

LSC를 사용하는 PEAP 또는 EAP-TLS에 대해 AP에 802.1X 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[Windows Server 2016 SCEP CA](#)

[인증서 템플릿 및 레지스트리 구성](#)

[9800에서 LSC 구성](#)

[AP LSC GUI 컨피그레이션 단계](#)

[AP LSC CLI 컨피그레이션 단계](#)

[AP LSC 확인](#)

[LSC 프로비저닝 문제 해결](#)

[LSC를 사용하는 AP 유선 802.1X 인증](#)

[AP 유선 802.1x 인증 컨피그레이션 단계](#)

[AP 유선 802.1x 인증 GUI 컨피그레이션](#)

[AP 유선 802.1x 인증 CLI 컨피그레이션](#)

[AP 유선 802.1x 인증 스위치 컨피그레이션](#)

[RADIUS 서버 인증서 설치](#)

[AP 유선 802.1x 인증 확인](#)

[802.1X 인증 문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 802.1X PEAP 또는 EAP-TLS 방법을 사용하여 스위치 포트에서 Cisco 액세스 포인트를 인증하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 무선 컨트롤러

- 액세스 포인트
- 스위치
- ISE 서버
- 인증 기관.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 무선 컨트롤러: 17.09.02를 실행하는 C9800-40-K9
- 액세스 포인트: C9117AXI-D
- 스위치: 17.06.04를 실행하는 C9200L-24P-4G
- AAA 서버: 3.1.0.518을 실행하는 ISE-VM-K9
- 인증 기관: Windows Server 2016

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

액세스 포인트(AP)가 802.1X를 사용하여 스위치 포트에 인증하도록 하려면 기본적으로 인증서가 필요하지 않은 EAP-FAST 인증 프로토콜을 사용합니다. AP가 PEAP-mschapv2 방법(AP 측에서는 자격 증명을 사용하지만 RADIUS 측에서는 인증서를 사용) 또는 EAP-TLS 방법(양측에서 인증서를 사용)을 사용하도록 하려면 먼저 LSC를 구성해야 합니다. 액세스 포인트에 신뢰할 수 있는/루트 인증서를 프로비저닝하는 유일한 방법입니다(EAP-TLS의 경우 디바이스 인증서도 제공). AP가 PEAP를 수행하고 서버 측 검증을 무시하는 것은 불가능합니다. 이 문서에서는 먼저 LSC를 구성한 다음 802.1X 컨피그레이션 측면에 대해 다룹니다.

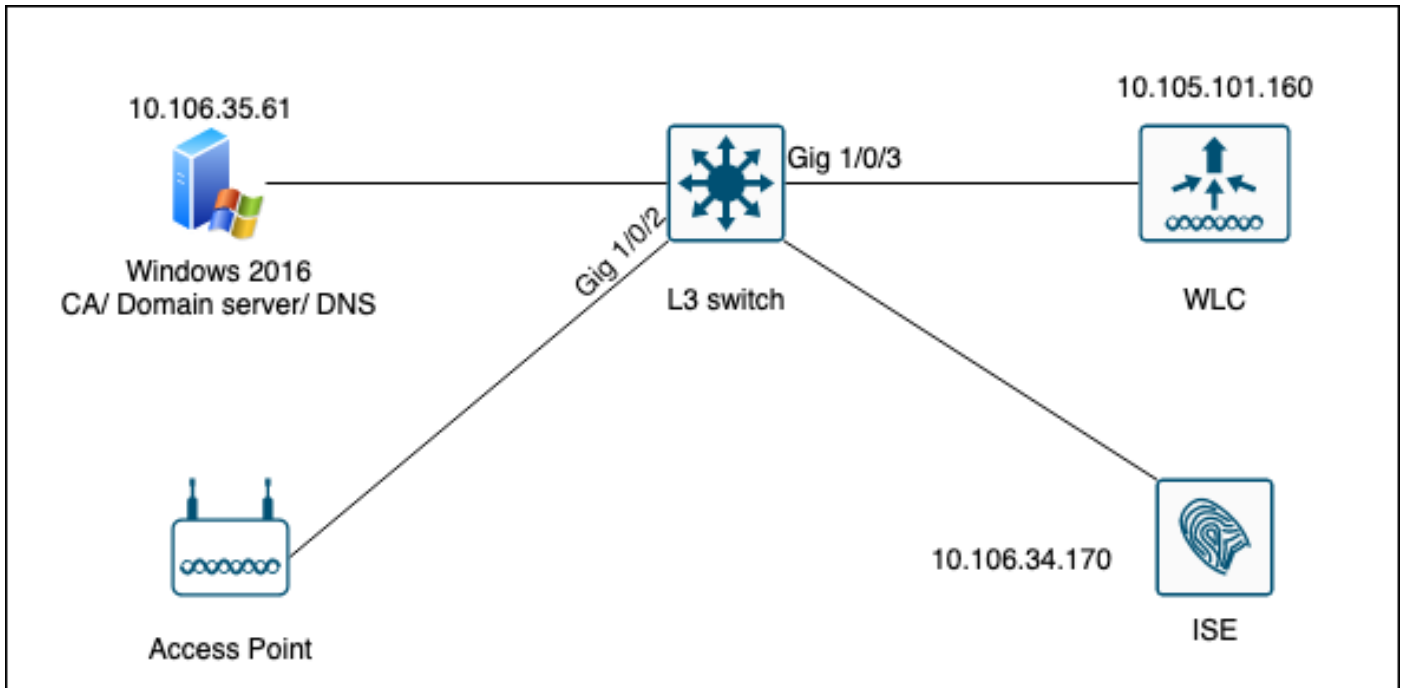
PKI가 더 나은 보안을 제공하고, CA(Certificate Authority)를 제어하고, 생성된 인증서에 대한 정책, 제한 및 사용을 정의하려면 LSC를 사용합니다.

LSC를 사용하면 컨트롤러는 CA에서 발급한 인증서를 받습니다. AP는 CA 서버와 직접 통신하지 않지만 WLC는 조인하는 AP를 대신하여 인증서를 요청합니다. CA 서버 세부사항은 컨트롤러에서 구성해야 하며 액세스할 수 있어야 합니다.

컨트롤러는 SCEP(Simple Certificate Enrollment Protocol)를 사용하여 디바이스에서 생성된 certReq를 CA로 전달하고 SCEP를 다시 사용하여 CA에서 서명된 인증서를 가져옵니다.

SCEP는 PKI 클라이언트 및 CA 서버가 인증서 등록 및 취소를 지원하는 데 사용하는 인증서 관리 프로토콜입니다. Cisco에서 널리 사용되며 많은 CA 서버에서 지원됩니다. SCEP에서는 HTTP가 PKI 메시지의 전송 프로토콜로 사용됩니다. SCEP의 기본 목표는 네트워크 디바이스에 인증서를 안전하게 발급하는 것입니다.

네트워크 다이어그램



구성

SCEP CA와 9800 WLC의 두 가지 주요 구성 사항이 있습니다.

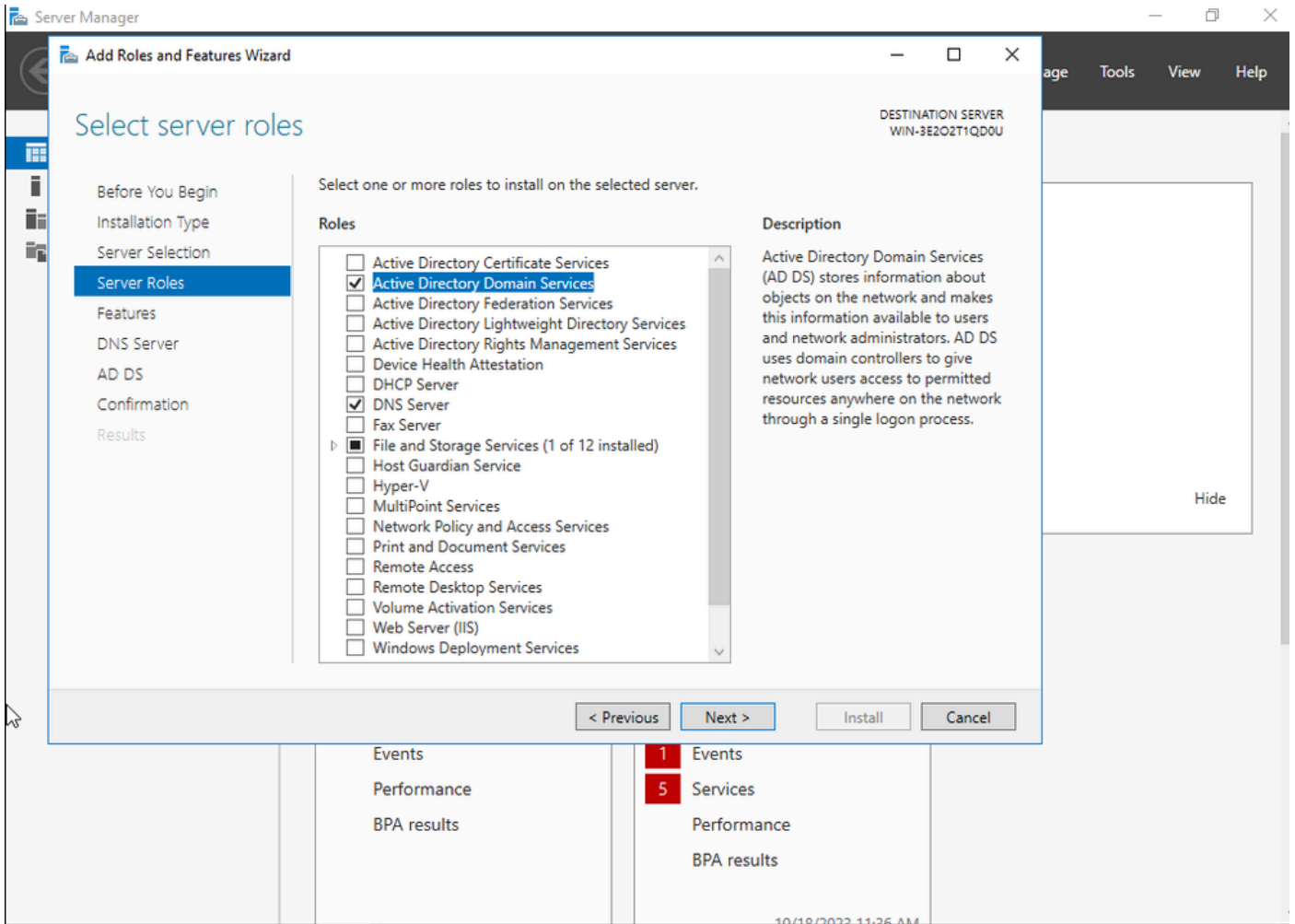
Windows Server 2016 SCEP CA

이 문서에서는 실습을 위한 Windows Server SCEP CA의 기본 설치에 대해 설명합니다. 실제 프로덕션 등급의 Windows CA는 기업 운영에 적합하도록 안전하고 적절하게 구성해야 합니다. 이 섹션에서는 Lab에서 테스트하고 이 컨피그레이션이 작동하도록 하는 데 필요한 설정에서 영감을 얻을 수 있습니다. 단계는 다음과 같습니다.

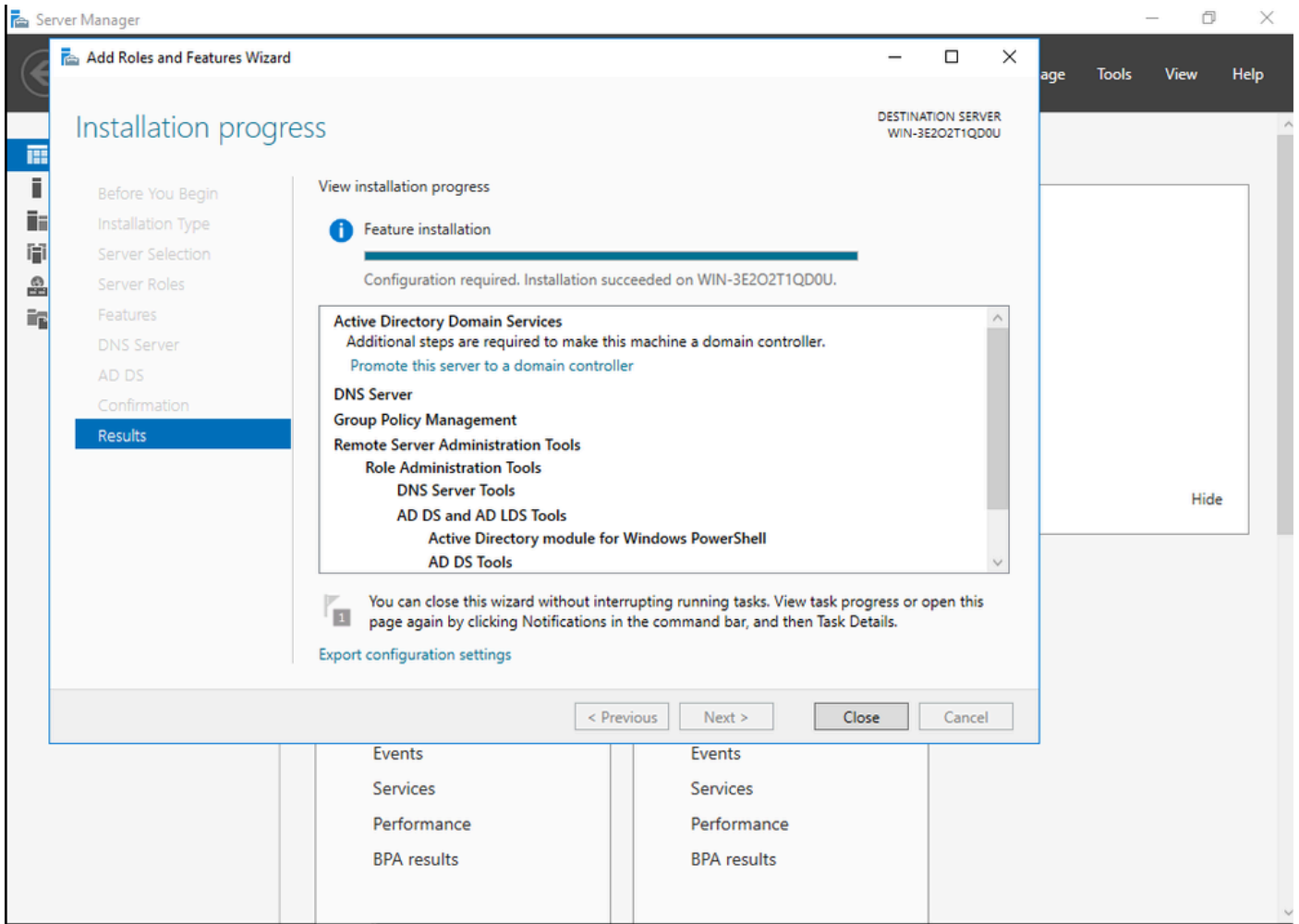
1단계. 새로운 Windows Server 2016 데스크톱 경험을 설치합니다.

2단계. 서버가 고정 IP 주소로 구성되어 있는지 확인합니다.

3단계. 새 역할 및 서비스를 설치하고 Active Directory 도메인 서비스 및 DNS 서버부터 시작합니다.

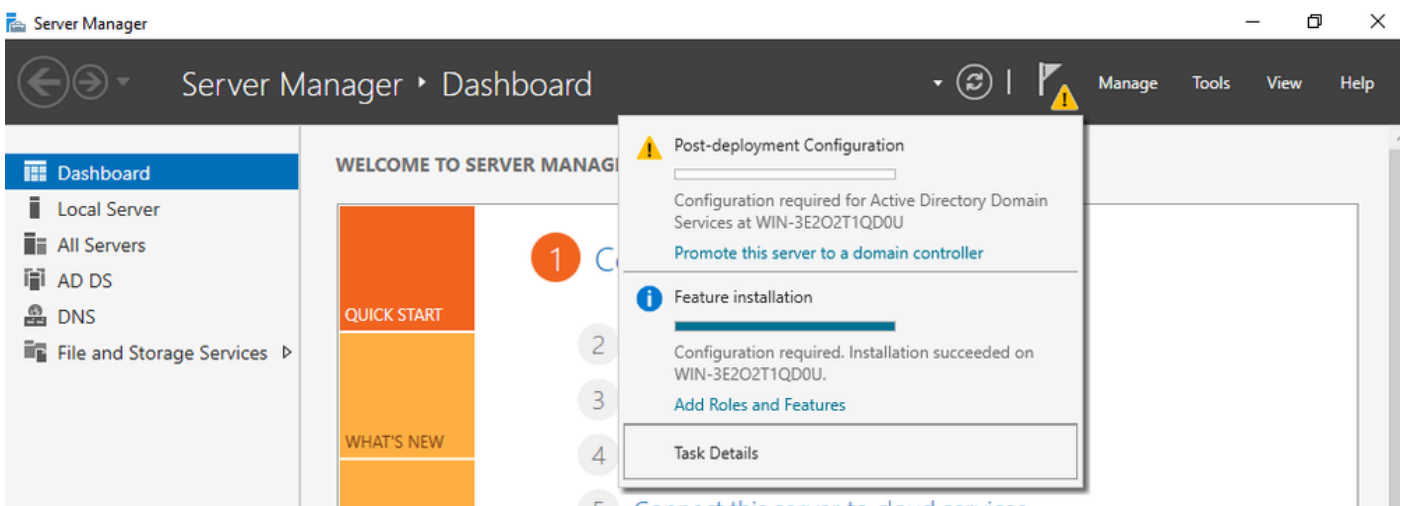


Active Directory 설치



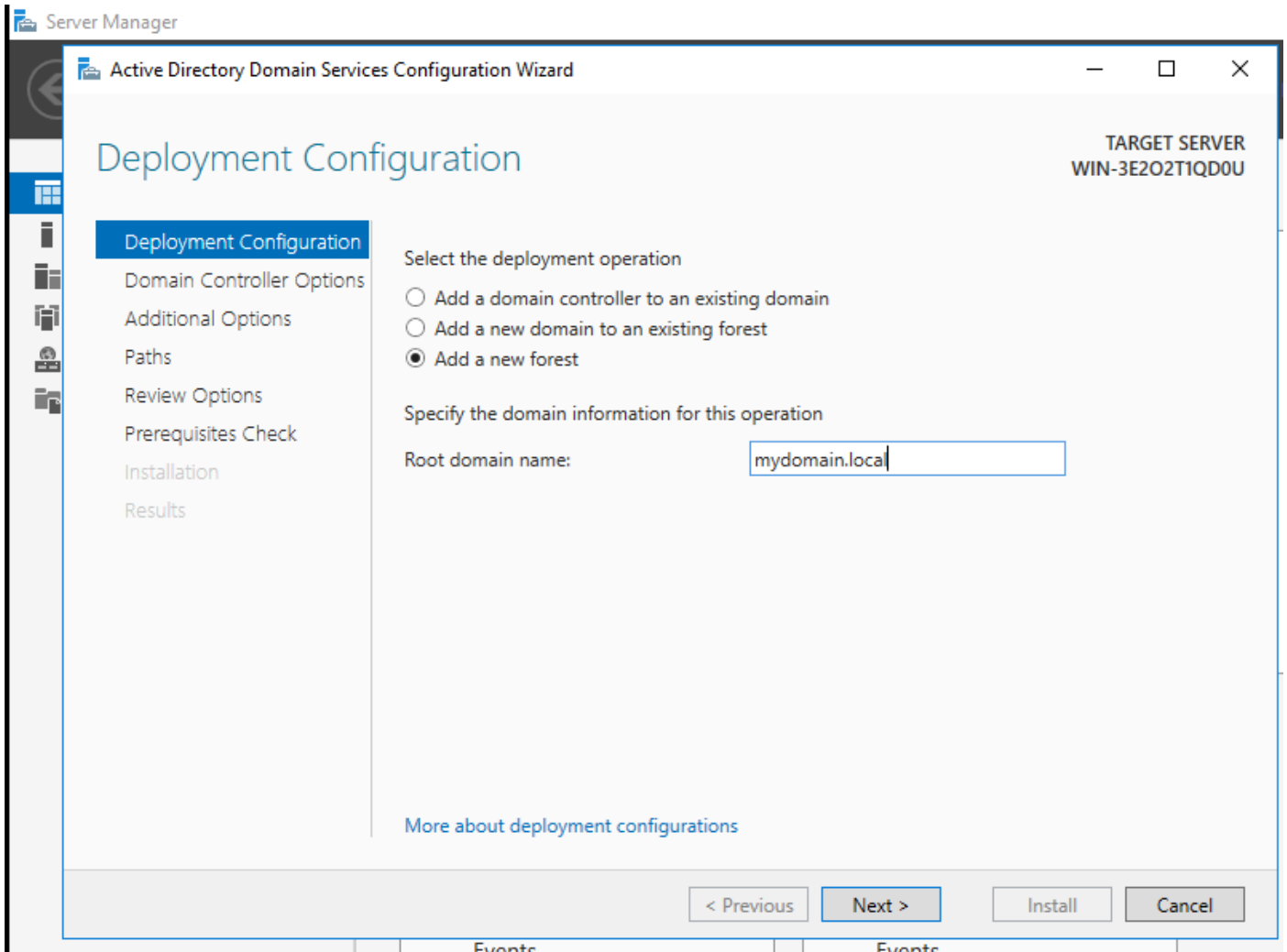
AD 설치 종료

4단계.작업이 완료되면 대시보드에서 Promote this server to a domain controller를 클릭합니다.



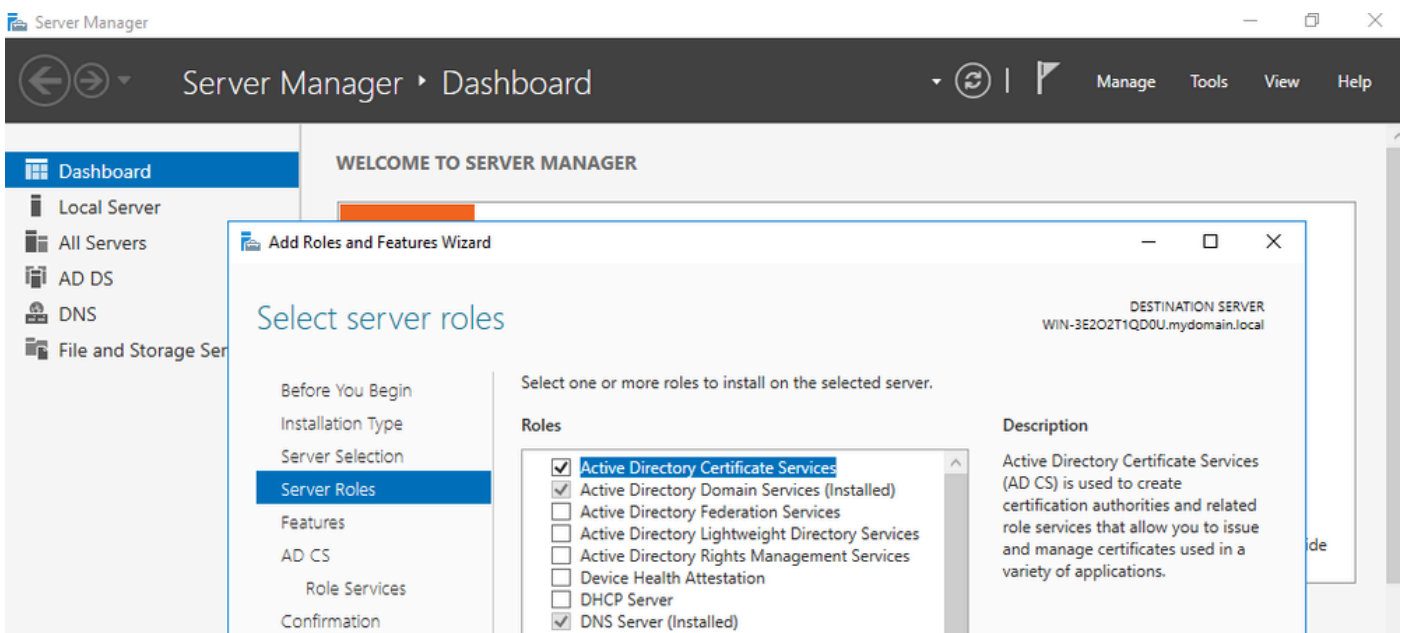
AD 서비스 구성

5단계.새 포리스트를 만들고 도메인 이름을 선택합니다.

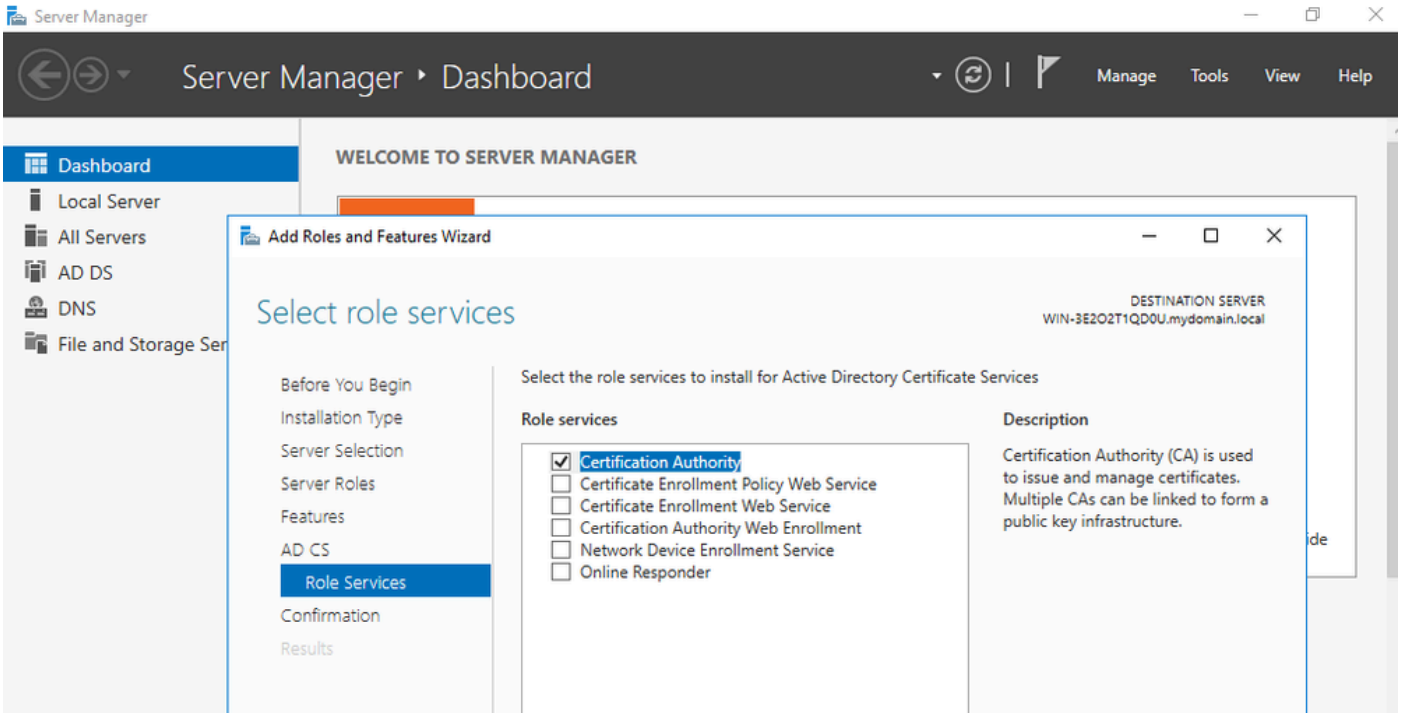


포리스트 이름 선택

6단계. 서버에 인증서 서비스 역할을 추가합니다.

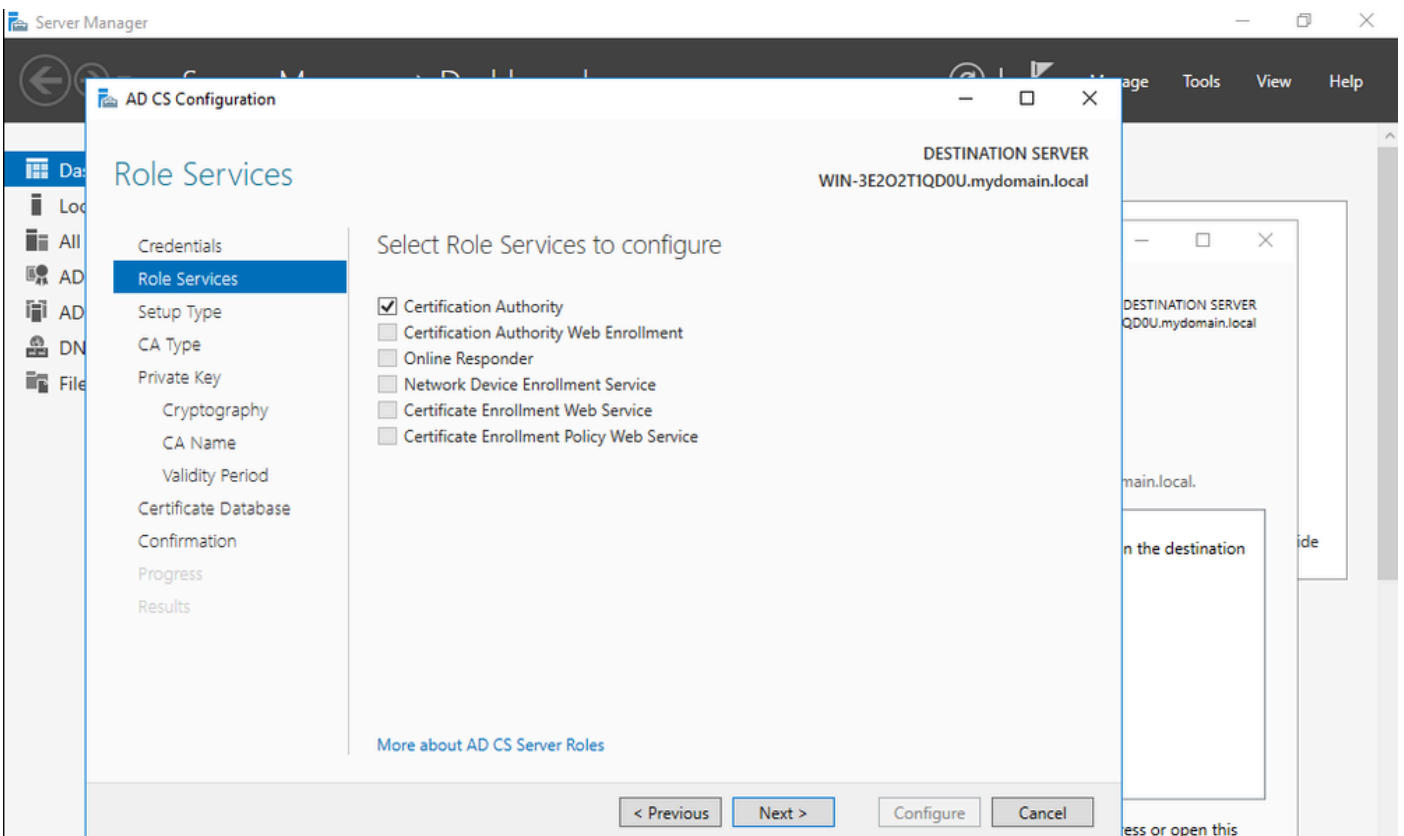


인증서 서비스 추가

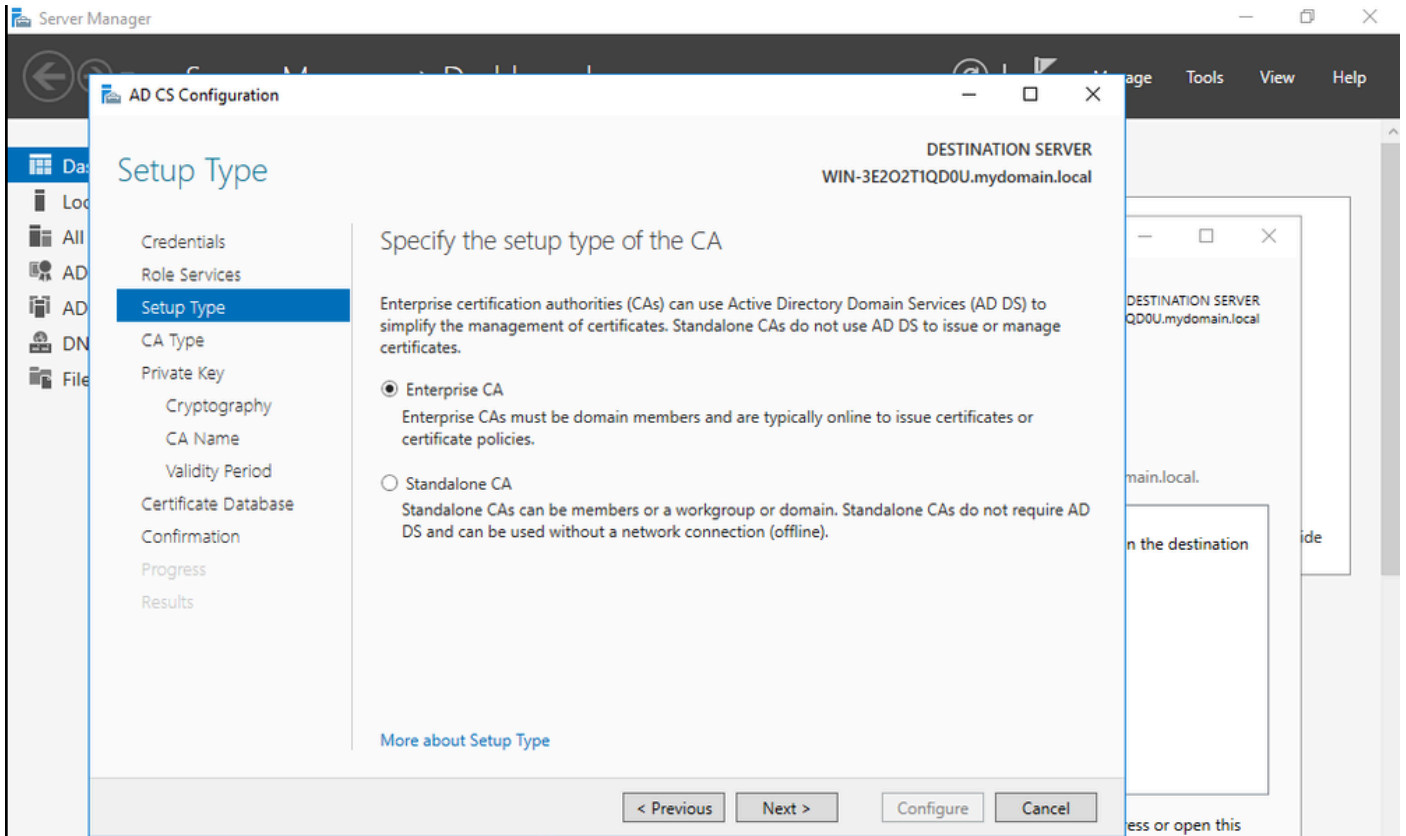


인증 기관만 추가

7단계.완료되면 인증 기관을 구성합니다.

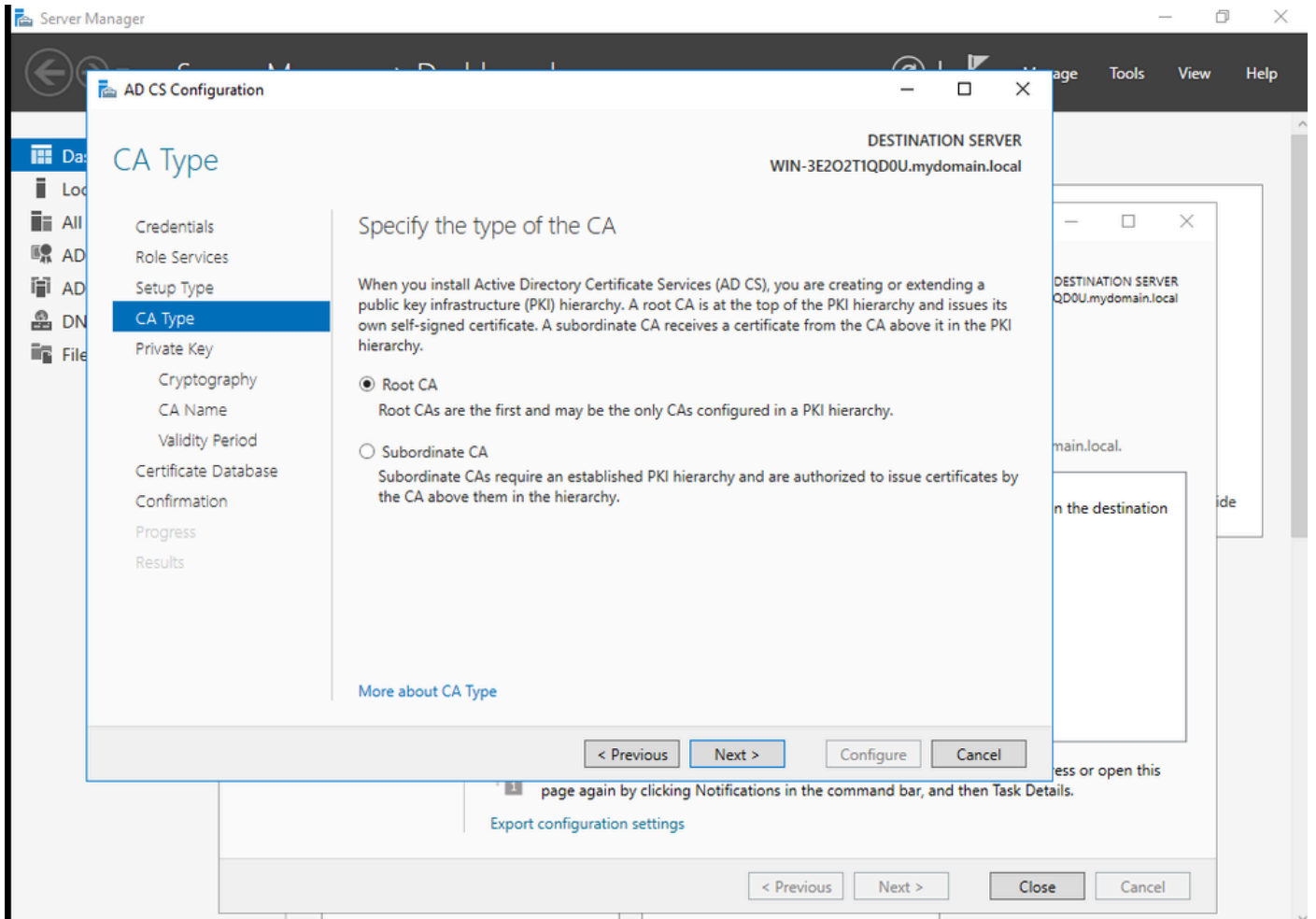


8단계.Enterprise CA를 선택합니다.



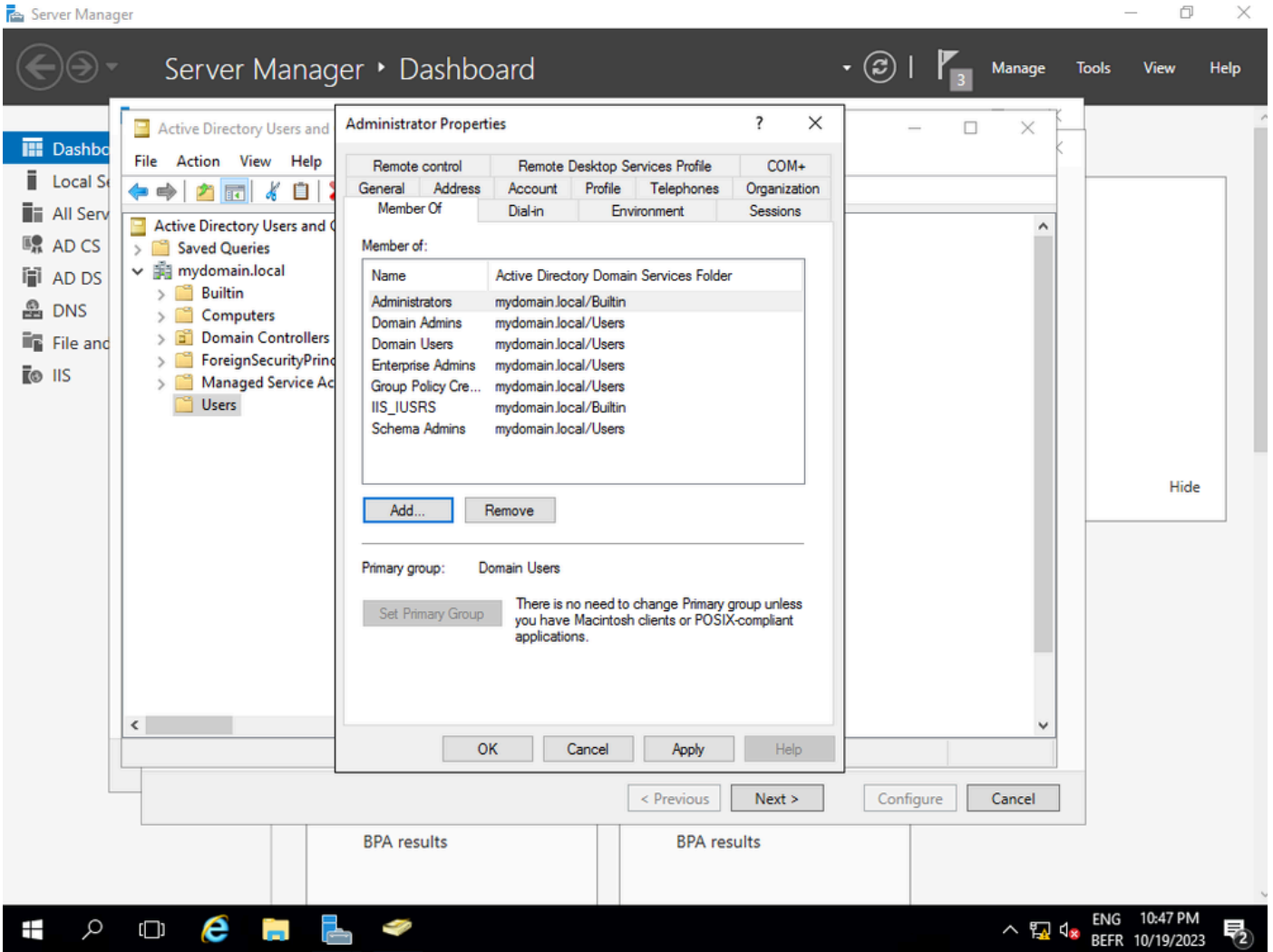
엔터프라이즈 CA

9단계.루트 CA로 설정합니다. Cisco IOS XE 17.6부터 LSC에 대해 하위 CA가 지원됩니다.



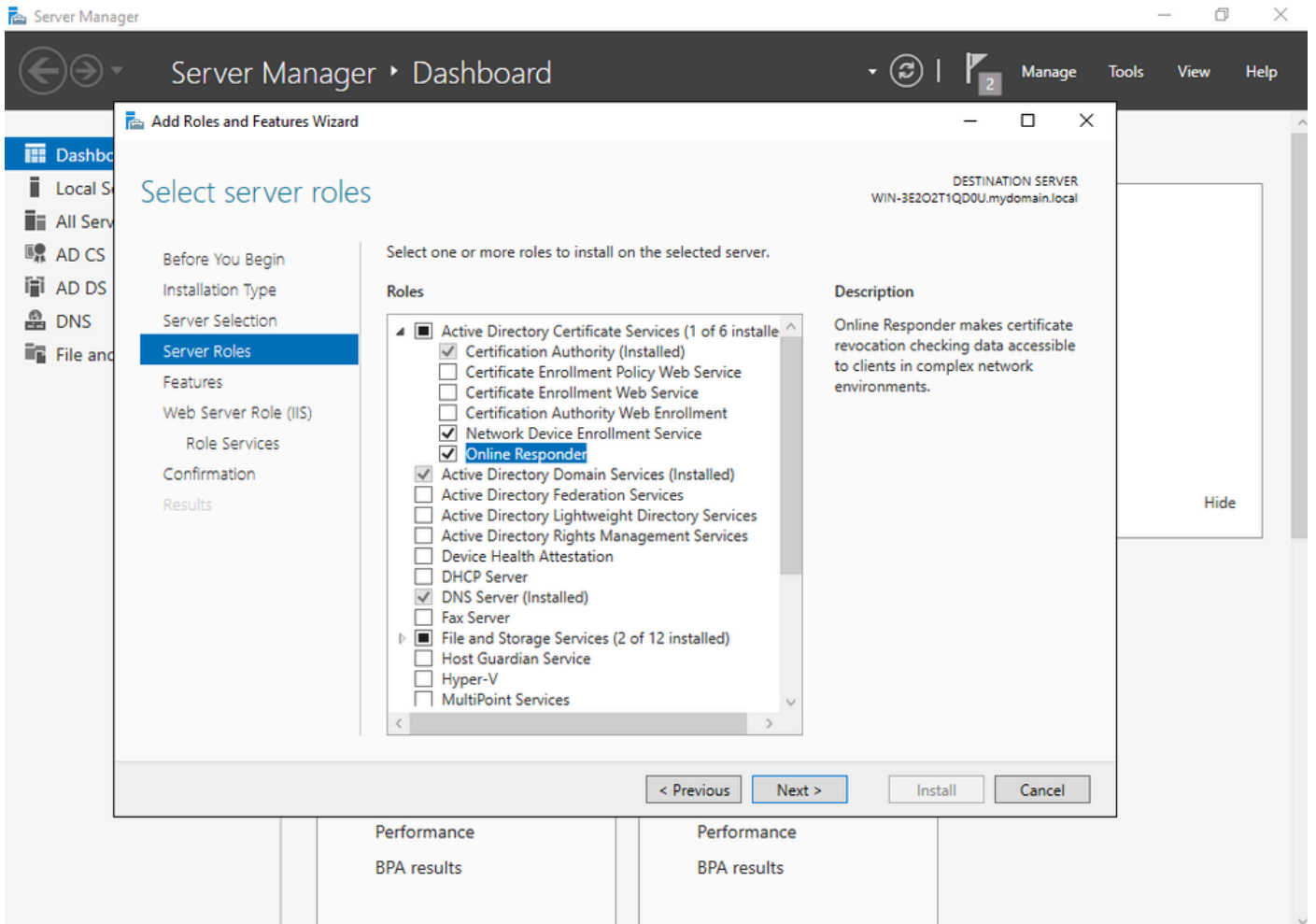
루트 CA 선택

CA가 IIS_IUSRS 그룹에 속하도록 하려면 해당 계정을 사용해야 합니다. 이 예에서는 관리자 계정을 사용하고 Active Directory 사용자 및 컴퓨터 메뉴로 이동하여 IIS_IUSRS 그룹에 관리자 사용자를 추가합니다.



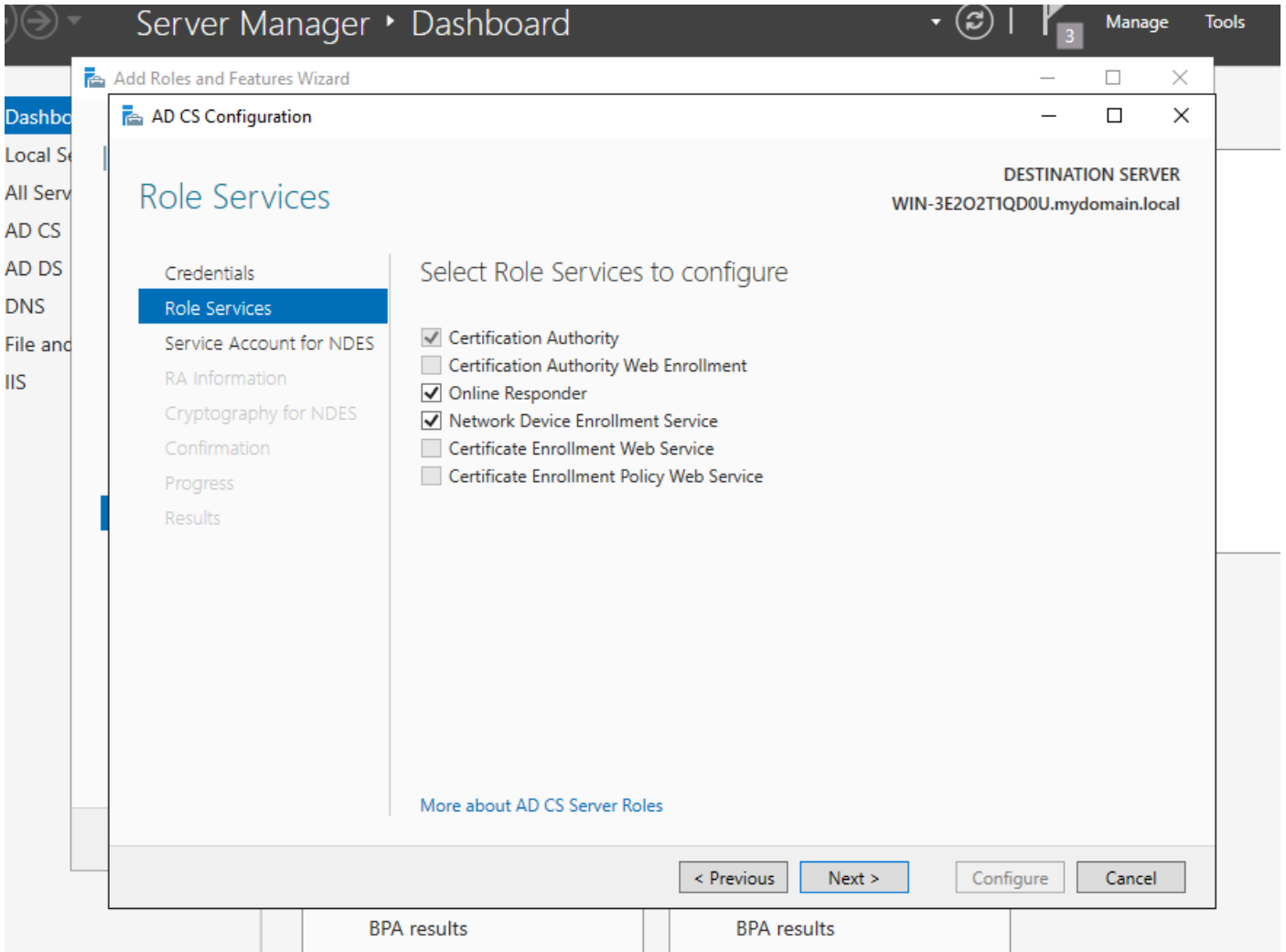
IIS_USER 그룹에 관리자 계정 추가

10단계.올바른 IIS 그룹에 사용자가 있으면 역할 및 서비스를 추가합니다. 그런 다음 인증 기관에 Online Responder 및 NDES 서비스를 추가합니다.



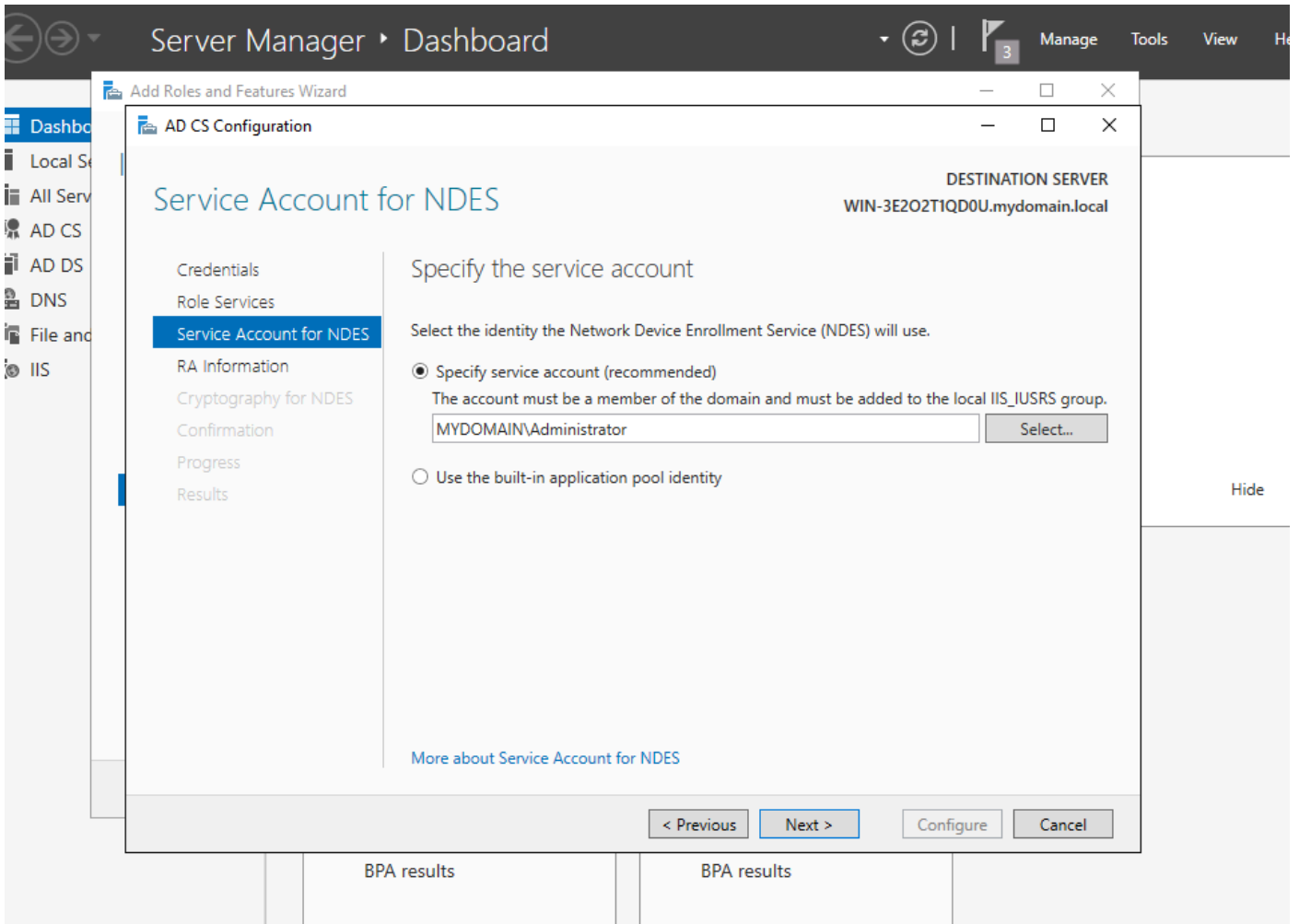
NDES 및 Online responder 서비스 설치

11단계. 완료되면 해당 서비스를 구성합니다.



온라인 응답기 및 NDES 서비스 설치

12단계.서비스 계정을 선택하라는 메시지가 표시됩니다. 이전에 IIS_IUSRS 그룹에 추가한 계정입니다.



IIS 그룹에 추가한 사용자 선택

13단계. 이 작업은 SCEP 작업에 충분하지만 802.1X 인증을 달성하려면 RADIUS 서버에 인증서도 설치해야 합니다. 따라서 Windows Server에서 ISE 인증서 요청을 쉽게 복사하여 붙여넣을 수 있도록 웹 등록 서비스를 쉽게 설치하고 구성합니다.

Select server roles

DESTINATION SERVER
WIN-3E202T1QD0U.mydomain.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services (3 of 6 installed)
 - Certification Authority (Installed)
 - Certificate Enrollment Policy Web Service
 - Certificate Enrollment Web Service
 - Certification Authority Web Enrollment
 - Network Device Enrollment Service (Installed)
 - Online Responder (Installed)
- Active Directory Domain Services (Installed)
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server (Installed)
- Fax Server
- File and Storage Services (2 of 12 installed)
 - Host Guardian Service
 - Hyper-V
 - MultiPoint Services

Description

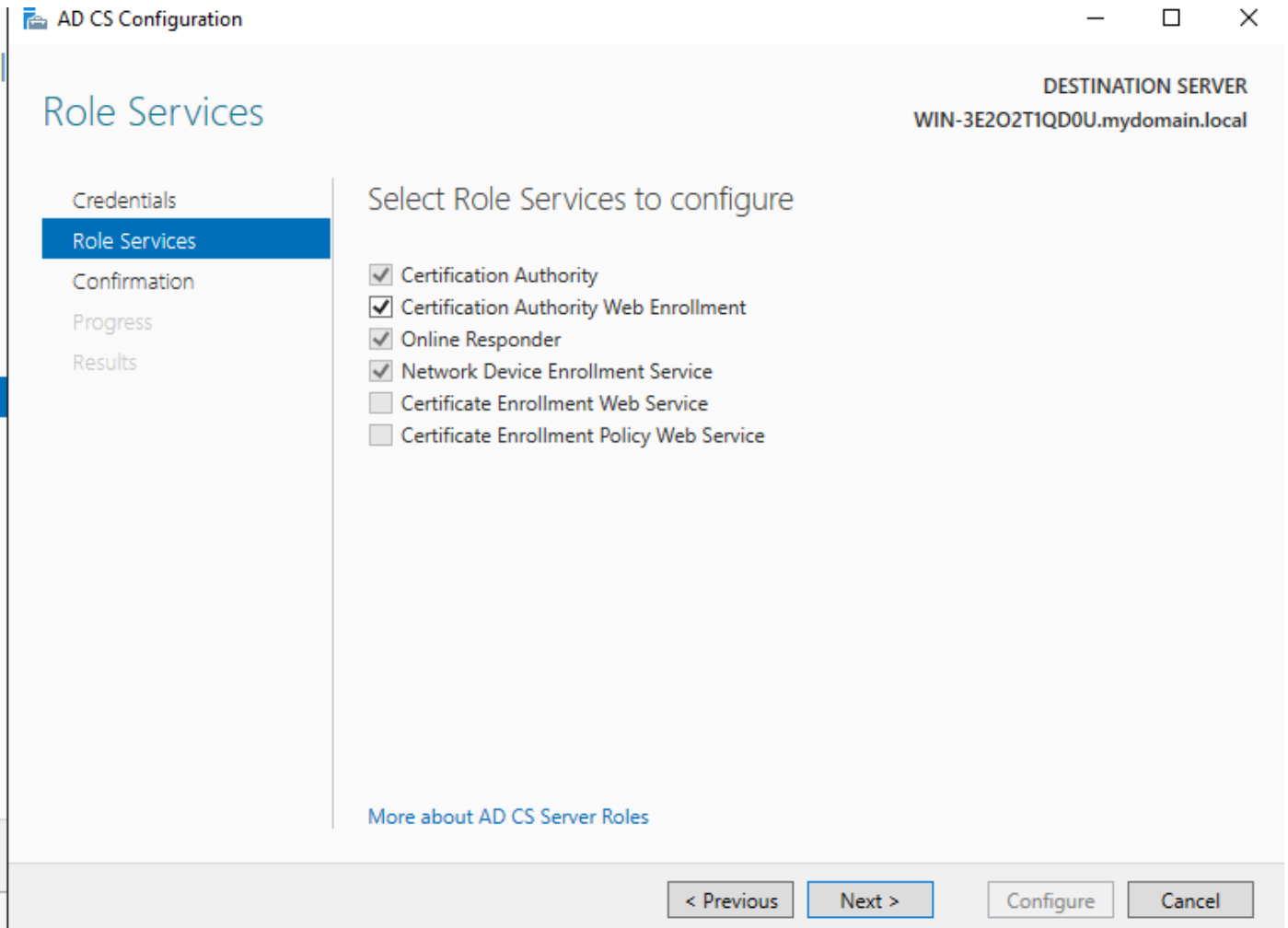
Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

< Previous

Next >

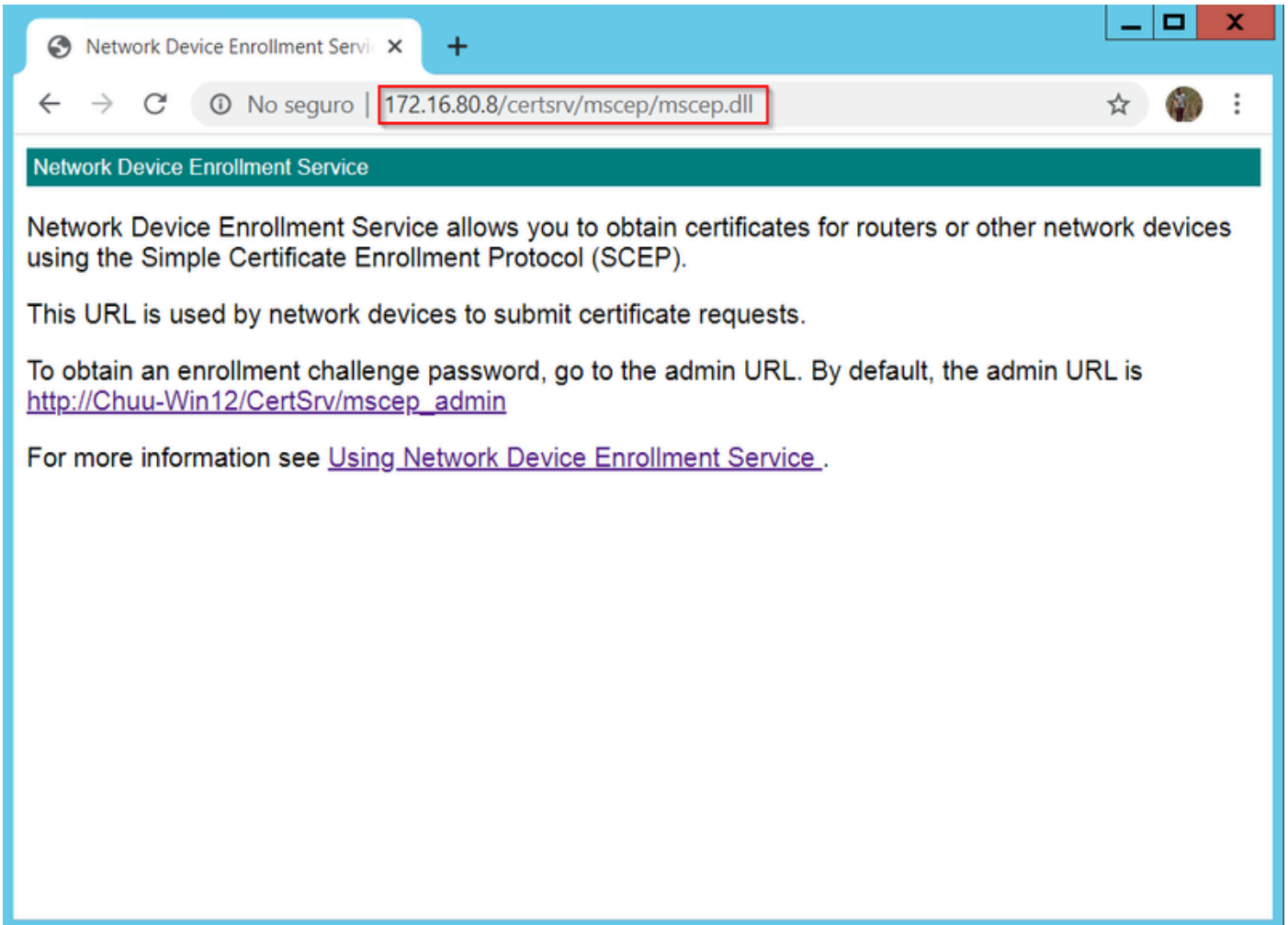
Install

Cancel



웹 등록 서비스 구성

14단계. <http://<serverip>/certsrv/mscep/mscep.dll>을 방문하여 SCEP 서비스가 제대로 작동하고 있는지 확인할 수 있습니다.



SCEP 포털 확인

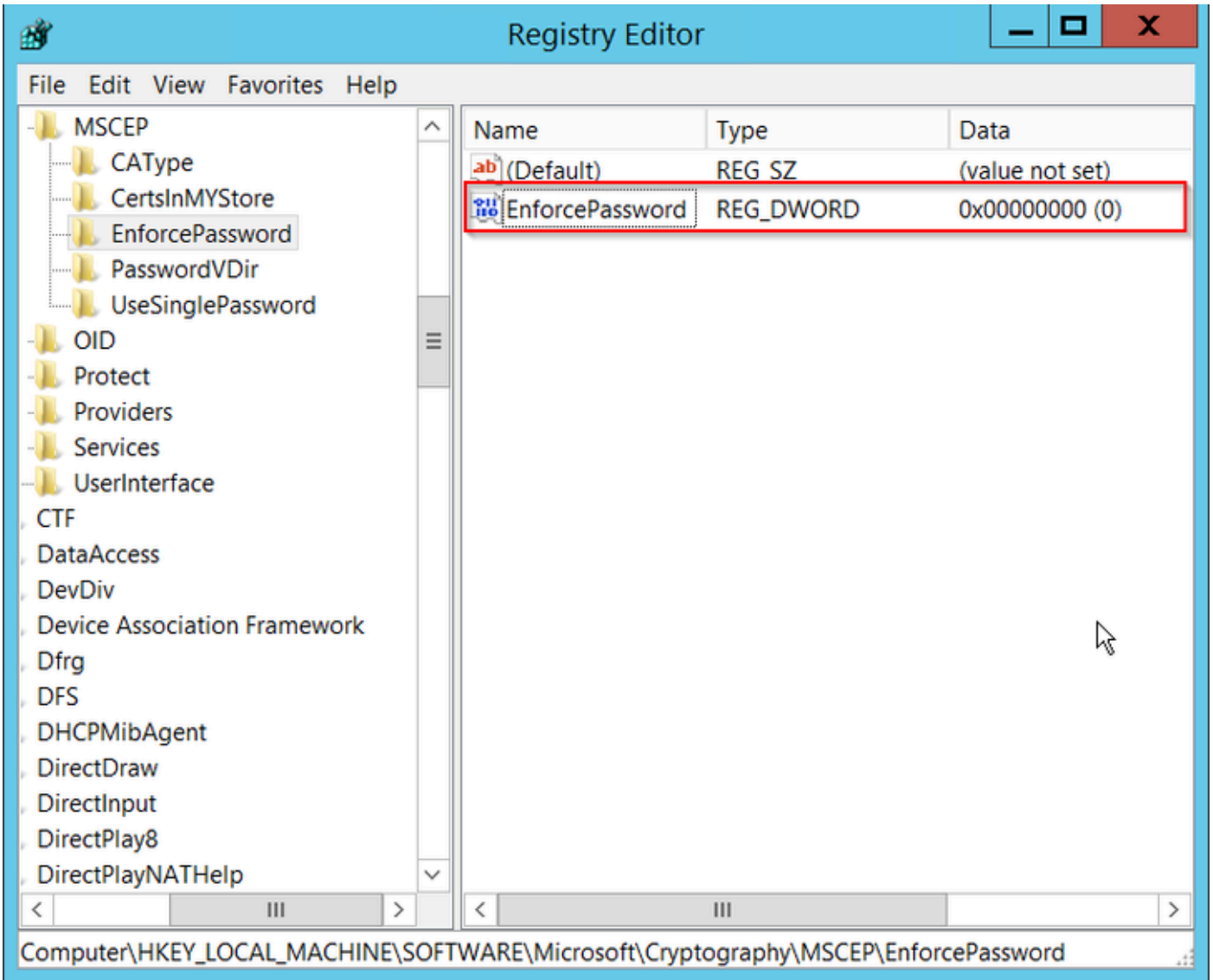
15단계.

기본적으로 Windows Server는 MSCEP(Microsoft SCEP) 내에서 등록하기 전에 클라이언트 및 엔드포인트 요청을 인증하는 데 동적 챌린지 암호를 사용했습니다. 이렇게 하려면 관리자 계정이 웹 GUI로 이동하여 각 요청에 대해 온디맨드 비밀번호를 생성해야 합니다(비밀번호는 요청 내에 포함되어야 함). 컨트롤러는 서버에 보내는 요청 내에 이 비밀번호를 포함할 수 없습니다. 이 기능을 제거하려면 NDES 서버의 레지스트리 키를 수정해야 합니다.

레지스트리 편집기를 열고 시작 메뉴에서 Regedit를 검색합니다.

Computer(컴퓨터) > HKEY_LOCAL_MACHINE > SOFTWARE(소프트웨어) > Microsoft > Cryptography(암호화) > MSCEP > EnforcePassword(비밀번호 적용)로 이동합니다.

EnforcePassword 값을 0으로 변경합니다. 이미 0이면 그대로 두십시오.



Enforcepassword 값 설정

인증서 템플릿 및 레지스트리 구성

인증서 및 연결된 키는 CA 서버 내의 애플리케이션 정책에 정의된 서로 다른 목적을 위해 여러 시나리오에서 사용될 수 있습니다. 애플리케이션 정책은 인증서의 EKU(Extended Key Usage) 필드에 저장됩니다. 인증자가 이 필드를 구문 분석하여 클라이언트가 해당 용도로 사용하는지 확인합니다. 적절한 애플리케이션 정책이 WLC 및 AP 인증서에 통합되도록 하려면 적절한 인증서 템플릿을 생성하고 이를 NDES 레지스트리에 매핑합니다.

1단계. Start(시작) > Administrative Tools(관리 툴) > Certification Authority(인증 기관)로 이동합니다.

2단계. CA Server(CA 서버) 폴더 트리를 확장하고 Certificate Templates(인증서 템플릿) 폴더를 마우스 오른쪽 버튼으로 클릭한 후 Manage(관리)를 선택합니다.

3단계. 사용자 인증서 템플릿을 마우스 오른쪽 단추로 클릭한 다음 컨텍스트 메뉴에서 Duplicate Template을 선택합니다.

4단계. General(일반) 탭으로 이동하여 템플릿 이름 및 유효 기간을 원하는 대로 변경하고 다른 모

든 옵션은 선택되지 않은 상태로 둡니다.



주의: 유효 기간을 수정할 경우 인증 기관 루트 인증서 유효보다 크지 않은지 확인합니다.

Properties of New Template



Subject Name		Server		Issuance Requirements	
Superseded Templates			Extensions		Security
Compatibility	General	Request Handling		Cryptography	Key Attestation

Template display name:

Template name:

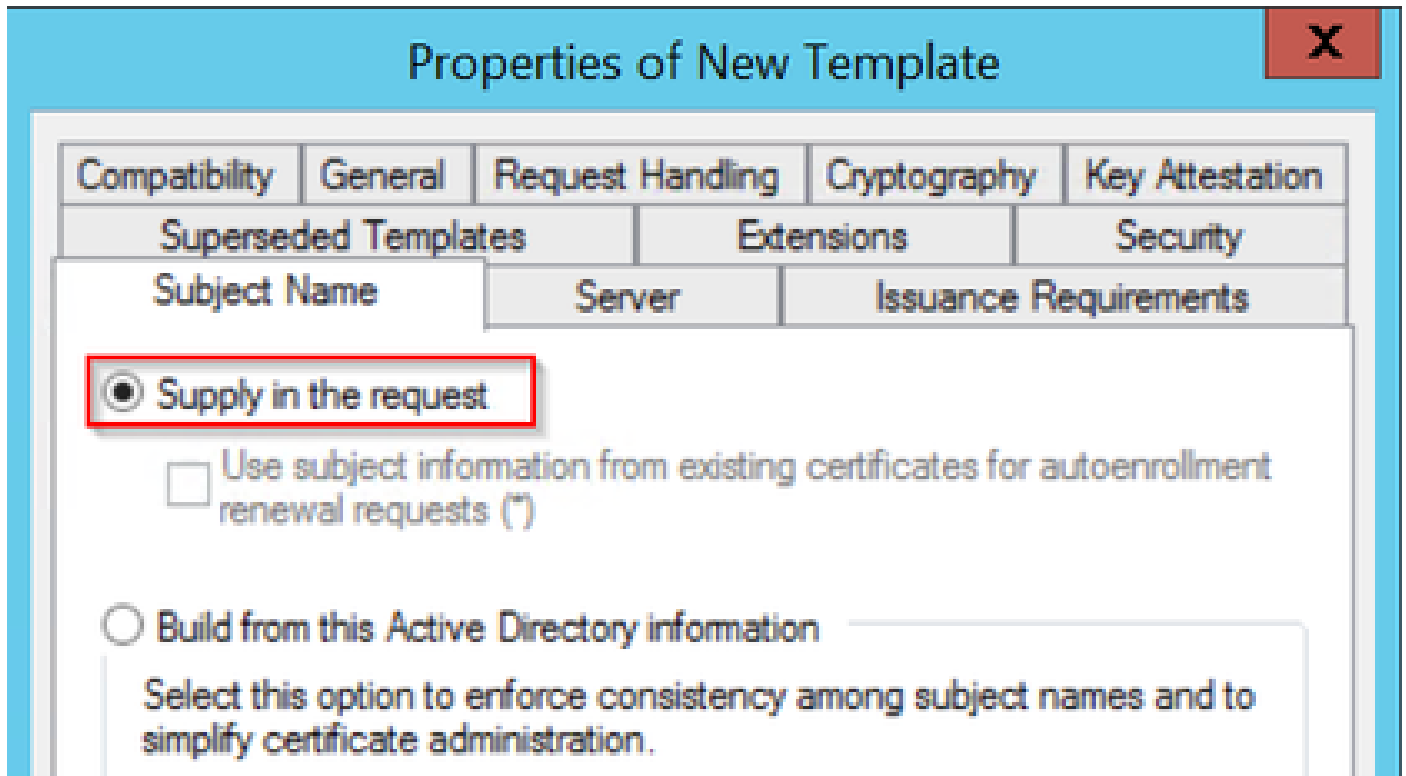
Validity period:

Renewal period:

Publish certificate in Active Directory

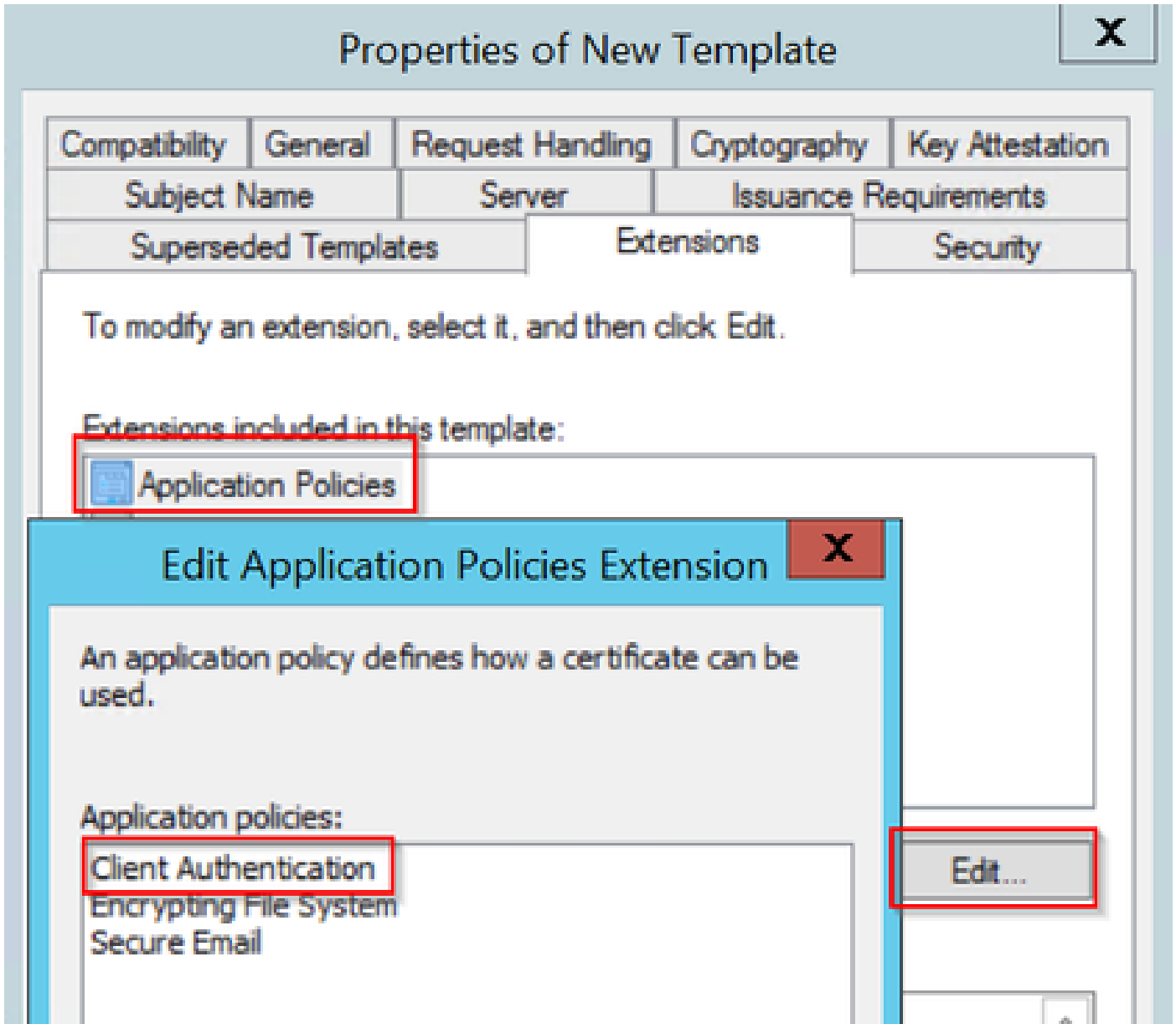
Do not automatically reenroll if a duplicate certificate exists in Active Directory

5단계. Subject Name(주체 이름) 탭으로 이동하여 요청의 Supply(공급)가 선택되었는지 확인합니다. 사용자가 인증서를 서명하기 위해 관리자 승인이 필요하지 않음을 나타내는 팝업이 나타나면 OK(확인)를 선택합니다.



요청의 공급

6단계. Extensions(확장) 탭으로 이동한 다음 Application Policies(애플리케이션 정책) 옵션을 선택하고 Edit...(편집..) 버튼을 선택합니다. 클라이언트 인증이 Application Policies(애플리케이션 정책) 창에 있는지 확인합니다. 그렇지 않으면 Add(추가)를 선택하여 추가합니다.



내선 번호 확인

7단계. Security(보안) 탭으로 이동하여 Windows Server에서 SCEP 서비스 활성화의 6단계에 정의된 서비스 계정에 템플릿의 전체 제어 권한이 있는지 확인한 다음 Apply(적용) 및 OK(확인)를 선택합니다.

Properties of New Template



Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server	Issuance Requirements	
Superseded Templates		Extensions		Security

Group or user names:

- Authenticated Users
- Administrator**
- Domain Admins (CHUU-DOMAIN\Domain Admins)
- Domain Users (CHUU-DOMAIN\Domain Users)
- Enterprise Admins (CHUU-DOMAIN\Enterprise Admins)

Add... Remove

Permissions for Administrator

	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>


For special permissions or advanced settings, click Advanced.

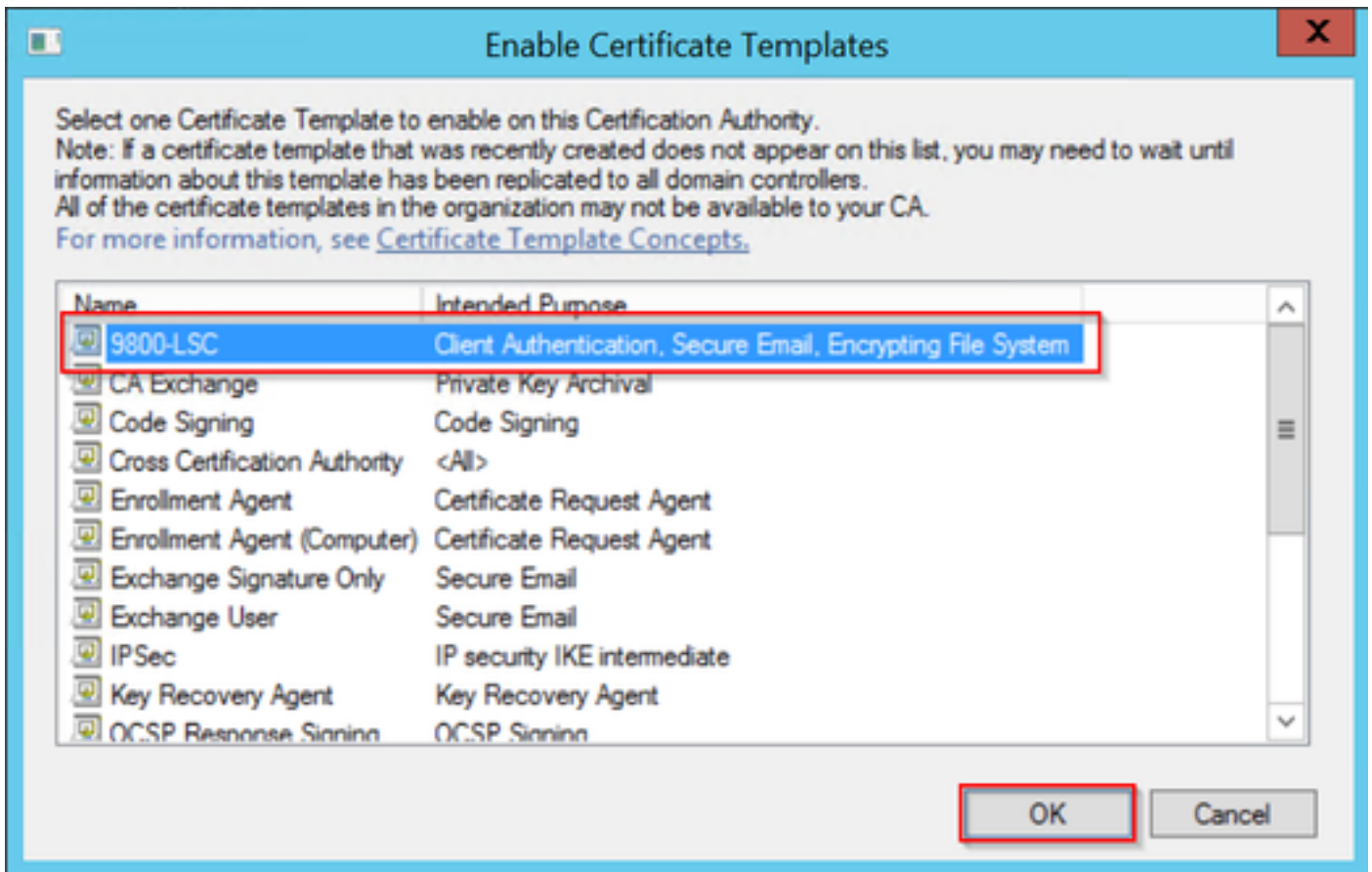
Advanced

OK Cancel **Apply** Help

8단계. Certification Authority 창으로 돌아가 Certificate Templates(인증서 템플릿) 폴더를 마우스 오른쪽 버튼으로 클릭하고 New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)를 선택합니다.

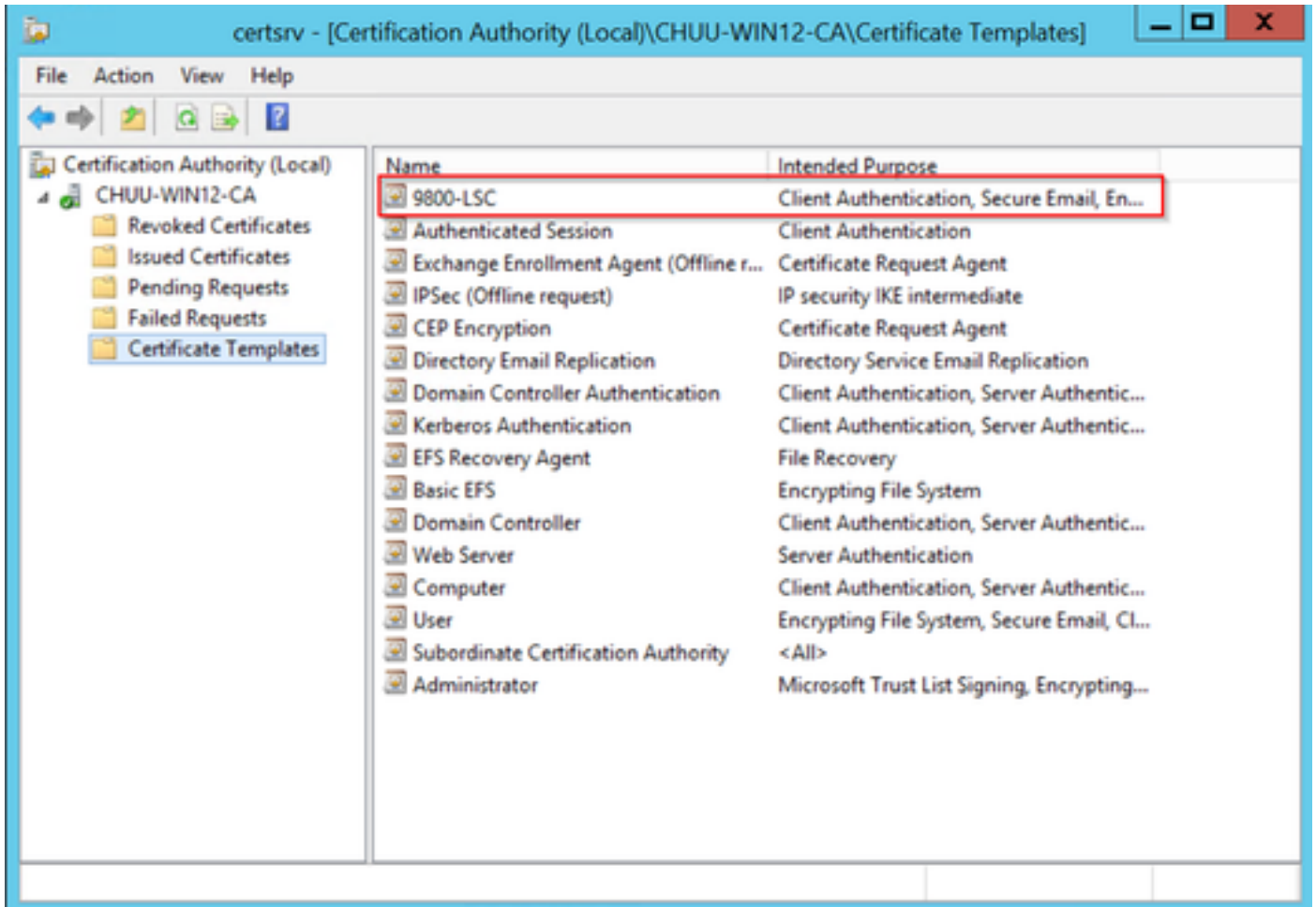
9단계. 이전에 생성한 인증서 템플릿을 선택합니다. 이 예에서는 9800-LSC이고 OK를 선택합니다.

 참고: 새로 생성된 인증서 템플릿은 모든 서버에 걸쳐 복제해야 하므로 여러 서버 구축에 나열되는 데 시간이 더 걸릴 수 있습니다.



템플릿 선택

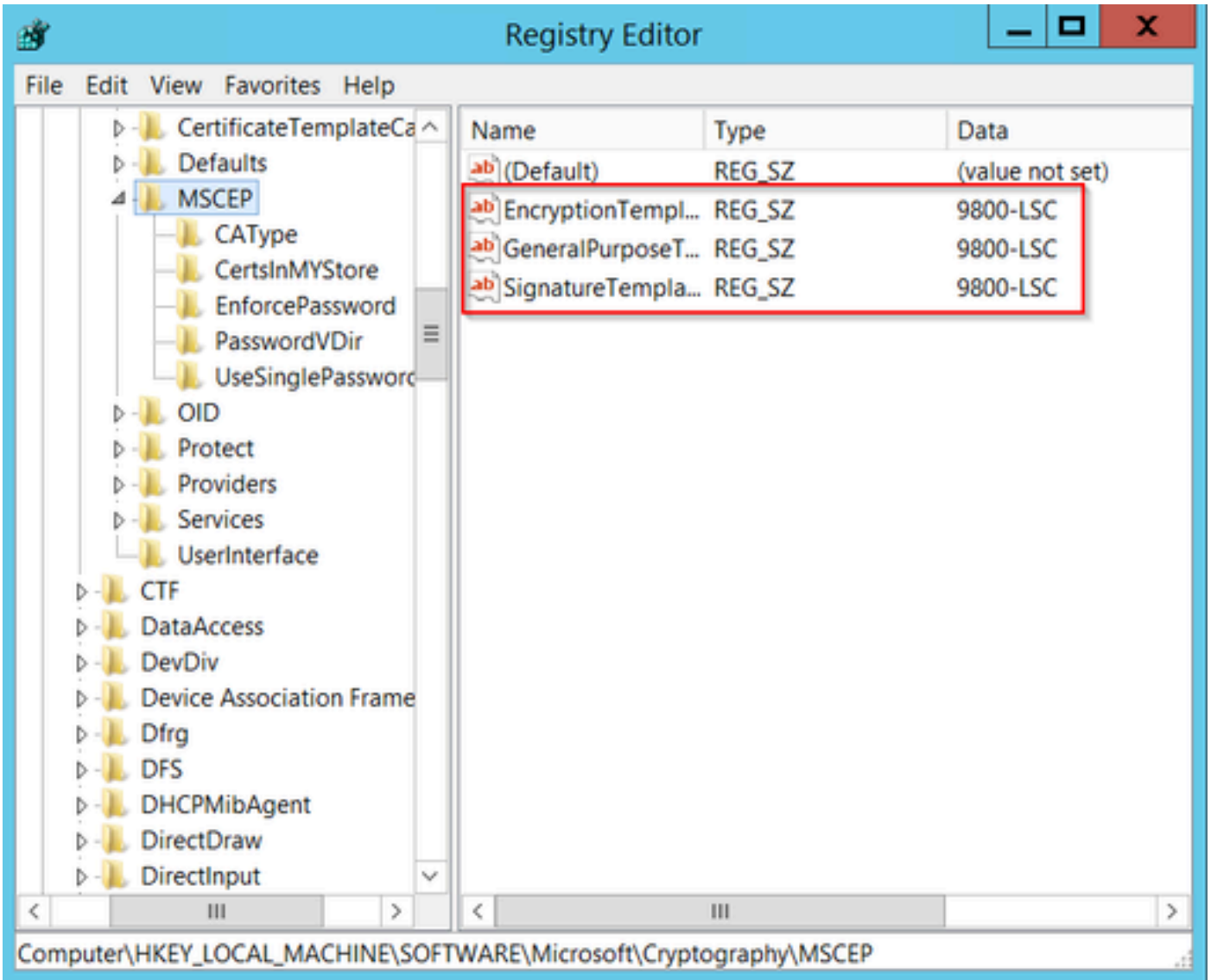
이제 새 인증서 템플릿이 Certificate Templates(인증서 템플릿) 폴더 내용에 나열됩니다.



LSC 선택

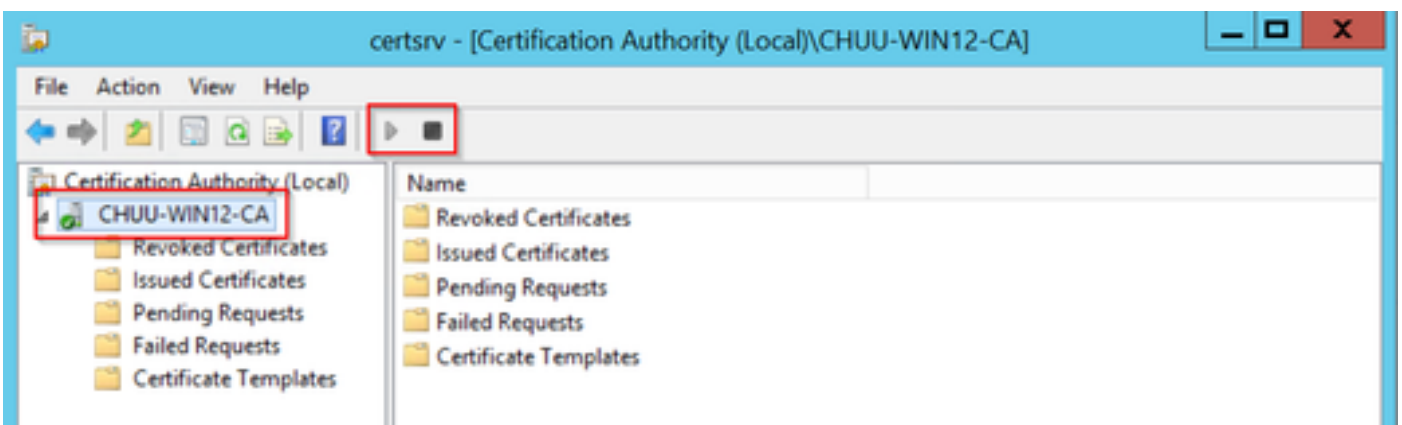
10단계. 레지스트리 편집기 창으로 돌아가 Computer(컴퓨터) > HKEY_LOCAL_MACHINE > SOFTWARE(소프트웨어) > Microsoft > Cryptography(암호화) > MSCEP로 이동합니다.

11단계. EncryptionTemplate, GeneralPurposeTemplate 및 SignatureTemplate 레지스트리가 새로 생성된 인증서 템플릿을 가리키도록 편집합니다.



레지스트리에서 템플릿 변경

12단계. NDES 서버를 재부팅하여 Certification Authority 창으로 돌아가서 서버 이름을 선택하고 Stop and Play 버튼을 차례로 선택합니다.



9800에서 LSC 구성

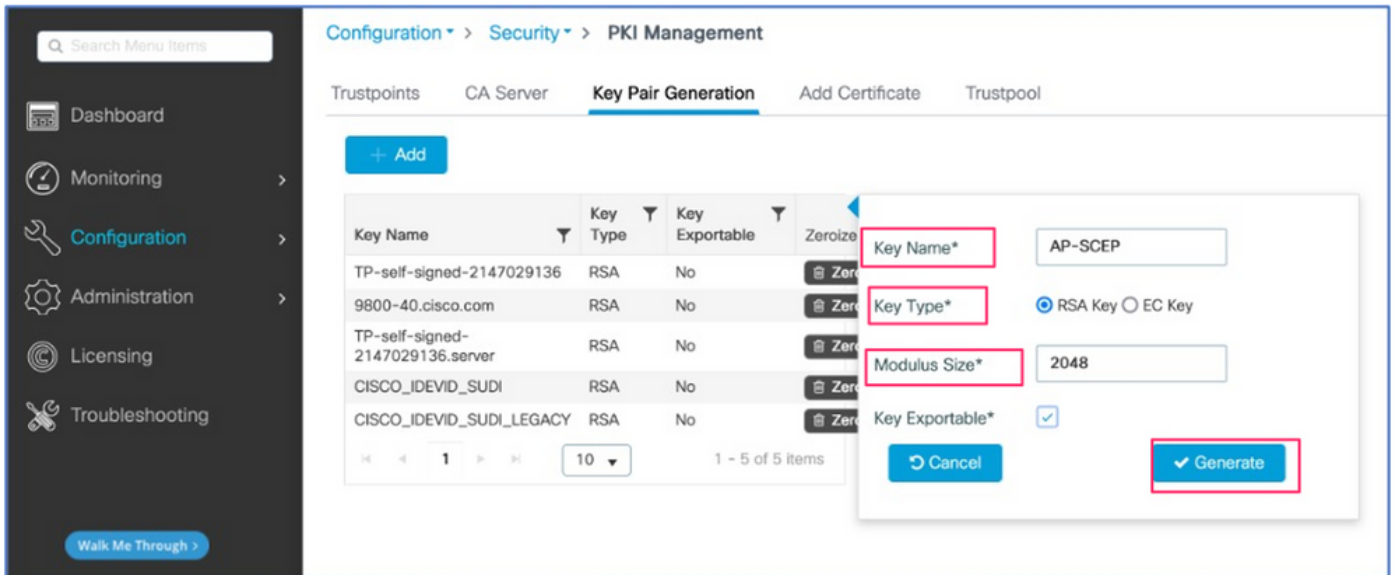
다음은 WLC에서 AP에 대해 LSC를 구성하는 단계입니다.

1. RSA 키를 생성합니다. 이 키는 나중에 PKI 신뢰 지점에 사용됩니다.
2. 신뢰 지점을 생성하고 생성된 RSA 키를 매핑합니다.
3. AP에 대한 LSC 프로비저닝을 활성화하고 신뢰 지점을 매핑합니다.
 1. 조인된 모든 AP에 대해 LSC를 활성화합니다.
 2. 프로비전 목록을 통해 선택한 AP에 대해 LSC를 활성화합니다.
4. 무선 관리 신뢰 지점을 변경하고 LSC 신뢰 지점을 가리킵니다.

AP LSC GUI 컨피그레이션 단계

1단계. Configuration(컨피그레이션) > Security(보안) > PKI Management(PKI 관리) > Key Pair Generation(키 쌍 생성)으로 이동합니다.

1. Add(추가)를 클릭하고 관련 이름을 지정합니다.
2. RSA 키 크기를 추가합니다.
3. 내보낼 수 있는 키 옵션은 선택 사항입니다. 이 명령은 키를 상자에서 내보내려는 경우에만 필요합니다.
4. Generate(생성)를 선택합니다



2단계. Configuration(컨피그레이션) > Security(보안) > PKI Management(PKI 관리) > Trustpoints(신뢰 지점)로 이동합니다

1. Add(추가)를 클릭하고 관련 이름을 지정합니다.
2. 등록 URL(URL은 <http://10.106.35.61:80/certsrv/mscep/mscep.dll>)과 나머지 세부사항을 입력합니다.
3. 1단계에서 생성한 RSA 키 쌍을 선택합니다.
4. Authenticate를 클릭합니다.
5. Enroll trustpoint(신뢰 지점 등록)를 클릭하고 비밀번호를 입력합니다.
6. Apply to Device(디바이스에 적용)를 클릭합니다.

Configuration > Security > PKI Management

Add Trustpoint

Label* Enrollment Type SCEP Terminal

Subject Name

Country Code State

Location Domain Name

Organization Email Address

Enrollment URL Authenticate

Key Generated Available RSA Keypairs

Enroll Trustpoint

Password*

Re-Enter Password*

3단계.Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동합니다. 아래로 스크롤하여 LSC Provision(LSC 프로비저닝)을 선택합니다.

1. 상태를 enabled(활성화됨)로 선택합니다. 이렇게 하면 이 WLC에 연결된 모든 AP에 대해 LSC가 활성화됩니다.
2. 2단계에서 생성한 신뢰 지점 이름을 선택합니다.

당신의 필요에 따라 나머지 세부사항을 작성하세요.

Configuration > Wireless > Access Points

All Access Points

Misconfigured APs
Tag: 0 Country Code: 0 LSC Fallback: 0 Select an Action

Total APs: 1

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Config Status
AP000-F89A-46E0	C9117AXI-D	2	●	0 days 0 hrs 26 mins 42 secs	10.105.101.158	80ec.3579.0300	0cd0.f99a.46e0	Local	Yes	Registered	Healthy

1 - 1 of 1 access points

6 GHz Radios

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Status

Trustpoint Name

Number of Join Attempts

Key Size

Certificate chain status Not Available

Number of certificates in chain 0

Subject Name Parameters

Country

State

City

Organization

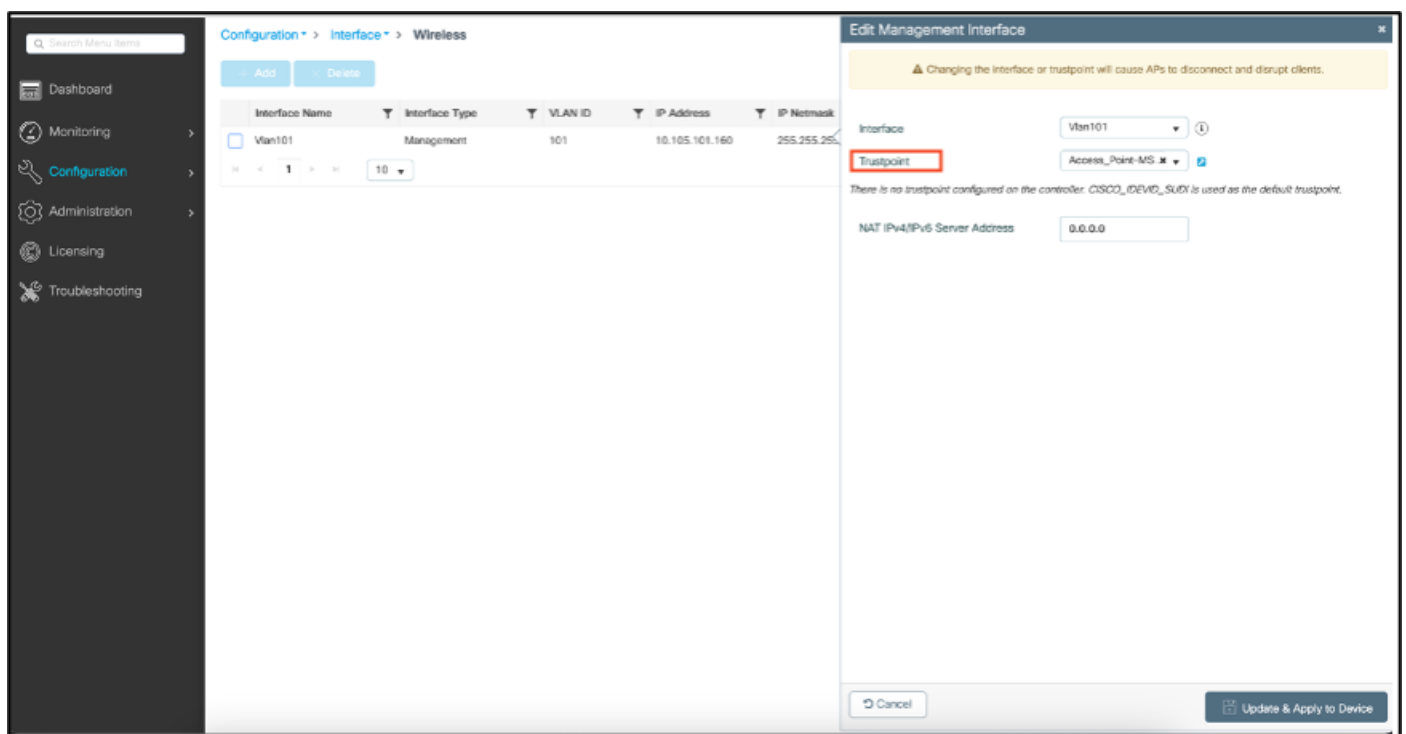
LSC를 활성화하면 AP가 WLC를 통해 인증서를 다운로드하고 재부팅합니다. AP 콘솔 세션에서 이 코드 조각과 같은 내용이 표시됩니다.

```
[*09/25/2023 10:03:28.0993] .....
[*09/25/2023 10:03:28.7016] .....+++++
[*09/25/2023 10:03:28.7663] writing new private key to '/tmp/lsc/priv_key'
[*09/25/2023 10:03:28.7666] -----
[*09/25/2023 10:03:28.9212] LSC_ENABLE: saving ROOT_CERT
[*09/25/2023 10:03:28.9212]
[*09/25/2023 10:03:28.9293] LSC_ENABLE: saving DEVICE_CERT
[*09/25/2023 10:03:28.9293]
[*09/25/2023 10:03:28.9635] LSC certs and private key verified
[*09/25/2023 10:03:28.9635]
[*09/25/2023 10:03:29.4997] LSC private key written to hardware TAM
[*09/25/2023 10:03:29.4997]
[*09/25/2023 10:03:29.5526] A[09/25/2023 10:03:29.6099] audit_printk_skb: 12 callbacks suppressed
```

4단계.LSC가 활성화되면 LSC 신뢰 지점과 일치하도록 무선 관리 인증서를 변경할 수 있습니다. 이렇게 하면 AP가 LSC 인증서로 조인하고 WLC는 AP 조인에 해당 LSC 인증서를 사용합니다. AP의 802.1X 인증만 수행하려는 경우 이 단계는 선택 사항입니다.

1. Configuration(컨피그레이션) > Interface(인터페이스) > Wireless(무선)로 이동하고 Management Interface(관리 인터페이스)를 클릭합니다.
2. 2단계에서 생성한 신뢰 지점과 일치하도록 신뢰 지점을 변경합니다.

이것으로 LSC GUI 컨피그레이션 부분을 마치겠습니다. AP가 LSC 인증서를 사용하여 WLC에 조인할 수 있어야 합니다.



AP LSC CLI 컨피그레이션 단계

1. 이 명령을 사용하여 RSA 키를 만듭니다.

```
9800-40(config)#crypto key generate rsa general-keys modulus 2048 label AP-SCEP
```

```
% You already have RSA keys defined named AP-SCEP.
% They will be replaced
```

```
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Sep 27 05:08:13.144: %CRYPTO_ENGINE-5-KEY_DELETED: A key named AP-SCEP has been removed from key storage
Sep 27 05:08:13.753: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named AP-SCEP has been generated or imported
```

2. PKI 신뢰 지점을 생성하고 RSA 키 쌍을 매핑합니다. 등록 URL과 나머지 세부사항을 입력합니다

```
9800-40(config)#crypto pki trustpoint Access_Point-MS-CA
9800-40(ca-trustpoint)#enrollment url http://10.106.35.61:80/certsrv/mscep/mscep.dll
9800-40(ca-trustpoint)#subject-name C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local,E=mail@tac-lab.
9800-40(ca-trustpoint)#rsaakeypair AP-SCEP
9800-40(ca-trustpoint)#revocation none
9800-40(ca-trustpoint)#exit
```

3. crypto pki authenticate <trustpoint> 명령을 사용하여 CA 서버에 PKI 신뢰 지점을 인증하고 등록합니다. 비밀번호 프롬프트에 비밀번호를 입력합니다.

```
9800-40(config)#crypto pki authenticate Access_Point-MS-CA
Certificate has the following attributes:
Fingerprint MD5: C44D21AA 9B489622 4BF548E1 707F9B3B
Fingerprint SHA1: D2DE6E8C BA665DEB B202ED70 899FDB05 94996ED2
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-40(config)#crypto pki enroll Access_Point-MS-CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:
Sep 26 01:25:00.880: %PKI-6-CERT_ENROLL_MANUAL: Manual enrollment for trustpoint Access_Point-MS-CA
Re-enter password:
% The subject name in the certificate will include: C=IN,L=Bengaluru,ST=KA,O=TAC,CN=TAC-LAB.cisco.local
% The subject name in the certificate will include: 9800-40.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: TTM244909MX
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose Access_Point-MS-CA' command will show the fingerprint.
Sep 26 01:25:15.062: %PKI-6-CSR_FINGERPRINT:
CSR Fingerprint MD5 : B3D551528B97DA5415052474E7880667
CSR Fingerprint SHA1: D426CE9B095E1B856848895DC14F997BA79F9005
CSR Fingerprint SHA2: B8CEE743549E3DD7C8FA816E97F2746AB48EE6311F38F0B8F4D01017D8081525
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint MD5 :B3D55152 8B97DA54 15052474 E78806
Sep 26 01:25:15.062: CRYPTO_PKI: Certificate Request Fingerprint SHA1 :D426CE9B 095E1B85 6848895D C14F9
Sep 26 01:25:15.063: CRYPTO_PKI: Certificate Request Fingerprint SHA2 :B8CEE743 549E3DD7 C8FA816E 97F27
Sep 26 01:25:30.239: %PKI-6-CERT_INSTALL: An ID certificate has been installed under
Trustpoint : Access_Point-MS-CA
```

```
Issuer-name : cn=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com
Subject-name : e=mail@tac-lab.local,cn=TAC-LAB.cisco.local,o=TAC,l=Bengaluru,st=KA,c=IN,hostname=9800-4
Serial-number: 5C0000001400DD405D77E6FE7F000000000014
End-date : 2024-09-25T06:45:15Z
9800-40(config)#
```

4. LSC 인증서로 AP 조인을 구성합니다.

```
9800-40(config)#ap lsc-provision join-attempt 10
9800-40(config)#ap lsc-provision subject-name-parameter country IN state KA city Bengaluru domain TAC-L
9800-40(config)#ap lsc-provision key-size 2048
9800-40(config)#ap lsc-provision trustpoint Access_Point-MS-CA
9800-40(config)#ap lsc-provision
In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration
Are you sure you want to continue? (y/n): y
```

5. 위에서 생성한 신뢰 지점과 일치하도록 무선 관리 신뢰 지점을 변경합니다.

```
9800-40(config)#wireless management trustpoint Access_Point-MS-CA
```

AP LSC 확인

LSC를 확인하려면 WLC에서 이 명령을 실행합니다.

```
#show wireless management trustpoint
#show ap lsc-provision summary
#show ap name < AP NAME > config general | be Certificate
```

```

9800-40#sho ap lsc-provision summ
AP LSC-provisioning : Enabled for all APs
Trustpoint used for LSC-provisioning : Access_Point-MS-CA
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash      : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : Bengaluru
Orgn : TAC
Dept : TAC-LAB.cisco.local
Email : mail@tac-lab.local
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 0

Mac Addresses :
-----

9800-40#sho wire
9800-40#sho wireless man
9800-40#sho wireless management tru
9800-40#sho wireless management trustpoint
Trustpoint Name : Access_Point-MS-CA
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : b7f12604ffe66b4d4abe01e32c92a417b5c6ca0c
Private key Info : Available
FIPS suitability : Not Applicable

9800-40#

```

```

9800-40#sho ap name AP0CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-OTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 002.lx LSC Status
Certificate status : Not Available
AP LSC authentication state : CAPWAP-OTLS

```

AP가 다시 로드되면 AP CLI에 로그인하고 다음 명령을 실행하여 LSC 컨피그레이션을 확인합니다.

```

#show crypto | be LSC
#show capwap cli config | in lsc
#show dtls connection

```

```

AP0CD0.F89A.46E0#sho crypto | be LSC
LSC: Enabled
----- Device Certificate -----
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    5c:00:00:00:18:18:14:ed:da:85:f9:bf:d1:00:00:00:00:00:00
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: DC = com, DC = tac-lab, DC = sumans, CN = sumans-lab-ca
  Validity
    Not Before: Sep 28 04:15:28 2023 GMT
    Not After : Sep 27 04:15:28 2024 GMT
  Subject: C = IN, ST = KA, L = Bengaluru, O = TAC, CN = ap1g6-0CD0F89A46E0 emailAddress = mail@tac-lab.local
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public-Key: (2048 bit)
    Modulus:

```

```

AP0CD0.F89A.46E0#sho crypto | in LSC
LSC: Enabled
AP0CD0.F89A.46E0#sho capwap cli config | in lsc
AP lsc enable : 1
AP lsc reboot cnt : 0
AP lsc max num of retry : 10
AP lsc mode : 0x1
AP lsc dtls fallback state : 0
AP0CD0.F89A.46E0#
Read timed out

```

```

AP0CD0.F89A.46E0#sho dtls connections

```

```

Number of DTLS connection = 1

```

```

[ClientIP]:ClientPort <=> [ServerIP]:ServerPort Ciphersuit Version
-----

```

```

[10.105.101.168]:5256 <=> [10.105.101.160]:5246 0xc02f 1.2

```

```

Current connection certificate issuer name: sumans-lab-ca

```

LSC 프로비저닝 문제 해결

WLC 또는 AP 업링크 스위치 포트에서 EPC 캡처를 가져와 AP가 CAPWAP 터널을 형성하는 데 사용하는 인증서를 확인할 수 있습니다. PCAP에서 DTLS 터널이 성공적으로 구축되었는지 확인합니다.

```

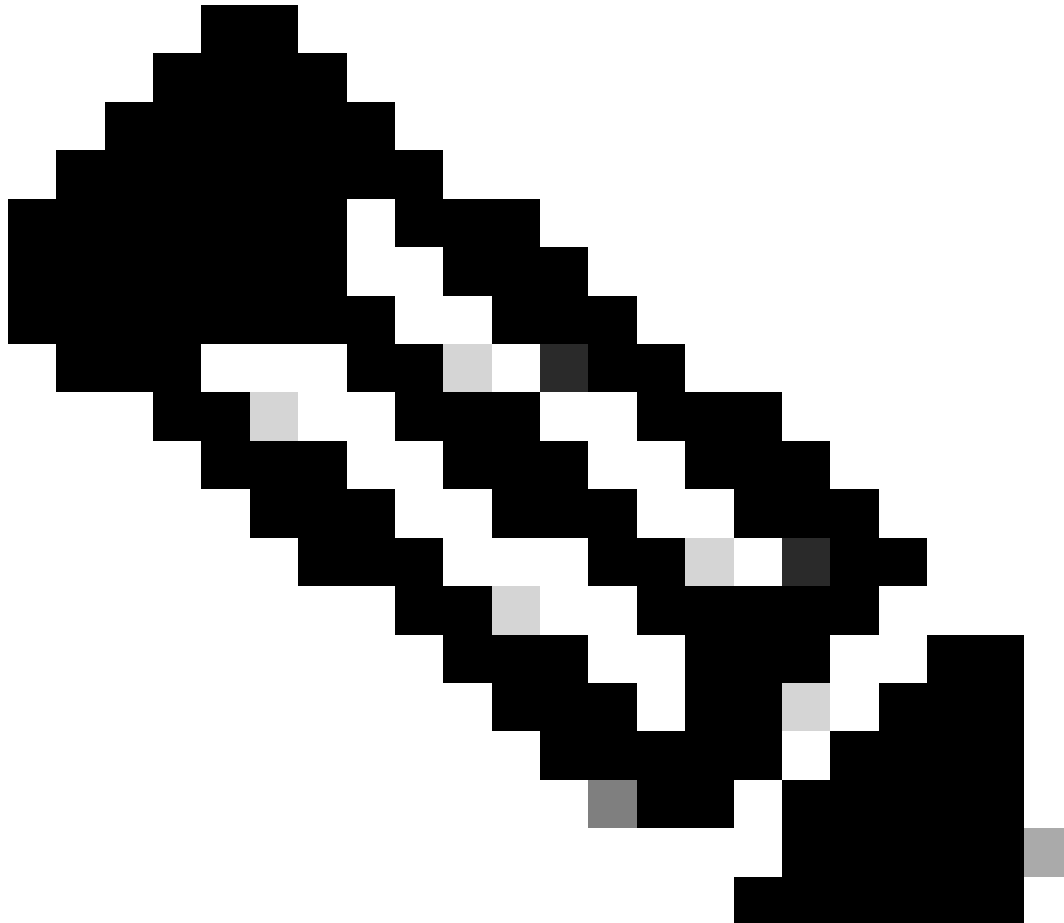
v Datagram Transport Layer Security
  v DTLSv1.2 Record Layer: Handshake Protocol: Certificate (Reassembled)
    Content Type: Handshake (22)
    Version: DTLS 1.2 (0xfefd)
    Epoch: 0
    Sequence Number: 5
    Length: 82
  v Handshake Protocol: Certificate (Reassembled)
    Handshake Type: Certificate (11)
    Length: 1627
    Message Sequence: 2
    Fragment Offset: 1557
    Fragment Length: 70
    Certificates Length: 1624
  v Certificates (1624 bytes)
    Certificate Length: 1621
  v Certificate: 3082065130820539a00302010202135c000000181814edda85f9bfd100000000018300d. (pkcs-9-at-emailAddress@mail@tac-lab.local,id-at-commonName=
  v signedCertificate
    version: v3 (2)
    serialNumber: 0x5c000000181814edda85f9bfd1000000000018
  v signature (sha256WithRSAEncryption)
    Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
  v issuer: rdnSequence (0)
  v rdnSequence: 4 items (id-at-commonName=sumans-lab-ca,dc=sumans,dc=tac-lab,dc=com)
  v RDNSquence item: 1 item (dc=com)
  v RelativeDistinguishedName item (dc=com)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: com
  v RDNSquence item: 1 item (dc=tac-lab)
  v RelativeDistinguishedName item (dc=tac-lab)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: tac-lab
  v RDNSquence item: 1 item (dc=sumans)
  v RelativeDistinguishedName item (dc=sumans)
    Object Id: 0.9.2342.19200300.100.1.25 (dc)
    IA5String: sumans
  v RDNSquence item: 1 item (id-at-commonName=sumans-lab-ca)
  v RelativeDistinguishedName item (id-at-commonName=sumans-lab-ca)
    Object Id: 2.5.4.3 (id-at-commonName)
    DirectoryString: printableString (1)
    printableString: sumans-lab-ca
  v validity
  v notBefore: utcTime (0)
    utcTime: 2023-09-28 04:15:28 (UTC)
  v notAfter: utcTime (0)
    utcTime: 2024-09-27 04:15:28 (UTC)
  v subject: rdnSequence (0)

```

DTLS 디버그는 인증서 문제를 파악하기 위해 AP 및 WLC에서 실행할 수 있습니다.

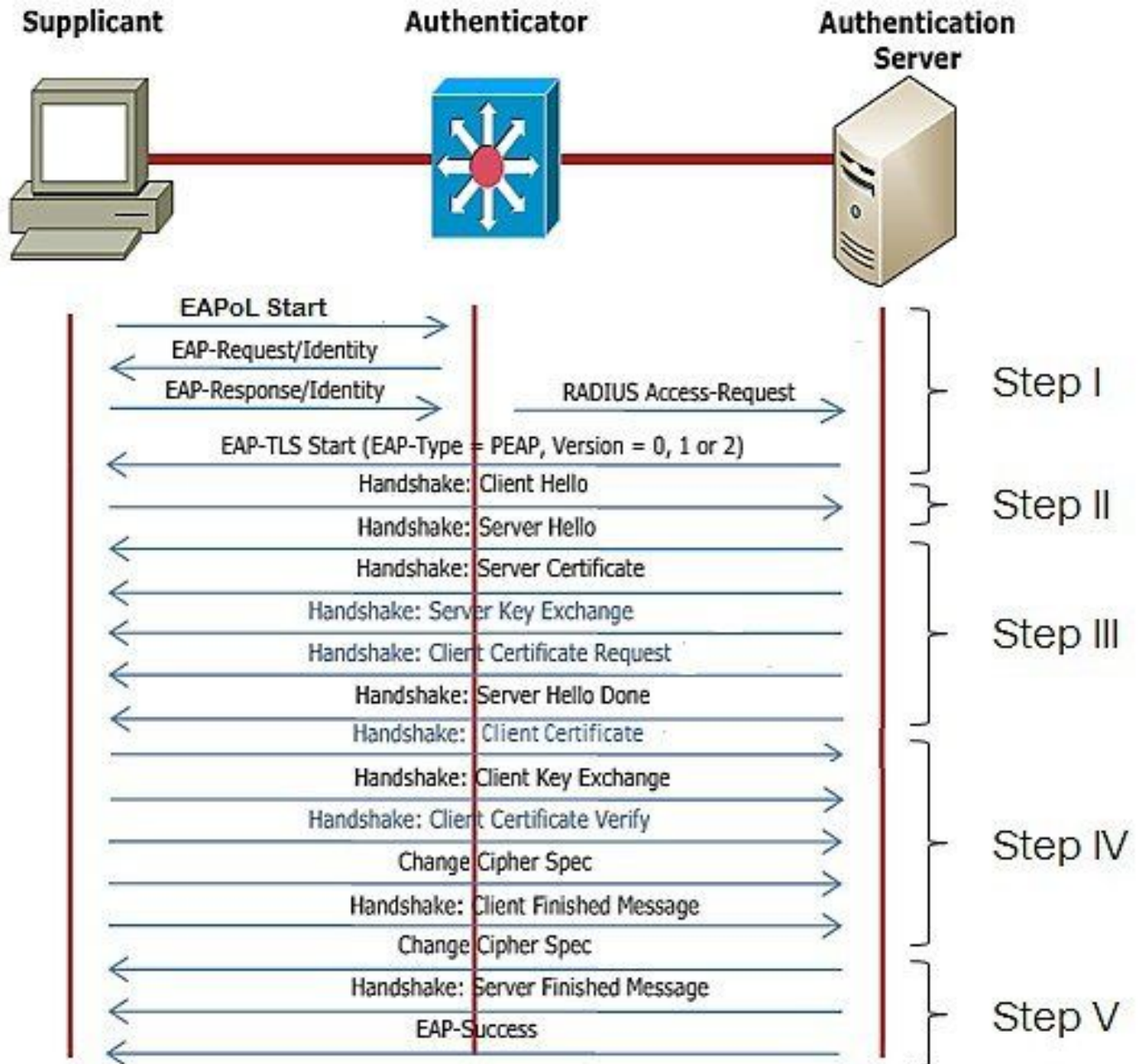
LSC를 사용하는 AP 유선 802.1X 인증

AP는 자신을 인증하는 데 동일한 LSC 인증서를 사용하도록 구성됩니다. AP는 802.1X 신청자 역할을 하며 ISE 서버에 대해 스위치에서 인증됩니다. ISE 서버가 백엔드에서 AD와 통신합니다.



참고: AP 업링크 스위치 포트에서 dot1x 인증이 활성화되면 AP는 인증이 통과될 때까지 트래픽을 전달하거나 수신할 수 없습니다. 인증에 실패한 AP를 복구하고 AP에 액세스하려면 AP 유선 스위치 포트에서 dot1x 인증을 비활성화합니다.

EAP-TLS 인증 워크플로 및 메시지 교환

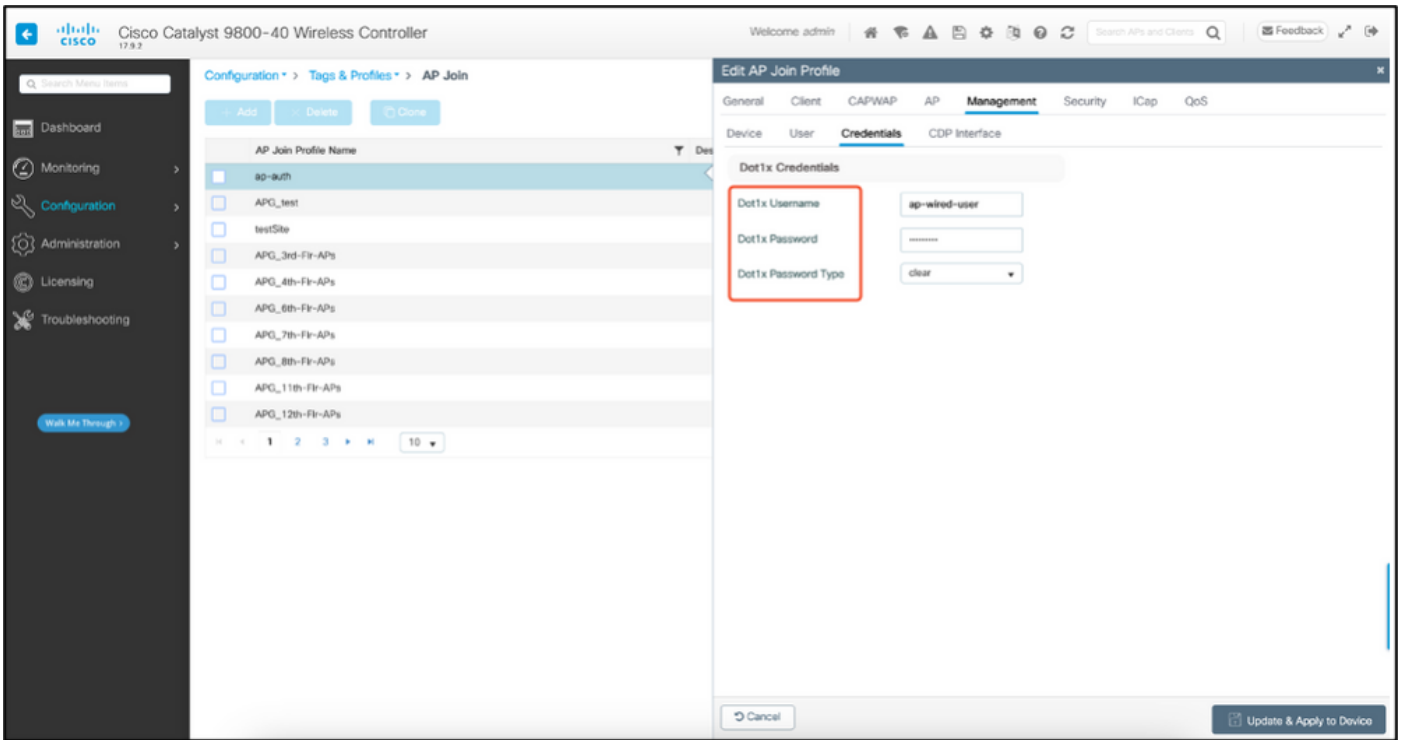
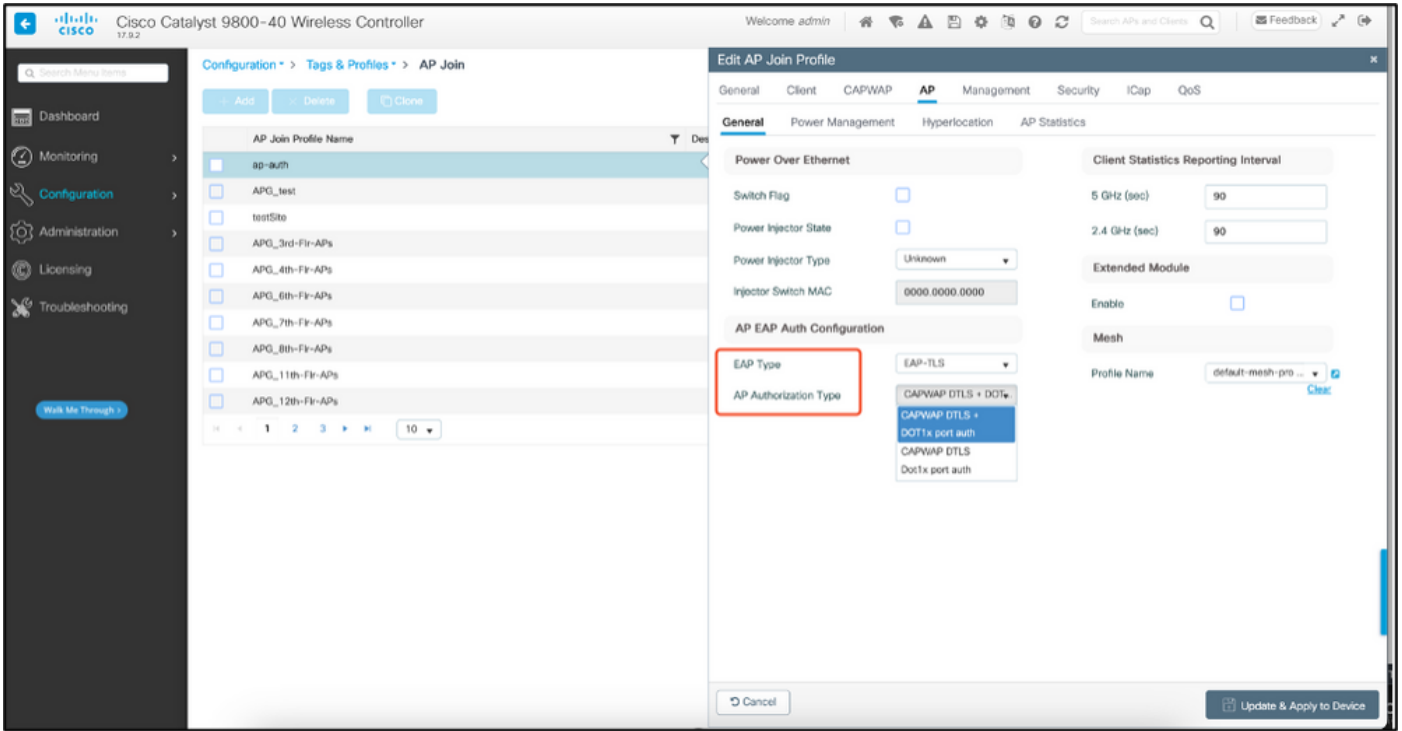


AP 유선 802.1x 인증 컨피그레이션 단계

1. CAPWAP DTLS와 함께 dot1x 포트 인증을 활성화하고 EAP 유형을 선택합니다.
2. AP에 대한 dot1x 자격 증명을 생성합니다.
3. 스위치 포트에서 dot1x를 활성화합니다.
4. RADIUS 서버에 신뢰할 수 있는 인증서를 설치합니다.

AP 유선 802.1x 인증 GUI 컨피그레이션

1. AP 가입 프로필로 이동하고 프로필을 클릭합니다.
 1. AP > General을 클릭합니다. EAP 유형 및 AP 권한 부여 유형을 "CAPWAP DTLS + dot1x port auth"로 선택합니다.
 2. Management(관리) > Credentials(자격 증명)로 이동하고 AP dot1x 인증을 위한 사용자 이름 및 비밀번호를 생성합니다.



AP 유선 802.1x 인증 CLI 컨피그레이션

CLI에서 AP에 대해 dot1x를 활성화하려면 다음 명령을 사용합니다. 이는 특정 가입 프로필을 사용하는 AP에 대해서만 유선 인증을 활성화합니다.

```
#ap profile ap-auth
#dot1x eap-type eap-tls
#dot1x lsc-ap-auth-state both
#dot1x username ap-wired-user password 0 cisco!123
```

```
9808-40(config)#ap profile ap-auth
9808-40(config-ap-profile)#dot1x cap-type cap-tls
9808-40(config-ap-profile)#dot1x lsc-ap-auth-state both
9808-40(config-ap-profile)#
```

AP 유선 802.1x 인증 스위치 컨피그레이션

이 스위치 컨피그레이션은 LAB에서 AP 유선 인증을 활성화하는 데 사용됩니다. 설계에 따라 다른 컨피그레이션을 가질 수 있습니다.

```
aaa new-model
dot1x system-auth-control
aaa authentication dot1x default group radius
aaa authorization network default group radius
radius server ISE
address ipv4 10.106.34.170 auth-port 1812 acct-port 1813
key cisco!123
!
interface GigabitEthernet1/0/2
description "AP-UPLINK-PORT-AUTH-ENABLED"
switchport access vlan 101
switchport mode access
authentication host-mode multi-host
authentication order dot1x
authentication priority dot1x
authentication port-control auto
dot1x pae authenticator
end
```

RADIUS 서버 인증서 설치

인증은 신청자 역할을 하는 AP와 RADIUS 서버 간에 발생합니다. 둘 다 서로 인증서를 신뢰해야 합니다. AP가 RADIUS 서버 인증서를 신뢰하도록 하는 유일한 방법은 RADIUS 서버가 AP 인증서도 발급한 SCEP CA에서 발급한 인증서를 사용하도록 하는 것입니다.

ISE에서 Administration(관리) > Certificates(인증서) > Generate Certificate Signing Requests(인증서 서명 요청 생성)로 이동합니다

CSR을 생성하고 필드를 ISE 노드의 정보로 채웁니다.

Certificate Management

- System Certificates
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Se...

Certificate Authority

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate
- ISE Messaging Service - Generate a Signing Certificate or generate a brand new Messaging Certificate.
- Data Connect Certificate - Connect to Oracle Database

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for EAP Authentication

Allow Wildcard Certificates O

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ISE99	ISE99#EAP Authentication

Subject

Common Name (CN) \$FQDN\$ O

Organizational Unit (OU) O

Organization (O) O

City (L)

State (ST)

생성된 후에는 내보내고 텍스트로 복사하여 붙여넣을 수도 있습니다.

Windows CA IP 주소로 이동하여 URL에 /certsrv/를 추가합니다

Request a certificate(인증서 요청)를 클릭합니다

← → ↻ Non sécurisé | 192.168.1.98/certsrv/

Microsoft Active Directory Certificate Services - mydomain-WIN-3E202T1QD0U-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Submit a certificate request by using a base-64(base-64를 사용하여 인증서 요청 제출)를 클릭합니다.

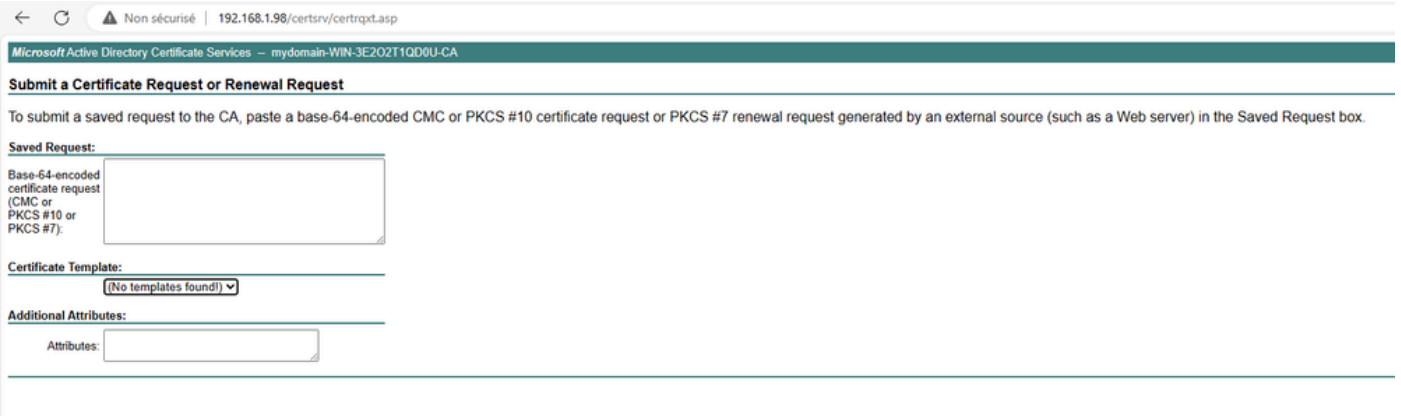
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

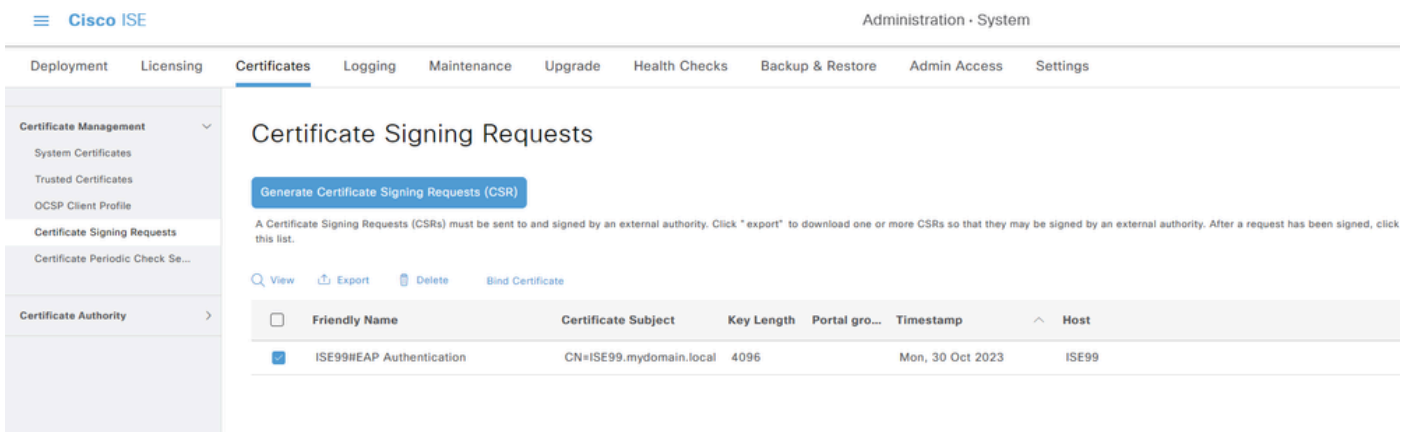
[Create and submit a request to this CA.](#)

[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

텍스트 상자에 CSR 텍스트를 붙여넣습니다. 웹 서버 인증서 템플릿을 선택합니다.



그런 다음 Certificate Signing Request(인증서 서명 요청) 메뉴로 돌아가 Bind certificate(인증서 바인딩)를 클릭하여 ISE에 이 인증서를 설치할 수 있습니다. 그런 다음 Windows C에서 가져온 인증서를 업로드할 수 있습니다.



Friendly Name	Certificate Subject	Key Length	Portal gro...	Timestamp	Host
ISE99#EAP Authentication	CN=ISE99.mydomain.local	4096		Mon, 30 Oct 2023	ISE99

AP 유선 802.1x 인증 확인

AP에 대한 콘솔 액세스 권한을 가지고 다음 명령을 실행합니다.

```
#show ap authentication status
```

Ap 인증이 활성화되지 않았습니다.

```
AP0CD0.F89A.46E0#sho ap authentication status
AP dot1x feature is disabled.
AP0CD0.F89A.46E0#
```

AP 인증을 활성화한 후 AP에서 콘솔 로그:

```
AP0CD0.F89A.46E0#[*09/26/2023 08:57:40.9154]
[*09/26/2023 08:57:40.9154] Restart for both CAPWAP DTLS & 802.1X LSC mode
[*09/26/2023 08:57:40.9719] AP Rebooting: Reset Reason - LSC mode ALL
```

AP 인증 성공:

```
AP0CD0.F89A.46E0#sho ap authentication status
ap mgmt IEEE 802.1X (no MPA)
ap state=COMPLETED
address=0c:d0:f8:9a:46:e0
supplicant pae state=AUTHENTICATED
supplicant status=Authorized
EAP state=SUCCESS
selectedMethod=13 (EAP-TLS)
EAP_TLS_version=TLSv1.2
EAP_TLS_cipher=ECDHE-RSA-AES256-GCM-SHA384
tls_session_reused=0
cap_session_id=0d7b91a744885a6e8e460d49fee7d2d5604ca2bdd11f40494a4325dc98d1919af48b9fb33ec526f18eda11effcb2ea0238cf95244aaf5f17decf336ad11e88121
AP0CD0.F89A.46E0#
```

WLC 확인:

```
9800-40#sho ap name AP0CD0.F89A.46E0 config general | begin Certificate
AP Certificate type : Locally Significant Certificate
AP Certificate Expiry-time : 09/25/2024 06:48:23
AP Certificate issuer common-name : sumans-lab-ca
AP Certificate Policy : Default
AP CAPWAP-DTLS LSC Status
Certificate status : Available
LSC fallback status : No
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP 802.1x LSC Status
Certificate status : Available
Issuer certificate hash : 611255bc69f565af537be59297f453593e432e1b
Certificate expiry time : 09/25/2024 06:48:23
AP LSC authentication state : CAPWAP-DTLS and 802.1x authentication
```

Switchport 인터페이스 상태가 인증 성공 후:

```
Switch#sho authentication sessions interface gigabitEthernet 1/0/2
Interface MAC Address Method Domain Status Fg Session ID
Gi1/0/2 0cd0.f89a.46e0 dot1x DATA Auth 9765690A0000005CCEED0FBF
```

다음은 성공적인 인증을 나타내는 AP 콘솔 로그 샘플입니다.

```
[*09/26/2023 07:33:57.5512] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5513] hostapd:EAP: Status notification: started (param=)
[*09/26/2023 07:33:57.5513] hostapd:EAP: EAP-Request Identity
[*09/26/2023 07:33:57.5633] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5634] hostapd:EAP: Status notification: accept proposed method (param=TLS)
[*09/26/2023 07:33:57.5673] hostapd:dot1x: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 13 (TLS) selected
[*09/26/2023 07:33:57.5907] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.5977] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6045] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6126] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6137] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/DC=com/DC=tac-lab
[*09/26/2023 07:33:57.6145] hostapd:dot1x: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=IN/ST=KA/L=BLR/
[*09/26/2023 07:33:57.6151] hostapd:EAP: Status notification: remote certificate verification (param=su
[*09/26/2023 07:33:57.6539] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6601] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.6773] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:dot1x: RX EAPOL from 40:f0:78:00:a1:02
[*09/26/2023 07:33:57.7812] hostapd:EAP: Status notification: completion (param=success)
[*09/26/2023 07:33:57.7812] hostapd:dot1x: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successf
[*09/26/2023 07:33:57.7813] hostapd:dot1x: State: ASSOCIATED -> COMPLETED
[*09/26/2023 07:33:57.7813] hostapd:dot1x: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 compl
```

802.1X 인증 문제 해결

AP 업링크에 PCAP를 적용하고 RADIUS 인증을 확인합니다. 다음은 성공적인 인증의 단편입니다.

479.	07:47:17.192983	Cisco_9a:46:e0	Nearest-non-TP...	EAP	1812	55431	Response, Identity(Packet size limited during capture)
479.	07:47:17.205205	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=251
479.	07:47:17.205983	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2			Encrypted Handshake Message
479.	07:47:17.206904	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=244
479.	07:47:17.256975	Cisco_9a:46:e0	Nearest-non-TP...	EAP	1812	55431	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.267976	Cisco_9a:46:e0	Nearest-non-TP...	EAP	1812	55431	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.274979	Cisco_9a:46:e0	Nearest-non-TP...	EAP	1812	55431	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.277002	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=247
479.	07:47:17.311988	Cisco_9a:46:e0	Nearest-non-TP...	EAP	1812	55431	Response, TLS EAP (EAP-TLS)
479.	07:47:17.314974	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=248
479.	07:47:17.318968	Cisco_9a:46:e0	Nearest-non-TP...	EAP	1812	55431	Response, TLS EAP (EAP-TLS)
479.	07:47:17.324988	Cisco_9a:46:e0	Nearest-non-TP...	TLV1.2			Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
479.	07:47:17.342969	Cisco_9a:46:e0	Nearest-non-TP...	EAP	1812	55431	Response, TLS EAP (EAP-TLS)(Packet size limited during capture)
479.	07:47:17.378979	10.100.34.178	10.100.101.151	RADIUS	1812	55431	Access-Accept id=251

TCPdump는 인증을 캡처하는 ISE에서 수집합니다.

80	07:47:18.171107	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=244
87	07:47:18.177802	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=244
88	07:47:18.182300	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=244
89	07:47:18.187000	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=244
90	07:47:18.191500	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=244
91	07:47:18.196000	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=244
92	07:47:18.199500	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=244
93	07:47:18.204000	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=247
94	07:47:18.208500	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=247
95	07:47:18.213000	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=248
96	07:47:18.217500	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=248
97	07:47:18.222000	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=250
98	07:47:18.226500	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Challenge id=250
99	07:47:18.231000	10.100.34.178	10.100.101.151	Radius	1812	55431	Access-Request id=251
82	07:47:18.945978	10.100.34.178	10.100.101.151	RADIUS	1812	55431	Access-Accept id=251

인증 중에 문제가 발견되면 AP 유선 업링크 및 ISE 측에서 동시 패킷 캡처가 필요합니다.

AP에 대한 디버그 명령:

```
#debug ap authentication packet
```

관련 정보

- [Cisco 기술 지원 및 다운로드](#)
- [AireOS를 사용하여 AP에 802.1X 구성](#)
- [LSC용 9800 컨피그레이션 가이드](#)
- [9800의 LSC 컨피그레이션 예](#)
- [9800의 AP에 대해 802.1X 구성](#)

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.