Identity Services Engine을 사용하는 무선 BYOD

목차

소개

Cisco ISE(Identity Services Engine)는 Cisco TrustSec 솔루션에 인증 및 권한 부여 인프라를 제공하는 Cisco의 차세대 정책 서버입니다. 또한 다음과 같은 두 가지 중요한 서비스도 제공합니다.

- 첫 번째 서비스는 Cisco ISE가 다양한 정보 소스에서 수신하는 특성을 기반으로 엔드포인트 디바이스 유형을 자동으로 프로파일링하는 방법을 제공하는 것입니다. 이 서비스(프로파일러)는 Cisco가 이전에 Cisco NAC 프로파일러 어플라이언스와 함께 제공했던 것과 동일한 기능을 제공합니다.
- Cisco ISE가 제공하는 또 다른 중요한 서비스는 엔드포인트 규정 준수(예: AV/AS 소프트웨어 설치 및 정의 파일 유효성(포스처라고 함)을 검사하는 것입니다. Cisco는 이전에 Cisco NAC Appliance에서만 이러한 정확한 상태 기능을 제공했습니다.

Cisco ISE는 동등한 수준의 기능을 제공하며 802.1X 인증 메커니즘과 통합됩니다.

WLC (무선 LAN 컨트롤러) 와 통합 된 Cisco ISE는 Apple iDevices (iPhone, iPad 및 iPod), Android 기반 스마트 폰 및 기타 같은 모바일 장치의 프로파일링 메커니즘을 제공 할 수 있습니다. 802.1X 사용자의 경우 Cisco ISE는 프로파일링 및 포스처 스캐닝과 같은 동일한 수준의 서비스를 제공할 수 있습니다. Cisco ISE의 게스트 서비스는 웹 인증 요청을 Cisco ISE로 리디렉션하여 Cisco WLC와 통합할 수도 있습니다.

이 문서에서는 알려진 엔드포인트 및 사용자 정책을 기반으로 차별화된 액세스를 제공하는 등 BYOD(Bring Your Own Device)용 무선 솔루션을 소개합니다. 이 문서에서는 BYOD의 완전한 솔루션을 제공하지는 않지만, 동적 액세스의 간단한 활용 사례를 보여 주는 역할을 합니다. 다른 컨피그레이션 예에는 권한 있는 사용자가 무선 게스트 액세스를 프로비저닝하기 위해 게스트를 스폰서할 수 있는 ISE 스폰서 포털 사용이 포함됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

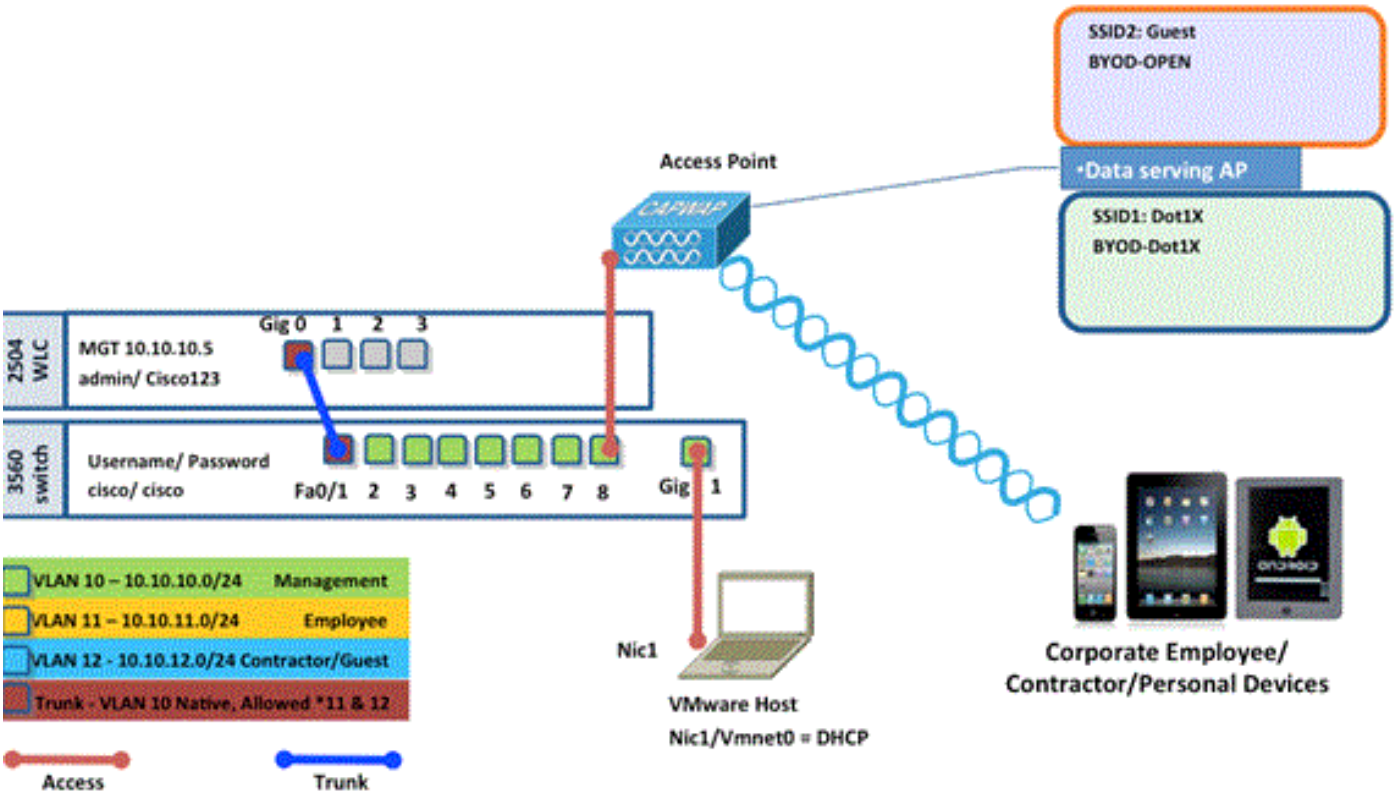
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Wireless LAN Controller 2504 또는 2106, 소프트웨어 버전 7.2.103
- Catalyst 3560 - 8개 포트
- WLC 2504

- Identity Services Engine 1.0MR(VMware 서버 이미지 버전)
- Windows 2008 Server(VMware 이미지) — 512M, 20GB 디스크액티브 디렉토리DNSDHCP인증서 서비스

토폴로지



Name	IP Address	Credential
Vmware Host	10.10.10.2	*(Machine used to host the ISE 1.0 MR vmware server files)*
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	*(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)*

표기 규칙

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

무선 LAN 컨트롤러 RADIUS NAC 및 CoA 개요

이 설정을 사용하면 WLC에서 ISE RADIUS 서버에서 오는 URL 리디렉션 AV 쌍을 찾을 수 있습니다. 이는 RADIUS NAC 설정이 활성화된 인터페이스에 연결된 WLAN에서만 가능합니다. URL 리디렉션용 Cisco AV 쌍을 받으면 클라이언트는 POSTURE_REQD 상태가 됩니다. 이는 기본적으로 컨트롤러 내부의 WEBAUTH_REQD 상태와 동일합니다.

ISE RADIUS 서버는 클라이언트가 Posture_Compliant라고 간주할 때 CoA ReAuth를 실행합니다. Session_ID는 Session_ID를 연결하는 데 사용됩니다. 이 새 AuthC (re-Auth) 에서는 URL-Redirect AV-Pairs 를 전송 하지 않습니다. URL Redirect AV-Pairs가 없으므로 WLC는 클라이언트에 더 이상 Posture가 필요하지 않음을 알고 있습니다.

RADIUS NAC 설정이 활성화되지 않으면 WLC는 URL Redirect VSA(VSA 리디렉션)를 무시합니다.

CoA-ReAuth: RFC 3576 설정으로 활성화됩니다. 이전에 지원되었던 기존 CoA 명령에 ReAuth 기능이 추가되었습니다.

RADIUS NAC 설정은 CoA가 작동하기 위해 필요하지만 이 기능에서 상호 배타적입니다.

사전 상태 ACL: 클라이언트가 POSTURE_REQ 상태에 있을 때 WLC의 기본 동작은 DHCP/DNS를 제외한 모든 트래픽을 차단하는 것입니다. Pre-Posture ACL(url-redirect-acl AV-Pair에서 호출됨)은 클라이언트에 적용되며, 해당 ACL에서 허용되는 것은 클라이언트가 연결할 수 있는 것입니다.

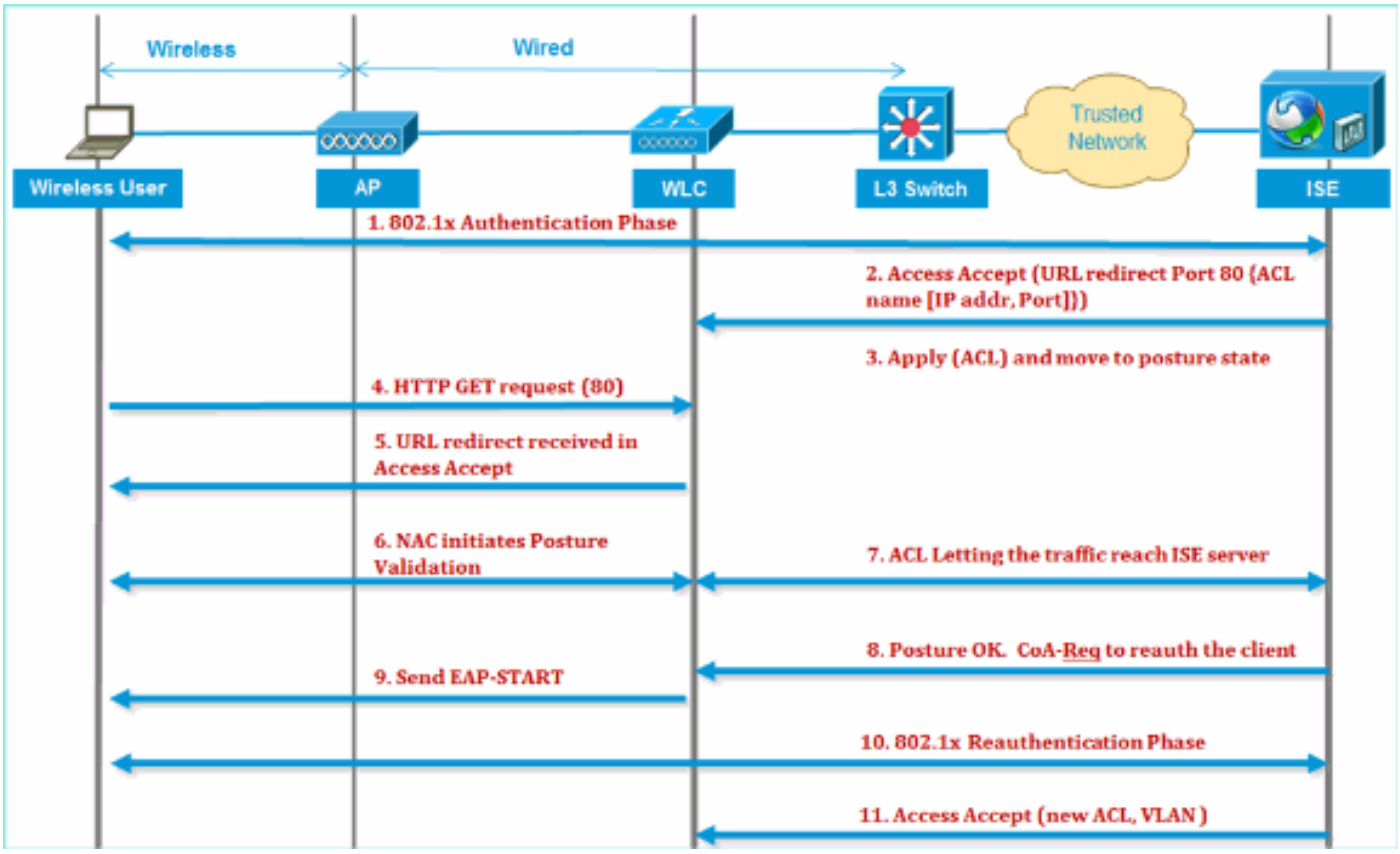
사전 인증 ACL 대 VLAN 재정의: 7.0MR1에서는 액세스 VLAN과 다른 격리 또는 AuthC VLAN이 지원되지 않습니다. 정책 서버에서 VLAN을 설정하면 전체 세션의 VLAN이 됩니다. 첫 번째 AuthZ 이후에 VLAN 변경이 필요하지 않습니다.

무선 LAN 컨트롤러 RADIUS NAC 및 CoA 기능 흐름

아래 그림에는 클라이언트가 백엔드 서버 및 NAC 상태 검증에 대해 인증될 때의 메시지 교환에 대한 세부 정보가 나와 있습니다.

1. 클라이언트는 dot1x 인증을 사용하여 인증합니다.
2. RADIUS Access Accept(RADIUS 액세스 수락)는 포트 80에 대한 리디렉션된 URL 및 IP 주소 및 포트 허용 또는 VLAN 격리를 포함하는 사전 인증 ACL을 전달합니다.
3. 클라이언트는 액세스 승인에 제공된 URL로 리디렉션되고 상태 검증이 완료될 때까지 새 상태로 전환됩니다. 이 상태의 클라이언트는 ISE 서버와 통신하며 ISE NAC 서버에 구성된 정책과 비교하여 자신을 검증합니다.
4. 클라이언트의 NAC Agent가 상태 검증(포트 80에 대한 트래픽)을 시작합니다. 에이전트가 포트 80에 HTTP 검색 요청을 전송하면 컨트롤러는 액세스 승인에 제공된 URL로 리디렉션합니다. ISE는 클라이언트가 연결을 시도하고 클라이언트에 직접 응답한다는 것을 알고 있습니다. 이렇게 하면 클라이언트가 ISE 서버 IP에 대해 알게 되고 이제부터 클라이언트가 ISE 서버와 직접 통신합니다.
5. ACL이 이 트래픽을 허용하도록 구성되어 있으므로 WLC에서 이 트래픽을 허용합니다. VLAN 재정의의 경우 트래픽이 ISE 서버에 도달하도록 브리지됩니다.
6. ISE 클라이언트가 평가를 완료하면 RADIUS CoA-Req(재인증 서비스 포함)가 WLC로 전송됩니다. 이렇게 하면 EAP-START를 전송하여 클라이언트의 재인증이 시작됩니다. 재인증이 성공하면 ISE는 새 ACL(있는 경우)과 URL 리디렉션 없음 또는 액세스 VLAN을 사용하여 액세스 승인을 보냅니다.
7. WLC는 RFC 3576에 따라 CoA-Req 및 Disconnect-Req를 지원합니다. RFC 5176에 따라 WLC는 재인증 서비스를 위해 CoA-Req를 지원해야 합니다.
8. 다운로드 가능한 ACL 대신 사전 구성된 ACL이 WLC에서 사용됩니다. ISE 서버는 컨트롤러에 이미 구성된 ACL 이름만 전송합니다.
9. 이 설계는 VLAN 및 ACL 케이스 모두에 적용되어야 합니다. VLAN 재정의의 경우 포트 80이 리디렉션되고 격리 VLAN의 나머지 트래픽을 허용합니다(브리지). ACL의 경우 액세스 수락에서 수신한 사전 인증 ACL이 적용됩니다.

이 그림에서는 이 기능 흐름을 시각적으로 보여줍니다.



ISE 프로파일링 개요

Cisco ISE 프로 파 일러 서비스는 엔터프라이즈 네트워크에 대한 적절 한 액세스를 보장 하고 유지 관리 하기 위해 장치 유형에 관계없이 네트워크에 연결 된 모든 엔드 포인트의 기능을 검색 하고, 검색 하고 결정 하는 기능을 제공 합니다. 네트워크에 있는 모든 엔드포인트의 속성 또는 속성 집합을 주로 수집하고 프로필에 따라 분류합니다.

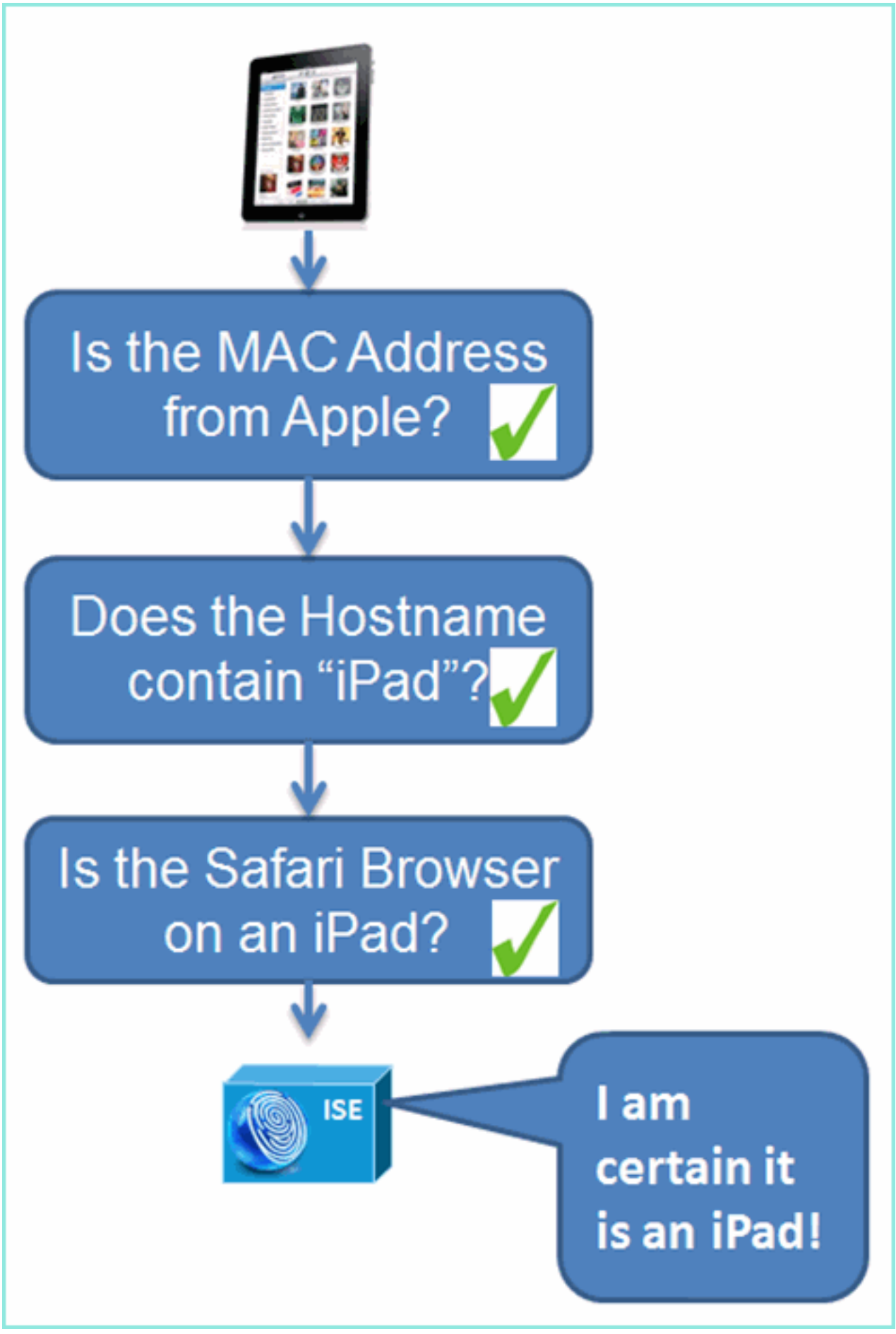
프로파일러는 다음 구성 요소로 구성됩니다.

- 이 센서는 여러 개의 프로브를 포함합니다. 프로브는 네트워크 액세스 디바이스를 쿼리하여 네트워크 패킷을 캡처하고 엔드포인트에서 수집된 특성 및 특성 값을 분석기로 전달합니다.
- 분석기는 구성 된 정책 및 ID 그룹을 사용 하여 속성 및 수집 된 속성 값과 일치 하는 엔드 포인트를 평가 합니다. 이 지정 된 그룹에 엔드 포인트를 분류 하고 Cisco ISE 데이터베이스에 일치 한 프로필이 있는 엔드 포인트를 저장 합니다.

모바일 디바이스를 탐지하려면 올바른 디바이스 식별을 위해 다음 프로브를 조합하여 사용하는 것이 좋습니다.

- RADIUS(Calling-Station-ID): MAC 주소(OUI)를 제공합니다.
- DHCP(host-name): 호스트 이름 - 기본 호스트 이름에는 디바이스 유형이 포함될 수 있습니다(예: jsmith-ipad).
- DNS(역방향 IP 조회): FQDN - 기본 호스트 이름에는 디바이스 유형이 포함될 수 있습니다.
- HTTP(User-Agent): 특정 모바일 디바이스 유형에 대한 세부사항

iPad의 이 예에서 프로파일러는 User-Agent 특성에서 웹 브라우저 정보를 캡처하고 요청 메시지에서 다른 HTTP 특성을 캡처하여 엔드포인트 특성 목록에 추가합니다.


Is the MAC Address from Apple?
Does the Hostname contain “iPad”?
Is the Safari Browser on an iPad?
ISE
I am certain it is an iPad!

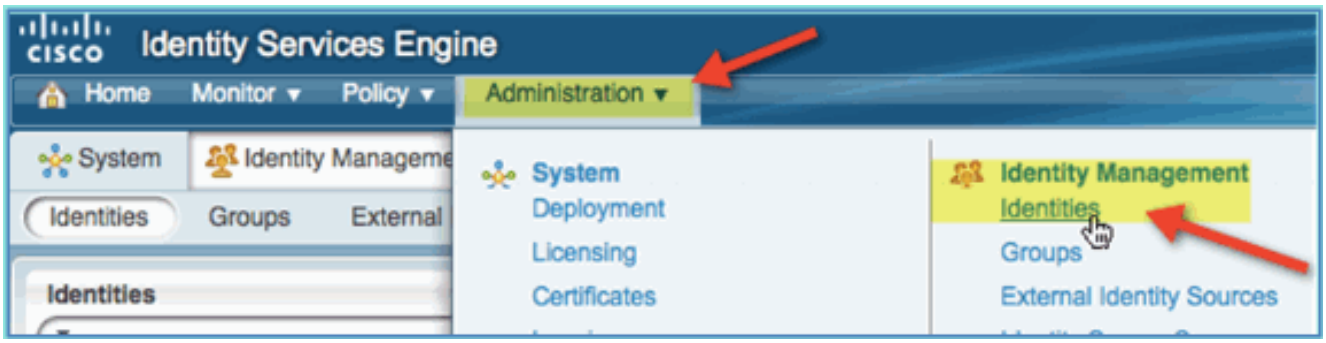
[내부 ID 사용자 생성]

MS AD(Active Directory)는 단순한 개념 증명을 위해 필요하지 않습니다. ISE는 액세스를 위한 사용자 액세스 차별화 및 세분화된 정책 제어를 포함하는 유일한 ID 저장소로 사용할 수 있습니다.

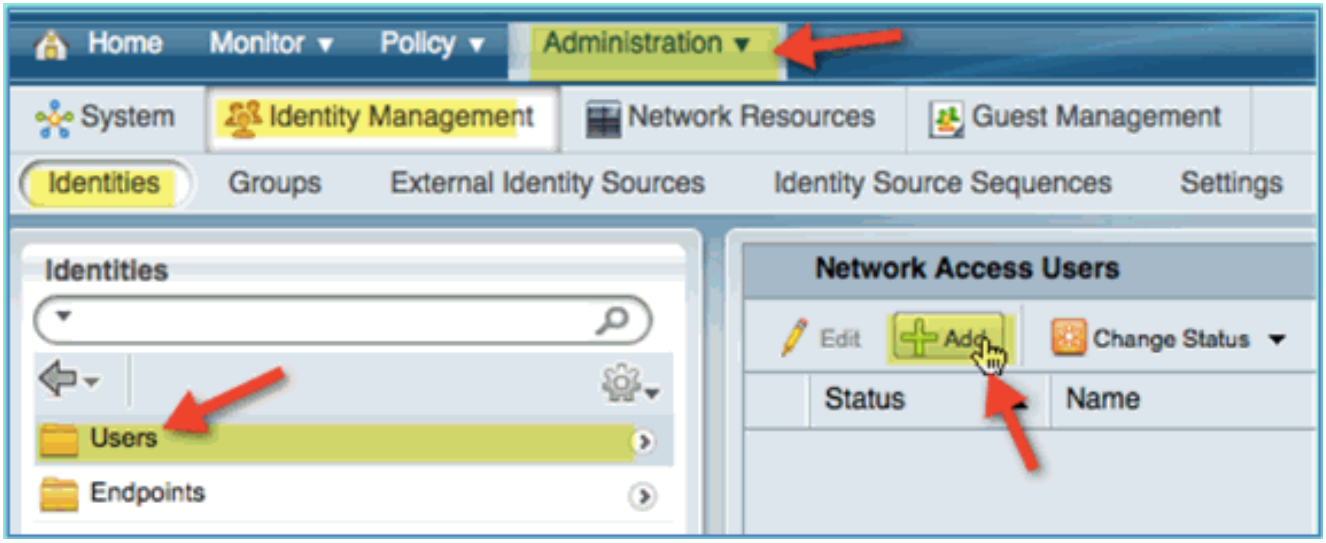
ISE 1.0 릴리스에서 AD 통합을 사용하여 ISE는 권한 부여 정책에서 AD 그룹을 사용할 수 있습니다. ISE 내부 사용자 저장소가 사용되는 경우(AD 통합 없음), 디바이스 ID 그룹과 함께 정책에서 그룹을 사용할 수 없습니다(ISE 1.1에서 확인할 확인된 버그). 따라서 장치 ID 그룹 외에 사용 시 직원 또는 계약자와 같이 개별 사용자만 차별화할 수 있습니다.

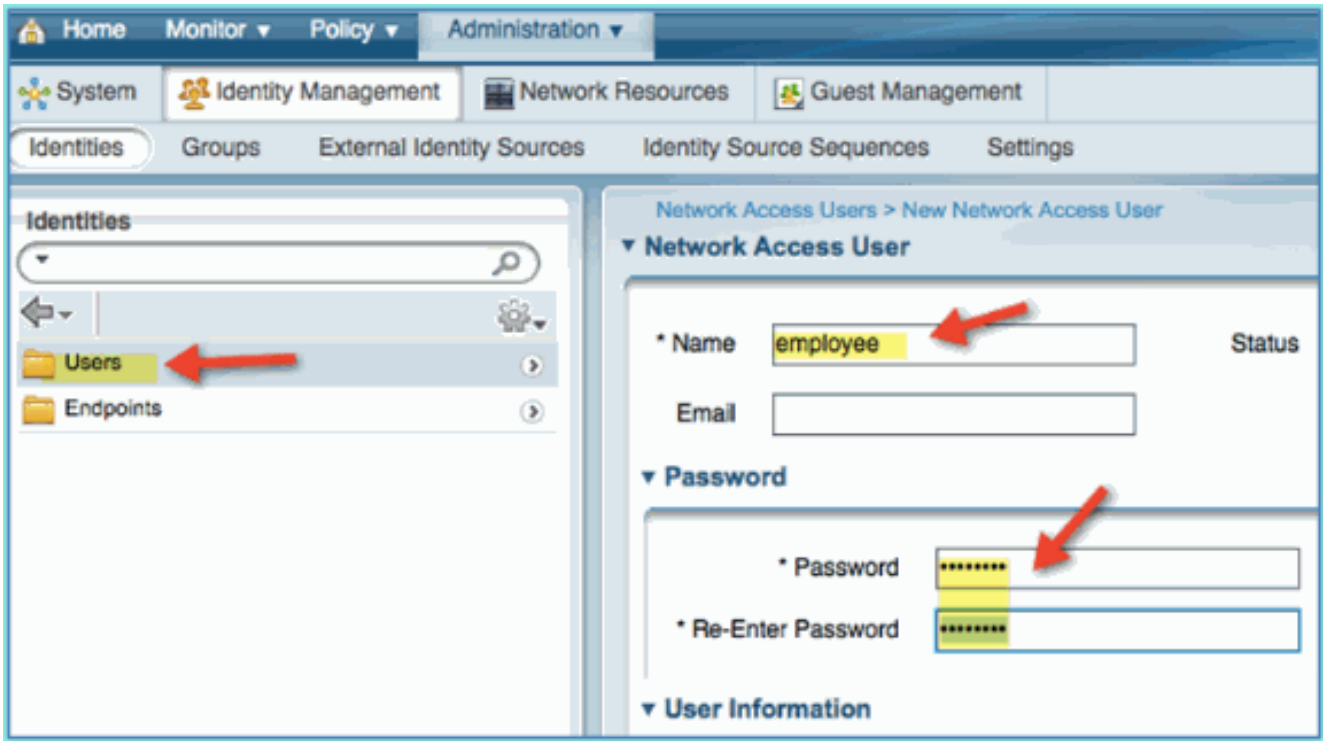
다음 단계를 완료하십시오.

1. https://ISEip 주소에 대한 브라우저 창을 엽니다.
2. Administration(관리) **> Identity Management(ID 관리) > Identities(ID)로 이동합니다**
.



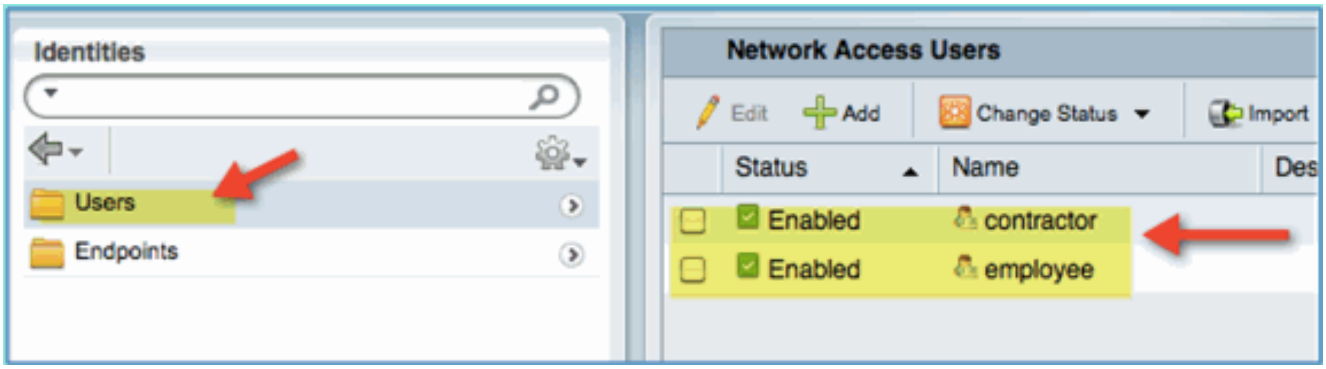
3. Users**(사용자)**를 선택한 다음 **Add** (Network Access User)(네트워크 액세스 사용자)를 클릭합니다. 다음 사용자 값을 입력하고 직원 그룹에 할당합니다.이름: employee비밀번호: XXXX





4. Submit(제출)**을 클릭합니다**.이름: 계약자비밀번호: XXXX
5. 두 어카운트가 모두 생성되었는지 확인합니다

.



ISE에 Wireless LAN Controller 추가

ISE에 대한 RADIUS 요청을 시작하는 모든 디바이스는 ISE에 정의가 있어야 합니다. 이러한 네트워크 디바이스는 IP 주소를 기반으로 정의됩니다. ISE 네트워크 디바이스 정의에서는 IP 주소 범위를 지정할 수 있으므로 정의가 여러 실제 디바이스를 나타낼 수 있습니다.

RADIUS 통신에 필요한 것 외에도 ISE 네트워크 디바이스 정의에는 SNMP 및 SSH와 같은 다른 ISE/디바이스 통신에 대한 설정이 포함되어 있습니다.

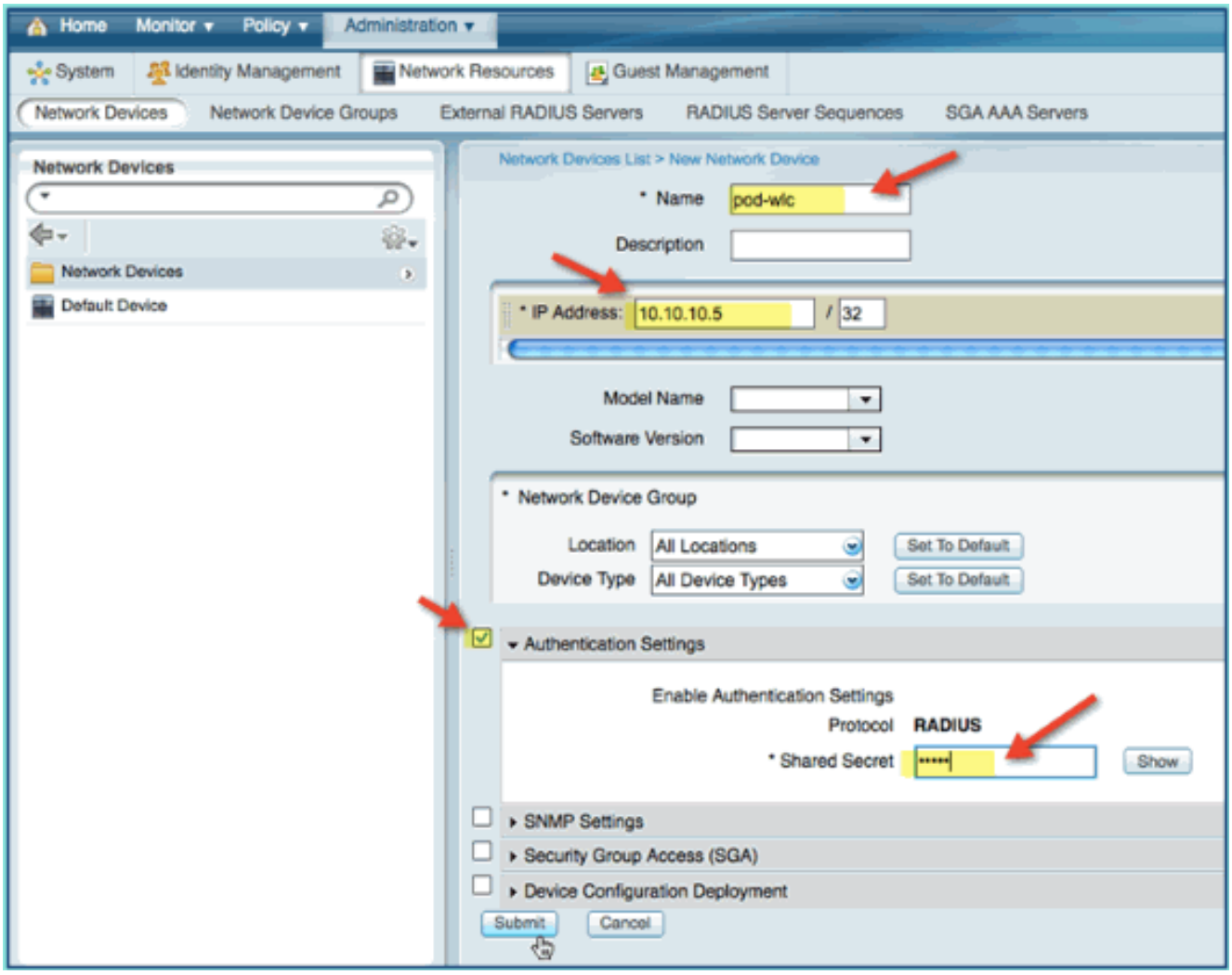
네트워크 디바이스 정의의 또 다른 중요한 측면은 디바이스를 적절히 그룹화하여 네트워크 액세스 정책에서 이 그룹화를 활용할 수 있도록 하는 것입니다.

이 연습에서는 실습에 필요한 디바이스 정의가 구성됩니다.

다음 단계를 완료하십시오.

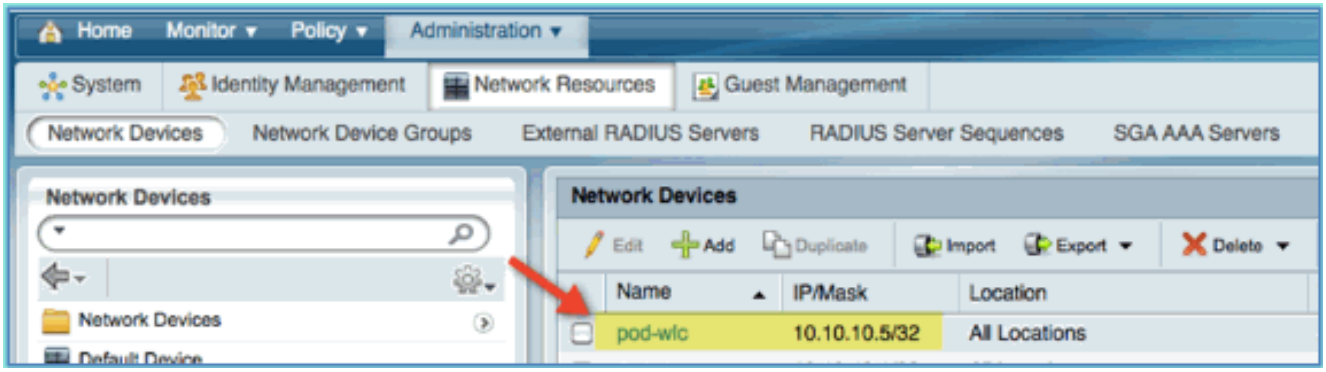
1. ISE에서 Administration(관리) **> Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다**

.



2. Network Devices(네트워크 디바이스)에서 Add(추가)**를 클릭합니다**. IP 주소를 입력하고 Authentication Setting(인증 설정)을 마스크 처리한 다음 공유 암호로 'cisco'를 입력합니다.
3. WLC 항목을 저장하고 목록에서 컨트롤러를 확인합니다

.



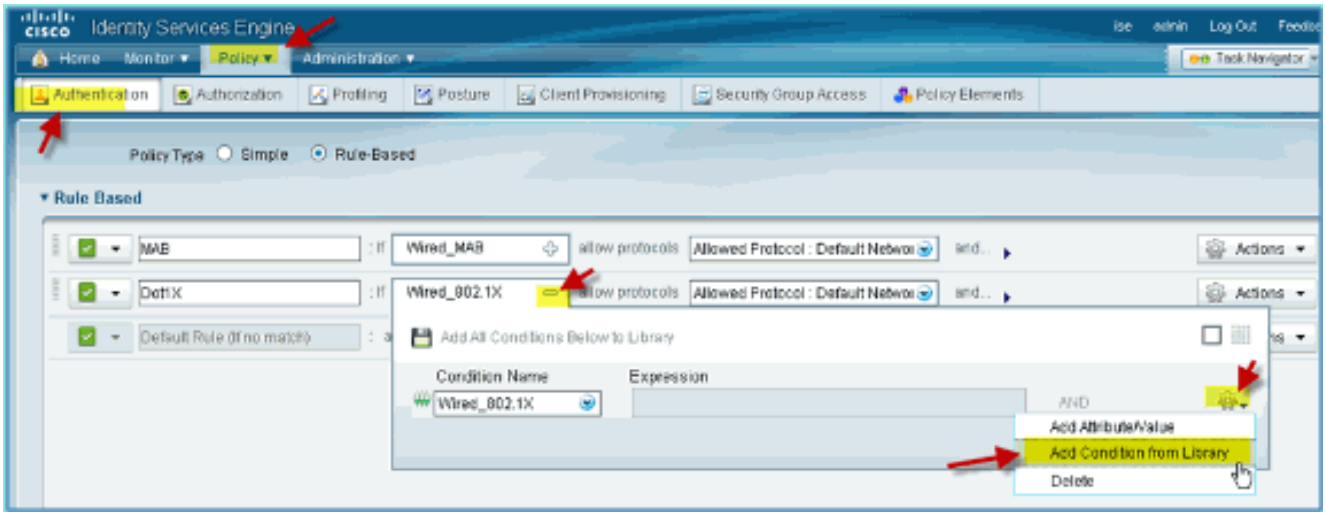
무선 인증을 위한 ISE 구성

802.1x 무선 클라이언트를 인증하고 ID 저장소로 Active Directory를 사용하도록 ISE를 구성해야 합니다.

다음 단계를 완료하십시오.

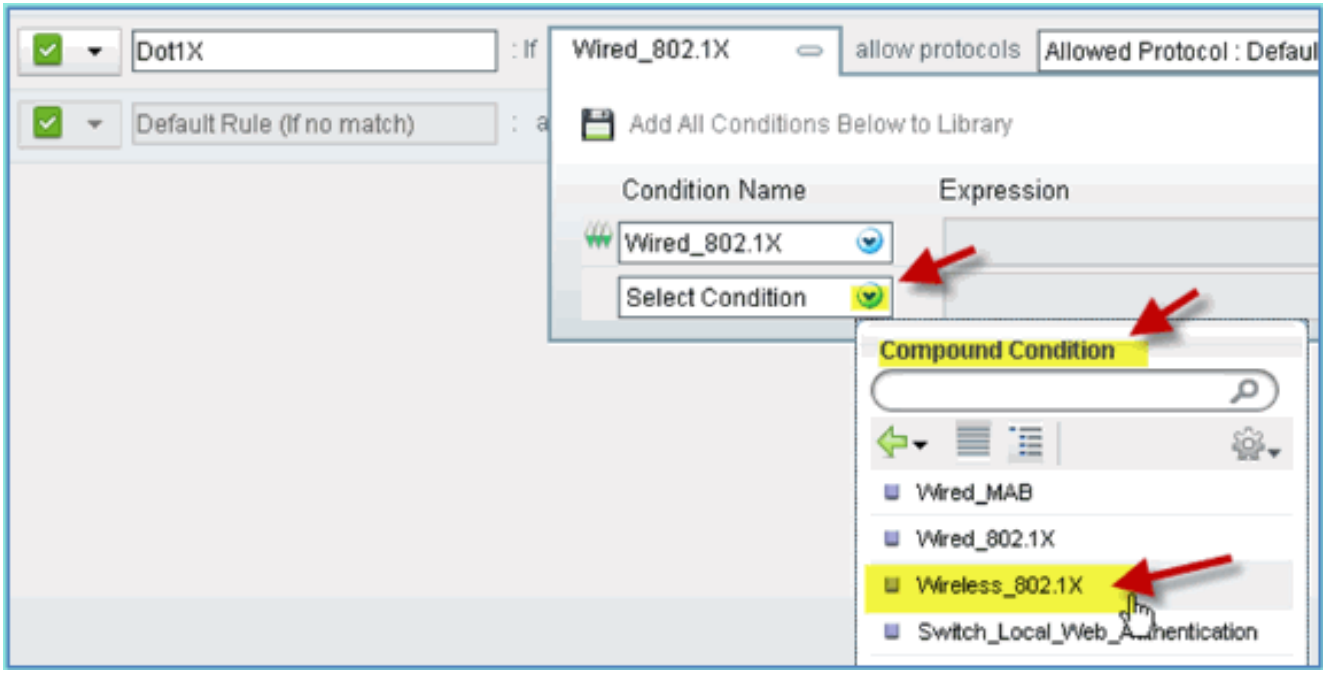
1. ISE에서 Policy(정책) > **Authentication(인증)으로 이동합니다**.
2. Dot1x > Wired_802.1X (-)를 클릭하여 확장합니다.
3. 기어 아이콘을 클릭하여 라이브러리**에서 조건을 추가합니다**

.



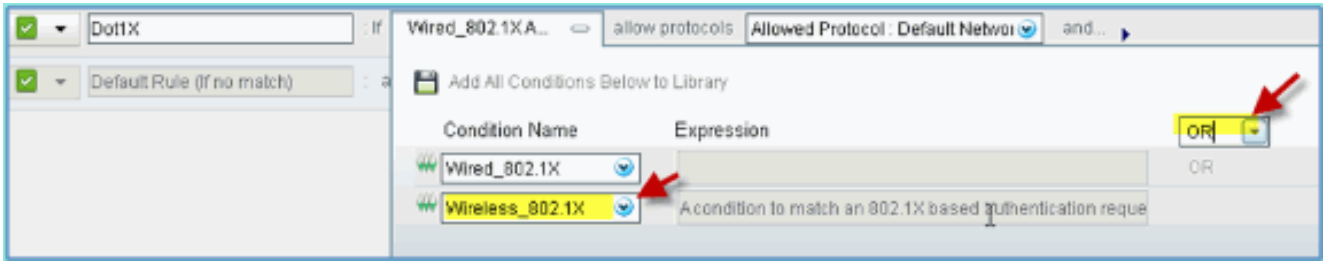
4. 조건 선택 드롭다운에서 **Compound Condition(복합 조건) > Wireless_802.1X를** 선택합니다

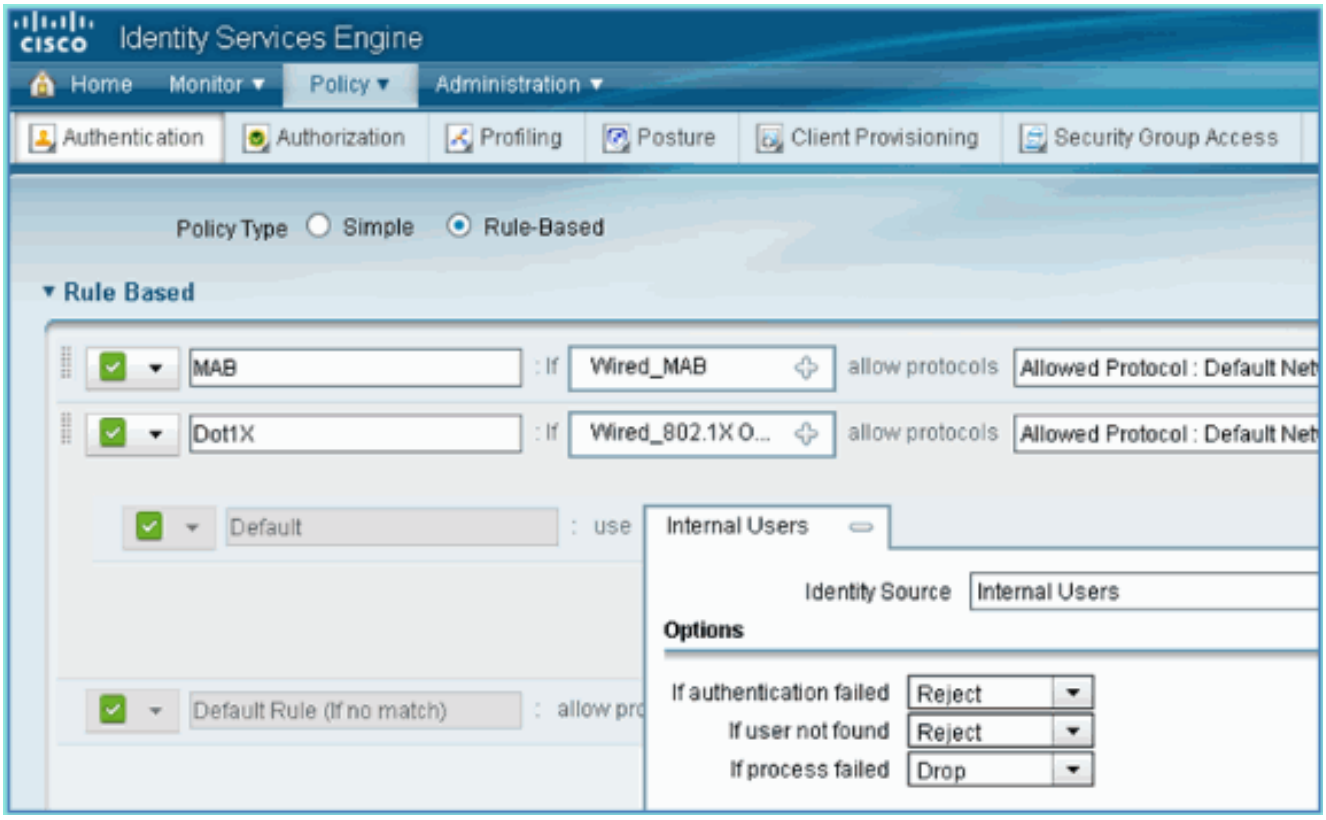
.



5. Express 조건을 OR로 **설정합니다**.
6. after allow protocols(프로토콜 허용 후) 옵션을 확장하고 기본 Internal Users(내부 사용자)(기본값)를 적용합니다

.





7. 다른 모든 항목은 기본값으로 둡니다. 저장을 클릭하여 단계를 완료합니다.

부트스트랩 무선 LAN 컨트롤러

네트워크에 WLC 연결

Cisco 2500 Wireless LAN Controller 구축 설명서는 Cisco 2500 Series Wireless Controller 구축 설명서에서도 제공됩니다.

Startup Wizard를 사용하여 컨트롤러 구성

```
(Cisco Controller)
 Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
 Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
   ISE-Podx Enter Administrative User Name (24 characters max): admin
   Enter Administrative Password
   (3 to 24 characters): Cisco123
   Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
 Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
 Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
 Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

```
 Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
 Configure a NTP server now? [YES][no]: no
Configure the ntp system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
 Configuration saved!
 Resetting system with new configuration...
Restarting system.
```

네이버 스위치 컨피그레이션

컨트롤러는 인접한 스위치(Fast Ethernet 1)의 이더넷 포트에 연결됩니다. 네이버 스위치 포트는 802.1Q 트렁크로 구성되며 트렁크의 모든 VLAN을 허용합니다. 네이티브 VLAN 10을 사용하면 WLC의 관리 인터페이스를 연결할 수 있습니다.

802.1Q 스위치 포트 구성은 다음과 같습니다.

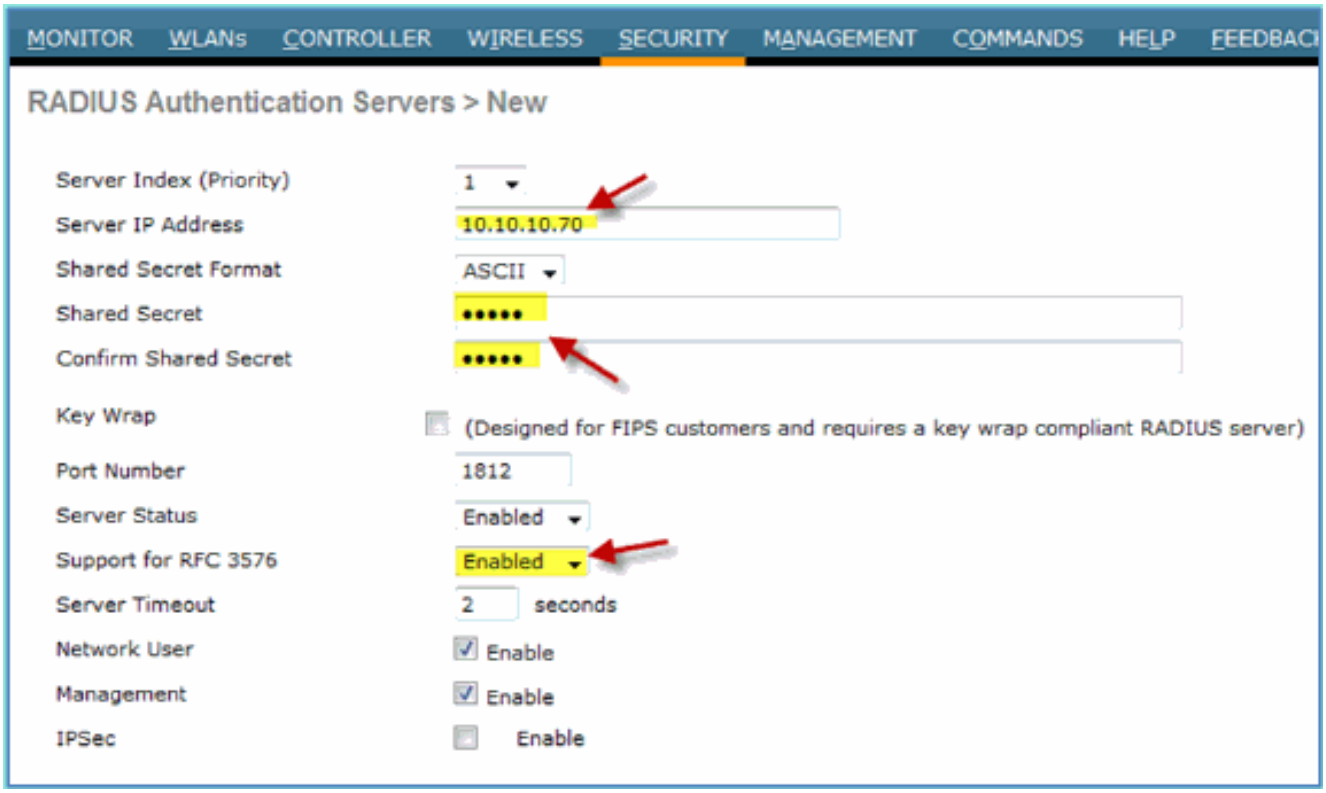
```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

WLC에 인증 서버(ISE) 추가

무선 엔드포인트에 802.1X 및 CoA 기능을 사용하려면 ISE를 WLC에 추가해야 합니다.

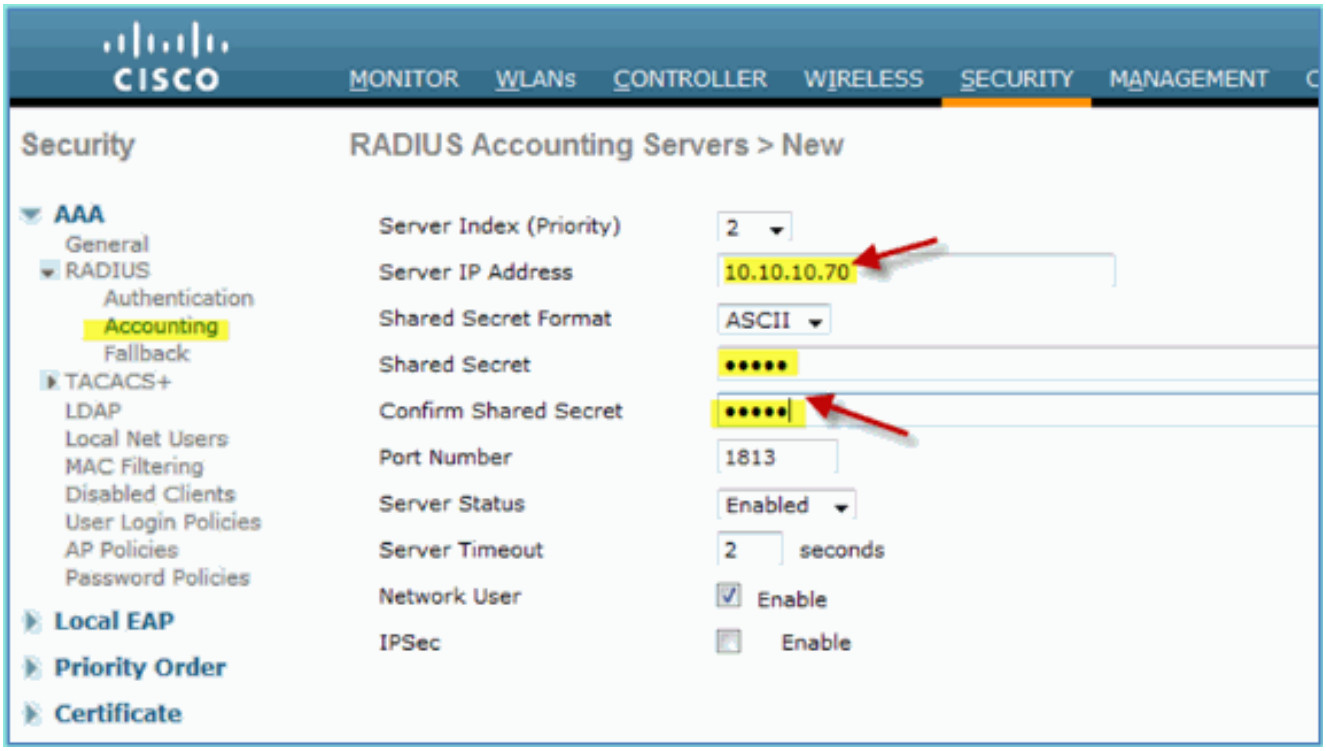
다음 단계를 완료하십시오.

1. 브라우저를 열고 Pod WLC(보안 HTTP 사용)에 연결합니다(https://wlc).
2. Security(**보안) > Authentication(인증) > New(새로 만들기)로 이동합니다**
   .



3. 다음 값을 입력합니다.서버 IP 주소: 10.10.10.70(할당 확인)공유 암호: ciscoRFC 3576(CoA) 지원: 사용(기본값)기타 모든 사항: 기본값
4. Apply(**적용**)를 클릭하여 계속 진행합니다.
5. RADIUS Accounting(**RADIUS 어카운팅) > ADD NEW(새로 추가)를 선택합니다**

.



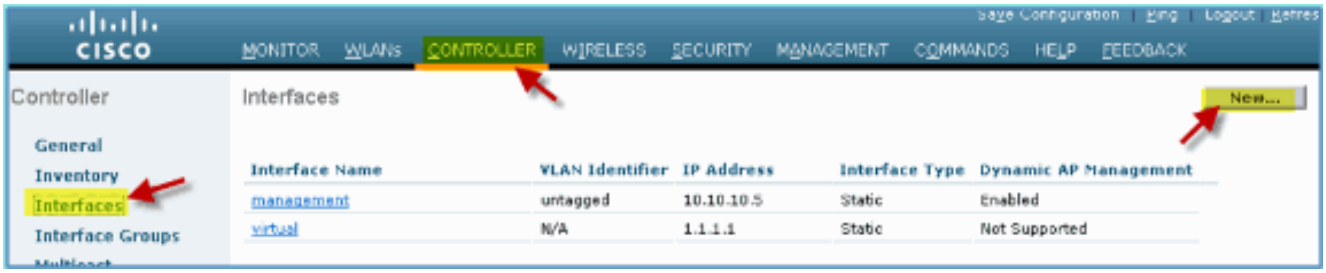
6. 다음 값을 입력합니다.서버 IP 주소: 10.10.10.70공유 암호: cisco기타 모든 사항: 기본값
7. Apply(**적용**)를 클릭한 다음 WLC에 대한 컨피그레이션을 저장합니다.

WLC 직원 동적 인터페이스 만들기

WLC에 대한 새 동적 인터페이스를 추가하고 이를 직원 VLAN에 매핑하려면 다음 단계를 완료하십

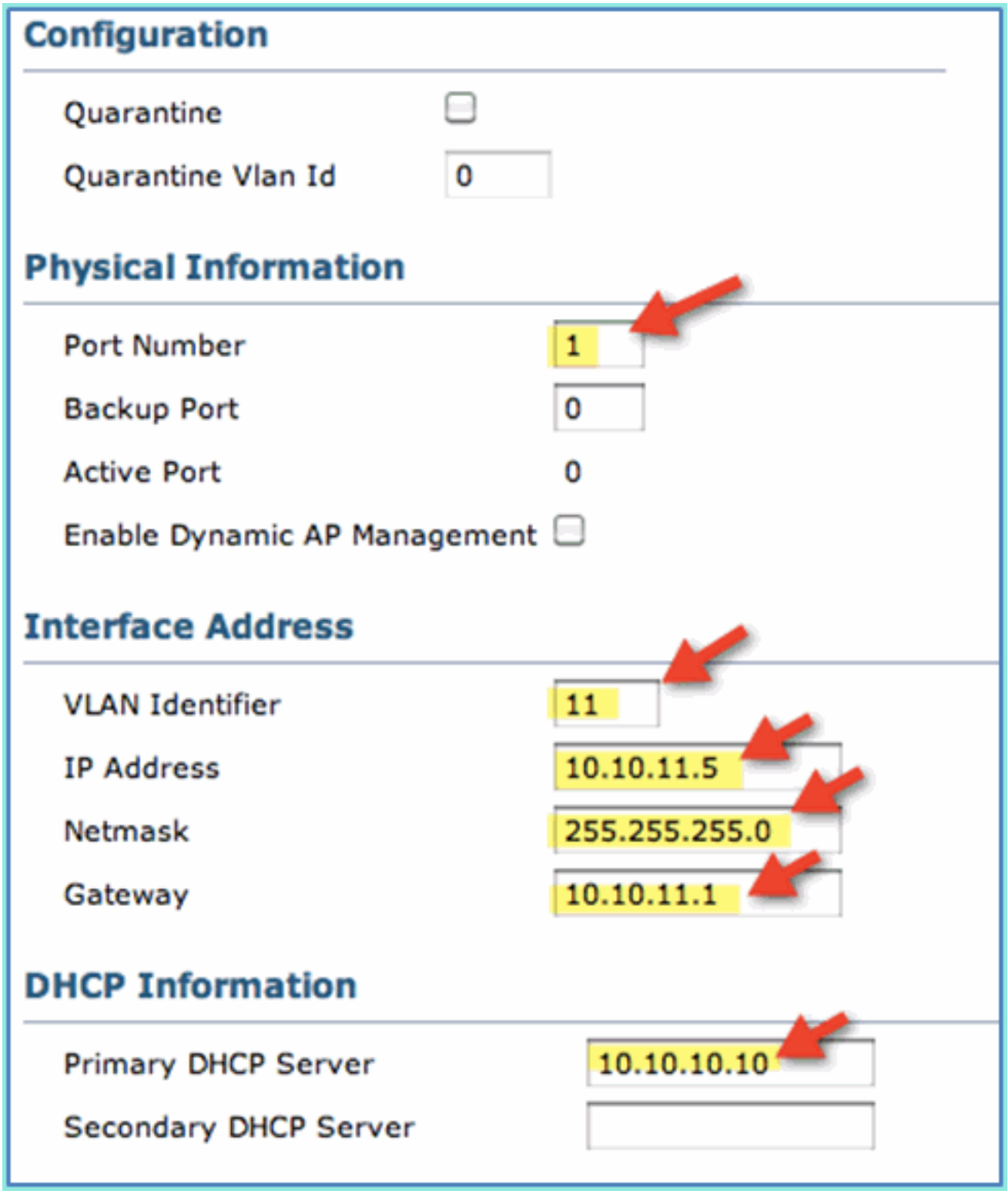
시오.

1. WLC에서 Controller(컨트롤러) **> Interfaces(인터페이스)로 이동합니다**. 그런 다음 New(새로 만들기)**를** 클릭합니다
.



2. WLC에서 Controller(컨트롤러) **> Interfaces(인터페이스)로 이동합니다**. 다음을 입력합니다.인터페이스 이름: EmployeeVLAN ID:
11

3. 사원 인터페이스에 다음을 입력합니다.포트 번호: 1VLAN 식별자: 11IP 주소: 10.10.11.5넷마스크: 255.255.255.0게이트웨이: 10.10.11.1DHCP:
10.10.10.10



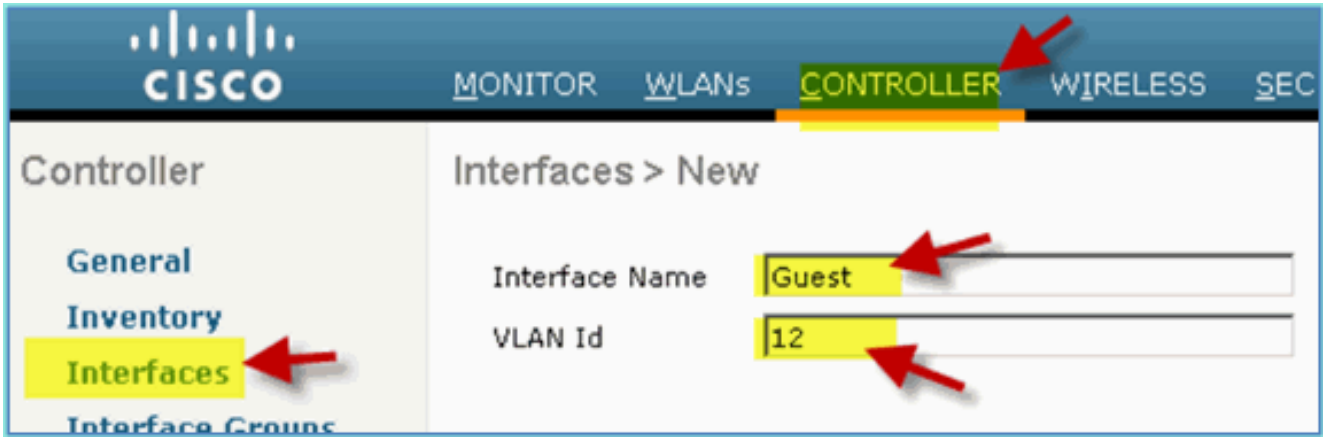
4. 신입 직원 동적 인터페이스가 생성되었는지 확인합니다

.

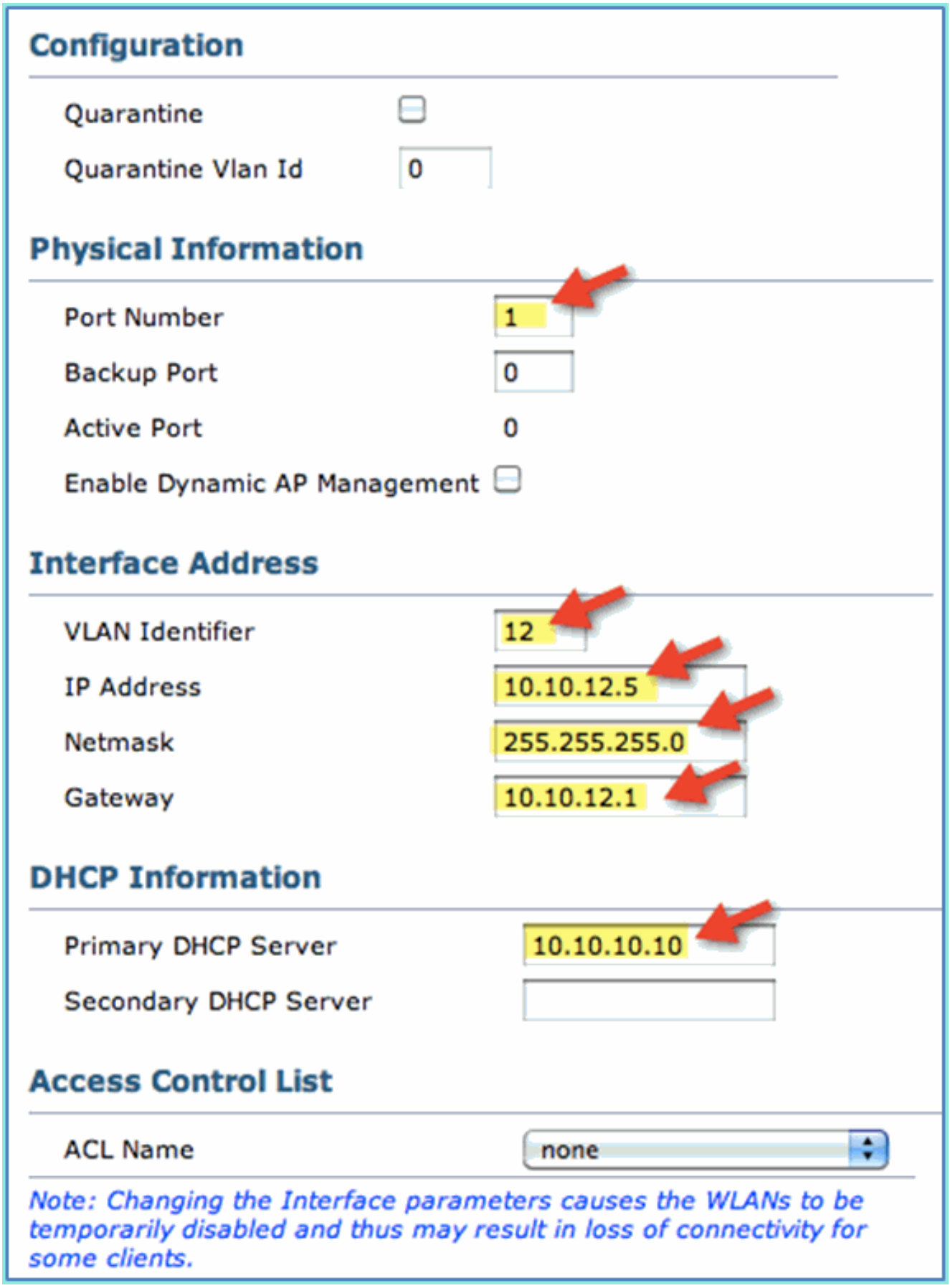
WLC 게스트 동적 인터페이스 생성

WLC에 대한 새 동적 인터페이스를 추가하고 이를 게스트 VLAN에 매핑하려면 다음 단계를 완료하십시오.

1. WLC에서 Controller(컨트롤러) **> Interfaces(인터페이스)로 이동합니다**. 그런 다음 New(새로 만들기)**를** 클릭합니다.
2. WLC에서 Controller(컨트롤러) **> Interfaces(인터페이스)로 이동합니다**. 다음을 입력합니다.인터페이스 이름: GuestVLAN ID:
   12

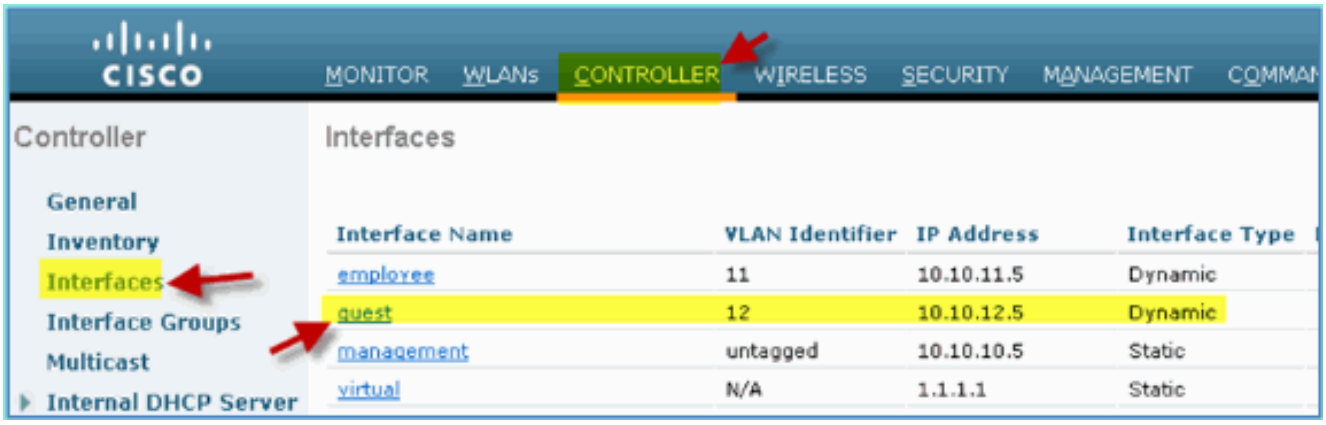


3. 게스트 인터페이스에 대해 다음을 입력 합니다.포트 번호: 1VLAN 식별자: 12IP 주소: 10.10.12.5넷마스크: 255.255.255.0게이트웨이: 10.10.12.1DHCP: 10.10.10.10



4. 게스트 인터페이스가 추가되었는지 확인합니다

.



802.1x WLAN 추가

WLC의 초기 부트스트랩에서 기본 WLAN이 생성되었을 수 있습니다. 이 경우 설명서에 설명된 대로 무선 802.1X 인증을 지원하도록 수정하거나 새 WLAN을 생성합니다.

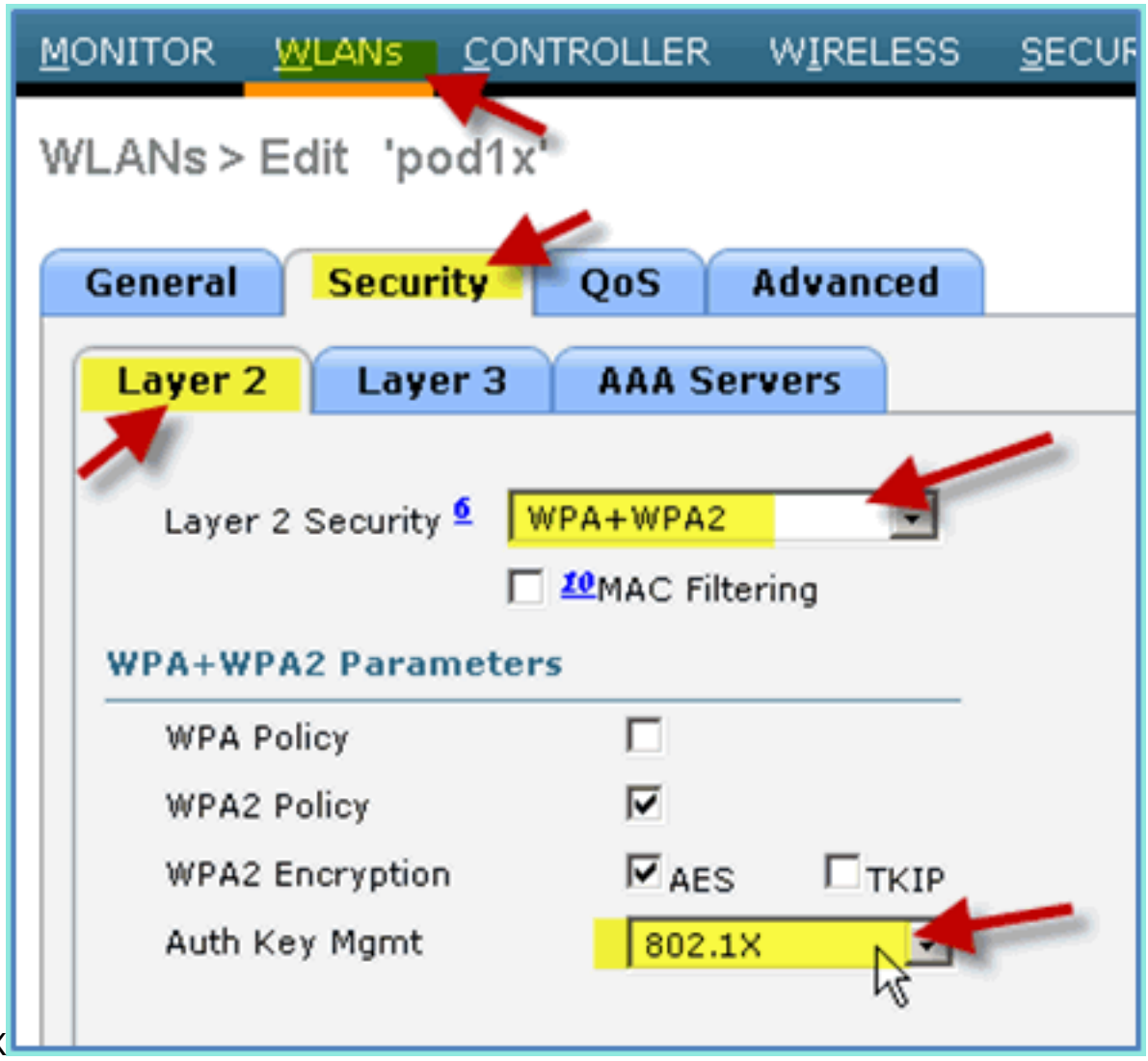
다음 단계를 완료하십시오.

1. WLC에서 WLAN(**WLAN) > Create New(새로 만들기)로 이동합니다**
.

2. WLAN에 다음을 입력합니다.프로필 이름: pod1xSSID: 동일

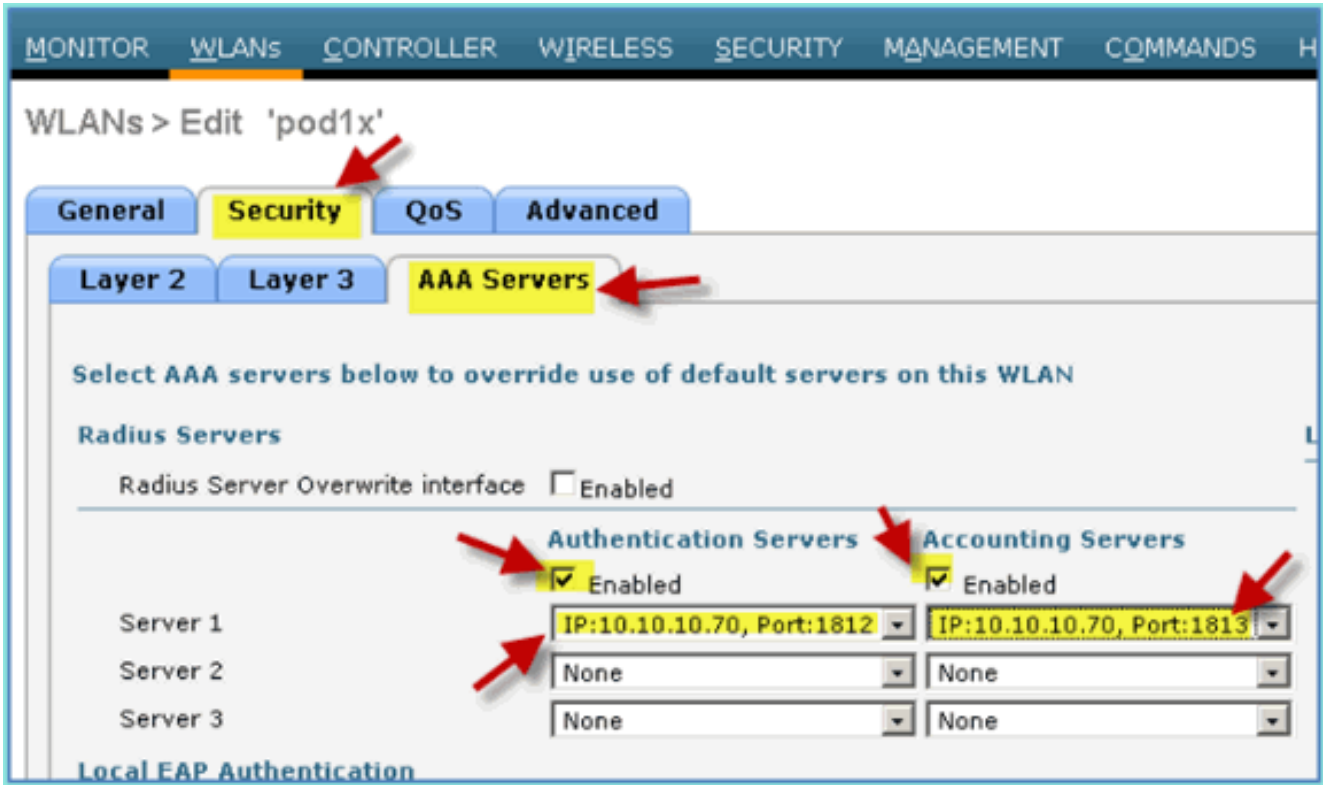
3. WLAN settings(WLAN 설정) > General(일반) 탭에서 다음을 사용합니다.무선 정책: 모두인터페이스/그룹: 관리기타 모든 사항: 기본값

4. WLAN > Security(보안) 탭 > Layer 2(레이어 2)에서 다음을 설정합니다.레이어 2 보안 :WPA+WPA2WPA2 정책/암호화: 사용/AES인증 키 관리:



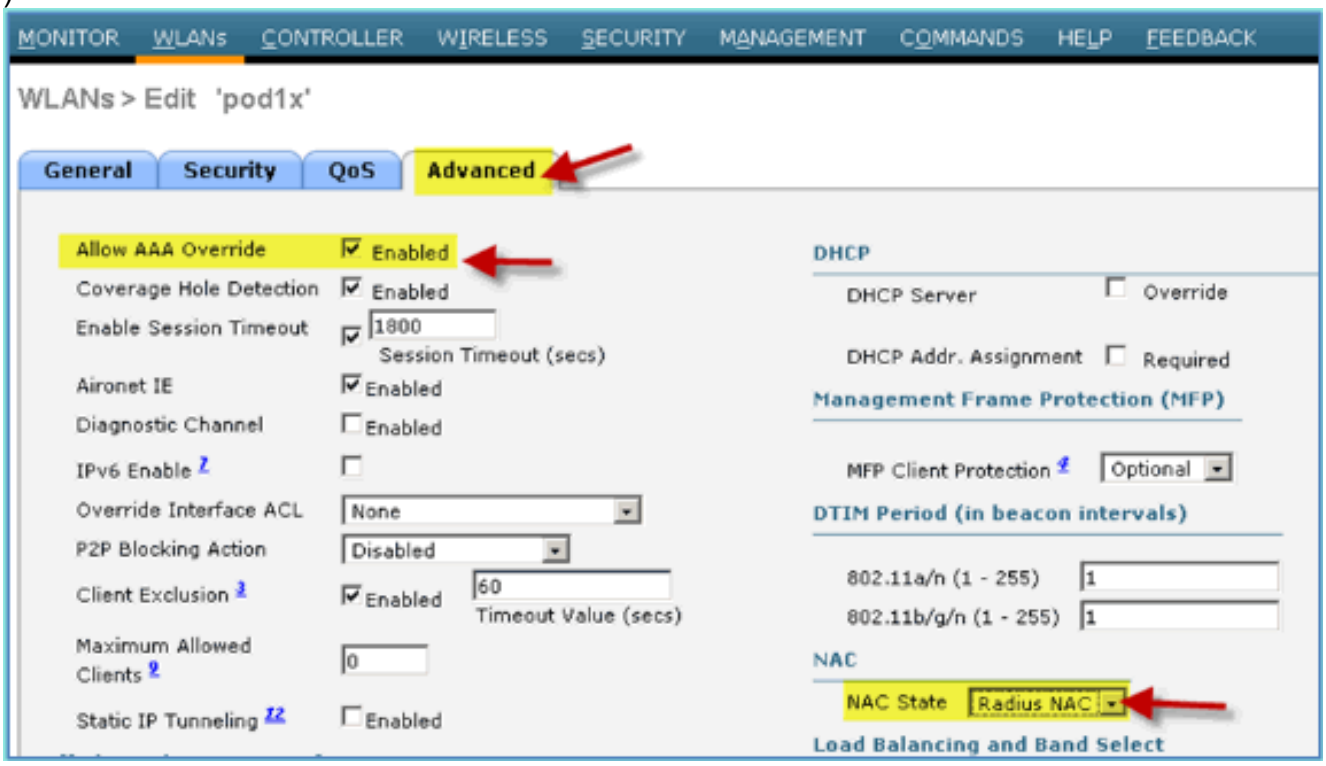
802.1X

5. WLAN > Security(보안) 탭 > AAA Servers(AAA 서버)에서 다음을 설정합니다.무선 서버 덮어쓰기 인터페이스: 사용 안 함인증/계정 관리 서버: 사용서버 1: 10.10.10.70

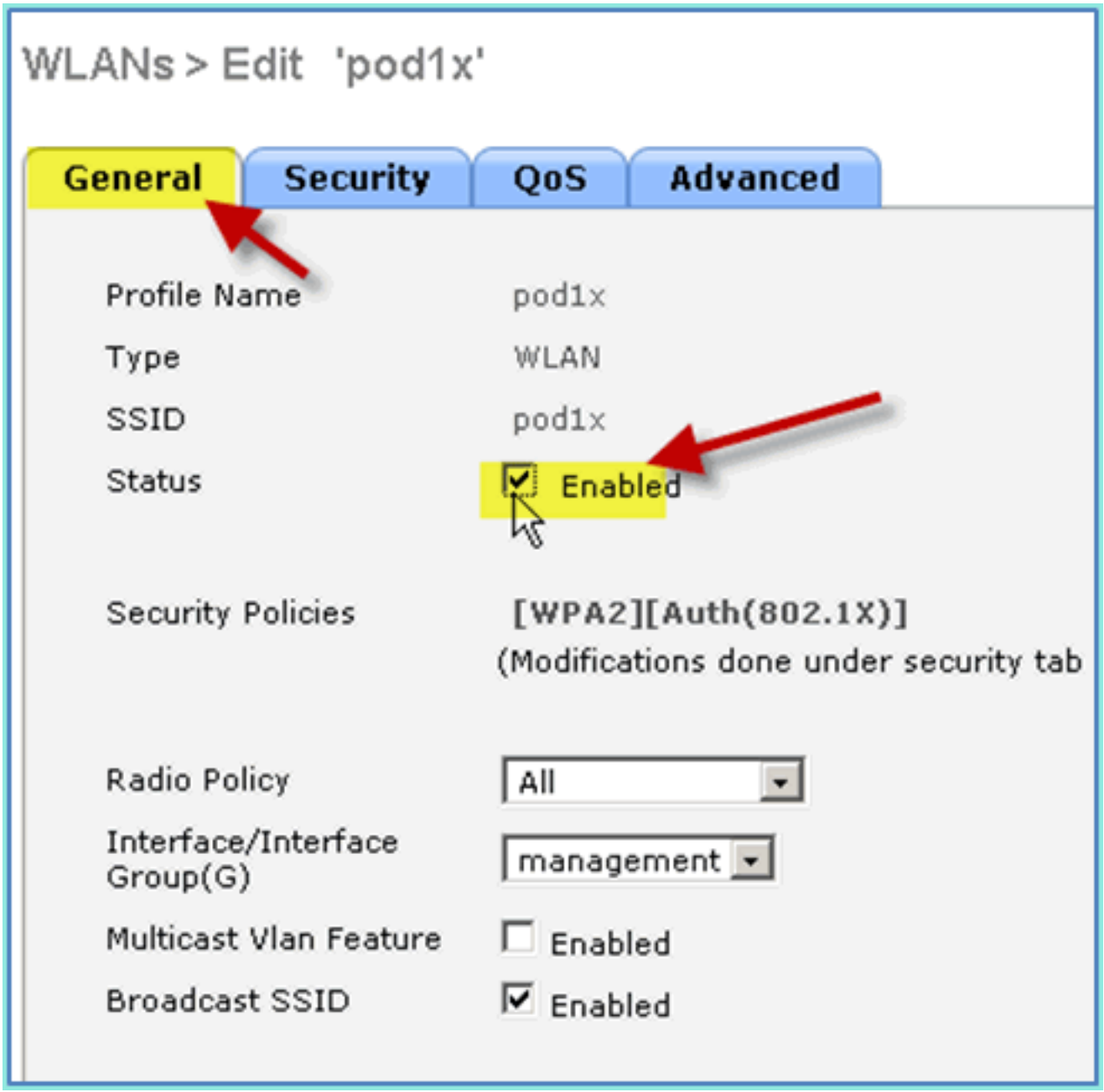


6. WLAN(WLAN) > Advanced(고급) 탭에서 다음을 설정합니다.Allow AAA Override(AAA 재정의

허용): Enabled(활성화)NAC State(NAC 상태): Radius NAC(선택
)



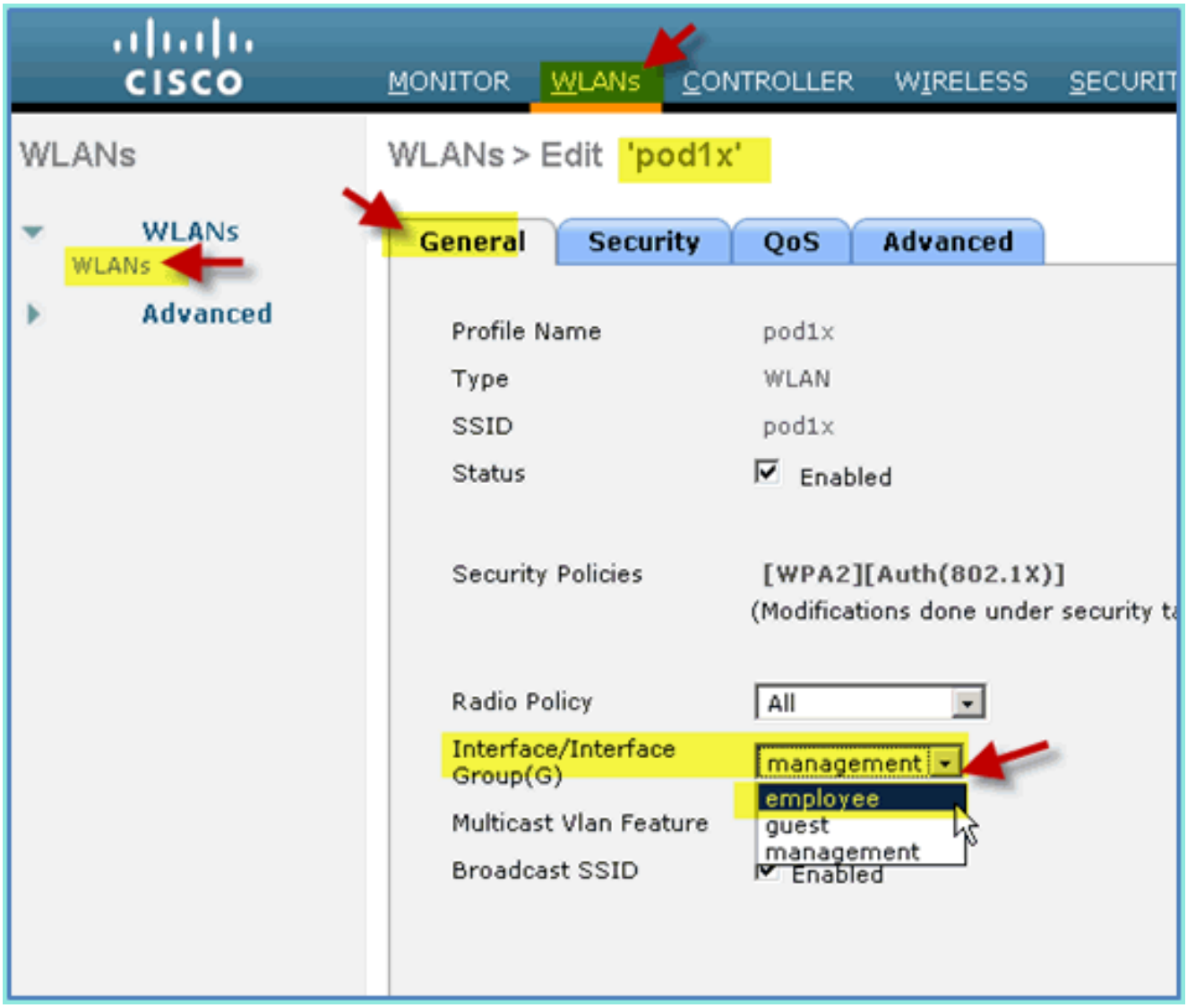
7. WLAN > General(일반) 탭 > Enable WLAN(WLAN 활성화)(확인란)으로 돌아갑니다
.



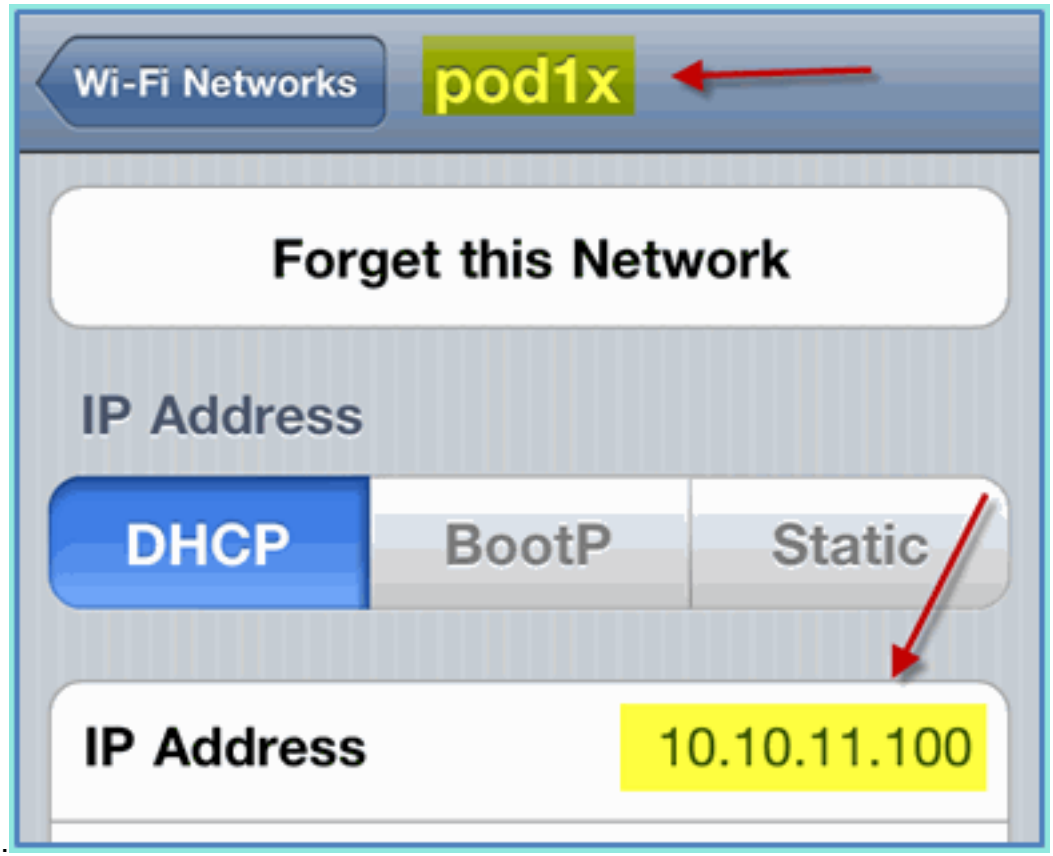
WLC 동적 인터페이스 테스트

유효한 직원 및 게스트 인터페이스를 신속하게 확인해야 합니다. 모든 디바이스를 사용하여 WLAN에 연결한 다음 WLAN 인터페이스 할당을 변경합니다.

1. WLC에서 WLAN(WLAN) **> WLANs(WLAN)로 이동합니다**. 이전 연습에서 생성한 보안 SSID를 수정하려면 클릭합니다.
2. Interface/Interface Group(인터페이스/인터페이스 그룹)을 **Employee(직원)**로 변경한 다음 Apply(적용)**를 클릭합니다**
.



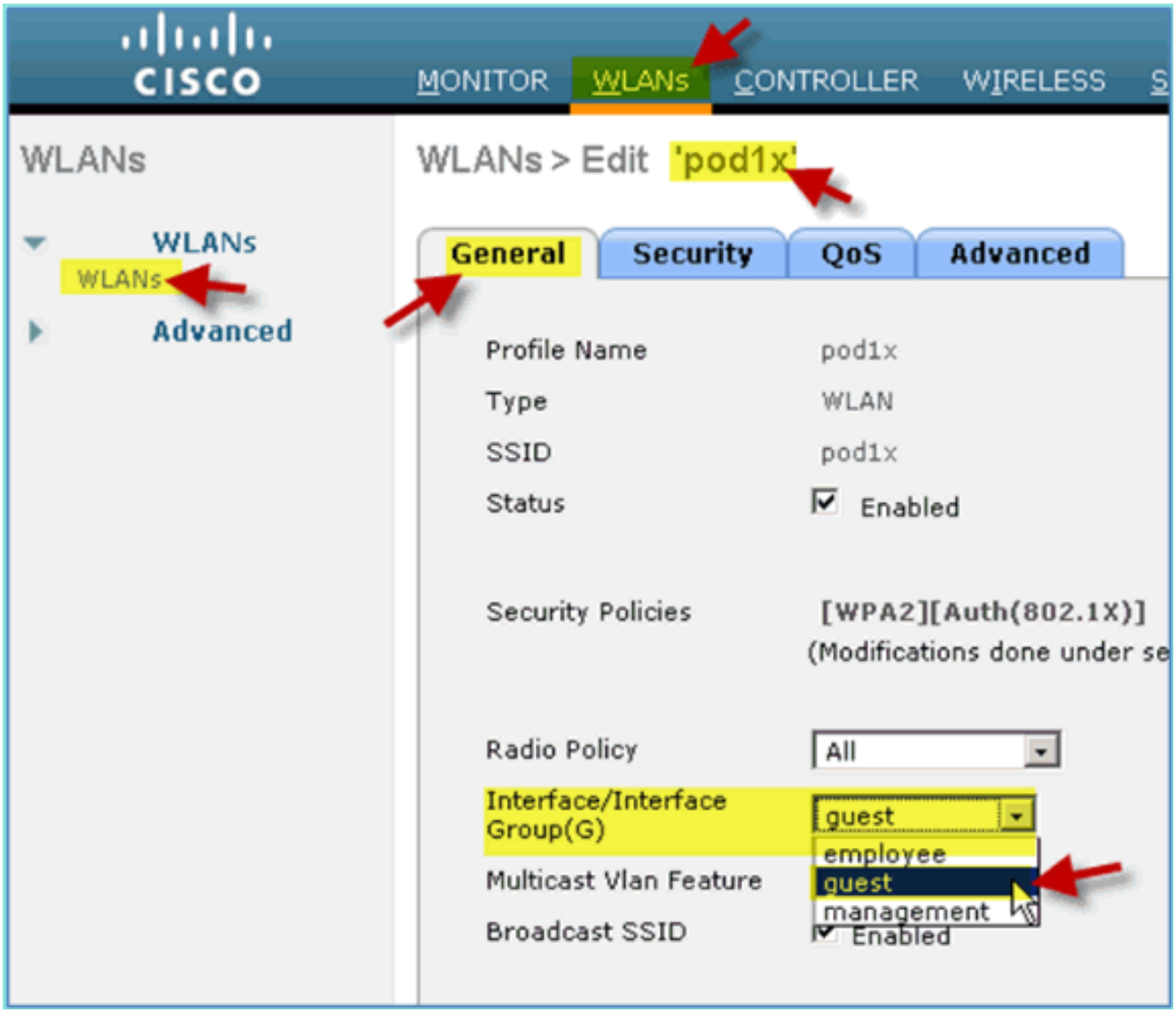
3. 올바르게 구성된 경우 디바이스는 직원 VLAN(10.10.11.0/24)에서 IP 주소를 수신합니다. 이 예에서는 새 IP 주소를 가져오는 iOS 디바이스를 보여줍니다



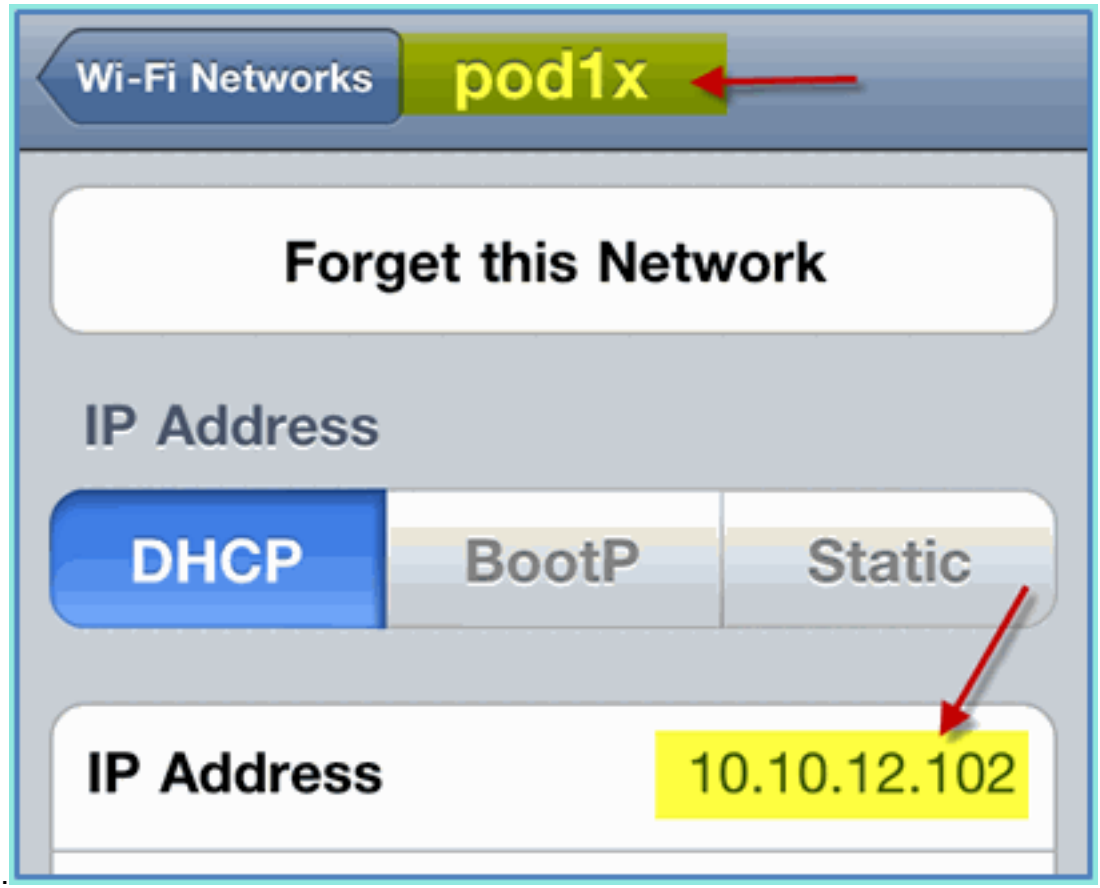
.

4. 이전 인터페이스가 확인되면 WLAN 인터페이스 할당을 Guest로 변경하고 **Apply**를 **클릭합니다**

.



5. 올바르게 구성된 경우 디바이스는 게스트 VLAN(10.10.12.0/24)에서 IP 주소를 수신합니다. 이 예에서는 새 IP 주소를 가져오는 iOS 디바이스를 보여줍니다



6. **중요:** 인터페이스 할당을 다시 원래 관리로 변경합니다.
7. Apply(**적용**)를 클릭하고 WLC에 대한 컨피그레이션을 저장합니다.

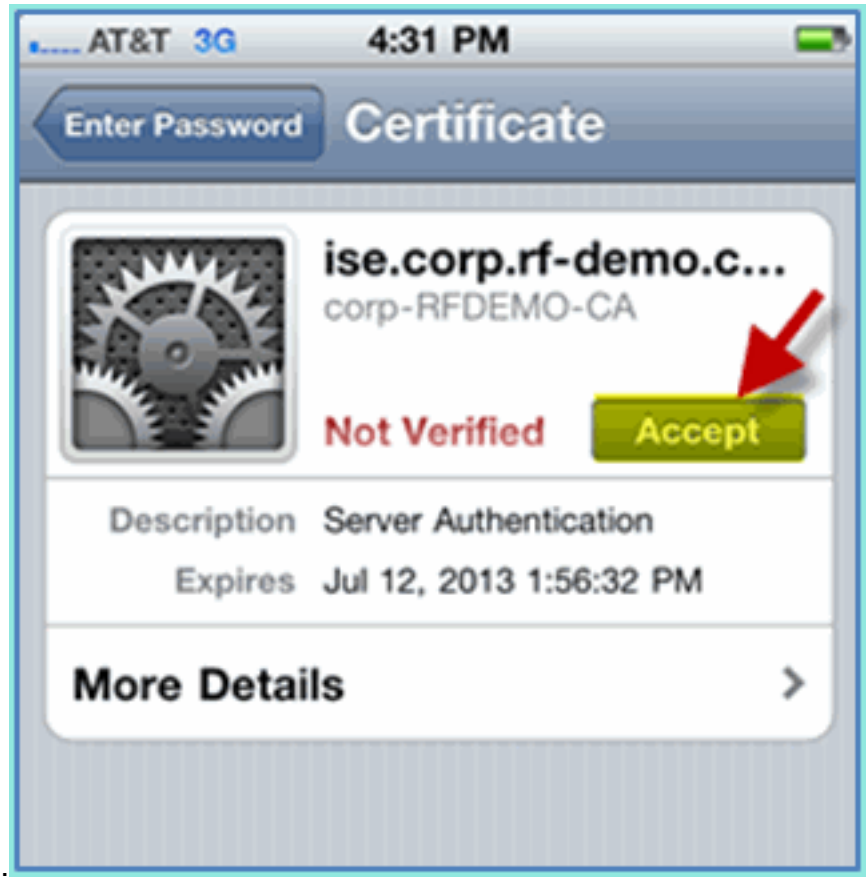
iOS(iPhone/iPad)용 무선 인증

iPhone, iPad 또는 iPod와 같은 iOS 디바이스를 사용하여 내부 사용자(또는 통합 AD 사용자)를 통해 인증된 SSID를 통해 WLC에 연결합니다. 해당되지 않는 경우 이 단계를 건너뜁니다.

1. iOS 디바이스에서 WLAN 설정으로 이동합니다. WIFI를 활성화한 다음 이전 섹션에서 생성한 802.1X 활성 SSID를 선택합니다.
2. 연결하려면 다음 정보를 제공하십시오.사용자 이름: employee (internal - Employee) 또는 contractor (internal - Contractor)비밀번호:

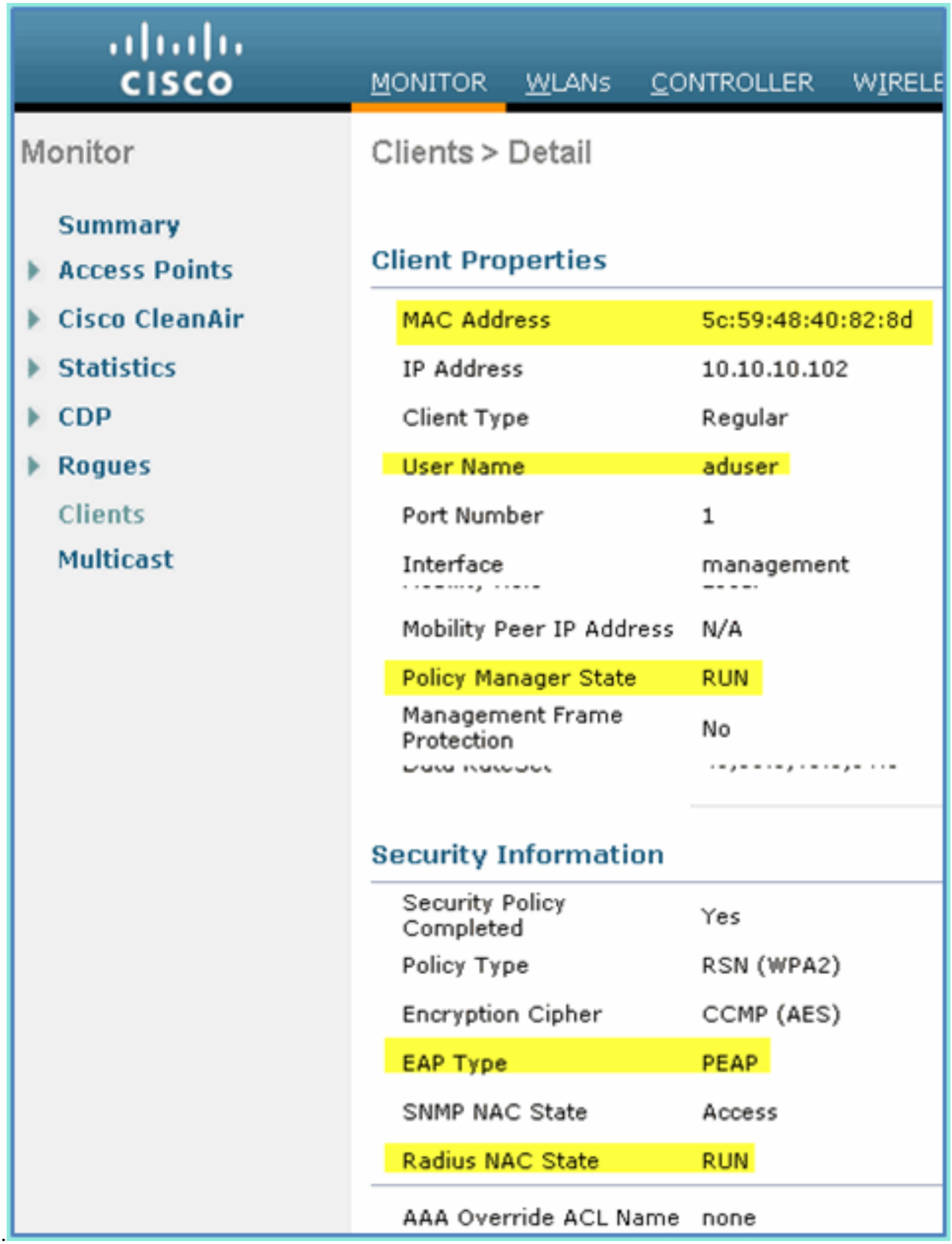
XXXX

3. ISE 인증서를 승인하려면 클릭합니다



4. iOS 디바이스가 관리(VLAN10) 인터페이스에서 IP 주소를 가져오고 있는지 확인합니다

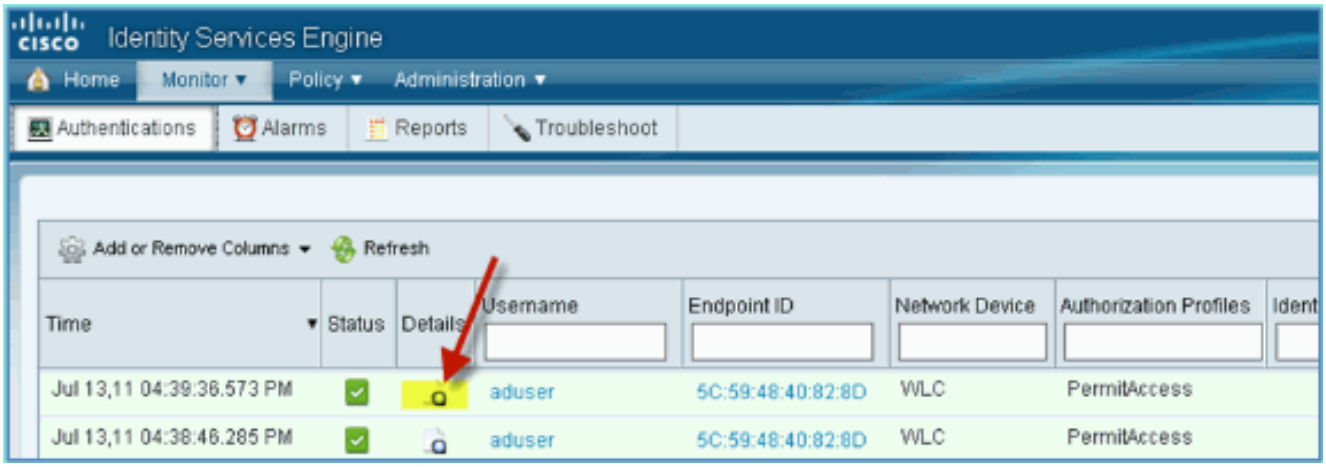
5. WLC > Monitor > Clients에서 사용, 상태 및 EAP 유형을 비롯한 엔드포인트 정보를 확인합니



다.

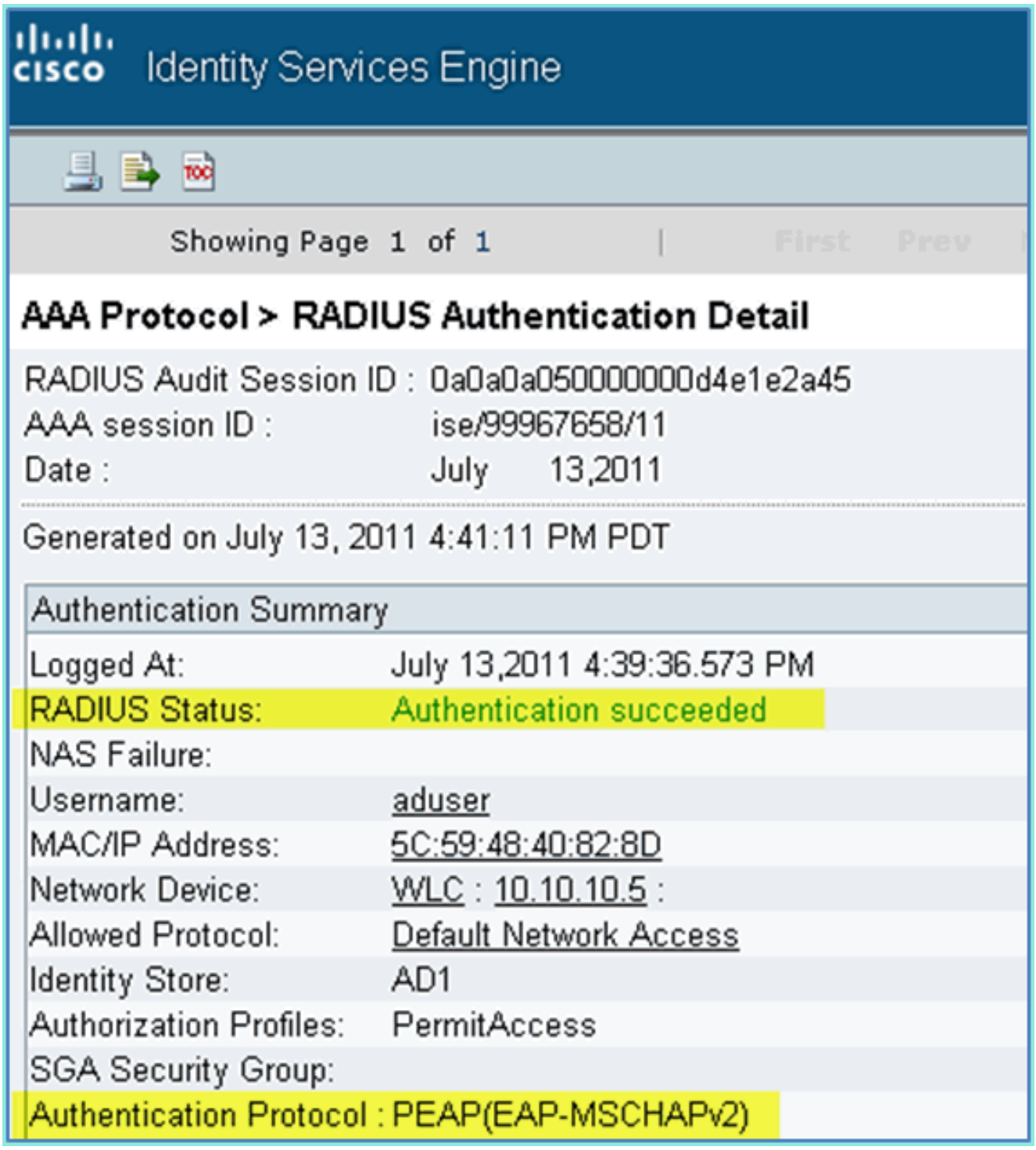
6. 마찬가지로 클라이언트 정보는 ISE > Monitor > Authentication 페이지에서 제공할 수 있습니다

.



7. 세션에 대한 자세한 정보를 보려면 **Details**(세부사항) 아이콘을 클릭합니다

.



WLC에 포스처 리디렉션 ACL 추가

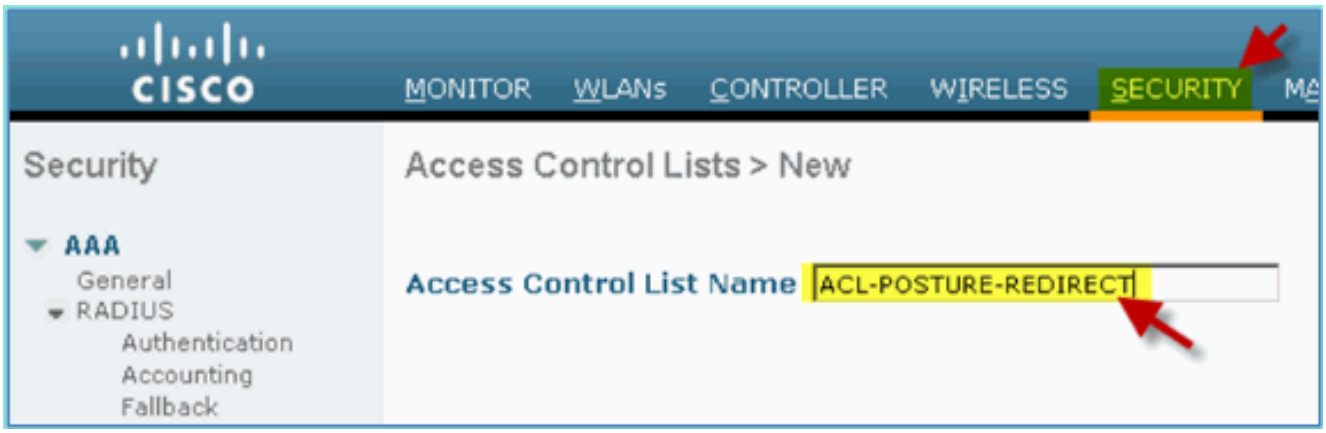
Posture 리디렉션 ACL은 ISE가 포스처에 대한 클라이언트를 제한하는 데 사용하는 WLC에서 구성됩니다. ACL은 ISE 간의 트래픽을 효과적으로 그리고 최소한 허용합니다. 필요한 경우 이 ACL에 선택적 규칙을 추가할 수 있습니다.

1. WLC > **Security > Access Control Lists > Access Control Lists**로 이동합니다. **새로 만들기**를 클릭합니다

.

2. ACL에 대한 이름(ACL-POSTURE-REDIRECT)을 제공합니다

.



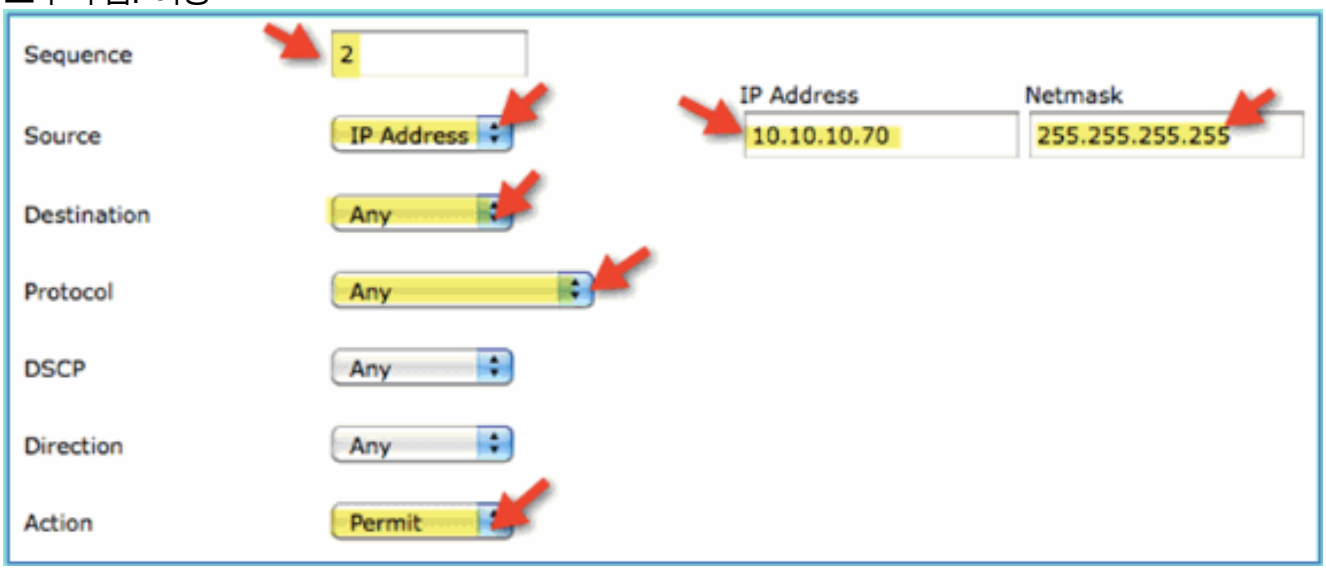
3. 새 **ACL에** 대한 **Add** New Rule을 클릭합니다. 다음 값을 ACL 시퀀스 값으로 #1. 완료되면 **Apply(적용)**를 클릭합니다.출처: Any대상: IP 주소 10.10.10.70, 255.255.255.255프로토콜: 모두작업: 허용

4. 시퀀스가 추가되었는지 확인합니다

.

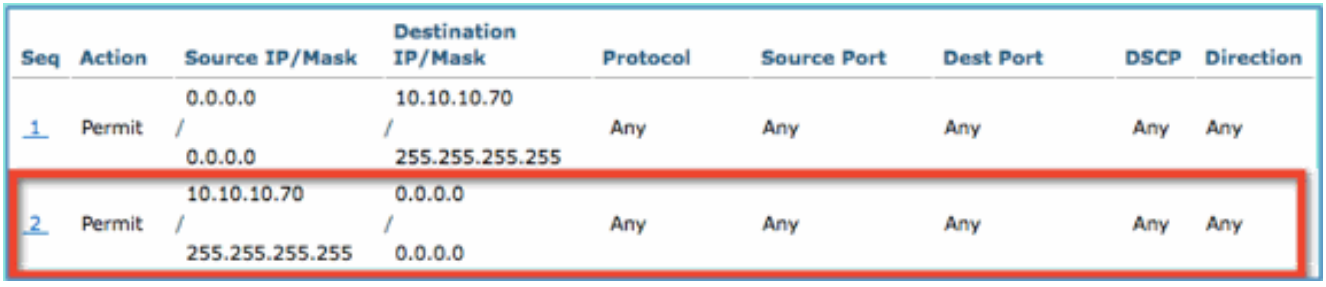
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. Add **New Rule을 클릭합니다**. 다음 값을 ACL 시퀀스 값으로 #2. 완료되면 **Apply(적용)**를 클릭합니다.출처: IP Address 10.10.10.70, 255.255.255.255Destination(대상): Any(모두)프로토콜: 모두작업: 허용



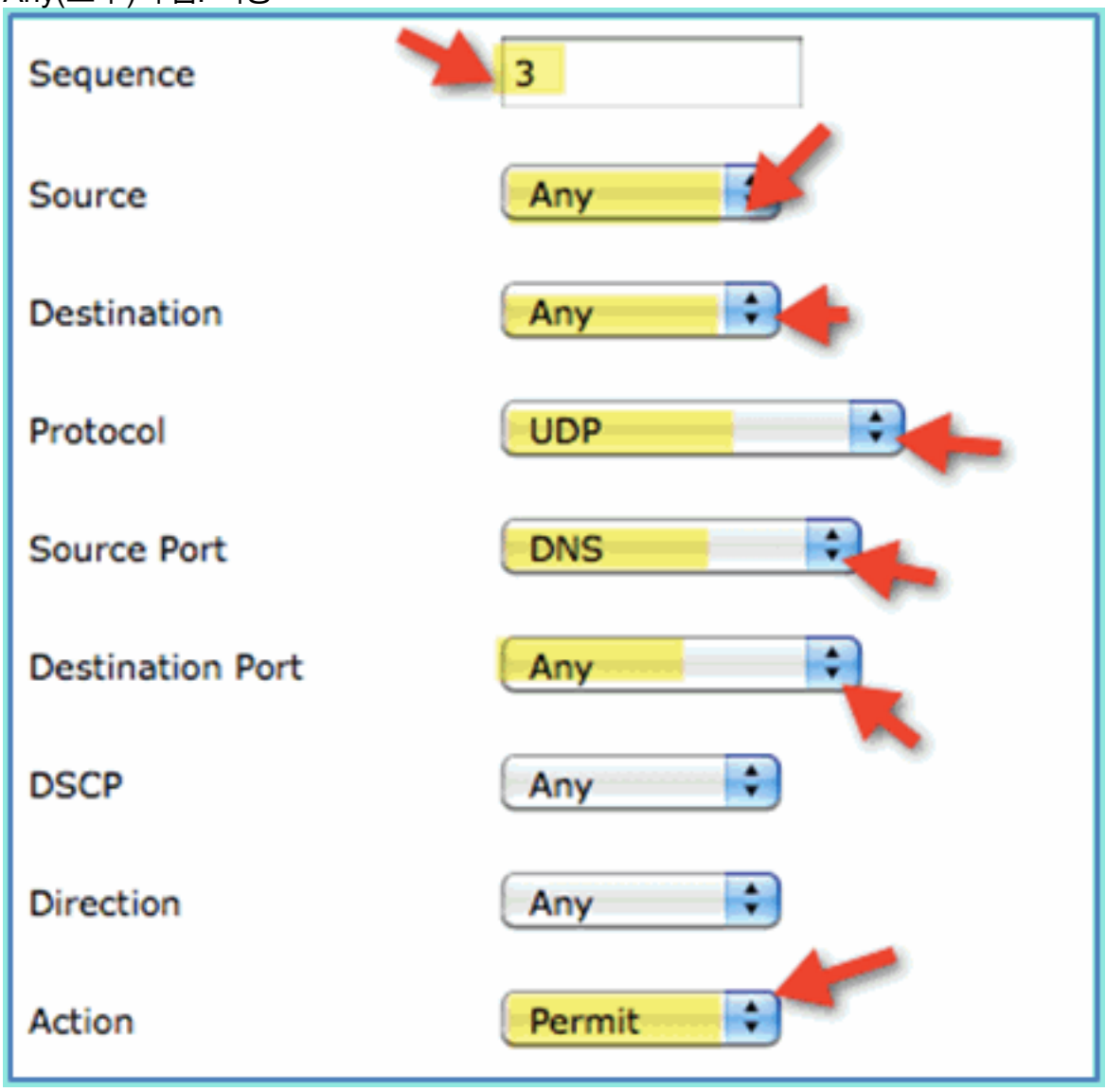
6. 시퀀스가 추가되었는지 확인합니다

.



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any

7. 다음 값을 ACL 시퀀스 값으로 #3. 완료되면 **Apply(적용)**를 클릭합니다.출처: AnyDestination(대상): Any(모두)프로토콜: UDP소스 포트: DNSDestination Port(대상 포트): Any(모두)작업: 허용

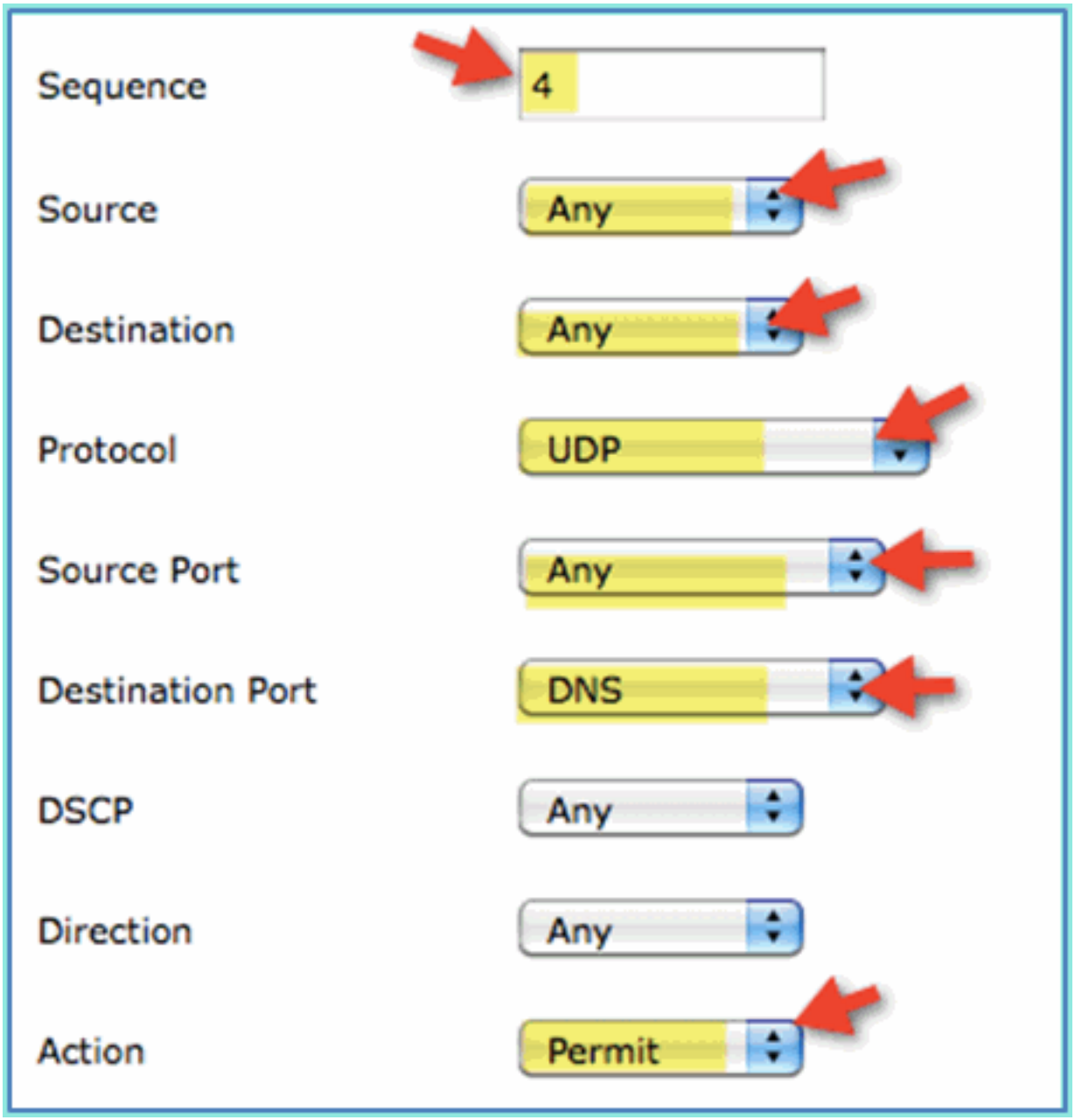


8. 시퀀스가 추가되었는지 확인합니다

.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any

9. Add **New Rule을 클릭합니다**. 다음 값을 ACL 시퀀스 값으로 #4. 완료되면 **Apply(적용)**를 클릭합니다.출처: AnyDestination(대상): Any(모두)프로토콜: UDP소스 포트: 모두대상 포트: DNS작업: 허용



10. 시퀀스가 추가되었는지 확인합니다

.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any
2	Permit	10.10.10.70 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any

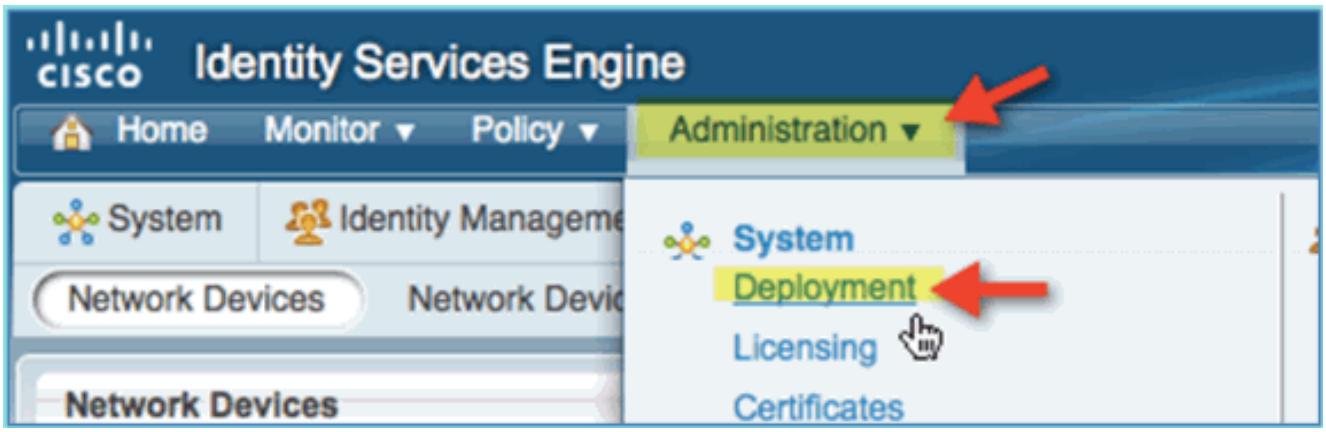
11. 현재 WLC 컨피그레이션을 저장합니다.

ISE에서 프로파일링 프로브 활성화

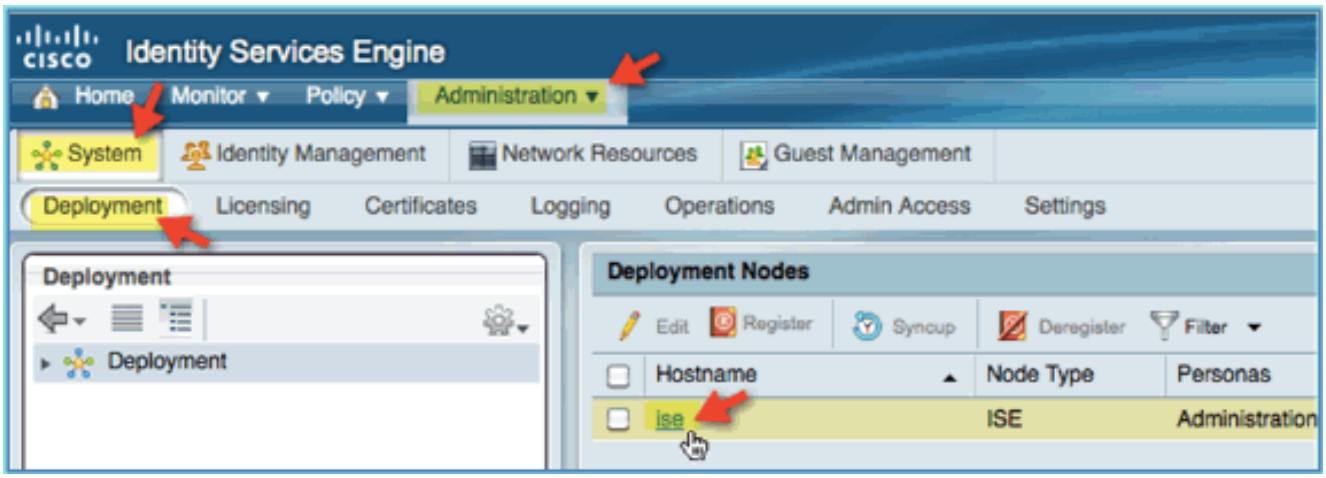
ISE는 엔드포인트를 효과적으로 프로파일링하기 위한 프로브로 구성해야 합니다. 기본적으로 이러

한 옵션은 비활성화되어 있습니다. 이 섹션에서는 ISE를 프로브로 구성하는 방법을 보여줍니다.

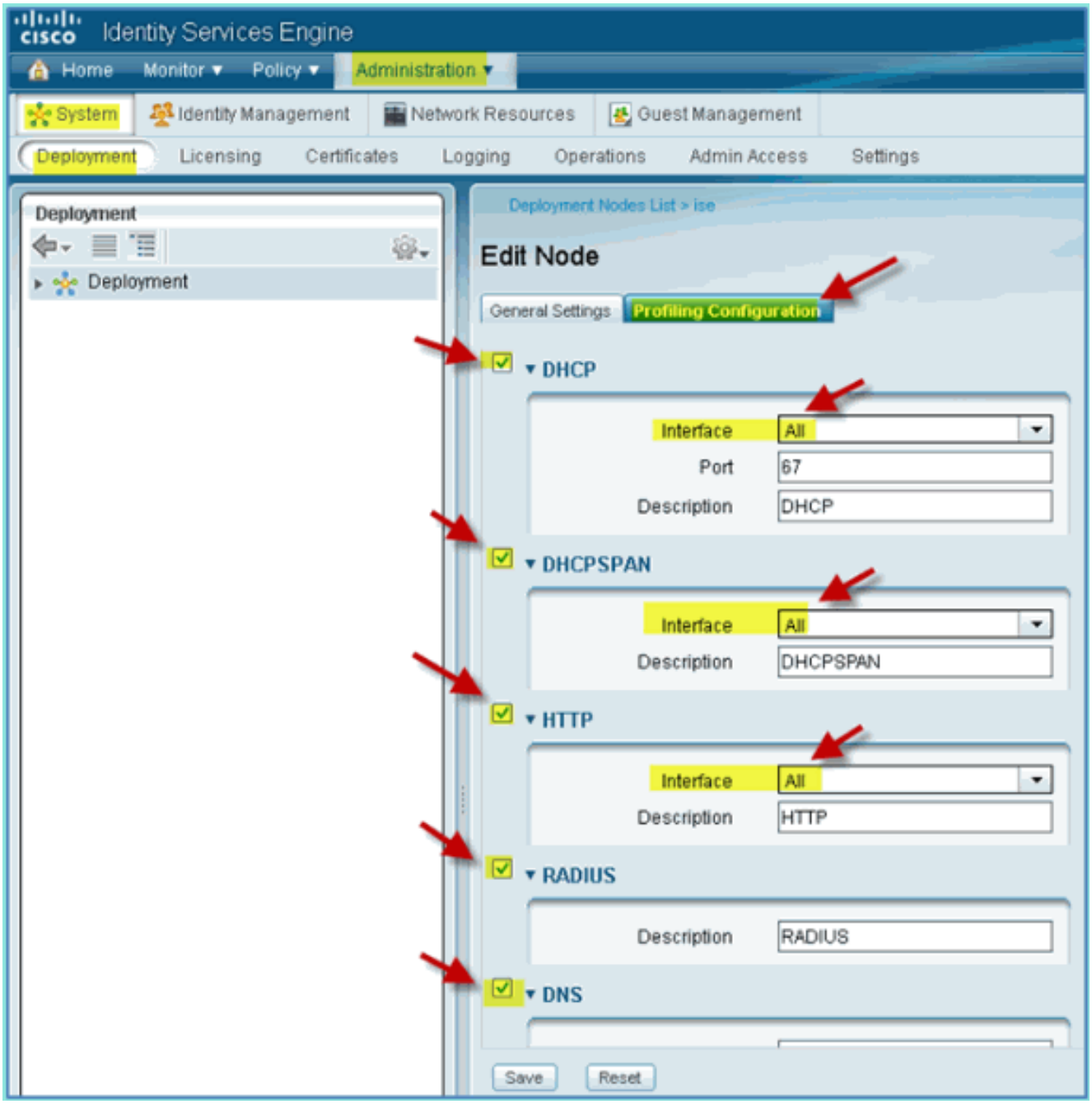
1. ISE 관리에서 Administration(관리) > **System(시스템) > Deployment(구축)로 이동합니다**
.



2. **ISE를 선택합니다**. Edit ISE **host(ISE 호스트 수정)를** 클릭합니다
.

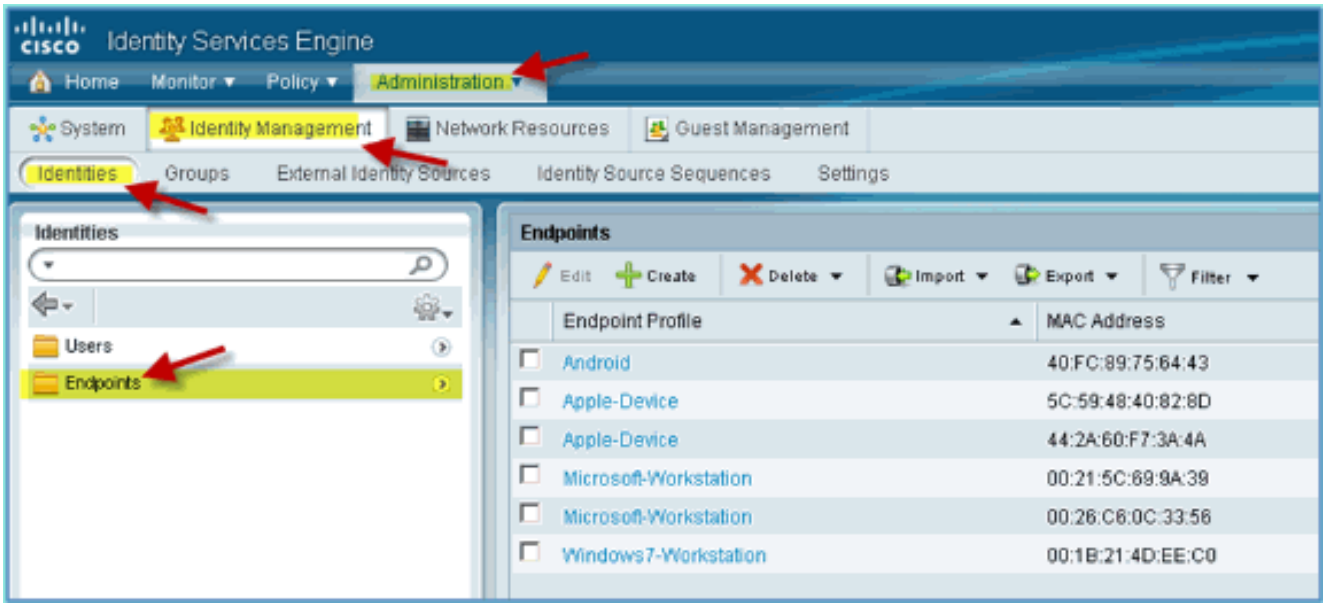


3. Edit Node(노드 수정) 페이지에서 Profiling Configuration(프로파일링 컨피그레이션)을 선택하고 다음을 구성합니다.DHCP: Enabled(활성화됨), All(모두)(또는 기본값)DHCPSPAN: Enabled, All(또는 기본값)HTTP: Enabled, All(또는 기본값)RADIUS: Enabled(활성화됨), N/ADNS: 사용, 해당 없음



4. 디바이스(iPhone/iPad/Droids/Mac 등)를 다시 연결합니다.
5. ISE 엔드포인트 ID를 확인합니다. Administration(관리) **> Identity Management(ID 관리) > Identities(ID)로 이동합니다**. 프로파일링된 항목을 나열하려면 Endpoints(엔드포인트)를 클릭합니다.**참고:** 초기 프로파일링은 RADIUS 프로브에서 가져옵니다

.

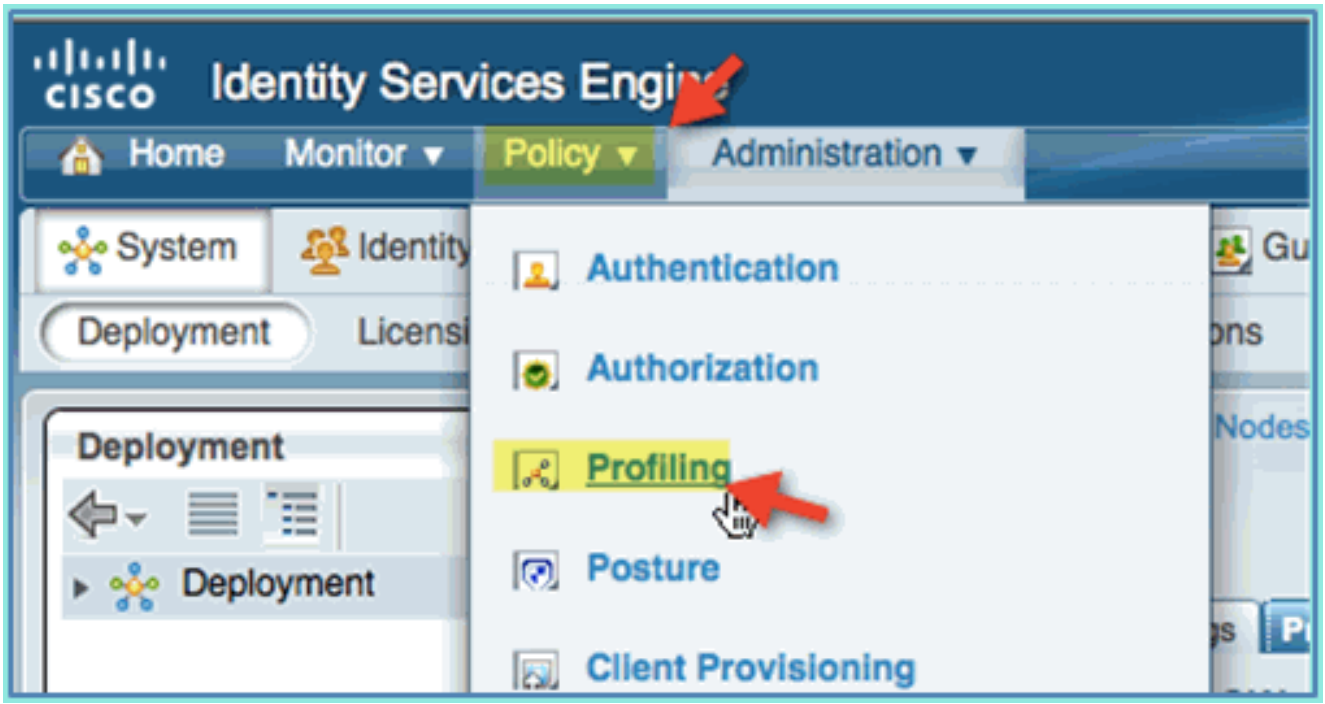


디바이스에 대한 ISE 프로파일 정책 활성화

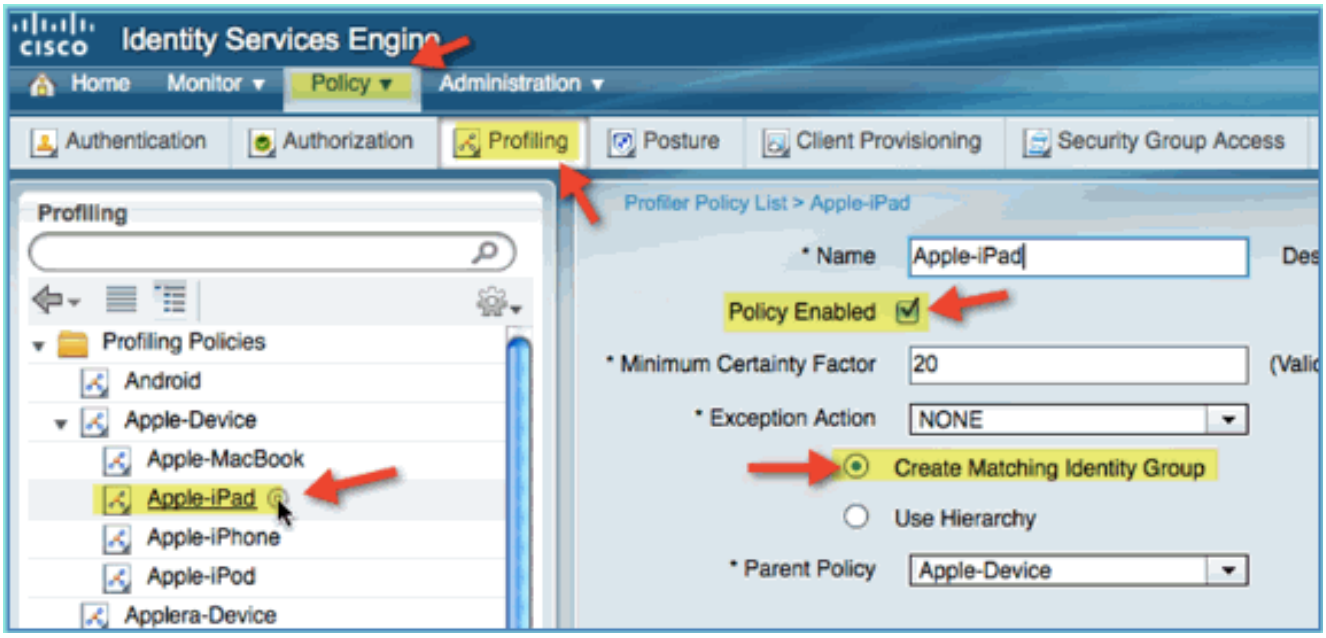
기본적으로 ISE는 다양한 엔드포인트 프로필의 라이브러리를 제공합니다. 디바이스에 대한 프로파일을 활성화하려면 다음 단계를 완료하십시오.

1. ISE에서 Policy(정책) **> Profiling(프로파일링)으로 이동합니다**

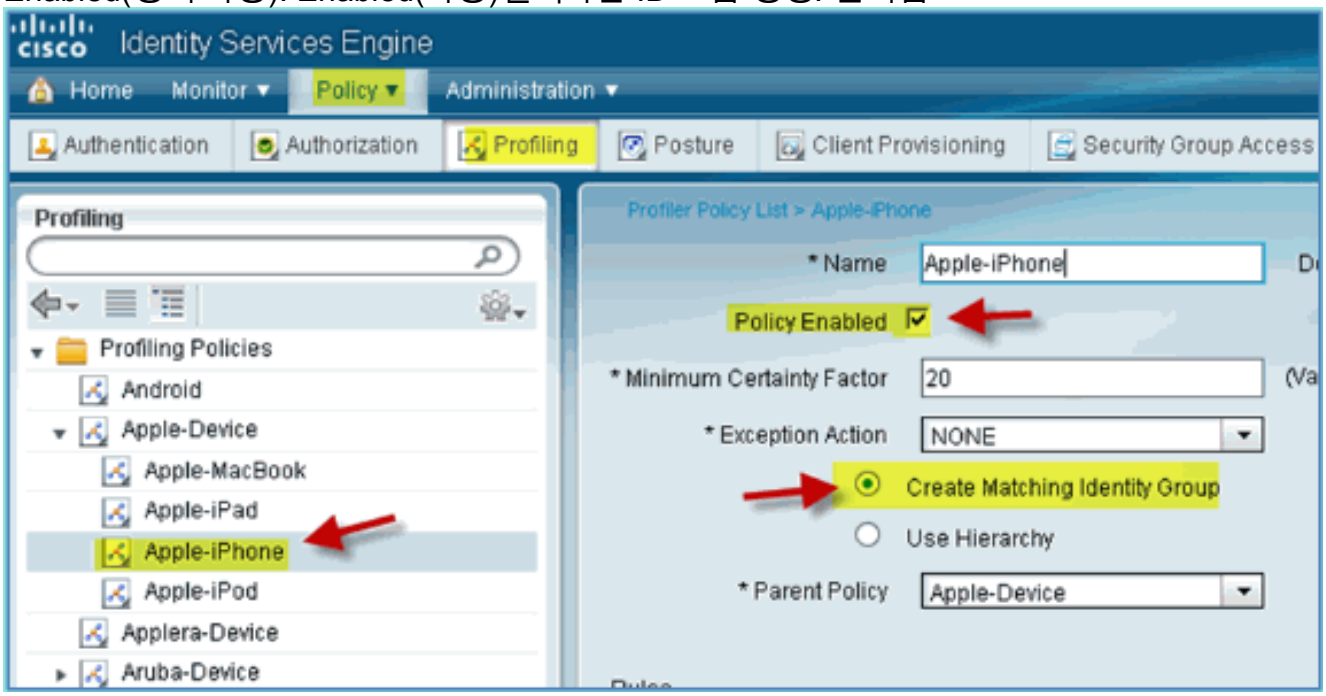
.



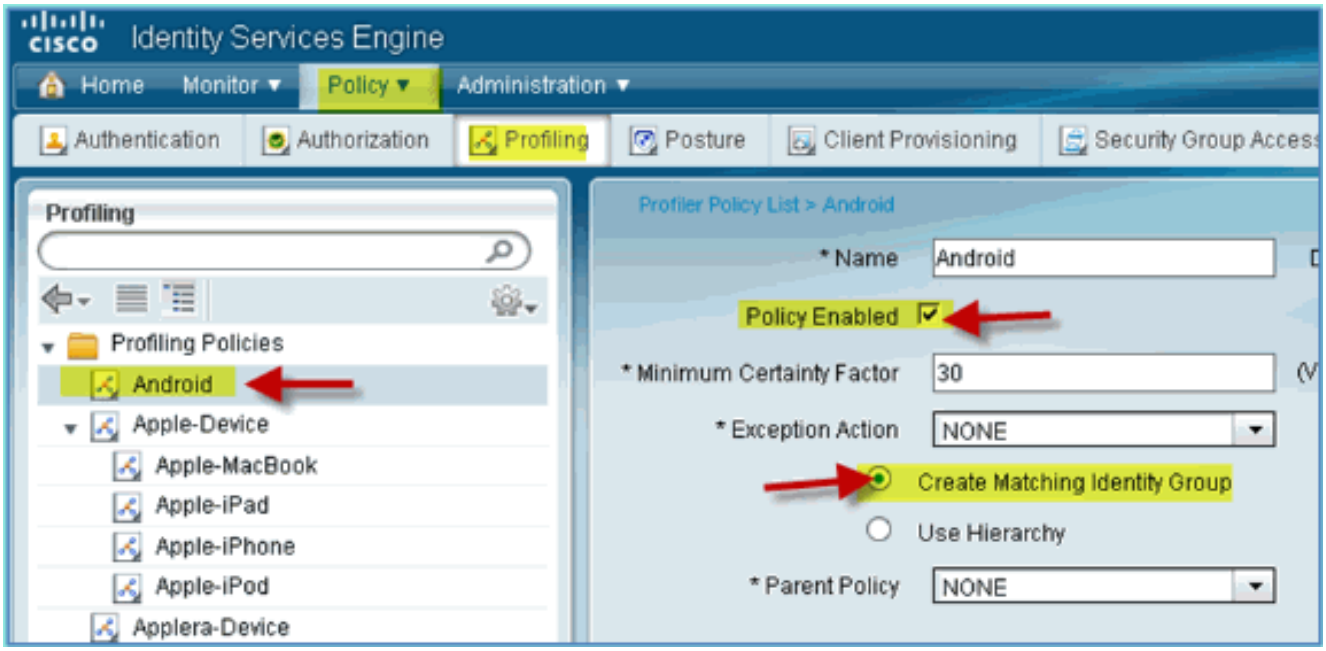
2. 왼쪽 창에서 Profiling Policies(프로파일링 정책)**를 확장합니다**.
3. Apple **Device(Apple 디바이스) > Apple iPad(Apple iPad)**를 클릭하고 다음을 설정합니다 .Policy Enabled(정책 사용): Enabled(사용)일치하는 ID 그룹 생성: 선택됨



4. Apple **Device(Apple 디바이스) > Apple iPhone**을 클릭하고 다음을 설정합니다.Policy Enabled(정책 사용): Enabled(사용)일치하는 ID 그룹 생성: 선택됨



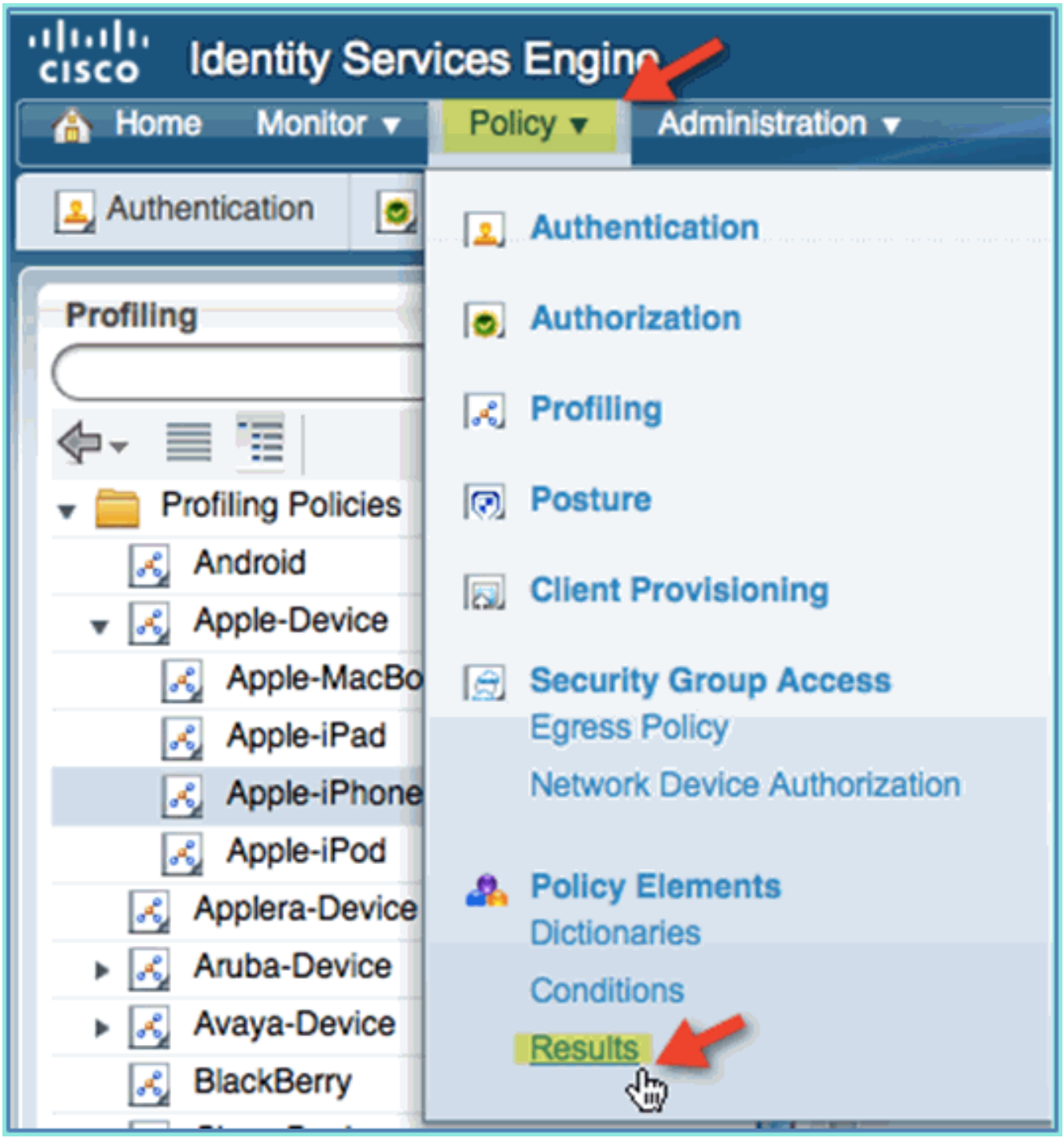
5. Android를 클릭하고 다음을 설정합니다.Policy Enabled(정책 사용): Enabled(사용)일치하는 ID 그룹 생성: 선택됨



상태 검색 리디렉션을 위한 ISE 권한 부여 프로파일

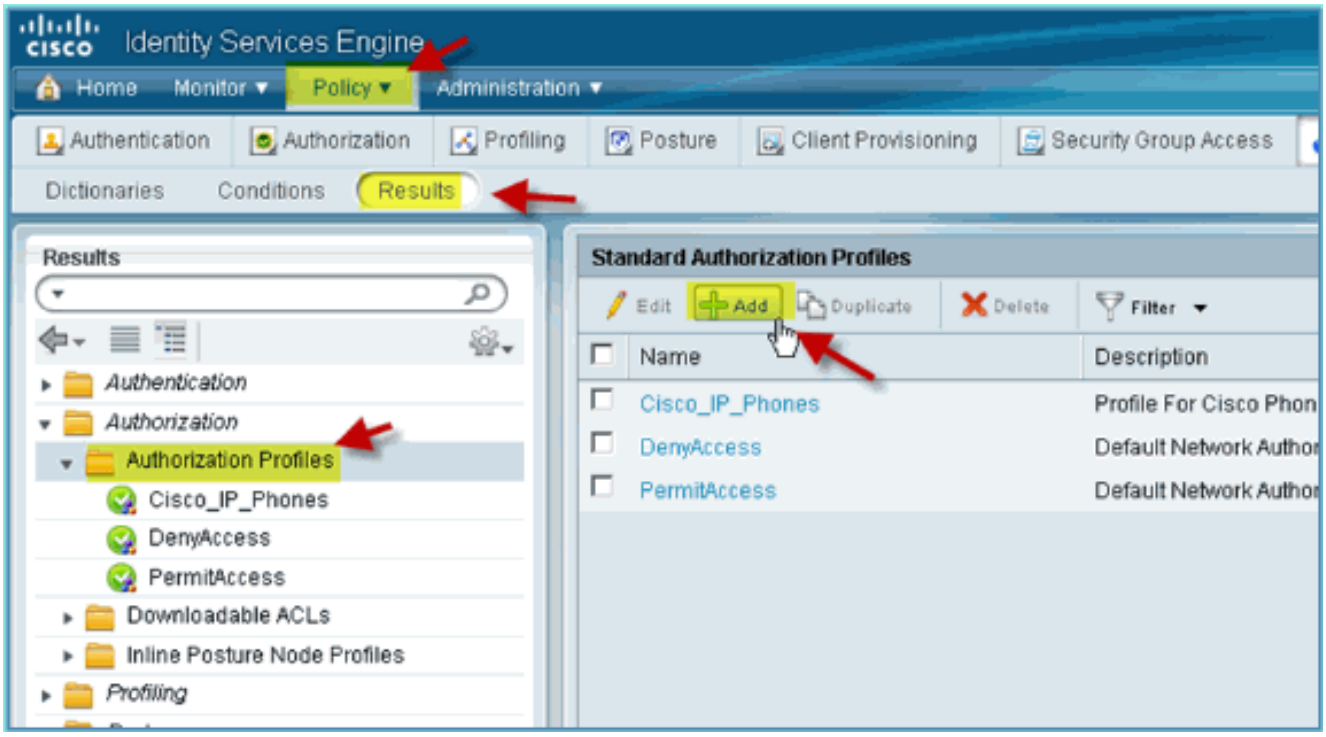
권한 부여 정책 상태 리디렉션을 구성하려면 다음 단계를 완료하면 새 디바이스를 ISE로 리디렉션하여 적절한 검색 및 프로파일링을 수행할 수 있습니다.

1. ISE에서 Policy(정책) > Policy Elements(**정책 요소) > Results(결과)로 이동합니다**
   .

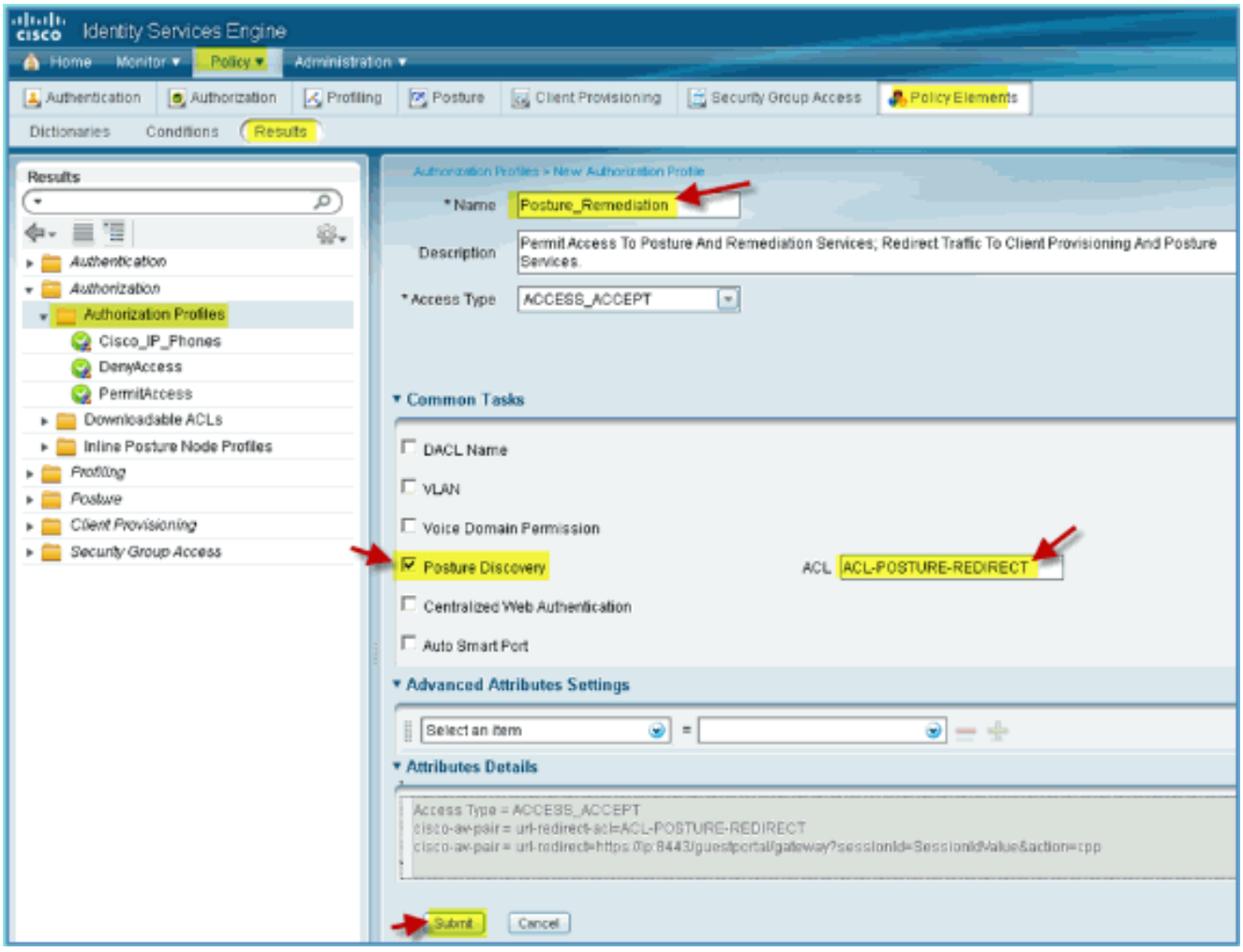


2. Authorization(권한 부여)**을 확장합니다**. Authorization **Profiles**(권한 부여 프로파일)(왼쪽 창)를 클릭하고 Add(추가)**를 클릭합니다**

.

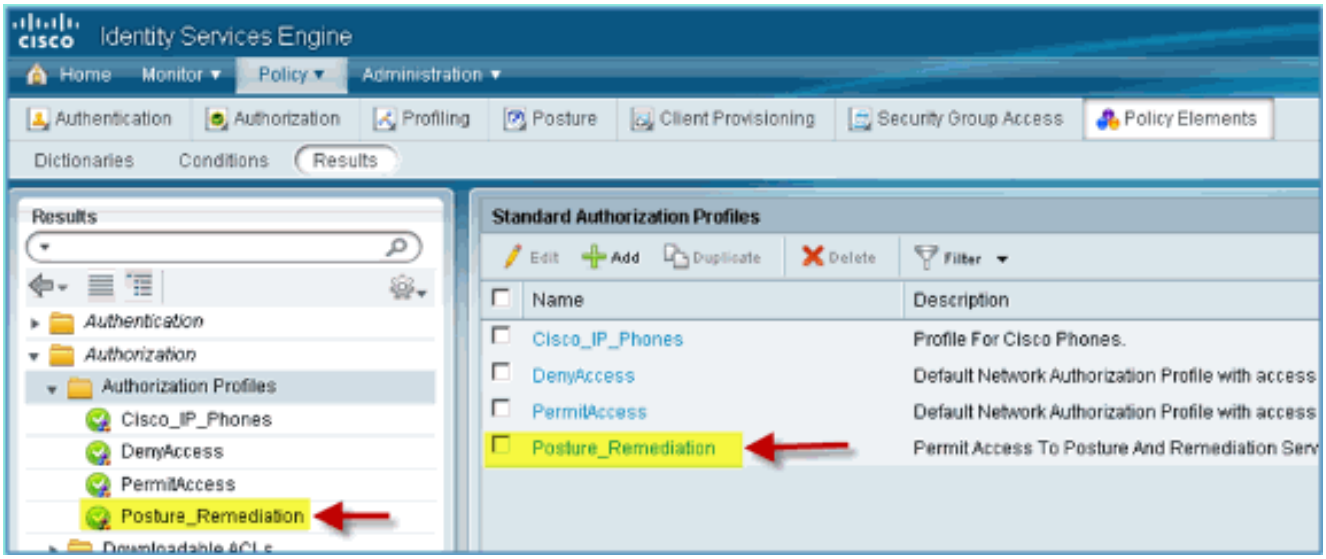


3. 다음을 사용하여 권한 부여 프로파일을 생성합니다.이름: Posture_Remediation액세스 유형: Access_Accept공통 툴:상태 검색, 활성화됨포스처 검색, ACL ACL-POSTURE-REDIRECT



4. Submit(**제출**)을 클릭하여 이 작업을 완료합니다.
5. 새 권한 부여 프로파일이 추가되었는지 확인합니다

.

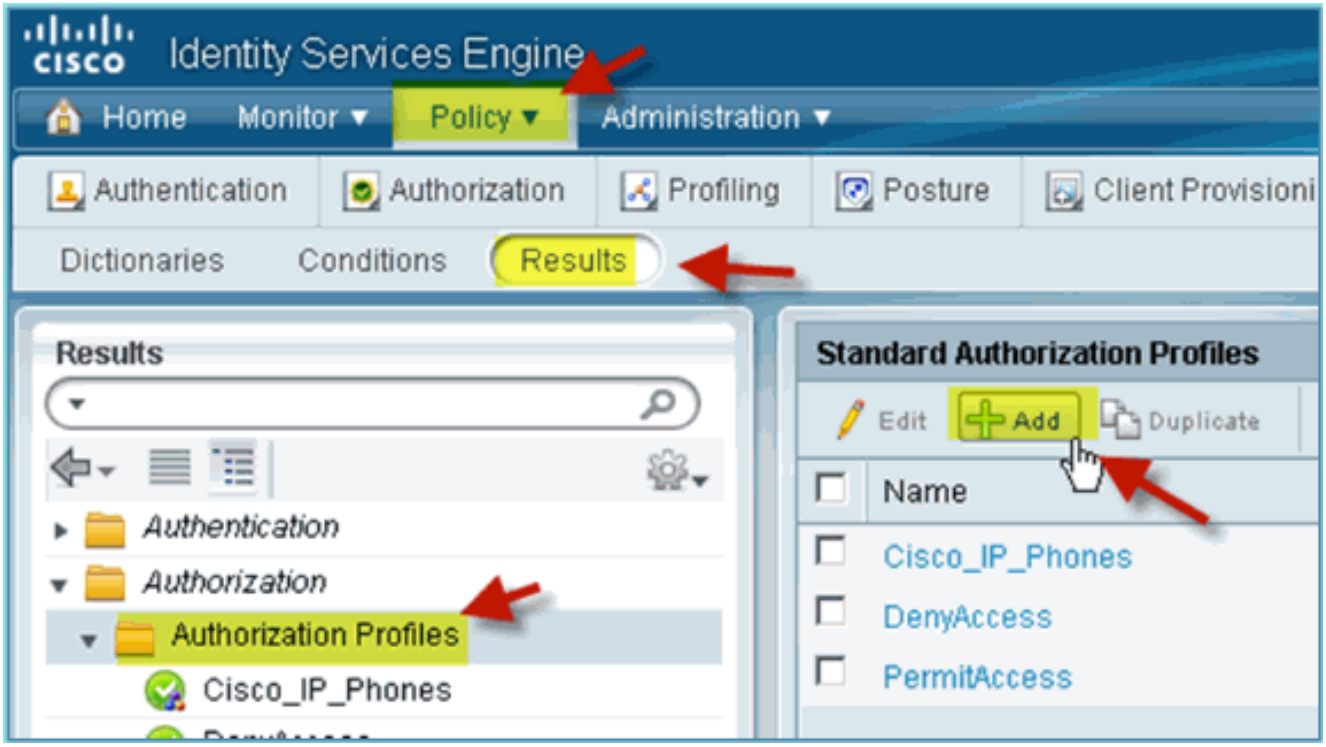


직원을 위한 ISE 권한 부여 프로파일 생성

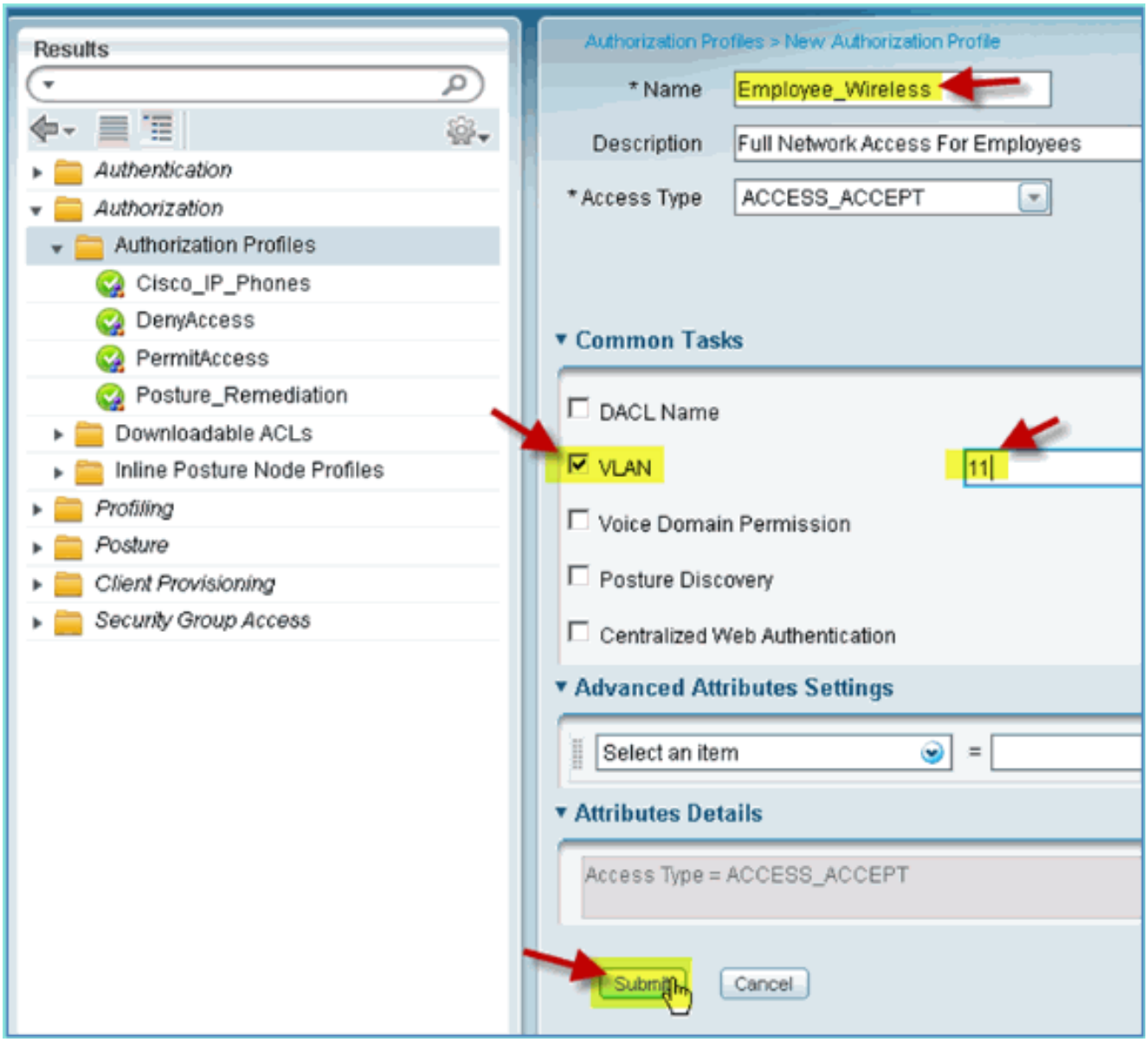
직원을 위한 권한 부여 프로파일을 추가하면 ISE에서 할당된 특성으로 액세스를 인증하고 허용할 수 있습니다. 이 경우 직원 VLAN 11이 할당됩니다.

다음 단계를 완료하십시오.

1. ISE에서 Policy(정책) **> Results(결과)로 이동합니다**. Authorization(**권한 부여**)을 확장한 다음 Authorization Profiles(권한 **부여 프로파일**)를 클릭하고 Add(추가)**를 클릭합니다**
.

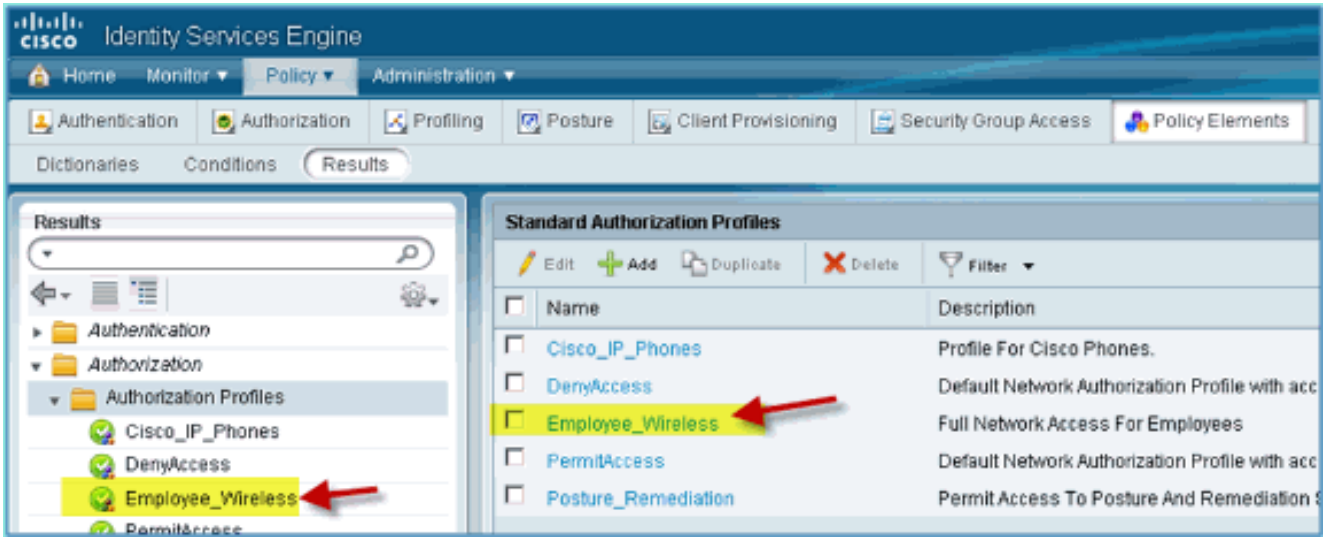


2. 사원 승인 프로파일에 대해 다음을 입력합니다.이름: Employee_Wireless일반 작업:VLAN, 활성화됨VLAN, 하위 값 11
3. Submit(**제출**)을 클릭하여 이 작업을 완료합니다
.



4. 새 직원 권한 부여 프로파일이 생성되었는지 확인합니다

.

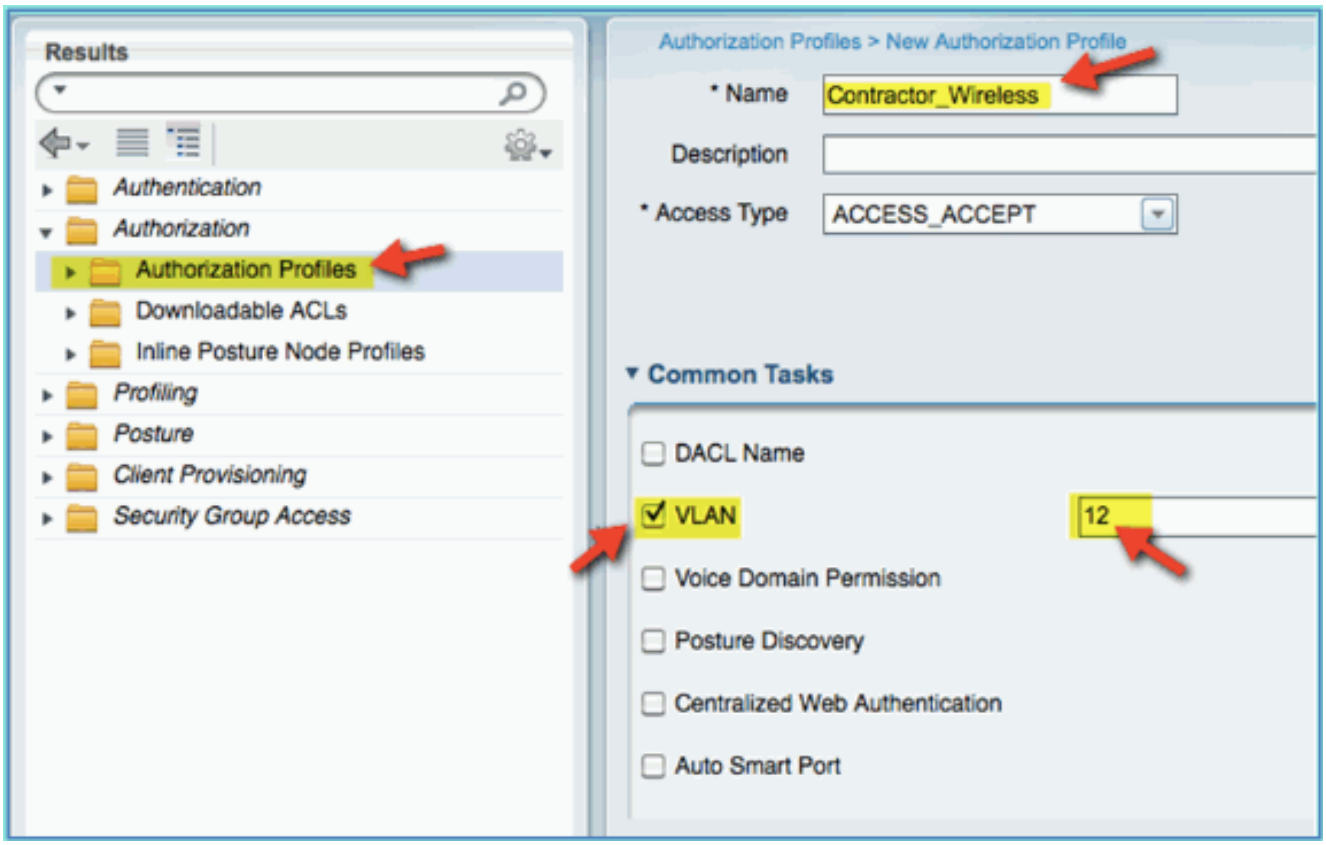


계약자에 대한 ISE 권한 부여 프로파일 생성

계약자에 대한 권한 부여 프로파일을 추가하면 ISE에서 할당된 특성으로 액세스를 인증하고 허용할 수 있습니다. 이 경우 계약자 VLAN 12가 할당됩니다.

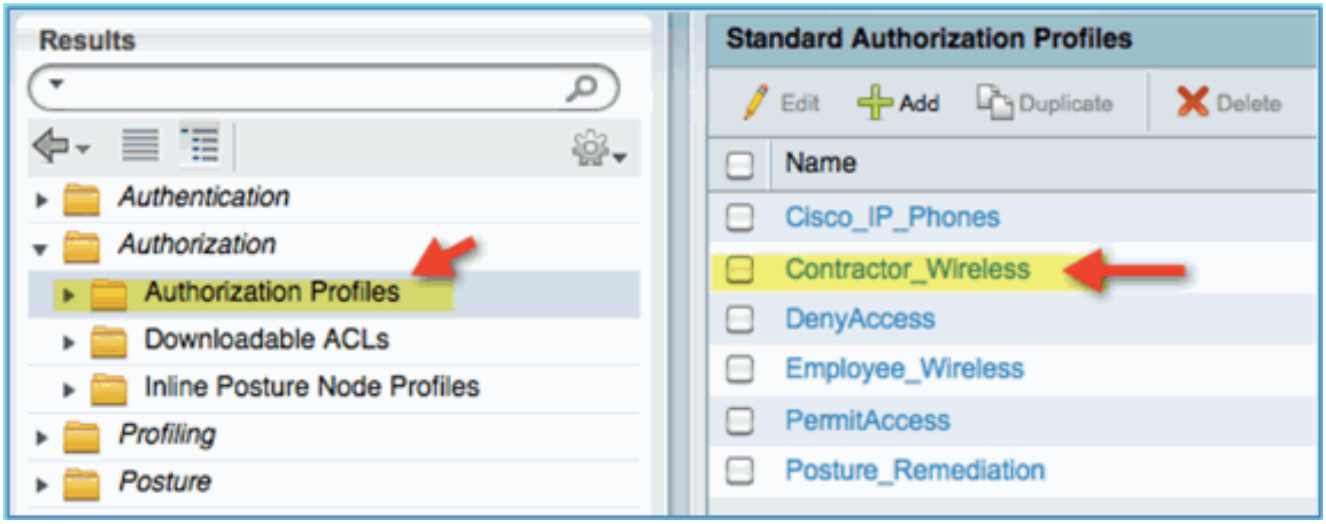
다음 단계를 완료하십시오.

1. ISE에서 Policy(정책) **> Results(결과)로 이동합니다**. Authorization(**권한 부여**)을 확장한 다음 Authorization Profiles(권한 **부여 프로파일**)를 클릭하고 Add(추가)**를 클릭합니다**.
2. 사원 승인 프로파일에 대해 다음을 입력합니다.이름: Employee_Wireless일반 작업:VLAN, 활성화됨VLAN, 하위 값
   12



3. Submit(**제출**)을 클릭하여 이 작업을 완료합니다.
4. 계약자 권한 부여 프로파일이 생성되었는지 확인합니다

.



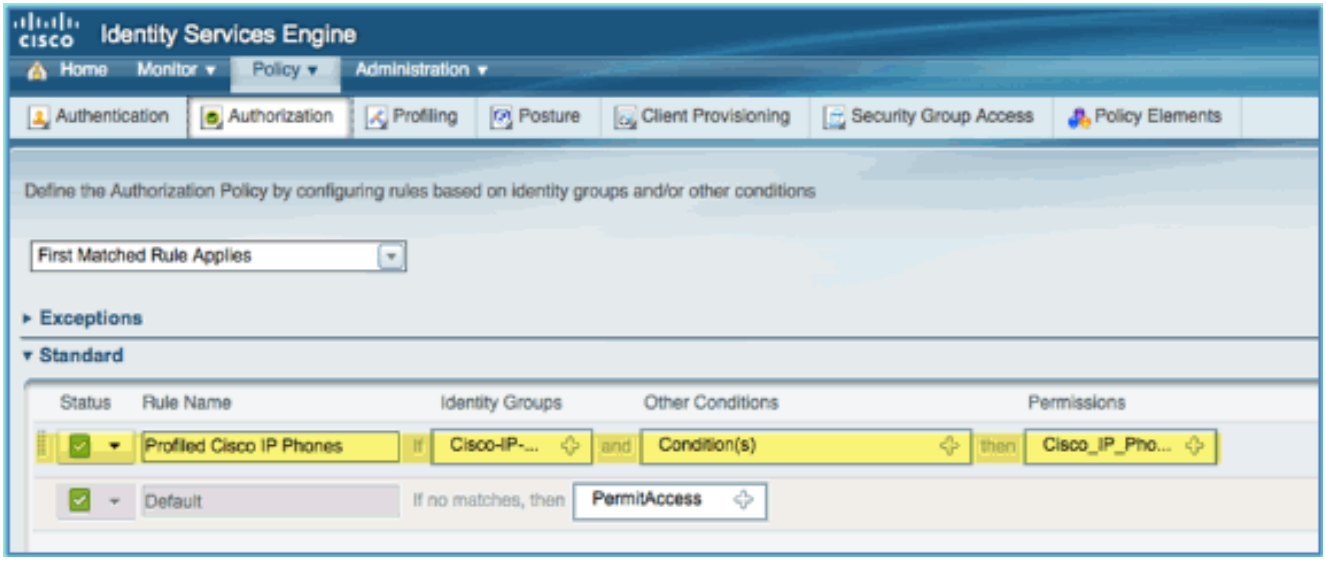
디바이스 상태/프로파일링에 대한 권한 부여 정책

새 디바이스가 네트워크에 처음 연결되면 관리자는 새 디바이스에 대해 알려진 정보가 거의 없으며 , 액세스를 허용하기 전에 알 수 없는 엔드포인트를 식별할 수 있도록 적절한 정책을 생성합니다. 이 연습에서는 새 디바이스가 상태 평가를 위해 ISE로 리디렉션되도록 권한 부여 정책이 생성됩니다

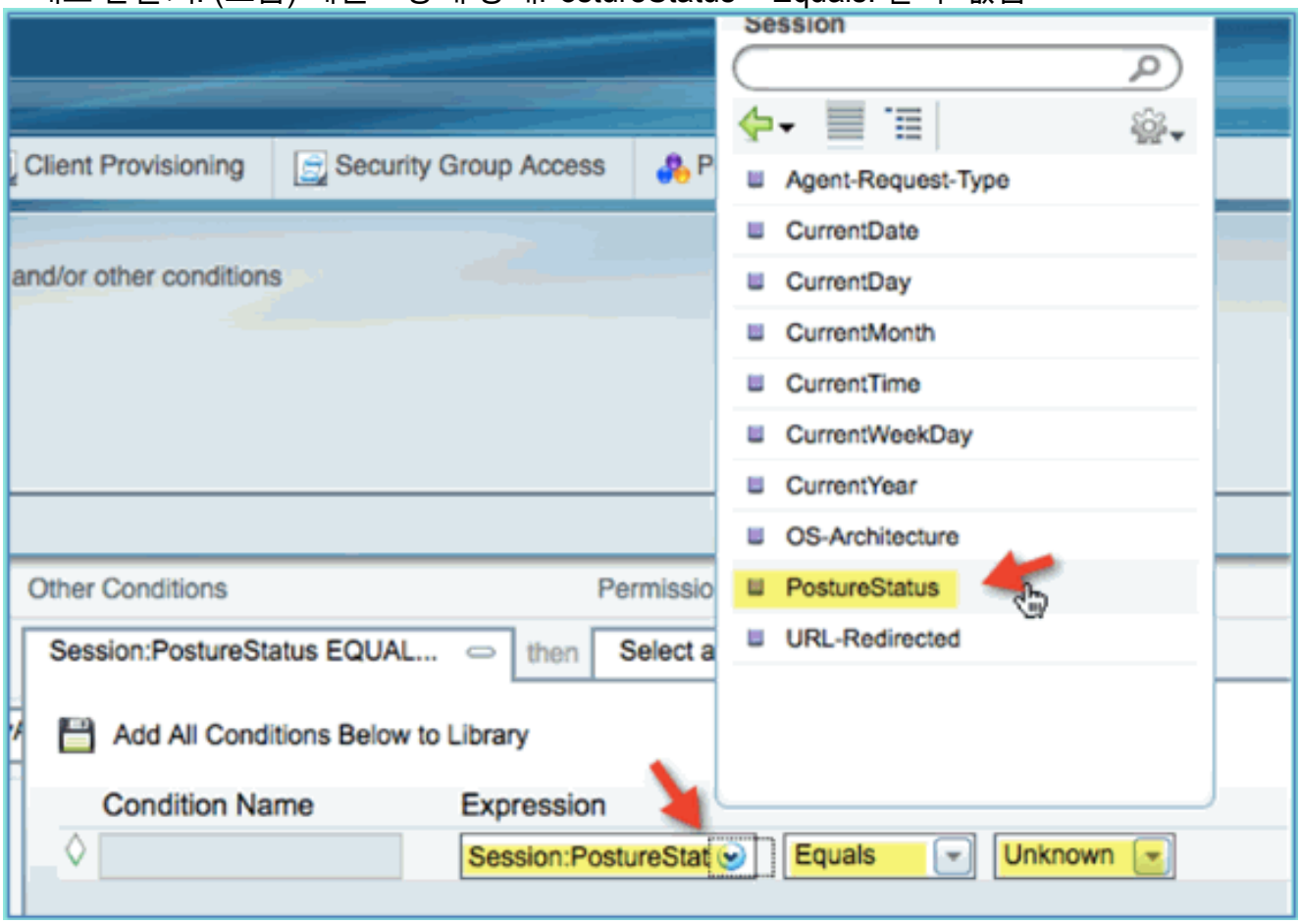
(모바일 디바이스의 경우 에이전트가 없으므로 프로파일링만 관련됨). 엔드포인트는 ISE 종속 포털로 리디렉션되고 식별됩니다.

다음 단계를 완료하십시오.

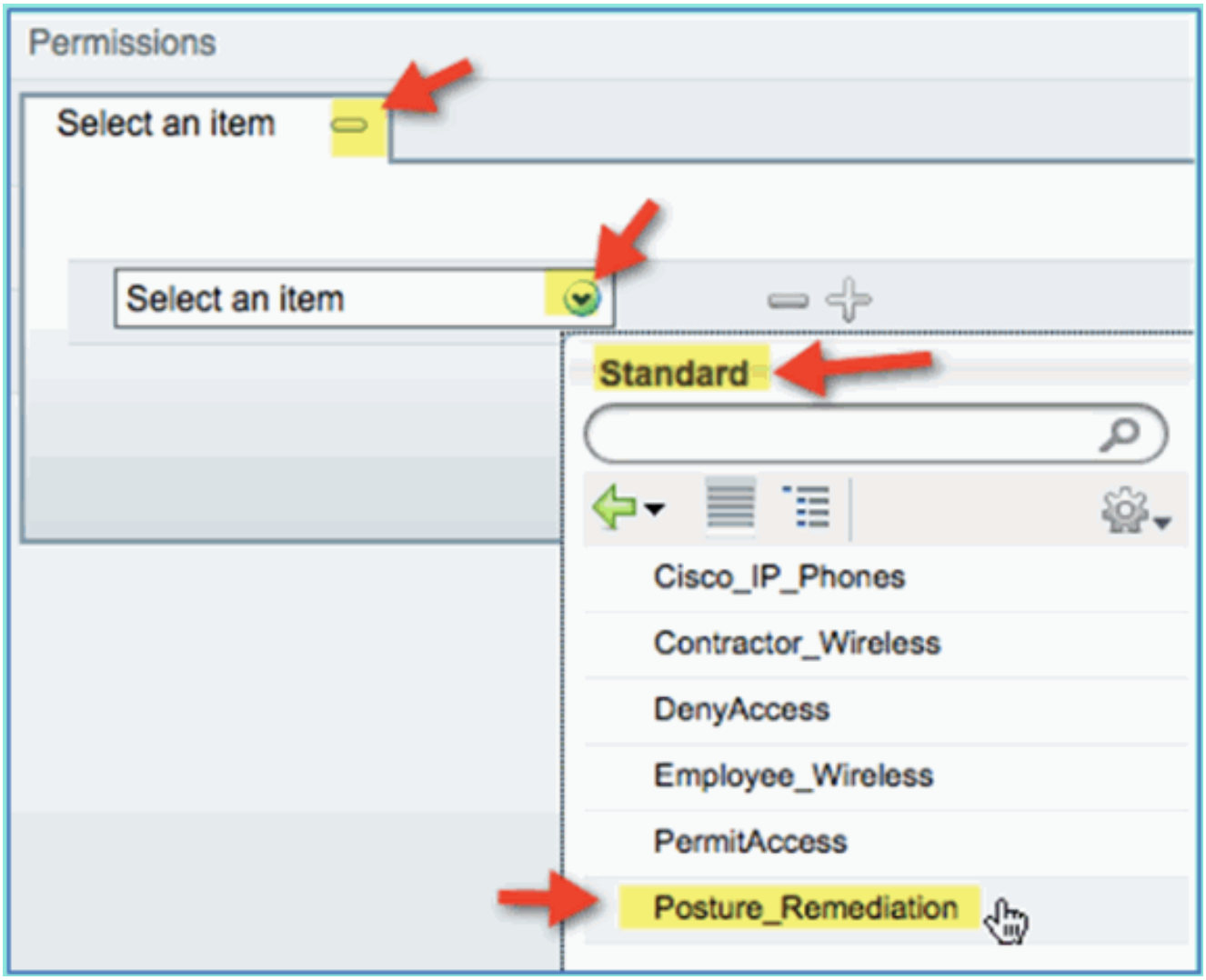
1. ISE에서 Policy(**정책) > Authorization(권한 부여)**으로 **이동합니다**
.



2. 프로파일링된 Cisco IP Phone에 대한 정책이 있습니다. 이건 기성복이에요. 이 정책을 상태 정책으로 수정합니다.
3. 이 정책에 대해 다음 값을 입력합니다.규칙 이름: Posture_RemediationID 그룹: 모두기타 조건 > 새로 만들기: (고급) 세션 > 상태 상태PostureStatus > Equals: 알 수 없음



4. 사용 권한에 대해 다음을 설정합니다.Permissions(권한) > Standard(표준): Posture_Remediation

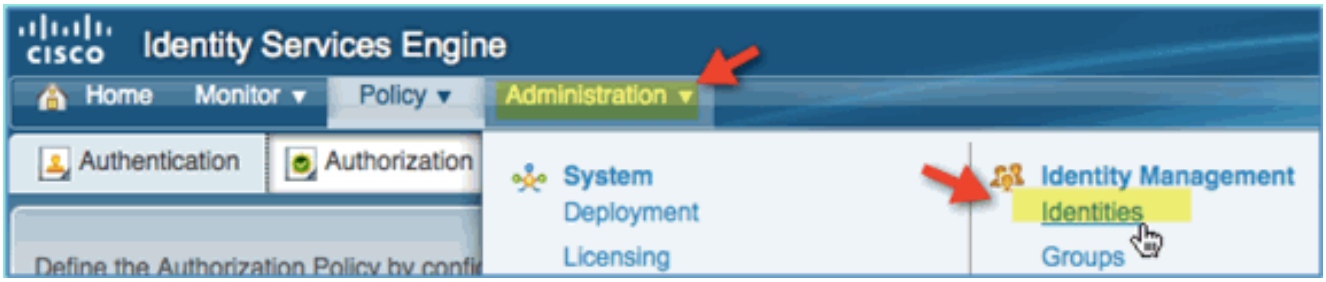


5. 저장을 **클릭합니다.참고:** 사용자 지정 정책 요소를 생성하여 사용 편의성을 추가할 수도 있습니다.

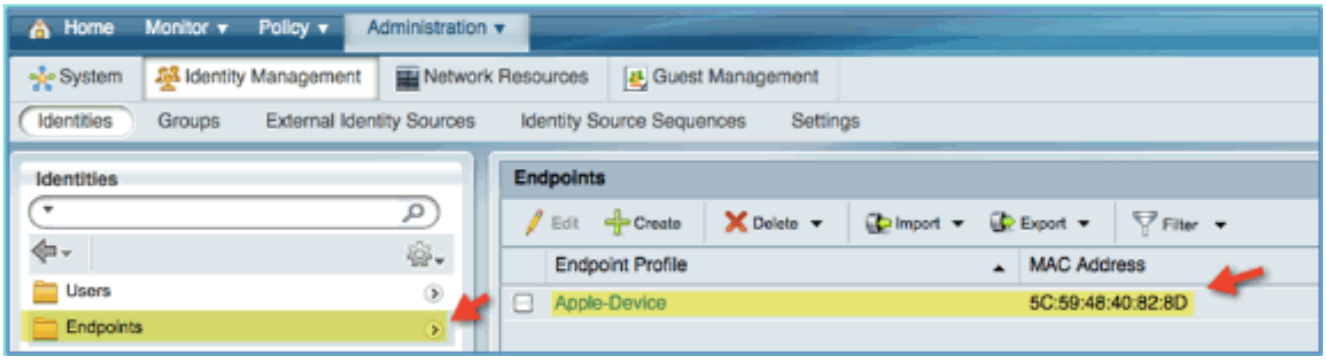
상태 교정 정책 테스트

ISE가 포스처 정책을 기반으로 새 디바이스를 제대로 프로파일링하고 있음을 보여주기 위해 간단한 데모를 수행할 수 있습니다.

1. ISE에서 Administration(관리) > Identity **Management(ID 관리) > Identities(ID)로 이동합니다**.

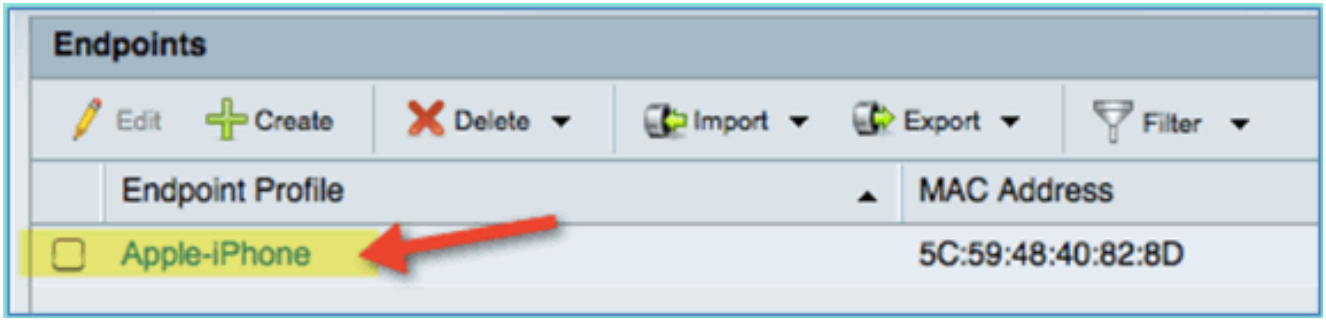


2. Endpoints(엔드포인트)**를 클릭합니다**. 디바이스(이 예에서는 iPhone)를 연결하고 연결합니다.



3. Endpoints(엔드포인트) 목록을 새로 고칩니다. 어떤 정보가 제공되는지 관찰합니다.
4. 엔드포인트 디바이스에서 다음으로 이동합니다.URL: http://www (또는 10.10.10.10)디바이스가 리디렉션됩니다. 인증서에 대한 모든 프롬프트를 수락합니다.
5. 모바일 디바이스가 완전히 리디렉션되면 ISE에서 엔드포인트 목록을 다시 새로 고칩니다. 무엇이 바뀌었는지 관찰하세요. 이전 엔드포인트(예: Apple-Device)는 'Apple-iPhone' 등으로 변경되어야 합니다. 그 이유는 HTTP 프로브가 종속 포털로 리디렉션되는 프로세스의 일부로 사용자 에이전트 정보를 효과적으로 가져오기 때문입니다

.



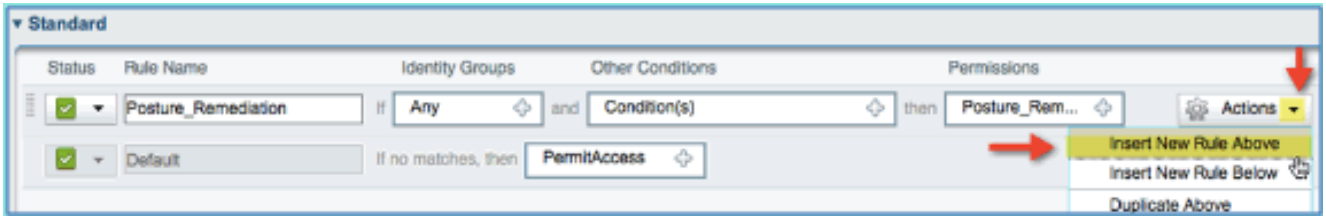
차별화된 액세스를 위한 권한 부여 정책

상태 권한 부여를 성공적으로 테스트한 후, 알려진 장치와 사용자 역할과 관련된 다른 VLAN 할당(이 시나리오에서는 직원 및 계약자)을 통해 직원 및 계약자에 대한 차별화된 액세스를 지원하는 정책을 계속 구축합니다.

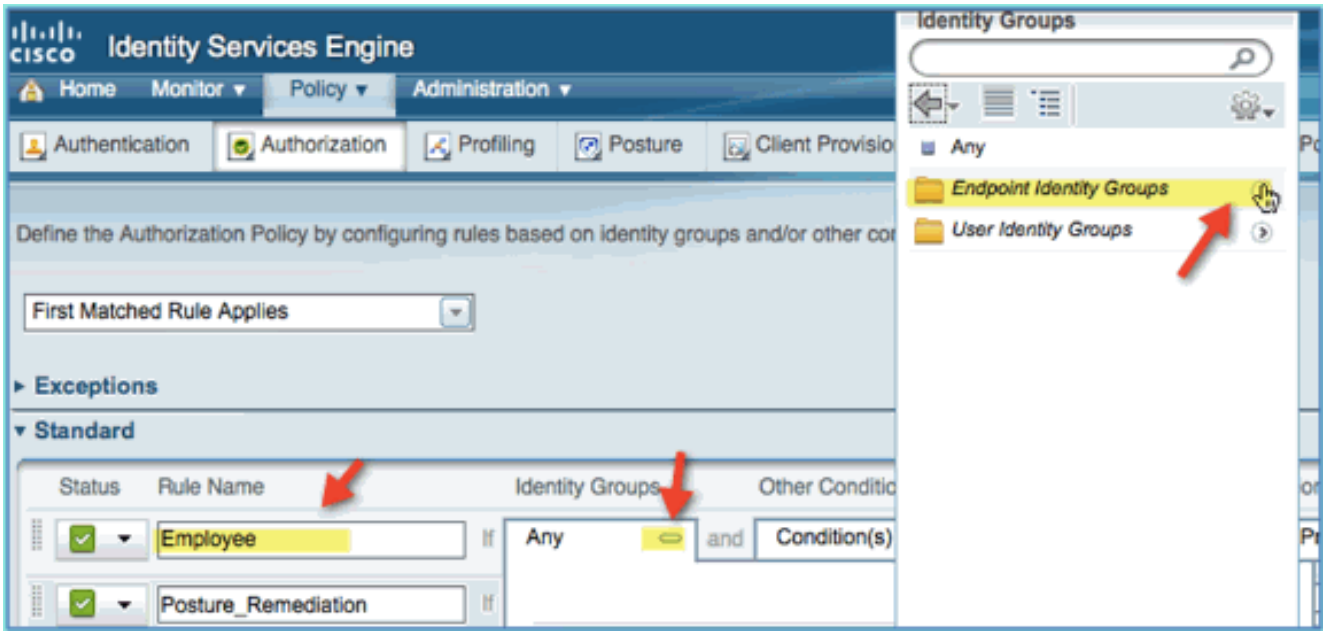
다음 단계를 완료하십시오.

1. ISE > **Policy > Authorization으로 이동합니다**.
2. 포스처 교정 정책/라인 위에 새 규칙을 추가/삽입합니다

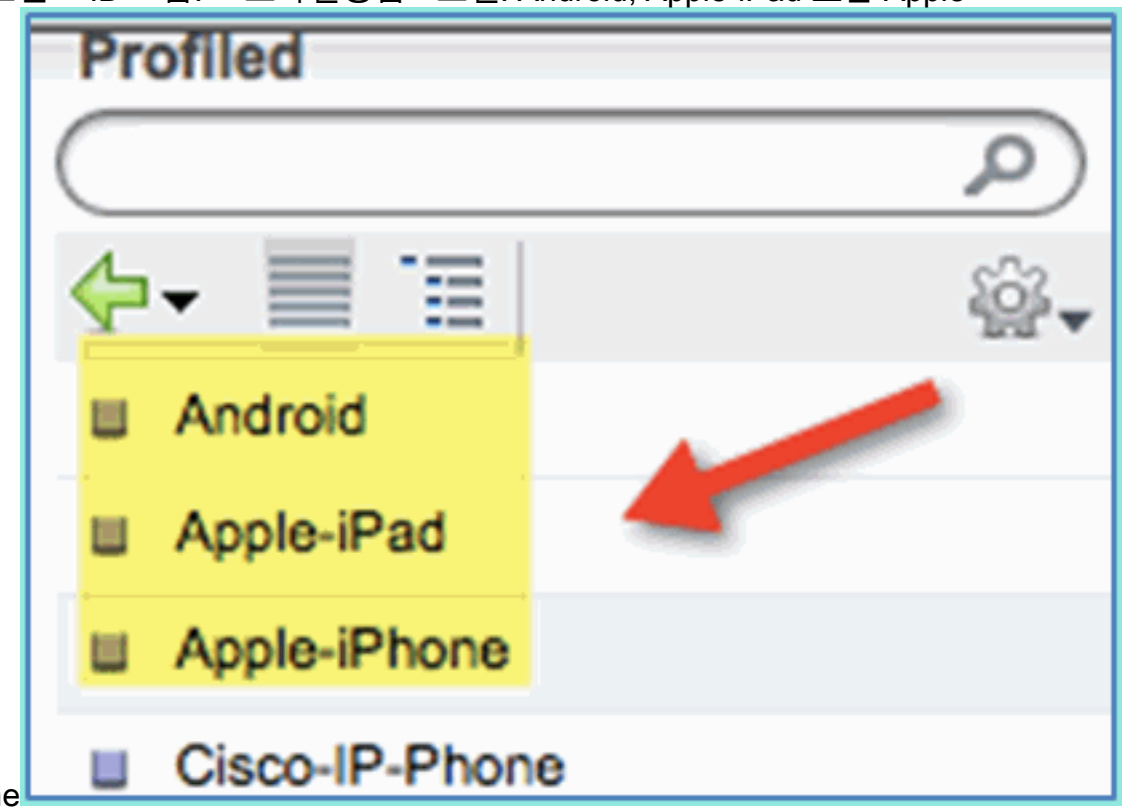
.



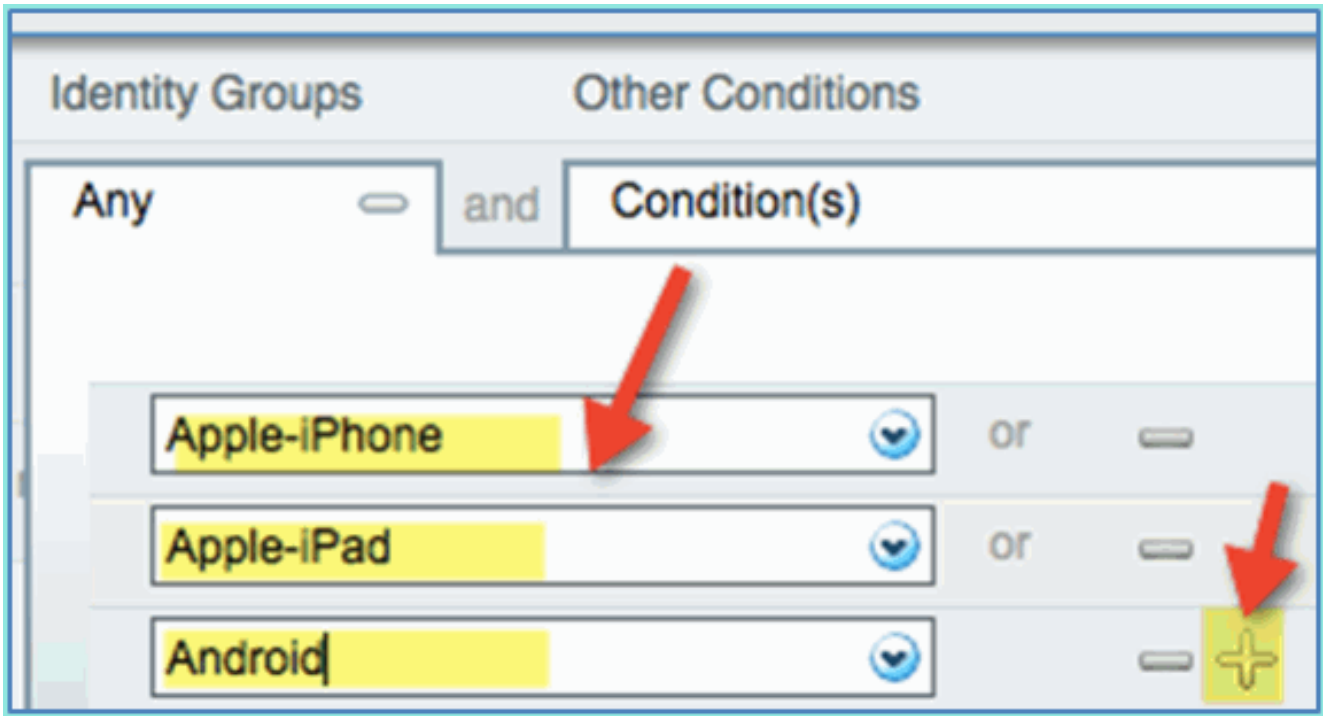
3. 이 정책에 대해 다음 값을 입력합니다.규칙 이름: 직원ID 그룹(확장): 엔드포인트 ID 그룹



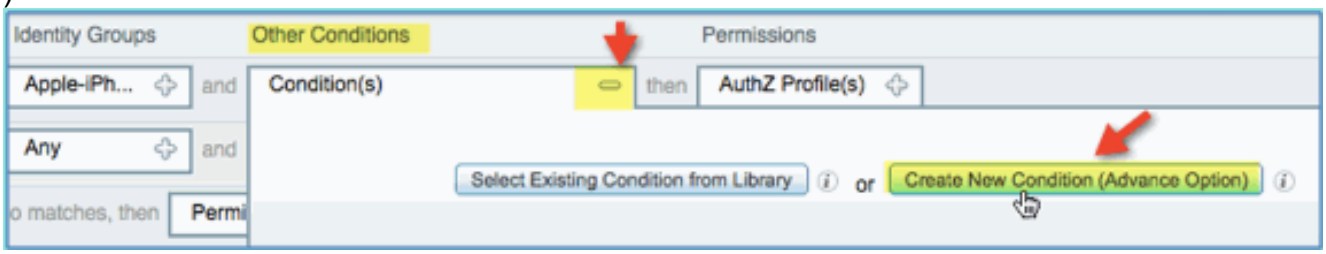
엔드포인트 ID 그룹: 프로파일링됨프로필: Android, Apple-iPad 또는 Apple-iPhone



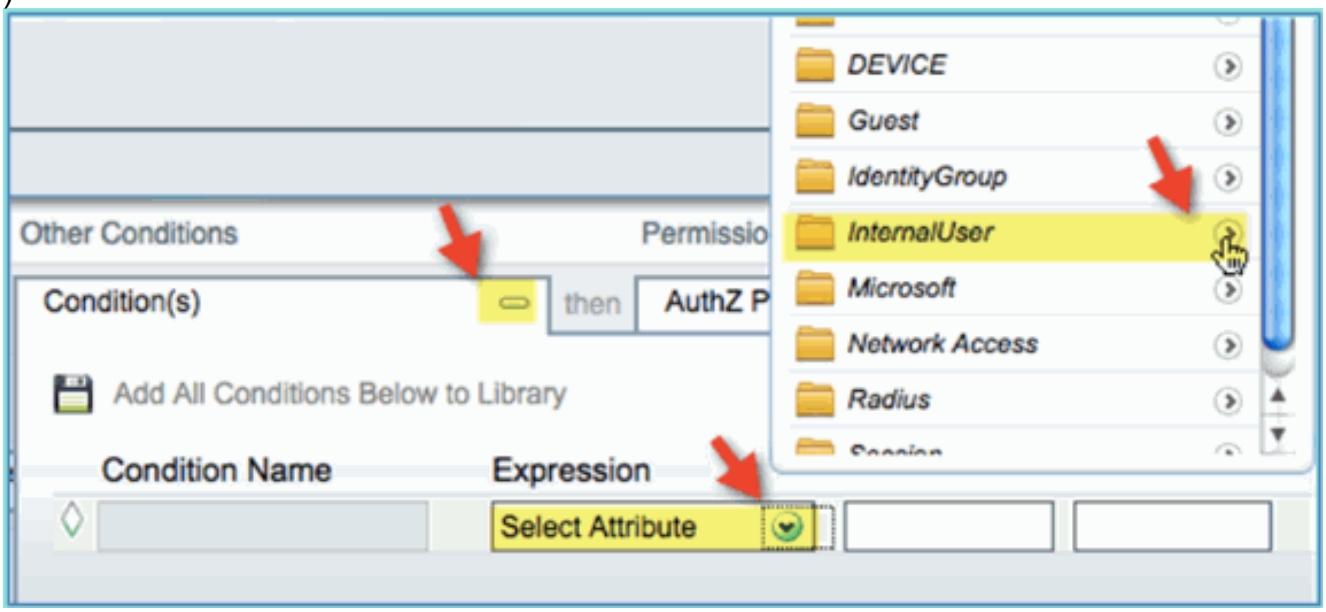
4. 추가 디바이스 유형을 지정하려면 +를 클릭하고 필요한 경우 추가 디바이스를 추가합니다.엔드포인트 ID 그룹: 프로파일링됨프로필: Android, Apple-iPad 또는 Apple-iPhone



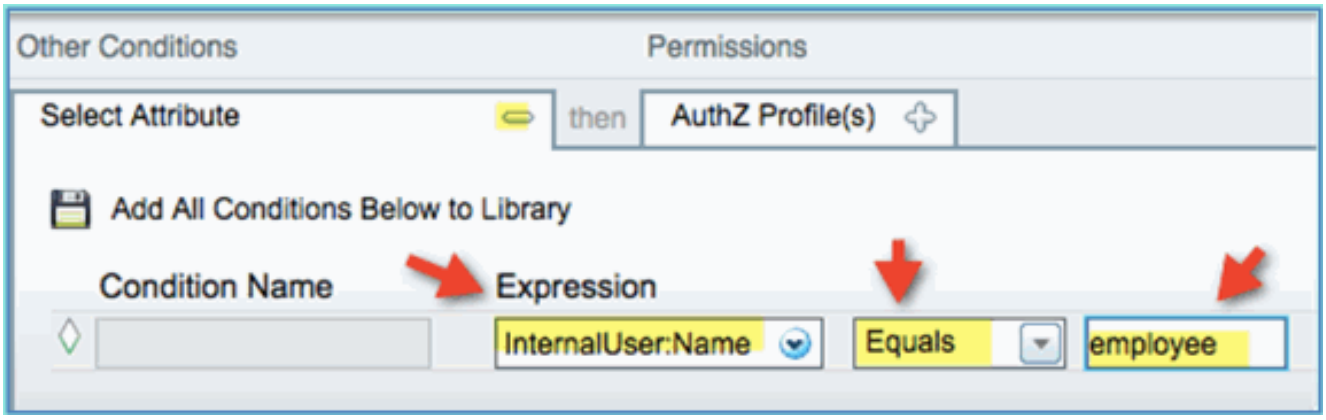
5. 이 정책에 대해 다음 Permissions(권한) 값을 지정합니다.기타 조건(확장): 새 조건 생성(고급 옵션
)



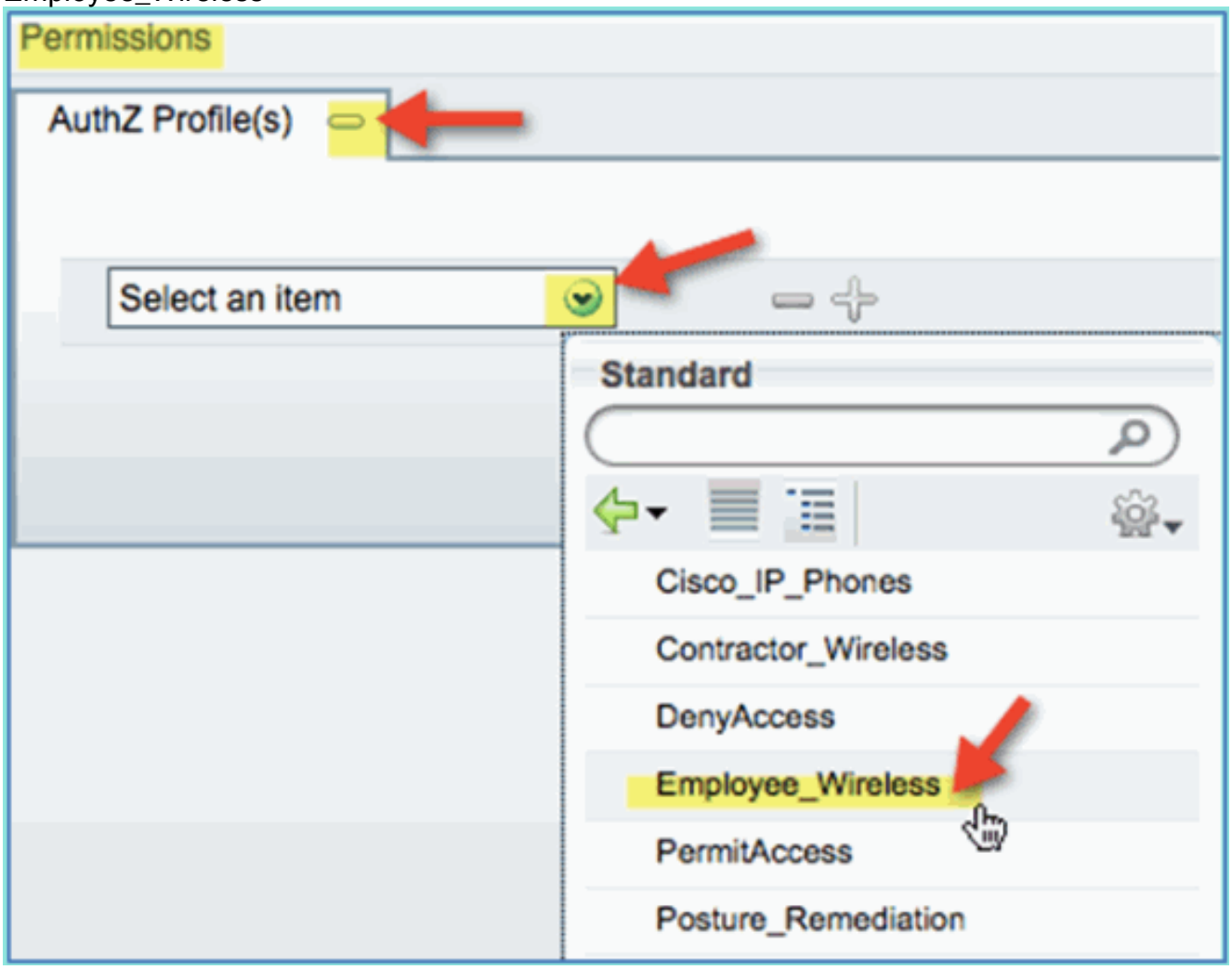
Condition(조건) > Expression (from list)(표현식(목록에서)): InternalUser(내부 사용자) > Name(이름
)



InternalUser > 이름:
employee

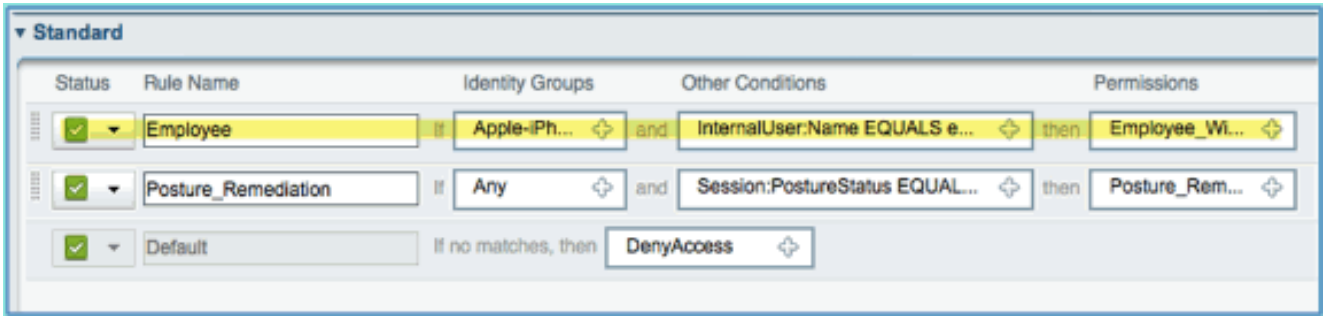


6. 포스처 세션 규정 준수에 대한 조건을 추가합니다.권한 > 프로파일 > 표준: Employee_Wireless



7. 저장을 **클릭합니다**. 정책이 올바르게 추가되었는지 확인합니다

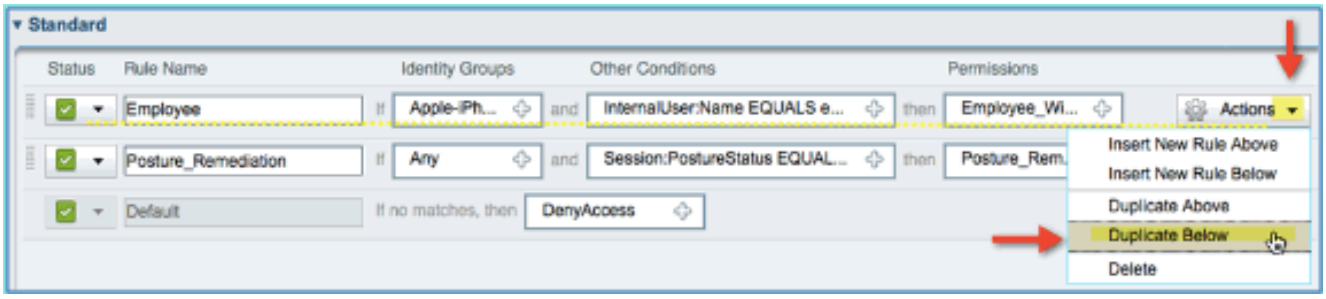
.



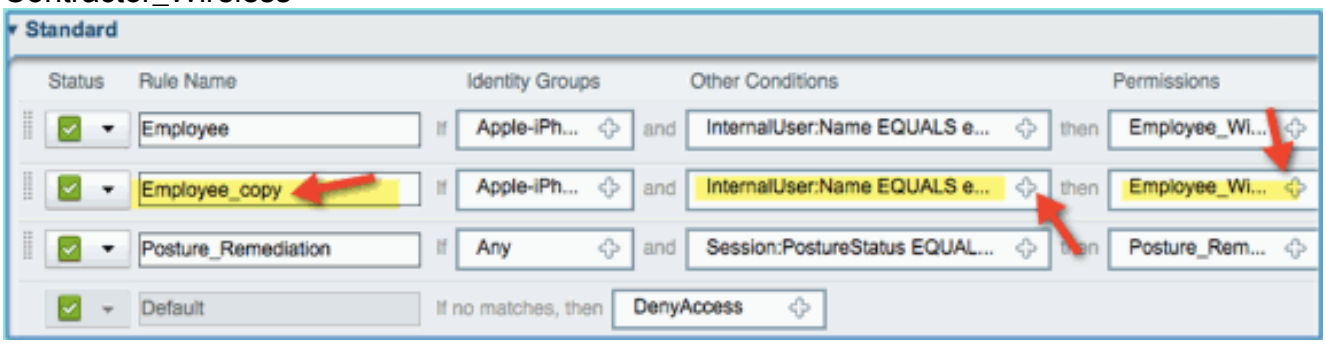
8. 계약업체 정책을 추가하여 계속 진행합니다. 이 문서에서는 프로세스를 신속하게 수행하기 위해(또는 모범 사례를 위해 수동으로 구성할 수 있음) 이전 정책이 복제됩니다.Employee

policy(직원 정책) > Actions(작업)에서 Duplicate Below(아래**에서 중복)**를 **클릭합니다**

.

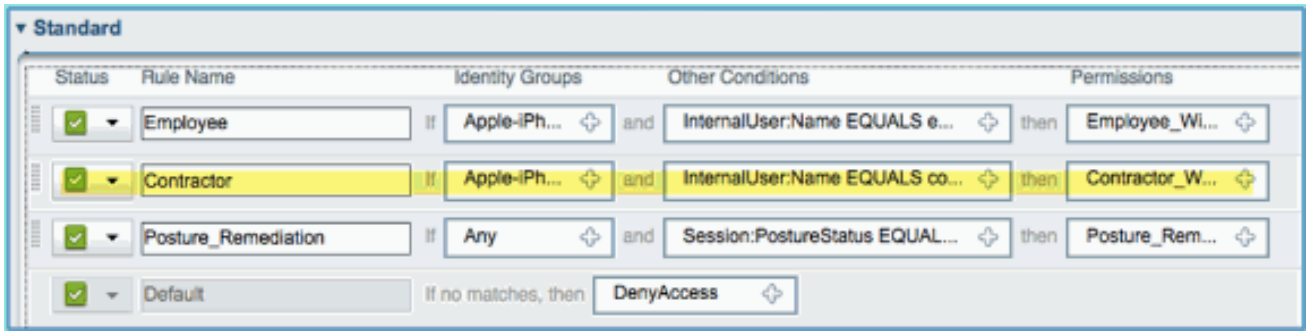


9. 이 정책에 대해 다음 필드를 편집합니다(복제).규칙 이름: 계약자기타 조건 > 내부 사용자 > 이름: 계약자권한:
Contractor_Wireless



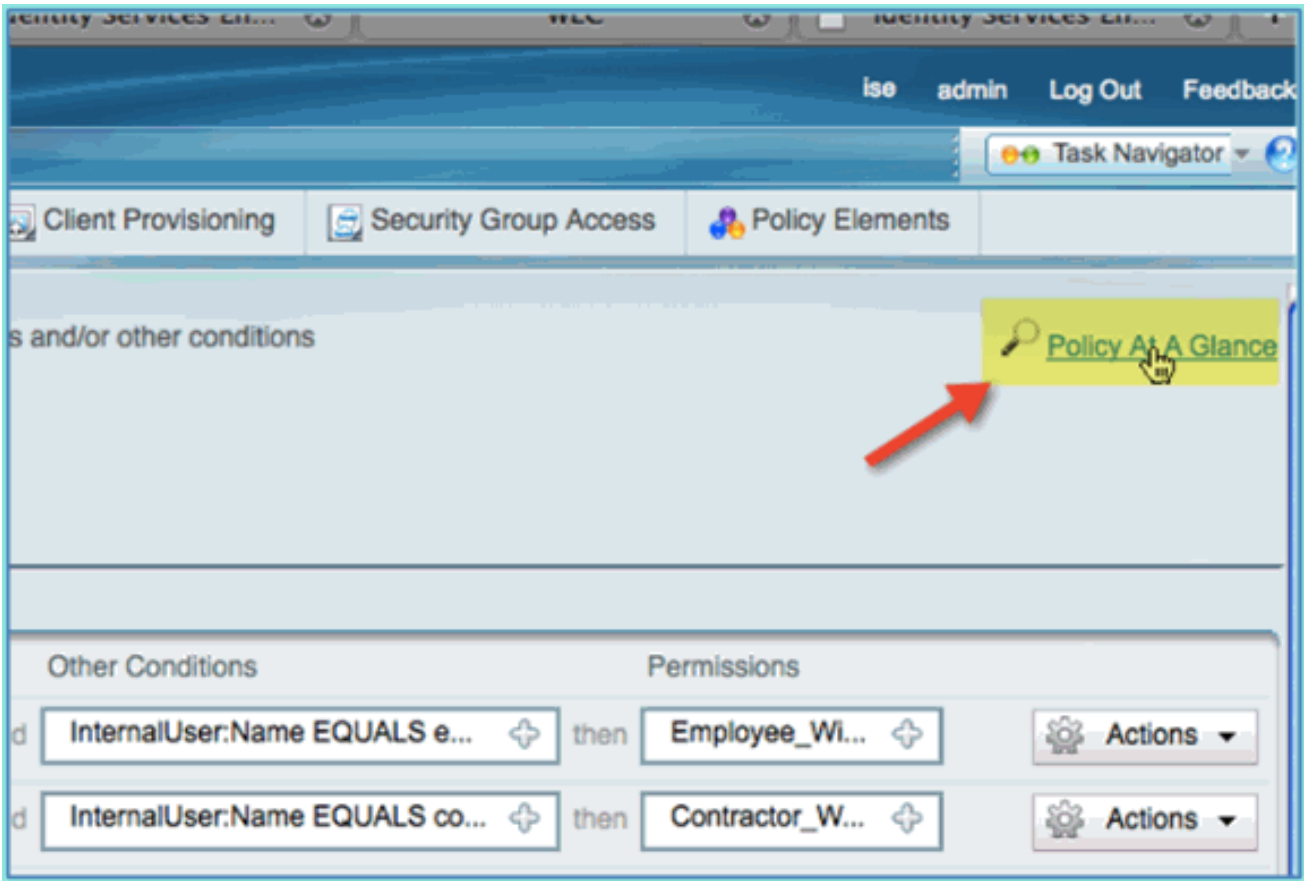
10. 저장을 **클릭합니다**. 이전 복제 사본(또는 새 정책)이 제대로 구성되었는지 확인합니다

.



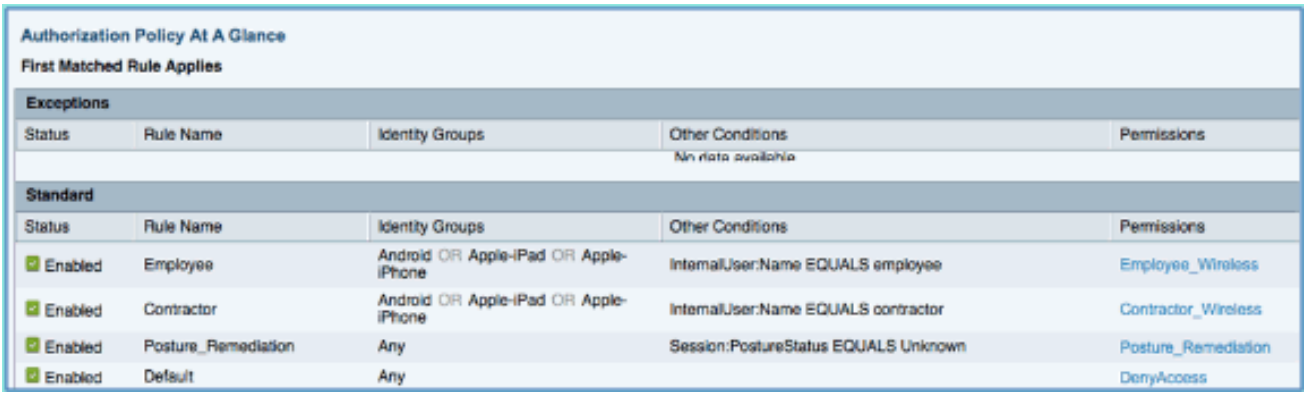
11. 정책을 미리 보려면 **Policy-at-a-Glance를 클릭합니다**

.



Policy at A Glance 보기에서는 통합되고 요약된 정책을 쉽게 확인할 수 있습니다

.



Authorization Policy At A Glance

First Matched Rule Applies

Exceptions

Status	Rule Name	Identity Groups	Other Conditions	Permissions
			No data available	

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Employee	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS employee	Employee_Wireless
Enabled	Contractor	Android OR Apple-iPad OR Apple-iPhone	InternalUser:Name EQUALS contractor	Contractor_Wireless
Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
Enabled	Default	Any		DenyAccess

차별화된 액세스에 대한 CoA 테스트

액세스 차별화를 위한 권한 부여 프로파일 및 정책이 준비되었으므로 이제 테스트를 수행할 차례입니다. 단일 보안 WLAN을 보유한 직원은 직원 VLAN을 할당받고 계약자는 계약자 VLAN을 담당하게 됩니다. 다음 예에서는 Apple iPhone/iPad가 사용됩니다.

다음 단계를 완료하십시오.

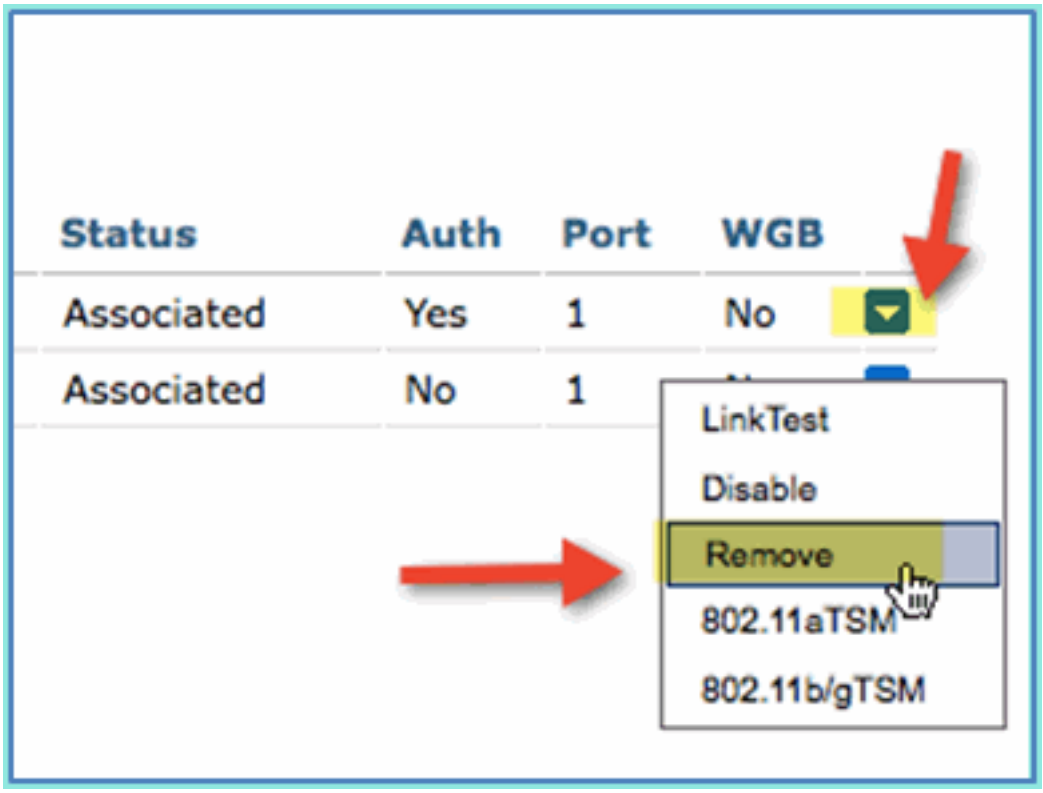
1. 모바일 디바이스로 보안 WLAN(POD1x)에 연결하고 다음 자격 증명을 사용합니다.사용자 이름: employee비밀번호:
   XXXXX

2. Join을 **클릭합니다**. 직원에게 VLAN 11(직원 VLAN)이 할당되었는지 확인합니다

3. Forget **this Network를 클릭합니다**. 삭제를 클릭하여 **확인합니다**

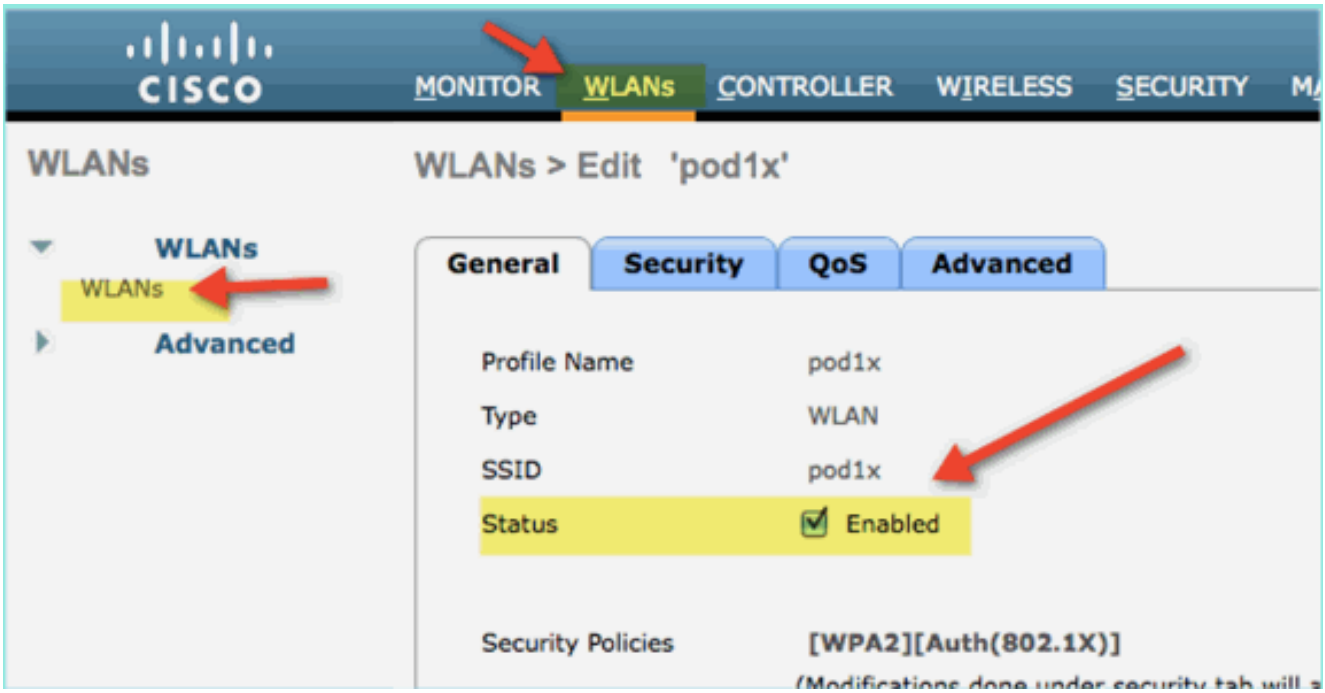
4. WLC로 이동하여 기존 클라이언트 연결을 제거합니다(이전 단계에서 동일한 연결을 사용한 경우). Monitor(**모니터**) > Clients(**클라이언트**) > MAC address(**MAC 주소**)로 이동한 다음 Remove(**제거**)를 클릭합니다


CISCO
MONITOR
WLANs
Monitor
Clients
Summary
Current Filter
Access Points
Cisco CleanAir
Client MAC Addr
Statistics
44:2a:60:f7:3a:4a
CDP
5c:59:48:40:82:8d
Rogues
Clients
Multicast


Status
Auth
Port
WGB
Associated
Yes
1
No
Associated
No
1
LinkTest
Disable
Remove
802.11aTSM
802.11b/gTSM

5. 이전 클라이언트 세션을 지우는 또 다른 확실한 방법은 WLAN을 비활성화/활성화하는 것입니다.WLC(**WLC) > WLANs(WLAN) > WLAN(WLAN**)으로 이동한 다음 WLAN을 클릭하여 수정합니다.Enabled(활성화됨) **> Apply(적용)**를 선택 취소합니다(비활성화하려면).Enabled(활성화됨) **> Apply(적용)**(다시 활성화하려면) 확인란을 선택합니다

.



6. 모바일 장치로 돌아갑니다. 다음 크리덴셜을 사용하여 동일한 WLAN에 다시 연결합니다.사용자 이름: contractor비밀번호:

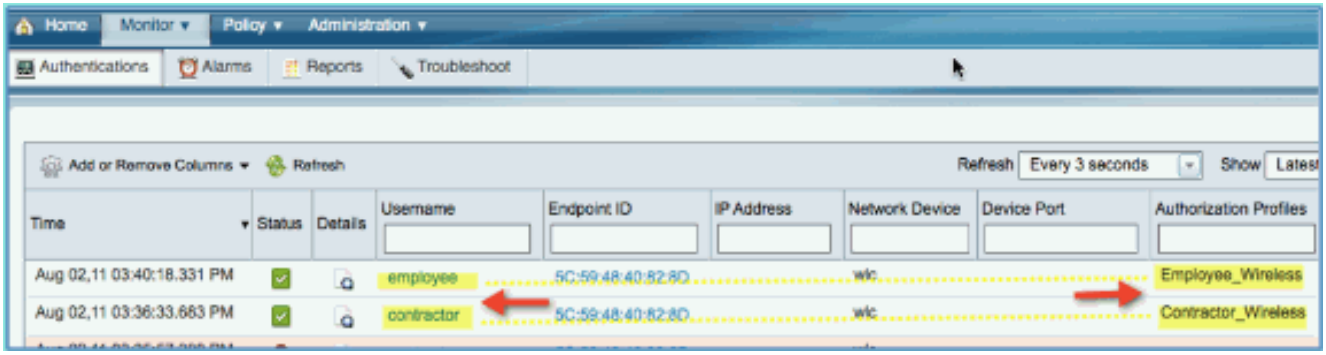
XXXX

7. Join을 **클릭합니다**. 계약자 사용자에게 VLAN 12(계약자/게스트 VLAN)가 할당되었는지 확인

합니다.

8. ISE > **Monitor > Authorizations**에서 ISE 실시간 로그 **보기를** 볼 수 있습니다. 개별 사용자(직원, 계약자)가 서로 다른 VLAN에서 차별화된 인증 프로파일 (Employee_WirelessContractor_Wireless)을 사용하는 것을 볼 수 있습니다

.



WLC 게스트 WLAN

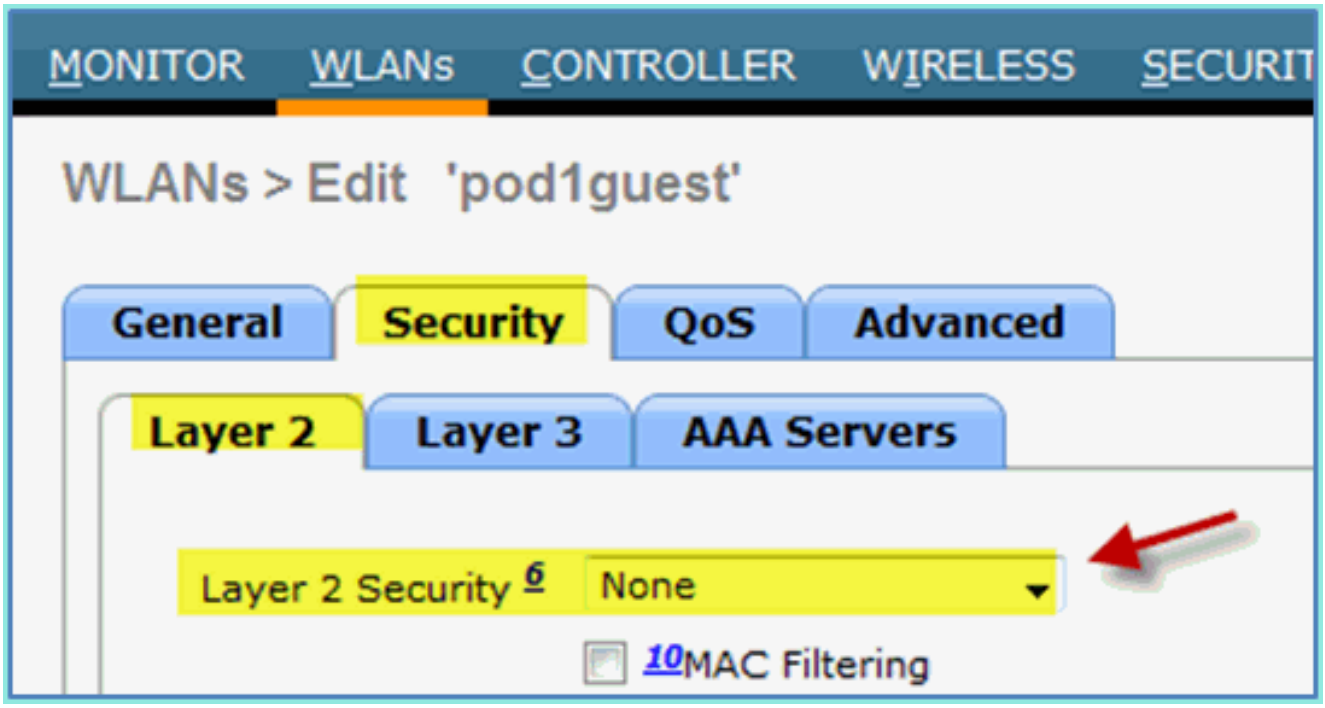
게스트가 ISE 스폰서 게스트 포털에 액세스할 수 있도록 게스트 WLAN을 추가하려면 다음 단계를

완료합니다.

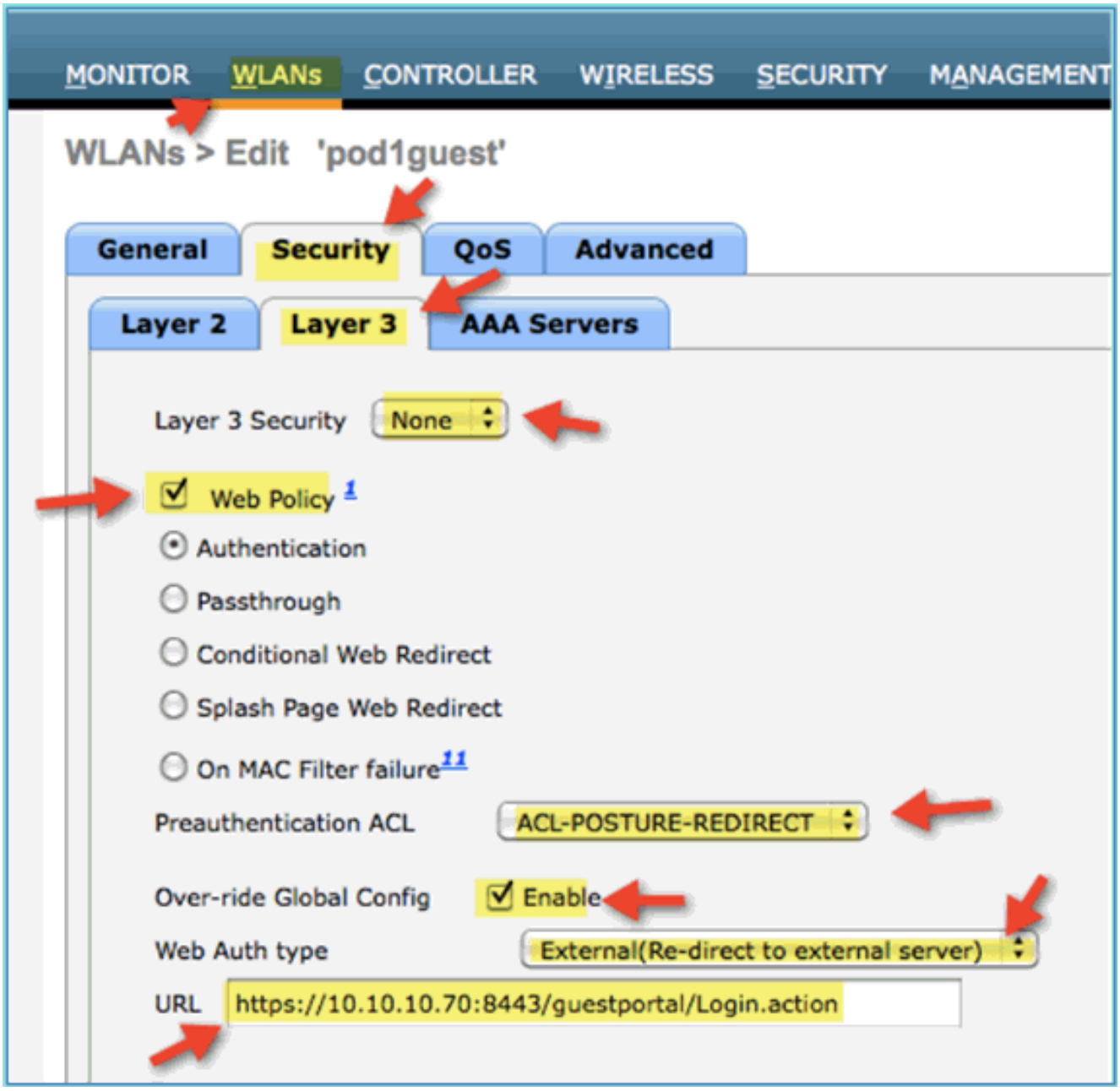
1. WLC에서 WLANs(WLANs) > WLANs(**WLANs) > Add New(새로 추가)로 이동합니다**.
2. 새 게스트 WLAN에 대해 다음을 입력합니다.프로필 이름: pod1guestSSID: pod1guest

3. Apply를 **클릭합니다**.
4. 게스트 WLAN > General(일반) 탭에서 다음을 입력합니다.상태: 사용 안 함인터페이스/인터페이스 그룹: 게스트

5. guest WLAN(게스트 **WLAN) > Security(보안) > Layer2(레이어 2)**로 이동하고 다음을 입력합니다.레이어 2 보안: 없음



6. guest WLAN(게스트 **WLAN) > Security(보안) > Layer3(레이어 3)** 탭으로 이동하고 다음을 입력합니다.레이어 3 보안: 없음웹 정책: 사용웹 정책 하위 값: 인증사전 인증 ACL: ACL-POSTURE-REDIRECT웹 인증 유형: 외부(외부 서버로 리디렉션)URL: https://10.10.10.70:8443/guestportal/Login.action



7. Apply를 **클릭합니다**.
8. WLC 컨피그레이션**을 저장해야 합니다**.

게스트 WLAN 및 게스트 포털 테스트

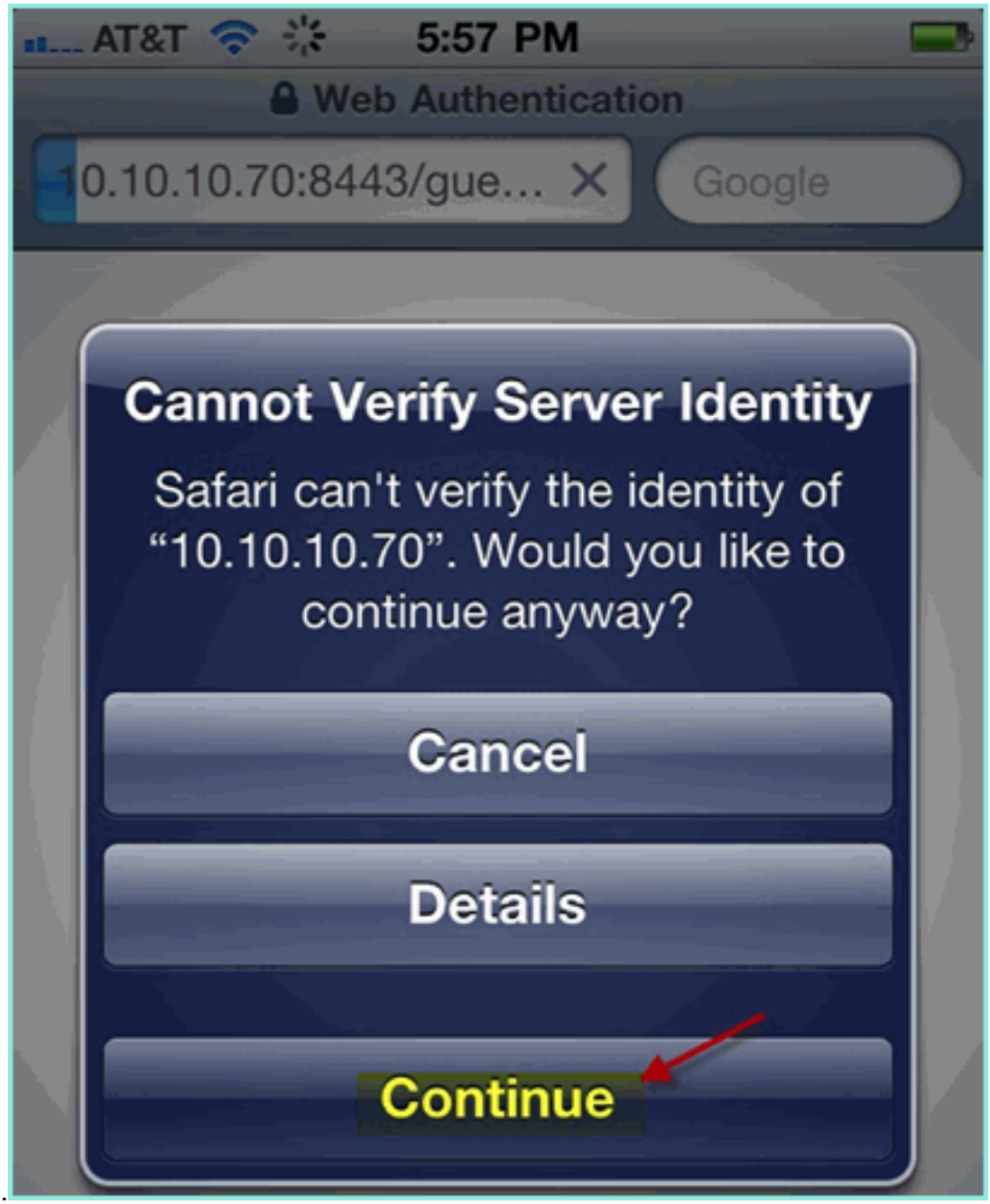
이제 게스트 WLAN 컨피그레이션을 테스트할 수 있습니다. ISE 게스트 포털에 게스트를 리디렉션해야 합니다.

다음 단계를 완료하십시오.

1. iPhone과 같은 iOS 디바이스에서 **Wi-Fi Networks(Wi-Fi 네트워크) > Enable(활성화)로 이동합니다**. 그런 다음 POD 게스트 네트워크를 선택합니다

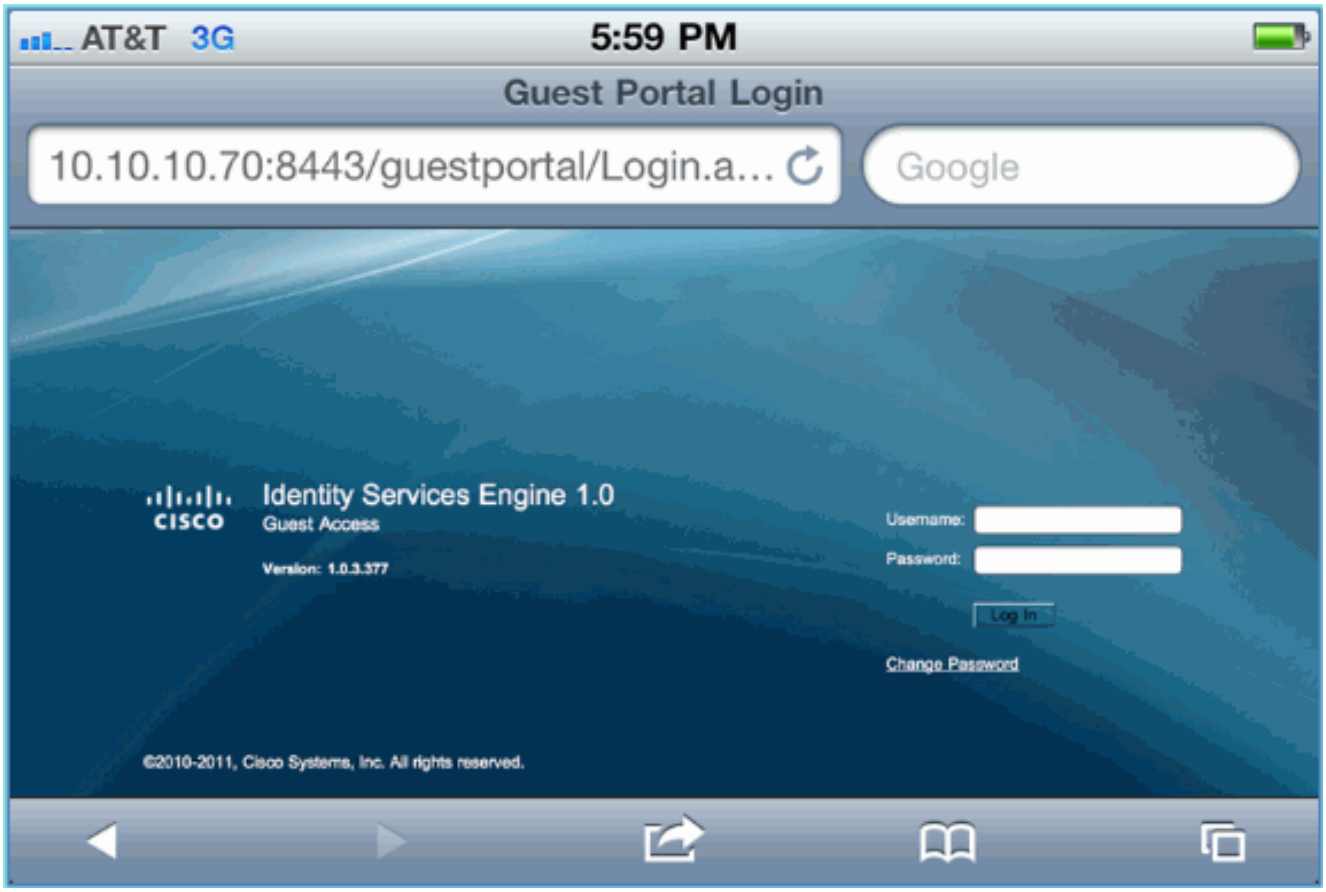
2. iOS 디바이스는 게스트 VLAN(10.10.12.0/24)에서 유효한 IP 주소를 표시해야 합니다

3. Safari 브라우저를 열고 다음에 연결합니다.URL: http://10.10.10.10웹 인증 리디렉션이 나타납니다.
4. ISE Guest Portal(ISE 게스트 포털) 페이지에 도착할 때까지 Continue(**계속**)를 클릭합니다



. 다음 샘플 스크린샷은 게스트 포털 로그인의 iOS 디바이스를 보여줍니다. 그러면 WLAN 및 ISE 게스트 포털에 대한 올바른 설정이 활성 상태임을 확인합니다

.

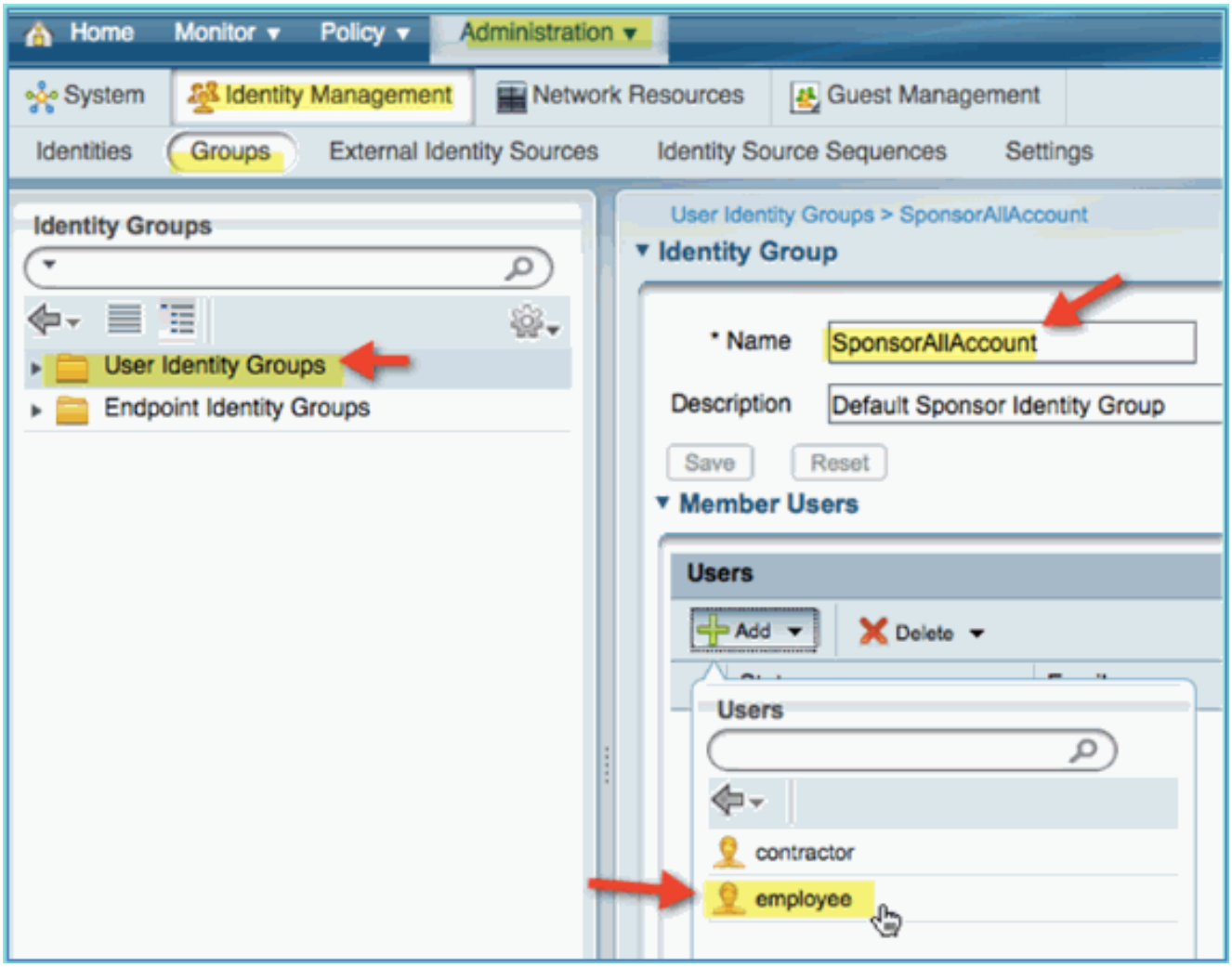


ISE 무선 스폰서 게스트 액세스

게스트가 스폰서되도록 ISE를 구성할 수 있습니다. 이 경우 내부 또는 AD 도메인(통합된 경우) 사용자가 게스트 액세스를 스폰서하도록 ISE 게스트 정책을 구성합니다. 또한 스폰서가 게스트 비밀번호(선택 사항)를 볼 수 있도록 ISE를 구성하며, 이는 이 Lab에 유용합니다.

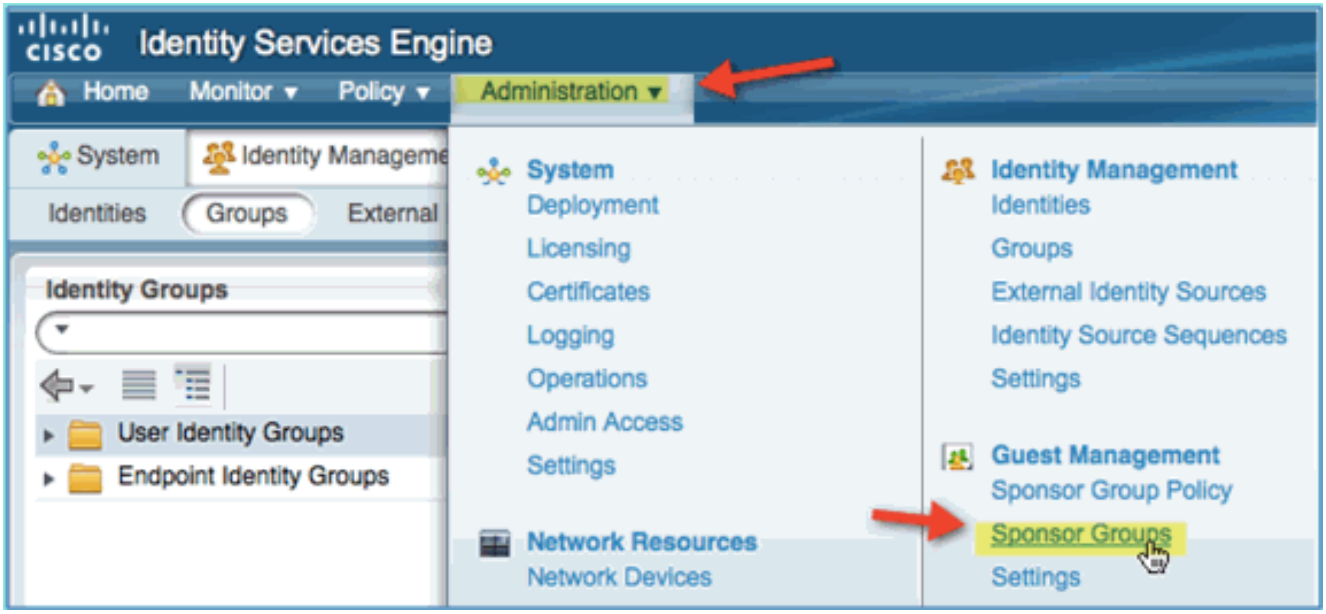
다음 단계를 완료하십시오.

1. SponsorAllAccount 그룹에 직원 사용자를 추가합니다. 이렇게 하는 방법에는 여러 가지가 있습니다. 바로 그룹으로 이동하거나 사용자를 편집하고 그룹을 할당합니다. 이 예에서는 Administration(관리) > Identity **Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹)로 이동합니다**. 그런 다음 SponsorAllAccount**를** 클릭하고 직원 사용자를 추가합니다
   .



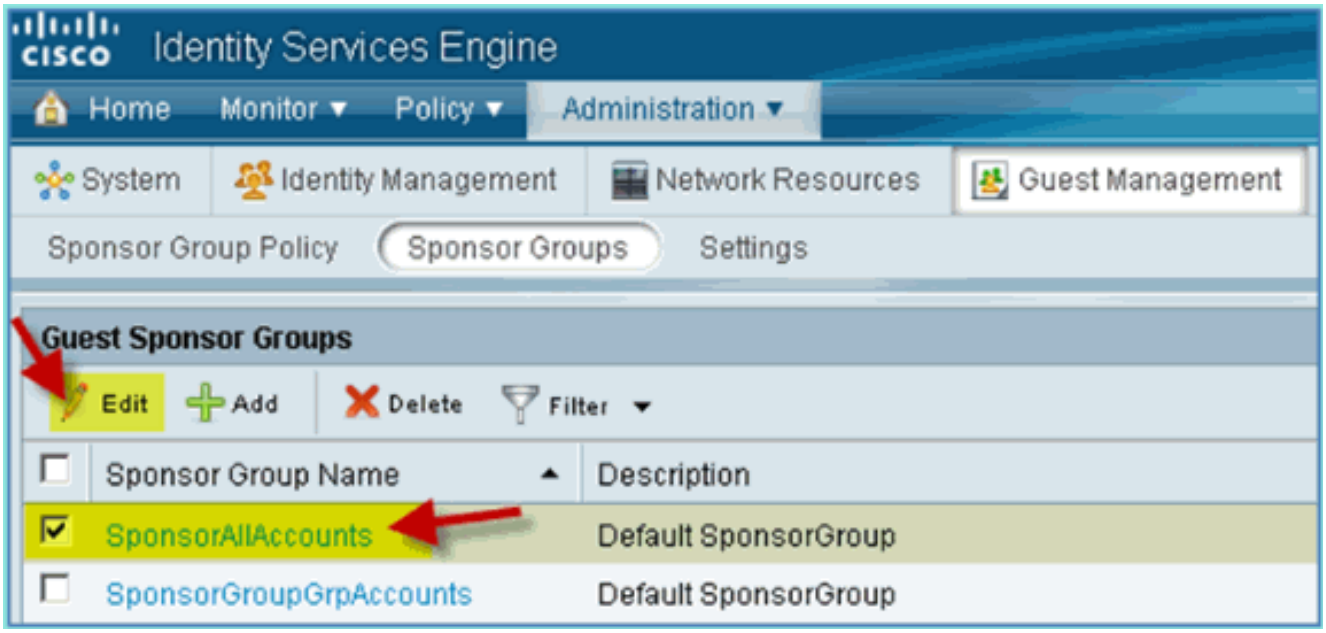
2. Administration(관리) **> Guest Management(게스트 관리) > Sponsor Groups(스폰서 그룹)로 이동합니다**

.

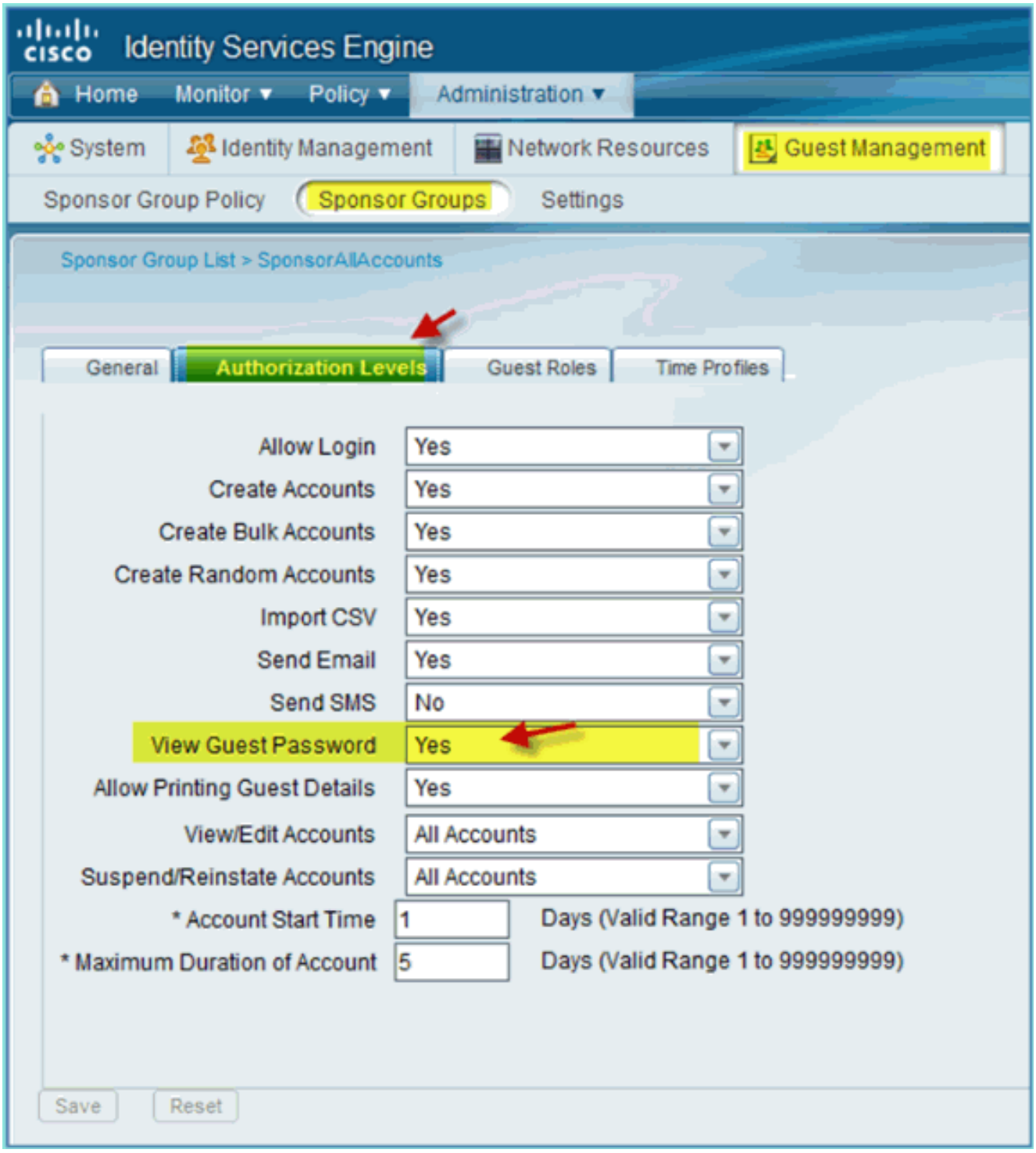


3. Edit를 **클릭한** 다음 SponsorAllAccounts를 **선택합니다**

.



4. Authorization Levels(권한 부여 레벨)를 선택하고 다음을 설정합니다.게스트 비밀번호 보기: 예



5. 이 **작업**을 완료하려면 Save를 클릭합니다.

후원 게스트

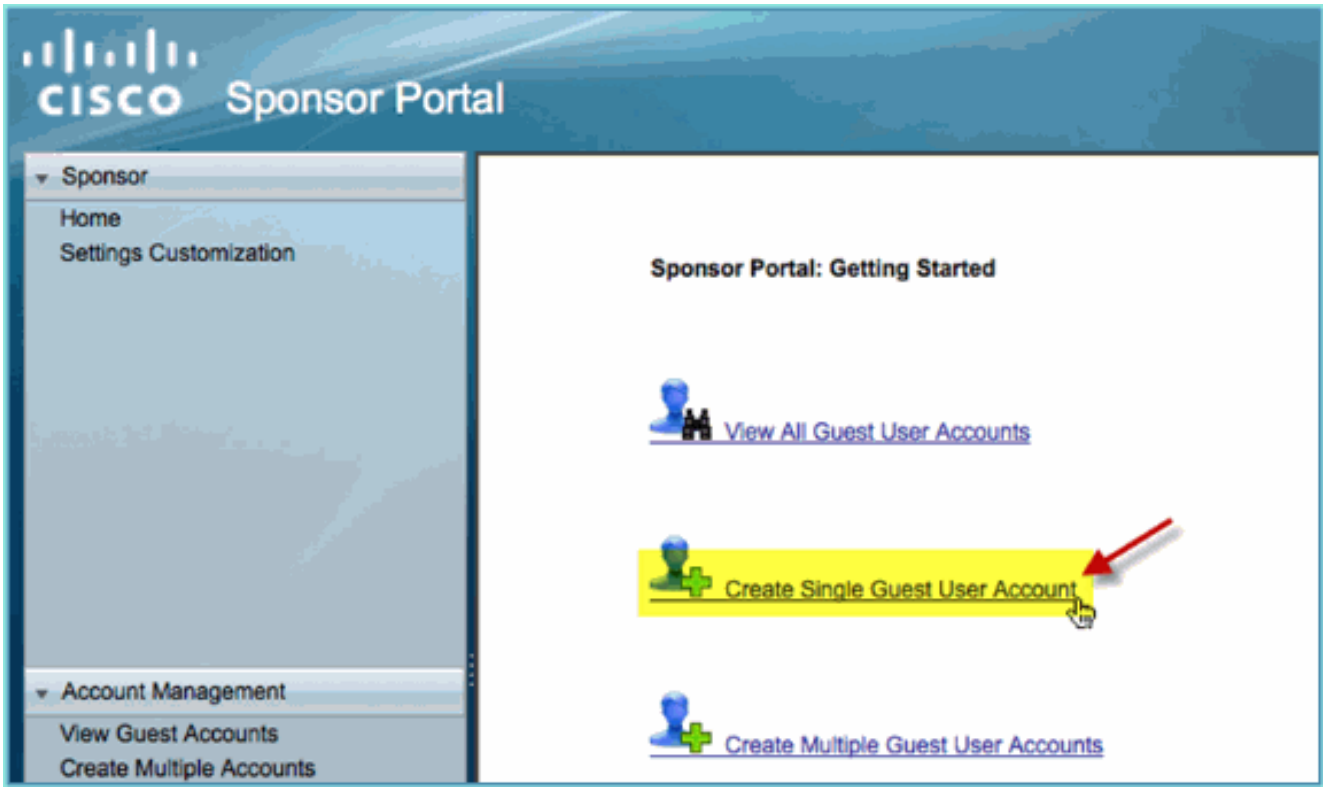
이전에는 AD 도메인 사용자가 임시 게스트를 스폰서할 수 있도록 적절한 게스트 정책 및 그룹을 구성했습니다. 다음으로, 후원자 포털에 액세스 하고 임시 게스트 액세스를 만듭니다.

다음 단계를 완료하십시오.

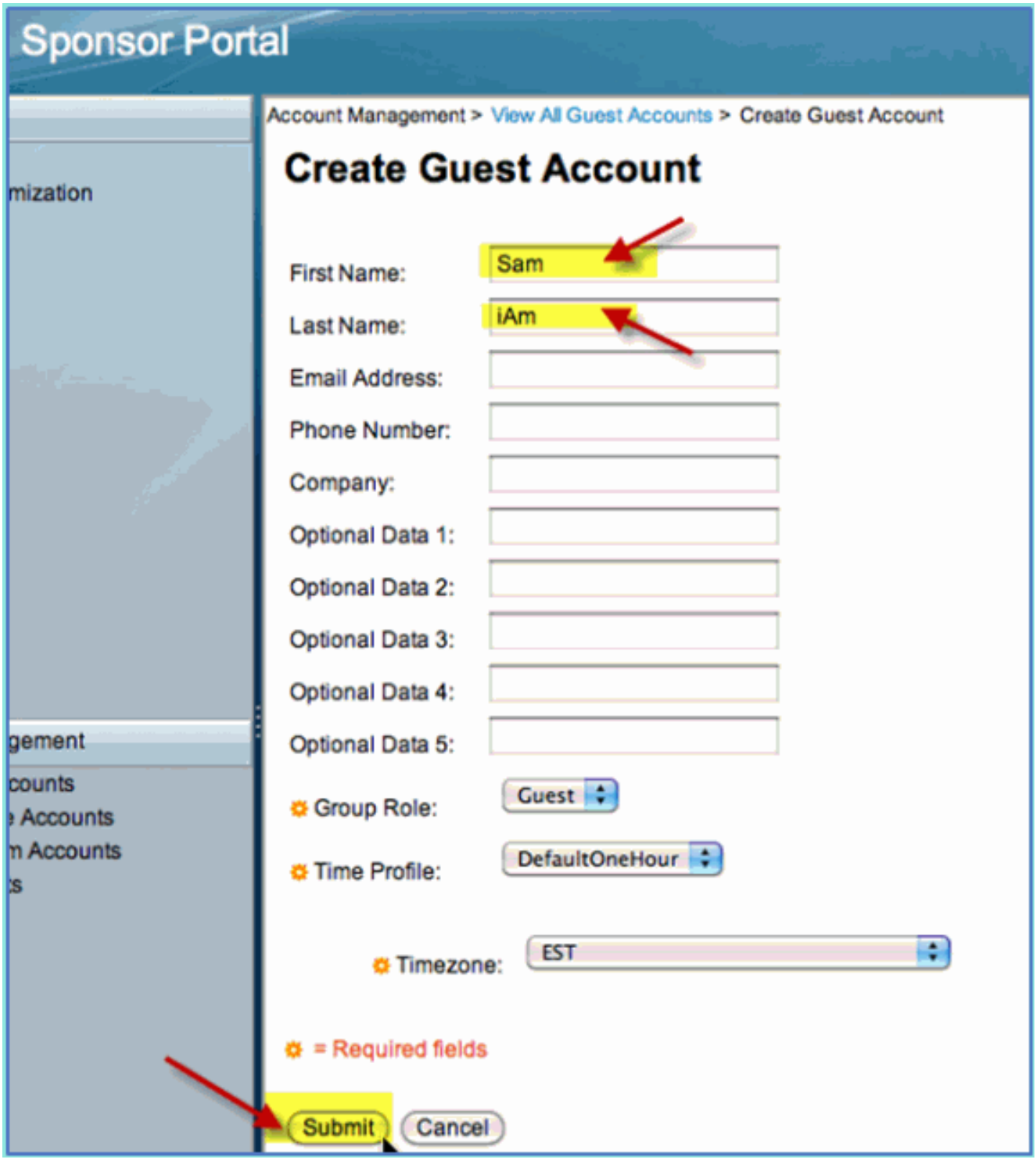
1. 브라우저에서 다음 URL 중 하나로 이동합니다. http://<ise ip>:8080/sponsorportal/ 또는 https://<ise ip>:8443/sponsorportal/ 그런 다음 다음을 사용하여 로그인합니다.사용자 이름: aduser(Active Directory), employee(Internal User)비밀번호: XXXX

2. Sponsor(스폰서) 페이지에서 Create **Single Guest User Account(단일 게스트 사용자 계정 생성)를 클릭합니다**

.

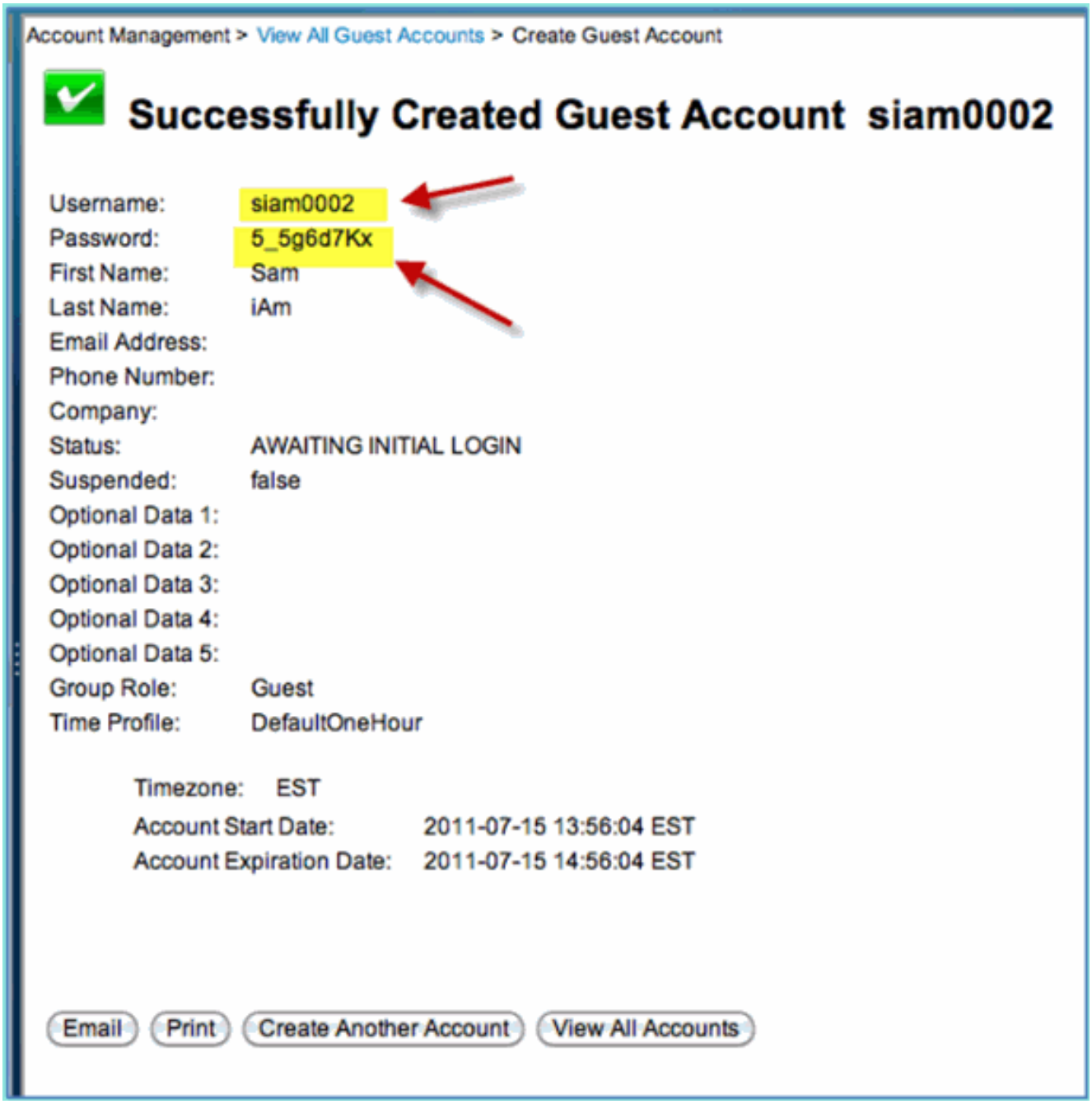


3. 임시 게스트의 경우 다음을 추가합니다.이름: 필수(예: Sam)성: 필수(예: Jones)그룹 역할: 게스트시간 프로필: DefaultOneHour표준 시간대:
   Any/Default



4. Submit(제출)**을 클릭합니다**.
5. 게스트 어카운트는 이전 항목을 기반으로 생성됩니다. 비밀번호는 해시 비밀번호와 달리 이전 연습에서 볼 수 ***.
6. 게스트의 사용자 이름 및 비밀번호가 표시된 이 창을 열어 둡니다. 게스트 포털 로그인 (다음)을 테스트 하는 데 사용 합니다

.



게스트 포털 액세스 테스트

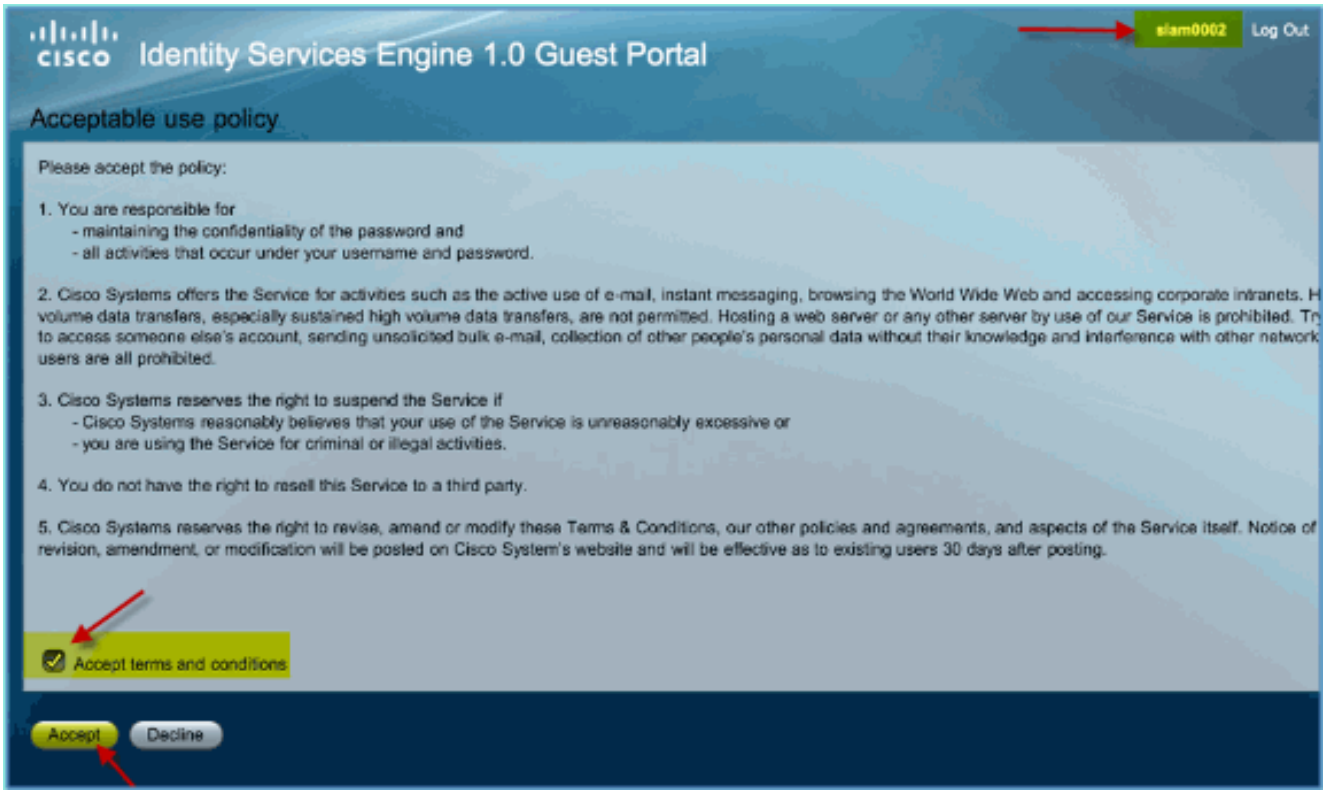
AD 사용자/스폰서가 생성한 새 게스트 계정을 사용하여 게스트 포털 및 액세스를 테스트할 차례입니다.

다음 단계를 완료하십시오.

1. 기본 설정 디바이스(이 예에서는 Apple iOS/iPad)에서 Pod Guest SSID에 연결하고 IP 주소/연결을 선택합니다.
2. 브라우저를 사용하여 http://www으로 이동하십시오.게스트 포털 로그인 페이지로 리디렉션됩니다
.

3. 이전 연습에서 생성한 게스트 계정을 사용하여 로그인합니다.성공하면 Acceptable use policy 페이지가 나타납니다.
4. Accept **terms and conditions(약관 수락)를 선택한** 다음 Accept(**수락**)를 클릭합니다

.



원래 URL이 완료되고 엔드포인트에 게스트로 액세스할 수 있습니다.

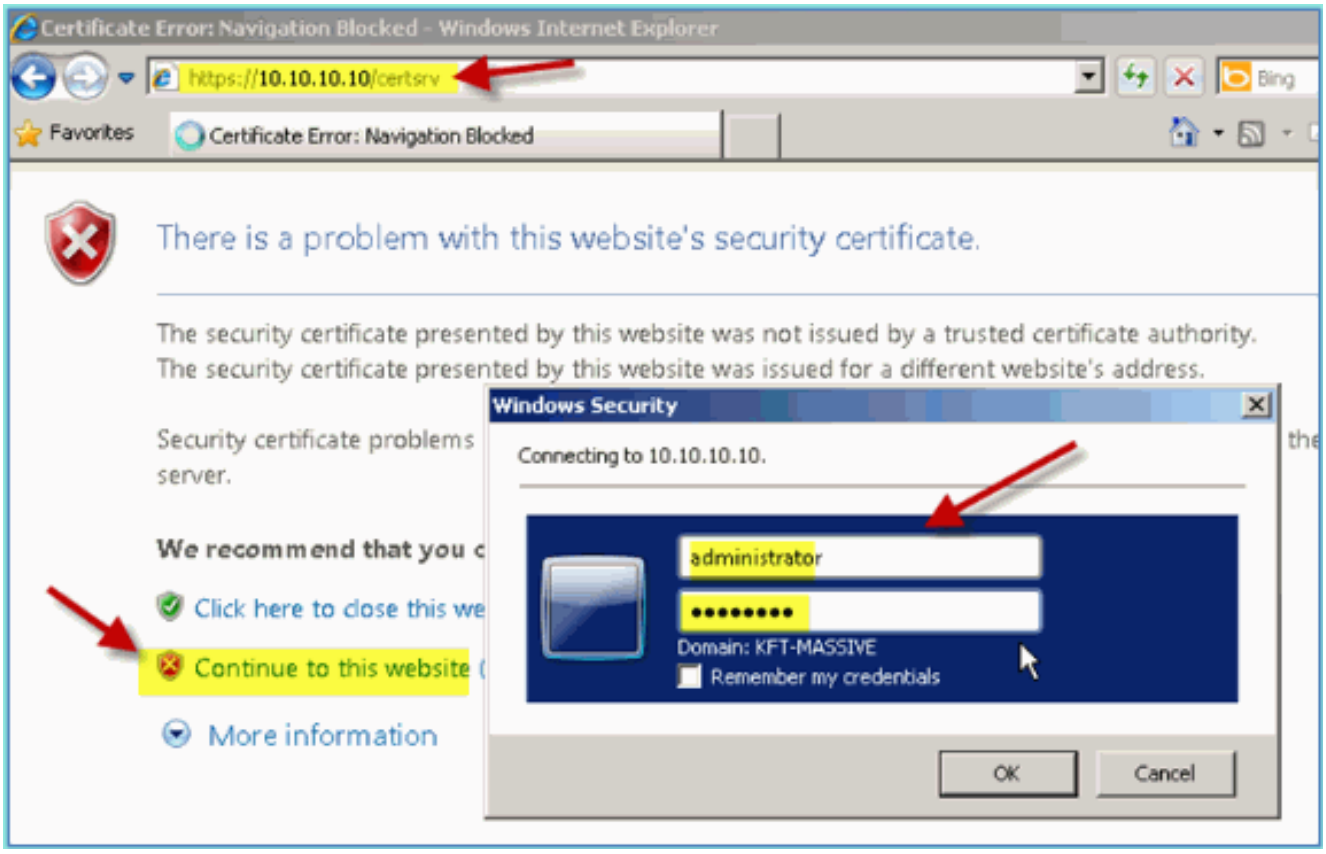
인증서 컨피그레이션

ISE와의 통신을 보호하려면 통신이 인증과 관련되었는지 ISE 관리용인지 확인합니다. 예를 들어, ISE 웹 UI를 사용하는 컨피그레이션의 경우 비대칭 암호화를 활성화하도록 X.509 인증서 및 인증서 신뢰 체인을 구성해야 합니다.

다음 단계를 완료하십시오.

1. 유선 연결 PC에서 브라우저 창을 열고 https://AD/certsrv을 엽니다.**참고:** 보안 HTTP를 사용합니다.**참고:** ISE에 액세스하려면 Mozilla Firefox 또는 MS Internet Explorer를 사용합니다.
2. administrator/Cisco123으로 로그인합니다

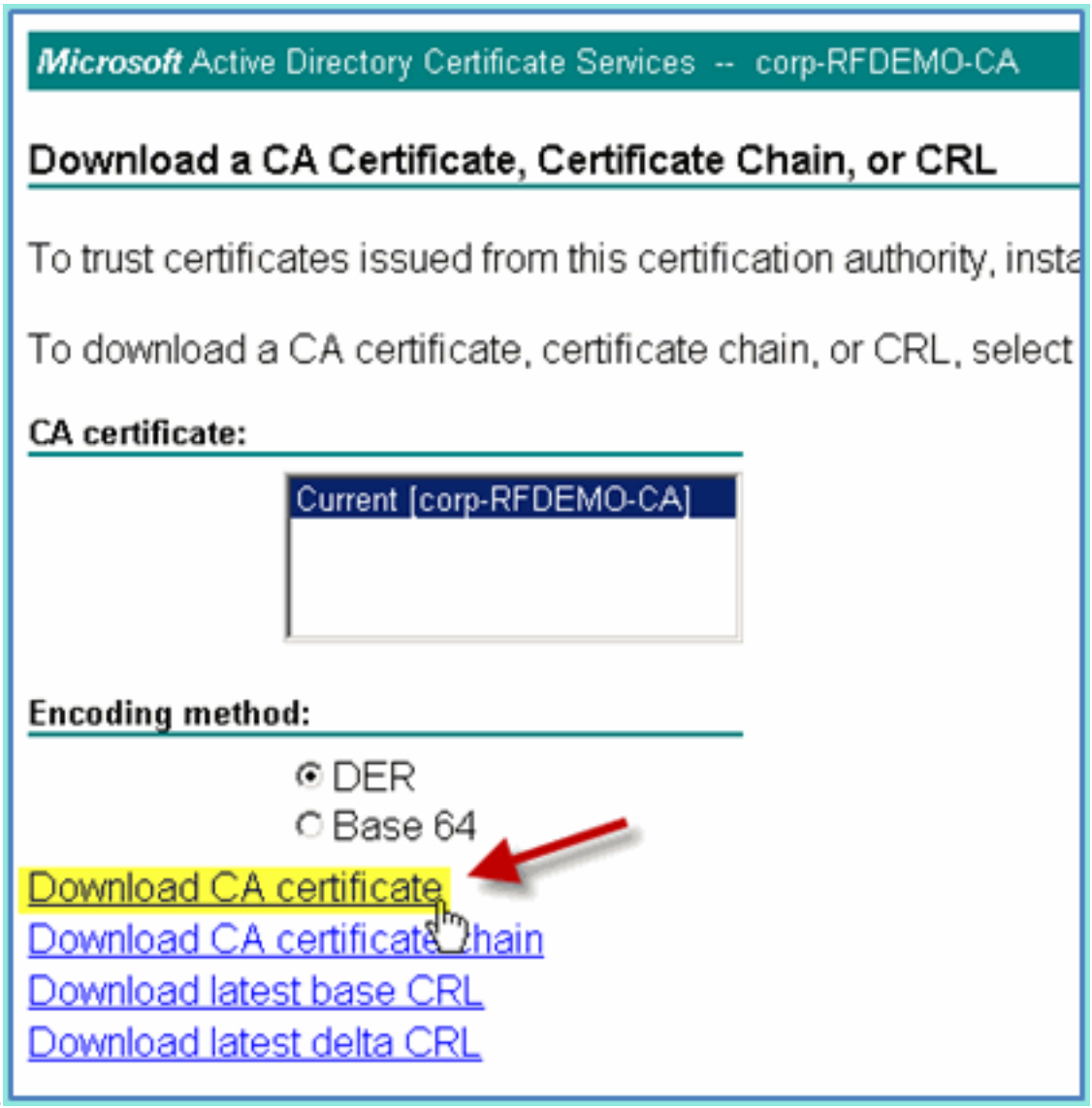
.



3. Download **a CA certificate, certificate chain, or CRL(CA 인증서, 인증서 체인 또는 CRL 다운로드)을 클릭합니다**

.

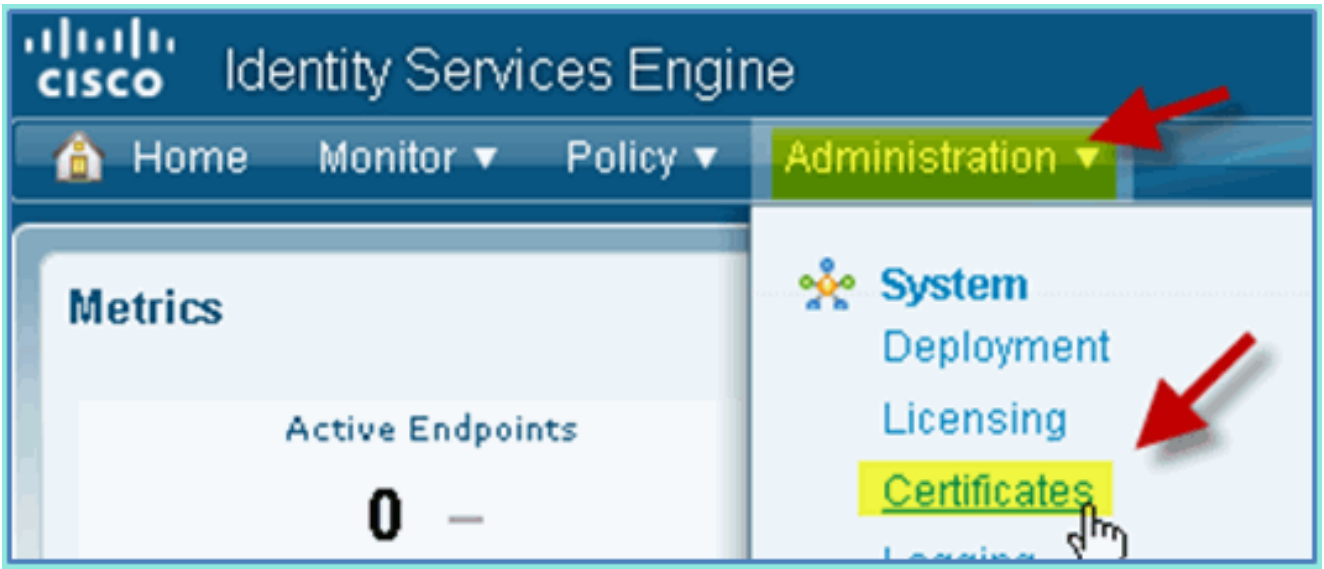
4. Download **CA certificate(CA 인증서 다운로드)**를 클릭하고 저장합니다(저장 위치 참고



).

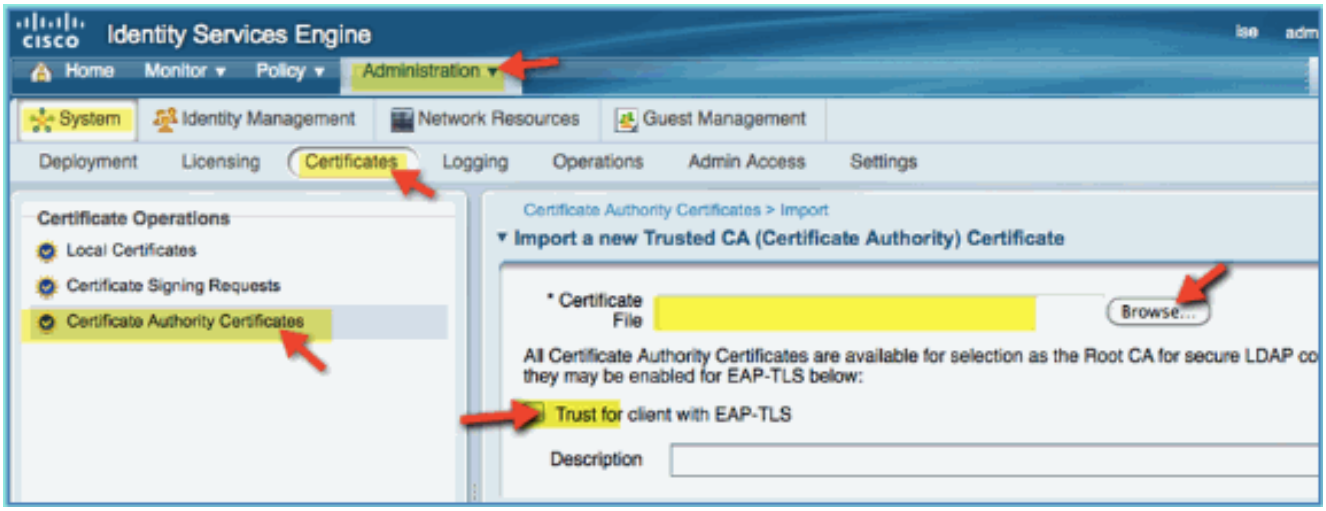
5. https://<Pod-ISE>에 대한 브라우저 창을 엽니다.
6. Administration(관리) **> System(시스템) > Certificates(인증서) > Certificates Authority Certificates(인증 기관 인증서)로 이동합니다**

.



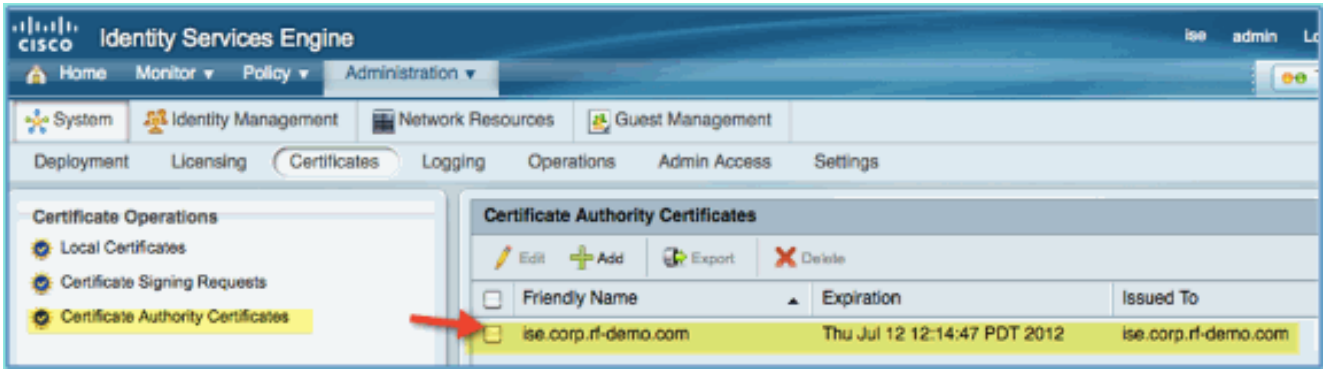
7. Certificate **Authority Certificates 작업**을 선택하고 이전에 다운로드한 CA 인증서를 찾습니다.
8. Trust **for client with EAP-TLS(EAP-TLS를 사용하는 클라이언트에 대해 신뢰)**를 선택한 다음 submit(제출)을 선택합니다

.



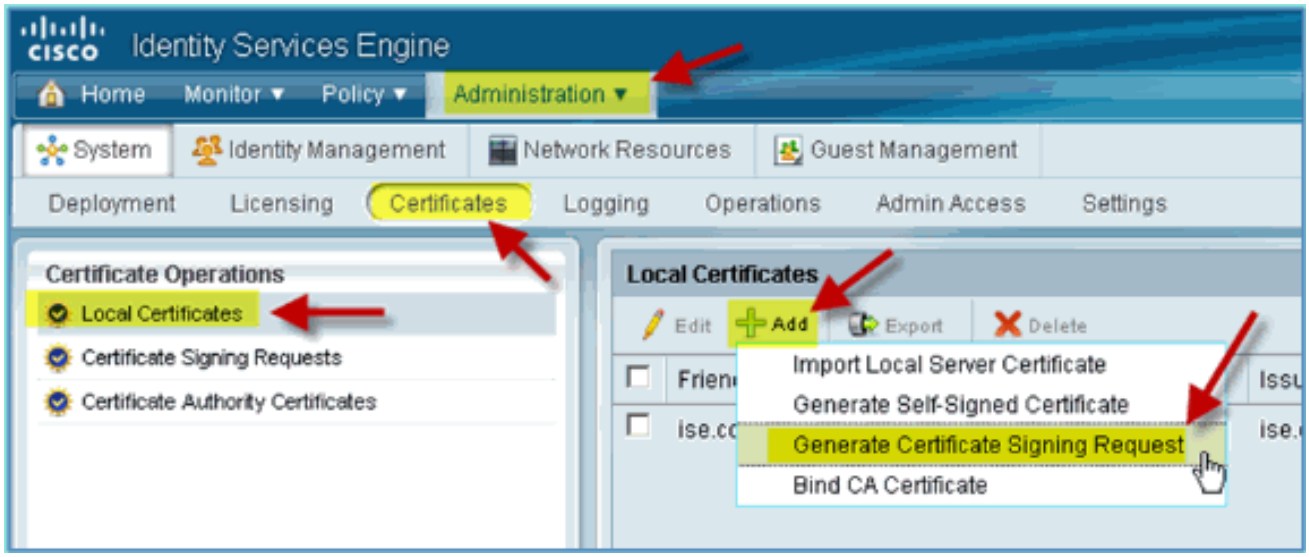
9. CA가 루트 CA로 신뢰받는 상태로 추가되었는지 확인합니다

.



10. 브라우저에서 **Administration > System > Certificates > Certificates Authority Certificates로 이동합니다**.
11. Add(**추가**)를 클릭한 다음 **Generate Certificate Signing Request(인증서 서명 요청 생성)를 클릭합니다**

.



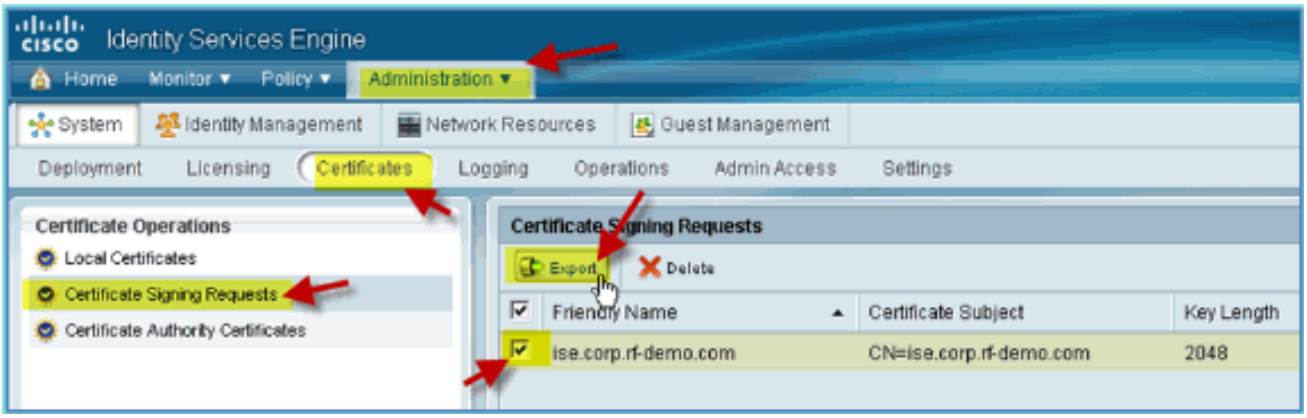
12. 다음 값을 제출합니다.인증서 주체: CN=ise.corp.rf-demo.com키 길이: 2048

13. ISE는 CSR 페이지에서 CSR을 사용할 수 있다는 프롬프트를 표시합니다. **OK(확인)**를 클릭합니다

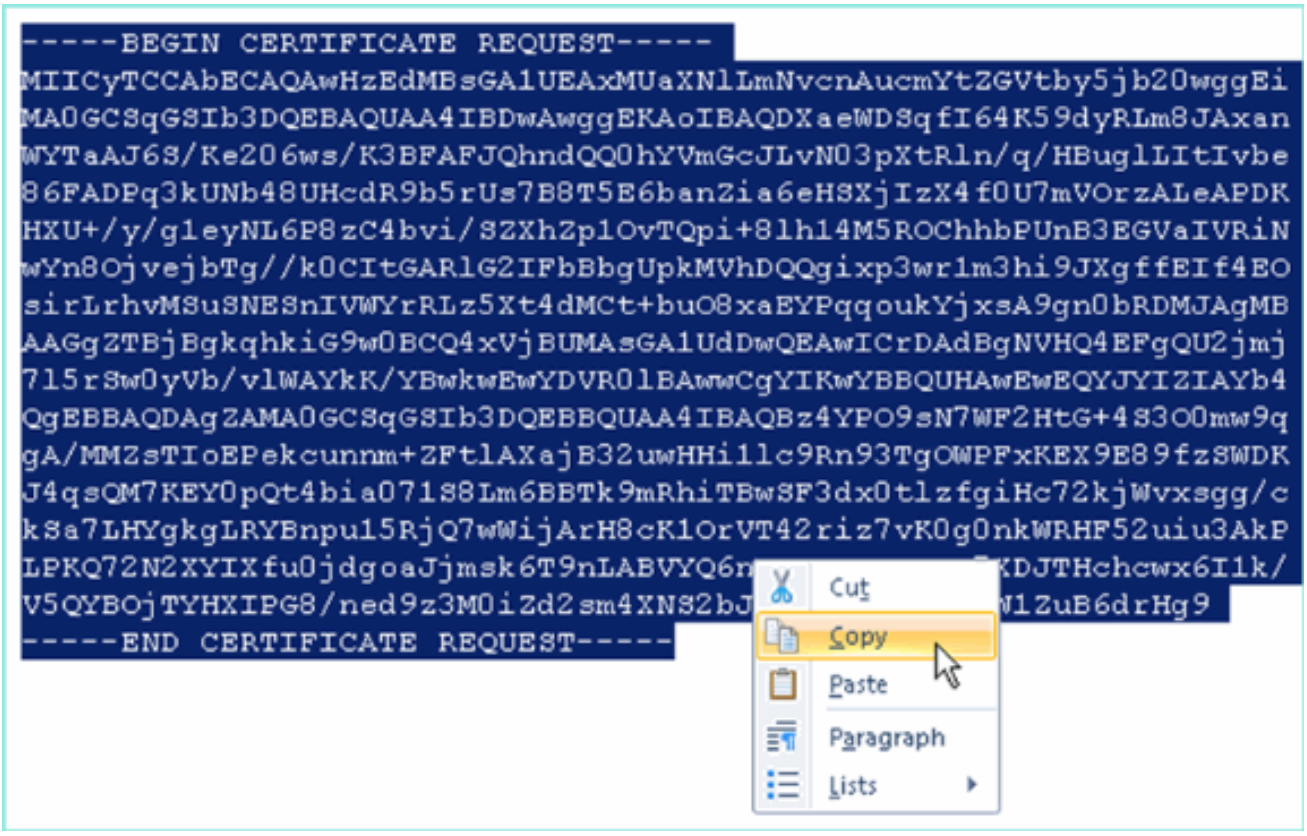
.

14. ISE CSR 페이지에서 CSR을 선택하고 Export를 **클릭합니다**.
15. 파일을 모든 위치(예: 다운로드 등)에 저장합니다.
16. 파일은 *.pem으로 저장됩니다

.

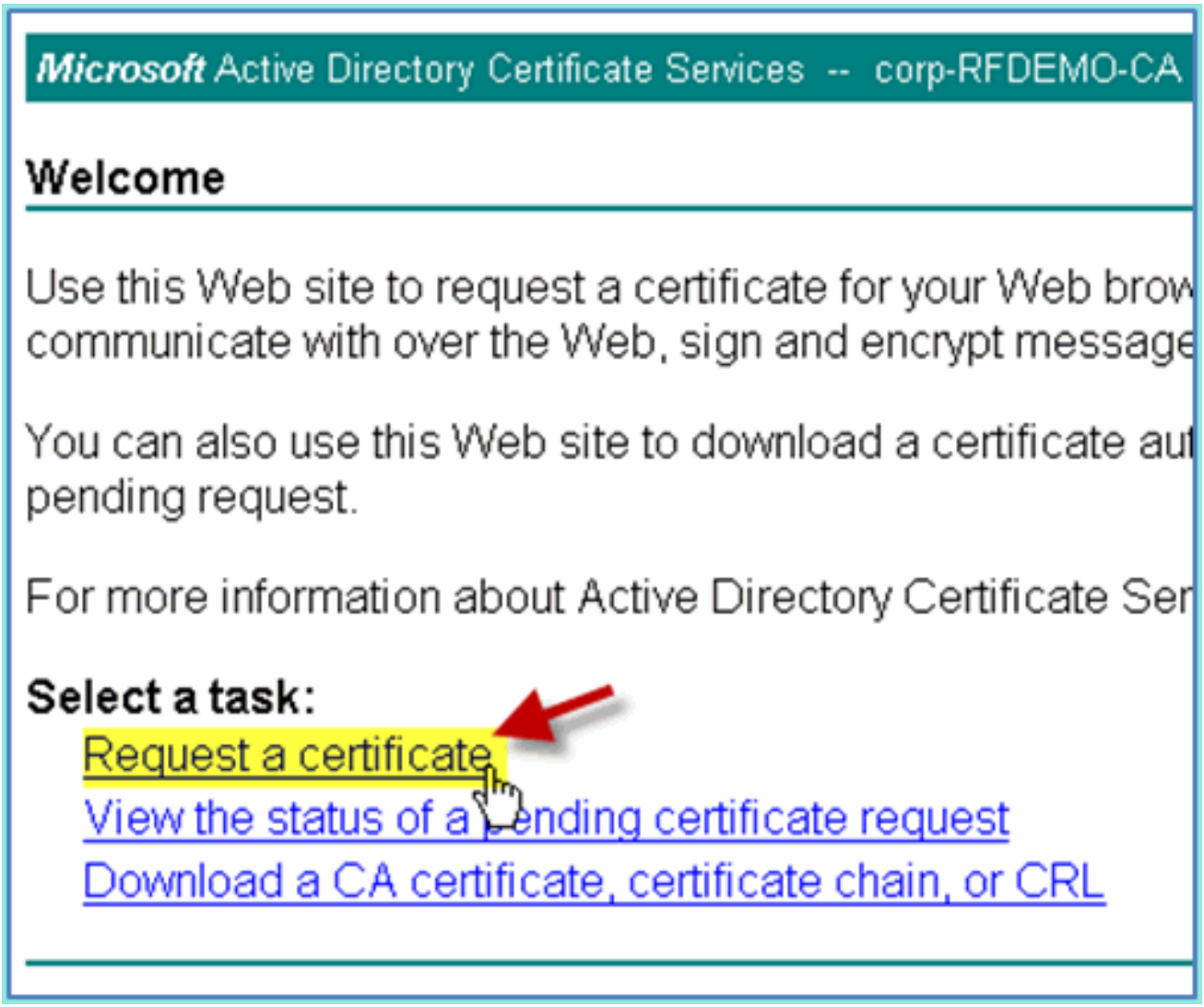


17. CSR 파일을 찾아 Notepad/Wordpad/TextEdit로 편집합니다.
18. 내용을 복사합니다(모두 선택 > 복사
).



19. https://<Pod-AD>/certsrv에 대한 브라우저 창을 엽니다.
20. Request **a certificate(인증서 요청)를 클릭합니다**

.

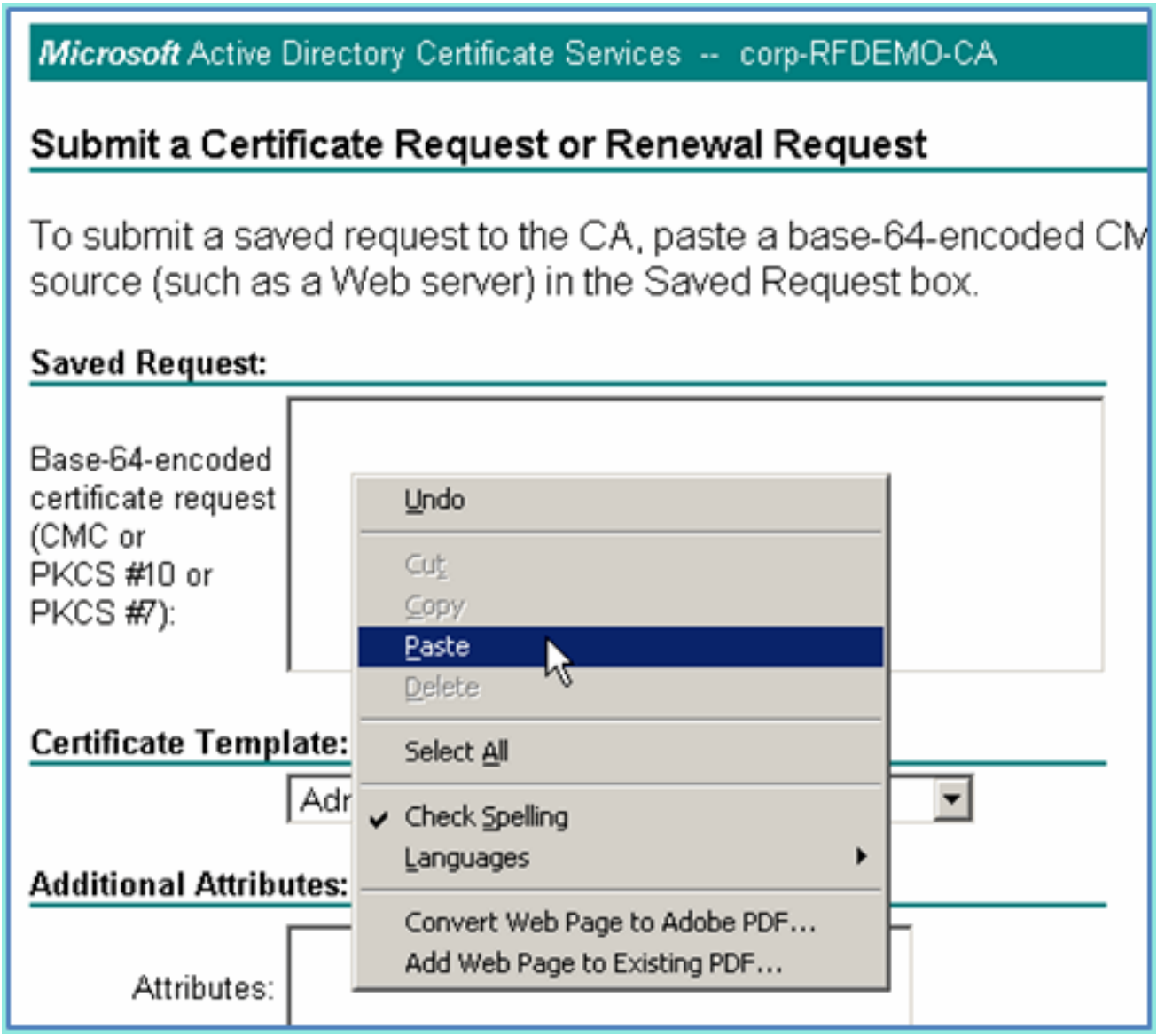


21. **고급 인증서 요청**을 제출하려면 **클릭합니다**

.

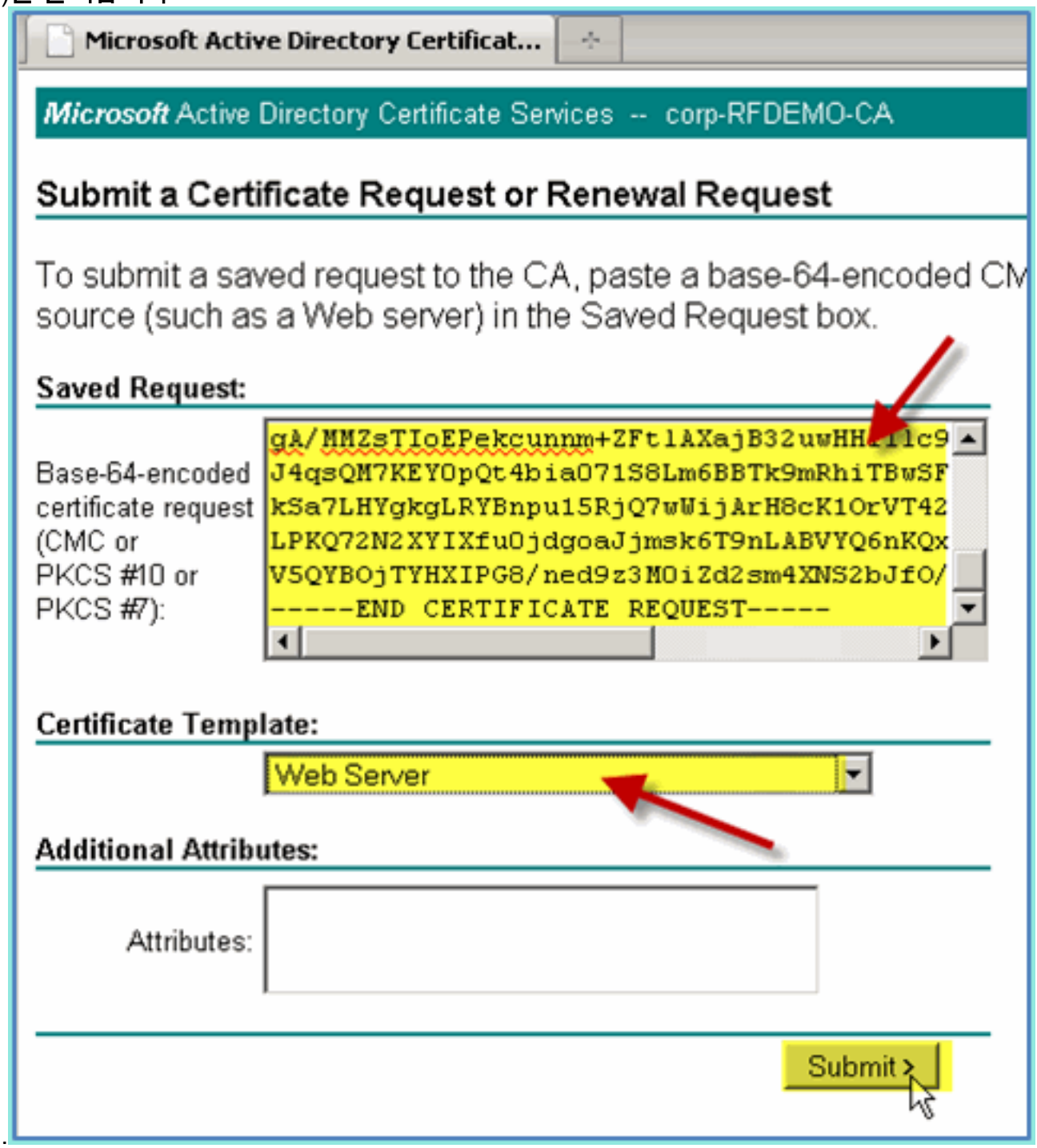
22. Saved Request(저장된 요청) 필드에 CSR 내용을 붙여넣습니다

.



23. Certificate **Template(인증서 템플릿)**으로 Web Server(웹 서버)를 선택한 다음 Submit(제출

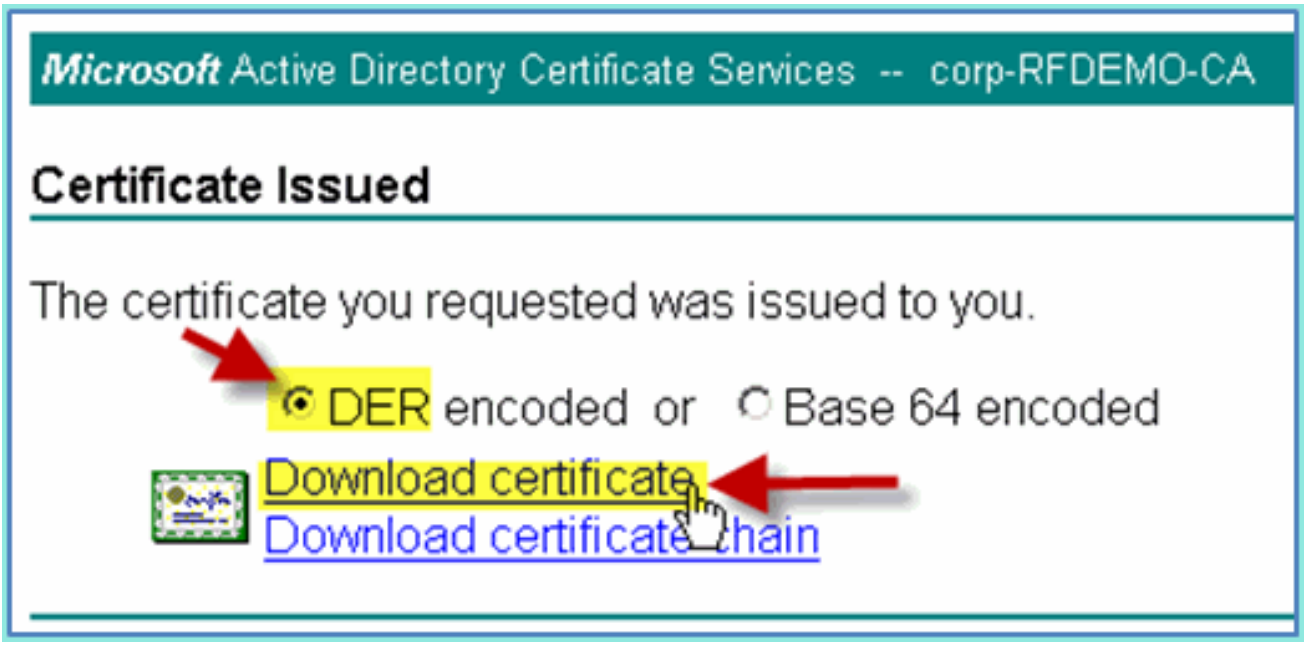
)을 클릭합니다



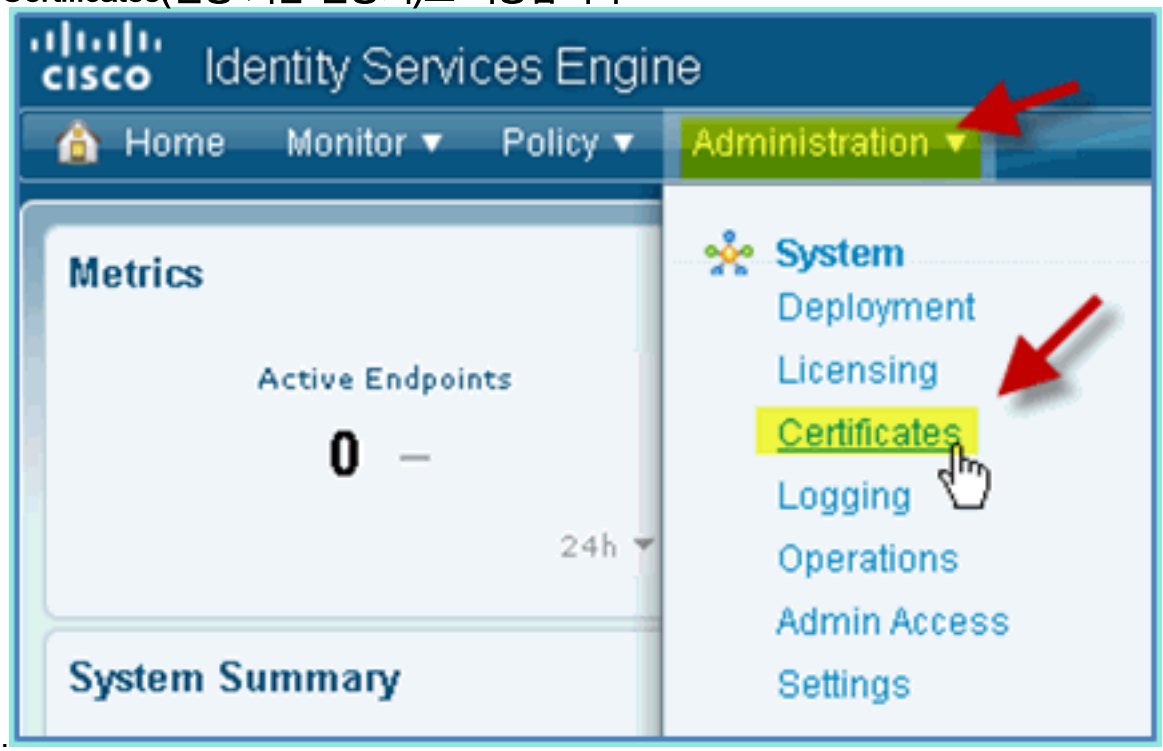
.

24. DER encoded(**DER 인코딩**)를 선택한 다음 **Download certificate(인증서 다운로드)**를 클릭합니다

.



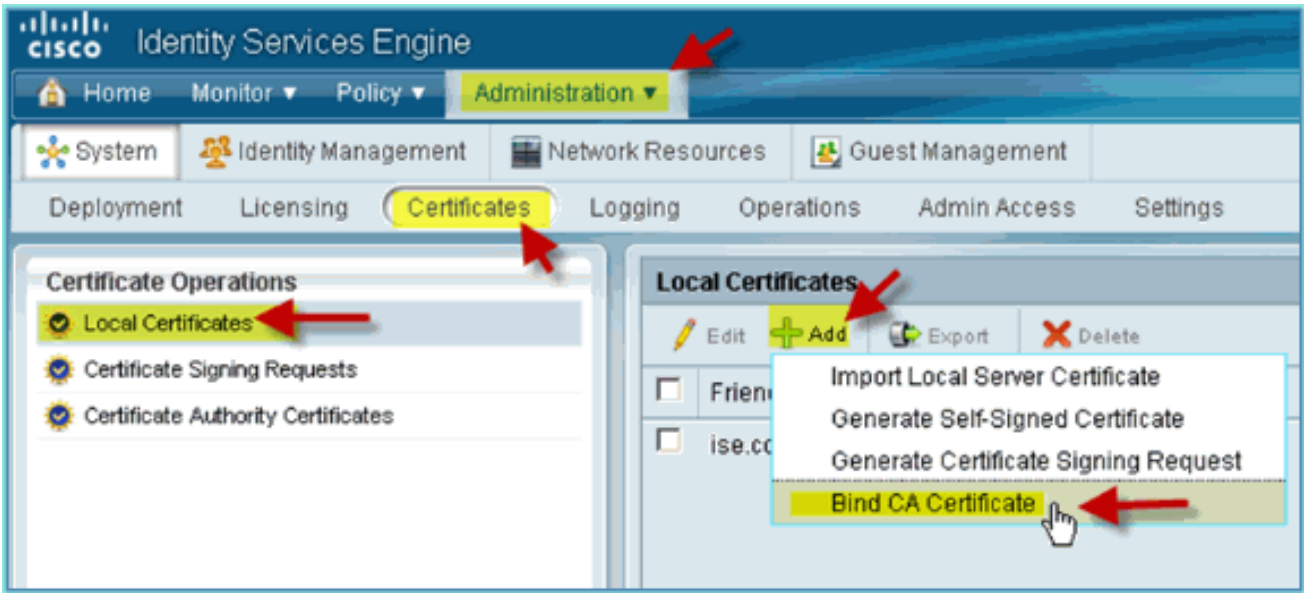
25. 파일을 알려진 위치(예: 다운로드)에 저장합니다.
26. Administration(관리) > System(시스템) > Certificates(인증서) > Certificates Authority Certificates(인증 기관 인증서)로 이동합니다



.

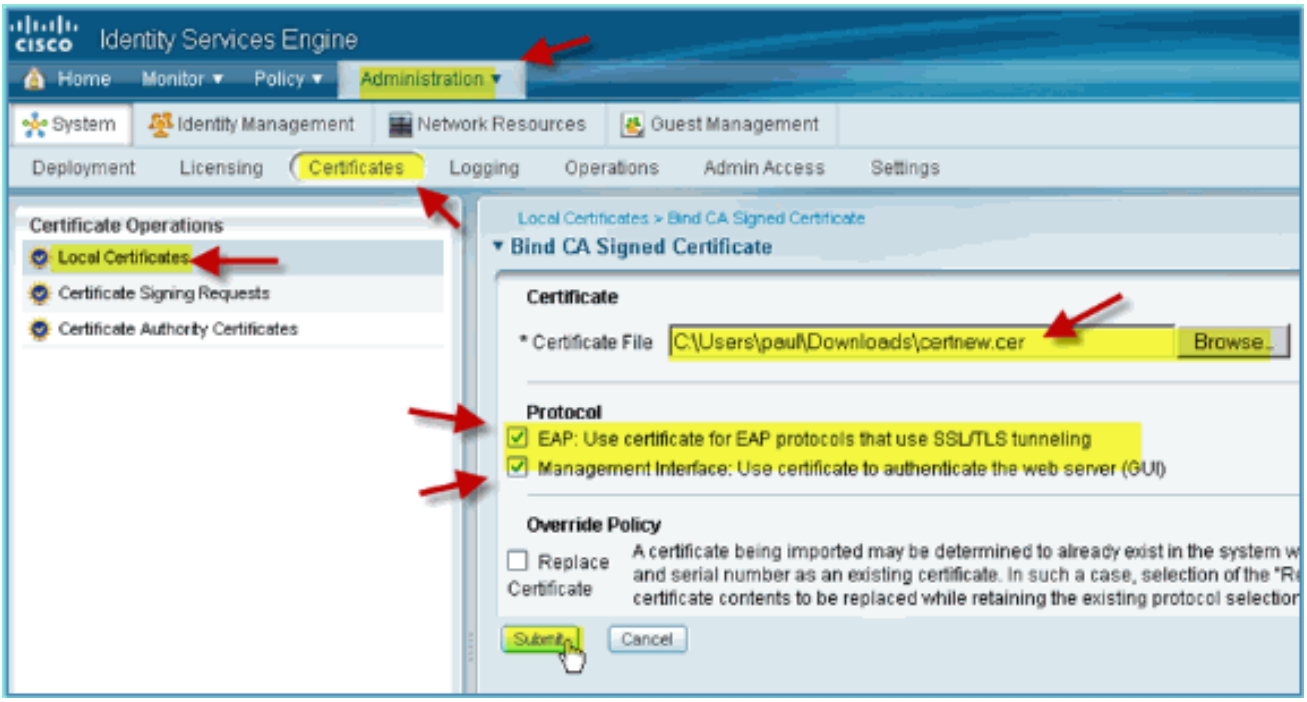
27. Add(추가) > Bind CA Certificate(CA 인증서 바인딩)를 클릭합니다

.



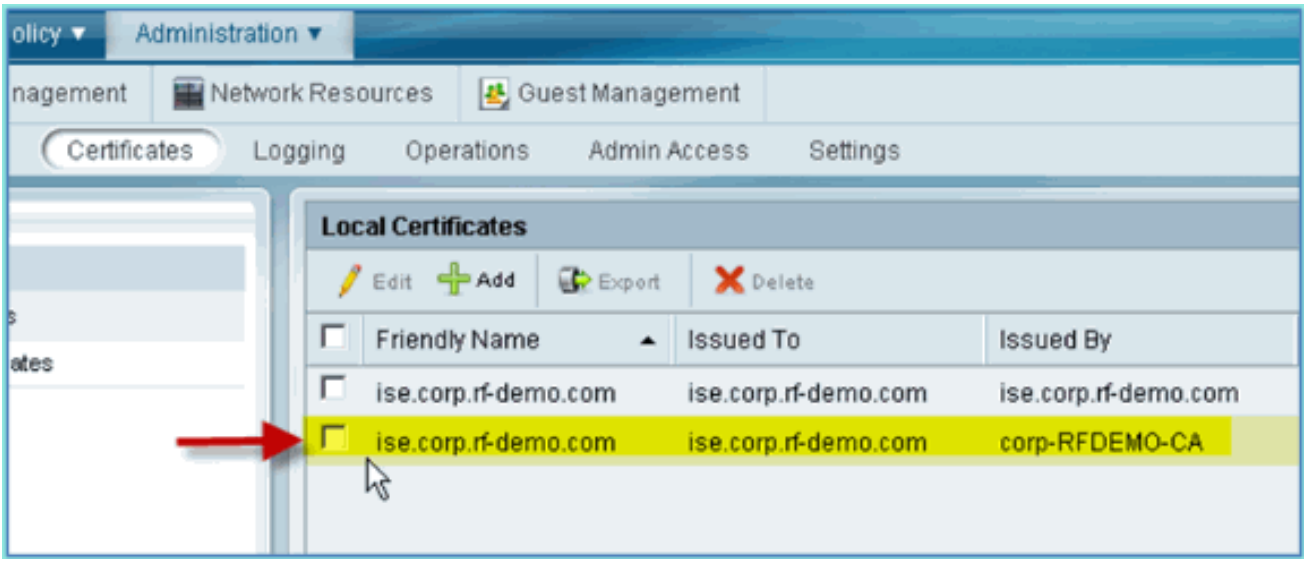
28. 이전에 다운로드한 CA 인증서를 찾습니다

.



29. Protocol EAP와 **Management Interface**를 모두 **선택한** 다음 Submit(제출)**을 클릭합니다**.
30. CA가 루트 CA로 신뢰받는 상태로 추가되었는지 확인합니다

.

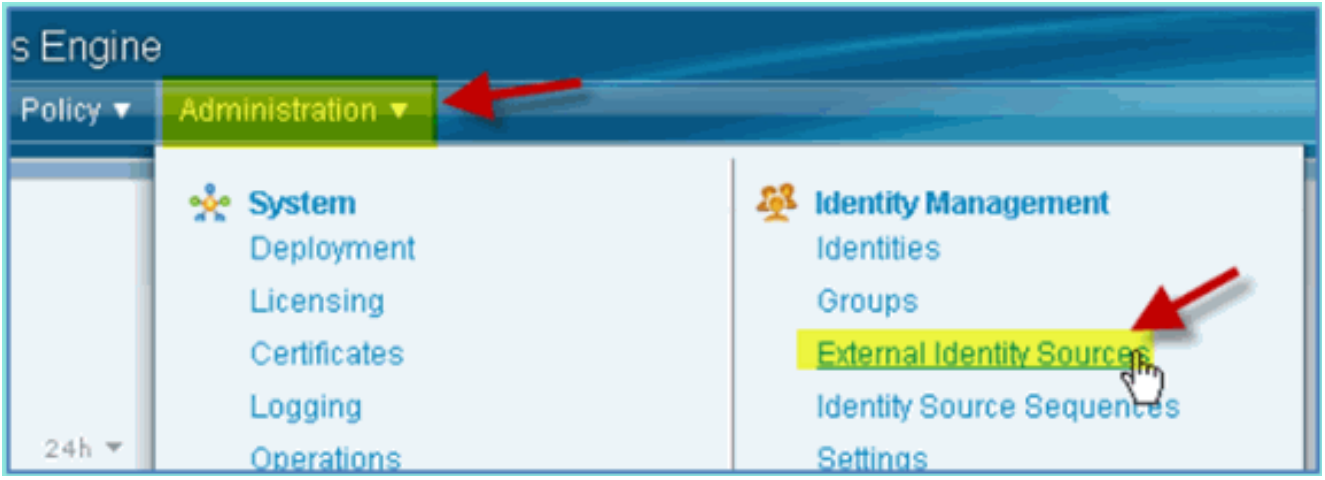


Windows 2008 Active Directory 통합

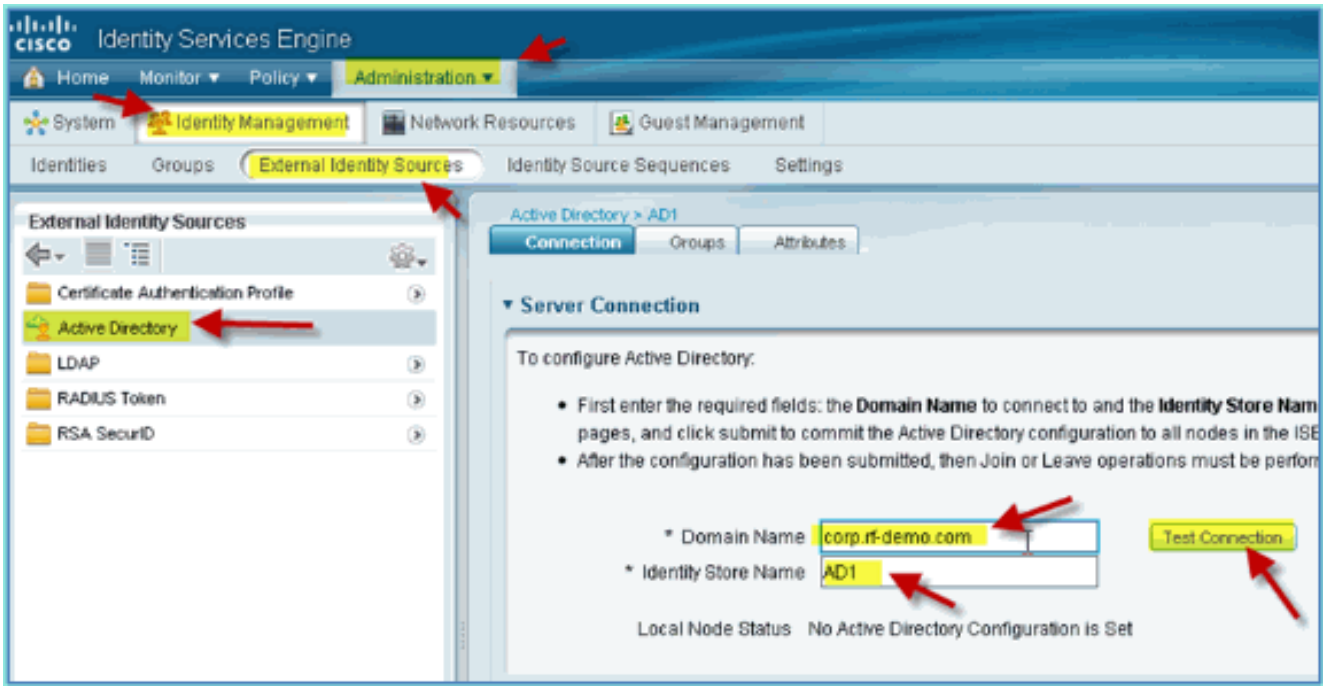
ISE는 사용자/머신 인증을 위해 또는 권한 부여 정보 사용자 특성을 검색하기 위해 AD(Active Directory)와 직접 통신할 수 있습니다. AD와 통신하려면 ISE가 AD 도메인에 '조인'되어야 합니다. 이 연습에서는 ISE를 AD 도메인에 가입시키고 AD 통신이 올바르게 작동하는지 확인합니다.

다음 단계를 완료하십시오.

1. ISE를 AD 도메인에 가입시키려면 ISE에서 Administration(관리) > Identity **Management(ID 관리) > External Identity Sources(외부 ID 소스)로 이동합니다**
.

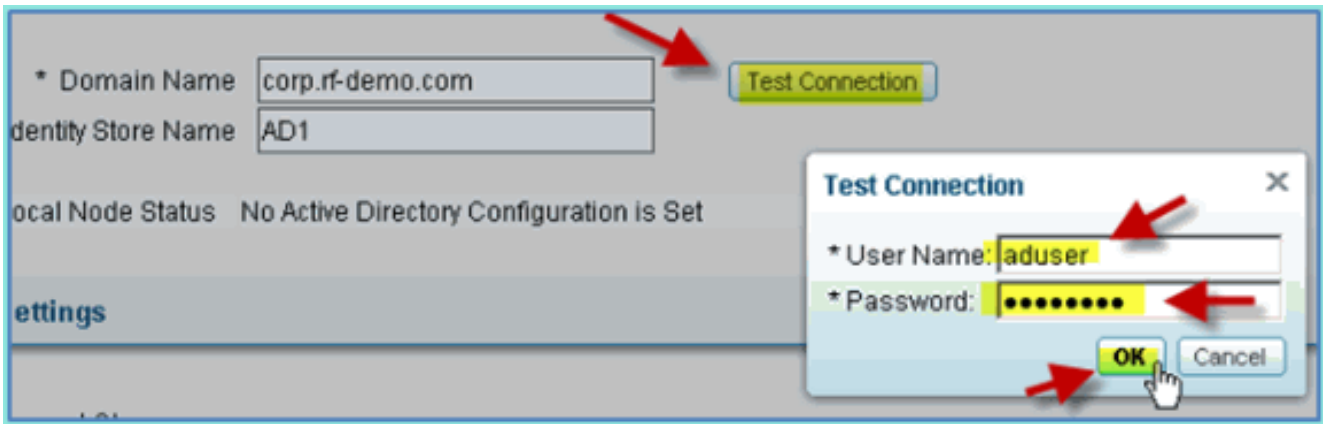


2. 왼쪽 창(외부 ID 소스)에서 **Active Directory**를 선택합니다.
3. 오른쪽에서 Connection(연결) 탭**을** 선택하고 다음을 입력합니다.도메인 이름: corp.rf-demo.comID 저장소 이름:
AD1



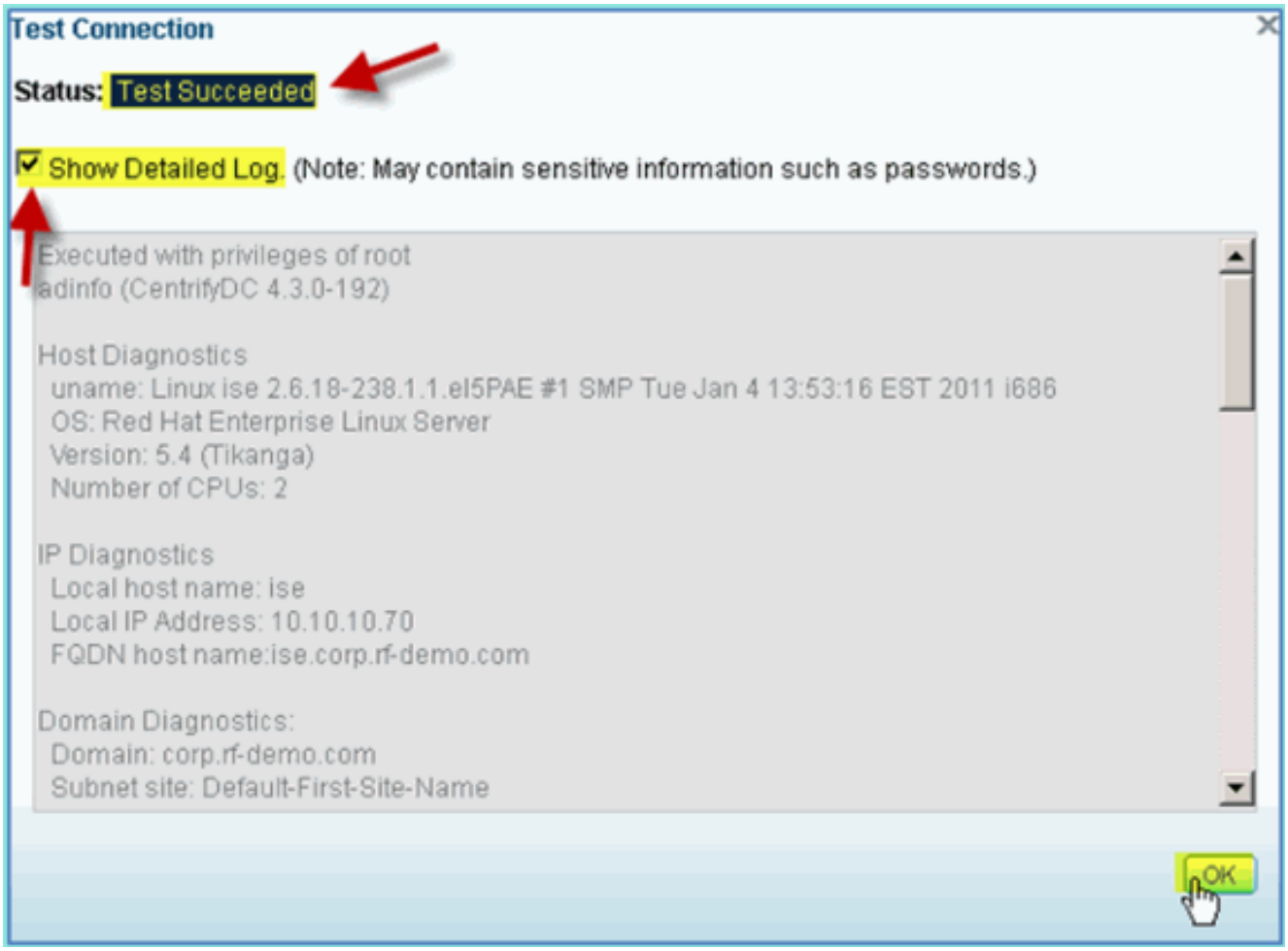
4. Test **Connection(연결 테스트)**을 클릭합니다. AD 사용자 이름(aduser/Cisco123)을 입력하고 **OK**(확인)를 클릭합니다

.



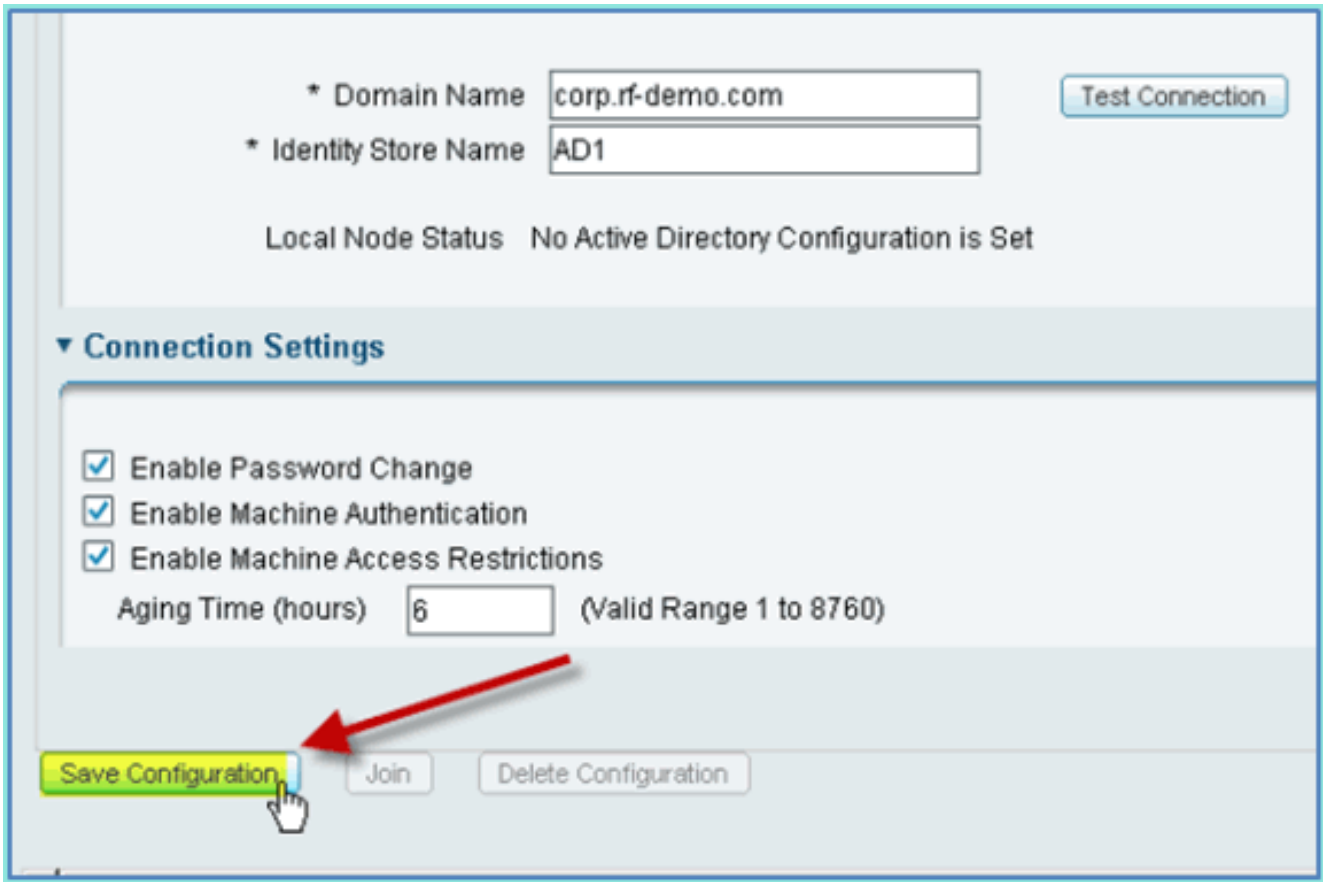
5. Test Status(테스트 상태)에 **Test Succeeded(테스트 성공)가 표시되는지 확인합니다**.
6. Show Detailed Log를 선택하고 문제 해결에 유용한 세부 정보를 확인합니다. OK(**확인**)를 클릭하여 계속합니다

.



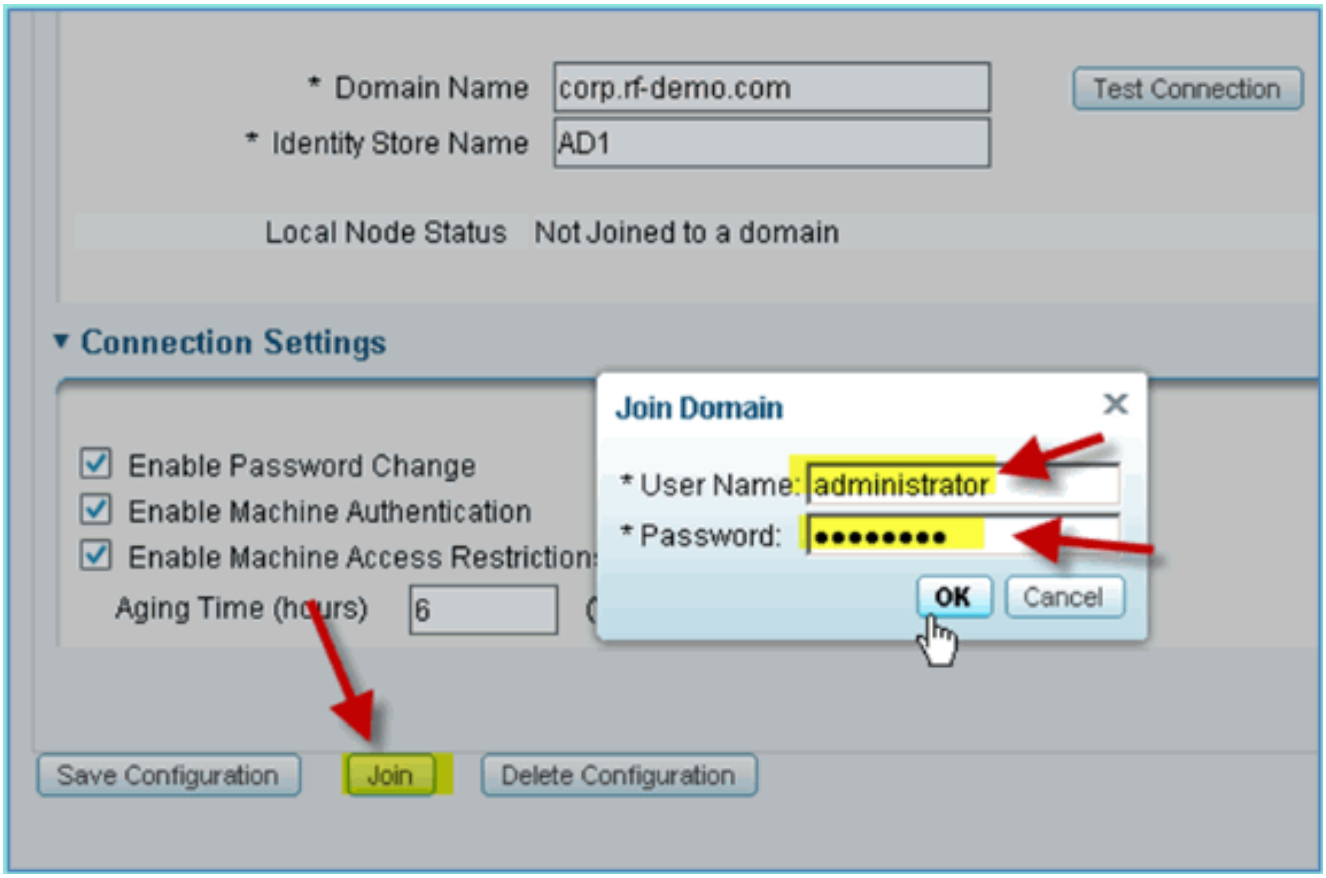
7. Save Configuration(컨피그레이션 **저장)을 클릭합니다**

.



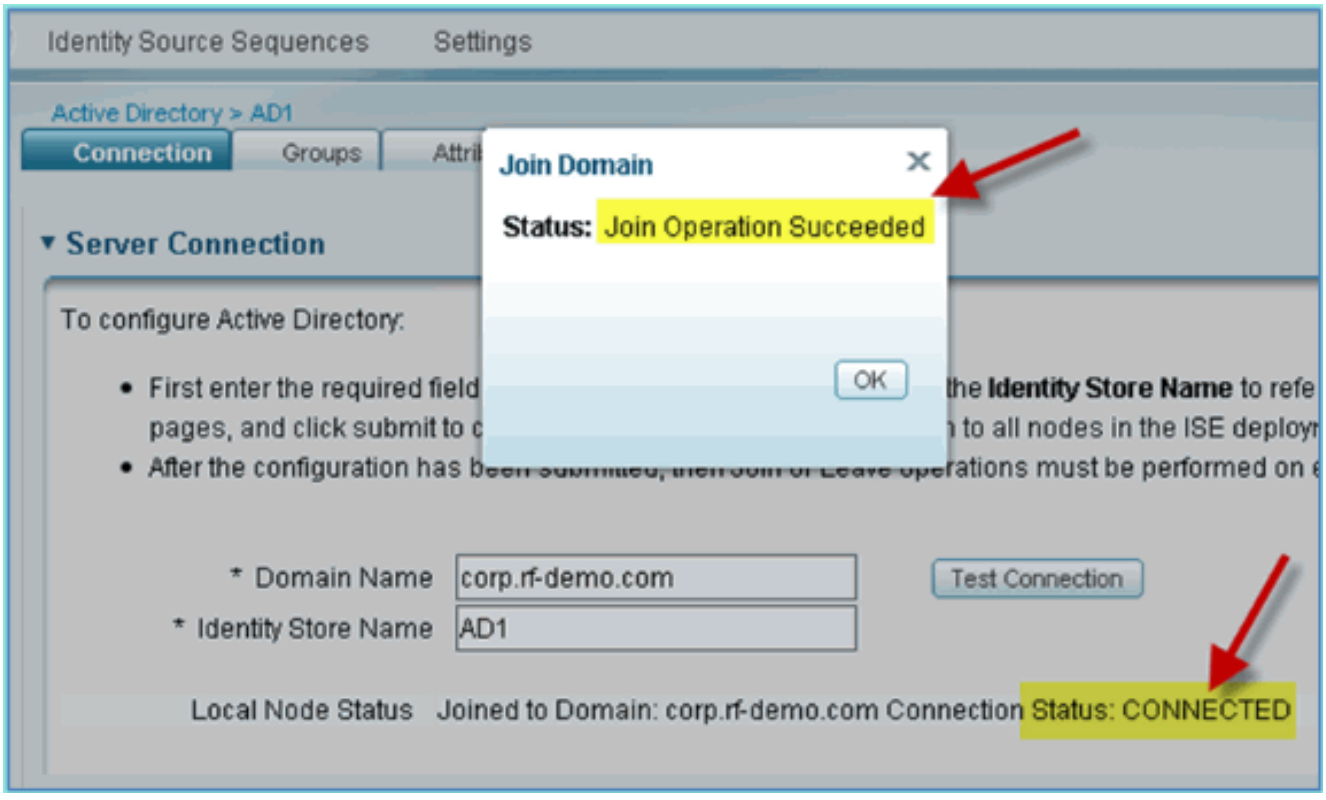
8. Join을 **클릭합니다**. AD 사용자(administrator/Cisco123)를 입력하고 **OK**(확인)를 클릭합니다

.



9. Join Operation Status(조인 작업 상태)에 Succeeded(**성공**)가 표시되는지 확인한 다음 **OK(확인)**를 클릭하여 계속합니다.Server Connection Status(서버 연결 상태)에는 CONNECTED(연결됨)**가 표시됩니다**. 이 상태가 언제든지 변경되면 테스트 연결을 통해 AD 작업 관련 문제를 해결할 수 있습니다

.



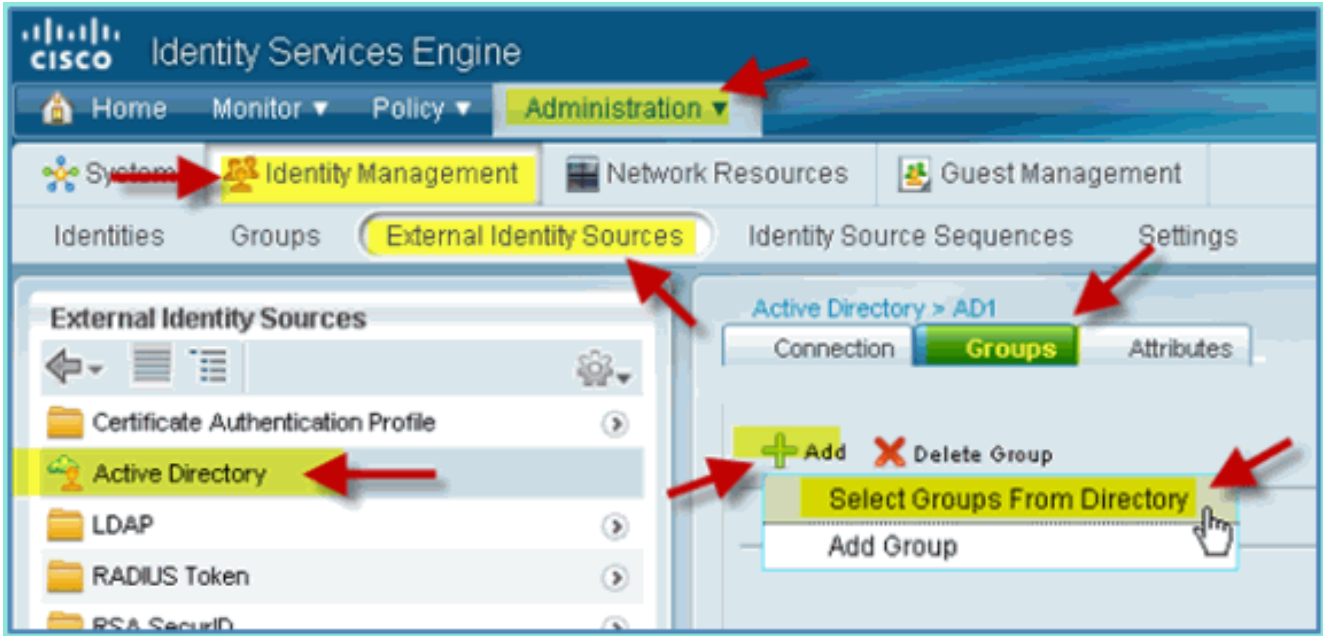
Active Directory 그룹 추가

AD 그룹이 추가되면 ISE 정책에 대해 더 세분화된 제어가 허용됩니다. 예를 들어, AD 그룹은 정책이 사용자만 제한되었던 이전 ISE 1.0 연습에서 관련 버그가 경험되지 않은 상태에서 직원 또는 계약자 그룹과 같은 기능적 역할에 따라 차별화될 수 있습니다.

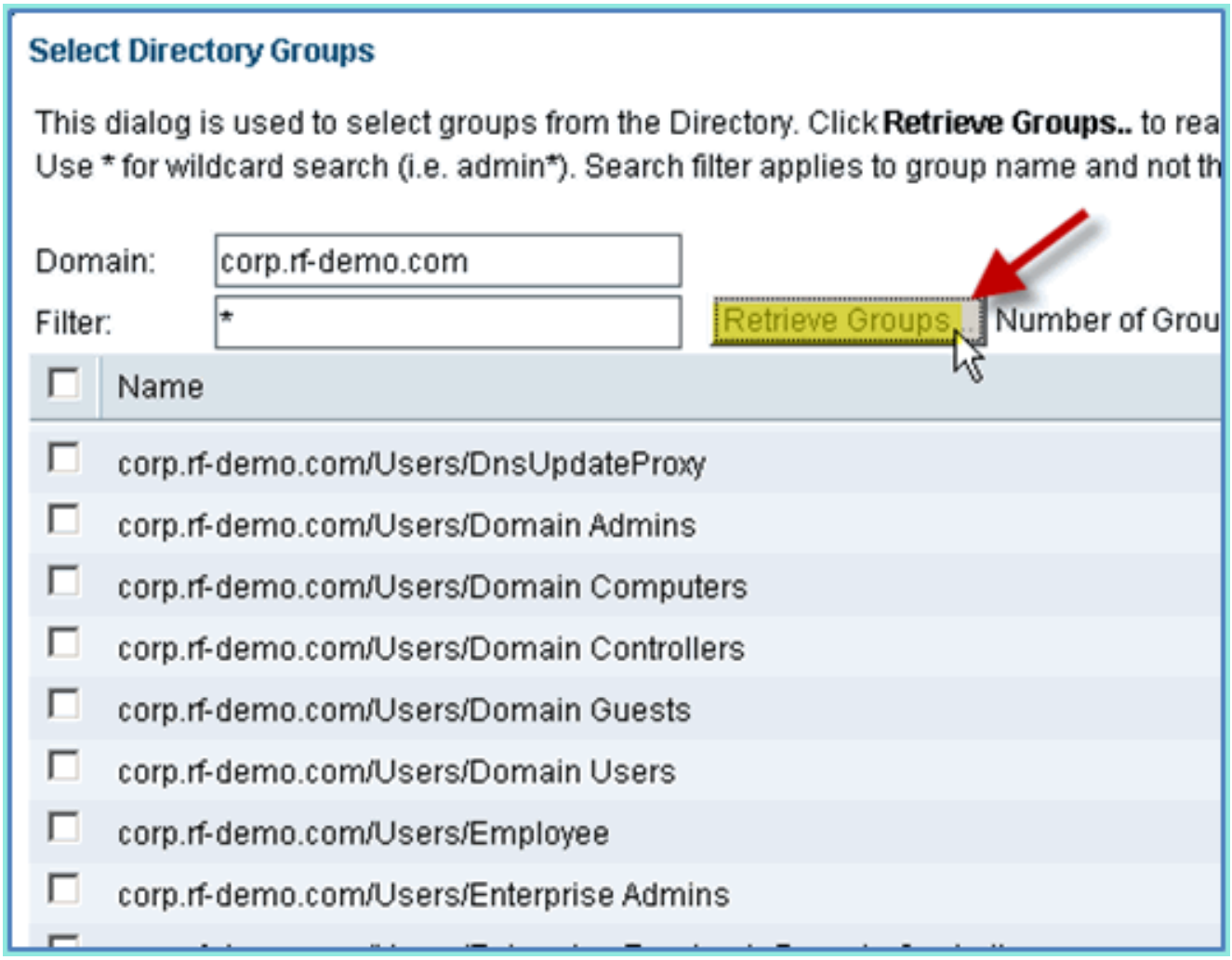
이 실습에서는 Domain Users(도메인 사용자) 및/또는 Employee(직원) 그룹만 사용됩니다.

다음 단계를 완료하십시오.

1. ISE에서 Administration(관리) > Identity **Management(ID 관리) > External Identity Sources(외부 ID 소스)로 이동합니다**.
2. **Active Directory > Groups 탭을** 선택합니다.
3. +Add**(추가)**를 클릭한 다음 **Groups From Directory(디렉토리에서 그룹)를 선택합니다**
.

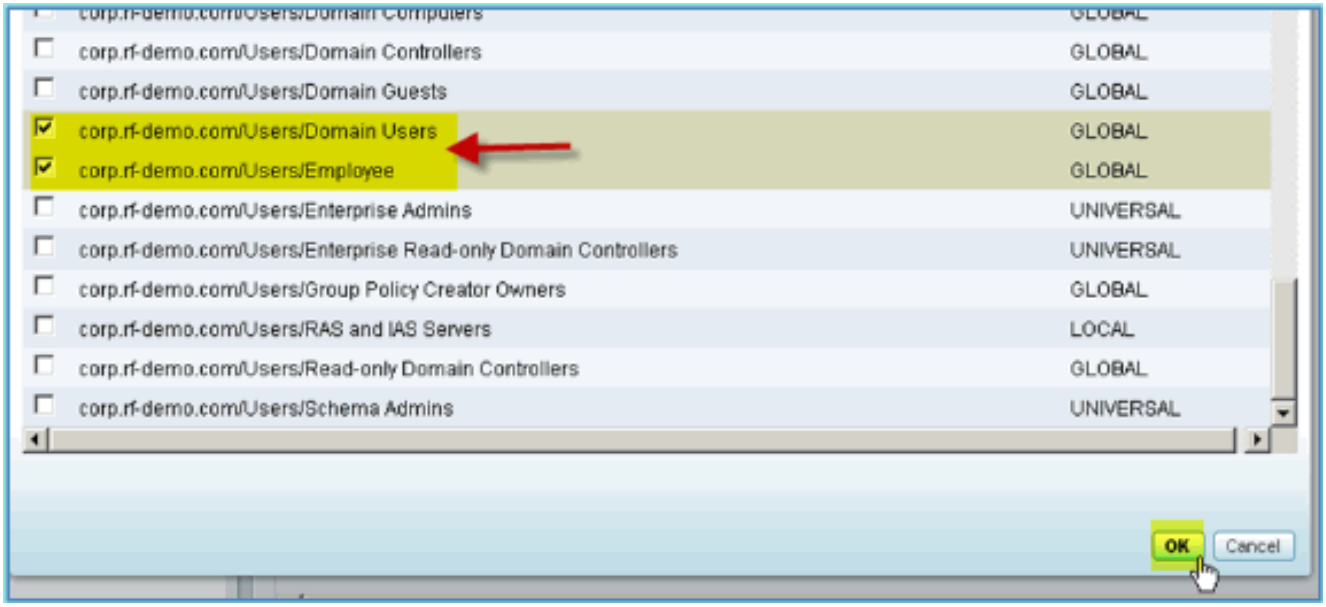


4. 후속 창(디렉터리 그룹 선택)에서 도메인(corp-rf-demo.com) 및 필터(*)의 기본값을 수락합니다. 그런 다음 Retrieve Groups(**그룹 검색)를 클릭합니다**
.



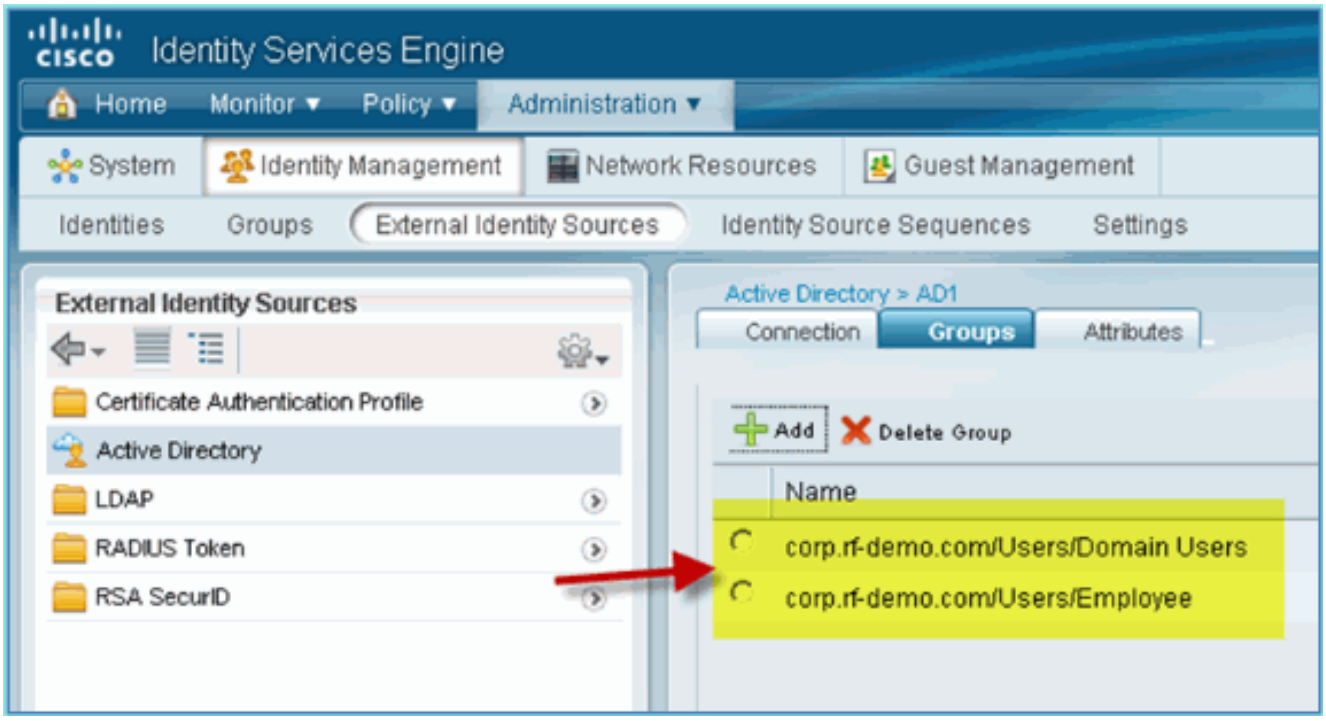
5. **Domain Users(도메인 사용자)** 및 **Employee** groups(직원 그룹)의 상자를 선택합니다. 완료되면 **OK(확인)**를 클릭합니다

.



6. 그룹이 목록에 추가되었는지 확인합니다

.

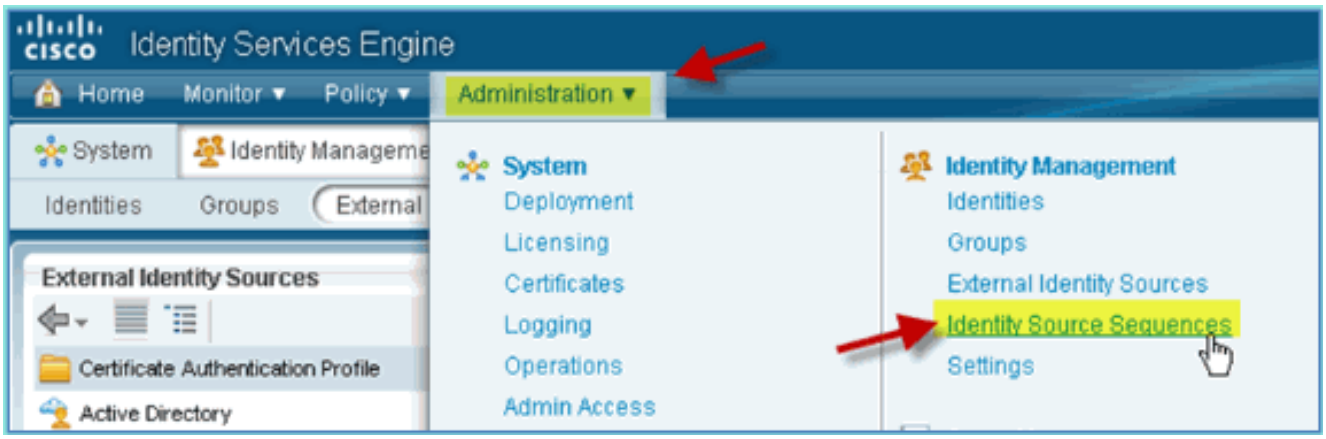


ID 소스 시퀀스 추가

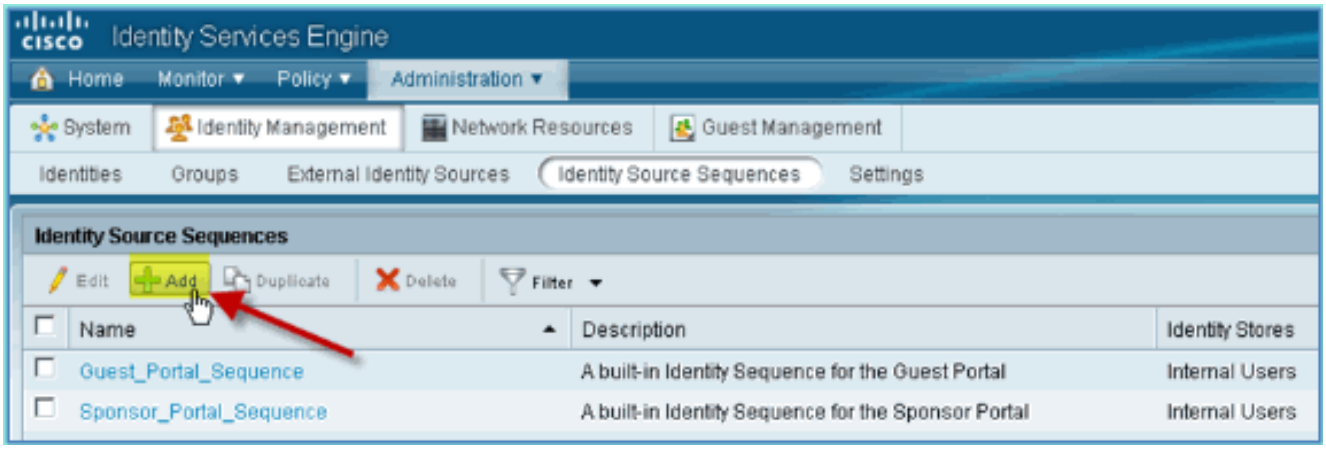
기본적으로 ISE는 내부 사용자를 인증 저장소에 사용하도록 설정됩니다. AD를 추가하면 ISE에서 인증을 확인하는 데 사용할 AD를 포함하도록 시퀀스의 우선 순위를 생성할 수 있습니다.

다음 단계를 완료하십시오.

1. ISE에서 Administration(관리) > Identity **Management(ID 관리) > Identity Source Sequences(ID 소스 시퀀스)로 이동합니다**
.

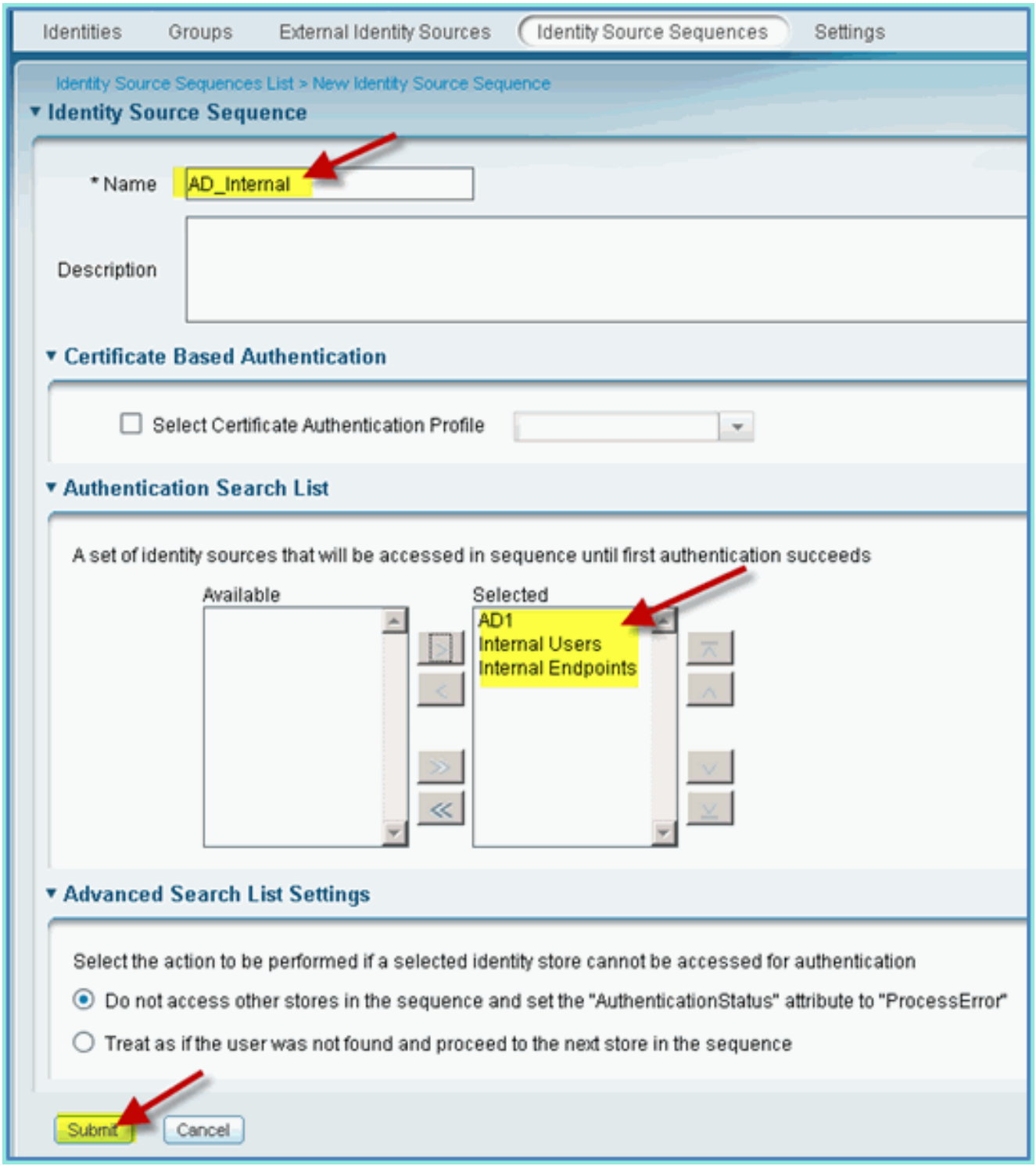


2. 새 시퀀스를 추가하려면 +Add를 클릭합니다
.



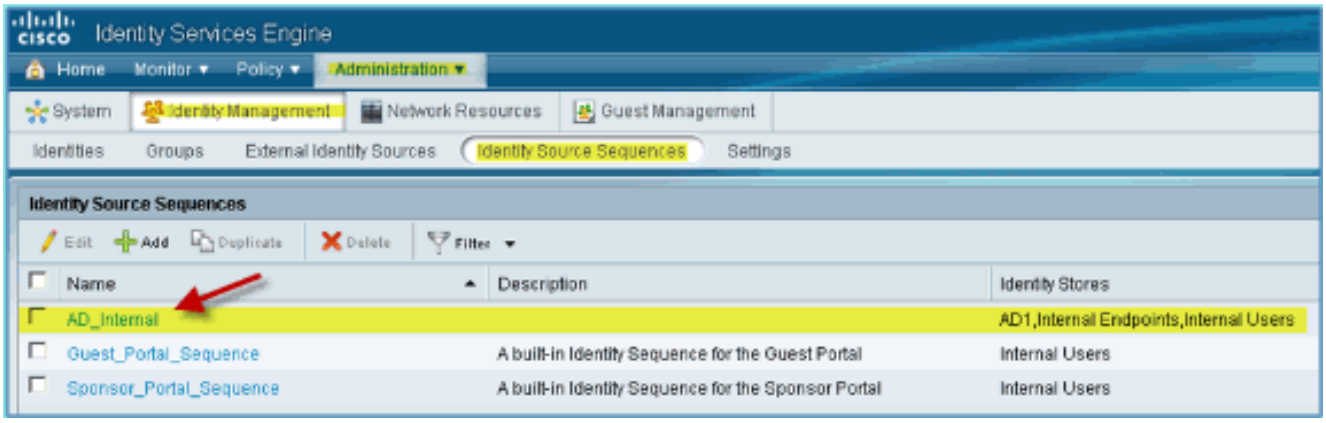
3. 새 이름 **AD_Internal**을 **입력합니다**. 사용 가능한 모든 소스를 Selected(선택됨) 필드에 추가합니다. 그런 다음 필요에 따라 순서를 다시 지정하여 AD1이 목록의 맨 위로 이동합니다. Submit(제출)**을 클릭합니다**

.



4. 시퀀스가 목록에 추가되었는지 확인합니다

.



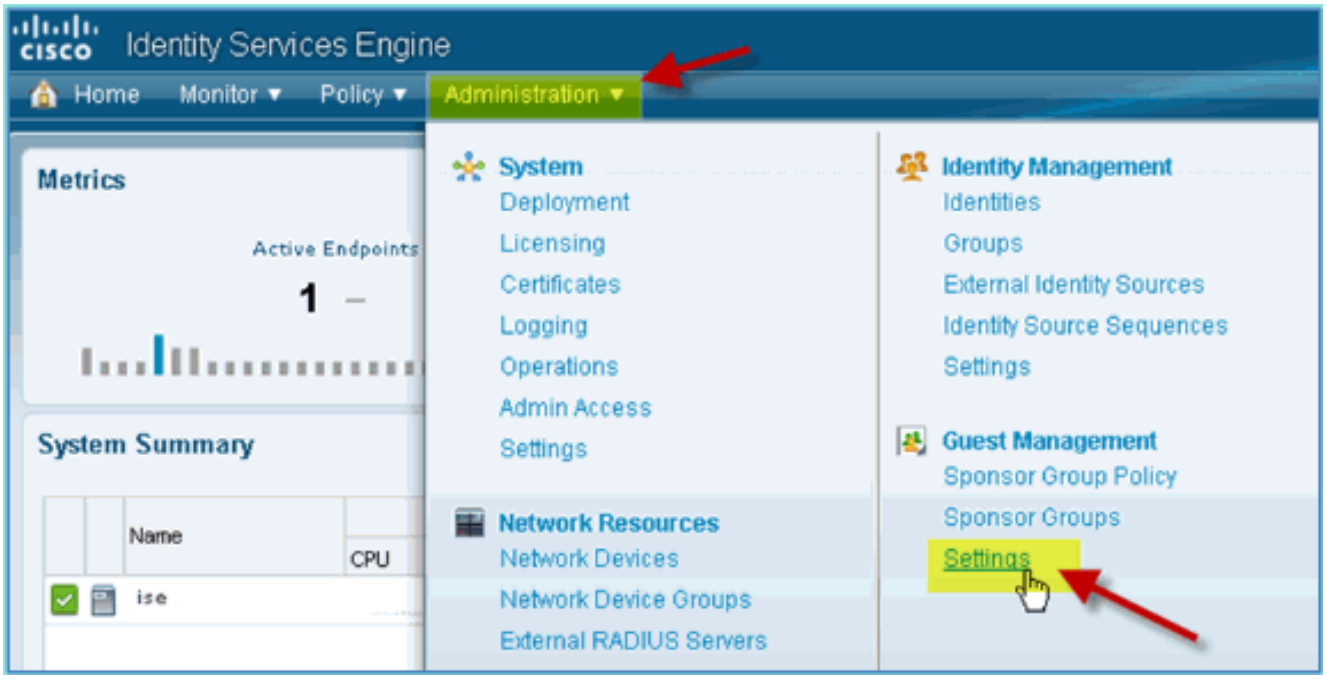
통합 AD를 사용하는 ISE 무선 스폰서 게스트 액세스

AD 도메인 사용자가 게스트 액세스를 스폰서하도록 허용하기 위해 게스트가 정책으로 스폰서되도록 ISE를 구성할 수 있습니다.

다음 단계를 완료하십시오.

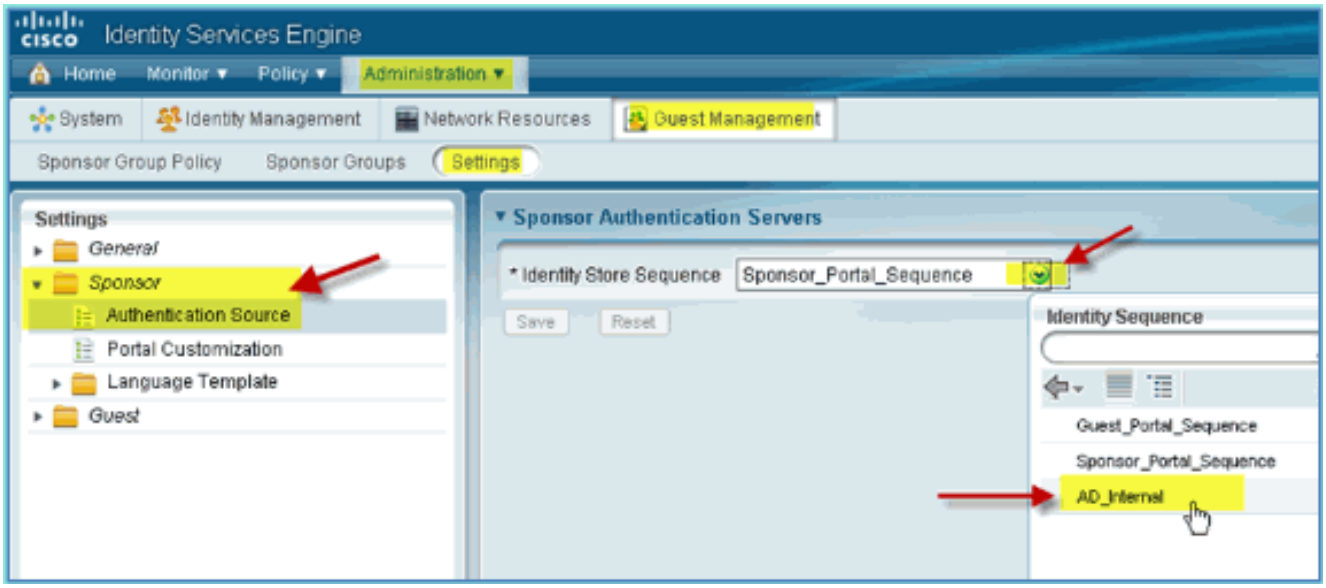
1. ISE에서 Administration(관리) > **Guest Management(게스트 관리) > Settings(설정)로 이동합니다**

.



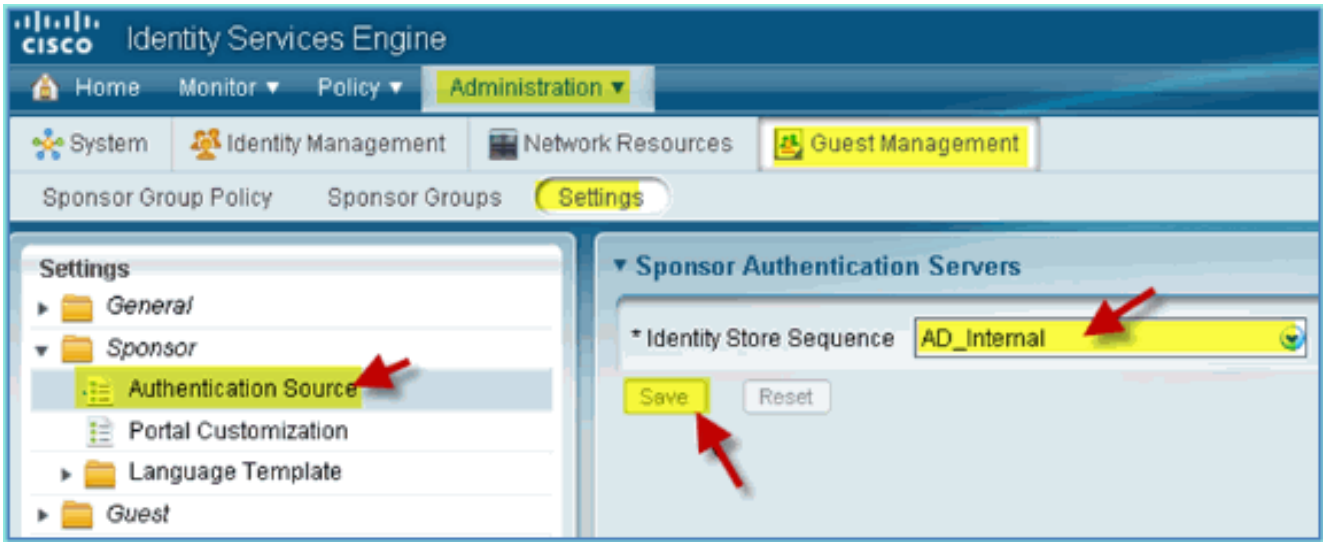
2. Sponsor(**스폰서**)를 확장하고 Authentication Source(**인증 소스**)를 클릭합니다. 그런 다음 **AD_Internal을** Identity Store Sequence로 선택합니다

.



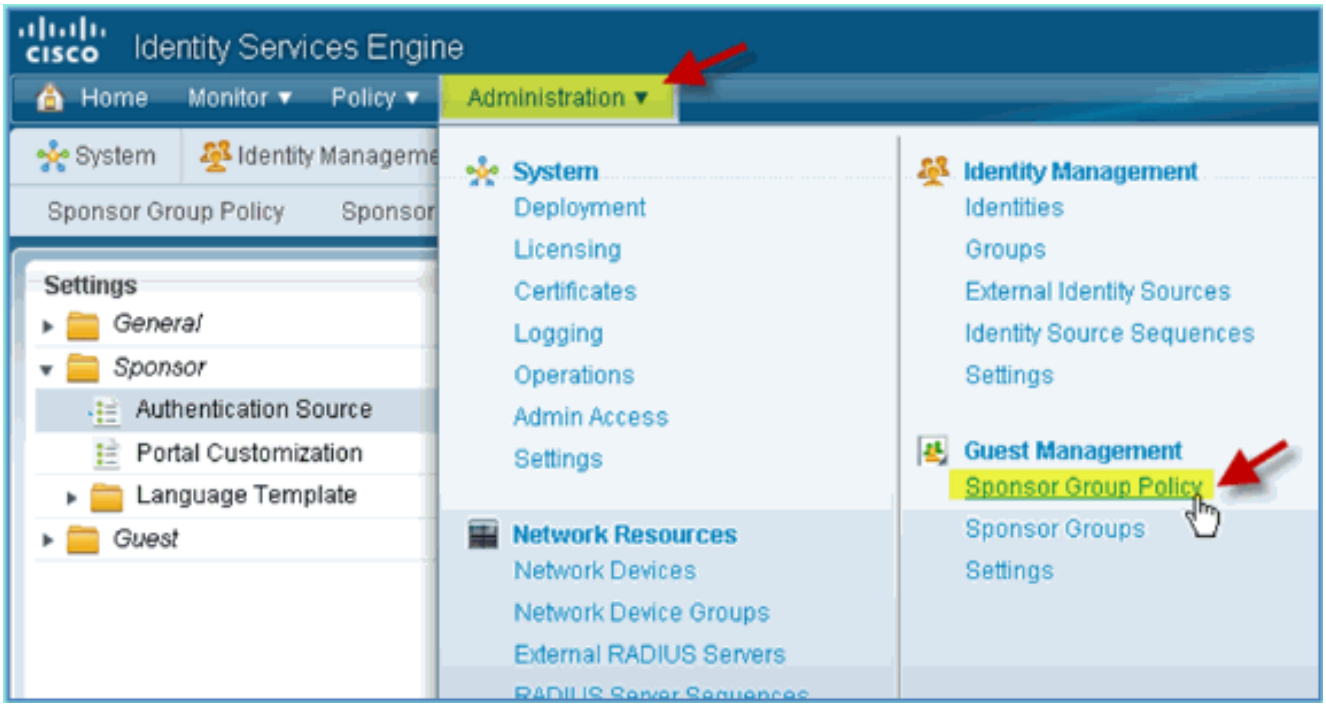
3. AD_Internal을 ID 저장소 시퀀스로 확인합니다. 저장을 **클릭합니다**

.

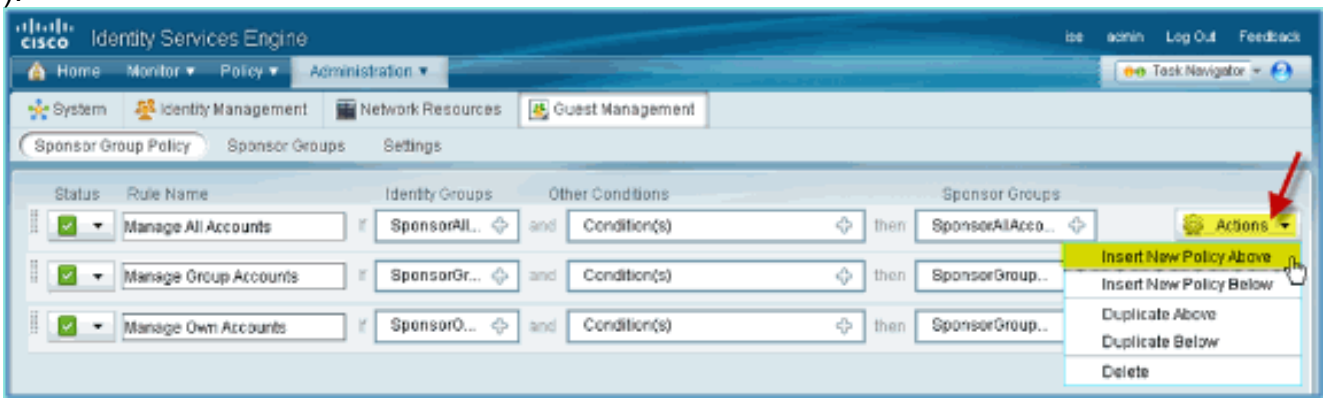


4. Administration(관리) **> Guest Management(게스트 관리) > Sponsor Group Policy(스폰서 그룹 정책)로 이동합니다**

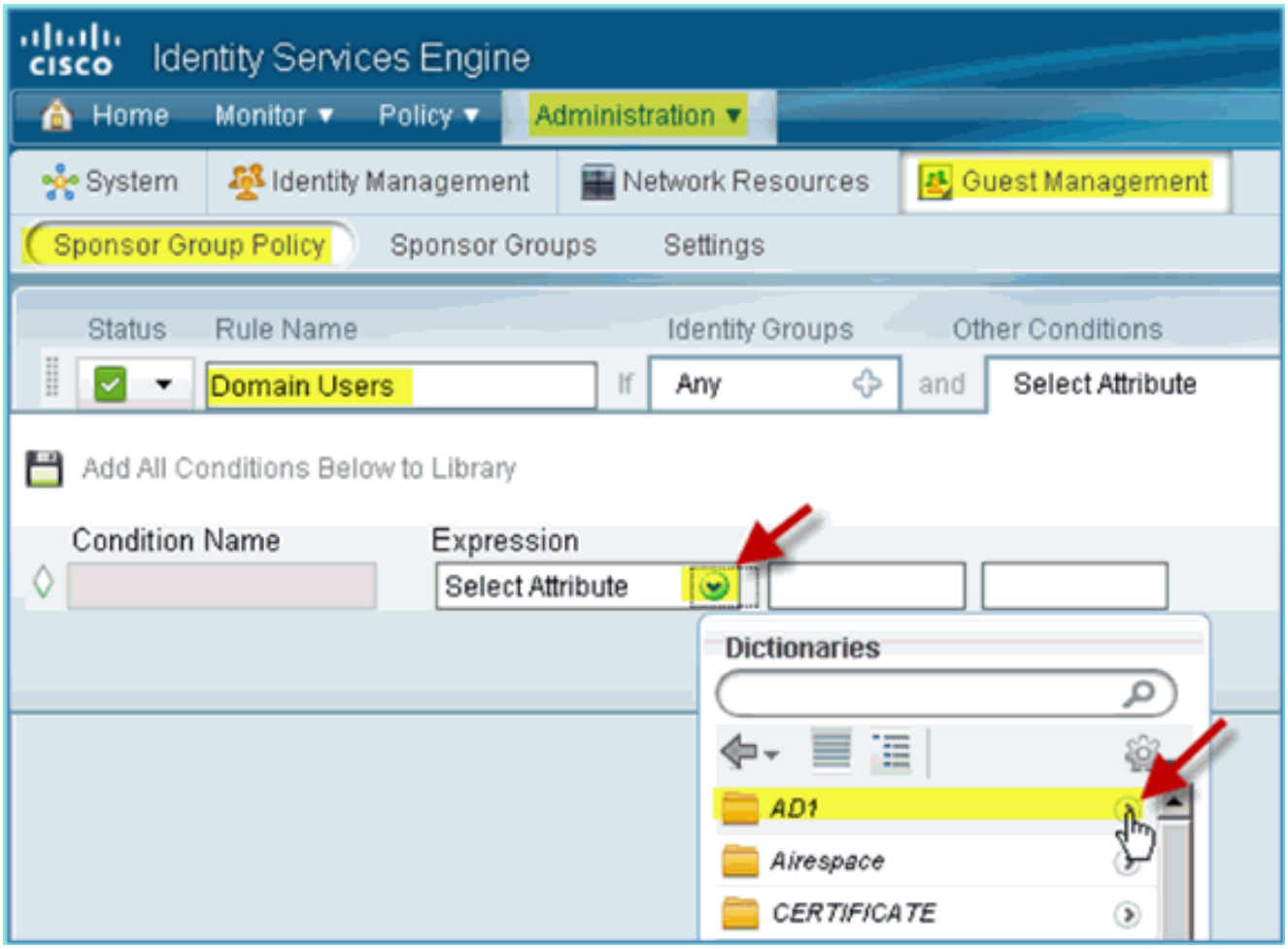
.



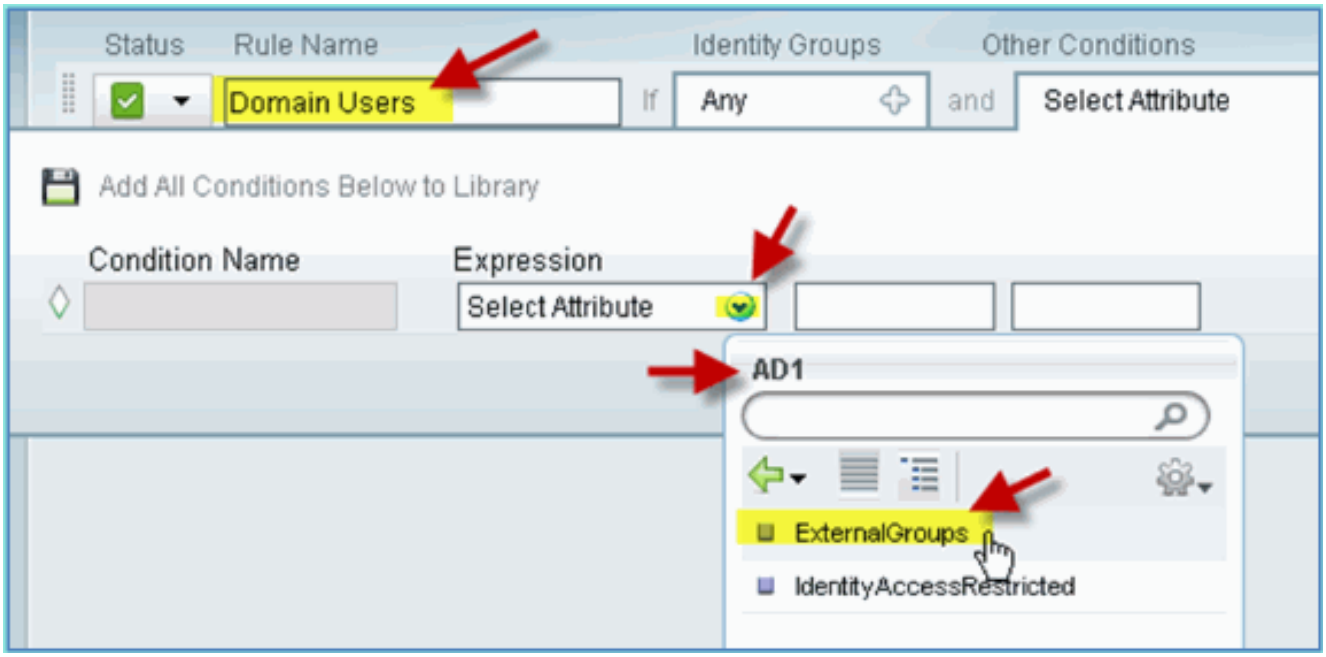
5. 첫 번째 규칙 위에 새 정책을 삽입합니다(오른쪽에서 **작업** 아이콘 클릭
).



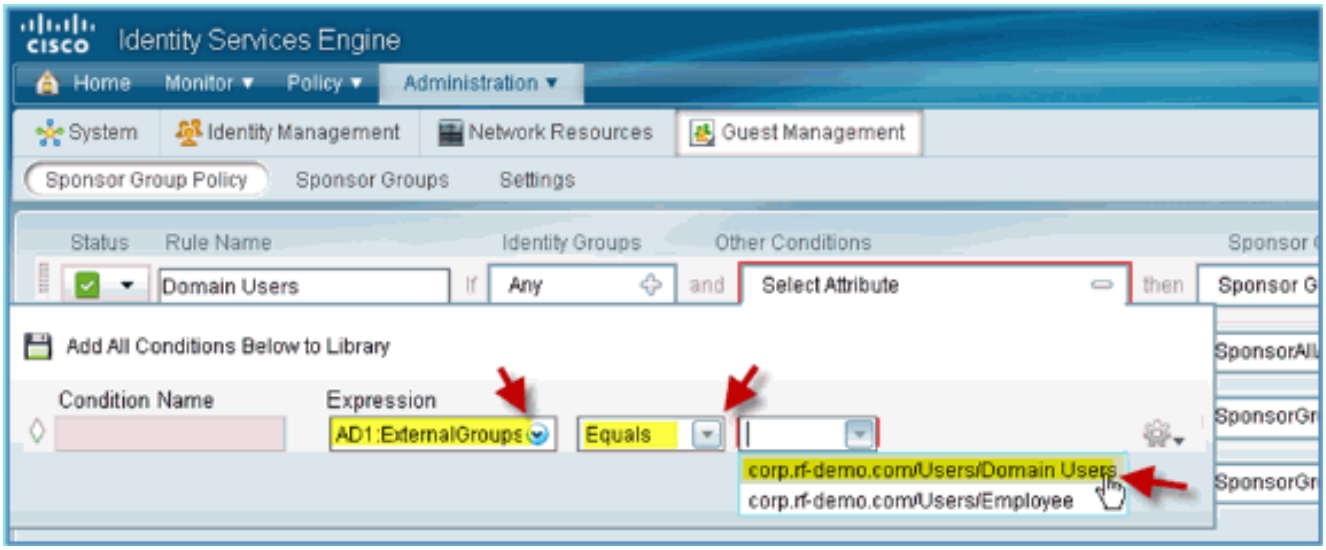
6. 새 스폰서 그룹 정책의 경우 다음을 생성합니다.규칙 이름: 도메인 사용자ID 그룹: 모두기타 조건: (Create New / Advanced) >
AD1



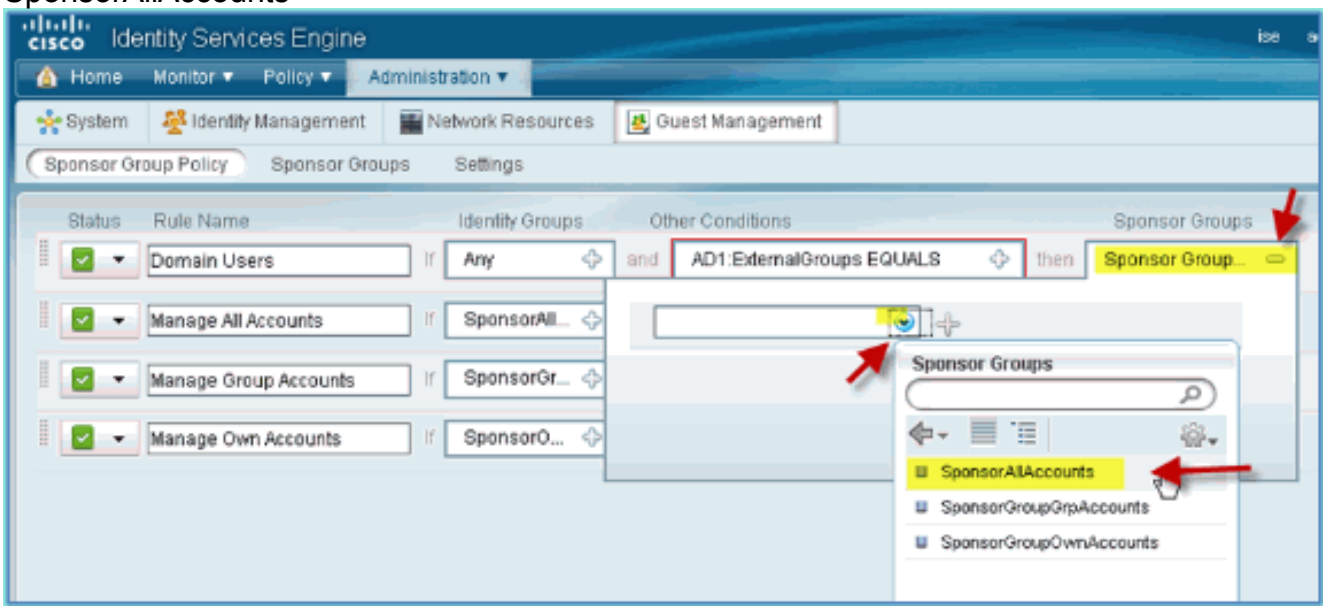
AD1: 외부 그룹



AD1 외부 그룹 > 같음 > corp.rf-demo.com/Users/Domain 사용자

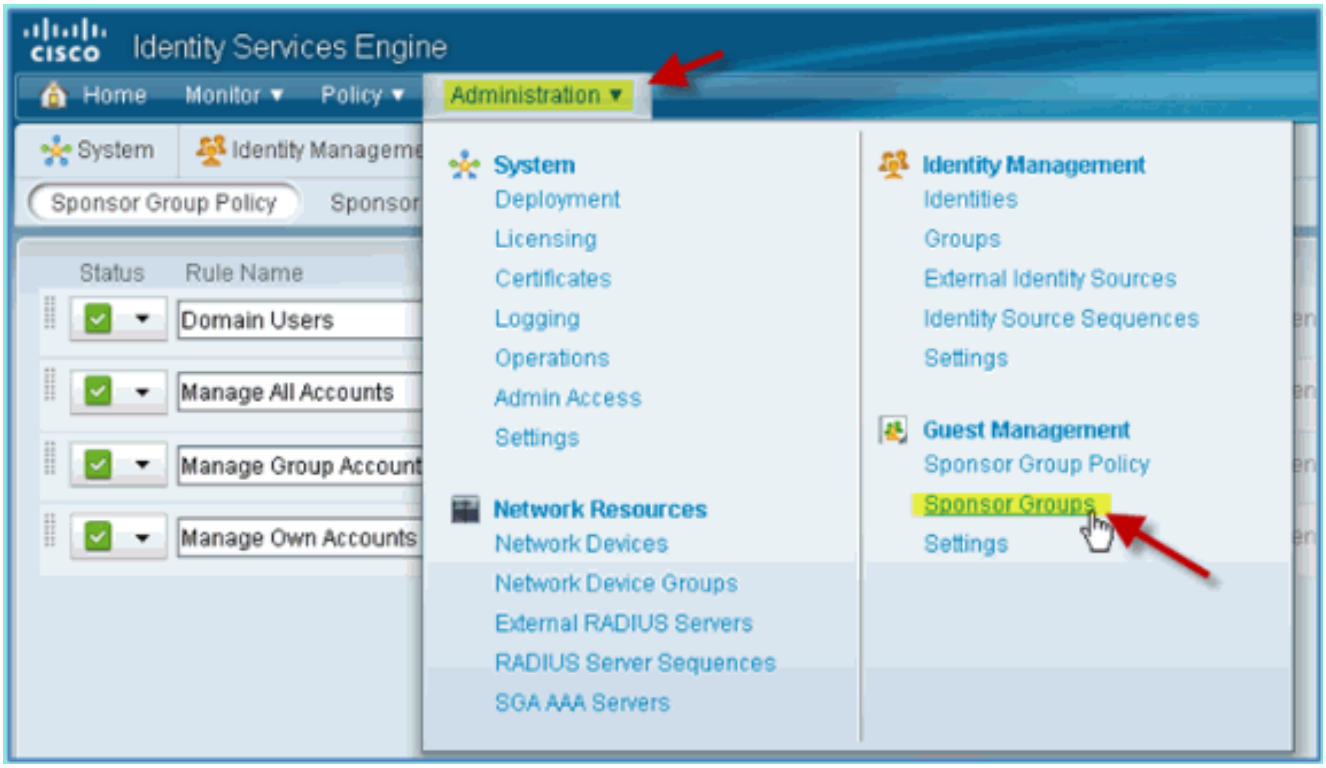


7. 스폰서 그룹에서 다음을 설정합니다.스폰서 그룹: SponsorAllAccounts



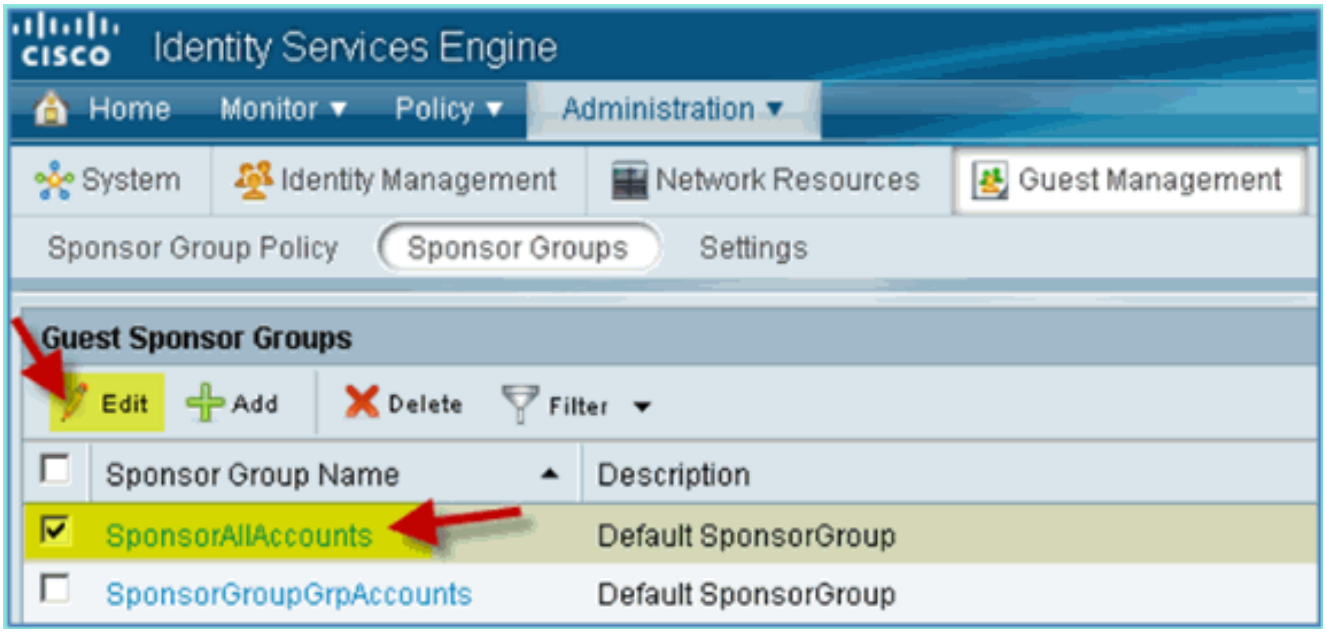
8. Administration(관리) **> Guest Management(게스트 관리) > Sponsor Groups(스폰서 그룹)로 이동합니다**

.

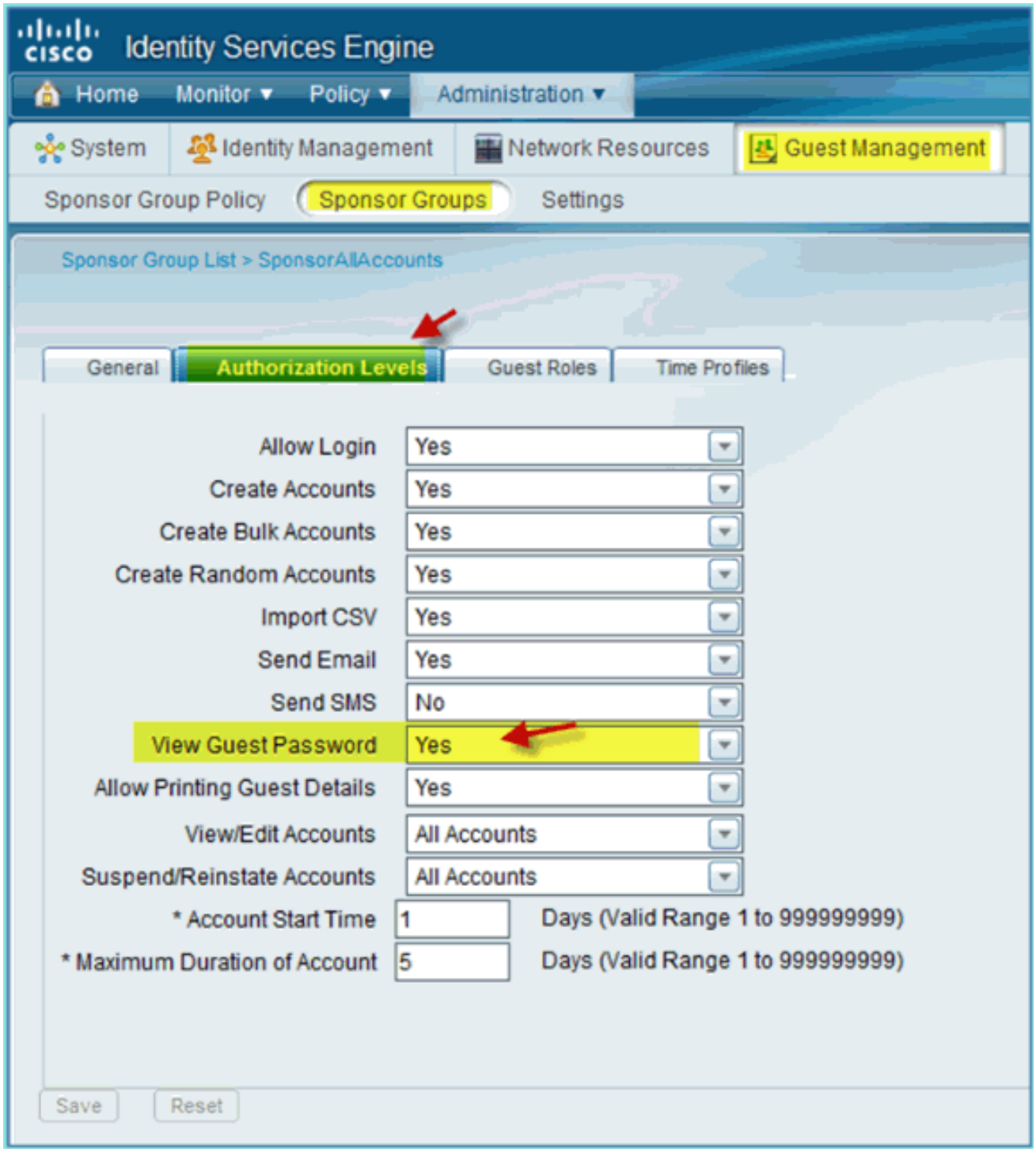


9. Edit(수정) > SponsorAll(스폰서)Accounts(**모든 어카운트)**를 **선택합니다**

.



10. Authorization Levels(권한 부여 레벨)를 선택하고 다음을 설정합니다.게스트 비밀번호 보기: 예



스위치에서 SPAN 구성

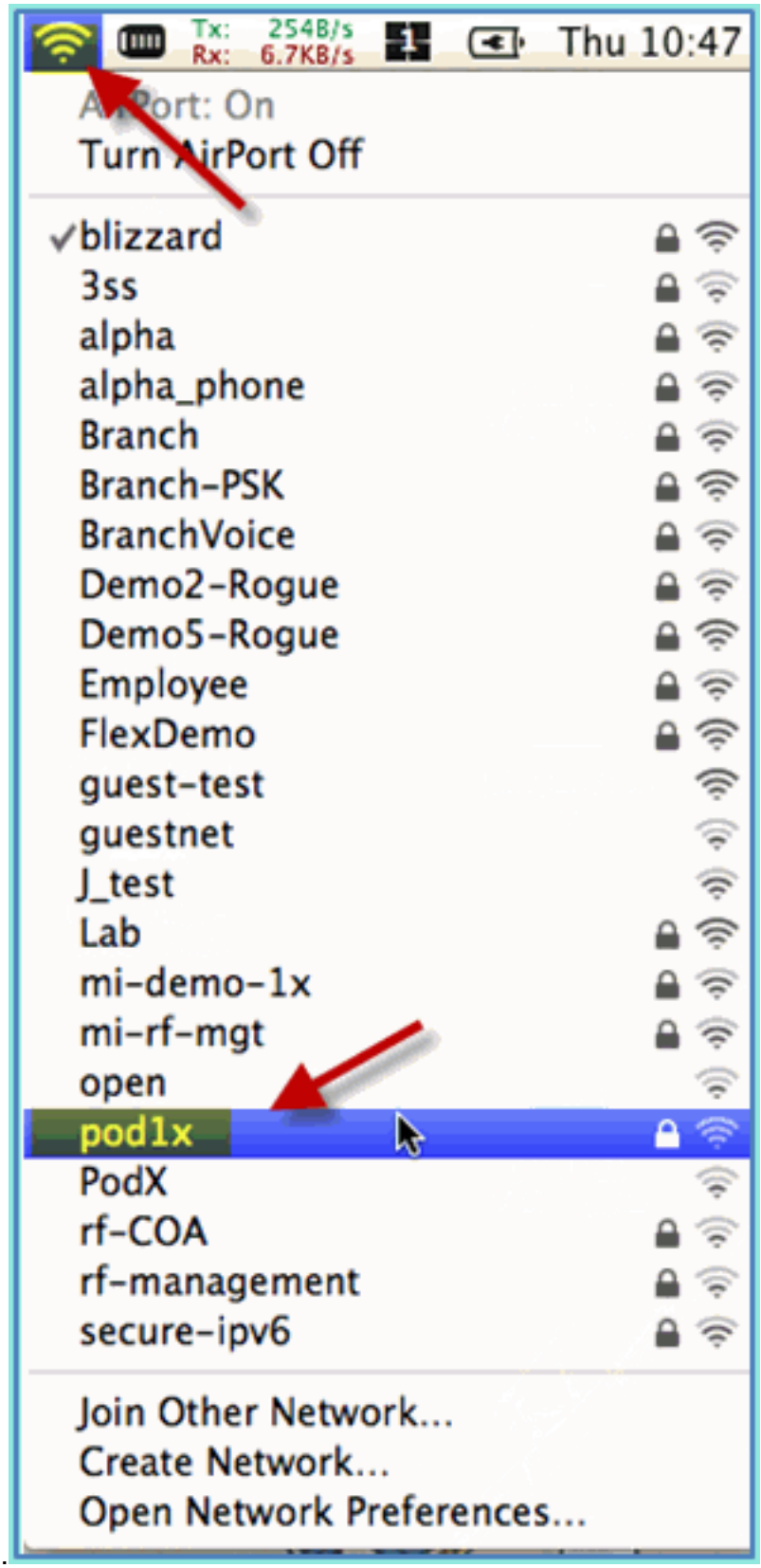
SPAN 구성 - ISE 관리/프로브 인터페이스는 WLC 관리 인터페이스에 인접한 L2입니다. 스위치는 SPAN 및 기타 인터페이스(예: 직원 및 게스트 인터페이스 VLAN)로 구성할 수 있습니다.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

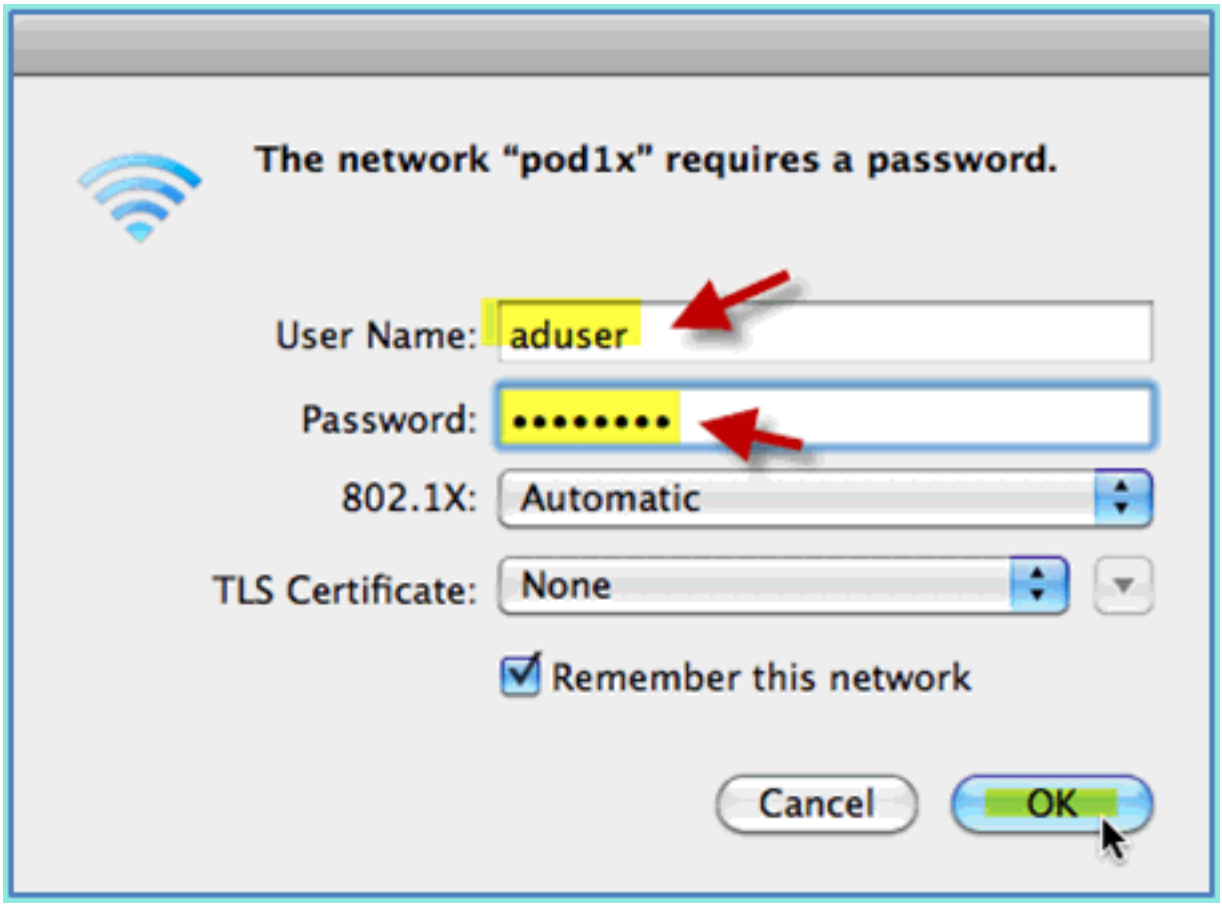
참조: Apple MAC OS X용 무선 인증

Apple Mac OS X 무선 노트북 컴퓨터를 사용하여 내부 사용자(또는 통합 AD 사용자)로 인증된 SSID를 통해 WLC에 연결합니다. 해당되지 않는 경우 건너뜁니다.

1. Mac에서 WLAN 설정으로 이동합니다. WIFI를 활성화한 다음 이전 연습에서 생성한 802.1X 활성 POD SSID를 선택하여 연결합니다



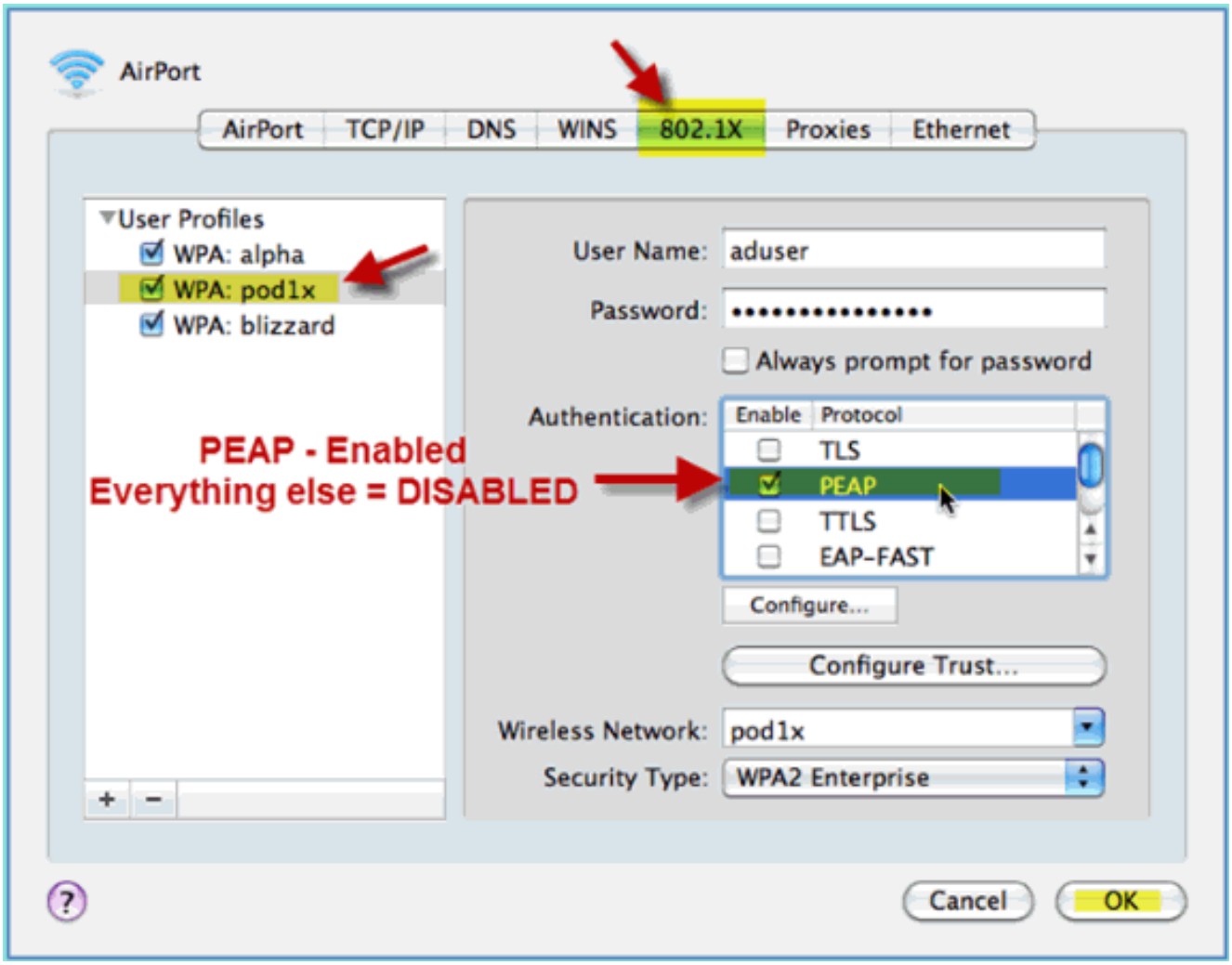
2. 연결하려면 다음 정보를 제공하십시오.사용자 이름: aduser(AD를 사용하는 경우), employee(internal - Employee), contractor(internal - Contractor)비밀번호: XXXX802.1X: 자동 TLS 인증서: 없음



이때 랩톱이 연결되지 않을 수 있습니다. 또한 ISE는 다음과 같이 실패한 이벤트를 발생시킬 수 있습니다.

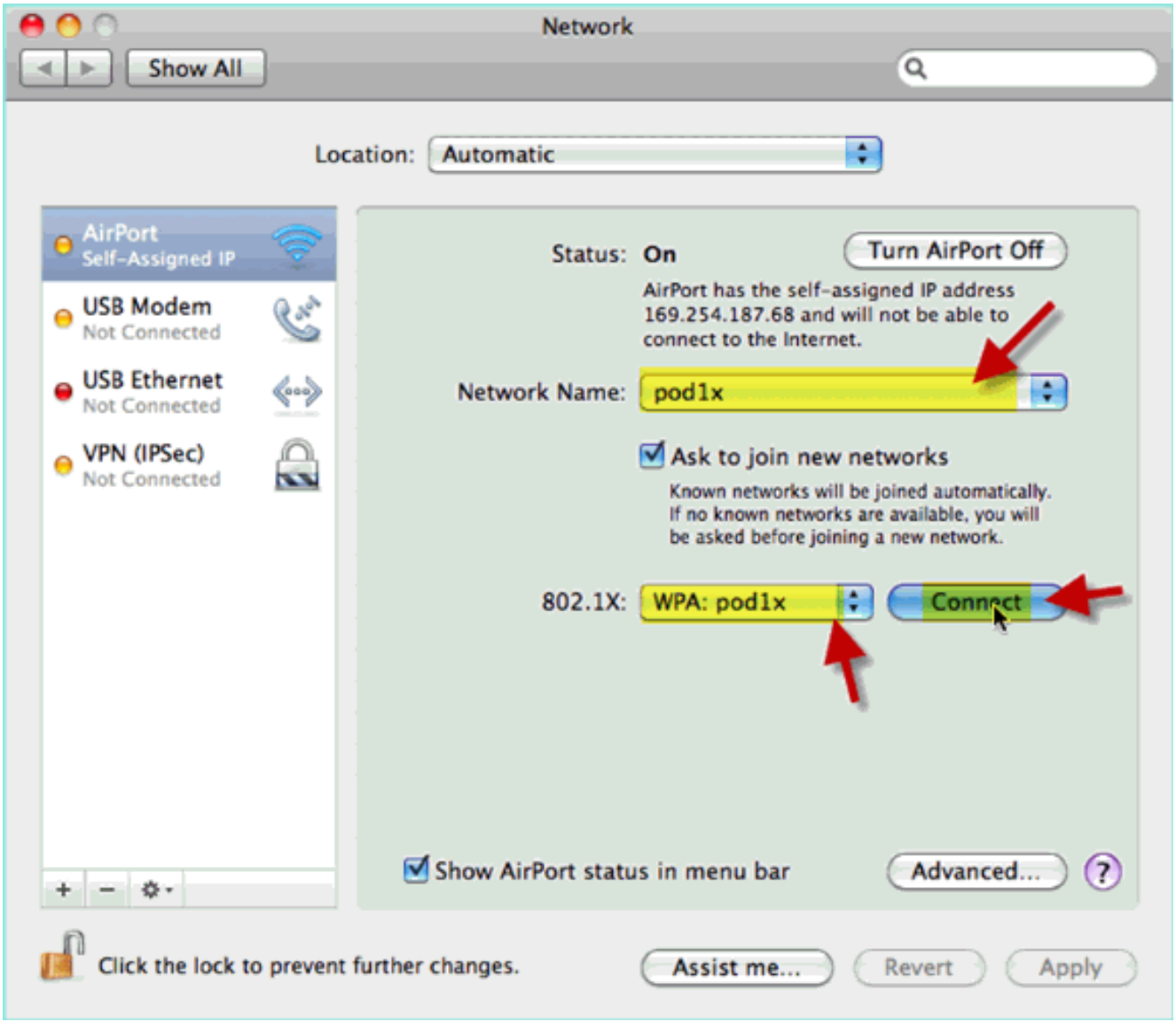
```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of
an unknown CA in the client certificates chain
```

3. **System Preference(시스템 기본 설정) > Network(네트워크) > Airport(공항) > 802.1X** 설정으로 이동하여 새 POD SSID/WPA 프로파일 인증을 다음과 같이 설정합니다.TLS: 사용 안 함PEAP: 사용TTLS: 사용 안 함EAP-FAST: 사용 안 함



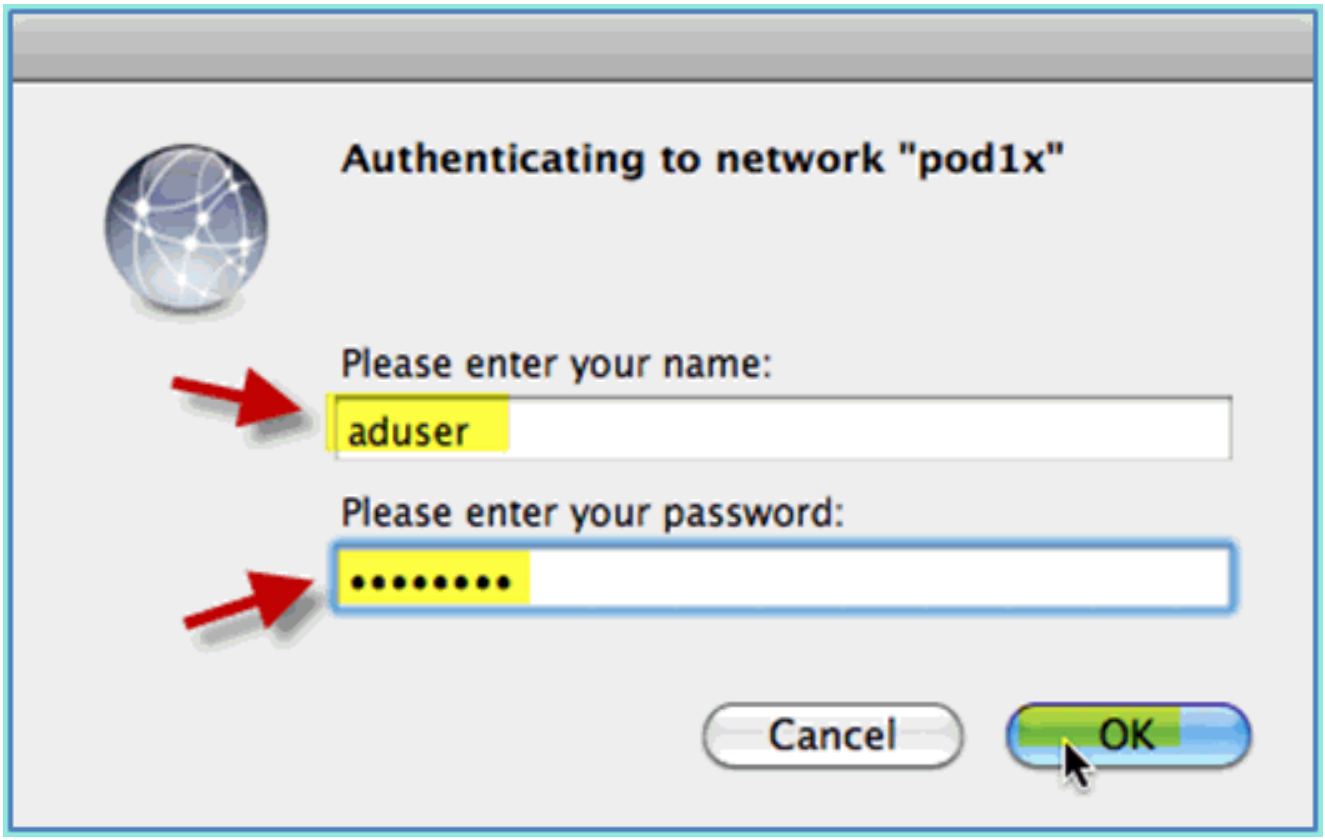
4. OK(**확인**)를 클릭하여 계속하고 설정을 저장합니다.
5. Network(네트워크) 화면에서 적절한 SSID + 802.1X WPA 프로파일을 선택하고 **Connect(연결)**를 클릭합니다

.



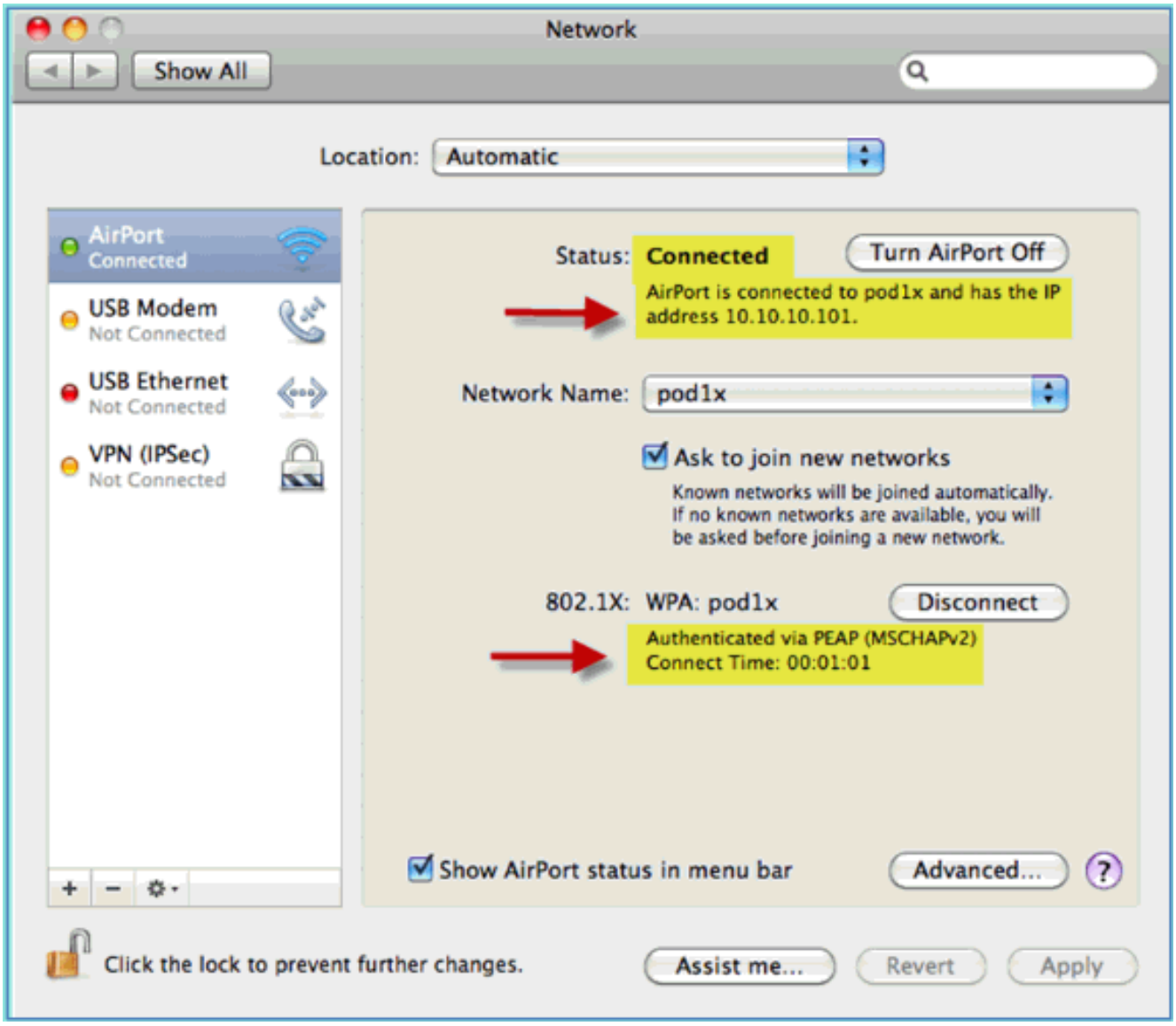
6. 사용자 이름과 비밀번호를 묻는 메시지가 표시될 수 있습니다. AD 사용자 및 암호 (aduser/XXXX)를 입력한 다음 **OK**(확인)를 클릭합니다

.



클라이언트는 유효한 IP **주소**와 함께 PEAP를 통해 연결됨을 표시해야 합니다

.

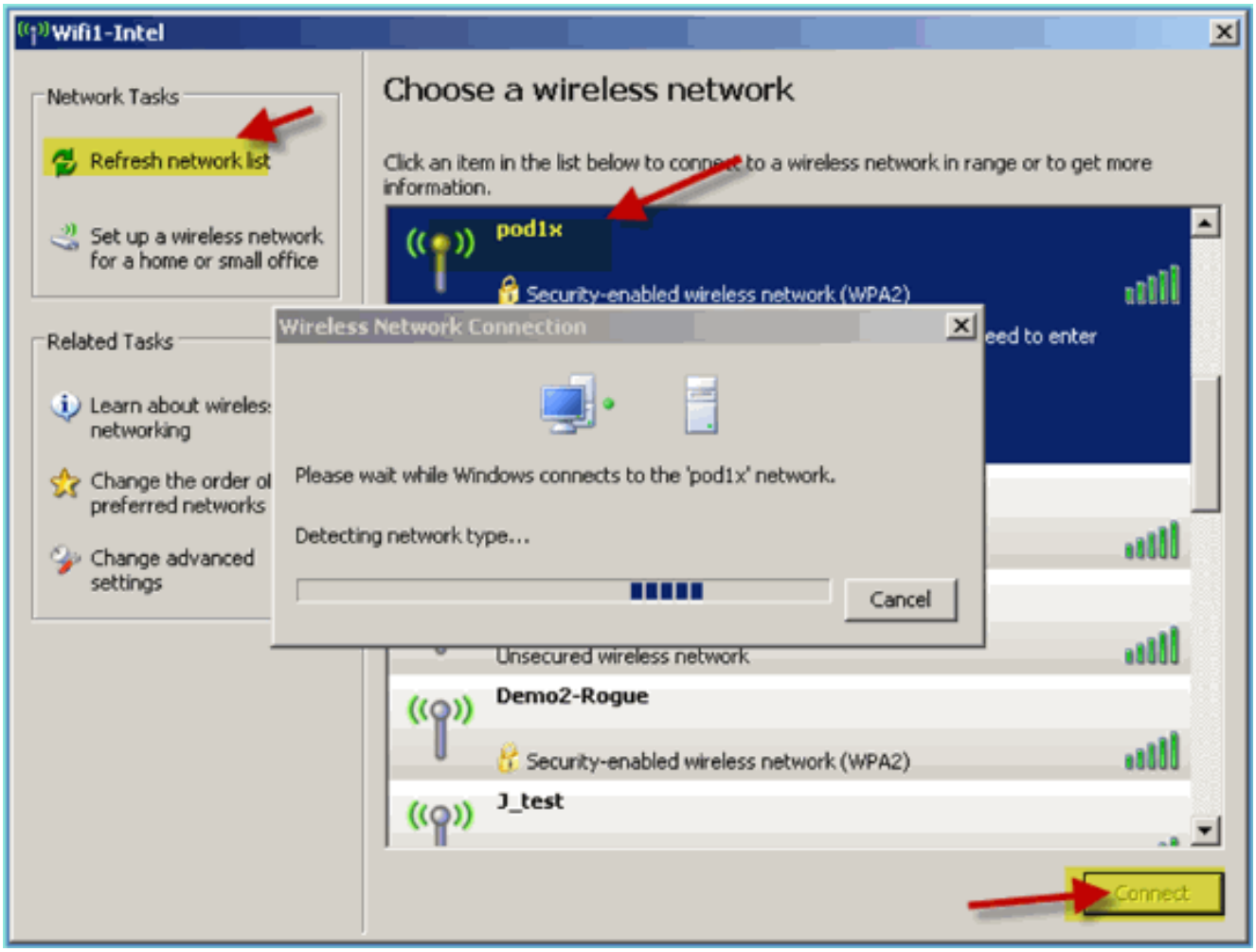


참조: Microsoft Windows XP용 무선 인증

Windows XP 무선 노트북 컴퓨터를 사용하여 내부 사용자(또는 통합 AD 사용자)로서 인증된 SSID를 통해 WLC에 연결합니다. 해당되지 않는 경우 건너뜁니다.

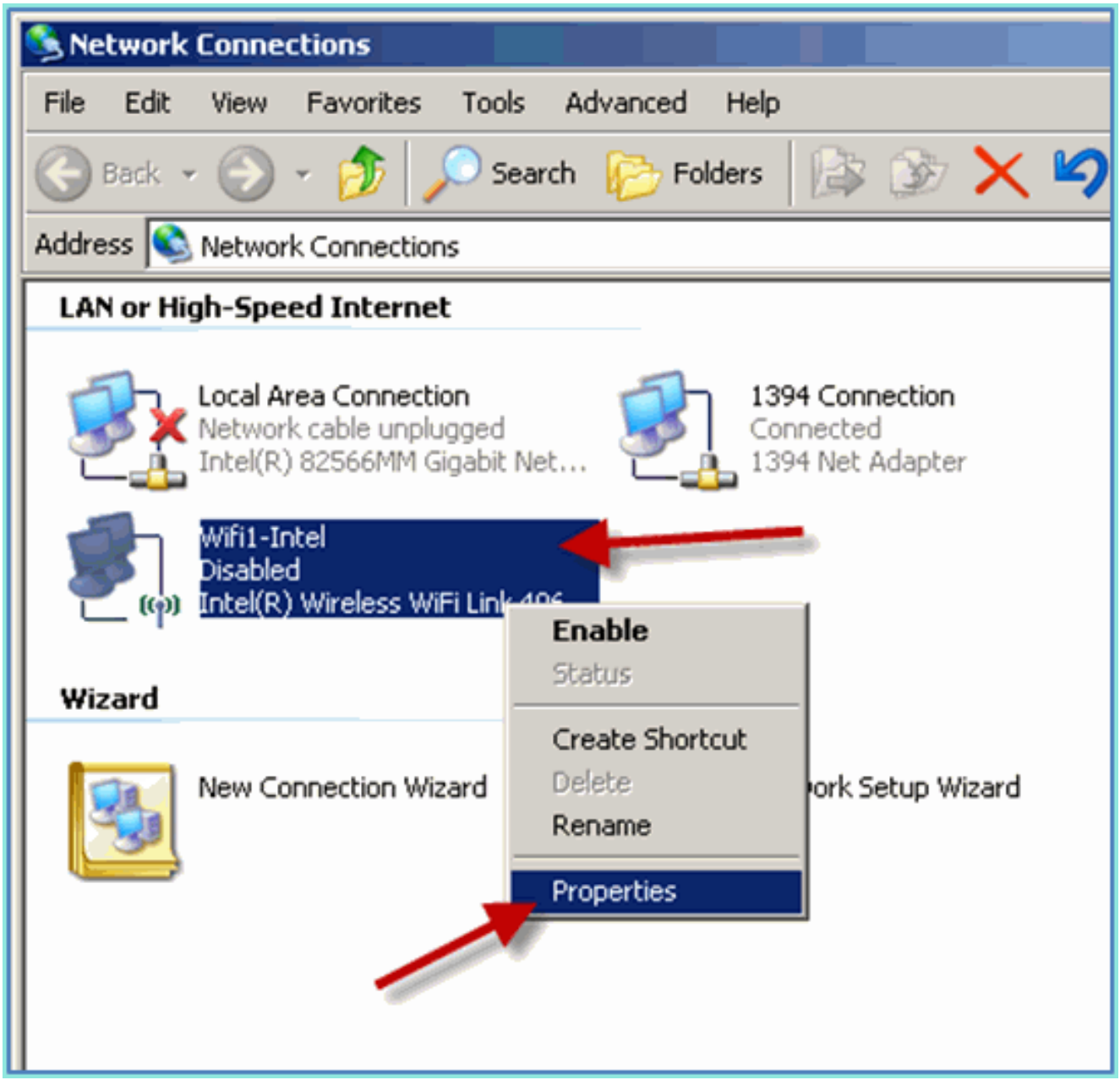
다음 단계를 완료하십시오.

1. 노트북 컴퓨터에서 WLAN 설정으로 이동합니다. WIFI를 활성화하고 이전 연습에서 생성한 802.1X 활성 POD SSID에 연결합니다
.



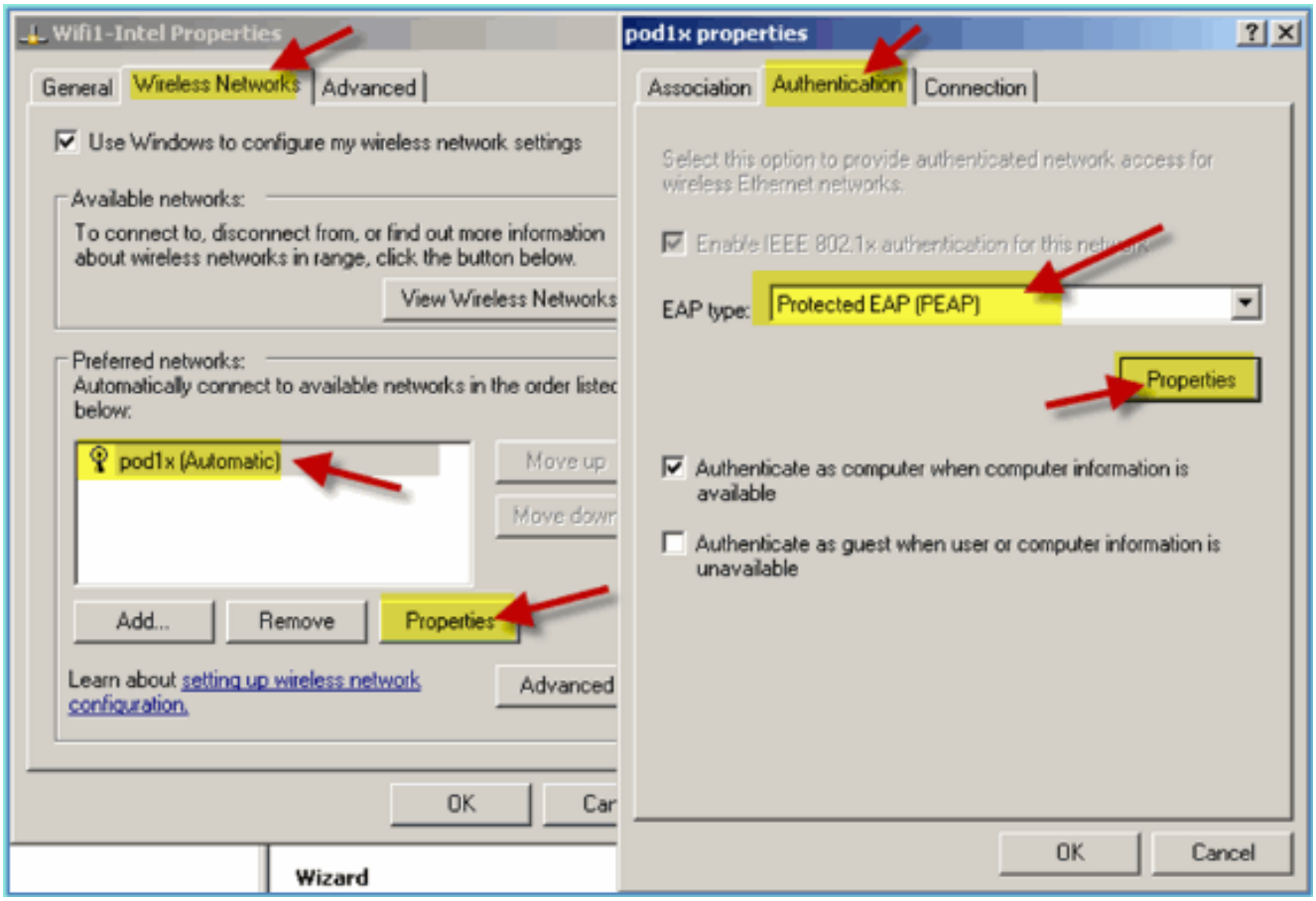
2. WIFI 인터페이스의 네트워크 속성에 액세스합니다

.

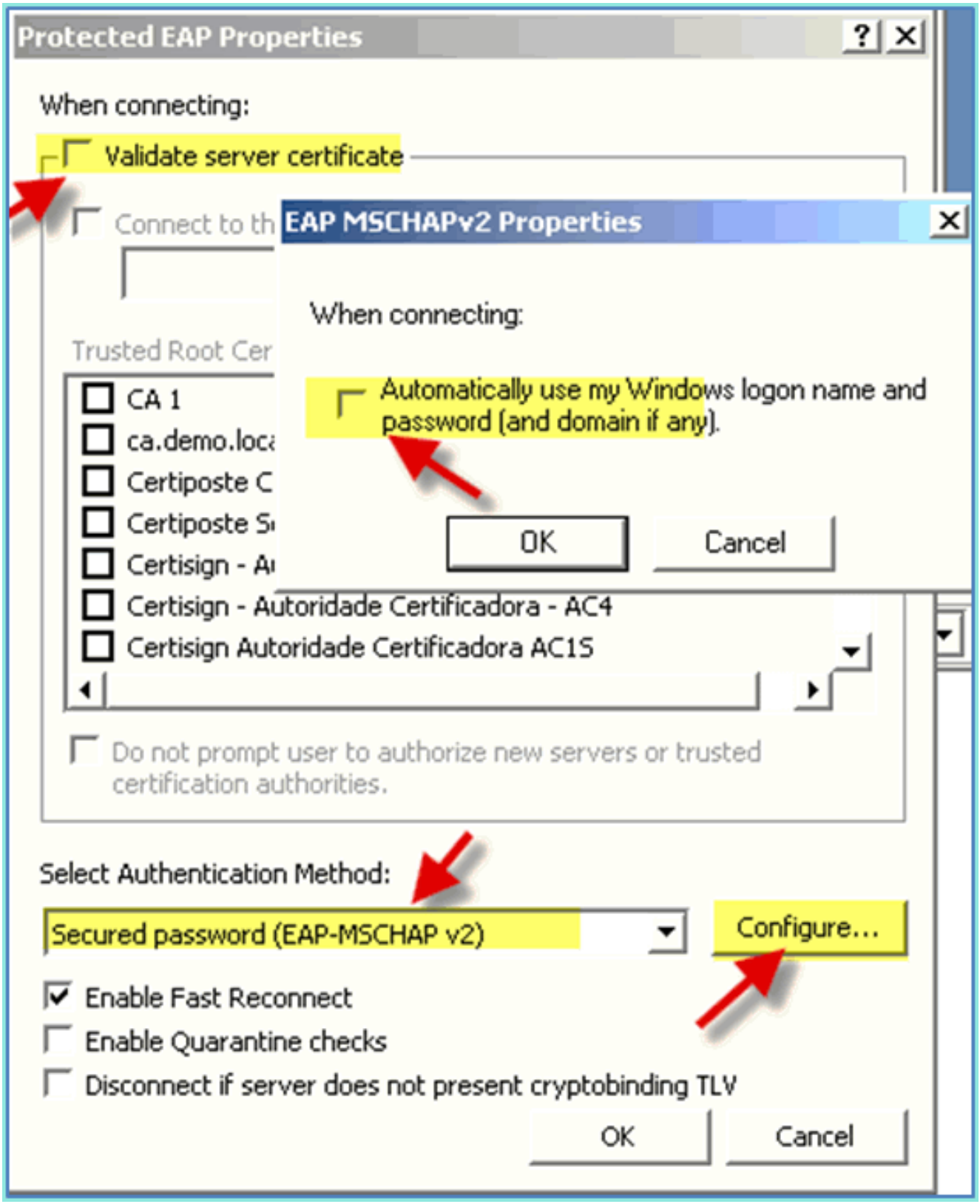


3. **무선 네트워크** 탭으로 이동합니다. Pod SSID Network Properties(포드 SSID 네트워크 속성) > Authentication(인증) 탭 > EAP type(EAP 유형) = Protected EAP (PEAP)(PEAP(보호된 EAP(PEAP))를 선택합니다

.



4. EAP Properties(EAP 속성)를 클릭합니다.
5. 다음을 설정합니다.서버 인증서 유효성 검사: 사용 안 함인증 방법: 보안 암호 (EAP-MSCHAP v2)

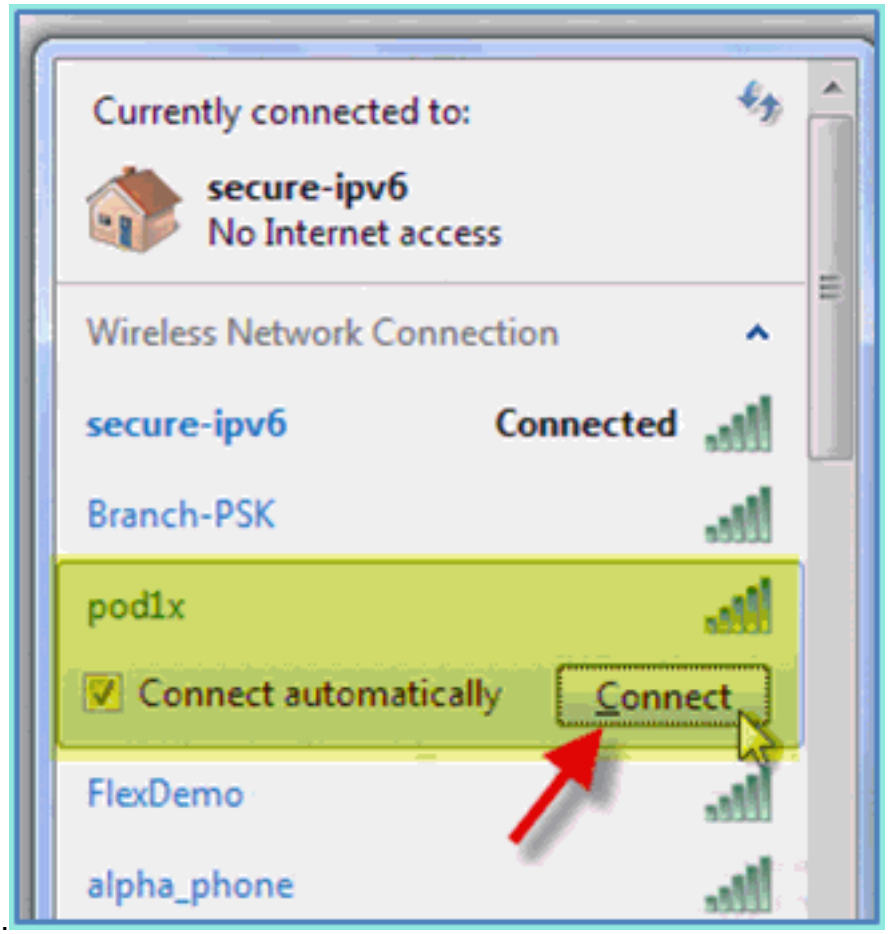


6. 모든 **창**에서 OK를 클릭하여 이 컨피그레이션 작업을 완료합니다.
7. Windows XP 클라이언트는 사용자 이름과 암호를 묻는 메시지를 표시합니다. 이 예에서는 aduser/XXXX입니다.
8. 네트워크 연결, IP 주소 지정(v4)을 확인합니다.

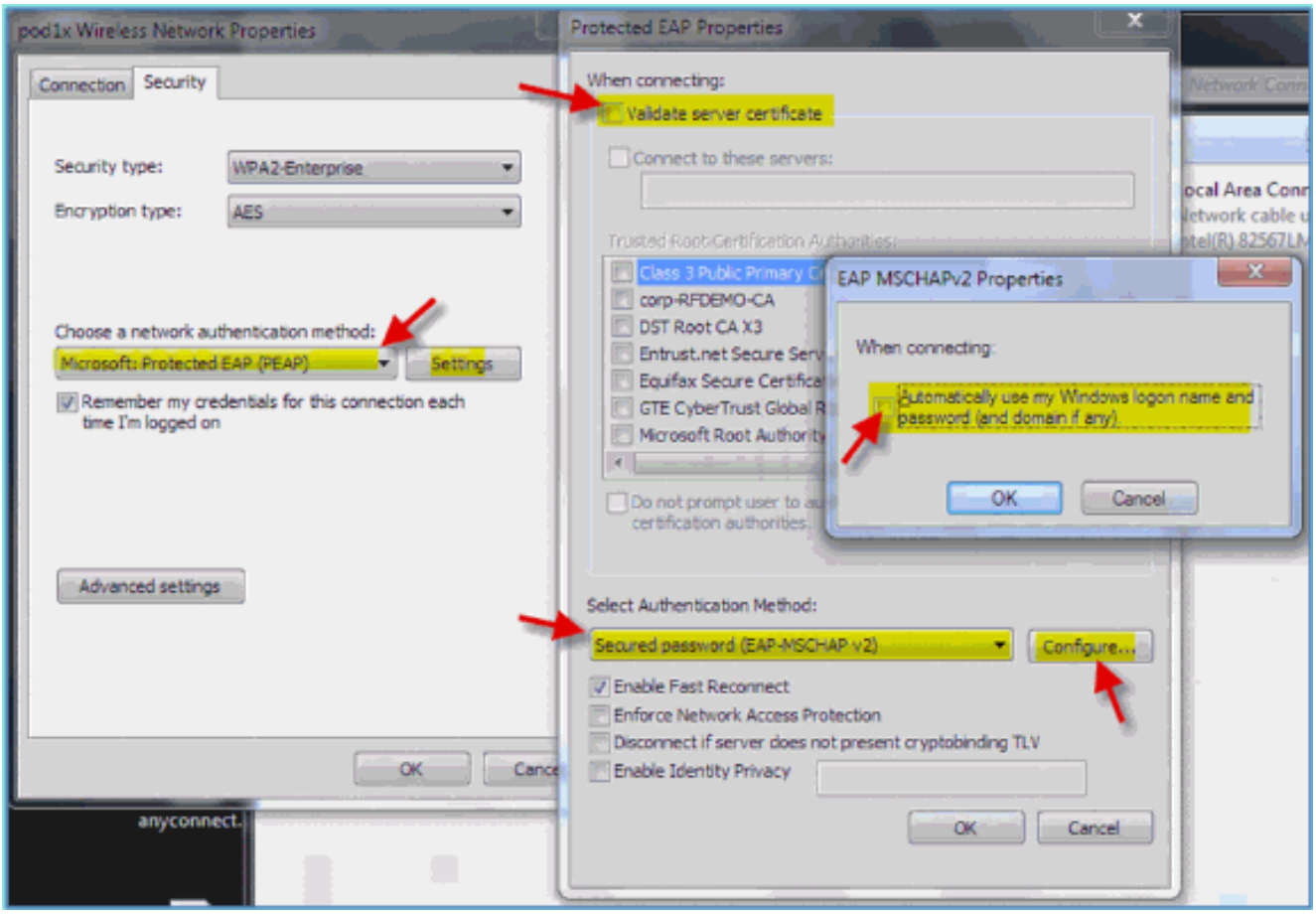
참조: Microsoft Windows 7용 무선 인증

Windows 7 무선 노트북 컴퓨터를 사용하여 내부 사용자(또는 통합 AD 사용자)로 인증된 SSID를 통해 WLC에 연결합니다.

1. 노트북 컴퓨터에서 WLAN 설정으로 이동합니다. WIFI를 활성화하고 이전 연습에서 생성한 802.1X 활성 POD SSID에 연결합니다



2. 무선 관리자에 액세스하여 새 POD 무선 프로파일을 편집합니다.
3. 다음을 설정합니다.인증 방법: PEAP내 자격 증명 기억...: 사용 안 함서버 인증서 유효성 검사(고급 설정): 사용 안 함인증 방법(고급 설정): EAP-MSCHAP v2자동으로 내 Windows 로그온 사용...: 사용 안 함



관련 정보

- 기술 지원 및 문서 – Cisco Systems

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.