LDAP 서버와의 통합을 위해 ISE 구성

목차

소개

이 문서에서는 Cisco LDAP 서버와의 통합을 위해 Cisco ISE(Identity Services Engine)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 1.3(패치 2 포함)
- Microsoft Windows 버전 7 x64(OpenLDAP 설치)
- Cisco WLC(Wireless LAN Controller) 버전 8.0.100.0
- Microsoft Windows용 Cisco AnyConnect 버전 3.1
- Cisco Network Access Manager 프로파일 편집기

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

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

다음 인증 방법은 LDAP에서 지원됩니다.

- 확장 가능 한 인증 프로토콜 - 일반 토큰 카드 (EAP-GTC)
- 확장 인증 프로토콜 - 전송 계층 보안(EAP-TLS)
- 보호 된 확장 가능 한 인증 프로토콜 - 전송 계층 보안 (PEAP-TLS)

구성

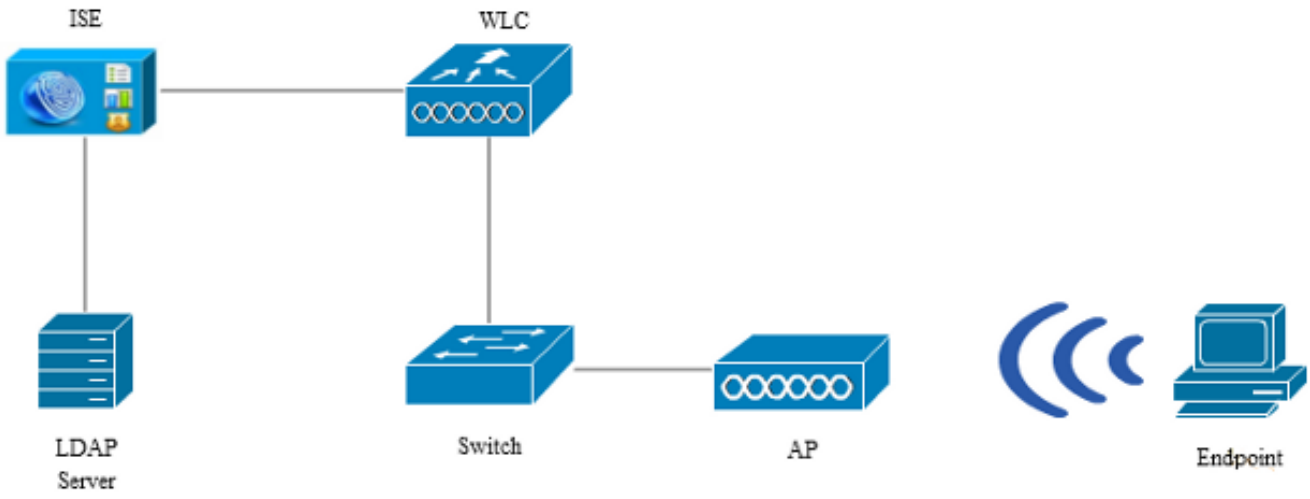
이 섹션에서는 네트워크 디바이스를 구성하고 ISE를 LDAP 서버와 통합하는 방법에 대해 설명합니다.

네트워크 다이어그램

이 컨피그레이션 예에서 엔드포인트는 무선 네트워크와 연결하기 위해 무선 어댑터를 사용합니다.

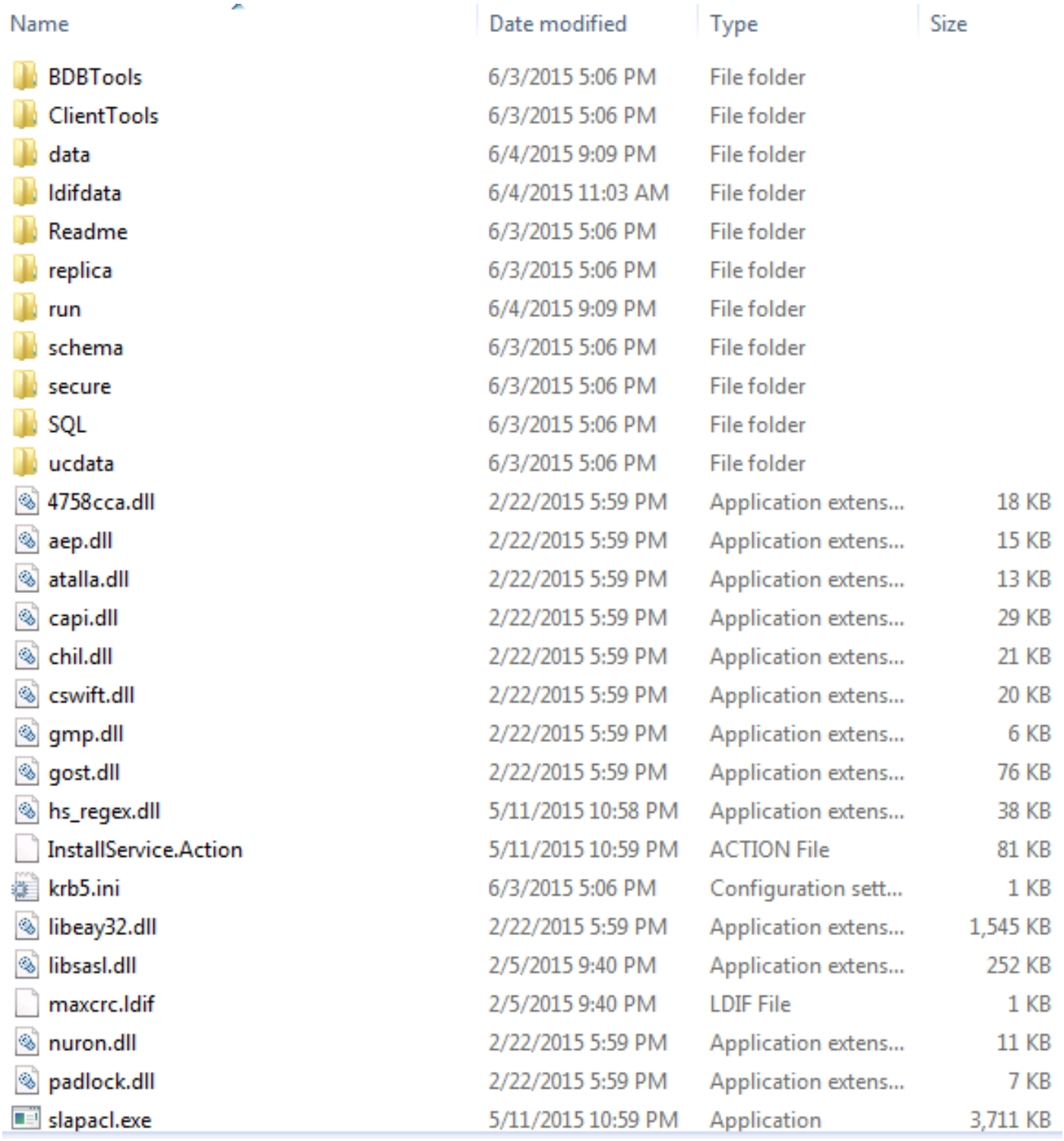
ISE를 통해 사용자를 인증하기 위해 WLC의 무선 LAN(WLAN)이 구성됩니다. ISE에서 LDAP는 외부 ID 저장소로 구성됩니다.

이 이미지는 사용되는 네트워크 토폴로지를 보여줍니다.



OpenLDAP 구성

Microsoft Windows용 OpenLDAP의 설치는 GUI를 통해 완료되며, 이는 간단합니다. 기본 위치는 C: > OpenLDAP입니다. 설치 후 다음 디렉토리가 표시되어야 합니다.

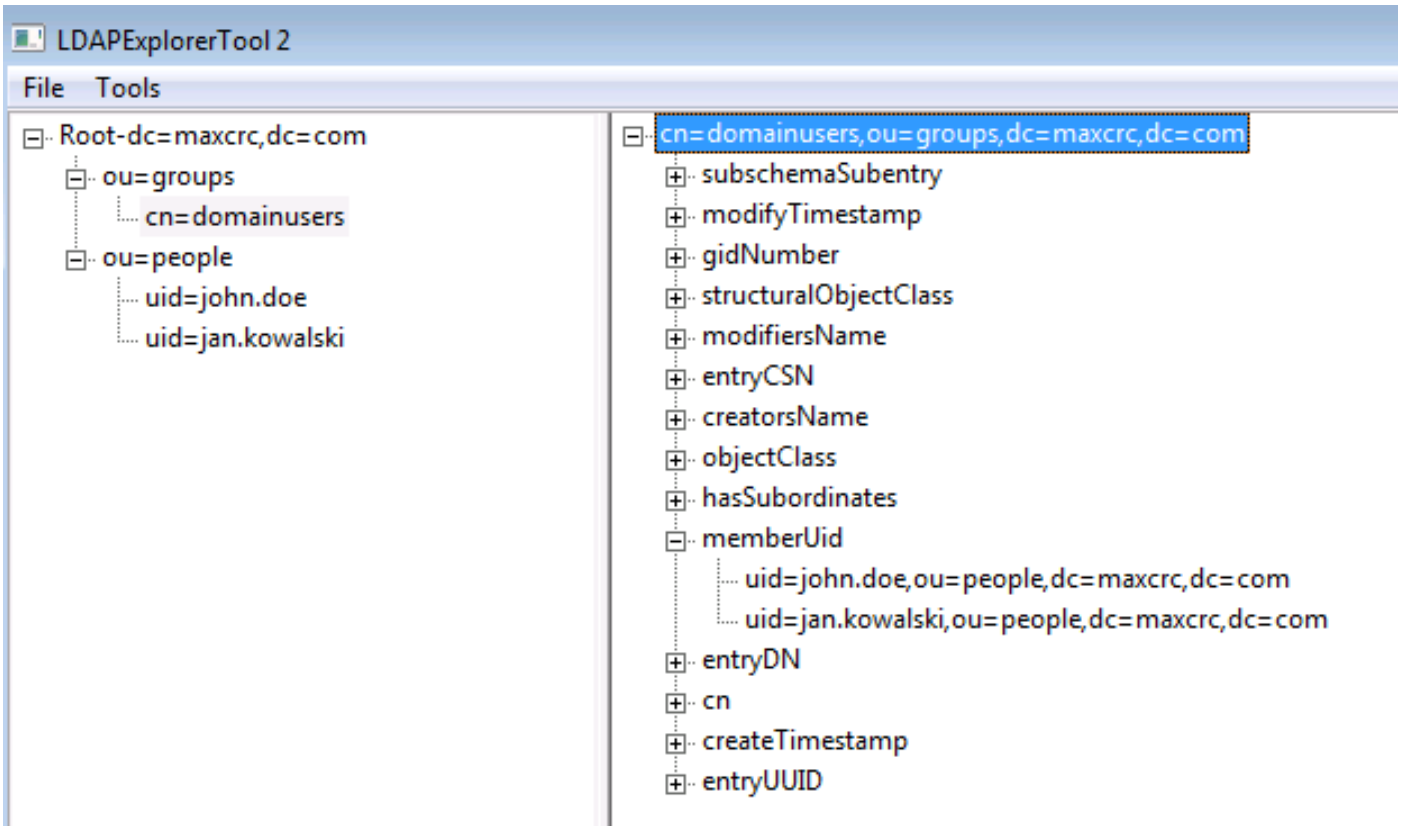


Name	Date modified	Type	Size
BDBTools	6/3/2015 5:06 PM	File folder	
ClientTools	6/3/2015 5:06 PM	File folder	
data	6/4/2015 9:09 PM	File folder	
ldifdata	6/4/2015 11:03 AM	File folder	
Readme	6/3/2015 5:06 PM	File folder	
replica	6/3/2015 5:06 PM	File folder	
run	6/4/2015 9:09 PM	File folder	
schema	6/3/2015 5:06 PM	File folder	
secure	6/3/2015 5:06 PM	File folder	
SQL	6/3/2015 5:06 PM	File folder	
ucdata	6/3/2015 5:06 PM	File folder	
4758cca.dll	2/22/2015 5:59 PM	Application extens...	18 KB
aep.dll	2/22/2015 5:59 PM	Application extens...	15 KB
atalla.dll	2/22/2015 5:59 PM	Application extens...	13 KB
capi.dll	2/22/2015 5:59 PM	Application extens...	29 KB
chil.dll	2/22/2015 5:59 PM	Application extens...	21 KB
cswift.dll	2/22/2015 5:59 PM	Application extens...	20 KB
gmp.dll	2/22/2015 5:59 PM	Application extens...	6 KB
gost.dll	2/22/2015 5:59 PM	Application extens...	76 KB
hs_regex.dll	5/11/2015 10:58 PM	Application extens...	38 KB
InstallService.Action	5/11/2015 10:59 PM	ACTION File	81 KB
krb5.ini	6/3/2015 5:06 PM	Configuration sett...	1 KB
libeay32.dll	2/22/2015 5:59 PM	Application extens...	1,545 KB
libsasl.dll	2/5/2015 9:40 PM	Application extens...	252 KB
maxcrc.ldif	2/5/2015 9:40 PM	LDIF File	1 KB
nuron.dll	2/22/2015 5:59 PM	Application extens...	11 KB
padlock.dll	2/22/2015 5:59 PM	Application extens...	7 KB
slapacl.exe	5/11/2015 10:59 PM	Application	3,711 KB

특히 다음 두 디렉토리를 기록해 둡니다.

- ClientTools - 이 디렉토리에는 LDAP 데이터베이스를 편집하는 데 사용되는 이진 파일 집합이 포함됩니다.
- ldifdata - LDAP 객체와 함께 파일을 저장해야 하는 위치입니다.

LDAP 데이터베이스에 이 구조를 추가합니다.



Root 디렉토리 아래에서 두 개의 OU(Organizational Unit)를 구성해야 합니다. OU=groups OU에는 1개의 하위 그룹(이 예에서는 cn=domainusers)이 있어야 합니다.

OU=people OU는 cn=domainusers 그룹에 속하는 두 개의 사용자 계정을 정의합니다.

데이터베이스를 채우려면 먼저 ldif 파일을 생성해야 합니다. 이전에 언급한 구조는 이 파일에서 생성되었습니다.

```
dn: ou=groups,dc=maxcrc,dc=com
changetype: add
ou: groups
description: All groups in organisation
objectclass: organizationalunit

dn: ou=people,dc=maxcrc,dc=com
changetype: add
ou: people
description: All people in organisation
objectclass: organizationalunit

dn: uid=john.doe,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
givenName: John
sn: Doe
cn: John Doe
mail: john.doe@example.com
```

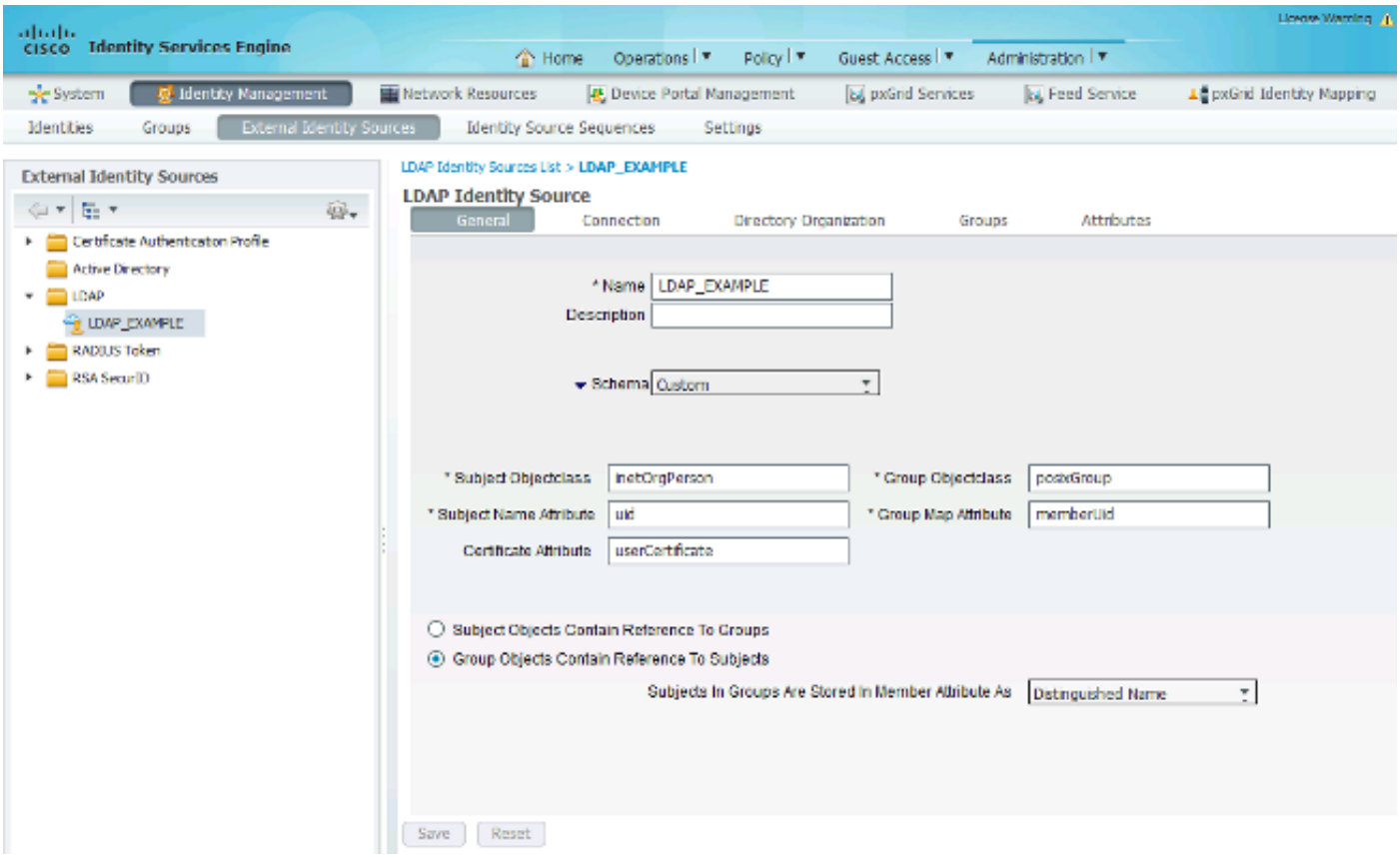
```
userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: jan.kowalski
givenName: Jan
sn: Kowalski
cn: Jan Kowalski
mail: jan.kowalski@example.com
userPassword: password

dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: posixGroup
gidNumber: 678
memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com
memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
```

LDAP 데이터베이스에 객체를 추가하려면 ldapmodify 이진을 사용합니다.

```
C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager,
dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif
ldap_connect_to_host: TCP localhost:389
ldap_new_socket: 496
ldap_prepare_socket: 496
ldap_connect_to_host: Trying ::1 389
ldap_pvt_connect: fd: 496 tm: -1 async: 0
attempting to connect:
connect success
adding new entry "ou=groups,dc=maxcrc,dc=com"

adding new entry "ou=people,dc=maxcrc,dc=com"

adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"
```

OpenLDAP를 ISE와 통합

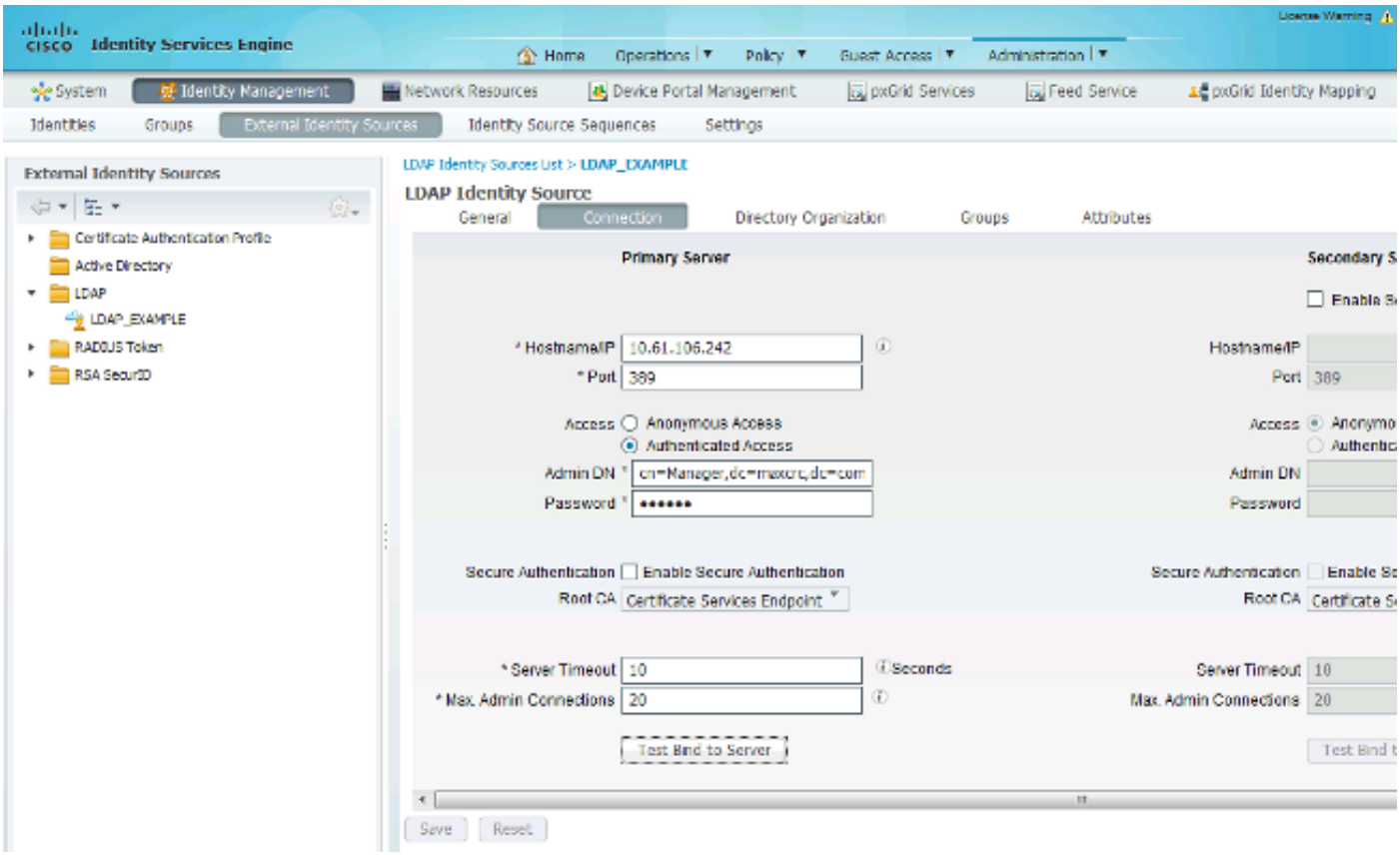
LDAP를 ISE의 외부 ID 저장소로 구성하려면 이 섹션 전체에서 이미지에 제공된 정보를 사용합니다
.



General(일반) 탭에서 이러한 특성을 구성할 수 있습니다.

- Subject Objectclass - 이 필드는 ldif 파일에 있는 사용자 계정의 개체 클래스에 해당합니다. LDAP 컨피그레이션에 따라 다음 네 가지 클래스 중 하나를 사용합니다.
    - 상단
    - 개인
    - 조직인
    - InetOrg사람
- 주체 이름 특성 - ISE가 특정 사용자 이름이 데이터베이스에 포함되어 있는지 여부를 문의할 때 LDAP에서 검색하는 특성입니다. 이 시나리오에서는 엔드포인트에서 john.doe 또는 jan.kowalski를 사용자 이름으로 사용해야 합니다.
- Group Objectclass - 이 필드는 ldif 파일의 그룹에 대한 객체 클래스에 해당합니다. 이 시나리오에서 cn=domainusers 그룹의 객체 클래스는 posixGroup입니다.
- 그룹 맵 특성 - 이 특성은 사용자가 그룹에 매핑되는 방법을 정의합니다. ldif 파일의 cn=domainusers 그룹에서 사용자에 해당하는 두 memberUid 특성을 볼 수 있습니다.

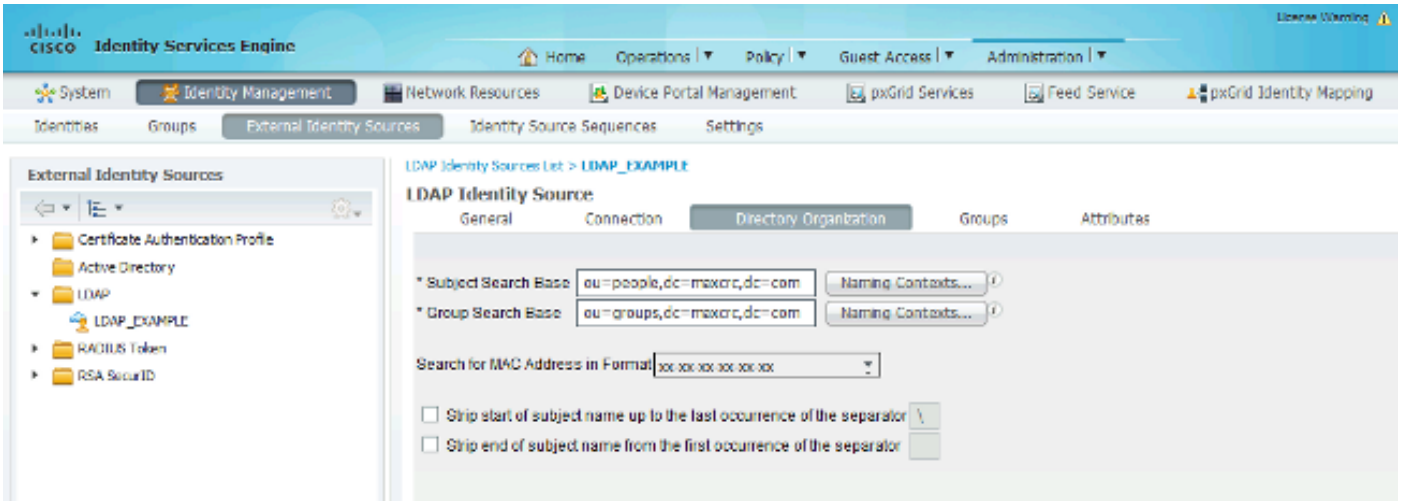
또한 ISE는 다음과 같이 사전 구성된 일부 스키마(Microsoft Active Directory, Sun, Novell)를 제공합니다.



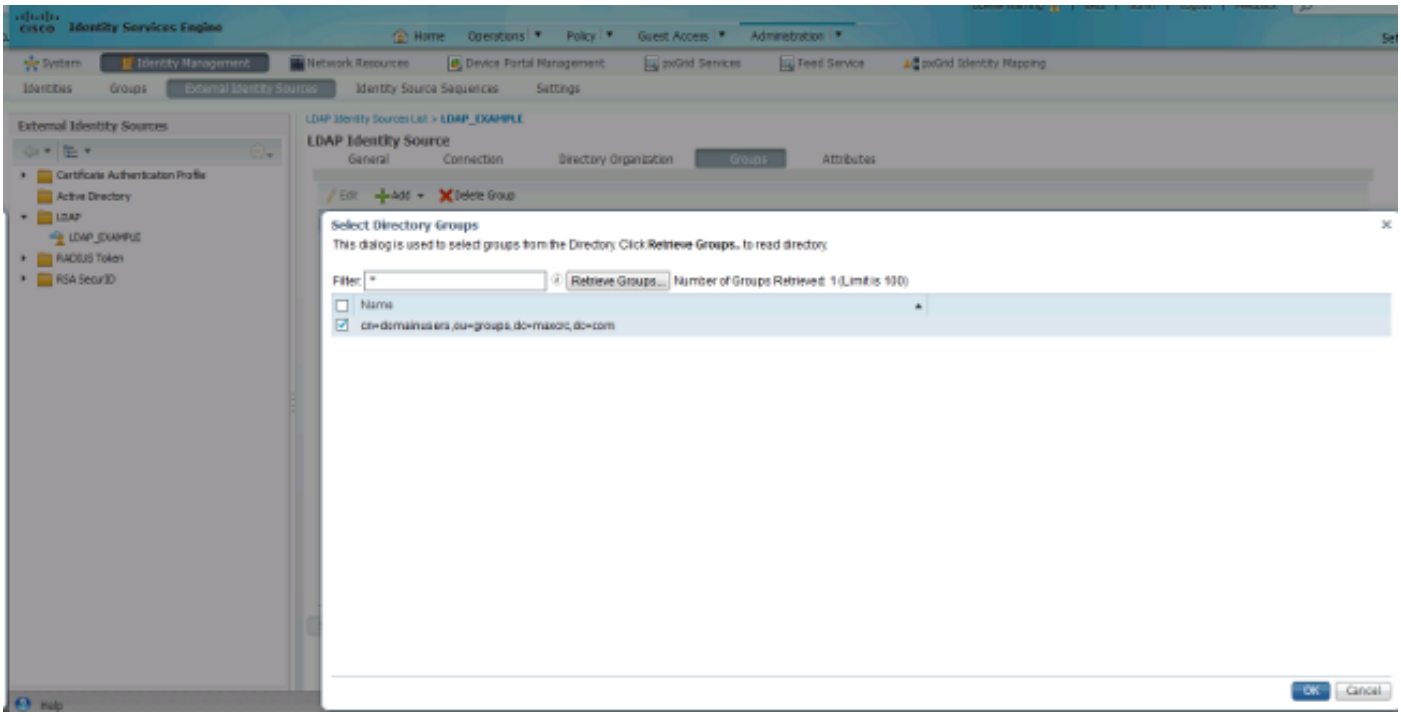
올바른 IP 주소 및 관리 도메인 이름을 설정한 후 서버에 대한 Test Bind를 수행할 수 있습니다. 검색 기준이 아직 구성되지 않았으므로 이 시점에서는 제목이나 그룹을 검색하지 않습니다.

다음 탭에서 Subject/Group Search Base(주체/그룹 검색 기반)를 구성합니다. LDAP에 대한 ISE의 조인 지점입니다. 가입 지점의 하위 멤버인 제목과 그룹만 검색할 수 있습니다.

이 시나리오에서는 OU=people의 제목과 OU=groups의 그룹이 검색됩니다.

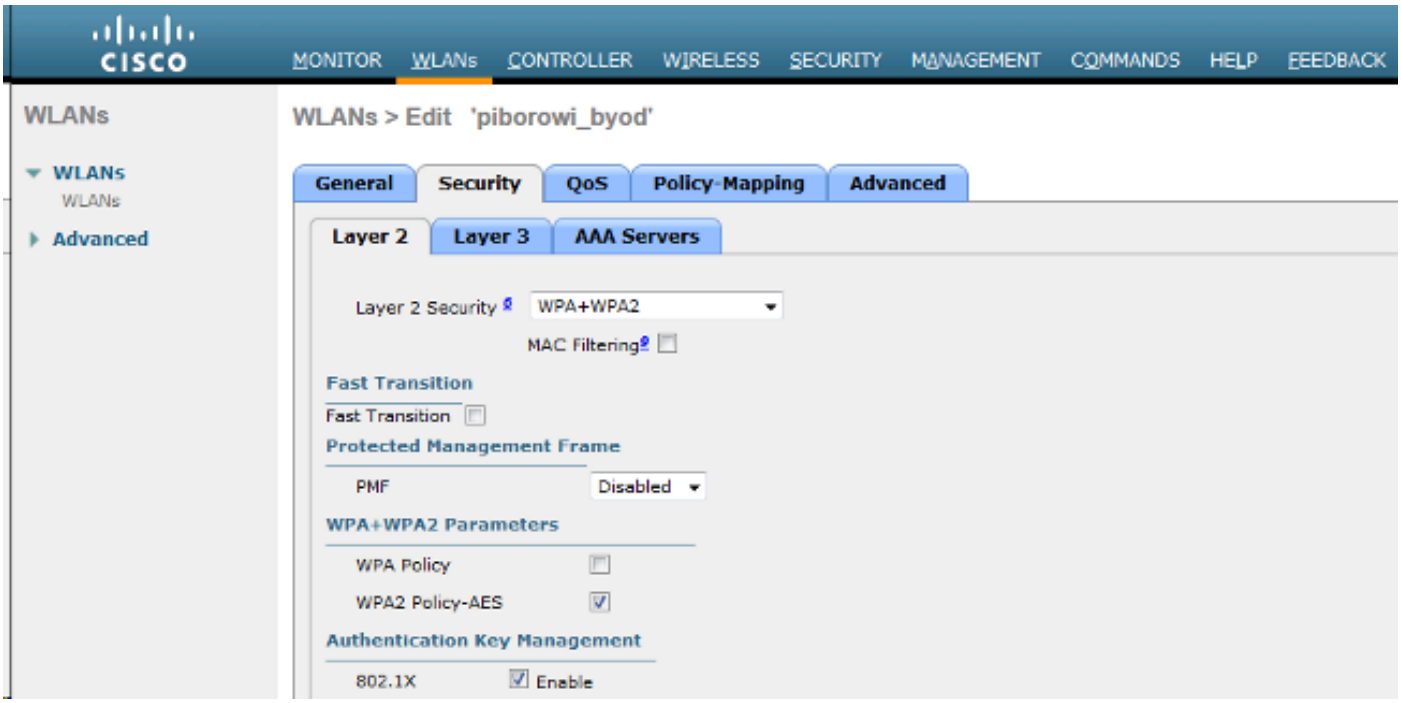


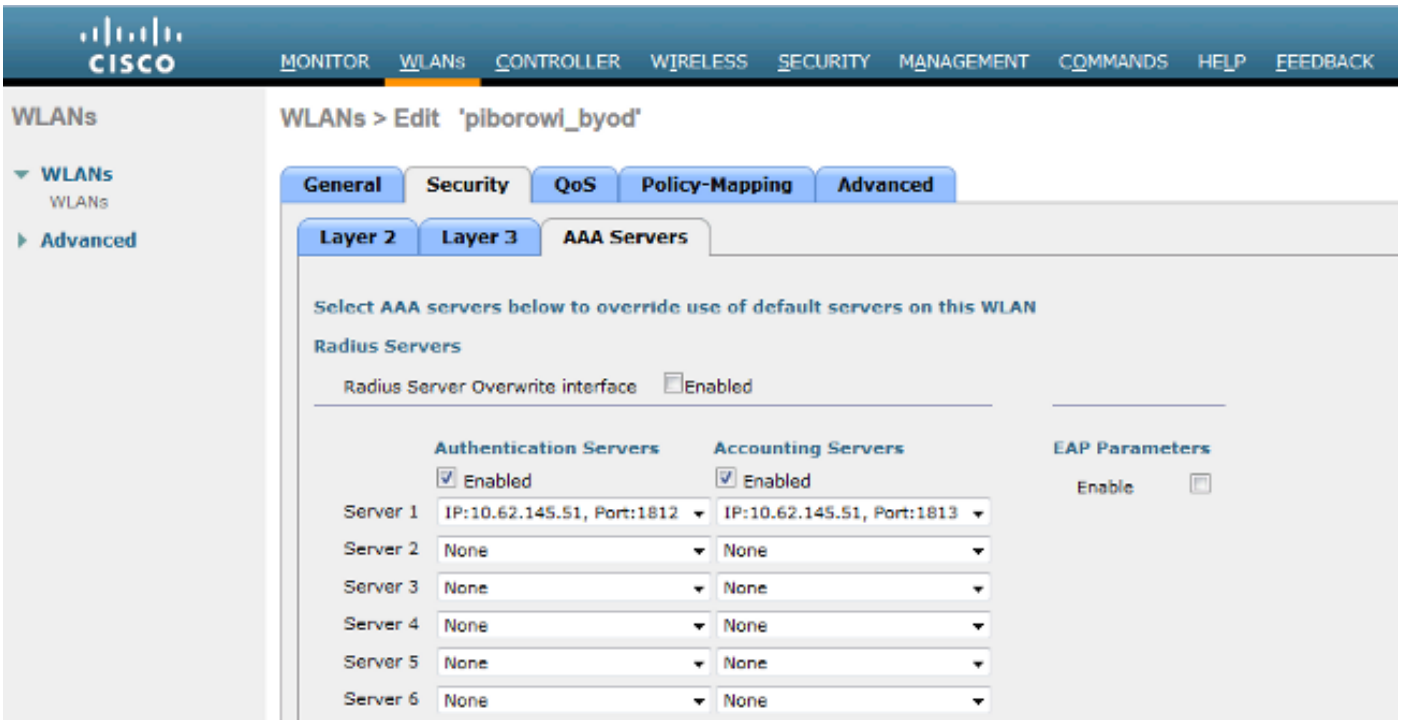
Groups(그룹) 탭에서 ISE의 LDAP에서 그룹을 가져올 수 있습니다.

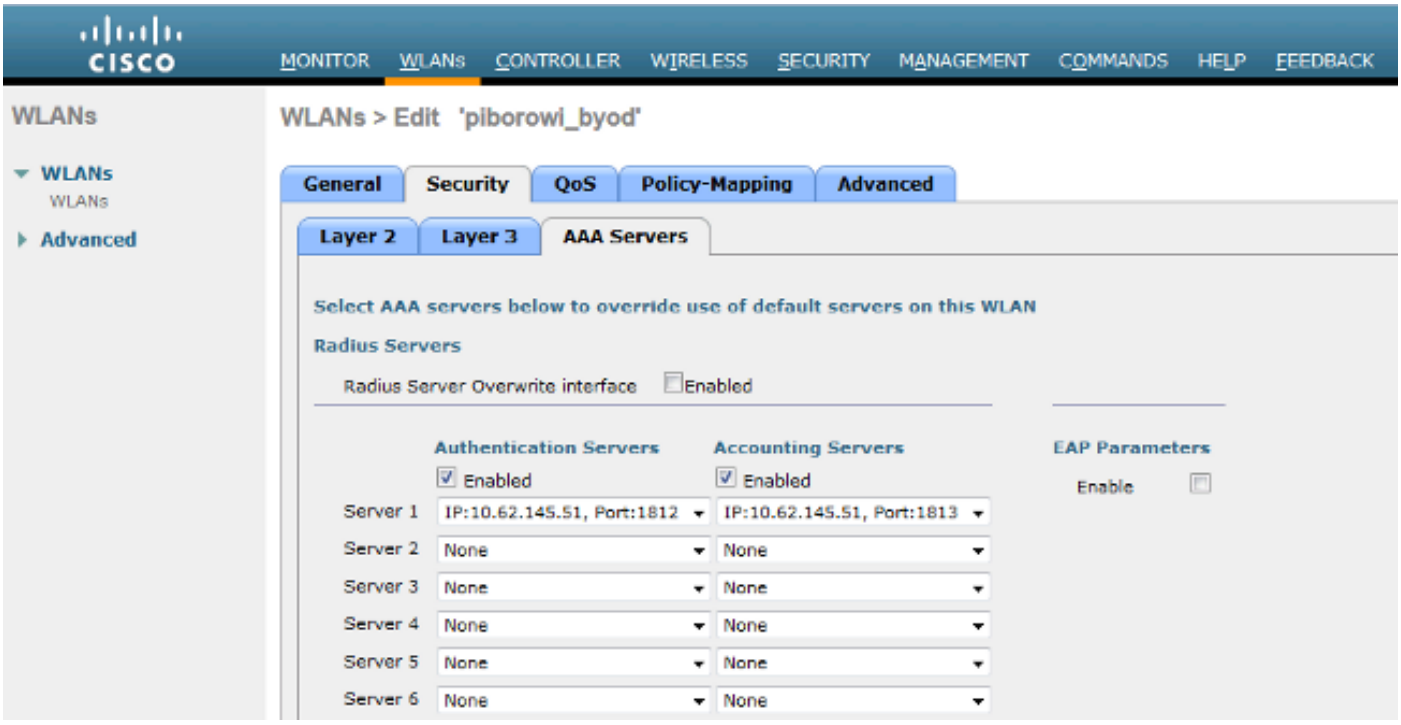


WLC 구성

802.1x 인증을 위해 WLC를 구성하려면 다음 이미지에 제공된 정보를 사용하십시오.







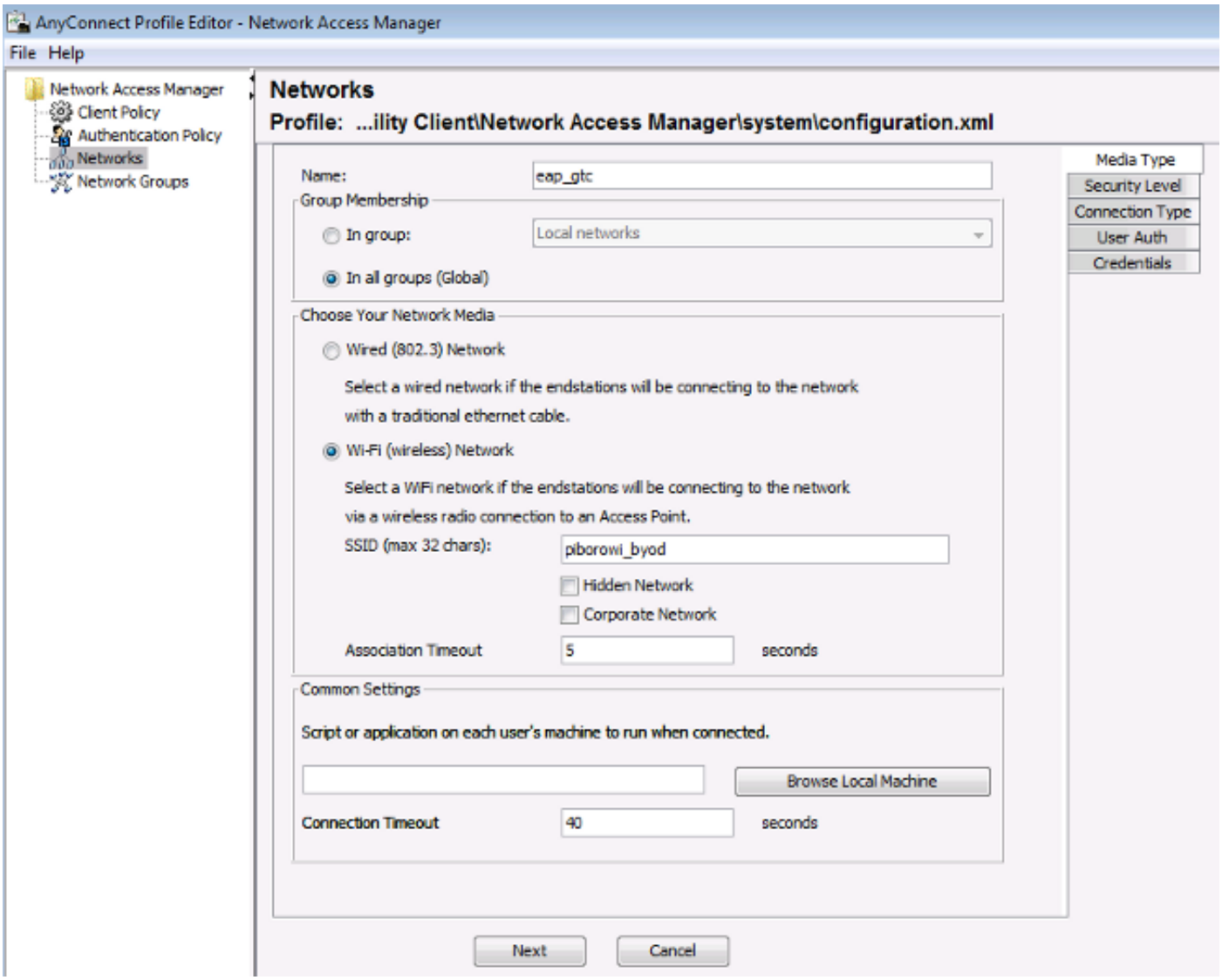
EAP-GTC 구성

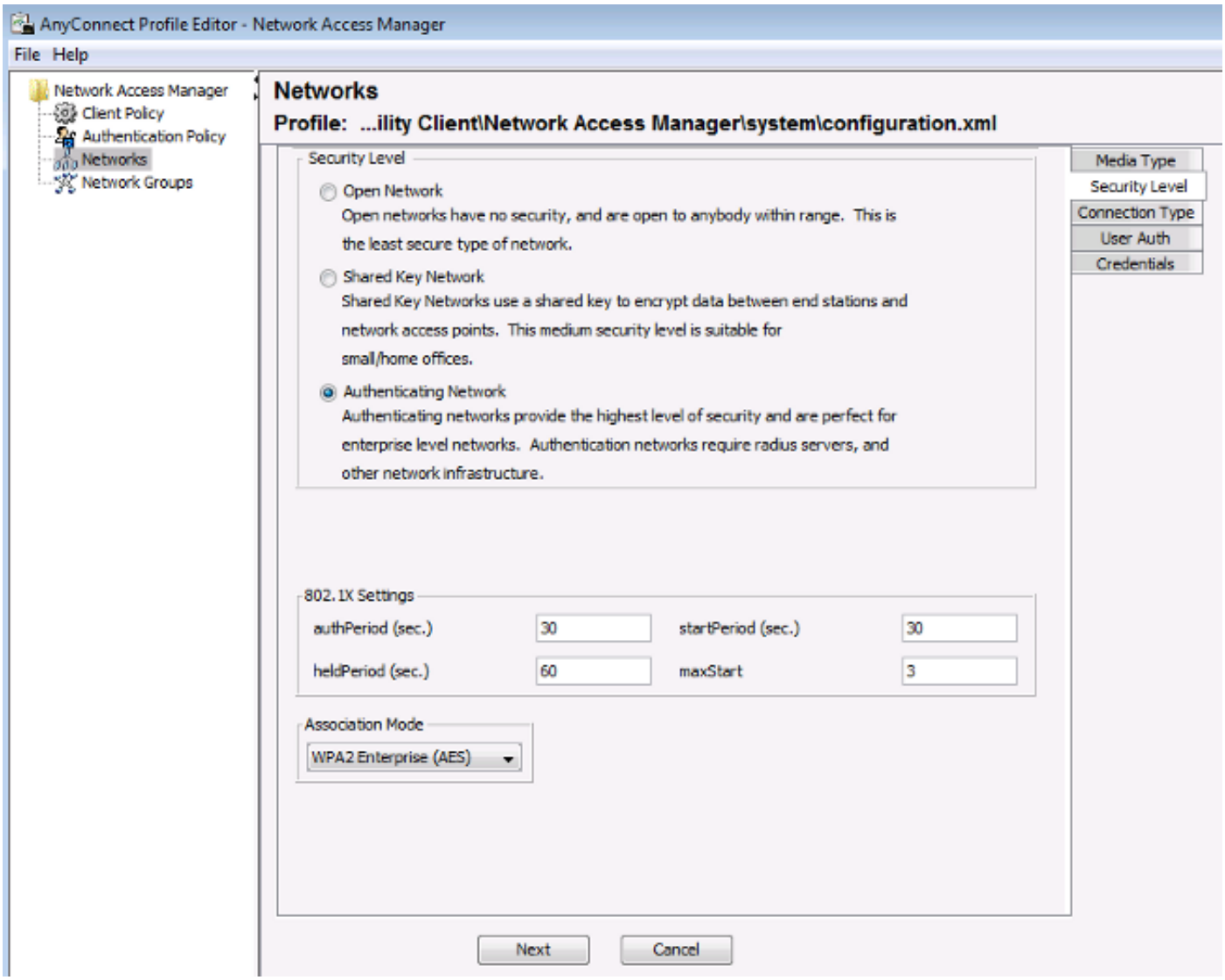
LDAP에 대해 지원되는 인증 방법 중 하나는 EAP-GTC입니다. Cisco AnyConnect에서 사용할 수 있지만 프로파일을 올바르게 구성하려면 Network Access Manager 프로파일 편집기를 설치해야 합니다.

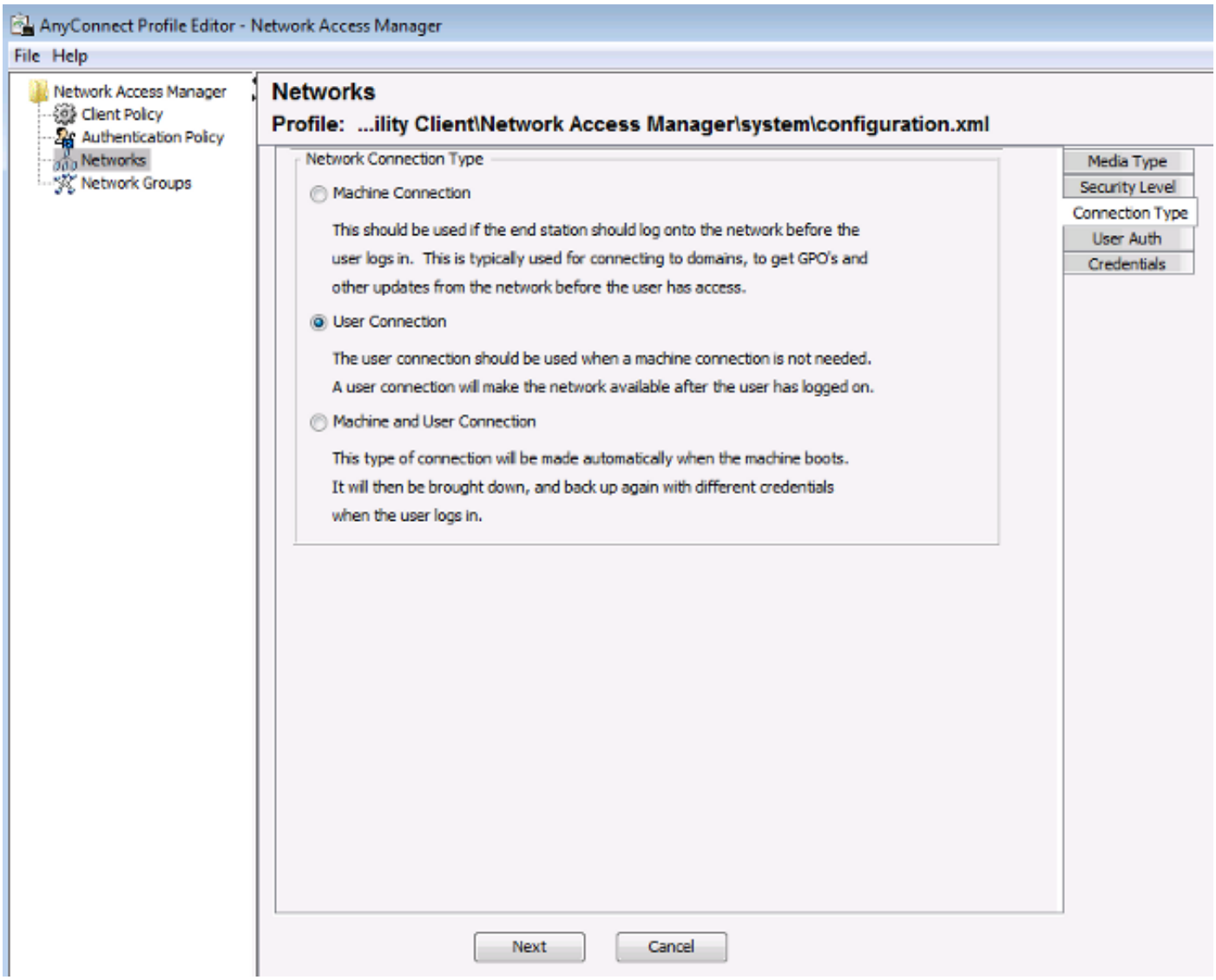
Network Access Manager 컨피그레이션도 편집해야 합니다. 이 컨피그레이션은 기본적으로 다음 위치에 있습니다.

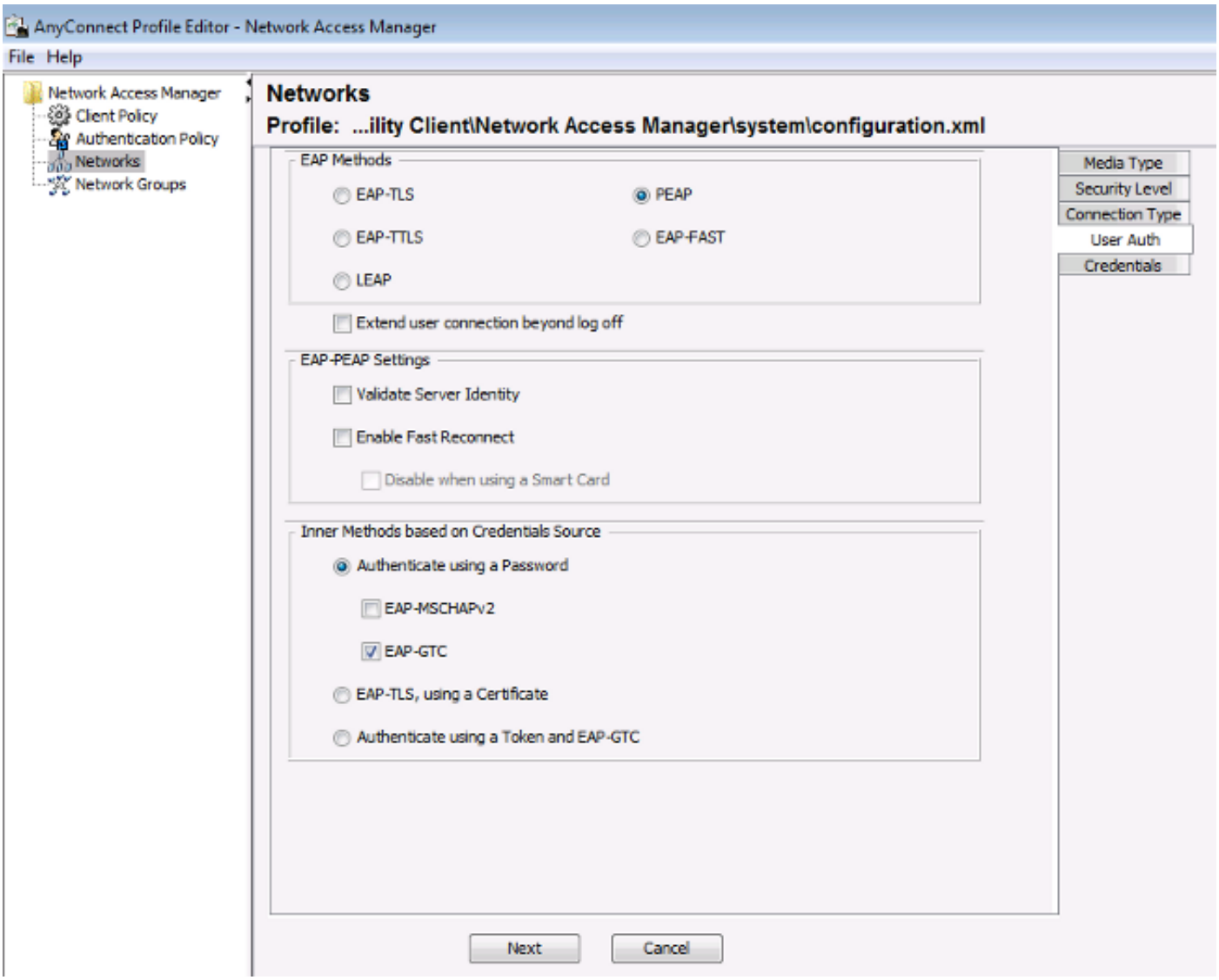
C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > system > configuration.xml 파일

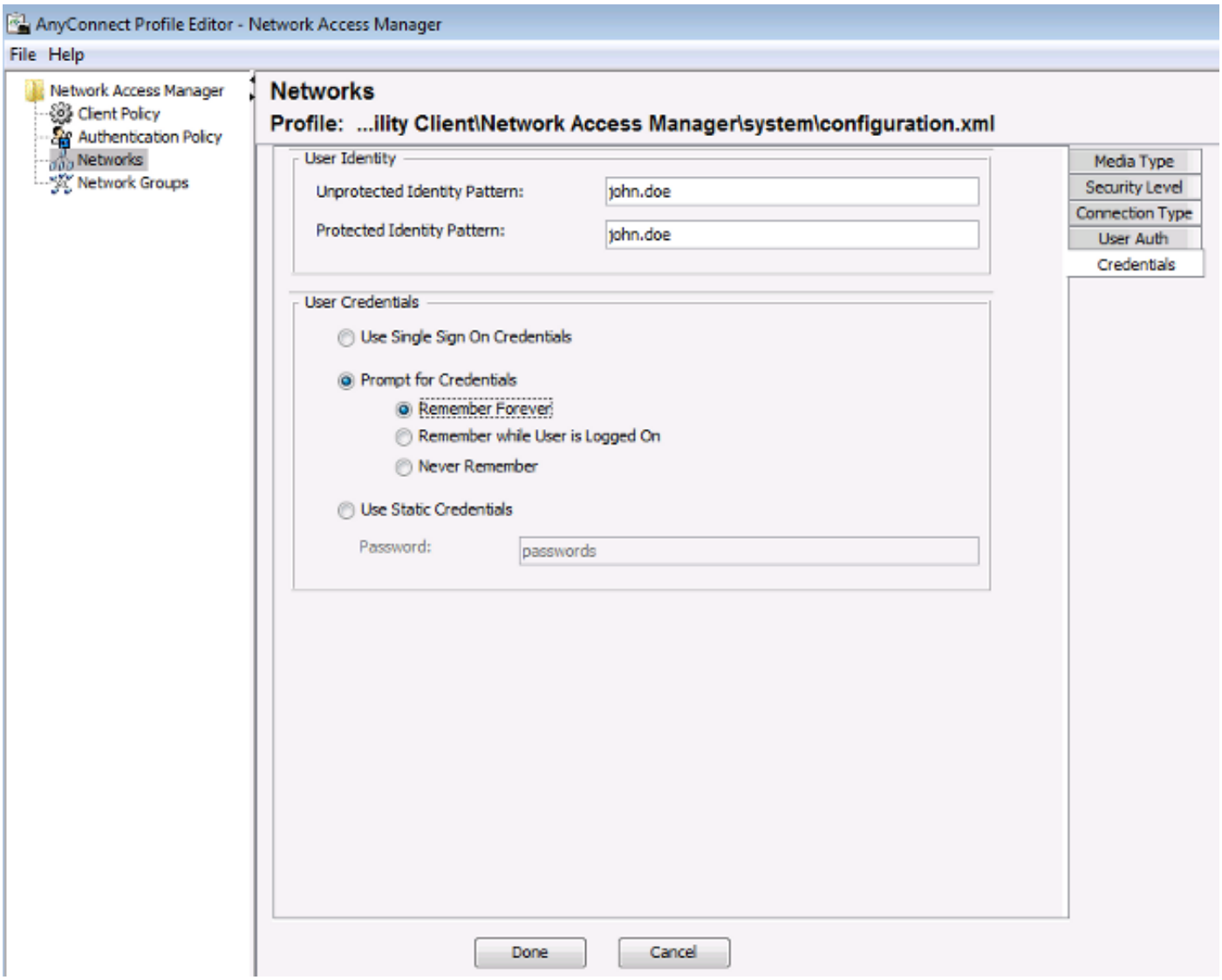
엔드포인트에서 EAP-GTC를 구성하려면 다음 이미지에 제공된 정보를 사용합니다.



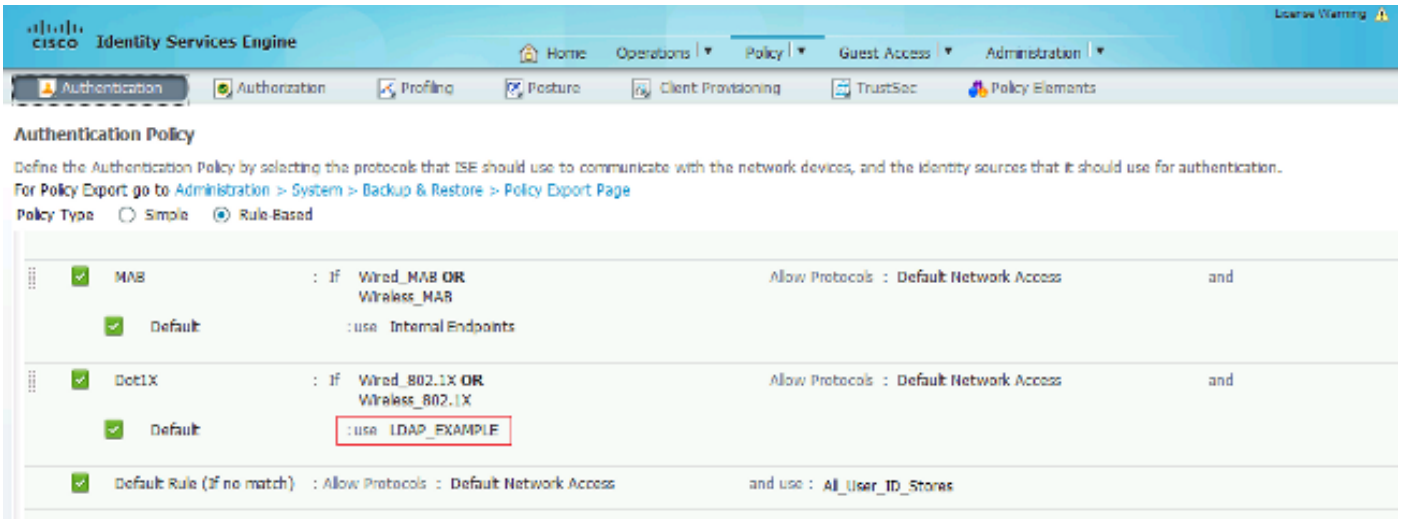

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Security Level
Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.
Shared Key Network
Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices.
Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.
Media Type
Security Level
Connection Type
User Auth
Credentials
802.1X Settings
authPeriod (sec.)
30
startPeriod (sec.)
30
heldPeriod (sec.)
60
maxStart
3
Association Mode
WPA2 Enterprise (AES)
Next
Cancel

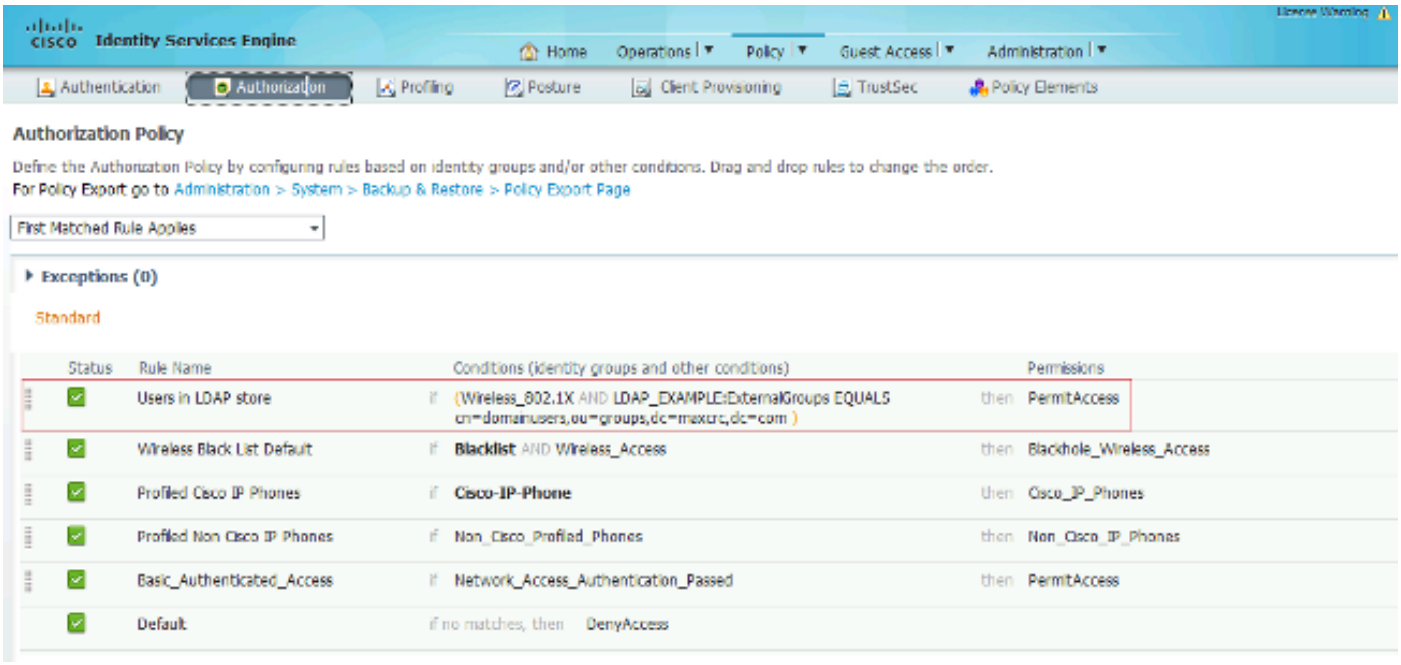

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
Network Connection Type
Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.
User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.
Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.
Media Type
Security Level
Connection Type
User Auth
Credentials
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: ...ility Client\Network Access Manager\system\configuration.xml
EAP Methods
EAP-TLS
PEAP
EAP-TTLS
EAP-FAST
LEAP
Extend user connection beyond log off
EAP-PEAP Settings
Validate Server Identity
Enable Fast Reconnect
Disable when using a Smart Card
Inner Methods based on Credentials Source
Authenticate using a Password
EAP-MSCHAPv2
EAP-GTC
EAP-TLS, using a Certificate
Authenticate using a Token and EAP-GTC
Media Type
Security Level
Connection Type
User Auth
Credentials
Next
Cancel

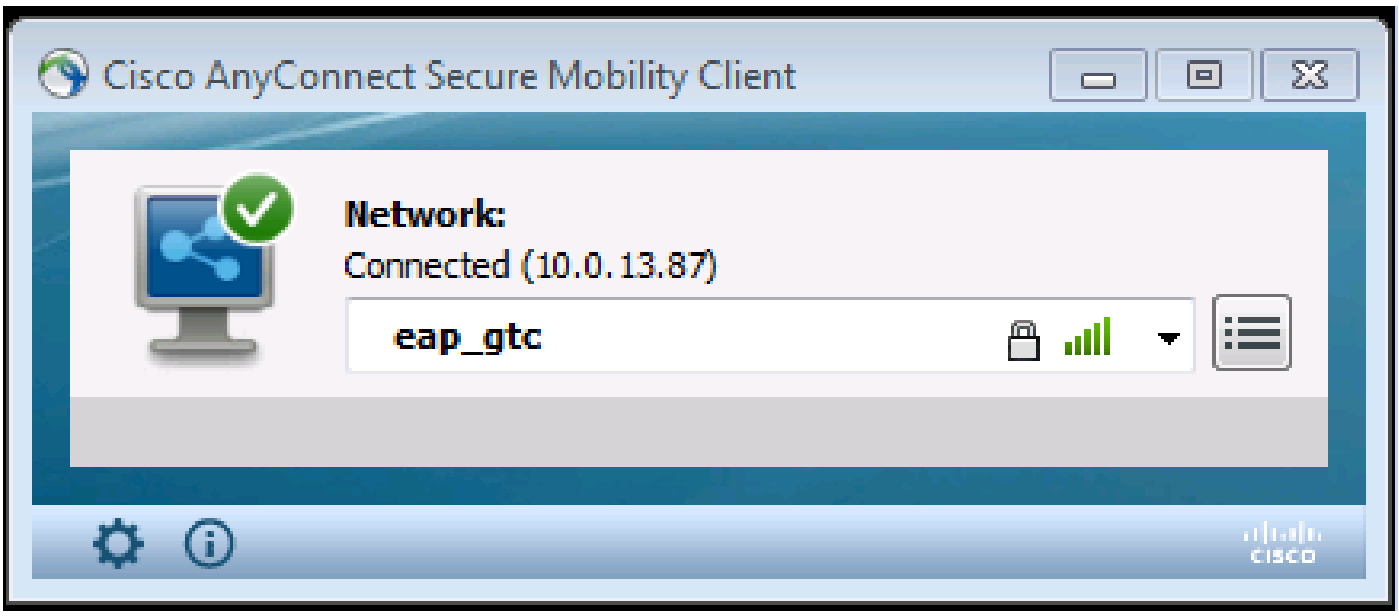


ISE의 인증 및 권한 부여 정책을 변경하려면 다음 이미지에 제공된 정보를 사용합니다.



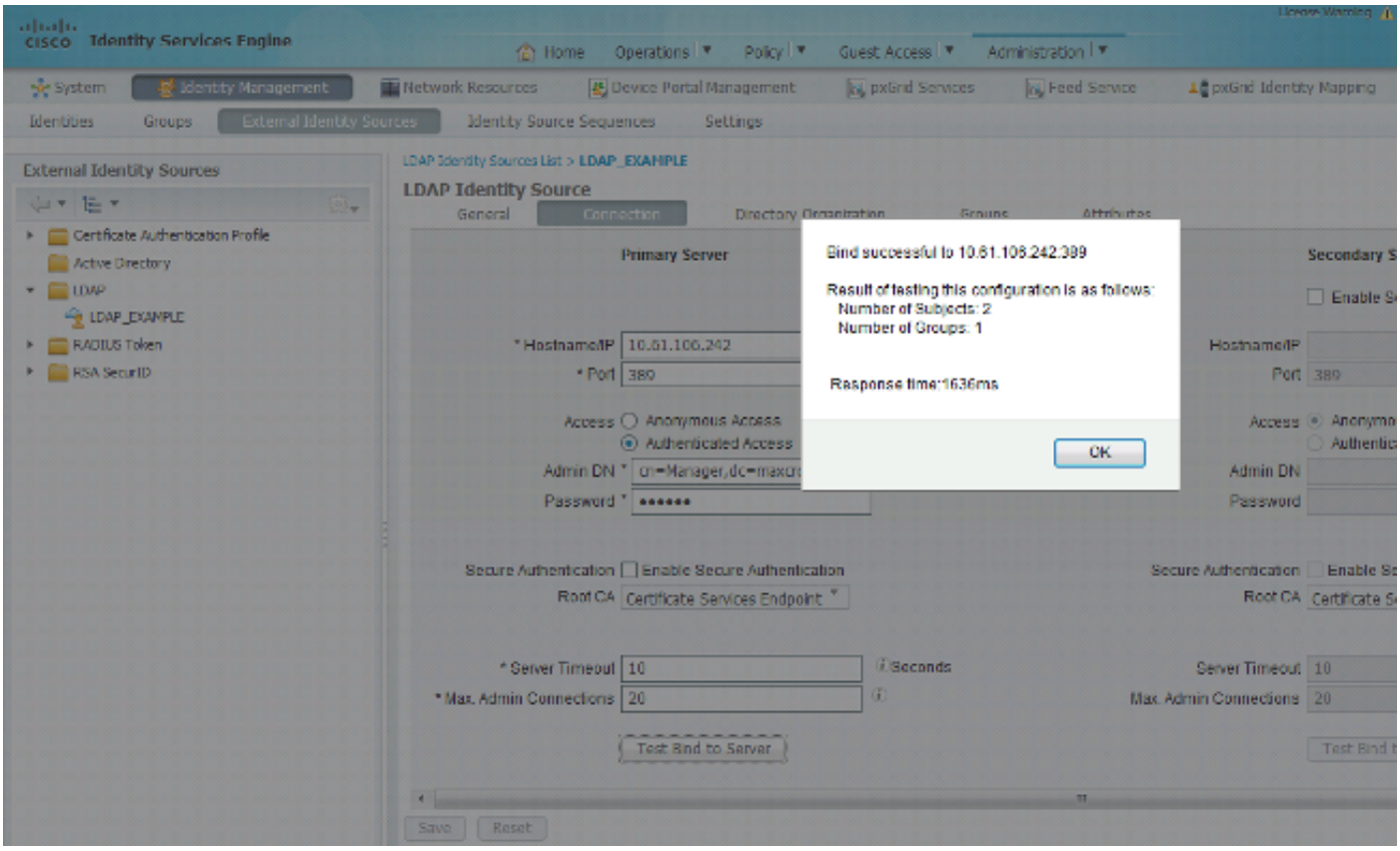


컨피그레이션을 적용한 후 네트워크에 연결할 수 있어야 합니다.

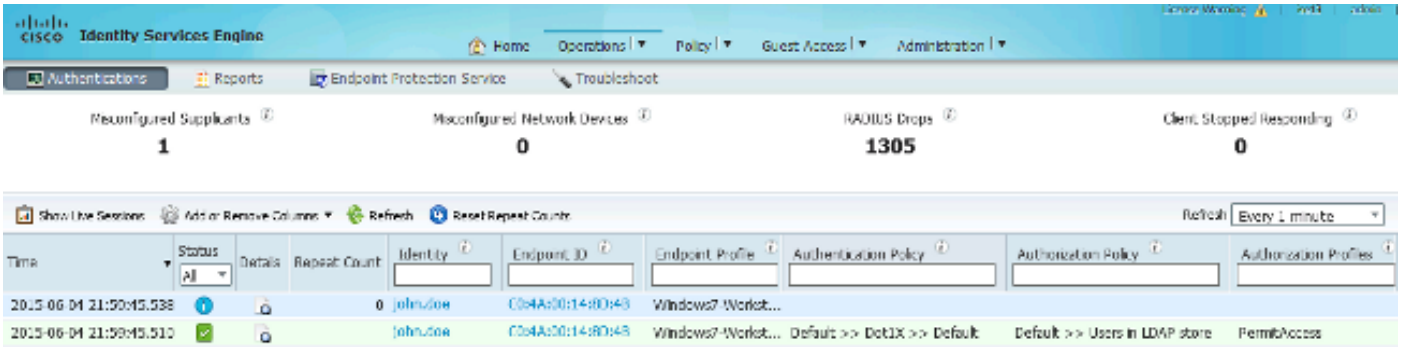


다음을 확인합니다.

LDAP 및 ISE 컨피그레이션을 확인하려면 서버에 대한 테스트 연결을 사용하여 주체 및 그룹을 검색합니다.



다음 이미지는 ISE의 샘플 보고서를 보여줍니다.



Authentication Details

Source Timestamp	2015-06-04 21:59:45.509
Received Timestamp	2015-06-04 21:59:45.51
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	john.doe
User Type	
Endpoint Id	C0:4A:00:14:8D:4B
Endpoint Profile	Windows7-Workstation
IP Address	
Authentication Identity Store	LDAP_EXAMPLE
Identity Group	Workstation
Audit Session Id	0a3e9465000010035570b956
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-GTC)
Service Type	Framed

AD ExternalGroups	cn=domainusers,ou=groups,dc=maxcrc,dc=com
IdentityDn	uid=john.doe,ou=people,dc=maxcrc,dc=com
RADIUS Username	john.doe

문제 해결

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

- OpenLDAP를 설치한 후 gssapi.dll이 없음을 나타내는 오류가 발생하면 Microsoft Windows를 다시 시작합니다.

- Cisco AnyConnect의 configuration.xml 파일을 직접 편집할 수 없습니다. 다른 위치에 새 컨피그레이션을 저장한 다음 이를 사용하여 이전 파일을 대체합니다.

- 인증 보고서에 다음과 같은 오류 메시지가 있습니다.

  <#root>

  Authentication method is not supported by any applicable identity store

  이 오류 메시지는 선택한 방법이 LDAP에서 지원되지 않음을 나타냅니다.

동일한 보고서의 인증 프로토콜에 지원되는 방법(EAP-GTC, EAP-TLS 또는 PEAP-TLS) 중 하나가 표시되는지 확인합니다.

- 인증 보고서에서 제목이 ID 저장소에 없음을 알게 되면 보고서의 사용자 이름이 LDAP 데이터베이스의 사용자에 대한 Subject Name 특성과 일치하지 않습니다.

이 시나리오에서 값은 이 특성에 대해 uid로 설정되었는데, 이는 ISE가 일치 항목을 찾으려고 할 때 LDAP 사용자의 uid 값을 살펴본다는 것을 의미합니다.

- 서버 테스트 바인딩 중에 제목 및 그룹이 올바르게 검색되지 않으면 검색 기준에 대한 구성이 올바르지 않습니다.

LDAP 계층 구조는 leaf-to-root 및 dc에서 지정해야 합니다(여러 단어로 구성될 수 있음).

팁: WLC측에서 EAP 인증 문제를 해결하려면 WLC(WLAN Controller)를 사용한 EAP 인증 컨피그레이션 예 Cisco 문서를 참조하십시오.

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.