

# FMC에서 관리하는 FTD에 보안 클라이언트 인증서 인증 구성

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[a. 서버 인증에 사용되는 인증서 생성/가져오기](#)

[b. 신뢰할 수 있는/내부 CA 인증서 추가](#)

[c. VPN 사용자를 위한 주소 풀 구성](#)

[d. 보안 클라이언트 이미지 업로드](#)

[e. XML 프로파일 생성 및 업로드](#)

[원격 액세스 VPN 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

---

## 소개

이 문서에서는 인증서 인증을 통해 FMC(Firepower Management Center)에서 관리하는 FTD(Firepower Threat Defense)에서 원격 액세스 VPN을 구성하는 프로세스에 대해 설명합니다.

기고자: Dolly Jain and Rishave Aggarwal, Cisco TAC 엔지니어

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 수동 인증서 등록 및 SSL의 기본 사항
- FMC
- 원격 액세스 VPN에 대한 기본 인증 지식
- Entrust, Geotrust, GoDaddy, Thawte, VeriSign과 같은 타사 CA(Certificate Authority)

### 사용되는 구성 요소

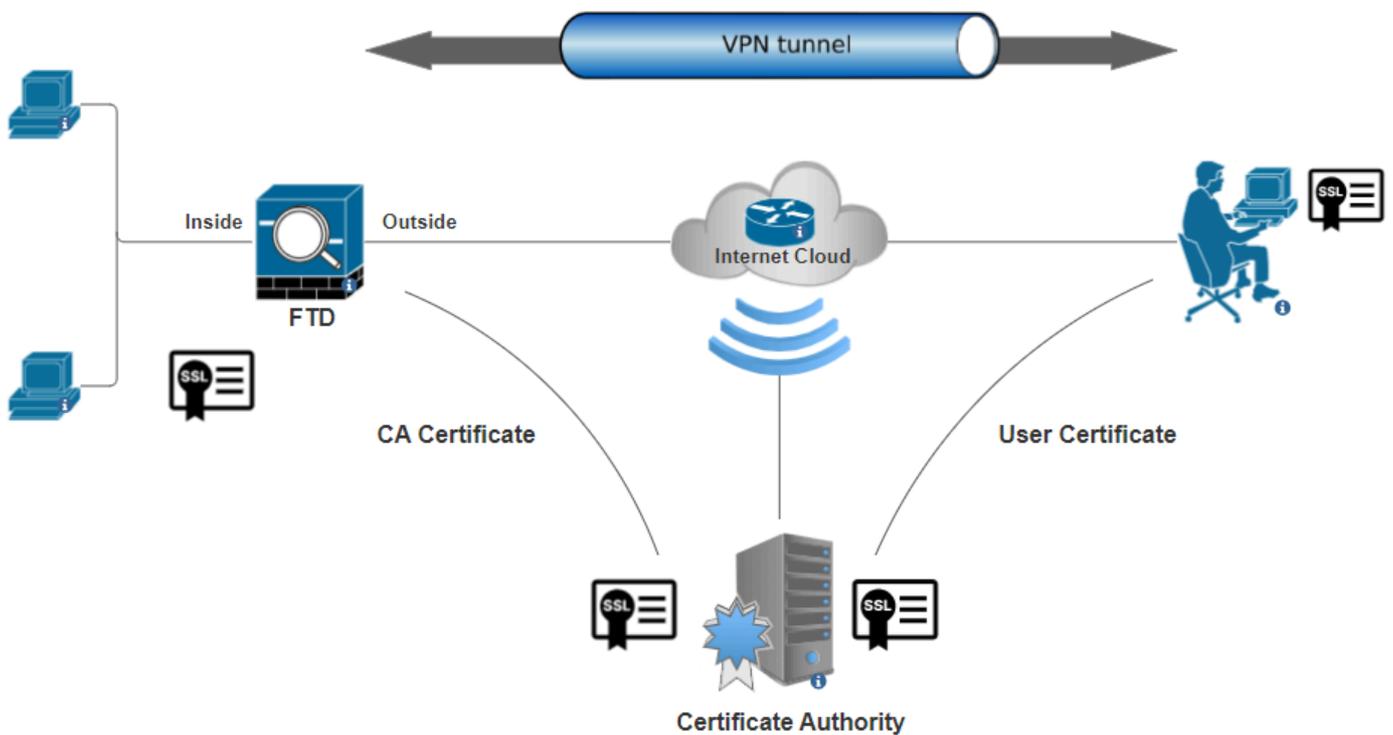
이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Firepower Threat Defense 버전 7.4.1
- FMC(Firepower 관리 센터) 버전 7.4.1
- Secure Client 버전 5.0.05040
- Microsoft Windows Server 2019를 CA 서버로 사용

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.

## 구성

### 네트워크 다이어그램



네트워크 다이어그램

## 설정

- a. 서버 인증에 사용되는 인증서 생성/가져오기



참고: FMC에서는 CSR을 생성하기 전에 CA 인증서가 필요합니다. 외부 소스(OpenSSL 또는 서드파티)에서 CSR이 생성된 경우 수동 방법이 실패하고 PKCS12 인증서 형식을 사용해야 합니다.

---

**1단계. 로 이동하고** Devices > Certificates를 클릭합니다Add. Device(디바이스)를 선택하고 Cert Enrollment(인증서 등록) 아래에서 더하기 기호(+)를 클릭합니다.

## Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

Cancel

Add

인증서 등록 추가

2단계. 에서 CA Information Enrollment Type(등록 유형)을 Manual 선택하고 CSR 서명에 사용된 CA(Certificate Authority) 인증서를 붙여넣습니다.

## Add Cert Enrollment



Name\*

ssl\_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

*Check this option if you do not require an identity certificate to be created from this CA*

CA Certificate:

```
HQYDVQQDEZXIEWRYRW50S
UQgU2VydMvYlENBIE8xMIIBlj
ANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA6
huZbDVWWMGj7XbFZQWI+uhh
0SleWhO8rI79MV4+7ZSj2
Lxos5e8za0H1JVVzTNPaup2G
o438C5zeaqaGtyUshV8D0xw
UiWyamspTao7PjjuC
h81+tp9z76rp1irjNMh5o/zeJ0
h3Kag5zQG9sfI7J7ihLnTFbArj
N7ID=ZeeQw
```

Validation Usage:



IPsec Client



SSL Client



SSL Server



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

Cancel

Save

CA 정보 추가

3단계. Validation Usage(검증 사용)에서 and(및)를 선택합니다IPsec Client, SSL ClientSkip Check for CA flag in basic constraints of the CA Certificate.

4단계. 아래에 Certificate Parameters주체 이름 세부 정보를 입력합니다.

## Add Cert Enrollment



Name\*

ssl\_certificate

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Don't use FQDN in certificate ▼

Include Device's IP Address:

Common Name (CN): certauth.cisco.com

Organization Unit (OU): TAC

Organization (O): Cisco

Locality (L): Bangalore

State (ST): KA

Country Code (C): IN

Email (E):

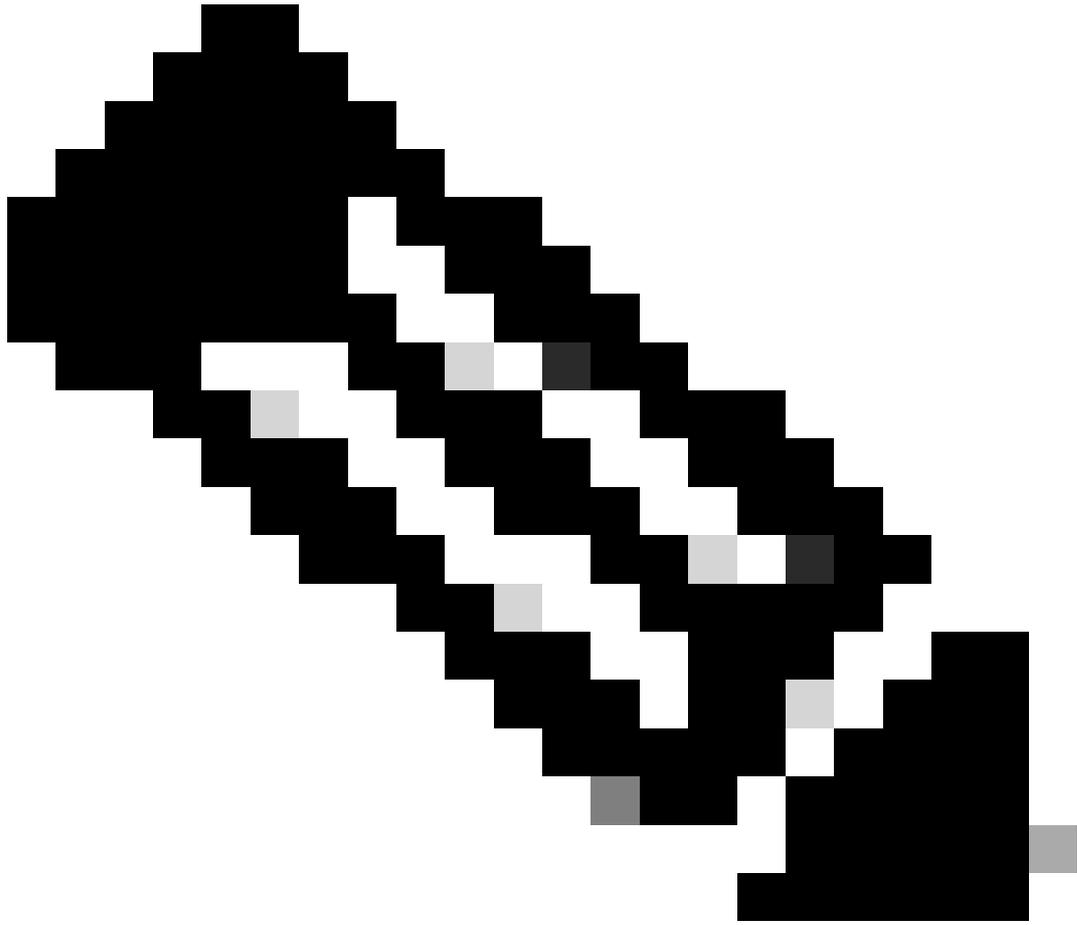
Include Device's Serial Number

Cancel

Save

인증서 매개변수 추가

5단계. 에서 키 이름과 크기의 키 유형을 RSA로 Key선택합니다. 를 Save 클릭합니다.



참고: RSA 키 유형의 경우 최소 키 크기는 2048비트입니다.

---

## Add Cert Enrollment



Name\*  
ssl\_certificate

Description

CA Information   Certificate Parameters   **Key**   Revocation

**Key Type:**  
 RSA    ECDSA    EdDSA

Key Name:\*  
rsakey

**Key Size:**  
2048 ▼

▼ Advanced Settings

Ignore IPsec Key Usage

Cancel   **Save**

RSA 키 추가

6단계. 아래 Cert Enrollment, 방금 생성한 드롭다운에서 신뢰 지점을 선택하고 을 클릭합니다 Add.

# Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

 +

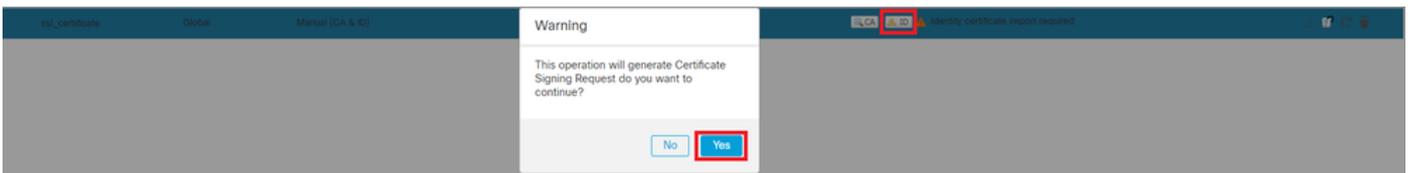
Cert Enrollment Details:

Name: ssl\_certificate  
Enrollment Type: Manual (CA & ID)  
Enrollment URL: N/A

새 인증서 추가

7단계. ID를 클릭한 다음 추가 프롬프트를 클릭하여Yes CSR을 생성합니다.



CSR 생성

8단계. CSR을 복사하고 인증 기관에서 서명을 받습니다. ID 인증서가 CA에 의해 발급되면 를 클릭하여 가져온 다음 을 Browse Identity Certificate 클릭합니다Import.

# Import Identity Certificate



## Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

```
-----BEGIN CERTIFICATE REQUEST-----  
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG  
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMakGA1UEBhMC  
SU4wggliMA0GCsqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK  
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO  
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1plLEdR4X6ZlnM5fNA/GLV9MnPoP  
ppzi0ulbVmb5iKQexllaur/e2PDccc3eC57e+D3QhKQ9SC7um8ulwueF+70fKYe
```

## Step 2

Once certificate authority responds back with identity certificate file, import it to device.

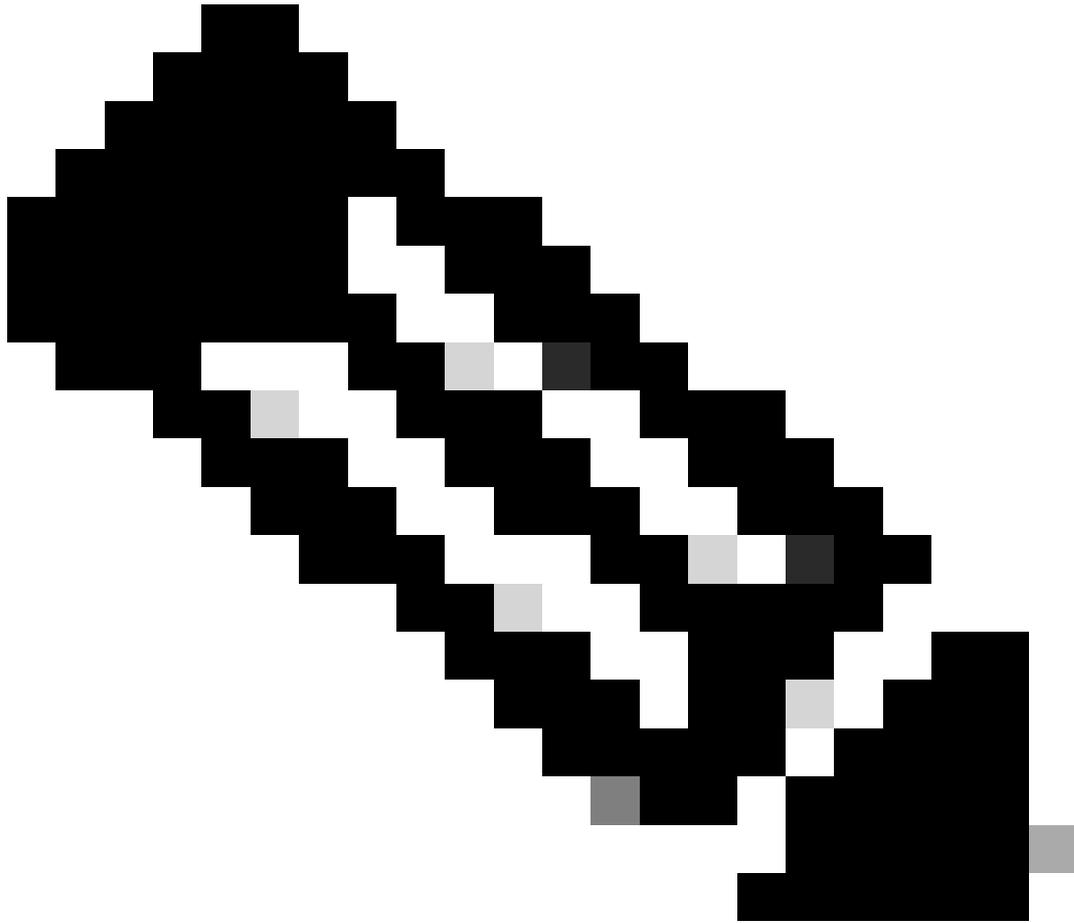
Identity Certificate File:

[Browse Identity Certificate](#)

[Cancel](#)

[Import](#)

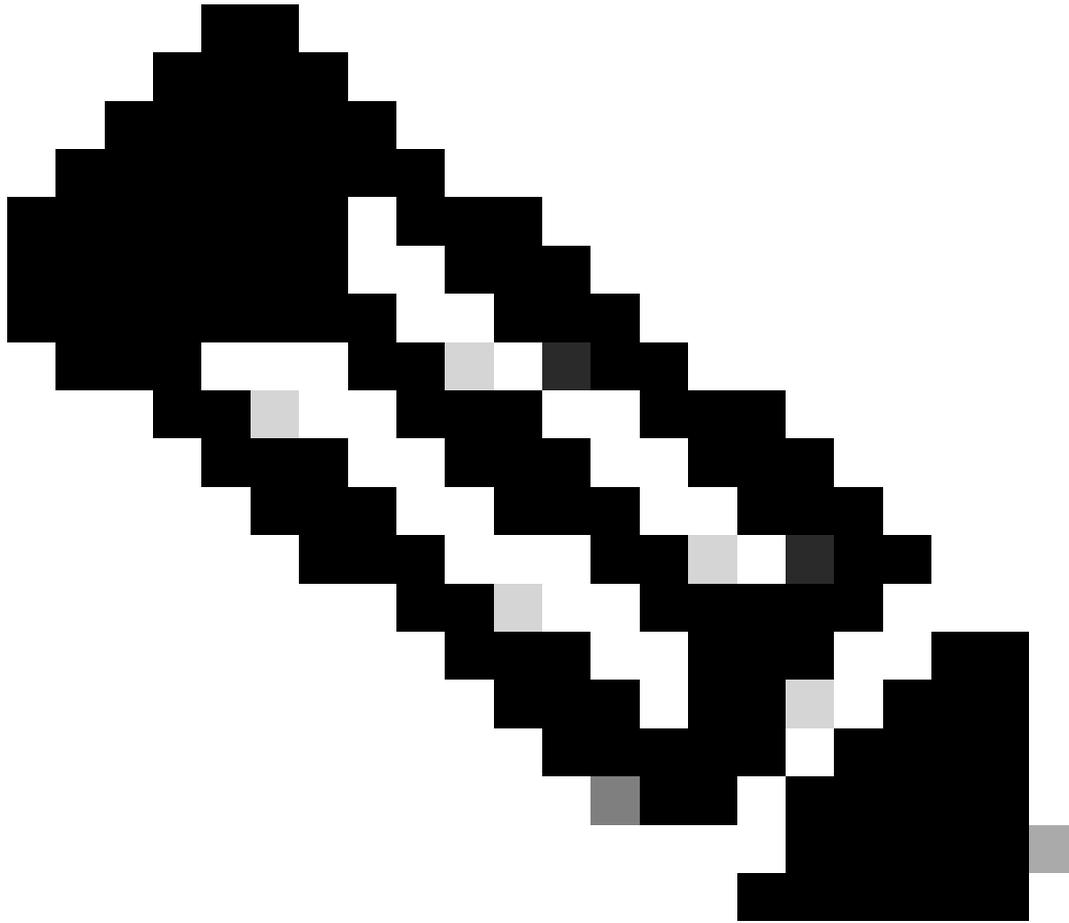
ID 인증서 가져오기



**참고:** ID 인증서 발급에 시간이 걸리는 경우 나중에 7단계를 반복할 수 있습니다. 이렇게 하면 동일한 CSR이 생성되며 ID 인증서를 가져올 수 있습니다.

---

b. 신뢰할 수 있는/내부 CA 인증서 추가



**참고:** (a)단계에서 사용된 CA(Certificate Authority), "**Create/Import a Certificate Used for Server Authentication(서버 인증에 사용되는 인증서 생성/가져오기)**"도 사용자 인증서를 발급하는 경우 (b), "**Add a Trusted/Internal CA Certificate(신뢰받는/내부 CA 인증서 추가)**"를 건너뛸 수 있습니다. 동일한 CA 인증서를 다시 추가할 필요가 없으며, 이 역시 방지해야 합니다. 동일한 CA 인증서를 다시 추가하면 RAVPN에 대한 인증서 인증에 영향을 줄 수 있는 "validation-usage none"으로 신뢰 지점이 구성됩니다.

---

1단계. 로 이동하고 Devices > Certificates 를 클릭합니다Add.

Device(디바이스)를 선택하고 Cert Enrollment(인증서 등록) 아래에서 더하기 기호(+)를 클릭합니다.

여기서 "auth-risaggar-ca"는 ID/사용자 인증서를 발급하는 데 사용됩니다.

General Details Certification Path



### Certificate Information

**This certificate is intended for the following purpose(s):**

- All issuance policies
- All application policies

**Issued to:** auth-risaggar-ca

**Issued by:** auth-risaggar-ca

**Valid from** 04-03-2023 **to** 04-03-2033

Issuer Statement

OK

auth-risaggar-ca

2단계. 신뢰 지점 이름을 입력하고 아래의 등록 유형으로 선택합니다ManualCA information.

3단계. PEM 형식CA Only로 신뢰할 수 있는/내부 CA 인증서를 확인하고 붙여넣습니다.

4단계. 확인 Skip Check for CA flag in basic constraints of the CA Certificate하고 클릭 Save 합니다.

### Add Cert Enrollment ?

Internal\_CA

Description

CA Information   Certificate Parameters   Key   Revocation

Enrollment Type: Manual

CA Only

*Check this option if you do not require an identity certificate to be created from this CA*

CA Certificate:

```
-----BEGIN CERTIFICATE-----  
--  
MIIG1jCCBL6gAwIBAgIQQAFu  
+wogXPrr4Y9x1zq7eDANBgk  
qhkiG9w0BAQsFADBK  
MQswCQYDVQQGEwJVUzES  
MBAGA1UEChMJSWRlbiRydX  
N0MScwJQYDVQQDEw5JZGVu  
u  
VHJ1c3QgQ29tbWVyY2lhbCB  
Sb290IENBIDUwHhcNMTkxMj
```

Validation Usage:  IPsec Client    SSL Client    SSL Server

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

Cancel   Save

신뢰 지점 추가

5단계. 아래 Cert Enrollment, 방금 생성한 드롭다운에서 신뢰 지점을 선택하고 을 클릭합니다 Add.

## Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device\*:

Cert Enrollment\*:

 +

Cert Enrollment Details:

Name: Internal\_CA  
Enrollment Type: Manual (CA Only)  
Enrollment URL: N/A

Cancel

Add

내부 CA 추가

6단계. 이전에 추가된 인증서는 다음과 같이 표시됩니다.

Internal_CA	Global	Manual (CA Only)	Mar 4, 2033	CA ID	⌵ ⌵ ⌵
-------------	--------	------------------	-------------	-------	-------

추가된 인증서

### c. VPN 사용자를 위한 주소 풀 구성

1단계. 로 Objects > Object Management > Address Pools > IPv4 Pools 이동합니다.

2단계. 마스크와 함께 이름 및 IPv4 주소 범위를 입력합니다.

## Edit IPv4 Pool



Name\*

vpn\_pool

Description

IPv4 Address Range\*

10.20.20.1-10.20.20.130

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask\*

255.255.255.0

Allow Overrides

**i** Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▶ Override (0)

Cancel

Save

IPv4 풀 추가

### d. 보안 클라이언트 이미지 업로드

1단계. [Cisco 소프트웨어](#) 사이트에서 OS에 따라 webdeploy 보안 클라이언트 [이미지](#)를 다운로드합니다.

2단계. 로 Objects > Object Management > VPN > Secure Client File > Add Secure Client File 이동합니다.

3단계. 이름을 입력하고 디스크에서 Secure Client 파일을 선택합니다.

4단계. 파일 유형을 (으)로 Secure Client Image 선택하고 를 클릭합니다Save.

# Edit Secure Client File



Name:\*

File Name:\*

File Type:\*

Description:

보안 클라이언트 이미지 추가

## e. XML 프로파일 생성 및 업로드

1단계. [Cisco Software](#) 사이트에서 Secure ClientProfile Editor를 [다운로드하고](#) 설치합니다.

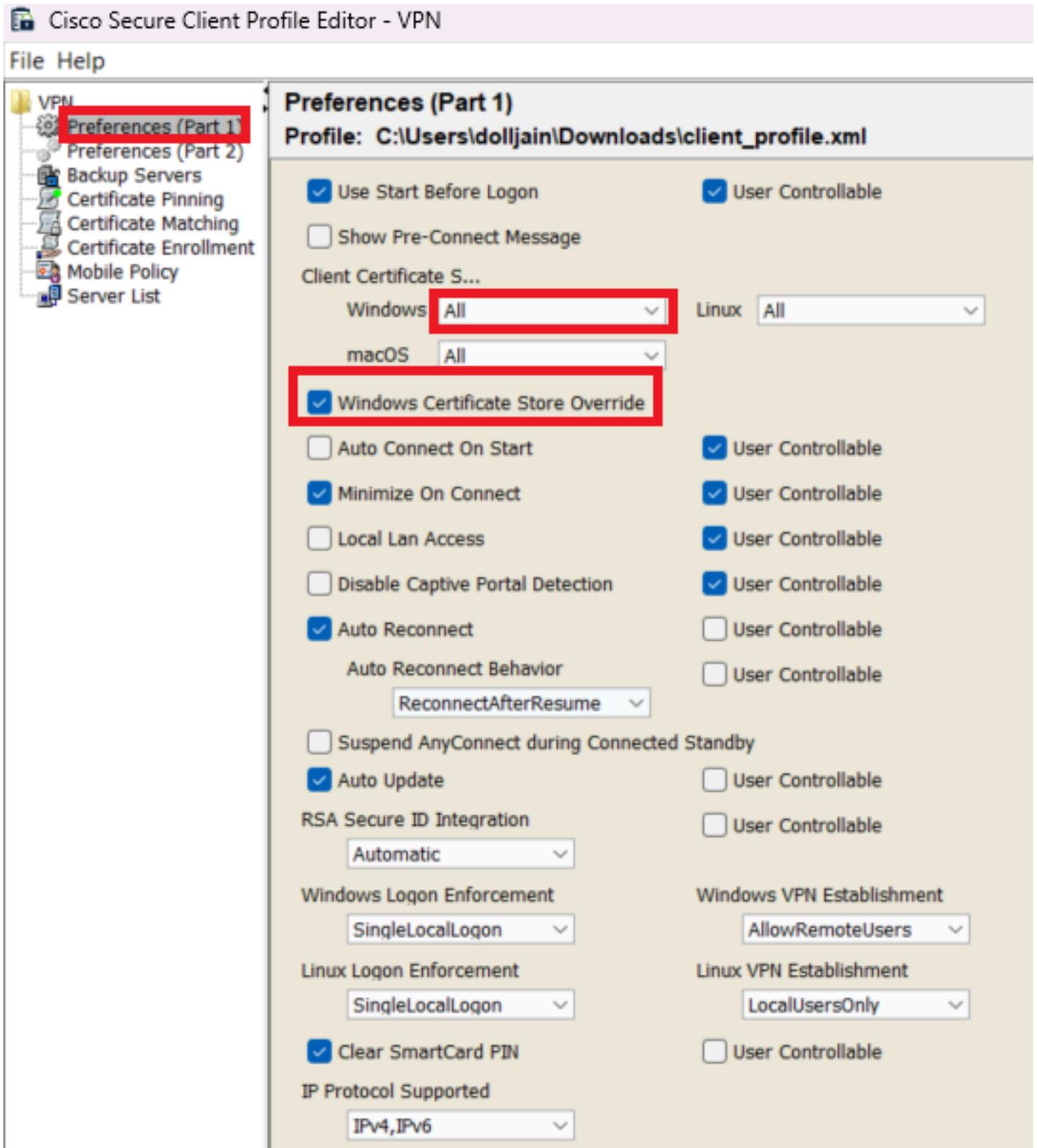
2단계. 새 프로필을 생성하고 Client Certificate Selection(클라이언트 인증서 선택) 드롭다운에서 선택합니다. 주로 Secure Client가 인증서를 저장 및 읽는 데 사용할 수 있는 인증서 저장소를 제어합니다.

사용 가능한 다른 두 가지 옵션은 다음과 같습니다.

- **컴퓨터** - 보안 클라이언트가 Windows 로컬 컴퓨터 인증서 저장소에서 인증서 조회로 제한됩니다.
- **사용자** - 보안 클라이언트가 로컬 Windows 사용자 인증서 저장소에서 인증서 조회로 제한됩니다.

인증서 저장소 재정의의 다음으로 True 설정합니다.

이를 통해 관리자는 Secure Client가 클라이언트 인증서 인증을 위해 Windows 시스템(로컬 시스템) 인증서 저장소의 인증서를 활용하도록 지시할 수 있습니다. Certificate Store Override(인증서 저장소 재정의)는 SSL에만 적용되며, SSL에서는 기본적으로 UI 프로세스에 의해 연결이 시작됩니다. IPSec/IKEv2를 사용할 때는 보안 클라이언트 프로파일의 이 기능을 적용할 수 없습니다.



환경 설정 추가(1부)

3단계. (선택 사항) 사용자가 Disable Automatic Certificate Selection 인증 인증서를 선택하라는 프롬프트를 표시하지 않으므로 의 선택을 취소합니다.

- VPN
- Preferences (Part 1)
- Preferences (Part 2)**
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

### Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client\_profile.xml

**Disable Automatic Certificate Selection**

User Controllable

#### Proxy Settings

Native

User Controllable

Public Proxy Server Address:

Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080

Allow Local Proxy Connections

Enable Optimal Gateway Selection

User Controllable

Suspension Time Threshold (hours)

Performance Improvement Threshold (%)

Automatic VPN Policy

Trusted Network Policy

Untrusted Network Policy

Bypass connect upon VPN session timeout

Trusted DNS Domains

Trusted DNS Servers

Note: adding all DNS servers in use is recommended with Trusted Network Detection

Trusted Servers @ https://<server>[:<port>]

https://

Add

Delete

Certificate Hash:

Set

Disable interfaces without trusted server connectivity while in truste...

Always On

(More Information)

Allow VPN Disconnect

Allow access to the following hosts with VPN disconn...

Connect Failure Policy

Allow Captive Portal Remediation

Remediation Timeout (min.)

Apply Last VPN Local Resource Rules

Captive Portal Remediation Browser Failover

Allow Manual Host Input

PPP Exclusion

User Controllable

PPP Exclusion Server IP

User Controllable

Enable Scripting

User Controllable

Terminate Script On Next Event

Enable Post SBL On Connect Script

Retain VPN on Logoff

User Enforcement

Authentication Timeout (seconds)

참고: 이 ACL은 Secure Client에서 내부 리소스에 보안 경로를 추가하는 데 사용됩니다.

2단계. 로 이동하고 Devices > VPN > Remote Access 를 클릭합니다Add.

3단계. 프로파일 이름을 입력한 다음 FTD 디바이스를 선택하고 Next(다음)를 클릭합니다.

The screenshot shows the 'Remote Access VPN Policy Wizard' interface. At the top, there are five steps: 1. Policy Assignment, 2. Connection Profile, 3. Secure Client, 4. Access & Certificate, and 5. Summary. The current step is 'Targeted Devices and Protocols'. Below this, there is a text box for 'Name:\*' containing 'RAVPN', a 'Description:' text box, and a section for 'VPN Protocols:' with checkboxes for 'SSL' and 'IPsec-IKEv2'. Under 'Targeted Devices:', there are two columns: 'Available Devices' with a search bar and a list containing 'FTD-A-7.4.1', 'FTD-B-7.4.0', and 'FTD-ZTNA-7.4.1'; and 'Selected Devices' with a list containing 'FTD-A-7.4.1'. An 'Add' button is located between the two columns. On the right side, there is a 'Before You Start' section with instructions on authentication servers, secure client packages, and device interfaces.

프로필 이름 추가

4단계. 를 Connection Profile Name 입력하고 AAA(Authentication, Authorization and Accounting Client Certificate Only) 아래에서 Authentication Method(인증 방법)를 선택합니다.

## 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:\*

**i** 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:  +  
(Realm or RADIUS)

Accounting Server:  +  
(RADIUS)

인증 방법 선택

5단계. Client Address Assignment(클라이언트 주소 할당) 아래 Use IP Address Pools 를 클릭하고 이전에 생성한 IPv4 주소 풀을 선택합니다.

## 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 (Realm or RADIUS only) **i**

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:  

IPv6 Address Pools:  

클라이언트 주소 할당 선택

6단계. 그룹 정책을 수정합니다.

## 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](#)

그룹 정책 편집

7단계. Split Tunnel Network List Type(스플릿 터널 네트워크 목록 유형)으로 General > Split Tunneling Tunnel networks specified below Standard Access List 이동하여 선택하고 선택합니다.

이전에 생성한 ACL을 선택합니다.

# Edit Group Policy



Name:\*

DfltGrpPolicy

Description:

General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Tunnel networks specified below ▼

IPv6 Split Tunneling:

Allow all traffic over tunnel ▼

Split Tunnel Network List Type:

Standard Access List  Extended Access List

Standard Access List:

Split\_ACL ▼ +

DNS Request Split Tunneling

DNS Requests:

Send DNS requests as per split t ▼

Domain List:

Cancel

Save

스플릿 터널링 추가

8단계. 로 Secure Client > Profile 이동하여 를 선택하고 Client Profile 를 클릭합니다Save.

# Edit Group Policy



Name:\*  
DfltGrpPolicy

Description:

General **Secure Client** Advanced

- Profile**
- Management Profile
- Client Modules
- SSL Settings
- Connection Settings
- Custom Attributes

Secure Client profiles contains settings for the VPN client functionality and optional features. The Firewall Threat Defense deploys the profiles during Secure Client connection.

Client Profile:  
 +

Standalone profile editor can be used to create a new or modify existing Secure Client profile. You can download the profile editor from [Cisco Software Download Center](#).

보안 클라이언트 프로파일 추가

9단계. 을 Next 클릭한 다음 을 선택하고 를 Secure Client Image 클릭합니다Next.

## Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input type="checkbox"/>	Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyconnectWin-5.0.05040	cisco-secure-client-win-5.0.05040-webde...	Windows

보안 클라이언트 이미지 추가

10단계. Network Interface for VPN Access(VPN 액세스용 네트워크 인터페이스)를 선택하고 를 Device Certificates 선택한 다음 sysopt permit-vpn을 선택하고 을 클릭합니다Next.

## Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:\*  +  
 Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

## Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:\*  +  
 Enroll the selected certificate object on the target devices

## Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  
*This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.*

VPN 트래픽에 대한 액세스 제어 추가

11단계. 마지막으로, 모든 컨피그레이션을 검토하고 **Finish**를 클릭합니다.

## Remote Access VPN Policy Configuration

---

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RAVPN
Device Targets:	FTD-B-7.4.0
Connection Profile:	RAVPN-CertAuth
Connection Alias:	RAVPN-CertAuth
AAA:	
Authentication Method:	Client Certificate Only
Username From Certificate:	-
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
Secure Client Images:	AnyconnectWin-5.0.05040
Interface Objects:	outside-zone
Device Certificates:	ssl_certificate

### Device Identity Certificate Enrollment

---

Certificate enrollment object 'ssl\_certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

원격 액세스 VPN 정책 구성

12단계. 원격 액세스 VPN의 초기 설정이 완료되면 생성된 연결 프로파일을 편집하고 Aliases 이동합니다.

13단계. 더하기 아이콘(+)을 클릭하여 group-alias 구성합니다.

### Edit Connection Profile

Connection Profile:\* RAVPN-CertAuth

Group Policy:\* DfltGrpPolicy +  
[Edit Group Policy](#)

Client Address Assignment   AAA   **Aliases**

Alias Names:  
Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
ssl-cert	Enabled	

URL Alias:  
Configure the list of UR following URLs, system

URL
-----

#### Edit Alias Name

Alias Name:  
ssl-cert

Enabled

Cancel   OK

Cancel   Save

그룹 별칭 편집

14단계. 더하기 아이콘(+)을 클릭하여 group-url구성합니다. 클라이언트 프로필에서 이전에 구성한 것과 동일한 그룹 URL을 사용합니다.

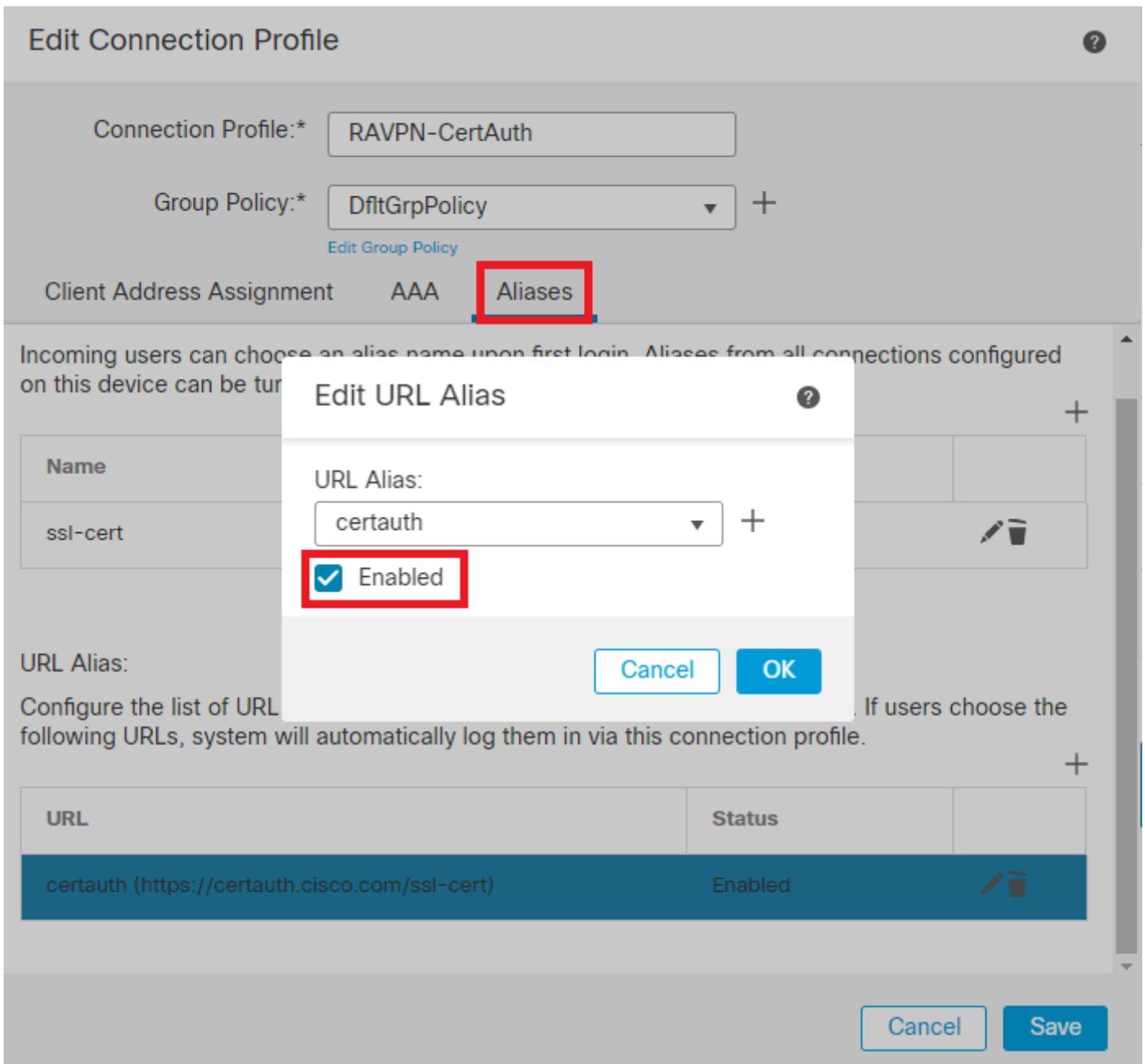
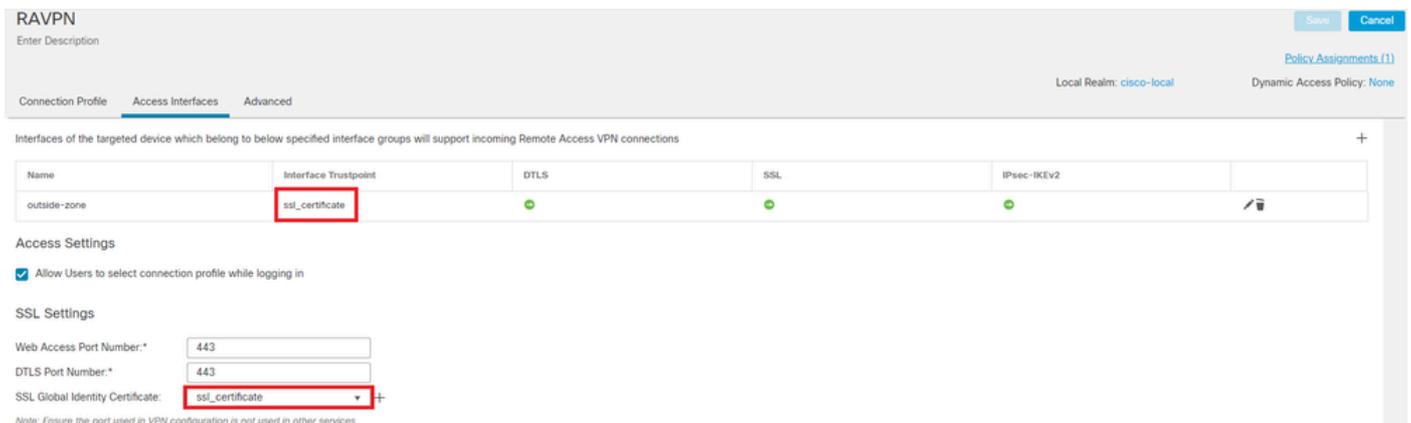


그림 URL 편집

15단계. Access Interfaces로 이동합니다. SSL 설정 Interface Trustpoint 아래에서 SSL Global Identity Certificate 및 을 선택합니다.



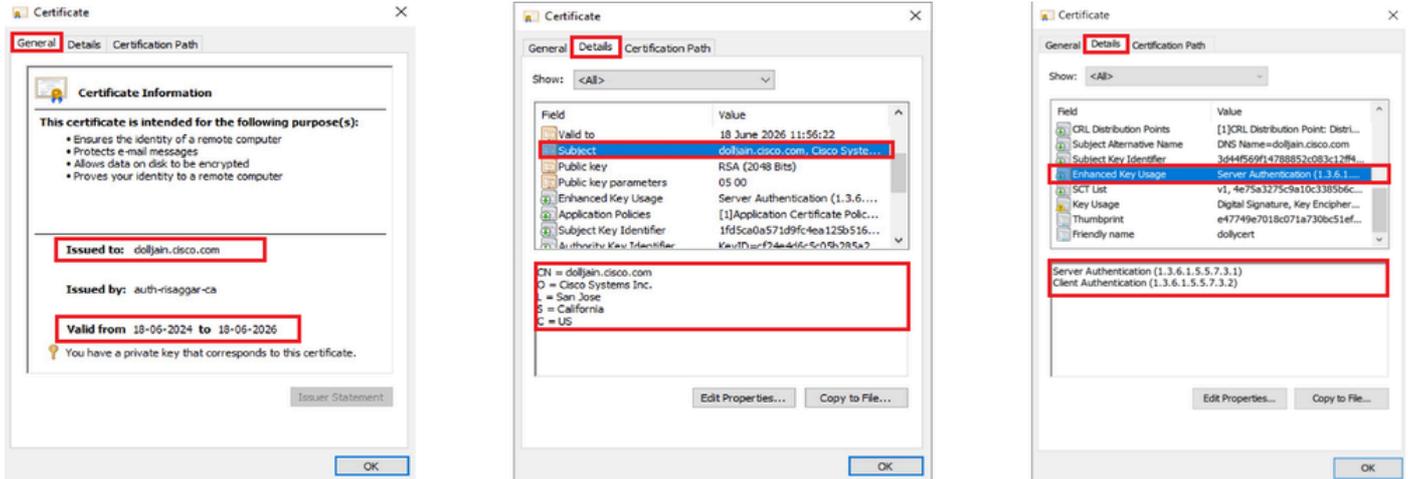
액세스 인터페이스 편집

16단계. 을 클릭하고Save 이러한 변경 사항을 구축합니다.

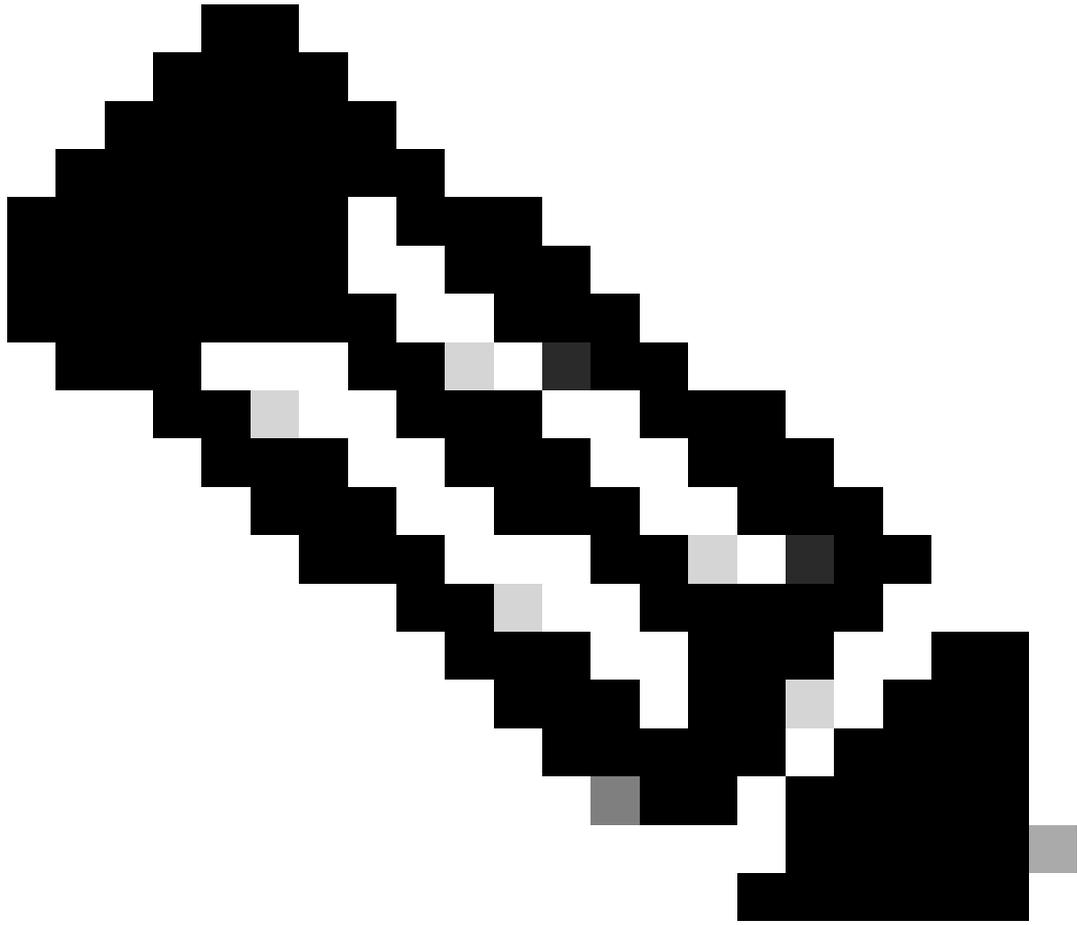
다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1. 보안 클라이언트 PC에는 사용자 PC에 유효한 날짜, 제목 및 EKU가 있는 인증서가 설치되어 있어야 합니다. 이 인증서는 앞서 설명한 것처럼 FTD에 설치된 인증서의 CA에서 발급해야 합니다. 여기서 ID 또는 사용자 인증서는 "auth-risaggar-ca"에 의해 발급된다.



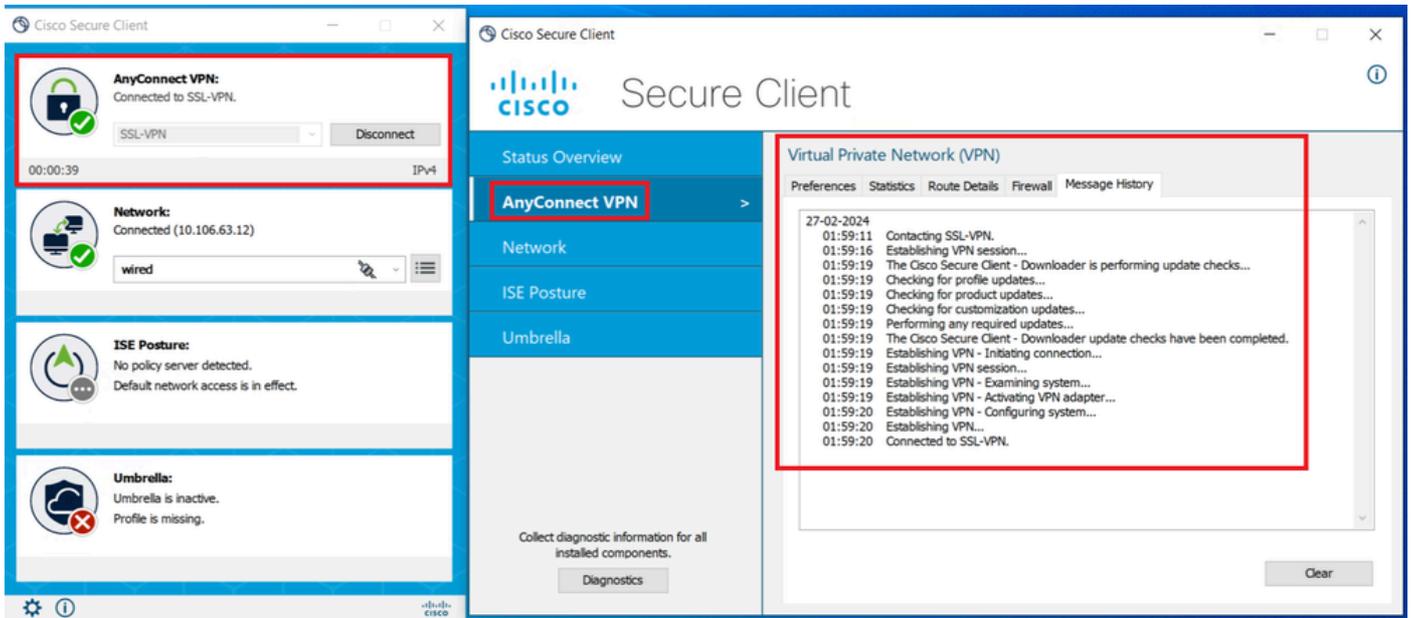
인증서 하이라이트



참고: 클라이언트 인증서에는 "클라이언트 인증" EKU(Enhanced Key Usage)가 있어야 합니다.

---

2. 보안 클라이언트가 연결을 설정해야 합니다.



보안 클라이언트 연결 성공

3. show vpn-sessiondb anyconnect 실행을 실행하여 사용된 터널 그룹 아래의 활성 사용자의 연결 세부 정보를 확인합니다.

firepower# show vpn-sessiondb anyconnect Session Type: AnyConnect Username : dolljain.cisco.com Index :

## 문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

1. 디버그는 FTD의 진단 CLI에서 실행할 수 있습니다.

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2. 일반적인 문제는 이 [가이드](#)를 참조하십시오.

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.