

FDM에서 관리하는 FTD에 인증서 설치 및 갱신

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[인증서 설치](#)

[자체 서명 등록](#)

[수동 등록](#)

[신뢰할 수 있는 CA 인증서 설치](#)

[인증서 갱신](#)

[일반적인 OpenSSL 작업](#)

[PKCS12 파일에서 ID 인증서 및 개인 키 추출](#)

[다음을 확인합니다.](#)

[FDM에서 설치된 인증서 보기](#)

[CLI에서 설치된 인증서 보기](#)

[문제 해결](#)

[디버그 명령](#)

[일반적인 문제](#)

[ASA에서 내보낸 PKCS12 가져오기](#)

소개

이 문서에서는 FTD에서 서드파티 CA 또는 내부 CA가 서명한 셀프 서명 인증서 및 인증서를 설치, 신뢰 및 갱신하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 수동으로 인증서를 등록하려면 신뢰할 수 있는 서드파티 CA(Certificate Authority)에 액세스해야 합니다. 서드파티 CA 벤더의 예로는 Entrust, Geotrust, GoDaddy, Thawte, VeriSign 등이 있습니다.
- FTD(Firepower Threat Defense)에 올바른 클록 시간, 날짜 및 표준 시간대가 있는지 확인합니다. 인증서 인증에서는 NTP(Network Time Protocol) 서버를 사용하여 FTD의 시간을 동기화하는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 6.5를 실행하는 FTDv
- 키 쌍 및 CSR(Certificate Signing Request) 생성에는 OpenSSL이 사용됩니다.

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

인증서 설치

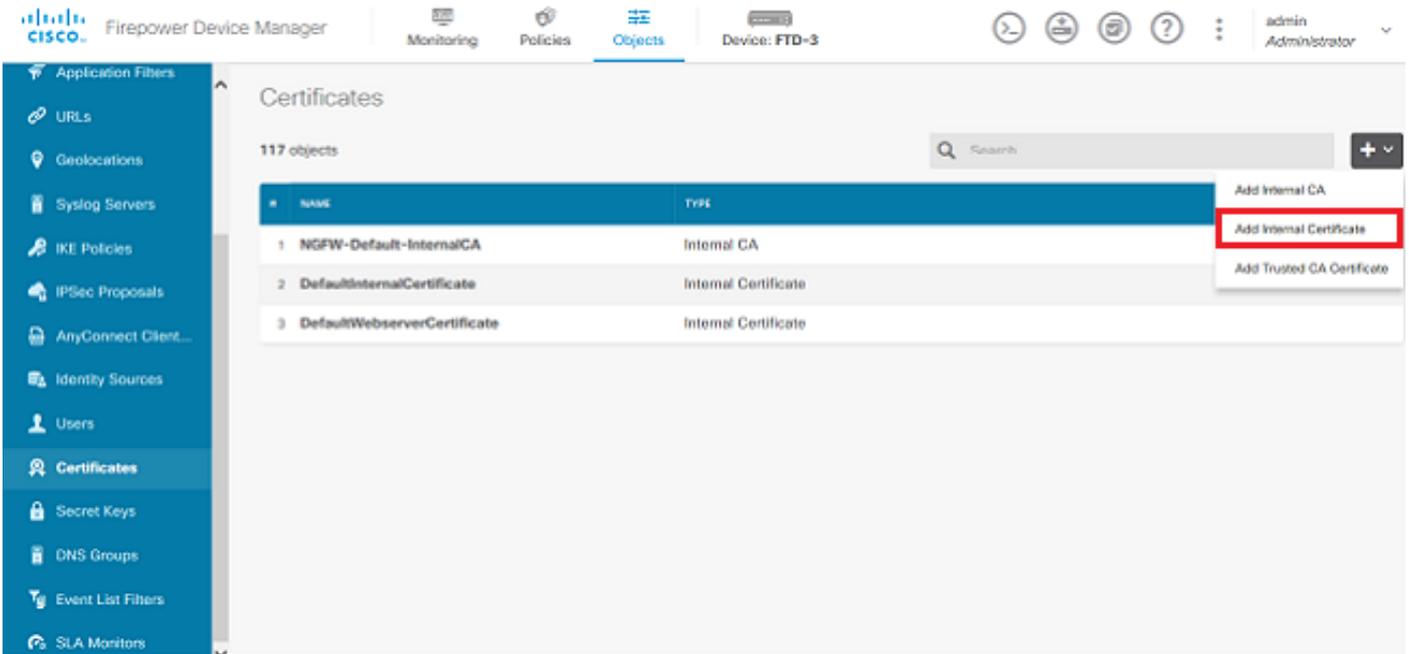
자체 서명 등록

자체 서명 인증서는 해당 필드가 FTD 디바이스에 추가된 인증서를 쉽게 가져올 수 있는 방법입니다. 대부분의 장소에서 신뢰할 수는 없지만 서드파티 서명 인증서와 유사한 암호화 혜택을 제공할 수 있습니다. 그래도 사용자와 다른 디바이스가 FTD에서 제공한 인증서를 신뢰할 수 있도록 신뢰할 수 있는 CA 서명 인증서를 보유하는 것이 좋습니다.

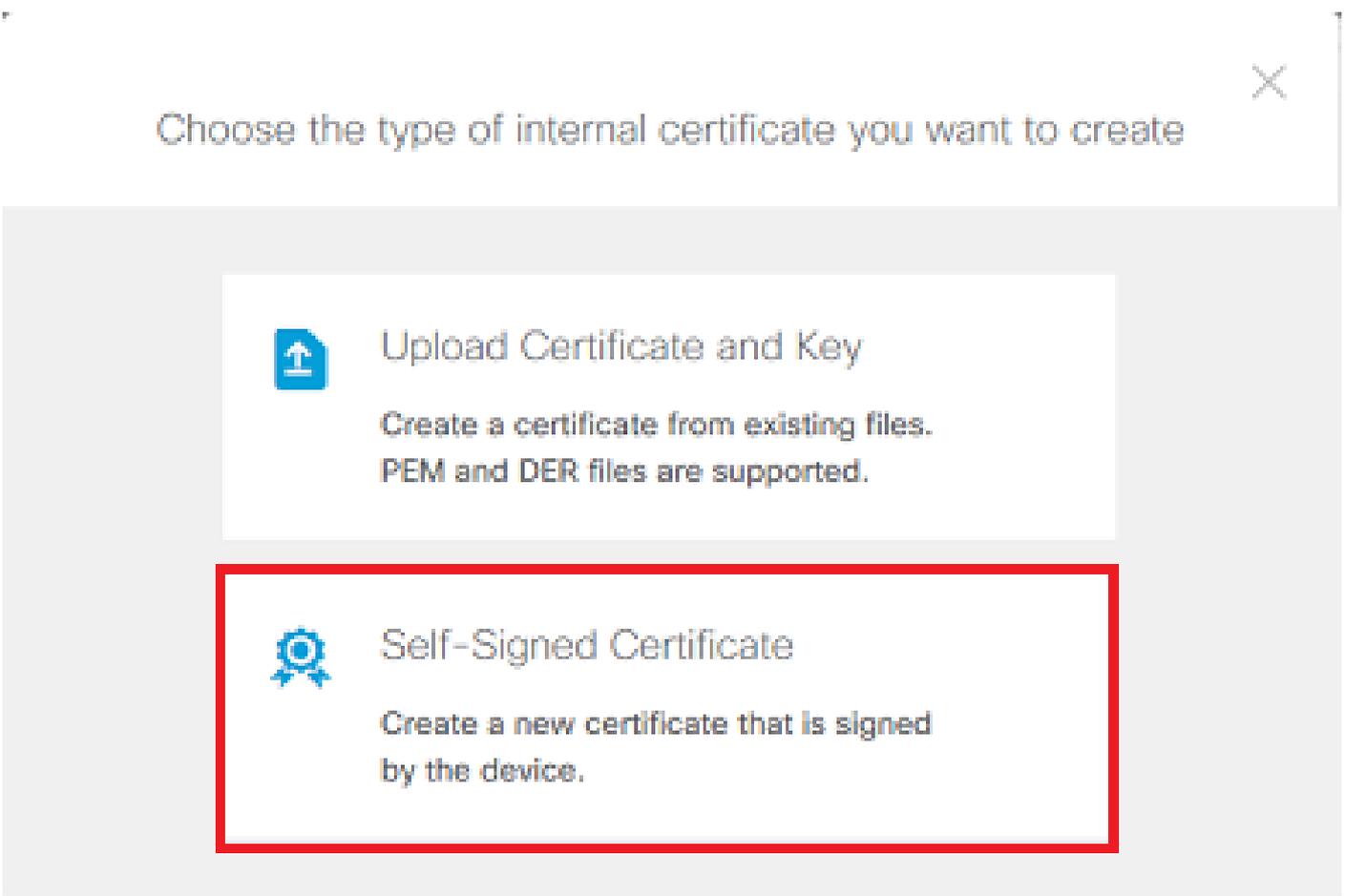


참고: FDM(Firepower 장치 관리)에는 유사한 용도로 사용할 수 있는 DefaultInternalCertificate라는 기본 자체 서명 인증서가 있습니다.

1. 객체 > 인증서로 이동합니다. +기호를 클릭한 다음 이미지에 표시된 대로 Add Internal Certificate(내부 인증서 추가)를 선택합니다.



2. 이미지에 표시된 대로 팝업 창에서 자체 서명 인증서를 선택합니다.



3. 신뢰 지점의 이름을 지정한 다음 주체 고유 이름 필드에 내용을 입력합니다. 최소한 Common Name(공통 이름) 필드는 추가할 수 있습니다. 이는 인증서가 사용되는 서비스의 FQDN(Fully Qualified Domain Name) 또는 IP 주소와 일치할 수 있습니다. 이미지에 표시된 대로 완료되면 저장을 클릭합니다.

Add Internal Certificate



Name

FTD-3-Self-Signed

Country

State or Province

Locality or City

Organization

Cisco Systems

Organizational Unit (Department)

TAC

Common Name

ftd3.example.com

You must specify a Common Name to use the certificate with remote access VPN.

CANCEL

SAVE

4. 화면 오른쪽 상단에서 이미지에 표시된 보류 중인 변경 단추를 클릭합니다.

CISCO Firepower Device Manager

Monitoring Policies **Objects** Device: FTD-3

admin Administrator

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

IPSec Proposals

AnyConnect Client...

Identity Sources

Users

Certificates

Secret Keys

DNS Groups

Event List Filters

SLA Monitors

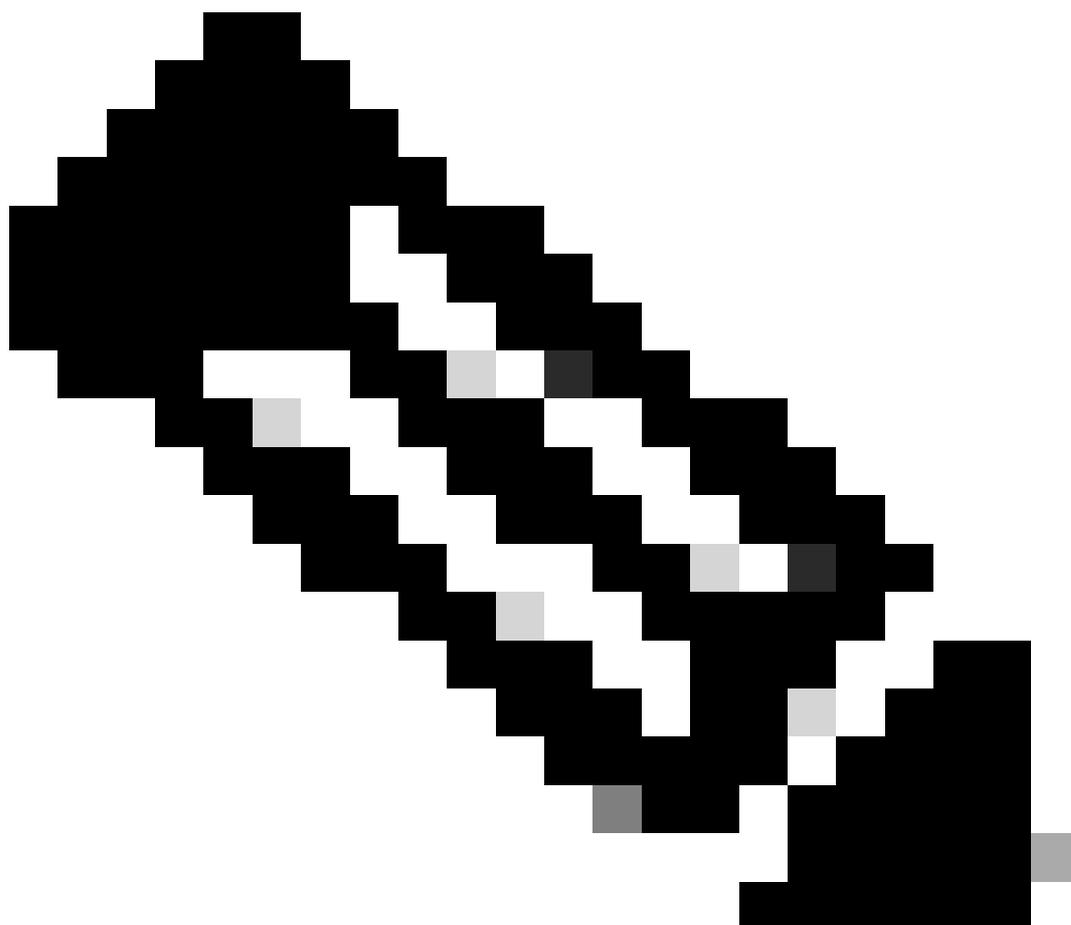
Certificates

118 objects

Search

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Self-Signed	Internal Certificate	

5. 지금 배치 버튼을 누릅니다.



참고: 구축이 완료되면 이미지에 표시된 대로 AnyConnect와 같이 인증서를 사용하는 서비스가 있어야 CLI에서 인증서를 볼 수 있습니다.

The screenshot shows a 'Pending Changes' window with a blue header. A green checkmark indicates 'Last Deployment Completed Successfully' on 13 Apr 2020 09:56 AM. Below this, there are two tabs: 'Deployed Version (13 Apr 2020 09:56 AM)' and 'Pending Version'. The 'Pending Version' tab is active and shows a legend with 'Removed', 'Added', and 'Edited' options. A plus sign icon indicates an 'Internal Certificate Added: FTD-3-Self-Signed'. The certificate details are listed in a table with a light green background:

-	cert.masked: false
-	cert.encryptedString: ***
-	privateKey.masked: false
-	privateKey.encryptedString: ***
-	issuerCommonName: ftd3.example.com
-	issuerCountry:
-	issuerLocality:
-	issuerOrganization: Cisco Systems
-	issuerOrganizationUnit: TAC
-	issuerState:
-	subjectCommonName: ftd3.example.com
-	subjectCountry:
-	subjectDistinguishedName: CN=ftd3.example.com, OU=TAC, O=...
-	subjectLocality:
-	subjectOrganization: Cisco Systems
-	subjectOrganizationUnit: TAC

At the bottom, there are three buttons: 'MORE ACTIONS' (with a dropdown arrow), 'CANCEL', and 'DEPLOY NOW' (highlighted with a red border and a dropdown arrow).

수동 등록

수동 등록은 신뢰할 수 있는 CA에서 발급한 인증서를 설치하는 데 사용할 수 있습니다. OpenSSL 또는 유사한 툴을 사용하여 CA 서명 인증서를 수신하는 데 필요한 개인 키 및 CSR을 생성할 수 있습니다. 이 단계에서는 개인 키 및 CSR을 생성하기 위한 일반적인 OpenSSL 명령과 인증서 및 개인 키를 가져온 후 설치하는 단계를 다룹니다.

1. OpenSSL 또는 이와 유사한 애플리케이션을 사용하여 개인 키 및 CSR(Certificate Signing Request)을 생성합니다. 이 예에서는 private.key라는 2048비트 RSA 키 및 OpenSSL에서 생성된 ftd3.csr이라는 CSR을 보여줍니다.

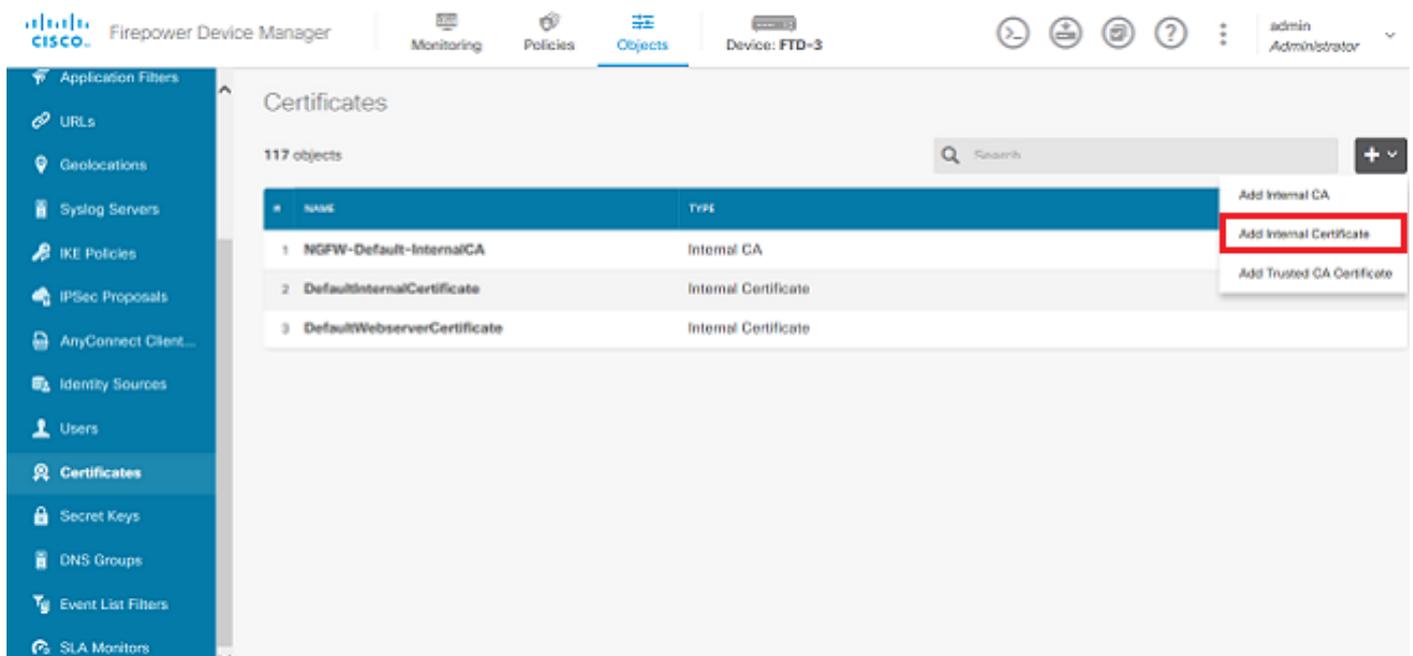
```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'private.key'
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

There are quite a few fields but you can leave some blank
For some fields there is be a default value,
If you enter '.', the field is left blank.

Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd3.example.com
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

2. 생성된 CSR을 복사하여 CA에 보냅니다. CSR이 서명되면 ID 인증서가 제공됩니다.
3. 객체 > 인증서로 이동합니다. 이미지에 표시된 대로 + 기호를 클릭한 다음 Add Internal Certificate(내부 인증서 추가)를 선택합니다.



4. 이미지에 표시된 것처럼 팝업 창에서 인증서와 키 업로드를 선택합니다.



Choose the type of internal certificate you want to create



Upload Certificate and Key

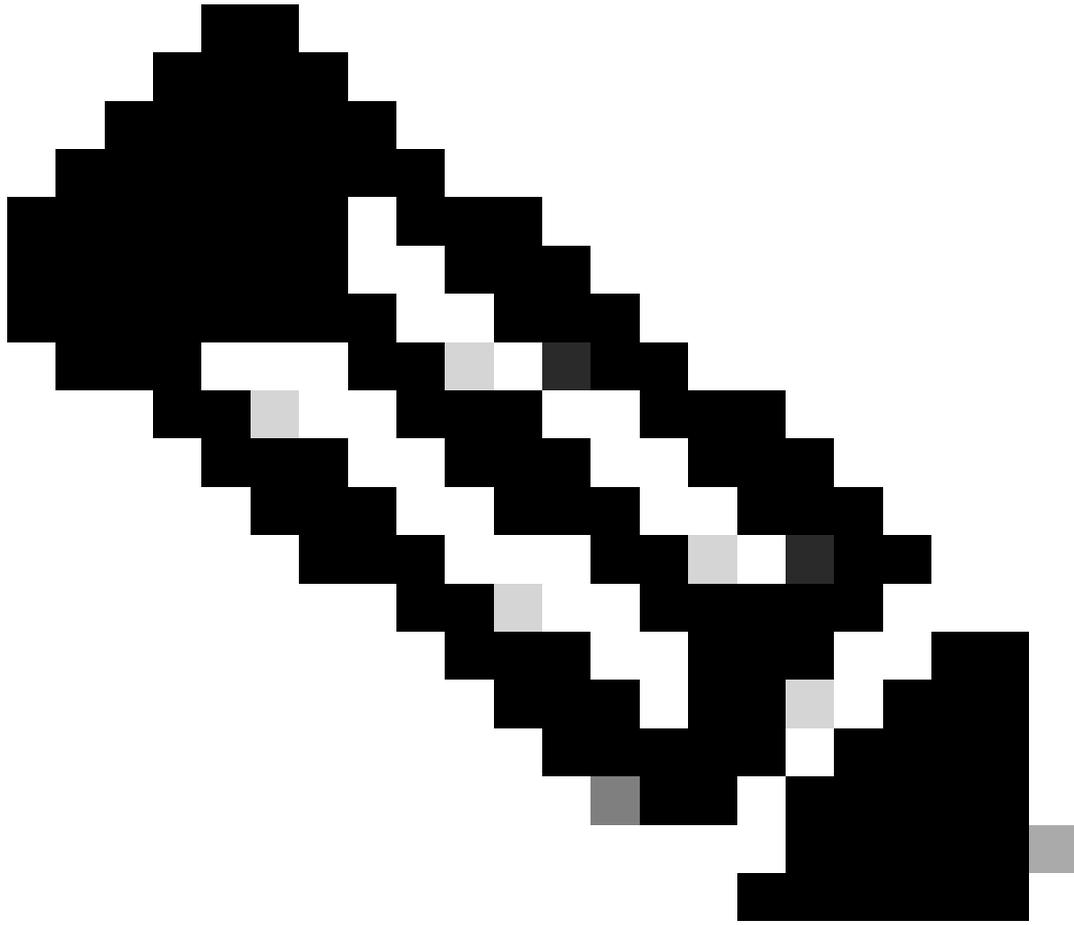
Create a certificate from existing files.
PEM and DER files are supported.



Self-Signed Certificate

Create a new certificate that is signed
by the device.

5. 신뢰 지점의 이름을 지정한 다음 ID 인증서와 개인 키를 PEM(Privacy Enhanced Mail) 형식으로 업로드하거나 복사하여 붙여넣습니다. CA가 단일 PKCS12에서 인증서와 키를 함께 제공한 경우 이 문서의 뒷부분에 나오는 PKCS12 파일에서 ID 인증서 및 개인 키 추출 섹션으로 이동하여 이들을 구분합니다.

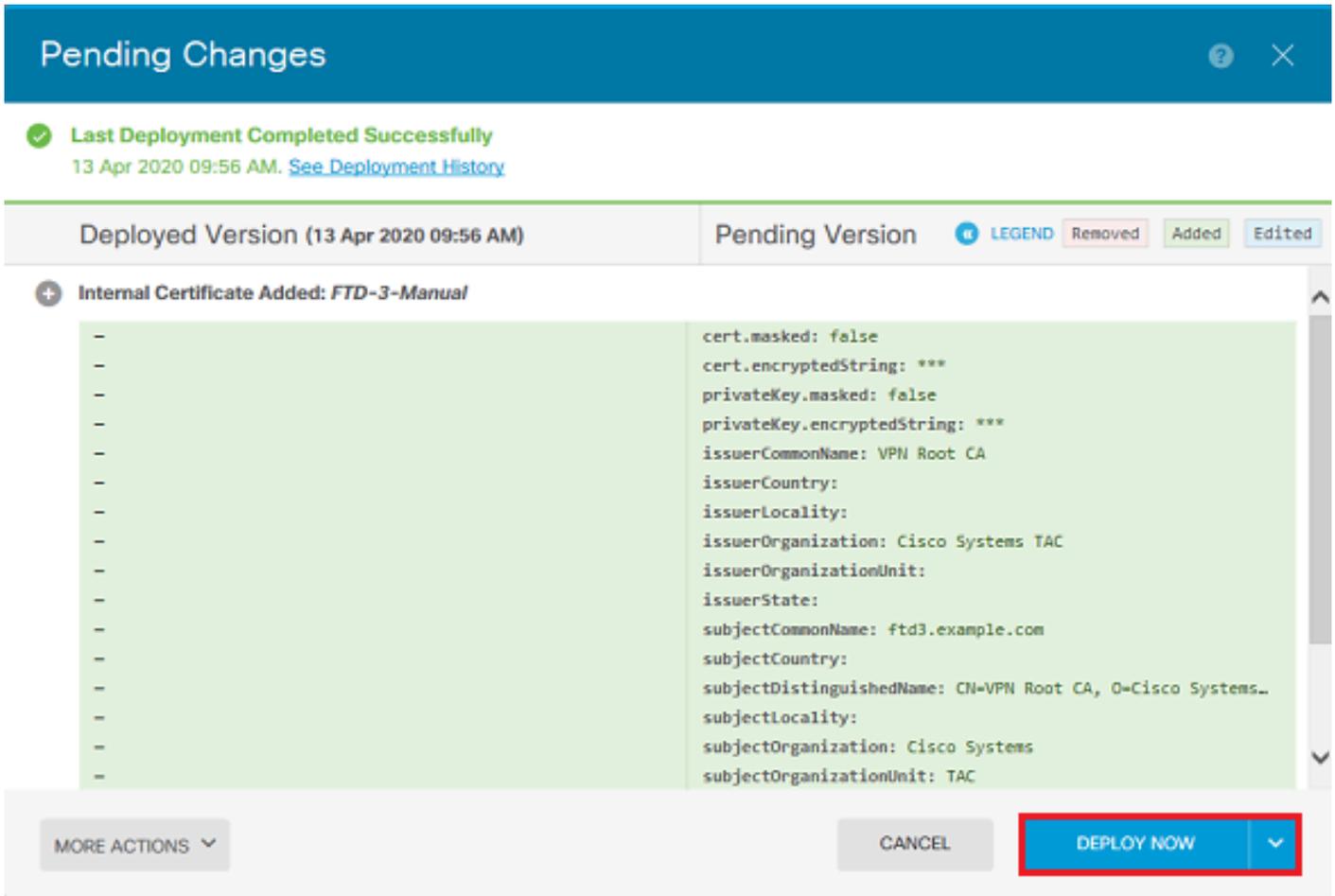


참고: 파일 이름에는 공백을 사용할 수 없거나 FDM에서 이를 허용하지 않습니다. 또한 개인 키는 암호화하지 않아야 합니다.

이미지에 표시된 대로 완료되면 OK(확인)를 클릭합니다.



참고: 구축이 완료되면 이미지에 표시된 대로 AnyConnect와 같이 인증서를 사용하는 서비스가 있어야 CLI에서 인증서를 볼 수 있습니다.



신뢰할 수 있는 CA 인증서 설치

신뢰할 수 있는 CA 인증서를 설치할 때 FTD에 ID 인증서를 제공하는 사용자 또는 디바이스를 성공적으로 인증하려면 이 인증서가 필요합니다. 일반적인 예로는 AnyConnect 인증서 인증 및 S2S VPN 인증서 인증이 있습니다. 이 단계에서는 CA 인증서를 신뢰하여 해당 CA에서 발급한 인증서도 신뢰하는 방법을 다룹니다.

1. 객체 > 인증서로 이동합니다. +기호를 클릭한 다음 이미지에 표시된 대로 Add Trusted CA Certificate(신뢰할 수 있는 CA 인증서 추가)를 선택합니다.

4. 이미지에 표시된 대로 지금 배치 버튼을 클릭합니다.

인증서 갱신

FDM에서 관리하는 FTD의 인증서 갱신에는 이전 인증서와 개인 키 교체가 포함됩니다. 원래 인증서를 생성하는 데 사용된 원래 CSR 및 개인 키가 없는 경우 새 CSR 및 개인 키를 생성해야 합니다.

1. 원래 CSR 및 개인 키가 있는 경우 이 단계를 무시할 수 있습니다. 그렇지 않으면 새 개인 키 및 CSR을 생성해야 합니다. OpenSSL 또는 유사한 애플리케이션을 사용하여 개인 키 및 CSR을 생성합니다. 이 예에서는 private.key라는 2048비트 RSA 키 및 OpenSSL에서 생성된 ftd3.csr이라는 CSR을 보여줍니다.

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd3.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'private.key'
-----
You are about to be asked to enter information that is incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there is a default value,
If you enter '.', the field is left blank.
-----
Country Name (2 letter code) [AU]:.
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco Systems
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd3.example.com
Email Address []:.
```

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

2. 생성된 CSR 또는 원래 CSR을 인증 기관에 보냅니다. CSR이 서명되면 갱신된 ID 인증서가 제공 됩니다.

3. 객체 > 인증서로 이동합니다. 갱신할 인증서 위에 마우스 커서를 올려 놓고 이미지에 표시된 View 버튼을 클릭합니다.

Firepower Device Manager

Monitoring Policies **Objects** Device: FTD-3

admin Administrator

Application Filters

- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- AnyConnect Client...
- Identity Sources
- Users
- Certificates**
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors

Certificates

118 objects

Search

#	NAME	TYPE	ACTIONS
1	NGFW-Default-InternalCA	Internal CA	
2	DefaultInternalCertificate	Internal Certificate	
3	DefaultWebserverCertificate	Internal Certificate	
4	FTD-3-Manual	Internal Certificate	

4. 팝업 창에서 이미지에 표시된 것처럼 Replace Certificate(인증서 교체)를 클릭합니다.

View Internal Certificate

Name

FTD-3-Manual

REPLACE CERTIFICATE

Subject Common Name
ftd3.example.com

Subject Organization
Cisco Systems

Subject Organization Unit
TAC

Issuer Common Name
VPN Root CA

Issuer Organization
Cisco Systems TAC

Valid Time Range
Apr 13 14:56:00 2020 GMT - Apr 13 14:56:00 2021 GMT

CANCEL SAVE

My57eGFtcGx1LmNvbTAeBg1ghkgBhvCAQ0EERYPeGNhIGN1cnRpZm1jYXR1MAOG
CSqGSIB3DQEBcUAA4ICAQCjJrMjruGH5fpcFND8qfuVU0hkszcWq201oMqMrvXn
gENKcXxT27z6AHnQXEX3vhDcY3zs+FzFSOP5tRRPmy/413HAN+QEP2L9MQVD9PH
f50rQ/Ke5c16hMOJ08daR7wNzvFkcBciCKLRH0EvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krg1ugp2UEqOug9HPTpgsbuNcHw8xXgFp6IA10LrytwrLeMIh5V+Vh5p11
yTl9wo5VADoYKGN408D21TeJIj6KB7YnYFB5wMgPGR5h5wx1qNq/MFixwFMXM4T1
Rk3E0dSTENqzq2ZwnqJ4HCoqar7AS1Q5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBU1bad1nEfi5J18G+/vZ16ykcMxe9hokKYxY8cg/U7170n/FbAmdYwRYgMAE4
RwfBp0voNzn97cG+qzogo7j/0kTFYu309DzdU3uy+R8JJkBrerkrZR7w70fP610
IAS86N5Zb18U14Gfc9m0eXHbN+/OB31JNhvWeyZfAbtgU1qstzvb2bc2GBoJJ1XC
YRQ1ft1FxHpn4zMkjI2Px0yam/bR0n0FoMCesHvvtcgcGjFJgZduZyBJ9u1EZ2H5
uwNEJF0iV0GV+UBRigpjXEaUfJj4yMwaMYerZcZQVJfZ75+8SS5rfGfpmWtIT47I
ng==

-----END CERTIFICATE-----

Certificate bag

Bag Attributes: <No Attributes>

subject=/O=Cisco Systems TAC/CN=VPN Root CA

issuer=/O=Cisco Systems TAC/CN=VPN Root CA

-----BEGIN CERTIFICATE-----

MIIFQzCCAyugAwIBAgIIQgRS/woJDigwDQYJKoZIhvcNAQELBQAwMjEaMBGGA1UE
ChMRQ21zY28gU31zdGVtcyBUQUUMxFDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTIw
MDQwNTIzMTYwMFoXDTMwMDQwNTIzMTYwMFowMjEaMBGGA1UEChMRQ21zY28gU31z
dGVtcyBUQUUMxFDASBgNVBAMTC1ZQTiBSb290IENBMBIICiJANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCCGKCAgEAXhTBKiB1xzLg2Jr48h/2u84RcWah0TmPYCNGYZg0PvSf
J0pKvAu5tz4z625Yx1nBtjSsEgzF+qETpSp1EhjW2NxIc1xuNirfrmsJQfIw51yT
PaFv7u+VhgyYbYsSxGAB/m6RWwpiNbg8SDoUACU7R/bvp1Rb8W6tXk/rsT1jc7L2
c/G5MeDLNmc/i/M1zuMjhj0tCphsJPhvNII71cnJ6K0pvg2yB/Md7PX0ZnLaz9pf
Ggpjph0zzKhdIMW/KII64IRpo8KVhpE5X2sFohjzot4u8/t2oP846z/CXm1HQcgp
g5BgZMGqro015rcq0PjtK9Tqg7q013Vf0kM1sofMp+Bu1CiFDpawF/j8uSPuswEs
rzvJ+8Gb0Y1WEHtohgNGjP00q8wnKQu0C47Ft1UMpdSwUsMMze0X43dyp/WoZtLW
4v/Pn/NibE3aoP0aMhIo4CdwSBHZ0gVag4INqVsuFX1uPKD25Whr109LQ93P/sN3
FhoAh98HK0cuQ64Ua3AaShdzornD+G2J2pd1Nf1Dah1z1skIMt1URSwDLjsHLKft
JqS0oLIs2stU8HutUZ4h6Lv2+da554zVjpRTQiYh/1yNexDsd1m6PH7mQj+iL8/9
c2qDhuich3cx11jINOLdB+/jQqkfzmx9ziB1PXnIshNRbf1LLrNfdD09agqQsvsC
AwEAAaNdMfswDAYDVR0TBAAUwAwEB/zAdBgNVHQ4EFgQUd6TMOeGLg7vbuaMte7AJ
FUWDKc4wHwYDVR0jBBgwFoAUd6TMOeGLg7vbuaMte7AJFUWDKc4wCwYDVR0PBAQD
AgEGMAOGCSqGSIB3DQEBcUAA4ICAQC6B+Y3obatEZqv0RQz1MS6oUmCgNwGi8d
kcRDxkY2F+zw3pBFa54Sin10FRPjvZvLNJV50dXmVH51uh6KJDMVrLMWniSgI7Tn
0ipqKraokS20o0STwQ7Q9wK1xCrwxMfTuDJFMe80qabFAU55705PDXPtFEutn0xz
Ou8VMLBRY+gDc+0WARsjFj+0gU0c2Wj3gQ81G1yoPYgufWRnztn5rQxwzFLSsCNN
jnIesjQv0vF3nY7SH5QasPN25AysGE0DFgp7rZLN2BH7G9rhi5hEn3Bv9ALZCQ6
p702FZ1y51xuzuA/wPnR89HiIkSF130MTpn0I13d6d07s3bwyNja8JikYTCf11e5
2CSsz4Cn/B1wfWyAcLN3HxUjG4Ev2818fWwPkYmuxujpKDFfZf0skpKAK53tNKPF
pn4+w5FyLo18o0AydtpoKjYkdqBvG/SRPbt92mdTIF7E6J+o8J60V3YL+IyrZ+u0
MYqPd450i4cgHdMFICandN3PYSrRGYHawfVxp+R+G4dTJWdMvthh3ftS0mkiKJ8
m1NH7WYST1kYcTbcokZi0IcZa+VvV5UOLIt/hD0VG7xqZ01pMQkKYUBzg5LbGINm
8ypfhQ1faI5fQRxpTIsmDv9rQzxBjuCyKn+23FkkUhfJt0D989UUyp08H9vDoJr
yzm9J0pMrg==

-----END CERTIFICATE-----

PKCS7 Data

Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048

Bag Attributes

localKeyID: 28 20 C1 B4 08 1E 65 2E 4D 1D F9 F3 25 07 62 F7 D9 96 A7 F4

friendlyName: ftd3.example.com

Key Attributes: <No Attributes>

Enter PEM pass phrase: [private-key-passcode]

Verifying - Enter PEM pass phrase: [private-key-passcode]

-----BEGIN ENCRYPTED PRIVATE KEY-----

MIIFDjBAbGkqhkiG9w0BBQowMzAbBgkqhkiG9w0BBQwwDgQIScA8T0ogup4CAggA
MBQGcCqGSIB3DQMHBAGkQoTuZzoXsASCBMg0TEb24ENJ14/qh3GpsE2C20CnJeid
ptDDIFdy0V4A+su30JWz1nHrCuIhJr8+/p/NOW1A73x47R4T6+u4w4/ctHkVebQj
gZJZzFWTed9Hqi dhcKxx0oM/w6/uDv/opc6/r1IZiaKp6F09h0ibq1GI9kjkWQC

EQR8cM1U2yi0vagL8p0YdeujCrzBtorRp9BMJe1CP1Mw9t0EbAC4mmuedzs+86r1
xadK7qHBUWUJc03SLXLcMx5yLSGteWcoaPZnIK09UhlxpUSJTkwLHr2VtE1ACMRc
R1PBXMLb70nMtPTqct158+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb
M6ZTWt0Z1sn0f4ohVePrW/kkd1QavJbPa+0dzjZvs88C1EXAJ/XIEgfSwifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jj1KgfouxbntuFq
un4EJD73K9RWeA+7IVmEceRTBMyFD+ZwZH0BuF1s+wZEmzYqw+cuc+I8XEFVOM18
P3ah28Nno0jXmk4MpFfJ1YMcMq66xj5gZtcVZx0GCOsw0CKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UuWi5Zp/NrbN31HkP0wt7+1DFGFit1pTTGv0FchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG115NSs1wKbtGiiwCYw0N8c09TXQb04rMomFDAv8
aef1aBsJmQEUkz0ZK0U2ZgTxM1ine8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfv+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc40
w94fQH/DJ/1KsmSVwBLQLEKR1/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaQ8
fN17vEB+aret+PmqCiQY1Hqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUR0TuBHQhRK
3XpHfGxpe/00GdW3LeiFNlvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzd0cJ3aGCeA184XuPRfQhHe/Aj7q616uqB
W3Kt+kMj9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRk3mx+8a1YLqk+h0MjWwBDEHX2mvbdKicK/jhwRdR/WmFOALq51phgtZ1z
Zed15UbPqWahJsjo09N5pp7Uq5iV0/xq4M1+/xQIYo2GIrQyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTFzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcd/okRRKZpmjH+ijp
FPD/WgQ/vm09HdCwW3f1hqceqfHff8C1CJYFLxsgZp4M3G+WyQTKy4J8+6uTn/mj
yyZ5JCZd1t42haSNqu/ynioCjh5XY4m8WMZs0JBNPjKziUX/vqVcc+/nod17VRZy
ELk=
-----END ENCRYPTED PRIVATE KEY-----

pkcs12file.pfx는 패키지 해제해야 하는 pkcs12 파일입니다.

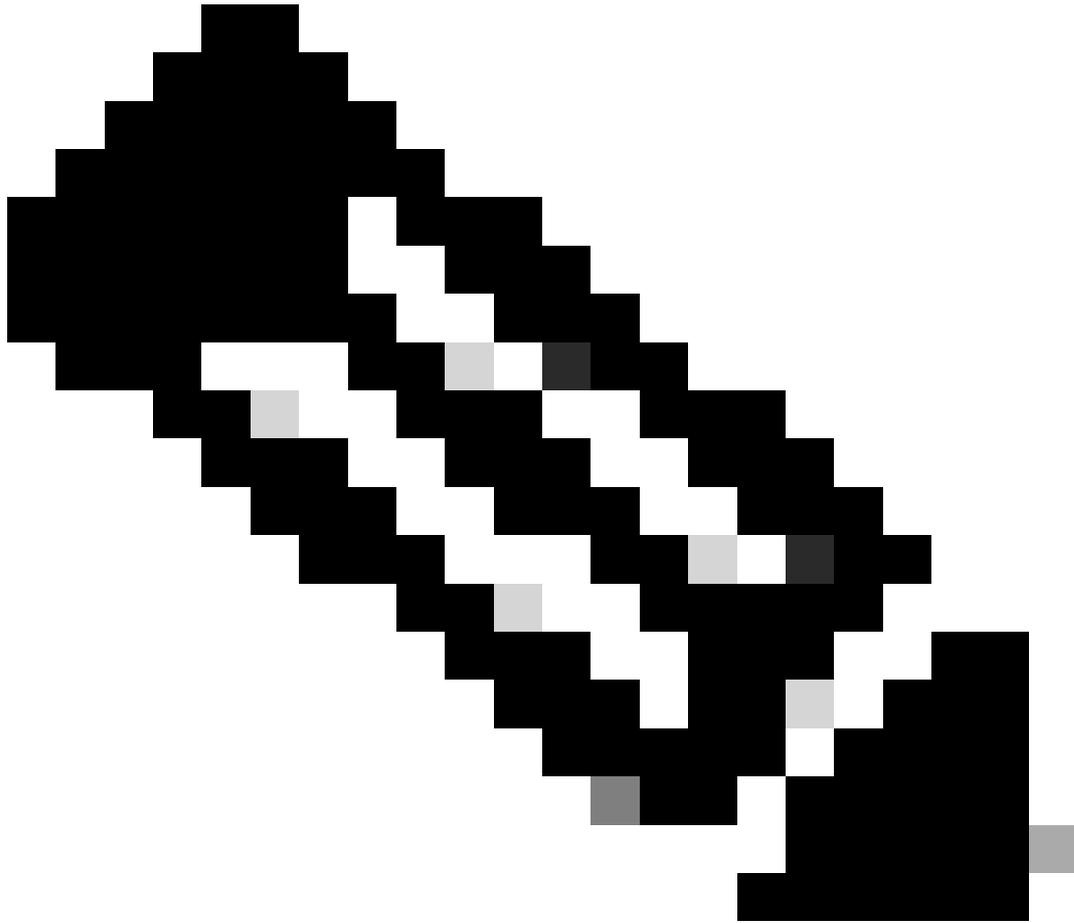
이 예에서는 세 개의 개별 파일이 생성됩니다.

ID 인증서용 1개. subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com으로 인해 ID 인증서
임을 알 수 있습니다.

```
subject=/O=Cisco Systems/OU=TAC/CN=ftd3.example.com
issuer=/O=Cisco Systems TAC/CN=VPN Root CA
-----BEGIN CERTIFICATE-----
MIIErTCCApGwAwIBAgIIa5PmhHEIRQUwDQYJKoZIhvcNAQELBQAwMjEaMBgGA1UE
ChMRQ21zY28gU31zdGVtcyBUQUUMxZDASBgNVBAMTC1ZQTiBSb290IENBMB4XDTEw
MDQxMzE2NDQwMFoXDTEwMDQxMzE2NDQwMFowQTEwMBQGA1UEChMNQ21zY28gU31z
dGVtcyEMMAoGA1UECXMDFEFDMDRkZmVhY2V0Y2V0Y2V0Y2V0Y2V0Y2V0Y2V0Y2V0
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnGpzMjuf+HtRG5ZYf80V6V1s
SyF7XhRxpjR180wUih5wBz6qNntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGb
myNz+A6jgNqAkTvaFMZV/RrWqCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqN
Bqotoz3/8CrZ0IcpzVqL6h0ziJFBgdiWJEYBoFuE1jmmsjI3qd39ib9+t6LhkS50
QpQDTgviD1bYpPiWkpS0g1PZDnX8b740s0pVKVXTsujQqSqH1va9BB6hK1JCoZa
HrP9Y0x09+MpVMH33R9vR13S0EF6kpZ6VEdGI4s6/IRvaM1z1BcK10N/N2+mjwID
AQABo4G3MIGOMAKGA1UdEwQCAAwHQYDVR0OBBYEFMcvjL0XiSTzNADJ/ptNb/cd
zB8wMB8GA1UdIwQYMBaAFHekzDnhI40727mjLXuwCRVfgyguMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwGwYDVR0RBBQwEoIQZnRk
My51teGfTcGx1LmNvbTAeBg1ghkgBhvCAQ0EERYPEGNhIGN1cnRpZm1jYXR1MAOG
CSqsGSIB3DQEBcUAA4ICAQCjJrMjruGH5fpcFND8qfVU0hkszcwq201oMqMrvXn
gENKcXxxT27z6AHnQXeX3vhDcY3zs+FzFSop5tRRPmy/413HAN+QEP2L9MQVD9PH
f50rQ/Ke5c16hMOJ08daR7wNzvFkcbicKCLRHOEvEoI0SPKsLyGSSxGmh6QXfZcM
GX3jG9Krg1ugp2UEqOug9HPTpgsbuNcHw8xXgFp6IA10LrytwrLeMIh5V+Vh5p11
yT19wo5VADoYKgn408D21TeJiJ6KB7YnYFB5wMgPGR5h5wx1qNq/MfixwFMXMT1
Rk3E0dSTENqzq2ZwnqJ4HCoqar7AS1Q5Zub5NY4+QfEpt8UHfYszp/e1BA+TviUC
DXGBU1bad1nEfi5J18G+/vZ16ykcMxe9hokKYxY8cg/U7170n/FbAmdYwRYgMAE4
```


R1PBXMLb70nMtPTqct158+Q/axtQCWUs8caHs3LvVf0nRG+War49/F8Ii8mqnNnb
M6ZTWT0Z1sn0f4ohVePrW/kkd1QavJbPa+0dzjZvs88C1EXAJ/XIegfSwifJAXqP
3d37VonXX7YRocJ4kzhkuE/SUDsu1sMC0hbM81uZcWiBbDAT2jjlKgfoxubtnuFq
un4EJD73K9RWeA+7IVmEceRTBMyfD+ZwZH0BuFls+wZEmzYqw+cuc+I8XEFVOM18
P3ah28Nno0jXMk4MpfFJlYMcMmq66xj5gZtcVZxOGC0swOCKU0JiFFQTEmmVf9/C
65a96np7YCI8s6UnUwi5Zp/NrbN31HkP0wt7+1DFGFit1pTTGvOFchtLYWeB3Kj0
h/C/R7ciq6ZNCzwBrbztGV8jG115NSs1wkBTGiiwCYw0N8c09TXQb04rMomFDV8
aef1aBsJMqEUkz0ZK0U2ZgTxMline8pqNs/BhWBCYGSNmnWDJ7UmdkdqCpKIubp0
qtmFX/DtSu9J2yevfV+3/YCwnSRkr02oTGs1jJkEM2wzTaAeEQfShQMCHQPHtc40
w94fQH/DJ/1KsmSVwBLQLEKR1/nIDz36kmA27+1nVtX42PbEaIaFgucU4xHKx3zN
mgSdbz7ikgiggNm+Dxq9GmYs+FuogaiiNdtvqNIHGq+LaQDwIPBBXmajXPhHVaq8
fN17vEB+aret+PmqCiQY1Hqe5TXcv6j7+VF4RTVpt5au9iX74sZ1qUR0TuBHQhRK
3XpHFGXpe/00GdW3LeifNLvrrQwyICoV9h7MNSpykbn/5wEpX671SqfZgrH6wNbP
VI9A+cSAAT1bWkuywx2uEo+9g1w/IFzd0cJ3aGCeA184XuPRfQhHe/Aj7q616uqB
W3Kt+kMJ9j8AIyQD58SvfpC7bGb26jE/+Mm1Peh+HmyjIF/zv/FQPwPf+TRpcM8/
QCyhIRk3mx+8a1YLqK+h0MjWwBDEHX2mvbdKicK/jhwRdR/WmFOALq51phgtZ1z
Zed15UbPqWahJsjo09N5pp7Uq5iV0/xq4M1+/xQIYo2GIrQyat4AdB2B6K8K3xQd
Pip/Q2/ttdKLyEDP3U/6rsu74zo3b/iXe2MZWTTFzH5zgneUwLwnuBAbGT3oMSQ/
OKXnhcmUGu8XvLEfU/PITvGzKr06o12/hHJtzXQ8eNPDJbvcd/okRRKZpmjH+ijp
FPD/WgQ/vm09HdCwW3f1hqceqfHff8C1CJYFLxsgZp4M3G+WyQTKy4J8+6uTn/mj
yyZ5JCZd1t42haSNqu/ynioCjh5XY4m8WMZs0JBNPjKZiUX/vqVcc+/nod17VRZy
ELk=

-----END ENCRYPTED PRIVATE KEY-----



참고: 개인 키는 암호화되며 FDM은 암호화된 개인 키를 허용하지 않습니다.

개인 키의 암호화를 해제하려면 암호화된 개인 키를 파일에 복사한 다음 이 openssl 명령을 실행합니다.

```
openssl rsa -in encrypted.key -out unencrypted.key
Enter pass phrase for encrypted.key: [private-key passphrase]
writing RSA key
```

- encrypted.key는 암호화된 개인 키를 보유한 파일의 이름입니다.
- unencrypted.key는 암호화되지 않은 키가 있는 파일의 이름입니다.

암호화되지 않은 개인 키는 다음 예에서 볼 수 있듯이 -----BEGIN ENCRYPTED PRIVATE KEY-----이 아닌 -----BEGIN RSA PRIVATE KEY-----을 표시할 수 있습니다.

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEAAnGpzMjuF+HtRG5ZYf80V6V1sSyF7XhRxjR180wUih5wBz6qN
ntQkd0JPog+CFqEXswTpeI7ibPMtaTEVUEzcBpGmyNz+A6jgNqAkTvaFMZV/RrW
qCNkt08ULEbIX+f67TMMBhtfZ2dpapEP2wQ2DVqNBqotoz3/8CrZOIcpzVqL6hOz
iJFBgdiWJEYBoFuE1jmmSJi3qd39ib9+t6LhkS50QpQDTgvIiD1bYpPiWKpS0g1P
ZDnX8b740s0pVKVXTsuJqQsqH1va9BB6hK1JCoZaHrP9Y0x09+MpVMH33R9vR13S
OEF6kpZ6VEdGI4s6/IRvaM1z1Bck10N/N2+mjwIDAQABAoIBAEQzCd1KMBrosdmk
eRvoMPi aemBbze2cX1JWXZ2orICSXhvM0okBGJFDQXN47ZCuVqYAq0ecjU9RzGgE
NbXYfUsD6+P91k+/Gj1RiCNLBHBwdgewzw1quTxP54zSpAV1IXyQ+Fo1TzjH1yfw
7iHhuSuJySAYLWPy4Yg3NpU2IdzeQoK5ViuSTTNx8LHYBKw1Qf7HVaQTfmsW0Ayg
/vjZqjRkukqKM41srgk0/HjPnEBDuUWVTehzMCk1etijENC7ttISzYIEMNPthe60
NpidXAHoJ11JM6HB9ZraBH5fu7MJZJZ00n6YVKQuCdW0WfnKiNQCDsXq7X5Ewsaj3
cgyjw1kCgYEAy33k1wxp7WEqg1zEwq0Vq7AtoL6i4V9QCenMThQAHwNAAUGGOSIF
JhpKyApm/BUogSIOMzIPse+NgAA66TRn4qfkbpvTI98CeCuxiUPcbRmqZnYxC0fp
Pzosv50nBL1toIoprI02S5a261w6JGNAFD95tCjCYrB8Cw/HbZOLPUCgYEAxMbZ
KVyosBxaAIFQinHaff3fVSTsEOZFPcBbLybgLcP8LsLdahBsJ6HK/hAffKX0dvm
35CAM7ZL/WCI1Jb+dx4YcD9q81bVMu4HTvS12deTZoZrBG2iFX60Ssn2rLKAH+cH
uLSHCNAj9cj9syldErGLZtBQpJtpLRd6iy0vMCgYBP/zoLYJHOBBLWeY3QioLO
cABABTG7L+EjRIpQ14QERr5oX/4IT9t+Uy+63HwH9b1qqpye6e359jUzUJbk4KT
1DU1VoT2wSETYmvK7qa1LUXT6fr12FtVw+T7m2w5azwxshDuBQmRRbq7ZBJnY61i
KwIJVUy1U/tSE9LsN1McUQKBgQC1c4ykeoRbj3sdcZ2GyrQru4pMzP6wNu3Xy5EH
HI6ja0i74ImCJDcY5/o/vjx7qb39qBJa5+Tj1iP0p5x1I5BSF7v0pV4G5Xvd1sY0
XSYWRGxriBnzXzspV3/M4oPGMVAJgve7Fg90GY4i2xx1yBH+geCf+CqnDt53Zhs7
YVz6gQKBgQDG42tZZ1kNAn0x/k1U1ZrEeF8iqdsyVcRf4fAvqsPbY3+kdae+80r
+cQpVoeWzOQLUKA6eMsiTLmcWYb62qMgdpluyKo0ciPG9+2AGNTvQp/ig34pF2F/
90GuVY1A1p7mkP8Vb1Mo1ugV0zUqAIjHKiGUzBWVsx0ZsGa+SY47uw==

-----END RSA PRIVATE KEY-----

개인 키를 암호화하지 않으면 ID 및 개인 키 파일을 업로드하거나 앞서 언급한 수동 등록 섹션의 3단계를 사용하여 FDM에 복사하여 붙여넣을 수 있습니다. 앞에서 설명한 신뢰할 수 있는 CA 인증서 설치 단계를 사용하여 발급 CA를 설치할 수 있습니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

FDM에서 설치된 인증서 보기

1. 객체 > 인증서로 이동합니다. 확인하려는 인증서 위에 마우스 커서를 올려 놓고 이미지에 표시된 것처럼 보기 버튼을 클릭합니다.

Firepower Device Manager

Monitoring Policies **Objects** Device: FTD-3

admin Administrator

Application Filters

- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- AnyConnect Client...
- Identity Sources
- Users
- Certificates**
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors

Certificates

118 objects

Search

NAME	TYPE	ACTIONS
1 NGFW-Default-InternalCA	Internal CA	
2 DefaultInternalCertificate	Internal Certificate	
3 DefaultWebserverCertificate	Internal Certificate	
4 FTD-3-Manual	Internal Certificate	

2. 팝업 창에는 그림과 같이 인증서에 대한 추가 세부사항이 표시됩니다.

View Internal Certificate

Name

FTD-3-Manual

REPLACE CERTIFICATE

Subject Common Name
ftd3.example.com

Subject Organization
Cisco Systems

Subject Organization Unit
TAC

Issuer Common Name
VPN Root CA

Issuer Organization
Cisco Systems TAC

Valid Time Range
Apr 13 16:44:00 2020 GMT - Apr 13 16:44:00 2021 GMT

CANCEL **SAVE**

CLI에서 설치된 인증서 보기

FDM에서 CLI 콘솔을 사용하거나 FTD에 SSH를 사용하여 `show crypto ca certificates` 명령을 실행하여 이미지에 표시된 대로 인증서가 디바이스에 적용되었는지 확인할 수 있습니다.

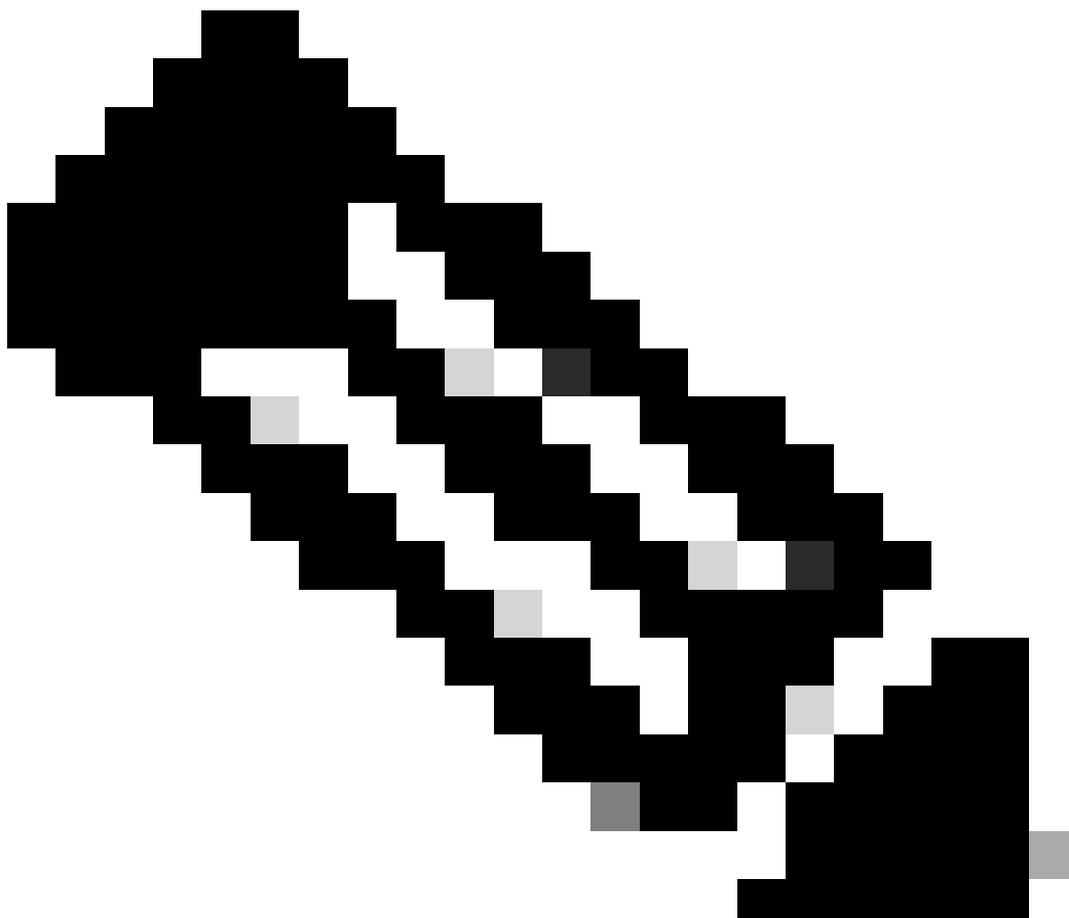


출력 예:

```
> show crypto ca certificates
```

Certificate

```
Status: Available
Certificate Serial Number: 6b93e68471084505
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
  cn=VPN Root CA
  o=Cisco Systems TAC
Subject Name:
  cn=ftd3.example.com
  ou=TAC
  o=Cisco Systems
Validity Date:
  start date: 16:44:00 UTC Apr 13 2020
  end date: 16:44:00 UTC Apr 13 2021
Storage: config
Associated Trustpoints: FTD-3-Manual
```



참고: ID 인증서는 AnyConnect와 같은 서비스와 함께 사용되는 경우에만 CLI에 표시됩니다. 신뢰할 수 있는 CA 인증서는 배포된 후에 나타납니다.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

디버그 명령

SSL 인증서 설치 실패 시 SSH를 통해 FTD를 연결한 후 진단 CLI에서 디버그를 실행할 수 있습니다. `debug crypto ca 14`

이전 버전의 FTD에서는 이러한 디버그를 사용할 수 있으며 문제 해결에 권장됩니다.

```
debug crypto ca 255
```

```
debug crypto ca message 255
```

debug crypto ca transaction 255

일반적인 문제

ASA에서 내보낸 PKCS12 가져오기

OpenSSL에서 내보낸 ASA PKCS12에서 ID 인증서 및 개인 키를 추출하려고 하면 다음과 유사한 오류가 발생할 수 있습니다.

```
openssl pkcs12 -info -in asaexportedpkcs12.p12
6870300:error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag:tasn_dec.c:1220:
6870300:error:0D07803A:asn1 encoding routines:ASN1_ITEM_EX_D2I:nested asn1 error:tasn_dec.c:386:Type=PK
```

이 문제를 해결하려면 먼저 pkcs12 파일을 DER 형식으로 변환해야 합니다.

```
openssl enc -base64 -d -in asaexportedpkcs12.p12 -out converted.pfx
```

이 작업을 마치면 ID 인증서 및 개인 키를 가져오기 위해 이 문서의 앞부분에 있는 PKCS12 파일에서 ID 인증서 및 개인 키 추출 섹션의 단계를 따를 수 있습니다.

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.