AnyConnect 클라이언트에 대해 FDM에서 관리하는 FTD에서 AD(LDAP) 인증 및 사용자 ID 구성

목차

소개

이 문서의 목적은 FDM(Firepower Device Management)에서 관리하는 Cisco Firepower Threat Defense(FTD)에 연결하는 AnyConnect 클라이언트에 대해 Active Directory(AD) 인증을 구성하는 방법을 자세히 설명하는 것입니다. AnyConnect 사용자를 특정 IP 주소 및 포트로 제한하기 위해 액세스 정책에서 사용자 ID가 사용됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FDM에서 RA VPN 구성에 대한 기본 지식
- FDM의 LDAP 서버 구성에 대한 기본 지식
- AD에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft 2016 서버
- 6.5.0 실행 중인 FTDv

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

네트워크 다이어그램 및 시나리오

Windows 서버는 사용자 ID를 테스트하기 위해 IIS(인터넷 정보 서비스) 및 RDP(원격 데스크톱 프로토콜)로 미리 구성되어 있습니다.이 컨피그레이션 가이드에서는 3개의 사용자 계정과 2개의 그룹이 생성됩니다.

사용자 계정:

- FTD 관리자:FTD가 AD 서버에 바인딩될 수 있도록 디렉터리 계정으로 사용됩니다.
- IT 관리자:사용자 ID를 시연하는 데 사용되는 테스트 관리자 계정입니다.
- 테스트 사용자:사용자 ID를 시연하는 데 사용되는 테스트 사용자 계정입니다.

그룹:

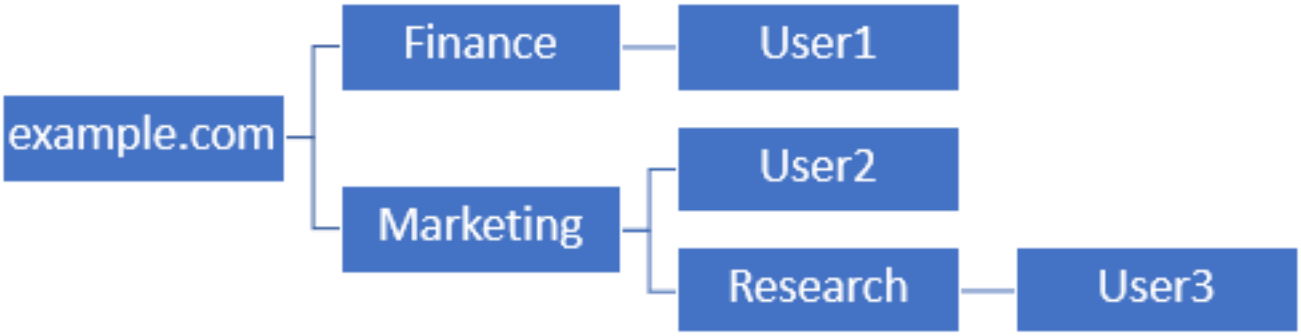
- AnyConnect 관리자:사용자 ID를 시연하기 위해 IT 관리자가 추가할 테스트 그룹입니다.이 그룹에는 Windows Server에 대한 RDP 액세스만 있습니다.
- AnyConnect 사용자:사용자 ID를 표시하기 위해 테스트 사용자가 추가되는 테스트 그룹입니다.이 그룹은 Windows Server에 대한 HTTP 액세스만 가집니다.

AD 구성

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

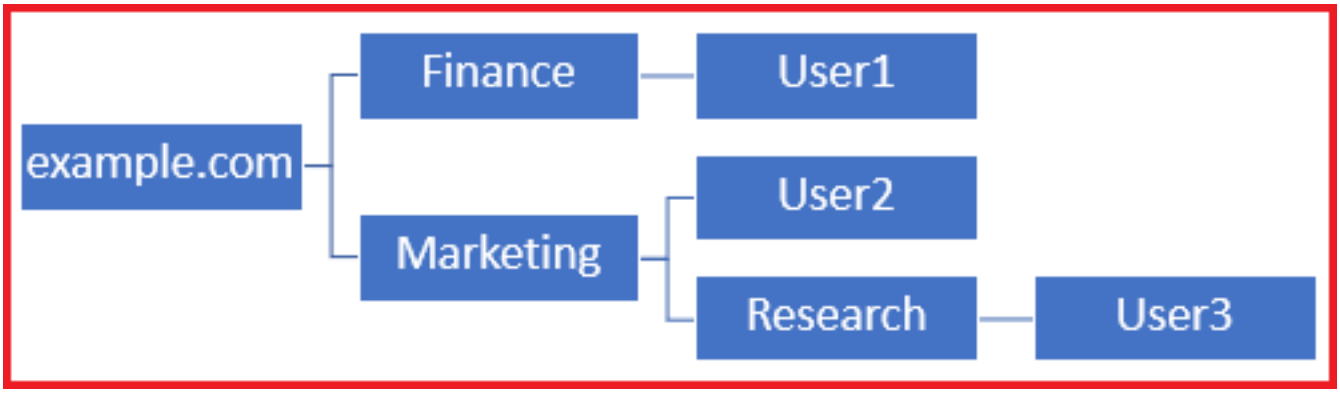
레이션을 수행하려면 먼저 Microsoft Server에서 이러한 모든 세부 정보를 생성하거나 수집해야 합니다.주요 값은 다음과 같습니다.

- 도메인 이름:서버의 도메인 이름입니다.이 컨피그레이션 가이드에서 example.com은 도메인 이름입니다.
- 서버 IP/FQDN 주소:Microsoft 서버에 연결하는 데 사용되는 IP 주소 또는 FQDN입니다 .FQDN을 사용하는 경우 FQDN을 확인하려면 FDM 및 FTD 내에서 DNS 서버를 구성해야 합니다.이 컨피그레이션 가이드에서 이 값은 **win2016.example.com**이며 192.168.1.1으로 확인됩니다.
- 서버 포트:LDAP 서비스에서 사용하는 포트입니다.기본적으로 LDAP 및 STARTTLS는 LDAP에 TCP 포트 389를 사용하고 LDAPS(LDAP over SSL)는 TCP 포트 636을 사용합니다.
- 루트 CA:LDAPS 또는 STARTTLS를 사용하는 경우 LDAPS에서 사용하는 SSL 인증서를 서명하는 데 사용되는 루트 CA가 필요합니다.
- 디렉토리 사용자 이름 및 비밀번호:FDM 및 FTD에서 LDAP 서버에 바인딩하고 사용자를 인증하고 사용자 및 그룹을 검색하는 데 사용하는 계정입니다.FTD Admin이라는 어카운트가 이 용도로 생성됩니다.
- 기본 DN(고유 이름):Base DN은 FDM의 시작점이며 FTD는 Active Directory에 사용자를 검색할 때 시작하도록 지시합니다.이 컨피그레이션 가이드에서 루트 도메인 example.com이 Base DN으로 사용됩니다.그러나 프로덕션 환경에서는 LDAP 계층 구조 내에서 기본 DN을 더 많이 사용하는 것이 더 나을 수 있습니다.예를 들어 다음 LDAP 계층 구조를 사용합니다.



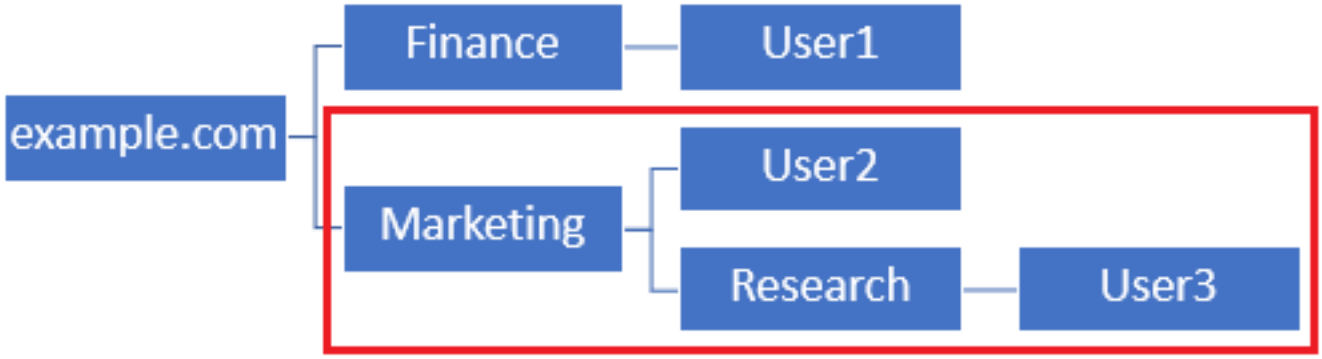
관리자가 마케팅 조직 구성 단위 내의 사용자가 기본 DN을 인증하도록 원할 경우 루트(example.com)로 설정할 수 있지만, 사용자 검색이 루트에서 시작되고 Finance, Marketing 및 Research로 내려가기 때문에 재무 조직 구성 단위 아래의 User1도 로그인할 수 있습니다.

기본 DN이 example.com으로 설정됩니다.



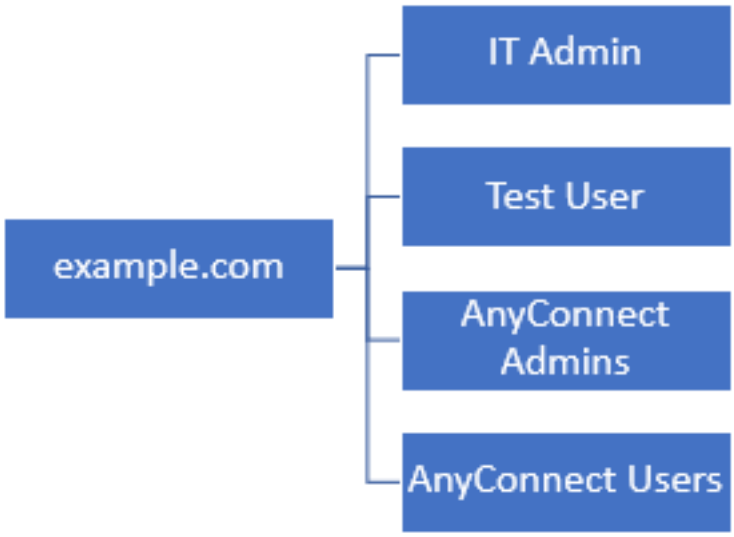
마케팅 조직 구성 단위 이하의 사용자만 로그인을 제한하기 위해 관리자는 기본 DN을 마케팅으로 설정할 수 있습니다.이제 User2 및 User3만 인증할 수 있습니다. Marketing에서 검색이 시작됩니다 .

마케팅으로 설정된 기본 DN:



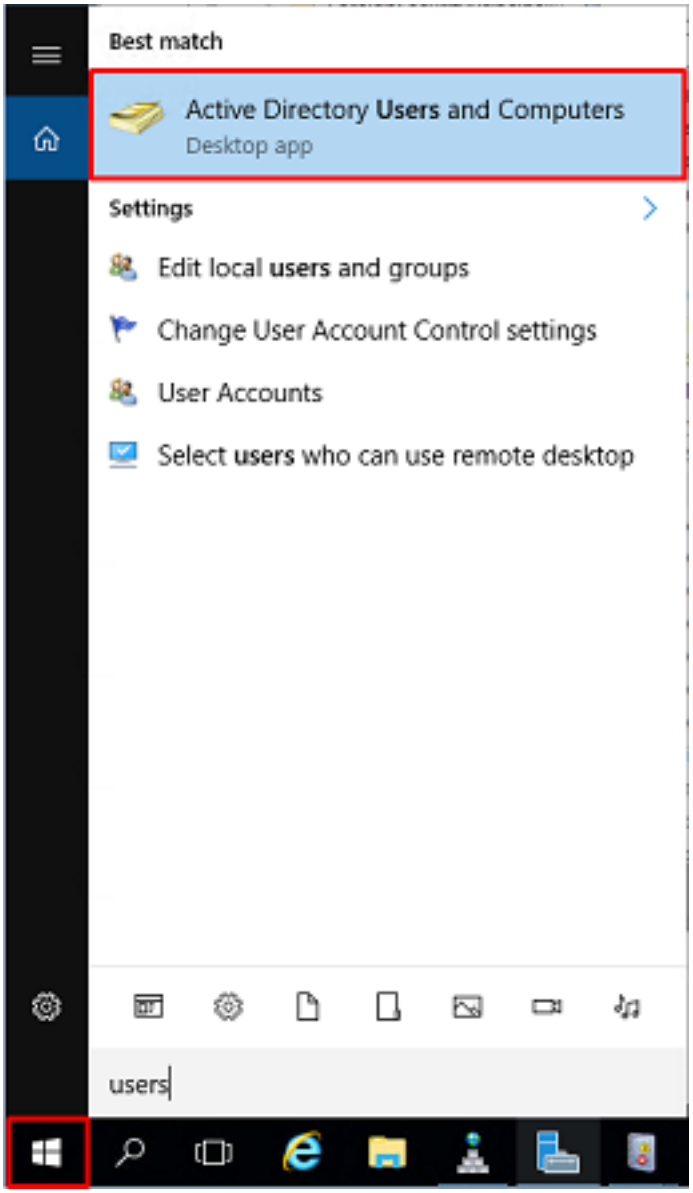
FTD 내에서 사용자가 AD 특성에 따라 다른 권한 부여를 할당하거나 연결할 수 있도록 보다 세분화된 제어를 수행하려면 LDAP 권한 부여 맵을 구성해야 합니다.

이 간소화된 LDAP 계층 구조는 이 컨피그레이션 가이드에서 사용되며 루트 example.com의 DN이 기본 DN에 사용됩니다.

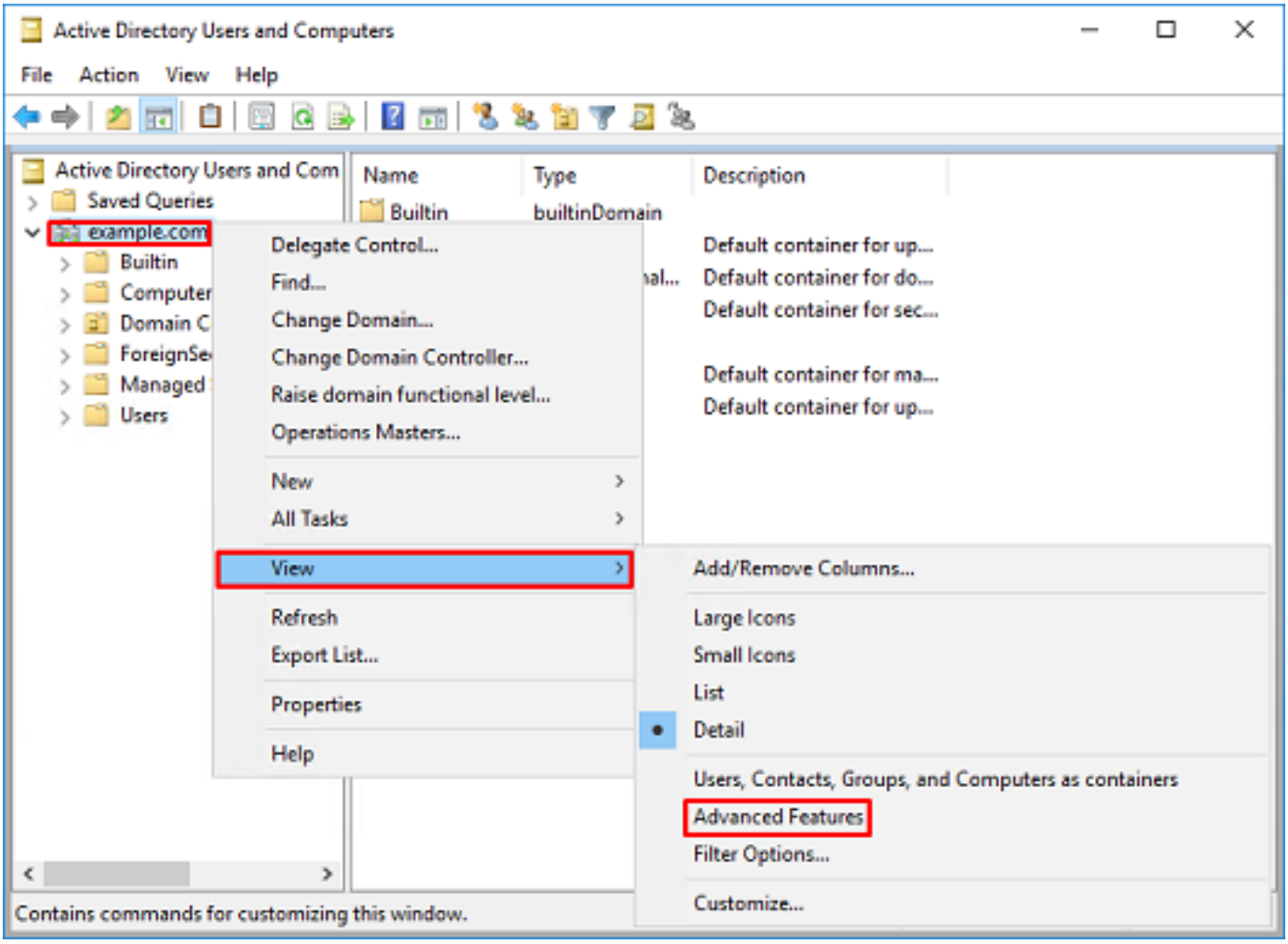


LDAP 기본 DN 확인

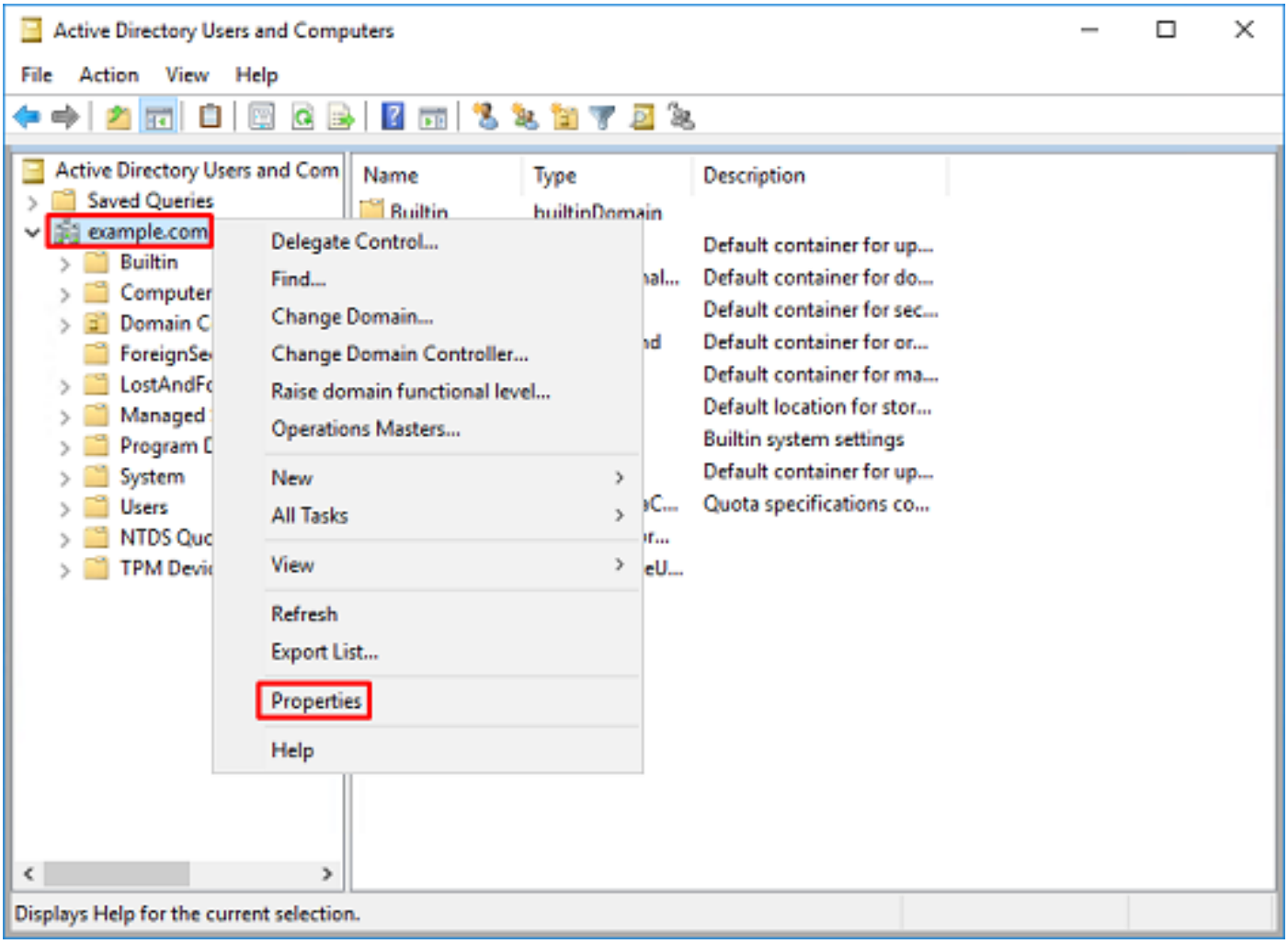
1. AD 사용자 및 컴퓨터를 엽니다.



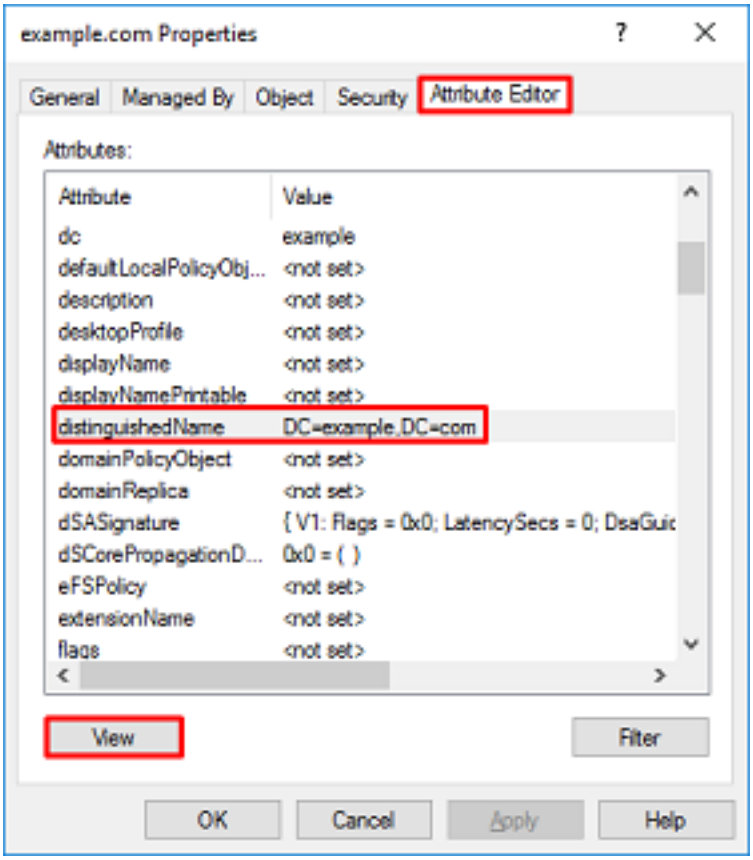
2. 루트 도메인을 마우스 왼쪽 버튼으로 클릭하고(컨테이너를 열려면) 루트 도메인을 마우스 오른쪽 버튼으로 클릭한 다음 **View(보기)**로 이동하고 **Advanced Features(고급 기능)**를 클릭합니다.



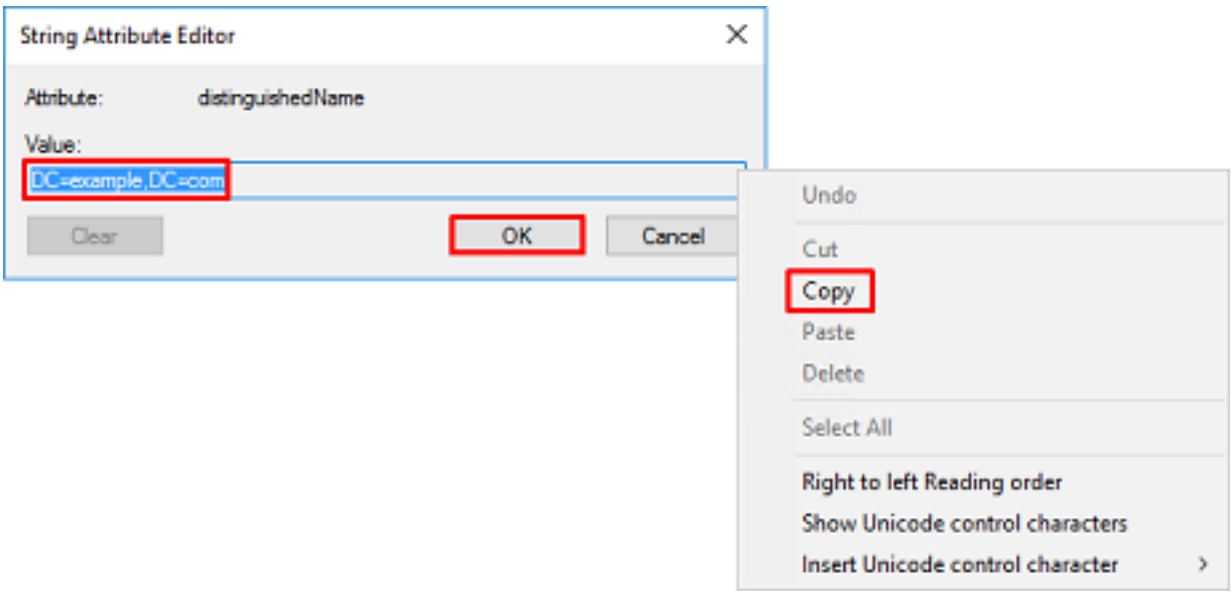
3. 이렇게 하면 AD 개체 아래의 추가 속성을 볼 수 있습니다.예를 들어, root example.com의 DN을 찾으려면 **example.com을** 마우스 오른쪽 버튼으로 클릭한 다음 **Properties로 이동합니다**.

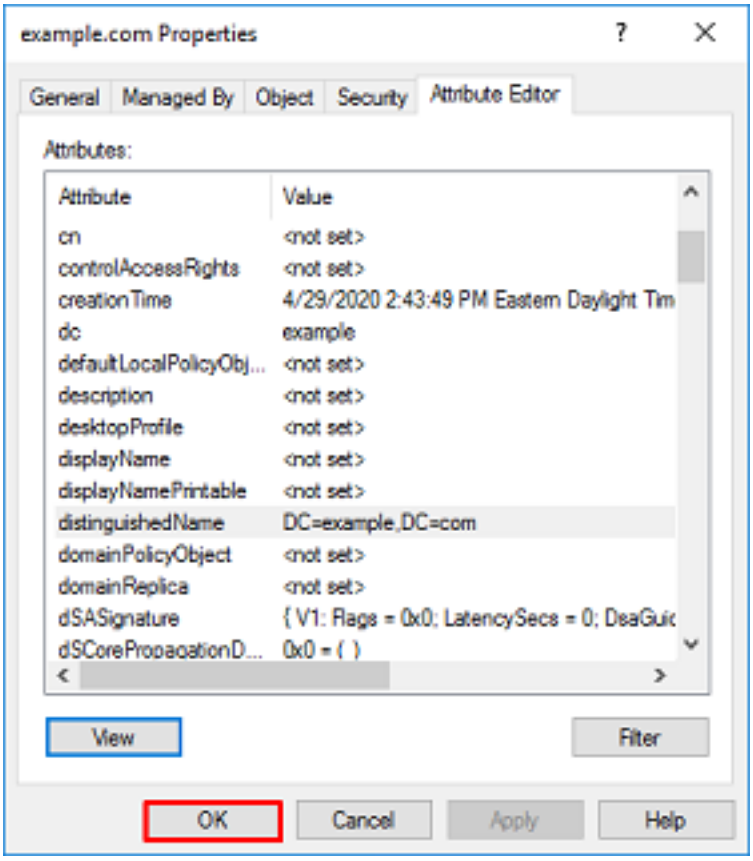


4. **등록 정보**에서 **속성 편집기** 탭을 클릭합니다.Attributes(특성) 아래에서 distinguishedName을 찾은 다음 **보기**를 클릭합니다.

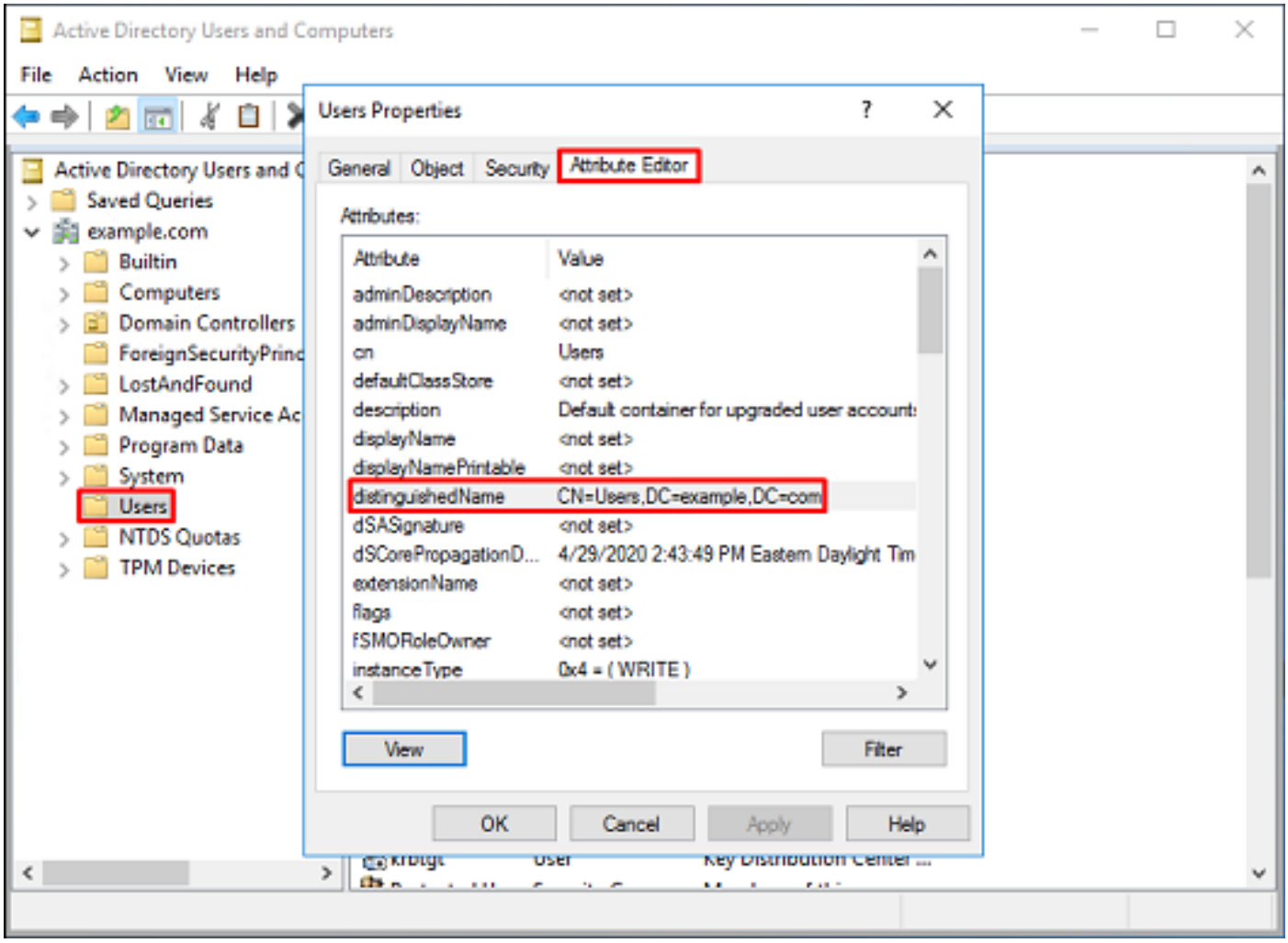


5. 이렇게 하면 나중에 DN을 복사하여 FDM에 붙여넣을 수 있는 새 창이 열립니다.이 예에서 루트 DN은 DC=example, DC=com입니다.값을 복사합니다.**OK(확인)**를 클릭하여 String Attribute Editor(문자열 속성 편집기) 창을 종료하고 **OK(확인)를** 다시 클릭하여 Properties(속성)를 종료합니다.

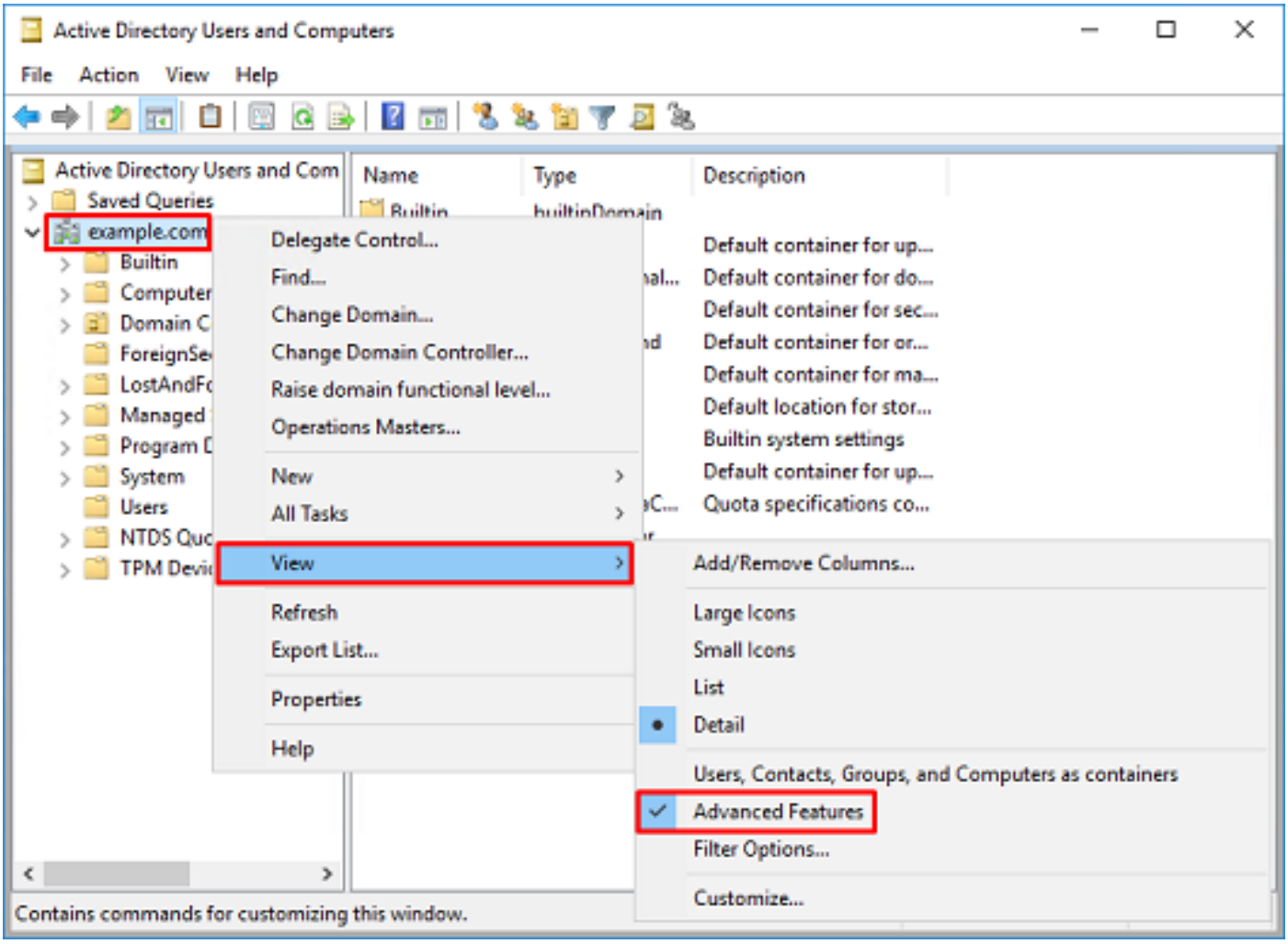




AD 내의 여러 객체에 대해 이 작업을 수행할 수 있습니다.예를 들어 다음 단계는 사용자 컨테이너의 DN을 찾는 데 사용됩니다.



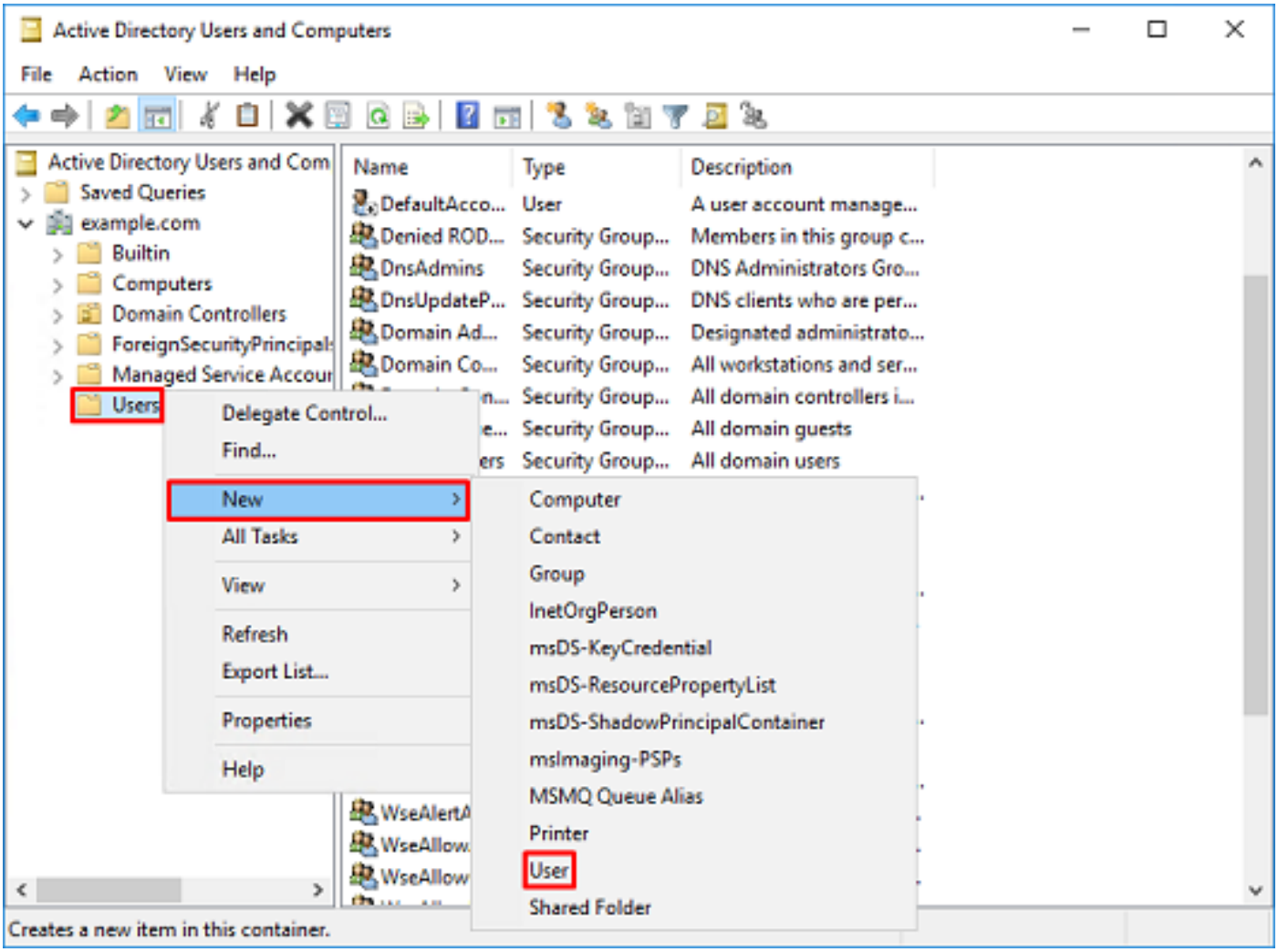
6. 고급 기능 보기를 제거할 수 있습니다.루트 DN을 마우스 오른쪽 버튼으로 클릭하고 **View(보기)**로 이동한 다음 **Advanced Features(고급 기능)**를 한 번 더 클릭합니다.



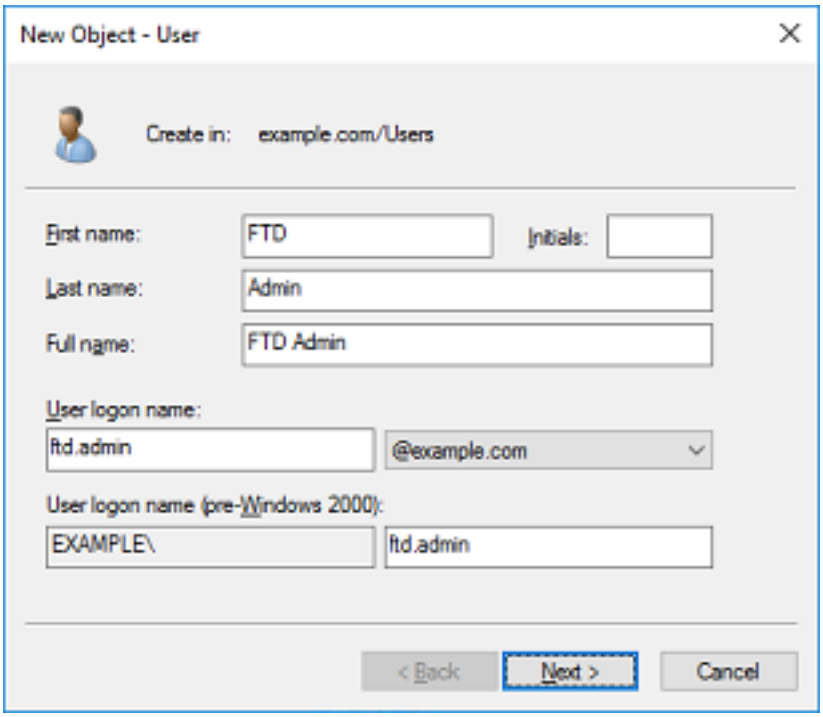
FTD 계정 생성

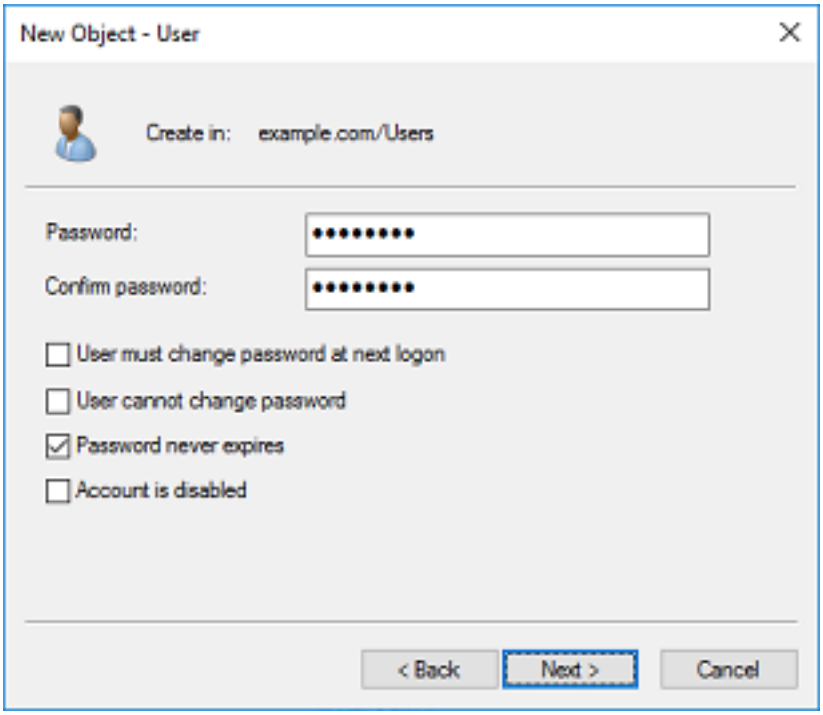
이 사용자 계정을 사용하면 사용자 및 그룹을 검색하고 인증하기 위해 FDM 및 FTD를 AD에 바인딩할 수 있습니다.별도의 FTD 계정을 생성하는 목적은 바인딩에 사용된 자격 증명이 손상된 경우 네트워크 내의 다른 곳에서 무단 액세스를 방지하는 것입니다.이 계정은 기본 DN의 범위 내에 있을 필요가 없습니다.

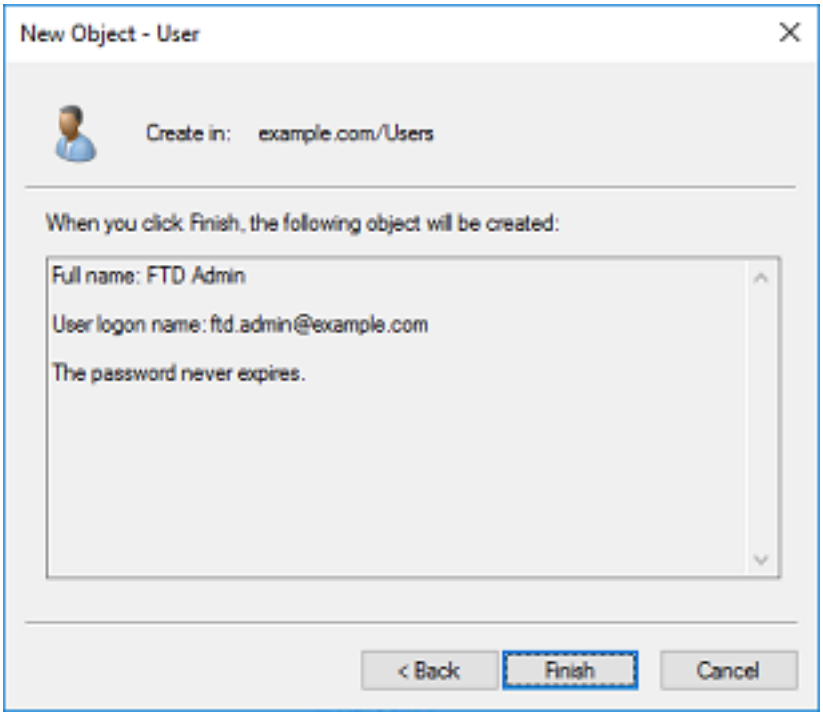
1. **Active Directory 사용자 및 컴퓨터**에서 FTD 계정이 추가될 컨테이너/조직을 마우스 오른쪽 버튼으로 클릭합니다.이 컨피그레이션에서는 사용자 이름 ftd.admin@example.com의 사용자 이름 아래에 FTD 계정이 **추가됩니다.사용자**를 마우스 오른쪽 단추로 클릭한 다음 새로 만들기 **> 사용자를 클릭합니다**.



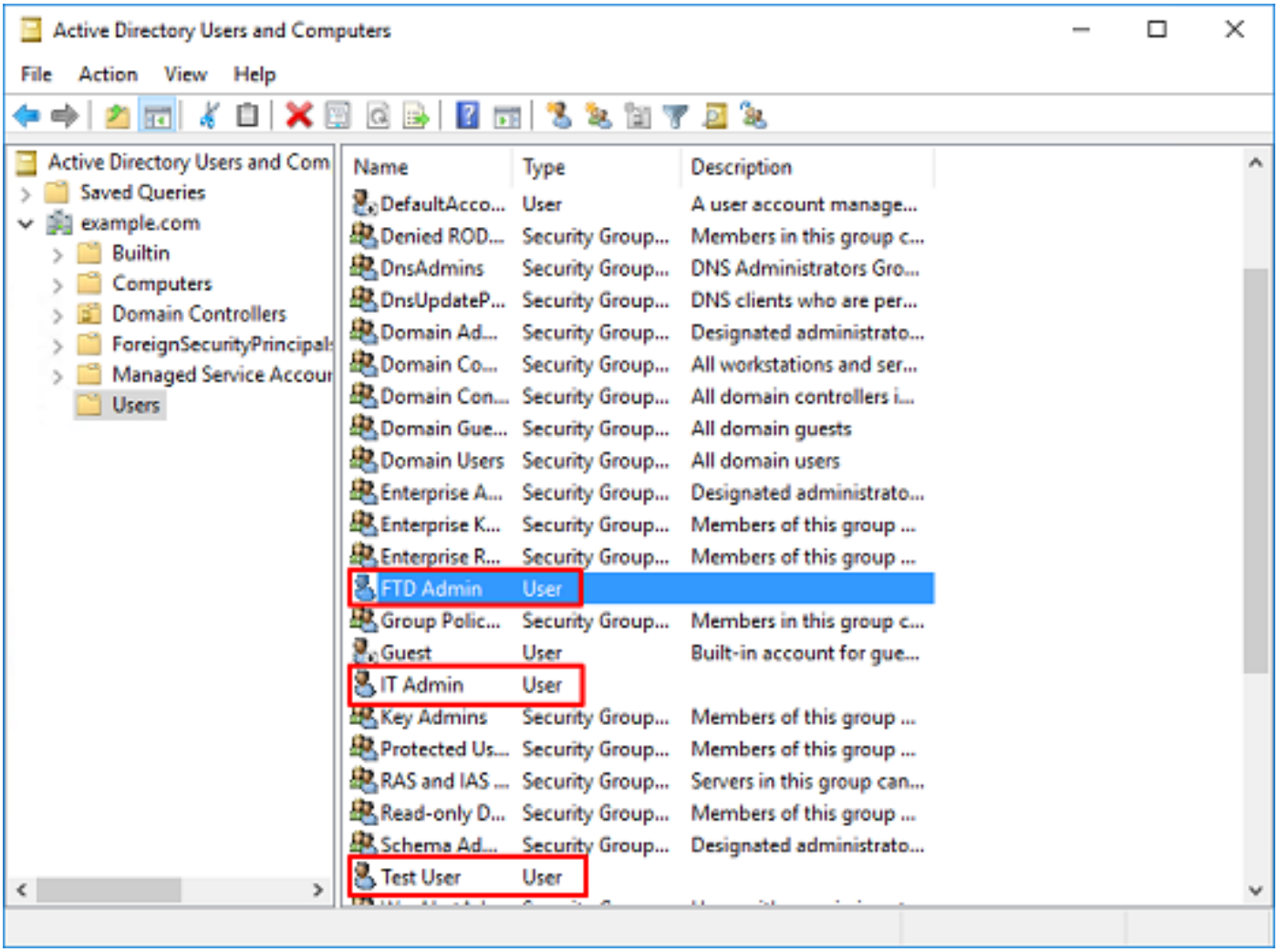
2. **신규 객체 - 사용자** 마법사를 탐색합니다.







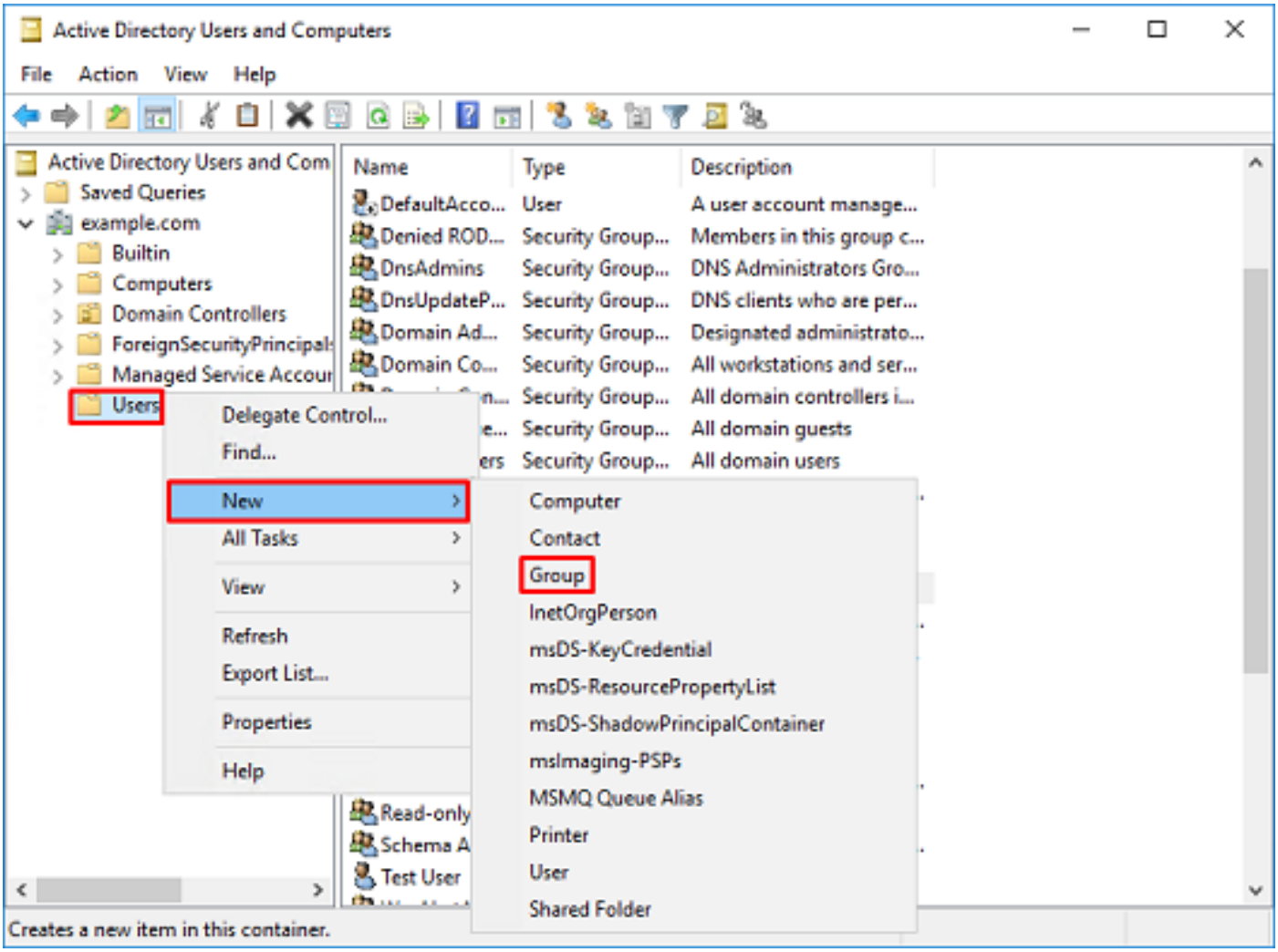
3. FTD 계정이 생성되었는지 확인합니다.또한 두 개의 추가 계정, 즉 **IT 관리자** 및 **테스트 사용자가 생성되었습니다**.



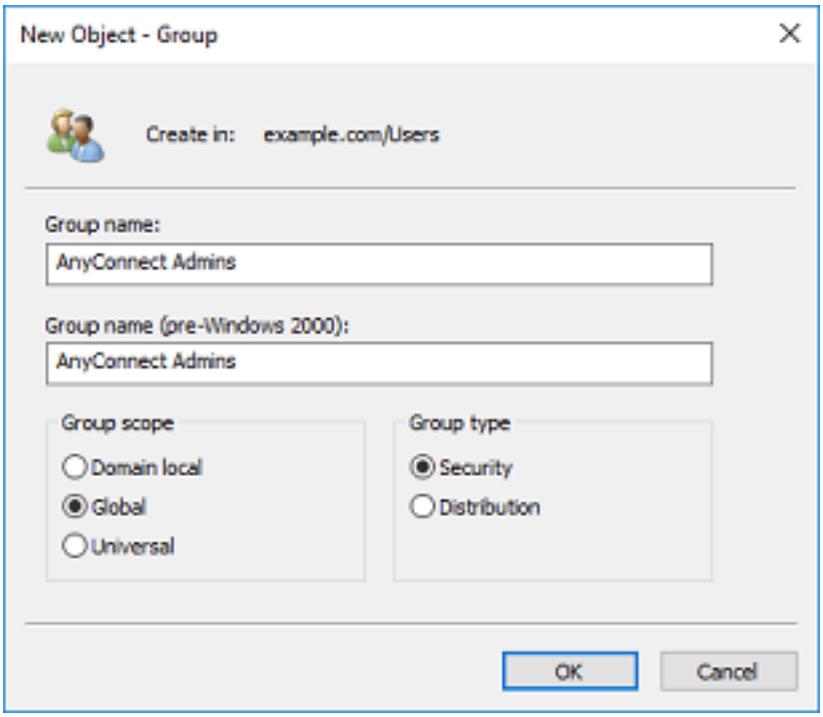
AD 그룹 생성 및 AD 그룹에 사용자 추가(선택 사항)

인증에는 필요하지 않지만, 여러 사용자에게 액세스 정책을 적용하고 LDAP 권한 부여를 적용하는 데 그룹을 사용할 수 있습니다.이 컨피그레이션 가이드에서 그룹은 나중에 FDM 내의 사용자 ID를 통해 액세스 제어 정책 설정을 적용하는 데 사용됩니다.

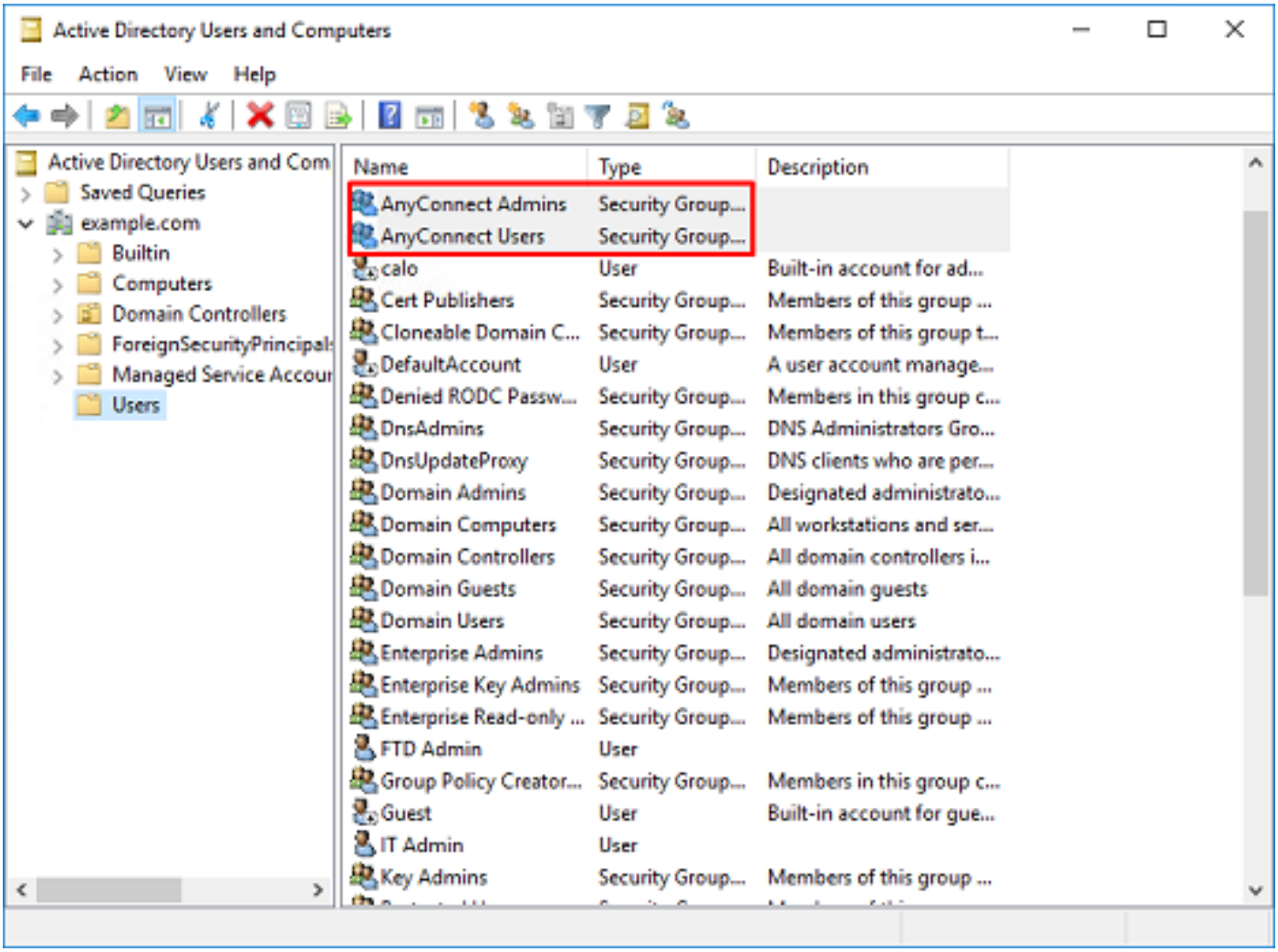
1. **Active Directory 사용자 및 컴퓨터**에서 새 그룹이 추가될 컨테이너/조직을 마우스 오른쪽 단추로 클릭합니다.이 예에서 그룹 AnyConnect **Admins가** Users 컨테이너 아래에 추가됩니다.**사용자**를 마우스 오른쪽 단추로 클릭한 다음 새로 만들기 **> 그룹을 클릭합니다**.



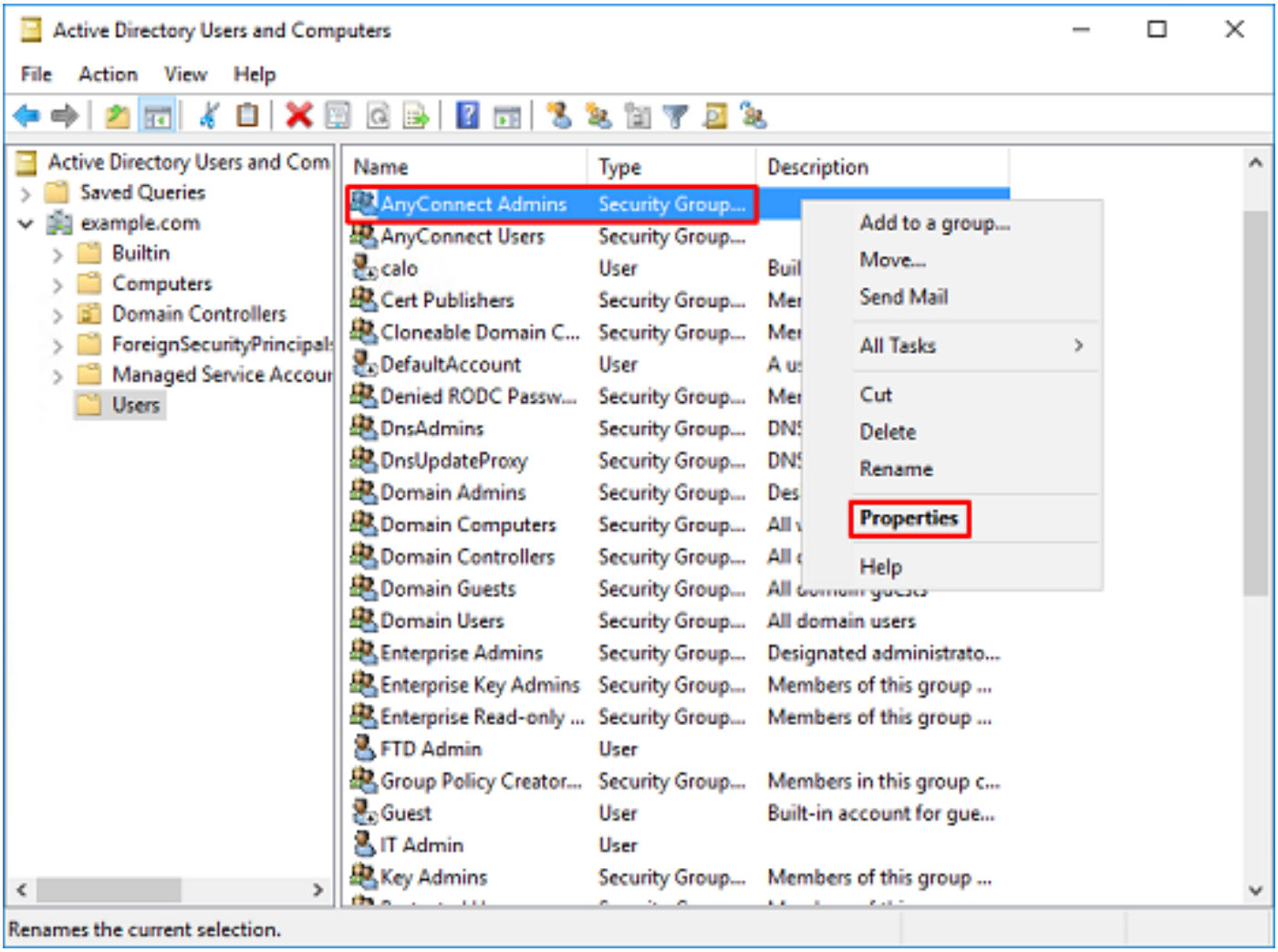
2. 이미지에 표시된 대로 **신규 객체 - 그룹** 마법사를 탐색합니다.



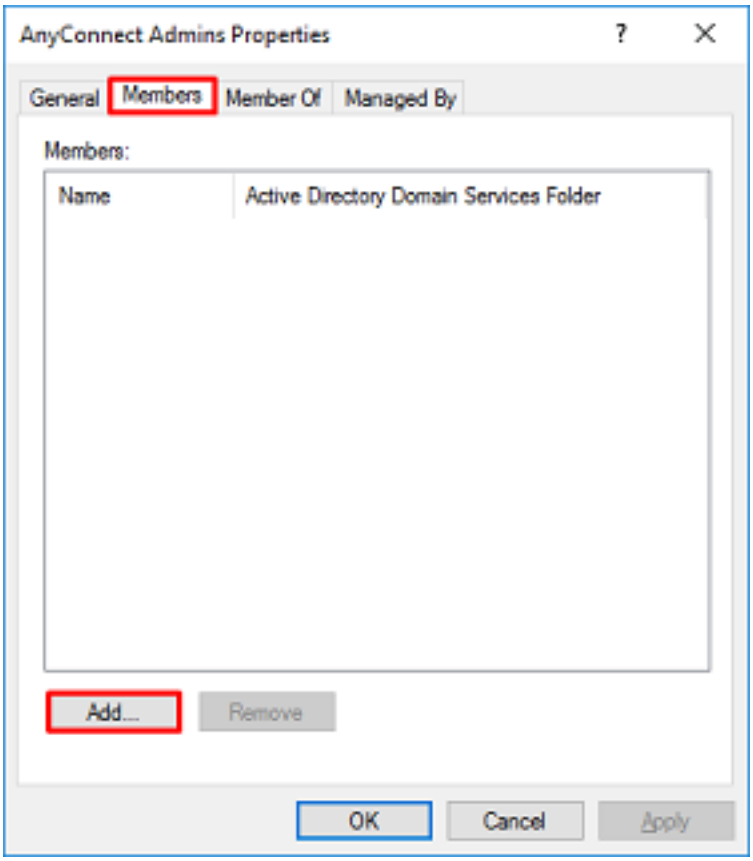
3. 그룹이 생성되었는지 확인합니다.AnyConnect **사용자** 그룹도 생성되었습니다.



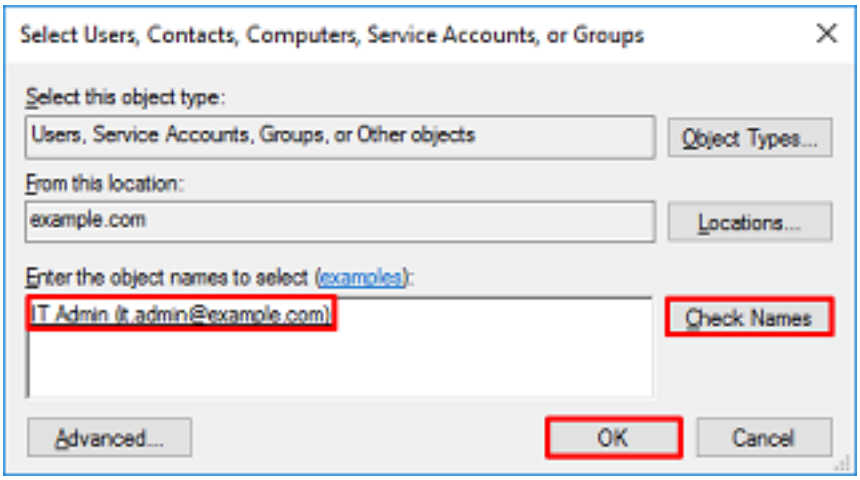
4. 사용자를 추가할 그룹을 마우스 오른쪽 단추로 클릭한 다음 **속성**을 선택합니다.이 컨피그레이션에서는 사용자 **IT 관리자**가 AnyConnect Admins 그룹에 추가되고 사용자 **테스트 사용자**가 AnyConnect **사용자** 그룹에 추가됩니다.



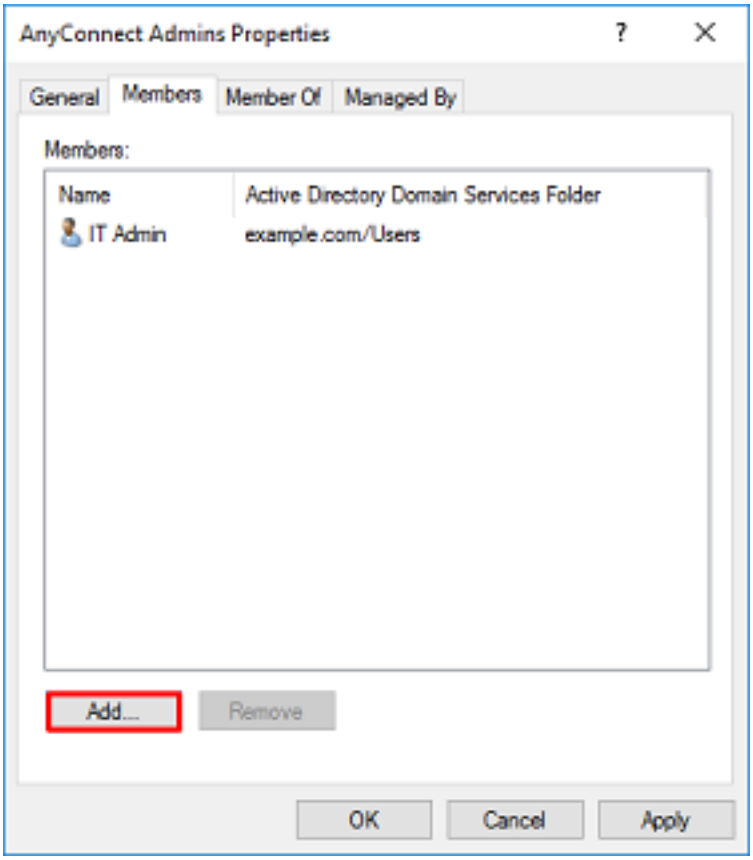
5. **멤버** 탭을 클릭한 다음 이미지에 표시된 대로 추가를 클릭합니다.



필드에 사용자를 입력하고 이름 **확인** 단추를 클릭하여 사용자를 찾습니다.확인되면 OK(확인)를 **클릭합니다**.

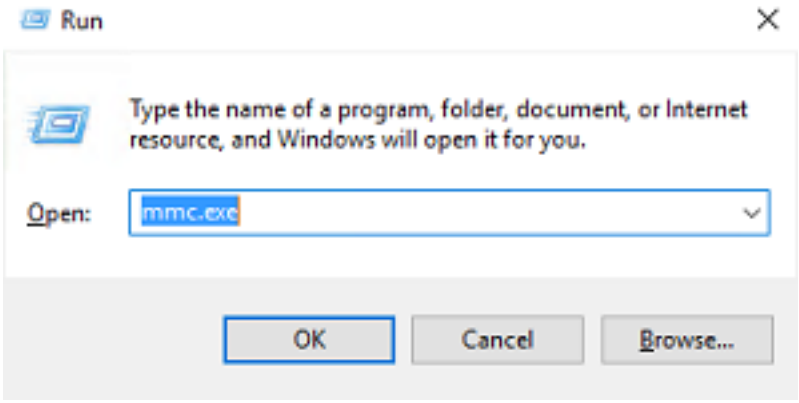


올바른 사용자가 추가되었는지 확인한 다음 **OK** 버튼을 클릭합니다.사용자 테스트 사용자도 동일한 단계를 사용하여 AnyConnect 사용자 그룹에 추가됩니다.

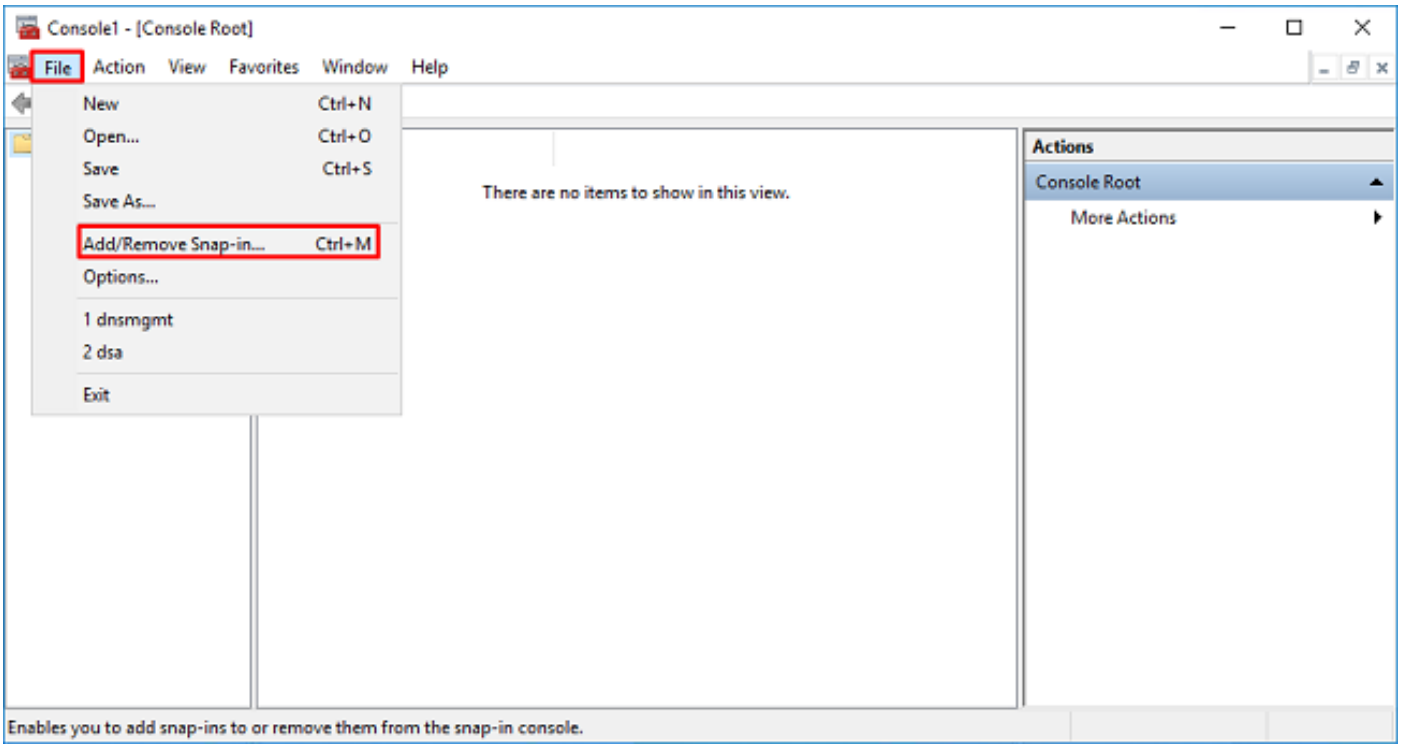


LDAPS SSL 인증서 루트 복사(LDAPS 또는 STARTTLS에만 필요)

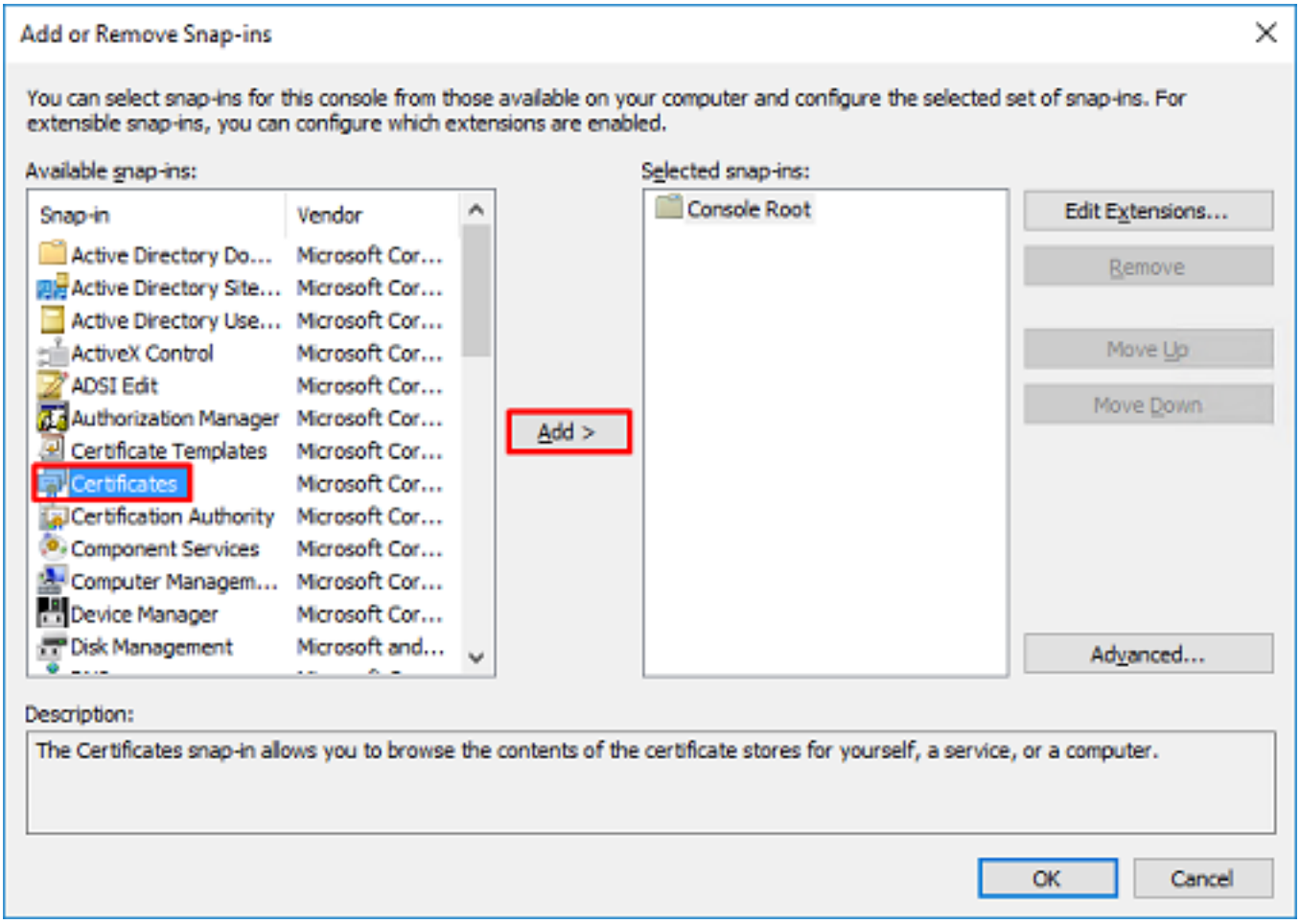
1. **Win+R을** 누르고 mmc.**exe를 입력합니다**.**확인**을 **클릭합니다**.



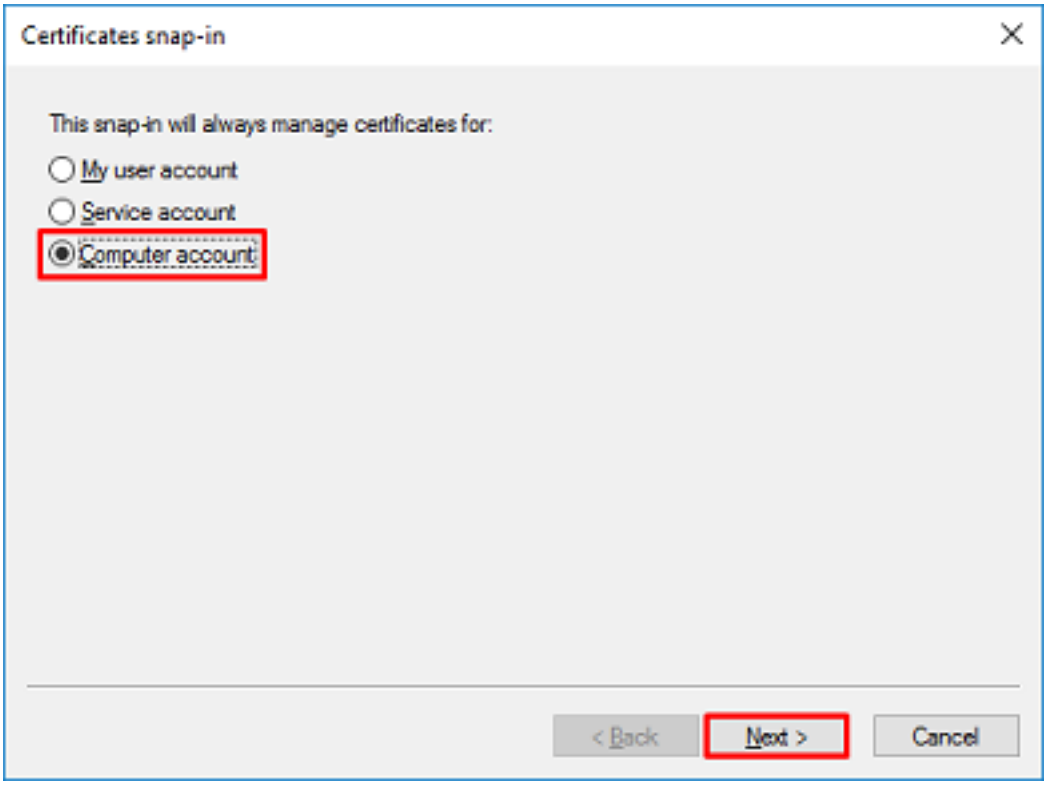
2. **파일 > 스냅인 추가/제거...로 이동합니다.** 이미지에 표시된 것처럼



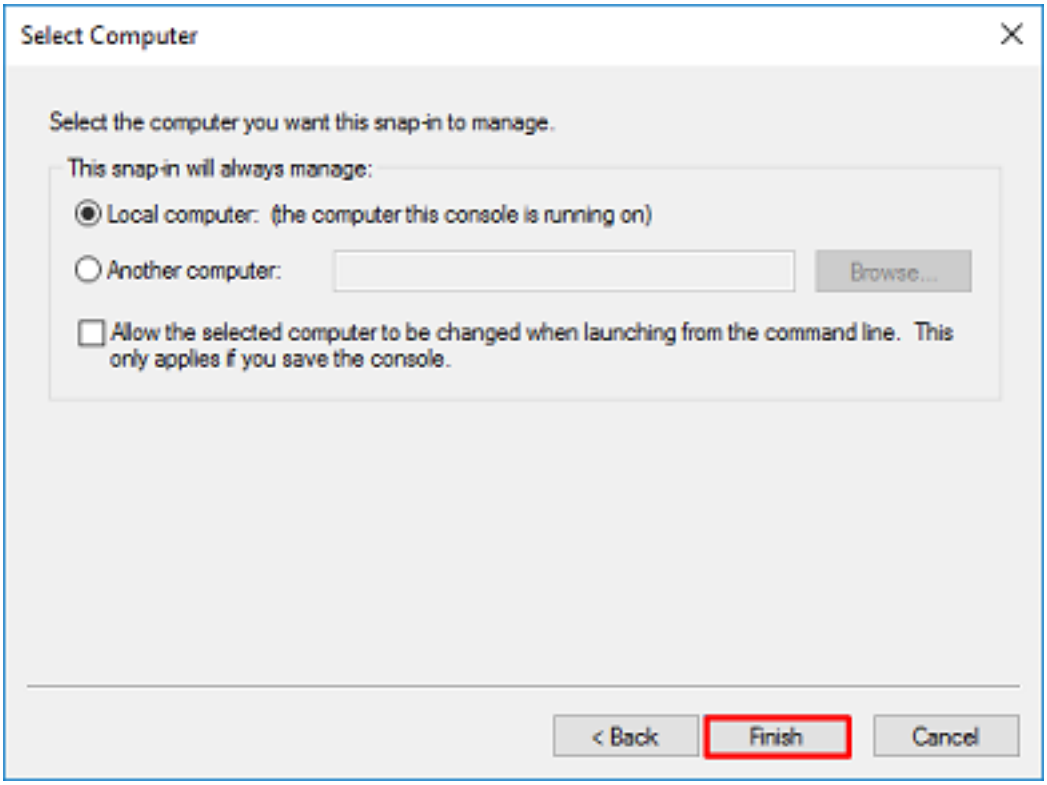
3. 사용 가능한 스냅인에서 **인증서**를 클릭한 다음 **추가**를 클릭합니다.



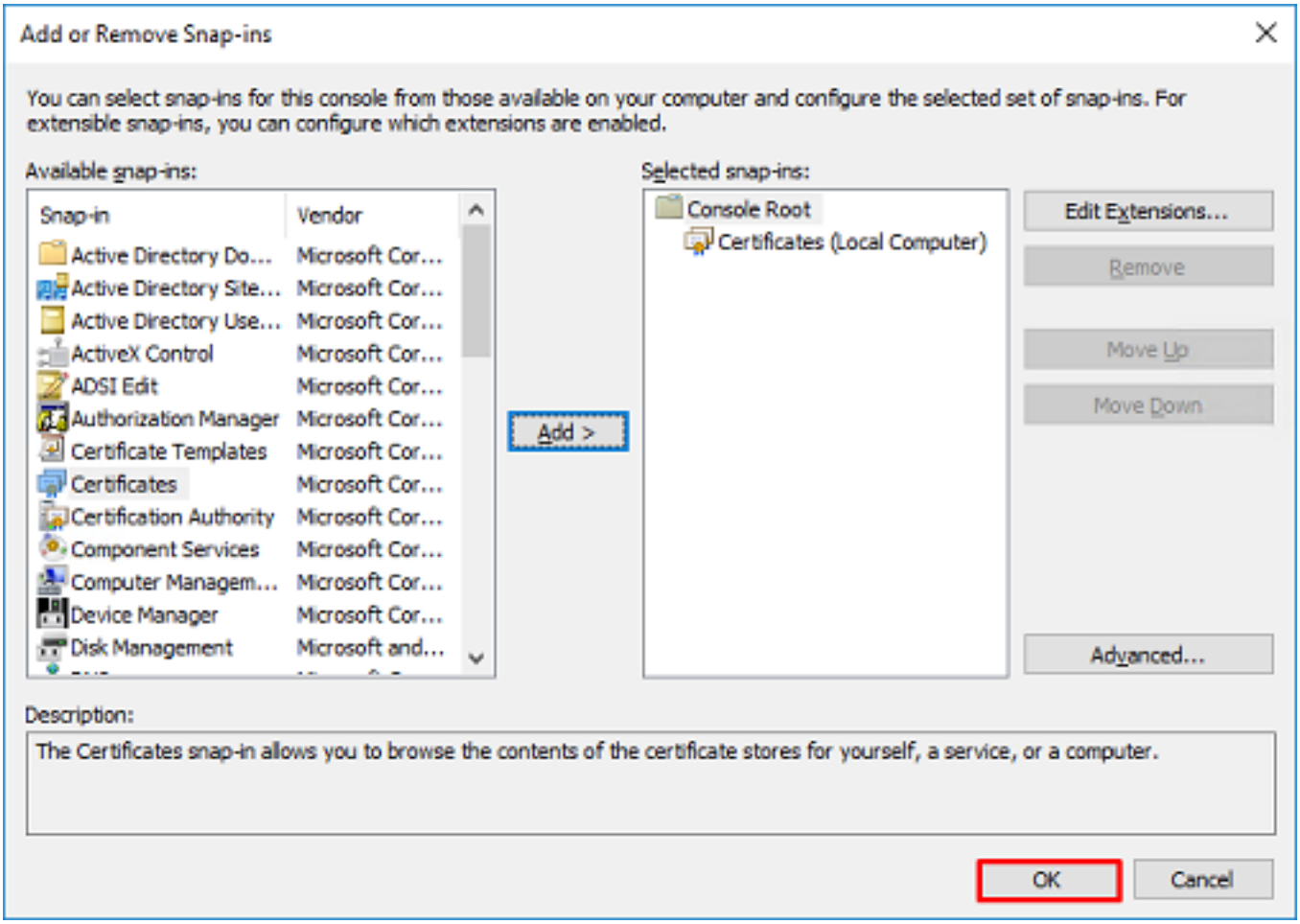
4. **컴퓨터 계정**을 선택한 다음 이미지에 표시된 대로 **다음**을 클릭합니다.



마침을 **클릭합니다**.



5. 확인을 **클릭합니다**.

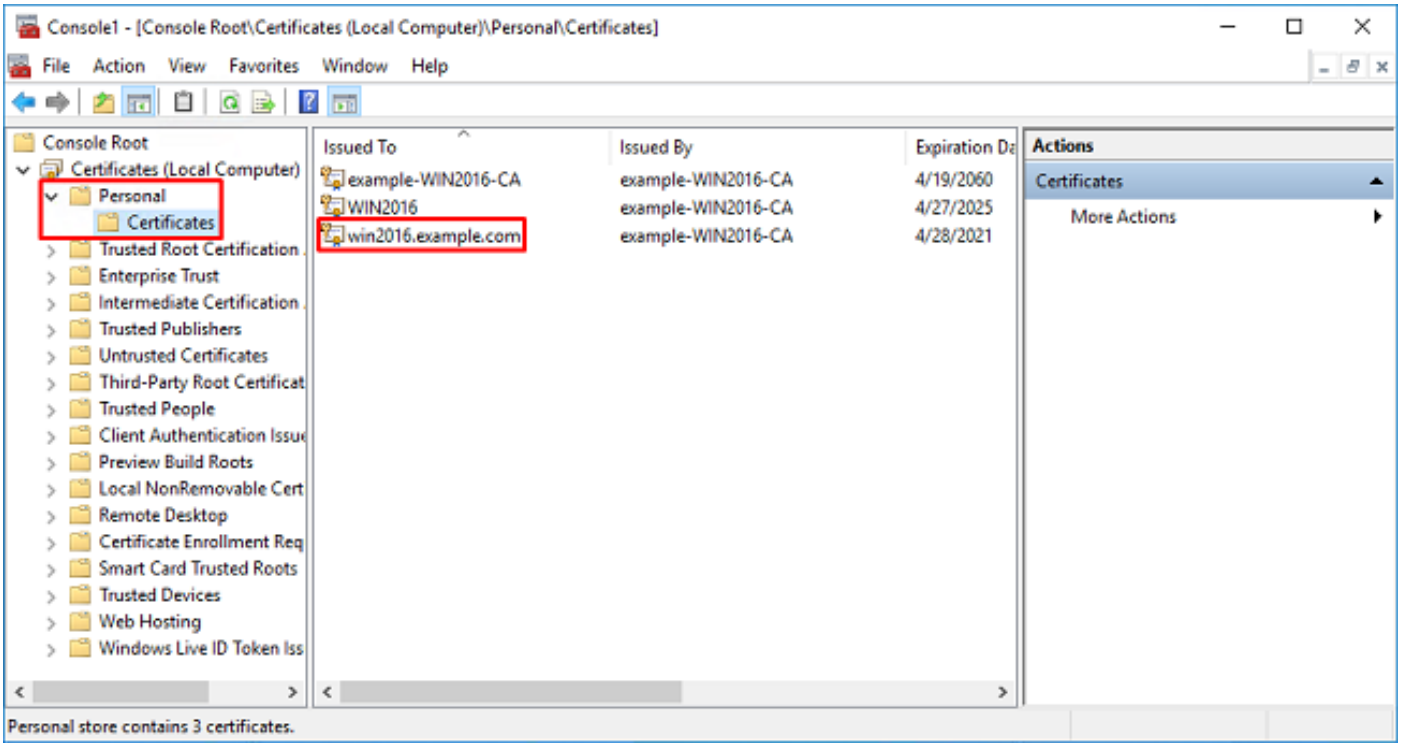


6. **개인** 폴더를 확장한 다음 **인증서**를 클릭합니다.LDAPS에서 사용하는 인증서는 Windows 서버의 FQDN(Fully Qualified Domain Name)에 발급해야 합니다.이 서버에는 3개의 인증서가 나열됩니다.

- WIN2016-CA에 발급된 CA 인증서.

- example-WIN2016-CA가 WIN2016에 발급한 ID 인증서입니다.
- example-WIN2016-CA에서 win2016.example.com에 발급된 ID 인증서입니다.

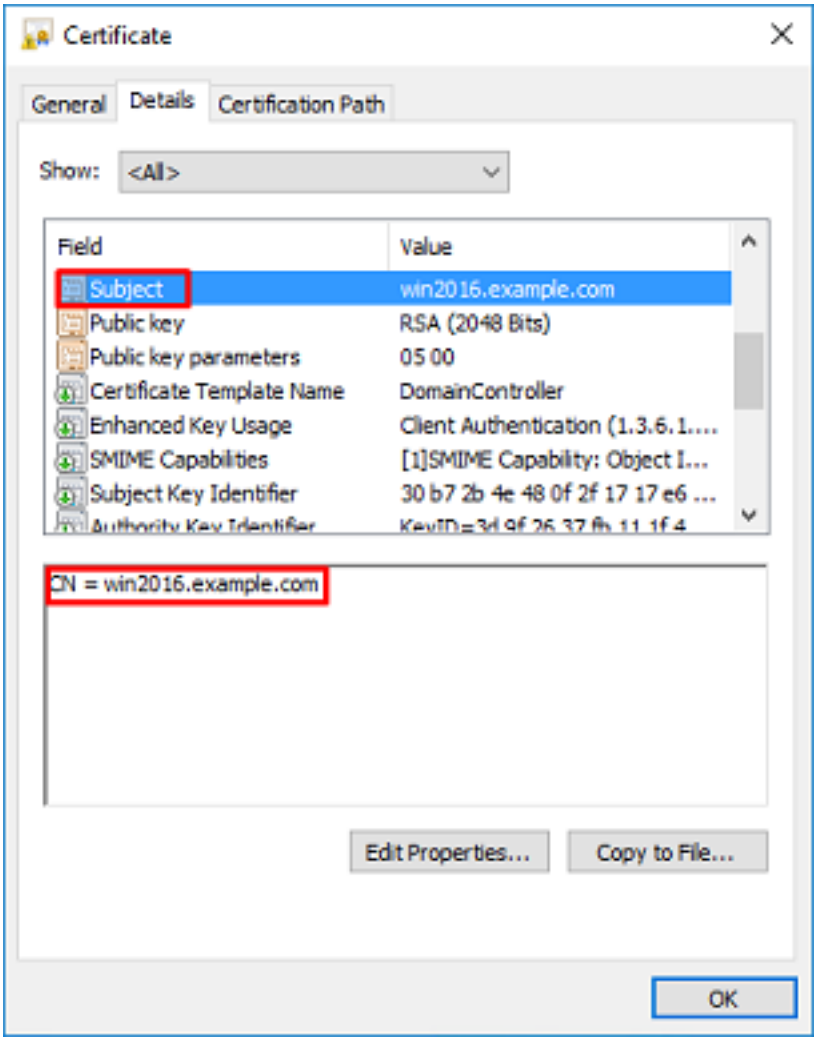
이 컨피그레이션 가이드에서 FQDN은 win2016.example.com이므로 처음 2개의 인증서는 LDAPS SSL 인증서로 사용할 수 없습니다.win2016.example.com에 발급된 ID 인증서는 Windows Server CA 서비스에서 자동으로 발급된 인증서입니다.인증서를 두 번 클릭하여 세부사항을 확인합니다.

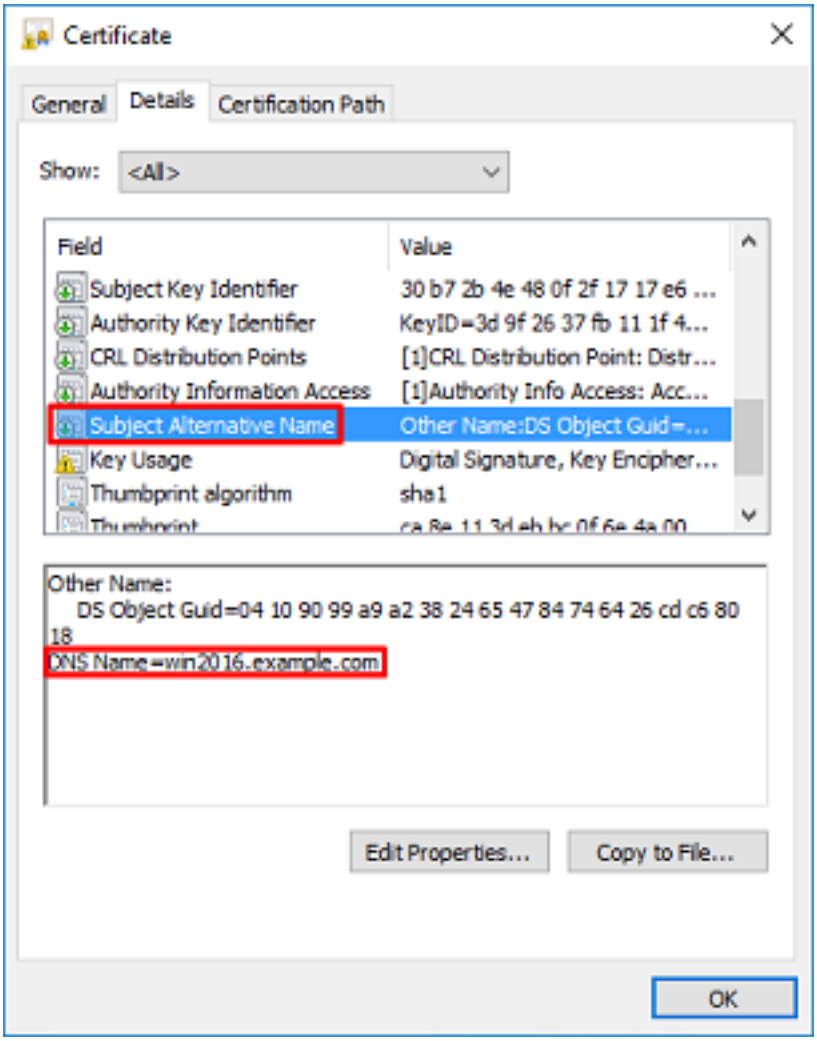


7. LDAPS SSL 인증서로 사용하려면 인증서가 다음 요구 사항을 충족해야 합니다.

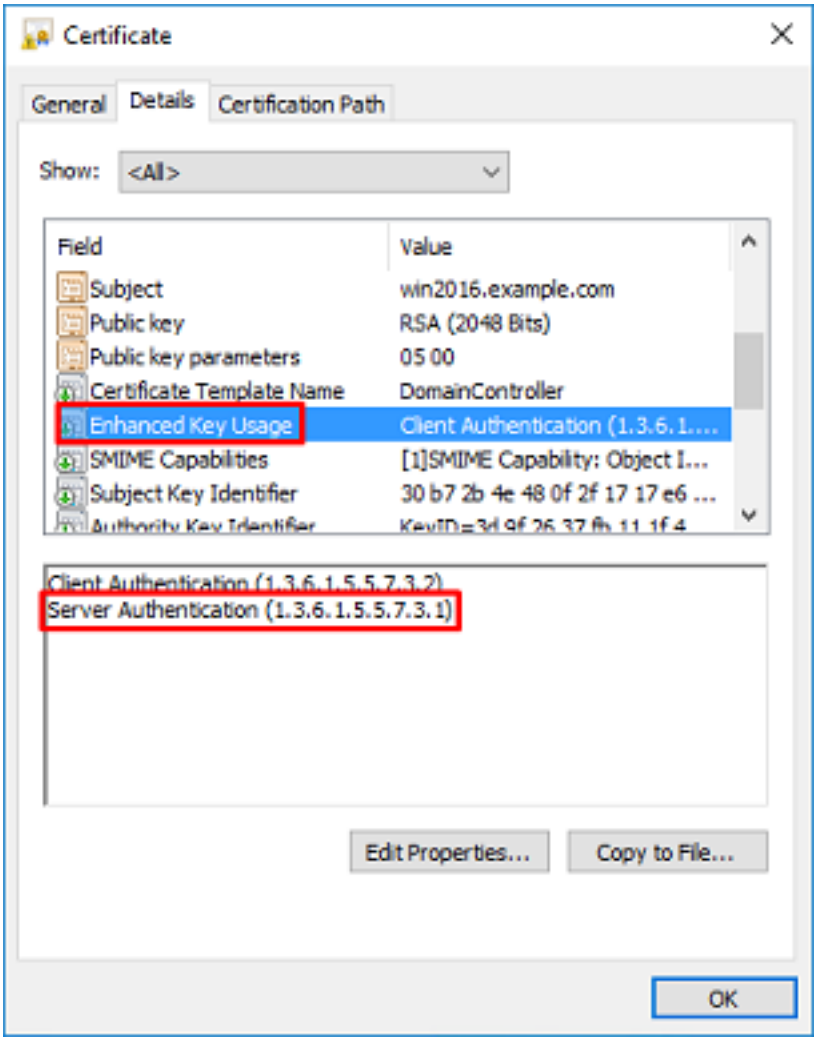
- 일반 이름 또는 DNS 주체 대체 이름이 Windows 서버의 FQDN과 일치합니다.
- 인증서에 Enhanced Key Usage(고급 키 사용) 필드 아래에 서버 인증이 있습니다.

인증서의 Details(세부사항) 탭 아래의 **Subject(주체)** 및 **Subject Alternative Name(주체 대체 이름)** 아래에 FQDN **win2016.example.com이** 있습니다.

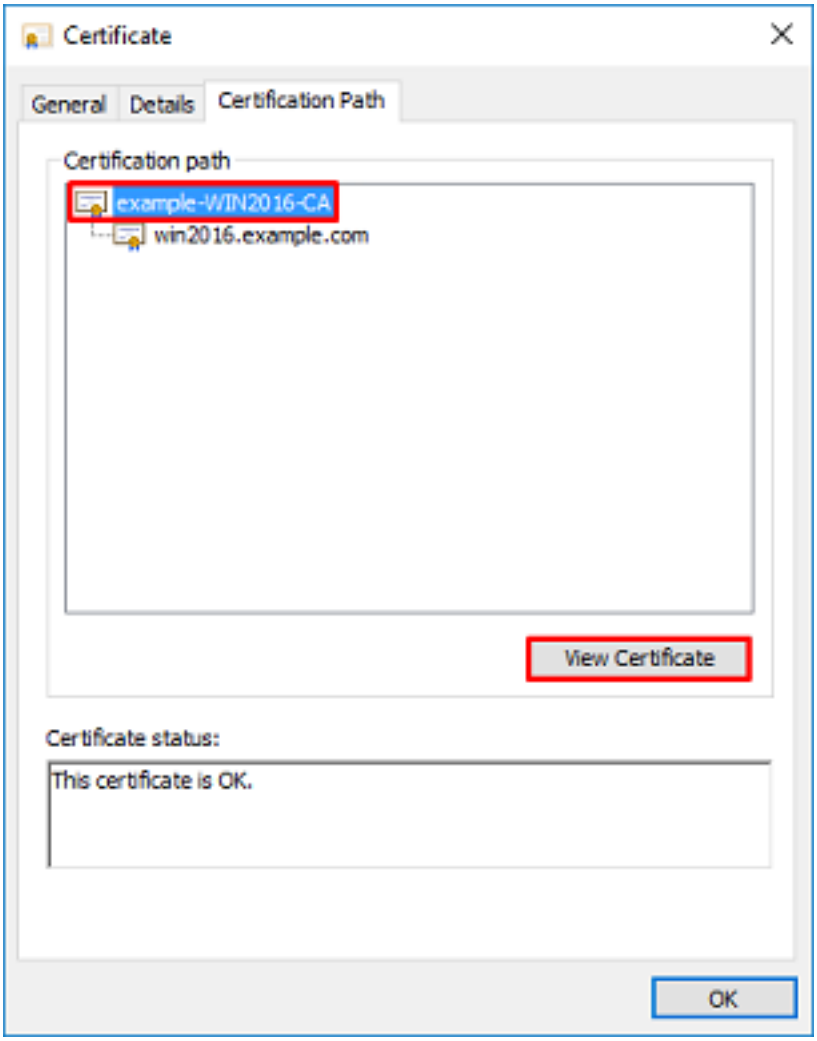

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...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



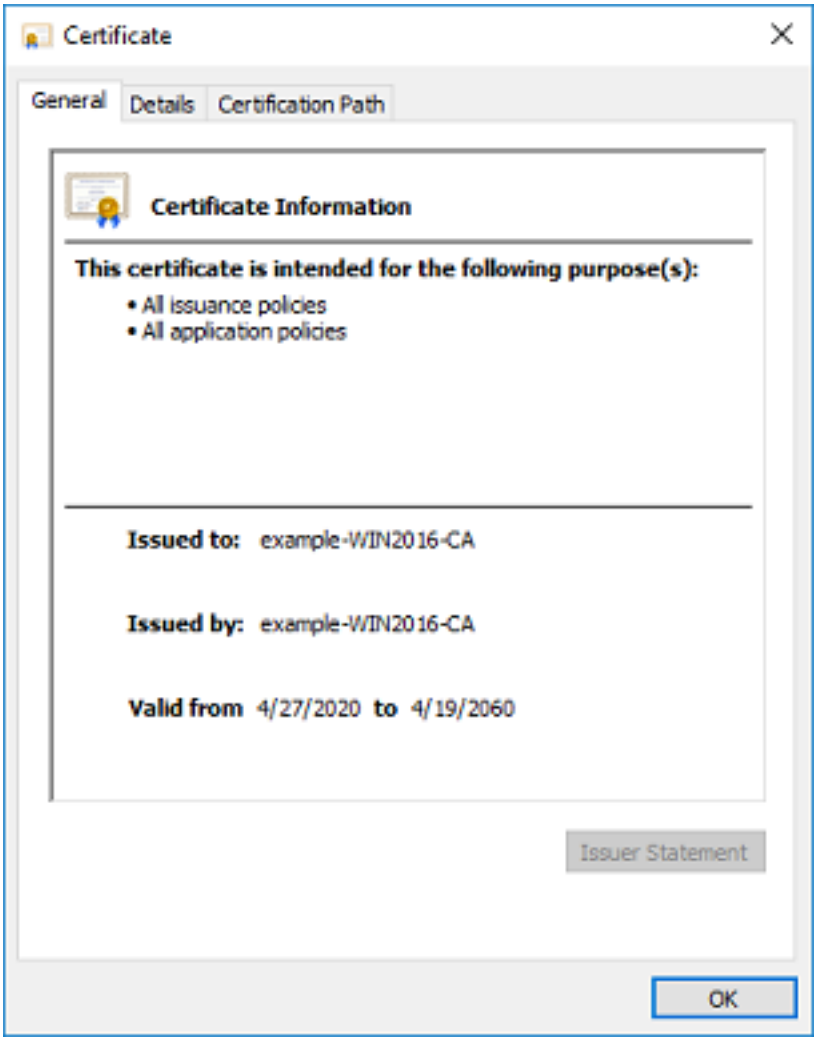
Enhanced **Key Usage(고급 키 사용)**에서 **Server Authentication(서버 인증)**이 표시됩니다.



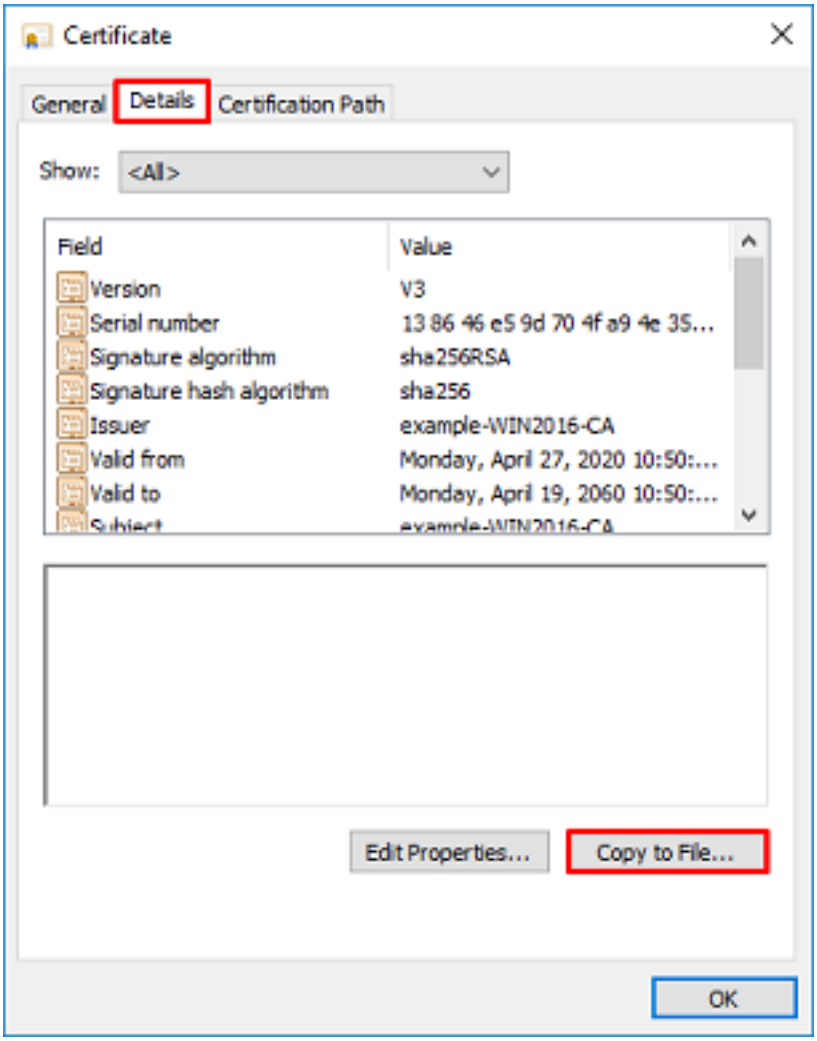
8. 확인되면 **인증 경로** 탭으로 이동합니다.루트 CA 인증서여야 하는 상위 인증서를 클릭한 다음 **View Certificate** 버튼을 클릭합니다.



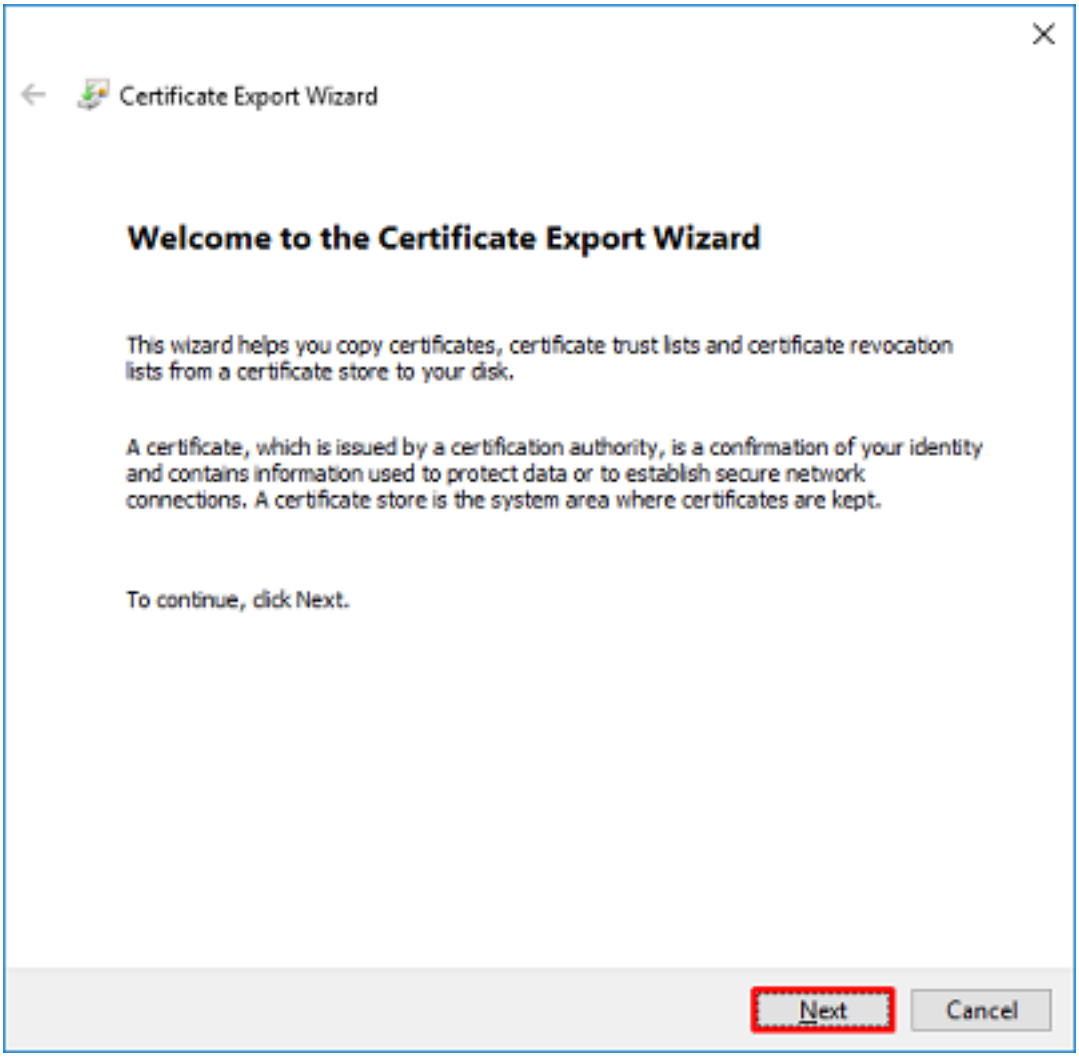
9. 루트 CA 인증서에 대한 인증서 세부 정보가 열립니다.



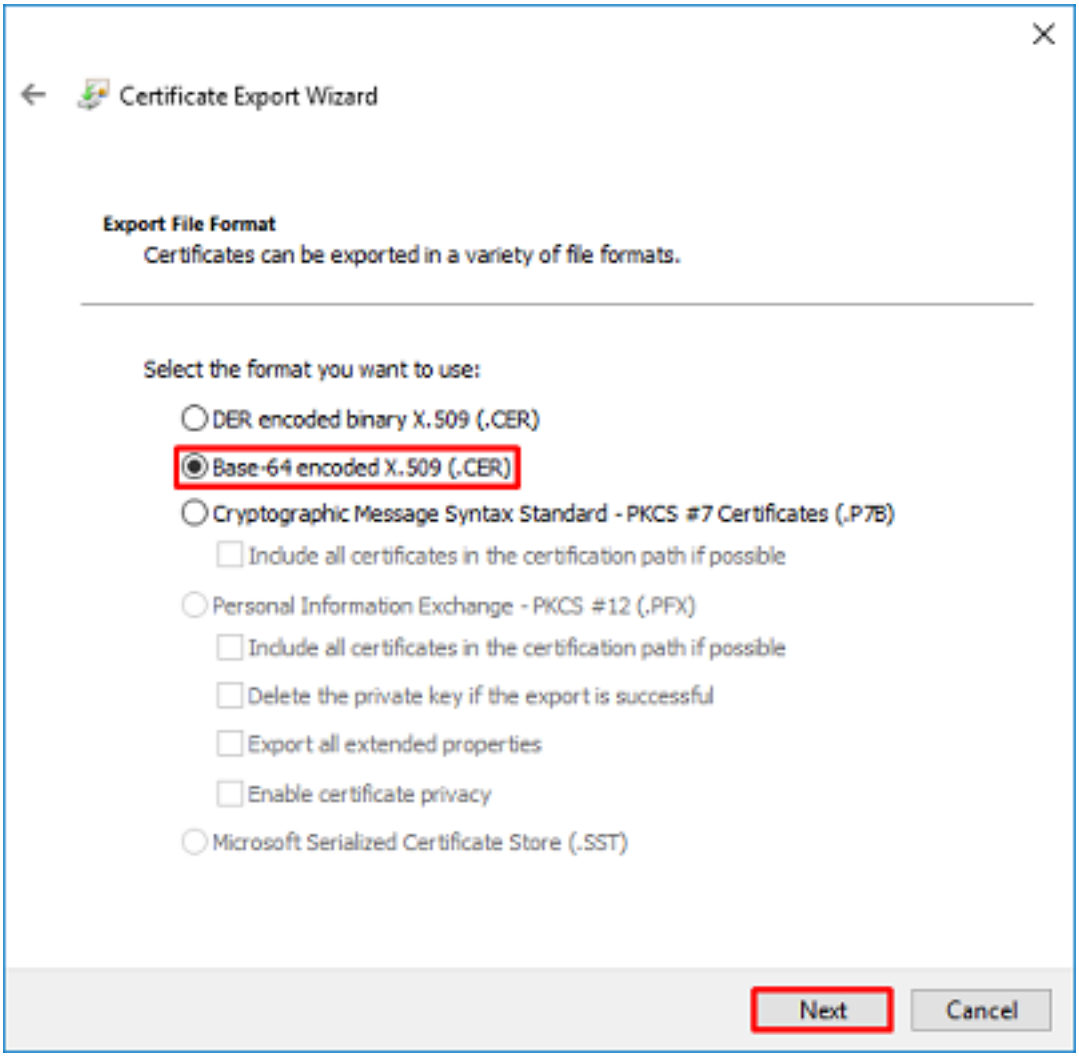
10. **세부 정보** 탭을 열고 **파일에 복사...를 클릭합니다.** 이미지에 표시된 것처럼



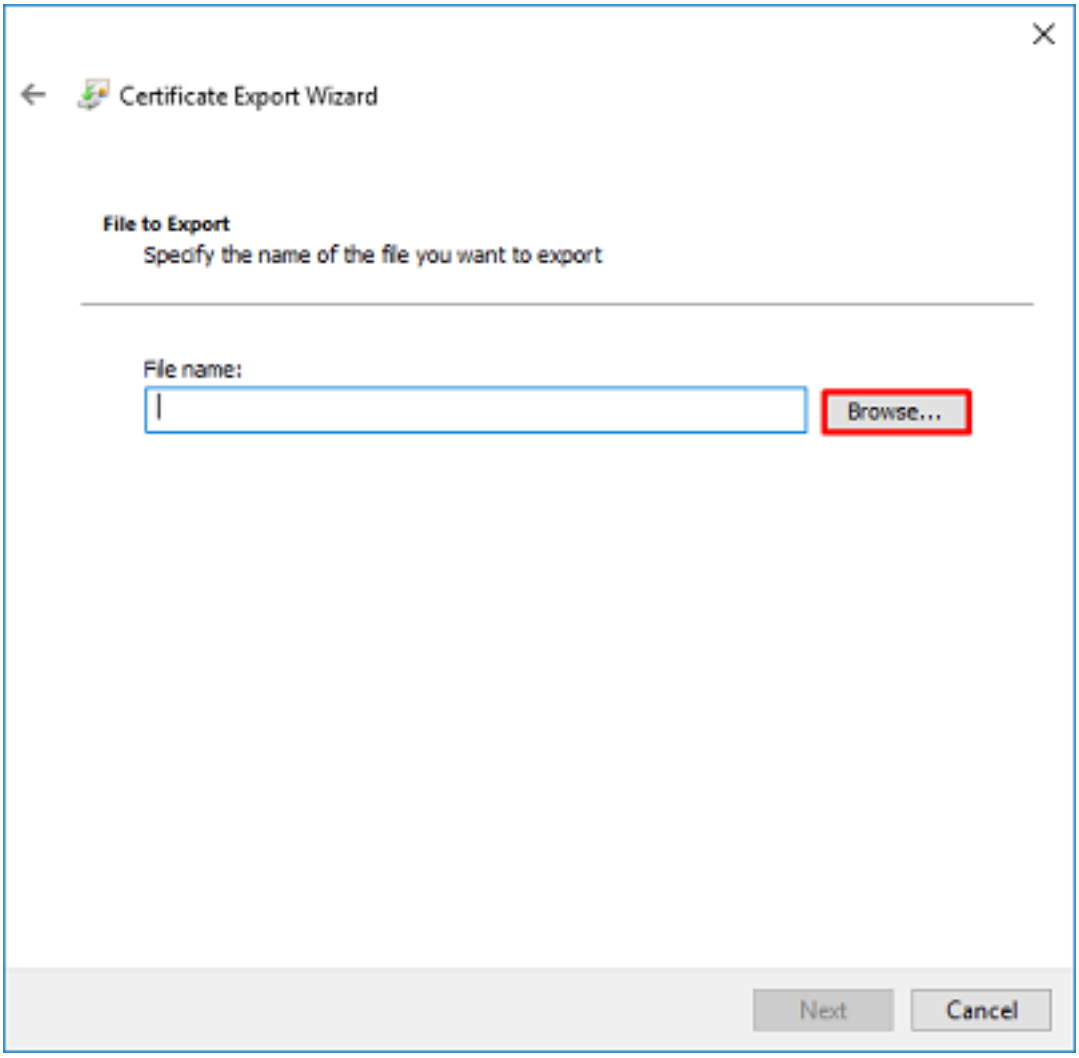
11. 루트 CA를 PEM 형식으로 내보낼 인증서 내보내기 마법사를 탐색합니다.

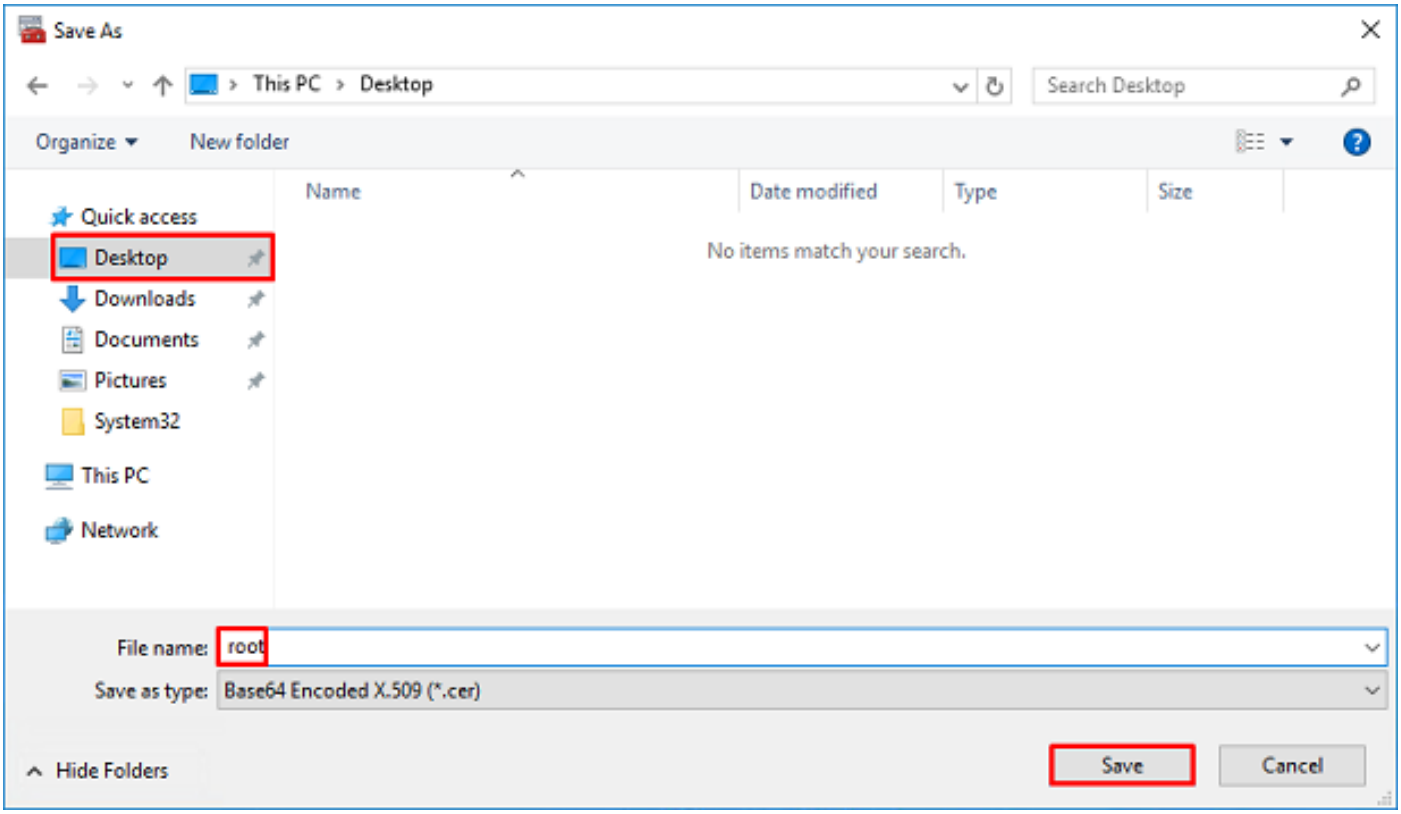


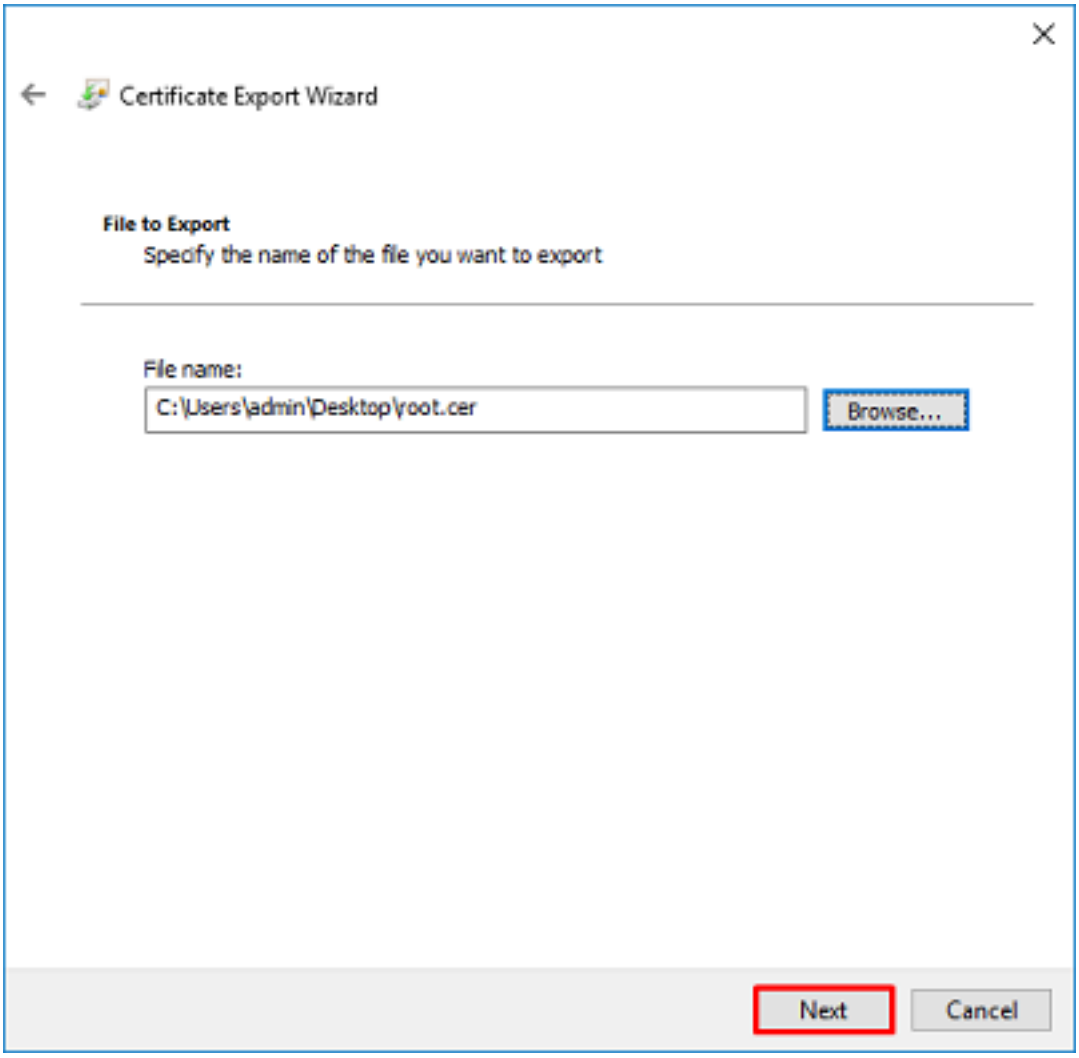
12. Base-64 인코딩 X.509를 선택합니다.



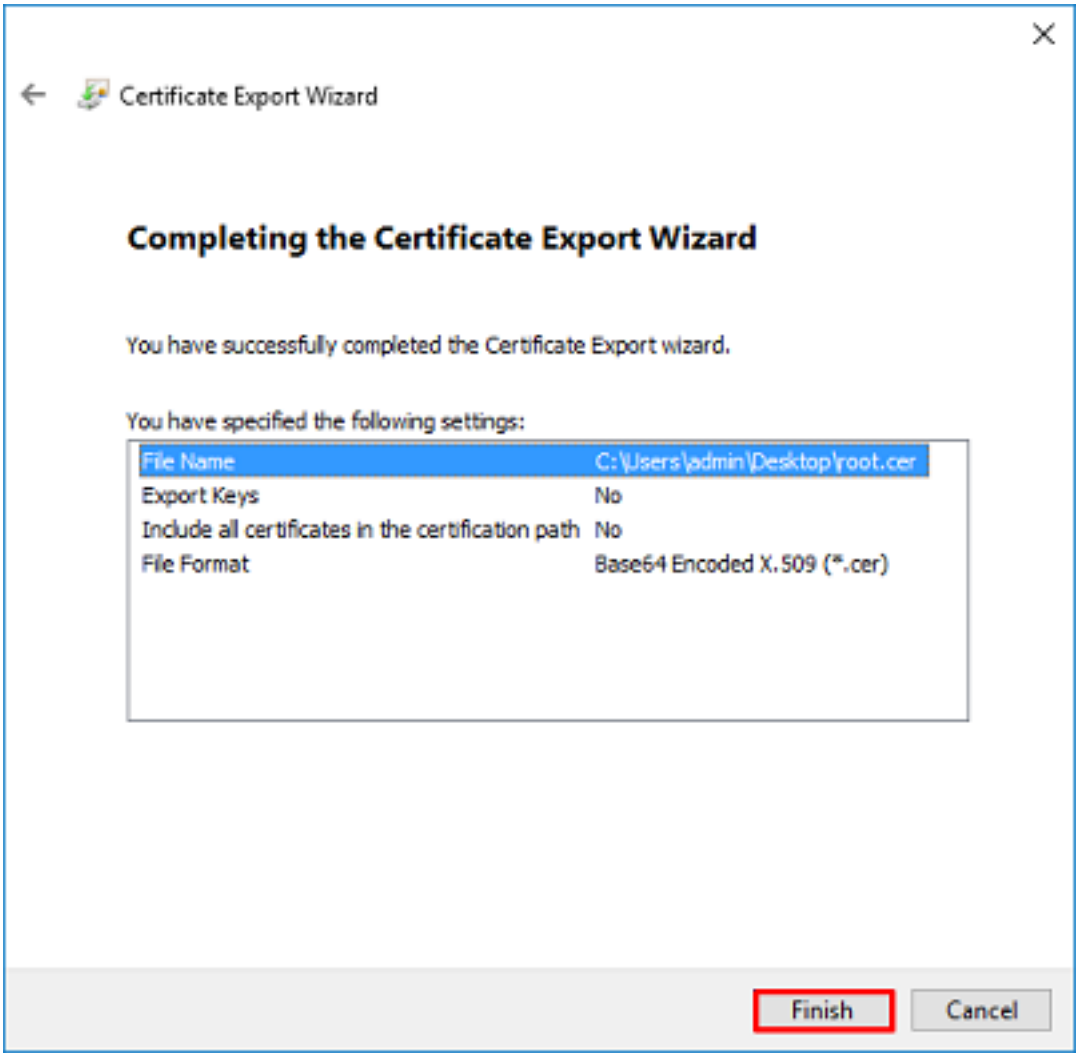
13. 파일의 이름과 내보낼 위치를 선택합니다.


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


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\admin\Desktop\root.cer
Browse...
Next
Cancel

14. 완료를 **클릭합니다**.



15. 이제 해당 위치로 이동하여 메모장이나 다른 텍스트 편집기로 인증서를 엽니다.그러면 PEM 형식 인증서가 표시됩니다.나중에 저장할 수 있습니다.

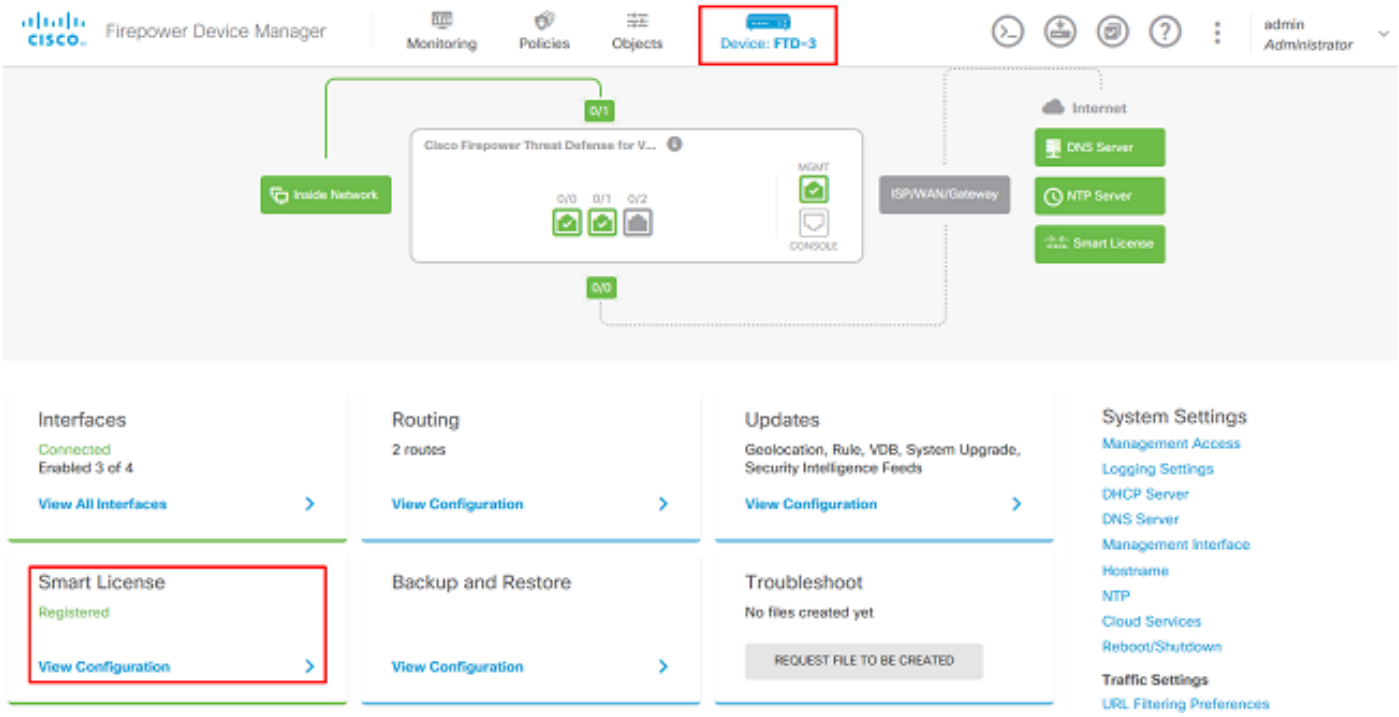
```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
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-----
```

FDM 구성

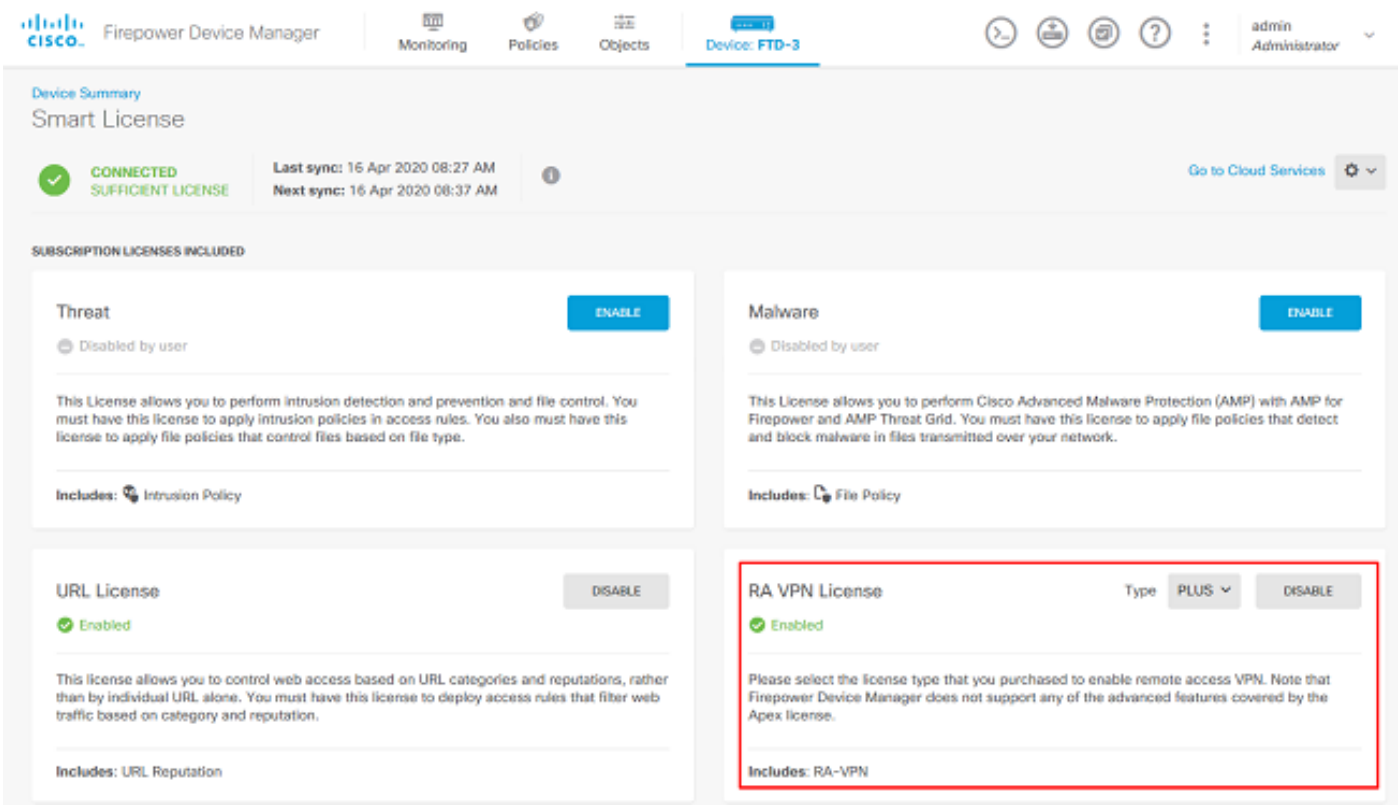
라이센스 확인

FDM에서 AnyConnect를 구성하려면 FTD를 Smart Licensing 서버에 등록해야 하며 유효한 Plus, Apex 또는 VPN Only 라이센스를 디바이스에 적용해야 합니다.

1. 이미지에 표시된 대로 **Device > Smart License**로 이동합니다.

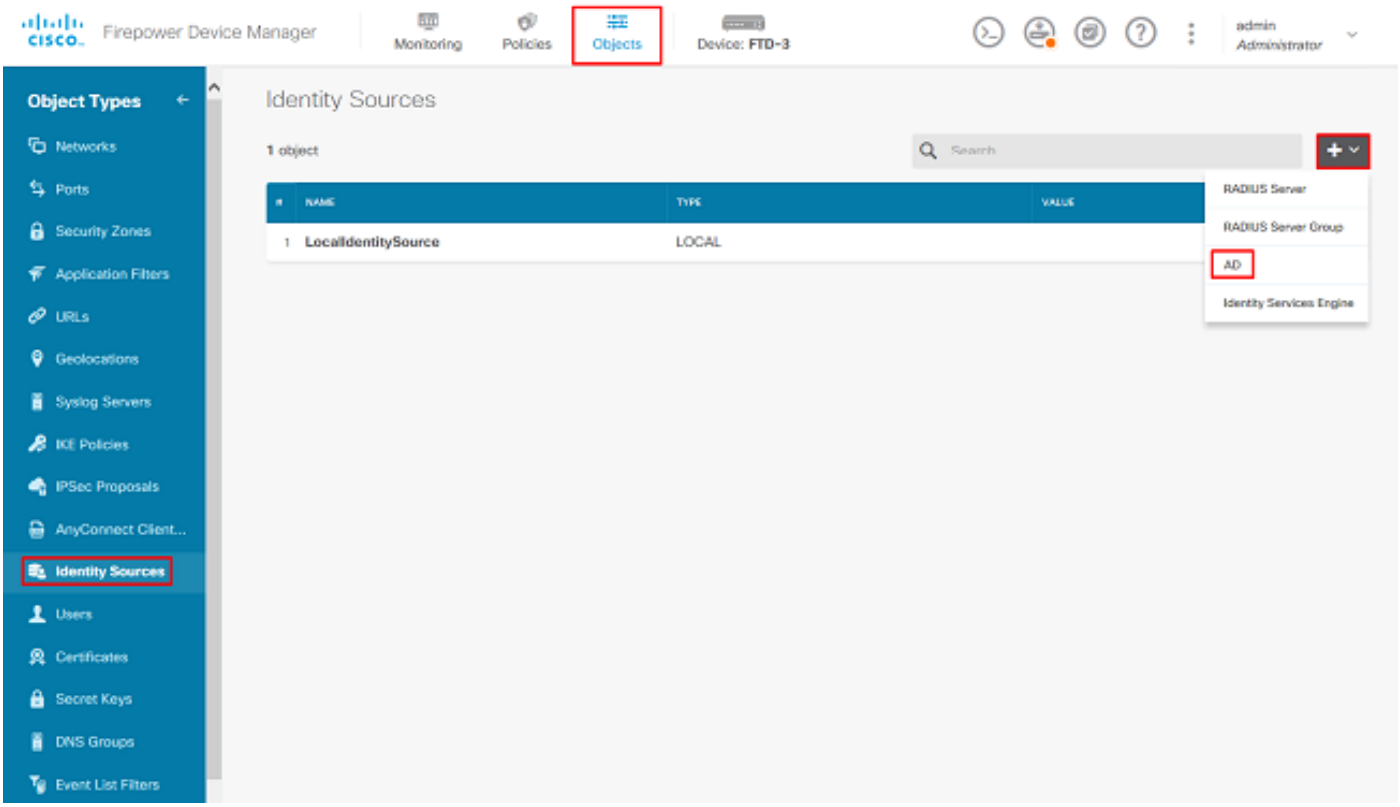


2. FTD가 Smart Licensing 서버에 등록되어 있고 AnyConnect Ux, Apex 또는 VPN Only 라이센스가 활성화되어 있는지 확인합니다.

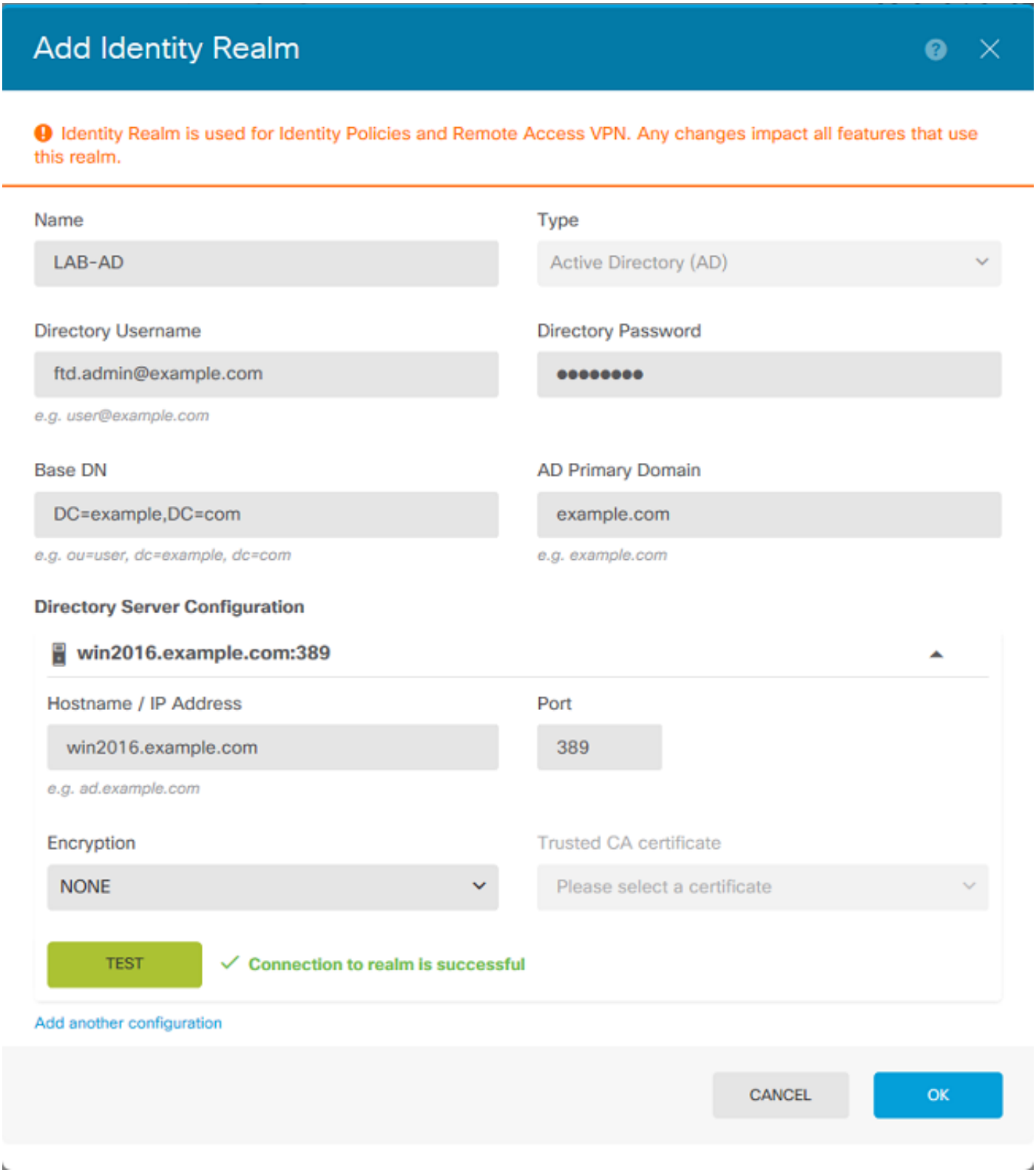


AD ID 소스 설정

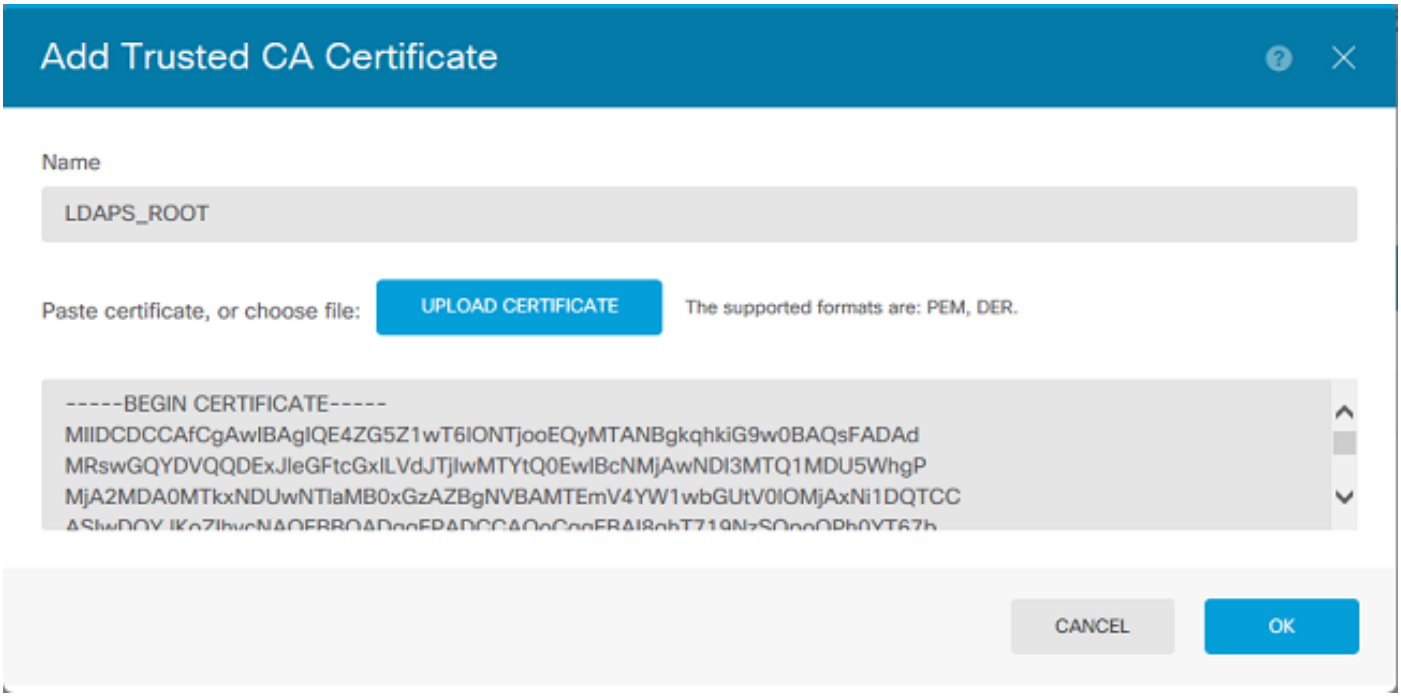
1. **객체 > ID 소스로** 이동한 다음 **+** 기호를 클릭하고 이미지에 표시된 대로 AD를 선택합니다.

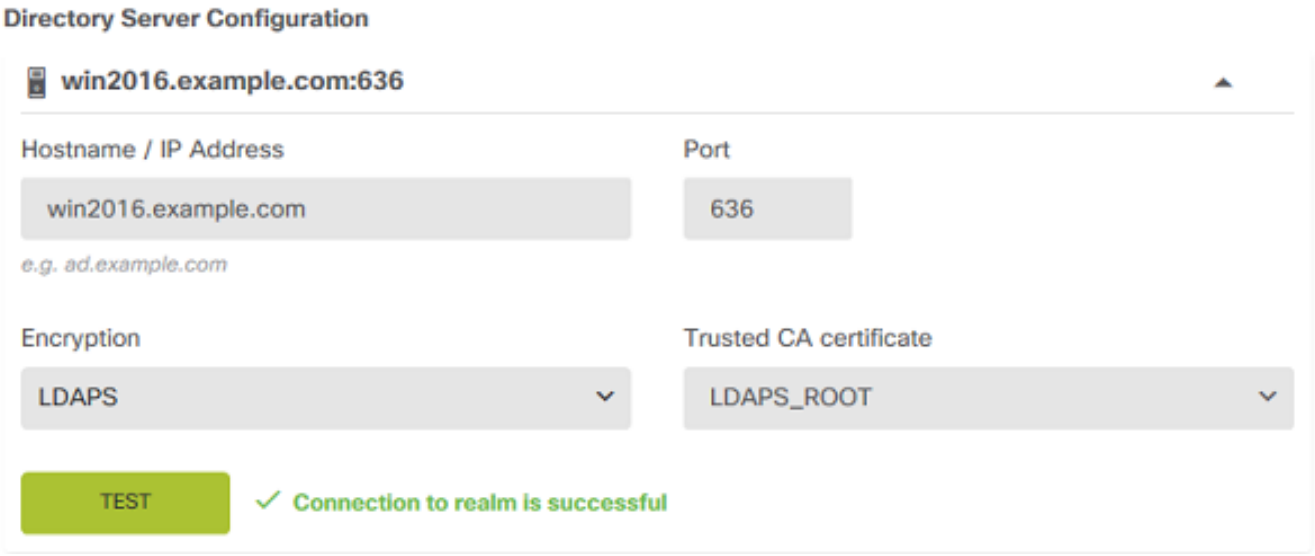


2. 이전에 수집한 정보로 Active Directory 서버에 대한 적절한 설정을 입력합니다.IP 주소 대신 Microsoft 서버에 대해 호스트 이름(FQDN)을 사용하는 경우 Objects(개체) **> DNS Group(DNS 그룹)** 아래에 적절한 DNS 그룹을 만들어야 합니다.그런 다음 **Device(디바이스) > System Settings(시스템 설정) > DNS Server(DNS 서버)로 이동하여 Management Interface(관리 인터페이스)** 및 **Data Interface(데이터 인터페이스)**에서 DNS 그룹을 적용한 다음 DNS 쿼리에 적합한 이그레스 인터페이스를 지정하여 FTD에 해당 DNS 그룹을 적용합니다.FTD의 관리 인터페이스에서 성공적으로 컨피그레이션 및 연결성을 확인하려면 **Test** 버튼을 클릭합니다.이러한 테스트는 FTD의 관리 인터페이스에서 시작되며 FTD에 구성된 라우팅 가능한 인터페이스(예: 내부, 외부, DMZ) 중 하나를 통해서가 아니므로 AnyConnect LDAP 인증 요청이 FTD의 라우팅 가능한 인터페이스 중 하나에서 시작되므로 연결에 성공하거나 실패한 경우에도 AnyConnect 인증에 대해 동일한 결과가 보장되지 않습니다.FTD에서 LDAP 연결 테스트에 대한 자세한 내용은 Troubleshooting(문제 해결) 영역에서 Test AAA and Packet Capture(AAA 및 패킷 캡처 테스트) 섹션을 참조하십시오.



LDAPS 또는 STARTTLS를 사용하는 경우 적절한 Encryption(암호화)을 선택한 다음 Trusted CA 인증서를 선택합니다.루트 CA가 아직 추가되지 않은 경우 Create **New Trusted CA Certificate(새 신뢰할 수 있는 CA 인증서 생성)를** 클릭합니다.루트 CA 인증서의 Name(이름)을 제공한 다음 이전에 수집된 PEM 형식 루트 ca 인증서를 붙여넣습니다.

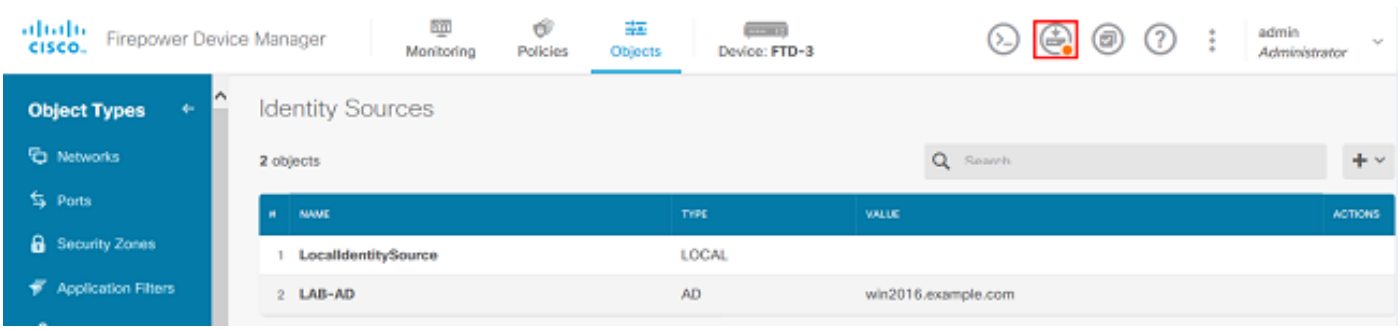




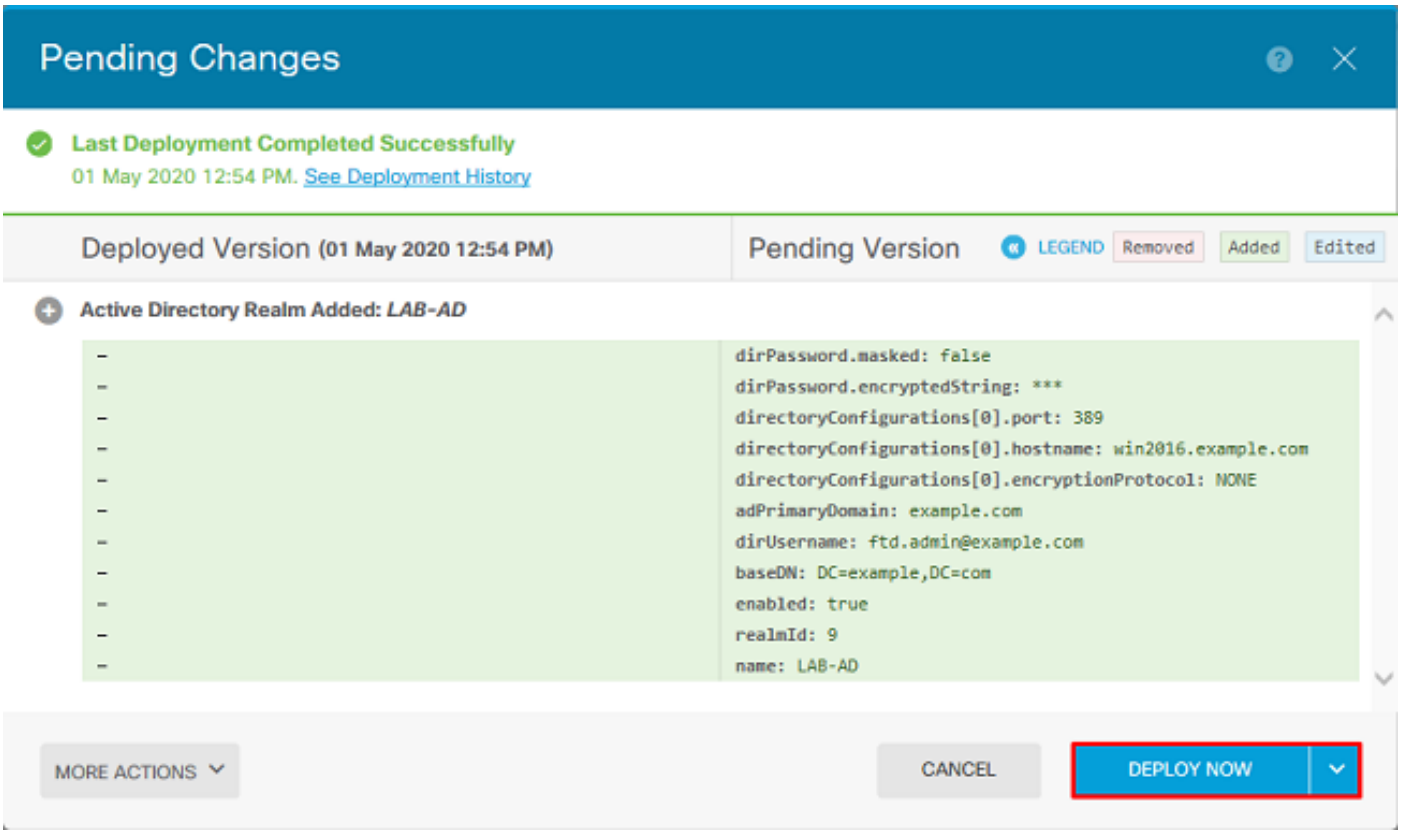
이 컨피그레이션에서는 다음 값이 사용되었습니다.

- 이름:랩-광고
- 디렉터리 사용자 이름:ftd.admin@example.com
- 기본 DN:DC=예,DC=com
- AD 주 도메인:example.com
- 호스트 이름/IP 주소:win2016.example.com
- 포트:389

3. 이미지에 표시된 대로 오른쪽 상단의 **보류** 변경 버튼을 클릭합니다.



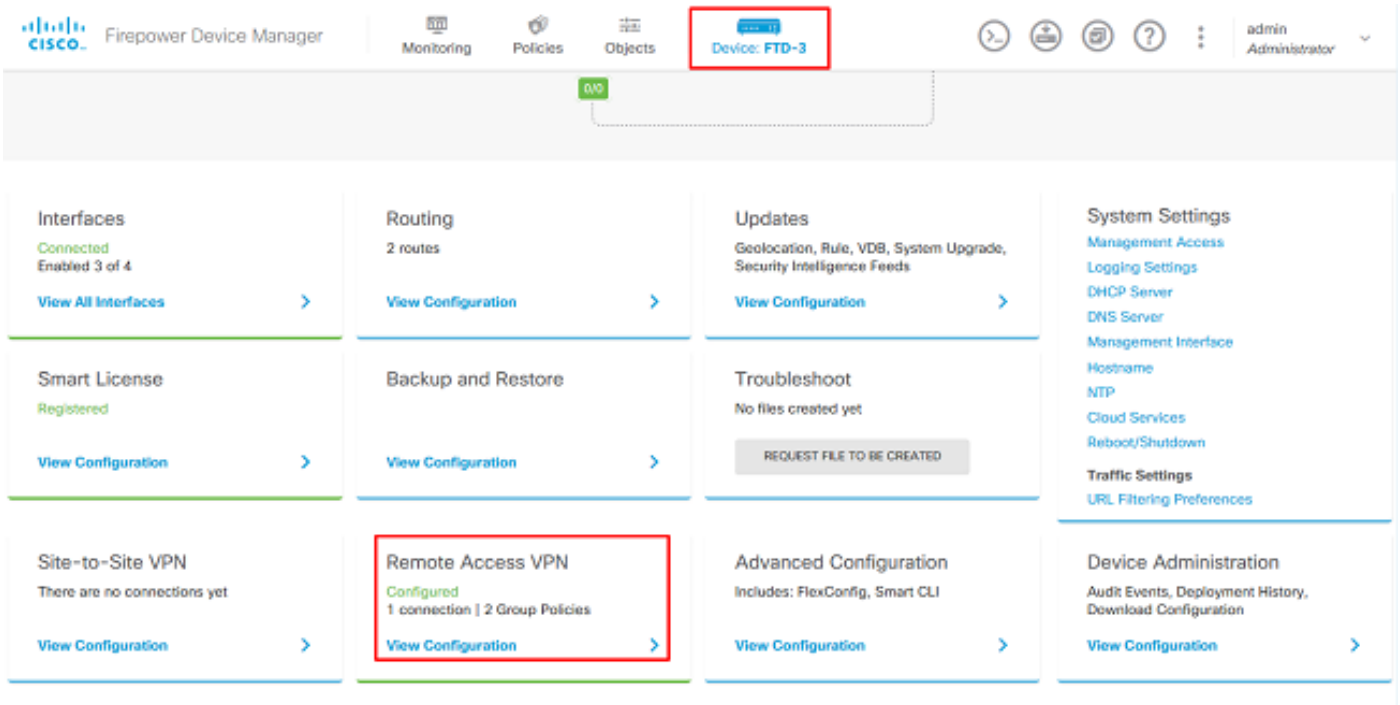
4. 지금 **배치** 버튼을 클릭합니다.



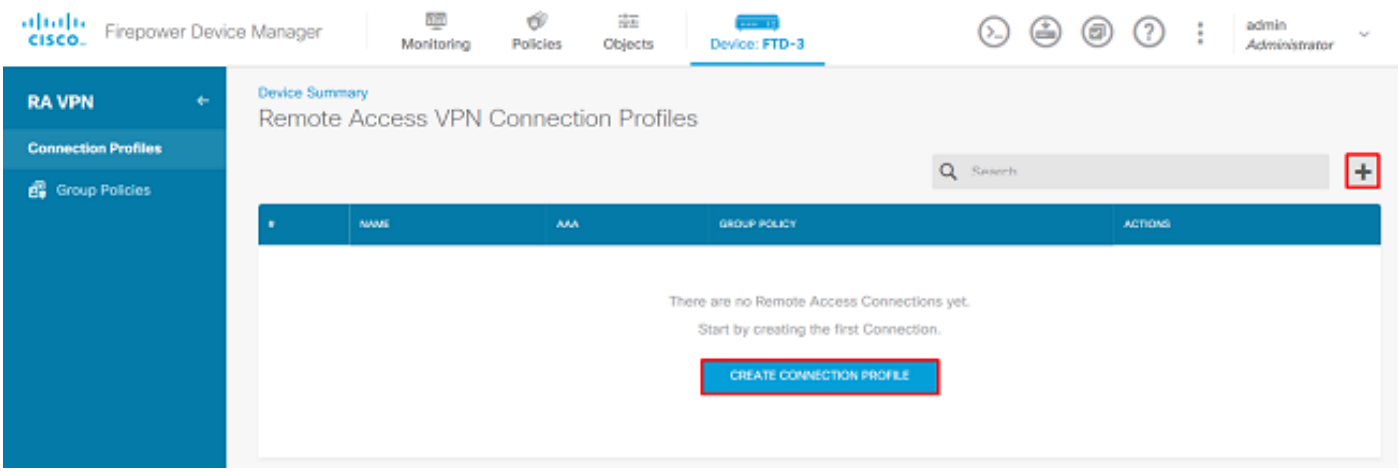
AD 인증을 위한 AnyConnect 구성

구성된 AD ID 소스를 사용하려면 AnyConnect 구성에 적용해야 합니다.

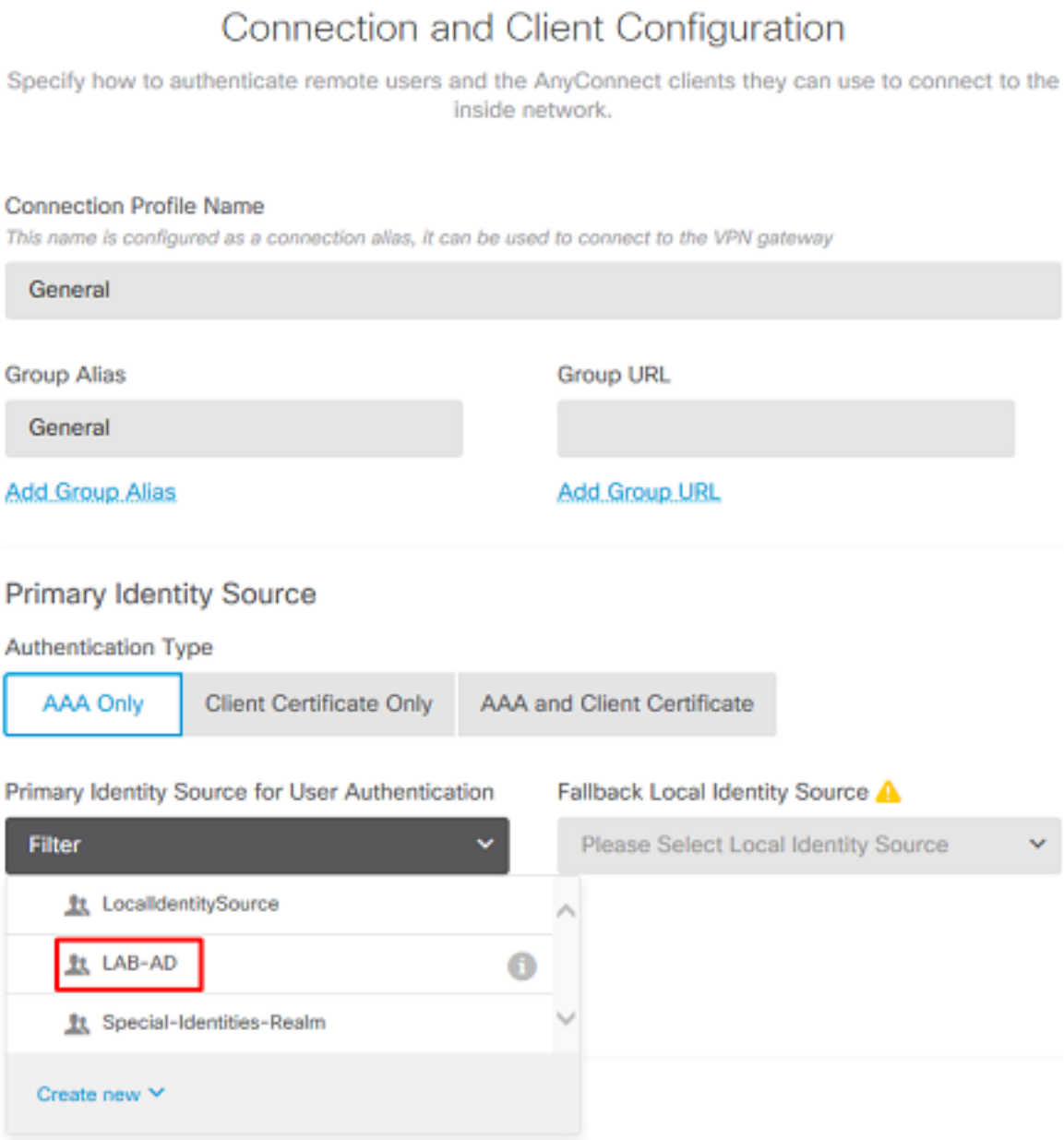
1. 이미지에 표시된 대로 **Device(디바이스) > Remote Access VPN(원격 액세스 VPN)**으로 이동합니다.

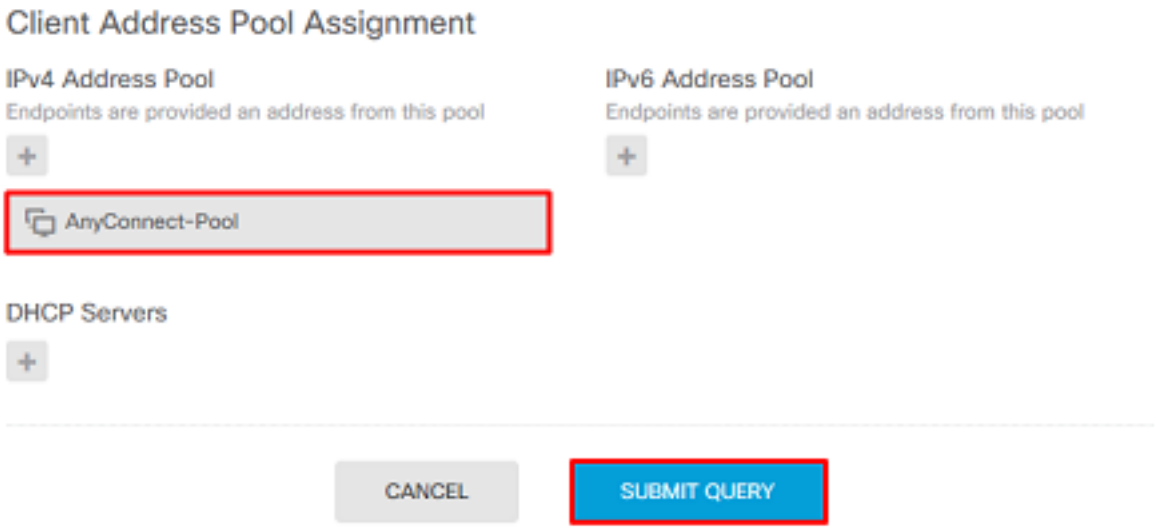


2. 이미지에 표시된 대로 +기호 또는 **연결 프로파일 생성** 버튼을 클릭합니다.

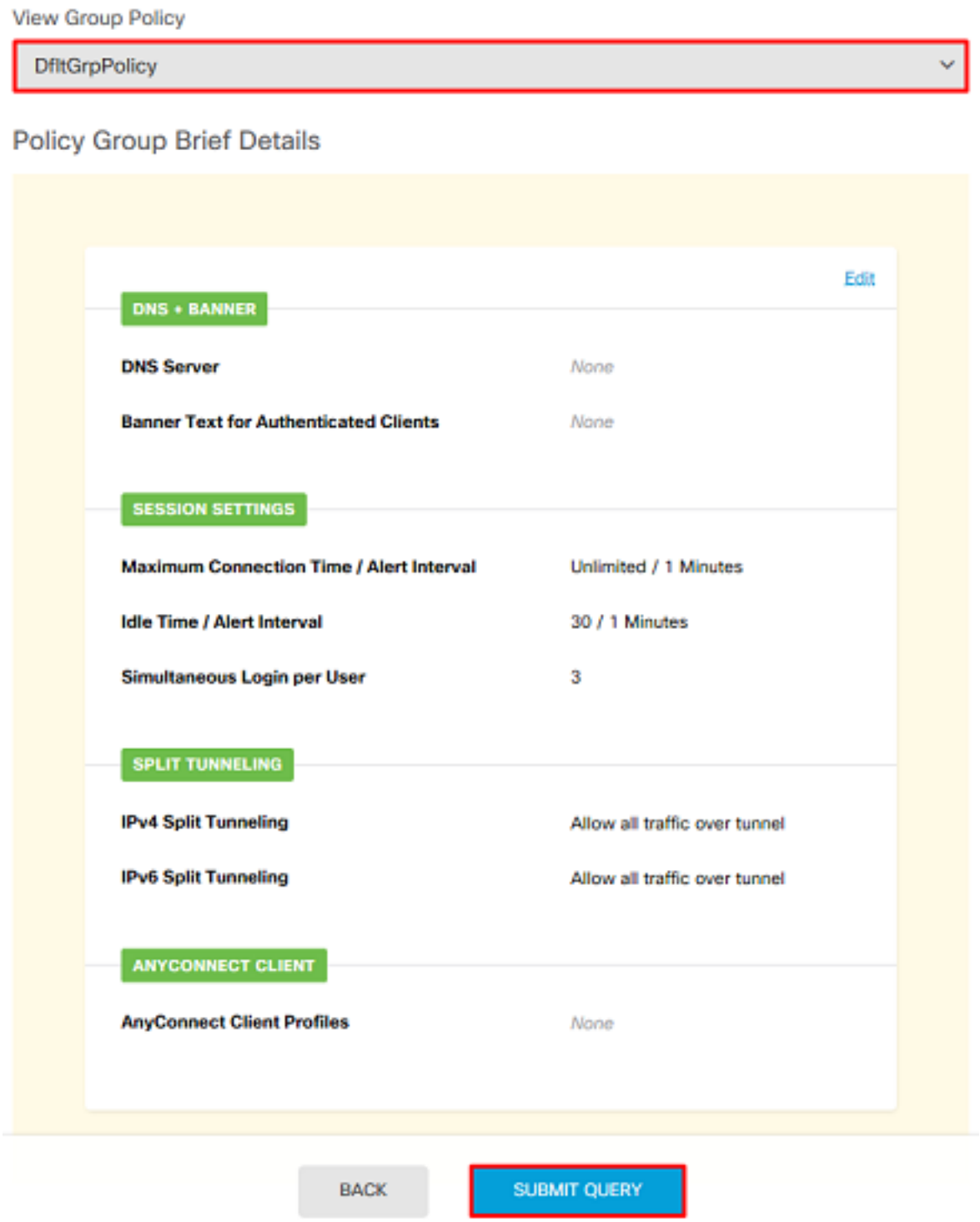


3. Connection and Client Configuration(연결 및 클라이언트 컨피그레이션) 섹션에서 앞서 생성한 AD ID 소스를 선택합니다.Connection Profile Name(연결 프로파일 이름) 및 Client Address Pool Assignment(클라이언트 주소 풀 할당) 등 다른 섹션에 적합한 값을 설정합니다.완료되면 **Submit Query(쿼리 제출)**를 클릭합니다.

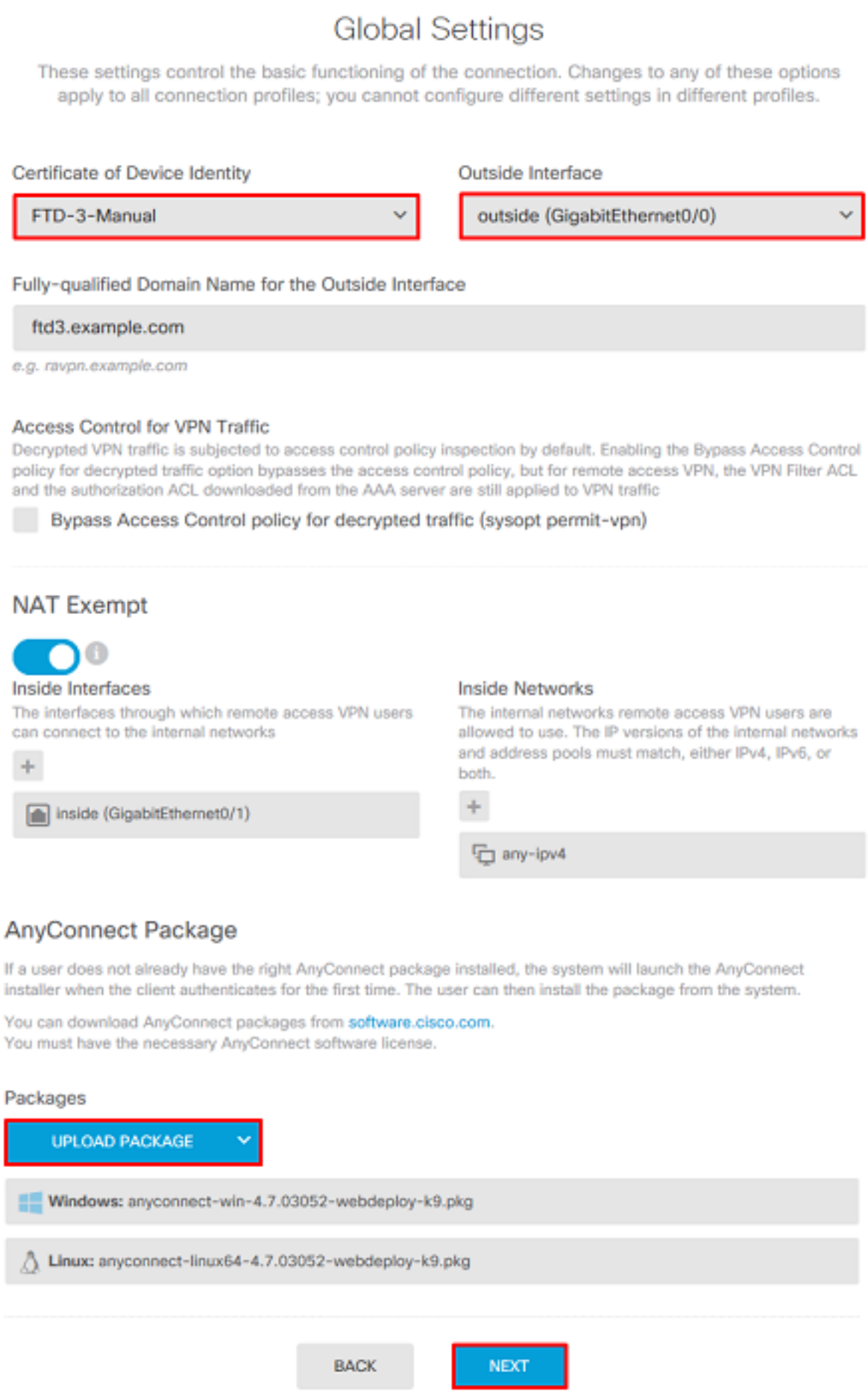




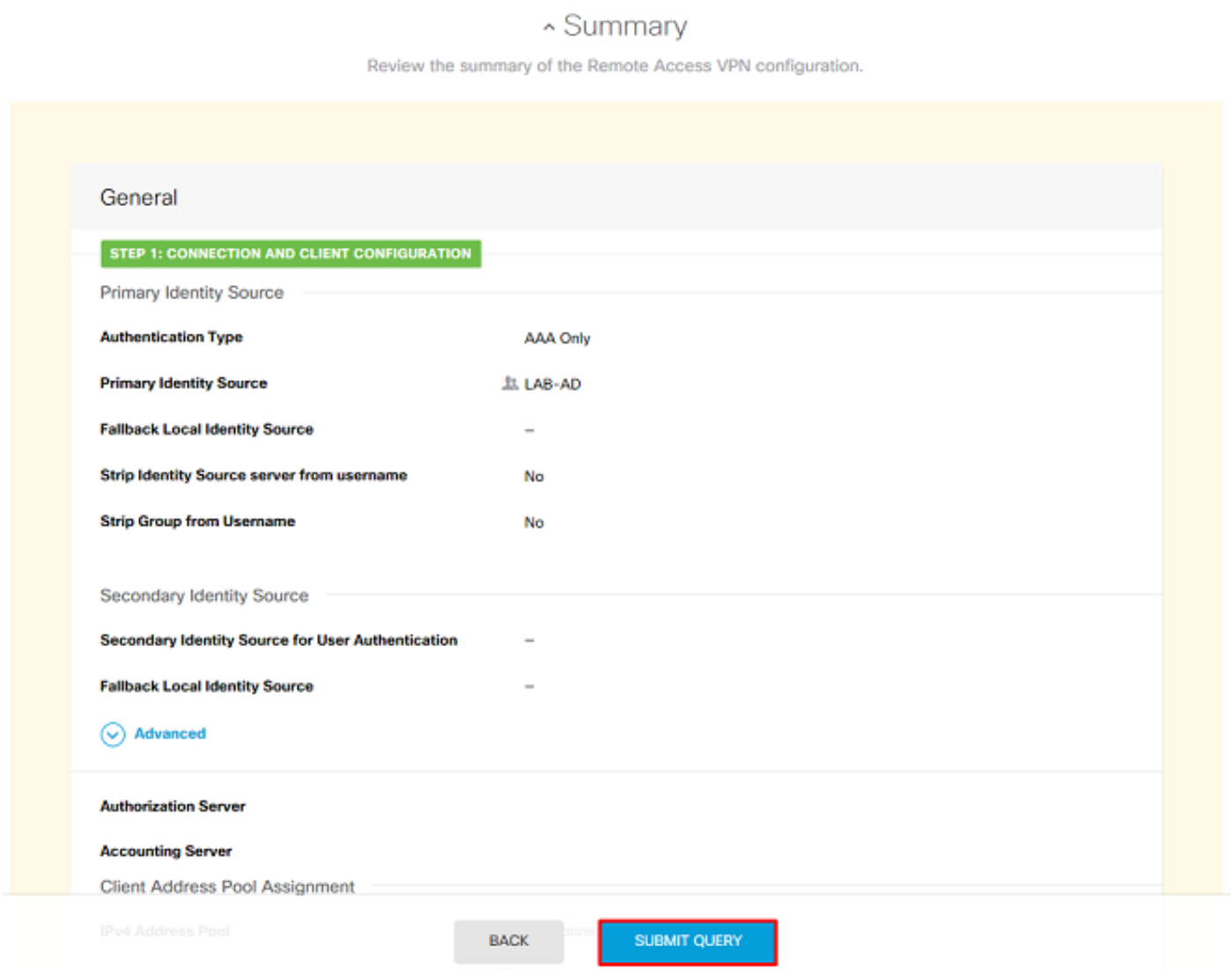
4. Remote User Experience(원격 사용자 환경) 섹션에서 적절한 그룹 정책을 선택합니다.기본적으로 DfltGrpPolicy가 사용됩니다.그러나 다른 항목을 만들 수 있습니다.



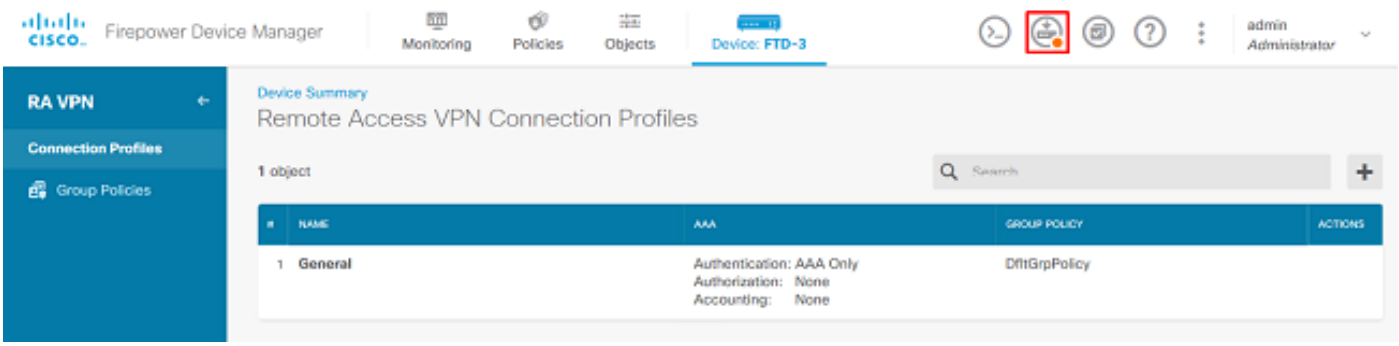
5. Global Settings(전역 설정) 섹션에서 최소한 SSL 인증서, 외부 인터페이스 및 AnyConnect 패키지를 지정합니다.인증서를 이전에 만들지 않은 경우 기본 자체 서명 인증서 (DefaultInternalCertificate)를 선택할 수 있지만 신뢰할 수 없는 서버 인증서 메시지가 표시됩니다 .암호 해독된 트래픽(sysopt permit-vpn)에 대한 Bypass Access Control 정책을 선택 취소해야 나중에 사용자 ID 액세스 정책 규칙이 적용됩니다.NAT 면제도 여기에서 구성할 수 있습니다.이 컨피그레이션에서는 AnyConnect 클라이언트 IP 주소로 이동하는 내부 인터페이스의 모든 ipv4 트래픽이 NAT에서 제외됩니다.외부 헤어피닝(outside to outside hairpinning)과 같은 보다 복잡한 설정을 위해 NAT 정책에 따라 추가 NAT 규칙을 생성해야 합니다.AnyConnect 패키지는 Cisco 지원 사이트에서 찾을 수 있습니다. https://software.cisco.com/download/homeAnyConnect 패키지를 다운로드하려면 유효한 Plus 또는 Apex 라이센스가 필요합니다.



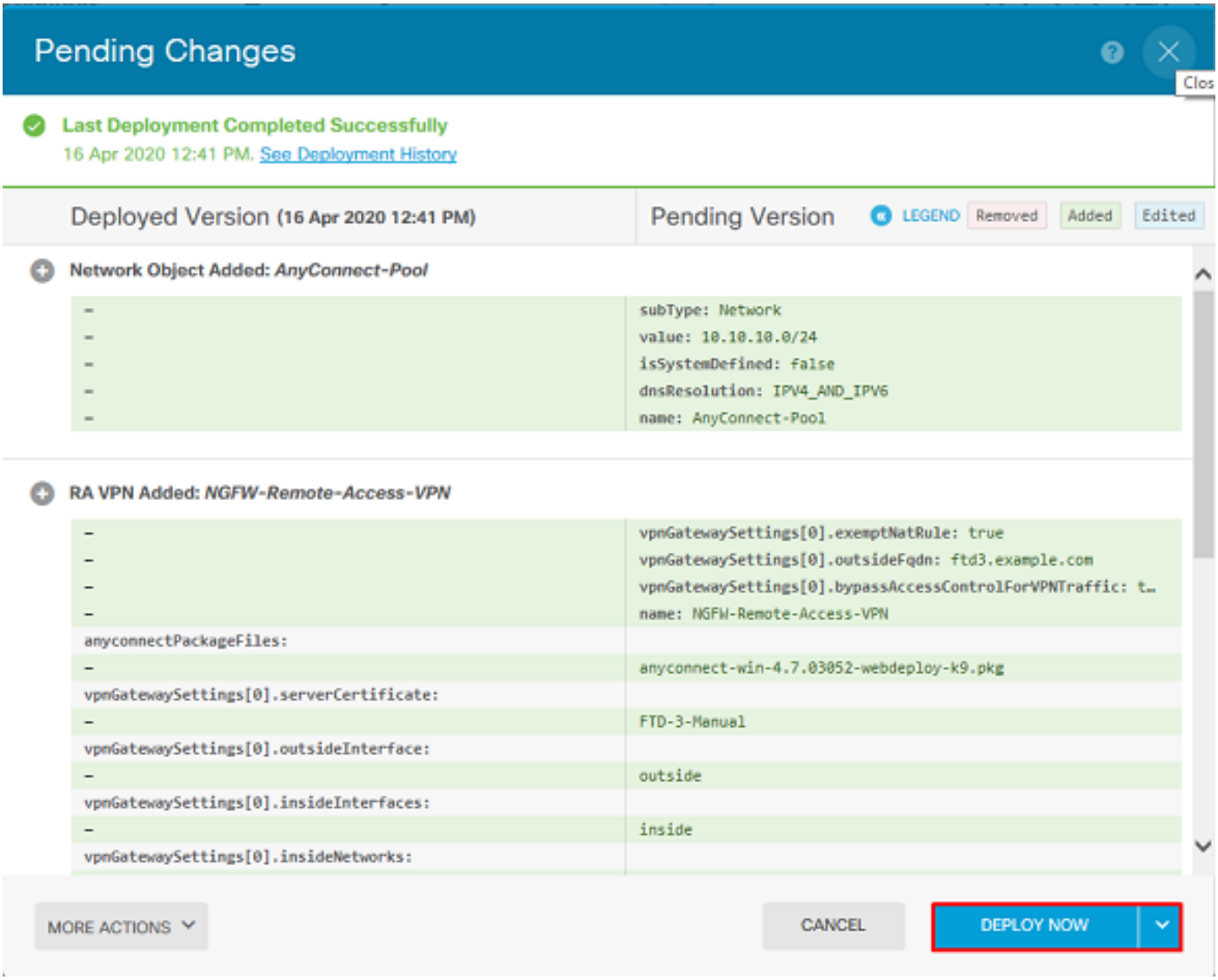
6. 요약 섹션에서 AnyConnect가 적절하게 설정되었는지 확인한 다음 질의 제출을 **클릭합니다**.



7. 이미지에 표시된 대로 오른쪽 상단의 **보류 중인 변경** 버튼을 클릭합니다.



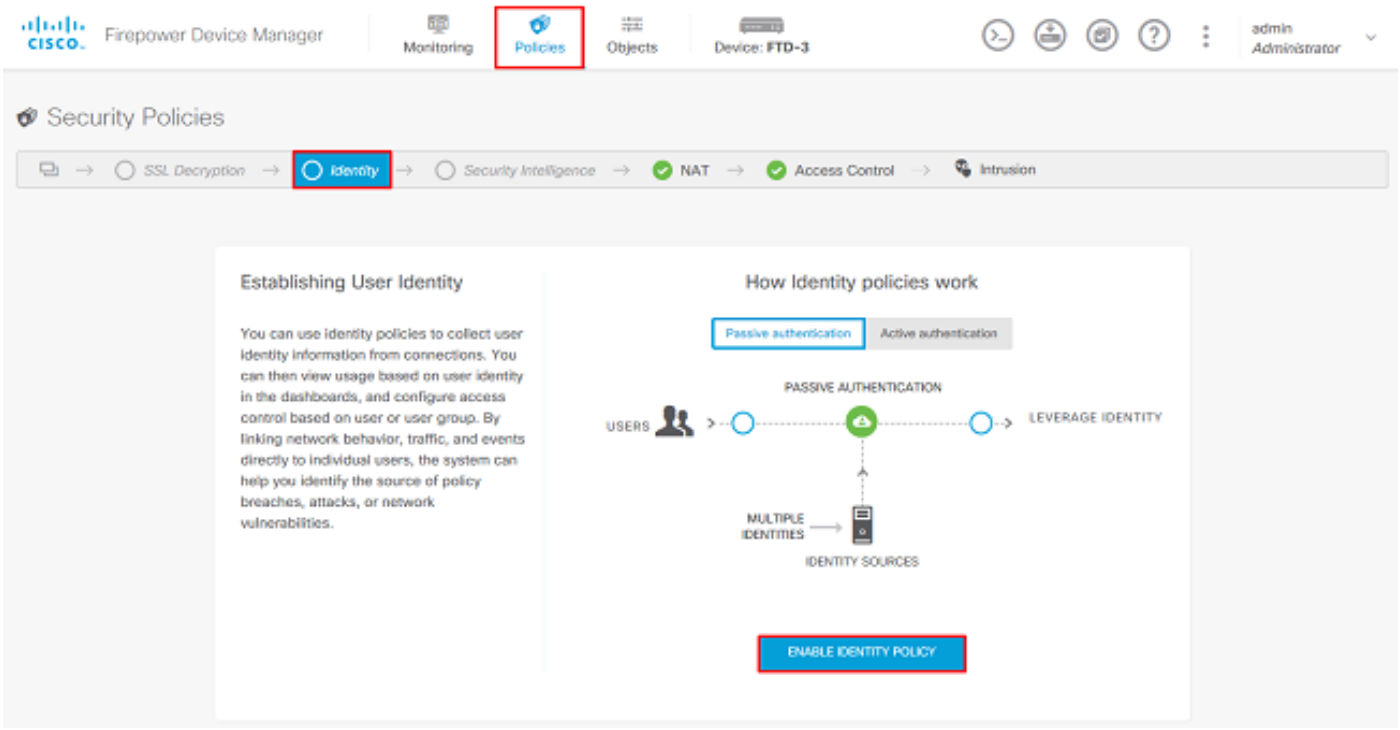
8. 지금 **구축을 클릭합니다**.



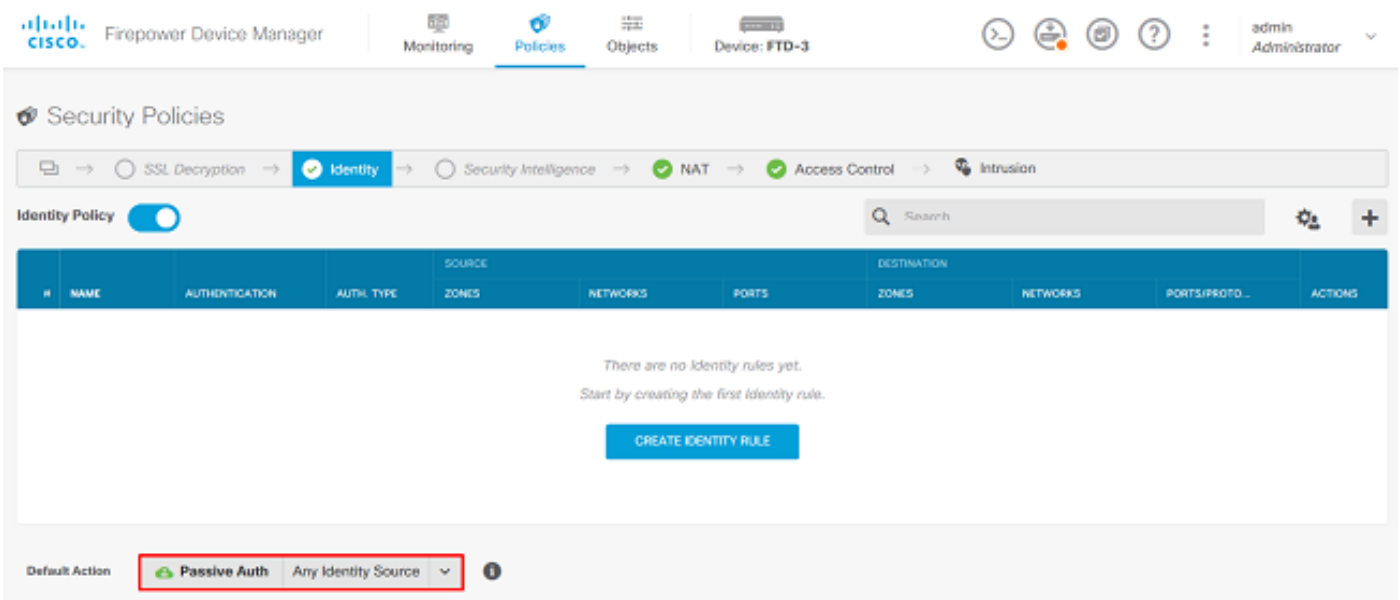
사용자 ID에 대한 ID 정책 활성화 및 보안 정책 구성

이때 AnyConnect 사용자는 성공적으로 연결할 수 있어야 하지만 특정 리소스에 액세스하지 못할 수 있습니다.이 단계에서는 AnyConnect 관리자 내의 사용자만 RDP를 사용하여 내부 리소스에 연결할 수 있도록 사용자 ID를 활성화하며, AnyConnect 사용자는 그룹 내의 사용자만 HTTP를 사용하여 내부 리소스에 연결할 수 있습니다.

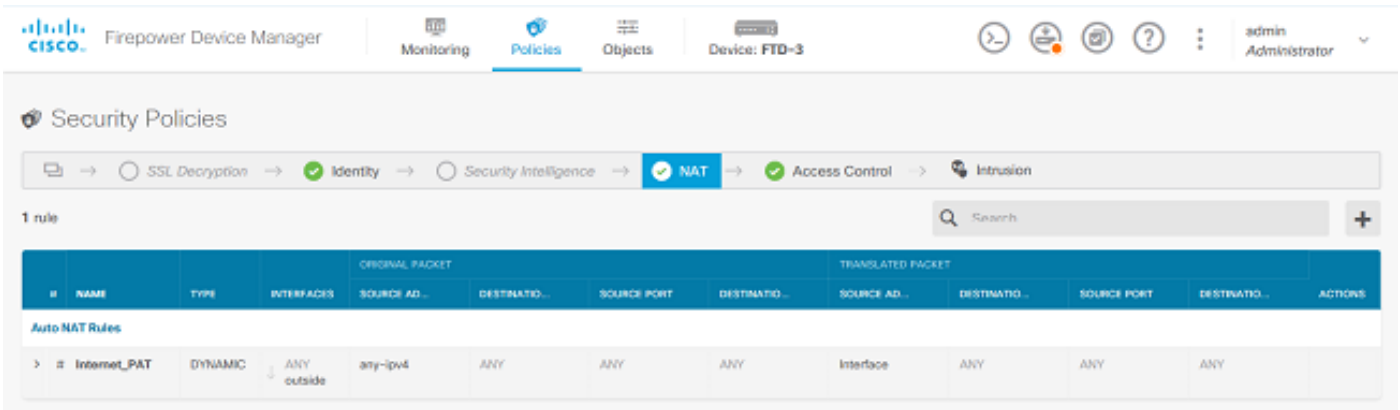
1. Policies(**정책) > Identity(ID)로** 이동하고 **Enable Identity Policy(ID 정책 활성화)를 클릭합니다**.



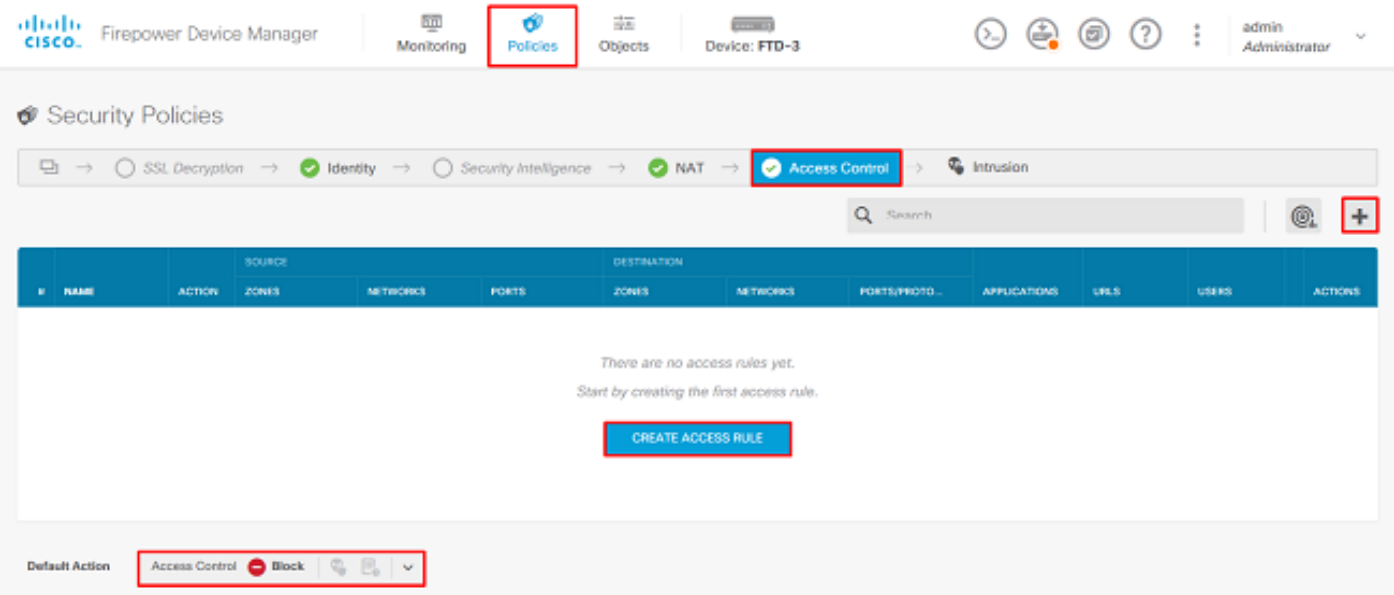
이 컨피그레이션에서는 추가 컨피그레이션이 필요하지 않으며 Default Action(기본 작업)으로도 충분합니다.



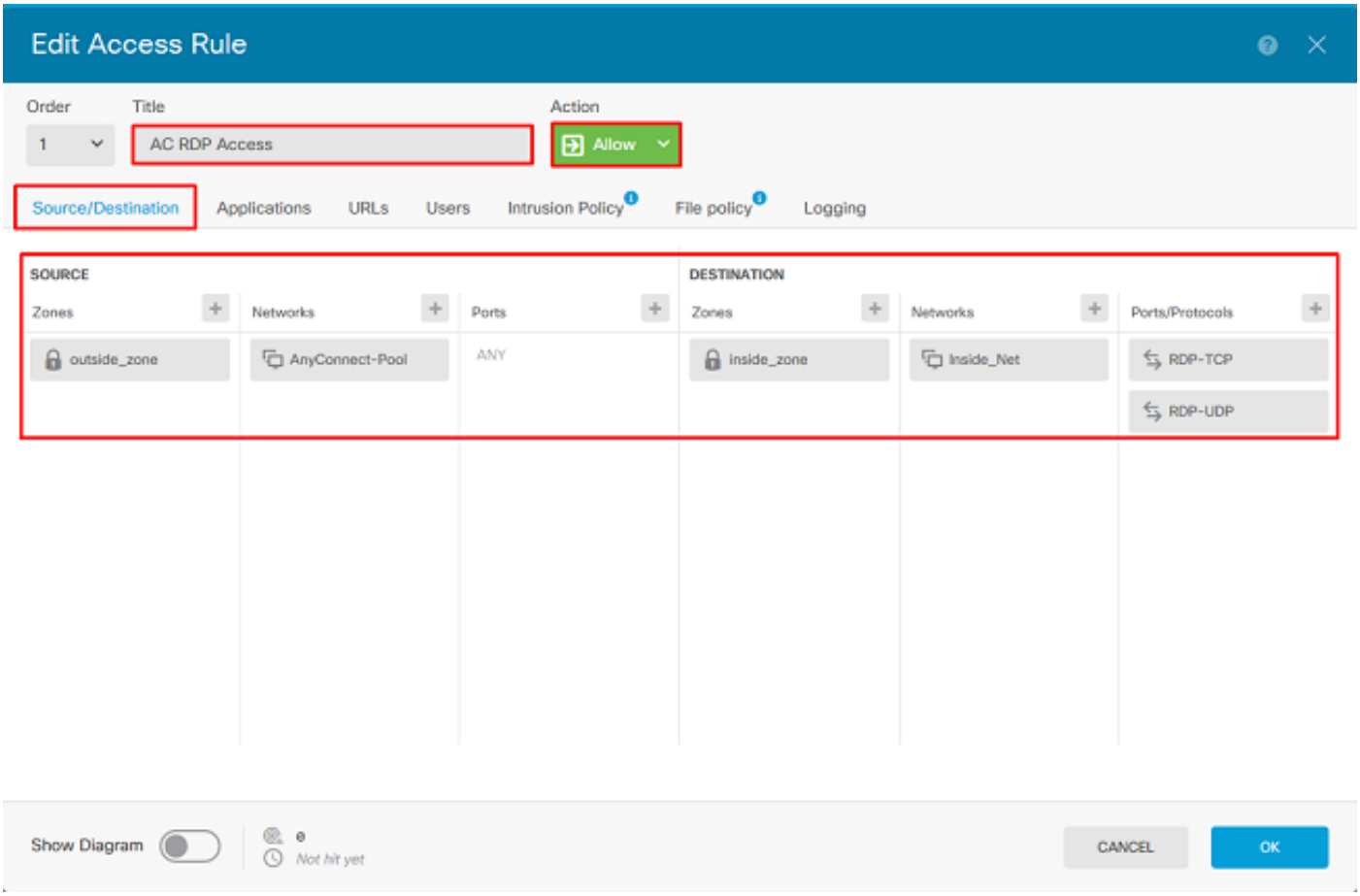
2. Policies(**정책) > NAT**로 이동하고 NAT가 적절하게 구성되었는지 확인합니다.AnyConnect 설정에 구성된 NAT 예외에 충분한 경우 여기에서 추가 컨피그레이션이 필요하지 않습니다.



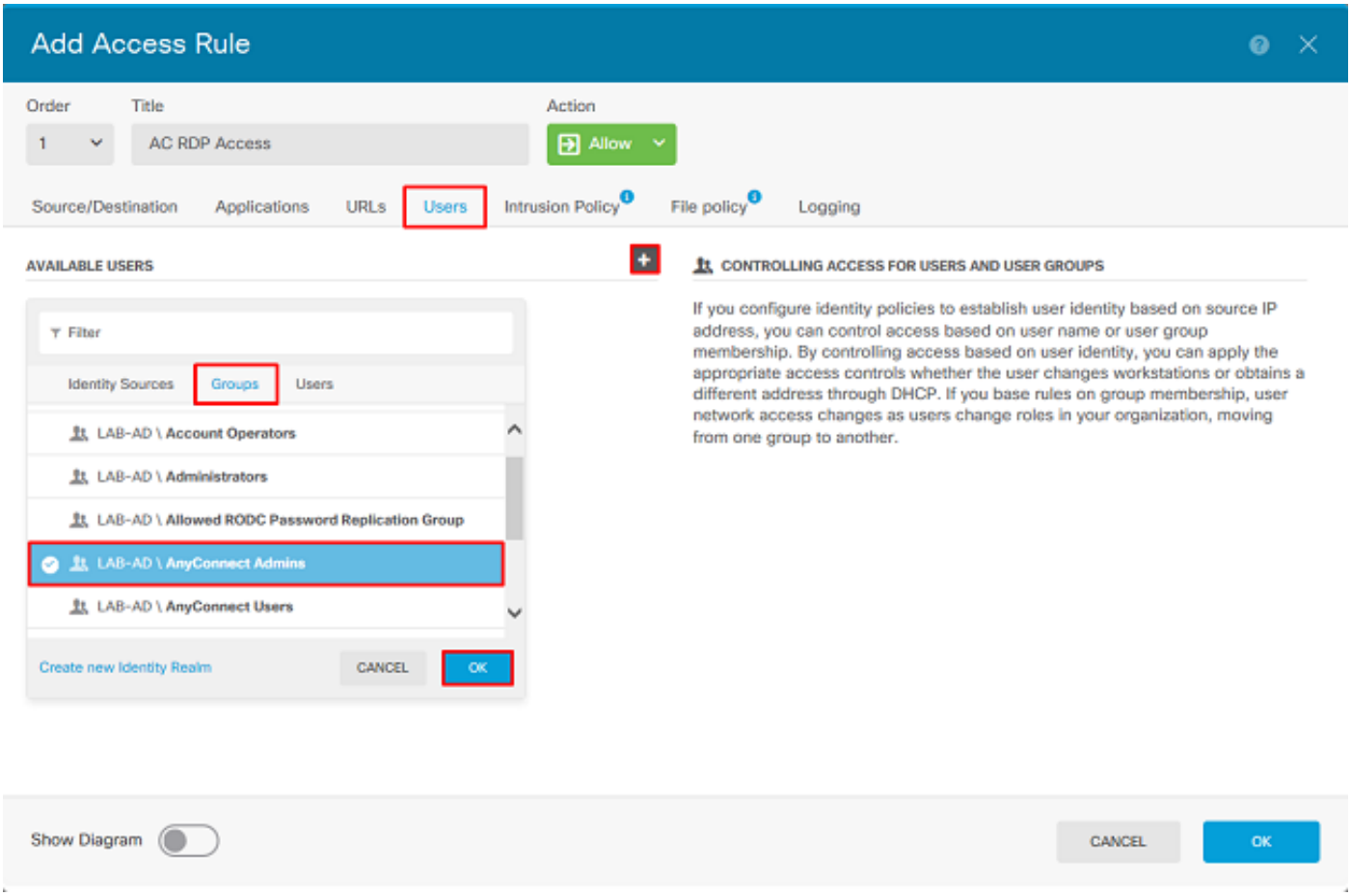
3. **정책 > 액세스 제어로 이동합니다**.이 섹션에서는 Default Action(기본 작업)이 Block(차단)으로 설정되고 액세스 규칙이 생성되지 않으므로 AnyConnect 사용자가 연결되면 아무 것도 액세스할 수 없습니다.+ 기호 또는 Create Access Rule을 클릭하여 새 규칙을 추가합니다.



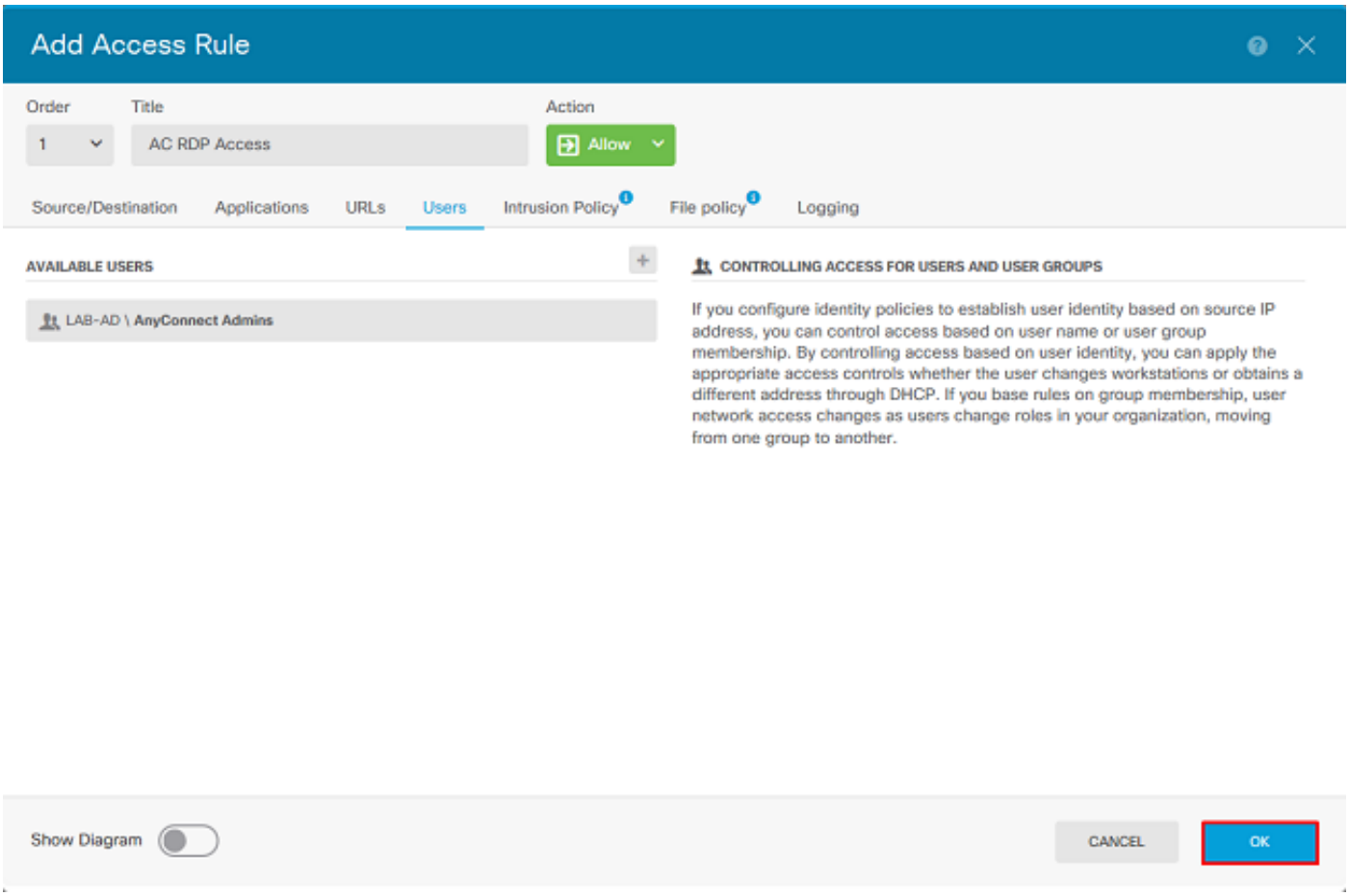
4. 적절한 값으로 필드를 입력합니다.이 컨피그레이션에서는 AnyConnect Admins 그룹 내의 사용자가 내부 네트워크의 Windows Server에 대한 RDP 액세스를 가져야 합니다.소스의 경우 영역은 AnyConnect 사용자가 연결할 외부 인터페이스인 outside_zone으로 구성되고 네트워크는 이전에 AnyConnect 클라이언트에 IP 주소를 할당하도록 구성된 AnyConnect-Pool 객체로 구성됩니다 .FDM의 사용자 ID의 경우 소스가 영역 및 네트워크가 사용자가 연결을 시작할 영역이어야 합니다 .대상의 경우 영역은 Windows Server가 있는 내부 인터페이스인 inside_zone으로 구성되고, 네트워크는 Windows Server가 있는 서브넷을 정의하는 개체인 Inside_Net 객체로 구성되며, 포트/프로토콜은 TCP 3389 및 UDP 3389를 통한 RDP 액세스를 허용하도록 두 개의 사용자 지정 포트 객체로 설정됩니다.



Users(사용자) 섹션에서 AnyConnect Admins(AnyConnect 관리자) 그룹이 추가되므로 이 그룹의 사용자는 Windows Server에 대한 RDP 액세스가 허용됩니다.+ 기호를 클릭하고 그룹 탭을 클릭한 다음 적절한 그룹을 클릭한 다음 **확인**을 클릭합니다.개별 사용자와 ID 소스 역시 선택할 수 있습니다.

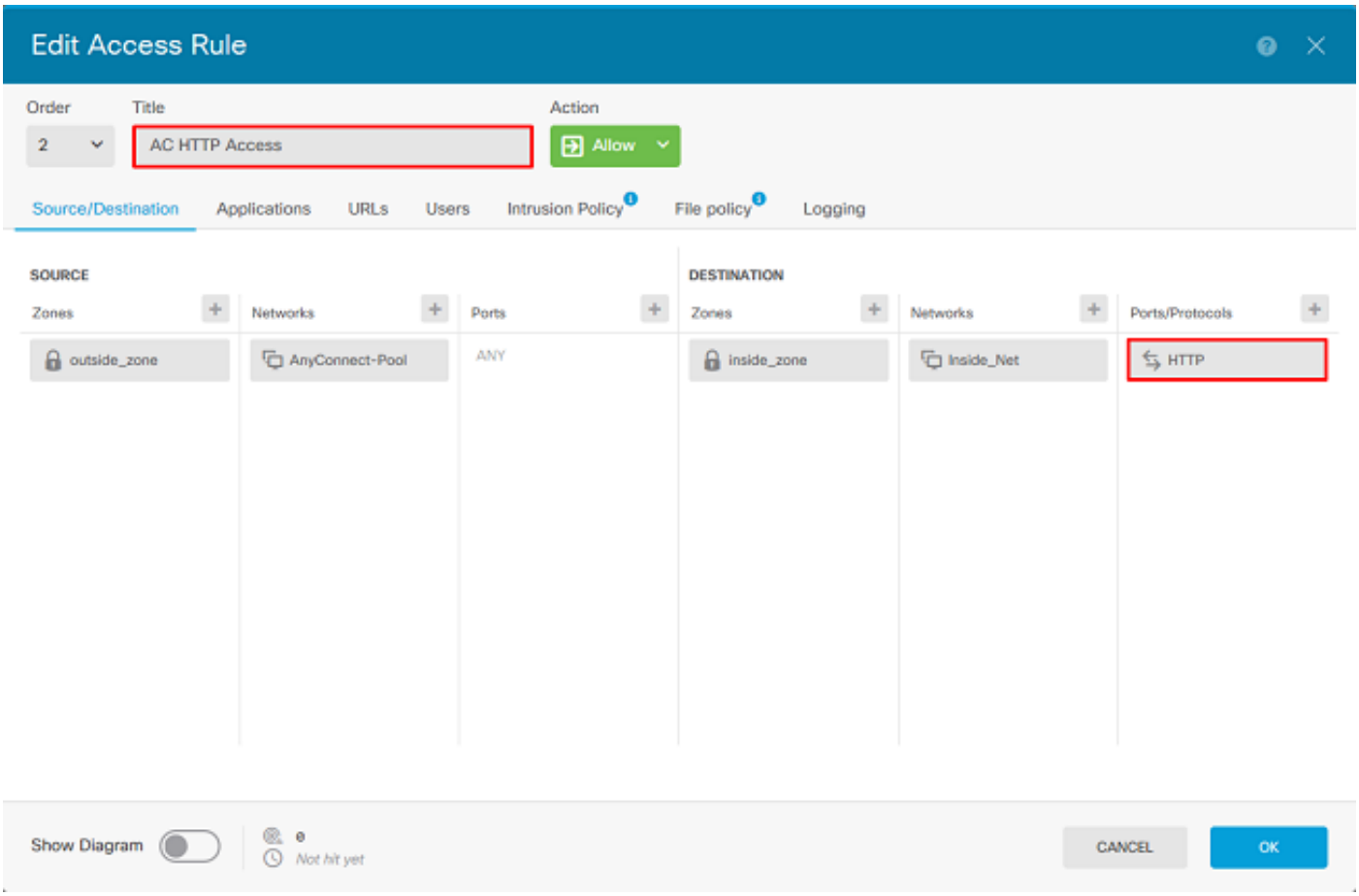


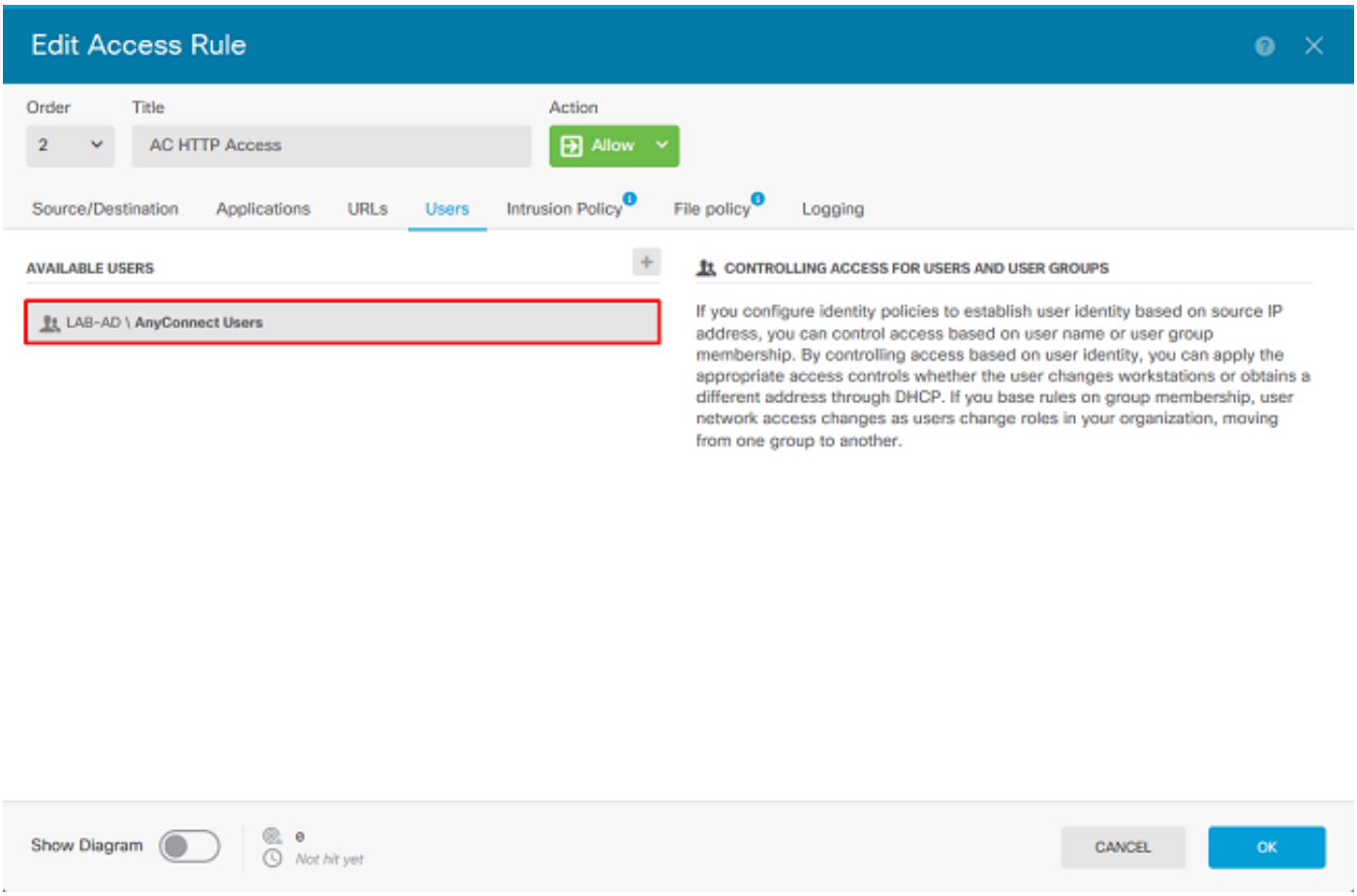
적절한 옵션을 선택했으면 **확인**을 클릭합니다.



5. 필요한 경우 추가 액세스 규칙을 생성합니다.이 컨피그레이션에서는 AnyConnect 사용자 그룹

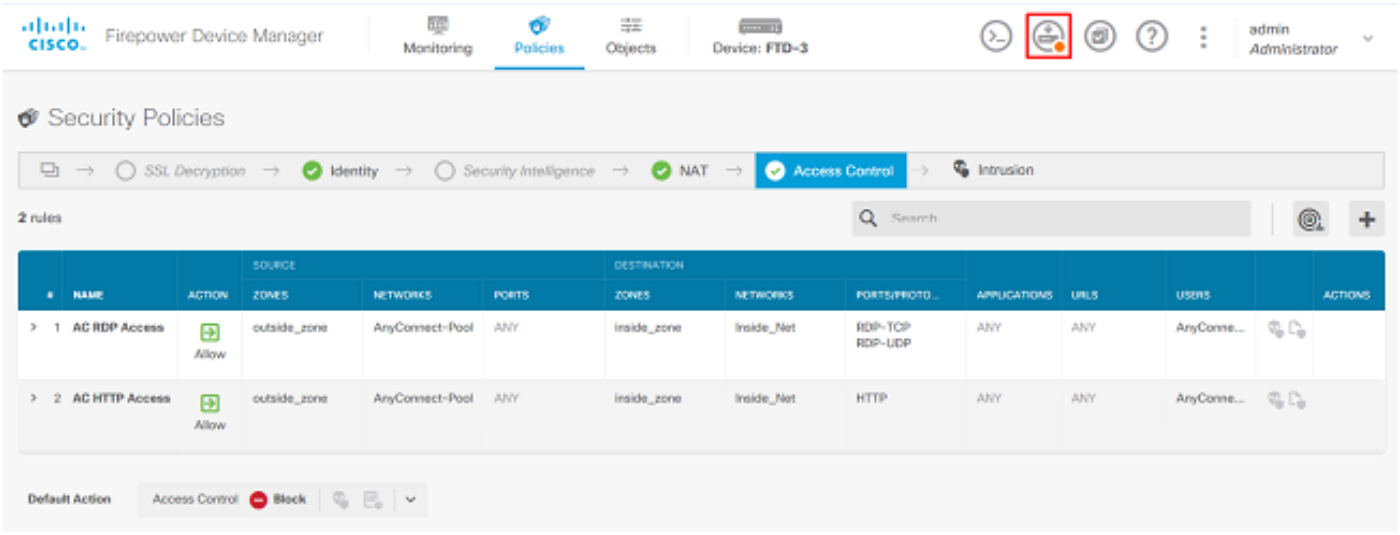
내의 사용자가 Windows Server에 대한 HTTP 액세스를 허용하도록 다른 액세스 규칙이 생성됩니다.



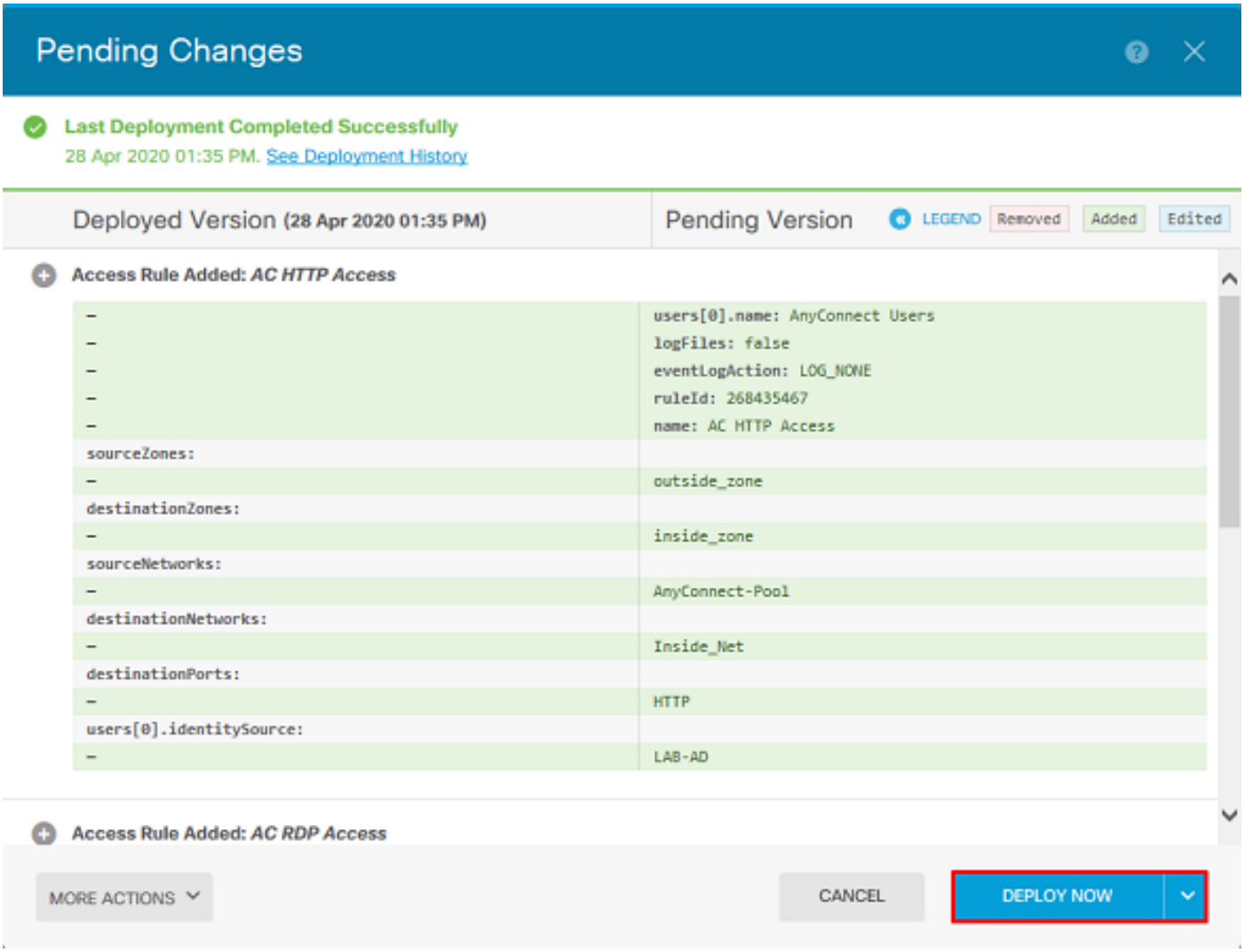


6. 액세스 규칙 컨피그레이션을 확인한 다음 이미지에 표시된 대로 오른쪽 상단에 있는 **Pending**

Changes(보류 중 변경 사항) 버튼을 클릭합니다.



7. 변경 사항을 확인한 다음 Deploy Now(지금 **구축)를 클릭합니다**.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

최종 구성

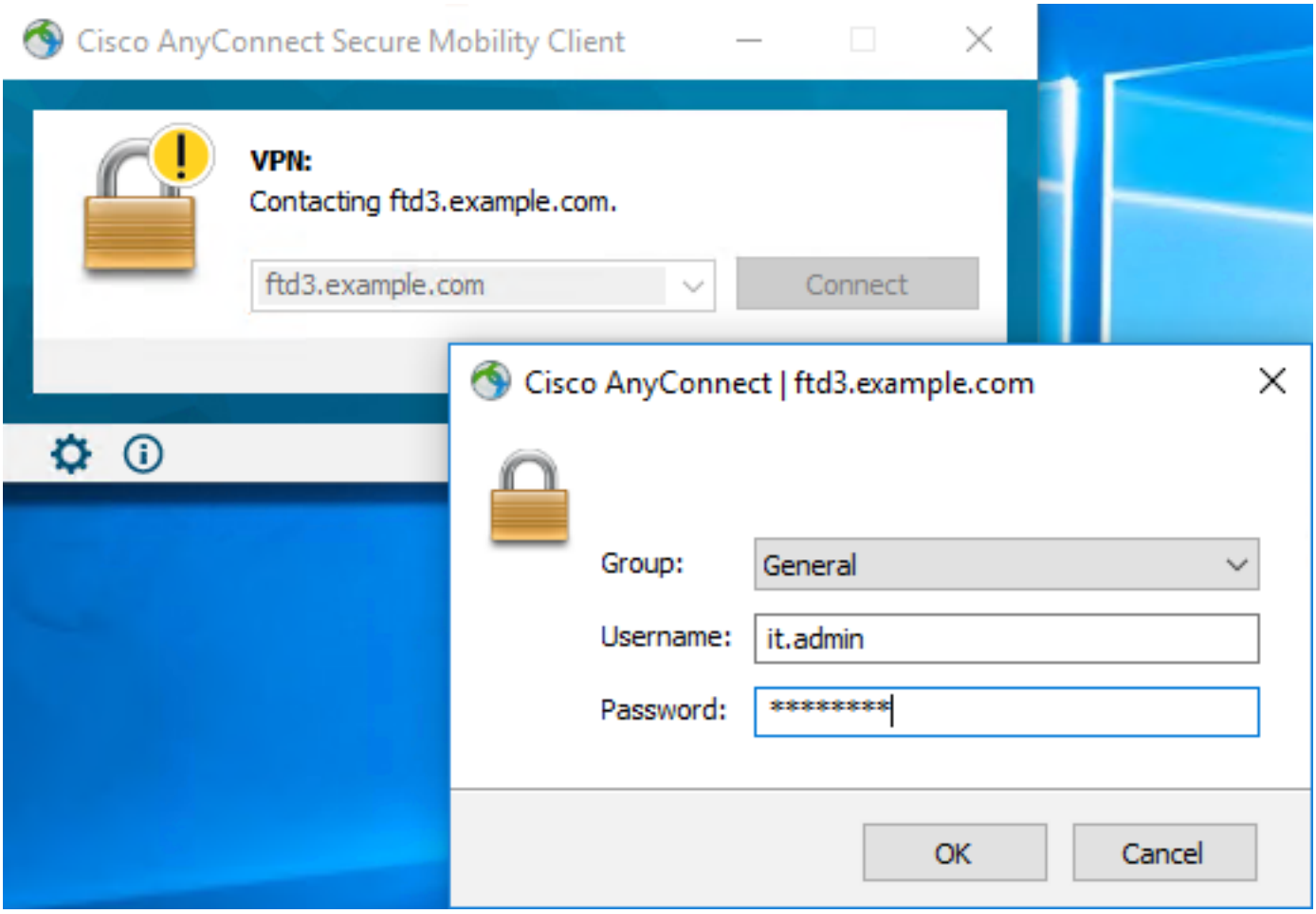
AAA 컨피그레이션

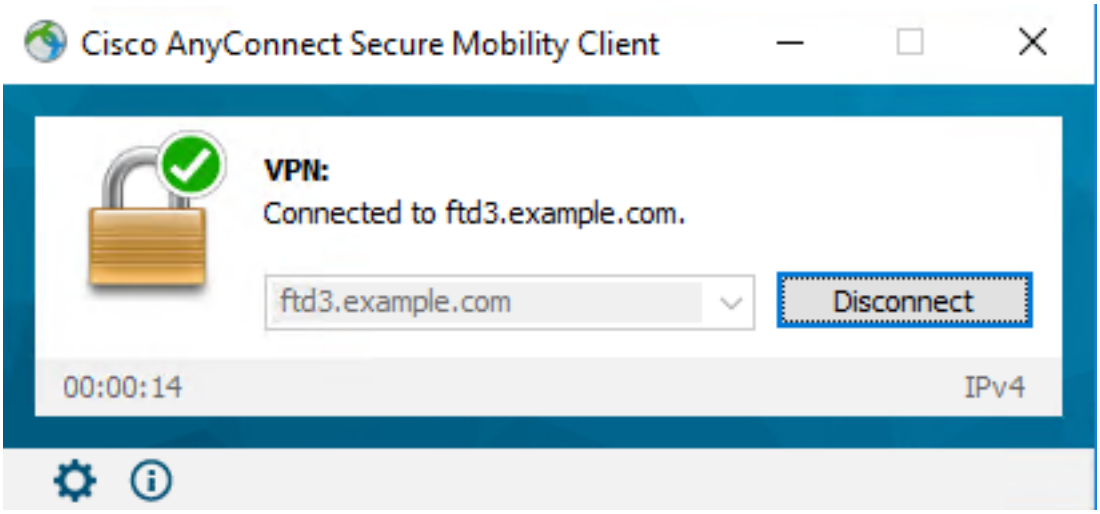
```
show running-configuration aaa-server
aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-
port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

AnyConnect 구성

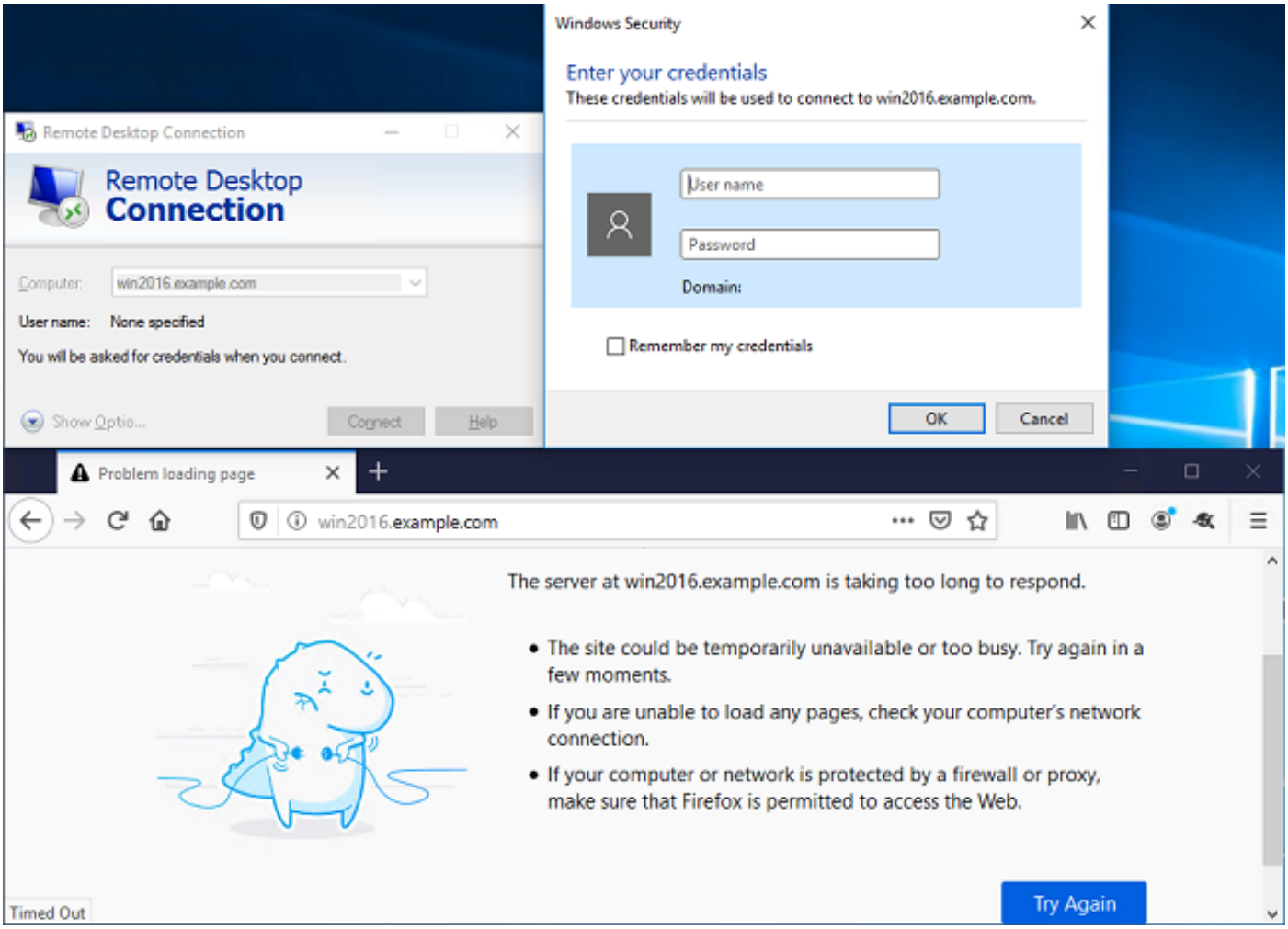
```
> show running-config webvpn
webvpn
 enable outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
 anyconnect enable
 tunnel-group-list enable
 cache
  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-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value DfltGrpPolicy|splitAcl
 webvpn
  anyconnect ssl dtls none

> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

AnyConnect로 연결 및 액세스 제어 정책 규칙 확인

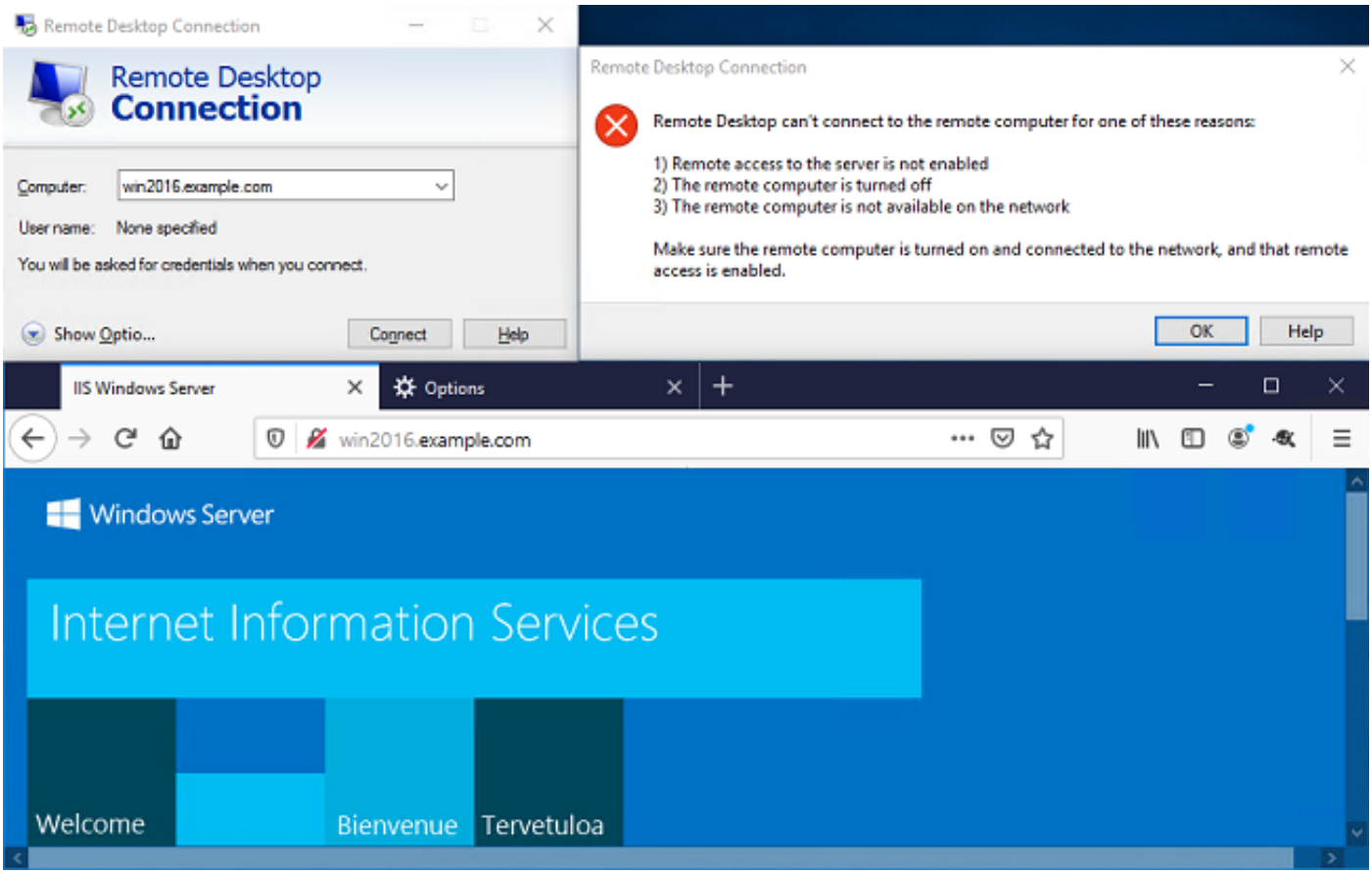




사용자 IT 관리자가 Windows Server에 대한 RDP 액세스 권한이 있는 AnyConnect 관리자 그룹에 있지만 HTTP에 액세스할 수 없습니다.이 서버에 대한 RDP 및 Firefox 세션을 열면 이 사용자가 RDP를 통해서만 서버에 액세스할 수 있는지 확인합니다.



HTTP 액세스 권한이 있지만 RDP 액세스 권한이 없는 AnyConnect 사용자 그룹에 있는 테스트 사용자로 로그인한 경우 액세스 제어 정책 규칙이 적용되는지 확인할 수 있습니다.



문제 해결

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

디버깅

이 디버그는 진단 CLI에서 실행하여 LDAP 인증 관련 문제를 해결할 수 있습니다.**debug ldap 255**.

사용자 ID 액세스 제어 정책 문제를 해결하기 위해 **시스템 지원 방화벽 엔진 디버그**를 클러스터링하여 트래픽이 예기치 않게 허용되거나 차단된 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 신뢰할 수 있는지 확인합니다.
- 올바른 IP 주소와 포트가 사용되는지 확인합니다.호스트 이름을 사용하는 경우 DNS가 올바른 IP 주소로 확인할 수 있는지 확인합니다.

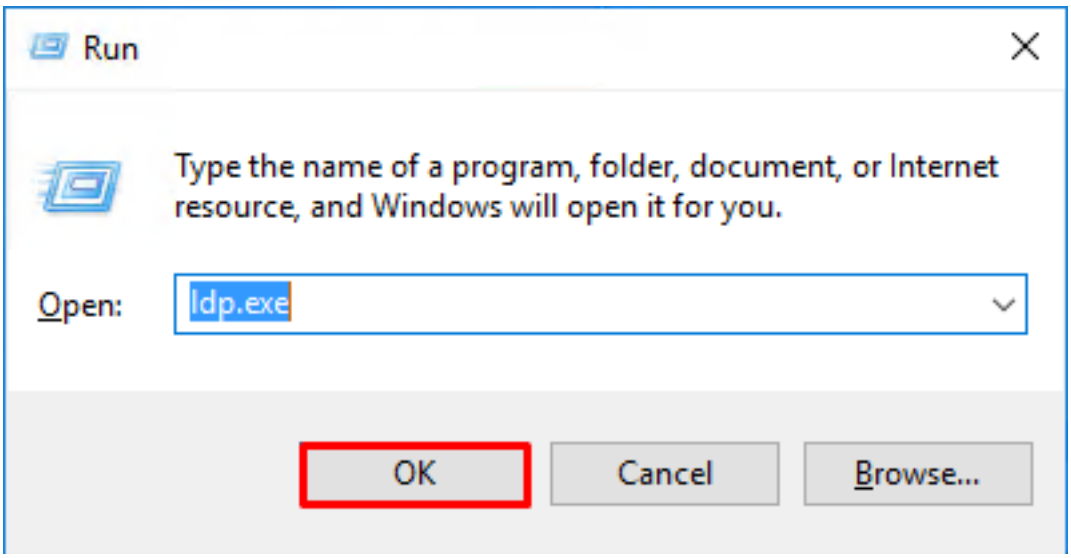
바인딩 로그인 DN 및/또는 암호가 잘못되었습니다.

```
[-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
```

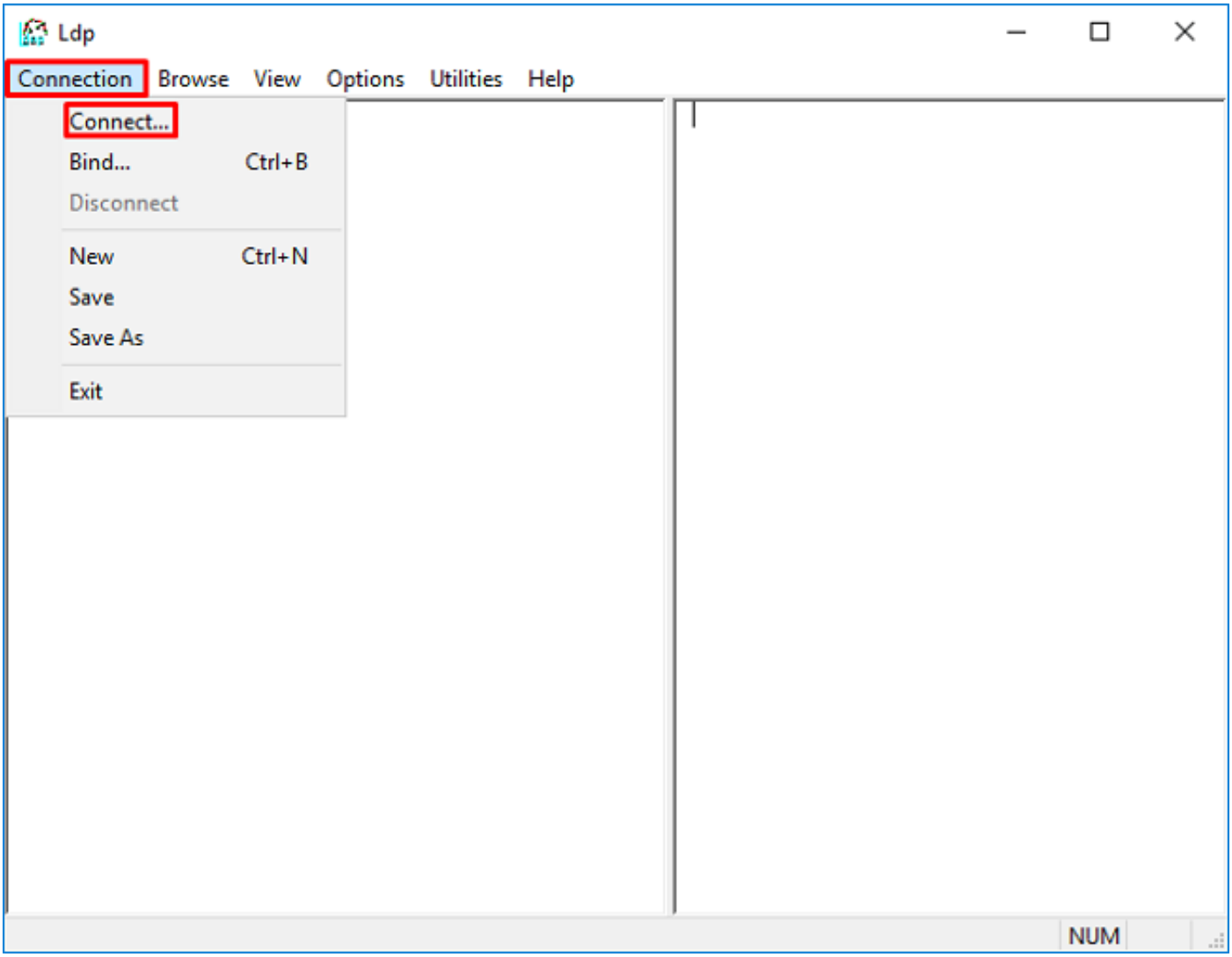
```
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

잠재적 솔루션:로그인 DN 및 로그인 비밀번호가 적절하게 구성되었는지 확인합니다.이는 ldp.**exe**를 사용하여 AD 서버에서 확인할 수 있습니다.계정이 ldp 사용과 성공적으로 바인드될 수 있는지 확인하려면 다음 단계를 수행하십시오.

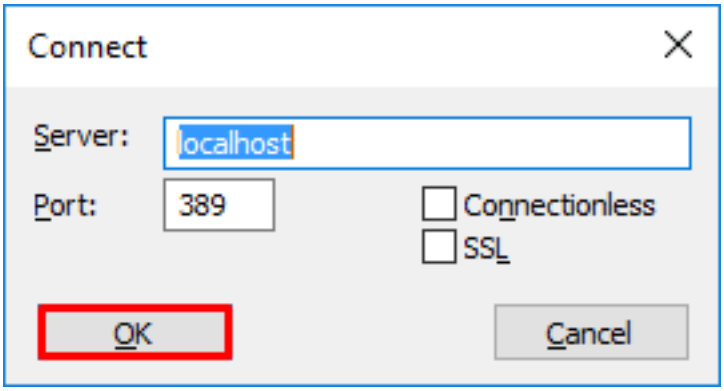
1. AD 서버에서 **Win+R**을 누르고 **ldp.exe**를 **검색합니다**.



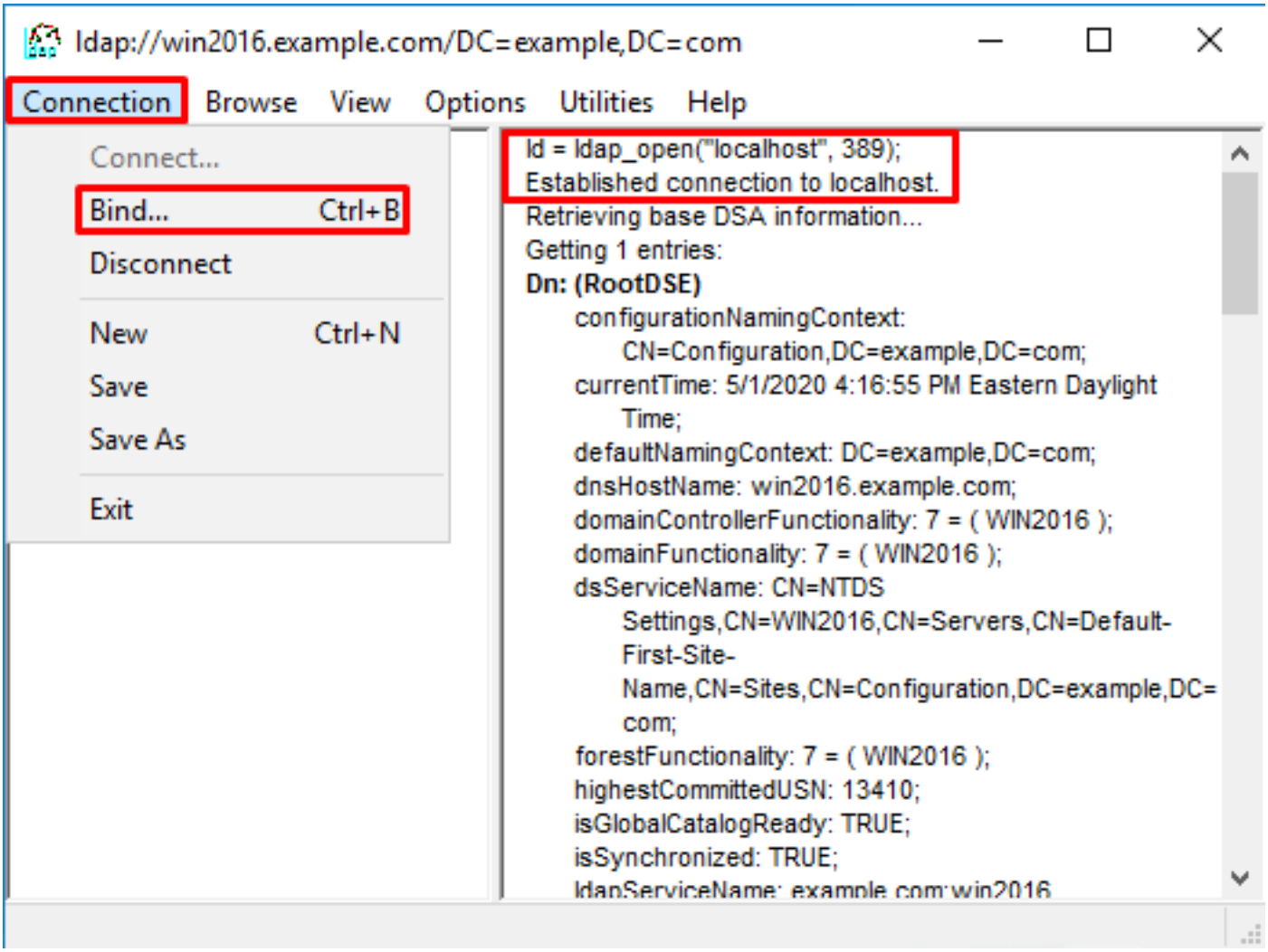
2. 연결 **> 연결...을 클릭합니다.** 이미지에 표시된 것처럼



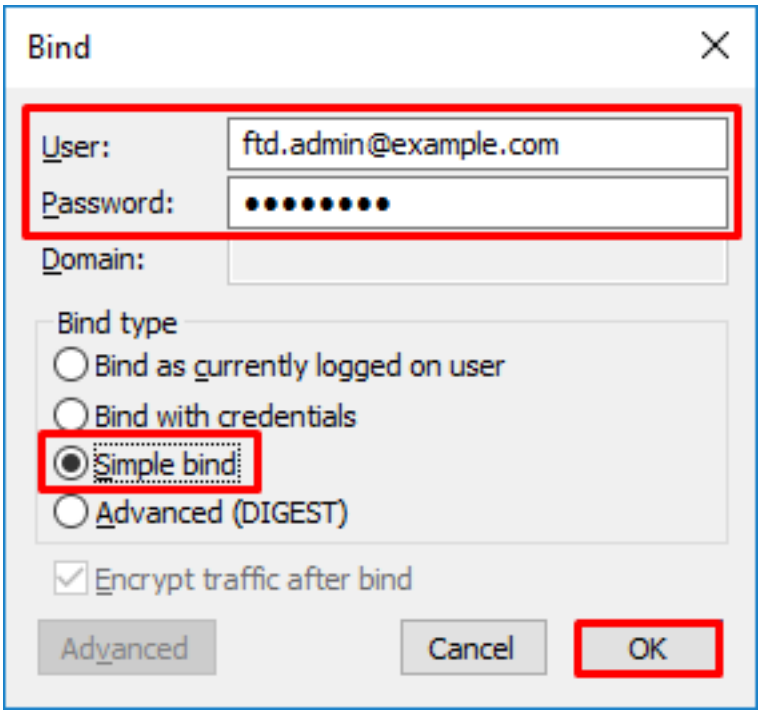
3. 서버의 localhost와 해당 포트를 지정한 다음 **확인**을 클릭합니다.



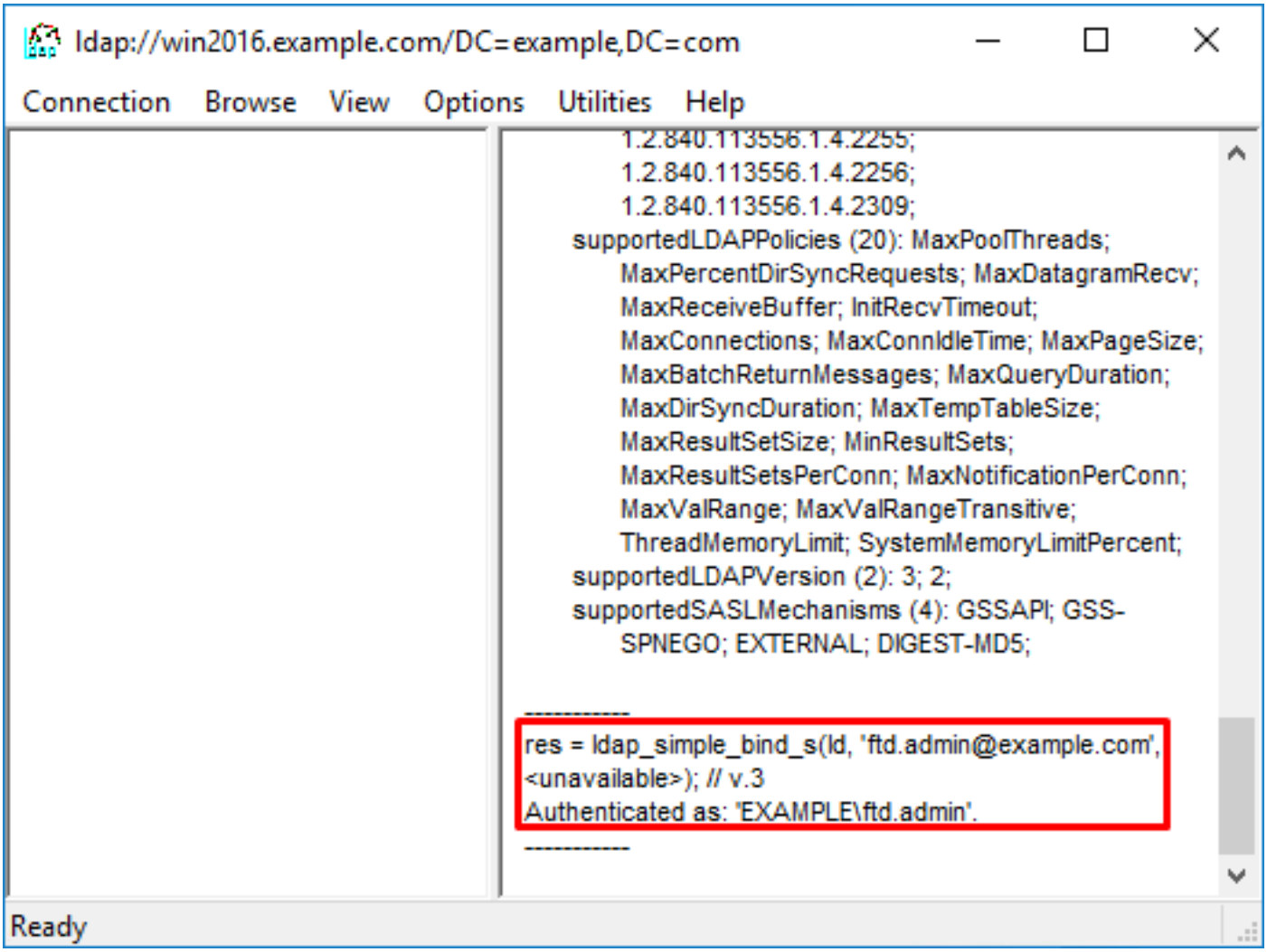
4. 오른쪽 열에는 성공적인 연결을 나타내는 텍스트가 표시됩니다.Connection(**연결**) **> Bind...를 클릭합니다.** 이미지에 표시된 것처럼



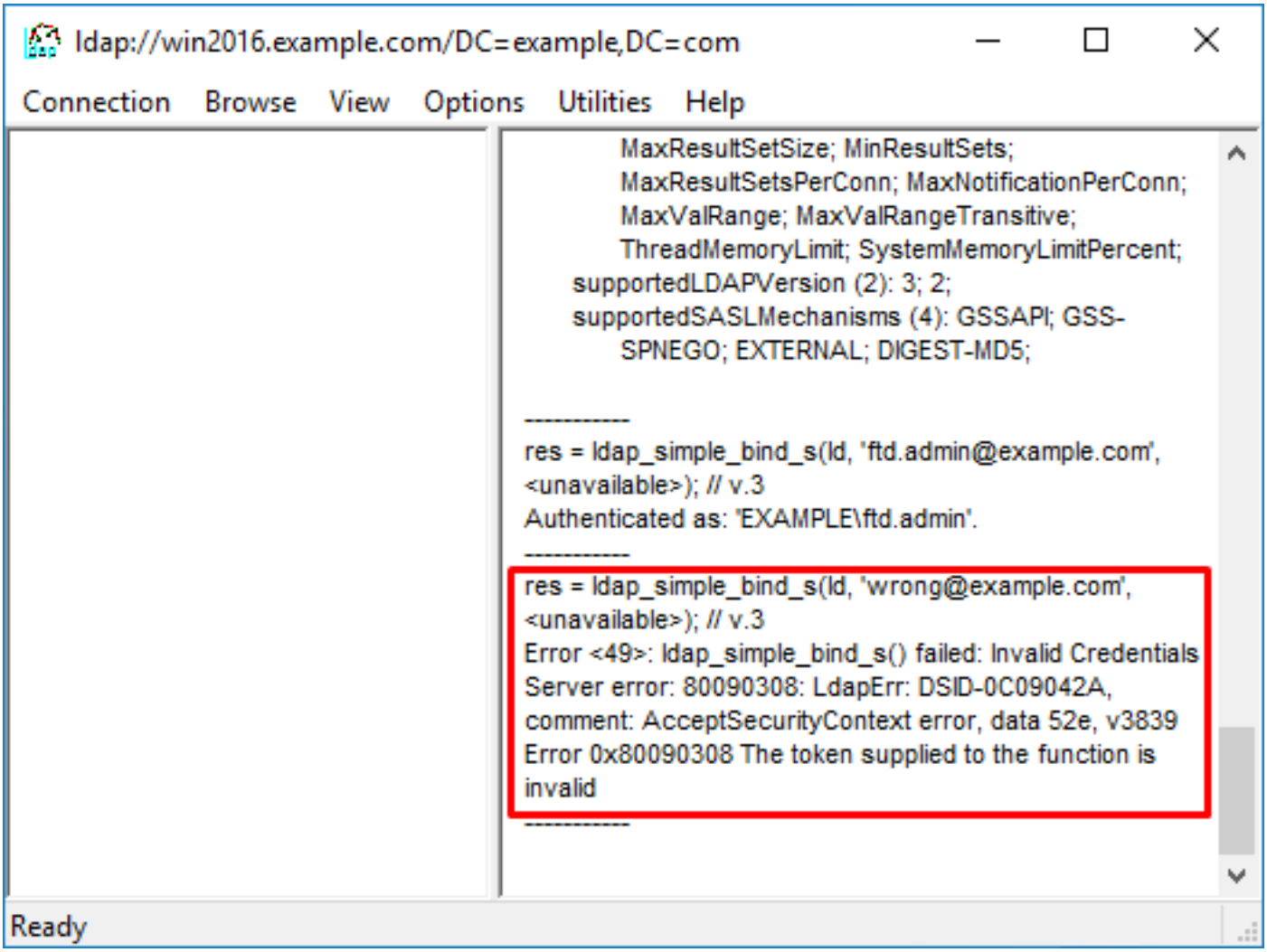
5. **단순 바인드**를 선택한 다음 디렉토리 계정 사용자 이름 및 비밀번호를 지정합니다.**확인**을 **클릭합니다**.



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



유효하지 않은 사용자 이름 또는 비밀번호로 바인딩을 시도하면 이러한 오류가 발생합니다.

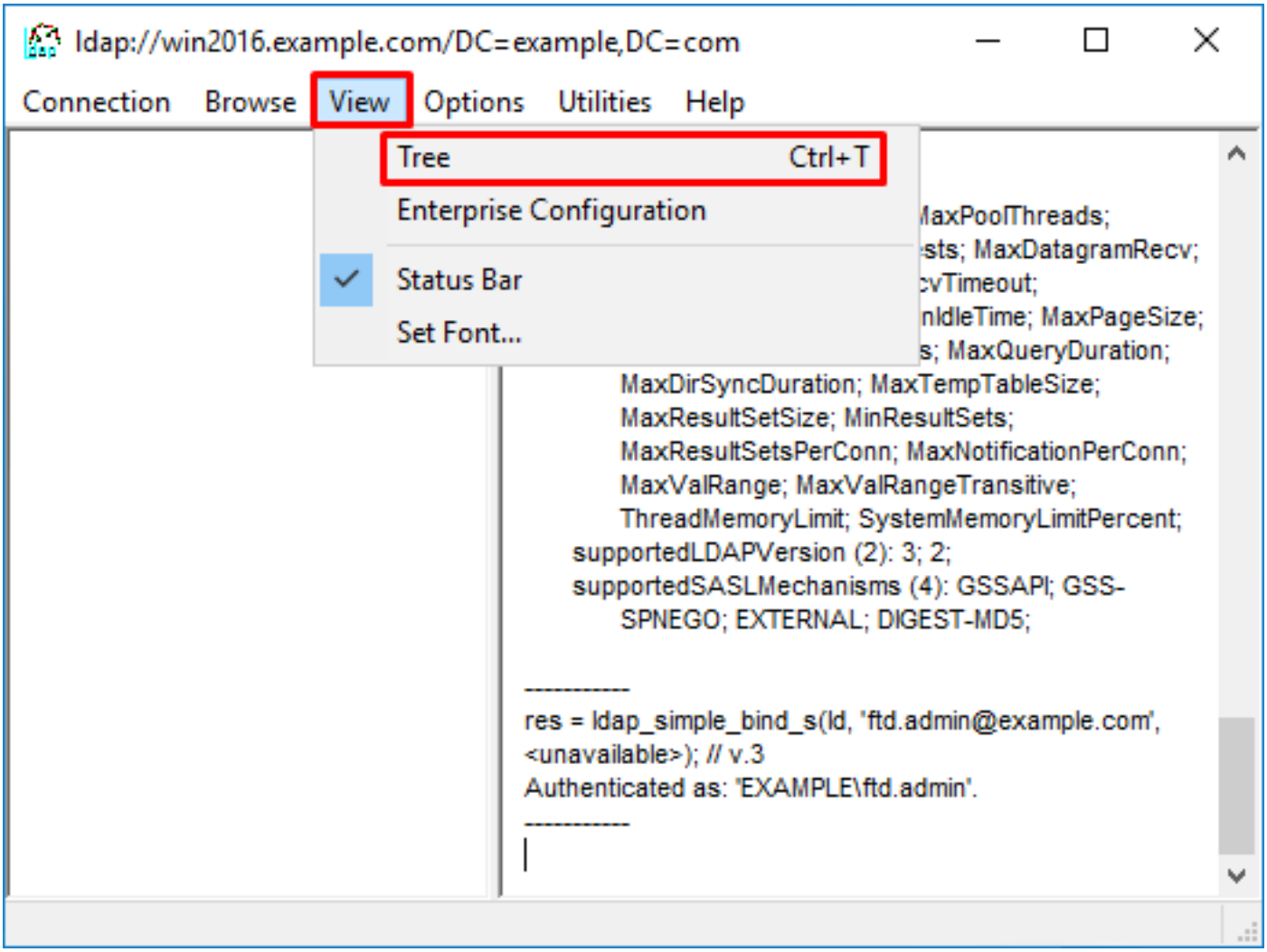


LDAP 서버에서 사용자 이름을 찾을 수 없음

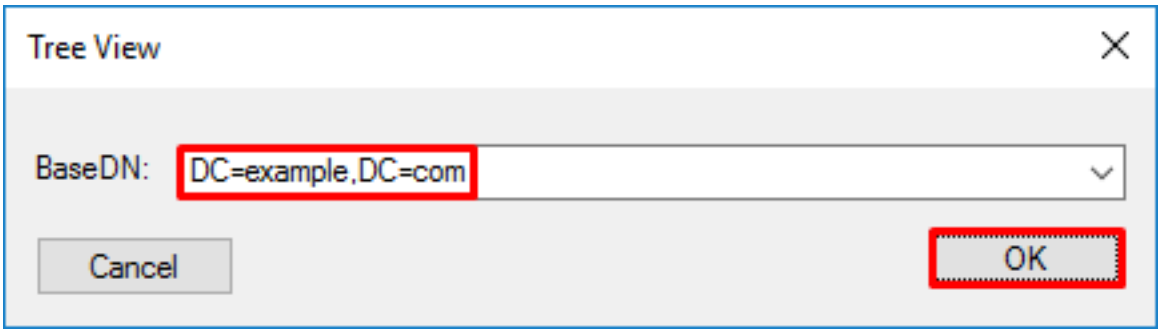
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] 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 수행한 검색으로 사용자를 찾을 수 있는지 확인합니다.ldp.exe도 사용할 수 있습니다.

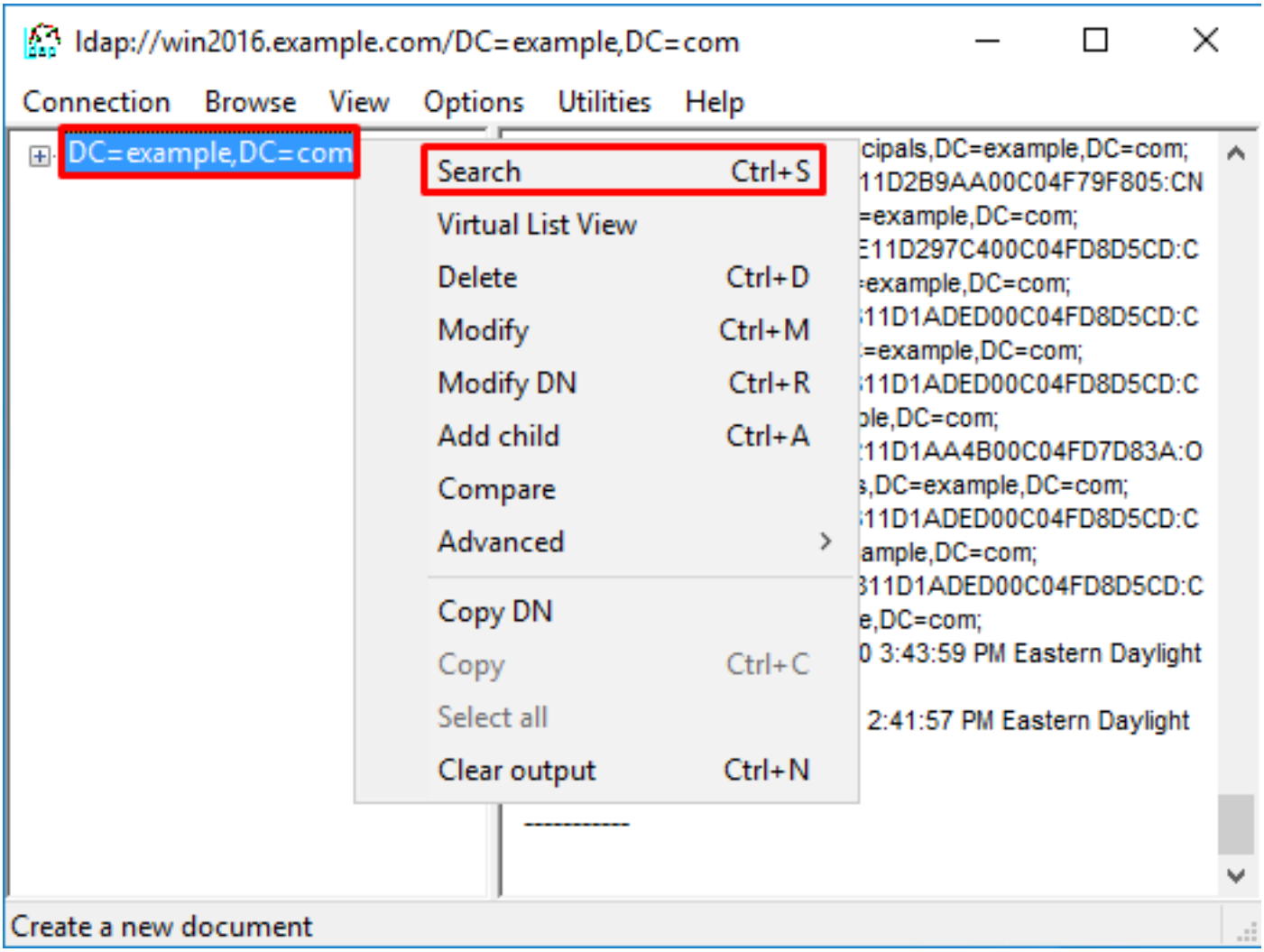
1. 바인딩이 성공적으로 완료되면 이미지에 표시된 대로 **보기 > 트리**로 이동합니다.



2. FTD에 구성된 기본 DN을 지정한 다음 **OK**를 클릭합니다.

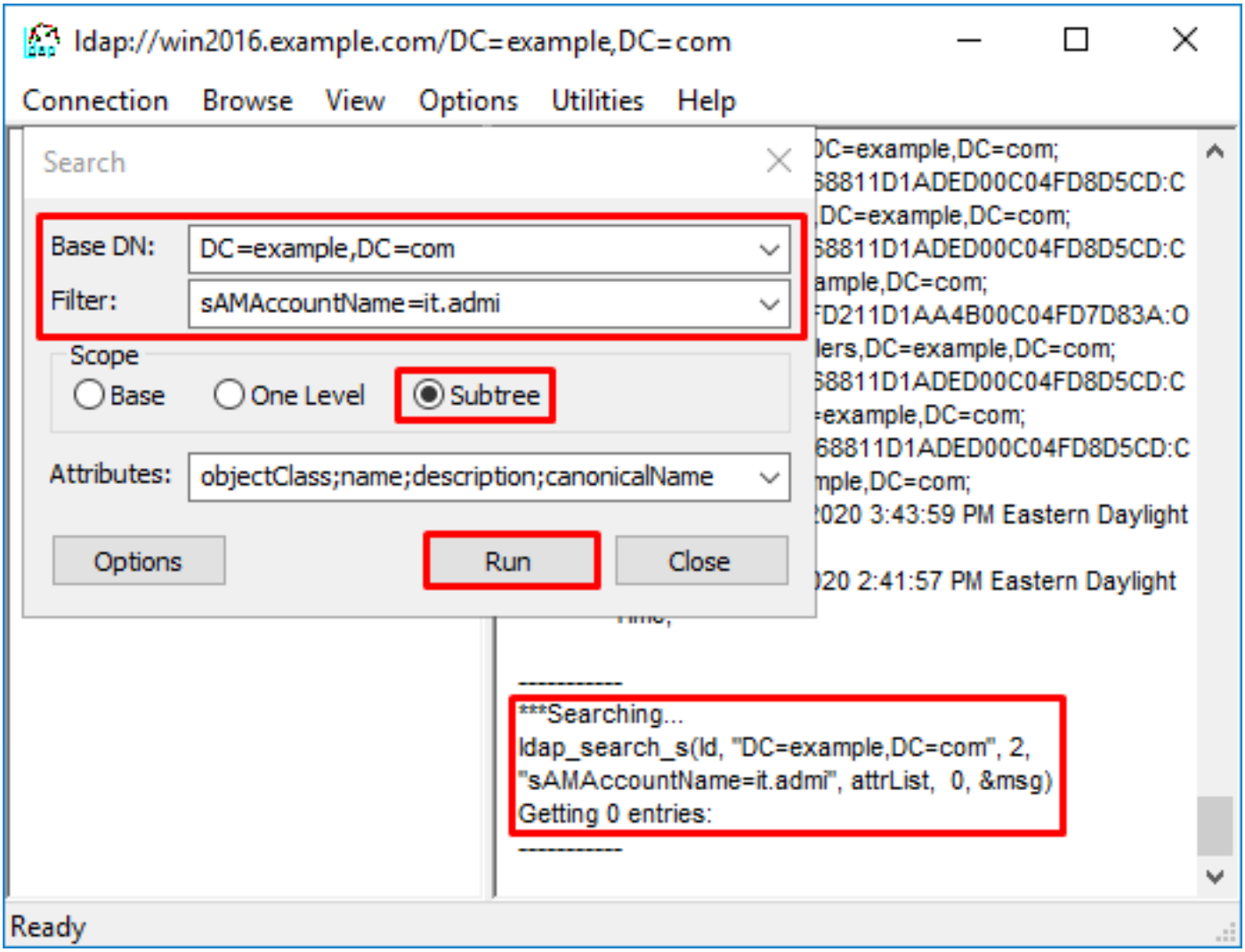


3. 기본 DN을 마우스 오른쪽 버튼으로 클릭한 다음 이미지에 표시된 대로 Search(검색)를 클릭합니다.



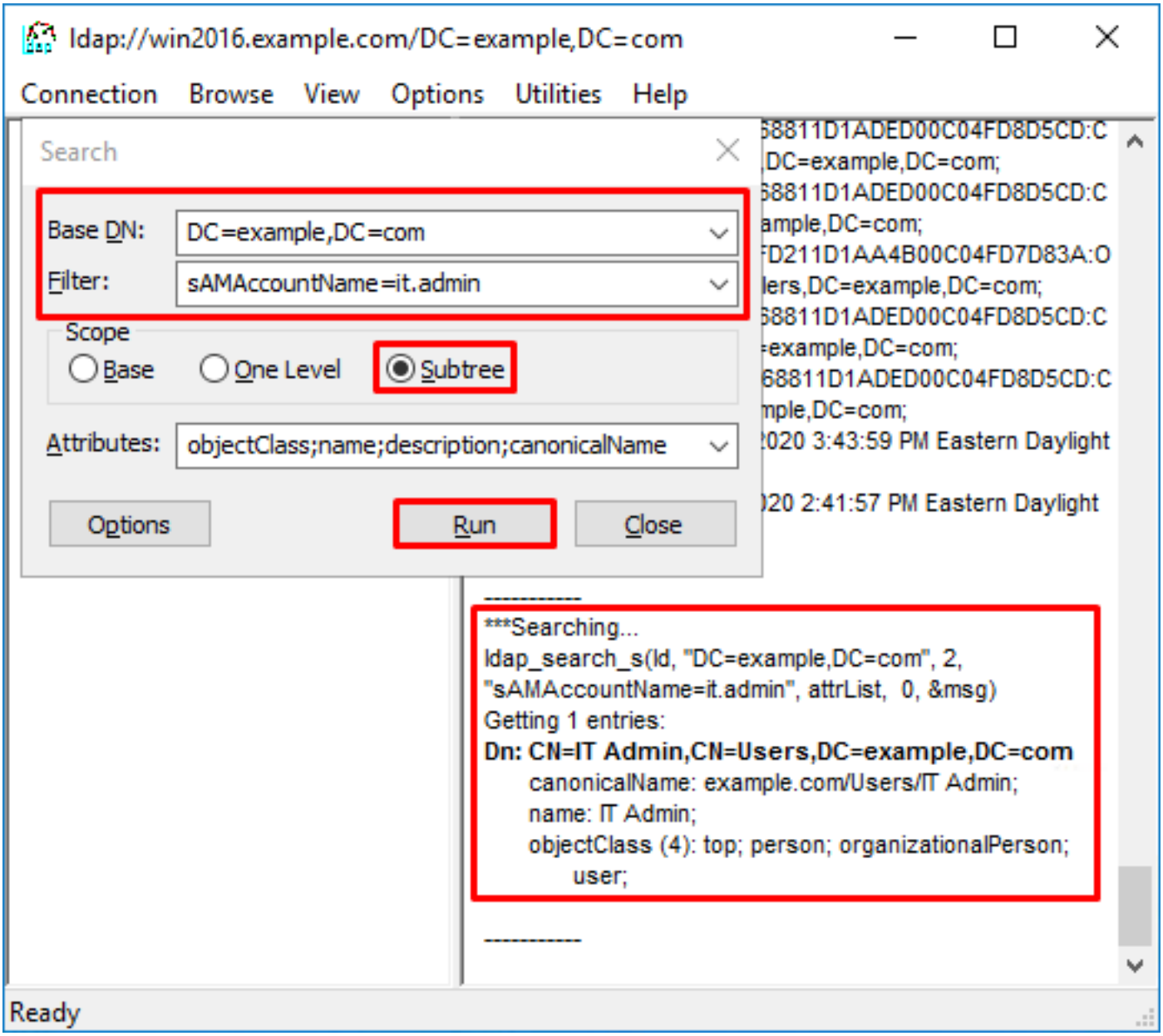
4. 디버그에 표시된 것과 동일한 기본 DB, 필터 및 범위 값을 지정합니다.이 예에서는 다음과 같습니다.

- 기본 DN:dc=예,dc=com
- 필터:samaccountname=it.admi
- 범위:SUBTREE



ldp는 Base DN dc=example,dc=com에서 samaccountname=**it.admi**를 가진 사용자 계정이 없기 때문에 0 항목을 찾습니다.

올바른 samaccountname=**it.admin으로** 다시 시도하면 다른 결과가 표시됩니다.ldp는 Base DN dc=example,dc=com 아래에서 1개의 항목을 찾고 해당 사용자의 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 솔루션:사용자의 비밀번호가 적절하게 구성되어 있고 만료되지 않았는지 확인합니다.로그인 DN과 마찬가지로 FTD는 사용자의 자격 증명을 사용하여 AD에 대해 바인딩을 수행합니다.이 바인딩은 AD가 동일한 사용자 이름과 암호 자격 증명을 인식할 수 있는지 확인하기 위해 ldp에서도 수행할 수 있습니다.ldp의 단계는 Binding Login **DN 및/또는 Password Incorrect** 섹션에 **표시됩니다**.또한 Microsoft Server Event Viewer 로그를 검토하면 가능한 이유를 알 수 있습니다.

테스트 AAA

특정 사용자 이름 및 비밀번호로 FTD에서 인증 시도를 시뮬레이션하기 위해 test aaa-server 명령을 사용할 수 있습니다.연결 또는 인증 실패를 테스트하는 데 사용할 수 있습니다.이 명령은 **테스트 aaa-server authentication [AAA-server] host [AD IP/hostname]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 연결할 수 있는지 확인할 수 있습니다.LDAP 패킷이 FTD에서 나가지만 응답이 없는 경우 라우팅 문제를 나타낼 수 있습니다.

다음은 양방향 LDAP 트래픽을 보여 주는 캡처입니다.

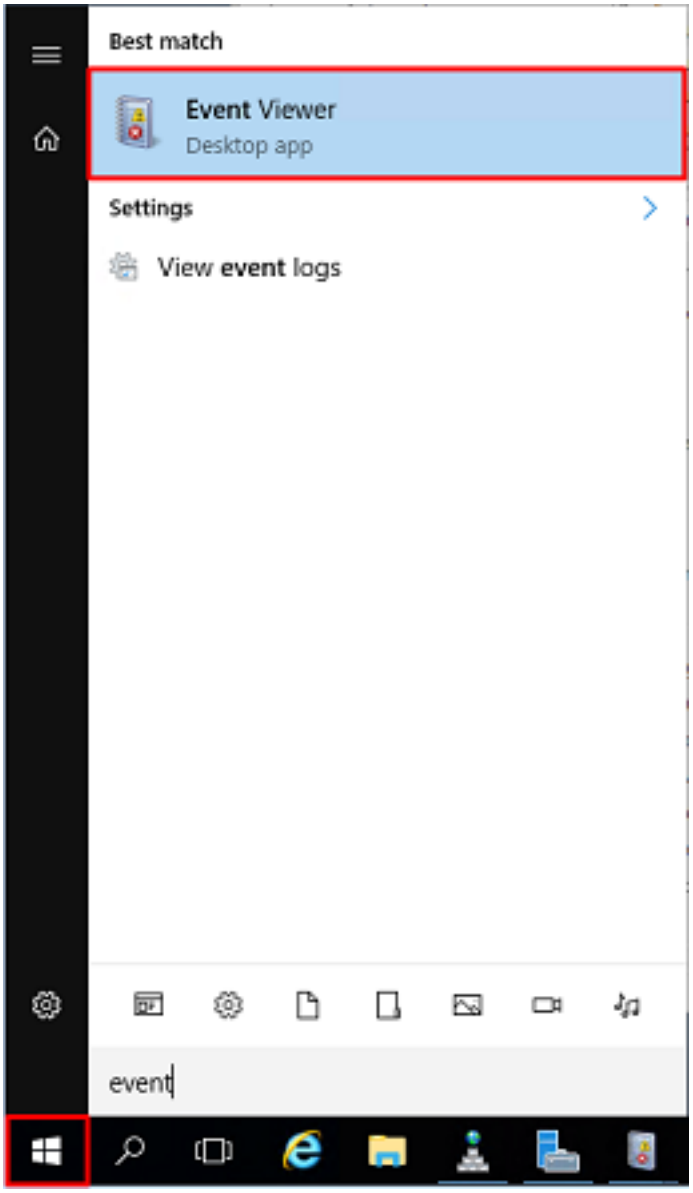
```
> show route 192.168.1.1

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
```

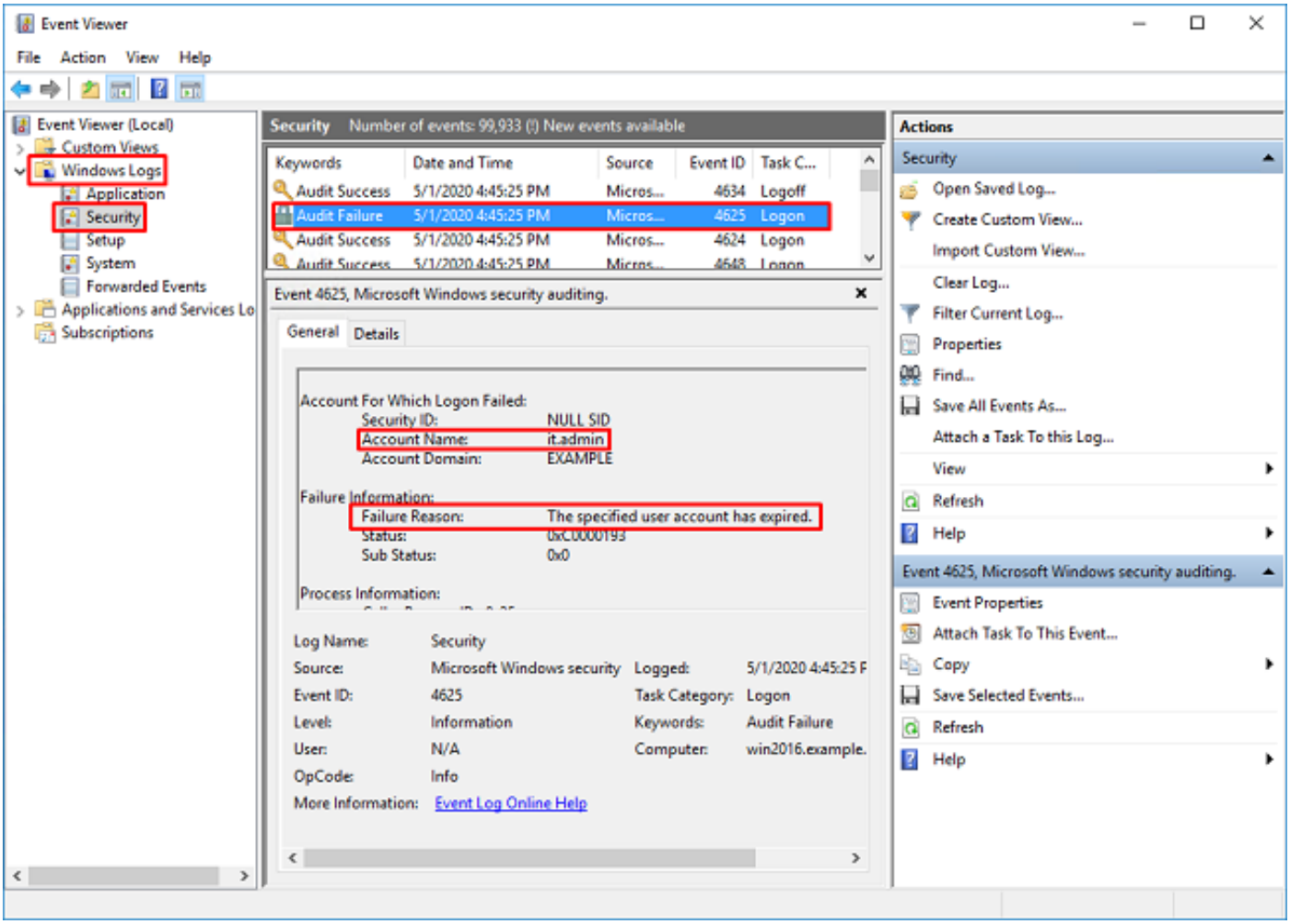
Windows Server 이벤트 뷰어 로그

AD 서버 밴의 이벤트 뷰어 로그는 오류가 발생한 이유에 대한 자세한 정보를 제공합니다.

1. **이벤트 뷰어**를 검색하고 엽니다.



2. **Windows 로그를 확장하고 보안**을 클릭합니다.사용자의 **계정** 이름으로 감사 실패를 검색하고 이미지에 표시된 대로 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