FMC에서 관리하는 보안 방화벽 Threat Defense에서 ACME 프로토콜로 인증서 등록 구성

소개

이 문서에서는 ACME(Automated Certificate Management Environment) 프로토콜을 통해 FTD(Secure Firewall Threat Defense) 플랫폼에서 TLS(Transport Layer Security) 인증서를 등록하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- 수동 인증서 등록 프로세스 및 SSL(Secure Sockets Layer)의 기본 사항
- 원격 액세스 VPN에 대한 기본 인증 개념
- CA(Certificate Authority) 경험

사용되는 구성 요소

- Cisco FTDv 버전 10.0.0-35.
- Cisco FMC 버전 10.0.0-35
- ACME 프로토콜을 지원하는 CA(Certificate Authority) 서버.

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.

요구 사항 및 제한 사항

Secure Firewall FTD에서 ACME 등록을 위한 현재 전제 조건 및 제약 조건은 다음과 같습니다.

- FTD 및 FMC 버전 10.0.0 이상에서 지원됩니다.
- ACME는 와일드카드 인증서의 발급을 허용하지 않습니다. 각 인증서 요청은 정확한 도메인 이름을 지정해야 합니다.
- ACME를 통해 등록된 각 신뢰 지점은 단일 인터페이스로 제한되므로 ACME를 통해 얻은 인증서는 여러 인터페이스에서 공유할 수 없습니다.
- 키 쌍은 자동으로 생성되며 ACME를 통해 등록된 각 인증서에 고유하므로 키 재사용을 방지하고 보안을 강화합니다.

다운그레이드 고려 사항

ACME 등록을 지원하지 않는 Secure Firewall FTD 버전으로 다운그레이드하는 경우(버전 7.7 이하):

- 버전 10.0.0 이상에서 도입된 모든 ACME 관련 신뢰 지점 컨피그레이션이 손실됩니다.
- ACME를 통해 등록된 인증서는 여전히 액세스할 수 있습니다. 그러나 다운그레이드 후 첫 번째 저장 후 재부팅하면 개인 키가 연결 해제됩니다.

다운그레이드가 필요한 경우 권장 해결 방법을 사용합니다.

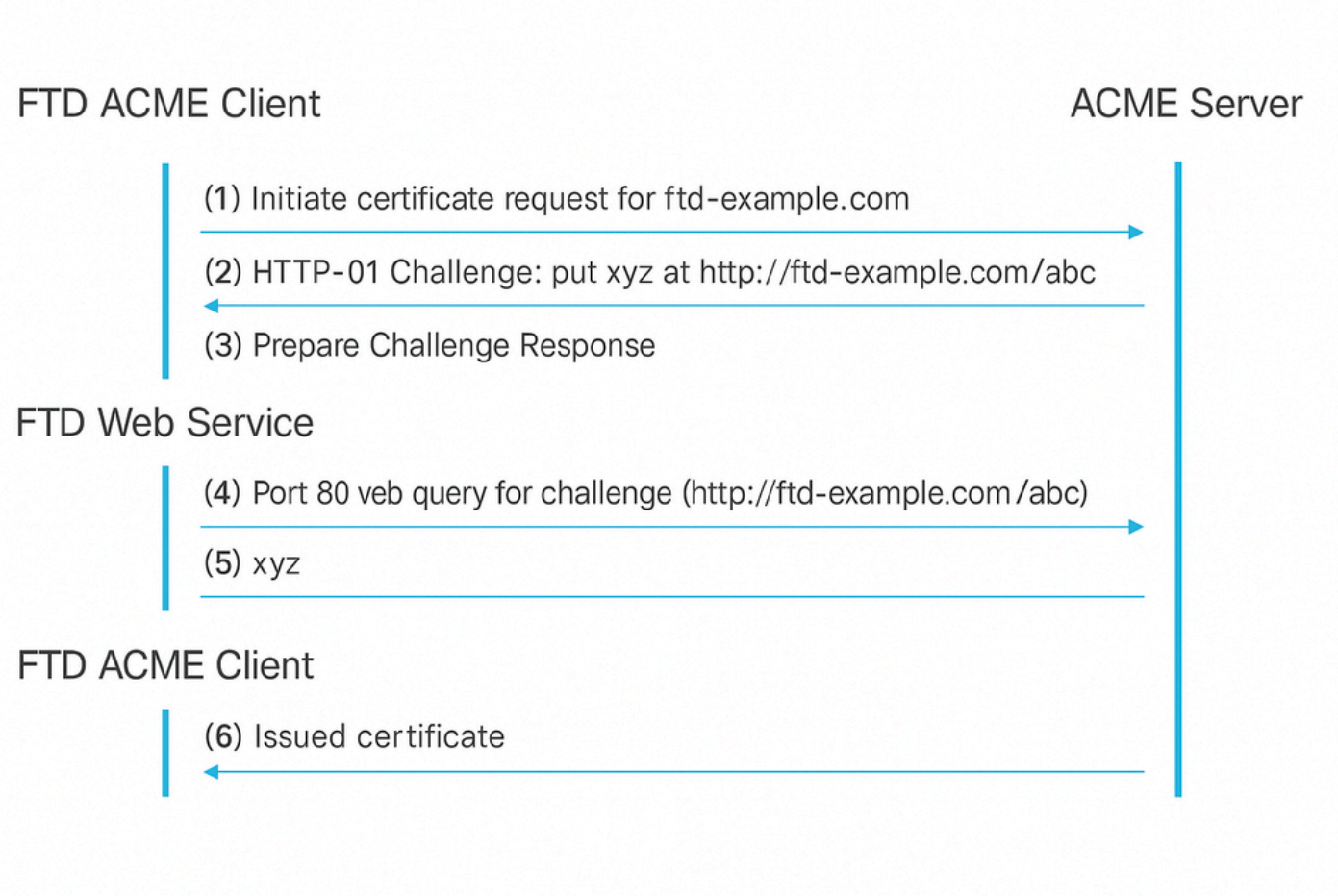
- 다운그레이드하기 전에 ACME 인증서를 PKCS12 형식으로 내보냅니다.
- 다운그레이드하기 전에 ACME 신뢰 지점 컨피그레이션을 제거합니다.
- 다운그레이드 후 PKCS12 인증서를 가져옵니다. 가져온 신뢰 지점은 ACME 발급 인증서가 만료될 때까지 유효합니다.

배경 정보

ACME 프로토콜은 네트워크 관리자를 위해 TLS 인증서 관리를 간소화하기 위한 것입니다. 관리자는 ACME를 통해 TLS 인증서 획득 및 갱신과 관련된 작업을 자동화할 수 있습니다. 이 자동화는 Let's Encrypt와 같은 CA(Certificate Authority)와 작업할 때 특히 유용합니다. Let's Encrypt는 ACME 프로토콜을 통해 무료로 자동화된 공개 액세스 가능 인증서를 제공합니다.ACME는 DV(Domain Validation) 인증서 발급을 용이하게 합니다. 이러한 인증서는 인증서 요청자가 지정된 도메인을 제어하는지 확인합니다. 검증은 일반적으로 HTTP 기반 챌린지 프로세스를 통해 수행되며, 여기서 지원자는 웹 서버에 지정된 파일을 배치합니다. 그런 다음 CA(Certificate Authority)는 도메인의 HTTP 서버를 통해 이 파일에 액세스하여 도메인 제어를 확인합니다. 이 챌린지를 성공적으로 통과하면 CA가 DV 인증서를 발급할 수 있습니다.

등록 프로세스에는 다음 단계가 포함됩니다.

1. 인증서 요청 시작: 클라이언트는 인증서가 필요한 도메인을 지정하여 ACME 서버에 인증서 요청을 제출합니다.
2. HTTP-01 챌린지 수신: ACME 서버는 클라이언트가 도메인 소유권을 증명하기 위해 사용해야 하는 고유한 토큰이 포함된 HTTP-01 챌린지에 응답합니다.
3. 챌린지 대응 준비:
    1. 클라이언트는 ACME 서버의 토큰을 계정 키와 결합하여 키 권한 부여를 생성합니다.
    2. 클라이언트는 특정 URL 경로에서 이 키 권한 부여를 제공하도록 웹 서버를 구성합니다.
4. ACME 서버가 챌린지 검색: ACME 서버는 키 권한 부여를 얻기 위해 제공된 URL에 대해 HTTP GET 요청을 수행합니다.
5. ACME 서버에서 소유권 확인: 서버는 검색된 키 권한 부여를 예상 값과 비교하여 도메인에 대한 클라이언트의 제어를 확인합니다.
6. 발급 인증서: 검증에 성공하면 ACME 서버는 SSL/TLS 인증서를 클라이언트에 발급합니다.



ACME 등록 HTTP-01 인증 흐름

ACME 프로토콜을 사용하여 Secure Firewall FTD에 TLS 인증서를 등록하면 다음과 같은 이점이 있습니다.

- 인증서 관리 자동화: ACME는 Secure Firewall FTD TLS 인터페이스에 대한 TLS 도메인 인증서를 가져오고 유지 관리하는 프로세스를 간소화하므로 수동 관리 작업이 크게 줄어듭니다.
- 자동 인증서 갱신: ACME 지원 신뢰 지점을 사용하면 인증서가 만료에 가까워지면 자동으로

갱신되므로 지속적인 관리 개입이 최소화됩니다.
- 지속적인 보안 보증: 이러한 자동화를 통해 중단 없이 인증서가 유효하게 유지되므로 예기치 않은 인증서 만료를 방지하고 보안 통신을 유지할 수 있습니다.

이러한 장점들은 보안 방화벽 FTD 구축을 위한 운영 효율성과 보안을 종합적으로 강화합니다.

구성

사전 요구 사항 컨피그레이션

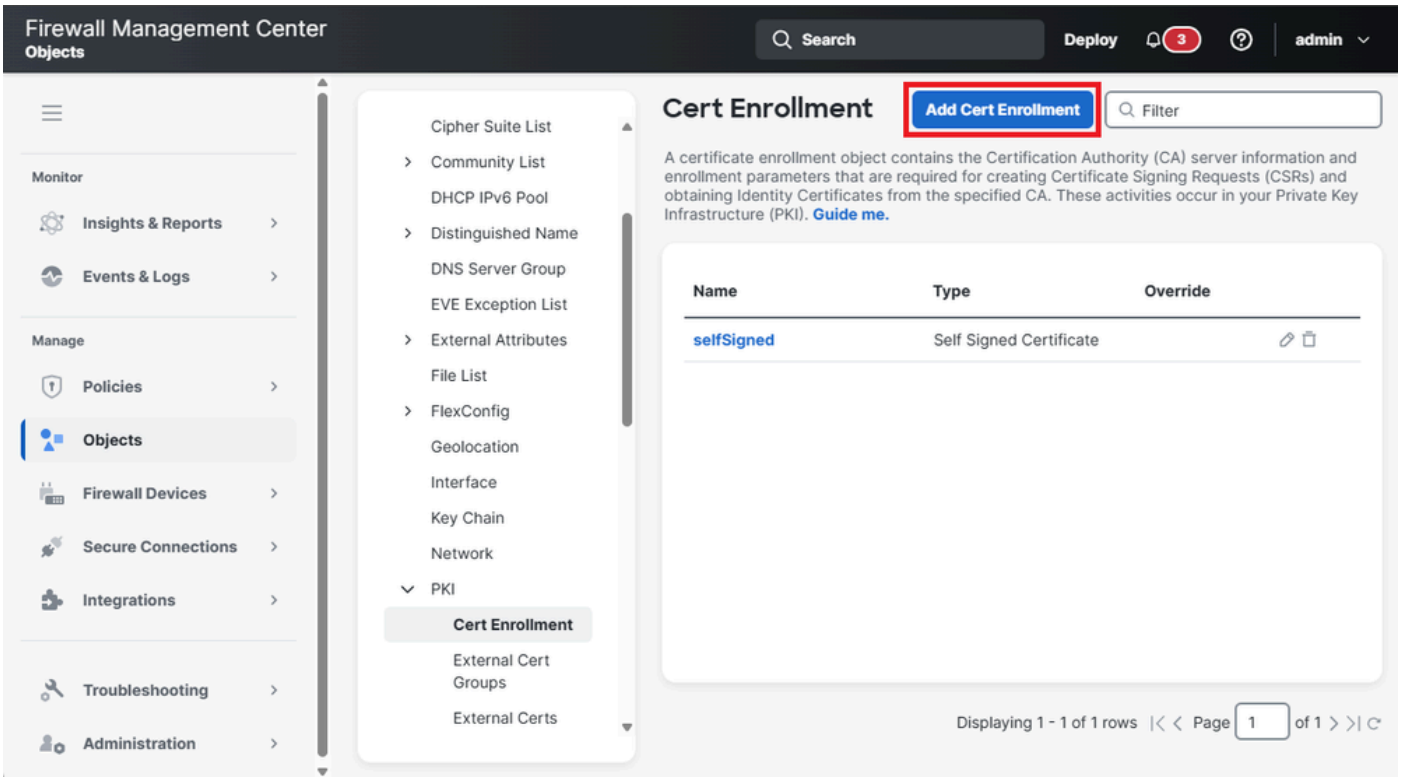
ACME 등록 프로세스를 시작하기 전에 다음 조건이 충족되는지 확인합니다.

1. 확인 가능한 도메인 이름: 인증서를 요청하는 도메인 이름은 ACME 서버에서 확인 가능해야 합니다. 이렇게 하면 서버에서 도메인 소유권을 확인할 수 있습니다.
2. ACME 서버에 대한 보안 방화벽 액세스: 보안 방화벽에는 인터페이스 중 하나를 통해 ACME 서버에 액세스할 수 있는 기능이 있어야 합니다. 이 액세스는 인증서가 요청되는 인터페이스를 통하지 않아도 됩니다.
3. TCP 포트 80 가용성: ACME CA 서버에서 도메인 이름에 해당하는 인터페이스로의 TCP 포트 80을 허용합니다. 이는 ACME 교환 프로세스에서 HTTP-01 챌린지를 완료하는 데 필요합니다.

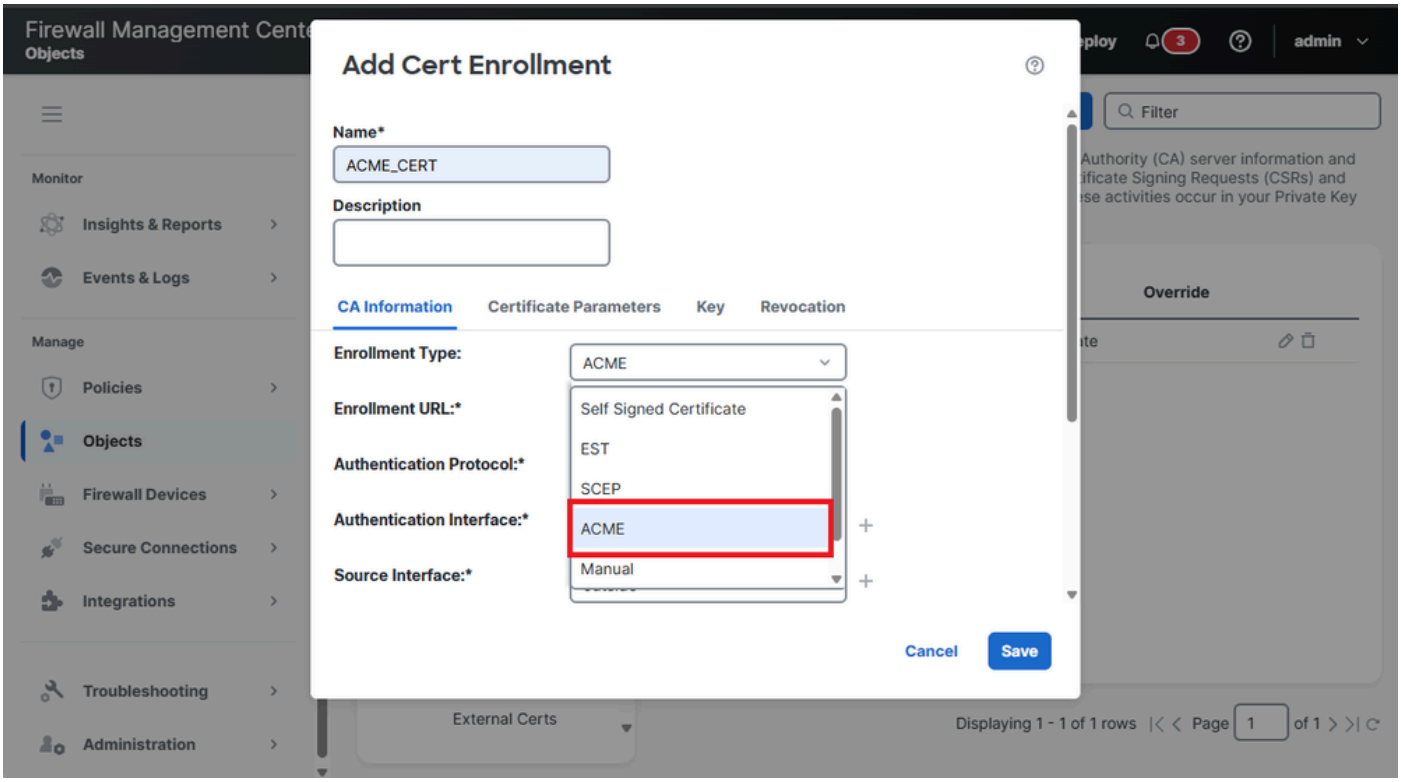
참고: 포트 80이 열려 있는 기간에는 ACME 챌린지 데이터만 액세스할 수 있습니다.

ACME 인증서 등록 객체 생성

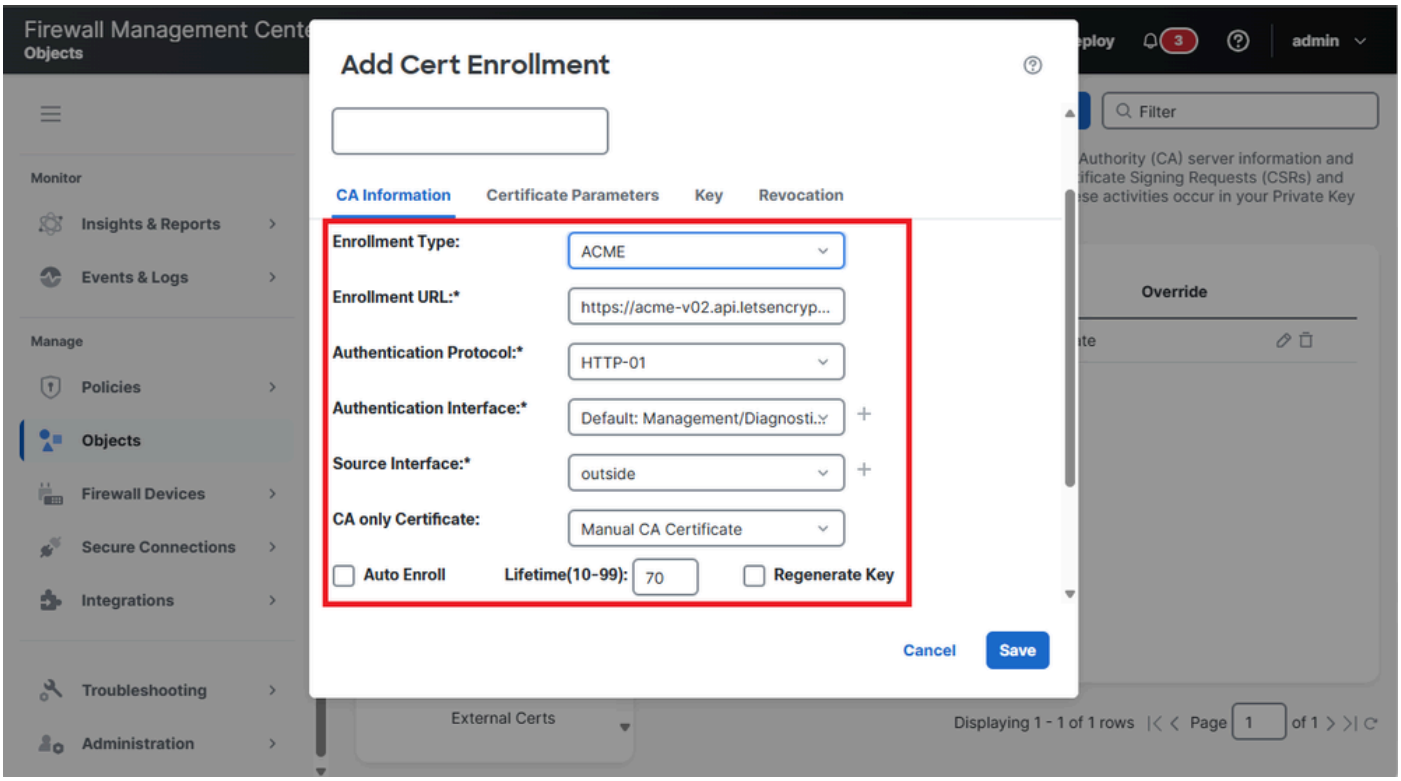
1. Objects(개체) > PKI > Cert Enrollment(인증서 등록)로 이동하고 Add Cert Enrollment(인증서 등록 추가)를 클릭하여 컨피그레이션 프로세스를 시작합니다.



2. ACME 등록 옵션은 다른 등록 방법과 함께 드롭다운 메뉴에 나열됩니다. Enrollment Type(등록 유형) 드롭다운에서 ACME를 선택하여 계속합니다.



3. 인증서 매개변수를 구성하는 옵션이 표시되면 해당 정보로 필드를 완료합니다.

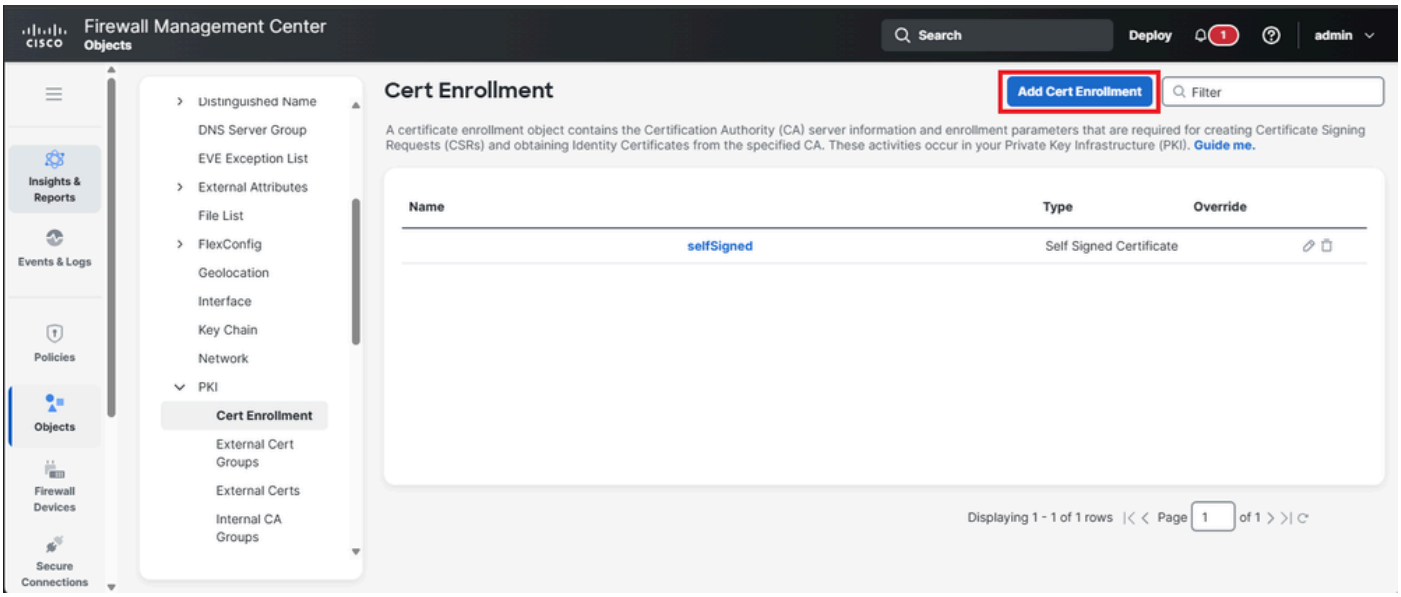


- 등록 URL: 인증서를 요청하고 검색하는 데 사용되는 ACME 서버(예: Let's Encrypt)의 주소입니다.
- 인증 프로토콜: 도메인 소유권을 확인하는 데 사용되는 방법을 지정합니다. ACME 챌린지에 대해 지원되는 프로토콜은 HTTP-01입니다.
- 인증 인터페이스: ACME 서버로부터 HTTP-01 챌린지를 수신하는 FTD 디바이스의 네트워크 인터페이스.
- CA 전용 인증서: ACME 서버를 신뢰할 수 있는 CA(인증 기관)의 인증서를 선택해야 합니다.

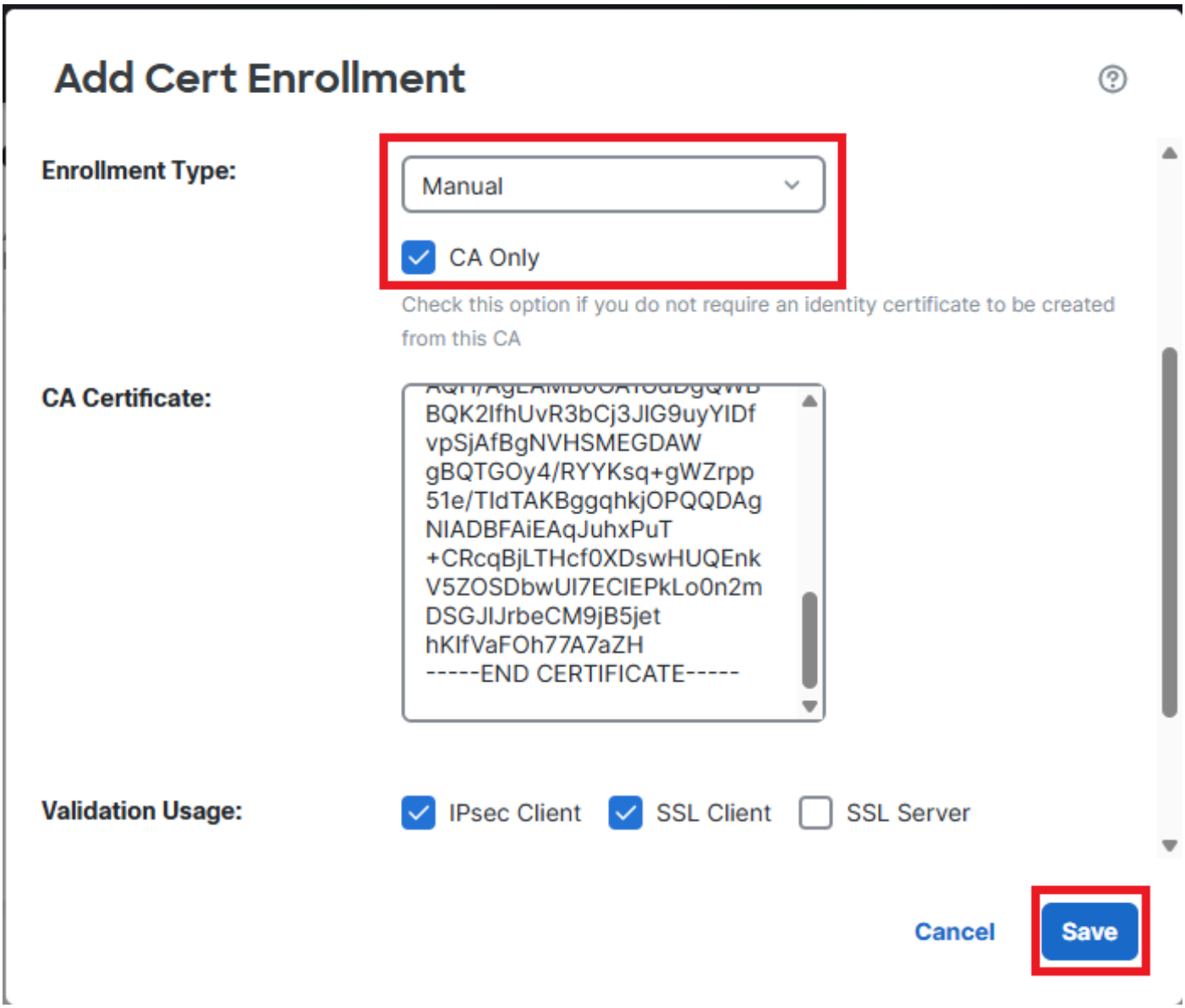
참고: 기본적으로 공용 Let's Encrypt 서비스 URL을 가리킵니다. https://acme-v02.api.letsencrypt.org/directory

---

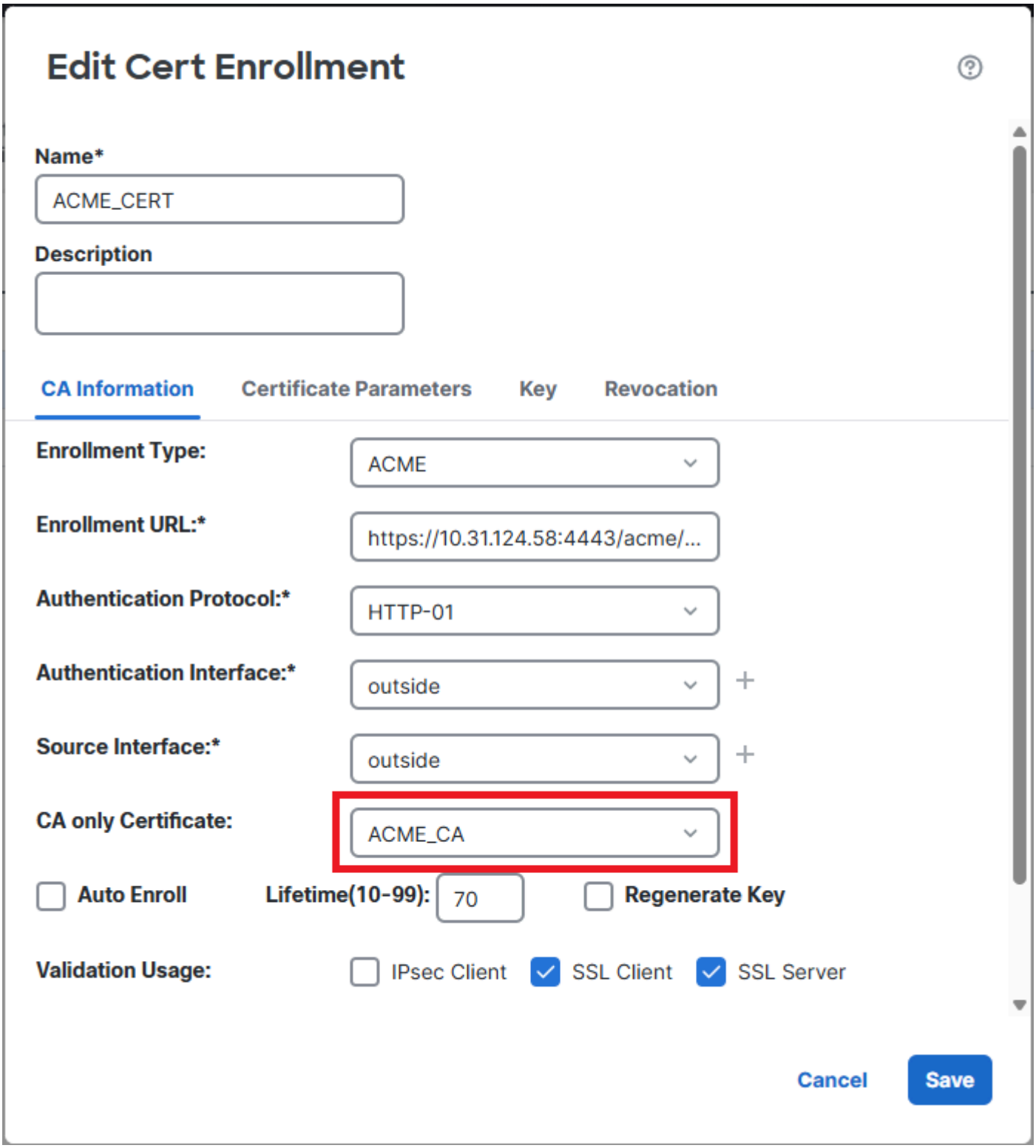
4. 잘 알려지지 않은 ACME 서버를 사용하는 경우 ACME 서버의 CA 인증서를 추가해야 합니다. Objects(개체) > Cert Enrollment(인증서 등록)로 이동하고 Add Cert Enrollment(인증서 등록 추가) 버튼을 클릭합니다.



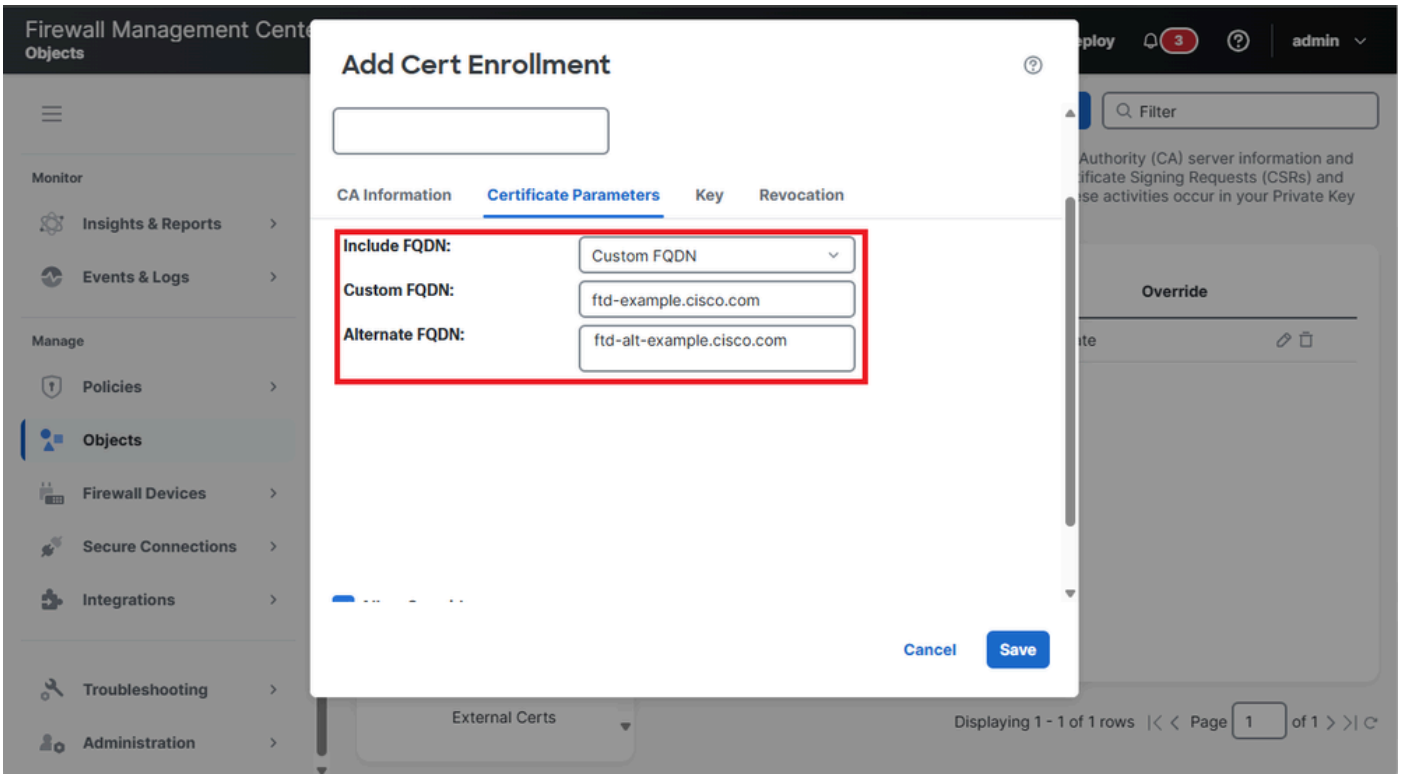
- 신뢰 지점의 이름을 지정하고 등록 유형을 수동으로 선택합니다. 그런 다음 CA Only(CA 전용) 옵션을 선택합니다. 마지막으로 ACME 서버의 CA 인증서를 붙여넣고 Save(저장)를 클릭합니다.



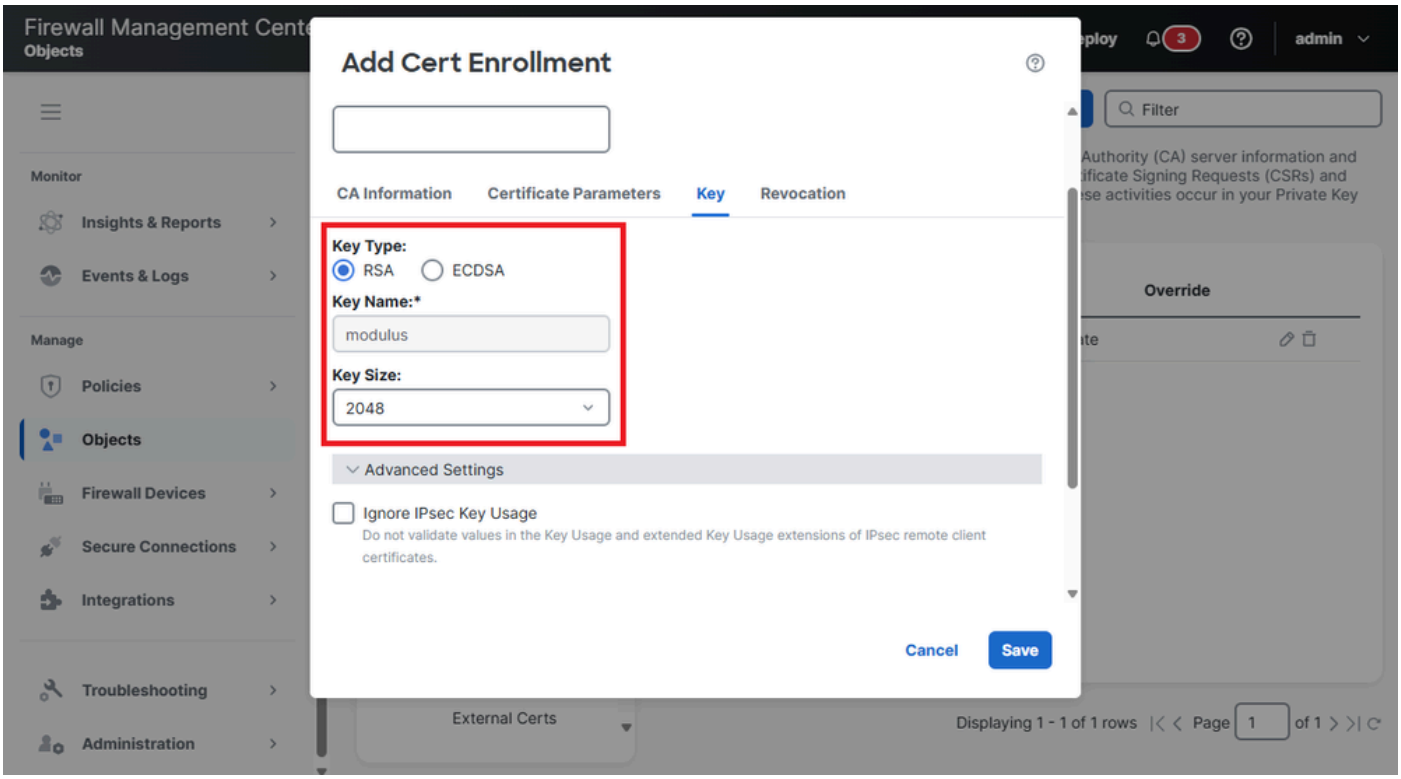
- 마지막으로, CA Only Certificate(CA 전용 인증서) 섹션에서 ACME CA 서버의 신뢰 지점을 선택합니다.



5. Certificate Parameters(인증서 매개변수)로 이동하고, Include FQDN(FQDN 포함) 상자에서 Custom FQDN(사용자 지정 FQDN) 옵션을 선택하고, Custom FQDN(사용자 지정 FQDN) 및 Alternate FQDN(대체 FQDN) 필드를 기본 FQDN 및 인증서에 포함할 대체 도메인 이름으로 채웁니다.



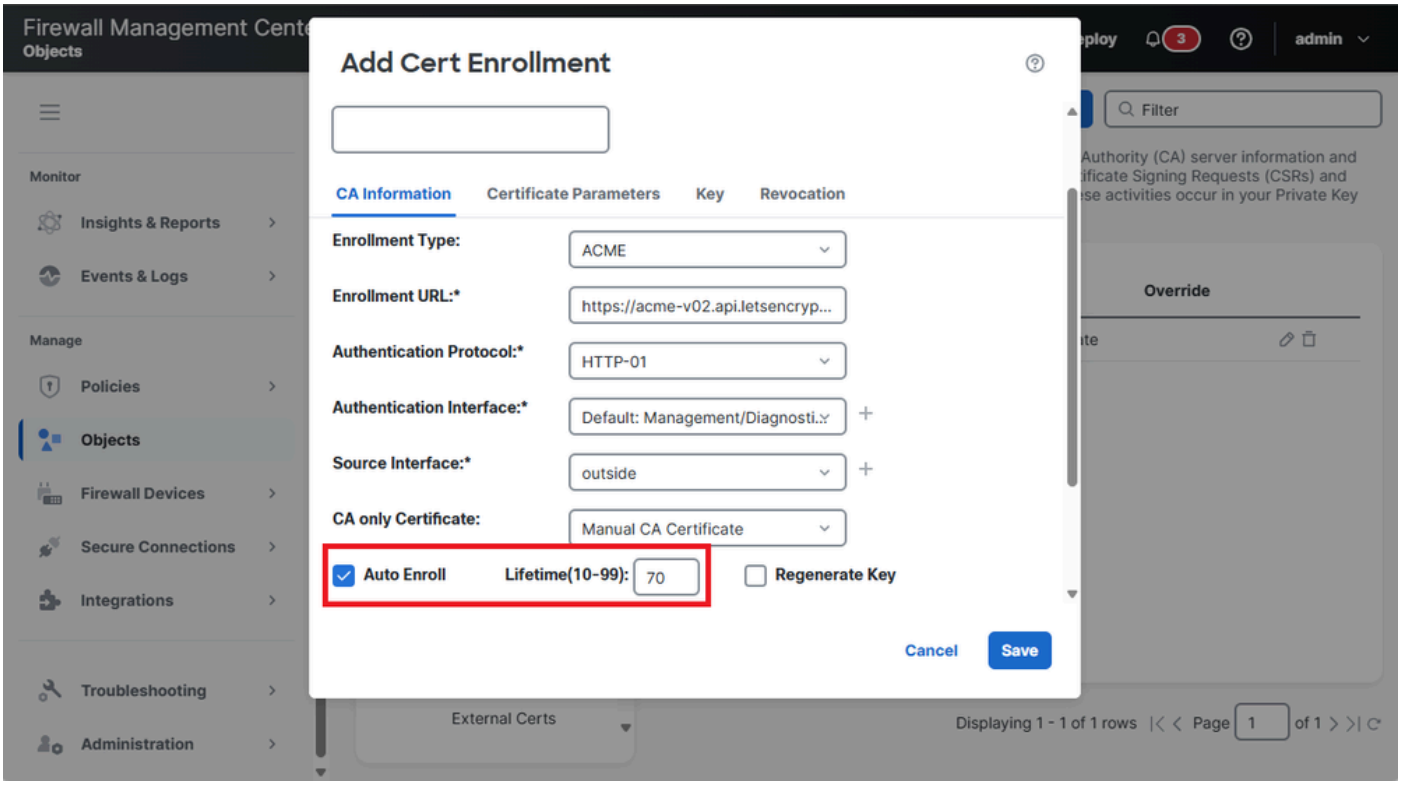
6. 키로 이동하여 키 유형과 키 크기 설정을 수정합니다.



7. (선택 사항) ID 인증서에 대한 자동 등록을 활성화합니다.

자동 등록 확인란을 선택하고 자동 등록 수명에 대한 백분율을 지정합니다.

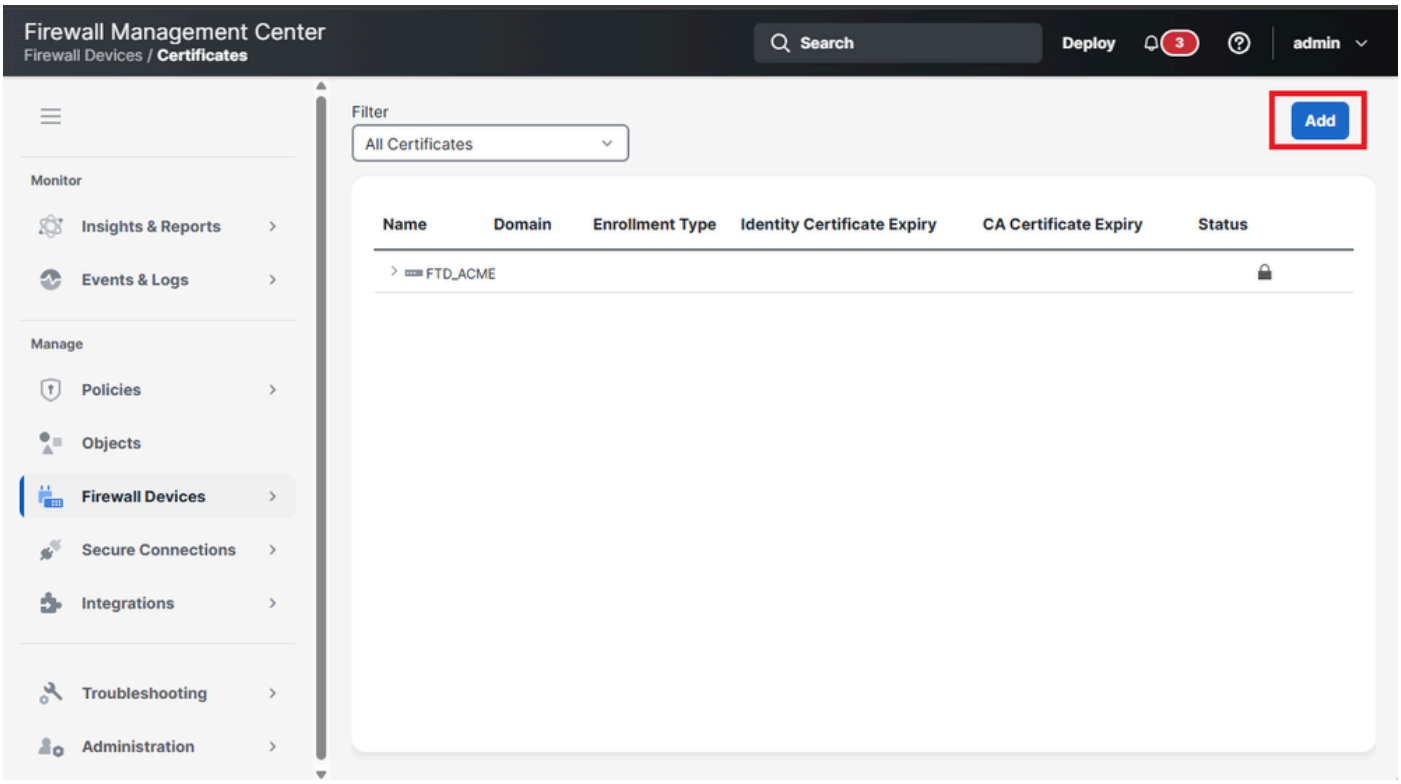
이 기능을 사용하면 인증서가 만료되기 전에 자동으로 갱신됩니다. 백분율은 인증서 만료 전에 갱신 프로세스가 시작되는 정도를 결정합니다. 예를 들어 80%로 설정하면 인증서가 유효 기간의 80%에 도달하면 갱신 프로세스가 시작됩니다.



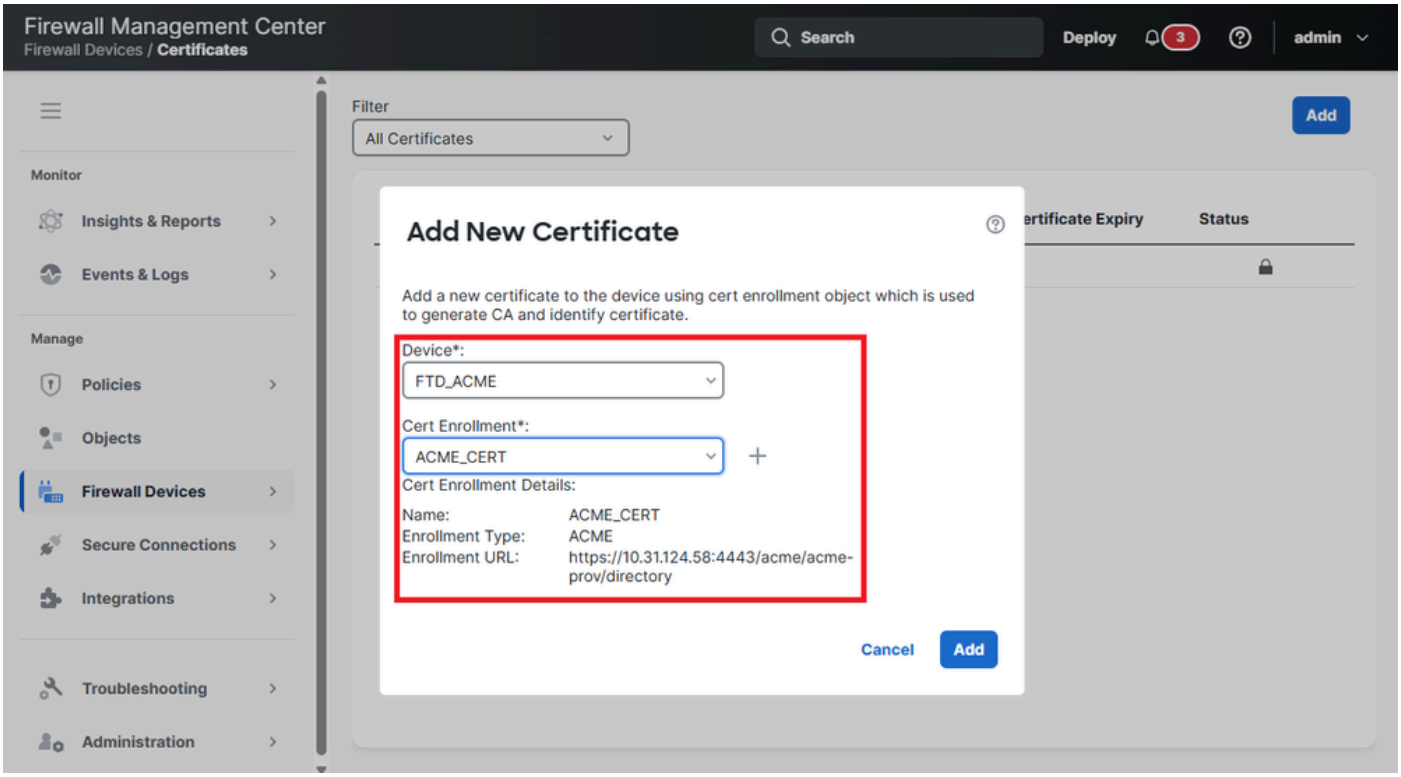
8. 저장을 클릭합니다.

디바이스의 ACME 인증서 등록

1.Firewall Devices(방화벽 디바이스) > Certificates(인증서)로 이동하고 Add(추가) 버튼을 클릭하여 새 인증서를 등록합니다.

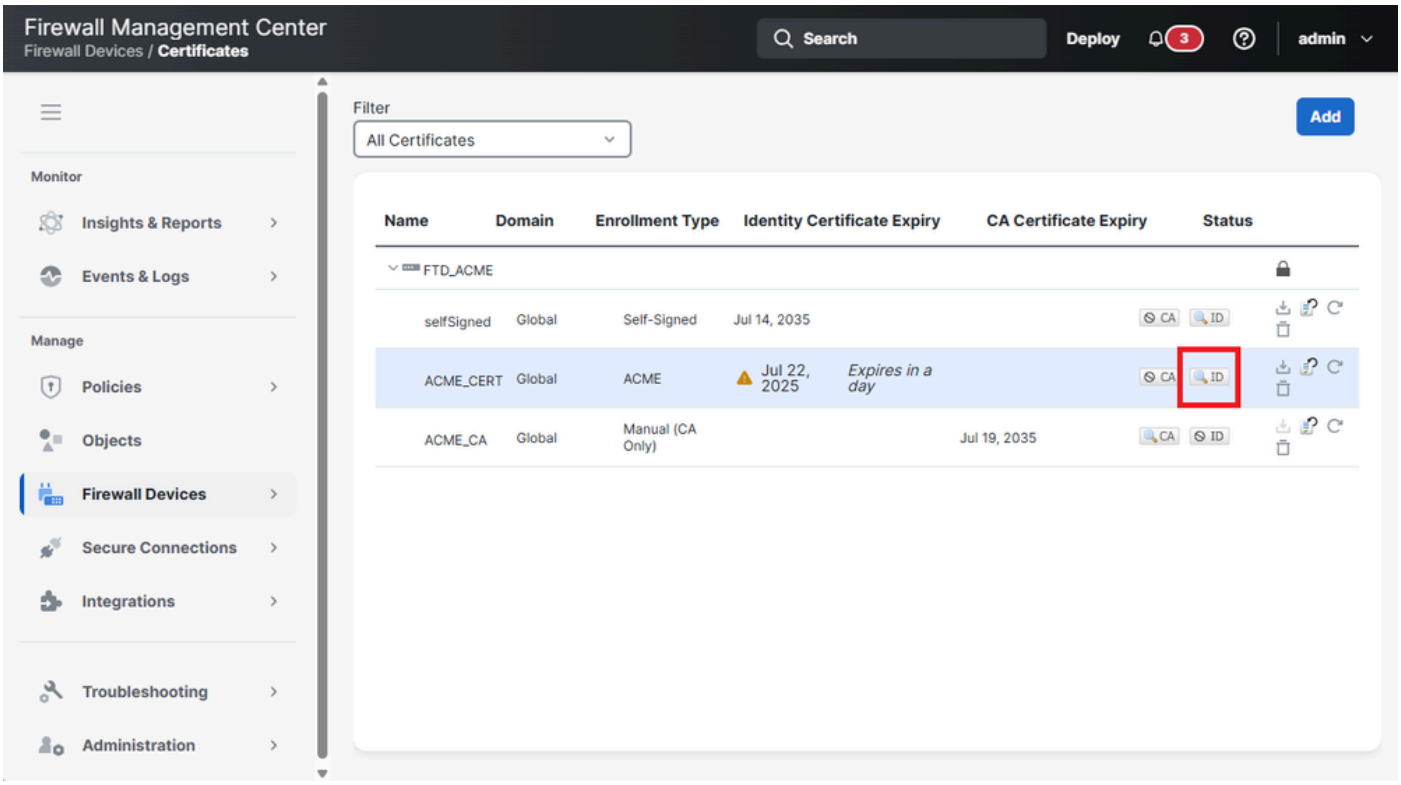


2. Device 드롭다운 목록에서 FTD 디바이스를 선택하고 Cert Enrollment에서 이전에 생성한 인증서 객체를 선택합니다.

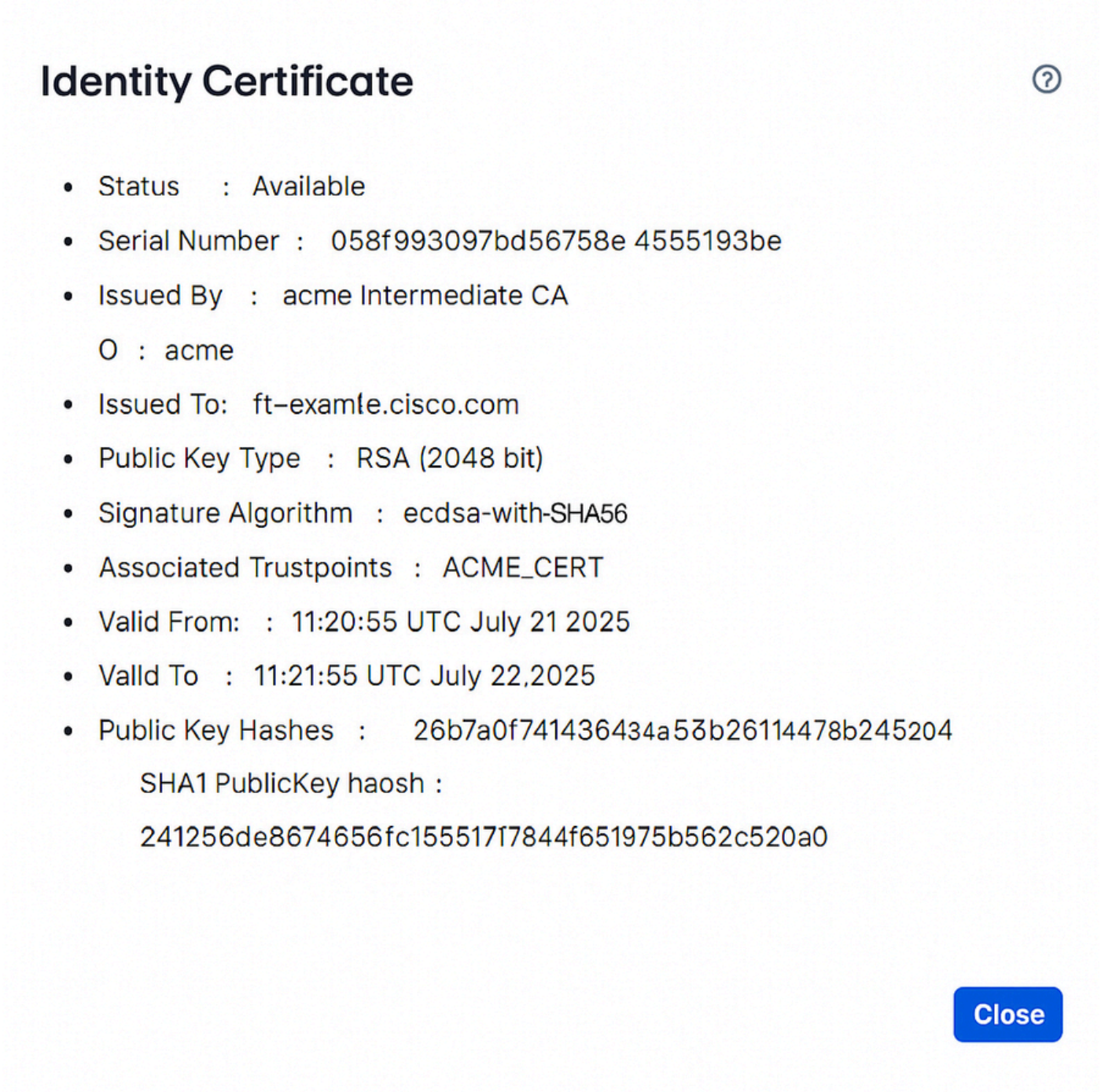


3. 추가를 클릭합니다.

4. 구축이 완료되면 상태 열에 ID 인증서 버튼이 표시됩니다.



5. ID 버튼을 클릭하여 ID 인증서 정보를 검증합니다.



다음을 확인합니다.

FTD에서 설치된 인증서 보기

인증서가 명령에 등록되었는지 확인합니다.show crypto ca certificates <Trust Point Name>.

<#root>

```
firepower#
```

show crypto ca certificates

ACME_CERT

```
Certificate
Status: Available
Certificate Serial Number: 058f993097bd56758e44554194a953be
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=acme Intermediate CA
O=acme
Subject Name:
CN=ftd-example.cisco.com
Validity Date:
start date: 11:20:55 UTC Jul 21 2025
end date: 11:21:55 UTC Jul 22 2025
Storage: immediate
Associated Trustpoints: ACME_CERT
Public Key Hashes:
SHA1 PublicKey hash: 26b7a0f7414364a45b246114478bb74f432520c4
SHA1 PublicKeyInfo hash: 24125d6e8674566c1551784f651975b562c520a
```

Syslog 이벤트

ACME 프로토콜을 사용하는 인증서 등록과 관련된 이벤트를 캡처하기 위해 Secure Firewall FTD에 새로운 syslog가 있습니다.

- 717067: ACME 인증서 등록이 시작되는 시점에 대한 정보를 제공합니다.

```
%FTD-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.
```

- 717068: ACME 인증서 등록 성공 시기에 대한 정보를 제공합니다.

```
%FTD-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069: ACME 등록 실패 시기에 대한 정보를 제공합니다.

```
%FTD-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070: 인증서 등록 또는 인증서 갱신을 위한 키 쌍과 관련된 정보를 제공합니다.

```
%FTD-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

문제 해결

ACME 인증서 등록이 실패할 경우 다음 단계를 수행하여 문제를 식별하고 해결합니다.

- 서버에 대한 연결 확인:보안 방화벽에 ACME 서버에 대한 네트워크 연결이 있는지 확인합니다. 통신을 차단하는 네트워크 문제 또는 방화벽 규칙이 없는지 확인합니다.
- 보안 방화벽 도메인 이름을 확인할 수 있는지 확인합니다.보안 방화벽 FTD에 구성된 도메인 이름을 ACME 서버에서 확인할 수 있는지 확인합니다. 이 확인은 서버에서 요청을 검증하는 데 중요합니다.
- 도메인 소유권 확인: 신뢰 지점에 지정된 모든 도메인 이름이 보안 방화벽 FTD에서 소유하고 있는지 확인합니다. 이렇게 하면 ACME 서버에서 도메인 소유권을 확인할 수 있습니다.

명령 문제 해결

자세한 내용은 다음 debug 명령의 출력을 수집합니다.

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

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.