Configurer l'authentification de certificat client sécurisé sur FTD géré par FMC

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configurations
    - Créer/importer un certificat utilisé pour l'authentification du serveur
    - Ajouter un certificat CA approuvé/interne
    - Configurer le pool d'adresses pour les utilisateurs VPN
    - Télécharger des images client sécurisées
    - Créer et télécharger un profil XML
  - Configuration VPN d'accès à distance
- Vérifier
- Dépannage

Introduction

Ce document décrit la configuration du VPN d'accès à distance sur FTD géré par FMC avec l'authentification de certificat.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FMC
- Connaissances de base en authentification pour VPN d'accès à distance
- Inscription manuelle des certificats et connaissances de base sur SSL (Secure Sockets Layer)
- Autorité de certification tierce (CA), telle que Entrust, Geotrust, GoDaddy, Thawte et VeriSign

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- FMC version 7.4.1
- Client sécurisé version 5.0.05040
- Défense contre les menaces Secure Firepower version 7.4.1
- Microsoft Windows Server 2019 en tant que serveur AC

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

Diagramme du réseau

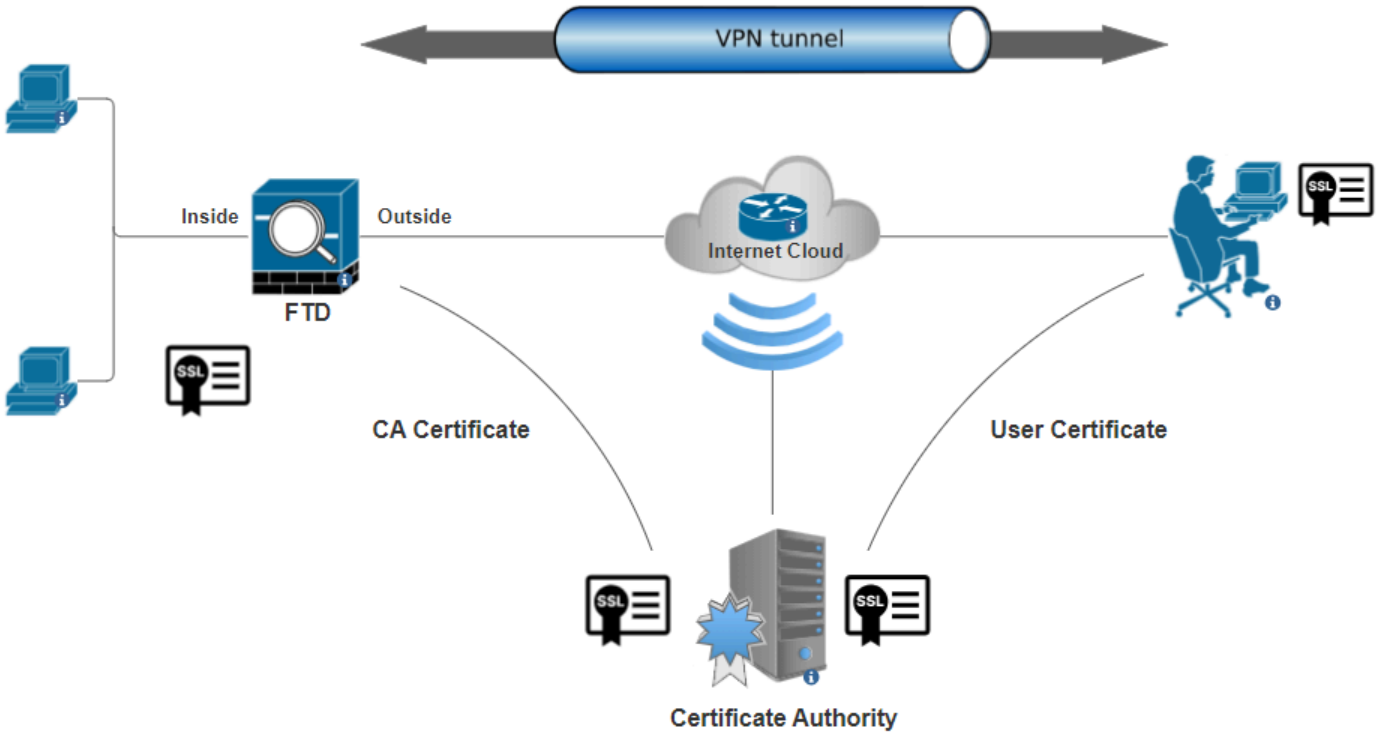


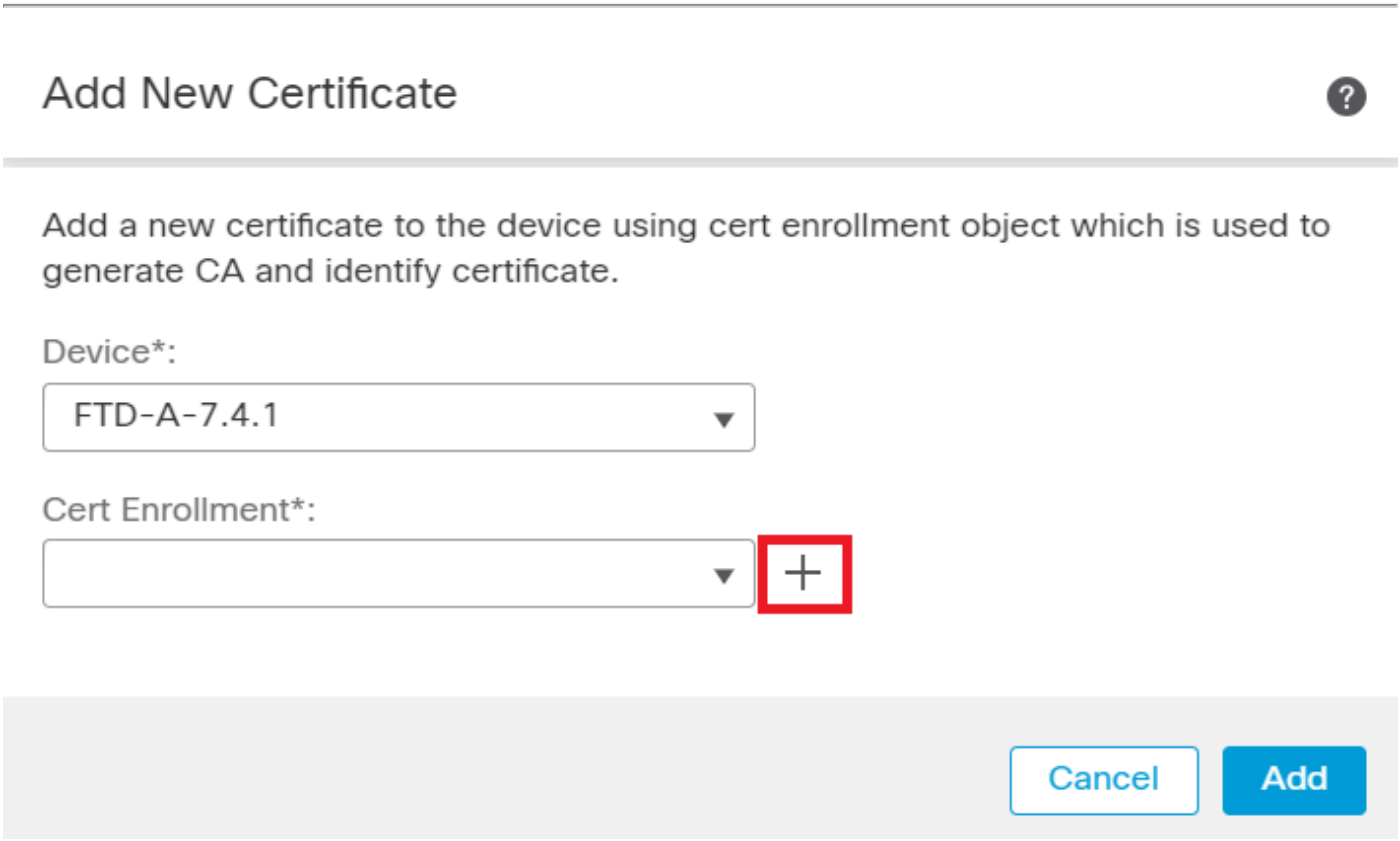
Diagramme du réseau

Configurations

Créer/importer un certificat utilisé pour l'authentification du serveur

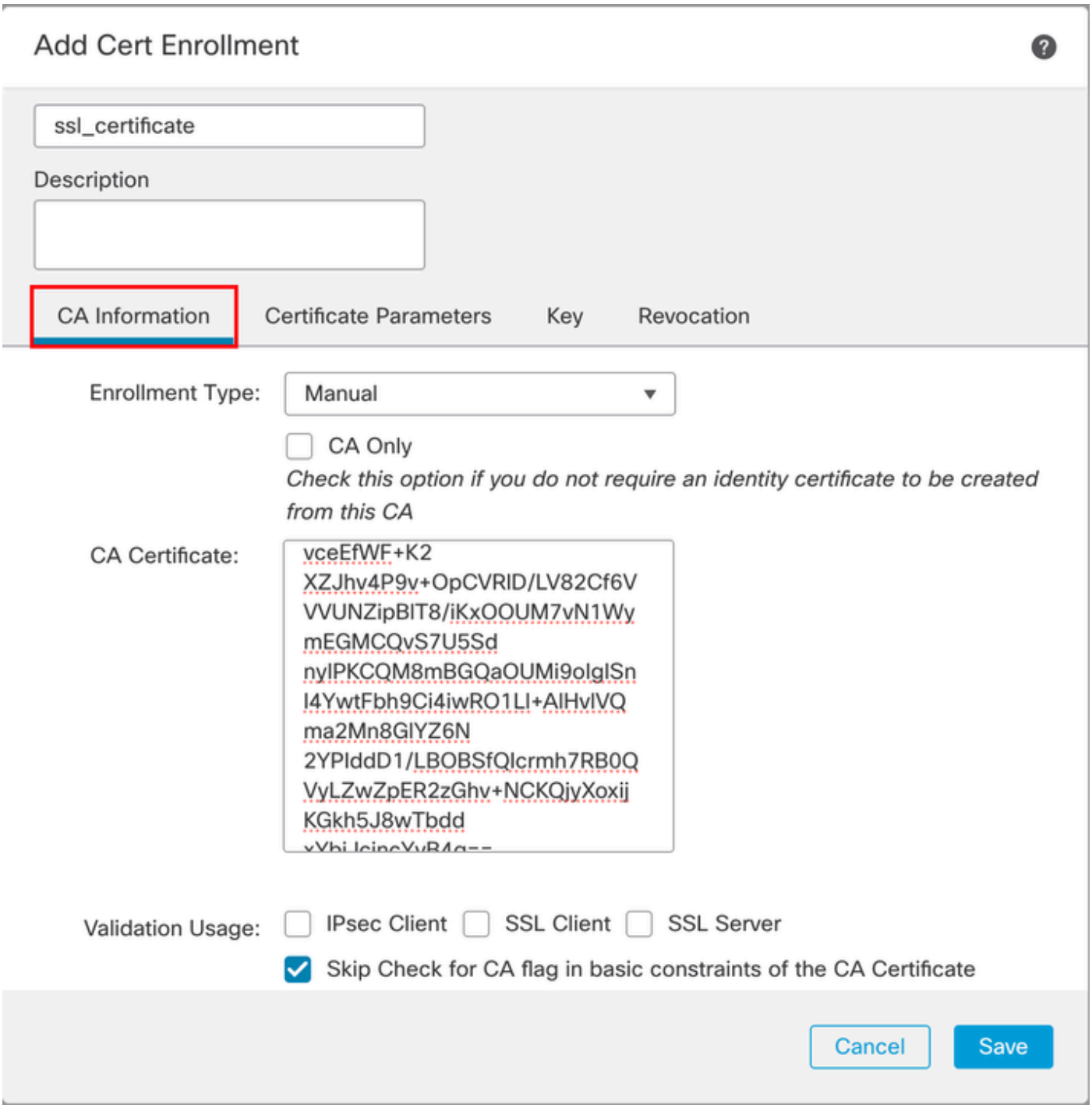
Remarque : Sur FMC, une autorité de certification (CA) est requise avant de pouvoir générer le CSR. Si le CSR est généré à partir d'une source externe (OpenSSL ou tierce partie), la méthode manuelle échoue et le format de certificat PKCS12 doit être utilisé.

1. Accédez à Périphériques > Certificats et cliquez sur Ajouter. Choisissez Device et cliquez sur le signe plus (+) sous Cert Enrollment.



Ajouter une inscription de certificat

2. Sous CA Information, sélectionnez le type d'inscription Manual et collez le certificat CA utilisé pour signer le CSR.



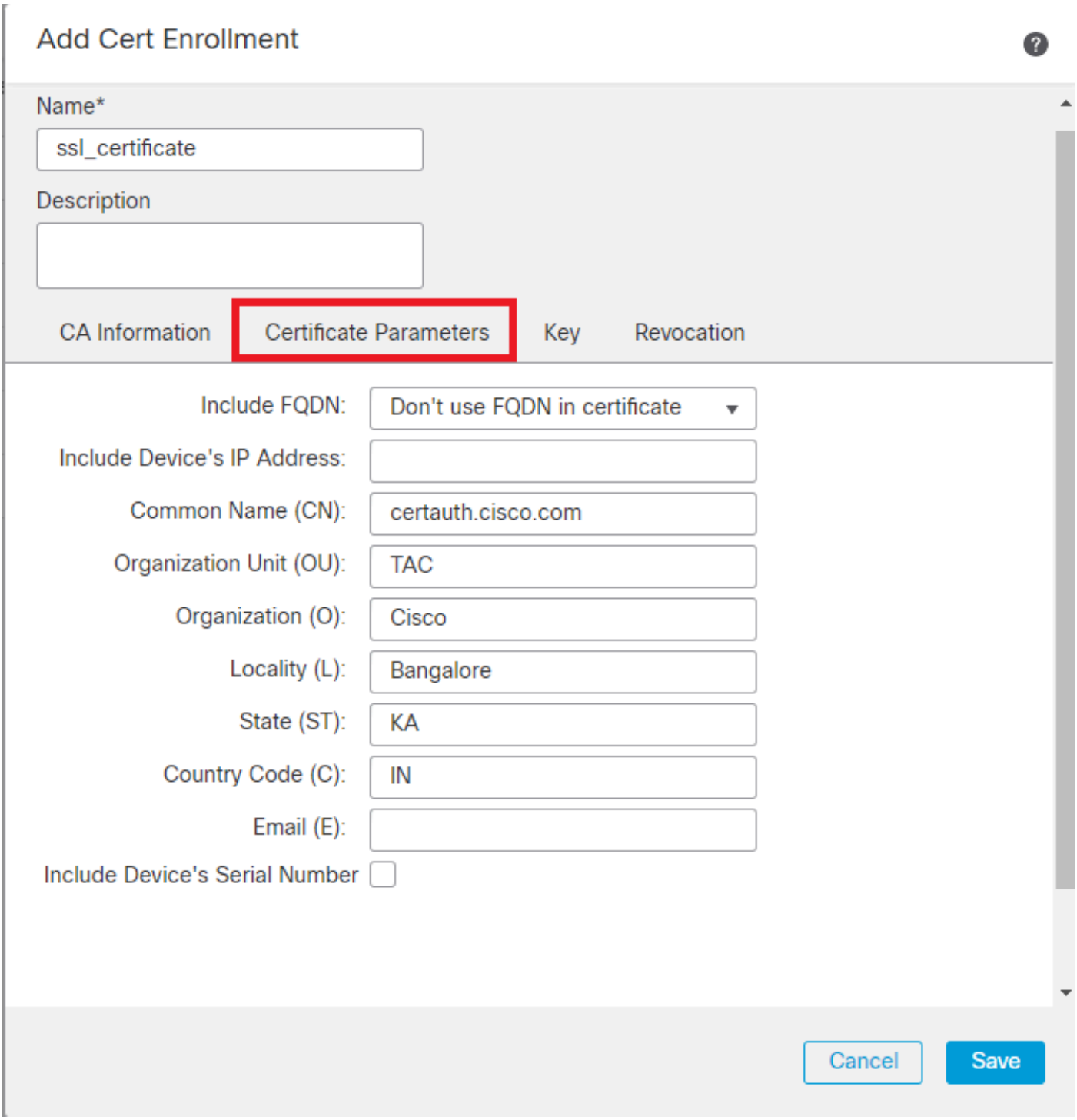
Ajouter des informations CA

---

3. Choisissez Ignorer la vérification de l'indicateur CA dans les contraintes de base du certificat CA as shown in the prior image.

---

4. Sous Certificate Parameters, renseignez les détails du nom du sujet.

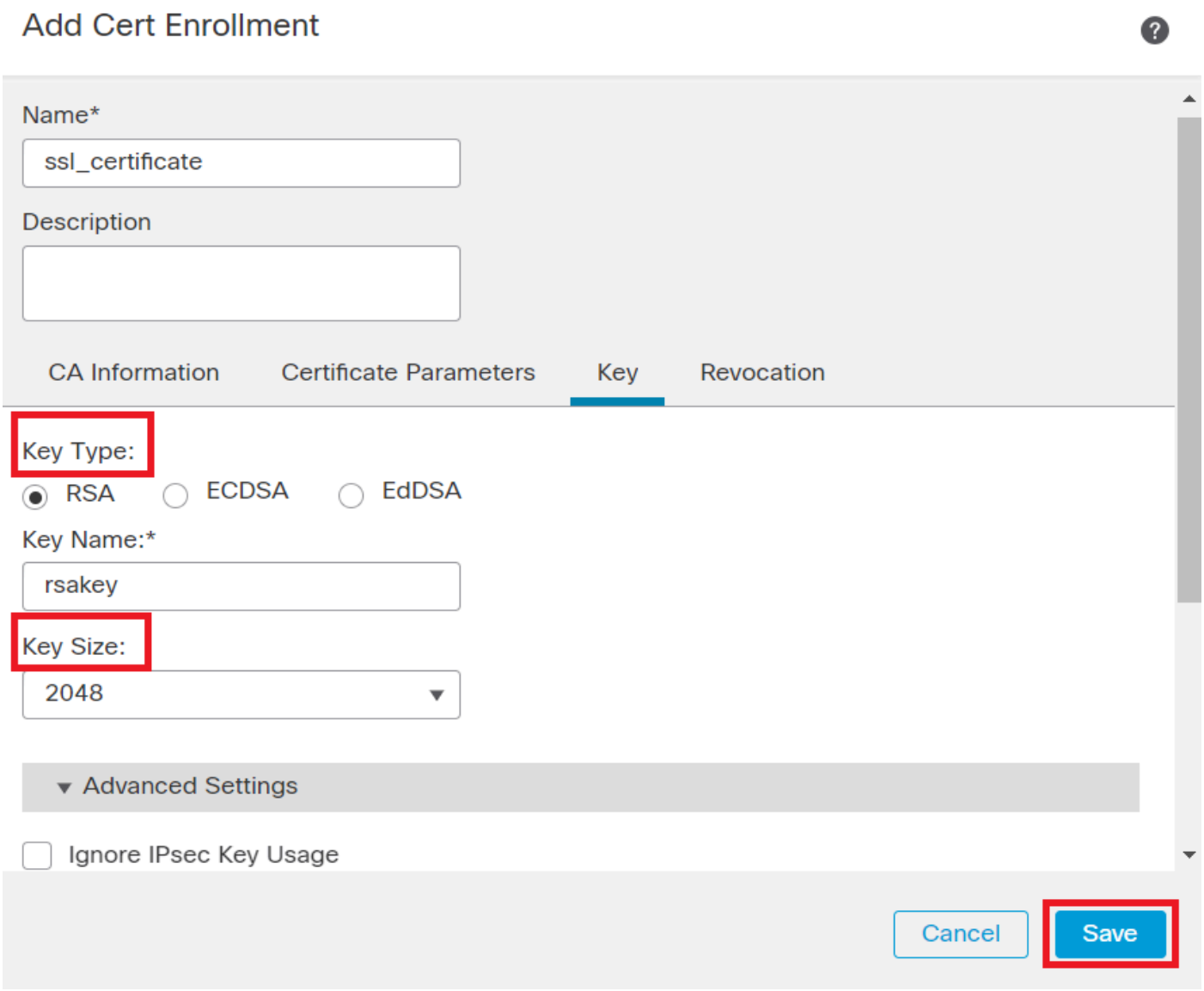


Ajouter des paramètres de certificat

---

5. Sous Clé, choisissez le type de clé RSA avec un nom et une taille de clé. Cliquez surSave.

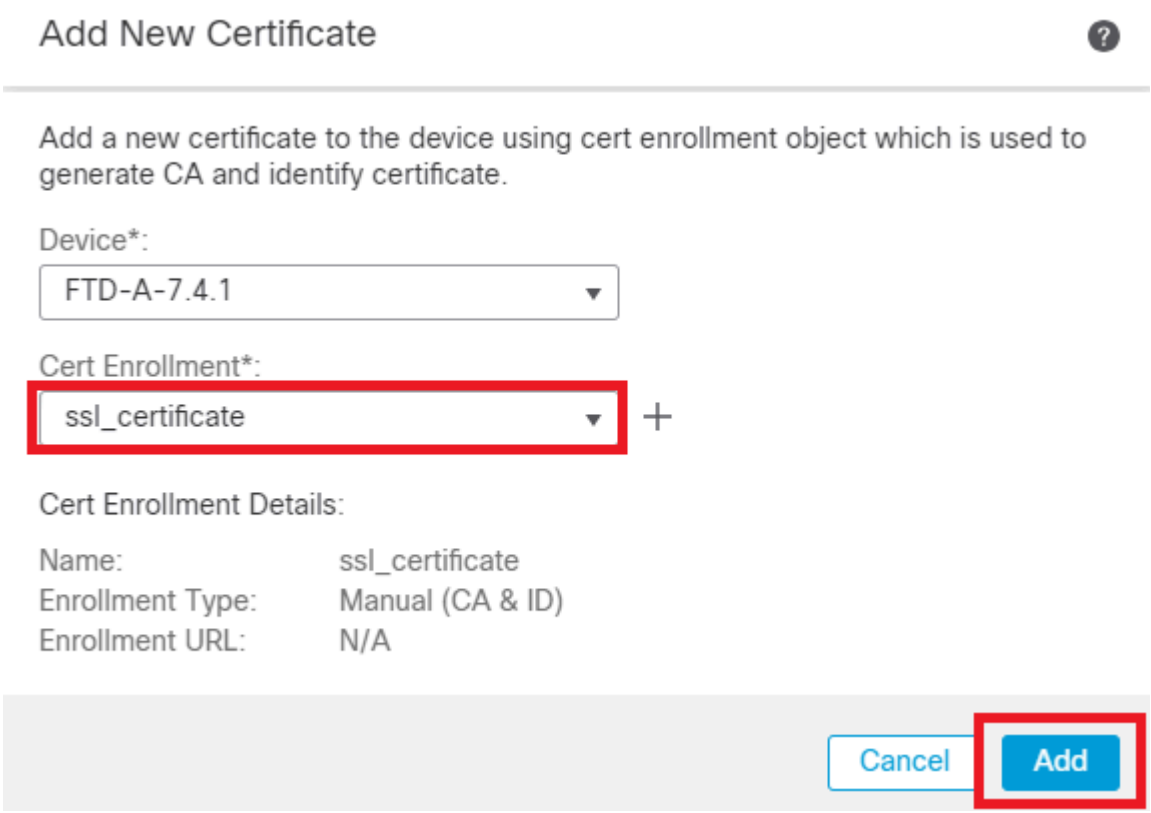
Remarque : Pour le type de clé RSA, la taille de clé minimale est de 2 048 bits.



Ajouter une clé RSA

---

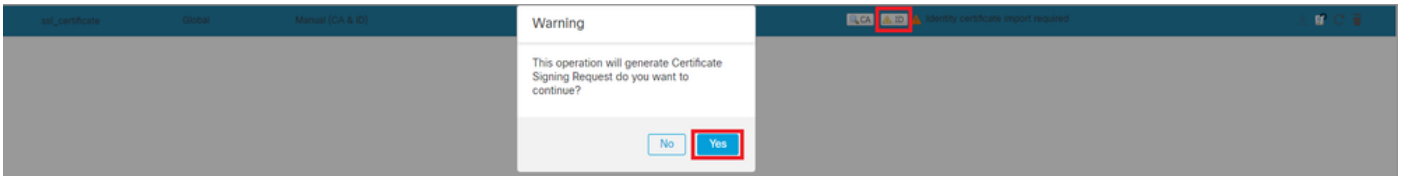
6. Sous Inscription de certificat, choisissez le point de confiance dans le menu déroulant, qui vient d'être créé, puis cliquez sur Ajouter.



Ajouter un nouveau certificat

---

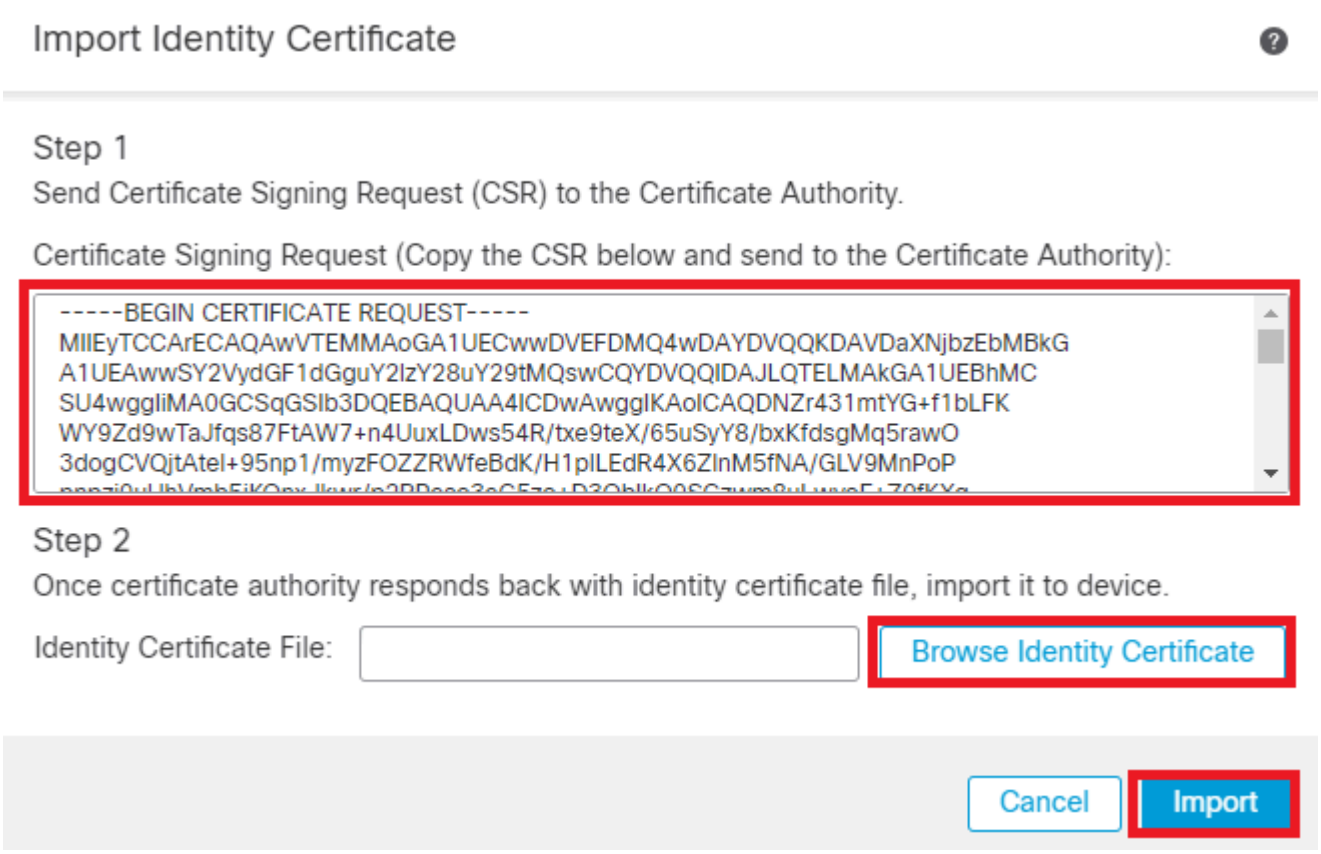
7. Cliquez sur ID, puis sur Yes, pour générer le CSR.



Générer CSR

---

8. Copier le REA et s'assurer qu'il est signé par l'AC. Une fois que le certificat d'identité est émis par l'autorité de certification, importez-le en cliquant sur Browse Identity Certificate et cliquez sur Import.



Importer le certificat ID

Remarque : Si l'émission du certificat d'ID prend du temps, vous pouvez répéter l'étape 7. ultérieurement. Cela génère le même CSR et vous pouvez importer le certificat d'ID.

Ajouter un certificat CA approuvé/interne

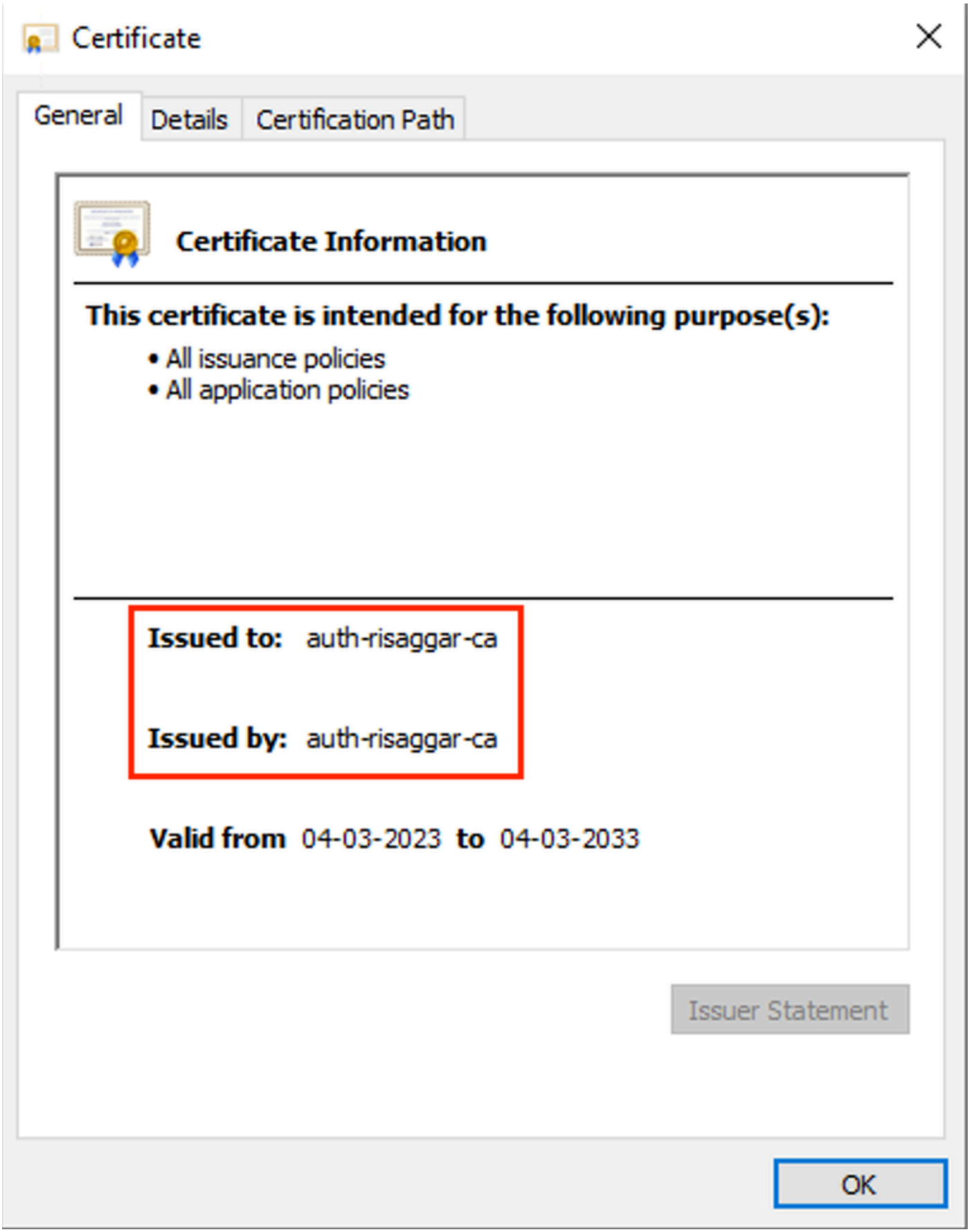
1. Accédez à Périphériques > Certificats et cliquez sur Ajouter.

---

2. Choisissez Device et cliquez sur le signe plus (+) sous Cert Enrollment.

---

3. Dans cet exemple, auth-risaggar-ca est utilisé pour émettre les certificats d'identité/d'utilisateur.



auth-risaggar-ca

---

4. Entrez un nom de point de confiance et choisissez Manuel comme type de souscription sous

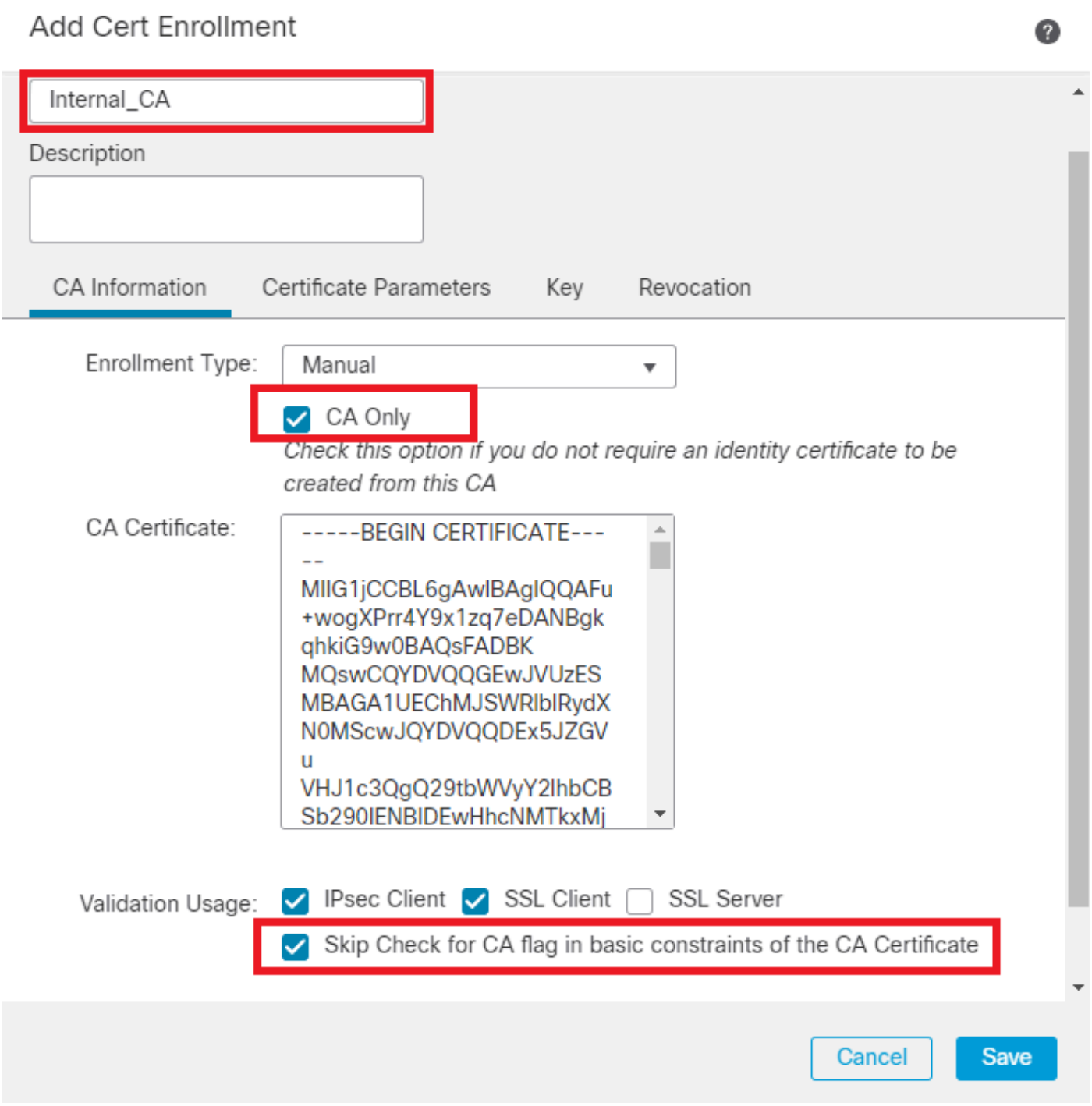
Informations CA.

---

5. Cochez CA Only et collez le certificat CA approuvé/interne au format pem.

---

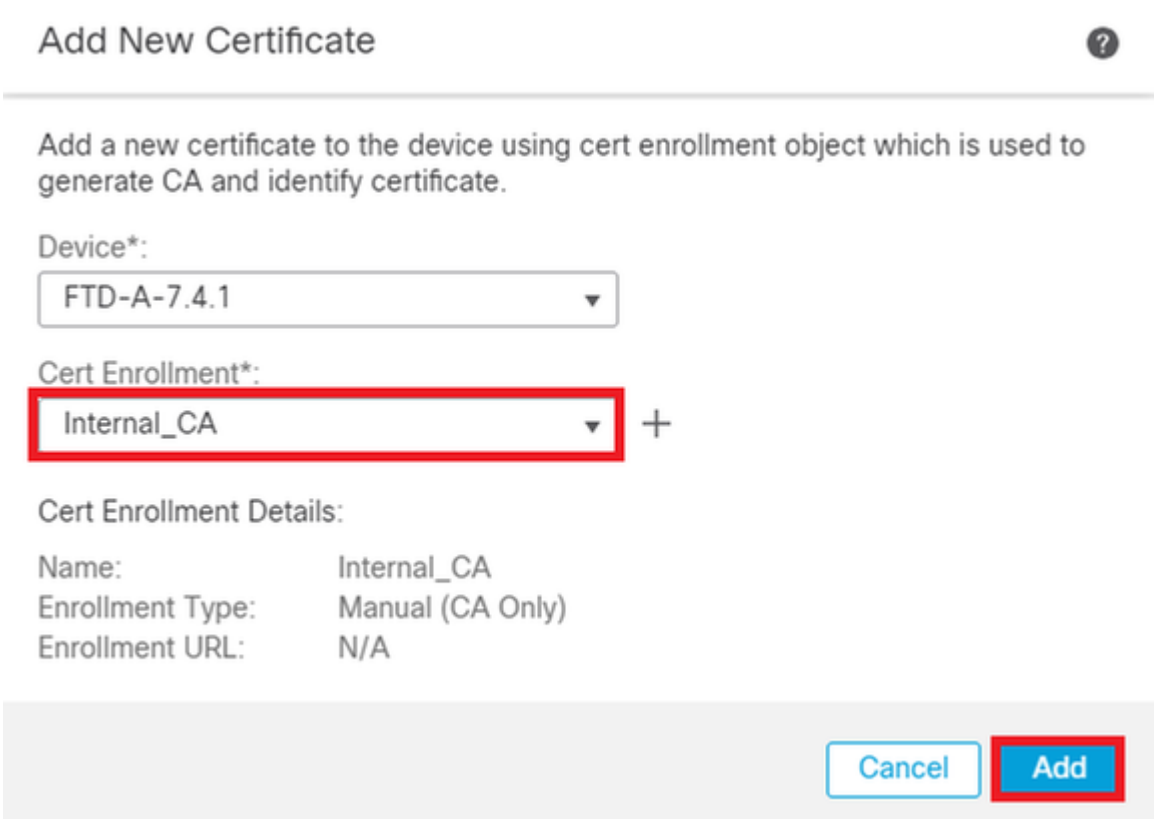
6. Cochez la case Ignorer la vérification de l'indicateur CA dans les contraintes de base du certificat CA et cliquez sur Save.



Ajouter un point de confiance

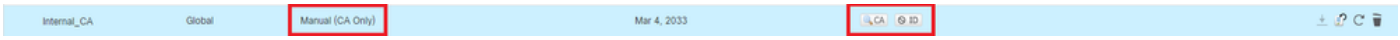
---

7. Sous Inscription de certificat, sélectionnez le point de confiance dans le menu déroulant, qui vient d'être créé, puis cliquez sur Add.



Ajouter une autorité de certification interne

8. Le certificat ajouté précédemment s'affiche comme suit :

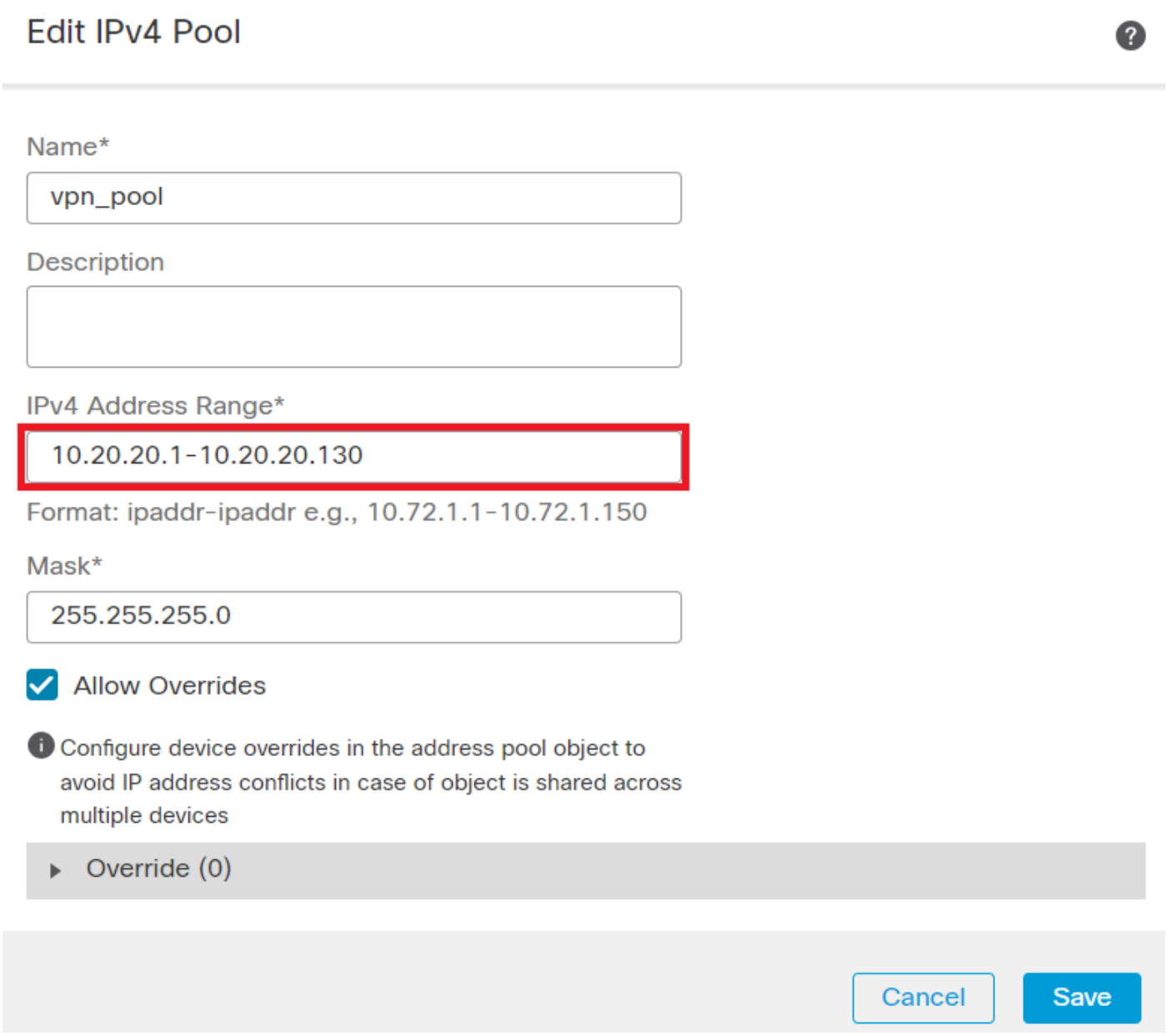


Certificat ajouté

Configurer le pool d'adresses pour les utilisateurs VPN

1. Accédez à Objets > Gestion des objets > Pools d'adresses > Pools IPv4.

2. Entrez le nom et la plage d'adresses IPv4 avec un masque.



Ajouter un pool IPv4

Télécharger des images client sécurisées

1. Téléchargez des images client sécurisées de déploiement Web par système d'exploitation à partir du site Cisco Software.

---

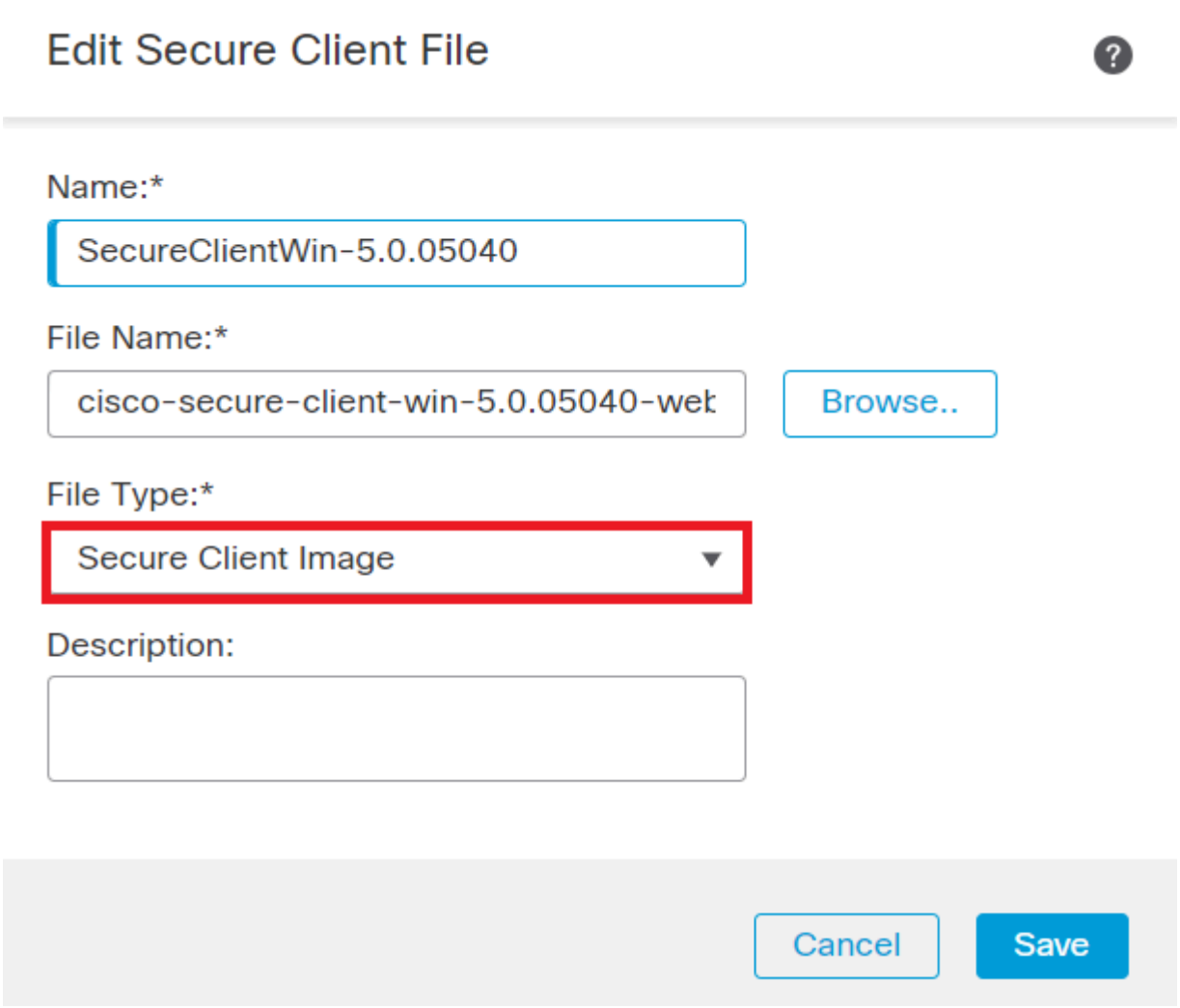
2. Accédez à Objects > Object Management > VPN > Secure Client File > Add Secure Client File.

---

3. Entrez le nom et choisissez le fichier Secure Client sur le disque.

---

4. Choisissez le type de fichier Secure Client Image et cliquez sur Save.



Ajouter une image de client sécurisé

Créer et télécharger un profil XML

1. Téléchargez et installez Secure Client Profile Editor à partir du site Cisco Software.

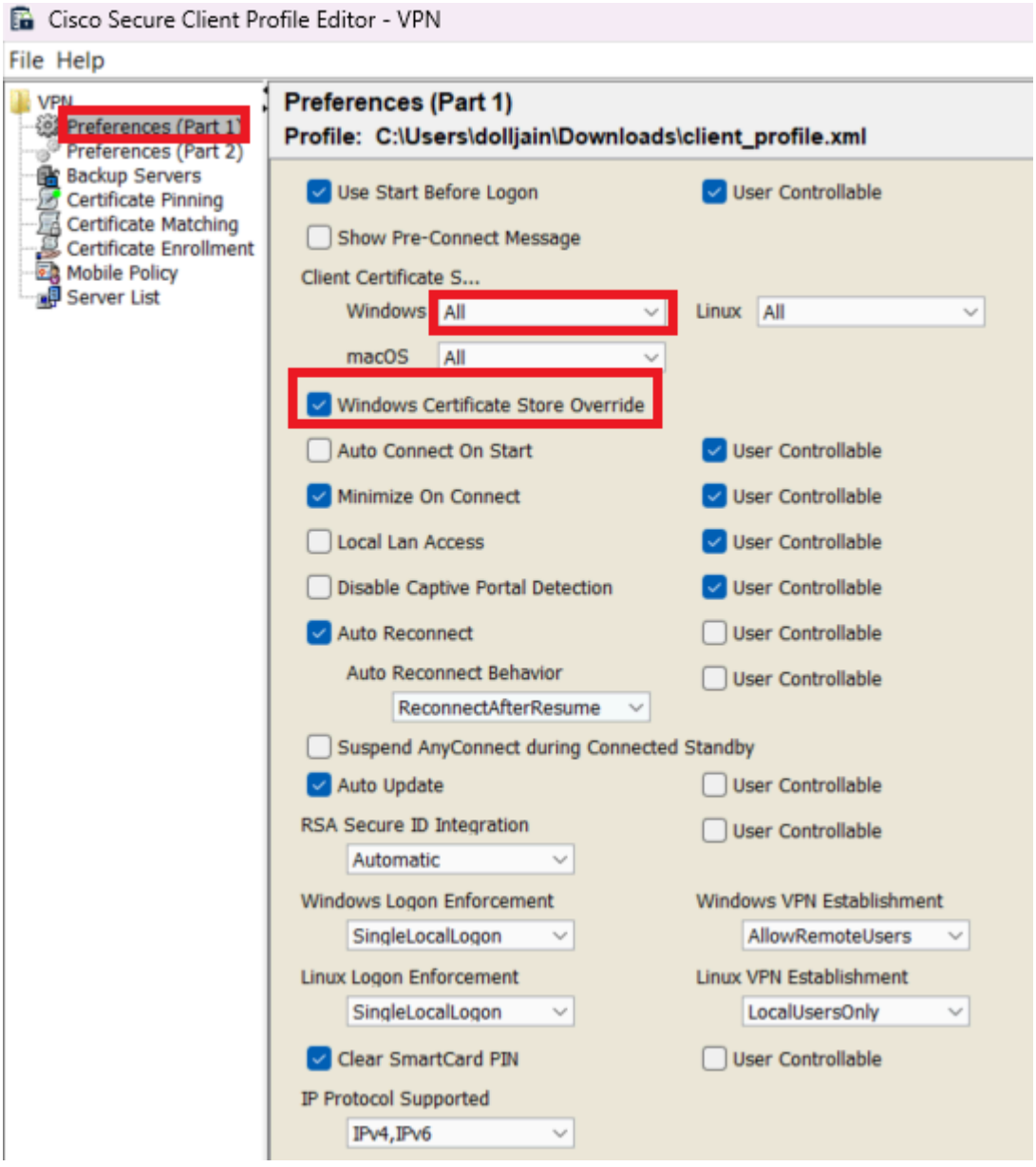
2. Créez un nouveau profil et choisissez All dans le menu déroulant Client Certificate Selection. Cela contrôle principalement quel certificat est stocké et quel certificat Secure Client peut utiliser pour en fonction de ce qui a été stocké et pour lire les certificats.

Deux autres options sont disponibles :

i. Machine : Le client sécurisé est limité à la recherche de certificats dans le magasin de certificats de l'ordinateur local Windows.
ii. Utilisateur : le client sécurisé est limité à la recherche de certificats sur le magasin de certificats d'utilisateur Windows local.

Définir le remplacement du magasin de certificats sur True.

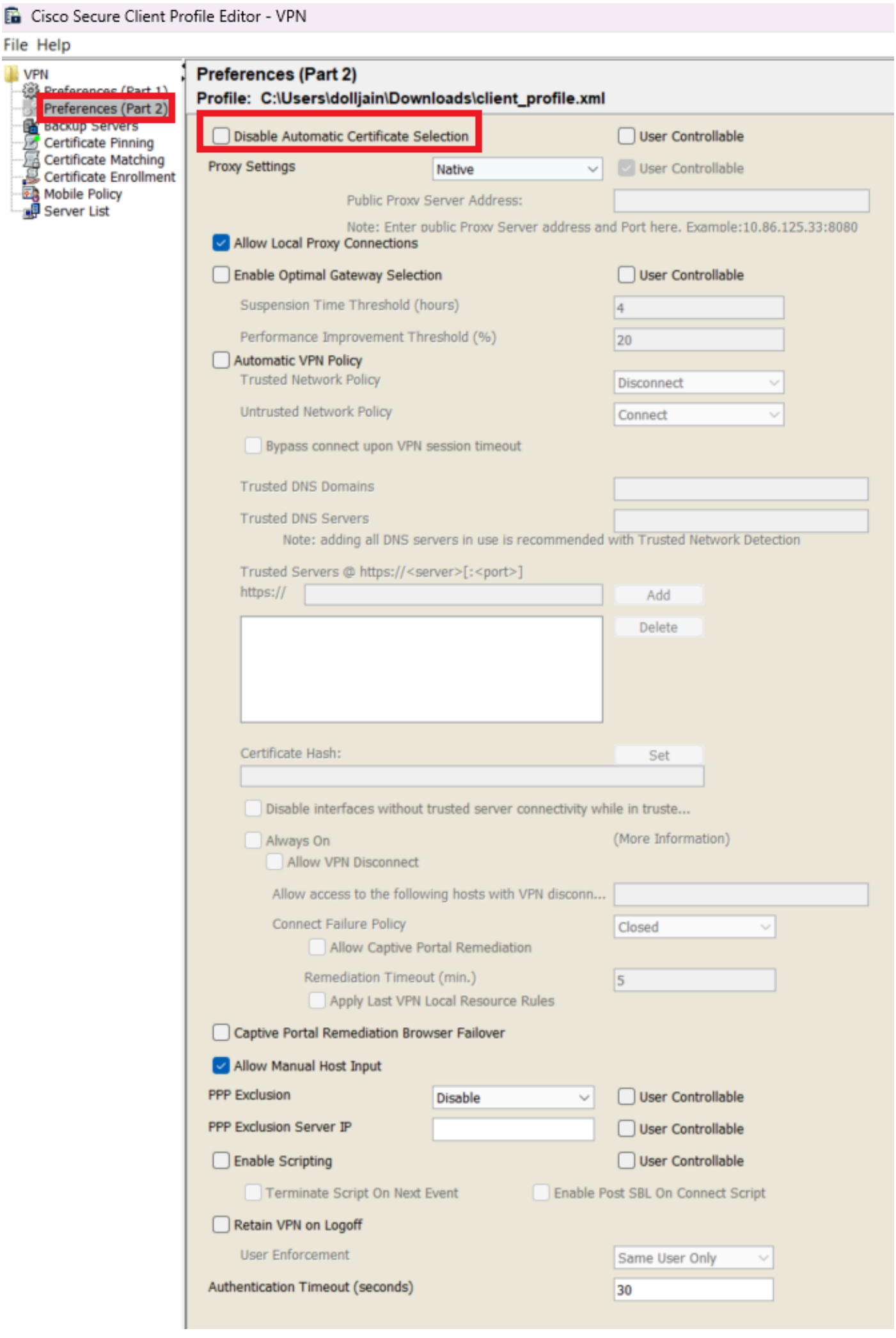
Cela permet à un administrateur d'indiquer au client sécurisé d'utiliser les certificats dans le magasin de certificats de l'ordinateur Windows (système local) pour l'authentification du certificat client. Le remplacement du magasin de certificats s'applique uniquement à SSL, où la connexion est initiée, par défaut dans le processus de l'interface utilisateur. Lorsque vous utilisez IPSec/IKEv2, cette fonctionnalité du profil client sécurisé n'est pas applicable.



Ajouter des préférences (Partie 1)

---

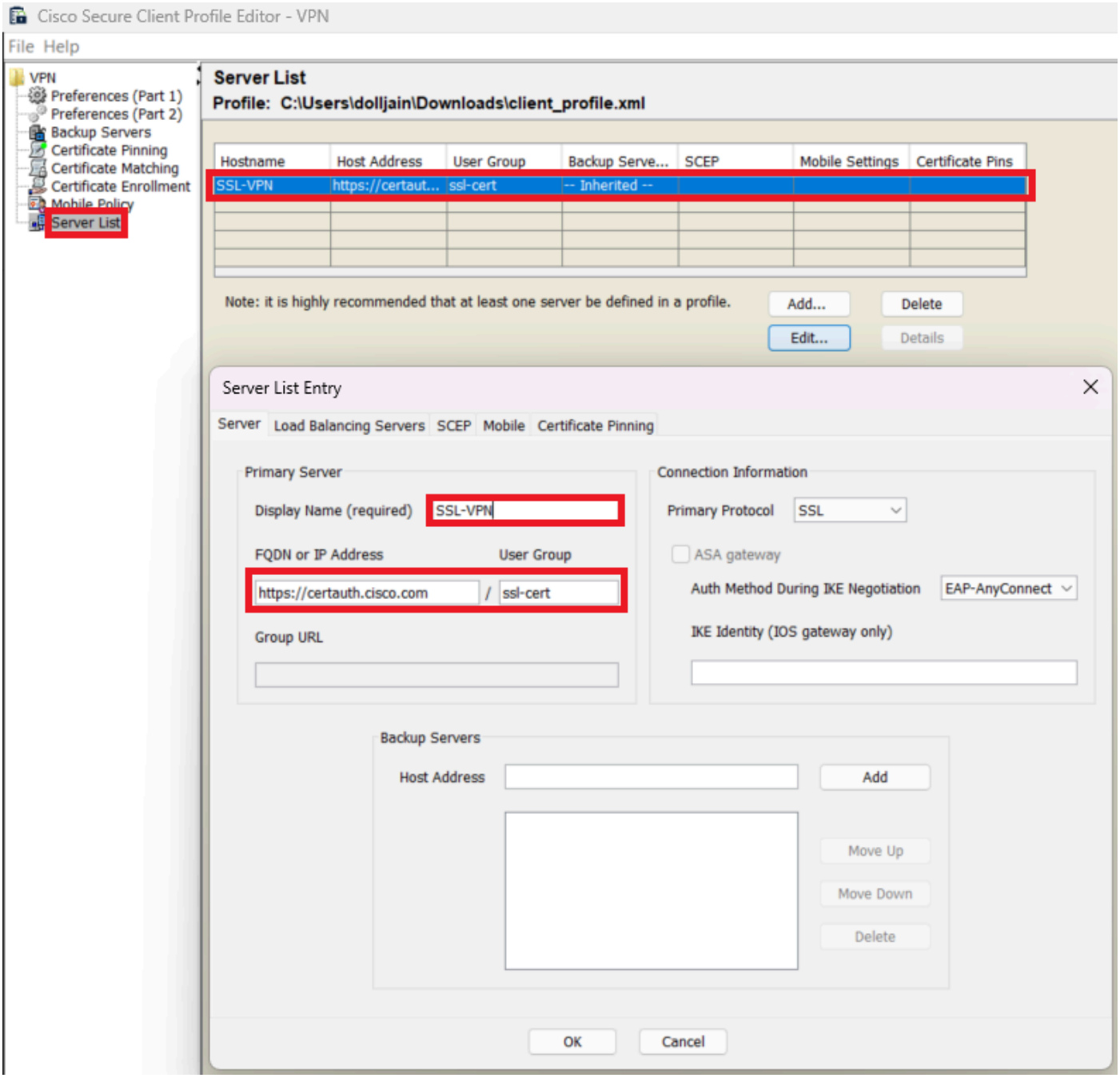
3. (Facultatif) Décochez la case Désactiver la sélection automatique de certificat, car elle évite l'invite de sélection du certificat d'authentification.


Cisco Secure Client Profile Editor - VPN
File Help
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Pinning
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Preferences (Part 2)
Profile: C:\Users\dolljain\Downloads\client_profile.xml
Disable Automatic Certificate Selection
User Controllable
Proxy Settings
Native
User Controllable
Public Proxy Server Address:
Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080
Allow Local Proxy Connections
Enable Optimal Gateway Selection
User Controllable
Suspension Time Threshold (hours)
4
Performance Improvement Threshold (%)
20
Automatic VPN Policy
Trusted Network Policy
Disconnect
Untrusted Network Policy
Connect
Bypass connect upon VPN session timeout
Trusted DNS Domains
Trusted DNS Servers
Note: adding all DNS servers in use is recommended with Trusted Network Detection
Trusted Servers @ https://<server>[:<port>]
https://
Add
Delete
Certificate Hash:
Set
Disable interfaces without trusted server connectivity while in truste...
Always On
(More Information)
Allow VPN Disconnect
Allow access to the following hosts with VPN disconn...
Connect Failure Policy
Closed
Allow Captive Portal Remediation
Remediation Timeout (min.)
5
Apply Last VPN Local Resource Rules
Captive Portal Remediation Browser Failover
Allow Manual Host Input
PPP Exclusion
Disable
User Controllable
PPP Exclusion Server IP
User Controllable
Enable Scripting
User Controllable
Terminate Script On Next Event
Enable Post SBL On Connect Script
Retain VPN on Logoff
User Enforcement
Same User Only
Authentication Timeout (seconds)
30

Ajouter des préférences (Partie 2)

---

4. Créez une Server List Entry interface pour configurer un profil dans Secure Client VPN en fournissant group-alias et group-url sous la liste des serveurs et enregistrez le profil XML.



Ajouter une liste de serveurs

---

5. Le profil XML est prêt à être utilisé.



```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
        <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <CertificateStore>All</CertificateStore>
        <CertificateStoreMac>All</CertificateStoreMac>
        <CertificateStoreLinux>All</CertificateStoreLinux>
        <CertificateStoreOverride>true</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
        <AuthenticationTimeout>30</AuthenticationTimeout>
        <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
        <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
        <LocalLanAccess UserControllable="true">false</LocalLanAccess>
        <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
        <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
        <AutoReconnect UserControllable="false">true
            <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
        </AutoReconnect>
        <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
        <AutoUpdate UserControllable="false">true</AutoUpdate>
        <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
        <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
        <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
        <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
        <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
        <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
        <PPPExclusion UserControllable="false">Disable
            <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
        </PPPExclusion>
        <EnableScripting UserControllable="false">false</EnableScripting>
        <EnableAutomaticServerSelection UserControllable="false">false
            <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
            <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
        </EnableAutomaticServerSelection>
        <RetainVpnOnLogoff>false
        </RetainVpnOnLogoff>
        <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
        <AllowManualHostInput>true</AllowManualHostInput>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>SSL-VPN</HostName>
            <HostAddress>https://certauth.cisco.com</HostAddress>
            <UserGroup>ssl-cert</UserGroup>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

Profil XML

L'emplacement des profils XML pour divers systèmes d'exploitation :

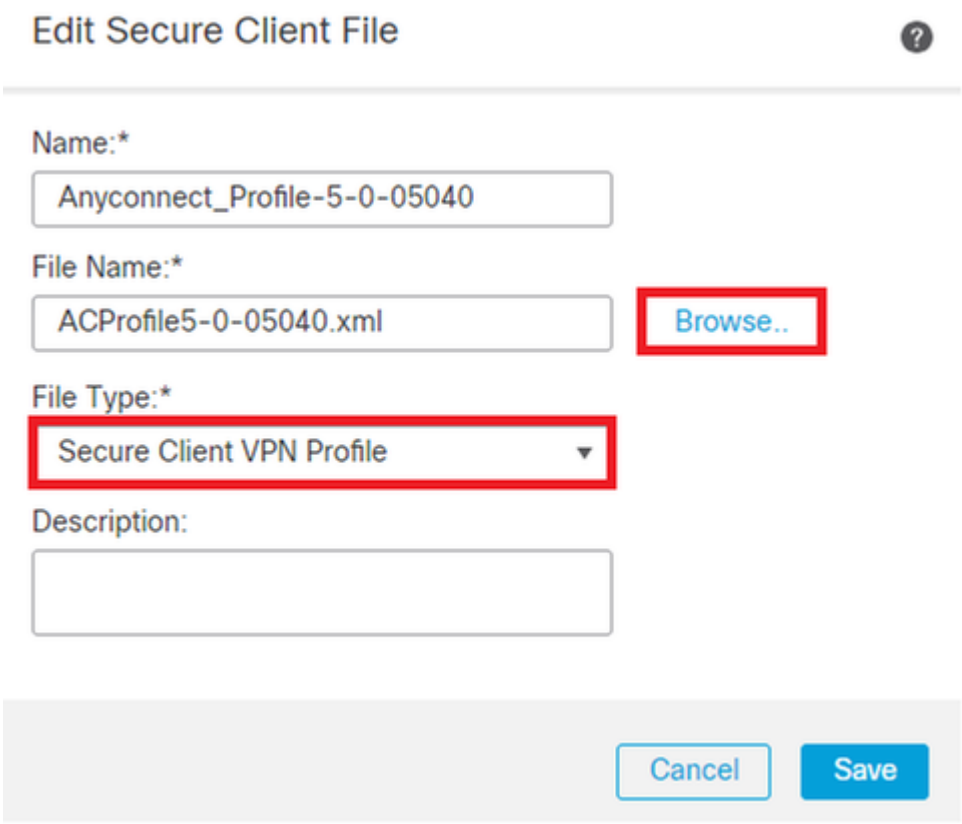
- Linux : /opt/cisco/anyconnect/profile
- MacOS - /opt/cisco/anyconnect/profile
- Windows : C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

---

6. Accédez à Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile.

---

7. Entrez le nom du fichier et cliquez sur Parcourir pour choisir le profil XML. Cliquez surSave.



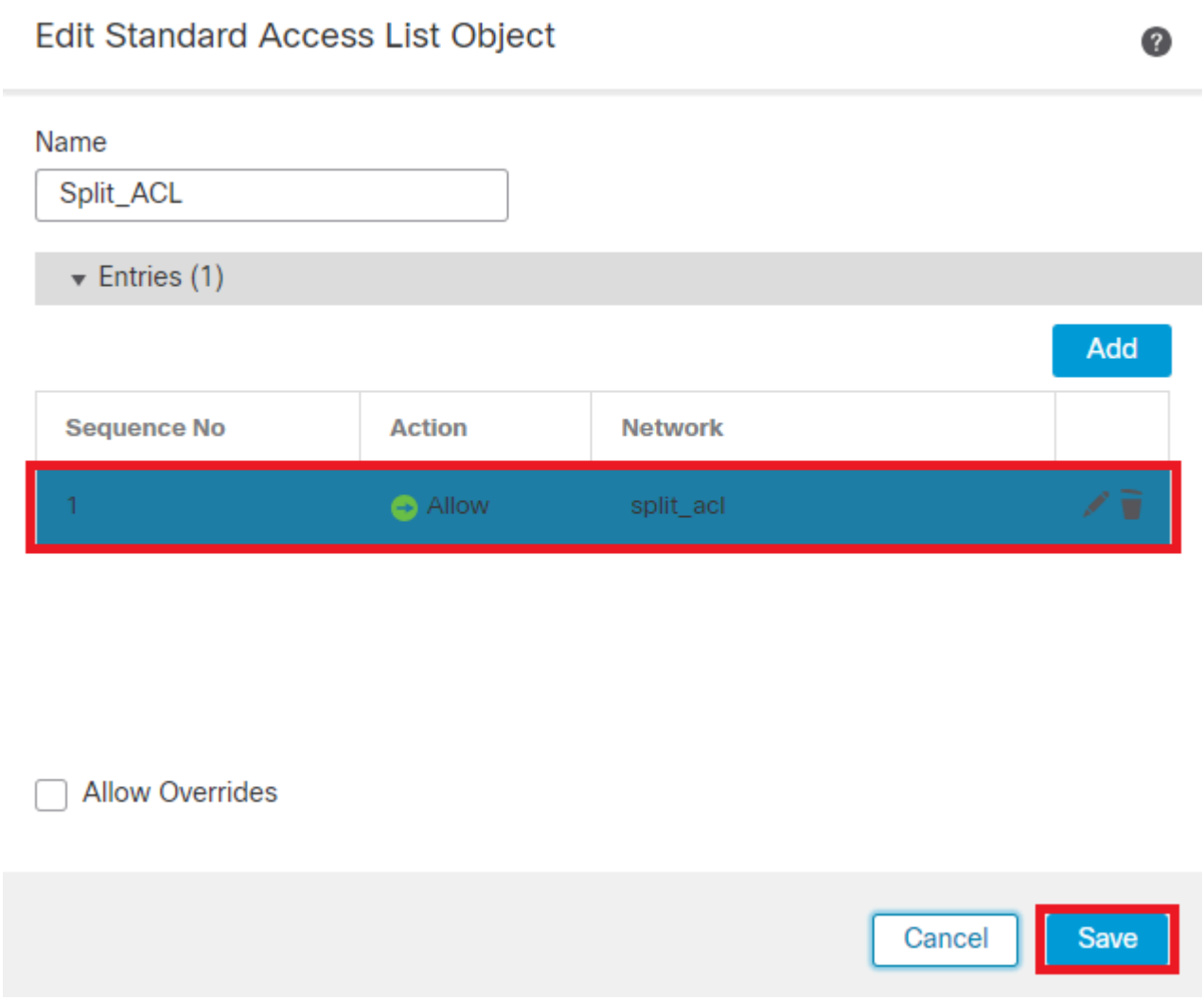
Ajouter un profil VPN client sécurisé

Configuration VPN d'accès à distance

1. Créez une liste de contrôle d’accès pour autoriser l’accès aux ressources internes.

---

2. Accédez à Objets > Gestion des objets > Liste d'accès > Standard et cliquez sur Ajouter une liste d'accès standard.



Ajouter une ACL standard

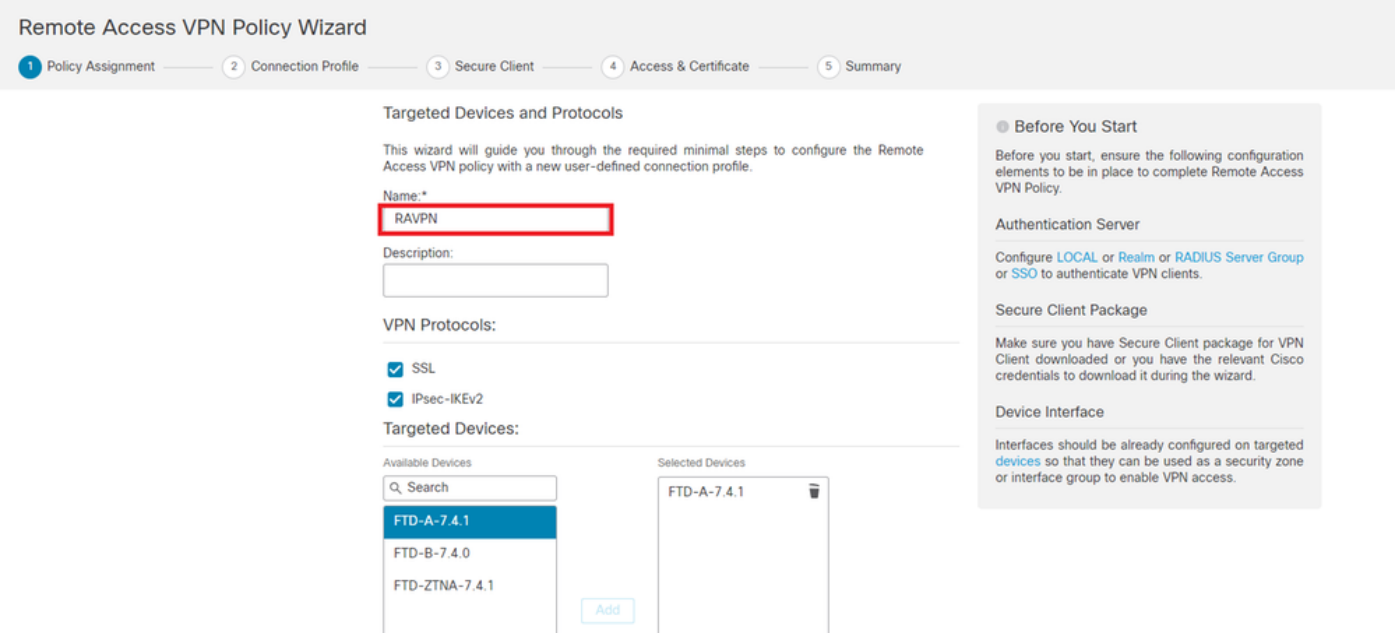
Remarque : Cette liste de contrôle d'accès est utilisée par le client sécurisé pour ajouter des routes sécurisées aux ressources internes.

---

3. Accédez à Devices > VPN > Remote Access et cliquez sur Add.

---

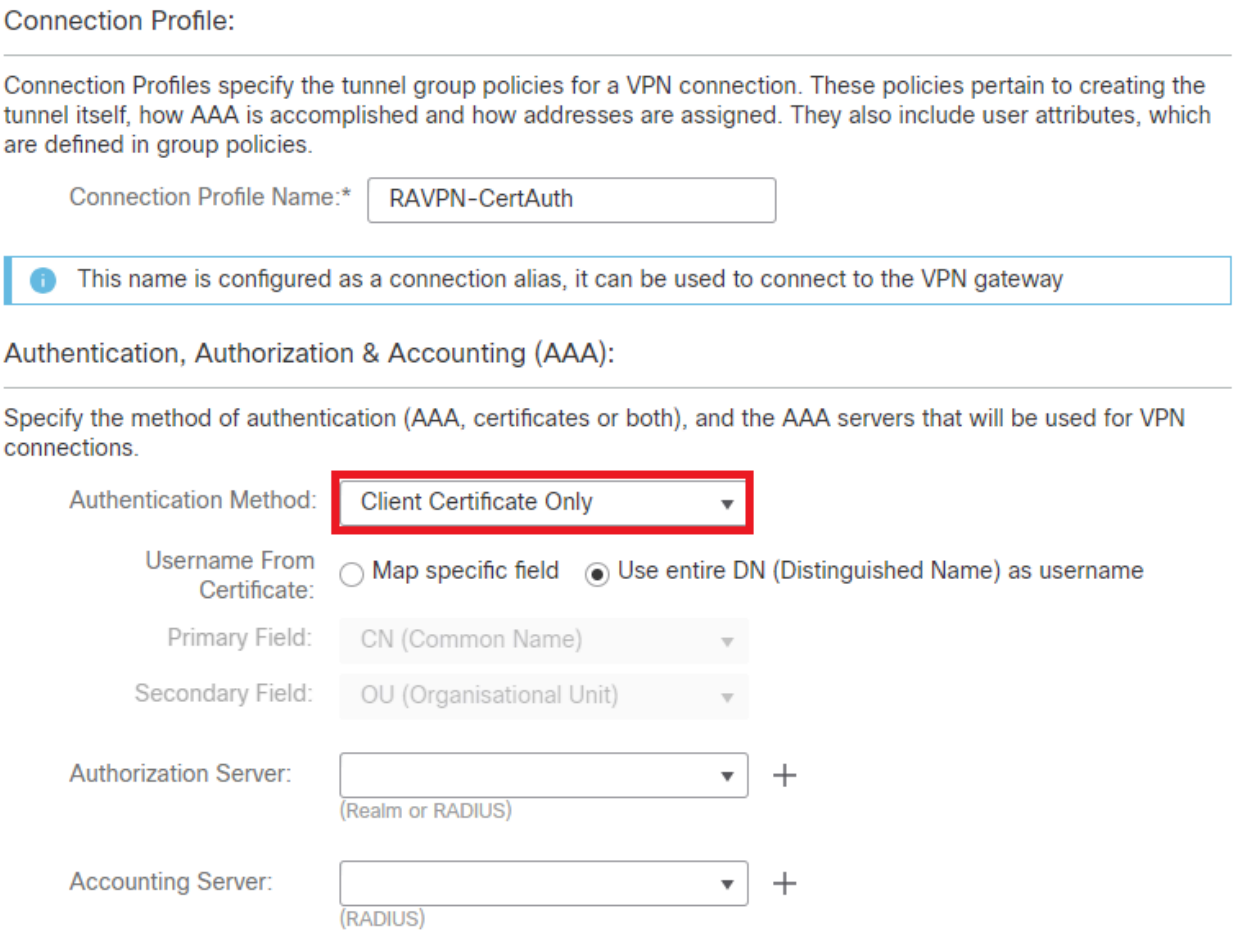
4. Entrez le nom du profil, puis choisissez le périphérique FTD et cliquez sur Suivant.



Ajouter un nom de profil

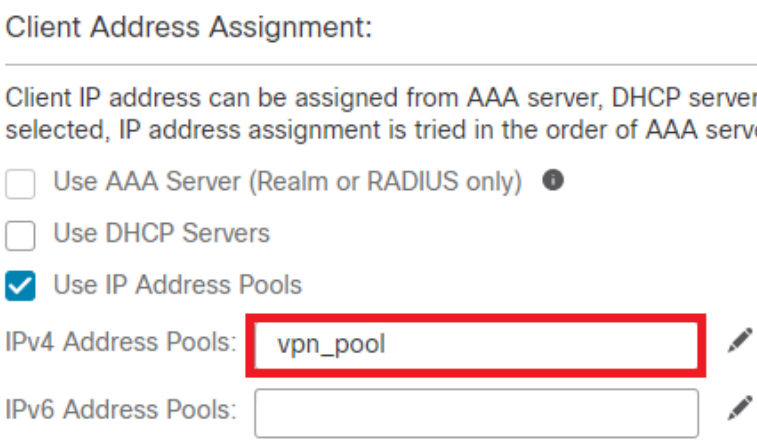
---

5. Entrez le nom du profil de connexion et choisissez la méthode d'authentification comme certificat client uniquement sous Authentication, Authorization, and Accounting (AAA).



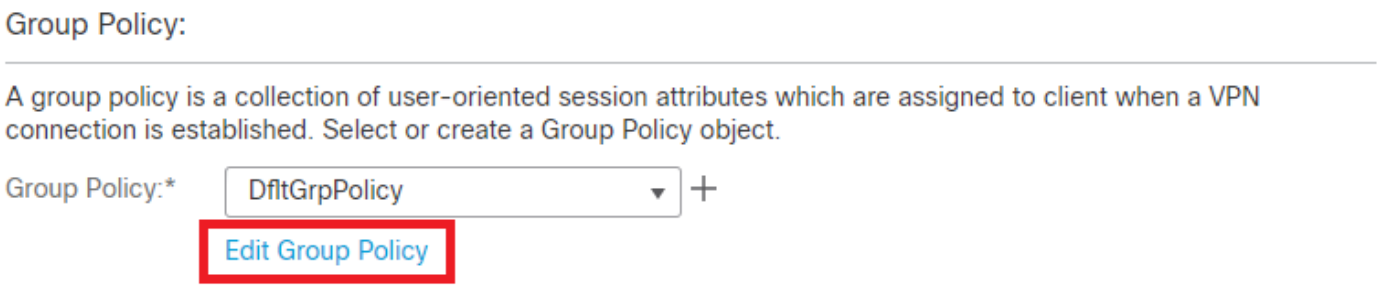
Sélectionner une méthode d'authentification

6. Cliquez sur Use IP Address Pools sous Client Address Assignment, et choisissez le pool d'adresses IPv4 créé précédemment.



Sélectionner l'affectation d'adresses client

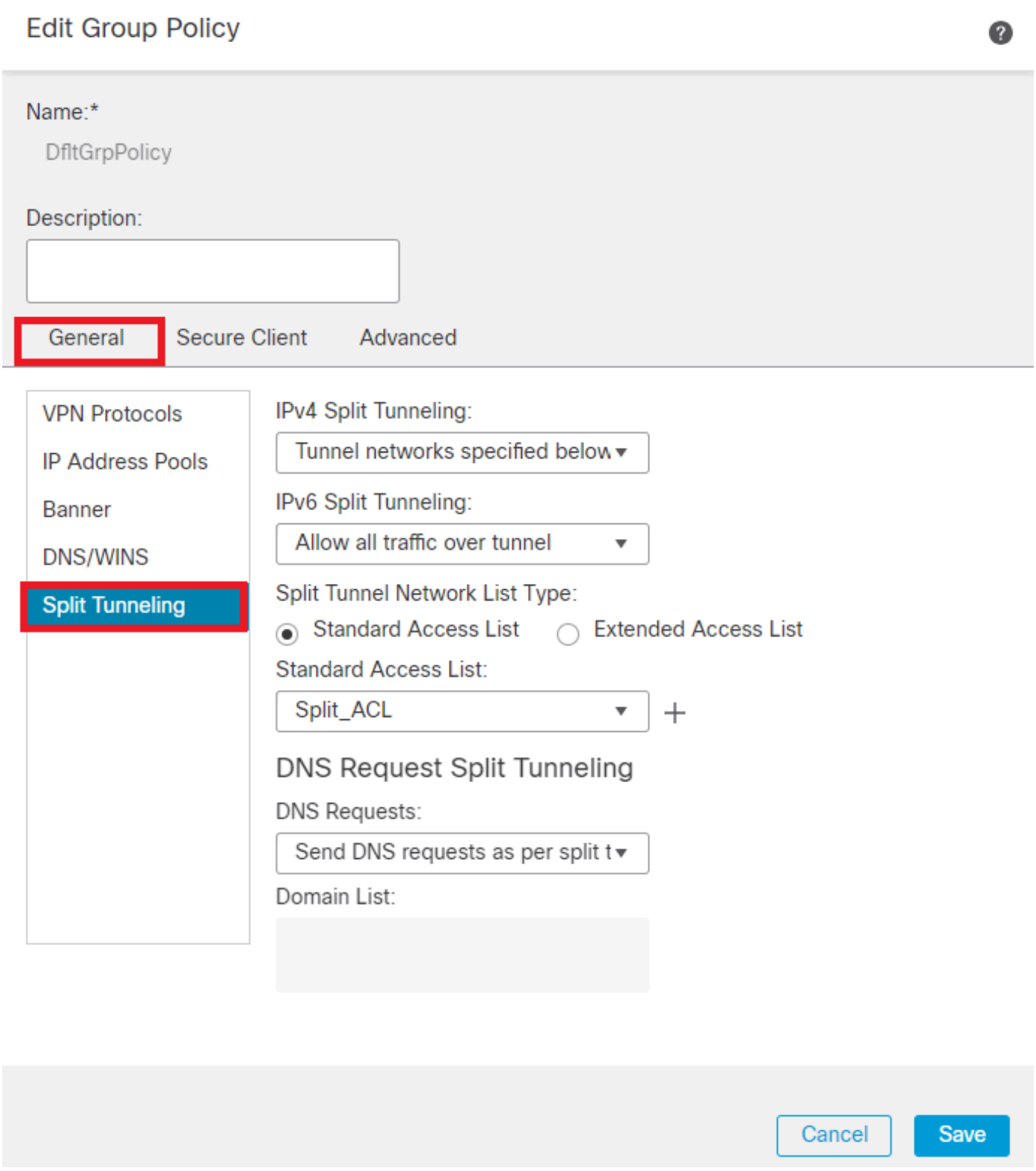
7. Modifiez la stratégie de groupe.



Modifier la stratégie de groupe

8. Accédez à General > Split Tunneling, choisissez Tunnel networks specified below, puis Standard Access List sous Split Tunnel Network List Type.

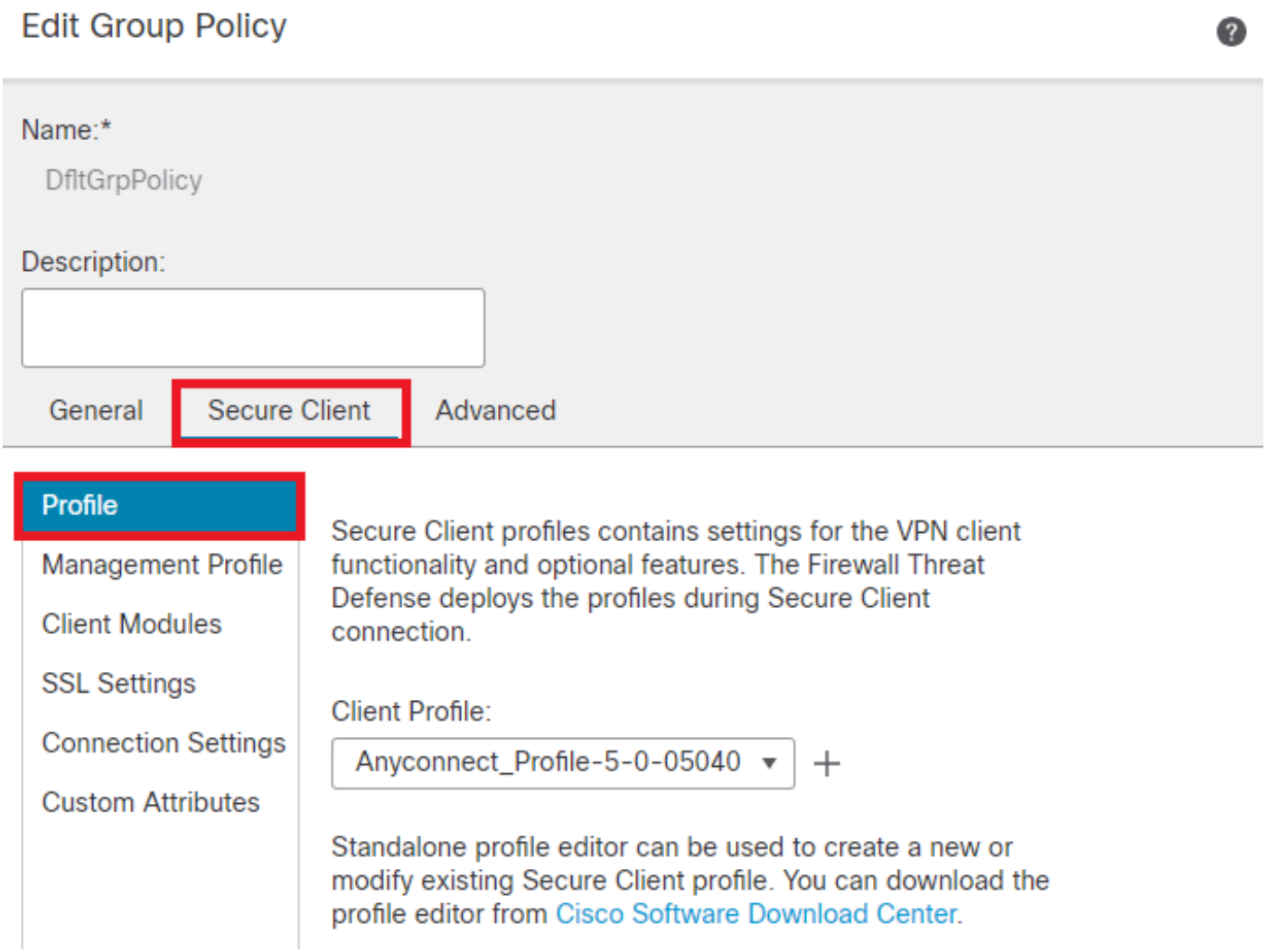
9. Choisissez la liste de contrôle d'accès créée précédemment.



Ajouter une tunnellisation partagée

---

10. Accédez à Secure Client > Profile, choisissez le Client Profile et cliquez sur Save.



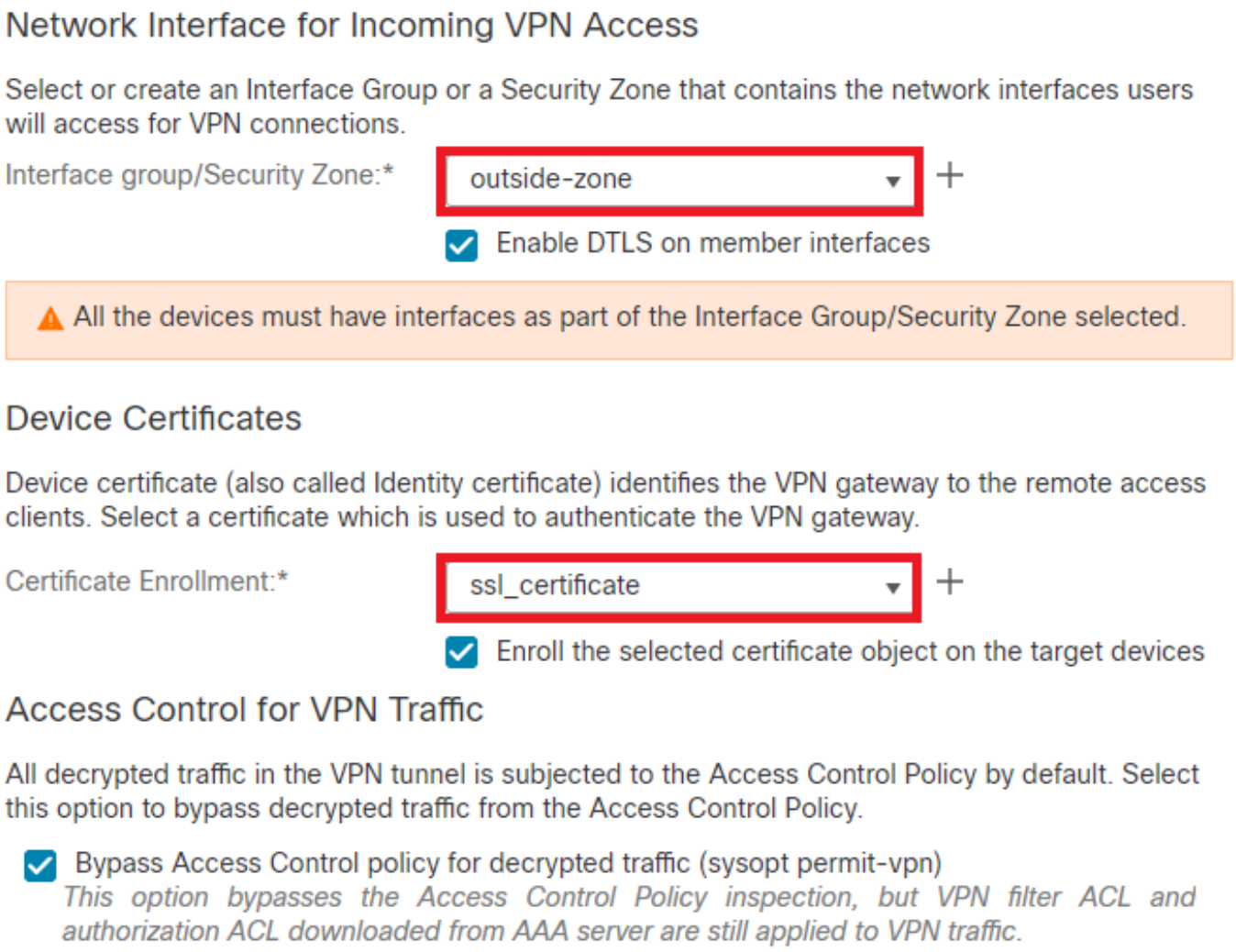
Ajouter un profil client sécurisé

11. Cliquez sur Next, puis sélectionnez Secure Client Image et cliquez surNext.



Ajouter une image de client sécurisé

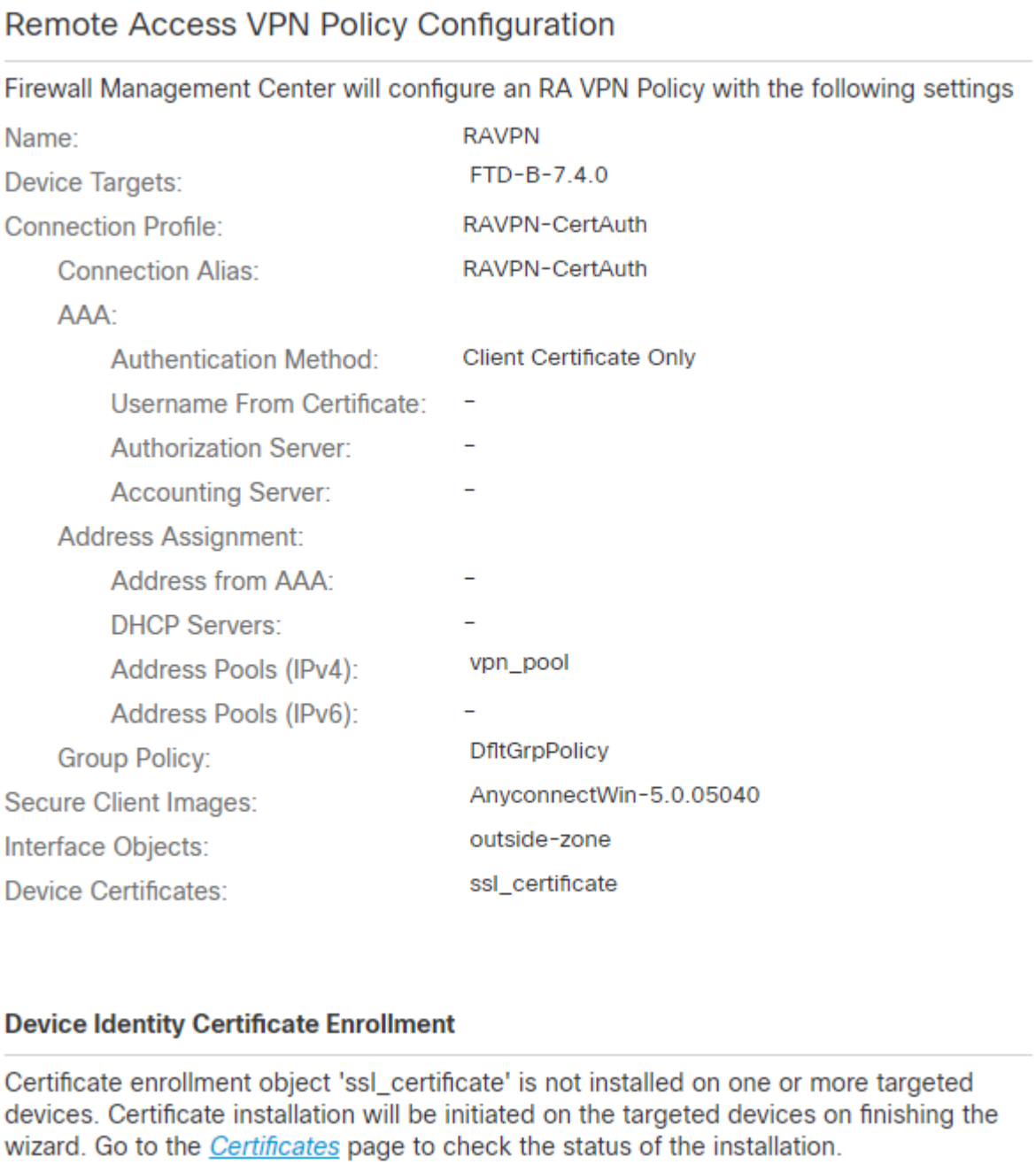
12. Choisissez l'interface réseau pour l'accès VPN, choisissez le Device Certificates et cochez sysopt permit-vpn et cliquez surNext.



Ajouter un contrôle d'accès pour le trafic VPN

---

13. Vérifiez toutes les configurations et cliquez sur Terminer.



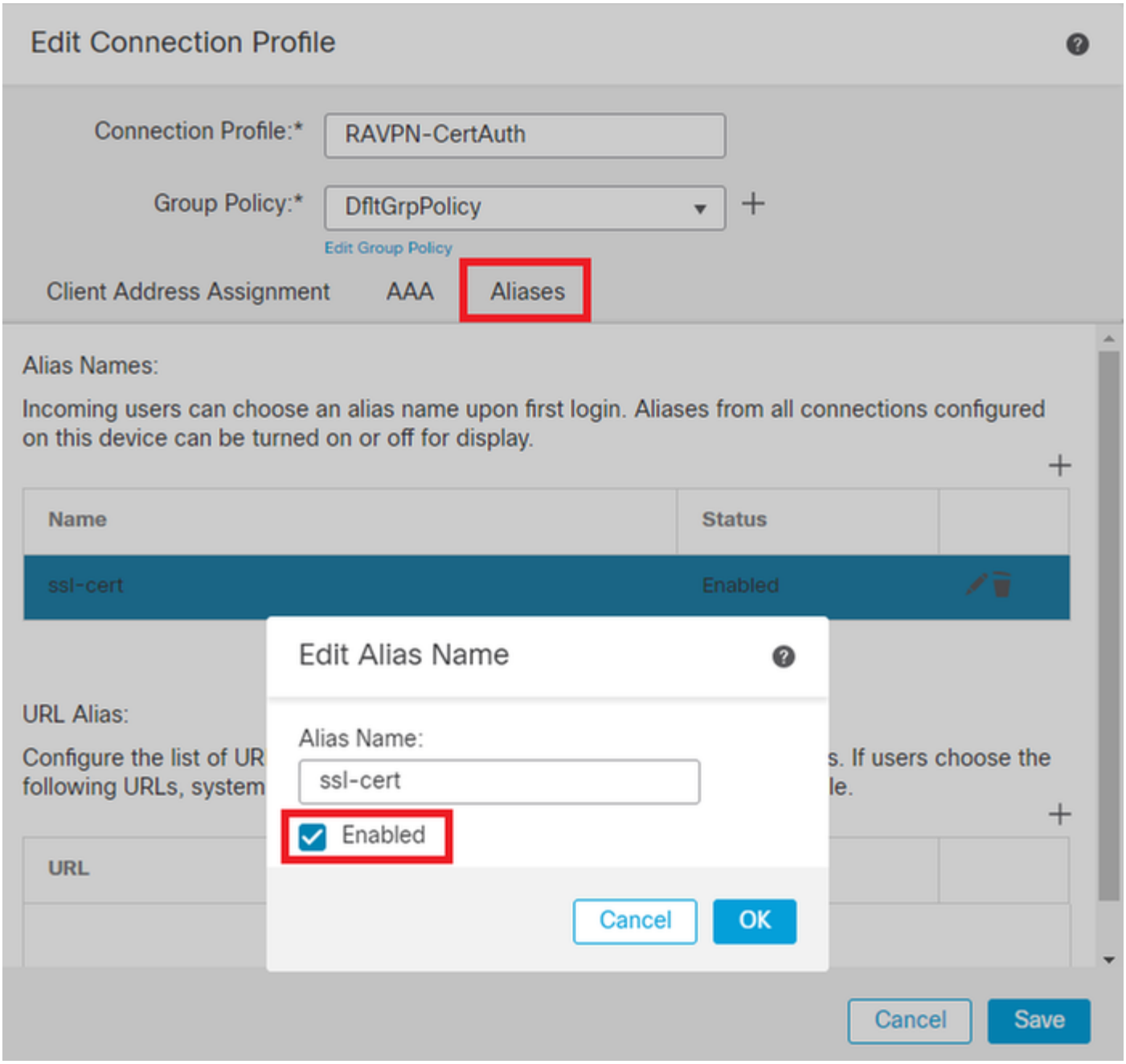
Configuration de la stratégie VPN d'accès à distance

---

14. Une fois la configuration initiale du VPN d'accès à distance terminée, modifiez le profil de connexion créé et accédez à Alias.

---

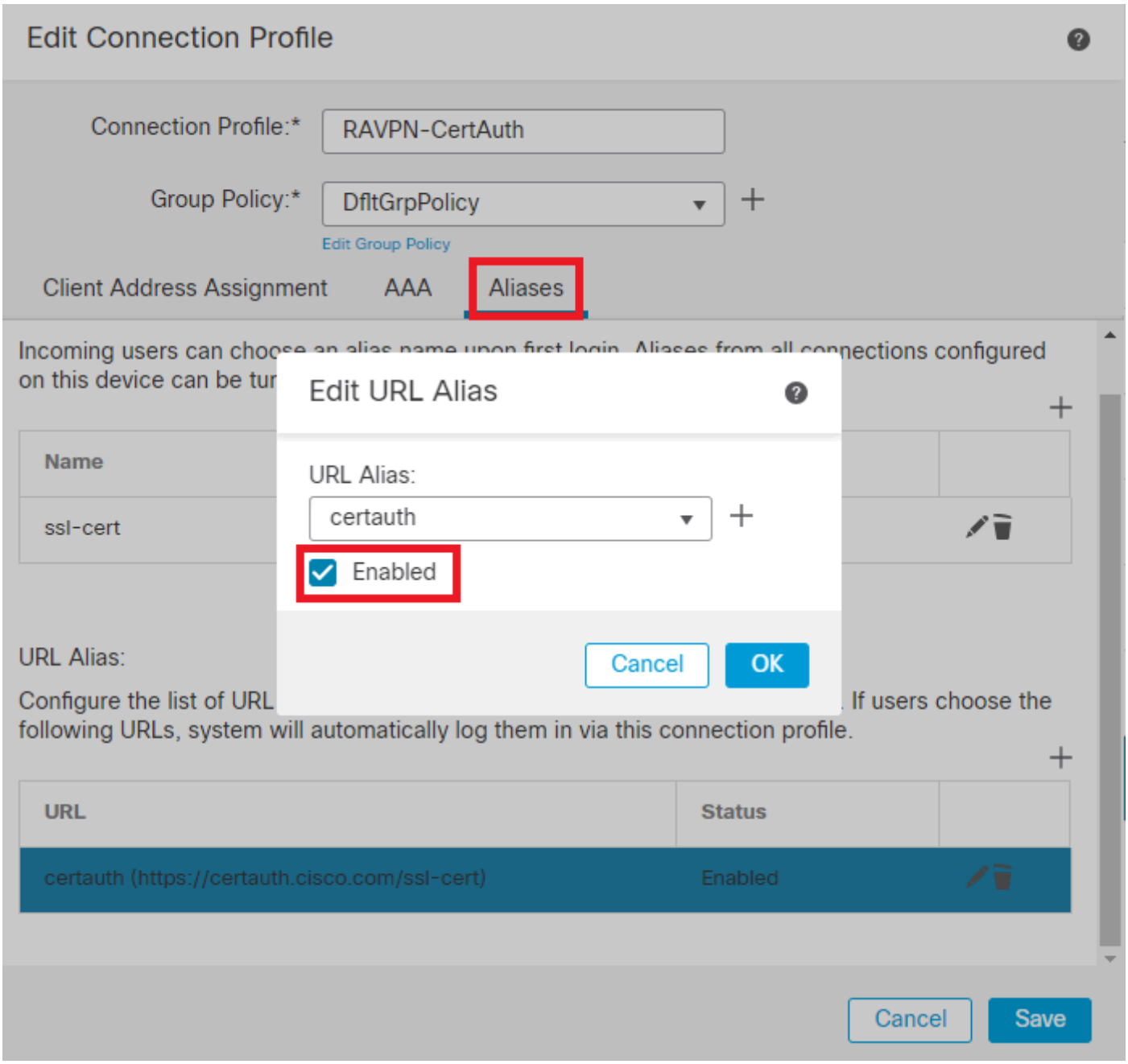
15. Configurez group-alias en cliquant sur l'icône plus (+).



Modifier un alias de groupe

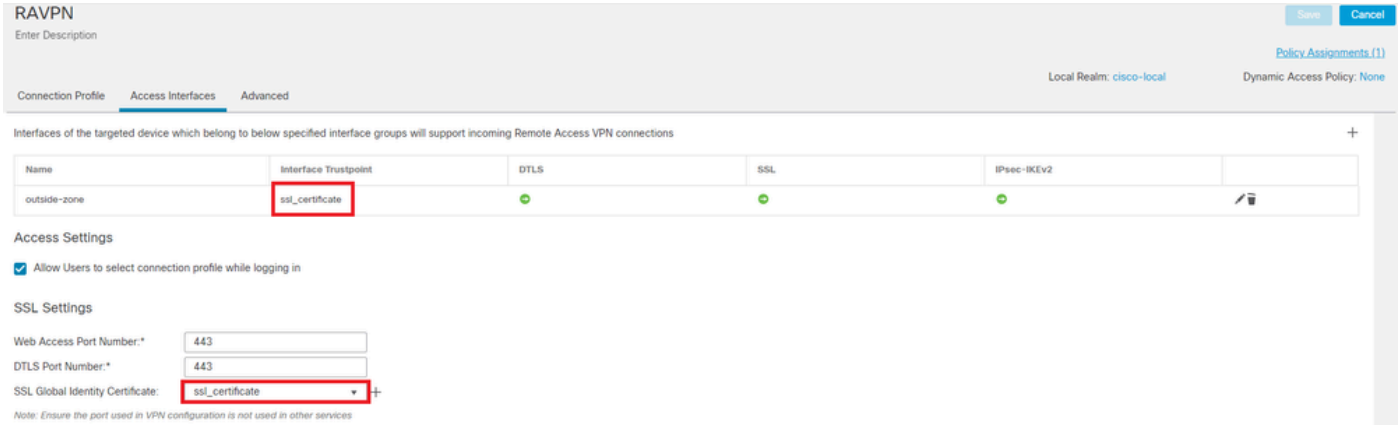
---

16. Configurez le group-url en cliquant sur l'icône plus (+). Utilisez la même URL de groupe que celle configurée précédemment dans le profil client.



Modifier l'URL du groupe

Étape 17. Accédez à Access Interfaces. Choisissez le point de confiance d'interface et le certificat d'identité globale SSL sous les paramètres SSL.



Modifier les interfaces d'accès

---

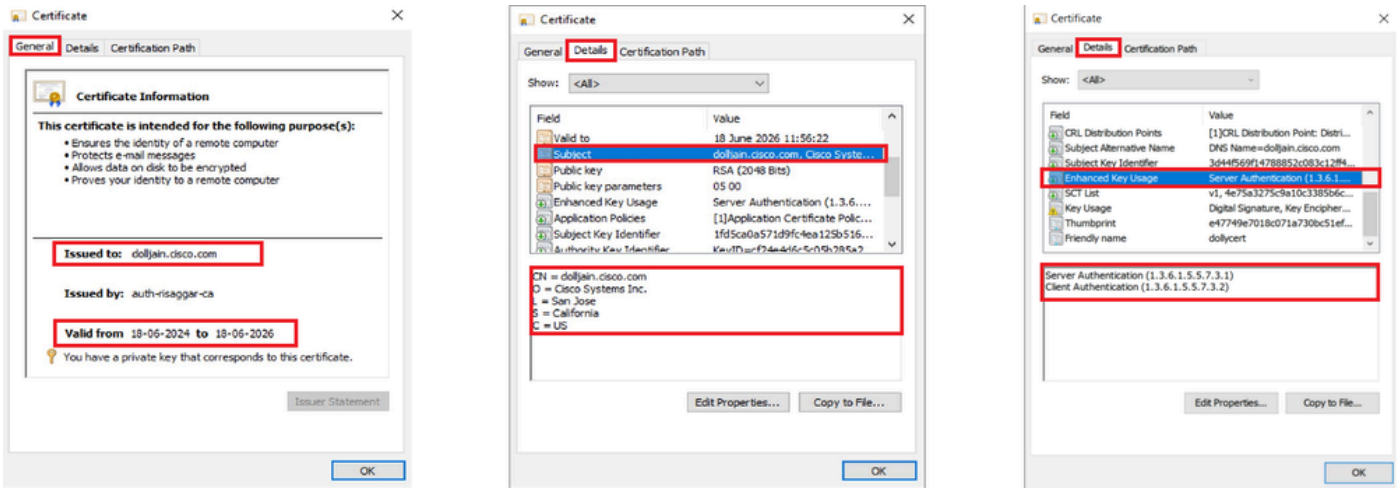
18. Cliquez sur Enregistrer et déployez les modifications.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

---

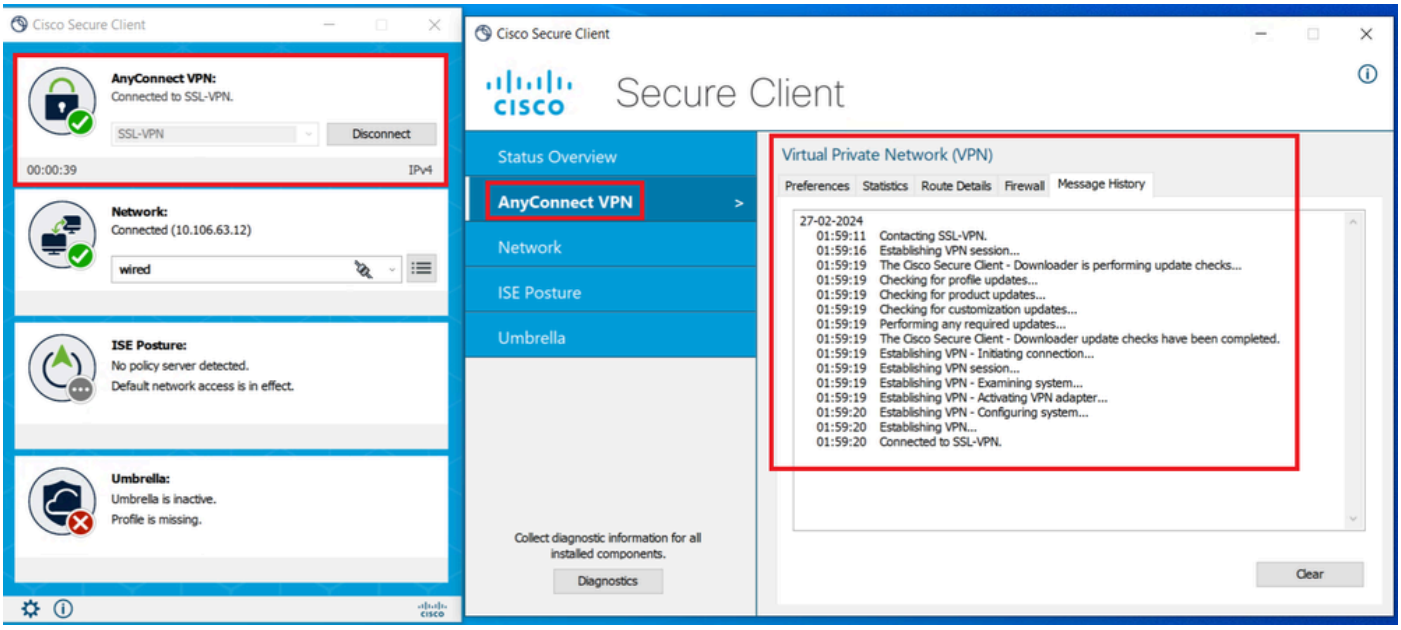
1. Le certificat du PC client sécurisé doit être installé avec une date valide, un objet et une utilisation améliorée de la clé (EKU) sur le PC de l'utilisateur. Ce certificat doit être émis par l'autorité de certification dont le certificat est installé sur le FTD comme indiqué précédemment. Dans l'exemple suivant, l'identité ou le certificat utilisateur est émis par auth-risaggar-ca.



Points saillants du certificat

Remarque : Le certificat client doit avoir l'EKU d'authentification client.

2. Le client sécurisé doit établir la connexion.



Connexion client sécurisée réussie

3. Exécutez la commande show vpn-sessiondb anyconnect pour confirmer les détails de connexion de l'utilisateur actif sous le groupe de tunnels utilisé.

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dolljain.cisco.com     Index        : 8
Assigned IP  : 10.20.20.1             Public IP    : 72.163.X.X
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256
Bytes Tx     : 14402                  Bytes Rx     : 9652
Group Policy : DfltGrpPolicy          Tunnel Group : RAVPN-CertAuth
Login Time   : 08:32:22 UTC Mon Mar 18 2024
Duration     : 0h:03m:59s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5de050000800065f7fc16
Security Grp : none                   Tunnel Zone  : 0
```

Dépannage

Cette section fournit des informations pour dépanner votre configuration.

---

1. Les débogages peuvent être exécutés à partir de l'interface de ligne de commande de diagnostic du FTD :

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

---

2. Reportez-vous au guide Troubleshoot Cisco Secure Client VPN Common Problems pour obtenir une assistance supplémentaire.

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.