

# 为移动访问配置基于Anyconnect证书的身份验证

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[在FTD上配置Cisco Anyconnect](#)

[网络图](#)

[向FTD添加证书](#)

[配置Cisco Anyconnect](#)

[为移动用户创建证书](#)

[在移动设备上安装](#)

[验证](#)

[故障排除](#)

[调试](#)

---

## 简介

本文档介绍在移动设备上实施基于证书的身份验证的示例。

## 先决条件

本指南中使用的工具和设备包括：

- 思科Firepower威胁防御(FTD)
- Firepower Management Center (FMC)
- Apple iOS设备(iPhone、iPad)
- 证书颁发机构 (CA)
- Cisco Anyconnect客户端软件

## 要求

Cisco 建议您了解以下主题：

- 基本VPN
- SSL/TLS
- 公钥基础设施
- 使用FMC的经验
- OpenSSL
- Cisco Anyconnect

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

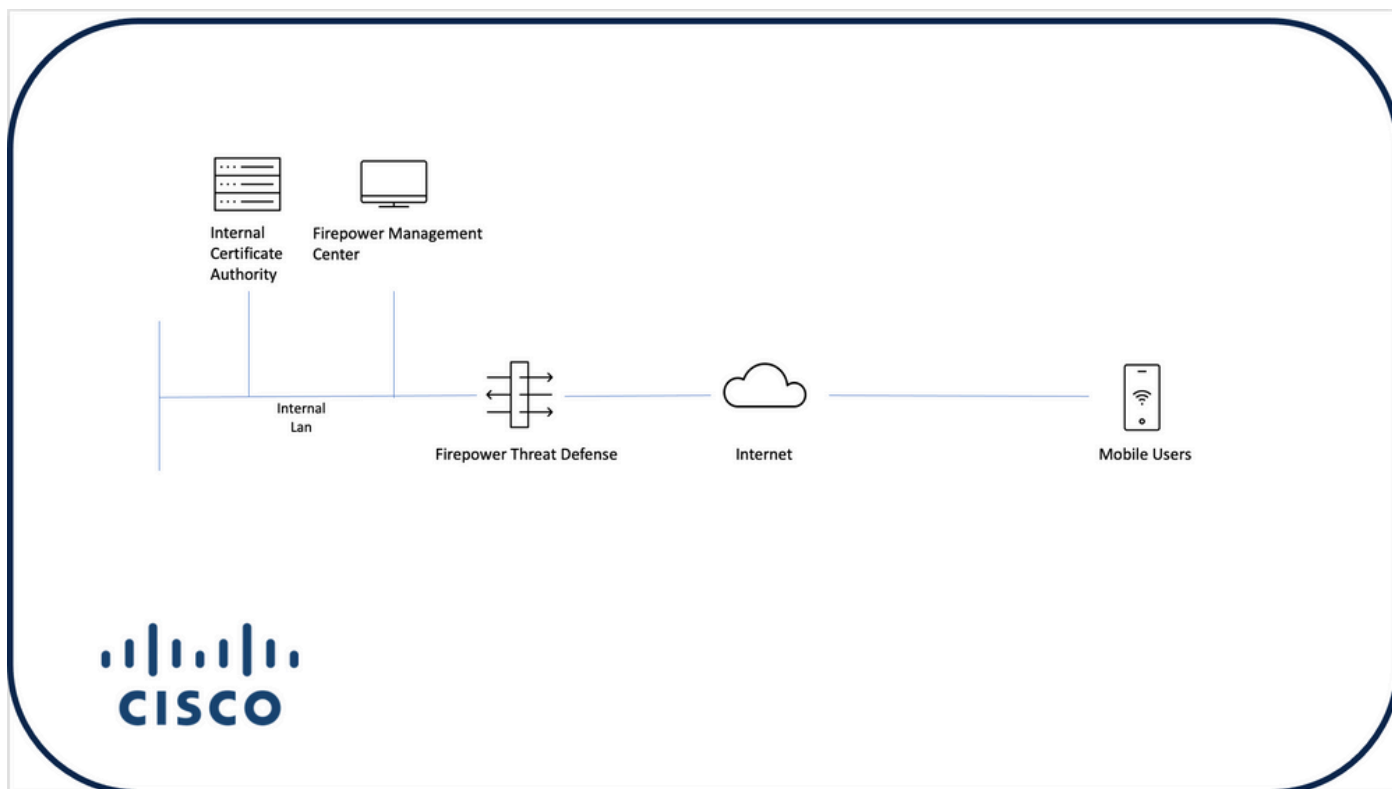
- 思科FTD
- 思科FMC
- Microsoft CA服务器
- XCA
- Cisco Anyconnect
- Apple ipad

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 在FTD上配置Cisco Anyconnect

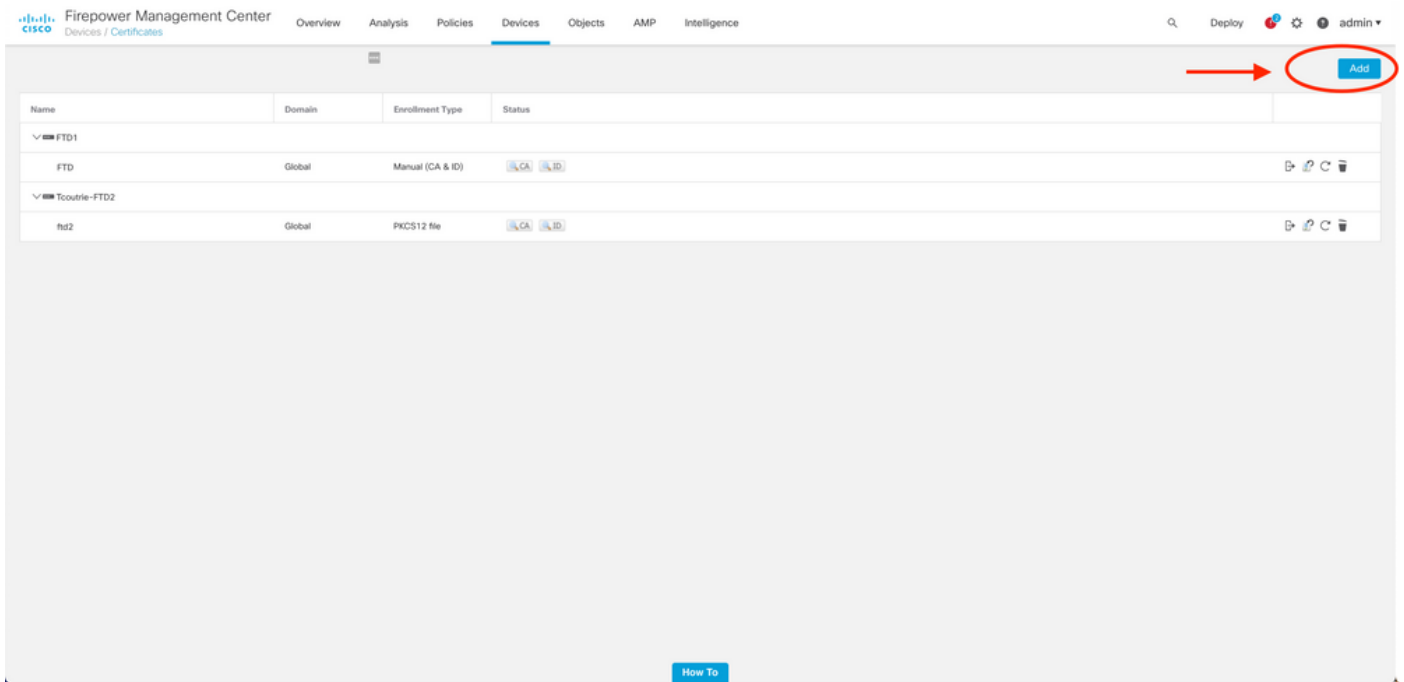
本节介绍通过FMC配置Anyconnect的步骤。开始之前，请务必部署所有配置。

### 网络图

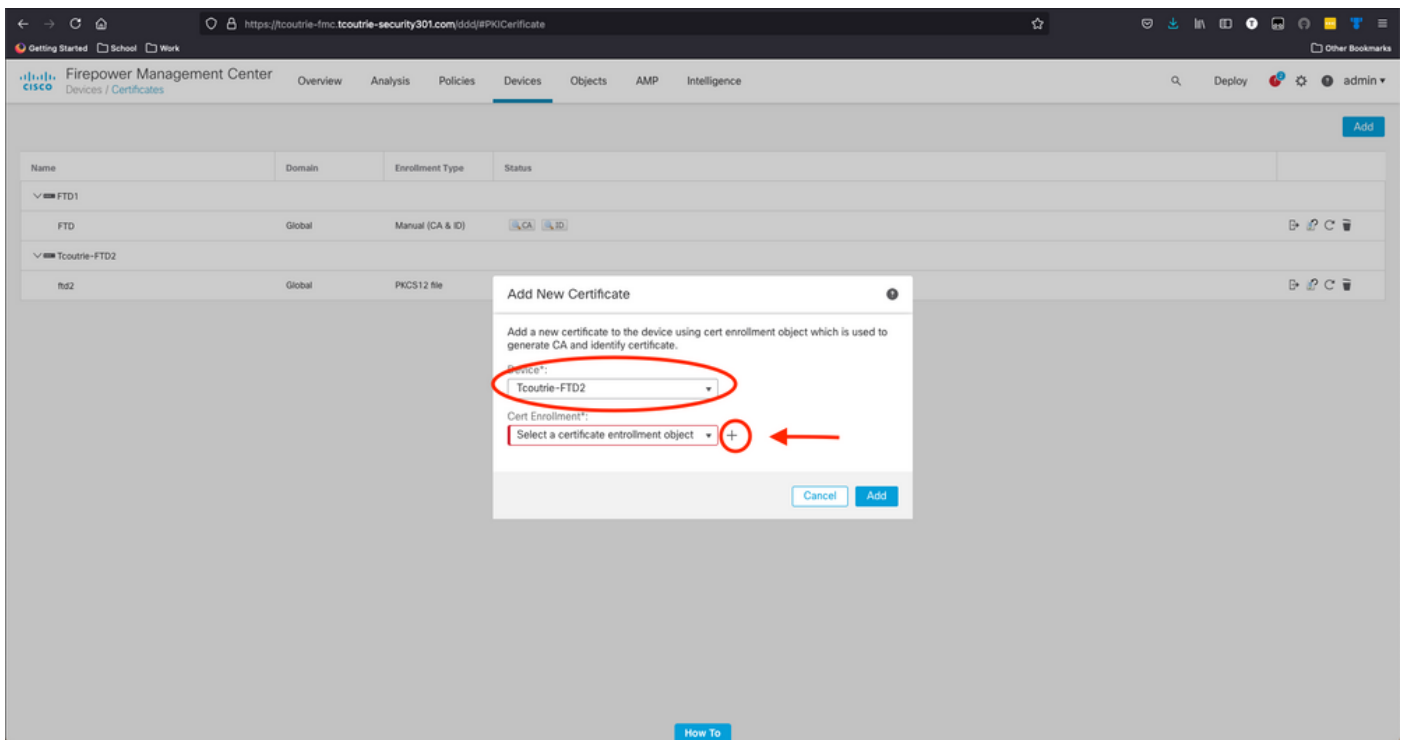


### 向FTD添加证书


步骤1:在FMC设备上为FTD创建证书。导航到设备>证书，然后选择添加，如下图所示：



第二步：选择VPN连接所需的FTD。从devices下拉列表中选择FTD设备。单击+图标可添加新的证书注册方法，如下图所示：



第三步：将证书添加到设备。选择在环境中获取证书的首选方法。

 提示：可用选项包括：自签名证书 — 本地生成新证书、SCEP — 使用简单证书注册协议从CA获取证书、手动 — 手动安装根和身份证书、PKCS12 — 上传包含根、身份和私钥的加密证书捆绑包。

第四步：将证书上传到FTD设备。输入密码（仅限PKCS12）并单击Save，如下图所示：

**Add Cert Enrollment**

Name\*  
ftdcert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File\*: Tcoutrie-ftd2.p12 [Browse PKCS12 File](#)

Passphrase: .....

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

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

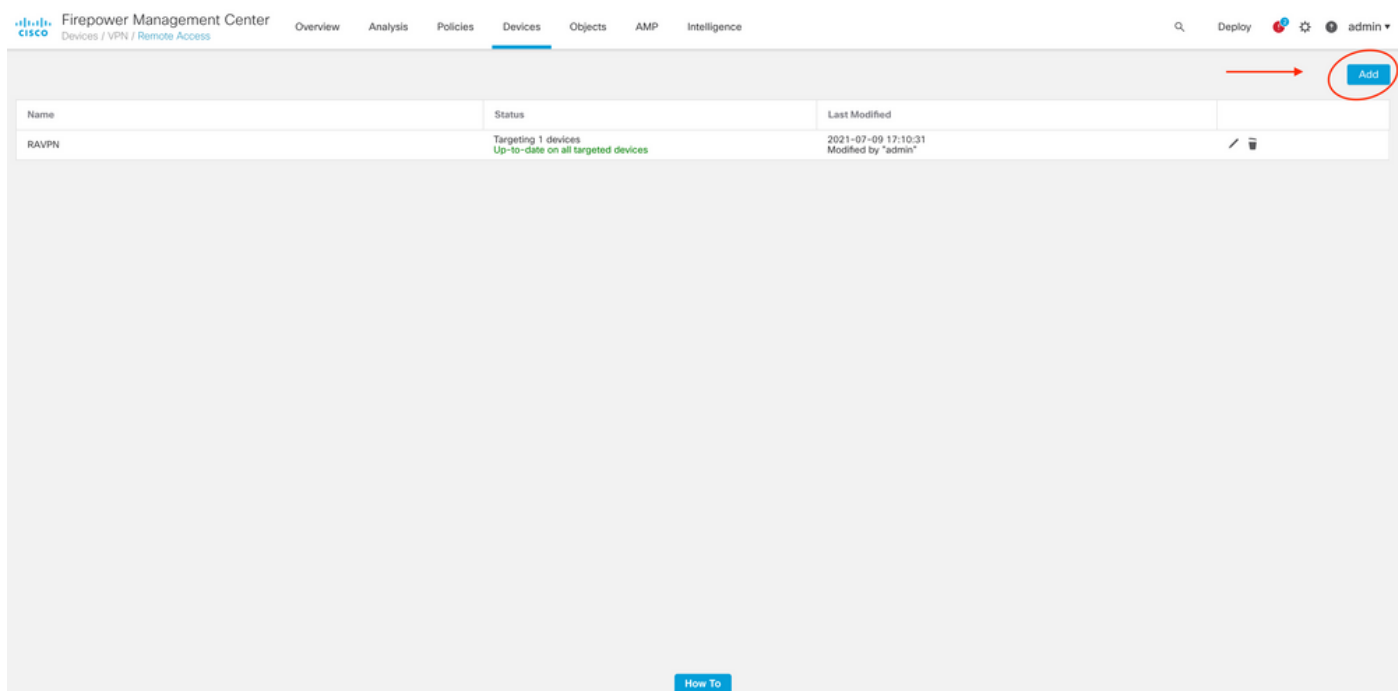
注意：保存文件后，立即部署证书。要查看证书详细信息，请选择ID。

## 配置Cisco Anyconnect

使用远程访问向导通过FMC配置Anyconnect。

步骤1:启动远程访问VPN策略向导以配置Anyconnect。

导航到设备>远程访问，然后选择添加。



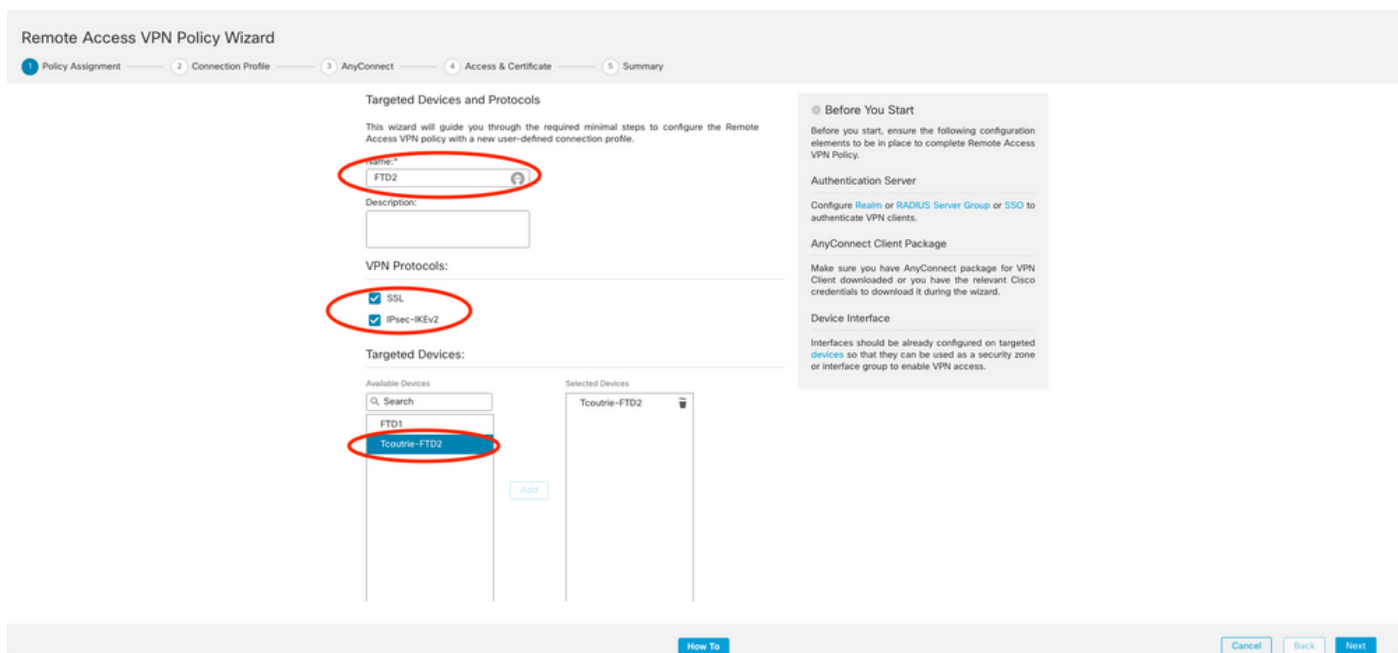
第二步：策略分配。

完成策略分配：

a.命名策略。

b.选择所需的VPN协议。

c.选择要应用配置的目标设备。



第三步：连接配置文件。

a.命名连接配置文件。

b.将身份验证方法设置为Client Certificate Only。

c.分配IP地址池，如果需要，创建新的组策略。

d.单击下一步。

Remote Access VPN Policy Wizard

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

Service User AnyConnect Client Internet VPN Gateway VPN Device Corporate Resources 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 assignments 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](#)

注意：选择要用于输入身份验证会话的用户名的主字段。本指南中使用了证书的CN。

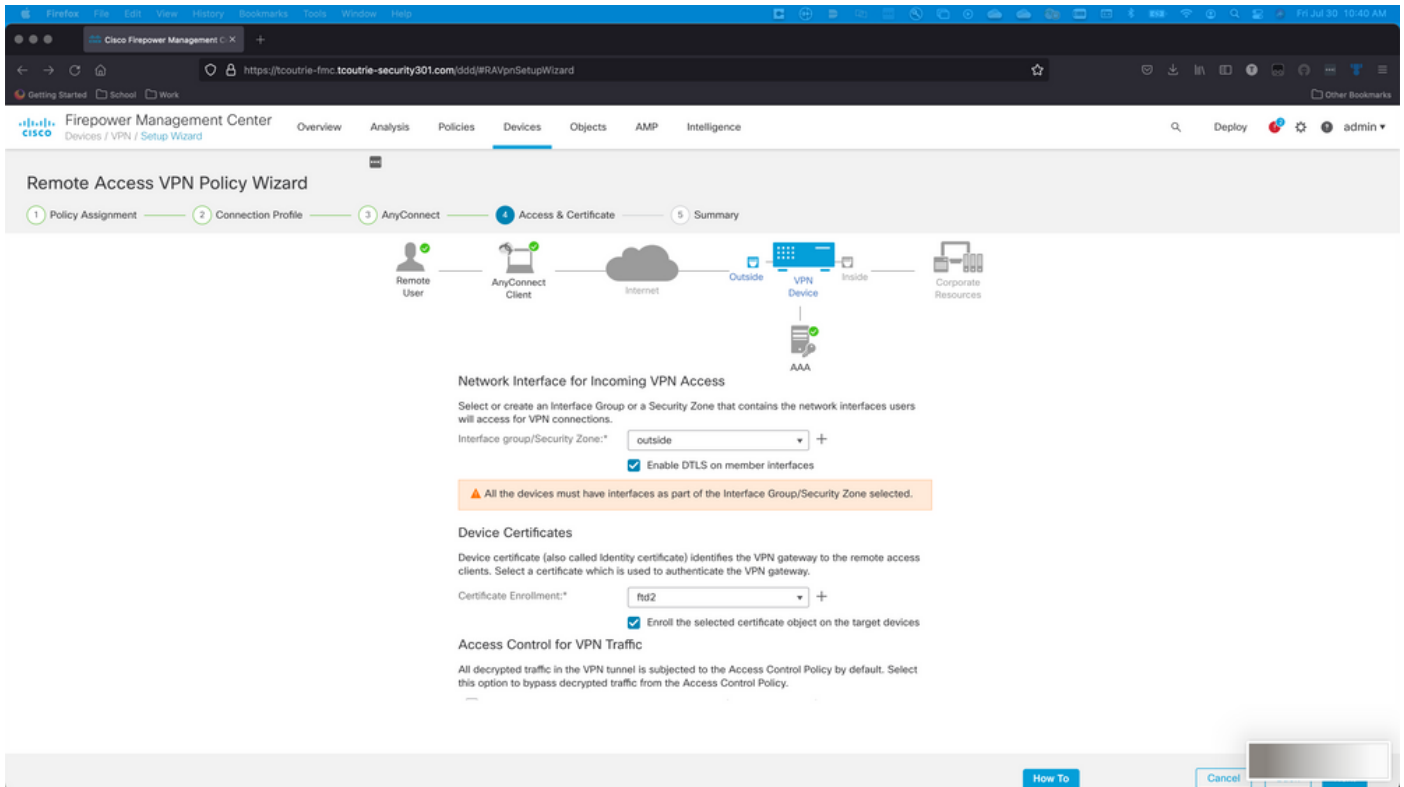
第四步：AnyConnect.

将Anyconnect映像添加到设备。上传Anyconnect的首选版本，然后单击Next。

注意：Cisco Anyconnect软件包可以从Software.Cisco.com下载。

第五步：访问和证书。

将证书应用到接口并在接口级别启用Anyconnect（如图所示），然后单击Next。



第六步：摘要。

检查配置。如果所有签出，请单击finish，然后单击deploy。

## 为移动用户创建证书

创建要添加到连接中使用的移动设备的证书。

步骤1:XCA。

a.打开XCA

b.启动新数据库

第二步：创建CSR

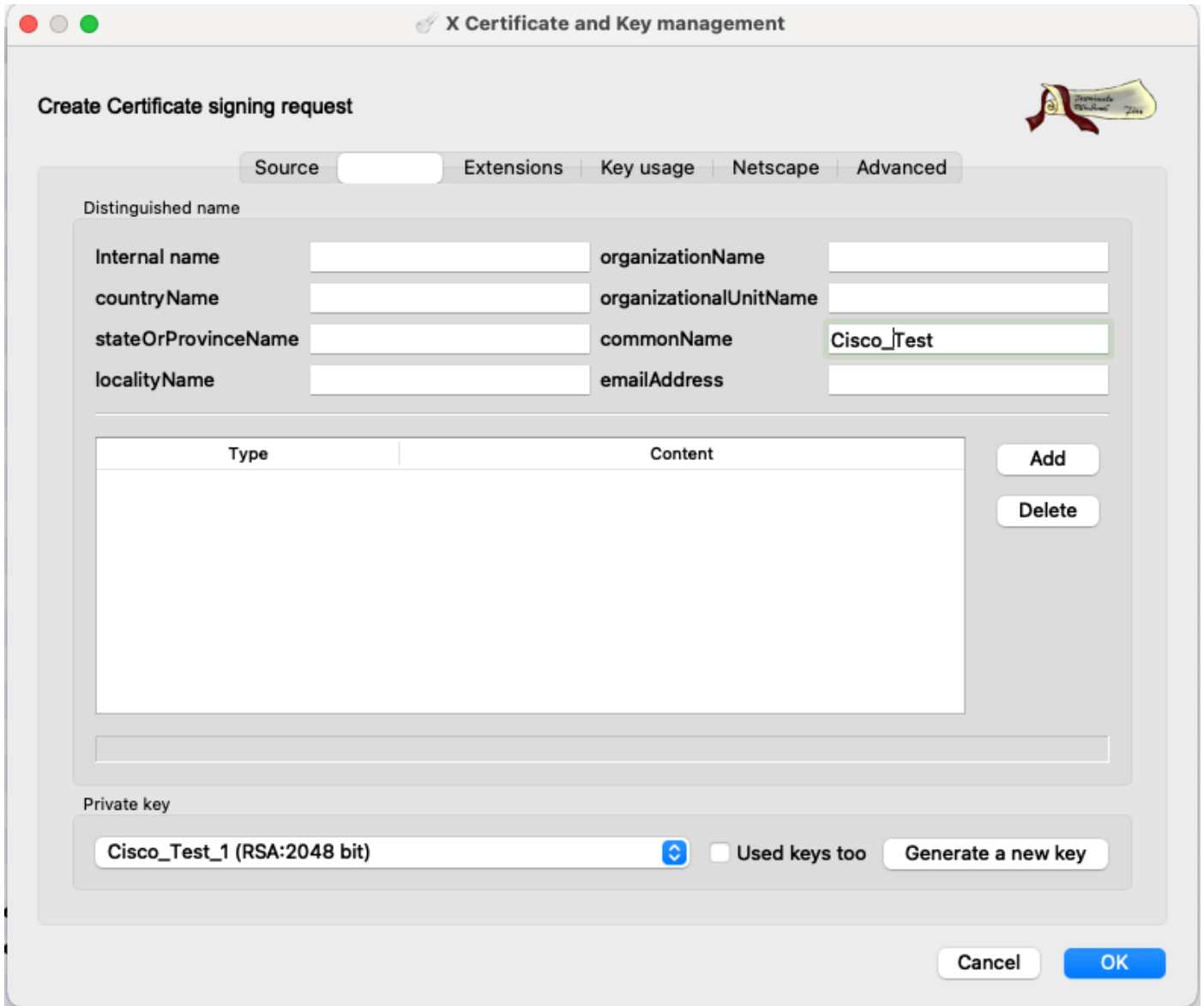
a.选择证书签名请求(CSR)


b.选择New Request

c.输入包含证书所需全部信息的值

d.生成新密钥

e.完成后，单击OK



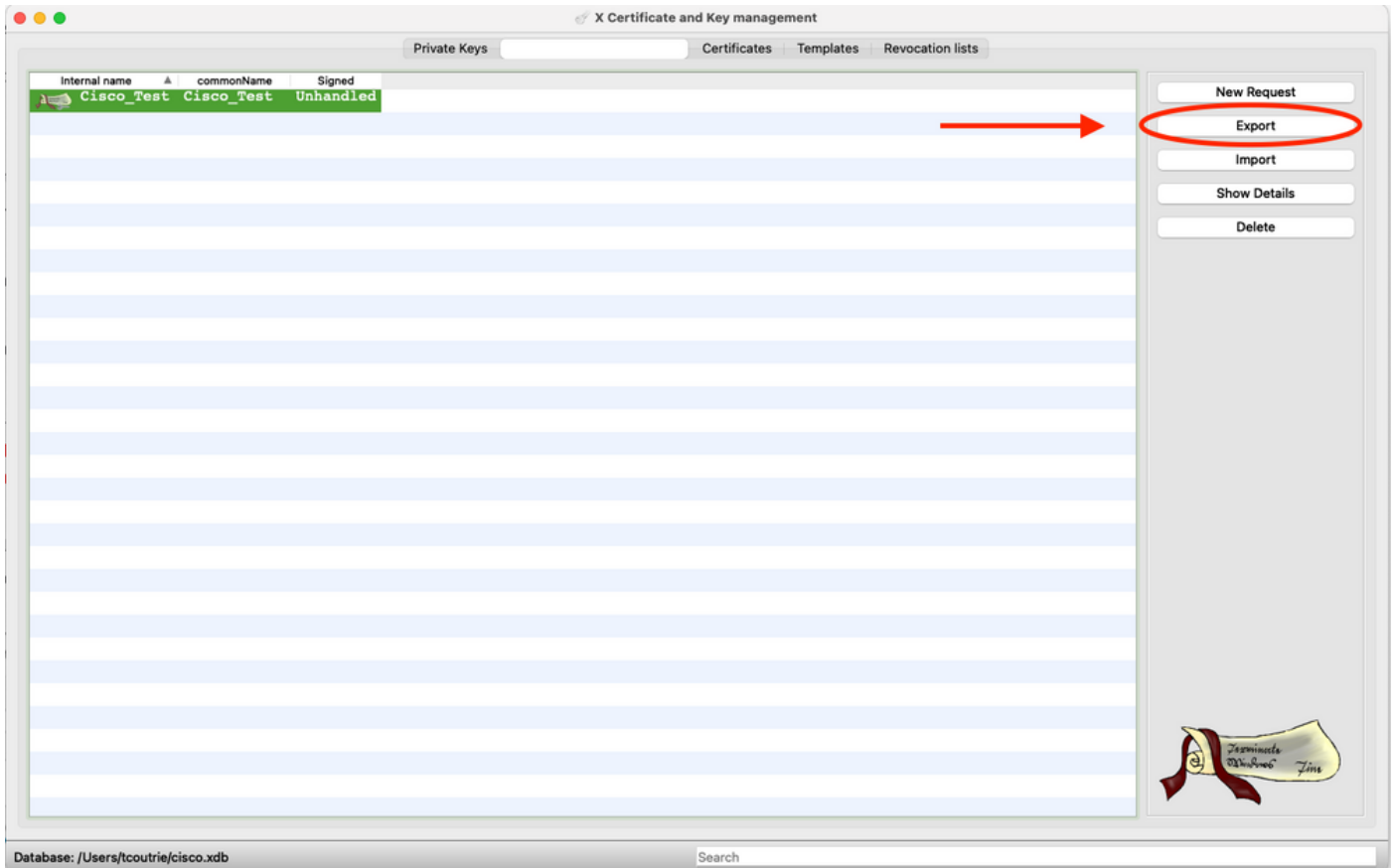
 注：本文档使用证书的CN。

第三步：提交企业社会责任。

a.导出CSR

b.向CA提交CSR以获取新证书






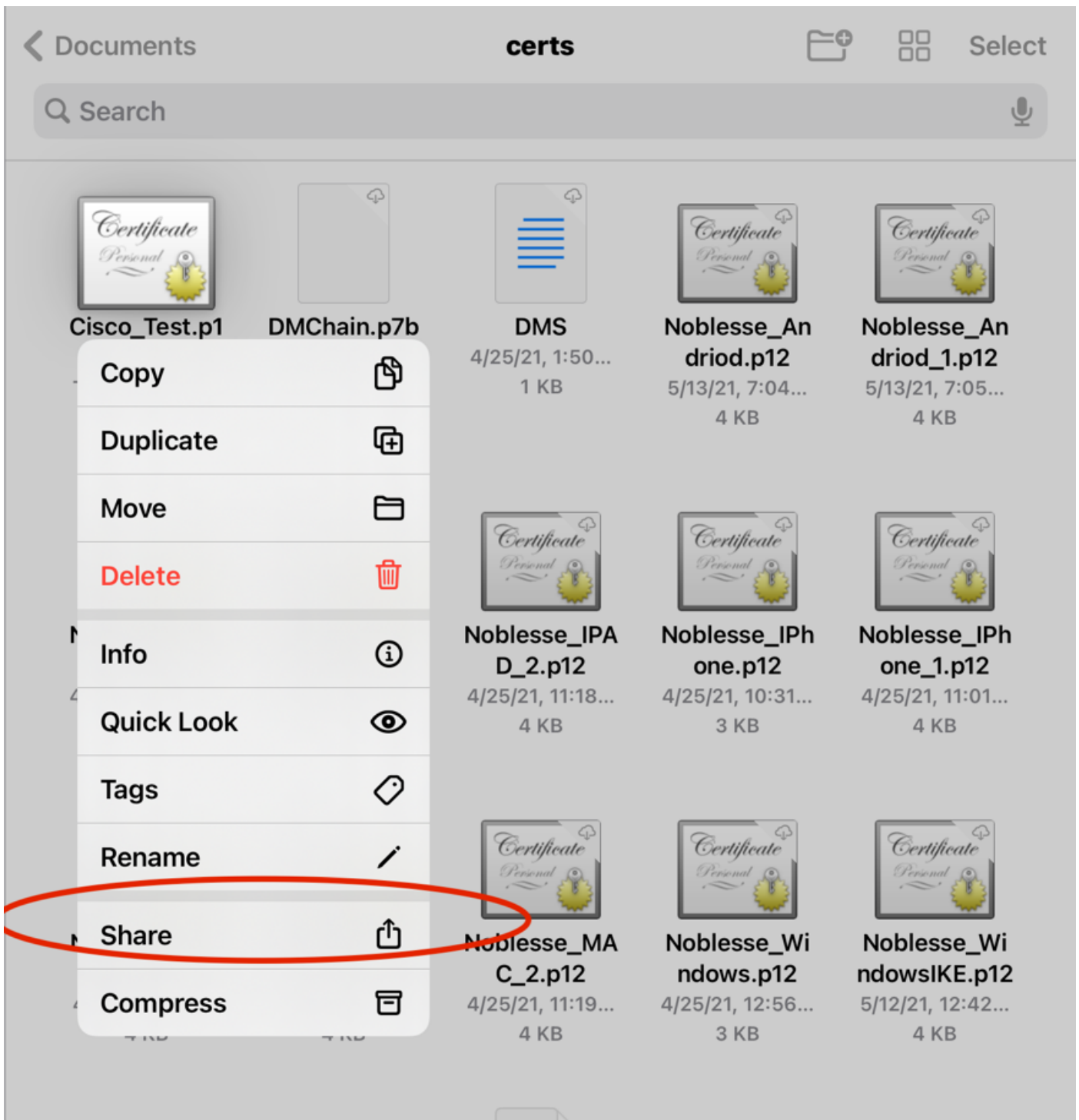
 注：使用CSR的PEM格式。

## 在移动设备上安装

步骤1:将设备证书添加到移动设备。

第二步：与Anyconnect应用共享证书以添加新的证书应用。

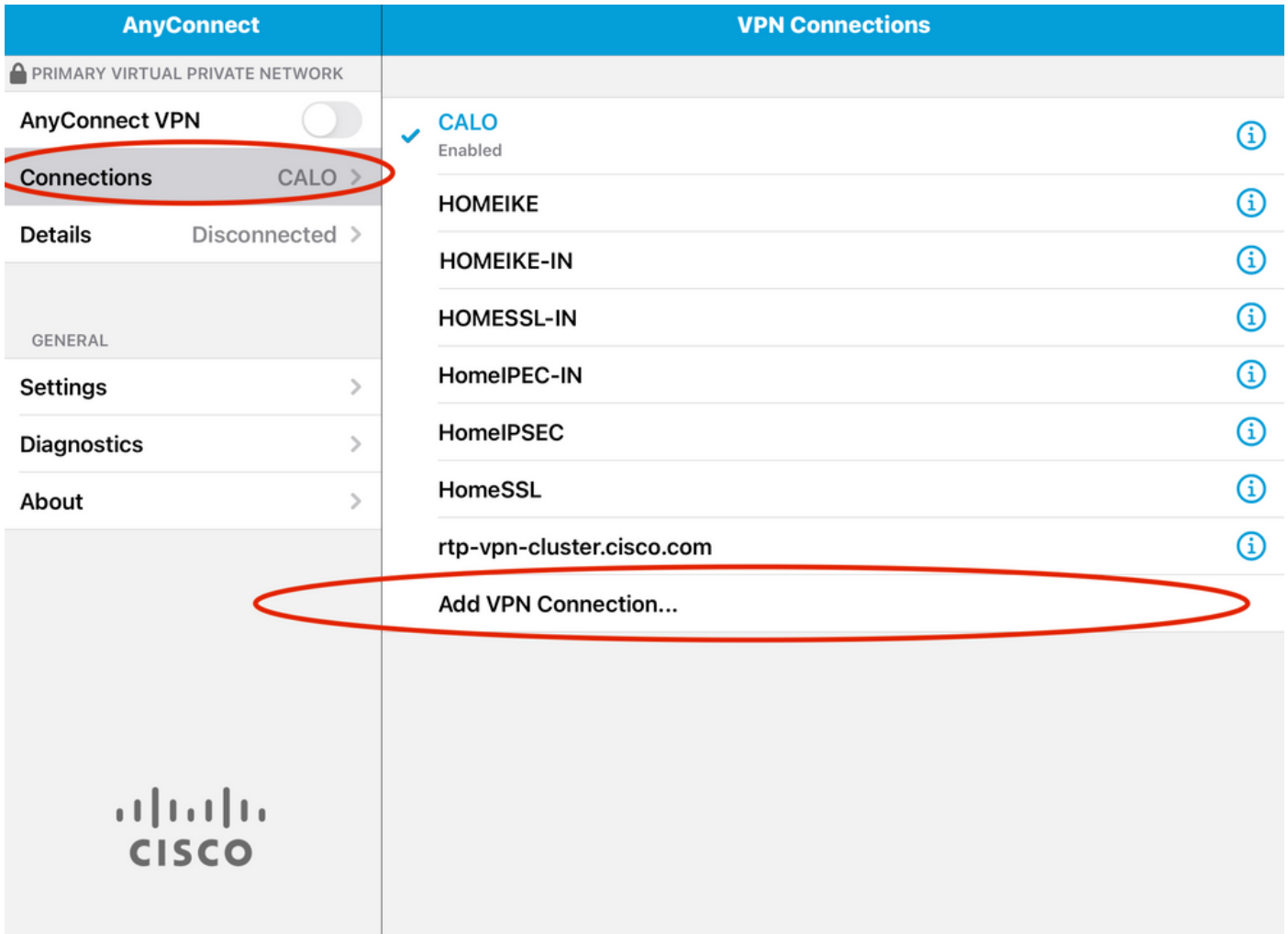
 注意：手动安装需要用户与应用程序共享证书。这不适用于通过MDM推送的证书。



第三步：输入PKCS12文件的证书密码。

第四步：在Anyconnect上创建新连接。

第五步：导航到新连接；Connections > Add VPN Connection。



第六步：输入新连接的信息。

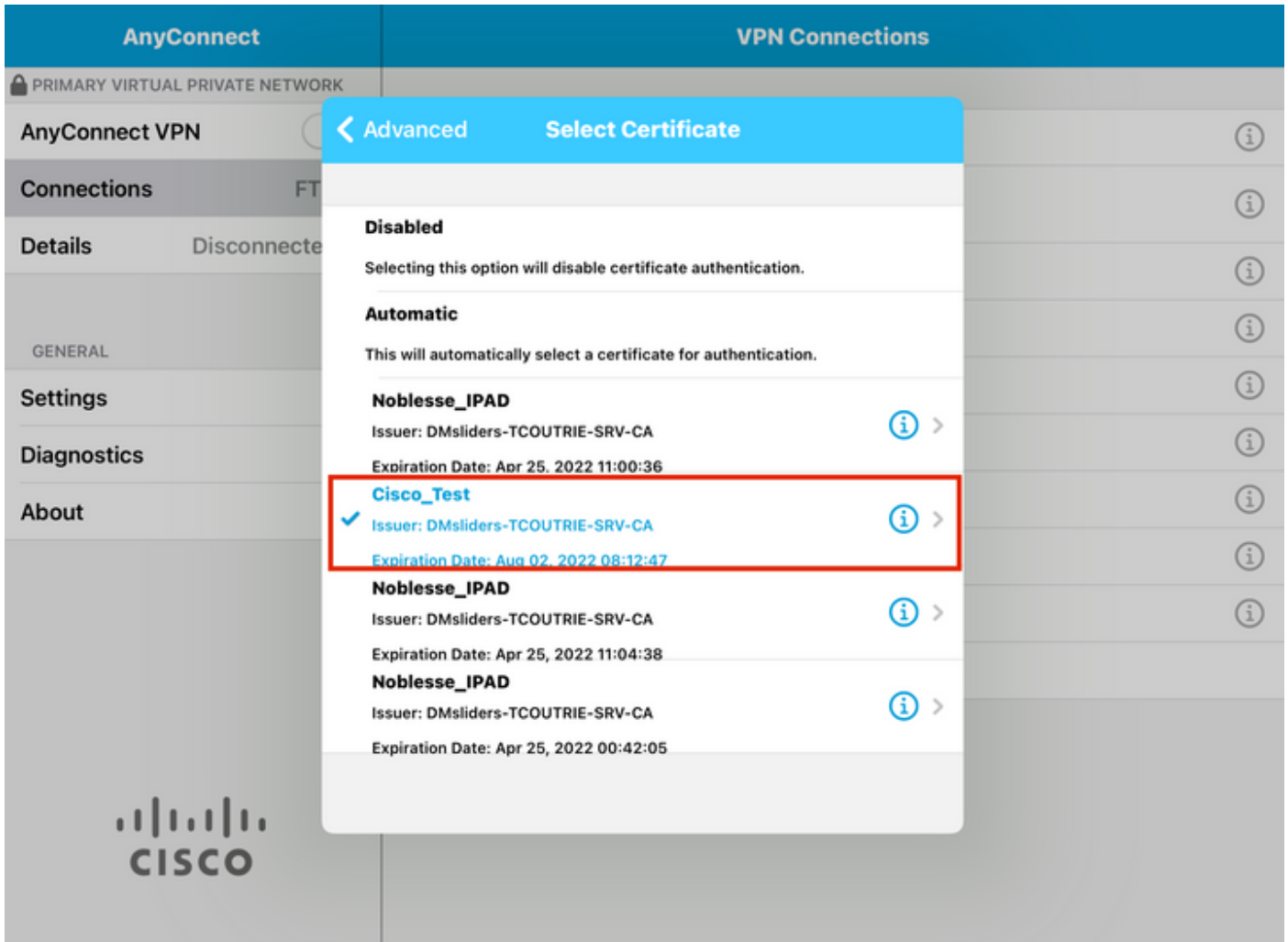
Description：为连接命名

服务器地址：IP地址或FQDN FTD

高级：其他配置

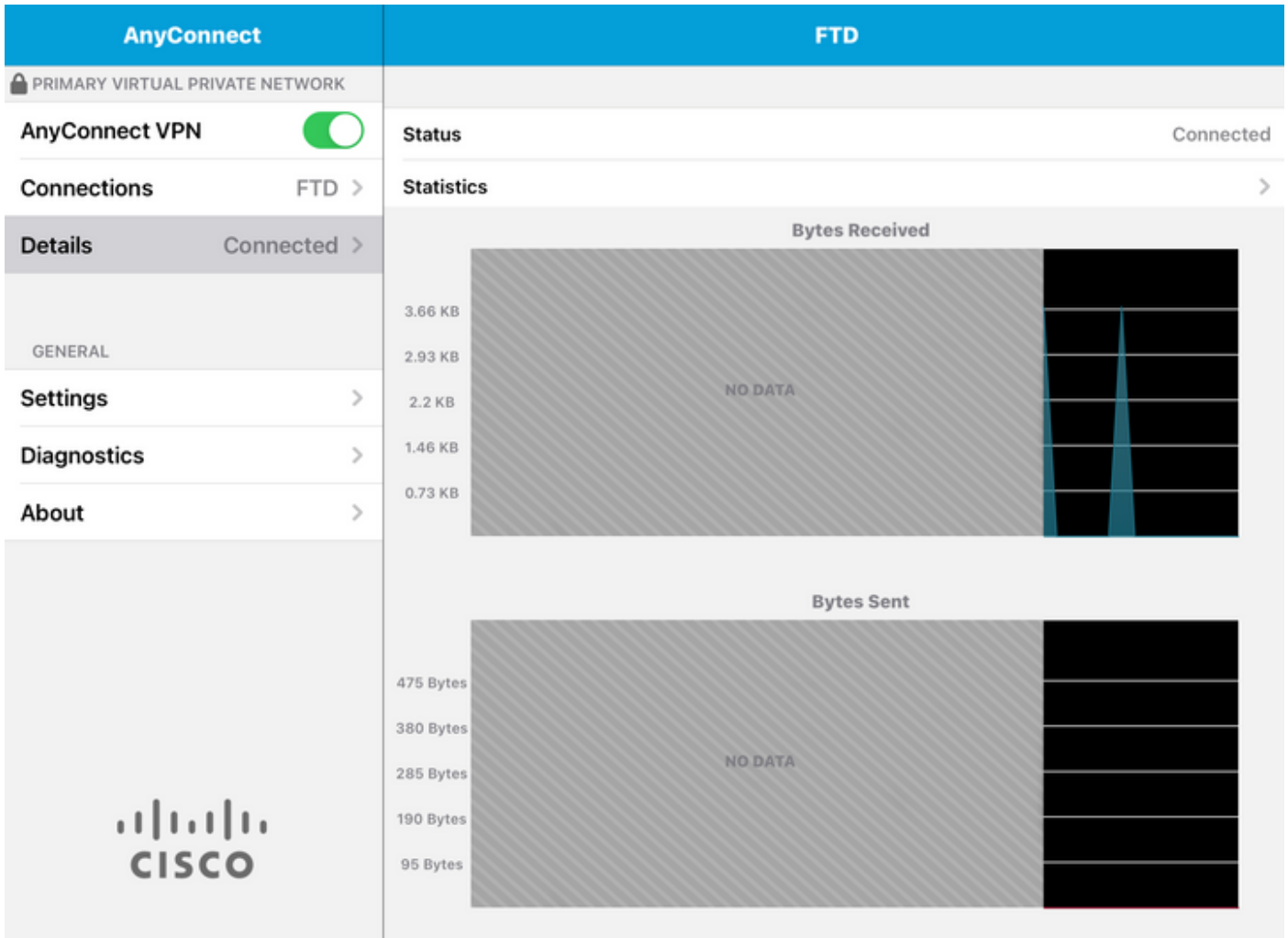
步骤 7.选择Advanced。

步骤 8选择Certificate，然后选择新添加的证书。




步骤 9返回Connections并测试。

一旦成功，切换将保持打开状态，详细信息将显示为已连接(connected)。



## 验证

命令 `show vpn-sessiondb detail Anyconnect` 显示有关所连接主机的所有信息。

 提示：进一步过滤此命令的选项是添加到命令中的“filter”或“sort”关键字。

例如：

```
Tcountrie-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

## 故障排除

### 调试

解决此问题所需的调试如下：

```
Debug crypto ca 14
```

```
Debug webvpn 255
```

```
Debug webvpn Anyconnect 255
```

如果连接是IPSEC而不是SSL:

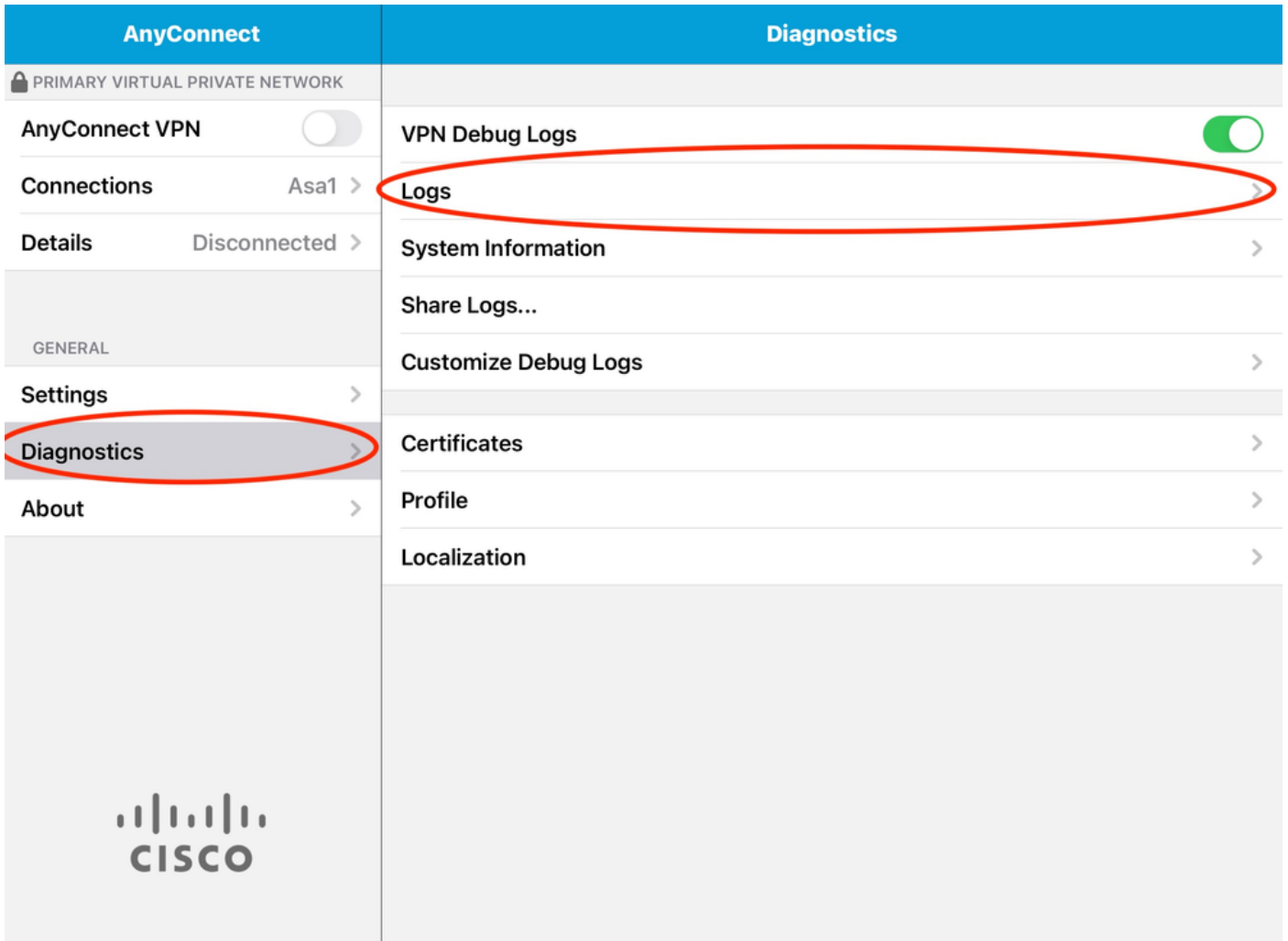
```
Debug crypto ikev2 platform 255
```

```
Debug crypto ikev2 protocol 255
```

```
debug crypto CA 14
```

Anyconnect移动应用的日志：

导航到诊断> VPN调试日志>共享日志。

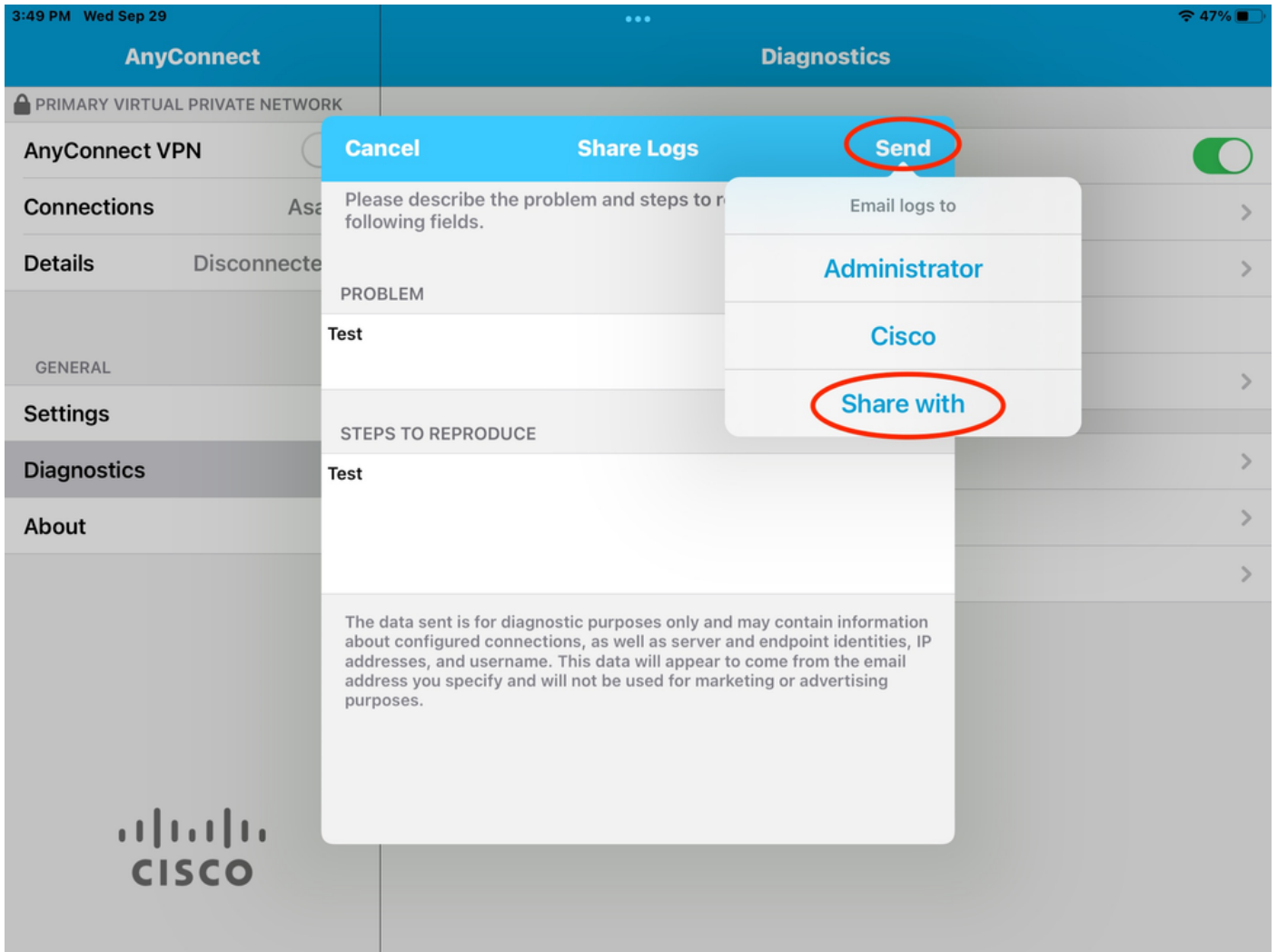


输入以下信息：

- 问题
- 复制步骤

然后导航到发送>共享对象。





此选项可用于使用电子邮件客户端发送日志。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。