보안 방화벽에서 ACME 프로토콜로 인증서 등록 구성

목차

- 소개
- 사전 요구 사항
  - 요구 사항
  - 사용되는 구성 요소
  - 요구 사항 및 제한 사항
  - 다운그레이드 고려 사항
- 배경 정보
- 구성
  - 사전 요구 사항 컨피그레이션
  - ASDM을 통한 ACME 등록
  - Secure Firewall ASA CLI를 사용한 ACME 등록
- 다음을 확인합니다.
  - ASA에 설치된 인증서 보기
  - Syslog 이벤트
- 문제 해결
  - 명령 문제 해결
  - 오류 코드
  - 이유
  - 가능한 원인 또는 치료
- 관련 정보

소개

이 문서에서는 Secure Firewall ASA에서 ACME(Automated Certificate Management Environment) 프로토콜을 사용하여 TLS(Transport Layer Security) 인증서를 등록하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Firewall ASA(Adaptive Security Appliance)
- PKI(Public Key Infrastructure)

사용되는 구성 요소

- Cisco ASAv 버전 9.23.1.
- Cisco ASDM 버전 7.23(1).
- 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 ASA의 ACME 등록에 대한 현재 요구 사항 및 제한 사항은 다음과 같습니다.

- ASA 버전 9.23.1 및 ASDM 7.23.1 이상에서 지원됨
- 다중 컨텍스트에서는 지원되지 않음
- ACME는 와일드카드 인증서 생성을 지원하지 않습니다. 각 인증서 요청은 정확한 도메인 이름을 지정해야 합니다.
- ACME를 통해 등록된 각 신뢰 지점은 단일 인터페이스로 제한되므로, ACME에 등록된 인증서는 여러 인터페이스에서 공유할 수 없습니다.
- 키 쌍은 자동으로 생성되며 ACME를 통해 등록된 인증서에 대해 공유할 수 없습니다. 각 인증서는 고유한 키 쌍을 사용하여 보안을 향상시키지만 키 재사용을 제한합니다.

다운그레이드 고려 사항

Secure Firewall ASA(9.22 이상)에서 ACME 등록을 지원하지 않는 버전으로 다운그레이드할 경우:

- 9.23.x 이상에 새로 추가된 모든 ACME 관련 신뢰 지점 컨피그레이션이 손실됨
- ACME를 통해 등록된 인증서는 계속 액세스할 수 있지만, 첫 번째 다운그레이드 후 저장 및 재부팅 후에는 개인 키의 연결이 해제됩니다

다운그레이드가 필요한 경우 다음 권장 해결 절차를 수행합니다.

1. 다운그레이드하기 전에 ACME 인증서를 PKCS12 형식으로 내보냅니다.
2. 다운그레이드하기 전에 ACME 신뢰 지점 컨피그레이션을 제거해야 합니다.
3. 다운그레이드 후 PKCS12 인증서를 가져옵니다. 결과 신뢰 지점은 ACME를 통해 발급된 인증서가 만료될 때까지 계속 유효합니다.

배경 정보

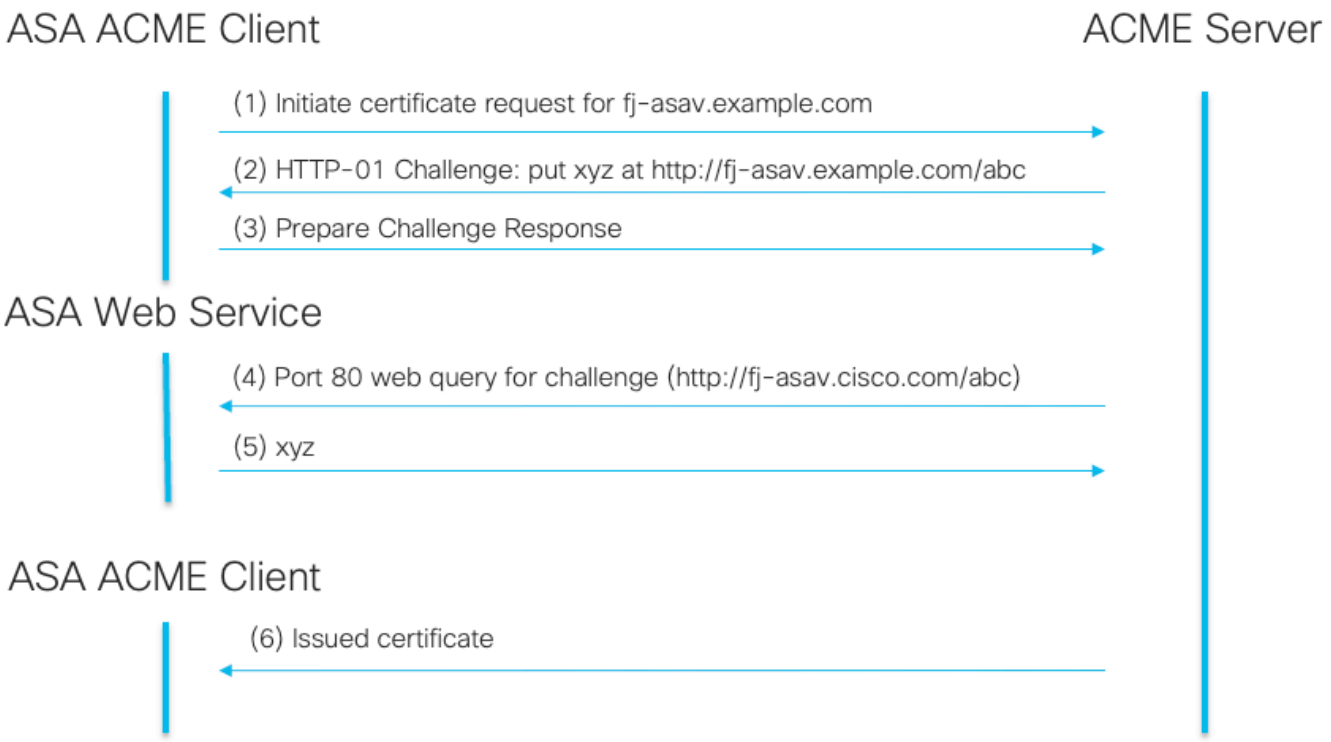
ACME 프로토콜은 네트워크 관리자를 위해 TLS 인증서 관리를 간소화하도록 설계되었습니다. 관리자는 ACME를 사용하여 TLS 인증서 획득 및 갱신과 관련된 프로세스를 자동화할 수 있습니다. 이러한 자동화는 Let's Encrypt와 같은 CA(Certificate Authority)를 활용할 때 특히 유용합니다. Let's

Encrypt는 ACME 프로토콜을 사용하여 무료로 자동화된 개방형 인증서를 제공합니다.

ACME는 DV(Domain Validation) 인증서 발급을 지원합니다. 이러한 인증서는 지정된 도메인에 대한 인증서 보유자의 제어를 확인하는 디지털 인증서의 유형입니다. DV 인증서의 유효성 검사 프로세스는 일반적으로 HTTP 기반 챌린지 메커니즘을 통해 수행됩니다. 이 메커니즘에서 지원자는 웹 서버에 특정 파일을 배치합니다. CA(Certificate Authority)는 도메인의 HTTP 서버를 통해 파일에 액세스하여 이를 확인합니다. 이 챌린지를 성공적으로 완료하면 CA는 지원자가 DV 인증서의 발급을 허용하면서 도메인을 제어할 수 있음을 보여 줍니다.

등록 절차는 다음과 같습니다.

1. 인증서 요청 시작: 클라이언트는 ACME 서버에서 인증서를 요청하고 인증서가 필요한 도메인을 지정합니다.
2. HTTP-01 챌린지 수신: ACME 서버는 클라이언트가 도메인 제어를 입증하는 데 사용할 수 있는 고유한 토큰과 함께 HTTP-01 챌린지를 제공합니다.
3. 챌린지 대응 준비:
    - 클라이언트는 ACME 서버의 토큰을 계정 키와 결합하여 키 권한 부여를 생성합니다.
    - 클라이언트는 특정 URL 경로에서 이 키 권한 부여를 제공하도록 웹 서버를 설정합니다.
4. ACME 서버가 챌린지 검색: ACME 서버는 키 권한 부여를 검색하기 위해 지정된 URL에 대한 HTTP GET 요청을 수행합니다.
5. ACME 서버에서 소유권 확인: 서버는 검색된 키 권한 부여가 예상 값과 일치하는지 확인하여 도메인에 대한 클라이언트 제어를 확인합니다.
6. 발급 인증서: 검증에 성공한 후 ACME 서버는 SSL/TLS 인증서를 클라이언트에 발급합니다.



ACME 등록 HTTP-01 인증 흐름

ACME 프로토콜을 사용하여 TLS 인증서를 등록하면 다음과 같은 혜택을 얻을 수 있습니다.

- ACME는 Secure Firewall ASA TLS 인터페이스에 대한 TLS 도메인 인증서의 획득 및 유지 관리를 용이하게 합니다. 이러한 자동화는 수동 작업을 크게 줄이고 지속적인 감독 없이 인증서를 최신 상태로 유지하는 데 도움이 됩니다.
- ACME 지원 신뢰 지점을 사용하면 인증서가 만료 임박에 따라 자동으로 갱신됩니다. 이 기능은 관리 개입의 필요성을 줄여 중단 없는 보안을 보장하고 예상치 못한 인증서 만료를 방지합니다.

구성

사전 요구 사항 컨피그레이션

ACME 등록 프로세스를 시작하기 전에 다음 조건이 충족되는지 확인합니다.

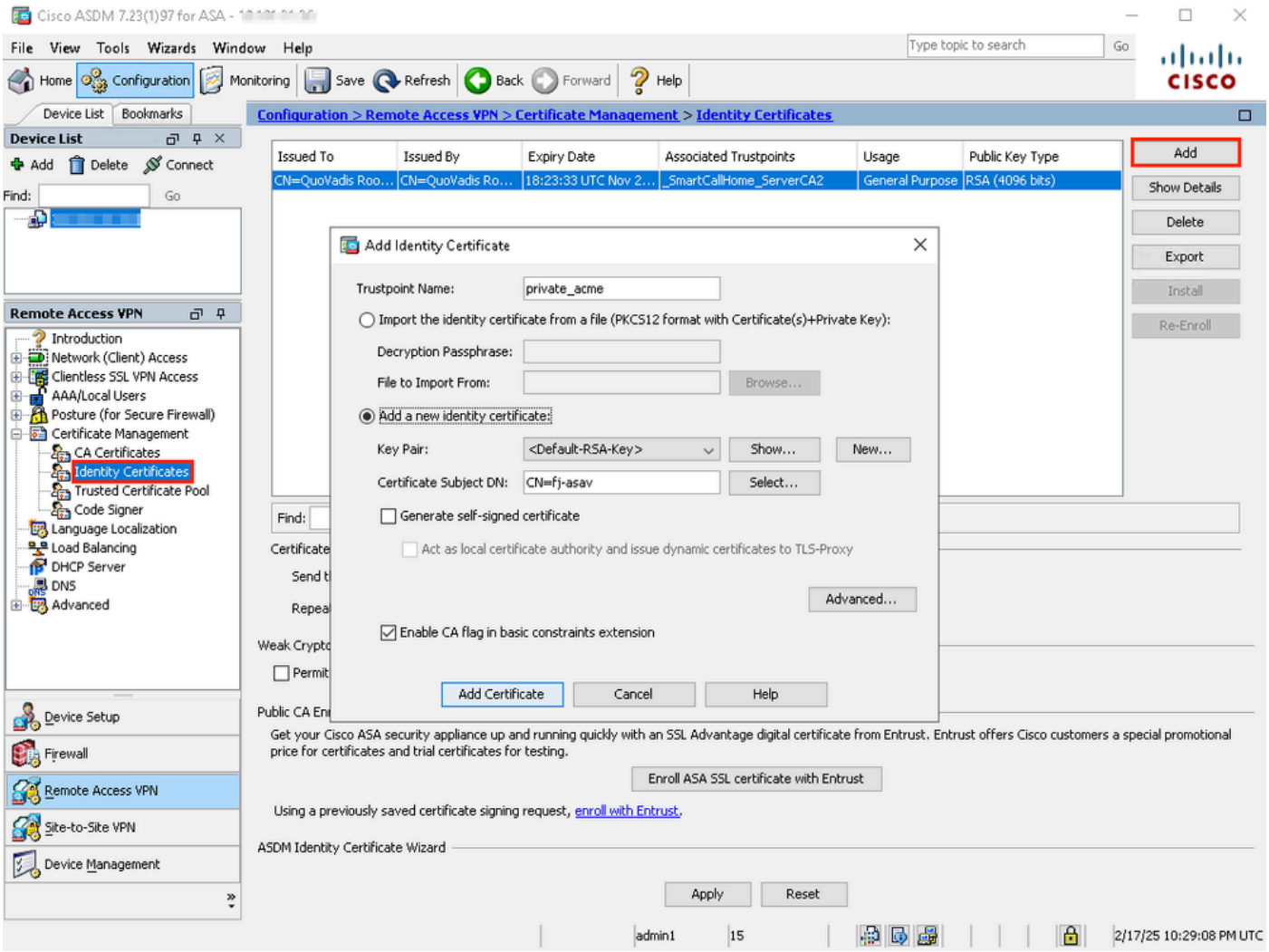
1. 확인 가능한 도메인 이름: 인증서를 요청하는 도메인 이름은 ACME 서버에서 확인할 수 있어야 합니다. 이렇게 하면 서버에서 도메인 소유권을 확인할 수 있습니다.
2. ACME 서버에 대한 보안 방화벽 액세스: 보안 방화벽은 인터페이스 중 하나를 통해 ACME 서버에 액세스할 수 있어야 합니다. 이 액세스는 인증서가 요청되는 인터페이스를 통하지 않아도 됩니다.
3. TCP 포트 80 가용성: ACME CA 서버에서 도메인 이름에 해당하는 인터페이스로 TCP 포트 80을 허용합니다. 이는 ACME 교환 프로세스에서 HTTP-01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

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

ASDM을 통한 ACME 등록

1. 새 ID 인증서를 추가합니다.

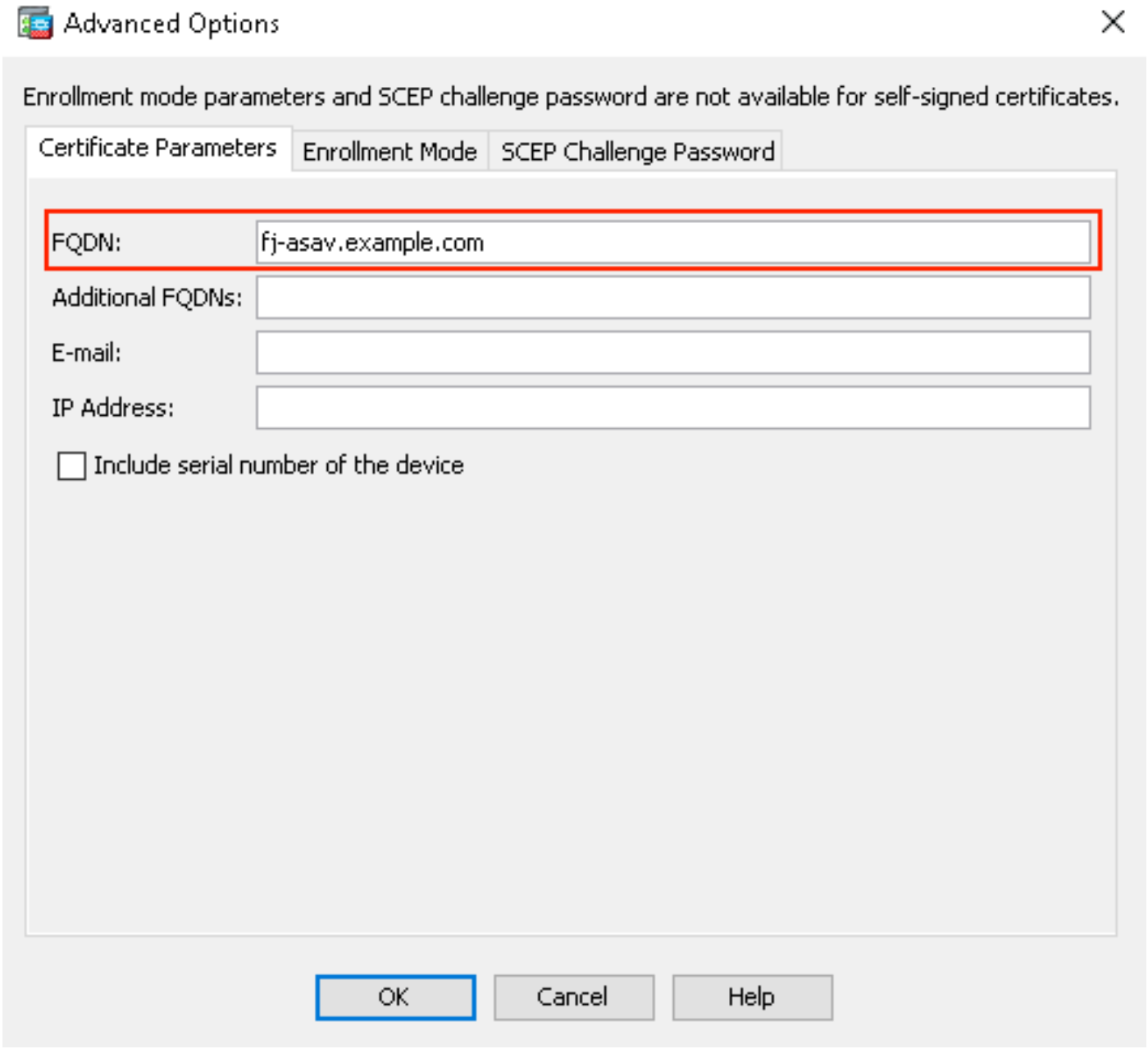
- Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Certificate Management(인증서 관리) > Identity Certificates(ID 인증서)로 이동합니다.
- 추가 버튼을 클릭하고 새 ID 인증서 추가를 선택합니다.



ACME 등록 ASDM ID 인증서

2. ID 인증서의 FQDN을 지정합니다.

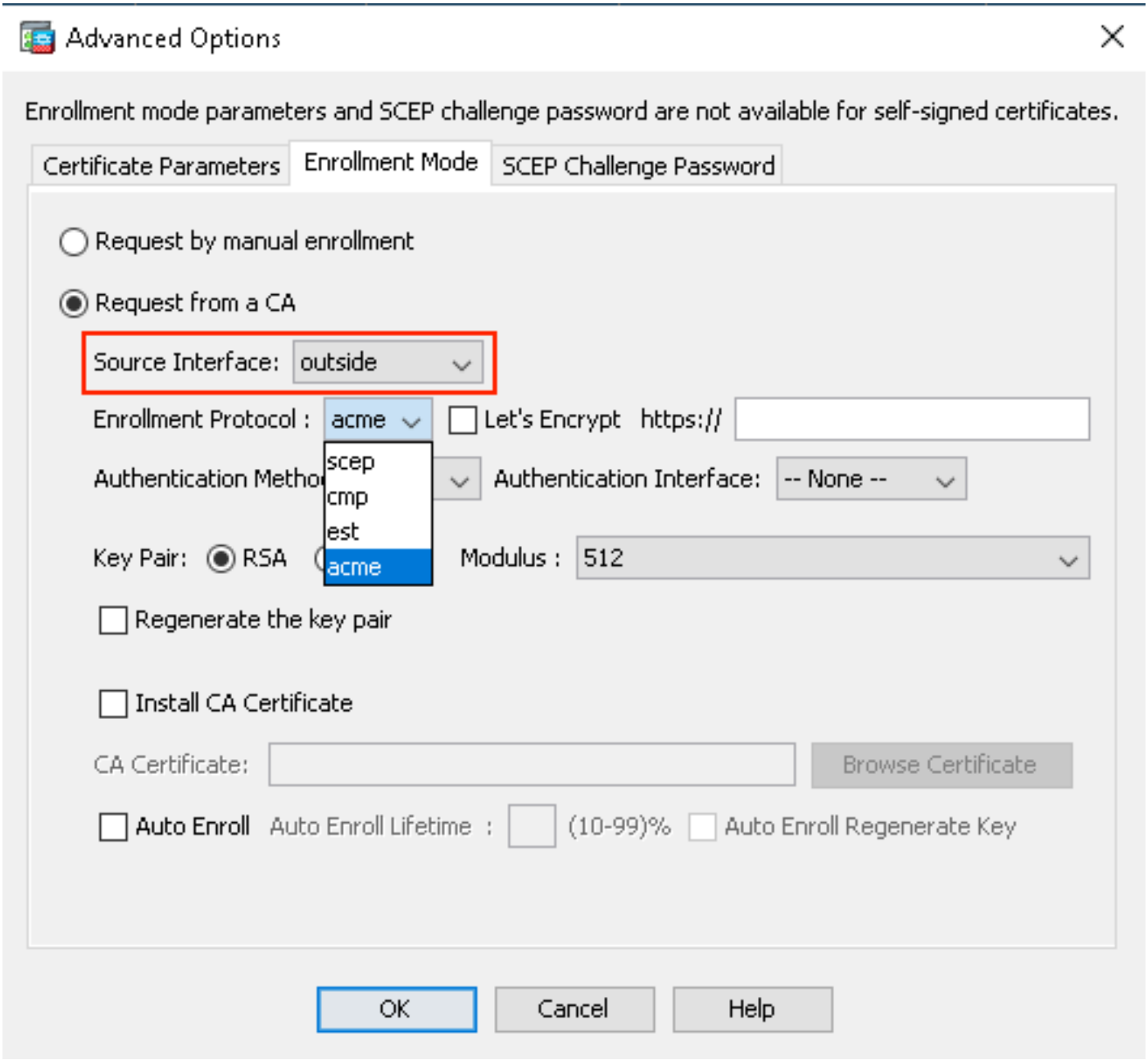
- Advanced(고급) 버튼을 클릭합니다.
- Certificate Parameters(인증서 매개변수) 탭 아래에서 인증서가 가져야 하는 FQDN을 지정합니다.



ACME 등록 ASDM FQDN입니다.

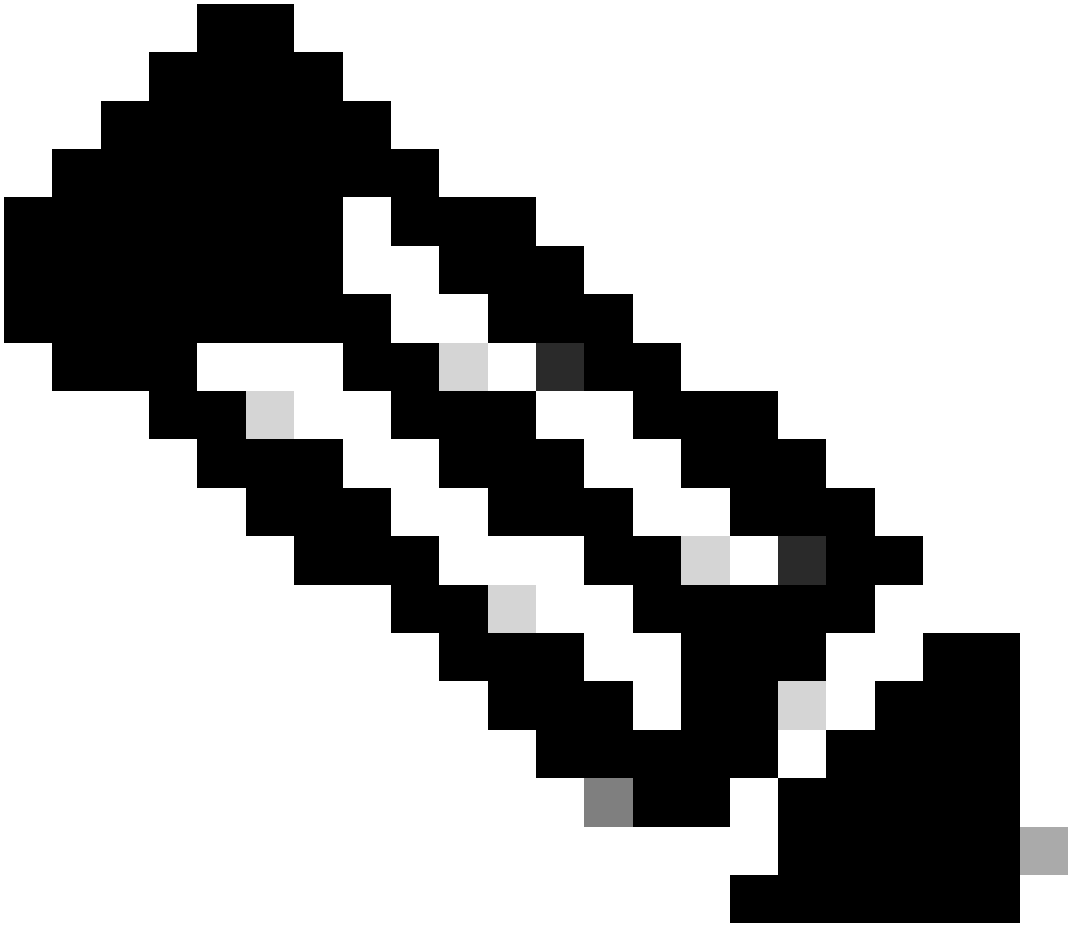
3. 등록 프로토콜로 ACME를 선택합니다.

- Enrollment Mode(등록 모드) 탭에서 Request from CA(CA에서 요청) 옵션을 선택합니다.
- Source Interface(소스 인터페이스)를 지정하고 Enrollment Protocol(등록 프로토콜)로 acme를 선택합니다.

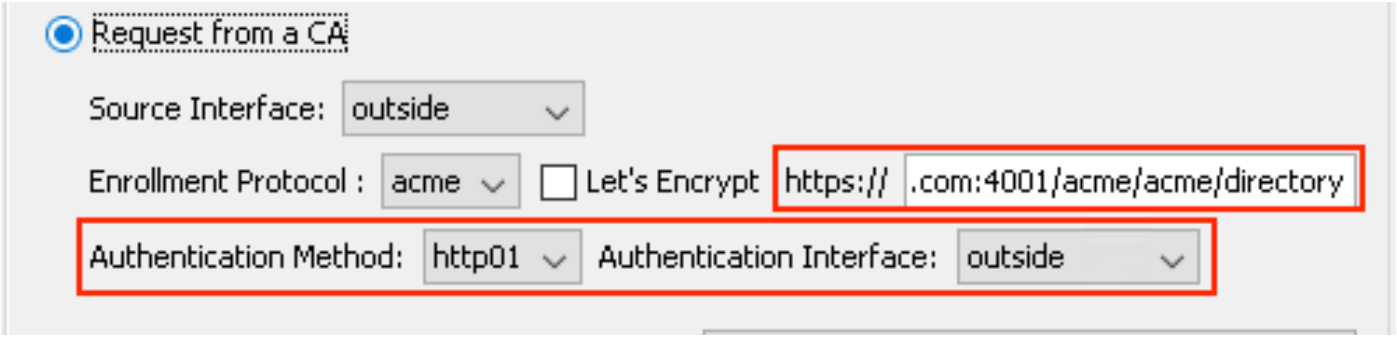


ACME 등록 ASDM acme 프로토콜. 선택

4. Let's Encrypt public CA에서 서명할 인증서에 대해 Let's Encrypt를 선택합니다. 그렇지 않으면 ACME 등록 프로토콜을 지원하는 내부 CA의 URL을 지정합니다. 또한 인증 인터페이스를 지정합니다.



참고: Let's Encrypt(암호화하겠습니다) 확인란을 선택하면 서버 URL이 자동으로 채워집니다.



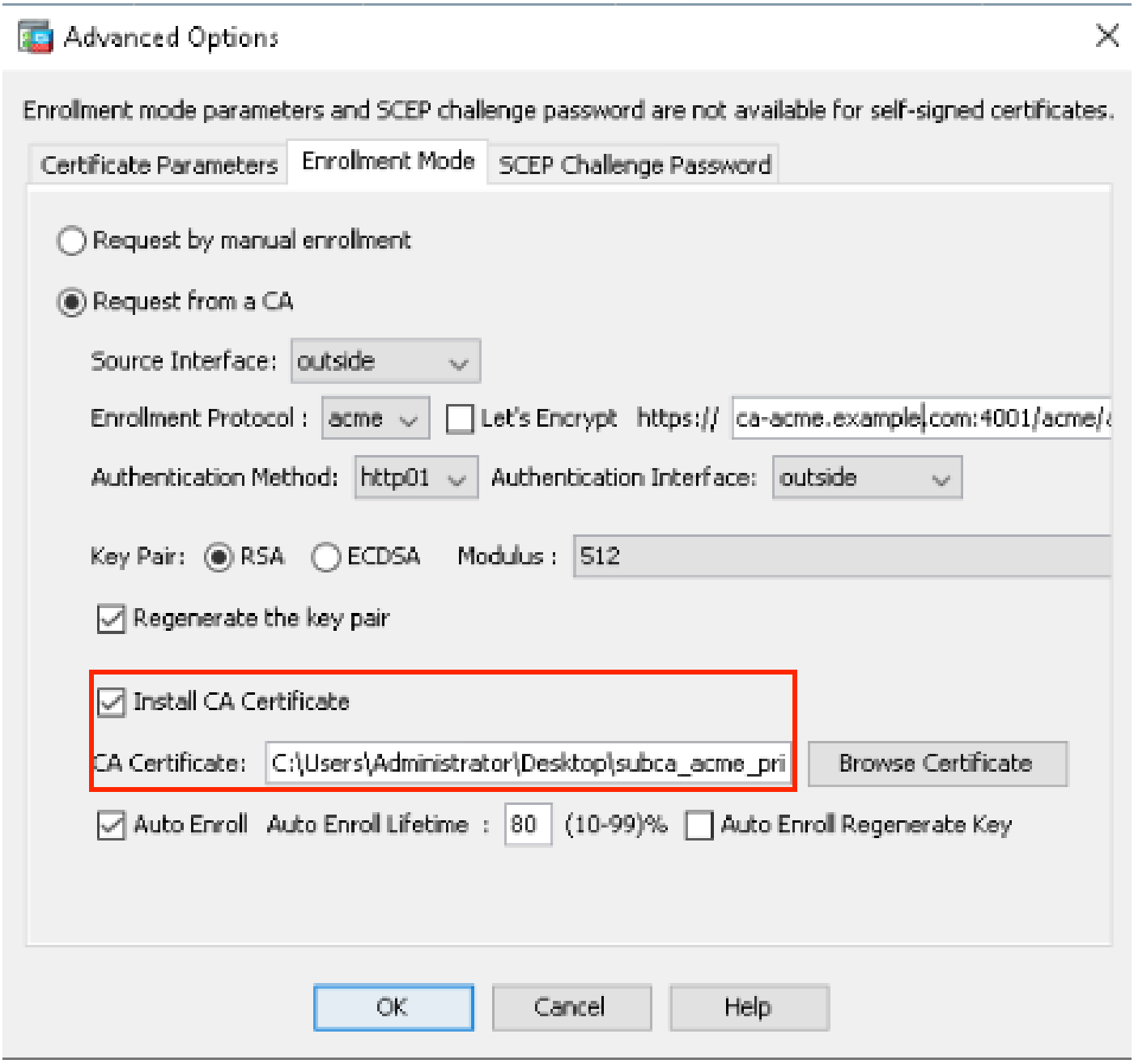
ACME 등록 ASDM 인증 방법

5. CA 인증서를 설치합니다.

Install CA Certificate(CA 인증서 설치) 옵션을 선택한 경우 인증서를 발급하는 즉시 CA의 인증서를 업로드해야 합니다.

참고: 이전 설치에서 또는 신뢰 풀 내에 CA 인증서가 이미 보안 방화벽에 있는 경우 이 옵션을 선택할 필요가 없습니다. Install CA Certificate(CA 인증서 설치) 확인란을 선택하지 않은 상태로 둡니다.

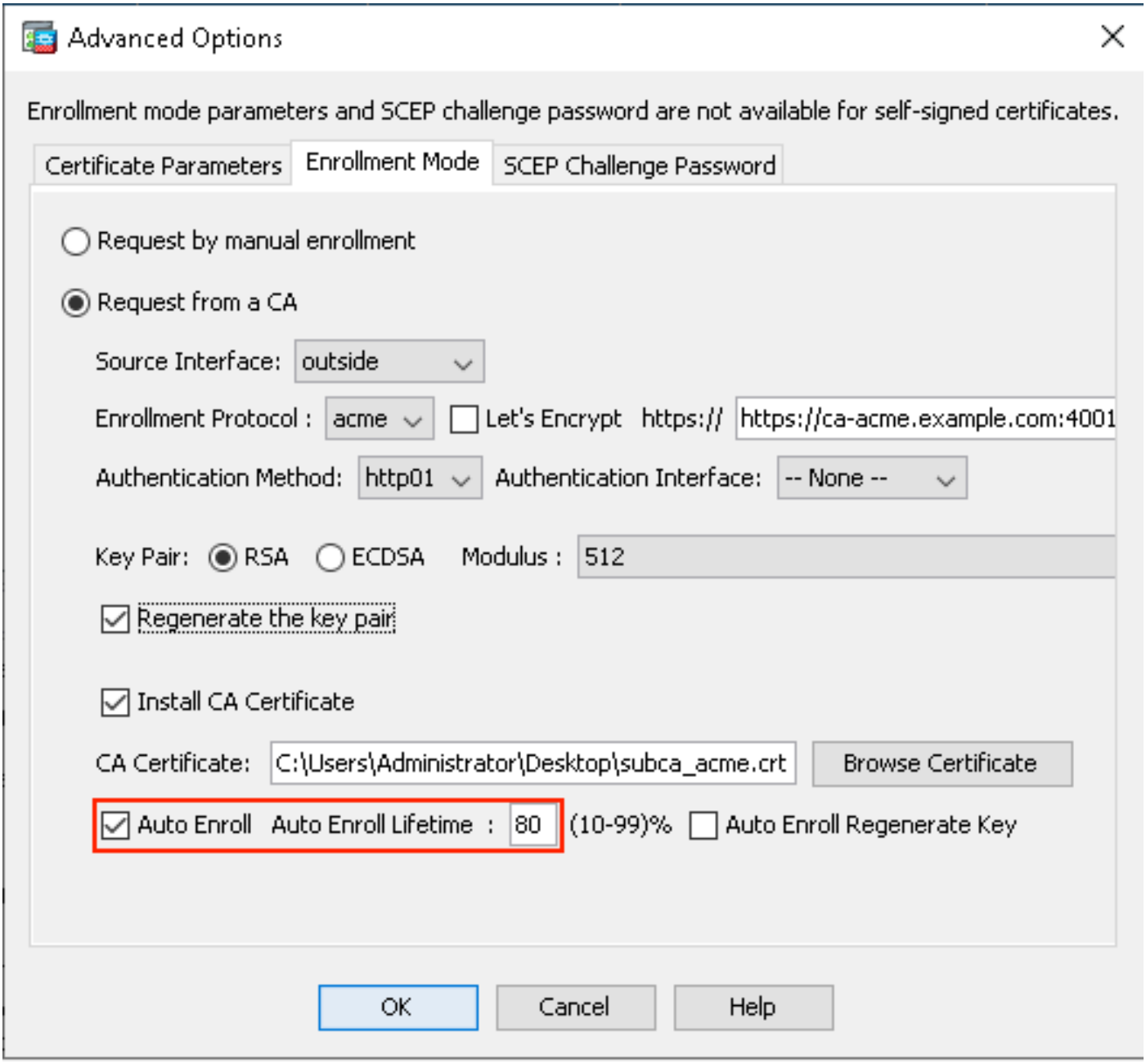
참고: Let's Encrypt 옵션을 선택한 경우 Let's Encrypt에 대한 루트 CA 인증서가 Secure Firewall 신뢰 풀에 이미 포함되어 있으므로 Install CA Certificate(CA 인증서 설치) 확인란을 선택하지 않은 상태로 둡니다.



6. (선택 사항) ID 인증서에 대한 자동 등록을 활성화합니다.

Auto Enroll(자동 등록) 확인란을 선택하고 Auto Enroll Lifetime(자동 등록 수명)의 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.



7. 확인을 클릭하고 구성을 저장합니다.

Secure Firewall ASA CLI를 사용한 ACME 등록

1. 새 신뢰 지점을 생성합니다.

신뢰 지점을 생성하고 등록 프로토콜로 acme를 지정합니다.

<#root>

```
asav(config)# crypto ca trustpoint private_acme
asav(config-ca-trustpoint)# enrollment protocol ?

crypto-ca-trustpoint mode commands/options:

acme Automatic Certificate Management Environment

  cmp Certificate Management Protocol Version 2
  est Enrollment over Secure Transport
  scep Simple Certificate Enrollment Protocol
```

2. 도메인 제어를 확인하려면 인증을 위한 HTTP-01 방법을 선택합니다.

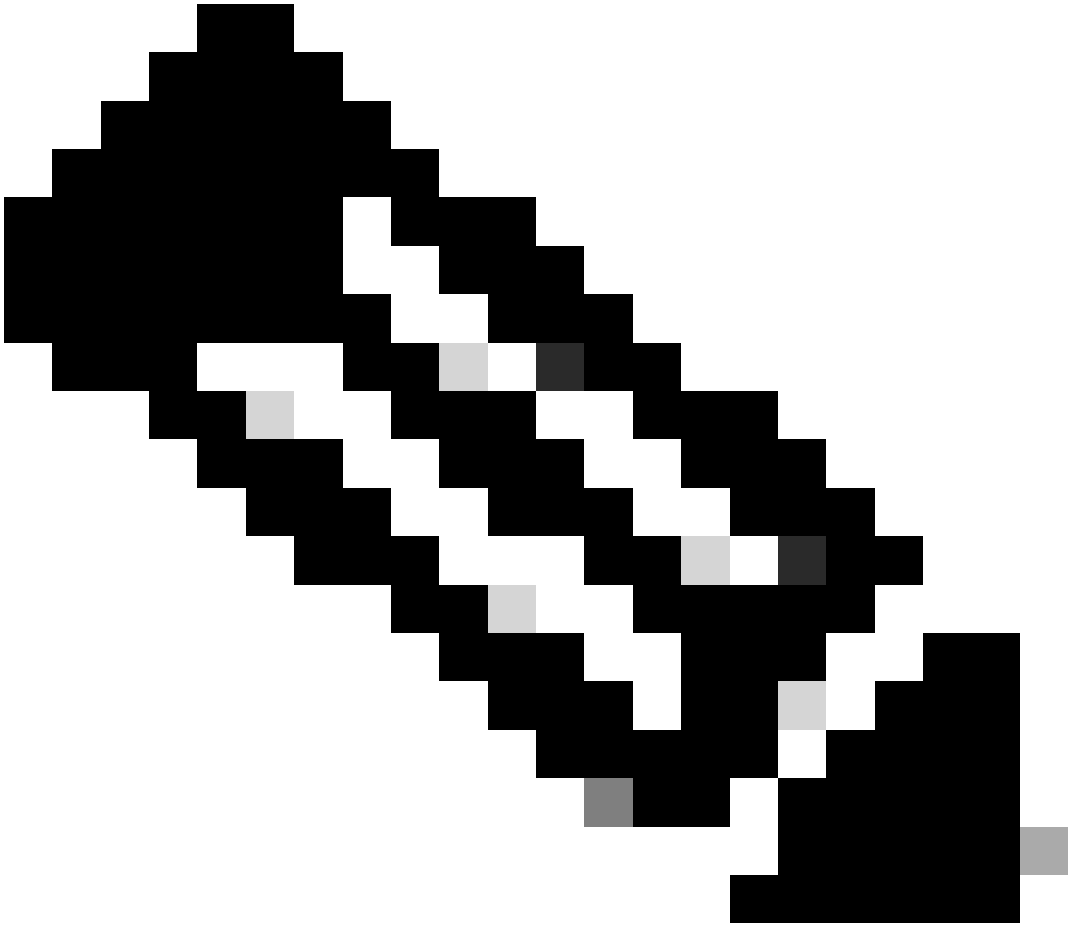
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

crypto-ca-trustpoint mode commands/options:
http01 Use the HTTP-01 method, which opens port 80 on the specified
interface
```

3. Let's Encrypt as the ACME CA를 선택합니다. ACME 프로토콜을 지원하는 다른 CA를 사용하는 경우 적절한 URL을 제공합니다.

```
asav(config-ca-trustpoint)# enrollment protocol acme url ?

crypto-ca-trustpoint mode commands/options:
LINE < 477 char URL
LetsEncrypt Use the Let's Encrypt CA
```



참고: LetsEncrypt 키워드가 구성되면 Let's Encrypt 서버 URL이 자동으로 채워집니다.

4. 인증서의 RSA 키 쌍, FQDN(Fully Qualified Domain Name) 및 주체 이름을 정의합니다.

```
crypto ca trustpoint private_acme
 enrollment interface outside
 enrollment protocol acme authentication http01 outside
 enrollment protocol acme url https://ca-acme.example.com:4001/acme/acme/directory
 fqdn fj-asav.cisco.com
 subject-name CN=fj-asav.example.com
 keypair rsa modulus 4096
 auto-enroll 80 regenerate
 crl configure
```

5. 신뢰 지점 인증

참고: CA가 보안 방화벽에 이미 있거나 Let's Encrypt를 사용할 경우 이 단계를 건너뛸 수 있습니다.

```
asav(config)# crypto ca authenticate private_acme
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIBwzCCAWqgAwIBAgIQedxaTD0J1G6tLgAGti6tizAKBggqhkjOPQQDAjAsMRAw
DgYDVQQKEwdjYS1hY21lMRgwFgYDVQQDEw9jYS1hY21lIFJvb3QgQ0EwHhcNMjQx
[truncated]
ADBEAiB7S4YZfnOK82K2yz5F5CzMe2t98LCpLRzoPJXMo7um1AIgH+K8EZMLstLN
AJQoplycJENo5D7kUmVrwUBBjREqv9I=
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: 40000000 40000000 40000000 40000000
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

6. 인증서 등록

```
asav(config)# crypto ca enroll private_acme
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=fj-asav.cisco.com

% The fully-qualified domain name in the certificate will be: fj-asav.example.com

% Include the device serial number in the subject name? [yes/no]: no

Request certificate from CA? [yes/no]: yes
```

다음을 확인합니다.

ASA에 설치된 인증서 보기

인증서가 등록되었는지 확인하고 갱신 날짜를 확인합니다.

```
asav# show crypto ca certificates private_acme
CA Certificate
Status: Available
```

```
Certificate Serial Number: 79d000000000000000000008b
Certificate Usage: General Purpose
Public Key Type: ECDSA (256 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Root CA
O=ca-acme
Subject Name:
CN=ca-acme Intermediate CA
O=ca-acme
Validity Date:
start date: 23:20:19 UTC Nov 26 2024
end date: 23:20:19 UTC Nov 24 2034
Storage: config
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: 8c8200000000000000000000000000000000000077
SHA1 PublicKeyInfo hash: 974c0000000000000000000000000000000009e1

Certificate
Status: Available
Certificate Serial Number: 666000000000000000000000000000be
Certificate Usage: General Purpose
Public Key Type: RSA (4096 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Intermediate CA
O=ca-acme
Subject Name:
CN=fj-asav.example.com
Validity Date:
start date: 20:51:00 UTC Feb 14 2025
end date: 20:52:00 UTC Feb 15 2025
renew date: 16:03:48 UTC Feb 15 2025
Storage: immediate
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: e6e000000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e300000000000000000000000000000000009f
```

Syslog 이벤트

ACME 프로토콜을 사용하는 인증서 등록과 관련된 이벤트를 캡처하기 위한 새로운 syslog가 보안 방화벽에 있습니다.

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

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

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

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

- 717069: ACME 등록 실패 시 정보 제공

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

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

```
%ASA-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.

- 서버 연결 확인: Secure Firewall이 ACME 서버에 네트워크로 연결되어 있는지 확인합니다. 통신을 차단하는 네트워크 문제 또는 방화벽 규칙이 없는지 확인합니다.
- 보안 방화벽 도메인 이름을 확인할 수 있는지 확인합니다. ACME 서버에서 보안 방화벽에 구성된 도메인 이름을 확인할 수 있는지 확인합니다. 이 확인은 서버에서 요청을 검증하는 데 중요합니다.
- 도메인 소유권 확인: 신뢰 지점에 지정된 모든 도메인 이름이 보안 방화벽에서 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>

일반적인 ACME 등록 오류:

오류 코드	이유	가능한 원인 또는 치료
7	서버에 연결할 수 없습니다.	서버에 연결할 수 있지만 ACME 서비스가 실행되고 있지 않습니

		다.
28	서버에 연결할 수 없습니다.	서버에 연결할 수 없습니다. ACME 서버에 대한 기본 네트워크 액세스를 확인합니다.
60	서버 인증서를 검증할 수 없습니다.	루트 또는 발급자 CA가 신뢰 지점 또는 신뢰 풀에 있는지 확인합니다.
124	ACME 처리 시간 초과	요청된 모든 FQDN이 HTTP-01 인증을 위해 구성된 인터페이스로 확인되어야 합니다. 구성된 ACME URL이 올바른지 확인합니다.

관련 정보

추가 지원이 필요한 경우 TAC에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco 전 세계 지원 문의처.
여기서 Cisco VPN Community를 방문할 수도 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.