CAPF Online CA를 통한 자동 인증서 등록 및 갱신 구성

목차

소개

이 문서에서는 CUCM(Cisco Unified Communications Manager)용 CAPF(Certificate Authority Proxy Function) Online 기능을 통한 자동 인증서 등록 및 갱신에 대해 설명합니다.

기고자: Michael Mendoza, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Unified Communications Manager
- X.509 인증서
- Windows 서버
- Windows AD(Active Directory)
- Windows 인터넷 정보 서비스(IIS)
- NT(신기술) NTLM(LAN Manager) 인증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 버전 12.5.1.10000-22
- Windows Server 2012 R2
- IP Phone CP-8865 / 펌웨어: SIP 12-1-1SR1-4 및 12-5-1SR2.

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

이 문서에서는 추가 연구를 위한 기능 및 관련 리소스의 구성을 다룹니다.

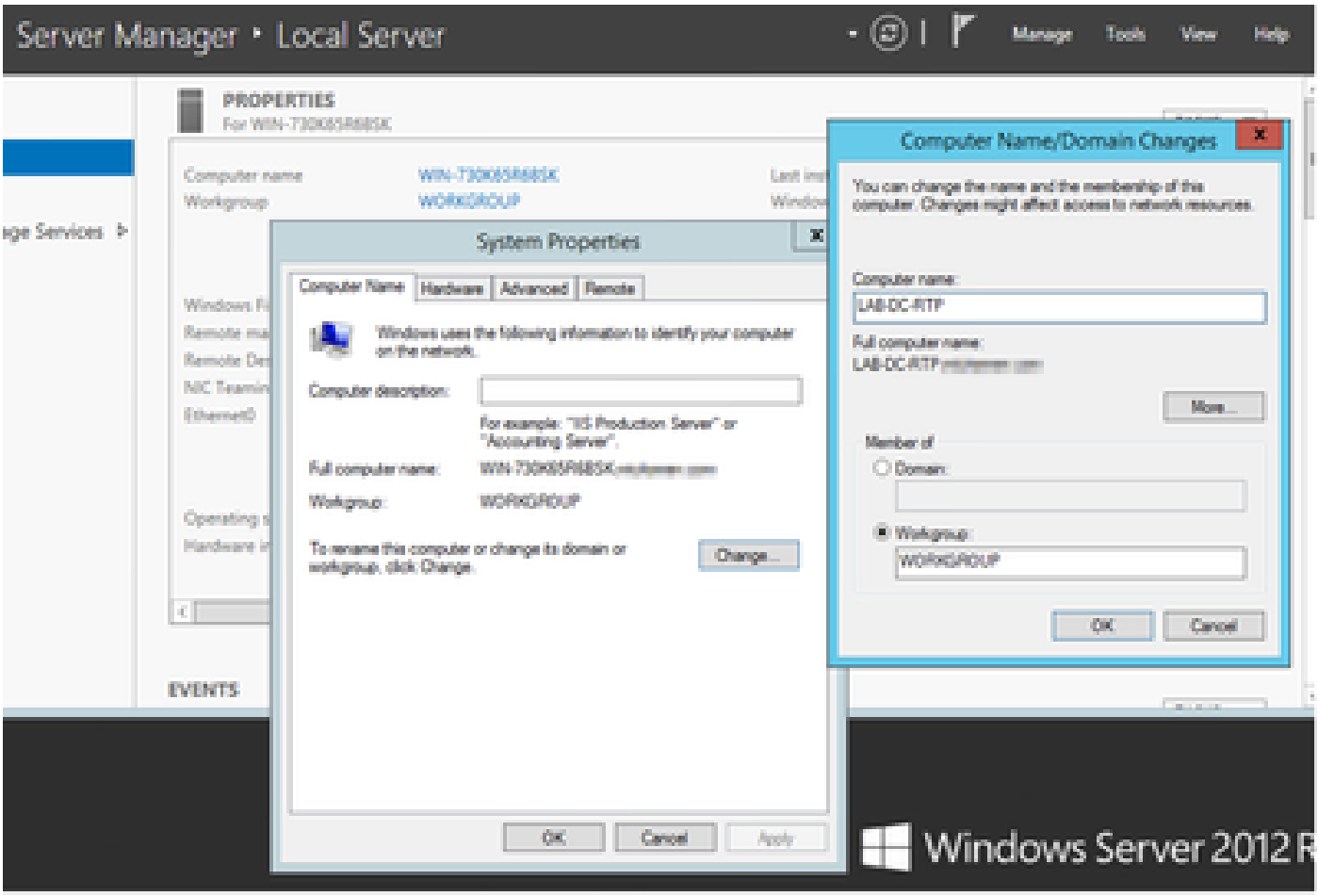
서버 시간 및 날짜 확인

Windows 서버가 서버의 루트 CA(Certificate Authority) 인증서뿐만 아니라 서버에서 발급한 인증서의 유효 시간에 영향을 미치므로 올바른 날짜, 시간 및 표준 시간대를 구성했는지 확인합니다.

업데이트 서버 컴퓨터 이름

기본적으로 서버의 컴퓨터 이름에는 WIN-730K65R6BSK와 같은 임의의 이름이 있습니다. AD 도메인 서비스를 활성화하기 전에 먼저 서버의 컴퓨터 이름을 설치 종료 시까지 서버의 호스트 이름 및 루트 CA 발급자 이름으로 업데이트해야 합니다. 그렇지 않으면 AD 서비스를 설치한 후 이를 변경하는 데 많은 추가 단계가 필요합니다.

- Local Server(로컬 서버)로 이동하여 Computer name(컴퓨터 이름)을 선택하여 System Properties(시스템 속성)를 엽니다
- 변경 단추를 선택하고 새 컴퓨터 이름을 입력합니다.



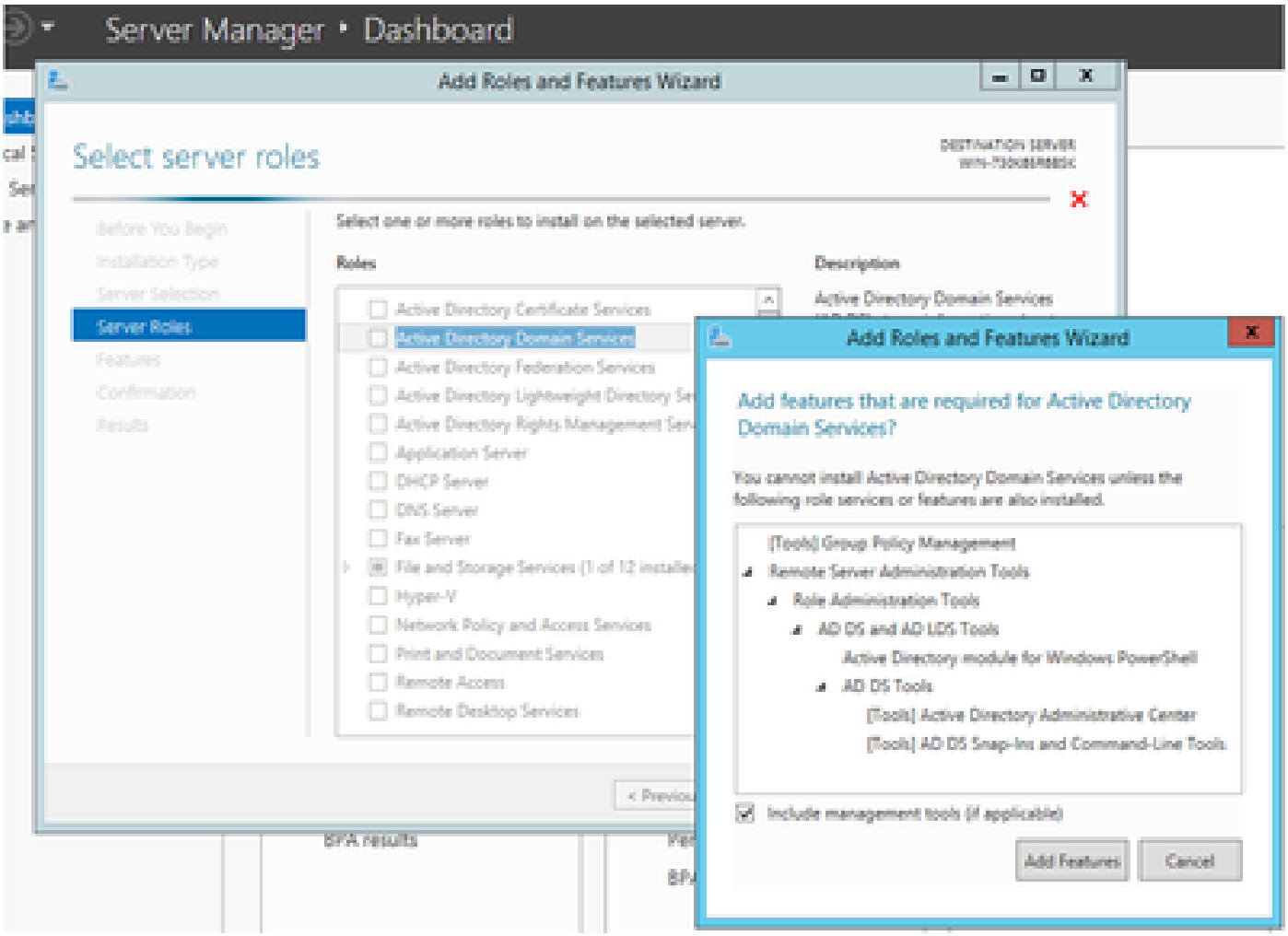
- 변경 내용을 적용하려면 서버를 다시 시작하십시오.

구성

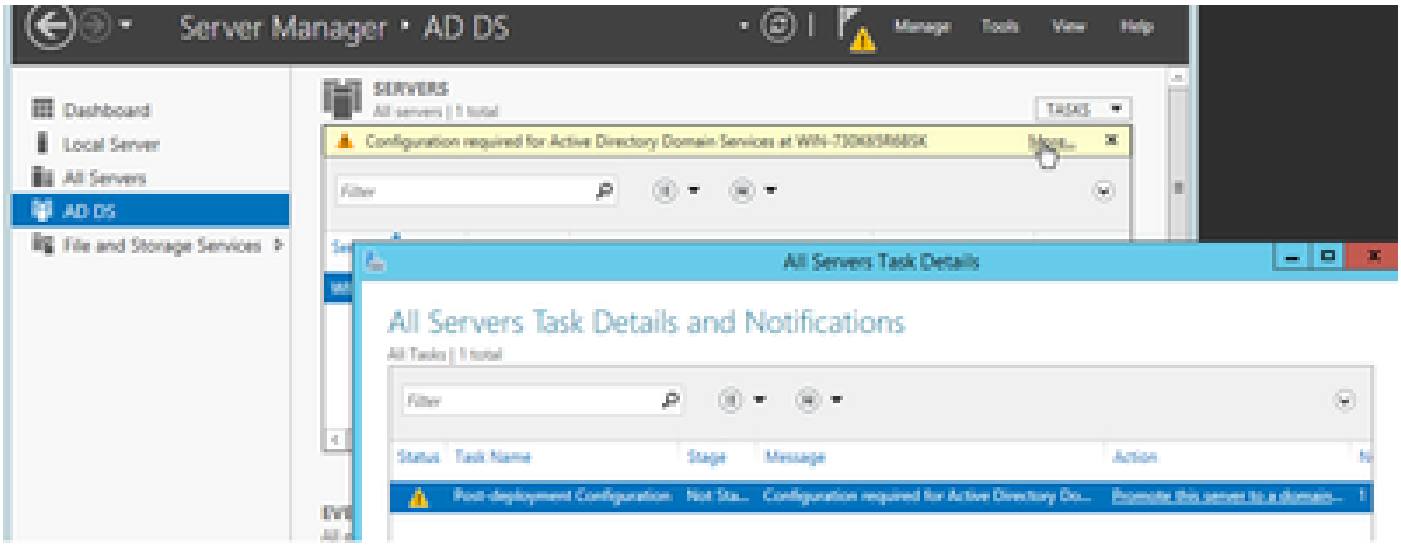
AD 서비스, 사용자 및 인증서 템플릿

Active Directory 서비스 활성화 및 구성

- 서버 관리자에서 [역할 및 기능 추가] 옵션을 선택하고 역할 기반 또는 기능 기반 설치를 선택한 다음 풀에서 서버를 선택한 다음(풀에는 하나만 있어야 함) Active Directory 도메인 서비스를 선택합니다.

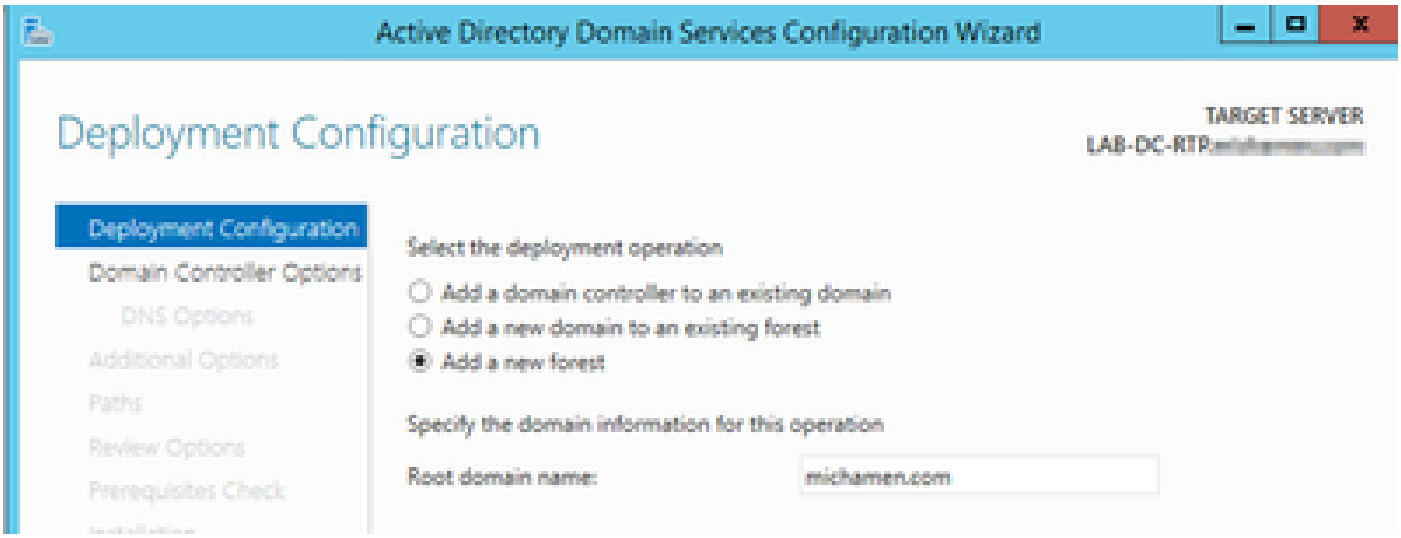


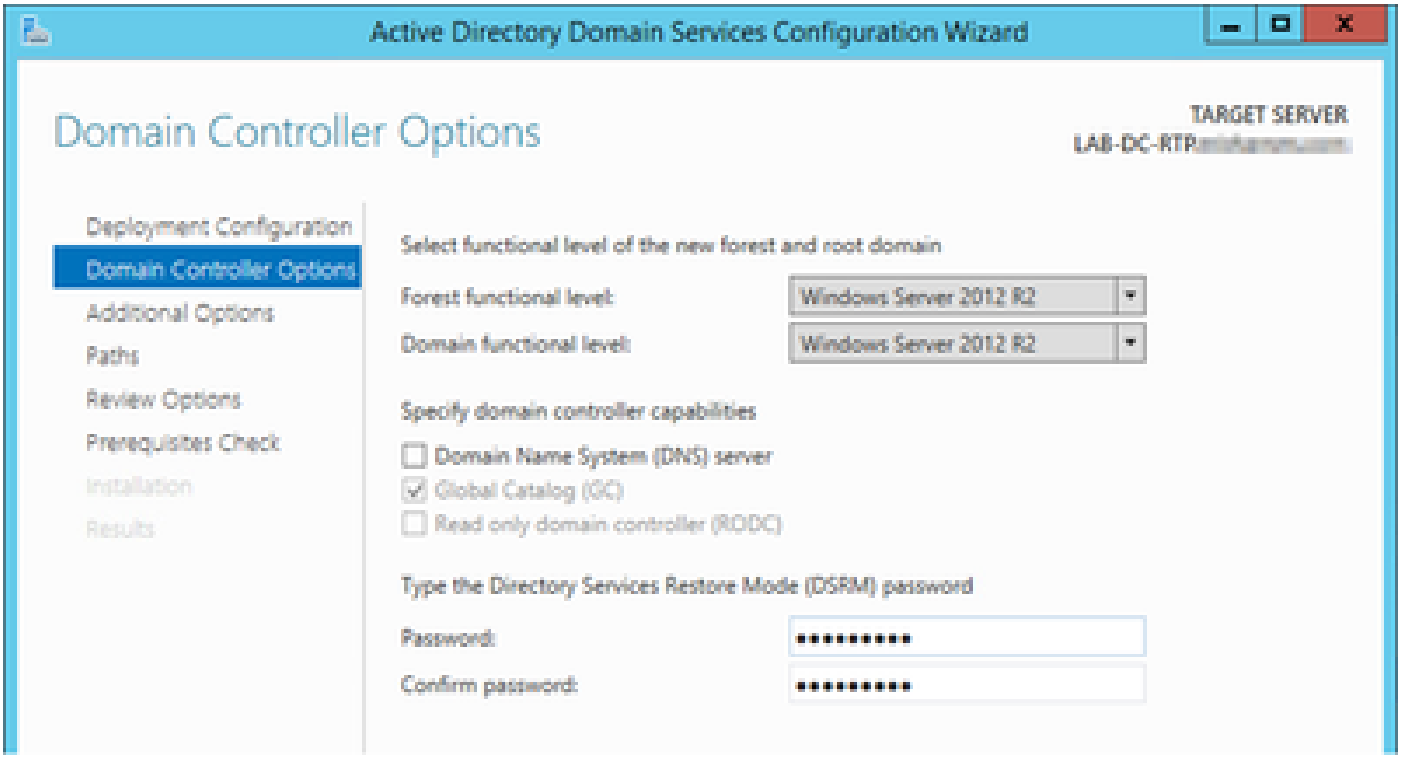
- 다음 단추를 계속 선택한 다음 설치
- 설치가 완료되면 닫기 단추를 선택합니다
- 서버 관리자 > AD DS 아래에 Active Directory 도메인 서비스에 필요한 구성 이라는 제목의 경고 탭이 나타납니다. 다른 링크를 선택한 다음 사용 가능한 작업을 선택하여 설치 마법사를 시작합니다.



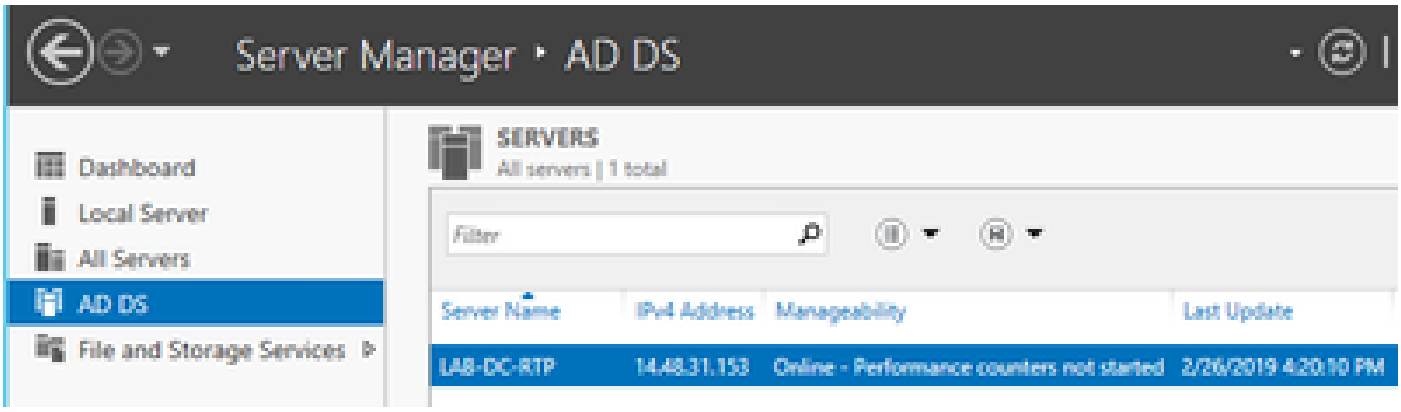
- 도메인 설정 마법사의 프롬프트에 따라 원하는 루트 도메인 이름(이 실습에 michamen.com 사용)을 사용하여 새 포리스트를 추가하고 사용 가능한 경우 DNS 확인란의 선택을 취소하고

DSRM 암호(이 실습에 C1sc0123 사용)를 정의합니다.



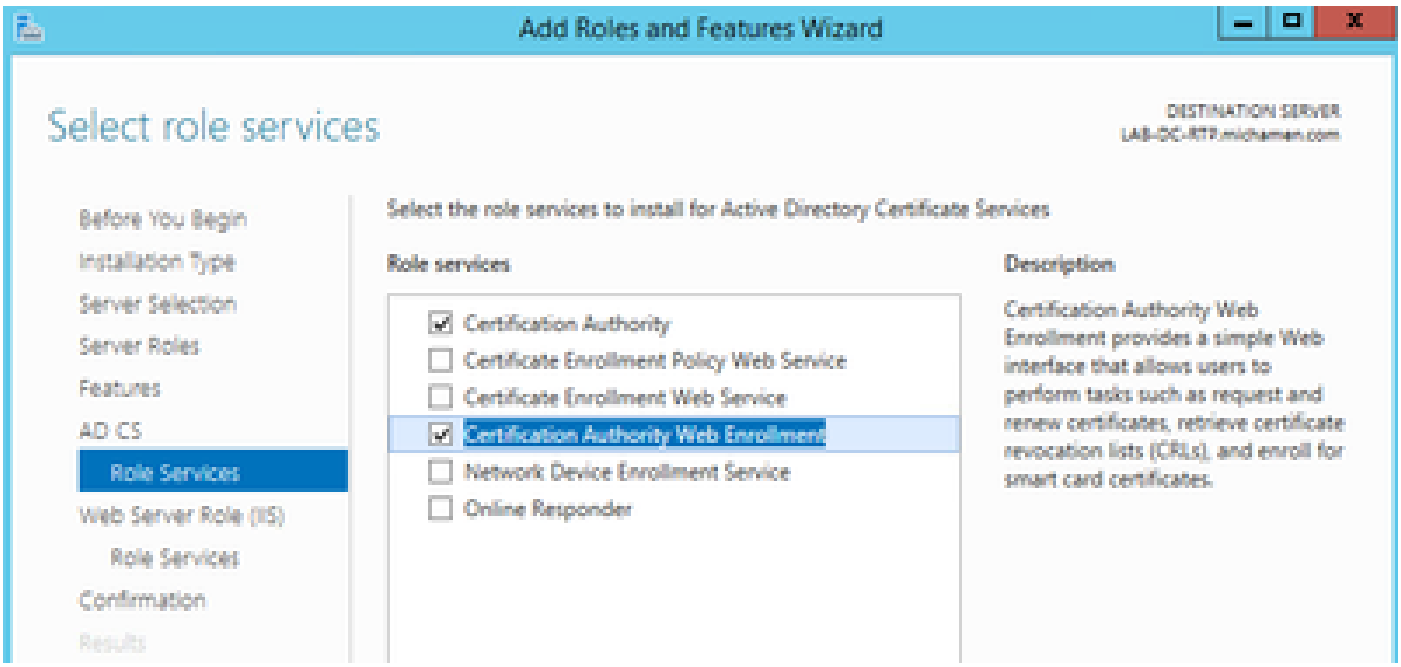


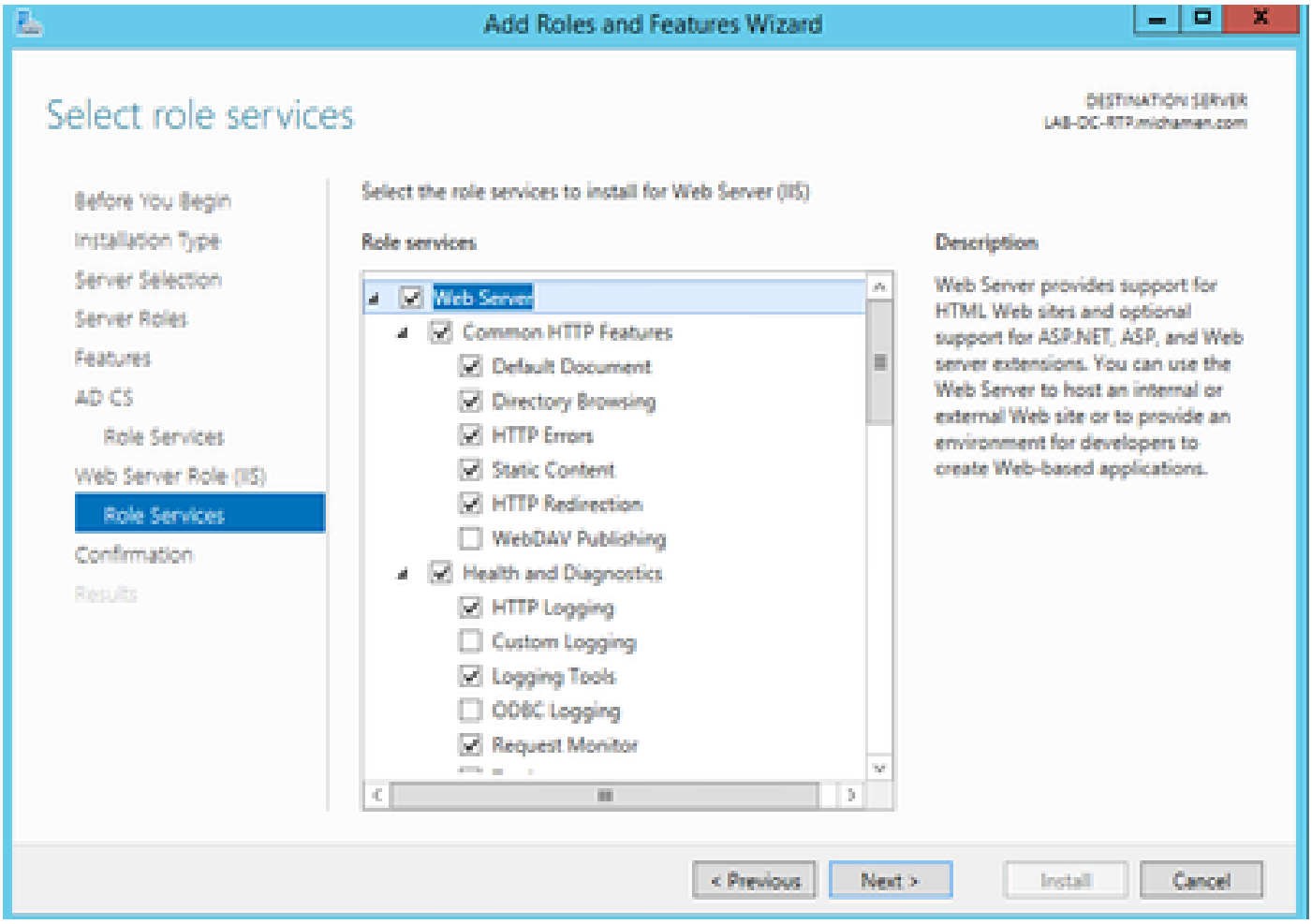
- NetBIOS 도메인 이름을 지정해야 합니다(이 실습에서 MICHAMEN1에 사용됨).
- 마법사를 따라 완료합니다. 그런 다음 서버가 재부팅되어 설치를 완료합니다.
- 다음에 로그인할 때 새 도메인 이름을 지정해야 합니다. 예: MICHAMEN1\Administrator.



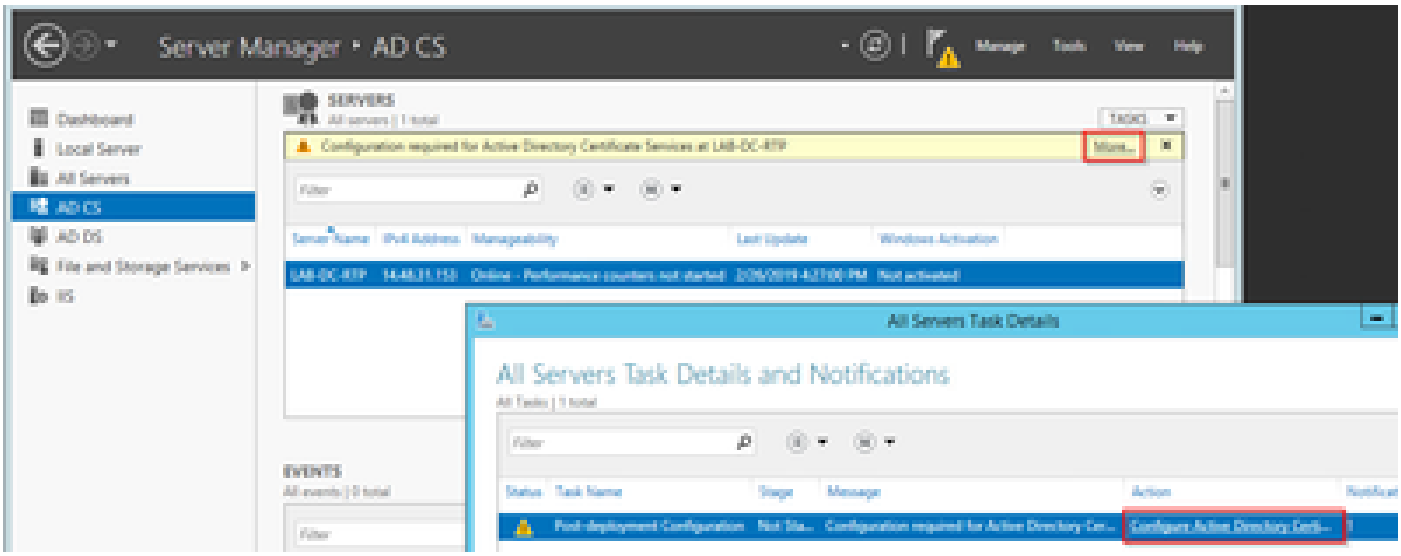
인증서 서비스 활성화 및 구성

- 서버 관리자에서 역할 및 기능 추가를 선택합니다
- Active Directory Certificate Services(Active Directory 인증서 서비스)를 선택하고 프롬프트에 따라 필요한 기능을 추가합니다(사용 가능한 모든 기능은 이 실습에 대해 활성화된 역할 서비스에서 선택됨).
- Role Services의 경우 인증 기관 웹 등록 확인



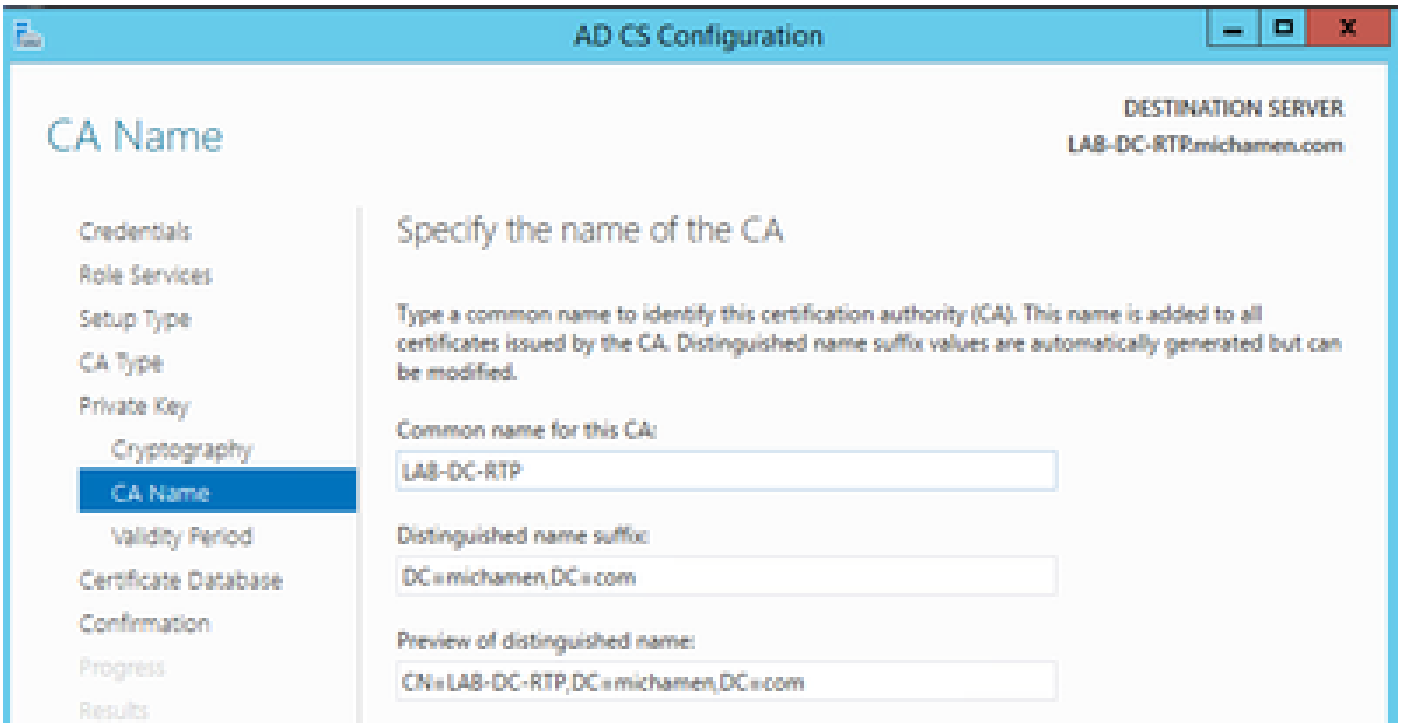


- 경고 탭은 서버 관리자 >AD DS 아래에 Active Directory 인증서 서비스에 필요한 구성 이라는 제목으로 나타나야 합니다. more 링크를 선택한 다음 사용 가능한 작업을 선택하십시오.



- AD-CS 설치 후 구성 마법사에서 다음 단계를 진행합니다.
- 인증 기관 및 인증 기관 웹 등록 역할 선택
- 옵션이 있는 Enterprise CA를 선택합니다.
- 루트 CA
- 새 개인 키 만들기
- 개인 키 사용 - SHA1(기본 설정 포함)

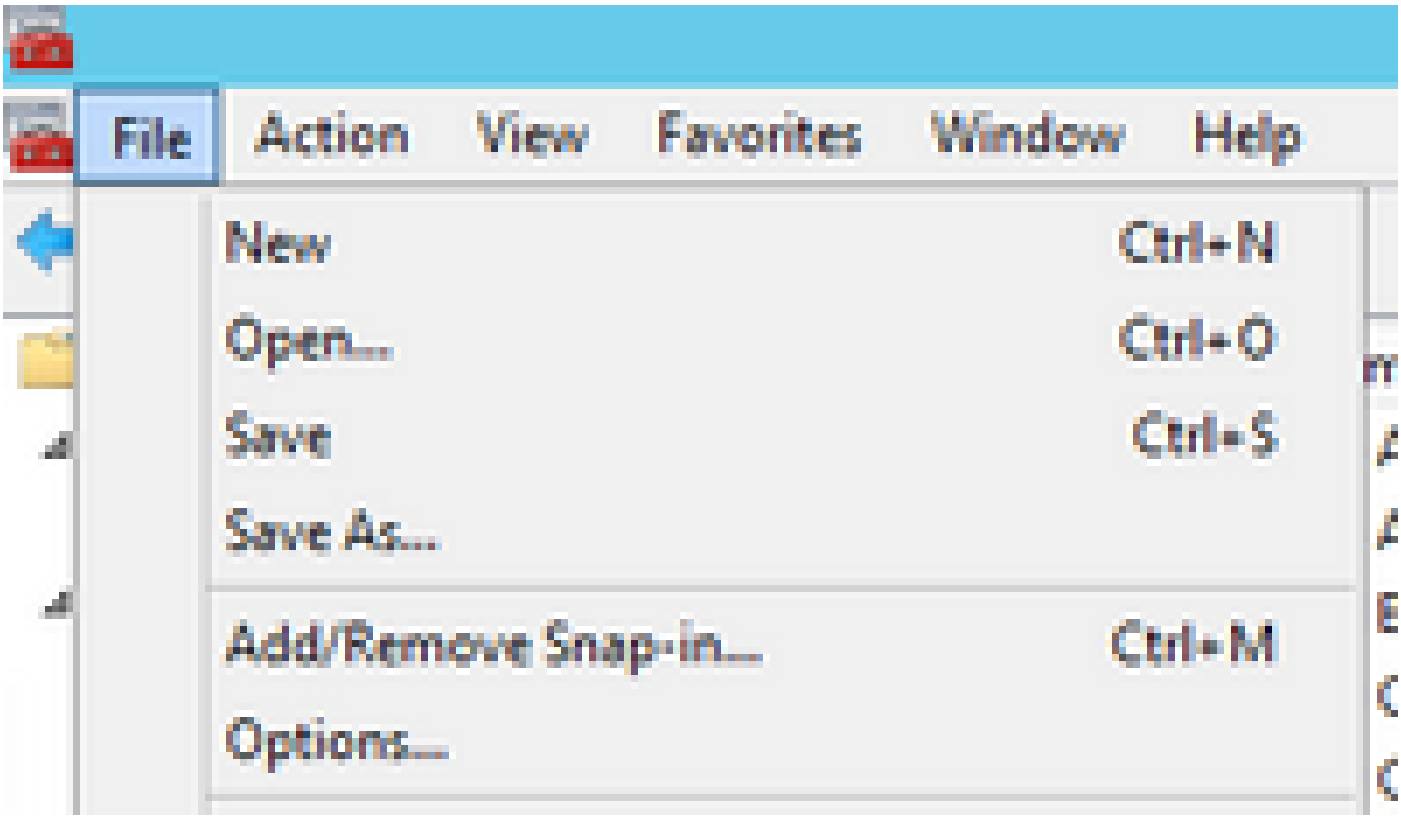
- CA의 Common Name(공통 이름)을 설정합니다(서버의 호스트 이름과 일치해야 함).

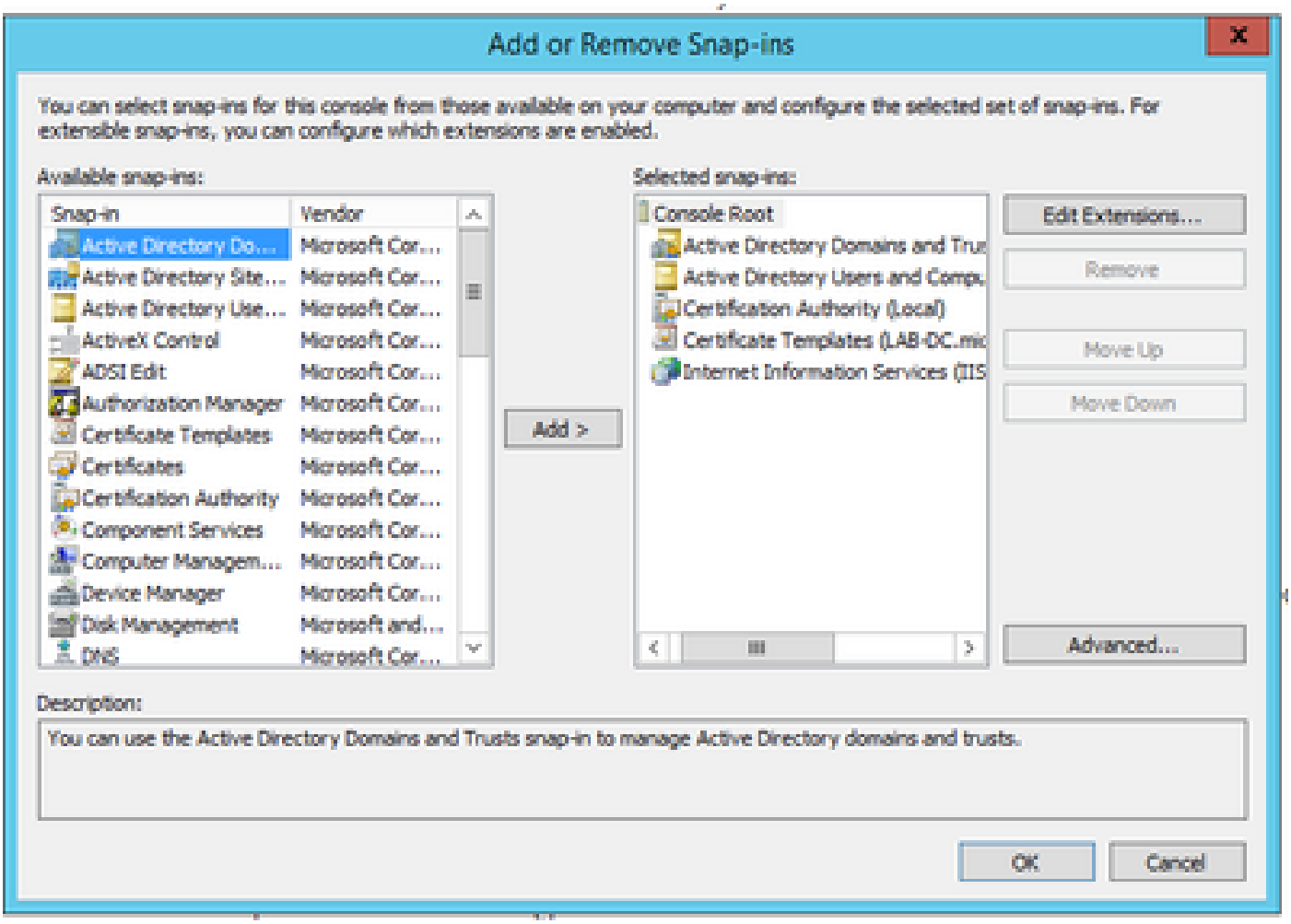


- 5년(원하는 경우 이상)으로 유효 기간 설정
- 마법사의 나머지 부분에서 다음 단추를 선택합니다.

CiscoRA용 인증서 템플릿 생성

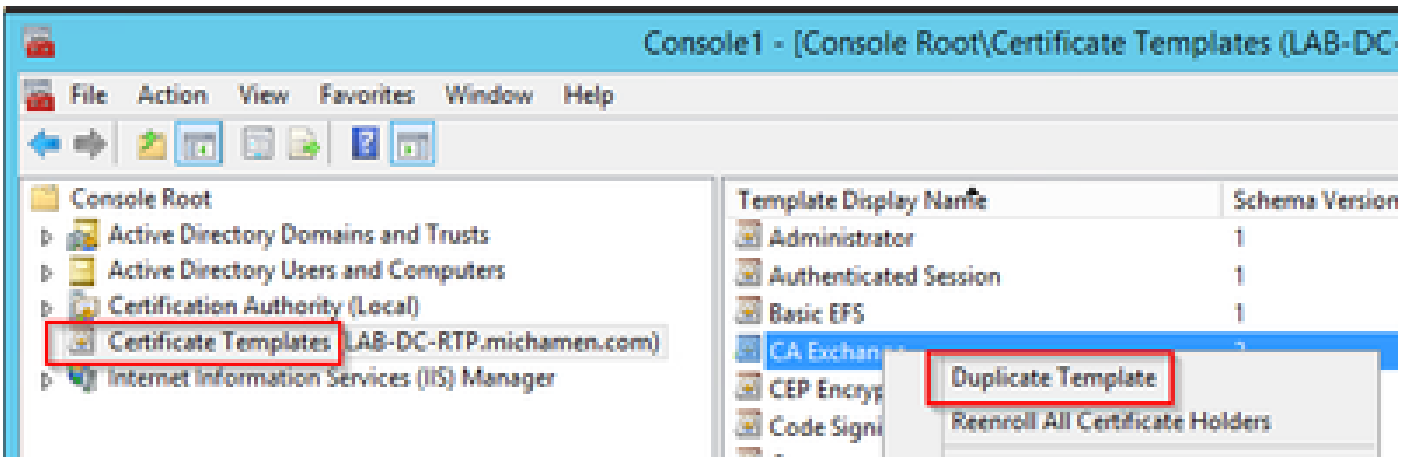
- MMC를 엽니다. Windows 시작 로고를 선택하고 실행에서 mmc를 입력합니다
- MMC 창을 열고 후속 스냅인(컨피그레이션의 다른 지점에서 사용됨)을 추가한 다음 OK(확인)를 선택합니다.



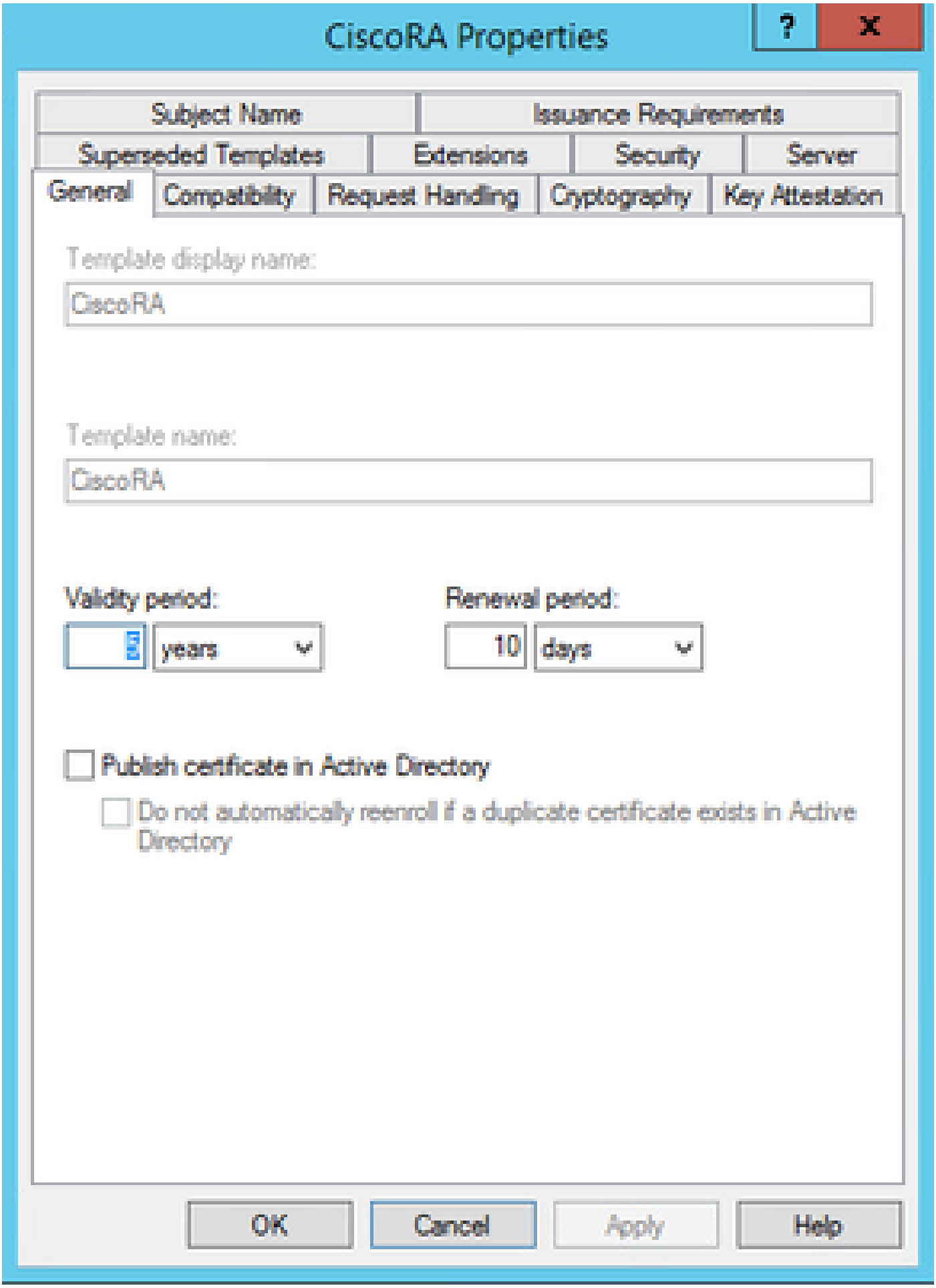


- File(파일) > Save(저장)를 선택하고 빠른 재액세스를 위해 이 콘솔 세션을 데스크톱에 저장합니다.

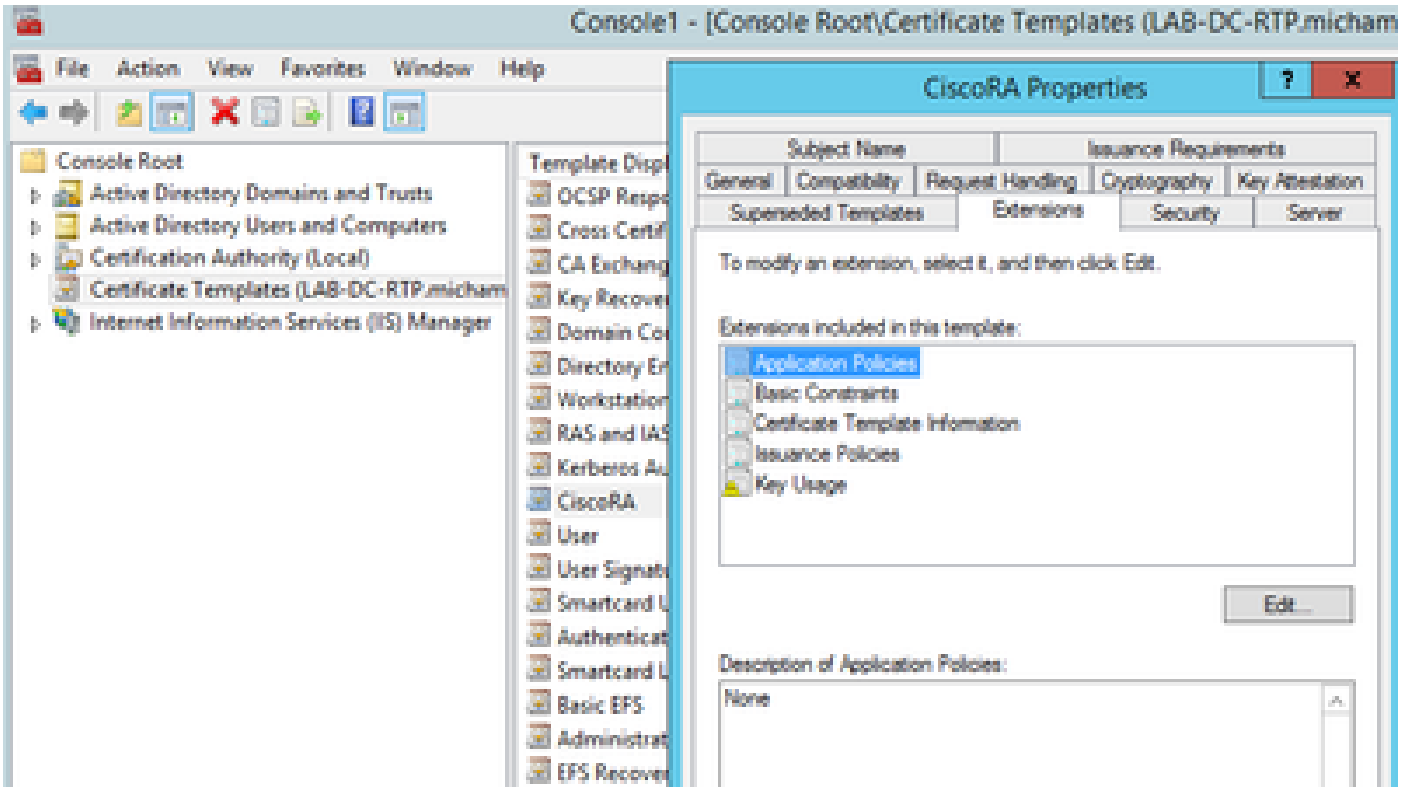
- 스냅인에서 인증서 템플릿을 선택합니다
- 템플릿(사용 가능한 경우 "루트 인증 기관" 템플릿)을 생성하거나 복제하고 이름을 CiscoRA로 지정합니다



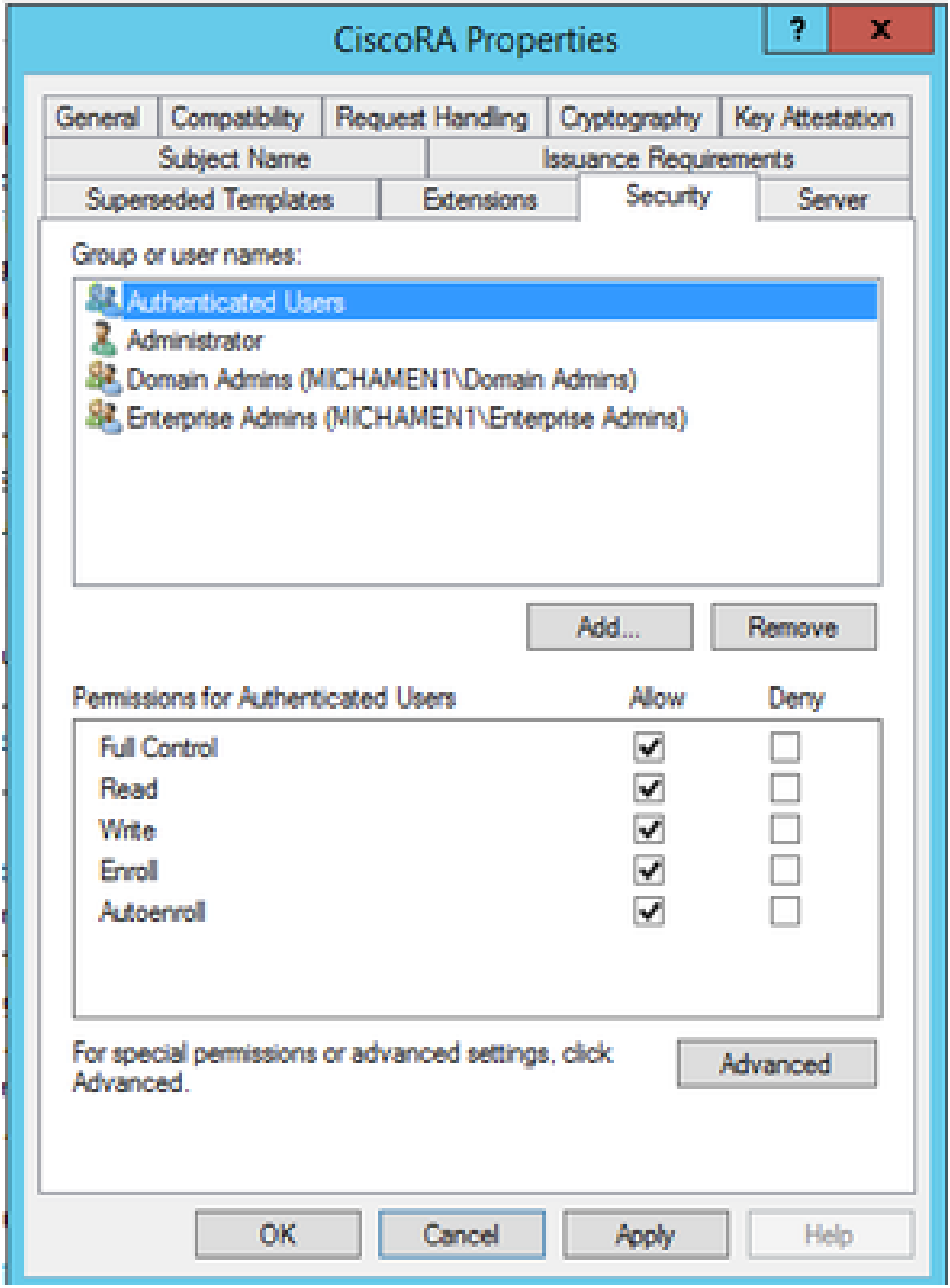
- 템플릿을 수정합니다. 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다.
- 일반 탭을 선택하고 유효 기간을 20년(또는 원하는 경우 다른 값)으로 설정합니다. 이 탭에서 템플릿의 "표시 이름" 및 "이름" 값이 일치하는지 확인합니다


CiscoRA Properties
Subject Name
Issuance Requirements
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Template display name:
CiscoRA
Template name:
CiscoRA
Validity period:
years
Renewal period:
10
days
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help

- Extensions(확장) 탭을 선택하고 Application Policies(애플리케이션 정책)를 선택한 다음 Edit(수정)를 선택합니다

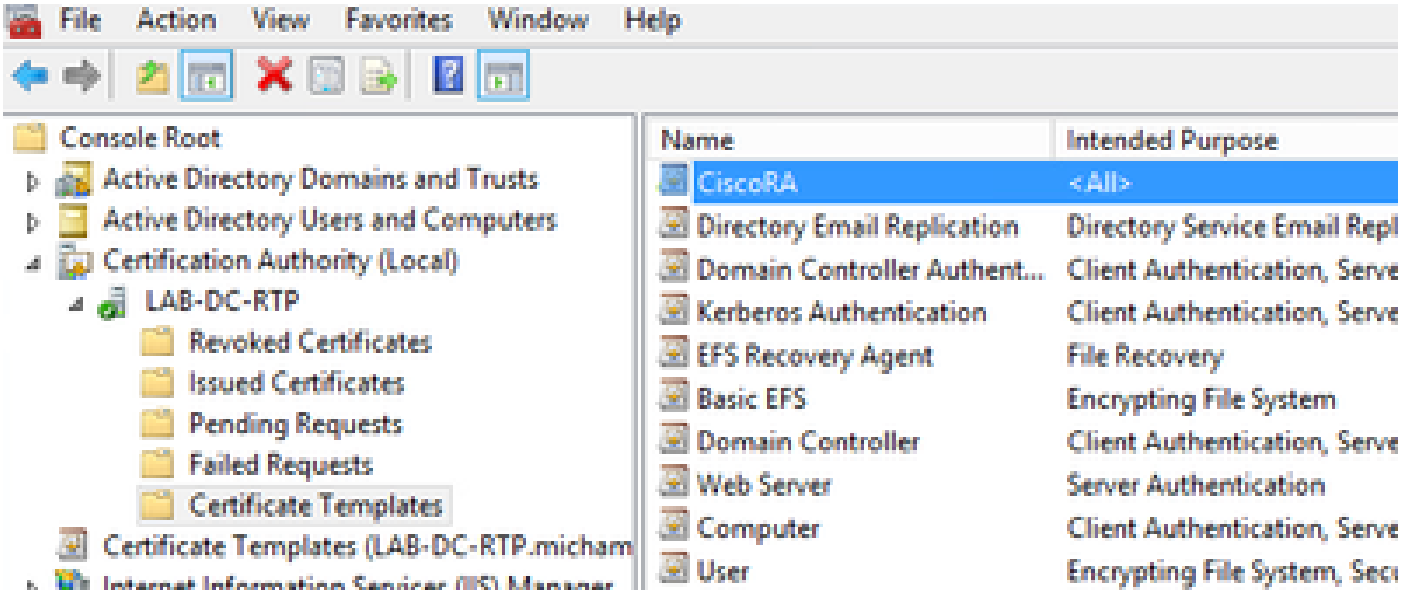


- 표시되는 창에 표시된 정책을 모두 제거합니다.
- Subject Name(주체 이름) 탭을 선택하고 Supply in Request(요청에서 공급) 라디오 버튼을 선택합니다
- 보안 탭을 선택하고 표시된 모든 그룹/사용자 이름에 대한 모든 권한을 부여합니다



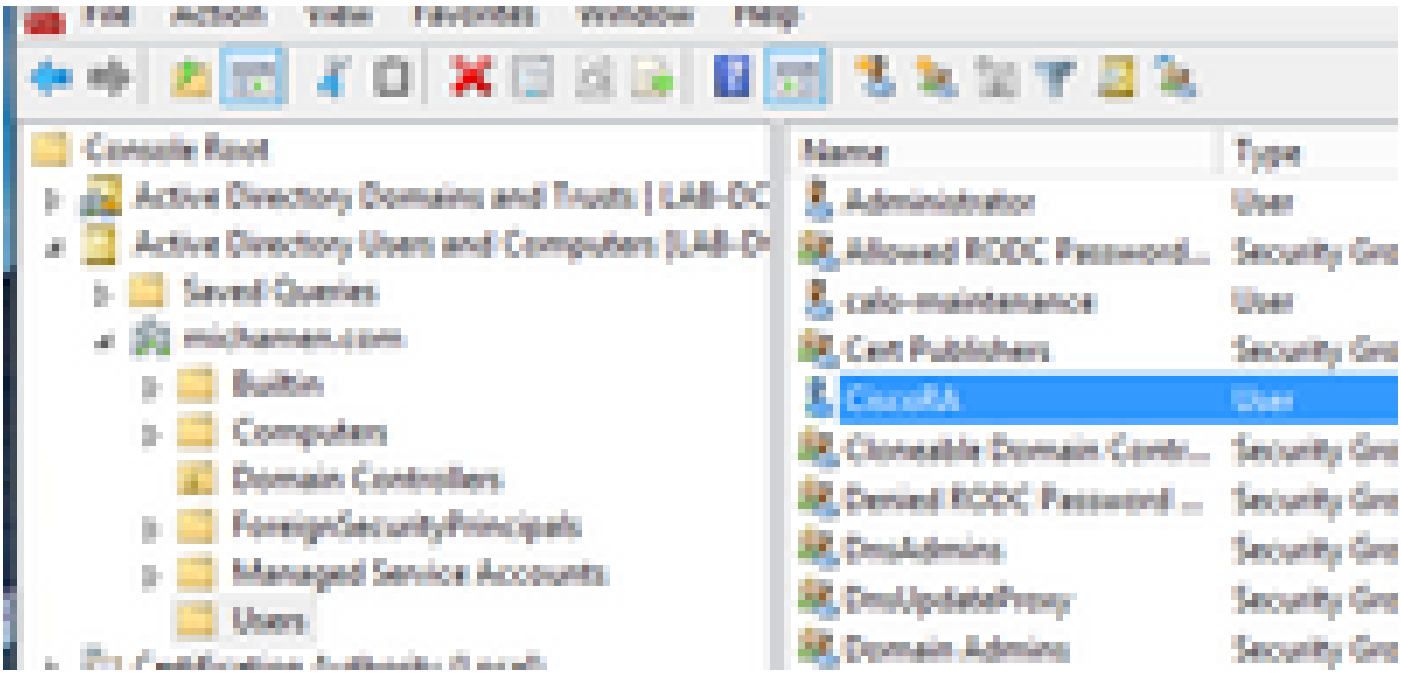
인증서 템플릿을 발급할 수 있도록 설정

- MMC 스냅인에서 Certification Authority(인증 기관)를 선택하고 폴더 트리를 확장하여 Certificate Templates(인증서 템플릿) 폴더를 찾습니다
- Name(이름) 및 Intended Purpose(목적)가 포함된 프레임의 공백을 마우스 오른쪽 단추로 클릭합니다.
- 발급할 새 및 인증서 템플릿 선택
- 새로 만들고 편집한 CiscoRA 템플릿을 선택합니다



Active Directory CiscoRA 계정 생성

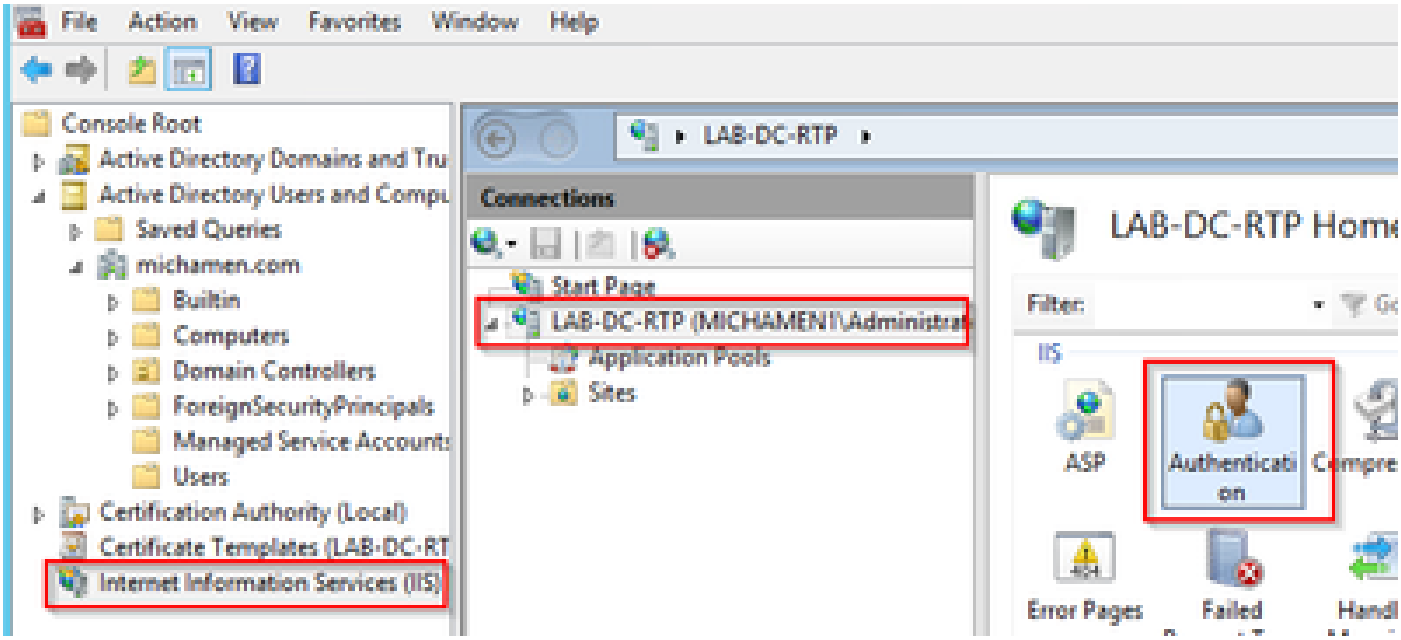
- MMC 스냅인으로 이동하여 Active Directory 사용자 및 컴퓨터를 선택합니다
- 맨 왼쪽 창의 트리에서 Users 폴더를 선택합니다
- 이름, 유형 및 설명이 포함된 프레임의 공백을 마우스 오른쪽 단추로 클릭합니다
- 새 및 사용자 선택
- 사용자 이름/비밀번호로 CiscoRA 계정(이 실습에 대해 ciscora/Cisco123이 사용됨)을 생성하고 표시된 경우 Password never expires(비밀번호가 만료되지 않음) 확인란을 선택합니다



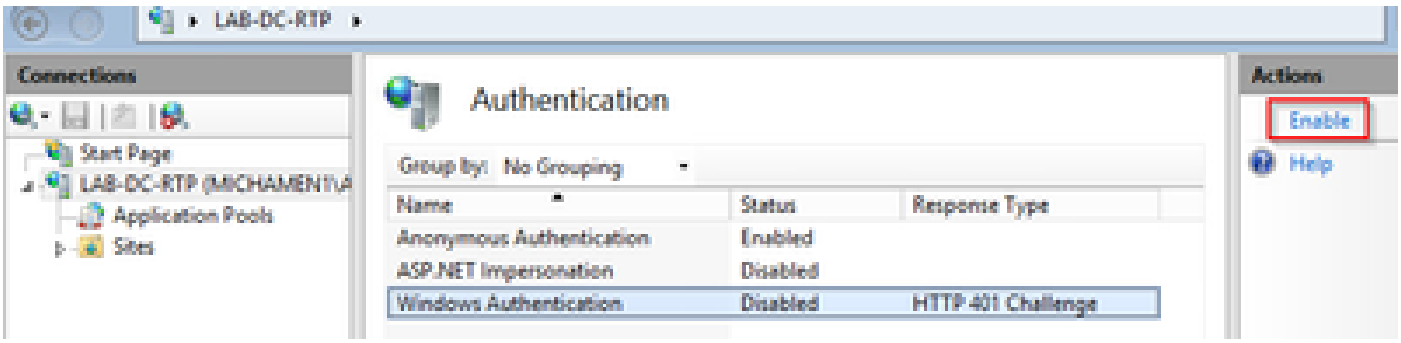
IIS 인증 및 SSL 바인딩 컨피그레이션

사용 NTLM 인증

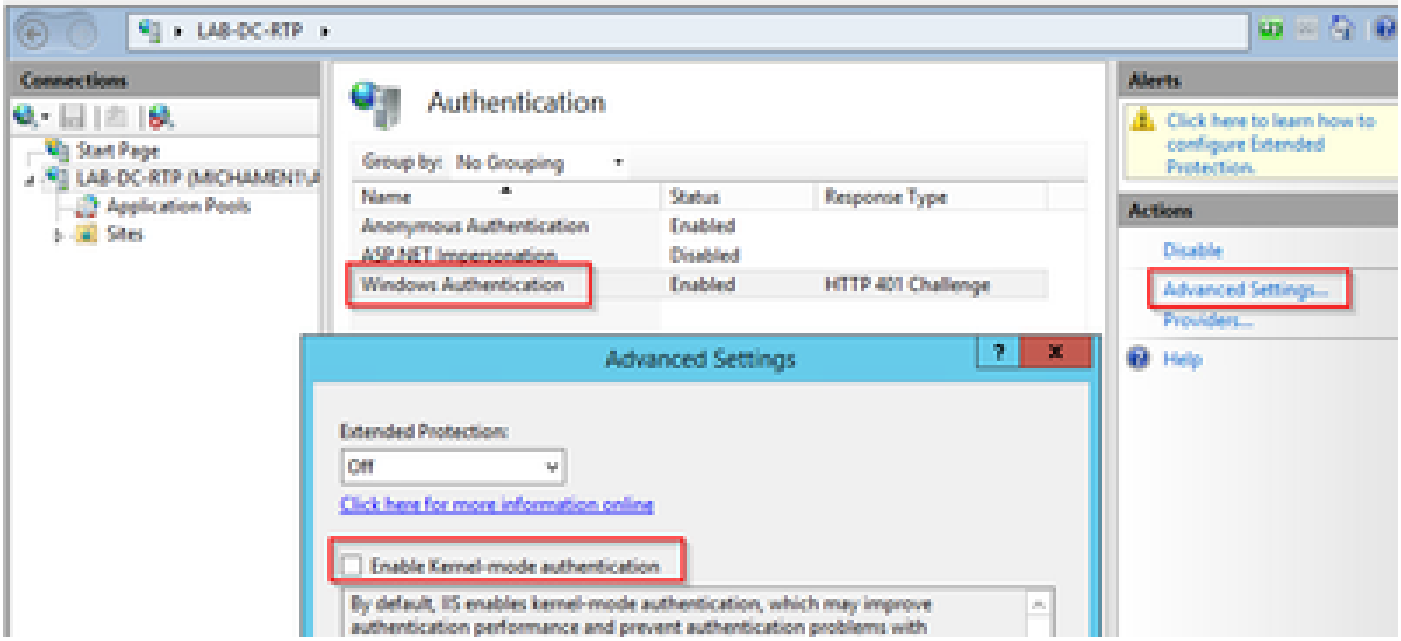
- MMC 스냅인으로 이동하고 IIS(인터넷 정보 서비스) 관리자 스냅인 아래에서 서버 이름을 선택합니다
- 기능 목록이 다음 프레임에 표시됩니다. 인증 기능 아이콘 을 두 번 클릭합니다



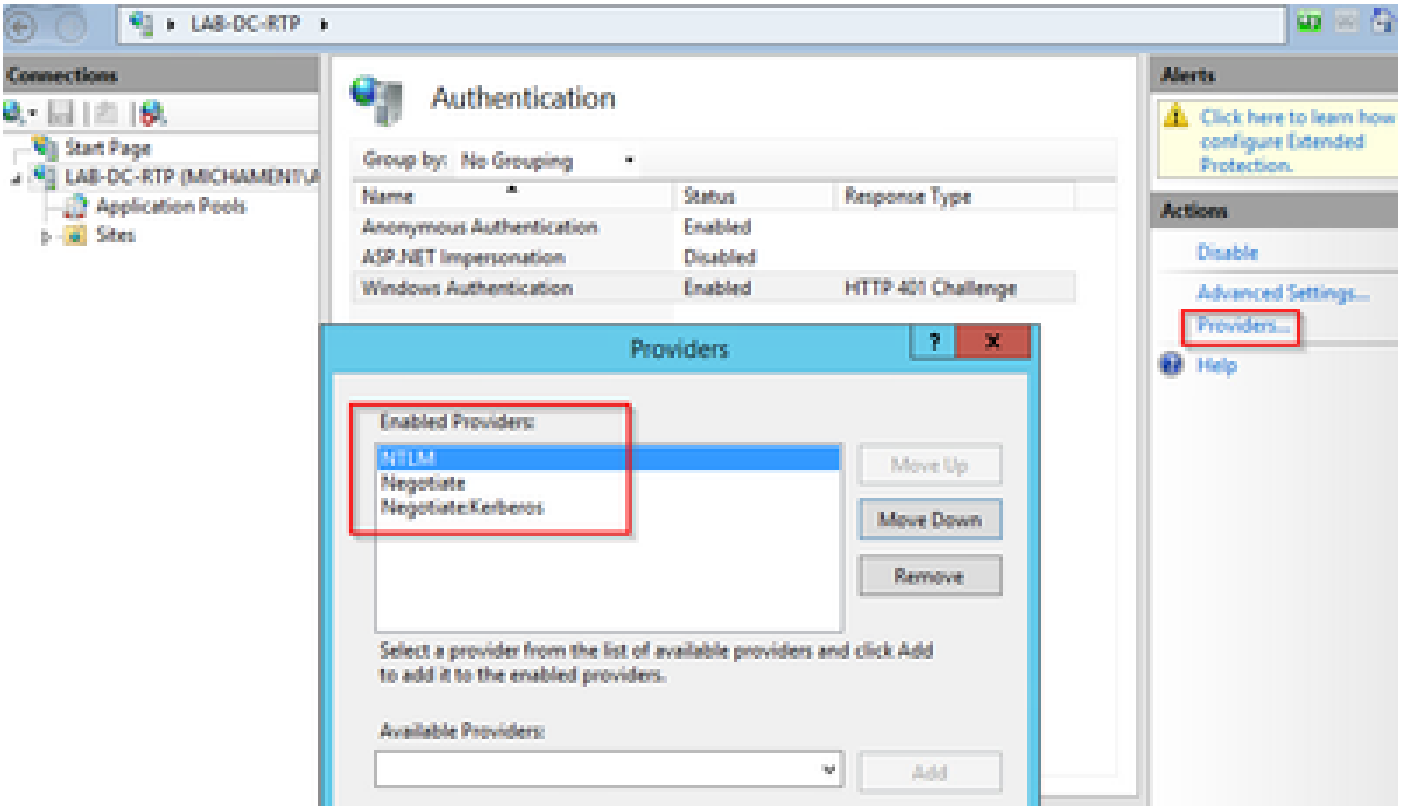
- Windows Authentication을 강조 표시하고 Actions(작업) 프레임(오른쪽 창)에서 Enable(활성화) 옵션을 선택합니다



- Actions(작업) 창에 Advanced Settings(고급 설정) 옵션이 표시됩니다. 이 옵션을 선택하고 Enable Kernel-mode authentication(커널 모드 인증 활성화)의 선택을 취소합니다



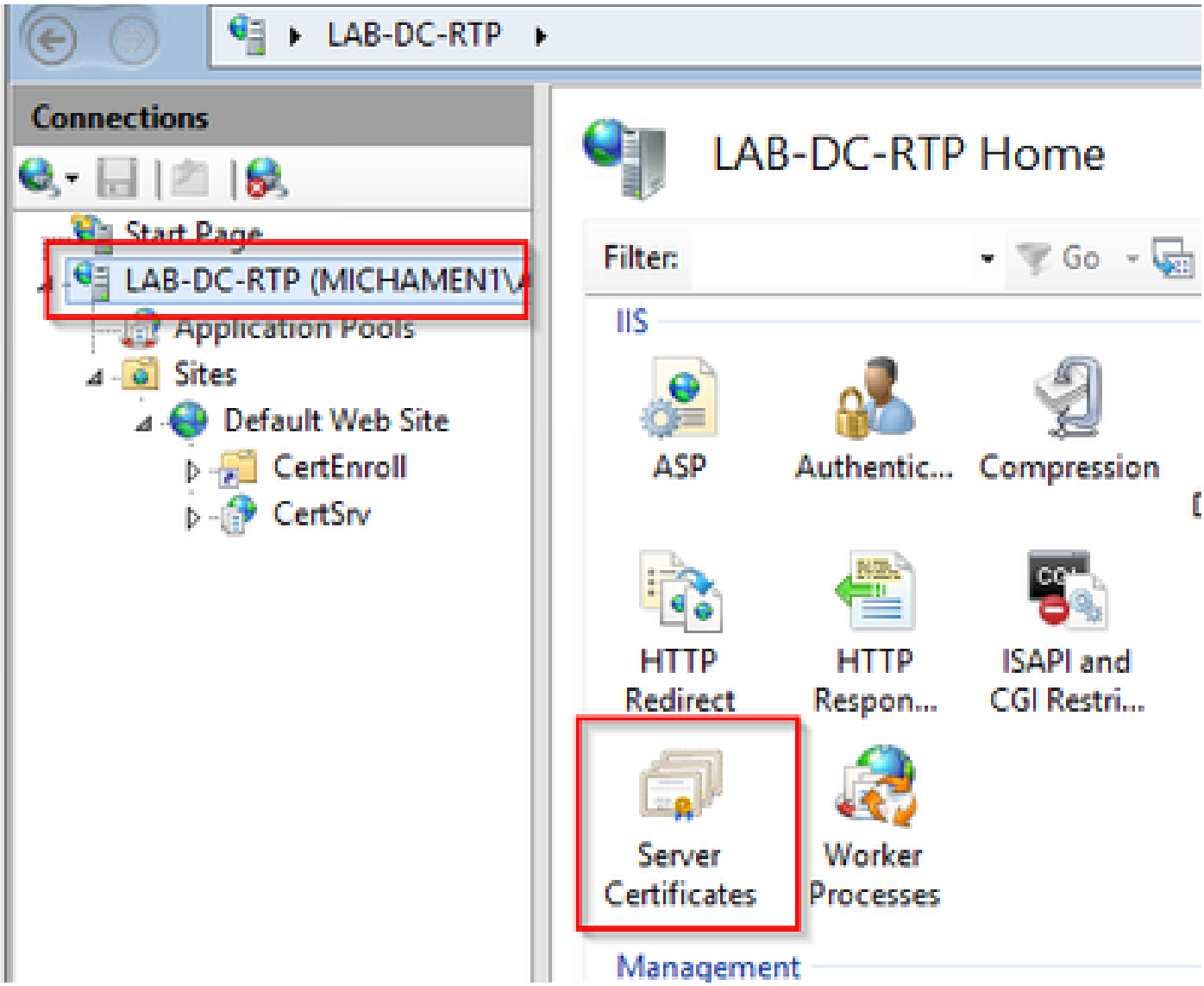
- Providers(사업자)를 선택하고 NTML을 선택한 다음 Negotiate(협상)를 순서대로 지정합니다.



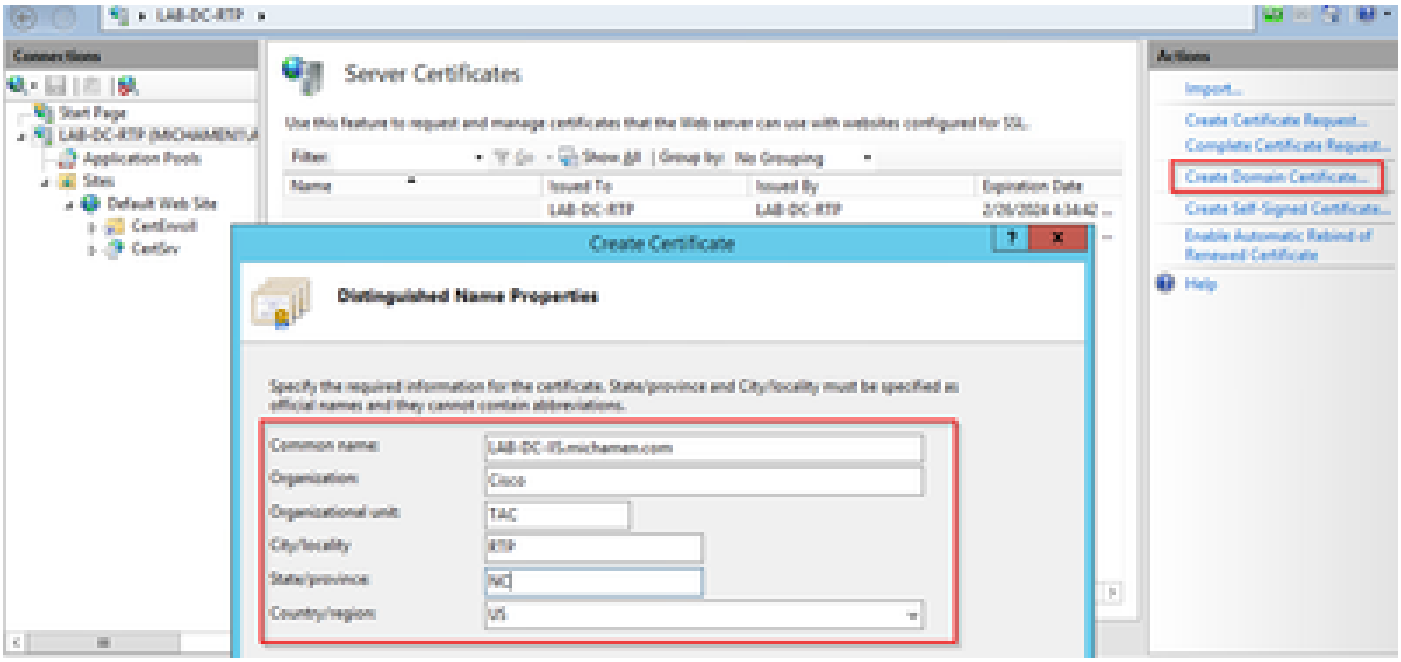
웹 서버에 대한 ID 인증서 생성

그렇지 않은 경우, 웹 서버의 인증서가 자체 서명된 경우 CiscoRA에서 연결할 수 없기 때문에 CA에서 서명한 웹 서비스에 대한 인증서 및 ID 인증서를 생성해야 합니다.

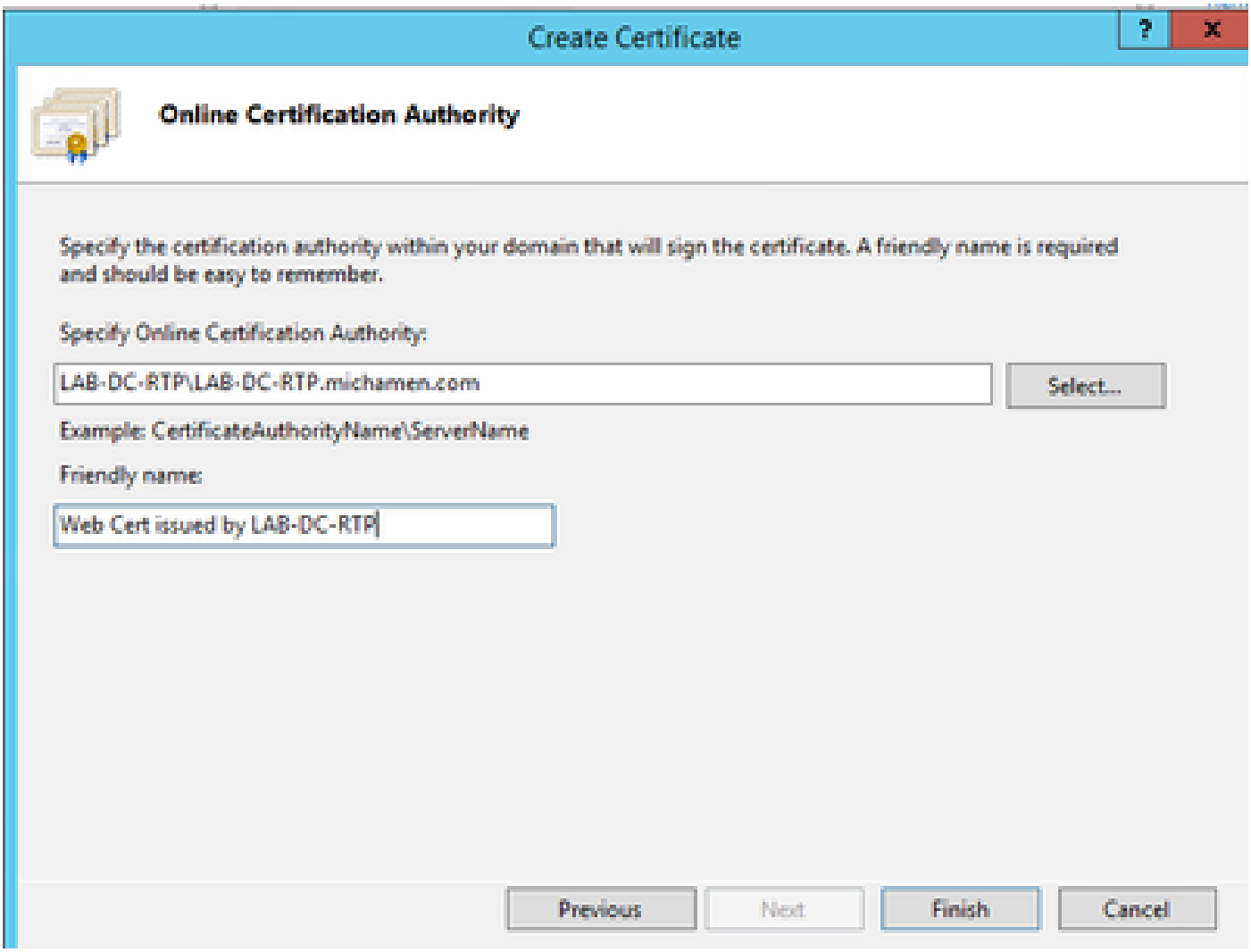
- IIS 스냅인에서 웹 서버를 선택하고 서버 인증서 기능 아이콘을 두 번 클릭합니다.



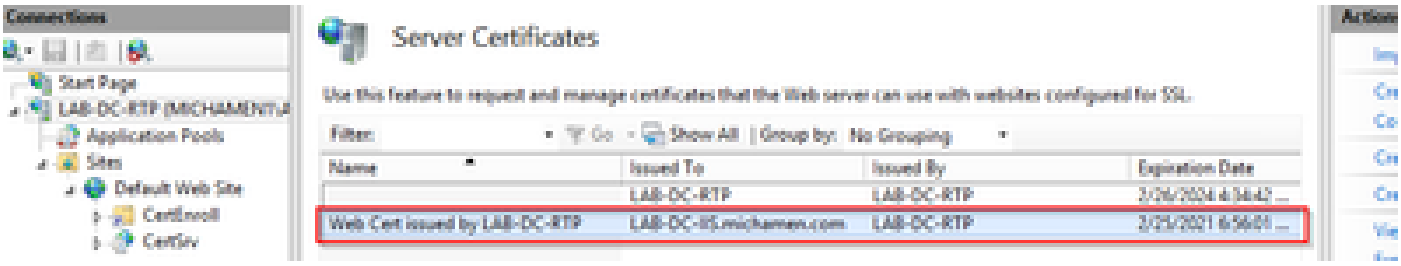
- 기본적으로 여기에 나열된 인증서 하나가 표시됩니다. 이는 자체 서명 루트 CA 인증서입니다. Actions(작업) 메뉴에서 Create Domain Certificate(도메인 인증서 생성) 옵션을 선택합니다. 새 인증서를 만들기 위해 구성 마법사에 값을 입력 합니다. 일반 이름이 확인 가능한 FQDN(Fully Qualified Domain Name)인지 확인한 후 다음을 선택합니다.



- 발급자가 될 루트 CA의 인증서를 선택하고 Finish(마침)를 선택합니다.

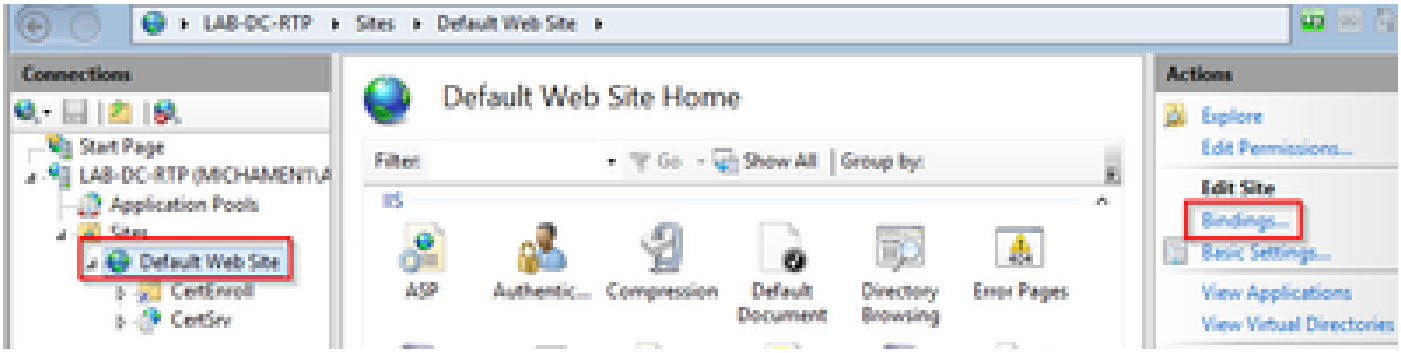


- CA 인증서 및 웹 서버의 ID 인증서가 모두 표시됩니다.

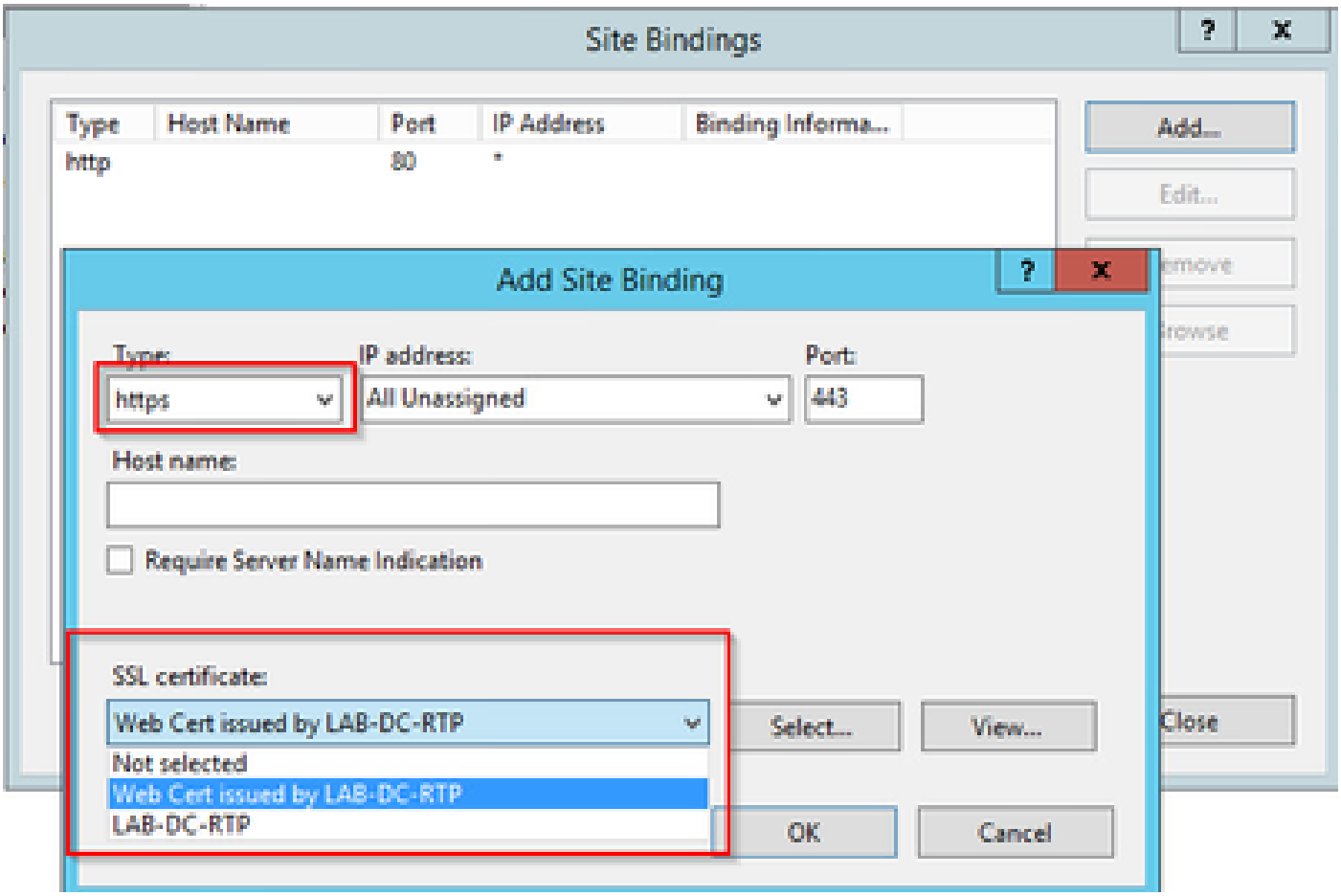


웹 서버 SSL 바인딩

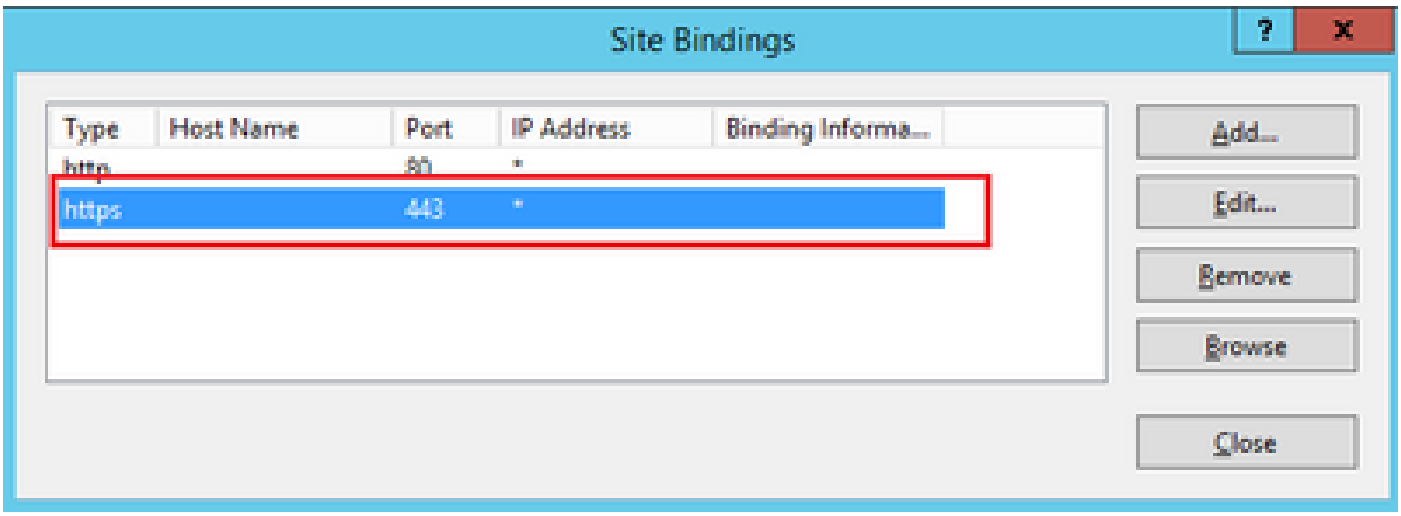
- 트리 보기에서 사이트를 선택하고(기본 웹 사이트를 사용하거나 특정 사이트로 좀 더 세분화할 수 있음) 작업 창에서 바인딩을 선택합니다. 웹 사이트에 대한 바인딩을 생성, 편집 및 삭제할 수 있는 바인딩 편집기가 나타납니다. 사이트에 새 SSL 바인딩을 추가하려면 Add를 선택합니다.

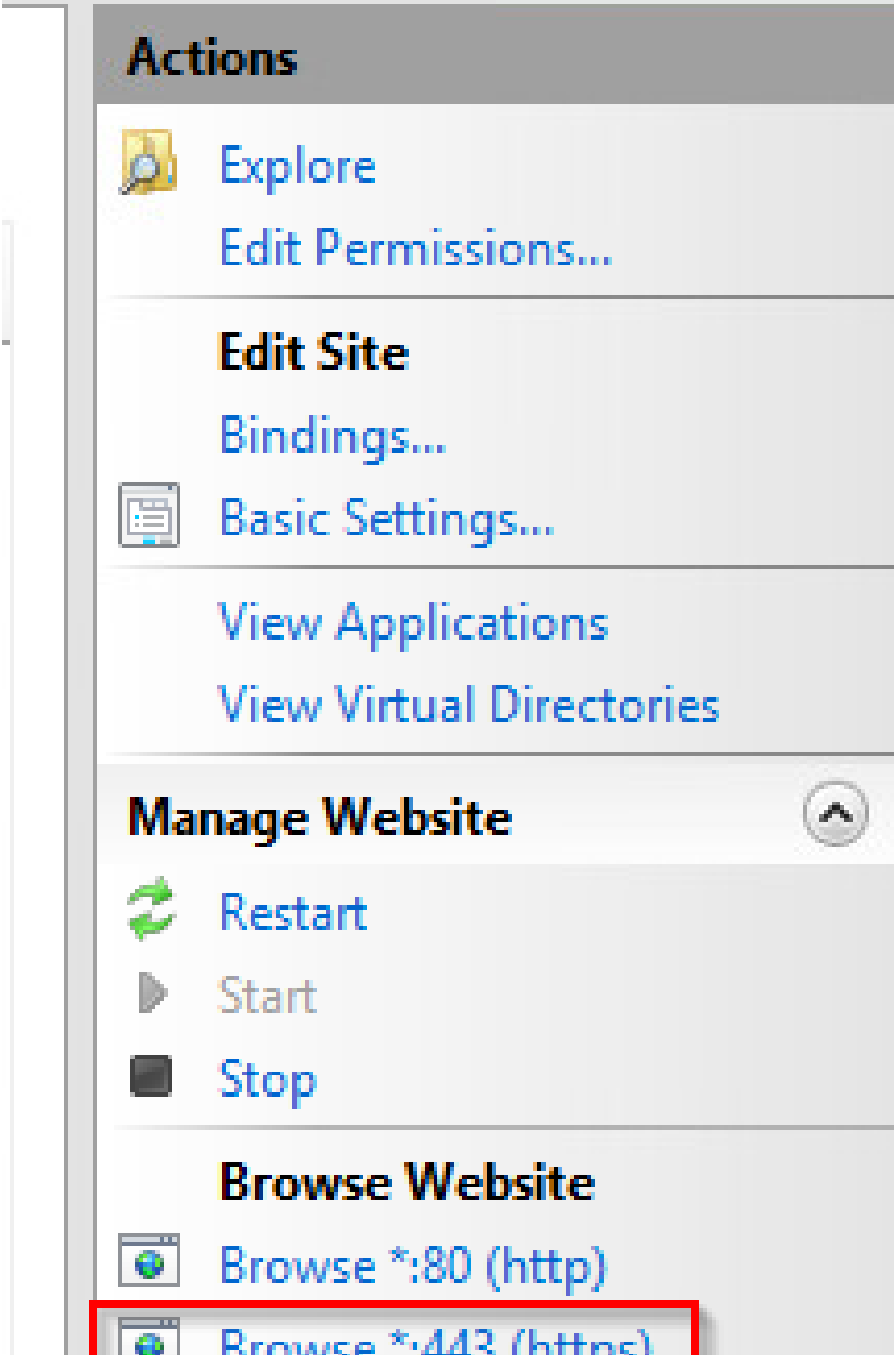


- 새 바인딩의 기본 설정은 포트 80에서 HTTP로 설정됩니다. Type 드롭다운 목록에서 https를 선택합니다. SSL Certificate 드롭다운 목록에서 이전 섹션에서 생성한 자체 서명 인증서를 선택한 다음 OK를 선택합니다.



- 이제 사이트에 새 SSL 바인딩이 있으며, 메뉴에서 Browse *:443 (https) 옵션을 선택하여 작동하는지 확인하고 기본 IIS 웹 페이지에서 HTTPS를 사용하는지 확인합니다.




Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Browse *:443 (https)

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.