Configuración de la Autenticación Basada en Certificado de Anyconnect para el Acceso Móvil

Contenido

Introducción

Este documento describe un ejemplo de la implementación de la autenticación basada en certificados en dispositivos móviles.

Prerequisites

Las herramientas y dispositivos utilizados en la guía son:

- Cisco Firepower Threat Defense (FTD)
- Centro de administración Firepower (FMC)
- Dispositivo Apple iOS (iPhone, iPad)
- Autoridad de certificación (CA)
- Software cliente Cisco Anyconnect

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN básica,
- SSL/TLS
- Infraestructura de clave pública
- Experiencia con FMC
- OpenSSL
- Cisco Anyconnect

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

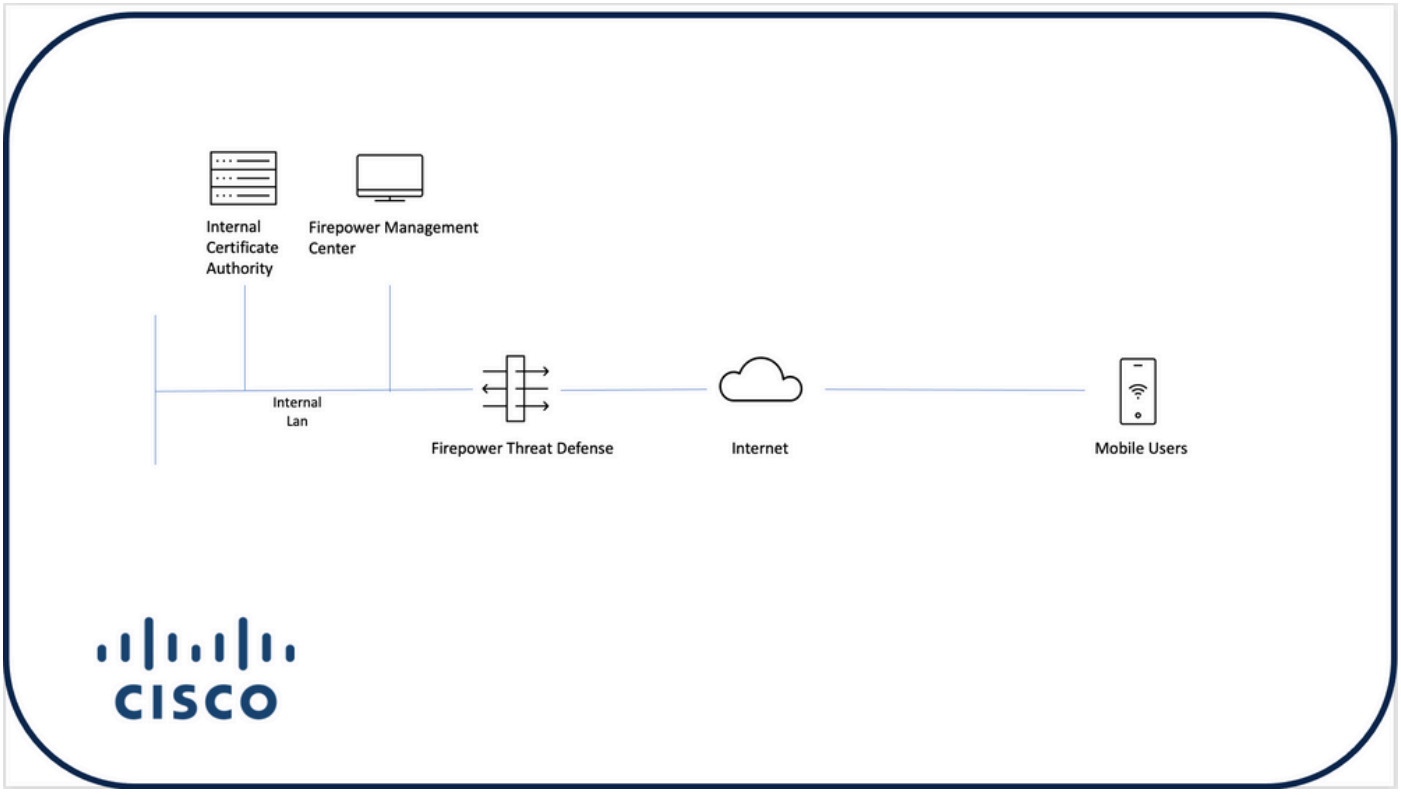
- FTD de Cisco
- Cisco FMC
- Microsoft CA Server
- XCA
- Cisco Anyconnect
- Apple Ipad

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración de Cisco Anyconnect en FTD

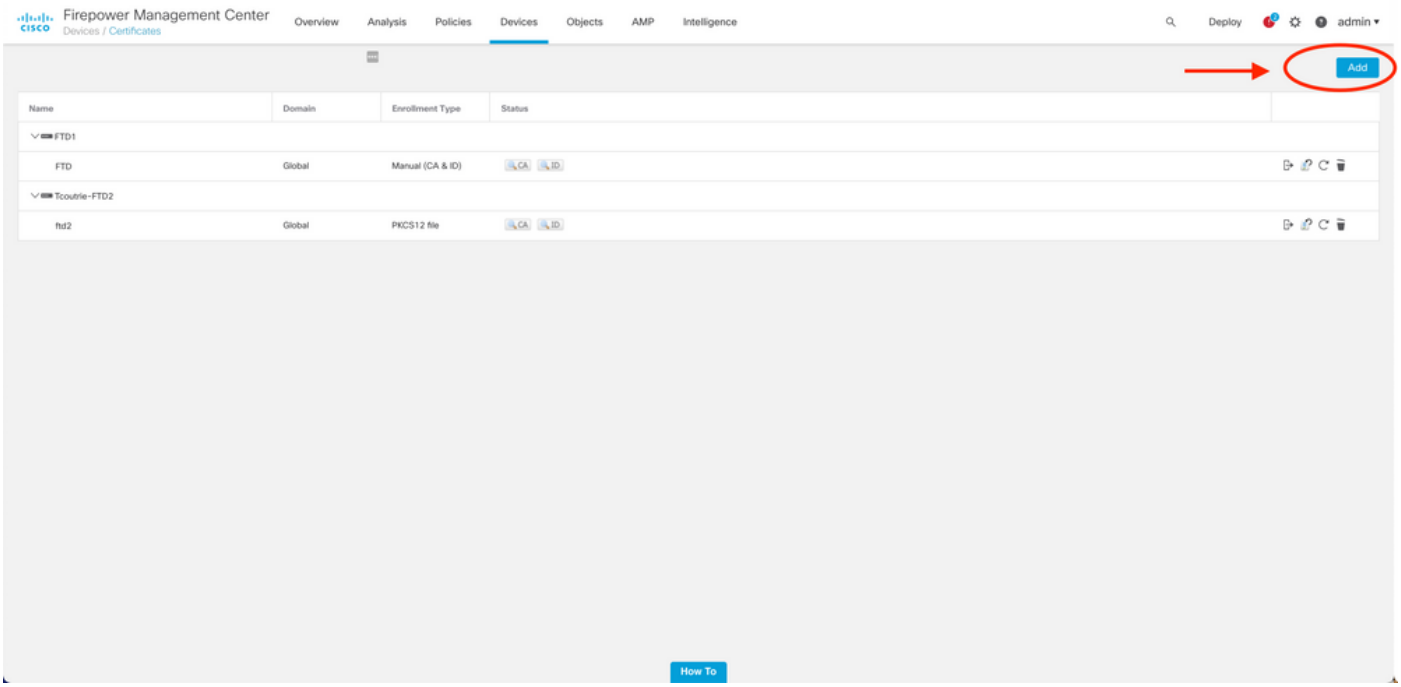
Esta sección describe los pasos para configurar Anyconnect a través de FMC. Antes de comenzar, asegúrese de implementar todas las configuraciones.

Diagrama de la red

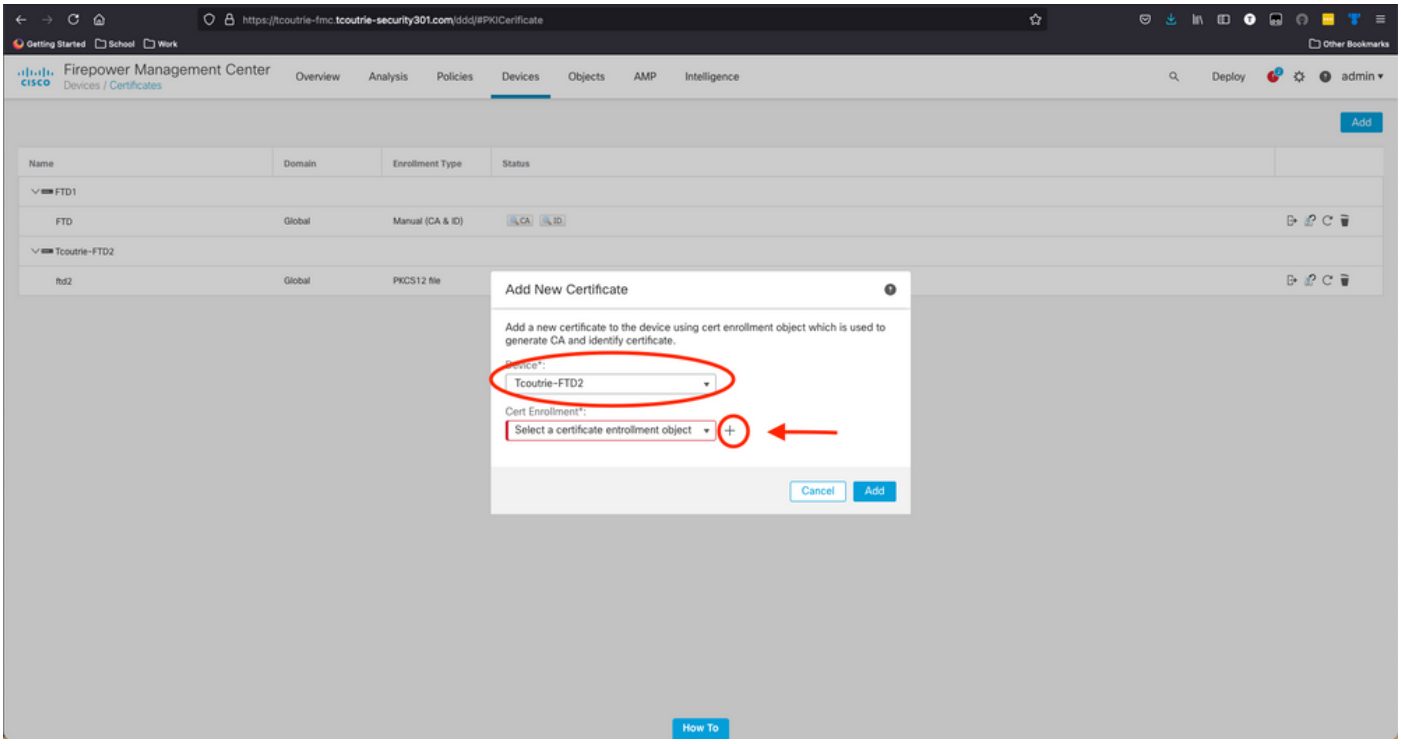


Agregar certificado a FTD

Paso 1. Cree un certificado para el FTD en el dispositivo FMC. Navegue hasta **Dispositivos > Certificado** y elija **Agregar**, como se muestra en esta imagen:



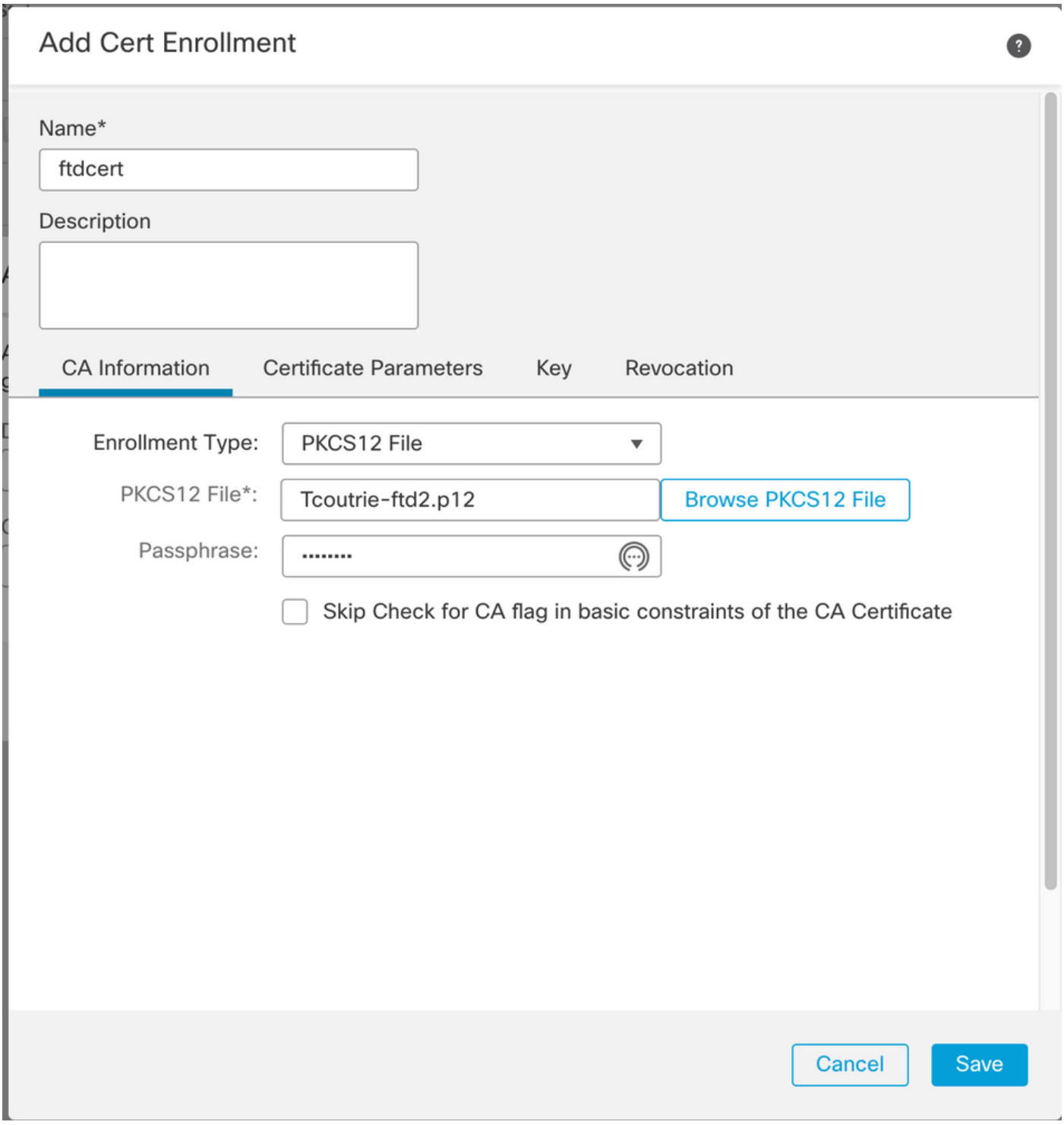
Paso 2. Elija el FTD deseado para la conexión VPN. Elija el **dispositivo FTD** del menú desplegable de dispositivos. Haga clic en el icono **+** para agregar un nuevo método de inscripción de certificados, como se muestra en esta imagen:



Paso 3. Agregue los certificados al dispositivo. Elija la opción que es el método preferido para obtener certificados en el entorno.

> **Consejo:** Las opciones disponibles son: **Certificado firmado automáticamente**: genere un nuevo certificado localmente, **SCEP** - Use Simple Certificate Enrollment Protocol para obtener un certificado de una CA, **Manual**- Instale manualmente el certificado raíz e identidad, **PKCS12** - Cargue un paquete de certificado cifrado con raíz, identidad y clave privada.

Paso 4. Cargue el certificado en el dispositivo FTD. Introduzca el código de acceso (sólo PKCS12) y haga clic en **Guardar**, como se muestra en esta imagen:



Nota: Una vez guardado el archivo, la implementación de los certificados se produce inmediatamente. Para ver los detalles del certificado, elija la ID.

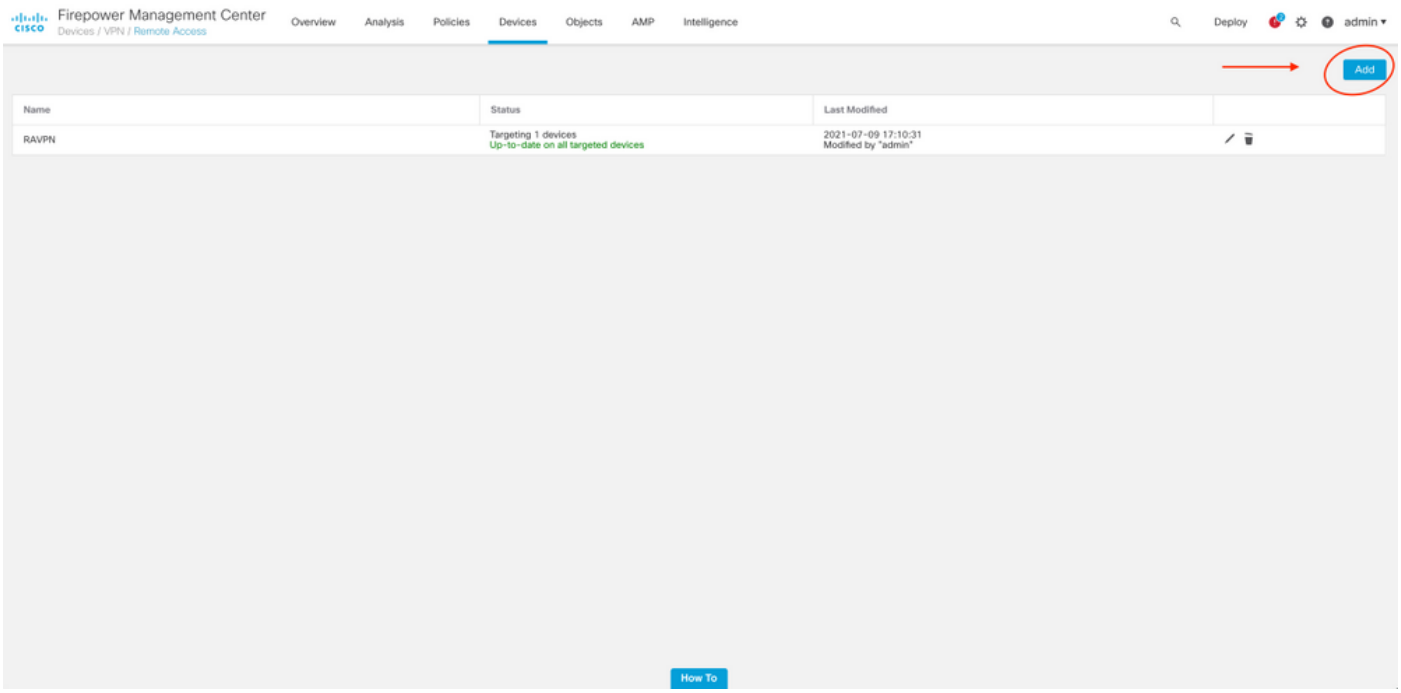
Configuración de Cisco Anyconnect

Configure Anyconnect a través de FMC con el asistente de acceso remoto.

Procedimiento:

Paso 1. Inicie el asistente de política VPN de acceso remoto para configurar Anyconnect.

Navegue hasta **Dispositivos > Acceso remoto** y elija **Agregar**.

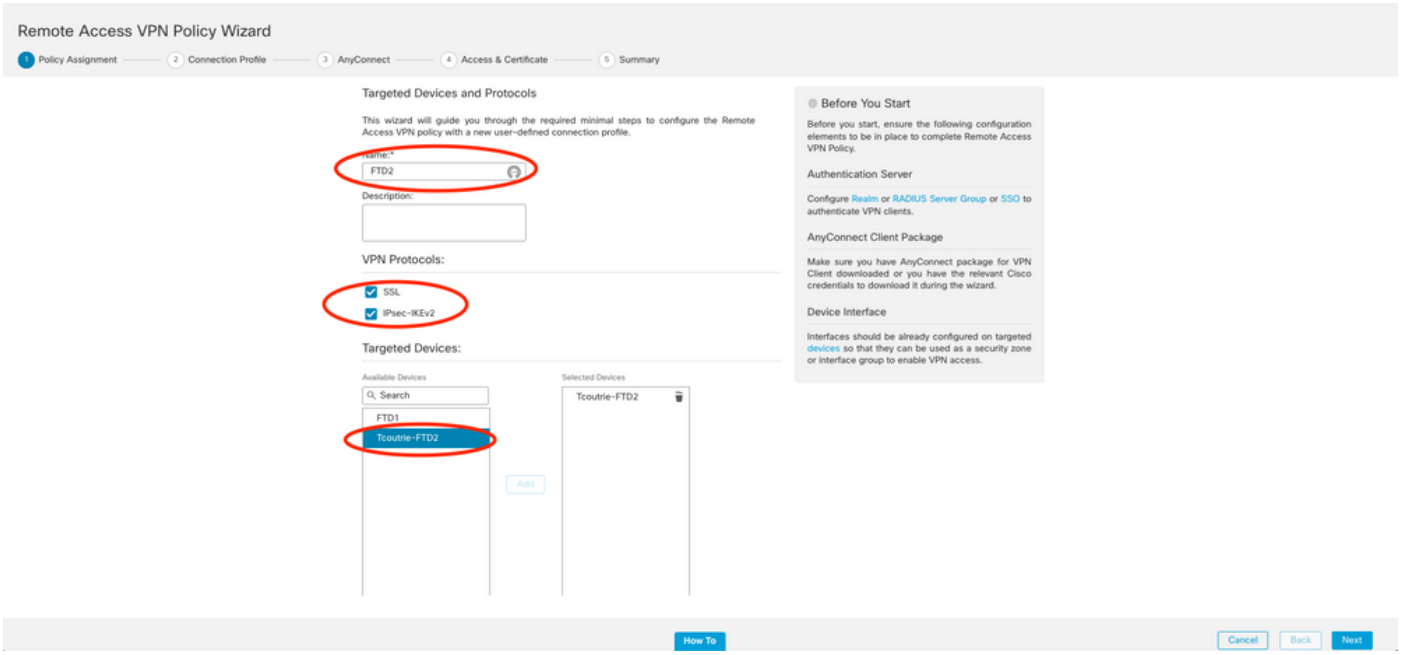


Paso 2. Asignación de política.

Complete la asignación de políticas:
a. Nombre la política

b. Elija los protocolos VPN deseados

c. Elija el dispositivo objetivo para aplicar la configuración

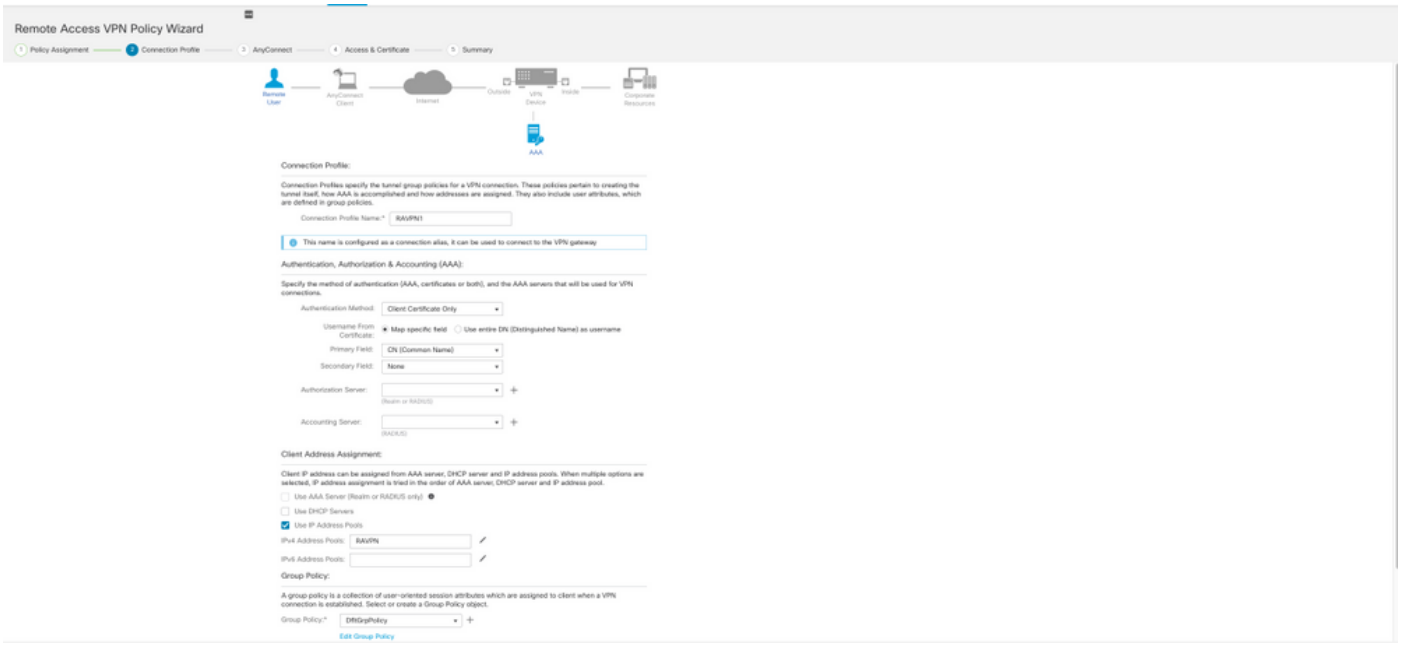


Paso 3. Perfil de conexión.

a. Nombre el perfil de conexión
b. Establezca el método de autenticación en Client Certificate Only

c. Asignar un conjunto de direcciones IP y, si es necesario, crear una nueva política de grupo

d. Haga clic en Next (Siguiente)



Nota: Elija el campo principal que se utilizará para introducir el nombre de usuario para las sesiones de autenticación. En esta guía se utiliza la CN del certificado.

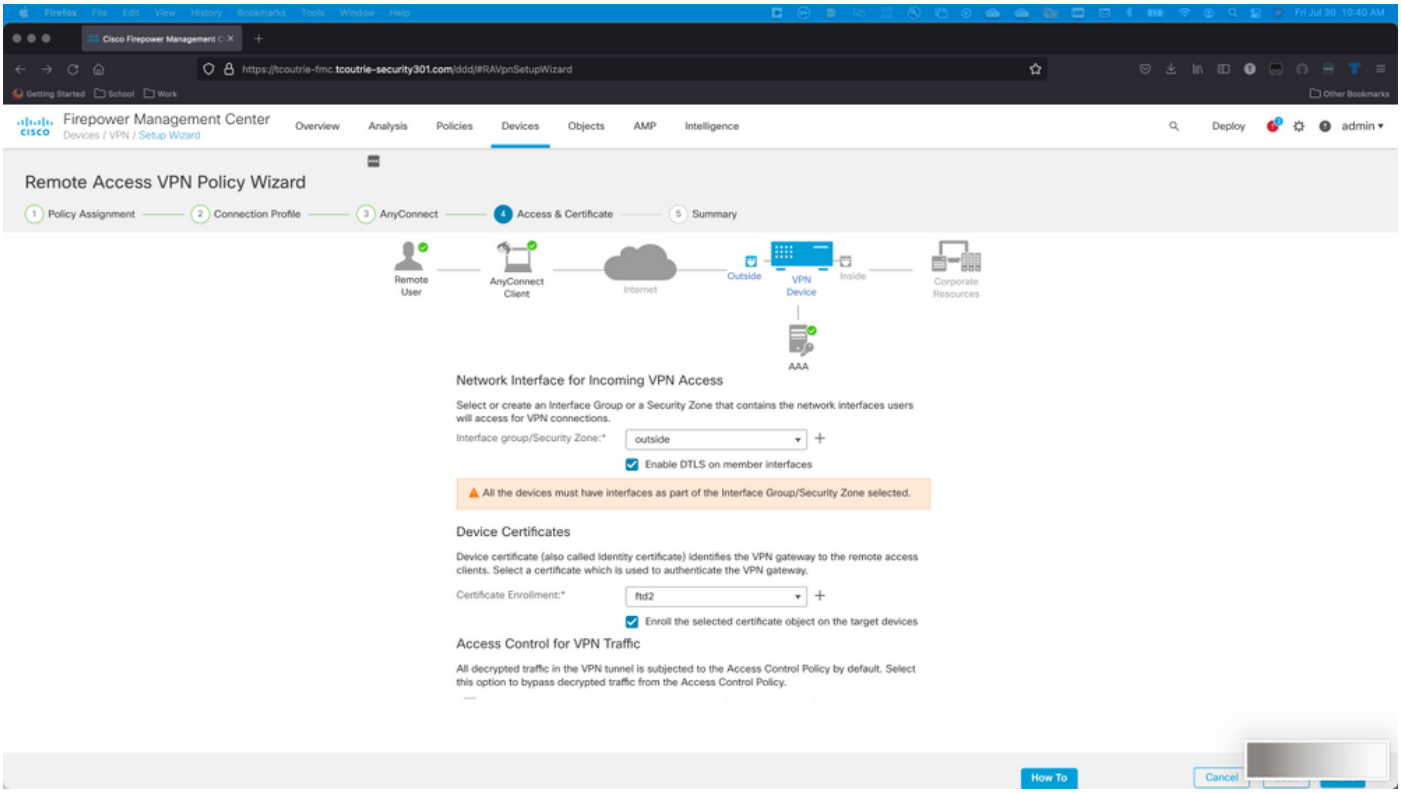
Paso 4. AnyConnect.

Agregue una imagen de Anyconnect al dispositivo. Cargue la versión preferida de Anyconnect y haga clic en **Next**.

Nota: Los paquetes de Cisco Anyconnect se pueden descargar desde **Software.Cisco.com**.

Paso 5. Acceso y certificado.

Aplique el Certificado a una Interfaz y habilite Anyconnect en el Nivel de Interfaz, como se muestra en esta imagen, y haga clic en **Siguiente.**



Paso 6. Summary.

Revise las configuraciones. Si se desprotege, haga clic en **finalizar** y, a continuación, **implementar**.

Crear certificado para usuarios móviles

Cree un certificado para agregarlo al dispositivo móvil utilizado en la conexión.

Paso 1. XCA.

a. Abrir XCA

b. Iniciar una nueva base de datos

Paso 2. Crear CSR

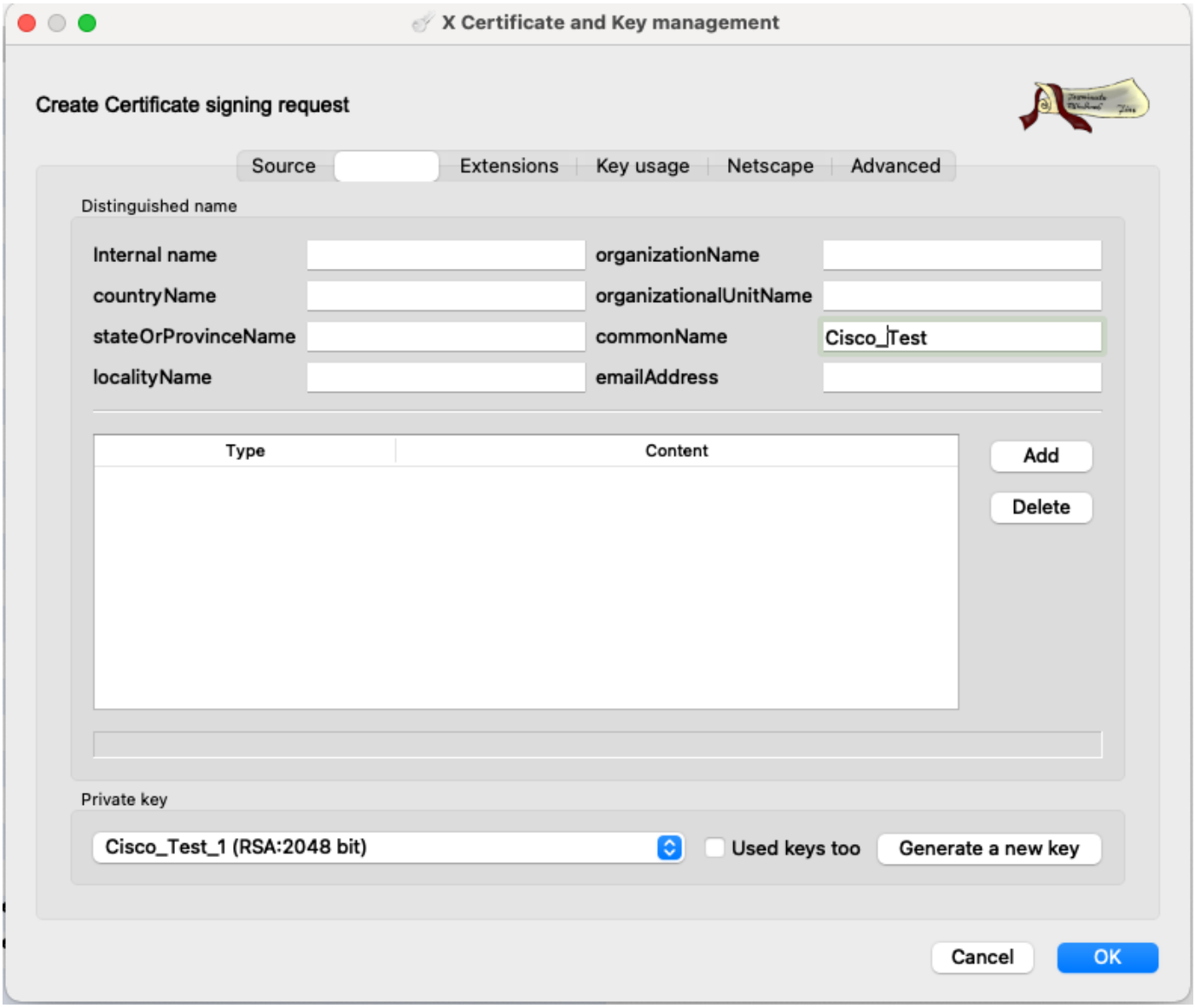
a. Elija **Solicitud de firma de certificado** (CSR)

b. Elija **Nueva solicitud**

c. Introduzca el valor con toda la información necesaria para el certificado

d. Generar una nueva clave

e. Cuando haya terminado, haga clic en **Aceptar**

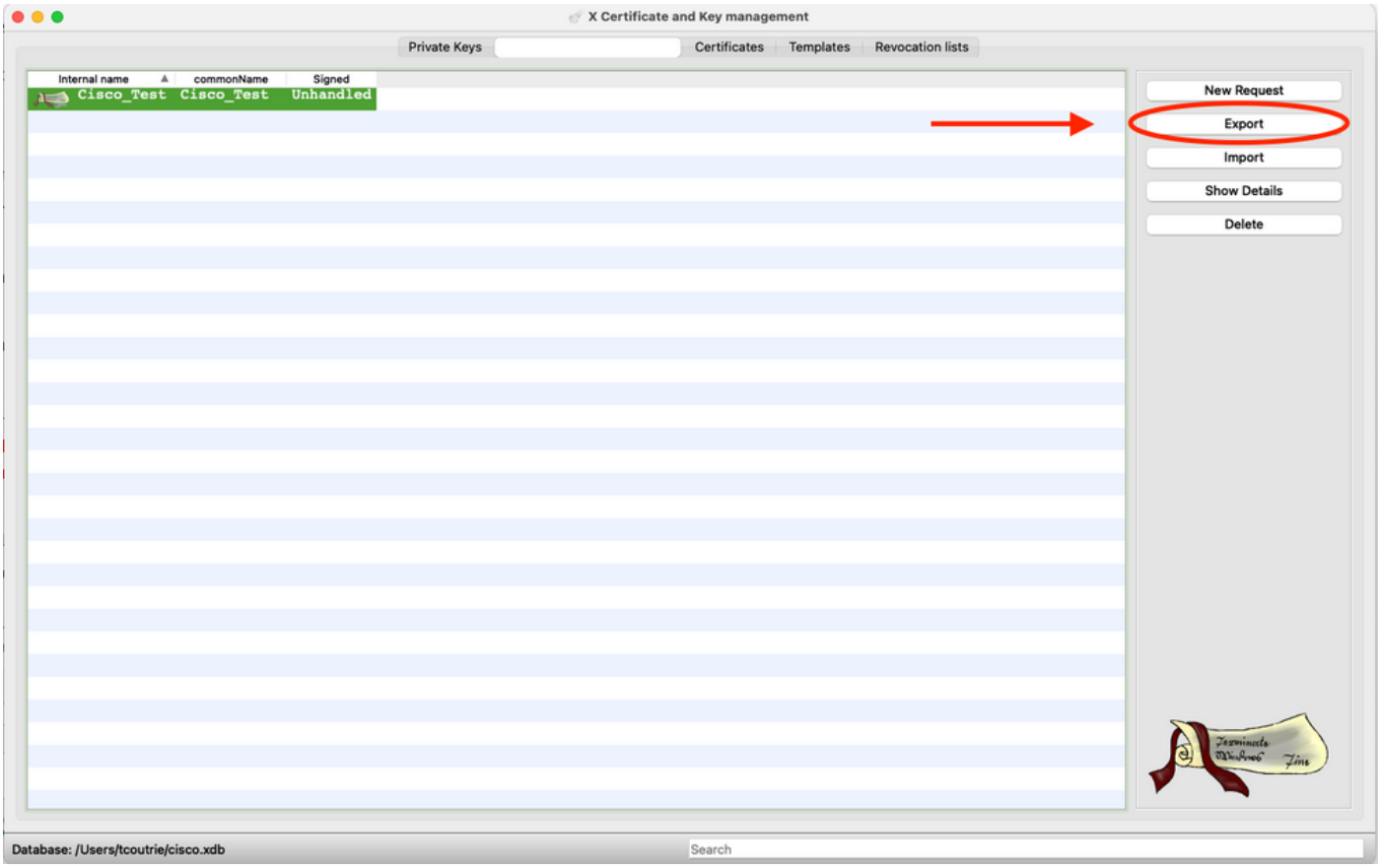


Nota: Este documento utiliza el CN del certificado.

Paso 3. Enviar CSR

a. Exportar CSR

b. Enviar CSR a CA para obtener un certificado nuevo

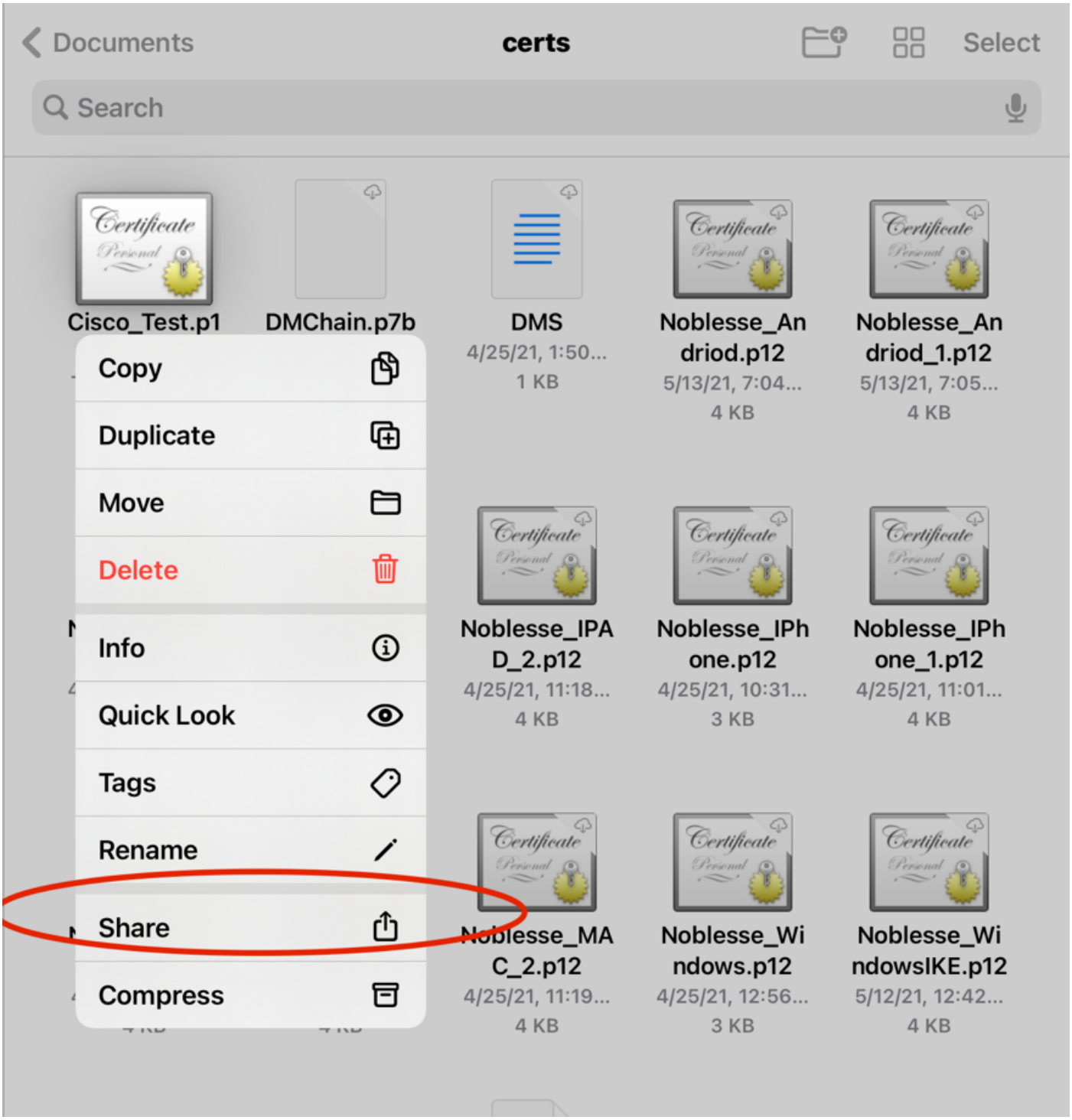


Nota: Utilice el formato PEM de la CSR.

Instalación en dispositivo móvil

Paso 1. Agregue el certificado del dispositivo al dispositivo móvil.
Paso 2. Comparta el certificado con la aplicación Anyconnect para agregar la nueva aplicación de certificado.

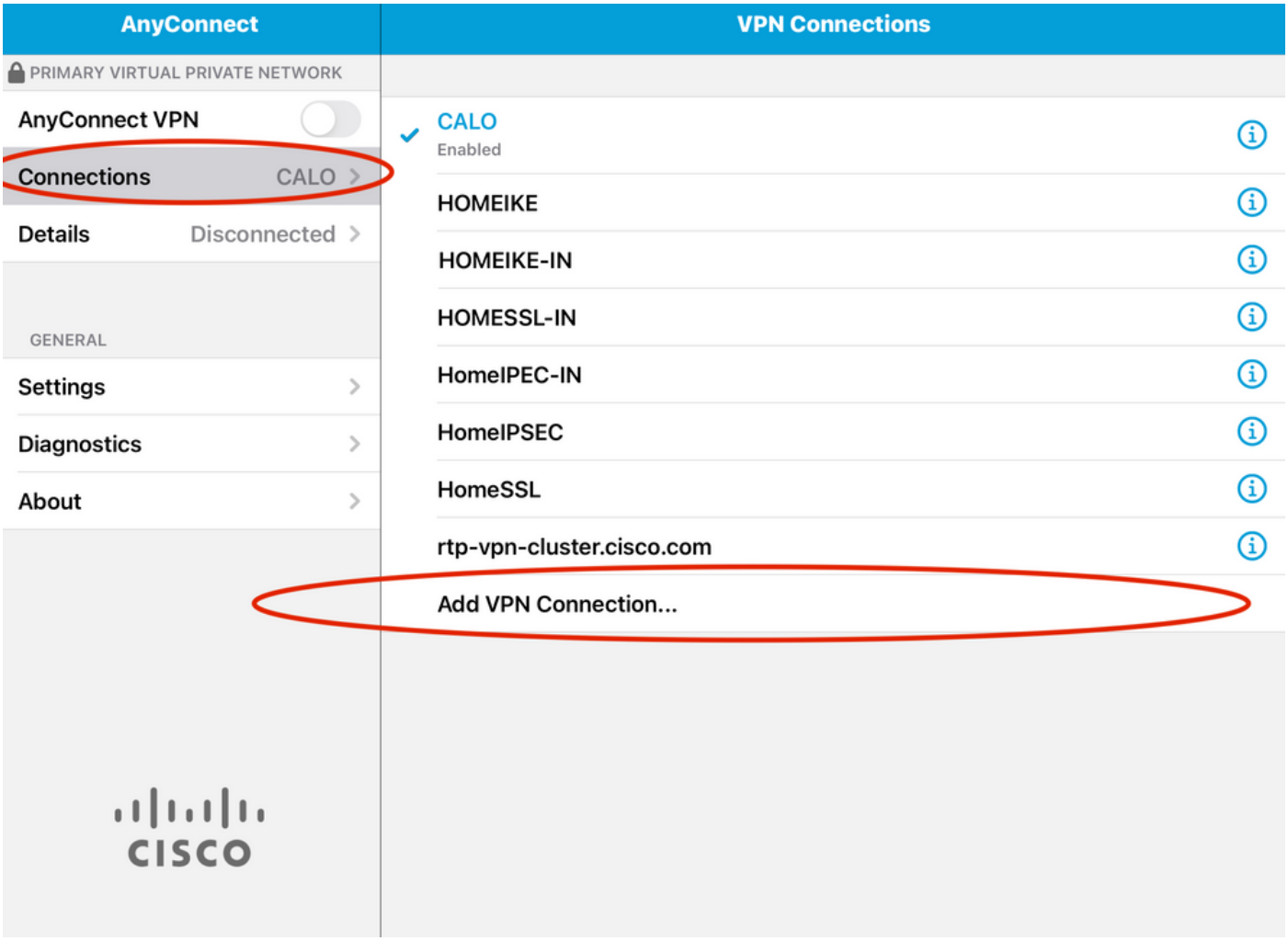
Precaución: La instalación manual requiere que el usuario comparta el certificado con la aplicación. Esto no se aplica a los certificados enviados a través de MDM.



Paso 3. Introduzca la contraseña del certificado para el archivo **PKCS12**.

Paso 4. Cree una nueva conexión en Anyconnect.

Paso 5. Navegar a nuevas conexiones; **Conexiones > Agregar conexión VPN**.



Paso 6. Introduzca la información de la nueva conexión.

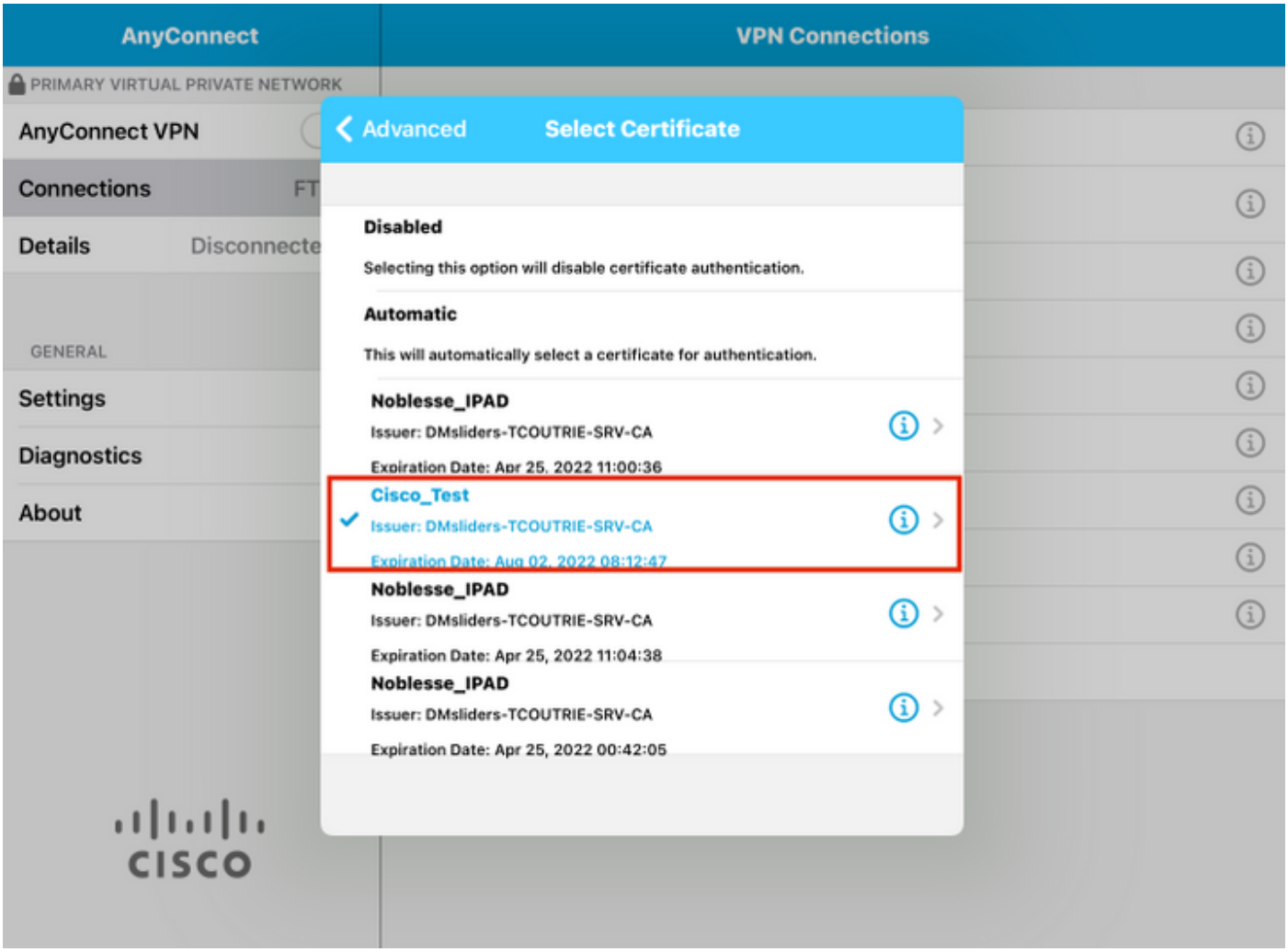
Descripción: Nombre de la conexión

Dirección del servidor: Dirección IP o FQDN de FTD

Avanzado: Configuraciones adicionales

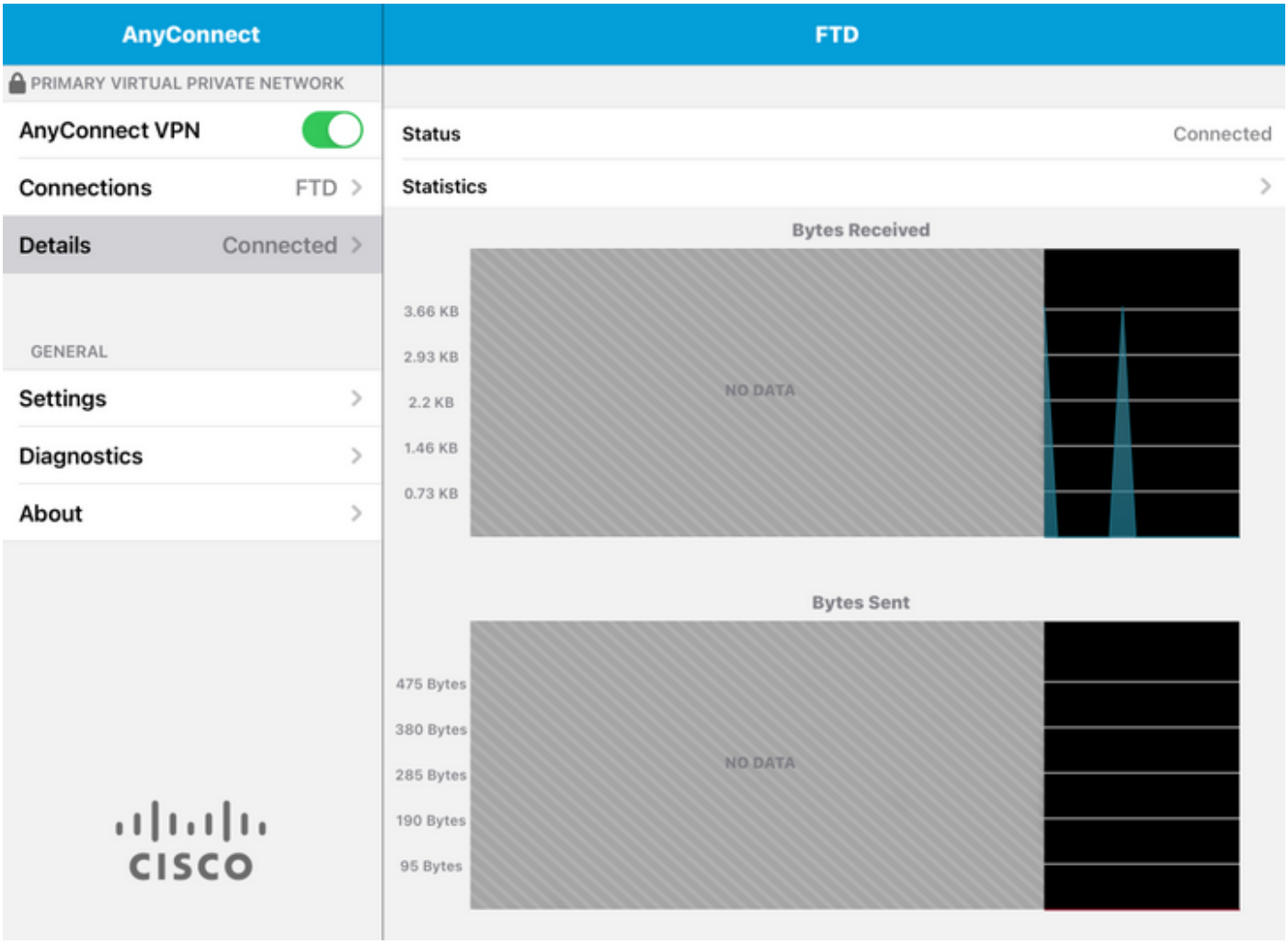
Paso 7. Elija **Advanced**.

Paso 8. Elija **Certificate** y elija su certificado recién agregado.



Paso 9. Vuelva a **Conexiones** y realice la prueba.

Una vez que se ha realizado correctamente, la alternancia permanece activa y los detalles se muestran en el estado conectado.



Verificación

El comando **show vpn-sessiondb detail Anyconnect** muestra toda la información sobre el host conectado.

> **Consejo:** La opción para filtrar este comando más a fondo son las palabras clave 'filter' o 'sort' agregadas al comando.

Por ejemplo:

```
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
```

Troubleshoot

Depuraciones

Las depuraciones necesarias para solucionar este problema son:

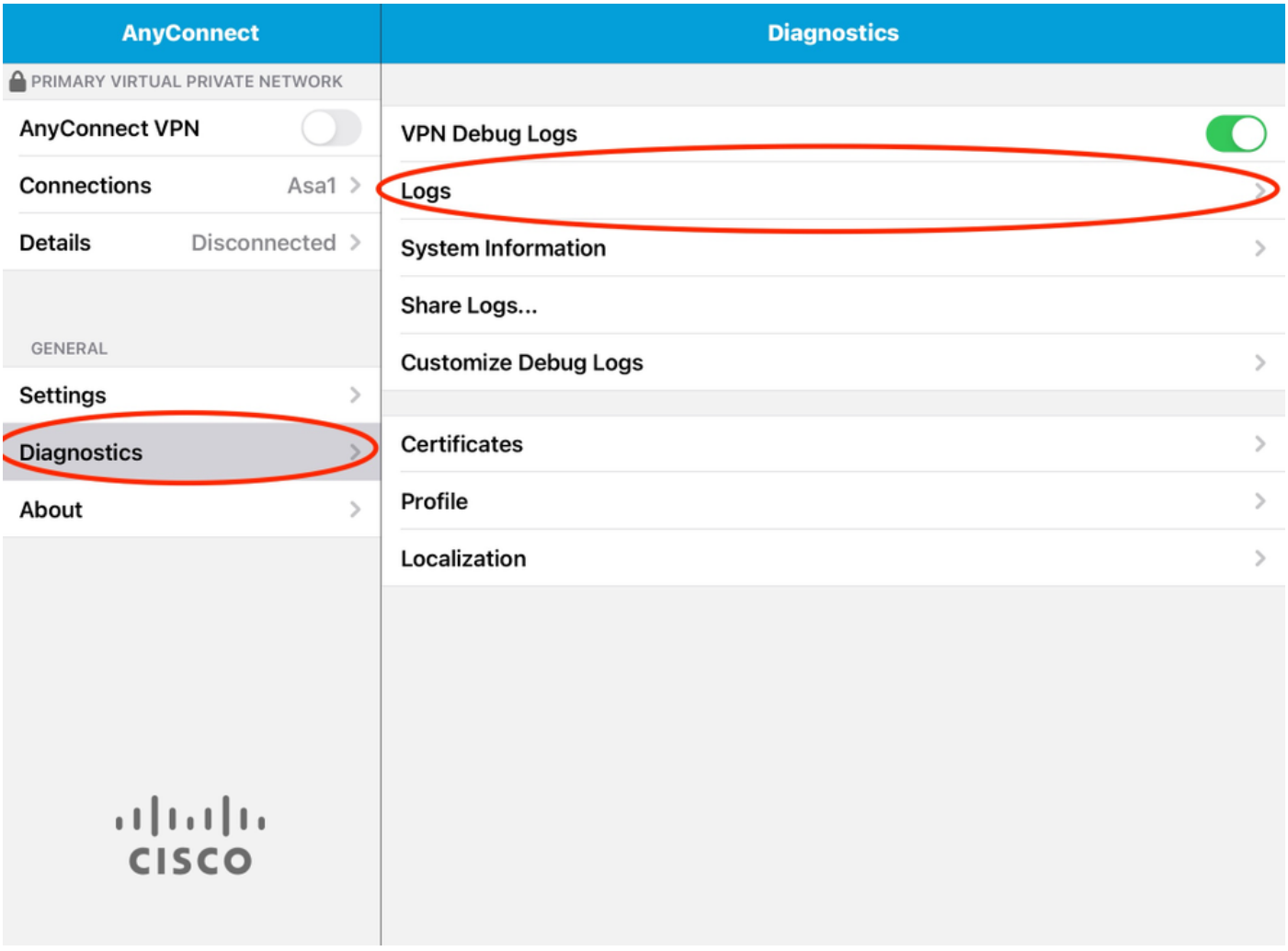
```
Debug crypto ca 14 Debug webvpn 255 Debug webvpn Anyconnect 255
```

Si la conexión es IPSEC y no SSL:

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

Registros de la aplicación móvil Anyconnect:

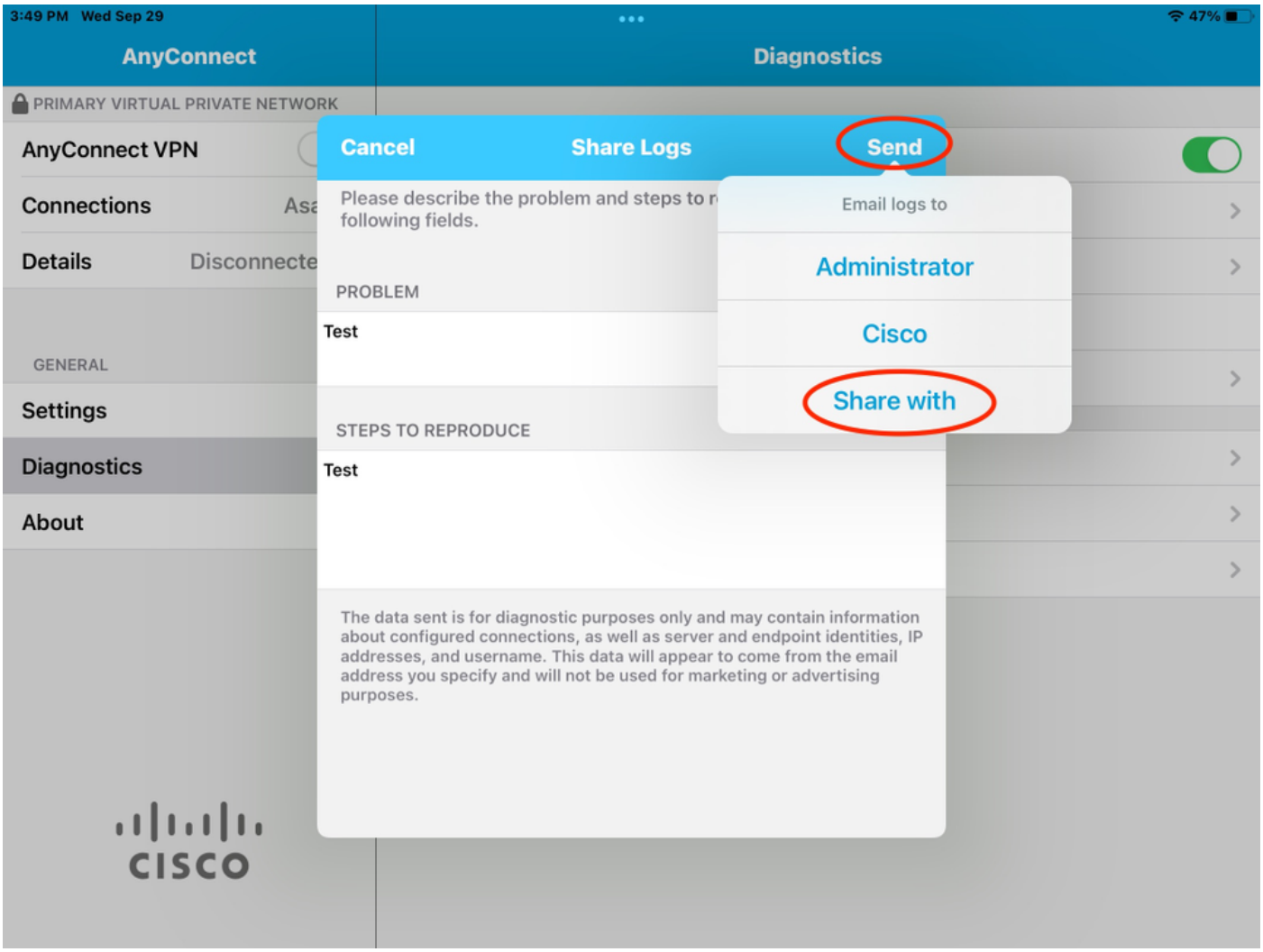
Vaya a **Diagnostic > VPN Debug Logs > Share logs**.



Introduzca la información:

- Problema
- Pasos para reproducir

A continuación, navegue hasta **Enviar > Compartir con**.



Esto presenta la opción de utilizar un cliente de correo electrónico para enviar los registros.