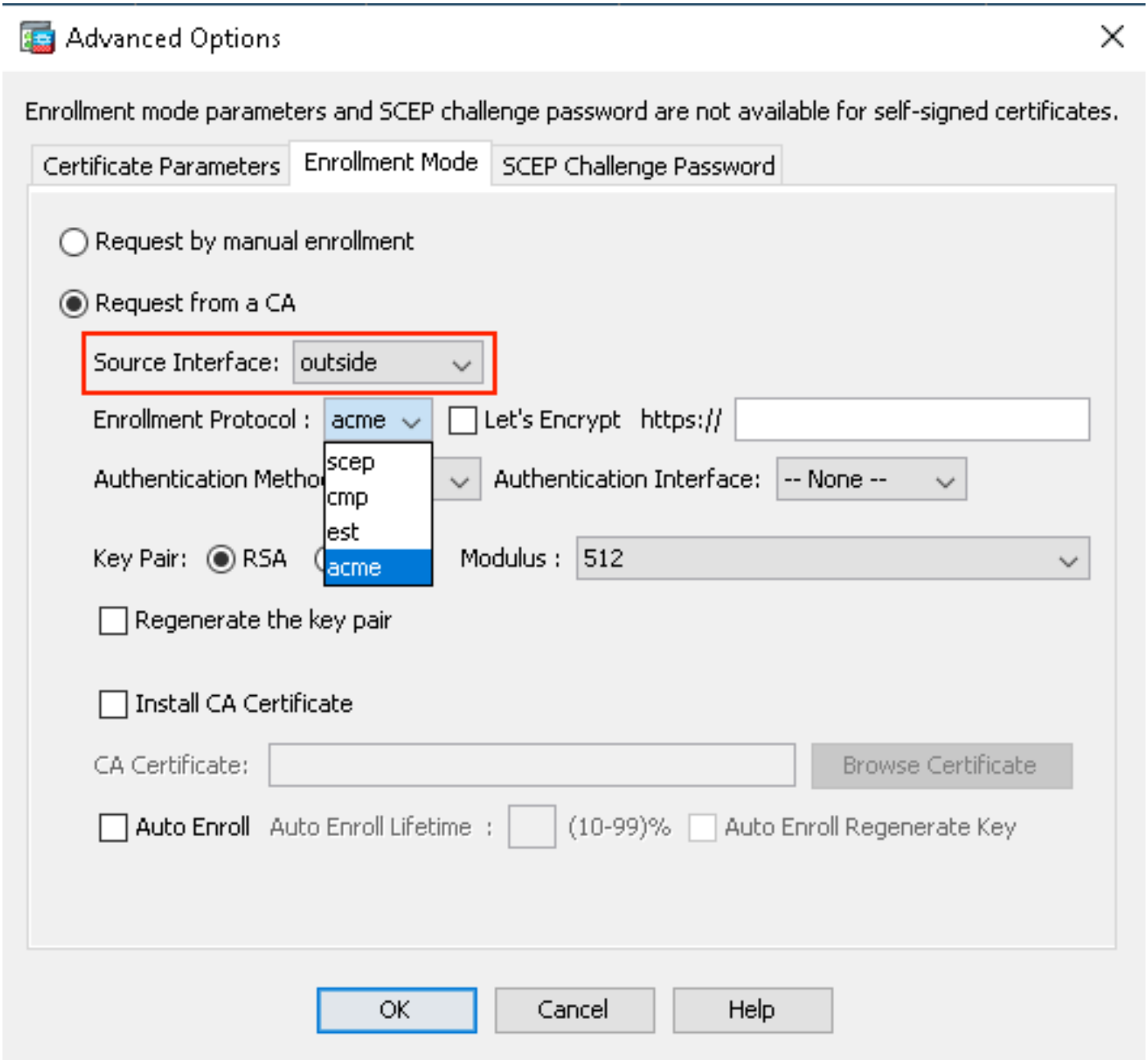
- Cliquez sur le bouton Avancé.
- Sous l'onglet Certificate Parameters, spécifiez le FQDN que le certificat doit avoir.



FQDN ASDM d'inscription ACME.

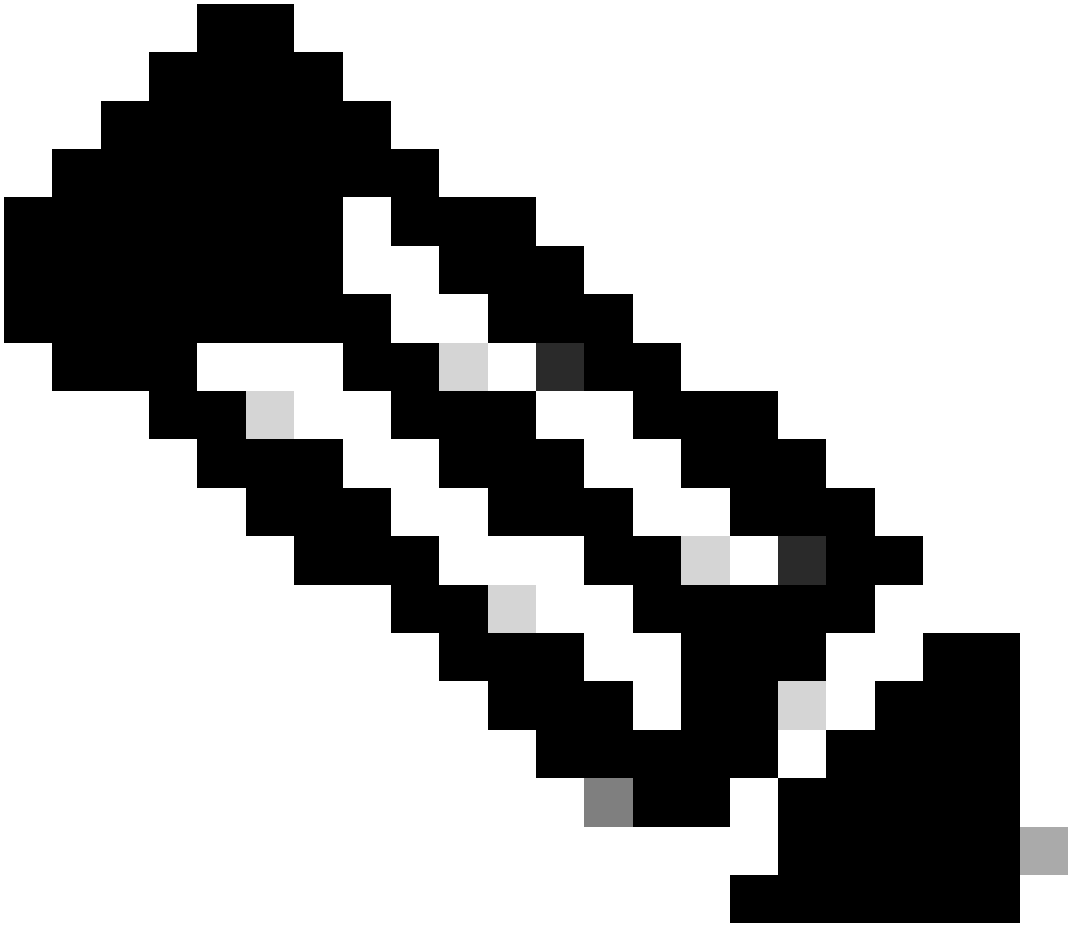
3. Sélectionnez ACME comme protocole d'inscription.

- Sous l'onglet Enrollment Mode, sélectionnez Request from CA.
- Spécifiez l'interface source et sélectionnez acme comme protocole d'inscription.

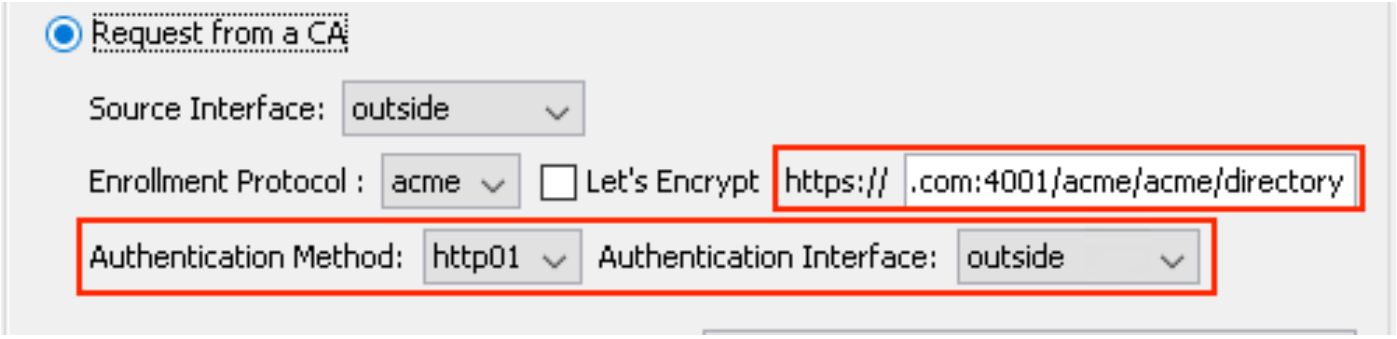


Inscription ACME Protocole ACME ASDM. sélection

4. Sélectionnez Let's Encrypt pour que votre certificat soit signé par Let's Encrypt public CA. Sinon, spécifiez l'URL de votre autorité de certification interne qui prend en charge le protocole d'inscription ACME. Spécifiez également l'interface d'authentification.



Remarque : Lorsque la case Let's Encrypt est cochée, l'URL du serveur est automatiquement renseignée.



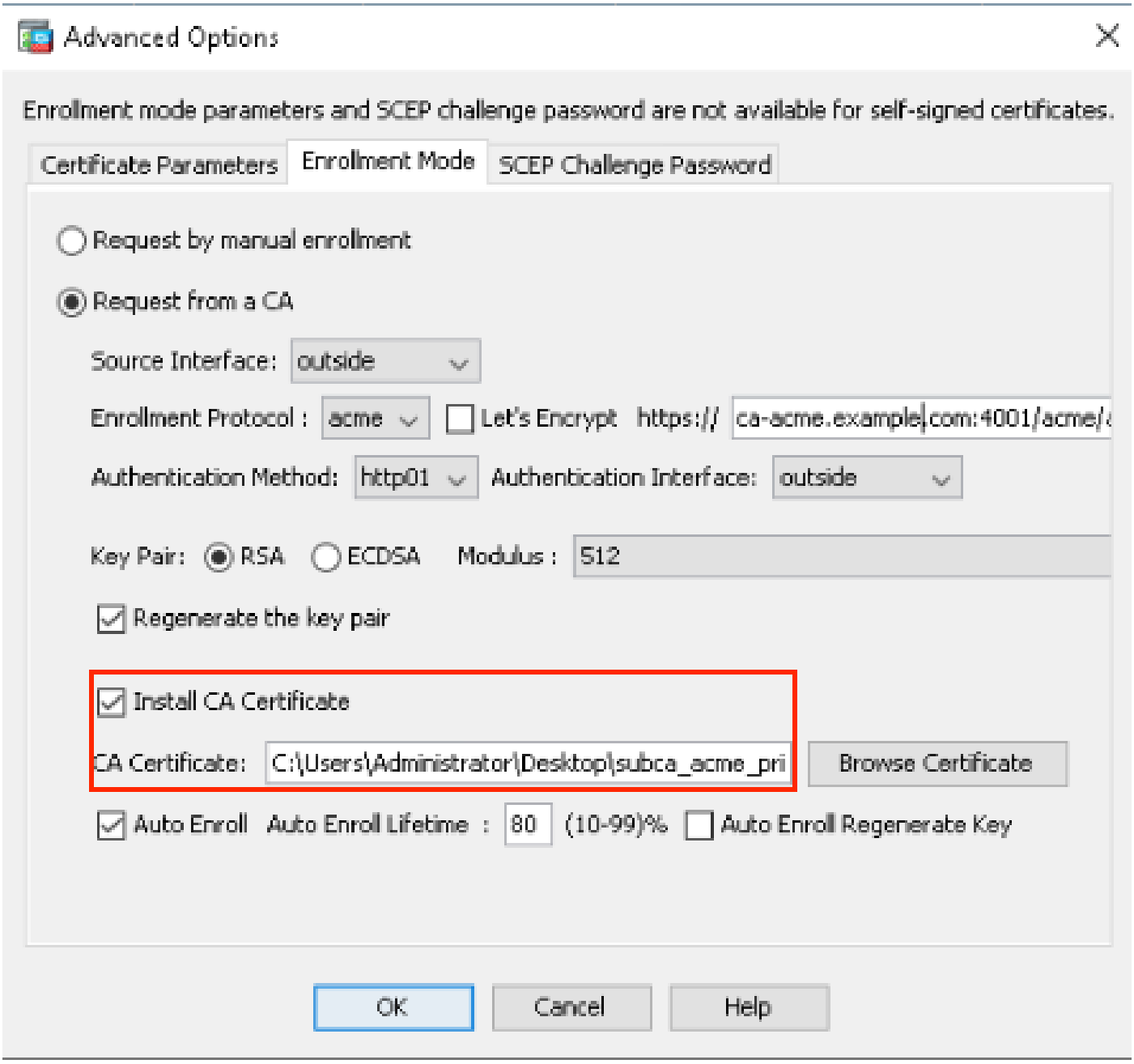
Méthode d'authentification ASDM d'inscription ACME.

5. Installez le certificat CA.

Si l'option Install CA Certificate est cochée, vous devez télécharger le certificat de l'autorité de certification immédiate qui émet votre certificat.

Remarque : Si le certificat d'autorité de certification existe déjà sur le pare-feu sécurisé, que ce soit à partir d'une installation précédente ou dans le pool de confiance, il n'est pas nécessaire de vérifier cette option. Laissez la case Installer le certificat AC décochée.

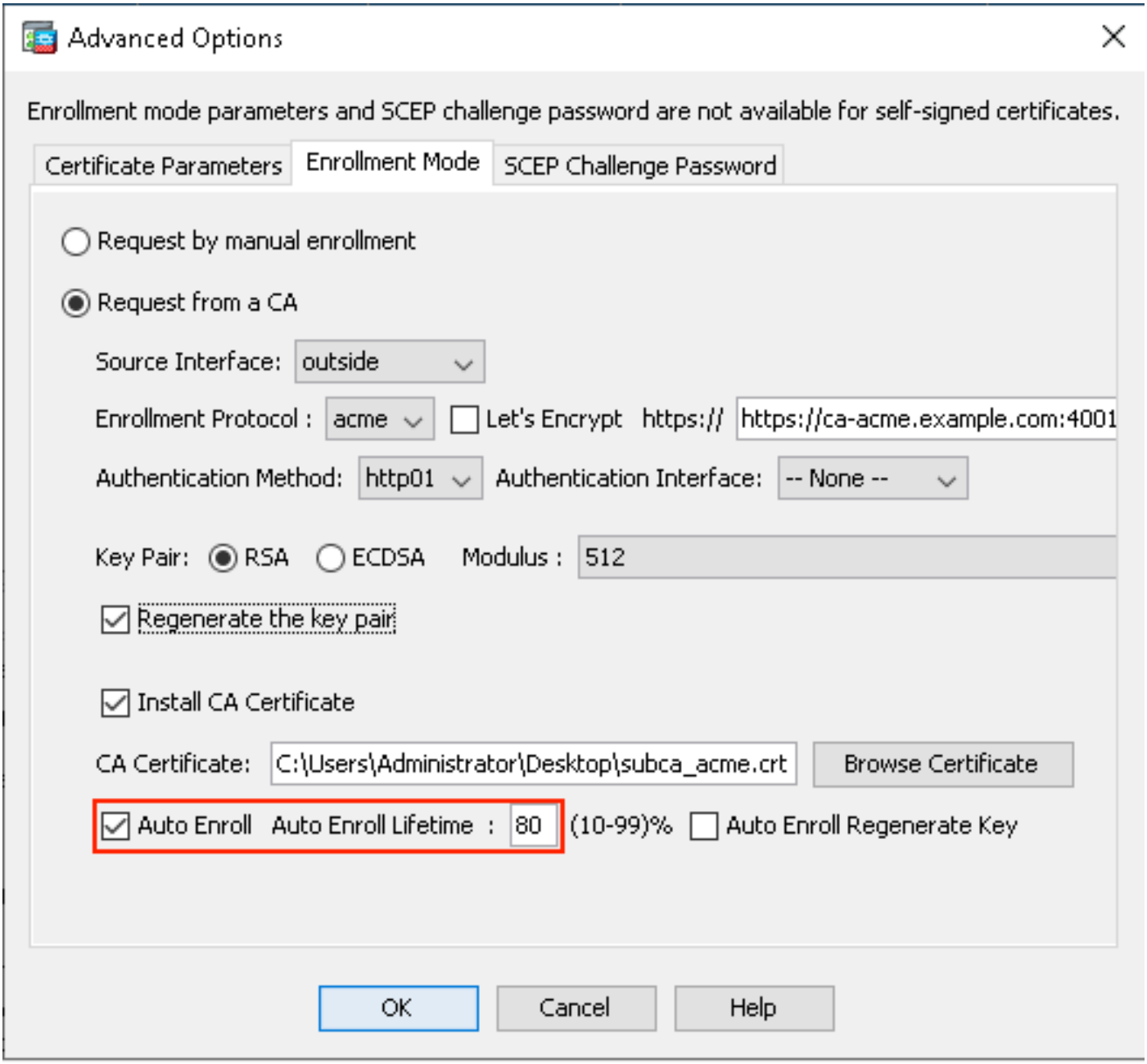
Remarque : Lorsque vous sélectionnez l'option Let's Encrypt, laissez la case à cocher Install CA Certificate décochée, car les certificats CA racine pour Let's Encrypt sont déjà inclus dans le groupe de confiance Secure Firewall.



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

Cochez la case Auto Enroll 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.



7. Cliquez sur OK et enregistrez la configuration.

Inscription ACME avec Secure Firewall ASA CLI

1. Créez un nouveau point de confiance.

Créez un point de confiance et spécifiez acme comme protocole d'inscription.

<#root>

```
asav(config)# crypto ca trustpoint private_acme
asav(config-ca-trustpoint)# enrollment protocol ?

crypto-ca-trustpoint mode commands/options:

acme Automatic Certificate Management Environment

  cmp Certificate Management Protocol Version 2
  est Enrollment over Secure Transport
  scep Simple Certificate Enrollment Protocol
```

2. Sélectionnez la méthode HTTP-01 d'authentification pour vérifier le contrôle du domaine.

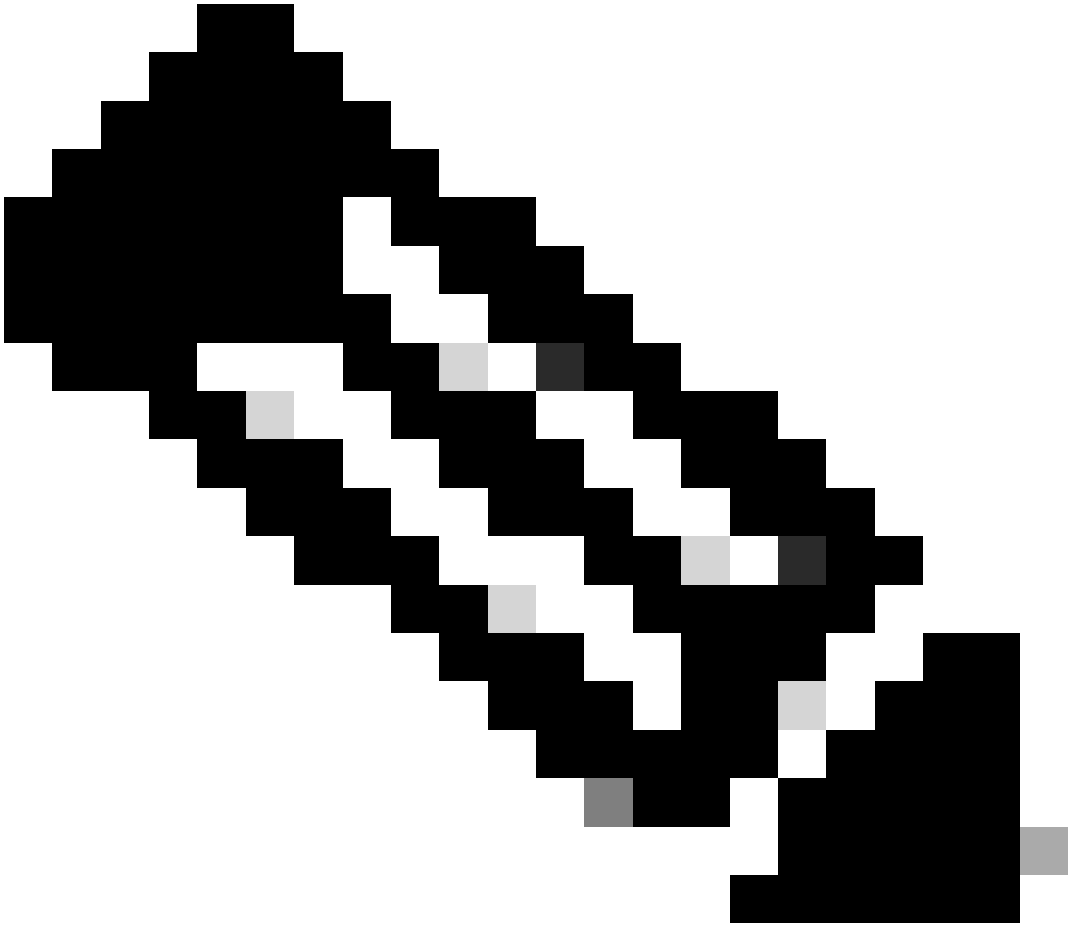
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

crypto-ca-trustpoint mode commands/options:
http01 Use the HTTP-01 method, which opens port 80 on the specified
interface
```

3. Sélectionnez Let's Encrypt comme CA ACME. Si vous utilisez une autre autorité de certification prenant en charge le protocole ACME, indiquez l'URL appropriée.

```
asav(config-ca-trustpoint)# enrollment protocol acme url ?

crypto-ca-trustpoint mode commands/options:
LINE < 477 char URL
LetsEncrypt Use the Let's Encrypt CA
```



Remarque : Lorsque le mot-clé LetEncrypt est configuré, l'URL du serveur Let's Encrypt est automatiquement renseignée.

4. Définissez la paire de clés RSA, le nom de domaine complet (FQDN) et le nom de sujet du certificat.

```
crypto ca trustpoint private_acme
 enrollment interface outside
 enrollment protocol acme authentication http01 outside
 enrollment protocol acme url https://ca-acme.example.com:4001/acme/acme/directory
 fqdn fj-asav.cisco.com
 subject-name CN=fj-asav.example.com
 keypair rsa modulus 4096
 auto-enroll 80 regenerate
 crl configure
```

5. Authentifiez le point de confiance.

Remarque : Si l'autorité de certification existe déjà sur le pare-feu sécurisé ou si vous utilisez l'option Chiffrement, cette étape peut être ignorée.

```
asav(config)# crypto ca authenticate private_acme
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIBwzCCAWqgAwIBAgIQedxaTDOJ1G6tLgAGti6tizAKBggqhkjOPQQDAjAsMRAw
DgYDVQQKEwdjYS1hY21lMRgwFgYDVQQDEw9jYS1hY21lIFJvb3QgQOEwHhcNMjQx
[truncated]
ADBEAiB7S4YZfnOK82K2yz5F5CzMe2t98LCpLRzoPJXMo7um1AIgH+K8EZMLstLN
AJQoplycJENo5D7kUmVrwUBBjREqv9I=
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: 40000000 40000000 40000000 40000000
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

6. Inscrivez le certificat.

```
asav(config)# crypto ca enroll private_acme
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=fj-asav.cisco.com

% The fully-qualified domain name in the certificate will be: fj-asav.example.com

% Include the device serial number in the subject name? [yes/no]: no

Request certificate from CA? [yes/no]: yes
```

Vérifier

Afficher le certificat installé dans ASA

Confirmez que le certificat est inscrit et vérifiez la date de renouvellement.

```
asav# show crypto ca certificates private_acme
```

```
CA Certificate
Status: Available
Certificate Serial Number: 79d000000000000000000008b
Certificate Usage: General Purpose
Public Key Type: ECDSA (256 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Root CA
O=ca-acme
Subject Name:
CN=ca-acme Intermediate CA
O=ca-acme
Validity Date:
start date: 23:20:19 UTC Nov 26 2024
end date: 23:20:19 UTC Nov 24 2034
Storage: config
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: 8c8200000000000000000000000000000000000077
SHA1 PublicKeyInfo hash: 974c0000000000000000000000000000000009e1

Certificate
Status: Available
Certificate Serial Number: 666000000000000000000000000000be
Certificate Usage: General Purpose
Public Key Type: RSA (4096 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Intermediate CA
O=ca-acme
Subject Name:
CN=fj-asav.example.com
Validity Date:
start date: 20:51:00 UTC Feb 14 2025
end date: 20:52:00 UTC Feb 15 2025
renew date: 16:03:48 UTC Feb 15 2025
Storage: immediate
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: e6e000000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e300000000000000000000000000000000009f
```

Événements Syslog

De nouveaux syslogs sont disponibles dans le pare-feu sécurisé 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

```
%ASA-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

```
%ASA-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

```
%ASA-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

```
%ASA-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 :

- Vérifiez la connectivité au serveur : Vérifiez que le pare-feu sécurisé dispose d'une connectivité réseau avec le 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 pare-feu sécurisé peut être résolu par le serveur ACME. Cette vérification est essentielle pour que le serveur puisse valider la requête.
- Confirmer la propriété du domaine : Vérifiez que tous les noms de domaine spécifiés dans le point de confiance appartiennent au pare-feu sécurisé. 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>

Erreurs courantes d'inscription ACME :

« Error Code	Motif	Cause possible ou correction
7	Connexion au serveur impossible	Le serveur est accessible mais le service ACME ne fonctionne pas.
28	Connexion au serveur impossible	Le serveur n'est pas accessible. Vérifiez l'accès réseau de base au serveur ACME.
60	Impossible de valider le certificat du serveur	Assurez-vous que l'autorité de certification racine ou émettrice est présente dans un point de confiance ou dans le pool de confiance.
124	Délai de traitement ACME	Assurez-vous que tous les noms de domaine complets demandés correspondent à l'interface configurée pour l'authentification HTTP-01. Assurez-vous que l'URL ACME configurée est correcte.

Informations connexes

Pour obtenir de l'aide supplémentaire, contactez le TAC. Un contrat d'assistance valide est requis : Coordonnées du service d’assistance Cisco à l’échelle mondiale.
Vous pouvez également visiter la communauté VPN Cisco ici.

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.