

# ASDM에서 관리하는 ASA에 인증서 설치 및 갱신

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[ASDM을 사용하여 새 ID 인증서 요청 및 설치](#)

[CSR\(Certificate Signing Request\)을 사용하여 새 ID 인증서 요청 및 설치](#)

[ASDM으로 CSR 생성](#)

[특정 이름으로 신뢰 지점 만들기](#)

[\(선택 사항\) 새 키 쌍 생성](#)

[키 쌍 이름 선택](#)

[인증서 주체 및 FQDN\(정규화된 도메인 이름\)을 구성합니다](#)

[CSR 생성 및 저장](#)

[ASDM을 사용하여 PEM 형식의 ID 인증서 설치](#)

[CSR에 서명한 CA 인증서 설치](#)

[ID 인증서 설치](#)

[새 인증서를 ASDM을 통해 인터페이스에 바인딩](#)

[ASDM을 사용하여 PKCS12 형식으로 받은 ID 인증서 설치](#)

[PKCS12 파일에서 ID 및 CA 인증서 설치](#)

[새 인증서를 ASDM을 통해 인터페이스에 바인딩](#)

[인증서 갱신](#)

[ASDM을 사용하여 CSR\(Certificate Signing Request\)로 등록된 인증서 갱신](#)

[ASDM을 사용하여 CSR 생성](#)

[특정 이름으로 새 신뢰 지점을 만듭니다.](#)

[\(선택 사항\) 새 키 쌍 생성](#)

[키 쌍 이름 선택](#)

[인증서 주체 및 FQDN\(정규화된 도메인 이름\)을 구성합니다](#)

[CSR 생성 및 저장](#)

[ASDM을 사용하여 PEM 형식의 ID 인증서 설치](#)

[CSR에 서명한 CA 인증서 설치](#)

[ID 인증서 설치](#)

[새 인증서를 ASDM을 통해 인터페이스에 바인딩](#)

[ASDM을 사용하여 PKCS12 파일에 등록된 인증서 갱신](#)

[PKCS12 파일에서 갱신된 ID 인증서 및 CA 인증서 설치](#)

[새 인증서를 ASDM을 통해 인터페이스에 바인딩](#)

[다음을 확인합니다.](#)

[ASDM을 통해 설치된 인증서 보기](#)

[문제 해결](#)

[자주 묻는 질문\(FAQ\)](#)

# 소개

이 문서에서는 ASDM으로 관리되는 Cisco ASA Software에서 특정 유형의 인증서를 요청, 설치, 신뢰 및 갱신하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

- 시작하기 전에 ASA(Adaptive Security Appliance)에 올바른 클록 시간, 날짜 및 표준 시간대가 있는지 확인합니다. 인증서 인증에서는 NTP(Network Time Protocol) 서버를 사용하여 ASA의 시간을 동기화하는 것이 좋습니다. 관련 정보를 참조하십시오.
- CSR(Certificate Signing Request)을 사용하는 인증서를 요청하려면 신뢰할 수 있는 내부 또는 서드파티 CA(Certificate Authority)에 대한 액세스 권한이 있어야 합니다. 서드파티 CA 벤더의 예로는 Entrust, Geotrust, GoDaddy, Thawte, VeriSign 등이 있습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASAv 9.18.1
- 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 정보

이 문서의 주소 인증서 유형은 다음과 같습니다.

- 자체 서명 인증서
- 서드파티 인증 기관 또는 내부 CA에서 서명한 인증서

EAP 인증 프로토콜용 SSL(Secure Socket Layer), TLS(Transport Layer Security) 및 IKEv2 rfc7296에서는 SSL/TLS/IKEv2 서버가 클라이언트에 서버 인증을 수행할 서버 인증서를 제공하도록 요구합니다. 이를 위해 신뢰할 수 있는 서드파티 CA를 사용하여 ASA에 SSL 인증서를 발급하는 것이 좋습니다.

Cisco에서는 사용자가 실수로 비인가 서버의 인증서를 신뢰하도록 브라우저를 구성할 수 있기 때문에 자체 서명 인증서의 사용을 권장하지 않습니다. 사용자가 보안 게이트웨이에 연결할 때 보안 경고에 대응해야 하는 불편도 있다.

## ASDM을 사용하여 새 ID 인증서 요청 및 설치

인증서는 CA(Certificate Authority)에서 요청하고 ASA에 설치하는 두 가지 방법으로 사용할 수 있습니다.

- CSR(Certificate Signing Request)을 사용합니다. 키 쌍을 생성하고, CSR을 사용하여 CA에서 ID 인증서를 요청하며, CA에서 얻은 서명된 ID 인증서를 설치합니다.
- CA에서 가져왔거나 다른 디바이스에서 내보낸 PKCS12 파일을 사용합니다. PKCS12 파일에는 키 쌍, ID 인증서, CA 인증서가 들어 있습니다.

## CSR(Certificate Signing Request)을 사용하여 새 ID 인증서 요청 및 설치

CSR은 ID 인증서가 필요한 디바이스에 생성되며, 디바이스에 생성된 키 쌍을 사용합니다.

CSR에는 다음이 포함됩니다.

- 인증서 요청 정보 - 요청된 주체 및 기타 특성, 키 쌍의 공개 키,
- 서명 알고리즘 정보,
- 키 쌍의 개인 키로 서명된 인증서 요청 정보의 디지털 서명.

CSR은 CA(Certificate Authority)에 전달되므로 PKCS#10 형식으로 서명합니다.

서명된 인증서는 CA에서 PEM 형식으로 반환됩니다.

---

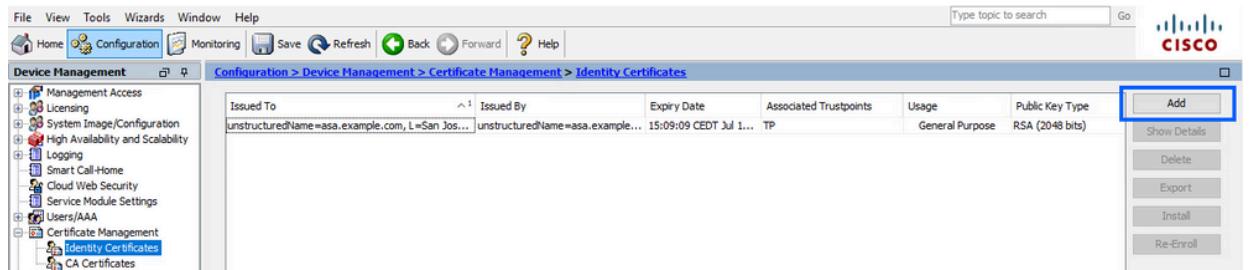
참고: CA는 CSR에 서명하고 서명된 ID 인증서를 생성할 때 신뢰 지점에 정의된 FQDN 및 주체 이름 매개변수를 변경할 수 있습니다.

---

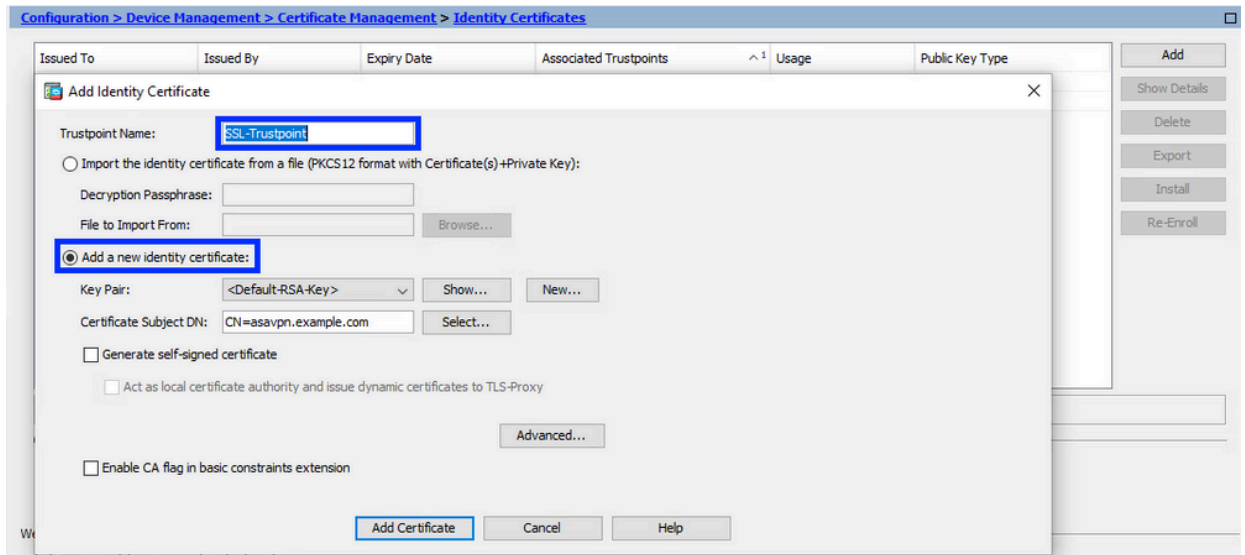
## ASDM으로 CSR 생성

### 1. 특정 이름으로 신뢰 지점 만들기

- a. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동합니다.



- b. Add(추가)를 클릭합니다.
- c. 신뢰 지점 이름을 정의합니다.

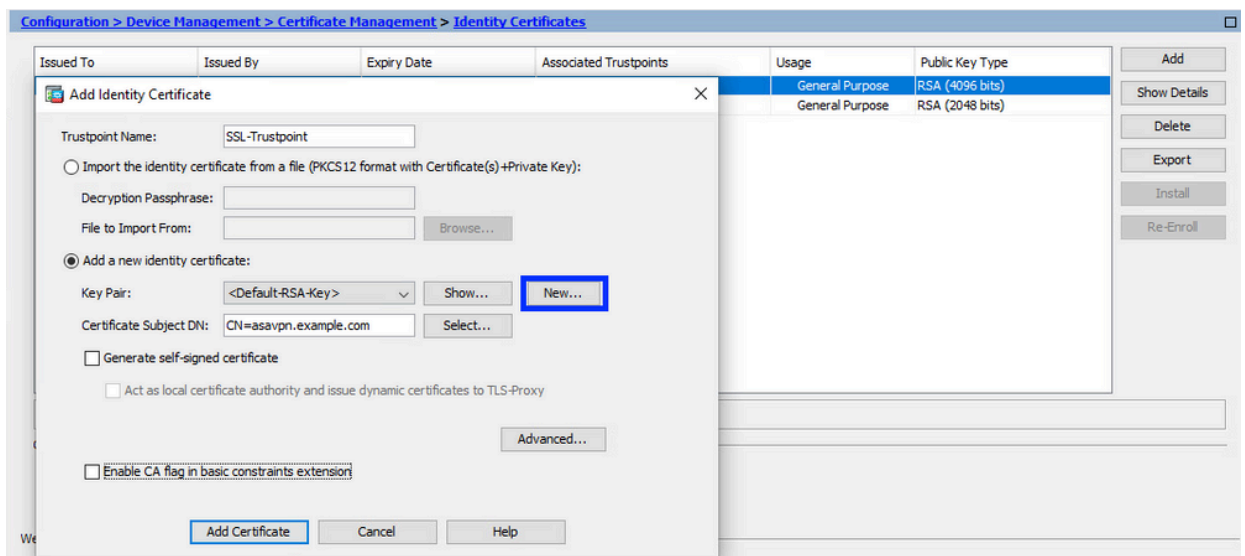


d. Add a New Identity Certificate(새 ID 인증서 추가) 라디오 버튼을 클릭합니다.

## 2. (선택 사항) 새 키 쌍 생성

참고: 기본적으로 Default-RSA-Key라는 이름과 2048의 크기를 갖는 RSA 키가 사용됩니다. 그러나 각 ID 인증서에 대해 고유한 개인/공용 키 쌍을 사용하는 것이 좋습니다.

a. New(새로 만들기)를 클릭하여 새 키 쌍을 생성합니다.

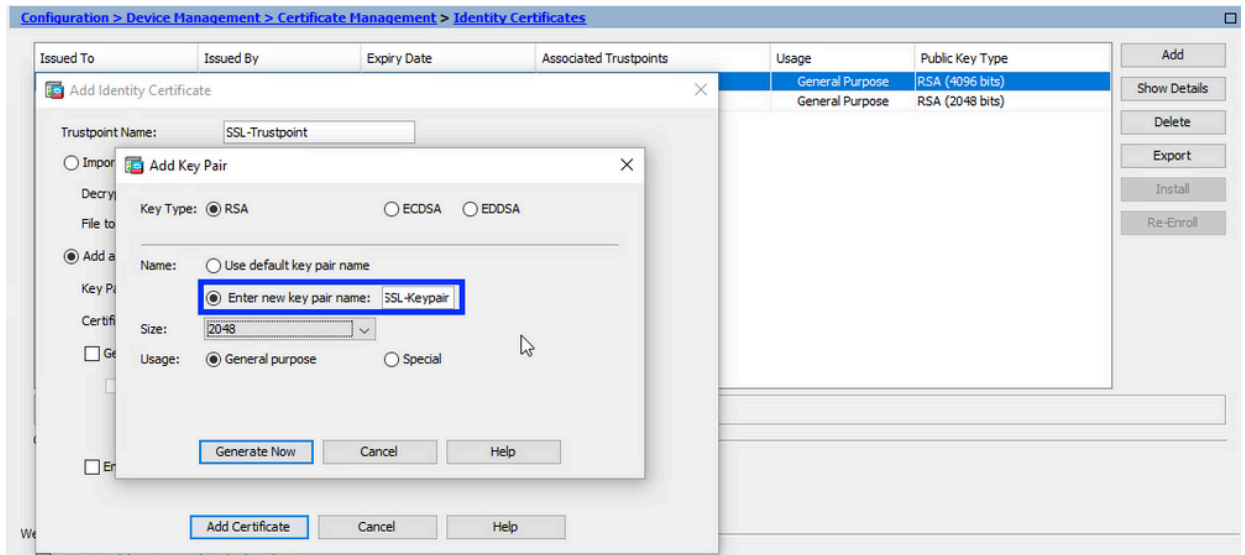


b. Enter new Key Pair name(새 키 쌍 이름 입력) 옵션을 선택하고 새 키 쌍의 이름을 입력합니다.

c. Key Type(키 유형) - RSA 또는 ECDSA를 선택합니다.

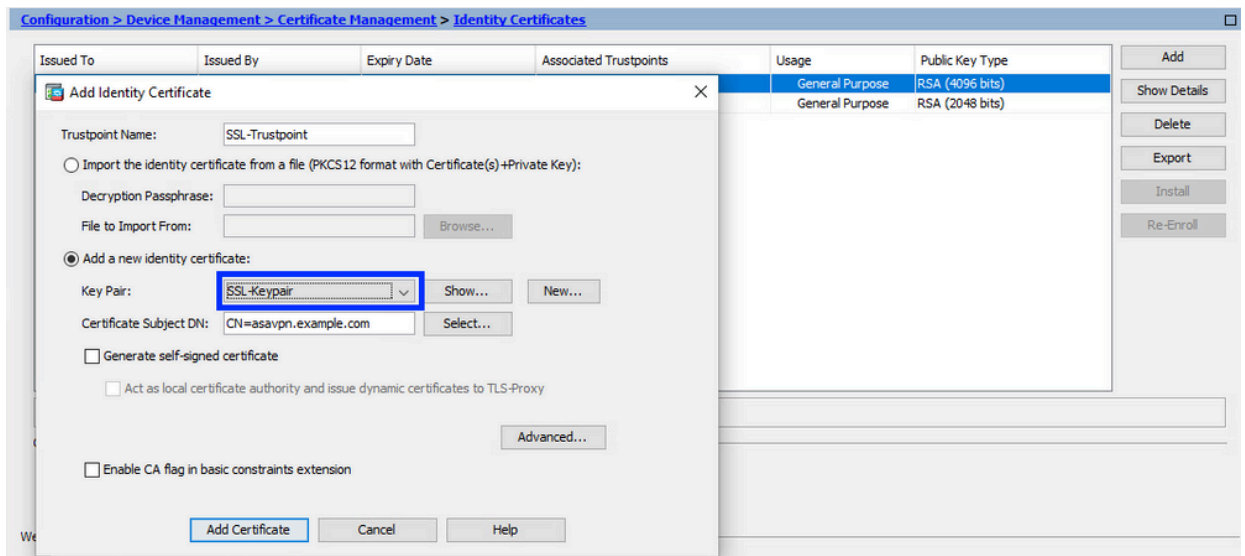
d. Key Size(키 크기)를 선택합니다. RSA의 경우 General purpose for Usage(사용 용도)를 선택합니다.

e. Generate Now(지금 생성)를 클릭합니다. 이제 키 쌍이 생성됩니다.



### 3. 키 쌍 이름 선택

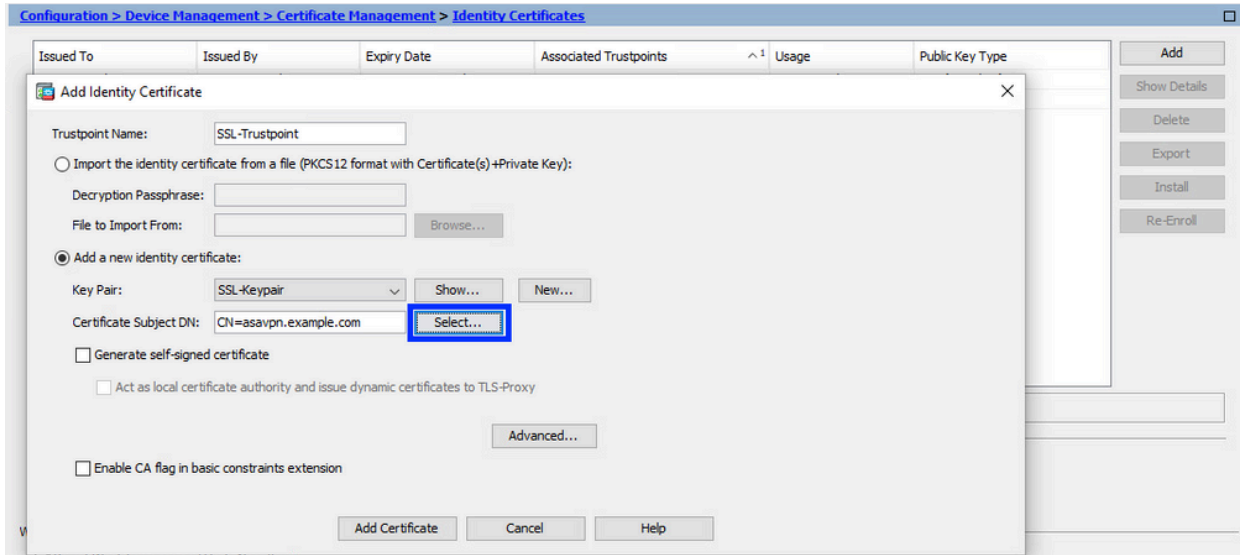
CSR에 서명하고 새 인증서와 바인딩할 키 쌍을 선택합니다.



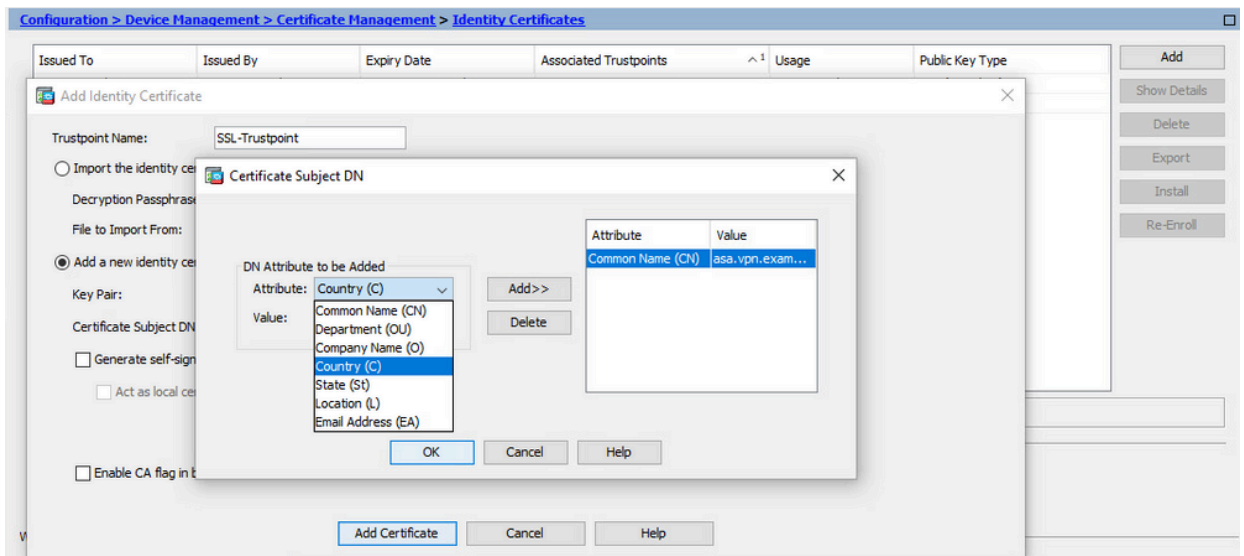
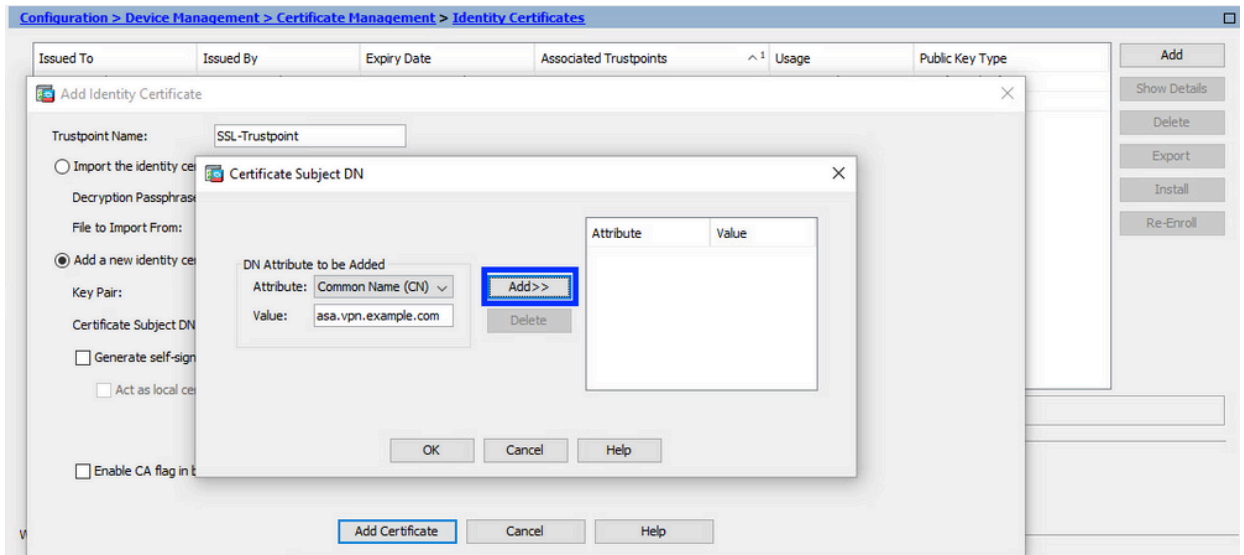
### 4. 인증서 주체 및 FQDN(정규화된 도메인 이름)을 구성합니다

주의: FQDN 매개변수는 ID 인증서가 사용되는 ASA 인터페이스의 FQDN 또는 IP 주소와 일치해야 합니다. 이 매개변수는 ID 인증서에 대해 요청된 SAN(Subject Alternative Name) 확장을 설정합니다. SAN 확장은 SSL/TLS/IKEv2 클라이언트에서 인증서가 연결되는 FQDN과 일치하는지 확인하는 데 사용됩니다.

a. 선택을 클릭합니다.



b. Certificate Subject DN(인증서 주체 DN) 창에서 인증서 특성을 구성합니다. 드롭다운 목록에서 특성을 선택하고 값을 입력한 다음 Add(추가)를 클릭합니다.

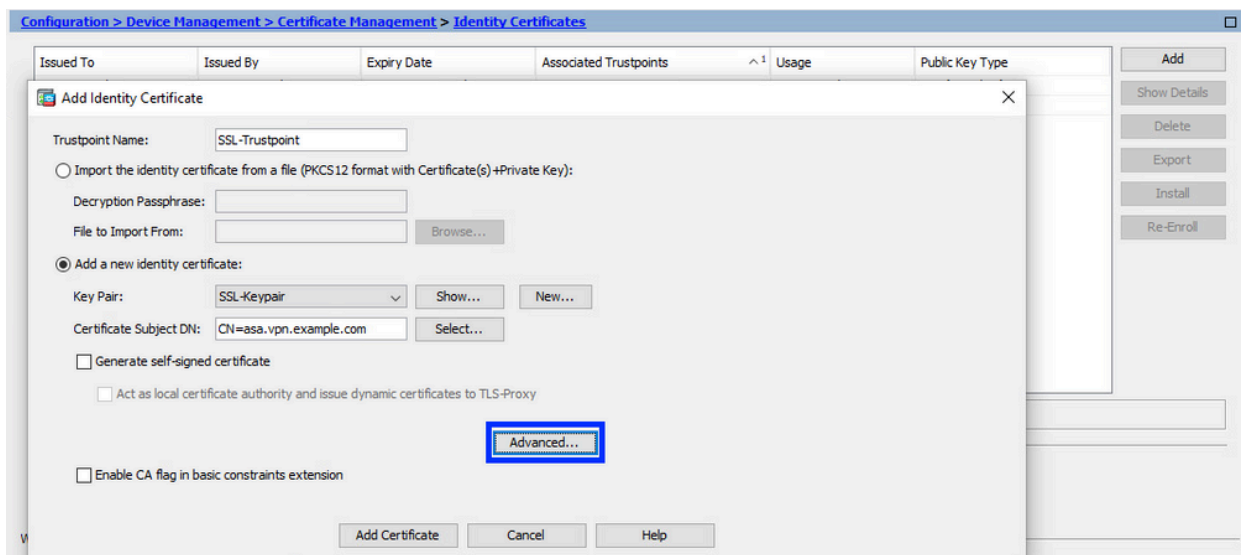


속성	설명
CN	방화벽에 액세스할 수 있는 이름(일반적으로 정규화된 도메인 이름(예: vpn.example.com)).
오우	조직 내 부서 이름
O	합법적으로 등록된 조직/회사 이름
C	국가 코드(문장 부호 없는 2자 코드)
ST	조직이 위치한 상태입니다.
L	조직이 위치한 도시입니다.
EA	이메일 주소

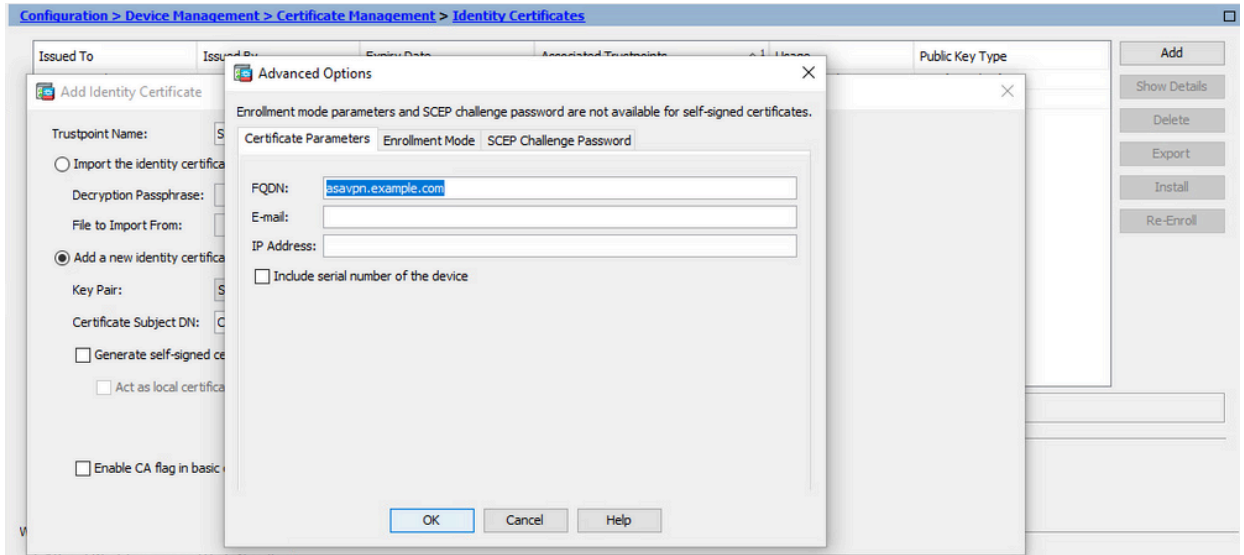
참고: 이전 필드 값은 64자 제한을 초과할 수 없습니다. 값이 길면 ID 인증서 설치에 문제가 발생할 수 있습니다. 또한 모든 DN 특성을 정의할 필요는 없습니다.

모든 특성을 추가한 후 OK를 클릭합니다.

- c. 디바이스 FQDN을 구성합니다. Advanced(고급)를 클릭합니다.

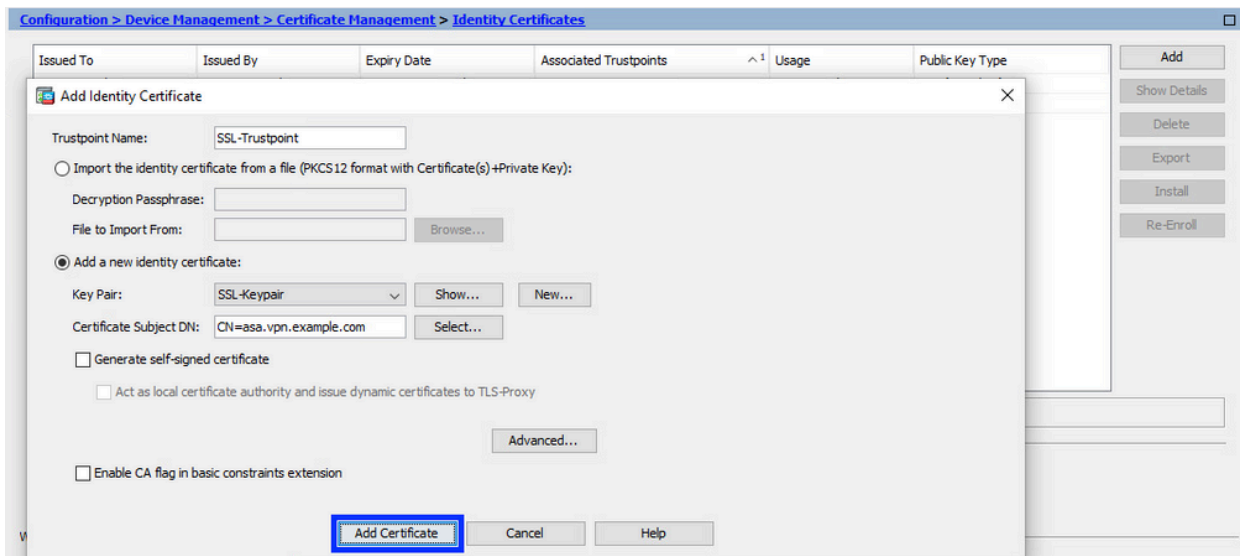


- d. FQDN 필드에 인터넷에서 디바이스에 액세스할 수 있는 정규화된 도메인 이름을 입력합니다. OK(확인)를 클릭합니다.

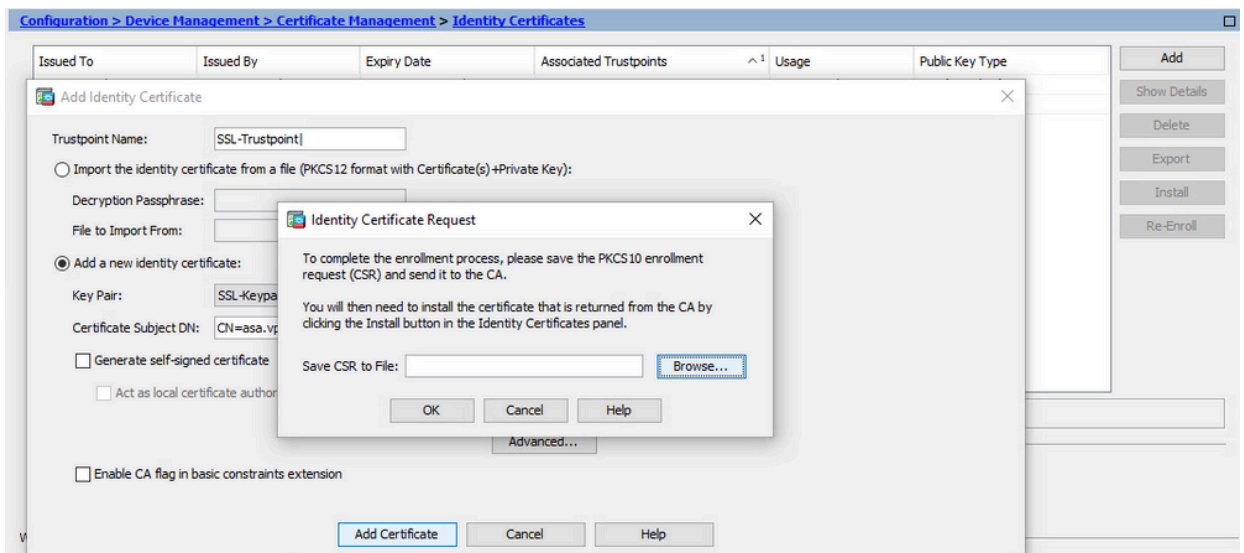


## 5. CSR 생성 및 저장

a. Add Certificate(인증서 추가)를 클릭합니다.



b. CSR을 로컬 시스템의 파일에 저장하기 위한 프롬프트가 표시됩니다.

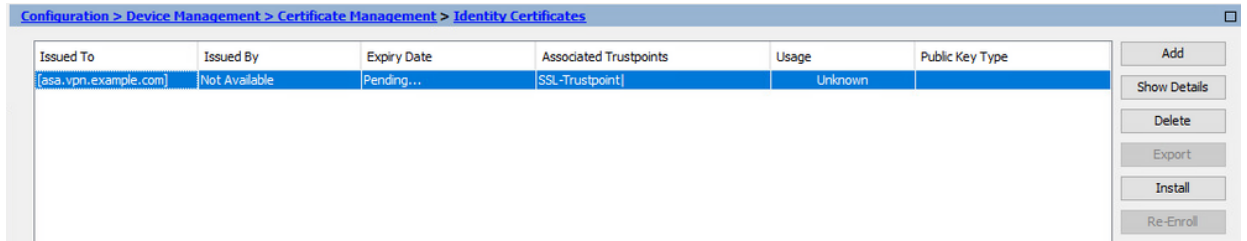




Browse(찾아보기)를 클릭하고 CSR을 저장할 위치를 선택한 다음 .txt 확장자로 파일을 저장합니다.

참고: 파일을 .txt 확장자로 저장하면 PKCS#10 요청을 열고 텍스트 편집기(예: 메모장)로 볼 수 있습니다.

c. 이제 새 신뢰 지점이 Pending(보류 중) 상태로 표시됩니다.



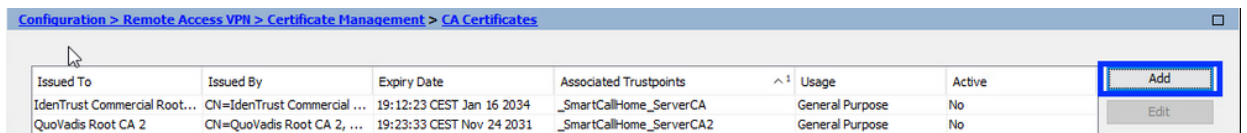
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	
[asa.vpn.example.com]	Not Available	Pending...	SSL-Trustpoint	Unknown		<input type="button" value="Add"/> <input type="button" value="Show Details"/> <input type="button" value="Delete"/> <input type="button" value="Export"/> <input type="button" value="Install"/> <input type="button" value="Re-Enroll"/>

## ASDM을 사용하여 PEM 형식의 ID 인증서 설치

설치 단계에서는 CA가 CSR에 서명하고 PEM 인코딩(.pem, .cer, .crt) ID 인증서 및 CA 인증서 번들을 제공했다고 가정합니다.

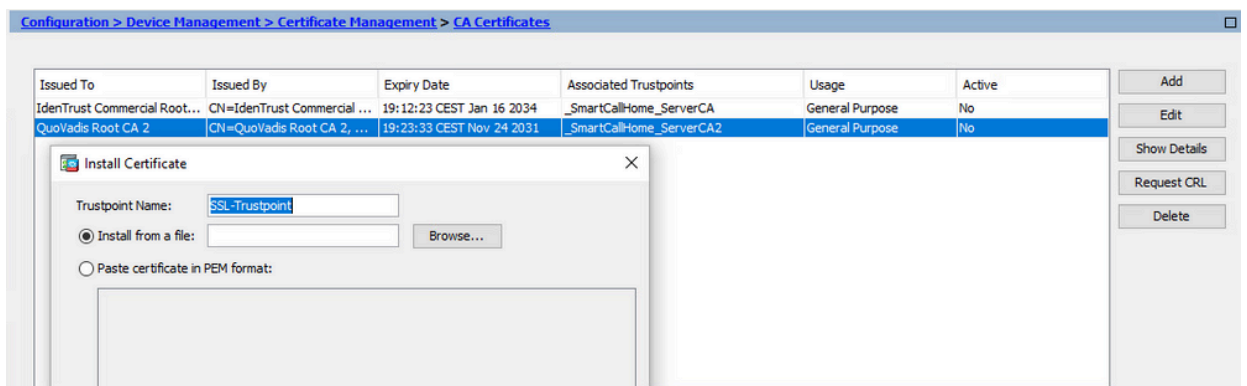
### 1. CSR에 서명한 CA 인증서 설치

a. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) >로 이동하고 CA Certificates(CA 인증서)를 선택합니다. Add(추가)를 클릭합니다.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	<input type="button" value="Add"/> <input type="button" value="Edit"/>
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	

b. 신뢰 지점 이름을 입력하고 Install From File(파일에서 설치)을 선택하고 Browse(찾아보기) 버튼을 클릭한 다음 중간 인증서를 선택합니다. 또는 텍스트 파일의 PEM 인코딩 CA 인증서를 텍스트 필드에 붙여넣습니다.



Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active	
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Show Details"/> <input type="button" value="Request CRL"/> <input type="button" value="Delete"/>
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No	

Install Certificate

Trustpoint Name:

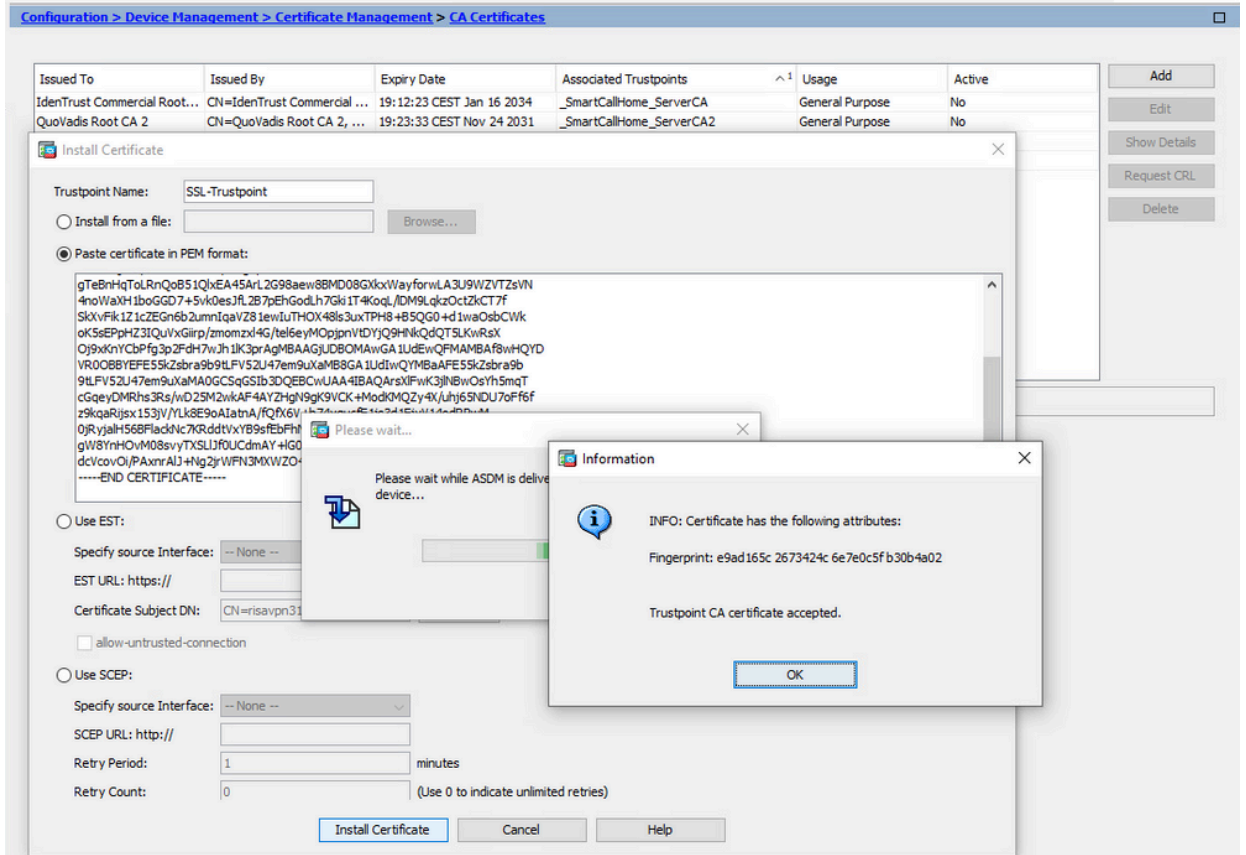
Install from a file:

Paste certificate in PEM format:

참고: CSR에 서명한 CA 인증서를 설치하고 ID 인증서와 동일한 신뢰 지점 이름을 사용합니다. PKI 계층 구조의 다른 CA 인증서는 별도의 신뢰 지점에 설치할 수 있

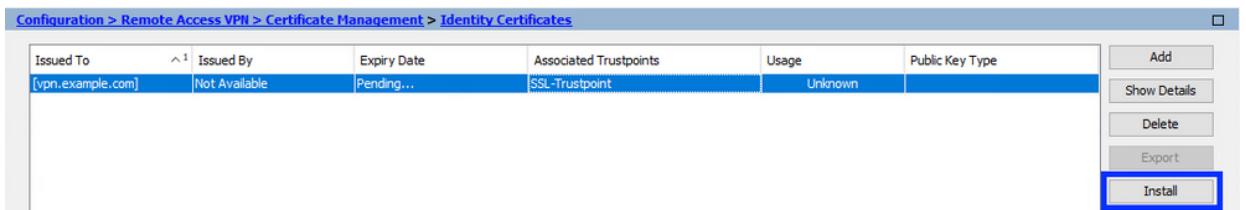
습니다.

c. Install Certificate를 클릭합니다.



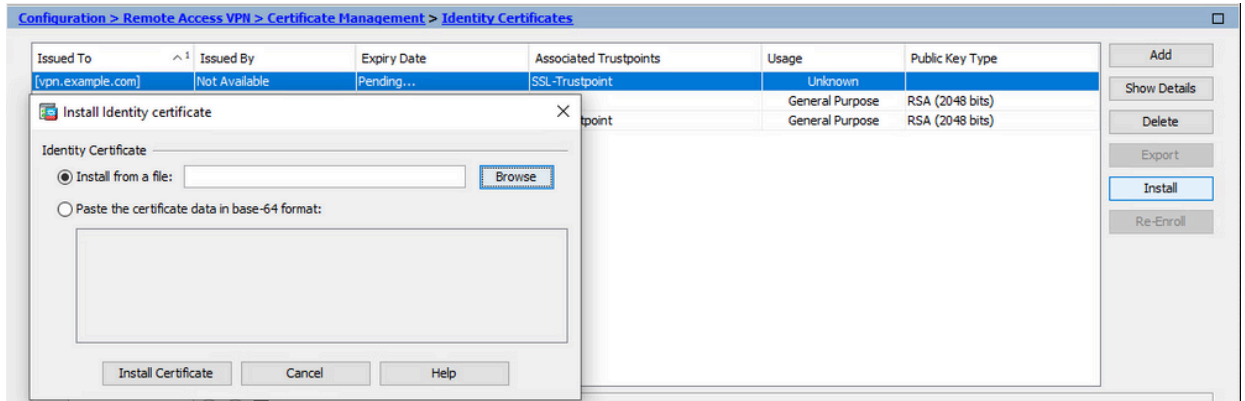
2. ID 인증서 설치

a. CSR 생성 중에 이전에 생성 된 ID 인증서를 선택 합니다. Install(설치)을 클릭합니다.



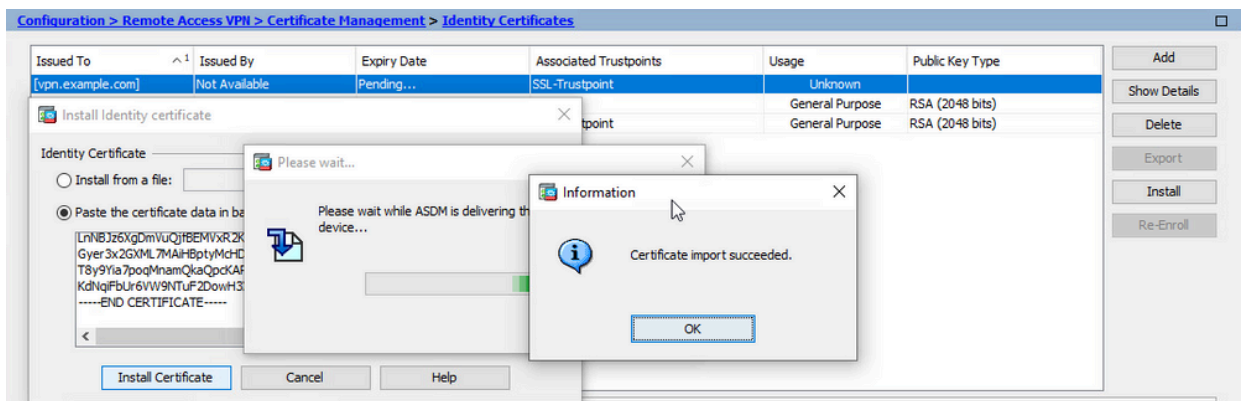
참고: Identity Certificate(ID 인증서)에는 Issued By(발급자) 필드를 Not available(사용할 수 없음)으로 지정하고 Expiry Date(만료일) 필드를 Pending(보류 중)으로 지정할 수 있습니다.

b. CA에서 받은 PEM 인코딩 ID 인증서가 포함된 파일을 선택하거나 텍스트 편집기에서 PEM 인코딩 인증서를 열고 CA에서 제공한 ID 인증서를 복사하여 텍스트 필드에 붙여 넣습니다.



참고: ID 인증서는 설치할 .pem, .cer, .crt 형식일 수 있습니다.

c. Install Certificate를 클릭합니다.



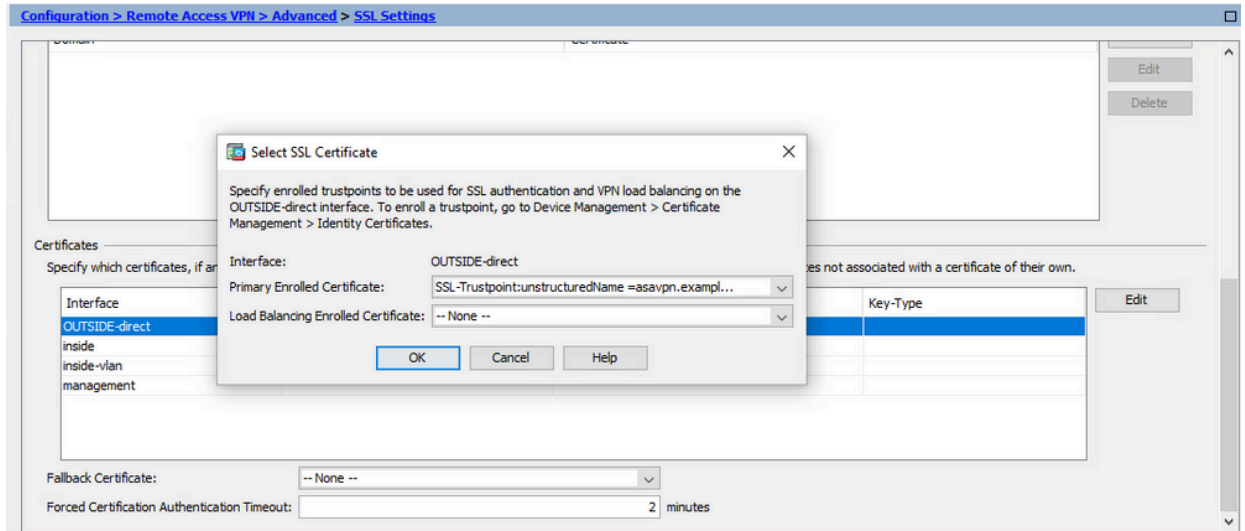
### 3. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

- Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.
- Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합니다. 이 예에서는 외부 인터페이스가 사용됩니다.

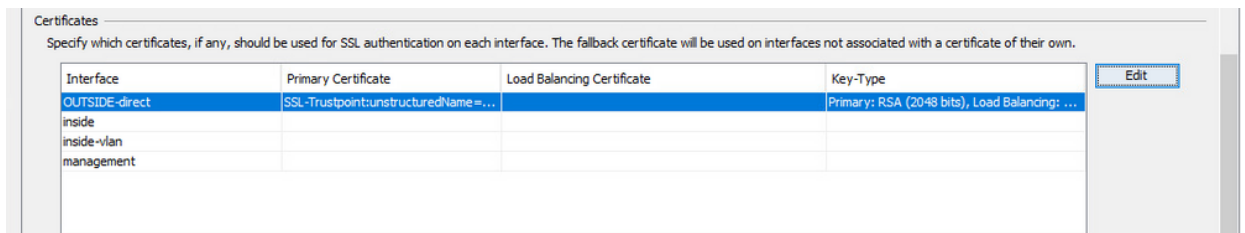
Edit를 클릭합니다.

- Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.



d. OK(확인)를 클릭합니다.

e. 적용을 클릭합니다.



이제 새 ID 인증서가 사용 중입니다.

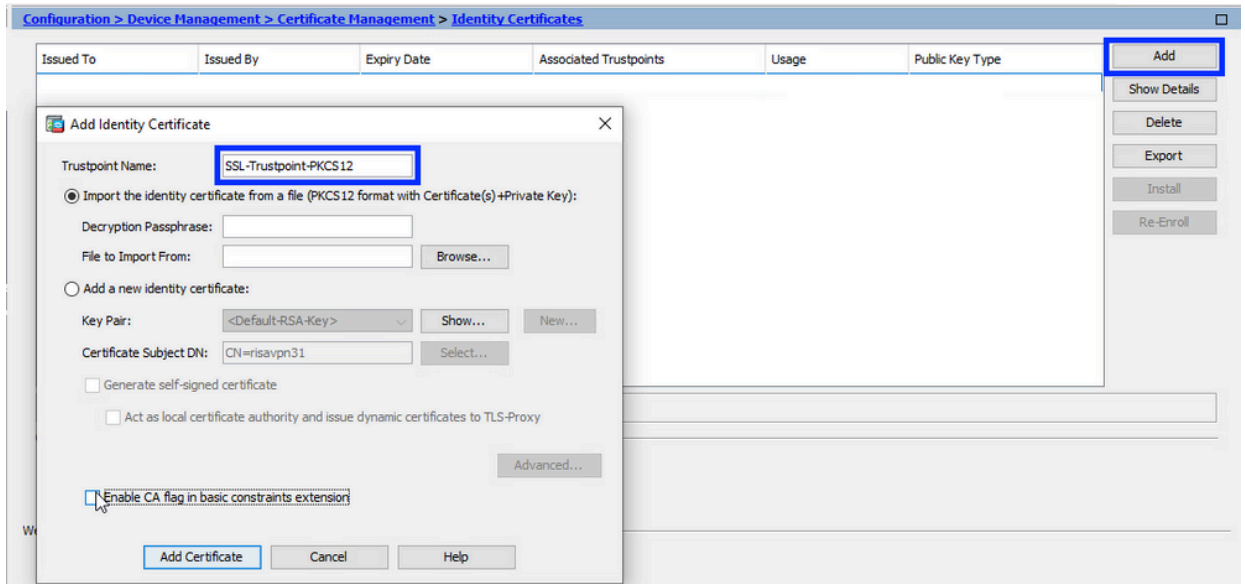
## ASDM을 사용하여 PKCS12 형식으로 받은 ID 인증서 설치

PKCS12 파일(.p12 또는 .pfx 형식)에는 ID 인증서, 키 쌍 및 CA 인증서가 포함되어 있습니다. 와일드카드 인증서의 경우처럼 CA에 의해 생성되거나 다른 디바이스에서 내보내집니다. 이진 파일이므로 텍스트 편집기로 볼 수 없습니다.

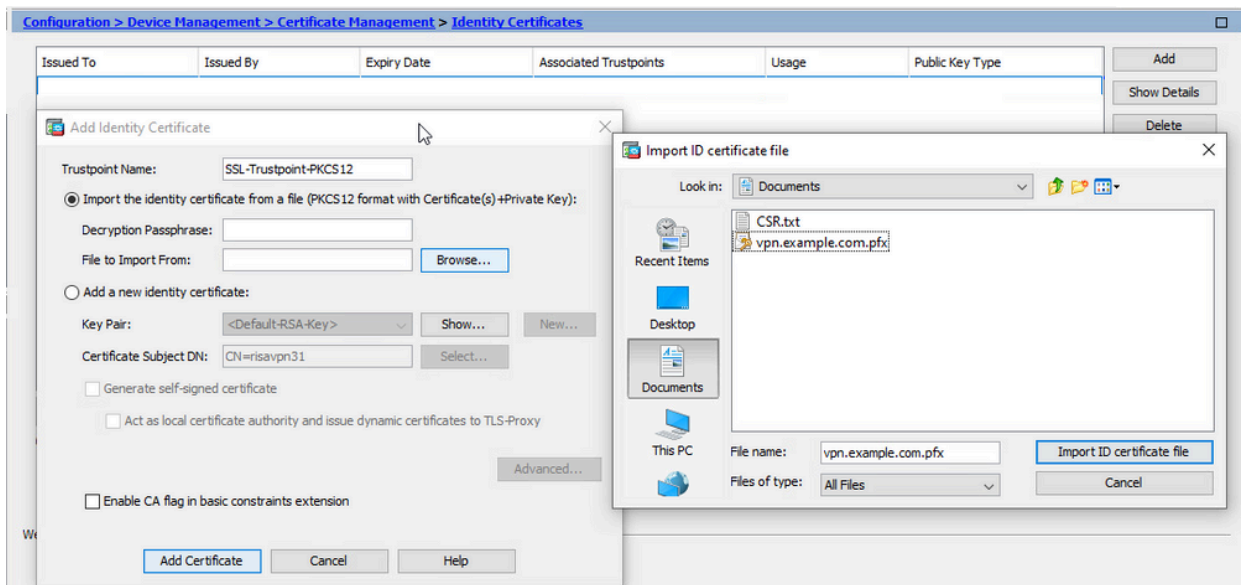
### 1. PKCS12 파일에서 ID 및 CA 인증서 설치

ID 인증서, CA 인증서 및 키 쌍은 단일 PKCS12 파일에 번들로 묶어야 합니다.

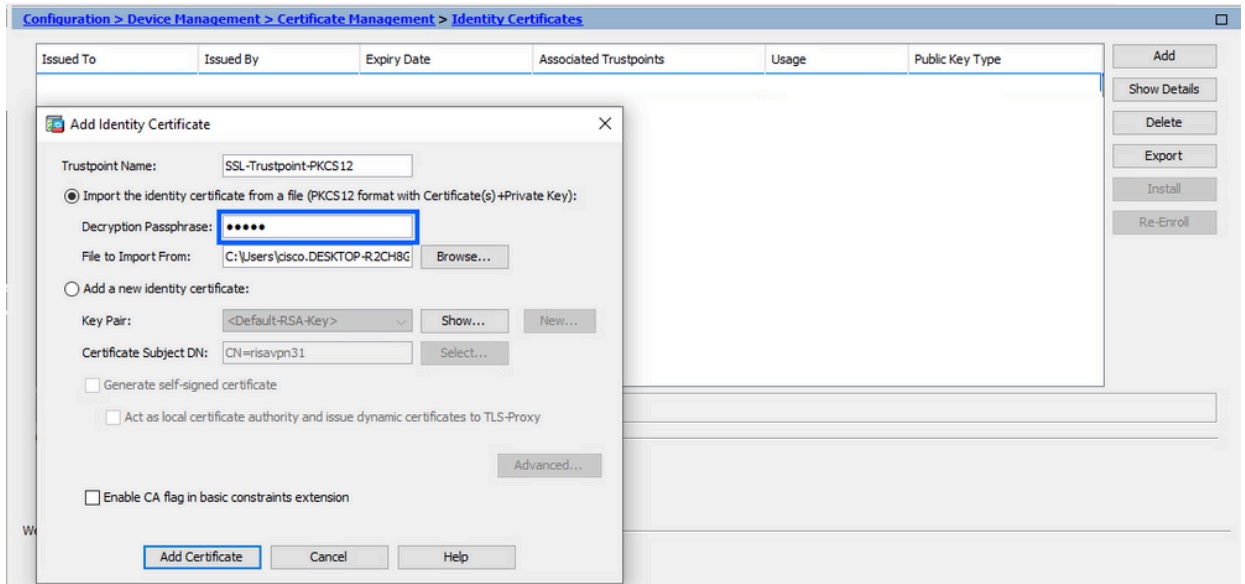
- Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리)로 이동하고 Identity Certificates(ID 인증서)를 선택합니다.
- Add(추가)를 클릭합니다.
- 신뢰 지점 이름을 지정합니다.



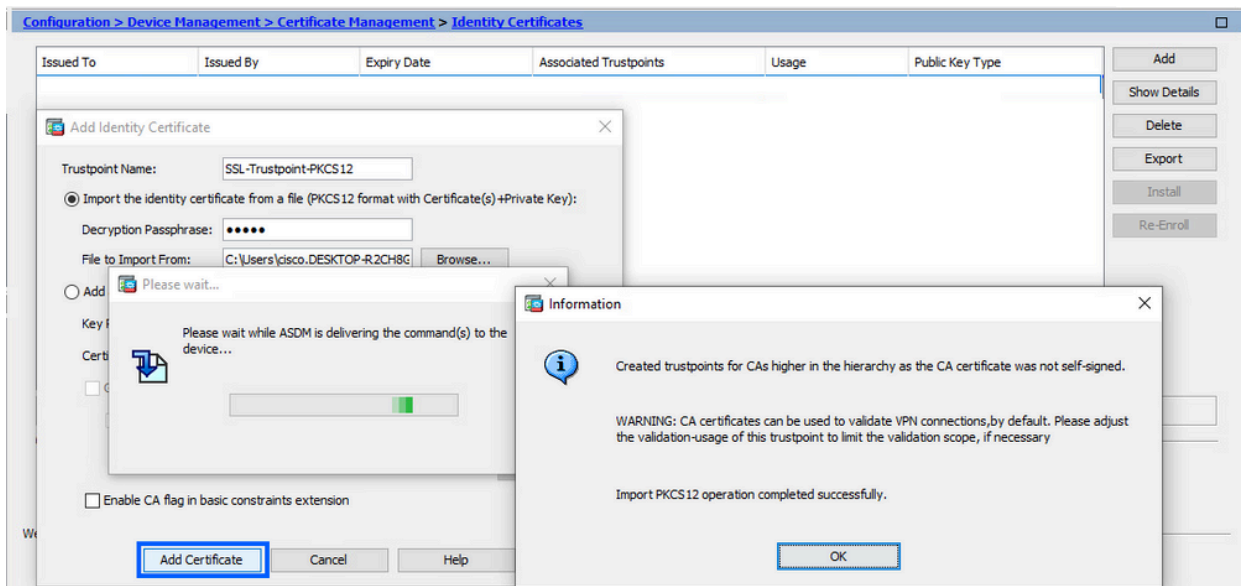
d. Import The Identity Certificate from a File(파일에서 ID 인증서 가져오기) 라디오 버튼을 클릭합니다.



e. PKCS12 파일을 생성하는 데 사용되는 패스프레이즈를 입력합니다.



f. Add Certificate를 클릭합니다.



참고: CA 인증서 체인이 포함된 PKCS12를 가져오면 ASDM은 -number 접미사가 추가된 이름과 함께 업스트림 CA 신뢰 지점을 자동으로 생성합니다.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub 1-1	CN=KrakowCA-sub 1	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12	Signature	Yes
KrakowCA-sub 1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-2	Signature	Yes

## 2. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

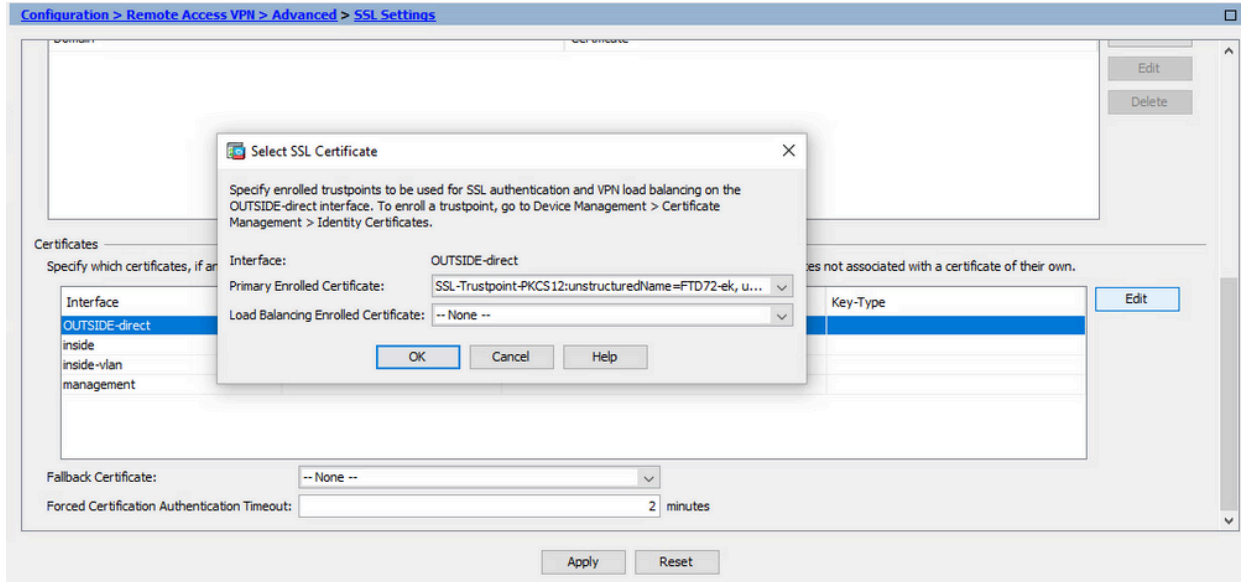
지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

a. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.

b. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합니다. 이 예에서는 외부 인터페이스가 사용됩니다.

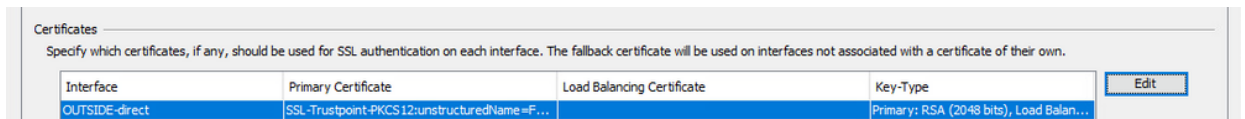
Edit를 클릭합니다.

c. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.



d. OK(확인)를 클릭합니다.

e. 적용을 클릭합니다.



이제 새 ID 인증서가 사용 중입니다.

## 인증서 갱신

### ASDM을 사용하여 CSR(Certificate Signing Request)로 등록된 인증서 갱신

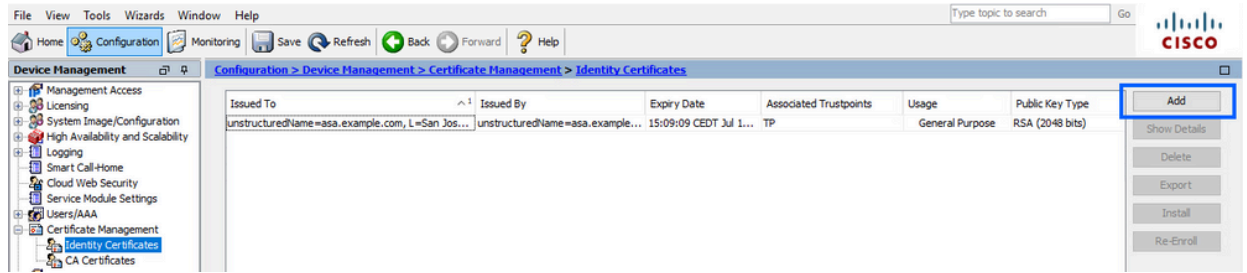
CSR 등록 인증서의 인증서 갱신은 새 신뢰 지점을 생성하고 등록해야 합니다. 다른 이름(예: 등록 연도 접미사가 있는 이전 이름)이 있어야 합니다. 이전 인증서와 동일한 매개변수와 키 쌍을 사용하거나 다른 매개변수를 사용할 수 있습니다.

#### ASDM으로 CSR 생성

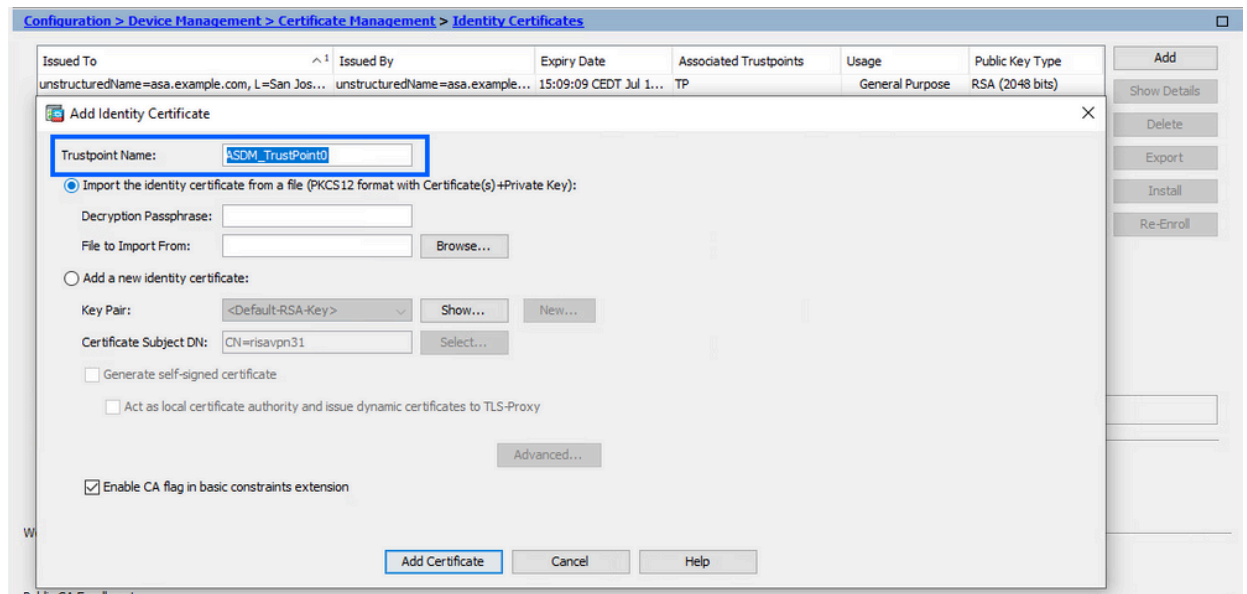
1. 특정 이름으로 새 신뢰 지점을 만듭니다.

a. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동합니다.





- b. Add(추가)를 클릭합니다.
- c. 신뢰 지점 이름을 정의합니다.



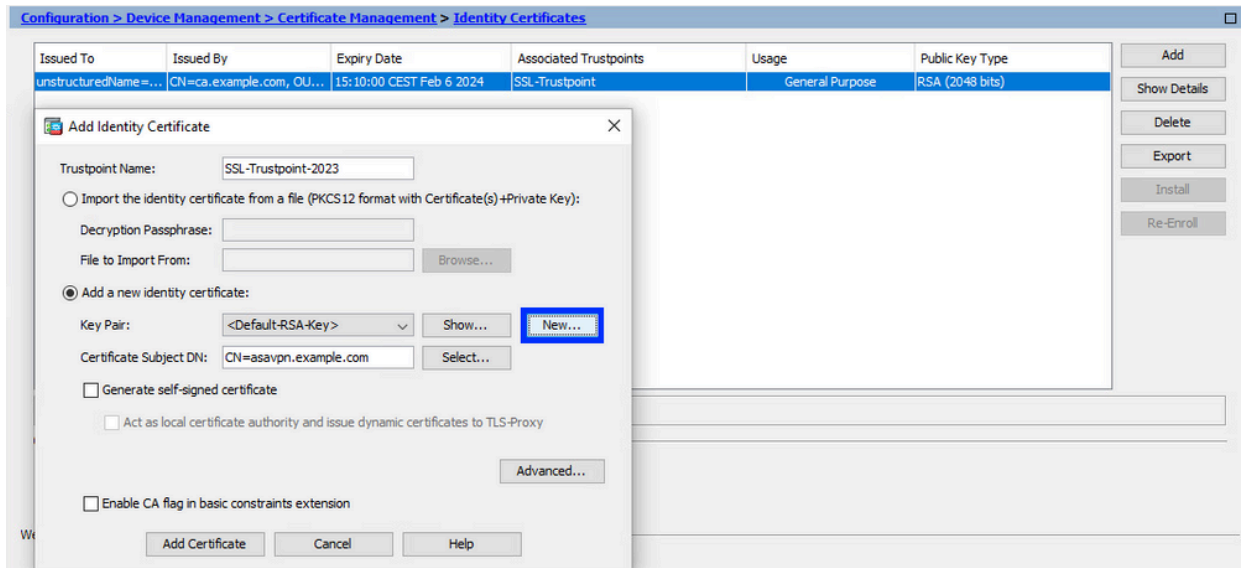
- d. Add a New Identity Certificate(새 ID 인증서 추가) 라디오 버튼을 클릭합니다.

## 2. (선택 사항) 새 키 쌍 생성

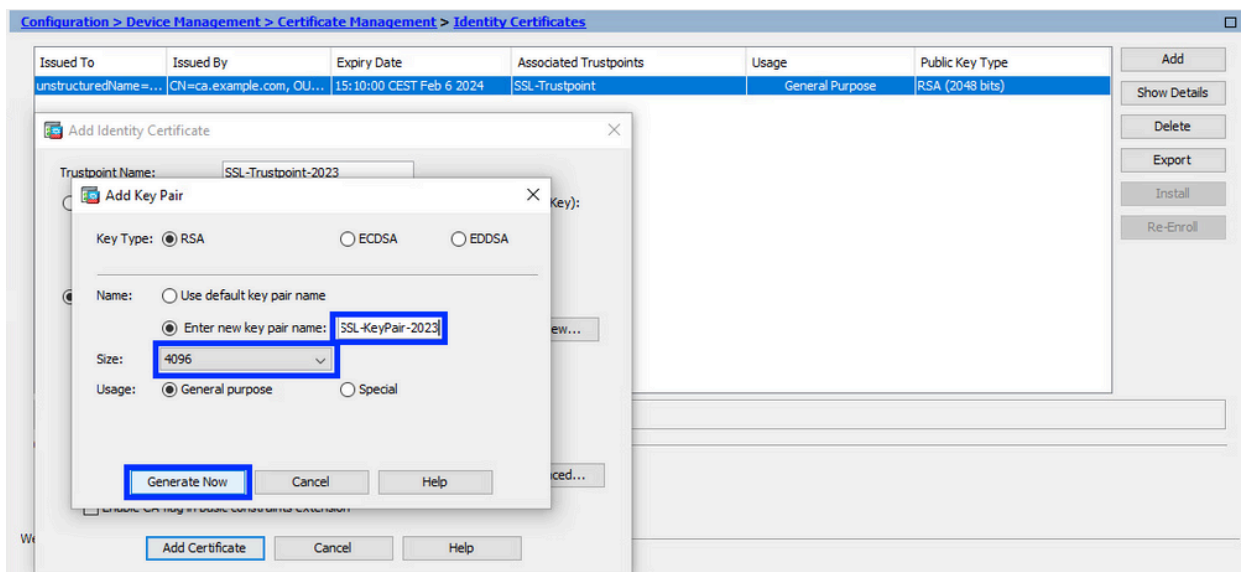
참고: 기본적으로 Default-RSA-Key라는 이름과 2048의 크기를 갖는 RSA 키가 사용됩니다. 그러나 각 ID 인증서에 대해 고유한 개인/공용 키 쌍을 사용하는 것이 좋습니다.

- a. New(새로 만들기)를 클릭하여 새 키 쌍을 생성합니다.



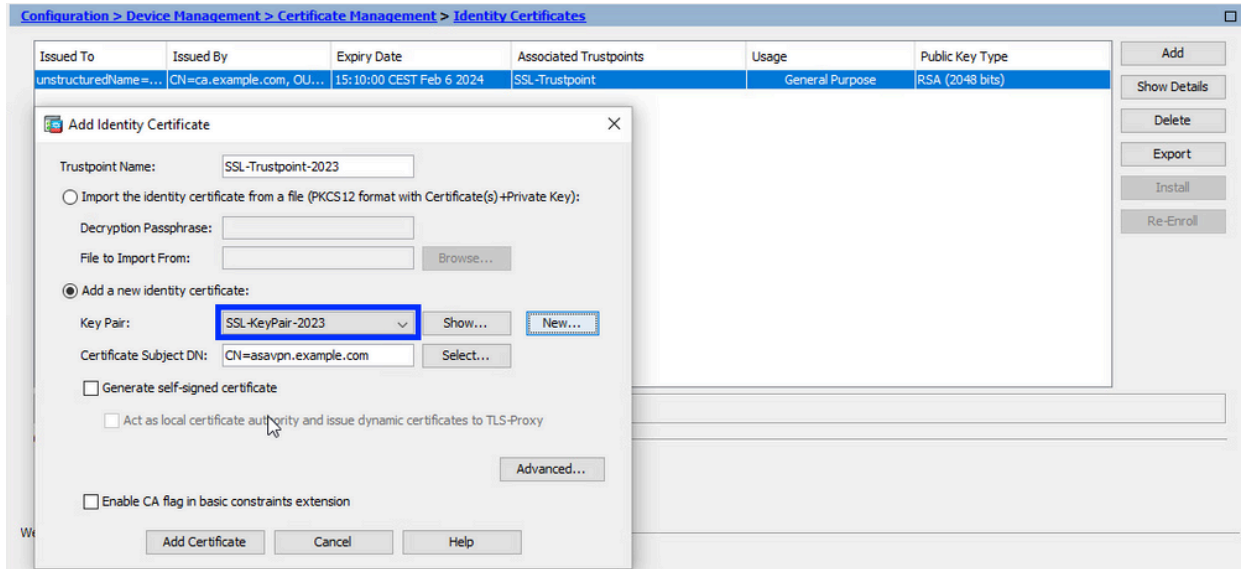


- b. Enter new Key Pair name(새 키 쌍 이름 입력) 옵션을 선택하고 새 키 쌍의 이름을 입력합니다.
- c. 키 유형(RSA 또는 ECDSA)을 선택합니다.
- d. Key Size(키 크기)를 선택합니다. RSA의 경우 General purpose for Usage(사용 용도)를 선택합니다.
- e. Generate Now(지금 생성)를 클릭합니다. 이제 키 쌍이 생성됩니다.



### 3. 키 쌍 이름 선택

CSR에 서명하고 새 인증서와 바인딩할 키 쌍을 선택합니다.

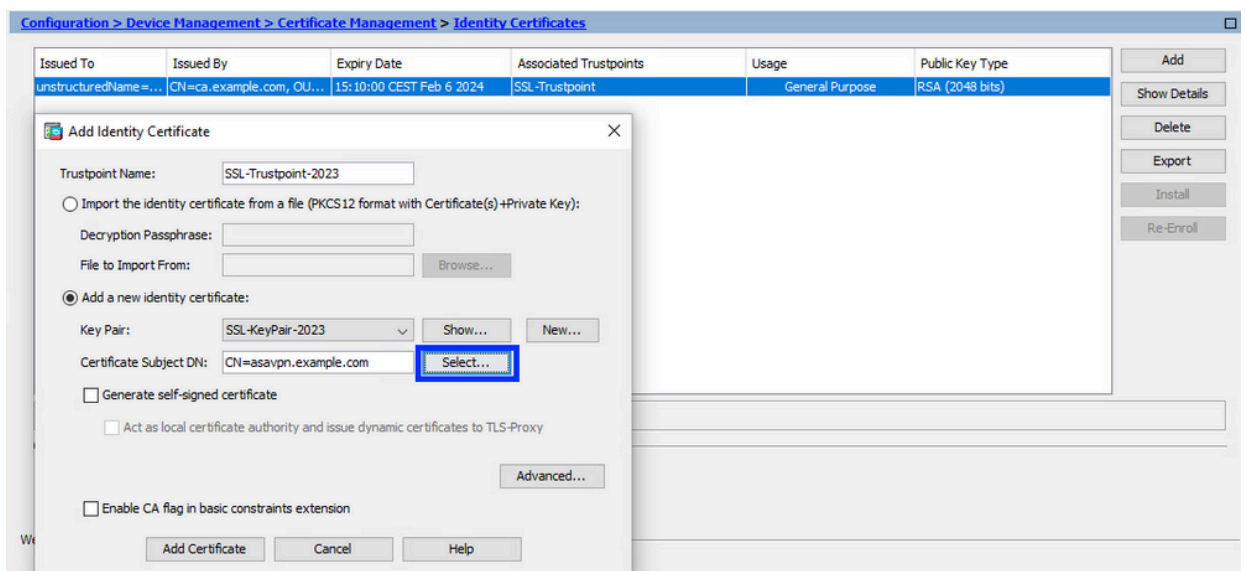


#### 4. 인증서 주체 및 FQDN(정규화된 도메인 이름)을 구성합니다

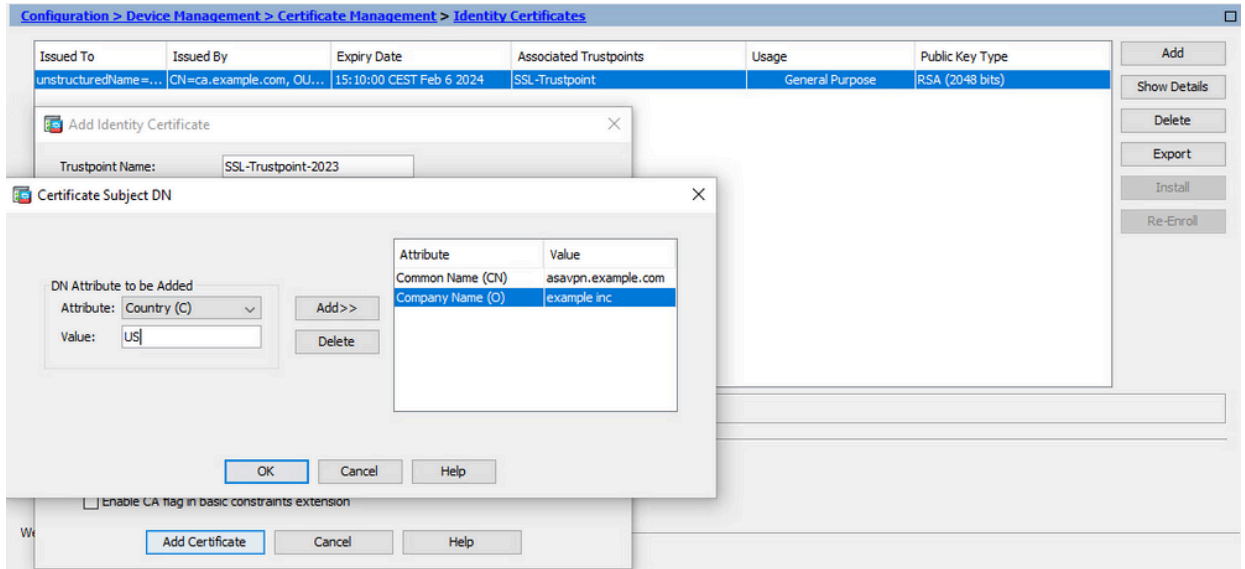
주의: FQDN 매개변수는 인증서가 사용되는 ASA 인터페이스의 FQDN 또는 IP 주소와 일치해야 합니다. 이 매개변수는 인증서의 SAN(주체 대체 이름)을 설정합니다. SAN 필드는 SSL/TLS/IKEv2 클라이언트에서 인증서가 연결되는 FQDN과 일치하는지 확인하는 데 사용됩니다.

참고: CA는 CSR에 서명하고 서명된 ID 인증서를 생성할 때 신뢰 지점에 정의된 FQDN 및 주체 이름 매개변수를 변경할 수 있습니다.

##### a. 선택을 클릭합니다.



##### b. Certificate Subject DN(인증서 주체 DN) 창의 드롭다운 목록에서 특성을 선택하여 인증서 특성을 구성하고 값을 입력하고 Add(추가)를 클릭합니다.

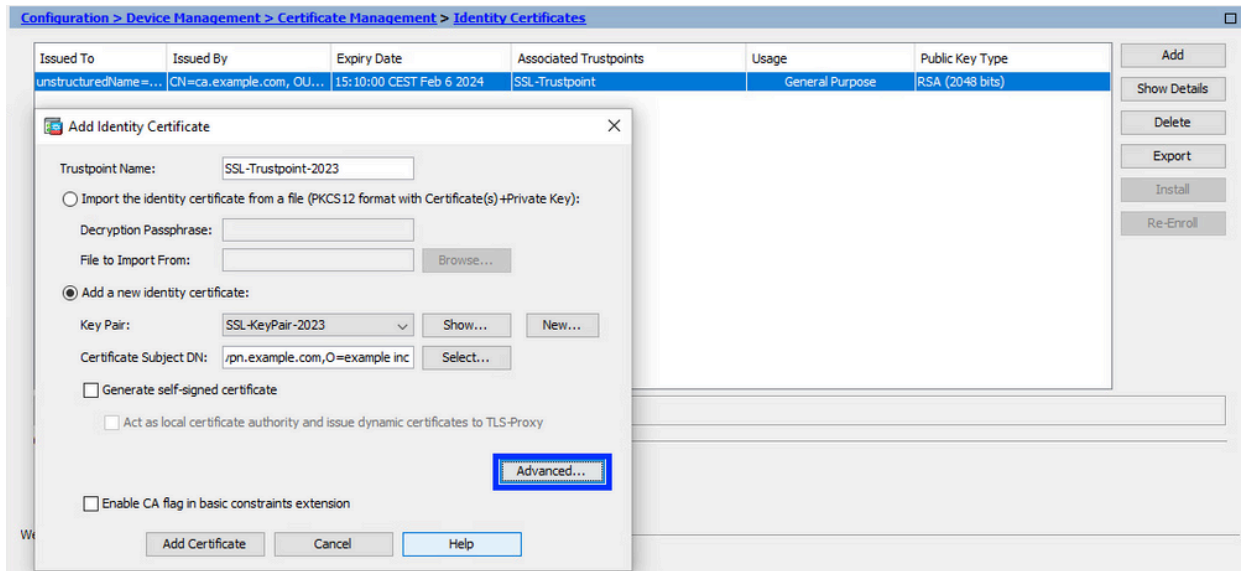


속성	설명
CN	방화벽에 액세스할 수 있는 이름(일반적으로 정규화된 도메인 이름(예: vpn.example.com)).
오우	조직 내 부서 이름
O	합법적으로 등록된 조직/회사 이름
C	국가 코드(문장 부호 없는 2자 코드)
ST	조직이 위치한 상태입니다.
L	조직이 위치한 도시입니다.
EA	이메일 주소

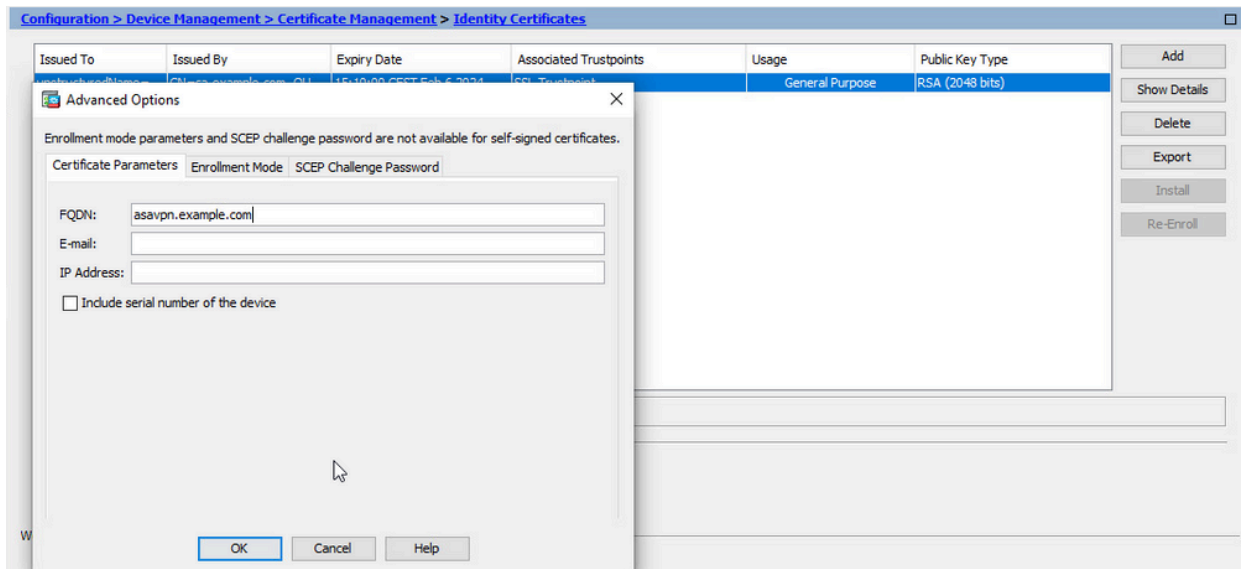
참고: 이전 필드는 64자 제한을 초과할 수 없습니다. 값이 길면 ID 인증서 설치에 문제가 발생할 수 있습니다. 또한 모든 DN 특성을 정의할 필요는 없습니다.

모든 특성을 추가한 후 OK를 클릭합니다.

c. 디바이스 FQDN을 구성하려면 Advanced(고급)를 클릭합니다.

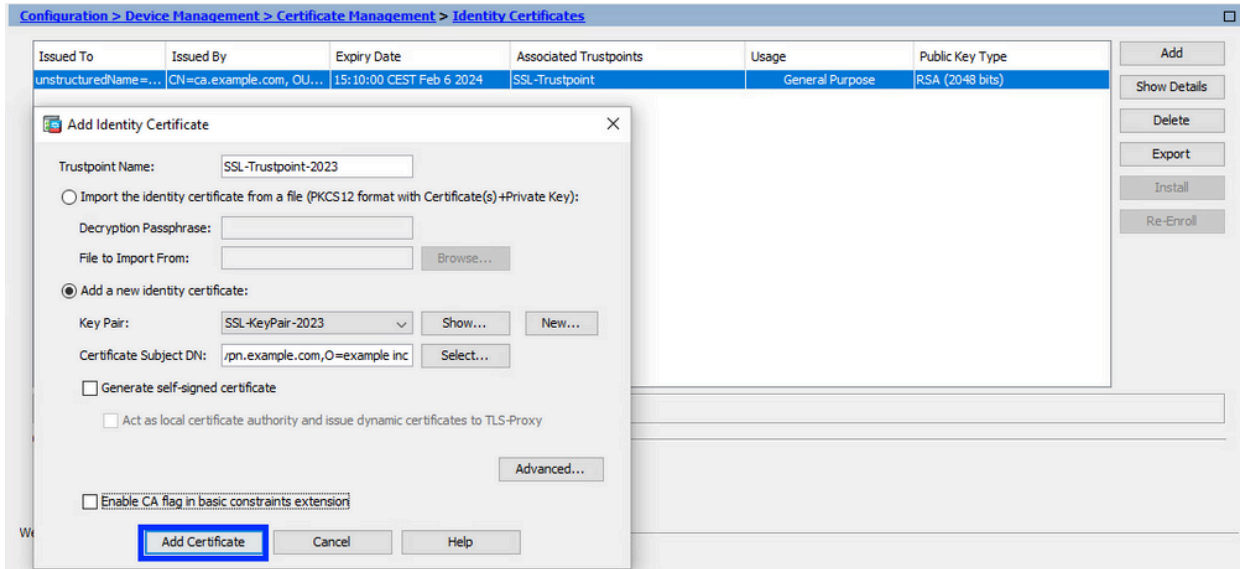


d. FQDN 필드에 인터넷에서 디바이스에 액세스할 수 있는 정규화된 도메인 이름을 입력합니다. OK(확인)를 클릭합니다.

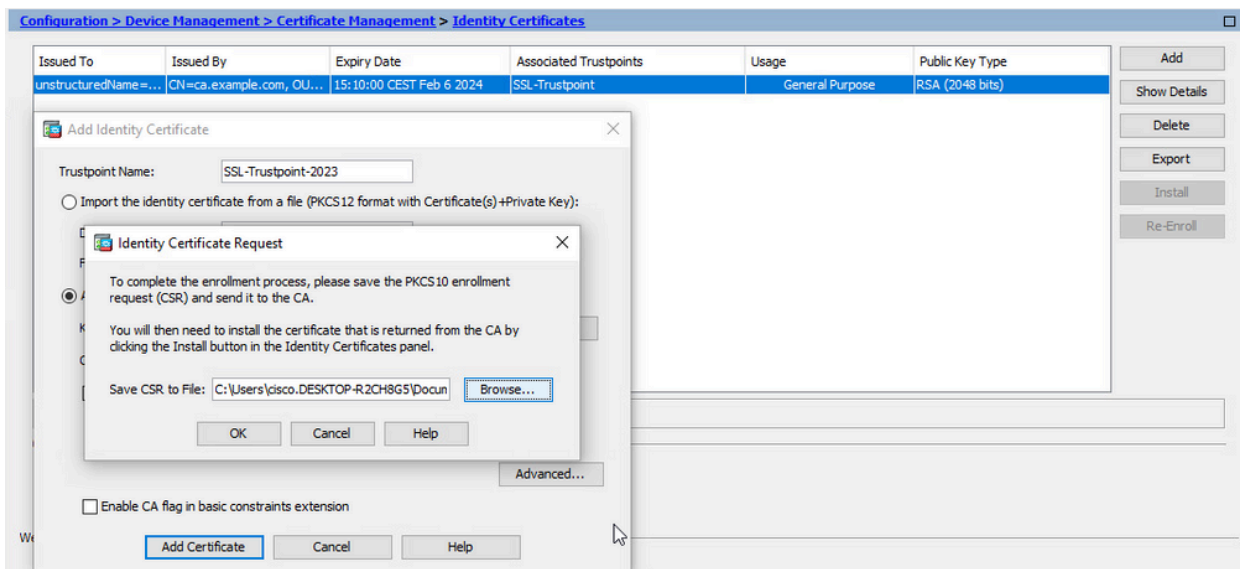


## 5. CSR 생성 및 저장

a. Add Certificate(인증서 추가)를 클릭합니다.



b. 로컬 시스템의 파일에 CSR을 저장하기 위한 프롬프트가 표시됩니다.



Browse(찾아보기)를 클릭합니다. CSR을 저장할 위치를 선택하고 .txt 확장자로 파일을 저장합니다.

참고: 파일을 .txt 확장자로 저장하면 PKCS#10 요청을 열고 텍스트 편집기(예: 메모장)로 볼 수 있습니다.

c. 이제 새 신뢰 지점이 Pending(보류 중) 상태로 표시됩니다.

Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU=...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[saavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Buttons: Add, Show Details, Delete, Export, Install, Re-Enroll

## ASDM을 사용하여 PEM 형식의 ID 인증서 설치

설치 단계에서는 CA가 CSR에 서명하고 PEM 인코딩(.pem, .cer, .crt)된 새 ID 인증서 및 CA 인증서 번들을 제공했다고 가정합니다.

### 1. CSR에 서명한 CA 인증서 설치

ID 인증서에 서명한 CA 인증서는 ID 인증서에 대해 생성된 신뢰 지점에 설치할 수 있습니다. ID 인증서가 중간 CA에 의해 서명된 경우 이 CA 인증서를 ID 인증서 신뢰 지점에 설치할 수 있습니다. 계층의 모든 업스트림 CA 인증서는 별도의 CA 신뢰 지점에 설치할 수 있습니다.

- Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) >로 이동하고 CA Certificates(CA 인증서)를 선택합니다. Add(추가)를 클릭합니다.

Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No

Buttons: Add, Edit, Show Details, Request CRL, Delete

- Trustpoint 이름을 입력하고 Install From File(파일에서 설치)을 선택하고 Browse(찾아보기) 버튼을 클릭한 다음 중간 인증서를 선택합니다. 또는 텍스트 파일의 PEM 인코딩 CA 인증서를 텍스트 필드에 붙여넣습니다.

Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes

Install Certificate dialog box:

Trustpoint Name: SSL-Trustpoint-2023

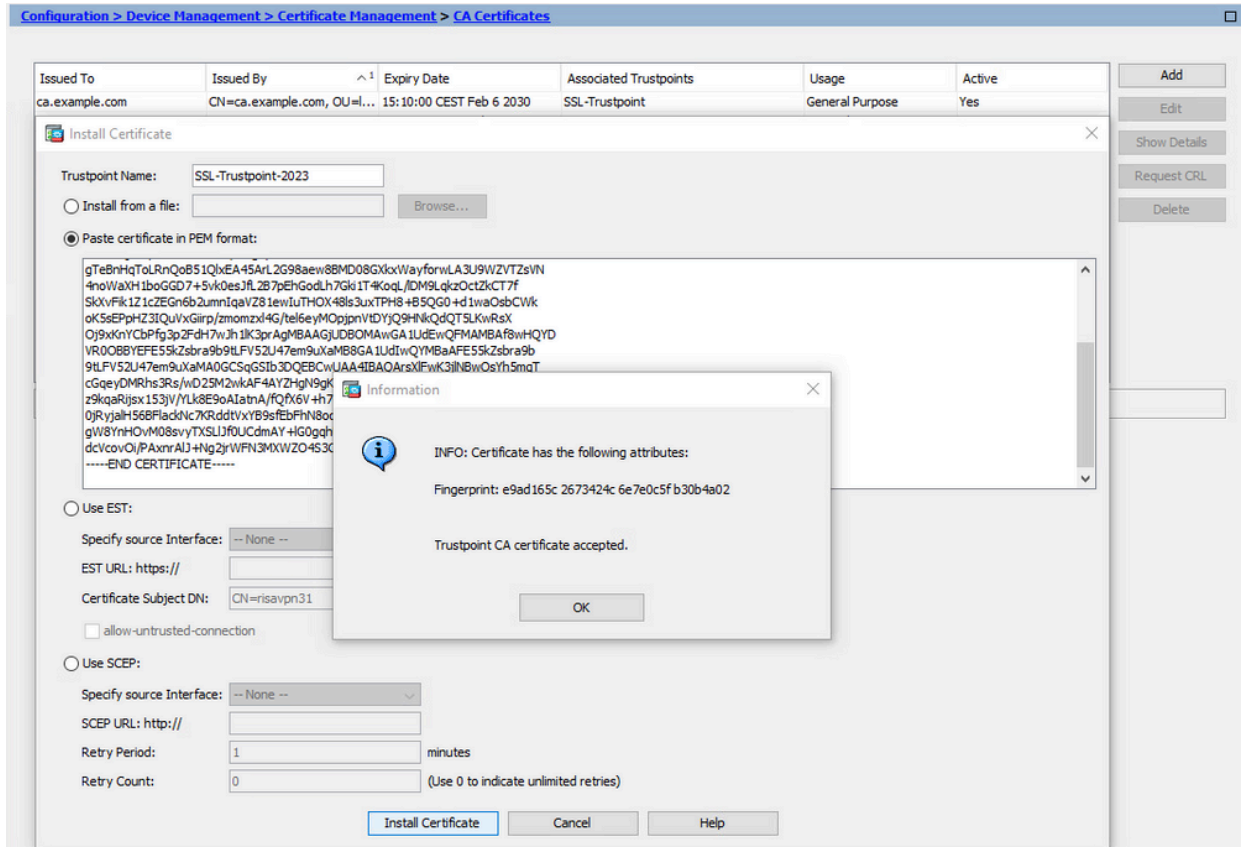
Install from a file:  Browse...

Paste certificate in PEM format:

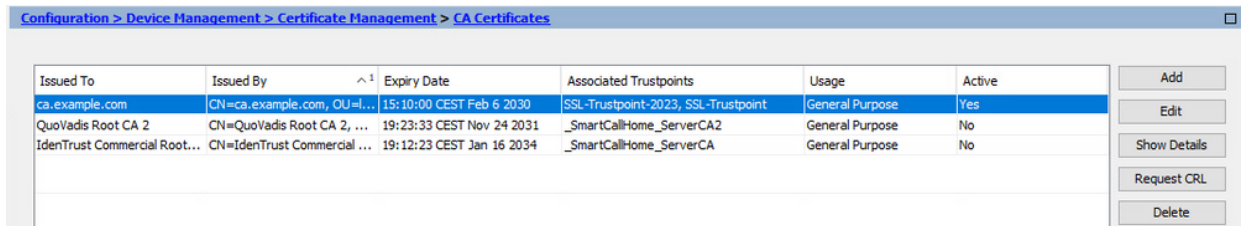
Buttons: Add, Edit, Show Details, Request CRL, Delete

참고: ID 인증서가 중간 CA 인증서로 서명된 경우 ID 인증서 신뢰 지점 이름과 동일한 신뢰 지점 이름으로 중간 인증서를 설치합니다.

- Install Certificate를 클릭합니다.

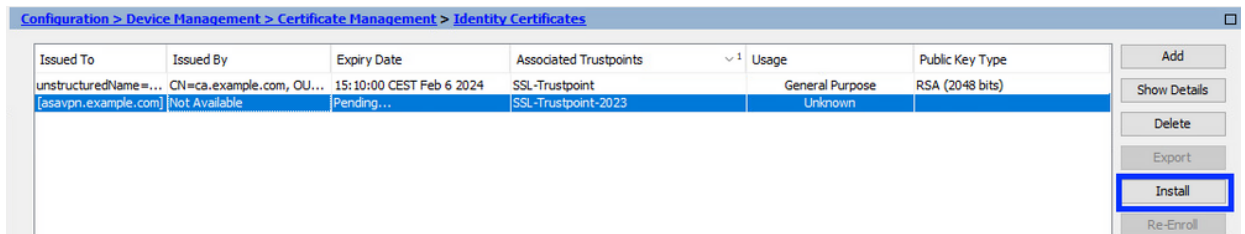


이 예에서 새 인증서는 이전 인증서와 동일한 CA 인증서로 서명됩니다. 동일한 CA 인증서가 이제 두 개의 신뢰 지점과 연결됩니다.



## 2. ID 인증서 설치

a. CSR 생성으로 이전에 생성한 ID 인증서를 선택합니다. Install(설치)을 클릭합니다.

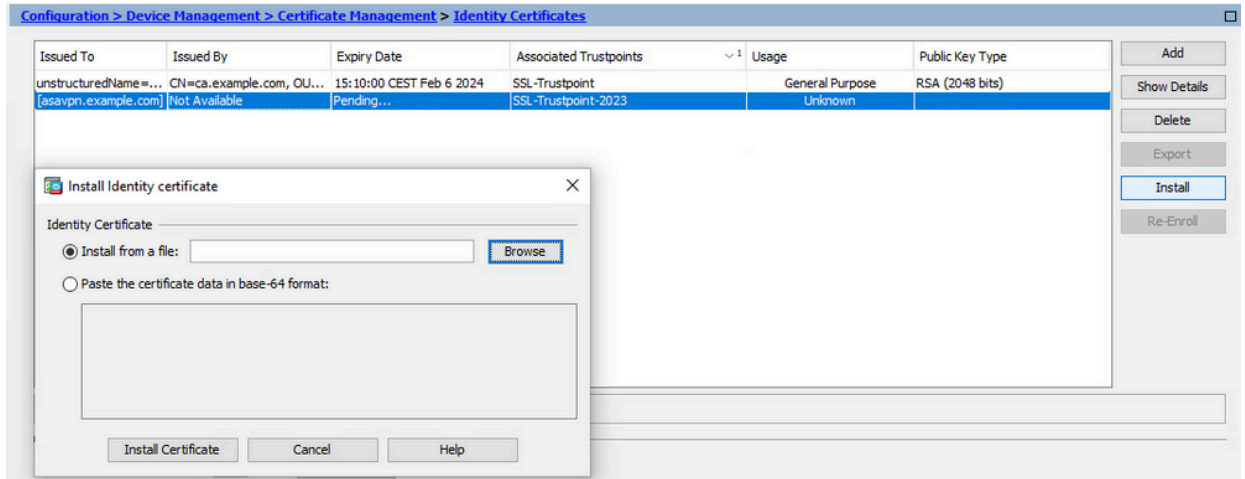


참고: Identity Certificate(ID 인증서)에는 Issued By(발급자) 필드를 Not available(사용 불가)으로 지정하고 Expiry Date(만료일) 필드를 Pending(보류 중)으로 지정할 수 있습니다.

b. CA에서 받은 PEM 인코딩 ID 인증서가 포함된 파일을 선택하거나 텍스트 편집기에서 PEM 인코딩 인증서를 열고 CA에서 제공한 ID 인증서를 복사하여 텍스트 필드에 붙여

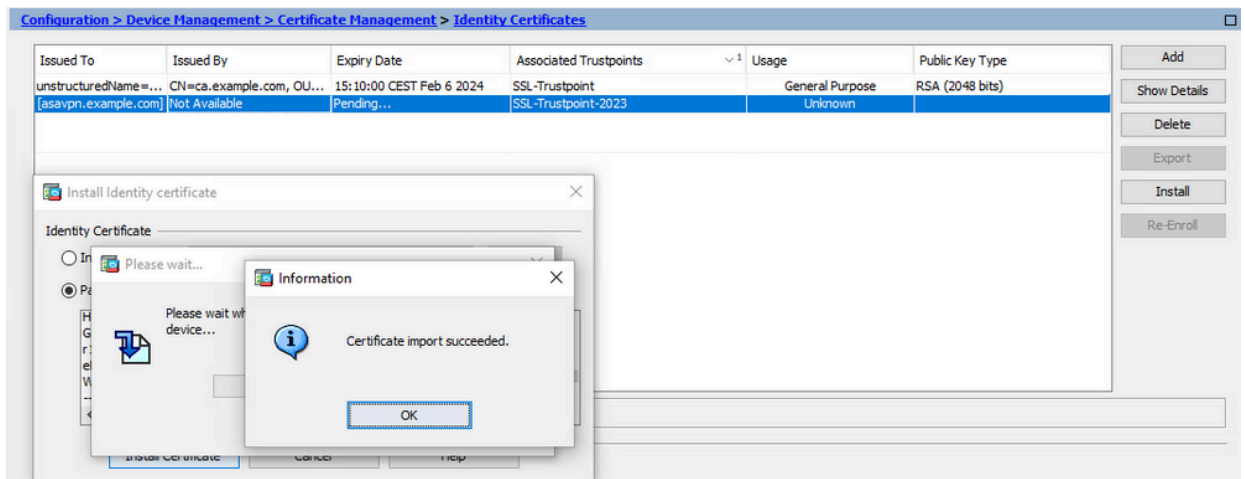


넣습니다.

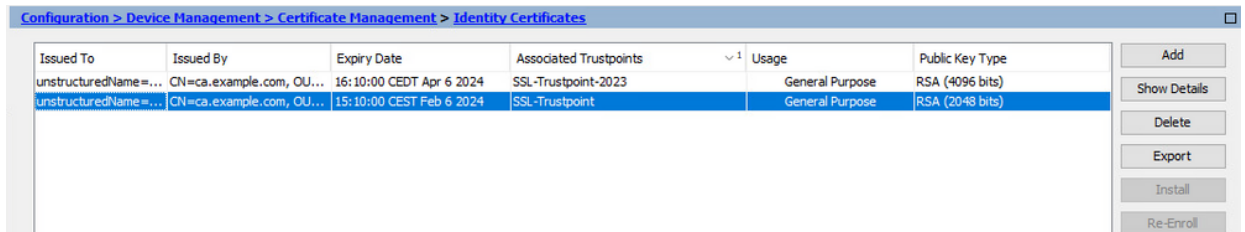


참고: ID 인증서는 설치할 .pem, .cer, .crt 형식일 수 있습니다.

c. Install Certificate를 클릭합니다.



설치 후 이전 및 새 ID 인증서가 있습니다.



3. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

a. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.

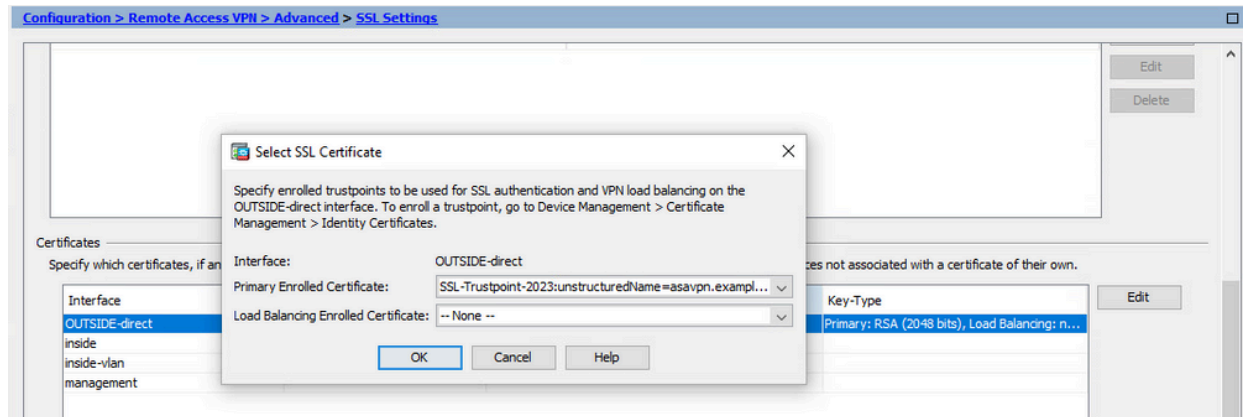
b. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합



니다. 이 예에서는 외부 인터페이스가 사용됩니다.

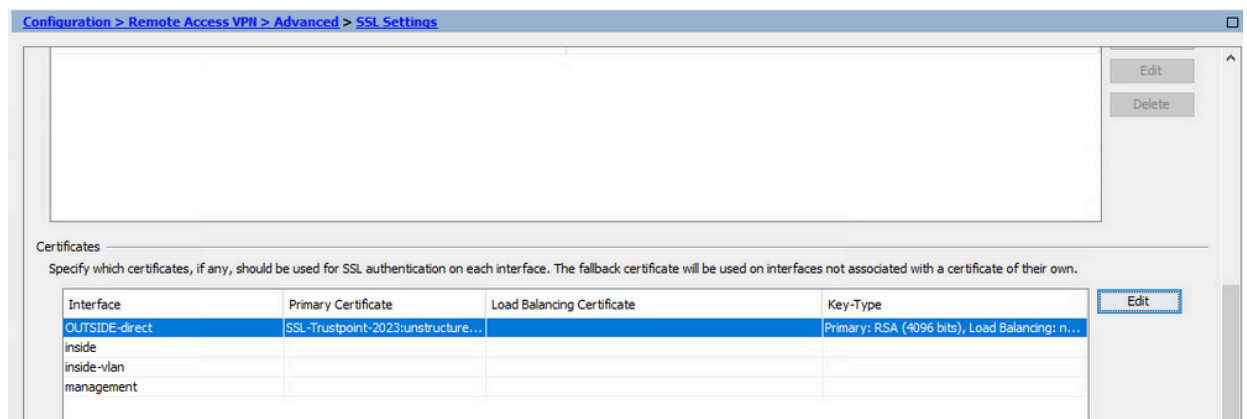
Edit를 클릭합니다.

c. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.



d. OK(확인)를 클릭합니다.

e. 적용을 클릭합니다. 이제 새 ID 인증서가 사용 중입니다.



## ASDM을 사용하여 PKCS12 파일에 등록된 인증서 갱신

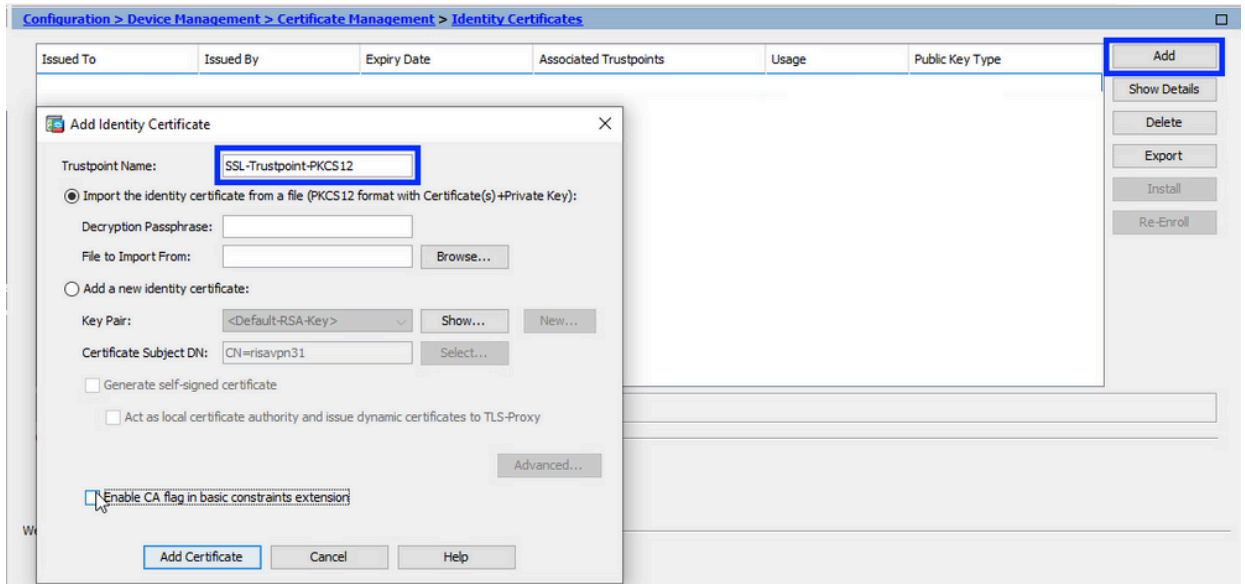
등록된 PKCS12 인증서의 인증서 갱신 시 새 신뢰 지점을 생성하고 등록해야 합니다. 다른 이름(예: 등록 연도 접미사가 있는 이전 이름)이 있어야 합니다.

PKCS12 파일(.p12 또는 .pfx 형식)에는 ID 인증서, 키 쌍 및 CA 인증서가 포함되어 있습니다. 예를 들어 와일드카드 인증서의 경우 CA가 생성하거나 다른 디바이스에서 내보냅니다. 이전 파일이며 텍스트 편집기로 볼 수 없습니다.

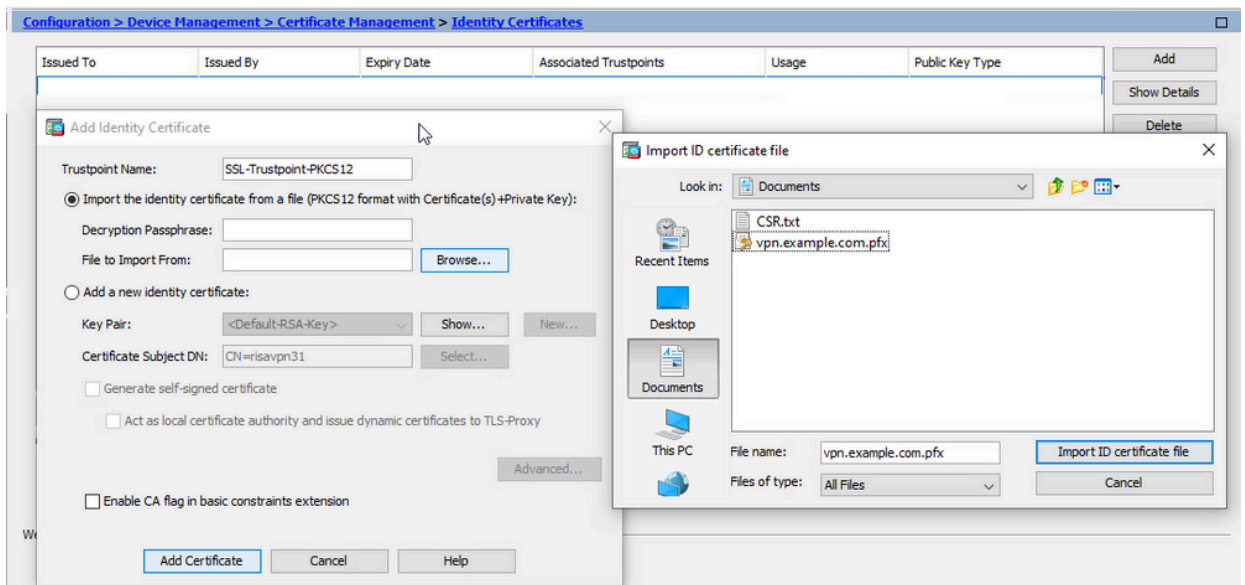
### 1. PKCS12 파일에서 갱신된 ID 인증서 및 CA 인증서 설치

ID 인증서, CA 인증서 및 키 쌍은 단일 PKCS12 파일에 번들로 묶어야 합니다.

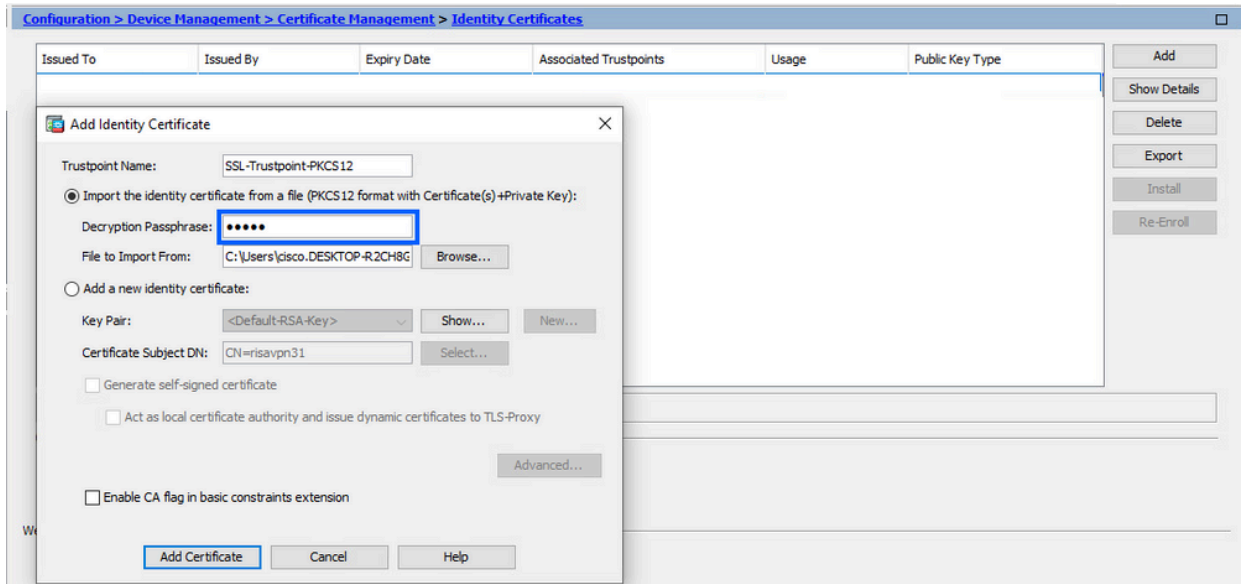
- Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리)로 이동하고 Identity Certificates(ID 인증서)를 선택합니다.
- Add(추가)를 클릭합니다.
- 새 신뢰 지점 이름을 지정합니다.



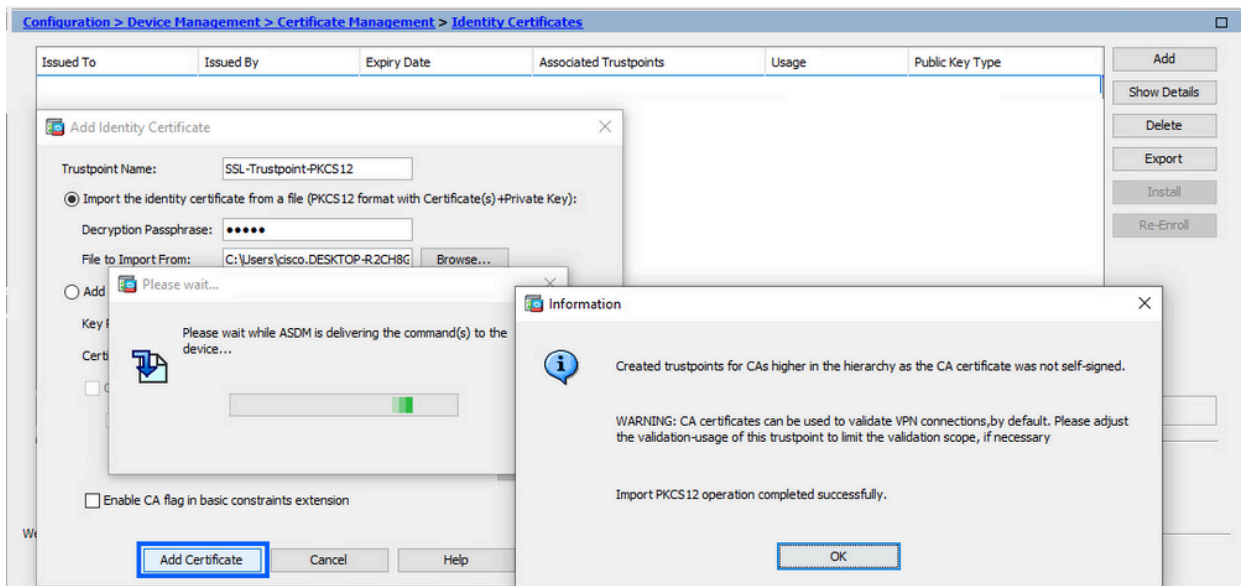
d. Import The Identity Certificate from a File(파일에서 ID 인증서 가져오기) 라디오 버튼을 클릭합니다.



e. PKCS12 파일을 생성하는 데 사용되는 패스프레이즈를 입력합니다.



f. Add Certificate를 클릭합니다.



참고: CA 인증서 체인이 있는 PKCS12를 가져오면 ASDM은 -number 접미사가 추가된 이름과 함께 업스트림 CA 신뢰 지점을 자동으로 생성합니다.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub 1-1	CN=KrakowCA-sub 1	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12	Signature	Yes
KrakowCA-sub 1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-2	Signature	Yes

## 2. 새 인증서를 ASDM을 통해 인터페이스에 바인딩

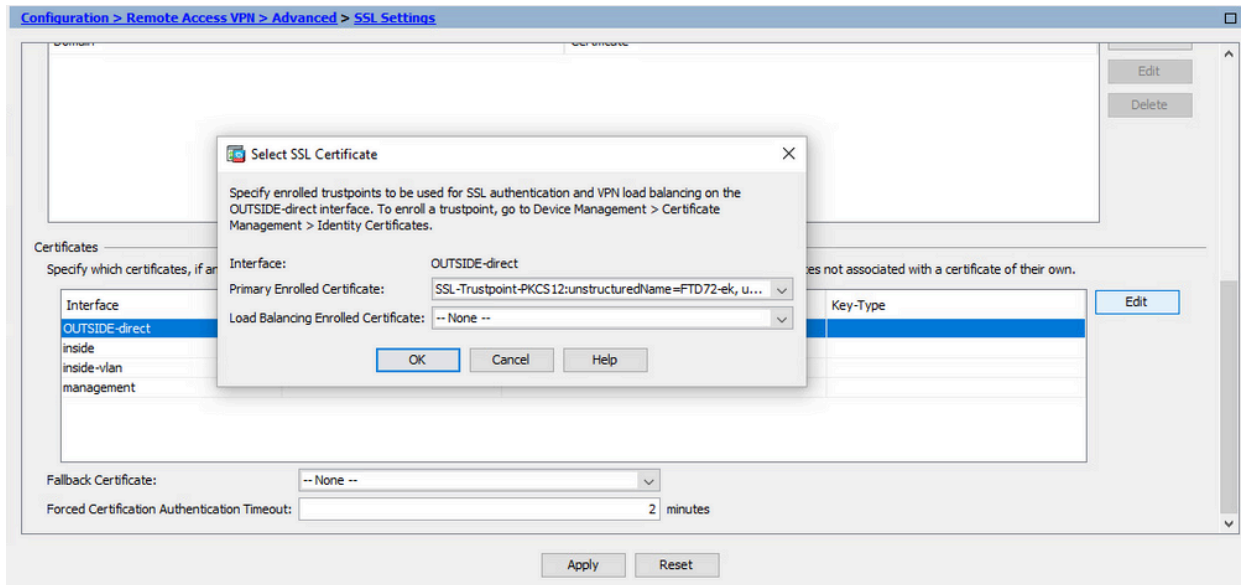
지정된 인터페이스에서 종료되는 WebVPN 세션에 대해 새 ID 인증서를 사용하도록 ASA를 구성해야 합니다.

a. Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Advanced(고급) > SSL Settings(SSL 설정)로 이동합니다.

b. Certificates(인증서)에서 WebVPN 세션을 종료하는 데 사용되는 인터페이스를 선택합니다. 이 예에서는 외부 인터페이스가 사용됩니다.

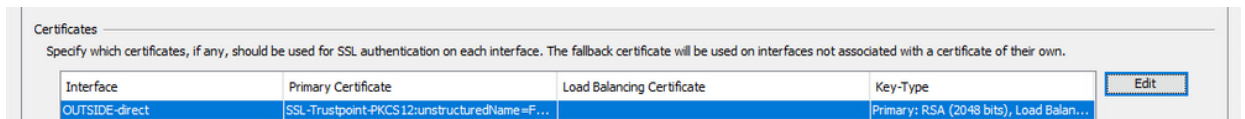
Edit를 클릭합니다.

c. Certificate(인증서) 드롭다운 목록에서 새로 설치된 인증서를 선택합니다.



d. OK(확인)를 클릭합니다.

e. 적용을 클릭합니다.



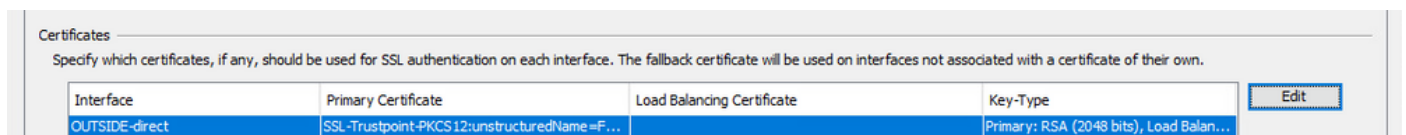
이제 새 ID 인증서가 사용 중입니다.

## 다음을 확인합니다.

타사 공급업체 인증서의 성공적인 설치를 확인하고 SSL VPN 연결에 을 사용하려면 다음 단계를 수행합니다.

## ASDM을 통해 설치된 인증서 보기

1. Configuration(컨피그레이션) > Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리)로 이동하고 Identity Certificates(ID 인증서)를 선택합니다.
2. 서드파티 벤더에서 발급한 ID 인증서가 나타날 수 있습니다.



## 문제 해결

이 debug 명령은 SSL 인증서 설치 실패 시 CLI에서 수집됩니다.

- debug crypto ca 14

## 자주 묻는 질문(FAQ)

Q. PKCS12란 무엇입니까?

A. 암호학에서 PKCS12는 많은 암호학 객체를 하나의 파일로 저장하기 위해 만든 아카이브 파일 형식을 정의합니다. 개인 키를 해당 X.509 인증서와 함께 번들로 묶거나 신뢰 체인의 모든 멤버를 번들로 묶는 데 일반적으로 사용됩니다.

Q. CSR이란 무엇입니까?

A. PKI(Public Key Infrastructure) 시스템에서 인증서 서명 요청(CSR 또는 인증 요청)은 디지털 ID 인증서를 신청하기 위해 신청자가 공용 키 인프라의 등록 기관에 보내는 메시지입니다. 일반적으로 인증서를 발급할 수 있는 공개 키, 서명된 인증서를 식별하는 데 사용되는 정보(예: Subject의 도메인 이름) 및 무결성 보호(예: 디지털 서명)가 포함됩니다.

Q. PKCS12의 비밀번호는 어디에 있습니까?

A. 인증서 및 키 쌍을 PKCS12 파일로 내보내면 비밀번호가 export 명령에 지정됩니다. pkcs12 파일을 가져오려면 CA 서버의 소유자 또는 다른 디바이스에서 PKCS12를 내보낸 사람이 비밀번호를 전달해야 합니다.

Q. 루트와 ID의 차이점은 무엇입니까?

A. 암호화 및 컴퓨터 보안에서 루트 인증서는 루트 CA(Certificate Authority)를 식별하는 공개 키 인증서입니다. 루트 인증서는 자체 서명되며(교차 서명된 루트에서 발급한 인증서인지 여부 등) 인증서에 여러 신뢰 경로가 있을 수 있음) X.509 기반 PKI(공개 키 인프라)의 기반을 형성합니다. 공개 키 인증서(디지털 인증서 또는 ID 인증서라고도 함)는 공개 키의 소유권을 증명하는 데 사용되는 전자 문서입니다. 인증서에는 키에 대한 정보, 소유자(주체라고 함)의 ID에 대한 정보, 인증서의 내용을 확인한 엔티티(발급자라고 함)의 디지털 서명이 포함됩니다. 서명이 유효하고 인증서를 검사하는 소프트웨어가 발급자를 신뢰하는 경우 해당 키를 사용하여 인증서의 주체와 안전하게 통신할 수 있습니다.

Q. 인증서를 설치했는데 왜 작동하지 않습니까?

A. 다음과 같은 여러 가지 이유로 인해 발생할 수 있습니다.

1. 인증서 및 신뢰 지점이 구성되었지만 이를 사용해야 하는 프로세스에 바인딩되지 않았습니다. 예를 들어, 사용할 신뢰 지점은 Anyconnect 클라이언트를 종료하는 외부 인터페이스에 바인딩되지 않습니다.
2. PKCS12 파일이 설치되었지만 PKCS12 파일에 없는 중간 CA 인증서로 인해 오류가 발생합니다. 중간 CA 인증서를 신뢰할 수 있지만 루트 CA 인증서를 신뢰할 수 없는 클라이언트는 전체 인증서 체인을 확인하고 서버 ID 인증서를 신뢰할 수 없는 것으로 보고할 수 없습니다.
3. 잘못된 특성으로 채워진 인증서는 설치 실패 또는 클라이언트 측 오류를 일으킬 수 있습니다. 예

를 들어, 특정 특성은 잘못된 형식을 사용하여 인코딩될 수 있습니다. 또 다른 이유는 ID 인증서에 SAN(주체 대체 이름)이 없거나 서버 액세스에 사용되는 도메인 이름이 SAN으로 존재하지 않기 때문입니다.

Q. 새 인증서를 설치하려면 유지 관리 기간이 필요한지, 아니면 다운타임이 발생합니까?

A. 새 인증서(ID 또는 CA)를 설치하는 것은 방해가 되지 않으며 다운타임을 발생시키거나 유지 보수 기간을 필요로 하지 않습니다. 기존 서비스에 새 인증서를 사용하도록 설정하려면 변경 사항이 있으며 변경 요청/유지 관리 기간이 필요할 수 있습니다.

Q. 인증서를 추가하거나 변경하면 연결된 사용자의 연결이 끊길 수 있습니까?

A. 아니요. 현재 연결된 사용자는 계속 연결되어 있습니다. 인증서는 연결 설정 시 사용됩니다. 사용자가 다시 연결하면 새 인증서가 사용됩니다.

Q: 와일드카드로 CSR을 생성하려면 어떻게 해야 합니까? 또는 SAN(Subject Alternative Name)입니까?

A. 현재 ASA/FTD는 와일드카드로 CSR을 생성할 수 없습니다. 그러나 이 프로세스는 OpenSSL을 사용하여 수행할 수 있습니다. CSR 및 ID 키를 생성하려면 다음 명령을 실행할 수 있습니다.

```
openssl genrsa -out id.key 2048
```

```
openssl req -out id.csr -key id.key -new
```

신뢰 지점이 FQDN(Fully Qualified Domain Name) 특성으로 구성된 경우 ASA/FTD에서 생성한 CSR에 해당 값의 SAN이 포함됩니다. CSR에 서명할 때 CA가 더 많은 SAN 특성을 추가하거나 OpenSSL을 사용하여 CSR을 생성할 수 있습니다

Q. 인증서 교체는 즉시 적용됩니까?

A. 새 서버 ID 인증서는 새 연결에 대해서만 사용됩니다. 새 인증서는 변경 직후 사용할 준비가 되었지만 실제로 새 연결에서 사용됩니다.

Q. 설치가 제대로 되었는지 확인하려면 어떻게 해야 합니까?

A. 확인할 CLI 명령: `show crypto ca cert <trustpointname>`

Q. ID 인증서, CA 인증서 및 개인 키에서 PKCS12를 생성하는 방법은 무엇입니까?

A. PKCS12는 OpenSSL을 사용하여 다음 명령을 사용하여 생성할 수 있습니다.

```
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt
```

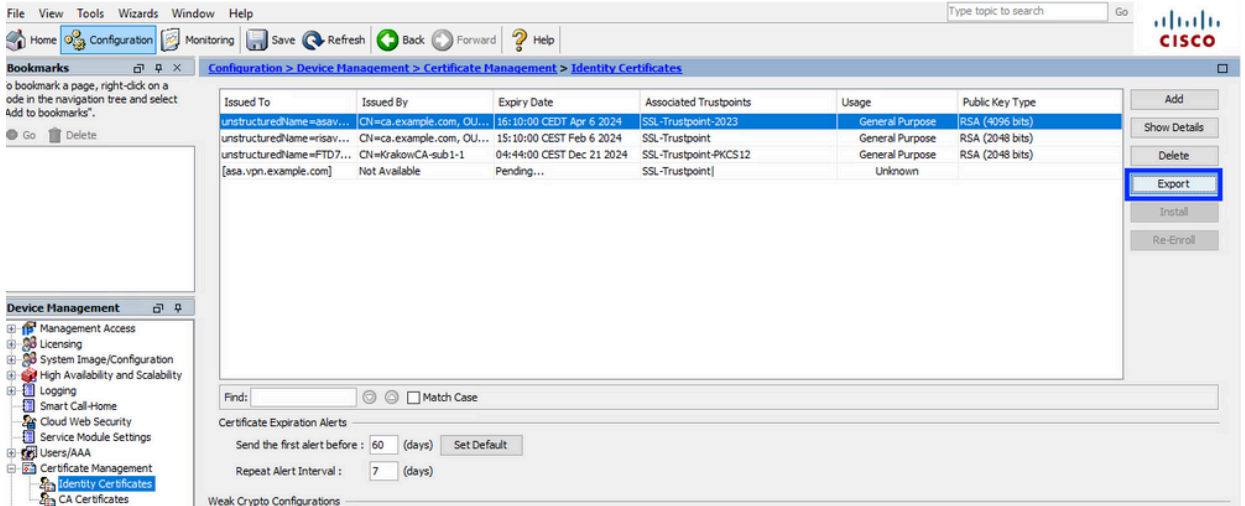
Q. 새 ASA에 설치하기 위해 인증서를 내보내는 방법은 무엇입니까?

A.

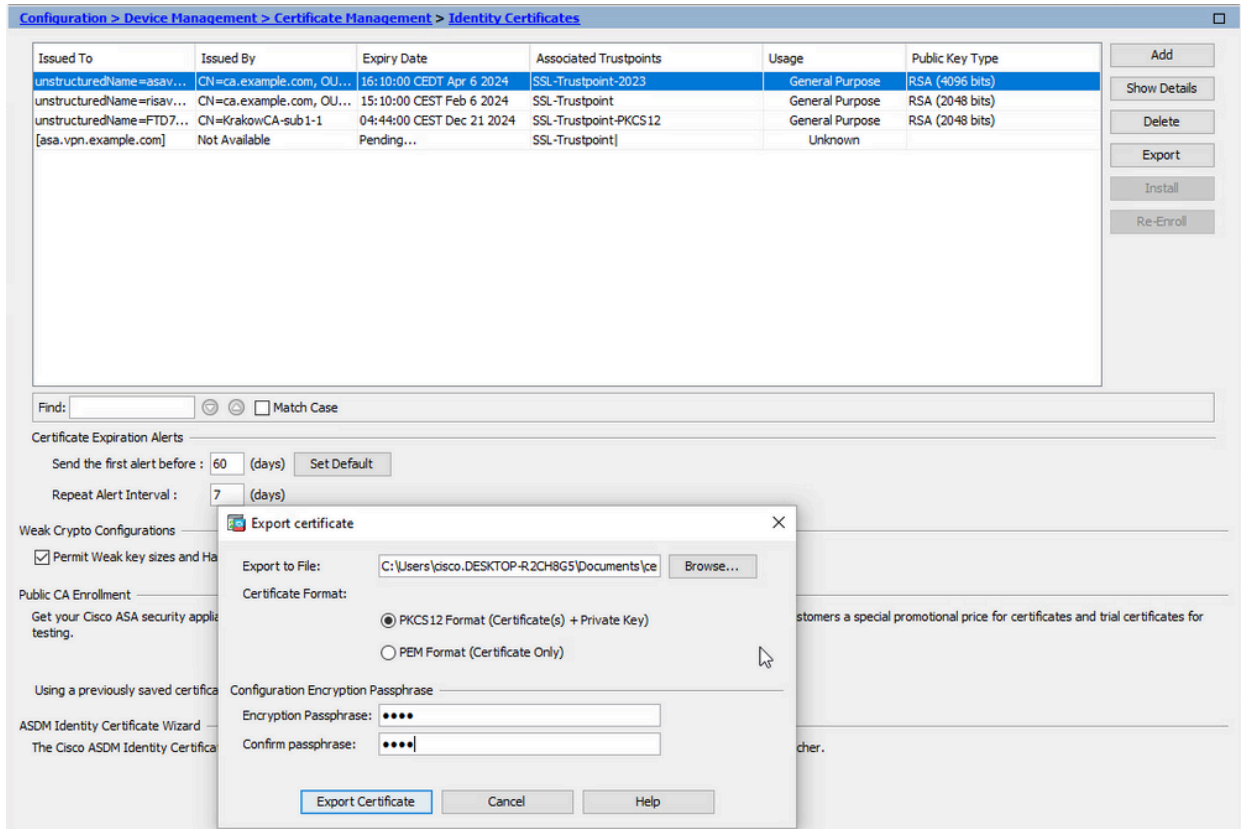
- CLI에서: `crypto ca export <trustpointname> pkcs12 <password>` 명령을 사용합니다.

- ASDM의 경우:

- a. Configuration(컨피그레이션) > Device Management(디바이스 관리) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동하고 Identity Certificate(ID 인증서)를 선택합니다. Export(내보내기)를 클릭합니다.



b. 파일을 내보낼 위치를 선택하고 내보내기 비밀번호를 지정한 다음 Export Certificate(인증서 내보내기)를 클릭합니다.



내보낸 인증서는 컴퓨터 디스크에 있을 수 있습니다. 안전한 곳에 암호를 적어 두십시오. 파일이 없으면 무용지물입니다.

Q. ECDSA 키를 사용하는 경우 SSL 인증서 생성 프로세스가 다른가요?

A. 컨피그레이션의 유일한 차이점은 키 쌍 생성 단계로, 여기서 RSA 키 쌍 대신 ECDSA 키 쌍을 생성할 수 있습니다. 나머지 단계는 동일하게 유지됩니다.

Q. 항상 새 키 쌍을 생성해야 합니까?

A. 키 쌍 생성 단계는 선택 사항입니다. 기존 키 쌍을 사용할 수 있습니다. 또는 PKCS12의 경우 키

쌍을 인증서와 함께 가져옵니다. 해당 등록/재등록 유형에 대한 키 쌍 이름 선택 섹션을 참조하십시오.

Q. 새 ID 인증서에 대한 새 키 쌍을 생성해도 안전합니까?

A. 새 키 쌍 이름을 사용하는 한 프로세스는 안전합니다. 이 경우 이전 키 쌍은 변경되지 않습니다.

Q. 방화벽을 교체할 때(예: RMA) 키를 다시 생성해야 합니까?

A. 새로운 방화벽은 설계상 기존 방화벽에 키 쌍이 없습니다.

실행 중인 컨피그레이션의 백업에는 키 쌍이 포함되어 있지 않습니다.

ASDM을 사용하여 수행한 전체 백업에는 키 쌍이 포함될 수 있습니다.

ASA에서 ASDM 또는 CLI를 사용하여 ID 인증서를 내보냈다가 실패할 수 있습니다.

장애 조치 쌍의 경우 인증서 및 키 쌍은 write standby 명령을 사용하여 스탠바이 유닛에 동기화됩니다. 장애 조치 쌍의 노드 하나를 교체하는 경우 기본 장애 조치를 구성하고 새 디바이스에 컨피그레이션을 푸시하는 데 충분합니다.

디바이스에서 키 쌍이 손실되고 백업이 없는 경우, 새 디바이스에 키 쌍이 있는 상태에서 새 인증서를 서명해야 합니다.



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.