

Configurazione dell'autenticazione basata sul certificato Anyconnect per l'accesso mobile

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione di Cisco Anyconnect su FTD](#)

[Esempio di rete](#)

[Aggiungi certificato a FTD](#)

[Configurazione Di Cisco Anyconnect](#)

[Crea certificato per utenti mobili](#)

[Installa nel dispositivo mobile](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Debug](#)

Introduzione

Questo documento descrive un esempio di implementazione dell'autenticazione basata su certificati su dispositivi mobili.

Prerequisiti

Gli strumenti e i dispositivi utilizzati nella guida sono:

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

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VPN di base
- SSL/TLS
- Infrastruttura a chiave pubblica
- Esperienza con FMC

- OpenSSL
- Cisco Anyconnect

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

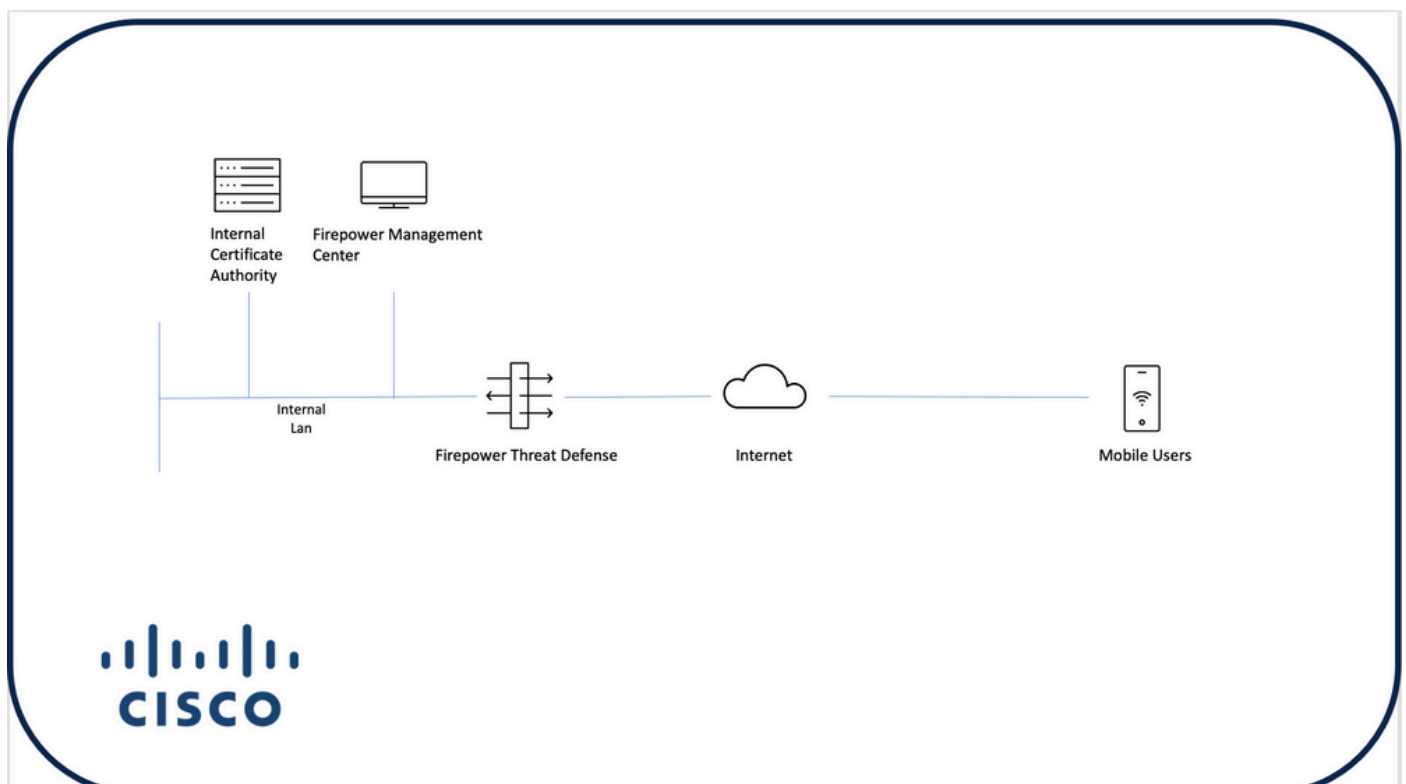
- Cisco FTD
- Cisco FMC
- Server CA Microsoft
- XCA
- Cisco Anyconnect
- Ipad Apple

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione di Cisco Anyconnect su FTD

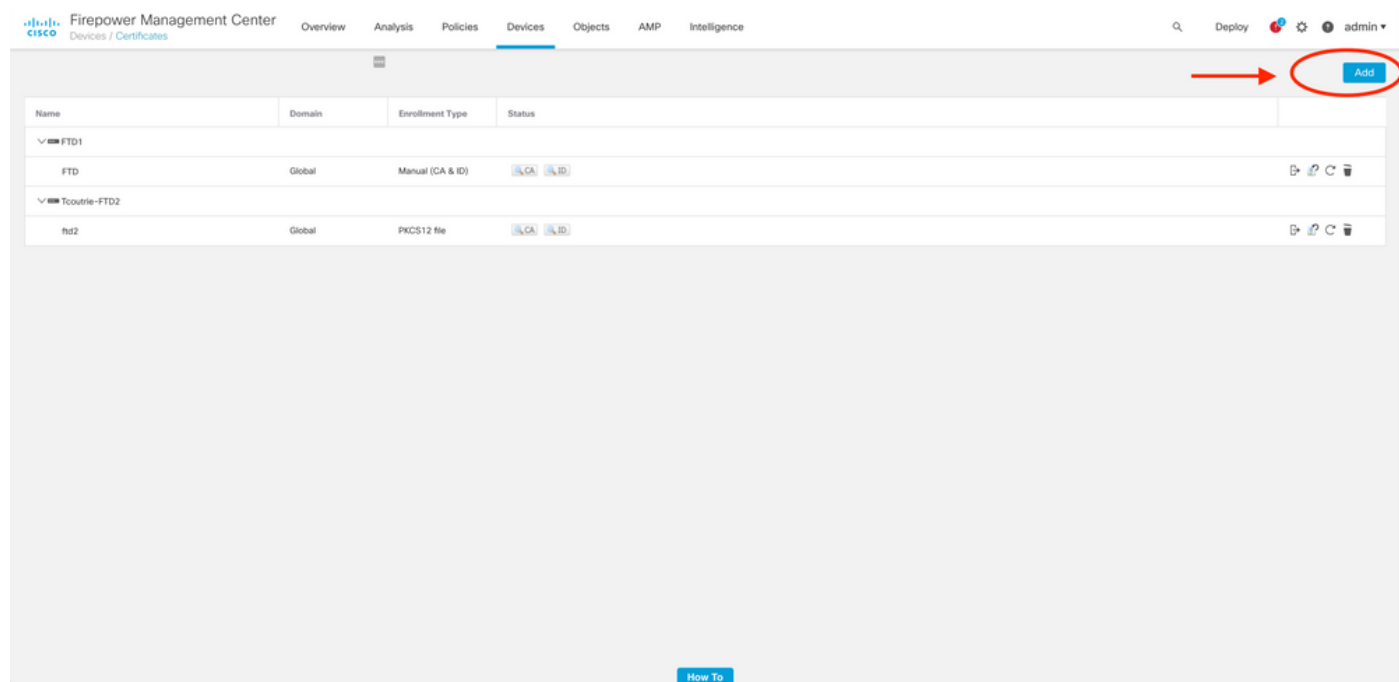
In questa sezione viene descritto come configurare Anyconnect tramite FMC. Prima di iniziare, assicurarsi di distribuire tutte le configurazioni.

Esempio di rete

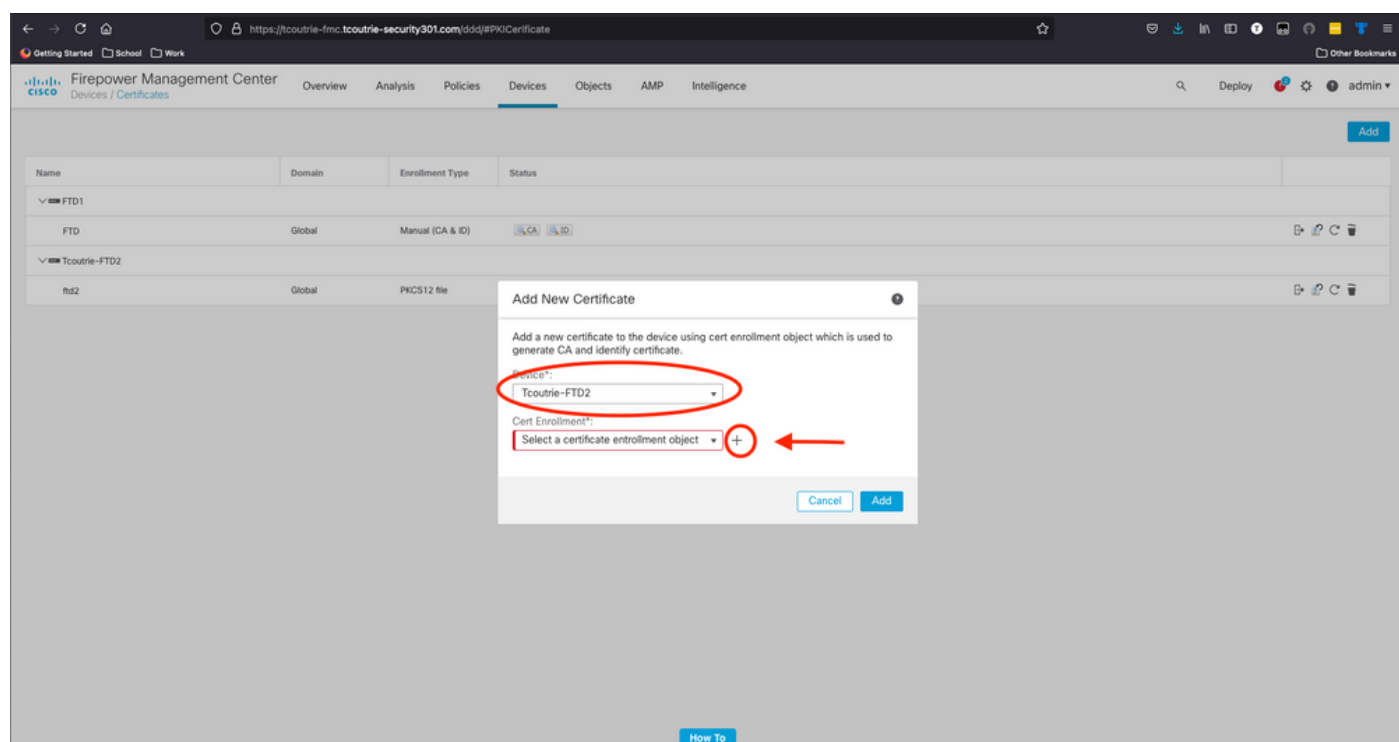


Aggiungi certificato a FTD

Passaggio 1. Creare un certificato per l'FTD sull'accessorio FMC. Passare a Dispositivi > Certificato e scegliere Aggiungi, come mostrato nell'immagine:




Passaggio 2. Scegliere l'FTD desiderato per la connessione VPN. Selezionare l'accessorio FTD dal menu a discesa dei dispositivi. Fare clic sull'icona + per aggiungere un nuovo metodo di registrazione dei certificati, come mostrato nell'immagine seguente:

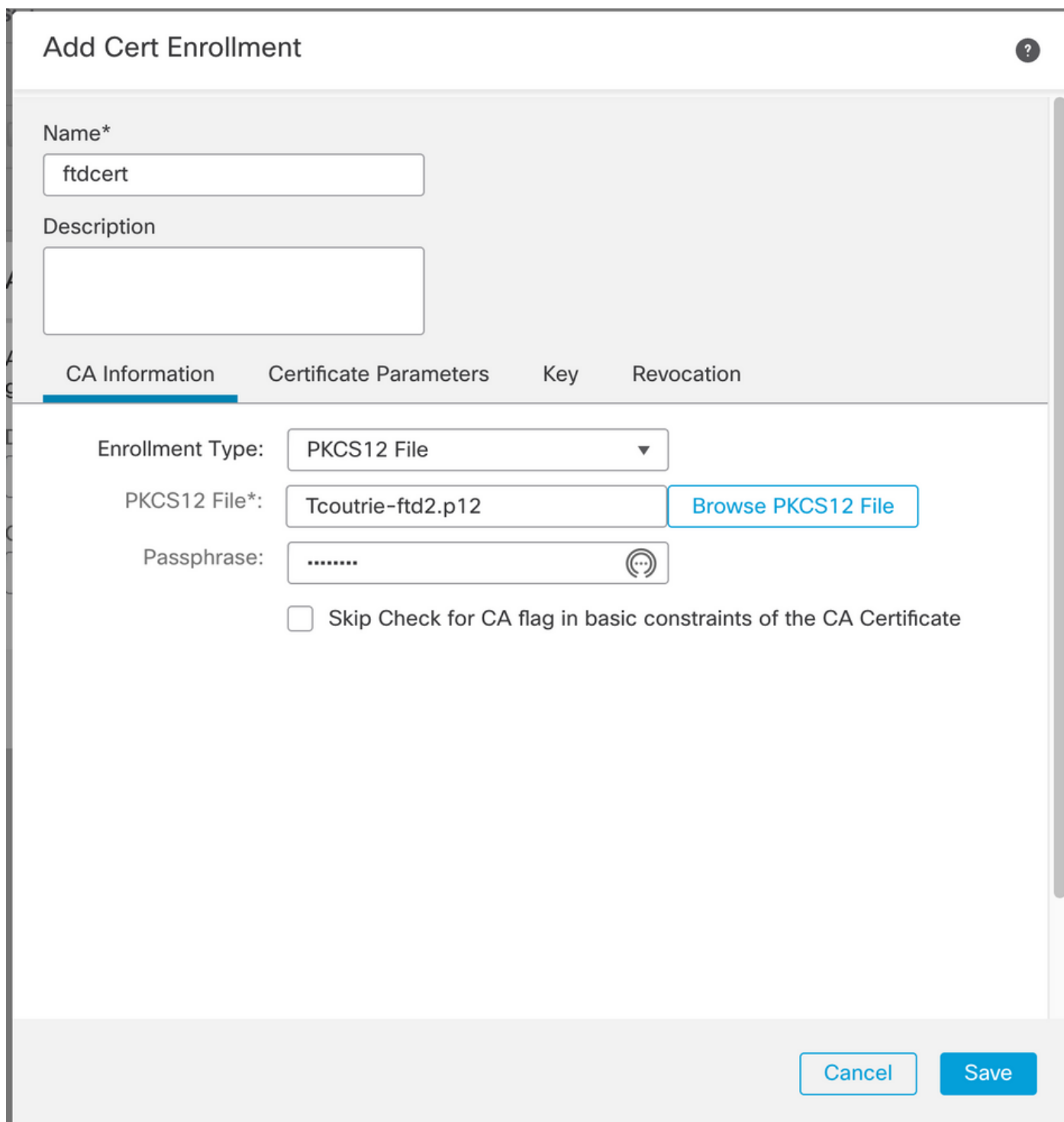


Passaggio 3. Aggiungere i certificati al dispositivo. Scegliere l'opzione che rappresenta il metodo

preferito per ottenere i certificati nell'ambiente.

 Suggerimento: le opzioni disponibili sono: Certificato autofirmato - Genera un nuovo certificato localmente, SCEP - Usa protocollo SCEP (Simple Certificate Enrollment Protocol) per ottenere un certificato da una CA, Manuale - Installa manualmente il certificato radice e identità, PKCS12 - Carica il bundle di certificati crittografati con radice, identità e chiave privata.

Passaggio 4. Caricare il certificato sul dispositivo FTD. Immettere il passcode (solo PKCS12) e fare clic su Save (Salva), come mostrato nell'immagine:



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](#)

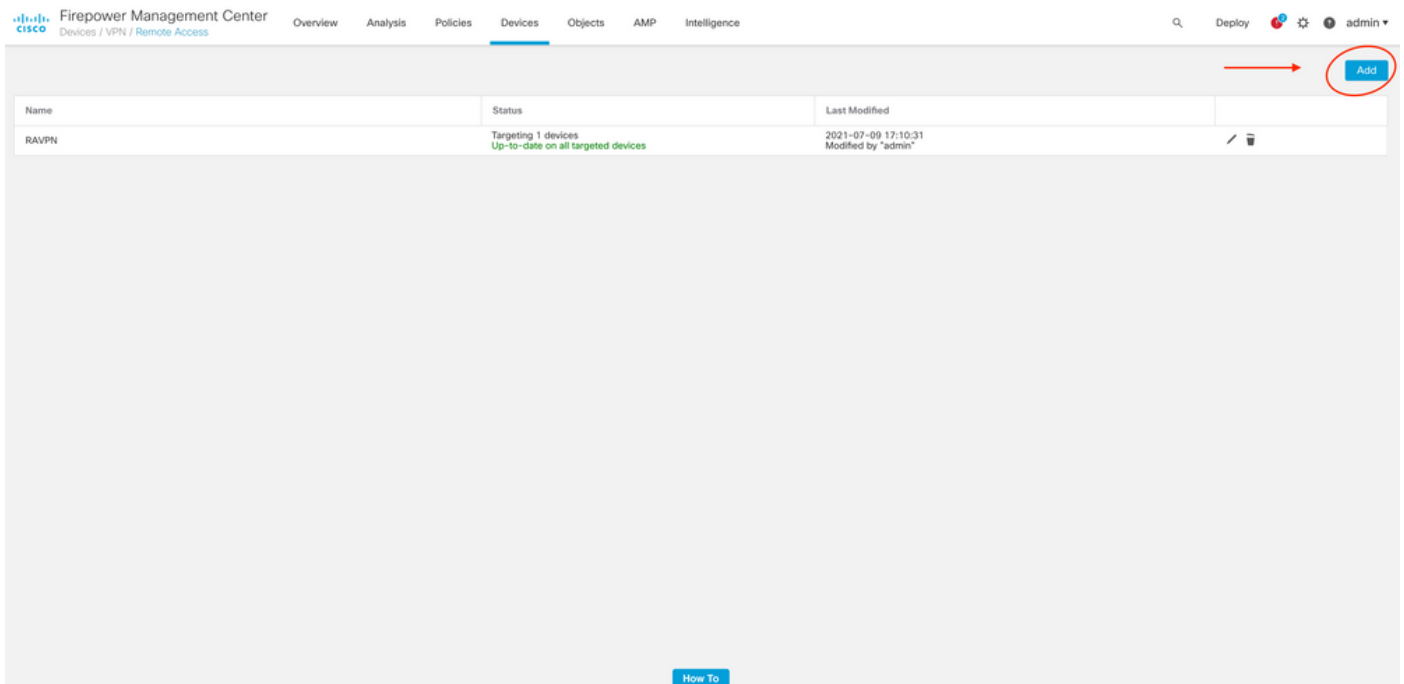
 Nota: una volta salvato il file, la distribuzione dei certificati viene eseguita immediatamente.
Per visualizzare i dettagli del certificato, scegliere l'ID.

Configurazione Di Cisco Anyconnect

Configurare Anyconnect tramite FMC con la procedura guidata di accesso remoto.

Passaggio 1. Avvia la Configurazione guidata criteri VPN di Accesso remoto per configurare Anyconnect.

Passare a Dispositivi > Accesso remoto e scegliere Aggiungi.



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

Passaggio 2. Assegnazione criteri.

Completare l'assegnazione dei criteri:

- Assegnare un nome al criterio.
- Scegliere i protocolli VPN desiderati.
- Scegliere il dispositivo di destinazione per applicare la configurazione.

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

Search

FTD1

Tcourtie-FTD2

Add

Selected Devices

Tcourtie-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 [RADIUS](#) 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

Cancel Back Next

Passaggio 3. Profilo di connessione.

- Assegnare un nome al profilo di connessione.
- Impostare il metodo di autenticazione su Solo certificato client.
- Assegnare un pool di indirizzi IP e, se necessario, creare un nuovo oggetto Criteri di gruppo.
- Fare clic su Next (Avanti).

Remote Access VPN Policy Wizard

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

Remote User AnyConnect Client Internet 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 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

 Nota: scegliere il campo Principale da utilizzare per immettere il nome utente per le sessioni di autenticazione. In questa guida viene utilizzato il CN del certificato.

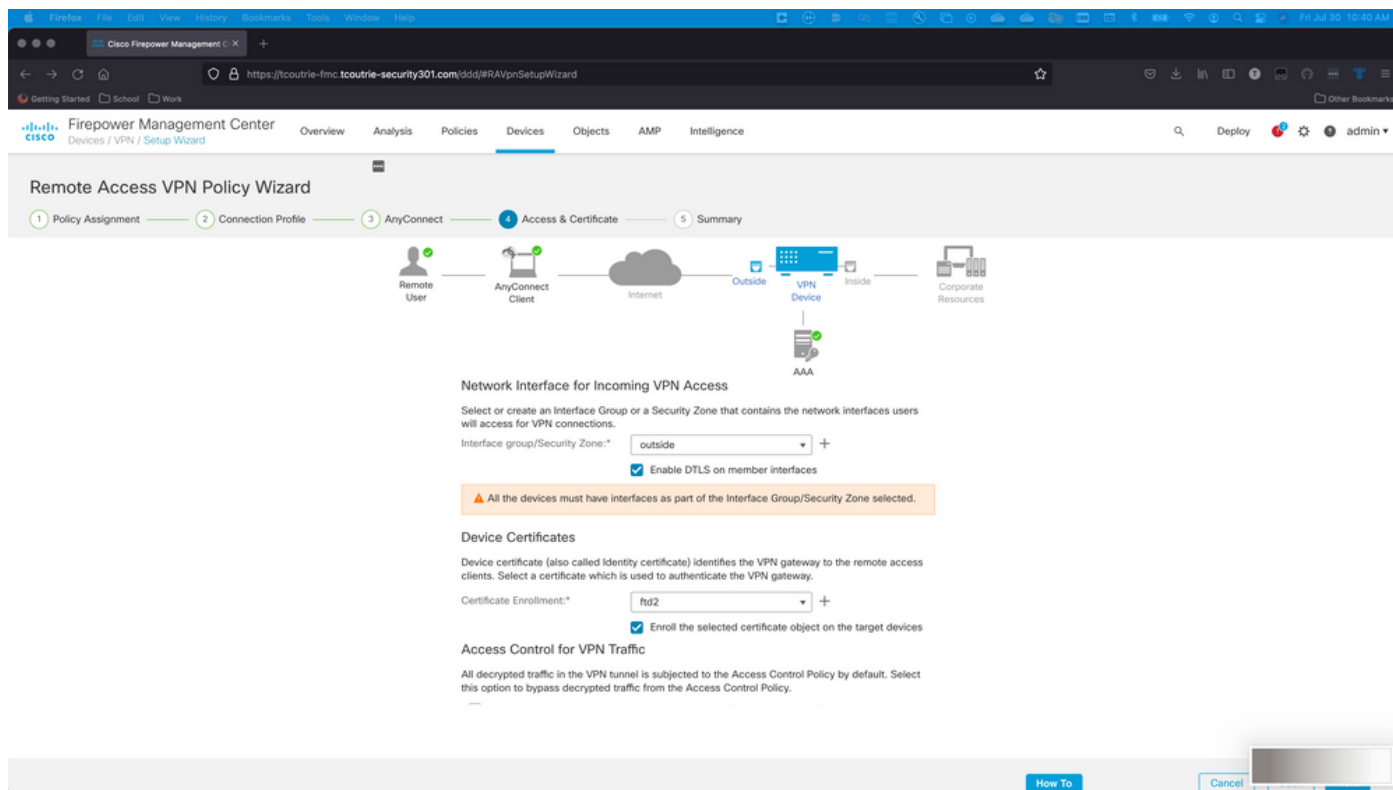
Passaggio 4. AnyConnect.

Aggiungere un'immagine Anyconnect all'accessorio. Caricare la versione preferita di Anyconnect e fare clic su Avanti.

 Nota: i pacchetti Cisco Anyconnect possono essere scaricati da [Software.Cisco.com](https://www.cisco.com).

Passaggio 5. Accesso e certificato.

Applicare il certificato a un'interfaccia e abilitare Anyconnect a livello di interfaccia, come mostrato nell'immagine, e fare clic su Avanti.



Passaggio 6. Riepilogo.

Esaminare le configurazioni. Se tutte le estrazioni sono state eseguite, fare clic su fine, quindi su distribuisci.

Crea certificato per utenti mobili

Creare un certificato da aggiungere al dispositivo mobile utilizzato nella connessione.

Passaggio 1. XCA

a. Apri XCA

b. Avvia un nuovo database

Passaggio 2. Creare CSR.

a. Scegliere Richiesta firma certificato (CSR)

- b. Scegli nuova richiesta
- c. Inserire il valore con tutte le informazioni necessarie per il certificato
- d. Genera una nuova chiave
- e. Al termine, fare clic su OK

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

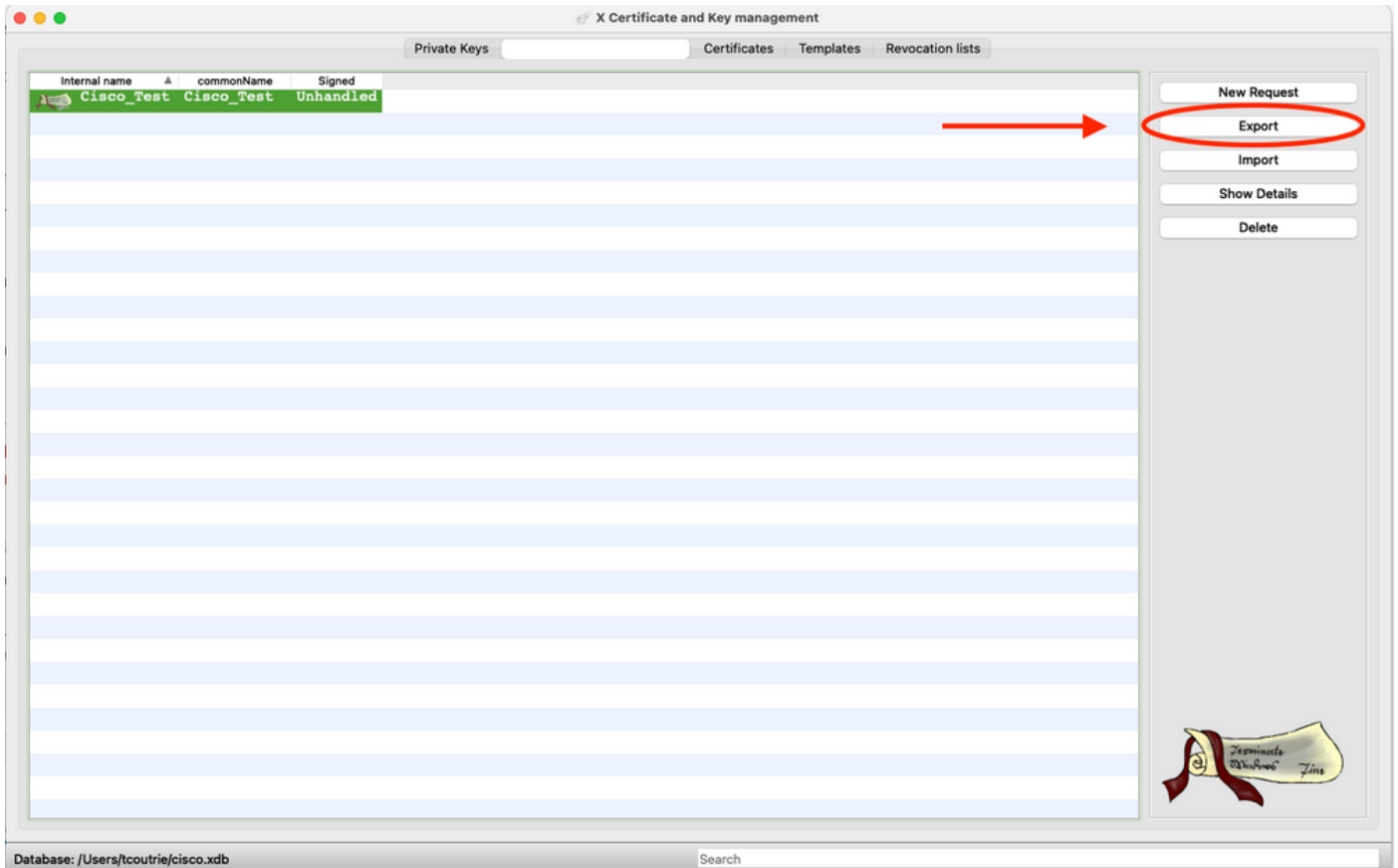
Cisco_Test_1 (RSA:2048 bit) Used keys too

Cancel OK

Nota: questo documento utilizza il CN del certificato.

Passaggio 3. Inviare CSR.

- a. Esportazione del CSR
- b. Inviare CSR a CA per ottenere un nuovo certificato




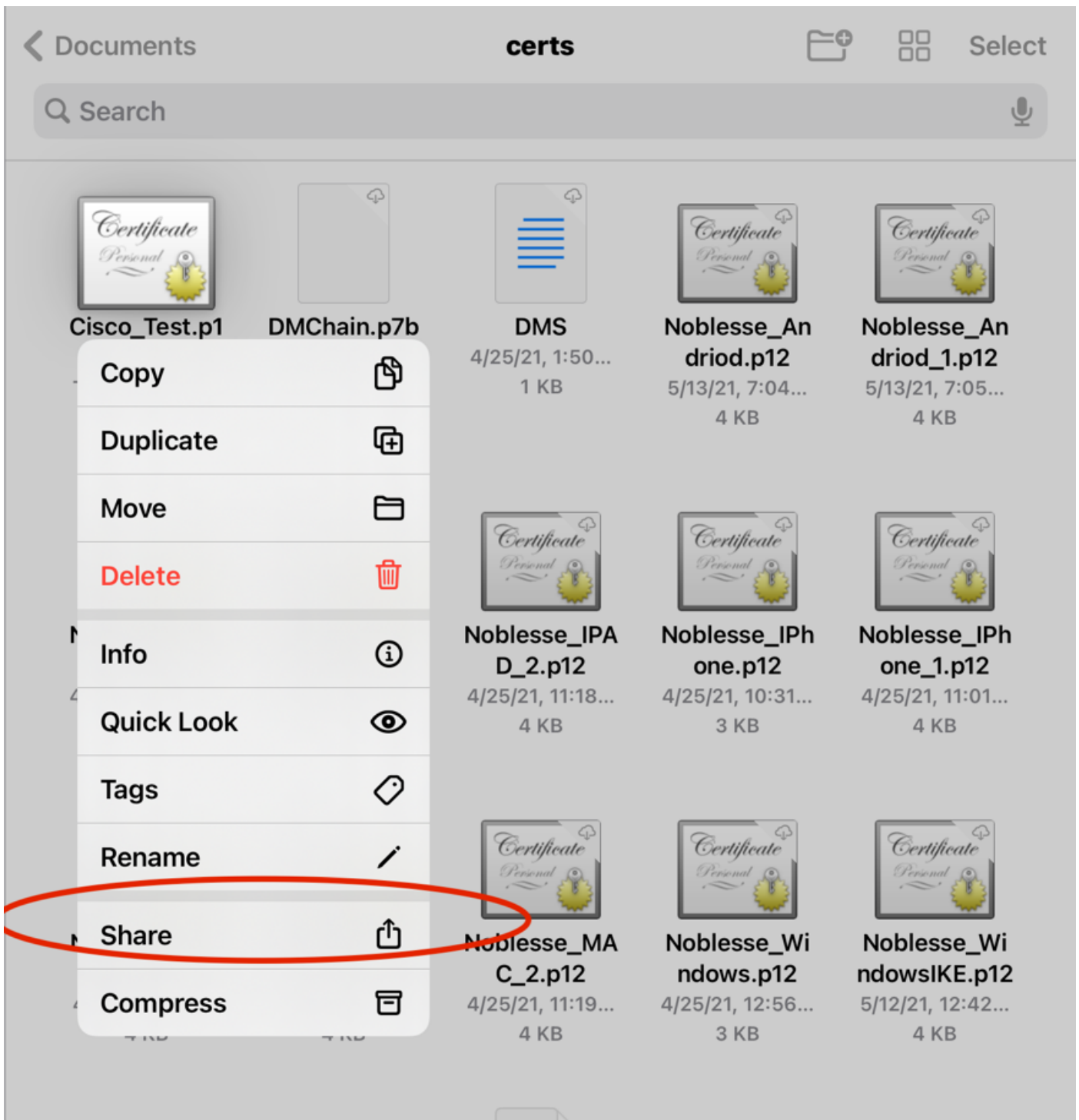
 Nota: utilizzare il formato PEM del CSR.

Installa nel dispositivo mobile

Passaggio 1. Aggiungere il certificato del dispositivo al dispositivo mobile.

Passaggio 2. Condividere il certificato con l'applicazione Anyconnect per aggiungere la nuova applicazione di certificato.

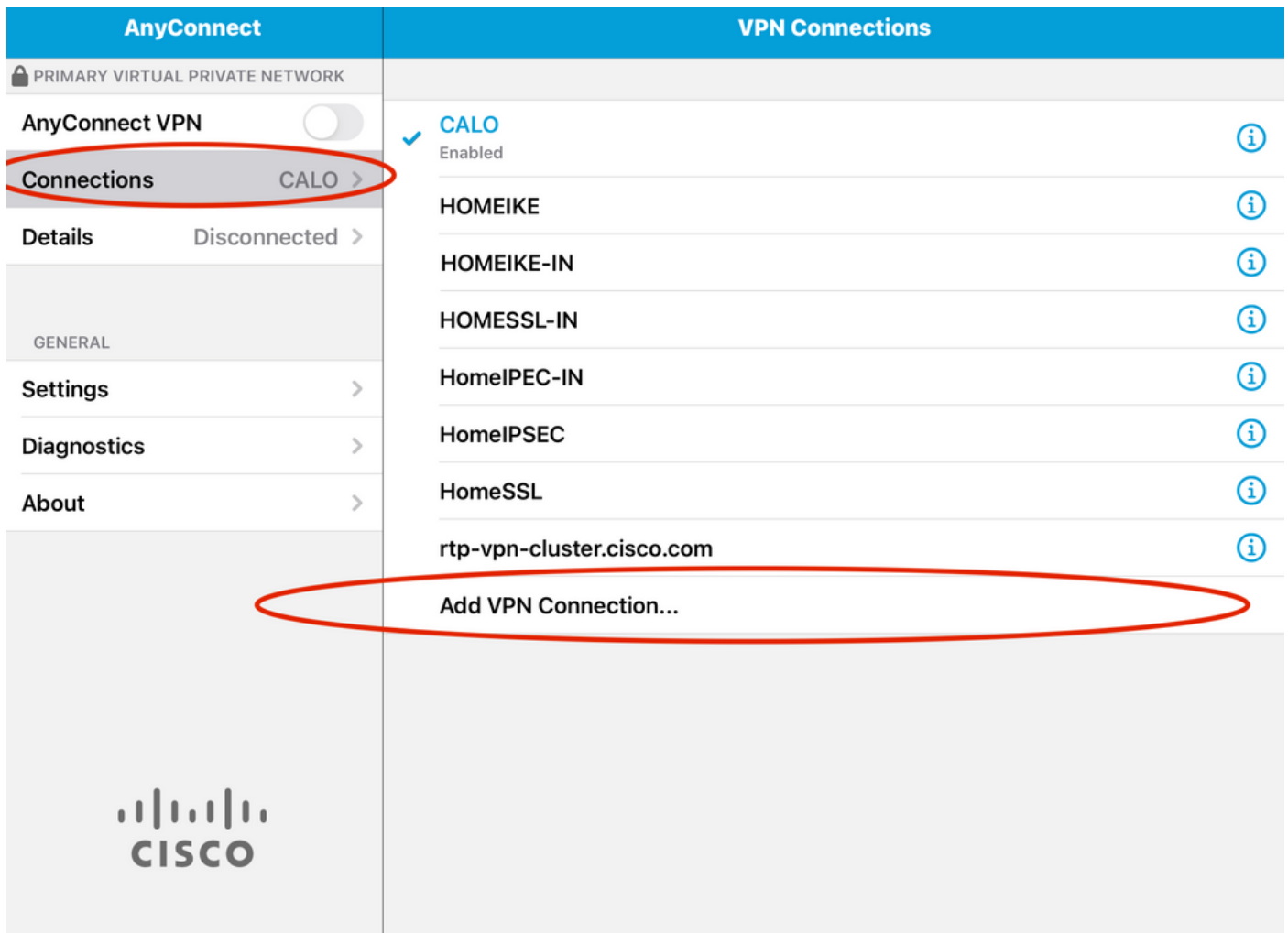
 **Attenzione:** l'installazione manuale richiede la condivisione del certificato con l'applicazione. Ciò non si applica ai certificati sottoposti a push tramite MDM.



Passaggio 3. Immettere la password del certificato per il file PKCS12.

Passaggio 4. Creare una nuova connessione su Anyconnect.

Passaggio 5. Passare a nuove connessioni; Connessioni > Aggiungi connessione VPN.



Passaggio 6. Immettere le informazioni per la nuova connessione.

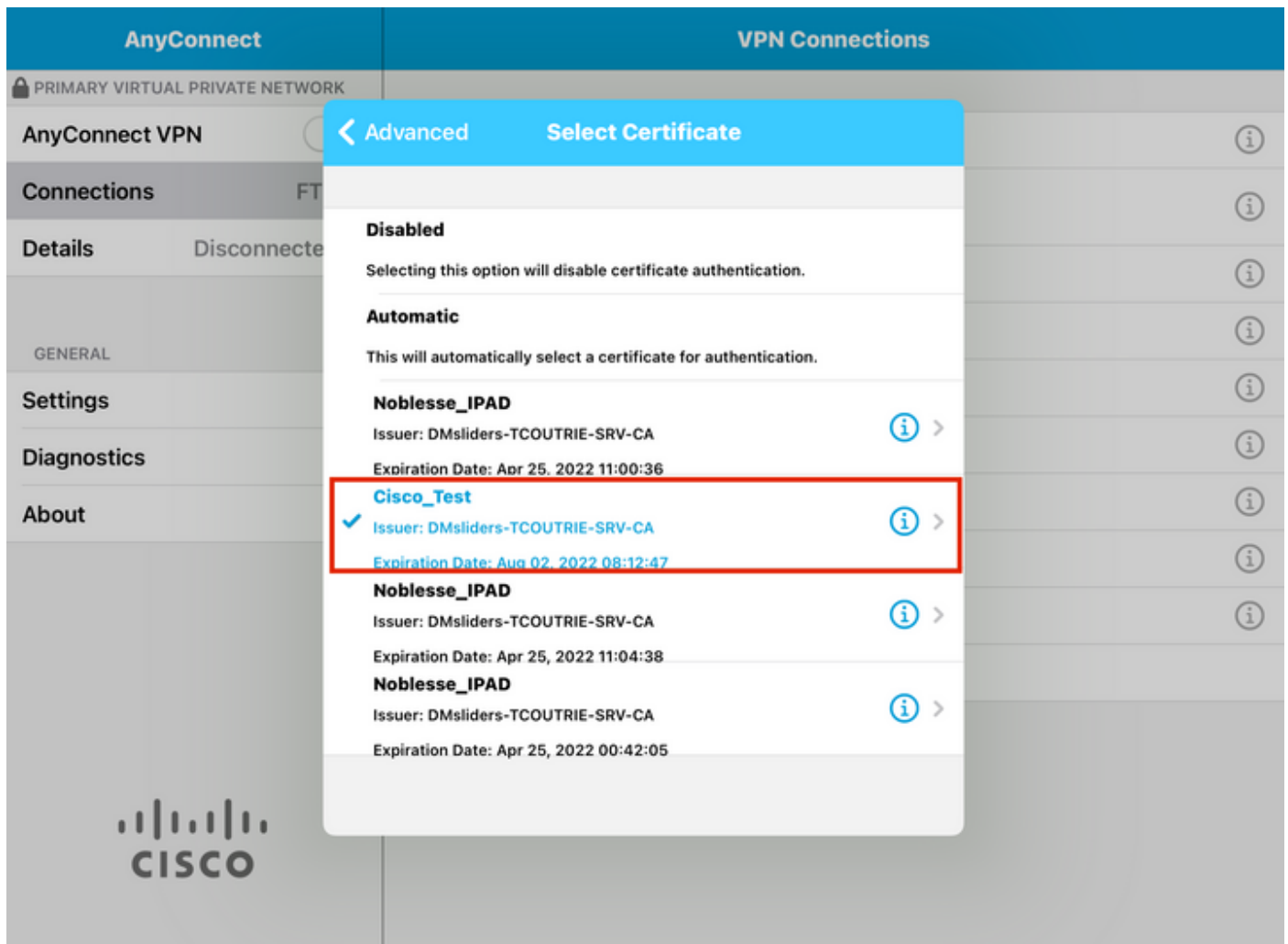
Descrizione: assegnare un nome alla connessione

Indirizzo server: indirizzo IP o FQDN FTD

Avanzate: configurazioni aggiuntive

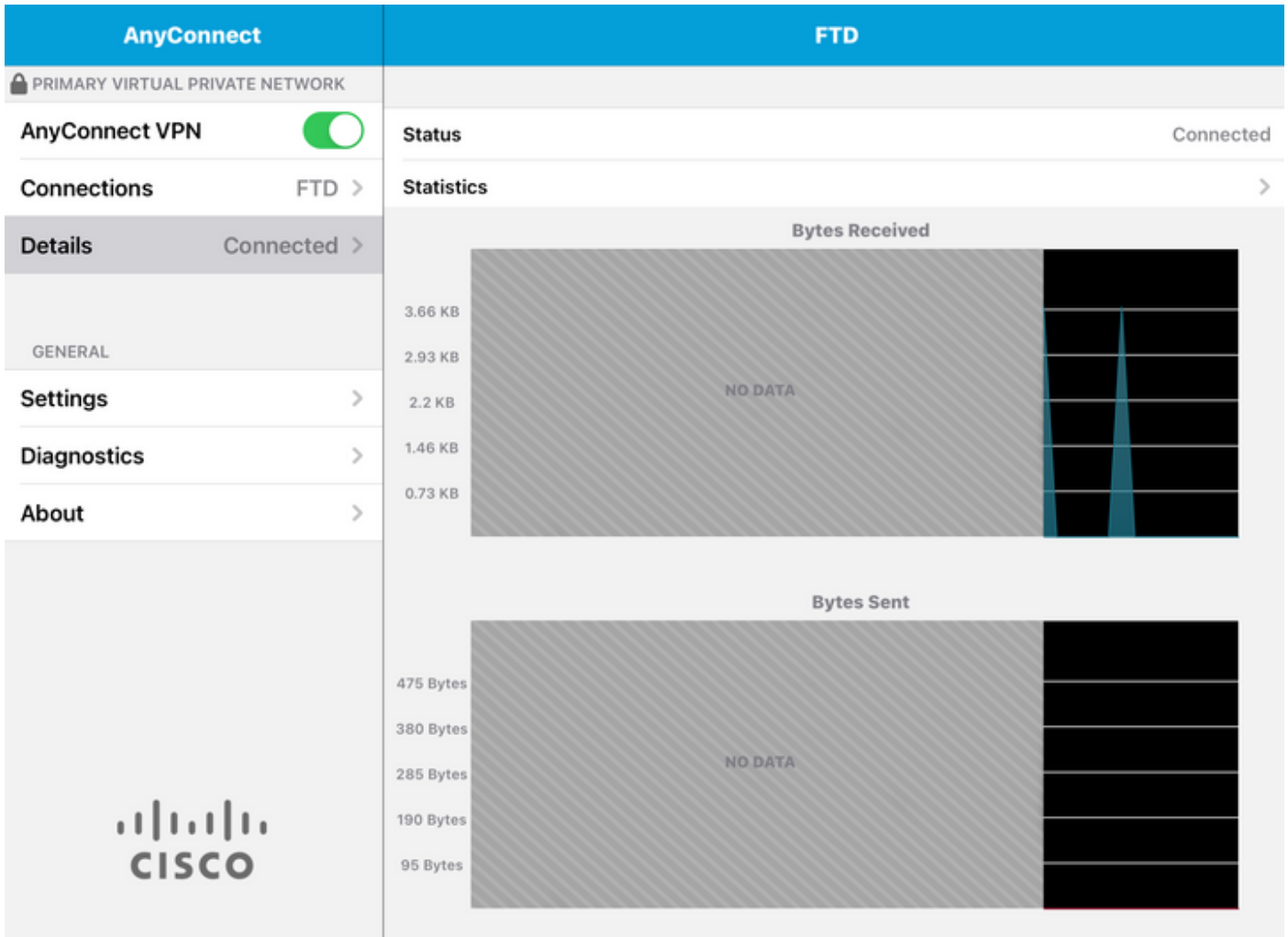
Passaggio 7. Scegliere Avanzate.

Passaggio 8. Scegliere Certificato e scegliere il certificato appena aggiunto.




Passaggio 9. Tornare a Connessioni e verificare.

Se l'operazione ha esito positivo, l'interruttore rimane acceso e i dettagli mostrano la connessione nello stato.



Verifica

Il comando `show vpn-sessiondb detail Anyconnect` permette di visualizzare tutte le informazioni sull'host connesso.

 Suggerimento: l'opzione per filtrare ulteriormente il comando è rappresentata dalle parole chiave 'filter' o 'sort' aggiunte al comando.

Ad esempio:

```
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

Risoluzione dei problemi

Debug

I debug necessari per risolvere il problema sono:

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

Se la connessione è IPSEC e non SSL:

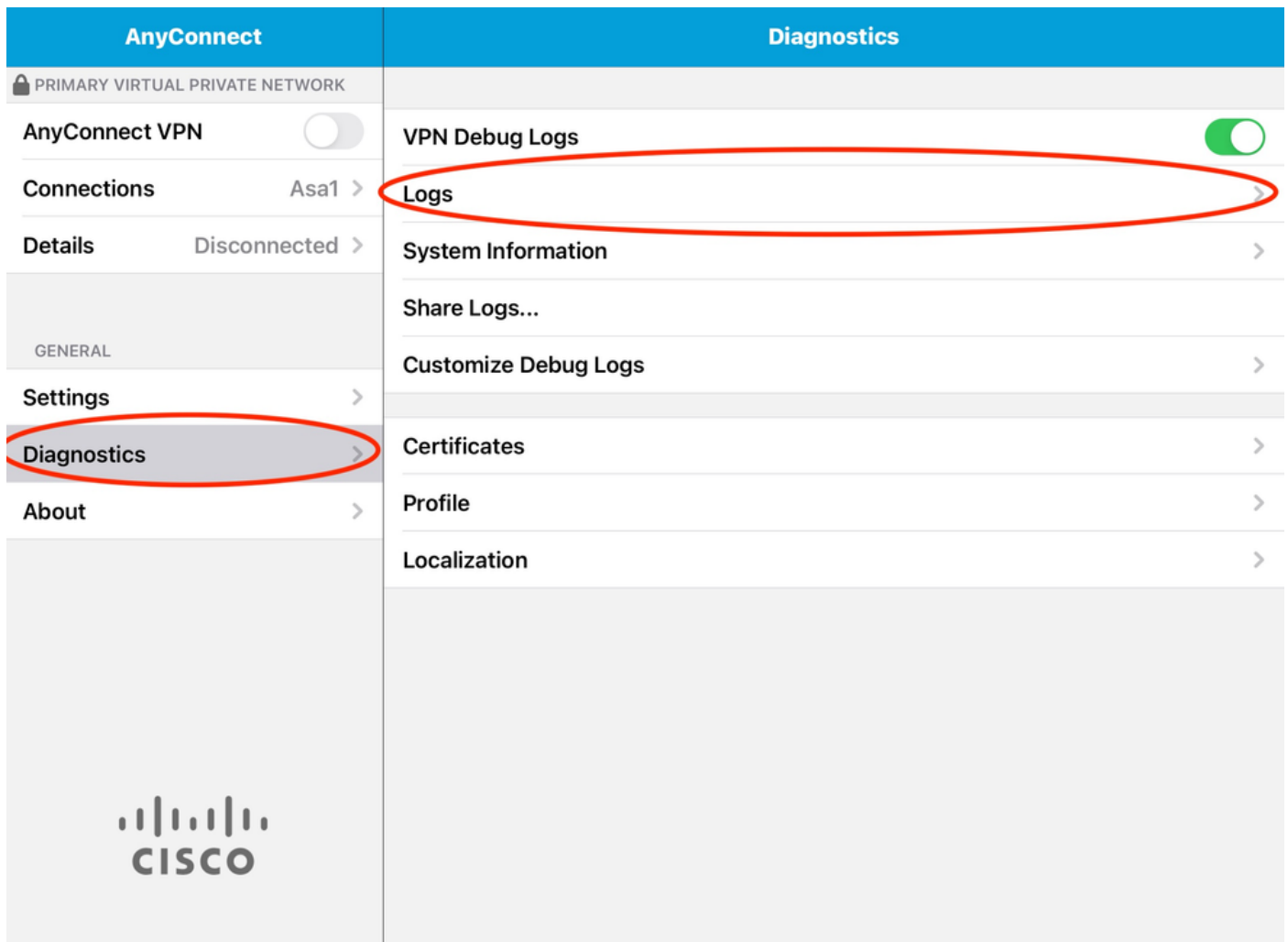
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

Registri dall'applicazione Anyconnect per dispositivi mobili:

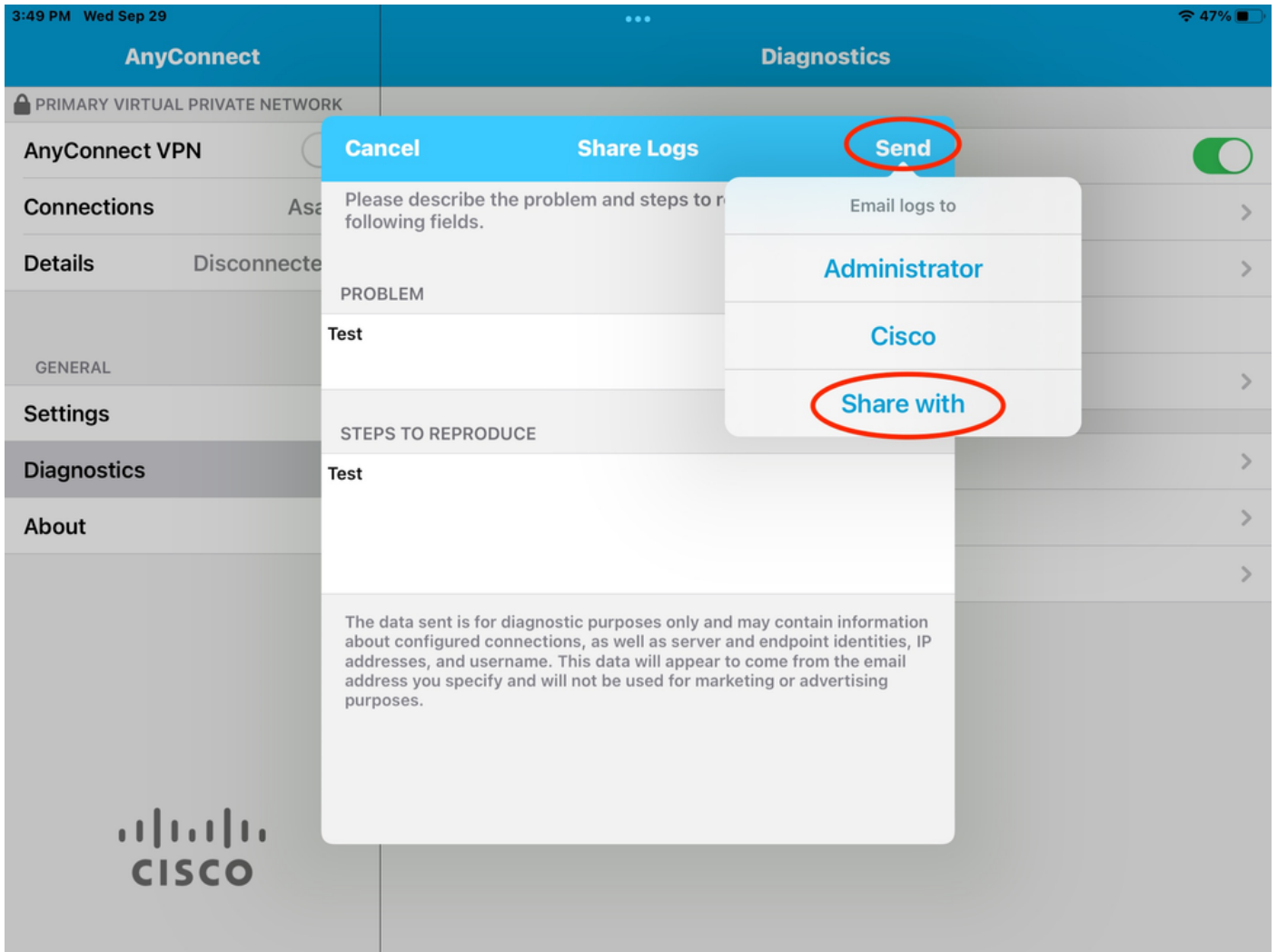
Selezionare Diagnostica > Log di debug VPN > Log di condivisione.



Immettere le informazioni:

- Problema
- Passi da riprodurre

Passare quindi a Invia > Condividi con.



In questo documento viene presentata l'opzione per l'utilizzo di un client di posta elettronica per l'invio dei log.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).