

Configure Anyconnect Certificate Based Authentication for Mobile Access

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure Cisco Anyconnect on FTD](#)

[Network Diagram](#)

[Add Certificate to FTD](#)

[Configure Cisco Anyconnect](#)

[Create Certificate for Mobile Users](#)

[Install on Mobile Device](#)

[Verify](#)

[Troubleshoot](#)

[Debugs](#)

Introduction

This document describes an example of the implementation of certificate-based authentication on mobile devices.

Prerequisites

The tools and devices used in the guide are:

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Apple iOS device (iPhone, iPad)
- Certificate Authority (CA)
- Cisco Anyconnect Client Software

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic VPN
- SSL/TLS
- Public Key Infrastructure
- Experience with FMC
- OpenSSL
- Cisco Anyconnect

Components Used

The information in this document is based on these software and hardware versions:

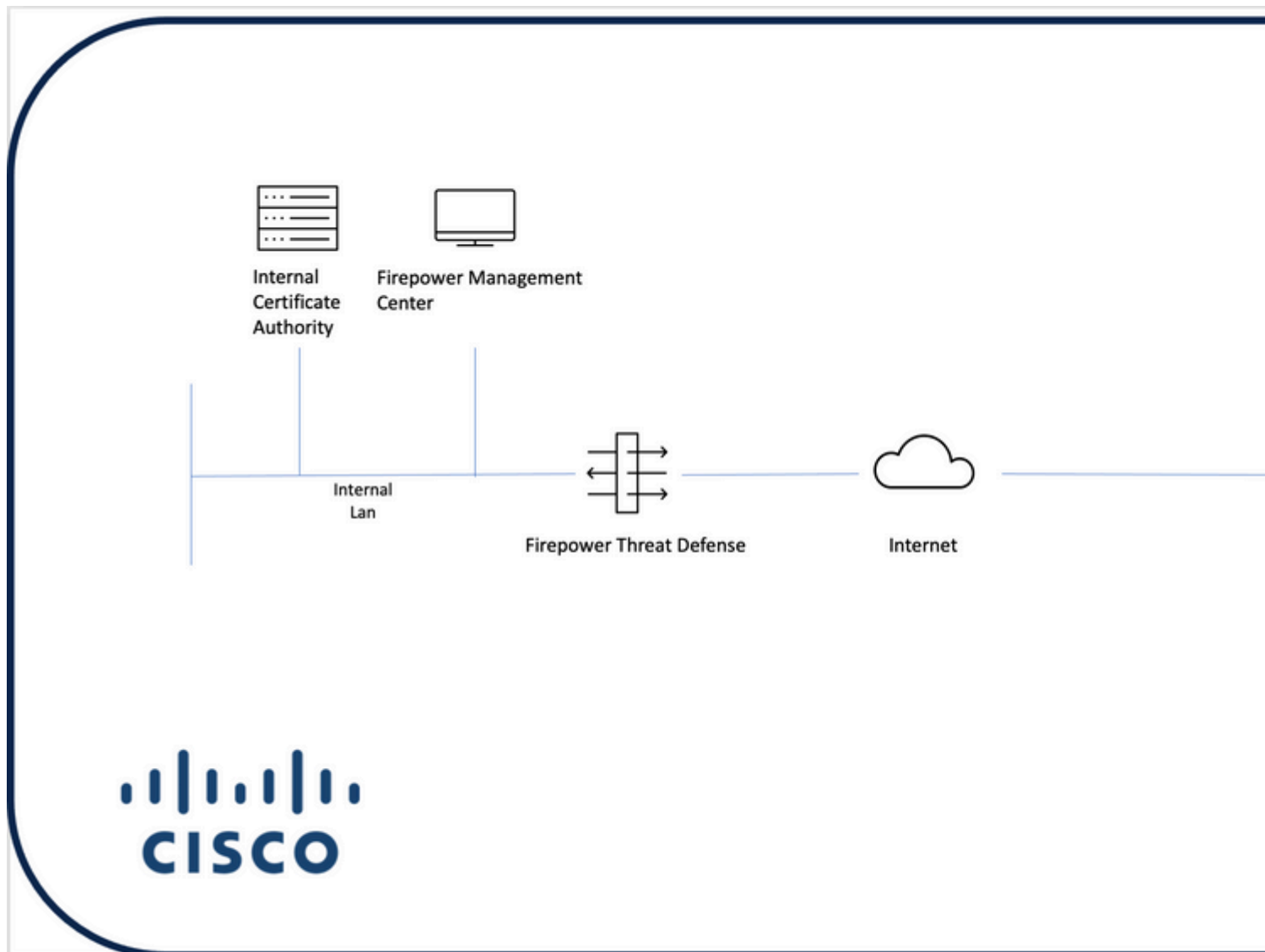
- Cisco FTD
- Cisco FMC
- Microsoft CA Server
- XCA
- Cisco Anyconnect
- Apple ipad

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure Cisco Anyconnect on FTD

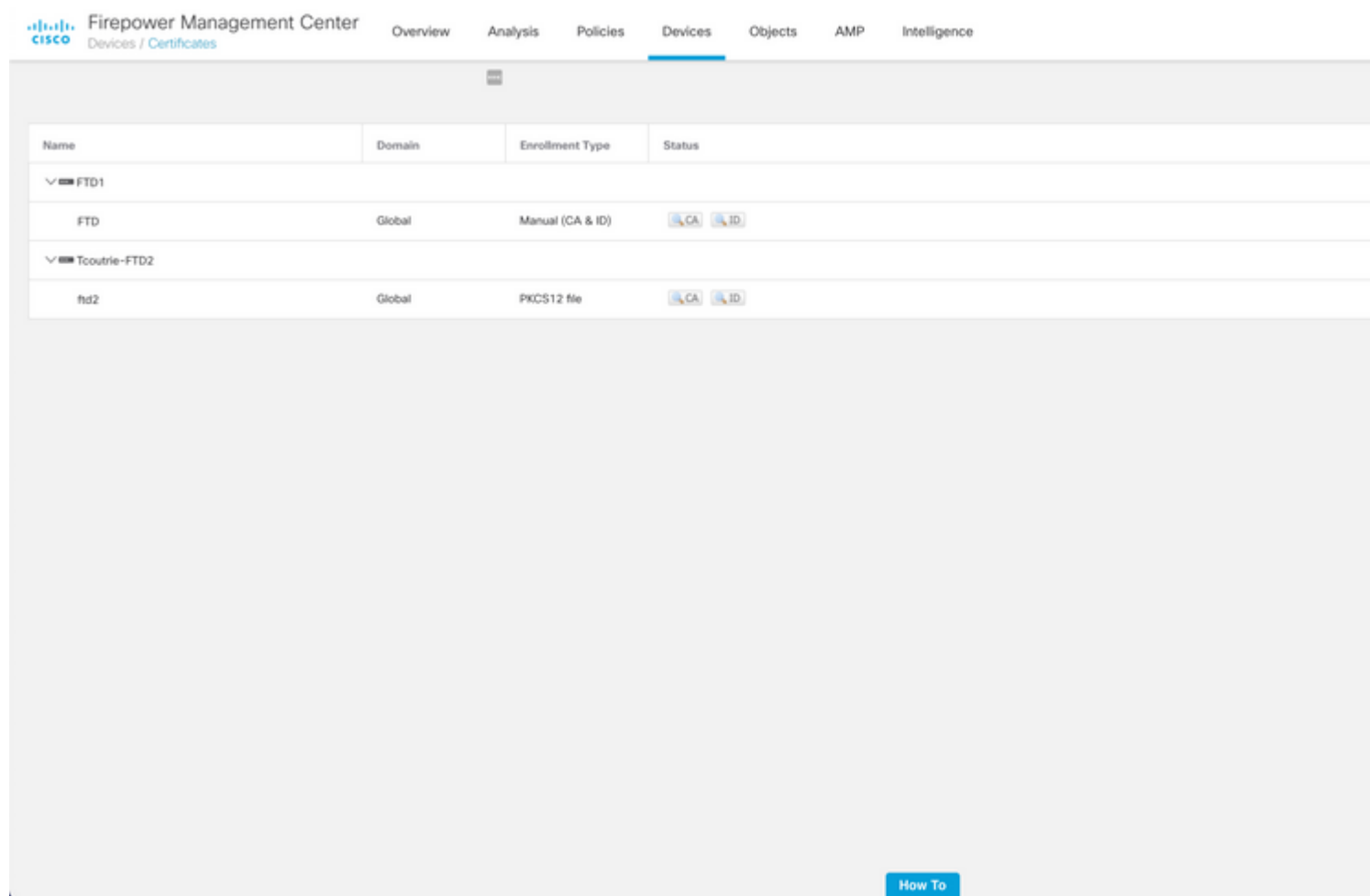
This section describes the steps to configure Anyconnect via FMC. Before you begin, be sure to deploy all configurations.

Network Diagram

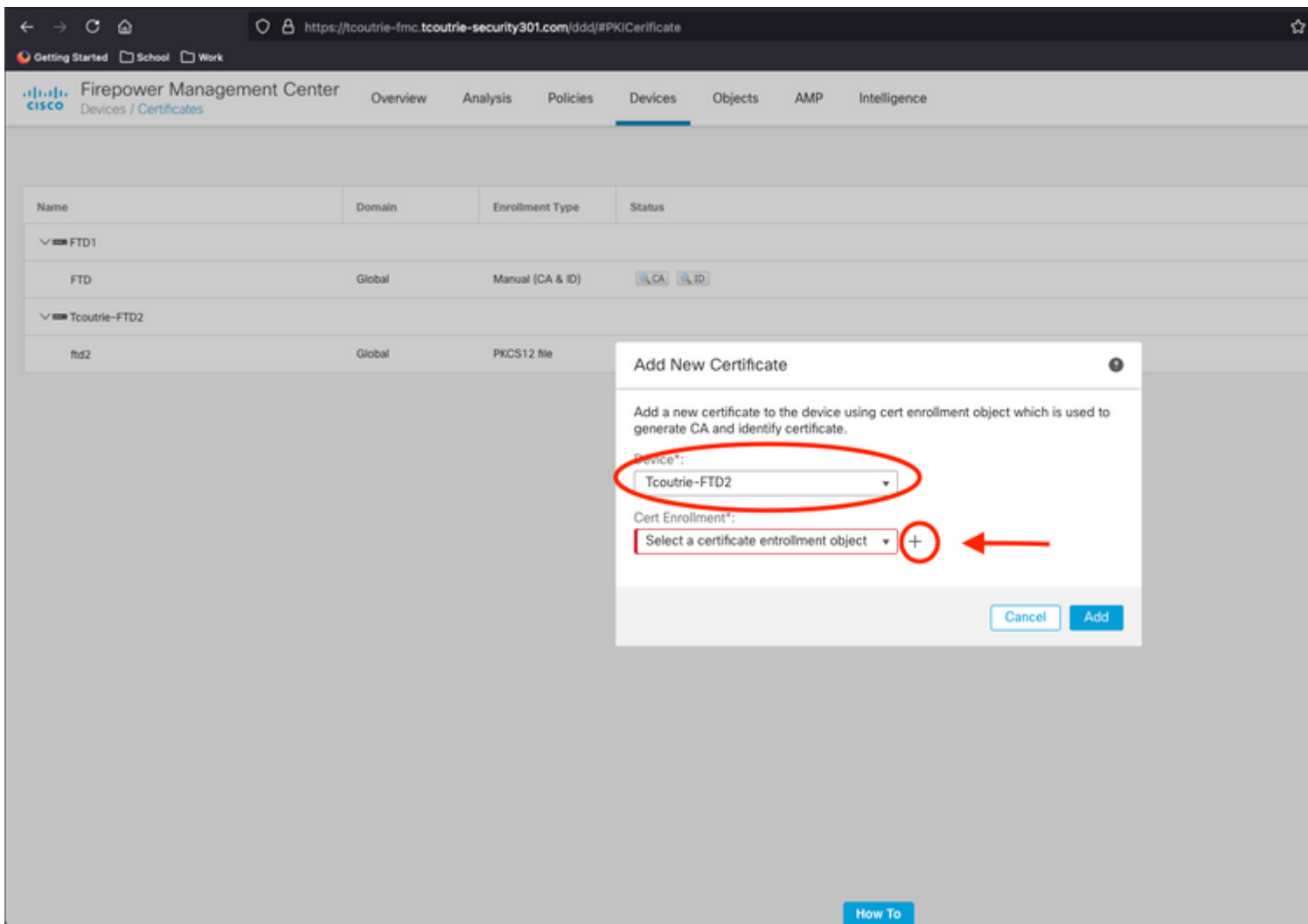


Add Certificate to FTD

Step 1. Create a certificate for the FTD on the FMC appliance. Navigate to **Devices > Certificate** and choose **Add**, as shown in this image:



Step 2. Choose the FTD desired for the VPN connection. Choose the **FTD appliance** from the devices dropdown. Click the + icon to add a new certificate enrollment method, as shown in this image:



Step 3. Add the certificates to the device. Choose the option that is the preferred method to obtain certificates in the environment.

Tip: The available options are: Self Signed Certificate - Generate a new certificate locally, SCEP - Use Simple Certificate Enrollment Protocol to obtain a certificate from a CA, Manual- Manually install the Root and Identity certificate, PKCS12 - Upload encrypted certificate bundle with root, identity, and private key.

Step 4. Upload the certificate to the FTD device. Enter the passcode (PKCS12 only) and click **Save**, as shown in this image:

Add Cert Enrollment

Name*

ftdcert

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

PKCS12 File

PKCS12 File*:

Tcoutrie-ftd2.p12

[Browse PKCS1](#)

Passphrase:

.....



Skip Check for CA flag in basic constraints of the CA

C

: Once you have saved the file, the deployment of the certificates occurs immediately. To see certificate details, choose the ID.

Configure Cisco Anyconnect

Configure Anyconnect via FMC with the remote access wizard.

Step 1. Start the Remote Access VPN policy wizard to configure Anyconnect.

Navigate to **Devices > Remote Access** and choose **Add**.

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the text "Firepower Management Center", and the breadcrumb "Devices / VPN / Remote Access". The main navigation menu has tabs for "Overview", "Analysis", "Policies", "Devices", "Objects", "AMP", and "Intelligence", with "Devices" currently selected. Below the navigation is a table with three columns: "Name", "Status", and "Last Modified".

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

A "How To" button is visible in the bottom right corner of the interface.

Step 2. Policy Assignment.

Complete the policy assignment:

- Name the policy.
- Choose the VPN protocols desired.
- Choose the targeted device to apply the configuration.

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:
FTD2

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Search"/> FTD1 Tcourrie-FTD2	Tcourrie-FTD2
<input type="button" value="Add"/>	

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.

[How To](#)

Step 3. Connection Profile.

- Name the Connection Profile.
- Set the authentication method to Client Certificate Only.
- Assign an IP address pool, and if needed, create a new Group Policy.
- Click **Next**.

Remote Access VPN Policy Wizard

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

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:

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: +
(RADIUS 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 (RADIUS or RADIUS only)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: +

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: +

[Edit Group Policy](#)

Note: Choose the Primary Field to be used to enter the user name for authentication sessions. The CN of the certificate is used in this guide.

Step 4. Anyconnect.

Add an Anyconnect image to the appliance. Upload the preferred version of Anyconnect and click **Next**.

Note: Cisco Anyconnect packages can be downloaded from **Software.Cisco.com**.

Step 5. Access and Certificate.

Apply the Certificate to an Interface and enable Anyconnect on Interface Level, as shown in this image, and click **Next**.

Step 6. Summary.

Review the configurations. If all checks out, click **finish** and then **deploy**.

Create Certificate for Mobile Users

Create a certificate to be added to the mobile device used in the connection.

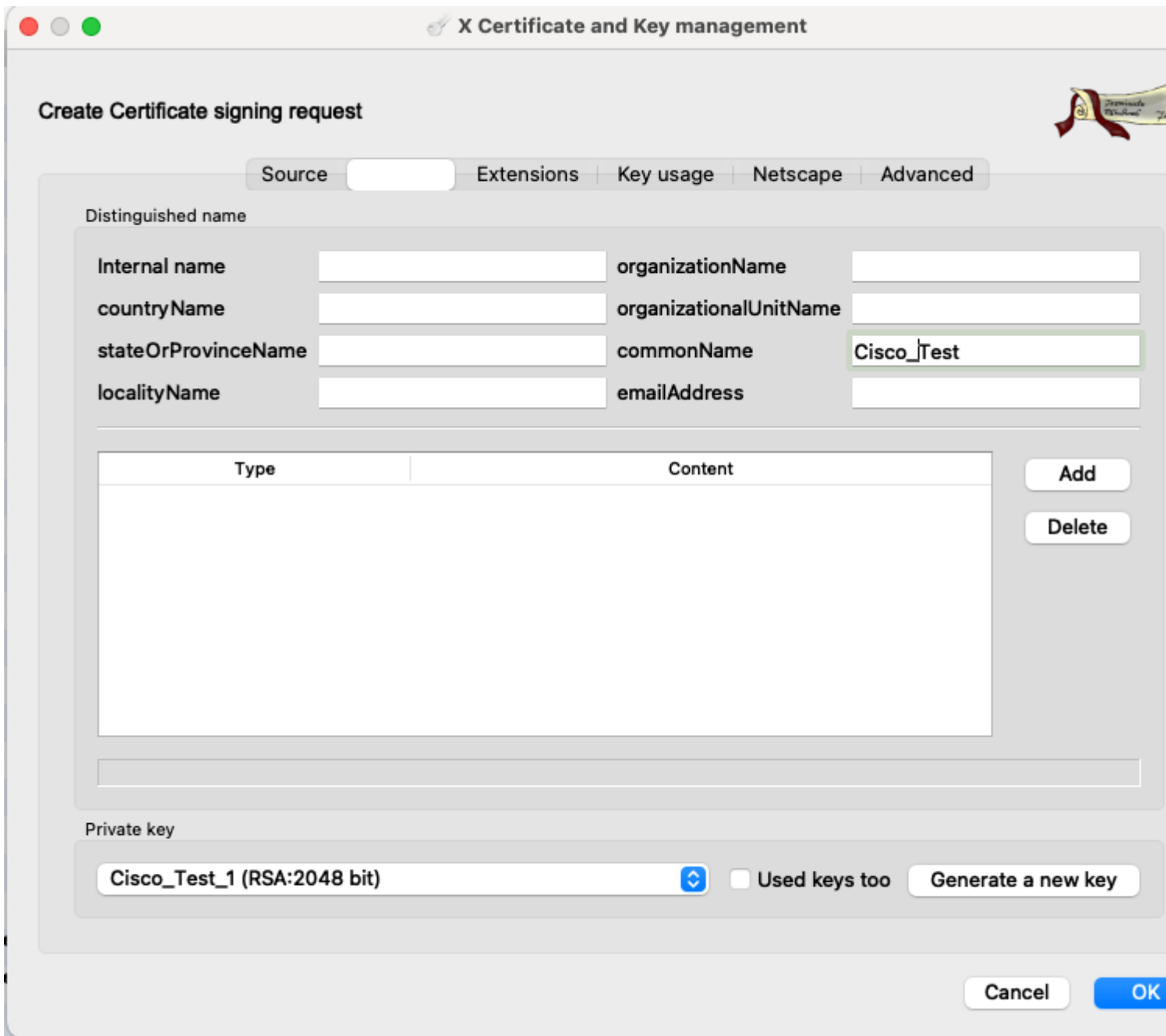
Step 1. XCA.

- a. Open XCA
- b. Start a new Database

Step 2. Create CSR.

- a. Choose **Certificate Signing Request (CSR)**
- b. Choose **New Request**
- c. Enter the value with all information needed for the certificate

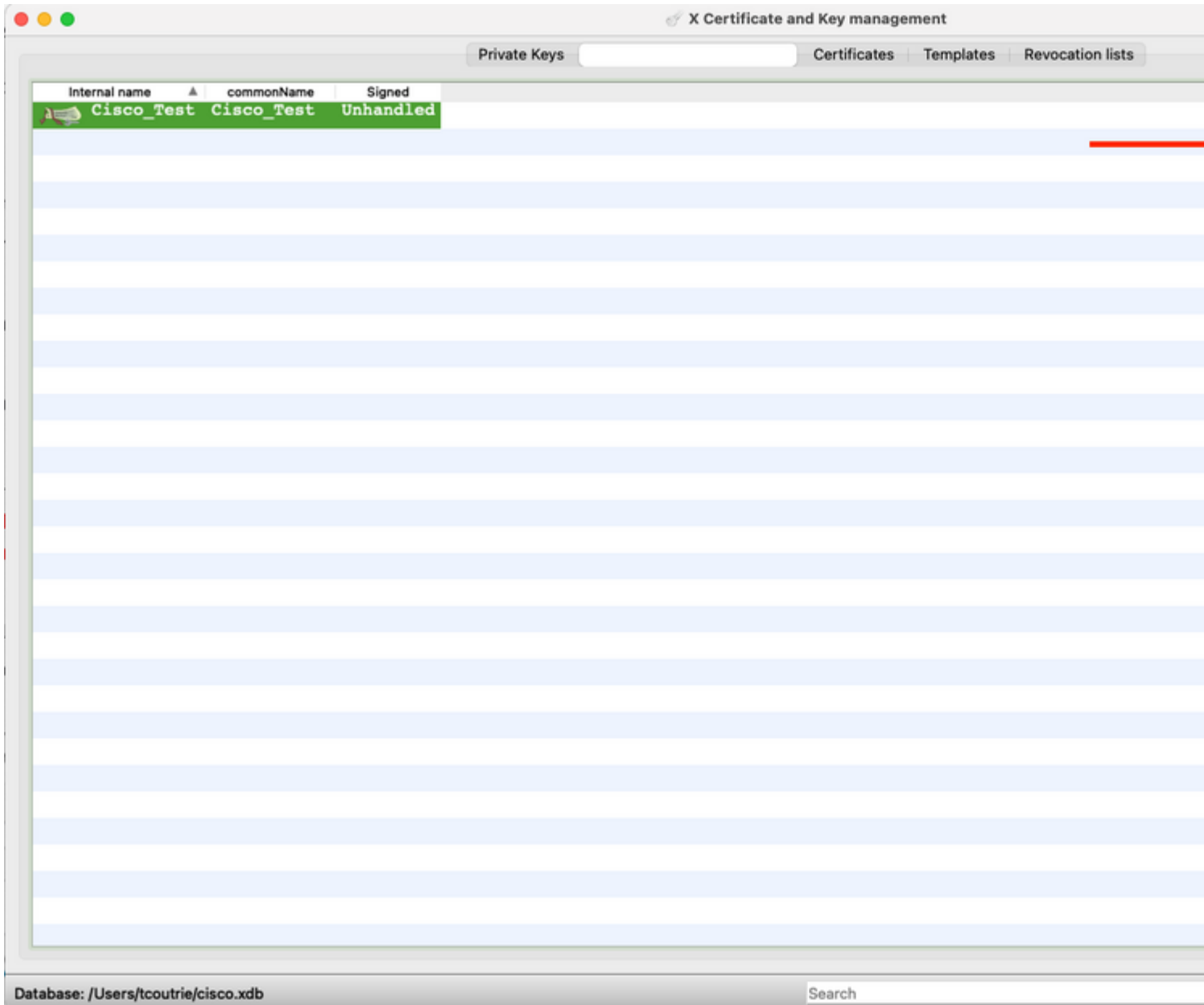
- d. Generate a new key
- e. When finished, click **OK**



Note: This document uses the CN of the certificate.

Step 3. Submit CSR.

- a. Export the CSR
- b. Submit CSR to CA to obtain a new Certificate



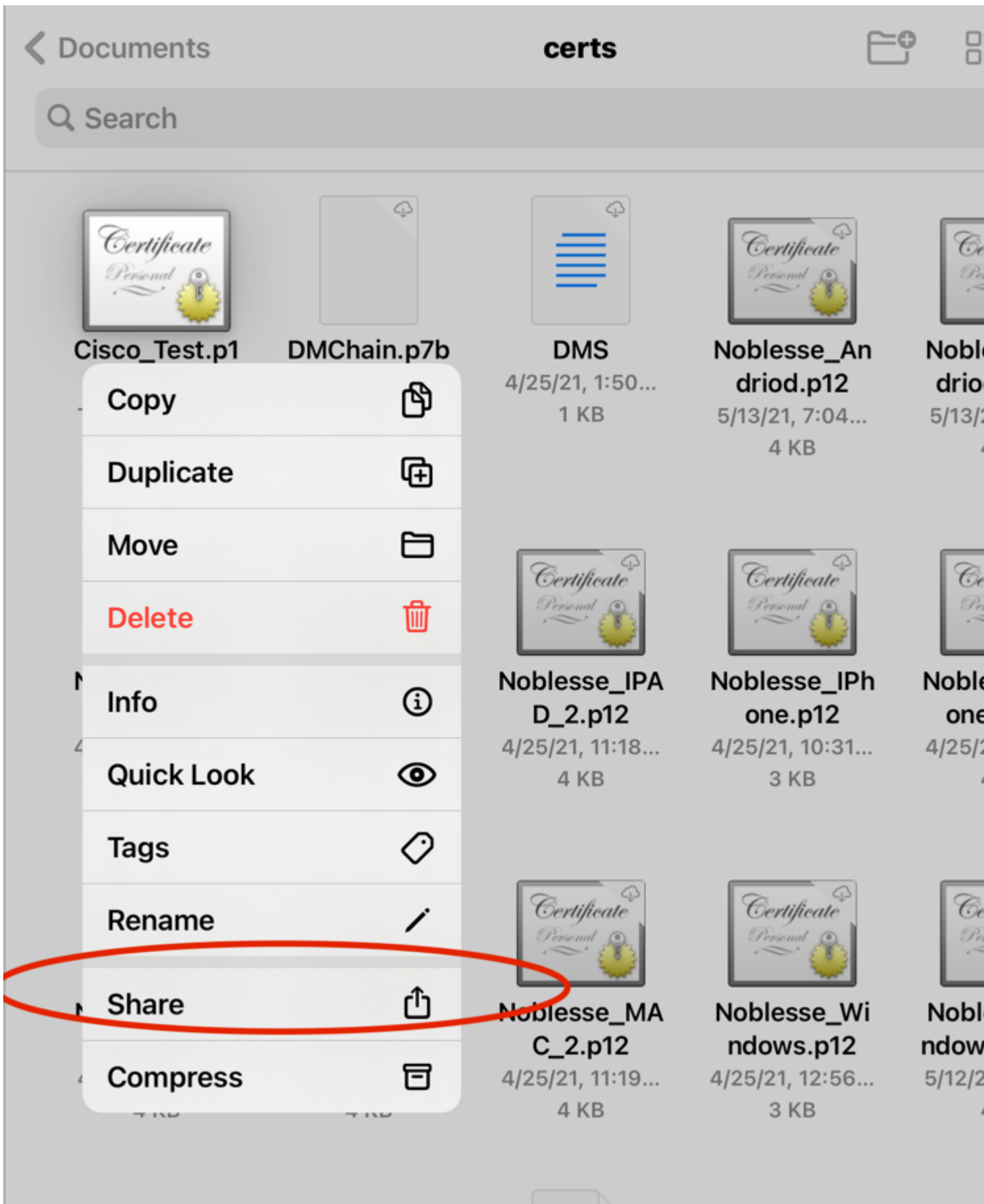
Note: Use the PEM format of the CSR.

Install on Mobile Device

Step 1. Add the device certificate to the mobile device.

Step 2. Share the certificate with the Anyconnect application to add the new certificate application.

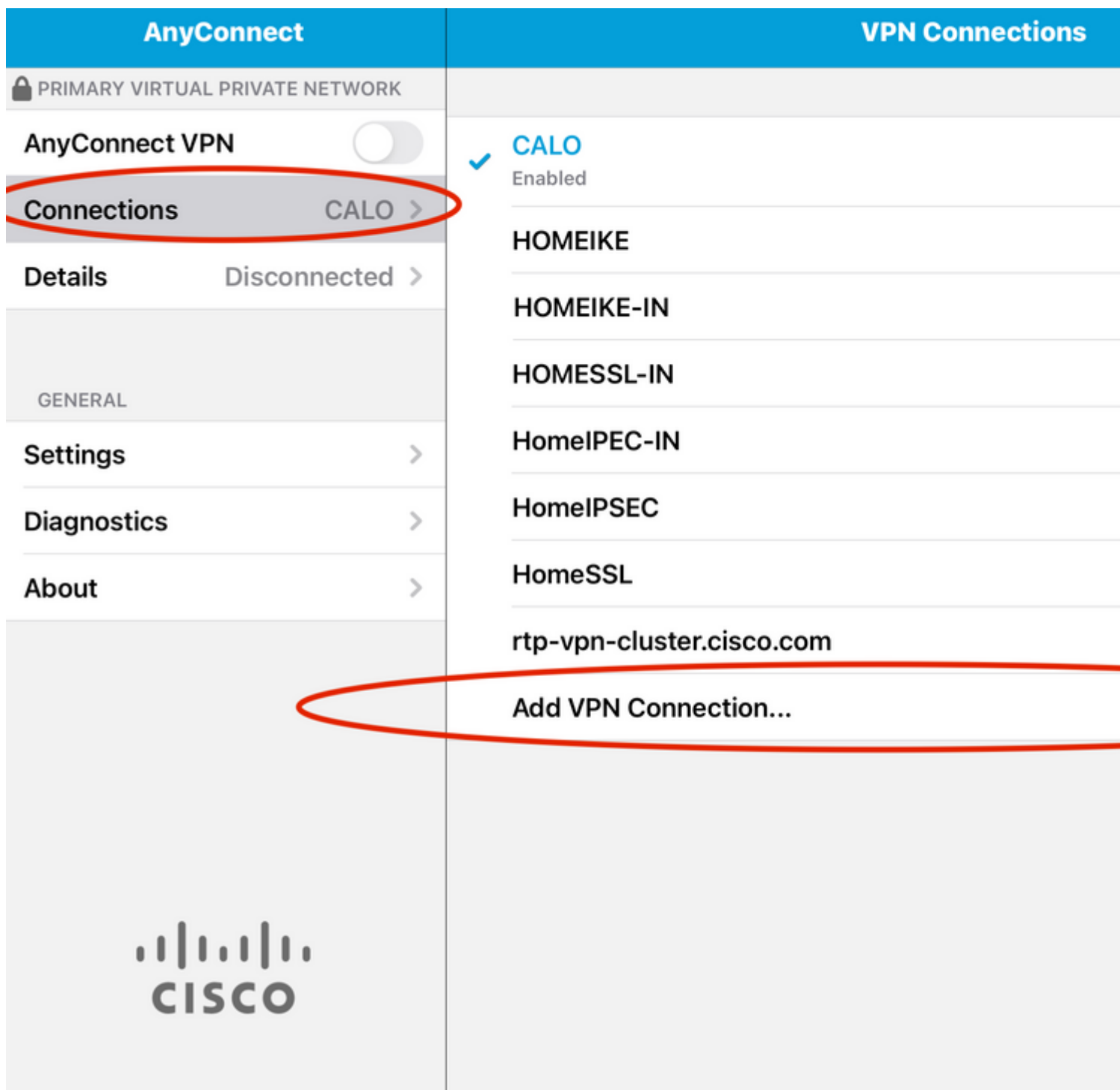
Caution: Manual installation requires the user to share the certificate with the application. This does not apply to certificates pushed via MDMs.



Step 3. Enter certificate password for **PKCS12** File.

Step 4. Create a New connect on Anyconnect.

Step 5. Navigate to new connections; **Connections** > **Add VPN Connection**.



Step 6. Enter the information for the new connection.â€Œ

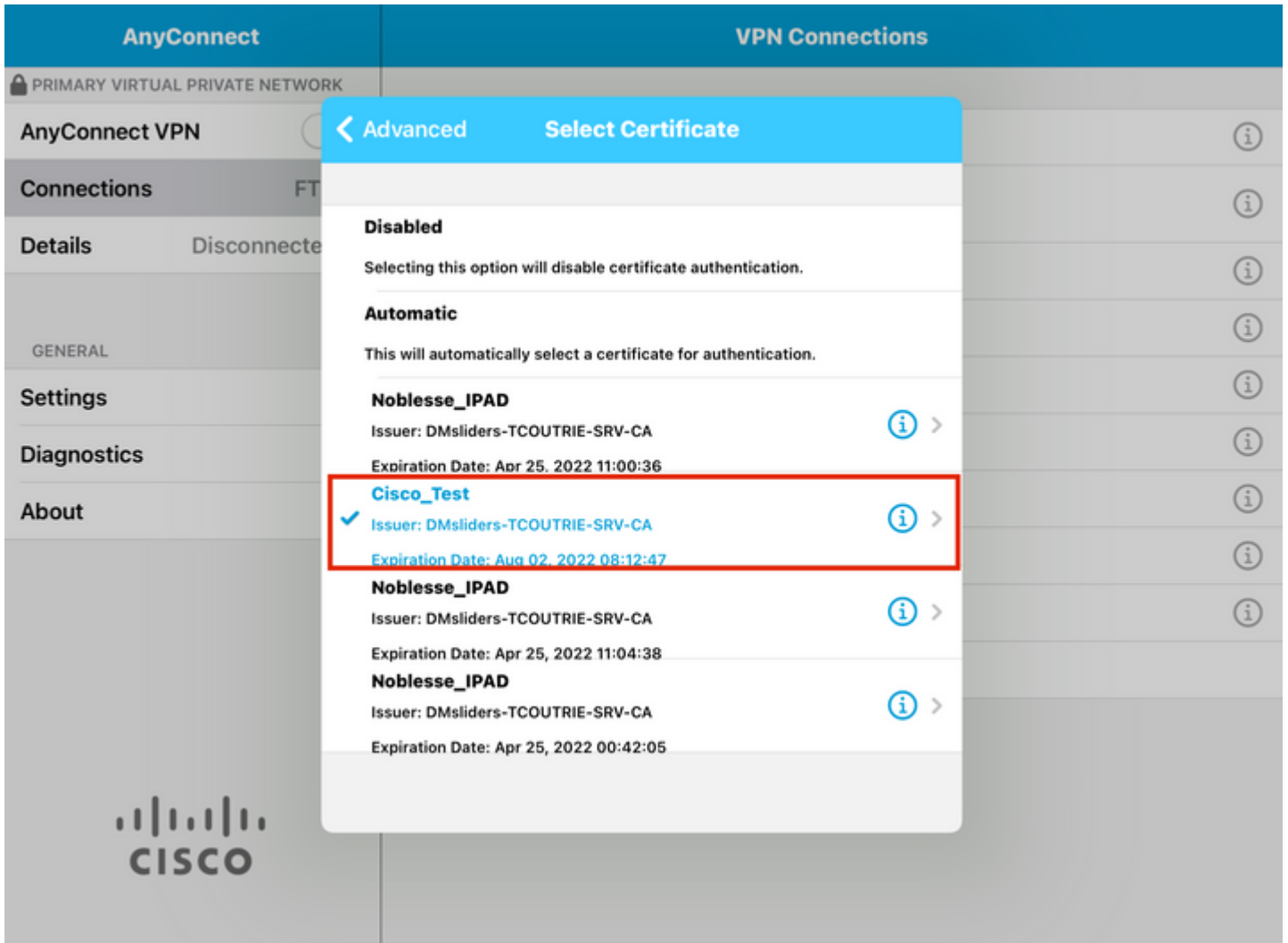
Description: Name the connect

Server Address: IP address or FQDN of FTD

Advanced: Additional configurations

Step 7. Choose **Advanced**.


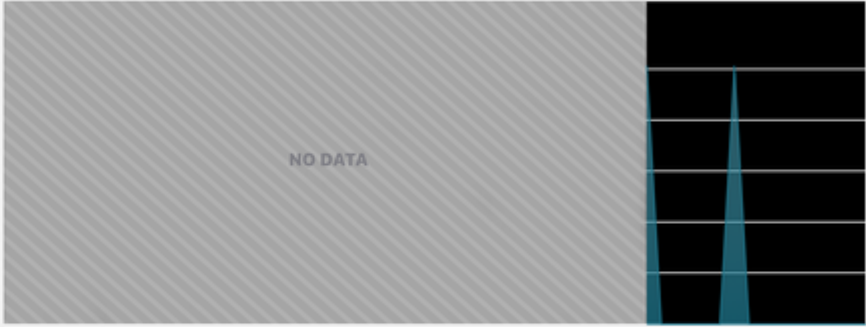

Step 8. Choose **Certificate** and choose your newly added certificate.



â€f

Step 9. Navigate back to **Connections** and test.

Once successful, the toggle stays on and details show connected in the status.

AnyConnect	FTD
PRIMARY VIRTUAL PRIVATE NETWORK	
AnyConnect VPN <input checked="" type="checkbox"/>	Status Connected
Connections FTD >	Statistics >
Details Connected >	
GENERAL	
Settings >	
Diagnostics >	
About >	
	<div style="text-align: center;">Bytes Received</div>  <div style="text-align: center;">Bytes Sent</div> 

Verify

The command **show vpn-sessiondb detail Anyconnect** shows all information about the connected host.

Tip: The option to further filter this command is the 'filter' or 'sort' keywords added to the command.

For example:

```
Tcoultrie-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

Troubleshoot

Debugs

Debugs that are required to troubleshoot this issue is:

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

If the connection is IPSEC and not SSL:

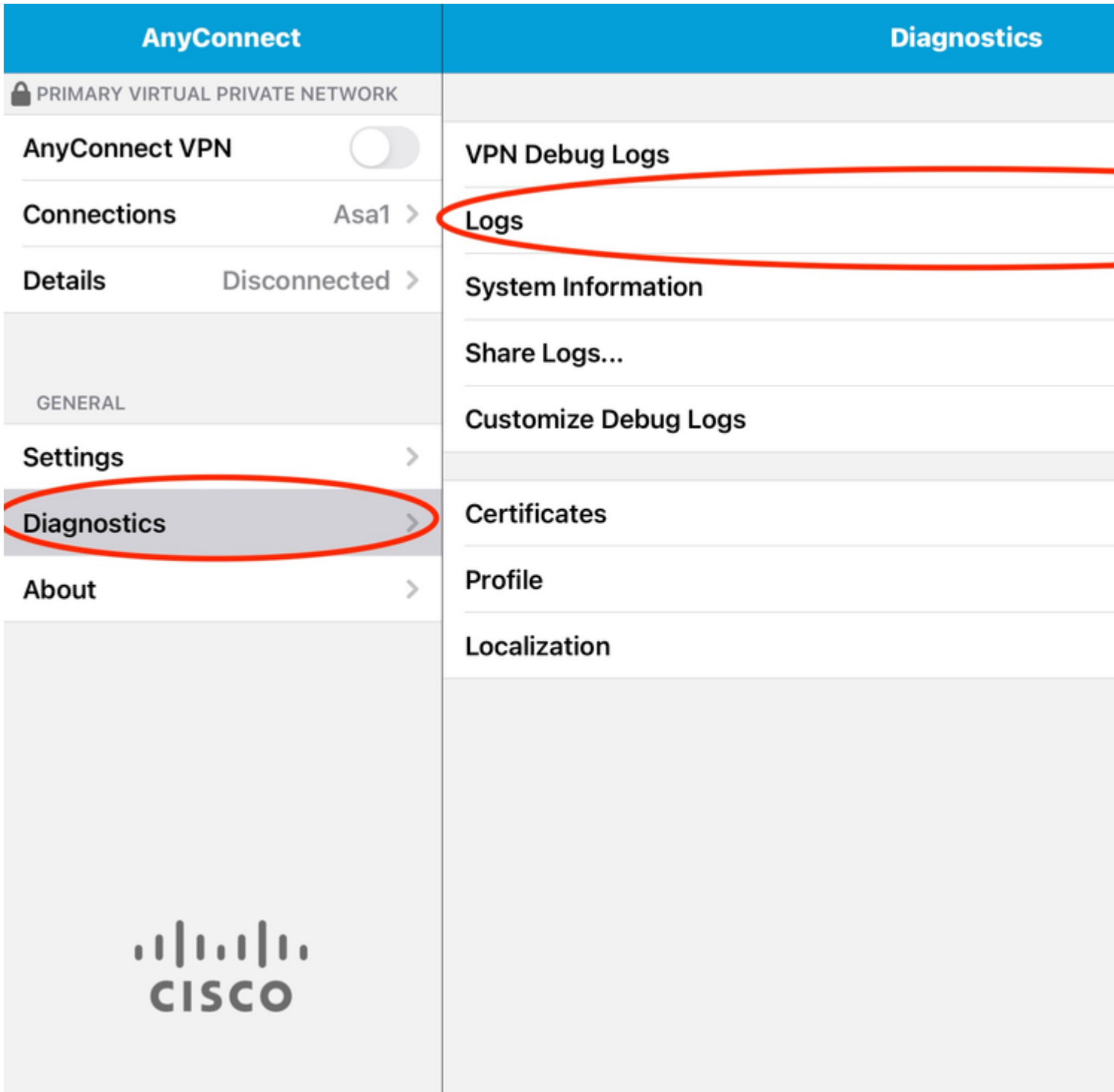
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

Logs from the Anyconnect mobile application:

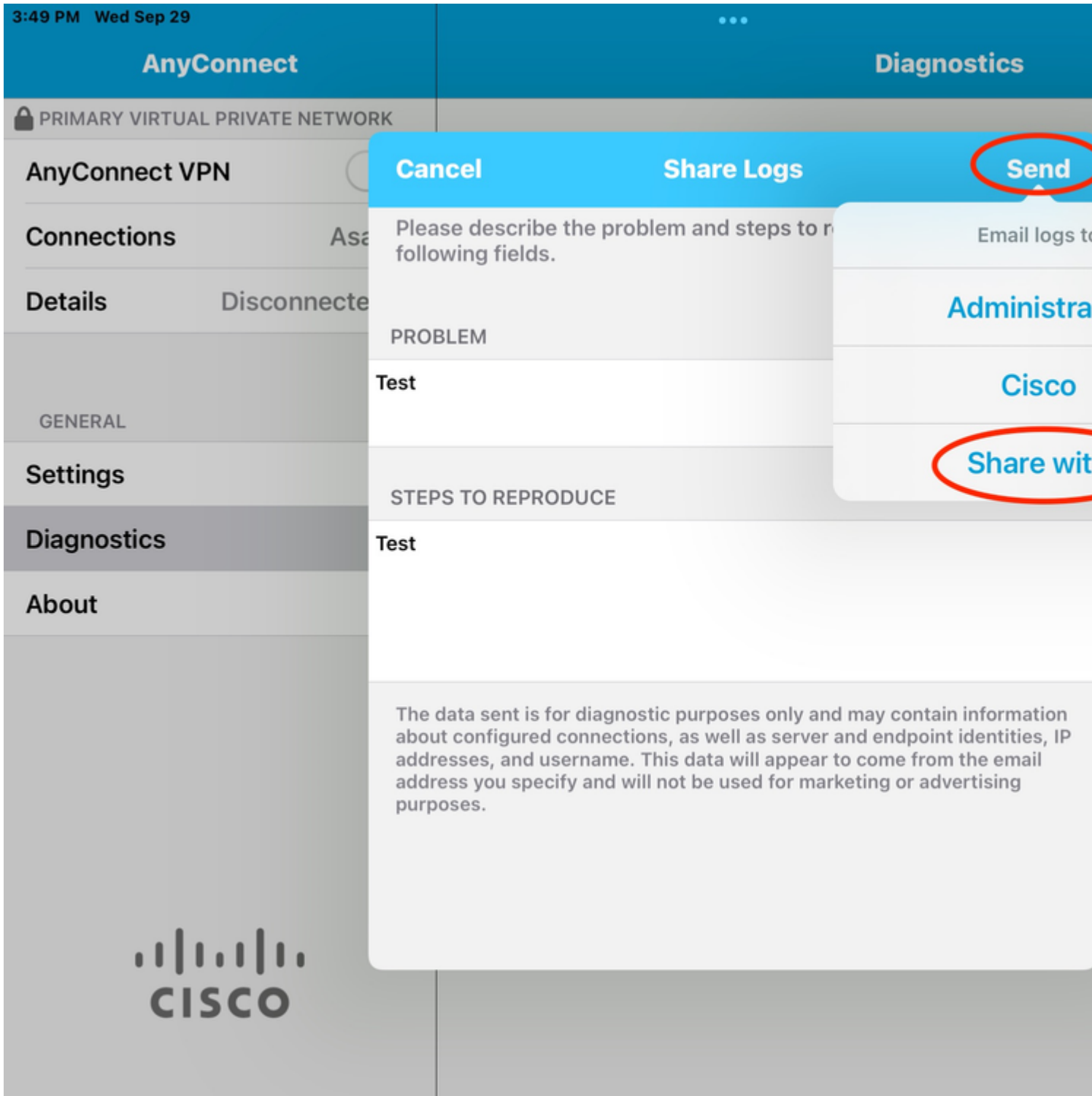
Navigate to **Diagnostic > VPN Debug Logs > Share logs**.



Enter in the information:

- Problem
- Steps to reproduce

Then navigate to **Send > Share with**.



This presents the option to use an email client to send the logs.