# Konfigurieren der auf AnyConnect-Zertifikaten basierenden Authentifizierung für den mobilen Zugriff

## Inhalt



## Einleitung

Dieses Dokument beschreibt ein Beispiel für die Implementierung einer zertifikatsbasierten Authentifizierung auf Mobilgeräten.

## Voraussetzungen

Die im Leitfaden verwendeten Tools und Geräte sind:

- Cisco FirePOWER Threat Defense (FTD)
- Firepower Management Center (FMC)
- Apple iOS-Gerät (iPhone, iPad)
- Zertifizierungsstelle (Certificate Authority, CA)
- Cisco AnyConnect Client-Software

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Basis-VPN
- SSL/TLS
- Public Key-Infrastruktur
- Erfahrung mit FMC

- OpenSSL
- Cisco AnyConnect

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

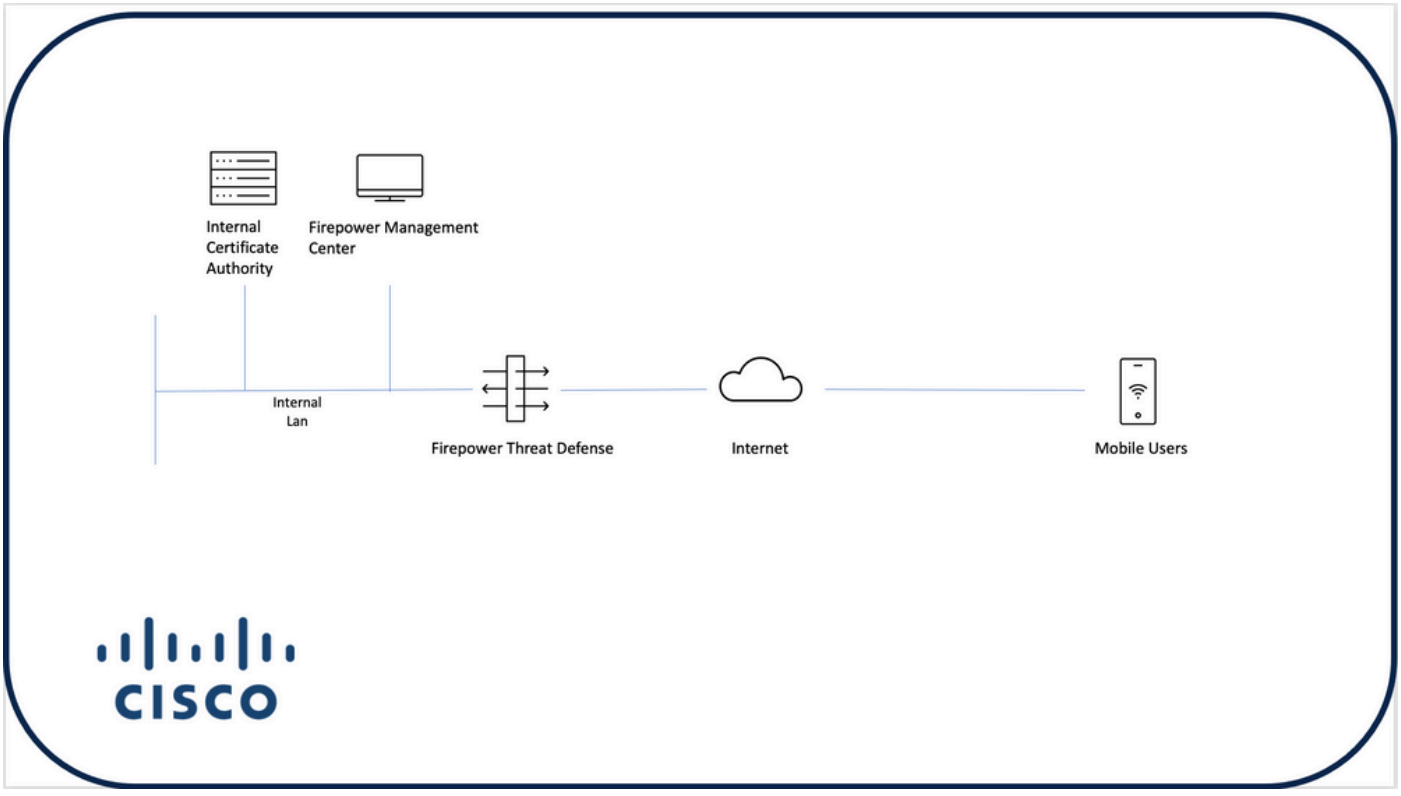
- FTD von Cisco
- Cisco FMC
- Microsoft CA-Server
- XCA
- Cisco AnyConnect
- Apple-iPad

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Konfigurieren von Cisco AnyConnect auf FTD

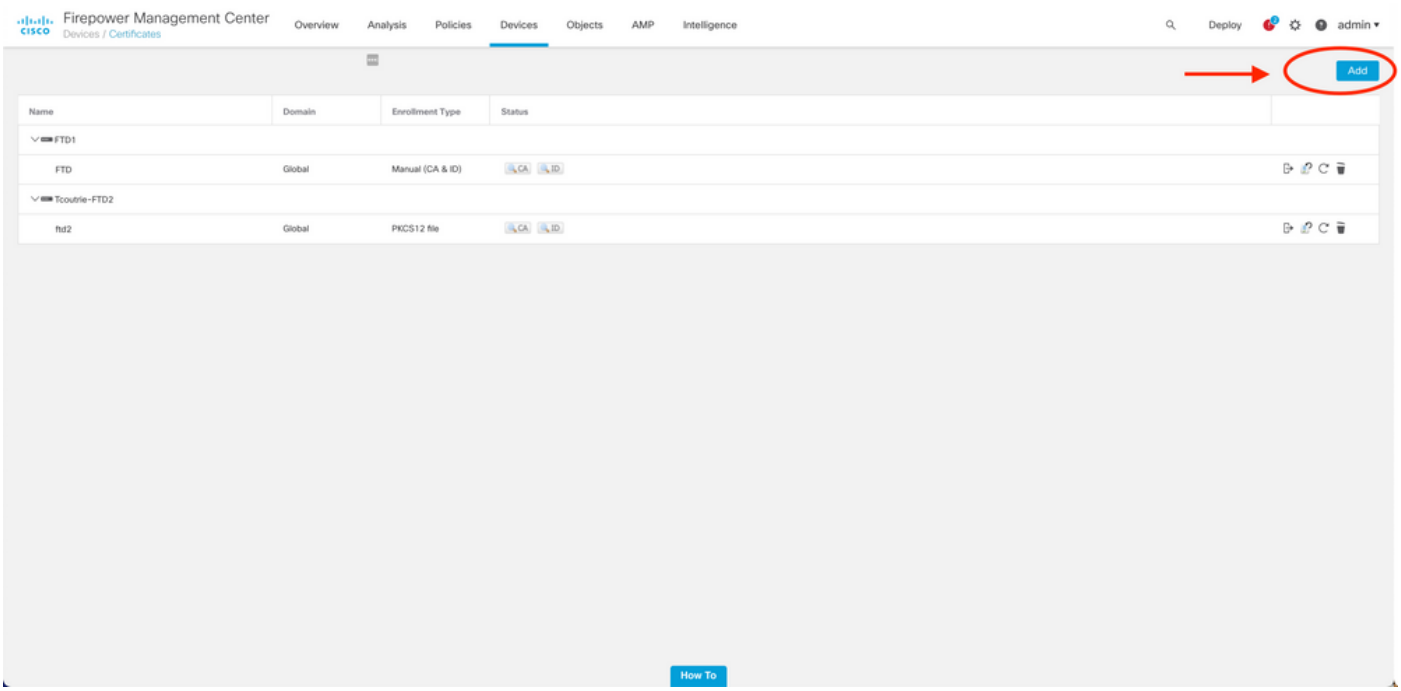
In diesem Abschnitt werden die Schritte zur Konfiguration von AnyConnect über FMC beschrieben. Bevor Sie beginnen, stellen Sie sicher, dass Sie alle Konfigurationen bereitstellen.

### Netzwerkdiagramm

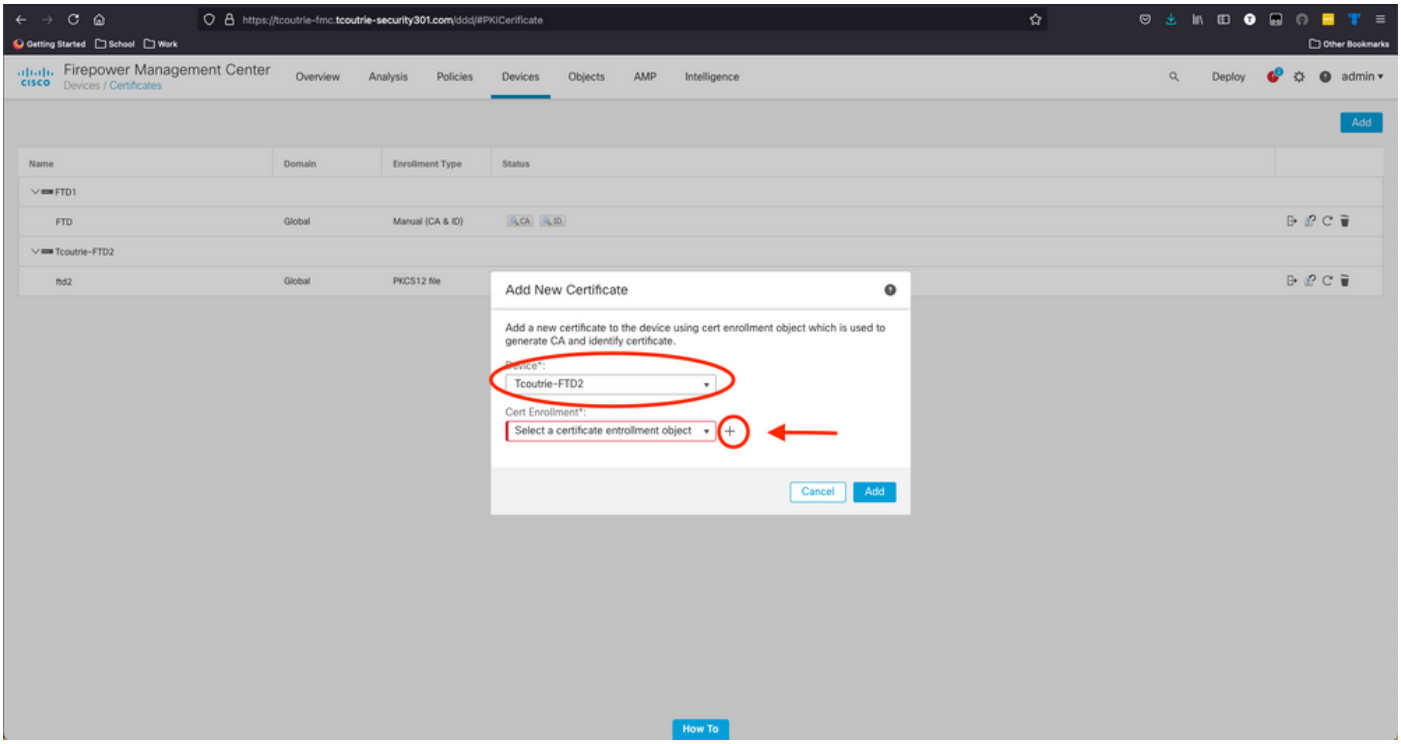



### Zertifikat zu FTD hinzufügen

Schritt 1: Erstellen Sie ein Zertifikat für die FTD auf der FMC-Appliance. Navigieren Sie zu **Devices > Certificate**, und wählen Sie **Add (Hinzufügen)** aus, wie in diesem Bild gezeigt:




Schritt 2: Wählen Sie die für die VPN-Verbindung gewünschte FTD aus. Wählen Sie die **FTD-Appliance** aus der Dropdown-Liste aus. Klicken Sie auf das **+** Symbol, um eine neue Methode zur Zertifikatsregistrierung hinzuzufügen, wie in diesem Bild gezeigt:

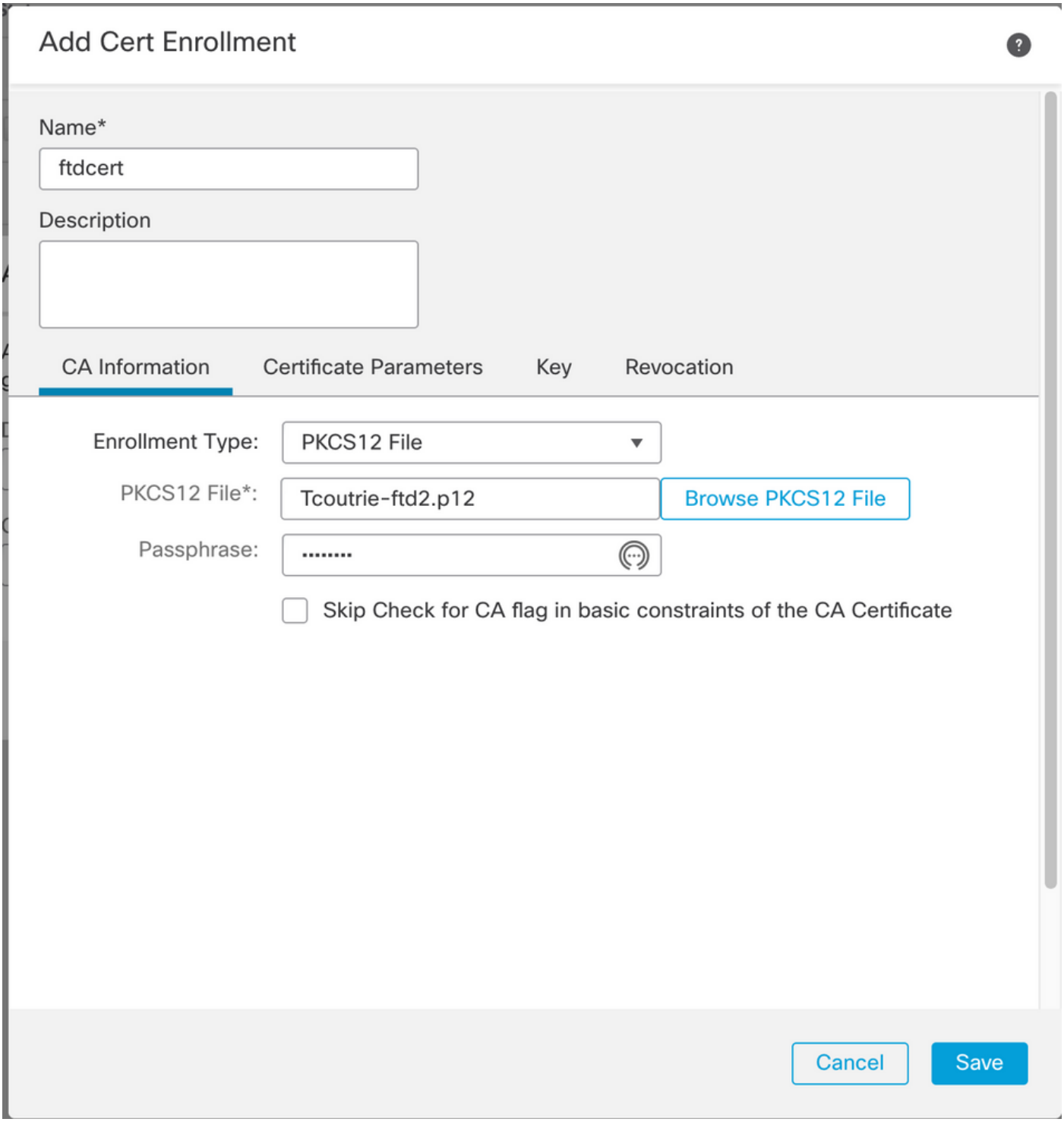



Schritt 3: Fügen Sie dem Gerät die Zertifikate hinzu. Wählen Sie die Option aus, die die bevorzugte Methode zum Abrufen von Zertifikaten in der Umgebung ist.

> **Tipp:** Folgende Optionen stehen zur Verfügung: **Selbstsigniertes Zertifikat** - Erstellen Sie lokal ein neues Zertifikat, **SCEP** - Verwenden Sie das Simple Certificate Enrollment Protocol, um ein Zertifikat von einer Zertifizierungsstelle zu erhalten. **Manuell**- Installieren Sie das

Root- und Identitätszertifikat manuell, **PKCS12** - Hochladen eines verschlüsselten Zertifikatspakets mit Stamm, Identität und privatem Schlüssel.

Schritt 4: Laden Sie das Zertifikat auf das FTD-Gerät hoch. Geben Sie den Passcode ein (nur PKCS12), und klicken Sie auf **Speichern**, wie in diesem Bild gezeigt:




**Anmerkung:** Nachdem Sie die Datei gespeichert haben, erfolgt die Bereitstellung der Zertifikate sofort. Wählen Sie die ID aus, um die Zertifikatdetails anzuzeigen.

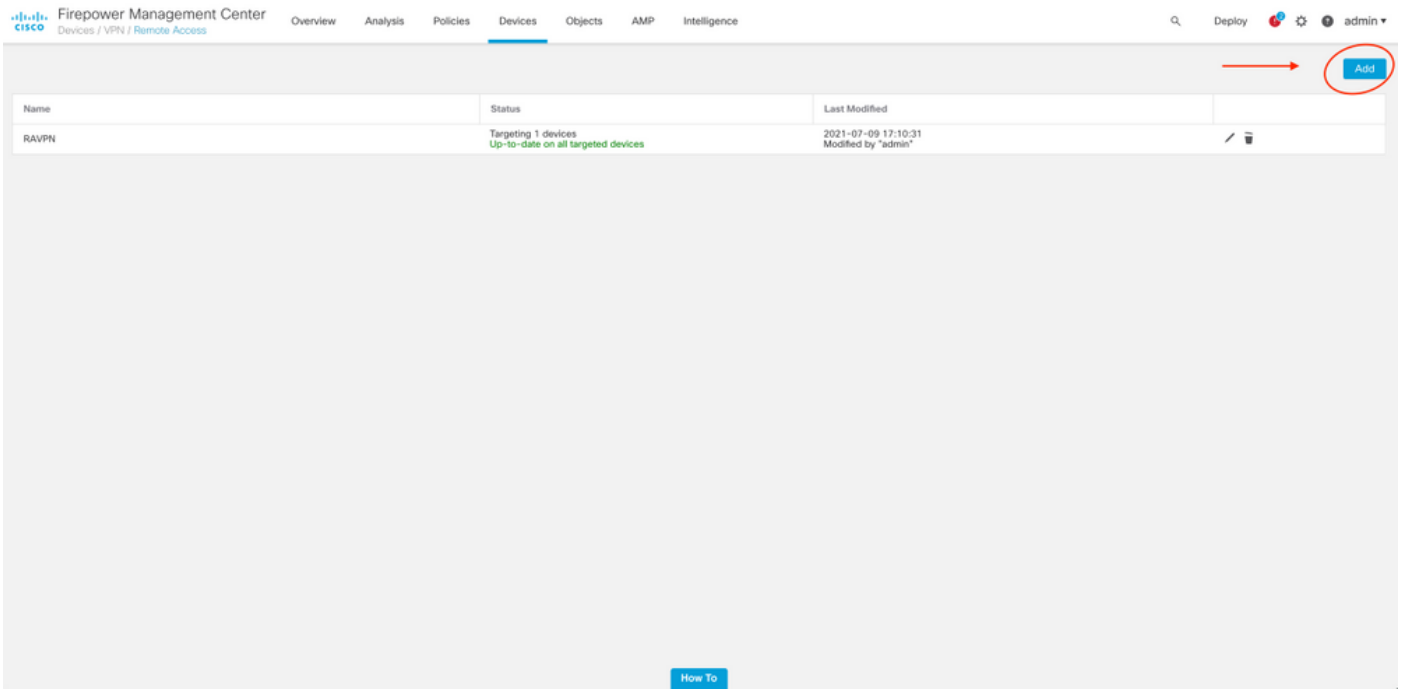
## Konfigurieren von Cisco AnyConnect

Konfigurieren Sie AnyConnect über FMC mit dem Remote-Zugriffs-Assistenten.

Verfahren:

Schritt 1: Starten Sie den Remote Access VPN Policy Wizard, um AnyConnect zu konfigurieren.

Navigieren Sie zu **Geräte > Remotezugriff,** und wählen Sie **Hinzufügen aus**.

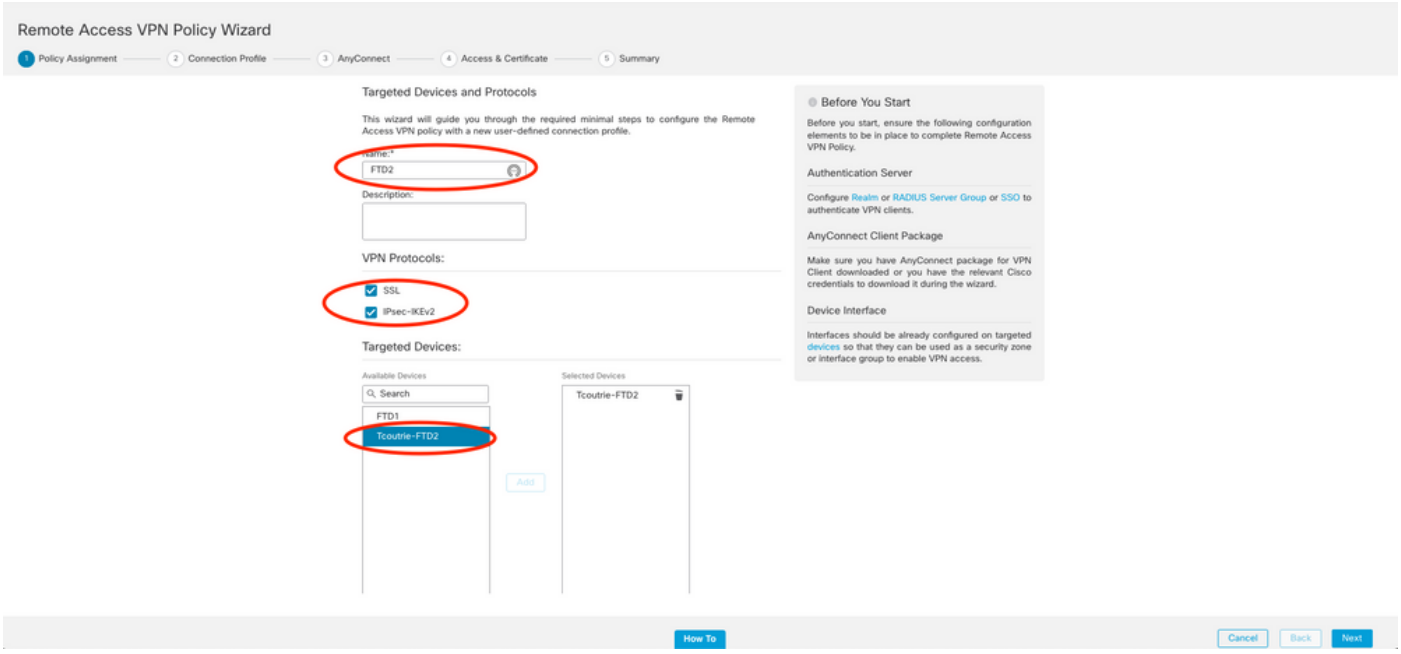



Schritt 2: Richtlinienzuweisung.

Führen Sie die Richtlinienzuweisung aus:
antwort: Policy benennen

b. Wählen Sie die gewünschten VPN-Protokolle

c. Wählen Sie das Zielgerät aus, um die Konfiguration anzuwenden.

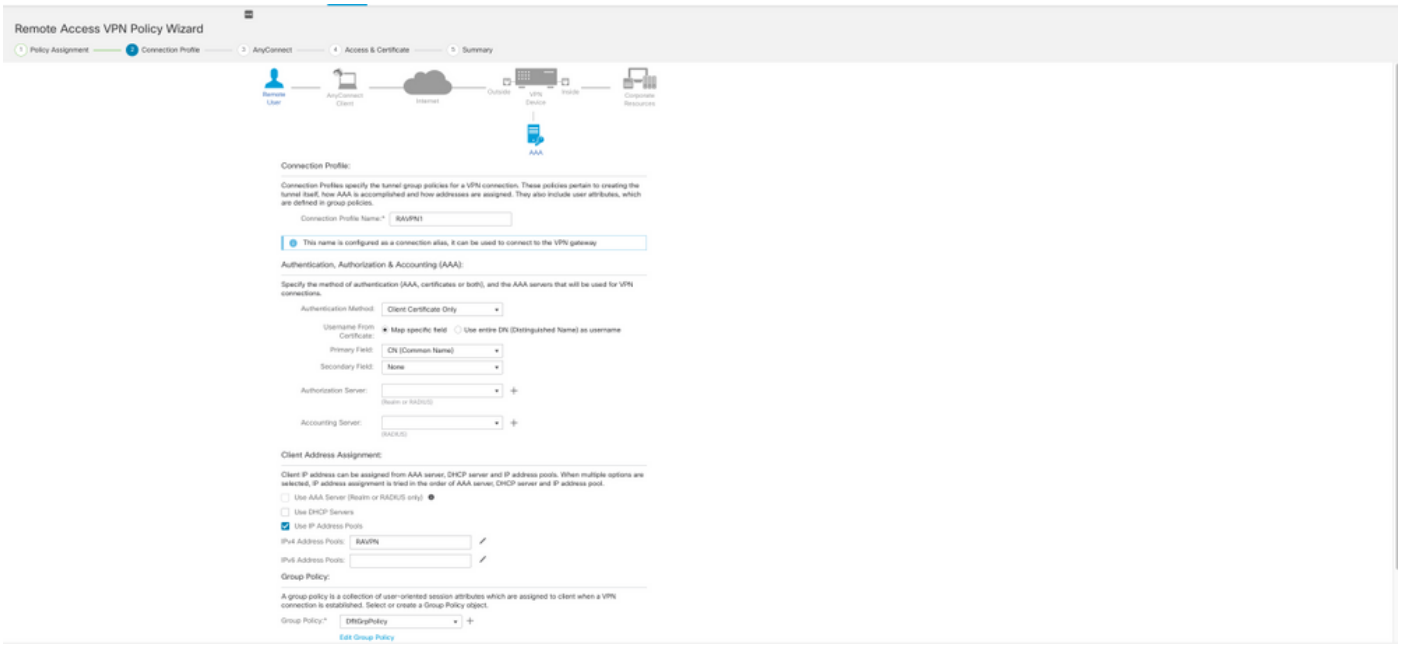



Schritt 3: Verbindungsprofil.

antwort: Benennen Sie das Verbindungsprofil.
b. Legen Sie die Authentifizierungsmethode auf Nur Clientzertifikat fest.

c. Zuweisen eines IP-Adresspools und ggf. Erstellen einer neuen Gruppenrichtlinie

d. Klicken Sie auf **Weiter**




> **Anmerkung:** Wählen Sie das primäre Feld aus, um den Benutzernamen für Authentifizierungssitzungen einzugeben. In diesem Leitfaden wird der CN des Zertifikats verwendet.

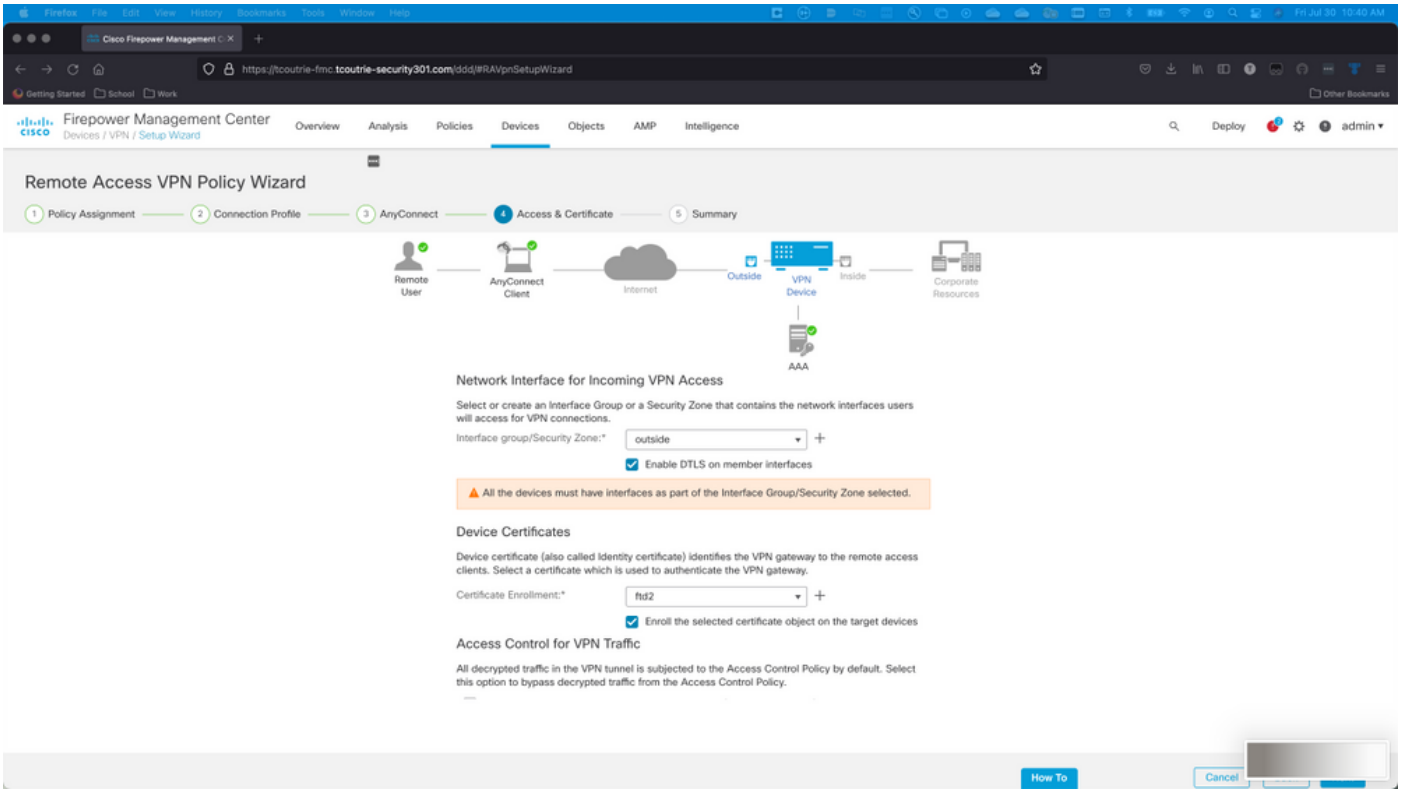
Schritt 4: AnyConnect.

Fügen Sie der Appliance ein AnyConnect-Image hinzu. Laden Sie die bevorzugte Version von AnyConnect hoch, und klicken Sie auf **Weiter**.

> **Anmerkung:** Cisco AnyConnect-Pakete können unter **Software.Cisco.com** heruntergeladen werden.

Schritt 5: Zugriff und Zertifikat.

Wenden Sie das Zertifikat auf eine Schnittstelle an, und aktivieren Sie Anyconnect auf Schnittstellenebene, wie in diesem Bild gezeigt, und klicken Sie auf **Weiter.**




Schritt 6: Zusammenfassung.

Überprüfen Sie die Konfigurationen. Wenn alle Auscheckvorgänge ausgeführt werden, klicken Sie auf **Fertig stellen** und dann **bereitstellen**.

# Zertifikat für mobile Benutzer erstellen

Erstellen Sie ein Zertifikat, das dem Mobilgerät hinzugefügt werden soll, das in der Verbindung verwendet wird.

Schritt 1: XCA

antwort: Öffnen von XCA

b. Neue Datenbank starten

Schritt 2: CSR erstellen

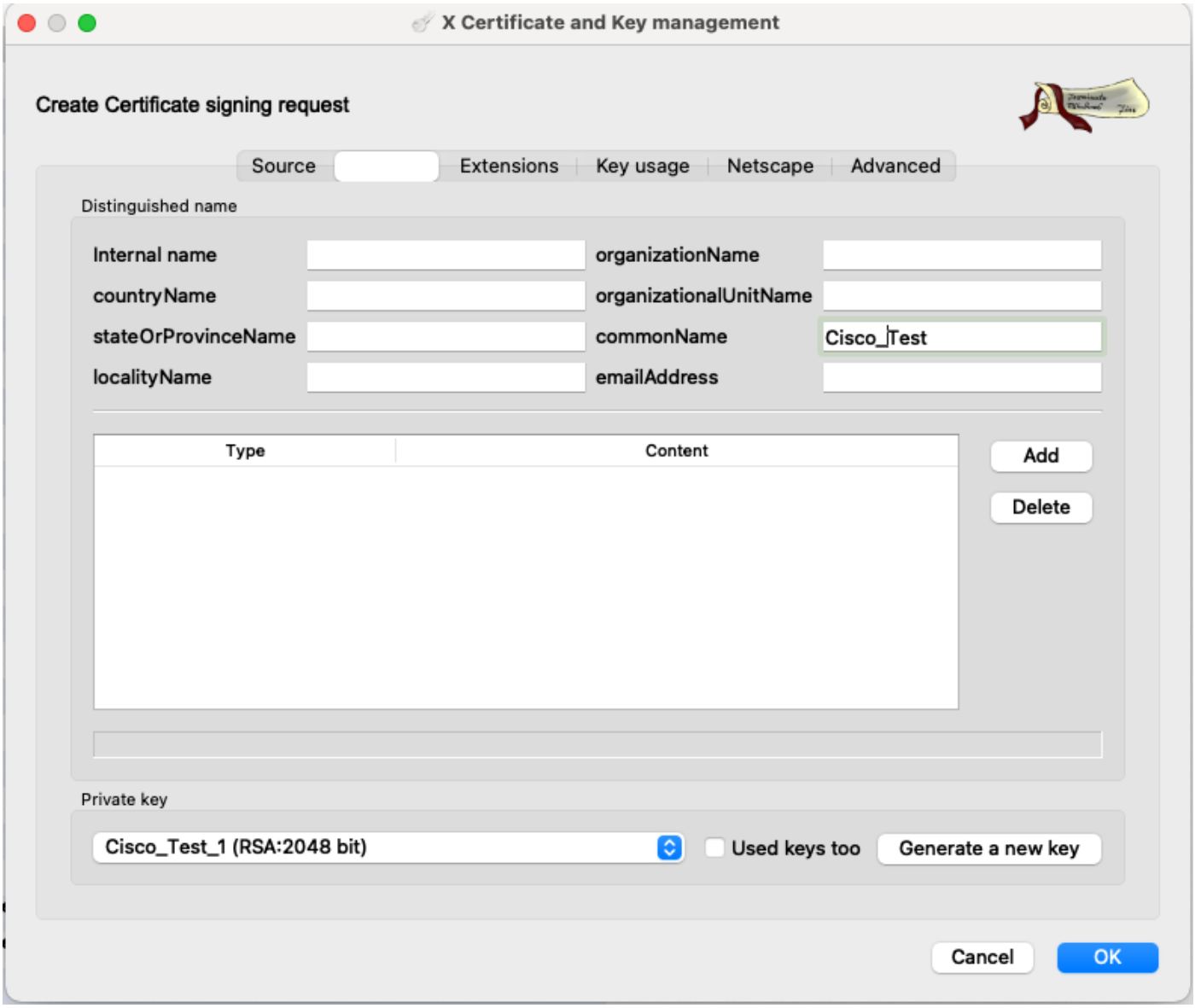
antwort: Wählen Sie **Certificate Signing Request** (CSR) aus.

b. **Neue Anforderung** auswählen

c. Geben Sie den Wert zusammen mit allen für das Zertifikat erforderlichen Informationen ein.

d. Erstellen eines neuen Schlüssels

e. Klicken Sie abschließend auf **OK**

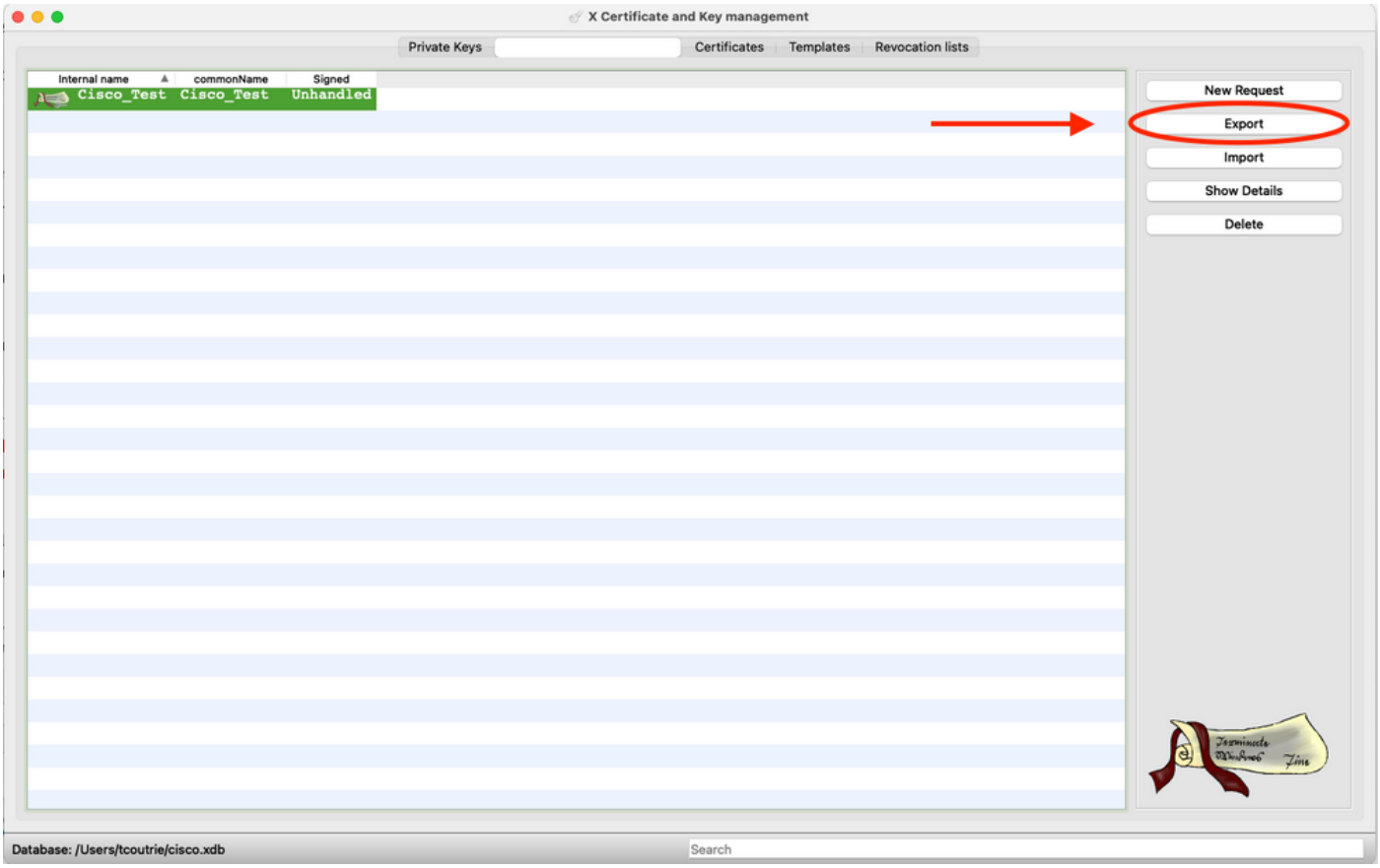



**Anmerkung:** In diesem Dokument wird der CN des Zertifikats verwendet.

Schritt 3: CSR senden

antwort: CSR exportieren

b. CSR an CA senden, um ein neues Zertifikat zu erhalten

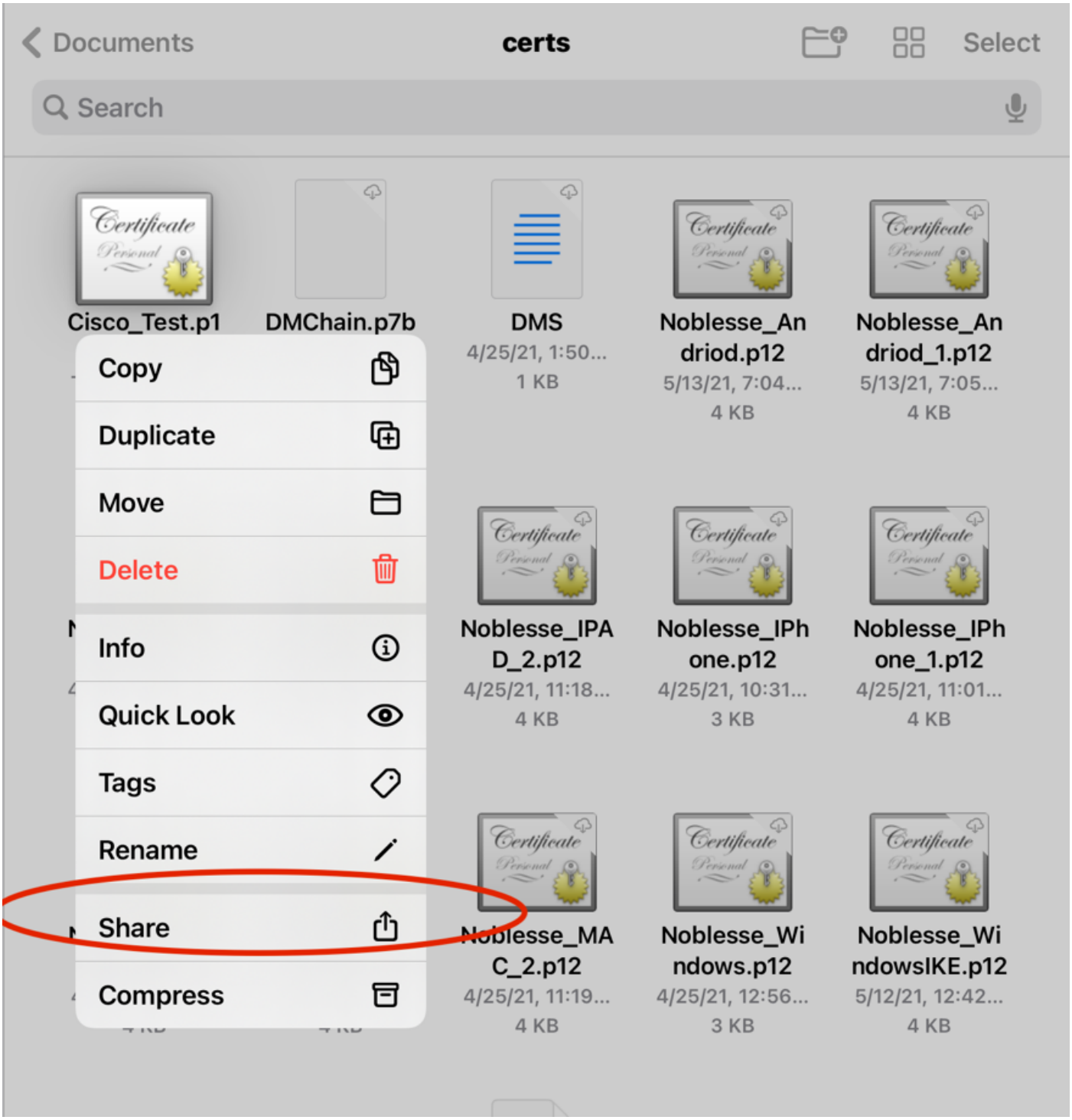



**Anmerkung:** Verwenden Sie das PEM-Format der CSR.

## Installation auf Mobilgeräten

Schritt 1: Fügen Sie das Gerätezertifikat dem Mobilgerät hinzu.
Schritt 2: Freigeben des Zertifikats an die AnyConnect-Anwendung, um die neue Zertifikatsanwendung hinzuzufügen

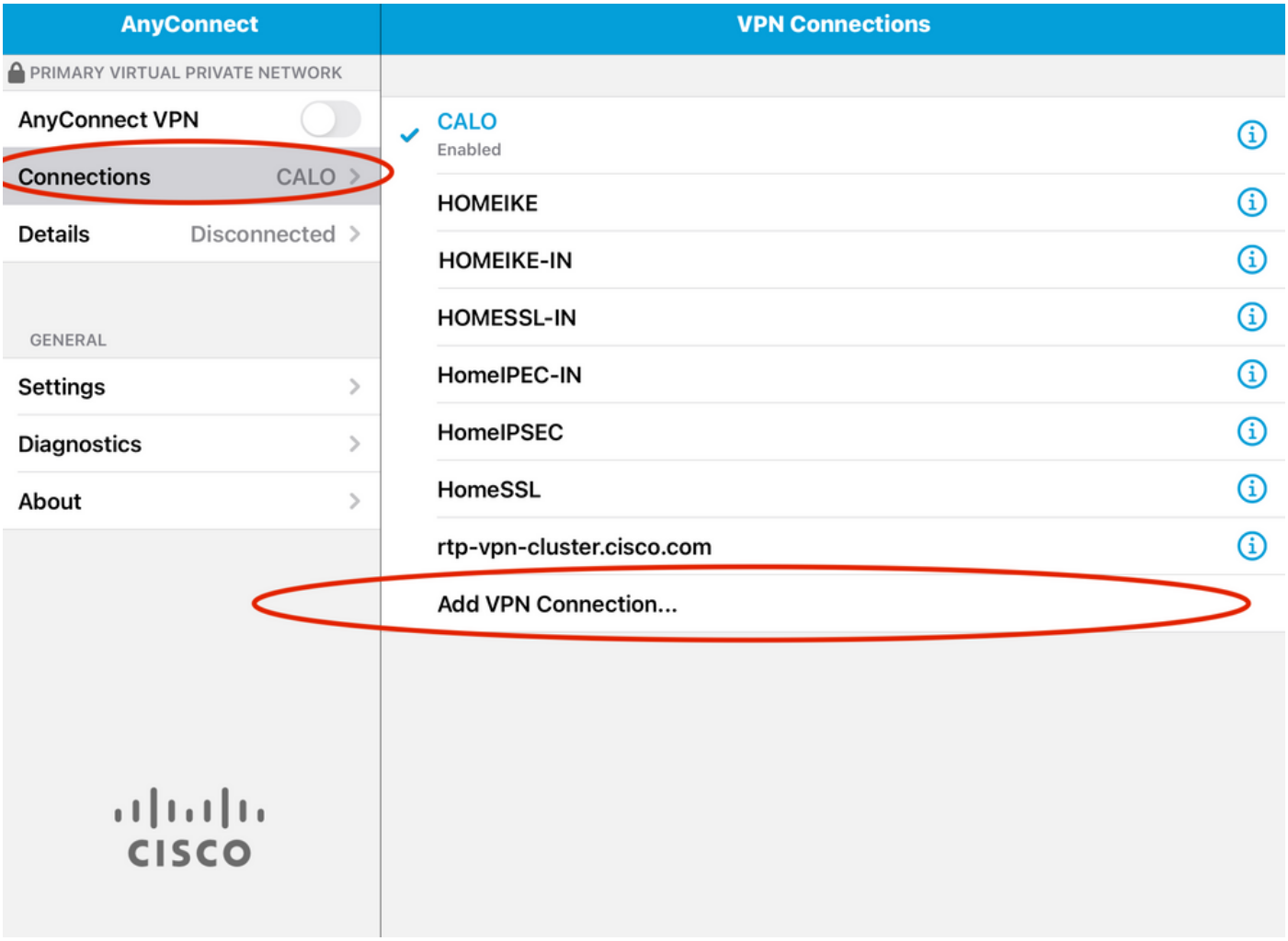
**Vorsicht:** Bei der manuellen Installation muss der Benutzer das Zertifikat für die Anwendung freigeben. Dies gilt nicht für Zertifikate, die über MDMs gesendet werden.




Schritt 3: Geben Sie das Zertifikatskennwort für die **PKCS12-**Datei ein.

Schritt 4: Erstellen Sie eine neue Verbindung auf AnyConnect.

Schritt 5: Navigieren zu neuen Verbindungen **Verbindungen > VPN-Verbindung hinzufügen**.




Schritt 6: Geben Sie die Informationen für die neue Verbindung ein.

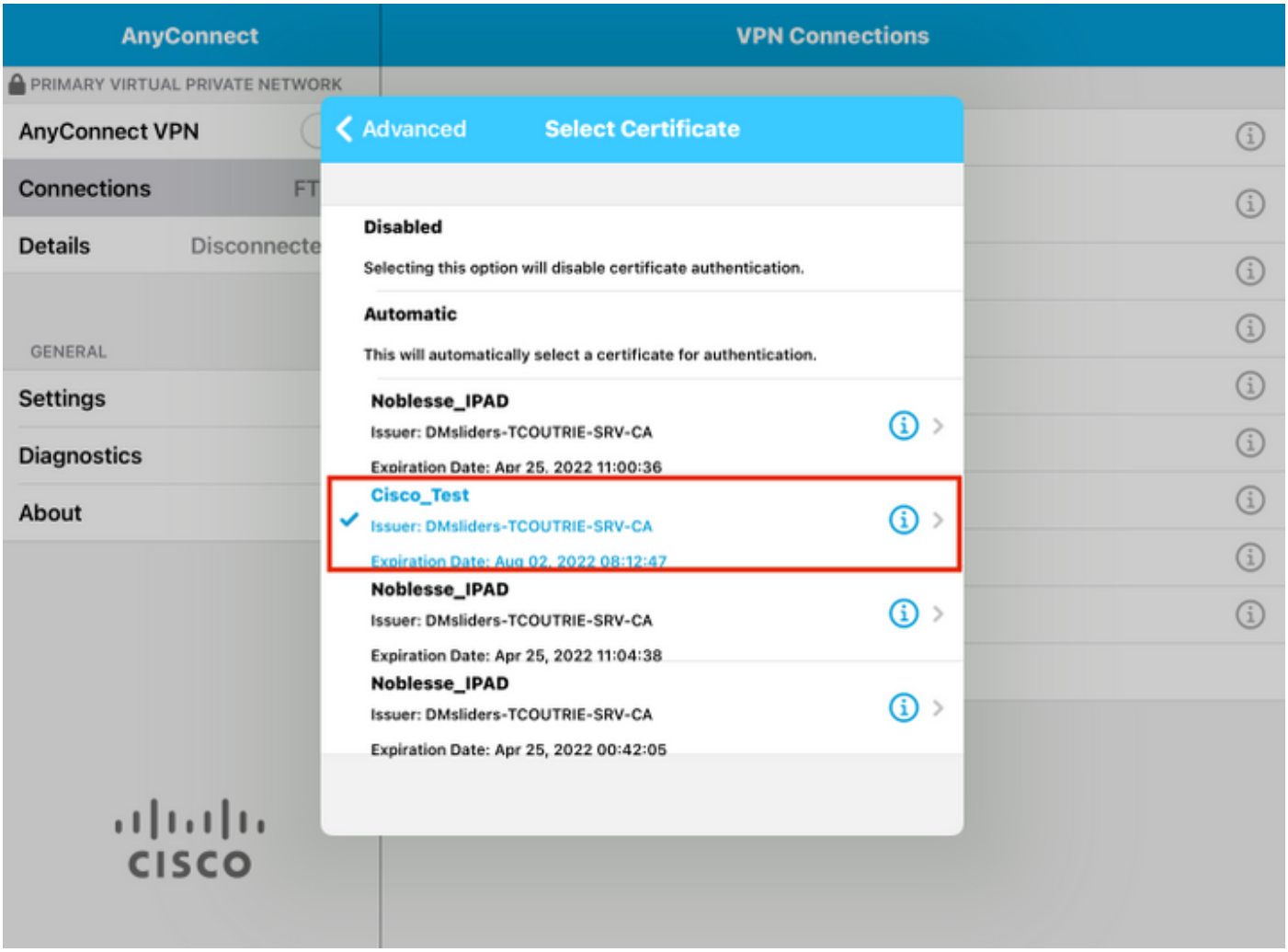
Beschreibung: Benennen Sie die Verbindung.

Serveradresse: IP-Adresse oder FQDN FTD

Erweitert: Zusätzliche Konfigurationen

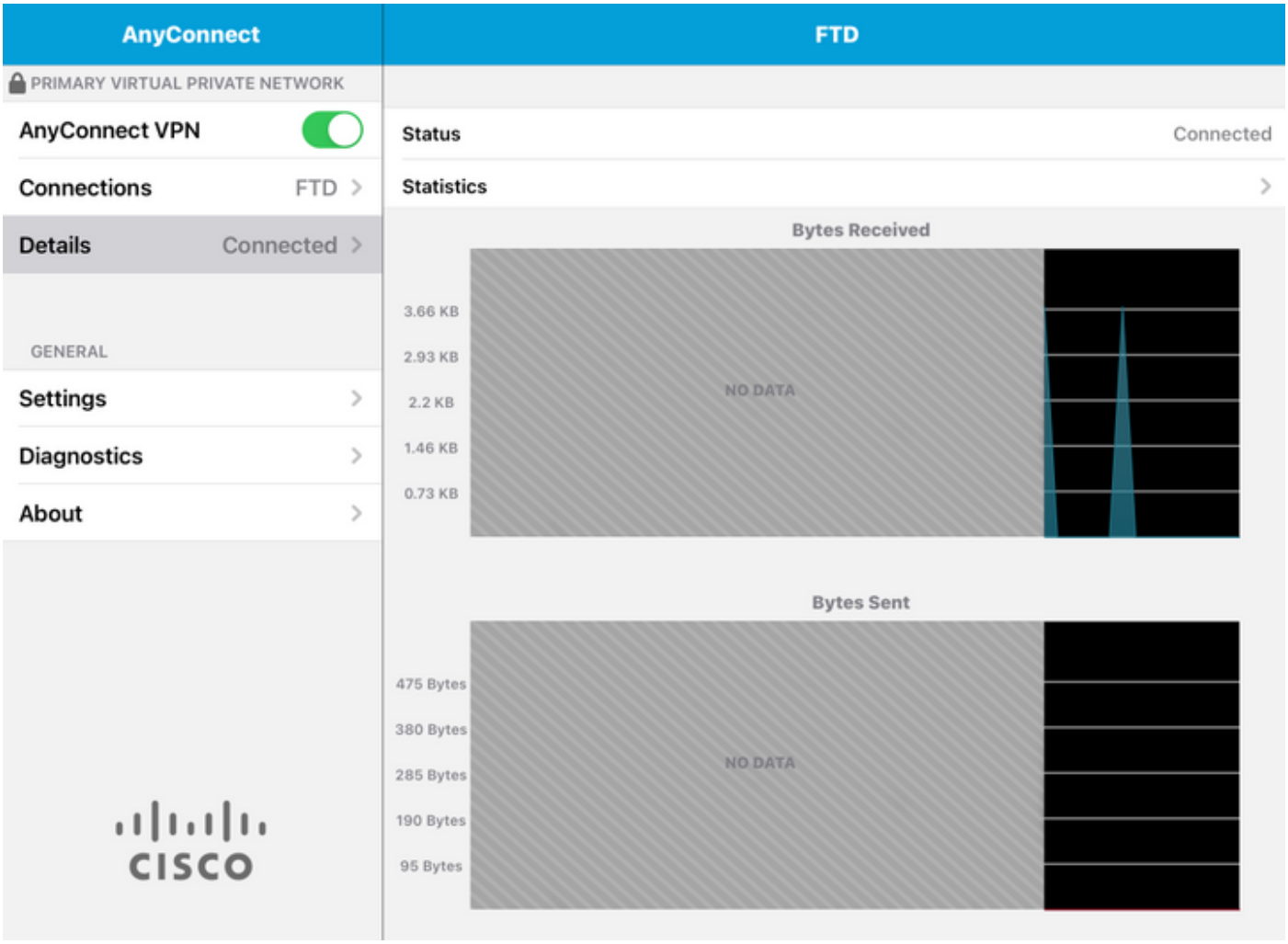
Schritt 7. Wählen Sie **Erweitert aus**.

Schritt 8: Wählen Sie **Zertifikat** und wählen Sie das neu hinzugefügte Zertifikat aus.




Schritt 9. Navigieren Sie zurück zu **Verbindungen**, und testen Sie.

Nach dem erfolgreichen Wechsel bleibt der Umschalter eingeschaltet und Details werden im Status als verbunden angezeigt.




# Überprüfung

Der Befehl **show vpn-sessiondb detail Anyconnect** zeigt alle Informationen über den angeschlossenen Host.

> **Tipp:** Die Option zum weiteren Filtern dieses Befehls sind die dem Befehl hinzugefügten Schlüsselwörter 'filter' oder 'sort'.

Beispiele:

```
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
```

# Fehlerbehebung

## Debugger

Folgende Debugger sind zur Behebung dieses Problems erforderlich:

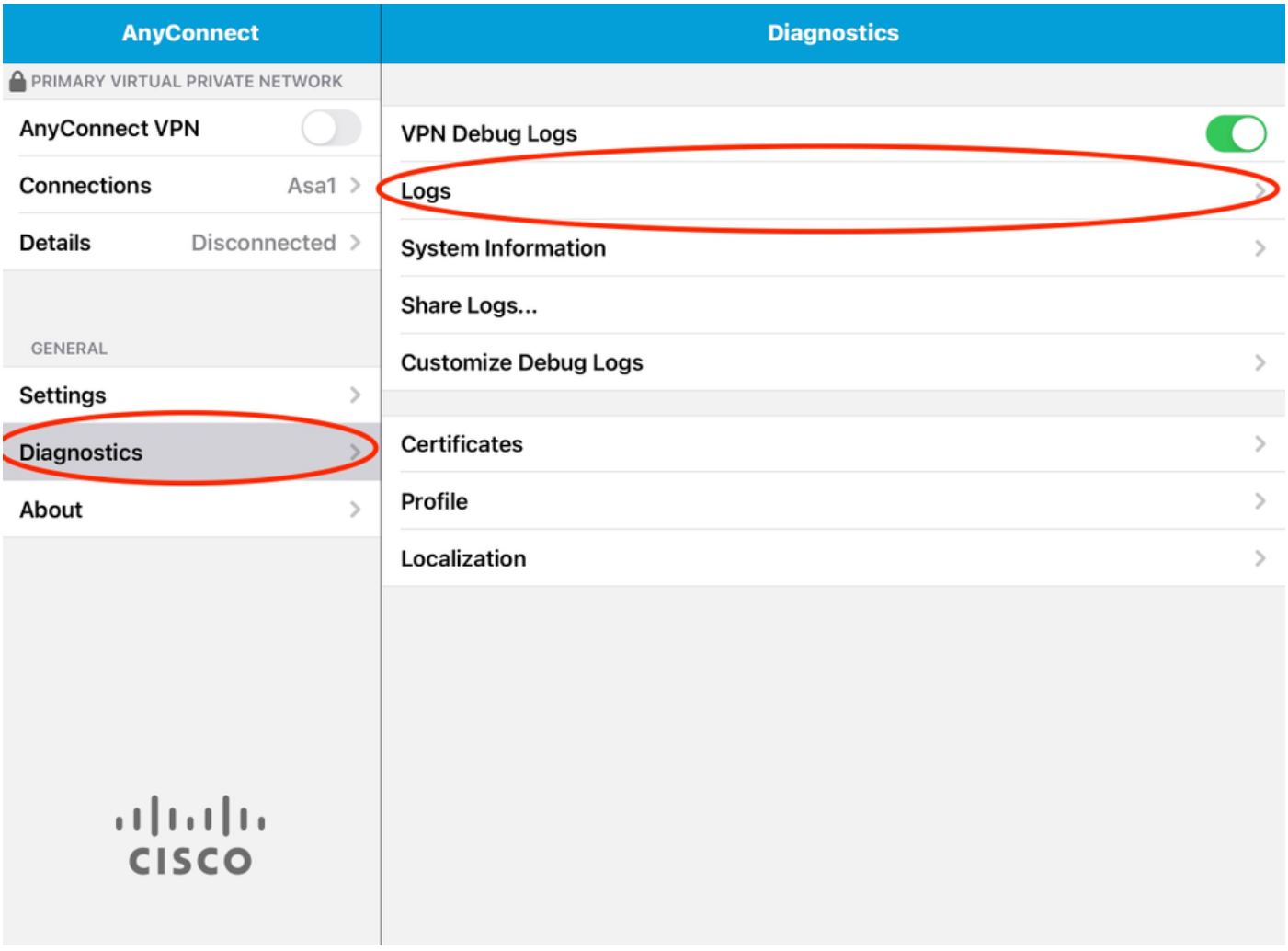
```
Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255
```

Wenn die Verbindung IPSEC und nicht SSL ist:

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

Protokolle der mobilen Anwendung AnyConnect:

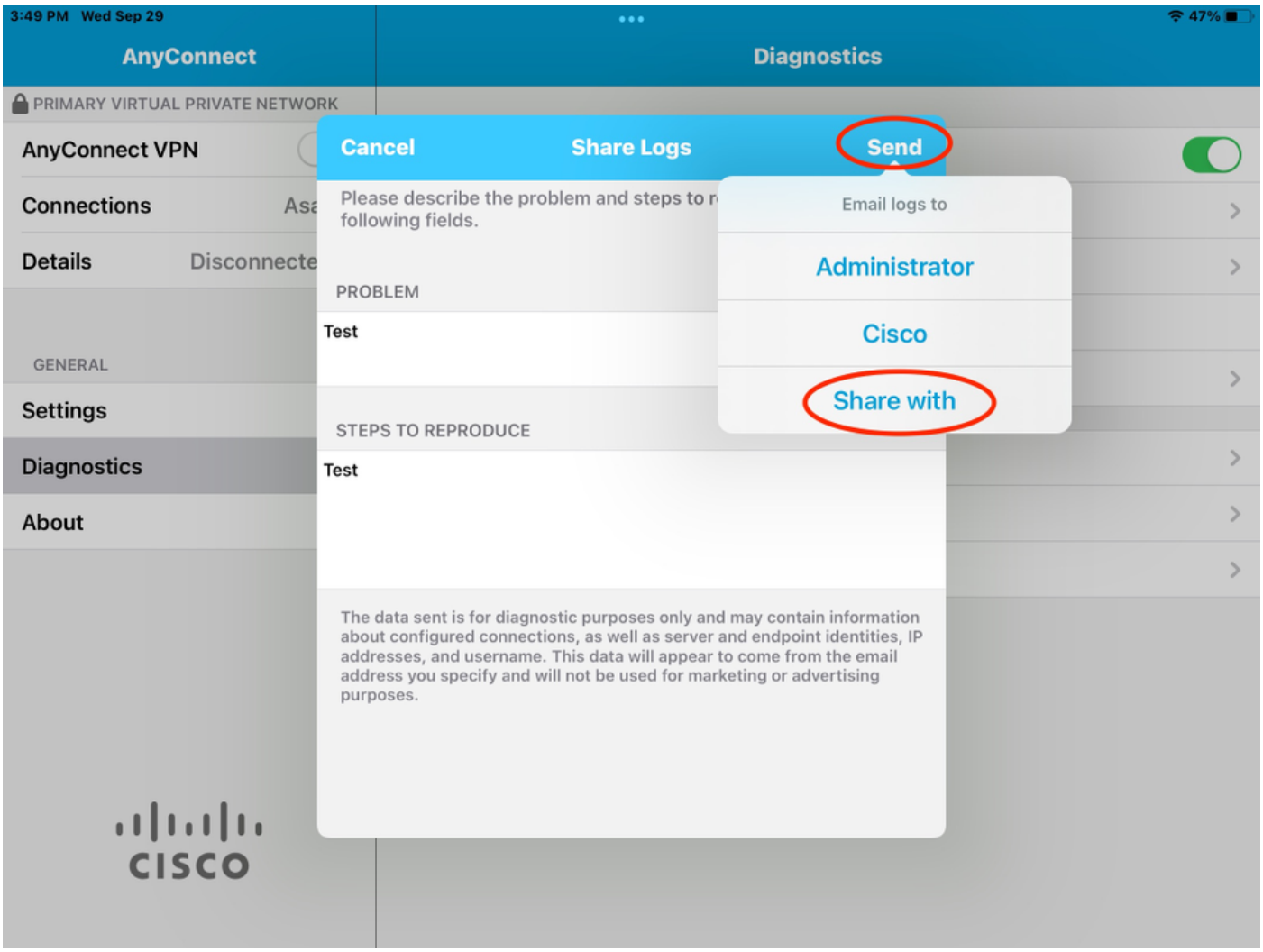
Navigieren Sie zu **Diagnostic > VPN Debug Logs > Share logs**.




Geben Sie Folgendes ein:

- Problem
- Schritte zur Reproduktion

Navigieren Sie dann zu **Senden > Freigeben mit**.




Dadurch wird die Option zum Senden der Protokolle mithilfe eines E-Mail-Clients angezeigt.