

외부 LDAPS ID 저장소로 ISE 구성 및 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[Active Directory에서 LDAPS 구성](#)

[도메인 컨트롤러에 ID 인증서 설치](#)

[LDAPS 디렉토리 구조 액세스](#)

[ISE를 LDAPS 서버와 통합](#)

[스위치 구성](#)

[엔드포인트 구성](#)

[ISE에서 정책 설정 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ISE와 Secure LDAPS 서버를 외부 ID 소스로 통합하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Service Engine) 관리에 대한 기본 지식
- Active Directory/LDAPS(Secure Lightweight Directory Access Protocol)에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 2.6 패치 7
- Active Directory LDS(Lightweight Directory Services)가 설치된 Microsoft Windows 버전 2012 R2
- 기본 신청자 및 사용자 인증서가 설치된 Windows 10 OS PC
- Cisco Switch C3750X with 152-2.E6 image

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

LDAPS에서는 디렉토리 바인딩이 설정될 때 전송 중인 LDAP 데이터(사용자 자격 증명 포함)의 암호화를 허용합니다. LDAPS는 TCP 포트 636을 사용합니다.

이러한 인증 프로토콜은 LDAPS에서 지원됩니다.

- EAP Generic Token Card(EAP-GTC)
- PAP(Password Authentication Protocol)
- EAP 전송 계층 보안(EAP-TLS)
- PEAP-TLS(Protected EAP Transport Layer Security)

 참고: EAP-MSCHAPV2(PEAP, EAP-FAST 또는 EAP-TTLS의 내부 방법), LEAP, CHAP 및 EAP-MD5는 LDAPS 외부 ID 소스에서 지원되지 않습니다.

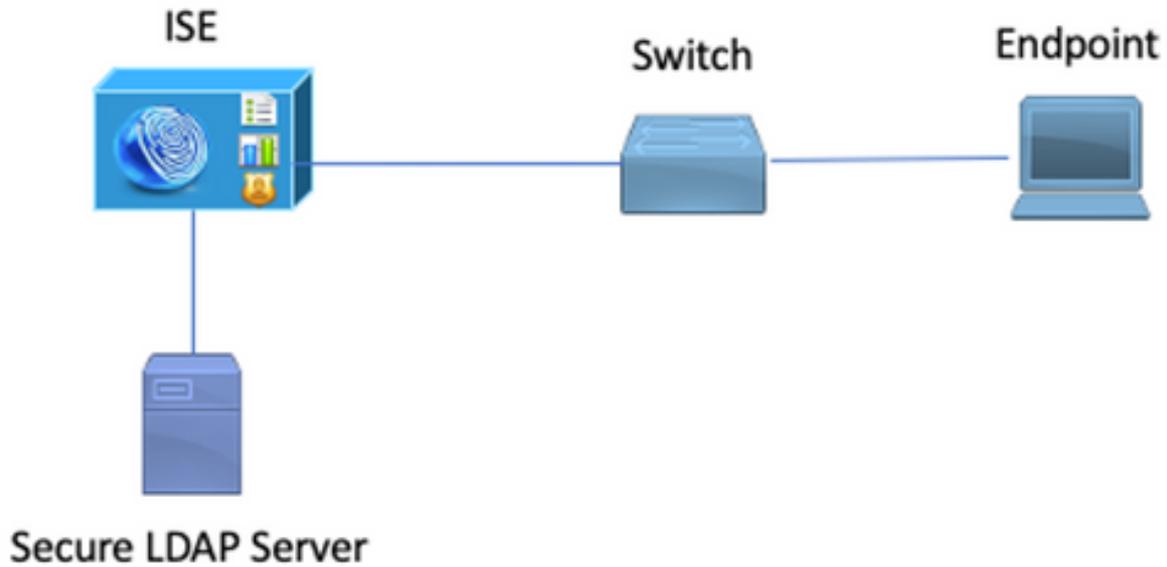
구성

이 섹션에서는 네트워크 디바이스의 컨피그레이션 및 ISE와 Microsoft AD(Active Directory) LDAPS 서버의 통합에 대해 설명합니다.

네트워크 다이어그램

이 컨피그레이션 예에서는 엔드포인트가 LAN(Local Area Network)에 연결하기 위해 스위치와의 이더넷 연결을 사용합니다. 연결된 switchport는 802.1x 인증을 위해 구성되어 ISE로 사용자를 인증합니다. ISE에서 LDAPS는 외부 ID 저장소로 구성됩니다.

이 이미지는 사용되는 네트워크 토폴로지를 보여줍니다.

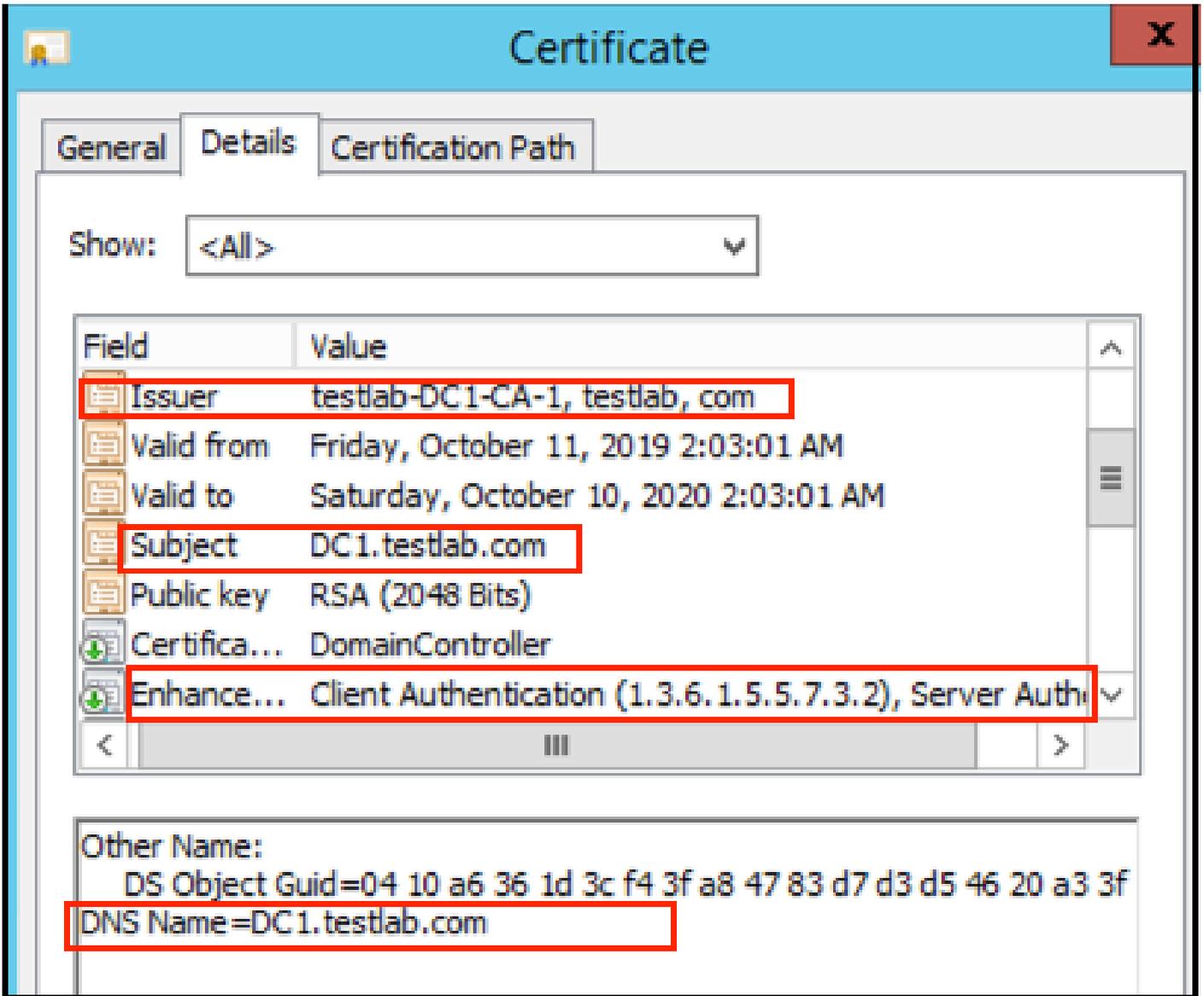


Active Directory에서 LDAPS 구성

도메인 컨트롤러에 ID 인증서 설치

LDAPS를 활성화하려면 다음 요구 사항을 충족하는 DC(Domain Controller)에 인증서를 설치합니다.

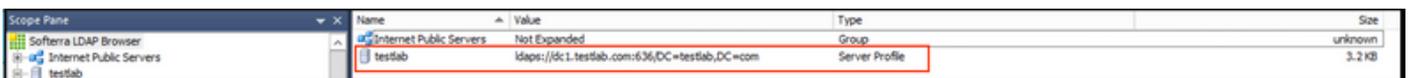
1. LDAPS 인증서는 도메인 컨트롤러의 개인 인증서 저장소에 있습니다.
2. 인증서와 일치하는 개인 키가 도메인 컨트롤러의 저장소에 있으며 인증서와 올바르게 연결되어 있습니다.
3. Enhanced Key Usage 확장에는 서버 인증(1.3.6.1.5.5.7.3.1) 개체 식별자(OID라고도 함)가 포함됩니다.
4. 도메인 컨트롤러(예: DC1.testlab.com)의 FQDN(Fully Qualified Domain Name)은 Subject(주체) 필드의 CN(Common Name) 및 Subject Alternative Name Extension(주체 대체 이름 확장)의 DNS 항목 특성 중 하나에 있어야 합니다.
5. 인증서는 도메인 컨트롤러와 LDAPS 클라이언트가 신뢰하는 CA(Certificate Authority)에서 발급해야 합니다. 신뢰할 수 있는 보안 통신의 경우 클라이언트와 서버는 서로의 루트 CA와 인증서를 발급한 중간 CA 인증서를 신뢰해야 합니다.
6. 키를 생성하려면 Schannel CSP(암호화 서비스 공급자)를 사용해야 합니다.



LDAPS 디렉토리 구조 액세스

Active Directory 서버의 LDAPS Directory에 액세스하려면 LDAP 브라우저를 사용합니다. 이 LAB에서는 Software LDAP Browser 4.5를 사용합니다.

1. TCP 포트 636에서 도메인에 대한 연결을 설정합니다.



2. 간소화를 위해 AD에서 ISE OU라는 OU(Organizational Unit)를 만들고 UserGroup이라는 그룹이 있어야 합니다. 두 명의 사용자(user1 및 user2)를 만들고 이 사용자를 UserGroup 그룹의 멤버로 만듭니다.

 참고: ISE의 LDAP ID 소스는 사용자 인증에만 사용됩니다.

Name	Value	Type
OU=ISE OU		
OU=LABISE		
CN=user 1		
CN=user 2		
CN=UserGroup		
CN=ComputerGroup		
CN=DESKTOP-19		
CN=ComputerGroup		
CN	ComputerGroup	Entry
CN	DESKTOP-19	Entry
CN	user 1	Entry
CN	user 2	Entry
CN	user2	Entry
CN	UserGroup	Entry
distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c...	Attribute
instanceType	[Writable]	Attribute
name	ISE OU	Attribute
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=...	Attribute
objectClass	organizationalUnit	Attribute
objectClass	top	Attribute
ou	ISE OU	Attribute
uSNChanged	607428	Attribute
uSNCreated	603085	Attribute
whenChanged	6/21/2020 2:44:06 AM	Attribute
whenCreated	6/20/2020 2:51:11 AM	Attribute
objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary Attribute

ISE를 LDAPS 서버와 통합

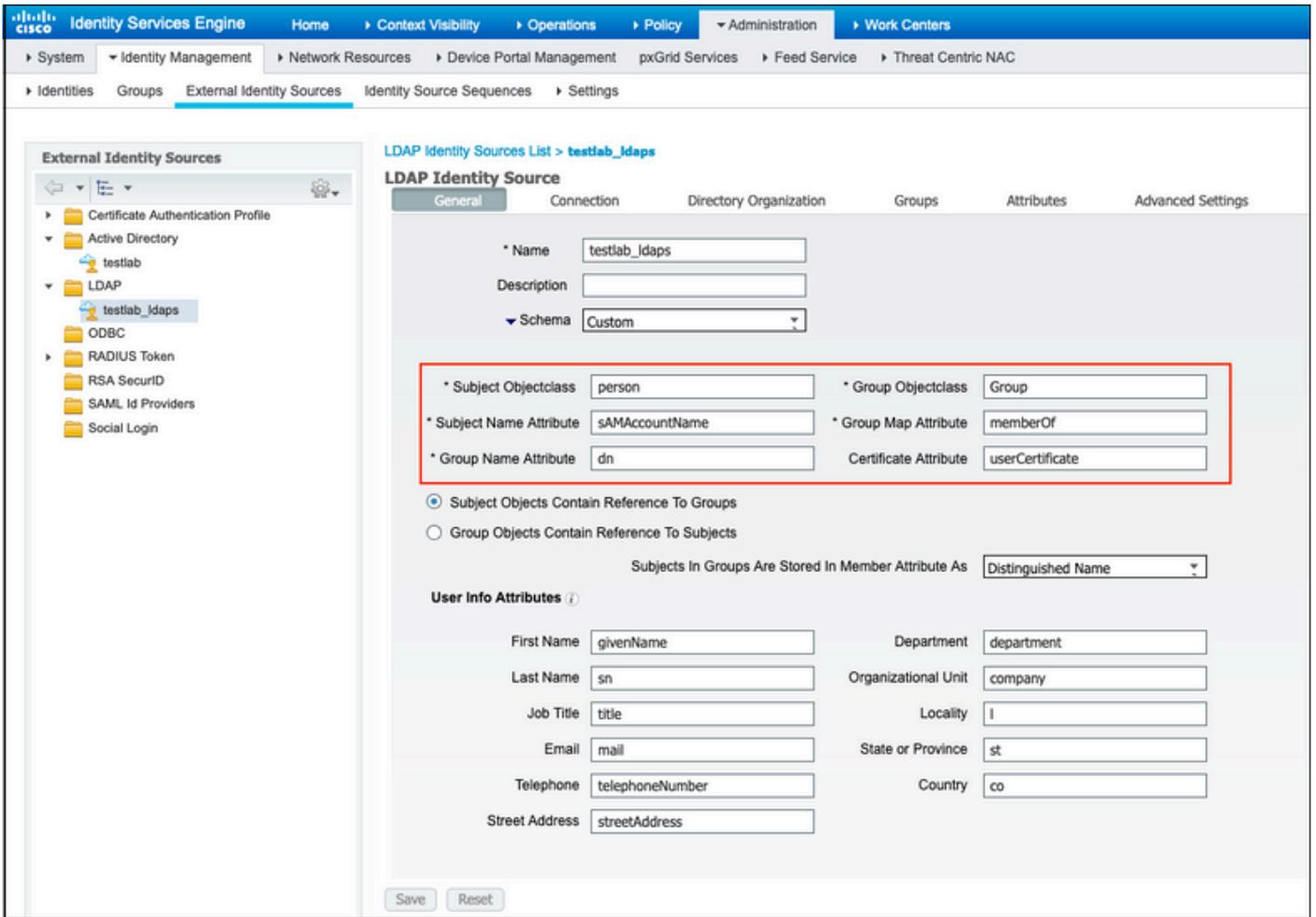
1. 신뢰할 수 있는 인증서에서 LDAP 서버 루트 CA 인증서를 가져옵니다.

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
DC1					
DC1-CA	Enabled	Infrastructure Cisco Services Endpoints	18 29 1C A7 00 13...	testlab-DC1-CA-1	testlab-DC1-CA-1

2. ISE 관리자 인증서를 검증하고 ISE 관리자 인증서 발급자 인증서가 신뢰할 수 있는 인증서 저장소에 있는지 확인합니다.

3. LDAPS 서버를 통합하려면 LDAPS 디렉토리의 다른 LDAP 속성을 사용합니다.

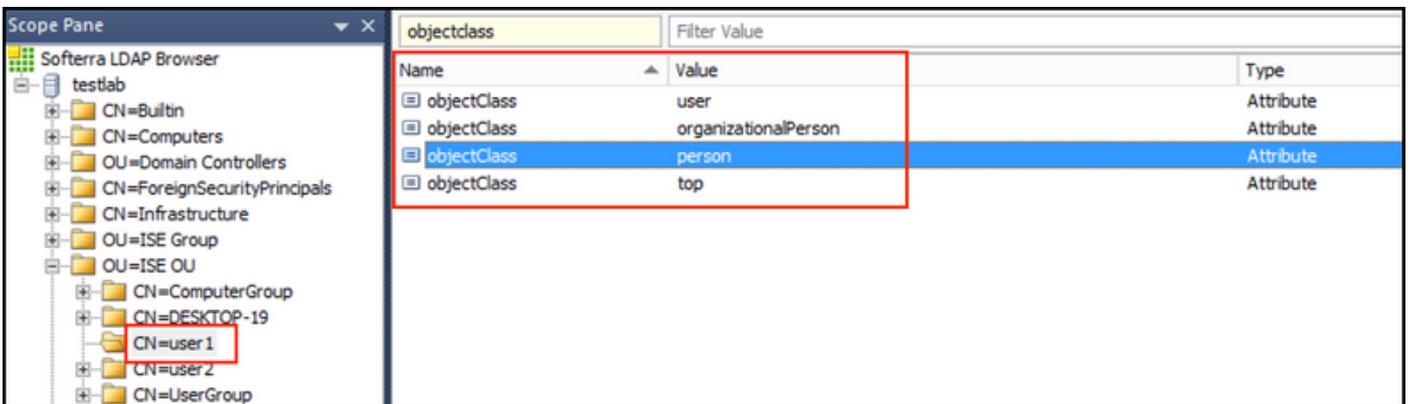
Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > LDAP Identity Sources(LDAP ID 소스) > Add(추가)로 이동합니다.



4. [일반 사항] 탭에서 다음 속성을 구성합니다.

Subject Objectclass: 이 필드는 사용자 계정의 Object 클래스에 해당합니다. 다음 네 가지 클래스 중 하나를 사용할 수 있습니다.

- 상단
- 개인
- 조직인
- InetOrg사람



주체 이름 특성: 이 필드는 요청의 사용자 이름을 포함하는 특성의 이름입니다. 이 특성은 ISE가 LDAP 데이터베이스의 특정 사용자 이름을 조회할 때 LDAPS에서 검색됩니다(cn,

sAMAccountName 등을 사용할 수 있음). 이 시나리오에서는 엔드포인트의 user1 사용자 이름이 사용됩니다.

LDAP browser showing user1 attributes. The sAMAccountName attribute is highlighted with a red box.

Name	Value	Type
cn	user1	Attribute
displayName	user1	Attribute
distinguishedName	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attribute
givenName	user1	Attribute
name	user1	Attribute
sAMAccountName	user1	Attribute
userPrincipalName	user1@testlab.com	Attribute
userCertificate	user1	Binary Attribute

Group Name Attribute(그룹 이름 특성): 그룹 이름을 보유한 특성입니다. LDAP 디렉토리의 그룹 이름 속성 값은 User groups(사용자 그룹) 페이지의 LDAP 그룹 이름과 일치해야 합니다

LDAP browser showing UserGroup attributes. The distinguishedName attribute is highlighted with a red box.

Name	Value	Type
cn	UserGroup	Attribute
distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
groupType	[GlobalScope, Security]	Attribute
instanceType	[Writable]	Attribute
member	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attribute
member	CN=user2,OU=ISE OU,DC=testlab,DC=com	Attribute
name	UserGroup	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute
objectClass	group	Attribute
objectClass	top	Attribute
sAMAccountName	UserGroup	Attribute
sAMAccountType	< samGroupObject >	Attribute

Group Objectclass: 이 값은 검색에서 그룹으로 인식되는 객체를 지정하는 데 사용됩니다.

LDAP browser showing UserGroup object classes. The objectClass attribute is highlighted with a red box.

Name	Value	Type
objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
objectGUID	{39967F90-89BE-44B5-9CC5-B28C0B0EB234}	Binary Attribute
objectClass	top	Attribute
objectClass	group	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

그룹 맵 특성: 이 특성은 사용자가 그룹에 매핑되는 방법을 정의합니다.

LDAP browser showing user1 memberOf attribute. The memberOf attribute is highlighted with a red box.

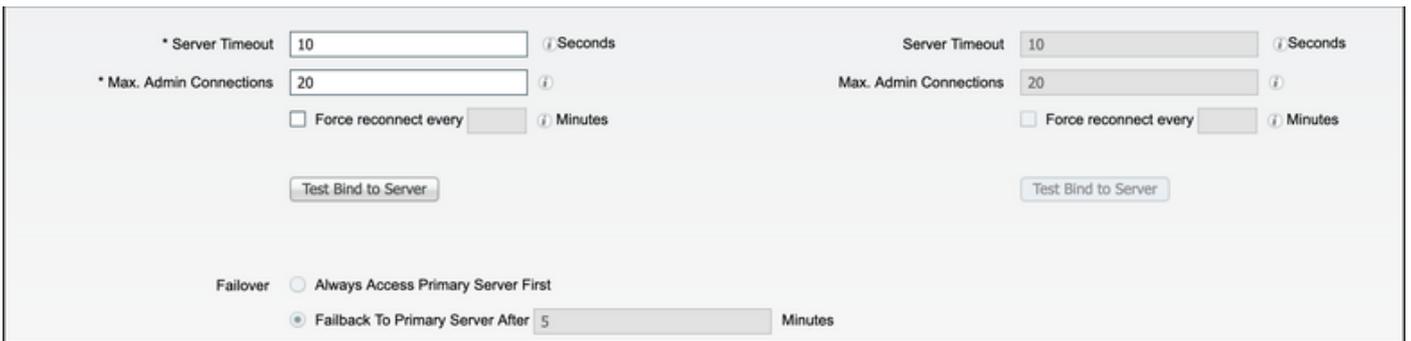
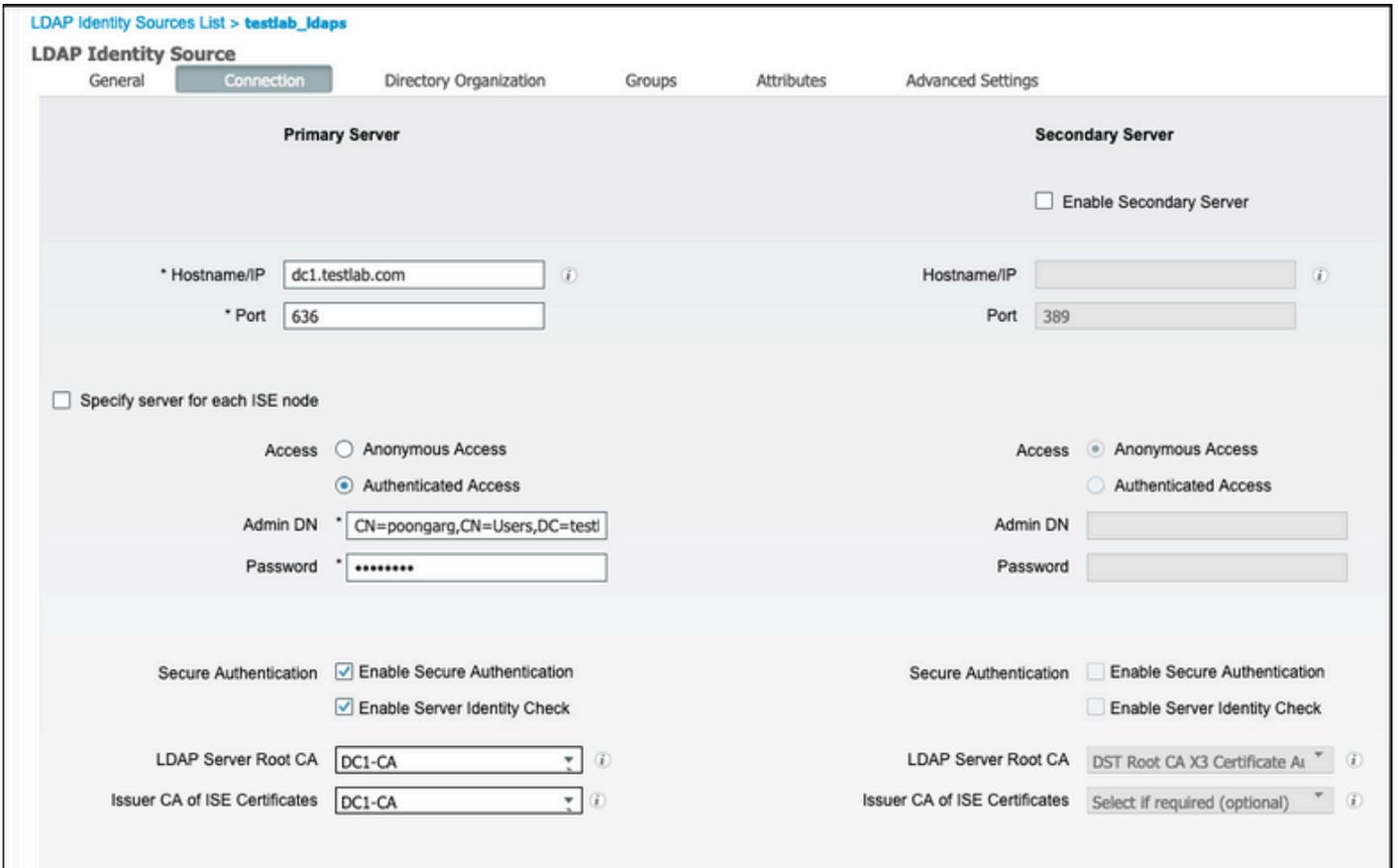
Name	Value	Type
memberOf	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute

Certificate Attribute(인증서 특성): 인증서 정의를 포함하는 특성을 입력합니다. 이러한 정의는 선택적으로 클라이언트가 인증서 인증 프로파일의 일부로 정의할 때 제시하는 인증서를 검증하는 데 사용할 수 있습니다. 이러한 경우 클라이언트 인증서와 LDAP ID 소스에서 검색된 인증서 간에 이진 비

교가 수행됩니다.



5. LDAPS 연결을 구성하려면 [연결] 탭으로 이동합니다.



6. 도메인 컨트롤러에서 dsquery를 실행하여 LDAP 서버에 연결하는 데 사용할 사용자 이름 DN을 가져옵니다.

```
PS C:\Users\Administrator> dsquery user -name poongarg  
"CN=poongarg,CN=Users,DC=testlab,DC=com"
```

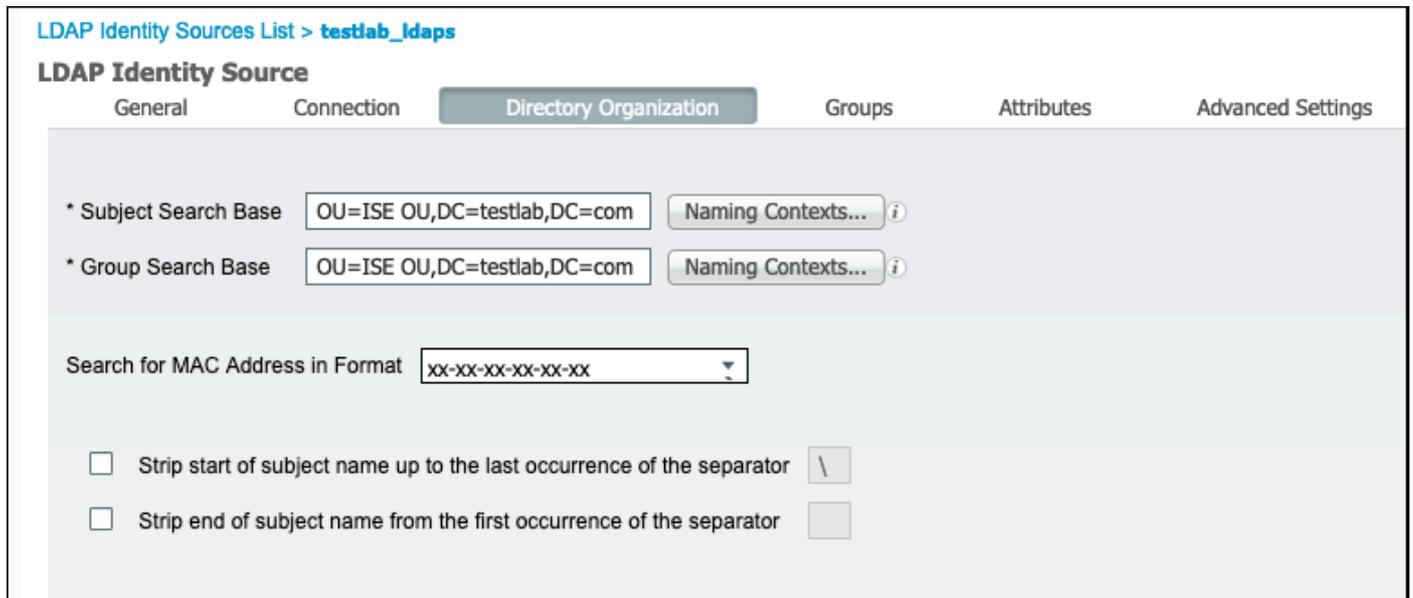
1단계. 초LDAP 서버의 올바른 IP 주소 또는 호스트 이름을 설정하고, LDAPS 포트(TCP 636) 및 관리 DN을 정의하여 SSL을 통해 LDAP에 연결합니다.

2단계. 보안 인증 및 서버 ID 확인 옵션을 활성화 합니다.

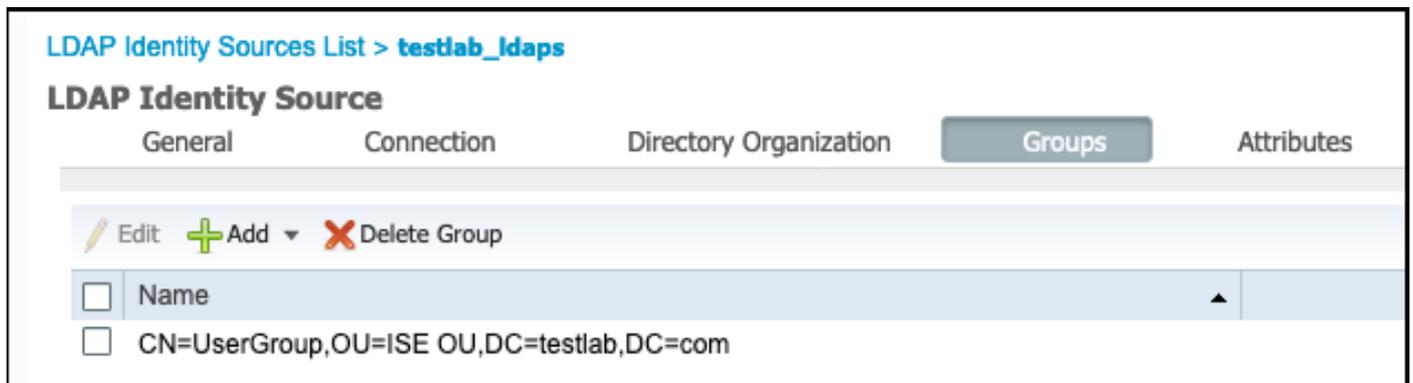
3단계. 드롭다운 메뉴에서 LDAP Server Root CA 인증서 및 ISE admin certificate Isser CA 인증서를 선택합니다(동일한 LDAP 서버에 설치된 인증 기관을 사용하여 ISE 관리 인증서도 발행함).

4단계. Test Bind to server를 선택합니다. 이 시점에서는 검색 기반이 아직 구성되지 않았기 때문에 어떤 주제나 그룹도 검색되지 않습니다.

7. Directory Organization(디렉토리 조직) 탭 아래에서 Subject/Group Search Base(주체/그룹 검색 기반)를 구성합니다. ISE가 LDAP에 조인하는 지점입니다. 이제 조인 지점의 하위 항목인 주체 및 그룹만 검색할 수 있습니다. 이 시나리오에서는 주체 및 그룹이 모두 OU=ISE OU에서 검색됩니다



8. 이 이미지에 표시된 대로 Groups(그룹)에서 Add(추가)를 클릭하여 ISE의 LDAP에서 그룹을 가져 오고 그룹을 검색합니다.



스위치 구성

802.1x 인증을 위해 스위치를 구성합니다. Windows PC가 switchport Gig2/0/47에 연결되었습니다.

```

aaa new-model

radius server ISE
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key xxxxxx
aaa group server radius ISE_SERVERS
server name ISE

!

aaa server radius dynamic-author
client x.x.x.x server-key xxxxxx

!
aaa authentication dot1x default group ISE_SERVERS local
aaa authorization network default group ISE_SERVERS
aaa accounting dot1x default start-stop group ISE_SERVERS
!
dot1x system-auth-control

ip device tracking
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
!

!

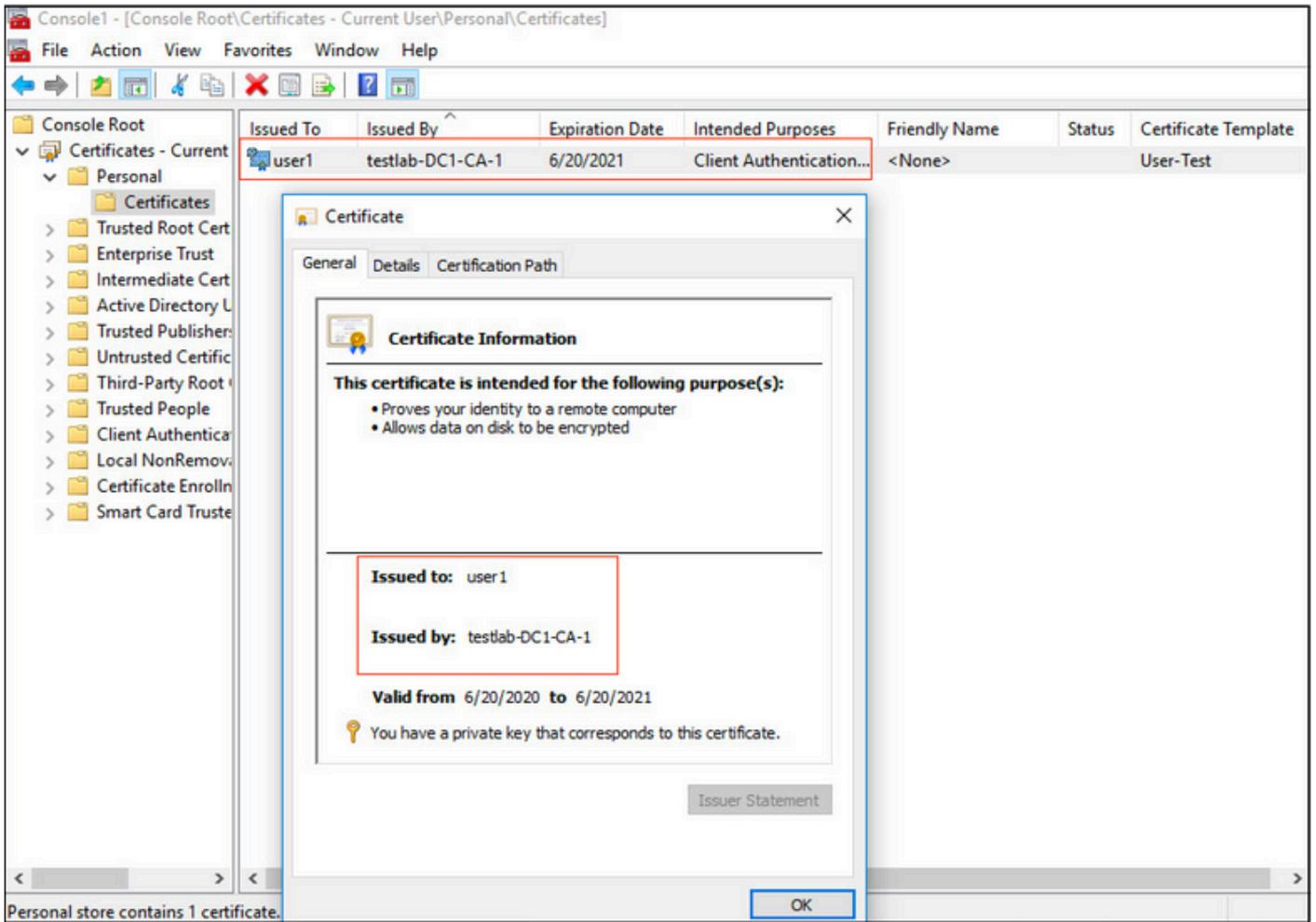
interface GigabitEthernet2/0/47
switchport access vlan xx
switchport mode access
authentication port-control auto
dot1x pae authenticator

```

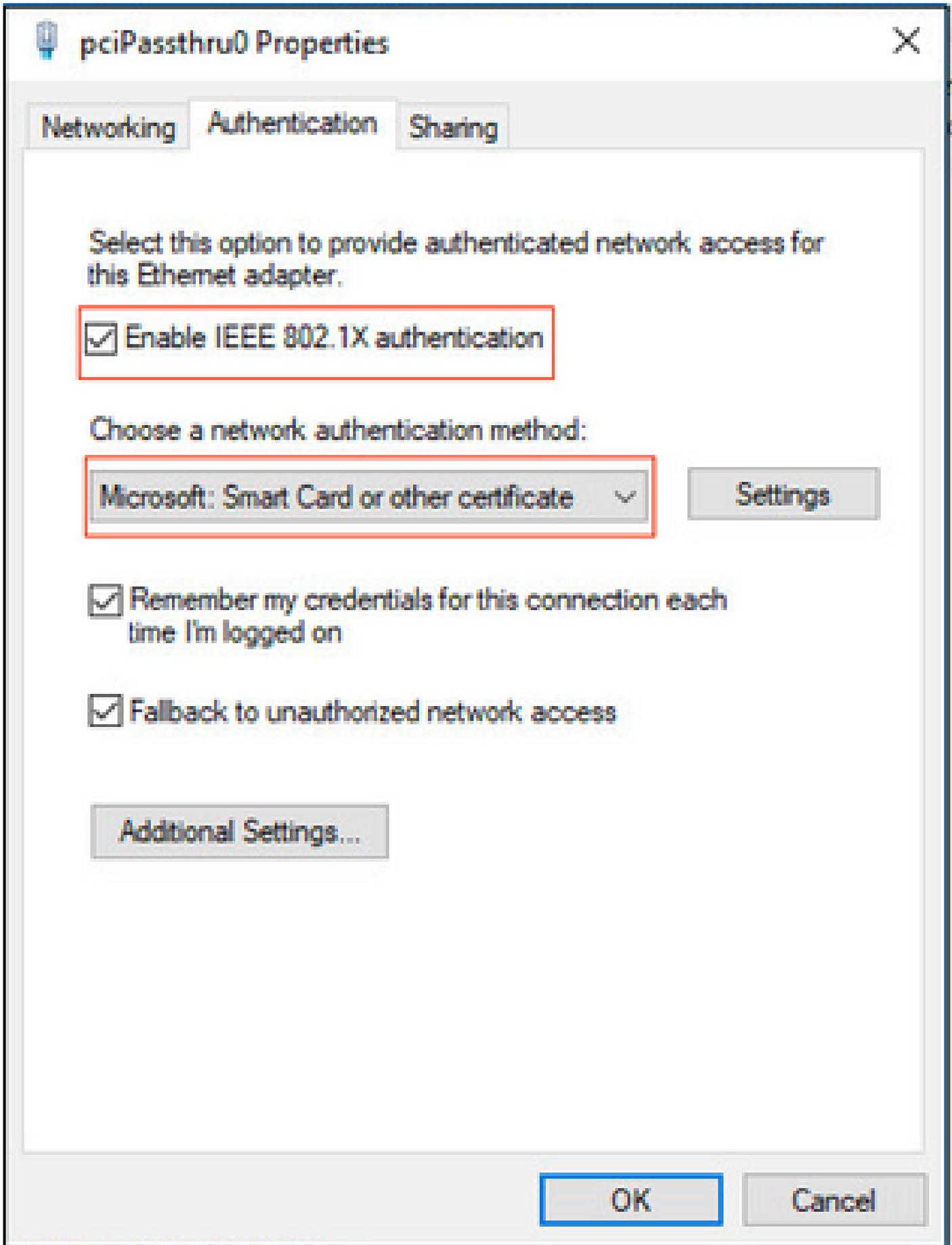
엔드포인트 구성

Windows 네이티브 서플리컨트가 사용되고 LDAP 지원 EAP 프로토콜 중 하나가 사용됩니다, 사용자 인증 및 권한 부여를 위한 EAP-TLS.

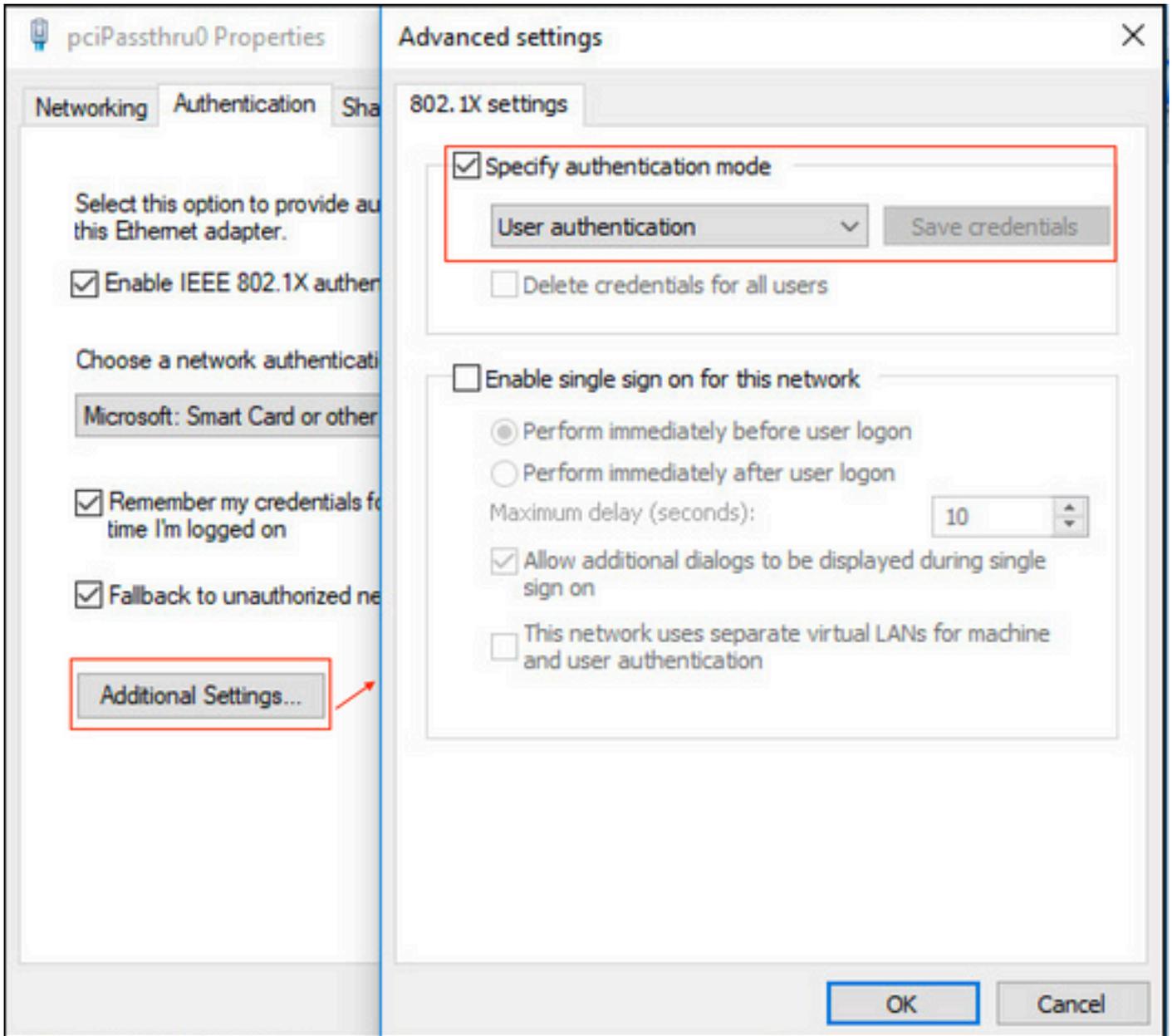
1. PC에 사용자 인증서(user1용)가 프로비저닝되어 있고 클라이언트 인증의 용도로 사용되고 있는지, 신뢰할 수 있는 루트 인증 기관에서 발급자 인증서 체인이 PC에 있는지 확인합니다.



2. Dot1x 인증을 활성화하고 Microsoft:Smart Card 또는 EAP-TLS 인증을 위한 기타 인증서로 인증 방법을 선택합니다.

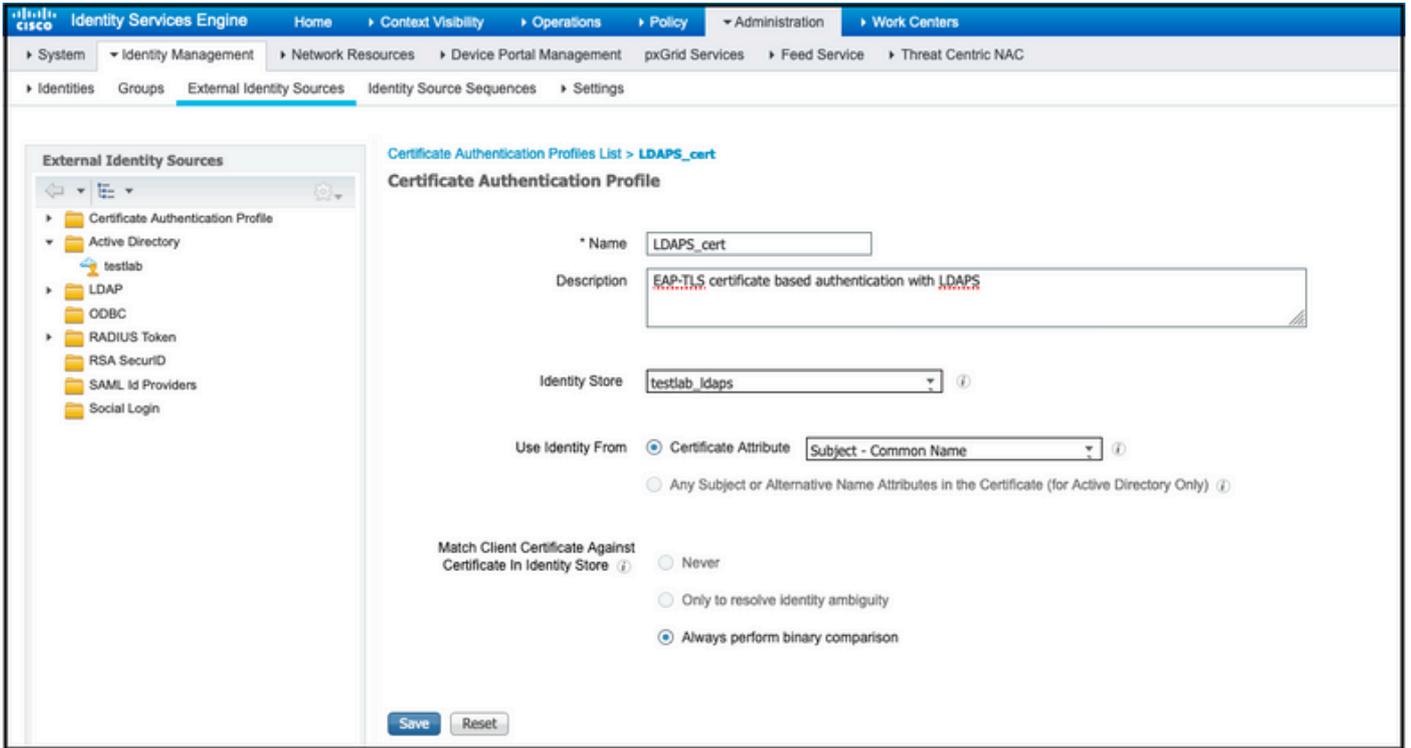


3. 추가 설정을 클릭하면 창이 열립니다. 이 이미지에 표시된 대로 인증 모드를 지정하고 사용자 인증을 선택합니다.



ISE에서 정책 설정 구성

EAP-TLS 프로토콜이 사용되므로 정책 집합을 구성하기 전에 인증서 인증 프로파일을 구성해야 하며 ID 소스 시퀀스가 나중에 인증 정책에서 사용됩니다.



ID 소스 시퀀스의 인증서 인증 프로파일을 참조하고 인증 검색 목록에서 LDAPS 외부 ID 소스를 정의합니다.

Identity Services Engine Administration > Identity Source Sequences

Identity Source Sequence

Identity Source Sequence

* Name:

Description:

Certificate Based Authentication

Select Certificate Authentication Profile:

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected	
Internal Endpoints	>	testlab_ldaps	⌵
Internal Users	<		⬆
Guest Users			⬇
testlab	⏏		⬇
All_AD_Join_Points	⏏		⬇
rad	⏏		⬇

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

이제 유선 Dot1x 인증에 대한 정책 집합을 구성합니다.

Identity Services Engine Administration > Policy Sets

Policy Sets → Wired Dot1x

Reset Policyset Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wired Dot1x		Wired_802.1X	Default Network Access	453

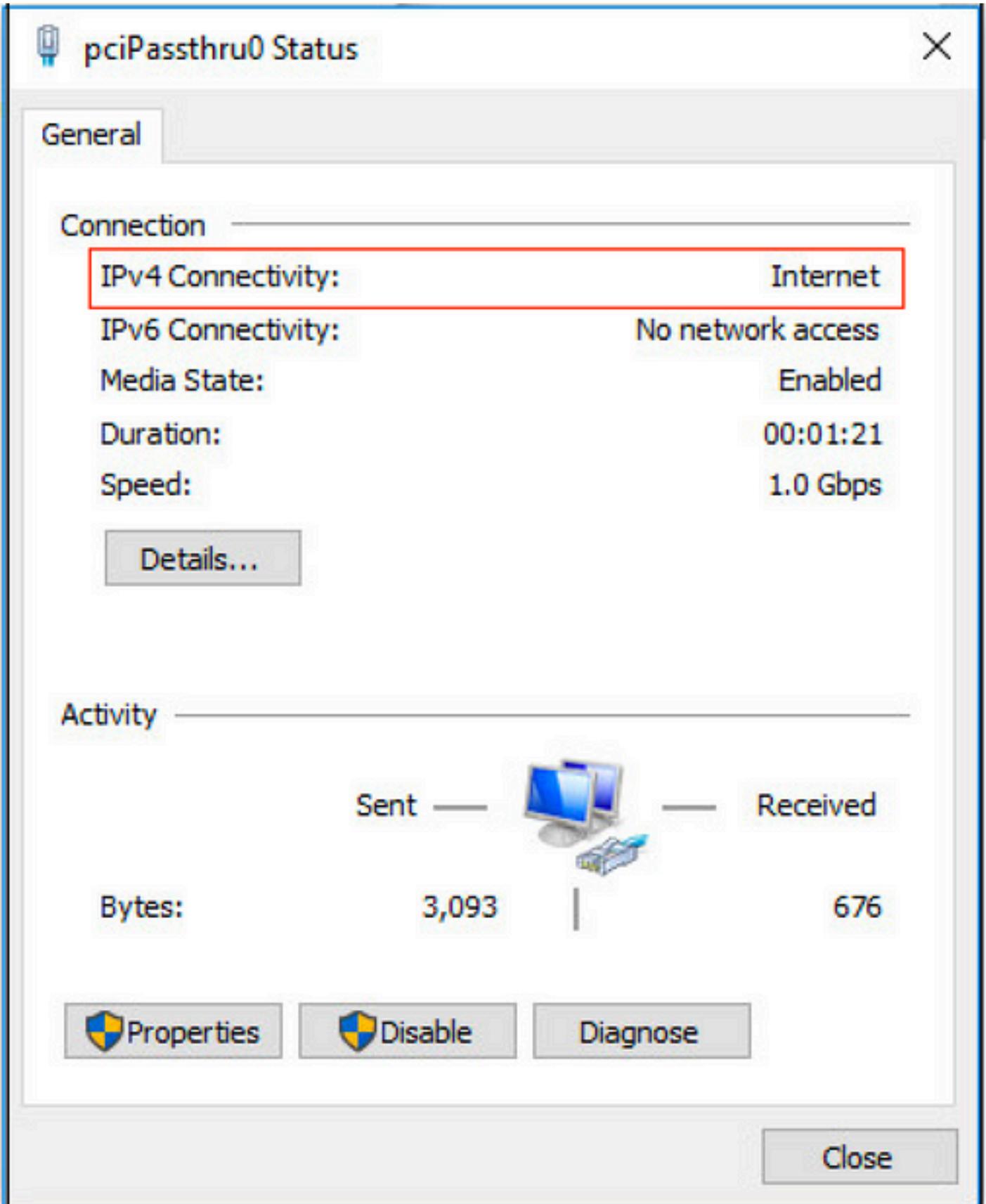
Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS	223	Options
✔	Default		LDAPS	0	Options

Authorization Policy (2)							
+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
Search							
<input checked="" type="checkbox"/>	Users in LDAP Store		testlab_ldaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	<input type="text" value="x PermiAccess"/>	<input type="text" value="Select from list"/>	207	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Default			<input type="text" value="x DenyAccess"/>	<input type="text" value="Select from list"/>	11	<input type="checkbox"/>

Reset Save

이 컨피그레이션 후 LDAPS ID 소스에 대해 EAP-TLS 프로토콜을 사용하여 엔드포인트를 인증할 수 있습니다.



다음을 확인합니다.

1. PC에 연결된 스위치 포트에서 인증 세션을 확인합니다.

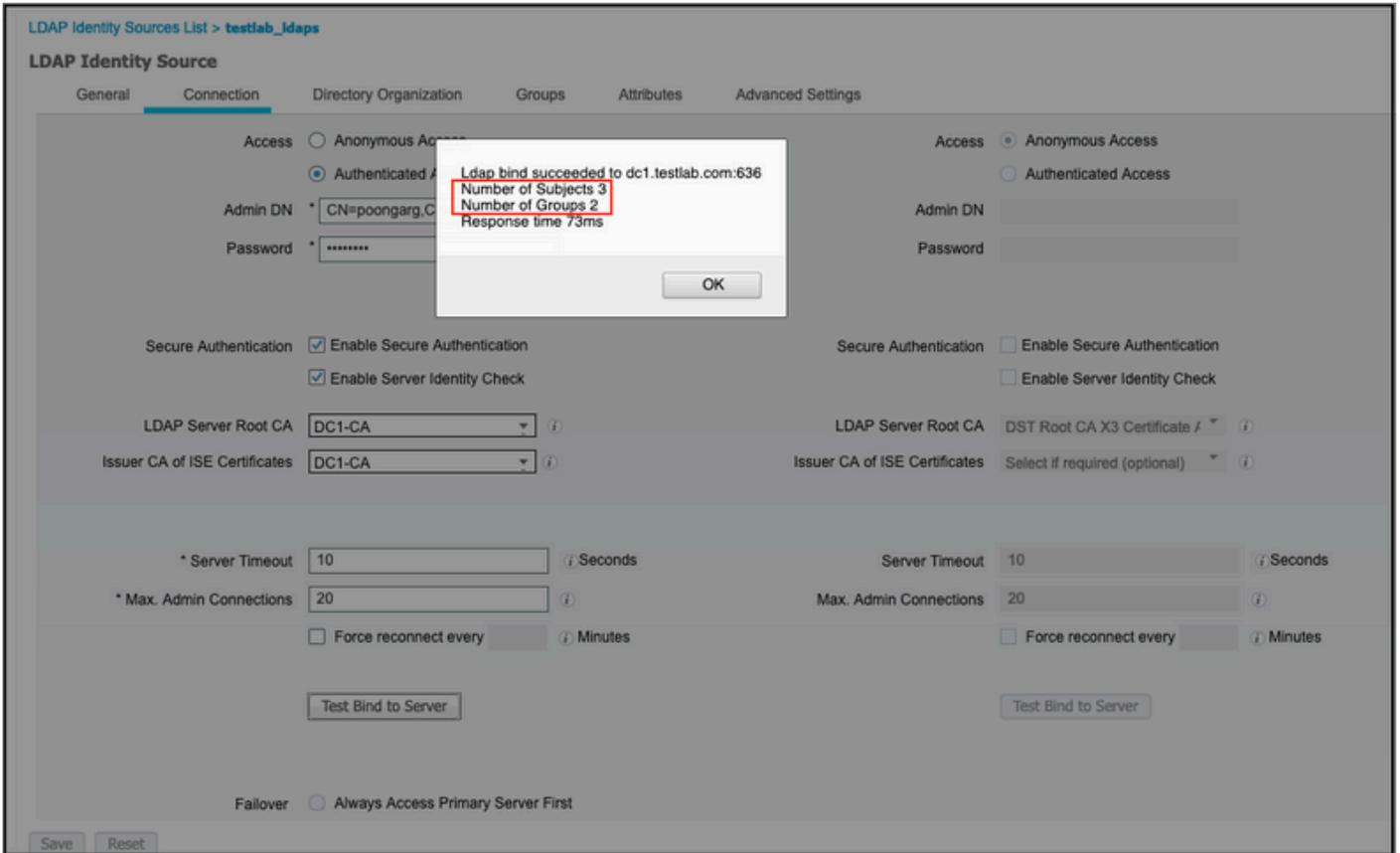
```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Periodic Acct timeout: N/A
      Session Uptime: 43s
      Common Session ID: 0A6A26390000130798C66612
      Acct Session ID: 0x00001224
      Handle: 0x6800002E
      Current Policy: POLICY_Gi2/0/47

Local Policies:
      Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
      Method          State
      dot1x           Authc Success
```

2. LDAPS 및 ISE 컨피그레이션을 확인하기 위해 서버에 대한 테스트 연결을 통해 주체 및 그룹을 검색할 수 있습니다.



3. 사용자 인증 보고서를 확인합니다.

Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...	Network De...	Device Port	Authentication Pro...
Jun 24, 2020 04:45:21.727 AM	●		user1	B4-96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess		GigabitEthernet2/0/47	EAP-TLS
Jun 24, 2020 04:45:20.671 AM	●		user1	B4-96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess	LAB-Switch	GigabitEthernet2/0/47	EAP-TLS

4. 엔드포인트에 대한 자세한 인증 보고서를 확인합니다.

Overview

Event 5200 Authentication succeeded

Username user1

Endpoint Id B4:96:91:26:DE:C0

Endpoint Profile Unknown

Authentication Policy Wired Dot1x >> Dot1x

Authorization Policy Wired Dot1x >> Users in LDAP Store

Authorization Result PermitAccess

Authentication Details

Source Timestamp 2020-06-24 04:40:52.124

Received Timestamp 2020-06-24 04:40:52.124

Policy Server ISE26-1

Event **5200 Authentication succeeded**

Username user1

Endpoint Id B4:96:91:26:DE:C0

Calling Station Id B4-96-91-26-DE-C0

Endpoint Profile Unknown

IPv4 Address 10.106.38.165

Authentication Identity Store testlab_idaps

Identity Group Unknown

Audit Session Id 0A6A26390000130C98CE6088

Authentication Method dot1x

Authentication Protocol EAP-TLS

Service Type Framed

Network Device LAB-Switch

15041 Evaluating Identity Policy

15048 Queried PIP - Network Access.NetworkDeviceName

22072 Selected identity source sequence - LDAPS

22070 Identity name is taken from certificate attribute

15013 Selected Identity Source - testlab_ldaps

24031 Sending request to primary LDAP server - testlab_ldaps

24016 Looking up user in LDAP Server - testlab_ldaps

24023 User's groups are retrieved - testlab_ldaps

24004 User search finished successfully - testlab_ldaps

22054 Binary comparison of certificates succeeded

22037 Authentication Passed

12506 EAP-TLS authentication succeeded

15036 Evaluating Authorization Policy

24209 Looking up Endpoint in Internal Endpoints IDStore - user1

24211 Found Endpoint in Internal Endpoints IDStore

15048 Queried PIP - testlab_ldaps.ExternalGroups

15016 Selected Authorization Profile - PermitAccess

22081 Max sessions policy passed

22080 New accounting session created in Session cache

11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

5. ISE에서 LDAPS 서버로 향하는 패킷 캡처를 수행하여 ISE와 LDAPS 서버 간에 데이터가 암호화되었는지 확인합니다.

No.	Time	Source	Destination	Protocol	Length	Address	64bits	Info
20	2020-06-24 10:40:24.205431	10.197.164.22	10.197.164.21	TCP	74	00:0c:29:98:ca:28,0...		28057 - 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=140972872 TSecr=0 WS=128
21	2020-06-24 10:40:24.206505	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f,0...		636 - 28057 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=30158962 TSecr=140972872
22	2020-06-24 10:40:24.206613	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 - 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
23	2020-06-24 10:40:24.206961	10.197.164.22	10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0...		Client Hello
24	2020-06-24 10:40:24.210413	10.197.164.21	10.197.164.22	TLSv1.2	2036	00:50:56:a0:3e:7f,0...		Server Hello, Certificate[Packet size limited during capture]
25	2020-06-24 10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 - 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0 TSval=140972877 TSecr=30158962
26	2020-06-24 10:40:24.215211	10.197.164.22	10.197.164.21	TLSv1.2	260	00:0c:29:98:ca:28,0...		Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	2020-06-24 10:40:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0...		Change Cipher Spec, Encrypted Handshake Message
28	2020-06-24 10:40:24.219113	10.197.164.22	10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28,0...		Application Data
29	2020-06-24 10:40:24.230384	10.197.164.21	10.197.164.22	TLSv1.2	167	00:50:56:a0:3e:7f,0...		Application Data
30	2020-06-24 10:40:24.231712	10.197.164.22	10.197.164.21	TLSv1.2	279	00:0c:29:98:ca:28,0...		Application Data
31	2020-06-24 10:40:24.238809	10.197.164.21	10.197.164.22	TLSv1.2	1079	00:50:56:a0:3e:7f,0...		Application Data[Packet size limited during capture]
32	2020-06-24 10:40:24.238958	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 - 636 [ACK] Seq=682 Ack=3992 Win=36864 Len=0 TSval=140972905 TSecr=30158965
33	2020-06-24 10:40:24.251944	10.197.164.22	10.197.164.21	TLSv1.2	263	00:0c:29:98:ca:28,0...		Application Data
34	2020-06-24 10:40:24.253658	10.197.164.21	10.197.164.22	TLSv1.2	295	00:50:56:a0:3e:7f,0...		Application Data
35	2020-06-24 10:40:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 - 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967
86	2020-06-24 10:40:57.946553	10.197.164.21	10.197.164.21	TLSv1.2	151	00:0c:29:98:ca:28,0...		Application Data
87	2020-06-24 10:40:57.947600	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 - 636 [FIN, ACK] Seq=964 Ack=4221 Win=39680 Len=0 TSval=141006614 TSecr=30158967

```

> Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Ethernet II, Src: Vmware_08:00:50:56:a0:3e:7f, Dst: Vmware_08:00:29:98:ca:28
> Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21
> Transmission Control Protocol, Src Port: 28057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133
  Source Port: 28057
  Destination Port: 636
  [Stream index: 2]
  [TCP Segment Len: 133]
  Sequence number: 336 (relative sequence number)
  [Next sequence number: 469 (relative sequence number)]
  Acknowledgment number: 2078 (relative ack number)
  1000 ... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
  Window size value: 259
  [Calculated window size: 33152]
  [Window size scaling factor: 128]
  Checksum: 0x5e61 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  > [Timestamps]
  > TCP payload (133 bytes)
  Secure Sockets Layer
  > TLSv1.2 Record Layer: Application Data Protocol: ldap
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 128
    Encrypted Application Data: 17301b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84...
  
```

→ Encrypted Data

문제 해결

이 섹션에서는 이 컨피그레이션에서 발생하는 몇 가지 일반적인 오류와 그 해결 방법에 대해 설명합니다.

- 인증 보고서에서 다음 오류 메시지를 볼 수 있습니다.

```
Authentication method is not supported by any applicable identity store
```

이 오류 메시지는 선택한 방법이 LDAP에서 지원되지 않음을 나타냅니다. 동일한 보고서의 인증 프로토콜이 지원되는 방법(EAP-GTC, EAP-TLS 또는 PEAP-TLS) 중 하나를 표시하는지 확인합니다.

- 서버에 대한 테스트 바인딩이 오류와 함께 종료되었습니다.

가장 일반적으로 이는 LDAPS 서버 인증서 유효성 검사 실패 때문입니다. 이러한 유형의 문제를 해결하려면 ISE에서 패킷 캡처를 수행하고 디버그 레벨에서 세 가지 런타임 및 prrt-jni 구성 요소를 모두 활성화하고, 문제를 다시 생성한 다음 prrt-server.log 파일을 확인합니다.

패킷 캡처가 잘못된 인증서에 대해 불평하고 포트 서버가 다음을 표시합니다.

```
04:10:20,197,ERROR,0x7f9c5b6f1700,LdapSslConnectionContext::checkCryptoResult(id = 1289): error message
```

 참고: LDAP 페이지의 호스트 이름은 인증서의 주체 이름(또는 임의의 주체 대체 이름)으로 구성해야 합니다. 따라서 주체 또는 SAN에 이러한 인증서가 없으면 작동하지 않으며 SAN 목록에 IP 주소가 있는 인증서가 필요합니다.

3. 인증 보고서에서 ID 저장소에서 주체를 찾을 수 없음을 알 수 있습니다. 즉, 보고서의 사용자 이름이 LDAP 데이터베이스의 사용자에게 대한 Subject Name Attribute와 일치하지 않습니다. 이 시나리오에서는 이 특성의 값이 sAMAccountName으로 설정되었습니다. 즉 ISE가 LDAP 사용자가 일치하는 항목을 찾으려고 할 때 LDAP 사용자의 sAMAccountName 값을 확인합니다.

4. 서버 테스트에 바인딩하는 동안 제목 및 그룹을 올바르게 검색할 수 없습니다. 이 문제의 가장 큰 원인은 검색 기준에 대한 잘못된 컨피그레이션입니다. LDAP 계층 구조는 leaf-to-root 및 dc(여러 단어로 구성 가능)에서 지정해야 합니다.

관련 정보

- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/119149-configure-ise-00.html#anc9>
- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-configure-eap-tls-authentication-with-is.html>

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.