ISE-Active Directory 그룹 맵을 기반으로 WLC를 사용하여 동적 VLAN 할당 구성

목차

소개

이 문서에서는 동적 VLAN 할당 개념에 대해 설명합니다.

사전 요구 사항

이 문서에서는 WLAN(무선 LAN) 클라이언트를 특정 VLAN에 동적으로 할당하기 위해 WLC(무선 LAN 컨트롤러) 및 ISE(Identity Services Engine) 서버를 구성하는 방법에 대해 설명합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC(Wireless LAN Controller) 및 LAP(Lightweight Access Point)에 대한 기본 지식
- ISE와 같은 AAA(Authentication, Authorization, and Accounting) 서버의 기능 지식
- 무선 네트워크 및 무선 보안 문제에 대한 철저한 지식
- 동적 VLAN 할당에 대한 기능적 및 구성 가능한 지식
- Microsoft Windows AD 서비스, 도메인 컨트롤러 및 DNS 개념에 대한 기본적인 이해
- CAPWAP(Control And Provisioning of Access Point Protocol)에 대한 기본적인 지식 보유

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 8.8.111.0을 실행하는 Cisco 5520 Series WLC
- Cisco 4800 Series AP
- 기본 Windows 서플리컨트 및 Anyconnect NAM
- Cisco Secure ISE 버전 2.3.0.298
- 도메인 컨트롤러로 구성된 Microsoft Windows 2016 Server
- 버전 15.2(4)E1을 실행하는 Cisco 3560-CX Series Switch

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

RADIUS 서버와의 동적 VLAN 할당

대부분의 WLAN 시스템에서 각 WLAN에는 SSID(Service Set Identifier)와 연결된 모든 클라이언트 또는 컨트롤러 용어의 WLAN에 적용되는 정적 정책이 있습니다. 이 방법은 강력하지만 클라이언트가 서로 다른 QoS 및 보안 정책을 상속하기 위해 서로 다른 SSID에 연결해야 하므로 한계가 있습니다.

Cisco WLAN 솔루션은 ID 네트워킹의 지원으로 이러한 제한을 해결합니다. 이렇게 하면 네트워크에서 단일 SSID를 알릴 수 있지만 특정 사용자가 사용자 자격 증명에 따라 서로 다른 QoS, VLAN 특성 및/또는 보안 정책을 상속할 수 있습니다.

동적 VLAN 할당은 사용자가 제공한 자격 증명을 기반으로 무선 사용자를 특정 VLAN에 배치하는 기능입니다. 특정 VLAN에 사용자를 할당하는 이 작업은 Cisco ISE와 같은 RADIUS 인증 서버에서 처리됩니다. 예를 들어, 무선 호스트가 캠퍼스 네트워크 내에서 이동할 때 동일한 VLAN에 유지되도록 하기 위해 이 기능을 사용할 수 있습니다.

Cisco ISE 서버는 내부 데이터베이스를 포함하는 여러 가능한 데이터베이스 중 하나에 대해 무선 사용자를 인증합니다. 예를 들면 다음과 같습니다.

- 내부 DB
- 액티브 디렉토리
- 일반 LDAP(Lightweight Directory Access Protocol)

- ODBC(Open Database Connectivity) 호환 관계형 데이터베이스
- Rivest, Shamir, and Adelman(RSA) SecurID 토큰 서버
- RADIUS 호환 토큰 서버

Cisco ISE 인증 프로토콜 및 지원되는 외부 ID 소스는 ISE 내부 및 외부 데이터베이스에서 지원하는 다양한 인증 프로토콜을 나열합니다.

이 문서에서는 Windows Active Directory 외부 데이터베이스를 사용하는 무선 사용자를 인증하는 데 중점을 둡니다.

인증에 성공한 후 ISE는 Windows 데이터베이스에서 해당 사용자의 그룹 정보를 검색하고 해당 사용자를 해당 권한 부여 프로파일에 연결합니다.

클라이언트가 컨트롤러에 등록된 LAP와의 연결을 시도할 때 LAP는 각 EAP 방법의 도움으로 사용자의 자격 증명을 WLC에 전달합니다.

WLC는 RADIUS 프로토콜을 사용하여(EAP 캡슐화) ISE에 이러한 자격 증명을 전송하고 ISE는 KERBEROS 프로토콜의 도움으로 검증을 위해 사용자의 자격 증명을 AD에 전달합니다.

AD는 사용자 자격 증명을 검증하고 인증에 성공하면 ISE에 알립니다.

인증이 성공하면 ISE 서버는 특정 IETF(Internet Engineering Task Force) 특성을 WLC에 전달합니다. 이러한 RADIUS 특성은 무선 클라이언트에 할당해야 하는 VLAN ID를 결정합니다. 클라이언트의 SSID(WLAN, WLC)는 사용자가 항상 미리 지정된 VLAN ID에 할당되므로 상관없습니다.

VLAN ID 할당에 사용되는 RADIUS 사용자 특성은 다음과 같습니다.

- IETF 64(터널 유형)—VLAN으로 설정
- IETF 65(터널 미디어 유형)—802로 설정
- IETF 81(터널 비공개 그룹 ID)—VLAN ID로 설정

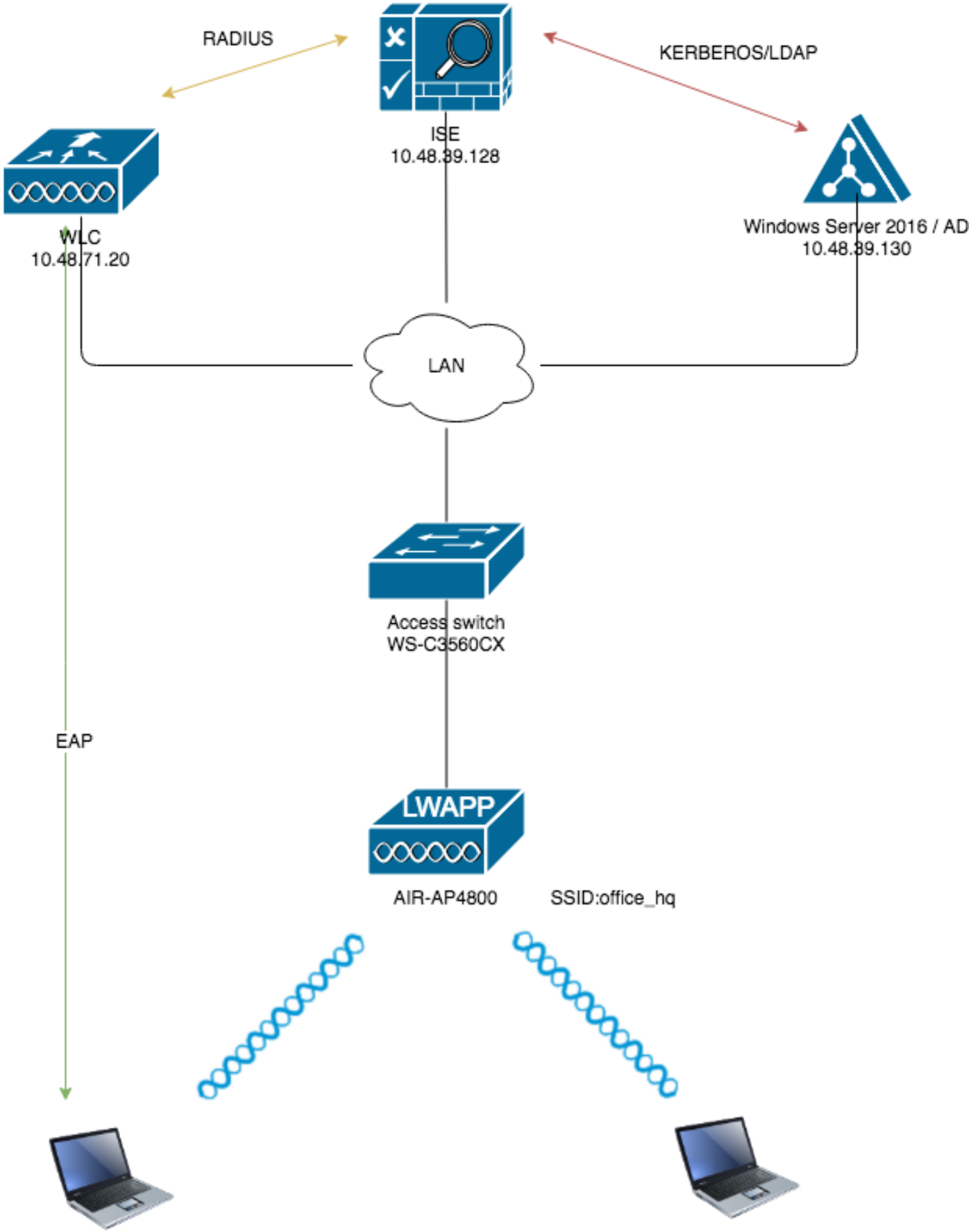
VLAN ID는 12비트이며 1에서 4094 사이의 값(포함)을 사용합니다. IEEE 802.1X에서 사용하는 RFC2868에 정의된 대로 Tunnel-Private- Group-ID는 문자열 유형이므로 VLAN ID 정수 값은 문자열로 인코딩됩니다. 이러한 터널 특성이 전송되면 Tag 필드를 입력해야 합니다.

RFC 2868, 섹션 3.1에 명시된 바와 같이: Tag 필드는 길이가 1 옥텟이며 동일한 터널을 참조하는 동일한 패킷에서 특성을 그룹화하는 수단을 제공하기 위한 것입니다. 이 필드에 유효한 값은 0x01~0x1F(포함)입니다. 태그 필드가 사용되지 않는 경우 0x00(영)이어야 합니다. 모든 RADIUS 특성에 대한 자세한 내용은 RFC 2868을 참조하십시오.

구성

이 섹션에서는 문서에서 설명된 기능을 구성하는 데 필요한 정보를 제공합니다.

네트워크 다이어그램

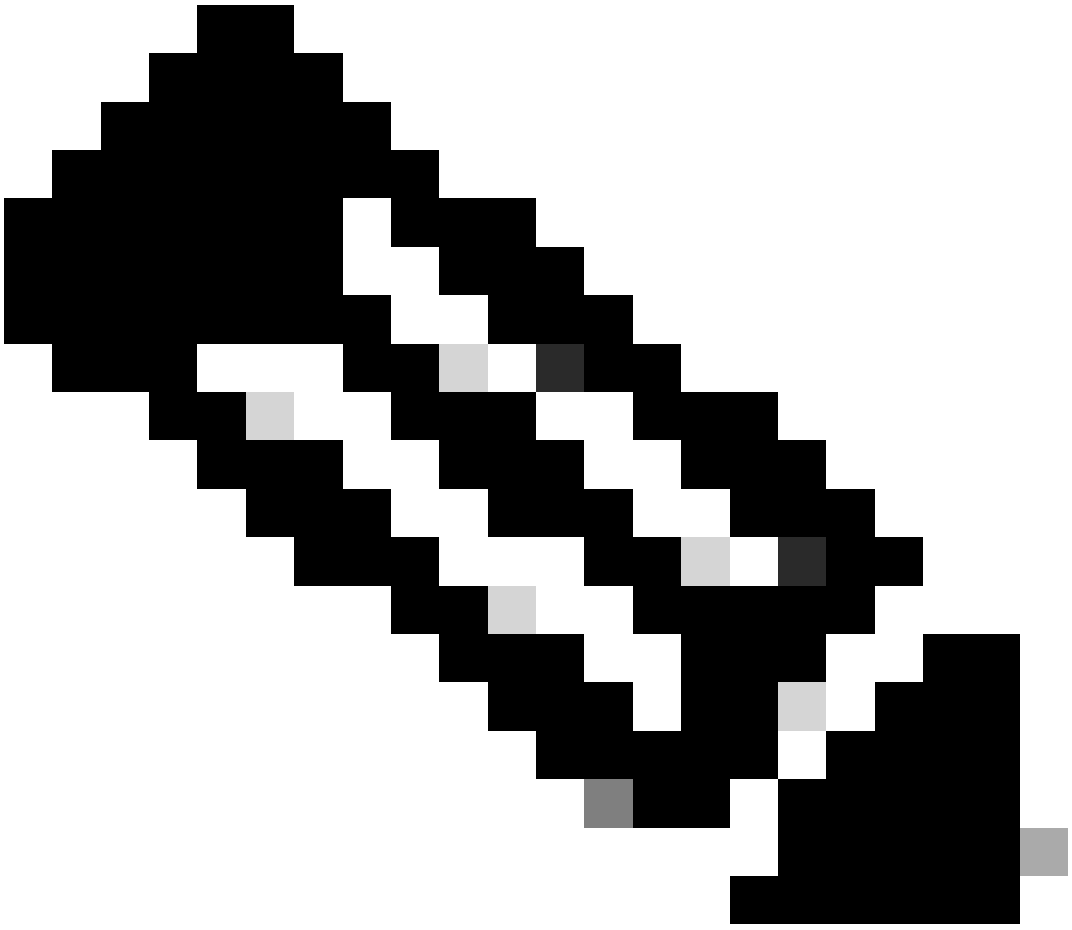


설정

다음은 이 다이어그램에서 사용되는 구성 요소의 컨피그레이션 세부 정보입니다.

- ISE(RADIUS) 서버의 IP 주소는 10.48.39.128입니다.
- WLC의 관리 및 AP 관리자 인터페이스 주소는 10.48.71.20입니다.
- DHCP 서버는 LAN 네트워크에 상주하며 각 클라이언트 풀에 대해 구성됩니다. 다이어그램에는 표시되지 않습니다.
- VLAN1477 및 VLAN1478은 이 컨피그레이션 전체에서 사용됩니다. 마케팅 부서의 사용자는 VLAN1477에, HR 부서 사용자는 RADIUS 서버에 의해 VLAN1478에 배치되도록 구성됩니다 두 사용자가 동일한 SSID에 연결하는 경우 — office_hq.

  VLAN1477: 192.168.77.0/24. 게이트웨이: 192.168.77.1 VLAN1478: 192.168.78.0/24. 게이트웨이: 192.168.78.1
- 이 문서에서는 802.1x를 보안 메커니즘으로PEAP-mschapv2사용합니다.



참고: WLAN을 보호하기 위해 EAP-FAST 및 EAP-TLS 인증과 같은 고급 인증 방법을 사용하는 것이 좋습니다.

이러한 가정은 이 컨피그레이션을 수행하기 전에 수행됩니다.

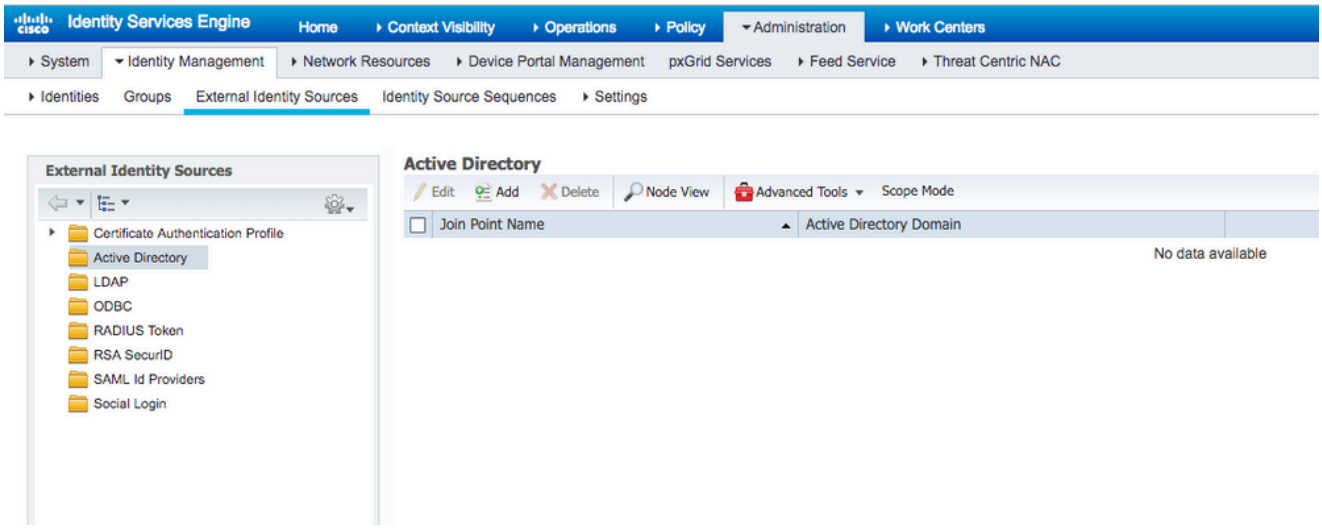
- LAP가 WLC에 이미 등록되어 있습니다.
- DHCP 서버에는 DHCP 범위가 할당됩니다
- 네트워크의 모든 디바이스 간에 레이어 3 연결이 존재합니다.
- 이 문서에서는 무선 측에 필요한 컨피그레이션에 대해 설명하고 유선 네트워크가 있는 것으로 가정합니다
- 각 사용자 및 그룹이 AD에 구성됨

ISE 대 AD 그룹 매핑을 기반으로 WLC를 사용하여 동적 VLAN 할당을 수행하려면 다음 단계를 수행해야 합니다.

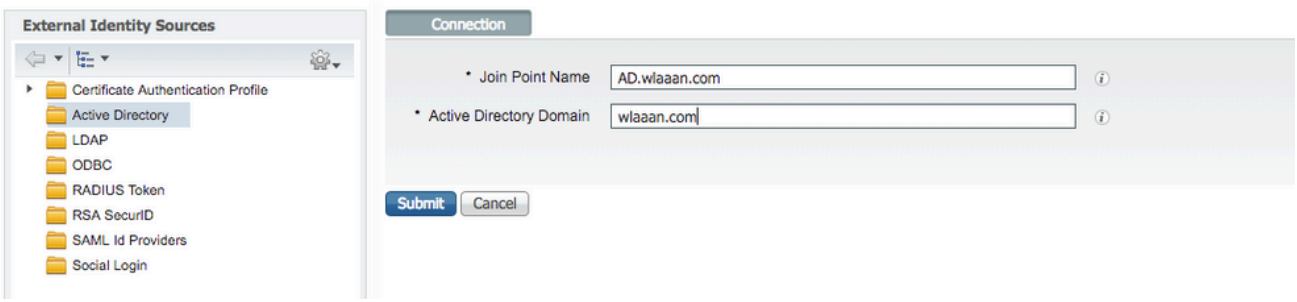
1. ISE에서 ISE의 사용자에 대한 인증 및 권한 부여 정책의 AD 통합 및 컨피그레이션으로의 ISE
2. SSID 'office_hq'에 대한 dot1x 인증 및 AAA 재정의를 지원하기 위한 WLC 컨피그레이션.
3. 최종 클라이언트 신청자 컨피그레이션입니다.

ISE에서 ISE의 사용자를 위한 AD 통합 및 인증 및 권한 부여 정책 구성

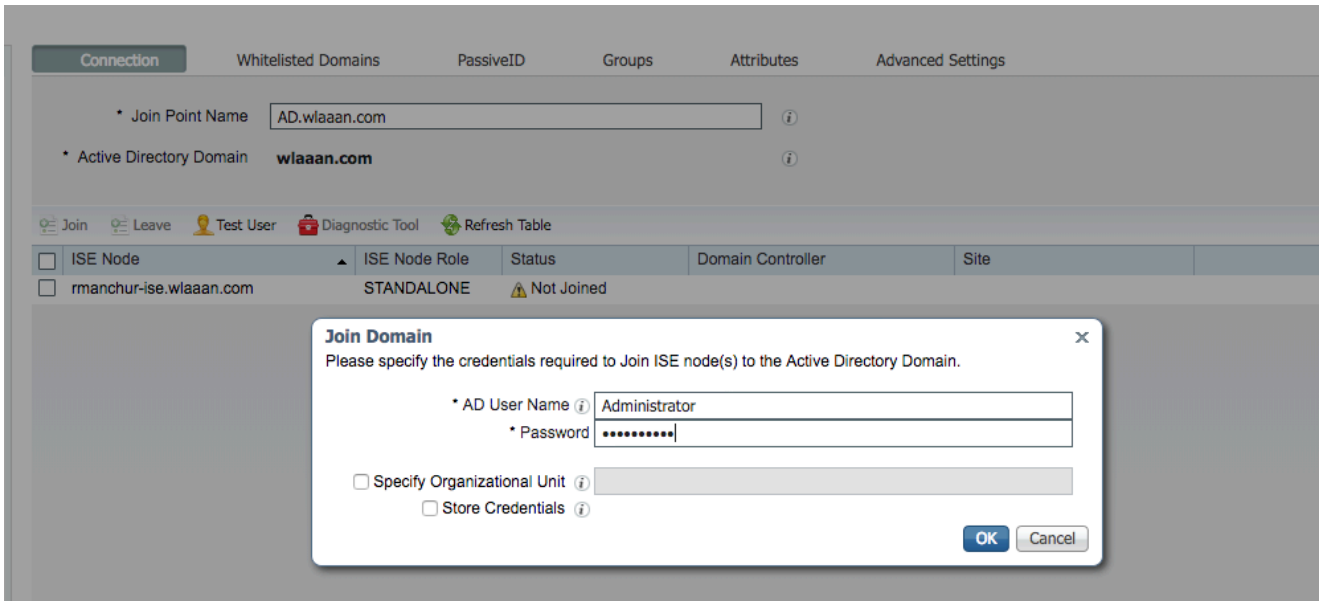
1. 관리자 계정을 사용하여 ISE 웹 UI 인터페이스에 로그인합니다.
2. 로Administration > Identity management > External Identity Sources > Active directory이동합니다.



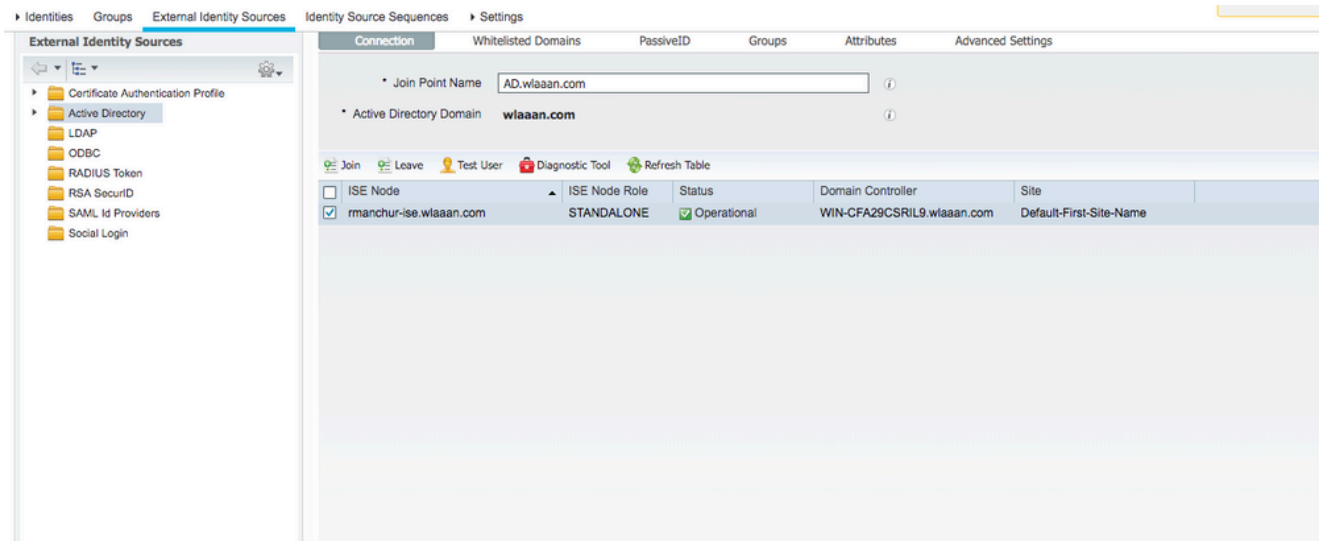
3. Add(추가)를 클릭하고 Active Directory Join Point Name(Active Directory 가입 포인트 이름) 설정에서 도메인 이름과 ID 저장소 이름을 입력합니다. 이 예에서 ISE는 도메인에 등록되며 wlaaan.comjoinpoint는 ISE에 로컬로 중요한AD.wlaaan.com이름으로 지정됩니다.



4. ISE를 AD에 즉시 조인할지Submit묻는 버튼을 누르면 팝업 창이 열립니다. 을Yes누르고 Active Directory 사용자 자격 증명에 관리자 권한을 제공하여 도메인에 새 호스트를 추가합니다.



5. 이 시점 이후에는 ISE가 AD에 성공적으로 등록되어야 합니다.



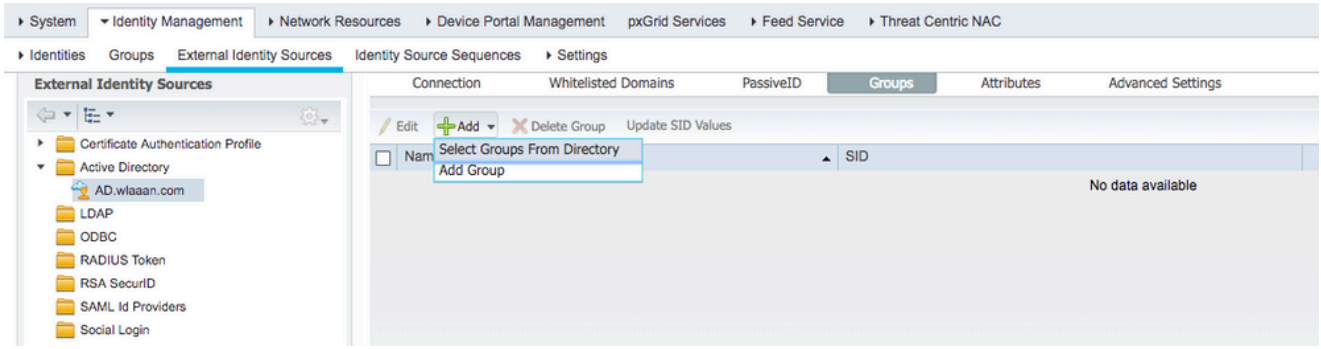
등록 프로세스에 문제가 있는 경우 를 사용하여 AD 연결Diagnostic Tool 에 필요한 테스트를 실행할 수 있습니다.

6. 각 권한 부여 프로파일을 할당하기 위해 사용 되는 활성 디렉토리의 그룹을 검색 해야 합니다.

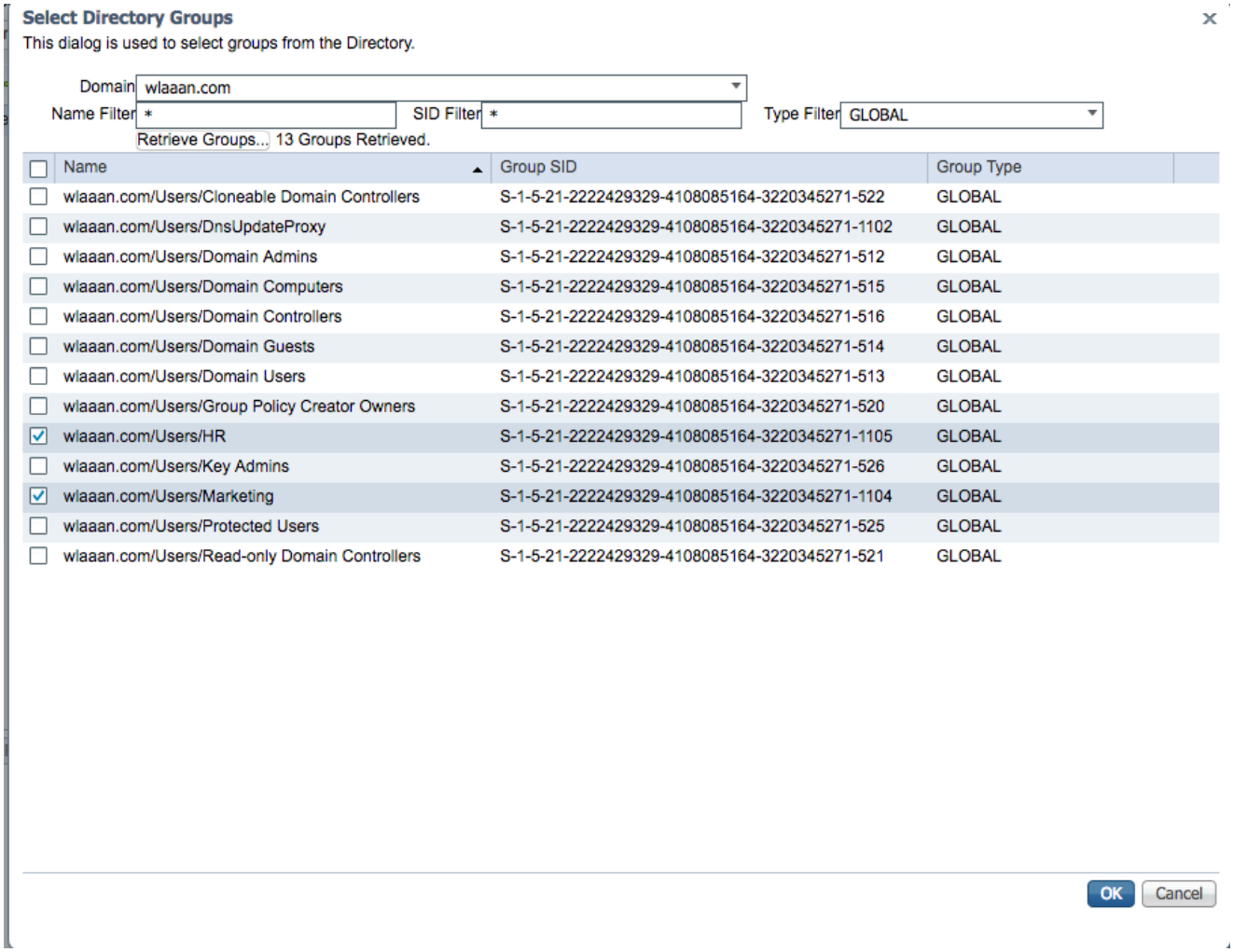
로 이동한Administration > Identity management > External Identity Sources > Active directory >

> Groups

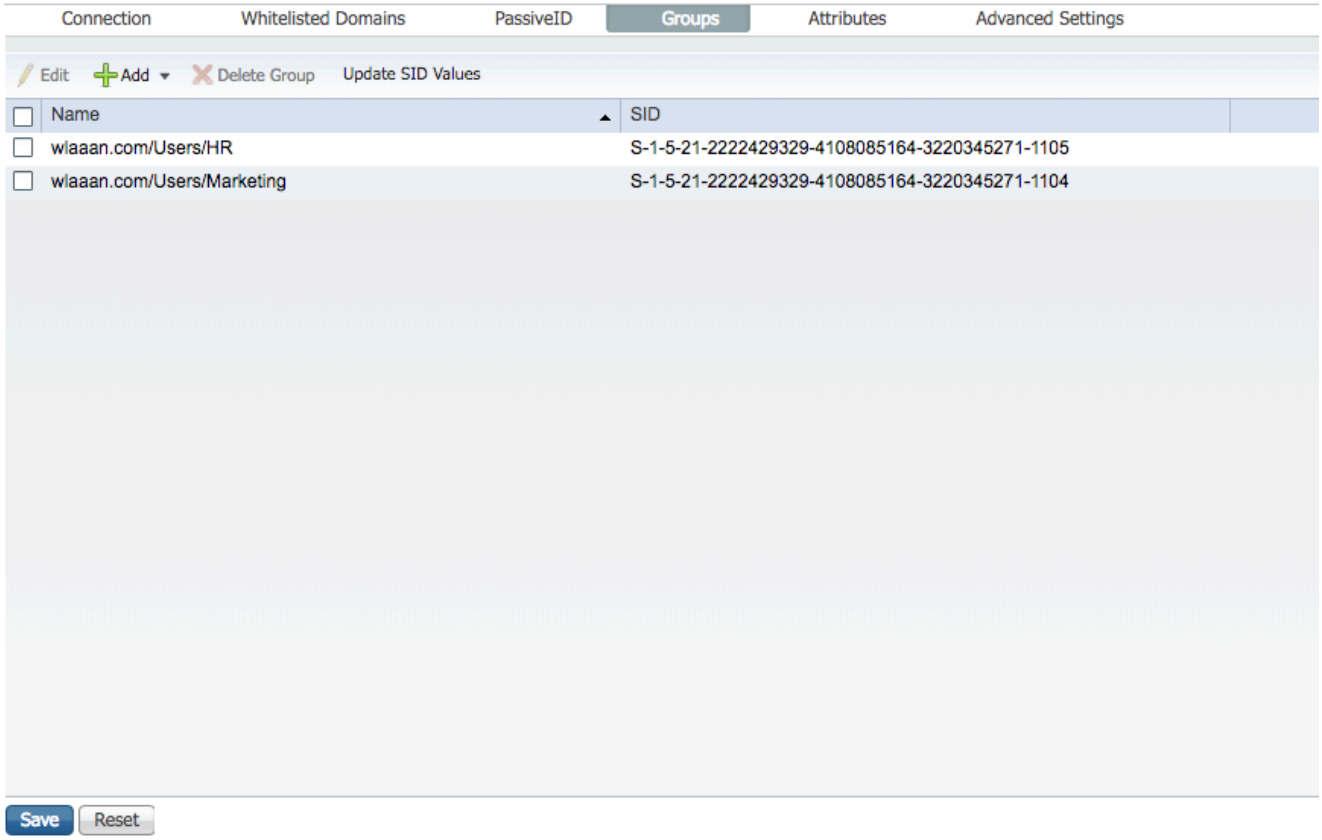
다음 을 클릭하고Add선택합니다Select Groups from Active Directory.



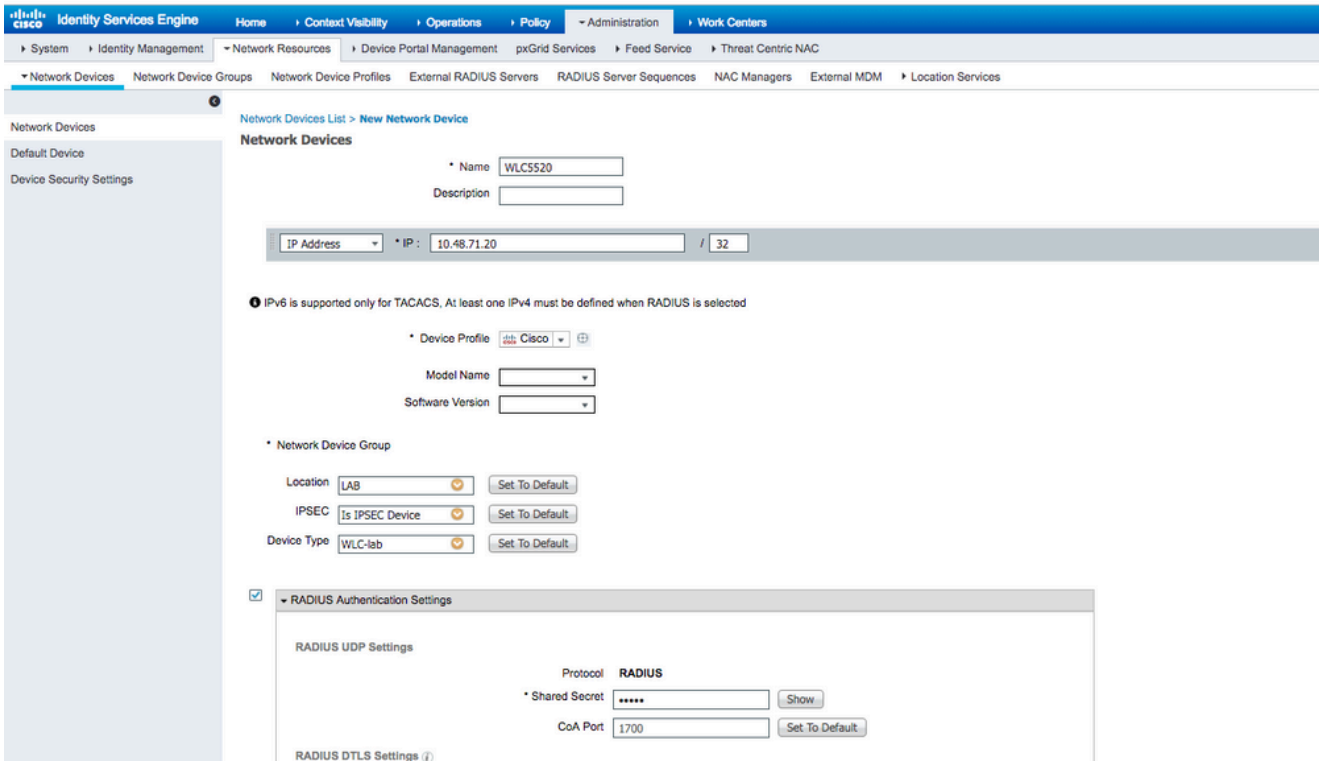
7. 특정 그룹을 검색하기 위해 필터를 지정하거나 AD에서 모든 그룹을 검색할 수 있는 새 팝업 창이 열립니다.
   AD 그룹 목록에서 해당 그룹을 선택하고 키를OK누릅니다.



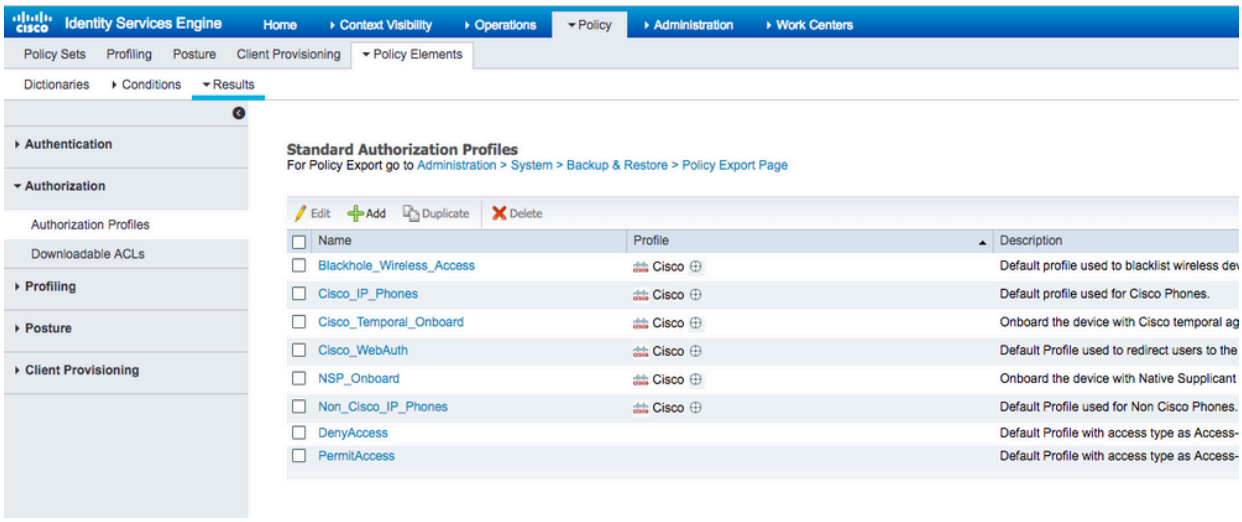
8. 각 그룹이 ISE에 추가되고 저장될 수 있습니다. 을 누릅니다Save.



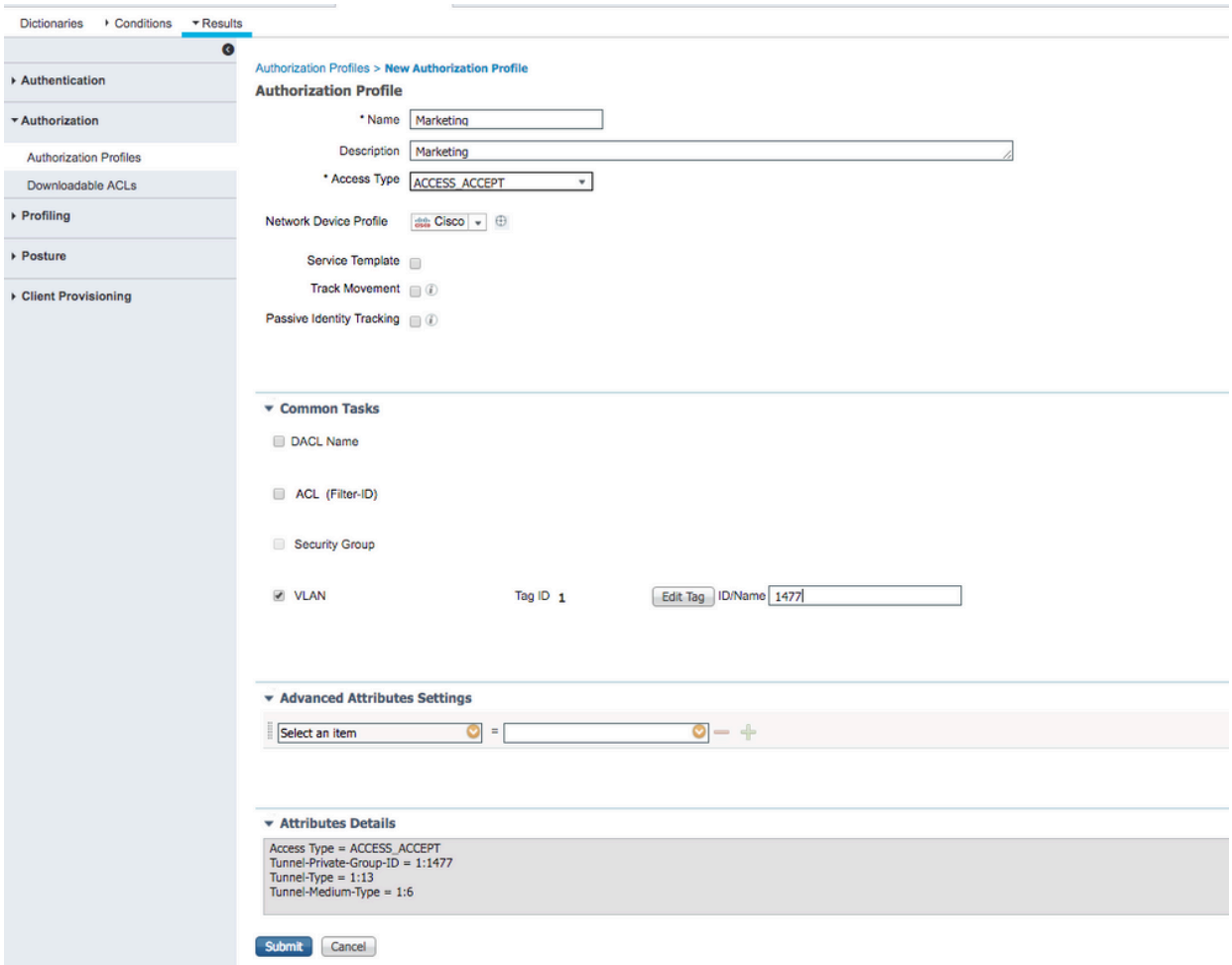
9. ISE 네트워크 디바이스 목록에 WLC 추가 - 로 이동하고Administration > Network Resources > Network Devices키를Add누릅니다.
   WLC와 ISE 간에 WLC 관리 IP 주소 및 RADIUS 공유 암호를 제공하여 완전한 컨피그레이션을 수행합니다.



10. 이제 ISE를 AD에 가입하고 WLC를 디바이스 목록에 추가한 후 사용자에 대한 인증 및 권한 부여 정책의 컨피그레이션을 시작할 수 있습니다.
    - Marketing에서 VLAN1477로 그리고 HR 그룹에서 VLAN1478로 사용자를 할당하기 위해 권한 부여 프로파일을 생성합니다.
      새 프로파일을 생성하려면Policy > Policy Elements > Results > Authorization > Authorization profiles로Add이동하여 버튼을 클릭합니다.

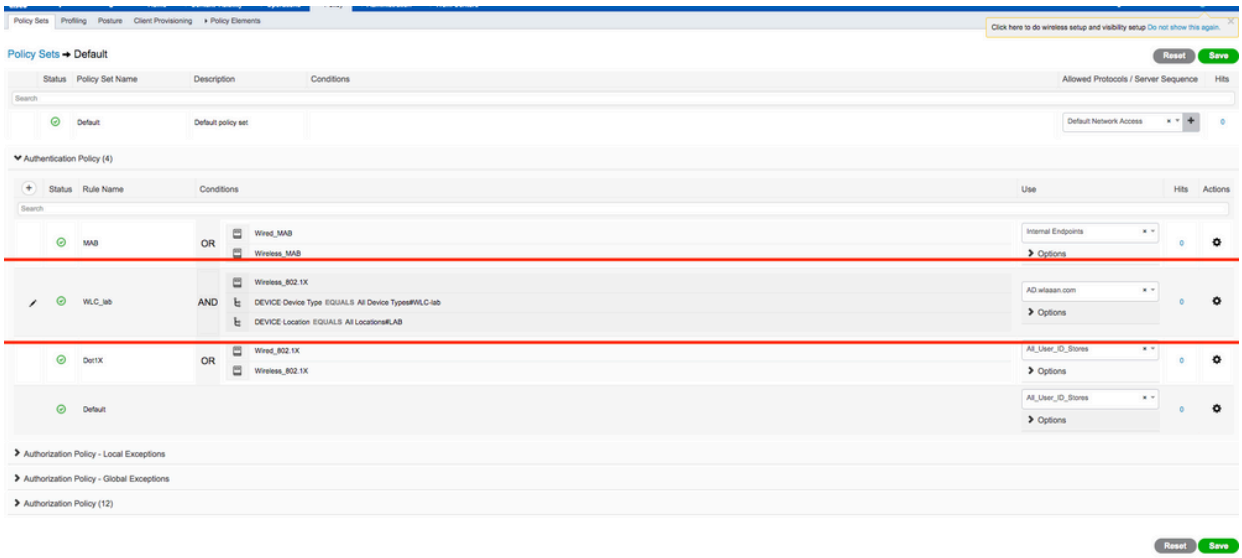


    - 각 그룹에 대한 VLAN 정보가 포함된 권한 부여 프로파일 컨피그레이션을 완료합니다.
      예는 그룹 컨피그레이션 설정을Marketing보여줍니다.

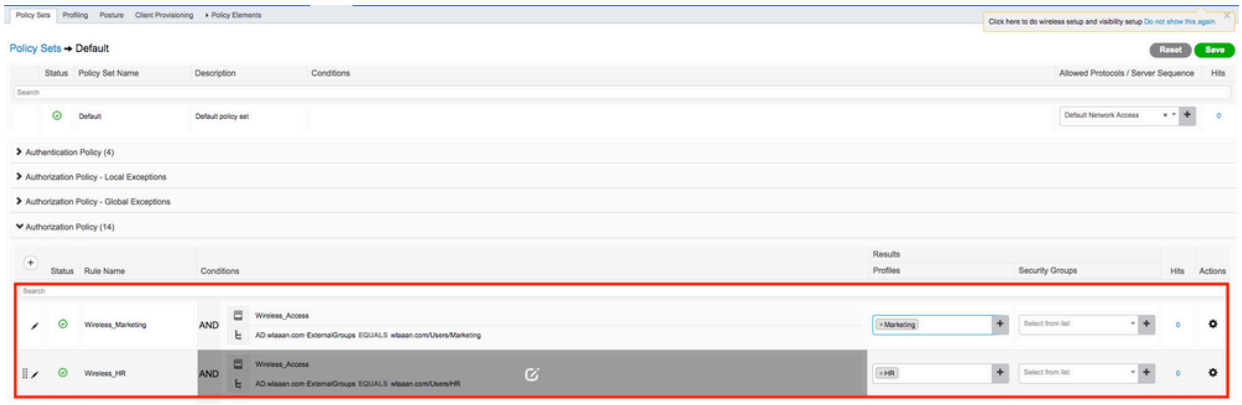


다른 그룹에 대해서도 유사한 컨피그레이션을 수행해야 하며 각 VLAN 태그 특성을 구성해야 합니다.

- 권한 부여 프로파일을 구성한 후 무선 사용자에 대한 인증 정책을 정의할 수 있습니다. 이 작업은 정책 집합을 구성하거나Custom수정하여 수행할 수Default있습니다. 이 예에서는 Default 정책 집합이 수정됩니다. 로Policy > Policy Sets > Default이동합니다. 인증 유형의dot1x경우 기본적으로 ISE는 현재 기본 설정에서도 작동하지만 AD는 의 ID 소스 목록의 일부이므로All_User_ID_StoresAll_User_ID_Stores이 예에서 해당 LAB 컨트롤러에 대해 더 구체적인 규칙WLC_lab을 사용하며 AD를 유일한 인증 소스로 사용합니다.

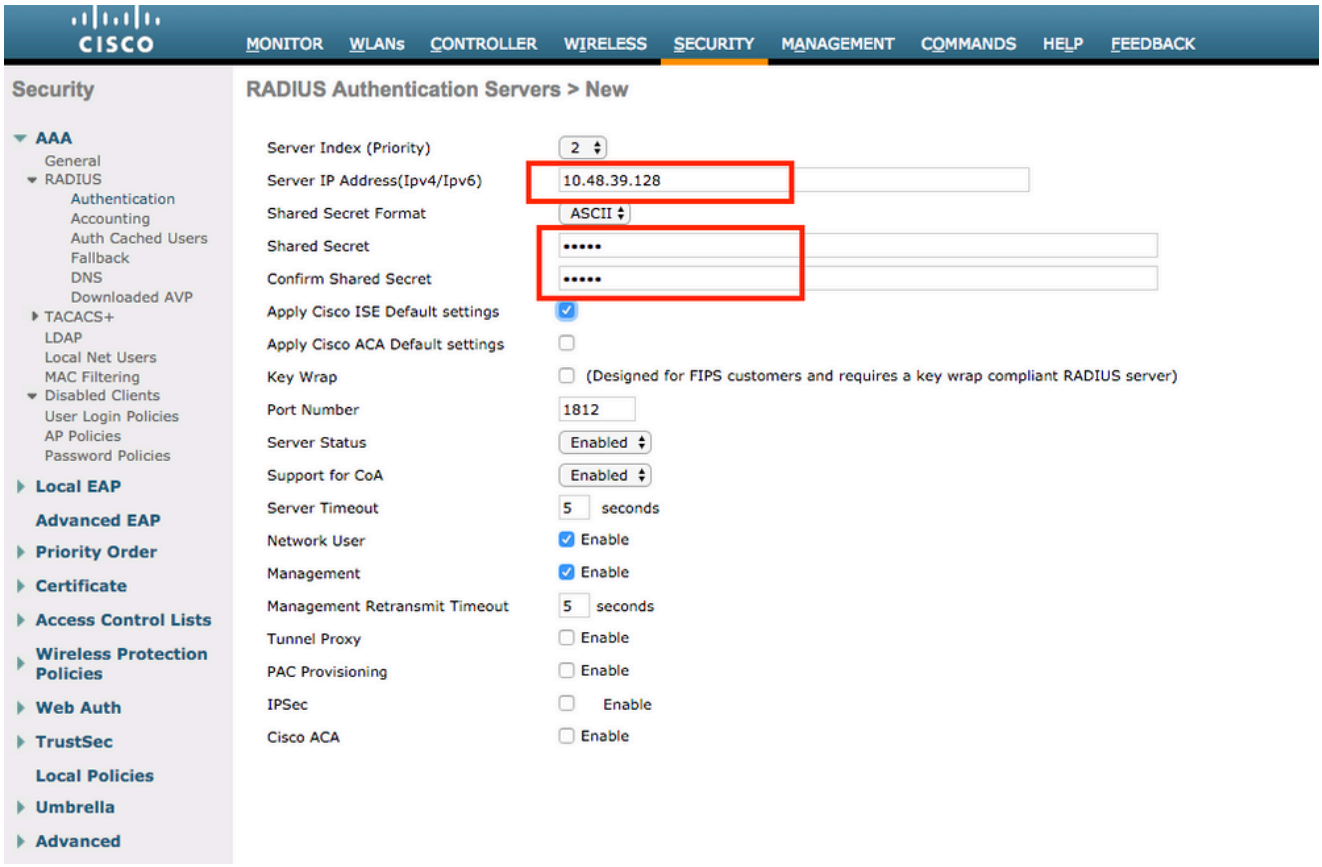


- 이제 그룹 멤버십을 기반으로 개별 권한 부여 프로파일을 할당하는 사용자에 대한 권한 부여 정책을 생성해야 합니다. 해당 요건을Authorization policy달성하기 위해 섹션으로 이동하여 정책을 생성합니다.

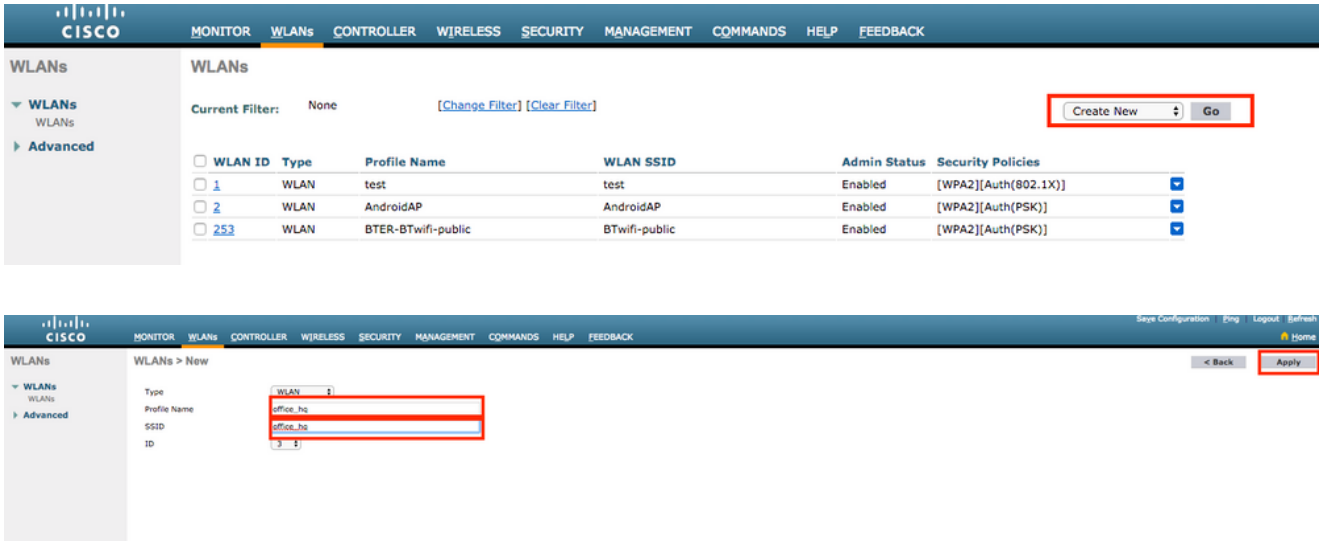


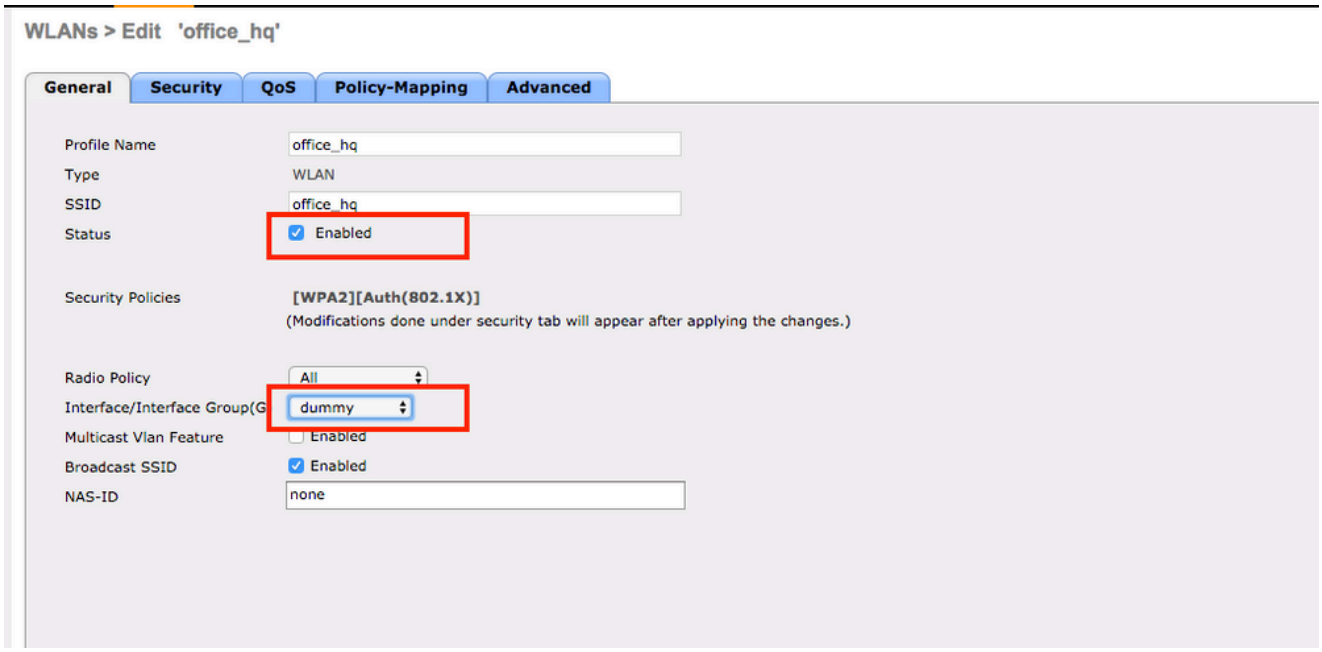
SSID 'office_hq'에 대한 dot1x 인증 및 AAA 재정의를 지원하는 WLC 구성

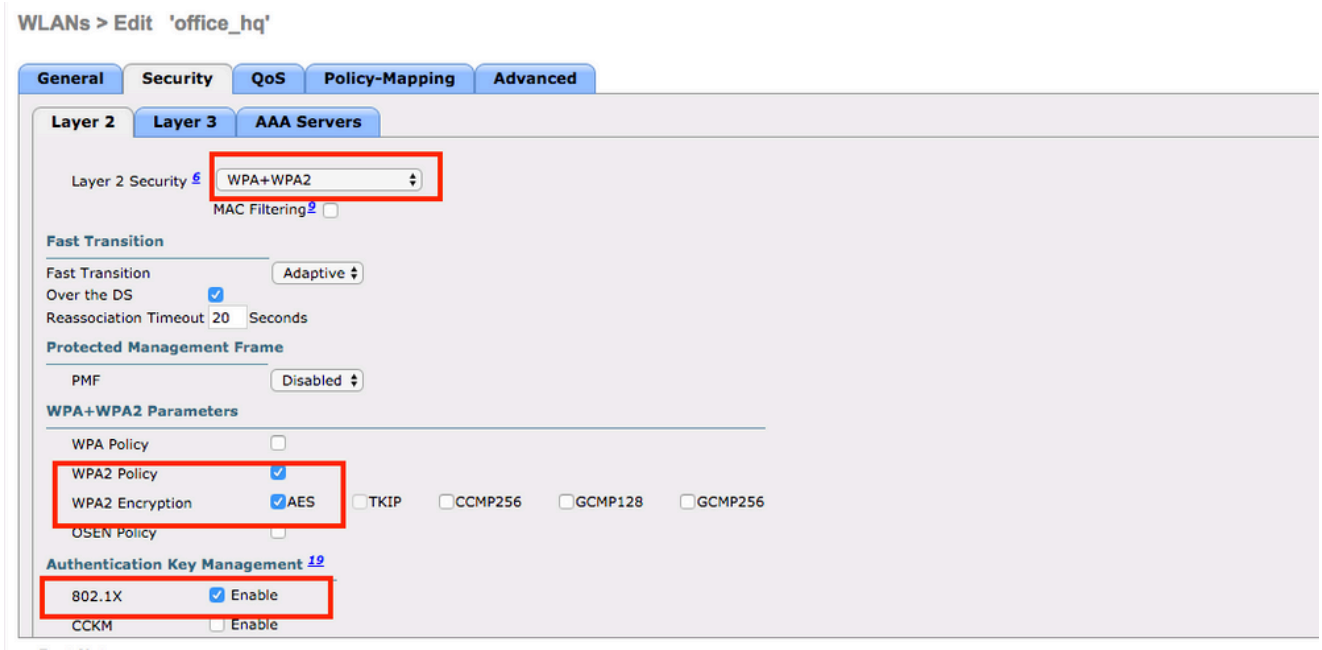
1. ISE를 WLC에서 RADIUS 인증 서버로 구성합니다. 웹 UISecurity > AAA > RADIUS > Authentication인터페이스의 섹션으로 이동하여 ISE IP 주소 및 공유 암호 정보를 제공합니다.

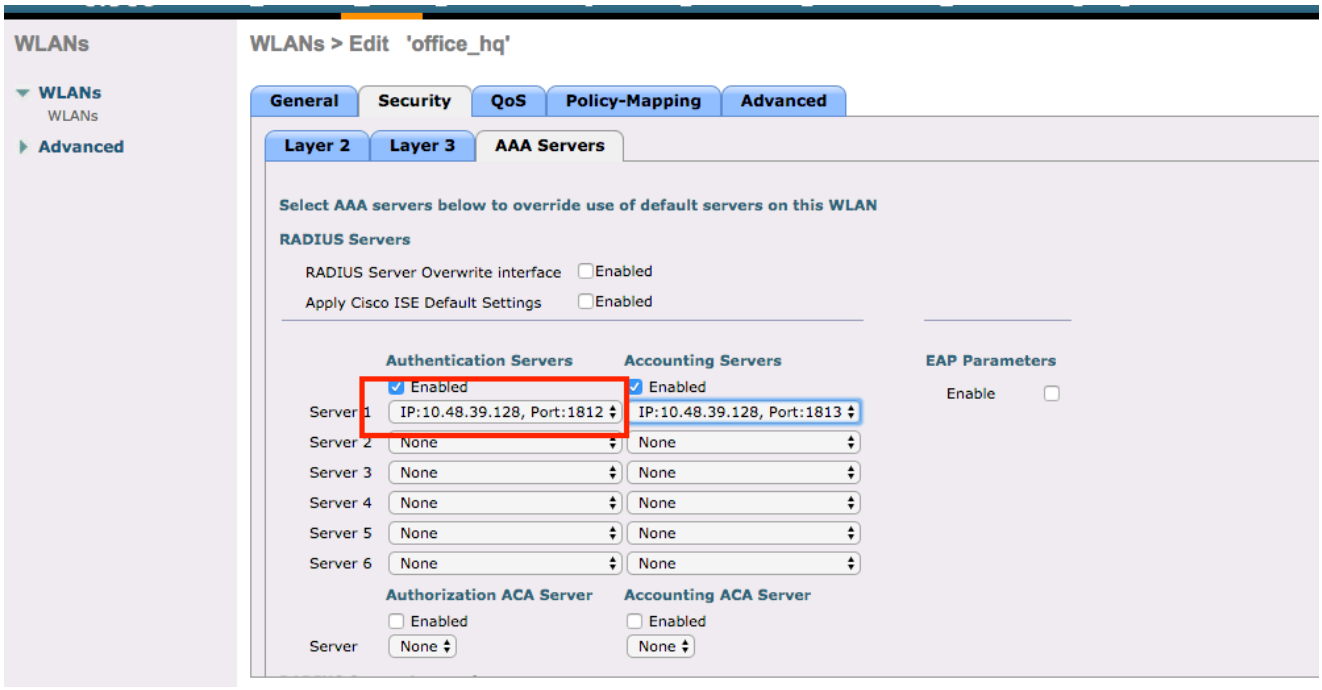


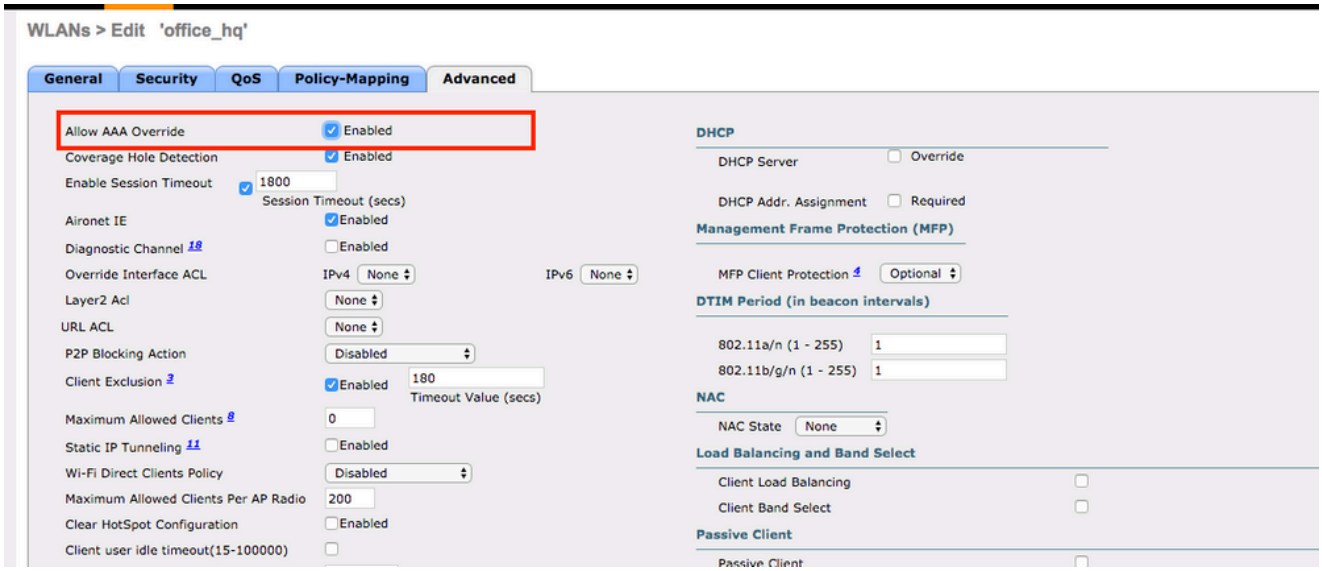
2. WLC의 섹션office_hq아래에WLANsSSID를 구성합니다. 이 예에서는 및 AAA 재정의를 WPA2/AES+dot1x사용하여 SSID를 구성합니다. 인터페이스Dummy는 RADIUS를 통해 적절한 VLAN이 할당되므로 WLAN에 대해 선택됩니다. 이 더미 인터페이스는 WLC에서 생성하고 IP 주소를 지정해야 하지만, IP 주소가 유효하지 않아도 되며, VLAN이 배치된 VLAN을 업링크 스위치에서 생성할 수 없으므로 VLAN이 할당되지 않을 경우 클라이언트가 아무 곳으로도 이동할 수 없습니다.



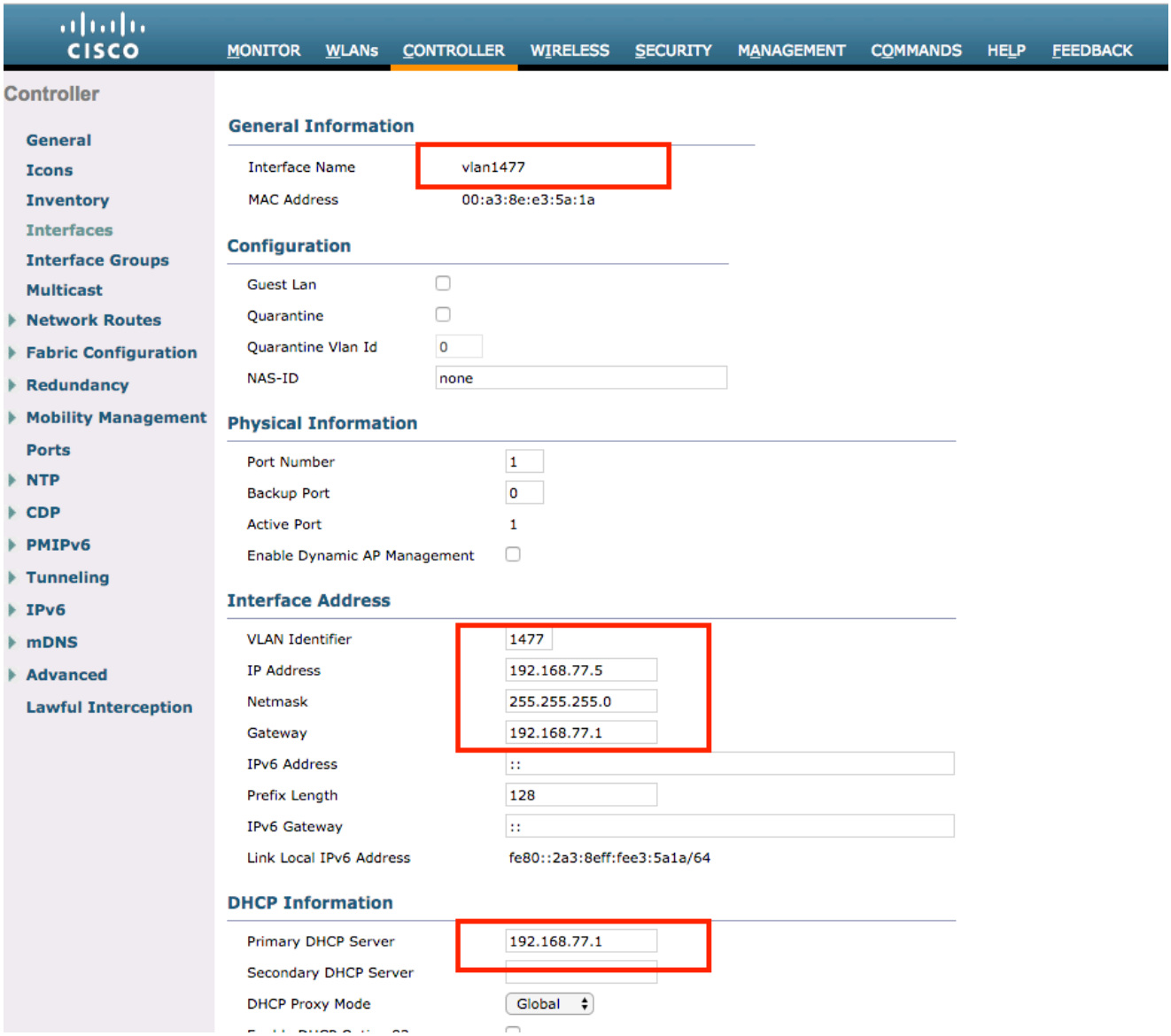

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable





3. 또한 사용자 VLAN에 대한 WLC에서 동적 인터페이스를 생성해야 합니다. UI 메뉴로Controller > Interfaces이동합니다. WLC는 해당 VLAN에 동적 인터페이스가 있는 경우에만 AAA를 통해 수신된 VLAN 할당을 승인할 수 있습니다.



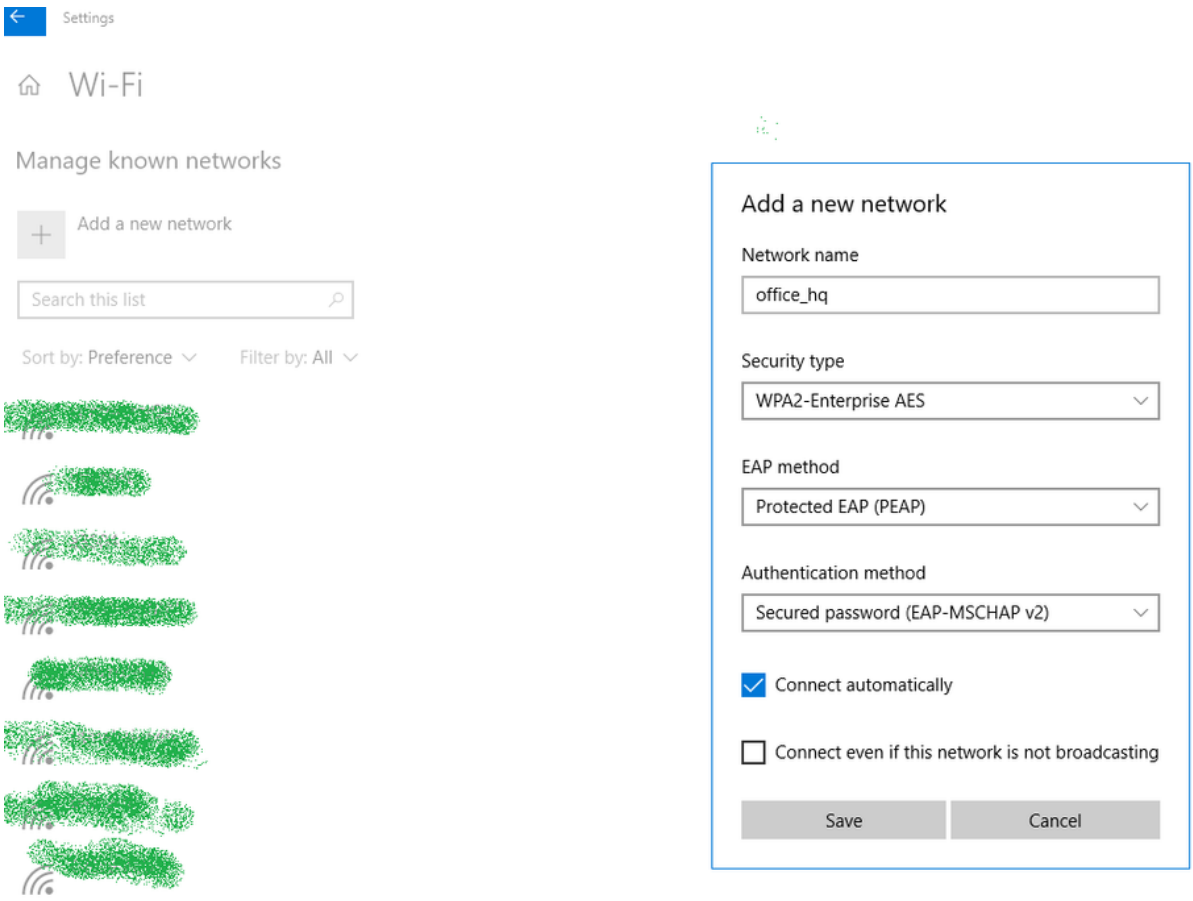
다음을 확인합니다.

연결을 테스트하려면 Windows 10 기본 신청자 및 Anyconnect NAM을 사용합니다.

EAP-PEAP 인증을 사용 중이고 ISE가 SSC(Self-Signed Certificate)를 사용 중이므로 인증서 경고에 동의하거나 인증서 검증을 비활성화해야 합니다. 기업 환경에서는 ISE에서 서명되고 신뢰할 수 있는 인증서를 사용하고 최종 사용자 디바이스에 신뢰할 수 있는 CA 목록 아래에 적절한 루트 인증서가 설치되어 있는지 확인해야 합니다.

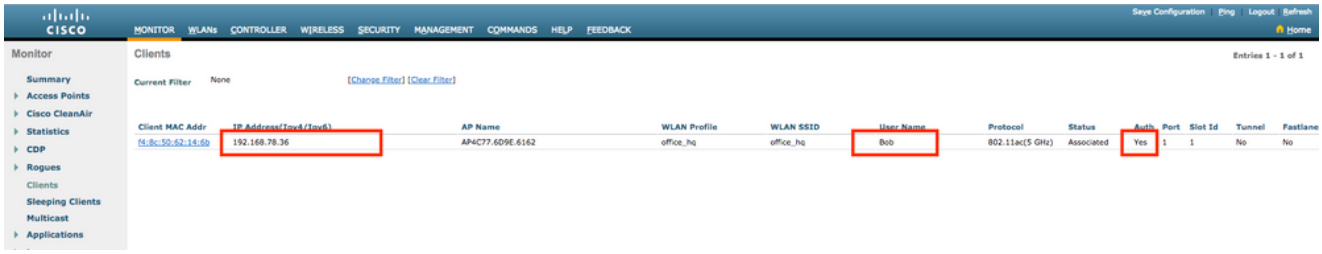
Windows 10 및 기본 신청자와의 연결 테스트:

1. 버튼Network & Internet settings > Wi-Fi > Manage known networks을 눌러 새 네트워크 프로파일을 열고 생성합니다.Add new network필요한 정보를 입력합니다.



2. ISE의 인증 로그를 확인하고 사용자에 대해 올바른 프로파일이 선택되었는지 확인합니다.

3. WLC에서 클라이언트 항목을 확인하고 올바른 VLAN에 할당되었으며 RUN 상태에 있는지 확인합니다.



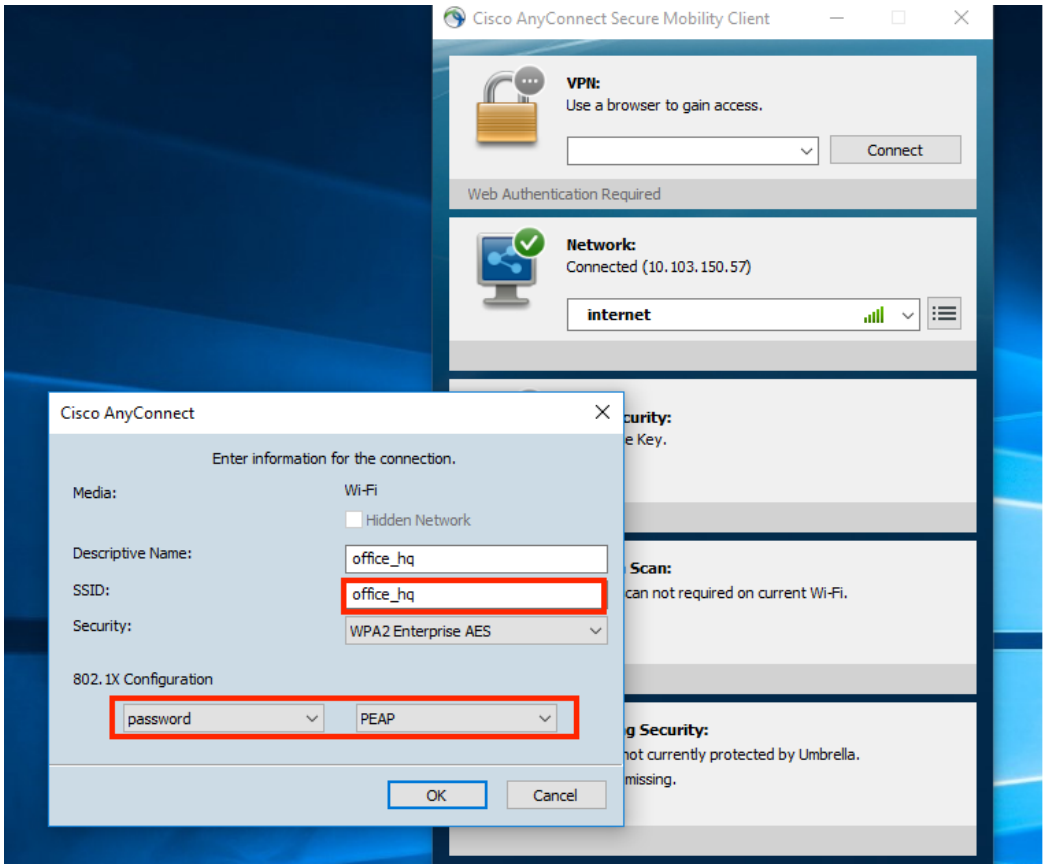
4. WLC CLI에서는show client dertails
를 사용하여 클라이언트 상태를 확인할 수 있습니다.

```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Bob
Client Webauth Username ........................ N/A
```

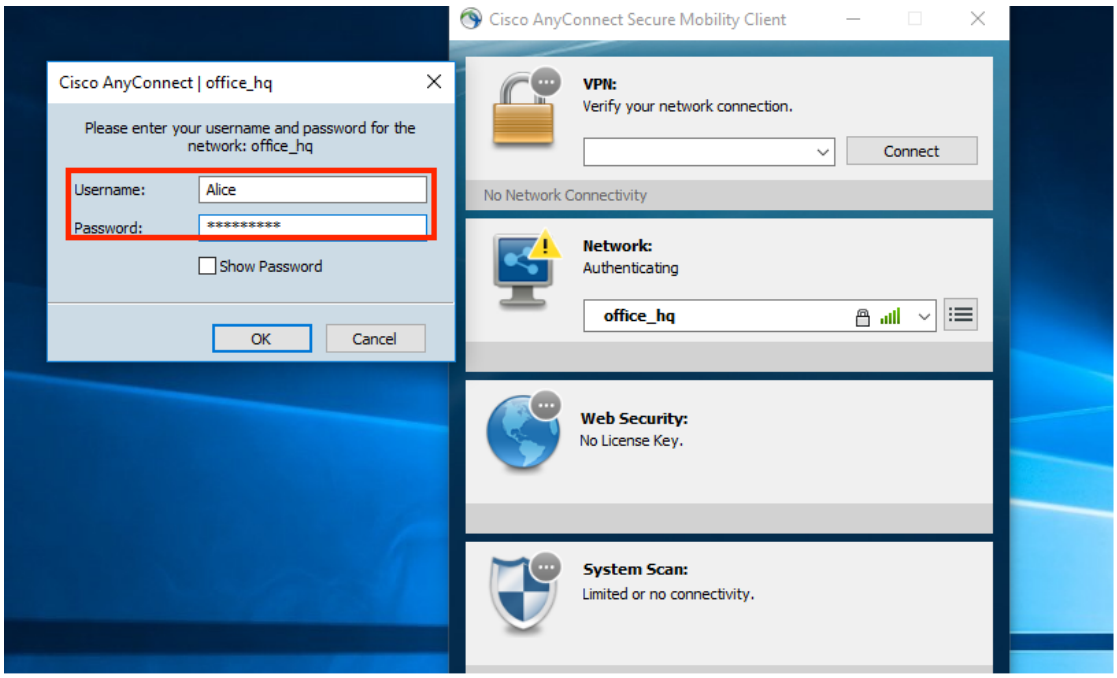
```
Hostname: .....
Device Type: ..................................... Intel-Device
AP MAC Address.................................... 70:69:5a:51:4e:c0
AP Name........................................... AP4C77.6D9E.6162
AP radio slot Id.................................. 1
Client State...................................... Associated
User Authenticated by ............................ RADIUS Server
Client User Group................................. Bob
Client NAC OOB State.............................. Access
Wireless LAN Id................................... 3
Wireless LAN Network Name (SSID).................. office_hq
Wireless LAN Profile Name......................... office_hq
Hotspot (802.11u)................................. Not Supported
Connected For .................................... 242 secs
BSSID............................................. 70:69:5a:51:4e:cd
Channel........................................... 36
IP Address........................................ 192.168.78.36
Gateway Address................................... 192.168.78.1
Netmask........................................... 255.255.255.0
...
Policy Manager State.............................. RUN
...
EAP Type.......................................... PEAP
Interface......................................... vlan1478
VLAN.............................................. 1478
Quarantine VLAN................................... 0
Access VLAN....................................... 1478
```

Windows 10 및 Anyconnect NAM과의 연결 테스트:

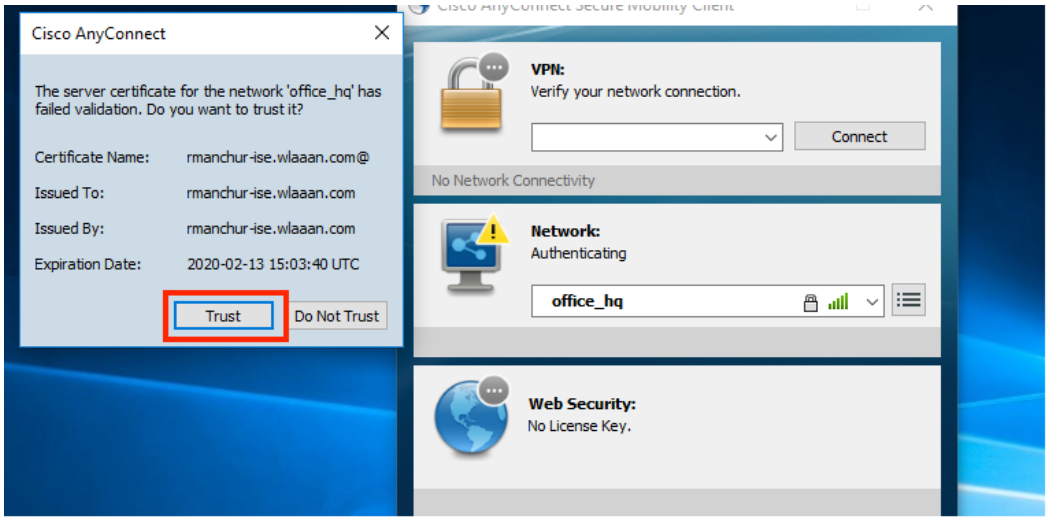
1. 사용 가능한 SSID 목록 및 해당 EAP 인증 유형(이 예에서는 PEAP) 및 내부 인증 양식에서 SSID를 선택합니다.



2. 사용자 인증을 위한 사용자 이름 및 비밀번호를 제공합니다.

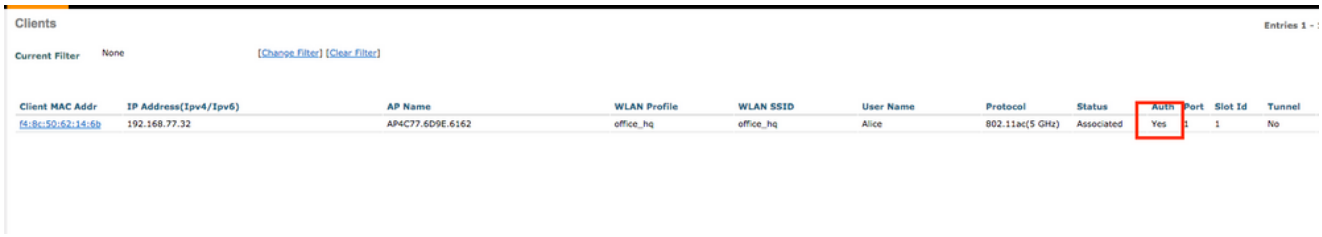


3. ISE가 SSC를 클라이언트에 전송하므로 인증서를 신뢰하도록 수동으로 선택해야 합니다(프로덕션 환경에서는 ISE에 신뢰받는 인증서를 설치하는 것이 매우 권장됨).



4. ISE의 인증 로그를 확인하고 사용자에 대해 올바른 권한 부여 프로파일이 선택되었는지 확인합니다.

5. WLC에서 클라이언트 항목을 확인하고 올바른 VLAN에 할당되었으며 RUN 상태에 있는지 확인합니다.



6. WLC CLI에서는show client dertails
를 사용하여 클라이언트 상태를 확인할 수 있습니다.

```
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Alice
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
```

```
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Alice
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 765 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.77.32
Gateway Address.................................. 192.168.77.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP-128 (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ vlan1477
VLAN............................................. 1477
```

문제 해결

1. WLC test aaa radius username

   password

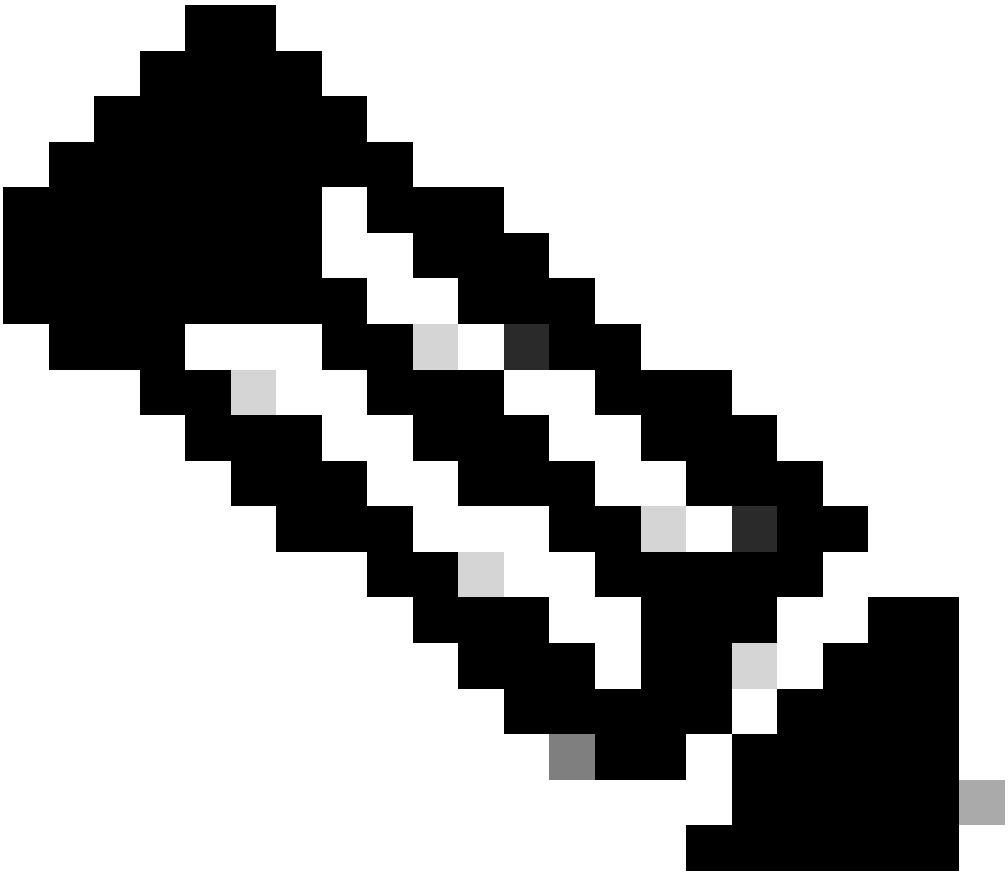
   wlan-id

   와 ISE 간의 RADIUS 연결을 테스트하려면 를 사용하고 결과를 test aaa show radius 표시하려면 를 사용합니다.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none

  Attributes                  Values
  ----------                  ------
  User-Name                   Alice
  Called-Station-Id           00-00-00-00-00-00:AndroidAP
  Calling-Station-Id          00-11-22-33-44-55
  Nas-Port                    0x00000001 (1)
```

```
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743


test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x000005c5 (1477)


(Cisco Controller) >
```

2. 무선 클라이언트 연결 문제를 해결하려면debug client
   를 사용합니다.
3. WLC에서debug aaa all enable인증 및 권한 부여 문제를 트러블슈팅하려면 를 사용합니다.



참고: 디버깅이 수행되는 MAC 주소에debug mac addr따라 출력을 제한하려면 이 명령을 와 함께만 사용하십시오.

4. 인증 실패 및 AD 통신 문제를 파악하려면 ISE 라이브 로그 및 세션 로그를 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.