

# 모바일 액세스를 위한 Anyconnect 인증서 기반 인증 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[FTD에서 Cisco Anyconnect 구성](#)

[네트워크 다이어그램](#)

[FTD에 인증서 추가](#)

[Cisco Anyconnect 구성](#)

[모바일 사용자를 위한 인증서 만들기](#)

[모바일 장치에 설치](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[디버그](#)

---

## 소개

이 문서에서는 모바일 디바이스에서 인증서 기반 인증을 구현하는 예를 설명합니다.

## 사전 요구 사항

이 가이드에서 사용하는 도구 및 장치는 다음과 같습니다.

- Cisco FTD(Firepower 위협 방어)
- FMC(Firepower Management Center)
- Apple iOS 장치(iPhone, iPad)
- CA(인증 기관)
- Cisco Anyconnect 클라이언트 소프트웨어

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 VPN
- SSL/TLS
- 공개 키 인프라
- FMC 경험
- OpenSSL

- Cisco Anyconnect

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

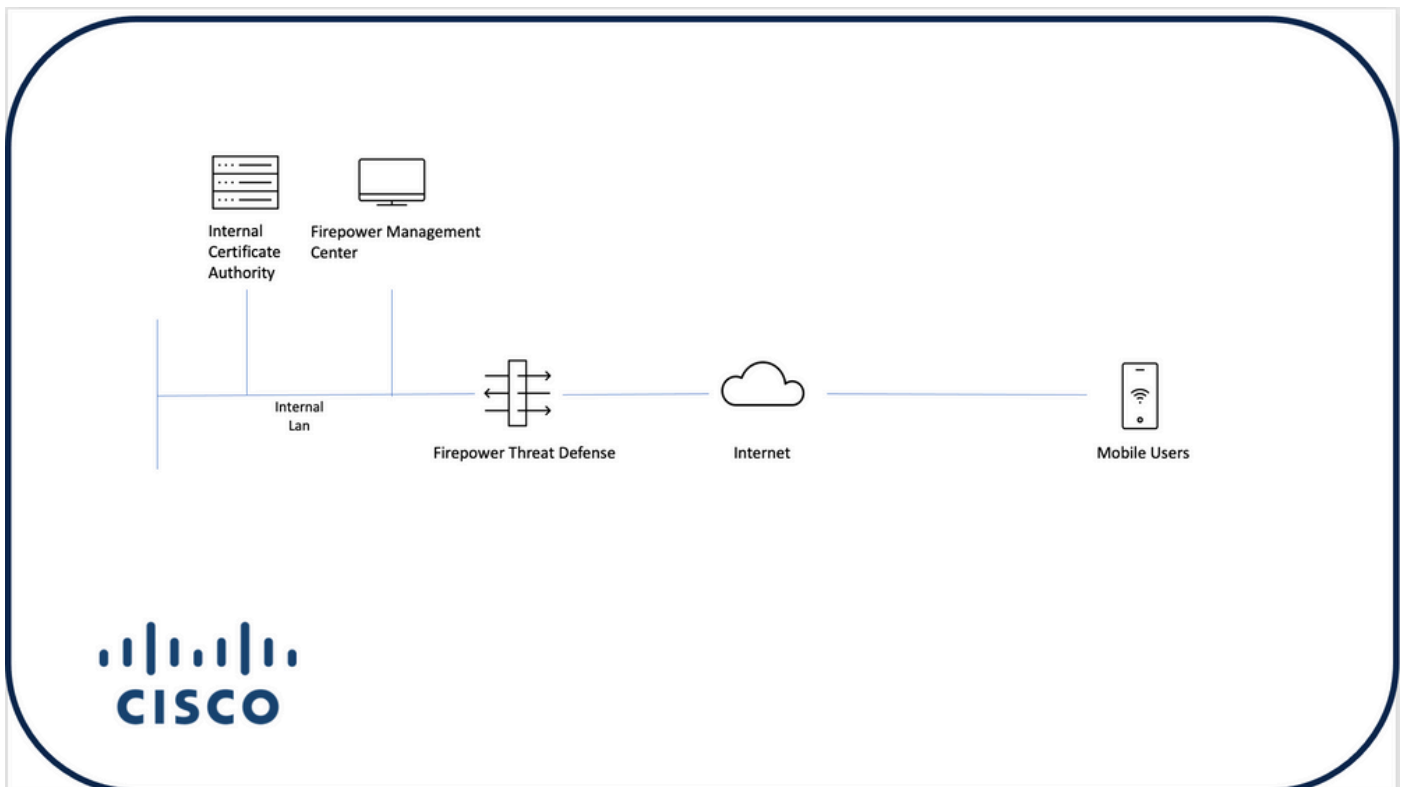
- Cisco FTD
- Cisco FMC
- Microsoft CA 서버
- XCA
- Cisco Anyconnect
- 애플 아이패드

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## FTD에서 Cisco Anyconnect 구성

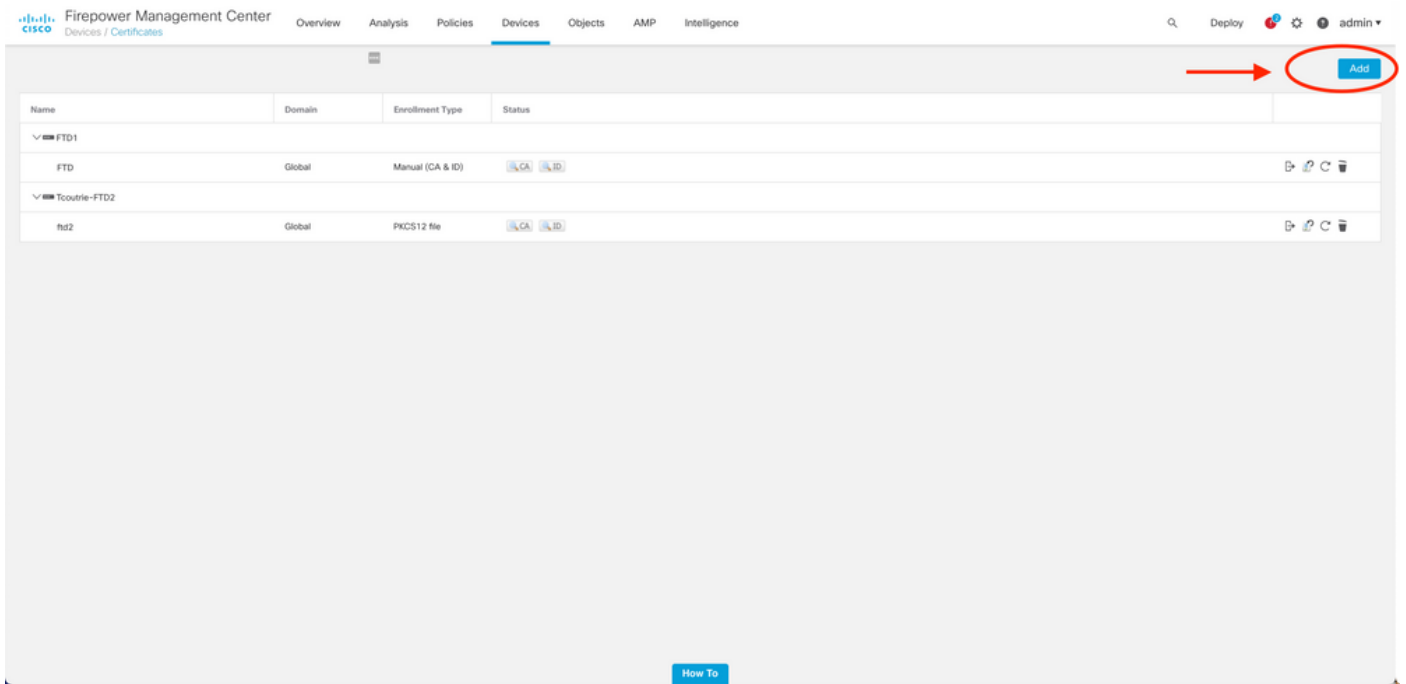
이 섹션에서는 FMC를 통해 Anyconnect를 구성하는 단계를 설명합니다. 시작하기 전에 모든 컨피그레이션을 구축해야 합니다.

### 네트워크 다이어그램

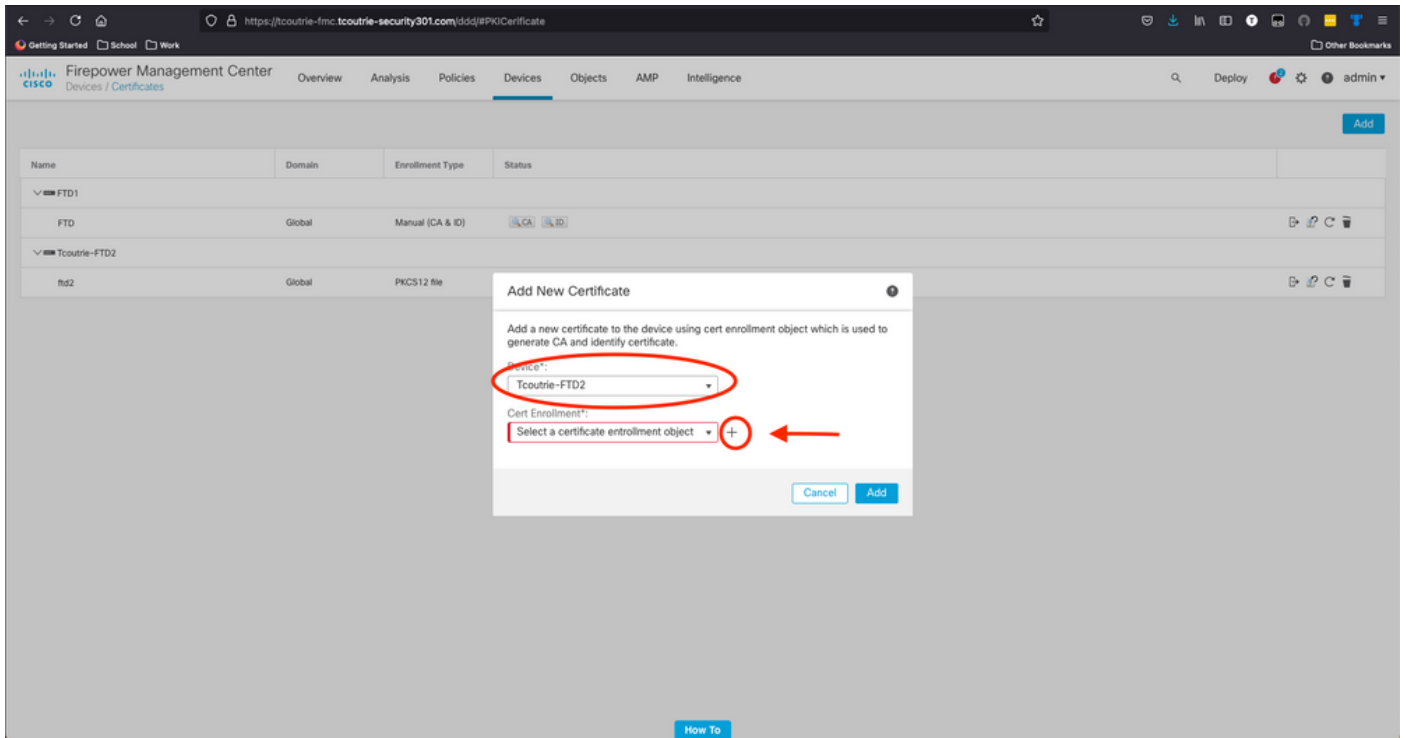


### FTD에 인증서 추가

1단계. FMC 어플라이언스에서 FTD에 대한 인증서를 생성합니다. 다음 이미지에 표시된 대로 Devices > Certificate(디바이스 > 인증서)로 이동하고 Add(추가)를 선택합니다.



2단계. VPN 연결에 필요한 FTD를 선택합니다. 디바이스 드롭다운에서 FTD 어플라이언스를 선택합니다. 다음 이미지에 표시된 것처럼 새 인증서 등록 방법을 추가하려면 + 아이콘을 클릭합니다.



3단계. 디바이스에 인증서를 추가합니다. 환경에서 인증서를 얻기 위해 선호하는 방법인 옵션을 선택합니다.

🔍 **팁:** 사용 가능한 옵션은 다음과 같습니다. Self Signed Certificate - Generate a new certificate locally(자체 서명 인증서 - 로컬에서 새 인증서 생성), SCEP - Use Simple Certificate Enrollment Protocol to obtain a certificate from a CA(SCEP(단순 인증서 등록 프로토콜 사용)), Manual(수동) - Root and Identity certificate(루트 및 ID 인증서) 수동 설치, PKCS12 - Upload encrypted certificate bundle with root(루트, ID 및 개인 키로 암호화된 인증서 번들 업로드)

4단계. FTD 디바이스에 인증서를 업로드합니다. 다음 이미지에 표시된 대로 암호(PKCS12에만 해당)를 입력하고 Save(저장)를 클릭합니다.

### Add Cert Enrollment ?

Name\*  
ftdcert

Description

CA Information   Certificate Parameters   Key   Revocation


Enrollment Type: PKCS12 File ▼

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

Passphrase: .....

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

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

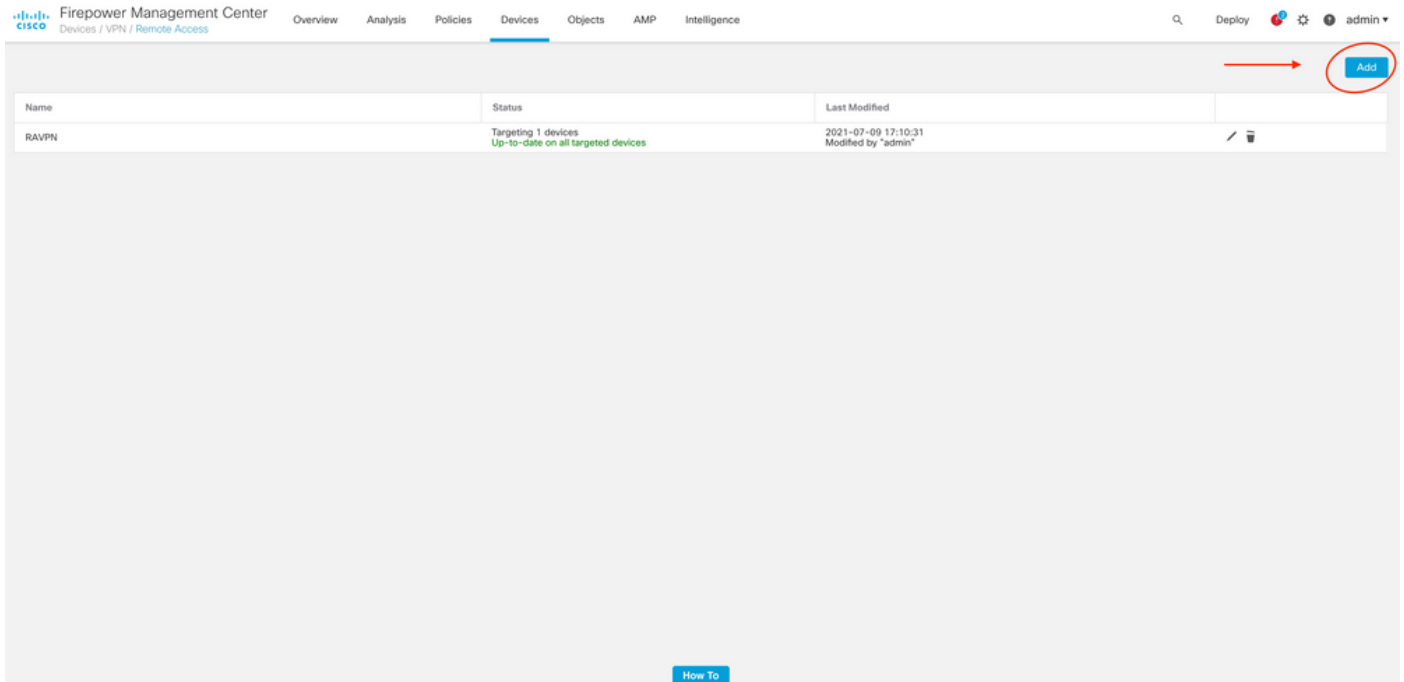
 참고: 파일을 저장하면 인증서 구축이 즉시 수행됩니다. 인증서 세부사항을 보려면 ID를 선택합니다.

## Cisco Anyconnect 구성

원격 액세스 마법사로 FMC를 통해 Anyconnect를 구성합니다.

1단계. 원격 액세스 VPN 정책 마법사를 시작하여 Anyconnect를 구성합니다.

Devices(디바이스) > Remote Access(원격 액세스)로 이동하고 Add(추가)를 선택합니다.



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Devices' tab is selected. The main content area displays a table with columns for 'Name', 'Status', and 'Last Modified'. A table row is visible with the name 'RAVPN', status 'Targeting 1 devices Up-to-date on all targeted devices', and last modified date '2021-07-09 17:10:31 Modified by "admin"'. An 'Add' button is circled in red in the top right corner of the table area. A 'How To' button is located at the bottom center of the page.

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

2단계. 정책 할당.

정책 할당을 완료합니다.

- a. 정책의 이름을 지정합니다.
- b. 원하는 VPN 프로토콜을 선택합니다.
- c. 컨피그레이션을 적용할 대상 디바이스를 선택합니다.

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:  FTD1 Tcoutire-FTD2

Selected Devices: Tcoutire-FTD2

How To

Cancel Back Next

### 3단계. 연결 프로파일.

- 연결 프로파일의 이름을 지정합니다.
- 인증 방법을 클라이언트 인증서 전용으로 설정합니다.
- IP 주소 풀을 할당하고, 필요한 경우 새 그룹 정책을 생성합니다.
- 다음을 클릭합니다.

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:

 참고: 인증 세션의 사용자 이름을 입력하는 데 사용할 기본 필드를 선택합니다. 이 설명서에서는 인증서의 CN을 사용합니다.

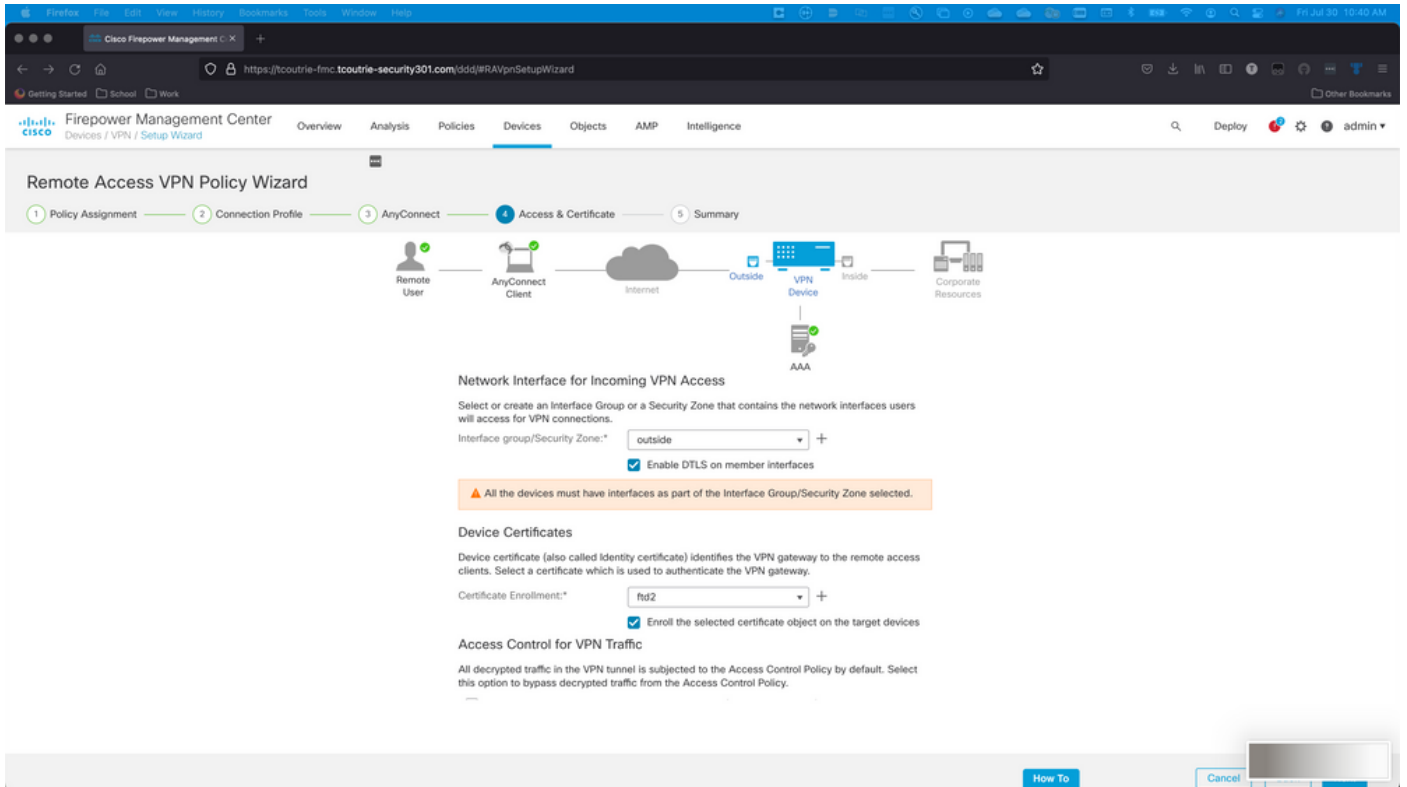
### 4단계. AnyConnect.

어플라이언스에 Anyconnect 이미지를 추가합니다. Anyconnect의 기본 버전을 업로드하고 Next(다음)를 클릭합니다.

 참고: Cisco Anyconnect 패키지는 Software.Cisco.com에서 다운로드할 수 있습니다.

5단계. 액세스 및 인증서.

이 이미지에 표시된 대로 인터페이스에 인증서를 적용하고 인터페이스 레벨에서 Anyconnect를 활성화하고 Next(다음)를 클릭합니다.



6단계. 요약.

구성을 검토합니다. 모두 체크 아웃한 경우 마침을 클릭한 다음 구축합니다.

## 모바일 사용자를 위한 인증서 만들기

연결에 사용되는 모바일 디바이스에 추가할 인증서를 만듭니다.

1단계. XCA.

a. XCA 열기

b. 새 데이터베이스 시작

2단계. CSR을 생성합니다.

a. CSR(Certificate Signing Request)을 선택합니다.

- b. 신규 요청을 선택합니다
- c. 인증서에 필요한 모든 정보가 포함된 값을 입력합니다
- d. 새 키 생성
- e. 완료되면 OK(확인)를 클릭합니다.

**Create Certificate signing request**

Source Extensions Key usage Netscape Advanced

Distinguished name

Internal name organizationName  
countryName organizationalUnitName  
stateOrProvinceName commonName Cisco\_Test  
localityName emailAddress

Type	Content

Add  
Delete

Private key  
Cisco\_Test\_1 (RSA:2048 bit)  Used keys too Generate a new key

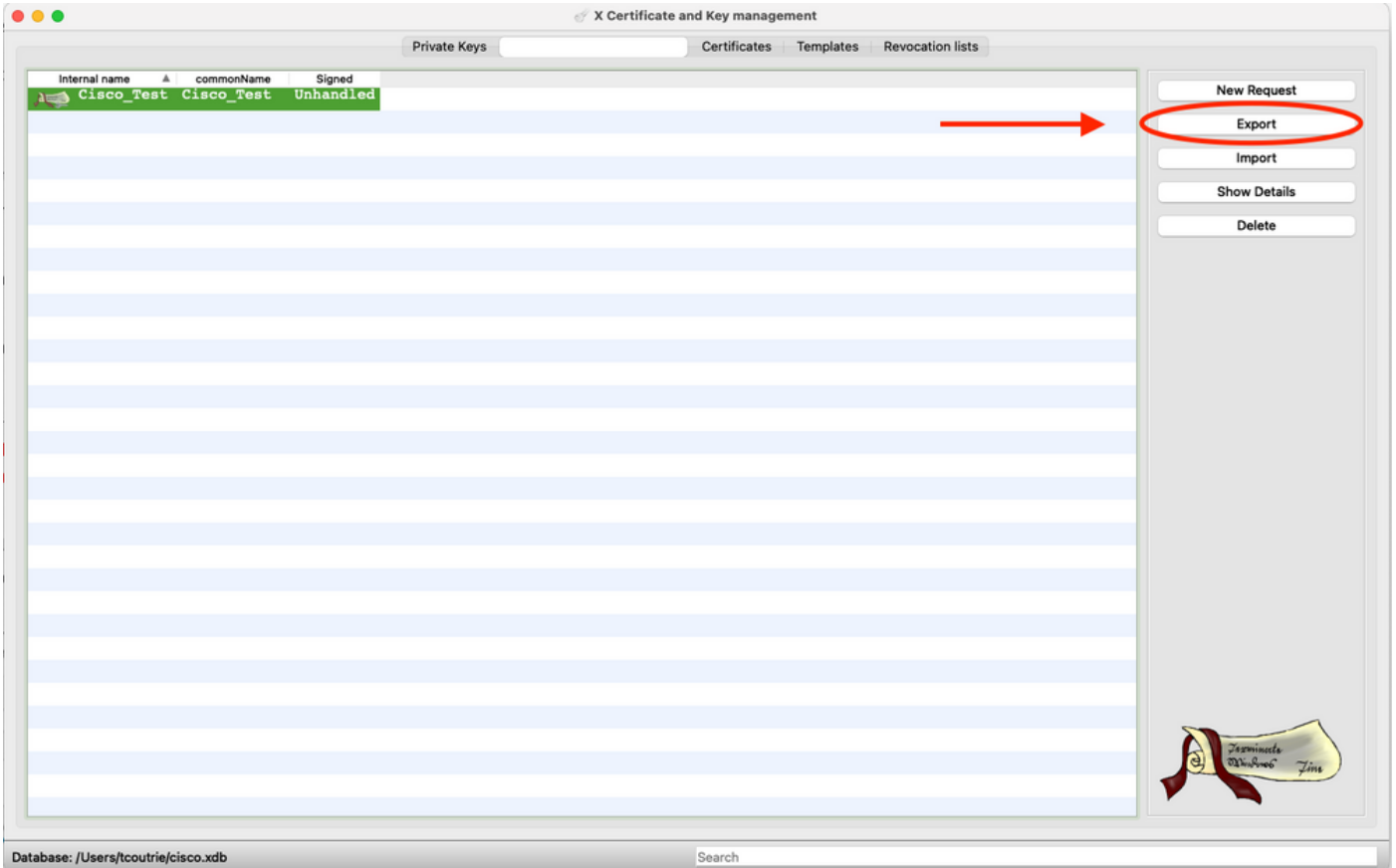
Cancel OK

참고: 이 문서에서는 인증서의 CN을 사용합니다.

3단계. CSR을 제출합니다.

- a. CSR 내보내기
- b. CA에 CSR을 제출하여 새 인증서 받기






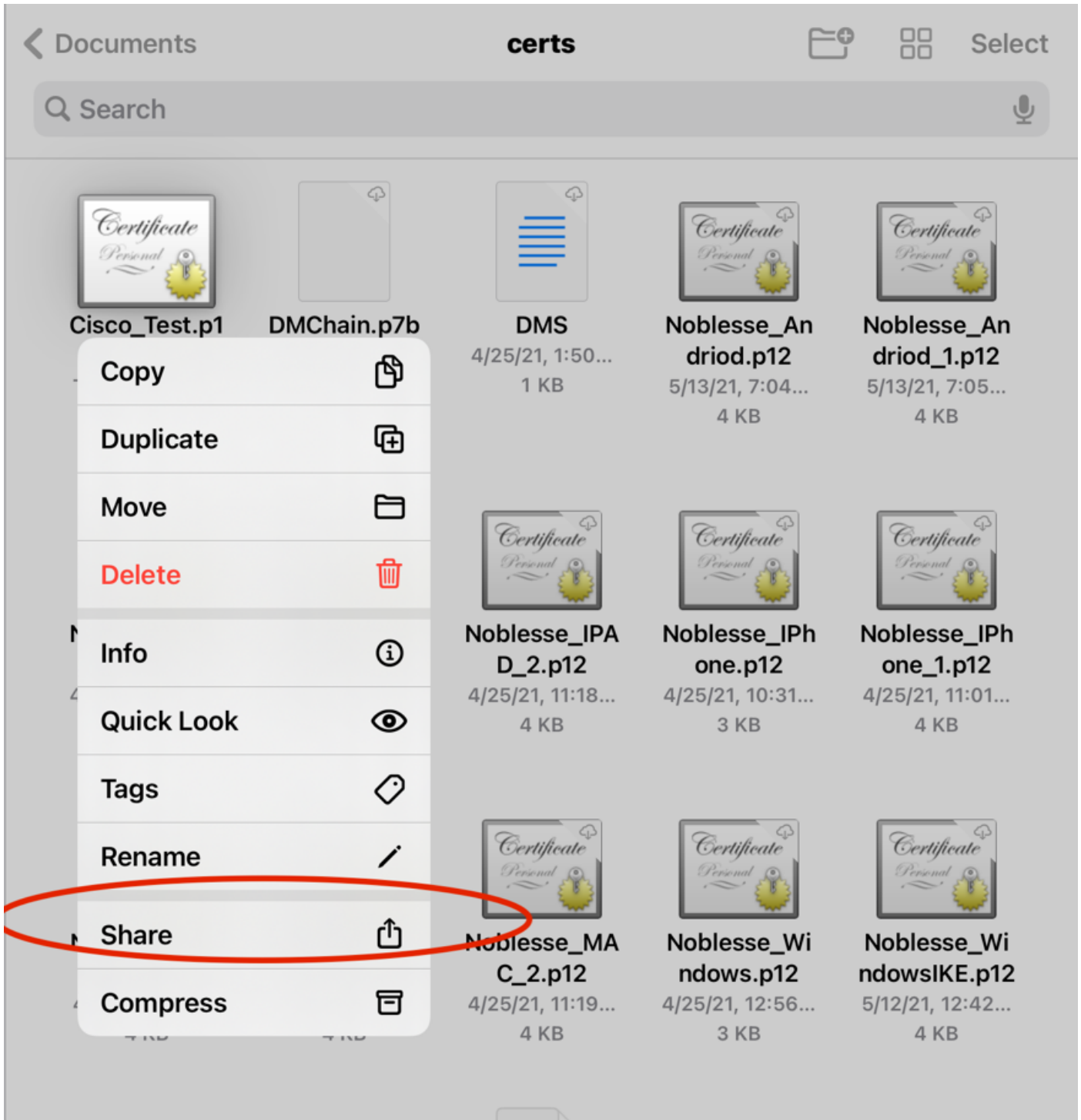
 참고: CSR의 PEM 형식을 사용합니다.

## 모바일 장치에 설치

1단계. 모바일 디바이스에 디바이스 인증서를 추가합니다.

2단계. Anyconnect 애플리케이션과 인증서를 공유하여 새 인증서 애플리케이션을 추가합니다.

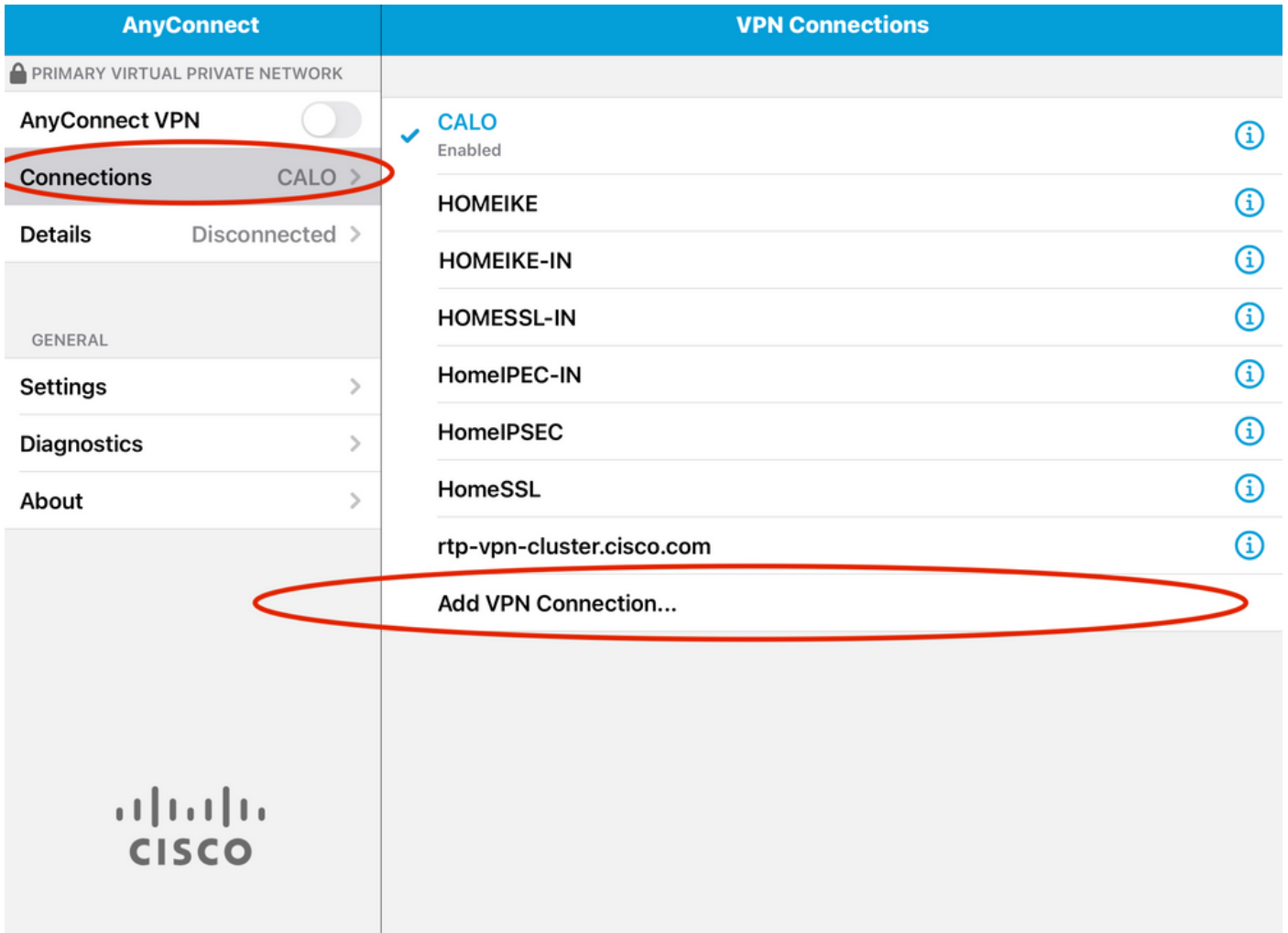
 주의: 수동으로 설치하려면 사용자가 인증서를 응용 프로그램과 공유해야 합니다. MDM을 통해 푸시되는 인증서에는 적용되지 않습니다.



3단계. PKCS12 파일의 인증서 비밀번호를 입력합니다.

4단계. Anyconnect에서 새 연결을 생성합니다.

5단계. Connections(연결) > Add VPN Connection(VPN 연결 추가)으로 이동합니다.



6단계. 새 연결에 대한 정보를 입력합니다.

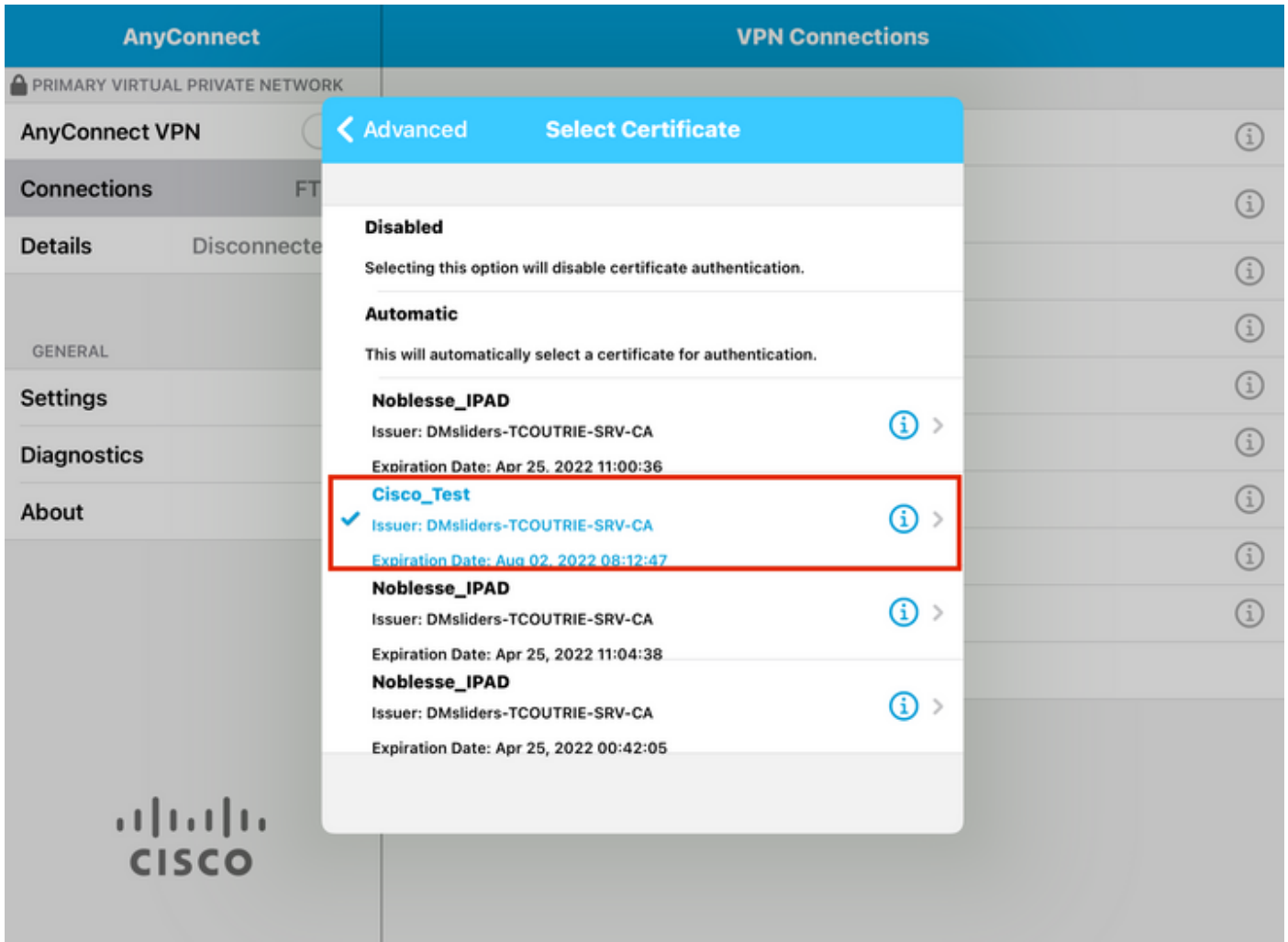
설명: 연결의 이름

서버 주소: FTD의 IP 주소 또는 FQDN

고급: 추가 구성



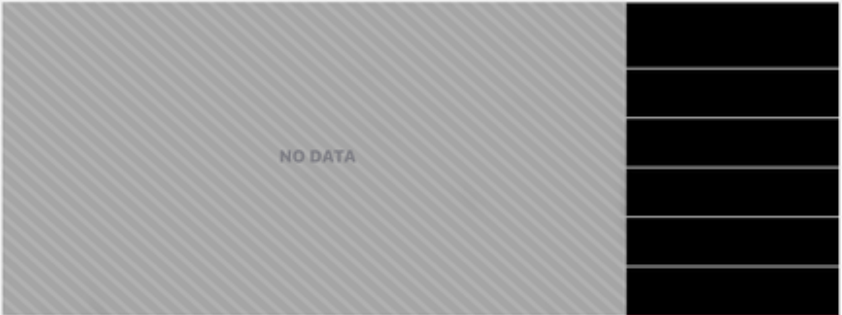
7단계. 고급을 선택합니다.

8단계. Certificate(인증서)를 선택하고 새로 추가한 인증서를 선택합니다.




9단계. 다시 Connections and test(연결 및 테스트)로 이동합니다.

성공하면 토글이 계속 켜져 있으며 세부 정보가 연결된 상태로 표시됩니다.

AnyConnect	FTD
PRIMARY VIRTUAL PRIVATE NETWORK	
AnyConnect VPN <span style="float: right;"><input checked="" type="checkbox"/></span>	Status <span style="float: right;">Connected</span>
Connections <span style="float: right;">FTD &gt;</span>	Statistics <span style="float: right;">&gt;</span>
Details <span style="float: right;">Connected &gt;</span>	
GENERAL	
Settings <span style="float: right;">&gt;</span>	
Diagnostics <span style="float: right;">&gt;</span>	
About <span style="float: right;">&gt;</span>	
	
	<div style="text-align: center;">Bytes Received</div>  <p>3.66 KB 2.93 KB 2.2 KB 1.46 KB 0.73 KB</p>
	<div style="text-align: center;">Bytes Sent</div>  <p>475 Bytes 380 Bytes 285 Bytes 190 Bytes 95 Bytes</p>

다음을 확인합니다.

show vpn-sessiondb detail Anyconnect 명령은 연결된 호스트에 대한 모든 정보를 표시합니다.

 **팁:** 이 명령을 추가로 필터링하는 옵션은 명령에 추가된 'filter' 또는 'sort' 키워드입니다.

예를 들면 다음과 같습니다.

```
Tcourtrie-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

## 문제 해결

### 디버그

이 문제를 해결하는 데 필요한 디버깅은 다음과 같습니다.

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

연결이 SSL이 아닌 IPSEC인 경우:

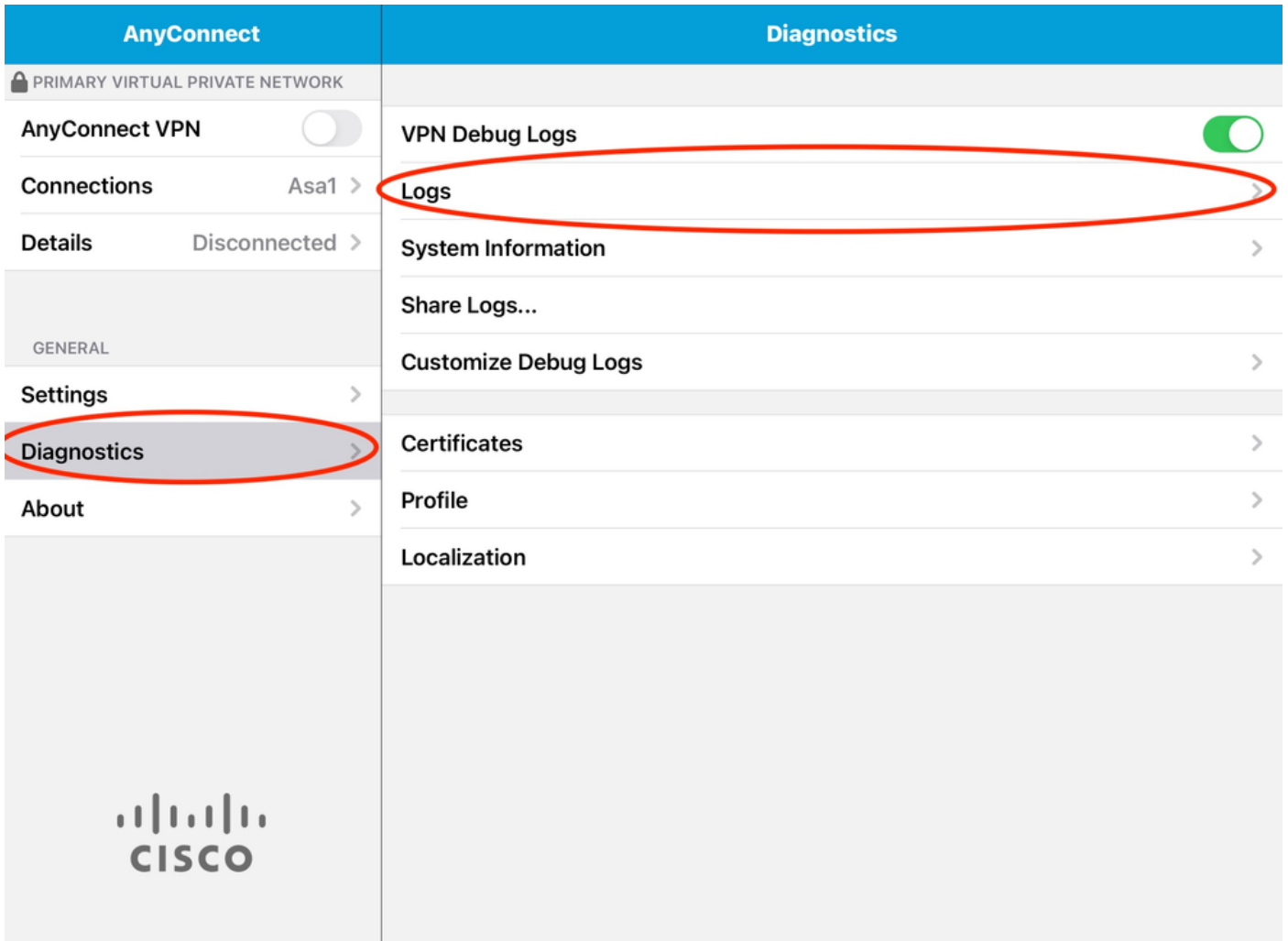
Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

Anyconnect 모바일 애플리케이션의 로그:

Diagnostic(진단) > VPN Debug Logs(VPN 디버그 로그) > Share logs(로그 공유)로 이동합니다.

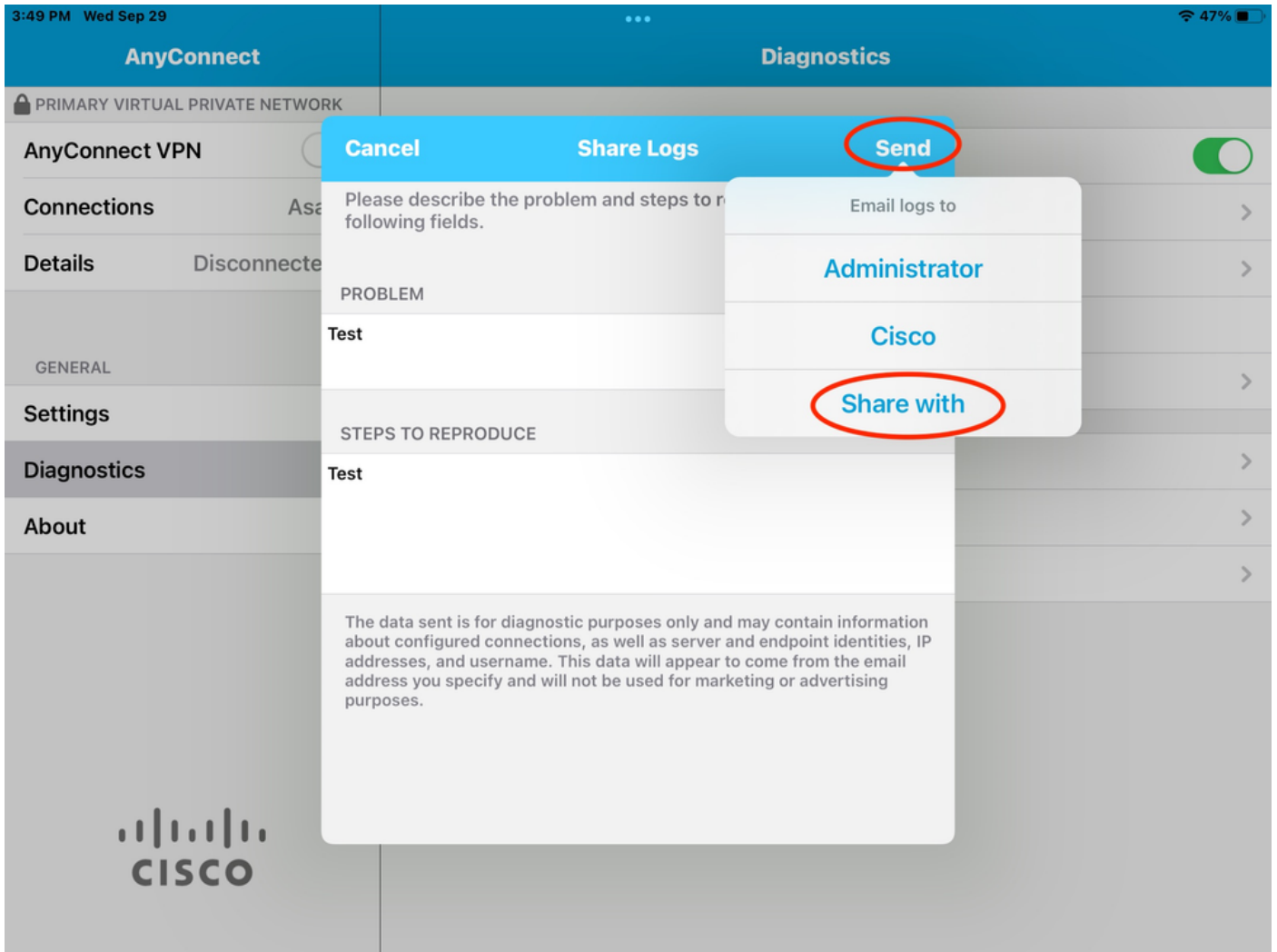


다음 정보를 입력합니다.

- 문제
- 재현 단계

그런 다음 Send(보내기) > Share with(공유)로 이동합니다.





그러면 이메일 클라이언트를 사용하여 로그를 전송하는 옵션이 표시됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.