Beveiligde verificatie van clientcertificaat configureren op FTD die wordt beheerd door FMC

Inhoud

Inleiding

Dit document beschrijft het proces van het configureren van externe toegang tot VPN op Firepower Threat Defence (FTD), beheerd door Firepower Management Center (FMC) met certificaatverificatie.

Bijgedragen door Dolly Jain en Rishabh Aggarwal, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

· Handmatige inschrijving van certificaten en basisgegevens van SSL
VCC
· Basiskennis van verificatie voor externe toegang via VPN
· Certificaat Autoriteit van derden (CA) zoals Entrust, Geotrust, GoDaddy, Thawte en VeriSign

Gebruikte componenten

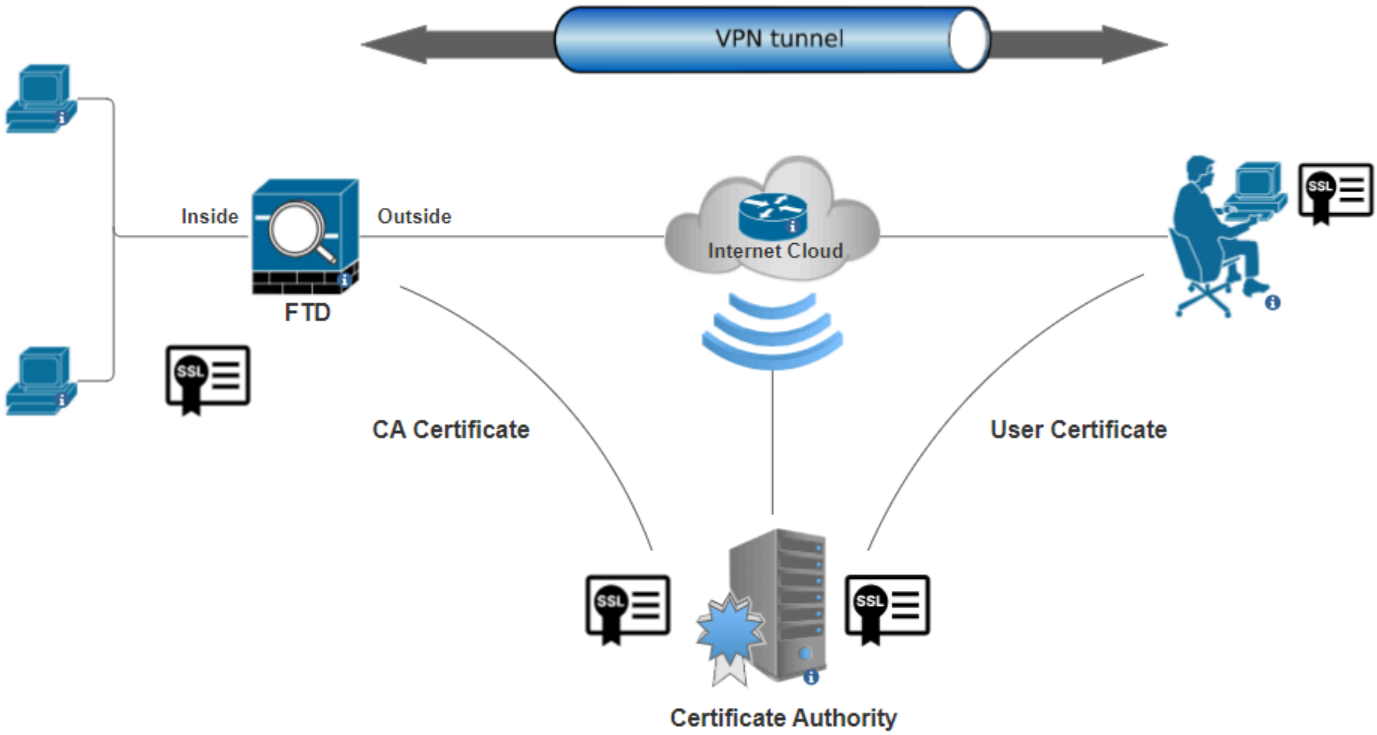
De informatie in dit document is gebaseerd op de volgende softwareversies:

· Secure Firepower Threat Defense versie 7.4.1
· Firepower Management Center (FMC) versie 7.4.1
· Secure Client versie 5.0.05040
· Microsoft Windows Server 2019 als CA-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

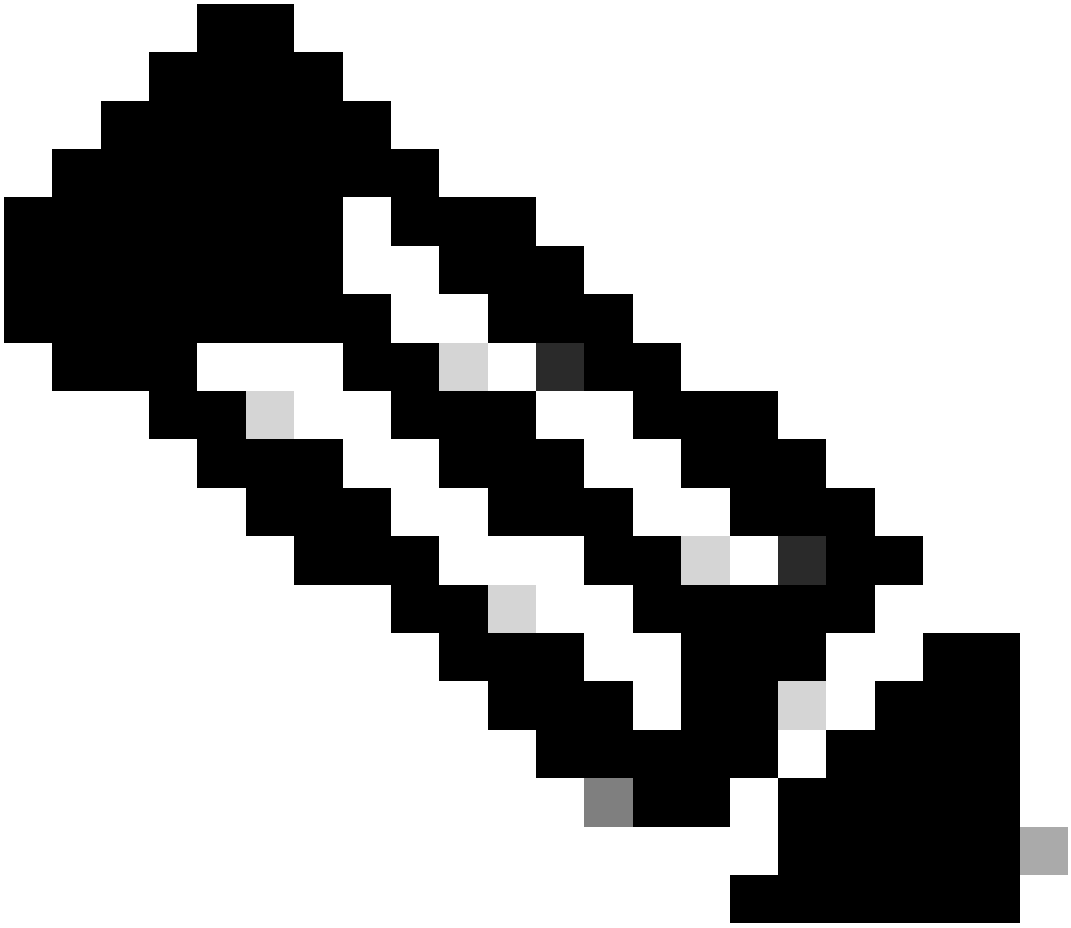
Netwerkdiagram



Netwerkdiagram

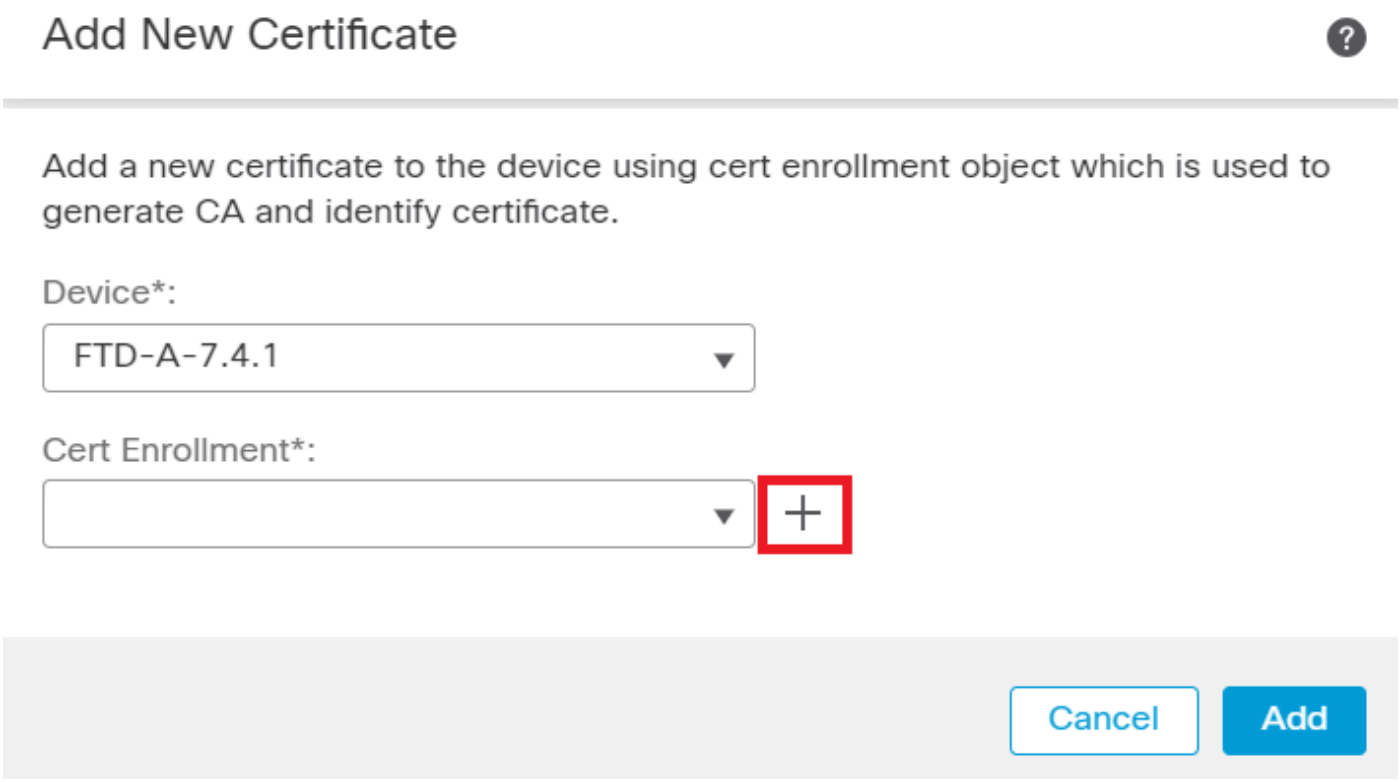
Configuraties

a. Een certificaat maken/importeren dat wordt gebruikt voor serververificatie



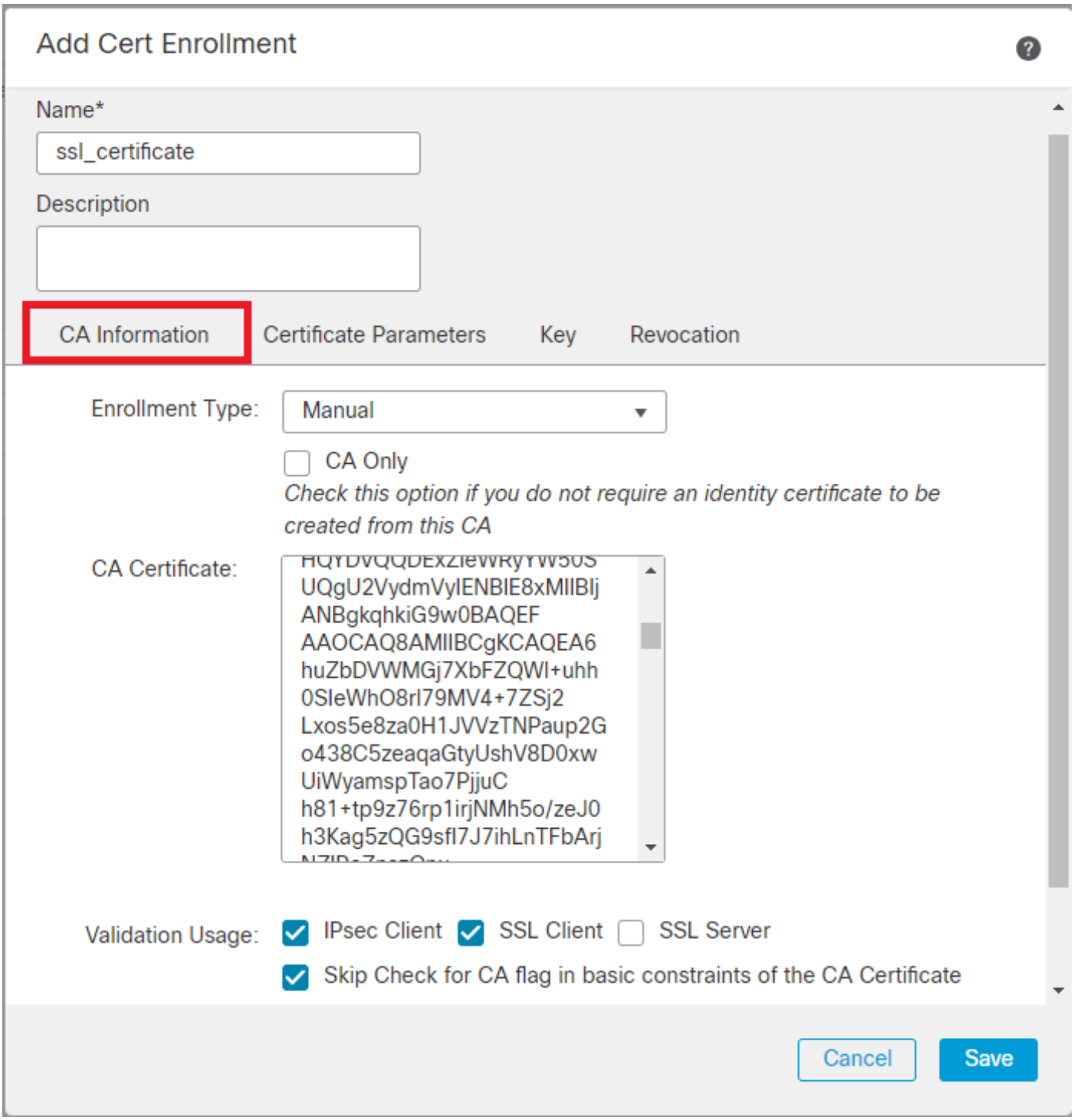
Opmerking: op VCC is een CA-certificaat nodig voordat u de CSR kunt genereren. Als MVO wordt gegenereerd vanuit een externe bron (OpenSSL of een derde partij), mislukt de handmatige methode en moet het PKCS12-certificaatformaat worden gebruikt.

Stap 1. Navigeer naar Devices > Certificatesen klik op Add. Selecteer Apparaat en klik op plusteken (+) onder Volledige inschrijving.



Registratie toevoegen

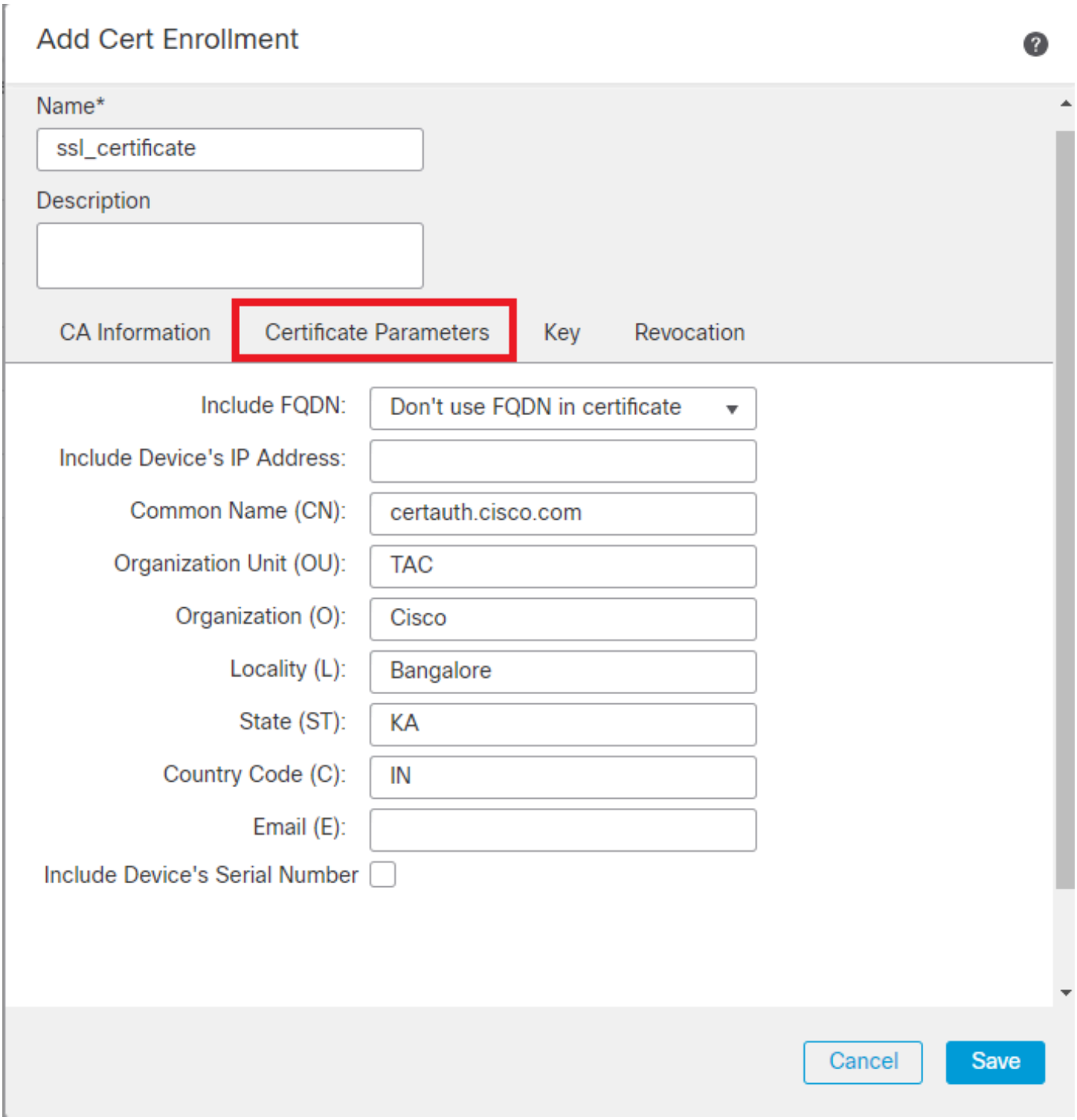
Stap 2. Selecteer onder het CA Information de optie Inschrijftype als Manual en plak het certificaat van de certificeringsinstantie (CA) dat wordt gebruikt om de CSR te ondertekenen.



CA-informatie toevoegen

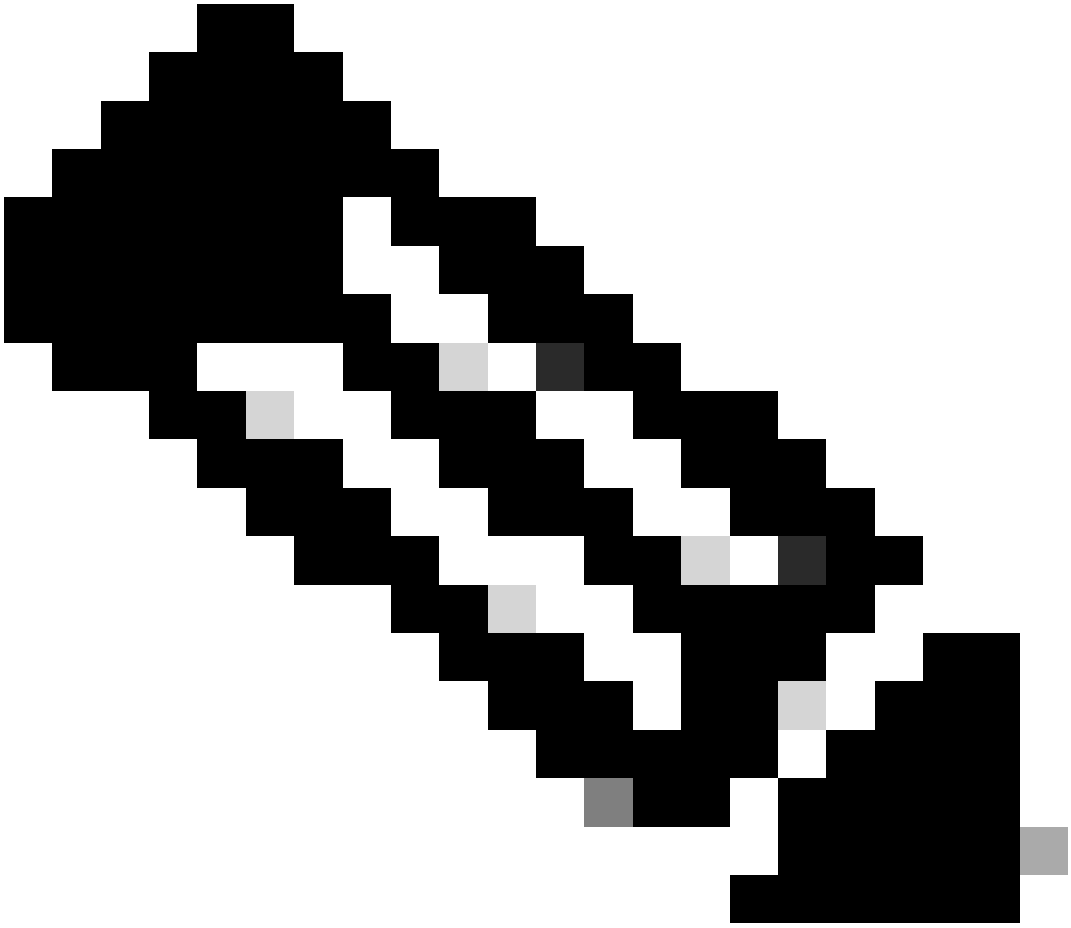
Stap 3. Selecteer IPsec Client, SSL Client en Skip Check for CA flag in basic constraints of the CA Certificate voor validatiegebruik.

Stap 4. Vul onder Certificate Parameters dit punt de onderwerpnaam in.

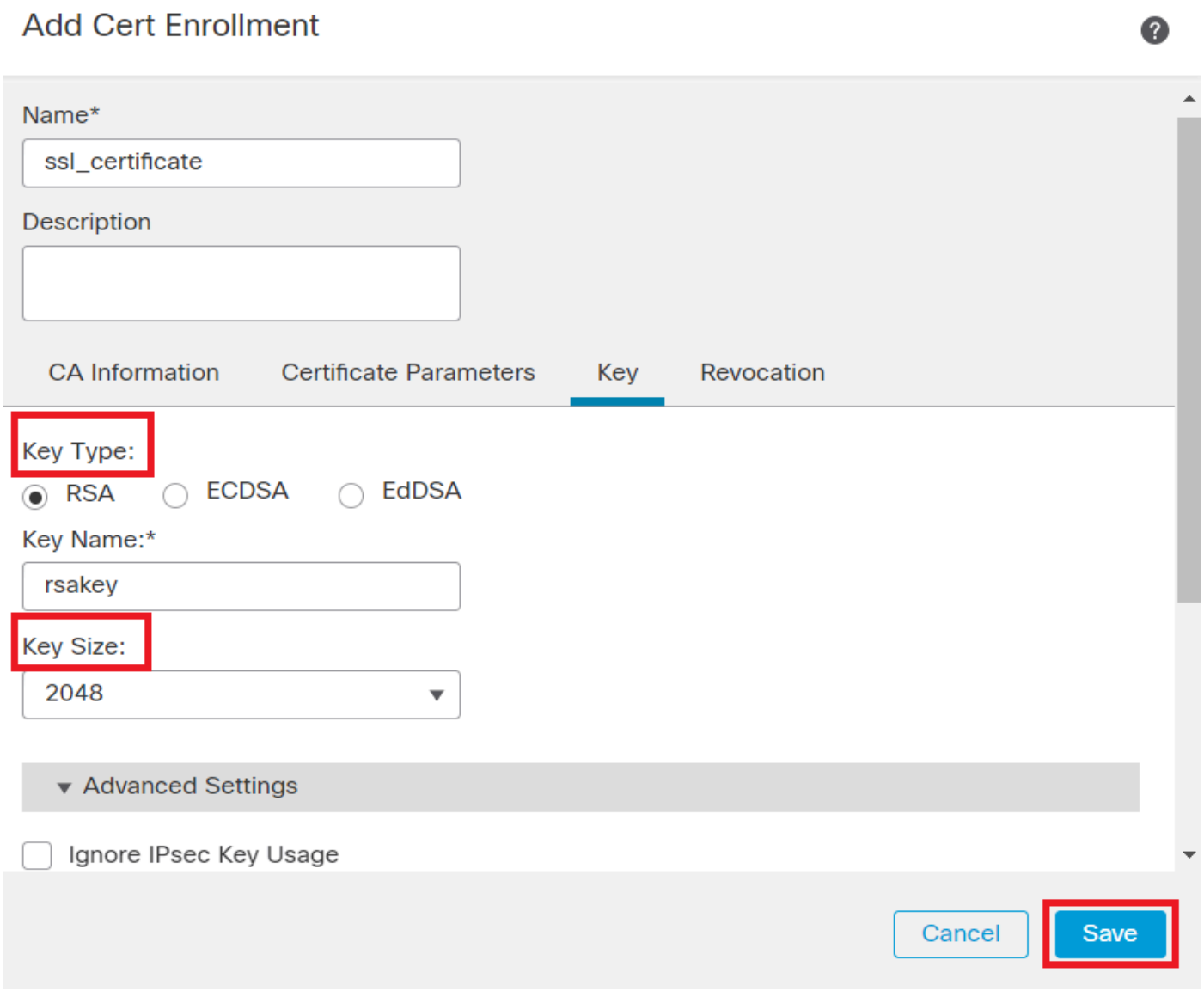


Certificaatparameters toevoegen

Stap 5. Selecteer onder Keyhet sleuteltype RSA met een toetsnaam en -grootte. Klik op Save.

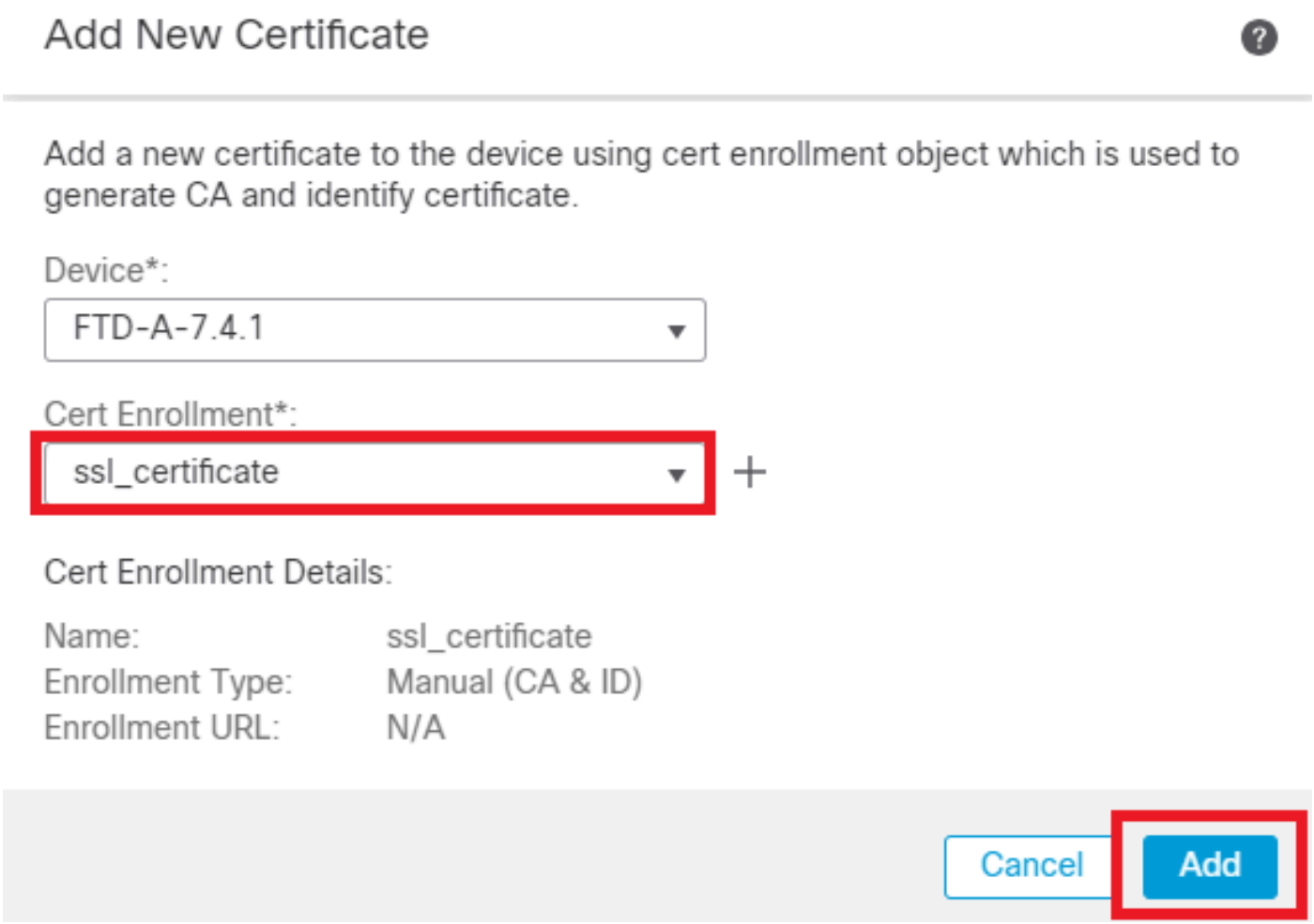


Opmerking: voor RSA-sleuteltype is de minimale sleutelgrootte 2048 bits.



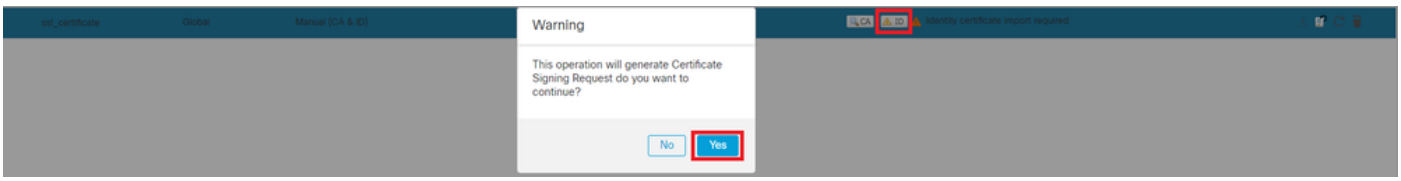
RSA-toets toevoegen

Stap 6. Selecteer onder Cert Enrollment het vertrouwenspunt uit de vervolgkeuzelijst die zojuist is gemaakt en klik op Add.



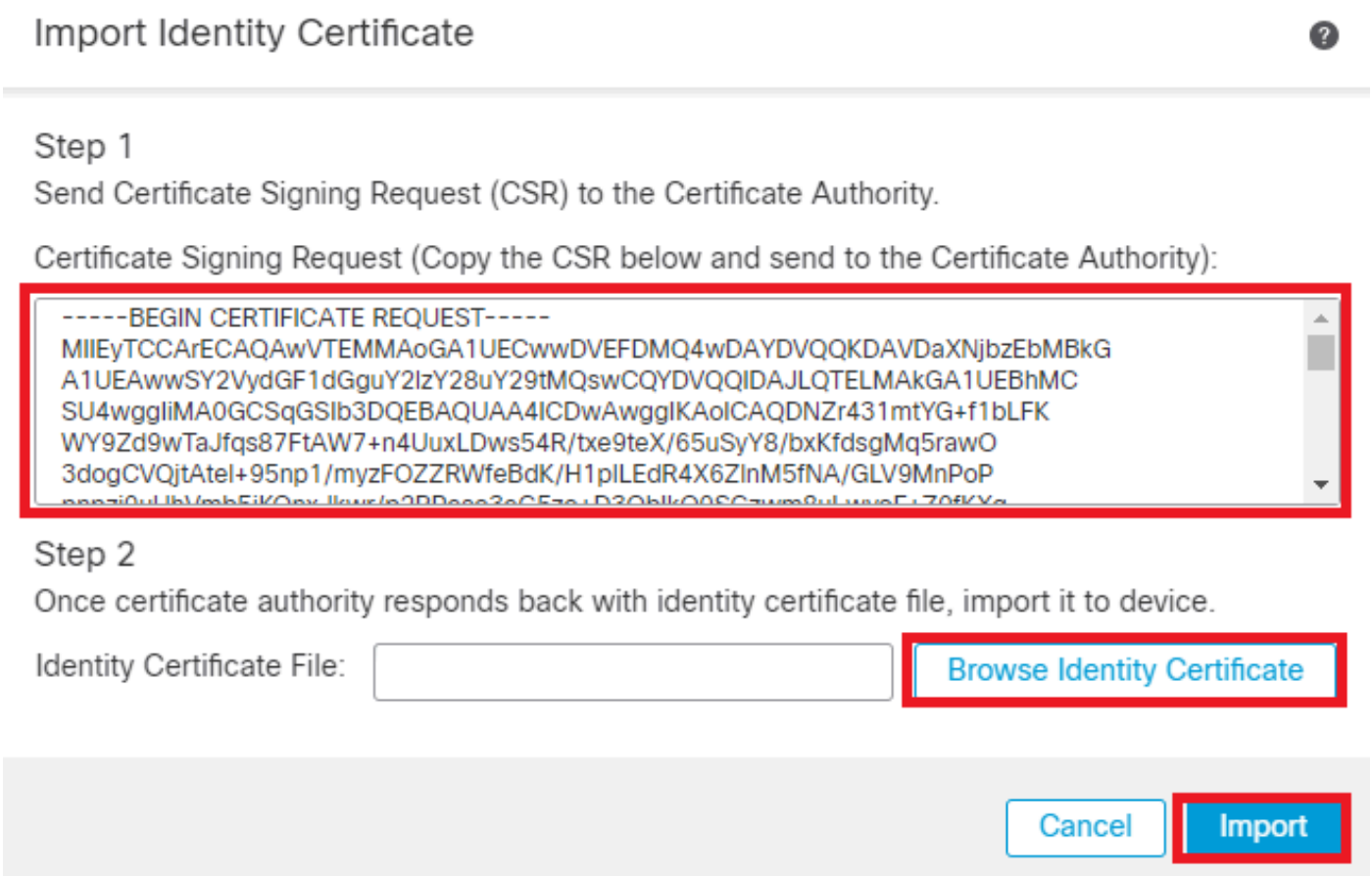
Nieuw certificaat toevoegen

Stap 7. Klik op ID en klik op Yes op verdere prompt om de MVO te genereren.

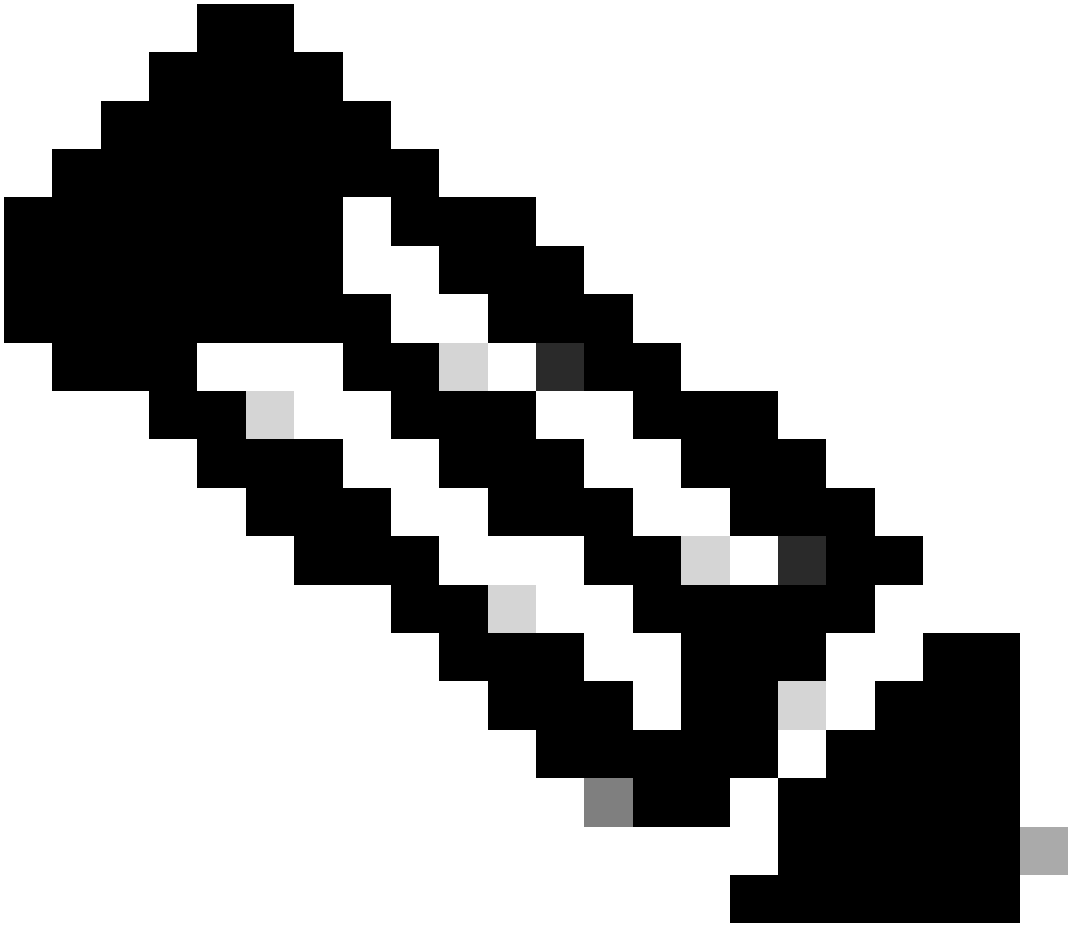


MVO genereren

Stap 8. Kopieer de MVO en laat deze ondertekenen door de Certificaatinstantie. Zodra het Identiteitscertificaat door CA is afgegeven, importeert u het door op te klikken Browse Identity Certificate en vervolgens te klikken Import .



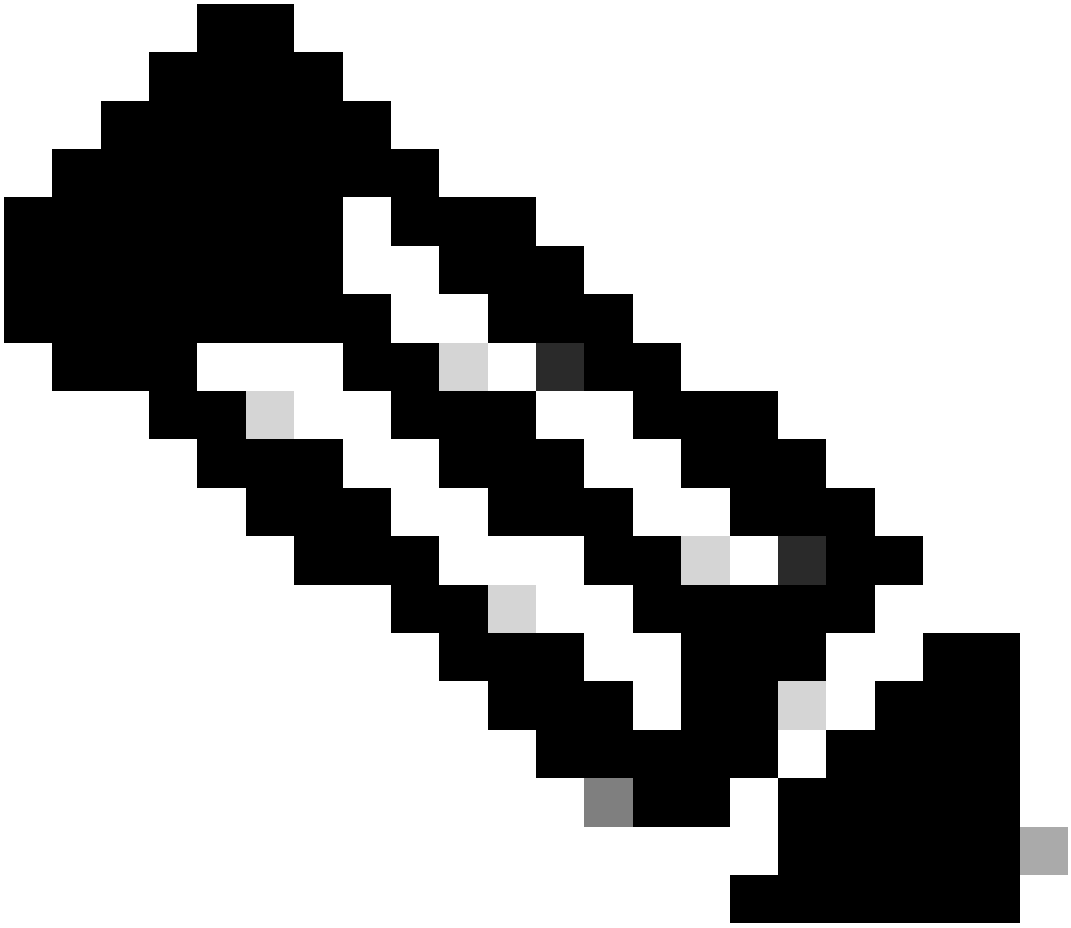
Certificaat van invoer-ID



Opmerking: als de uitgifte van het ID-certificaat tijd in beslag neemt, kunt u stap 7 later herhalen. Dit zal hetzelfde MVO genereren en we kunnen het ID-certificaat importeren.

---

b. Een betrouwbaar/intern CA-certificaat toevoegen

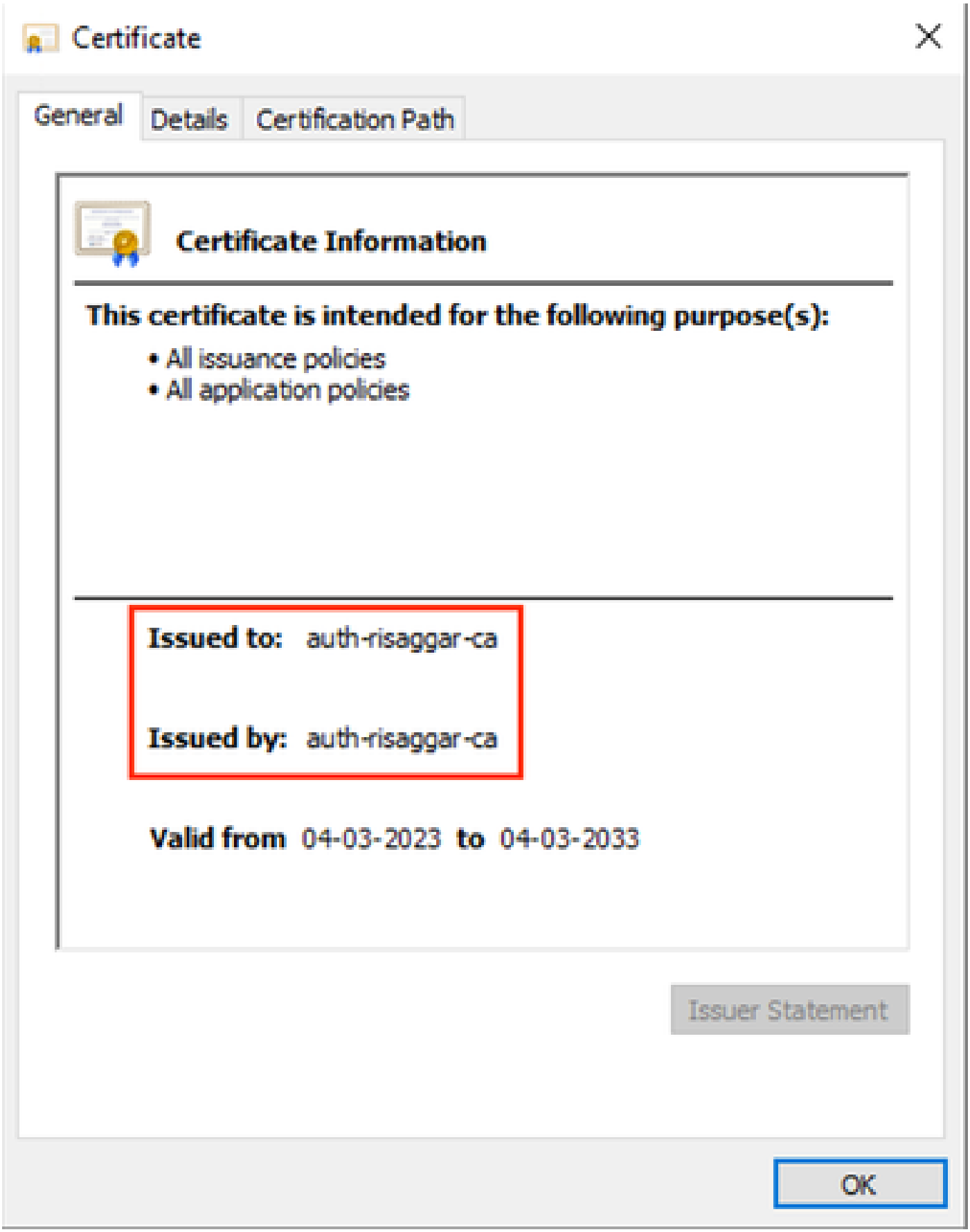


Opmerking: Als de certificeringsinstantie (CA) gebruikt in stap a), **"Maak/importeer een certificaat dat gebruikt wordt voor serververificatie"** ook gebruikerscertificaten afgeeft, kunt u **stap b)**, **"Voeg een betrouwbaar/intern CA-certificaat toe".** Het is niet nodig om hetzelfde CA certificaat opnieuw toe te voegen en het moet ook worden vermeden. Als hetzelfde CA-certificaat opnieuw wordt toegevoegd, is trustpoint geconfigureerd met "validatie-gebruik geen" wat invloed kan hebben op de certificaatverificatie voor RAVPN.

Stap 1. Navigeer naar Devices > Certificates en klik op Add.

Selecteer Apparaat en klik op plusteken (+) onder Volledige inschrijving.

Hier wordt "auth-risaggar-ca" gebruikt om identiteits-/gebruikerscertificaten af te geven.

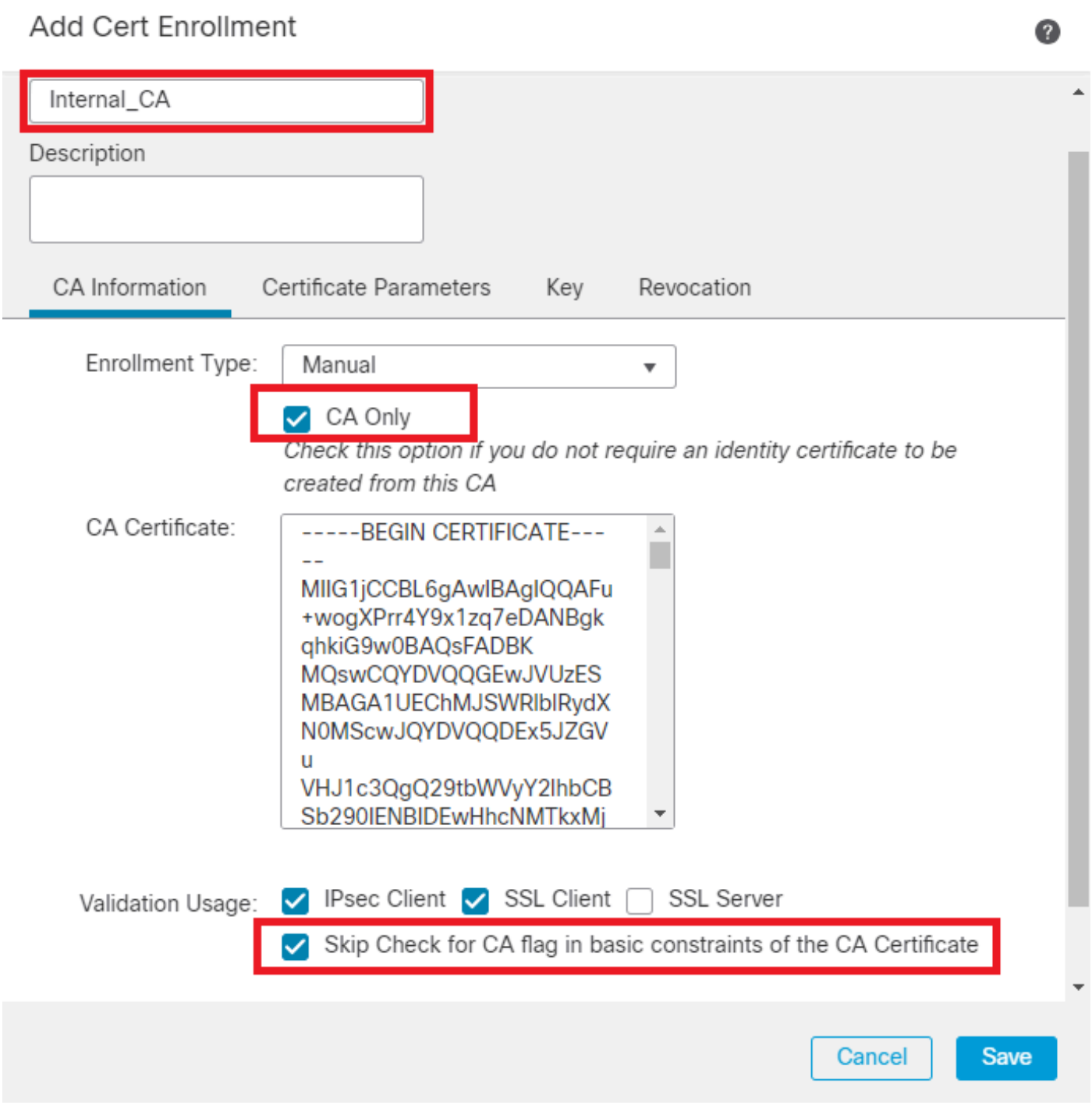


auth-risaggar-ca

Stap 2. Voer een trustpoint naam in en selecteerManual als het inschrijvingstype onder CA information.

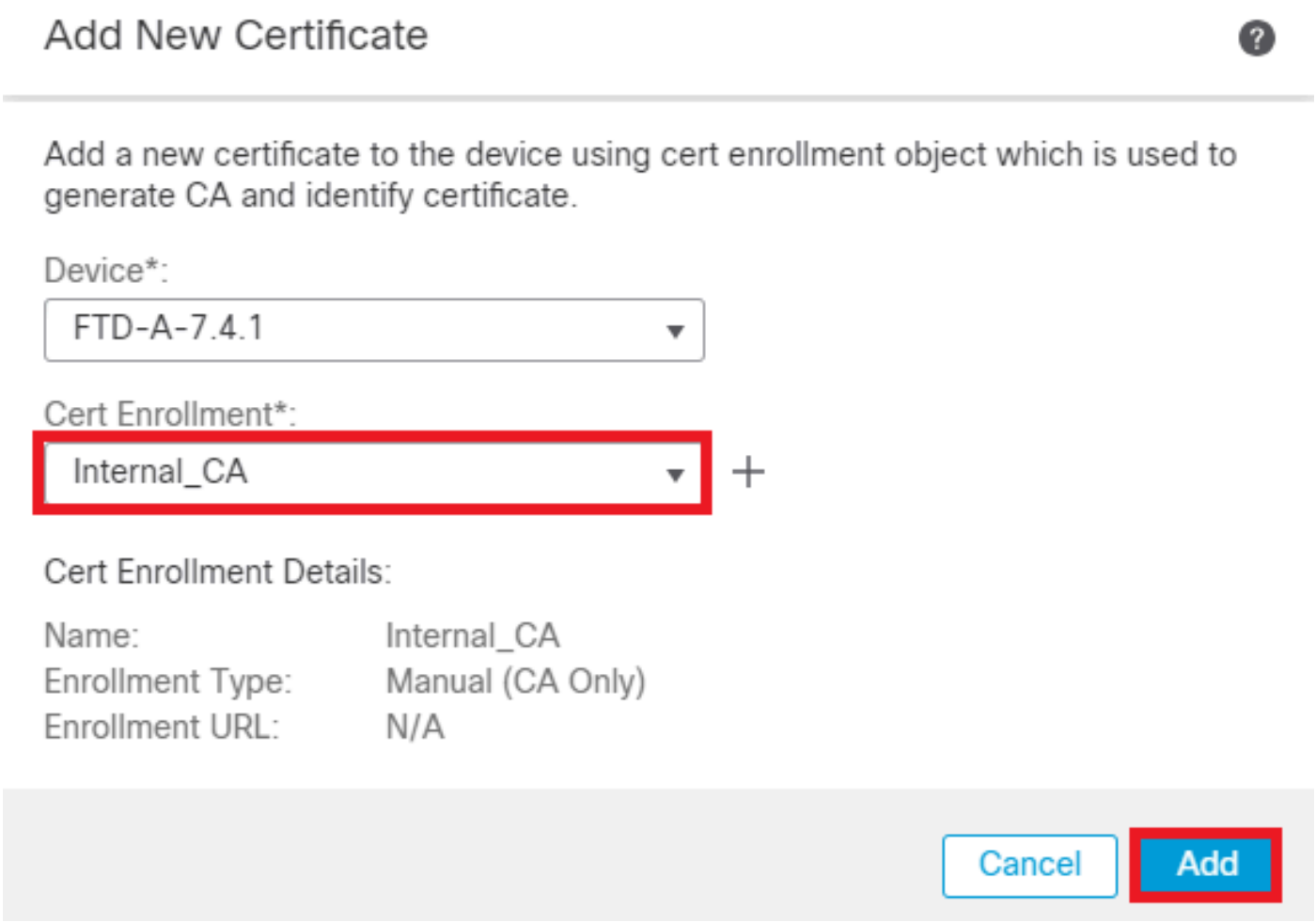
Stap 3. Controleer CA Onlyen plak het vertrouwde/interne CA-certificaat in pem-indeling.

Stap 4. Controleer **Skip Check for CA flag in basic constraints of the CA Certificate**en klik op Save.



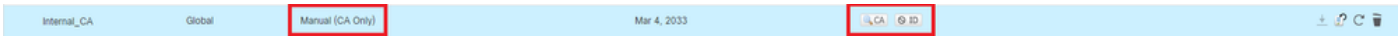
Trustpoint toevoegen

Stap 5. Onder Cert Enrollment, selecteer het trustpoint van dropdown die net werd gecreëerd en klik Add.



Interne CA toevoegen

Stap 6. Het eerder toegevoegde certificaat wordt weergegeven als:

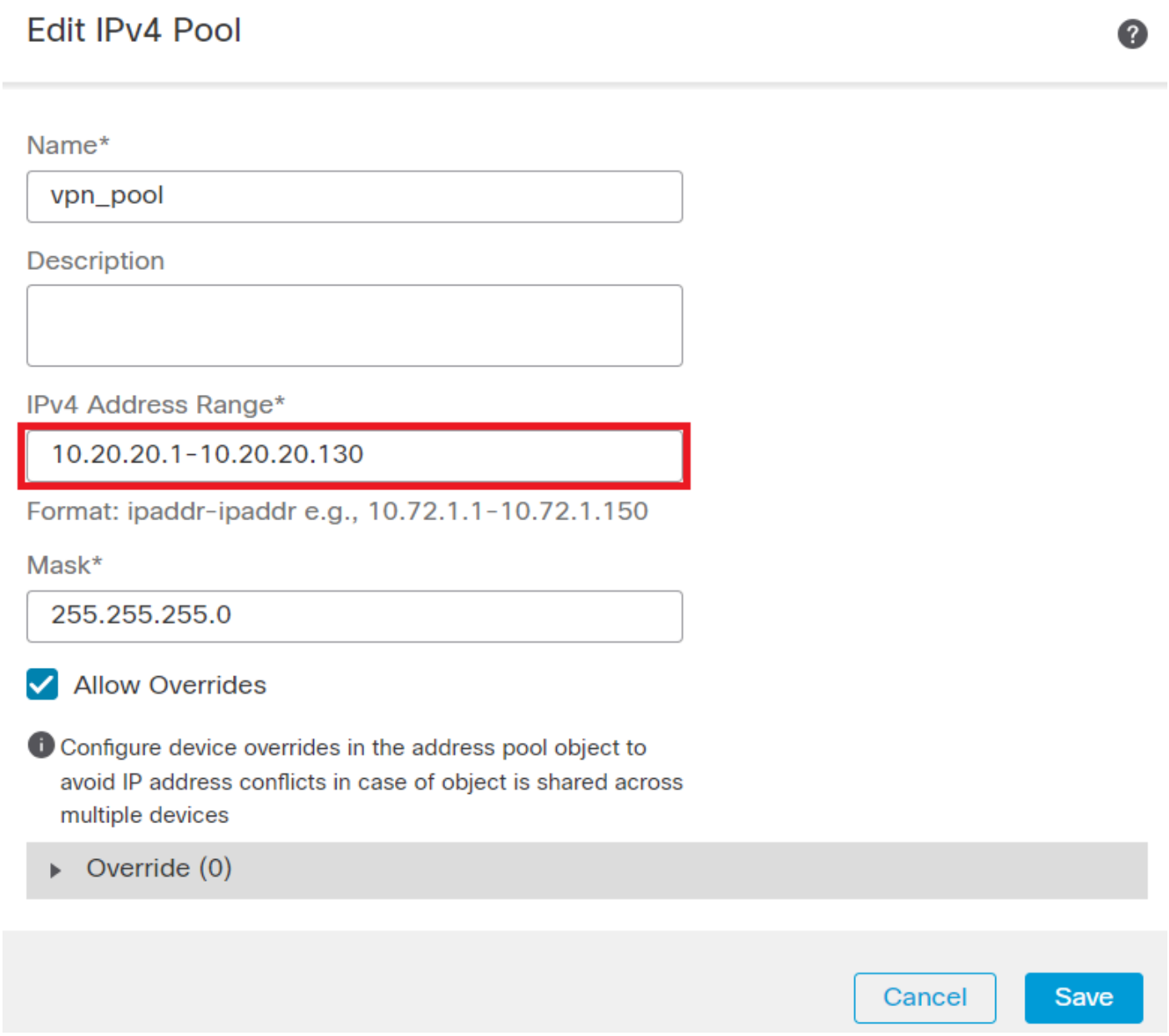


Toegevoegd certificaat

c. Adresgroep voor VPN-gebruikers configureren

Stap 1. Navigeer naar Objects > Object Management > Address Pools > IPv4 Pools .

Stap 2. Voer de naam en het IPv4-adresbereik in met een masker.



IPv4-pool toevoegen

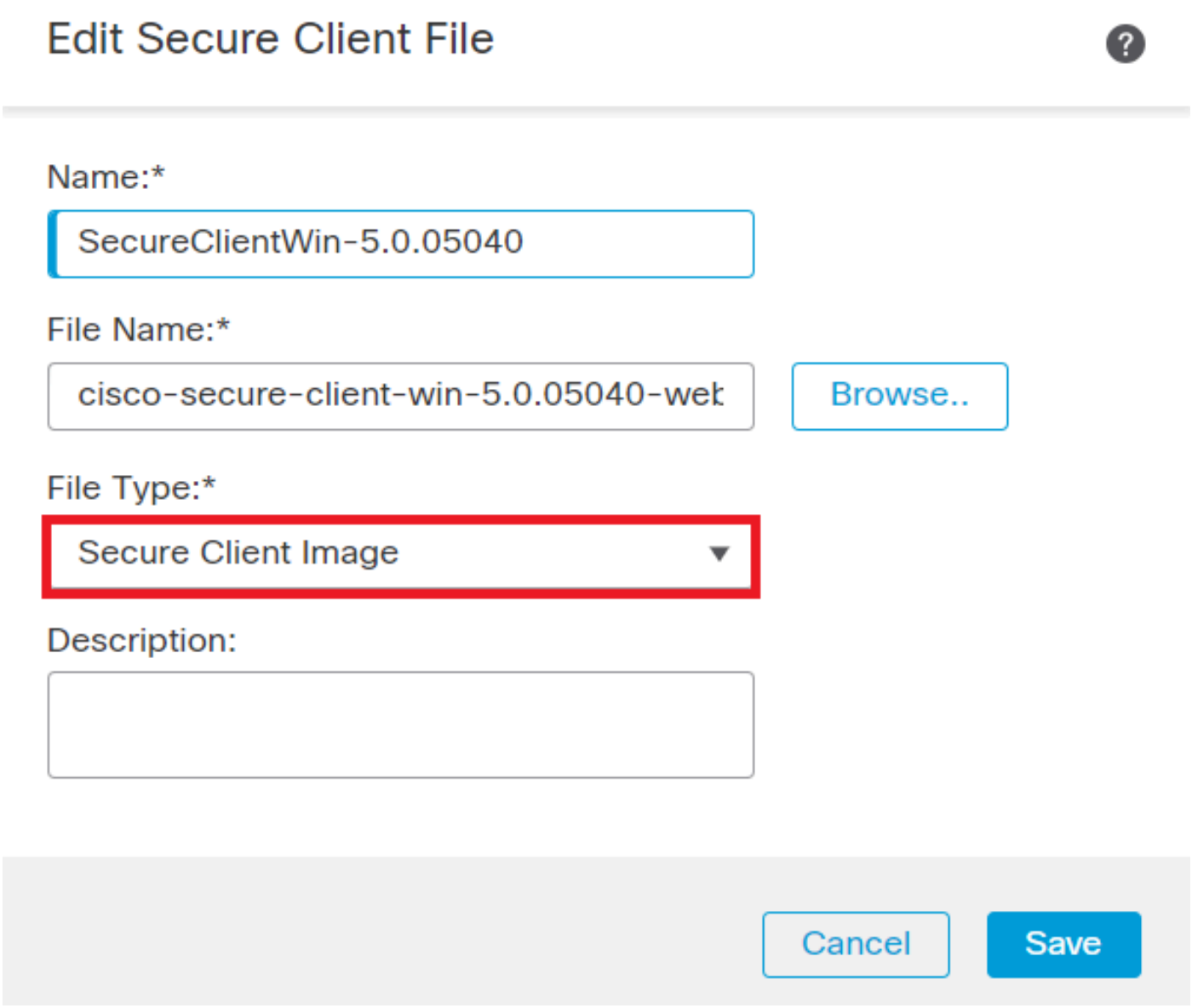
d. Beveiligde clientafbeeldingen uploaden

Stap 1. Download webimplementeer beveiligde client-afbeeldingen volgens het besturingssysteem van de Cisco-softwaresite.

Stap 2. Navigeer naar Objects > Object Management > VPN > Secure Client File > Add Secure Client File .

Stap 3. Voer de naam in en selecteer het bestand Secure Client (Beveiligde client) op de schijf.

Stap 4. Selecteer het bestandstype als Secure Client Image en klik op Save.



Een beveiligde clientafbeelding toevoegen

e. XML-profiel maken en uploaden

Stap 1. Download en installeer de Secure Client Profile Editor vanaf de Cisco-softwaresite.

Stap 2. Maak een nieuw profiel en selecteer All uit de vervolgkeuzelijst Clientcertificaat. Het regelt voornamelijk welke certificaatopslag(en) Secure Client kan gebruiken om certificaten op te slaan en te lezen.

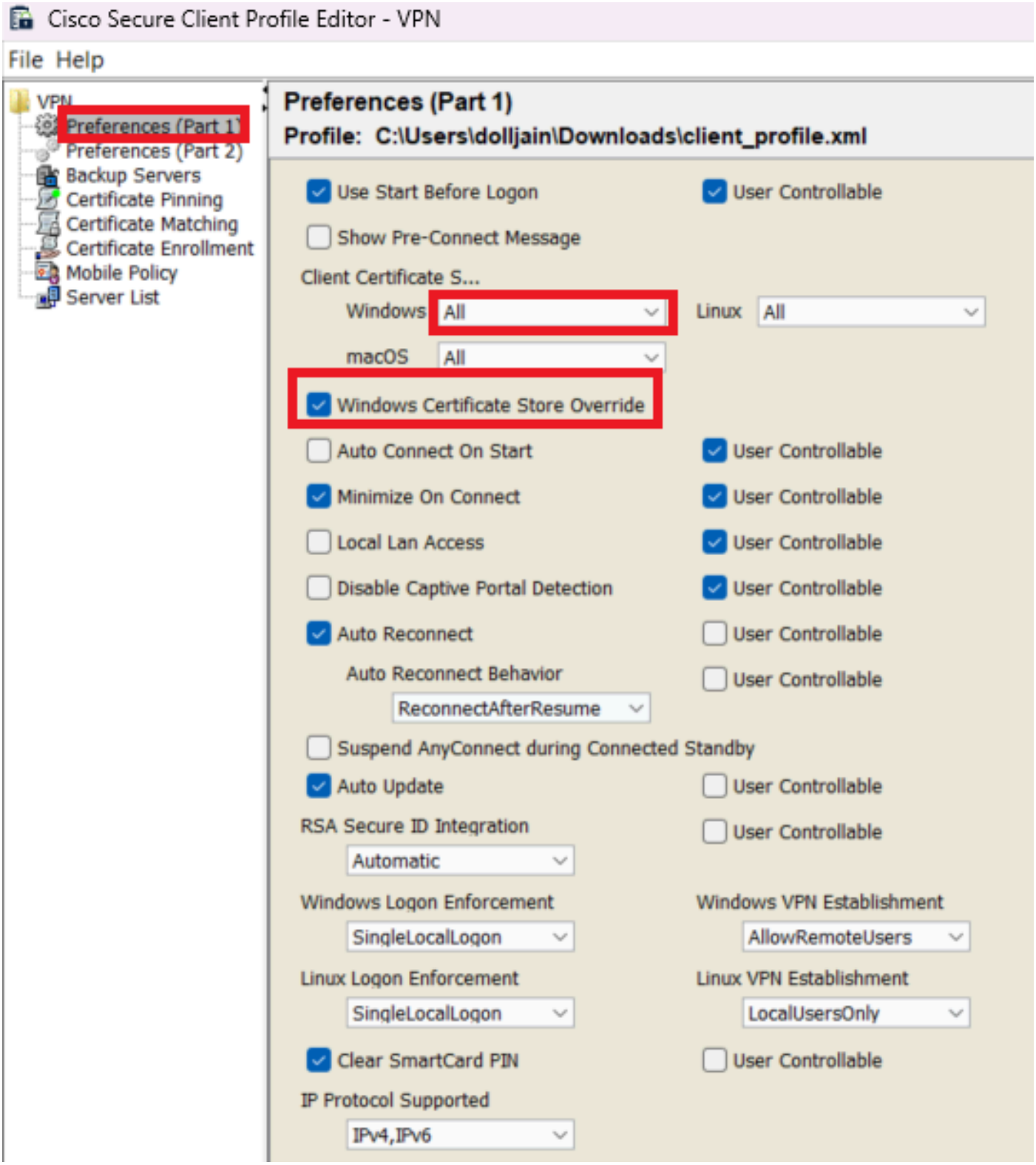
Twee andere beschikbare opties zijn:

- **Machine** - Secure Client is beperkt tot het opzoeken van certificaten in het lokale Windows-certificaatarchief.
- **Gebruiker** - Secure Client is beperkt tot het opzoeken van certificaten in het lokale Windows-gebruikerscertificaatarchief.

certificaatarchief instellen op True .

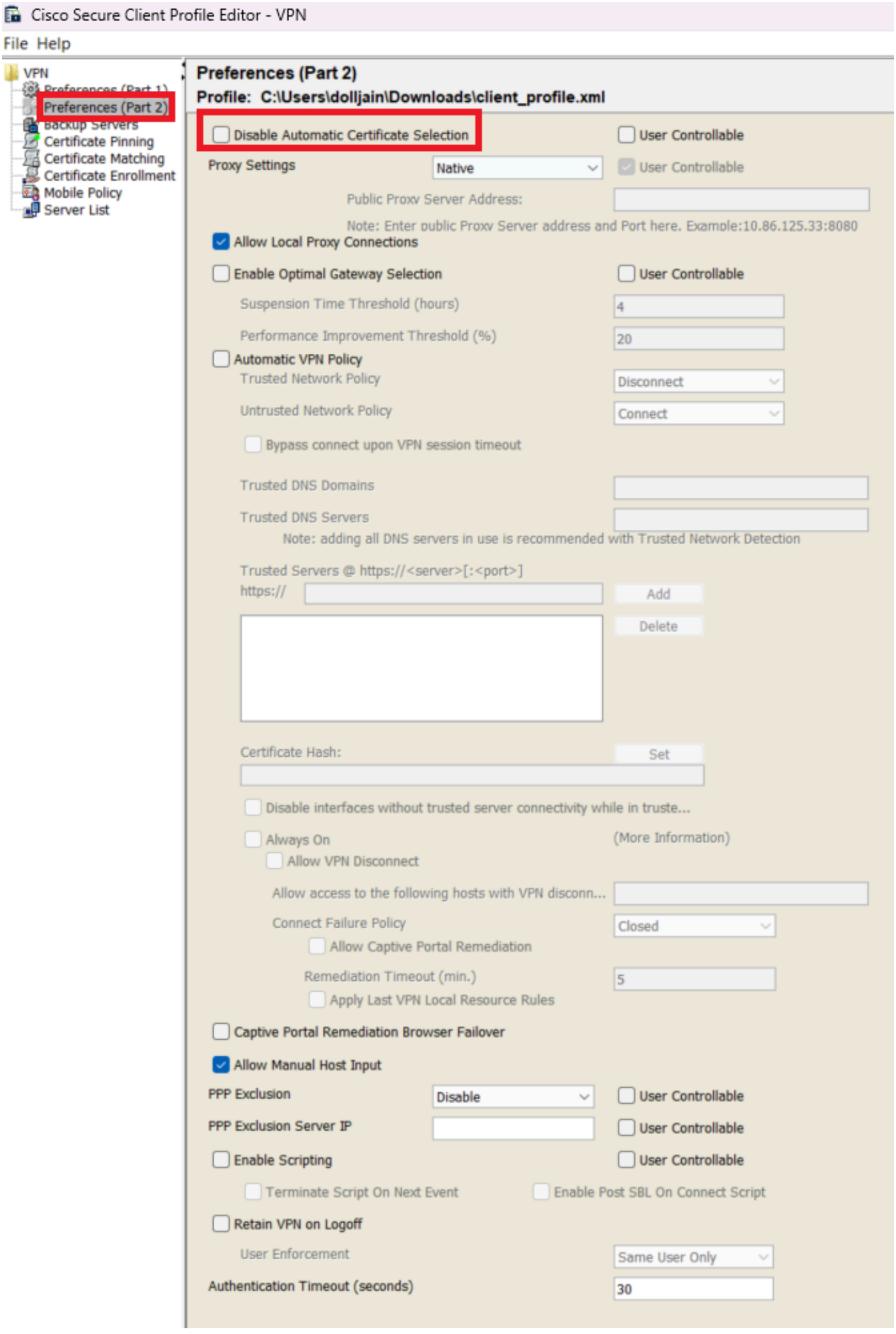
Hiermee kan een beheerder beveiligde client opdracht geven om certificaten te gebruiken in het certificeringsarchief van het Windows-systeem

(lokaal systeem) voor de verificatie van clientcertificaten. Certificate Store Override is alleen van toepassing op SSL, waar de verbinding standaard wordt geïnitieerd door het UI-proces. Wanneer u IPSec/IKEv2 gebruikt, is deze voorziening in het beveiligde clientprofiel niet van toepassing.



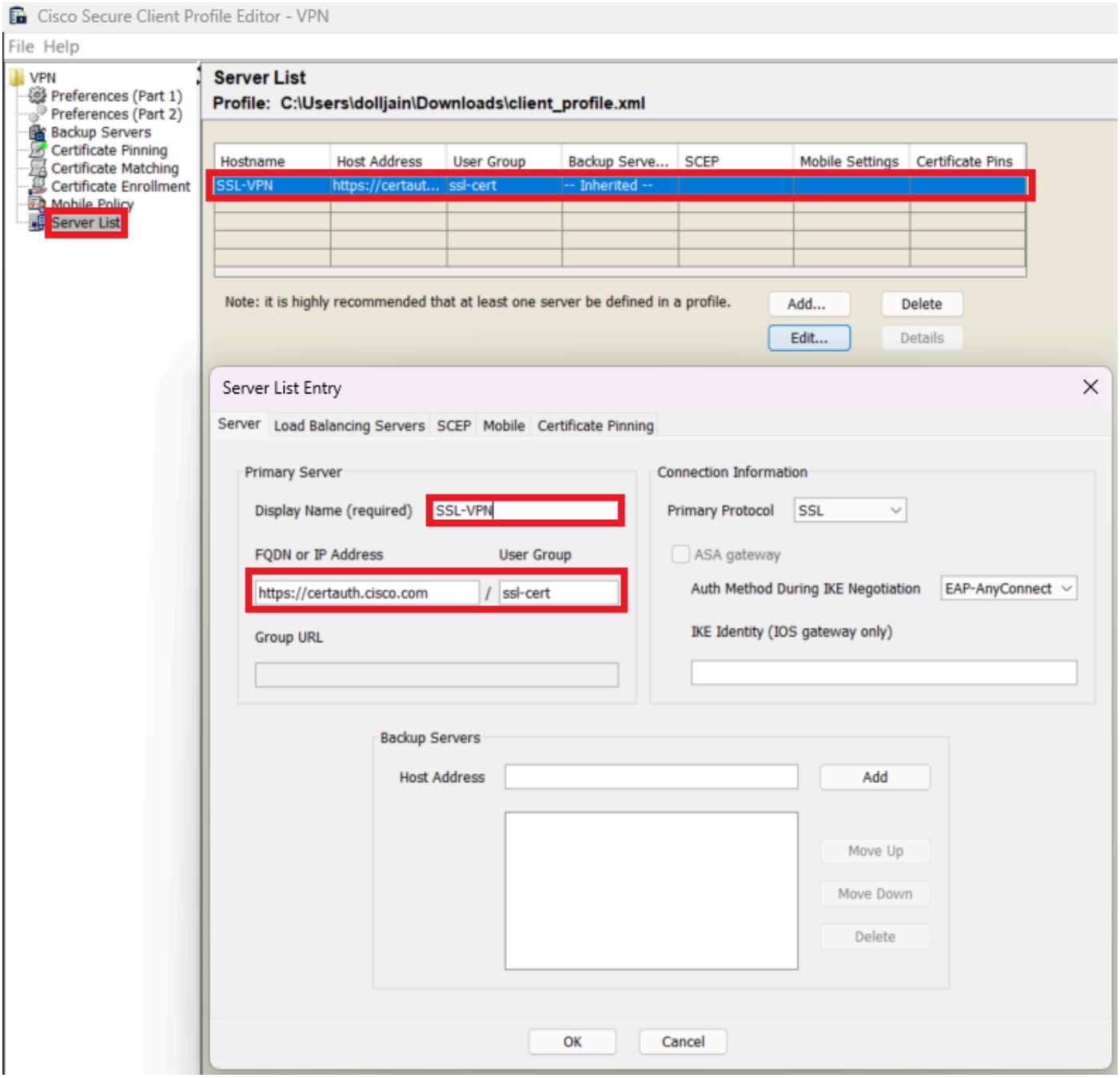
Voorkeuren toevoegen (Deel 1)

Stap 3. (Optioneel) Schakel de optie uit omdat de gebruiker niet wordt gevraagd hetDisable Automatic Certificate Selection verificatiecertificaat te selecteren.



Voorkeuren toevoegen (Deel 2)

Server List Entry voor het instellen van een profiel in Secure Client VPN door groep-alias en groep-url te bieden onder de Serverlijst en sla het XML-profiel op.



Serverlijst toevoegen

Stap 5. Tot slot is het XML profiel klaar voor gebruik.

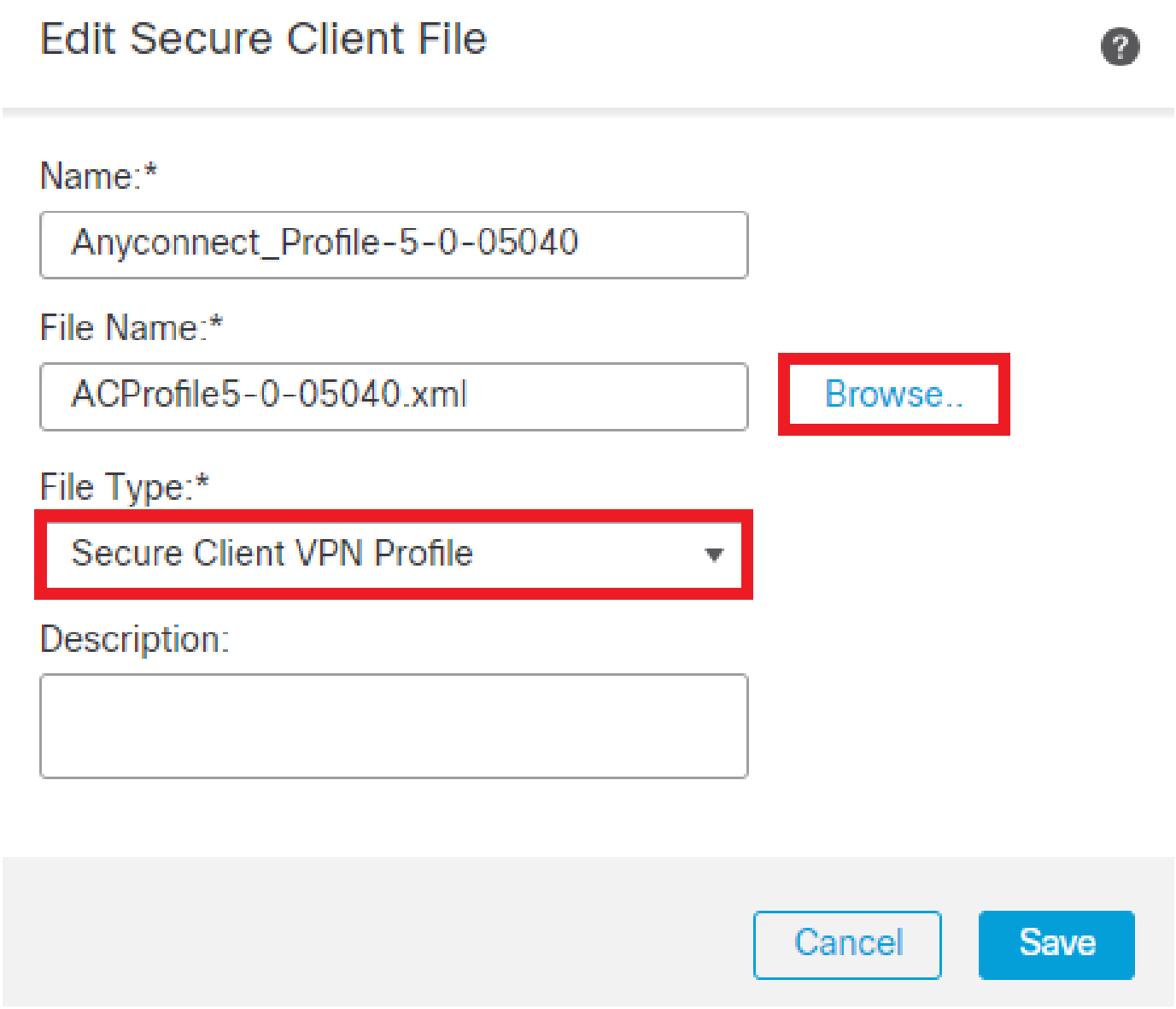
XML-profiel

Locatie van XML profielen voor verschillende besturingssystemen:

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

Stap 6. Navigeer naar Objects > Object Management > VPN > Secure Client File > Add Secure Client Profile .

Voer de naam voor het bestand in en klik op Browse om het XML-profiel te selecteren. Klik op de knop .Save

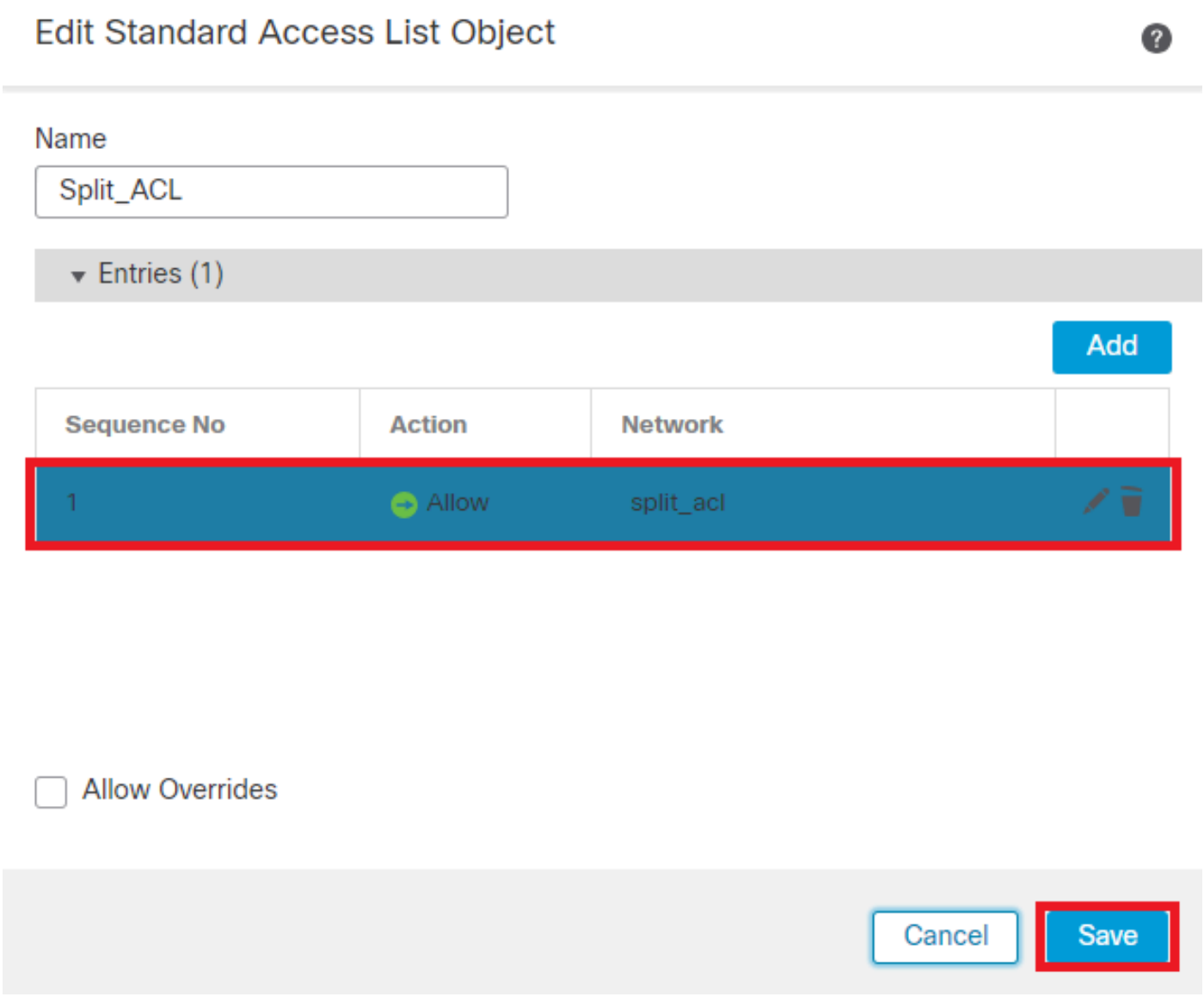


VPN-profiel voor beveiligde client toevoegen

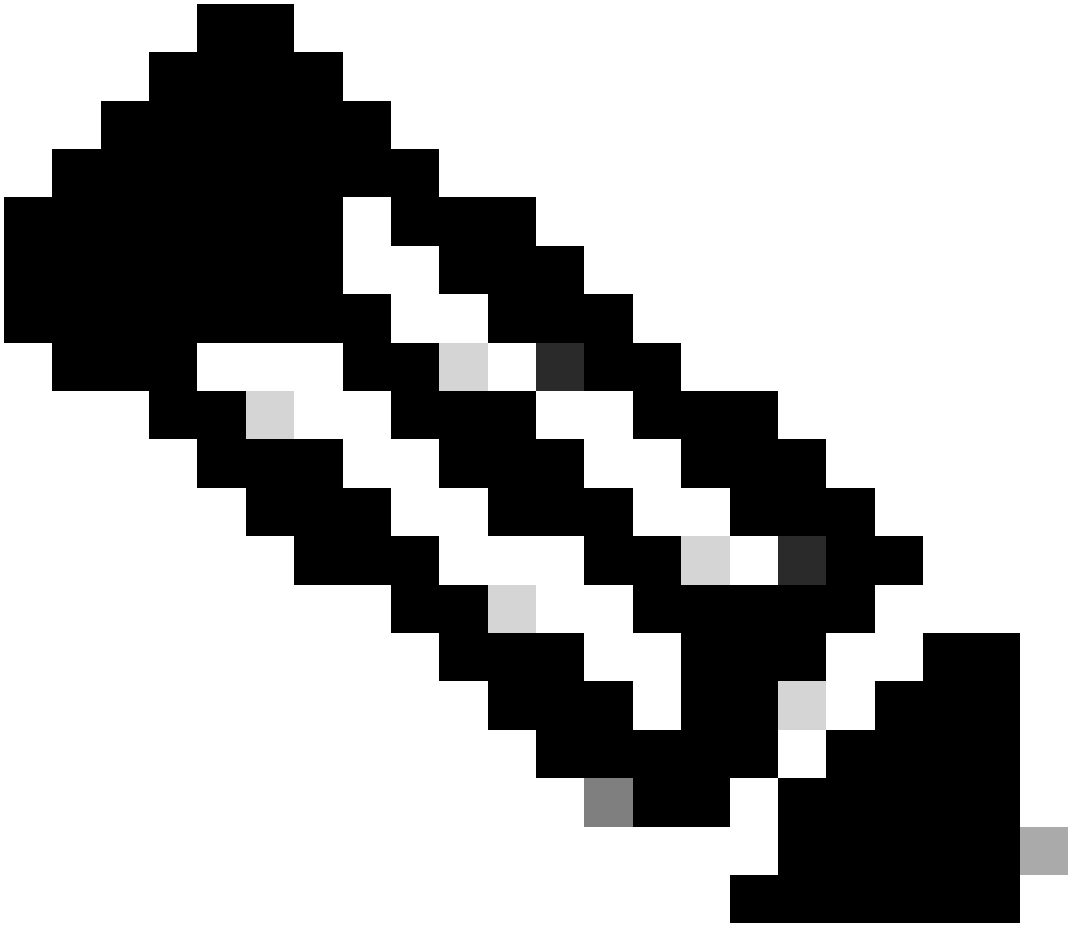
Configuratie van VPN voor externe toegang

Stap 1. Maak een ACL per vereiste om toegang tot interne bronnen te verlenen.

Navigeer naar Objects > Object Management > Access List > Standard en klik op Add Standard Access List.



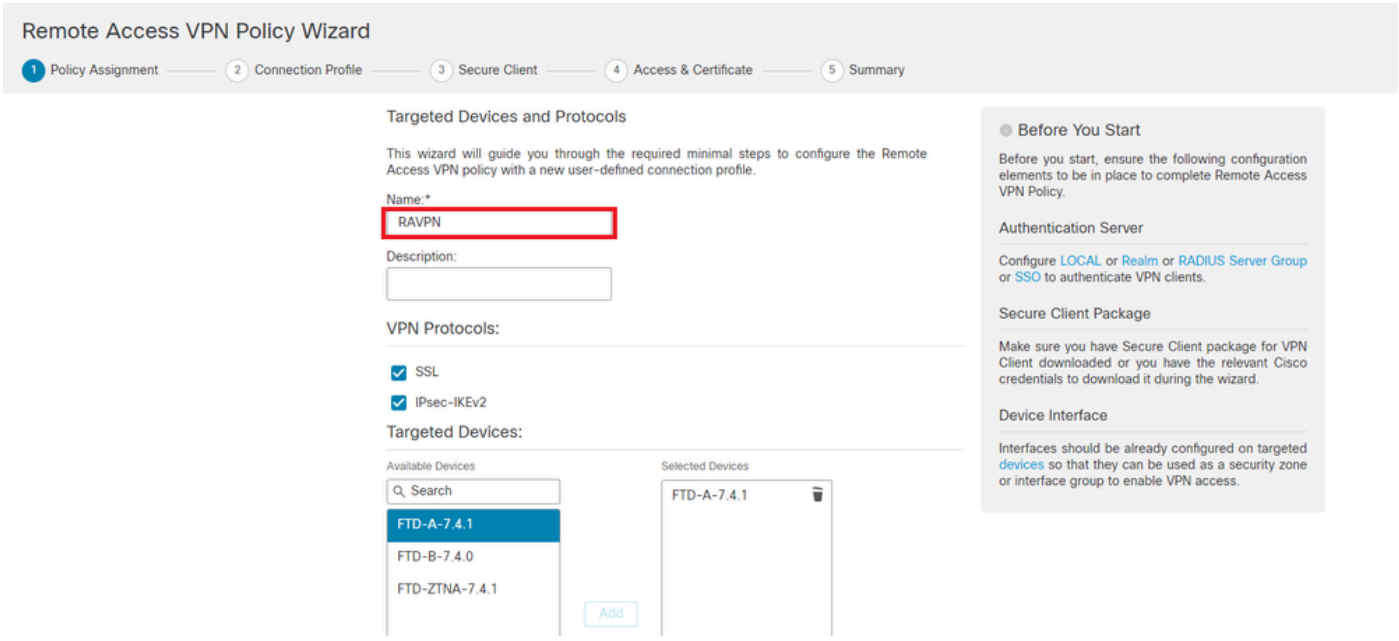
Standaard ACL toevoegen



Opmerking: deze ACL wordt gebruikt door beveiligde client om beveiligde routes aan interne bronnen toe te voegen.

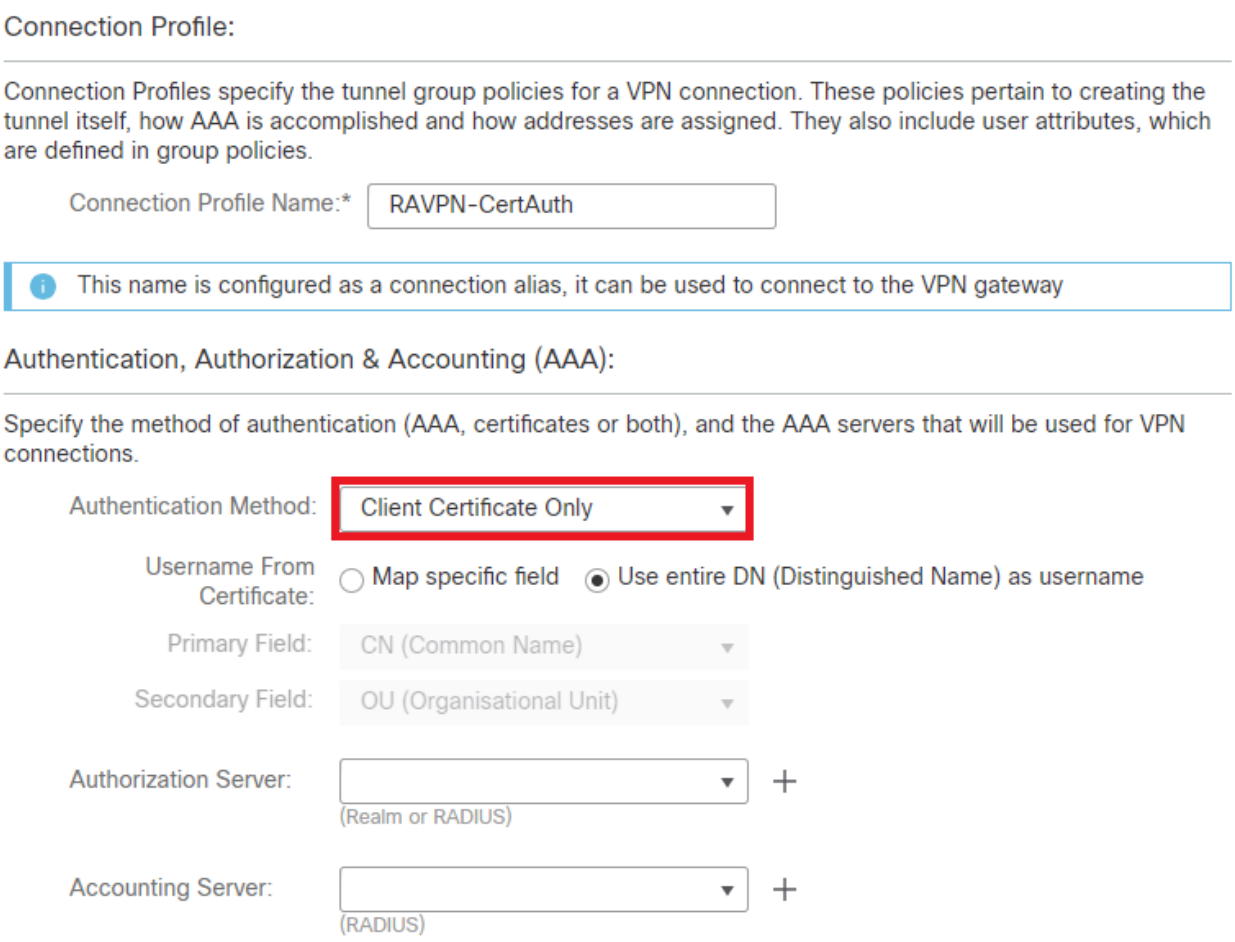
Stap 2. Navigeer naar Devices > VPN > Remote Access en klik op Add.

Stap 3. Typ de naam van het profiel, selecteer vervolgens het FTD-apparaat en klik op Volgende.



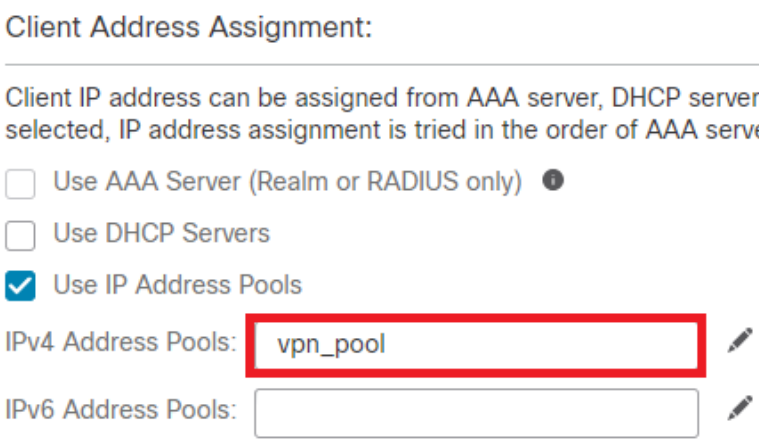
Profielnaam toevoegen

Stap 4. Voer de gegevens in Connection Profile Nameen selecteer de verificatiemethode zoals Client Certificate Only onder Verificatie, autorisatie en accounting (AAA).



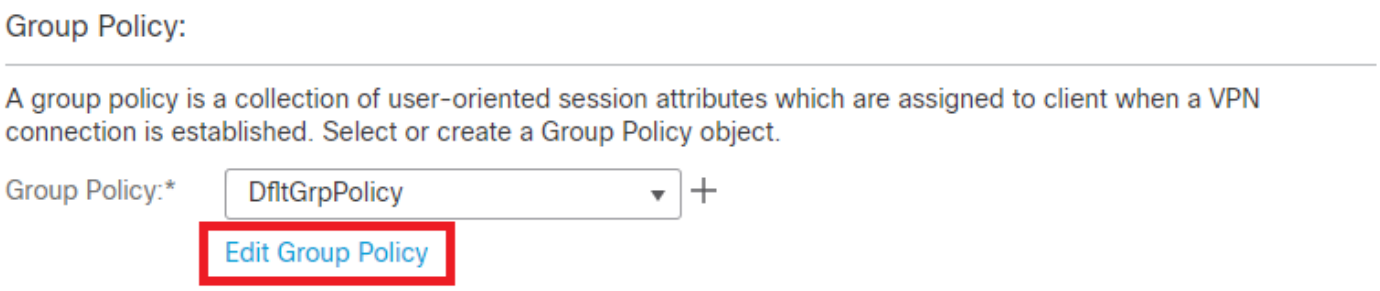
Selecteer een verificatiemethode

Stap 5. Klik op Use IP Address Pools onder Toewijzing clientadres en selecteer de IPv4-adresgroep die eerder is gemaakt.



Selecteer Toewijzing van clientadres

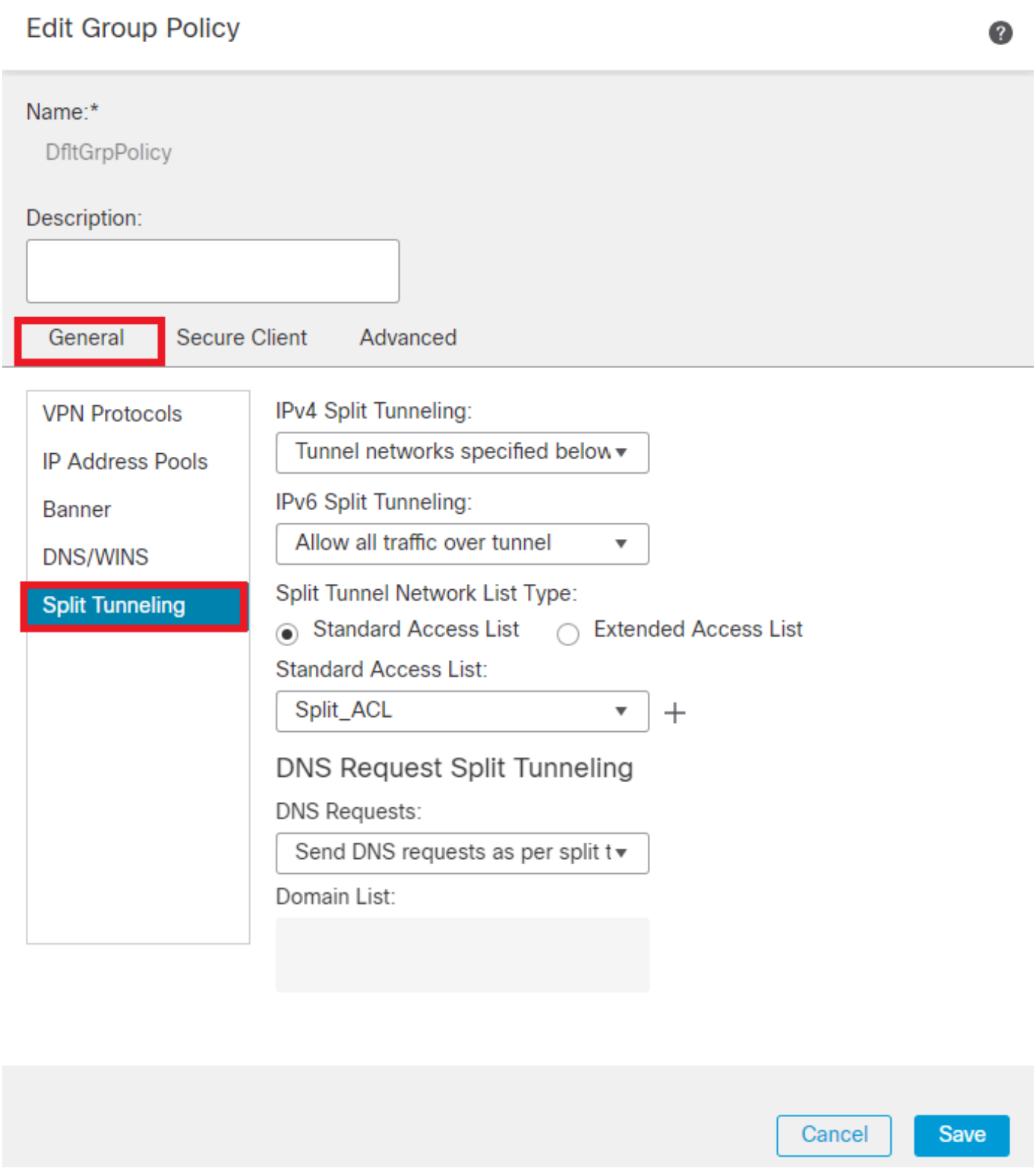
Stap 6. Bewerk het groepsbeleid.



Groepsbeleid bewerken

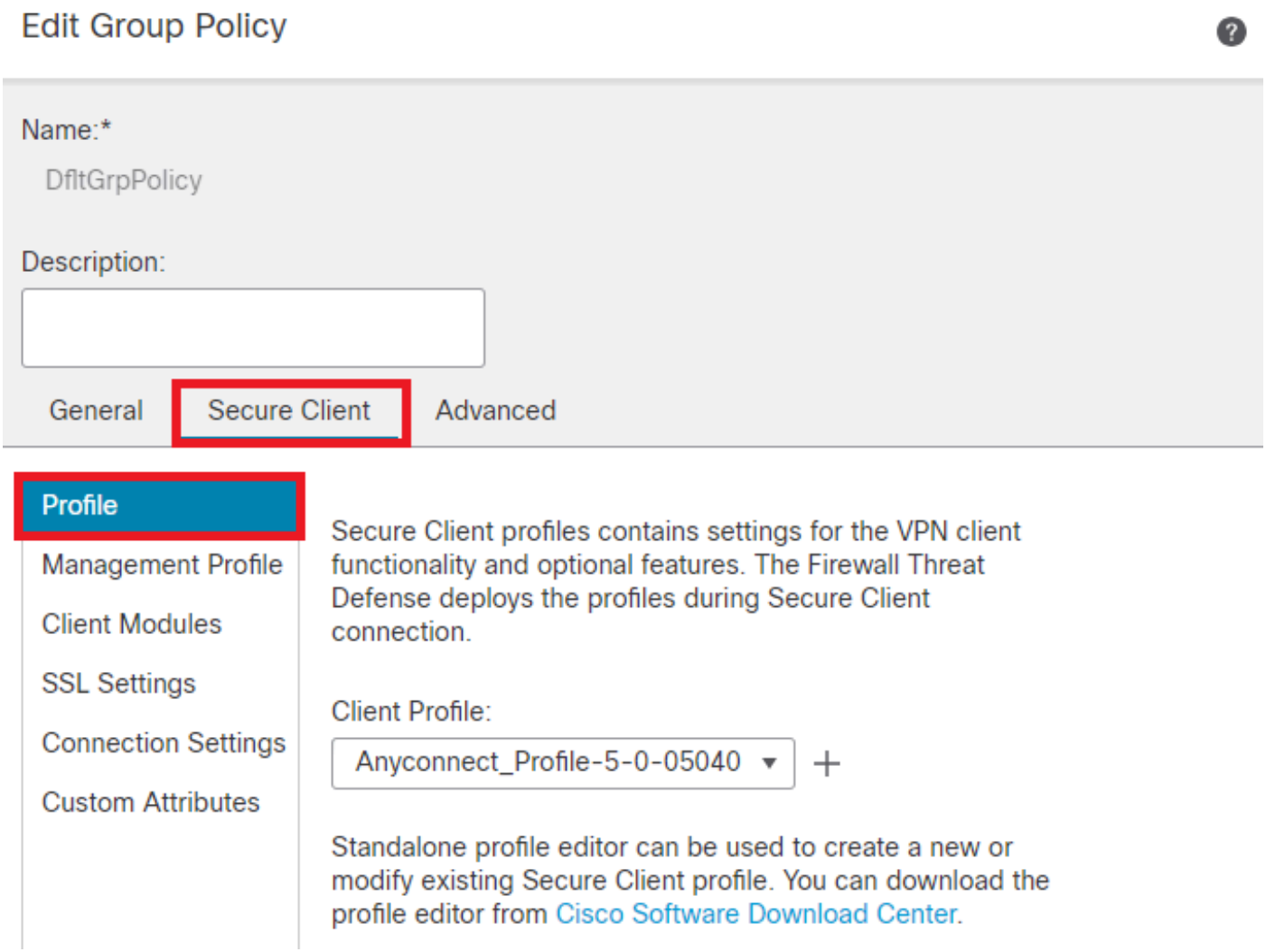
Stap 7. Navigeer naar General > Split Tunneling , selecteer Tunnel networks specified below en selecteer Standard Access List onder Netwerklijsttype splitter tunnel.

Selecteer de ACL die eerder is gemaakt.



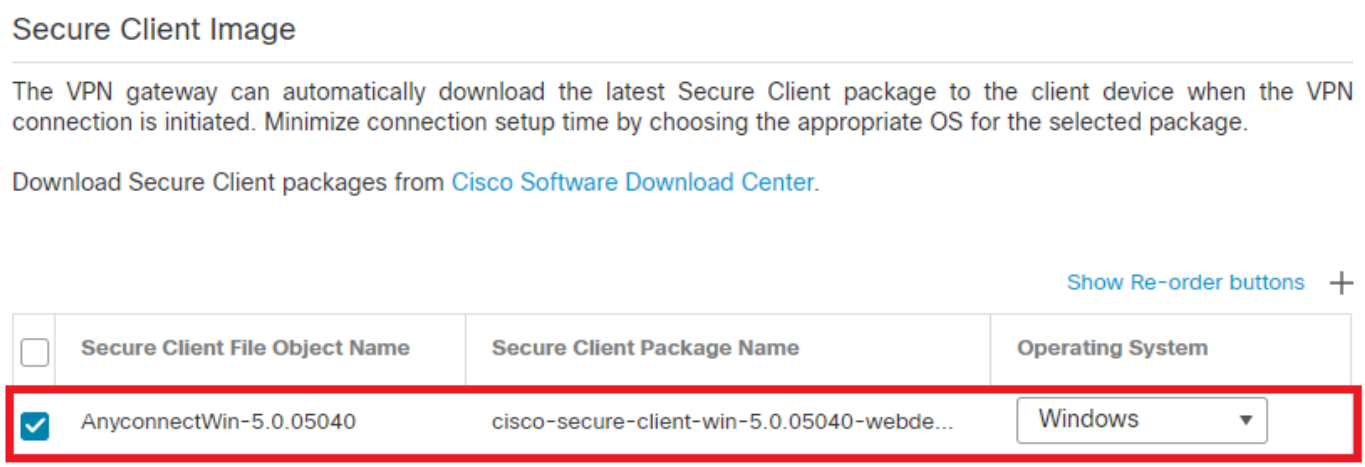
Split-tunneling toevoegen

Stap 8. Navigeer naar Secure Client > Profile , selecteer de Client Profile en klik Save.



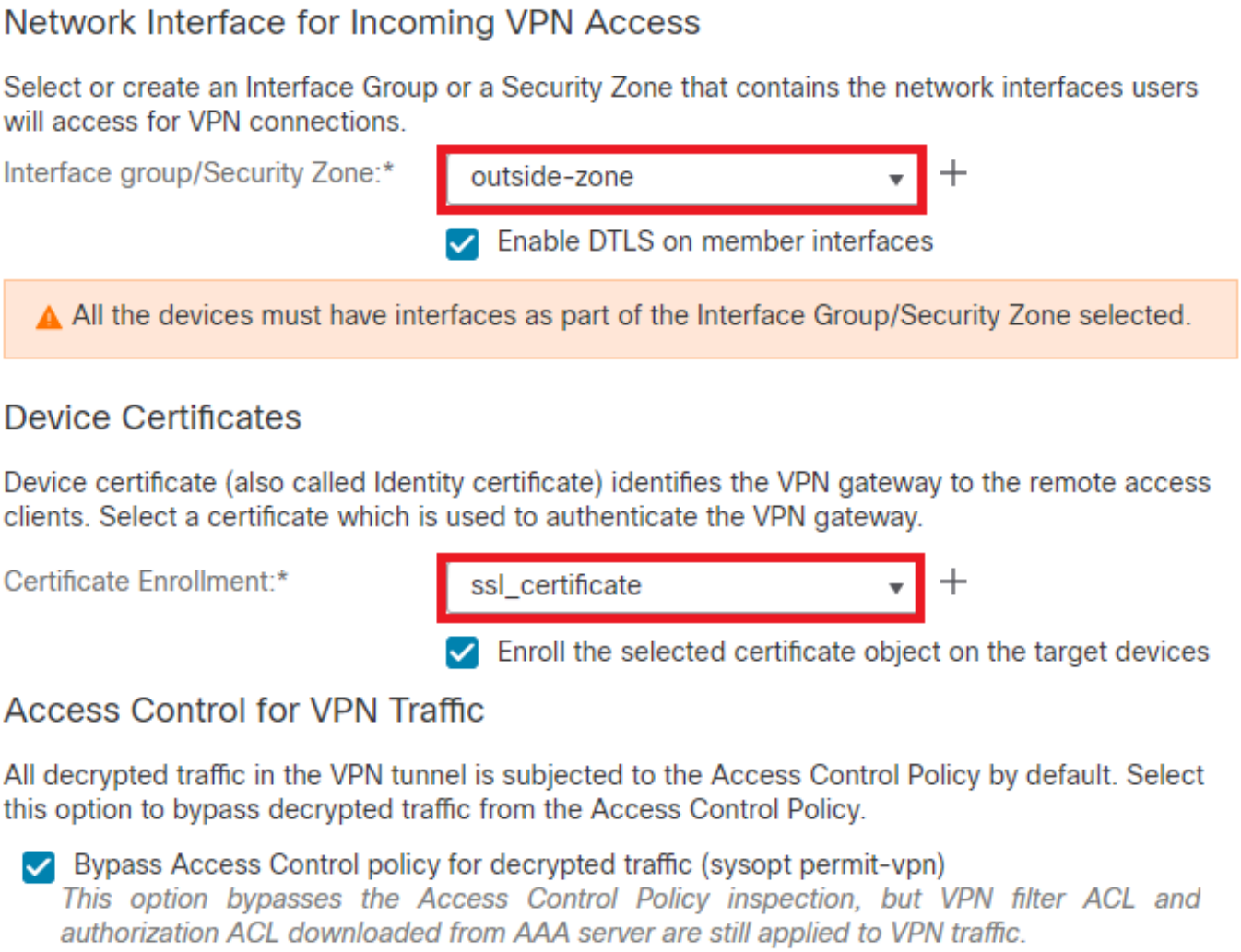
Beveiligd clientprofiel toevoegen

Stap 9. Klik op Next, selecteer vervolgens de knop Secure Client Image en klik op Next.



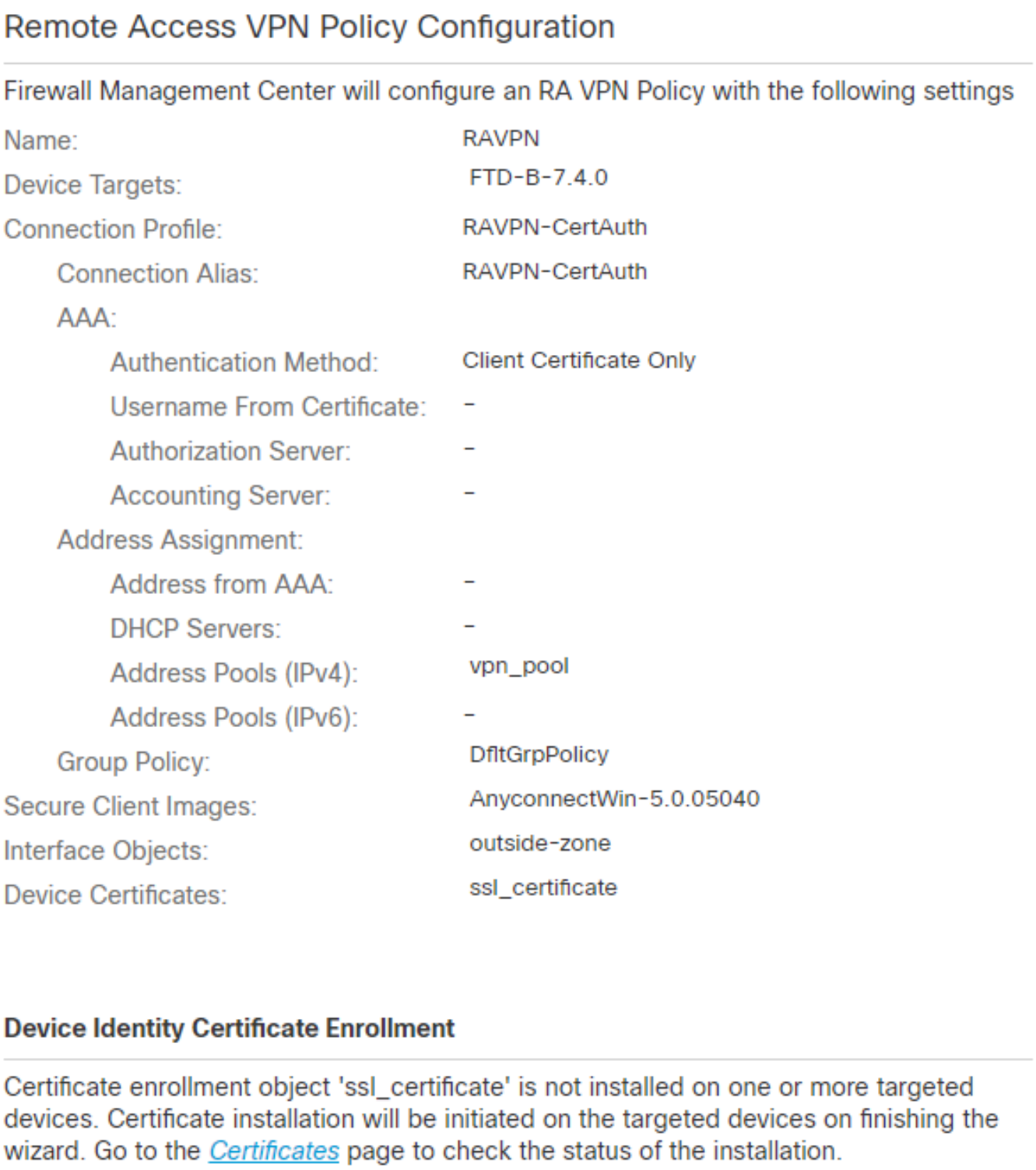
Een beveiligde clientafbeelding toevoegen

Stap 10. Selecteer de Netwerkinterface voor VPN-toegang, kies de Device Certificates en controleer sysopt license-vpn en klik op Next.



Add Access Control voor VPN-verkeer

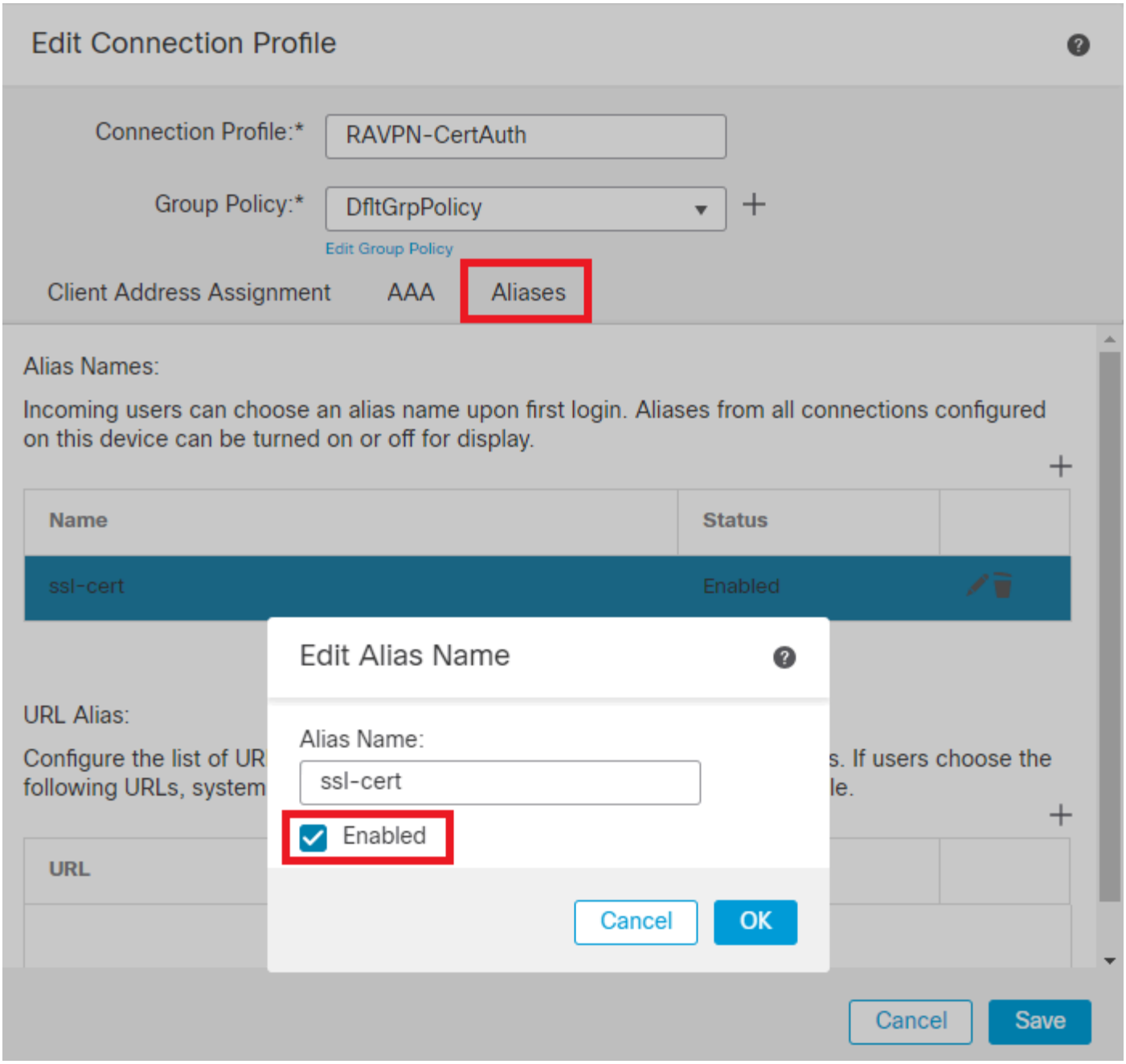
Stap 11. Controleer tot slot alle configuraties en klik op Finish.



Configuratie van VPN-beleid voor externe toegang

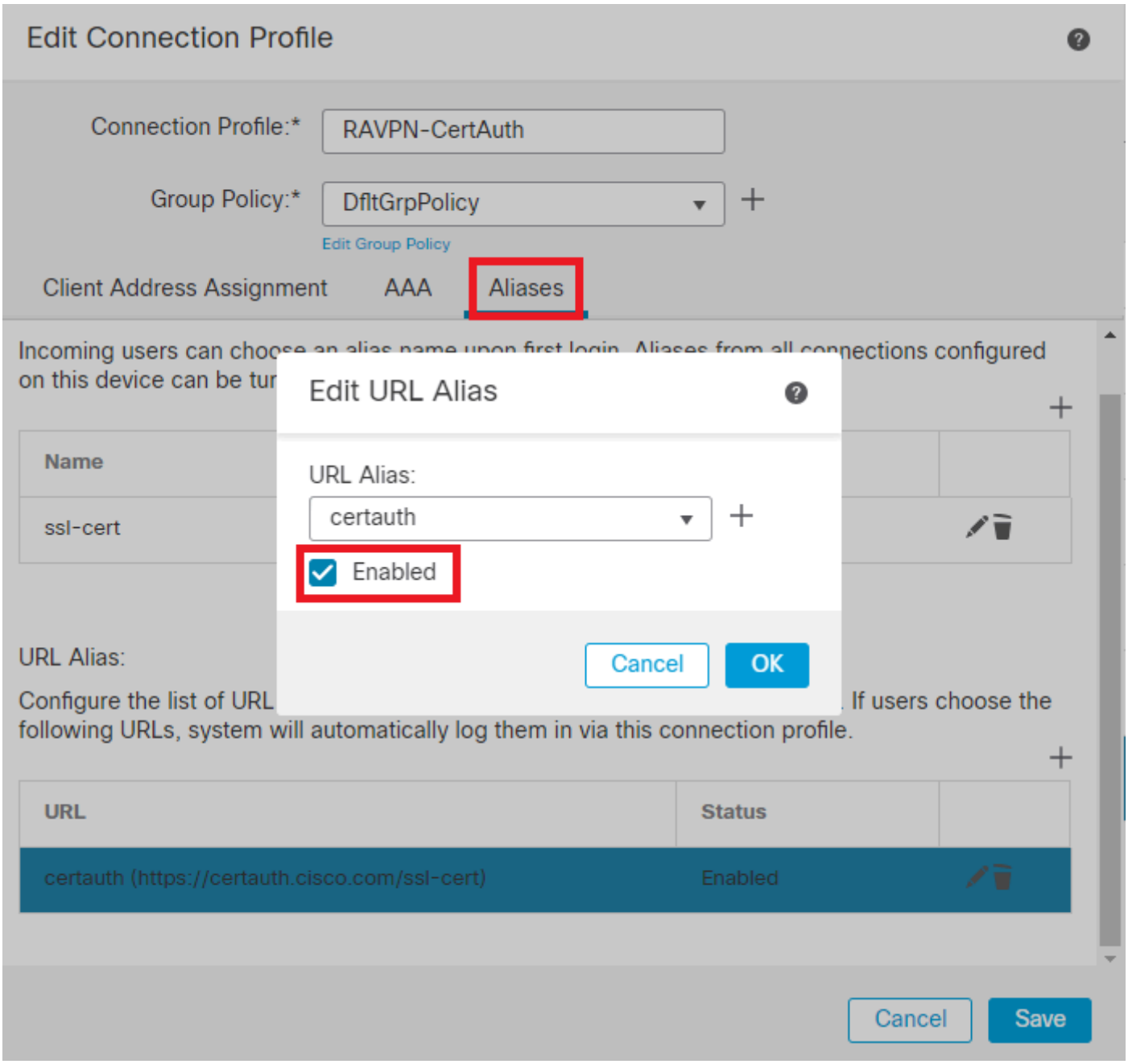
Stap 12. Nadat de eerste configuratie van Remote Access VPN is voltooid, bewerk je het verbindingsprofiel dat is gemaakt en ga je naar Aliases.

Stap 13. Configureer group-alias door op het plus-pictogram (+) te klikken.



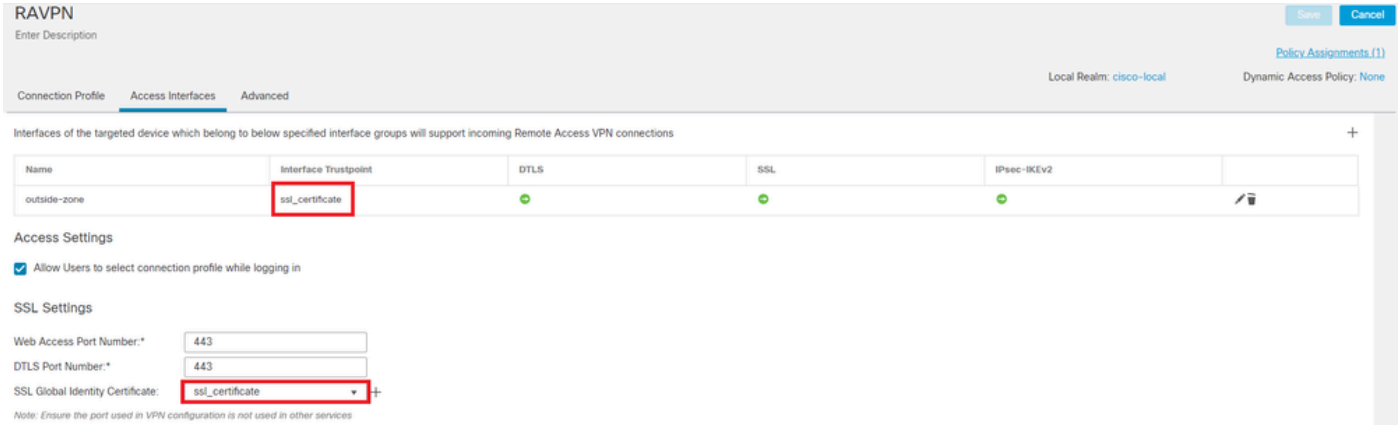
Groepsalias bewerken

Stap 14. Configureer group-url door op het plus-pictogram (+) te klikken. Gebruik dezelfde URL voor groep die eerder in het clientprofiel is geconfigureerd.



URL voor groep bewerken

Stap 15. Navigeren naar toegangsinterfaces. Selecteer de Interface Truspoint en de SSL Global Identity Certificate onder de SSL-instellingen.



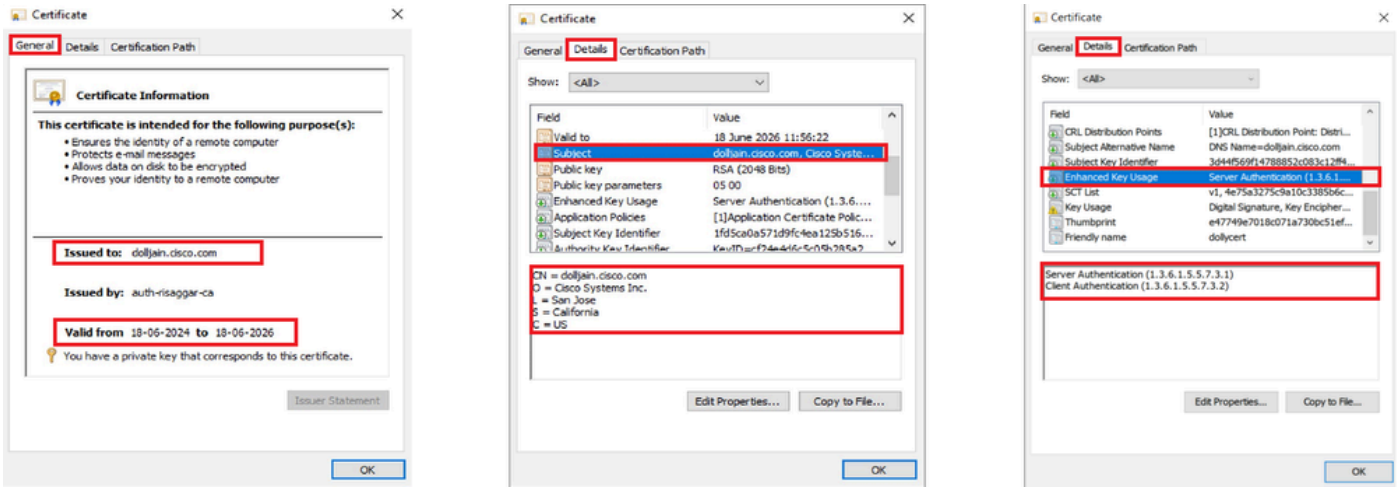
Toegangsinterfaces bewerken

Stap 16. KlikSave en implementeer deze wijzigingen.

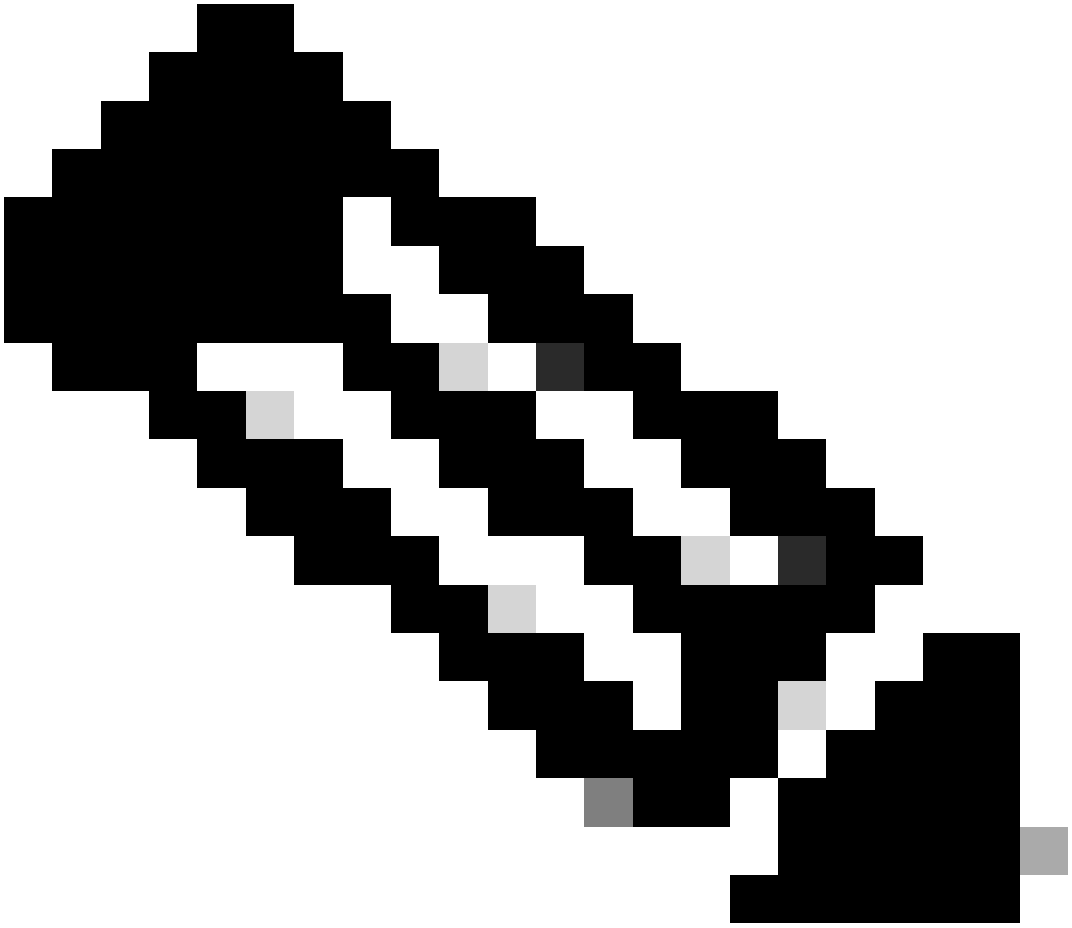
Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

1. Op de beveiligde client-pc moet het certificaat met een geldige datum, onderwerp en EKU op de pc van de gebruiker zijn geïnstalleerd. Dit certificaat moet worden afgegeven door de bevoegde instantie waarvan het certificaat op het FTD is geïnstalleerd, zoals eerder is aangegeven. Hier wordt het identiteits- of gebruikerscertificaat afgegeven door "auth-risaggar-ca".

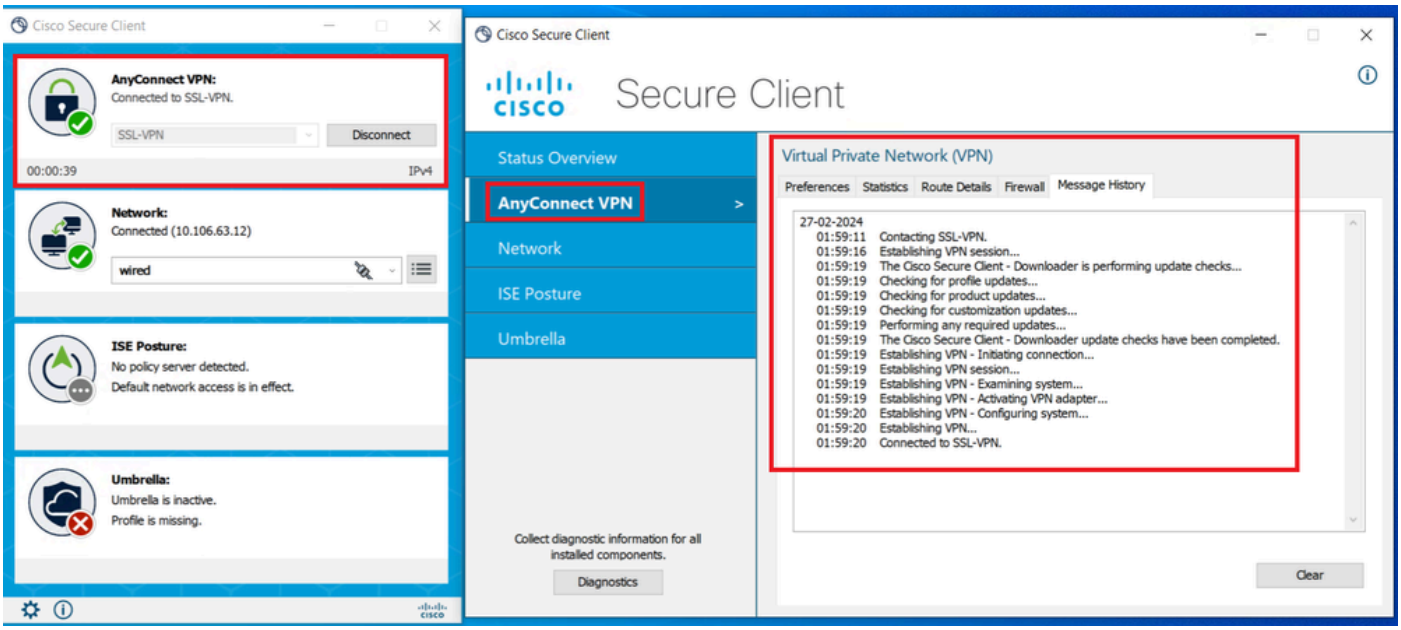


Kenmerken certificaat



Opmerking: voor het clientcertificaat moet de EKU (Enhanced Key Usage) voor clientverificatie zijn ingevoerd.

2. Secure Client moet de verbinding tot stand brengen.



Succesvolle beveiligde clientverbinding

3. Uitvoeren show vpn-sessiondb anyconnect om de verbindingsgegevens van de actieve gebruiker in de gebruikte tunnelgroep te bevestigen.

```
firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

1. Debugs kunnen worden uitgevoerd vanaf de diagnostische CLI van de FTD:

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

2. Raadpleeg deze handleiding voor algemene problemen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.