FMC에서 관리하는 FTD에 인증서 설치 및 갱신

목차

소개

이 문서에서는 FMC에서 관리하는 FTD에 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 CA에 액세스해야 합니다.
- 서드파티 CA 벤더의 예로는 Entrust, Geotrust, GoDaddy, Thawte, VeriSign 등이 있습니다.
- FTD에 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 FMCv
- 6.5를 실행하는 FTDv
- PKCS12 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.

배경

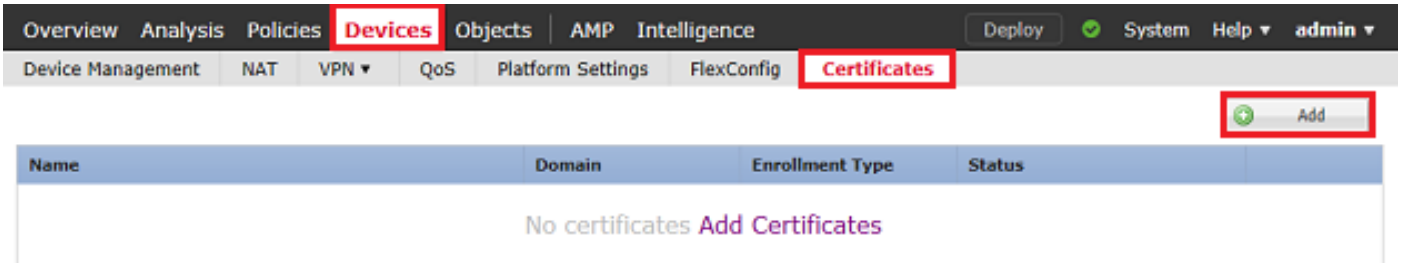
이 문서에서는 FMC(Firepower Management Center)에서 관리하는 FTD(Firepower Threat Defense)에 서명한 타사 CA(Certificate Authority)나 내부 CA가 자체 서명한 인증서와 인증서를 설치, 신뢰 및 갱신하는 방법에 대해 설명합니다.

구성

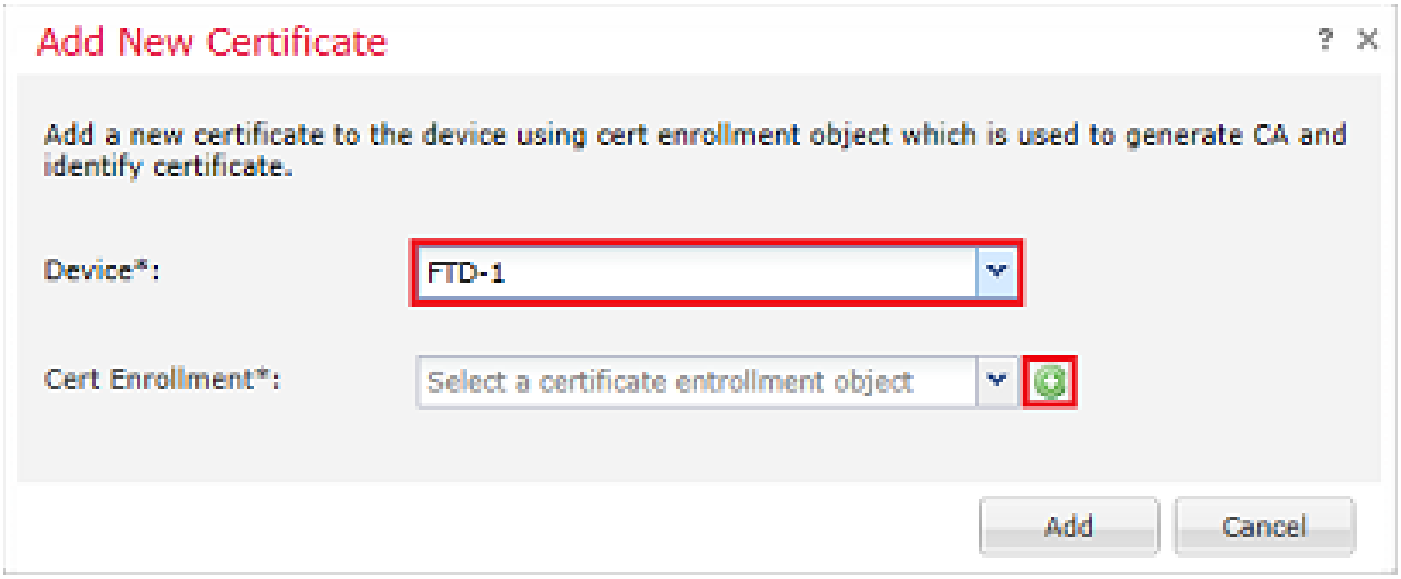
인증서 설치

자체 서명 등록

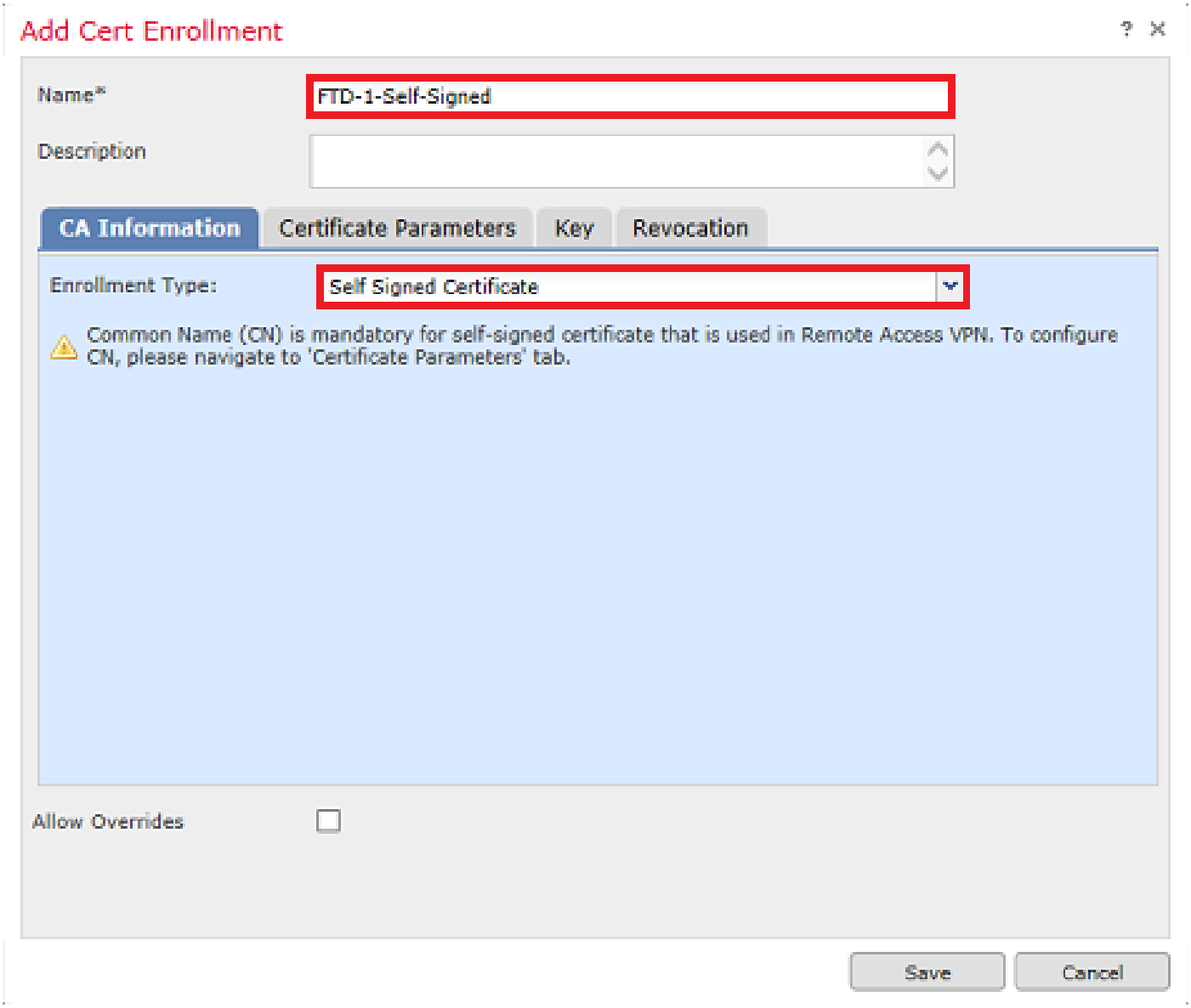
1. 이미지에 표시된 대로 Devices(디바이스) > Certificates(인증서)로 이동한 다음 Add(추가)를 클릭합니다.



2. 장치를 선택하고 장치* 드롭다운에서 인증서가 추가됩니다. 그런 다음 이미지에 표시된 녹색 + 기호를 클릭합니다.

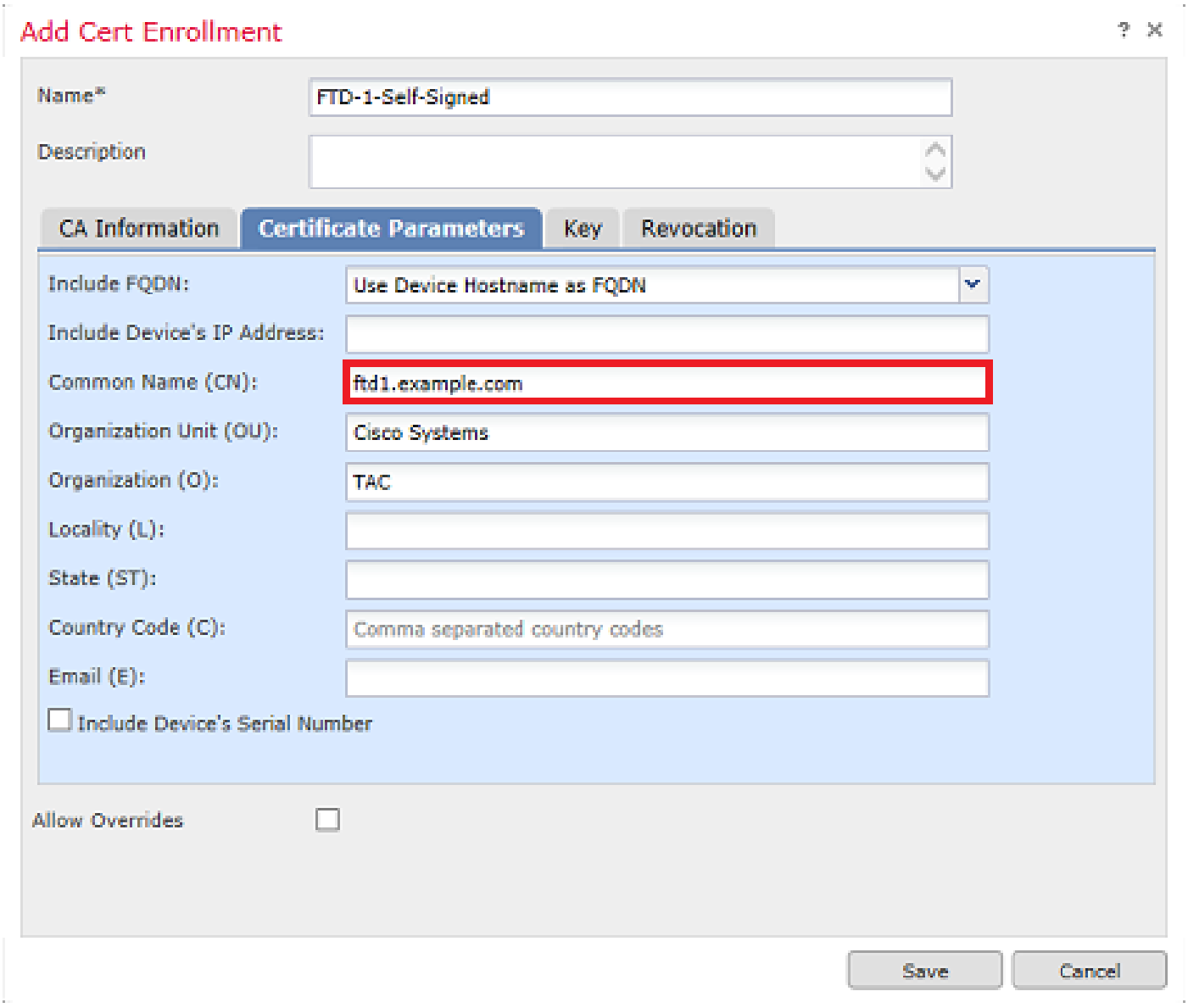


3. 신뢰 지점의 이름을 지정하고 CA Information(CA 정보) 탭 아래에서 Enrollment Type(등록 유형): Self Signed Certificate(자체 서명 인증서)를 선택합니다.

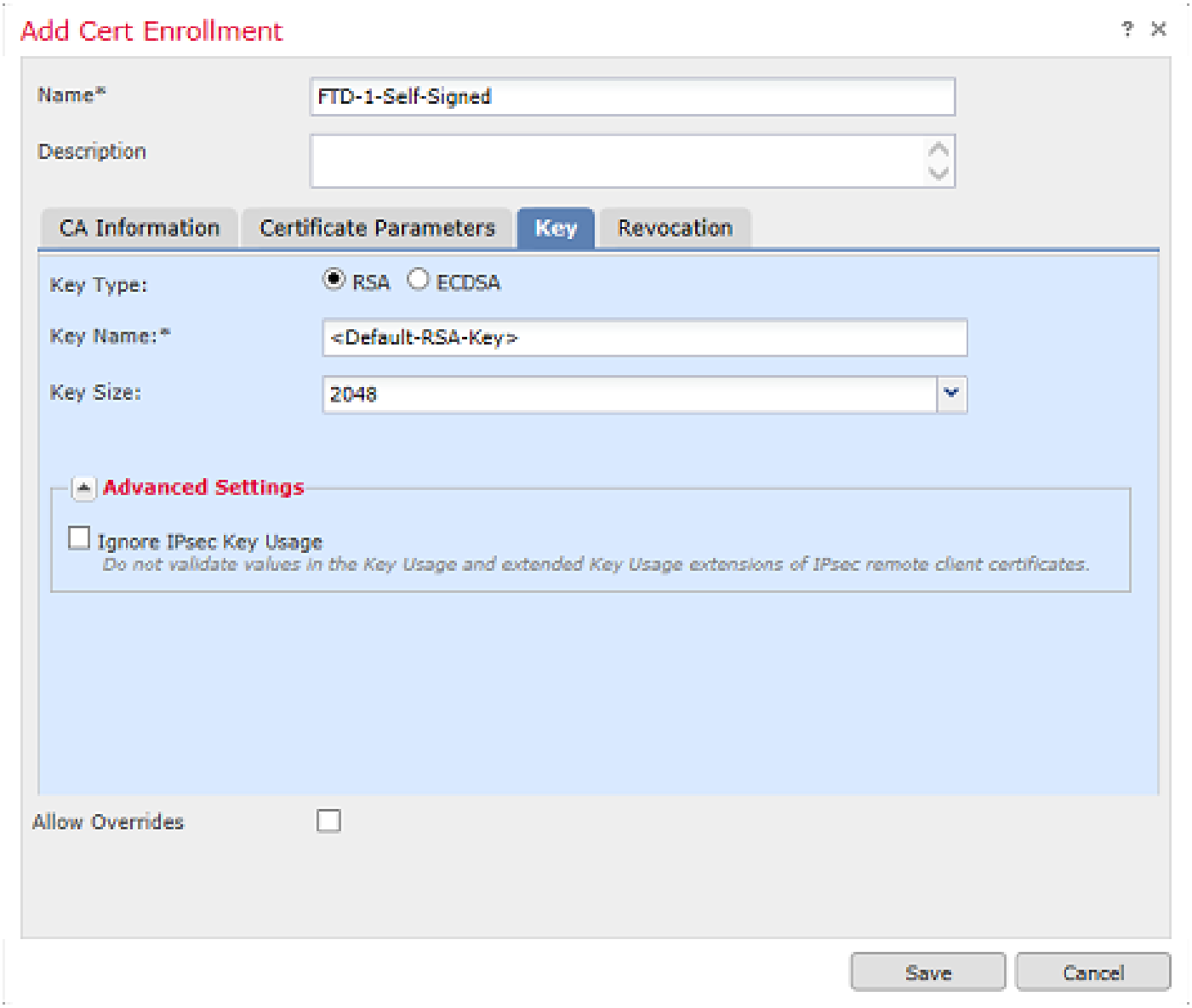


4. Certificate Parameters(인증서 매개변수) 탭 아래에 인증서의 CN을 입력합니다. 이는 이미지에

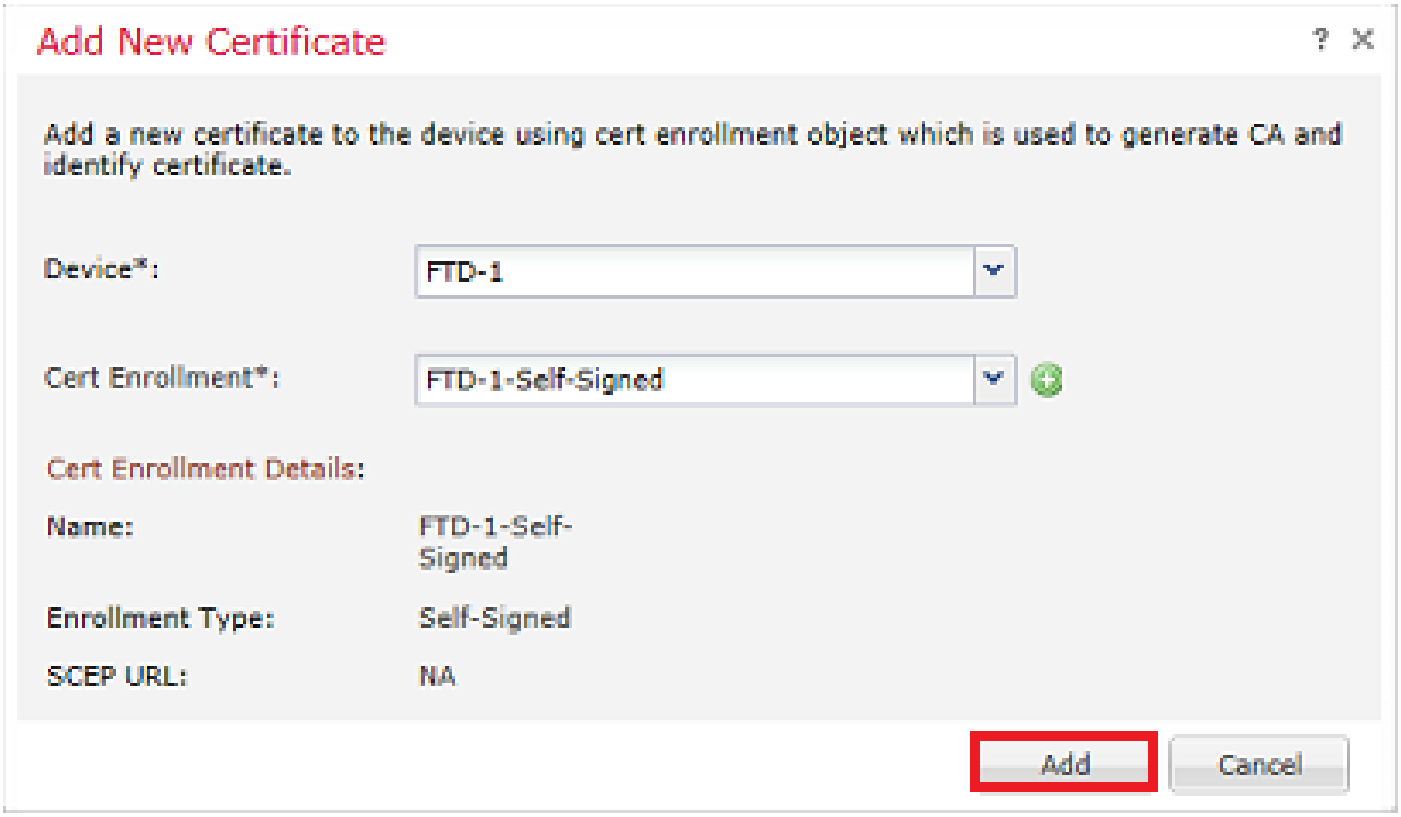
표시된 대로 인증서가 사용되는 서비스의 fqdn 또는 IP 주소와 일치해야 합니다.



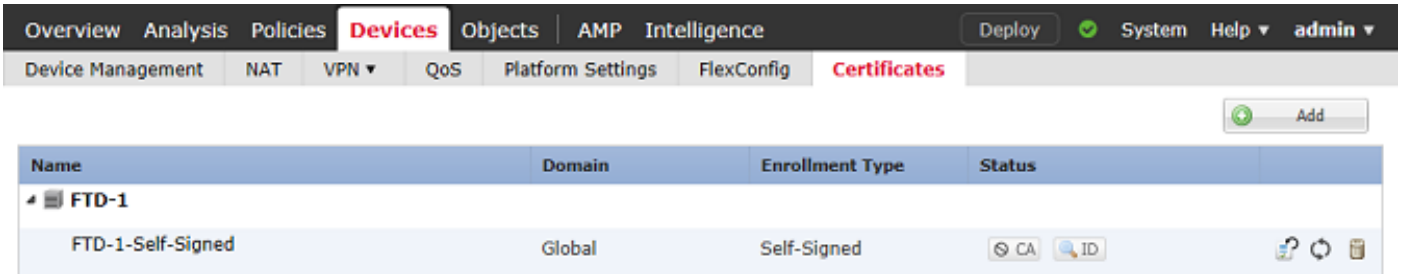
5. (선택 사항) Key(키) 탭에서 인증서에 사용되는 개인 키의 유형, 이름 및 크기를 지정할 수 있습니다. 기본적으로 키는 <Default-RSA-Key> 이름과 2048 크기의 RSA 키를 사용합니다. 그러나 이미지에 표시된 것과 동일한 개인/공용 키 쌍을 사용하지 않도록 각 인증서에 고유한 이름을 사용하는 것이 좋습니다.



6. 완료되면 이미지에 표시된 대로 저장을 클릭한 다음 추가를 클릭합니다.

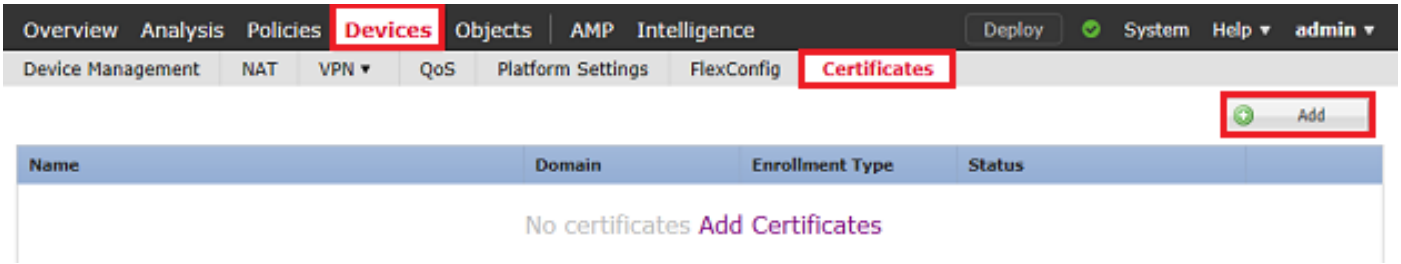


7. 완료되면 자체 서명 인증서가 이미지에 표시됩니다.

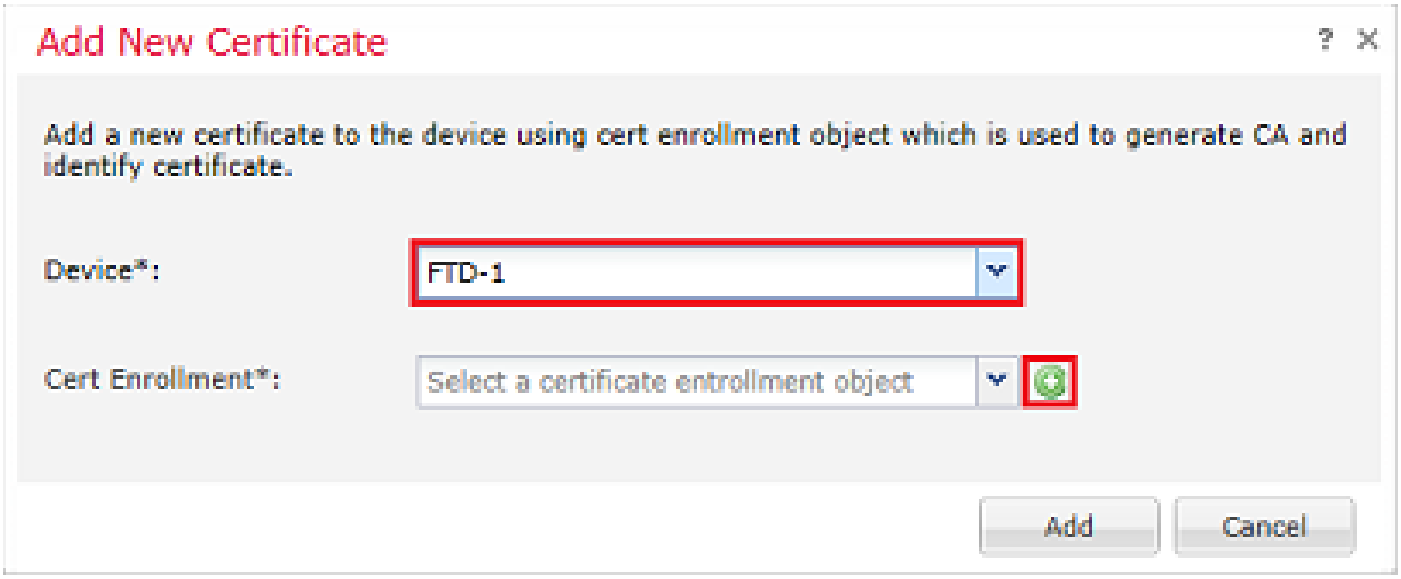


수동 등록

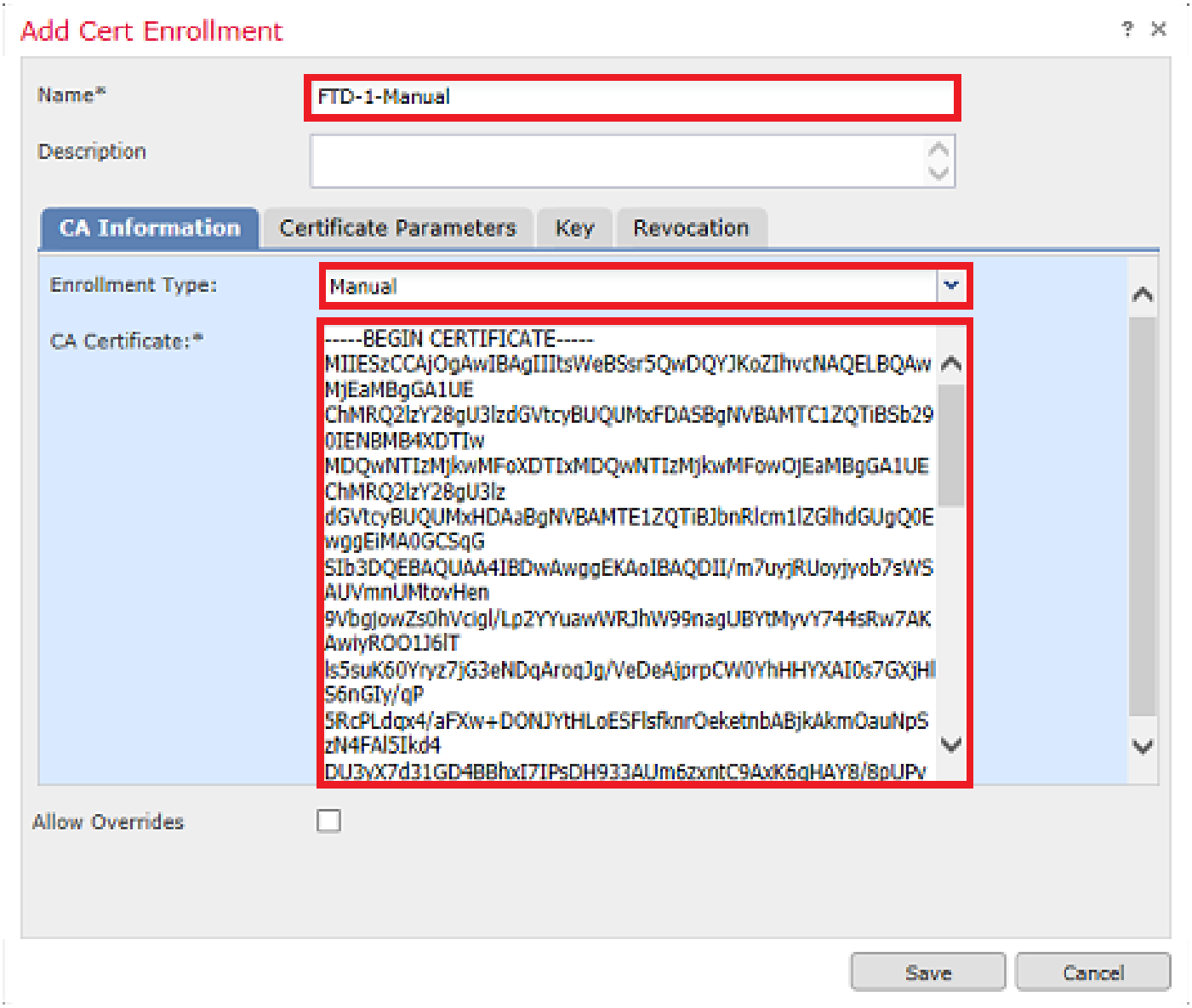
1. 이미지에 표시된 대로 Devices(디바이스) > Certificates(인증서)로 이동한 다음 Add(추가)를 클릭합니다.



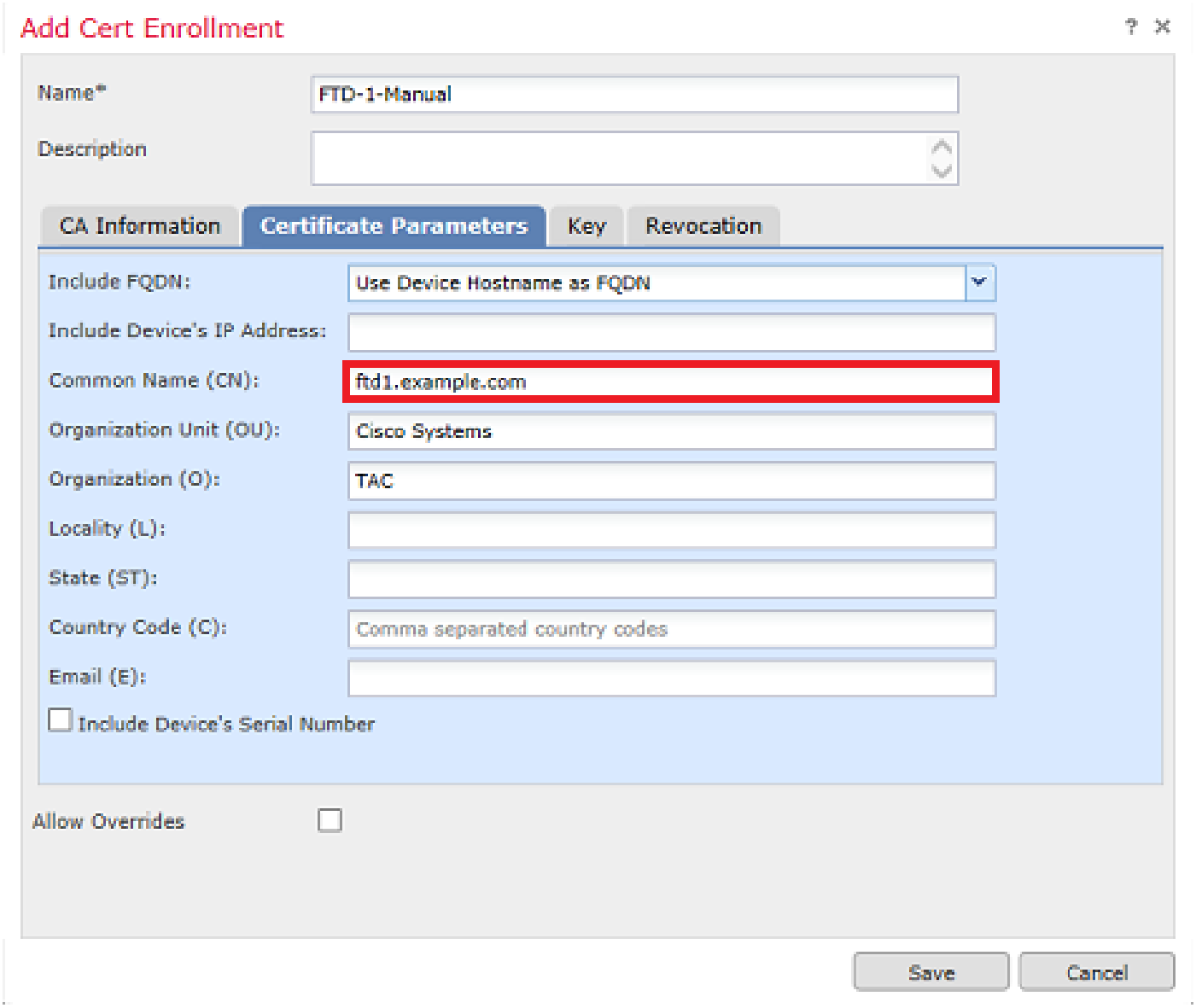
2. Device*(디바이스*) 드롭다운에서 인증서가 추가된 디바이스를 선택한 다음 이미지와 같이 녹색 + 기호를 클릭합니다.



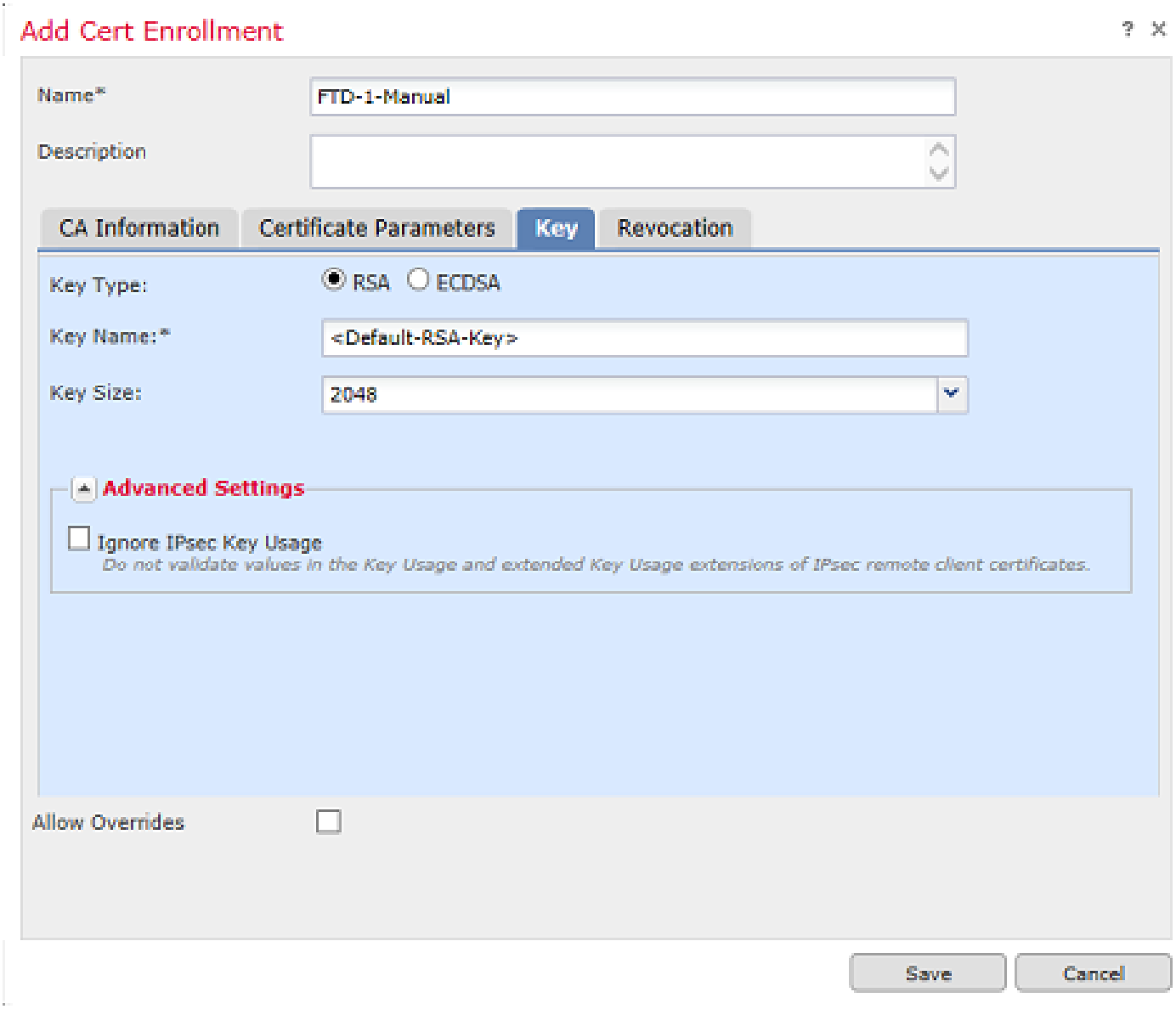
3. 신뢰 지점의 이름을 지정하고 CA Information(CA 정보) 탭에서 Enrollment Type(등록 유형): Manual(수동)을 선택합니다. ID 인증서를 서명하는 데 사용되는 CA의 pem 형식 인증서를 입력합니다. 현재 이 인증서를 사용할 수 없거나 알 수 없는 경우 CA 인증서를 자리 표시자로 추가하고, ID 인증서가 발급되면 이 단계를 반복하여 이미지에 표시된 대로 실제 발급 CA를 추가합니다.



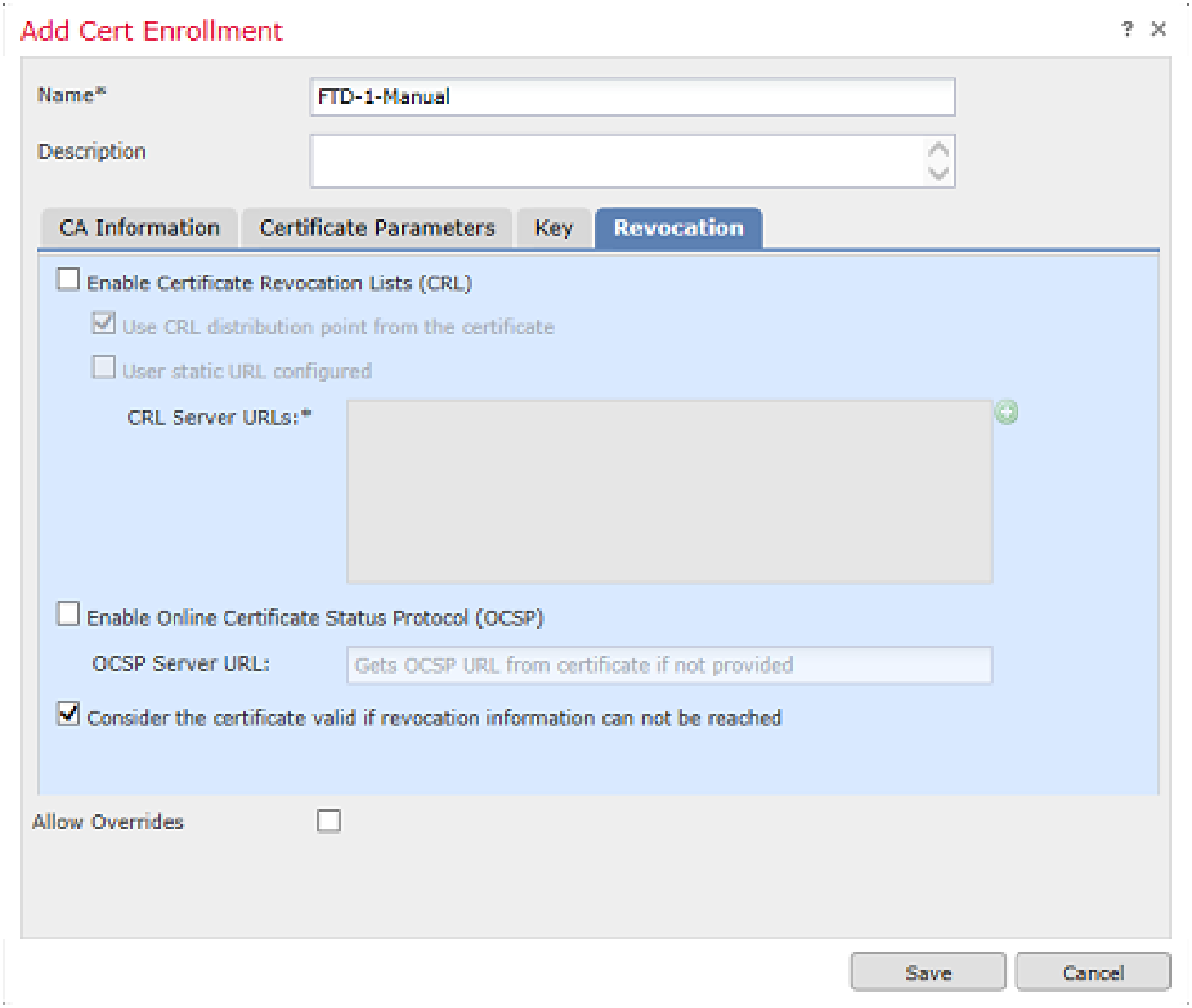
4. Certificate Parameters(인증서 매개변수) 탭 아래에 인증서의 CN을 입력합니다. 이는 이미지에 표시된 대로 인증서가 사용되는 서비스의 fqdn 또는 IP 주소와 일치해야 합니다.



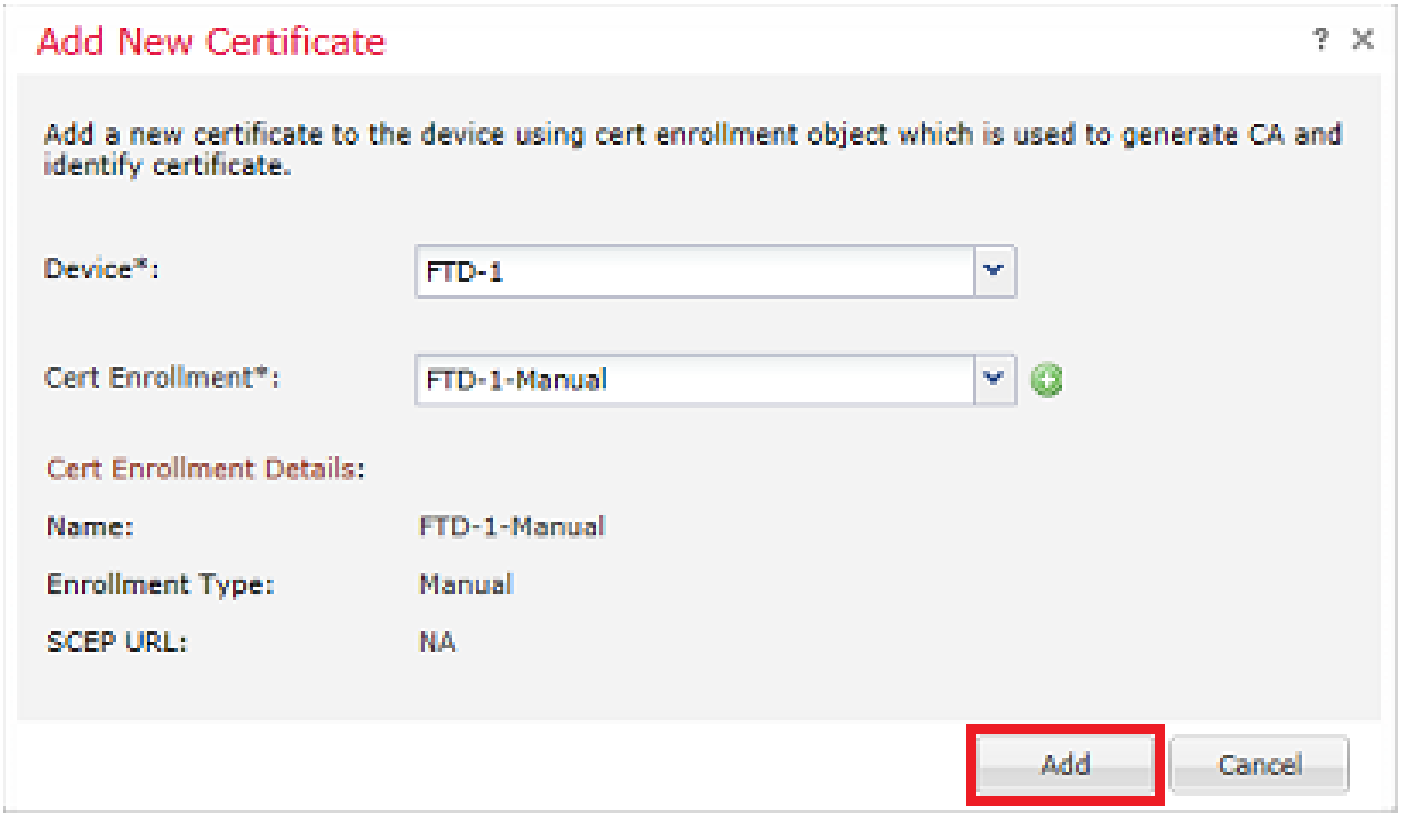
5. (선택 사항) 키 탭 아래에서 인증서에 사용되는 개인 키의 유형, 이름 및 크기를 선택적으로 지정할 수 있습니다. 기본적으로 키는 <Default-RSA-Key> 이름과 2048 크기의 RSA 키를 사용합니다. 그러나 이미지에 표시된 것과 같은 개인/공용 키 쌍을 사용하지 않도록 각 인증서에 고유한 이름을 사용하는 것이 좋습니다.



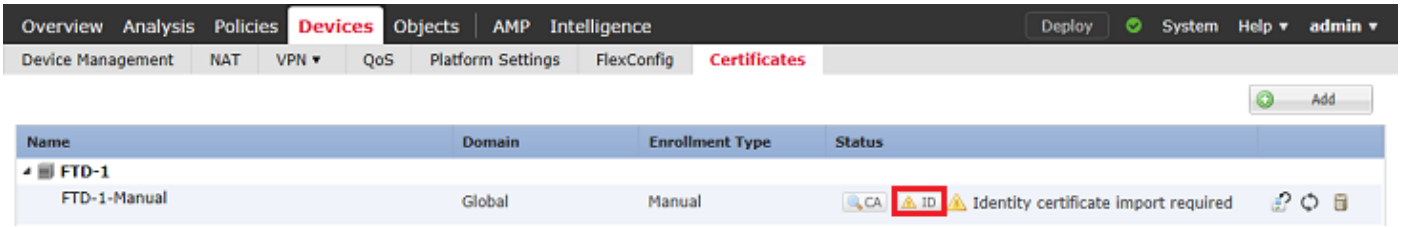
6. (선택 사항) Revocation(해지) 탭에서 CRL(Certificate Revocation List) 또는 OCSP(Online Certificate Status Protocol) 해지를 선택하고 구성할 수 있습니다. 기본적으로 둘 다 이미지에 표시된 대로 선택되지 않습니다.



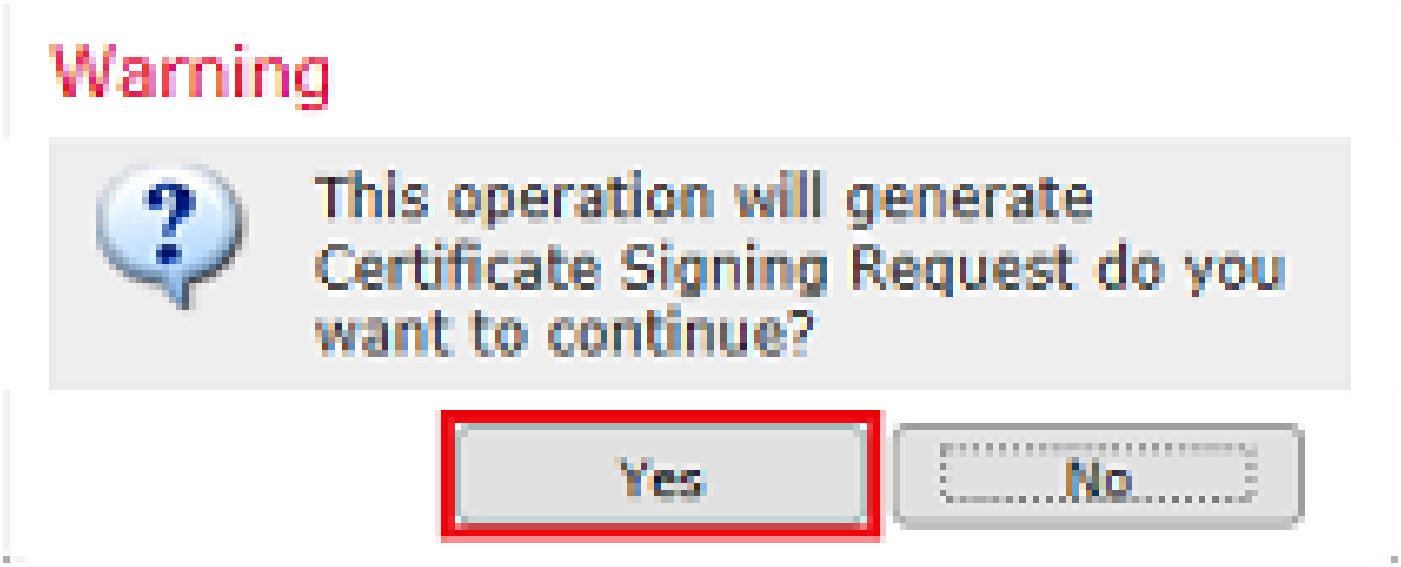
7. 완료되면 그림과 같이 저장을 클릭한 다음 추가를 클릭합니다.



8. 요청을 처리한 후 FMC는 ID 인증서를 추가할 수 있는 옵션을 제공합니다. 이미지에 표시된 대로 ID 버튼을 클릭합니다.

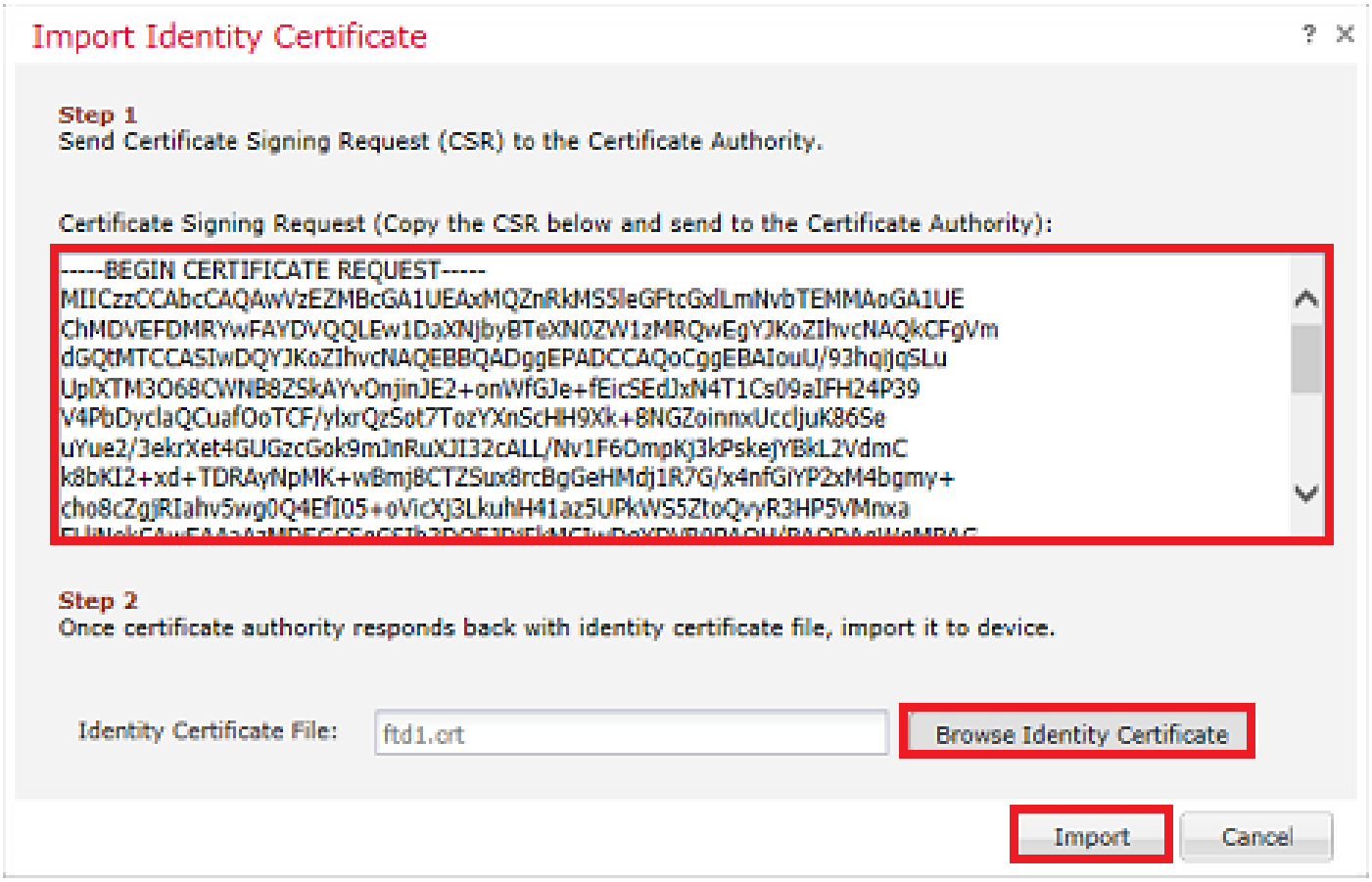


9. CSR이 생성되었음을 알리는 창이 나타납니다. 이미지에 표시된 대로 Yes(예)를 클릭합니다.

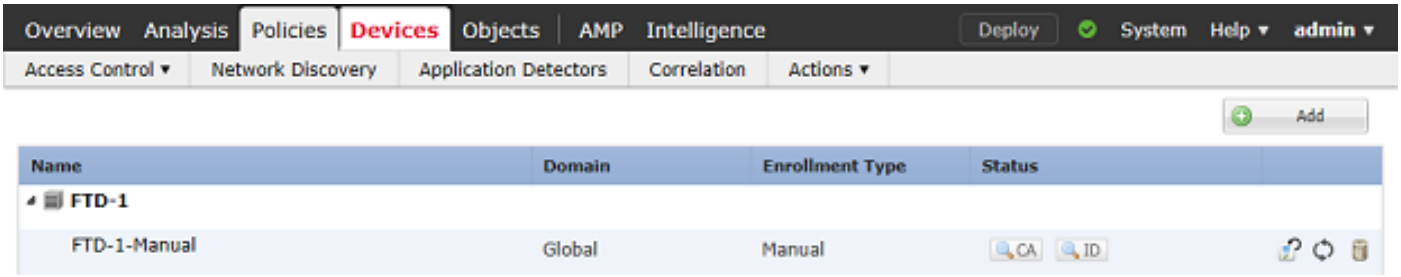


10. 그런 다음 복사하여 CA로 전송할 수 있는 CSR이 생성됩니다. CSR이 서명되면 ID 인증서가 제공됩니다. 제공된 ID 인증서를 찾아 선택한 다음 이미지에 표시된 대로 Import(가져오기)를 클릭합

니다.

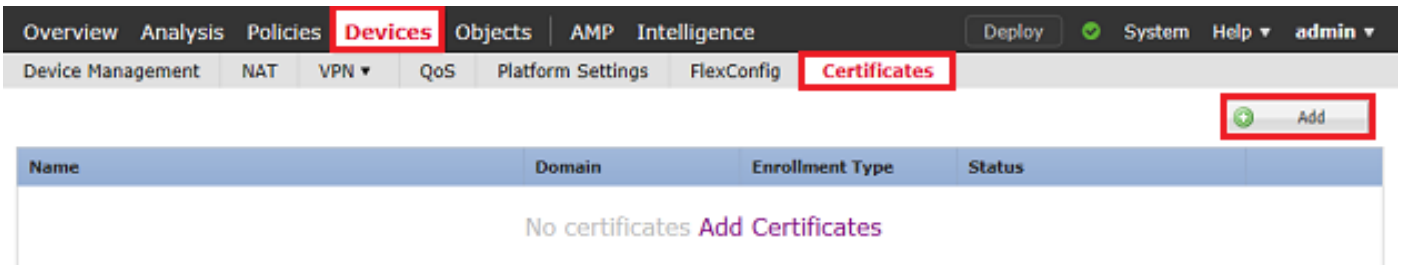


11. 완료되면 그림과 같이 수동 인증서가 표시됩니다.

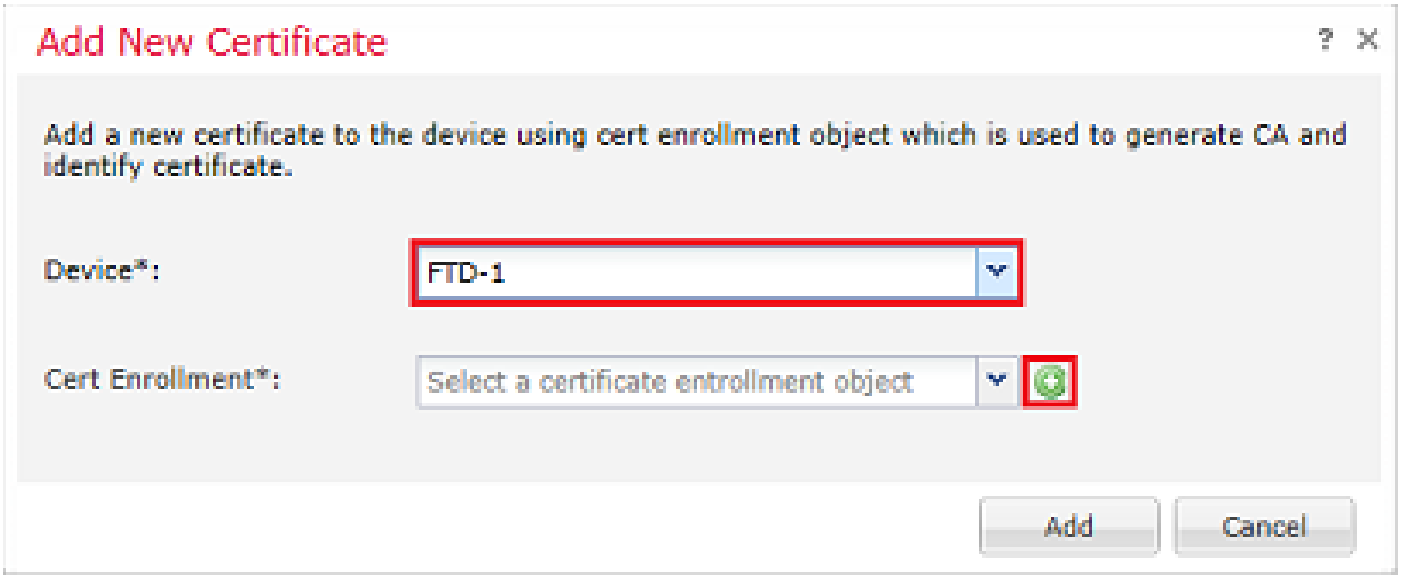


PKCS12 등록

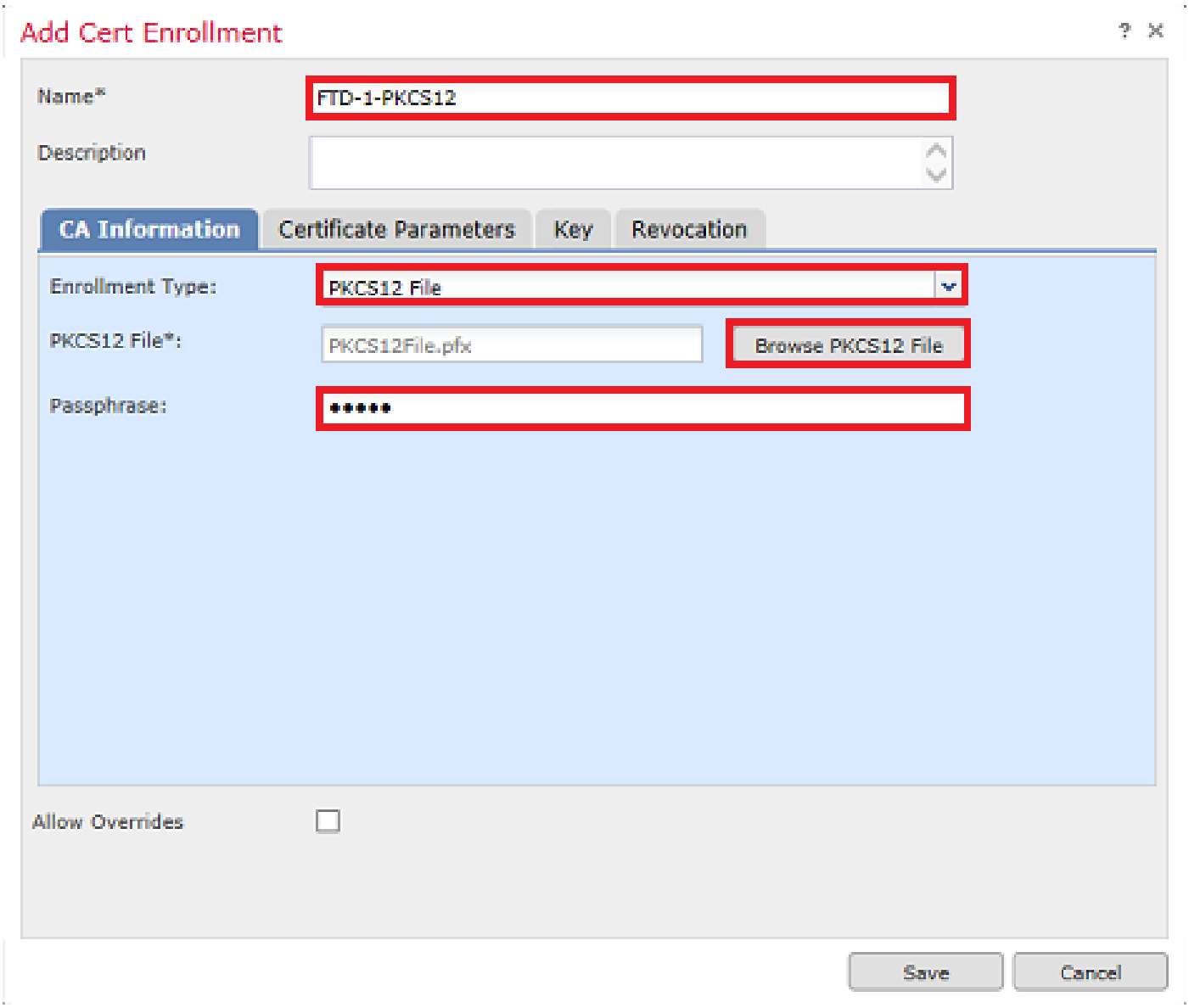
1. 수신되거나 생성된 PKCS12 파일을 설치하려면 이미지에 표시된 대로 Devices(디바이스) > Certificates(인증서)로 이동한 다음 Add(추가)를 클릭합니다.



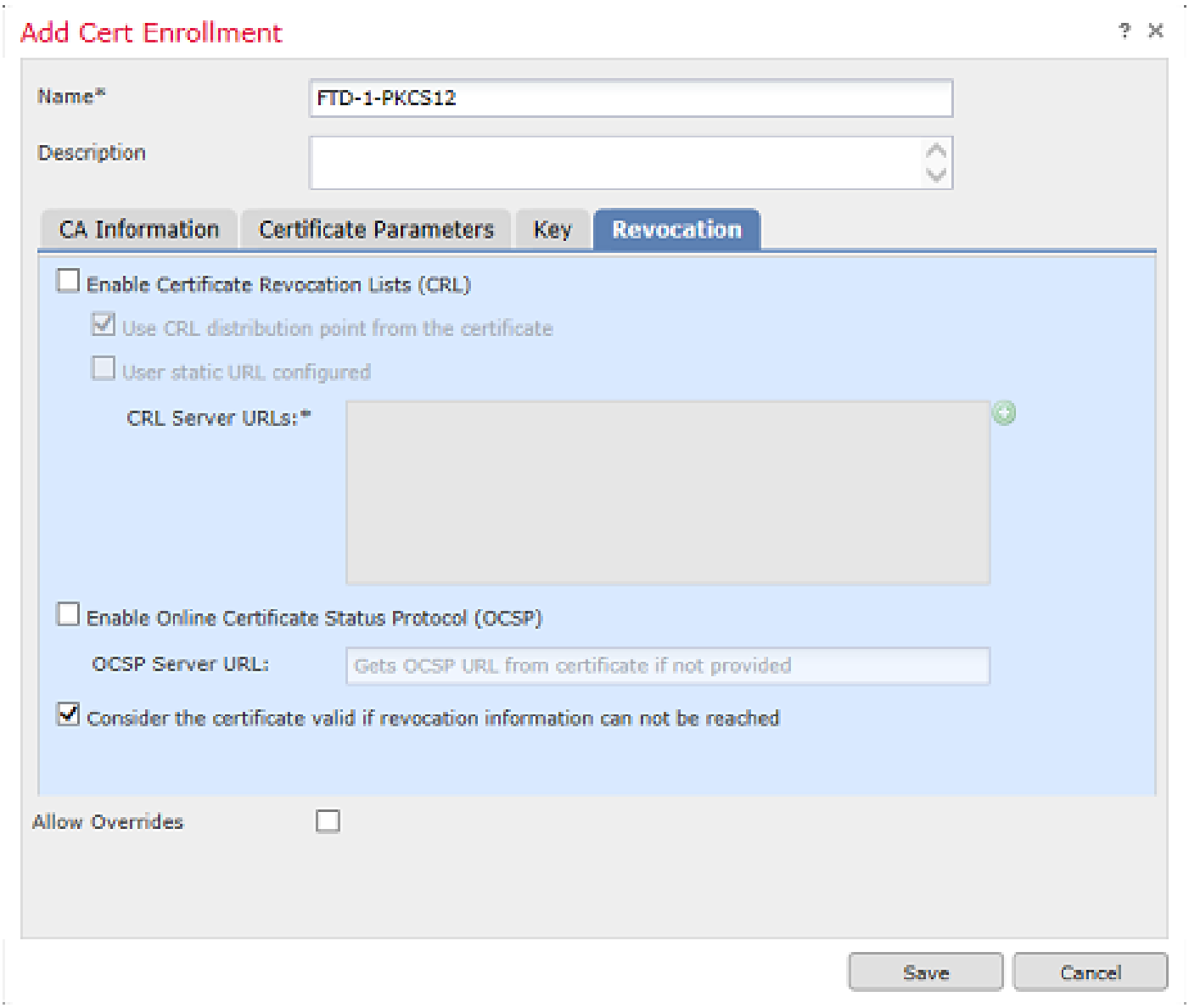
2. Device*(디바이스*) 드롭다운에서 인증서가 추가된 디바이스를 선택한 다음 이미지와 같이 녹색 + 기호를 클릭합니다.



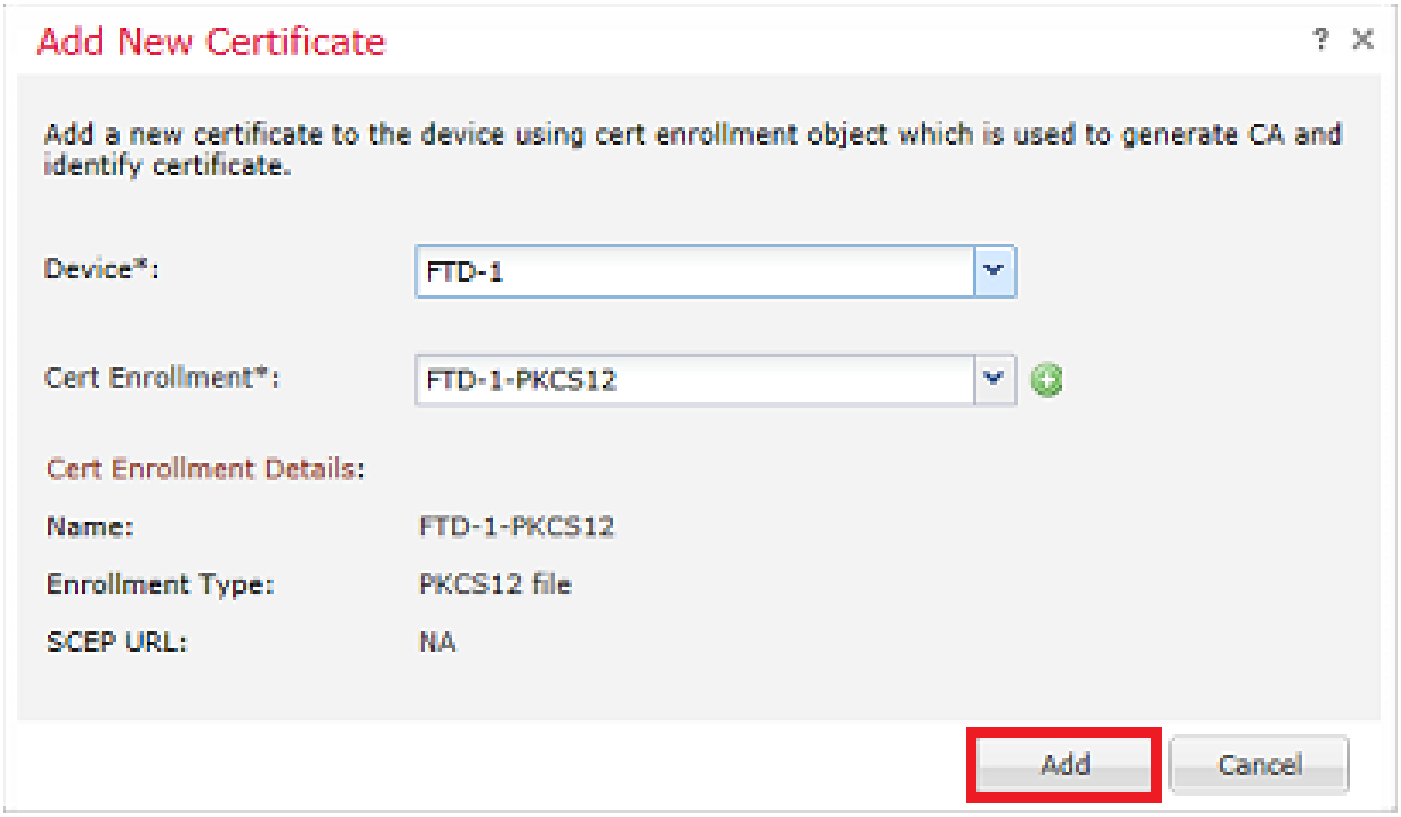
3. 신뢰 지점의 이름을 지정하고 CA Information(CA 정보) 탭에서 Enrollment Type(등록 유형): PKCS12 File(PKCS12 파일)을 선택합니다. 생성된 PKCS12 파일을 찾아 선택합니다. 이미지에 표시된 대로 PKCS12를 생성할 때 사용되는 패스코드를 입력합니다.



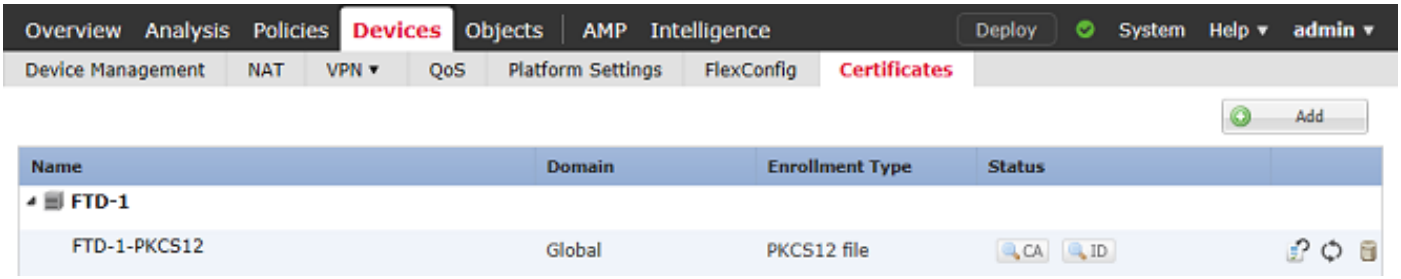
4. (선택 사항) Certificate Parameters(인증서 매개변수) 및 Key(키) 탭은 PKCS12로 이미 생성되었으므로 회색으로 표시되지만, Revocation(해지) 탭은 CRL 및/또는 OCSP 폐기 검사를 활성화하도록 수정할 수 있습니다. 기본적으로 둘 다 이미지에 표시된 대로 선택되지 않습니다.



5. 완료되면 이미지에 표시된 대로 저장을 클릭한 다음 이 창에서 추가를 클릭합니다.



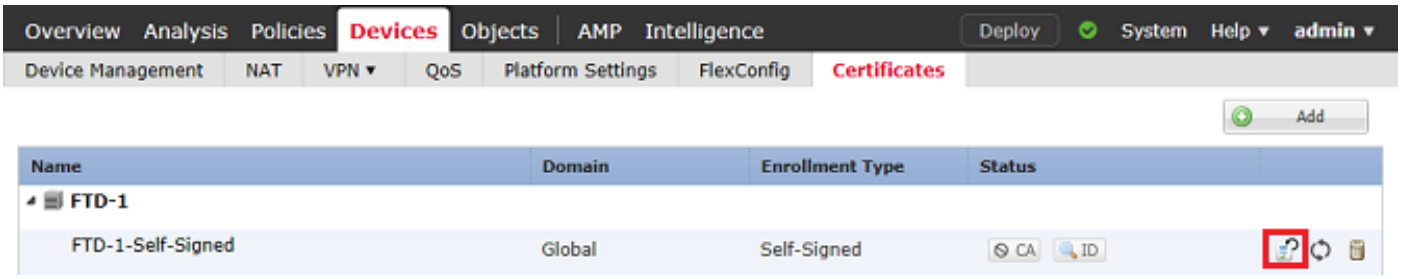
6. 완료되면 PKCS12 인증서가 이미지에 표시된 것처럼 표시됩니다.



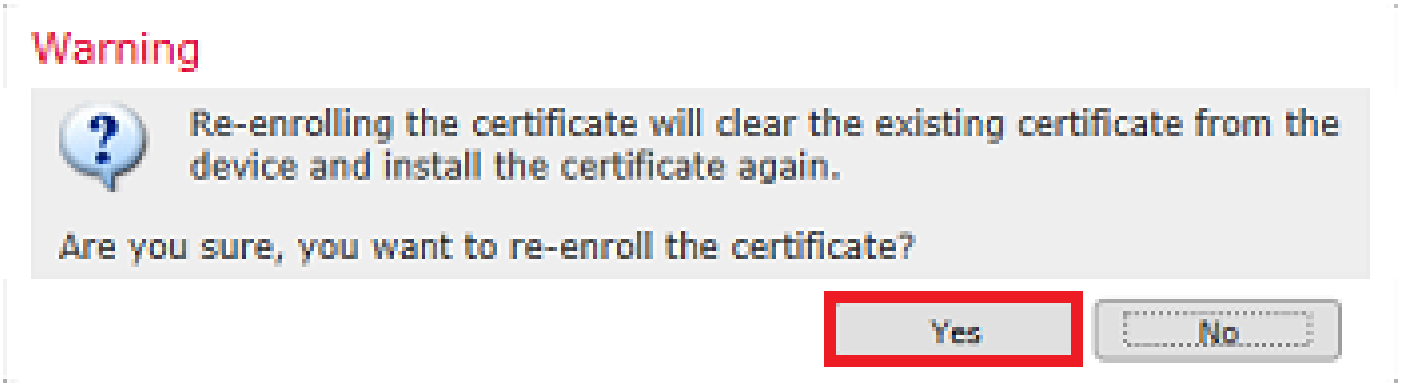
인증서 갱신

자체 서명 인증서 갱신

1. 이미지에 표시된 대로 Re-enroll certificate(인증서 재등록) 버튼을 누릅니다.



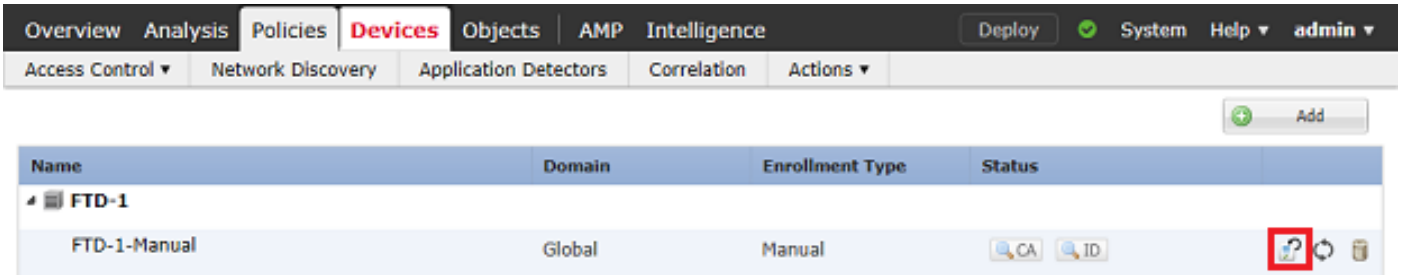
2. 자체 서명 인증서를 제거하고 대체하라는 메시지가 표시됩니다. 이미지에 표시된 대로 Yes(예)를 클릭합니다.



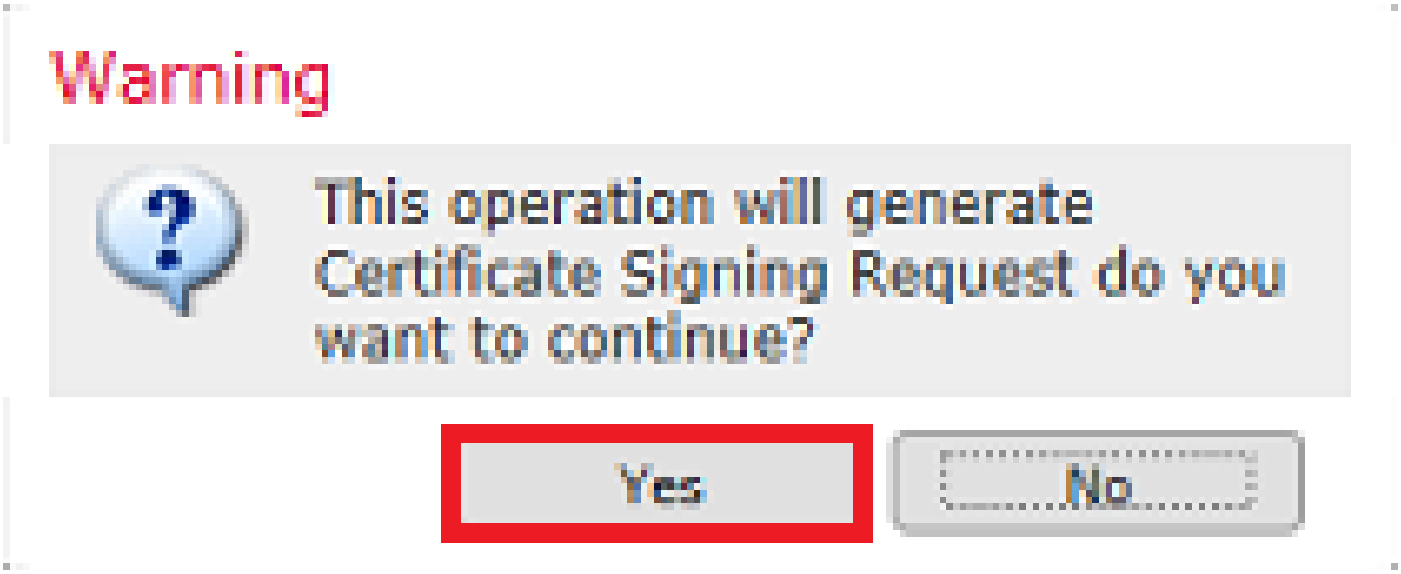
3. 갱신된 자체 서명이 FTD에 푸시됩니다. ID 버튼을 클릭하고 Valid time(유효 시간)을 선택하면 이를 확인할 수 있습니다.

수동 인증서 갱신

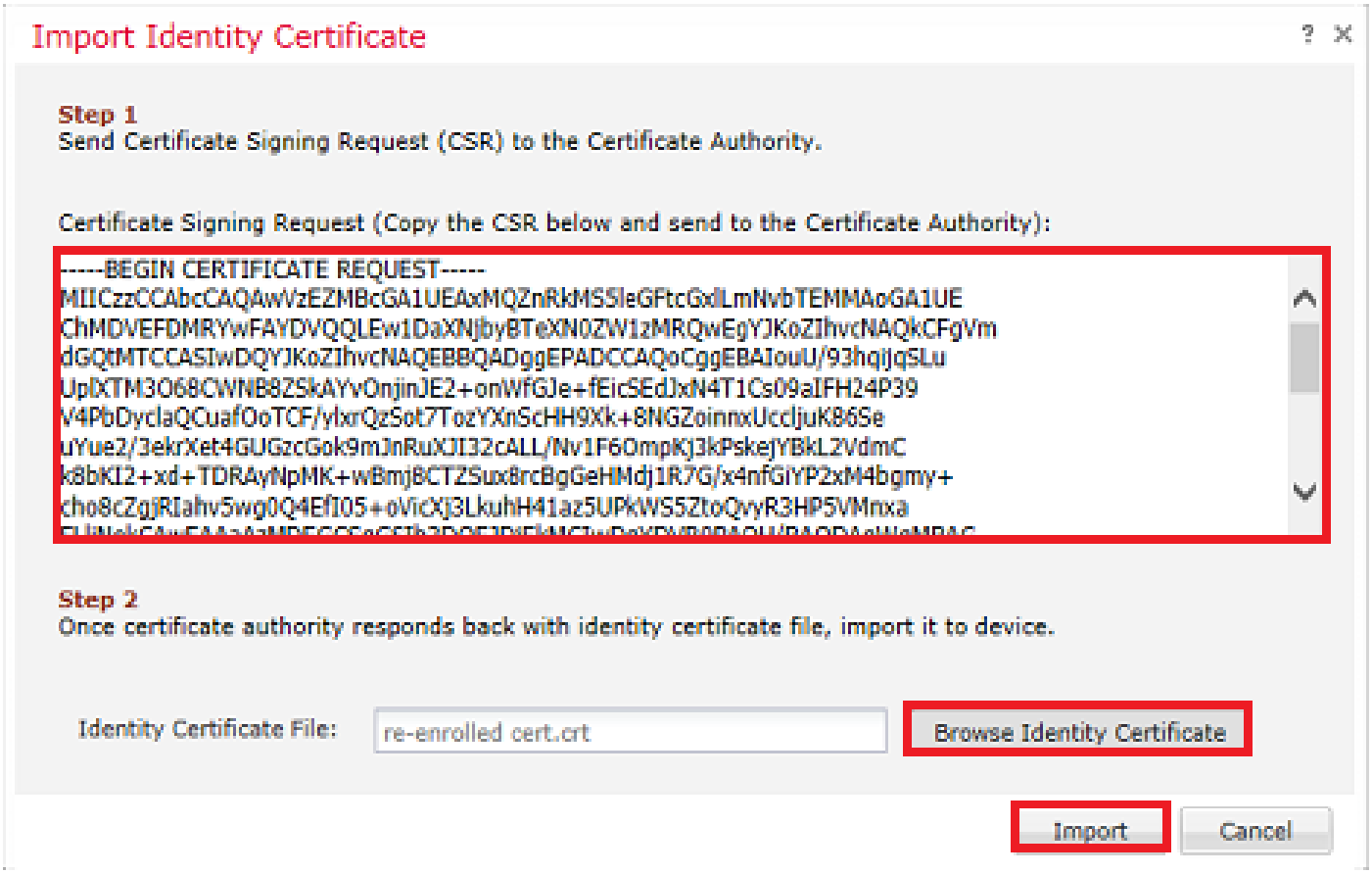
1. 이미지에 표시된 대로 Re-enroll certificate(인증서 재등록) 버튼을 누릅니다.



2. CSR(Certificate Signing Request)이 생성되었다는 메시지가 표시됩니다. 이미지에 표시된 대로 Yes(예)를 클릭합니다.



3. 이 창에서는 ID 인증서를 이전에 서명한 CA에 복사하여 전송할 수 있는 CSR이 생성됩니다. CSR이 서명되면 갱신된 ID 인증서가 제공됩니다. 제공된 ID 인증서를 찾아 선택한 다음 이미지에 표시된 대로 Import(가져오기)를 클릭합니다.



4. 갱신된 수동 인증서가 FTD에 푸시됩니다. ID 버튼을 클릭하고 Valid time(유효 시간)을 선택하면 이를 확인할 수 있습니다.

PKCS12 갱신

Re-enroll certificate(인증서 재등록) 버튼을 클릭하면 인증서가 갱신되지 않습니다. PKCS12를 갱신하려면 앞에서 설명한 방법을 사용하여 새 PKCS12 파일을 만들고 업로드해야 합니다.

OpenSSL을 사용한 PKCS12 생성

1. OpenSSL 또는 이와 유사한 애플리케이션을 사용하여 개인 키 및 CSR(Certificate Signing Request)을 생성합니다. 다음 예에서는 private.key라는 2048비트 RSA 키와 OpenSSL에서 생성된 ftd1.csr이라는 CSR을 보여줍니다.

```
openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out ftd1.csr
Generating a 2048 bit RSA private key
.....................................+++
.....................................................................+++
written to a 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) []:ftd1.example.com
Email Address []:.

Please enter these'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. 일반적으로 CA 인증서도 제공됩니다. PKCS12를 생성하려면 OpenSSL에서 다음 명령 중 하나를 실행합니다.

PKCS12 내에서 발급된 CA 인증서만 포함하려면 다음 명령을 사용합니다.

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -certfile ca.crt
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

- ftd.pfx는 openssl에서 내보낸 pkcs12 파일의 이름(der 형식)입니다.
- ftd.crt는 CA가 pem 형식으로 발급한 서명된 ID 인증서의 이름입니다.
- private.key는 1단계에서 만든 키 쌍입니다.
- ca.crt는 pem 형식의 인증 기관 인증서입니다.

인증서가 루트 CA와 1개 이상의 중간 CA가 있는 체인의 일부인 경우 이 명령을 사용하여 PKCS12에 전체 체인을 추가할 수 있습니다.

```
openssl pkcs12 -export -out ftd.pfx -in ftd.crt -inkey private.key -chain -CAfile cachain.pem
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

- ftd.pfx는 OpenSSL에서 내보낸 pkcs12 파일(der 형식)의 이름입니다.
- ftd.crt는 CA가 pem 형식으로 발급한 서명된 ID 인증서의 이름입니다.
- private.key는 1단계에서 만든 키 쌍입니다.
- cachain.pem은 발급하는 중간 CA로 시작하여 pem 형식의 루트 CA로 끝나는 체인에 CA 인증서가 포함된 파일입니다.

PKCS7 파일(.p7b, .p7c)이 반환되면 이러한 명령을 사용하여 PKCS12를 생성할 수도 있습니다. p7b가 der 형식인 경우 인수에 der를 추가해야 하며, 그렇지 않으면 포함하지 않습니다.

```
openssl pkcs7 -in ftd.p7b -inform der -print_certs -out ftdpem.crt
```

```
openssl pkcs12 -export -in ftdpem.crt -inkey private.key -out ftd.pfx
Enter Export Password: *****
Verifying - Enter Export Password: *****
```

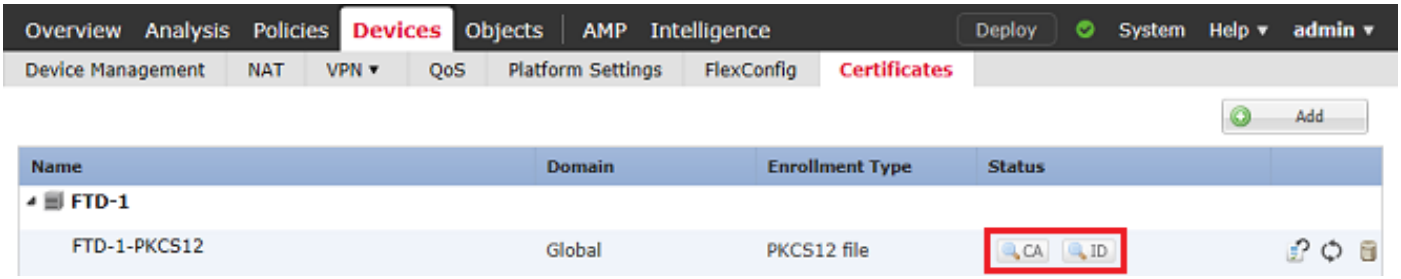
- ftd.p7b는 서명된 ID 인증서 및 CA 체인을 포함하는 CA에서 반환되는 PKCS7입니다.
- ftdpem.crt는 변환된 p7b 파일입니다.
- ftd.pfx는 OpenSSL에서 내보낸 pkcs12 파일(der 형식)의 이름입니다.
- private.key는 1단계에서 만든 키 쌍입니다.

다음을 확인합니다.

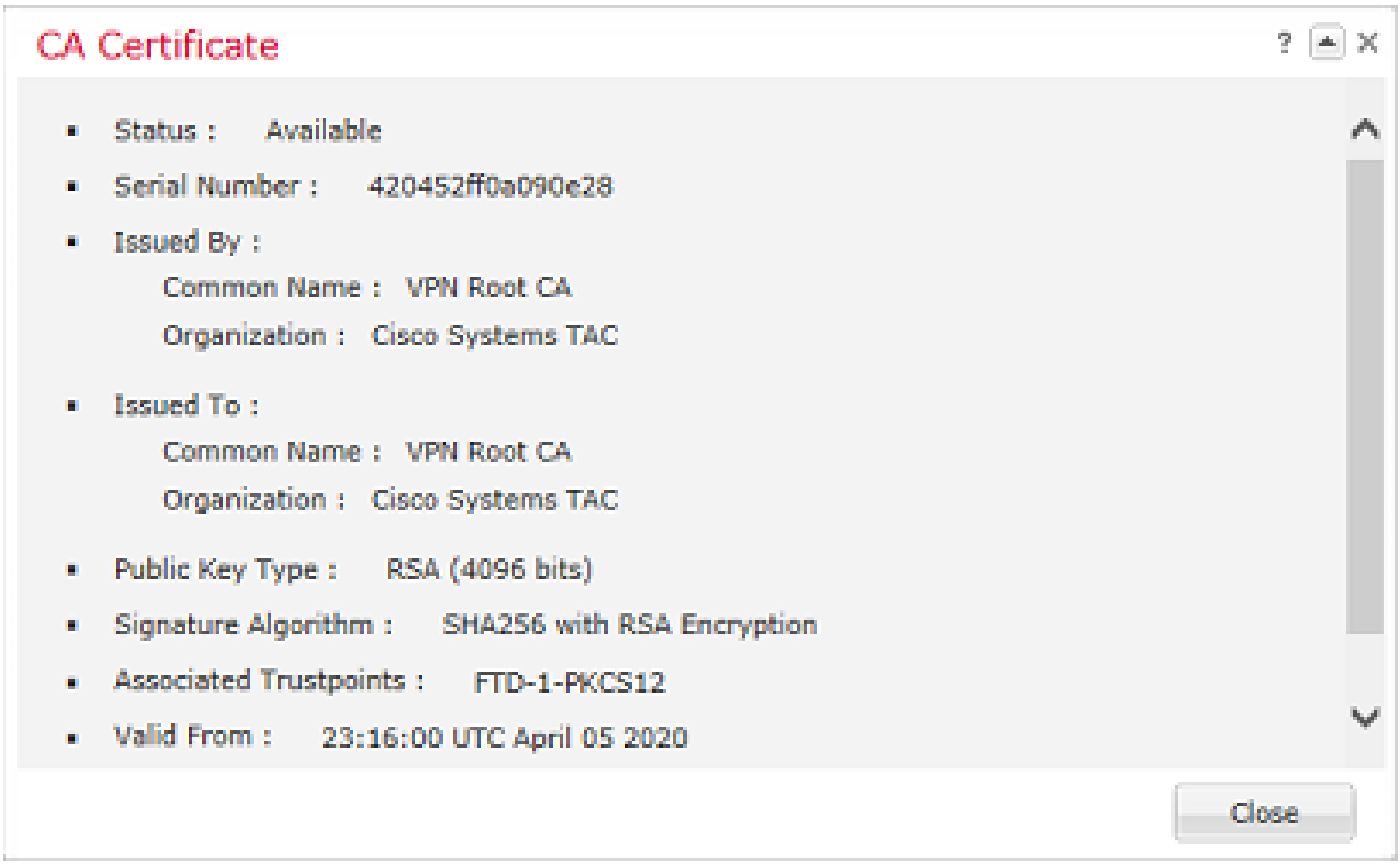
구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

FMC에서 설치된 인증서 보기

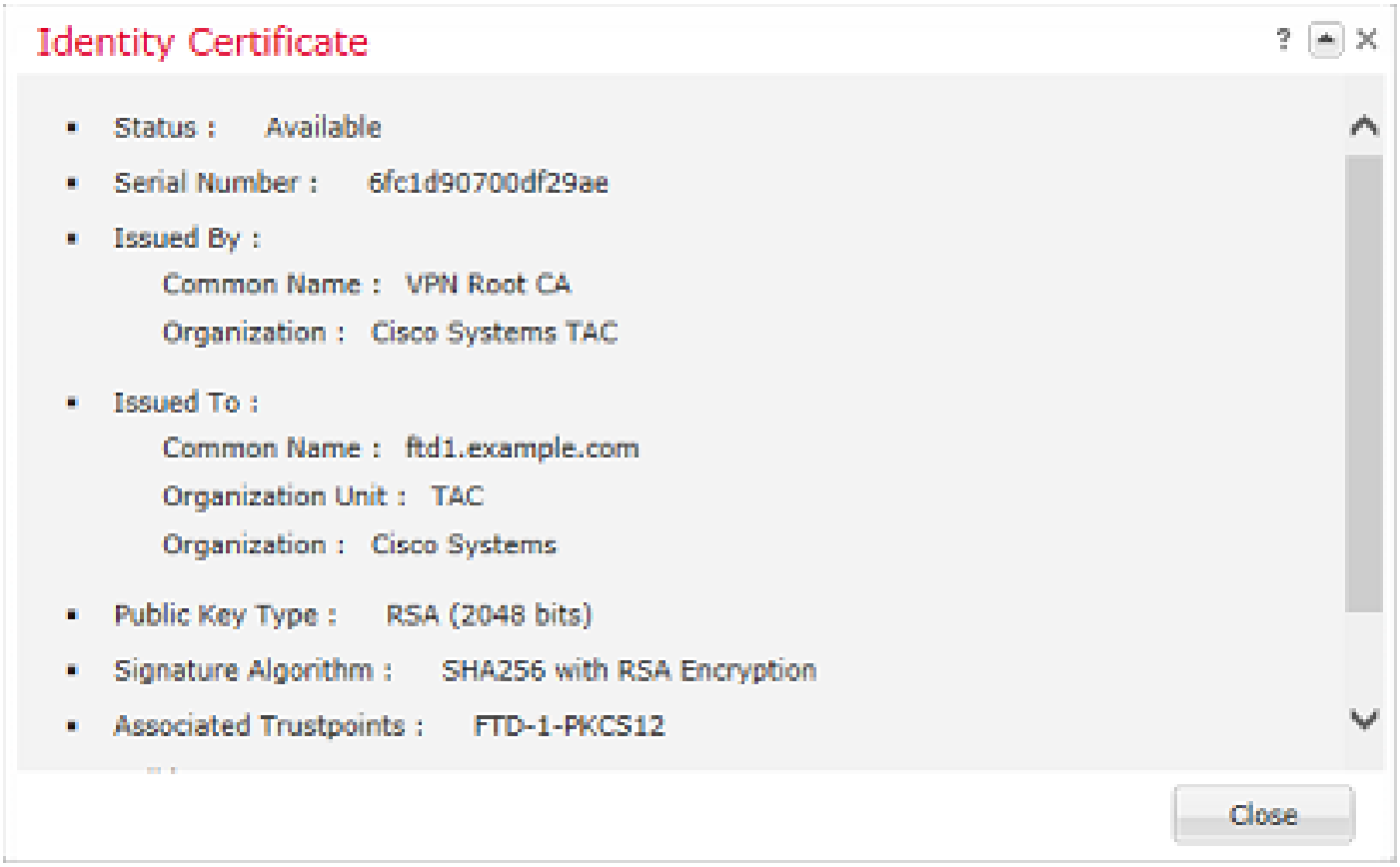
FMC에서 Devices(디바이스) > Certificates(인증서)로 이동합니다. 관련 신뢰 지점의 CA 또는 ID를 클릭하여 이미지에 표시된 것처럼 인증서에 대한 자세한 정보를 봅니다.



이미지에 표시된 대로 CA 인증서를 확인합니다.



이미지에 표시된 대로 ID 인증서를 확인합니다.



CLI에서 설치된 인증서 보기

FTD에 SSH를 입력하고 show crypto ca certificate 명령을 입력합니다.

```
> show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 6fc1d90700df29ae
  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=ftd1.example.com
    ou=TAC
    o=Cisco Systems
  Validity Date:
    start date: 15:47:00 UTC Apr 8 2020
    end   date: 15:47:00 UTC Apr 8 2021
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12

CA Certificate
  Status: Available
  Certificate Serial Number: 420452ff0a090e28
  Certificate Usage: General Purpose
  Public Key Type: RSA (4096 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Subject Name:
    cn=VPN Root CA
    o=Cisco Systems TAC
  Validity Date:
    start date: 23:16:00 UTC Apr 5 2020
    end   date: 23:16:00 UTC Apr 5 2030
  Storage: config
  Associated Trustpoints: FTD-1-PKCS12
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

디버그 명령

SSL 인증서 설치 실패 시 FTD가 SSH를 통해 연결된 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

발급된 ID 인증서를 가져온 후에도 "ID 인증서 가져오기 필요" 메시지가 표시됩니다.

이는 두 가지 문제로 인해 발생할 수 있습니다.

1. 수동 등록 시 발급된 CA 인증서가 추가되지 않았습니다.

ID 인증서를 가져오면 수동 등록 시 CA Information(CA 정보) 탭 아래에 추가된 CA 인증서와 대조됩니다. 네트워크 관리자가 ID 인증서를 서명하는 데 사용되는 CA에 대한 CA 인증서가 없는 경우도 있습니다. 이 경우 수동 등록을 수행할 때 자리 표시자 CA 인증서를 추가해야 합니다. ID 인증서가 발행되고 CA 인증서가 제공되면 올바른 CA 인증서로 새 수동 등록을 수행할 수 있습니다. 수동 등록 마법사를 다시 진행할 때 원래 수동 등록에서 수행한 것과 동일한 키 쌍의 이름과 크기를 지정해야 합니다. 완료되면 CA에 다시 전달된 CSR 대신 이전에 발급된 ID 인증서를 올바른 CA 인증서로 새로 생성된 신뢰 지점으로 가져올 수 있습니다.

동일한 CA 인증서가 수동 등록 시 적용되었는지 확인하려면 Verify 섹션에 지정된 CA 버튼을 클릭하거나 show crypto ca certificates의 출력을 확인합니다. Issued to(발급 대상) 및 Serial Number(일련 번호)와 같은 필드는 인증 기관에서 제공하는 CA 인증서의 필드와 비교할 수 있습니다.

2. 생성된 신뢰 지점의 키 쌍이 발급된 인증서에 대해 CSR을 생성할 때 사용되는 키 쌍과 다릅니다.

수동 등록을 사용하면 키 쌍 및 CSR이 생성될 때 공개 키가 CSR에 추가되어 발급된 ID 인증서에 포함될 수 있습니다. 어떤 이유로 FTD의 키 쌍이 수정되거나 발급된 ID 인증서에 다른 공개 키가 포함된 경우, FTD는 발급된 ID 인증서를 설치하지 않습니다. 이 문제가 발생했는지 확인하려면 두 가지 테스트가 있습니다.

OpenSSL에서는 CSR의 공개 키와 발급된 인증서의 공개 키를 비교하기 위해 다음 명령을 실행할 수 있습니다.

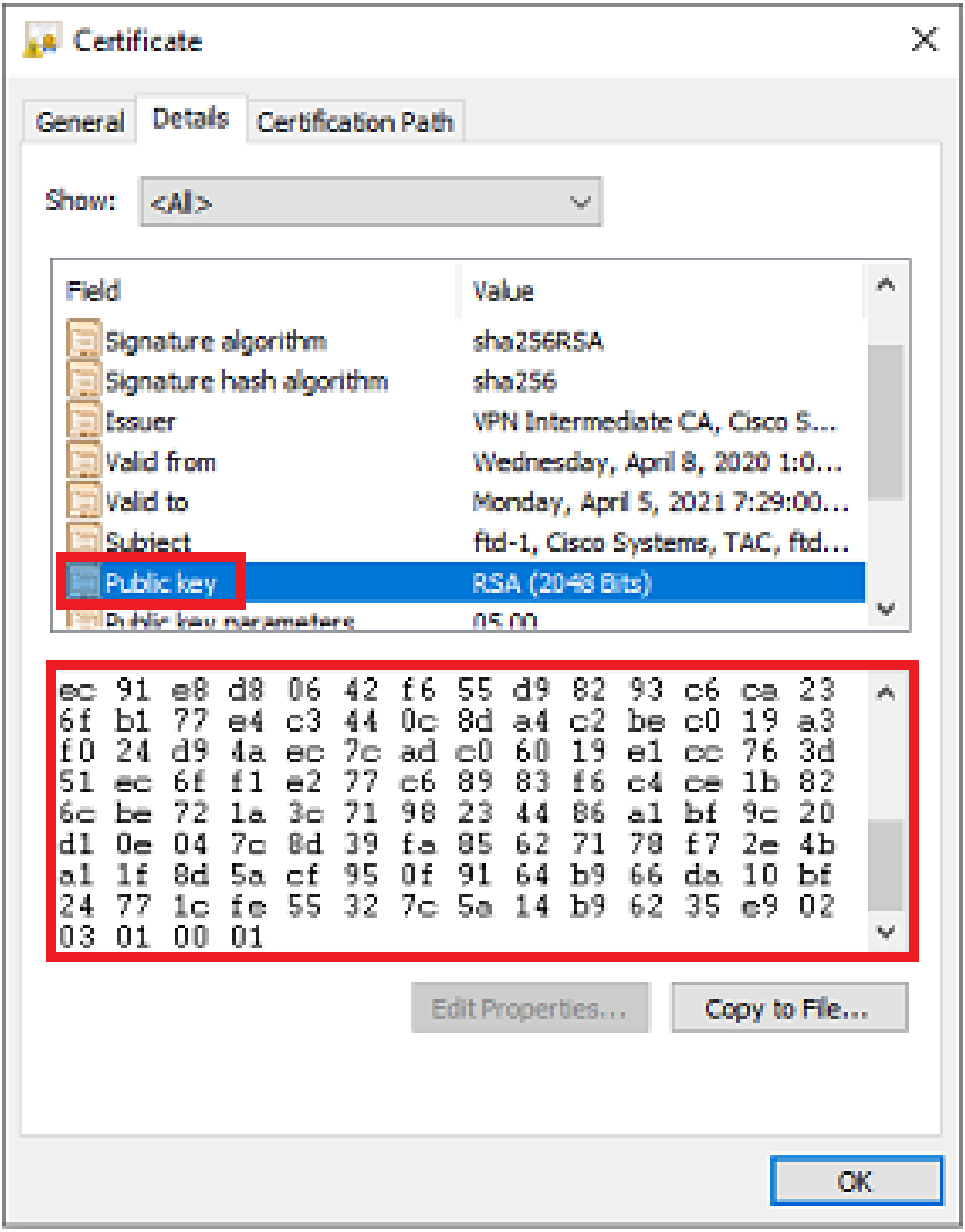
```
openssl req -noout -modulus -in ftd.csr
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9

openssl x509 -noout -modulus -in id.crt
Modulus=8A2E53FF7786A8A3A922EE5299574CCDCEEBC096341F194A4018BCE9E38A7244DBEA2759F1897BE7C489C484749C4DE
0FDFD5783DB0F27256900AE69F3A84C217FCA5C6B4334A8B7B4E8CD85E749C1C7F5793EF0D199A229E7C5471C963B8AF3A49EB9
81941B3706A24F6626746E5C9237D9C00B2FF36FD45E8E9A92A3DE43EC91E8D80642F655D98293C6CA236FB177E4C3440C8DA4C
C7CADC06019E1CC763D51EC6FF1E277C68983F6C4CE1B826CBE721A3C7198234486A1BF9C20D10E047C8D39FA85627178F72E4B
B966DA10BF24771CFE55327C5A14B96235E9
```

- ftd.csr은 수동 등록 시 FMC에서 복사한 CSR입니다.
- id.crt는 CA에서 서명한 ID 인증서입니다.

또는 FTD의 공개 키 값을 발급된 ID 인증서 내의 공개 키와 비교할 수도 있습니다. 패딩으로 인해 인증서의 첫 문자가 FTD 출력의 첫 문자와 일치하지 않습니다.

Windows PC에서 열린 발급된 ID 인증서:



ID 인증서에서 추출된 공개 키 출력:

```
3082010a02820101008a2e53ff7786a8a3a922ee5299574ccdceebc096341f194a4018bce9e38a7244dbea2759f1897be7c489c
```

```
f6e0fdfd5783db0f27256900ae69f3a84c217fca5c6b4334a8b7b4e8cd85e749c1c7f5793ef0d199a229e7c5471c963b8af3a49
1b3706a24f6626746e5c9237d9c00b2ff36fd45e8e9a92a3de43ec91e8d80642f655d98293c6ca236fb177e4c3440c8da4c2bec
e1cc763d51ec6ff1e277c68983f6c4ce1b826cbe721a3c7198234486a1bf9c20d10e047c8d39fa85627178f72e4ba11f8d5acf9
55327c5a14b96235e90203010001
```

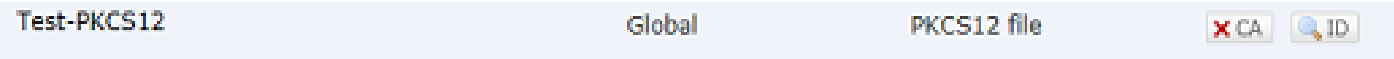
FTD의 암호화 키 mypubkey rsa 출력을 표시합니다. 수동 등록이 완료되면 <Default-RSA-Key>를 사용하여 CSR을 생성했습니다. 굵게 표시된 섹션은 ID 인증서에서 추출된 공개 키 출력과 일치합니다.

```
> show crypto key mypubkey rsa
Key pair was generated at: 16:58:44 UTC Jan 25 2019
 Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
  008a2e53 ff7786a8 a3a922ee 5299574c cdceebc0 96341f19 4a4018bc e9e38a72
  44dbea27 59f1897b e7c489c4 84749c4d e13d42b3 4f5a2051 f6e0fdfd 5783db0f
  27256900 ae69f3a8 4c217fca 5c6b4334 a8b7b4e8 cd85e749 c1c7f579 3ef0d199
  a229e7c5 471c963b 8af3a49e b98b9edb fdde92b5 deb78194 1b3706a2 4f662674
  6e5c9237 d9c00b2f f36fd45e 8e9a92a3 de43ec91 e8d80642 f655d982 93c6ca23
  6fb177e4 c3440c8d a4c2bec0 19a3f024 d94aec7c adc06019 e1cc763d 51ec6ff1
  e277c689 83f6c4ce 1b826cbe 721a3c71 98234486 a1bf9c20 d10e047c 8d39fa85
  627178f7 2e4ba11f 8d5acf95 0f9164b9 66da10bf 24771cfe 55327c5a 14b96235
  e9020301 0001
```

FMC에서 CA 옆에 빨간색 X 표시

이는 CA 인증서가 PKCS12 패키지에 포함되어 있지 않기 때문에 PKCS12 등록 시 발생할 수 있습니다.



이를 해결하려면 PKCS12에 CA 인증서가 추가되어야 합니다.

ID 인증서 및 개인 키를 추출하기 위해 이러한 명령을 실행합니다. PKCS12 및 보안 개인 키 생성 시 사용되는 비밀번호가 필요합니다.

```
openssl pkcs12 -info -in test.p12
Enter Import Password: [pkcs12 pass phrase here]
MAC Iteration 1
MAC verified OK
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
subject=/CN=ftd1.example.com
```

```
issuer=/O=Cisco Systems TAC/CN=VPN Intermediate CA
-----BEGIN CERTIFICATE-----
MIIC+TCCAeGgAwIBAgIIAUIM3+3IMhIwDQYJKoZIhvcNAQELBQAwOjEaMBgGA1UE
ChMRQ2lzY28gU3lzdGVtcyBUQUMxHDAaBgNVBAMTE1ZQTiBJbnRlcm1lZGlhdGUg
Q0EwHhcNMjAwNDA4MTY1ODAwWhcNMjEwNDA1MjMyOTAwWjAbMRkwFwYDVQQDExBm
dGQxLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
043eLVPl8K0jnYfHCBZuFUYrXTTB28Z1ouIJ5yyrDzCN781GFrHb/wCczRx/jW4n
pF9q2z7FHr5bQCI4oSUSX4OUQfr0/u0K5riI1uZumPUx1Vp1zVkYuqDd/i1r0+0j
PyS7BmyGfV7aebYWZnr8R9ebDsnC2U3nKjP5RaE/wNdVGTS/18OHlrIjMpcFMXps
LwxdxiEz0hCMnDm9RC+7uWZQdlwZ9oNANCbQC0px/Zikj9Dz7ORhhbzBTeUNKD3p
sN3VqdDPvGZHFGlPCnhKYyZ79+6p+CHC8X8BFjuTJYoo1l6uGgiB4Jz2Y9ZeFSQz
Q11IH3v+xKMJnv6IkZLuvwIDAQABoyIwIDAeBglghkgBhvhCAQ0EERYPeGNhIGNl
cnRpZmljYXRlMA0GCSqGSIb3DQEBCwUAA4IBAQCV/MgshWxXtwpwmMF/6KqEj8nB
Sljbfzl zNuPV/LLMSnxMLDo6+LB8tizNR+ao9dGATRyY54taRI27W+gLneCbQAux
9amxXuhpxP5EOhnk+tsYS9eriAKpHuS1Y/2uwN92fHIbh3HEXPO1HBJueI8PH3ZK
4lrPKA9oIQPUW/uueHEF+xCbG4xCLi5HOGeHX+FTigGNqazaX5GM4RBUa4bk8jks
Ig53twvop71wE53COTH0EkSRCsVCw5mdJsd9BUZHjguhpw8Giv7Z36qWv18I/Owf
RhLhtsgenc25udglvv9Sy5xK53a5Ieg8biRpWL9tIjgUgjxYZwtyVeHi32S7
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    friendlyName: Test
    localKeyID: 76 8F D1 75 F0 69 FA E6 2F CF D3 A6 83 48 01 C4 63 F4 9B F2
Key Attributes: <No Attributes>
Enter PEM pass phrase: [private-key pass phrase here]
Verifying - Enter PEM pass phrase: [private-key pass phrase here]
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIlKyWXk8cgTMCAggA
MBQGCCqGSIb3DQMHBAgGmOqRXh/dcwSCBMiF7BpgJNIpHdU5Zorn1jm3pmsI/XkJ
MRHc1Reel0ziSLCZ0STr84JFQxNpbThXLhsHC9WhpPy5sNXIvXS7Gu+U10/VlNSA
rWlX6SPftAYiFq5QXyEutSHdZZwgQIqpj97seu3Px0agvIObW1Lo8or5lSydnMjp
Ptv5OKo95BShWWYcqkTAia4ZKxytyIc/mIu5m72LucOFmoRBO5JZu1avWXjbCAA+
k2ebkblFT0YRQT1Z4tZHSqX1LFPZe17ONZEUg7rIcWAk1Yw7XNUPhOn6FHL/ieIZ
IhvIfj+1gQKeovHkSKuwzb24Zx0exkhafPsgp0PMAPxBnQ/Cxh7Dq2dh1FD8P15E
Gnh8r3l9O3AlkPMBkMdxOqlpzo2naIy2KGrUnOSHajVWcLr9dTPWIDyjdn95YoeS
IUE7MaOOpjJcO2FNBwyNxRrYt+4hp3aJt0ZW83FHiSlB5UIzGrBMAgKJc2Hb2RTV
9gxZGve1cRcolLeJRYoK9+PeZ7t17xzLSg5wad4R/ZPKUwTBUaShn0wHzridF8Zn
FO6XvBDSyuXVSpkxwAdlTwxq62tUnLIkyRXo2CSz8z8W29UXmFO4o3G67n28//LJ
Ku8wj1jeqlvFgXSQiWLADNhIY772RNwzCMeobfxGlBprF9DPT8yvyBdQviUIuFpJ
nNs5FYbLTv9ygZ1S9xwQpTcqEu+y4F5BJuYLmHqcZ+VpFA4nMOYHhZ5M3sceRSR4
1L+a3BPJJshlTIJQg0TIxDaveCfpDcpS+ydUgS6YWY8xW17vO+1f7y5zlt4TkZRt
ItBHHA6yDzR0Cn0/ZH3y88a/asDcukw6bsRaY5iT8nAWgTQVed3xXj+EgeRs25HB
dIBBX5gTvqN7qDanhkaPUcEawj1/38MOpAYULei3elfKKrhwAySBFaV/BeUMWuNW
BmKprkKKQv/JdWnoJl49KcS4bfa3GHG9XXnyvbg8HxopcYFMTEjao+wLZH9agqKe
YOjyoHFN6ccBBC7vn7u12tmXOM5RcnPLmaDaBFDSBBFS8Y8VkeHn3P0q7+sEQ26d
vL8O7WdgLH/wKqovoJRyxwzz+TryRq9cd5BNyyLaABESalsWRhk81C2P+B+Jdg9w
d6RsvJ2dt3pdl/+pUR3CdC0b8qRZOoLO3+onUIUoEsCCNdp0x8Yj/mvc6ReXtOKB
2qVmhVMYseiUlrOAQGt7XMe1UuiJ+dRnqcfAfbdGeOp+6epm1TK1BJL2mAlQWx5l
73Qo4M7rR7laeq/dqob3olPhcoMLa5z/Lo5vDe7S+LZMuAWjRkSfsoOKQOY3kAP1
eZ2Eh2go4eJ7hHf5VFqBLL8Ci3rd3EOijRkNm3fAQmFJlaFmooBM3Y2Ba+U8cMTH
lgjSFkl1FAWpfwx9aSEECNCvEMm1Ghm6/tJDLV1jyTqwajHnWIZCc+P2AXgnlLzG
HVVfxsOc8FGUJPQHatXYd7worWCxszauhfJ99E4PaoZnAOYUFw2jaZEwoONBPbD1
AjQ8aciuosv0FKpp/jXDI78/aYAEk662tPsfGmxvAWB+UMFarA9ZTiihK3x/tDPy
GZ6ByGWJYp/0tNNmJRCFhcAYY83EtzHK9h+8LatFA6WrJ4j3dhceUPzrPXjMffNN
0Yg=
-----END ENCRYPTED PRIVATE KEY-----
```

완료되면 ID 인증서와 개인 키를 별도의 파일에 넣고 CA 인증서를 새 PKCS12 파일로 가져올 수 있

습니다. OpenSSL로 PKCS12 생성의 2단계에서 설명한 단계를 사용합니다.

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.