ISE 및 LDAP 특성 기반 인증

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)를 구성하고 LDAP(Lightweight Directory Access Protocol) 개체 특성을 사용하여 디바이스를 동적으로 인증하고 권한을 부여하는 방법에 대해 설명합니다.

> **참고:이 문서는 ISE 인증 및 권한 부여를 위한 외부 ID 소스로 LDAP를 사용하는 설정에 유효합니다.**

기고자: 엠마뉴엘 카노 및 마우리시오 라모스 Cisco Professional Services 엔지니어

Neri Cruz Cisco TAC 엔지니어가 편집했습니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 알고 있는 것이 좋습니다.

- ISE 정책 집합, 인증 및 권한 부여 정책에 대한 기본 지식
- MAB(Mac Authentication Bypass)
- RADIUS 프로토콜에 대한 기본 지식
- Windows 서버에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE, 버전 2.4 패치 11
- Microsoft Windows Server, 버전 2012 R2 x64
- Cisco Switch Catalyst 3650-24PD, 버전 03.07.05.E(15.2(3)E5)
- Microsoft Windows 7 컴퓨터

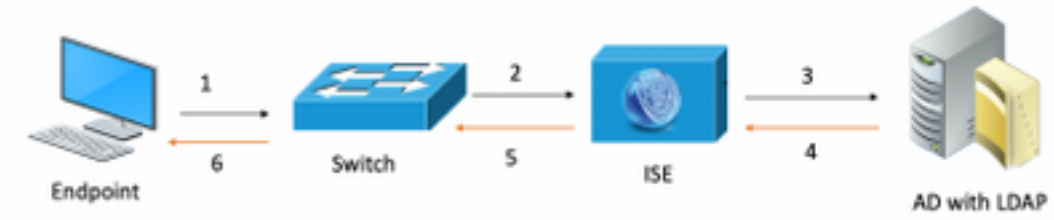
> **참고:**이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 네트워크 디바이스를 구성하고, ISE와 LDAP를 통합하며, 마지막으로 ISE 권한 부여 정책에서 사용할 LDAP 특성을 구성하는 방법에 대해 설명합니다.

네트워크 다이어그램

이 그림에서는 사용되는 네트워크 토폴로지를 보여 줍니다.



다음은 네트워크 다이어그램에 표시된 트래픽 흐름입니다.

1. 사용자는 PC/랩톱을 지정된 스위치 포트에 연결합니다.
2. 스위치는 해당 사용자에 대한 RADIUS 액세스 요청을 ISE로 전송합니다.
3. ISE가 정보를 수신하면 권한 부여 정책 조건에 사용할 속성을 포함하는 특정 사용자 필드에 대해 LDAP 서버에 쿼리합니다.
4. ISE가 특성(스위치 포트, 스위치 이름 및 디바이스 mac 주소)을 수신하면 스위치에서 제공하는 정보를 비교합니다.
5. 스위치에서 제공하는 특성 정보가 LDAP에서 제공하는 것과 동일한 경우 ISE는 권한 부여 프로파일에 구성된 권한으로 RADIUS Access-Accept를 보냅니다.

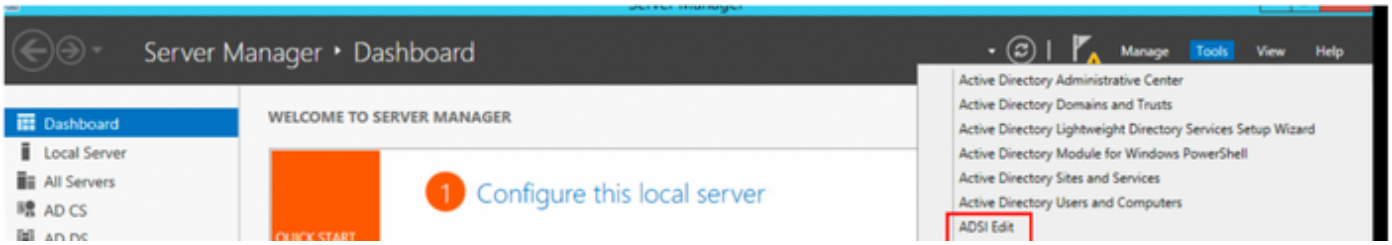
구성

LDAP, 스위치 및 ISE를 구성하려면 이 섹션을 사용합니다.

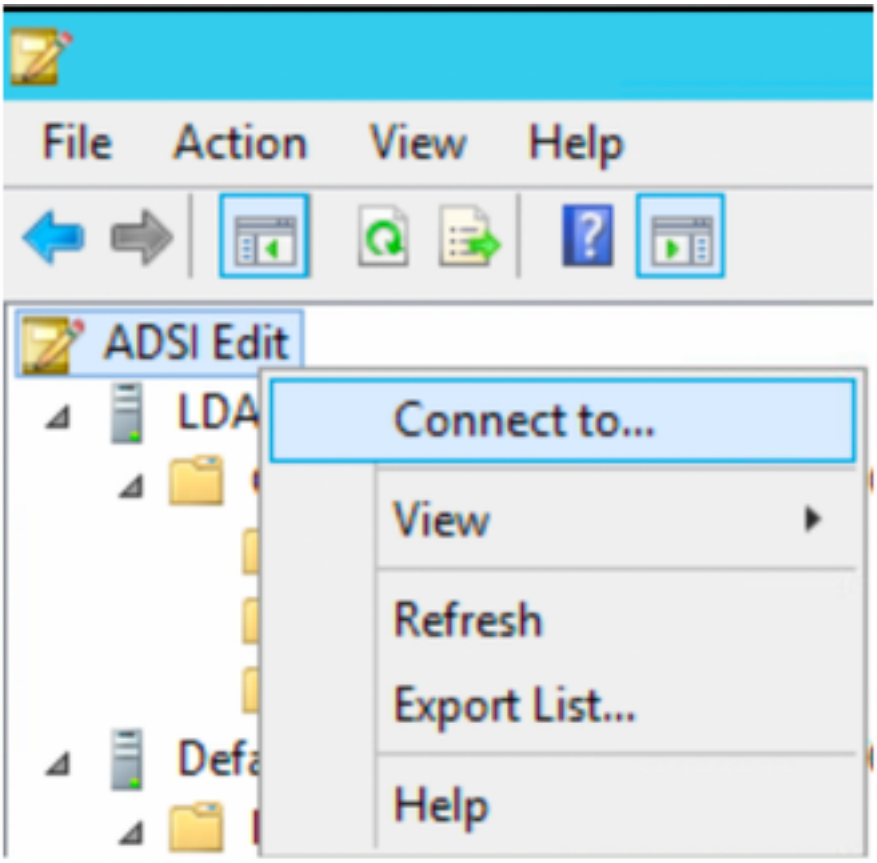
구성 LDAP

LDAP 서버를 구성하려면 다음 단계를 완료합니다.

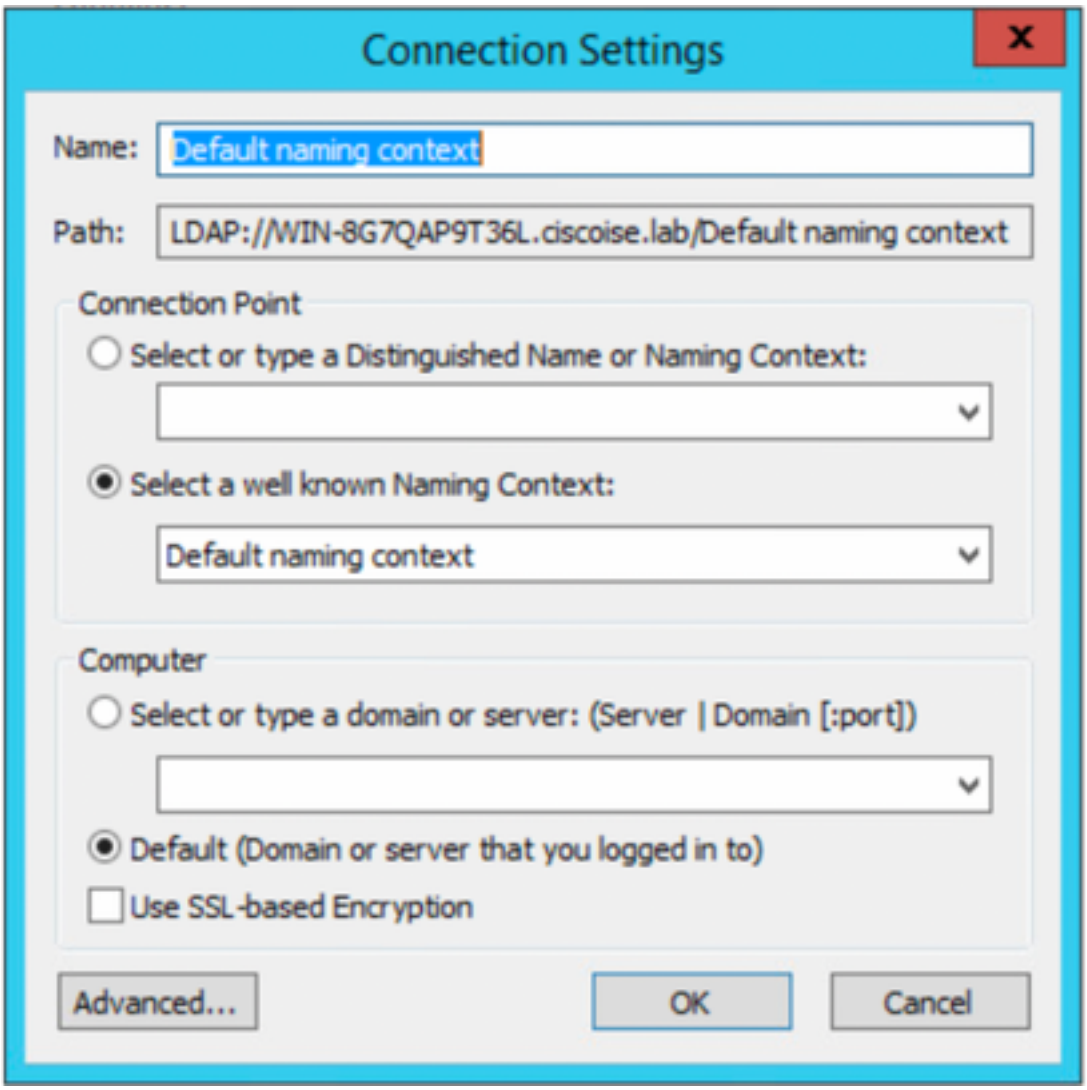
1. **서버 관리자 > 대시보드 > 도구 > ADSI 편집으로 이동합니다.**



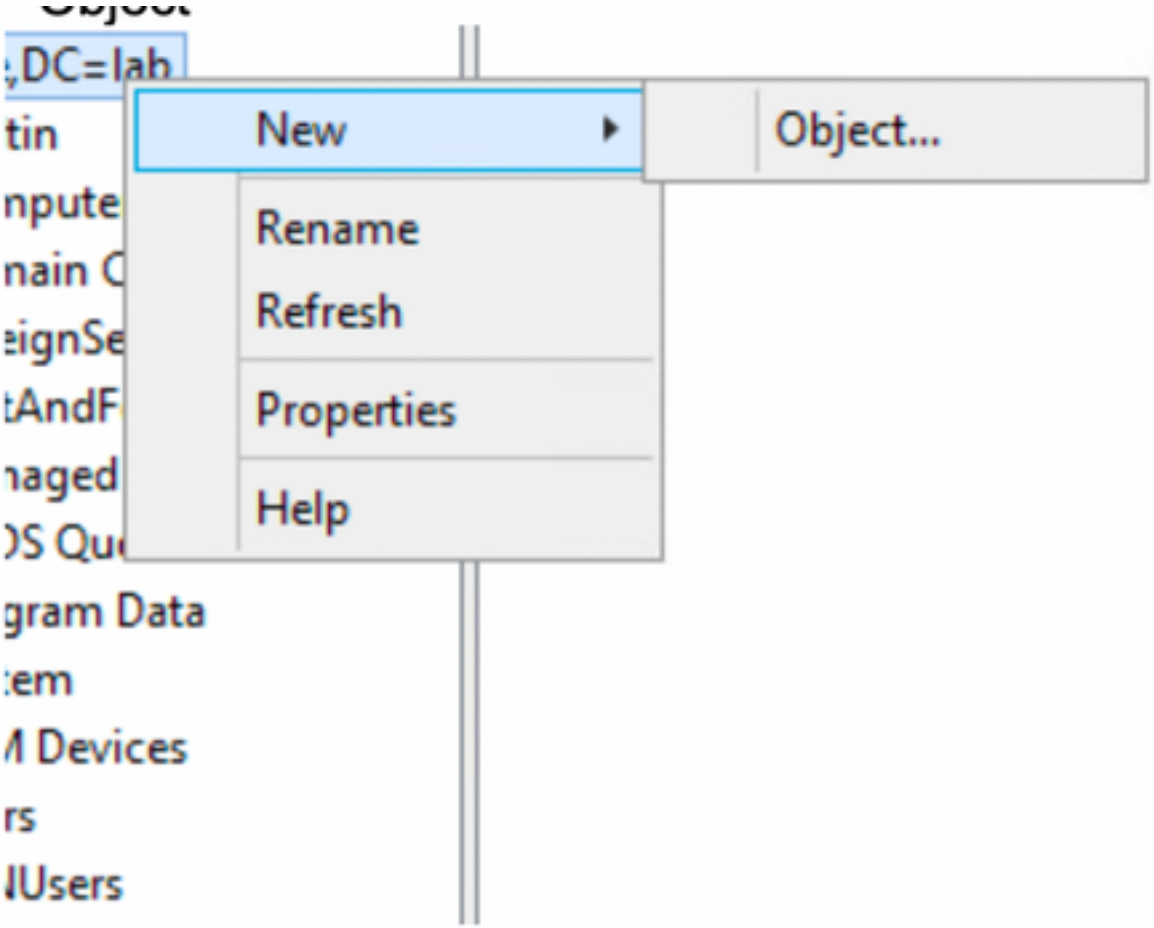
2. ADSI Edit(ADSI 수정) 아이콘을 마우스 오른쪽 버튼으로 클릭하고 Connect to..(연결 대상...)를 선택합니다.



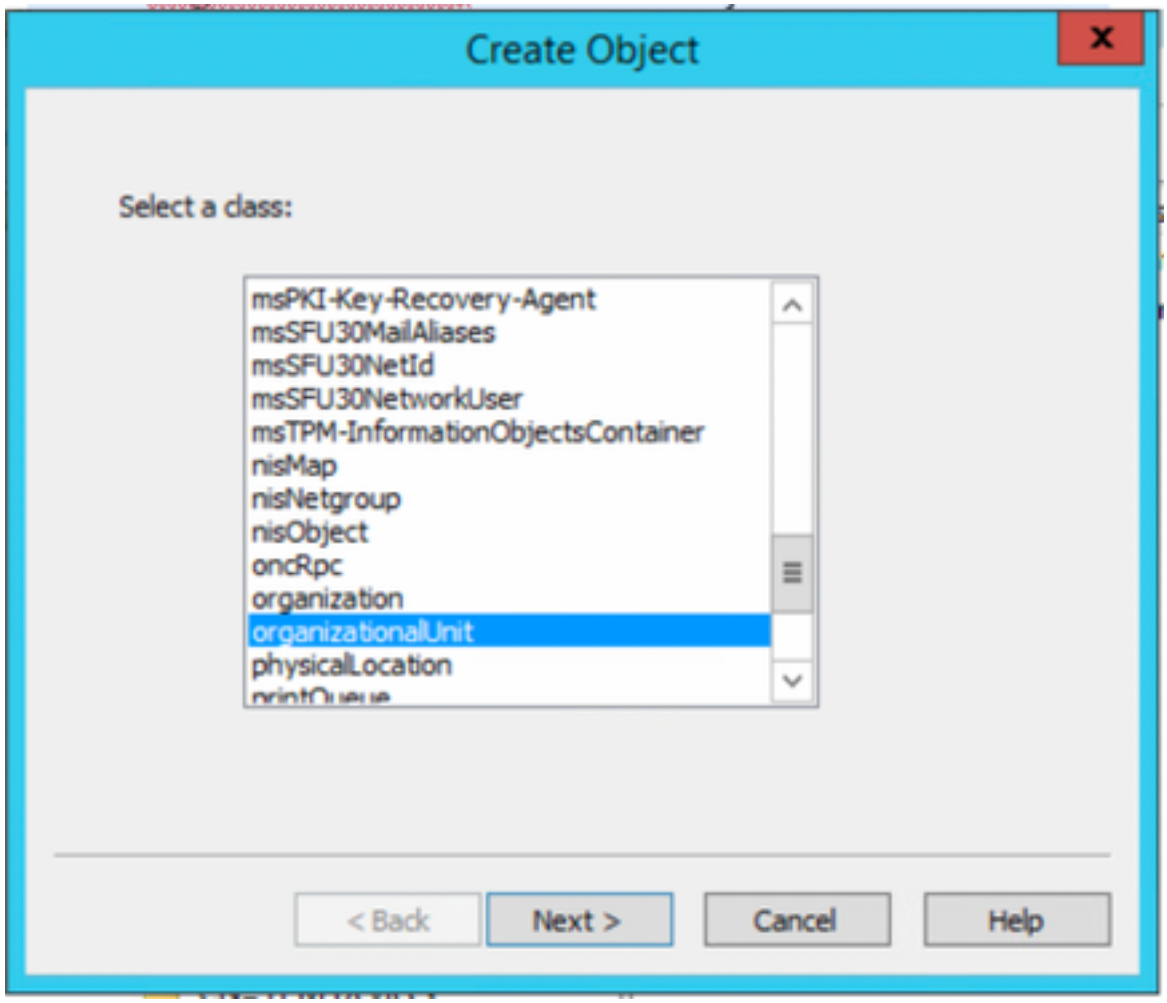
3. 연결 설정에서 이름을 정의하고 **확인** 버튼을 선택하여 연결을 시작합니다.



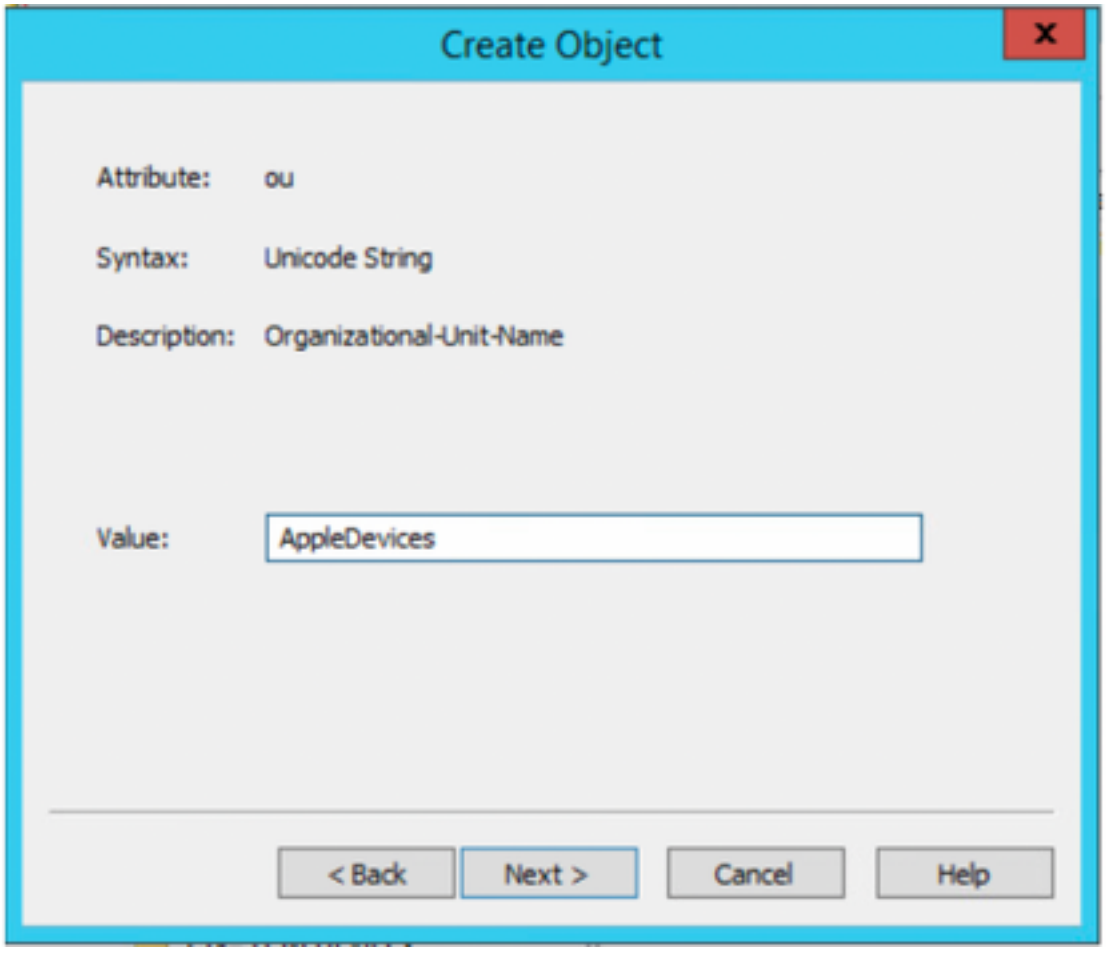
4. 동일한 ADSI 편집 메뉴에서 DC 연결(DC=ciscodemo, DC=lab)을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기를** 선택한 다음 옵션 **개체**를 선택합니다.



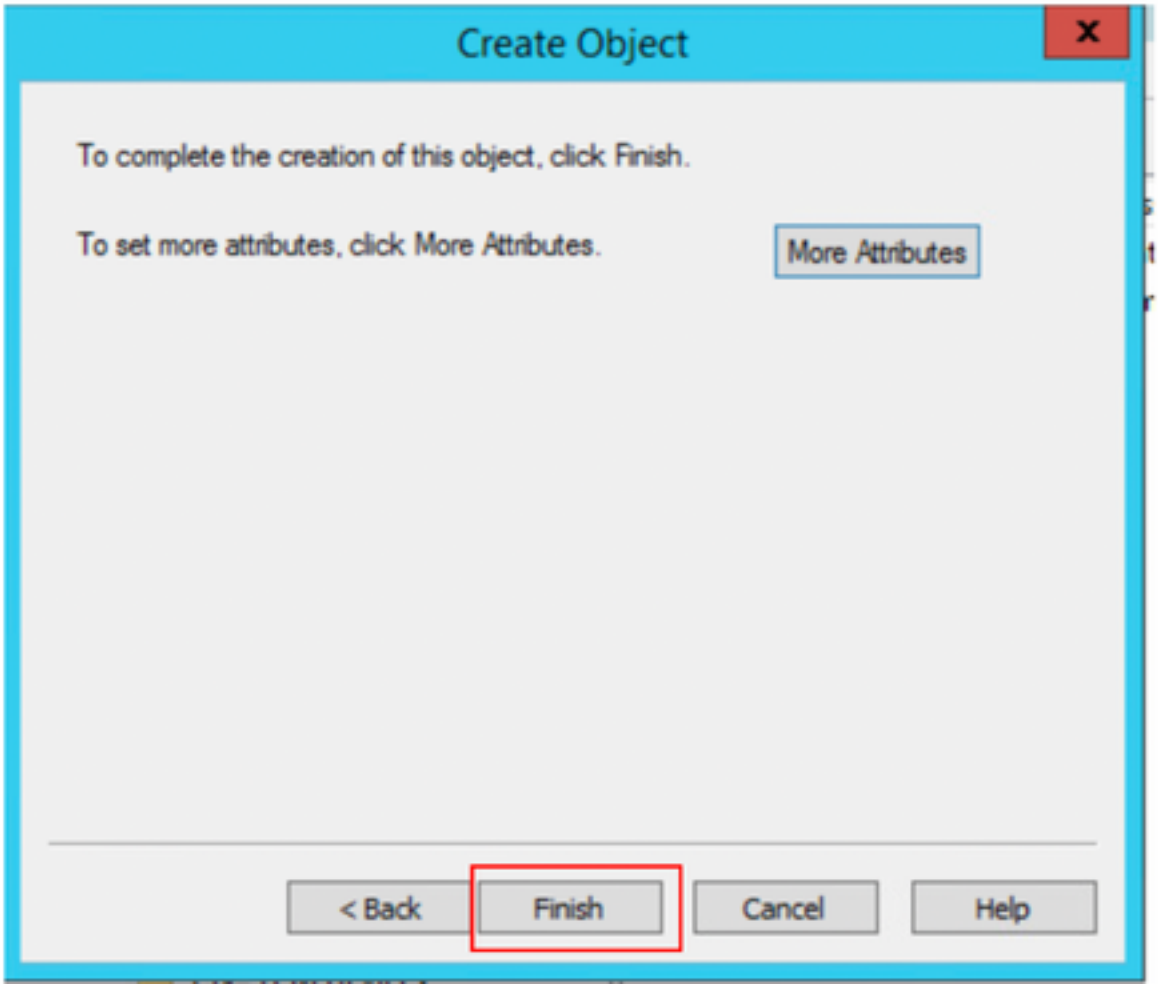
5. 옵션 OrganizationalUnit을 새 개체로 선택하고 **다음**을 선택합니다.



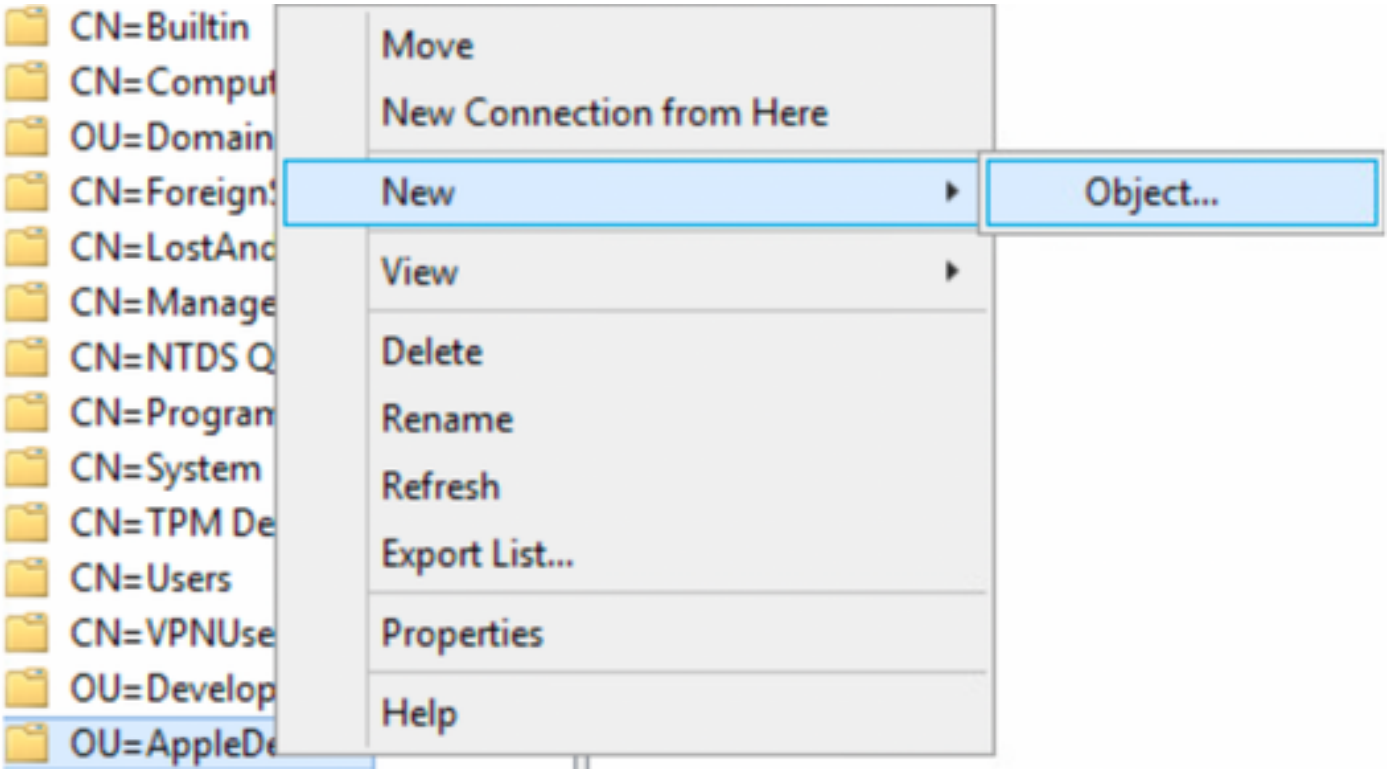
6. 새 조직 단위의 이름을 정의하고 **다음**을 선택합니다.



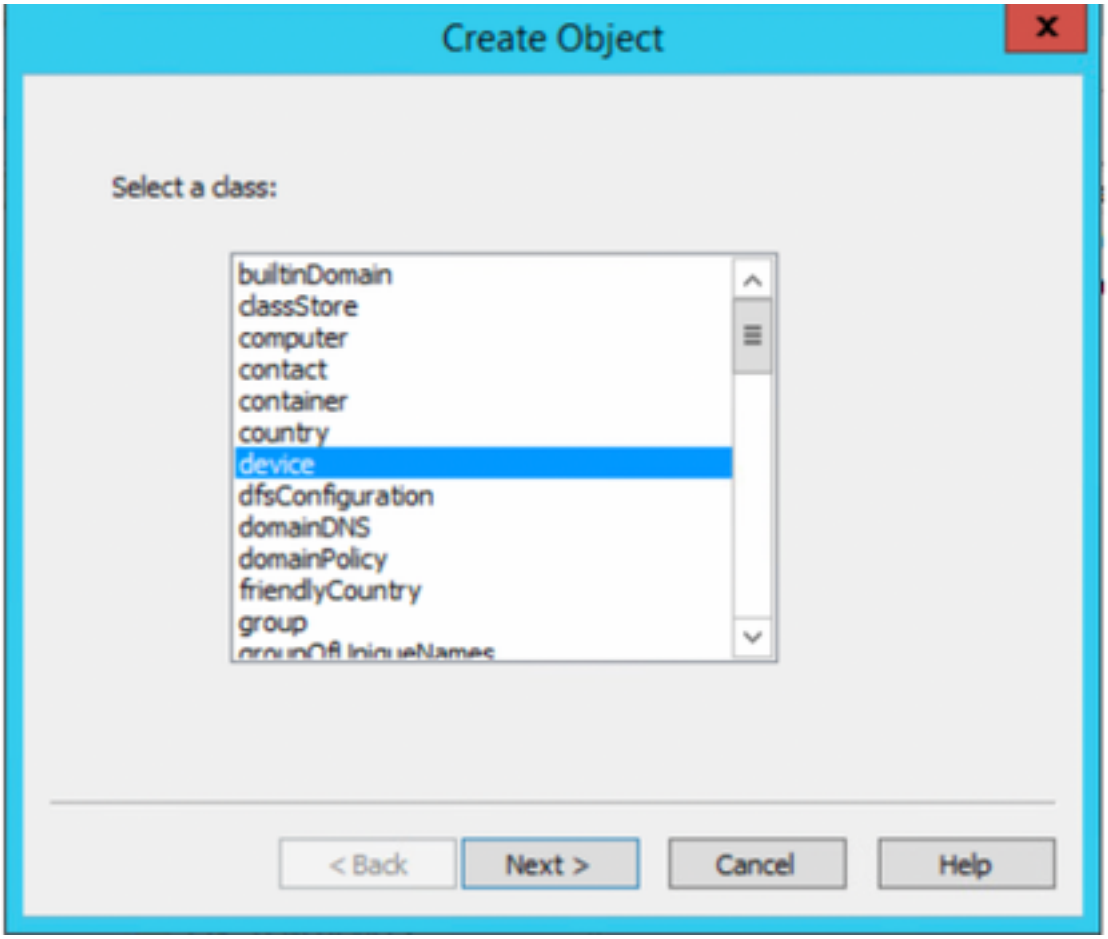
7. 새 **조직** 단위를 만들려면 완료를 선택합니다.



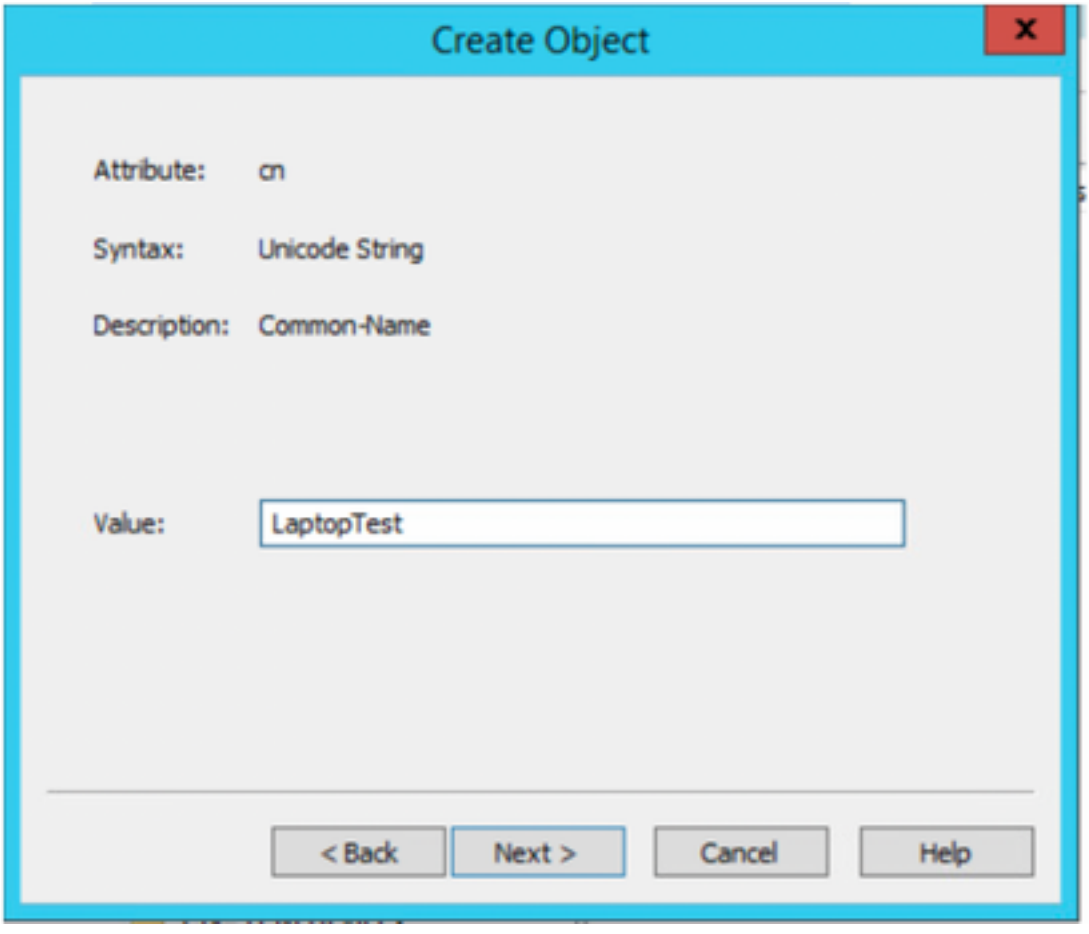
8. 방금 만든 OrganizationalUnit을 마우스 오른쪽 단추로 클릭하고 **새로 만들기 > 개체**를 선택합니다.



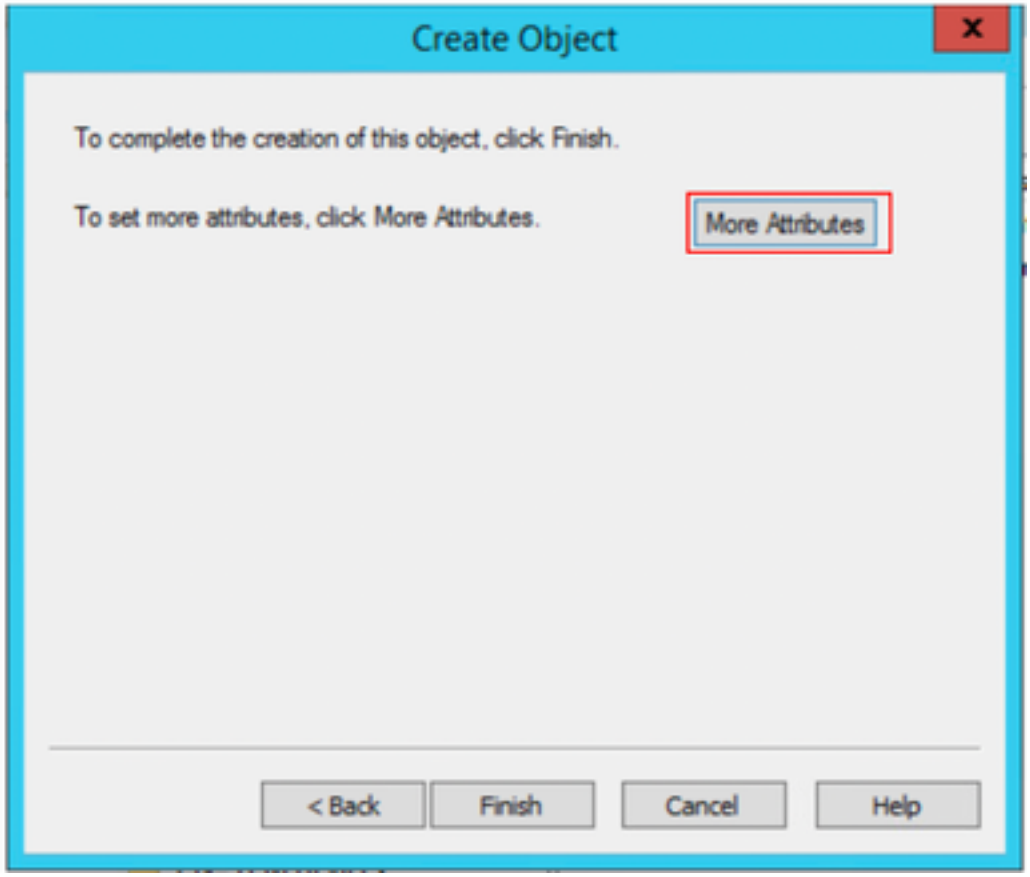
9.객체 클래스로 디바이스를 선택하고 **다음**



10.값 필드에서 이름을 정의하고 **다음**을 선택합니다.

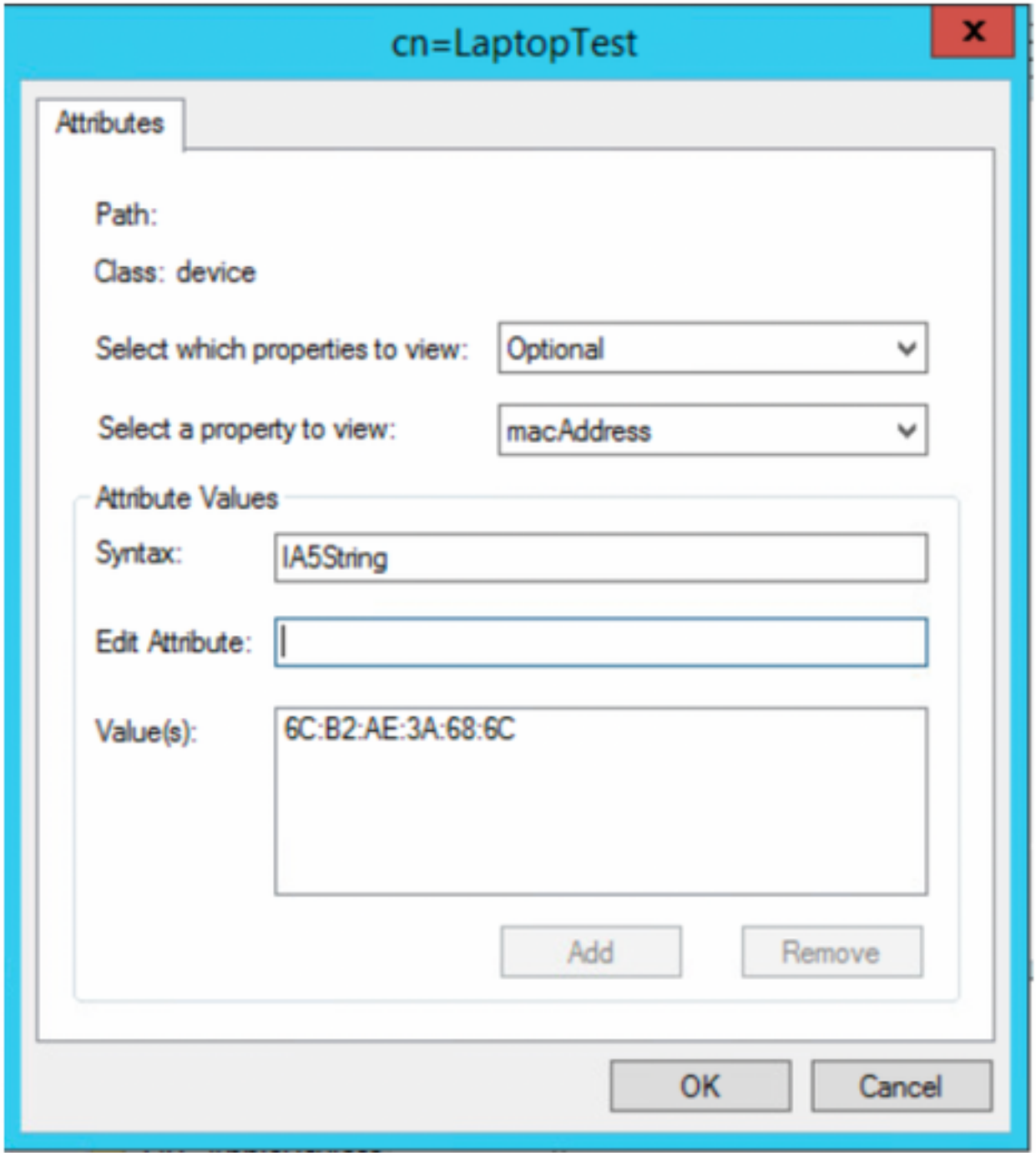


11. 추가 속성 옵션을 **선택합니다.**



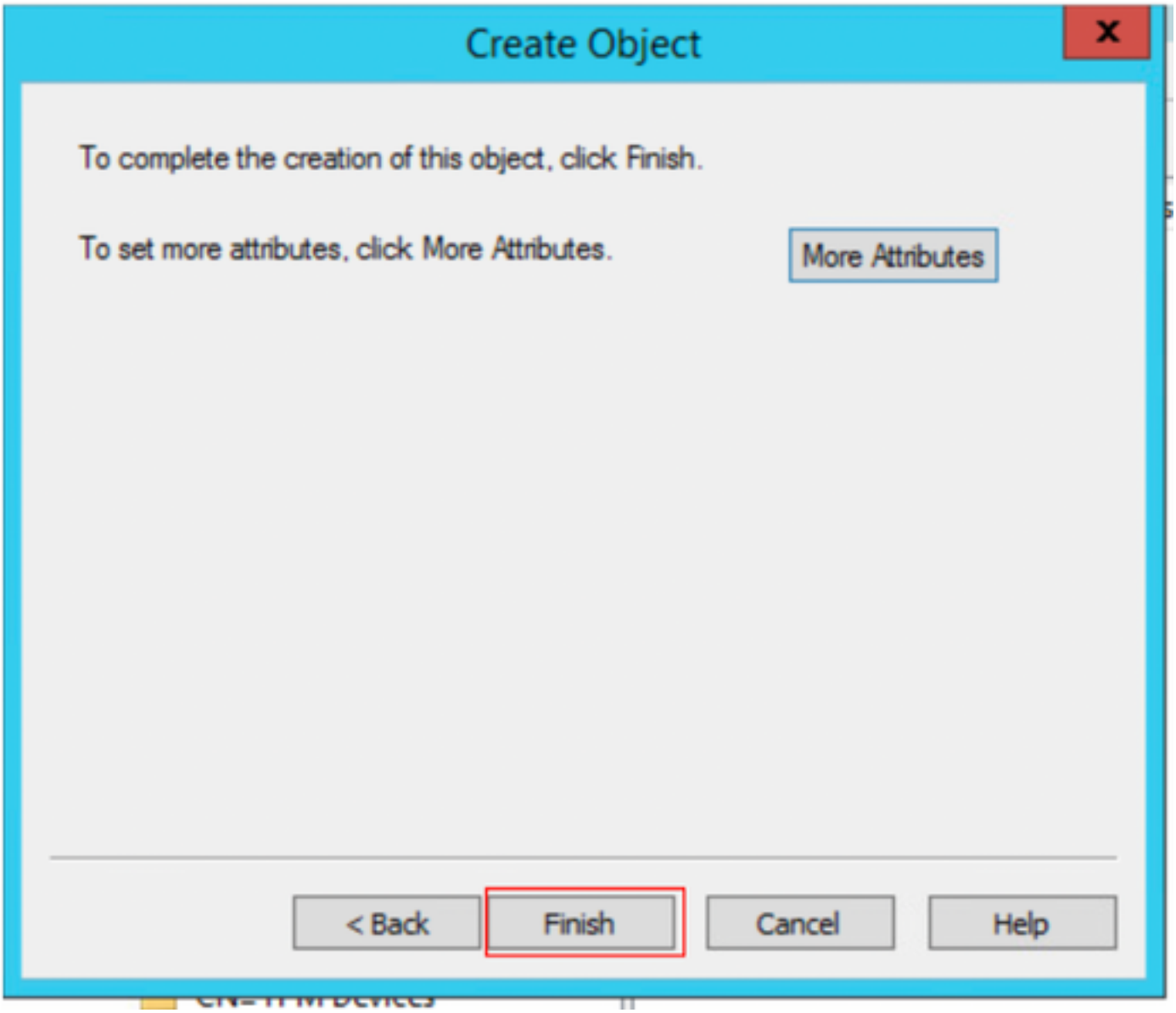
11. 드롭다운 메뉴에서 **볼 등록 정보를 선택하고 macAddress** 옵션**을** 선택한 다음 **Edit** attribute 필드에서 인증할 엔드포인트 Mac 주소를 정의하고 **추가** 버튼을 클릭하여 디바이스 MAC 주소를 저장합니다.

참고: mac 주소 8진수 사이에 점 또는 하이픈 대신 이중 콜론을 사용합니다.

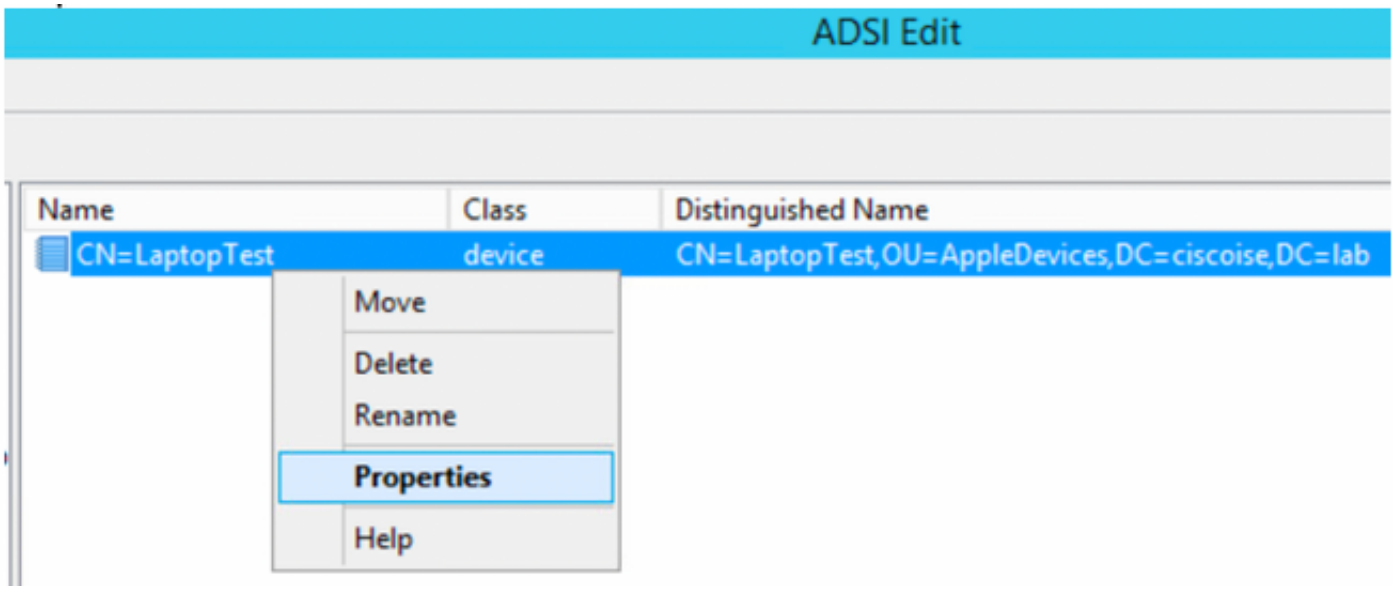


12. 정보를 저장하고 디바이스 객체 구성을 계속하려면 **확인**을 선택합니다.

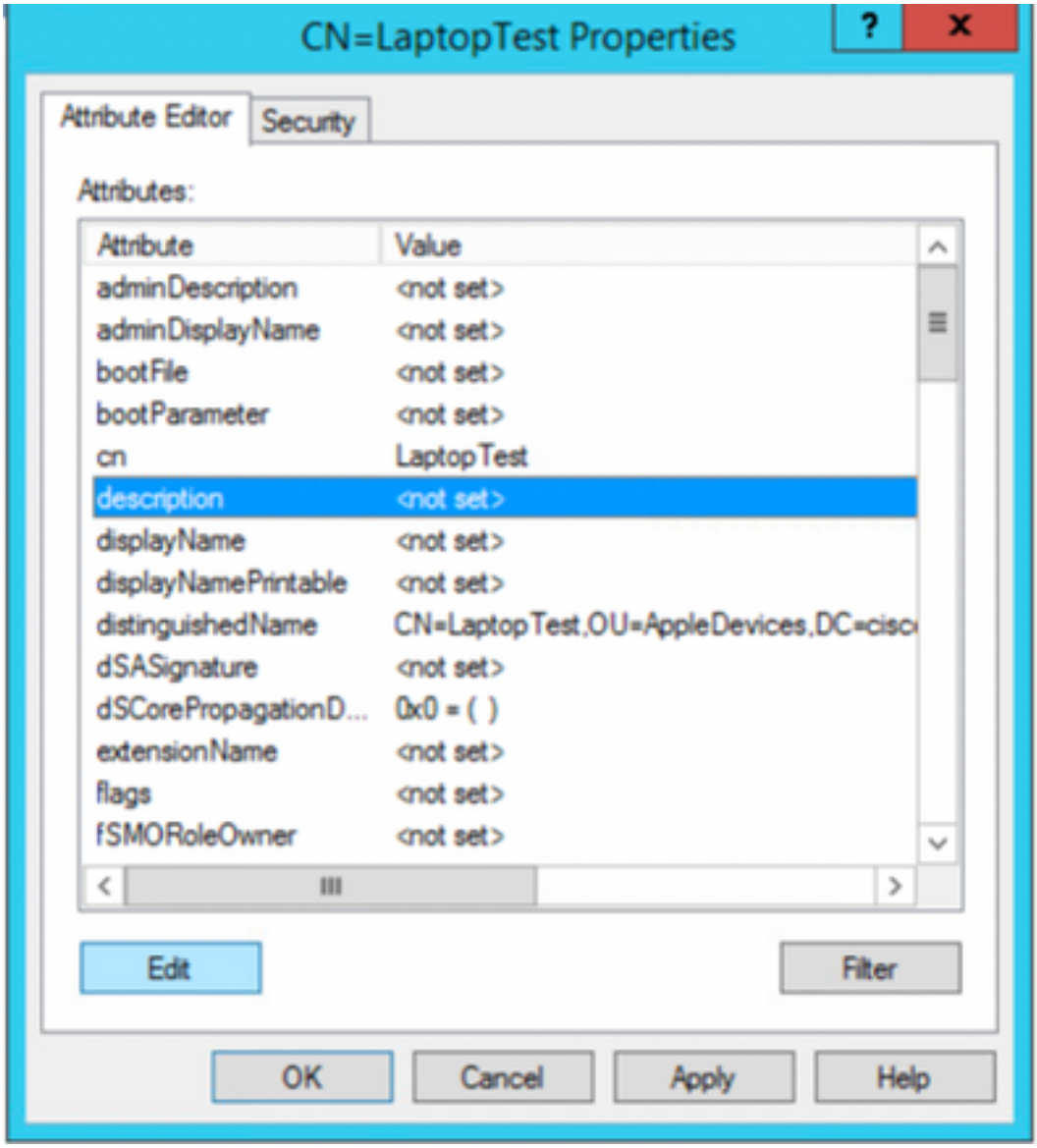
13. 새 디바이스 객체를 생성하려면 완료를 선택합니다.



14. 장치 개체를 마우스 오른쪽 단추로 클릭하고 옵션 **속성**을 선택합니다.

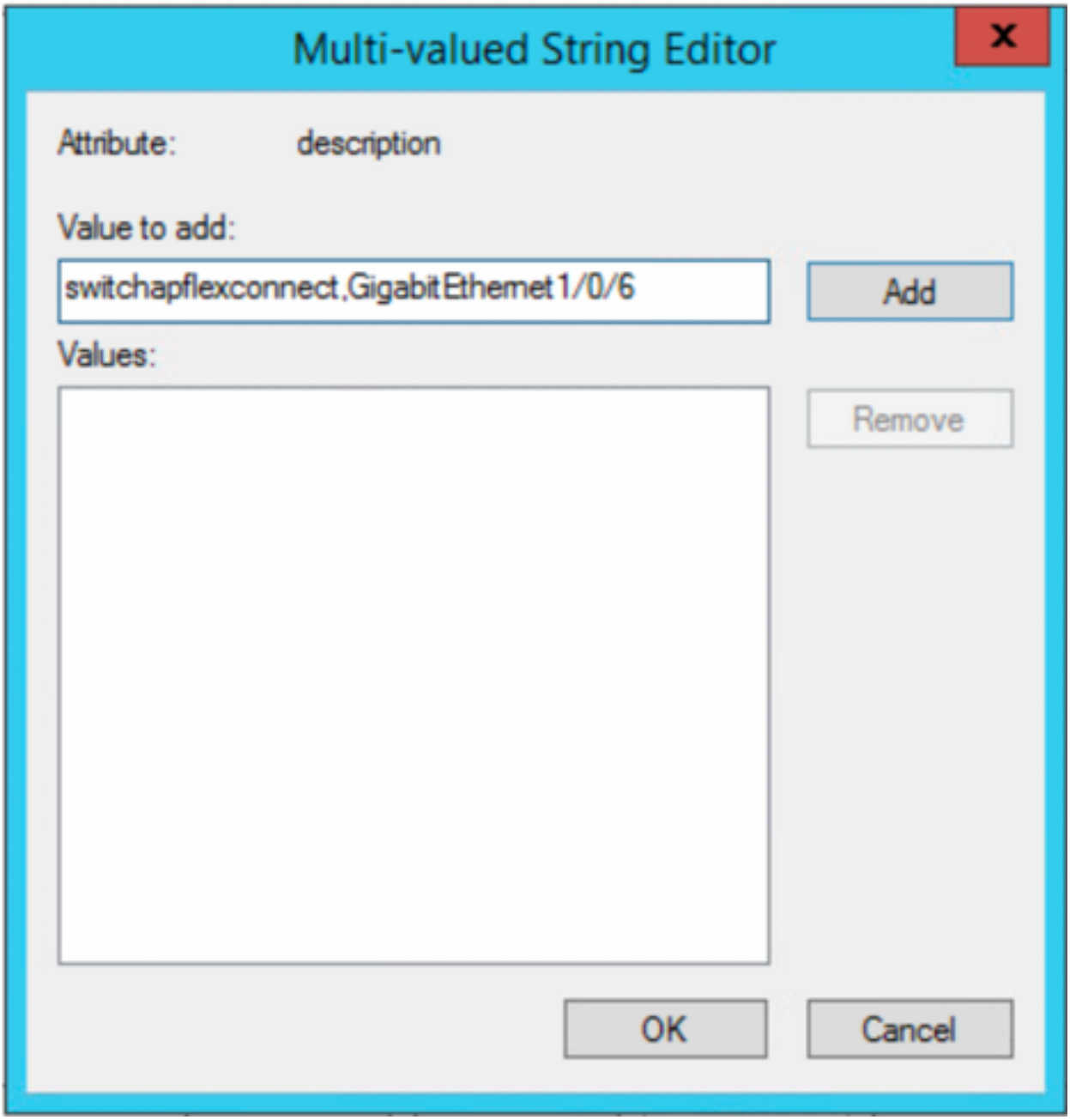


15. 옵션 **설명**을 선택하고 편집을 선택하여 디바이스가 연결될 스위치 이름과 스위치 포트를 정의



합니다.

16. 스위치 이름과 스위치 포트를 정의합니다. 각 값을 구분하려면 쉼표를 사용하십시오.Add(**추가**)를 선택한 다음 **Ok(확인)**를 선택하여 정보를 저장합니다.



- **Switchapflexconnect는 스위치 이름입니다.**
- **GigabitEthernet1/0/6은 엔드포인트가 연결된 스위치 포트입니다.**

참고:특정 필드에 속성을 추가하기 위해 스크립트를 사용할 수 있지만 이 예제에서는 값을 수동으로 정의합니다

참고:AD 특성은 대/소문자를 구분하며, 소문자로 모든 Mac 주소를 사용하는 경우 LDAP 쿼리 중에 ISE가 대문자로 변환됩니다.이러한 동작을 방지하려면 허용된 프로토콜 아래에서 프로세스 호스트 조회를 비활성화합니다.자세한 내용은 다음 링크에서 확인할 수 있습니다 .https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

스위치 구성

ISE 802.1x .

```
aaa new-model ! aaa group server radius ISE server name ISE deadtime 15 ! aaa authentication
dot1x default group ISE aaa authorization network default group ISE aaa accounting update
newinfo aaa accounting dot1x default start-stop group ISE ! aaa server radius dynamic-author
client 10.81.127.109 server-key XXXXabc ! aaa session-id common switch 1 provision ws-c3650-24pd
```

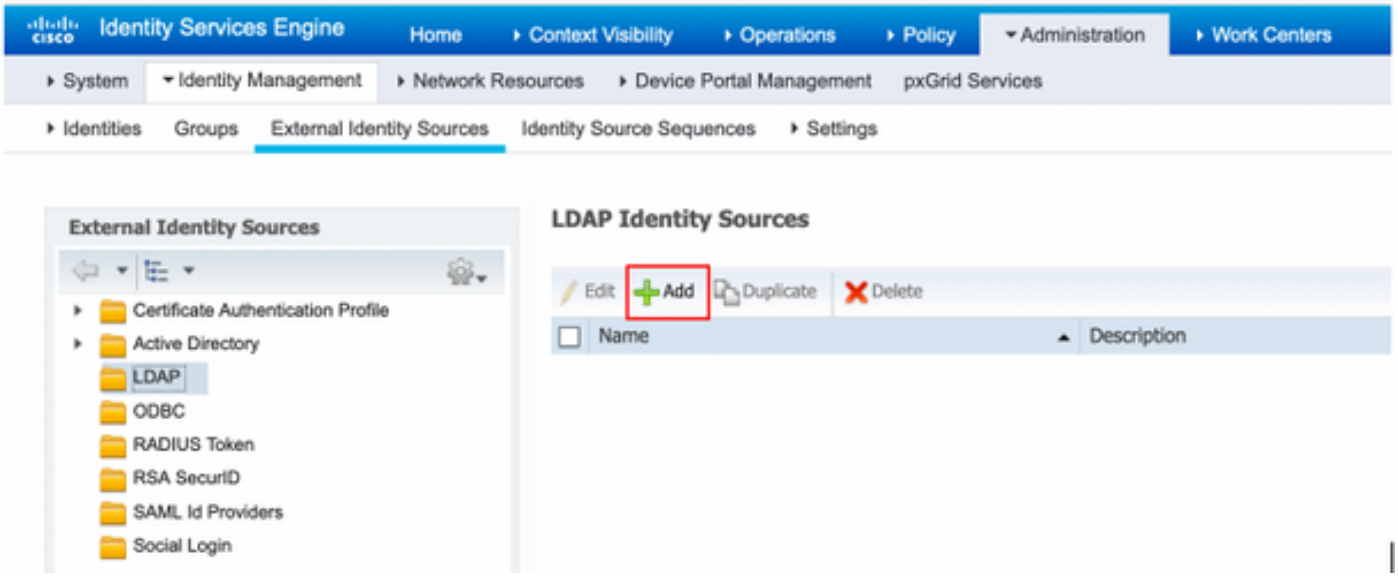
```
! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree
mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level
3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127
switchport mode access authentication event fail action next-method authentication event server
dead action authorize vlan 127 authentication event server alive action reinitialize
authentication host-mode multi-domain authentication open authentication order dot1x mab
authentication priority dot1x mab authentication port-control auto authentication periodic
authentication timer reauthenticate server authentication timer inactivity server dynamic
authentication violation restrict mab dot1x pae authenticator dot1x timeout tx-period 10
spanning-tree portfast ! radius server ISE address ipv4 10.81.127.109 auth-port 1812 acct-port
1813 automate-tester username radiustest idle-time 5 key XXXXabc !
```

참고:환경에서 전역 및 인터페이스 컨피그레이션을 조정해야 할 수 있습니다.

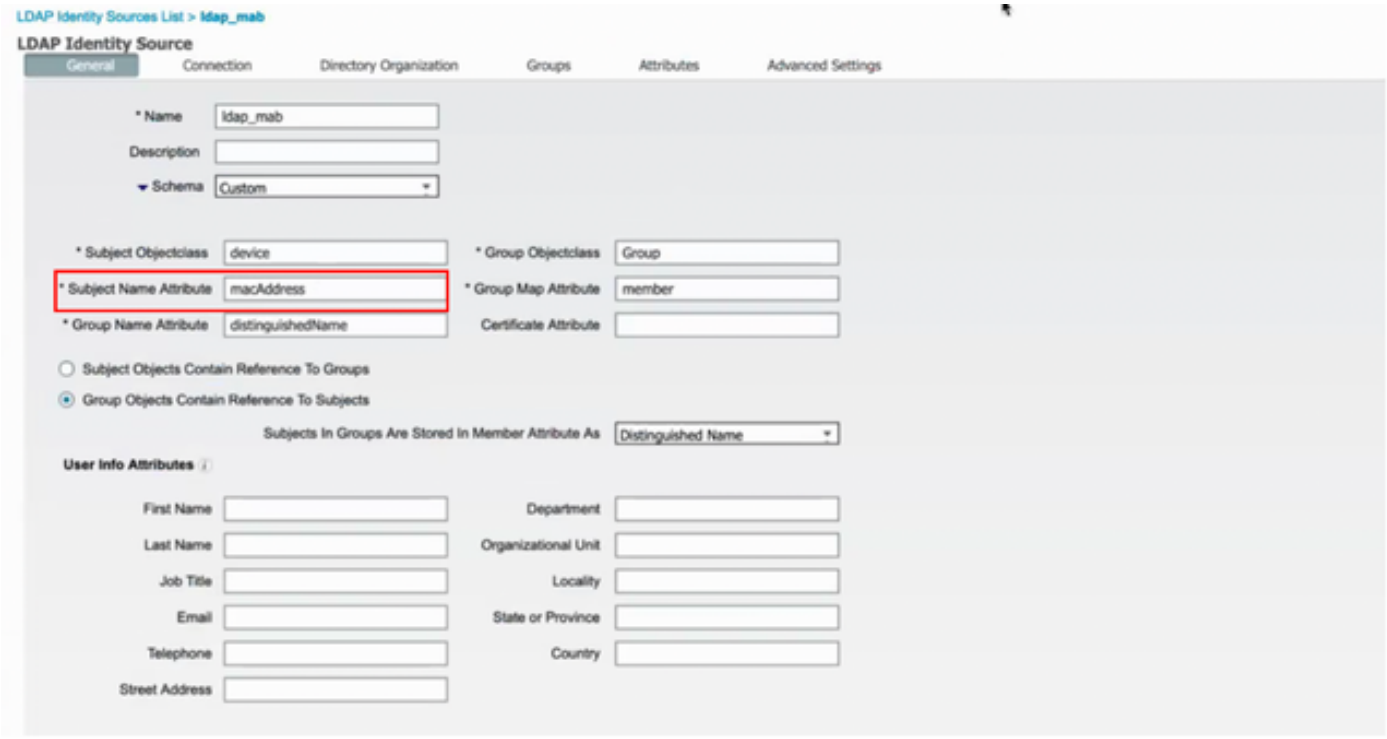
ISE 컨피그레이션

다음은 LDAP 서버에서 특성을 가져오고 ISE 정책을 구성하기 위한 ISE의 컨피그레이션에 대해 설명합니다.

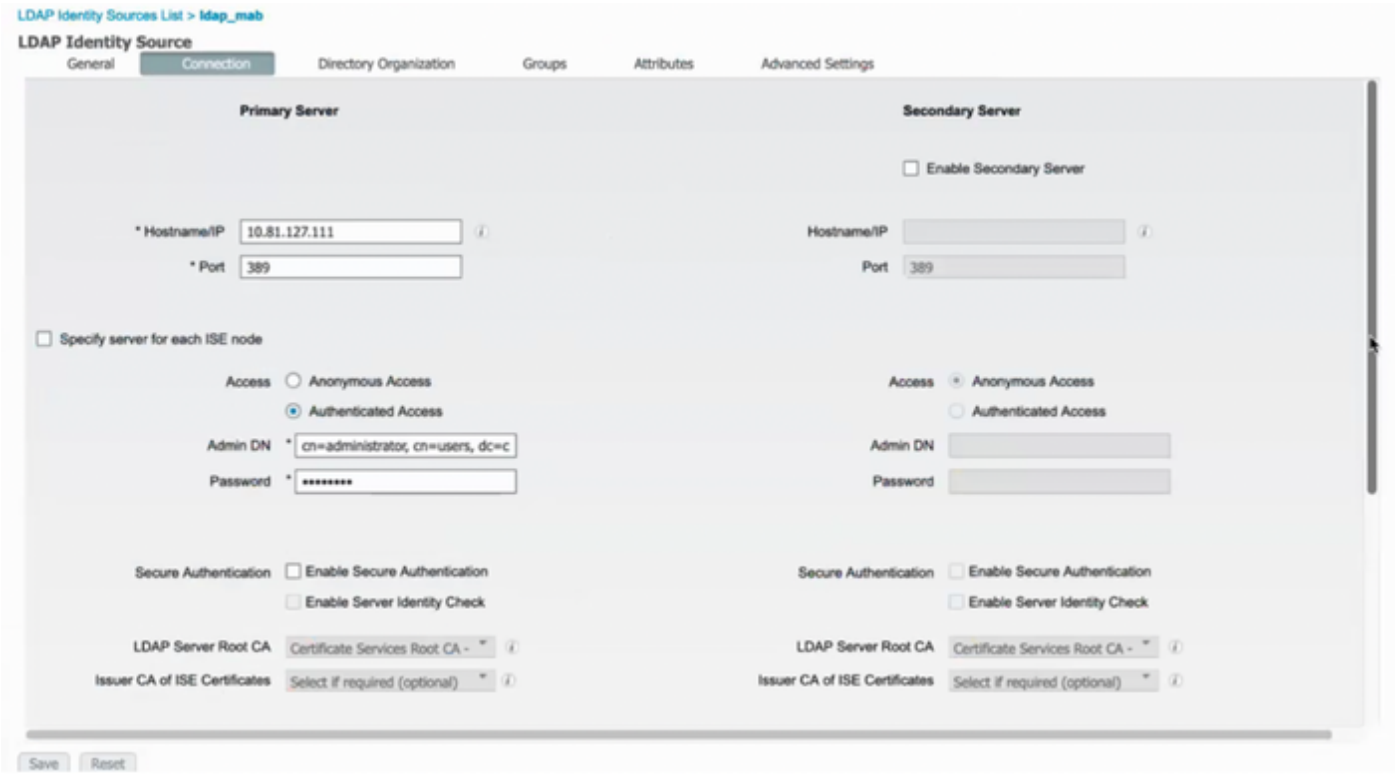
1. ISE에서 **Administration(관리)->Identity Management(ID 관리)->External Identity Sources(외부 ID 소스)로** 이동하여 **LDAP** 폴더를 선택하고 Add(**추가**)를 클릭하여 LDAP와 새 연결을 생성합니다.



2.**일반** 탭에서 이름을 정의하고 mac 주소를 주체 이름 속성으로 선택합니다.

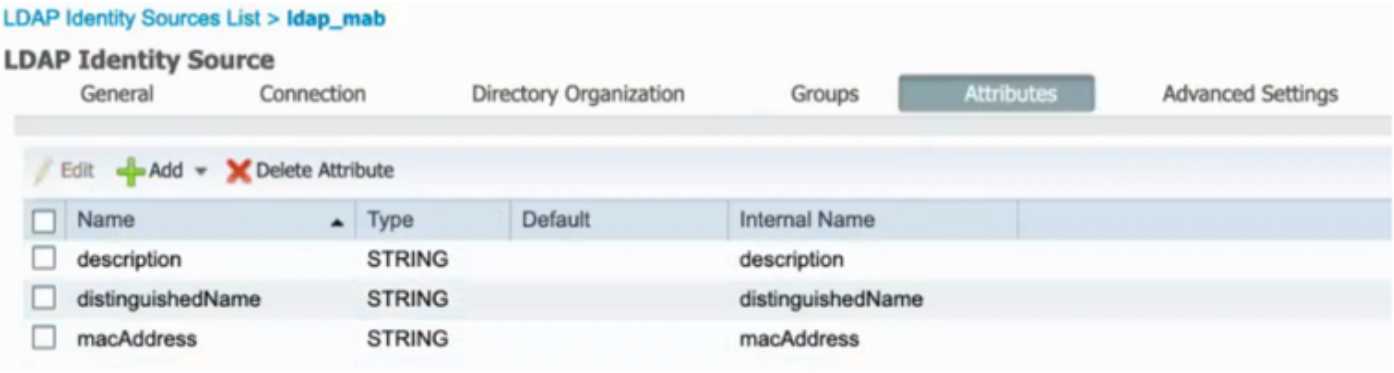


3. **Connection(연결)** 탭에서 LDAP 서버의 IP 주소, 관리자 DN 및 비밀번호를 구성하여 성공적으로 연결합니다.

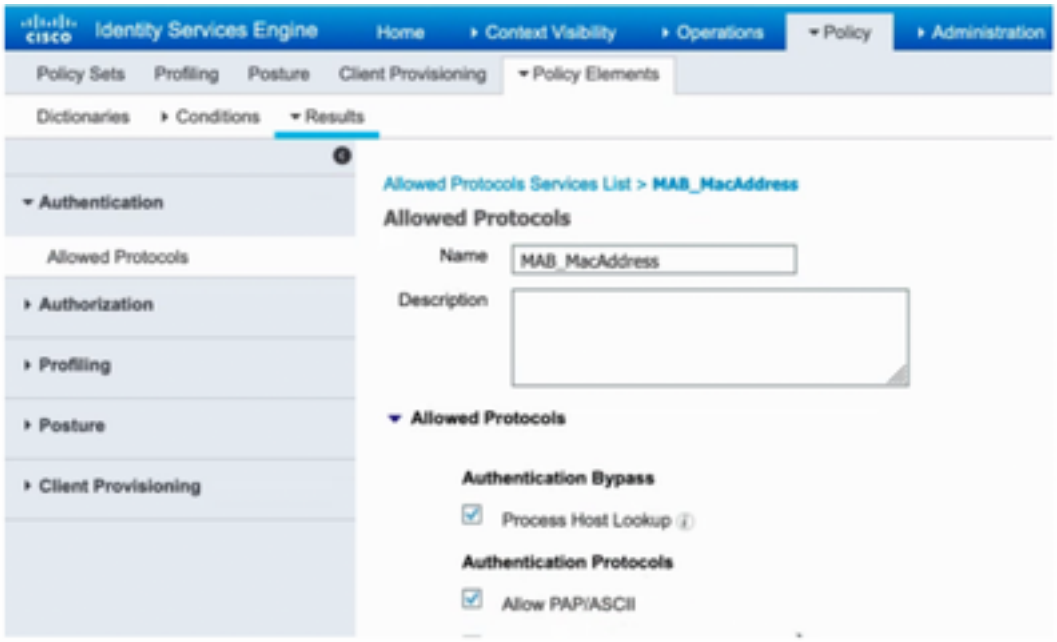


참고: Port 389는 기본 포트가 사용됩니다.

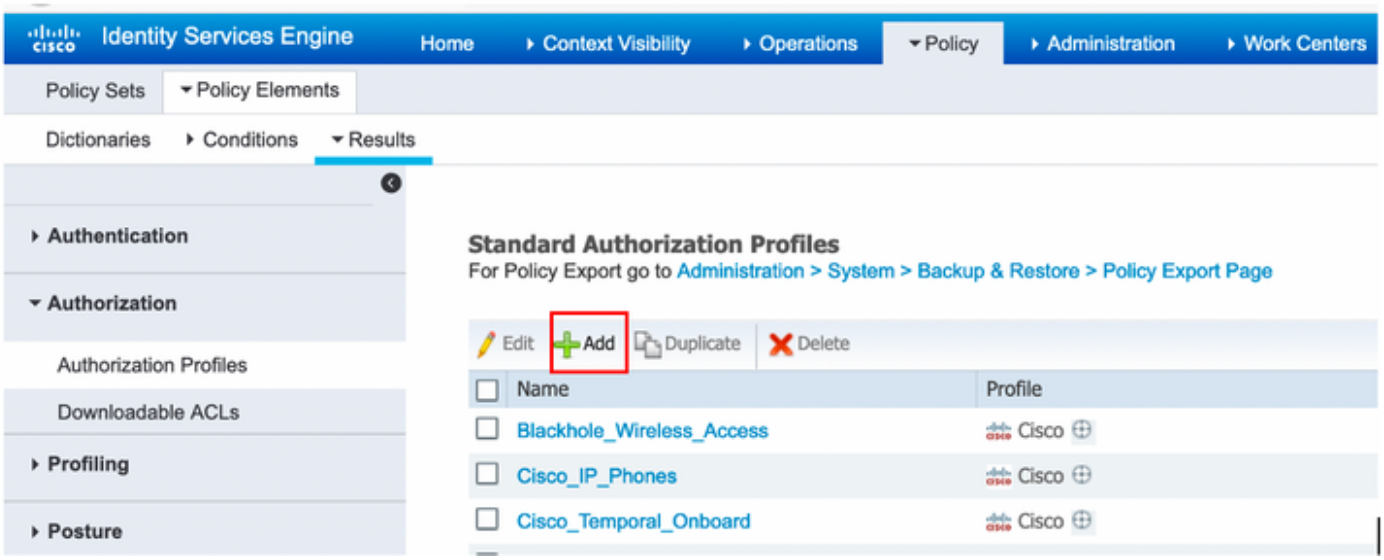
4. **속성** 탭에서 macAddress 및 설명 특성을 선택하면 권한 부여 정책에 이러한 속성이 사용됩니다.

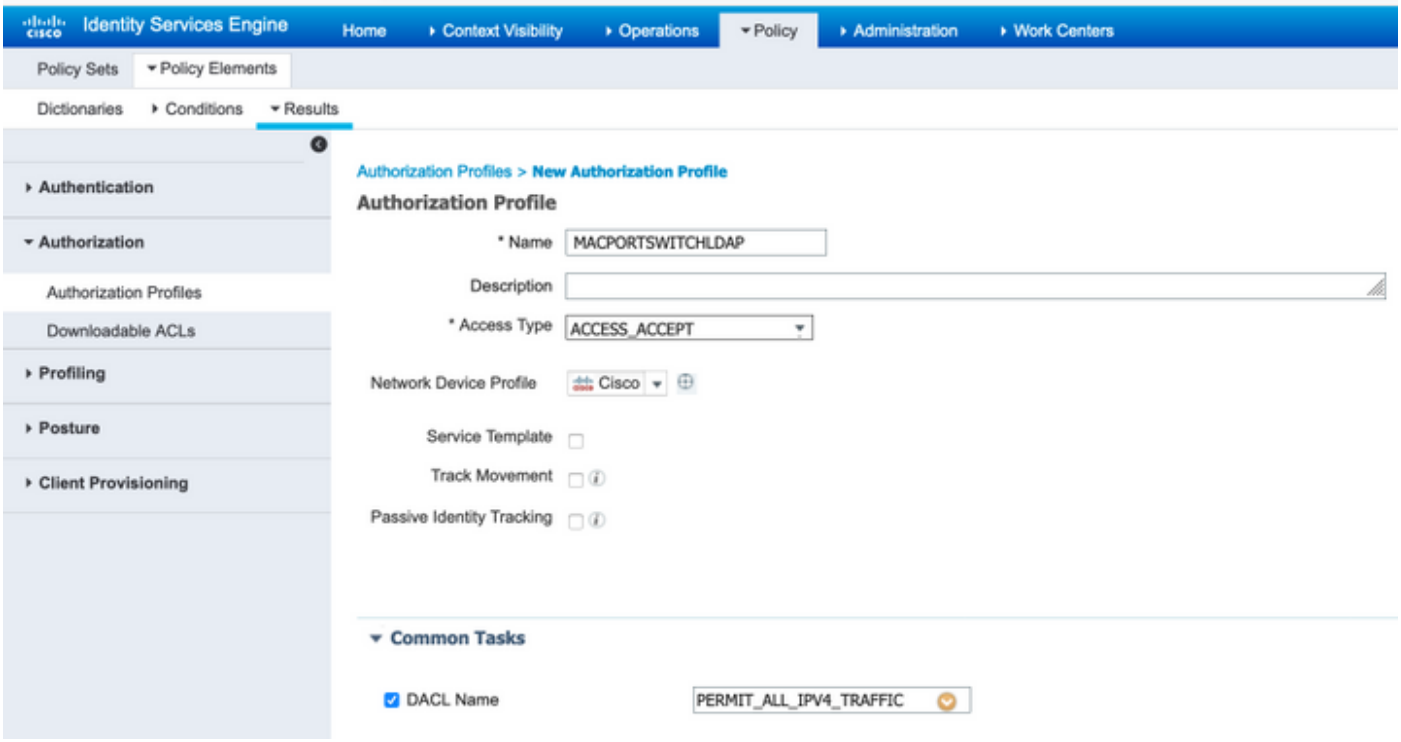


5. 허용된 프로토콜을 생성하려면 Policy(정책)->Policy Elements(정책 요소)->Results(결과)->Authentication(인증)->Allowed Protocols(허용된 프로토콜)로 이동합니다.Process Host Lookup(프로세스 호스트 조회) 및 Allow PAP/ASCII(PAP/ASCII 허용)를 유일한 허용 프로토콜로 정의하고 선택합니다.마지막으로 **저장**을 선택합니다.

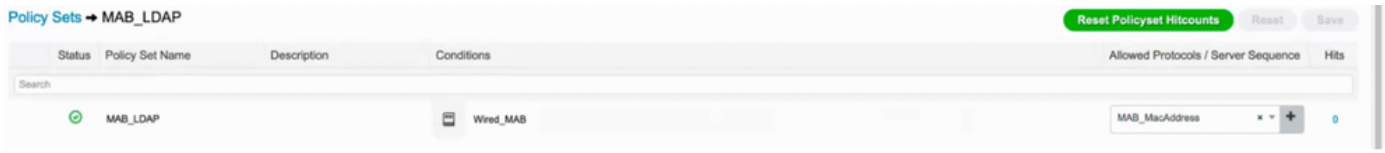


6. 권한 부여 프로파일을 생성하려면 **정책->정책 요소->결과->권한 부여->권한 부여 프로파일로** 이동합니다.Add(**추가**)를 선택하고 엔드포인트에 할당될 권한을 정의합니다.

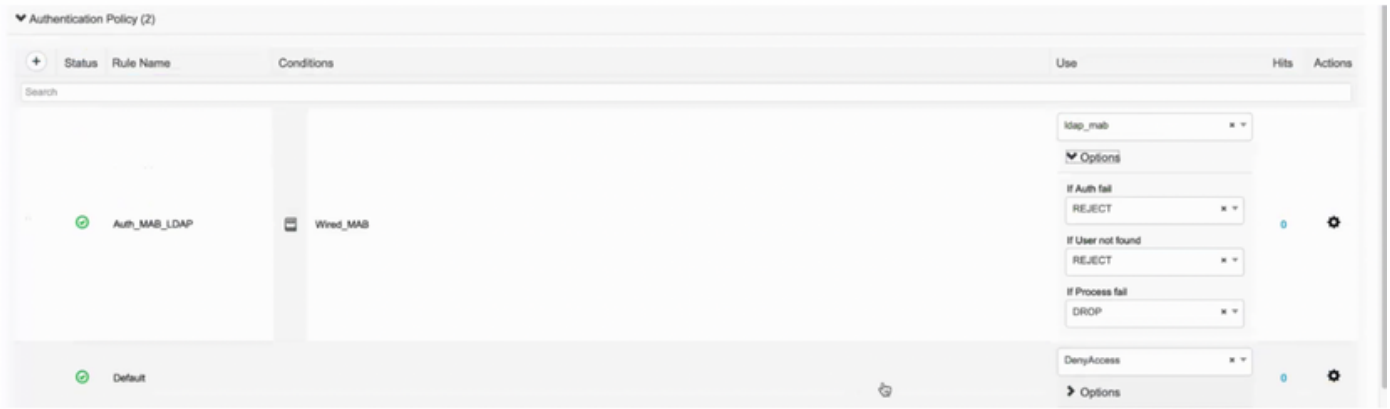




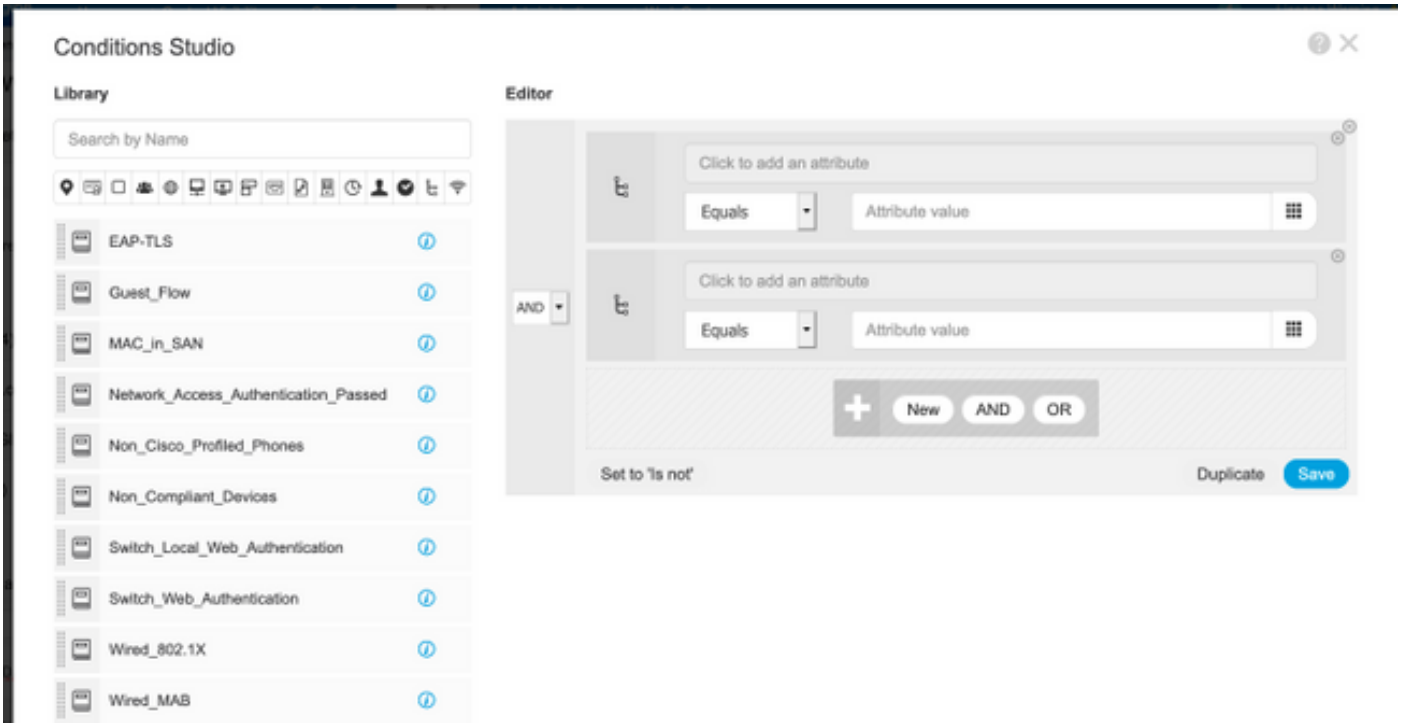
7.Policy(정책)-> Policy Set(정책 집합)로 이동하여 미리 정의된 조건 Wired_MAB 및 5단계에서 생성한 Allowed Protocol(허용되는 프로토콜)을 사용하여 정책 집합을 생성합니다.

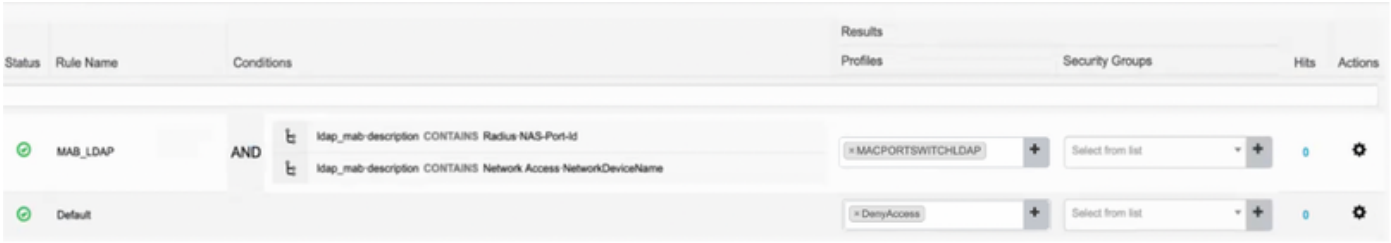


8.생성된 새 정책 집합에서 미리 정의된 **Wired_MAB** Library 및 **LDAP** 연결을 외부 ID 소스 시퀀스로 사용하여 인증 정책을 생성합니다



9. **권한 부여 정책**에서 LDAP 특성 설명, Radius NAS 포트 ID 및 NetworkDeviceName을 사용하여 이름을 정의하고 복합 조건을 만듭니다.마지막으로 6단계에서 생성한 권한 부여 프로파일을 추가합니다.





컨피그레이션을 적용한 후에는 사용자 개입 없이 네트워크에 연결할 수 있어야 합니다.

다음을 확인합니다.

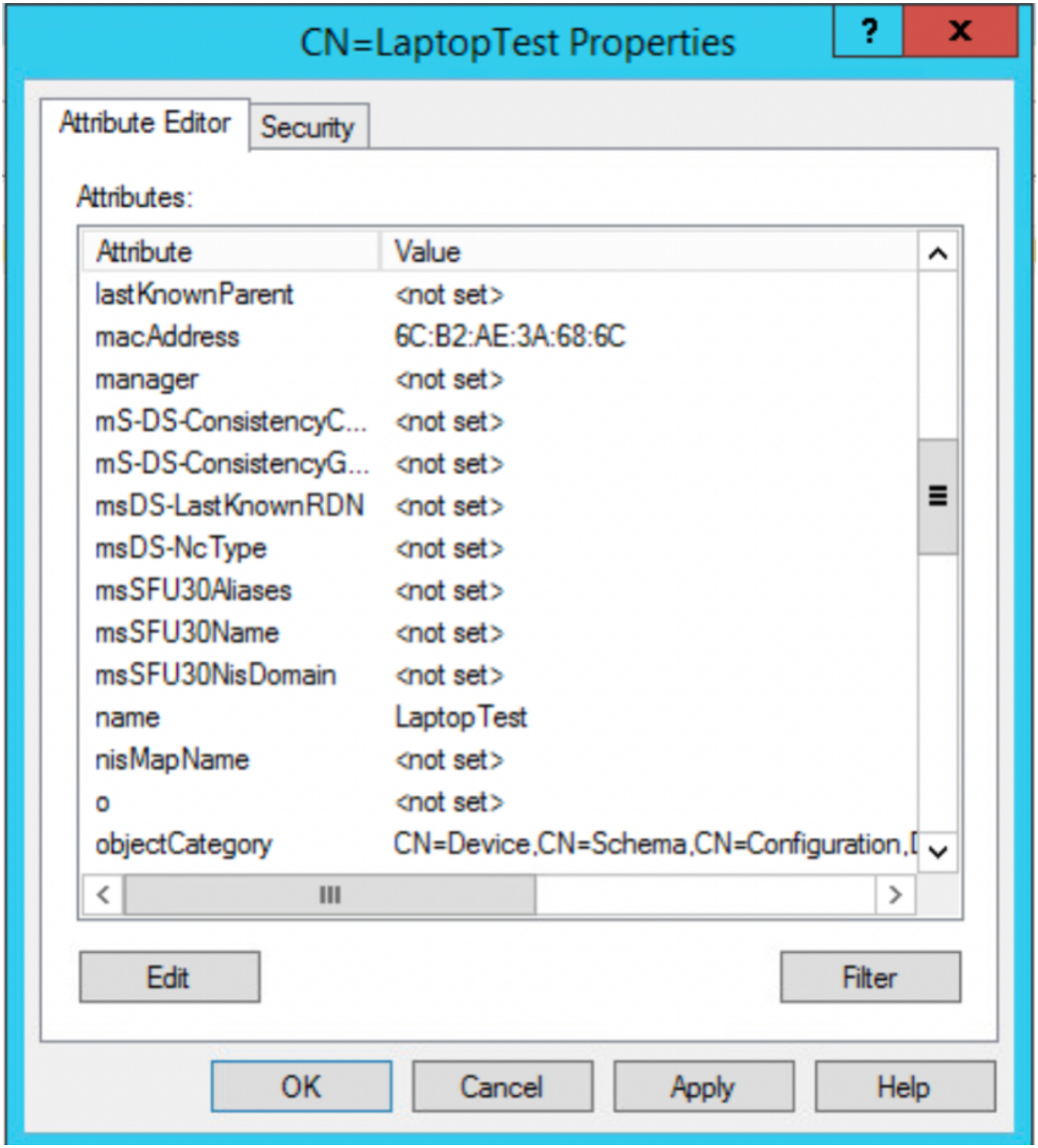
지정된 스위치 포트에 연결되면 **show authentication session interface GigabitEthernet X/X/X details를 입력하여** 디바이스의 인증 및 권한 부여 상태를 확인할 수 있습니다.

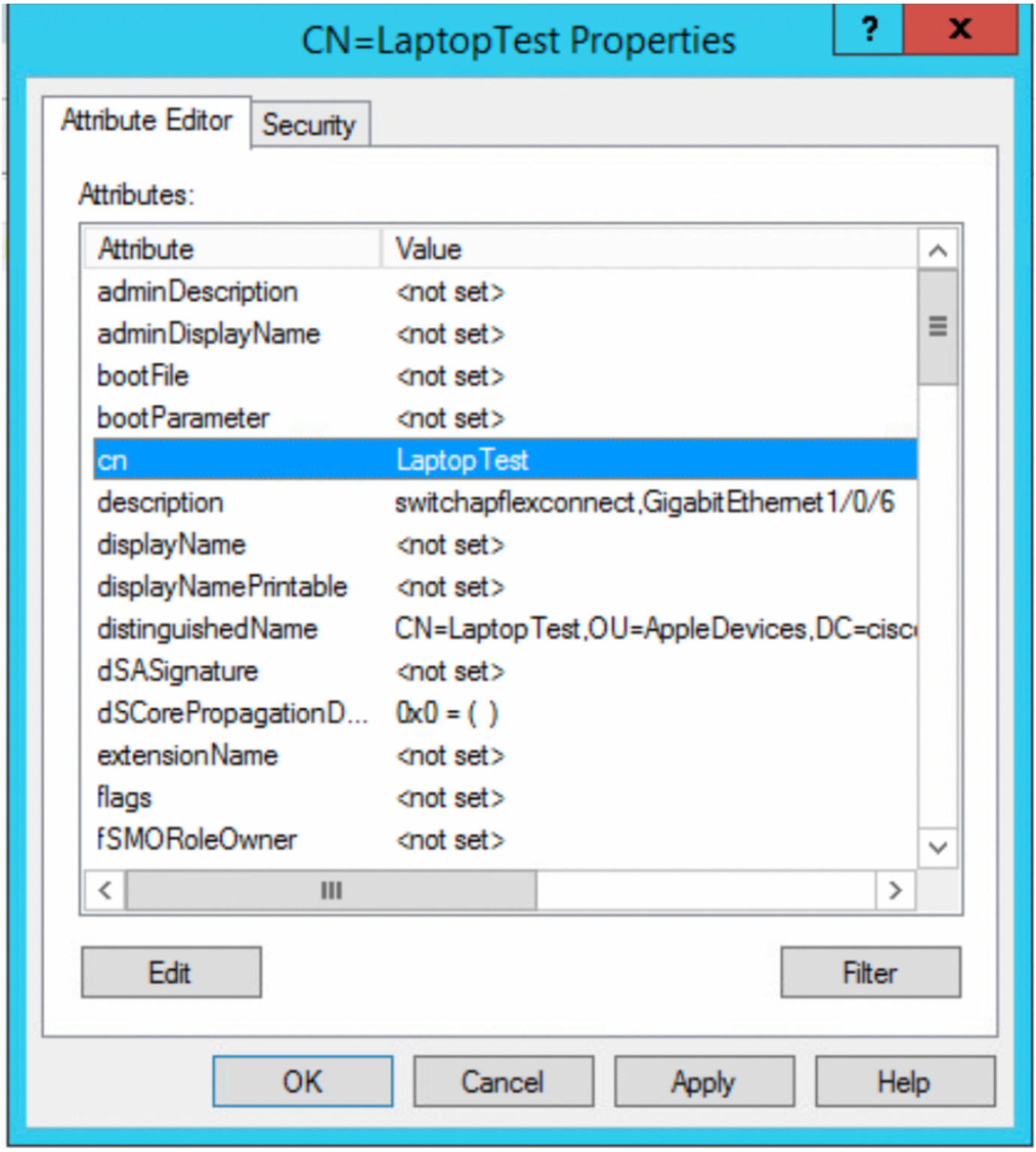
```
Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID:
0x103DFC0000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-
B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir:
both Session timeout: N/A Restart timeout: N/A Common Session ID: 0A517F65000013DA87E85A24 Acct
session ID: 0x000015D9 Handle: 0x9300005C Current Policy: Policy_Gi1/0/6 Local Policies: Service
Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Security Policy: Should Secure
Security Status: Link Unsecure Method status list: Method State mab Authc Success
```

ISE에서 확인을 위해 Radius Live Logs를 사용할 수 있습니다.

문제 해결

LDAP 서버에서 생성된 디바이스에 Mac 주소, 적절한 스위치 이름 및 스위치 포트가 구성되었는지 확인합니다.


CN=LaptopTest Properties
?
X
Attribute Editor
Security
Attributes:
Attribute
Value
lastKnownParent
<not set>
macAddress
6C:B2:AE:3A:68:6C
manager
<not set>
mS-DS-ConsistencyC...
<not set>
mS-DS-ConsistencyG...
<not set>
msDS-LastKnownRDN
<not set>
msDS-NcType
<not set>
msSFU30Aliases
<not set>
msSFU30Name
<not set>
msSFU30NisDomain
<not set>
name
LaptopTest
nisMapName
<not set>
o
<not set>
objectCategory
CN=Device,CN=Schema,CN=Configuration,
Edit
Filter
OK
Cancel
Apply
Help



ISE에서 LDAP에서 ISE로 전송 중인 값을 확인하기 위해 패킷 캡처(**Operations->Troubleshoot->Diagnostic Tool->TCP Dumps**로 이동)를 가져올 수 있습니다.