

モバイルアクセス用のAnyconnect証明書ベース認証の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[FTDでのCisco Anyconnectの設定](#)

[ネットワーク図](#)

[FTDへの証明書の追加](#)

[Cisco Anyconnectの設定](#)

[モバイルユーザ用の証明書の作成](#)

[モバイルデバイスでのインストール](#)

[確認](#)

[トラブルシューティング](#)

[デバッグ](#)

概要

このドキュメントでは、モバイルデバイスに証明書ベースの認証を実装する例について説明します。

前提条件

このガイドで使用するツールとデバイスは次のとおりです。

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Apple iOSデバイス(iPhone、iPad)
- 認証局 (CA)
- Cisco Anyconnectクライアントソフトウェア

要件

次の項目に関する知識があることが推奨されます。

- 基本的なVPN
- SSL/TLS
- 公開キーインフラストラクチャ
- FMCの使用経験

- OpenSSL
- Cisco AnyConnect

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

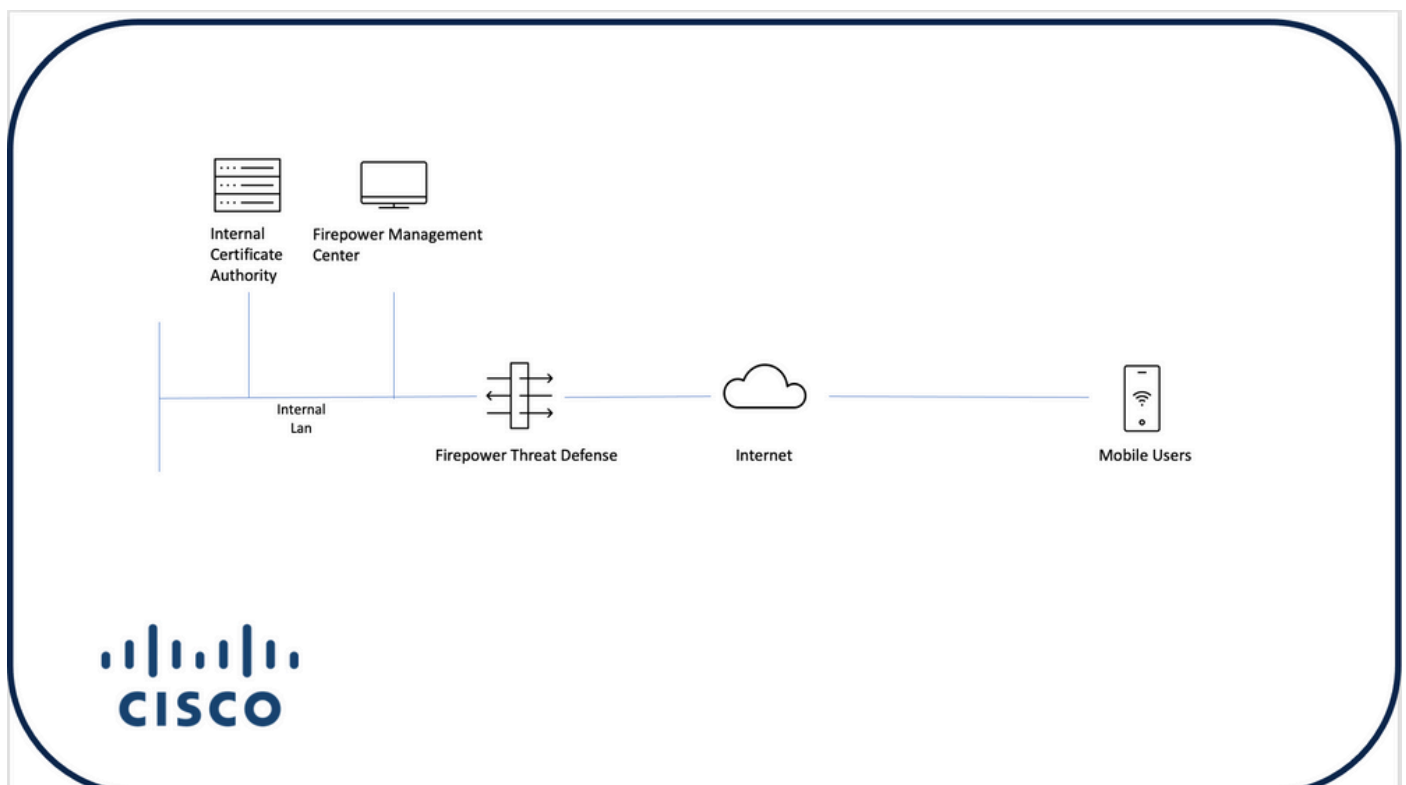
- シスコFTD
- Cisco FMC
- Microsoft CA Server
- XCA
- Cisco AnyConnect
- Apple ipad

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

FTDでのCisco Anyconnectの設定

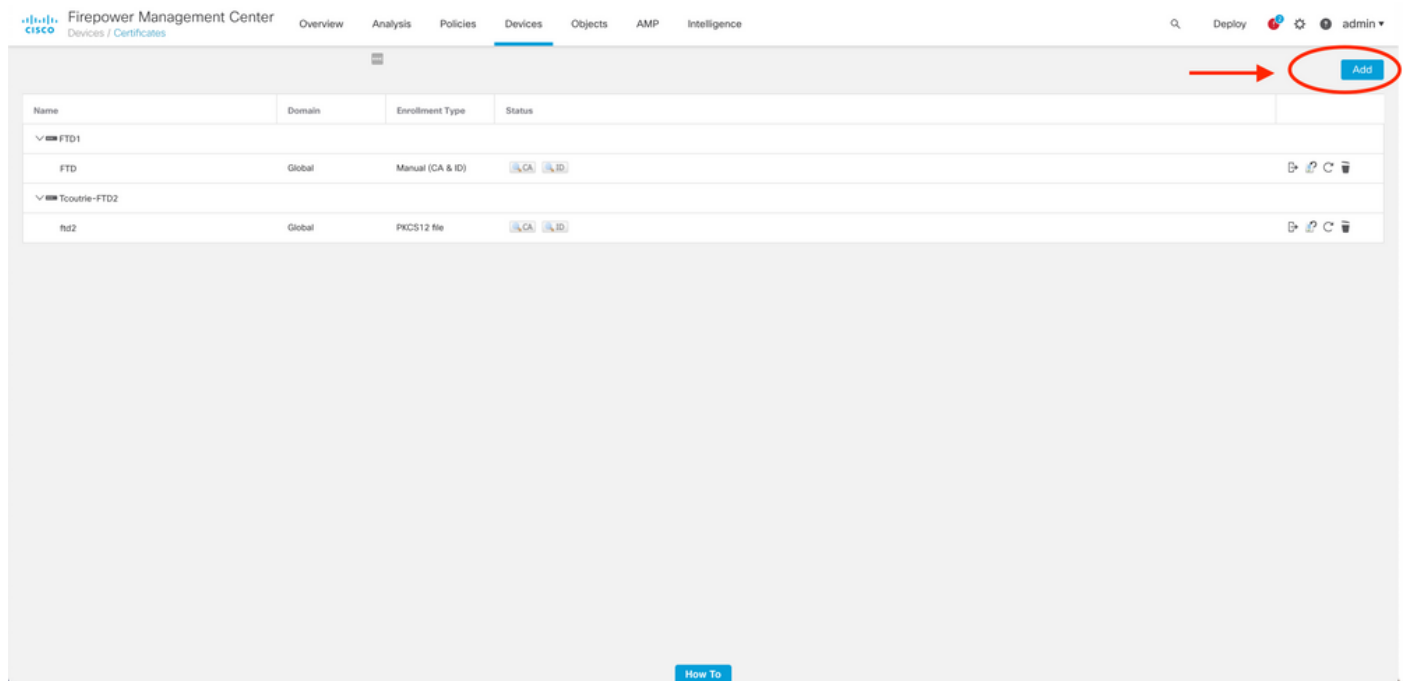
ここでは、FMC経由でAnyConnectを設定する手順について説明します。開始する前に、すべての設定を必ず導入してください。

ネットワーク図

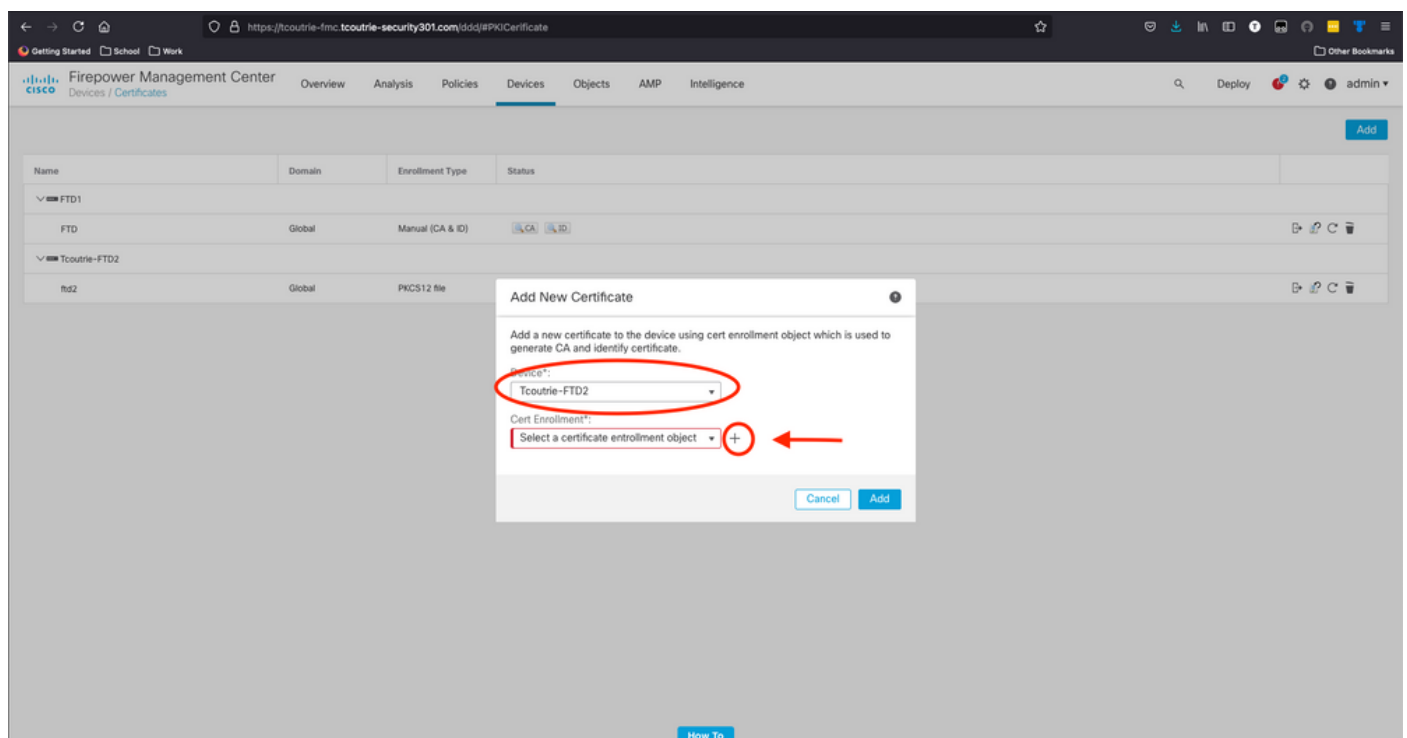


FTDへの証明書の追加

ステップ 1：FMCアプライアンスでFTDの証明書を作成します。次の図に示すように、Devices > Certificateの順に移動し、Addを選択します。




ステップ 2：VPN接続に必要なFTDを選択します。デバイスドロップダウンからFTDアプライアンスを選択します。+アイコンをクリックして、次の図に示すように新しい証明書登録方式を追加します。



ステップ 3：デバイスに証明書を追加します。環境内で証明書を取得するための推奨される方法

を選択します。

 ヒント：使用可能なオプションは次のとおりです。自己署名証明書 – 新しい証明書をローカルに生成する、SCEP - CAから証明書を取得する、手動 – ルート証明書とID証明書を手動でインストールする、PKCS12 – 暗号化された証明書バンドルをルート、ID、秘密キーと一緒にアップロードする。

ステップ 4：証明書をFTDデバイスにアップロードします。パスコード (PKCS12のみ) を入力し、次の図に示すようにSaveをクリックします。

Add Cert Enrollment ?


Name*

Description

CA Information Certificate Parameters Key Revocation


Enrollment Type:

PKCS12 File*: [Browse PKCS12 File](#)

Passphrase: 

Skip Check for CA flag in basic constraints of the CA Certificate

[Cancel](#) [Save](#)

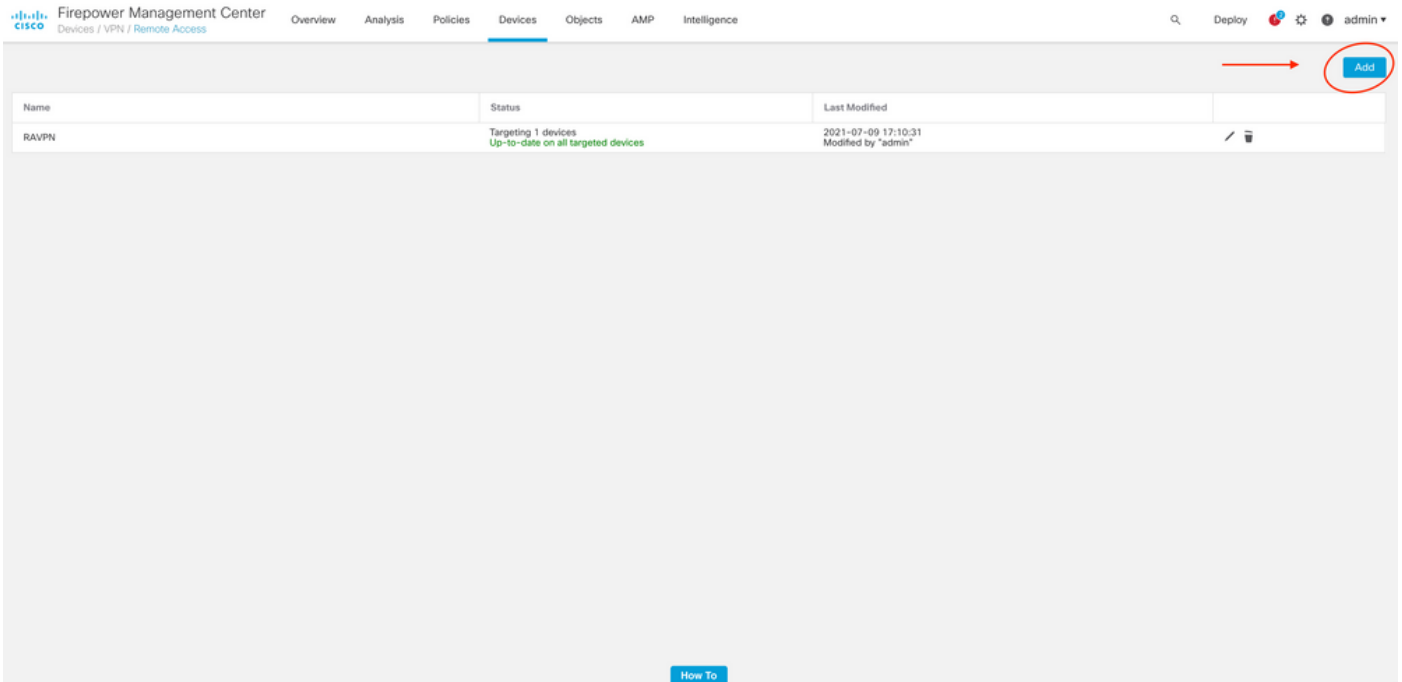
 注：ファイルを保存すると、証明書の展開がただちに行われます。証明書の詳細を表示するには、IDを選択します。

Cisco Anyconnectの設定


リモートアクセスウィザードを使用して、FMC経由でAnyConnectを設定します。

ステップ 1：リモートアクセスVPNポリシーウィザードを起動して、Anyconnectを設定します。

Devices > Remote Accessの順に移動し、Addを選択します。



The screenshot shows the Cisco Firepower Management Center interface. The breadcrumb navigation is "Devices / VPN / Remote Access". The main content area displays a table with the following data:

| Name | Status | Last Modified | |
|-------|---|--|---|
| RAVPN | Targeting 1 devices Up-to-date on all targeted devices | 2021-07-09 17:10:31 Modified by "admin" |  |

An arrow points from the text above to the "Add" button in the table. A "How To" button is visible at the bottom of the page.

ステップ 2：ポリシーの割り当て

ポリシーの割り当てを完了します。

- a. ポリシーに名前を付けます。
- b. 必要なVPNプロトコルを選択します。
- c. 設定を適用するターゲットデバイスを選択します。

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:

Description:

VPN Protocols:

- SSL
- IPsec-IKEv2

Targeted Devices:

Available Devices

- FTD1
- Tcourtie-FTD2

Selected Devices

- Tcourtie-FTD2

How To

Cancel Back Next

ステップ 3 : 接続プロファイル。

- 接続プロファイルに名前を付けます。
- 認証方式を Client Certificate Only に設定します。
- IPアドレスプールを割り当て、必要に応じて新しいグループポリシーを作成します。
- Next をクリックします。

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

AAA

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:

This name is configured as a connection alias. It can be used to connect to the VPN gateway.

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Username From Certificate: Map specific field Use entire DN (Distinguished Name) as username

Primary Field:

Secondary Field:

Authorization Server:

Accounting Server:

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS or RADIUS only)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pool:


IPv6 Address Pool:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:

Edit Group Policy

 注：認証セッションのユーザ名の入力に使用するプライマリフィールドを選択します。このガイドでは、証明書のCNを使用します。

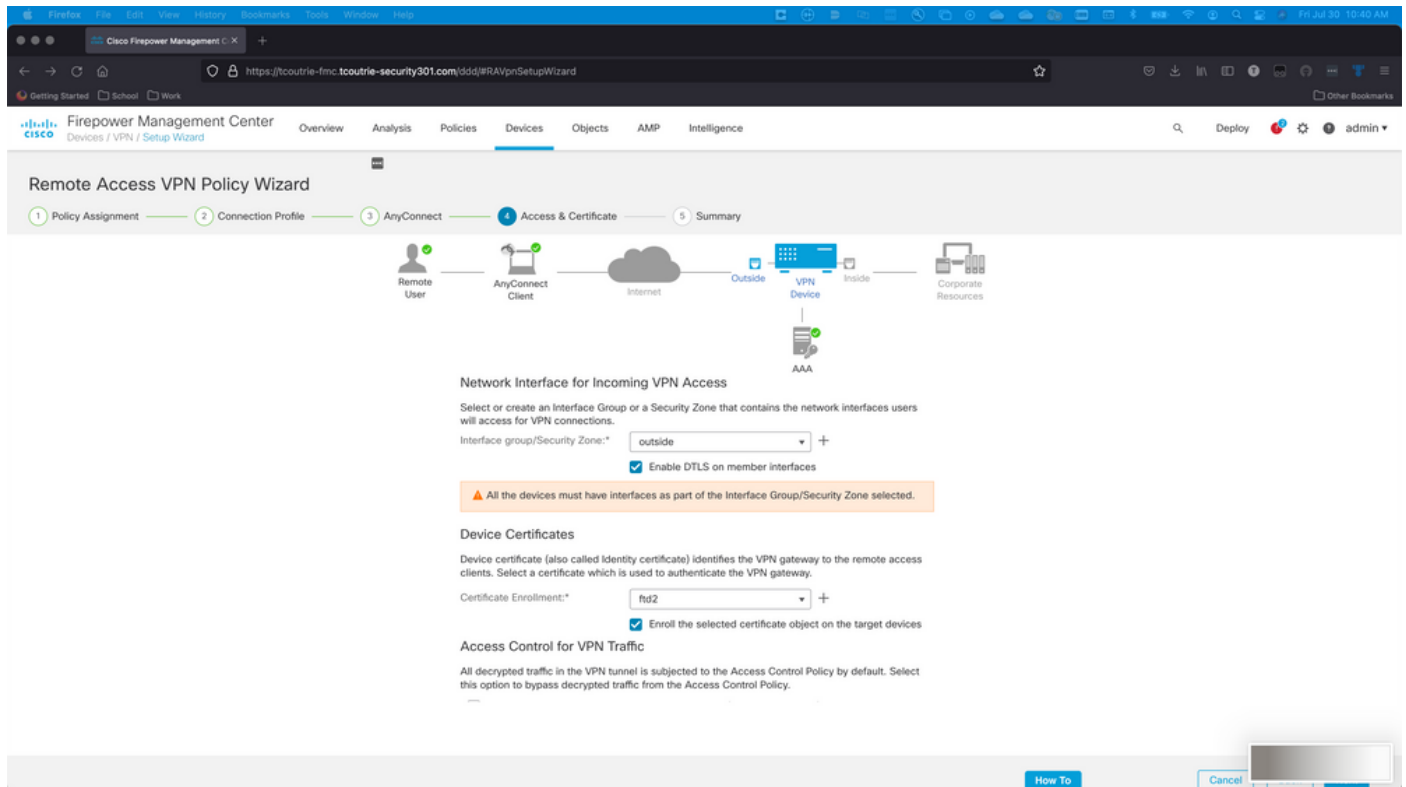
ステップ 4 : AnyConnect.

Anyconnectイメージをアプライアンスに追加します。Anyconnectの推奨バージョンをアップロードし、Nextをクリックします。

 注: Cisco Anyconnectパッケージは、Software.Cisco.comからダウンロードできます。

ステップ 5 : アクセスおよび証明書。

次の図に示すように、証明書をインターフェイスに適用し、インターフェイスレベルでAnyconnectを有効にして、Nextをクリックします。



手順 6 : 要約.

設定を確認します。すべてチェックアウトしたら、finishをクリックしてからdeployをクリックします。

モバイルユーザ用の証明書の作成

接続に使用するモバイルデバイスに追加する証明書を作成します。

ステップ 1 : XCAです。

a. XCAを開きます

b.新しいデータベースの起動

ステップ 2 : CSRを作成します。

a. Certificate Signing Request(CSR)を選択します

- b. New Requestの選択
- c. 証明書に必要なすべての情報とともに値を入力します
- d. 新しいキーを生成する
- e. 終了したら、OKをクリックします。

X Certificate and Key management

Create Certificate signing request

Source Extensions Key usage Netscape Advanced

Distinguished name

| | | | |
|---------------------|----------------------|------------------------|----------------------|
| Internal name | <input type="text"/> | organizationName | <input type="text"/> |
| countryName | <input type="text"/> | organizationalUnitName | <input type="text"/> |
| stateOrProvinceName | <input type="text"/> | commonName | Cisco_Test |
| localityName | <input type="text"/> | emailAddress | <input type="text"/> |

| Type | Content |
|------|---------|
|------|---------|

Add
Delete

Private key

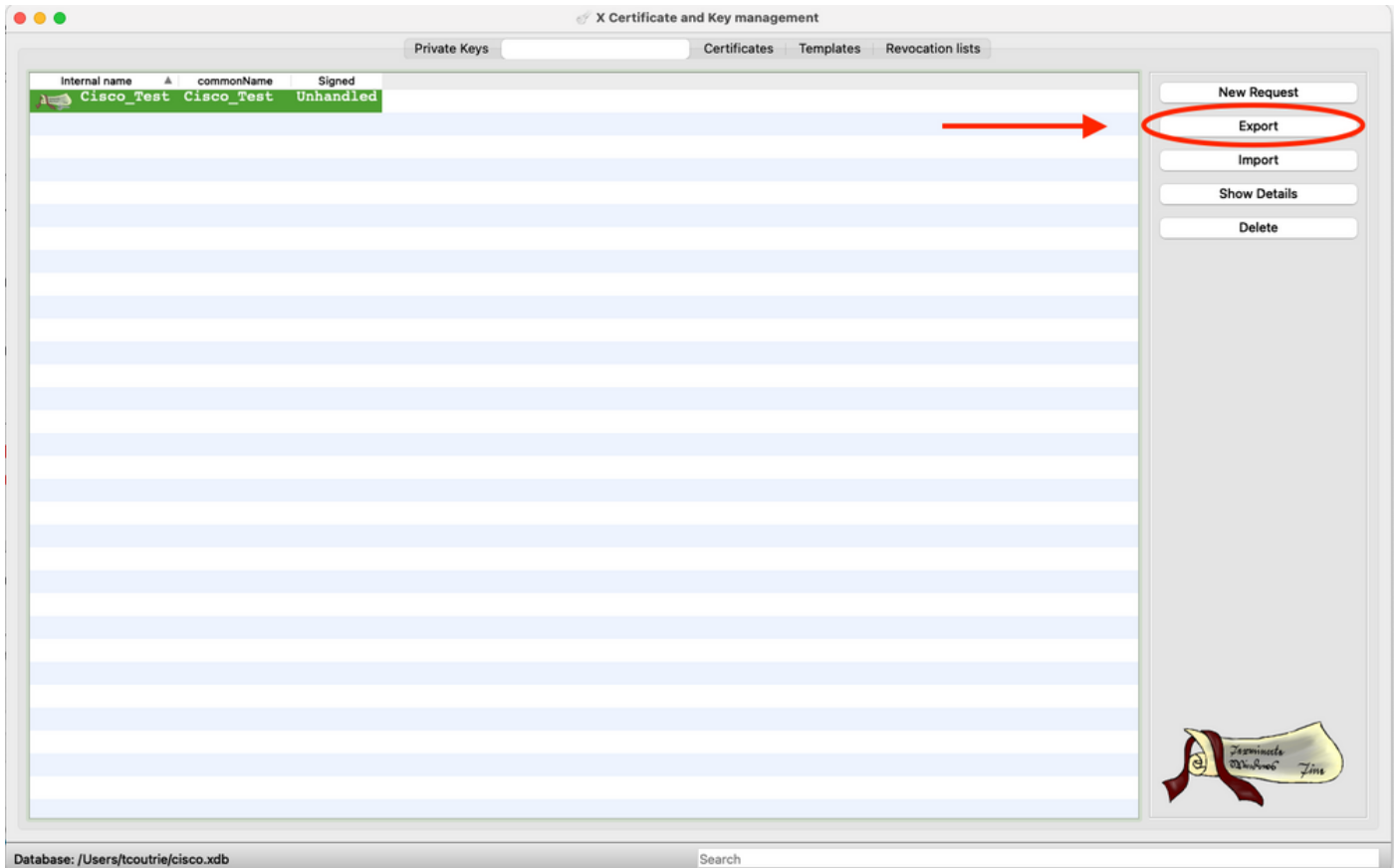
Cisco_Test_1 (RSA:2048 bit) Used keys too


Cancel OK

注：このドキュメントでは、証明書のCNを使用します。

ステップ 3：CSRを送信します。

- a. CSRのエクスポート
- b. CSRをCAに送信して新しい証明書を取得する




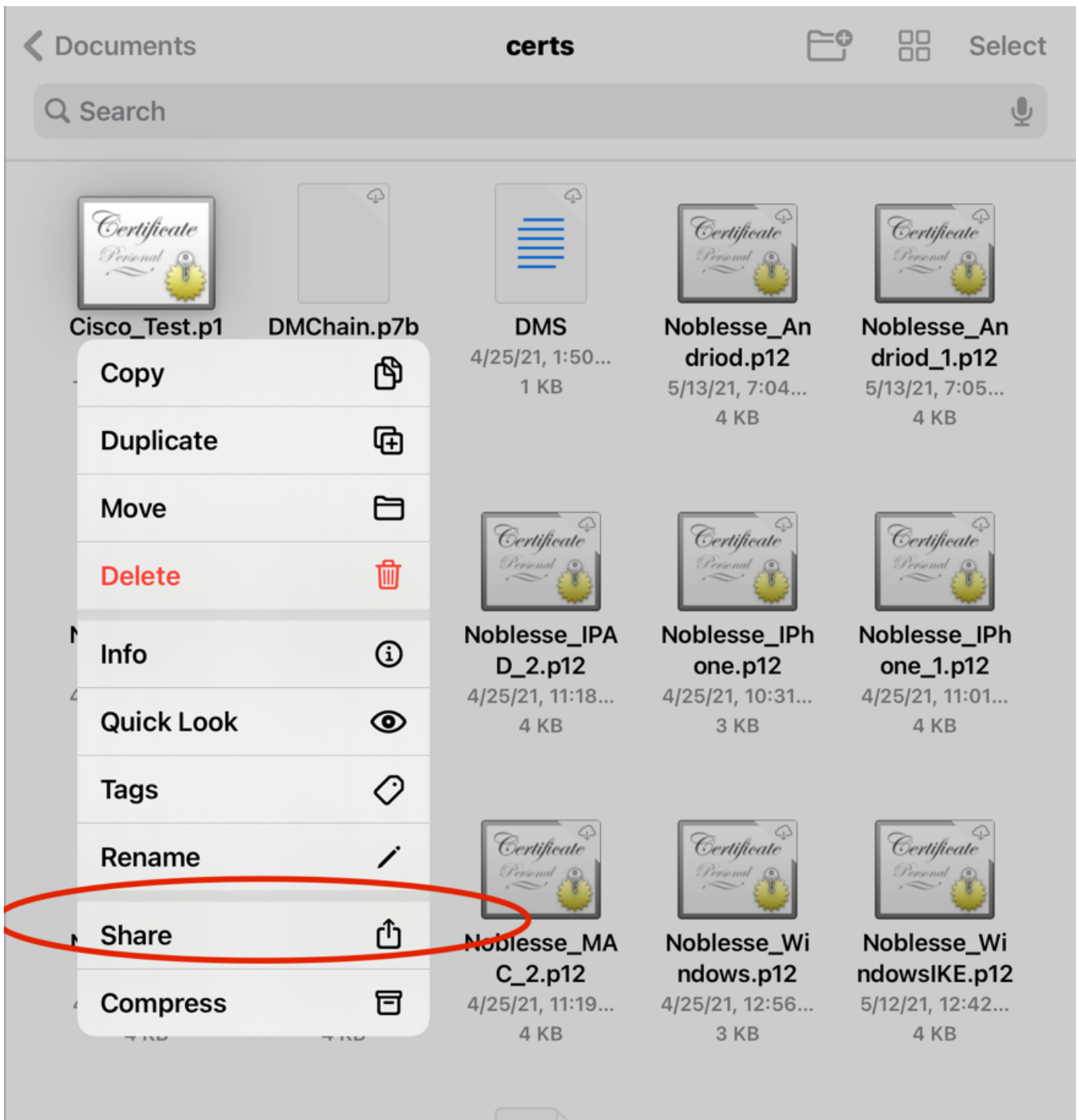
 注:CSRのPEM形式を使用してください。

モバイルデバイスでのインストール

ステップ 1 : モバイルデバイスにデバイス証明書を追加します。

ステップ 2 : Anyconnectアプリケーションと証明書を共有して、新しい証明書アプリケーションを追加します。

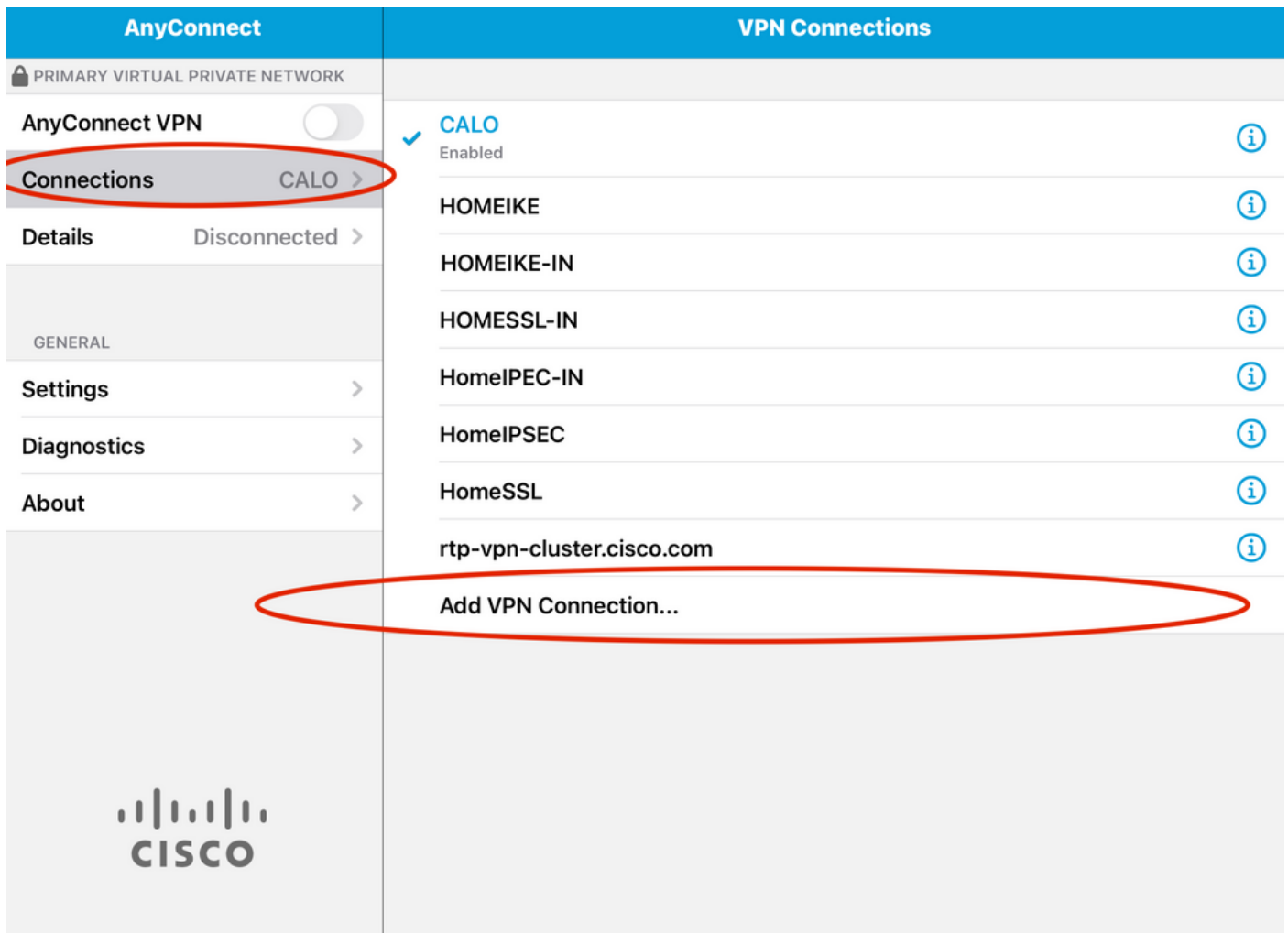
 注意 : 手動インストールでは、ユーザは証明書をアプリケーションと共有する必要があります。これは、MDM経由でプッシュされた証明書には適用されません。



ステップ 3 : PKCS12ファイルの証明書パスワードを入力します。

ステップ 4 : Anyconnectで新しい接続を作成します。

ステップ 5 : 新しい接続に移動します。Connections > Add VPN Connection。



手順 6 : 新しい接続の情報を入力します。

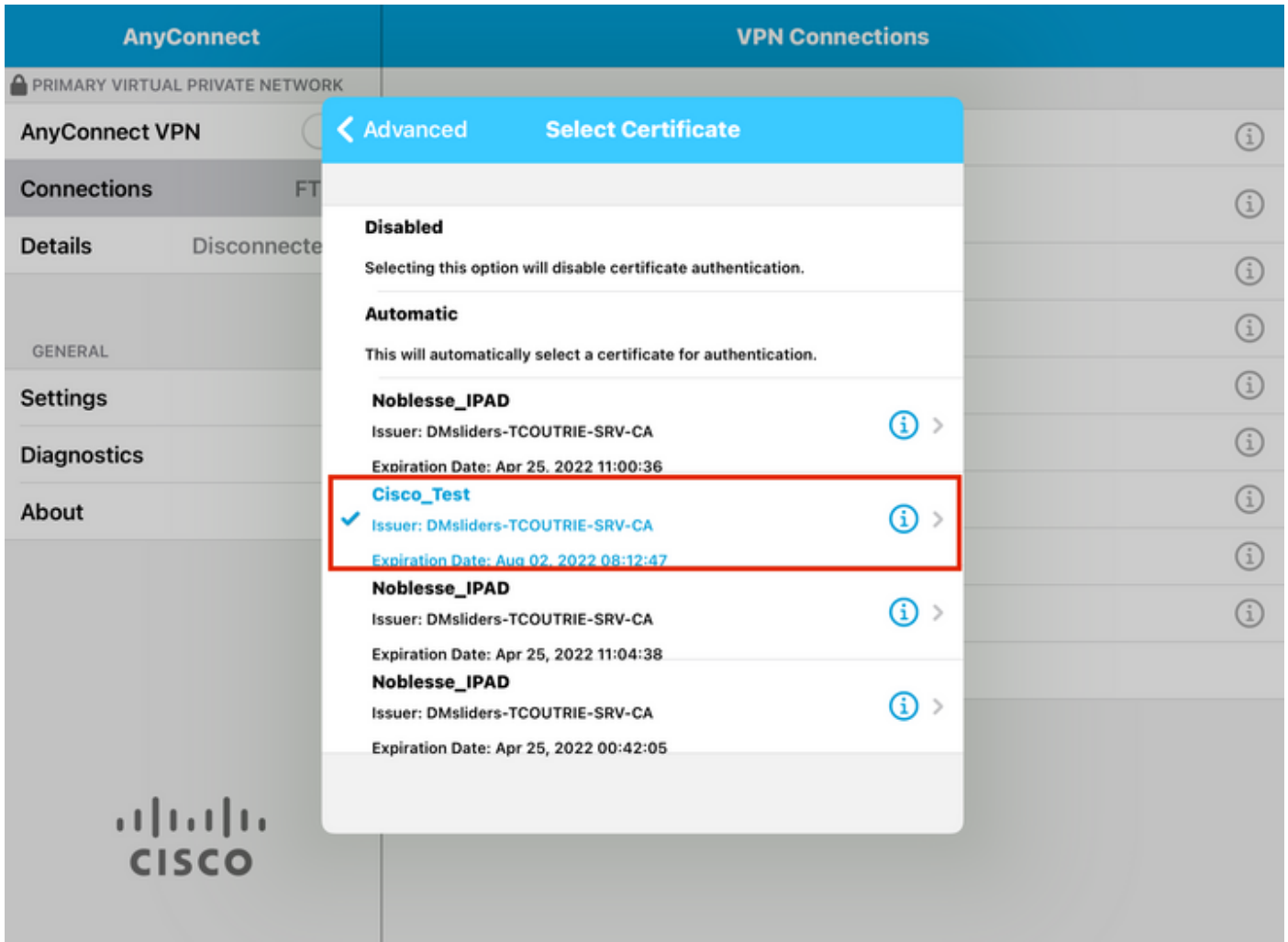
説明 : 接続に名前を付けます。

サーバアドレス : FTDのIPアドレスまたはFQDN

Advanced : その他の設定

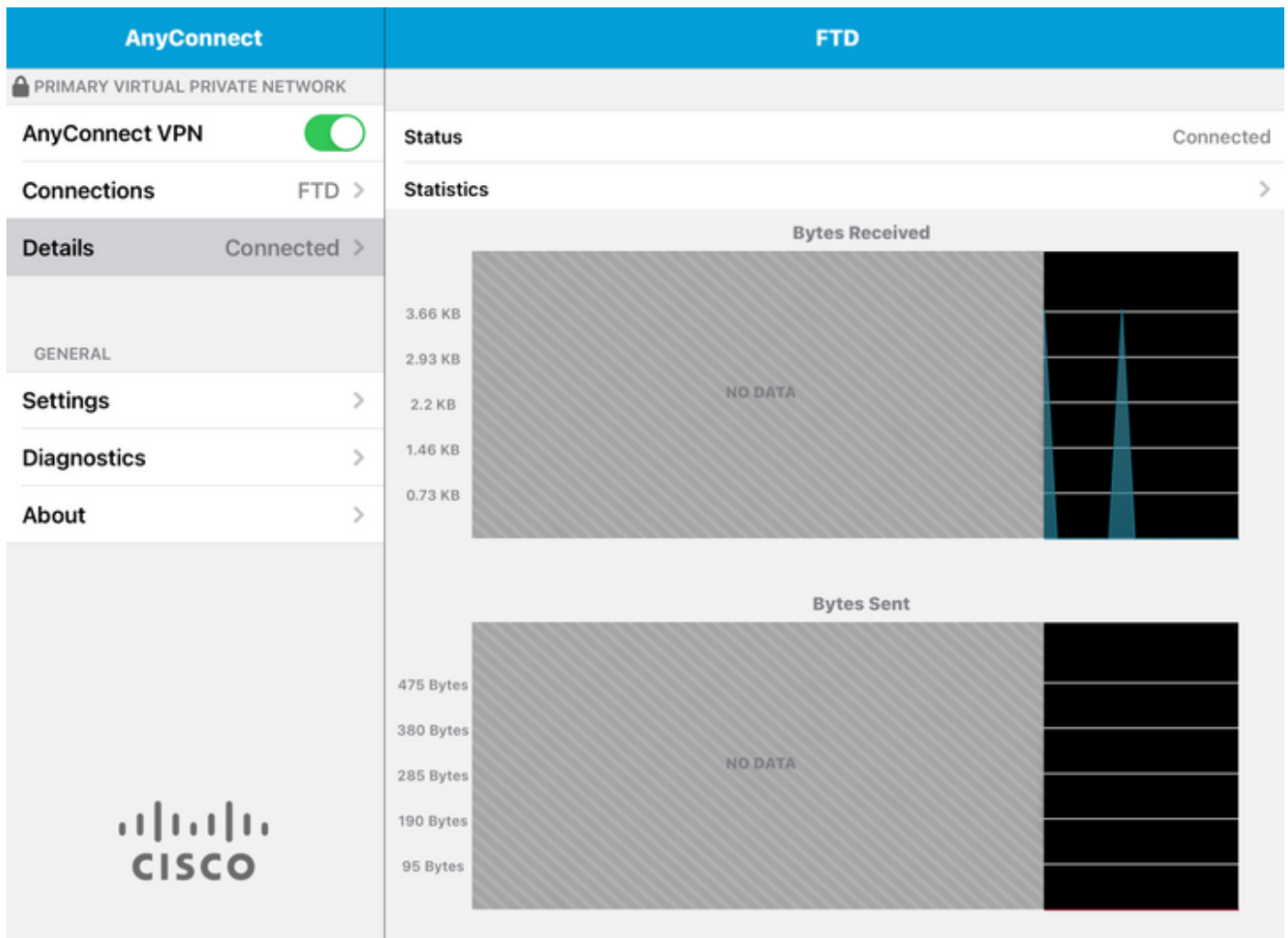
手順 7 : [Advanced] を選択します。

ステップ 8 : Certificateを選択し、新しく追加した証明書を選択します。




ステップ 9 : Connectionsに戻り、テストします。

正常に完了すると、切り替えはオンのままになり、ステータスに詳細がconnectedと表示されます。



確認

show vpn-sessiondb detail Anyconnectコマンドは、接続されているホストに関するすべての情報を表示します。

 ヒント：このコマンドをさらにフィルタリングするオプションは、コマンドに追加された「filter」キーワードまたは「sort」キーワードです。

例：

```
Tcourtie-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

トラブルシュート

デバッグ

この問題のトラブルシューティングに必要なデバッグは次のとおりです。

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

接続がSSLではなくIPSECの場合：

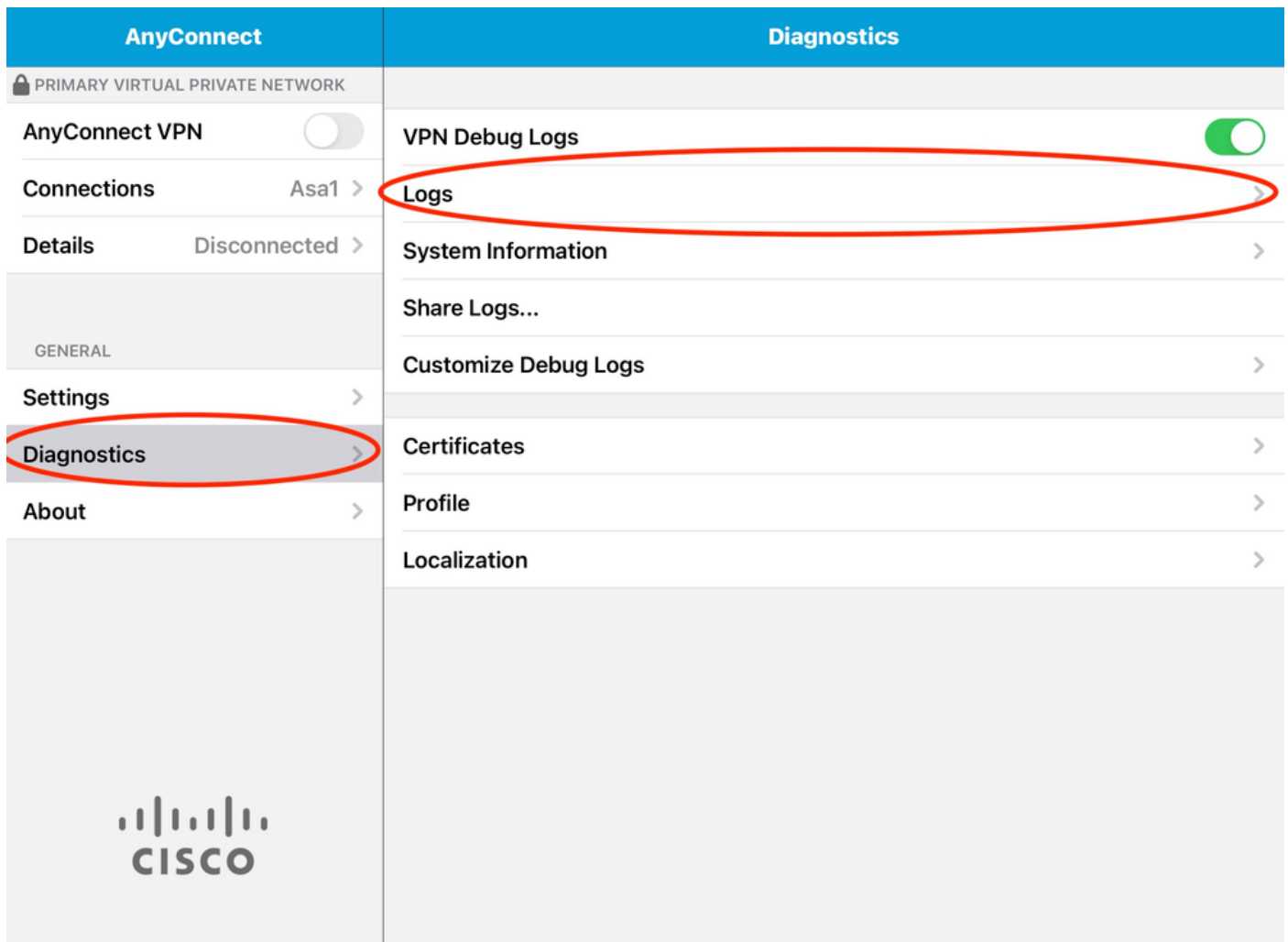
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

Anyconnectモバイルアプリケーションからのログ：

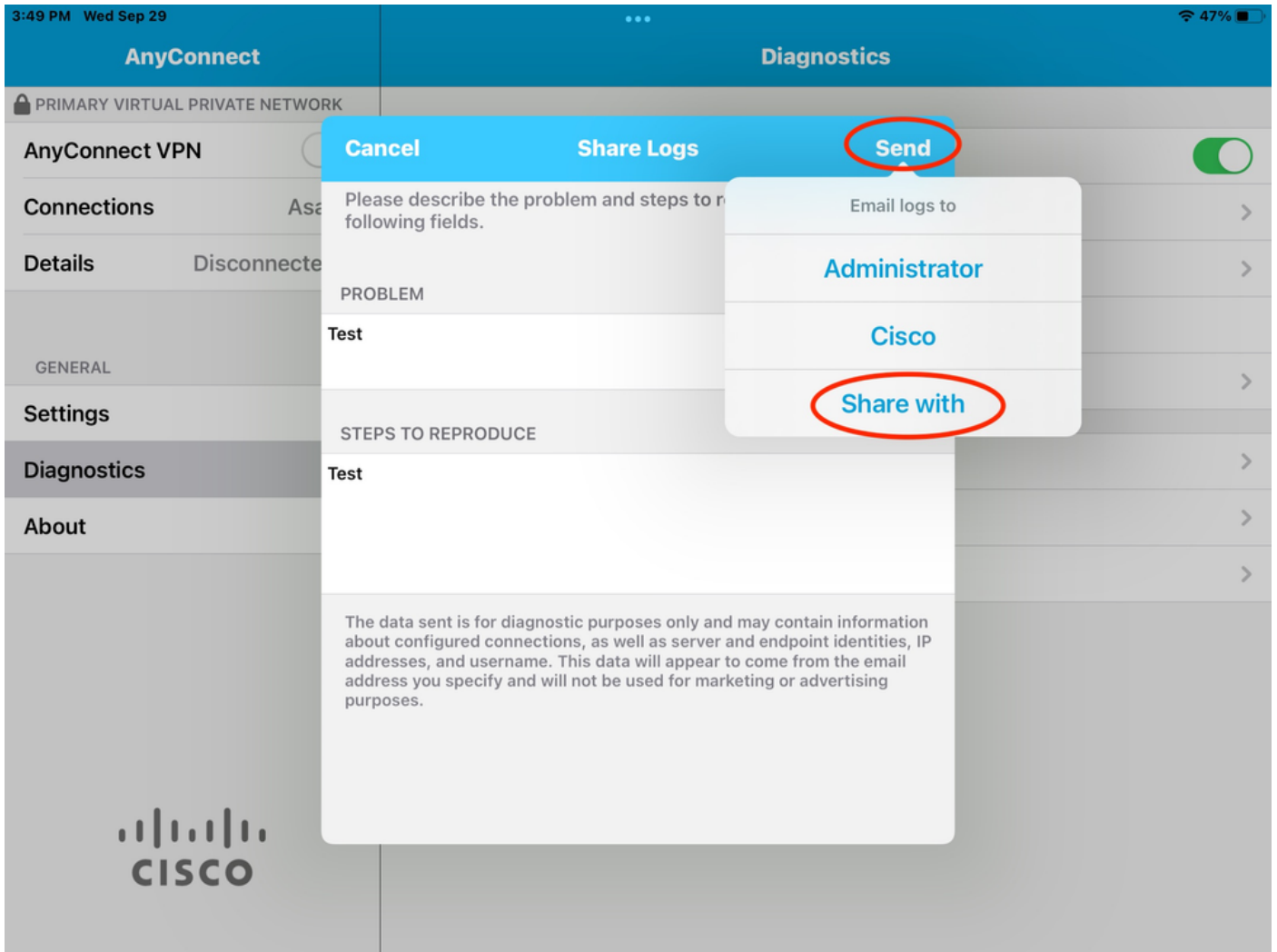
Diagnostic > VPN Debug Logs > Share logsの順に移動します。



次の情報を入力します。

- 問題
- 再現手順

次に、Send > Share withの順に移動します。



これは、電子メールクライアントを使用してログを送信するオプションを提供します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。