Secure Endpoint Private Cloud 3.x 이후 설치에 필요한 인증서 생성 및 추가

목차

소개

이 문서에서는 Secure Console Private Cloud를 새로 설치할 때마다 업로드해야 하는 인증서를 생성하거나 설치된 인증서 서비스를 갱신하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows Server 2008

- CentOS 7/8
- Secure Console Virtual Private Cloud 3.0.2(이후)
- OpenSSL 1.1.1

사용되는 구성 요소

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Windows Server 2008(이후)
- Secure Console Private Cloud 설치
- 공개 키 인프라
- OpenSSL
- Linux CLI

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

Secure Console Private Cloud 3.X가 도입됨에 따라 다음 모든 서비스에 호스트 이름, 인증서/키 쌍이 필요합니다.

- 관리 포털
- 인증(Private Cloud 3.X의 새로운 기능)
- 보안 콘솔
- 서버 분류
- Disposition Server - 확장 프로토콜
- 속성 업데이트 서비스
- Firepower Management Center

이 문서에서는 필요한 인증서를 빠르게 생성하고 업로드하는 방법에 대해 설명합니다. 조직의 정책에 따라 해싱 알고리즘, 키 크기 및 기타 매개변수를 비롯한 각 매개변수를 조정할 수 있으며, 이러한 인증서를 생성하는 메커니즘이 여기에서 설명하는 것과 일치하지 않을 수 있습니다.

> **경고**: 아래에 설명된 절차는 CA 서버 컨피그레이션에 따라 달라질 수 있습니다. 선택한 CA 서버가 이미 프로비전되어 있고 동일한 CA 서버의 컨피그레이션이 완료된 것으로 예상됩니다. 다음 기술에서는 인증서를 생성하는 예만 설명하며, Cisco TAC는 인증서 생성 및/또는 CA 서버 문제와 관련된 문제를 해결하는 데 관여하지 않습니다.

인증서 생성

Window 서버에서 인증서 생성

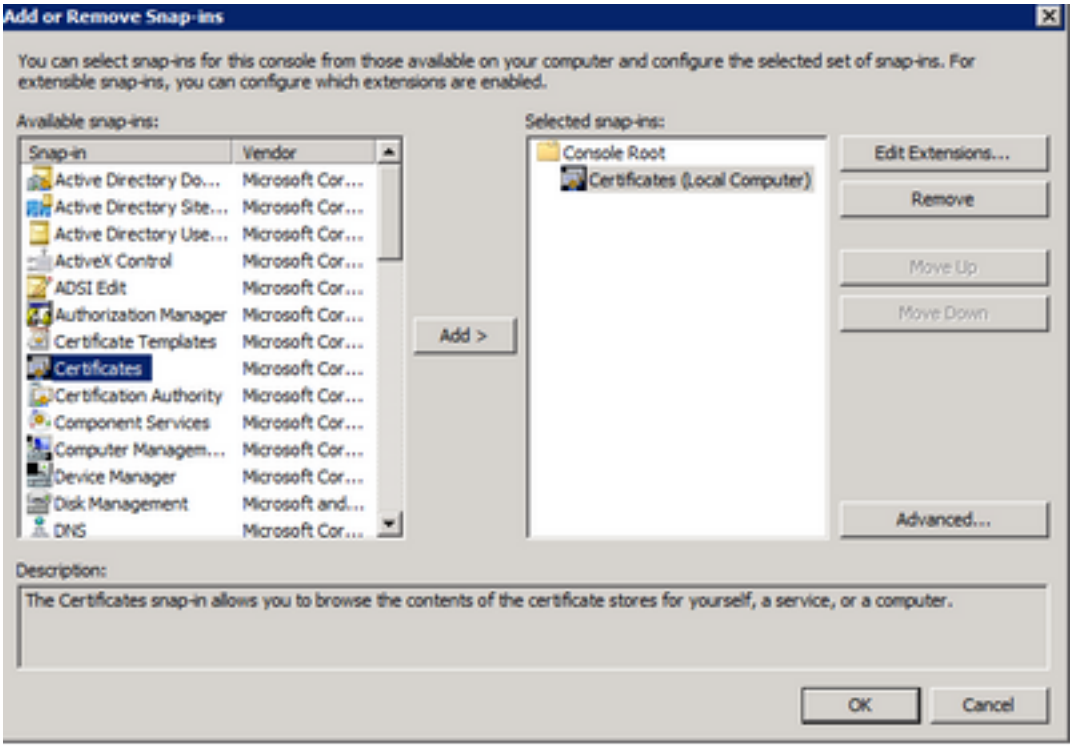
Windows Server에 다음 역할이 설치 및 구성되어 있는지 확인합니다.

- Active Directory 인증서 서비스
- 인증 기관
- 인증 기관 웹 등록

- 온라인 응답기
- 인증서 등록 웹 서비스
- 인증서 등록 정책 웹 서비스
- Active Directory 도메인 서비스
- DNS 서버
- 웹 서버(IIS)

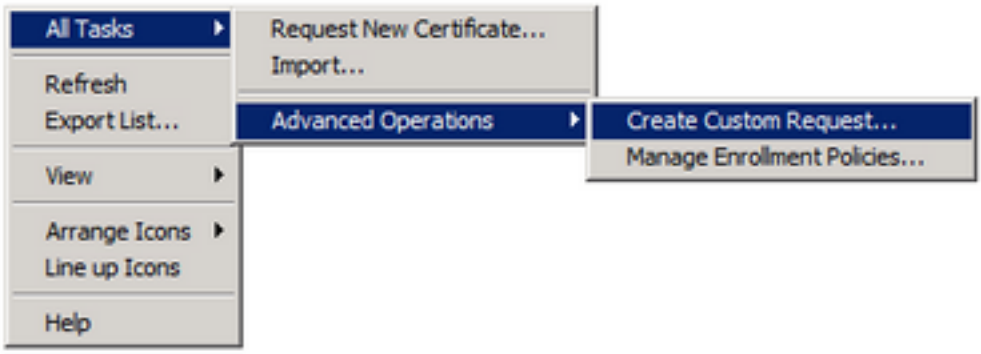
CSR(Certificate Signing Request) 생성

1단계. MMC 콘솔로 이동하여 여기 이미지에 표시된 대로 컴퓨터 계정에 대한 인증서 스냅인을 추가합니다.

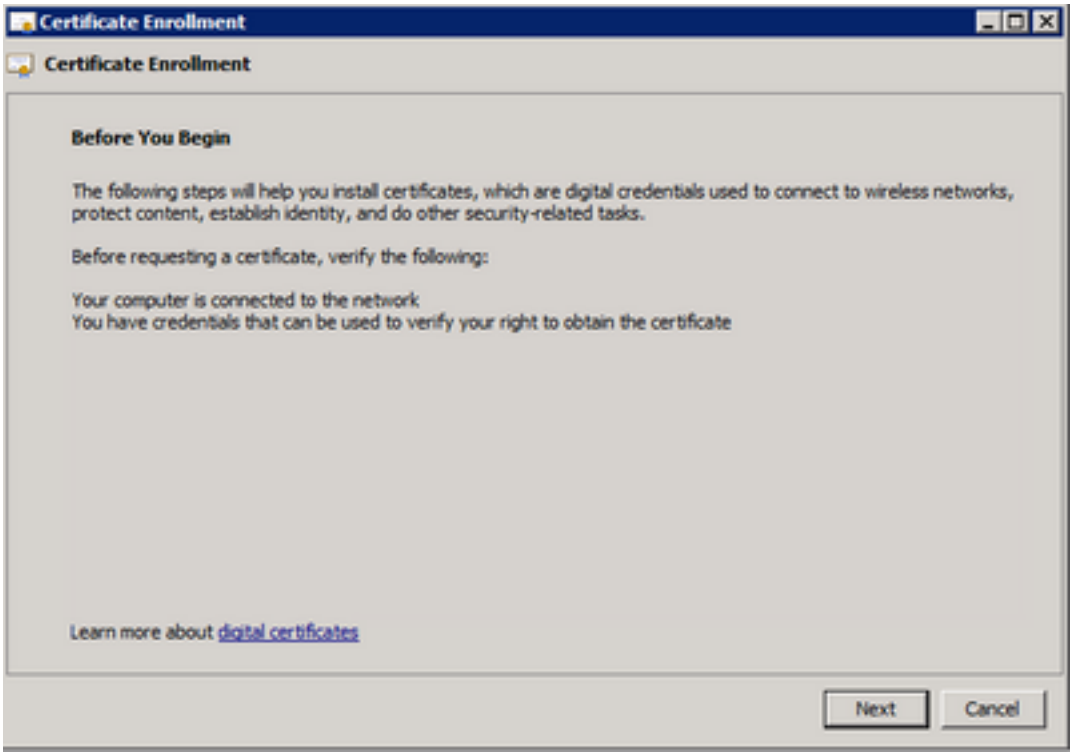


2단계. Certificates(**로컬 컴퓨터) > Personal(개인) > Certificates(인증서)를 드릴다운합니다**.

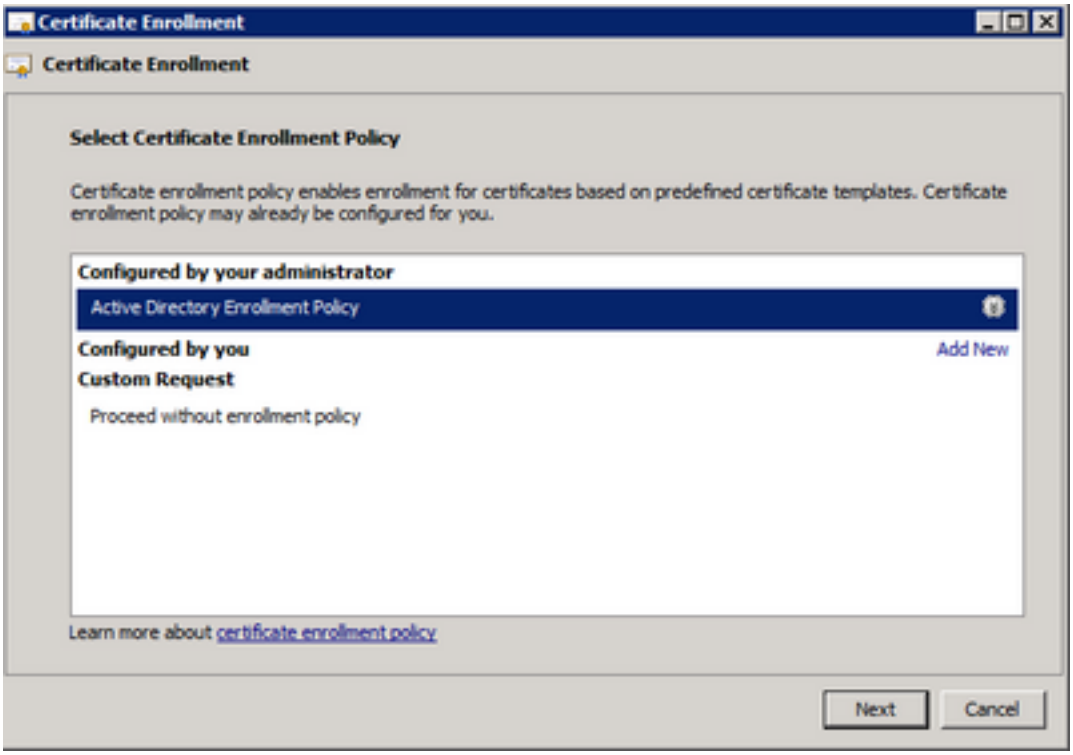
3단계. 빈 공간을 마우스 오른쪽 단추로 클릭하고 **All Tasks(모든 작업) > Advanced Operations(고급 작업) > Create Custom Request(맞춤형 요청 생성)를** 선택합니다.



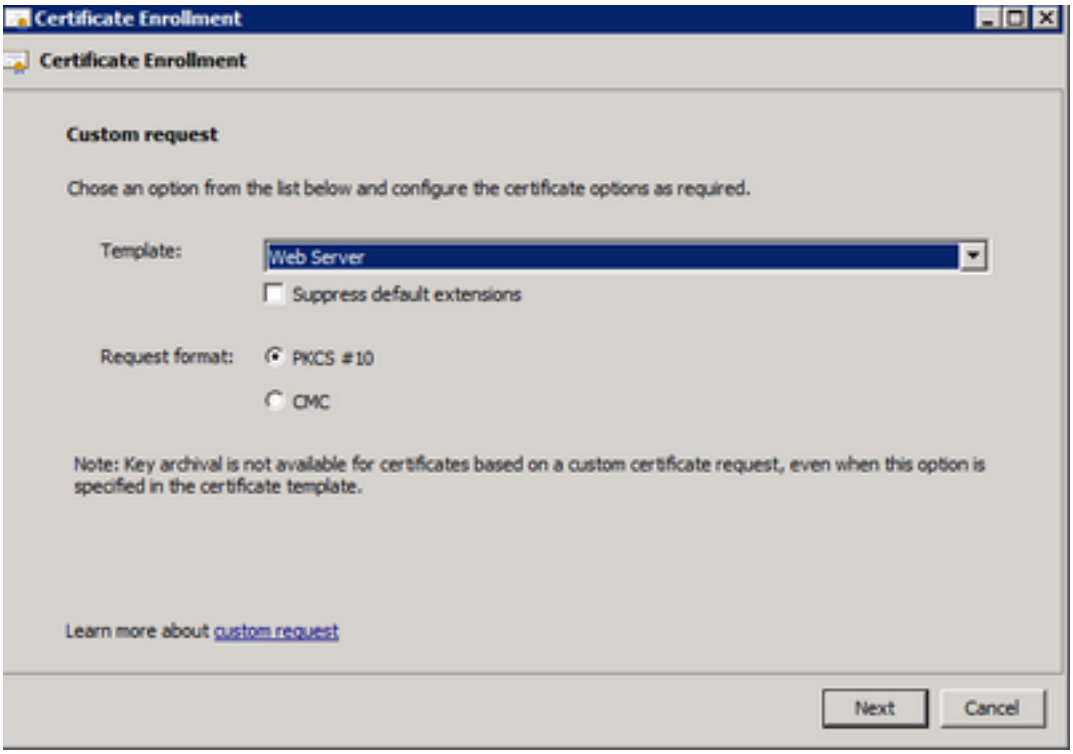
4단계. 등록 **창**에서 다음을 선택합니다.



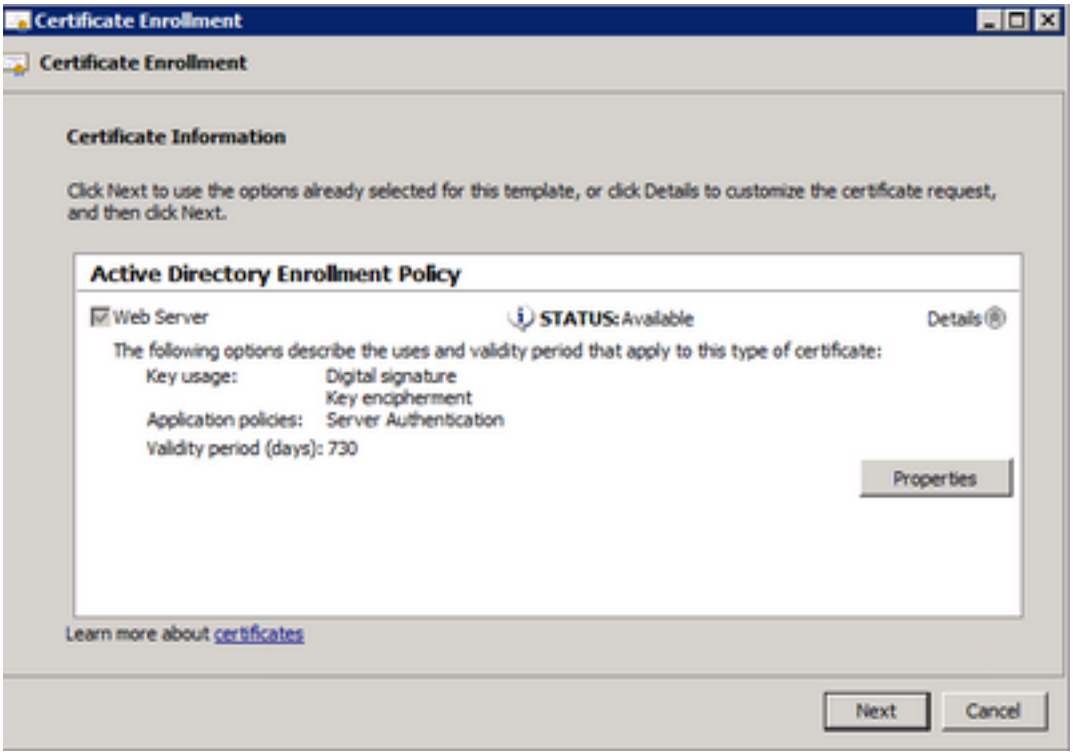
5단계. 인증서 등록 정책을 선택하고 다음을 **선택합니다**.



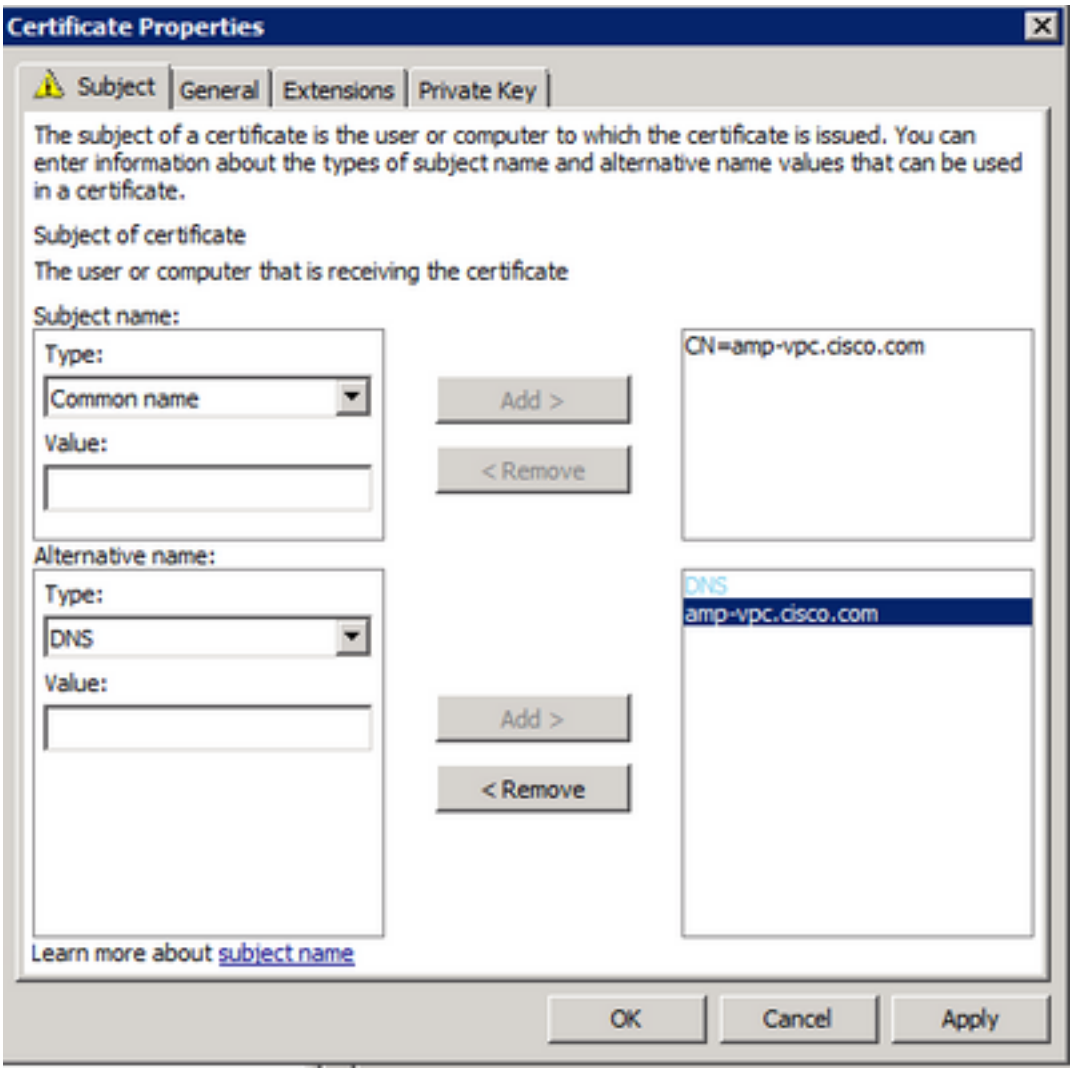
6단계. 템플릿을 **웹** 서버로 **선택하고 Next(다음)**를 선택합니다.



7단계. "웹 서버" 템플릿이 올바르게 구성되어 있고 등록에 사용할 수 있는 경우, "사용 가능" 상태가 표시됩니다. Details(**세부사항)**를 선택하여 Properties(속성)를 확장합니다.

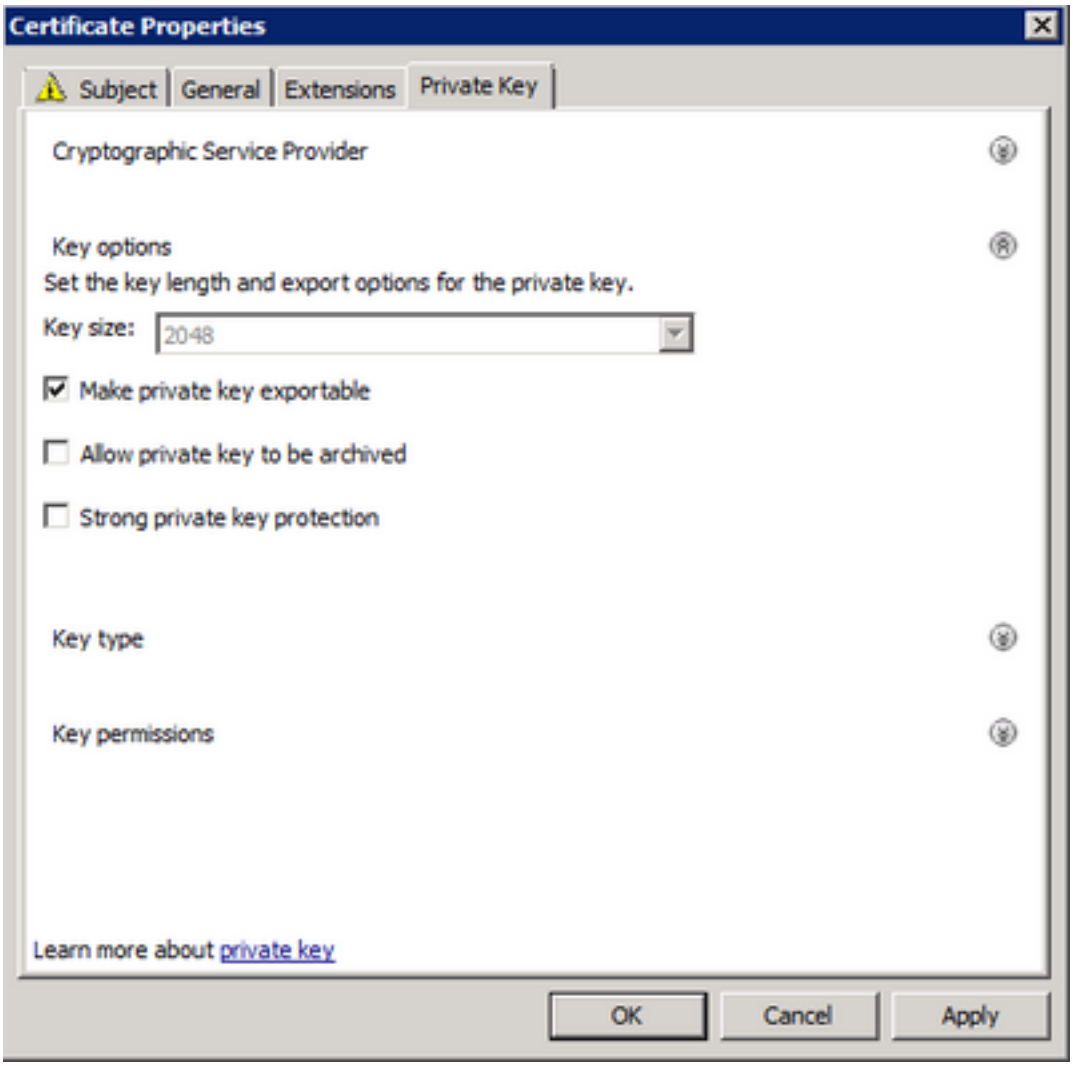


8단계. 최소한 CN 및 DNS 특성을 추가합니다. 나머지 특성은 보안 요구 사항에 따라 추가할 수 있습니다.



9단계. 선택적으로, **General(일반)** 탭 아래에 Friendly Name(친숙한 이름)을 입력합니다.

10단계. **Private Key(개인 키)** 탭에서 을 선택하고 **Key Options(키 옵션) 섹션**에서 Make private key exportable(개인 키를 내보낼 수 있게 함)을 활성화합니다.

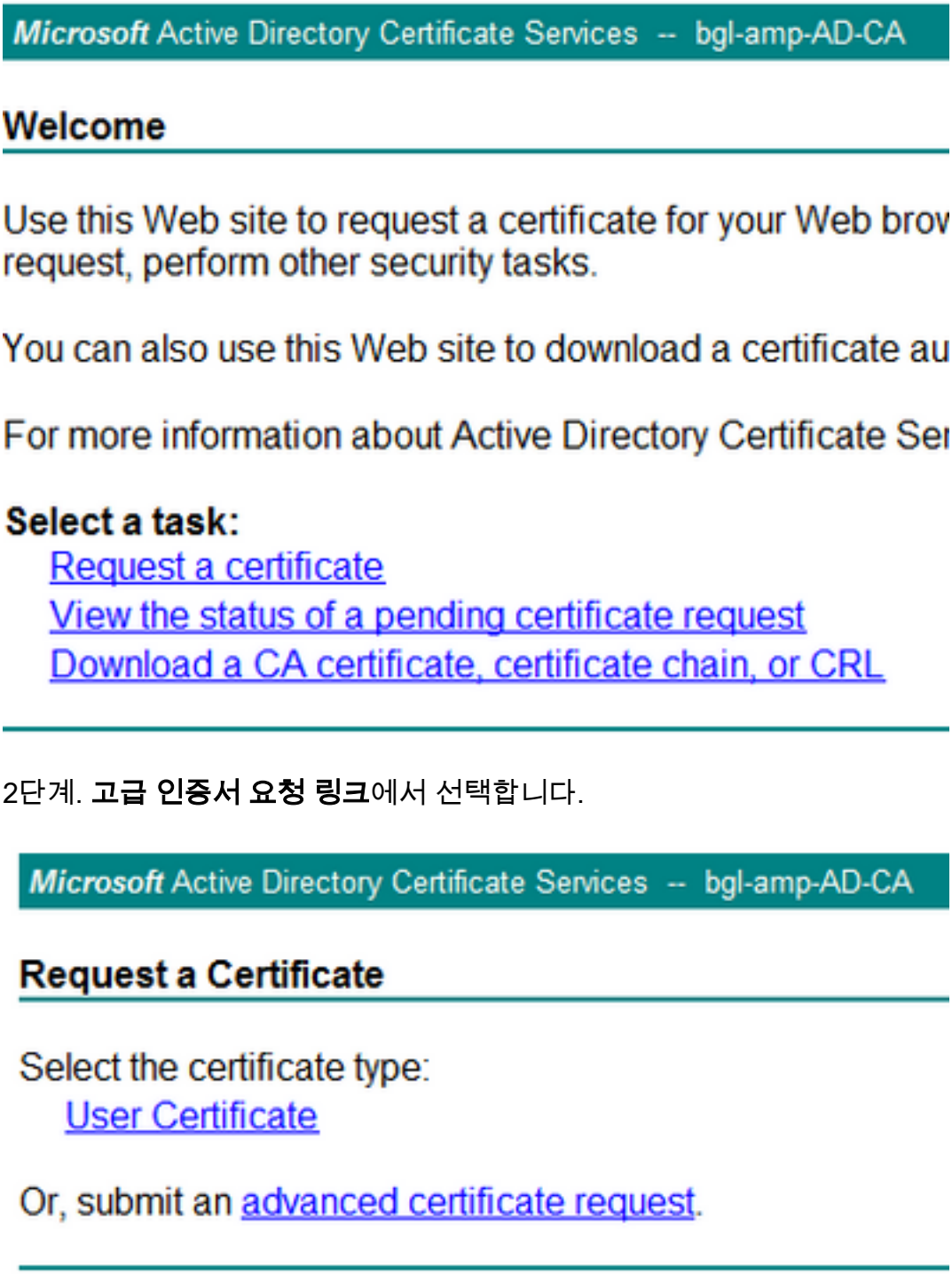


11단계. 마지막으로 **OK**(확인)를 **선택합니다**. 그러면 다음을 선택할 수 있는 Certificate Enrollment(인증서 등록) 대화 상자로 이동해야 **합니다**.

12단계. 서명을 위해 CA 서버에 제출된 .req 파일을 저장할 위치를 찾습니다.

CSR을 CA에 제출하고 인증서 생성

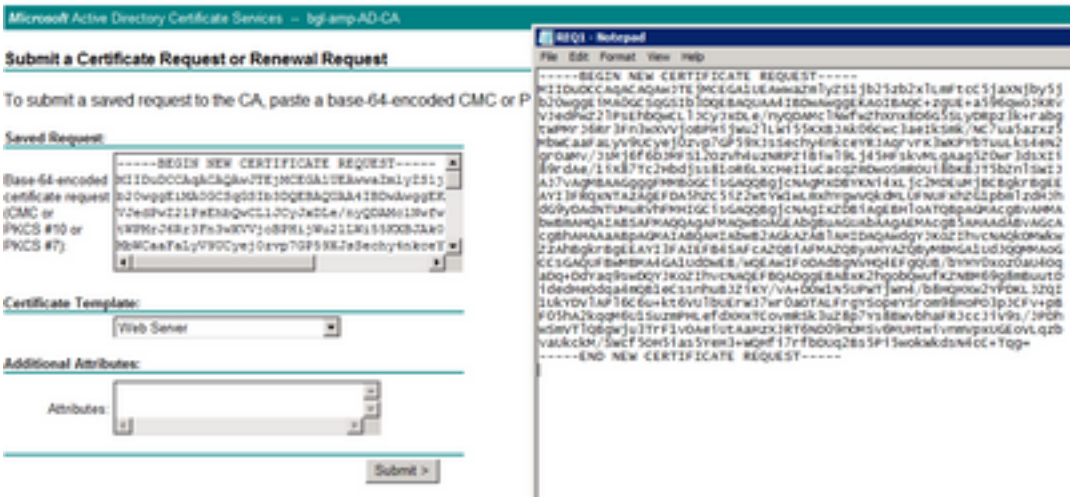
1단계. 아래와 같이 MS AD Certificate Services(MS AD 인증서 서비스) 웹 페이지로 이동하고 Request **a Certificate(인증서 요청)를** 선택합니다.



2단계. **고급 인증서 요청 링크**에서 선택합니다.

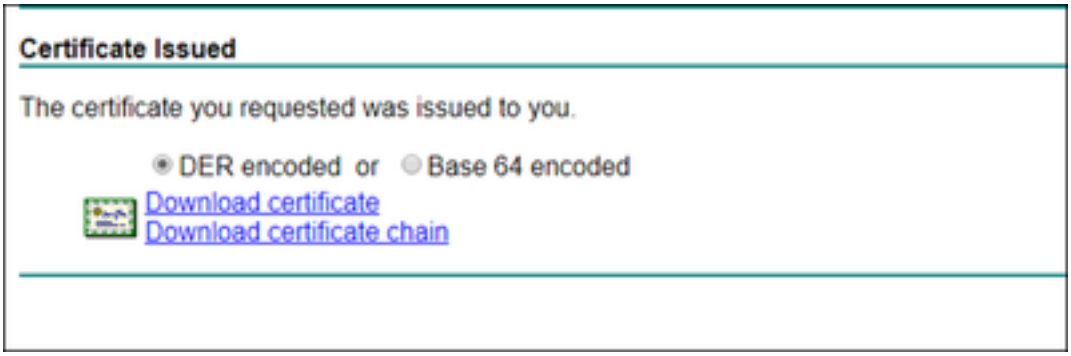
3단계. Submit **a certificate request by using a base-64-encoded CMC or PKCS #10 file(Base-64-encoded CMC 또는 PKCS #7 파일을 사용하여 인증서 요청 제출)을 선택합니다**.

4단계. 메모장을 통해 이전에 저장한 CSR(.req file)의 내용을 엽니다. 내용을 복사해서 여기에 붙여 주세요. 인증서 템플릿이 **웹** 서버로 선택되었는지 **확인합니다**



5단계. 마지막으로 제출을 **선택합니다**.

6단계. 이때 이미지에 표시된 것처럼 **인증서**를 다운로드할 수 있어야 합니다.



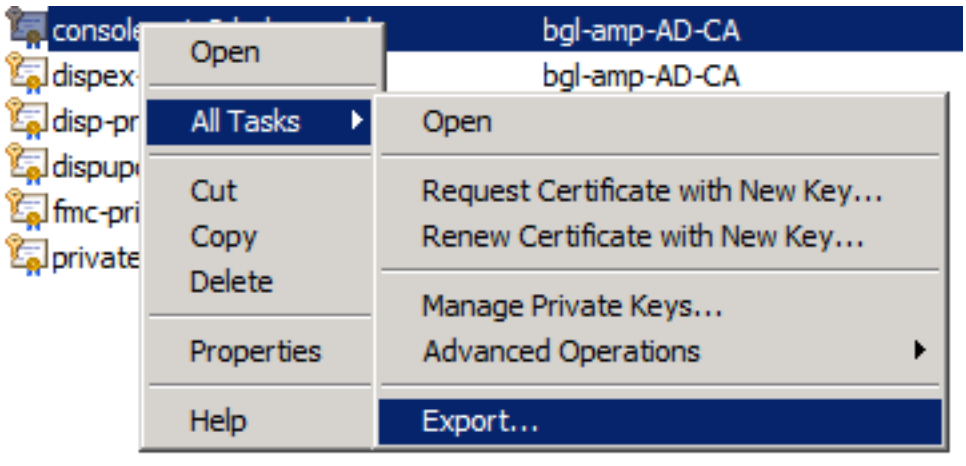
개인 키 내보내기 및 PEM 형식으로 변환

1단계. .cer 파일을 열고 Install Certificate를 선택하여 인증서를 인증서 저장소에 **설치합니다**.

2단계. 이전에 선택한 MMC 스냅인으로 이동합니다.

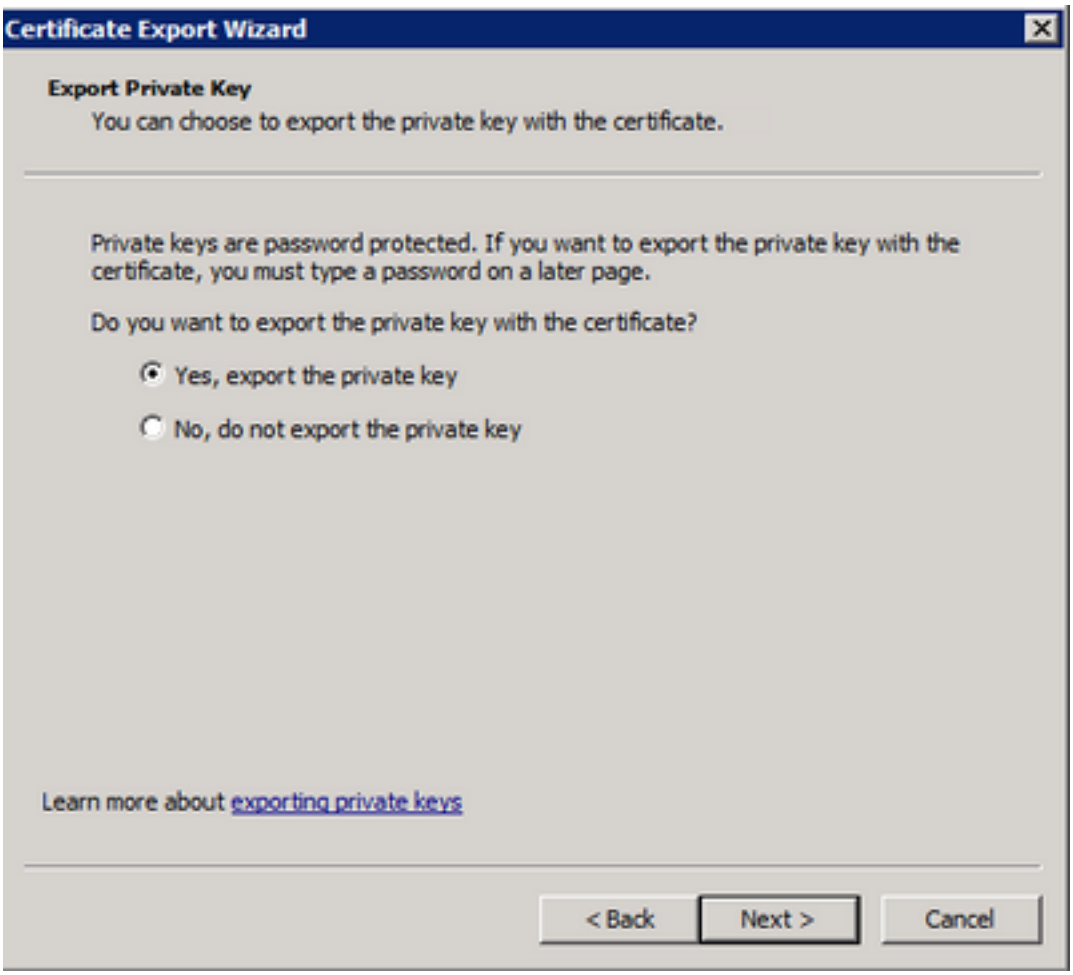
3단계. 인증서가 설치된 저장소로 이동합니다.

4단계. 올바른 인증서를 마우스 오른쪽 단추로 클릭하고 **All Tasks(모든 작업) > Export(내보내기)**를 선택합니다.



5단계. Certificate Export Wizard(인증서 내보내기 마법사)에서 이미지에 표시된 대로 개인 키 내보

내기를 확인합니다.



6단계. 암호를 입력하고 **다음**을 선택하여 개인 키를 디스크에 저장합니다.

7단계. 이렇게 하면 개인 키가 .PFX 형식으로 저장되지만 이 키를 Secure Endpoint Private Cloud와 함께 사용하려면 .PEM 형식으로 변환해야 합니다.

8단계. OpenSSL 라이브러리를 설치합니다.

9단계. 명령 프롬프트 창을 열고 OpenSSL을 설치한 디렉토리로 변경합니다.

10단계. 다음 명령을 실행하여 개인 키를 추출하여 새 파일에 저장합니다. (PFX 파일이 OpenSSL 라이브러리가 저장된 경로와 동일하지 않은 경우 파일 이름과 정확한 경로를 지정해야 합니다.)

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes
```

11단계. 이제 다음 명령을 실행하여 퍼블릭 인증서도 추출하고 새 파일에 저장합니다.

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes
```

Linux 서버에서 인증서 생성(엄격한 SSL 확인 사용 안 함)

> **참고**: 엄격한 TLS 확인에서는 인증서가 Apple의 TLS 요구 사항을 충족하는지 확인합니다. 자세한 내용은 관리 가이드를 참조하십시오.

필요한 인증서를 생성하려는 Linux 서버에 OpenSSL 1.1.1 라이브러리가 설치되어 있는지 확인합니다. 아래 나열된 절차 및 이 절차는 실행 중인 Linux 배포판마다 다를 수 있는지 확인합니다. 이 부분은 CentOS 8.4 Server에서 수행한 것과 같이 문서화되었습니다.

자체 서명 RootCA 생성

1단계. 루트 CA 인증서에 대한 개인 키를 생성합니다.

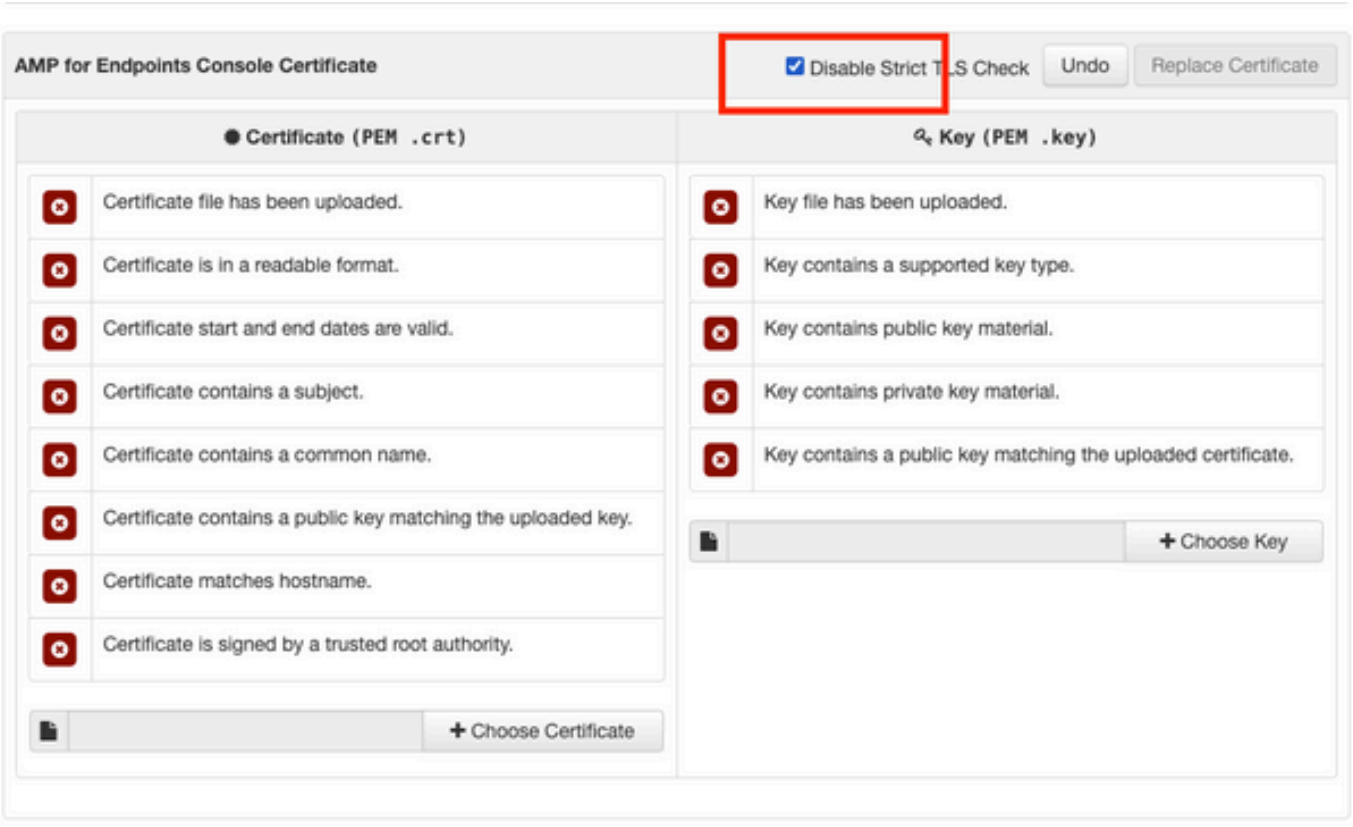
```
openssl genrsa -out
```

2단계. CA 인증서를 생성합니다.

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

각 서비스에 대한 인증서 생성

DNS 이름 항목에 따라 Authentication, Console, Disposition, Disposition-Extended, Update server, FMC(Firepower Management Center) 서비스용 인증서를 생성합니다. 각 서비스(인증, 콘솔 등)에 대해 아래 인증서 생성 프로세스를 반복해야 합니다.



개인 키 생성

```
openssl genrsa -out
```
<YourServiceName.key>를 Auth-Cert.key로 만들 새 KEY 파일 이름으로 바꿉니다.

CSR 생성

```
openssl req -new \
-subj '/CN=
-key
```
교체 Auth-Cert.key와 같은 현재(또는 새) 인증서 KEY 파일이 있는 <YourServiceName.key>

<YourServiceName.csr>을 만들 CSR 파일 이름(예: Auth-Cert.crt)으로 바꿉니다.

인증서 생성

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```
<YourServiceName.csr>을 실제(또는 새) 인증서 CSR(예: Auth-Cert.csr)로 교체합니다.

<YourRootCAName.pem>을 실제(또는 새) PEM 파일 이름으로 RootCAName.pem으로 바꿉니다.

<YourServiceName.key>를 Auth-Cert.key와 같은 현재(또는 새) 인증서 KEY 파일로 바꿉니다.

<YourServiceName.crt>를 Auth-Cert.crt와 같이 만들 파일 이름으로 바꿉니다.

Linux 서버에서 인증서 생성(Strict SSL check ENABLED)

> **참고**: 엄격한 TLS 확인에서는 인증서가 Apple의 TLS 요구 사항을 충족하는지 확인합니다. 자세한 내용은 관리 가이드를 참조하십시오.

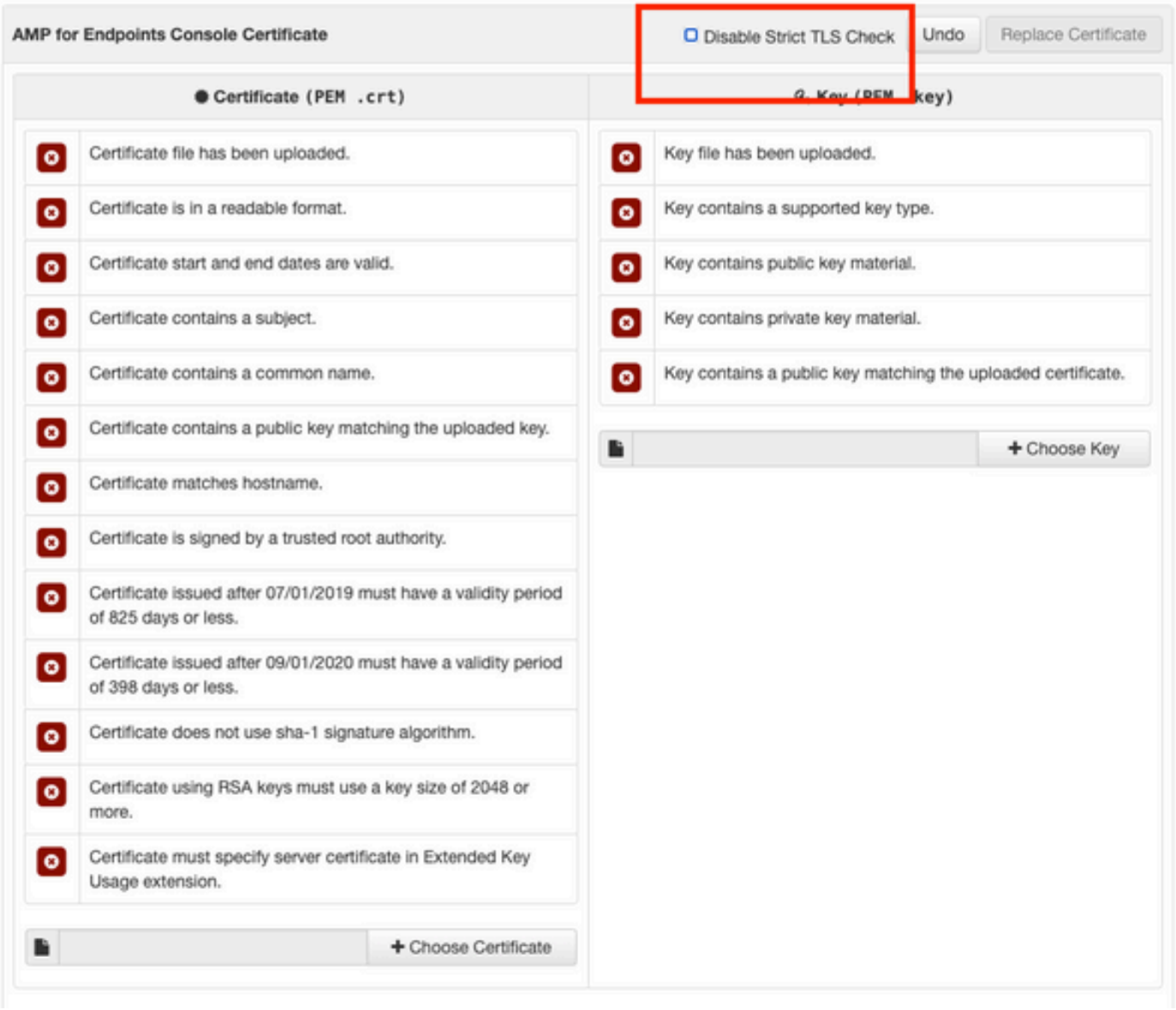
자체 서명 RootCA 생성

1단계. 루트 CA 인증서에 대한 개인 키를 생성합니다.

```
openssl genrsa -out
```
2단계. CA 인증서를 생성합니다.

```
openssl req \
-subj '/CN=
-outform pem -out
-key
-days "1000"
```
각 서비스에 대한 인증서 생성

DNS 이름 항목에 따라 Authentication, Console, Disposition, Disposition-Extended, Update server, FMC(Firepower Management Center) 서비스용 인증서를 생성합니다. 각 서비스(인증, 콘솔 등)에 대해 아래 인증서 생성 프로세스를 반복해야 합니다.



확장 구성 파일을 만들고 저장합니다(extensions.cnf).

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

개인 키 생성

```
openssl genrsa -out
```

<YourServiceName.key>를 Auth-Cert.key로 만들 새 KEY 파일 이름으로 바꿉니다.

CSR 생성

```
openssl req -new \
-key
-subj '/CN=
-out
```

교체 Auth-Cert.key와 같은 현재(또는 새) 인증서 키가 있는 <YourServiceName.key>

<YourServiceName.csr>을 현재(또는 새) 인증서 CSR(예: Auth-Cert.csr)로 교체합니다.

인증서 생성

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

<YourServiceName.csr>을 현재(또는 새) 인증서 CSR(예: Auth-Cert.csr)로 교체합니다.

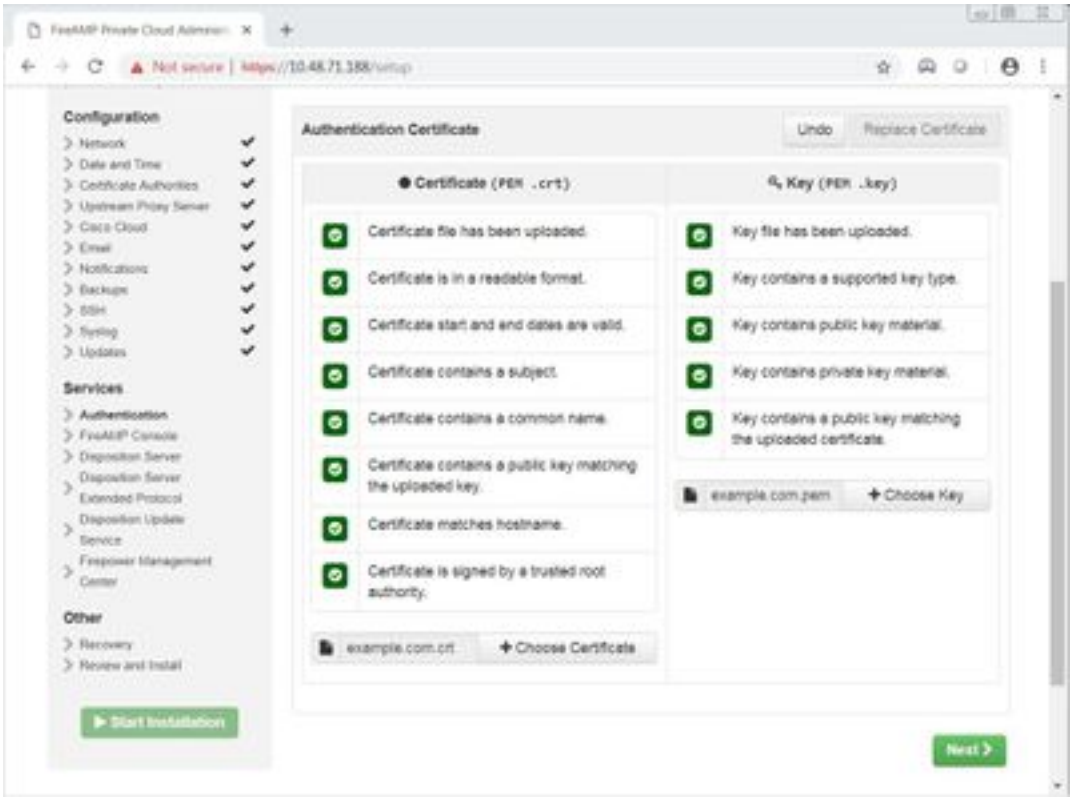
<YourRootCAName.pem>을 현재(또는 새) PEM 파일 이름으로 RootCAName.pem으로 바꿉니다.

<YourServiceName.key>를 Auth-Cert.key와 같은 현재(또는 새) 인증서 KEY 파일로 바꿉니다.

<YourServiceName.crt>를 Auth-Cert.crt와 같이 만들 파일 이름으로 바꿉니다.

Secure Console Private Cloud에 인증서 추가

1단계. 위의 방법 중 하나에서 인증서가 생성되면 각 서비스에 해당하는 인증서를 업로드합니다. 올바르게 생성된 경우, 모든 확인 표시가 여기 이미지에 표시된 대로 활성화됩니다.



다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

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.