Configurer l'authentification basée sur certificat Anyconnect pour l'accès mobile

Table des matières

Introduction

Ce document décrit un exemple de mise en oeuvre de l'authentification basée sur les certificats sur les périphériques mobiles.

Conditions préalables

Les outils et périphériques utilisés dans le guide sont les suivants :

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Appareil Apple iOS (iPhone, iPad)
- Autorité de certification (CA)
- Logiciel client Cisco Anyconnect

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN de base
- SSL/TLS
- Infrastructure à clé publique
- Expérience avec FMC

- OpenSSL
- Cisco Anyconnect

Composants utilisés

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

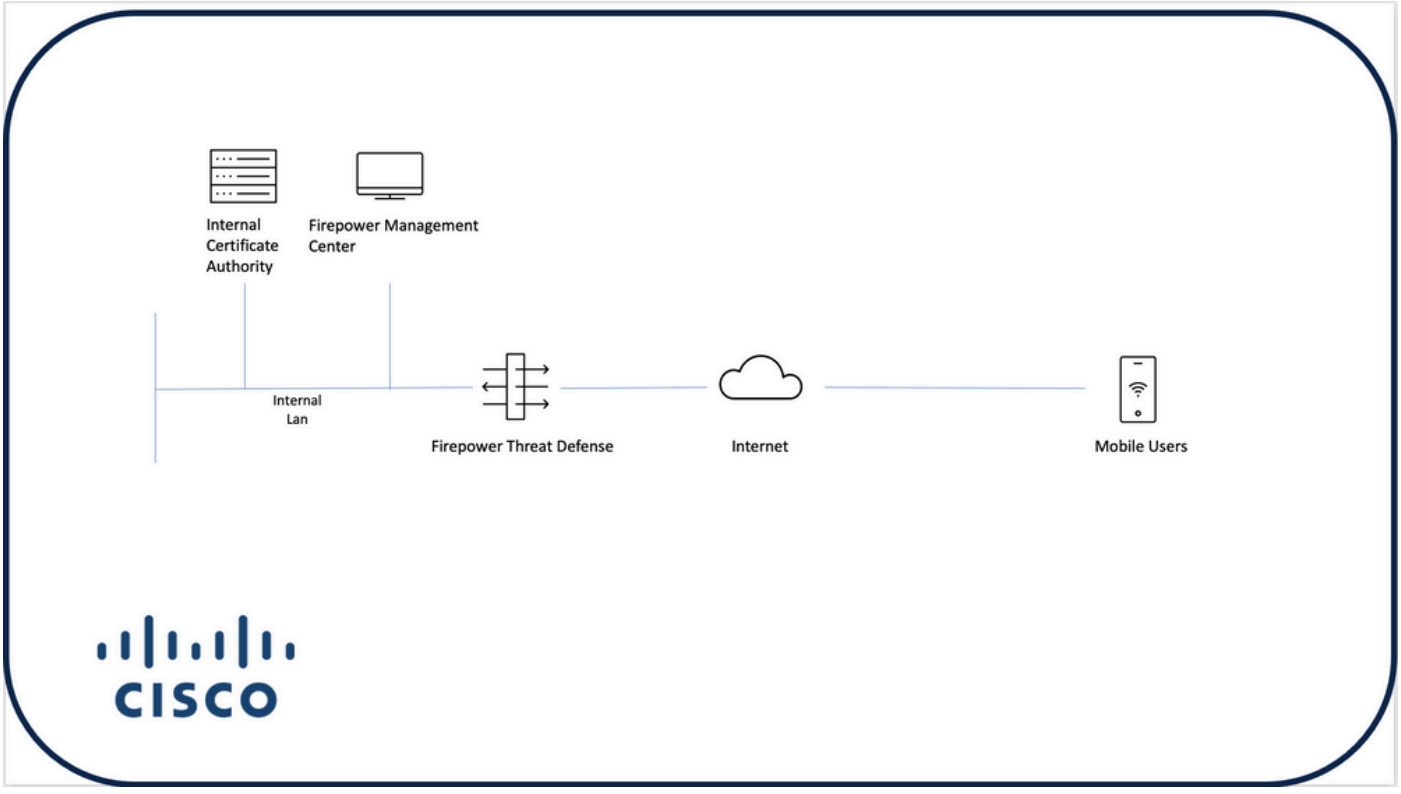
- Périphérique FTD Cisco
- Cisco FMC
- Serveur CA Microsoft
- XCA
- Cisco Anyconnect
- ipad Apple

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 Cisco Anyconnect sur FTD

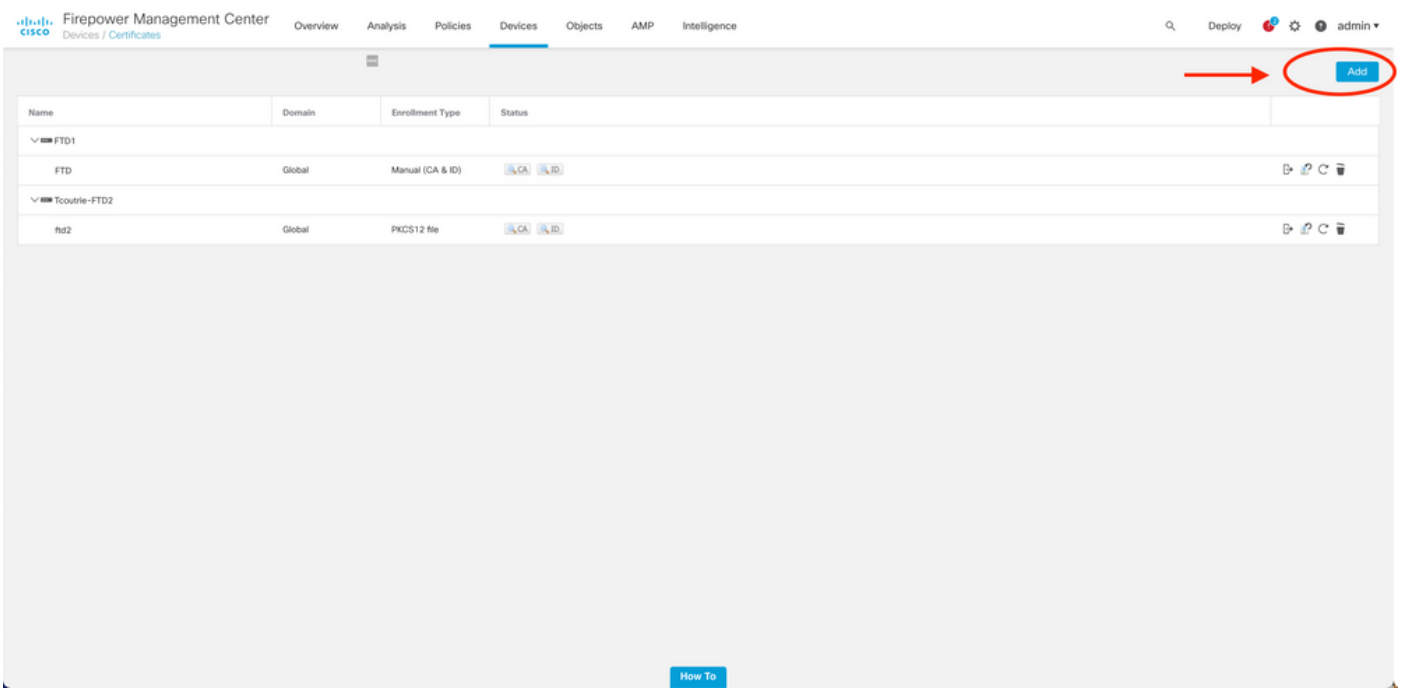
Cette section décrit les étapes à suivre pour configurer Anyconnect via FMC. Avant de commencer, assurez-vous de déployer toutes les configurations.

Diagramme du réseau

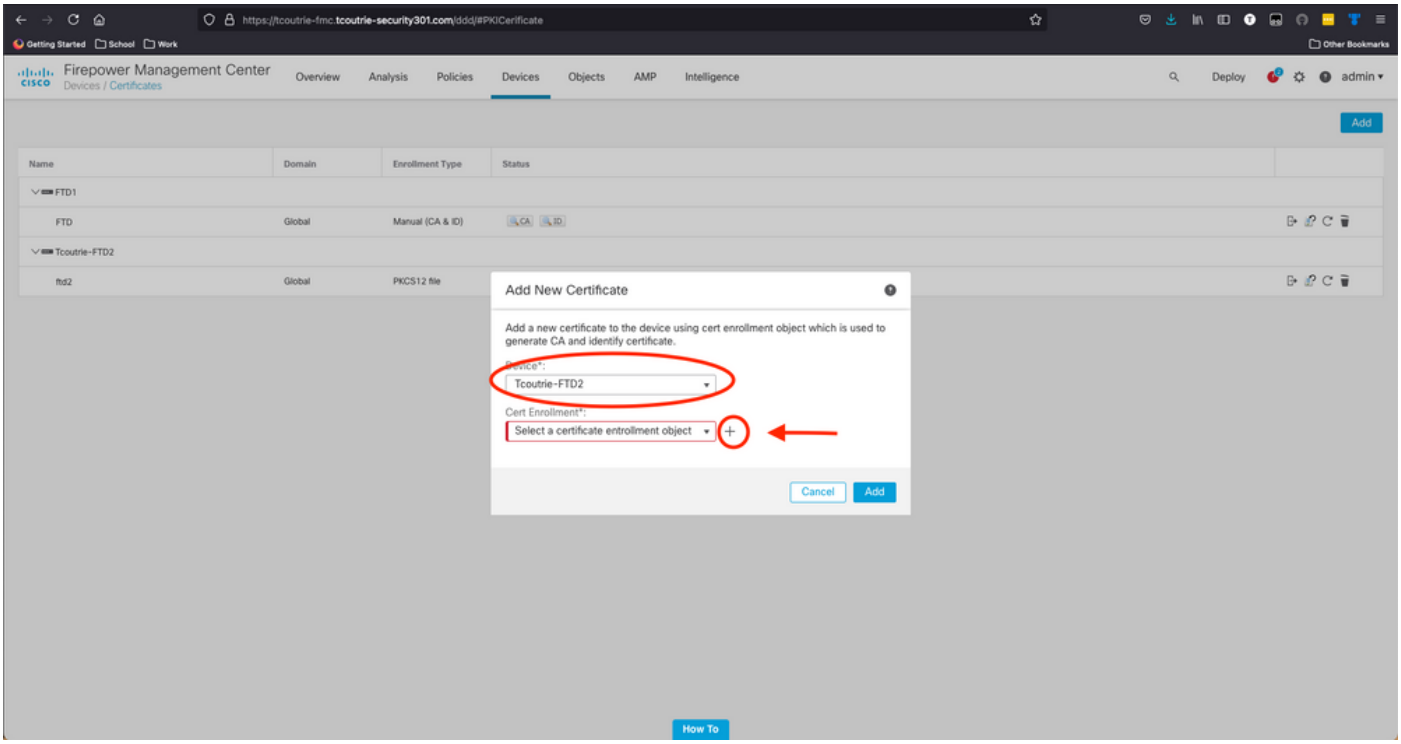


Ajouter un certificat au FTD

Étape 1. Créez un certificat pour le FTD sur l'appliance FMC. Accédez à Devices > Certificate et choisissez Add, comme illustré dans cette image :



Étape 2. Sélectionnez le FTD souhaité pour la connexion VPN. Sélectionnez le dispositif FTD dans la liste déroulante des périphériques. Cliquez sur l'icône + pour ajouter une nouvelle méthode d'inscription de certificat, comme illustré dans cette image :

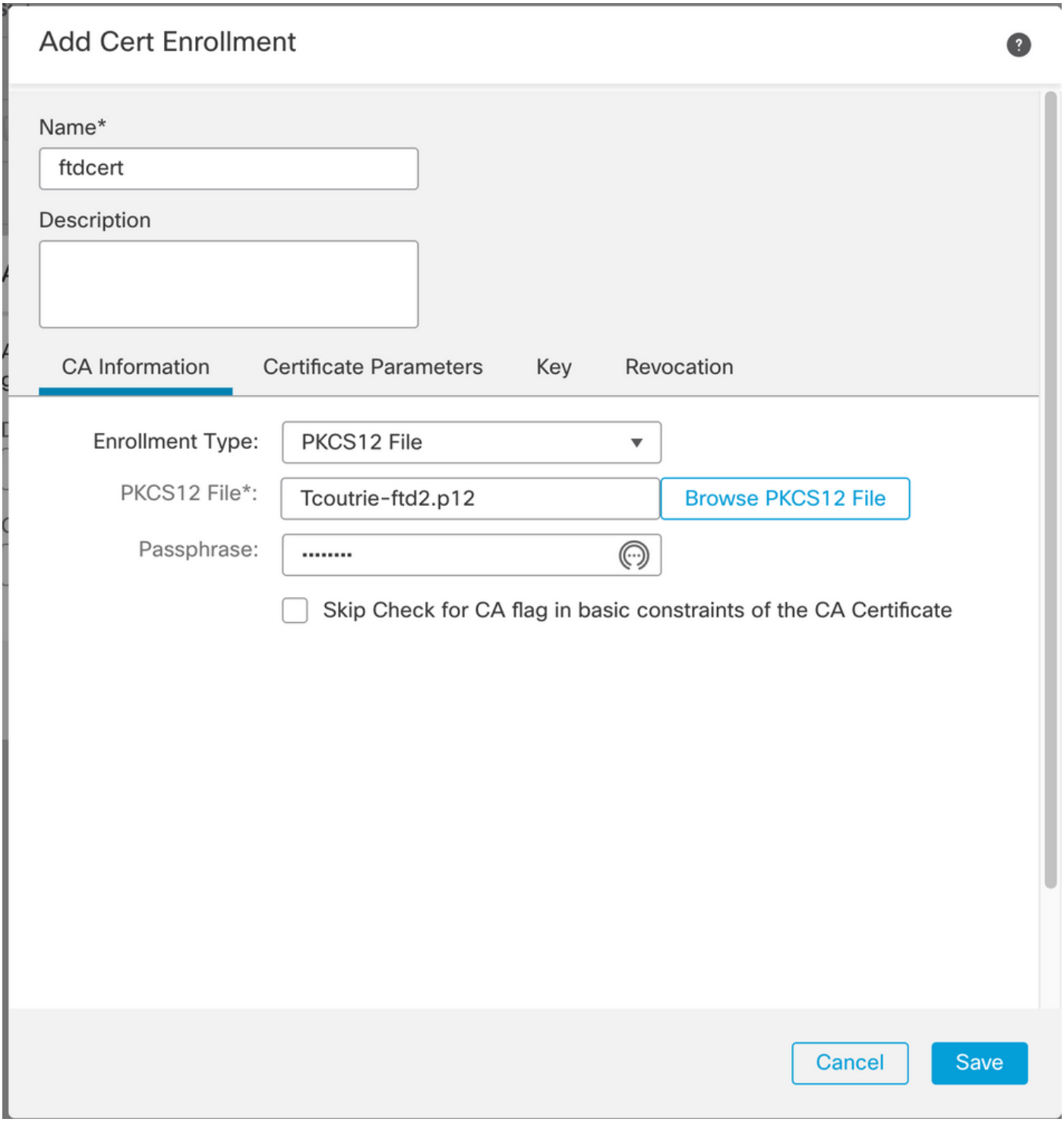


Étape 3. Ajoutez les certificats au périphérique. Choisissez l'option qui est la méthode préférée

pour obtenir des certificats dans l'environnement.

Conseil : les options disponibles sont les suivantes : Certificat auto-signé - Générer un nouveau certificat localement, SCEP - Utiliser le protocole d'inscription de certificat simple pour obtenir un certificat auprès d'une autorité de certification, Manuel - Installer manuellement le certificat racine et le certificat d'identité, PKCS12 - Charger le lot de certificats chiffrés avec la racine, l'identité et la clé privée.

Étape 4. Téléchargez le certificat sur le périphérique FTD. Entrez le code secret (PKCS12 uniquement) et cliquez sur Save, comme illustré dans cette image :



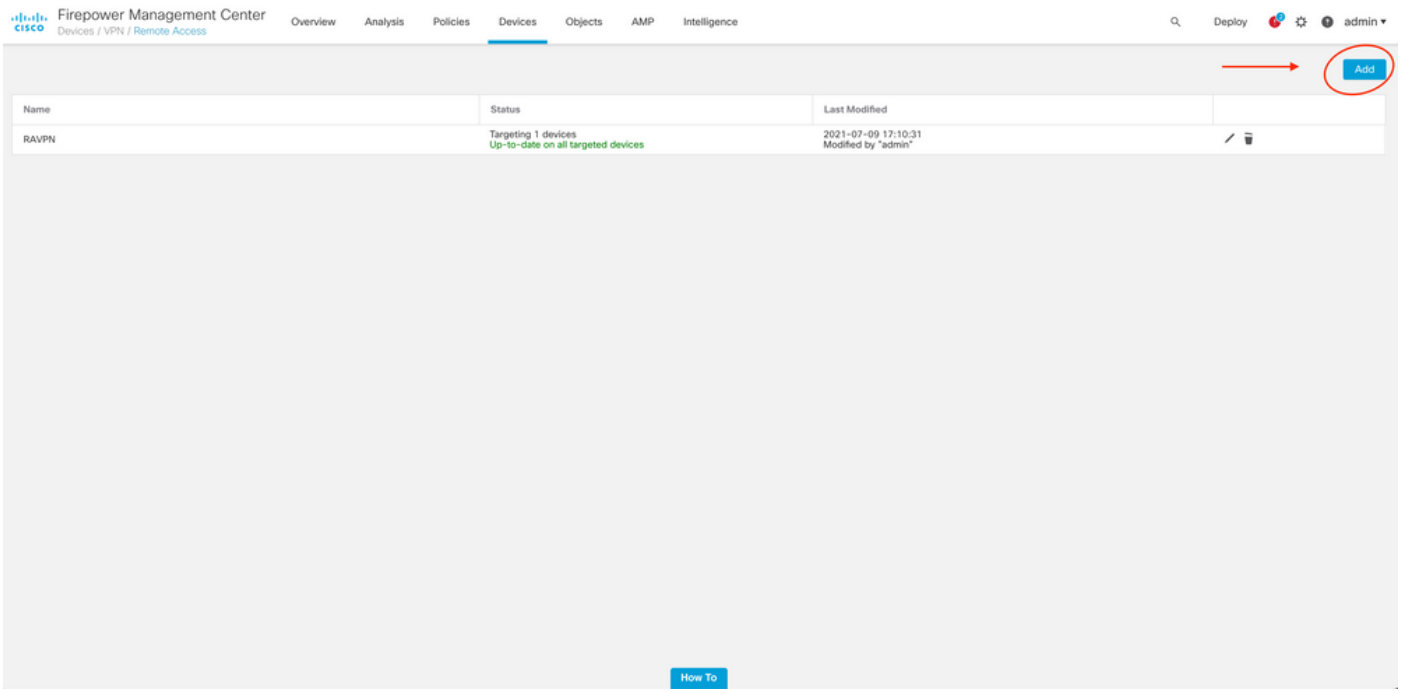
Remarque : une fois le fichier enregistré, le déploiement des certificats a lieu immédiatement. Pour afficher les détails du certificat, sélectionnez l'ID.

Configuration de Cisco Anyconnect

Configurez Anyconnect via FMC avec l'assistant d'accès à distance.

Étape 1. Démarrez l'assistant de stratégie VPN d'accès à distance pour configurer Anyconnect.

Accédez à Périphériques > Accès à distance et choisissez Ajouter.

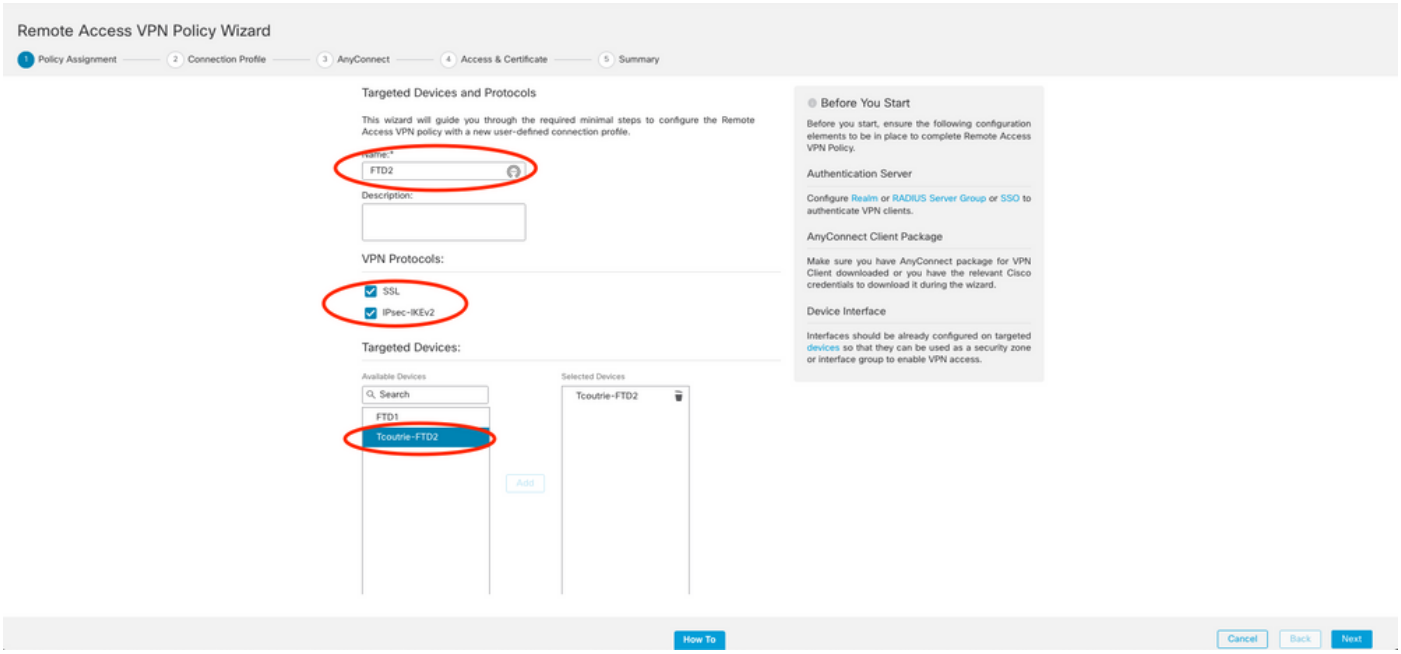


Étape 2. Affectation de stratégie.

Terminez l'affectation de la stratégie :
a. Nommez la stratégie.

b. Choisissez les protocoles VPN souhaités.

c. Choisissez le périphérique ciblé pour appliquer la configuration.

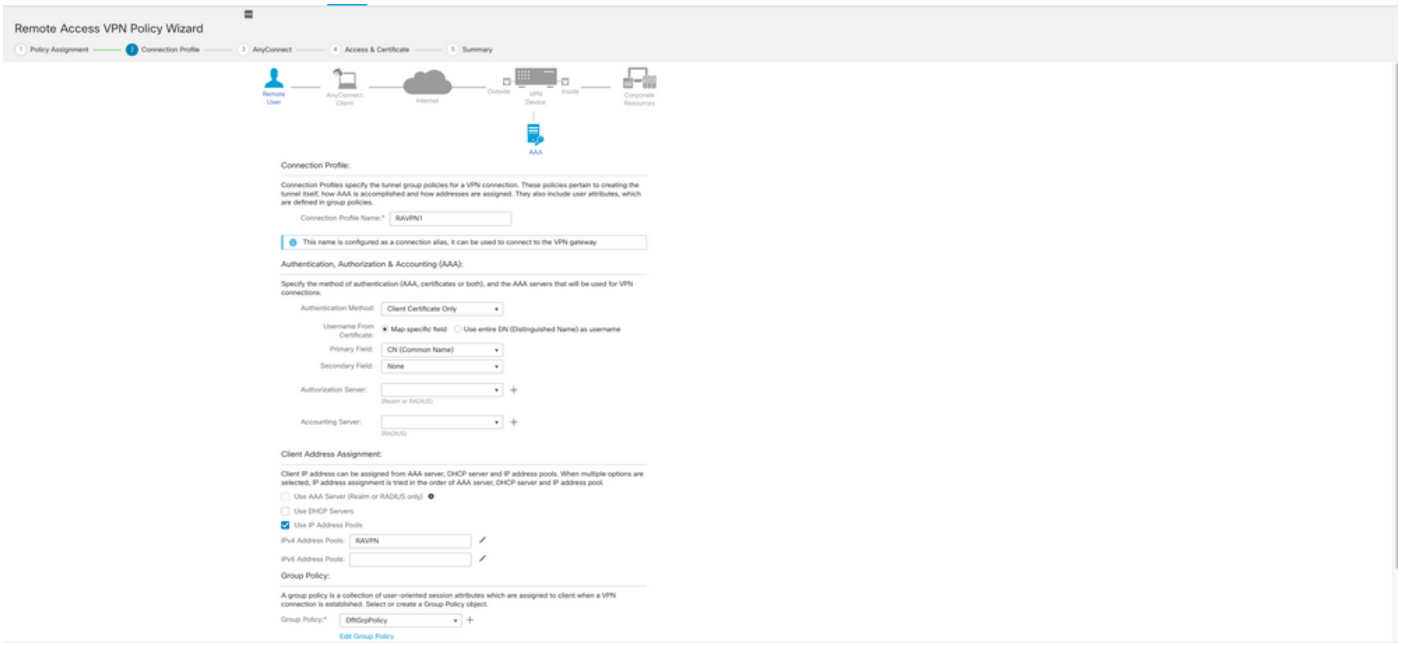


Étape 3. Profil de connexion.

a. Nommez le profil de connexion.
b. Définissez la méthode d'authentification sur Certificat client uniquement.

c. Attribuez un pool d'adresses IP et, si nécessaire, créez une nouvelle stratégie de groupe.

d. Cliquez sur Next.



Remarque : sélectionnez le champ principal à utiliser pour entrer le nom d'utilisateur des sessions d'authentification. Le CN du certificat est utilisé dans ce guide.

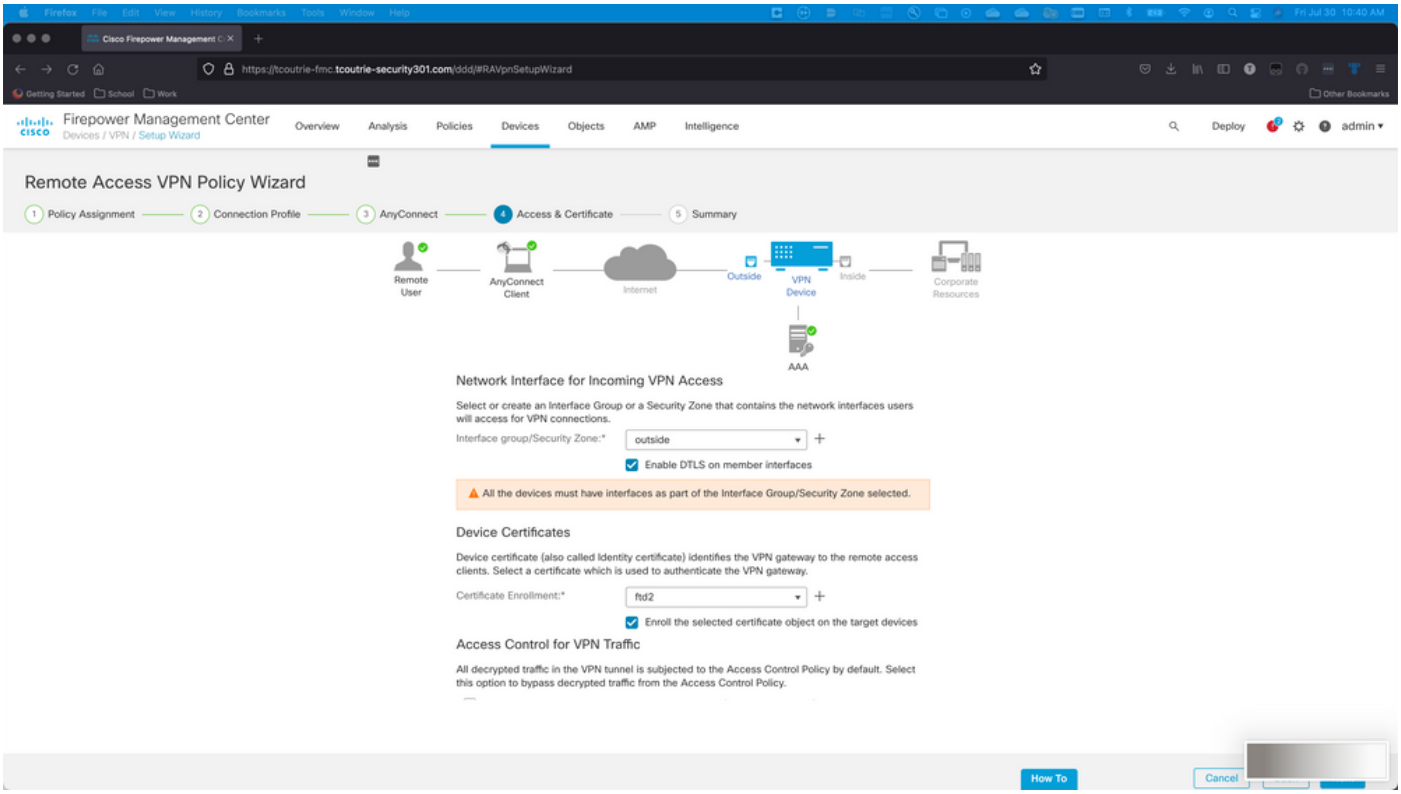
Étape 4. AnyConnect .

Ajoutez une image Anyconnect à l'appliance. Téléchargez la version préférée d'Anyconnect et cliquez sur Next.

Remarque : les packages Cisco Anyconnect peuvent être téléchargés à partir de Software.Cisco.com.

Étape 5. Accès et certificat.

Appliquez le certificat à une interface et activez Anyconnect au niveau de l'interface, comme illustré dans cette image, et cliquez sur Next.



Étape 6. Résumé.

Vérifiez les configurations. Si tous les extraient, cliquez sur Terminer, puis sur Déployer.

Créer un certificat pour les utilisateurs mobiles

Créez un certificat à ajouter au périphérique mobile utilisé dans la connexion.

Étape 1. XCA.

a. Ouvrir XCA

b. Démarrez une nouvelle base de données

Étape 2. Créer CSR.

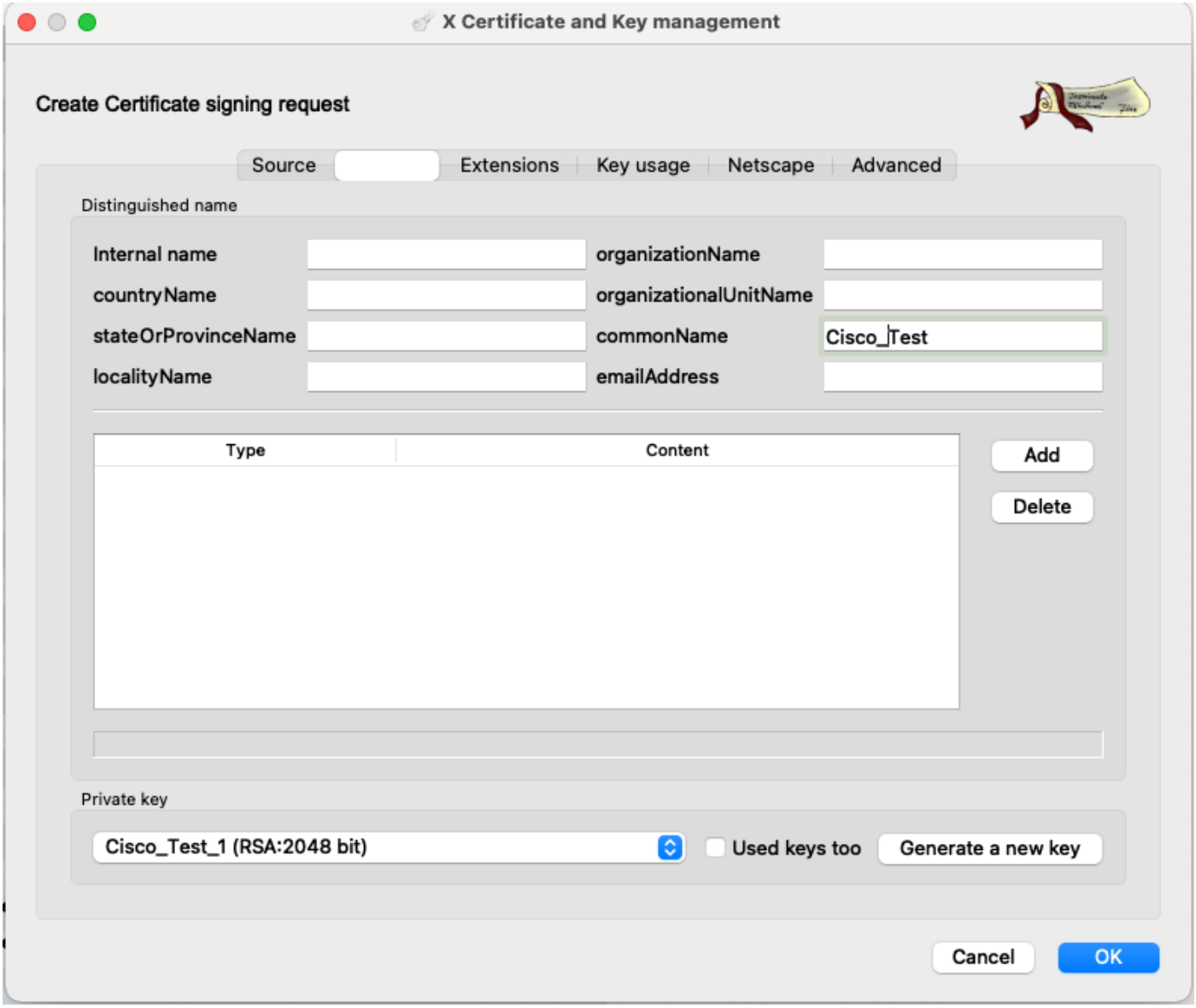
a. Sélectionnez Demande de signature de certificat (CSR)

b. Choisissez Nouveau traitement

c. Entrez la valeur avec toutes les informations requises pour le certificat

d. Générez une nouvelle clé

e. Lorsque vous avez terminé, cliquez sur OK

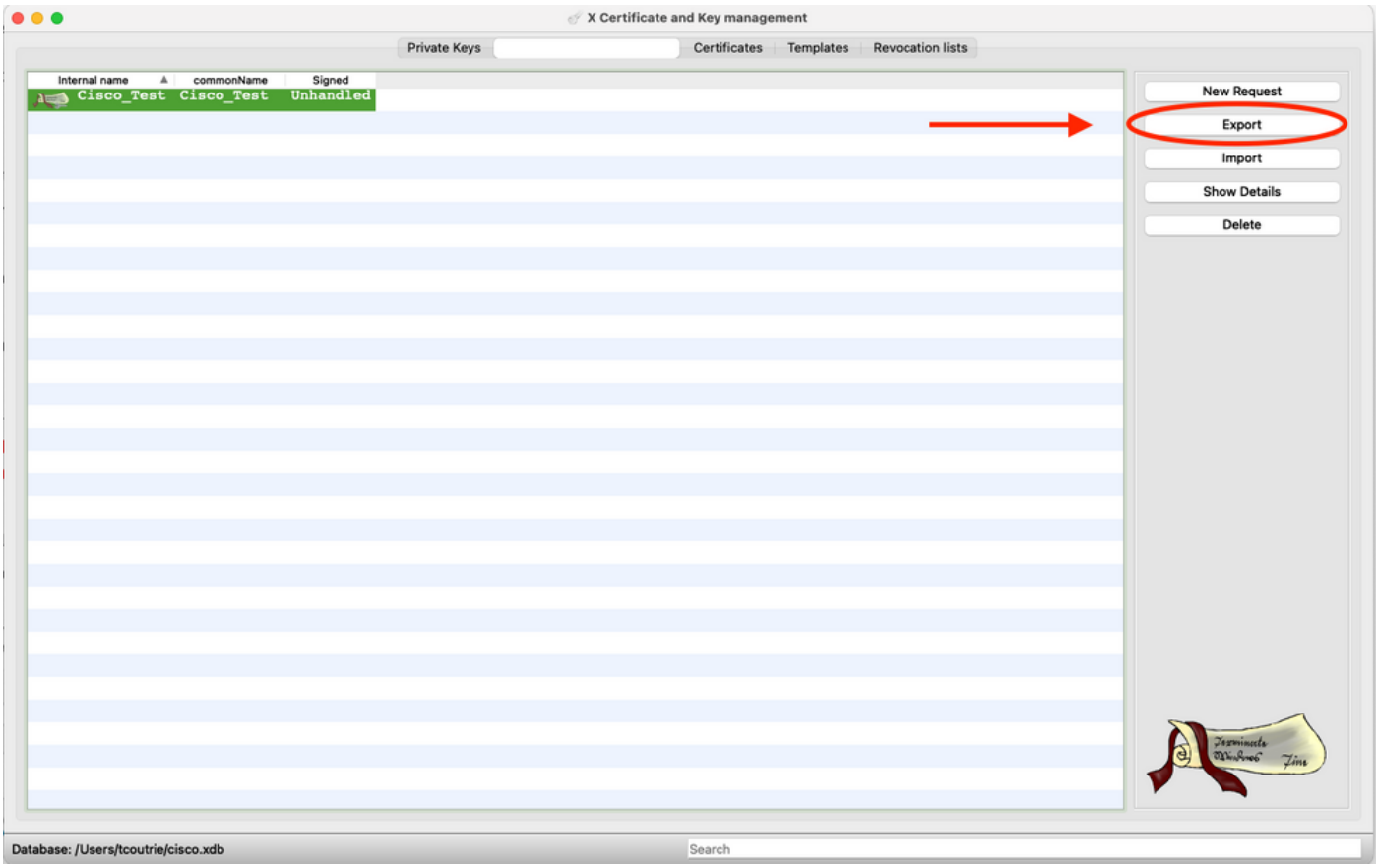


Remarque : ce document utilise le CN du certificat.

Étape 3. Envoyer un CSR

a. Exporter le CSR

b. Soumettre un CSR à l'AC pour obtenir un nouveau certificat

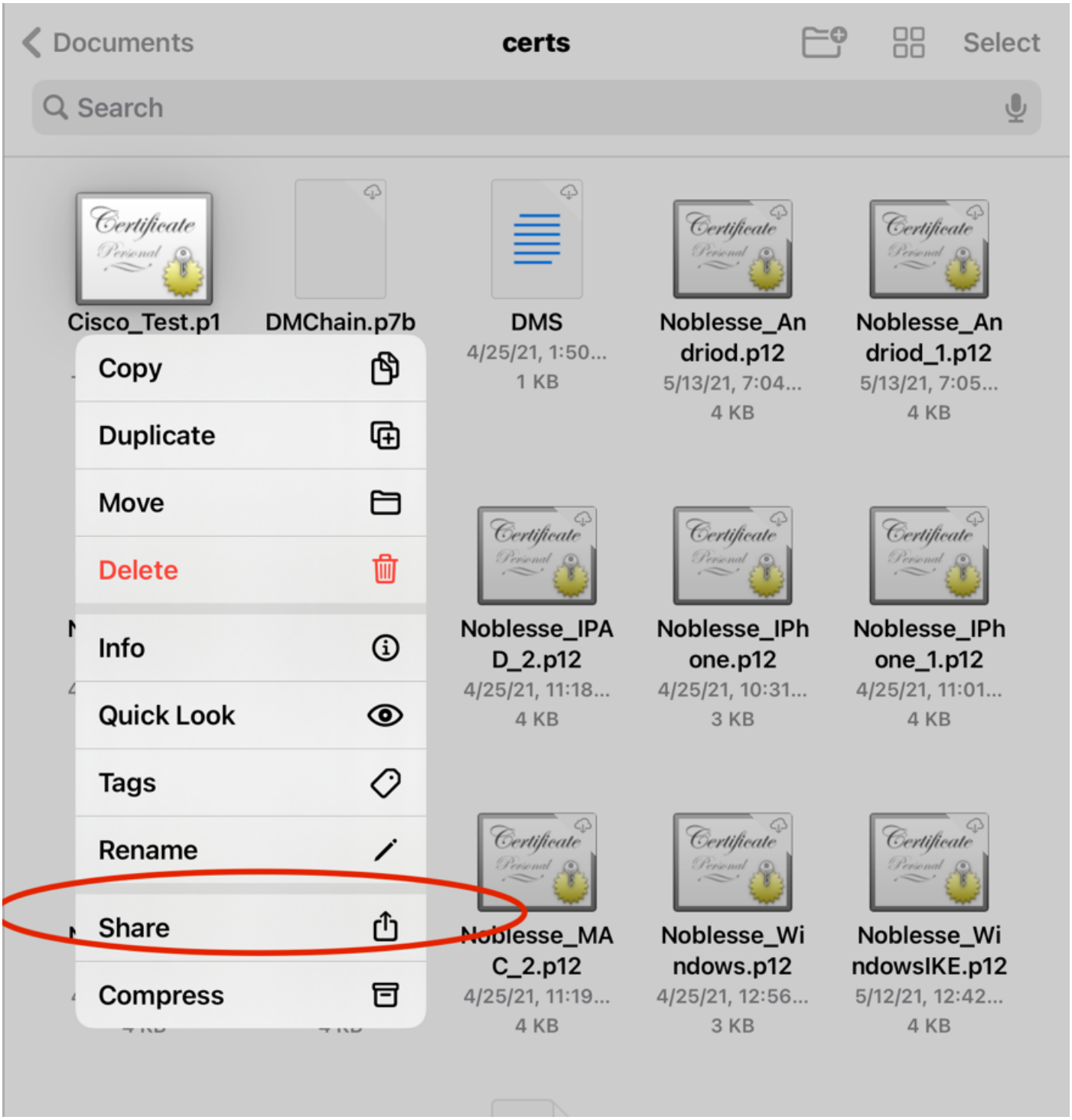


Remarque : utilisez le format PEM du CSR.

Installation sur un appareil mobile

Étape 1. Ajoutez le certificat du périphérique à l'appareil mobile.
Étape 2. Partagez le certificat avec l’application Anyconnect pour ajouter la nouvelle application de certificat.

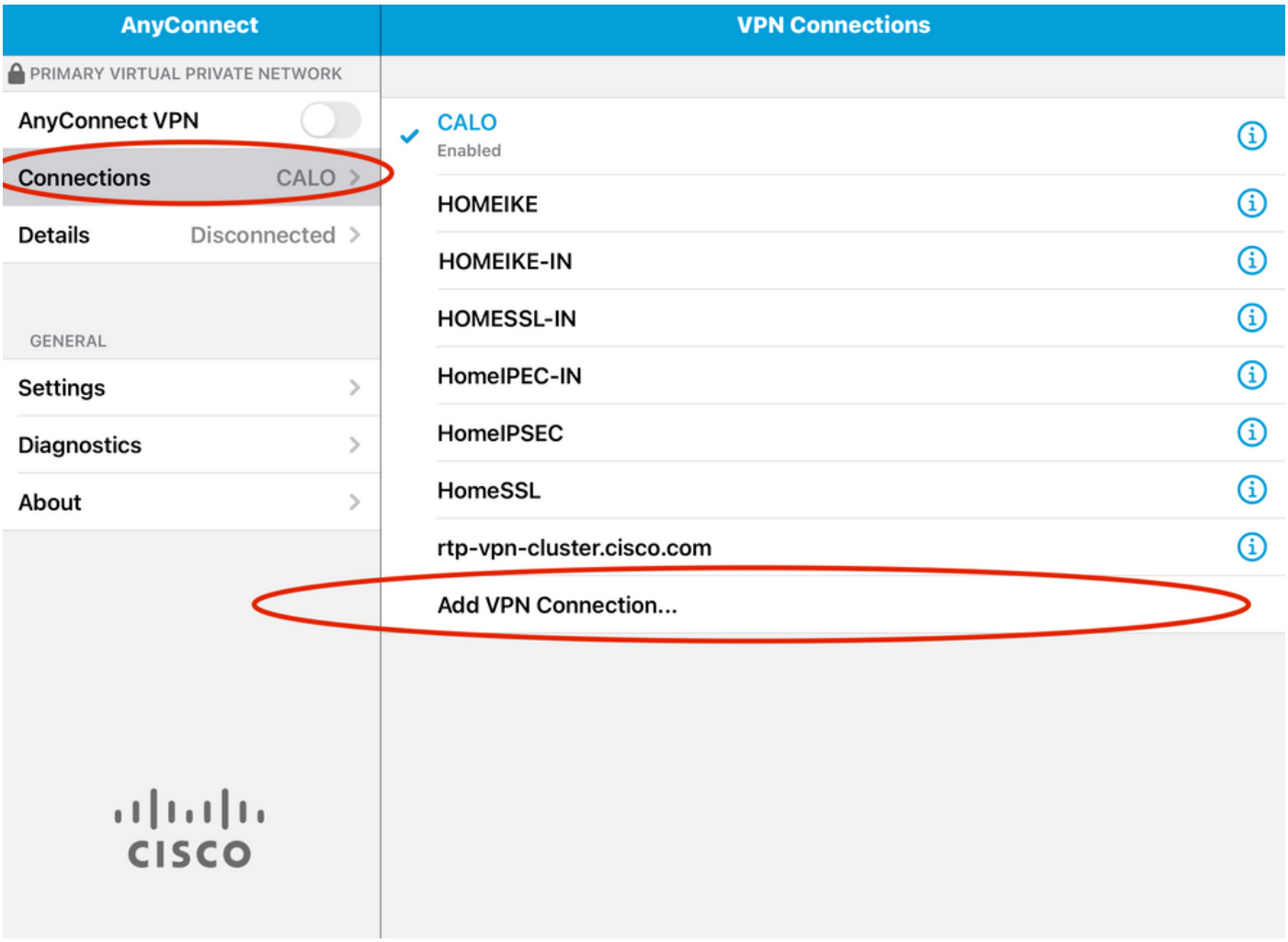
Attention : l'installation manuelle nécessite que l'utilisateur partage le certificat avec l'application. Cela ne s'applique pas aux certificats transmis via des MDM.



Étape 3. Entrez le mot de passe du certificat pour le fichier PKCS12.

Étape 4. Créez une nouvelle connexion sur Anyconnect.

Étape 5. Accédez à de nouvelles connexions ; Connexions > Ajouter une connexion VPN.



Étape 6. Saisissez les informations relatives à la nouvelle connexion.

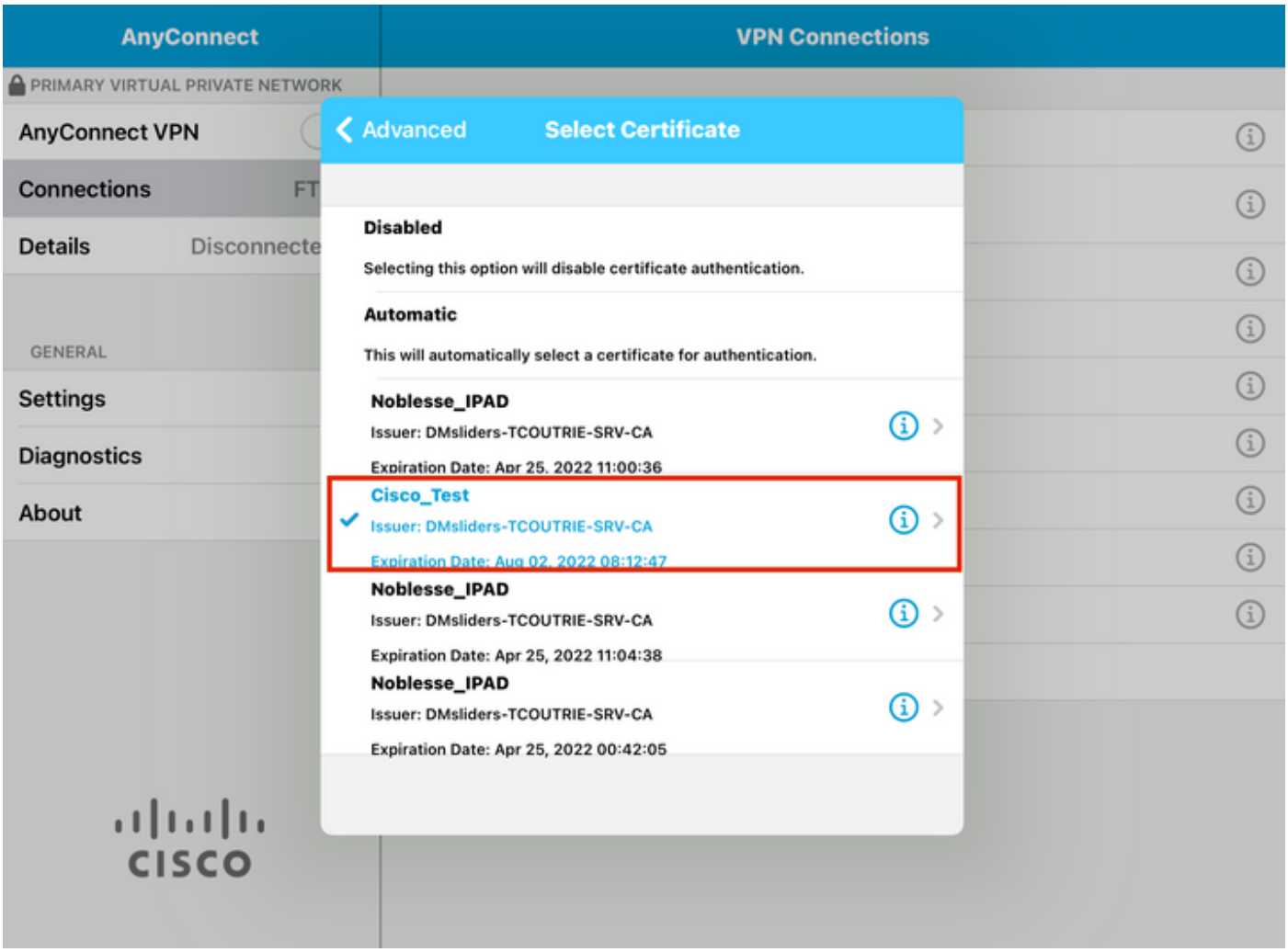
Description : Nommez la connexion

Adresse du serveur : adresse IP ou nom de domaine complet de FTD

Avancé : configurations supplémentaires

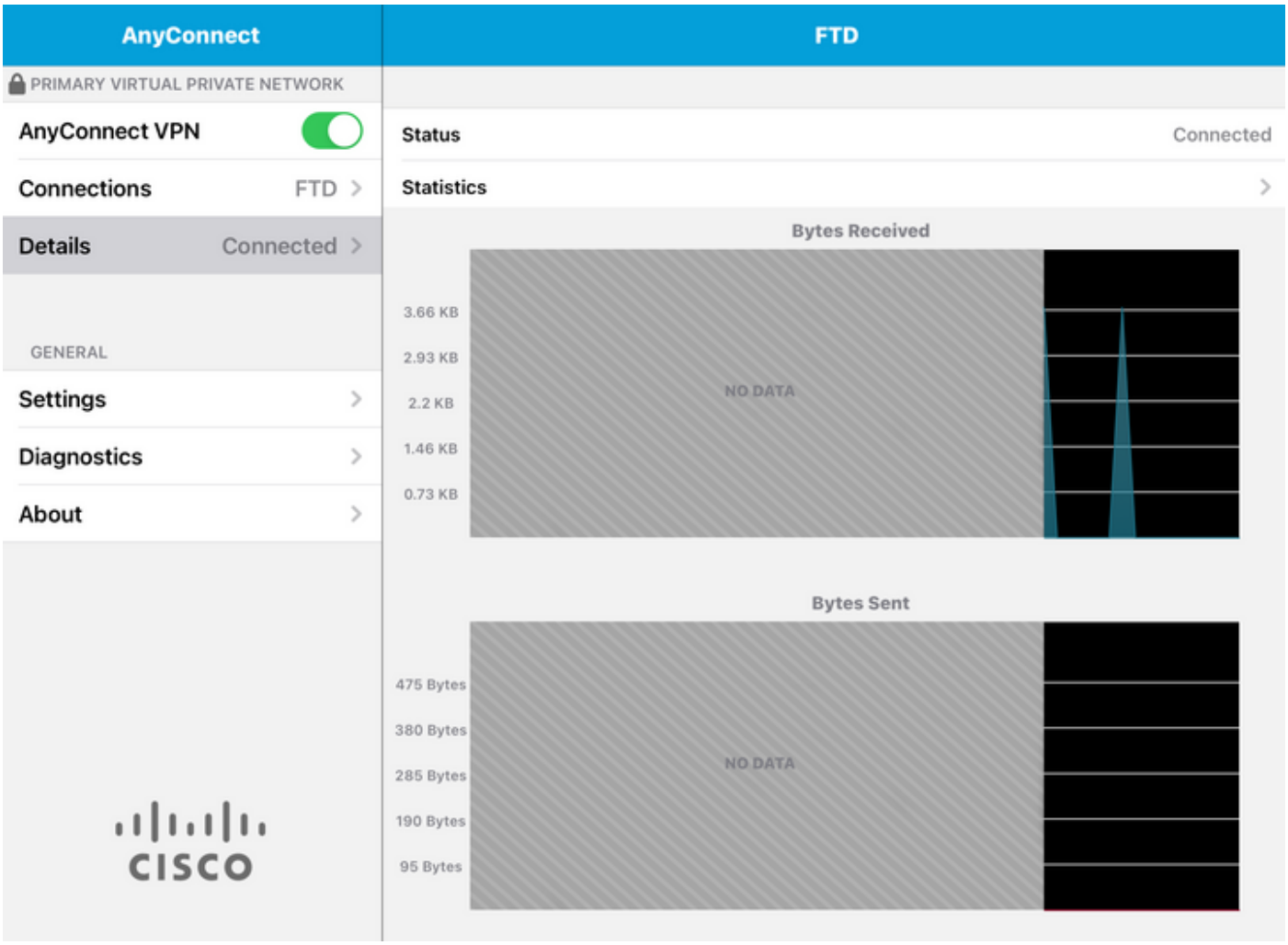
Étape 7. Sélectionnez Avancé.

Étape 8. Choisissez Certificate et choisissez votre nouveau certificat ajouté.



Étape 9. Revenez à Connexions et testez.

Une fois l'opération terminée, la bascule reste activée et les détails apparaissent connectés dans l'état.



Vérifier

La commande show vpn-sessiondb detail Anyconnect affiche toutes les informations sur l'hôte connecté.

Conseil : l'option permettant de filtrer davantage cette commande est les mots-clés « filter » ou « sort » ajoutés à la commande.

Exemple :

```
Tcoutrie-FTD3# show vpn-sessiondb detail Anyconnect


Username : Cisco_Test Index : 23
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel
License : Anyconnect Premium, Anyconnect for Mobile
Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 8627 Bytes Rx : 220
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

```
Group Policy : SSL Tunnel Group : SSL
Login Time : 13:03:28 UTC Mon Aug 2 2021
Duration : 0h:01m:49s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a7aa95d000170006107ed20
Security Grp : none Tunnel Zone : 0

Anyconnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

Anyconnect-Parent:
Tunnel ID : 23.1
Public IP : 10.118.18.168
Encryption : none Hashing : none
TCP Src Port : 64983 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : apple-ios
Client OS Ver: 14.6
Client Type : Anyconnect
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 6299 Bytes Rx : 220
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 23.2
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 64985
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : SSL VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 2328 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 23.3
Assigned IP : 10.71.1.2 Public IP : 10.118.18.168
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 51003
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Apple iOS
Client Type : DTLS VPN Client
Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Dépannage

Déboguages

Les débogages requis pour résoudre ce problème sont les suivants :

```
Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255
```

Si la connexion est IPSEC et non SSL :

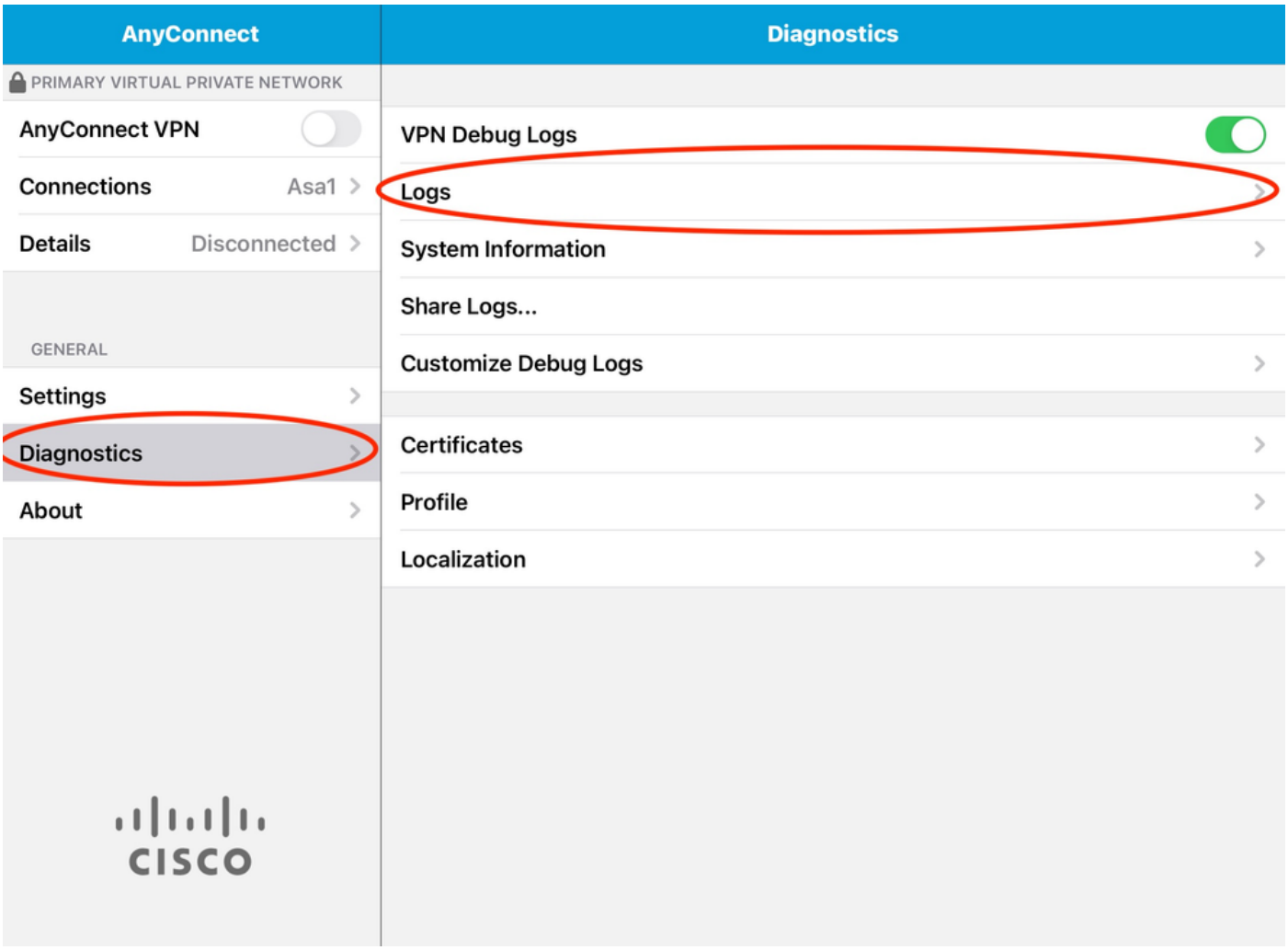
```
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14
```

Journaux de l'application mobile Anyconnect :

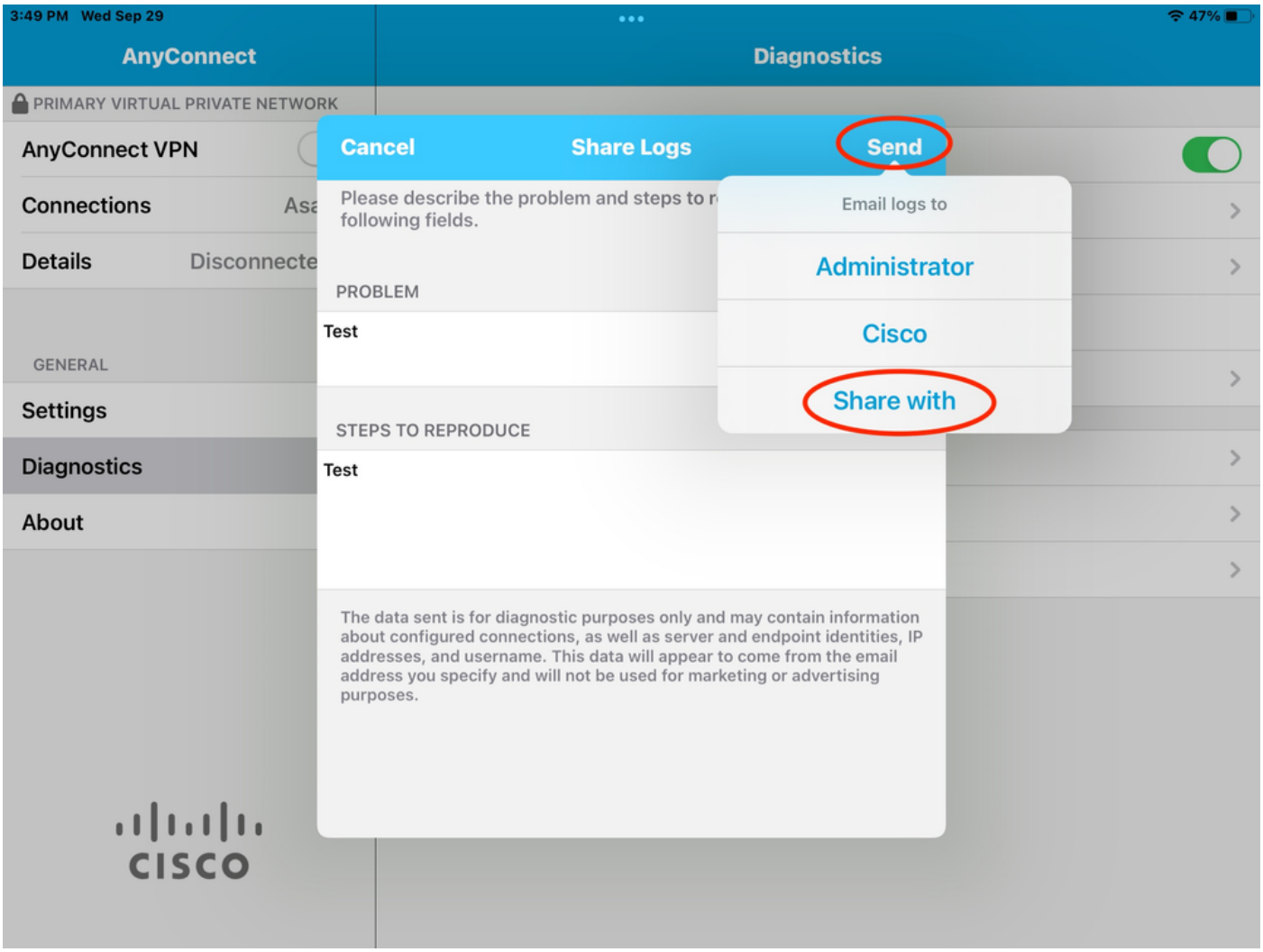
Accédez à Diagnostic > VPN Debug Logs > Share logs.



Saisissez les informations suivantes :

- Problème
- Étapes à reproduire

Accédez ensuite à Send > Share with.



Cette option permet d'utiliser un client de messagerie pour envoyer les journaux.

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.