為移動訪問配置基於Anyconnect證書的身份驗證

目錄

簡介

必要條件

- 需求
- 採用元件

設定FTD上的Cisco Anyconnect

- 網路圖表
- 將憑證新增到FTD
- 配置Cisco Anyconnect

為移動使用者建立證書

- 在流動裝置上安裝

驗證

疑難排解

- 調試

簡介

本檔案介紹在行動裝置上實作基於憑證的驗證之範例。

必要條件

本指南中使用的工具和裝置包括：

- Cisco Firepower威脅防禦(FTD)
- Firepower Management Center (FMC)
- Apple iOS裝置(iPhone、iPad)
- 證書頒發機構(CA)
- Cisco Anyconnect使用者端軟體

需求

思科建議您瞭解以下主題：

- 基本VPN
- SSL/TLS
- 公開金鑰基礎架構
- 使用FMC的經驗
- OpenSSL
- Cisco Anyconnect

採用元件

本文中的資訊係根據以下軟體和硬體版本：

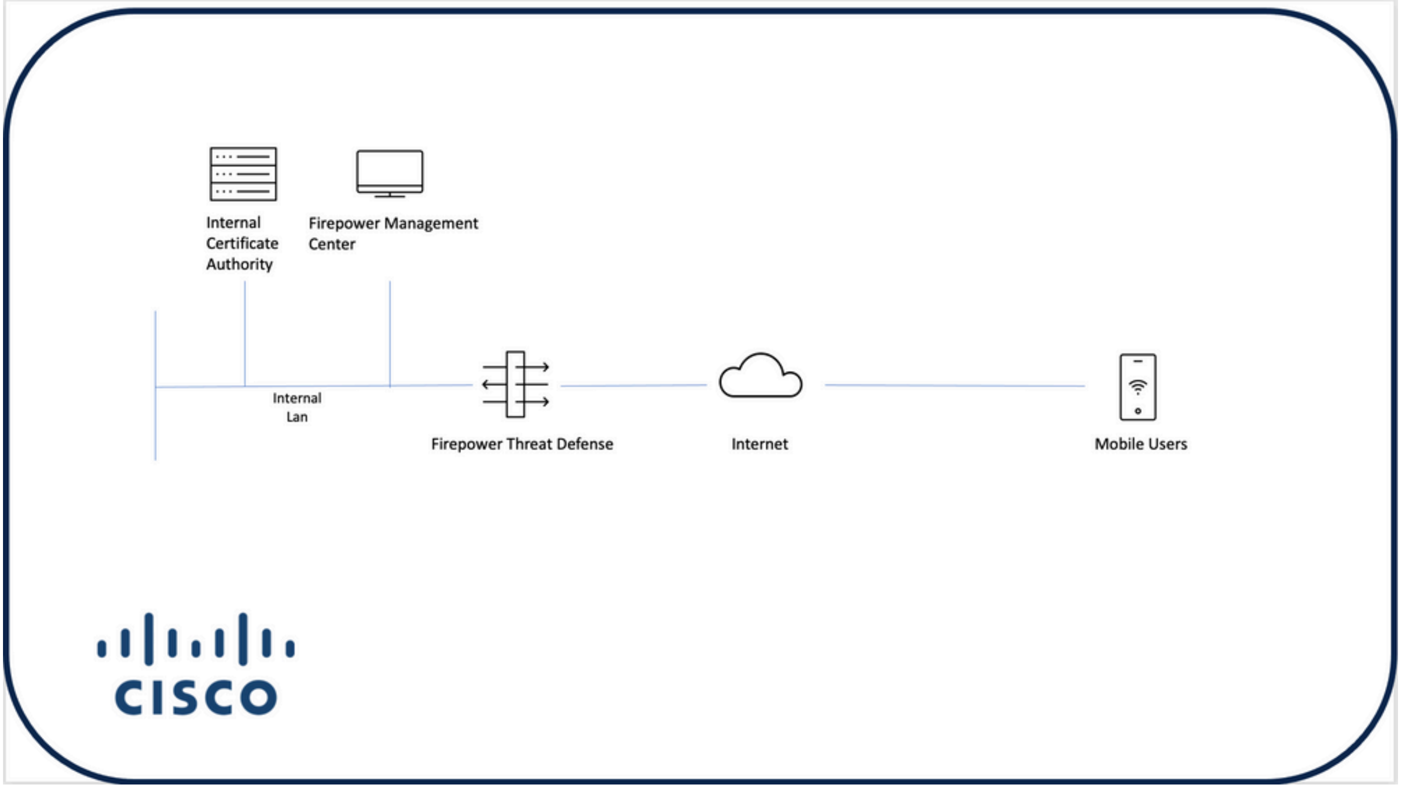
- Cisco FTD
- Cisco FMC
- Microsoft CA伺服器
- XCA
- Cisco Anyconnect
- Apple ipad

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定FTD上的Cisco Anyconnect

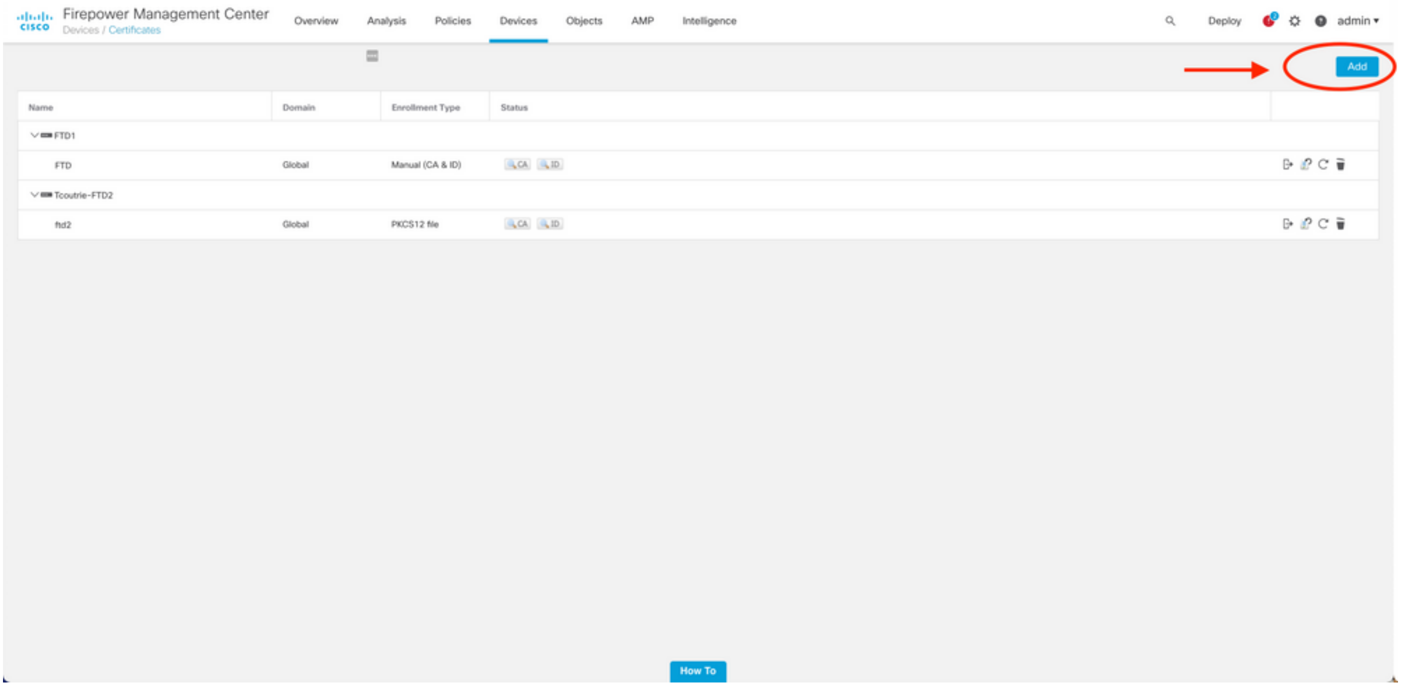
本節介紹通過FMC配置Anyconnect的步驟。開始之前，請務必部署所有配置。

網路圖表



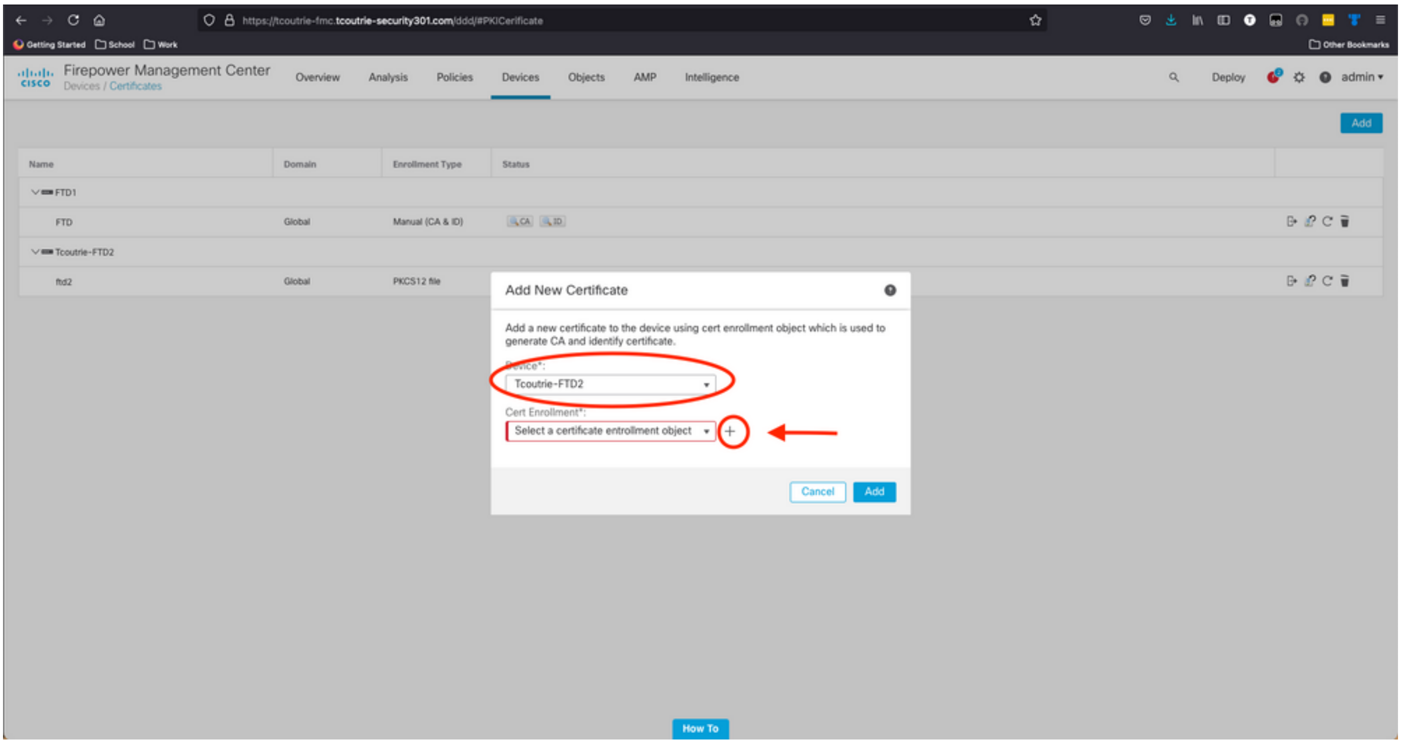
將憑證新增到FTD

步驟 1.在FMC裝置上為FTD建立憑證。導覽至Devices > Certificate，然後選擇Add，如下圖所示：



Name	Domain	Enrollment Type	Status
FTD1			
FTD	Global	Manual (CA & ID)	CA ID
Tcoutrie-FTD2			
ftd2	Global	PKCS12 file	CA ID

步驟 2.選擇VPN連線所需的FTD。從devices下拉選單中選擇FTD裝置。按一下+圖示可新增新的證書註冊方法，如下圖所示：



Name	Domain	Enrollment Type	Status
FTD1			
FTD	Global	Manual (CA & ID)	CA ID
Tcoutrie-FTD2			
ftd2	Global	PKCS12 file	

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: Tcoutrie-FTD2

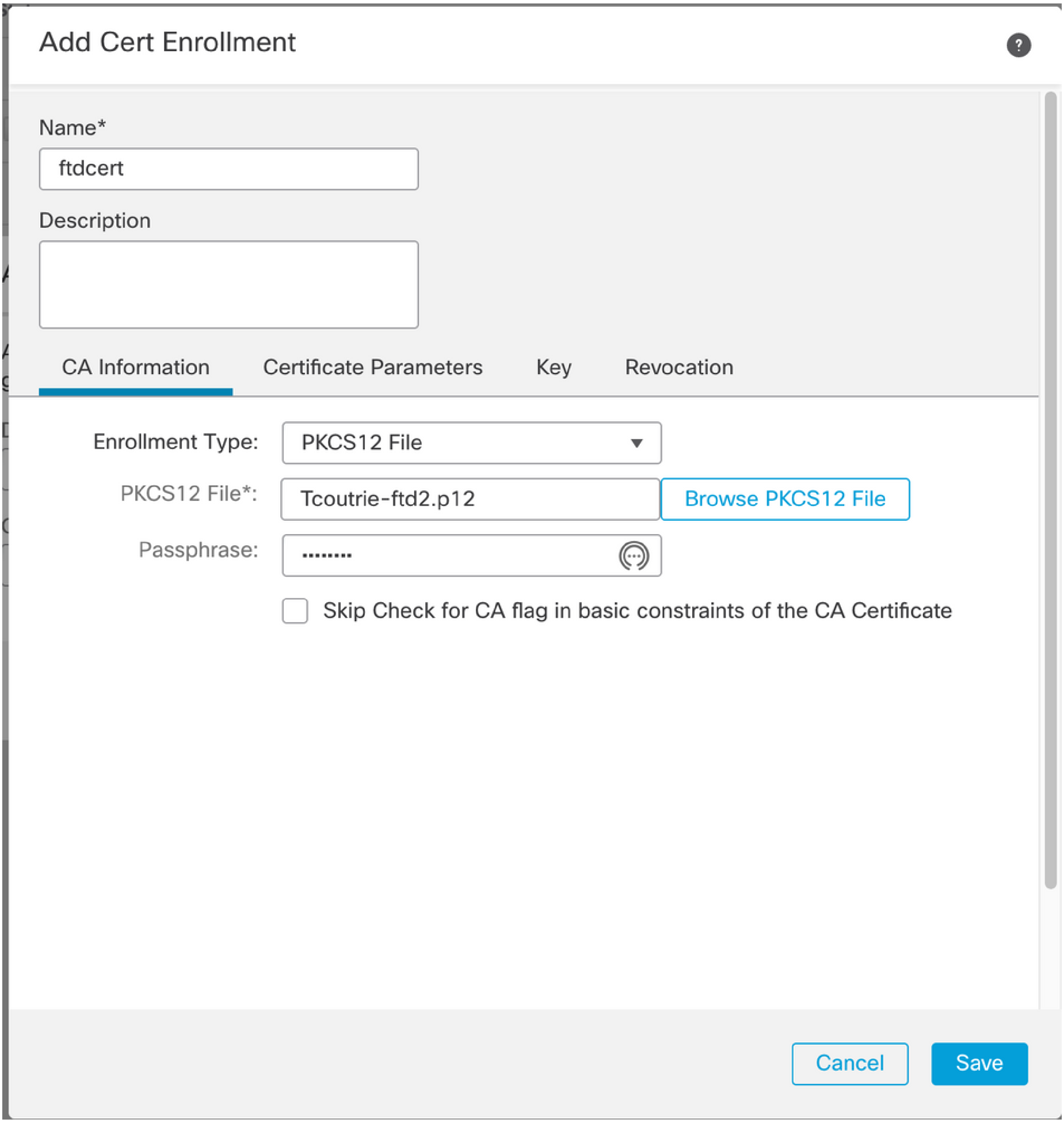
Cert Enrollment*: Select a certificate entrollment object +

Cancel Add

步驟 3.將證書新增到裝置。選擇在環境中獲取證書的首選方法。

提示：可用選項包括：自簽名證書 — 本地生成新證書、SCEP — 使用簡單證書註冊協定從CA獲取證書、手動 — 手動安裝根和身份證書、PKCS12 — 上傳包含根、身份和私鑰的加密證書捆綁包。

步驟 4.將憑證上傳到FTD裝置。輸入密碼（僅限PKCS12）並按一下Save，如下圖所示：



Add Cert Enrollment

Name*

ftdcert

Description

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: Tcoutrie-ftd2.p12

Passphrase: ••••••••

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

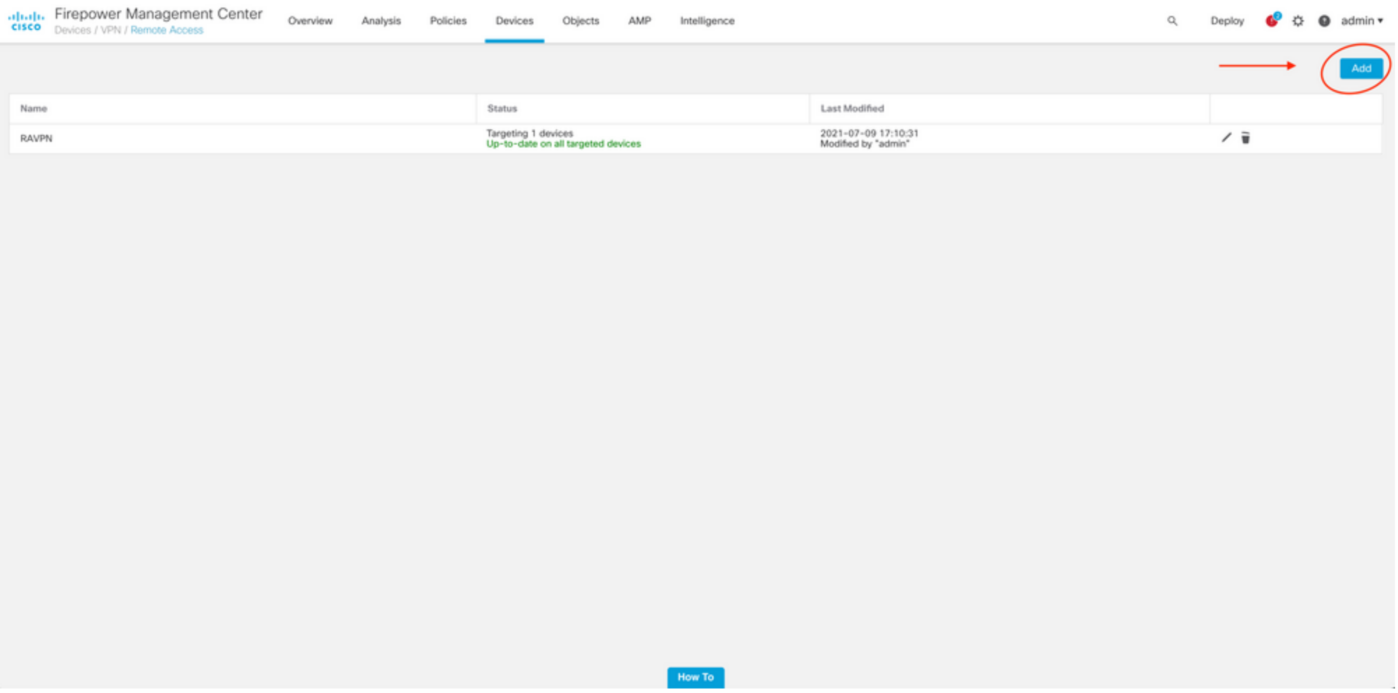
註：儲存檔案後，立即部署證書。要檢視證書詳細資訊，請選擇ID。

配置Cisco Anyconnect

使用遠端訪問嚮導通過FMC配置Anyconnect。

步驟 1.啟動遠端訪問VPN策略嚮導以配置Anyconnect。

導覽至Devices > Remote Access，然後選擇Add。



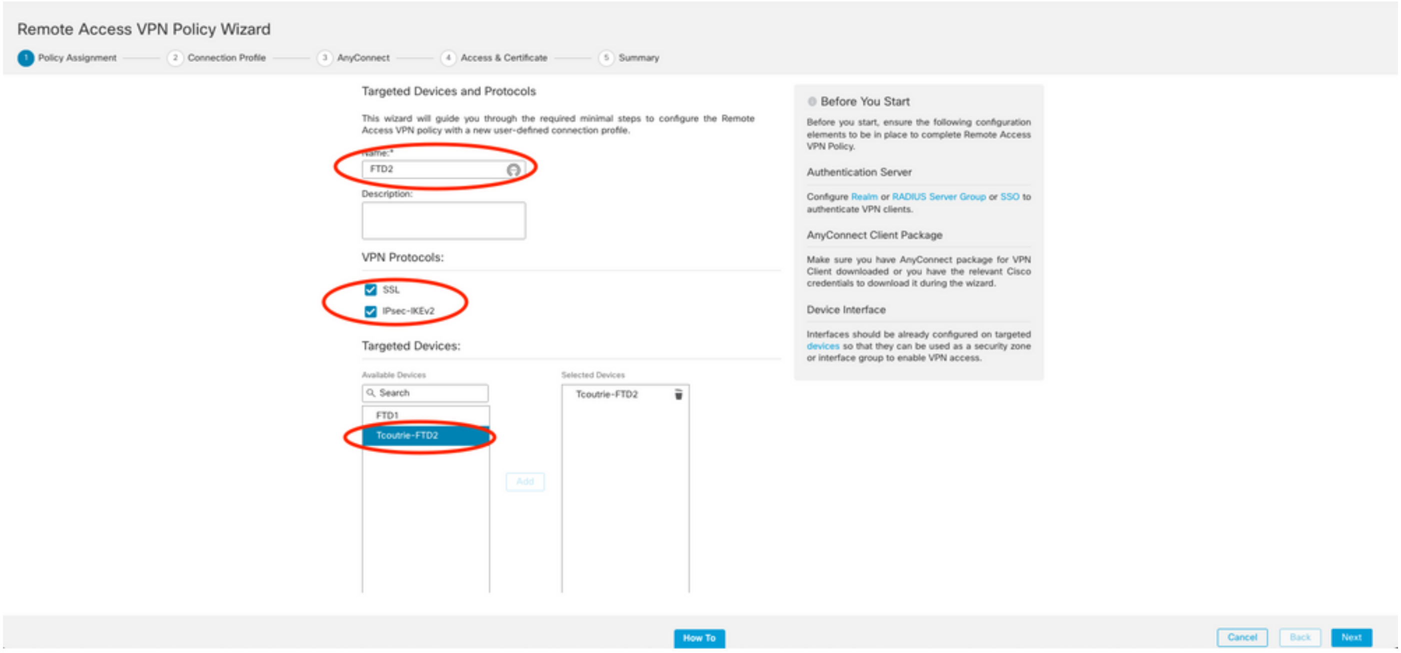
Name	Status	Last Modified
RAVPN	Targeting 1 devices Up-to-date on all targeted devices	2021-07-09 17:10:31 Modified by "admin"

步驟 2.策略分配。

完成策略分配：
a.命名策略。

b.選擇所需的VPN協定。

c.選擇要應用配置的目標裝置。



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:* FTD2

Description:

VPN Protocols:

☑ SSL

☑ IPsec-IKEv2

Targeted Devices:

Available Devices: FTD1, Tcoutrie-FTD2

Selected Devices: Tcoutrie-FTD2

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure Realm or RADIUS Server Group or SSO to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

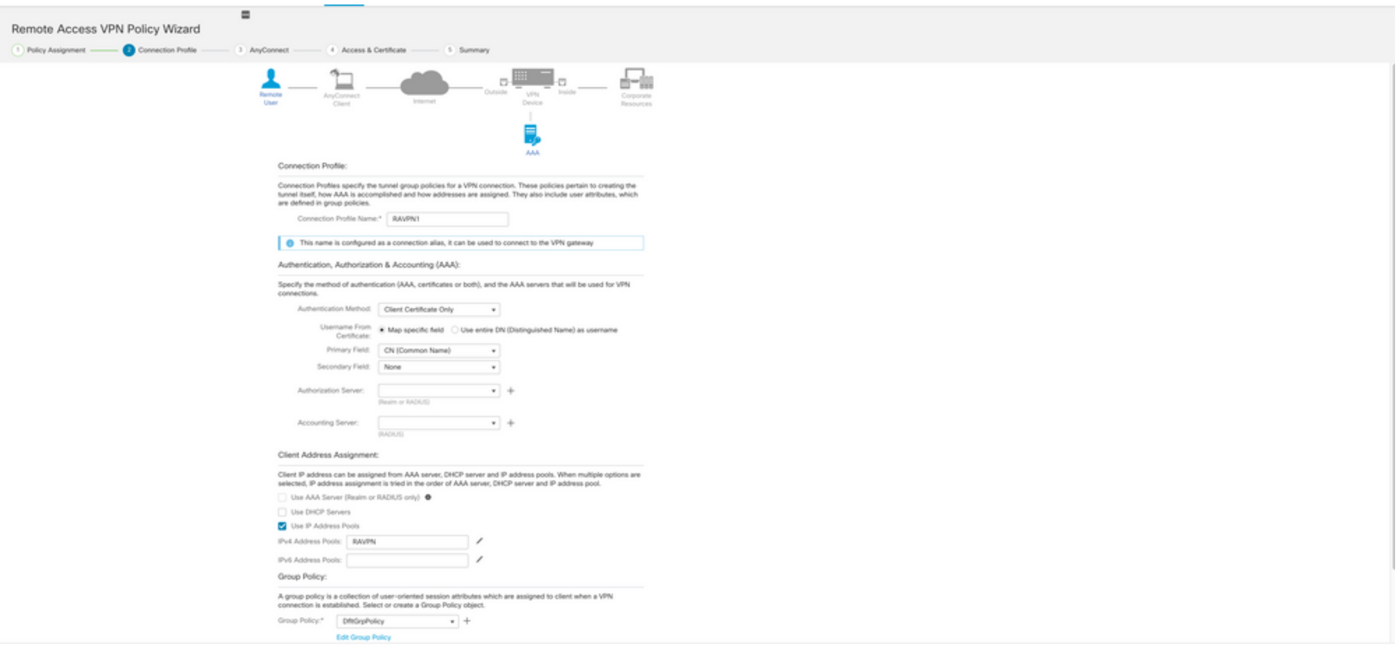
步驟 3.連線配置檔案。

a.命名連線配置檔案。

b.將身份驗證方法設定為「僅客戶端證書」。

c.分配IP地址池，如果需要，建立新的組策略。

d.按一下下一步。



Remote Access VPN Policy Wizard

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:* RAVPN1

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: Client Certificate Only

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

Primary Field: CN (Common Name)

Secondary Field: None

Authorization Server: (Realm or RADIUS)

Accounting Server: (RADIUS)

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 (Realm or RADIUS only)

□ Use DHCP Servers

☑ Use IP Address Pools

IPv4 Address Pools: RAVPN

IPv6 Address Pools:

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:* DfltGrpPolicy

Edit Group Policy

注意：選擇用於輸入身份驗證會話的使用者名稱的主欄位。本指南中使用的是證書的CN。

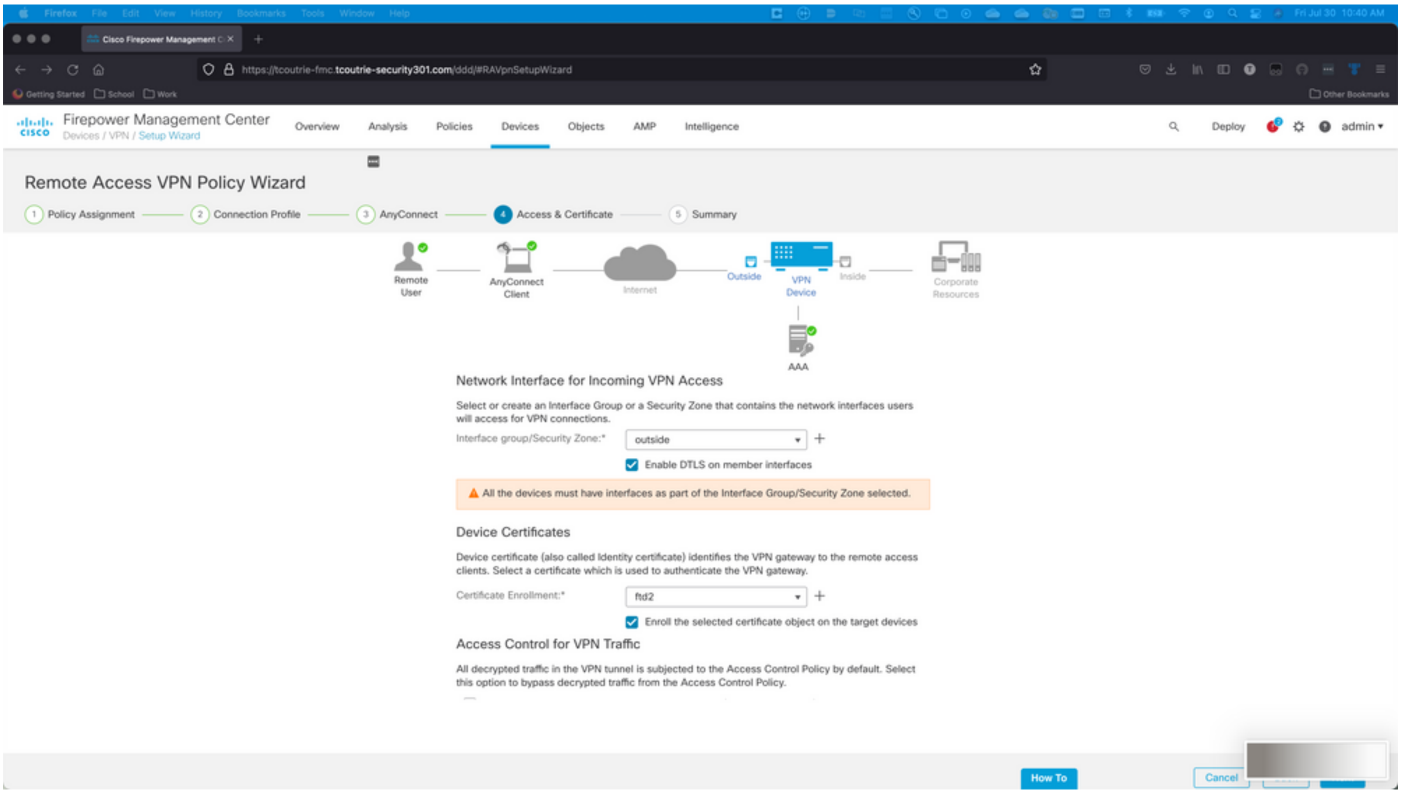
步驟 4.AnyConnect.

將Anyconnect映像新增到裝置。上傳Anyconnect的首選版本，然後按一下Next。

註:Cisco Anyconnect軟體包可以從Software.Cisco.com下載。

步驟 5.Access和Certificate。

將憑證套用到介面並在介面層級啟用Anyconnect，如下圖所示，然後按一下Next。



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* outside

☑ Enable DTLS on member interfaces

All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* ftd2

☑ Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

步驟 6.摘要.

檢查配置。如果所有簽出，請按一下finish，然後deploy。

為移動使用者建立證書

建立要新增到連線中使用的流動裝置的證書。

步驟 1.XCA。

a.開啟XCA

b.啟動新資料庫

步驟 2.建立CSR。

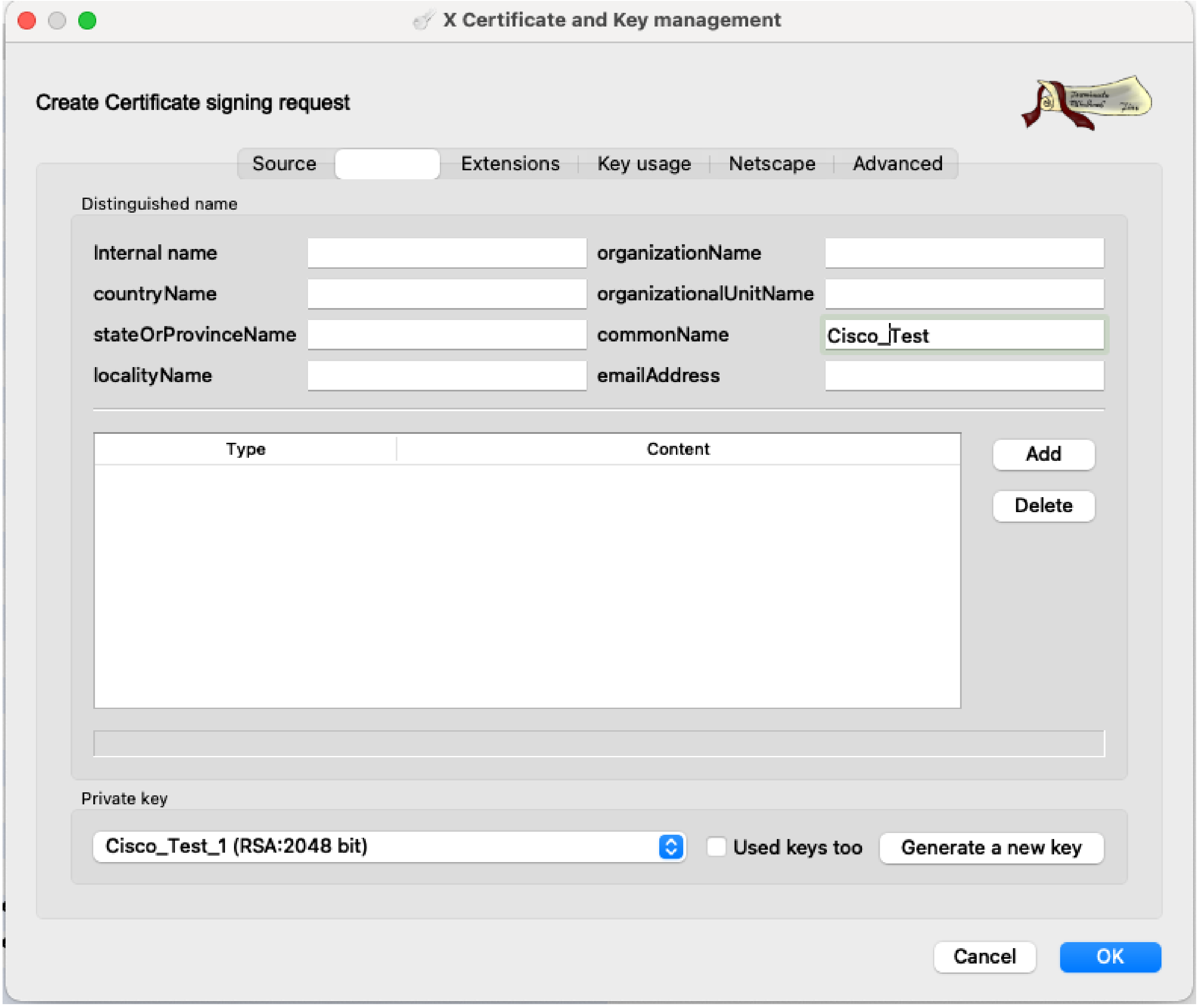
a.選擇Certificate Signing Request(CSR)

b.選擇新請求

c.輸入包含證書所需全部資訊的值

d.生成新金鑰

e.完成後，按一下OK


X Certificate and Key management
Create Certificate signing request
Source
Extensions
Key usage
Netscape
Advanced
Distinguished name

Internal name:
countryName:
stateOrProvinceName:
localityName:
organizationName:
organizationalUnitName:
commonName: Cisco_Test
emailAddress:

Type	Content

Private key: Cisco_Test_1 (RSA:2048 bit)

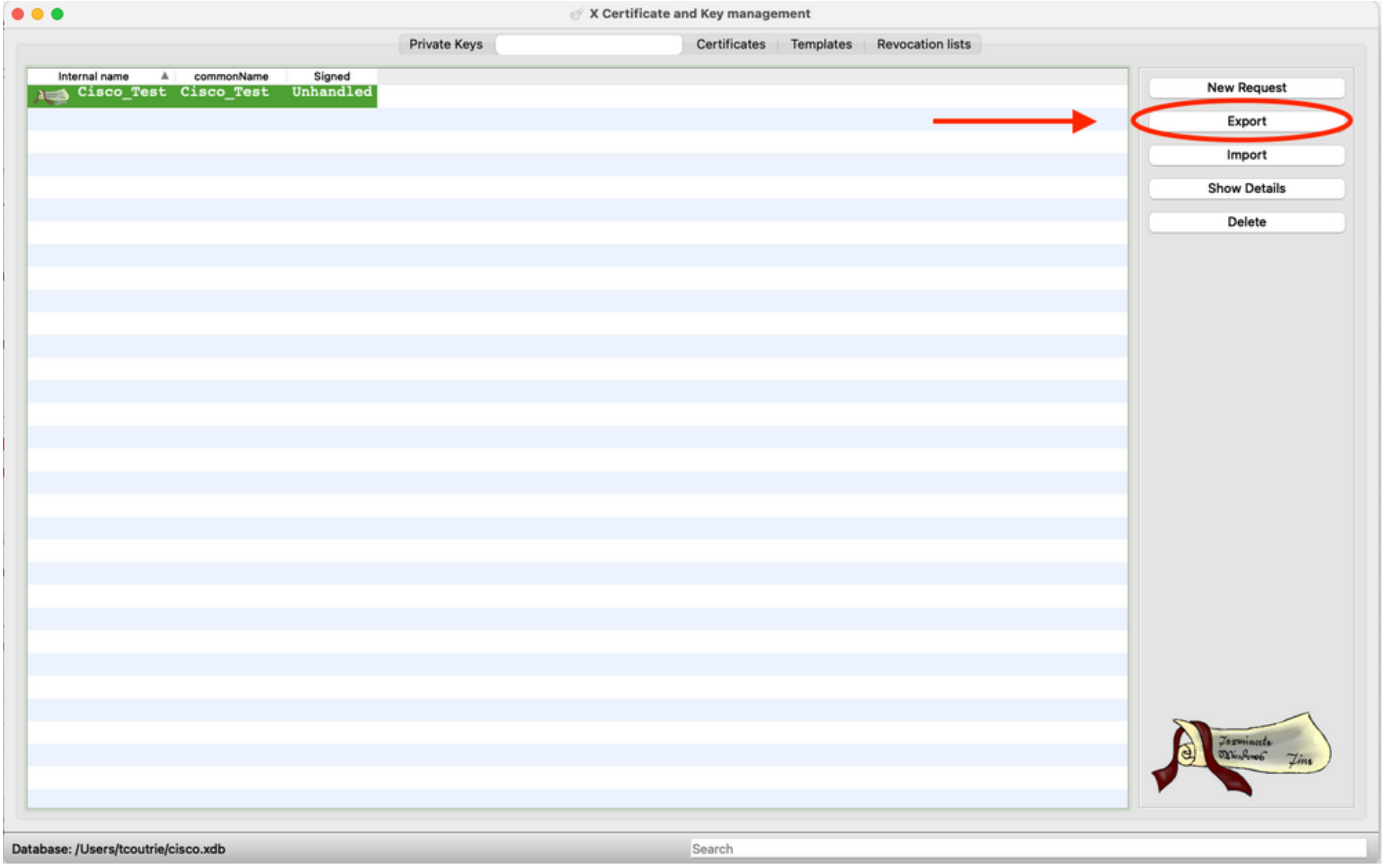
□ Used keys too

註：本檔案使用憑證的CN。

步驟 3.提交CSR。

a.匯出CSR

b.將CSR提交到CA以獲取新證書

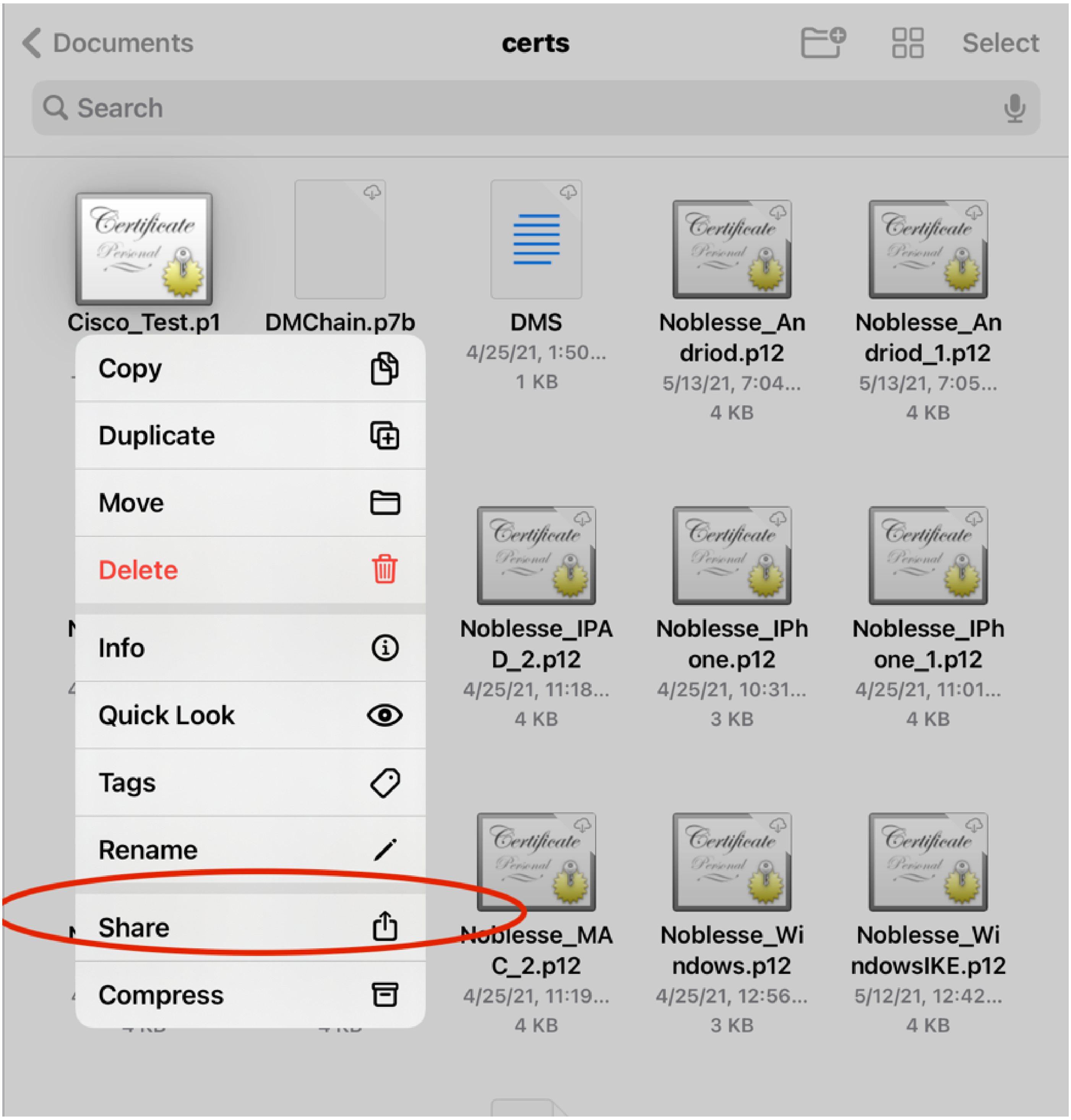


註：使用CSR的PEM格式。

在流動裝置上安裝

步驟 1.將裝置證書新增到流動裝置。
步驟 2.與Anyconnect應用程式共用證書以新增新的證書應用程式。

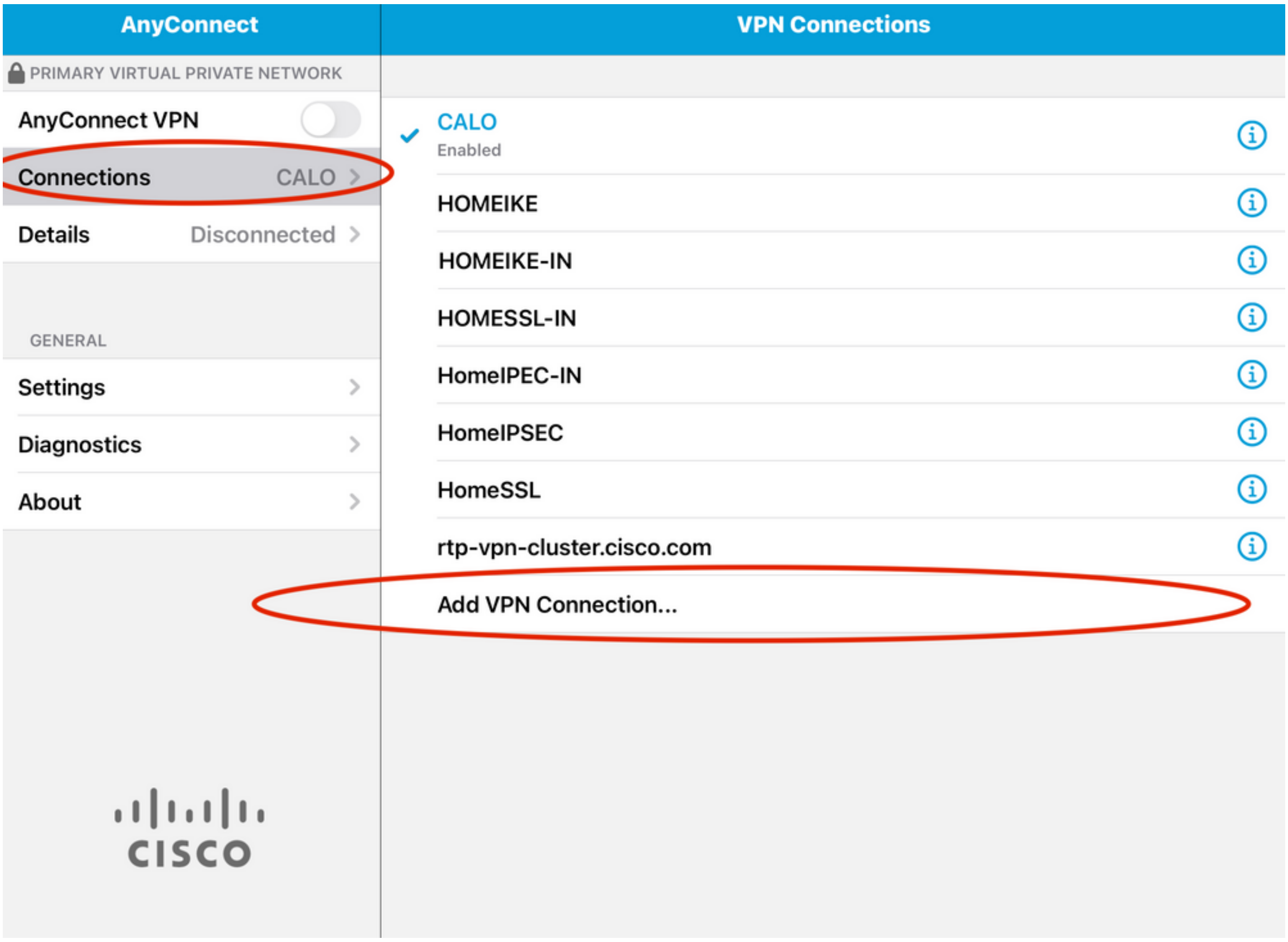
注意：手動安裝需要使用者與應用程式共用證書。這不適用於透過MDM推送的憑證。



步驟 3.輸入PKCS12檔案的證書密碼。

步驟 4.在Anyconnect上建立新連線。

步驟 5.導航到新連線；Connections > Add VPN Connection。



AnyConnect

PRIMARY VIRTUAL PRIVATE NETWORK

AnyConnect VPN

Connections CALO

Details Disconnected

GENERAL

Settings

Diagnostics

About

VPN Connections

✓ CALO
Enabled

HOMEIKE

HOMEIKE-IN

HOMESSL-IN

HomeIPEC-IN

HomeIPSEC

HomeSSL

rtp-vpn-cluster.cisco.com

Add VPN Connection...

步驟 6.輸入新連線的資訊。

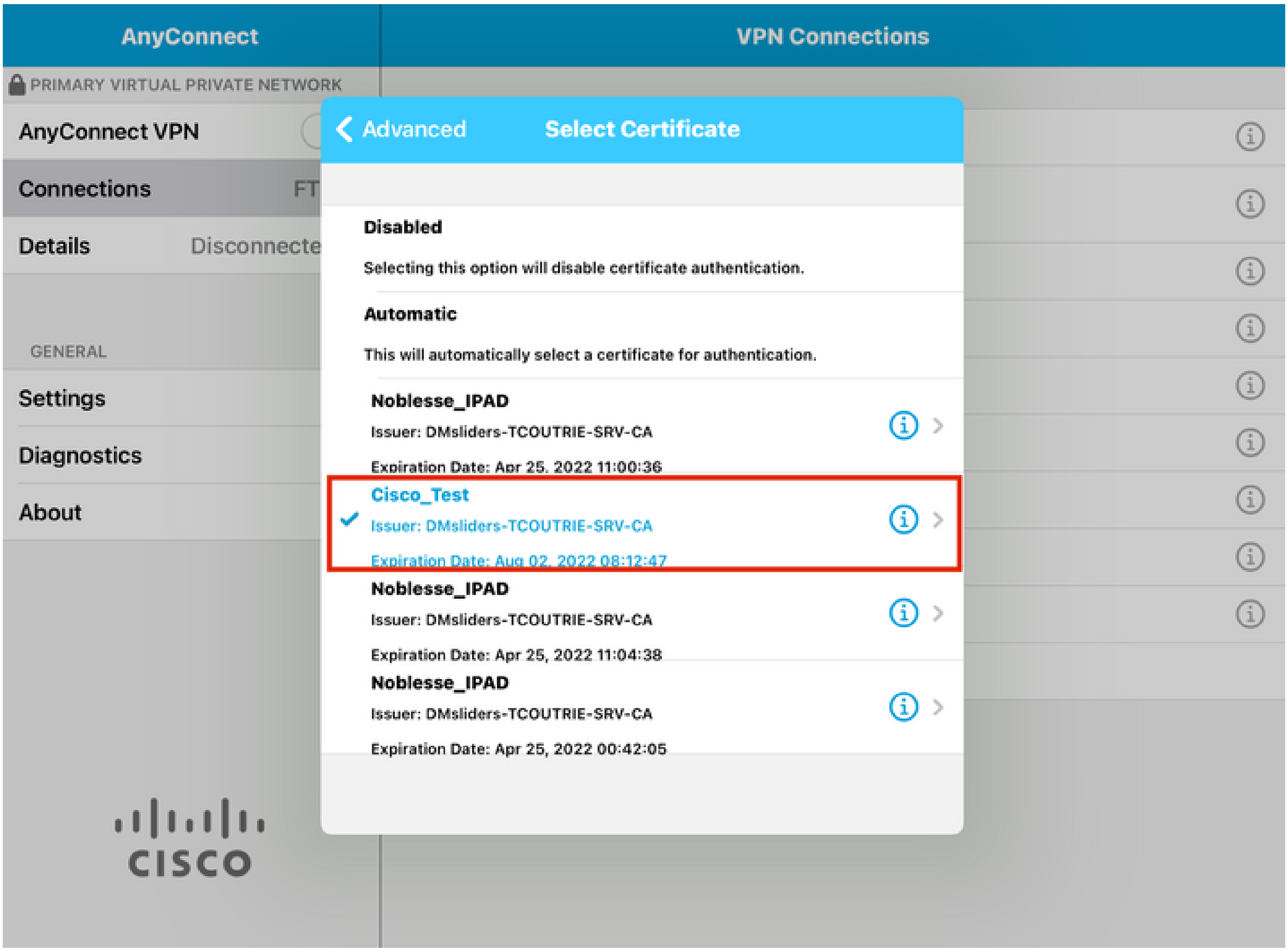
說明：為連線命名

伺服器地址： IP地址或FTD的FQDN

高級：其他配置

步驟 7.選擇Advanced。

步驟 8.選擇「Certificate」，然後選擇您新增的憑證。



AnyConnect

VPN Connections

PRIMARY VIRTUAL PRIVATE NETWORK

AnyConnect VPN

Connections FT

Details Disconnecte

GENERAL

Settings

Diagnostics

About

Advanced

Select Certificate

Disabled

Selecting this option will disable certificate authentication.

Automatic

This will automatically select a certificate for authentication.

Noblesse_IPAD
Issuer: DMsliders-TCOUTRIE-SRV-CA
Expiration Date: Apr 25, 2022 11:00:36

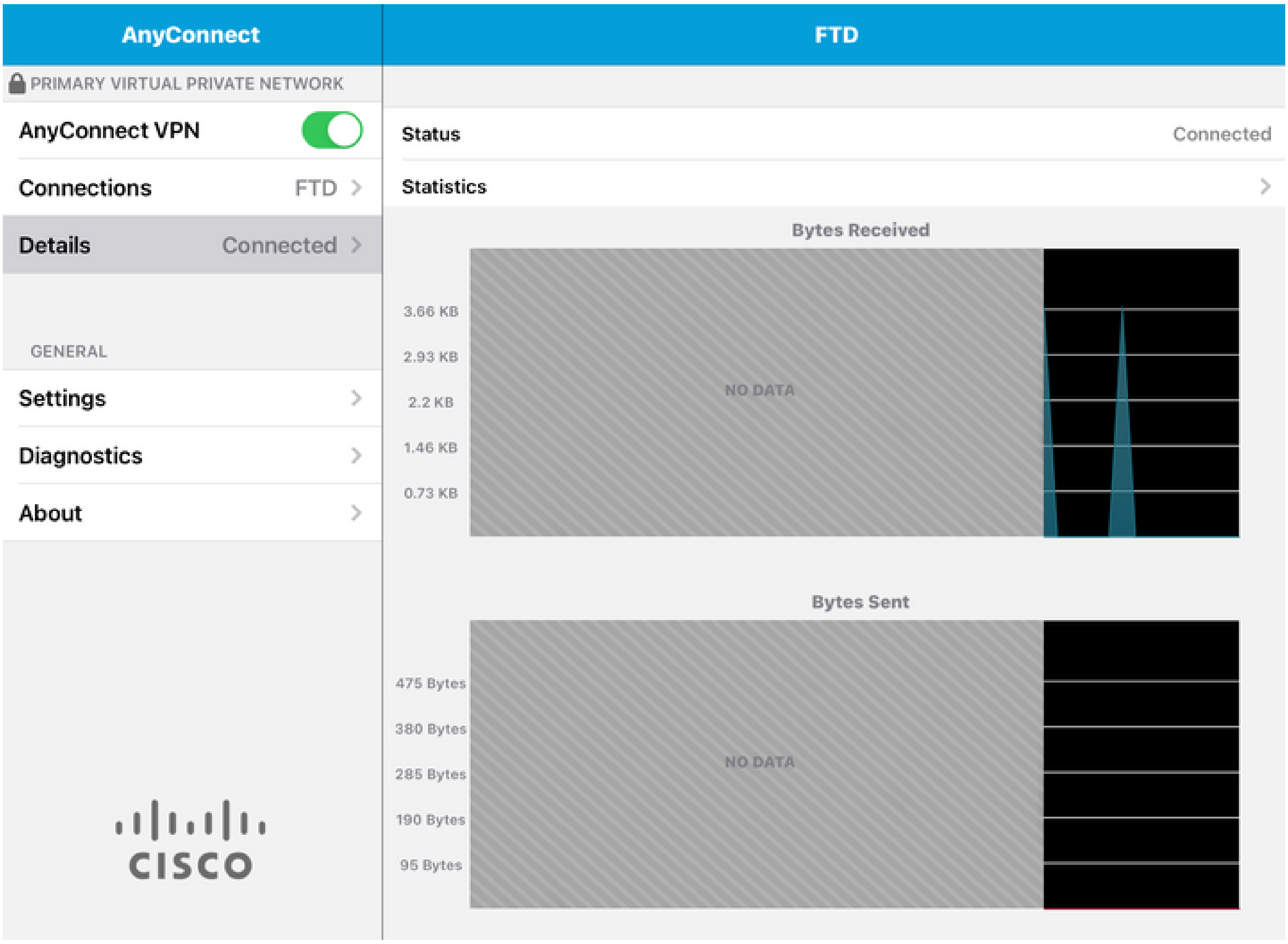
✓ **Cisco_Test**
Issuer: DMsliders-TCOUTRIE-SRV-CA
Expiration Date: Aug 02, 2022 08:12:47

Noblesse_IPAD
Issuer: DMsliders-TCOUTRIE-SRV-CA
Expiration Date: Apr 25, 2022 11:04:38

Noblesse_IPAD
Issuer: DMsliders-TCOUTRIE-SRV-CA
Expiration Date: Apr 25, 2022 00:42:05

步驟 9.導覽回Connections並進行測試。

一旦成功，切換將開啟，詳細資訊將顯示為已連線。



驗證

命令show vpn-sessiondb detail Anyconnect顯示有關所連線主機的所有資訊。

提示：進一步篩選此命令的選項是新增到命令中的「filter」或「sort」關鍵字。

舉例來說：

```
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
```

疑難排解

調試

解決此問題所需的調試是：

```
Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255
```

如果連線是IPSEC而不是SSL:

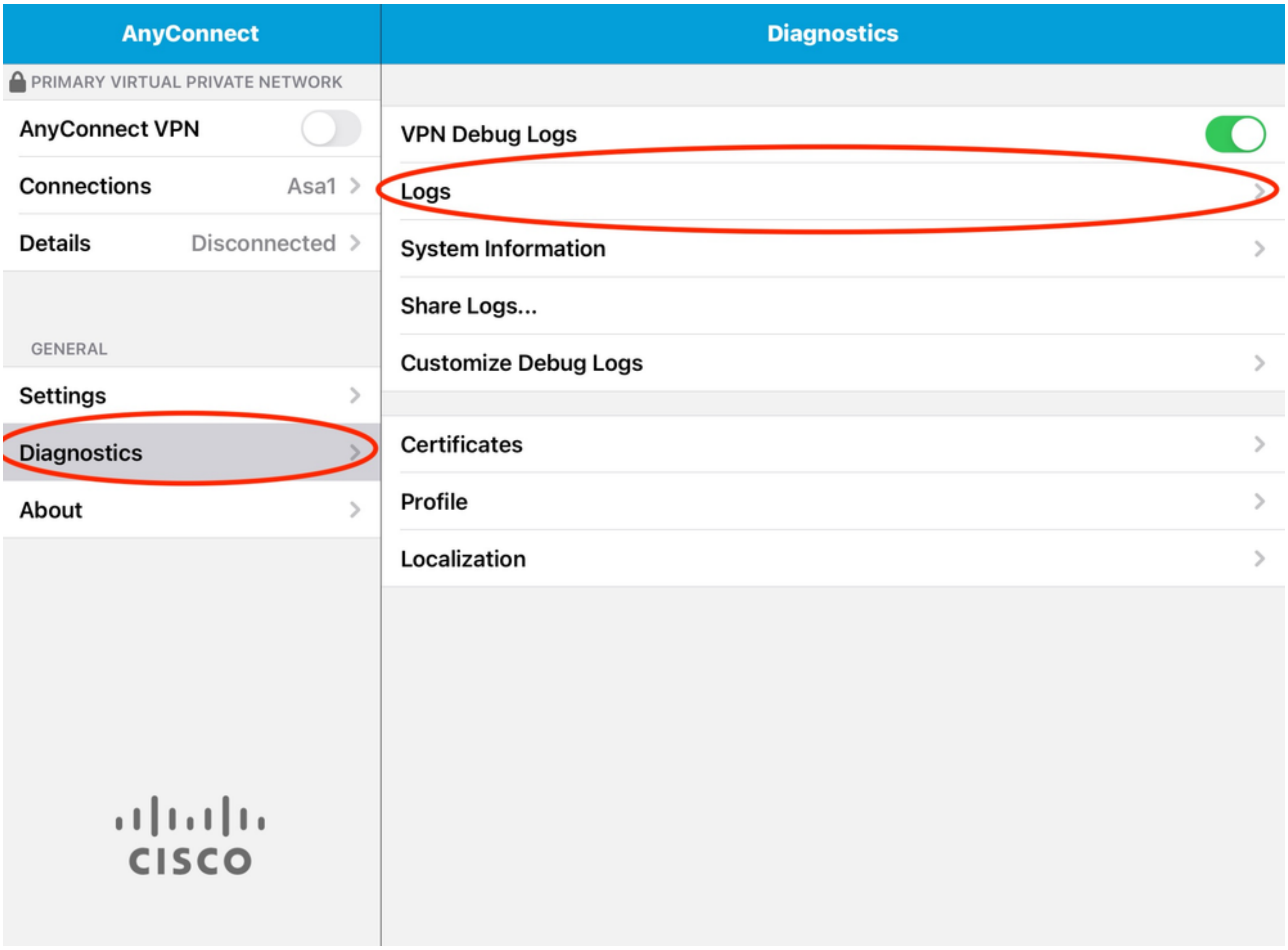
```
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14
```

來自Anyconnect移動應用程式的日誌：

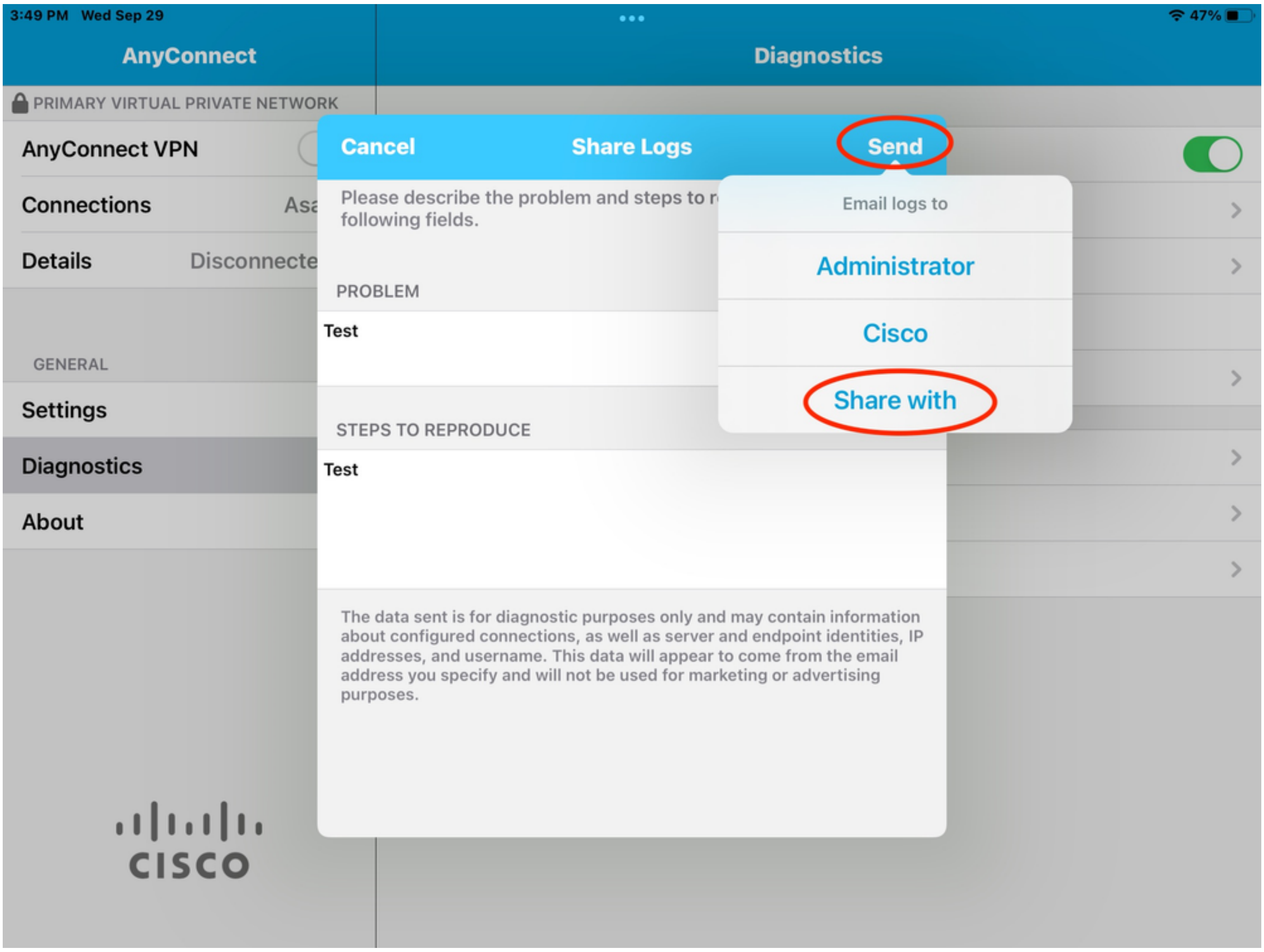
導航到Diagnostic > VPN Debug Logs > Share log。



輸入以下資訊：

- 問題
- 複製步驟

然後導覽至Send > Share with。



3:49 PM Wed Sep 29

47%

AnyConnect

Diagnostics

PRIMARY VIRTUAL PRIVATE NETWORK

AnyConnect VPN

Connections Asa

Details Disconnecte

GENERAL

Settings

Diagnostics

About

Cancel Share Logs Send

Please describe the problem and steps to r
following fields.

PROBLEM

Test

STEPS TO REPRODUCE

Test

The data sent is for diagnostic purposes only and may contain information about configured connections, as well as server and endpoint identities, IP addresses, and username. This data will appear to come from the email address you specify and will not be used for marketing or advertising purposes.

Email logs to

Administrator

Cisco

Share with

此選項提供使用電子郵件客戶端傳送日誌的選項。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。