AnyConnect 클라이언트에 대해 FMC에서 관리하는 FTD에서 AD(LDAP) 인증 및 사용자 ID 설정

목차

소개

이 문서에서는 Cisco FTD(Firepower Threat Defense)에 연결하는 AnyConnect 클라이언트에 대해 AD 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC의 RA VPN 구성에 대한 기본 지식
- FMC의 LDAP 서버 컨피그레이션에 대한 기본 지식
- AD(Active Directory)에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft 2016 서버
- 6.5.0을 실행하는 FMCv
- 6.5.0을 실행하는 FTDv

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.

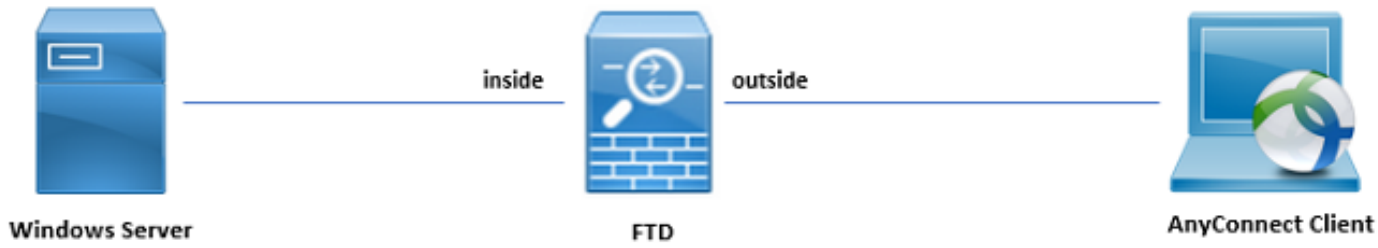
배경 정보

이 문서에서는 FMC(Firepower Management Center)에서 관리하는 Cisco FTD(Firepower Threat Defense)에 연결하는 AnyConnect 클라이언트에 대해 AD(Active Directory) 인증을 구성하는 방법에 대해 설명합니다.

사용자 ID는 액세스 정책에서 AnyConnect 사용자를 특정 IP 주소 및 포트로 제한하는 데 사용됩니다.

구성

네트워크 다이어그램 및 시나리오



Windows 서버는 사용자 ID를 테스트하기 위해 IIS 및 RDP로 미리 구성되어 있습니다. 이 컨피그레이션 가이드에서는 3개의 사용자 계정과 2개의 그룹이 생성됩니다.

사용자 계정:

- FTD 관리: FTD가 Active Directory 서버에 바인딩될 수 있도록 디렉토리 계정으로 사용됩니다.
- IT 관리자: 사용자 ID를 시연하는 데 사용되는 테스트 관리자 계정입니다.
- 테스트 사용자: 사용자 ID를 시연하는 데 사용되는 테스트 사용자 계정입니다.

그룹:

- AnyConnect 관리자: 사용자 ID를 시연하기 위해 IT 관리자가 추가하는 테스트 그룹입니다. 이 그룹에는 Windows Server에 대한 RDP 액세스만 있습니다.
- AnyConnect Users(AnyConnect 사용자): 사용자 ID를 입증하기 위해 Test User(사용자 테스트)가 추가된 테스트 그룹입니다. 이 그룹에는 Windows Server에 대한 HTTP 액세스만 있습니다.

Active Directory 구성

FTD에서 AD 인증 및 사용자 ID를 적절하게 구성하려면 몇 가지 값이 필요합니다.

FMC에서 컨피그레이션을 수행하려면 먼저 Microsoft Server에서 이 모든 세부 정보를 만들거나 수집해야 합니다. 주요 값은 다음과 같습니다.

- **도메인 이름**:

서버의 도메인 이름입니다. 이 컨피그레이션 가이드에서 example.com은 도메인 이름입니다.

- **서버 IP/FQDN 주소**:

Microsoft 서버에 연결하는 데 사용되는 IP 주소 또는 FQDN. FQDN을 사용하는 경우 FQDN을 확인하려면 FMC 및 FTD 내에서 DNS 서버를 구성해야 합니다.

이 컨피그레이션 가이드에서 이 값은 win2016.example.com(192.168.1.1로 확인됨)입니다.

- **서버 포트**:

LDAP 서비스에서 사용하는 포트. 기본적으로 LDAP 및 STARTTLS는 LDAP에 TCP 포트 389를 사용하고 LDAP over SSL(LDAPS)은 TCP 포트 636을 사용합니다.

- **루트 CA**:

LDAPS 또는 STARTTLS를 사용하는 경우 LDAPS에서 사용하는 SSL 인증서에 서명하는 데 사용되는 루트 CA가 필요합니다.

- **디렉토리 사용자 이름 및 비밀번호**:

FMC 및 FTD가 LDAP 서버에 바인딩하고 사용자를 인증하며 사용자 및 그룹을 검색하는 데 사용하는 계정입니다.

FTD Admin이라는 이름의 어카운트가 이 용도로 생성됩니다.

- **기본 및 그룹 DN(고유 이름)**:

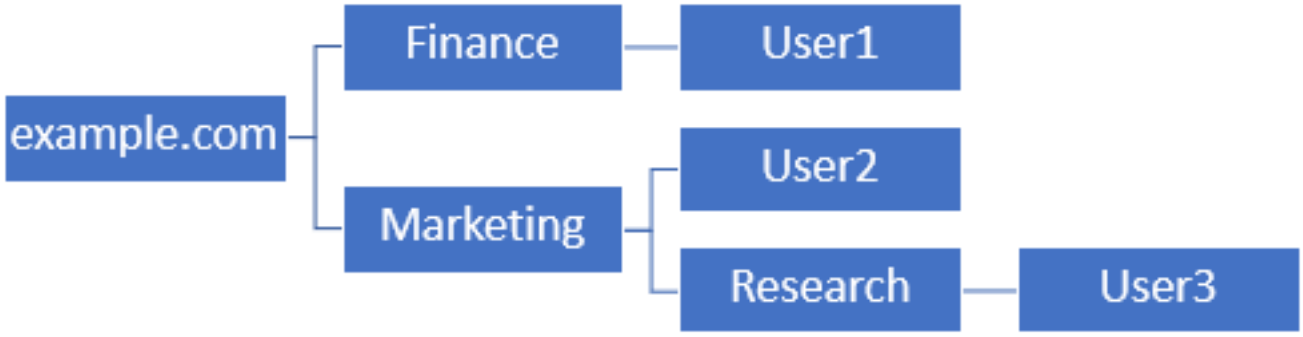
기본 DN은 FMC의 시작점이며 FTD는 Active Directory에 사용자 검색을 시작하고 인증하도록 지시합니다.

마찬가지로, 그룹 DN은 FMC가 Active Directory에 사용자 ID에 대한 그룹 검색을 시작할 위치를 알려주는 시작점입니다.

이 컨피그레이션 가이드에서는 루트 도메인 example.com이 Base DN 및 Group DN으로 사용됩니다.

그러나 프로덕션 환경에서는 LDAP 계층 내에서 **Base DN** 및 **Group DN**을 더 많이 사용하는 것이 좋습니다.

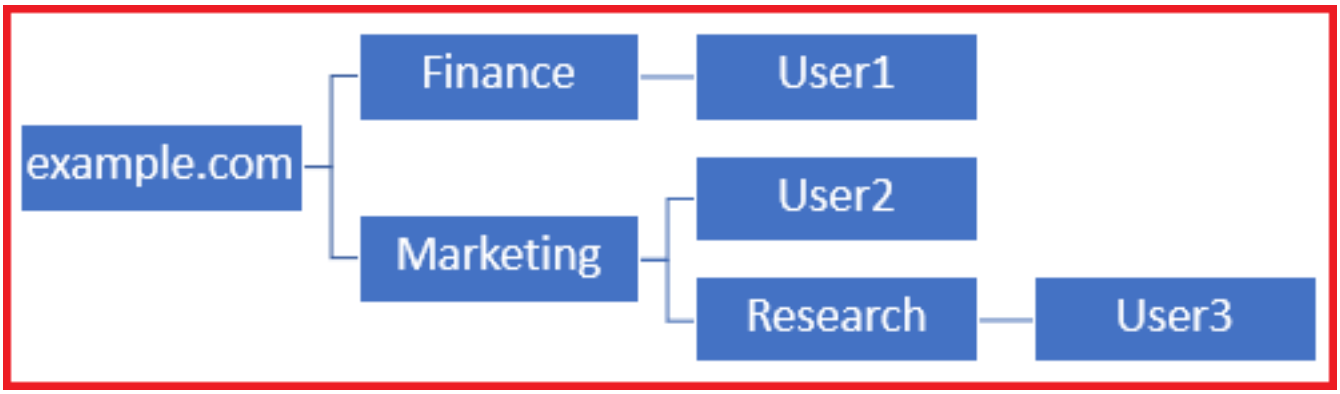
예를 들어, 이 LDAP 계층 구조는 다음과 같습니다.



관리자가 **Marketing** 조직 단위의 사용자가 기본 DN을 인증할 수 있도록 하려는 경우 루트(example.com)로 설정할 수 있습니다.

그러나 **Finance** 조직 단위의 User1도 로그인할 수 있습니다. 사용자 검색이 루트에서 시작되어 **Finance, Marketing** 및 Research로 내려가기 **때문입니다**.

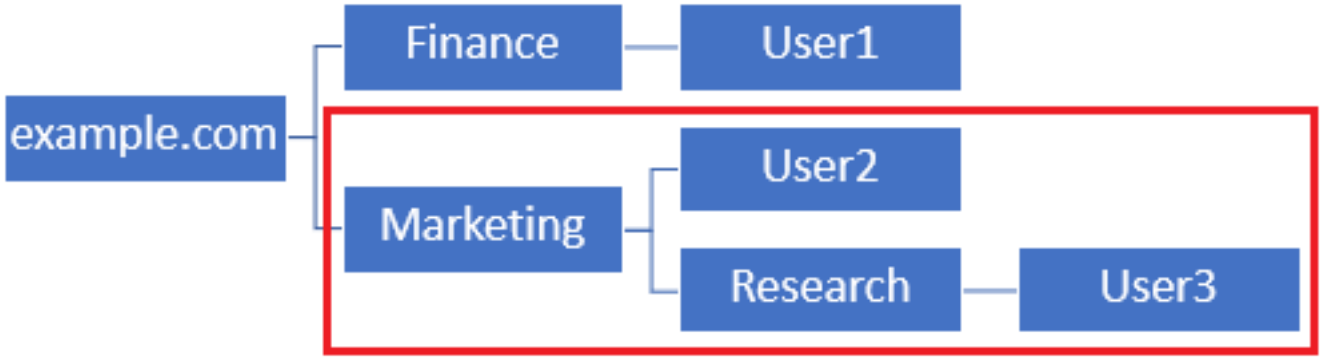
기본 DN이 example.com으로 설정됩니다.



Marketing 조직 단위 이하의 유일한 사용자에 대한 로그인을 제한하기 위해, 관리자는 대신 기본 DN을 Marketing으로 설정할 수 **있습니다**.

이제 Marketing에서 검색이 시작되므로 User2 및 User3만 인증할 수 **있습니다**.

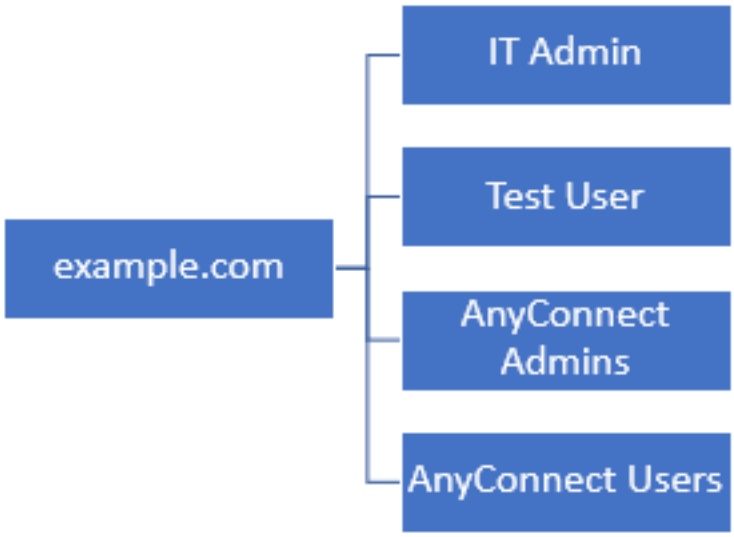
기본 DN을 마케팅으로 설정



사용자가 연결할 수 있는 FTD 내에서 보다 세분화된 제어를 수행하거나 AD 특성에 따라 다른 권한 부여를 할당하려면 LDAP 권한 부여 맵을 구성해야 합니다.

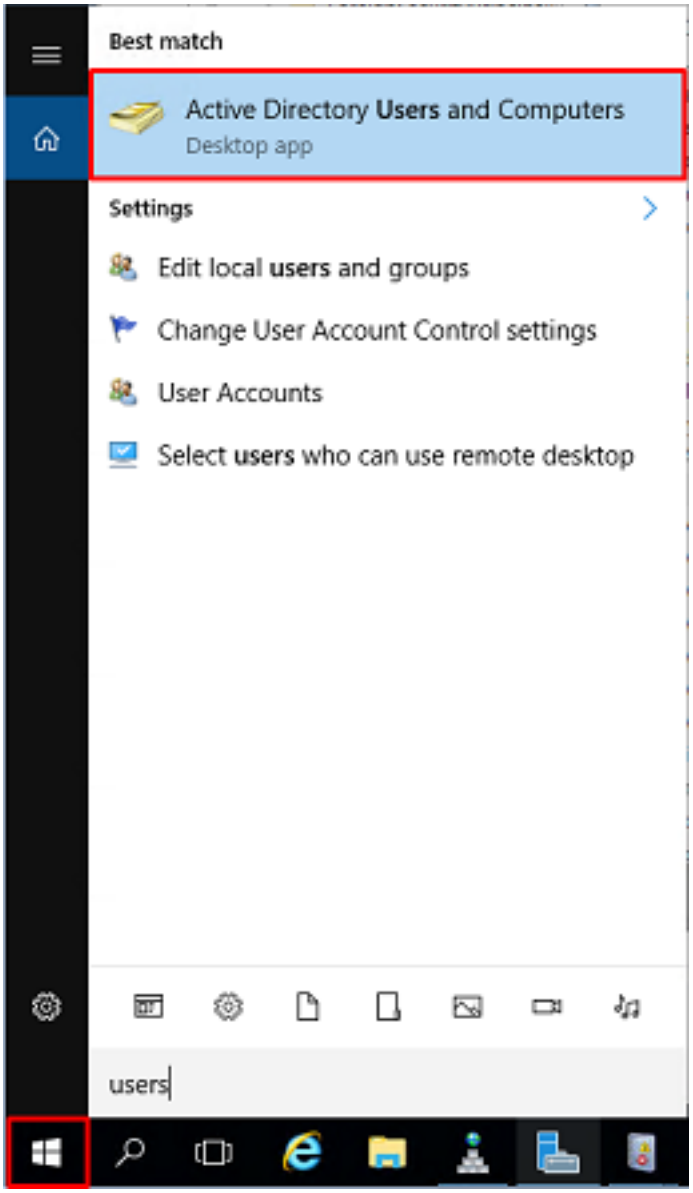
이에 대한 자세한 내용은 FTD(Firepower Threat Defense)에서 AnyConnect LDAP 매핑을 구성하십시오.

이 간소화된 LDAP 계층 구조는 이 컨피그레이션 가이드에서 사용되며 루트 example.com의 DN은 Base DN 및 Group DN 모두에 사용됩니다.

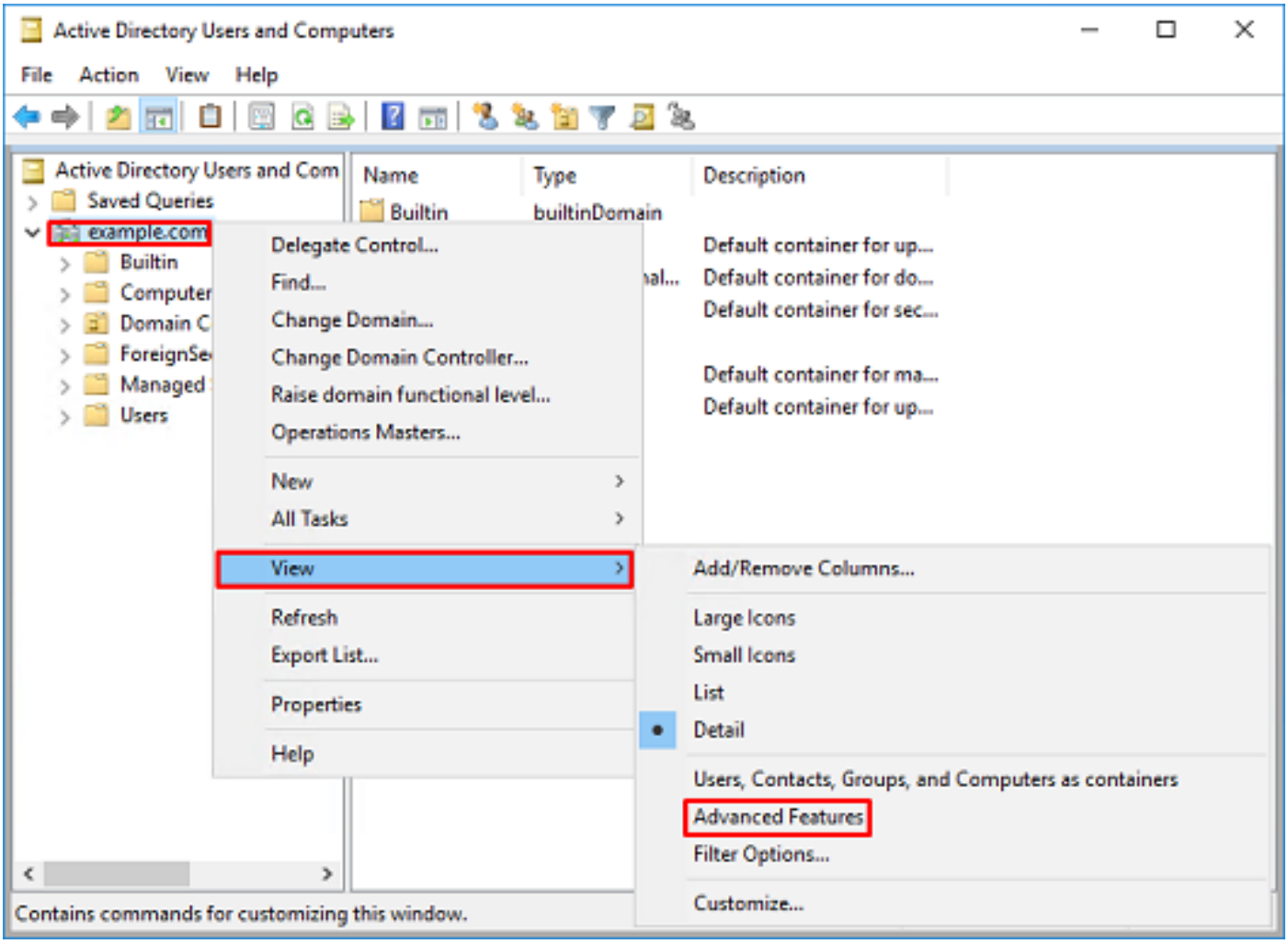


LDAP 기본 DN 및 그룹 DN 결정

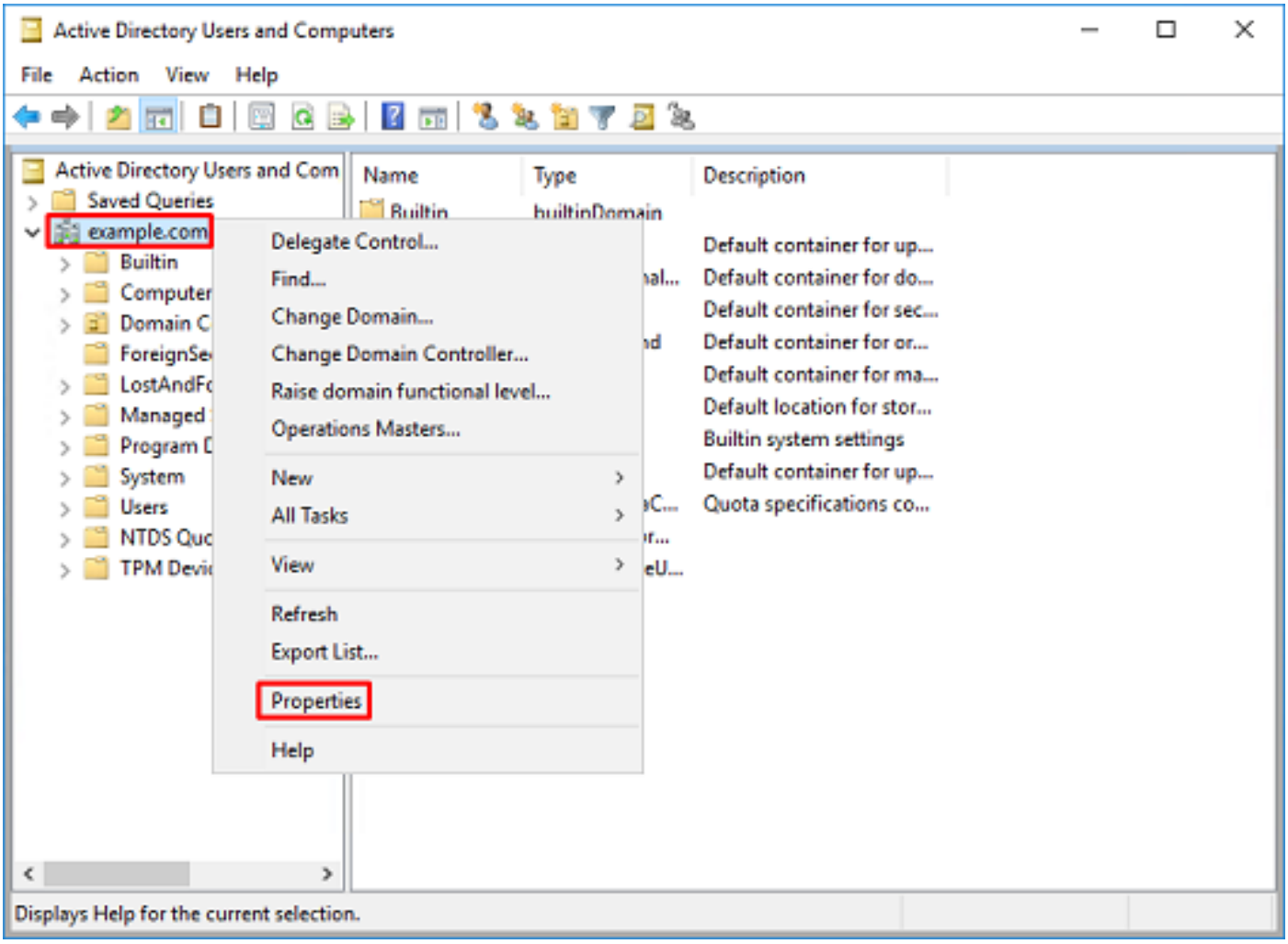
1. **Active Directory 사용자 및 컴퓨터를 엽니다.**



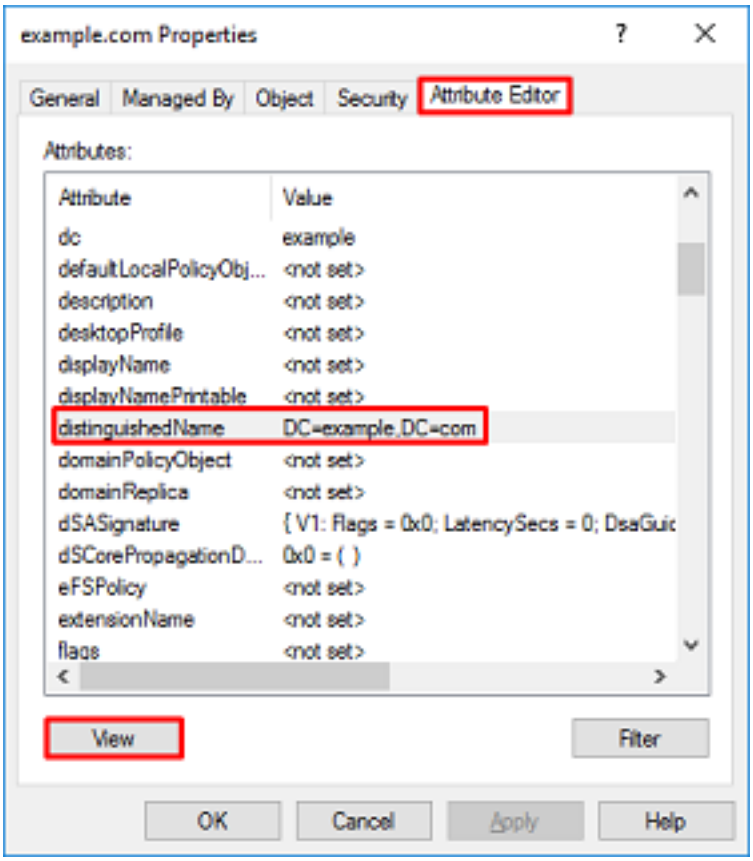
2. **루트 도메인**을 마우스 왼쪽 단추로 클릭하고(컨테이너를 열려면) **루트 도메인**을 마우스 오른쪽 단추로 클릭한 다음 **보기**에서 **고급** 기능을 **클릭합니다**.



3. 이렇게 하면 AD 개체 아래의 추가 속성을 볼 수 있습니다. 예를 들어, 루트 example.com에 대한 DN을 찾으려면 example.com을 마우스 오른쪽 버튼으로 클릭한 다음 Properties(속성)를 **선택합니다**.

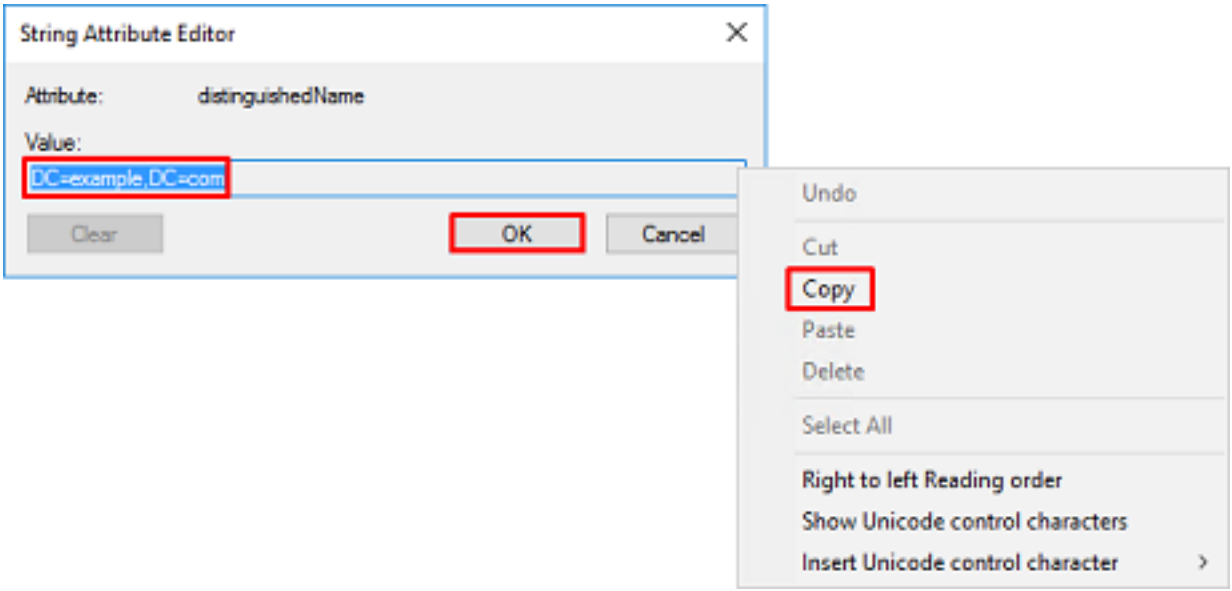


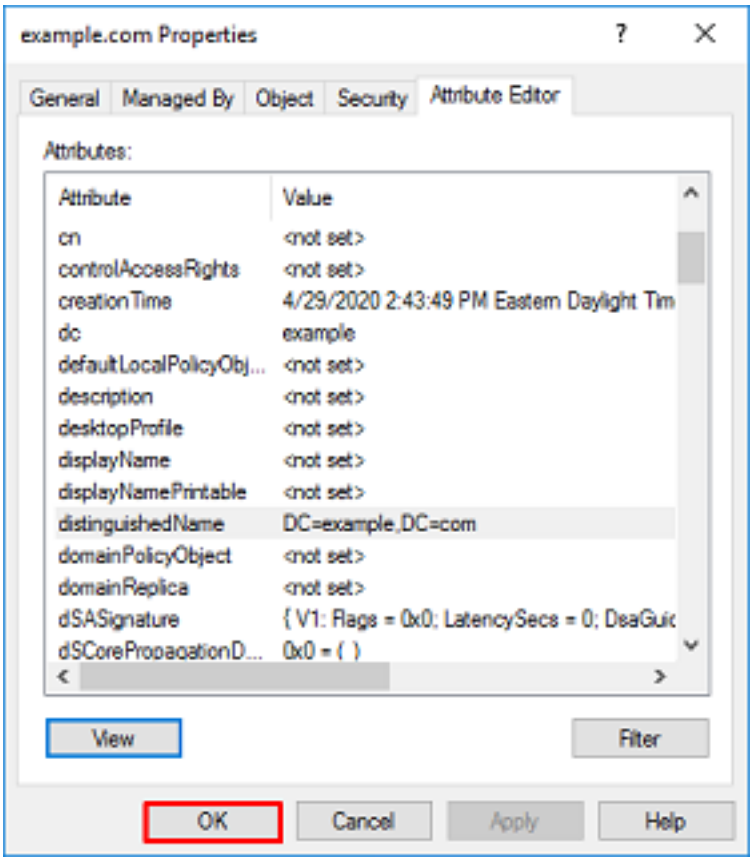
4. 등록 **정보**에서 속성 편집기 **탭을** 선택합니다. Attributes(**특성)** 아래에서 **distinguishedName**을 찾은 다음 View(**보기)를 클릭합니다**.



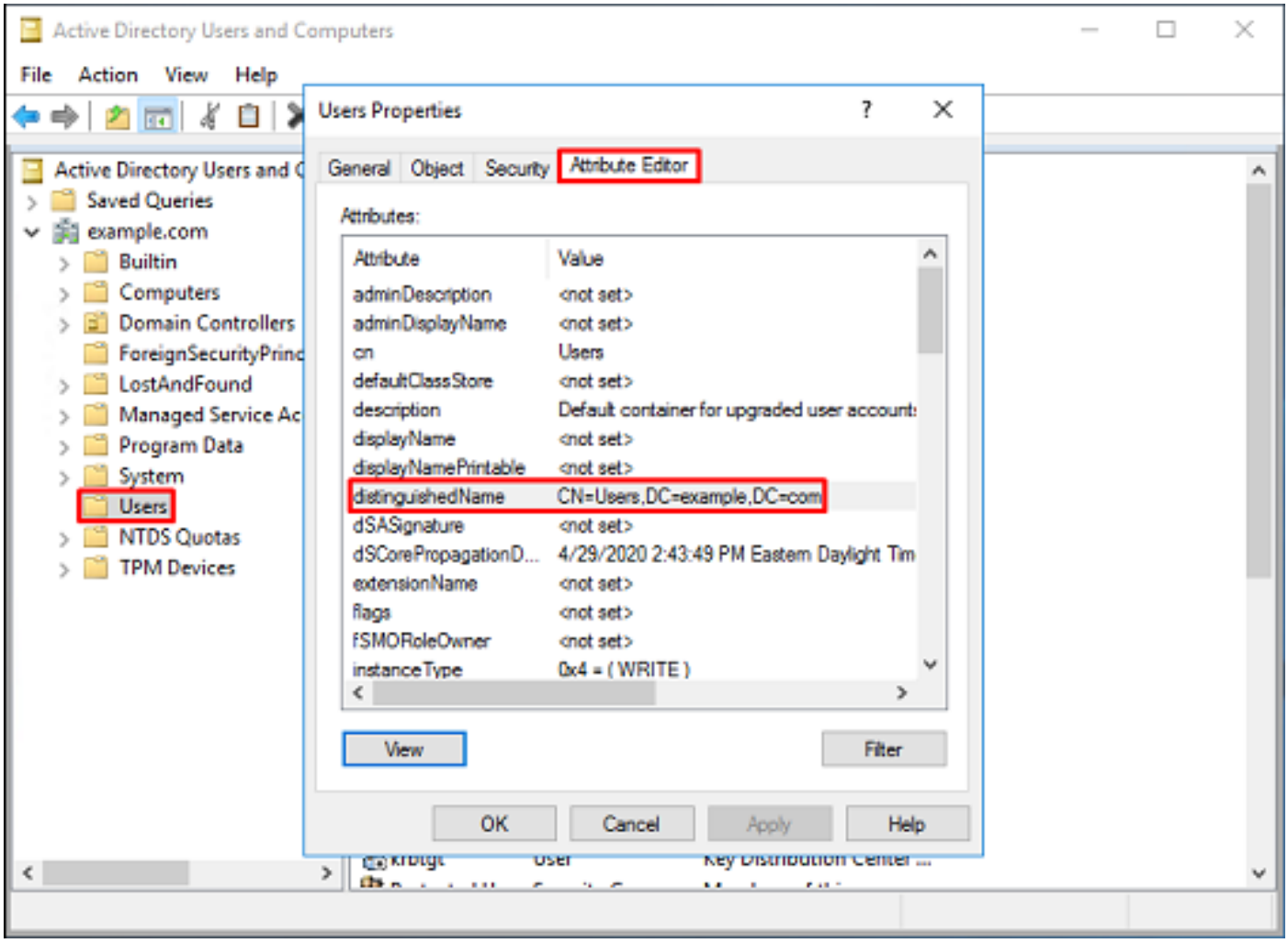
5. 이렇게 하면 나중에 DN을 복사하여 FMC에 붙여넣을 수 있는 새 창이 열립니다. 이 예에서 루트 DN은 DC=example,DC=com입니다.

값을 복사하여 나중에 저장할 수 있습니다. OK(**확인**)를 클릭하여 **String Attribute Editor(문자열 특성 편집기) 창**을 종료하고 OK(확인)를 다시 클릭하여 Properties(**속성**)**를 종료합니다**.

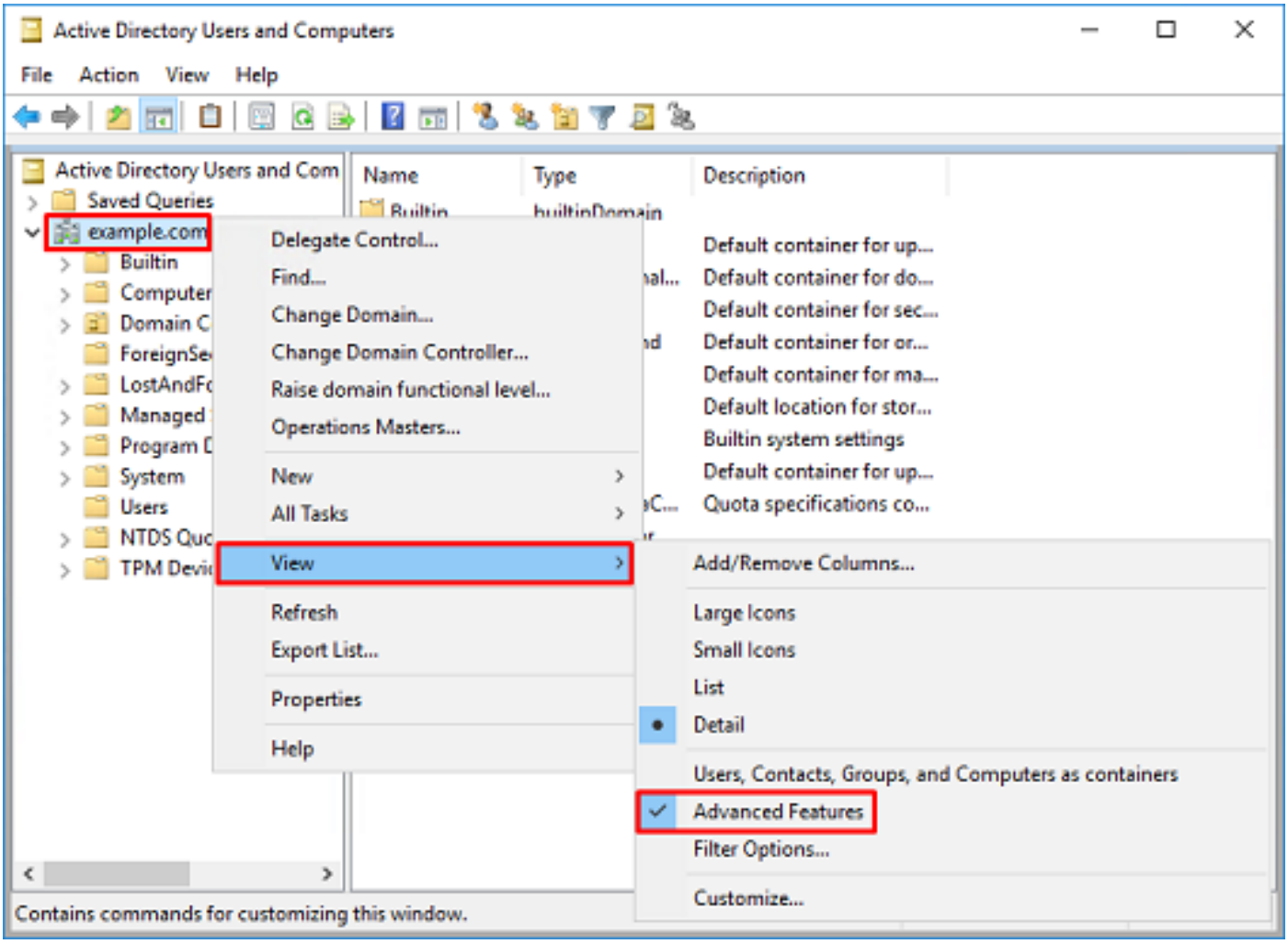




Active Directory 내의 여러 개체에 대해 이 작업을 수행할 수 **있습니다**. 예를 들어, 다음 단계는 **사용자** 컨테이너의 DN을 찾는 데 사용됩니다.



6. **Advanced Features(고급 기능)** 보기는 루트 DN을 마우스 오른쪽 단추로 다시 누른 다음 **보기** 아래에서 **Advanced Features(고급 기능)**를 한 번 더 눌러 제거할 수 있습니다.



FTD 어카운트 생성

이 사용자 계정은 FMC 및 FTD가 사용자 및 그룹을 검색하고 사용자를 인증하기 위해 Active Directory에 바인딩할 수 있도록 합니다.

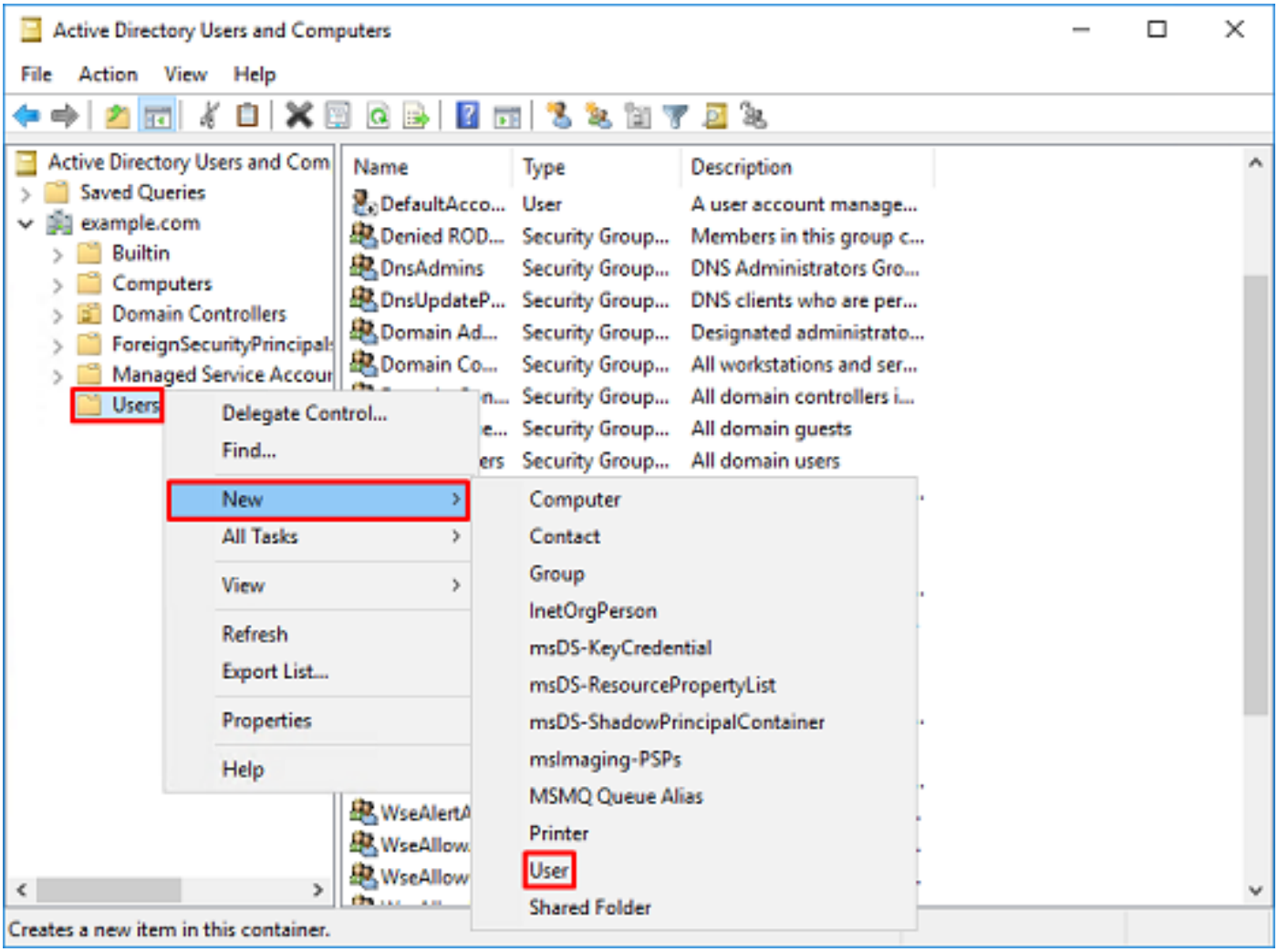
별도의 FTD 어카운트를 만드는 목적은 바인딩에 사용된 자격 증명이 손상된 경우 네트워크 내의 다른 위치에서 무단 액세스를 방지하기 위한 것입니다.

이 계정은 기본 DN 또는 그룹 DN의 범위에 속할 필요가 없습니다.

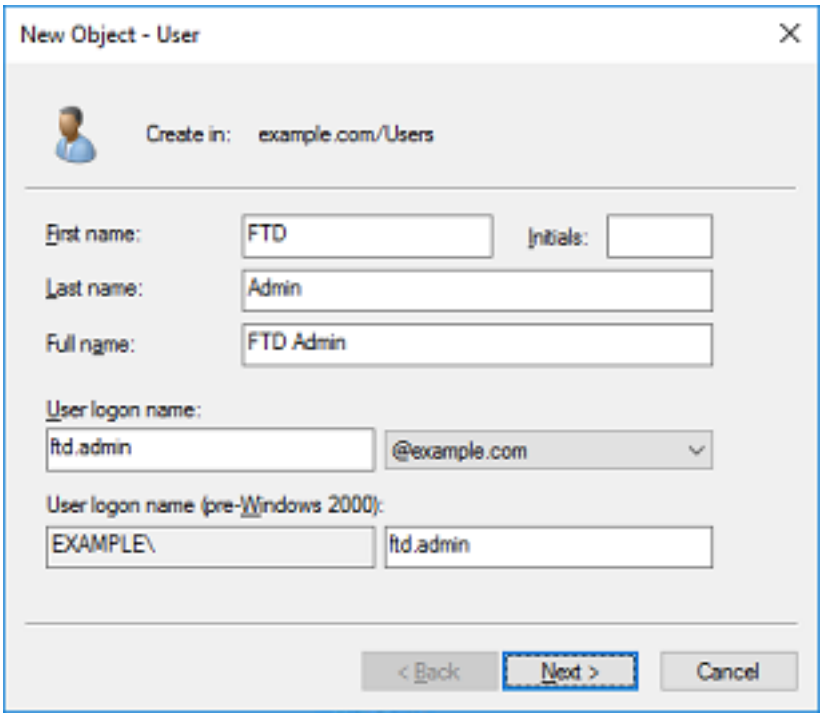
1. **Active Directory 사용자 및 컴퓨터**에서 FTD 계정이 추가된 컨테이너/조직을 마우스 오른쪽 단추로 클릭합니다.

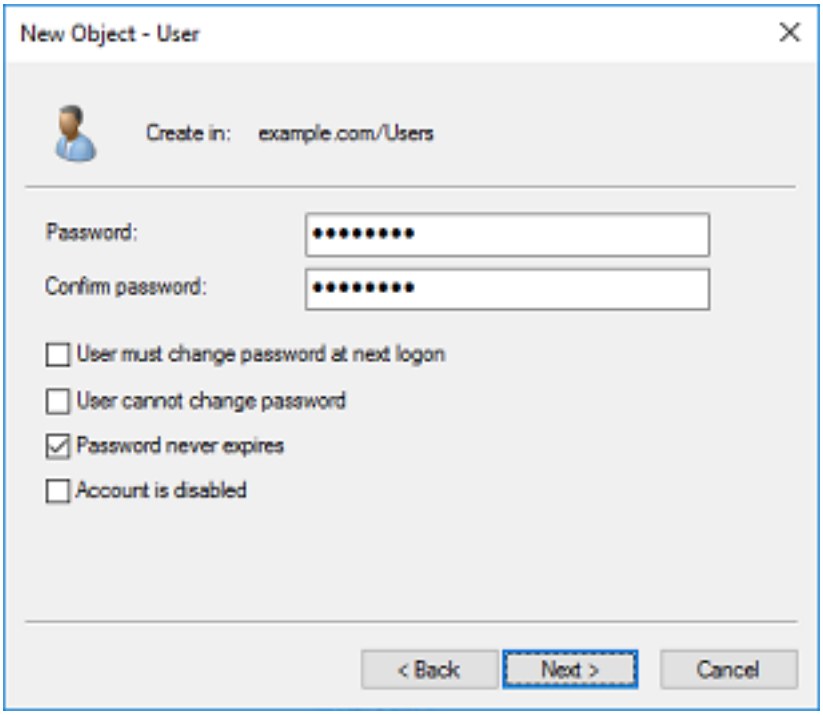
이 컨피그레이션에서 FTD 어카운트는 사용자 이름 ftd.admin@example.com**의 Users** 컨테이너 아래에 추가됩니다.

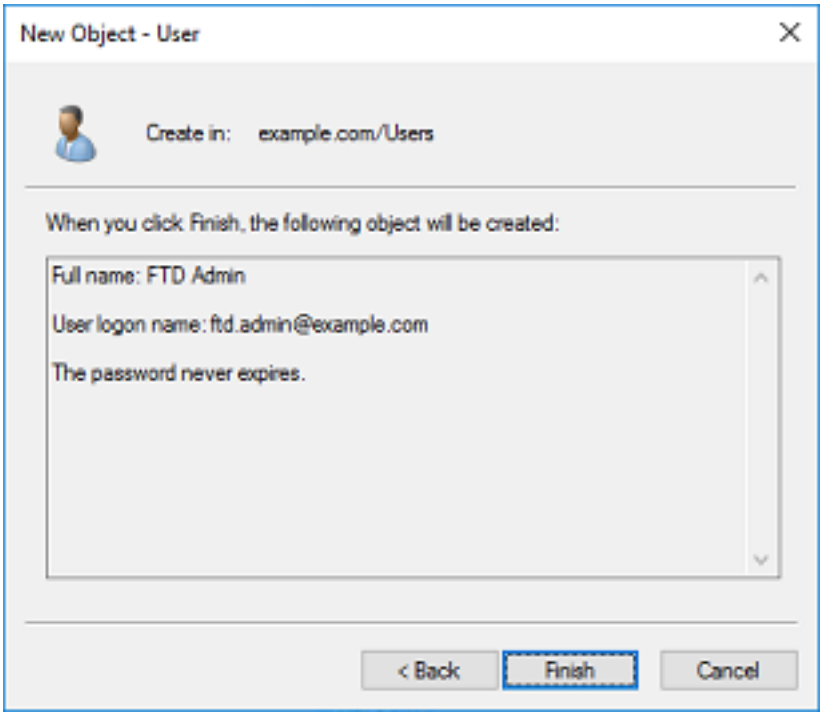
사용자를 마우스 오른쪽 **버튼**으로 클릭한 다음 **새로 만들기 > 사용자**로 **이동합니다**.



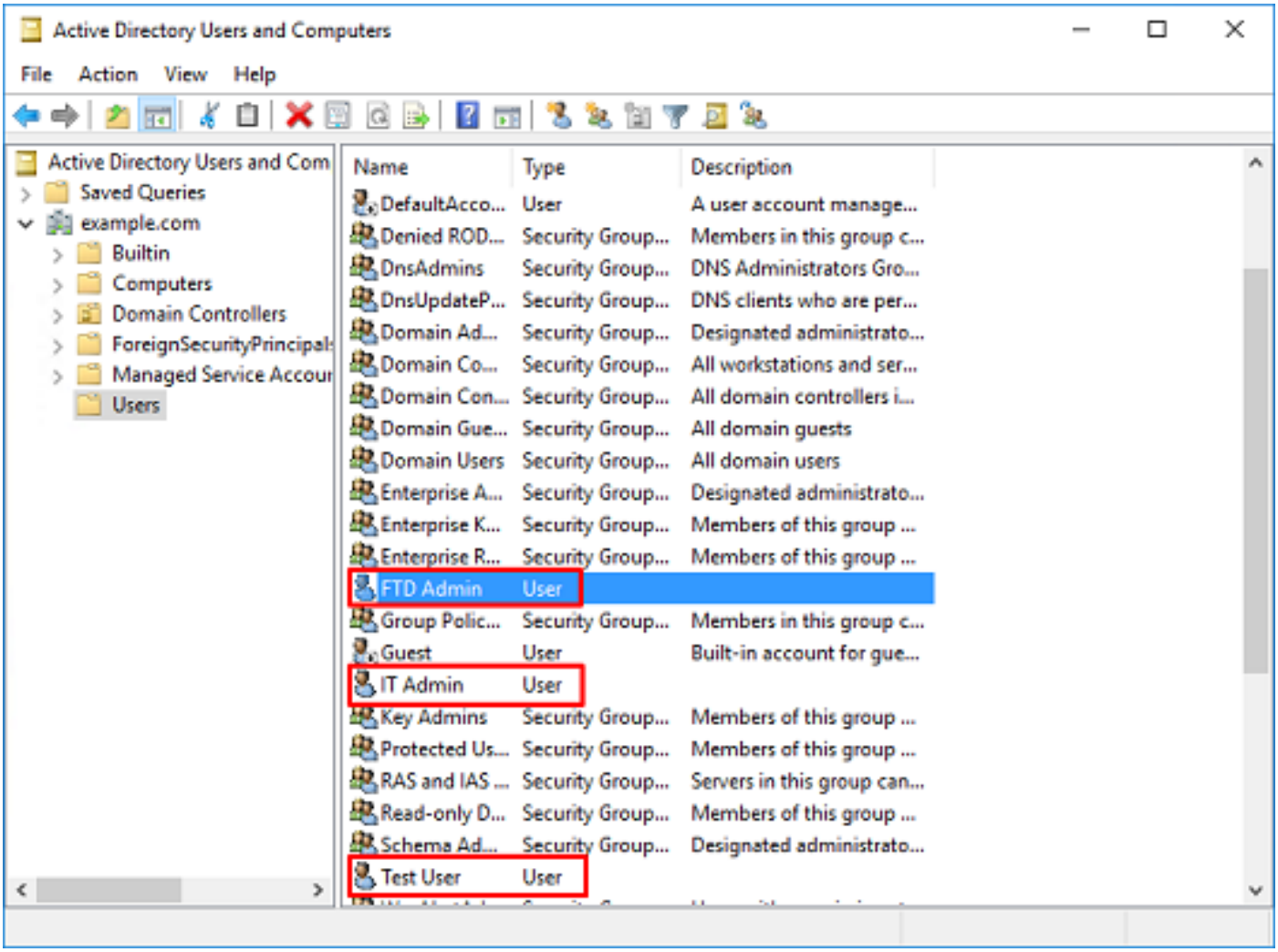
2. **새 개체 - 사용자 마법사**를 진행합니다.







3. FTD 계정**이 생성되었는지** 확인합니다. **IT** 관리자와 **테스트 사용자**, 두 **개의** 추가 **어카운트가 생성됩니다**.



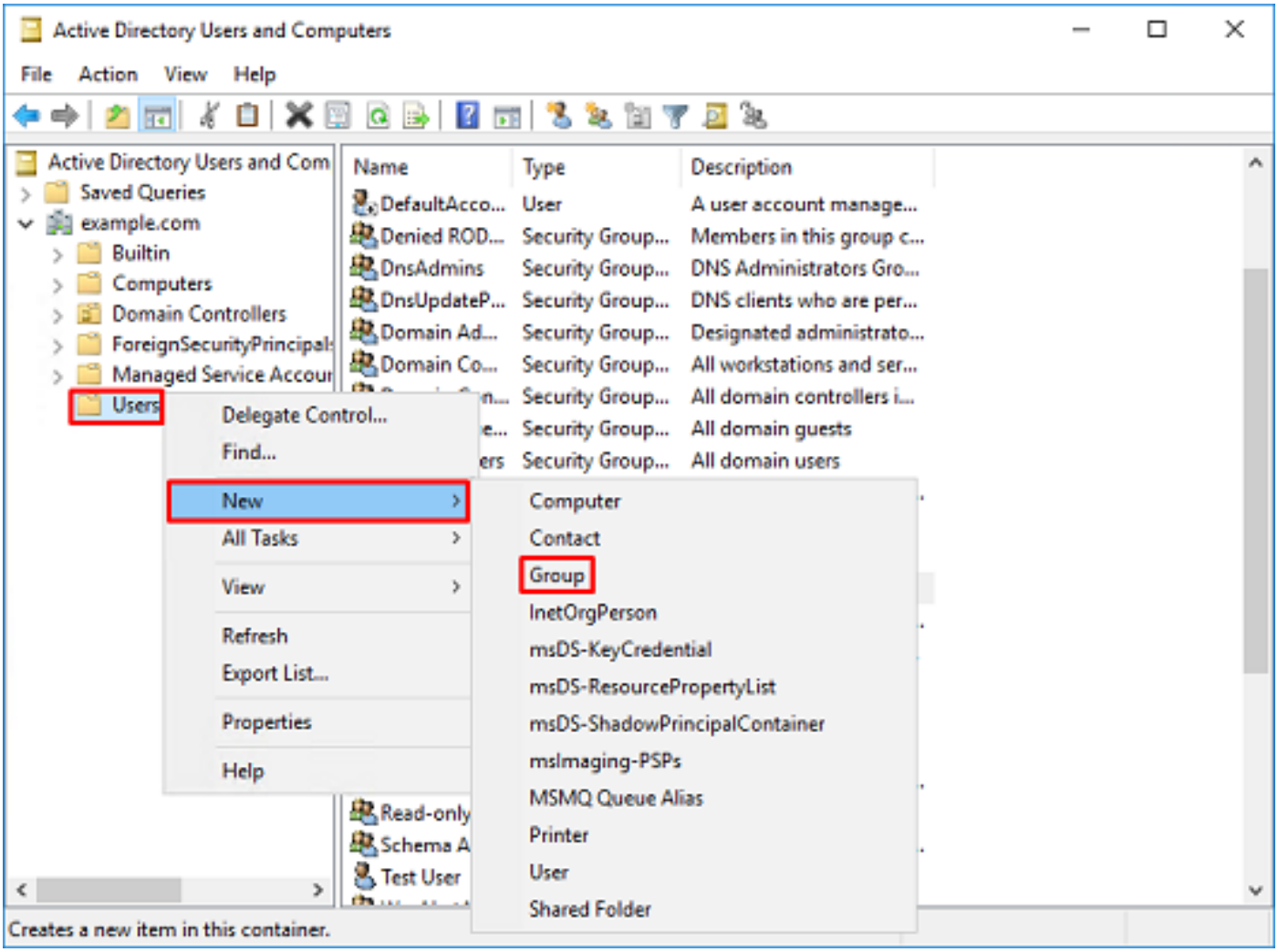
AD 그룹 생성 및 AD 그룹에 사용자 추가(선택 사항)

인증에는 필요하지 않지만 그룹을 사용하여 여러 사용자에게 액세스 정책을 더 쉽게 적용하고 LDAP 권한 부여를 수행할 수 있습니다.

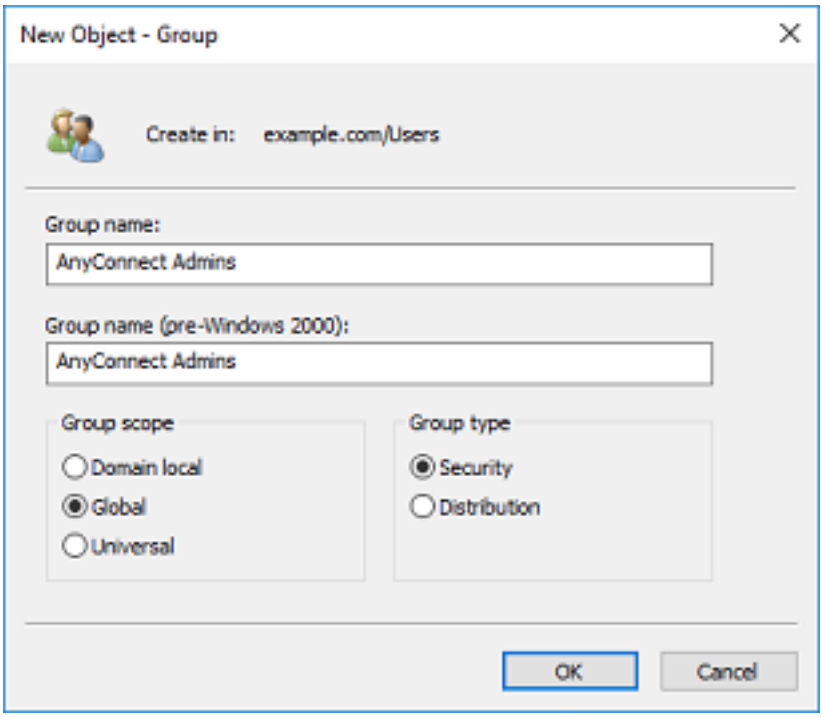
이 컨피그레이션 가이드에서는 나중에 FMC 내에서 사용자 ID를 통해 액세스 제어 정책 설정을 적용하는 데 그룹을 사용합니다.

1. **Active Directory 사용자 및 컴퓨터**에서 새 그룹이 추가된 컨테이너 또는 조직 구성 단위를 마우스 오른쪽 단추로 클릭합니다.

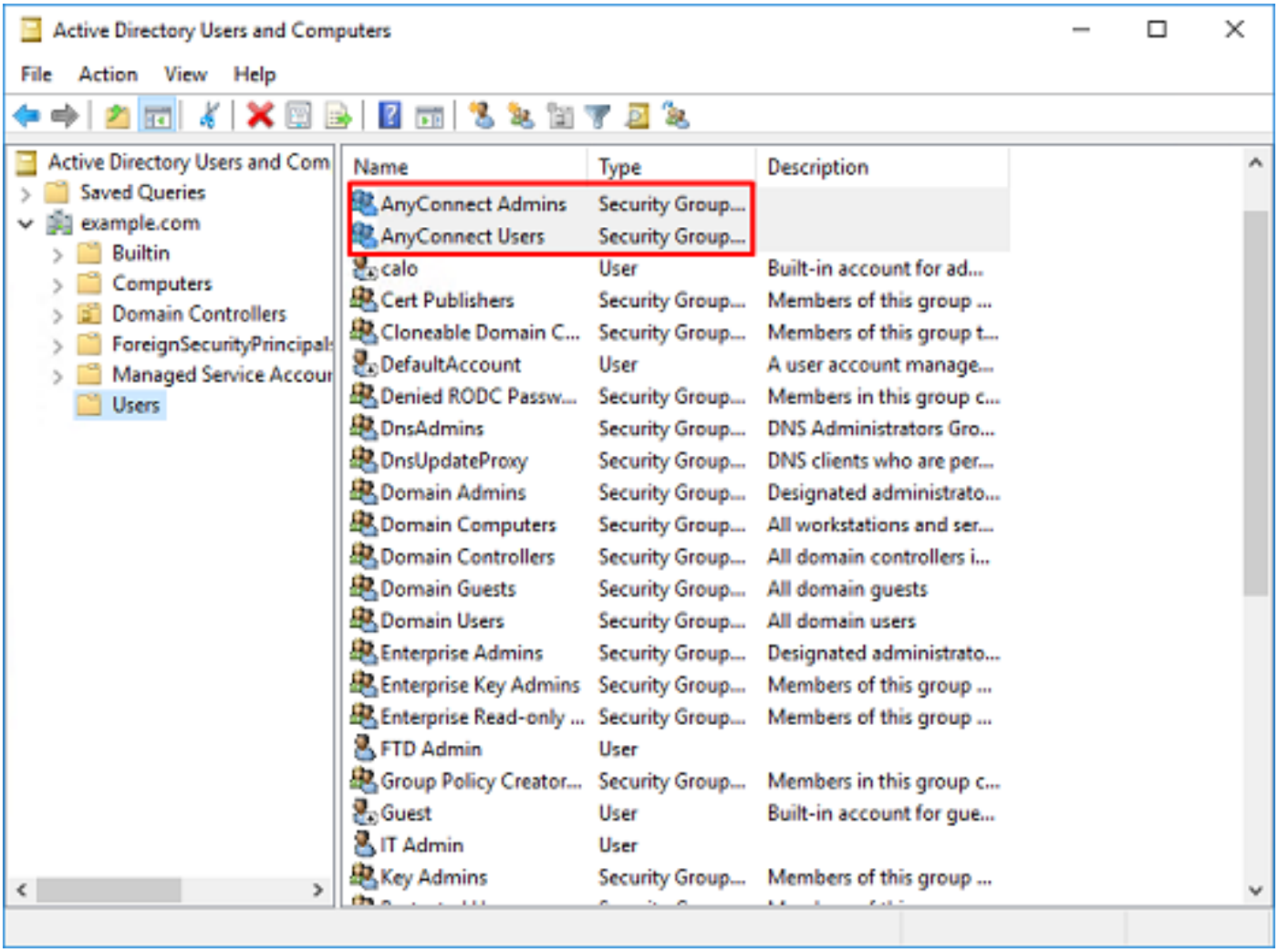
이 예에서는 그룹 AnyConnect Admins가 Users(사용자) 컨테이너 **아래에** 추가됩니다. Users(사용자)를 마우스 오른쪽 **버튼**으로 클릭한 다음 **New(새로 만들기) > Group(그룹)으로 이동합니다**.



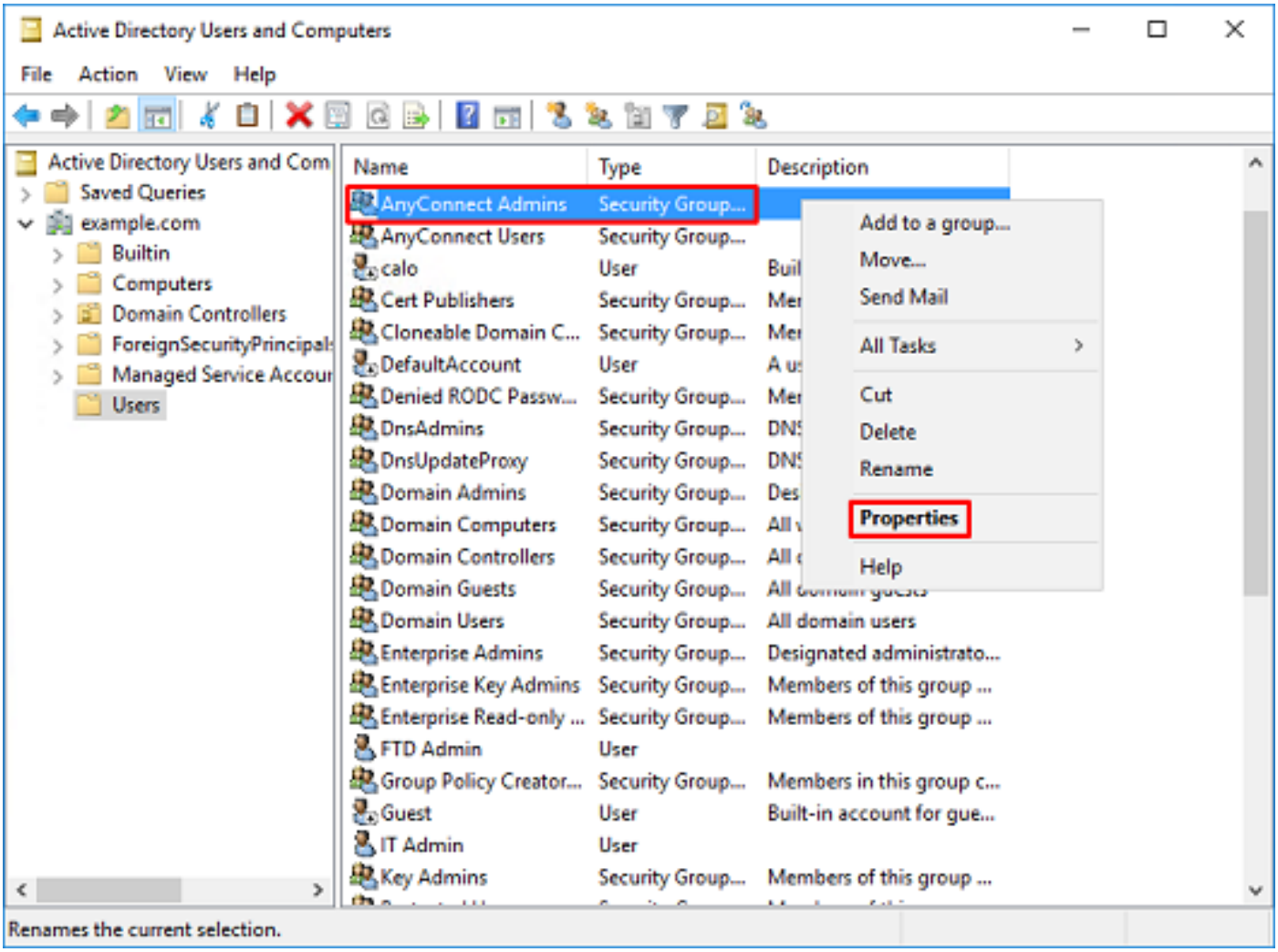
2. **새 개체 - 그룹 마법사**를 진행합니다.



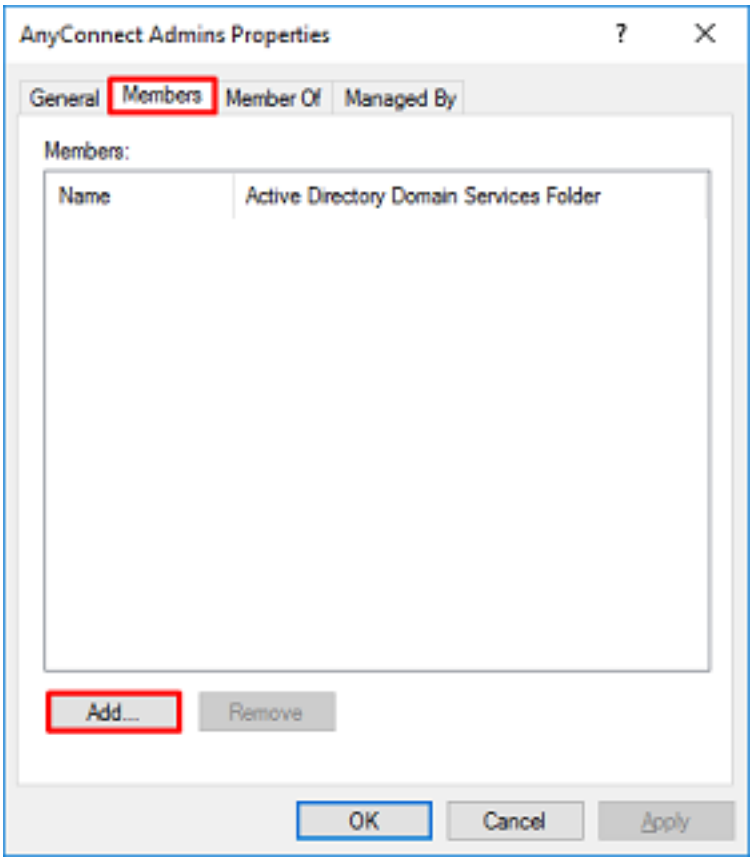
3. 그룹이 생성되었는지 확인합니다. AnyConnect **사용자** 그룹도 생성됩니다.



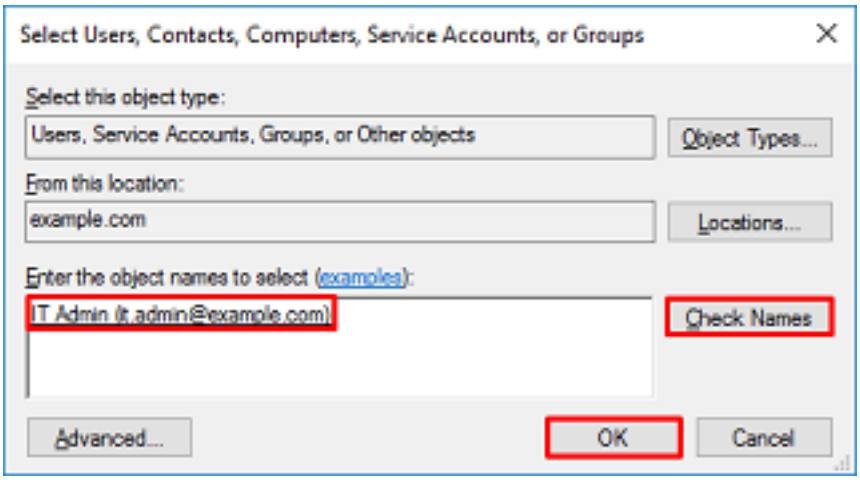
4. 사용자 그룹을 마우스 오른쪽 단추로 클릭한 다음 등록 정보**를 선택합니다**. 이 컨피그레이션에서는 사용자 IT 관리자가 AnyConnect 관리자 그룹에 추가되고 사용자 **테스트 사용자**가 AnyConnect 사용자 그룹에 **추가됩니다**.



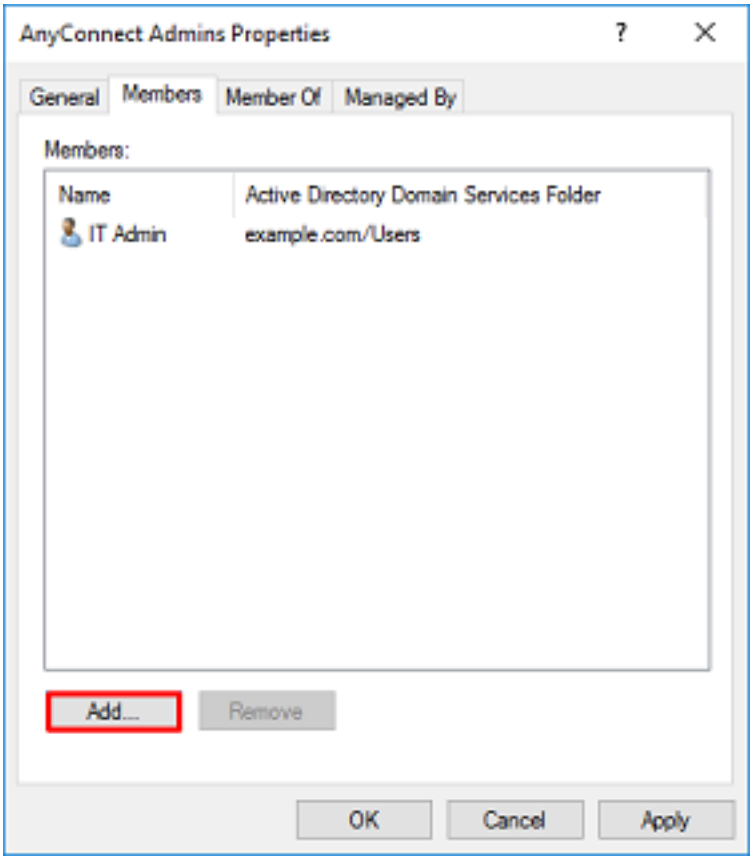
5. **구성원** 탭에서 추가를 **클릭합니다**.



필드에 사용자를 입력하고 이름 **확인**을 클릭하여 사용자를 확인합니다. 확인했으면 확인을 **클릭합니다**.

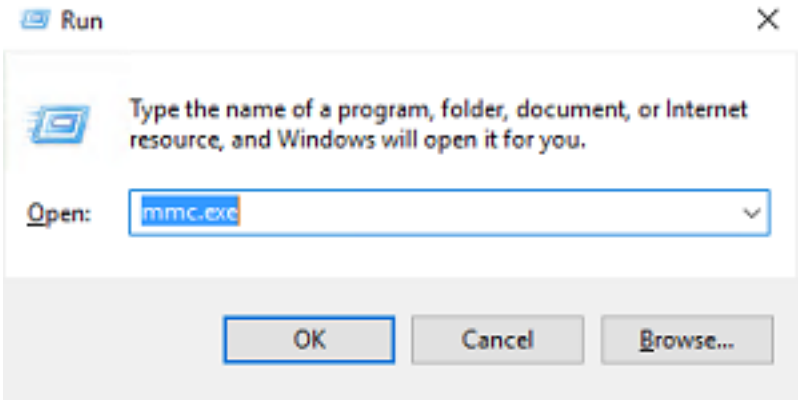


올바른 사용자가 추가되었는지 확인한 다음 OK(확인) 버튼을 클릭합니다. 사용자 **테스트 사용자**는 동일한 단계를 사용하여 **AnyConnect 사용자** 그룹에도 추가됩니다.

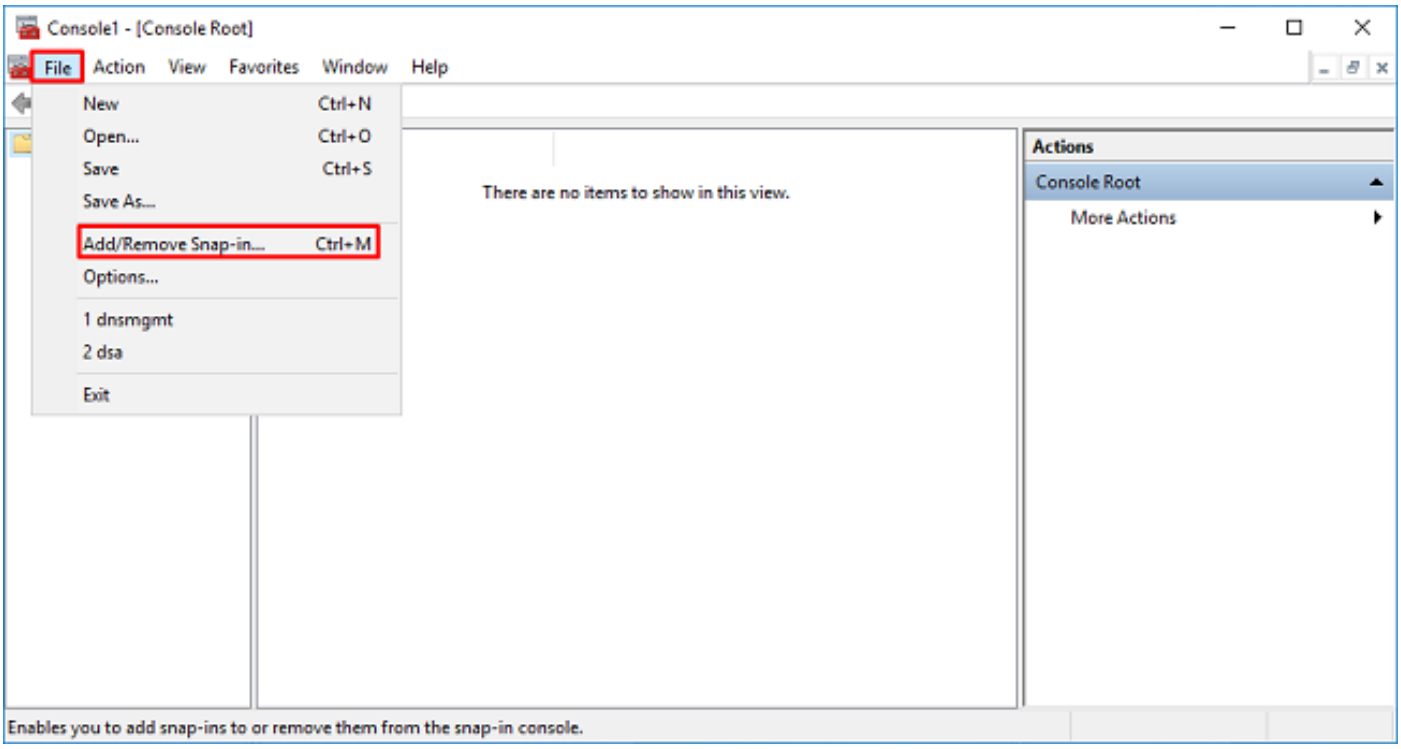


LDAPS SSL 인증서 루트 복사(LDAPS 또는 STARTTLS에만 필요)

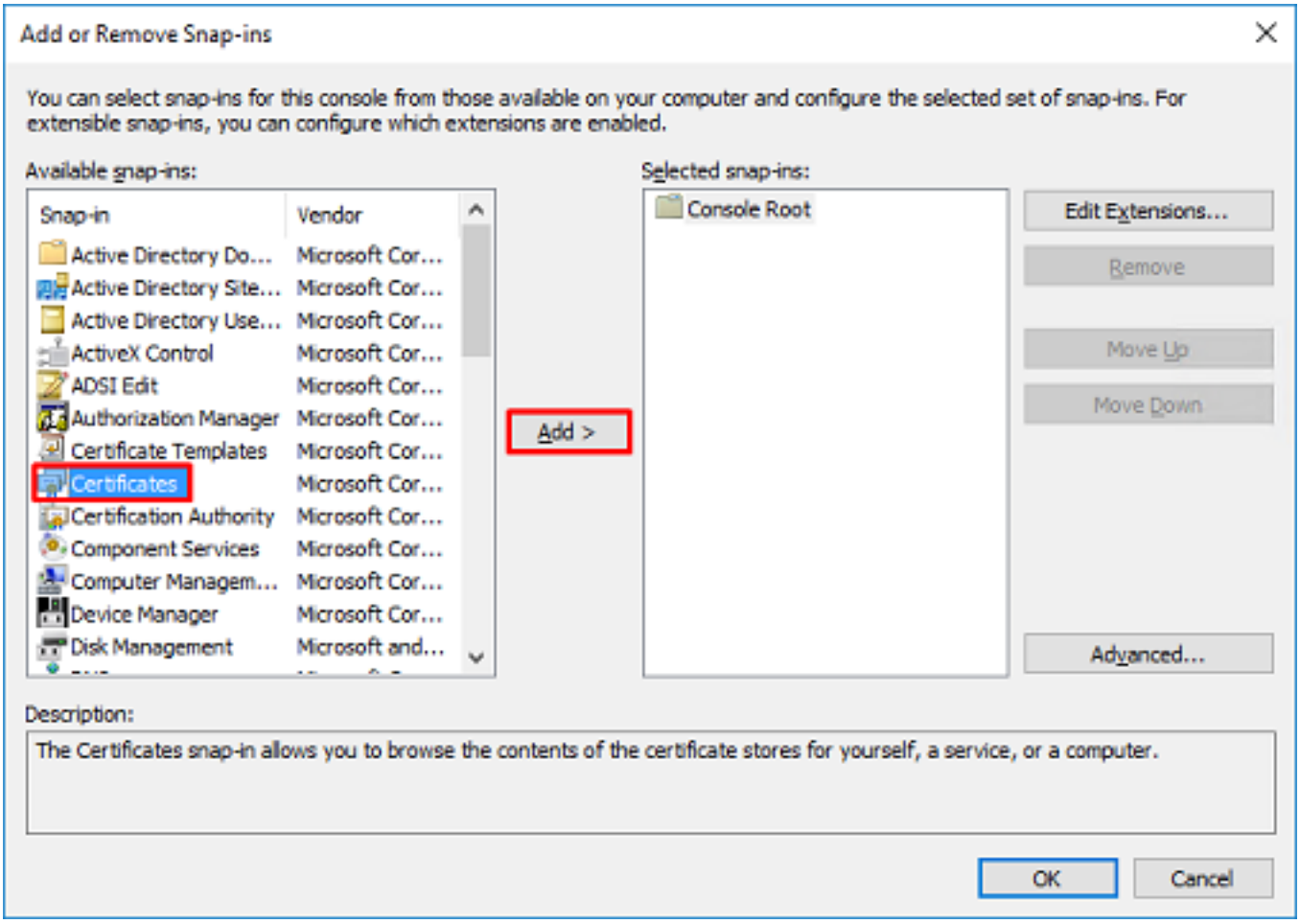
1. **Win+R을** 누르고 mmc.**exe**를 입력한 다음 확인을 클릭합니다.



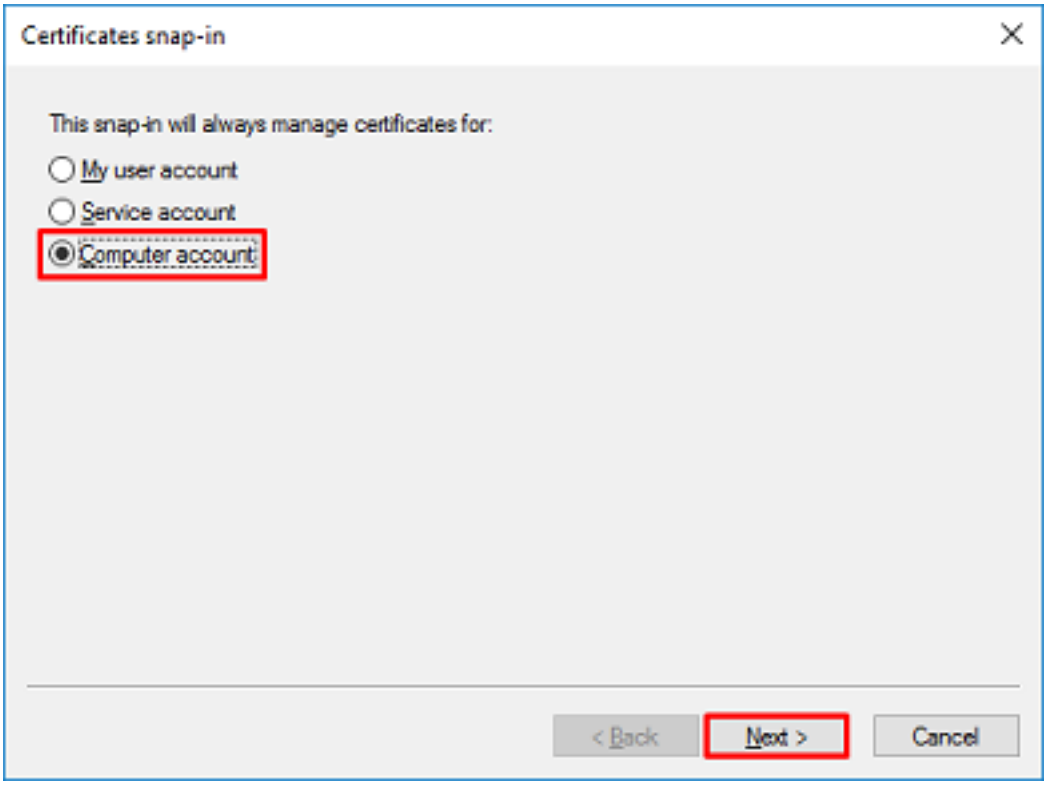
2. **파일 > 스냅인 추가/제거로 이동합니다.**



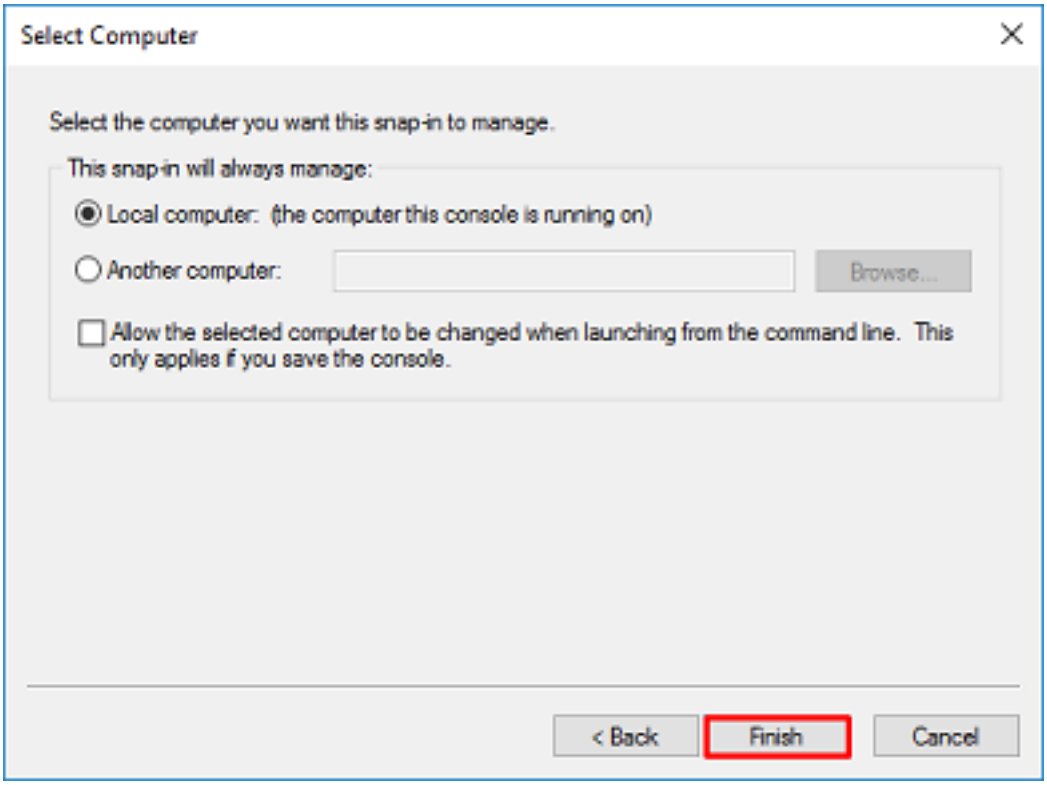
3. Available 스냅인에서 Certificates를 선택한 다음 **Add**를 클릭합니다.



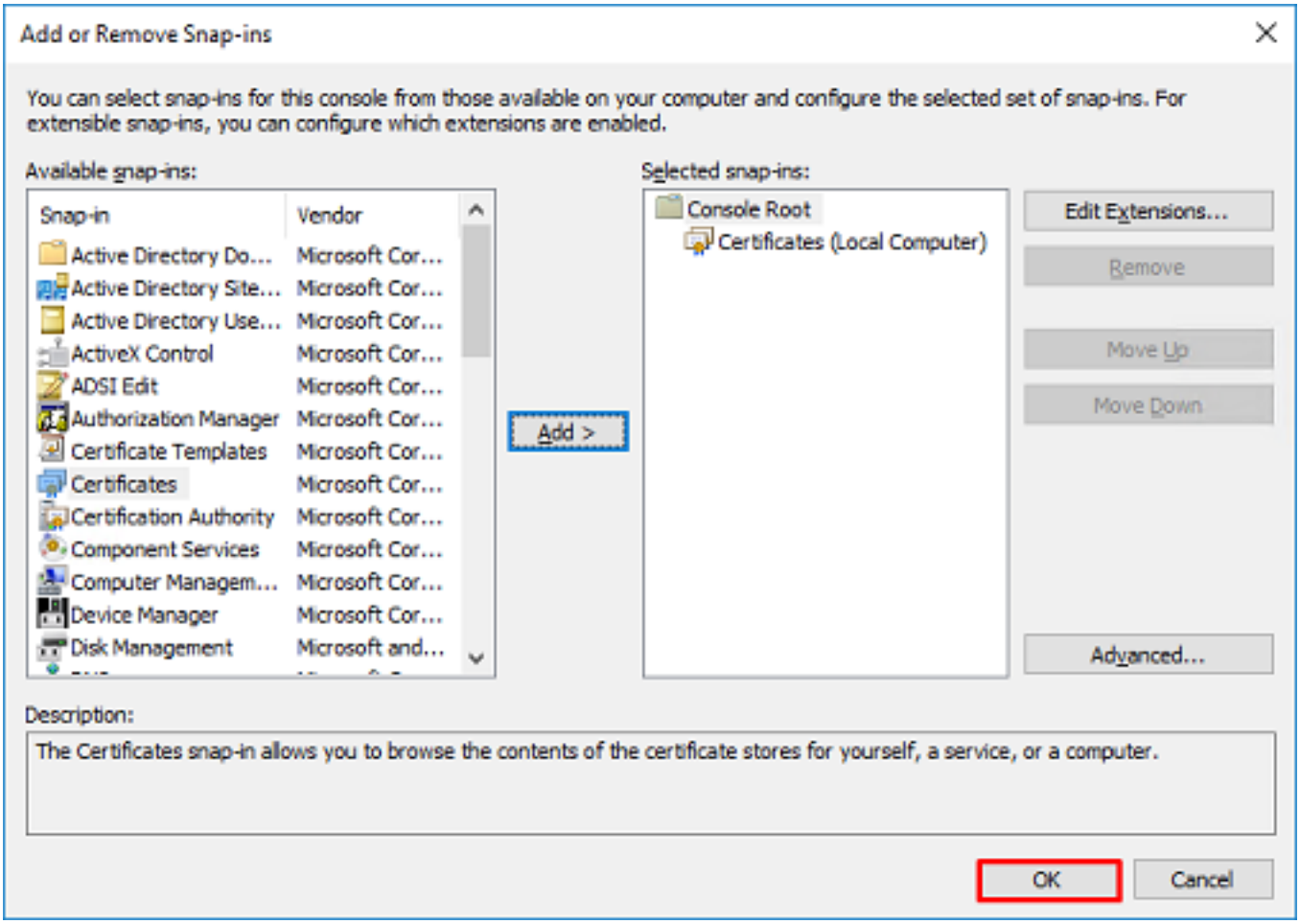
4. **컴퓨터** 계정**을 선택한** 후 다음을 **클릭합니다**.



Finish(마침)를 클릭합니다.



5. 이제 확인을 **클릭합니다**.

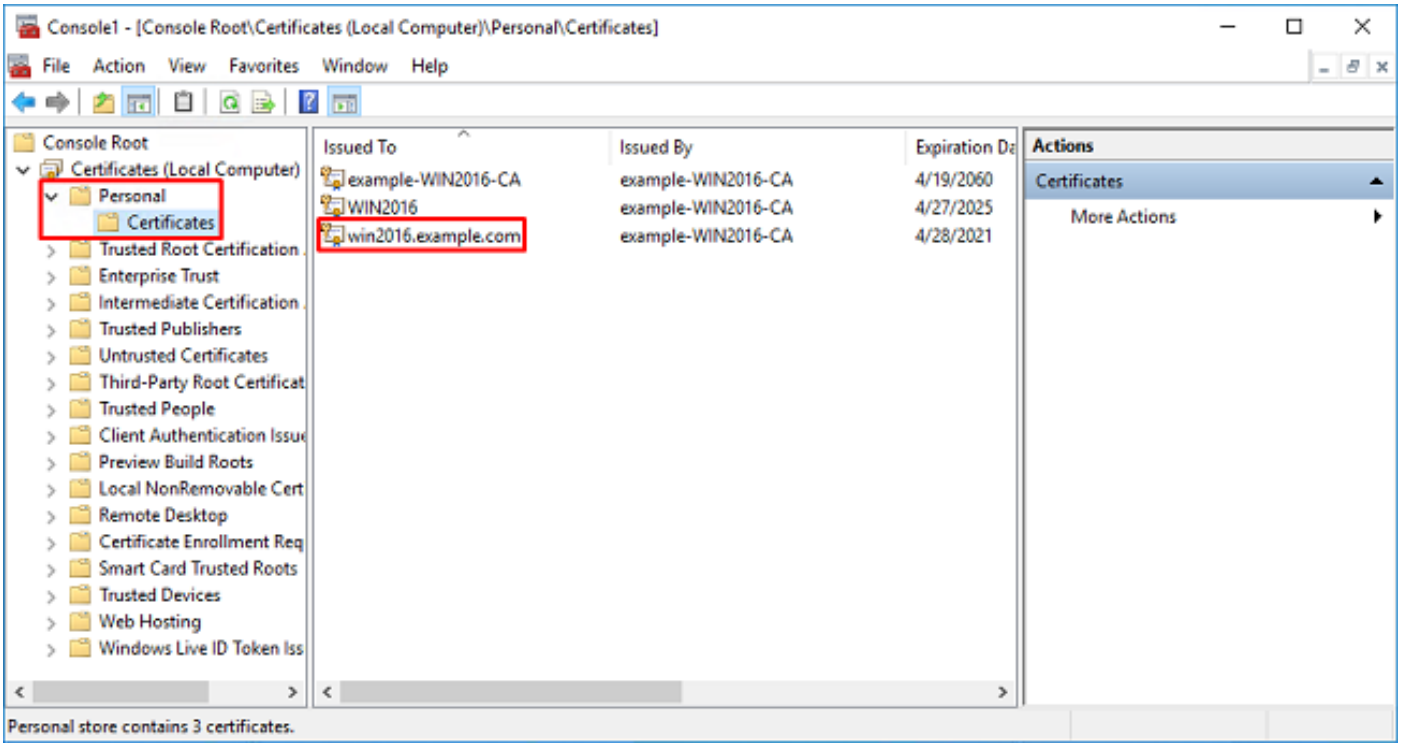


6. **개인** 폴더를 **확장한** 다음 인증서를 **클릭합니다**. LDAPS에서 사용하는 인증서가 Windows 서버의 **FQDN(Fully Qualified Domain Name)**에 발급됩니다. 이 서버에는 3개의 인증서가 나열됩니다.

- example-WIN2016-CA에서 발급한 CA 인증서.

- example-WIN2016-CA가 WIN2016에 발급한 ID 인증서입니다.
- example-WIN2016-CA가 win2016.example.com에 발급한 ID 인증서

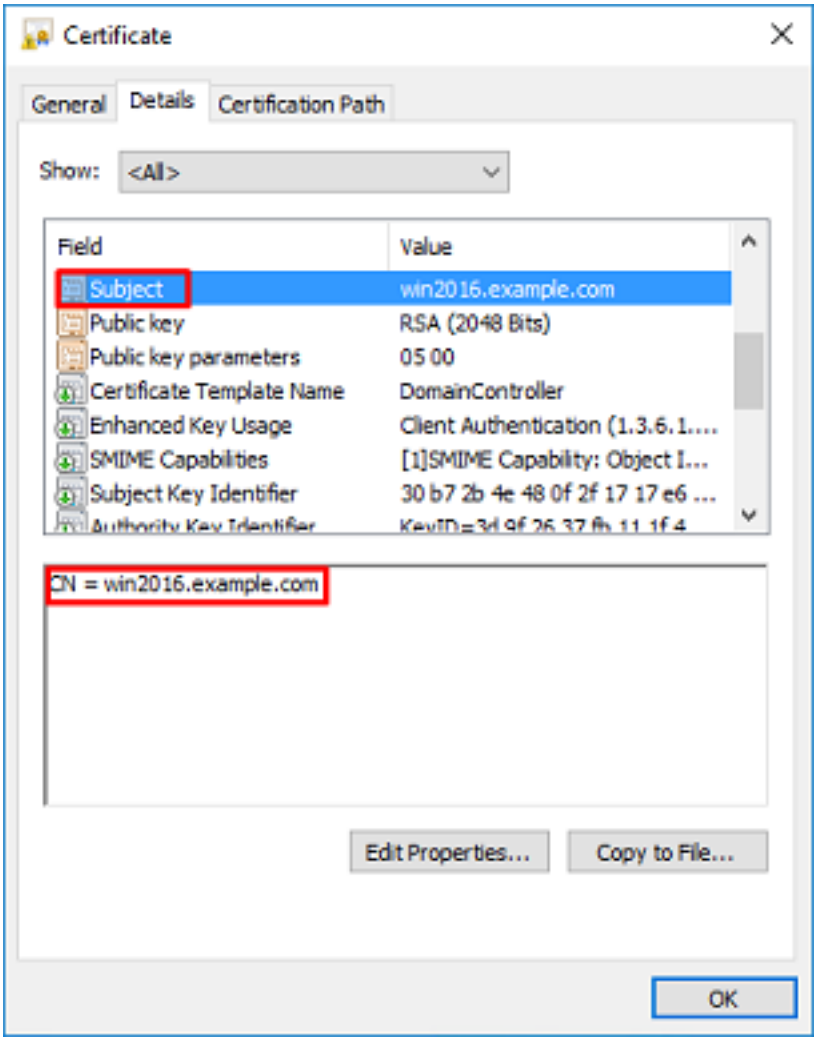
이 컨피그레이션 가이드에서 FQDN은 win2016.example.com이므로 처음 2개의 인증서는 LDAPS SSL 인증서로 사용할 수 없습니다. win2016.example.com에 발급된 ID 인증서는 Windows Server CA 서비스에서 자동으로 발급된 인증서입니다. 세부 정보를 확인하려면 인증서를 두 번 클릭합니다.

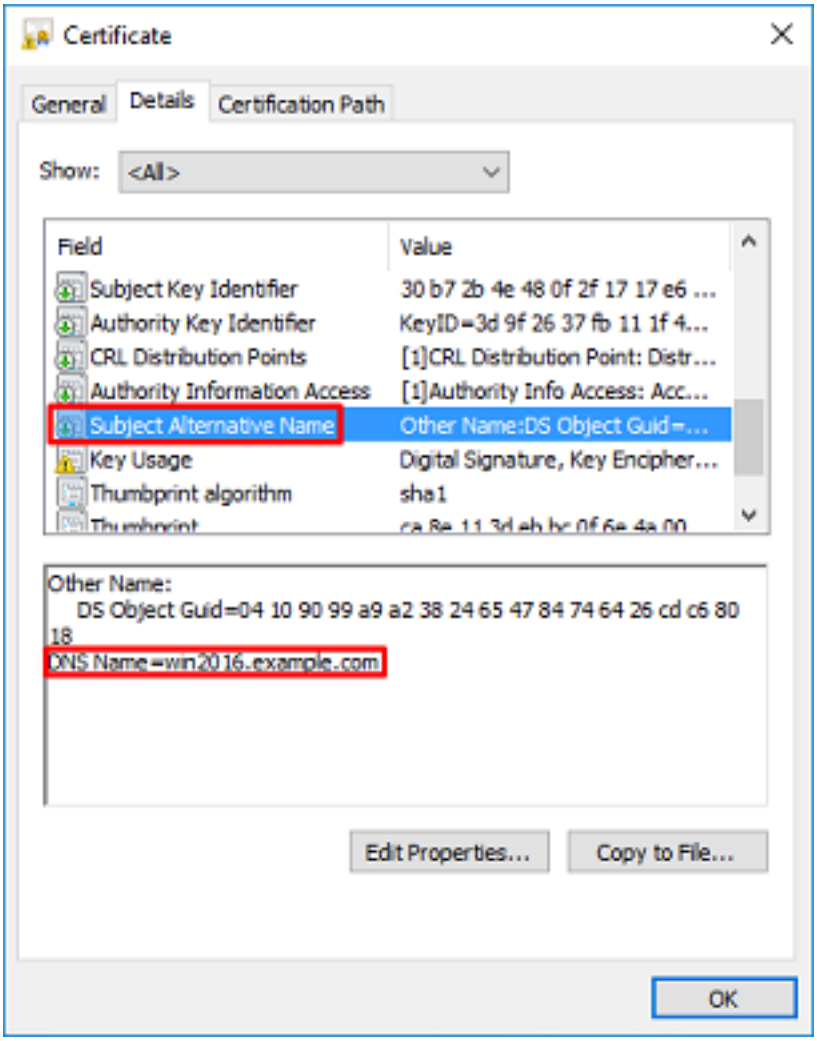


7. LDAPS SSL 인증서로 사용하려면 인증서가 다음 요구 사항을 충족해야 합니다.

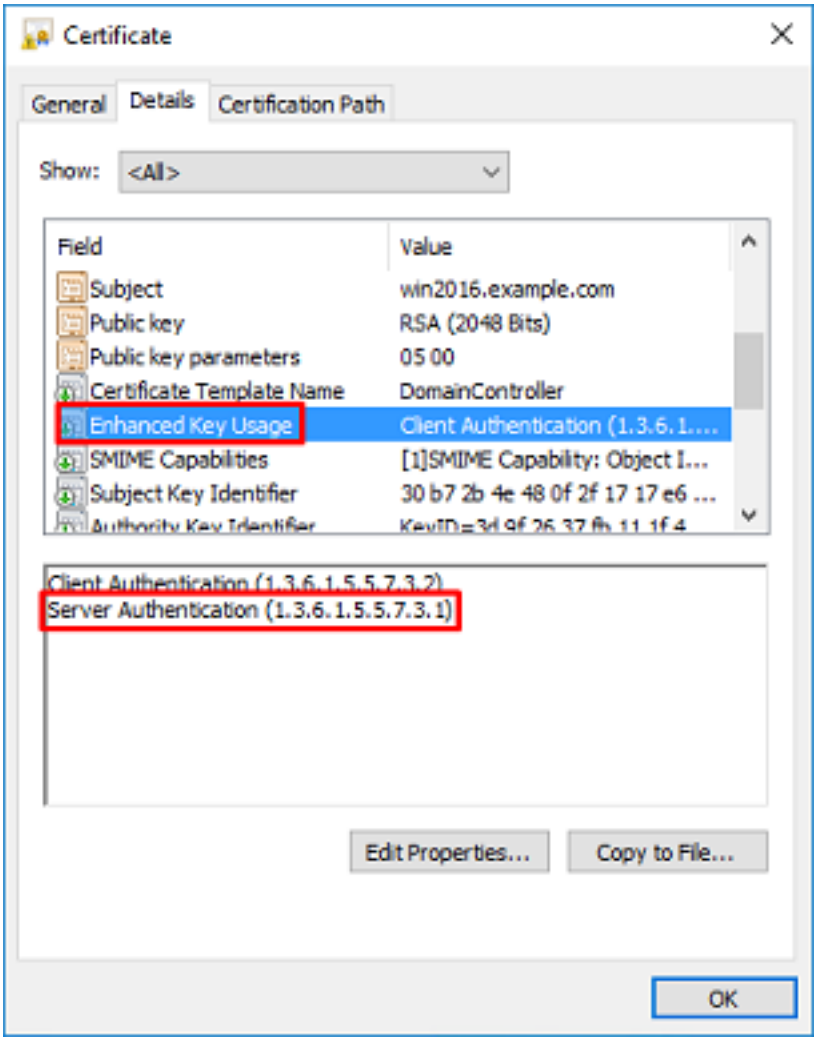
- 공용 이름 또는 **DNS 주체 대체 이름**은 Windows Server의 FQDN과 일치합니다.
- 인증서에는 Enhanced **Key Usage(고급 키 사용) 필드** 아래에 **서버 인증이** 있습니다.

인증서의 **Details**(세부사항) 탭에서 **Subject(주체)** 및 **Subject Alternative Name(주체 대체 이름)을** 선택합니다. FQDN win2016.example.com이 있습니다.

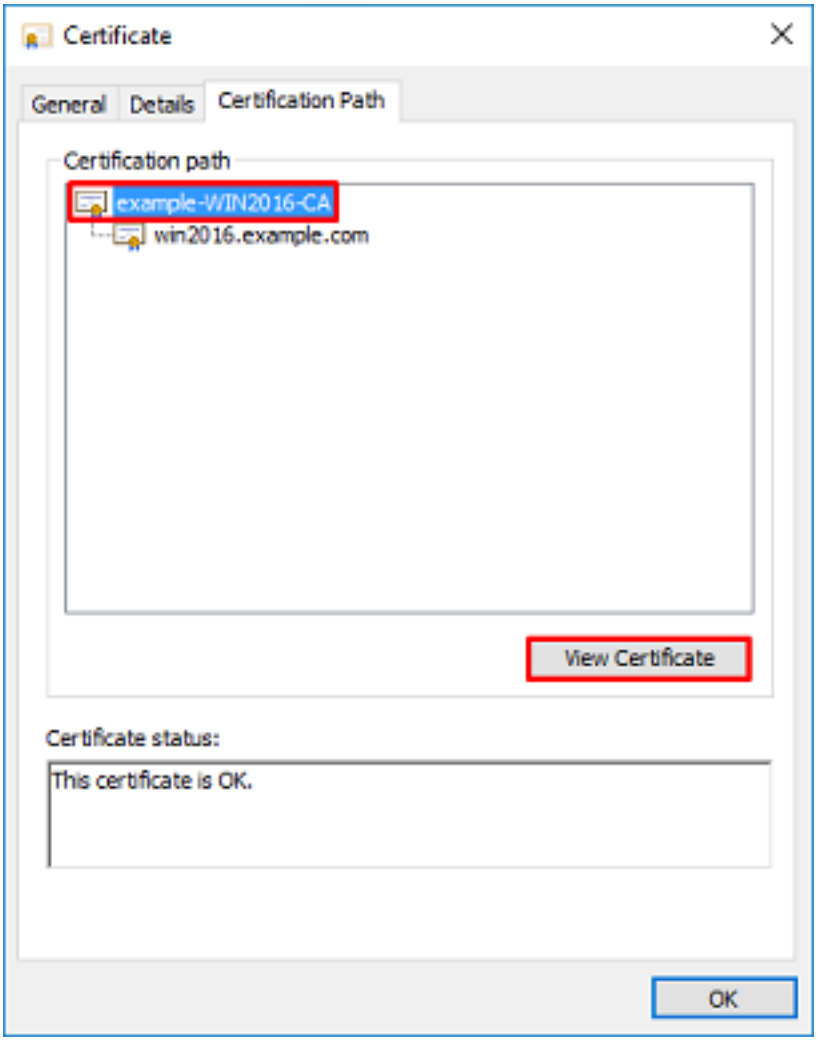

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...
Subject Key Identifier
30 b7 2b 4e 48 0f 2f 17 17 e6 ...
CN = win2016.example.com
Edit Properties...
Copy to File...
OK



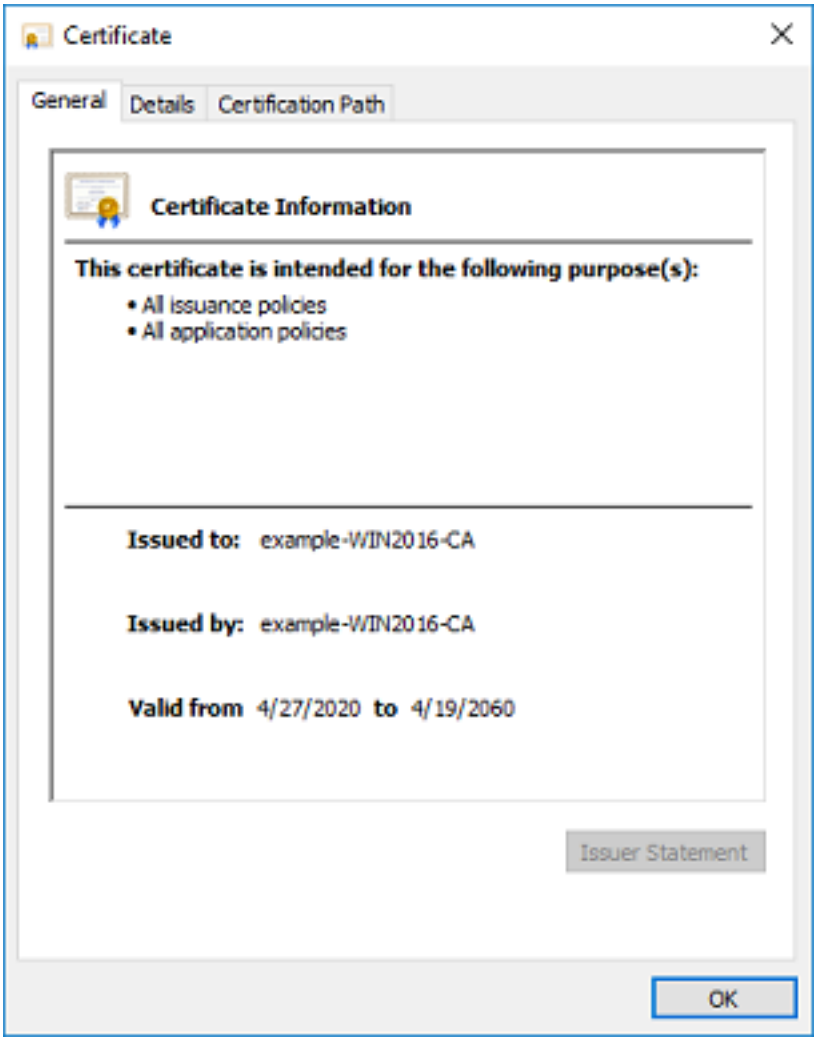
Enhanced **Key Usage(고급 키 사용)** 아래에 **Server Authentication(서버 인증)**이 있습니다.



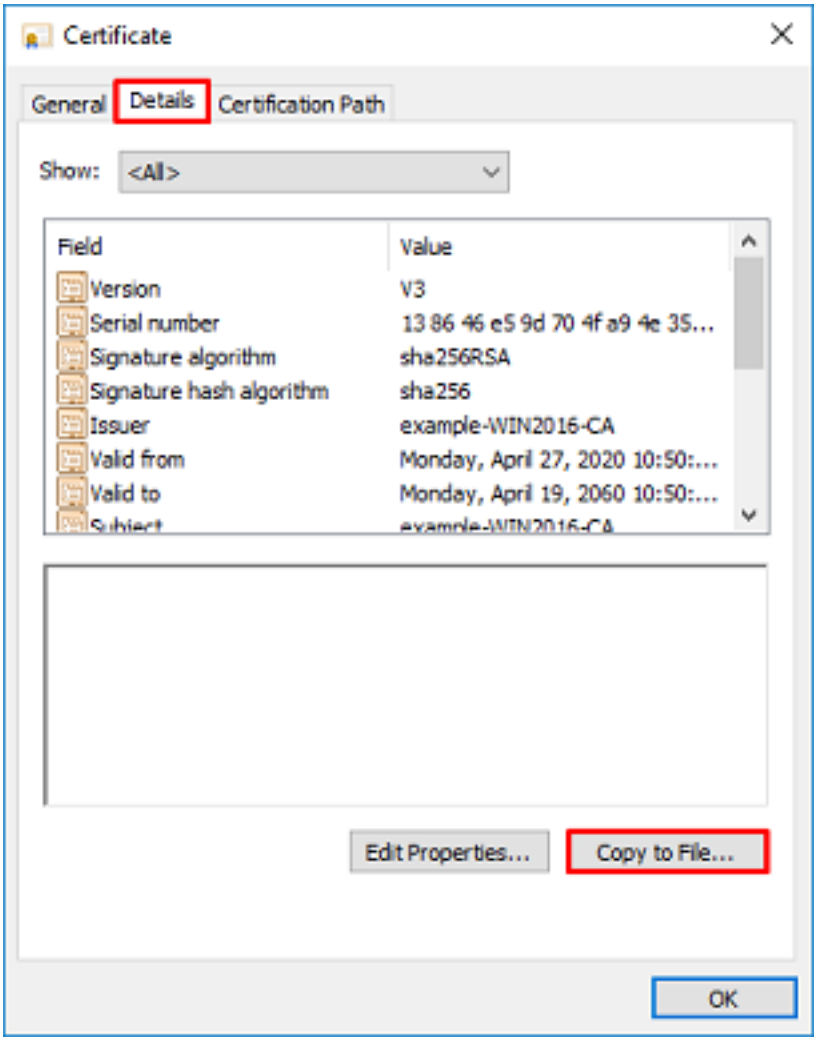
8. 확인이 완료되면 **Certification Path(인증 경로)** 탭에서 루트 CA 인증서인 최상위 인증서를 선택한 다음 View Certificate(**인증서 보기**)를 클릭합니다.



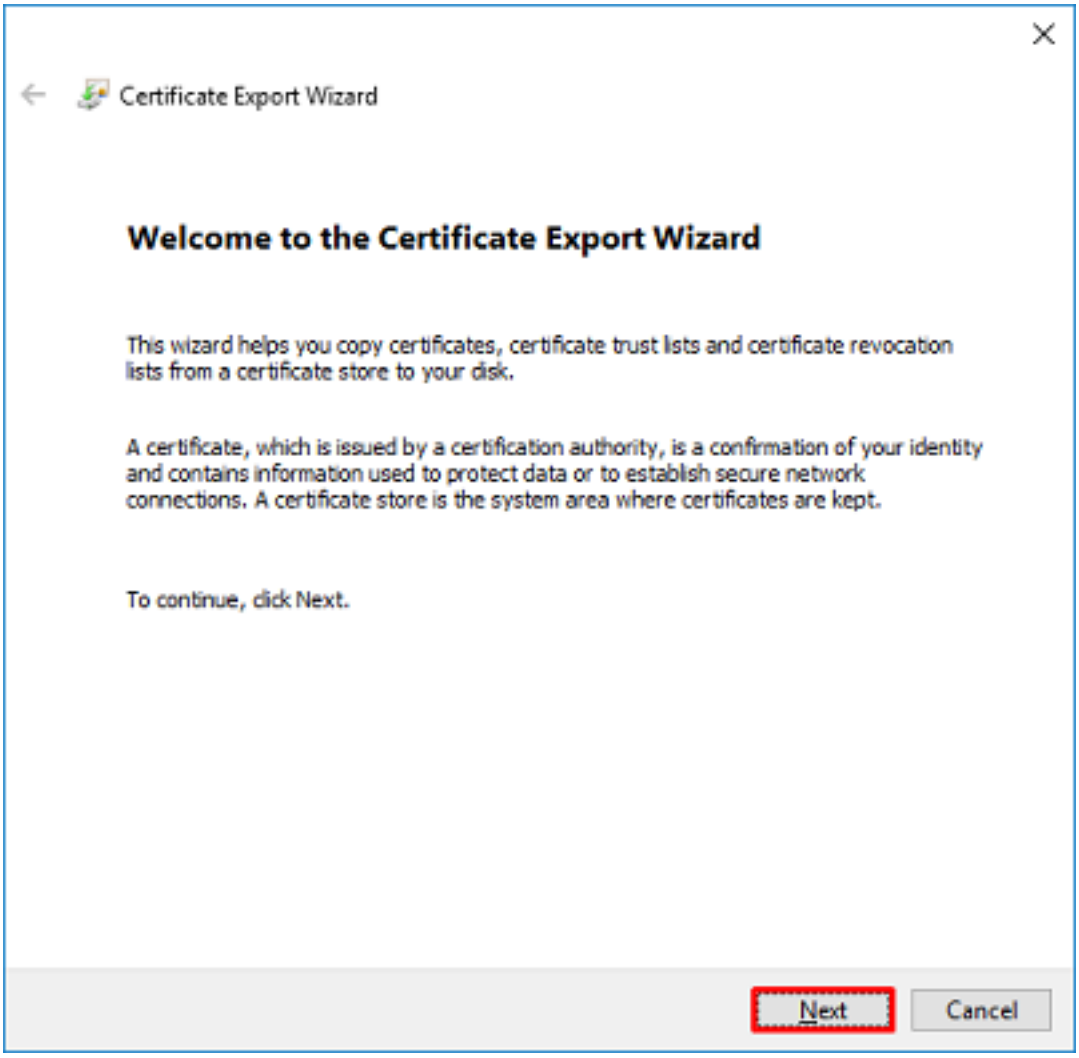
9. 루트 CA 인증서에 대한 인증서 세부사항이 열립니다.



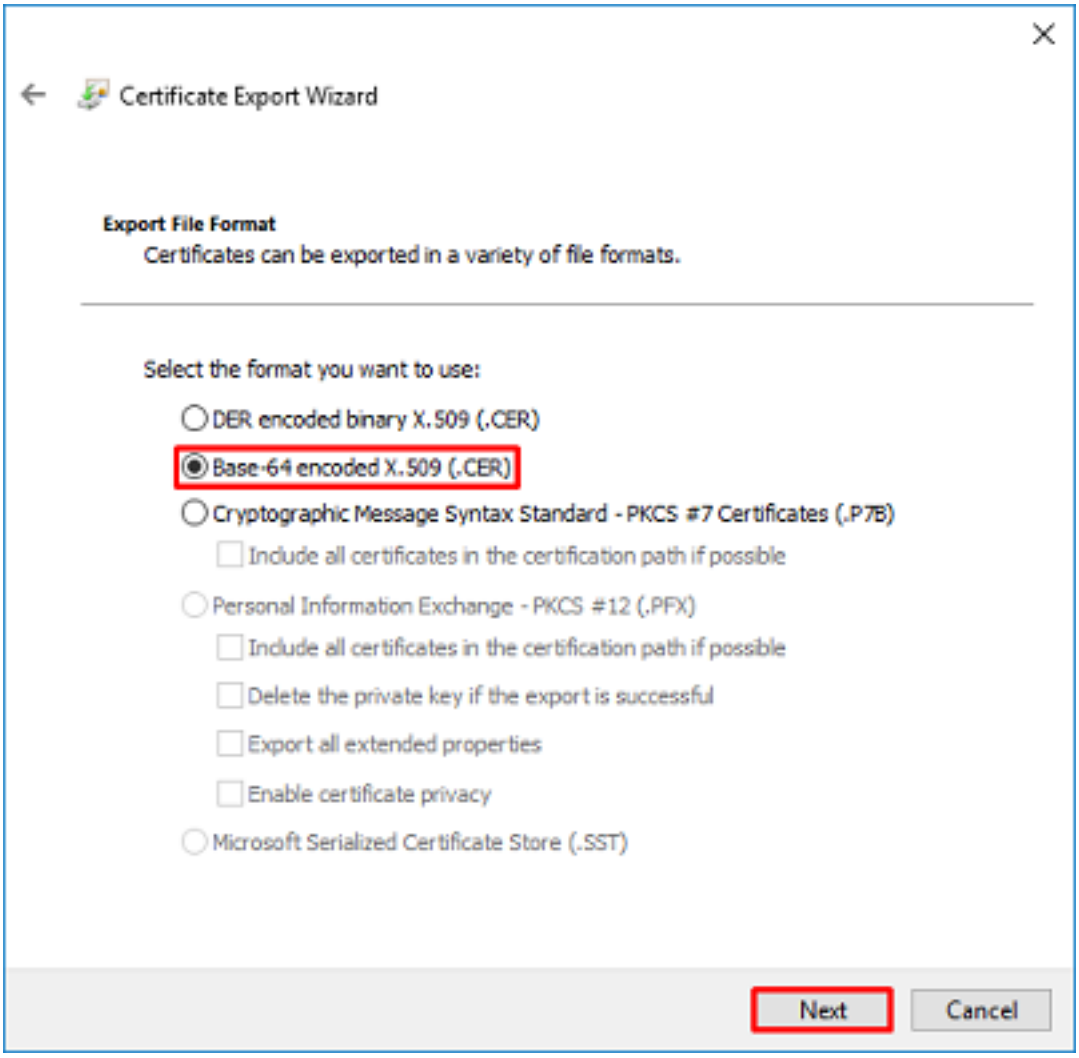
Details 탭에서 Copy **to File...(파일에 복사...)을** 클릭합니다.



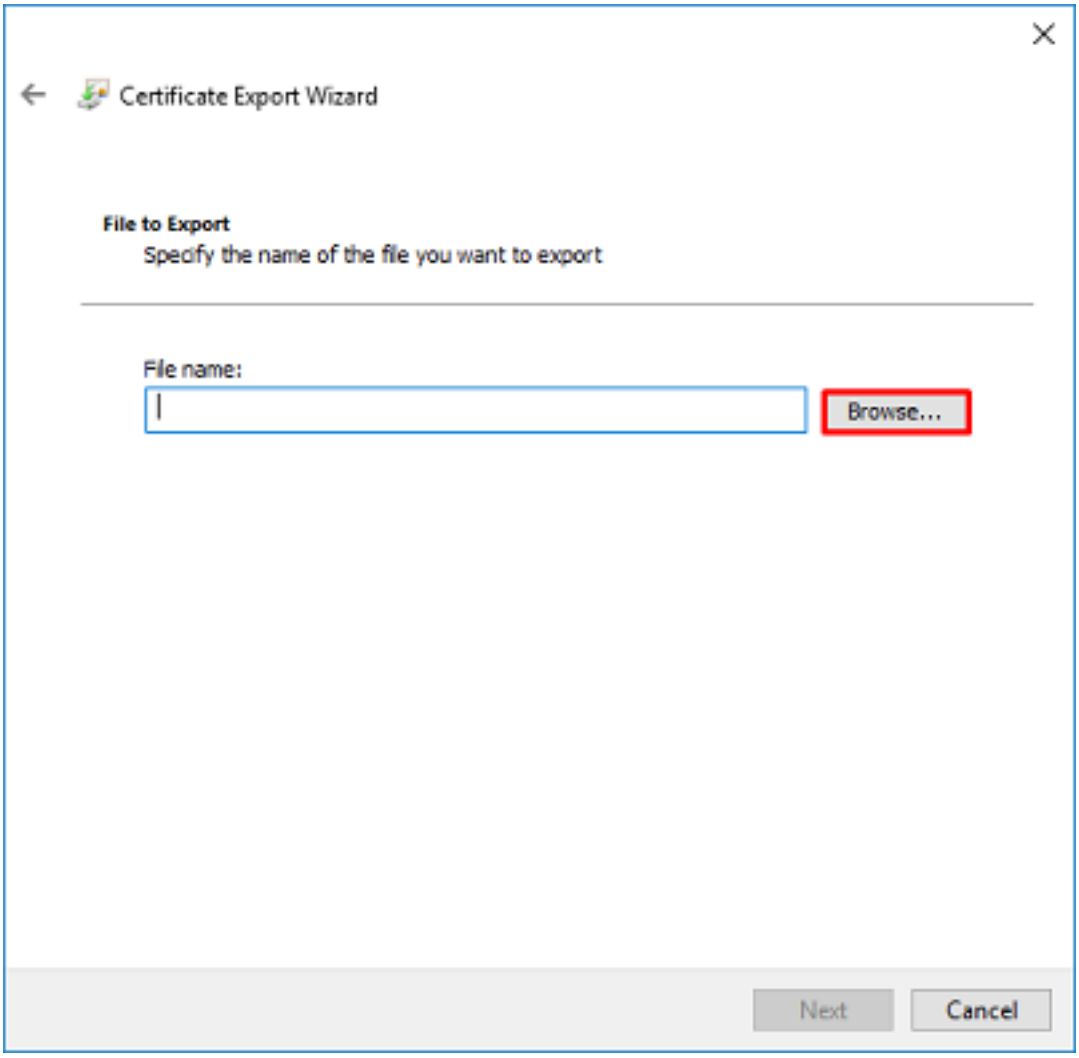
10. 루트 CA를 **PEM** 형식으로 내보내는 인증서 내보내기 마법사를 진행합니다.

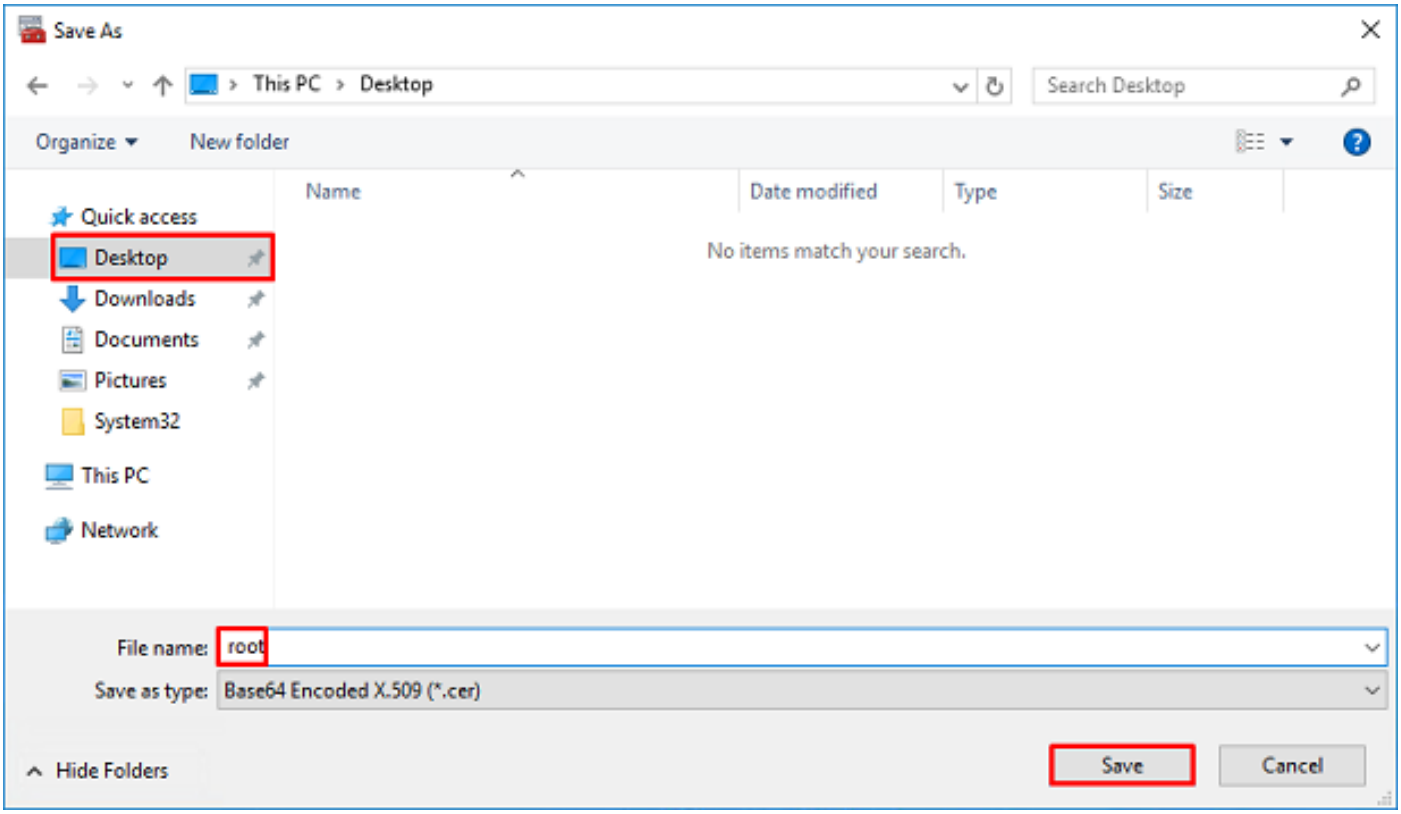


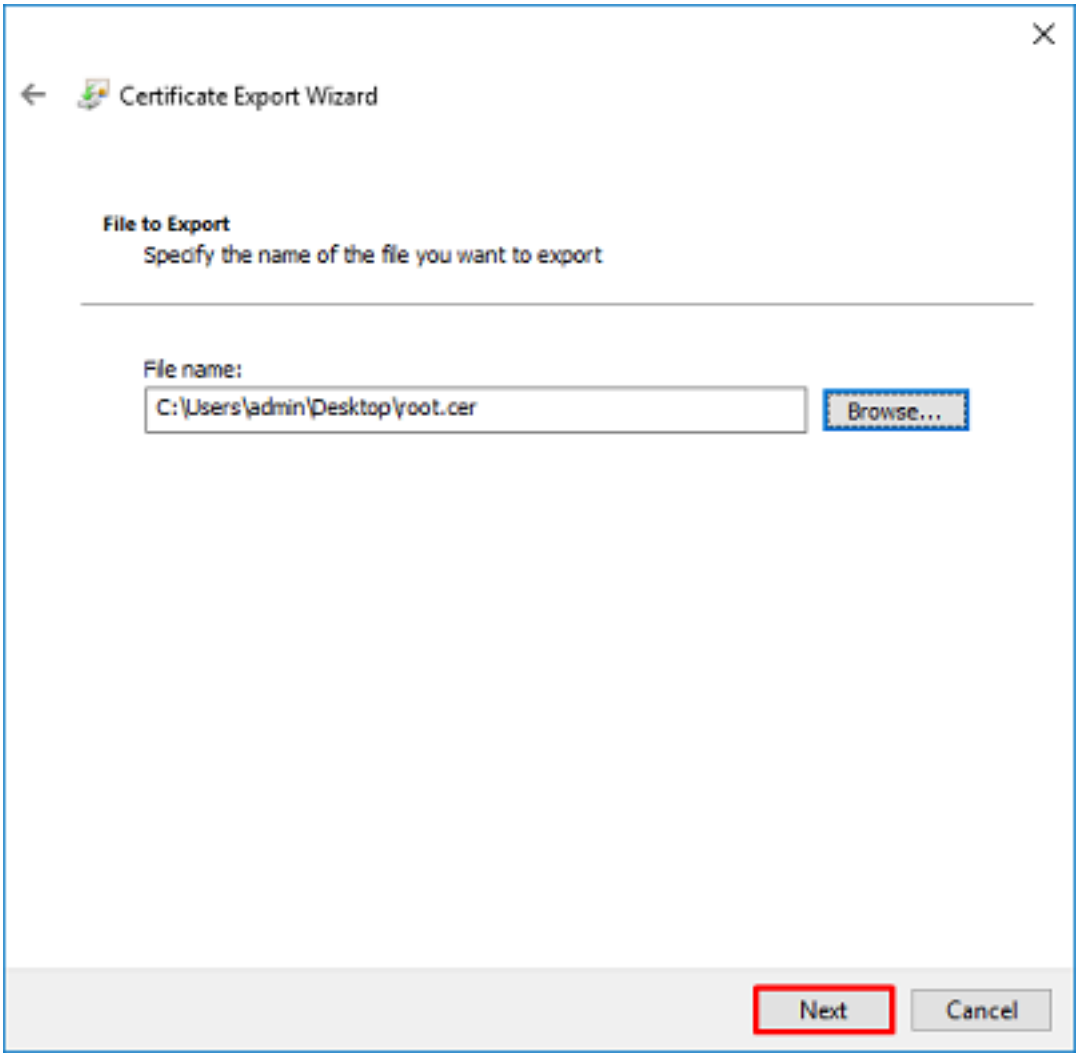
Base-64 인코딩 X.509를 선택합니다.



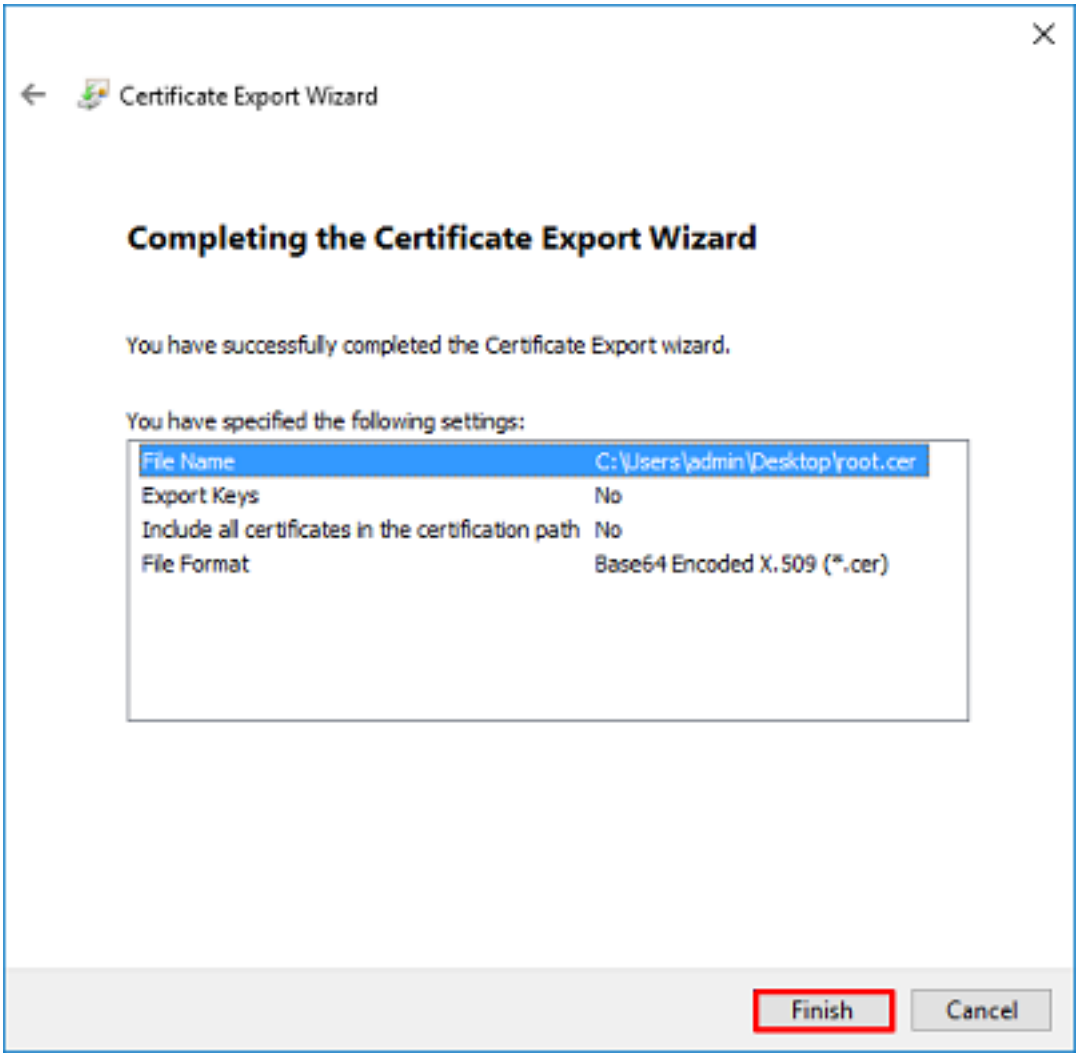
파일의 이름과 내보낼 위치를 선택합니다.


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
Browse...
Next
Cancel


Save As
This PC
Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
No items match your search.
File name:
root
Save as type:
Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel



이제 Finish(마침)**를 클릭합니다**.



11. 이제 위치로 이동하여 메모장이나 다른 텍스트 편집기로 인증서를 엽니다. PEM 형식 인증서가 표시됩니다. 나중에 사용할 수 있도록 저장하십시오.

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

12. (선택 사항) LDAPS에서 사용할 수 있는 ID 인증서가 여러 개 있고 사용 여부가 불확실하거나 LDAPS 서버에 대한 액세스 권한이 없는 경우 Windows 서버 또는 FTD에서 수행한 패킷 캡처에서 루트 ca를 추출할 수 있습니다.

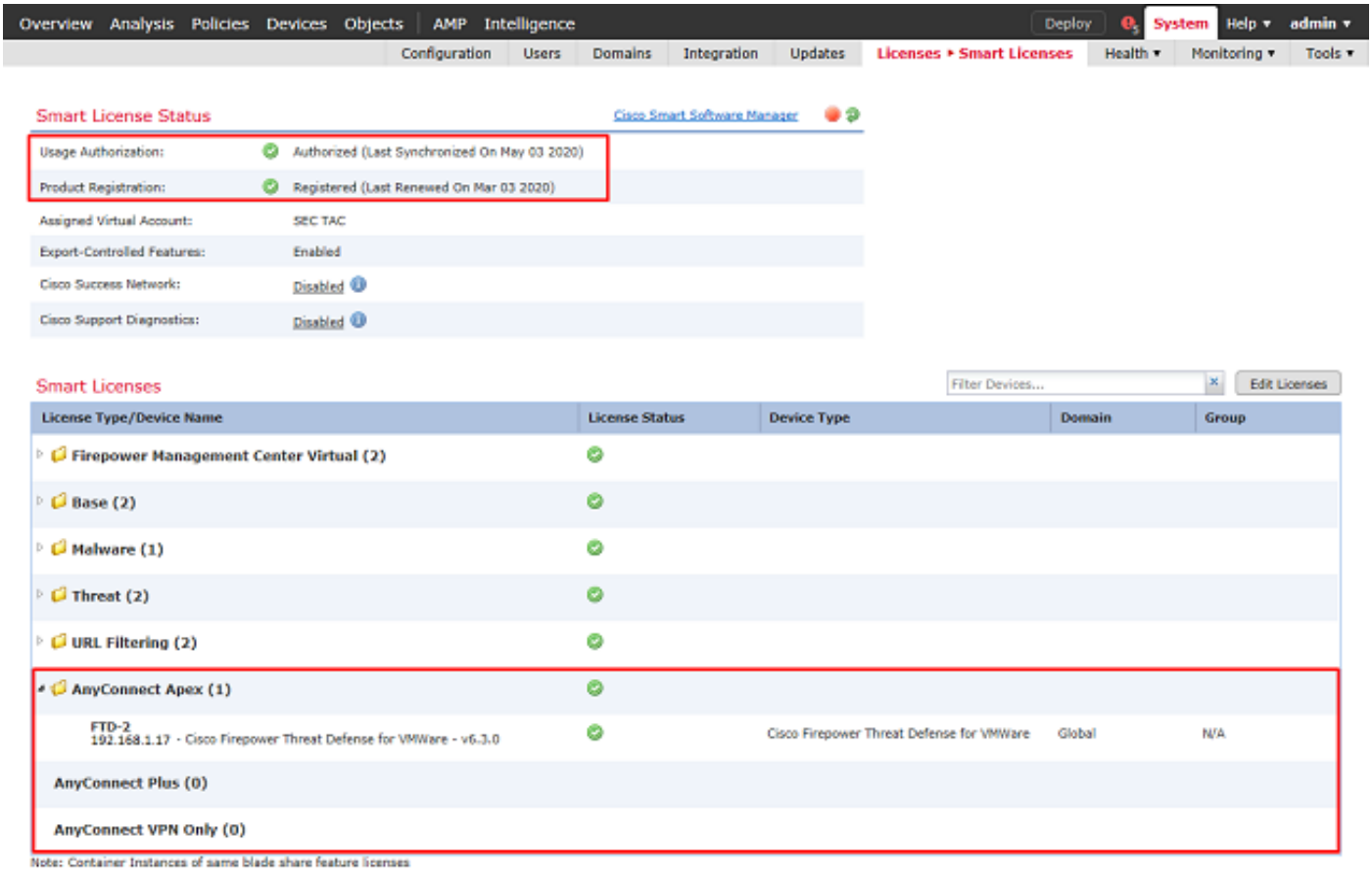
FMC 컨피그레이션

라이센싱 확인

AnyConnect 컨피그레이션을 구축하려면 FTD를 Smart Licensing Server에 등록해야 하며 유효한 Plus, Apex 또는 VPN Only 라이센스를 디바이스에 적용해야 합니다.

1. **System > Licenses > Smart Licensing으로 이동합니다**.

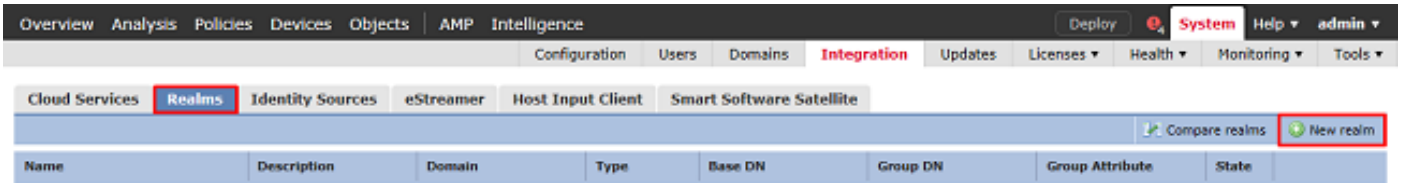
2. 장치가 규정을 준수하고 성공적으로 등록되었는지 확인합니다. 디바이스가 AnyConnect **Apex**, **Plus** 또는 **VPN 전용** 라이센스에 등록되어 **있는지 확인합니다**.



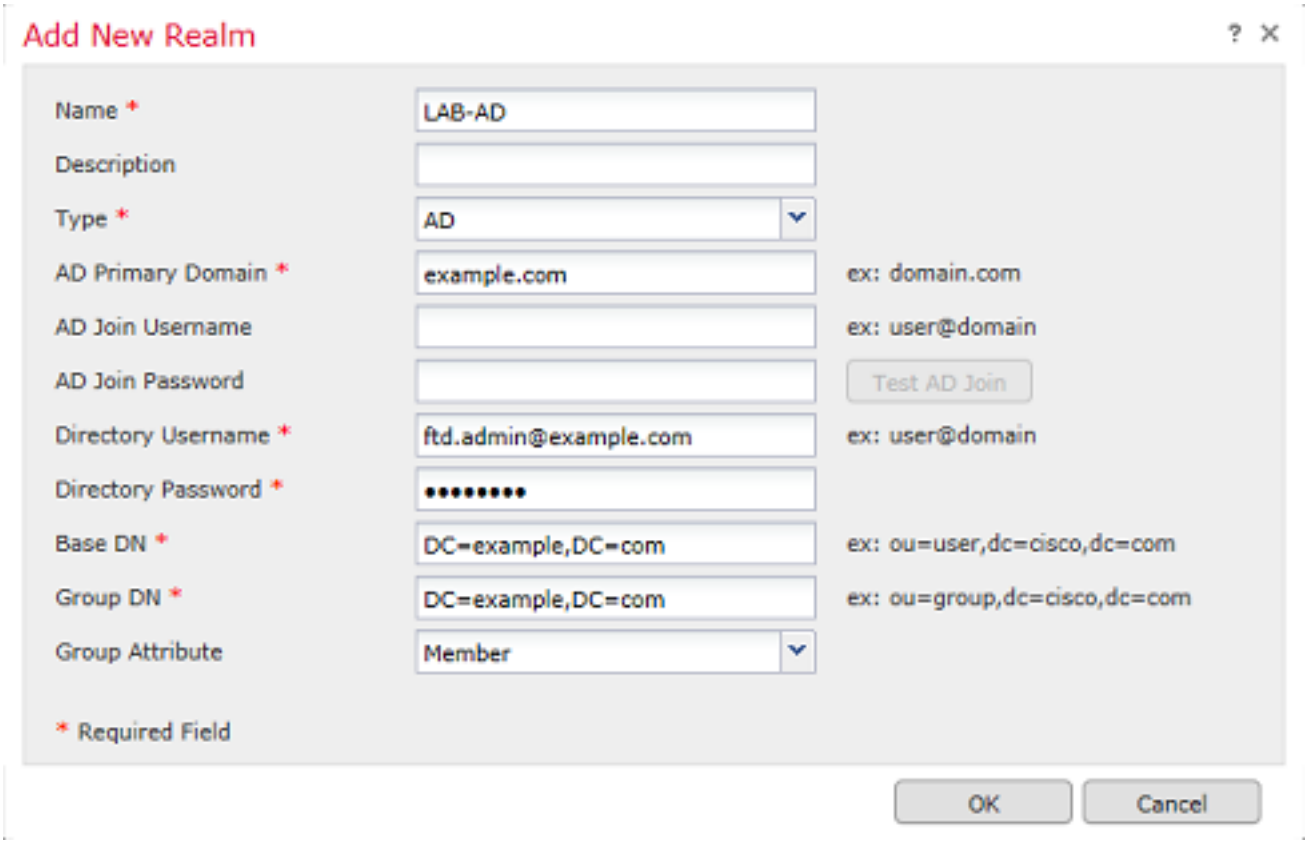
영역 설정

1. **시스템 > 통합으로 이동합니다**.

2. 영역 **아래**에서 **새** 영역을 **누릅니다**.



3. Microsoft 서버에서 수집한 정보를 바탕으로 적절한 필드를 입력합니다. 완료되면 확인을 **클릭합니다**.

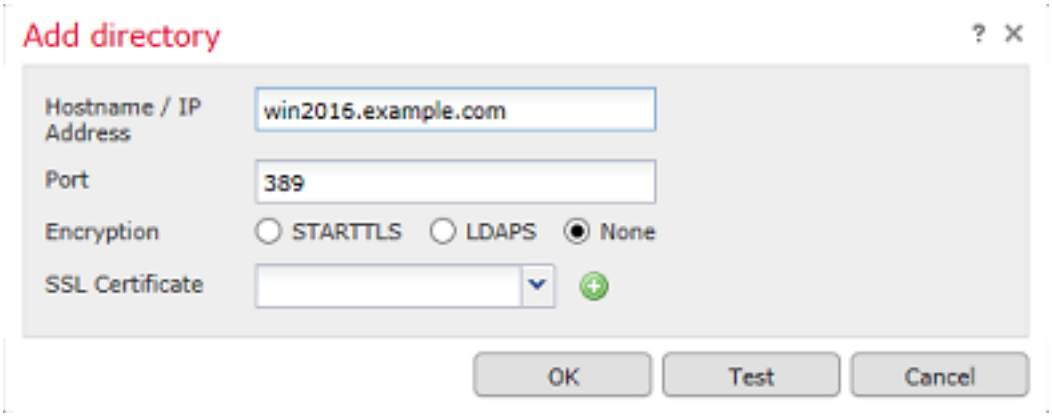


4. 신규 창에서 디렉토리를 선택하고 아직 선택하지 않은 경우 **디렉토리** 추가를 **누릅니다**.

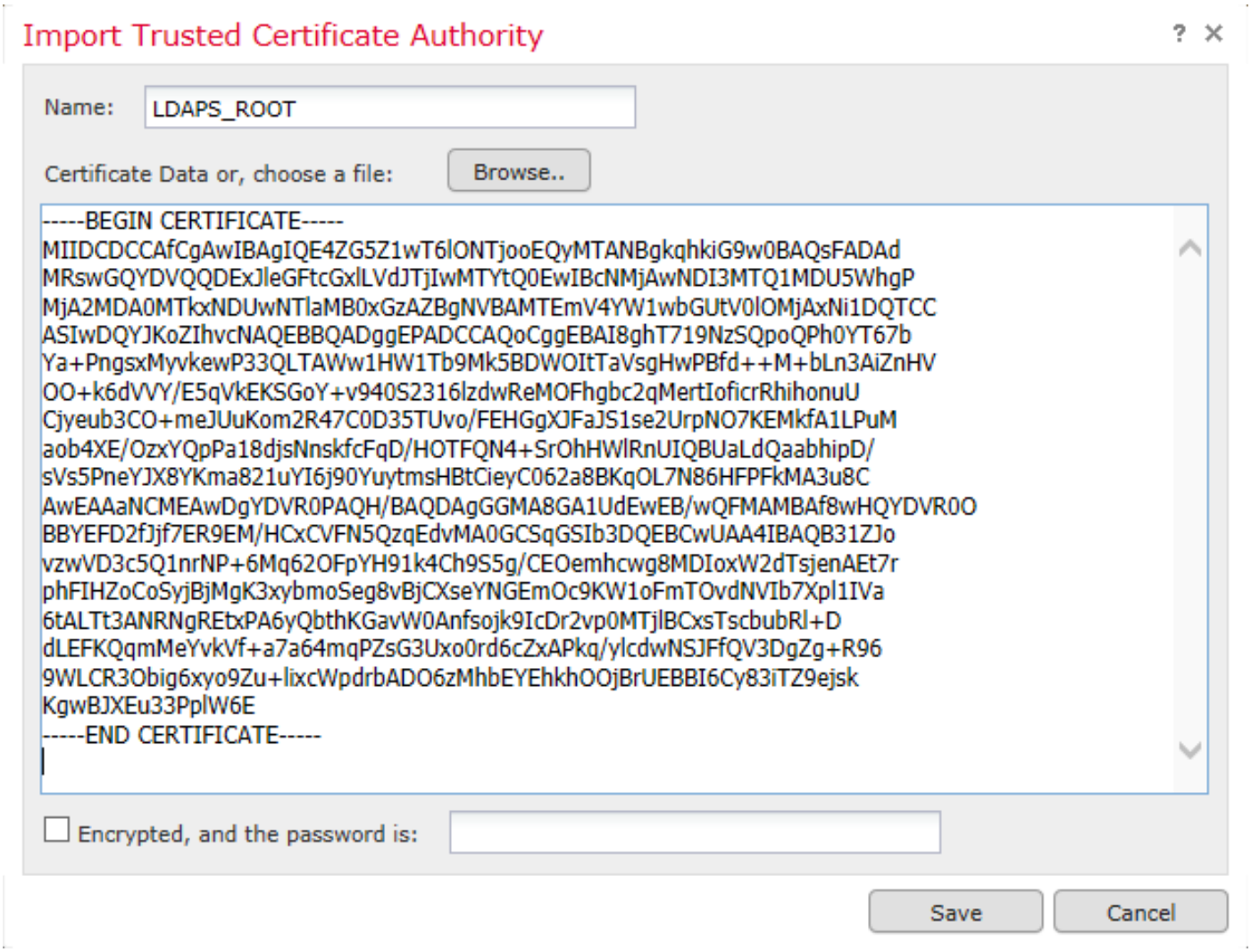
AD 서버에 대한 세부 정보를 입력합니다. FQDN을 사용하는 경우 FQDN을 확인하도록 DNS를 구성하지 않으면 FMC 및 FTD를 성공적으로 바인딩할 수 없습니다.

FMC에 대한 DNS를 설정하려면 **System > Configuration**으로 이동하고 **Management** Interfaces를 **선택합니다**.

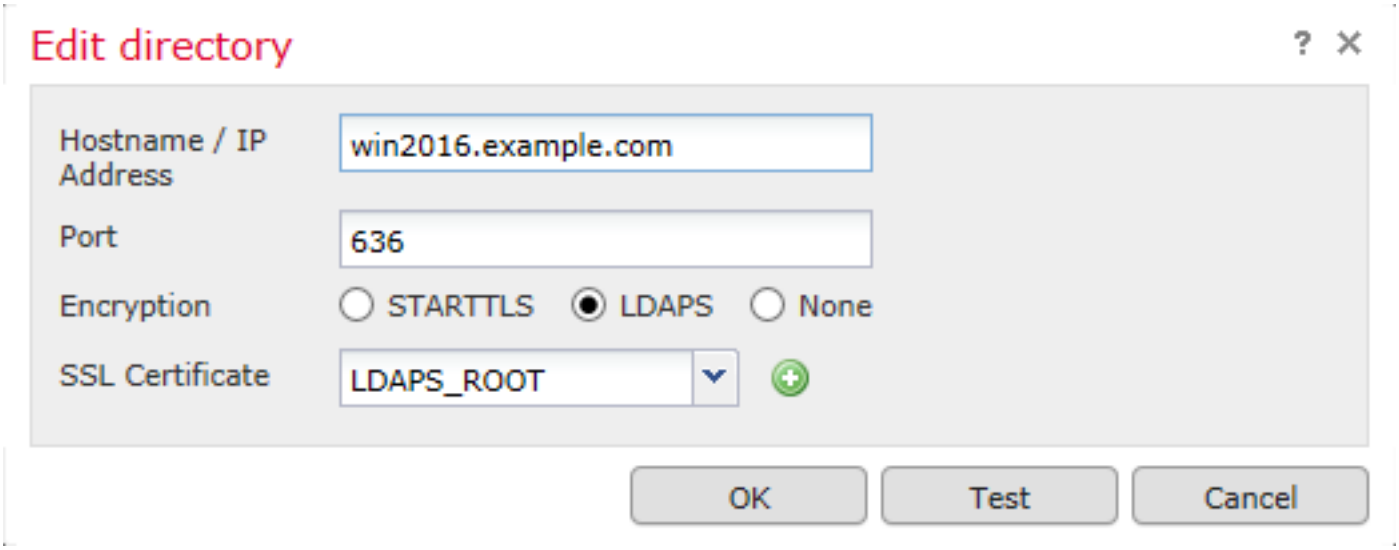
FTD에 대한 DNS를 설정하려면 **Devices(디바이스) > Platform Settings(플랫폼 설정)로** 이동하고, 새 정책을 생성하거나, 현재 정책을 수정한 다음 DNS로 이동합니다.



LDAPS 또는 STARTTLS를 사용하는 경우 녹색 **+** 기호를 클릭하고 인증서에 이름을 지정한 다음 PEM 형식의 루트 CA 인증서를 복사합니다. 완료되면 **Save**(저장)를 클릭합니다.



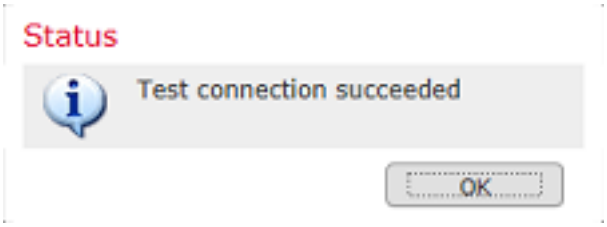
SSL Certificate(SSL 인증서) 옆의 드롭다운에서 새로 추가된 루트 CA를 선택하고 STARTTLS(STARTTLS) 또는 LDAPS를 클릭합니다.



Test(테스트)를 클릭하여 FMC가 이전 단계에서 제공한 디렉토리 사용자 이름 및 비밀번호로 성공적으로 바인딩할 수 있는지 확인합니다.

이러한 테스트는 FTD에 구성된 라우팅 가능한 인터페이스(예: 내부, 외부, dmz)를 통하지 않고 FMC에서 시작되므로, AnyConnect LDAP 인증 요청이 FTD 라우팅 가능한 인터페이스 중 하나에서 시작되므로 연결에 성공하거나 실패하더라도 AnyConnect 인증에 대한 동일한 결과가 보장되지 않습니다.

FTD에서 LDAP 연결을 테스트하는 방법에 대한 자세한 내용은 Troubleshooting(문제 해결) 영역의 Test AAA and Packet Capture(AAA 및 패킷 캡처 테스트) 섹션을 참조하십시오.



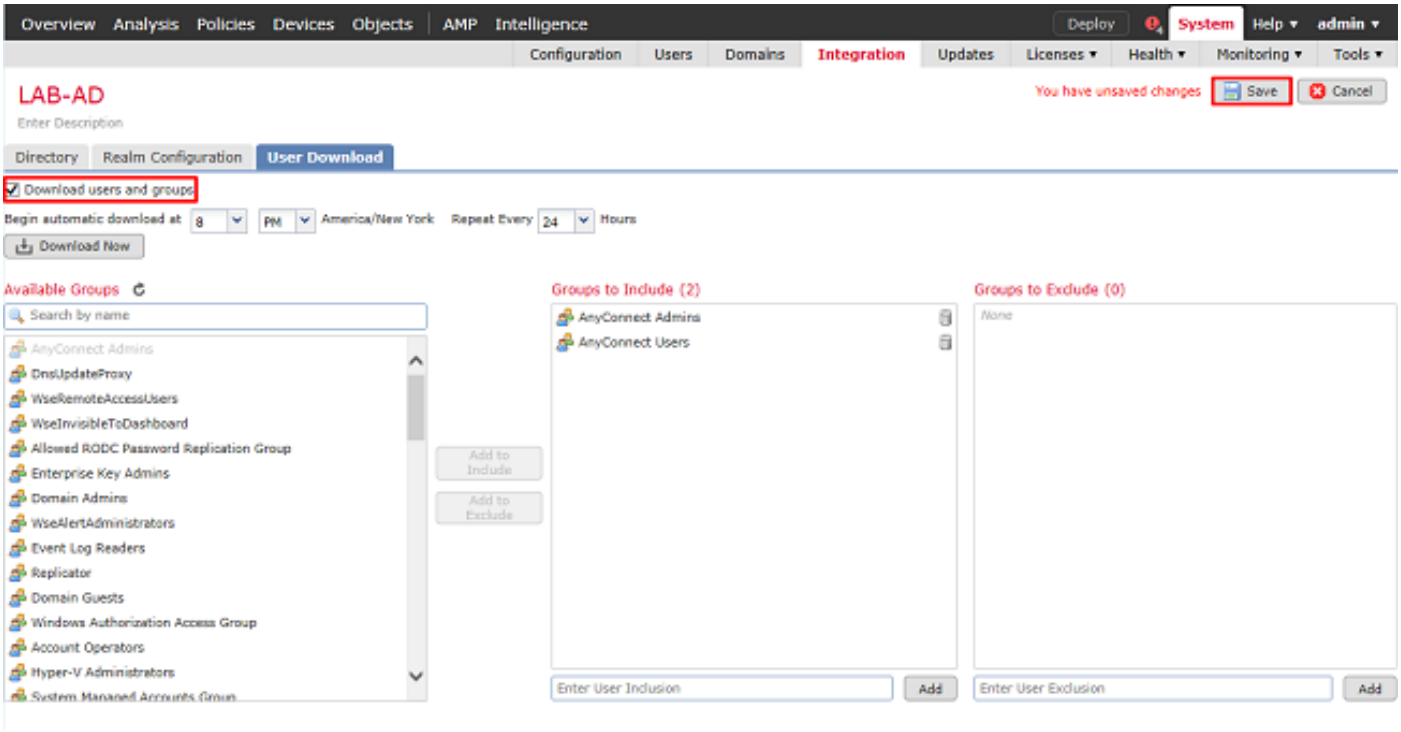
5. **User Download(사용자 다운로드)** 아래에서 이후 단계에서 사용자 ID에 사용되는 그룹을 다운로드합니다.

사용자 및 그룹 다운로드 확인란을 선택하고 **사용 가능한** 그룹의 **열이** Active Directory 내에 구성된 그룹으로 채워집니다.

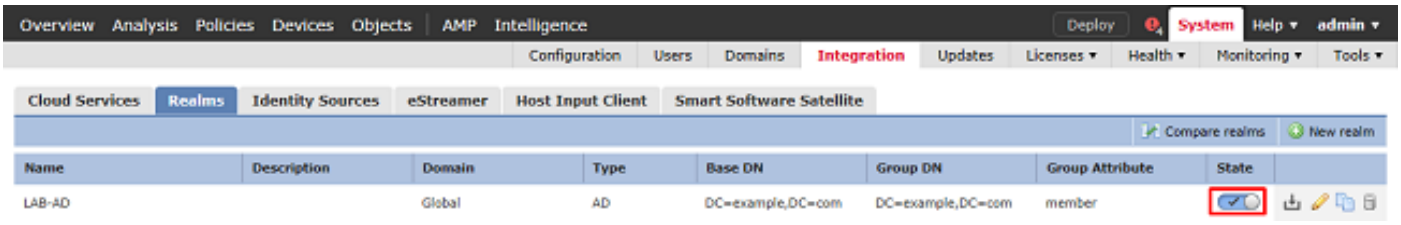
그룹은 Include(포함) 또는 Excluded(제외됨)일 수 있지만, 기본적으로 Group DN(그룹 DN) 아래에 있는 모든 그룹이 포함됩니다.

특정 사용자를 포함하거나 제외할 수도 있습니다. 포함된 모든 그룹 및 사용자를 나중에 사용자 ID에 대해 선택할 수 있습니다.

완료되면 저장을 **클릭합니다**.

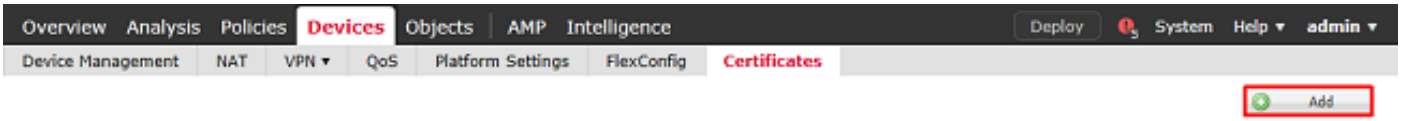


6. 새 영역을 사용으로 설정합니다.

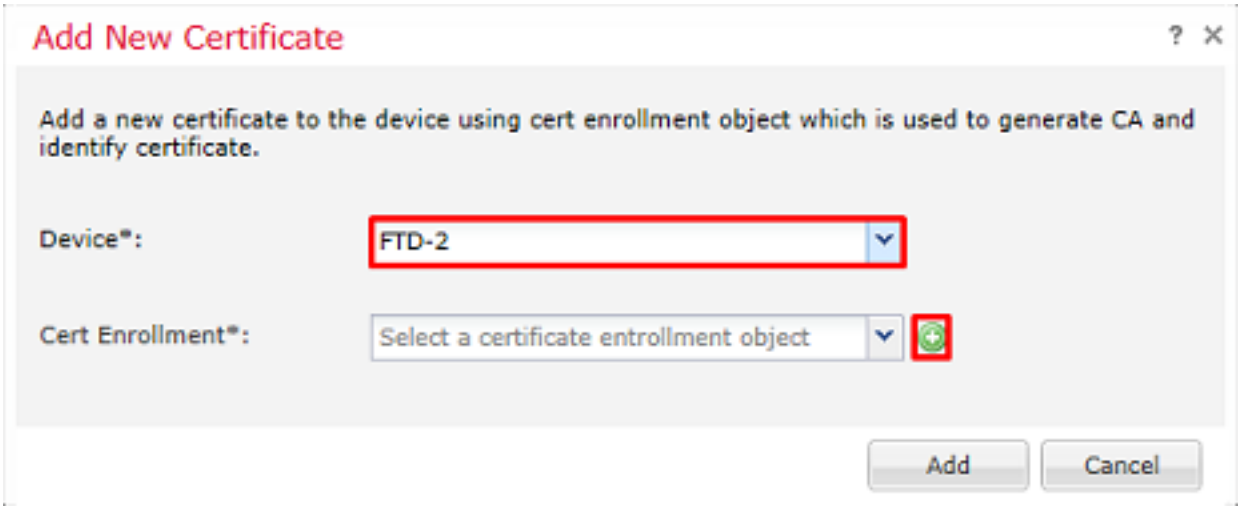


7. LDAPS 또는 STARTTLS를 사용하는 경우 FTD에서 루트 CA도 신뢰해야 합니다. 이 작업을 수행하려면 먼저 Devices(디바이스) **> Certificates(인증서)로 이동합니다**.

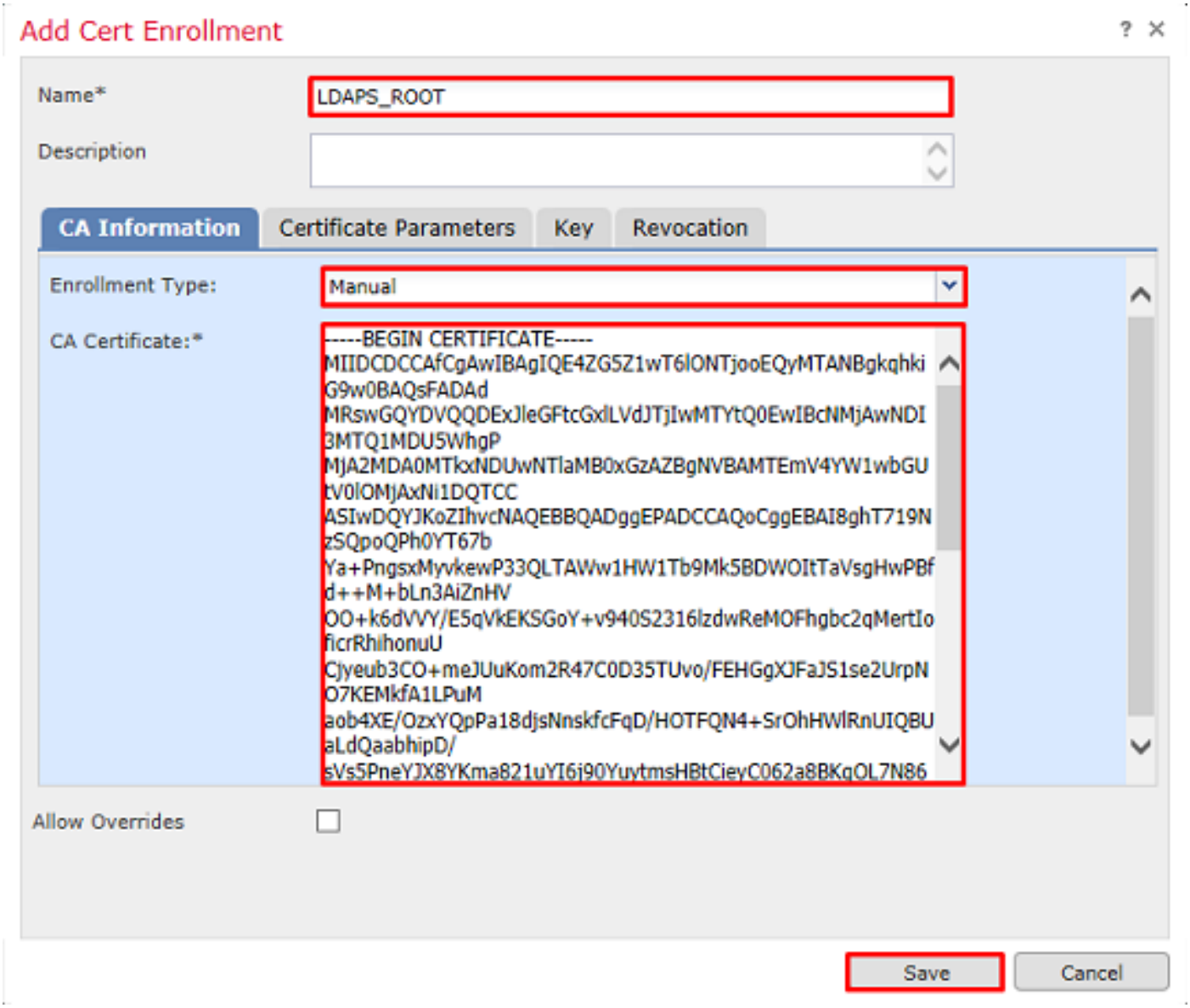
오른쪽 상단의 Add(추가)를 클릭합니다.



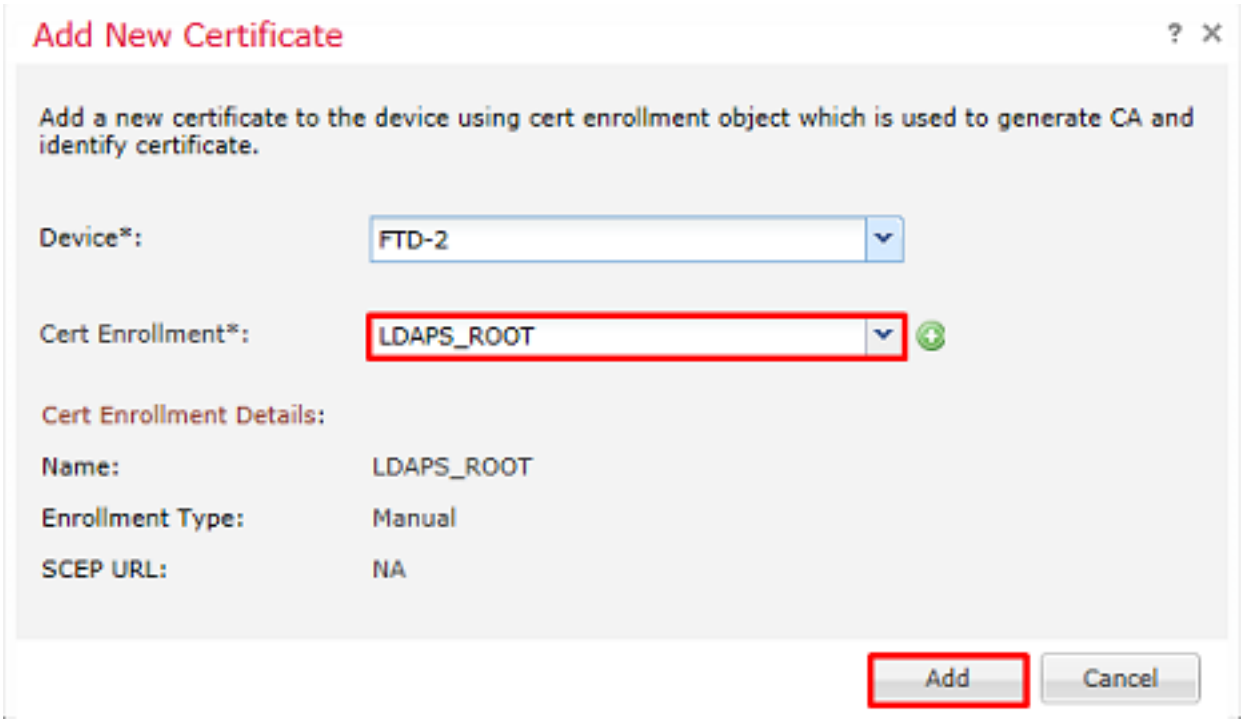
FTD를 선택하고 LDAP 컨피그레이션이 추가된 다음 녹색 + 기호를 클릭합니다.



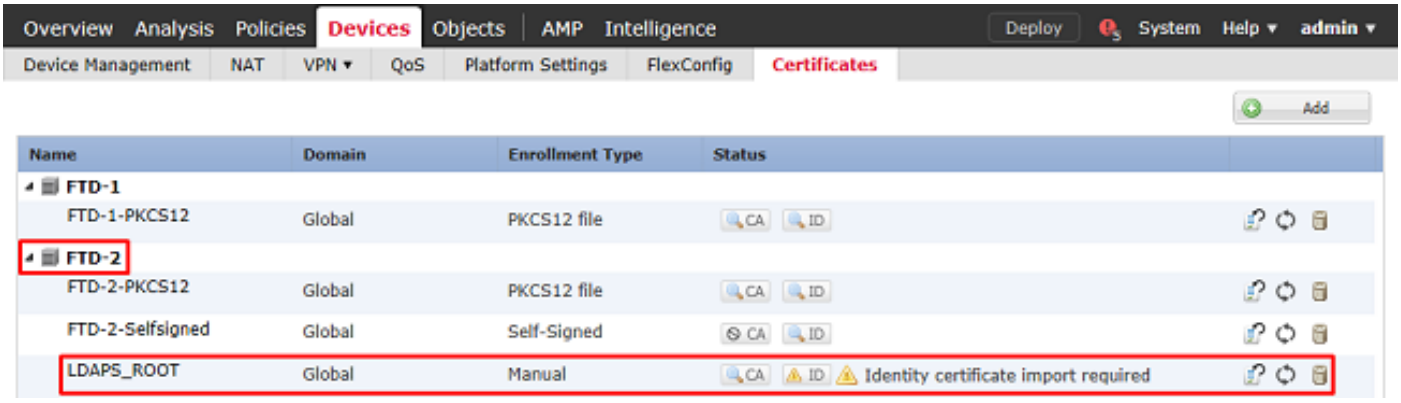
신뢰 지점에 이름을 **지정한** 다음 Enrollment Type(**등록 유형) 드롭다운**에서 Manual enrollment(수동 등록)**를** 선택합니다. 여기에 PEM 루트 ca 인증서를 붙여넣은 다음 Save를 **클릭합니다**.



생성된 신뢰 지점이 선택되었는지 확인한 후 Add(추가)**를 클릭합니다**.



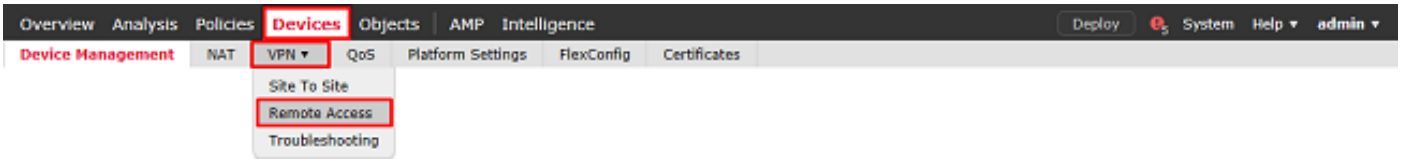
새 신뢰 지점이 FTD 아래에 나타납니다. ID 인증서 가져오기가 필요하다고 언급하지만 LDAPS 서버에서 보낸 SSL 인증서를 FTD에서 인증할 필요가 없으므로 이 메시지를 무시할 수 있습니다.



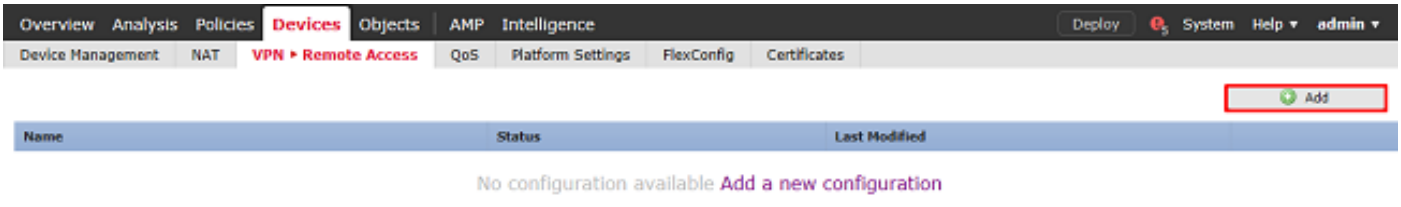
AD 인증을 위해 AnyConnect 구성

1. 이 단계에서는 원격 액세스 vpn 정책이 아직 생성되지 않았다고 가정합니다. 정책을 생성한 경우 해당 정책의 수정 버튼을 클릭하고 3단계로 건너뜁니다.

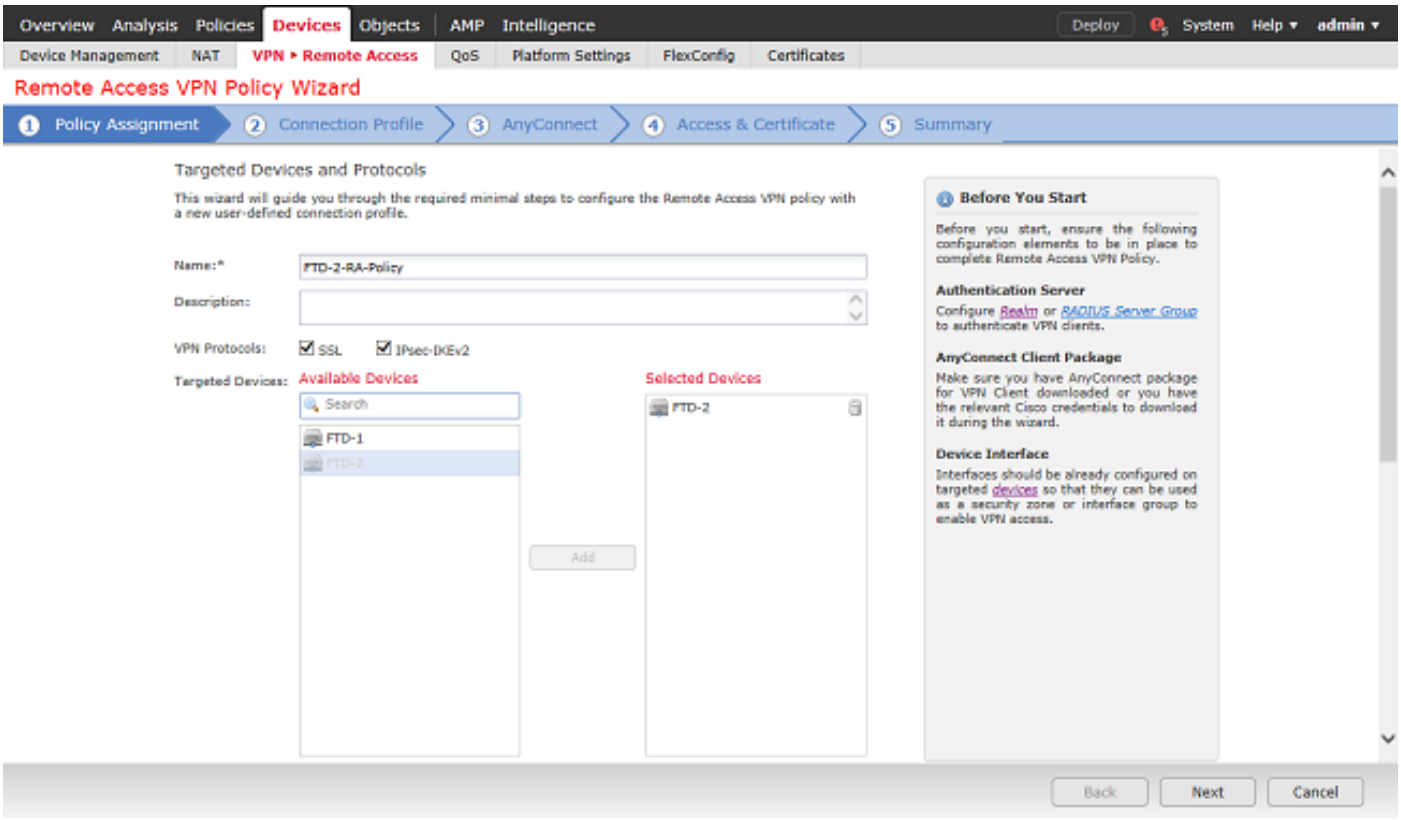
Devices(**디바이스**) > VPN > Remote Access(**원격 액세스**)로 이동합니다.



Add(**추가**)를 클릭하여 새 원격 액세스 VPN 정책을 생성합니다



2. **원격 액세스 VPN 정책 마법사를 완료합니다**. Policy **Assignment**(정책 할당)에서 정책 및 정책이 적용되는 디바이스의 이름을 지정합니다.

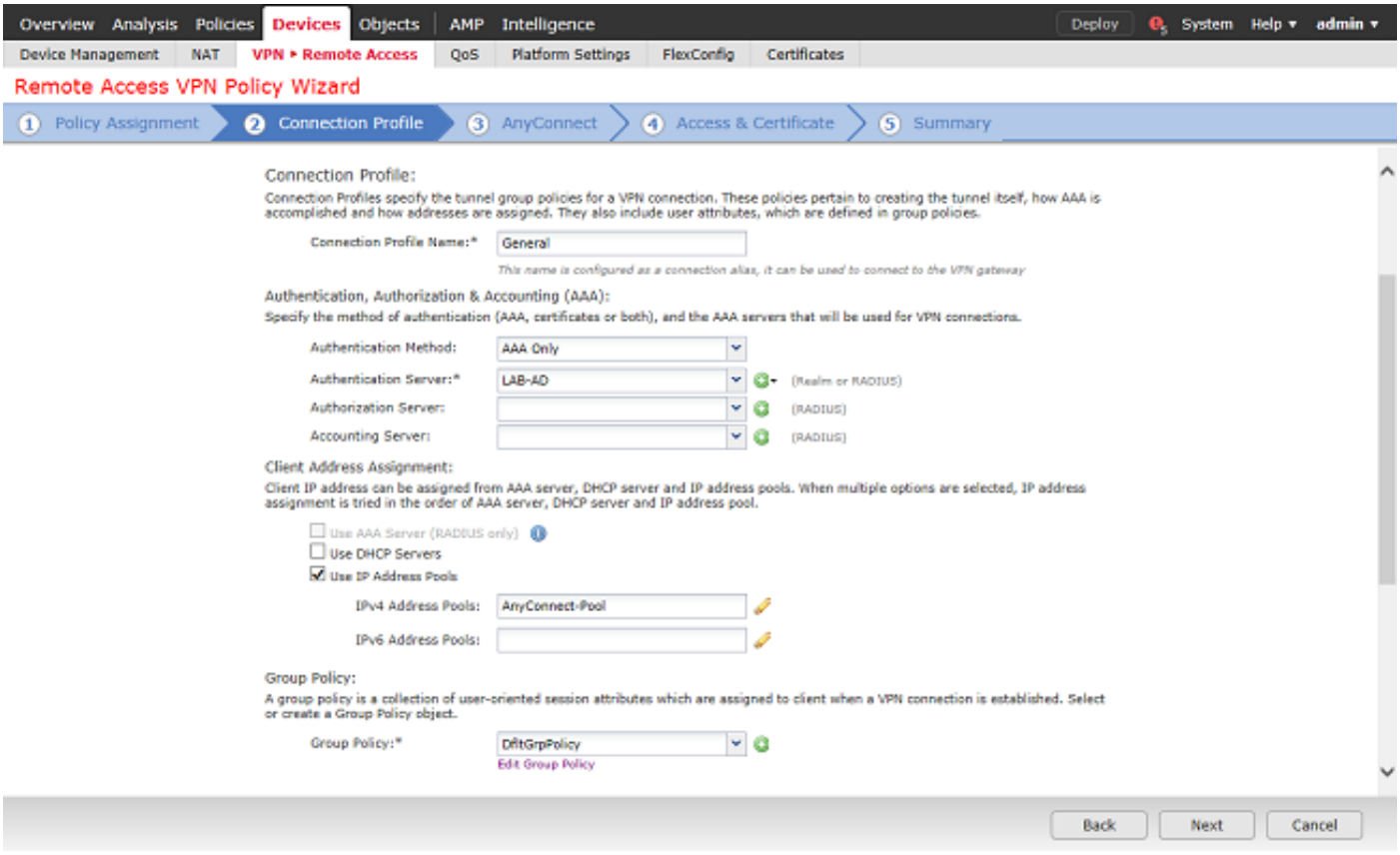


Connection **Profile(연결 프로파일)**에서 AnyConnect 사용자가 **연결될** 때 표시되는 그룹 별칭으로도 사용되는 연결 프로파일의 이름을 지정합니다.

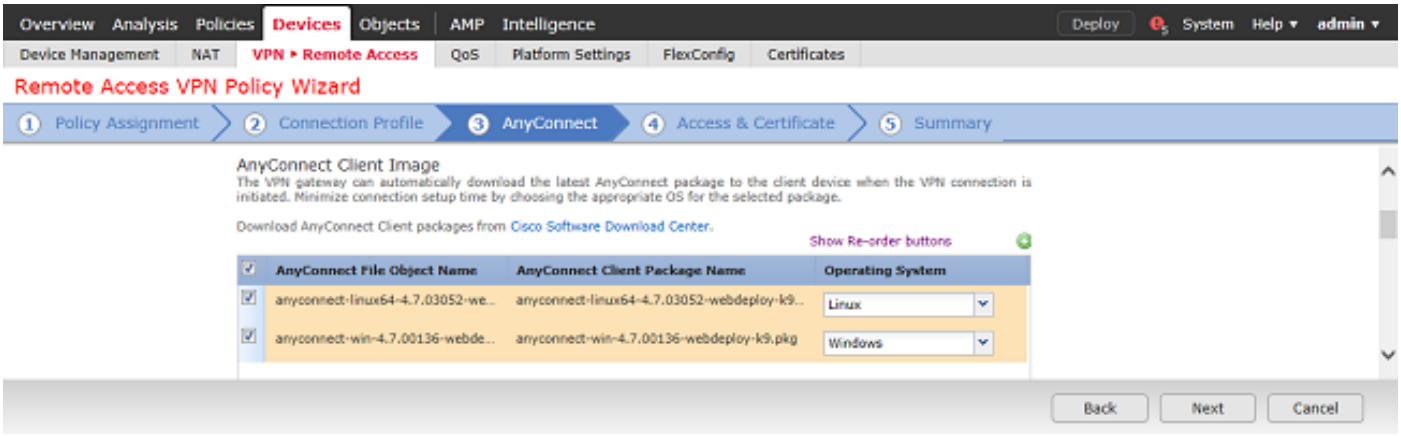
인증 서버에서 이전에 생성한 영역**을 지정합니다**.

AnyConnect 클라이언트에 IP 주소를 할당하는 방법을 지정합니다.

이 연결 프로파일에 사용되는 기본 그룹 정책을 지정합니다.



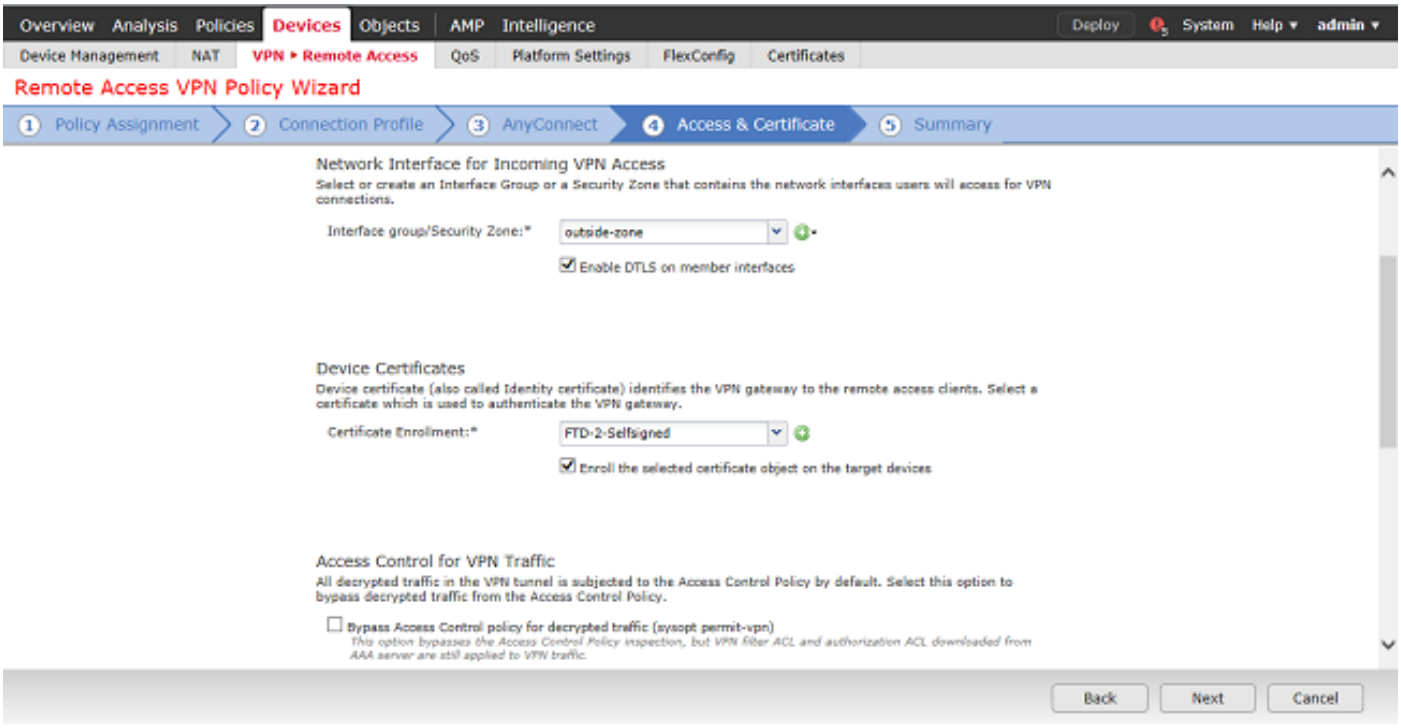
AnyConnect에서 사용되는 AnyConnect 패키지를 업로드하고 지정합니다.



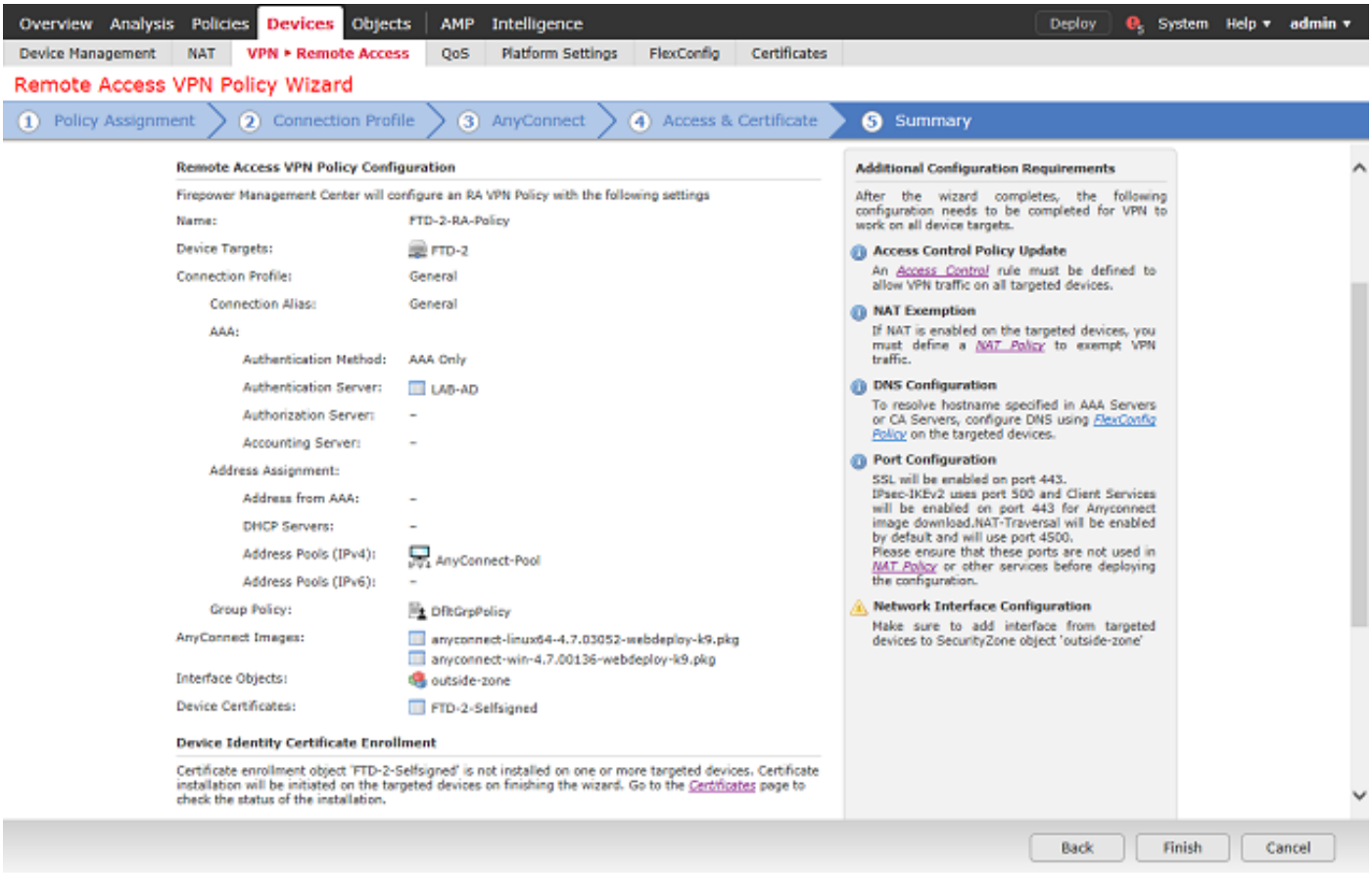
Access **& Certificate(액세스 및 인증서)**에서 AnyConnect 사용자가 AnyConnect에 액세스할 인터페이스를 지정합니다.

SSL 핸드셰이크 중에 FTD에서 사용하는 인증서를 만들거나 지정합니다.

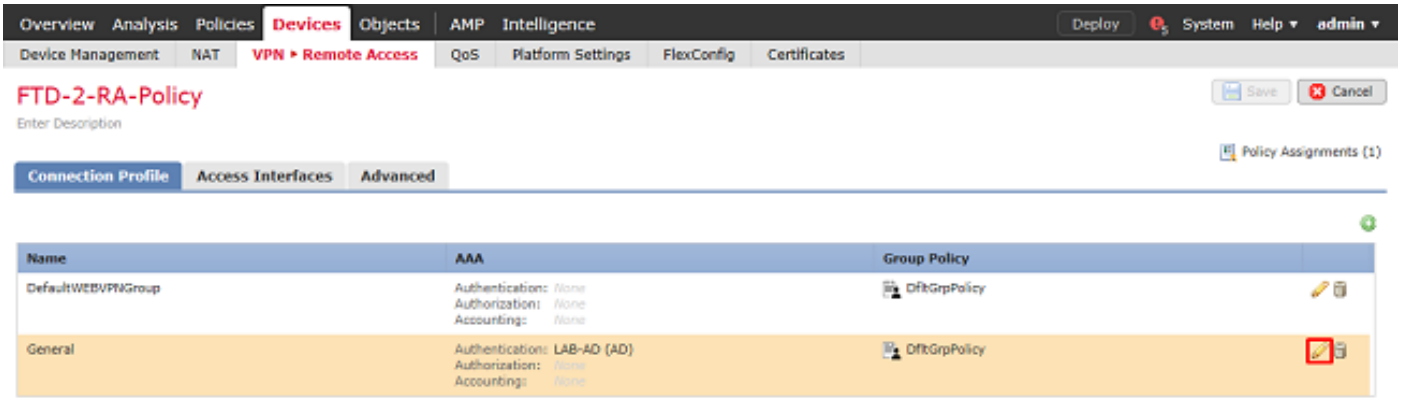
암호 해독된 트래픽에 대한 **액세스 제어 정책 우회**(sysopt permit-vpn) 확인란이 선택되지 않은 상태로 유지되어 나중에 생성된 사용자 ID가 RAVPN 연결에 적용되는지 확인합니다.



Summary(**요약**)에서 컨피그레이션을 검토하고 Finish(마침)를 **클릭합니다**.



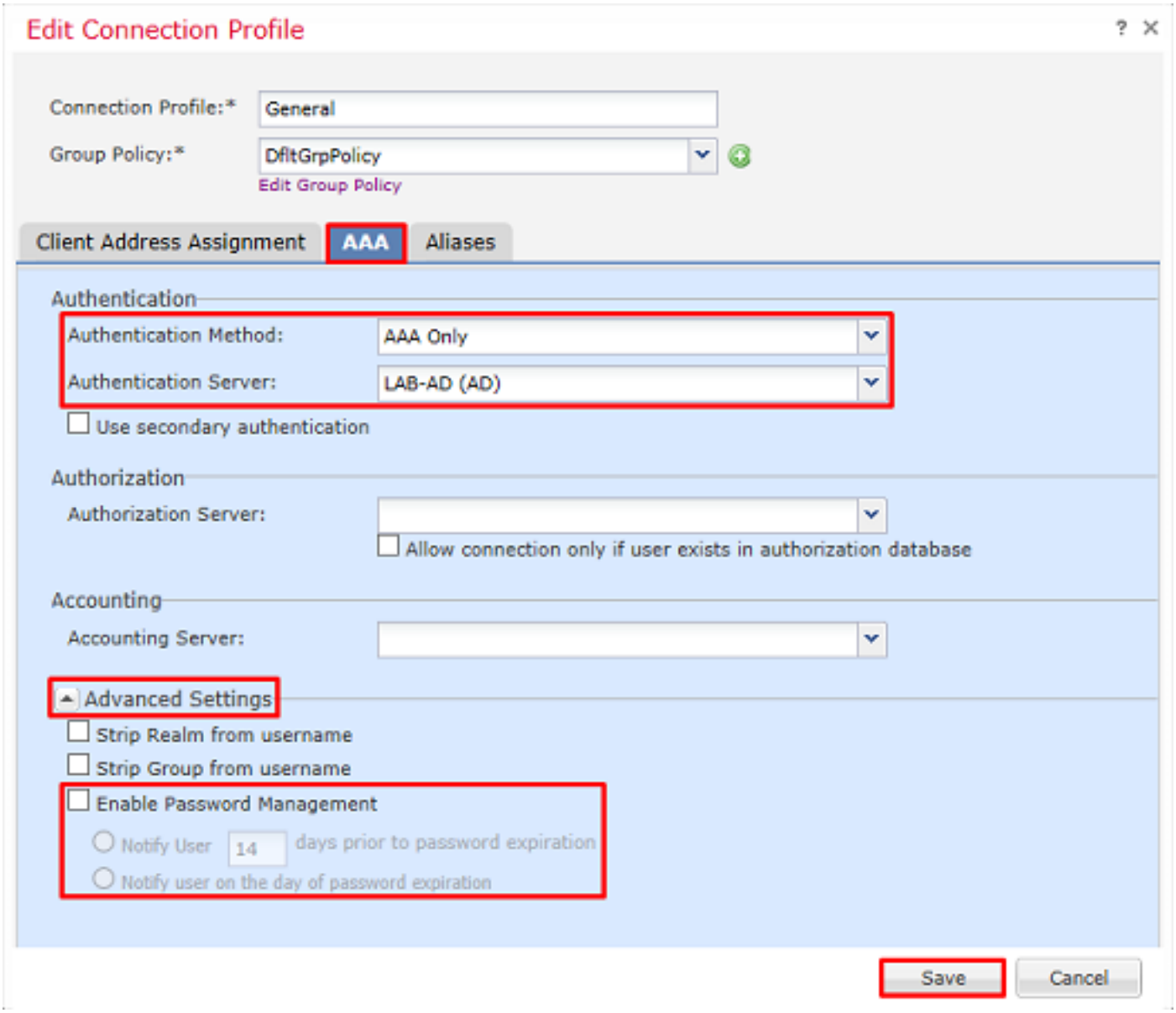
3. **Remote Access VPN Policy(원격 액세스 VPN 정책)** 아래에서 **edit**(수정)를 클릭하여 알맞은 **연결** 프로필을 **선택합니다**.



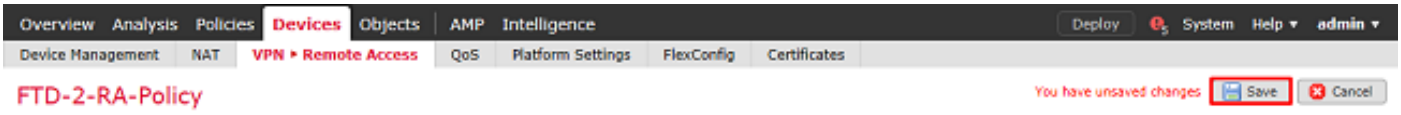
인증 서버가 이전에 생성한 영역으로 설정되어 있는지 확인합니다.

고급 설정에서 **비밀번호 관리** 사용을 선택하여 비밀번호가 만료되기 전에 사용자가 비밀번호를 변경할 수 있도록 할 수 있습니다.

그러나 이 설정에서는 영역이 LDAPS를 사용해야 합니다. 변경 사항이 있으면 저장을 **클릭합니다**.



완료되면 오른쪽 상단에서 **Save(저장)**를 클릭합니다.

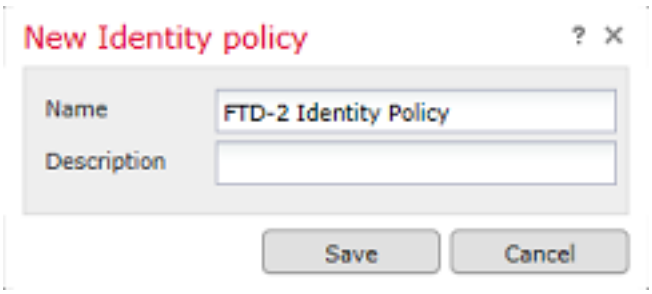


ID 정책 활성화 및 사용자 ID에 대한 보안 정책 구성

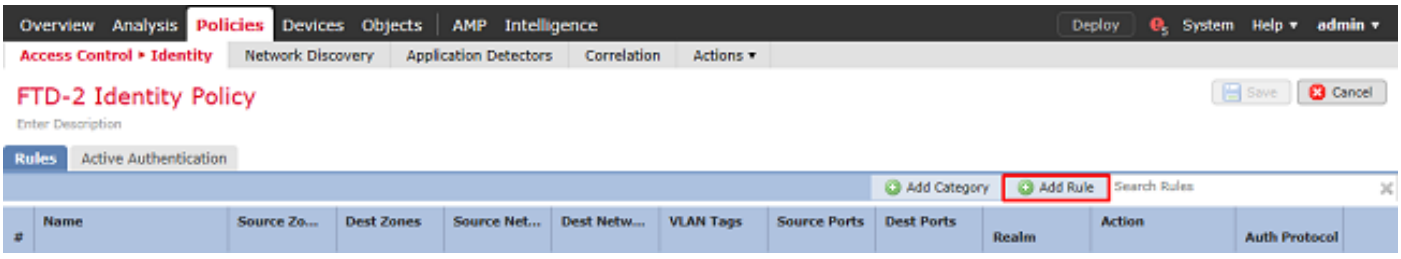
1. Policies(정책) > Access Control(액세스 제어) > Identity(ID)로 이동합니다.

새 ID 정책을 만듭니다.

새 ID **정책**의 이름을 **지정합니다**.



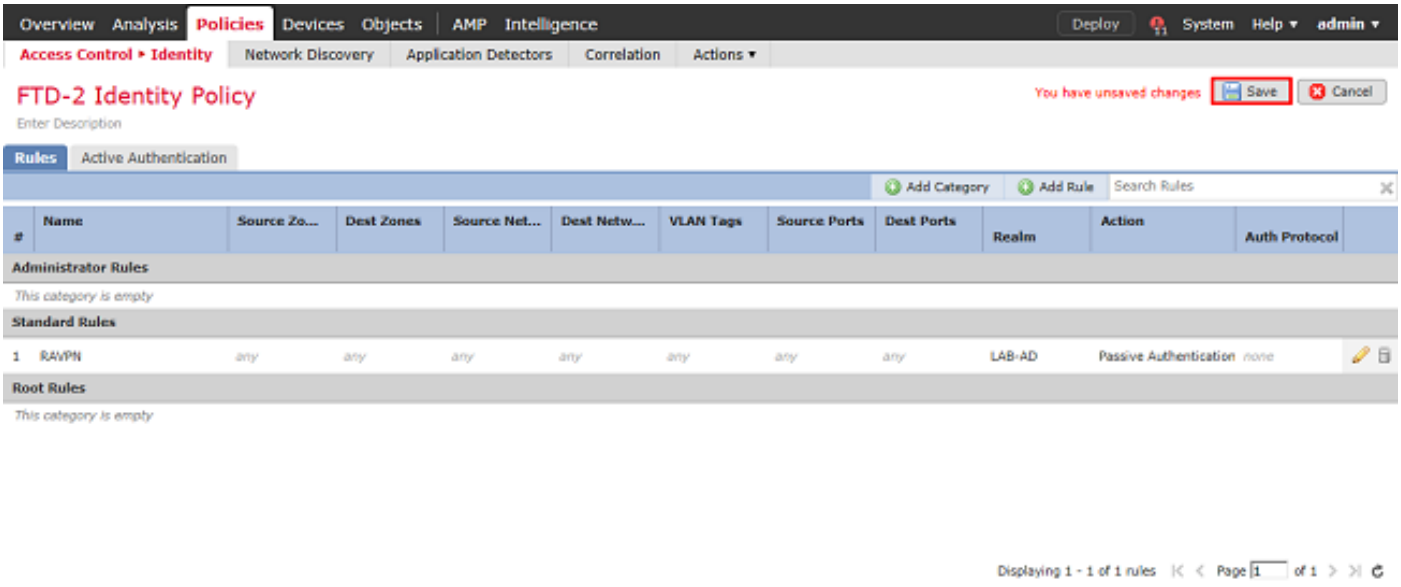
2. **규칙** 추가**를 클릭합니다**.



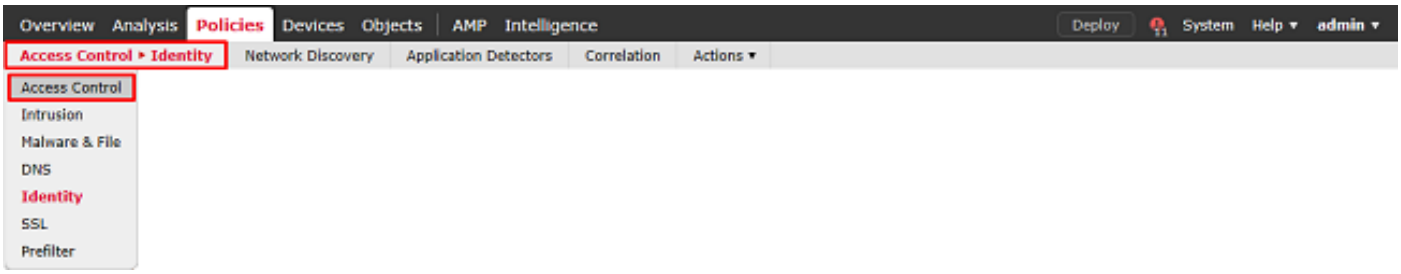
3. 새 **규칙**의 이름을 지정합니다. 활성화되었고 작업이 수동 인증으로 설정되어 있는지 확인합니다.

Realm & Settings(영역 및 설정) 탭을 클릭하고 이전에 생성한 영역을 선택합니다. 완료되면 **Add**(추가)를 클릭합니다.

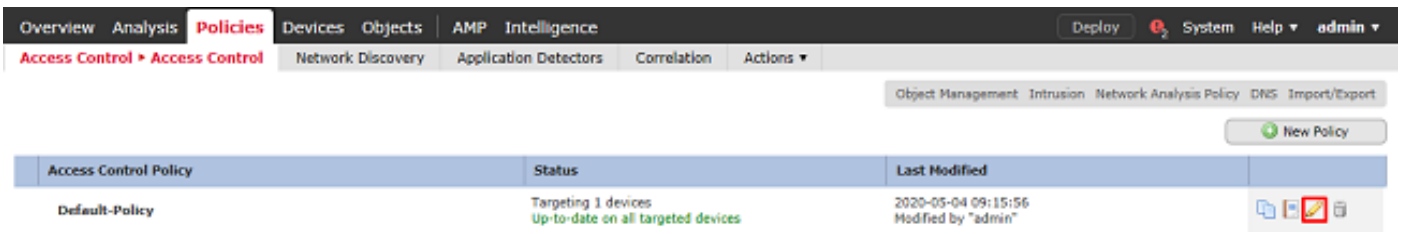
4. 저장을 **클릭합니다**.



5. **정책 > 액세스 제어 > 액세스 제어로 이동합니다**.

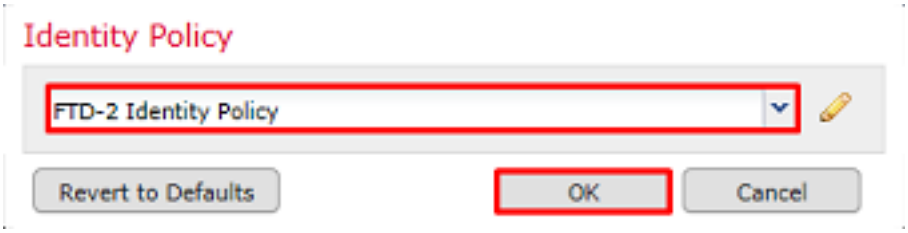


6. FTD가 구성된 **액세스 제어** 정책을 편집합니다.

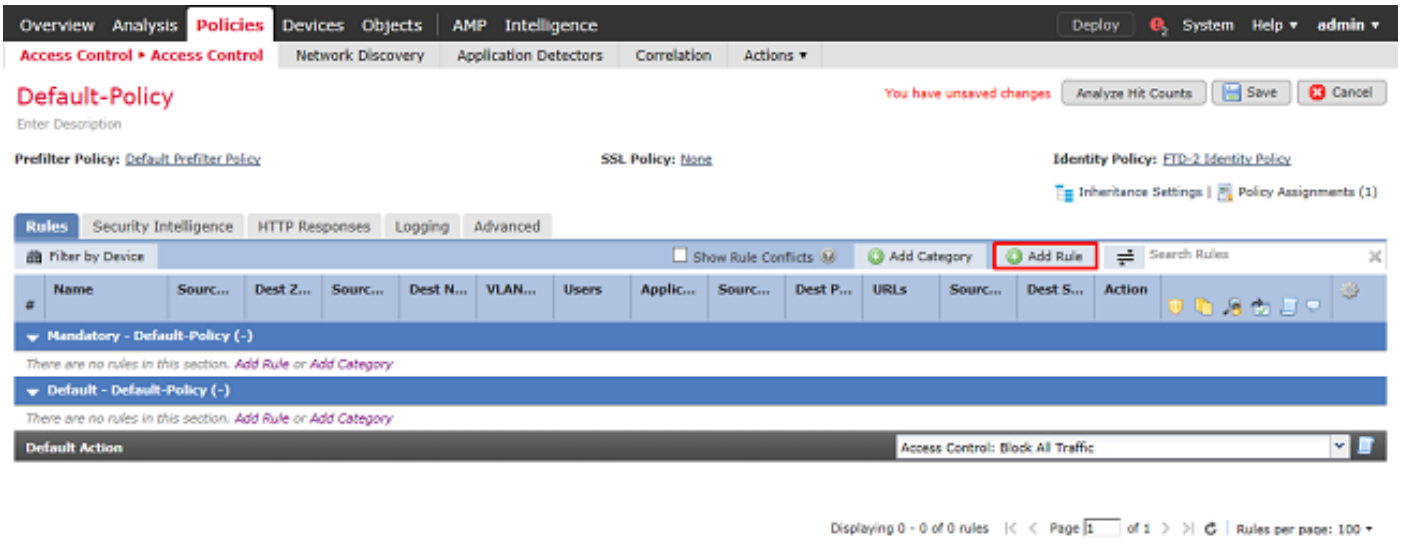


7. ID **정책** 옆의 값을 **클릭합니다.**

앞서 생성한 **ID 정책**을 선택한 다음 **OK(확인)**를 클릭합니다.



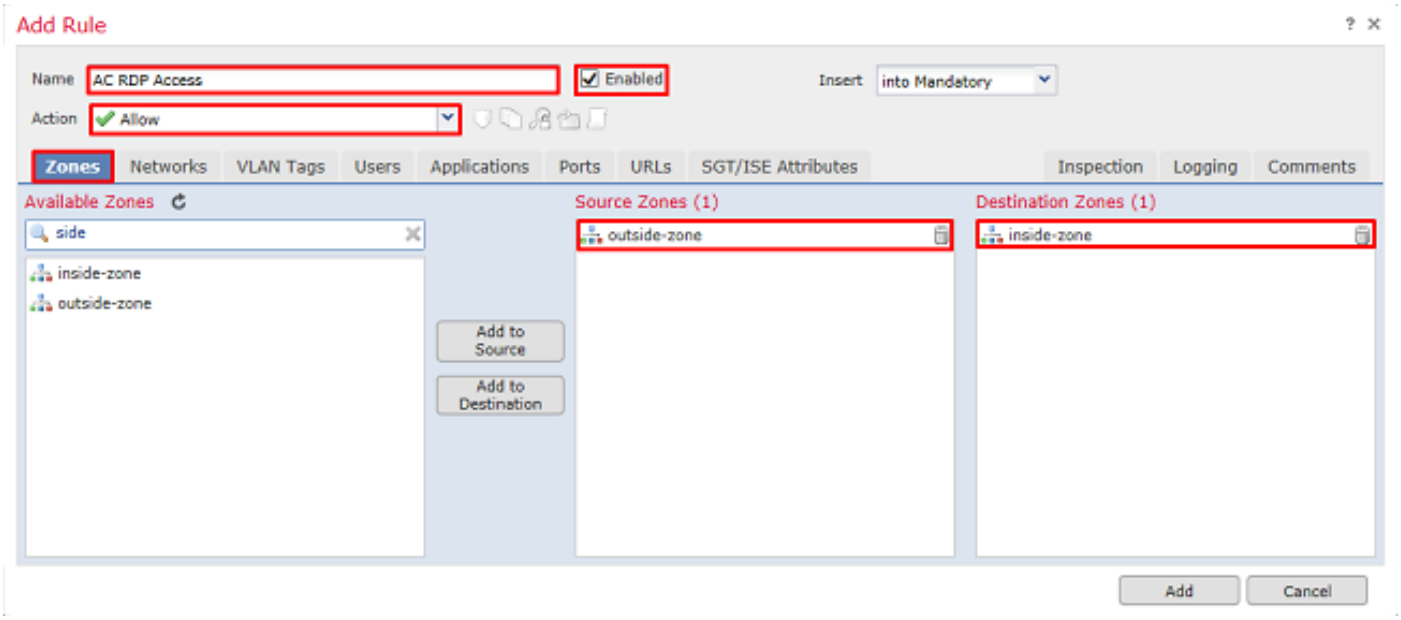
8. 새 **ACP 규칙**을 생성하려면 규칙 추가를 누릅니다. 이러한 단계에서는 AnyConnect Admins 그룹 내의 사용자가 RDP를 사용하여 내부 네트워크 내의 장치에 연결할 수 있도록 허용하는 규칙을 만듭니다.



규칙의 Name을 지정합니다. 규칙이 활성화되어 있고 적절한 Action이 있는지 확인합니다.

Zones(**영역**) 탭에서 관심 트래픽에 적합한 영역을 지정합니다.

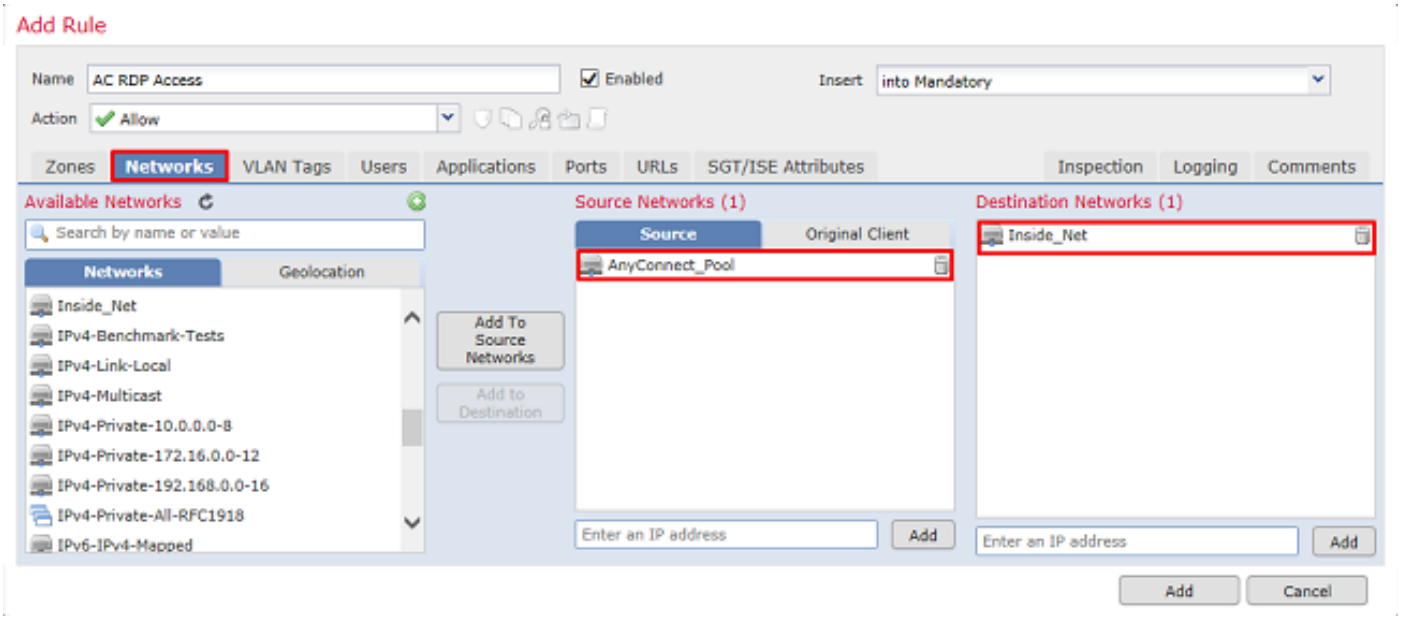
사용자가 시작한 RDP 트래픽은 외부 영역 인터페이스에서 제공된 FTD로 유입되어 내부 영역으로 이그레스(egress)됩니다.



Networks(**네트워크**)에서 소스 및 목적지 네트워크를 정의합니다.

개체 AnyConnect_Pool에는 AnyConnect 클라이언트에 할당된 IP 주소가 포함됩니다.

Object Inside_Net에는 내부 네트워크 서브넷이 포함됩니다.

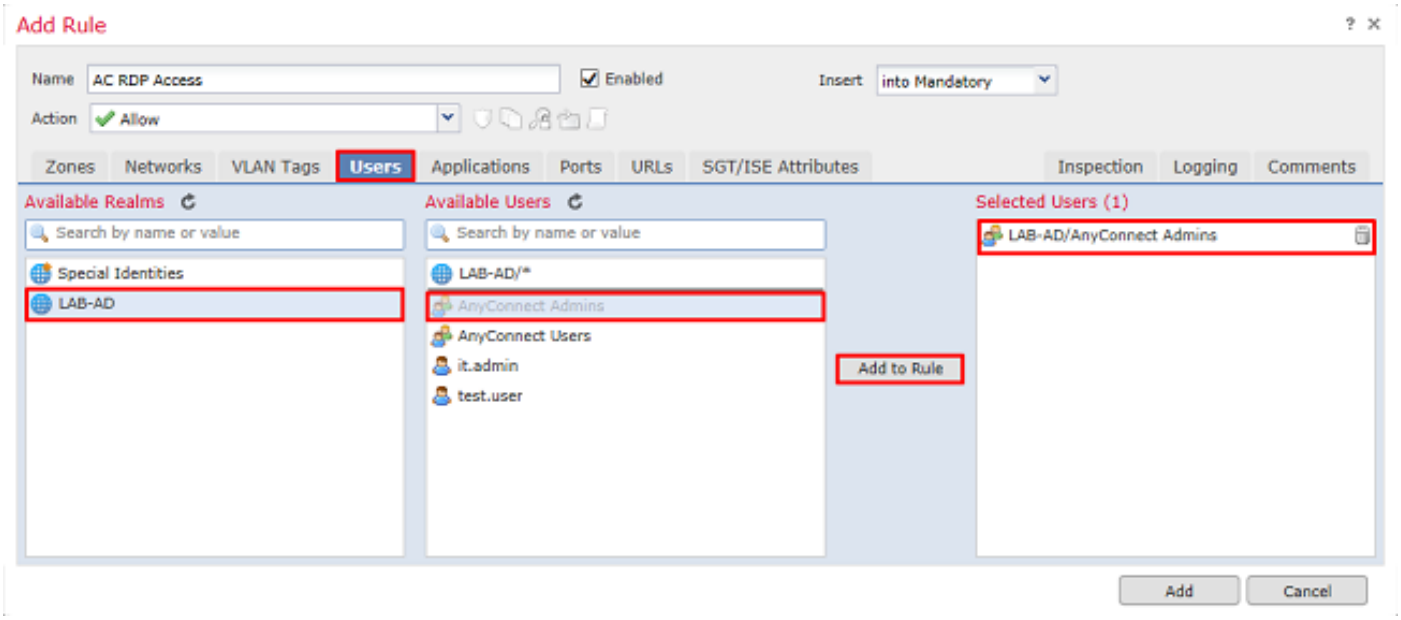


Users(**사용자**)의 Available Realms(사용 가능한 **영역**) 아래에서 이전에 생성한 영역을 클릭하고 Available Users(**사용 가능한 사용자**)에서 적절한 그룹/사용자를 클릭한 다음 Add to Rule(규칙에 **추가**)**을 클릭합니다**.

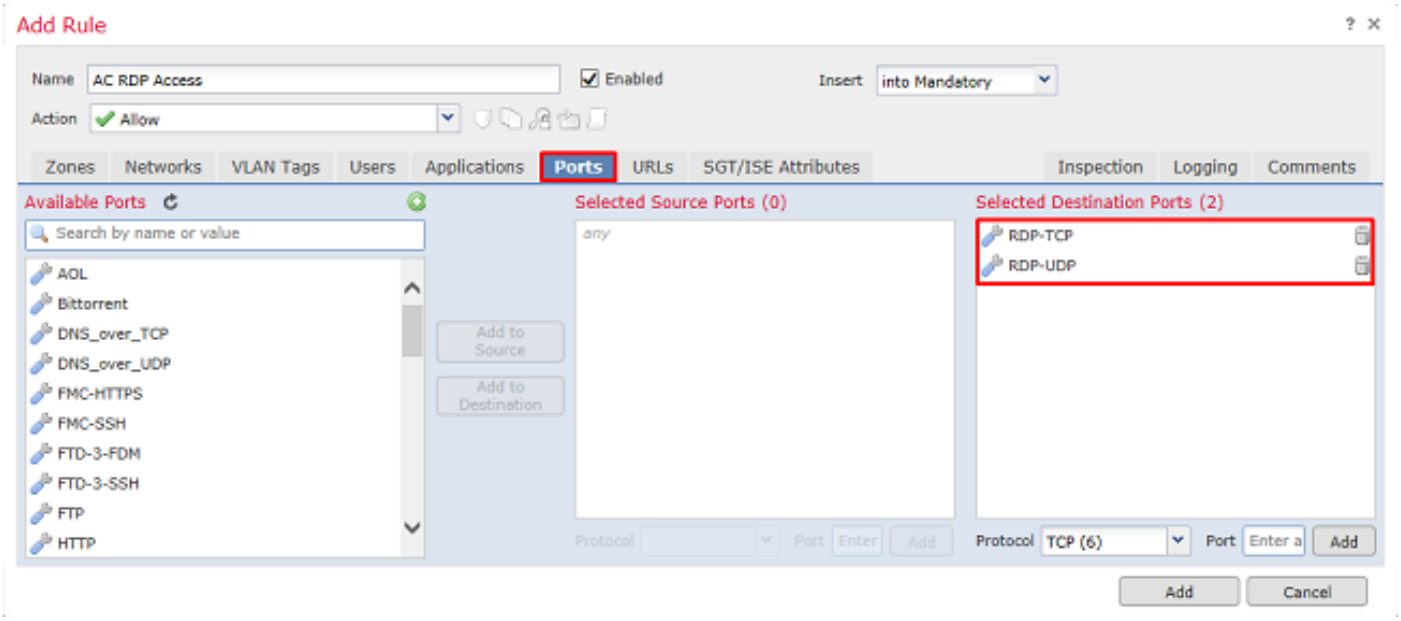
Available Users 섹션 아래에서 사용 가능한 사용자 또는 그룹이 없는 경우, FMC가 영역 섹션 아래에서 **Users** 및 **Groups**를 다운로드할 수 있는지, 그리고 적절한 **Groups/User가** 포함되어 있는지 확인하십시오.

여기에 지정된 **사용자/**그룹이 소스 관점에서 선택됩니다.

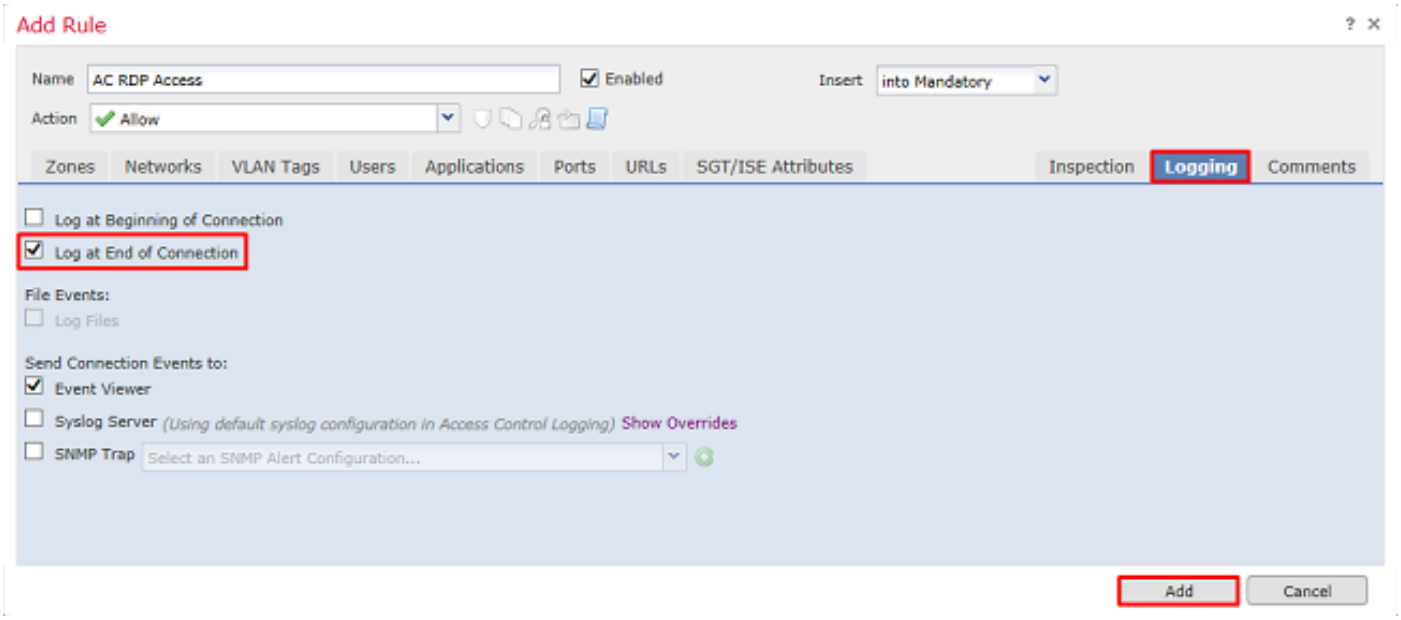
예를 들어, 지금까지 이 규칙에 정의된 대로 FTD는 트래픽이 외부 영역에서 시작되어 내부 영역으로 향하고, AnyConnect_Pools 개체의 네트워크에서 시작되어 Inside_Net 개체의 네트워크로 향하며, AnyConnect Admins 그룹의 사용자로부터 시작되었다고 평가합니다.



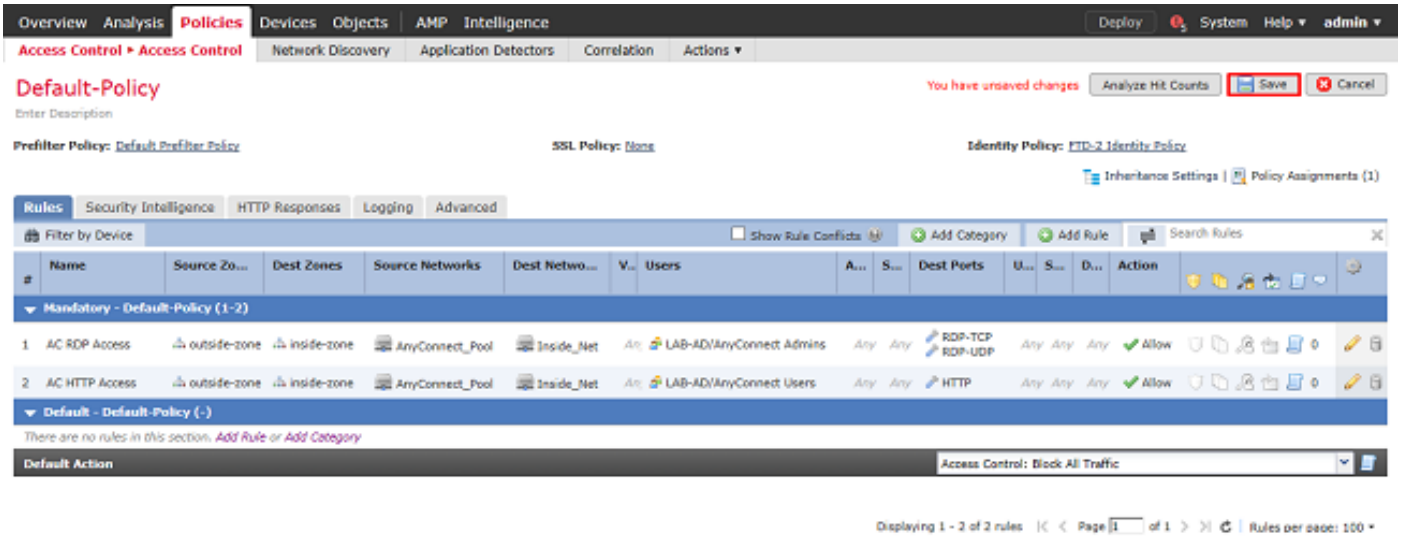
Ports(포트)에서 TCP 및 UDP 포트 3389를 허용하기 위해 사용자 지정 RDP 객체가 생성 및 추가되었습니다. RDP는 Applications(애플리케이션) 섹션에 **추가되었을** 수 있지만, 간소화를 위해 포트만 확인합니다.



마지막으로 Logging(**로깅**)에서 **Log at End of Connection(연결 종료 시** 로깅)을 선택하면 나중에 추가 확인이 이루어집니다. 완료되면 **Add**(추가)를 클릭합니다.



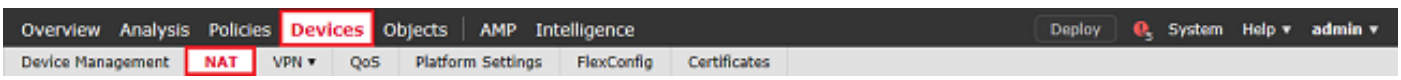
9. 그룹 AnyConnect 사용자 내의 사용자가 **Windows Server** IIS 웹 사이트에 액세스할 수 있도록 HTTP **액세스**에 대한 추가 **규칙이** 생성됩니다. 저장을 **클릭합니다**.



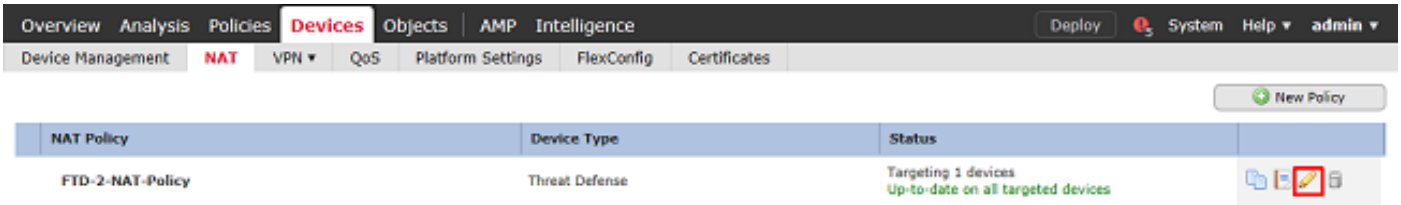
NAT 예외 구성

인터넷 PAT 규칙과 같이 AnyConnect 트래픽에 영향을 주는 NAT 규칙이 있는 경우, AnyConnect 트래픽이 NAT에 영향을 받지 않도록 NAT 예외 규칙을 구성하는 것이 중요합니다.

1. Devices(디바이스) **> NAT로 이동합니다**.

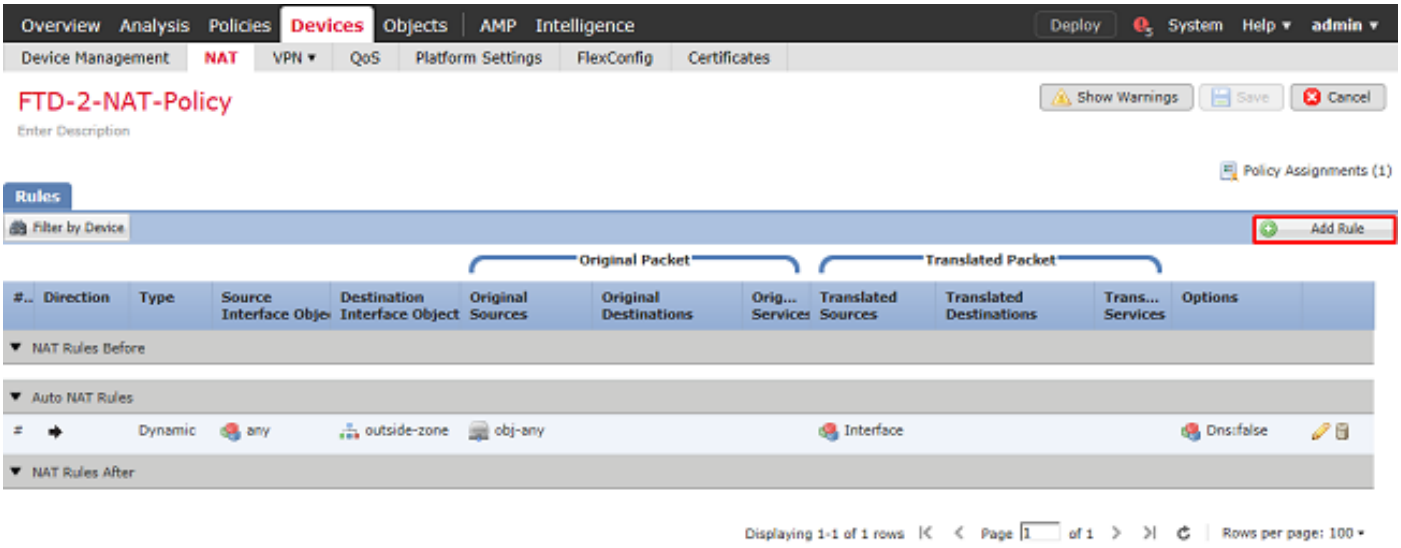


FTD에 적용되는 NAT 정책을 선택합니다.



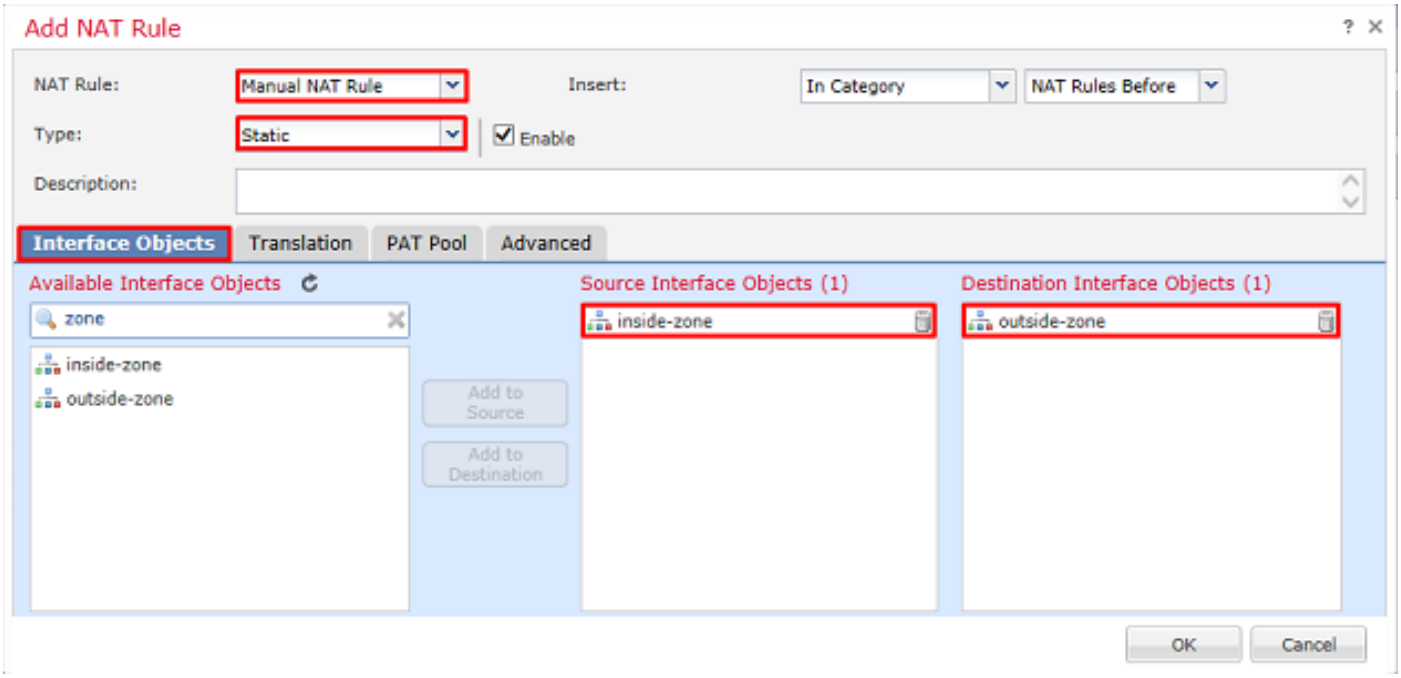
2. 이 NAT 정책에는 외부 인터페이스를 외부 인터페이스로 이그레스(egress)하는 모든 트래픽(AnyConnect 트래픽 포함)에 PAT가 영향을 주는 동적 PAT가 마지막에 있습니다.

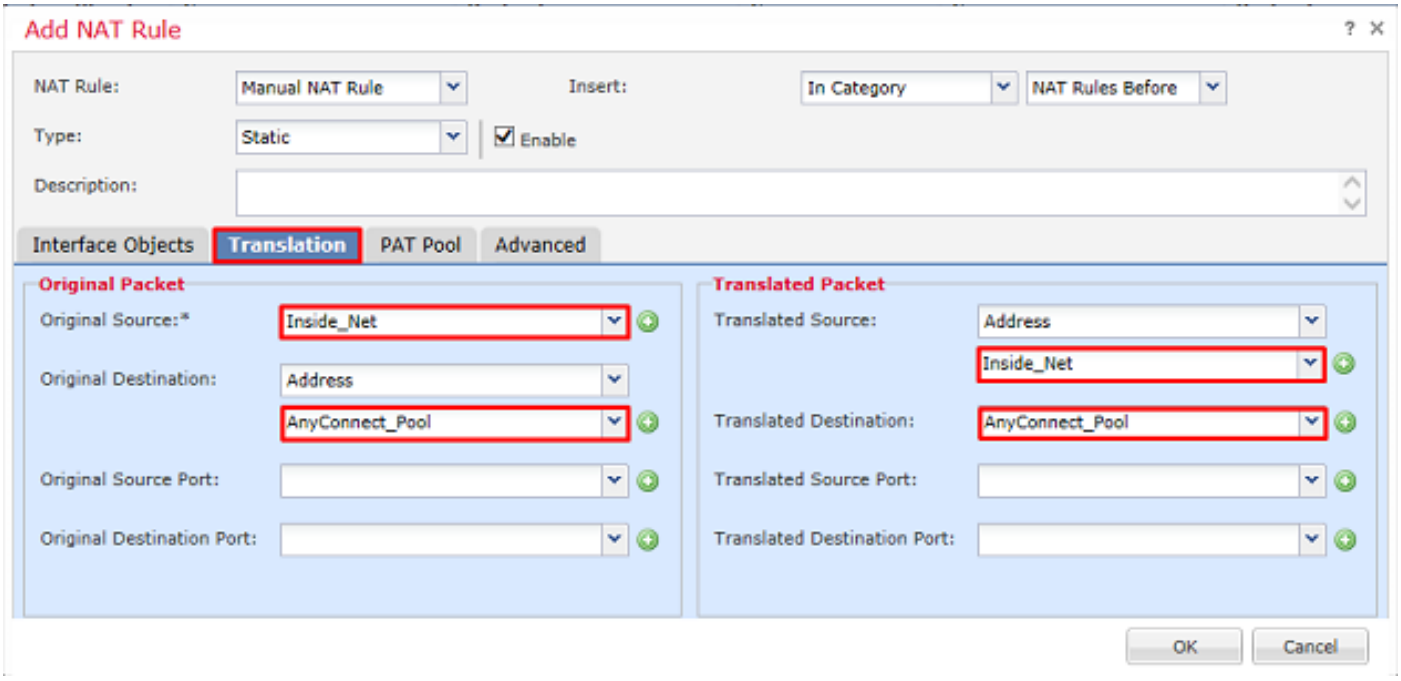
AnyConnect 트래픽이 NAT에 영향을 받지 않도록 하려면 오른쪽 상단에서 **Add Rule(규칙 추가)**을 클릭합니다.



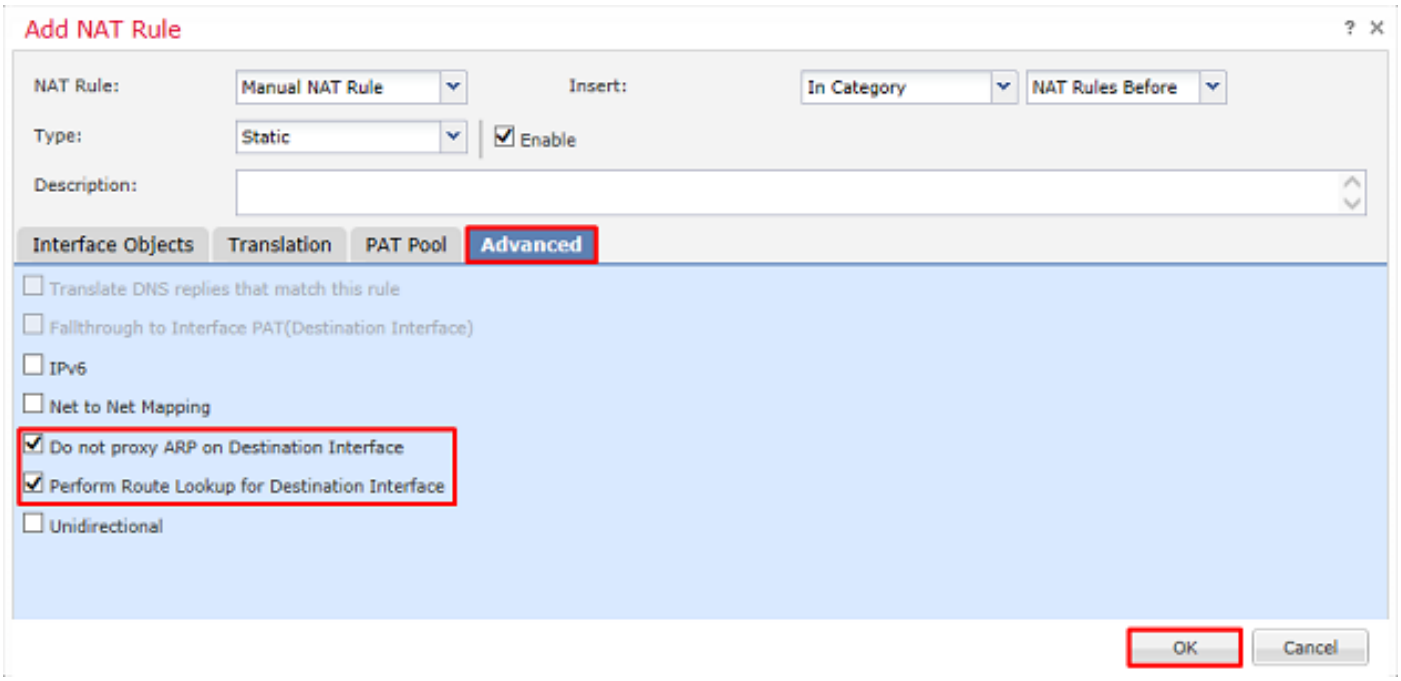
3. NAT 예외 규칙을 구성하고, 규칙이 유형이 고정인 수동 NAT 규칙인지 확인합니다. AnyConnect 트래픽에 적용되는 양방향 NAT 규칙입니다.

이러한 설정을 통해 FTD가 Inside_Net에서 시작하고 AnyConnect IP 주소(AnyConnect_Pool로 정의됨)로 향하는 트래픽을 탐지하면, 트래픽이 inside_zone을 인그레스하고 outside_zone을 이그레스할 때 소스가 동일한 값(Inside_Net)으로 변환되고 목적지가 동일한 값(AnyConnect_Pool)으로 변환됩니다. 이는 기본적으로 이러한 조건이 충족될 때 NAT를 우회합니다.

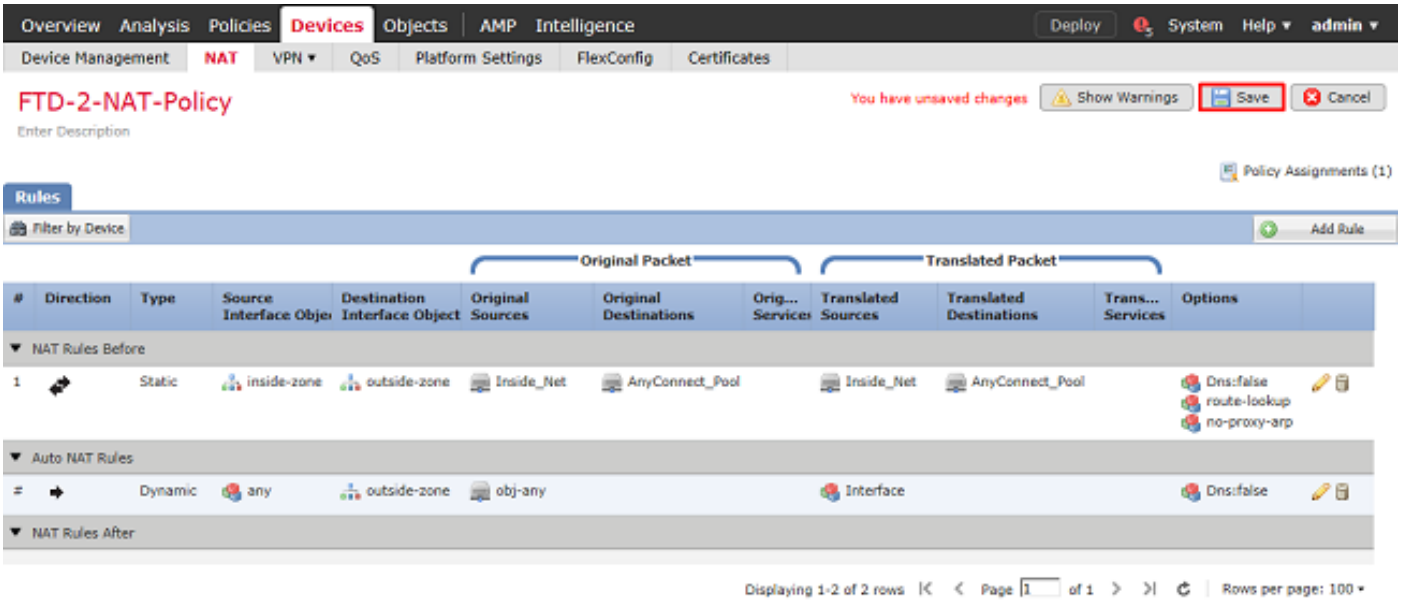




또한 FTD는 프록시 ARP가 아니라 이 트래픽에 대해 경로 조회를 수행하도록 설정됩니다. 완료되면 **OK(확인)**를 클릭합니다.

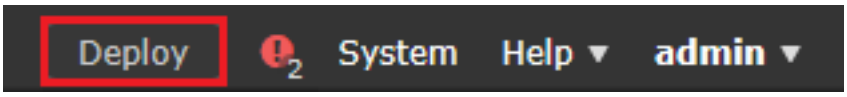


4. 저장을 **클릭합니다**.

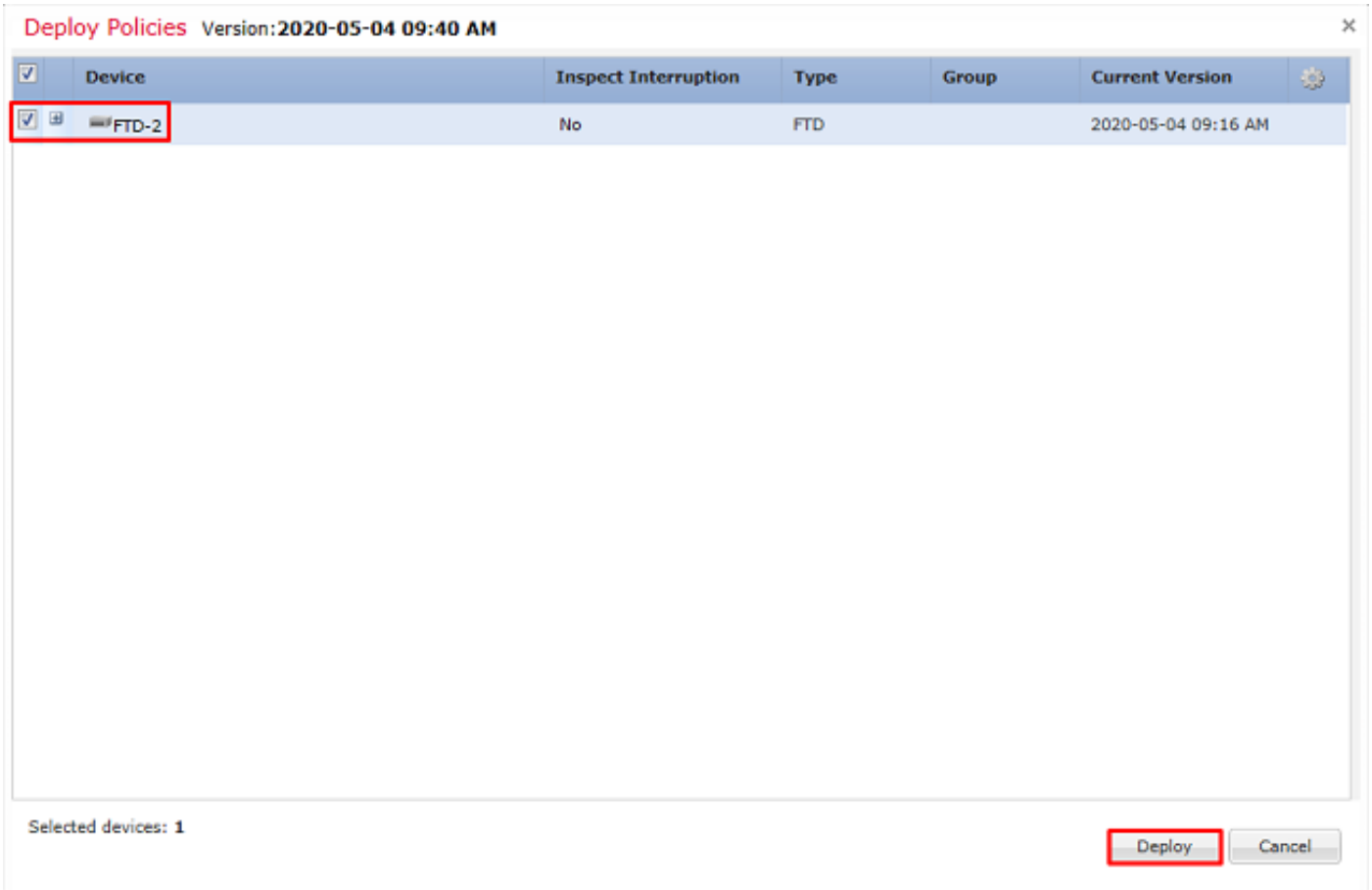


구축

1. 컨피그레이션이 완료되면 오른쪽 상단에서 **Deploy**(구축) 버튼을 클릭합니다.



2. 구성이 적용되는 FTD 옆에 있는 확인란을 클릭하고 구축을 **클릭합니다**.



다음을 확인합니다.

최종 컨피그레이션

AAA 컨피그레이션

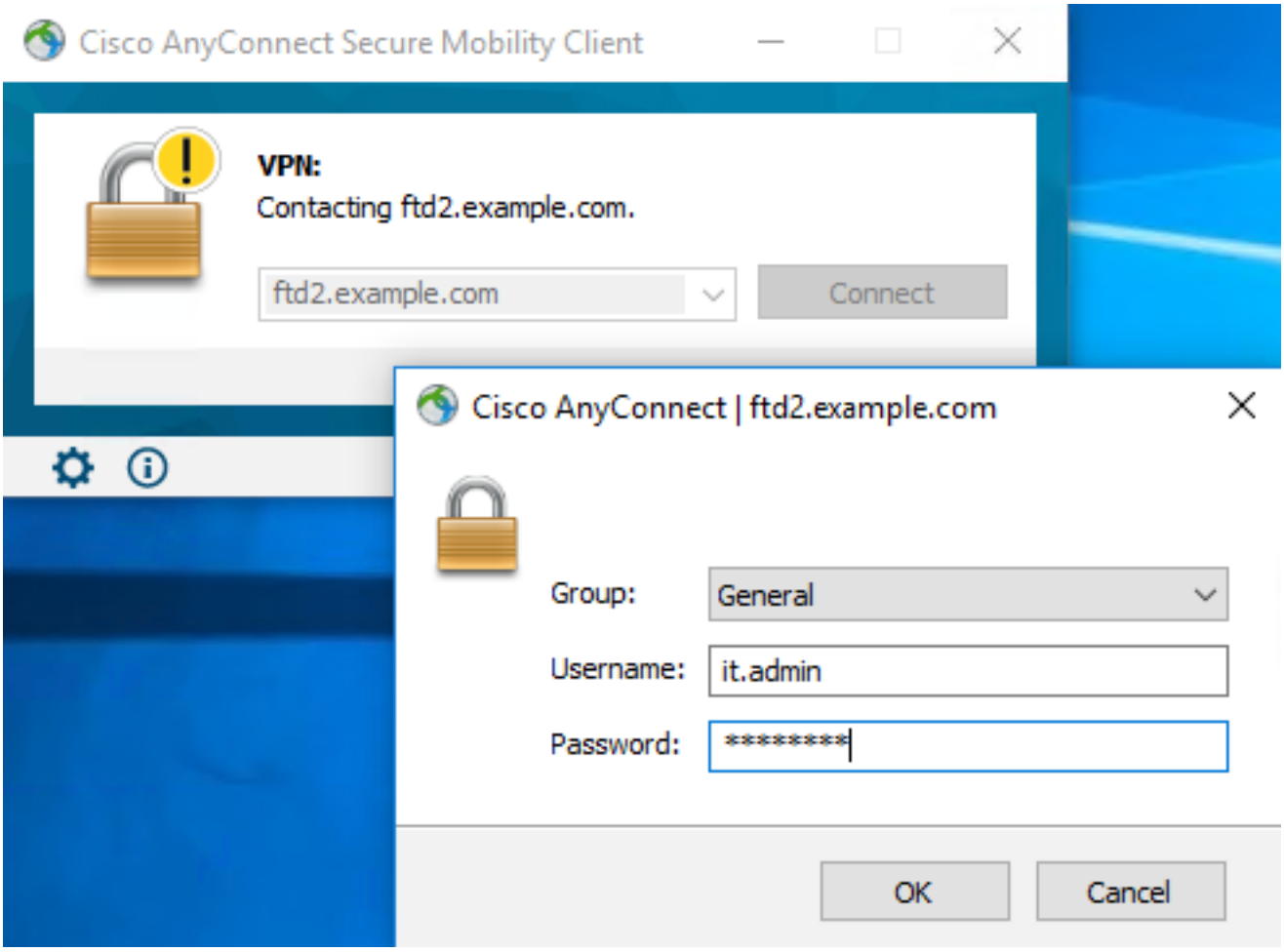
```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 max-failed-attempts 4
 realm-id 5
aaa-server LAB-AD host win2016.example.com
 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-group-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-naming-attribute samaccountname
 ldap-login-password *****
 ldap-login-dn ftd.admin@example.com
 server-type microsoft
```

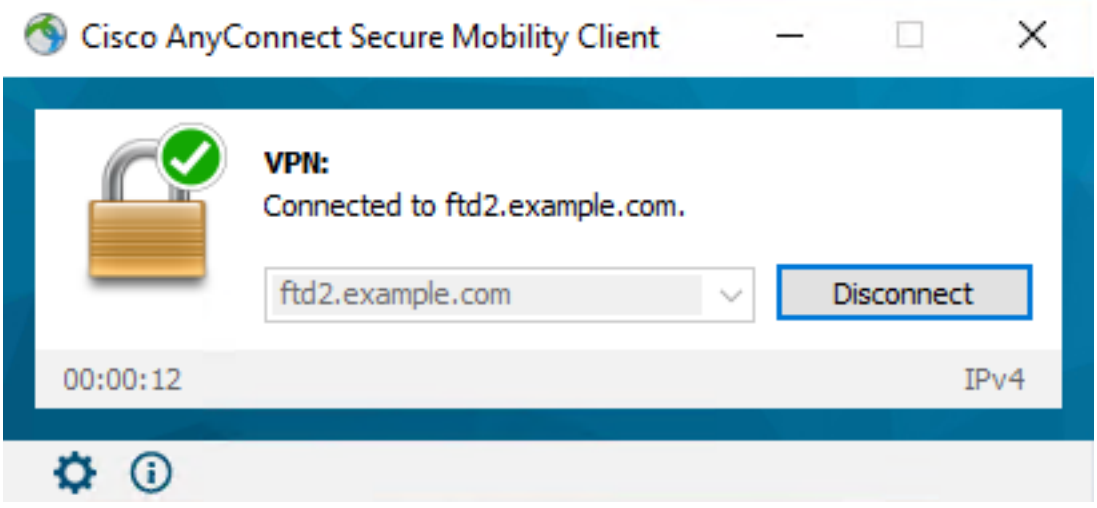
AnyConnect 컨피그레이션

```
> show running-config webvpn
webvpn
 enable Outside
 anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
 anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
 anyconnect profiles Lab disk0:/csm/lab.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  no disable
 error-recovery disable

> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
 address-pool AnyConnect-Pool
 authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
 group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Lab
 user-authentication-idle-timeout none
 webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable
```

```
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

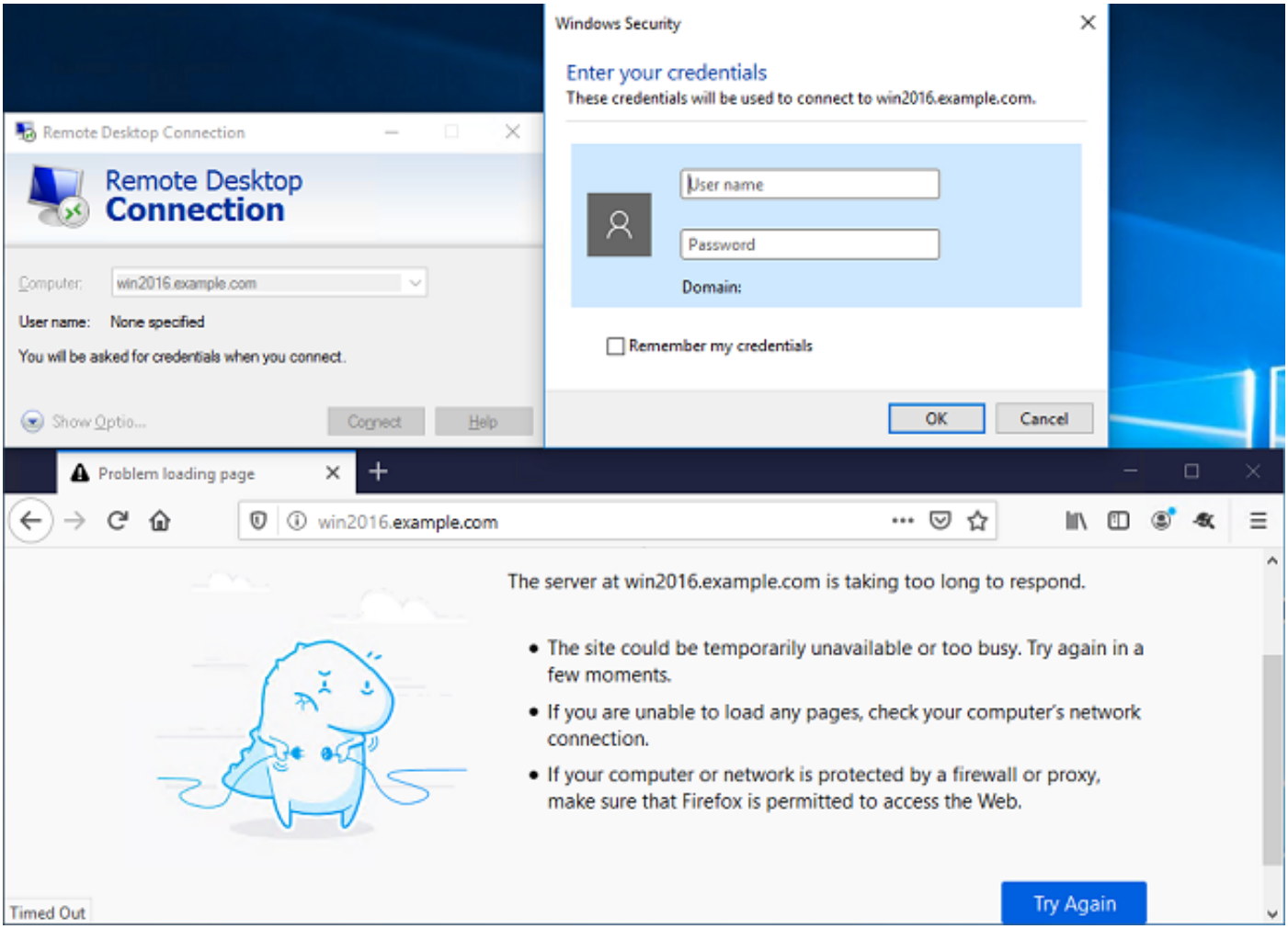
AnyConnect로 연결 및 액세스 제어 정책 규칙 확인



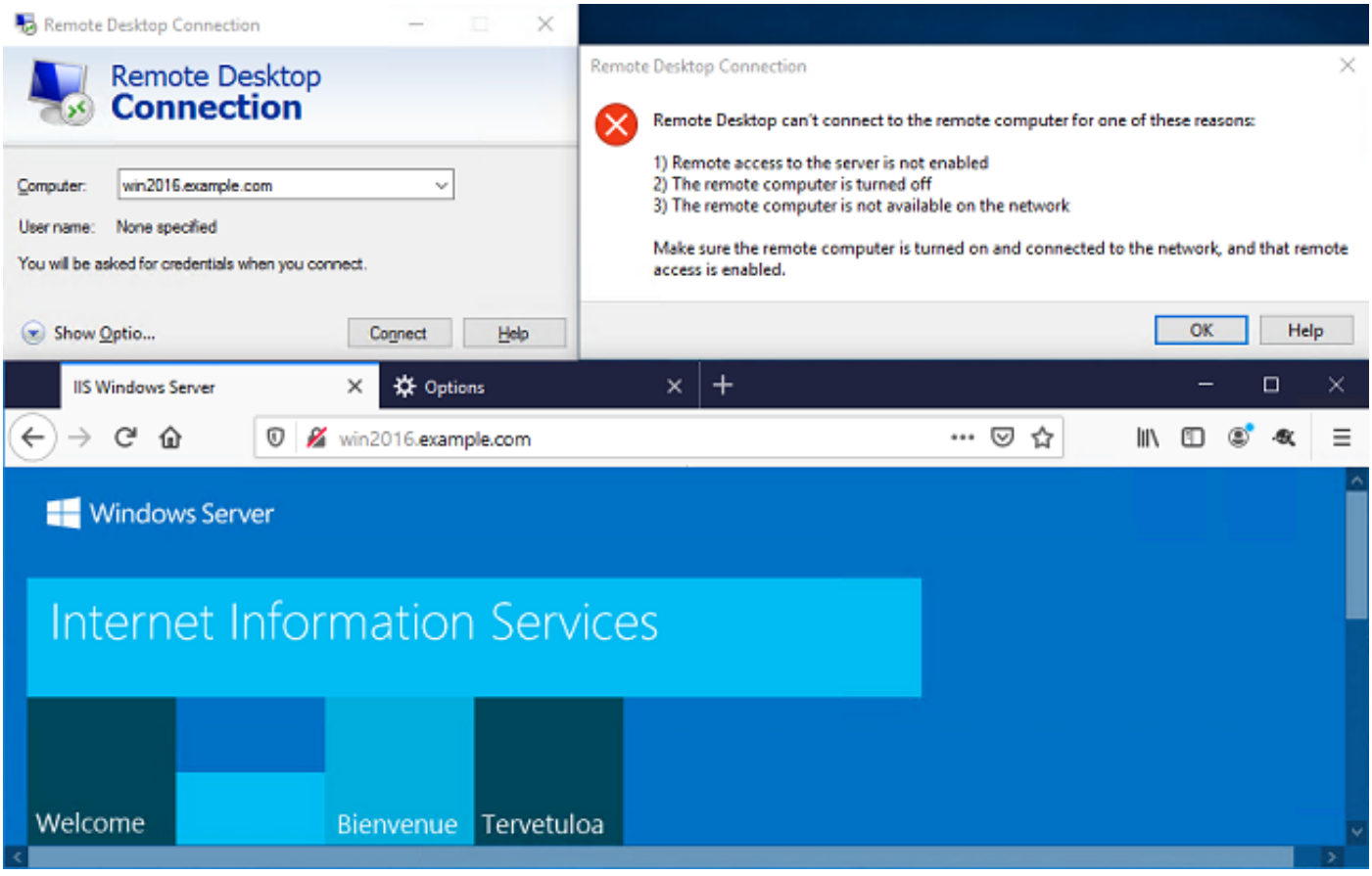


사용자 IT 관리자는 Windows Server에 대한 RDP 액세스 권한이 있지만 HTTP에 대한 액세스 권한이 없는 AnyConnect 관리자 그룹에 있습니다.

이 서버에 대한 RDP 및 Firefox 세션을 열면 이 사용자가 RDP를 통해서만 서버에 액세스할 수 있는지 확인합니다.



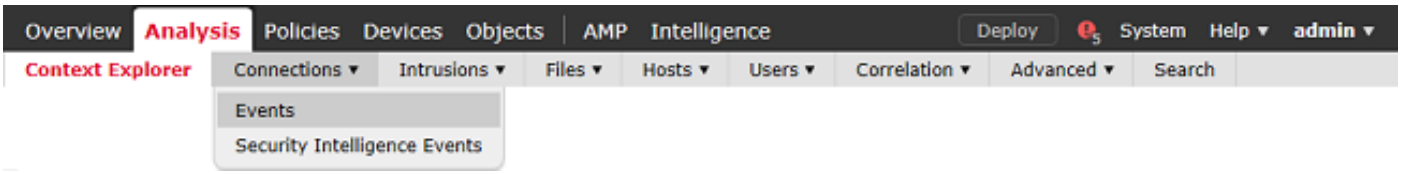
HTTP 액세스이지만 RDP 액세스는 아닌 AnyConnect 사용자 그룹에 있는 사용자 테스트 사용자로 로그인한 경우 액세스 제어 정책 규칙이 적용되는지 확인할 수 있습니다.



FMC 연결 이벤트로 확인

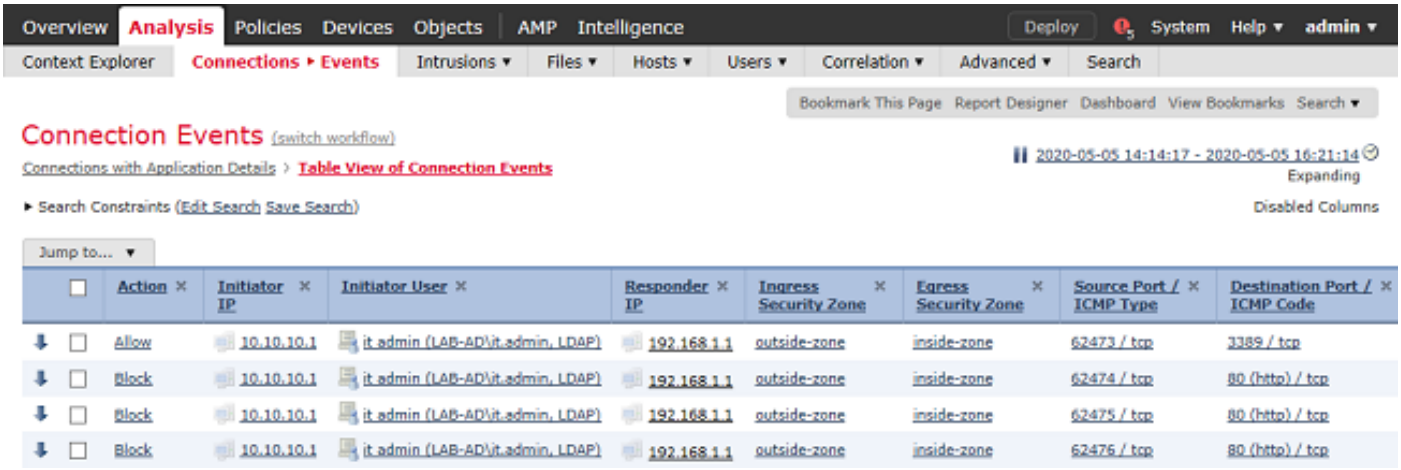
로깅이 액세스 제어 정책 규칙에서 활성화되었으므로, 해당 규칙과 일치하는 모든 트래픽에 대해 연결 이벤트를 확인할 수 있습니다

Analysis(분석) **> Connections(연결) > Events(이벤트)로 이동합니다**.

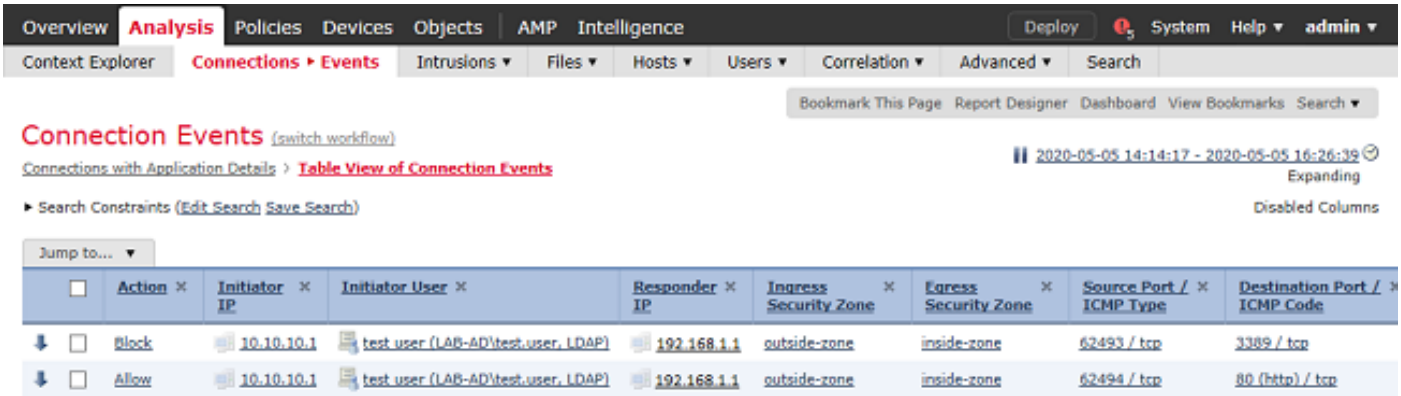


연결 이벤트**의 테이블 보기**에서 로그는 IT 관리자에 대한 연결 이벤트만 표시하도록 필터링됩니다.

여기서 서버에 대한 RDP 트래픽(TCP 및 UDP 3389)이 허용되는지 확인할 수 있지만 포트 80 트래픽은 차단됩니다.



사용자 **테스트 사용자**의 경우 서버에 대한 RDP 트래픽이 차단되고 포트 80 트래픽이 허용되는지 확인할 수 있습니다.



문제 해결

디버그

이 디버그는 진단 CLI에서 LDAP 인증 관련 문제를 해결하기 위해 실행할 수 있습니다. debug ldap **255**

사용자 ID 액세스 제어 정책 문제를 해결하기 위해 **시스템 지원 firewall-engine-debug를 클라이언트로 실행하여 트래픽**이 예기치 않게 허용되거나 차단되는 이유를 확인할 수 있습니다.

LDAP 디버깅 작업

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
        Base DN = [DC=example,DC=com]
        Filter  = [sAMAccountName=it.admin]
        Scope   = [SUBTREE]
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]    objectClass: value = top
[53]    objectClass: value = person
[53]    objectClass: value = organizationalPerson
[53]    objectClass: value = user
[53]    cn: value = IT Admin
[53]    sn: value = Admin
[53]    givenName: value = IT
[53]    distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]    instanceType: value = 4
[53]    whenCreated: value = 20200421025811.0Z
[53]    whenChanged: value = 20200421204622.0Z
[53]    displayName: value = IT Admin
[53]    uSNCreated: value = 25896
[53]    memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]    uSNChanged: value = 26119
[53]    name: value = IT Admin
[53]    objectGUID: value = &...J..O..2w...c
[53]    userAccountControl: value = 512
[53]    badPwdCount: value = 6
[53]    codePage: value = 0
[53]    countryCode: value = 0
[53]    badPasswordTime: value = 132320354378176394
[53]    lastLogoff: value = 0
[53]    lastLogon: value = 0
[53]    pwdLastSet: value = 132319114917186142
[53]    primaryGroupID: value = 513
[53]    objectSid: value = .............{I...;.....j...
[53]    accountExpires: value = 9223372036854775807
[53]    logonCount: value = 0
[53]    sAMAccountName: value = it.admin
[53]    sAMAccountType: value = 805306368
[53]    userPrincipalName: value = it.admin@example.com
```

```
[53]    objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]    dSCorePropagationData: value = 16010101000000.0Z
[53]    lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

LDAP 서버와의 연결을 설정할 수 없음

```
[-2147483611] Session Start
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

잠재적 솔루션:

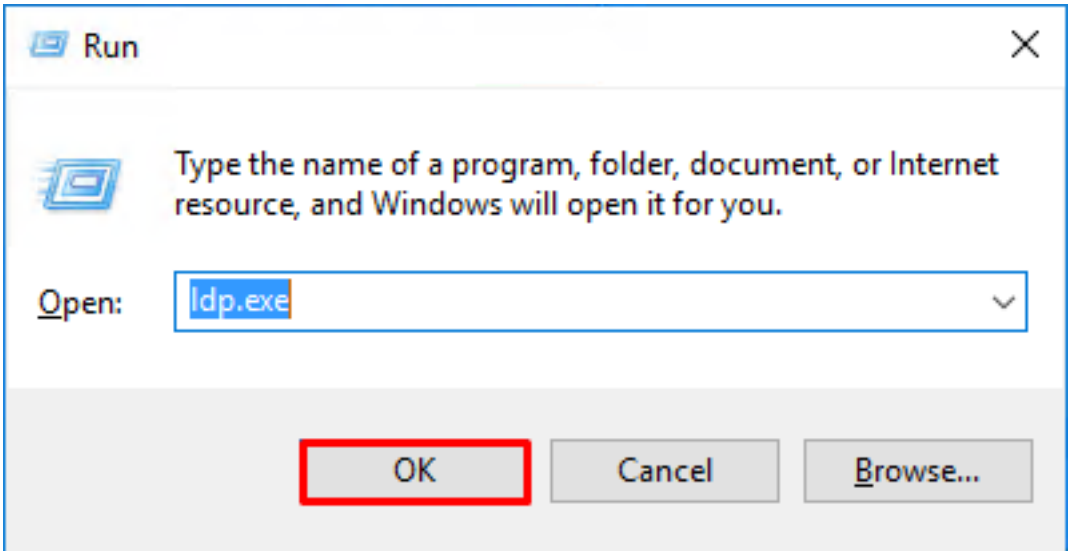
- 라우팅을 확인하고 FTD가 LDAP 서버로부터 응답을 수신하는지 확인합니다.
- LDAPS 또는 STARTTLS를 사용하는 경우 SSL 핸드셰이크가 성공적으로 완료될 수 있도록 올바른 루트 CA 인증서를 신뢰해야 합니다.
- 올바른 IP 주소 및 포트가 사용되었는지 확인합니다. 호스트 이름을 사용하는 경우 DNS에서 올바른 IP 주소로 확인할 수 있는지 확인합니다.

로그인 DN 및/또는 비밀번호 바인딩이 잘못되었습니다.

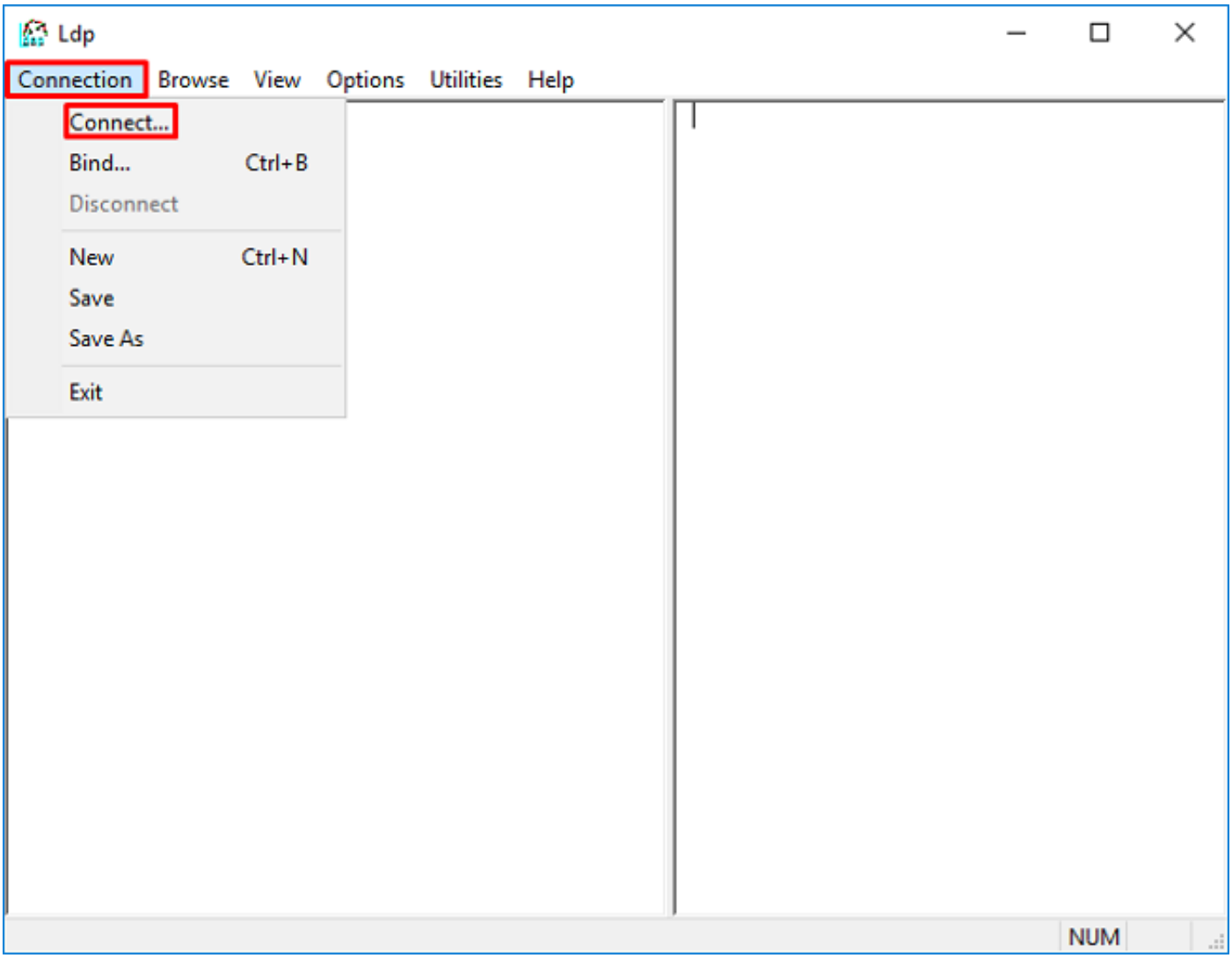
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid
credentials
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

잠재적 솔루션: 로그인 DN과 로그인 비밀번호가 적절하게 구성되었는지 확인합니다. 이는 AD 서버에서 ldp.exe를 사용하여 확인할 수 있습니다. 계정이 ldp를 사용하여 성공적으로 바인딩할 수 있는지 확인하려면 다음 단계를 수행하십시오.

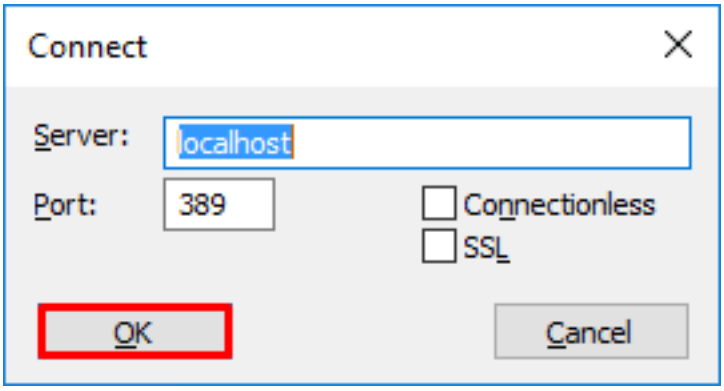
1. AD 서버에서 **Win+R**을 누르고 **ldp.exe**를 검색합니다.



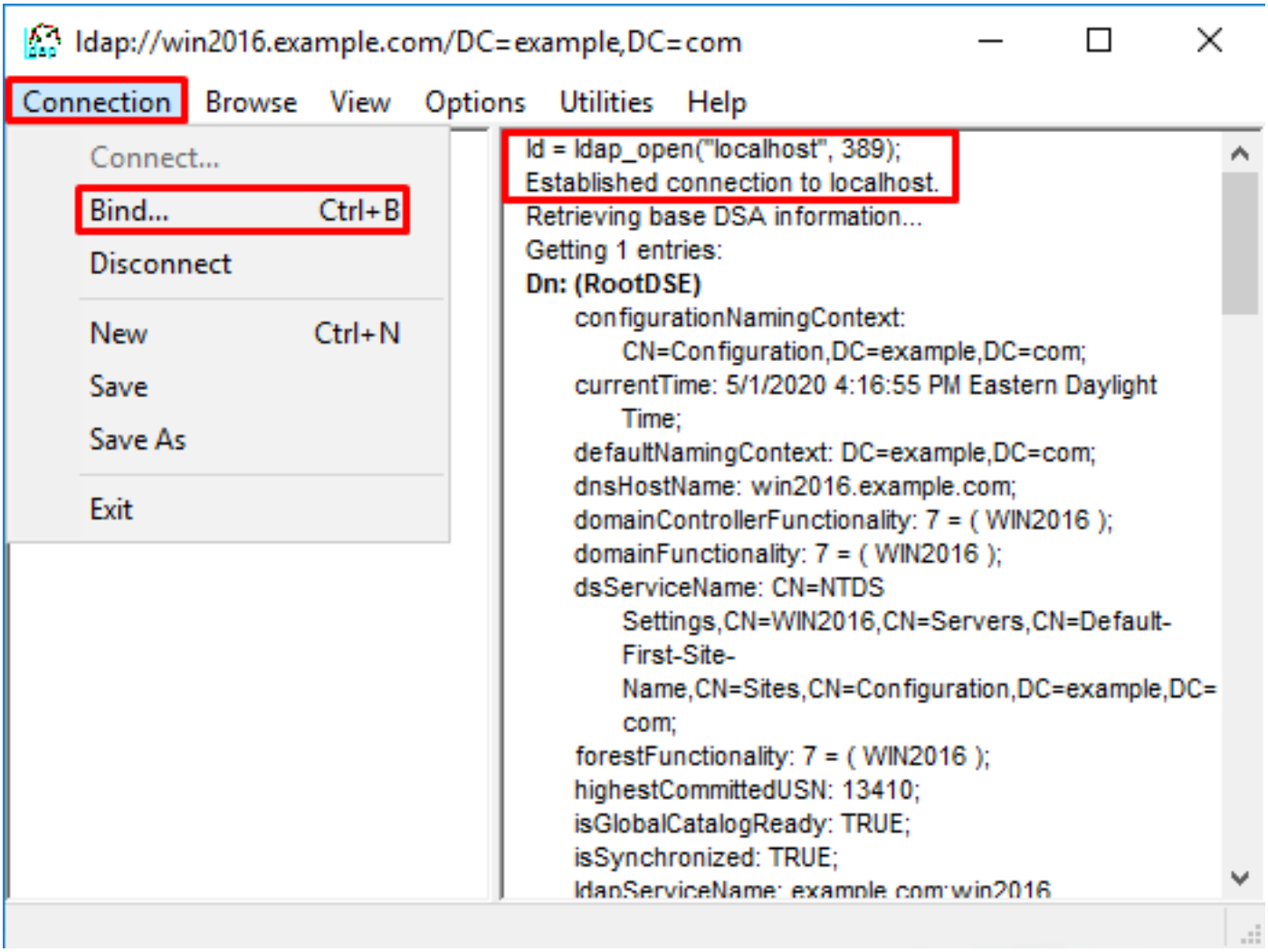
2. **연결** 아래에서 **연결...을 선택합니다.**



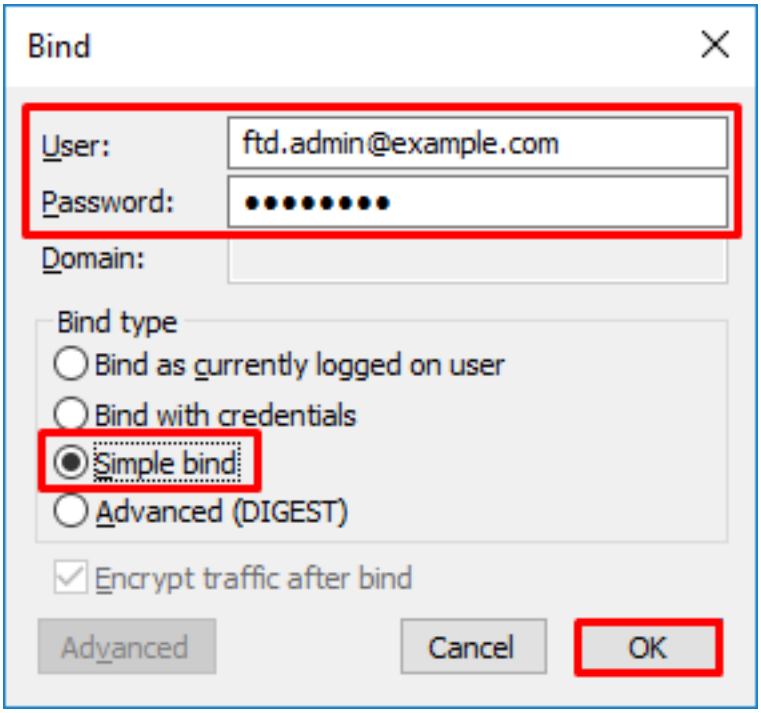
3. 서버의 localhost 및 적절한 포트를 지정한 다음 확인을 **클릭합니다**.



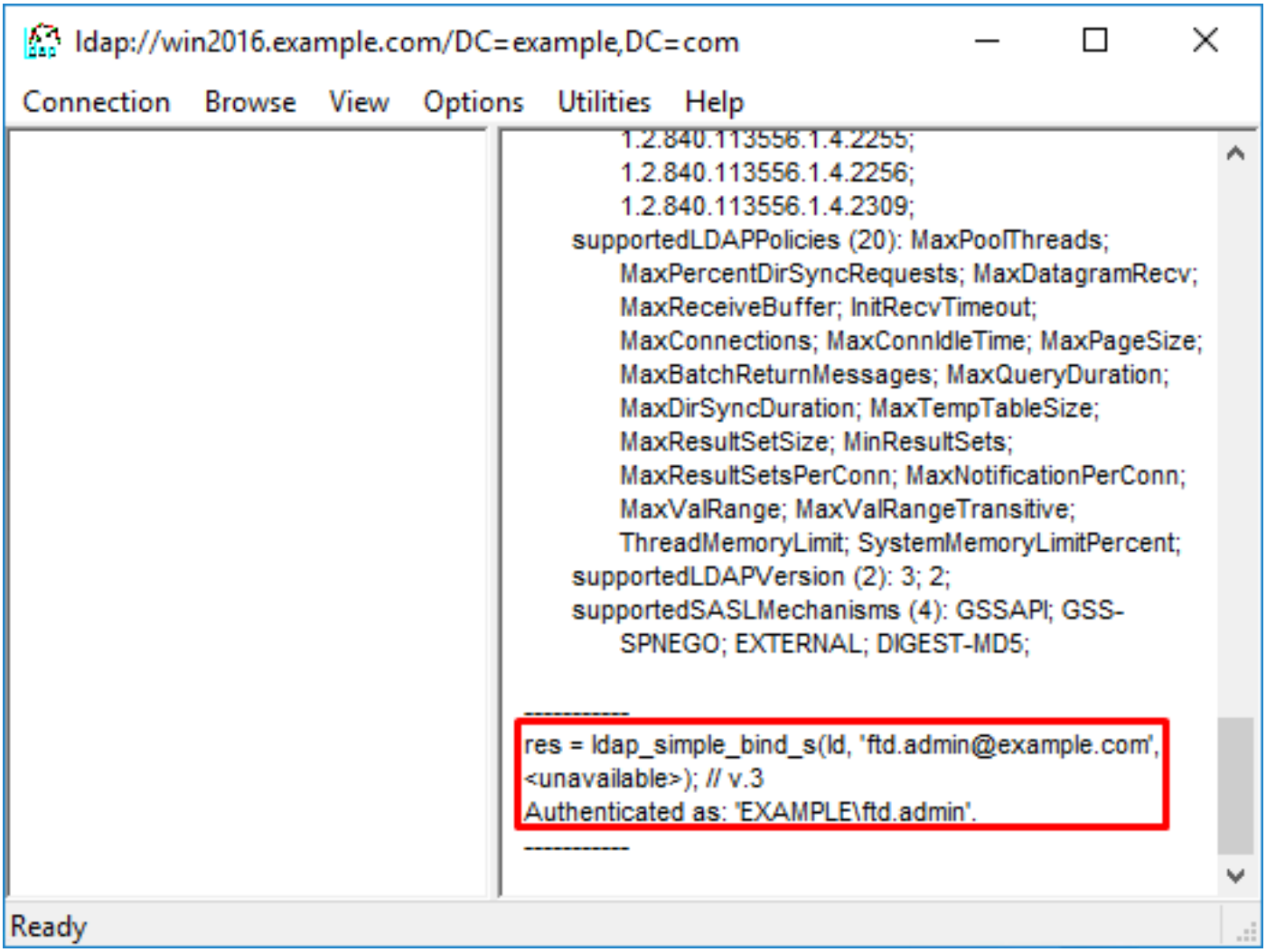
4. 오른쪽 열에는 성공적인 연결을 나타내는 텍스트가 표시됩니다. Connection(**연결**) > **Bind...(바인딩...)로 이동합니다.**



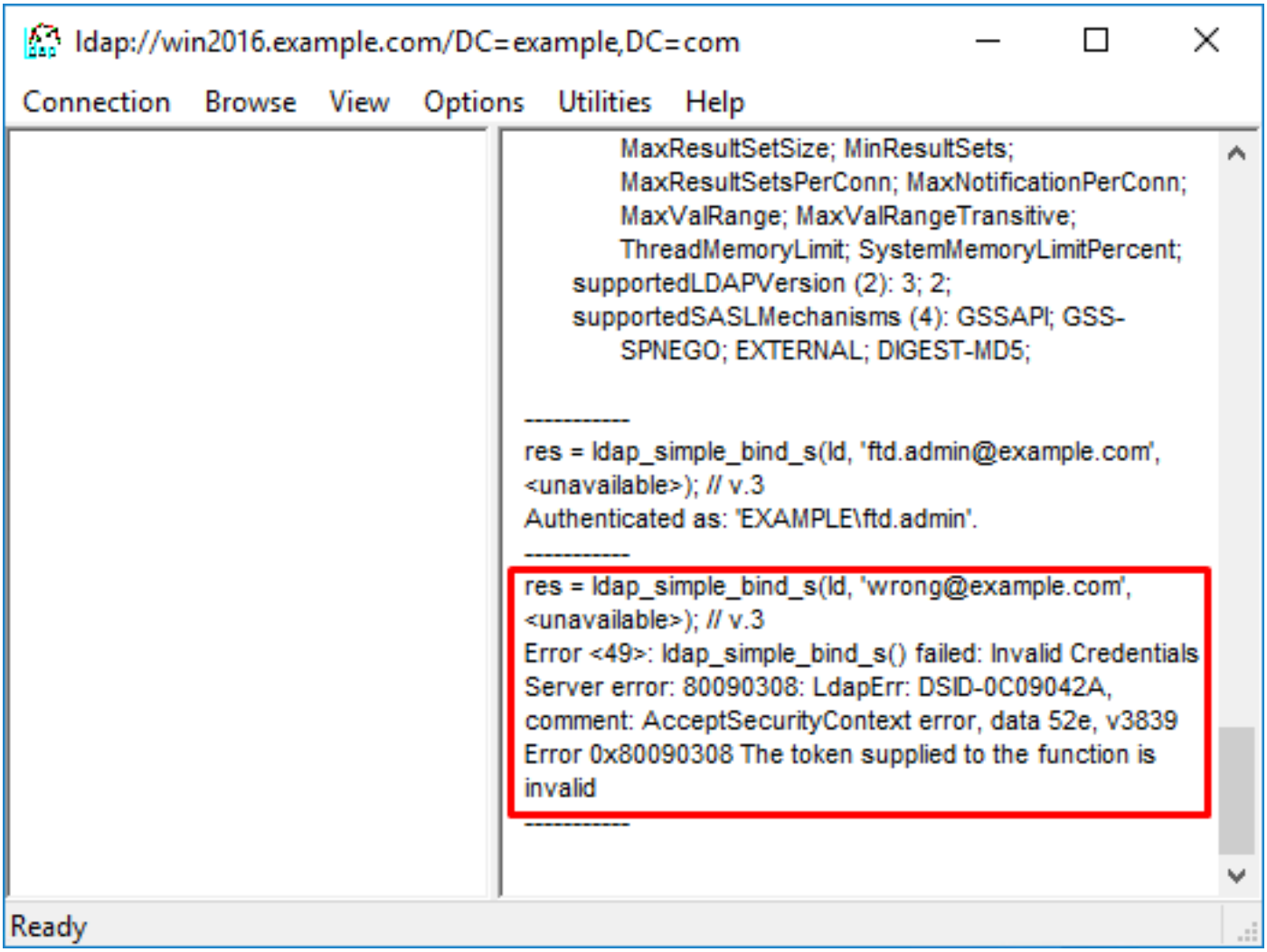
5. **단순 바인드를** 선택한 다음 **디렉토리 계정 사용자 이름**과 **비밀번호**를 **지정합니다.** OK(확인)를 클릭합니다.



바인딩이 성공하면 ldp는 Authenticated as: DOMAIN\username(DOMAIN\username으로 인증됨)을 **표시합니다.**



유효하지 않은 사용자 이름 또는 비밀번호로 바인딩을 시도하면 여기에 표시된 2와 같은 실패가 발생합니다.

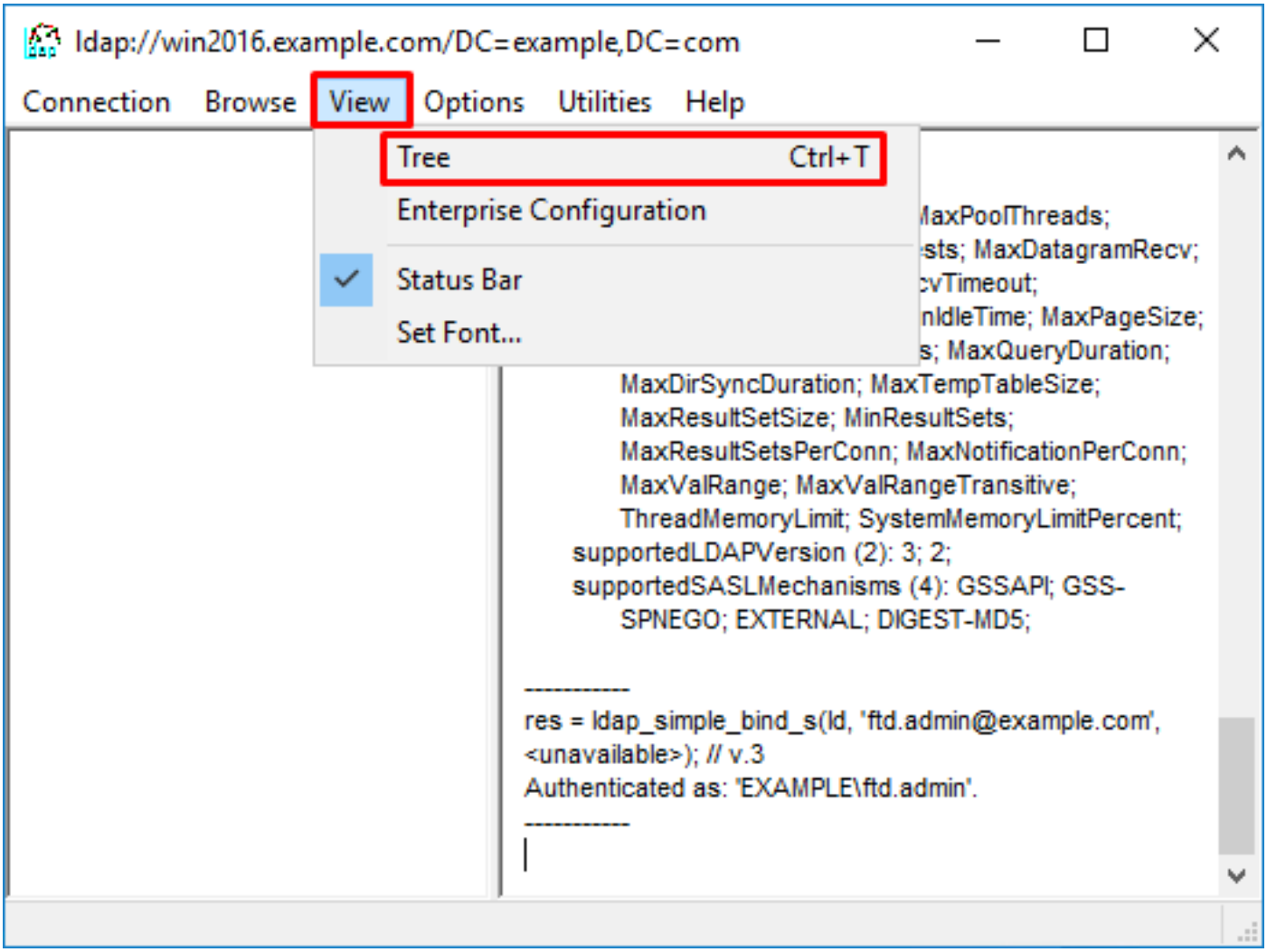


LDAP 서버가 사용자 이름을 찾을 수 없음

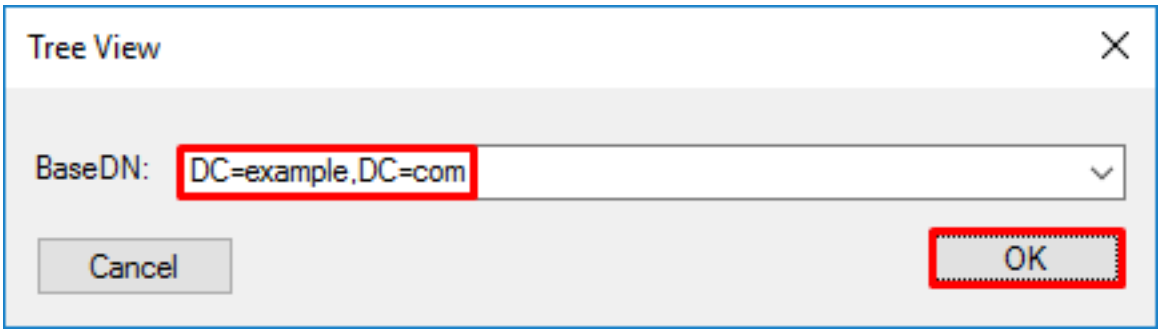
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admi]
        Scope   = [SUBTREE]
[-2147483612] Search result parsing returned failure status
[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End
```

잠재적 솔루션: AD가 FTD에서 검색한 사용자를 찾을 수 있는지 확인합니다. 이 작업은 **ldp.exe**로도 가능합니다.

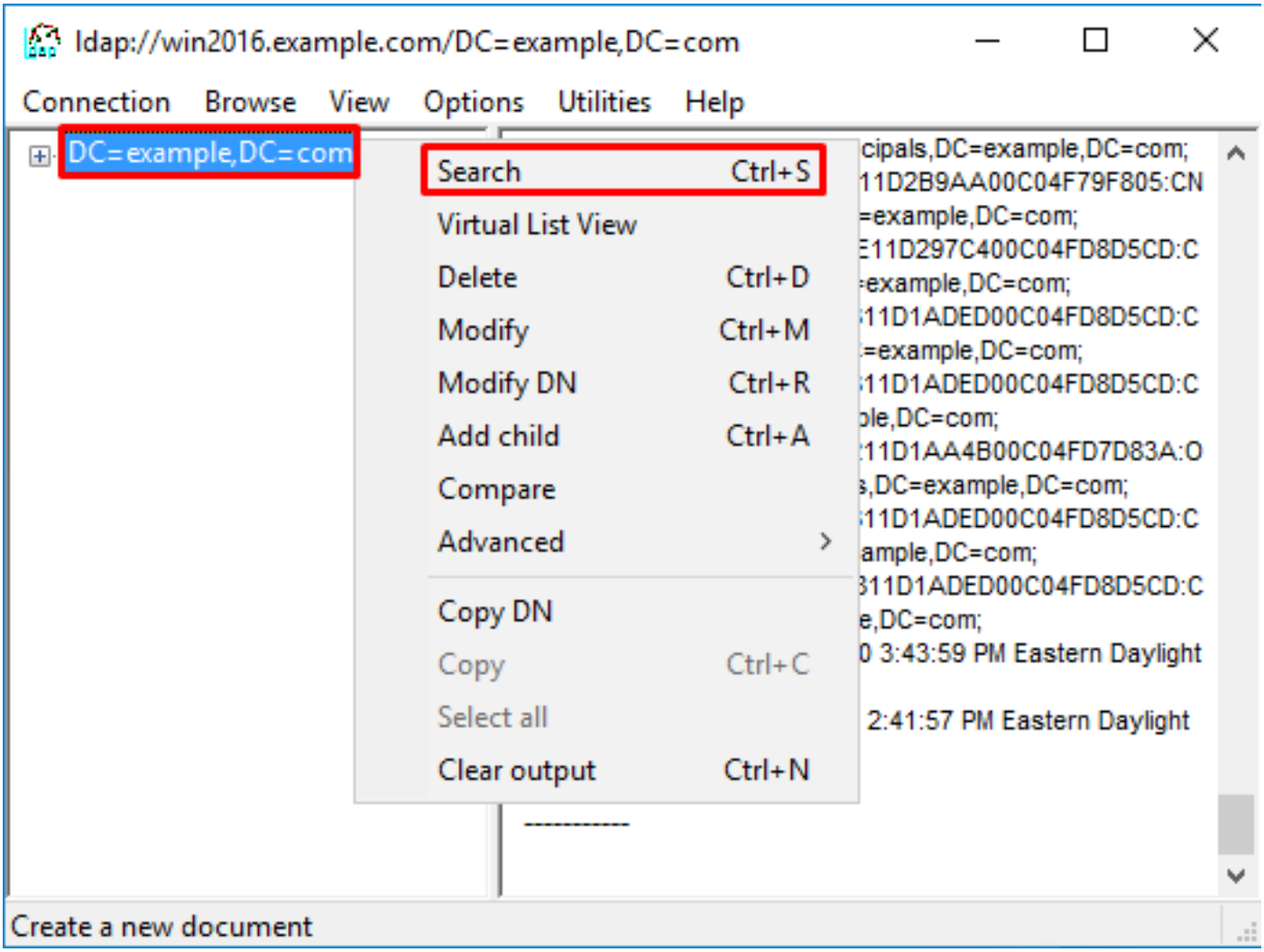
1. 위에 표시된 대로 성공적으로 바인딩한 후 **보기 > 트리**로 **이동합니다**.



2. FTD에 구성된 기본 DN을 지정한 다음 확인을 클릭합니다.



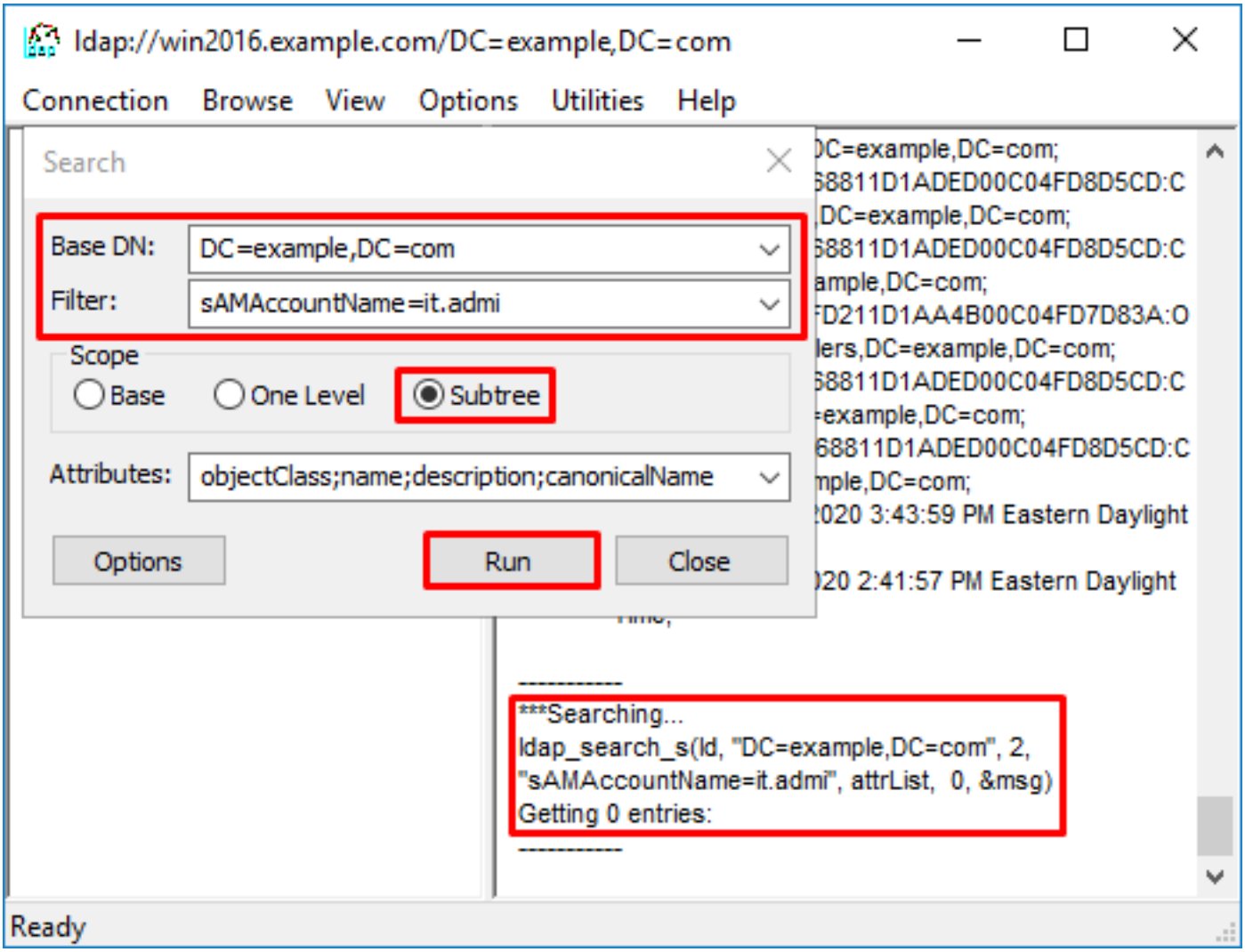
3. 기본 DN을 마우스 오른쪽 버튼으로 클릭한 다음 검색**을 클릭합니다**.



4. 디버그에 표시된 것과 동일한 **기본 DB**, **필터** 및 **범위** 값을 지정합니다.

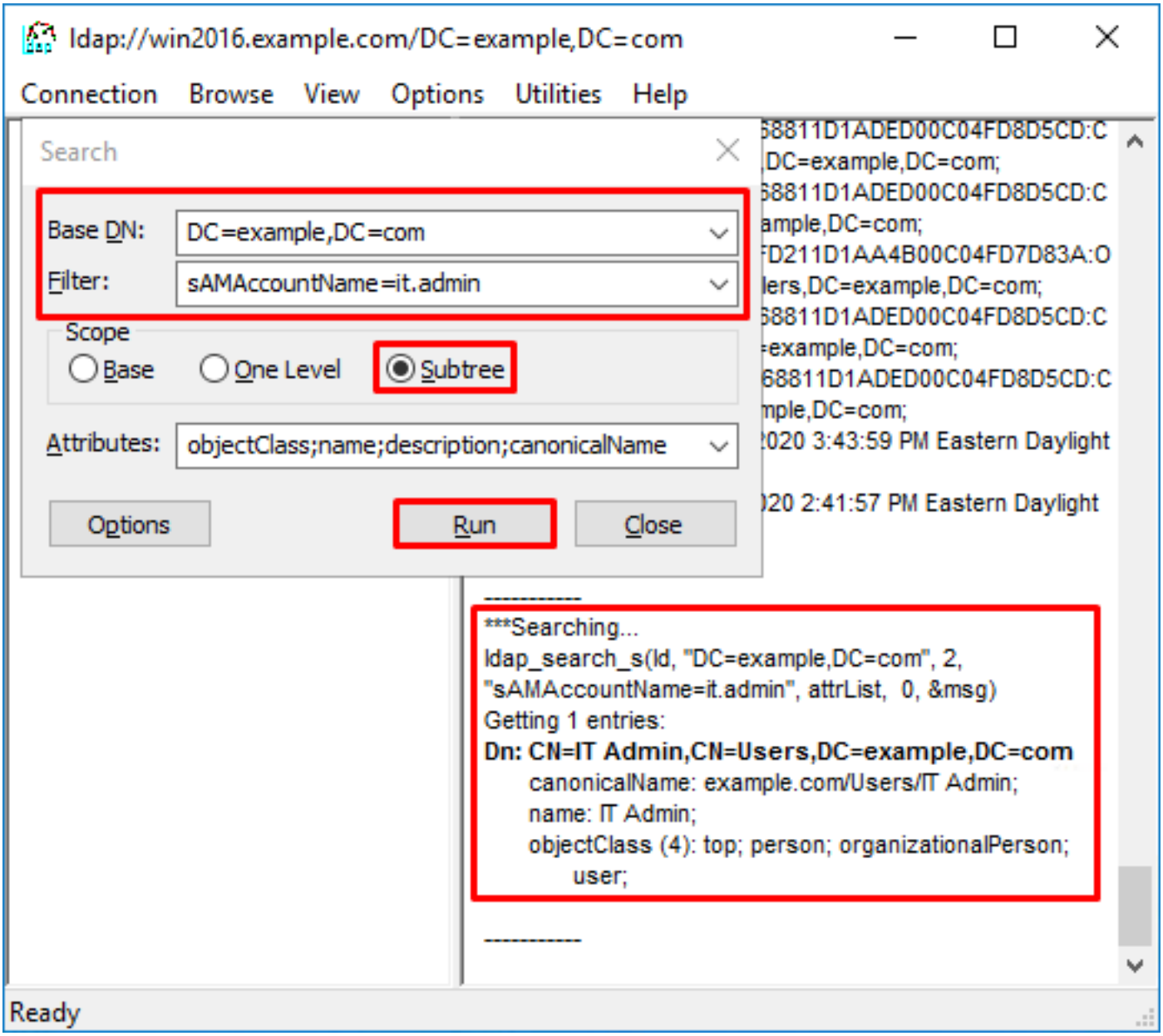
이 예에서는 다음과 같습니다.

- 기본 DN: dc=example,dc=com
- 필터: samaccountname=it.admi
- 범위:하위 트리



기본 DN dc=example,dc=com 아래에 samaccountname **it.admi**를 가진 사용자 계정이 없기 때문에 ldp는 0개의 항목을 찾습니다

올바른 samaccountname **it.admin**을 사용한 또 다른 시도로 다른 결과가 표시됩니다. ldp는 기본 DN dc=example,dc=com 아래에서 1개의 항목을 찾고 해당 사용자 DN을 인쇄합니다.



사용자 이름에 대한 잘못된 비밀번호

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admin]
        Scope   = [SUBTREE]
[-2147483613] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
```

```
[-2147483613] Simple authentication for it.admin returned code (49) Invalid credentials
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment:
AcceptSecurityContext error, data 52e, v3839
[-2147483613] Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

잠재적 해결 방법: 사용자 비밀번호가 적절하게 구성되어 있고 만료되지 않았는지 확인하십시오. 로그인 DN과 마찬가지로 FTD는 사용자 자격 증명을 사용하여 AD에 바인딩합니다.

이 바인딩은 AD가 동일한 사용자 이름 및 비밀번호 자격 증명을 인식할 수 있는지 확인하기 위해 ldp에서도 수행할 수 있습니다. ldp의 단계는 Binding Login **DN and/or password incorrect 섹션에 나와 있습니다**.

또한 Microsoft server **Event Viewer 로그**를 검토할 수 있습니다.

테스트 AAA

test **aaa-server 명령**을 사용하여 특정 사용자 이름 및 비밀번호로 FTD에서 인증 시도를 시뮬레이션할 수 있습니다. 연결 또는 인증 실패를 테스트하는 데 사용할 수 있습니다. 이 명령은 **test aaa-server authentication [AAA-server] host [AD IP/hostname](aaa-server 인증[AAA-server] 호스트 테스트)입니다.**

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 realm-id 7
aaa-server LAB-AD host win2016.example.com
 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-login-password *****
 ldap-login-dn ftd.admin@example.com
 server-type auto-detect

> test aaa-server authentication LAB-AD host win2016.example.com
Username: it.admin
Password: ********
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

패킷 캡처

패킷 캡처를 사용하여 AD 서버에 대한 연결성을 확인할 수 있습니다. LDAP 패킷이 FTD를 떠났지만 응답이 없는 경우 라우팅 문제를 나타낼 수 있습니다.

Capture(캡처)는 양방향 LDAP 트래픽을 표시합니다.

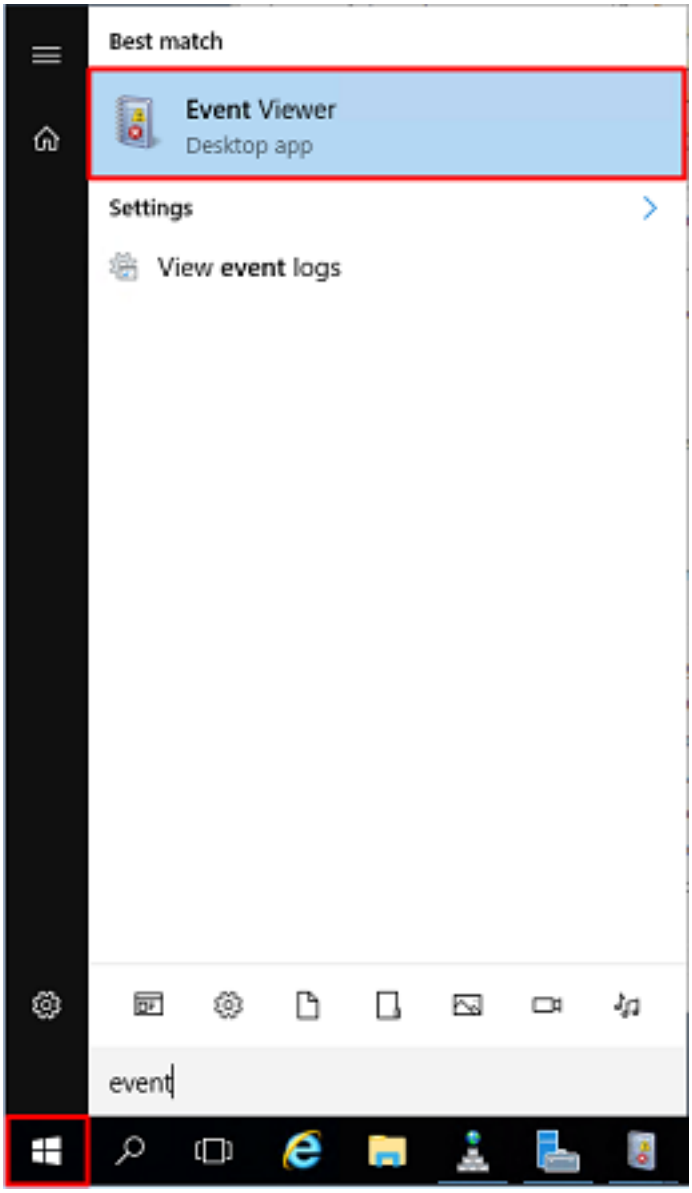
```
> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via inside
      Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389
```

```
> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
  match tcp any host 192.168.1.1 eq ldap

> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
  match tcp any host 192.168.1.1 eq ldap

> show capture AD

54 packets captured

   1: 23:02:16.770712       192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
   2: 23:02:16.772009       192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
   3: 23:02:16.772039       192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
<nop,nop,timestamp 1061373058 762393884>
   4: 23:02:16.772482       192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
   5: 23:02:16.772924       192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
   6: 23:02:16.772955       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
   7: 23:02:16.773428       192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
   8: 23:02:16.775030       192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
   9: 23:02:16.775075       192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

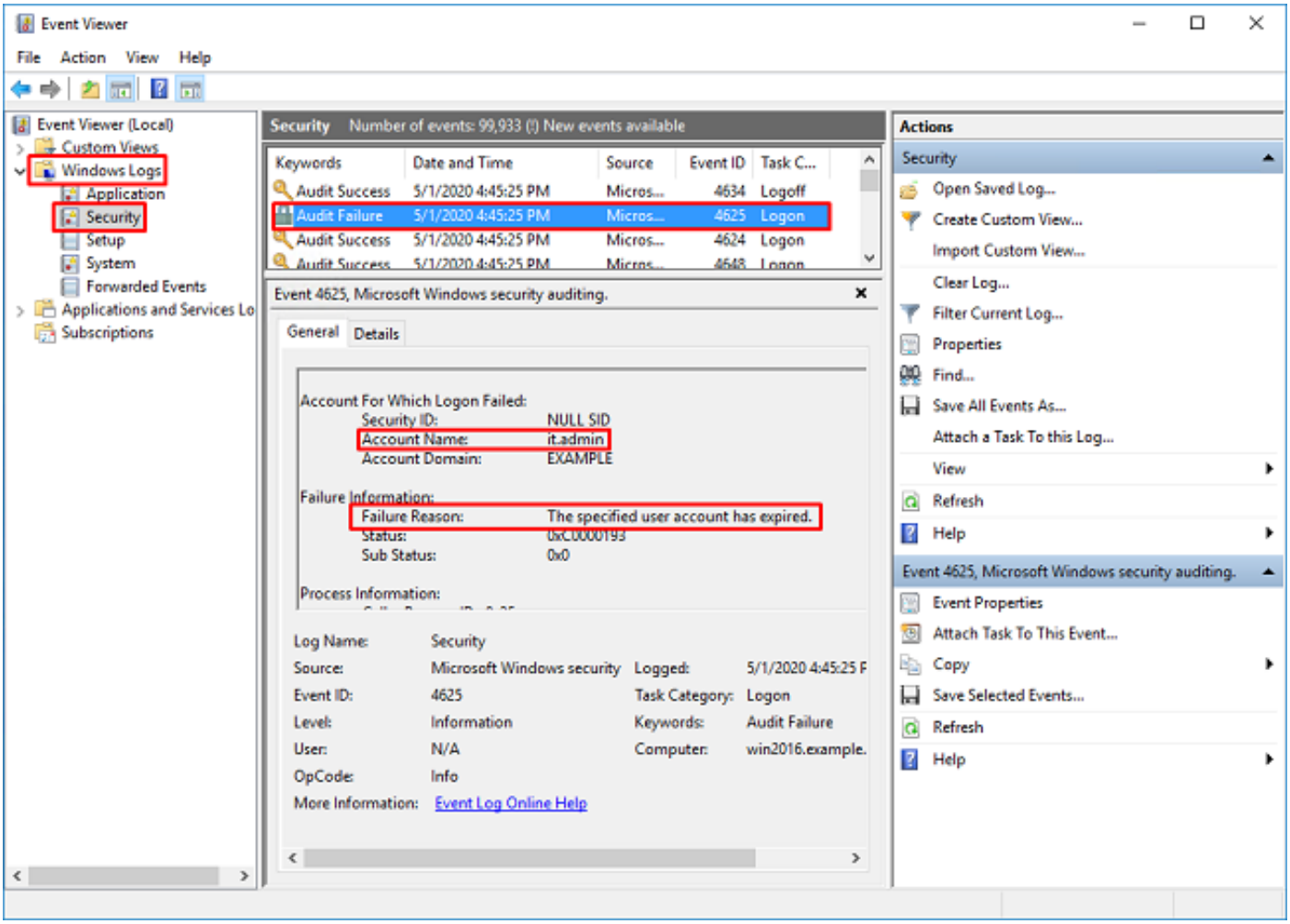
Windows Server 이벤트 뷰어 로그

AD **서버**에 대한 **이벤트 뷰어** 로그는 장애가 발생한 이유에 대한 자세한 정보를 제공할 수 있습니다.

1. **이벤트** 뷰어를 검색하여 **엽니다**.



2. **Windows** 로그**를 확장하고 보안** 을 클릭합니다. 사용자 계정 **이름**으로 **감사** 실패를 검색하고 실패 정보를 검토합니다.



An account failed to log on.

Subject:
Security ID:SYSTEM
Account Name:WIN2016$
Account Domain:EXAMPLE
Logon ID:0x3E7

Logon Type:3

Account For Which Logon Failed:
Security ID:NULL SID
Account Name:it.admin
Account Domain:EXAMPLE

Failure Information:
Failure Reason:The specified user account has expired.
Status:0xC0000193
Sub Status:0x0

Process Information:
Caller Process ID:0x25c
Caller Process Name:C:\Windows\System32\lsass.exe

Network Information:
Workstation Name:WIN2016
Source Network Address:192.168.1.17
Source Port:56321

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.