

WLC 및 Windows Server 2012 컨피그레이션을 사용하는 LSC(Locally Significant Certificates) 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[Microsoft Windows Server 구성](#)

[WLC 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 WLC(Wireless LAN Controller) 및 새로 설치된 Microsoft Windows Server 2012 R2를 사용하여 LSC(Locally Significant Certificates)를 구성하는 방법에 대해 설명합니다.

참고: 실제 배포는 여러 점에서 다를 수 있으며 Microsoft Windows Server 2012의 설정을 완벽하게 제어하고 알아야 합니다. 이 컨피그레이션 예는 Cisco 고객이 LSC가 작동하도록 Microsoft Windows Server 컨피그레이션을 구현하고 조정하는 데 사용할 수 있는 참조 템플릿으로만 제공됩니다.

사전 요구 사항

요구 사항

Microsoft Windows Server의 모든 변경 사항을 이해하고 필요한 경우 관련 Microsoft 설명서를 확인하는 것이 좋습니다.

참고: WLC의 LSC는 중간-CA에서 지원되지 않습니다. 컨트롤러가 중간 CA만 가져오기 때문에 루트 CA가 WLC에서 누락되기 때문입니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- WLC 버전 7.6
- Microsoft Windows Server 2012 R2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든

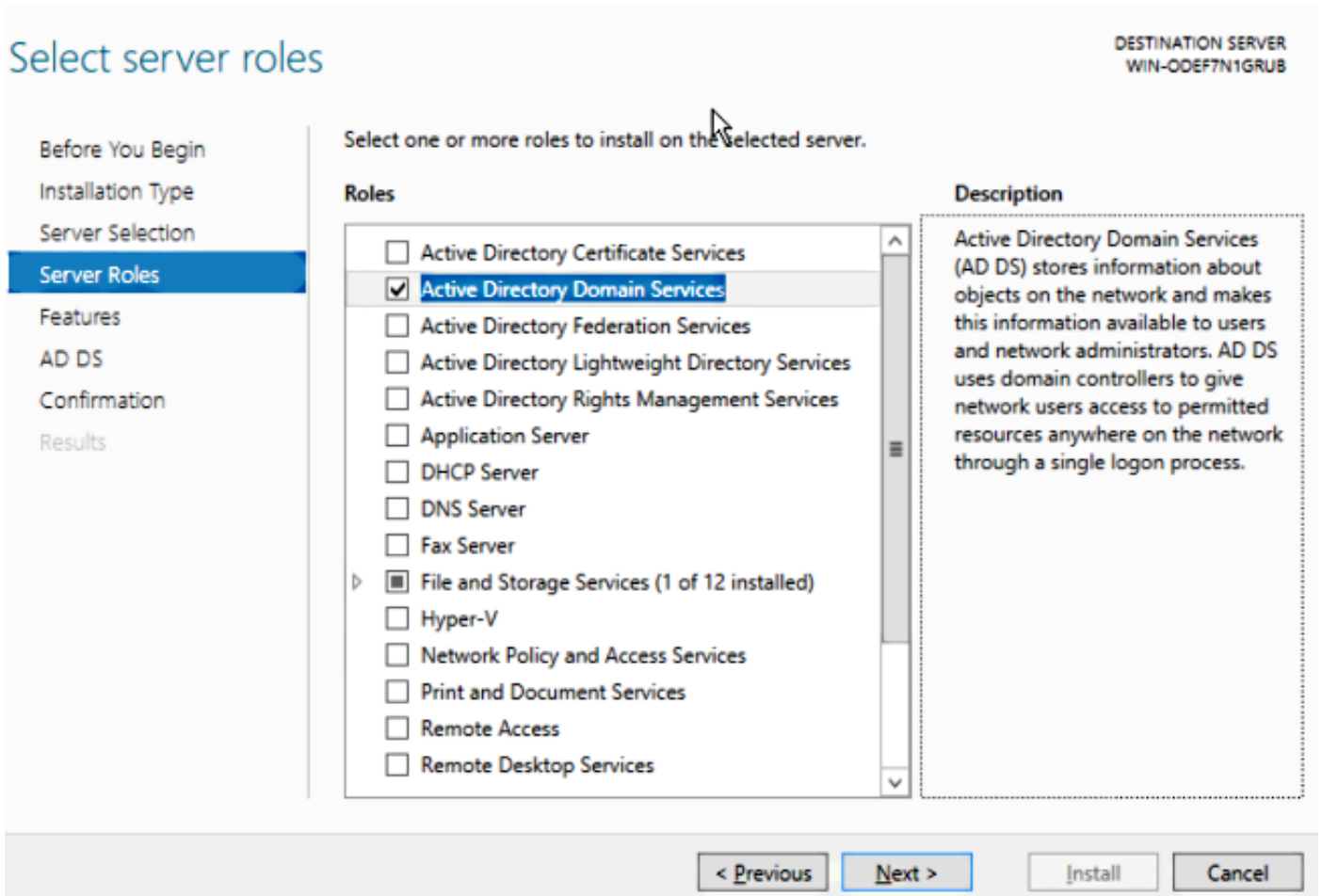
명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

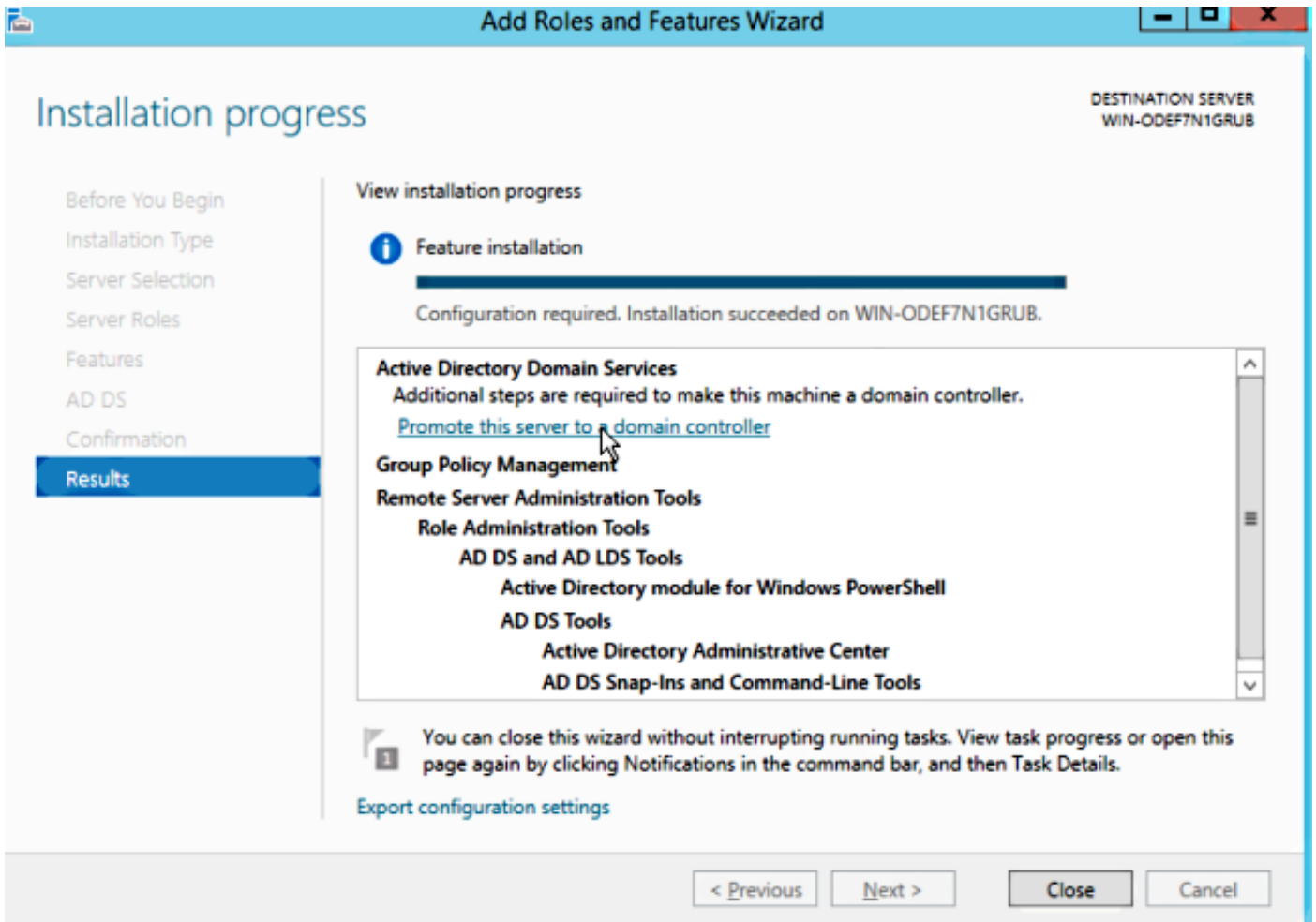
Microsoft Windows Server 구성

이 컨피그레이션은 새로 설치된 Microsoft Windows Server 2012에서 수행되는 것처럼 표시됩니다. 도메인 및 컨피그레이션에 단계를 조정해야 합니다.

1단계. 역할 및 기능 마법사에 대한 Active Directory 도메인 서비스를 설치합니다.

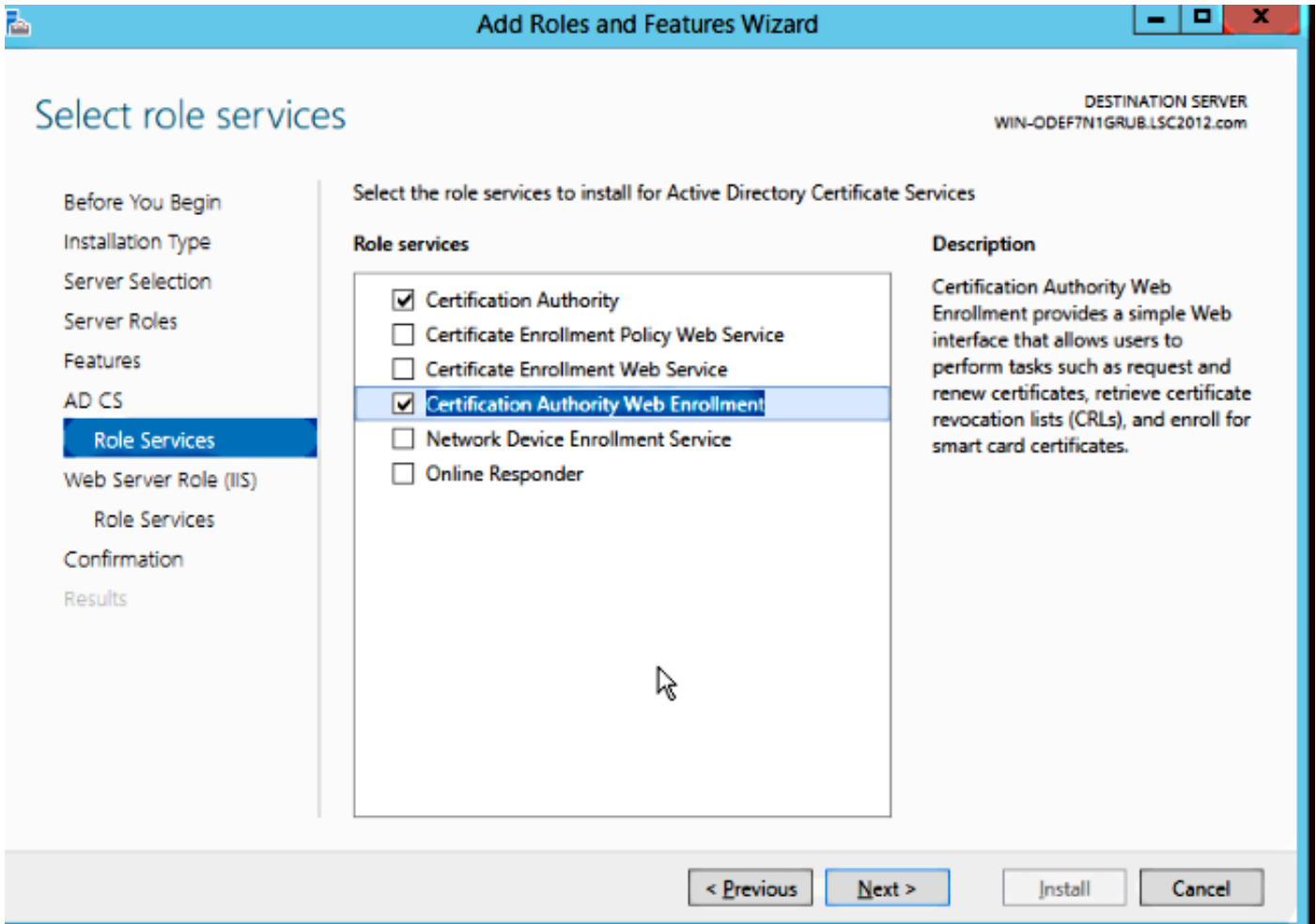


2단계. 설치 후 서버를 도메인 컨트롤러로 승격해야 합니다.

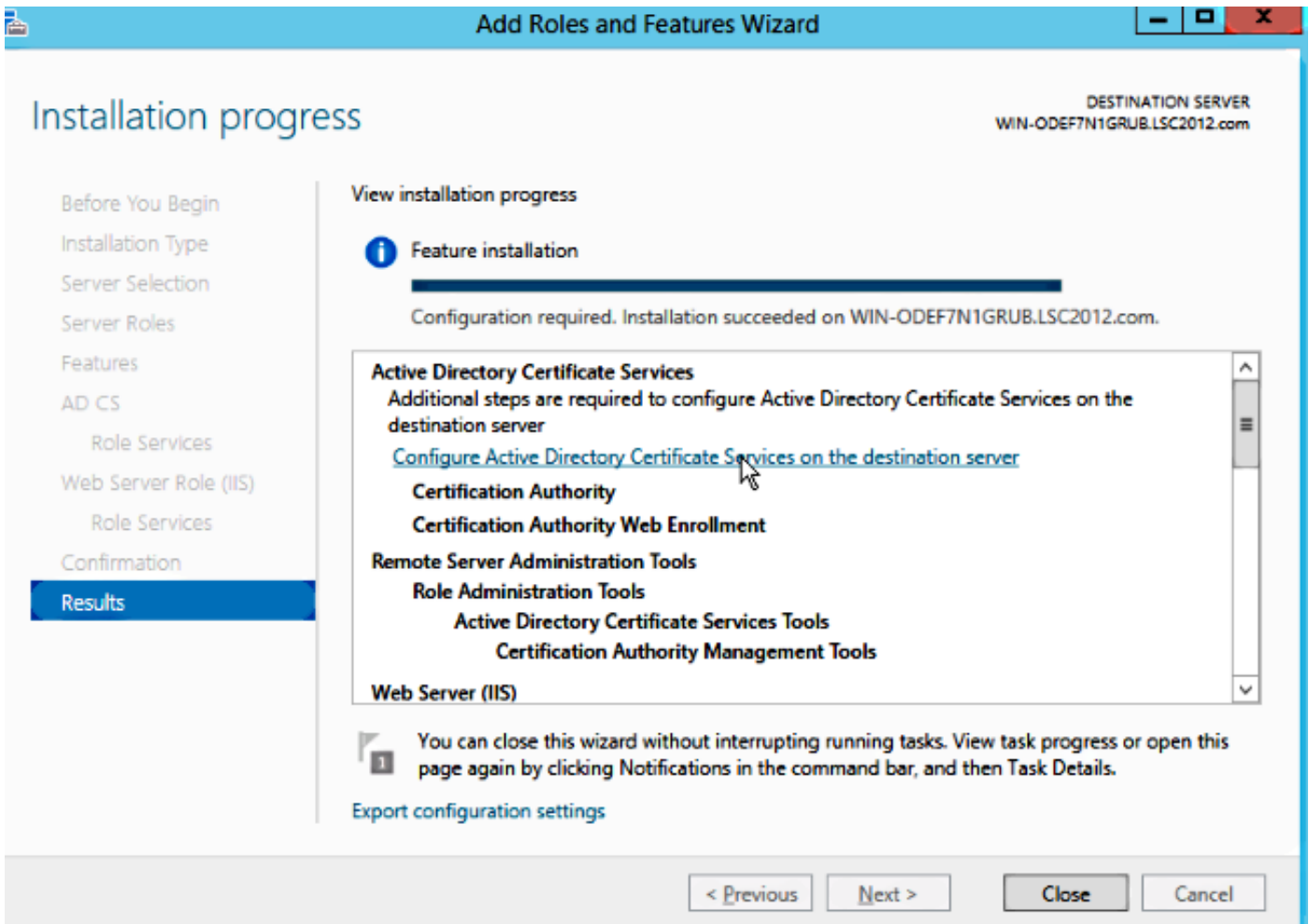


3단계. 새 설정이므로 새 포리스트를 구성합니다.일반적으로 기존 구축에서는 도메인 컨트롤러에서 이러한 지점을 구성하기만 하면 됩니다.여기서 LSC2012.com 도메인을 선택합니다.이렇게 하면 DNS(Domain Name Server) 기능도 활성화됩니다.

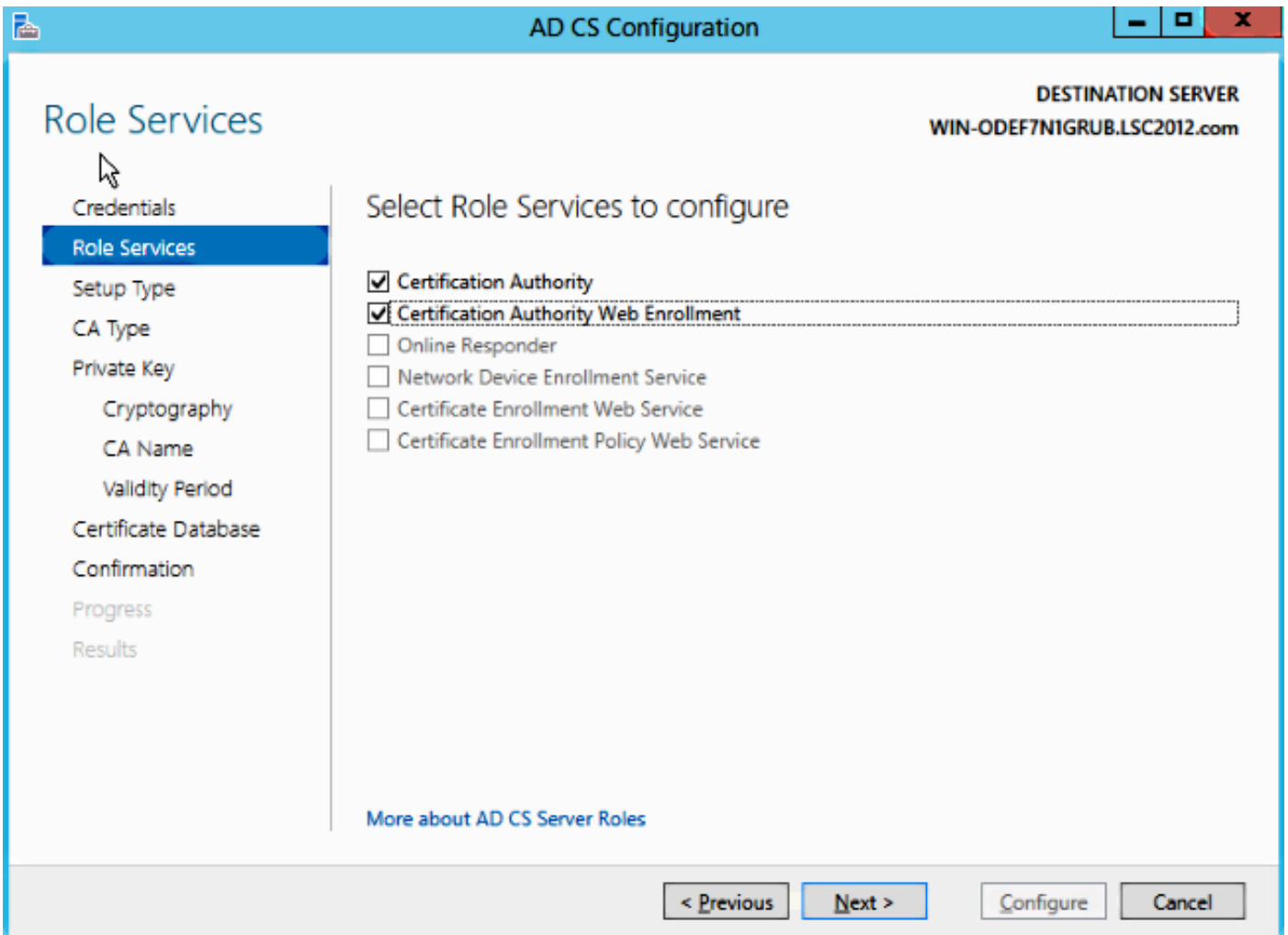
4단계. 재부팅한 후 CA(Certificate Authority) 서비스와 웹 등록을 설치합니다.



5단계.구성합니다.



6단계. Enterprise CA를 선택하고 모든 항목을 기본값으로 둡니다.

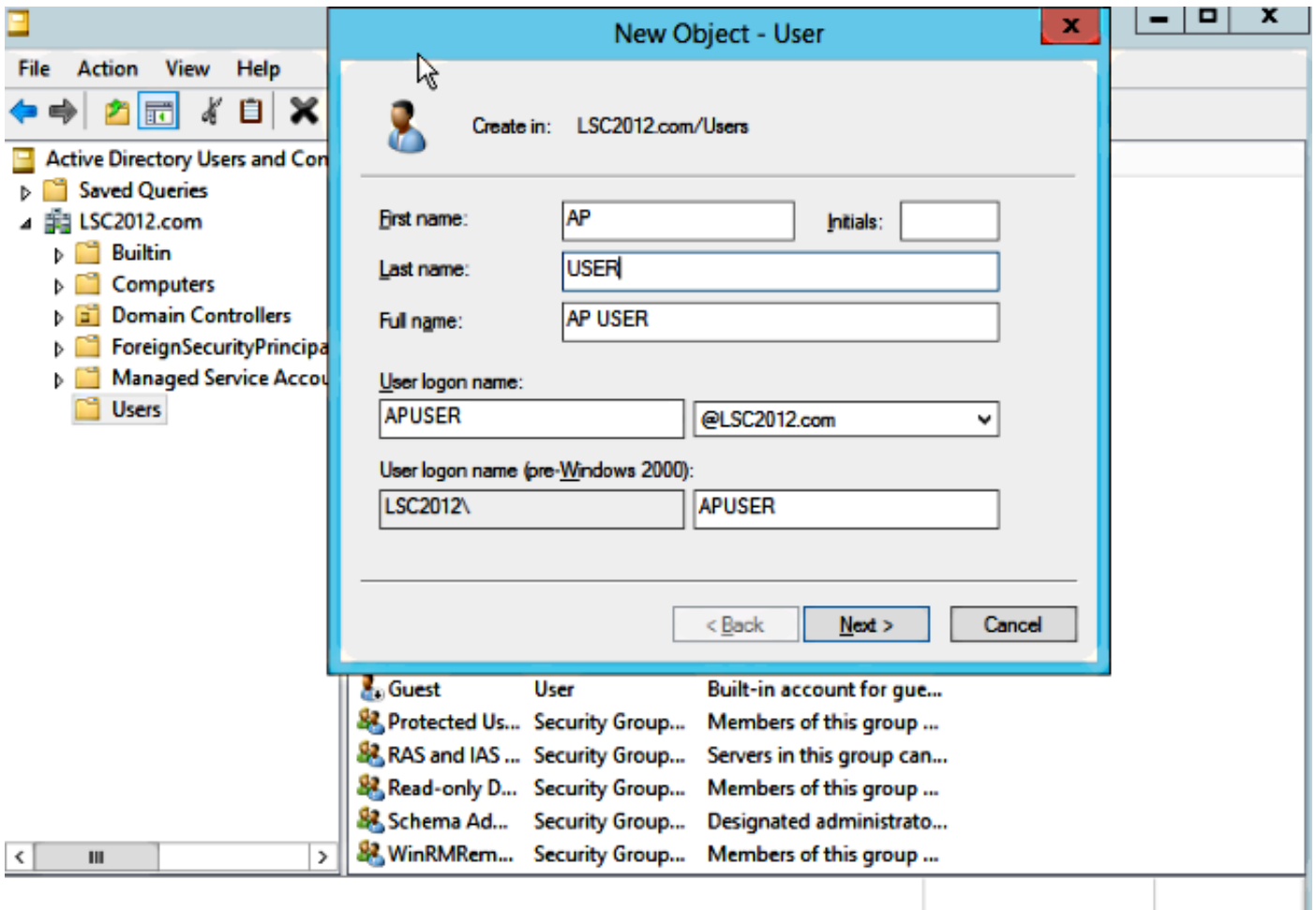


7단계. Microsoft Windows/Start 메뉴를 클릭합니다.

8단계. 관리 도구를 클릭합니다.

9단계. Active Directory 사용자 및 컴퓨터를 클릭합니다.

10단계. 도메인을 확장하고 Users 폴더를 마우스 오른쪽 버튼으로 클릭한 다음 New Object > User를 선택합니다.

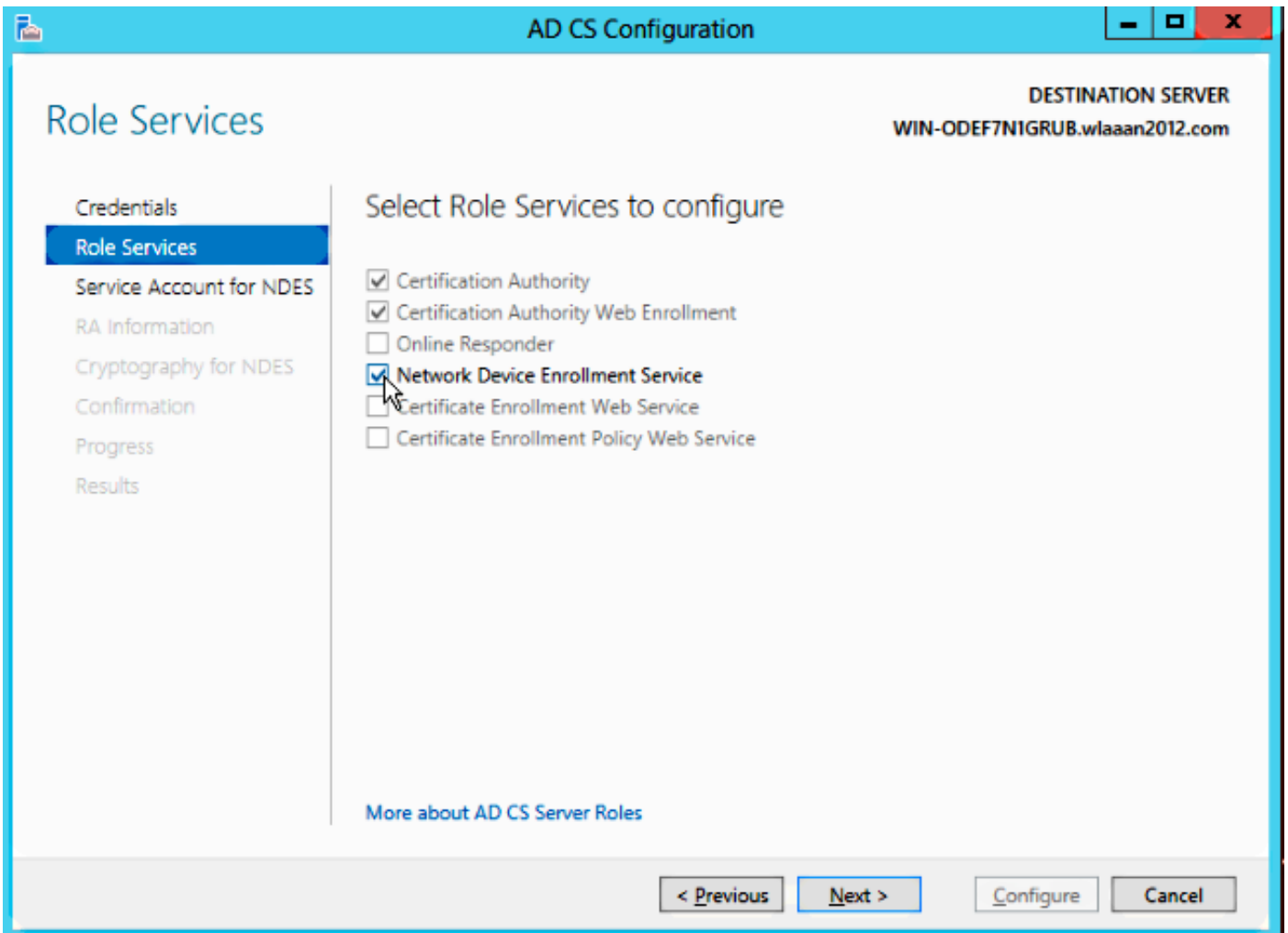


11단계. 이 예에서는 APUSER라는 이름을 지정합니다. 만든 후에는 사용자를 편집하고 MemberOf 탭을 클릭하여 IIS_IUSRS 그룹의 멤버로 만들어야 합니다.

필요한 사용자 권한 할당은 다음과 같습니다.

- 로컬로 로그인 허용
- 서비스로 로그인

12단계. NDES(Network Device Enrollment Service)를 설치합니다.



- IIS_USRS 그룹의 계정 멤버인 **APUSER**를 NDES의 서비스 계정으로 선택합니다.

13단계. 관리 도구로 이동합니다.

14단계. IIS(인터넷 정보 서비스)를 클릭합니다.

15단계. Server(서버) > Sites(사이트) > Default web site(기본 웹 사이트) > Cert Srv(인증서 srv)를 확장합니다.

16단계. mscep 및 mscep_admin 모두의 경우 인증을 클릭합니다. 익명 인증이 활성화되었는지 확인합니다.

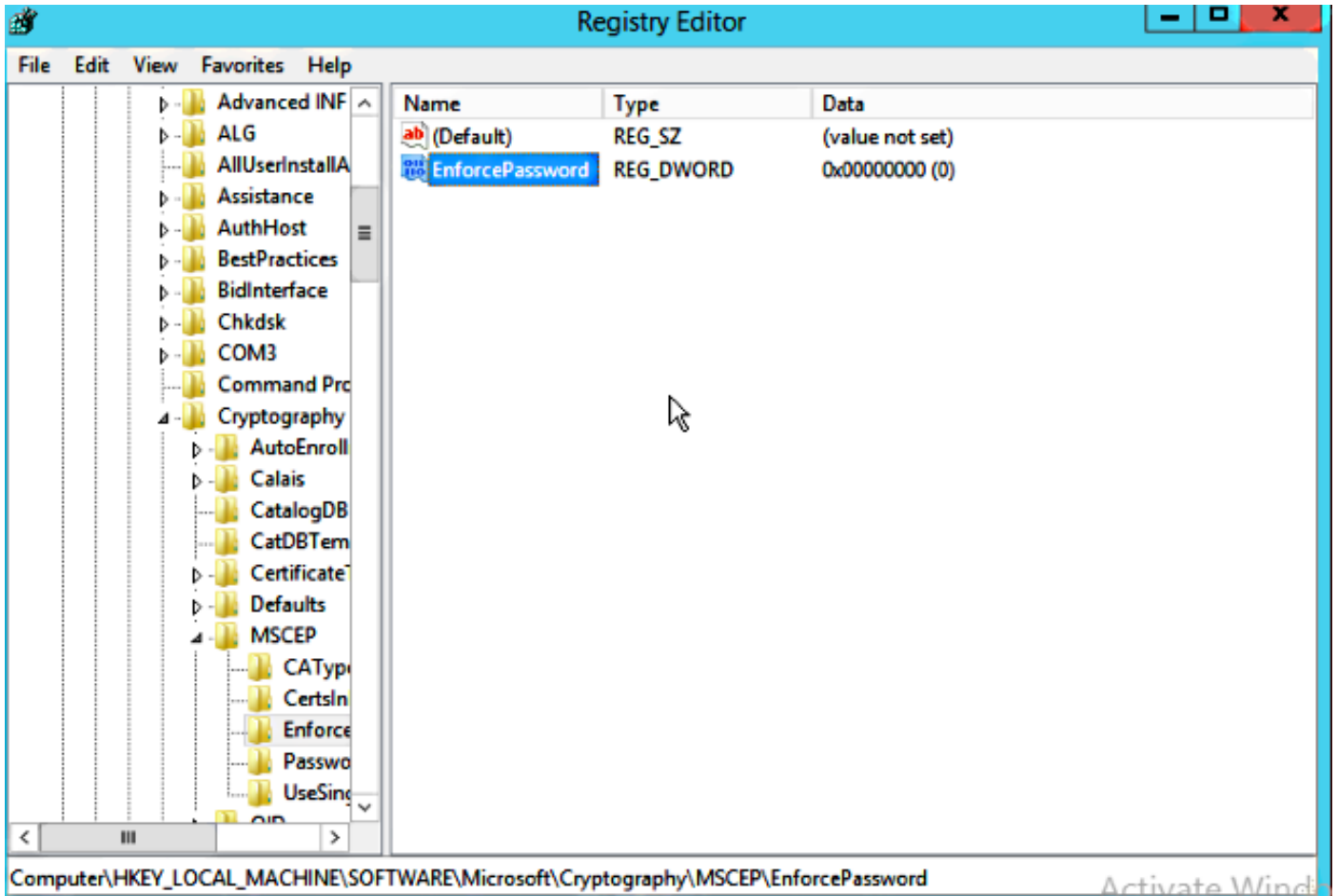
17단계. 마우스 오른쪽 버튼으로 Windows 인증을 클릭하고 Providers(제공자)를 선택합니다 .NTLM(NT LAN Manager)이 목록의 첫 번째 항목인지 확인합니다.

18단계. 레지스트리 설정에서 인증 챌린지를 비활성화하십시오. 그렇지 않으면 SCEP(Simple Certificate Enrollment Protocol)은 WLC에서 지원하지 않는 챌린지 비밀번호 인증을 요구합니다.

19단계. regedit 애플리케이션을 엽니다.

20단계. HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\으로 이동합니다.

21단계. EnforcePassword를 0으로 설정합니다.



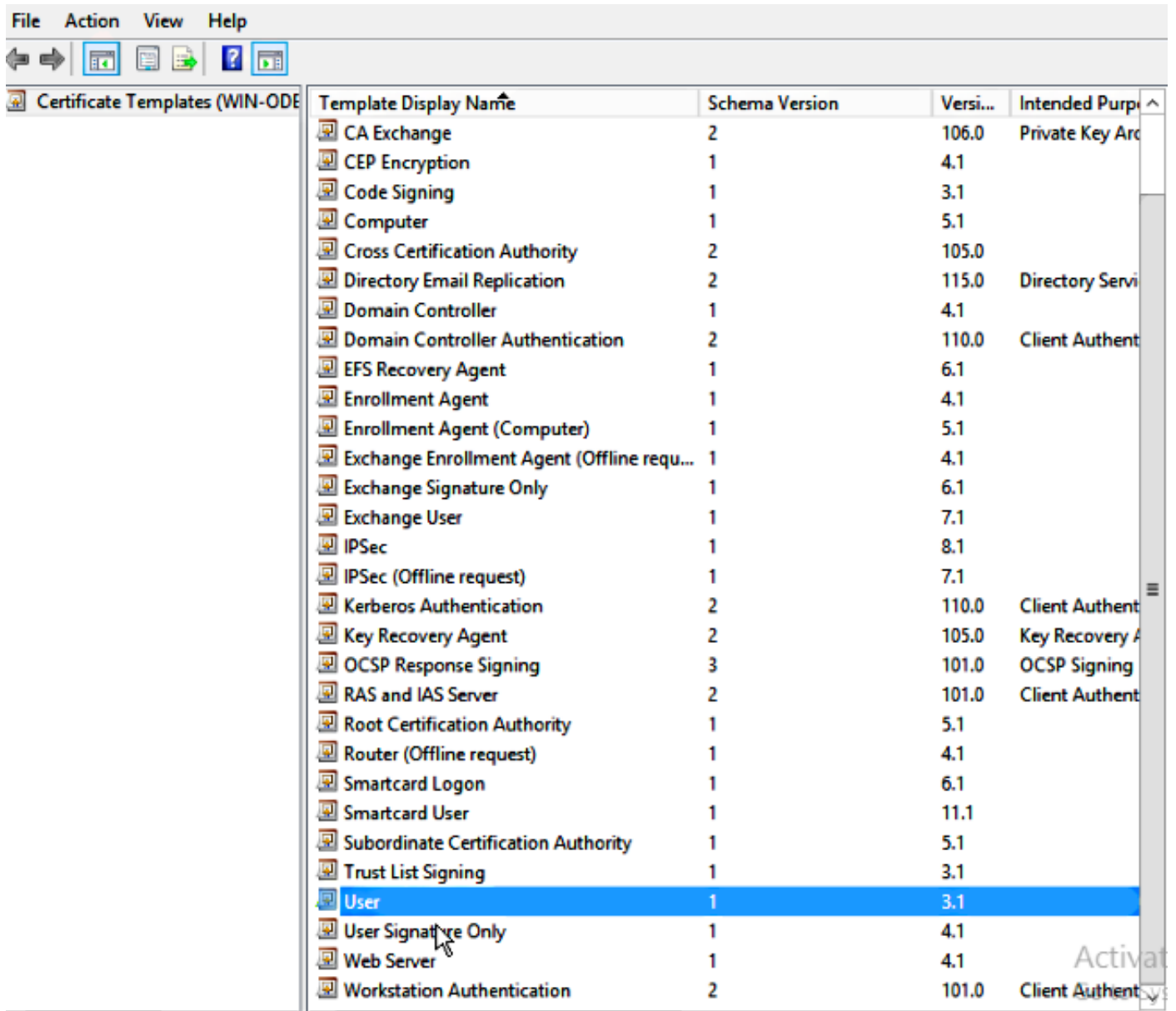
22단계. Microsoft Windows/Start 메뉴를 클릭합니다.

23단계. MMC를 입력합니다.

24단계. [파일] 메뉴에서 [스냅인 추가/제거]를 선택합니다. Certification Authority를 선택합니다.

25단계. Certificate Template(인증서 템플릿) 폴더를 마우스 오른쪽 버튼으로 클릭하고 Manage(관리)를 클릭합니다.

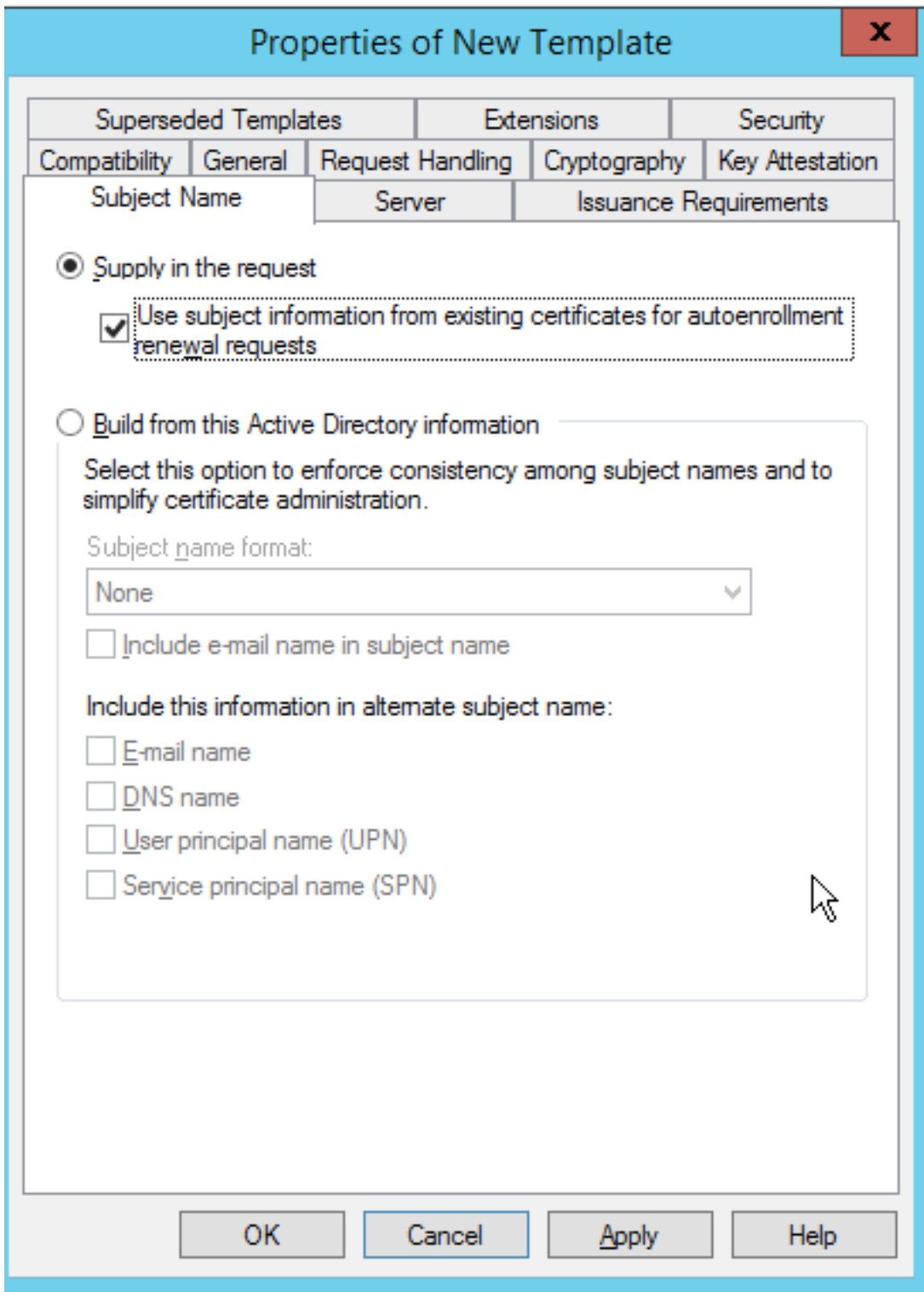
26단계. User와 같은 기존 템플릿을 마우스 오른쪽 버튼으로 클릭하고 Duplicate Template(템플릿 복제)을 선택합니다.



27단계. Microsoft Windows 2012 R2로 사용할 CA를 선택합니다.

28단계. General(일반) 탭에서 WLC 및 유효 기간과 같은 표시 이름을 추가합니다.

29단계. Subject Name(주체 이름) 탭에서 요청의 Supply in the request(공급)가 선택되었는지 확인합니다.



30단계. Issuance **Requirements** 탭을 클릭합니다. Cisco에서는 일반적인 계층적 CA 환경에서 발급 정책을 공백으로 두는 것이 좋습니다.

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

Require the following for enrollment:

CA certificate manager approval

This number of authorized signatures:

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Require the following for reenrollment:

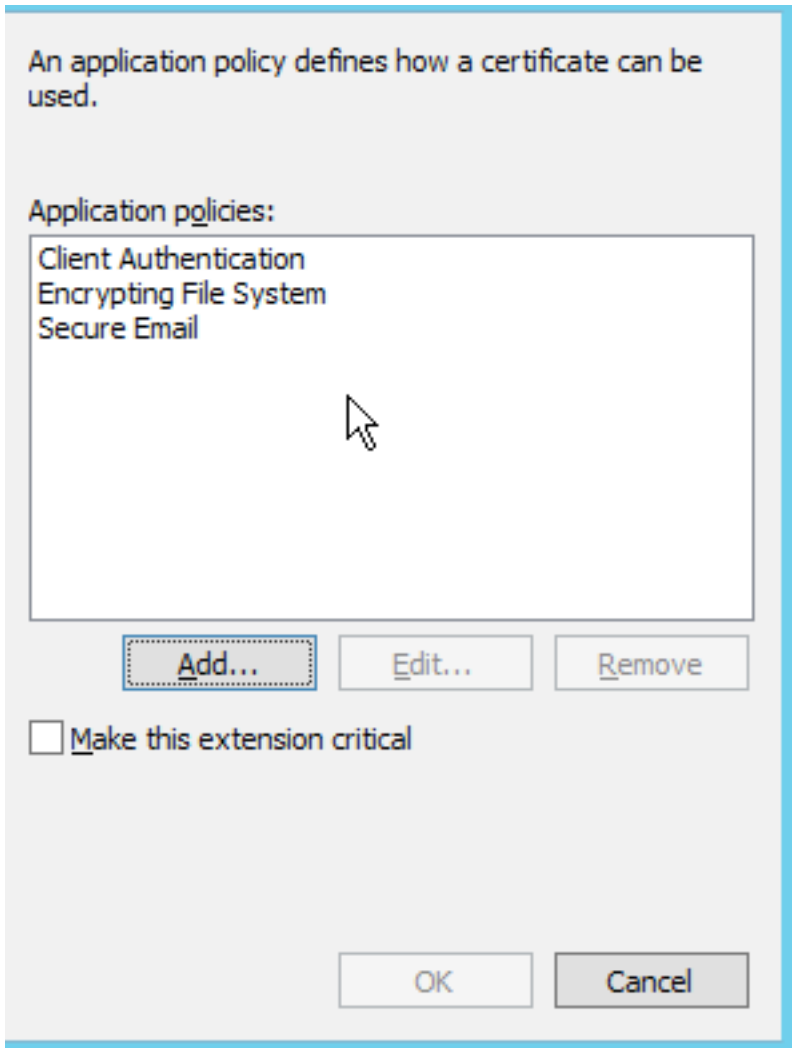
Same criteria as for enrollment

Valid existing certificate

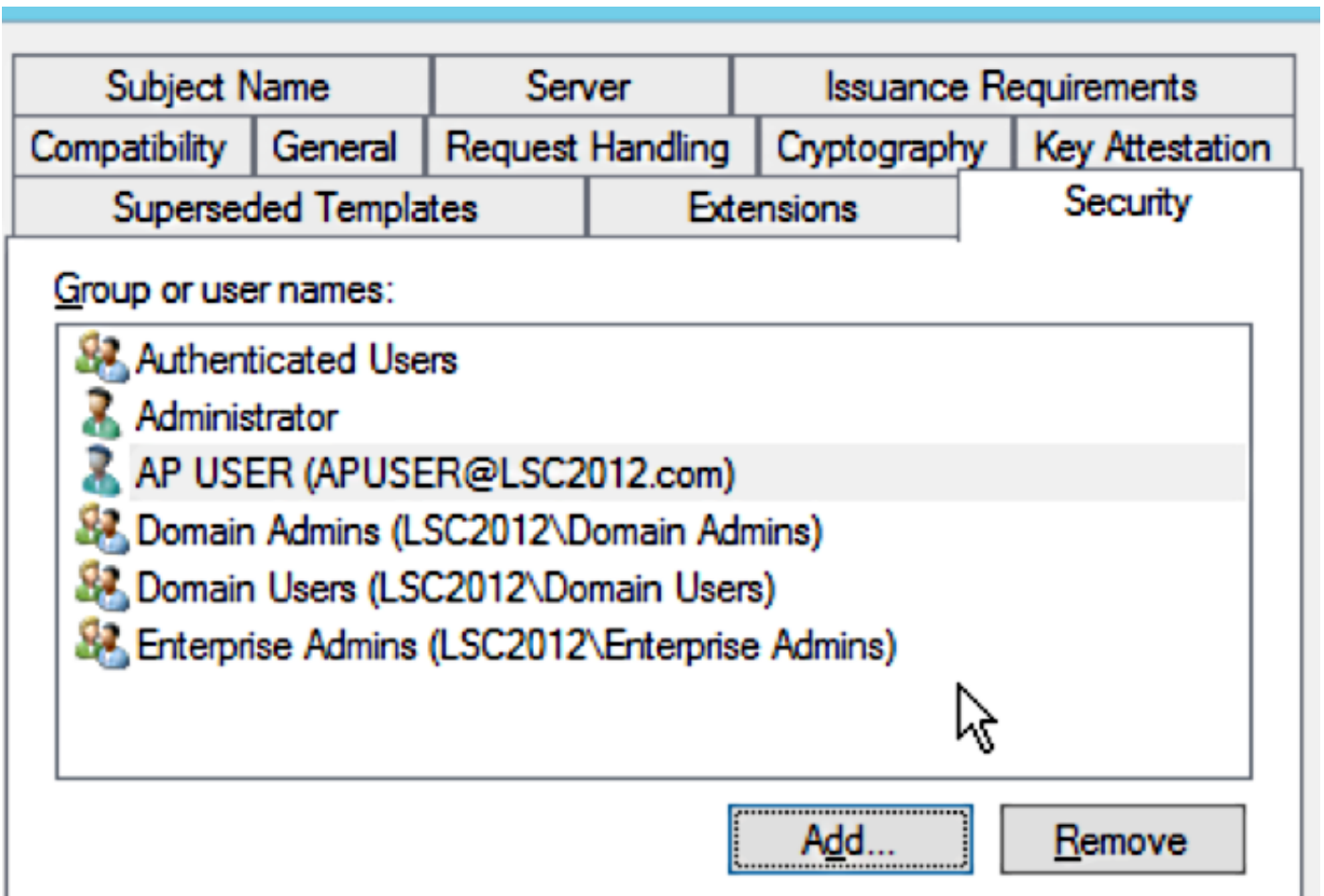
Allow key based renewal

Requires subject information to be provided within the certificate request.

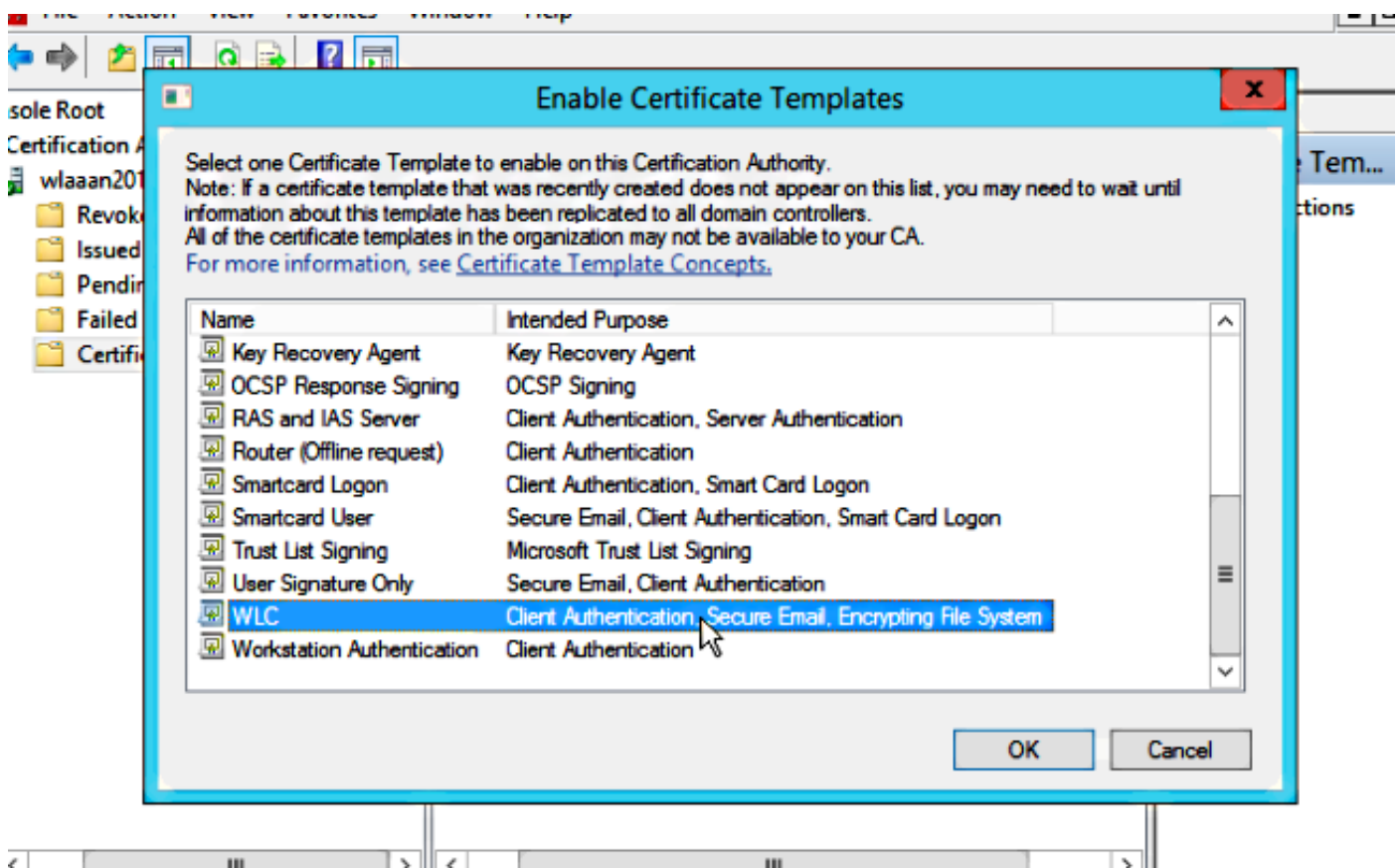
31단계. Extensions 탭, Application Policies(애플리케이션 정책)를 클릭한 다음 Edit(수정)를 클릭합니다. Add(추가)를 클릭하고 Client Authentication(클라이언트 인증)이 애플리케이션 정책으로 추가되었는지 확인합니다. 확인을 클릭합니다.



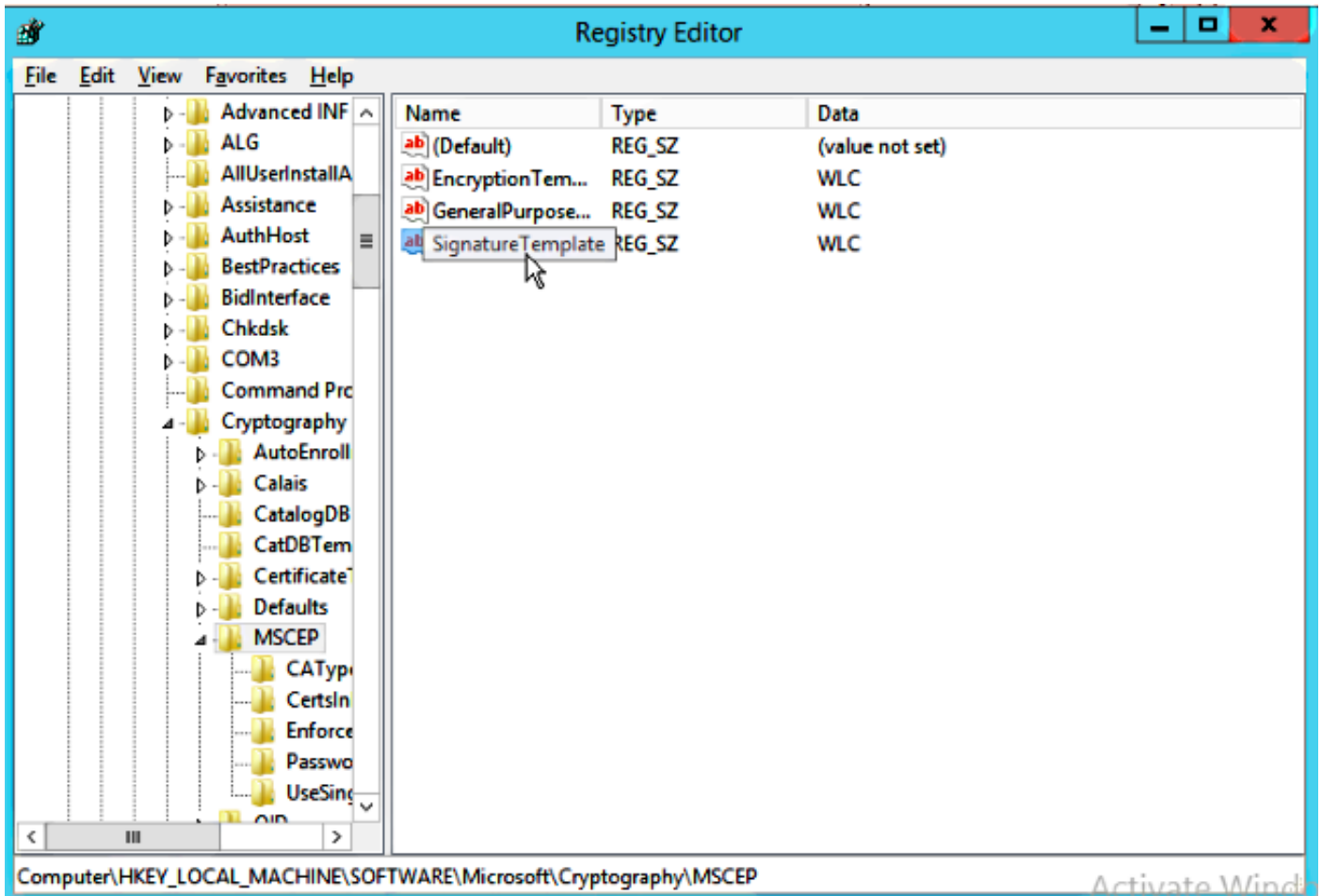
32단계. 보안 탭을 클릭한 다음 추가...를 클릭합니다..NDES 서비스 설치에 정의된 SCEP 서비스 계정이 템플릿을 완전히 제어하는지 확인하고 OK(확인)를 클릭합니다.



33단계. 인증 기관 GUI 인터페이스로 돌아갑니다. Certificate Templates 디렉토리를 마우스 오른쪽 버튼으로 클릭합니다. New(새로 만들기) > Certificate Template to Issue(발급할 인증서 템플릿)로 이동합니다. 이전에 구성한 WLC 템플릿을 선택하고 OK를 클릭합니다.



34단계. Computer(컴퓨터) > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP의 레지스트리 설정에서 기본 SCEP 템플릿을 변경합니다.
EncryptionTemplate, GeneralPurposeTemplate 및 SignatureTemplate 키를 IPsec(Offline Request)에서 이전에 만든 WLC 템플릿으로 변경합니다.



35단계. 시스템을 재부팅합니다.

WLC 구성

1단계. WLC에서 Security(보안) 메뉴로 이동합니다.Certificates > LSC를 클릭합니다.

2단계. Enable LSC on Controller(컨트롤러에서 LSC 활성화) 확인란을 선택합니다.

3단계. Microsoft Windows Server 2012 URL을 입력합니다.기본적으로 /certsrv/mscep/mscep.dll이 추가됩니다.

4단계. Params(매개변수) 섹션에 세부사항을 입력합니다.

5단계. 변경 사항을 적용합니다.

Local Significant Certificates (LSC)

Apply

General

AP Provisioning

Certificate Type

Status

CA

Present



General

Enable LSC on Controller



CA Server

CA server URL

http://10.48.39.197/certsrv/mscep/mscep.dll

(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code

BE

State

Belgium

City

Brussel

Organization

Cisco

Department

R&D

E-mail

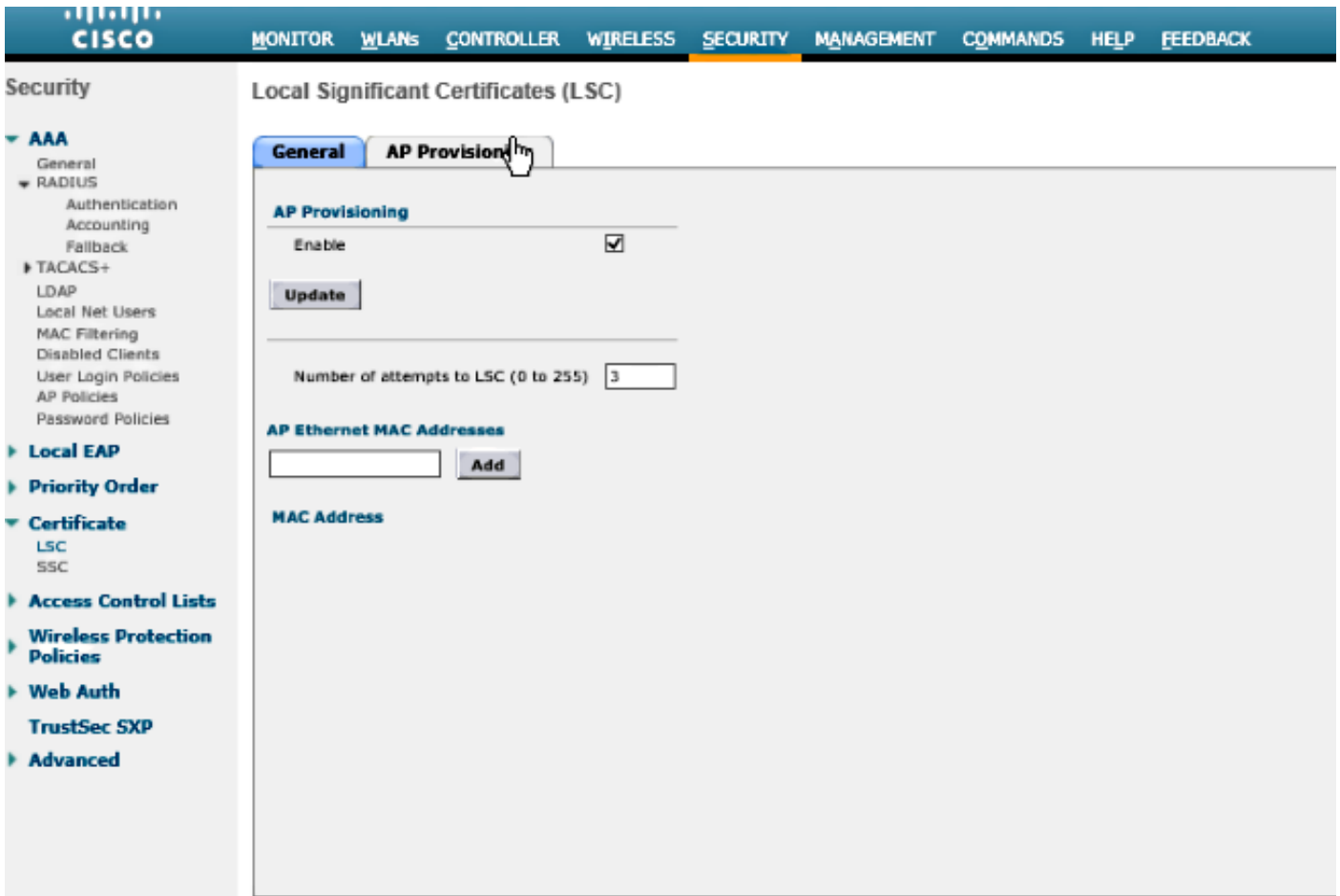
rmanchur@wlaaan.com

Key Size

2048

6단계. 위쪽 CA 행에서 파란색 화살표를 클릭하고 Add(추가)를 선택합니다. 상태를 Not present(없음)에서 present(있음)로 변경해야 합니다.

7단계. AP 프로비저닝 탭을 클릭합니다.



8단계. AP Provisioning(AP 프로비저닝) 아래에서 Enable(활성화) 확인란을 선택하고 Update(업데이트)를 클릭합니다.

9단계. 액세스 포인트가 재부팅되지 않은 경우 재부팅합니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

재부팅 후 액세스 포인트는 Wireless(무선) 메뉴에서 LSC와 함께 다시 연결하고 인증서 유형으로 표시됩니다.

Wireless

All APs Entries 1 - 2 of 2

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

Number of APs: 2

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode	Certificate Type
CAP1501-1	AIR-CA735011-2-K9	c8:9c:1d:6e:a3:cd	0 d, 00 h 35 m 21 s	Disabled	REG	1	Local	LSC
LAP1142-1	AIR-LAP1142N-1-K9	ac:f2:c5:73:33:ce	0 d, 00 h 02 m 35 s	Enabled	REG	1	Local	LSC

참고:8.3.112 후에는 LSC가 활성화되면 MIC AP가 전혀 참여할 수 없습니다.따라서 "LSC 시도" 카운트 기능은 제한된 사용이 됩니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.