Wireless BYOD for FlexConnect 구축 설명서

목차

소개

모바일 장치는 점점 더 컴퓨팅 파워가 높아지고 소비자들 사이에서 인기를 얻고 있다. 수백만 대의 이러한 장치가 고속 Wi-Fi를 통해 소비자에게 판매되어 사용자가 커뮤니케이션하고 협업할 수 있습니다. 소비자들은 이제 이러한 모바일 장치가 생활에 가져다 주는 생산성 향상에 익숙해져 있으며, 개인 경험을 작업 공간에 구현하고자 노력하고 있습니다. 따라서 업무 공간에서 BYOD(Bring Your Own Device) 솔루션의 기능 요구 사항이 생겨납니다.

이 문서에서는 BYOD 솔루션의 브랜치 구축을 제공합니다. 직원이 새 iPad를 사용하여 회사 SSID(Service Set Identifier)에 연결하고 셀프 등록 포털로 리디렉션됩니다. Cisco ISE(Identity Services Engine)는 기업 AD(Active Directory)에 대해 사용자를 인증하고 iPad MAC 주소와 사용자 이름이 포함된 인증서를 dot1x 연결을 위한 방법으로 EAP-TLS(Extensible Authentication Protocol-

Transport Layer Security)를 사용하도록 시행하는 신청자 프로파일과 함께 iPad에 다운로드합니다. ISE의 권한 부여 정책에 따라 사용자는 dot1x를 사용하여 연결하고 적절한 리소스에 액세스할 수 있습니다.

7.2.110.0 이전 버전의 Cisco Wireless LAN Controller 소프트웨어 릴리스의 ISE 기능은 FlexConnect AP(액세스 포인트)를 통해 연결되는 로컬 스위칭 클라이언트를 지원하지 않았습니다. 릴리스 7.2.110.0에서는 로컬 스위칭 및 중앙 인증 클라이언트를 위한 FlexConnect AP에 대해 이러한 ISE 기능을 지원합니다. 또한 ISE 1.1.1과 통합된 릴리스 7.2.110.0에서는 다음과 같은 무선용 BYOD 솔루션 기능을 제공합니다(이에 국한되지 않음).

- 장치 프로파일링 및 상태
- 디바이스 등록 및 신청자 프로비저닝
- 개인 디바이스 온보딩(iOS 또는 Android 디바이스 프로비저닝)

참고: 지원되지만 PC 또는 Mac 무선 노트북 컴퓨터와 워크스테이션 등의 다른 디바이스는 이 설명서에 포함되지 않습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

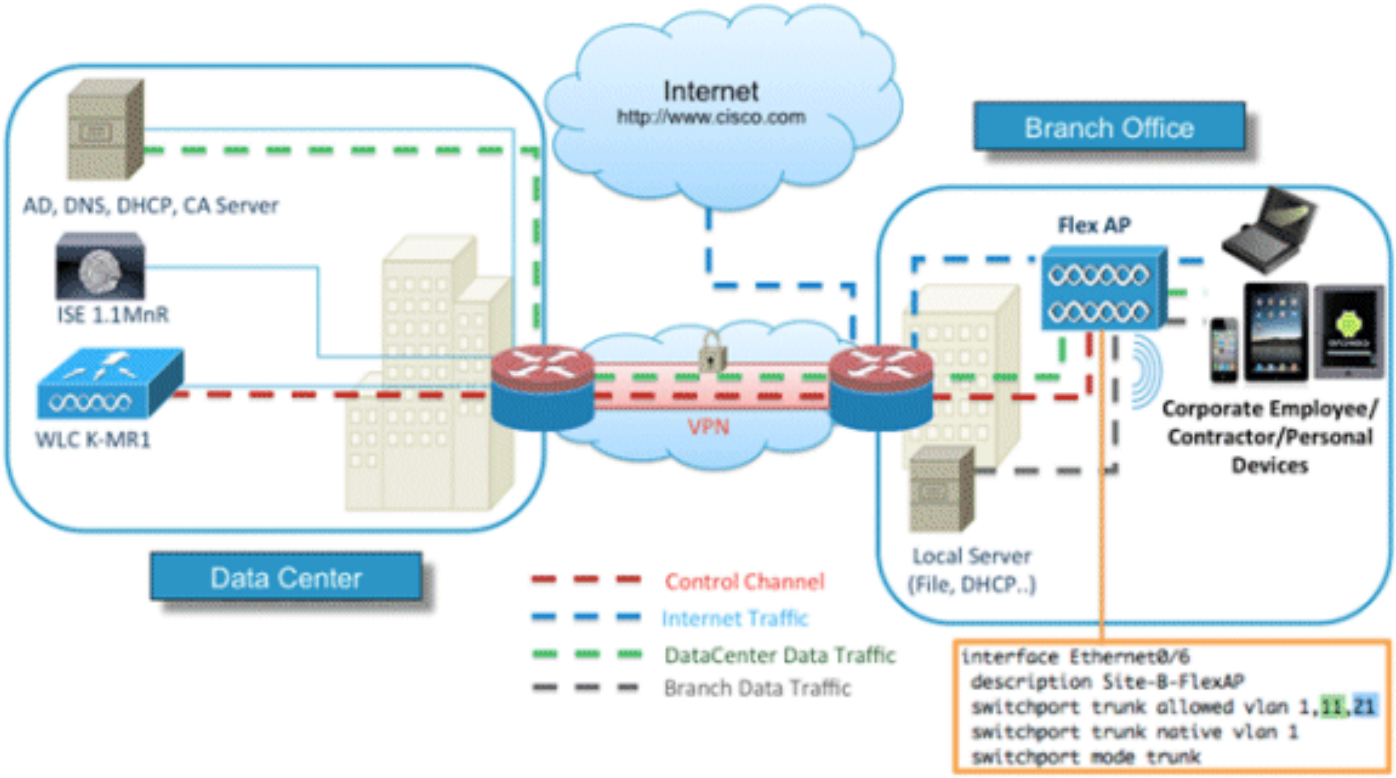
- Cisco Catalyst 스위치
- Cisco WLAN(Wireless LAN) 컨트롤러
- Cisco WLC(WLAN Controller) 소프트웨어 릴리스 7.2.110.0 이상
- FlexConnect 모드의 802.11n AP
- Cisco ISE 소프트웨어 릴리스 1.1.1 이상
- CA(Certificate Authority)가 있는 Windows 2008 AD
- DHCP 서버
- DNS(Domain Name System) 서버
- NTP(Network Time Protocol)
- 무선 클라이언트 노트북 컴퓨터, 스마트폰 및 태블릿(Apple iOS, Android, Windows 및 Mac)

참고: 이 소프트웨어 릴리스에 대한 중요 정보는 Cisco Wireless LAN Controller 릴리스 노트 및 Lightweight Access Points 릴리스 7.2.110.0을 참조하십시오. 소프트웨어를 로드하고 테스트하기 전에 Cisco.com 사이트에 로그인하여 최신 릴리스 정보를 확인하십시오.

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

토폴로지

이러한 기능을 제대로 구현하고 테스트하려면 이 다이어그램에 표시된 것처럼 최소한의 네트워크 설정이 필요합니다.



이 시뮬레이션에는 FlexConnect AP가 있는 네트워크, 로컬 DHCP, DNS, WLC 및 ISE가 있는 로컬/원격 사이트가 필요합니다. FlexConnect AP가 트렁크에 연결되어 여러 VLAN의 로컬 스위칭을 테스트합니다.

디바이스 등록 및 신청자 프로비저닝

기본 신청자가 dot1x 인증을 위해 프로비저닝될 수 있도록 디바이스를 등록해야 합니다. 올바른 인증 정책에 따라 사용자는 게스트 페이지로 리디렉션되고 직원 자격 증명으로 인증됩니다. 사용자는 디바이스 정보를 요청하는 디바이스 등록 페이지를 볼 수 있습니다. 그러면 디바이스 프로비저닝 프로세스가 시작됩니다. OS(운영 체제)가 프로비저닝에 지원되지 않는 경우, MAB(MAC Authentication Bypass) 액세스에 해당 디바이스를 표시하기 위해 사용자가 자산 등록 포털로 리디렉션됩니다. OS가 지원되는 경우 등록 프로세스가 시작되고 dot1x 인증을 위해 디바이스의 기본 신청자를 구성합니다.

자산 등록 포털

Asset Registration Portal은 직원이 인증 및 등록 프로세스를 통해 엔드포인트의 온보딩을 시작할 수 있도록 하는 ISE 플랫폼의 요소입니다.

관리자는 엔드포인트 ID 페이지에서 에셋을 삭제할 수 있습니다. 각 직원은 자신이 등록한 자산을 편집, 삭제 및 블랙리스트에 추가할 수 있습니다. 블랙리스트 엔드포인트는 블랙리스트 ID 그룹에 할당되며, 블랙리스트 엔드포인트에 의한 네트워크 액세스를 방지하기 위해 권한 부여 정책이 생성됩니다.

셀프 등록 포털

CWA(Central Web Authentication) 흐름에서 직원은 자격 증명을 입력하고 인증하며 등록하려는 특정 자산의 세부 사항을 입력할 수 있는 포털로 리디렉션됩니다. 이 포털을 셀프 프로비저닝 포털이라고 하며 디바이스 등록 포털과 유사합니다. 이를 통해 직원은 엔드포인트에 대한 의미 있는 설명뿐만 아니라 MAC 주소를 입력할 수 있습니다.

인증 및 프로비저닝

직원이 셀프 등록 포털을 선택하면 프로비저닝 단계로 진행하기 위해 유효한 직원 자격 증명 집합을 제공해야 합니다. 인증에 성공하면 엔드포인트를 엔드포인트 데이터베이스에 프로비저닝할 수 있으며, 엔드포인트에 대한 인증서가 생성됩니다. 이 페이지의 링크를 통해 직원은 SPW(신청자 파일럿 마법사)를 다운로드할 수 있습니다.

> **참고**: BYOD에 대한 최신 FlexConnect 기능 매트릭스를 보려면 FlexConnect Feature Matrix Cisco 문서를 참조하십시오.

iOS용 프로비저닝(iPhone/iPad/iPod)

EAP-TLS 컨피그레이션의 경우 ISE는 OTA(Apple Over-the-Air) 등록 프로세스를 따릅니다.

- 인증에 성공한 후 평가 엔진은 클라이언트 프로비저닝 정책을 평가하며, 그 결과 신청자 프로필이 생성됩니다.
- 신청자 프로파일이 EAP-TLS 설정용인 경우 OTA 프로세스는 ISE가 자체 서명 또는 알 수 없는 CA에 의해 서명된 것을 사용하는지 여부를 결정합니다. 조건 중 하나가 참인 경우 사용자는 등록 프로세스를 시작하기 전에 ISE 또는 CA의 인증서를 다운로드하라는 요청을 받습니다.
- 다른 EAP 방법의 경우 ISE는 인증에 성공하면 최종 프로파일을 푸시합니다.

Android용 프로비저닝

보안 고려 사항으로 인해 Android 에이전트는 Android 마켓플레이스 사이트에서 다운로드해야 하며 ISE에서 프로비저닝할 수 없습니다. Cisco는 Cisco Android 마켓플레이스 게시자 계정을 통해 Android 마켓플레이스에 마법사의 릴리스 후보 버전을 업로드합니다.

다음은 Android 프로비저닝 프로세스입니다.

1. Cisco는 확장자가 .apk인 Android 패키지를 만들기 위해 SDK(Software Development Kit)를 사용합니다.
2. Cisco는 Android 마켓플레이스에 패키지를 업로드합니다.
3. 사용자는 적절한 매개변수를 사용하여 클라이언트 프로비저닝에서 정책을 구성합니다.
4. 장치를 등록한 후 dot1x 인증에 실패하면 최종 사용자가 클라이언트 프로비저닝 서비스로 리디렉션됩니다.
5. 프로비저닝 포털 페이지는 SPW를 다운로드할 수 있는 Android Marketplace 포털로 사용자를 리디렉션하는 버튼을 제공합니다.

6. Cisco SPW가 시작되고 신청자의 프로비저닝을 수행합니다. SPW는 ISE를 검색하고 ISE에서 프로필을 다운로드합니다.SPW는 EAP-TLS에 대한 인증서/키 쌍을 생성합니다.SPW는 SCEP(Simple Certificate Enrollment Protocol) 프록시 요청 호출을 ISE에 수행하고 인증서를 가져옵니다.SPW는 무선 프로파일을 적용합니다.프로필이 성공적으로 적용되면 SPW에서 재인증을 트리거합니다.SPW가 종료됩니다.

이중 SSID 무선 BYOD 셀프 등록

이중 SSID 무선 BYOD 셀프 등록 프로세스입니다.

1. 사용자가 게스트 SSID에 연결합니다.
2. 사용자가 브라우저를 열고 ISE CWA 게스트 포털로 리디렉션됩니다.
3. 사용자는 게스트 포털에 직원 사용자 이름 및 암호를 입력 합니다.
4. ISE는 사용자를 인증하며, 사용자가 게스트가 아닌 직원이라는 사실을 기반으로 사용자를 Employee Device Registration 게스트 페이지로 리디렉션합니다.
5. MAC 주소는 DeviceID의 Device Registration guest 페이지에 미리 입력되어 있습니다. 사용자가 설명을 입력하고 필요한 경우 AUP(Acceptable Use Policy)에 동의합니다.
6. 사용자가 Accept(**수락**)를 선택하고 SPW 다운로드 및 설치를 시작합니다.
7. 해당 사용자 디바이스의 신청자는 인증서와 함께 프로비저닝됩니다.
8. CoA가 발생하면 디바이스가 기업 SSID(CORP)에 다시 연결되고 EAP-TLS(또는 해당 신청자에 대해 사용 중인 다른 인증 방법)로 인증됩니다.

단일 SSID 무선 BYOD 셀프 등록

이 시나리오에서는 PEAP(Protected Extensible Authentication Protocol) 및 EAP-TLS를 모두 지원하는 CORP(Corporate Access)용 단일 SSID가 있습니다. 게스트 SSID가 없습니다.

단일 SSID 무선 BYOD 셀프 등록 프로세스입니다.

1. 사용자가 CORP에 연결합니다.
2. 사용자는 PEAP 인증을 위한 신청자에 직원 사용자 이름 및 비밀번호를 입력합니다.
3. ISE는 사용자를 인증하며, PEAP 방법에 따라 Employee Device Registration 게스트 페이지로 리디렉션할 때 수락하는 권한 부여 정책을 제공합니다.
4. 사용자가 브라우저를 열고 Employee Device Registration 게스트 페이지로 리디렉션됩니다.
5. MAC 주소는 DeviceID의 Device Registration guest 페이지에 미리 입력되어 있습니다. 사용자가 설명을 입력하고 AUP를 수락합니다.
6. 사용자가 Accept(**수락**)를 선택하고 SPW 다운로드 및 설치를 시작합니다.
7. 해당 사용자 디바이스의 신청자는 인증서와 함께 프로비저닝됩니다.
8. CoA가 발생하고 디바이스가 CORP SSID에 다시 연결되고 EAP-TLS로 인증됩니다.

기능 컨피그레이션

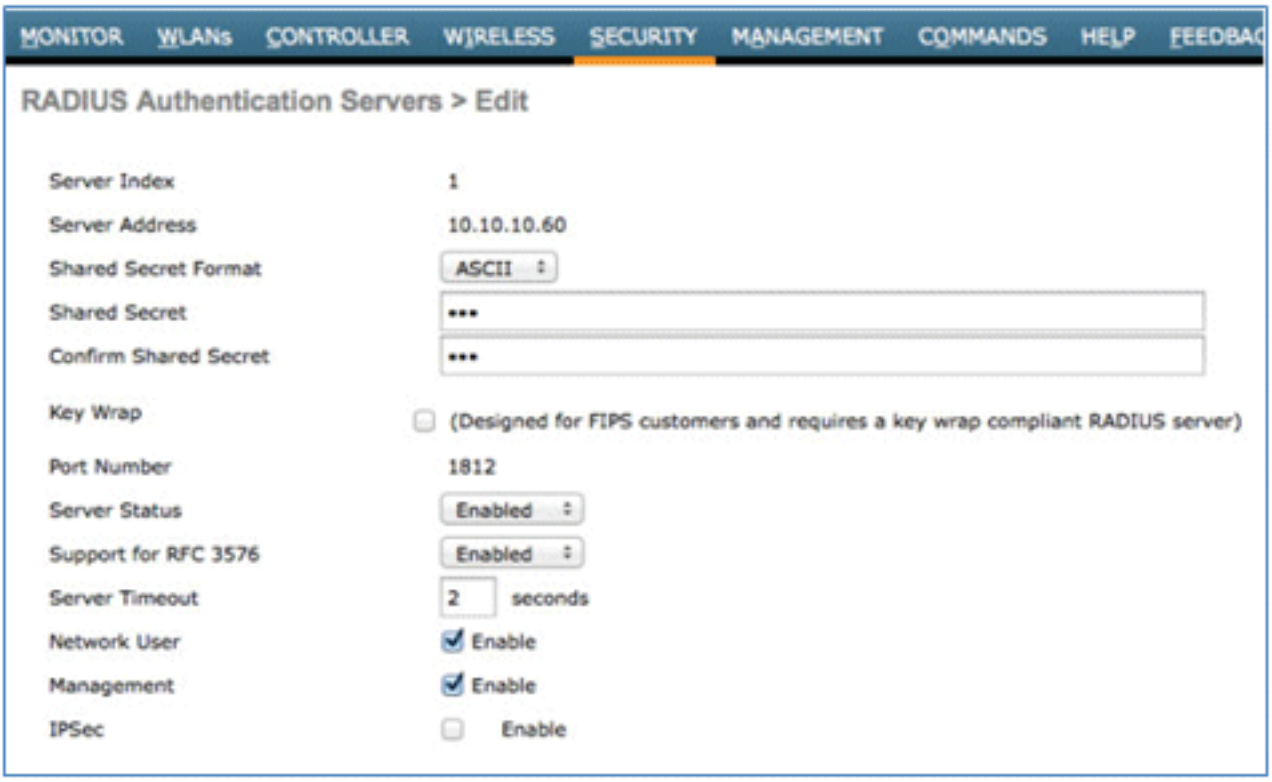
구성을 시작하려면 다음 단계를 완료하십시오.

1. 이 가이드에서는 WLC 버전이 7.2.110.0 이상인지 확인합니다.

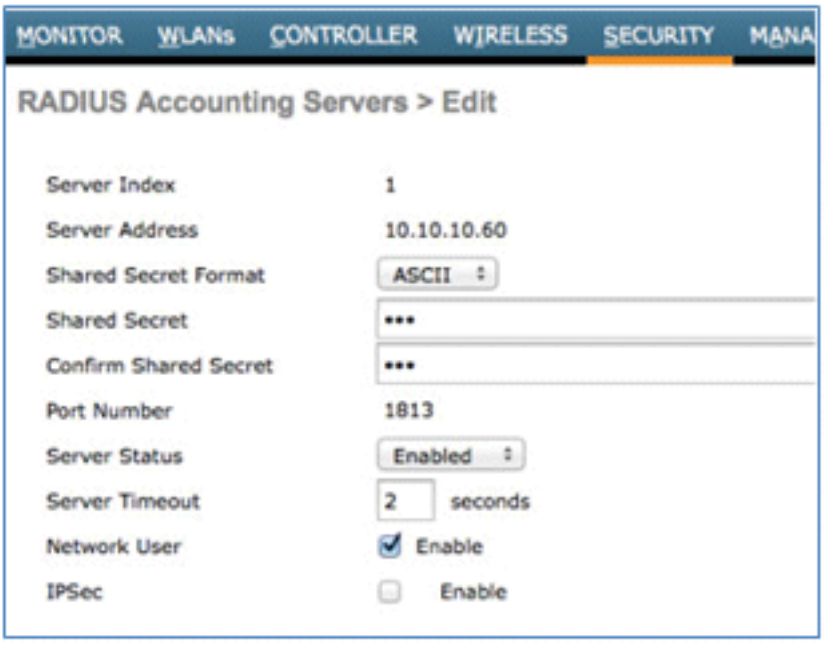
2. **Security(보안) > RADIUS > Authentication(인증)**으로 이동하여 RADIUS 서버를 WLC에 추가합니다.

3. WLC에 ISE 1.1.1을 추가합니다.

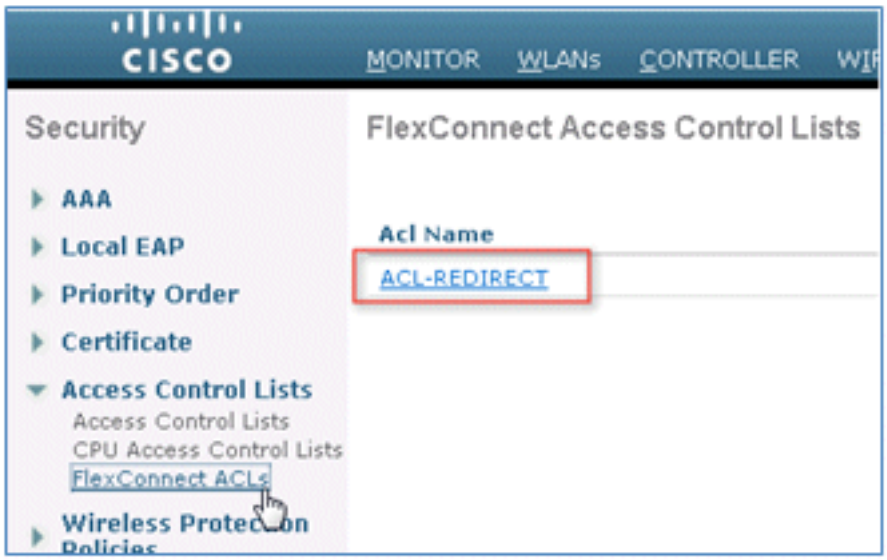
   공유 암호를 입력합니다.RFC 3576에 대한 지원을 Enabled(활성화됨)로 **설정합니다**.



4. 동일한 ISE 서버를 RADIUS 어카운팅 서버로 추가합니다.



5. 나중에 ISE 정책에서 사용할 WLC 사전 인증 ACL을 생성합니다. WLC > **Security > Access Control Lists > FlexConnect ACLs로 이동하여 ACL**-REDIRECT**라는** 새 FlexConnect ACL을 **생성합니다(이 예에서는).**

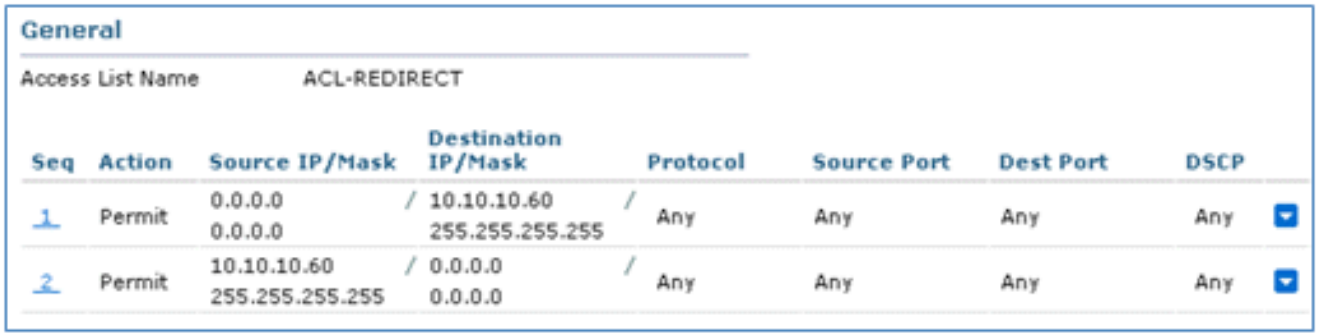


6. ACL 규칙에서 ISE를 오가는 모든 트래픽을 허용하고 신청자 프로비저닝 중에 클라이언트 트래픽을 허용합니다.

   첫 번째 규칙(시퀀스 1)의 경우:

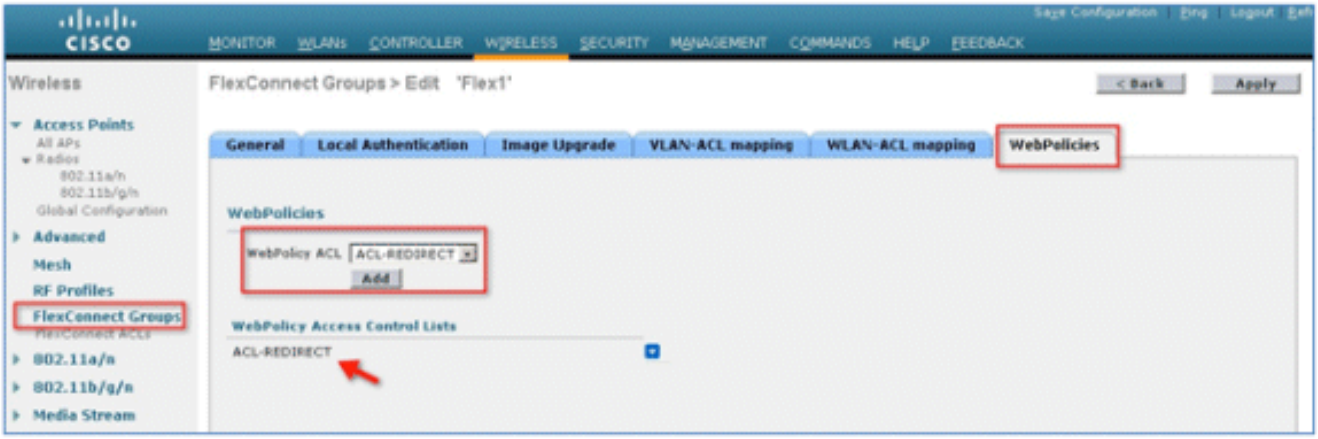
   Source를 Any로 **설정합니다**.IP(ISE 주소)/넷마스크 **255.255.255.255를 설정합니다**.Action을 Permit로 **설정합니다**.

   두 번째 규칙(시퀀스 2)의 경우 소스 IP(ISE 주소)/마스크 255.255.255.255.255를 Any로 설정하고 **Action** to Permit을 **지정합니다**.



7. Flex1이라는 새 FlexConnect 그룹을 생성합니다(이 예에서는).

   FlexConnect **그룹 > WebPolicies 탭**으로 이동합니다.WebPolicy ACL(웹 정책 ACL) 필드에서 Add(추가)를 클릭하고 **ACL-REDIRECT(ACL-REDIRECT)**를 선택하거나 이전에 생성한 FlexConnect ACL을 선택합니다.WebPolicy **Access Control Lists(웹 정책 액세스 제어 목록) 필드가 채워졌는지** 확인합니다.



8. Apply(**적용**) 및 Save Configuration(**컨피그레이션 저장**)**을 클릭합니다**.

WLAN 구성

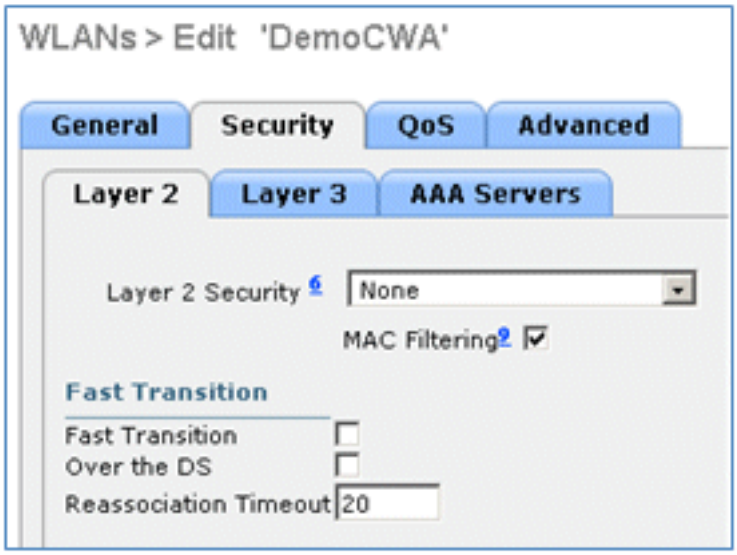
WLAN을 구성하려면 다음 단계를 완료합니다.

1. 이중 SSID에 대해 Open WLAN SSID를 생성합니다. 예:

   WLAN 이름 DemoCWA**를 입력합니다**(이 예에서는).Status(상태)에 대해 Enabled(활성화됨) 옵션을 선택합니다.

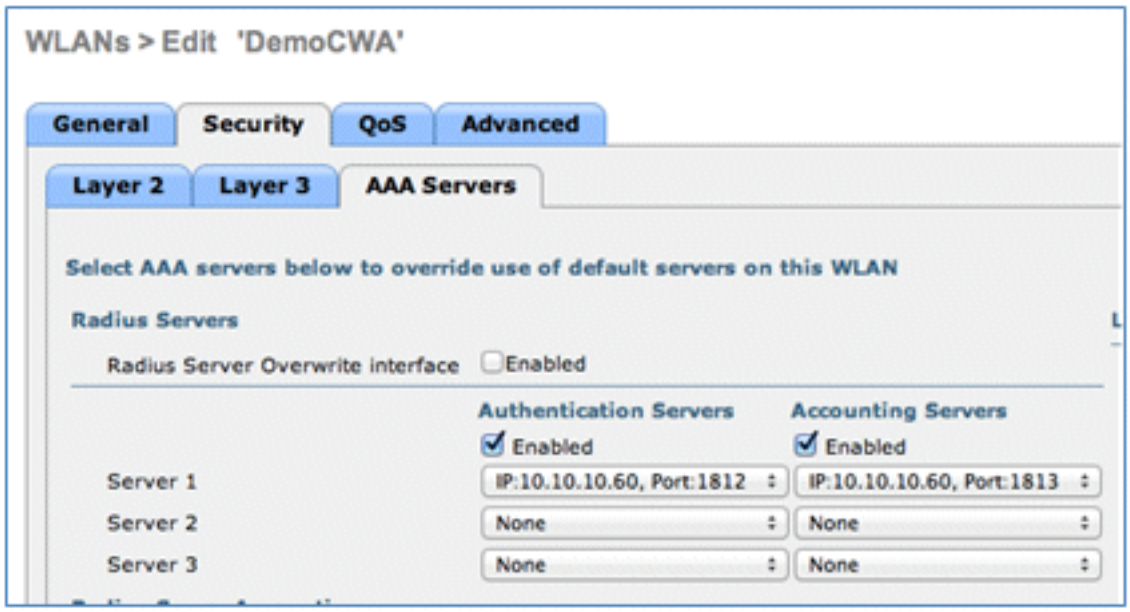
2. **Security** 탭 > **Layer 2** 탭으로 이동하여 다음 특성을 설정합니다.

레이어 2 보안: **없음**MAC Filtering(MAC 필터링): **Enabled**(활성화됨)(상자가 선택됨)빠른 전환 : **사용 안** 함(상자는 선택되지 않음)



3. **AAA Servers(AAA 서버)** 탭으로 이동하여 다음 특성을 설정합니다.

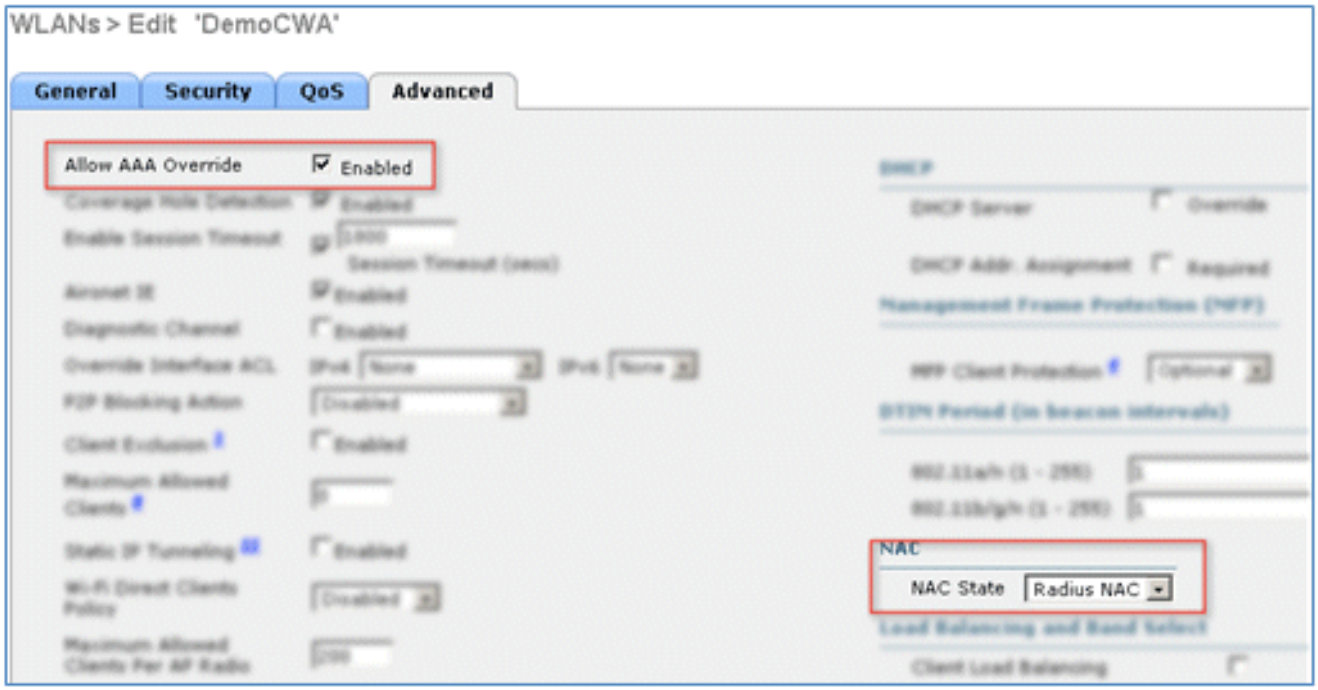
   인증 및 계정 서버: **사용**서버 1: *<ISE IP 주소>*



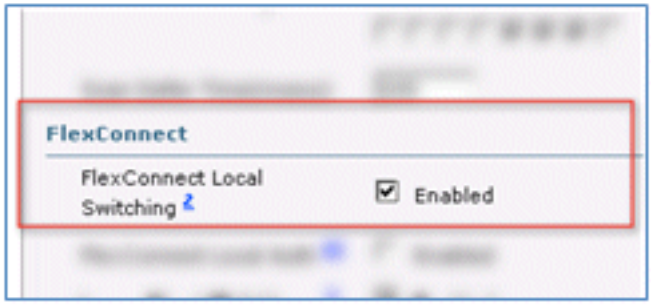
4. **AAA Servers(AAA 서버) 탭**에서 아래로 스크롤합니다. Authentication priority order for web-auth user(웹 인증 사용자의 인증 우선순위 순서)에서 **RADIUS**가 인증에 사용되고 나머지는 사용되지 않는지 확인합니다.

5. **고급** 탭으로 **이동하여** 다음 특성을 설정합니다.

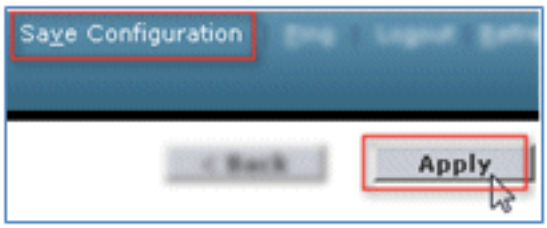
   Allow AAA Override(AAA 재정의 허용): **Enabled(활성화됨)**NAC State(NAC 상태): **Radius NAC**



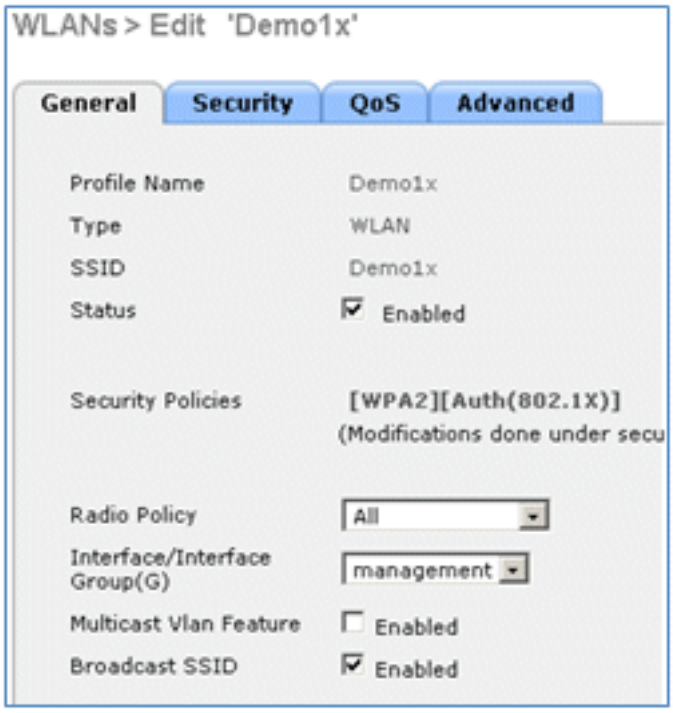
   참고: RADIUS NAC(Network Admission Control)는 FlexConnect AP가 연결 해제 모드에 있을 때 지원되지 않습니다. 따라서 FlexConnect AP가 독립형 모드에 있으며 WLC에 대한 연결이 끊어질 경우 모든 클라이언트가 연결이 끊어지고 SSID가 더 이상 알려지지 않습니다.
6. Advanced(고급) 탭에서 아래로 스크롤하여 FlexConnect Local Switching(FlexConnect 로컬 스위칭)을 Enabled(활성화됨)로 **설정합니다**.



7. Apply(**적용**) 및 Save Configuration(**컨피그레이션 저장**)**을 클릭합니다**.

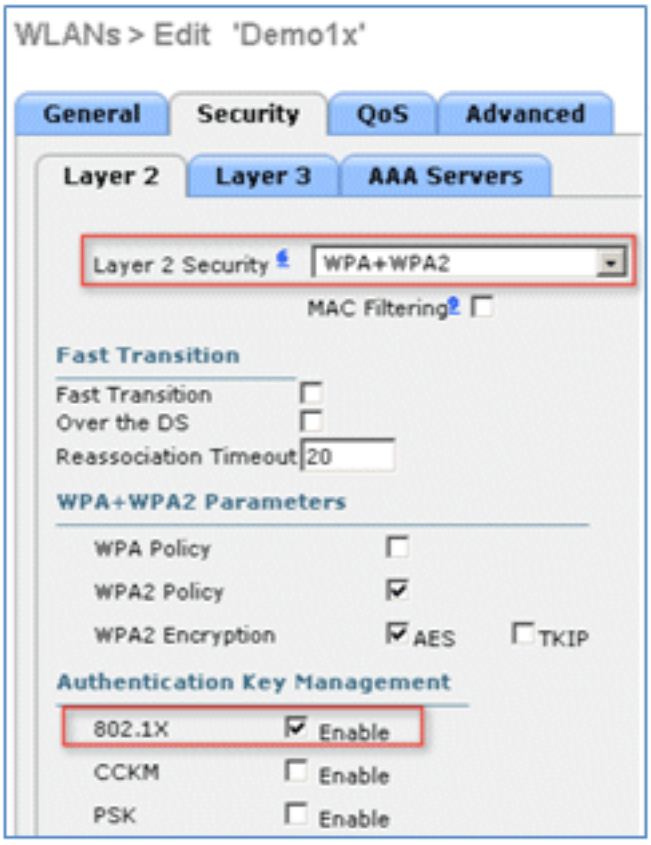


8. 단일 및 이중 SSID 시나리오에 대해 Demo**1x**(이 예에서는)라는 802.1X WLAN SSID를 생성합니다.



9. **Security** 탭 > **Layer 2** 탭으로 이동하여 다음 특성을 설정합니다.

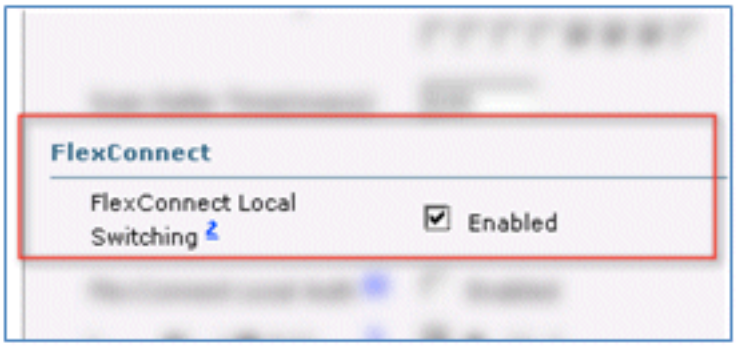
   레이어 2 보안: **WPA+WPA2**빠른 전환: **사용 안** 함(상자는 선택되지 않음)인증 키 관리: 802.IX: **사용**



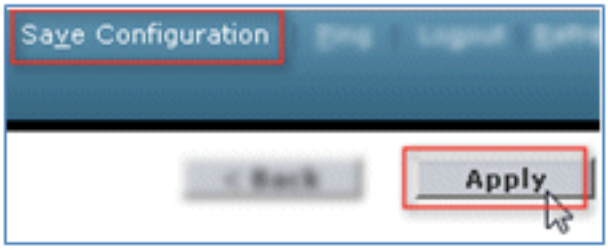
10. **고급** 탭으로 **이동하여** 다음 특성을 설정합니다.

    Allow AAA Override(AAA 재정의 허용): **Enabled(활성화됨)**NAC State(NAC 상태): **Radius NAC**

11. **Advanced(고급)** 탭에서 아래로 스크롤하여 FlexConnect Local Switching(FlexConnect 로컬 스위칭)을 Enabled(활성화됨)로 **설정합니다**.



12. Apply(**적용**) 및 Save Configuration(**컨피그레이션 저장**)**을 클릭합니다**.



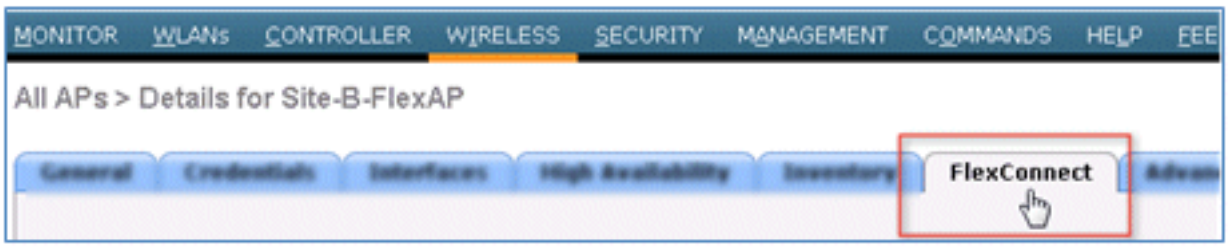
13. 새 WLAN이 둘 다 생성되었는지 확인합니다.

FlexConnect AP 컨피그레이션

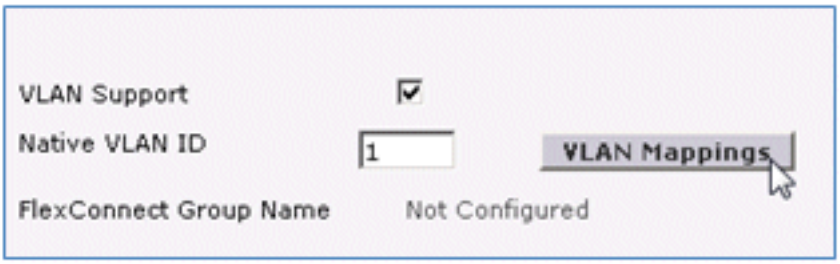
FlexConnect AP를 구성하려면 다음 단계를 완료하십시오.

1. WLC > **Wireless로 이동하고** 대상 FlexConnect AP를 클릭합니다.

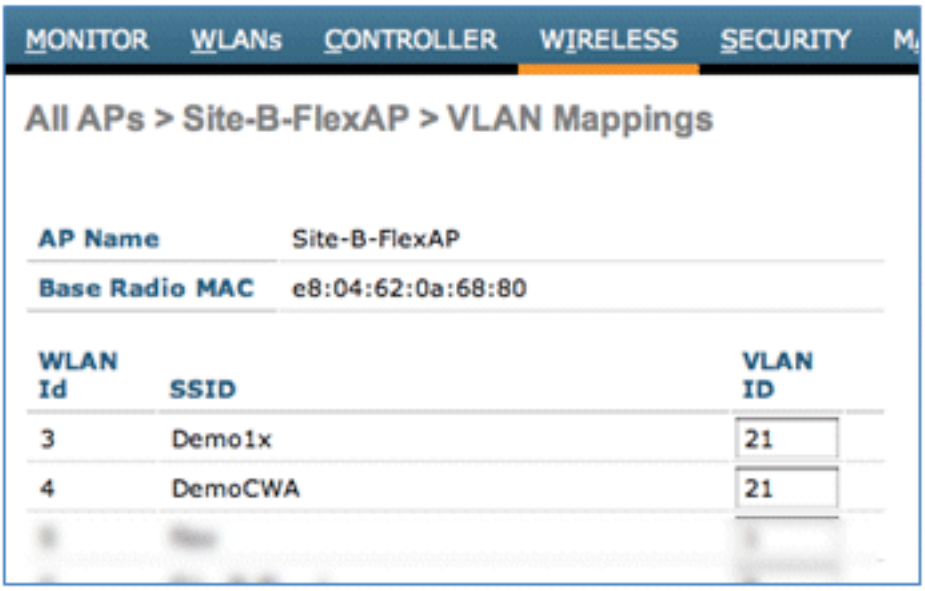
2. FlexConnect 탭**을** 클릭합니다.



3. Enable VLAN Support(VLAN 지원 활성화)(상자가 선택됨)를 선택하고 Native VLAN ID(네이티브 VLAN ID)를 설정한 다음 VLAN Mappings(VLAN 매핑)**를 클릭합니다**.



4. 로컬 스위칭을 위한 SSID에 대해 VLAN ID를 **21**(이 예에서는)으로 설정합니다.



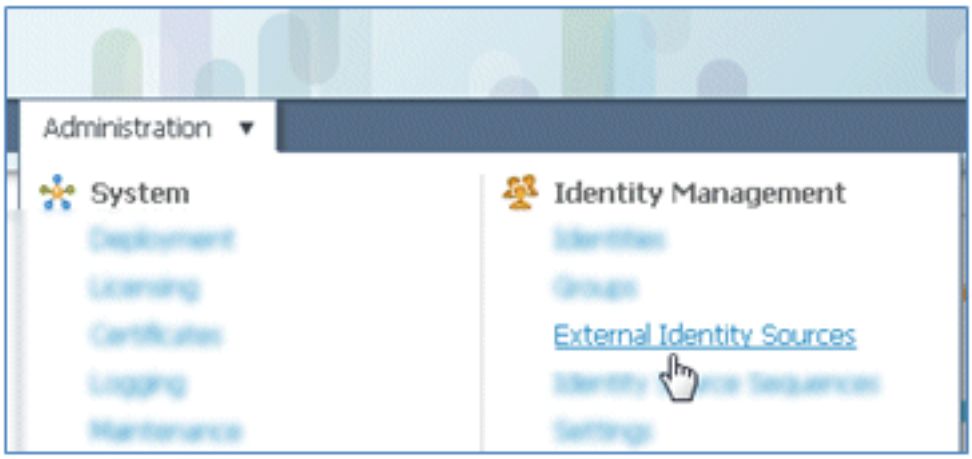
5. Apply(**적용**) 및 Save Configuration(**컨피그레이션 저장**)**을 클릭합니다**.

ISE 구성

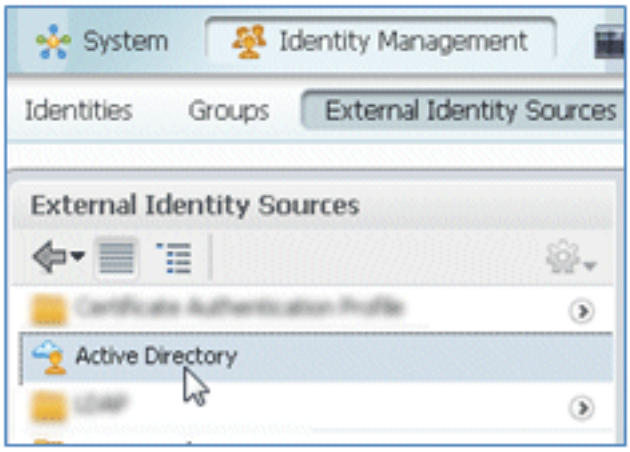
ISE를 구성하려면 다음 단계를 완료하십시오.

1. ISE 서버에 로그인합니다. <https://ise>.

2. **Administration > Identity Management > External Identity Sources로** 이동합니다.

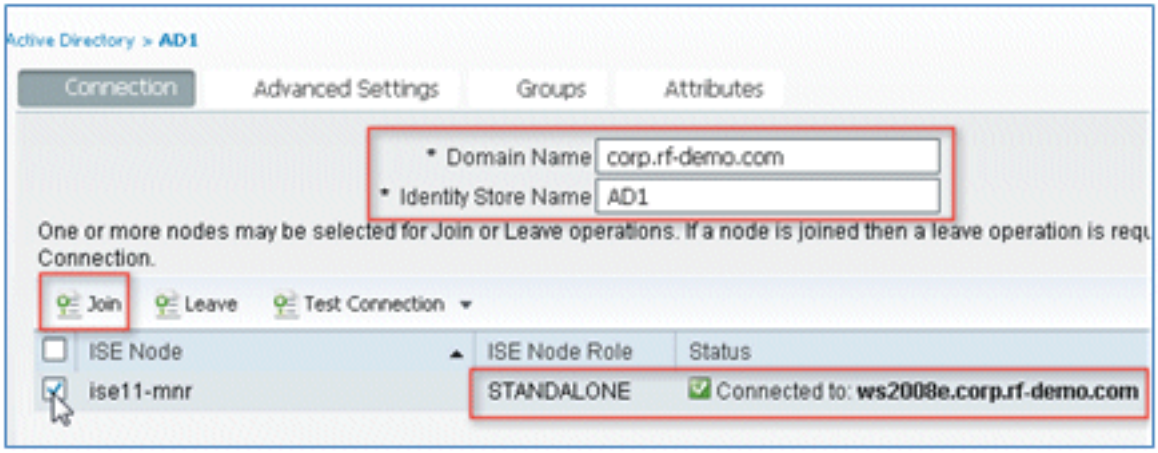


3. **Active Directory**를 **클릭합니다**.

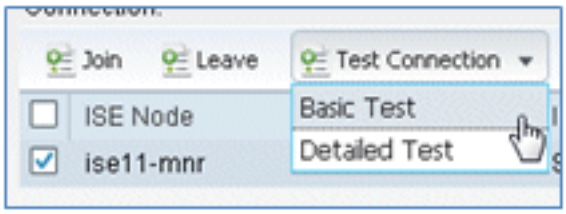


4. Connection(연결) 탭에서

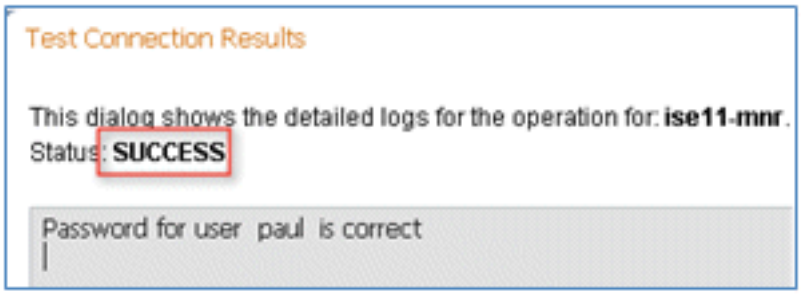
corp.rf-demo.com의 Domain Name(이 예에서)을 추가하고 Identity Store Name(ID 저장소 이름) 기본값을 **AD1**로 변경합니다.Save Configuration(컨피그레이션 **저장)을 클릭합니다** .Join(**참여**)을 클릭하고 가입에 필요한 AD 관리자 계정 사용자 이름 및 비밀번호를 제공합니다 .Status(상태)는 녹색이어야 합니다. Enable **Connected to(연결됨** 활성화): (확인란이 선택됨).



5. 현재 도메인 사용자와 AD에 대한 기본 연결 테스트를 수행합니다.

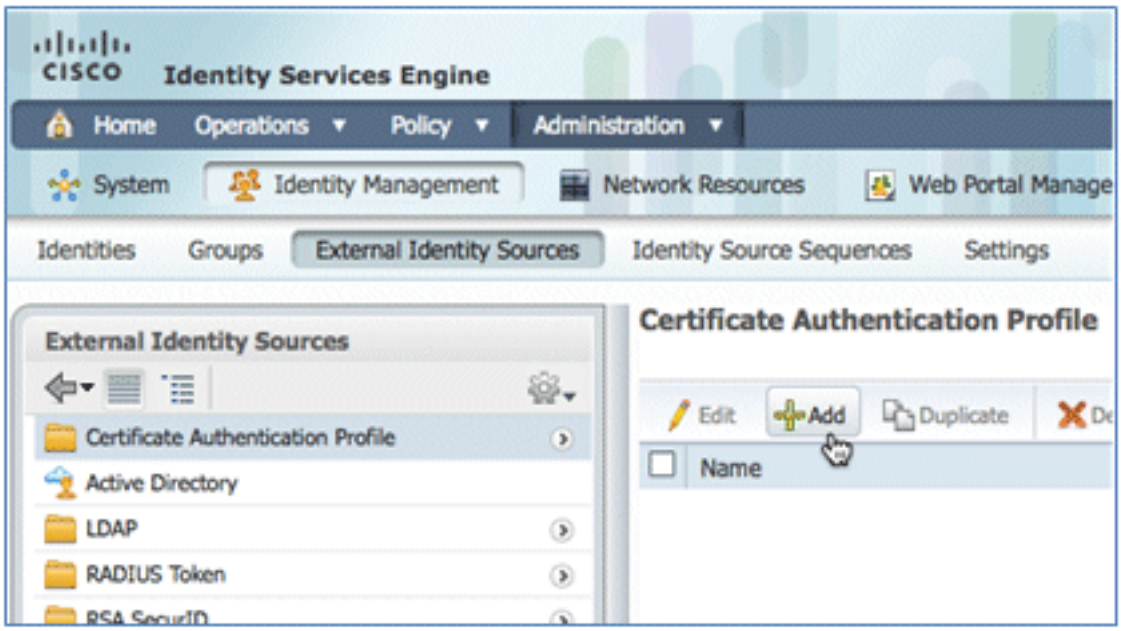


6. AD에 연결되면 대화 상자에서 암호가 올바른지 확인합니다.

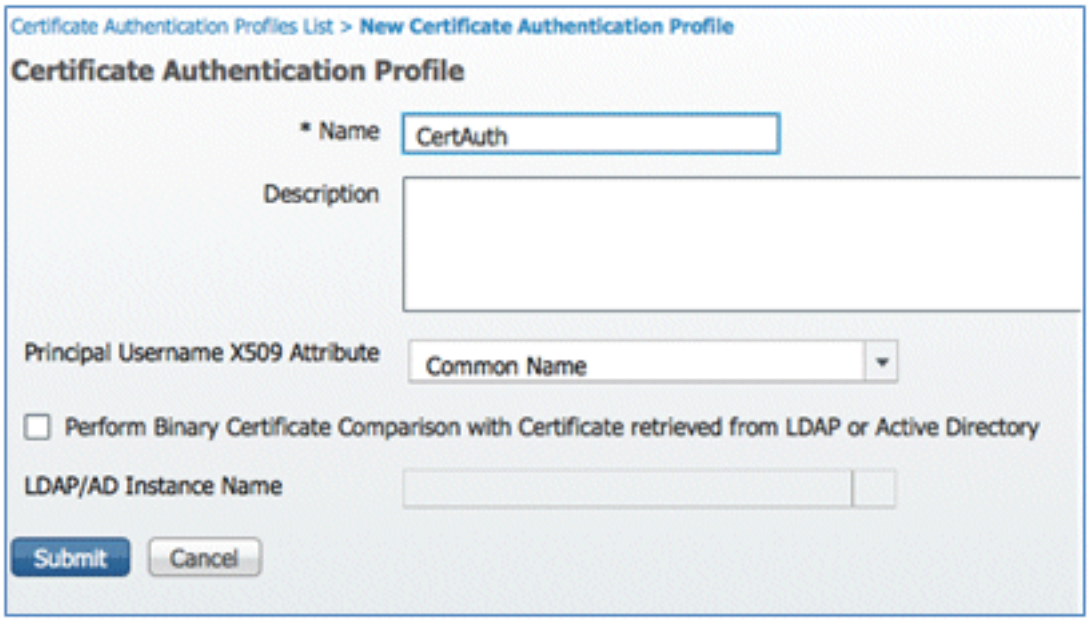


7. Administration(**관리**) > Identity **Management(ID 관리) > External Identity Sources(외부 ID 소스)로 이동합니다**.

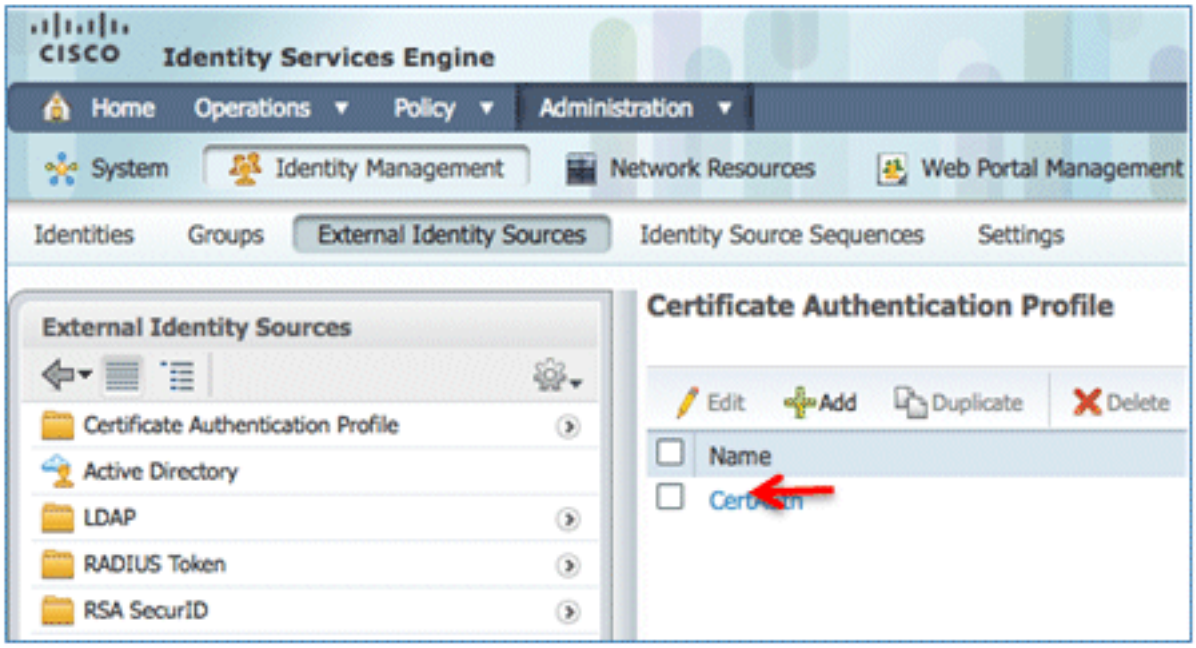
   Certificate **Authentication Profile을 클릭합니다**.새 CAP(Certificate Authentication Profile)에 대해 Add를 클릭합니다.



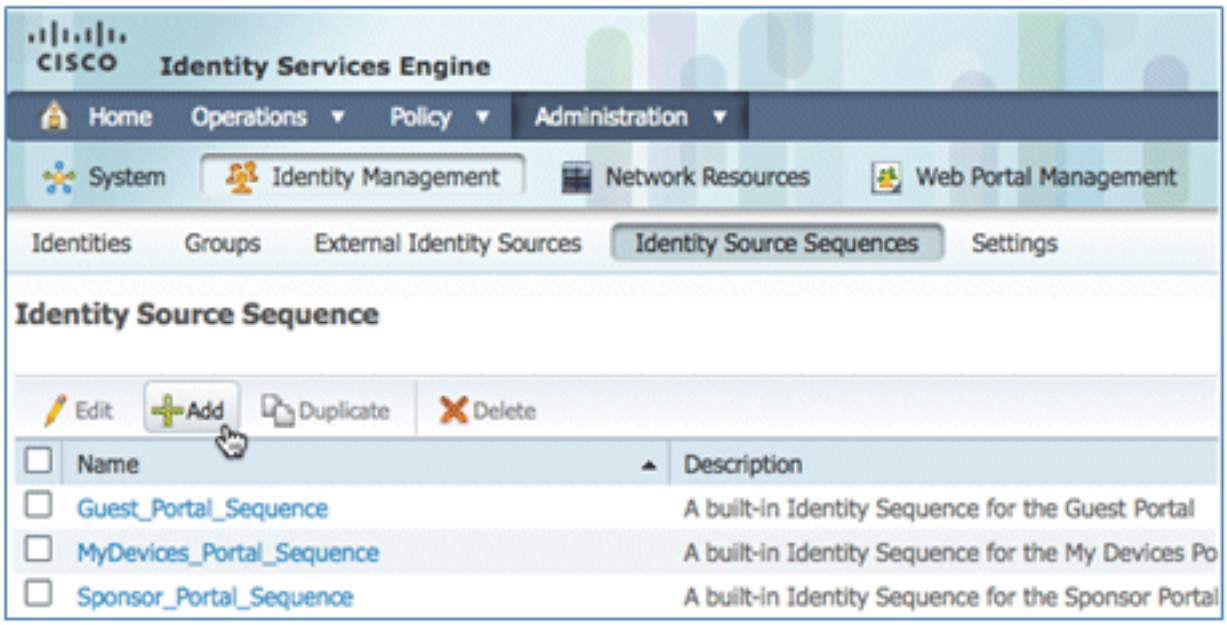
8. CAP의 **CertAuth**(이 예에서는) 이름을 입력합니다. Principal Username X509 Attribute(사용자 이름 X509 특성)에서 **Common Name(일반 이름)을** 선택한 다음 Submit(**제출)을** 클릭합니다.



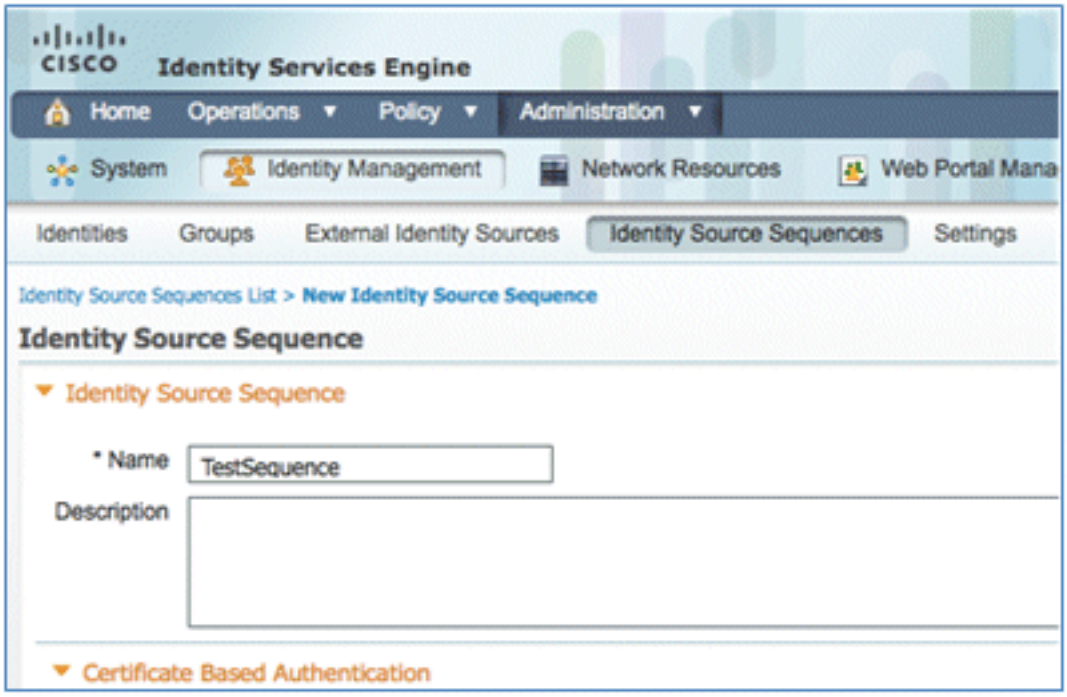
9. 새 CAP가 추가되었는지 확인합니다.



10. **Administration > Identity Management > Identity Source Sequences로** 이동하고 Add를 **클릭합니다**.

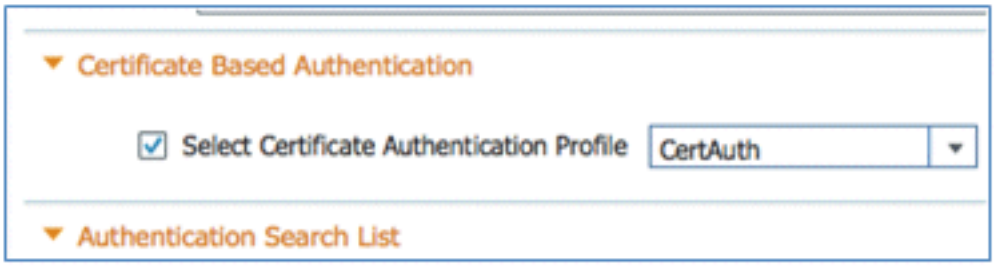


11. 시퀀스의 이름을 TestSequence**로 지정합니다**(이 예에서는).



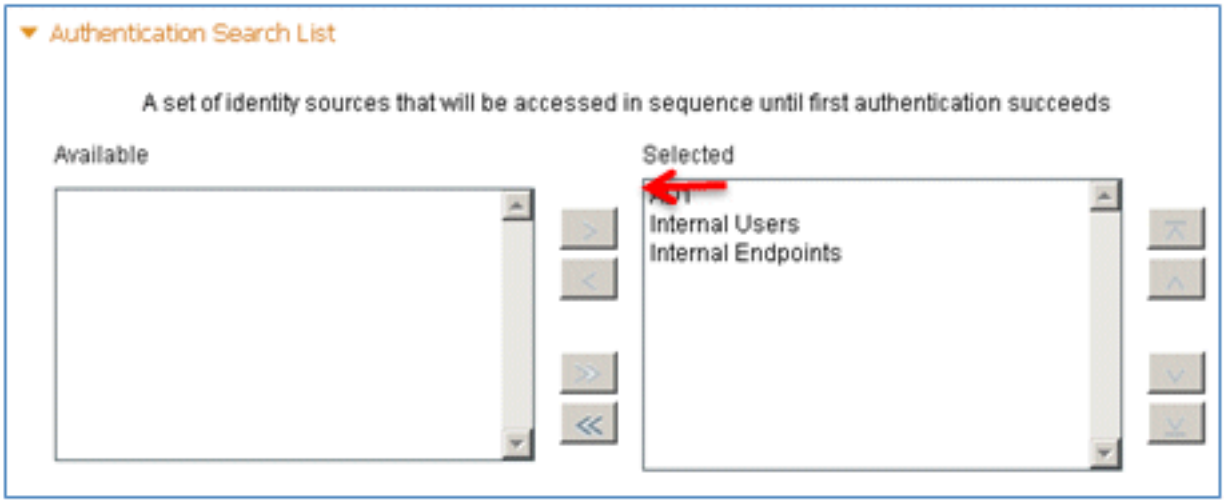
12. 아래로 스크롤하여 **Certificate Based Authentication(인증서 기반 인증)으로 이동합니다**.

    Select **Certificate Authentication Profile(인증서 인증 프로파일 선택)** 활성화(상자가 선택됨)CertAuth(**또는** 이전에 생성한 다른 CAP 프로파일)를 선택합니다.

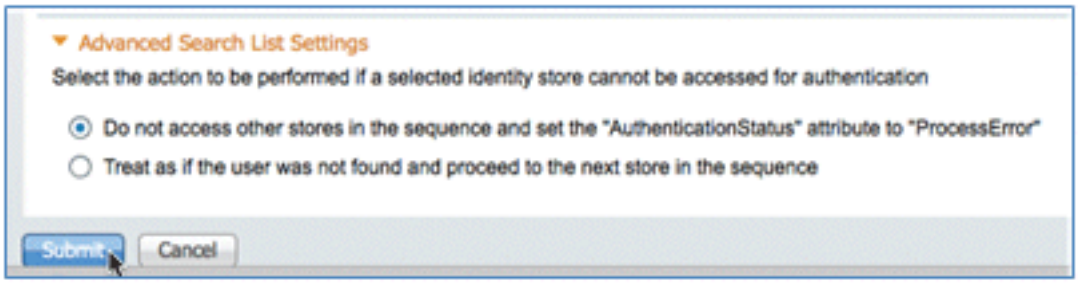


13. 아래로 스크롤하여 **Authentication Search List(인증 검색 목록)로 이동합니다**.

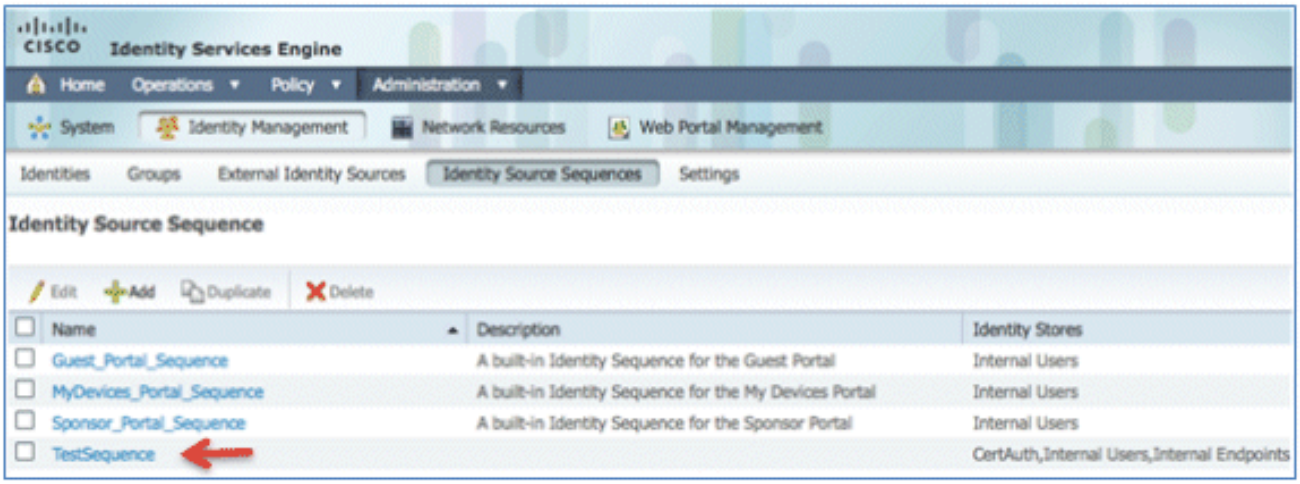
AD1을 Available(사용 가능)에서 Selected(선택)로 이동합니다.AD1을 최우선 순위로 이동하려면 위로 버튼을 클릭합니다.



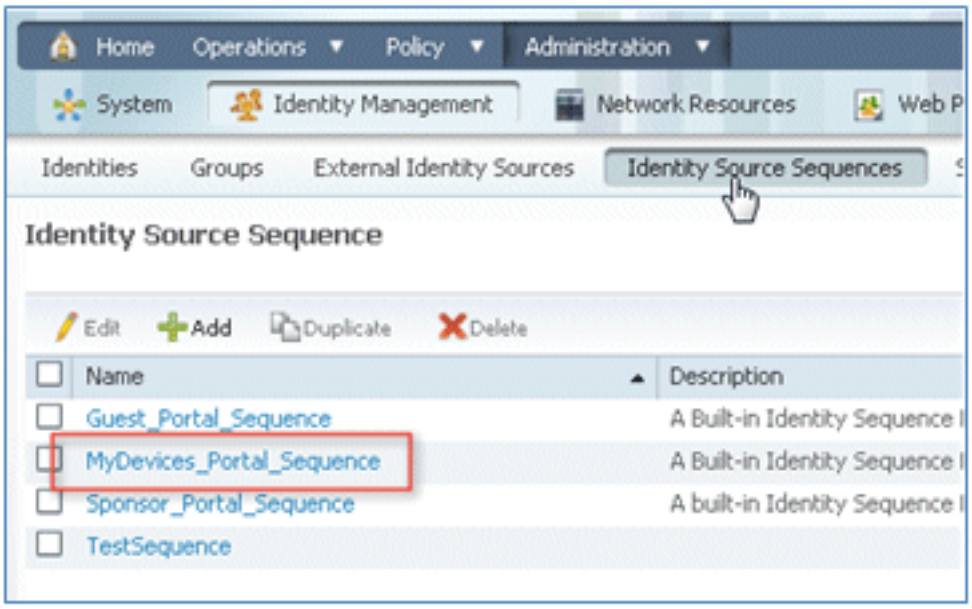
14. Submit(**제출**)을 클릭하여 저장합니다.



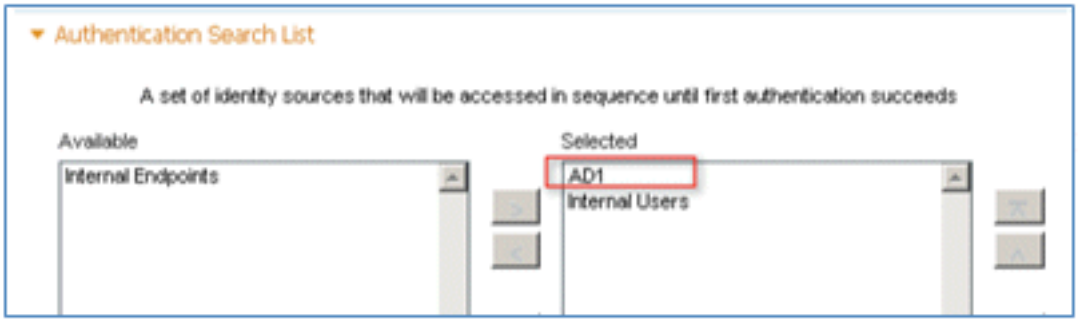
15. 새 ID 소스 시퀀스가 추가되었는지 확인합니다.



16. 내 디바이스 포털을 인증하려면 AD를 사용합니다. ISE > **Administration(관리) > Identity Management(ID 관리) > Identity Source Sequence(ID 소스 시퀀스)로 이동하고 MyDevices**_Portal_Sequence**를 편집합니다.**



17. AD1을 최우선 순위로 이동하려면 Selected(선택됨) 목록에 AD1을 추가하고 up(위로) 버튼을 클릭합니다.

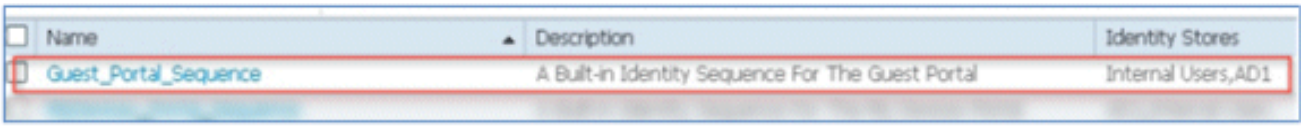


18. 저장을 **클릭합니다**.

19. MyDevices_Portal_Sequence의 ID 저장소 시퀀스에 **AD1**이 포함되어 있는지 **확인합니다**.

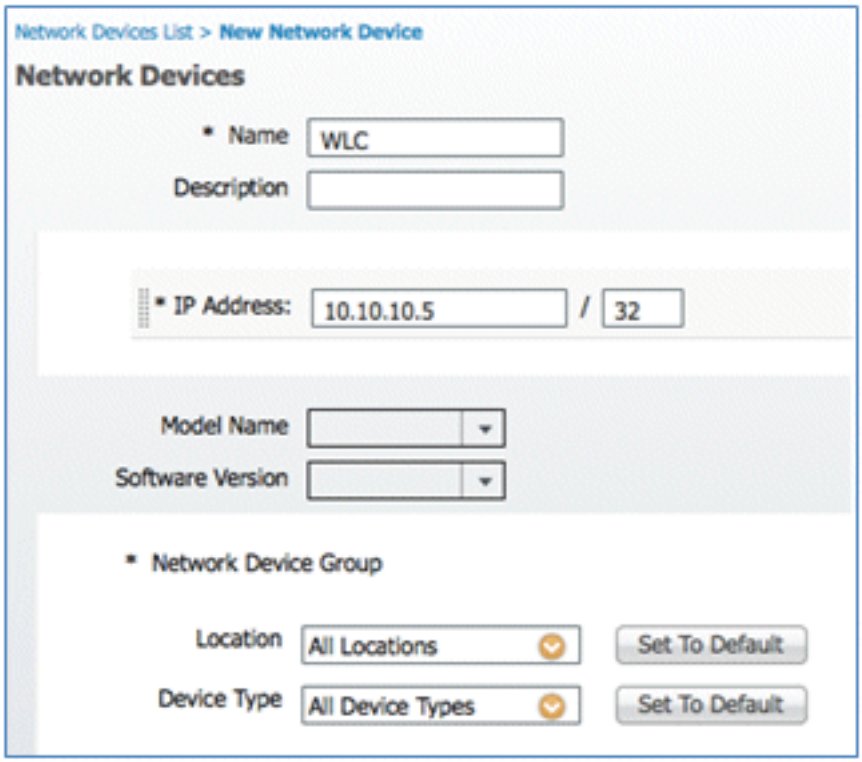
20. 16-19단계를 반복하여 Guest_Portal_Sequence에 대한 AD1을 추가하고 Save를 **클릭합니다**.

21. Guest_Portal_Sequence에 **AD1**이 포함되어 있는지 **확인합니다**.

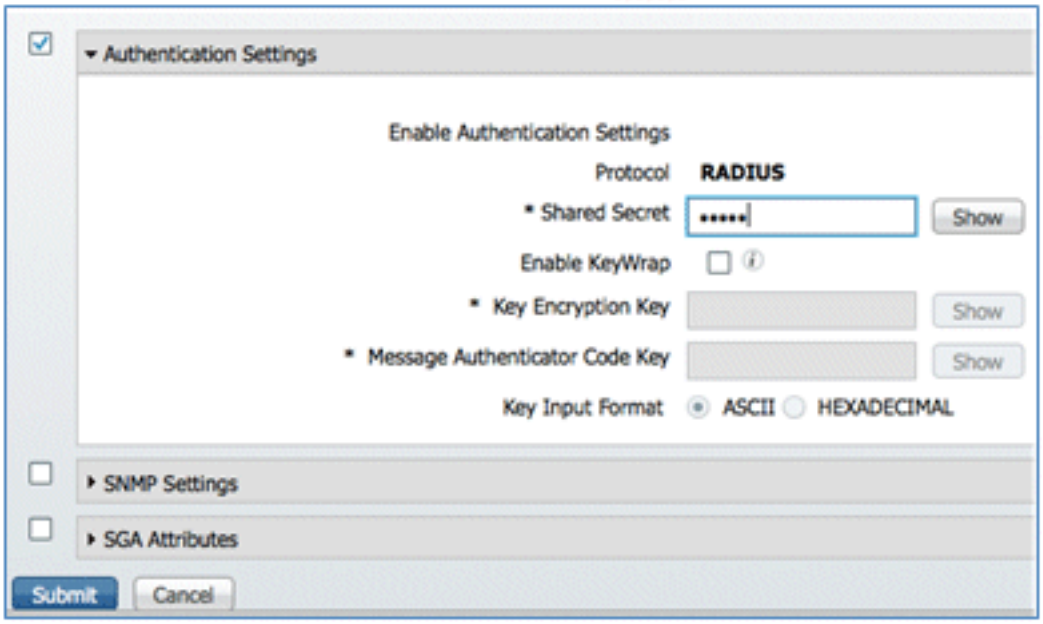


22. WLC(Network Access Device)에 WLC를 추가하려면 **Administration(관리) > Network Resources(네트워크 리소스)** > Network Devices(**네트워크 디바이스)로** 이동하고 **Add(추가)**를 클릭합니다.

23. WLC 이름, IP 주소, 서브넷 마스크 등을 추가 합니다.

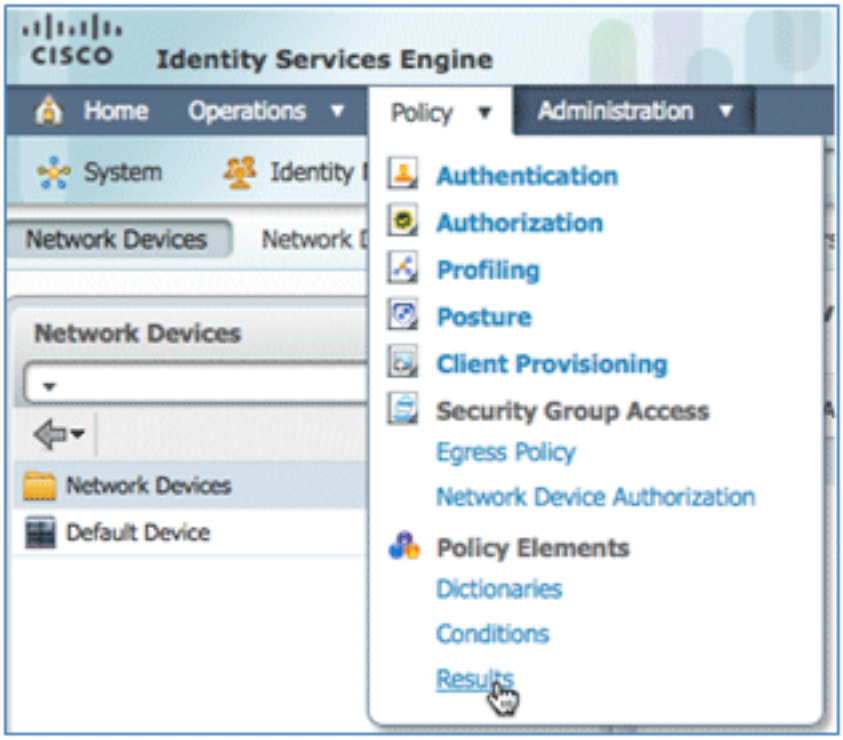


24. 아래로 스크롤하여 Authentication Settings(인증 설정)로 이동하고 Shared Secret(공유 암호)를 입력합니다. 이는 WLC RADIUS의 공유 암호와 일치해야 합니다.

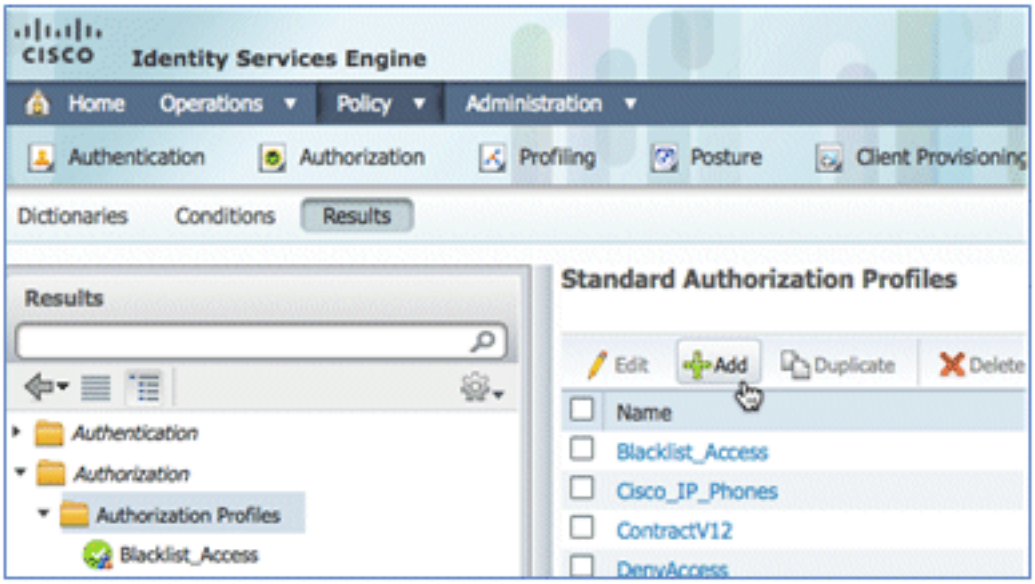


25. Submit(제출)을 클릭합니다.

26. ISE > Policy > Policy Elements > Results로 이동합니다.

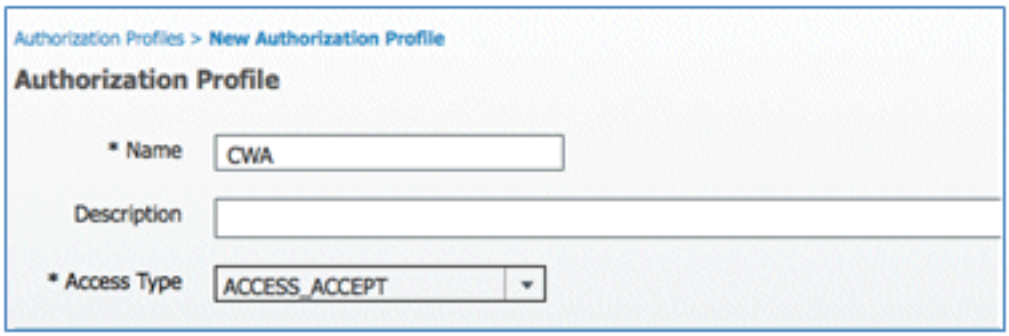


27. Results and **Authorization(결과 및 권한 부여)**을 확장하고 **Authorization Profiles(권한 부여 프로파일)**를 클릭한 다음 **Add**(추가)를 클릭하여 새 프로파일을 선택합니다.



28. 이 프로필에 다음 값을 지정합니다.

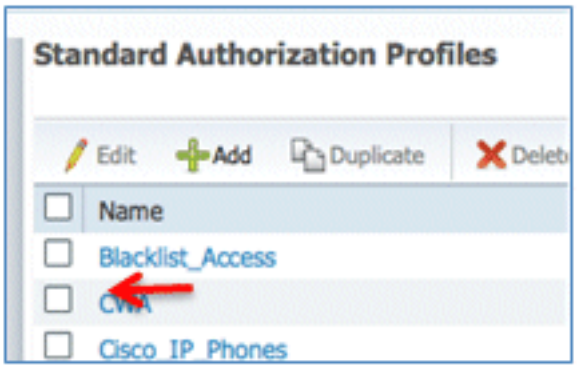
이름: **CWA**



Enable Web Authentication(웹 인증 활성화)(상자가 선택됨):

웹 인증: **중앙 집중식**ACL: **ACL-REDIRECT**(WLC 사전 인증 ACL 이름과 일치해야 함)리디렉션: **기본값**

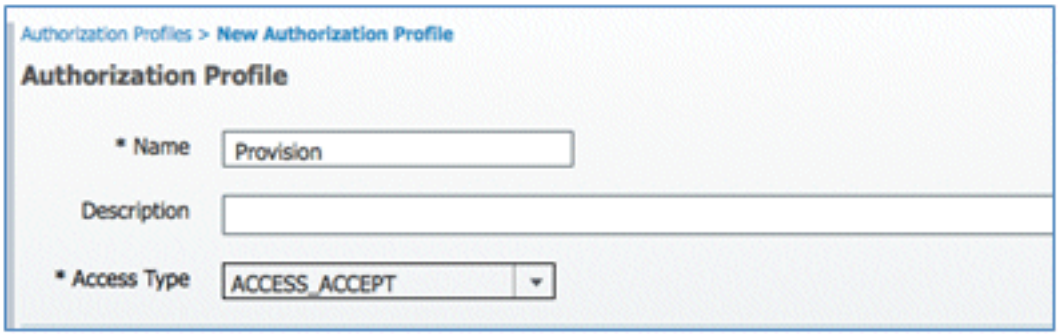
29. Submit(**제출**)을 클릭하고 CWA 권한 부여 프로파일이 추가되었는지 확인합니다.



30. 새 권한 **부여** 프로필을 생성하려면 Add를 클릭합니다.

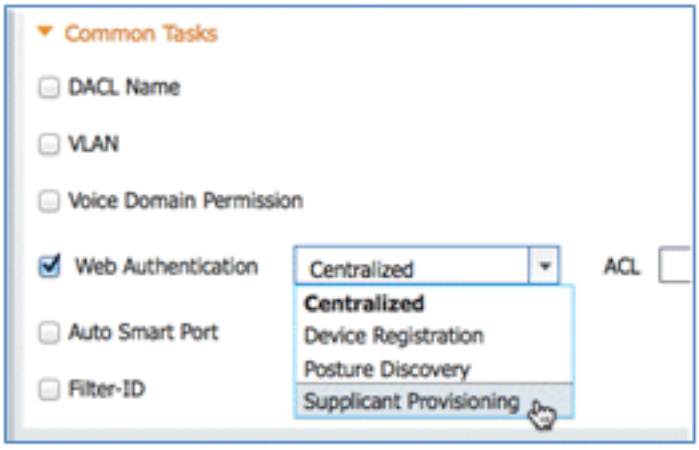
31. 이 프로필에 다음 값을 지정합니다.

    Name(이름): **Provision(프로비저닝)**

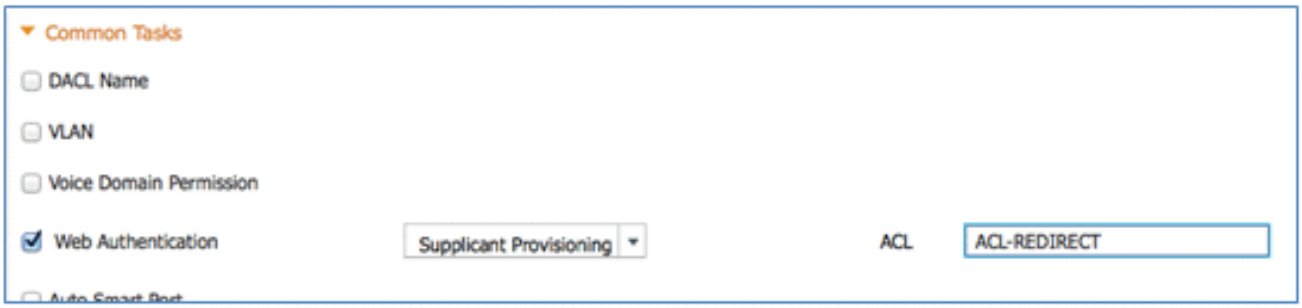


    Enable Web Authentication(웹 인증 활성화)(상자가 선택됨):

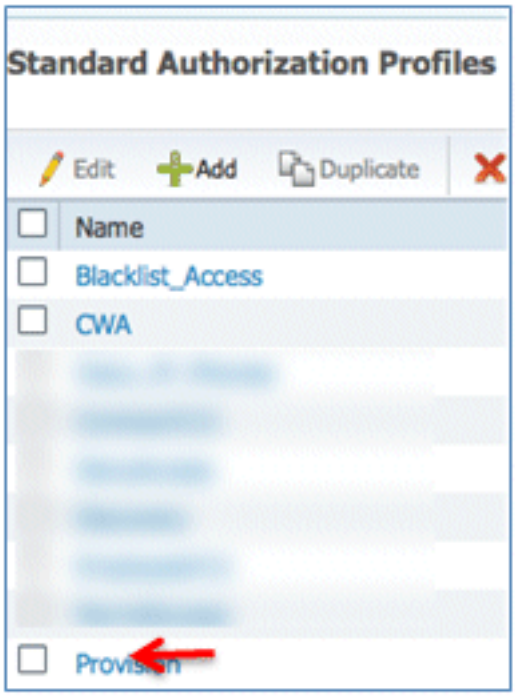
    웹 인증 값: **신청자 프로비저닝**



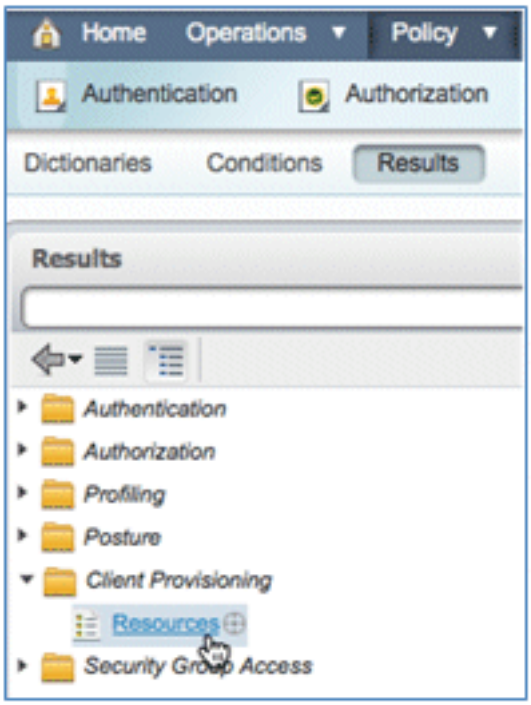
    ACL: **ACL-REDIRECT**(WLC 사전 인증 ACL 이름과 일치해야 함)



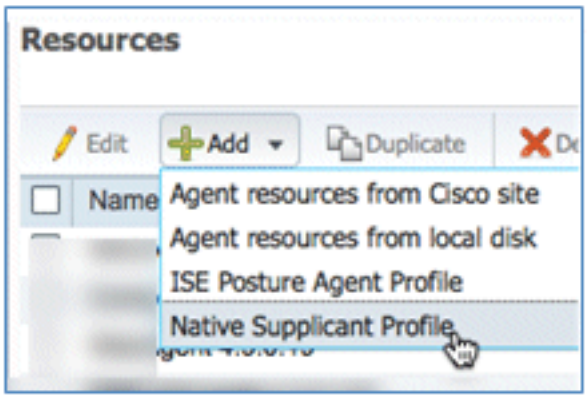
32. Submit(**제출**)을 클릭하고 Provision authorization(프로비저닝 권한 부여) 프로파일이 추가되었는지 확인합니다.



33. Results(결과)에서 아래로 스크롤하여 **Client Provisioning(클라이언트 프로비저닝)**을 확장하고 Resources(리소스)**를 클릭합니다**.



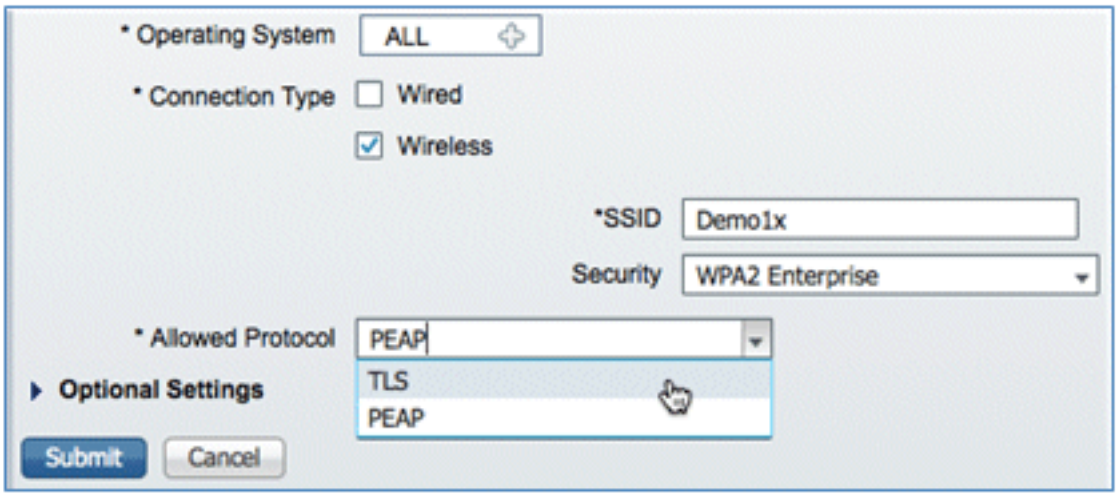
34. Native **Supplicant Profile을 선택합니다**.



35. 프로필에 WirelessSP **이름**을 지정합니다(이 예에서는).

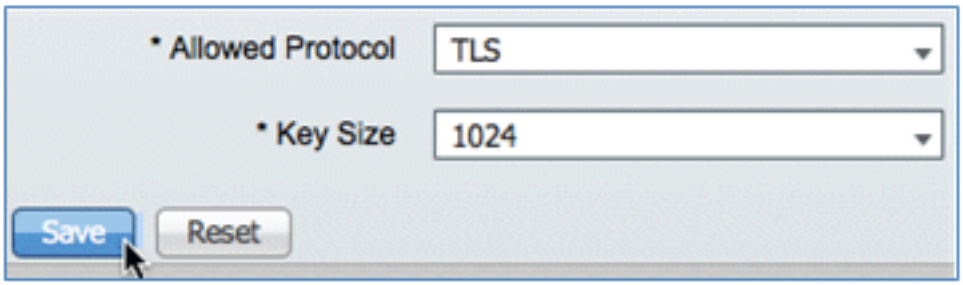
36. 다음 값을 입력합니다.

    연결 유형: **무선**SSID: **Demo1x**(이 값은 WLC 802.1x WLAN 컨피그레이션에서 가져온 것입니다.)허용되는 프로토콜: **TLS**키 크기: **1024**

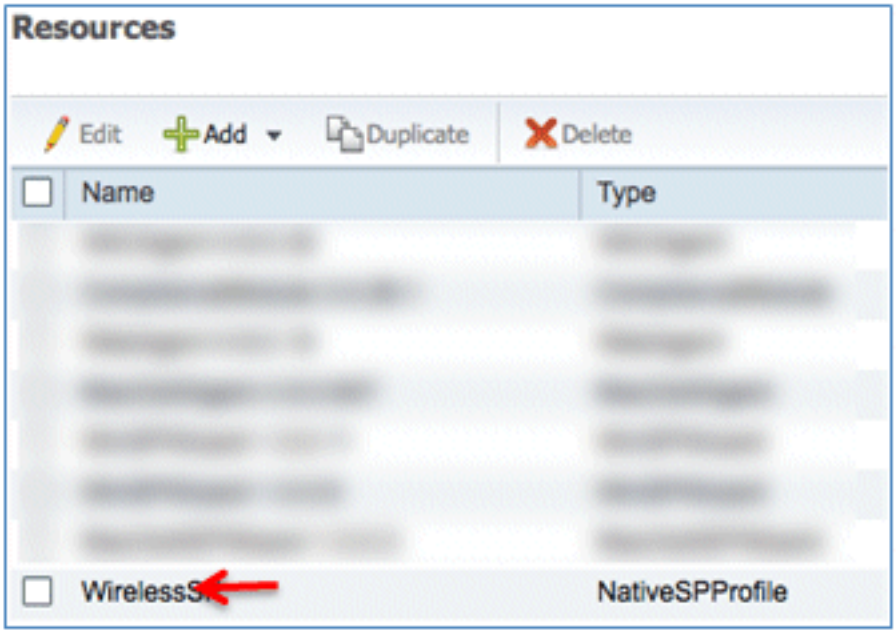


37. Submit(제출)**을 클릭합니다**.

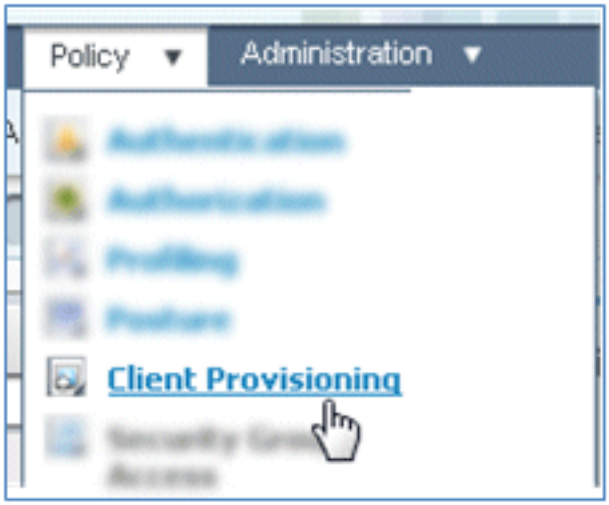
38. 저장을 **클릭합니다**.



39. 새 프로파일이 추가되었는지 확인합니다.

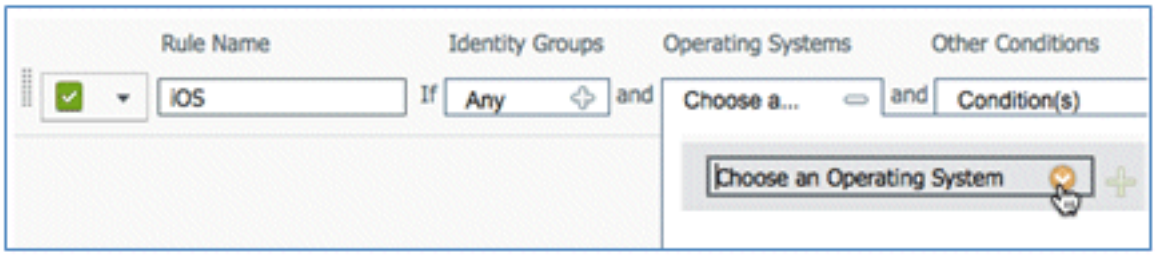


40. **Policy > Client Provisioning(정책 >** 클라이언트 프로비저닝)**으로 이동합니다**.

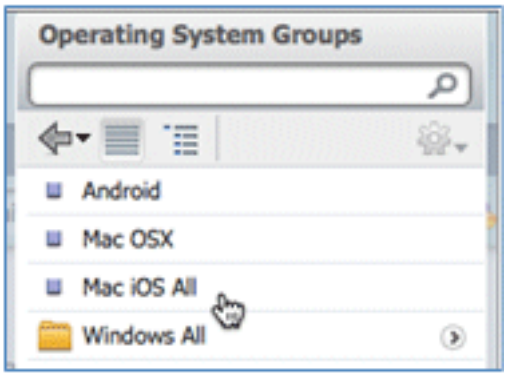


41. iOS 디바이스의 프로비저닝 규칙에 대해 다음 값을 입력합니다.

규칙 이름: **iOS**ID 그룹: **모두**

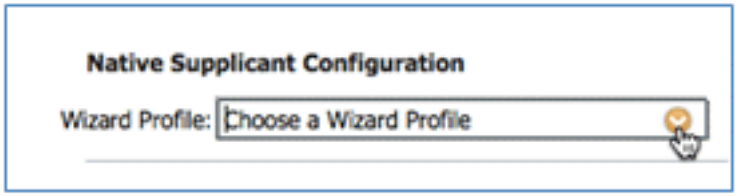


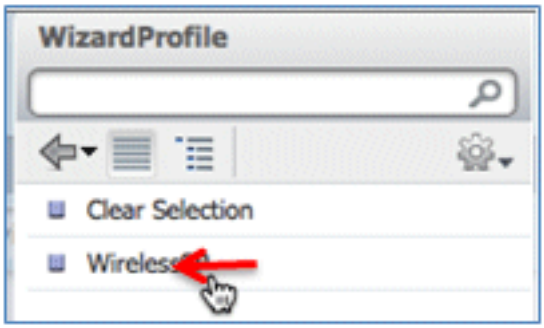
운영 체제: **Mac iOS All**



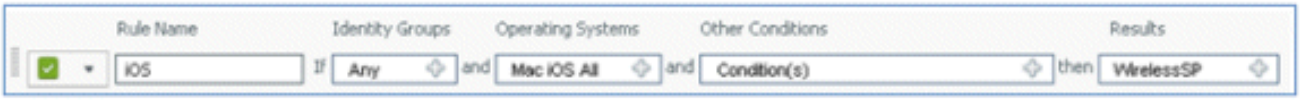
결과: **WirelessSP**(이전에 생성한 기본 신청자 프로파일)

Results > Wizard Profile (드롭다운 목록) > WirelessSP로 **이동합니다**.

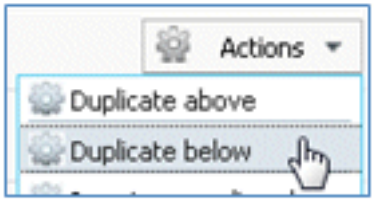




42. iOS 프로비저닝 프로파일이 추가되었는지 확인합니다.

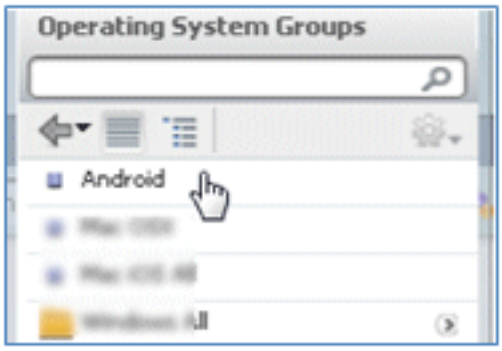


43. 첫 번째 규칙의 오른쪽에서 Actions(작업) 드롭다운 목록을 찾은 다음 아래(**또는** 위)에서 Duplicate(복제)를 선택합니다.



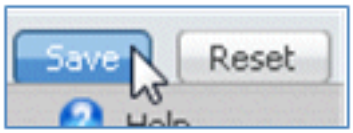
44. 새 규칙의 Name(이름)을 Android로 **변경합니다**.

45. 운영 체제를 Android로 **변경합니다**.

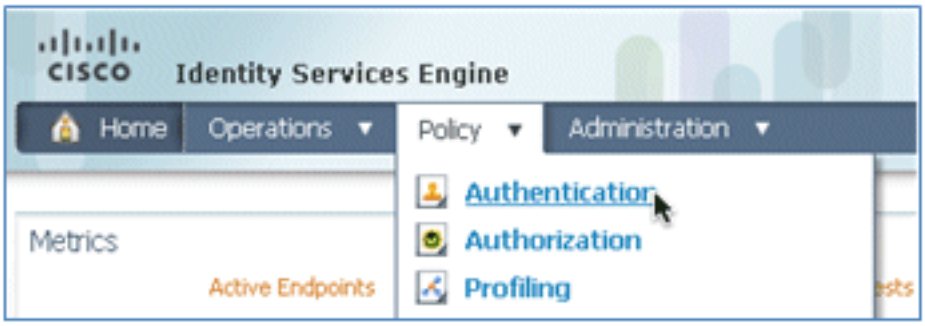


46. 다른 값은 변경하지 않습니다.

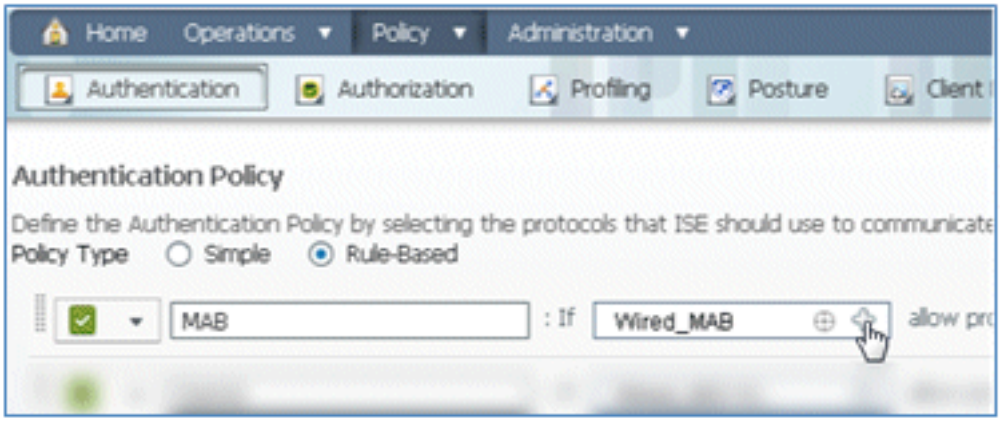
47. **저장**(왼쪽 하단 화면)을 클릭합니다.



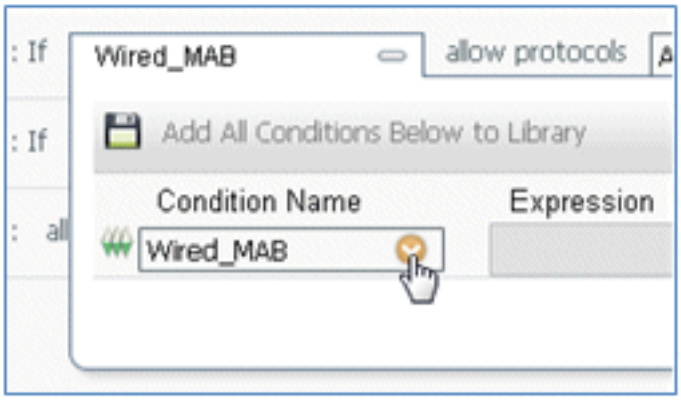
48. ISE > **Policy(정책)** > Authentication(**인증)으로 이동합니다**.



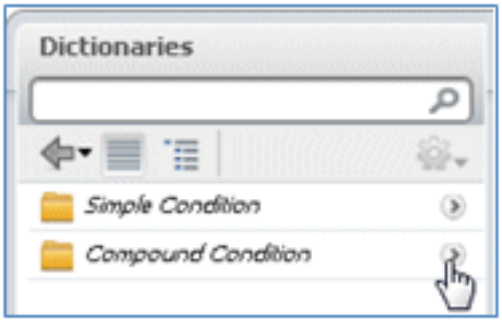
49. Wireless_MAB를 포함하도록 조건을 수정하고 Wired_**MAB를 확장합니다**.



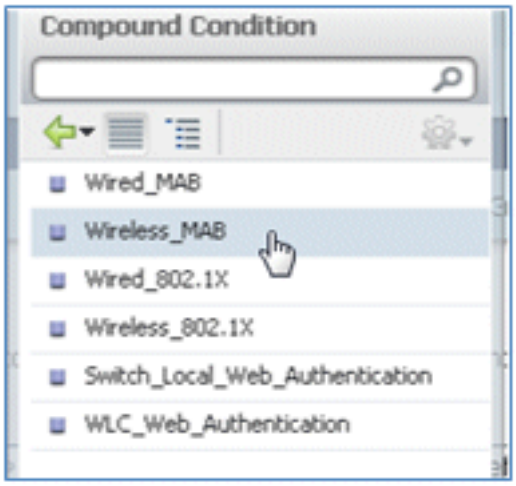
50. **Condition Name** 드롭다운 목록을 클릭합니다.



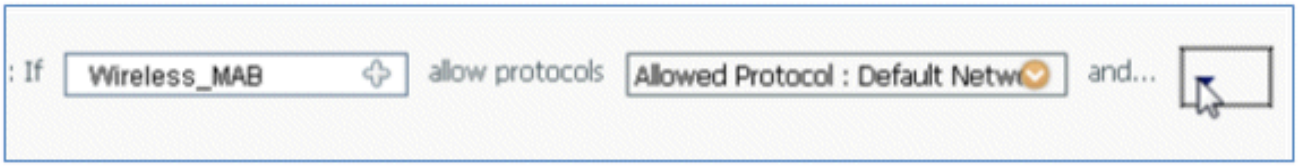
51. Dictionaries(**사전**) > Compound **Condition(복합 조건)을 선택합니다**.



52. Wireless_**MAB를 선택합니다**.

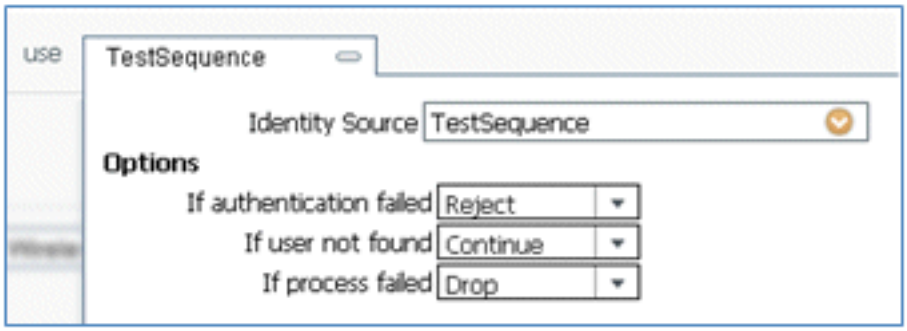


53. 규칙의 오른쪽에서 확장할 화살표를 선택합니다.

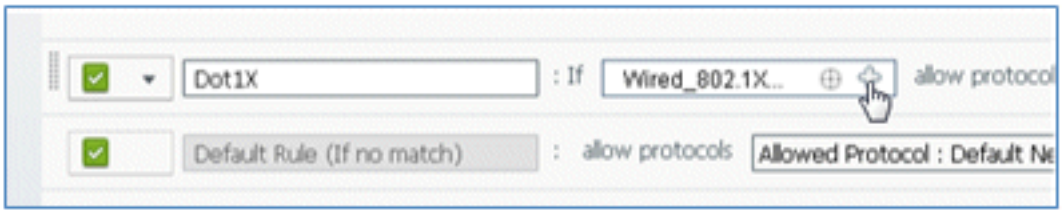


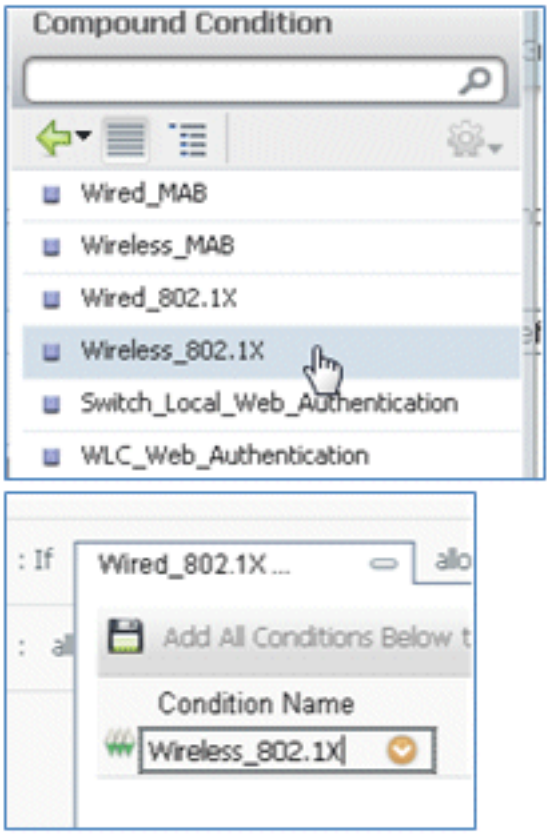
54. 드롭다운 목록에서 다음 값을 선택합니다.

ID 소스: **TestSequence**(이전에 만든 값)인증에 실패한 경우: **거부**사용자를 찾을 수 없는 경우: **계속**프로세스가 실패한 경우: **삭제**



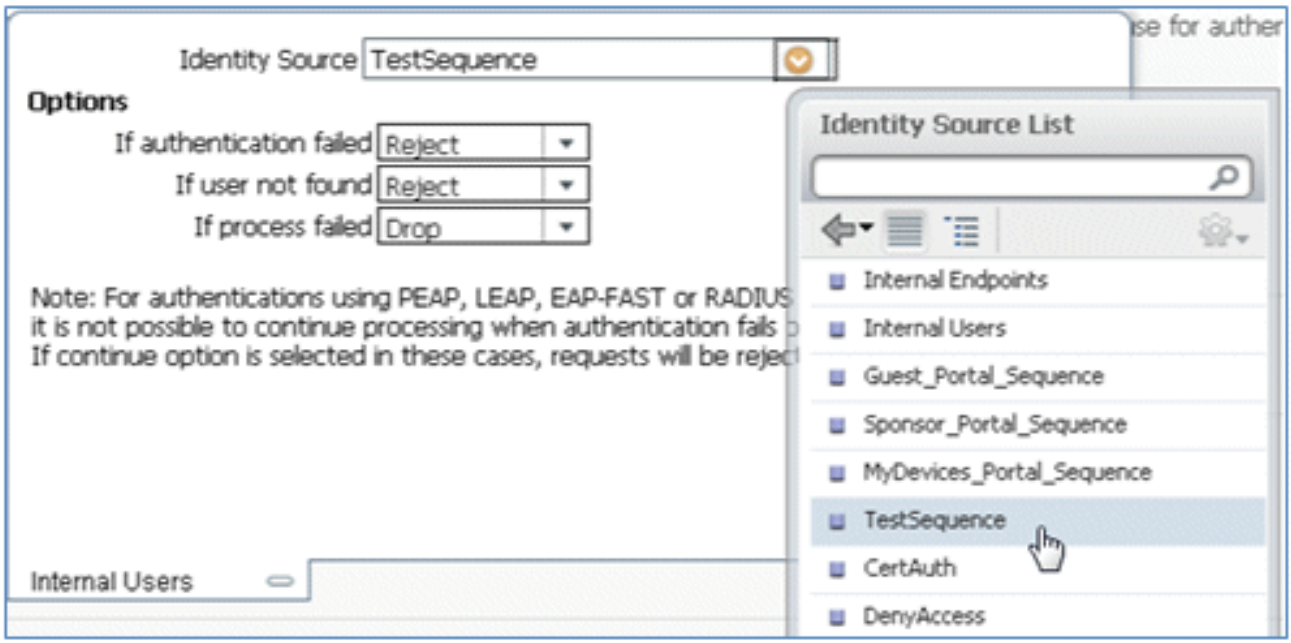
55. **Dot1X** 규칙으로 이동하여 다음 값을 변경합니다.





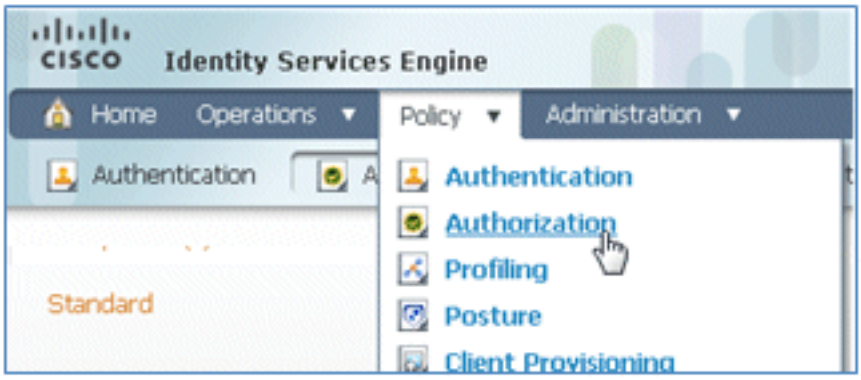
조건: **Wireless_802.1X**

ID 소스: **TestSequence**

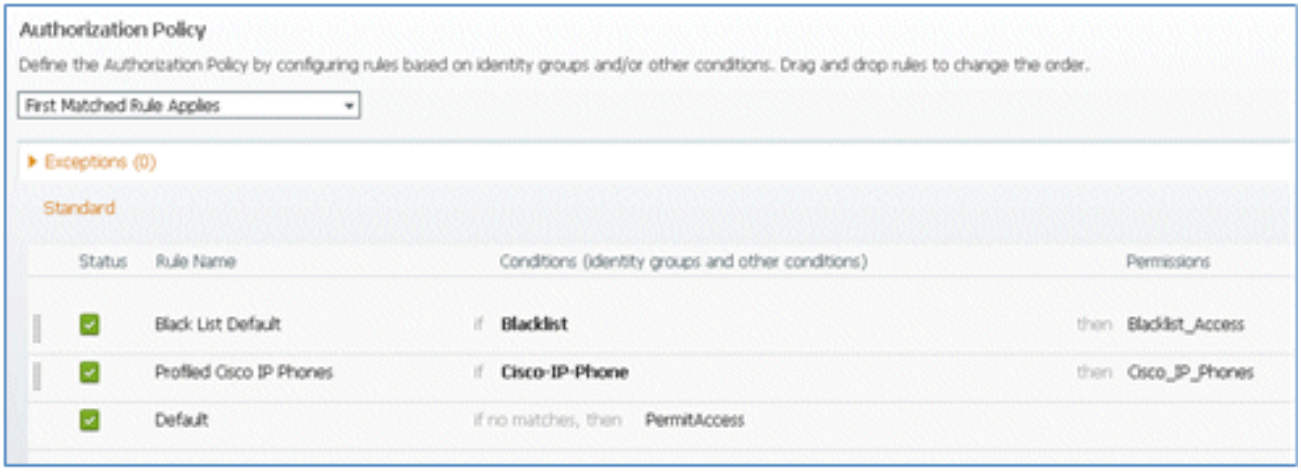


56. 저장을 **클릭합니다**.

57. **ISE > Policy >** Authorization으로 **이동합니다**.



58. 기본 규칙(예: Black List Default, Profiled 및 Default)은 설치에서 이미 구성되어 있습니다. 처음 두 규칙은 무시해도 됩니다. Default 규칙은 나중에 편집할 수 있습니다.



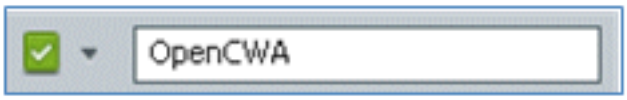
59. 두 번째 규칙(프로파일링된 Cisco IP Phone)의 오른쪽에서 Edit(수정) 옆의 아래쪽 화살표를 클릭하고 Insert **New Rule Below(아래에 새 규칙 삽입)를** 선택합니다.

새 표준 규칙 번호가 추가됩니다

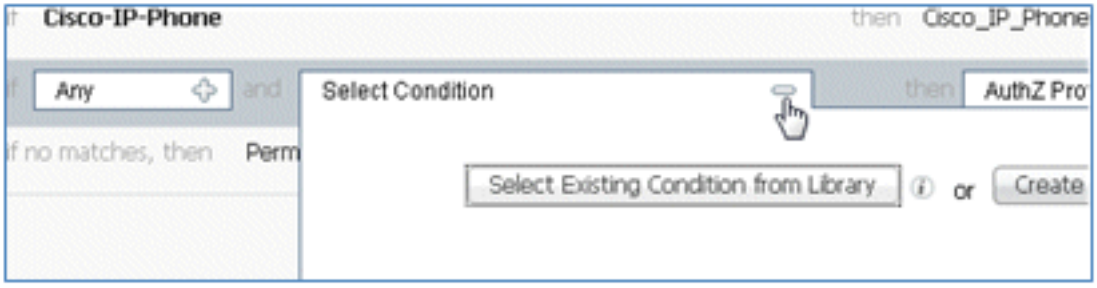
.

60. 규칙 이름을 Standard Rule #(표준 규칙 번호)에서 OpenCWA로 **변경합니다**. 이 규칙은 디바

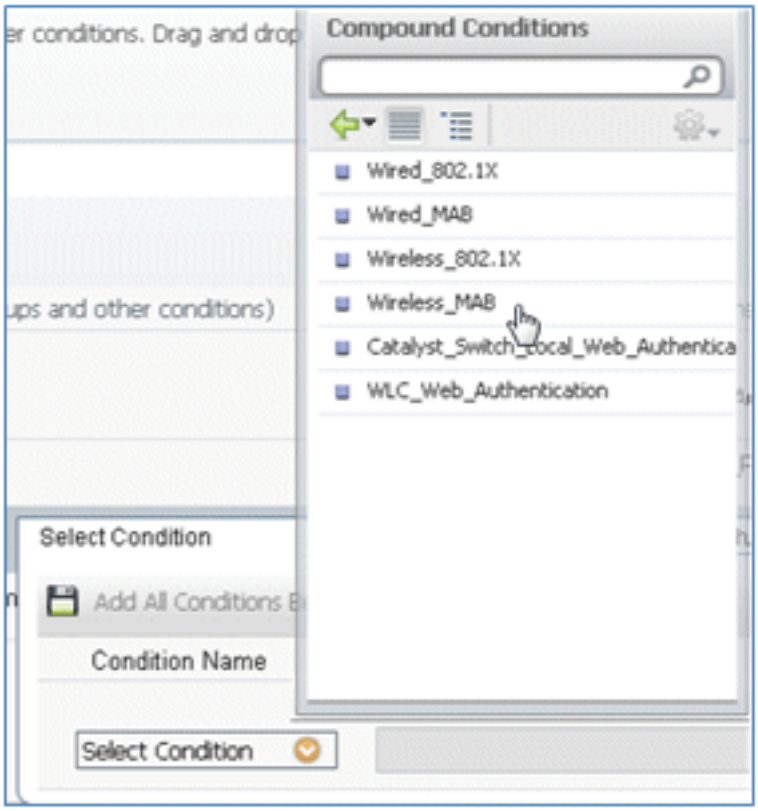
이스를 프로비저닝하기 위해 게스트 네트워크에 오는 사용자에 대해 개방형 WLAN(이중 SSID)에서 등록 프로세스를 시작합니다.



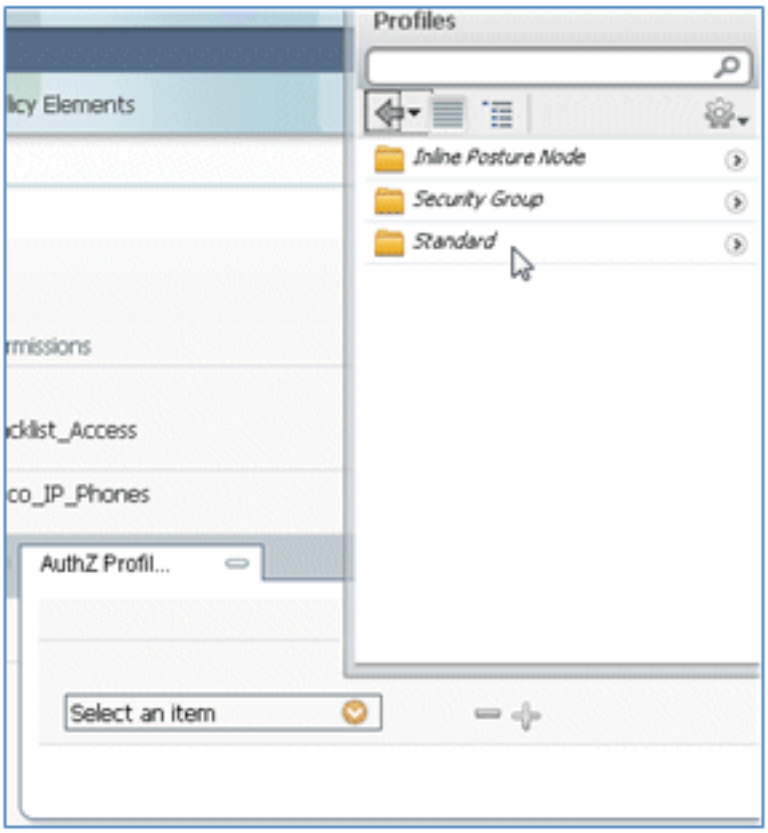
61. Condition(s)에 대한 더하기 기호(+)를 클릭하고 Select Existing Condition **from Library(라이브러리에서 기존 조건 선택)를 클릭합니다**.



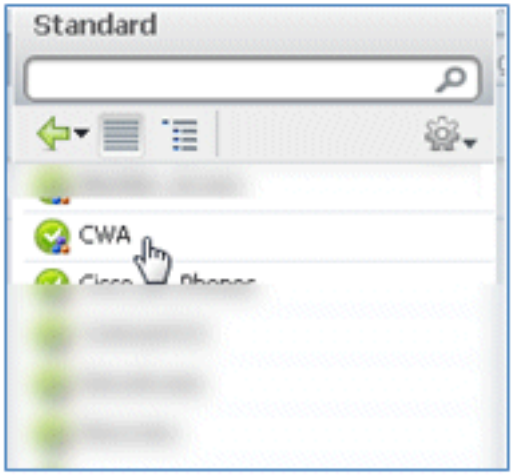
62. Compound **Conditions > Wireless_MAB를 선택합니다**.



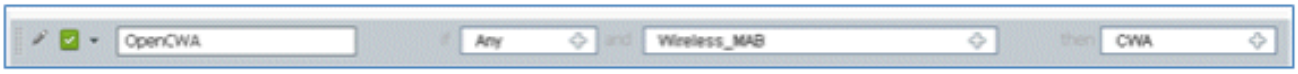
63. AuthZ Profile(AuthZ 프로필)에서 더하기 기호(+)를 클릭하고 **Standard(표준)**를 선택합니다.



64. 표준 CWA(**이전**에 생성한 권한 부여 프로파일)를 선택합니다.



65. 올바른 조건 및 권한 부여를 사용하여 규칙이 추가되었는지 확인합니다.



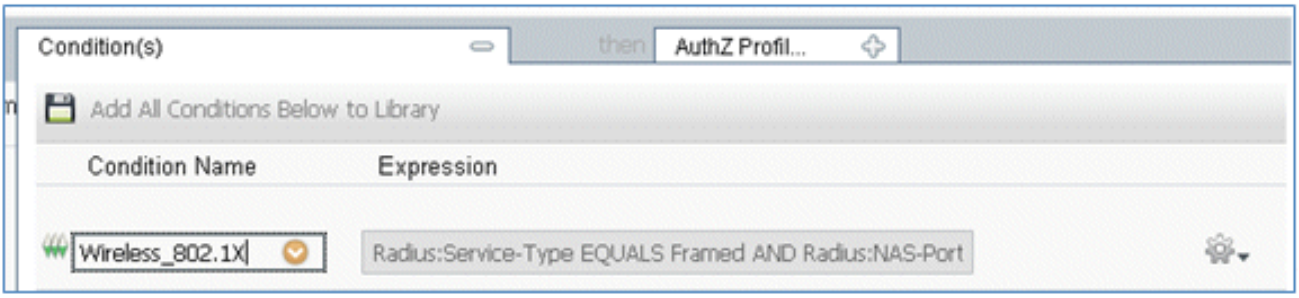
66. 규칙의 오른쪽에 있는 Done을 **클릭합니다**.

67. 동일한 규칙의 오른쪽에서 Edit 옆의 아래쪽 화살표를 클릭하고 Insert **New Rule Below**를 선

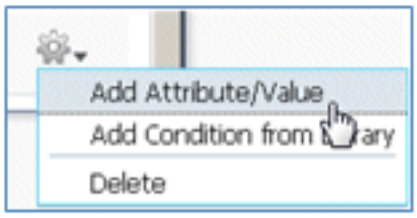
택합니다.

68. Rule Name(규칙 이름)을 Standard Rule #(표준 규칙 번호)에서 **PEAPrule(**이 예에서는 PEAPrule)로 변경합니다. 이 규칙은 PEAP(단일 SSID 시나리오에도 사용됨)가 TLS(Transport Layer Security)가 없는 802.1X 인증 및 이전에 생성한 프로비전 권한 부여 프로파일로 네트워크 신청자 프로비저닝을 시작했는지 확인하기 위한 것입니다.

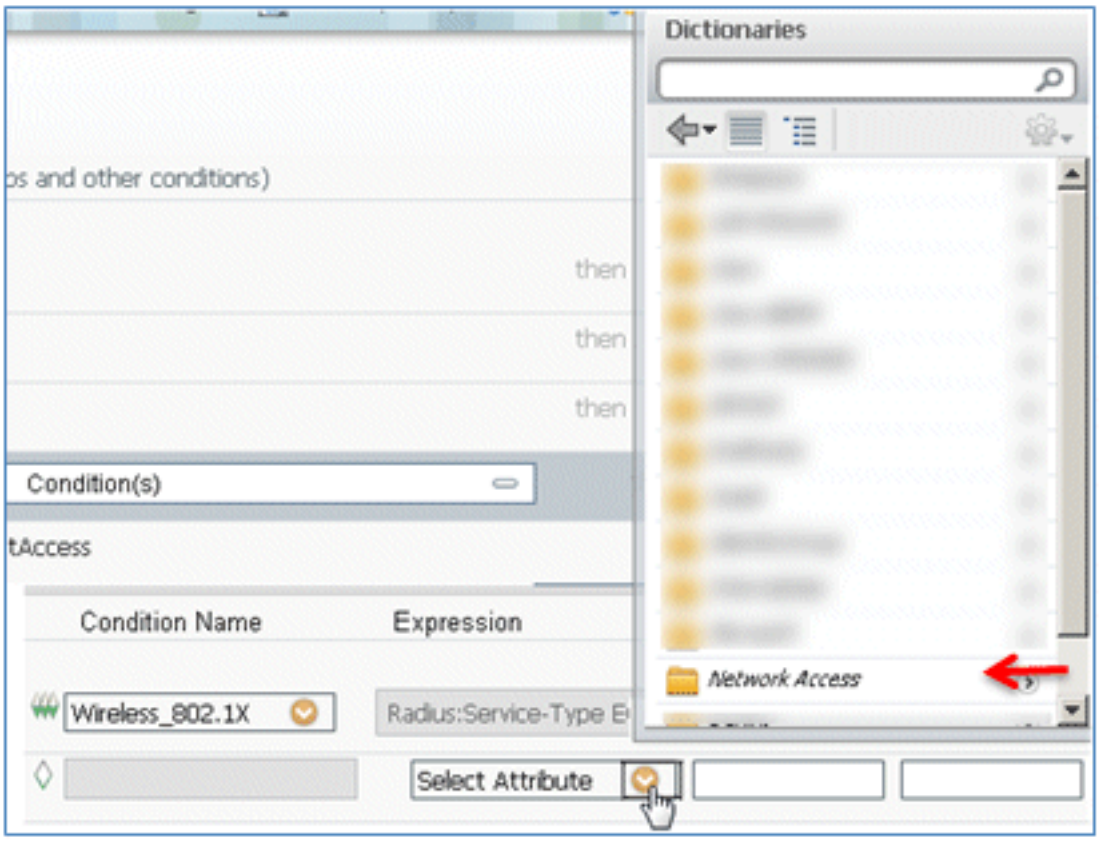
69. 조건을 **Wireless_802.1X로 변경합니다**.



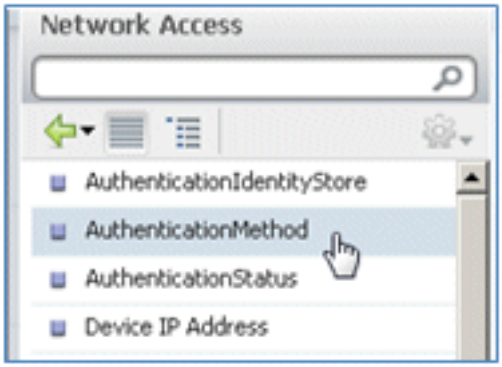
70. 조건 오른쪽의 톱니바퀴 모양 아이콘을 클릭하고 Add Attribute**/Value(특성/값 추가)를** 선택합니다. 이는 'and' 조건이지 'or' 조건이 아닙니다.



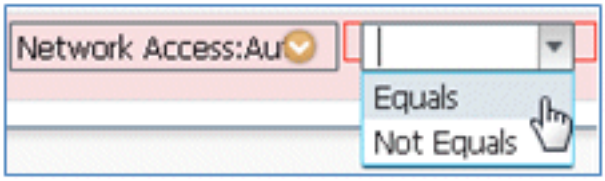
71. Network Access(**네트워크 액세스**)를 찾아 **선택합니다**.



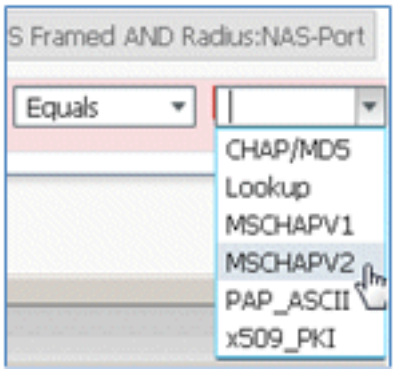
72. AuthenticationMethod를 선택하고 다음 값을 입력합니다.



AuthenticationMethod: **같음**

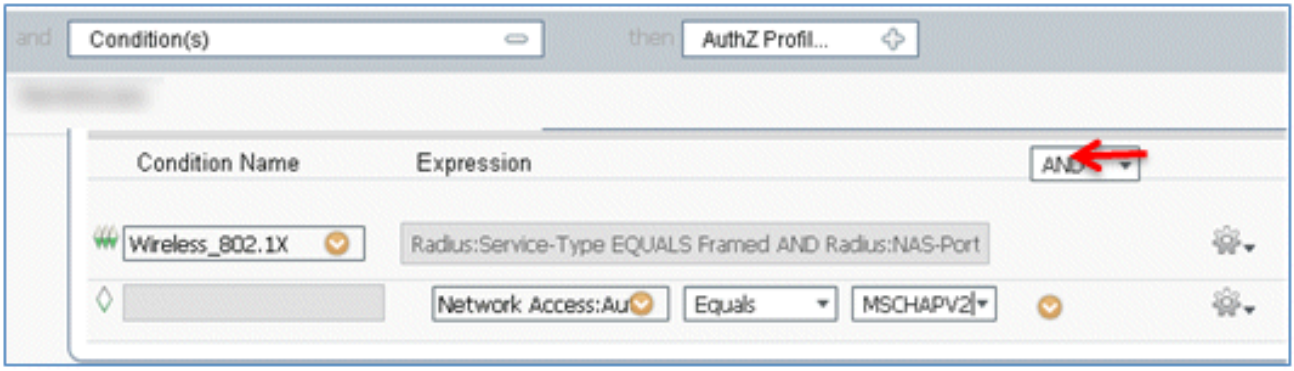


MSCHAPV2를 **선택합니다**.

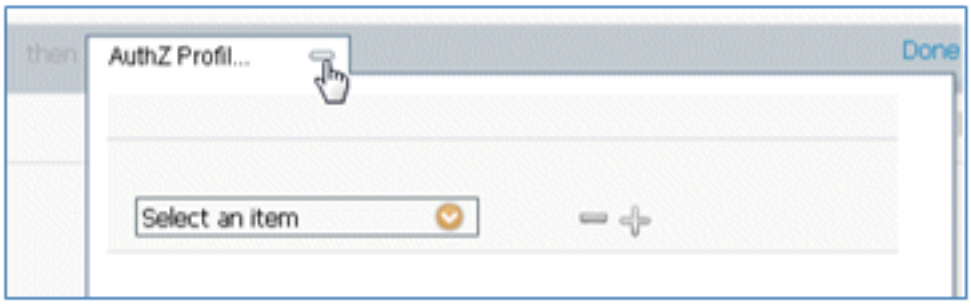


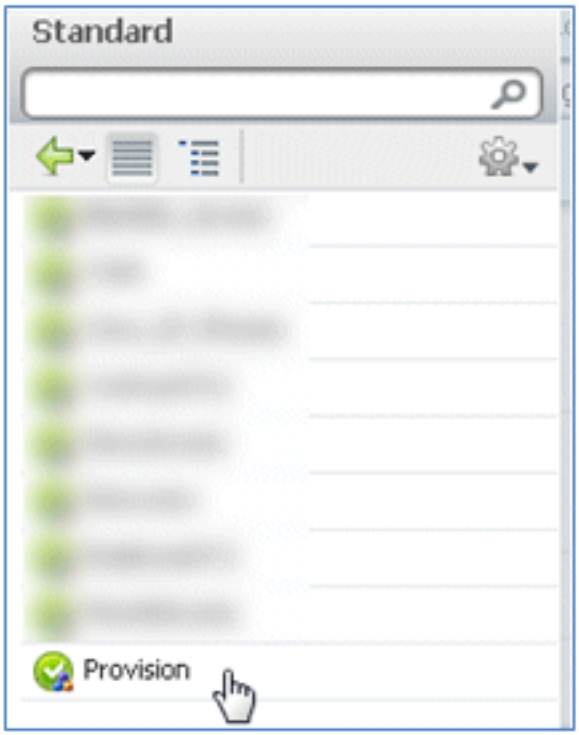
규칙의 예입니다. Condition이 AND인지 확인하십시오

.



73. AuthZ Profile(AuthZ 프로필)에서 **Standard(표준) > Provision**(프로비저닝)을 선택합니다(앞서 생성한 권한 부여 프로필).

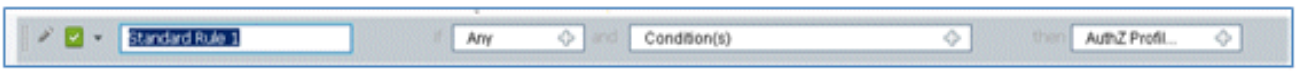




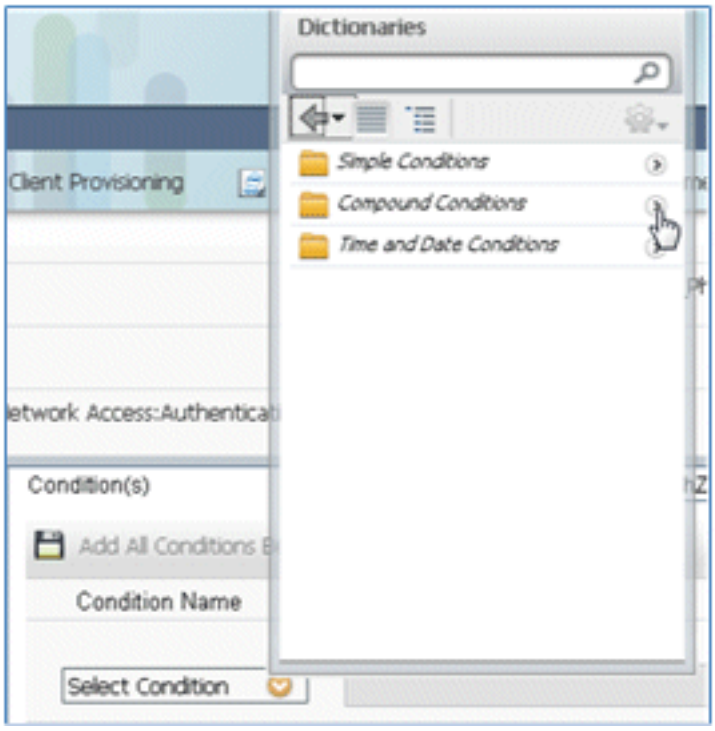
74. 완료를 **클릭합니다**.

75. PEAPrule 오른쪽의 Edit 옆에 있는 아래쪽 화살표를 클릭하고 Insert **New Rule Below**를 선택합니다.

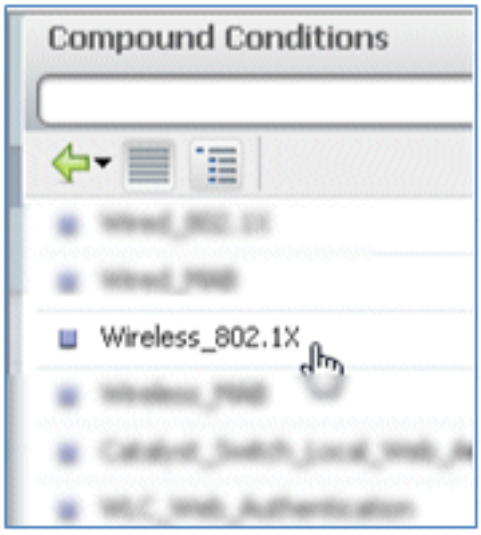
76. Rule Name(규칙 이름)을 Standard Rule #(표준 규칙 번호)에서 **AllowRule(규칙** 허용)로 변경합니다(이 예에서는). 이 규칙은 인증서가 설치된 등록된 디바이스에 대한 액세스를 허용하는 데 사용됩니다.



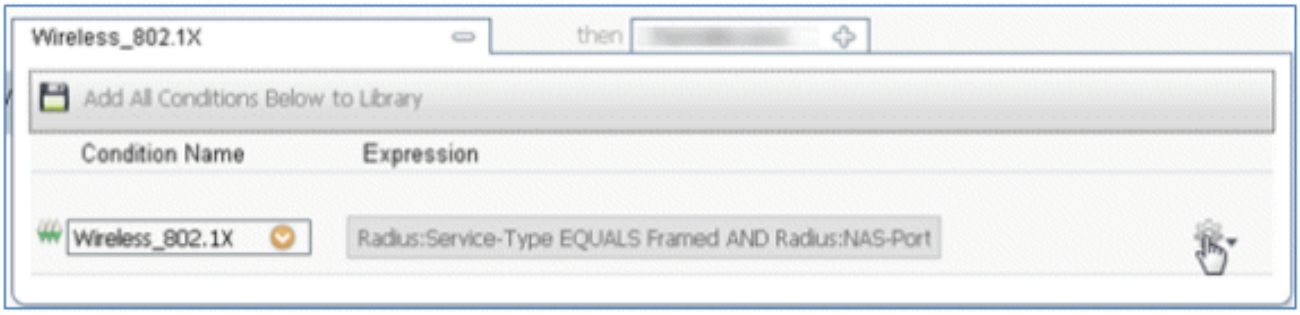
77. Condition(s)(조건)에서 Compound Conditions(복합 **조건)를 선택합니다**.



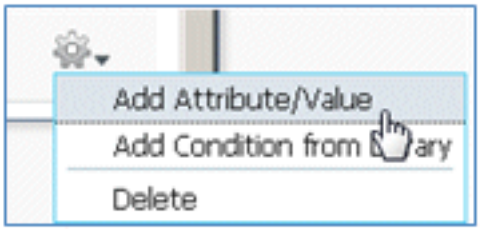
78. **Wireless_802.1X**를 선택합니다.



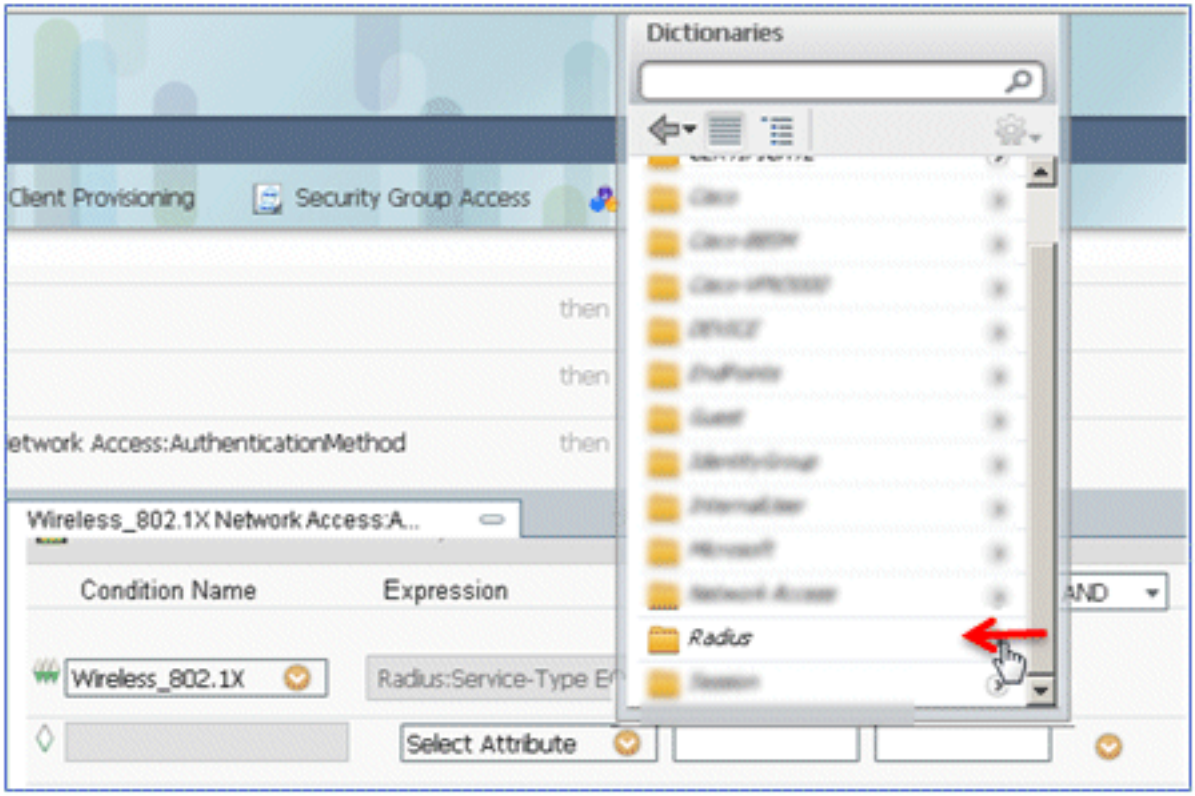
79. AND 특성을 추가합니다.



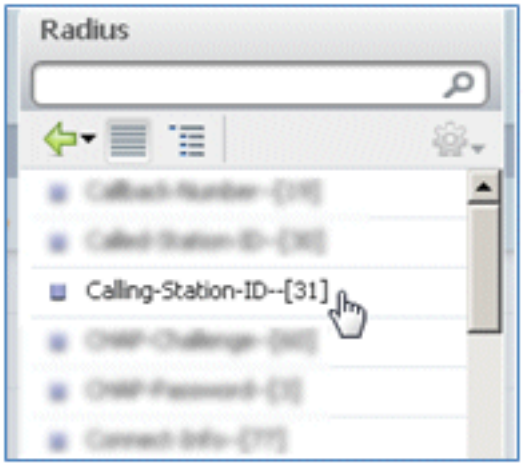
80. 조건 오른쪽의 톱니바퀴 모양 아이콘을 클릭하고 Add Attribute/**Value(특성/값 추가)**를 선택합니다.



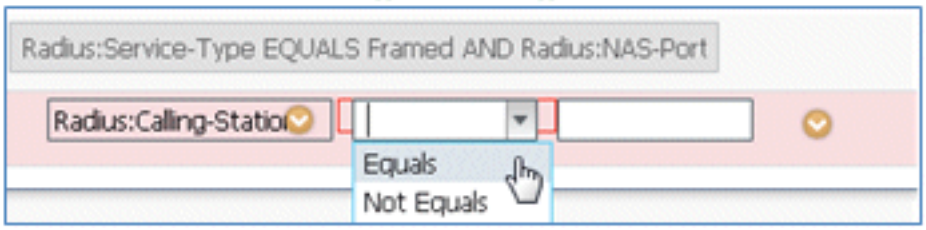
81. Radius를 찾아 **선택합니다**.



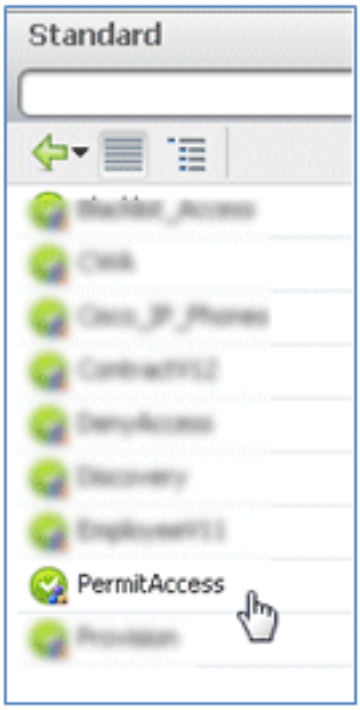
82. Calling-**Station-ID를 선택합니다—[31]**.



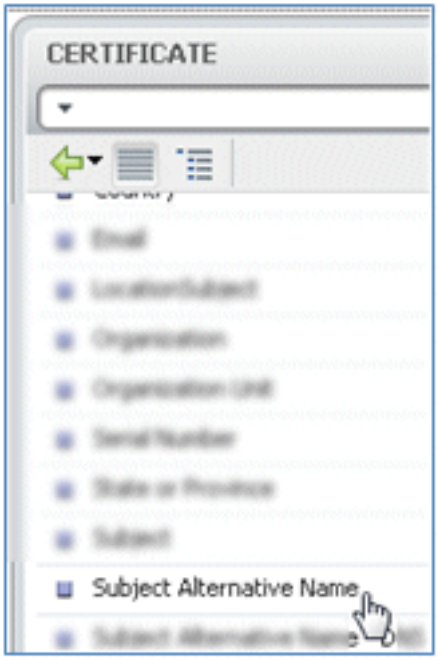
83. 같음**을 선택합니다**.



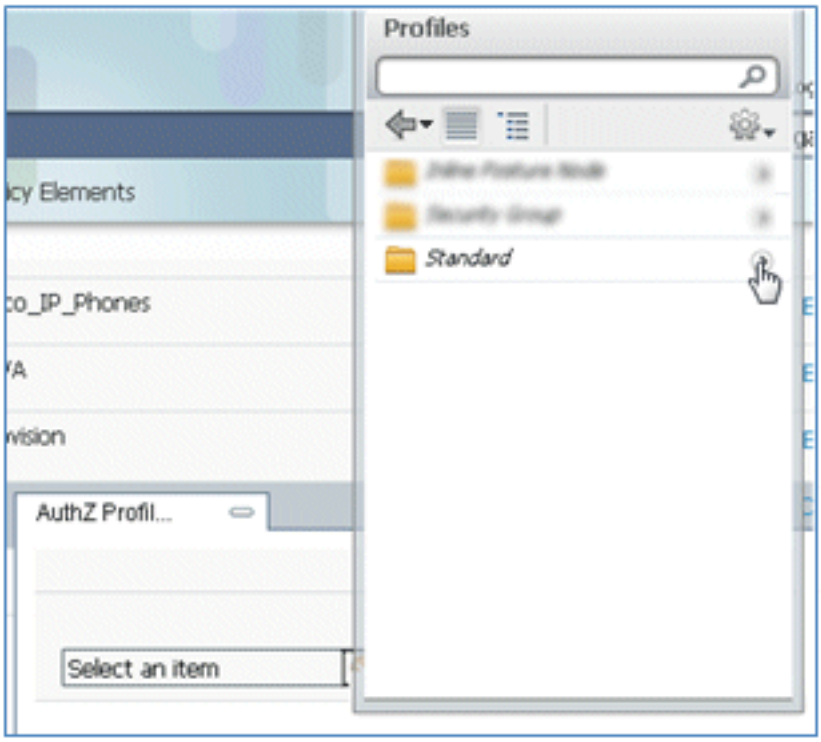
84. CERTIFICATE(**인증서**)로 이동하여 오른쪽 화살표를 클릭합니다.



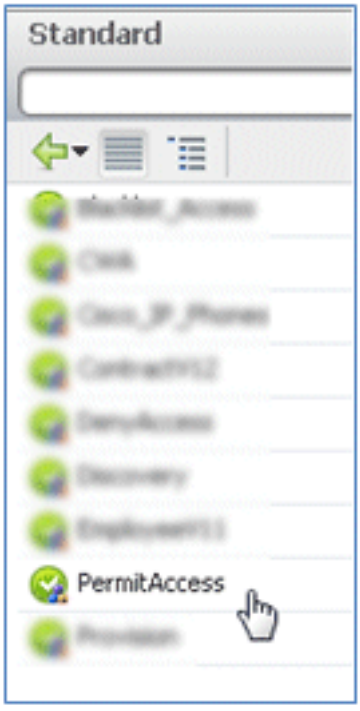
85. Subject **Alternative Name을 선택합니다**.



86. AuthZ Profile(AuthZ 프로파일)에서 Standard(표준)**를 선택합니다**.



87. Permit **Access를 선택합니다**.

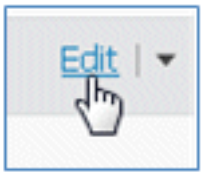


88. 완료를 **클릭합니다**.

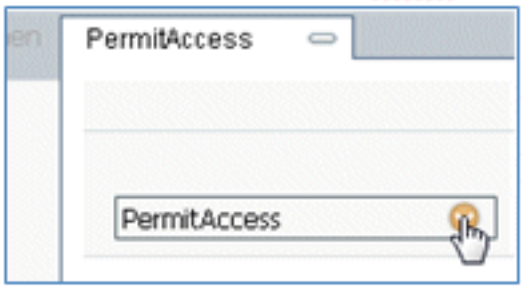
다음은 규칙의 예입니다.

89. Default 규칙을 찾아 PermitAccess를 DenyAccess로 변경합니다.

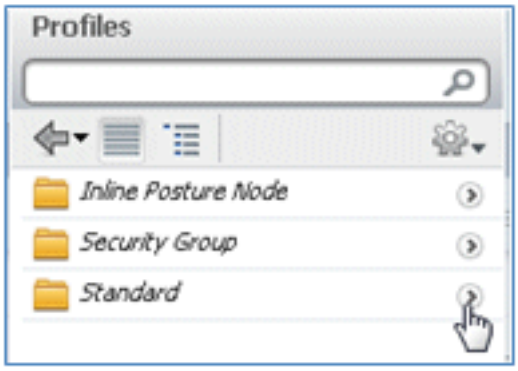
90. Default **규칙**을 수정하려면 Edit를 클릭합니다.



91. PermitAccess의 기존 AuthZ 프로필로 이동합니다.



92. 표준을 **선택합니다**.



93. DenyAccess**를 선택합니다**.

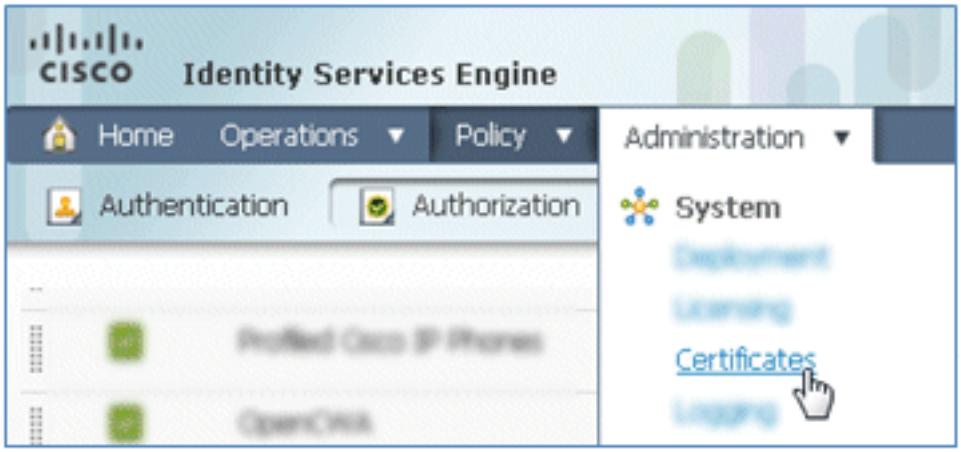
94. 일치하는 항목이 없는 경우 기본 규칙에 DenyAccess가 있는지 확인합니다.

95. 완료를 **클릭합니다**.

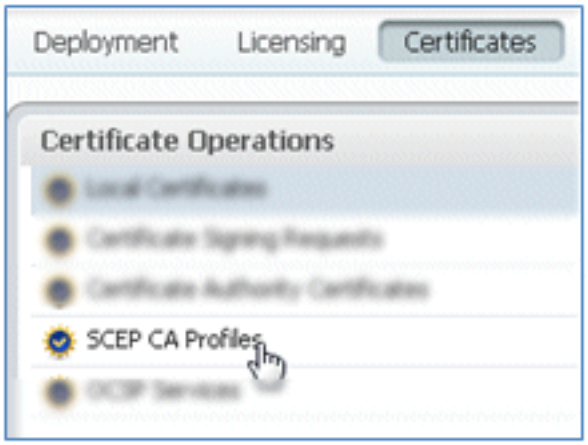
이 테스트에 필요한 기본 규칙의 예입니다. 단일 SSID 또는 이중 SSID 시나리오에 적용됩니다.

96. 저장을 **클릭합니다**.

97. SCEP 프로필로 **ISE** 서버를 구성하려면 **ISE > Administration > System > Certificates**로 이동합니다.



98. Certificate Operations(인증서 작업)에서 SCEP **CA Profiles(SCEP CA 프로필)를 클릭합니다**.



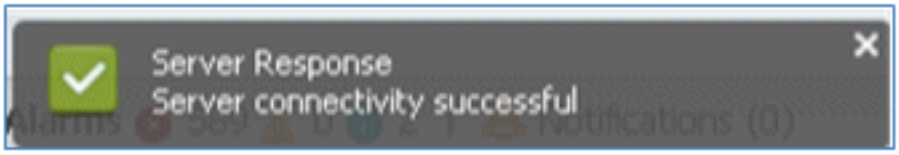
99. **Add(추가)**를 클릭합니다.

100. 이 프로파일에 대해 다음 값을 입력합니다.

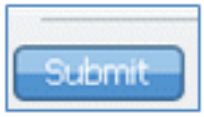
Name(이름): **mySCEP**(이 예에서는)URL: **https://*<ca-server>*/CertSrv/mscep/** (CA 서버 구성에서 올바른 주소를 확인하십시오.)

101. SCEP **연결**의 연결을 테스트하려면 Test Connectivity(연결 테스트)를 클릭합니다.

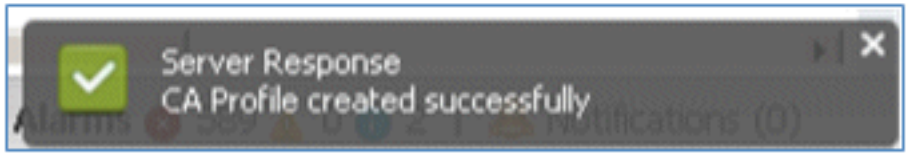
102. 이 응답은 서버 연결이 성공했음을 보여줍니다.



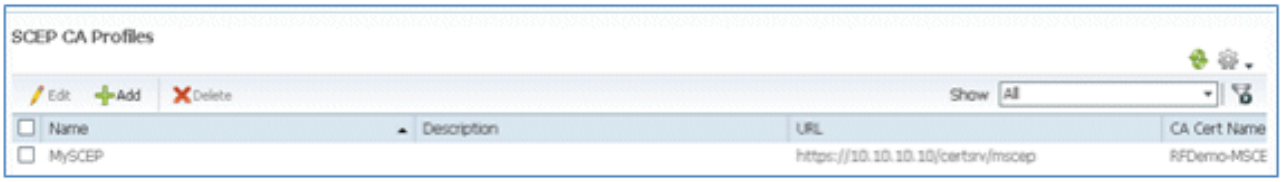
103. Submit(제출)**을 클릭합니다**.



104. 서버는 CA 프로파일이 성공적으로 생성되었다고 응답합니다.



105. SCEP CA 프로파일이 추가되었는지 확인합니다.



사용자 환경 - iOS 프로비저닝

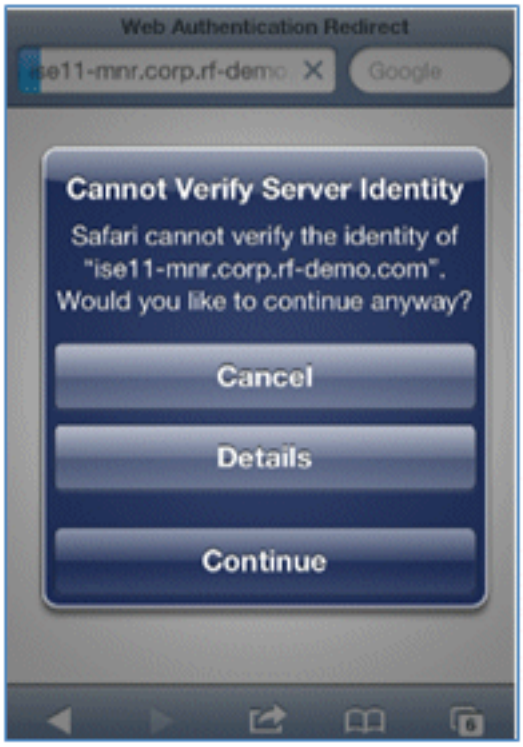
듀얼 SSID

이 섹션에서는 이중 SSID에 대해 설명하고 프로비저닝할 게스트에 연결하는 방법과 802.1x WLAN에 연결하는 방법에 대해 설명합니다.

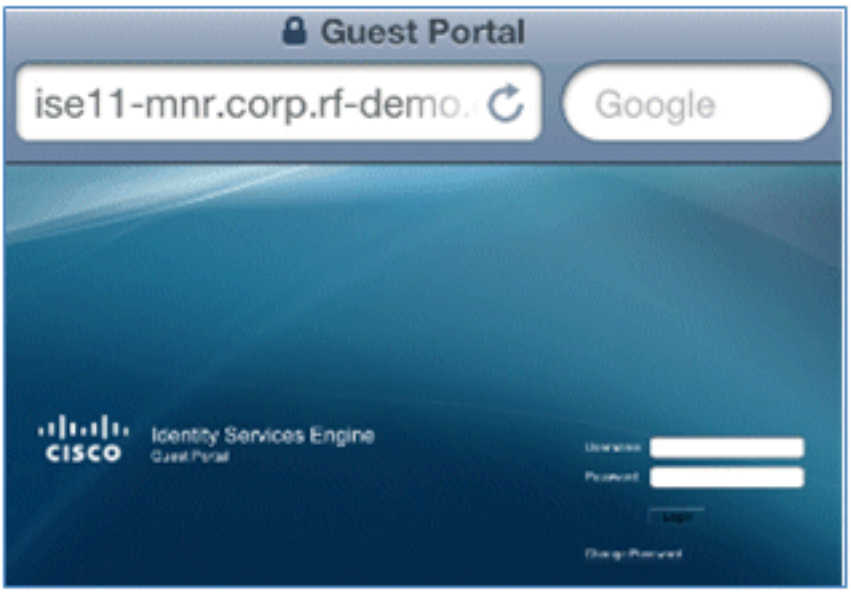
이중 SSID 시나리오에서 iOS를 프로비저닝하려면 다음 단계를 완료하십시오.

1. iOS 디바이스에서 **Wi-Fi** Networks(**Wi-Fi 네트워크)로** 이동하여 DemoCWA(**DemoCWA**)(WLC에 구성된 개방형 WLAN)를 선택합니다.

2. iOS 디바이스에서 Safari 브라우저를 열고 연결 가능한 URL(예: 내부/외부 웹 서버)을 방문합니다. ISE에서 포털로 리디렉션합니다. **Continue(계속)**를 클릭합니다.



3. 로그인을 위해 게스트 포털로 리디렉션됩니다.



4. AD 사용자 계정 및 비밀번호로 로그인합니다. 프롬프트가 표시되면 CA 프로파일을 설치합니다.

5. Install trusted certificate of the CA server(CA 서버의 신뢰할 수 있는 인증서 설치)를 **클릭합니다**.

6. 프로파일**이** 완전히 설치되면 Done을 클릭합니다.

7. 브라우저로 돌아가 Register(**등록**)를 **클릭합니다**. 디바이스의 MAC 주소가 포함된 디바이스 ID를 기록해 둡니다.

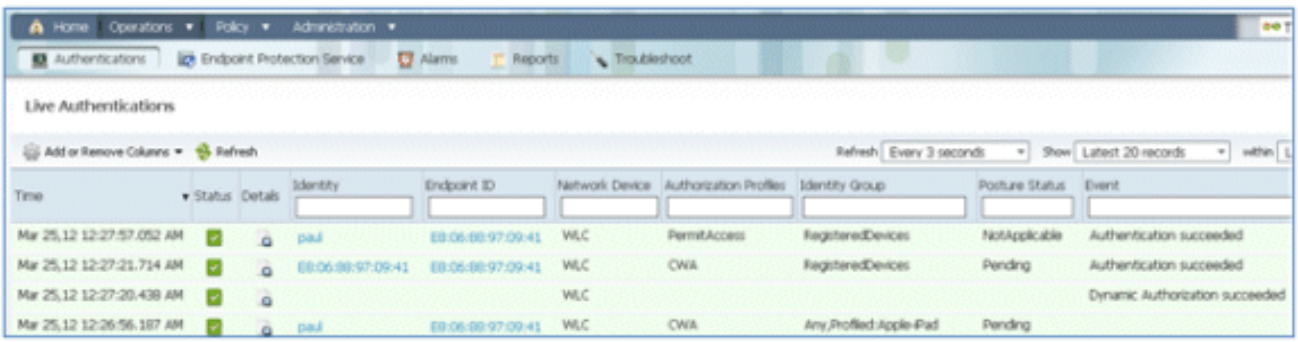
8. 확인된 **프로파일**을 설치하려면 Install(설치)을 클릭합니다.

9. Install **Now(지금 설치)를 클릭합니다**.

10. 프로세스가 완료되면 WirelessSP 프로필에서 프로필이 설치되었음을 확인합니다. 완료를 **클릭합니다**.

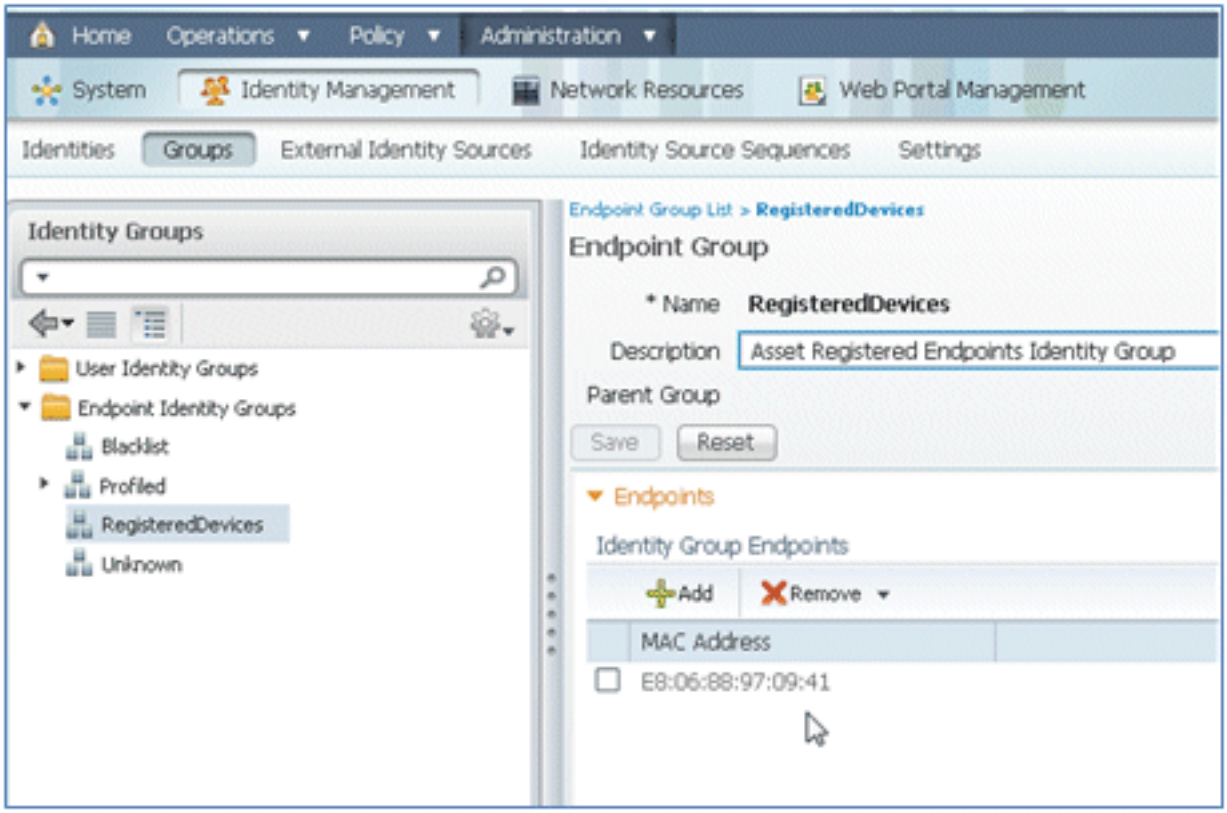
11. **Wi-Fi** Networks(**Wi-Fi 네트워크**)로 이동하여 네트워크를 Demo**1x**(**데모1x**)로 변경합니다. 디바이스가 이제 연결되어 있으며 TLS를 사용합니다.

12. ISE에서 **Operations**(운영) > Authentications(**인증)로 이동합니다**. 이 이벤트는 디바이스가 열린 게스트 네트워크에 연결되고 신청자 프로비저닝과 함께 등록 프로세스를 거치고 등록 후 액세스 허용이 허용되는 프로세스를 보여줍니다.



13. ISE > Administration(관리) > Identity Management(ID 관리) > **Groups(그룹)** > Endpoint

Identity Groups(엔드포인트 ID 그룹) > RegisteredDevices로 **이동합니다.** MAC 주소가 데이터베이스에 추가되었습니다.

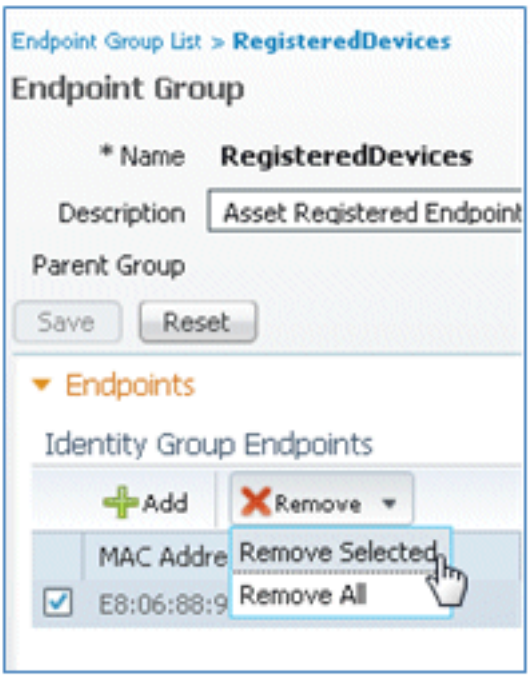


단일 SSID

이 섹션에서는 단일 SSID에 대해 설명하고 802.1x WLAN에 직접 연결하고, PEAP 인증을 위한 AD 사용자 이름/비밀번호를 제공하고, 게스트 계정을 통해 프로비저닝하고, TLS에 다시 연결하는 방법에 대해 설명합니다.

단일 SSID 시나리오에서 iOS를 프로비저닝하려면 다음 단계를 완료하십시오.

1. 동일한 iOS 디바이스를 사용하는 경우 등록된 디바이스에서 엔드포인트를 제거합니다.



2. iOS 디바이스에서 Settings(설정) > General(**일반**) > **Profiles(프로파일**)로 **이동합니다**. 이 예에 설치된 프로파일을 제거합니다.

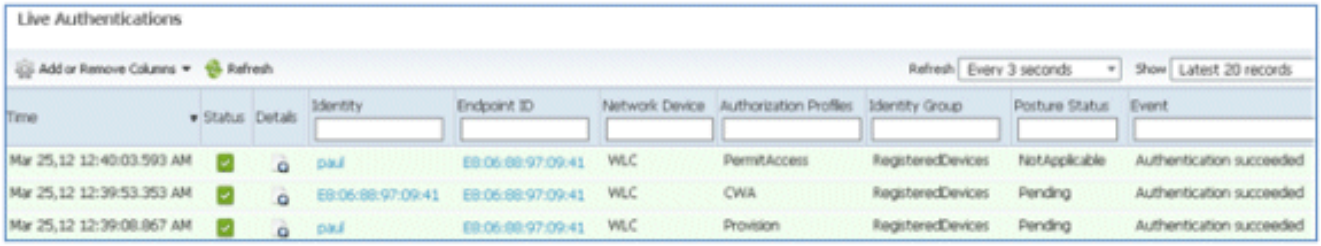
3. 이전 **프로파일**을 제거하려면 Remove(제거)를 클릭합니다.

4. 기존(지워진) 디바이스 또는 새 iOS 디바이스를 사용하여 802.1x에 직접 연결합니다.

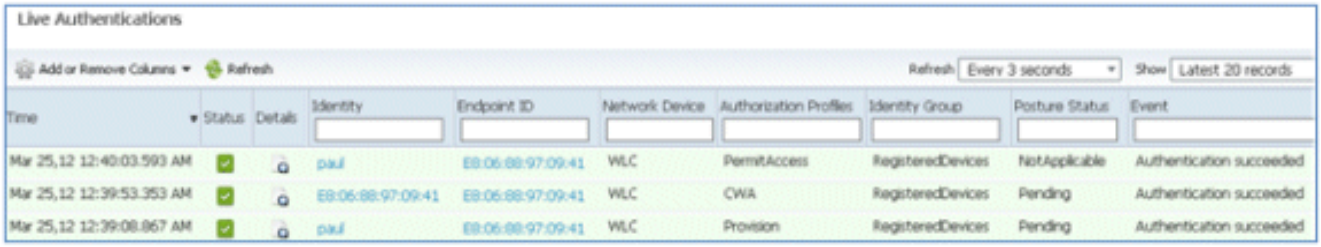
5. **Dot1x**에 연결하고 사용자 이름과 암호를 입력한 다음 Join을 **클릭합니다**.

6. 적절한 프로파일이 완전히 설치될 때까지 [ISE 컨피그레이션 섹션](#)에서 90단계 및 를 반복합니다.

7. 프로세스를 모니터링하려면 **ISE > Operations > Authentications**로 이동합니다. 이 예에서는 802.1X WLAN에 프로비저닝될 때 직접 연결되고, TLS를 사용하여 연결을 끊고, 동일한 WLAN에 다시 연결하는 클라이언트를 보여줍니다.



8. WLC > **Monitor(모니터링) > [Client MAC]으로 이동합니다**. 클라이언트 세부 정보에서 클라이언트는 RUN 상태이고, 해당 데이터 스위칭은 local로 설정되었으며, 인증은 Central이라는 점에 유의하십시오. 이는 FlexConnect AP에 연결하는 클라이언트에 적용됩니다.



사용자 환경 - Android 프로비저닝

듀얼 SSID

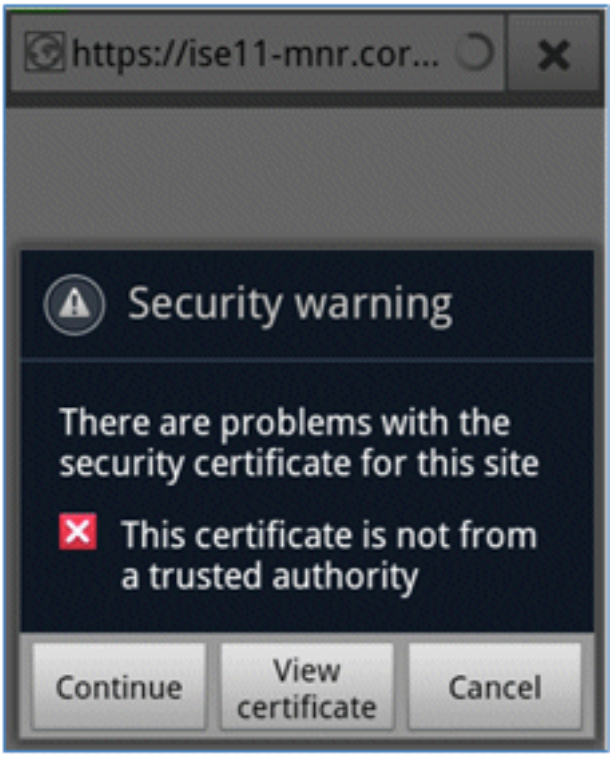
이 섹션에서는 이중 SSID에 대해 설명하고 프로비저닝할 게스트에 연결하는 방법과 802.1x WLAN에 연결하는 방법에 대해 설명합니다.

Android 디바이스의 연결 프로세스는 iOS 디바이스(단일 또는 이중 SSID)의 연결 프로세스와 매우 유사합니다. 그러나 중요한 차이점은 Android 디바이스에서 Google Marketplace(현재 Google Play)에 액세스하여 신청자 에이전트를 다운로드하려면 인터넷에 액세스해야 한다는 점입니다.

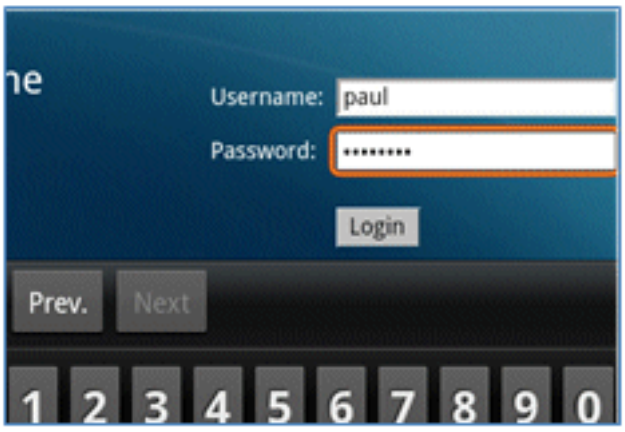
이중 SSID 시나리오에서 Android 디바이스(예: 이 예의 Samsung Galaxy)를 프로비저닝하려면 다음 단계를 완료하십시오.

1. Android 디바이스에서 Wi-Fi를 사용하여 DemoCWA에 연결하고 **게스트** WLAN을 엽니다.

2. ISE에 연결하기 위해 모든 인증서를 수락합니다.

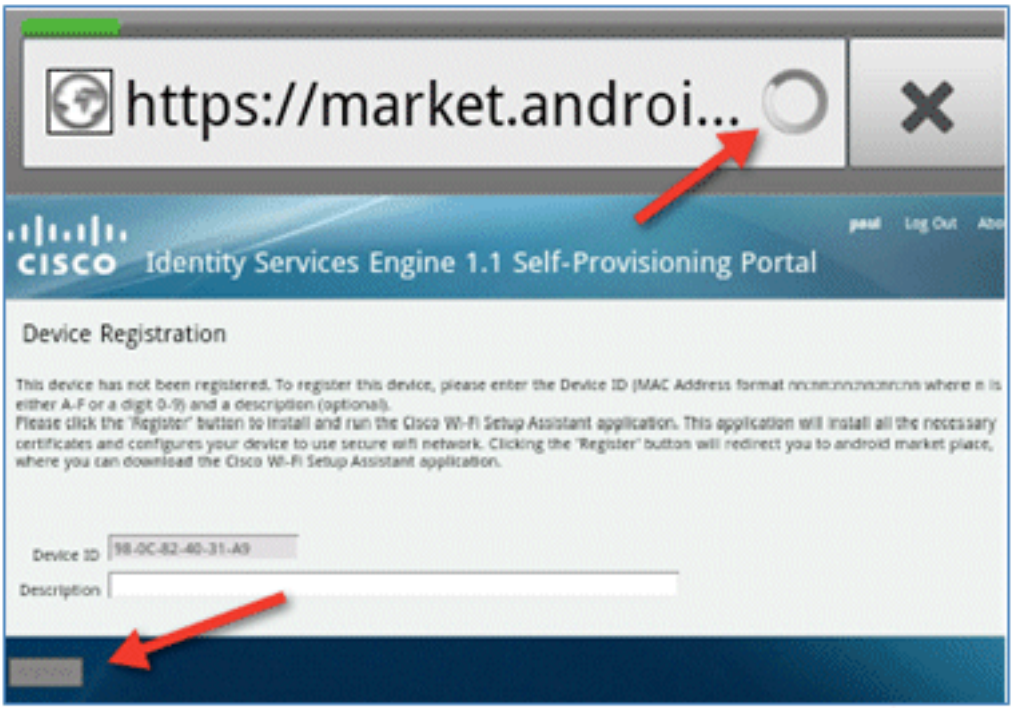


3. 게스트 포털에 로그인 하려면 사용자 이름 및 암호를 입력 합니다.

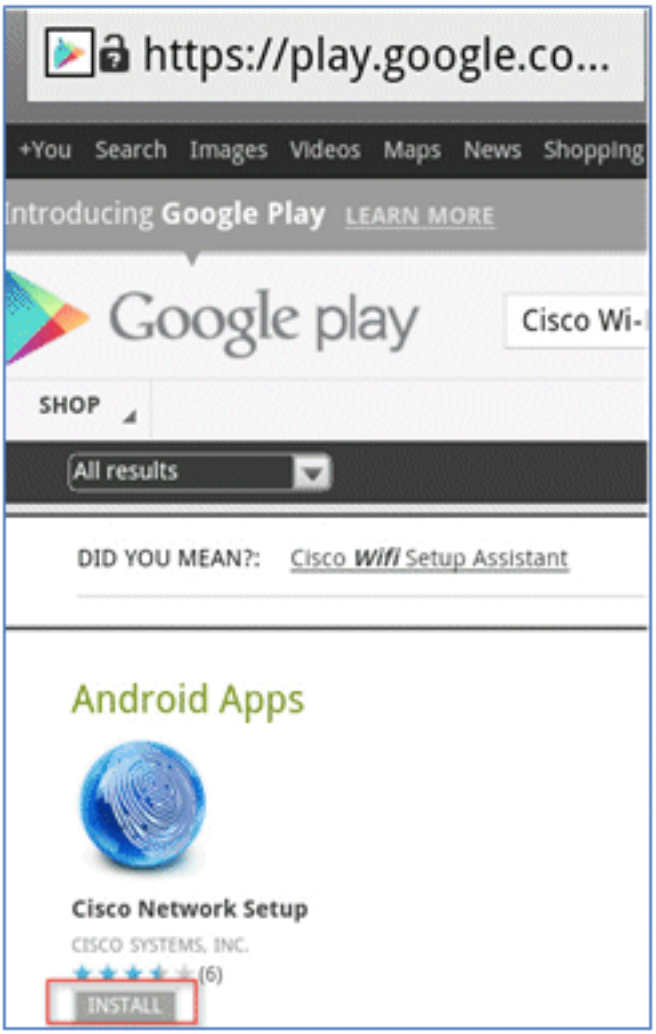


4. Register(등록)**를 클릭합니다**. 장치는 Google Marketplace에 액세스하기 위해 인터넷에 연결

하려고 시도합니다. 인터넷 액세스를 허용하기 위해 컨트롤러의 사전 인증 ACL(예: ACL-REDIRECT)에 추가 규칙을 추가합니다.

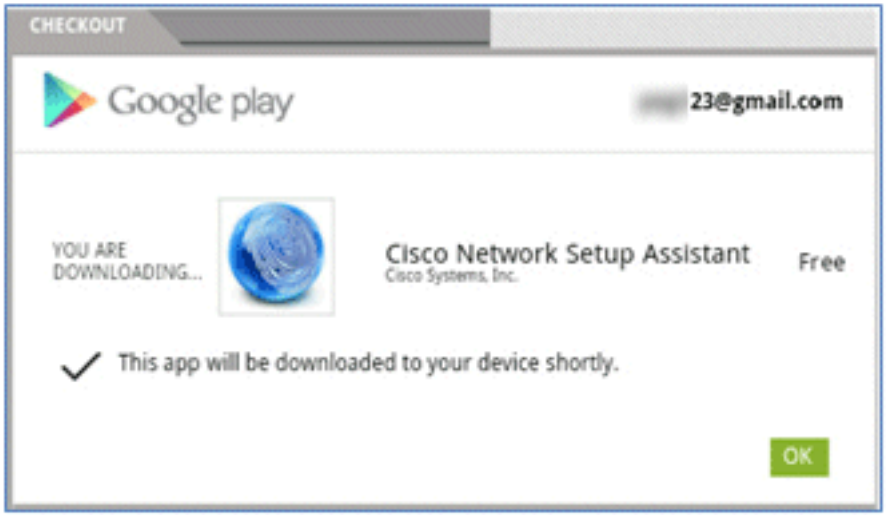


5. Google은 Cisco Network Setup을 Android 앱으로 나열합니다. Install(설치)**을 클릭합니다**.

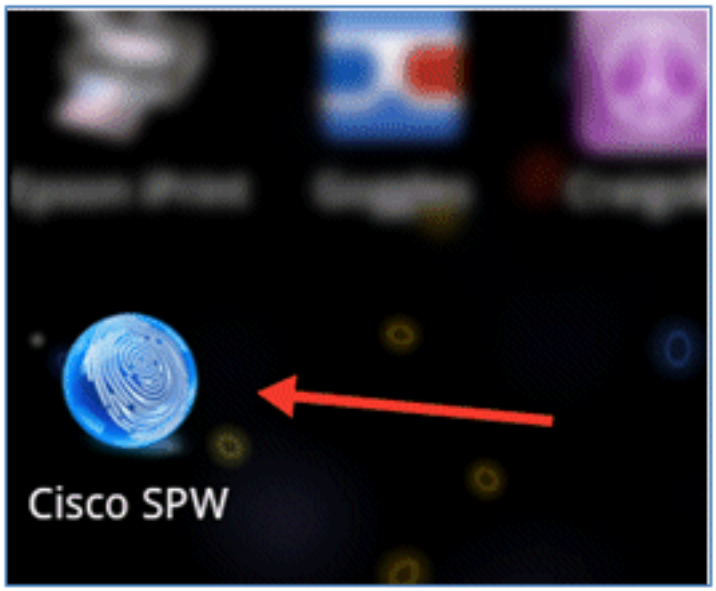


6. Google에 로그인하고 INSTALL을 **클릭합니다**.

7. **OK(확인)**를 클릭합니다.



8. Android 디바이스에서 설치된 **Cisco SPW 앱**을 찾아 엽니다.



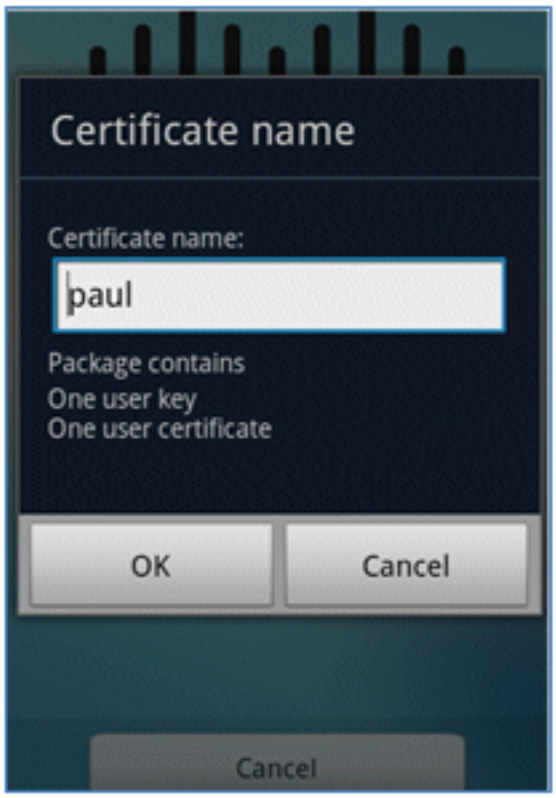
9. Android 디바이스에서 게스트 포털에 계속 로그인되어 있는지 확인합니다.

10. Wi-Fi Setup Assistant를 시작하려면 **시작** 을 클릭합니다.

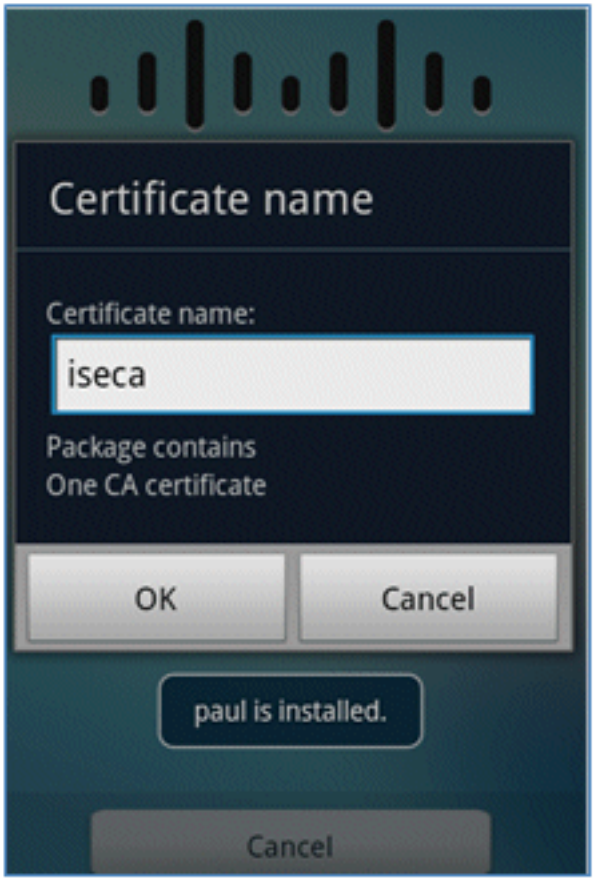
11. Cisco SPW에서 인증서 설치를 시작합니다.

12. 프롬프트가 표시되면 자격 증명 저장을 위한 비밀번호를 설정합니다.

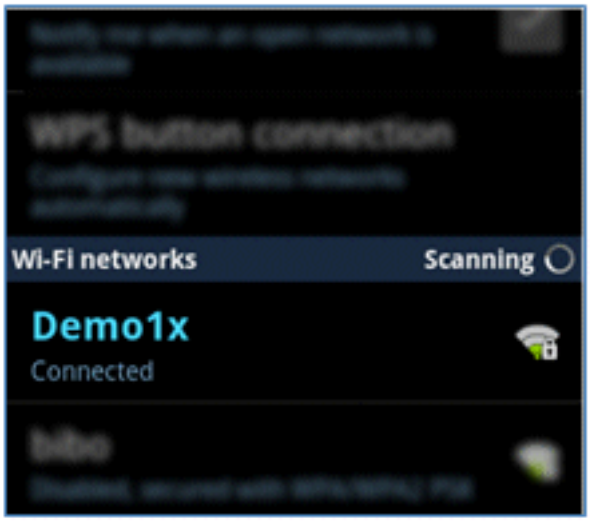
13. Cisco SPW는 사용자 키 및 사용자 인증서가 포함된 인증서 이름으로 반환됩니다. OK(**확인**)를 클릭하여 확인합니다.



14. Cisco SPW는 CA 인증서가 포함된 다른 인증서 이름을 계속 입력하라는 메시지를 표시합니다. 이 예에서 **이름** iseca를 입력한 다음 **OK(확인)**를 클릭하여 계속합니다.



15. 이제 Android 장치가 연결되었습니다.

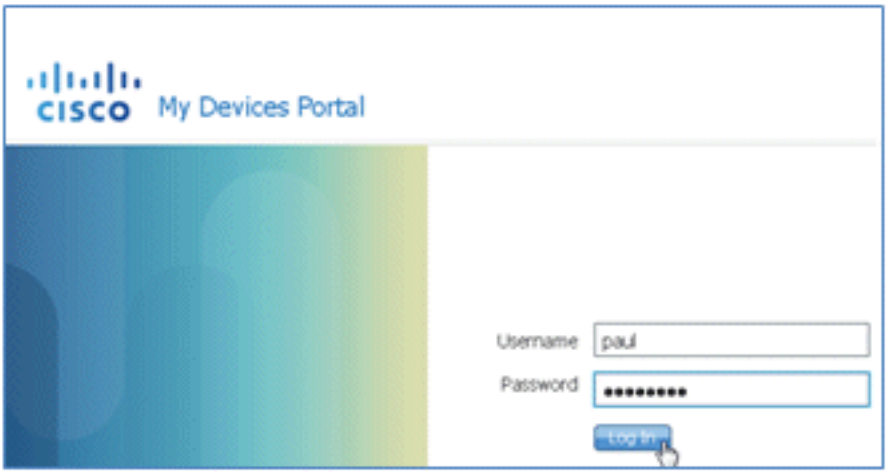


내 디바이스 포털

My Devices Portal(내 디바이스 포털)에서는 디바이스를 분실하거나 도난당한 경우 사용자가 이전에 등록된 디바이스를 블랙리스트에 추가할 수 있습니다. 또한 필요한 경우 다시 등록할 수 있습니다.

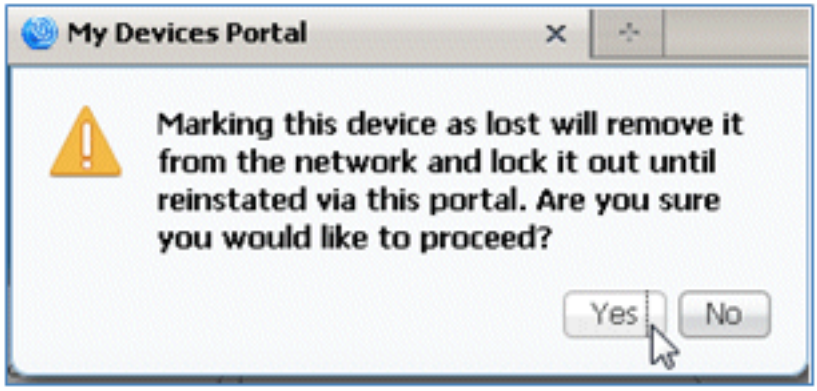
디바이스를 블랙리스트에 추가하려면 다음 단계를 완료하십시오.

1. My Devices Portal(내 디바이스 포털)에 로그인하려면 브라우저를 열고 https://ise-server:8443/mydevices(포트 번호 8443 참고)에 연결한 다음 AD 계정으로 로그인합니다.



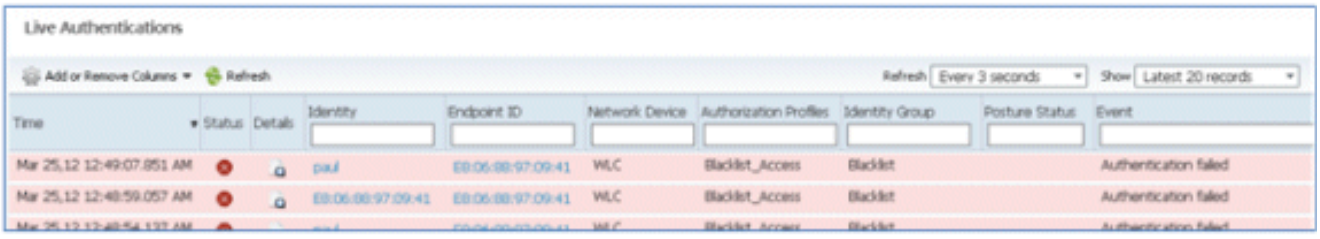
2. Device ID(디바이스 ID)에서 디바이스를 찾고 Lost(**분실**)를 클릭하여 디바이스의 블랙리스트 작성을 시작합니다.

3. ISE에서 경고 메시지가 표시되면 **Yes(예)**를 클릭하여 계속 진행합니다.

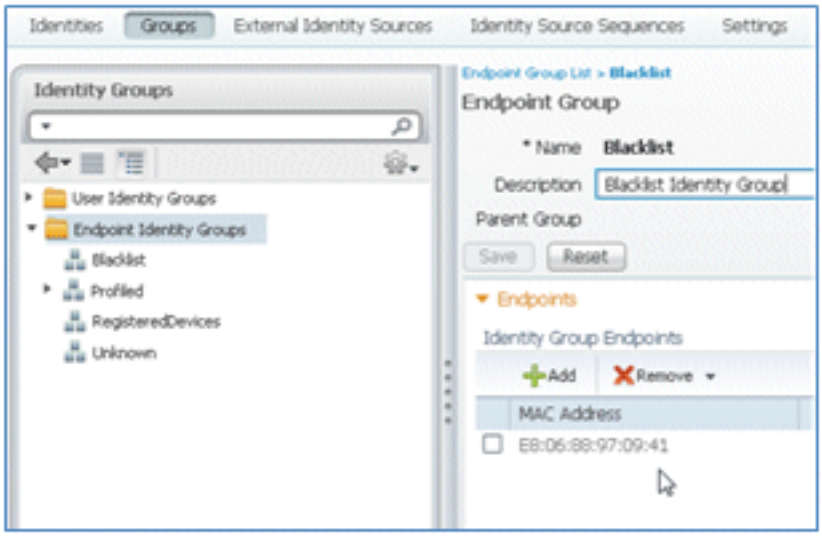


4. ISE에서 디바이스가 **lost(분실)**로 표시되었음을 **확인합니다**.

5. 이전에 등록된 디바이스로 네트워크에 연결하려는 시도는 이제 유효한 인증서가 설치된 경우에도 차단됩니다. 다음은 인증에 실패한 블랙리스트 디바이스의 예입니다.



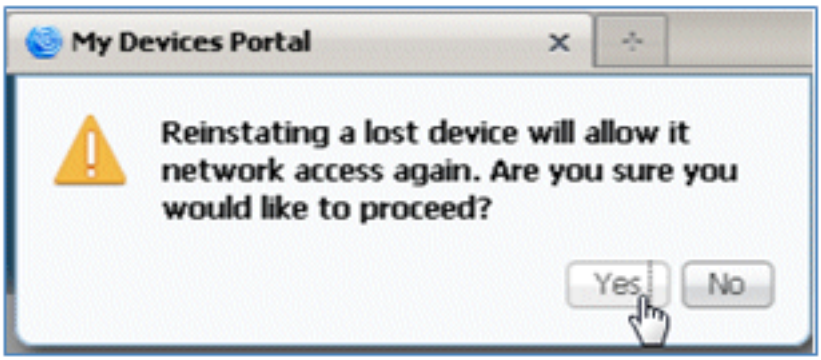
6. 관리자는 ISE > Administration(관리) > Identity Management(ID 관리) > **Groups(그룹)로** 이동하고 **Endpoint Identity Groups(엔드포인트 ID 그룹)** > Blacklist(블랙리스트)를 클릭한 다음 디바이스**가 블랙리스트에 추가되었는지 확인할** 수 **있습니다.**



블랙리스트 디바이스를 복구하려면 다음 단계를 완료하십시오.

1. My Devices Portal(내 디바이스 포털)에서 해당 **디바이스**에 대해 Reinstate(복원)를 클릭합니다.

2. ISE에서 경고 메시지가 표시되면 **Yes(예)**를 클릭하여 계속 진행합니다.



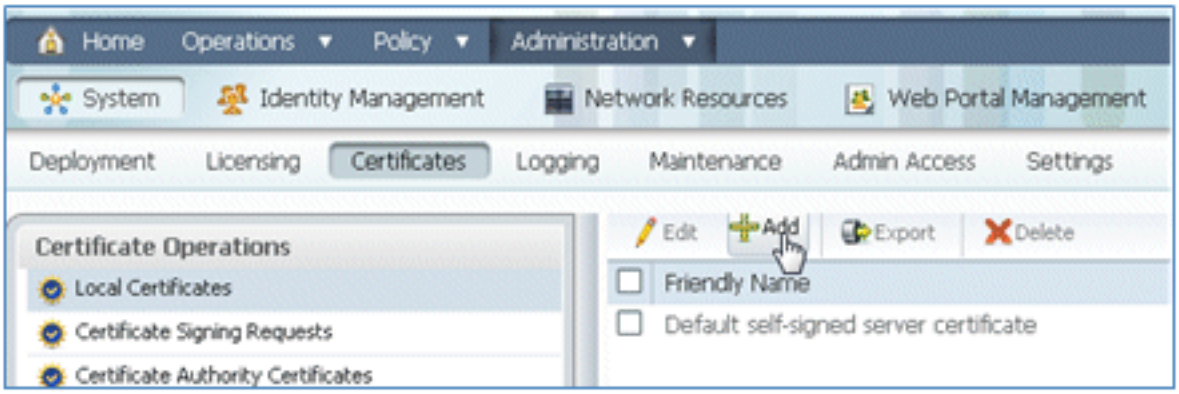
3. ISE에서 디바이스가 성공적으로 복원되었음을 확인합니다. 디바이스를 허용할지 테스트하기 위해 복구된 디바이스를 네트워크에 연결합니다.

참조 - 인증서

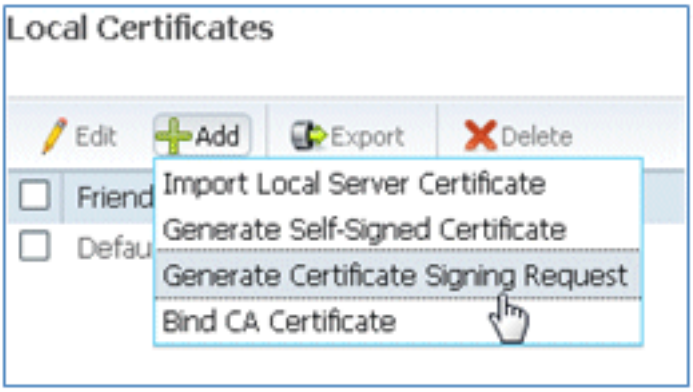
ISE에는 유효한 CA 루트 인증서가 필요할 뿐 아니라 CA에서 서명한 유효한 인증서도 필요합니다.

신뢰할 수 있는 새 CA 인증서를 추가, 바인딩 및 가져오려면 다음 단계를 완료하십시오.

1. ISE > Administration(관리) > System(시스템) > **Certificates(인증서)로** 이동하고 **Local Certificates(로컬 인증서)**를 클릭한 다음 Add(추가)를 **클릭합니다.**

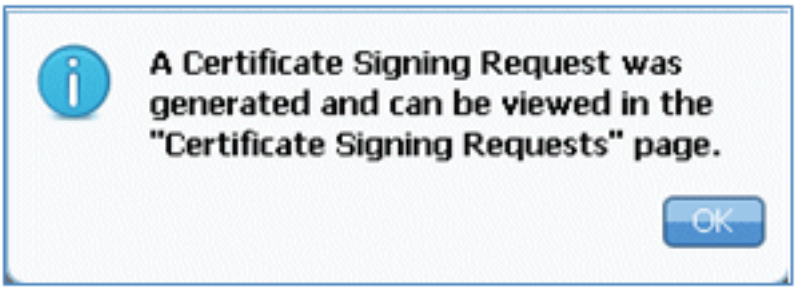


2. Generate **Certificate Signing Request** (CSR)(CSR 생성)를 선택합니다.

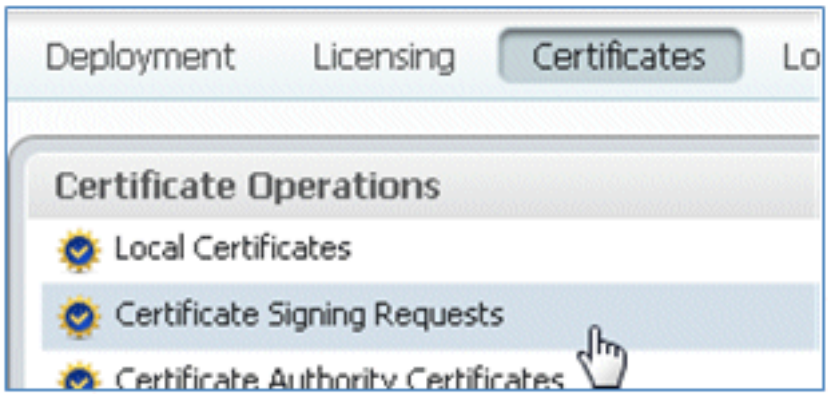


3. 인증서 주체 **CN=<*ISE-SERVER hostname.FQDN*>*을 입력합니다*.** 다른 필드에서는 기본값 또는 CA 설정에 필요한 값을 사용할 수 있습니다. Submit(제출)**을 클릭합니다**.

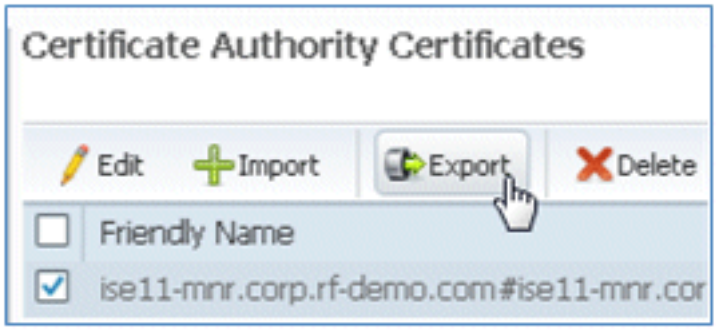
4. ISE는 CSR이 생성되었는지 확인합니다.



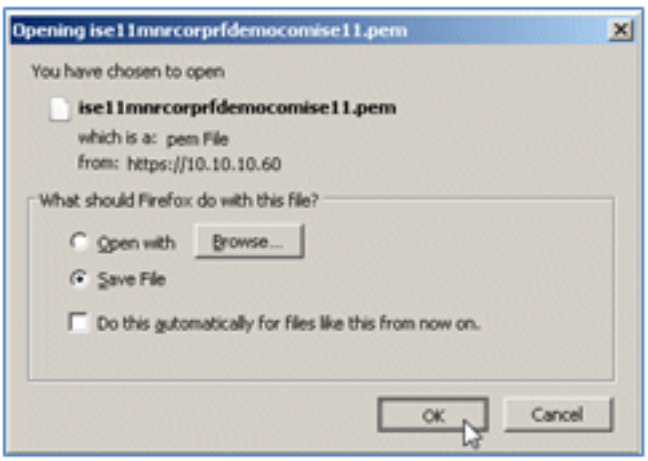
5. CSR에 액세스하려면 Certificate Signing Requests(**인증서 서명 요청) 작업**을 클릭합니다.



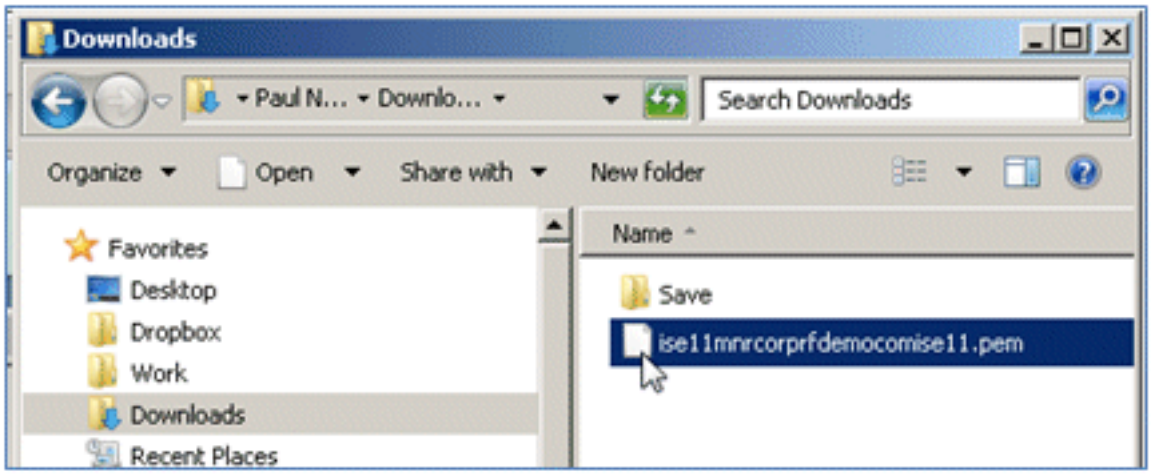
6. 최근 생성된 CSR을 선택한 다음 Export(내보내기)**를 클릭합니다**.



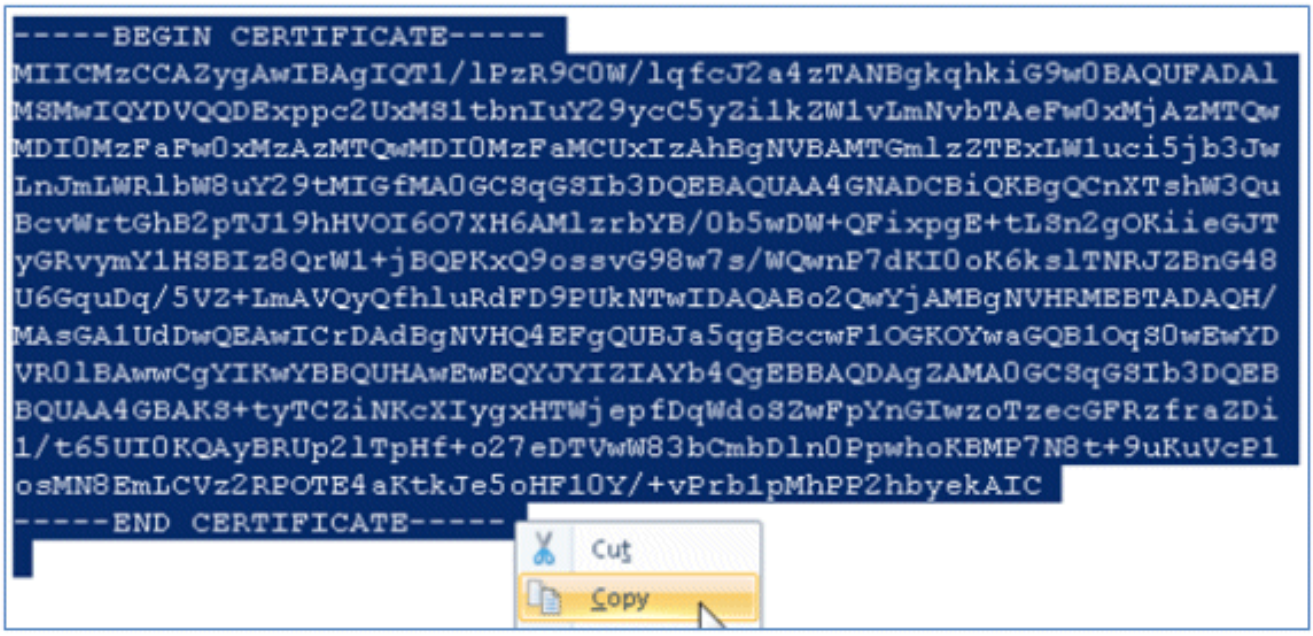
7. ISE는 CSR을 .pem 파일로 내보냅니다. 파일 **저장**을 클릭한 다음 **확인**을 클릭하여 로컬 시스템에 파일을 저장합니다.



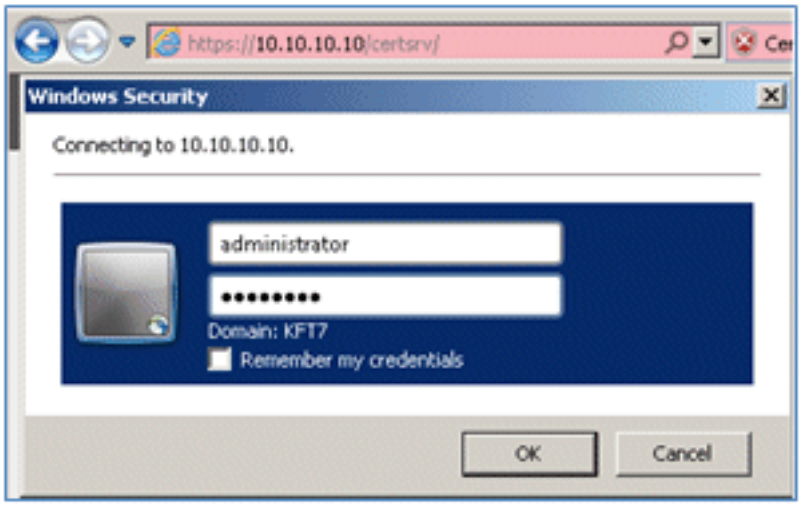
8. 텍스트 편집기를 사용하여 ISE 인증서 파일을 찾아 엽니다.



9. 인증서의 전체 내용을 복사합니다.

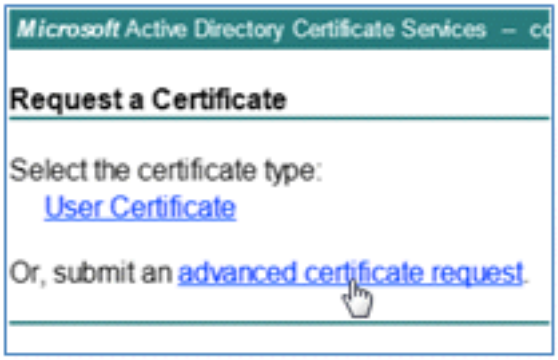


10. CA 서버에 연결하고 관리자 계정으로 로그인합니다. 서버는 Microsoft 2008 CA(https://10.10.10.10/certsrv)입니다(이 예에서는).

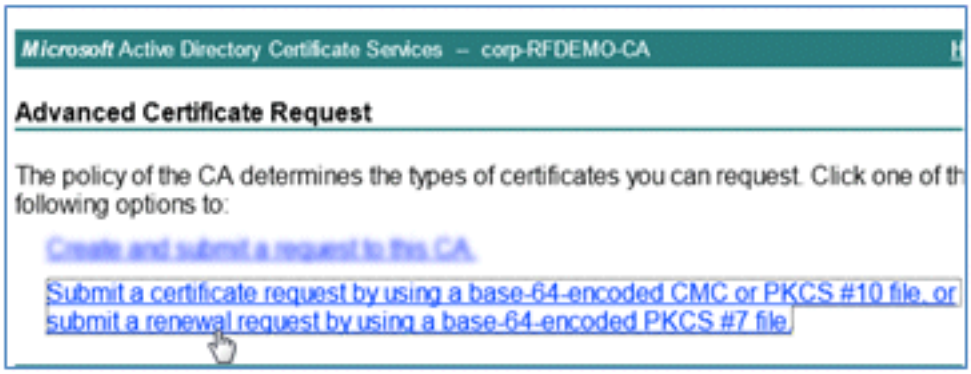


11. Request **a certificate(인증서 요청)를 클릭합니다**.

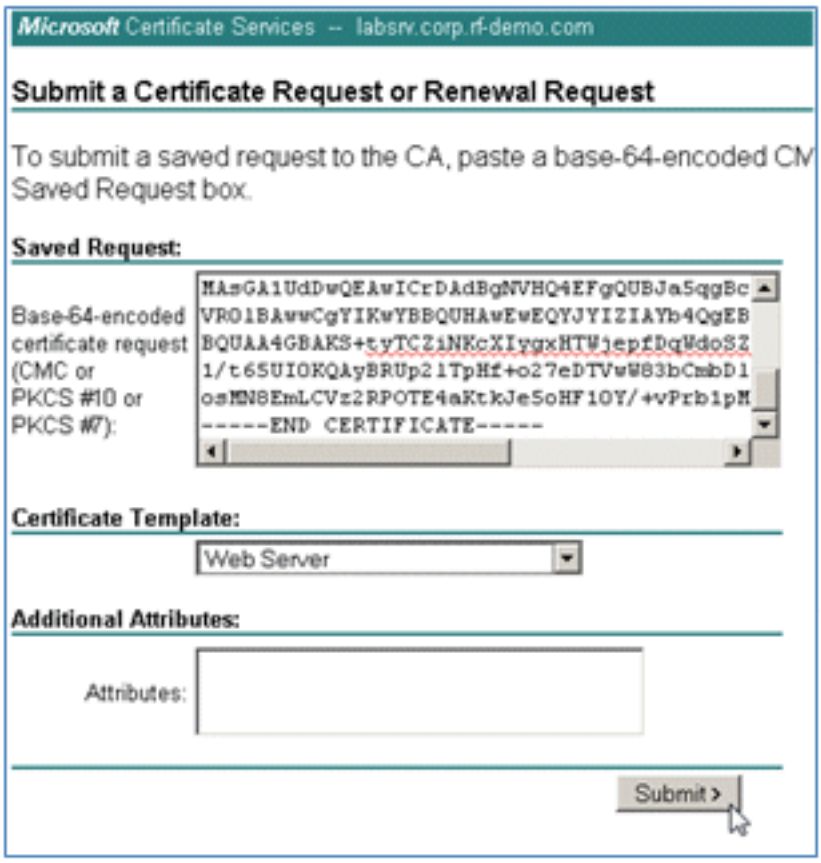
12. **고급 인증서 요청**을 **클릭합니다**.



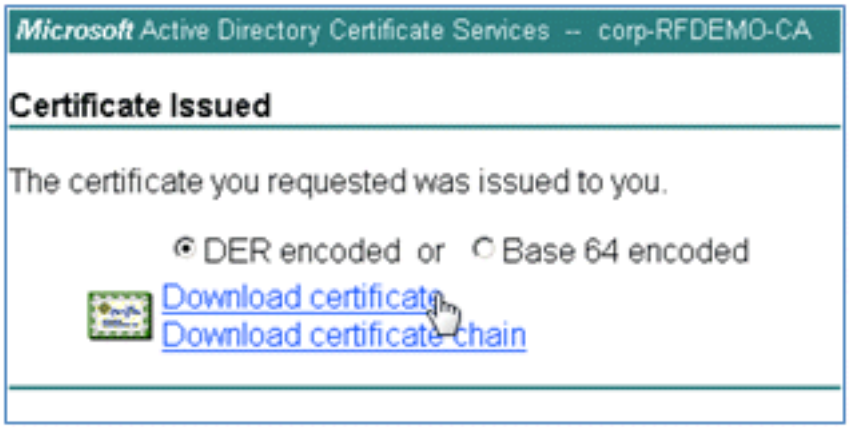
13. 두 번째 옵션을 클릭하여 **Base64 인코딩 CMC 또는 ...** .



14. ISE 인증서 파일(.pem)의 내용을 Saved Request(저장된 요청) 필드에 붙여넣고, 인증서 템플릿이 **웹 서버인지** 확인하고, Submit(제출)을 **클릭합니다**.

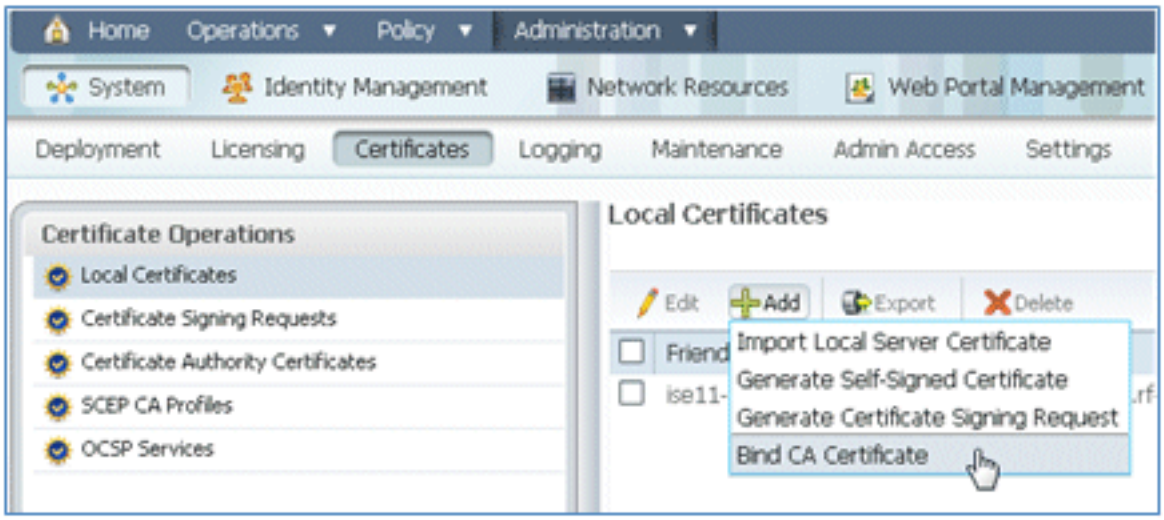


15. Download certificate(**인증서 다운로드)를 클릭합니다**.

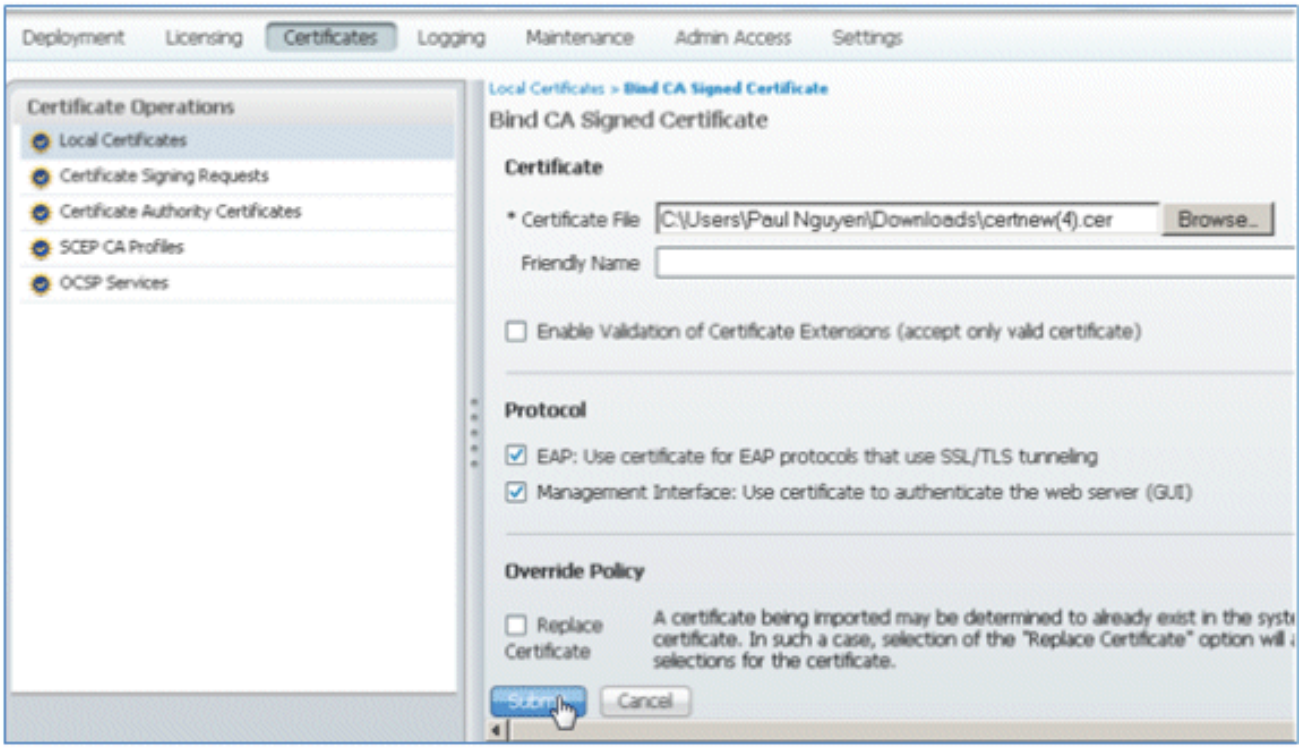


16. certnew.cer 파일을 저장합니다. 나중에 ISE와 바인딩하는 데 사용됩니다.

17. ISE Certificates(ISE **인증서)**에서 Local Certificates(**로컬 인증서)**로 이동하고 Add(추가) > Bind CA Certificate(**CA 인증서 바인딩)를** 클릭합니다.



18. 이전 단계에서 로컬 시스템에 저장된 인증서를 찾아 EAP와 **관리 인터페이스 프로토콜**을 모두 활성화하고(상자가 선택됨) **Submit(제출)**을 클릭합니다. ISE에서 서비스를 다시 시작하는 데 몇 분 이상 걸릴 수 있습니다.

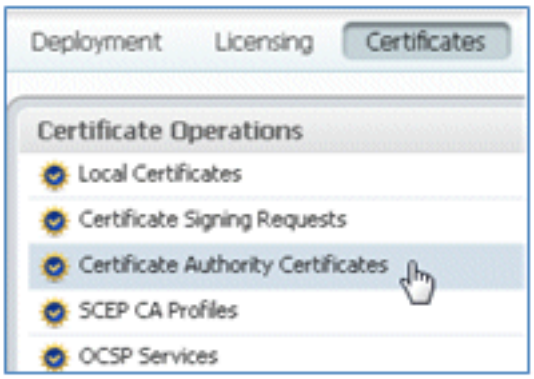


19. CA의 랜딩 페이지(https://CA/certsrv/)로 돌아가 **Download a CA certificate, certificate chain 또는 CRL을 클릭합니다**.

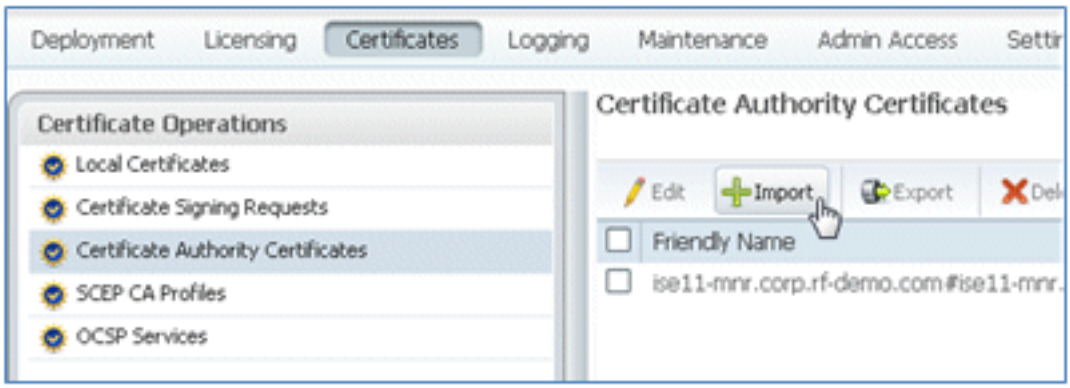
20. Download **CA certificate(CA 인증서 다운로드)를 클릭합니다**.

21. **파일**을 로컬 시스템에 저장합니다.

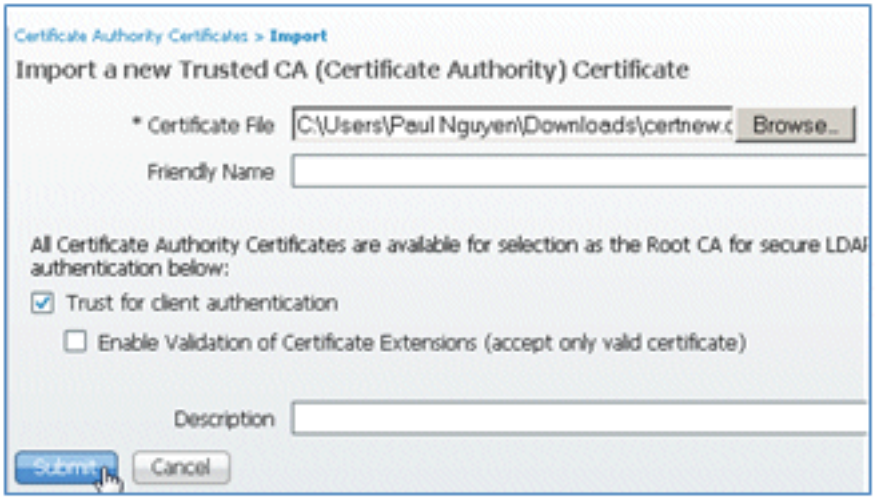
22. ISE 서버를 온라인으로 설정한 상태에서 Certificates(**인증서**)로 이동하여 **Certificate Authority Certificates(인증 기관 인증서)**를 클릭합니다.



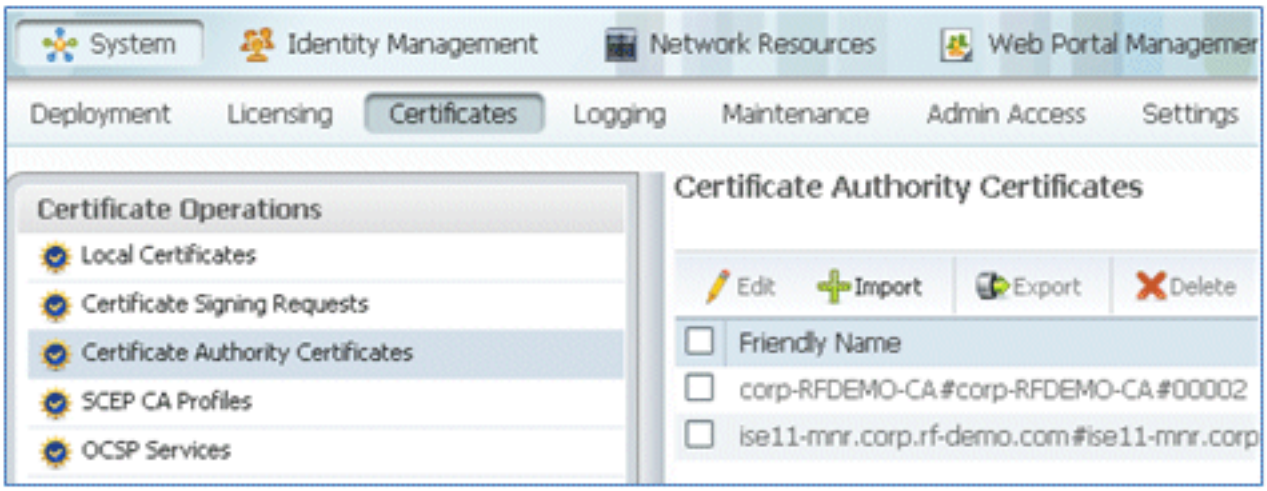
23. **Import(가져오기)**를 클릭합니다.



24. CA 인증서를 찾아 **클라이언트** 인증을 **위한 Trust를 활성화하고**(상자가 선택됨) Submit을 **클릭합니다**.



25. 신뢰할 수 있는 새 CA 인증서가 추가되었는지 확인합니다.



관련 정보

- Cisco Identity Services Engine 하드웨어 설치 설명서, 릴리스 1.0.4
- Cisco 2000 Series Wireless LAN Controller
- Cisco 4400 Series Wireless LAN Controller
- Cisco Aironet 3500 Series
- Flex 7500 Wireless Branch Controller 구축 설명서
- Bring Your Own Device - 통합 디바이스 인증 및 일관된 액세스 환경
- Identity Services Engine을 사용하는 무선 BYOD
- 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.