SD-Access에서 중앙 웹 인증 구성

목차

소개

이 문서에서는 CWA(Central Web Authentication)를 구성하기 위한 단계별 가이드와 모든 구성 요소에 대한 확인 절차를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Catalyst 센터
- Cisco ISE(Identity Services Engine)
- Catalyst 9800 Wireless Controller 아키텍처
- 인증, 권한 부여 및 계정 관리(AAA)

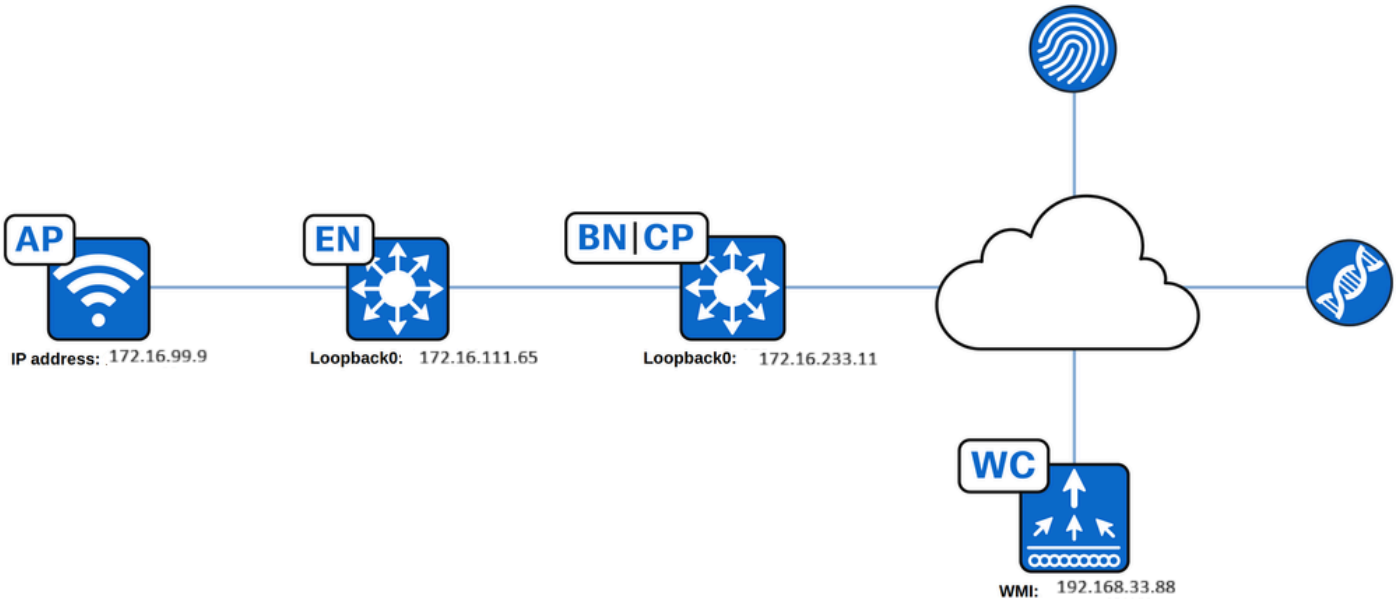
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco WLC(Wireless LAN Controller) - C9800-CL, Cisco IOS® XE 17.12.04
- Cisco Catalyst Center - 버전 2.3.7.7
- Cisco ISE(Identity Services Engine) - 버전 3.0.0.458
- SDA 에지 노드 - C9300-48P, Cisco IOS® XE 17.12.05
- SDA 보더 노드/컨트롤 플레인 - C9500-48P, Cisco IOS® XE17.12.05
- Cisco Access Point - C9130AXI-A, 버전 17.9.5.47

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

토폴로지



개요

CWA(Central Web Authentication)는 구성된 리디렉션 ACL을 사용하여 Cisco ISE에서 호스팅하는 종속 포털에 사용자의 웹 브라우저를 리디렉션하기 위해 게스트 유형 SSID를 사용합니다. 종속 포털을 사용하면 사용자가 등록 및 인증할 수 있으며, 인증에 성공한 후 WLC(Wireless LAN Controller)가 적절한 권한 부여를 적용하여 전체 네트워크 액세스를 허용합니다. 이 가이드에서는 Cisco Catalyst Center를 사용하여 CWA를 구성하기 위한 단계별 지침을 제공합니다.

Cisco Catalyst Center에서 CWA 구성

네트워크 프로파일 생성

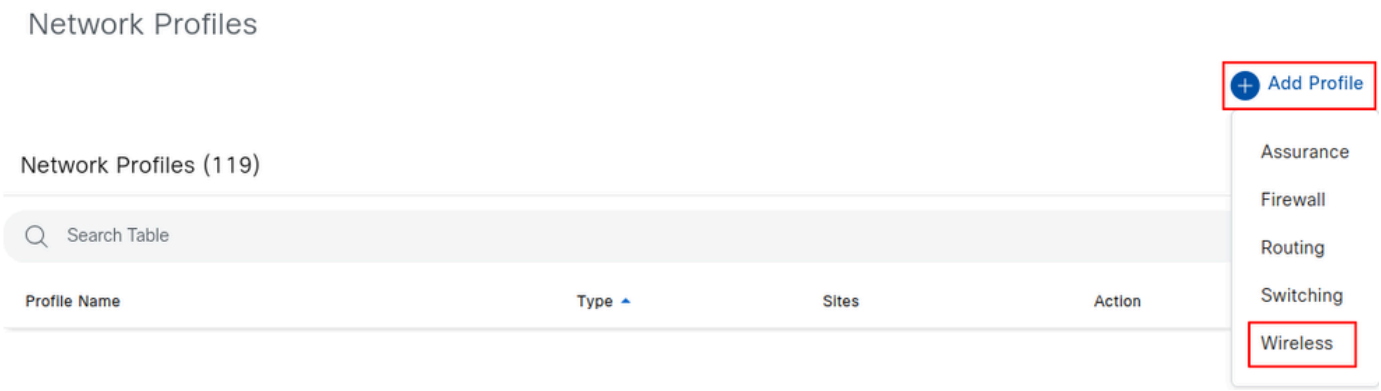
네트워크 프로필에서는 특정 사이트에 적용할 수 있는 설정을 구성할 수 있습니다. Cisco Catalyst Center의 다양한 요소에 대해 다음과 같은 네트워크 프로파일을 생성할 수 있습니다.

- 보증

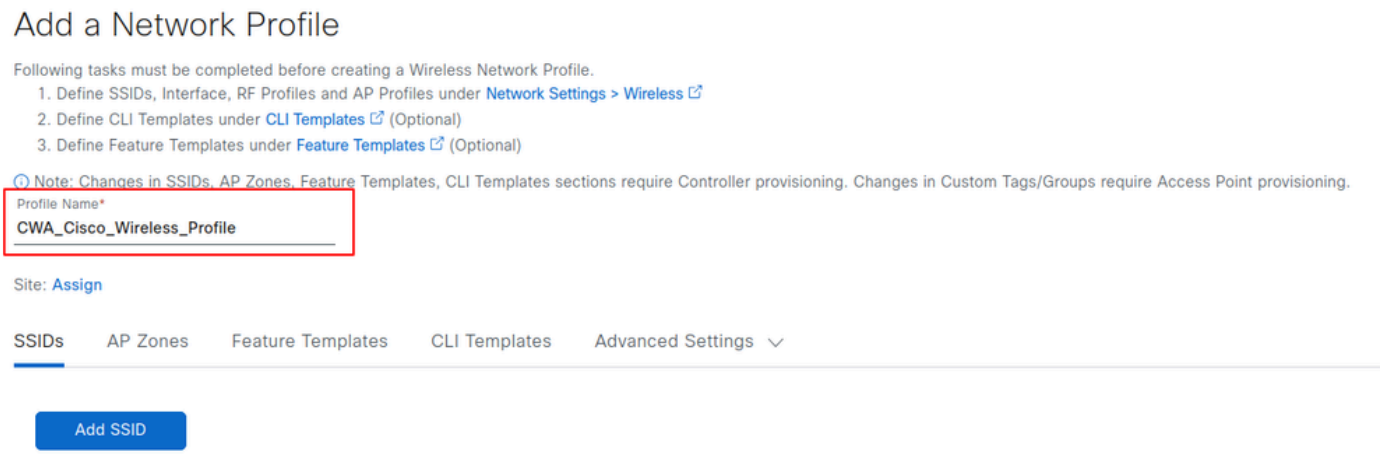
- 방화벽
- 라우팅
- 스위칭
- 텔레메트리 어플라이언스
- 무선

CWA의 경우 무선 프로필을 구성해야 합니다.

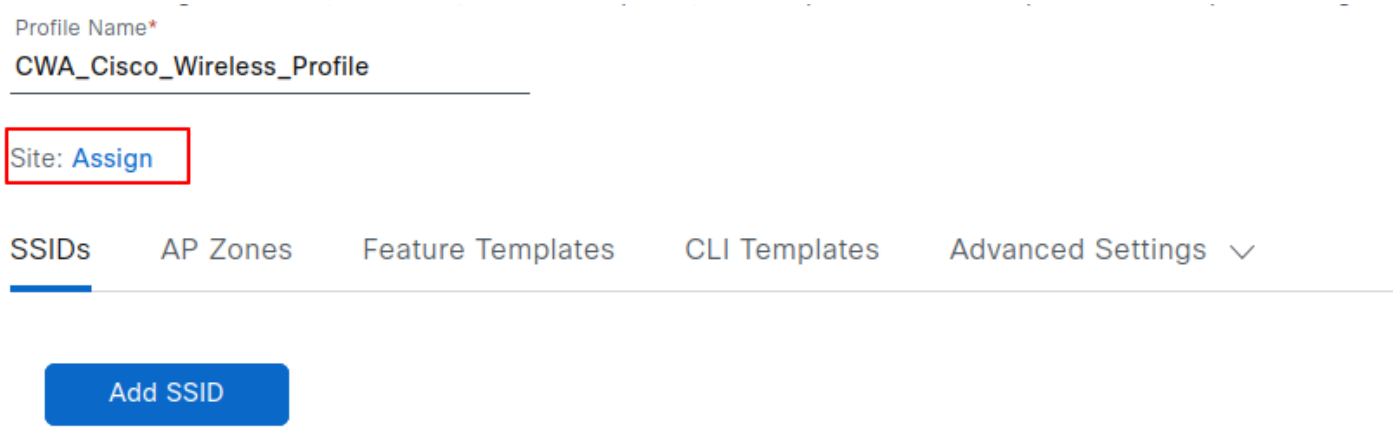
무선 프로필을 구성하려면 Design > Network Profiles로 이동하여 Add Profile(프로필 추가)을 클릭하고 Wireless(무선)를 선택합니다.



프로파일의 이름을 필요에 따라 지정합니다. 이 예에서 무선 프로파일의 이름은 CWA_Cisco_Wireless_Profile입니다. Add SSID(SSID 추가)를 선택하여 기존 SSID를 이 프로파일에 추가할 수 있습니다. SSID 생성에 대해서는 다음 섹션에서 설명합니다.

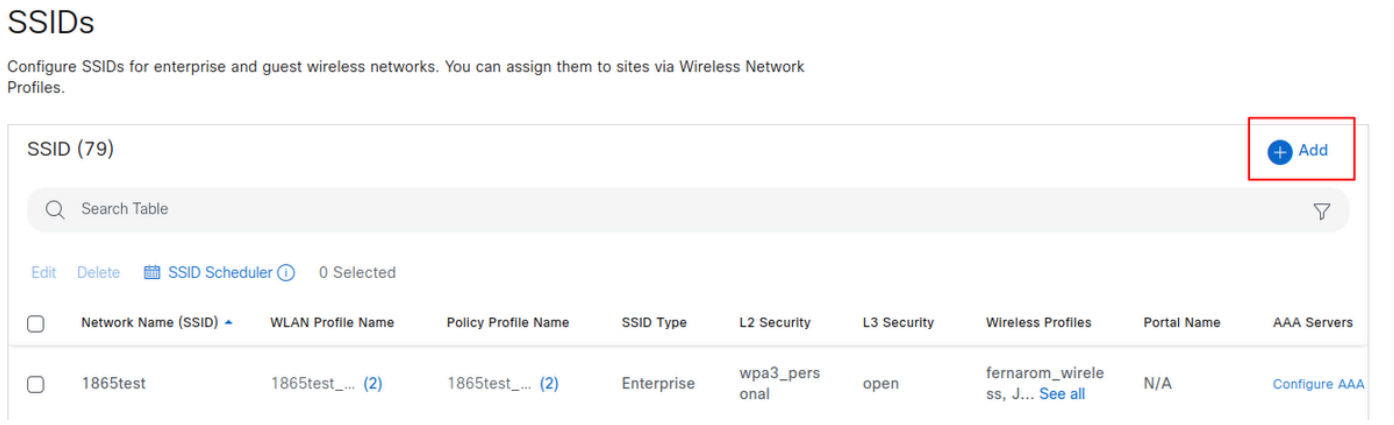


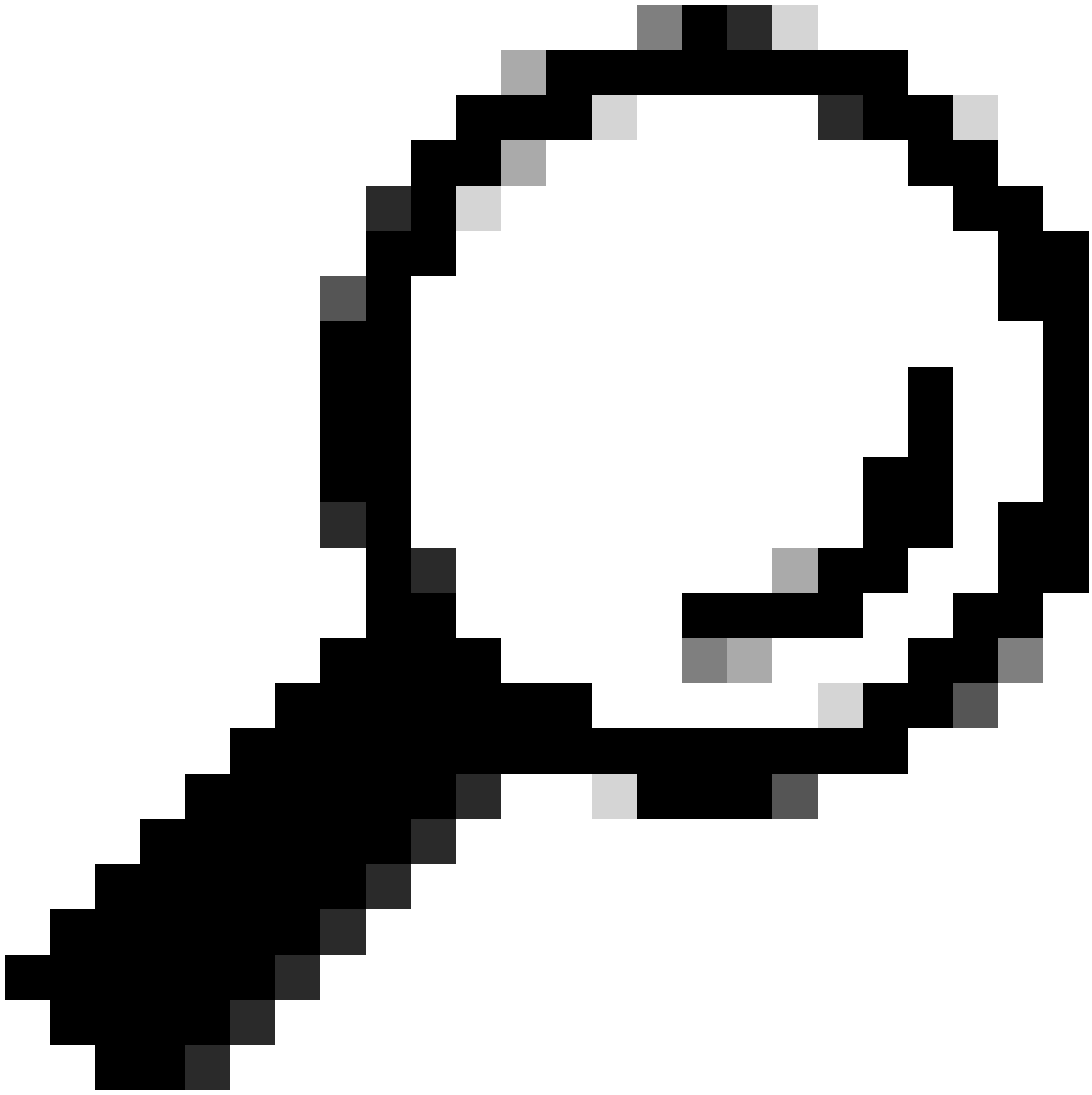
Assign(할당)을 선택하여 이 프로파일을 적용할 사이트를 선택한 다음 원하는 사이트를 선택합니다. 사이트를 선택한 후 저장을 클릭합니다.



SSID 생성

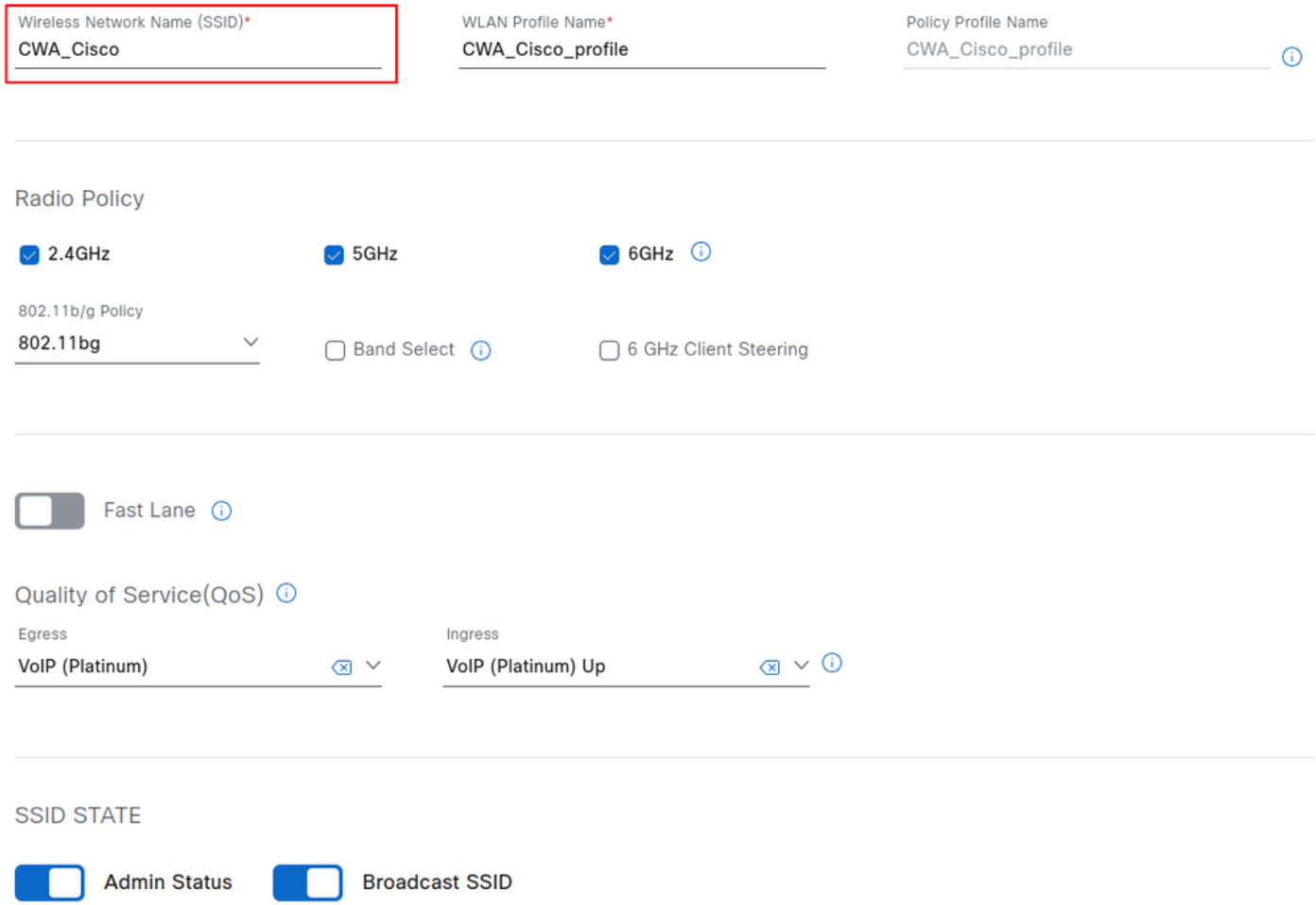
Design(설계) > Network Settings(네트워크 설정) > Wireless(무선) > SSIDs(SSID)로 이동하고 Add(추가)를 클릭합니다.



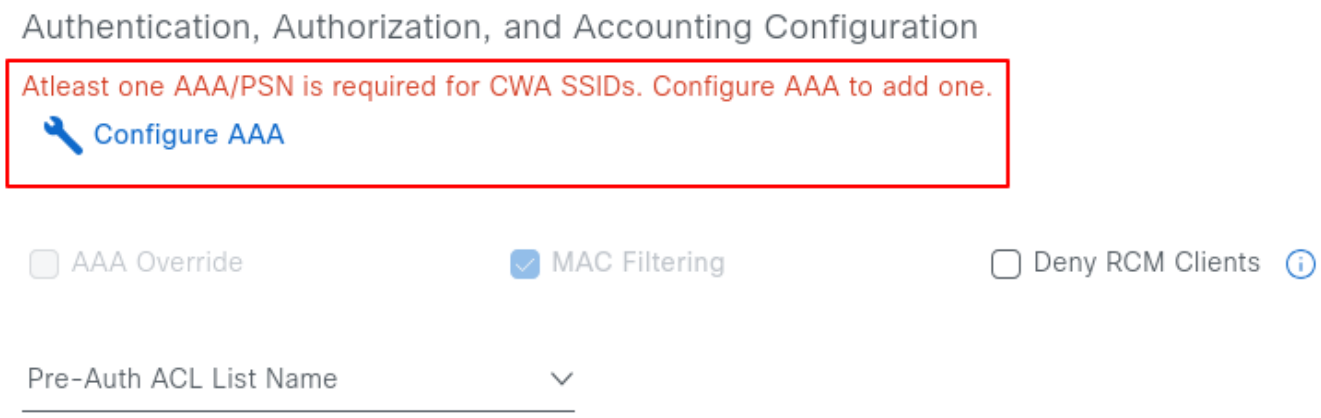


팁: CWA에 대한 SSID를 생성할 때 게스트 유형을 선택해야 합니다. 이렇게 선택하면 WLC의 SSID 무선 정책 프로파일에 명령이 추가됩니다. nac 명령 - 사용자가 종속 포털에 등록한 후 CoA를 재인증에 사용할 수 있습니다. 이러한 컨피그레이션이 없으면 사용자는 포털에 등록하고 리디렉션되는 무한 루프를 반복해서 경험할 수 있습니다.

Add(추가)를 선택한 후 SSID 컨피그레이션 워크플로를 진행합니다. 첫 번째 페이지에서 SSID 이름을 구성하면 라디오 정책 대역을 선택하고 관리 상태 및 SSID 브로드캐스트 설정을 비롯한 SSID 상태를 정의할 수 있습니다. 이 컨피그레이션 가이드에서 SSID의 이름은 CWA_Cisco입니다.



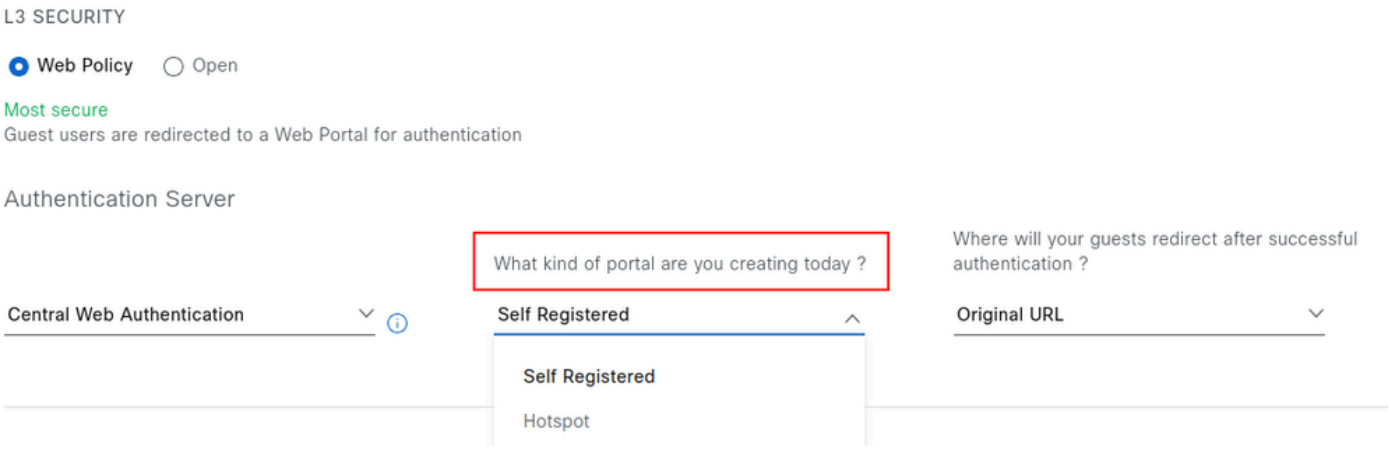
SSID 이름을 입력하면 WLAN 프로파일 이름 및 정책 프로파일 이름이 자동으로 생성됩니다. 다음을 선택하여 진행합니다.
CWA SSID에 대해 하나 이상의 AAA/PSN을 구성해야 합니다. 구성되지 않은 경우 Configure AAA(AAA 구성)를 선택하고 드롭다운 목록에서 PSN IP 주소를 선택합니다.



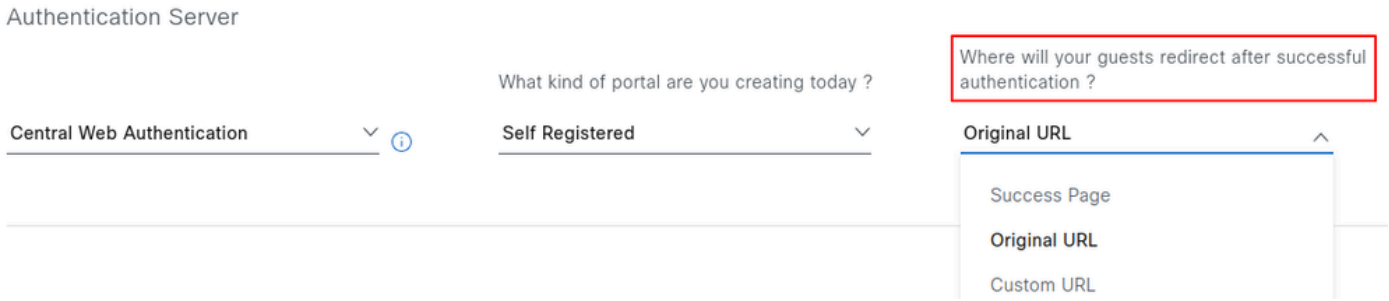
AAA 서버를 선택한 후 Layer 3 보안 매개변수를 설정하고 포털 유형을 선택합니다. 셀프 등록 또는 핫스팟.

핫스팟 게스트 포털: 핫스팟 게스트 포털에서는 사용자 이름 및 비밀번호 없이도 게스트에 대한 네트워크 액세스를 제공합니다. 여기서 사용자는 AUP(Acceptable Use Policy)에 동의해야 네트워크에 대한 액세스를 얻을 수 있으며, 이는 후속 인터넷 액세스로 이어집니다. 자격 증명이 지정된 게스

트 포털을 통해 액세스하려면 게스트에게 사용자 이름 및 비밀번호가 있어야 합니다.



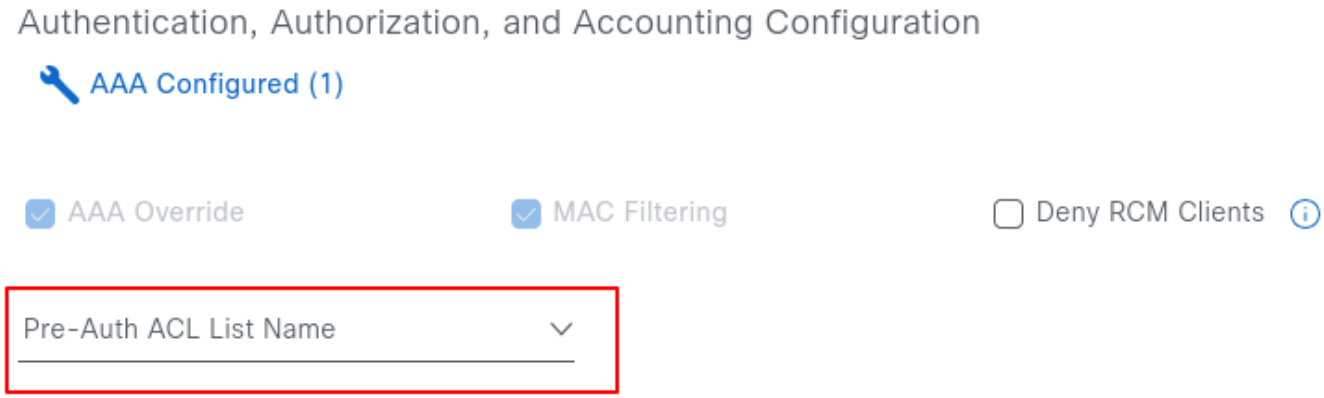
사용자가 사용 정책을 등록하거나 수락한 후 발생하는 작업도 구성할 수 있습니다. 다음 세 가지 옵션을 사용할 수 있습니다. 성공 페이지, 원래 URL 및 사용자 지정 URL



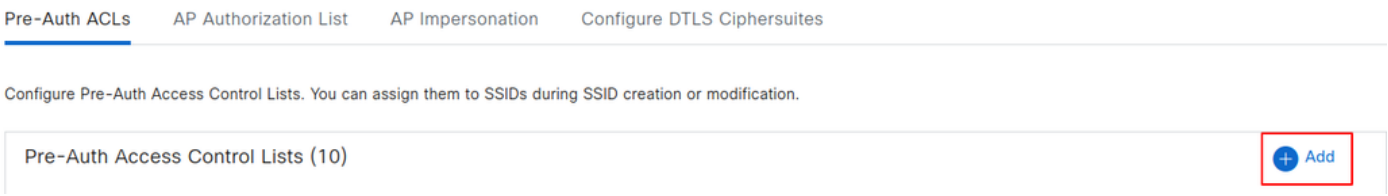
다음은 각 옵션의 동작에 대해 설명합니다.

성공 페이지: 인증이 성공했음을 나타내는 확인 페이지로 사용자를 리디렉션합니다.
Original URL: 종속 포털에서 가로채기 전에 요청된 원래 URL로 사용자를 리디렉션합니다.
사용자 지정 URL: 사용자를 지정된 사용자 지정 URL로 리디렉션합니다. 이 옵션을 선택하면 추가 필드에서 대상 URL을 정의할 수 있습니다

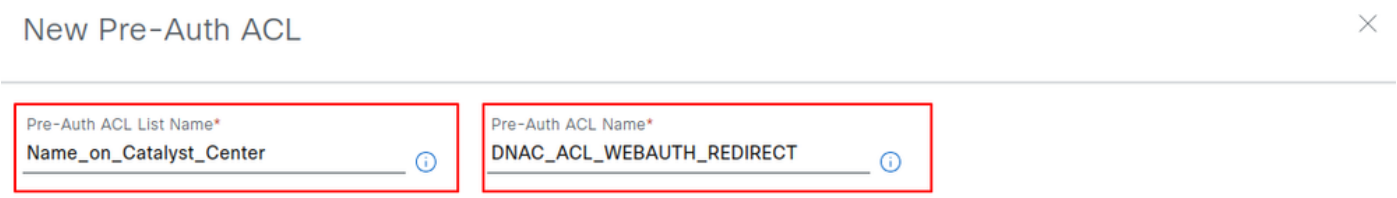
같은 페이지의 Authentication, Authorization, and Accounting Configuration(인증, 권한 부여 및 어카운팅 컨피그레이션)에서 사전 인증 ACL도 구성할 수 있습니다. 이 ACL을 사용하면 DHCP, DNS 또는 PSN IP 주소를 초과하는 프로토콜에 추가 항목을 추가할 수 있습니다. 이는 네트워크 설정에서 가져오며 프로비저닝 중에 리디렉션 ACL에 추가됩니다. 이 기능은 Cisco Catalyst Center 버전 2.3.3.x 이상에서 사용할 수 있습니다.



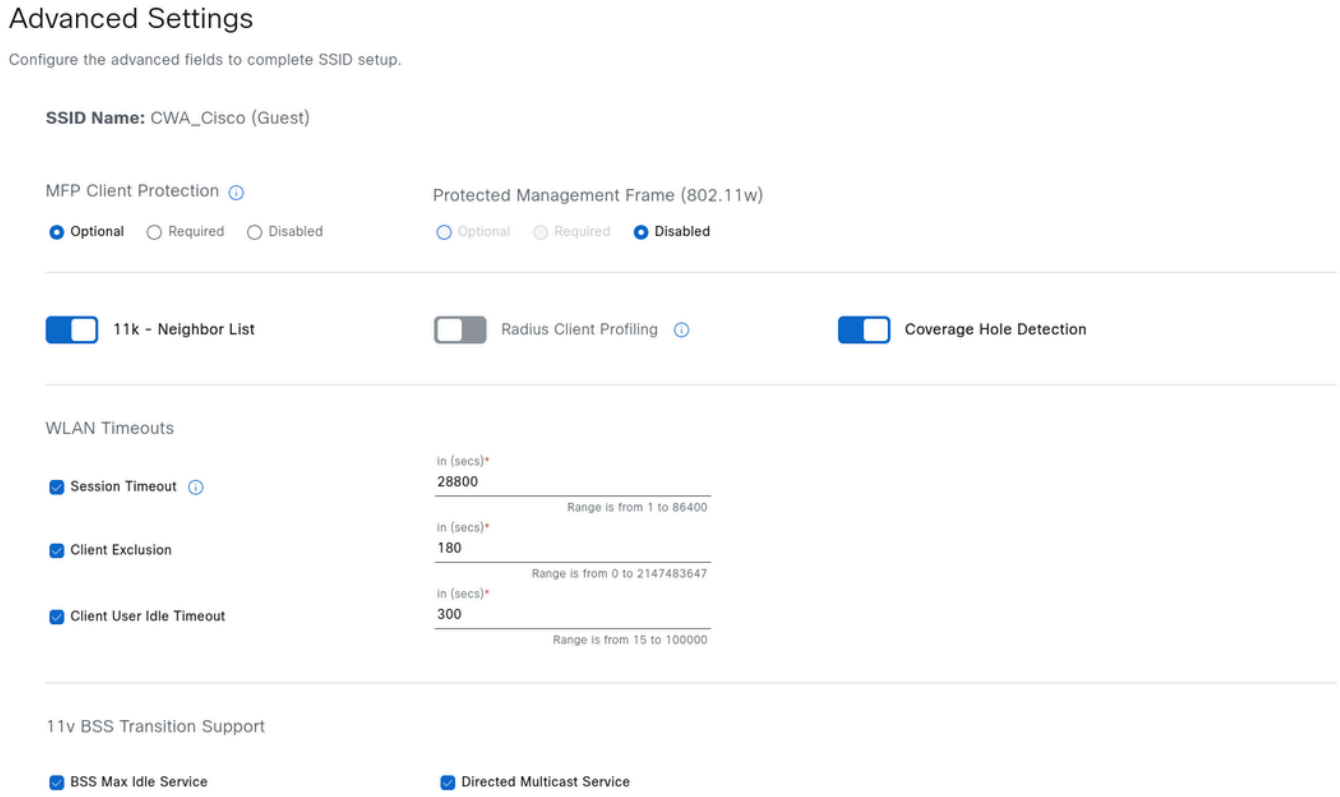
사전 인증 ACL을 구성하려면 Design(설계) > Network Settings(네트워크 설정) > Wireless(무선) > Security Settings(보안 설정)로 이동하고 Add(추가)를 클릭합니다.



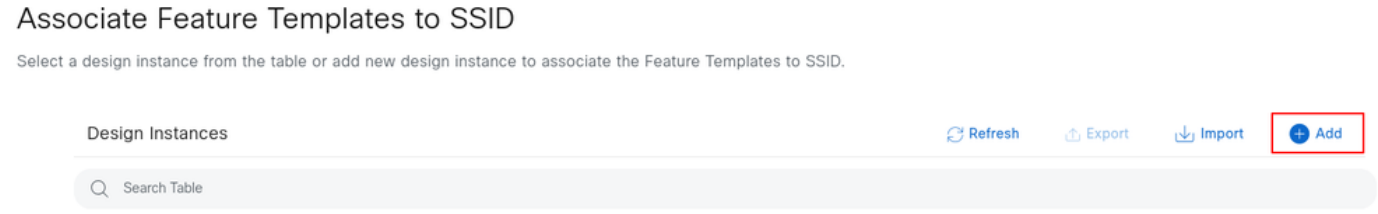
첫 번째 이름은 Catalyst Center에서 ACL을 식별하고, 두 번째 이름은 WLC의 ACL 이름에 해당합니다. 두 번째 이름은 WLC에 구성된 기존 리디렉션 ACL과 일치할 수 있습니다. 참고로 Catalyst Center는 WLC에 Cisco DNA_ACL_WEBAUTH_REDIRECT라는 이름을 프로비저닝합니다. 사전 인증 ACL의 항목은 기존 항목 뒤에 추가됩니다.



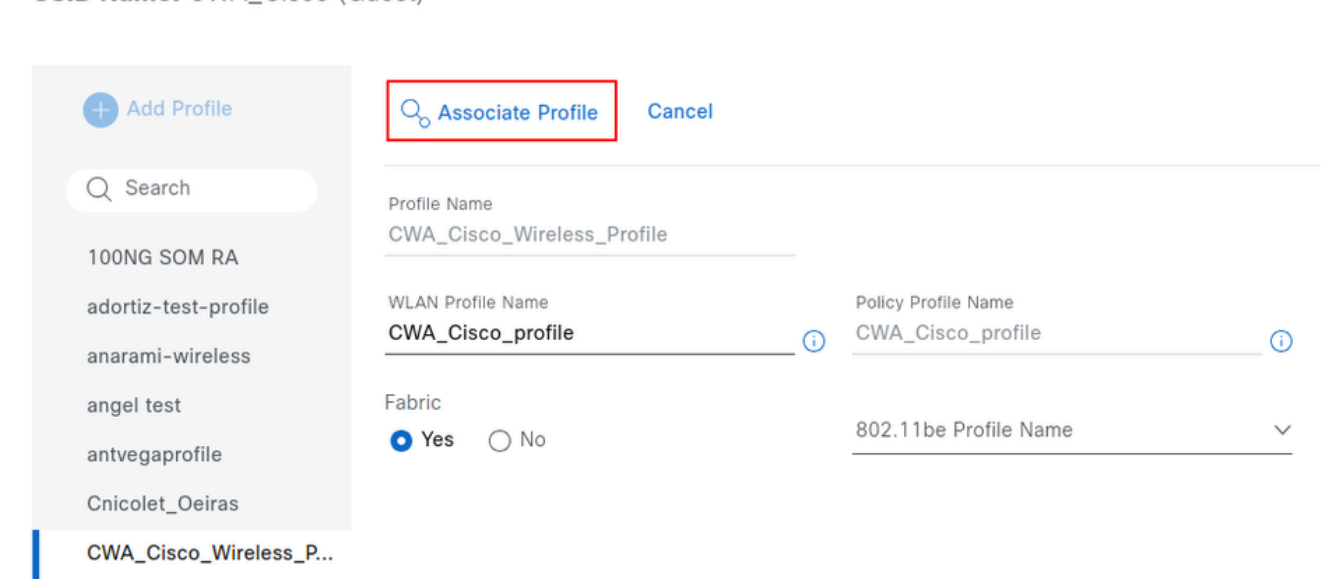
SSID 생성 워크플로로 돌아가서 Next를 선택하면 빠른 전환, 세션 시간 초과, 클라이언트 사용자 시간 초과, 속도 제한 등의 고급 설정이 표시됩니다. 필요에 따라 매개변수를 조정한 다음 다음을 선택하여 진행합니다. 이 컨피그레이션 가이드에서는 기본 설정을 유지합니다.



Next(다음)를 선택하면 모든 기능 템플릿을 SSID와 연결하라는 프롬프트가 나타납니다. 필요한 경우 Add(추가)를 클릭하여 원하는 템플릿을 선택하고 완료되면 Next(다음)를 클릭합니다.



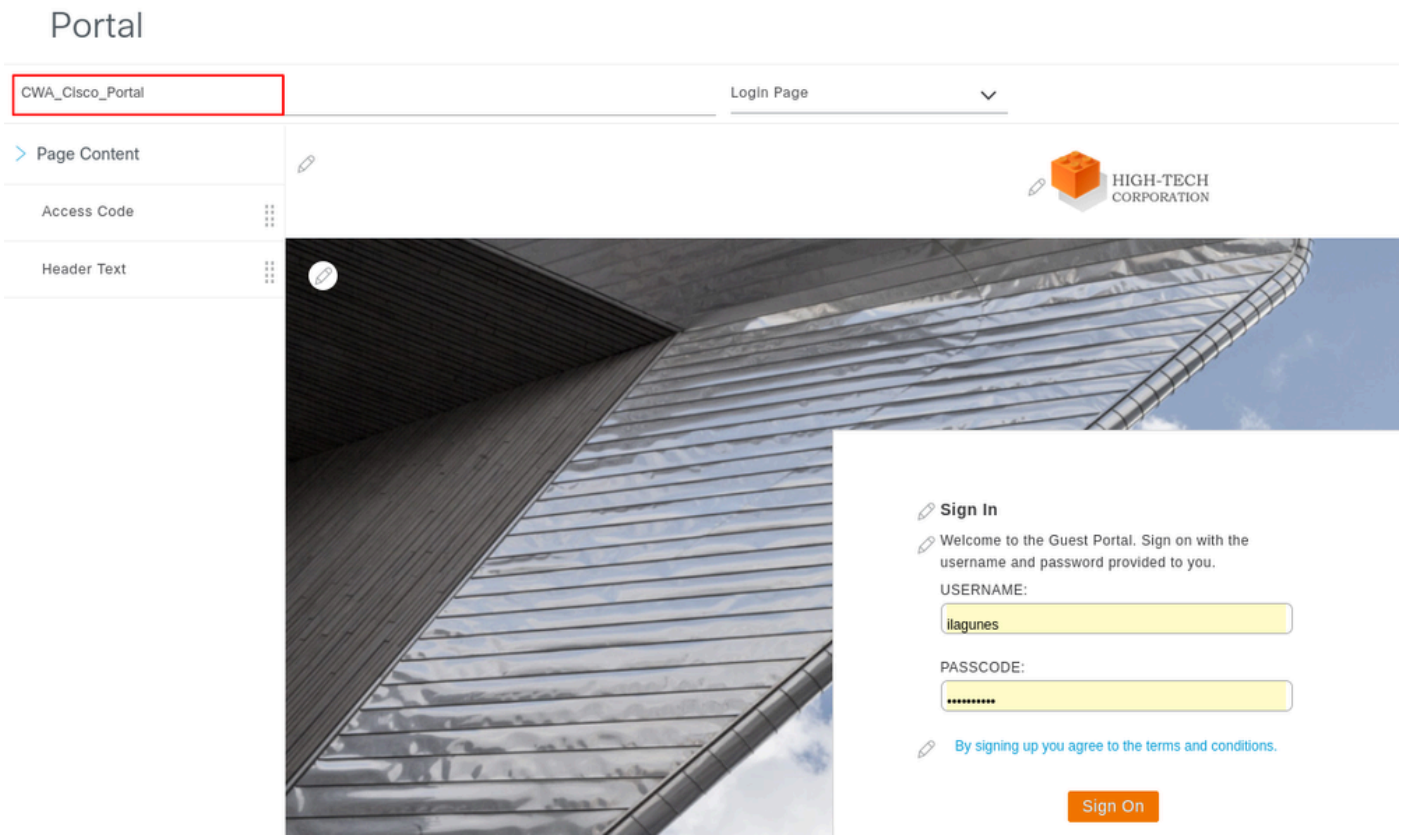
SSID를 이전에 생성한 무선 프로파일과 연결합니다. 자세한 내용은 무선 네트워크 프로파일 생성 섹션을 참조하십시오. 이 섹션에서는 SSID가 패브릭을 활성화했는지 여부를 선택할 수도 있습니다. 완료되면 Associate profile(프로필 연결)을 클릭합니다.



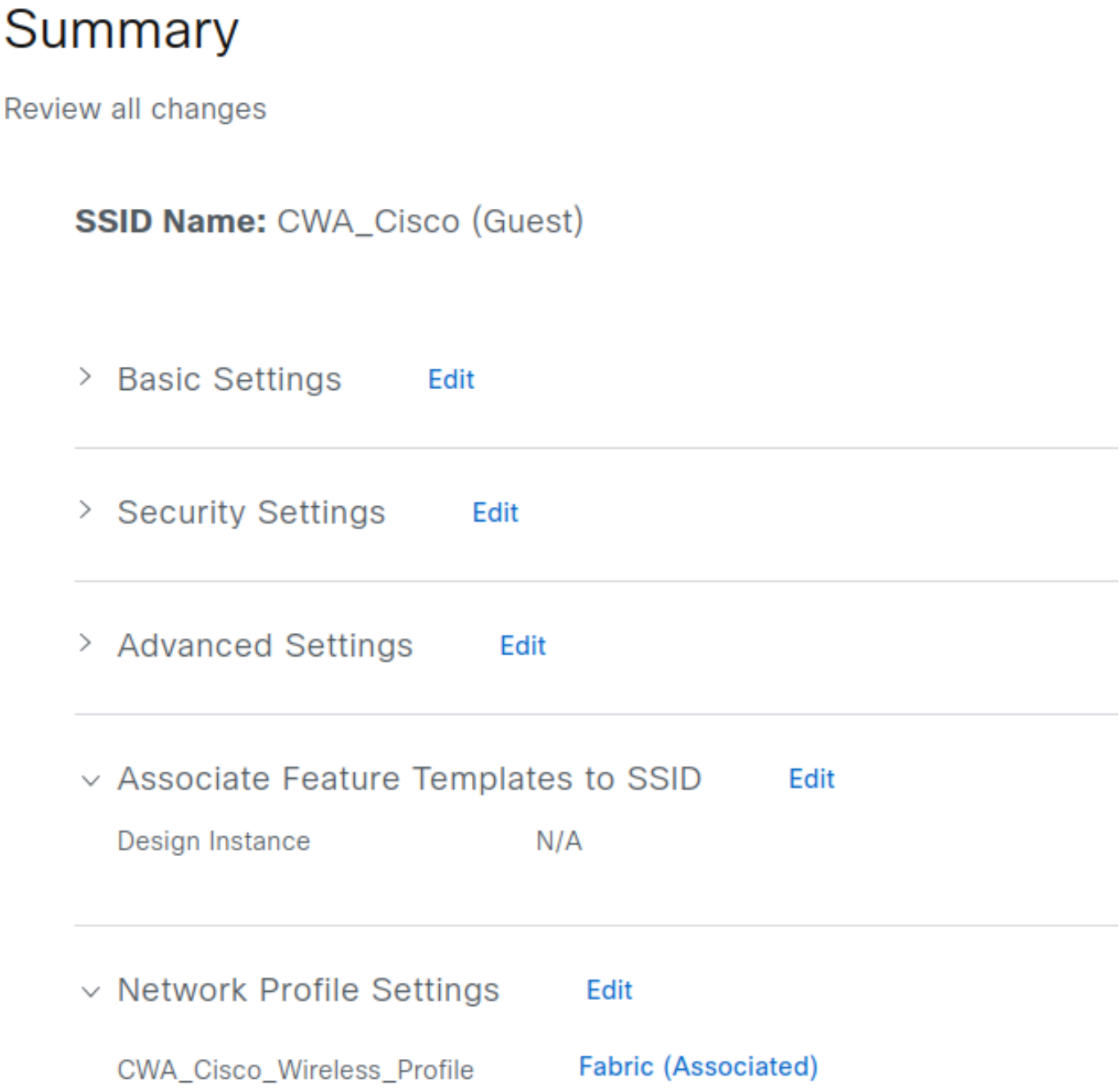
무선 관리 신뢰 지점 표시

프로파일이 SSID와 연결되면 다음을 클릭하여 종속 포털을 생성 및 설계하고 시작하려면 Create Portal(포털 생성)을 클릭합니다.

포털 이름은 FQDN의 도메인 이름과 ISE의 정책 집합 이름을 정의합니다. 완료되면 Save(저장)를 클릭합니다. 포털은 편집 가능한 상태로 유지되며 필요한 경우 삭제할 수 있습니다.



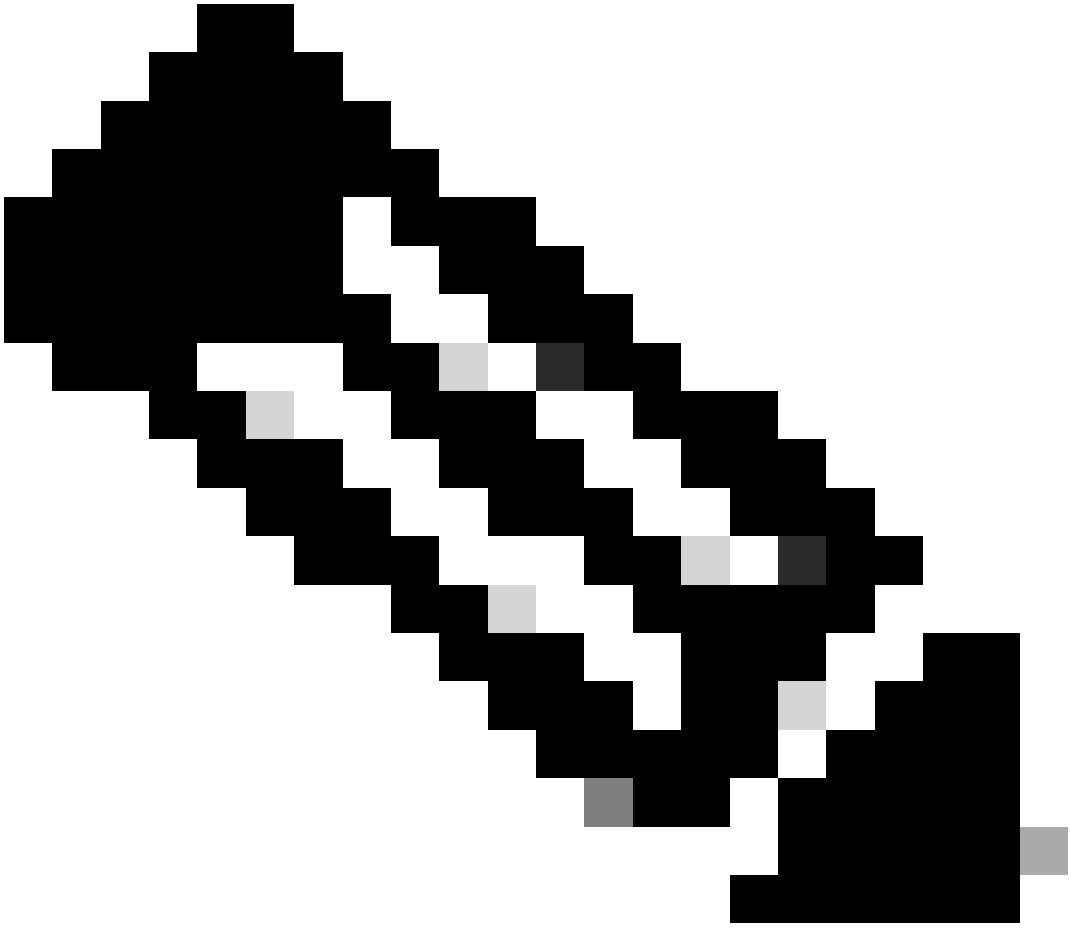
이전 단계에서 정의된 모든 컨피그레이션 매개변수의 요약을 표시하려면 다음을 선택합니다.



컨피그레이션 세부사항을 확인한 다음 저장을 선택하여 변경 사항을 적용합니다.

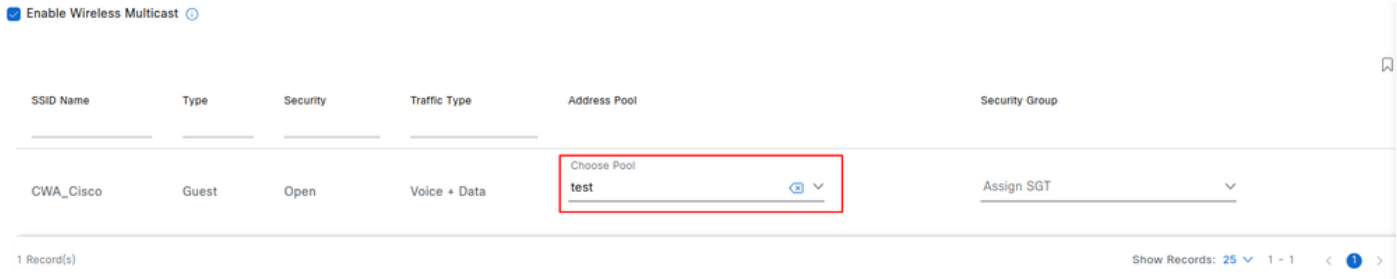
패브릭 프로비저닝

무선 네트워크 프로파일을 패브릭 사이트와 연결한 후 SSID가 Provision(프로비저닝) > Fabric Sites(패브릭 사이트) > (Your site)(사용자 사이트) > Wireless SSIDs(무선 SSID) 아래에 나타납니다.

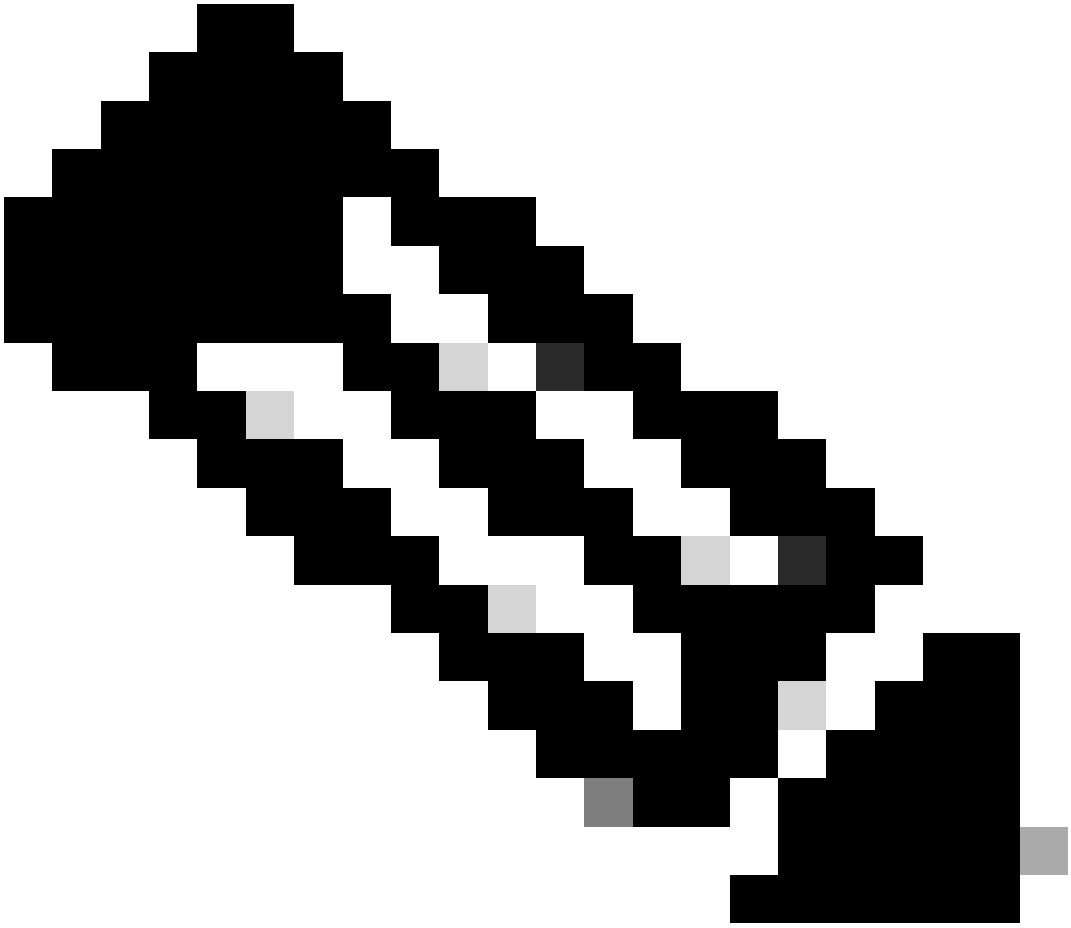


참고: Wireless SSIDs(무선 SSID)에 표시할 SSID에 대한 사이트에 무선 LAN 컨트롤러를 제공해야 합니다

SSID 풀을 선택하고 선택적으로 보안 그룹 태그를 연결한 다음 Deploy를 클릭합니다. 풀이 할당된 경우에만 액세스 포인트가 SSID를 브로드캐스트합니다.



AireOS 및 Catalyst 9800 컨트롤러에서 네트워크 설정에서 SSID 컨피그레이션이 변경된 후 Wireless LAN Controller를 다시 프로비저닝합니다.



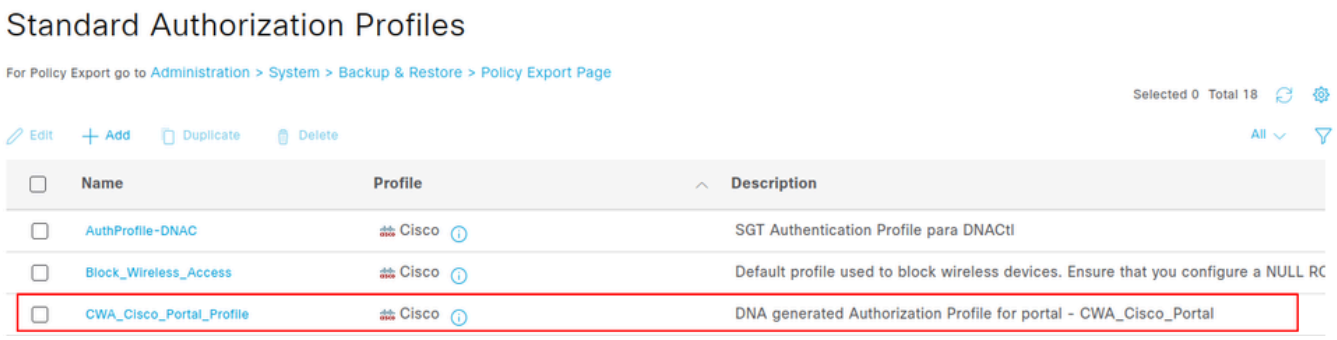
참고: 풀이 SSID에 할당되지 않은 경우 AP가 풀을 브로드캐스트하지 않을 것으로 예상됩니다. SSID는 풀이 할당된 후에만 브로드캐스트됩니다. 풀이 할당되면 컨트롤러를 다시 프로비저닝할 필요가 없습니다.

Cisco ISE에 프로비저닝된 컨피그레이션을 검토합니다.

이 섹션에서는 Catalyst Center에서 Cisco ISE에 프로비저닝한 컨피그레이션에 대해 살펴봅니다.

권한 부여 프로파일

Catalyst Center가 Cisco ISE에 프로비저닝하는 컨피그레이션의 일부가 권한 부여 프로파일입니다. 이 프로파일은 해당 매개변수를 기반으로 클라이언트에 할당된 결과를 정의하며 VLAN 할당, ACL 또는 URL 리디렉션과 같은 특정 설정을 포함할 수 있습니다.
ISE에서 권한 부여 프로파일을 보려면 Policy(정책) > Policy Elements(정책 요소) > Results(결과)로 이동합니다. 포털 이름이 CWA_Cisco_Portal이면 프로필 이름은 CWA_Cisco_Portal_Profile입니다. 설명 필드에 다음 텍스트가 표시됩니다. 포털 - CWA_Cisco_Portal에 대한 DNA 생성 권한 부여 프로파일.



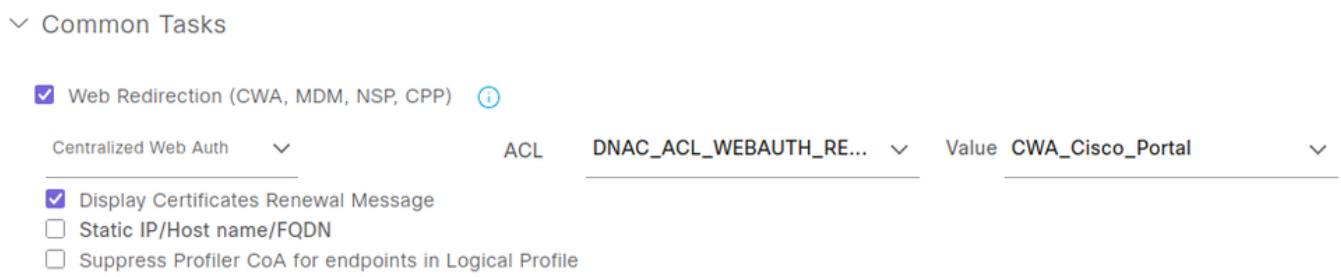
이 권한 부여 프로파일로 Wireless LAN Controller에 전송된 특성을 보려면 권한 부여 프로파일 이름을 클릭하고 일반 작업 섹션을 참조하십시오.
이 권한 부여 프로파일은 리디렉션 ACL 및 리디렉션 URL을 제공합니다.

웹 리디렉션 특성에는 두 가지 매개 변수가 포함됩니다.

1. ACL Name(ACL 이름): Cisco DNA_ACL_WEBAUTH_REDIRECT로 설정합니다.
2. 값: 종속 포털의 이름을 나타냅니다(이 예에서는 CWA_Cisco_Portal).

Display Certificates Renewal Message(인증서 갱신 메시지 표시) 옵션을 사용하면 엔드포인트가 현재 사용 중인 인증서를 갱신하는 데 포털을 사용할 수 있습니다.

추가 옵션인 Static IP/Host Name/FQDN은 Display Certificates Renewal Message(인증서 갱신 메시지 표시)에서 사용할 수 있습니다. 이 기능을 사용하면 FQDN 대신 포털의 IP 주소를 전달할 수 있습니다. 이는 종속 포털이 DNS 서버에 연결할 수 없어 로드할 수 없는 경우에 유용합니다.



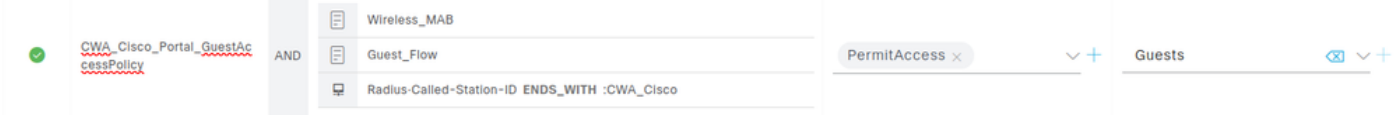
정책 집합

Policy(정책) > Policy Sets(정책 집합) > Default(기본값) > Authorization Policy(권한 부여 정책)로 이동하여 CWA_Cisco_Portal이라는 포털에 대해 생성된 두 정책 집합을 확인합니다. 이러한 정책 집합은 다음과 같습니다.

- CWA_Cisco_Portal_GuestAccessPolicy
- Cisco_Cisco_Portal_RedirectPolicy

클라이언트가 자체 등록 또는 핫스팟 포털을 통해 웹 인증 프로세스를 이미 완료한 경우

CWA_Cisco_Portal_GuestAccessPolicy 정책이 적용됩니다.

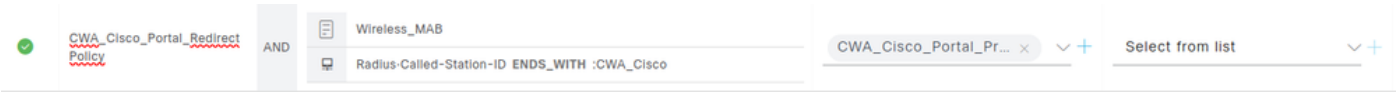


이 정책 집합은 세 가지 기준과 일치합니다.

- Wireless_MAB: Cisco ISE가 무선 LAN 컨트롤러에서 MAB(MAC Authentication Bypass) 인증 요청을 수신할 때 사용됩니다.
- Guest_Flow: GuestEndpoints ID 그룹에 대해 엔드포인트의 MAC 주소를 확인하는 ISE를 참조합니다. 엔드포인트 MAC 주소가 이 그룹에 없으면 정책이 적용되지 않습니다.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-ID는 브리지 또는 액세스 포인트 MAC 주소를 ASCII 형식으로 저장하고 액세스 중인 SSID를 세미콜론(:)으로 구분하여 추가하는 ISE의 RADIUS 특성입니다. 이 예에서 CWA_Cisco는 SSID 이름을 나타냅니다.

PermitAccess라는 이름이 표시된 열 프로필 아래에 있는 예약된 권한 부여 프로필로, 편집할 수 없으며 네트워크에 대한 전체 액세스 권한을 제공하며 Security Groups(보안 그룹) 열 아래에 SGT를 할당할 수도 있습니다(이 경우 Guests).

PermitAccess 프로필이 사용됩니다. 이는 수정할 수 없는 예약된 권한 부여 프로파일이며 네트워크에 대한 전체 액세스 권한을 부여합니다. SGT는 Security Groups(보안 그룹) 열 아래에도 할당할 수 있습니다. 이 경우 SGT는 Guests로 설정됩니다.
검토할 다음 정책은 CWA_Cisco_Portal_RedirectPolicy입니다.



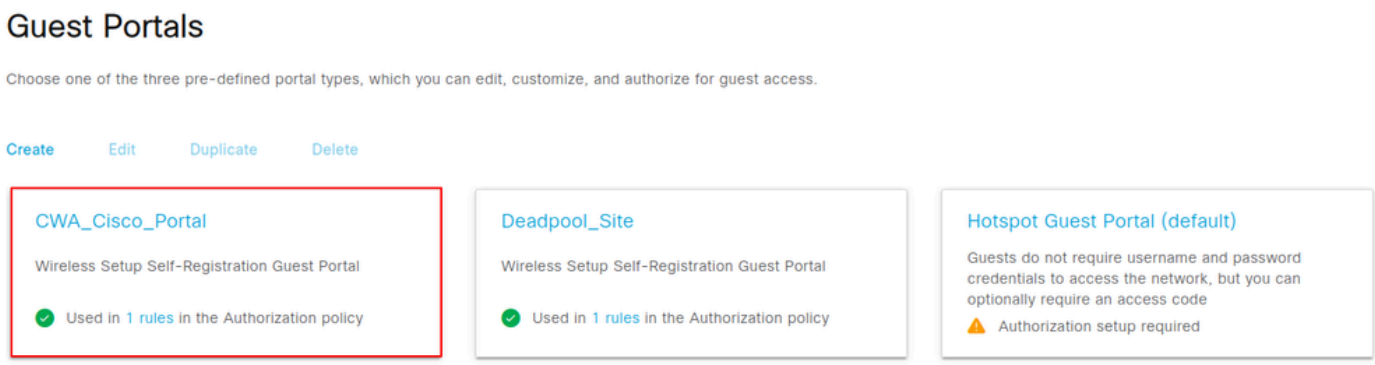
이 정책 집합은 다음 두 가지 기준과 일치합니다.

- Wireless_MAB: Cisco ISE가 무선 LAN 컨트롤러에서 MAB 인증 요청을 받을 때 사용됩니다.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-ID는 브리지 또는 액세스 포인트 MAC 주소를 ASCII 형식으로 저장하고 액세스 중인 SSID를 세미콜론(:)으로 구분하여 추가하는 ISE의 RADIUS 특성입니다. 이 예에서 :CWA_Cisco는 SSID 이름을 나타냅니다.

이러한 정책의 순서는 매우 중요합니다. CWA_Cisco_Portal_RedirectPolicy가 목록에 먼저 나타나면 RADIUS 특성 Called-Station-ID ENDS_WITH :CWA_Training을 사용하여 MAB 인증 및 SSID 이름만 확인합니다. 이 컨피그레이션에서는 엔드포인트가 포털을 통해 이미 인증된 경우에도 이 정책과 무기한 매칭이 계속됩니다. 따라서 PermitAccess 프로필을 통해 전체 액세스 권한이 부여되지 않으며 클라이언트는 인증 및 포털로의 리디렉션의 연속 루프에 머물러 있습니다.

게스트 포털 컨피그레이션

Work Centers(작업 센터) > Guest Access(게스트 액세스) > Portals & Components(포털 및 구성 요소)로 이동하여 포털을 봅니다.
여기서 생성한 게스트 포털은 Catalyst Center CWA_Cisco_Portal에서와 동일한 이름을 사용합니다. 추가 세부 정보를 보려면 포털 이름을 선택합니다.

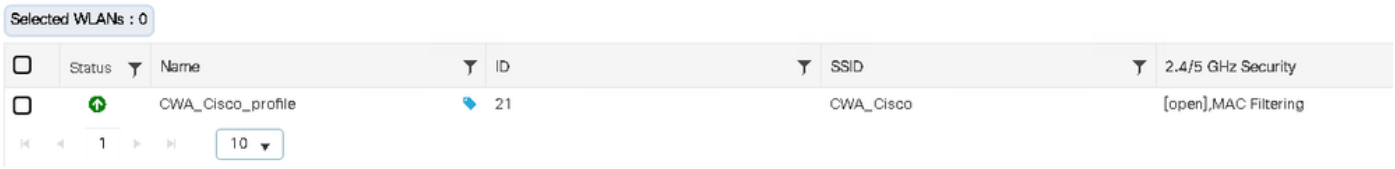


WLC에 프로비저닝된 컨피그레이션을 검토합니다.

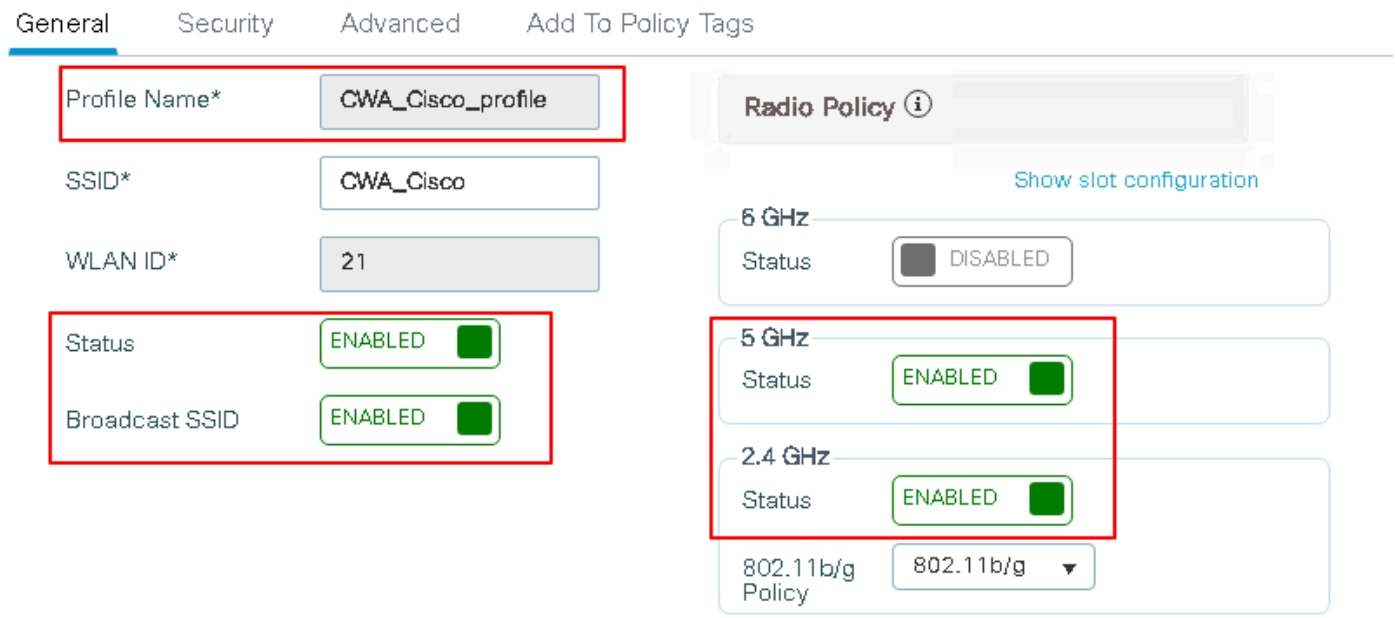
이 섹션에서는 Catalyst Center에서 무선 LAN 컨트롤러에 프로비저닝한 컨피그레이션에 대해 살펴봅니다.

SSID 컨피그레이션

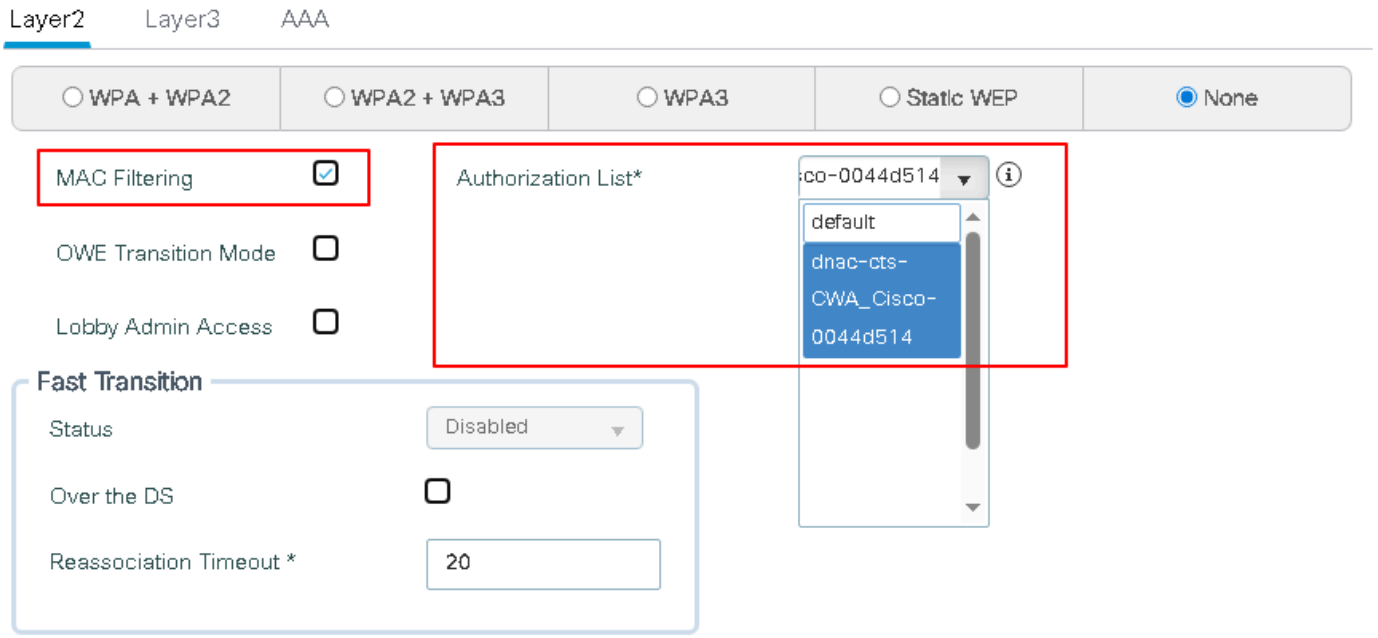
WLC GUI에서 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동하여 SSID 컨피그레이션을 확인합니다.



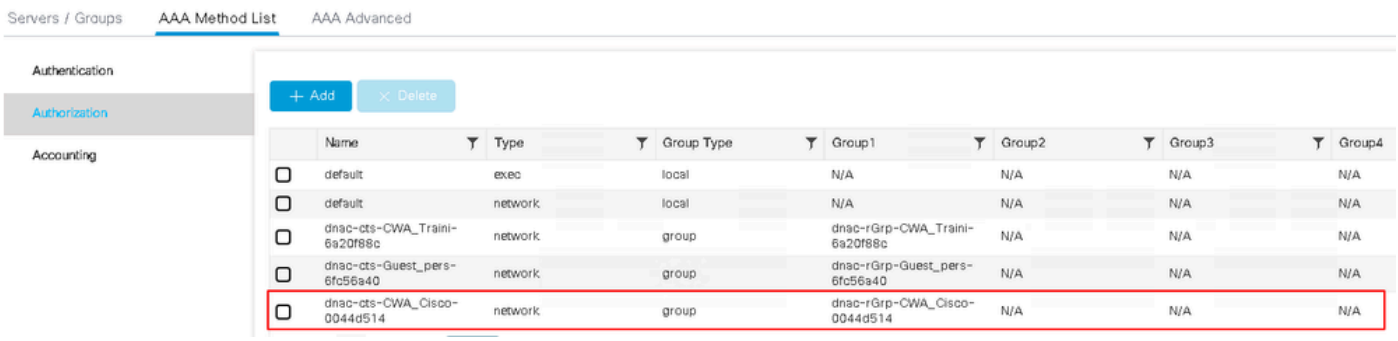
SSID CWA_Cisco는 WLC에서 이름 CWA_Cisco_profile을 가지며, ID는 21이고 MAC 필터링을 사용하는 Open 보안 유형입니다. SSID를 두 번 클릭하여 컨피그레이션을 확인합니다.



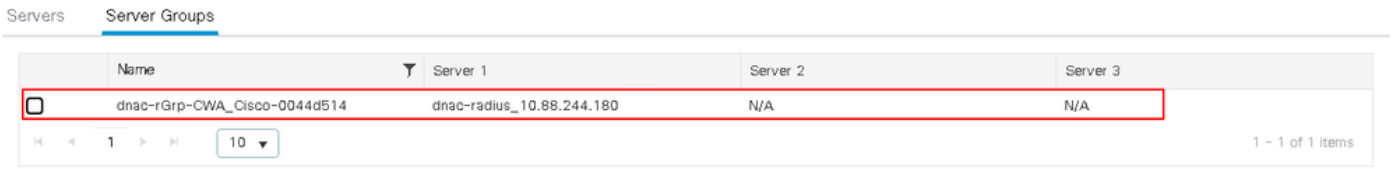
SSID는 5GHz 및 2.4GHz 채널에서 UP 및 브로드캐스트되며 정책 프로파일 CWA_CIsco_Profile에 연결됩니다. 설정을 보려면 보안 탭을 클릭합니다.



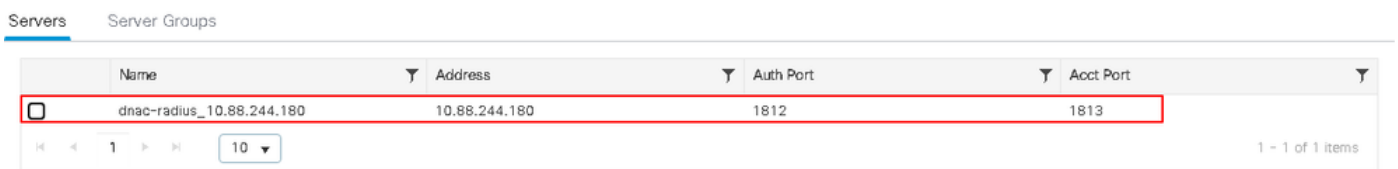
주요 설정에는 레이어 2 보안 방법(MAC 필터링) 및 AAA 권한 부여 목록(Cisco DNA-cts-CWA_Cisco-0044d514)이 포함됩니다. 컨피그레이션을 검토하려면 Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여)으로 이동합니다.



이 방법 목록은 Group1 열의 RADIUS 그룹 Cisco DNA-rGrp-CWA_Cisco-0044d514를 가리킵니다. 컨피그레이션을 보려면 Configuration(컨피그레이션) > Security(보안) > AAA > Server/Groups(서버/그룹) > Server Groups(서버 그룹)로 이동합니다.



서버 그룹 Cisco DNA-rGrp-CWA_Cisco-0044d514는 서버 1 열에서 Cisco DNA-radius_10.88.244.180을 가리킵니다. Servers(서버) 탭에서 컨피그레이션을 확인합니다.



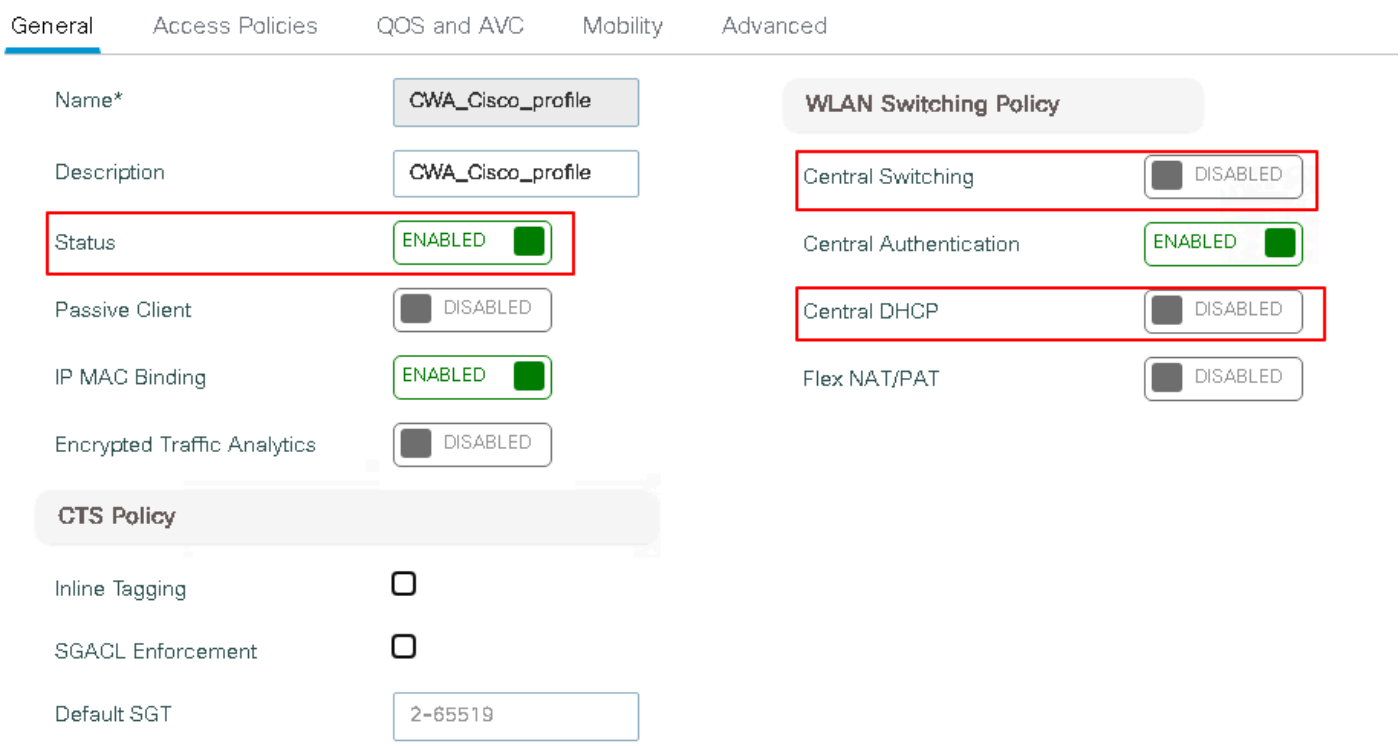
서버 Cisco DNA-radius_10.88.244.180의 IP 주소는 10.88.244.180입니다. 컨피그레이션을 보려면 이름을 클릭하십시오.

중요한 컨피그레이션은 종속 포털에서 인증된 후 AAA(Authentication, Authorization, and Accounting) 세션의 특성을 수정할 수 있는 메커니즘을 제공하는 CoA(Change of Authorization)입니다. 이 기능을 사용하지 않으면 엔드포인트는 포털에서 등록을 완료한 후에도 웹 인증 보류 상태로 유지됩니다.

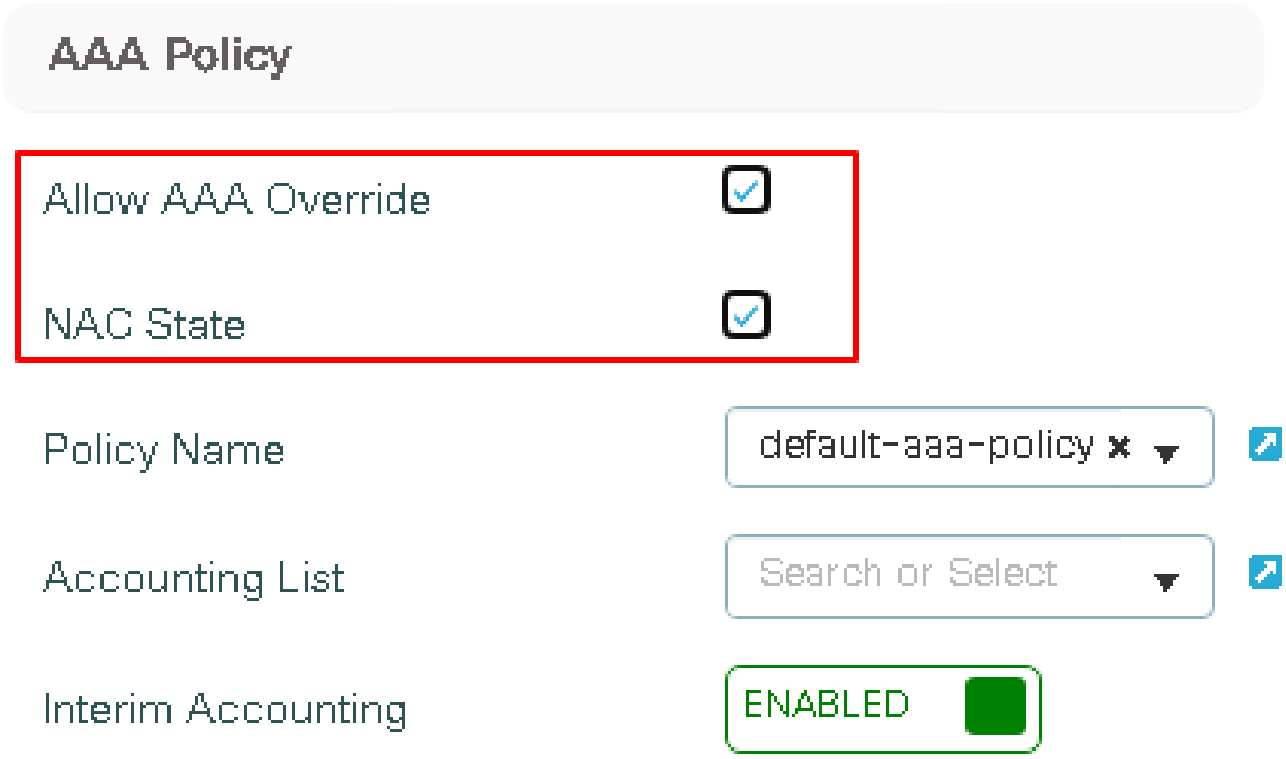
무선 정책 프로파일 컨피그레이션

정책 프로필 내에서 클라이언트에는 VLAN, ACL, QoS, Mobility Anchor, 타이머와 같은 설정을 할당할 수 있습니다. 정책 프로필에 대한 컨피그레이션을 보려면 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다.

컨피그레이션을 보려면 정책 이름을 클릭합니다.



정책 상태는 Enabled(활성화됨)이고 패브릭 SSID, 중앙 스위칭 및 중앙 DHCP와 마찬가지로 비활성화됩니다. Advanced(고급) 탭을 클릭한 다음 AAA Policy(AAA 정책) 섹션으로 이동하여 추가 컨피그레이션 세부 정보를 봅니다.



AAA 재정의와 NAC(Network Access Control)를 모두 활성화할 수 있습니다. AAA Override를 사용하면 컨트롤러가 RADIUS 서버에서 반환하는 특성(예: ACL 또는 URL)을 수락하고 이러한 특성을 클라이언트에 적용할 수 있습니다. NAC는 클라이언트가 포털에 등록 한 후 CoA (Change of Authorization) 를 활성화 합니다.
이 컨피그레이션은 WLC의 CLI를 통해서도 볼 수 있습니다.

정책 프로필을 확인하려면 SSID를 연결하여 명령을 실행합니다.

<#root>

```
WLC#show fabric wlan summary


Number of Fabric wlan : 1

WLAN  Profile Name       SSID       Status
------------------------------------------------------------------------------
21
CWA_Cisco_profile

  CWA_Cisco  UP
```

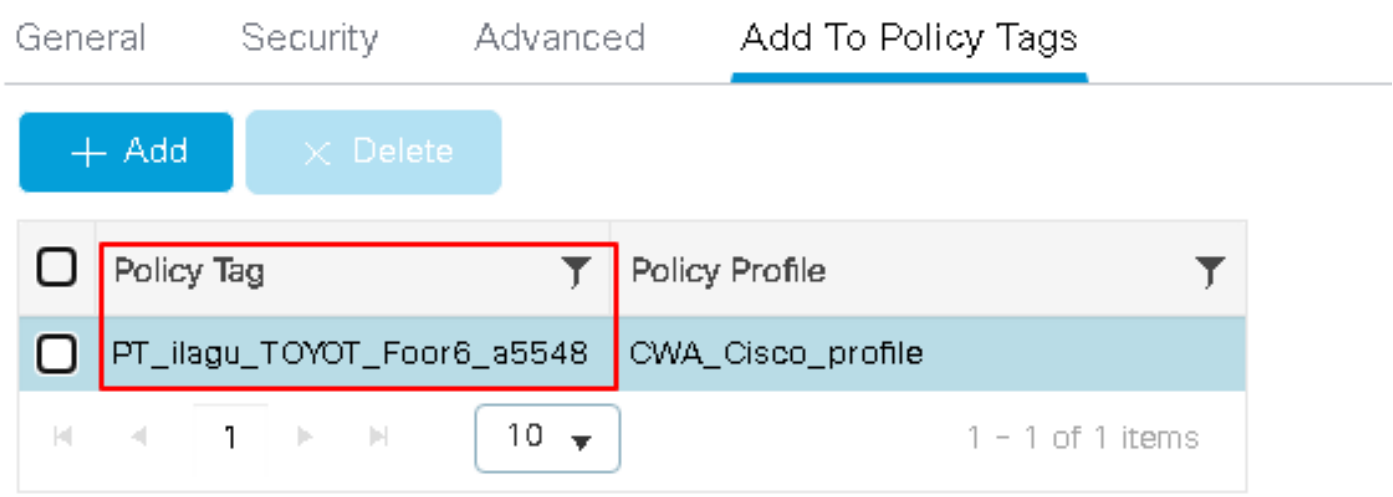
정책 프로필 CWA_Cisco_profile에 대한 컨피그레이션을 보려면 다음 명령을 실행합니다.

<#root>

```
WLC#show running-config | section policy CWA_Cisco_profile


wireless profile policy CWA_Cisco_profile

 aaa-override


 no central dhcp


 no central switching


 description CWA_Cisco_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric CWA_Cisco_profile
 http-tlv-caching

 nac


 service-policy input platinum-up
 service-policy output platinum
 no shutdown
```

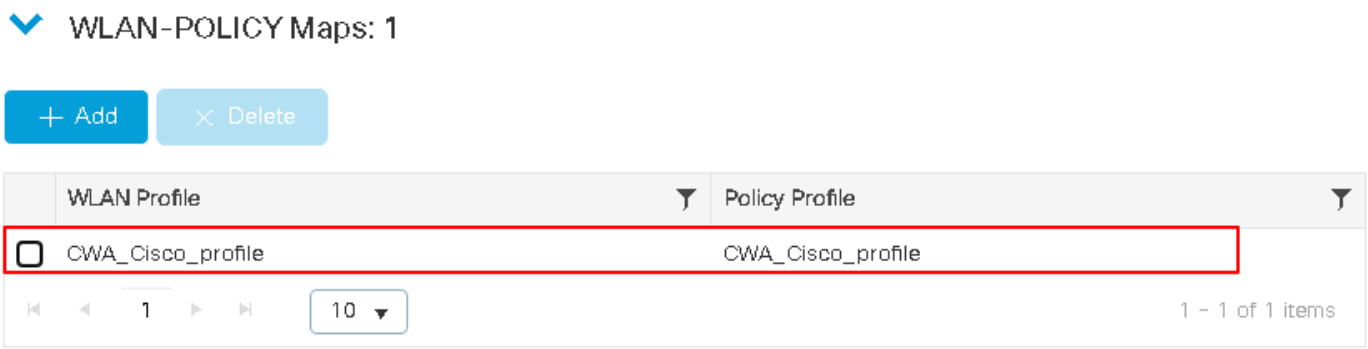
정책 태그 구성

정책 태그는 WLAN을 Policy Profile(정책 프로파일)과 링크하고 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > WLANs(WLAN)로 이동한 다음 WLAN 이름을 클릭하고 Add to Policy Tags(정책 태그에 추가)로 이동하여 SSID에 할당된 정책 태그를 식별하는 방법입니다.



SSID CWA_Cisco_profile의 경우 정책 태그 PT_ilagu_TOYOT_For6_a5548을 사용하여 이 컨피그레이션을 확인합니다. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Policy(정책)로 이동합니다.

세부 정보를 보려면 이름을 클릭합니다. 정책 태그 PT_ilagu_TOYOT_For6_a5548은 WLC의 이름 CWA_Cisco_profile과 연결된 WLAN CWA_Cisco를 정책 프로파일 CWA_Cisco_profile에 연결합니다(WLAN 페이지 참조).

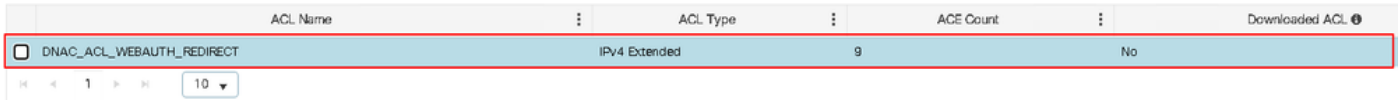


WLAN 이름 CWA_Cisco_profile은 WLAN CWA_Cisco를 참조합니다.

ACL 구성 리디렉션

CWA에서 Redirect Access Control List(리디렉션 액세스 제어 목록)는 추가 처리를 위해 WLC로 리디렉션되는 트래픽과 리디렉션을 우회하는 트래픽을 정의합니다
이 컨피그레이션은 SSID를 생성하고 인벤토리에서 WLC를 프로비저닝한 후 WLC에 푸시됩니다. 이를 보려면 Configuration(컨피그레이션) > Security(보안) >ACL(ACL)로 이동합니다. Catalyst Center에서 리디렉션 ACL에 사용하는 ACL의 이름은 Cisco DNA_ACL_WEBAUTH_REDIRECT입

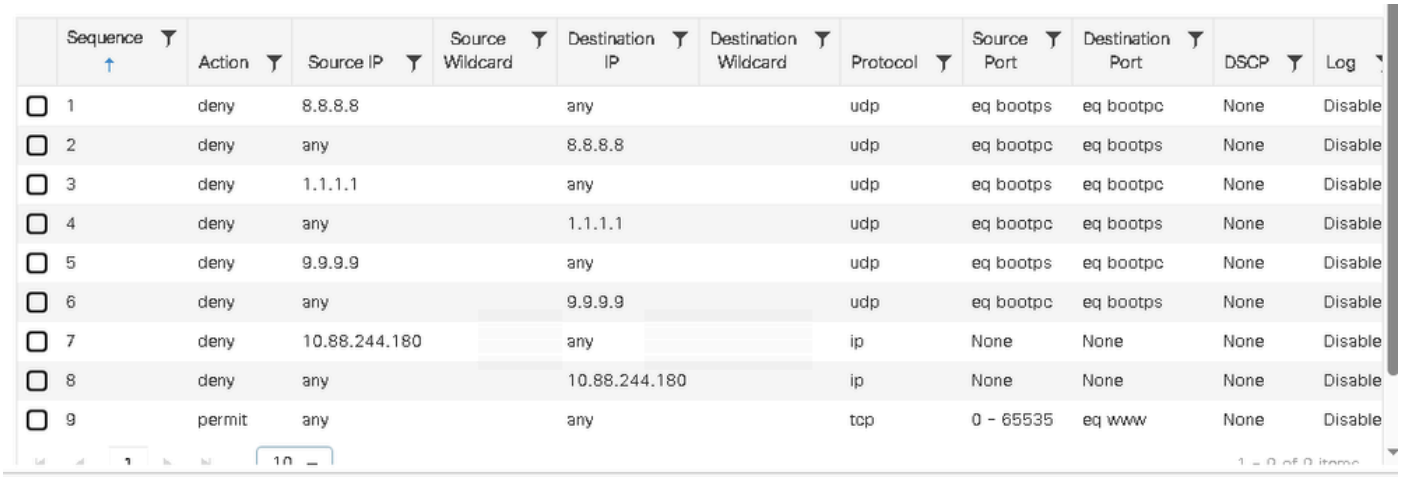
니다.



ACL Name	ACL Type	ACE Count	Downloaded ACL
DNAC_ACL_WEBAUTH_REDIRECT	IPv4 Extended	9	No

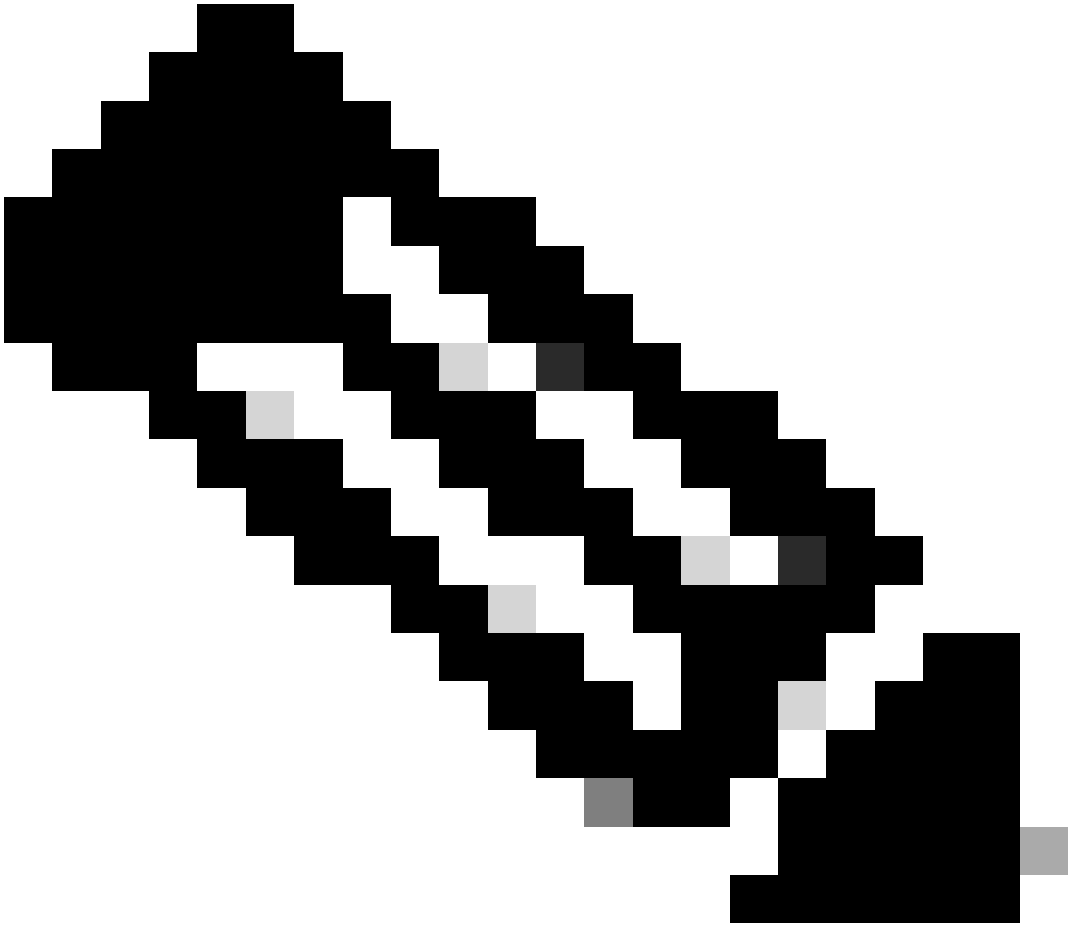
1 10

컨피그레이션을 보려면 이름을 클릭합니다. 값은 Catalyst Center의 사이트에서 네트워크 설정의 네트워크 설정에서 파생됩니다.



Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
1	deny	8.8.8.8		any		udp	eq bootps	eq bootpc	None	Disable
2	deny	any		8.8.8.8		udp	eq bootpc	eq bootps	None	Disable
3	deny	1.1.1.1		any		udp	eq bootps	eq bootpc	None	Disable
4	deny	any		1.1.1.1		udp	eq bootpc	eq bootps	None	Disable
5	deny	9.9.9.9		any		udp	eq bootps	eq bootpc	None	Disable
6	deny	any		9.9.9.9		udp	eq bootpc	eq bootps	None	Disable
7	deny	10.88.244.180		any		ip	None	None	None	Disable
8	deny	any		10.88.244.180		ip	None	None	None	Disable
9	permit	any		any		tcp	0 - 65535	eq www	None	Disable

1 10



참고: 이 값은 Catalyst Center에 구성된 사이트의 네트워크 설정에서 가져오며 DHCP/DNS 값은 WLAN에 구성된 풀에서 가져옵니다. ISE PSN IP 주소는 SSID 워크플로 내의 AAA 컨피그레이션에서 참조됩니다.

WLC CLI에서 리디렉션 ACL을 보려면 다음 명령을 실행합니다.

<#root>

```
WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```

리디렉션 ACL은 Flex Profile에 적용되어 액세스 포인트로 전송될 수 있습니다. 이 명령을 실행하여 이 구성을 확인합니다.

<#root>

```
WLC#show running-config | section flex

wireless profile flex default-flex-profile
 acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT

central-webauth

urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

액세스 포인트에서 ACL 리디렉션

액세스 포인트에서 허용 및 거부 값이 반전됩니다. permit은 전달 트래픽을 나타내고 deny는 리디렉션을 나타냅니다. AP의 리디렉션 ACL에 대한 컨피그레이션을 검토하려면 다음 명령을 실행합니다 .

<#root>

```
AP#sh ip access-lists

Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
7 permit ip 10.88.244.180 0.0.0.0 any
8 permit ip any 10.88.244.180 0.0.0.0
9 deny tcp any range 0 65535 any eq 80
```

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.