AnyConnect certificaatgebaseerde verificatie voor mobiele toegang configureren

Inhoud

Inleiding

In dit document wordt een voorbeeld beschreven van de invoering van op certificaten gebaseerde echtheidscontrole op mobiele apparatuur.

Voorwaarden

De gereedschappen en hulpmiddelen die in de handleiding worden gebruikt, zijn:

- Cisco Firepower Threat Defense (FTD)
- FireSIGHT Management Center (FMC)
- Apple iOS-apparaat (iPhone, iPad)
- certificaatinstantie (CA)
- Cisco AnyConnect-clientsoftware

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis VPN,
- SSL/TLS
- Infrastructuur in openbare vorm
- Ervaring met FMC
- OpenSSL
- Cisco AnyConnect

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

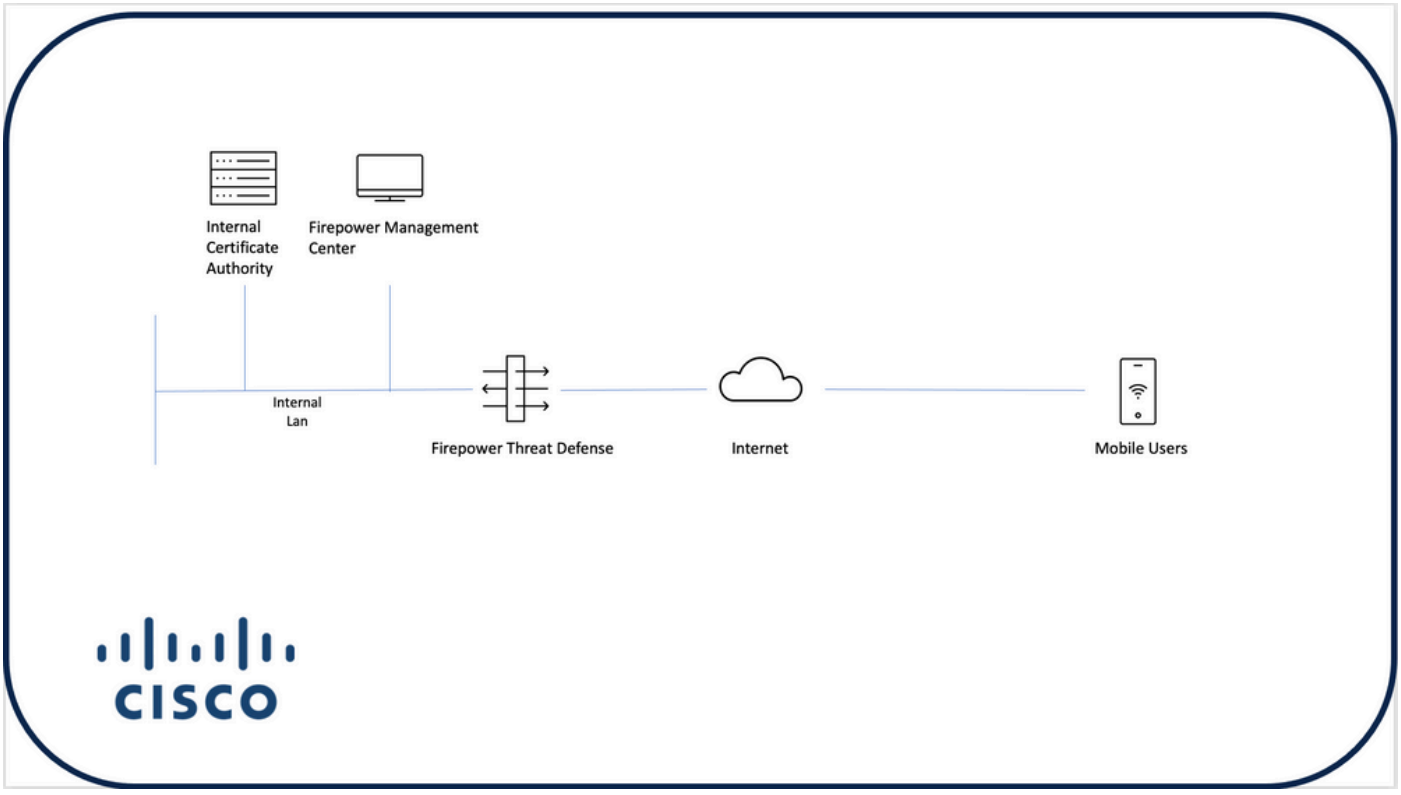
- Cisco FTD
- Cisco FMC
- Microsoft CA-server
- XCA
- Cisco AnyConnect
- Apple iPad

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.

Cisco AnyConnect op FTD configureren

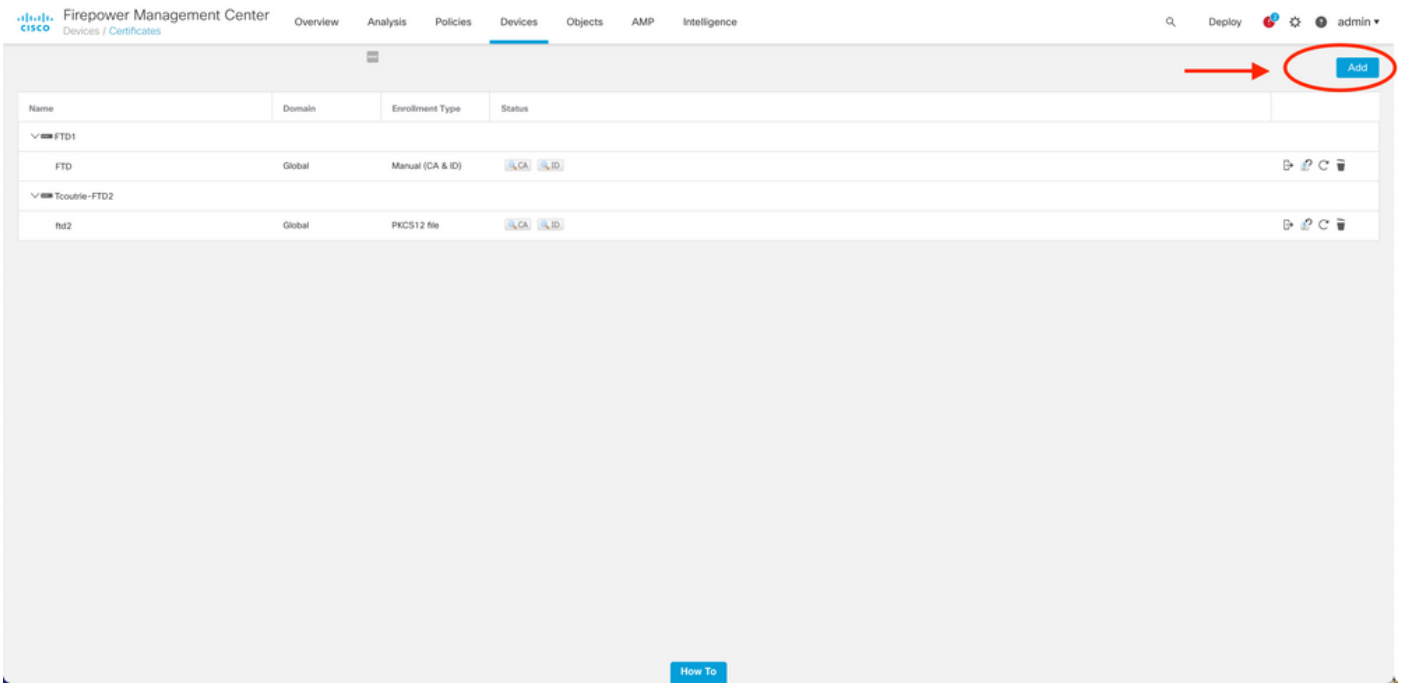
In dit gedeelte worden de stappen beschreven om AnyConnect via FMC te configureren. Zorg ervoor dat alle configuraties worden geïnstalleerd voordat u begint.

Netwerkdiagram

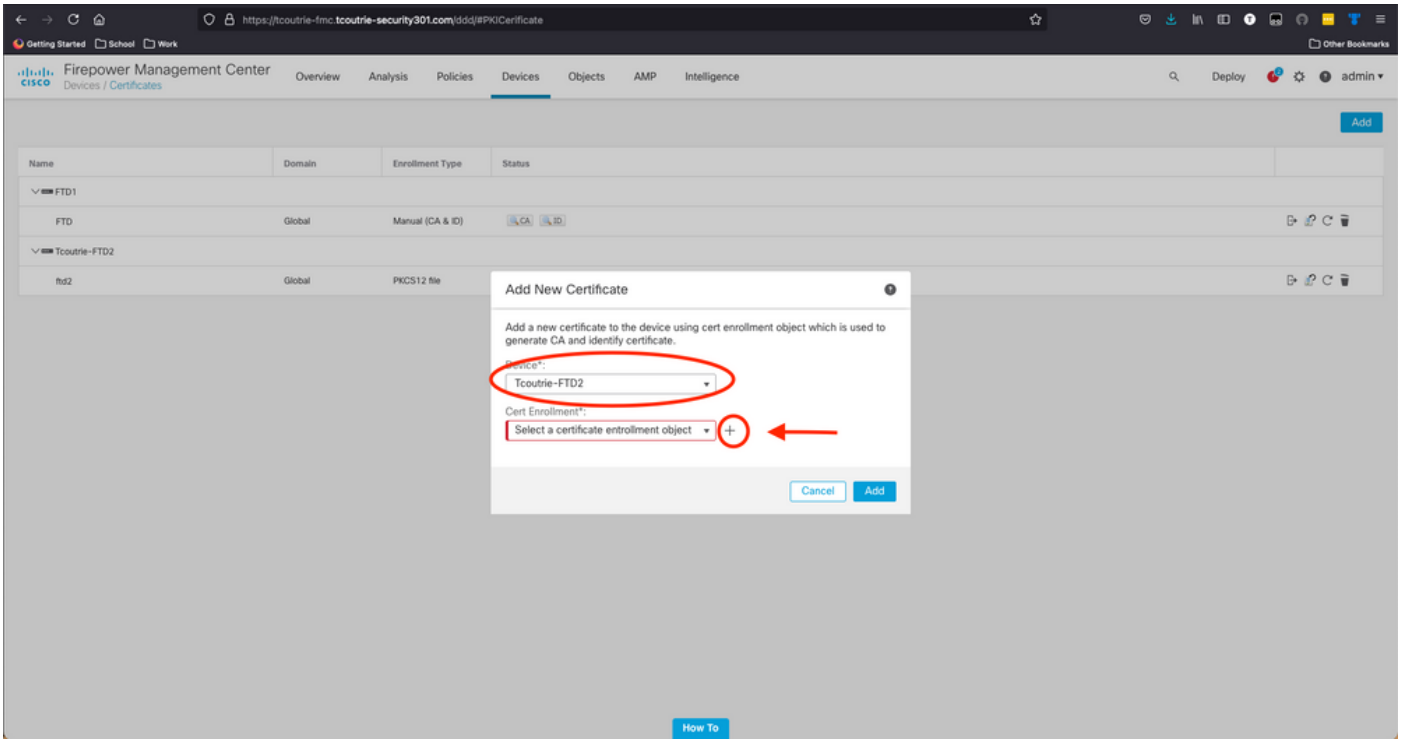


Certificaat aan FTD toevoegen

Stap 1. Maak een certificaat voor de FTD op het FMC-apparaat. Navigeren in op **Apparaten > Certificaat** en kiezen **Toevoegen**, zoals in deze afbeelding:



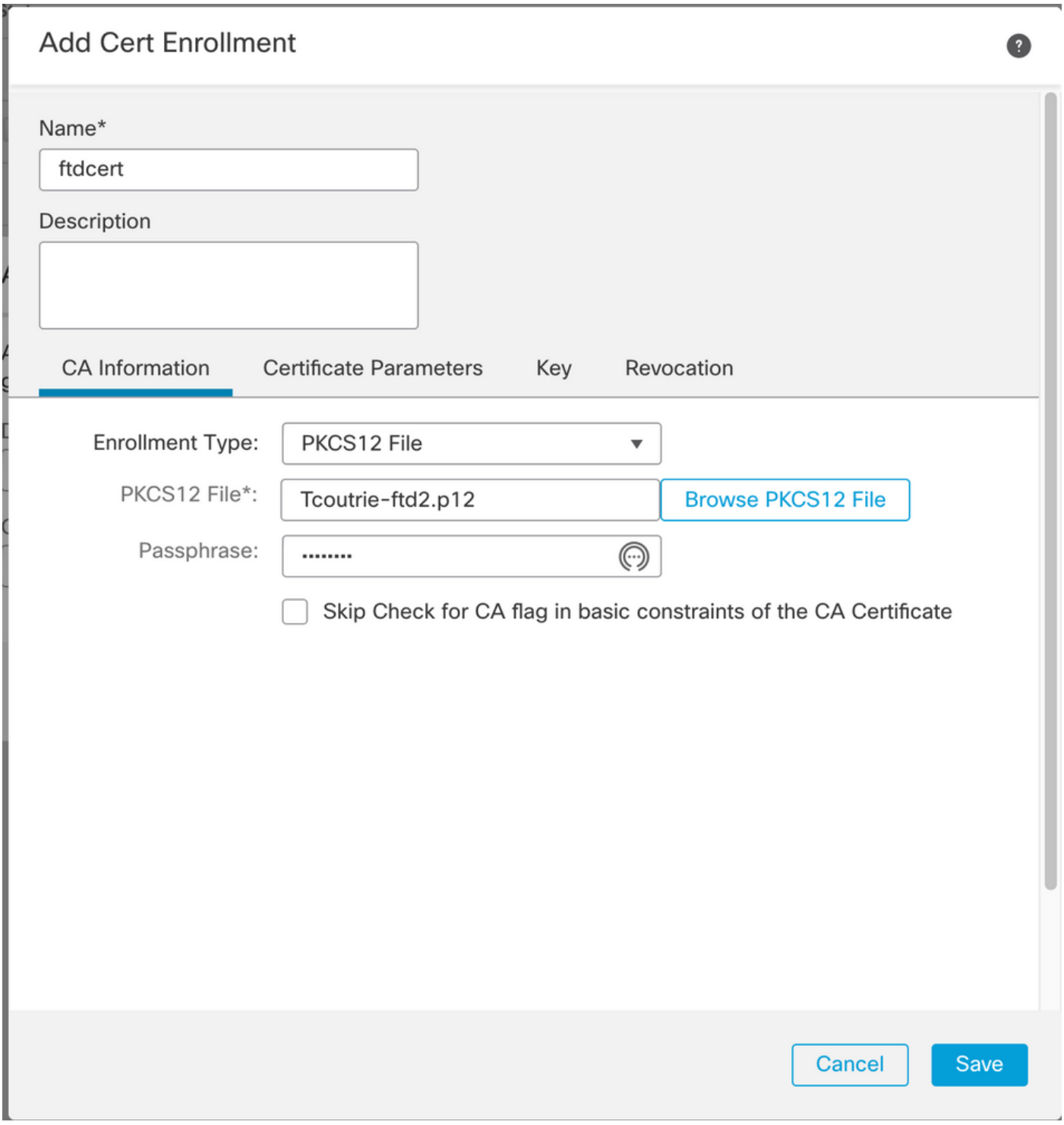
Stap 2. Kies de gewenste FTD voor de VPN-verbinding. Kies het **FTD** apparaat uit de afvoerslang. Klik op het pictogram **+** om een nieuwe inlogmethode voor certificaten toe te voegen, zoals in deze afbeelding:



Stap 3. Voeg de certificaten toe aan het apparaat. Kies de optie die de beste methode is om certificaten in de omgeving te verkrijgen.

> **Tip**: De beschikbare opties zijn: **Zelfgetekend certificaat** - genereer lokaal een nieuw certificaat, **SCEP** - gebruik eenvoudig protocol voor **certificaatinschrijving** voor een certificaat bij een CA, **handleiding** - installeer handmatig het **PKCS12**-geüpload certificaat met wortel, identiteit en privé-sleutel.

Stap 4. Upload het certificaat naar het FTD-apparaat. Voer de wachtcode in (alleen PKCS12) en klik op **Opslaan**, zoals in deze afbeelding:



Opmerking: Zodra u het bestand hebt opgeslagen, vindt de implementatie van de certificaten onmiddellijk plaats. Selecteer de gewenste ID voor de certificeringsgegevens.

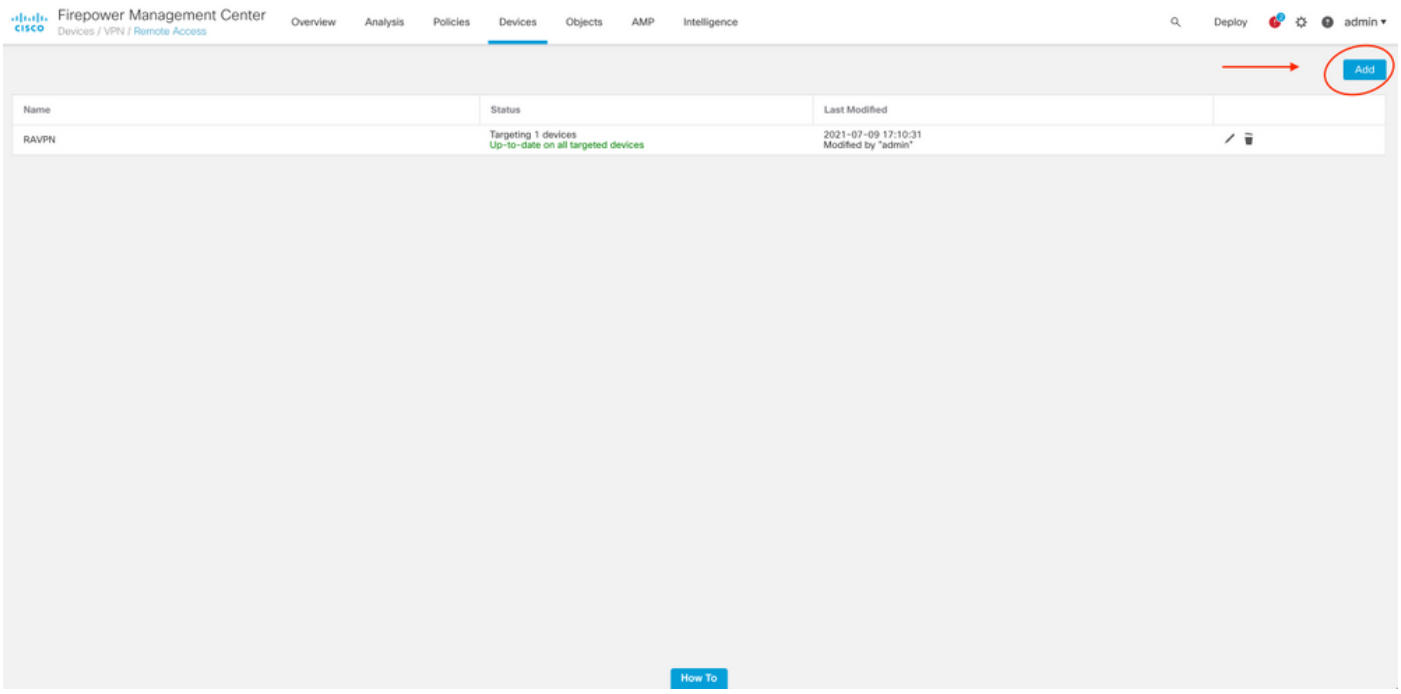
Cisco AnyConnect configureren

Elke verbinding via FMC configureren met de wizard Toegang op afstand.

Procedure: Initiatief

Stap 1. Start de wizard Remote Access VPN om AnyConnect te configureren.

Navigeren in op **Apparaten > Externe Toegang** en kiezen **Toevoegen**.

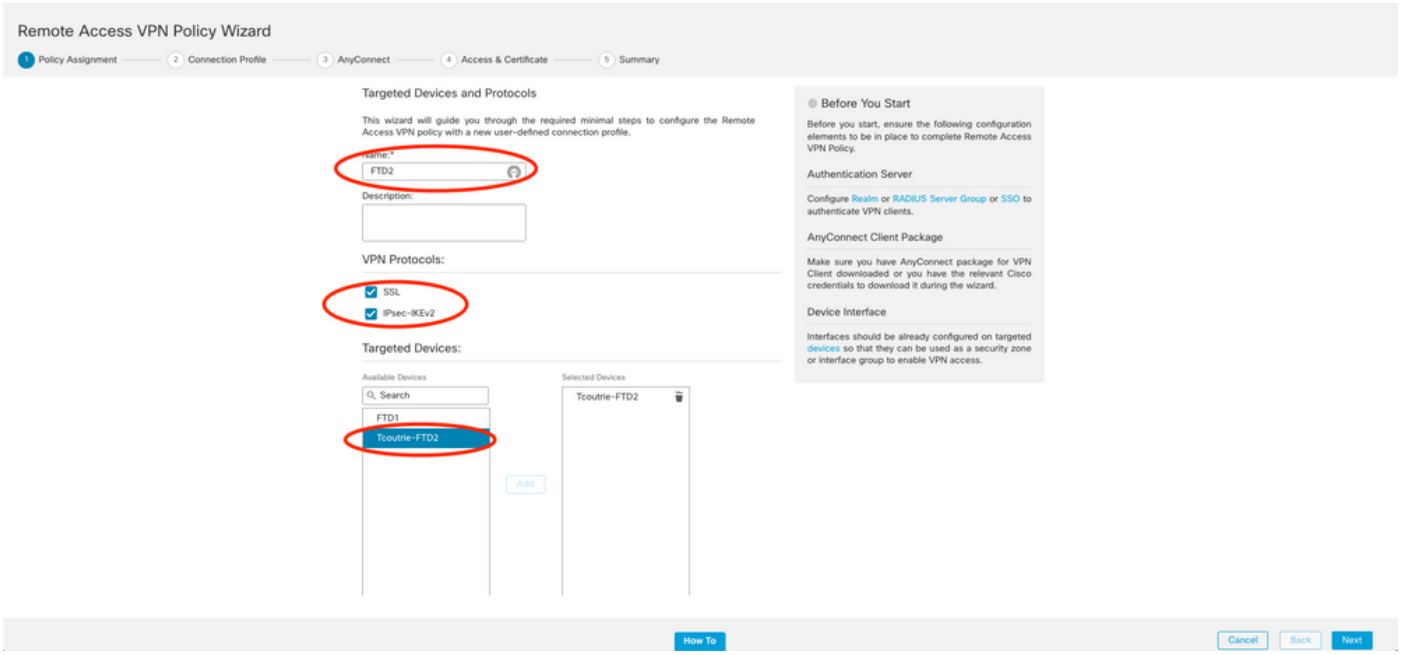


Stap 2. Beleidstoewijzing.

Voltooi de beleidstaak:
a. Geef het beleid een naam

b. Kies de gewenste VPN-protocollen

c. Kies het doelapparaat om de configuratie toe te passen

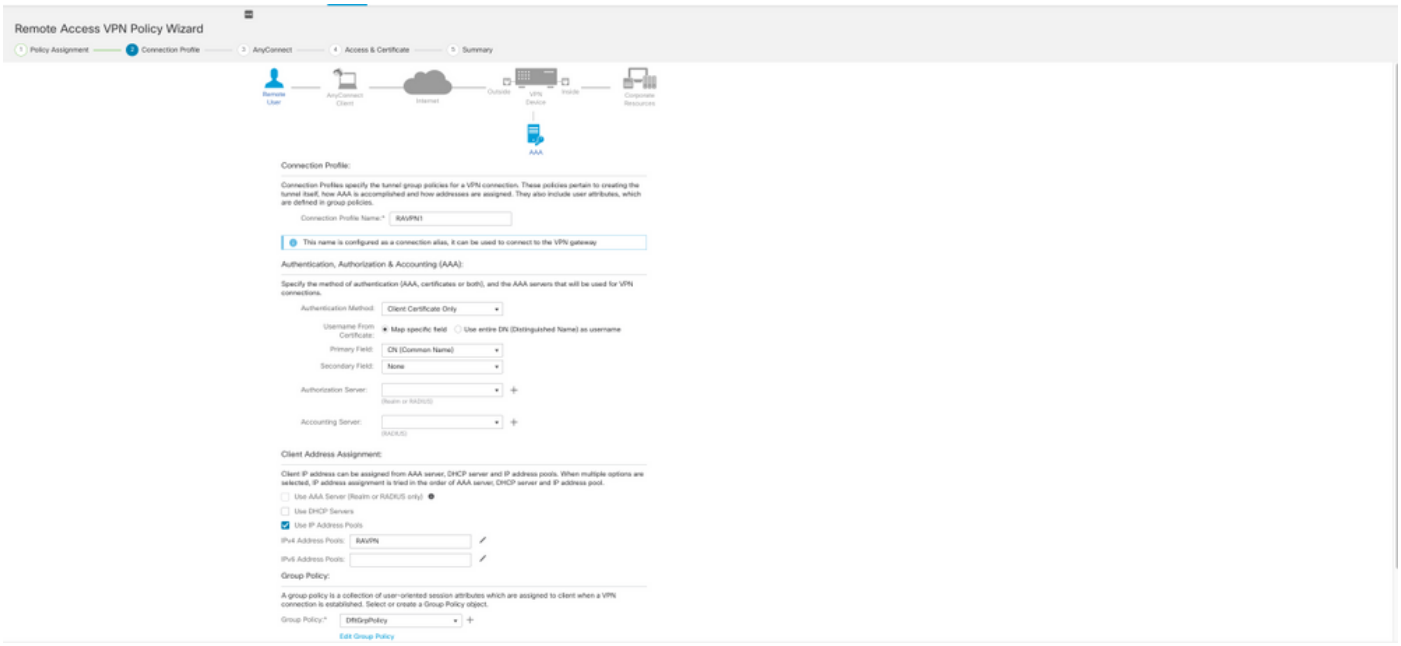


Stap 3. Connection-profiel.

a. Naam van het verbindingsprofiel
b. Stel de verificatiemethode alleen in op clientcertificaat

c. Pas een IP-adrespool aan en indien nodig een nieuw groepsbeleid.

d. Klik op **Volgende**



Opmerking: Kies het Primaire veld dat gebruikt moet worden om de gebruikersnaam voor de verificatiesessie in te voeren. De GN van het certificaat wordt in deze handleiding gebruikt.

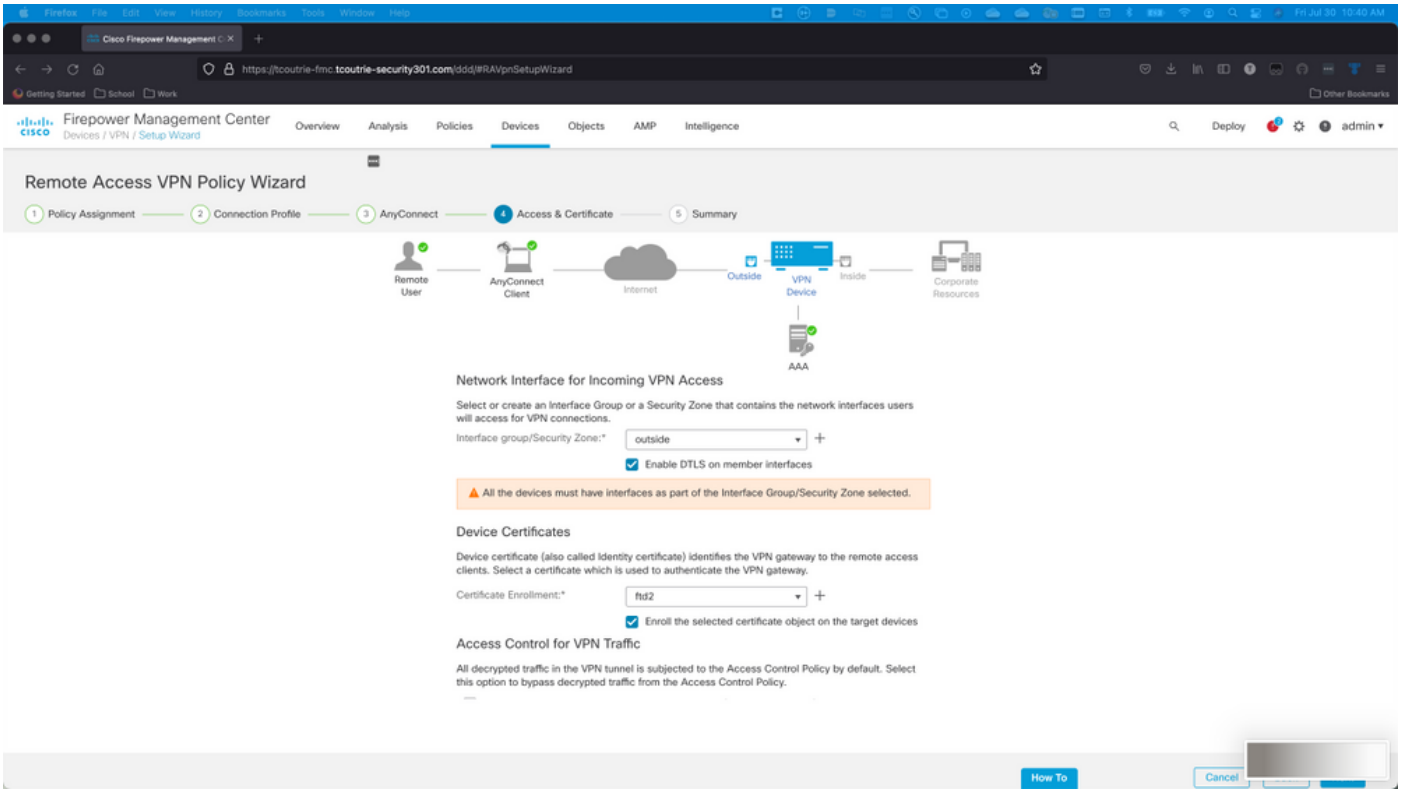
Stap 4. Verbinding.

Voeg een AnyConnect-afbeelding aan het apparaat toe. Upload de gewenste versie van AnyConnect en klik op **Volgende**.

Opmerking: Cisco AnyConnect-pakketten kunnen worden gedownload van **Software.Cisco.com**.

Stap 5. Toegang en certificaat.

Pas het certificaat op een interface toe en schakelt AnyConnect op interfaceniveau in zoals in deze afbeelding, en klik op **Volgende.**



Stap 6. Samenvatting

Bekijk de configuraties. Als alle controles zijn uitgevoerd, klik op **Voltooien** en **stel** dan **in**.

Certificaat voor mobiele gebruikers maken

Maak een certificaat dat wordt toegevoegd aan het mobiele apparaat dat in de verbinding wordt gebruikt.

Stap 1. XCA.

a. Open XCA

b. Een nieuwe database starten

Stap 2. Maak CSR.

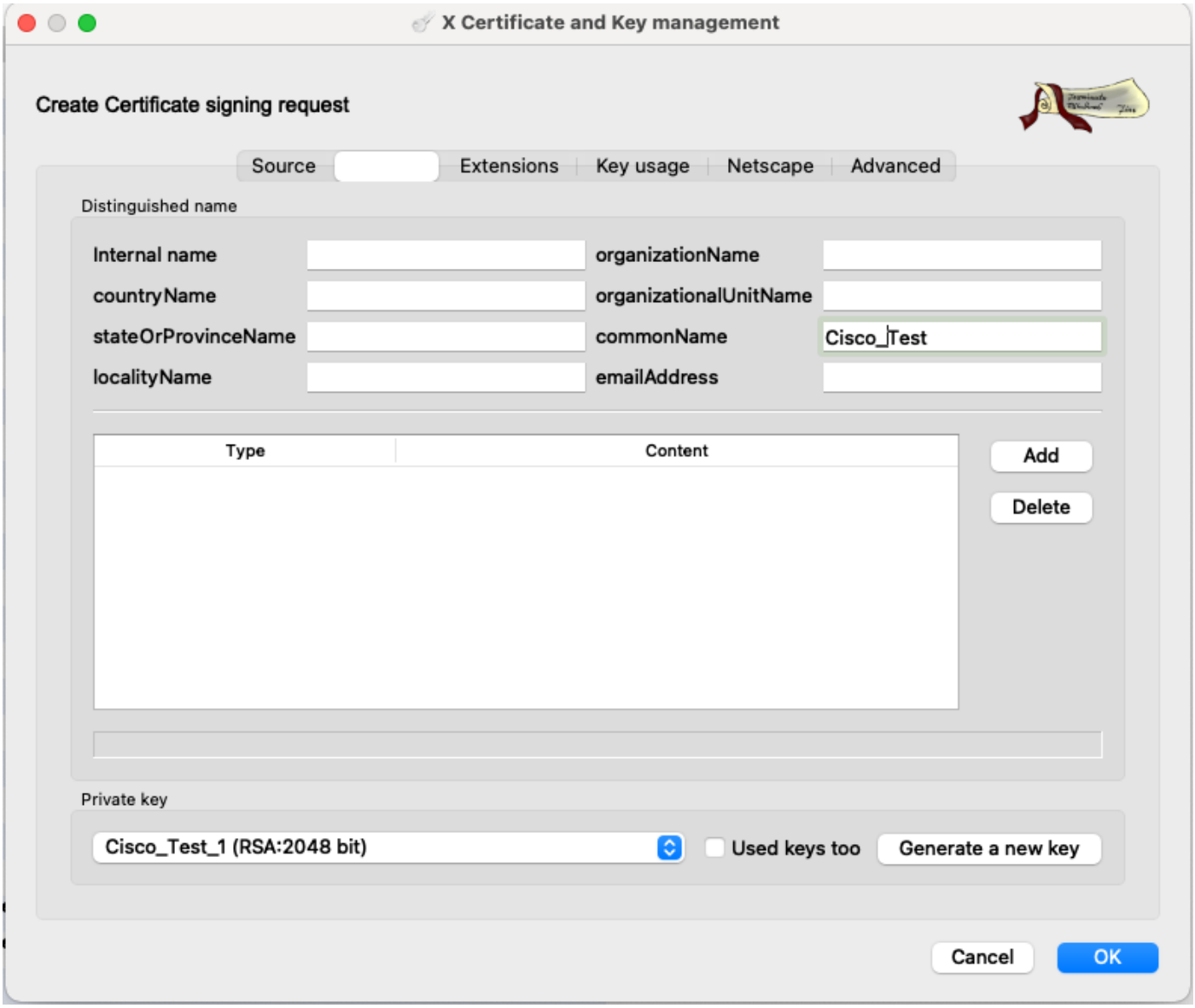
a. Kies **certificaataanvraag** (CSR)

b. Kies **nieuwe aanvraag**

c. Voer de waarde in met alle informatie die voor het certificaat nodig is

d. Een nieuwe sleutel genereren

e. Klik na voltooiing op **OK**

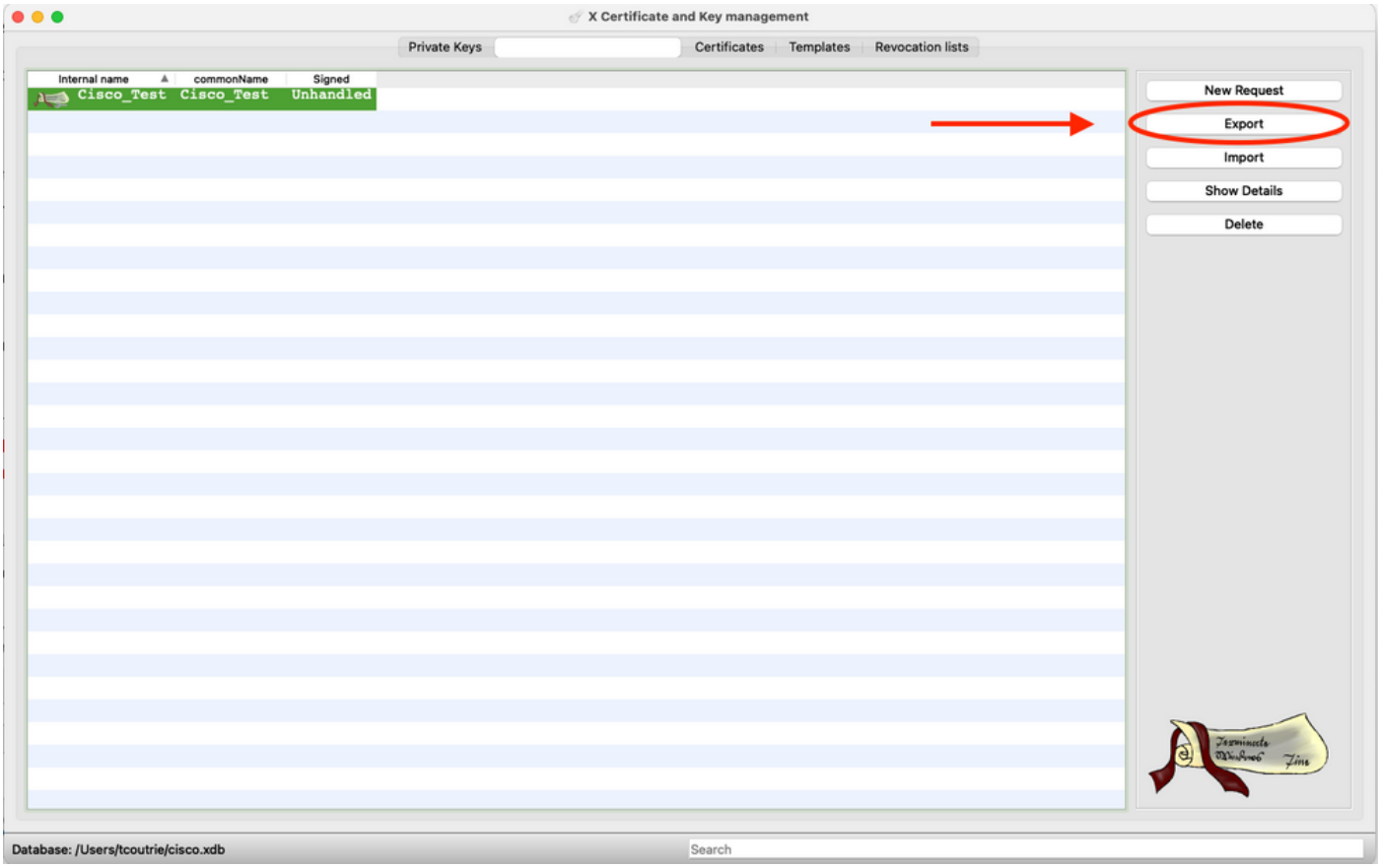


Opmerking: In dit document wordt de GN van het certificaat gebruikt.

Stap 3. Vermeld CSR.

a. CSR exporteren

b. CSR aan CA indienen om een nieuw certificaat te verkrijgen

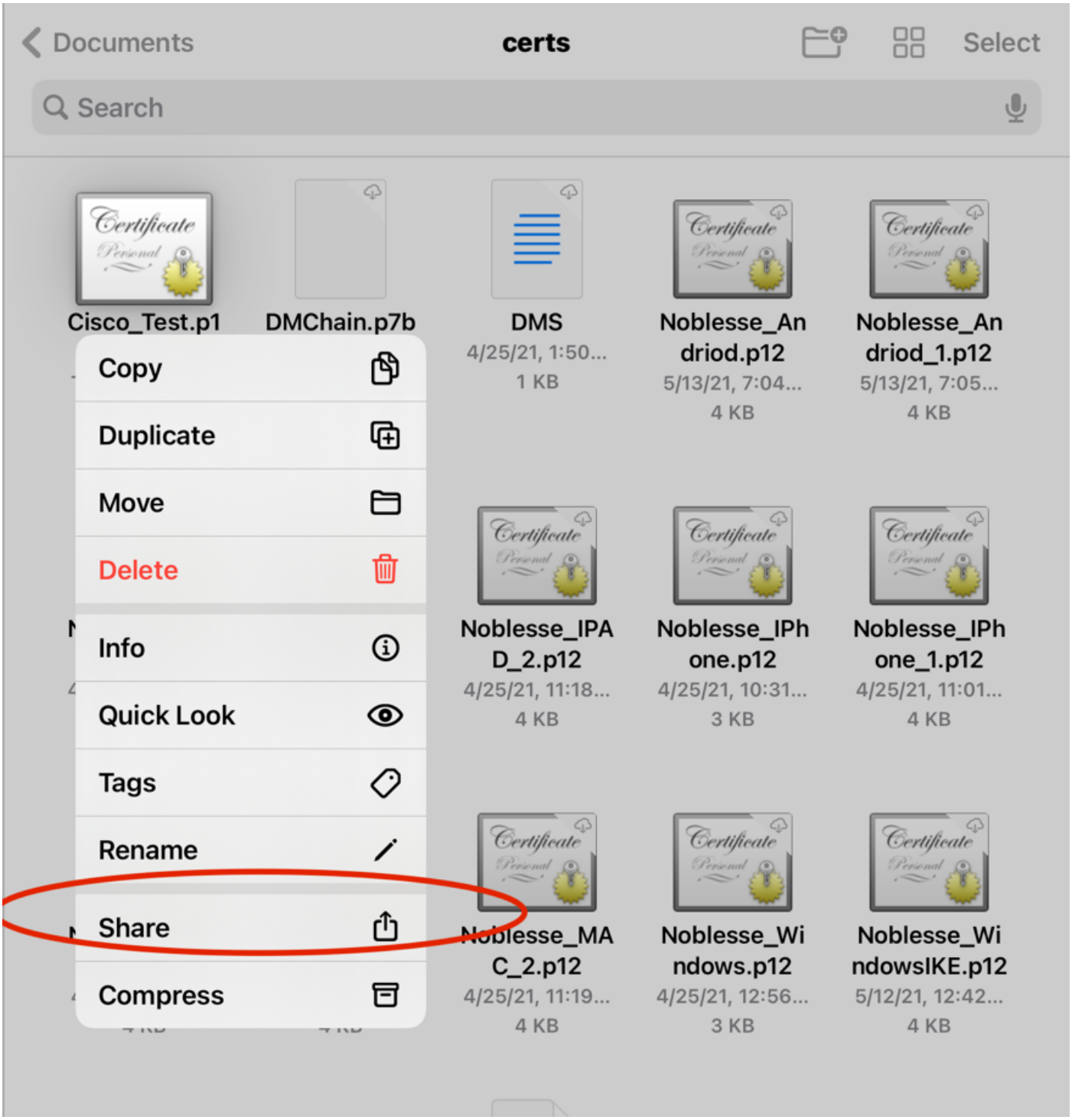


Opmerking: Gebruik het PEM-formaat van de CSR.

Installatie op mobiel apparaat

Stap 1. Voeg het apparaatcertificaat toe aan het mobiele apparaat.
Stap 2. Deel het certificaat met de AnyConnect-toepassing om de nieuwe certificaattoepassing toe te voegen.

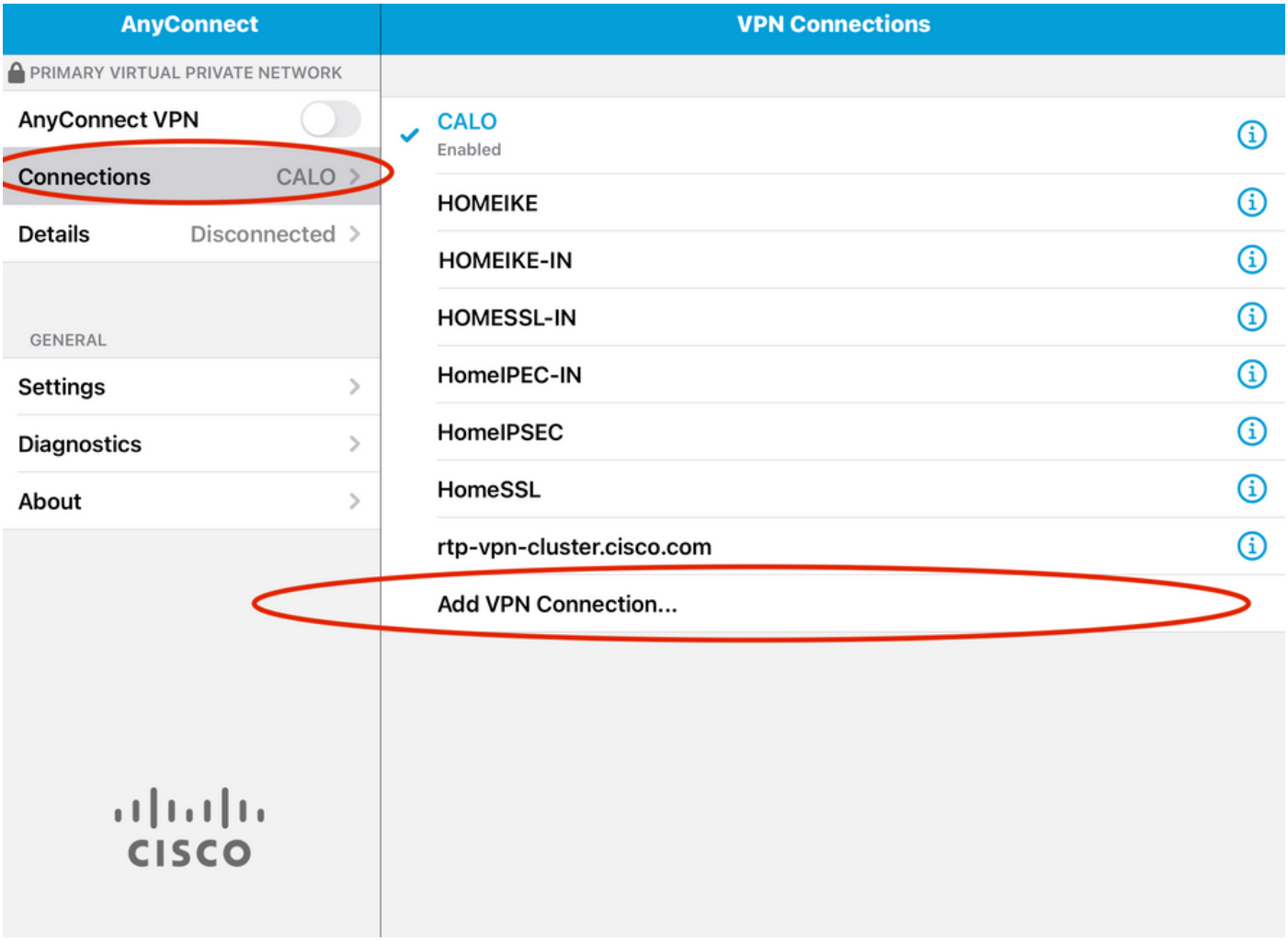
Voorzichtig: De handmatige installatie vereist dat de gebruiker het certificaat met de toepassing deelt. Dit is niet van toepassing op certificaten die via MDM's worden geduwd.



Stap 3. Voer het certificaatwachtwoord in voor **het** bestand **PKCS12**.

Stap 4. Maak een nieuwe verbinding op AnyConnect.

Stap 5. Navigeer naar nieuwe verbindingen; **Aansluitingen > VPN-verbinding toevoegen**.



Stap 6. Voer de informatie in voor de nieuwe verbinding.

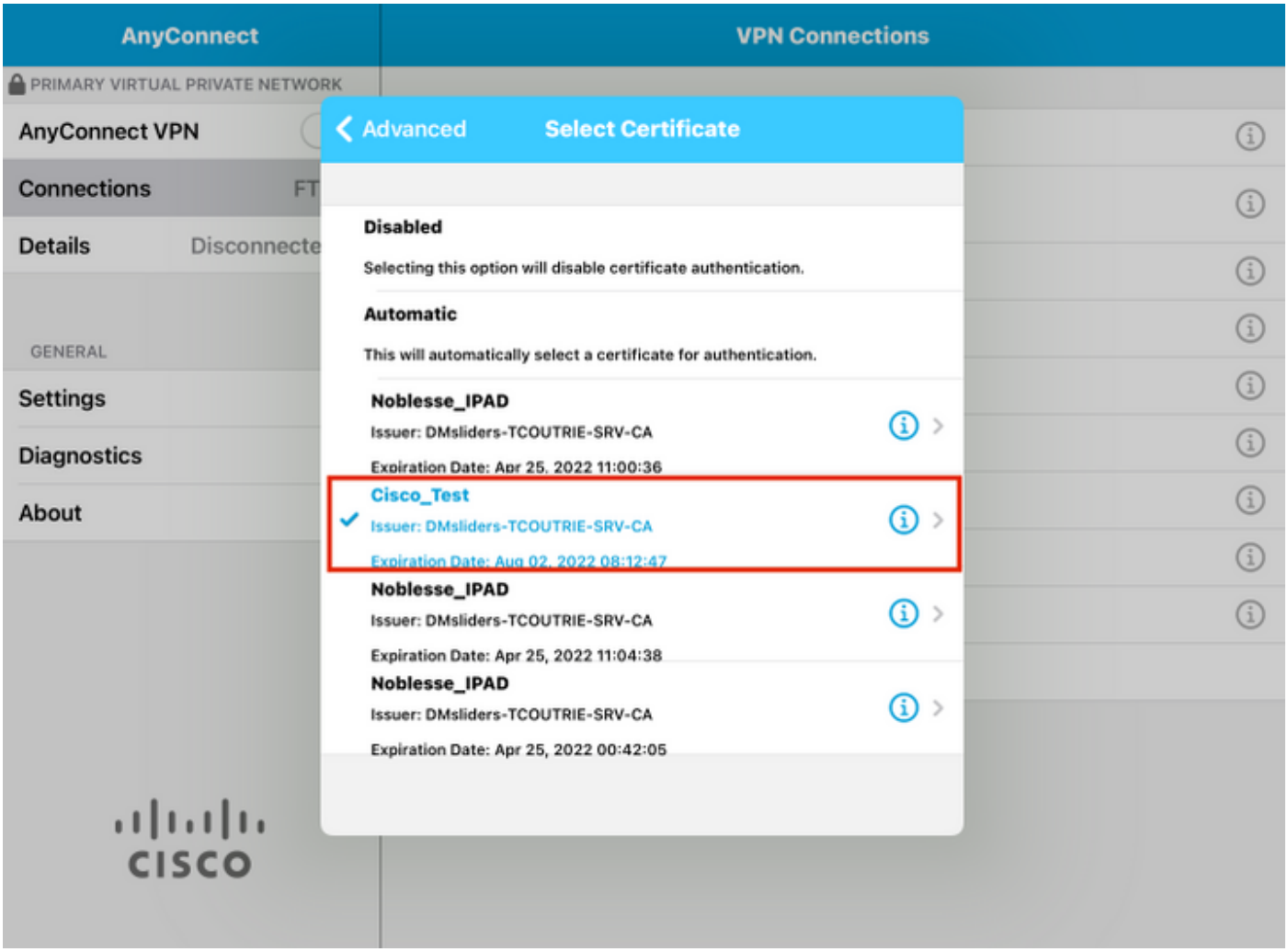
Beschrijving: Geef de connectie een naam

Serveradres: IP-adres voor FQDN-exemplaar van FTD

Geavanceerd: Aanvullende configuraties

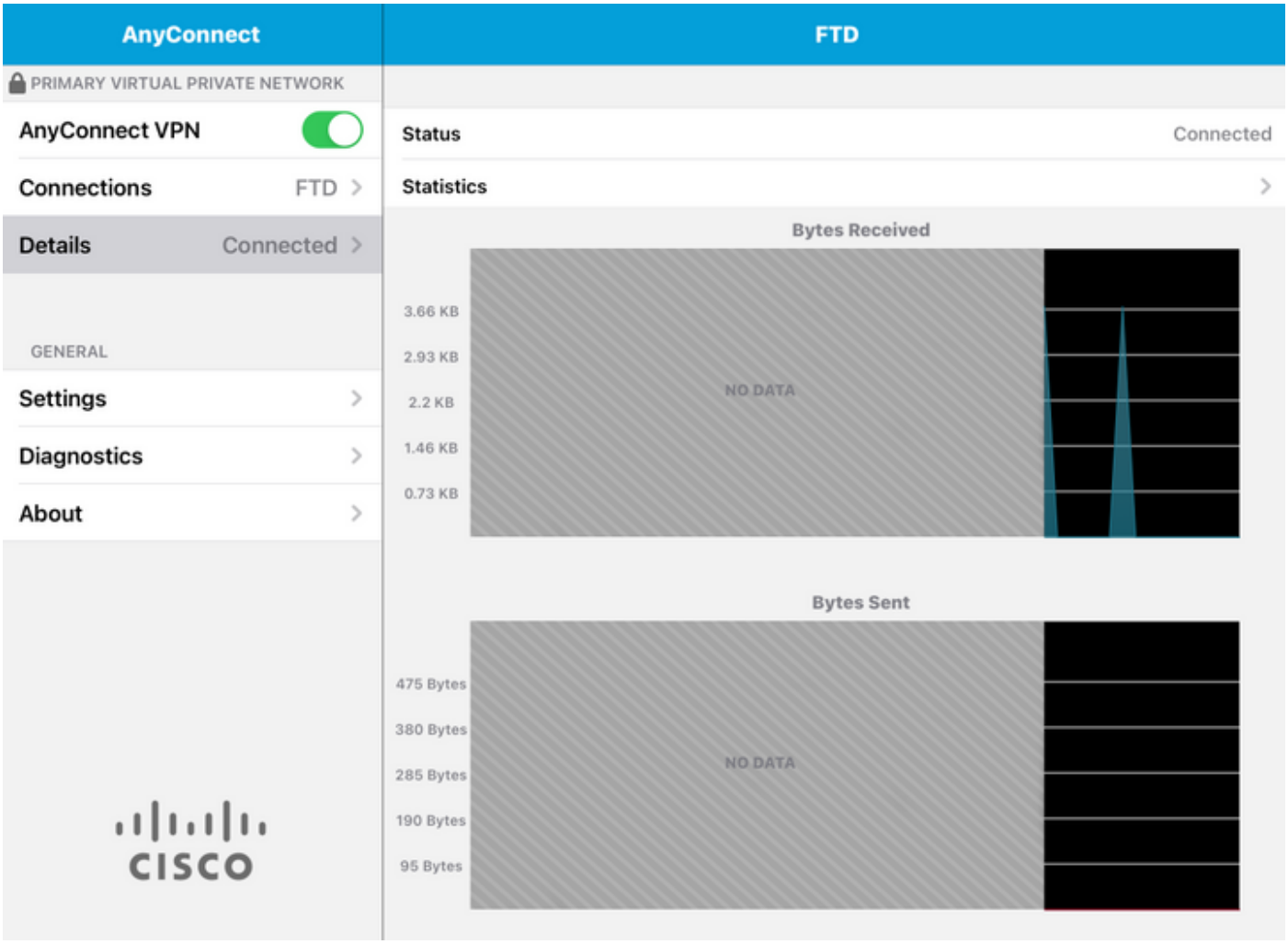
Stap 7. Kies **Geavanceerd**.

Stap 8. Kies **Certificaat** en kies uw nieuwe certificaat.



Stap 9. Navigeer terug naar **verbindingen** en test.

Zodra dit gelukt is, blijft de draaiknop ingeschakeld en tonen de gegevens de verbinding in de status.



Verifiëren

De opdracht **toont vpn-sessionedetails Any** toont alle informatie over de aangesloten host.

> **Tip**: De optie om deze opdracht verder te filteren is de 'filter' of 'type'-sleutelwoorden die aan de opdracht worden toegevoegd.

Voorbeeld:

```
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
```

Problemen oplossen

Debugs

Debugs die nodig zijn om een oplossing voor dit probleem te vinden, zijn:

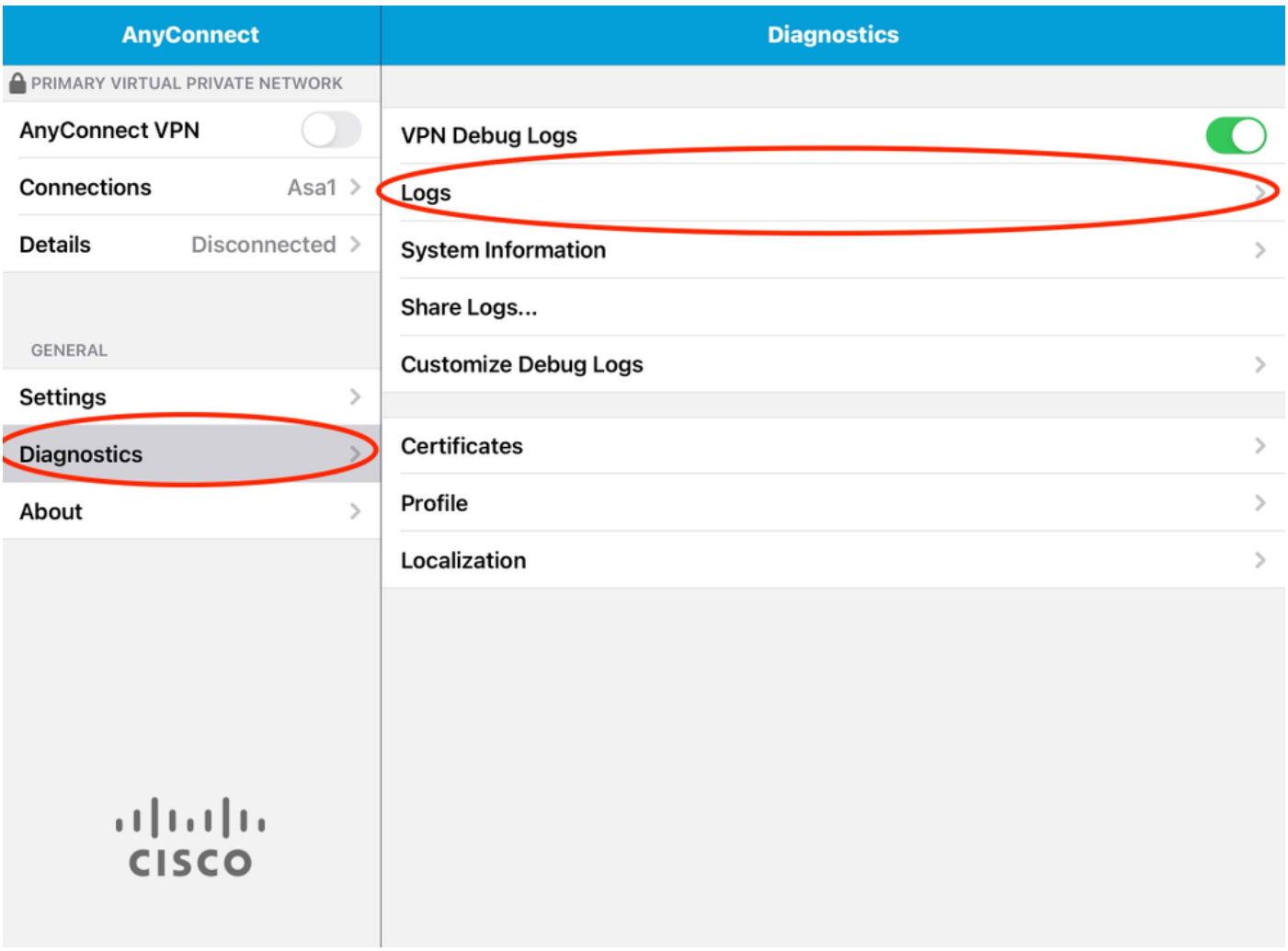
```
Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255
```

Als de verbinding IPSEC en niet SSL is:

```
Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14
```

Logs van de mobiele applicatie AnyConnect:

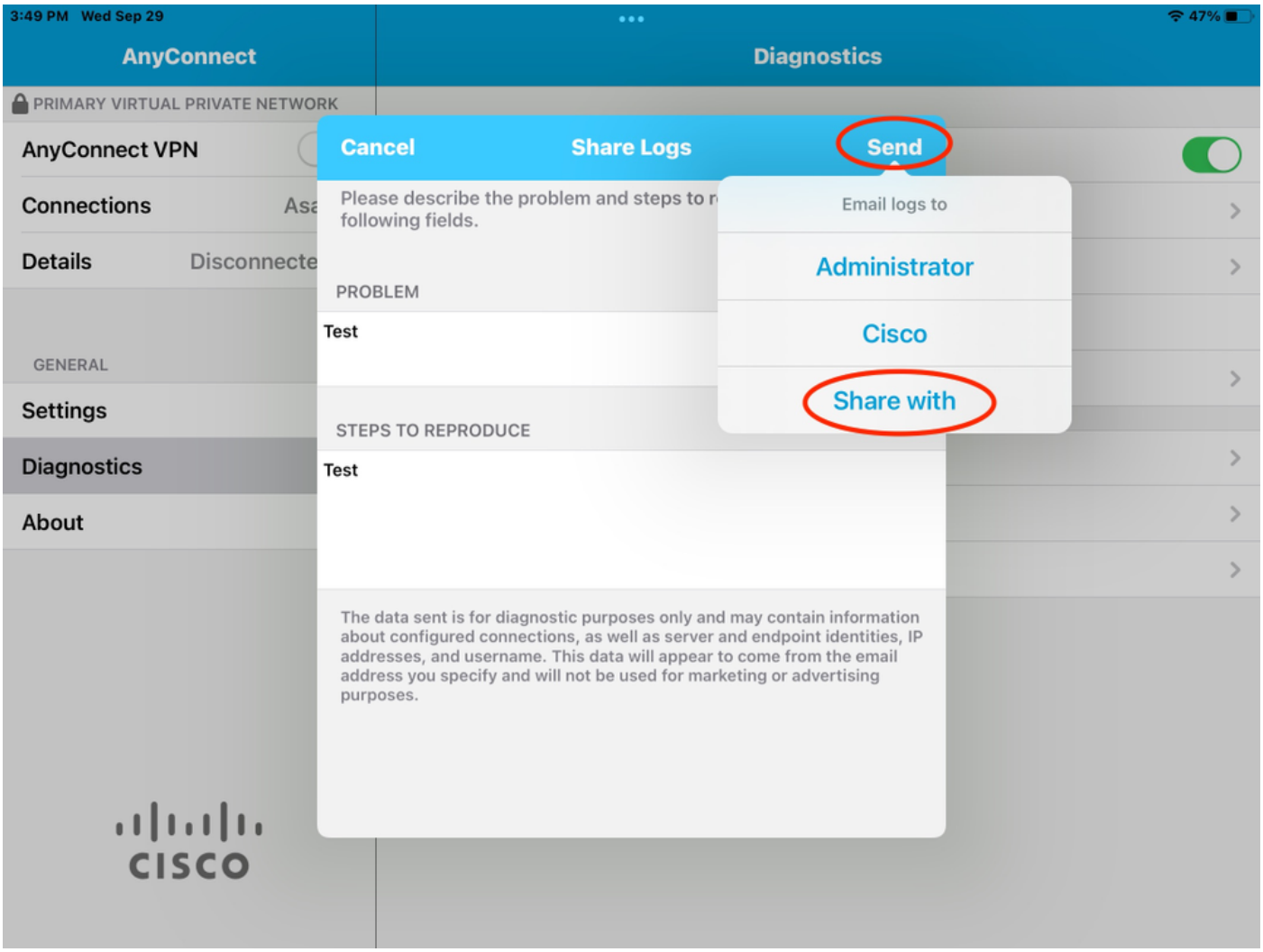
Navigeren in naar **diagnostiek > VPN Debug Logs > Share logs**.



Voer de informatie in:

- Probleem
- Stappen om te reproduceren

Navigeer dan om **te verzenden > Delen met**.



Dit biedt de optie om een e-mailclient te gebruiken om de logbestanden te verzenden.