WLAN별 ACS 버전 5.2 및 WLC 인증 컨피그레이션 예

목차

소개

이 문서에서는 SSID(Service Set Identifier)를 기반으로 사용자별로 무선 LAN(WLAN)에 대한 액세스를 제한하는 컨피그레이션 예를 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 작동을 위해 WLC(Wireless LAN Controller) 및 LAP(Lightweight Access Point)를 구성하는 방법
- Cisco ACS(Secure Access Control Server)를 구성하는 방법
- LWAPP(Lightweight Access Point Protocol) 및 무선 보안 방법

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 버전 7.4.110을 실행하는 Cisco 5500 Series WLC
- Cisco 1142 Series LAP
- Cisco Secure ACS Server 버전 5.2.0.26.11

구성

이 설정에 대한 디바이스를 구성하려면 다음을 수행해야 합니다.

1. 두 WLAN 및 RADIUS 서버에 대한 WLC를 구성합니다.

2. Cisco Secure ACS를 구성합니다.
3. 무선 클라이언트를 구성하고 구성을 확인합니다.

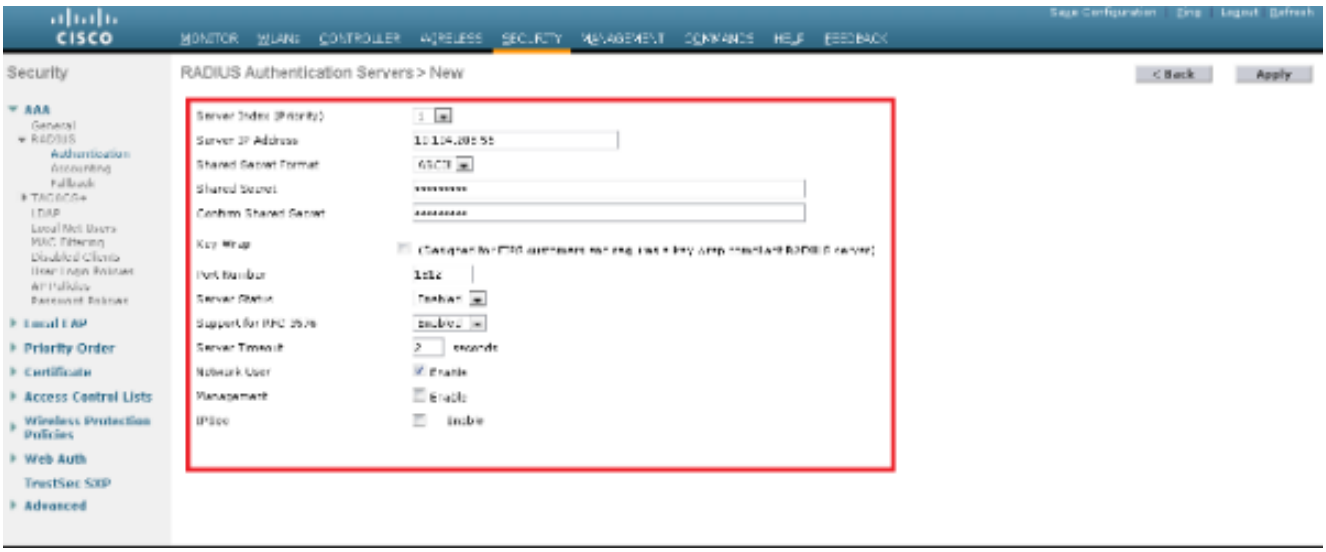
WLC 구성

이 설정에 대한 WLC를 구성하려면 다음 단계를 완료합니다.

1. 사용자 자격 증명을 외부 RADIUS 서버로 전달하도록 WLC를 구성합니다.그런 다음 외부 RADIUS 서버(이 경우 Cisco Secure ACS)에서 사용자 자격 증명을 검증하고 무선 클라이언트에 대한 액세스를 제공합니다.다음 단계를 완료하십시오. RADIUS **Authentication** Servers 페이지를 표시하려면 컨트롤러 GUI에서 Security > RADIUS Authentication을 선택합니다.

RADIUS 서버 매개변수를 정의하려면 New(새로 만들기)를 클릭합니다. 이러한 매개변수에는 RADIUS 서버 IP 주소, 공유 암호, 포트 번호 및 서버 상태가 포함됩니다.Network User and Management(네트워크 사용자 및 관리) 확인란은 RADIUS 기반 인증이 관리 및 네트워크 사용자에게 적용되는지 결정합니다.이 예에서는 Cisco Secure ACS를 IP 주소가 10.104.208.56인 RADIUS 서버로 사용합니다

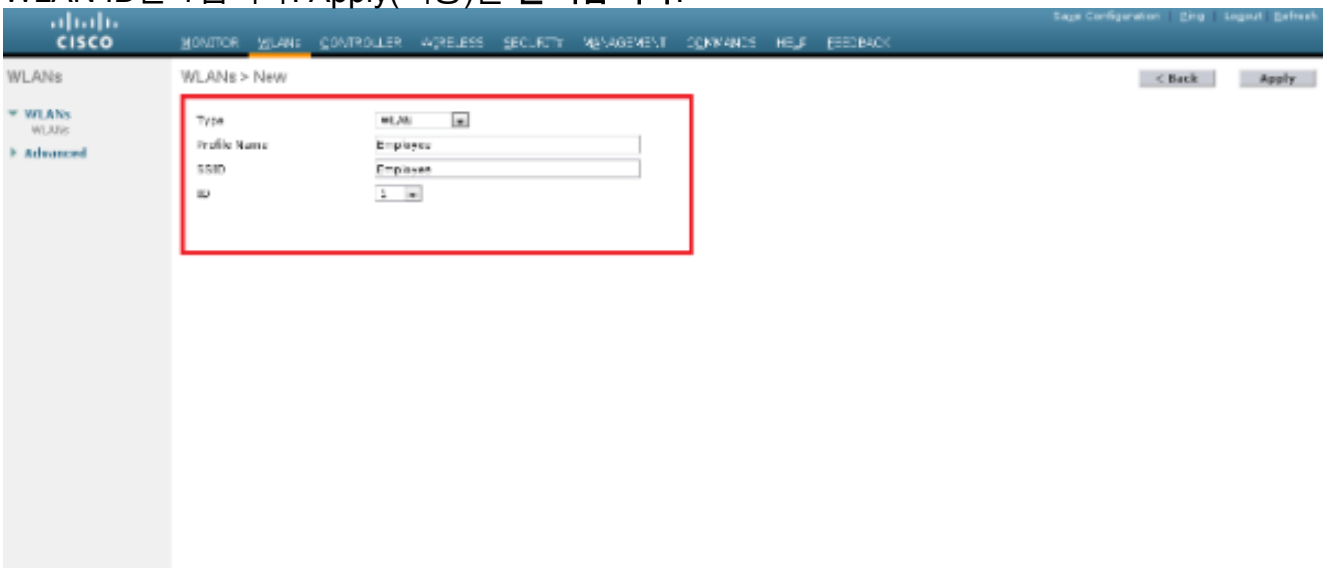
.



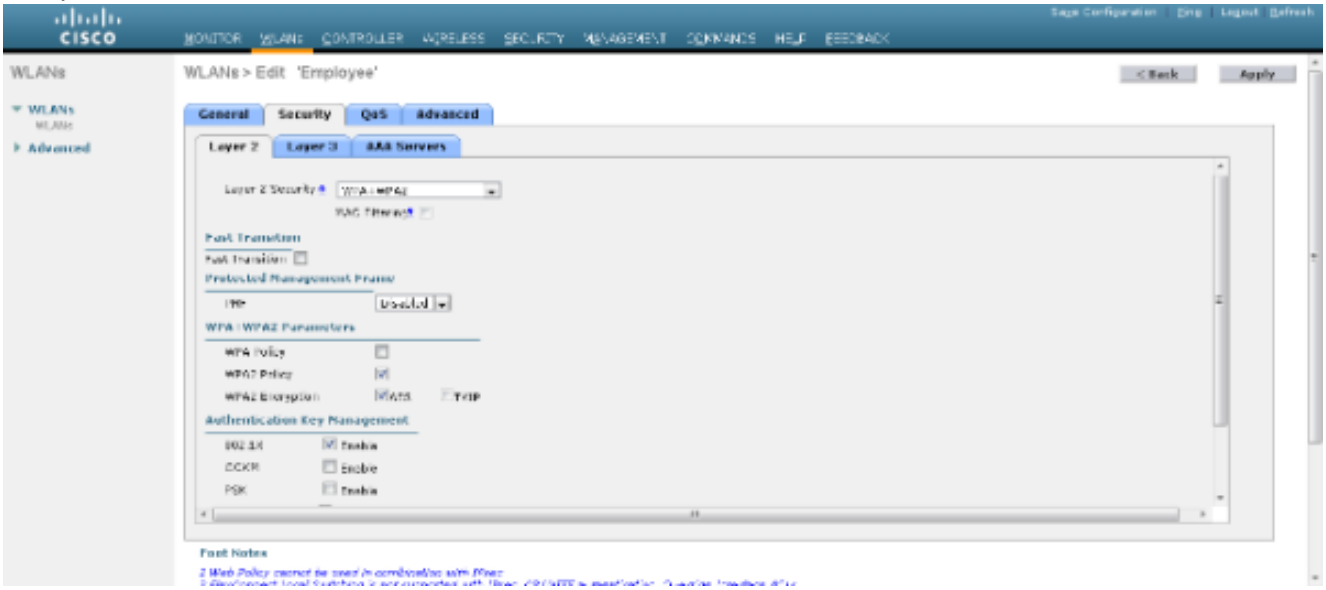
Apply를 **클릭합니다**.

2. SSID **직원**이 있는 직원의 WLAN 1개와 SSID **계약자**가 있는 계약자의 다른 WLAN을 구성하려면 다음 단계를 **완료합니다**. WLAN**을** 생성하려면 컨트롤러 GUI에서 WLANs를 클릭합니다.WLANs 창이 나타납니다.이 창에는 컨트롤러에 구성된 WLAN이 나열됩니다.새 WLAN을 구성하려면 **New**(새로 만들기)를 클릭합니다.이 예에서는 Employee라는 WLAN을 생성하고

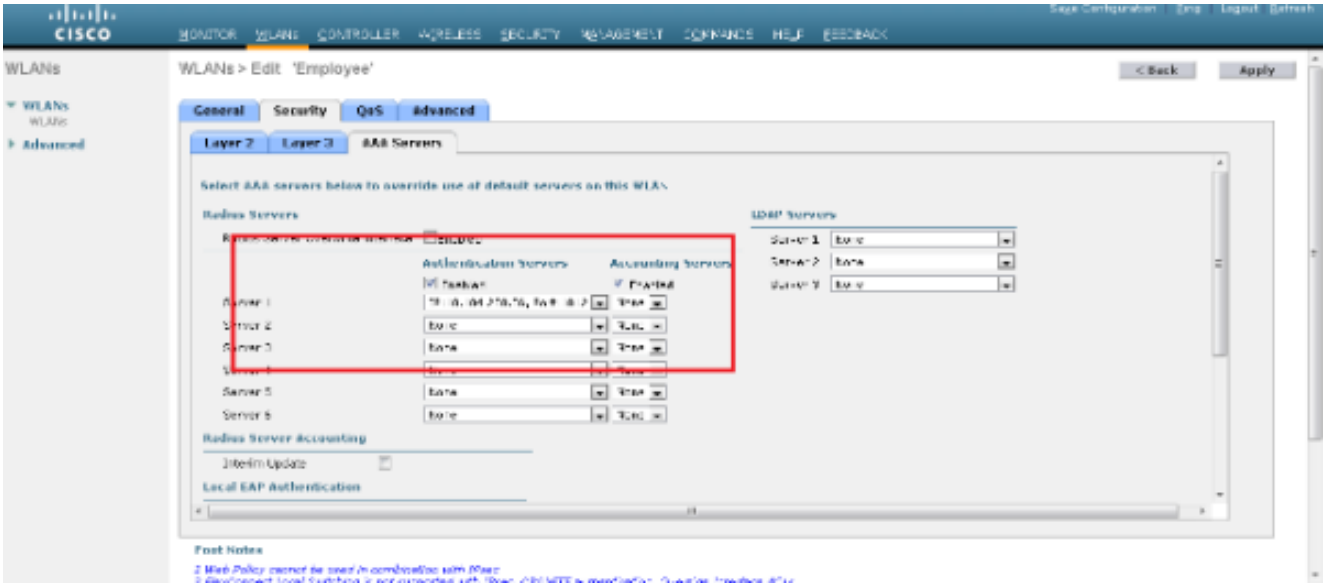
WLAN ID는 1입니다. Apply(적용)를 **클릭합니다**.



WLAN **> Edit(편집)** 창을 선택하고 WLAN에 해당하는 매개변수를 정의합니다. Layer 2 Security(레이어 2 보안) 탭에서 **802.1x를** 선택합니다.기본적으로 레이어 2 보안 옵션은 802.1x입니다.이렇게 하면 WLAN에 대한 802.1 x/EAP(Extensible Authentication Protocol) 인증이 활성화됩니다.



AAA servers(AAA 서버) 탭의 RADIUS Servers(RADIUS 서버) 드롭다운 목록에서 적절한 RADIUS 서버를 선택합니다.다른 매개변수는 WLAN 네트워크의 요구 사항에 따라 수정할 수 있습니다.Apply를 **클릭합니다**.



마찬가지로 계약자에 대한 WLAN을 생성하려면 b~d 단계를 반복합니다.

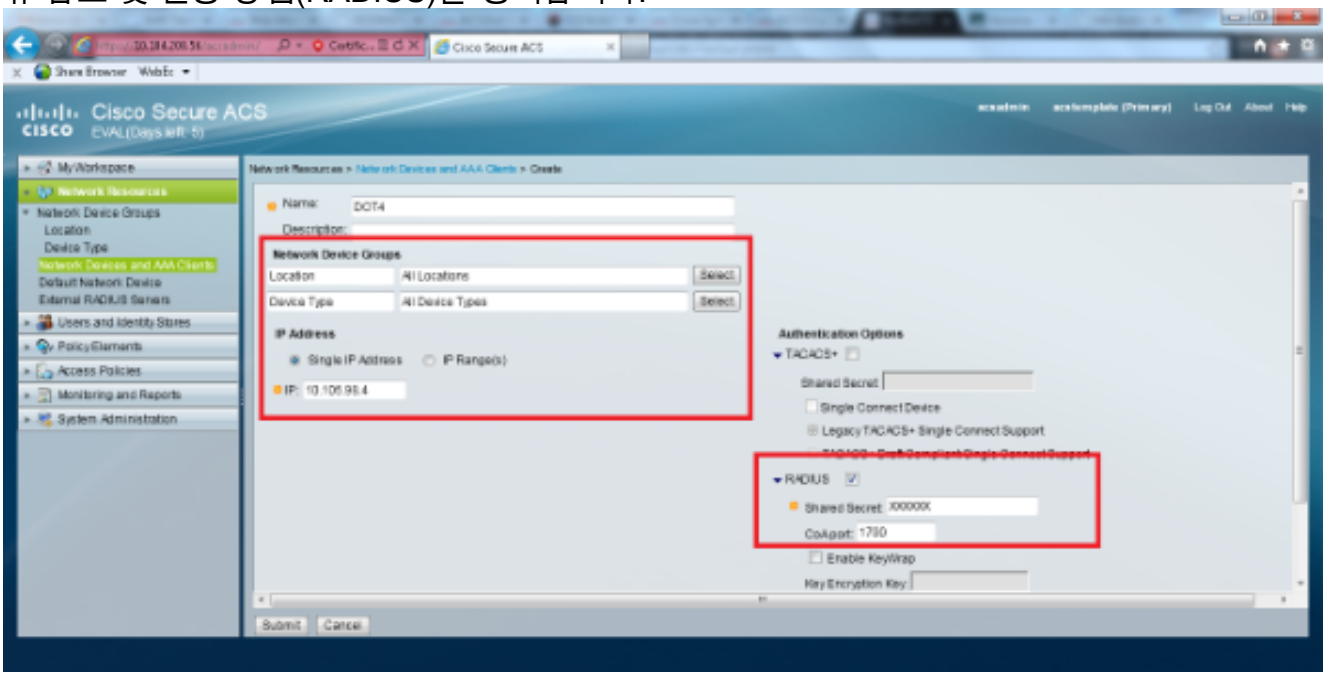
Cisco Secure ACS 구성

Cisco Secure ACS 서버에서 다음을 수행해야 합니다.

1. WLC를 AAA 클라이언트로 구성합니다.
2. SSID 기반 인증을 위한 사용자 데이터베이스(자격 증명)를 생성합니다.
3. EAP 인증을 활성화합니다.

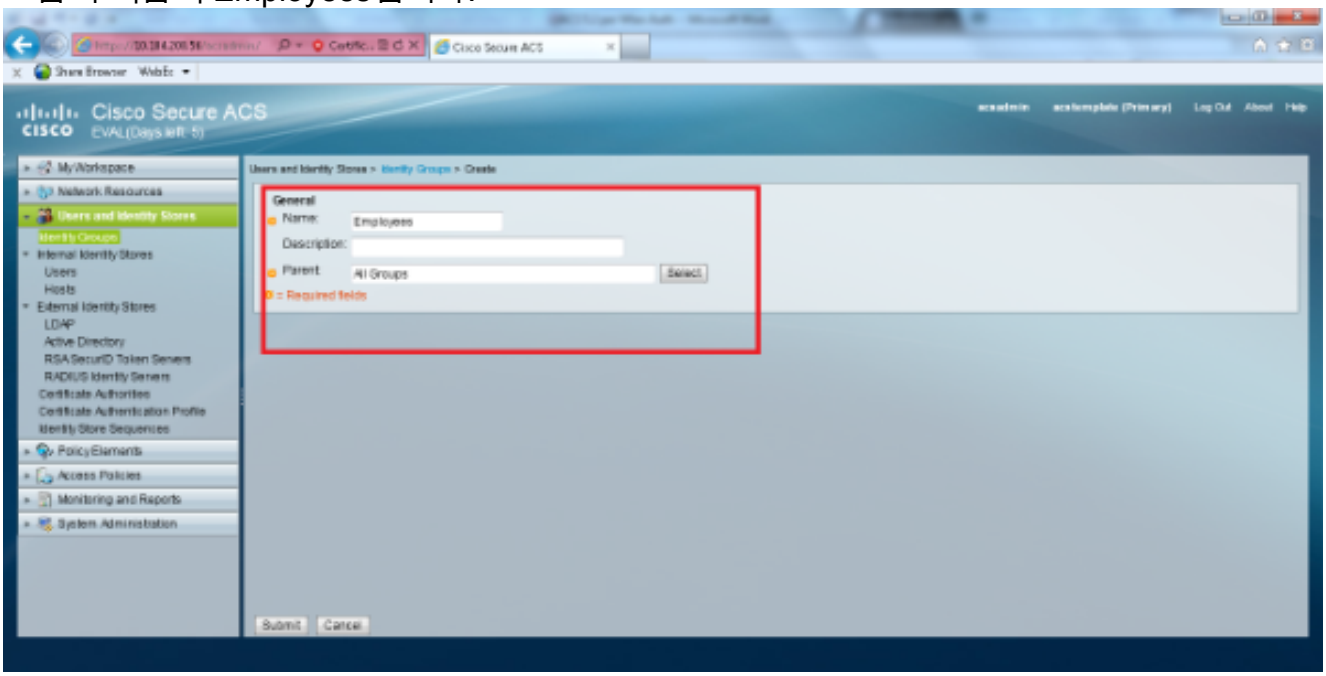
Cisco Secure ACS에서 다음 단계를 완료합니다.

1. 컨트롤러를 ACS 서버에서 AAA 클라이언트로 정의하려면 ACS GUI에서 **Network Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)**를 선택합니다.Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)**에서 Create(생성)를 클릭합니다.**
2. Network Configuration(네트워크 컨피그레이션) 페이지가 나타나면 WLC의 이름, IP 주소, 공유 암호 및 인증 방법(RADIUS)을 정의합니다.



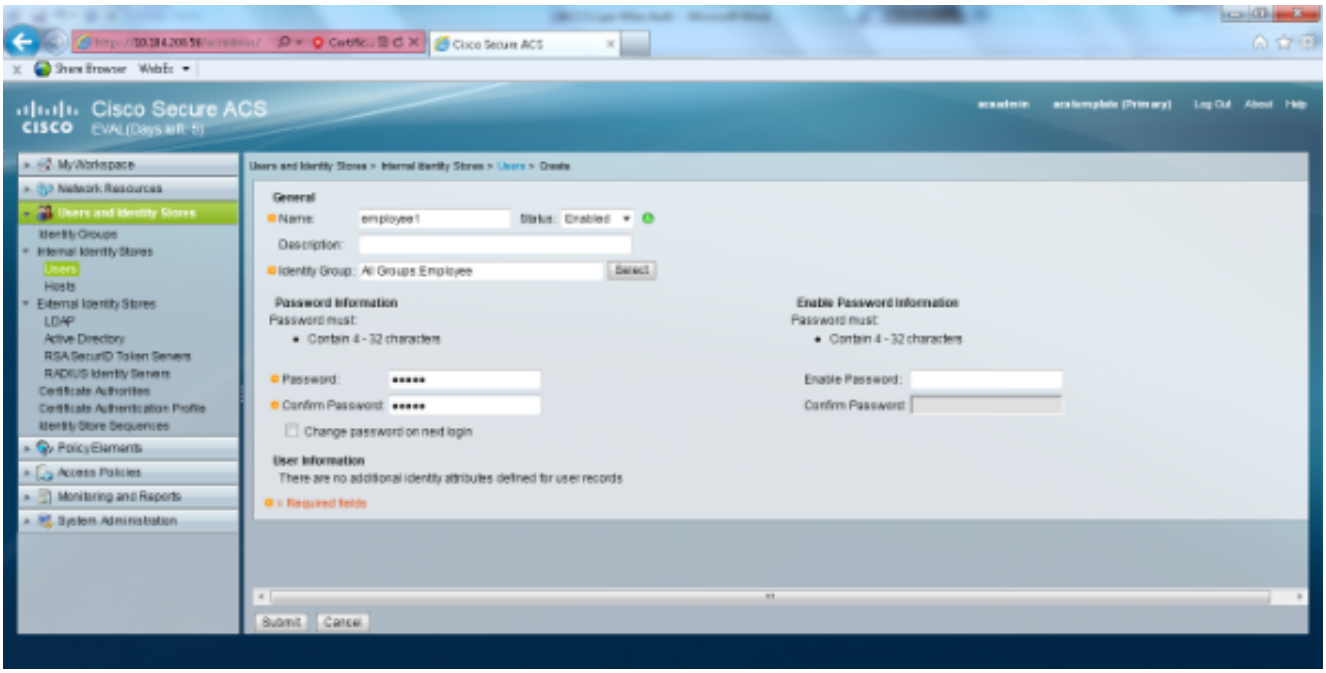
3. ACS **GUI에서 Users and Identity Stores(사용자 및 ID 저장소) > Identity Groups(ID 그룹)**를

선택합니다.사원 및 계약자에 대한 각 그룹을 생성하고 생성을 **누릅니다**.이 예에서는 생성된 그룹의 이름이 Employees입니다.

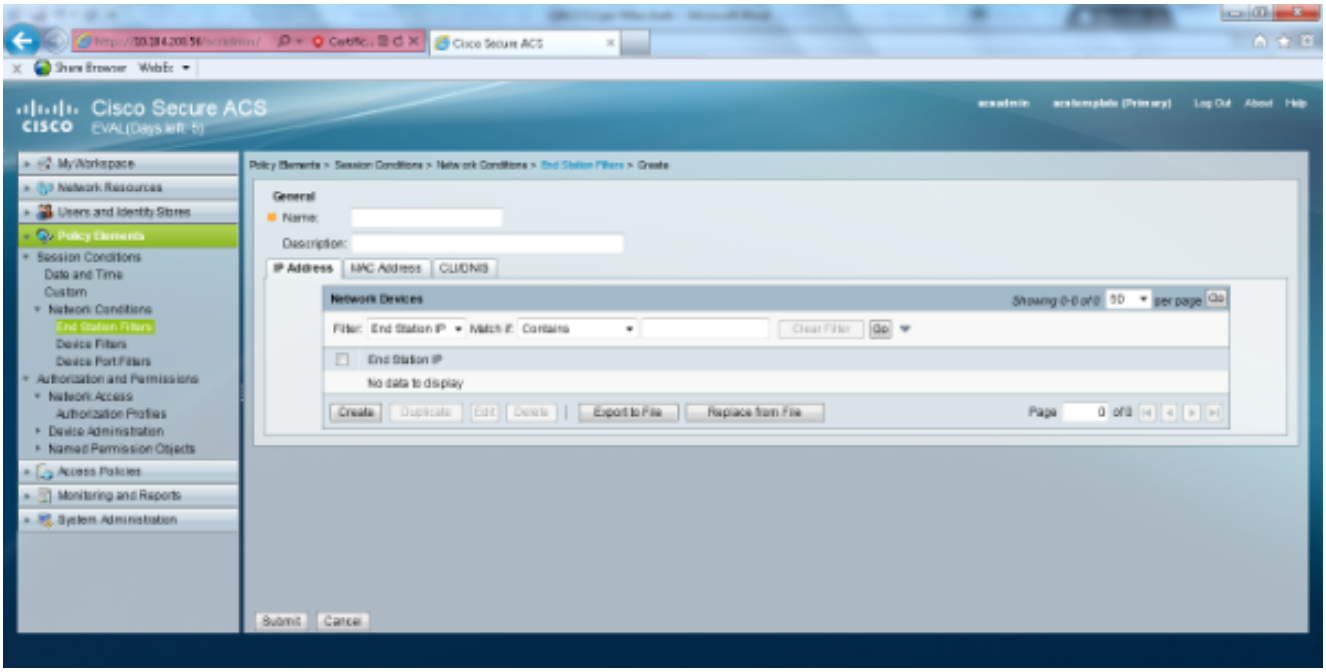


4. Users **and Identity Stores > Internal Identity Stores를 선택합니다**.Create(**생성**)를 클릭하고 사용자 이름을 입력합니다.올바른 그룹에 넣고 암호를 정의한 다음 **제출을** 클릭합니다.이 예에서는 직원 그룹의 employee1이라는 사용자가 생성됩니다.마찬가지로 그룹 계약자 아래에 contractor1이라는 사용자를 생성합니다

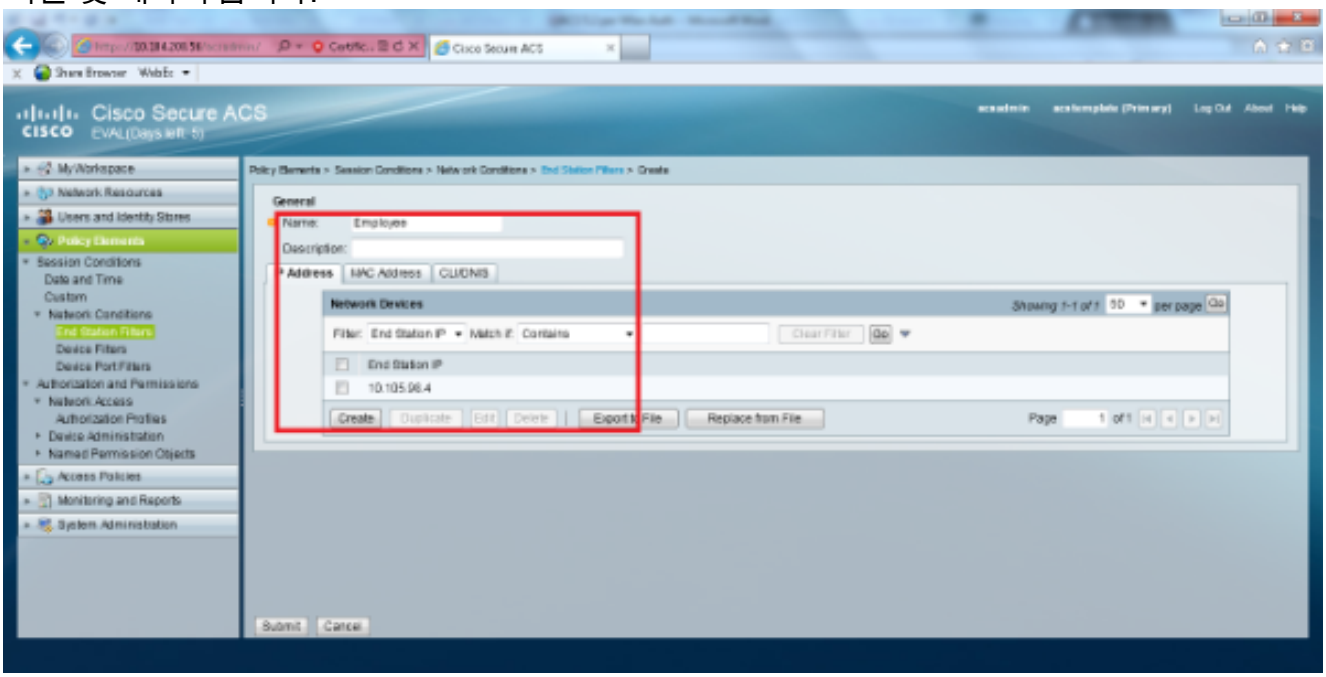
.



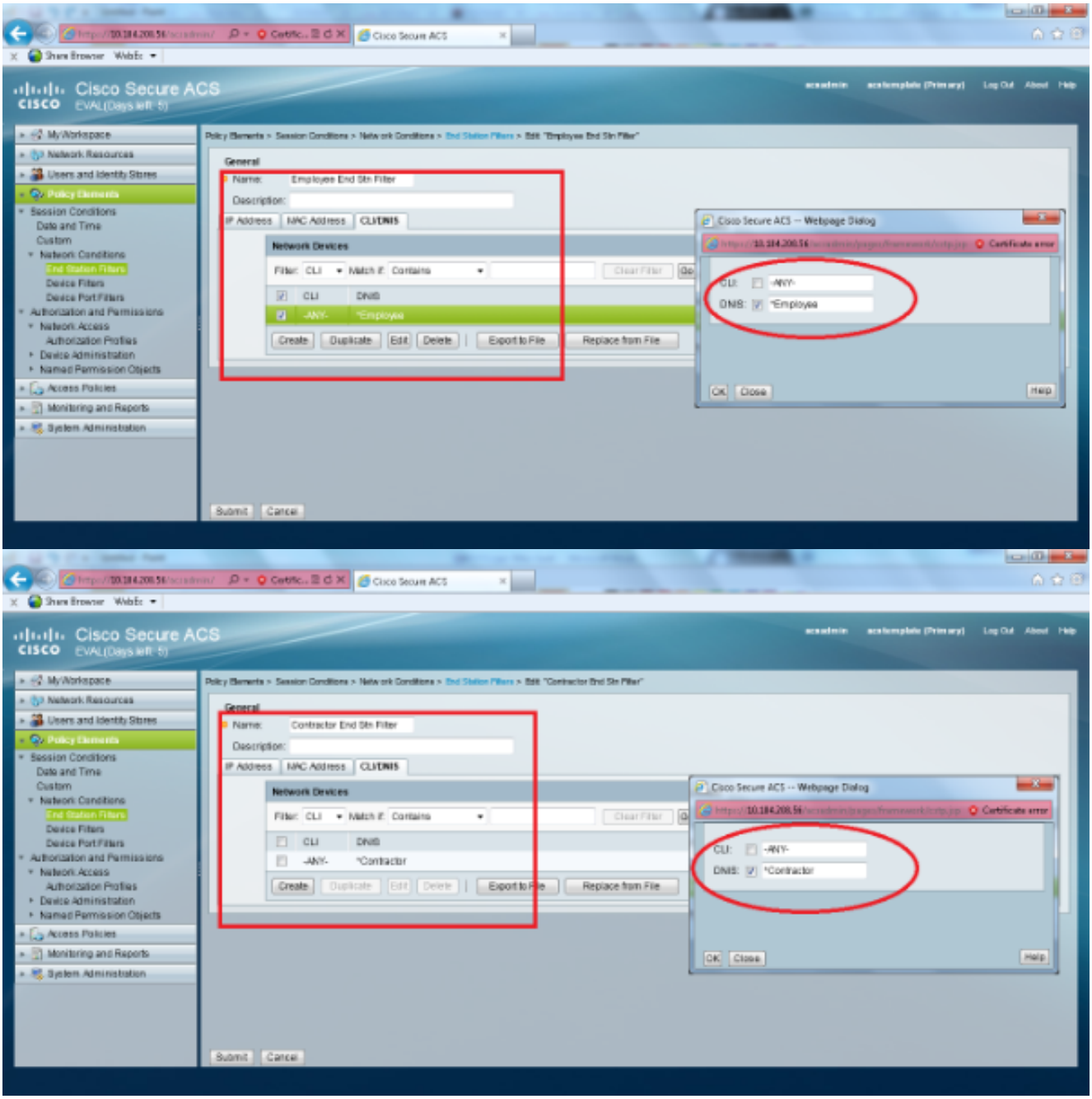
5. Policy **Elements(정책 요소) > Network Conditions(네트워크 조건) > End Station Filters(엔드 스테이션 필터)를 선택합니다**.Create를 **클릭합니다**.



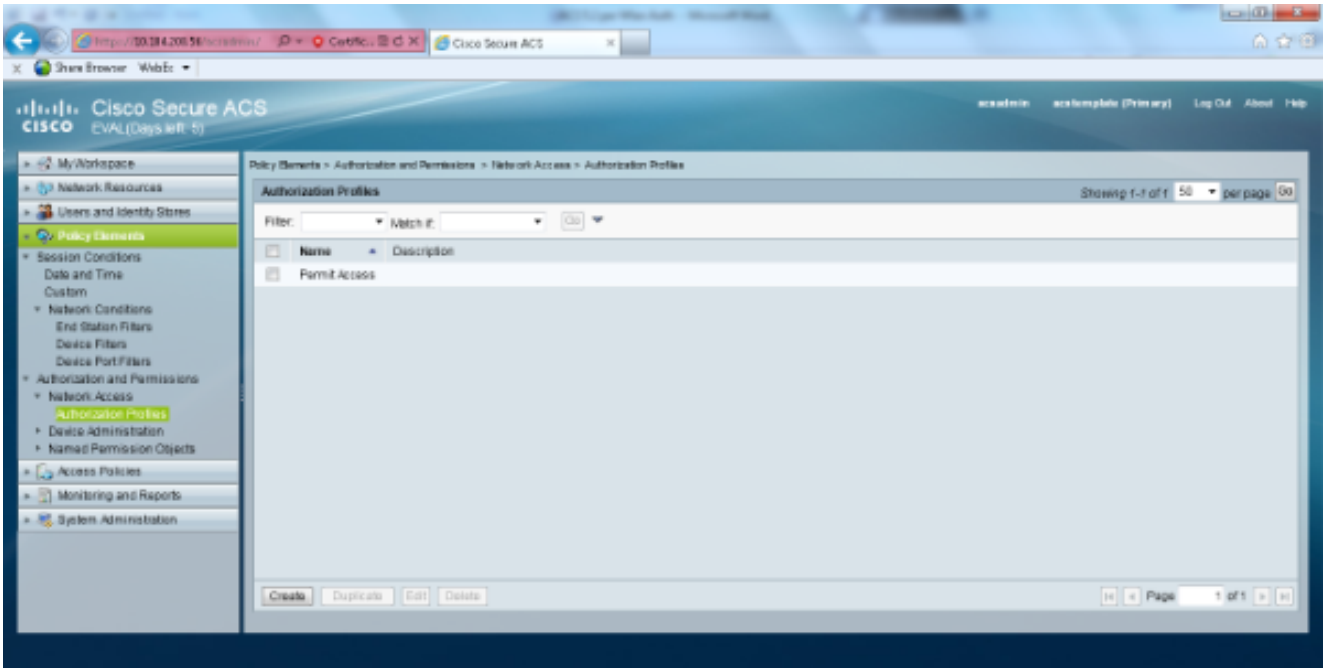
의미 있는 이름을 입력하고 **IP 주소** 탭 아래에 WLC의 IP 주소를 입력합니다.이 예에서 이름은 직원 및 계약자입니다.



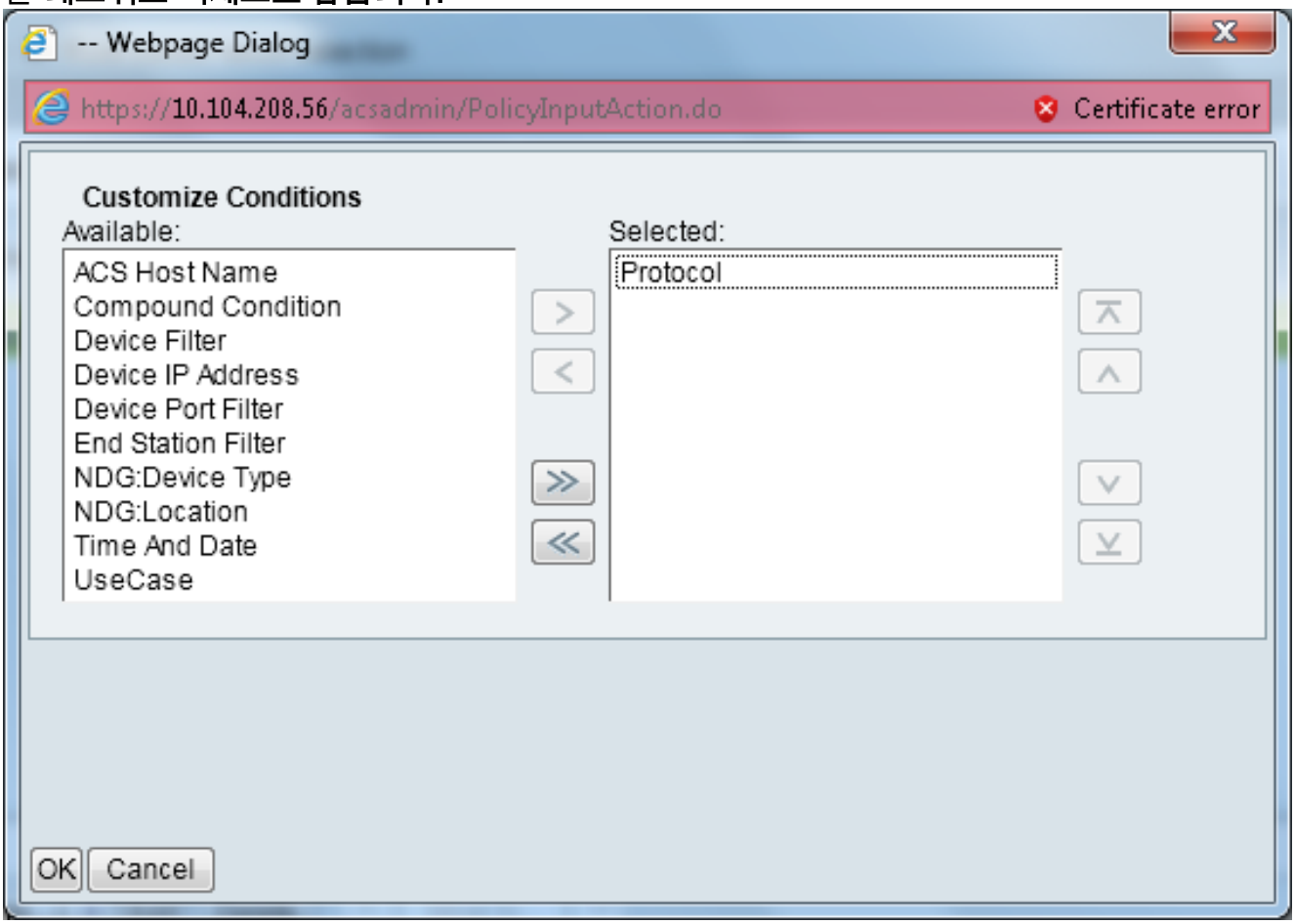
CLI/DNIS 탭에서 CLI를 -ANY-(모두)로 두고 DNIS를 *<SSID>로 입력합니다.이 예에서는 이 엔드 스테이션 필터를 사용하여 직원 WLAN에 대한 액세스만 제한하므로 DNIS 필드가 *Employee로 입력됩니다.DNIS 특성은 사용자가 액세스할 수 있는 SSID를 정의합니다 .WLC는 DNIS 특성의 SSID를 RADIUS 서버로 전송합니다.계약자 종료 스테이션 필터에 대해 동일한 단계를 반복합니다.

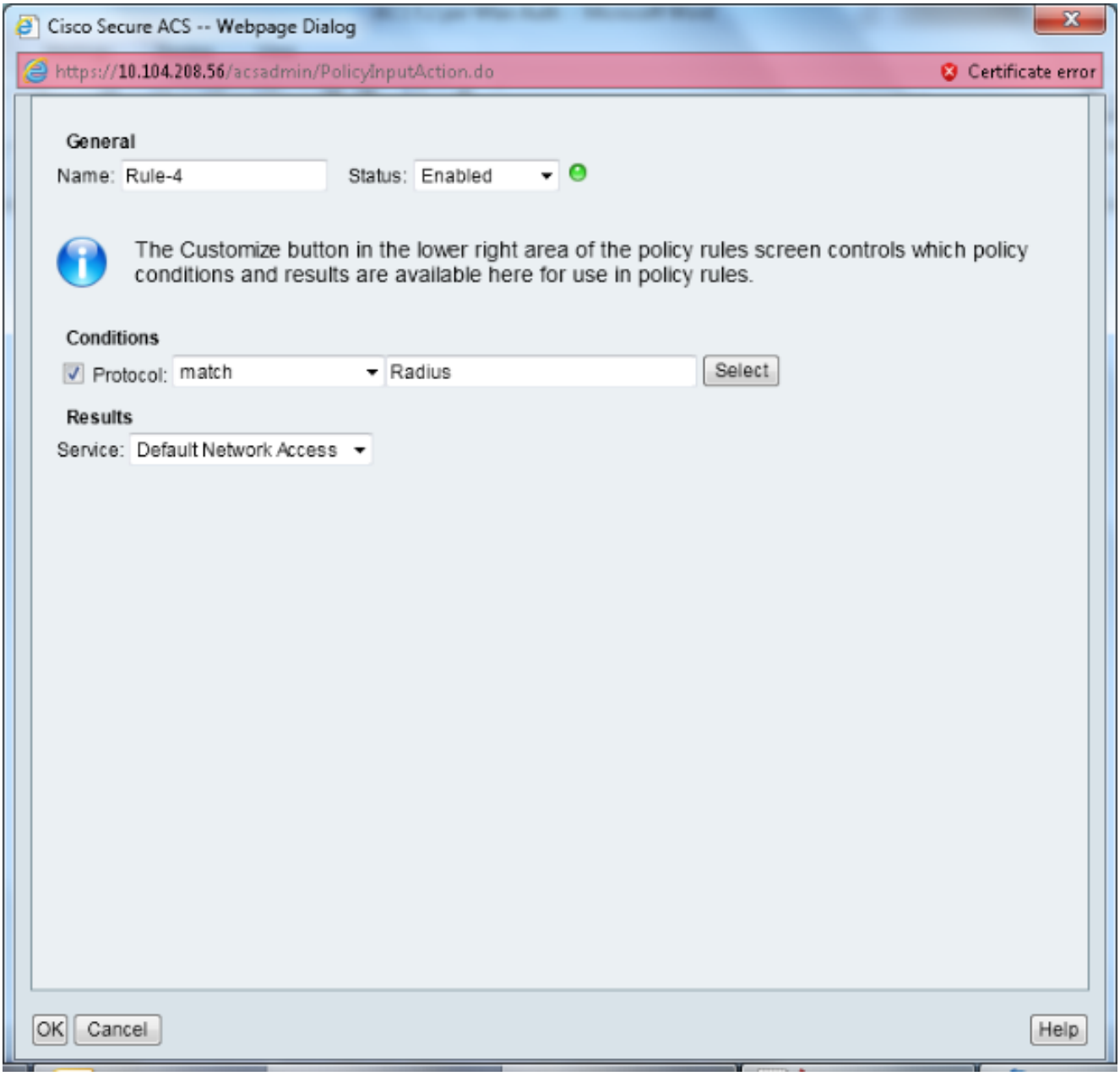


6. Policy **Elements(정책 요소) > Authorization and Permissions(권한 부여 및 권한) > Network Access(네트워크 액세스) > Authorization Profiles(권한 부여 프로파일)를 선택합니다**.액세스 허용에 대한 기본 프로파일이 있어야 합니다.

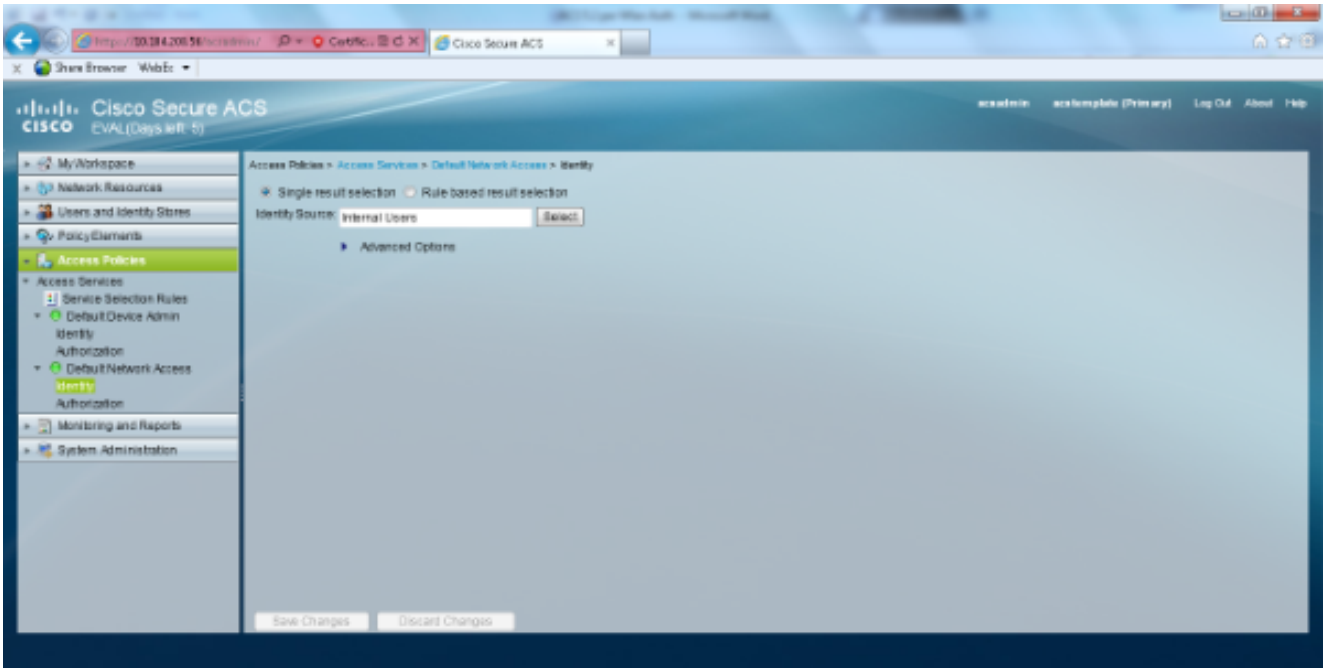


7. Access **Policies > Access Services > Service Selection Rules를 선택합니다**.사용자 정의**를 클릭합니다**. 적절한 조건을 추가합니다.이 예에서는 Protocol을 Radius로 일치 조건으로 사용합니다.Create를 **클릭합니다**.규칙의 이름을 지정합니다.Protocol**을** 선택하고 **Radius**를 선택합니다.Results(**결과**)에서 적절한 Access Service(액세스 서비스)를 선택합니다.이 예에서는 기본 **네트워크 액세스**로 **남습니다.**

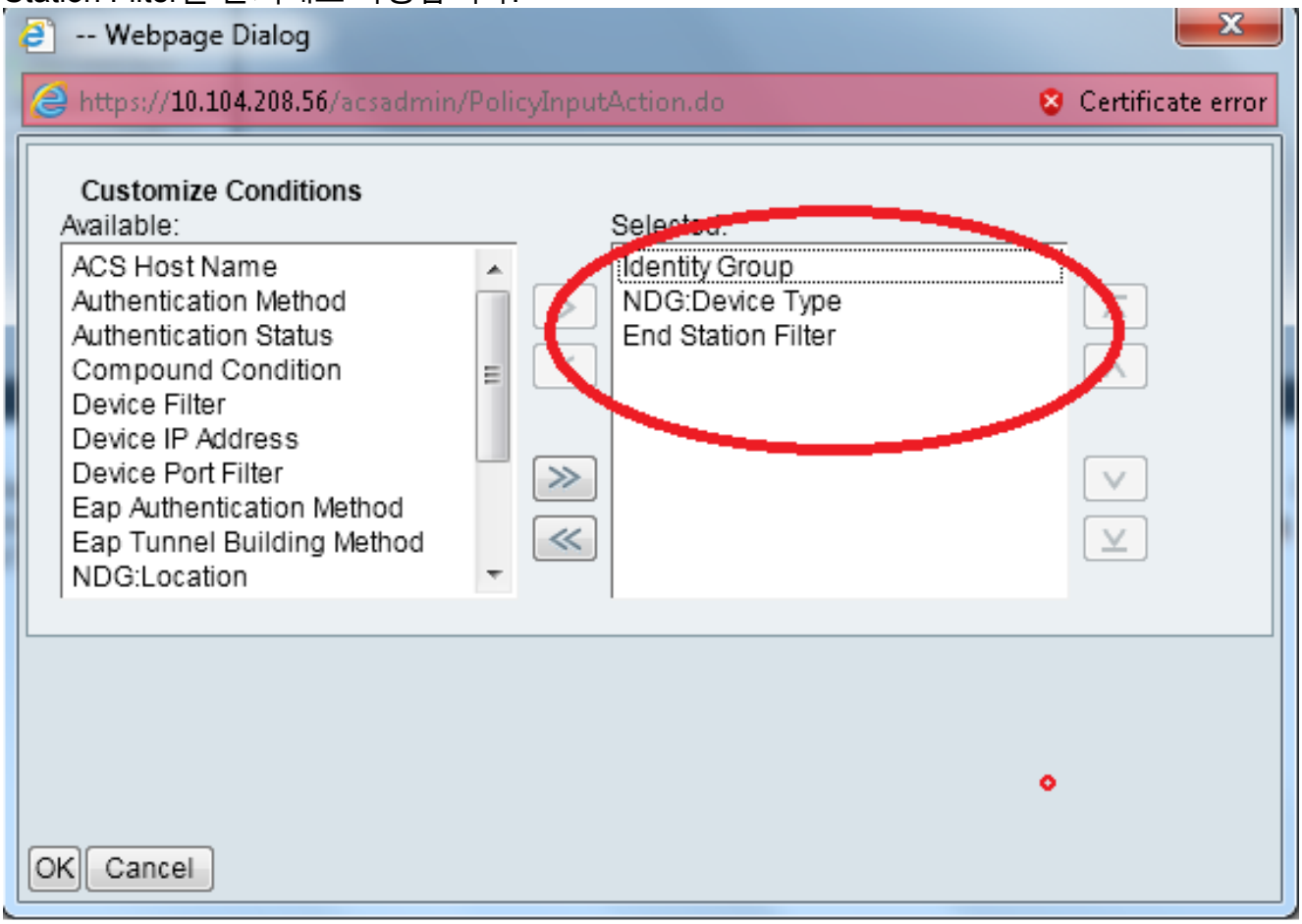




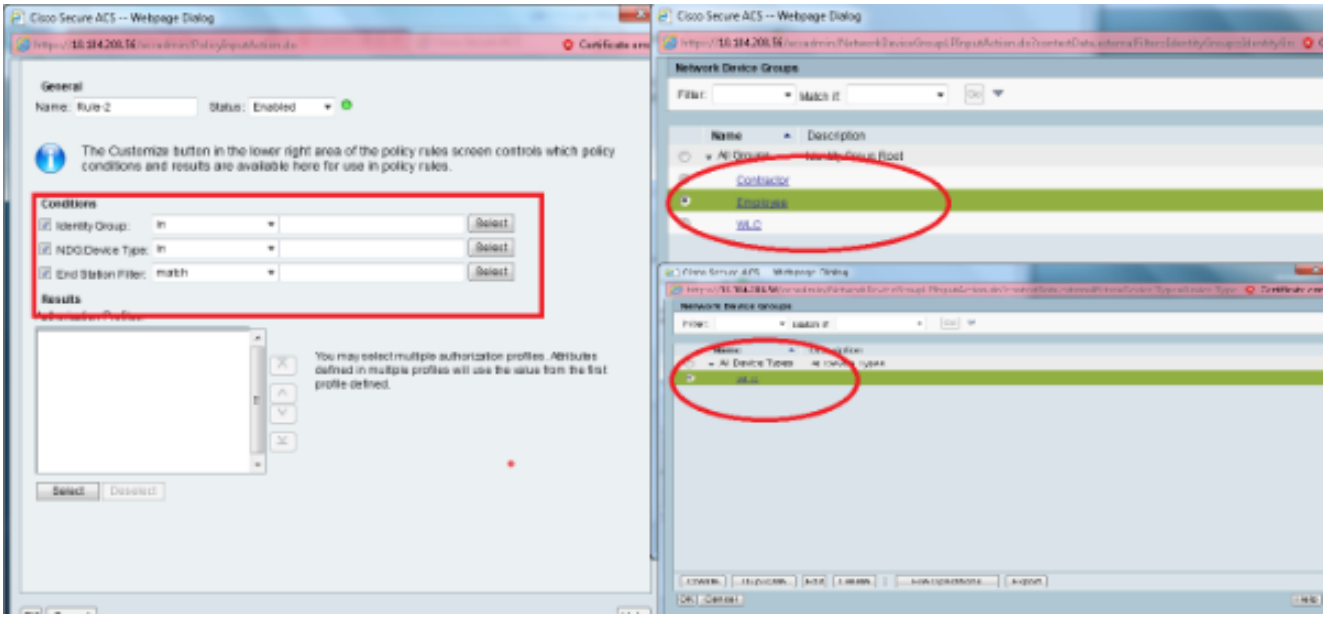
8. Access **Policies > Access Services > Default Network Access > Identity를 선택합니다**.Single Result Selection(단일 결과 선택) 및 **Identity Source(ID 소스)**를 Internal Users(내부 사용자)로 선택합니다.



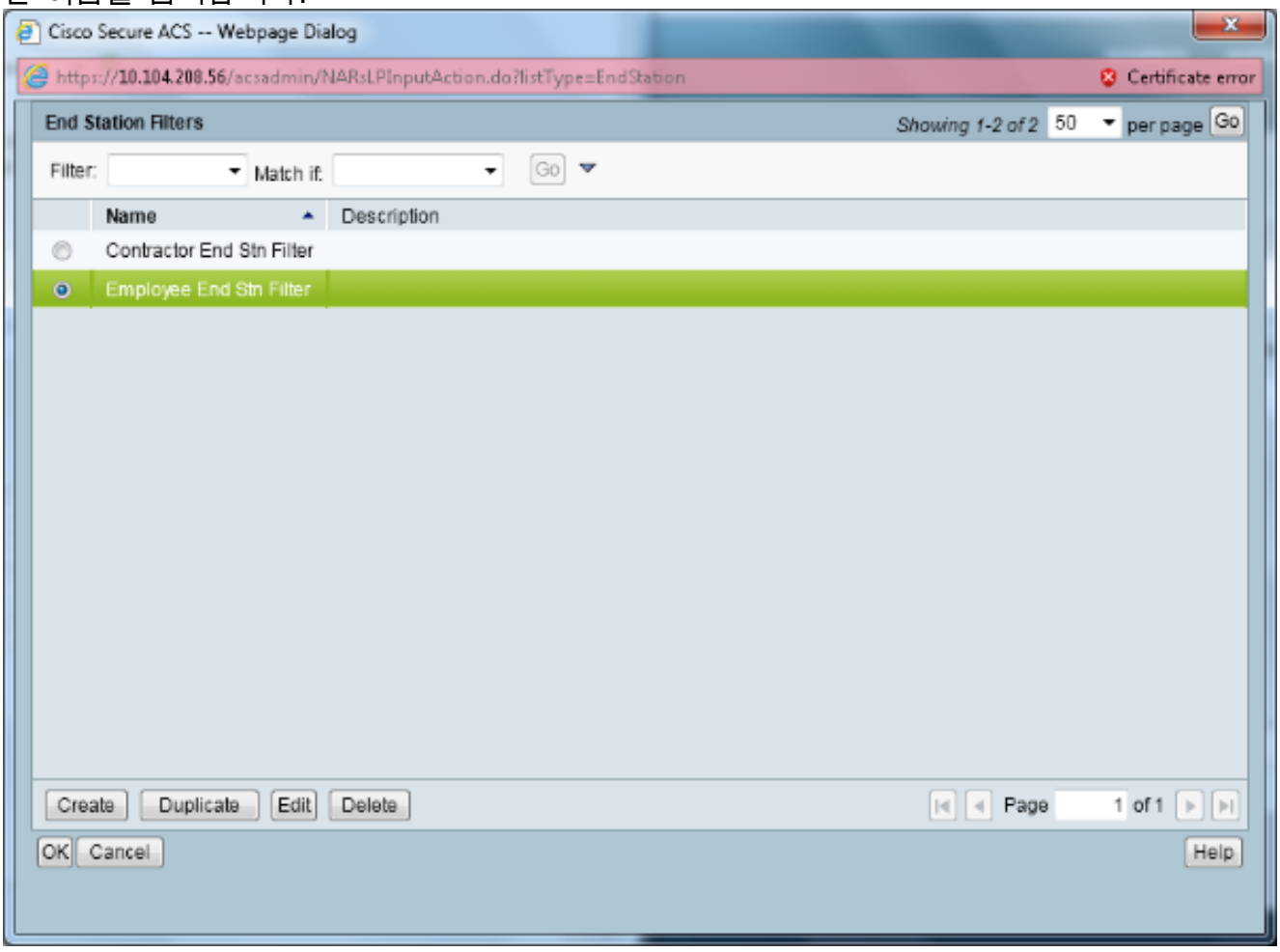
액세스 **정책 > 액세스 서비스 > 기본 네트워크 액세스 > 권한 부여를 선택합니다. 사용자 정의를** 누르고 사용자 정의 조건을 추가합니다.이 예에서는 ID 그룹, NDG:Device Type 및 End Station Filter를 순서대로 사용합니다.



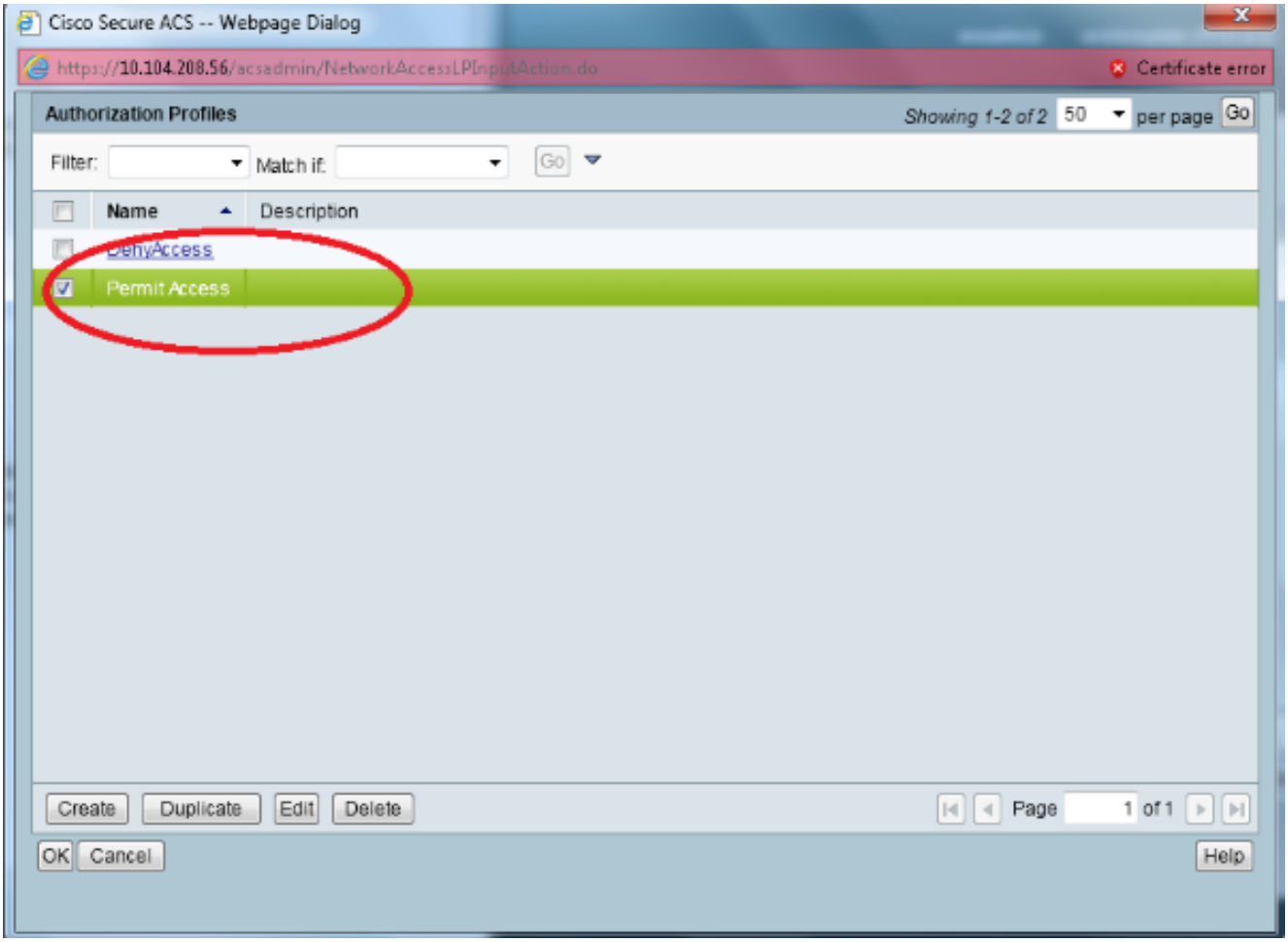
Create를 **클릭합니다**.규칙의 이름을 지정하고 All Groups(모든 그룹) 아래에서 적절한 ID 그룹을 선택합니다.이 예에서는 Employee입니다.



Employee **End Stn Filter** 라디오 버튼을 클릭하거나 "Configure the WLC" 섹션에서 1b에 입력한 이름을 입력합니다.

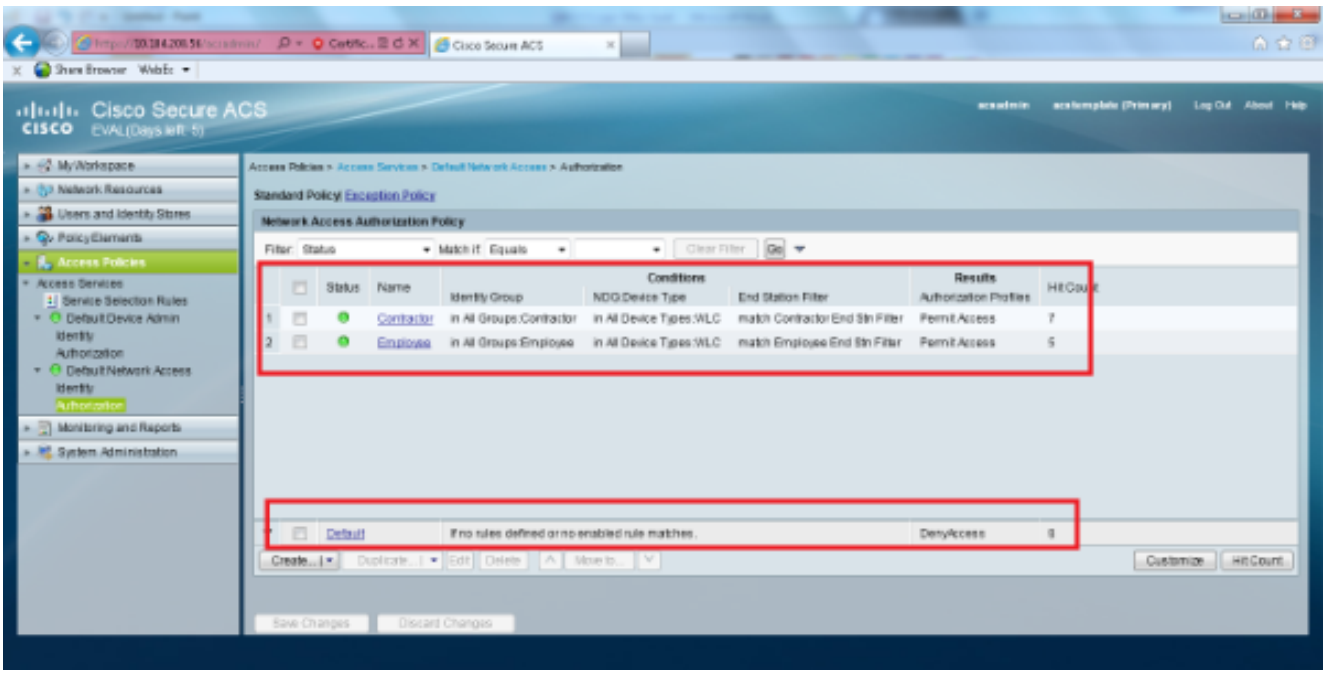


Permit **Access** 확인란을 선택합니다.



계약자 규칙에도 위와 같은 단계를 반복합니다.Default Action(기본 작업)이 Deny Access(**액세스 거부**)인지 **확인합니다**. e 단계를 완료했으면 규칙이 다음 예와 같아야 합니다

.



이것으로 컨피그레이션을 마치겠습니다.이 섹션 다음에는 연결하려면 SSID 및 보안 매개변수를 사용하여 클라이언트를 적절히 구성해야 합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.