외부 인증으로 로컬 웹 인증 구성

목차

소개

이 문서에서는 9800 WLC 및 ISE에서 외부 인증을 사용하여 로컬 웹 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC(Wireless LAN Controller) 컨피그레이션
- LAP(Lightweight Access Point)
- 외부 웹 서버 ISE(Identity Services Engine)를 설정 및 구성하는 방법.
- DHCP 및 DNS 서버를 설정 및 구성하는 방법.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800-40 WLC Cisco IOS® XE, 버전 17.18.4a(APSP1 및 APSP2)
- ISE(Identity Services Engine) 버전 3.2.0.542
- Cisco® Wireless 9172I Series Wi-Fi 7 Access Point, 버전 17.18.4.202

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.

웹 인증

웹 인증은 게스트 사용자가 네트워크에 액세스 할 수 있도록 하는 레이어 3 보안 기능입니다.

이 기능은 사용자 프로필을 구성할 필요 없이 개방형 SSID에 대한 쉽고 안전한 게스트 액세스를 제공하도록 설계되었으며, 레이어 2 보안 방법과도 함께 사용할 수 있습니다.

웹 인증의 목적은 보안 메커니즘으로 구성할 수 있는 게스트 WLAN을 통해 신뢰할 수 없는 디바이

스(게스트)가 제한된 네트워크 액세스 권한으로 네트워크에 액세스하도록 허용하고 네트워크 보안이 손상되지 않도록 하는 것입니다. 게스트 사용자가 네트워크에 액세스 할 수 있도록 하려면 성공적 인 인증 해야 합니다. 즉, 네트워크에 액세스 할 수 있도록 올바른 자격 증명을 제공 하거나 AUP (Acceptable Use Policy)에 수락 해야 합니다.

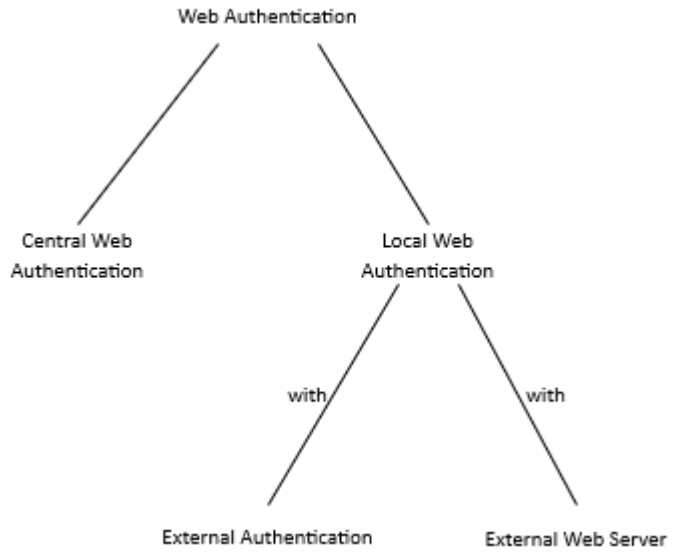
웹 인증은 사용자 충성도를 높이고, 게스트 사용자가 동의해야 하는 면책조항을 준수하도록 하며, 기업이 방문자와 교류할 수 있도록 하기 때문에 기업에게 유익합니다.

웹 인증을 구축하려면 게스트 포털 및 인증이 처리되는 방식을 고려해야 합니다. 두 가지 일반적인 방법이 있습니다.

- 로컬 웹 인증(LWA): WLC에서 포털에 직접 게스트 사용자를 리디렉션하는 방법. 리디렉션 및 사전 WebAuth ACL은 WLC에서 로컬로 구성됩니다.
- 중앙 웹 인증(CWA): 리디렉션 URL 및 리디렉션 ACL이 외부 서버(예: ISE)에서 중앙에서 구성되고 RADIUS를 통해 WLC에 전달되는 게스트 사용자의 리디렉션 방법입니다. 중앙 웹 인증에서 리디렉션 URL 및 리디렉션 ACL은 외부 서버(예: RADIUS)의 중앙에 있습니다. RADIUS 서버는 인증을 처리하는 서버이며 WLC에 명령을 보냅니다. CWA에서는 WLC에 로컬 웹 인증 인증서가 필요하지 않으며 중앙 웹 포털에 하나의 인증서만 필요하고 ISE와 같은 중앙 인증 서버가 필요합니다. CWA를 더 자세히 읽으려면 Catalyst 9800 WLC 및 ISE에서 CWA(Central Web Authentication) 구성으로 이동합니다.

로컬 웹 인증에서 웹 포털은 WLC 또는 외부 서버에 있을 수 있습니다. 외부 인증이 있는 LWA에서 웹 포털은 WLC에 있습니다. 외부 웹 서버가 있는 LWA에서 웹 포털은 외부 서버(예: Cisco DNA Spaces)에 있습니다. 외부 웹 서버가 있는 LWA의 예는 다음에서 자세히 설명합니다. Catalyst 9800 WLC로 DNA Spaces Captive Portal을 구성합니다.

여러 웹 인증 방법에 대한 다이어그램:



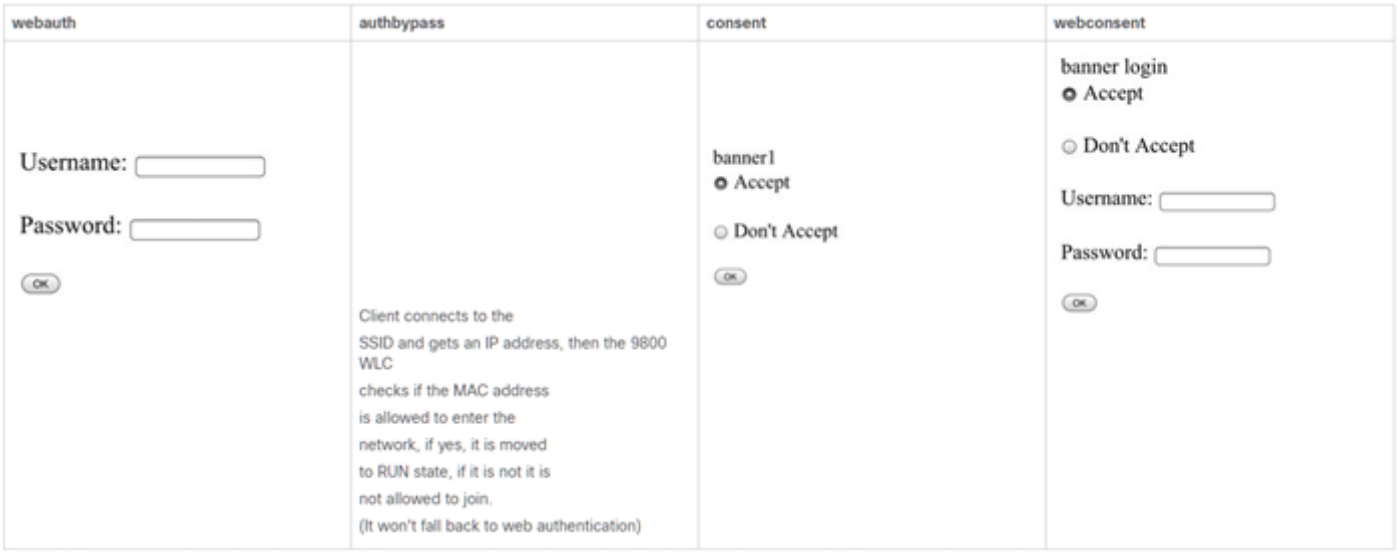
다양한 웹 인증 방법 다이어그램

참고: 9800 WLC에서 웹 인증을 사용하여 Wi-Fi 7 AP를 구축하는 경우 17.18.4a 이상과 같은 권장 Cisco IOS XE 릴리스를 실행하고 있는지 확인합니다.

인증 유형

게스트 사용자를 인증하는 인증에는 네 가지 유형이 있습니다.

- 웹 인증: 사용자 이름 및 비밀번호를 입력합니다.
- 동의(웹 통과): AUP를 수락합니다.
- Authbypass: 게스트 사용자 장치의 MAC 주소를 기반으로 하는 인증.
- 웹 동의: 사용자 이름/비밀번호와 AUP 수락 사이의 조합.



게스트 사용자 인증을 위한 4 가지 유형의 인증

인증을 위한 데이터베이스

인증용 자격 증명은 LDAP 서버, WLC 또는 RADIUS 서버에 로컬로 저장할 수 있습니다.

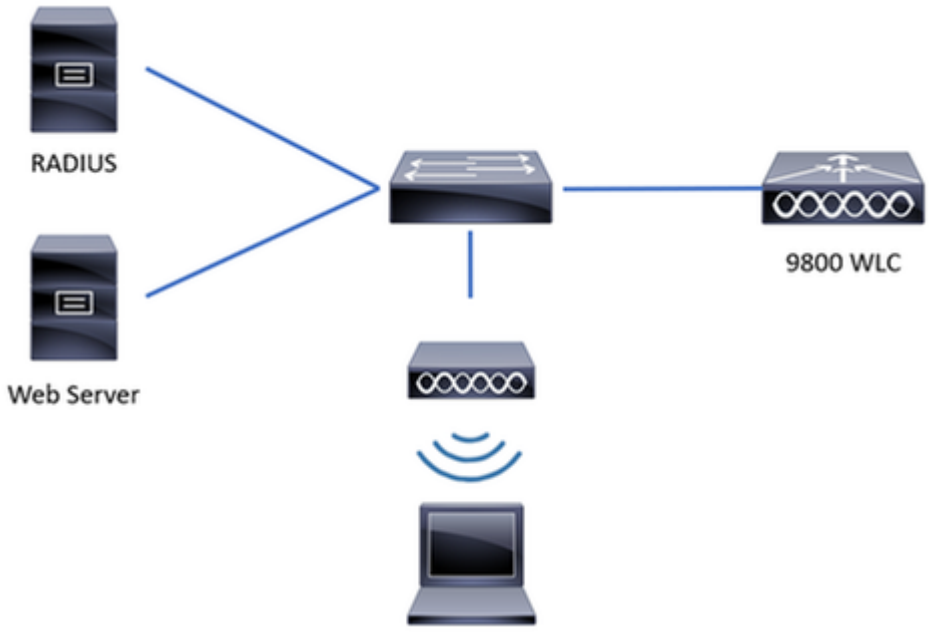
- 로컬 데이터베이스: 자격 증명(사용자 이름 및 비밀번호)은 WLC에 로컬로 저장됩니다.
- LDAP 데이터베이스: 자격 증명은 LDAP 백엔드 데이터베이스에 저장됩니다. WLC는 데이터베이스에 있는 특정 사용자의 자격 증명을 위해 LDAP 서버에 쿼리합니다.
- RADIUS 데이터베이스: 자격 증명은 RADIUS 백엔드 데이터베이스에 저장됩니다. WLC는 데이터베이스에 있는 특정 사용자의 자격 증명을 RADIUS 서버에 쿼리합니다.

로컬 웹 인증

로컬 웹 인증에서는 게스트 사용자가 WLC에서 직접 웹 포털로 리디렉션됩니다.

웹 포털은 WLC 또는 다른 서버에 있을 수 있습니다. 로컬로 만드는 것은 리디렉션 URL 및 트래픽과 일치하는 ACL이 웹 포털의 위치가 아니라 WLC에 있어야 한다는 사실입니다. LWA에서 게스트 사용자가 게스트 WLAN에 연결할 때 WLC는 게스트 사용자의 연결을 인터셉트하고 웹 포털 URL로 리디렉션합니다. 여기서 게스트 사용자는 인증을 받아야 합니다. 게스트 사용자가 자격 증명(사용자 이름 및 비밀번호)을 입력하면 WLC가 자격 증명을 캡처합니다. WLC는 LDAP 서버, RADIUS 서버 또는 로컬 데이터베이스(WLC에 로컬로 존재하는 데이터베이스)를 사용하여 게스트 사용자를 인증합니다. RADIUS 서버(ISE와 같은 외부 서버)의 경우 자격 증명을 저장할 뿐만 아니라 디바이스 등록 및 셀프 프로비저닝을 위한 옵션을 제공하는 데에도 사용할 수 있습니다. Cisco DNA Spaces와 같은 외부 웹 서버의 경우 웹 포털이 여기에 있습니다. LWA에는 WLC에 하나의 인증서가 있고 웹 포털에 다른 인증서가 있습니다.

이 이미지는 LWA의 일반 토폴로지를 나타냅니다.



LWA의 일반 토폴로지

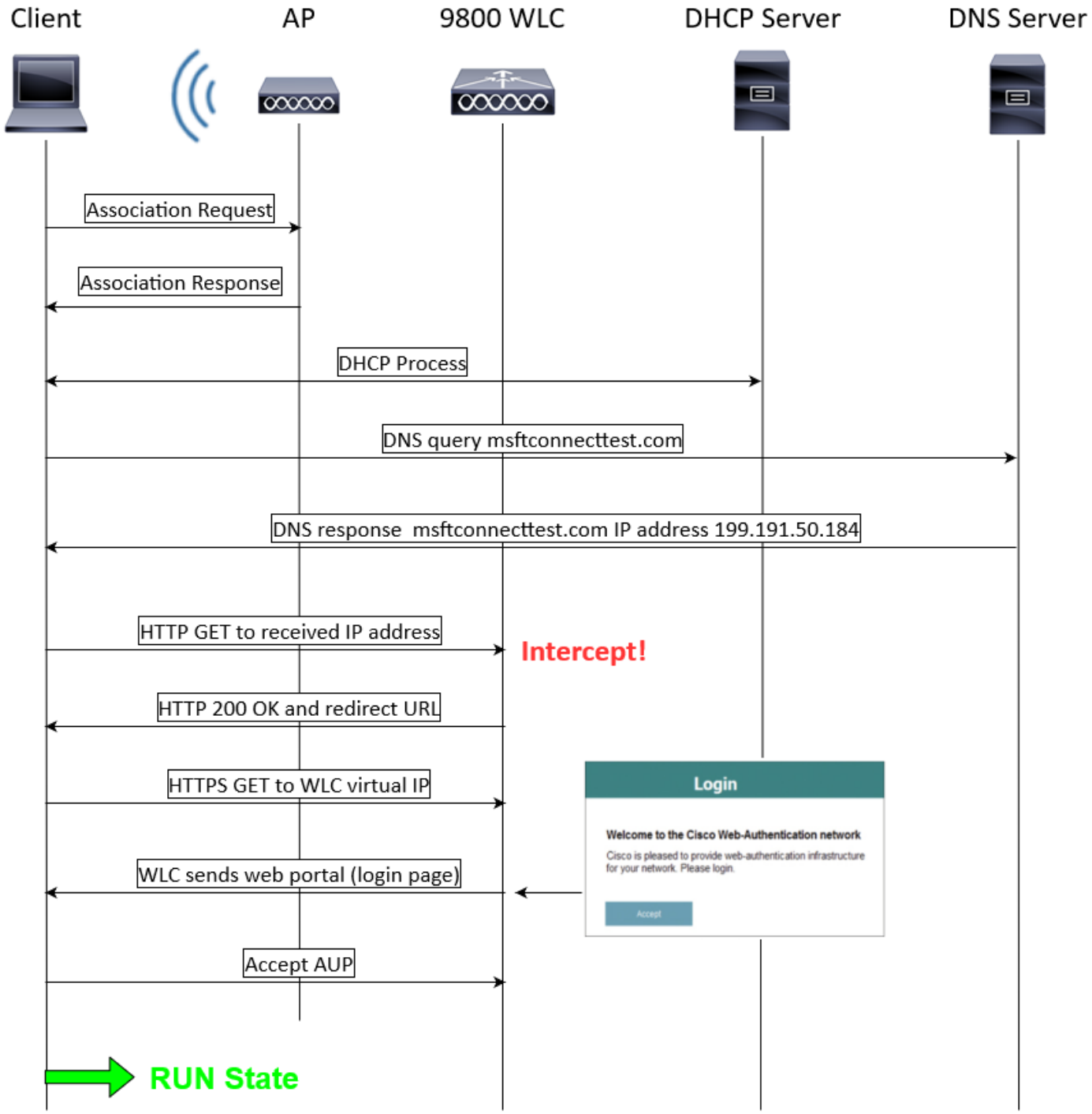
LWA의 네트워크 토폴로지에 있는 디바이스:

- 클라이언트: DHCP 및 DNS 서버에 요청을 보내고 게스트 WLAN에 대한 액세스를 요청하고 WLC의 요청에 응답합니다.
- 액세스 포인트: 스위치에 연결되어 게스트 WLAN을 브로드캐스트하고 게스트 사용자 디바이스에 무선 연결을 제공합니다. 또한 게스트 사용자가 인증되기 전에(유효한 자격 증명을 입력하기 전에) DHCP 및 DNS 패킷을 허용합니다.

- WLC: AP 및 클라이언트를 관리합니다. WLC는 리디렉션 URL 및 트래픽과 일치하는 ACL을 호스팅합니다. 게스트 사용자의 HTTP 요청을 가로채고 게스트 사용자가 인증해야 하는 웹 포털(로그인 페이지)로 리디렉션합니다. 자격 증명을 캡처하고 게스트 사용자를 인증하며 외부 서버, LDAP 서버 또는 로컬 데이터베이스에 액세스 요청을 전송하여 자격 증명이 유효한지 확인합니다.
- 인증 서버: WLC의 액세스 요청에 액세스 허용/거부를 통해 응답합니다. 인증 서버는 게스트 사용자의 자격 증명을 확인하고 자격 증명이 유효하거나 유효하지 않은 경우 WLC에 알립니다. 자격 증명이 유효한 경우 게스트 사용자는 네트워크에 액세스할 수 있는 권한이 부여됩니다(인증 서버는 디바이스 등록 및 셀프 프로비저닝에 대한 옵션을 제공합니다). 자격 증명이 유효하지 않으면 게스트 사용자가 네트워크에 대한 액세스가 거부됩니다.

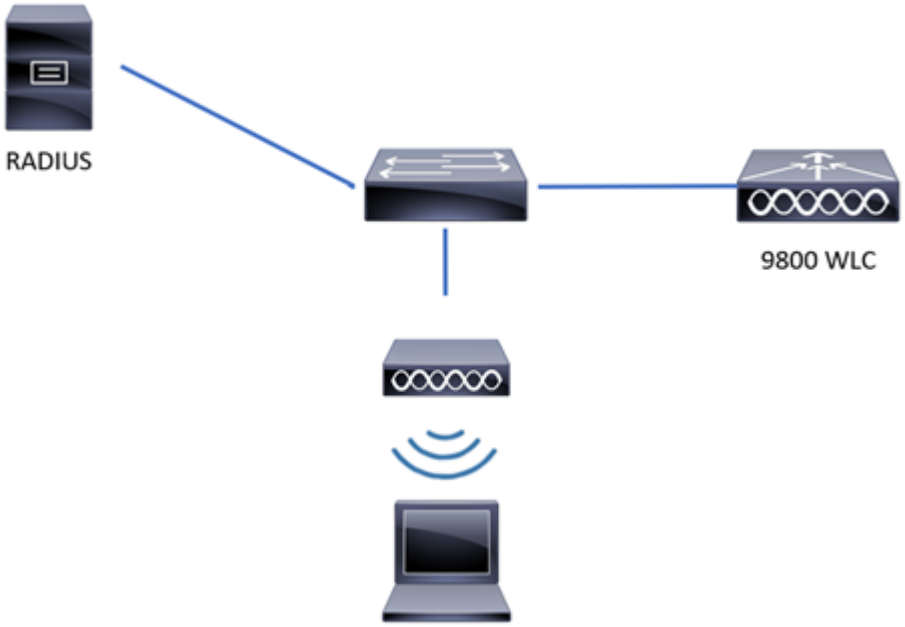
LWA 흐름:

- 게스트 사용자는 게스트 WLAN을 브로드캐스트하는 AP와 연결합니다.
- 게스트 사용자는 IP 주소를 얻기 위해 DHCP 프로세스를 거칩니다.
- 게스트 사용자는 종속 포털에 대한 인터넷 연결을 확인하려고 합니다. Apple 디바이스인 경우 Apple 종속 포털을 시도합니다. Android 디바이스인 경우 Android 종속 포털을 시도합니다. Windows 디바이스인 경우 Windows 연결 테스트 포털을 시도합니다.
- 게스트 사용자가 종속 포털 IP 주소를 묻는 DNS 쿼리를 보냅니다. DNS 서버는 해당 IP 주소로 쿼리에 응답합니다.
- 게스트 사용자는 종속 포털의 IP 주소로 HTTP GET 메시지를 보냅니다.
- WLC는 해당 메시지를 가로채고 HTTP 200 OK 및 리디렉션 URL을 사용하여 게스트 사용자에게 응답합니다.
- 게스트 사용자가 WLC 가상 IP에 HTTPS GET 메시지를 보내고 WLC가 웹 포털에 응답합니다.
- 게스트 사용자는 웹 포털에 인증 자격 증명을 입력 하라는 메시지가 표시 됩니다.
- 웹 포털은 제공된 자격 증명을 사용하여 사용자를 WLC로 다시 리디렉션합니다(외부 웹 포털이 사용되는 경우).
- WLC는 로컬 데이터베이스를 통해 게스트 사용자를 인증하거나 RADIUS 또는 LDAP 서버에 쿼리를 보내 자격 증명이 올바른지 확인합니다(인증 유형이 webconsent 또는 webauth인 경우).
- 자격 증명이 올바르면 WLC에서 게스트 사용자를 인증하고 RUN 상태로 전환합니다. 자격 증명이 잘못된 경우 WLC는 게스트 사용자를 삭제합니다.
- WLC는 웹 브라우저에 입력한 원래 URL로 클라이언트를 다시 리디렉션합니다.



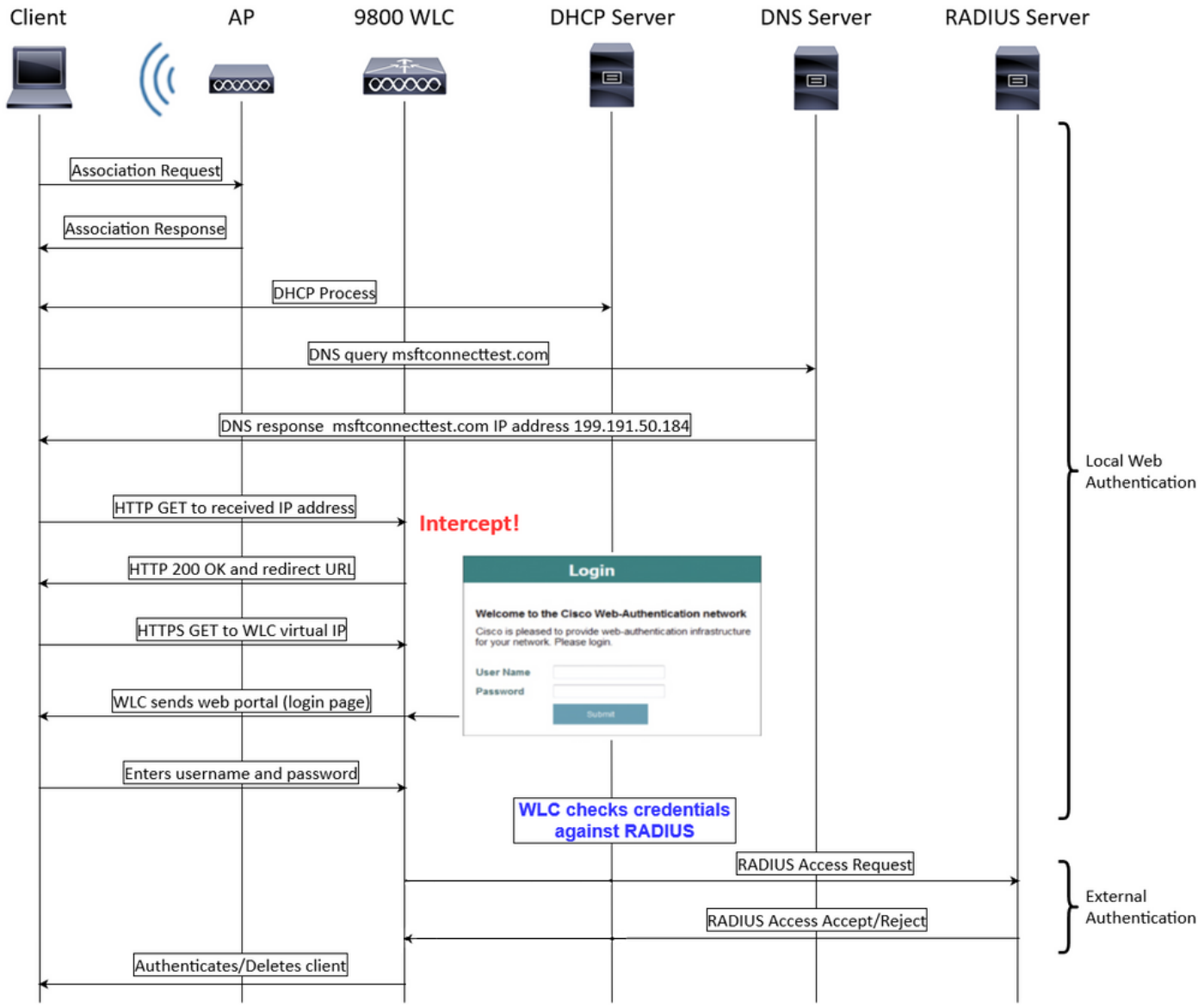
LWA 흐름

외부 인증을 사용하는 로컬 웹 인증



LWA-EA의 일반 토폴로지

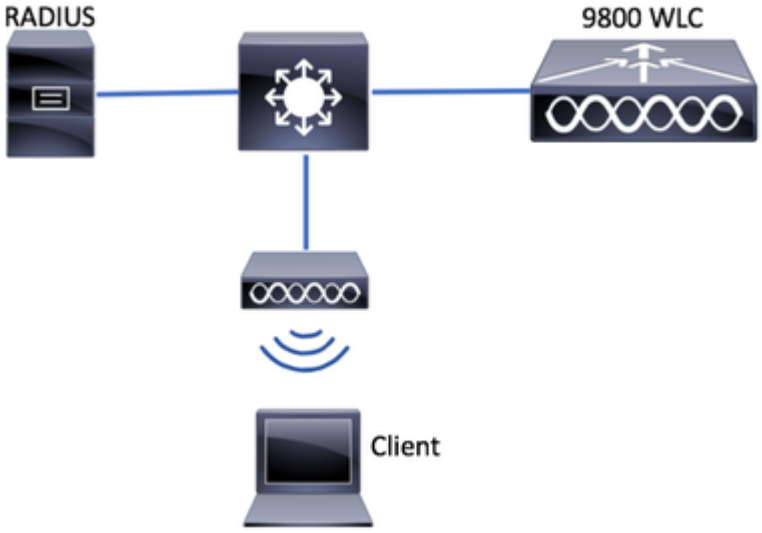
LWA-EA는 웹 포털 및 리디렉션 URL이 WLC에 있고 자격 증명이 ISE와 같은 외부 서버에 저장되는 LWA의 방법입니다. WLC는 자격 증명을 캡처하고 외부 RADIUS 서버를 통해 클라이언트를 인증합니다. 게스트 사용자가 자격 증명을 입력하면 WLC는 RADIUS에 대해 자격 증명을 확인하고 RADIUS 액세스 요청을 전송하고 RADIUS 서버에서 RADIUS 액세스 수락/거부를 수신합니다. 자격 증명이 올바르면 게스트 사용자가 RUN 상태로 전환됩니다. 자격 증명이 올바르지 않으면 게스트 사용자가 WLC에 의해 삭제됩니다.



LWA-EA 플로우

구성

네트워크 다이어그램



네트워크 다이어그램

참고: 이 컨피그레이션 예에서는 중앙 스위칭/인증만 다룹니다. Flex Local Switching 컨피그레이션에는 웹 인증을 구성하기 위한 약간 다른 요구 사항이 있습니다.

CLI에서 외부 인증을 사용하여 로컬 웹 인증 구성

AAA 서버 및 서버 그룹 구성

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4


      auth-port 1812 acct-port 1813

9800WLC(config-radius-server)#key cisco

9800WLC(config-radius-server)#exit

9800WLC(config)#aaa group server radius RADIUSGROUP

9800WLC(config-sg-radius)#server name RADIUS

9800WLC(config-sg-radius)#end
```

로컬 인증 및 권한 부여 구성

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#end
```

WLAN 보안 매개변수 구성

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

무선 정책 프로파일 생성

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan




9800WLC(config-wireless-policy)#no shutdown


9800WLC(config-wireless-policy)#end
```

정책 태그 생성

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

AP에 정책 태그 할당

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap


     >


9800WLC(config-ap-tag)#policy-tag POLICY_TAG


9800WLC(config-ap-tag)#end
```

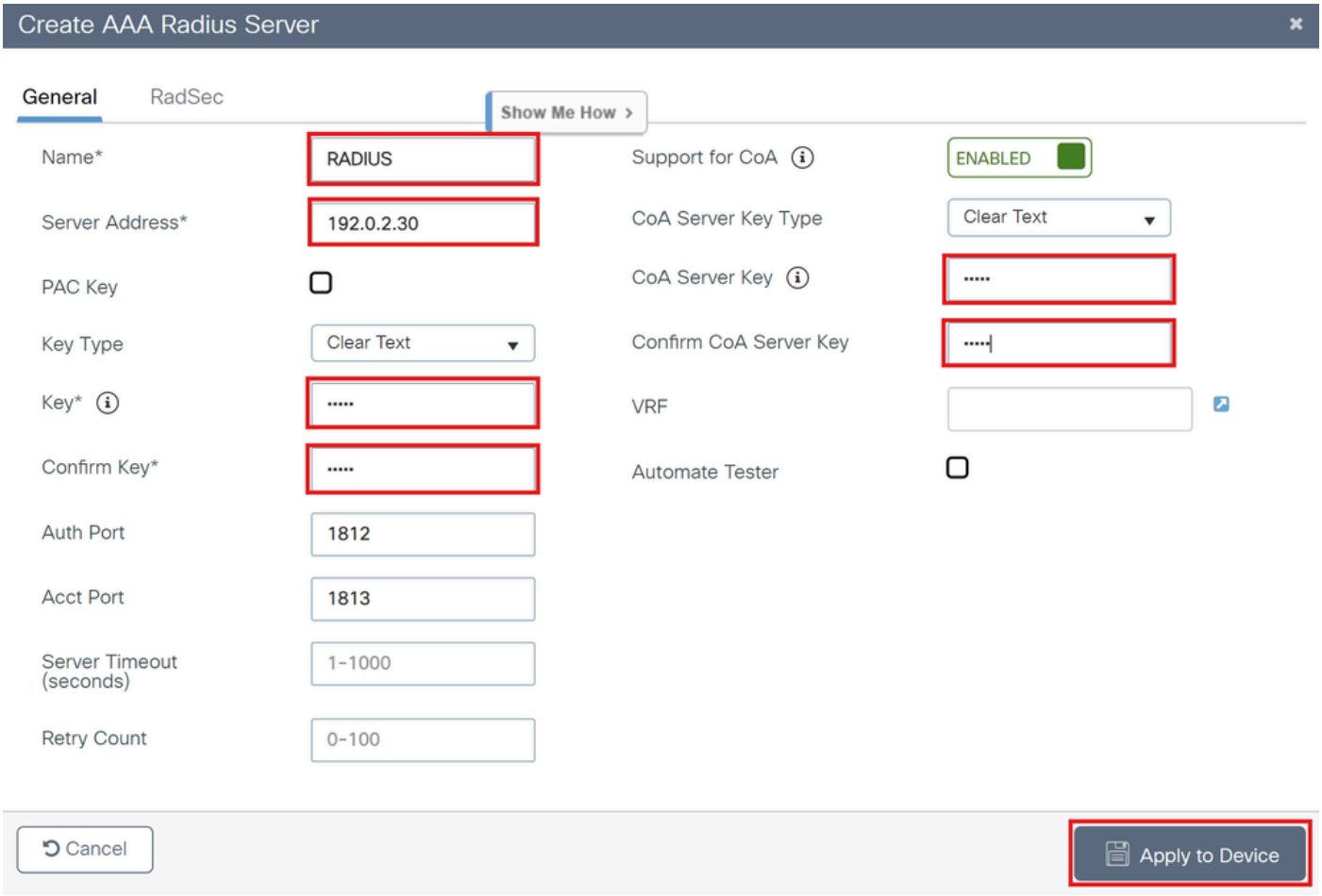
ISE 측에서 컨피그레이션을 완료하려면 ISE Configuration(ISE 컨피그레이션) 섹션으로 이동하십시오.

WebUI에서 외부 인증을 사용하여 로컬 웹 인증 구성

9800 WLC의 AAA 구성

1단계. 9800 WLC 컨피그레이션에 ISE 서버를 추가합니다.

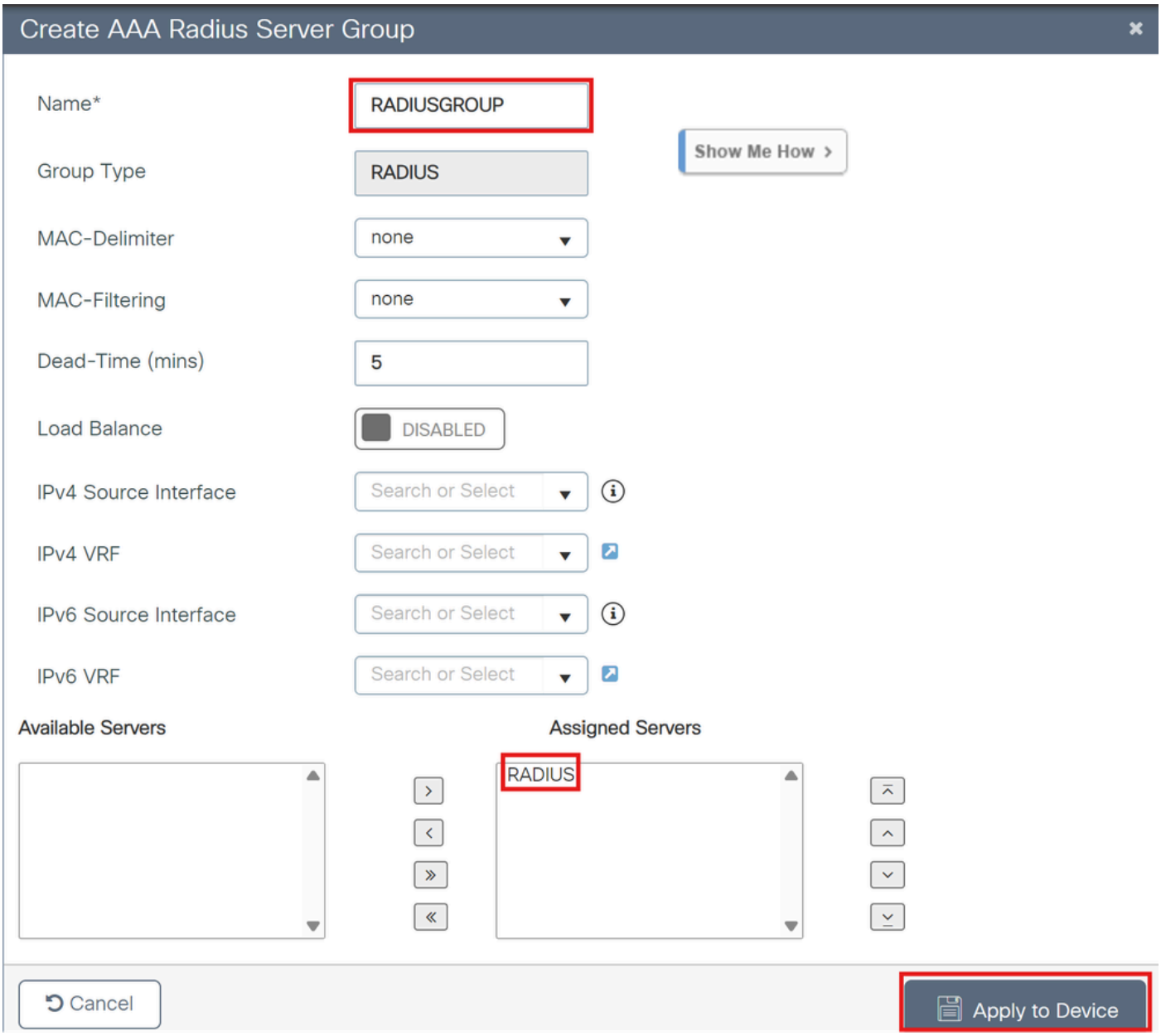
Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Servers(서버) > + Add(추가)로 이동하고 이미지에 표시된 대로 RADIUS 서버 정보를 입력합니다.



9800 WLC의 AAA 구성

2단계. RADIUS 서버 그룹을 추가합니다.

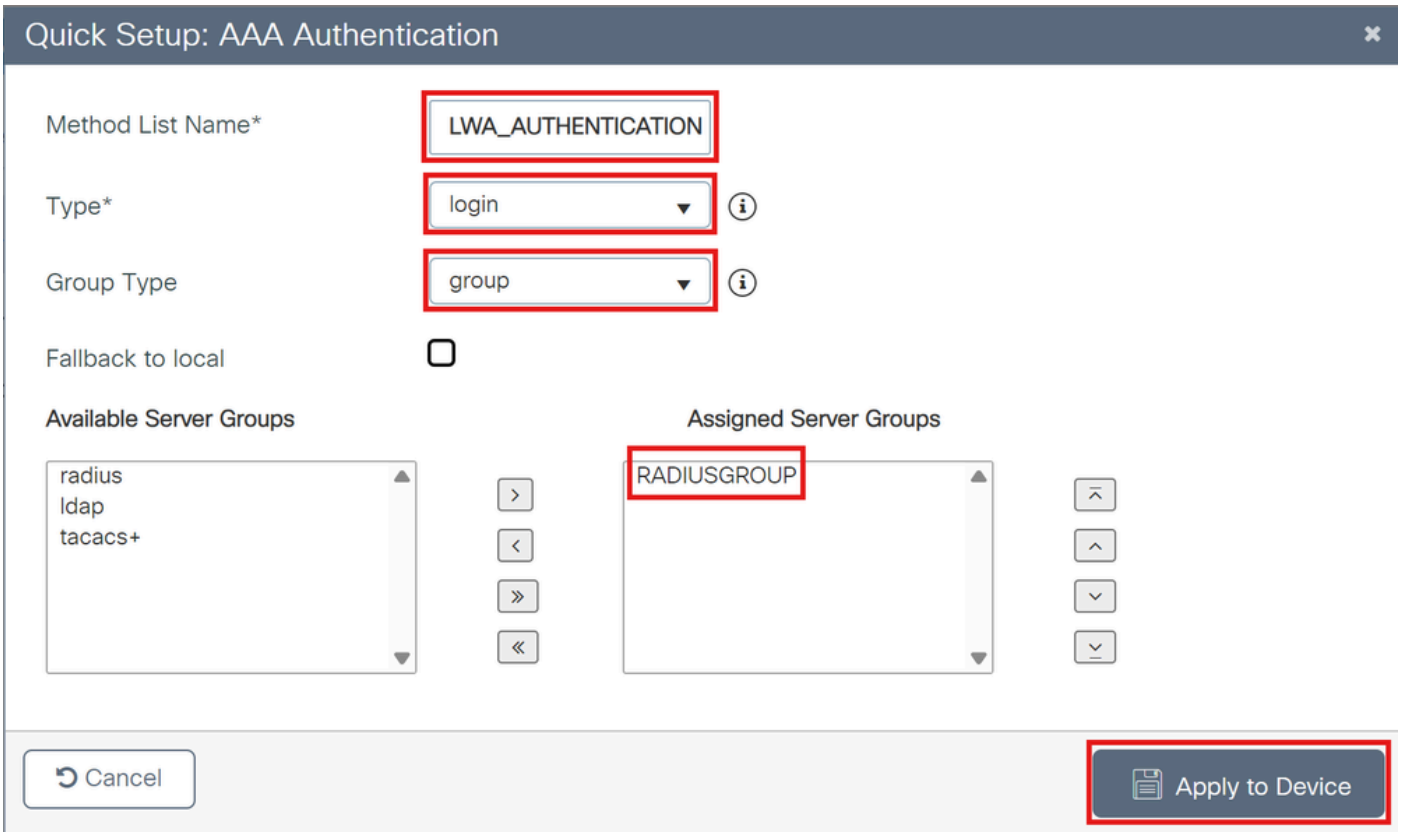
Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Servers Group(서버 그룹) > + Add(추가)로 이동하고 RADIUS 서버 그룹 정보를 입력합니다.



RADIUS 서버 그룹 추가

3단계. 인증 방법 목록을 생성합니다.

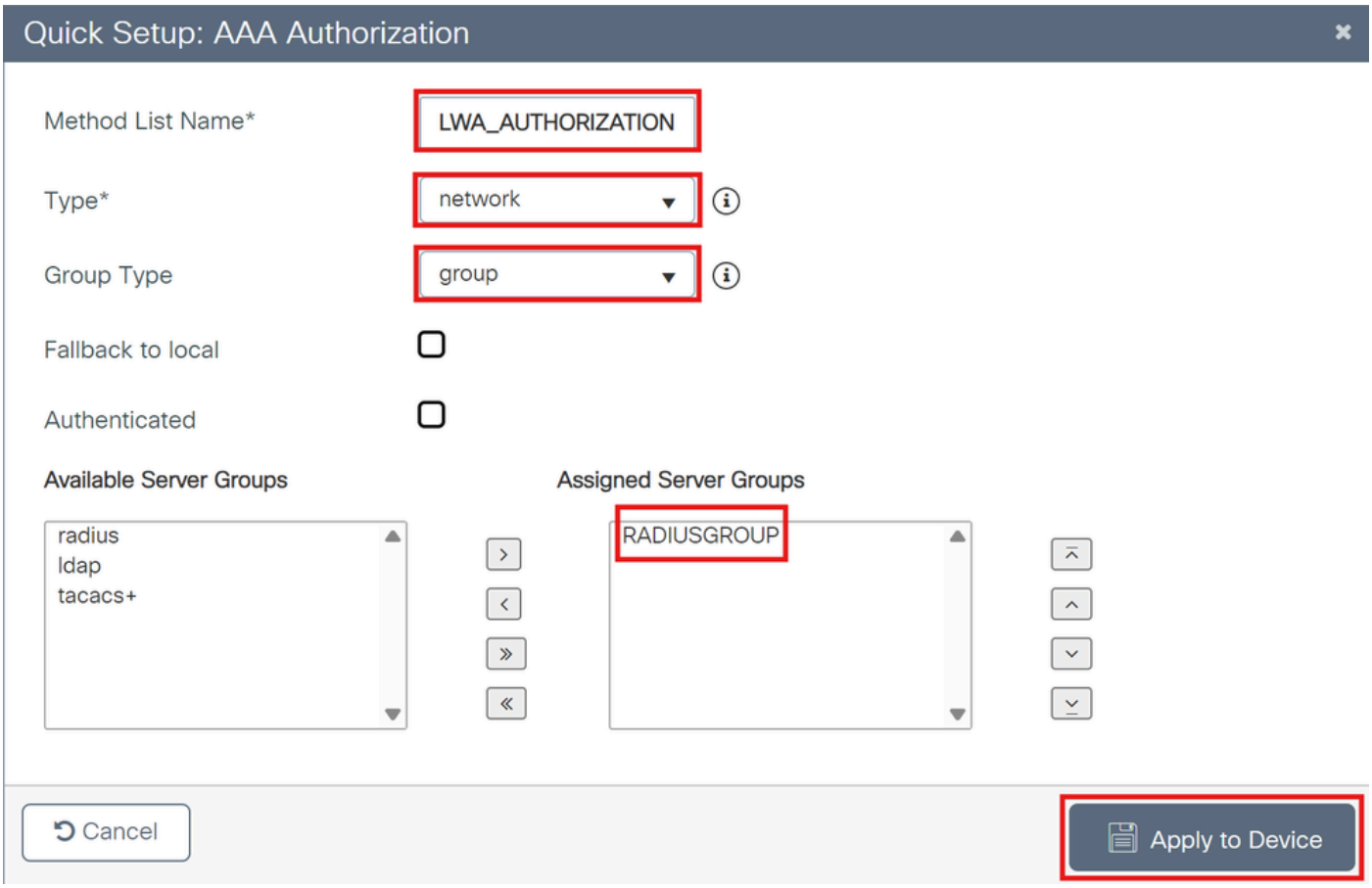
Configuration > Security > AAA > AAA Method List > Authentication > + Add로 이동합니다:



인증 방법 목록 만들기

4단계. 권한 부여 방법 목록을 생성합니다.

Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여) > + Add(추가)로 이동합니다.

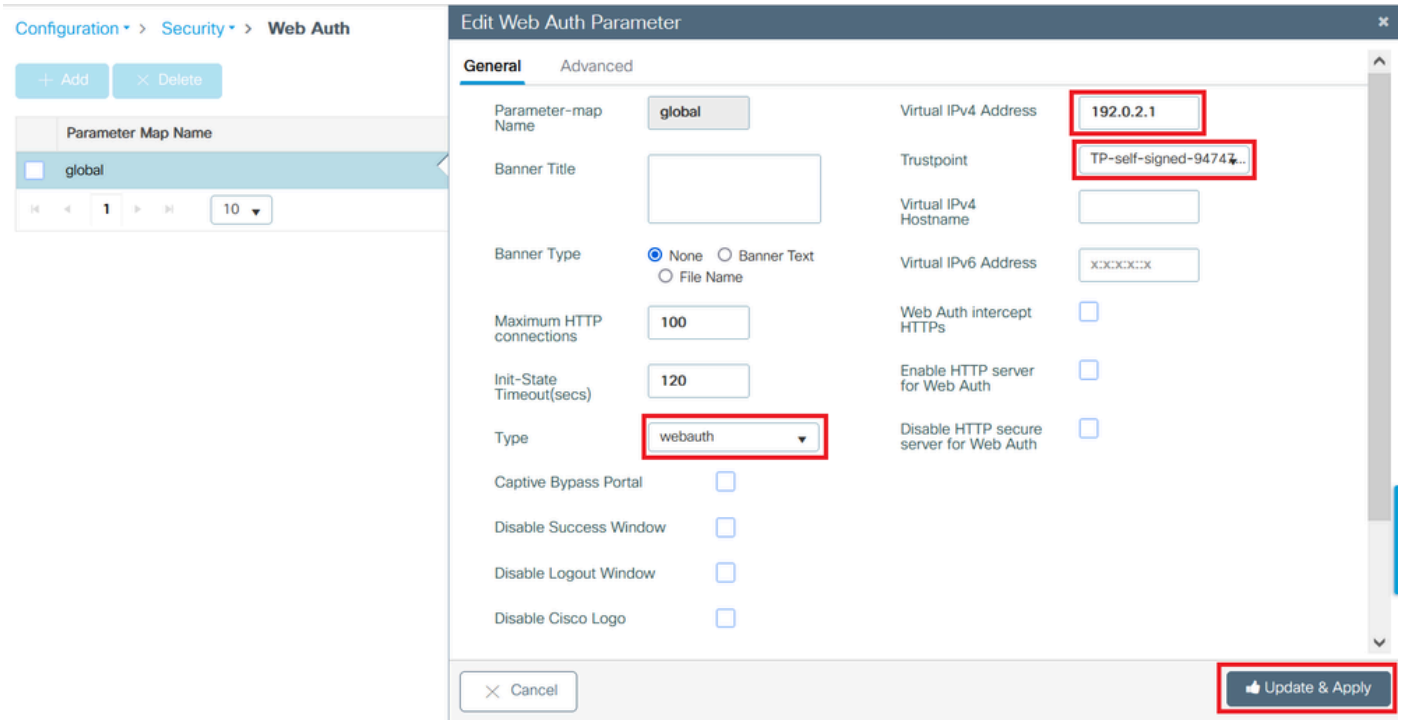


권한 부여 방법 목록 만들기

WebAuth 구성

매개변수 맵을 생성하거나 편집합니다. 유형을 webauth로 선택합니다. Virtual IPv4 Address(가상 IPv4 주소)는 IP 주소 충돌을 방지하기 위해 네트워크에서 사용되지 않는 주소여야 하며 신뢰 지점을 추가합니다.

Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증) > + Add(추가)로 이동하거나 매개변수 맵을 선택합니다.

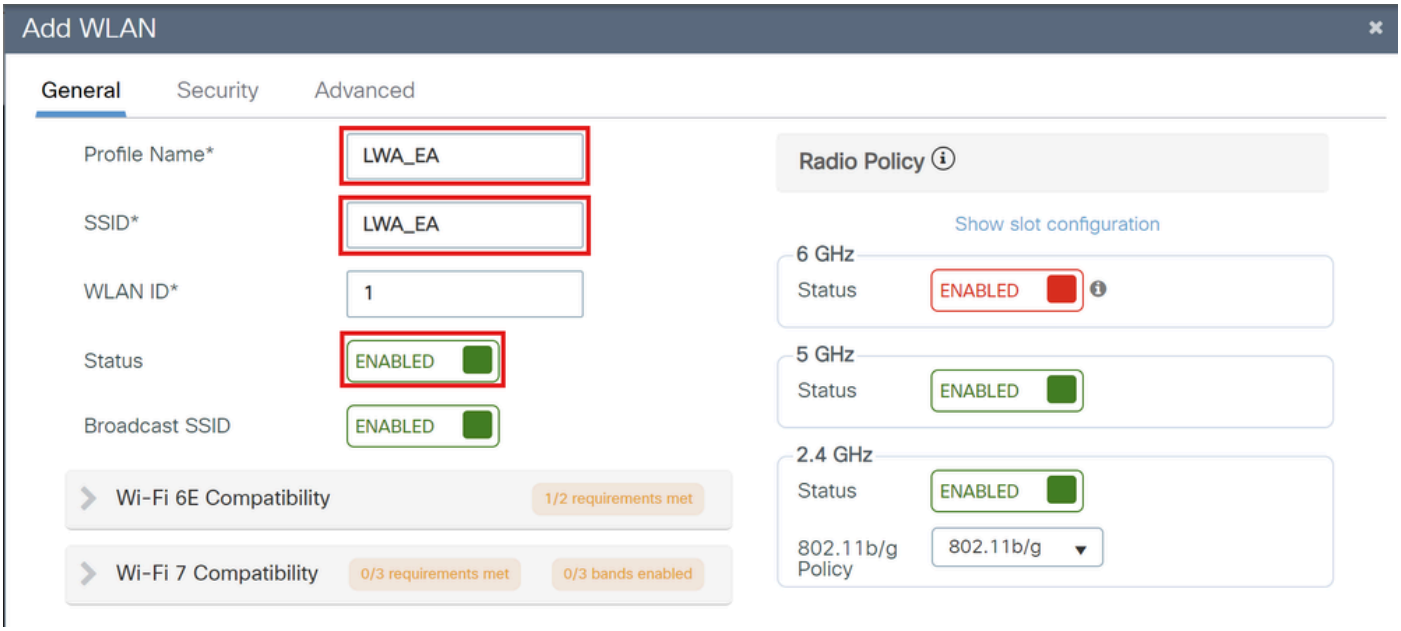


WebAuth 구성

WLAN 구성

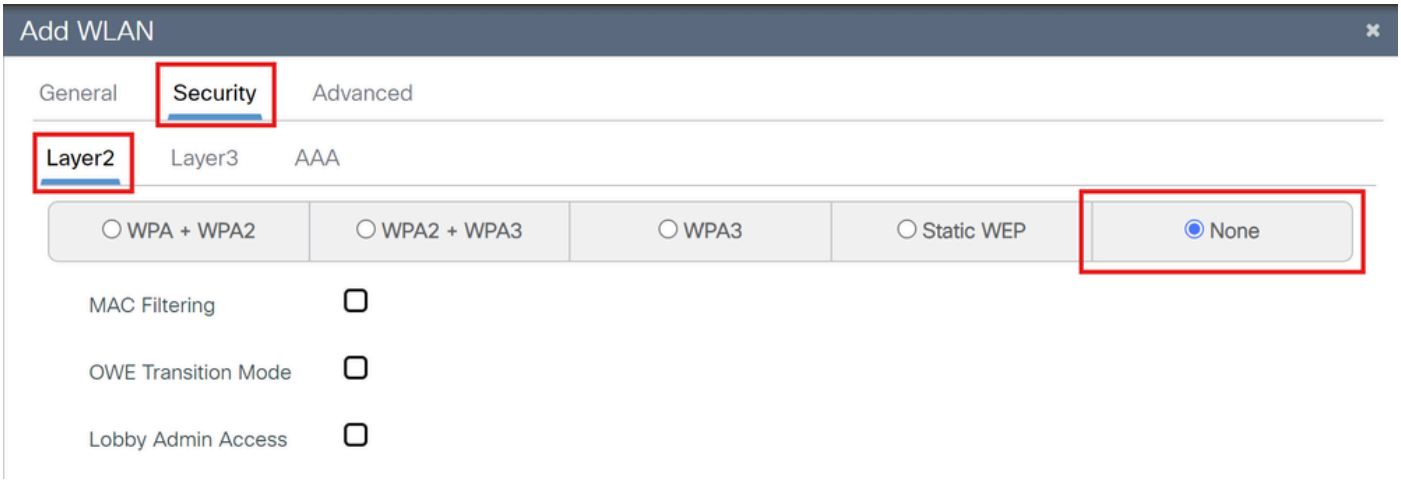
1단계. WLAN 생성.

Configuration(구성) > Tags & Profiles(태그 및 프로파일) > WLAN > + Add(+ 추가)로 이동하고 필요에 따라 네트워크를 구성합니다.



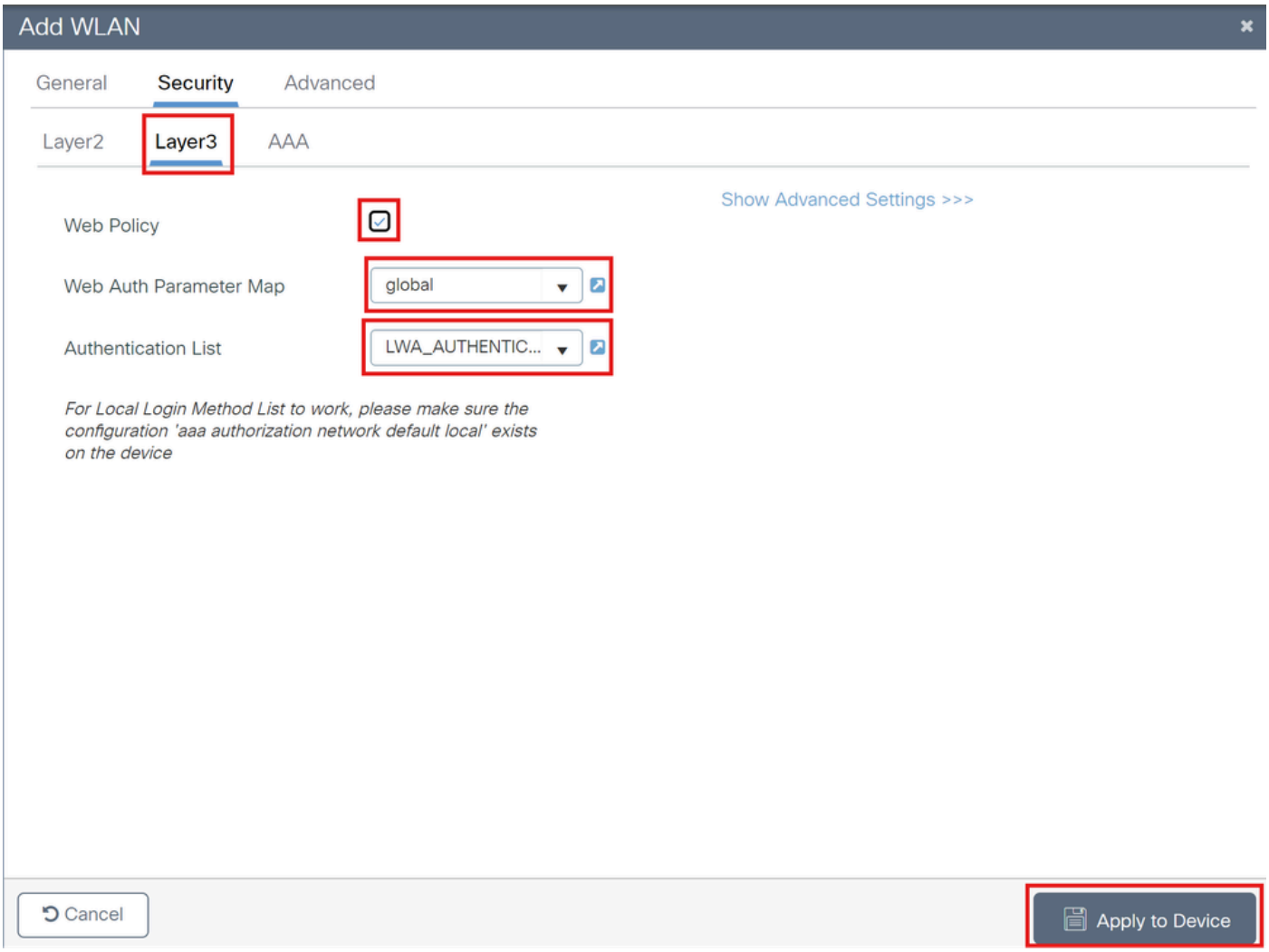
WLAN 생성

2단계. Security(보안) > Layer2(레이어 2)로 이동하고 Layer 2 Security Mode(레이어 2 보안 모드)에서 None(없음)을 선택합니다.



WLAN 보안 생성

3단계. Security(보안) > Layer3로 이동하고 Web Policy(웹 정책)에서 Web Auth Parameter Map(웹 인증 매개변수 맵)에서 매개변수 이름을 선택하고 Authentication List(인증 목록)에서 이전에 생성한 인증 목록을 선택합니다.



WLAN 인증 목록 생성

WLAN이 WLAN 목록에 표시됩니다.

생성된 WLAN

정책 프로파일 구성

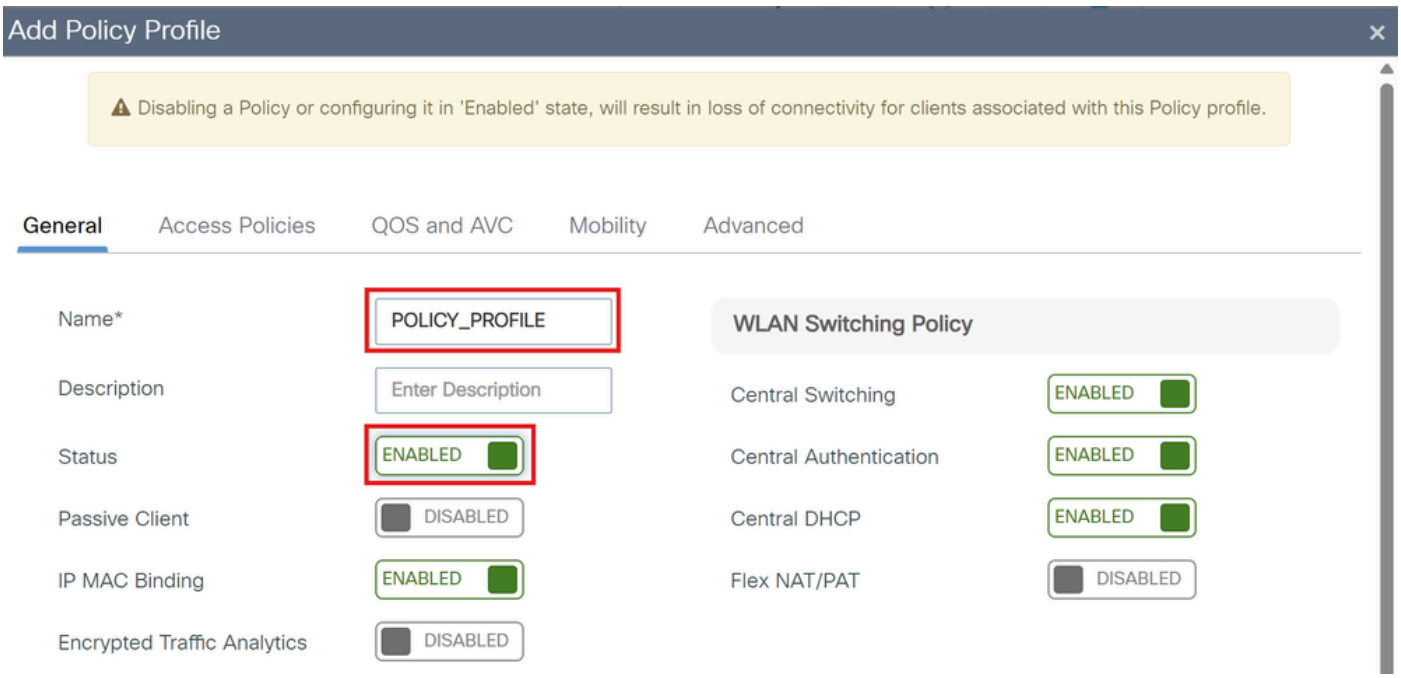
정책 프로필 내에서 다른 설정 중에서 클라이언트를 할당하는 VLAN을 선택할 수 있습니다.

기본 정책 프로파일을 사용하거나 새 프로파일을 생성할 수 있습니다.

1단계. 새 정책 프로파일을 생성합니다.

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동하여 기본 정책 프로필을 구성하거나 새 프로필을 만듭니다.

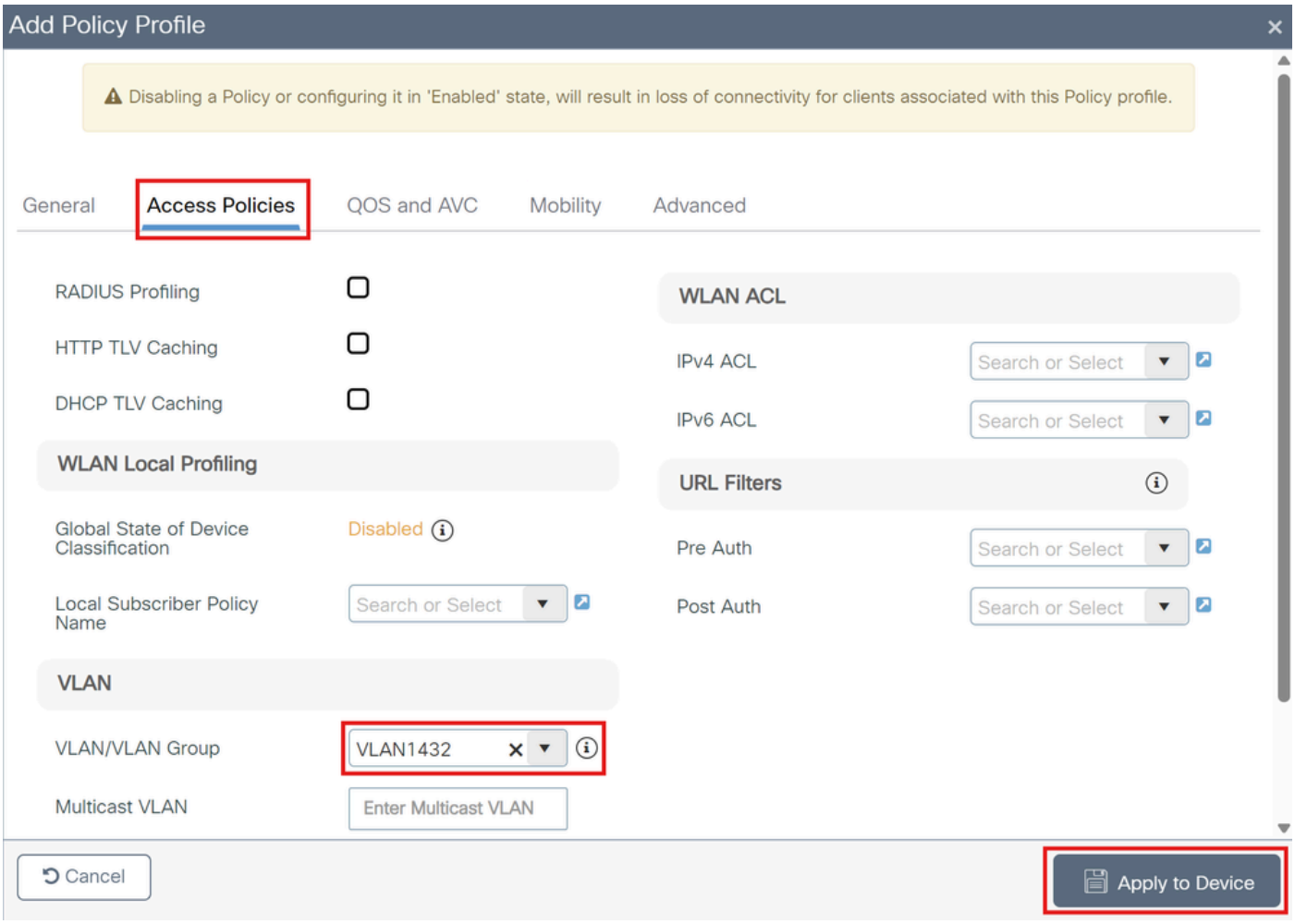
프로파일이 활성화되어야 합니다.



새 정책 프로필 생성

2단계. VLAN을 선택합니다.

Access Policies(액세스 정책) 탭으로 이동하고 드롭다운에서 VLAN 이름을 선택하거나 VLAN ID를 수동으로 입력합니다.



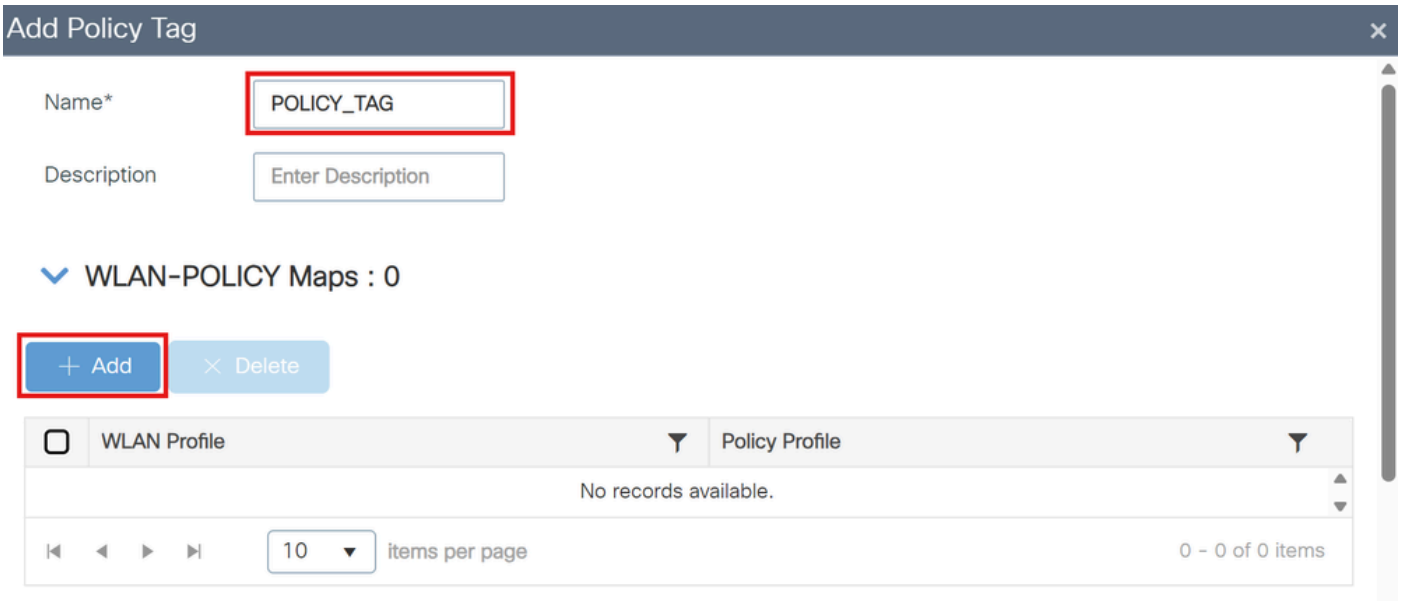
VLAN 선택

정책 태그 구성

정책 태그 내부에서는 SSID를 정책 프로파일과 연결합니다. 새 정책 태그를 생성하거나 default-policy 태그를 사용할 수 있습니다.

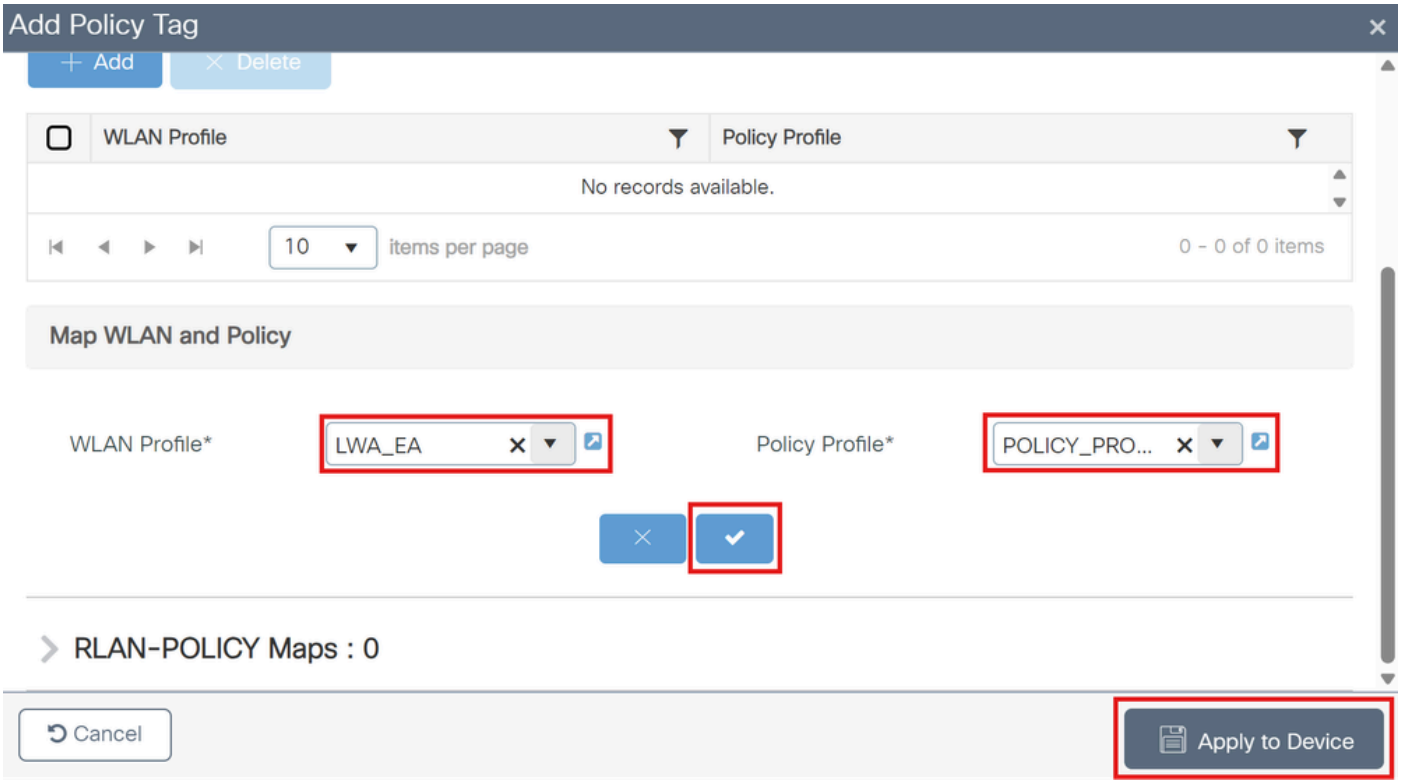
이미지에 표시된 것과 같이 Configuration(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그) > Policy(정책)로 이동하고 필요에 따라 새로 추가합니다.

선택 + 추가:



정책 태그 구성

WLAN 프로파일을 원하는 정책 프로파일에 연결합니다:

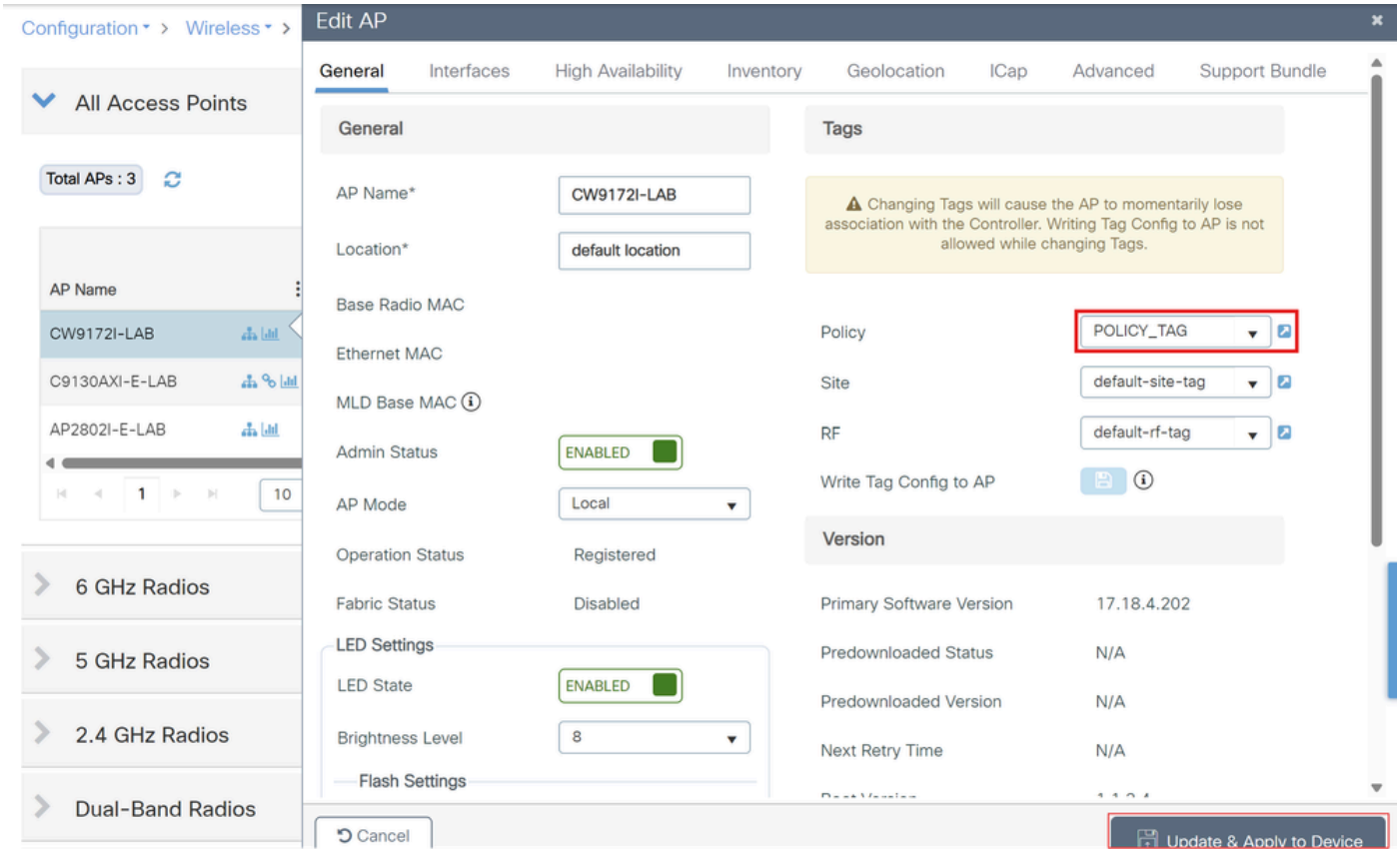


정책 태그 구성

정책 태그 할당

필요한 AP에 정책 태그를 할당합니다.

AP 하나에 태그를 할당하려면 Configuration(구성) > Wireless(무선) > Access Points(액세스 포인트) > AP Name(AP 이름) > General Tags(일반 태그)로 이동하고 필요에 따라 할당한 다음 업데이트 및 장치에 적용을 클릭합니다.

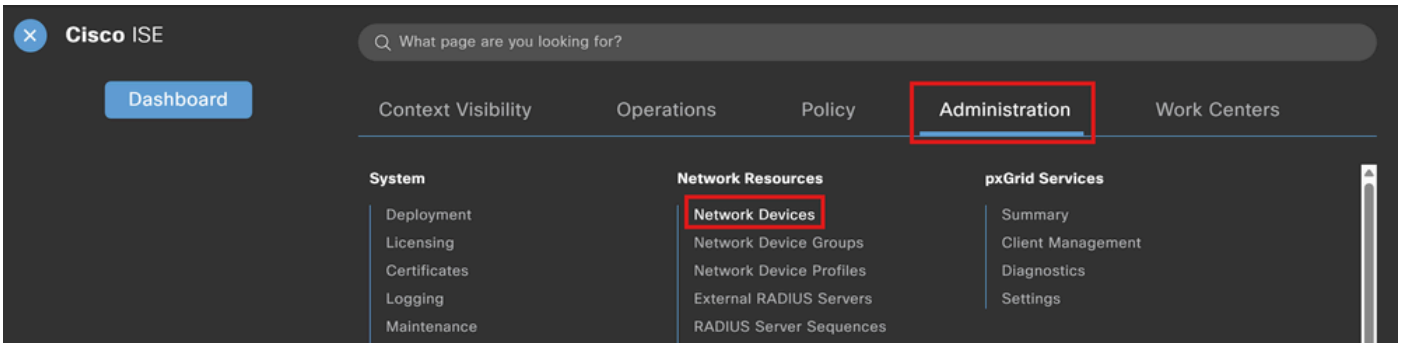


정책 태그 할당

ISE 구성

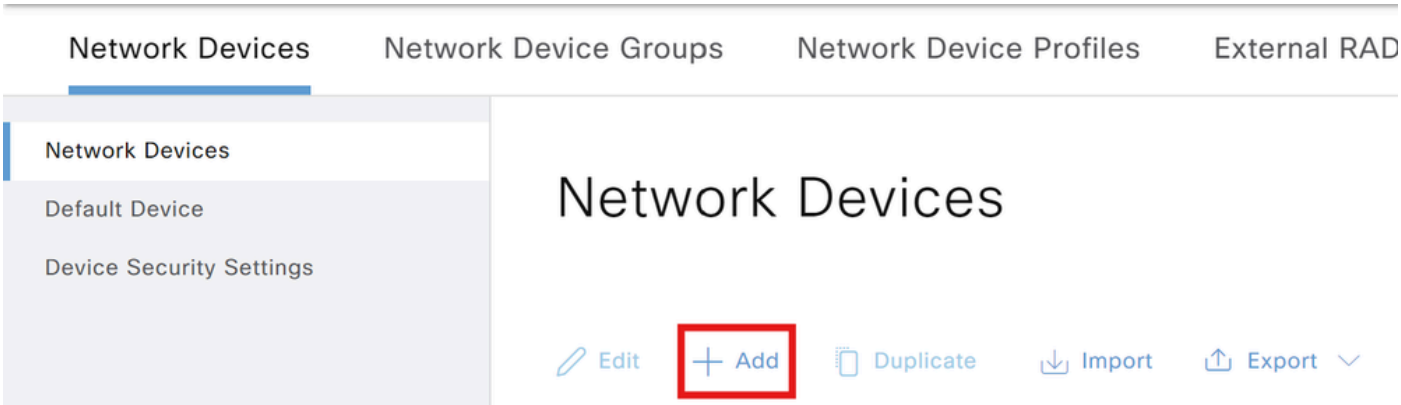
ISE에 9800 WLC 추가

1단계. 이미지에 표시된 것과 같이 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.



ISE에 9800 WLC 추가

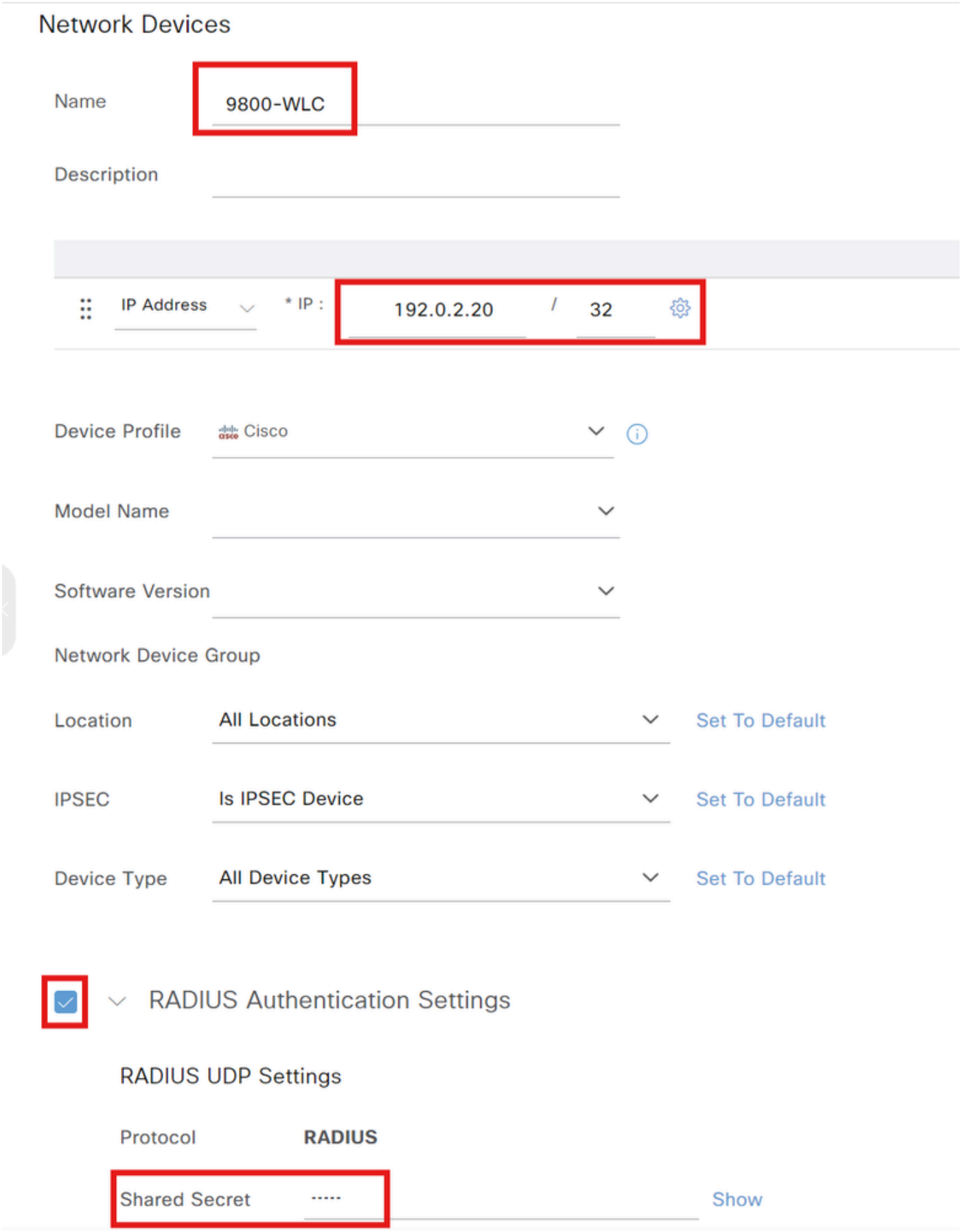
2단계. +Add를 클릭합니다.



네트워크 디바이스 추가

지정된 모델 이름, 소프트웨어 버전, 설명 및 디바이스 유형, 위치 또는 WLC를 기반으로 하는 할당 네트워크 디바이스 그룹이 될 수 있습니다.

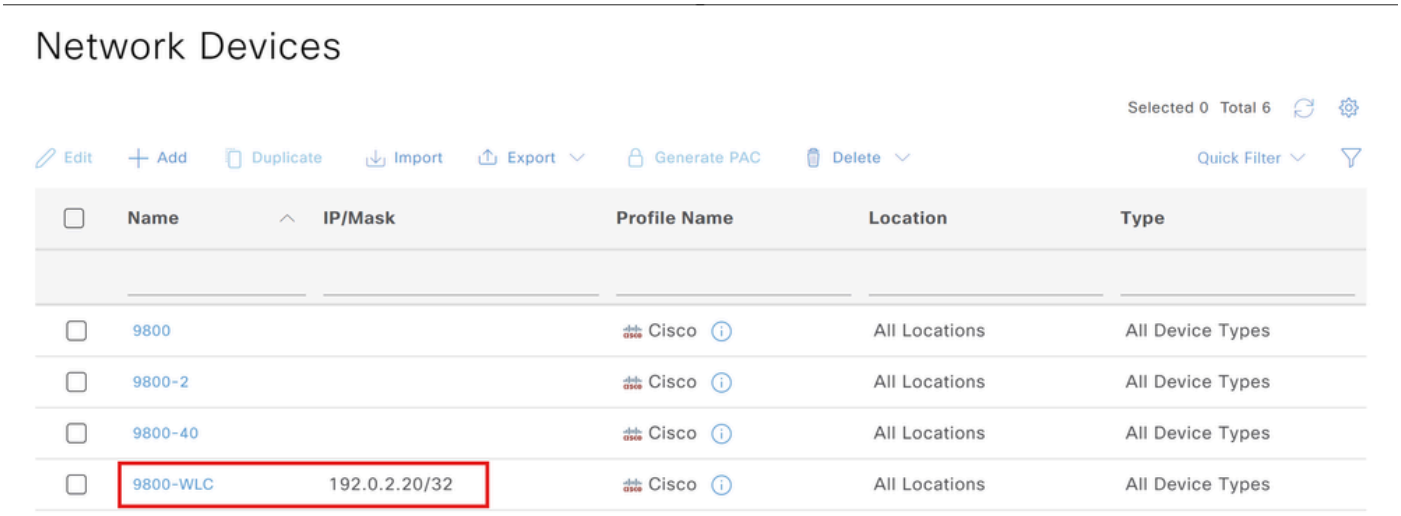
3단계. 이미지에 표시된 대로 9800 WLC 설정을 입력합니다. WLC 측에서 서버 생성 시 정의된 것과 동일한 RADIUS 키를 입력합니다. 그런 다음 Submit(제출)을 클릭합니다.



9800 WLC 설정

4단계. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크

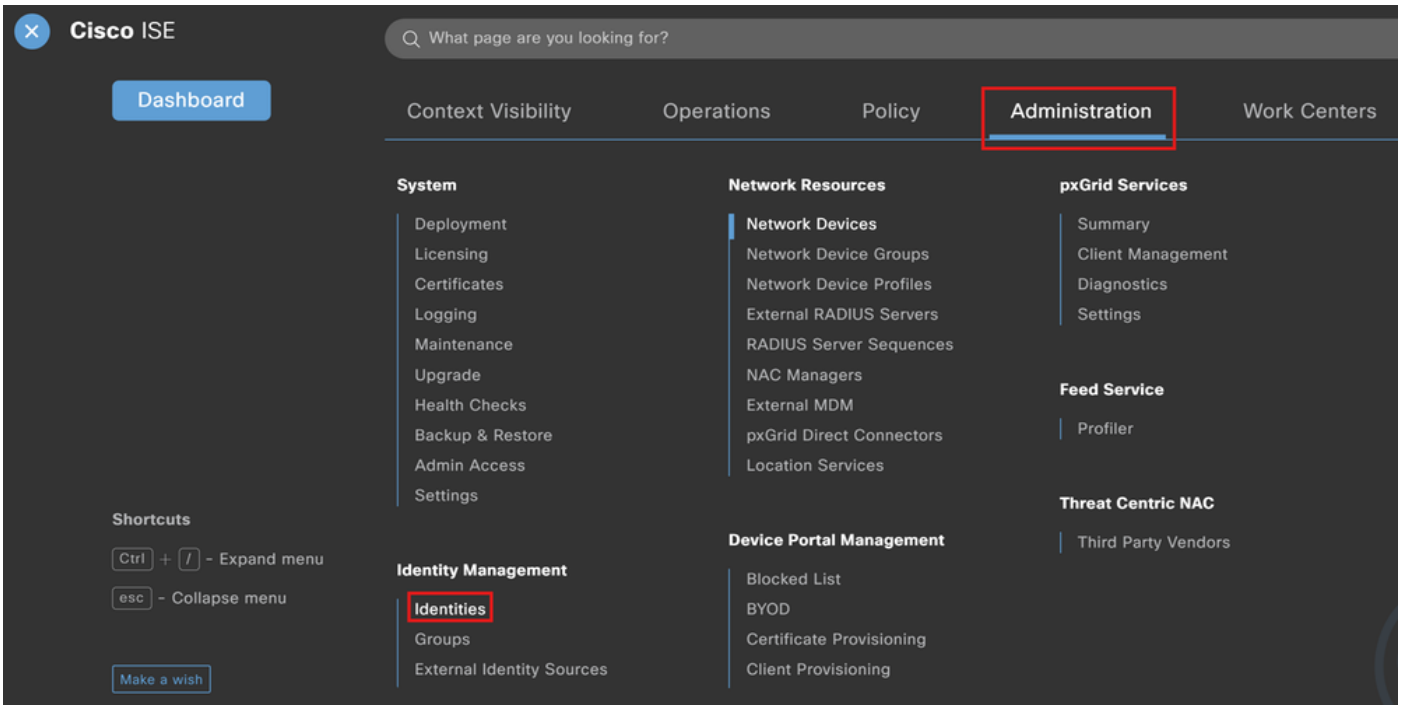
디바이스)로 이동하면 네트워크 디바이스 목록이 표시됩니다.



네트워크 장치 목록

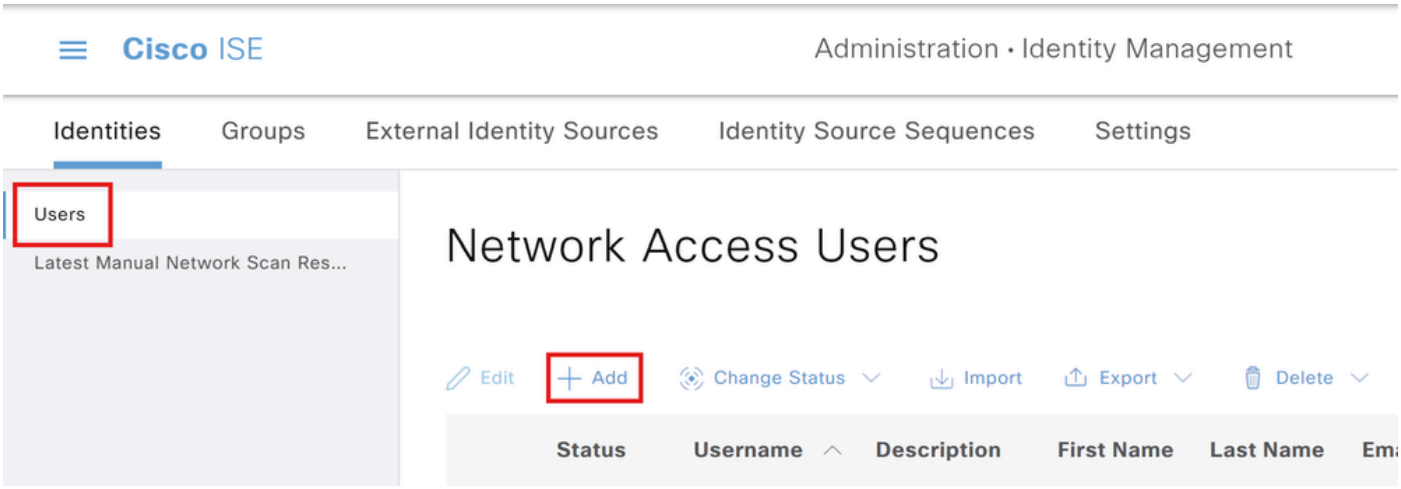
ISE에서 새 사용자 생성

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



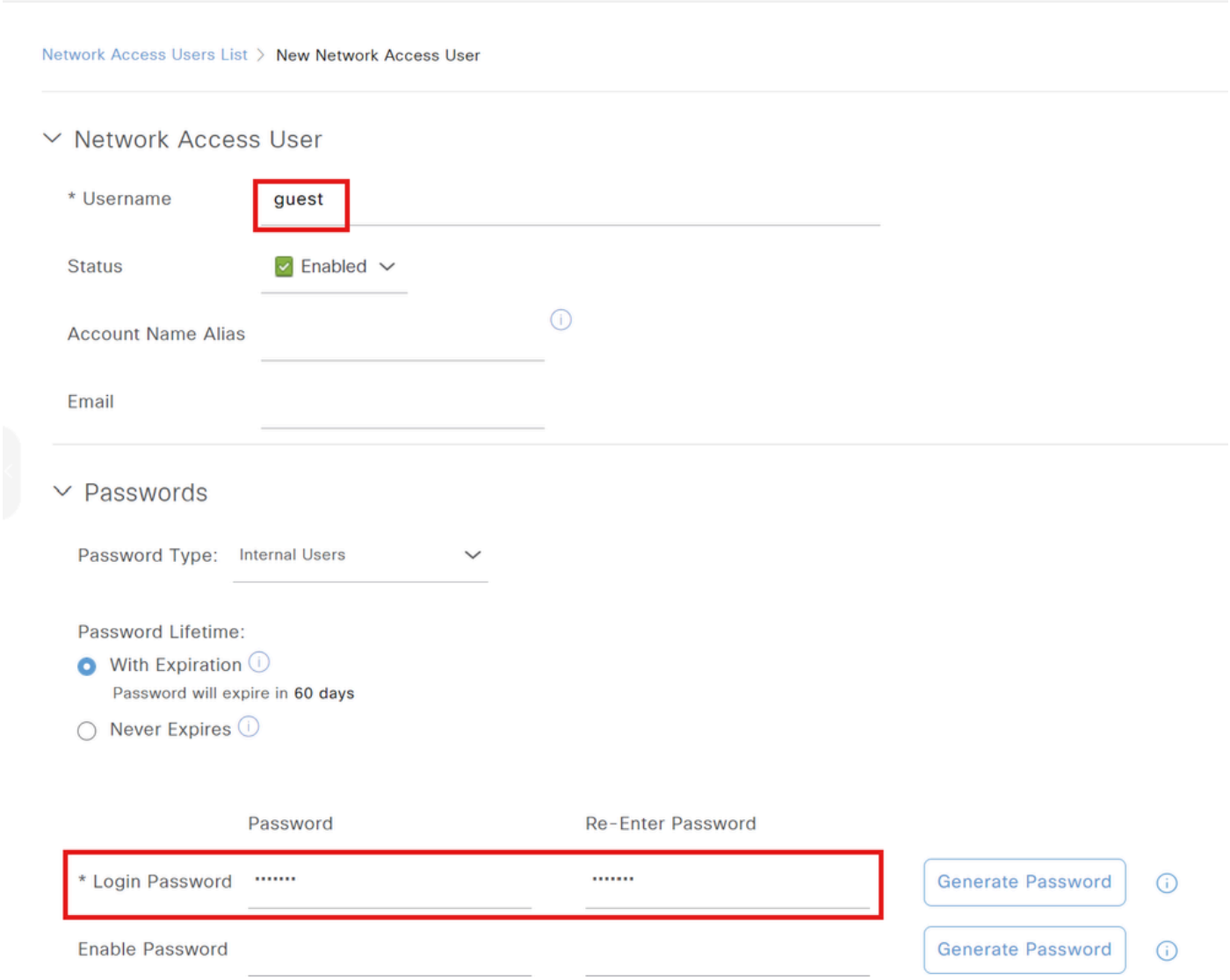
ISE 관리 - ID

2단계. Users(사용자)로 이동하여 +Add(추가)를 클릭합니다.



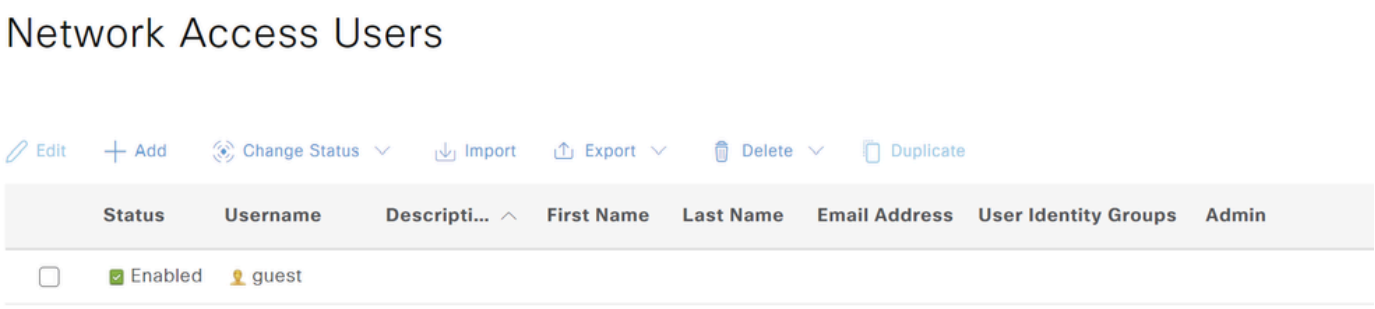
사용자 추가

3단계. 게스트 사용자의 사용자 이름 및 비밀번호를 입력하고 Submit(제출)을 클릭합니다.



ISE에서 새 사용자 생성

4단계. Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자)로 이동하면 사용자 목록을 볼 수 있습니다.



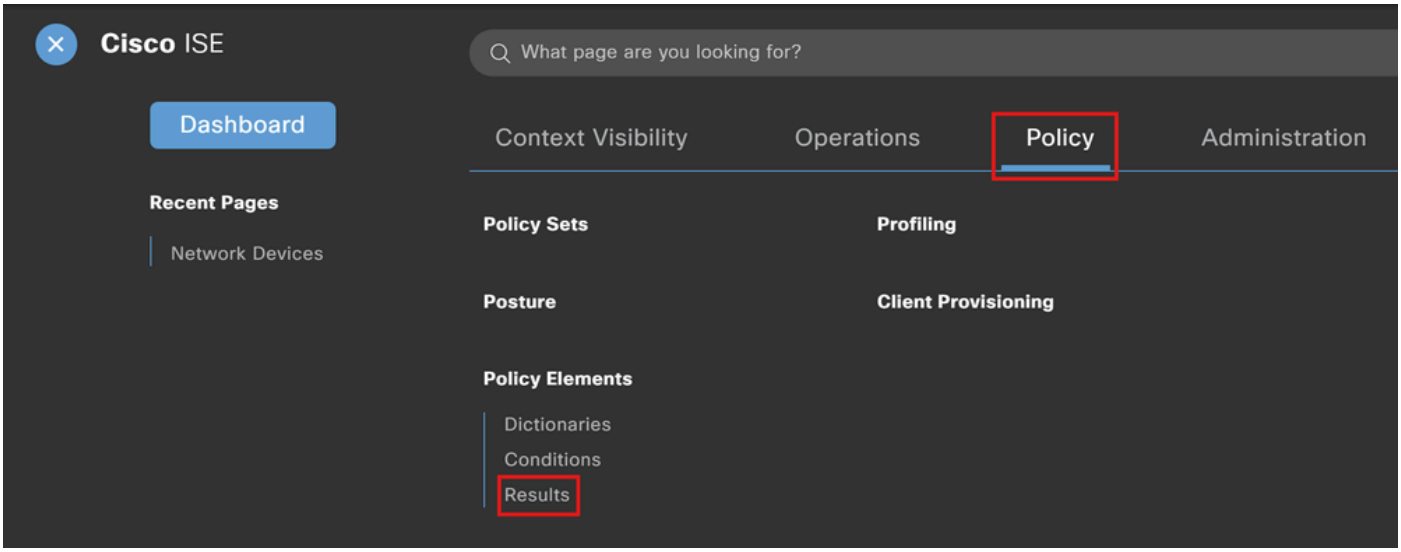
네트워크 액세스 사용자 목록

권한 부여 프로파일 생성

정책 프로파일은 매개변수(MAC 주소, 자격 증명, 사용된 WLAN 등)를 기반으로 클라이언트에 할당된 결과입니다. VLAN(Virtual Local Area Network), ACL(Access Controls List), URL(Uniform Resource Locator) 리디렉션 등의 특정 설정을 할당할 수 있습니다.

이 단계에서는 클라이언트를 인증 포털로 리디렉션하는 데 필요한 권한 부여 프로파일을 생성하는 방법을 보여줍니다. 최신 버전의 ISE에는 Cisco_Webauth 권한 부여 결과가 이미 있습니다. 여기에서 WLC에 구성한 것과 일치하도록 리디렉션 ACL 이름을 수정하도록 편집할 수 있습니다.

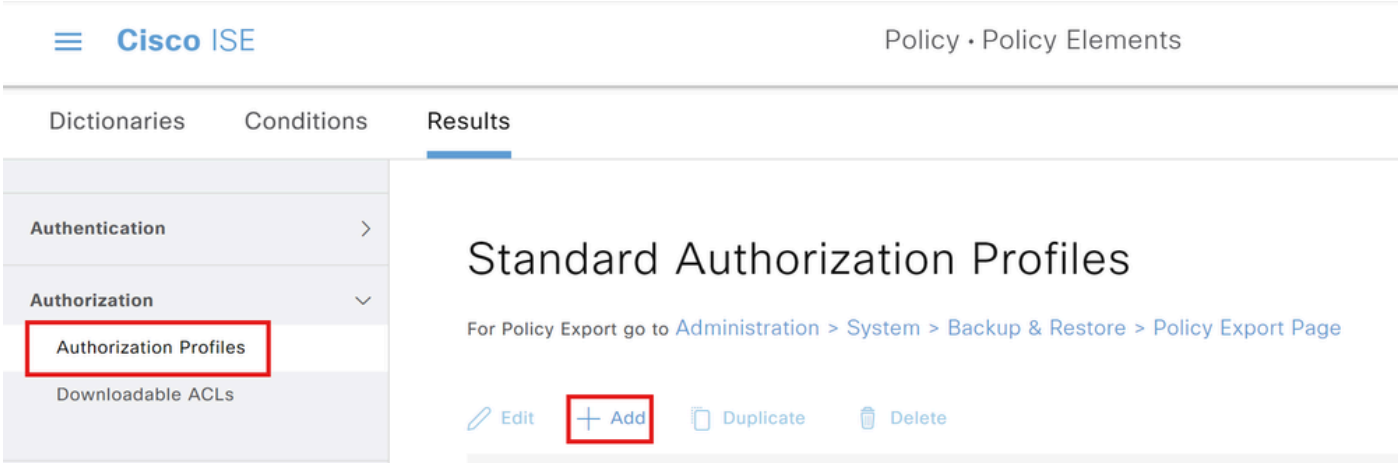
1단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과)로 이동합니다.



ISE 정책 - 결과

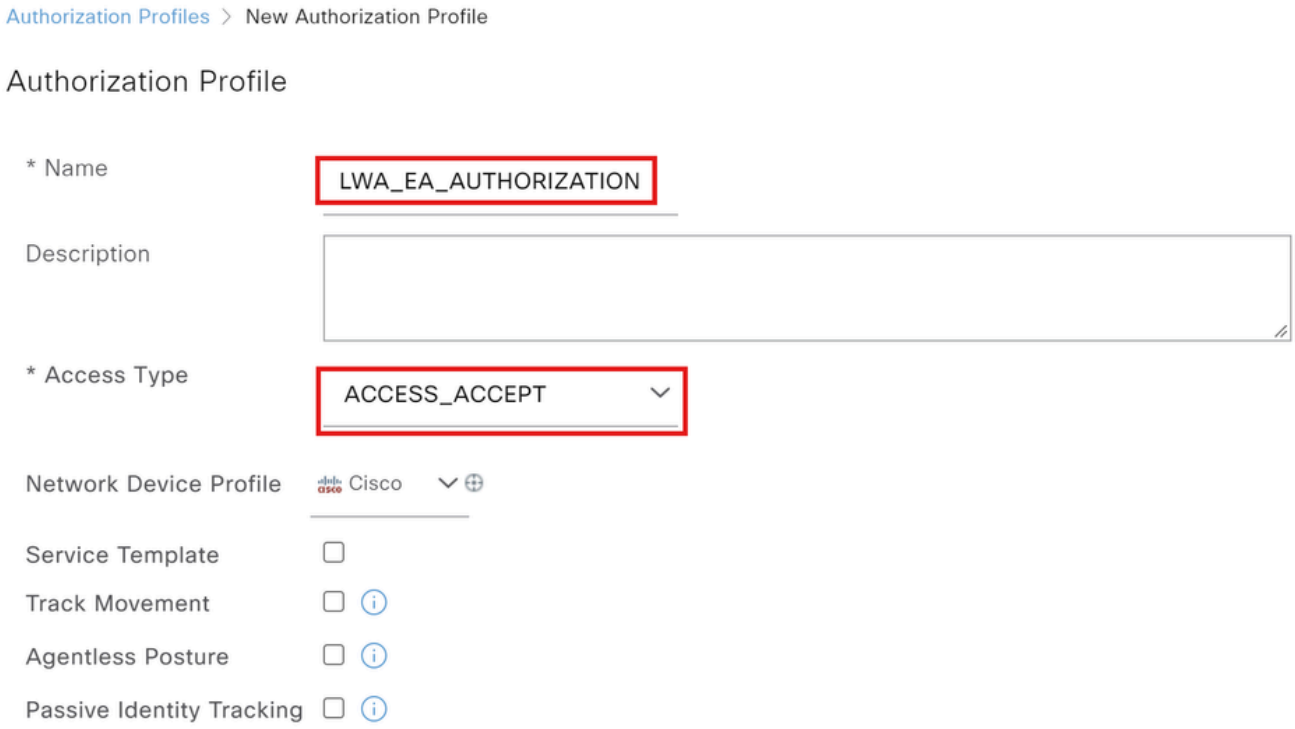
2단계. Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동합니다. 권한

부여 프로파일을 생성하려면+Add를 클릭합니다.



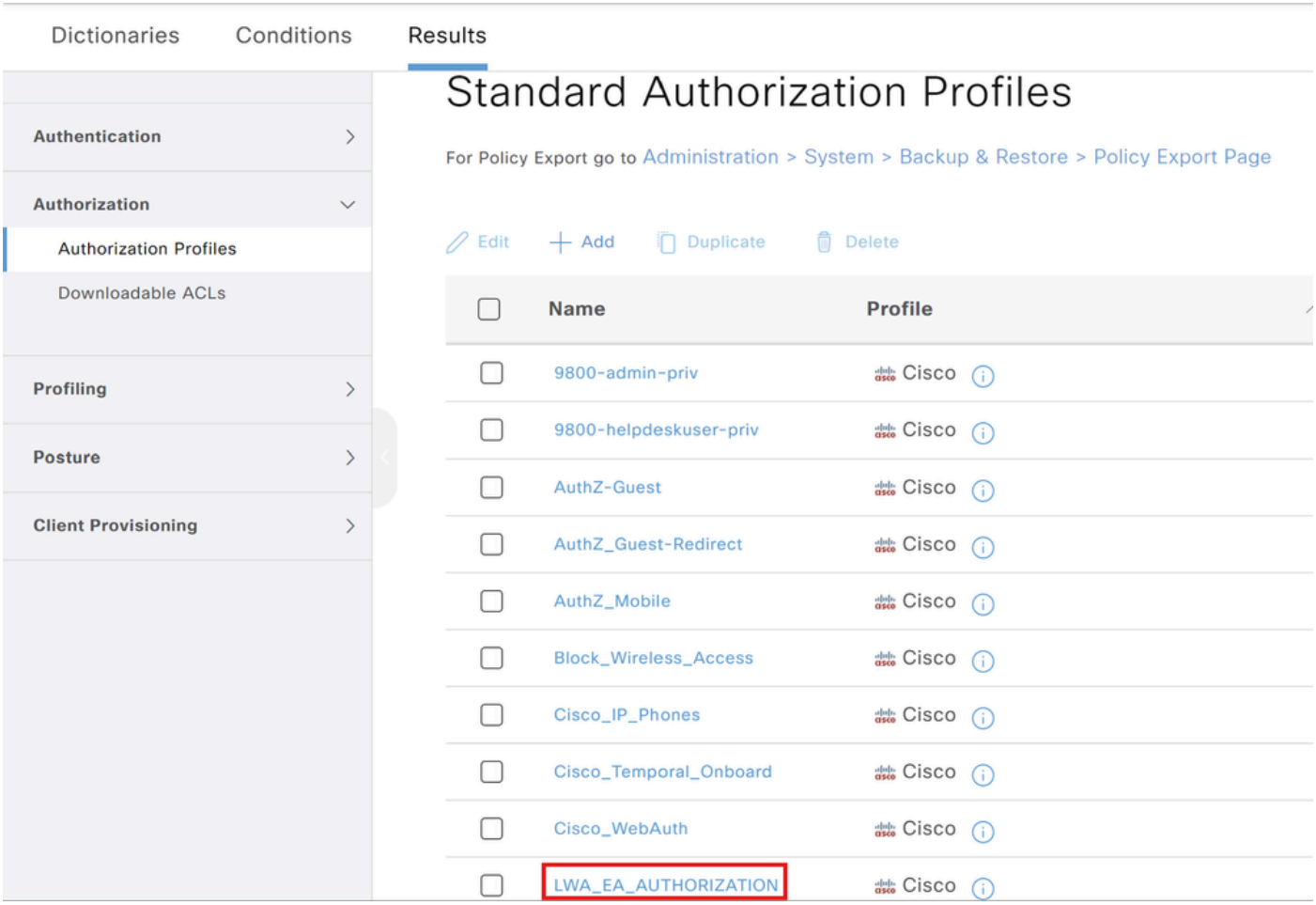
권한 부여 프로파일 추가

3단계. 권한 부여 프로파일 LWA_EA_AUTHORIZATION을 생성합니다. 속성 세부 정보는 액세스 유형=ACCESS_ACCEPT여야 합니다. Submit(제출)을 클릭합니다.



권한 부여 프로파일 생성

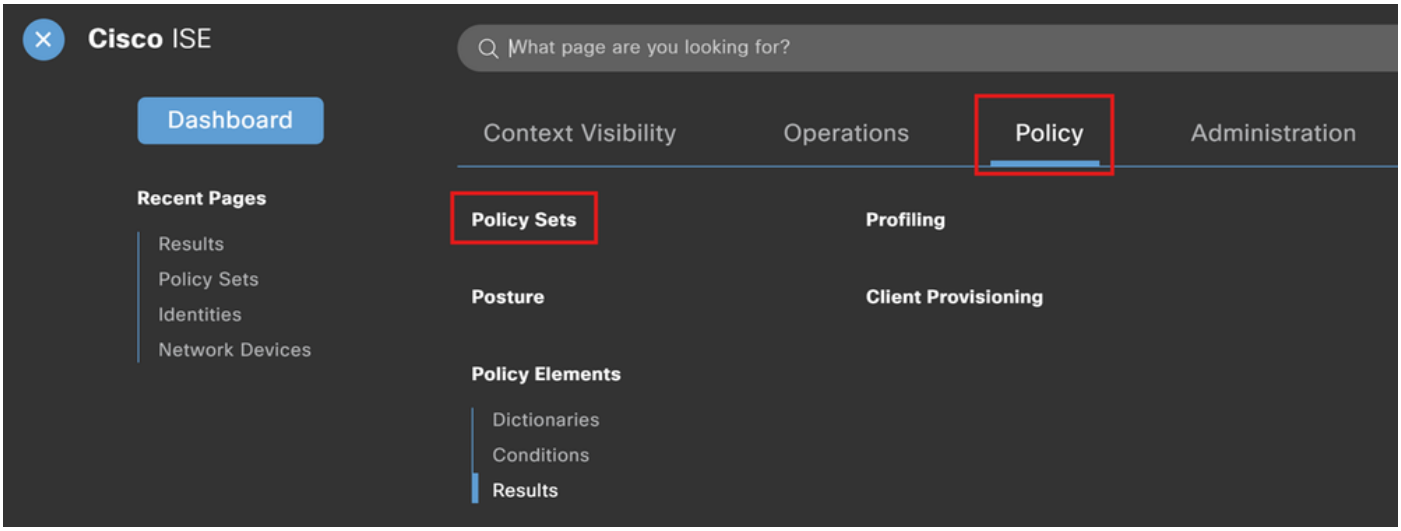
4단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동하여 권한 부여 프로파일을 볼 수 있습니다.



권한 부여 프로파일 목록

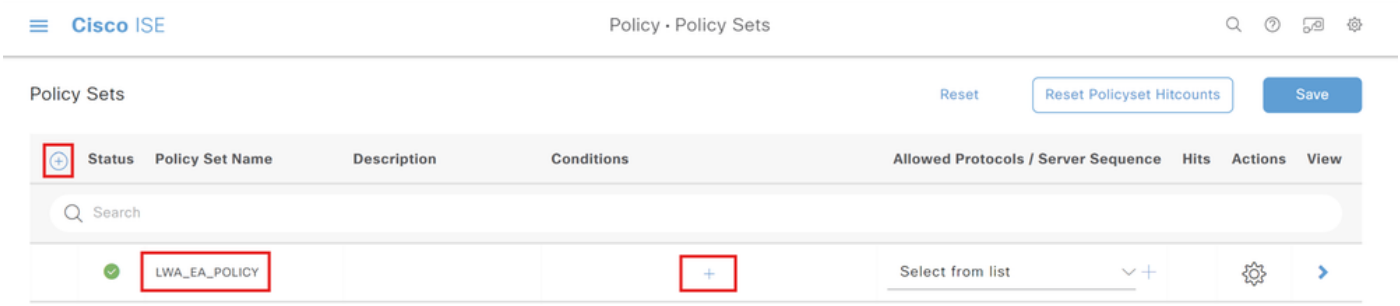
인증 규칙 구성

1단계. Policy(정책) > Policy Sets(정책 집합)로 이동합니다.



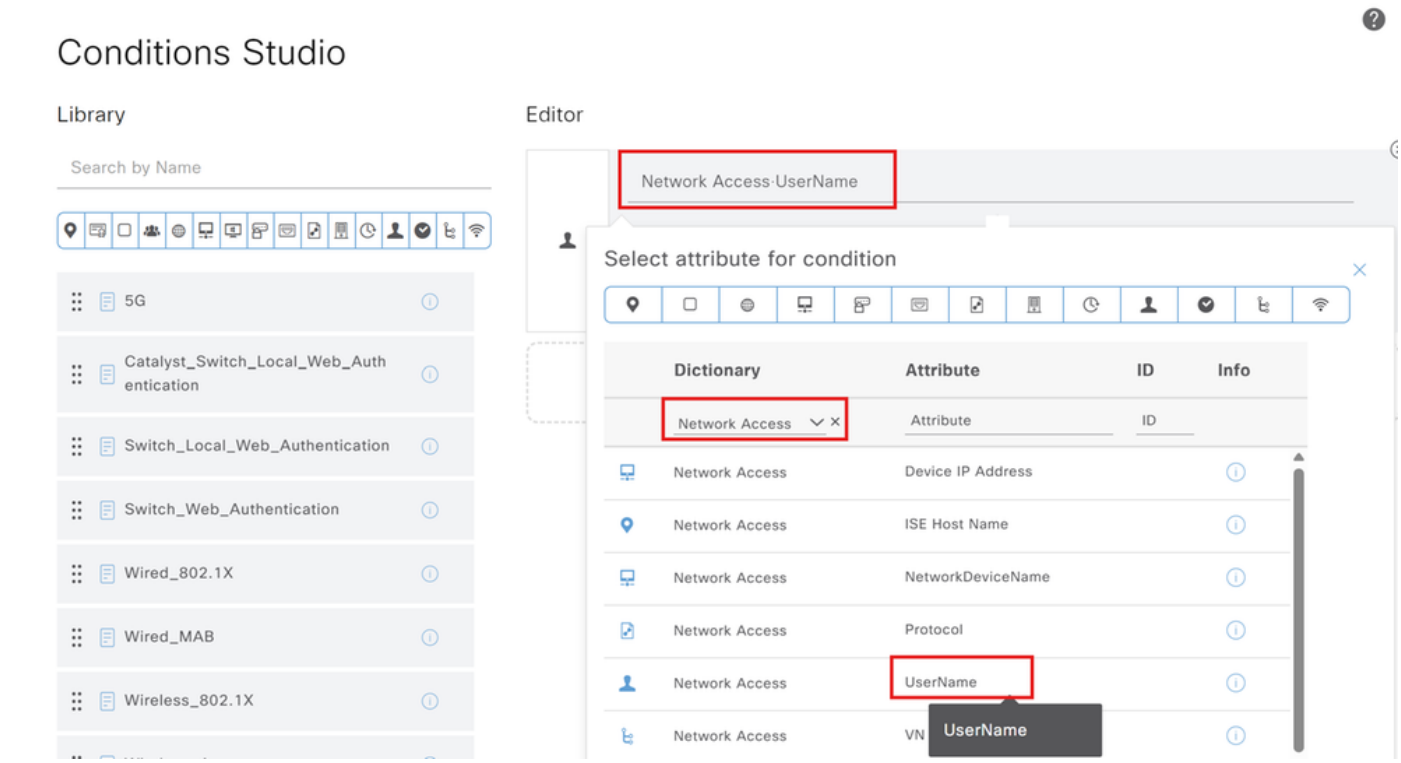
ISE 정책 - 정책 집합

2단계. + 기호를 선택하고 정책 집합 LWA_EA_POLICY의 이름을 입력합니다. Conditions(조건) 열을 클릭합니다.



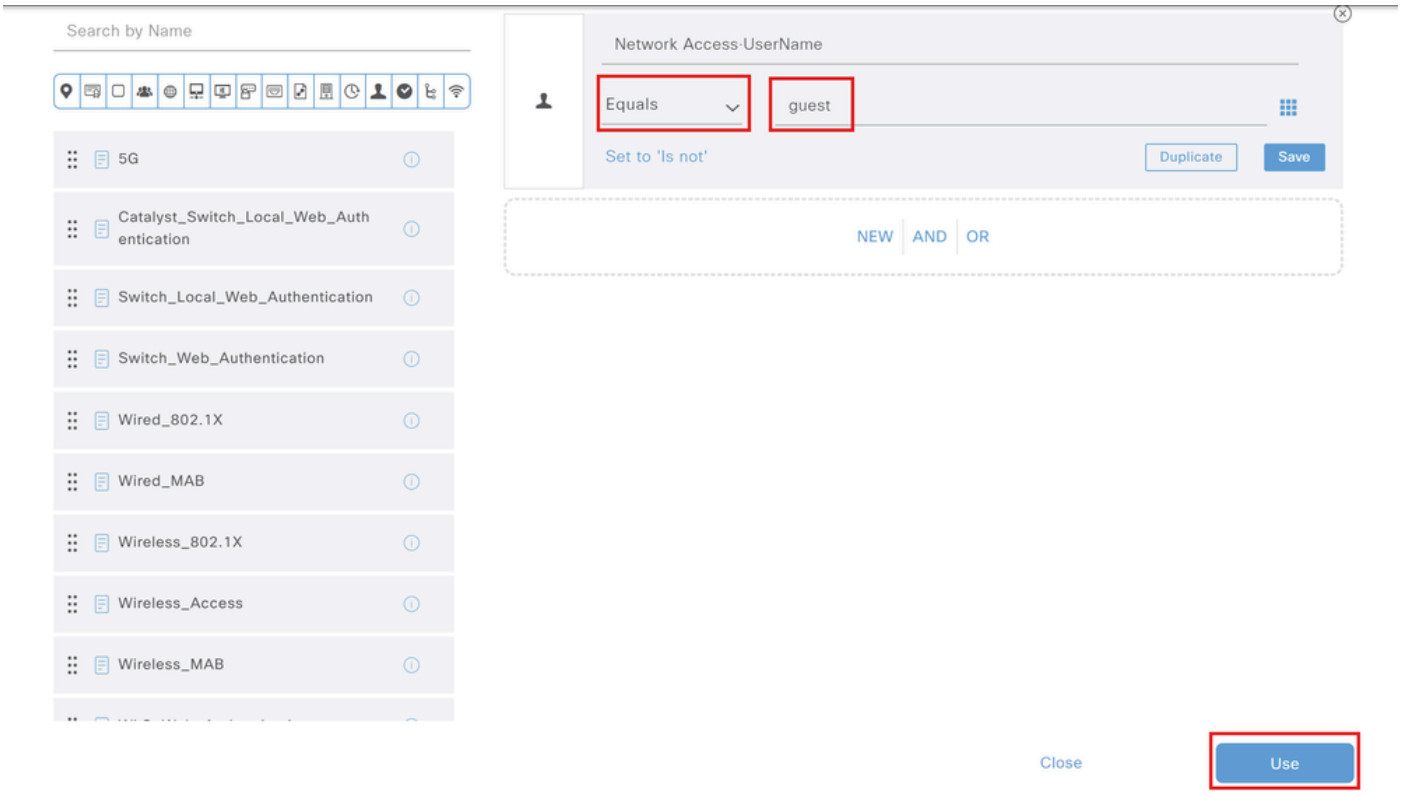
인증 규칙 구성

3단계. 사전에서 네트워크 액세스를 선택합니다. 속성에서 사용자 이름을 선택합니다.



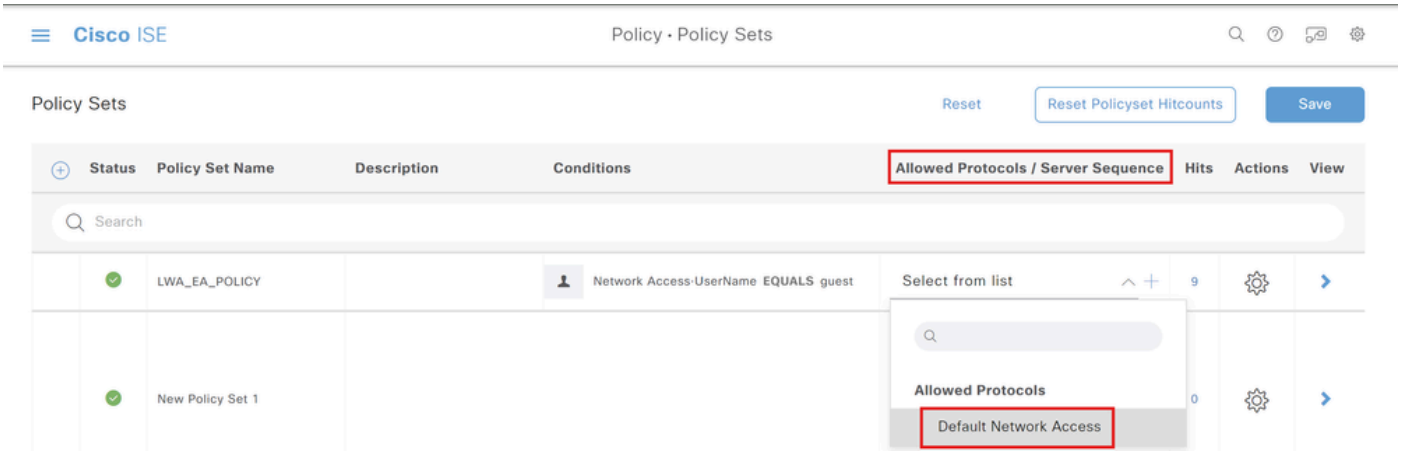
기본 네트워크 액세스

4단계. Equals(같음)를 설정하고 텍스트 상자에 guest(관리 > ID 관리 > ID > 사용자에 정의된 사용자 이름)를 입력합니다. 변경 사항을 저장하려면 저장(Save)을 클릭합니다.



사용자 이름 게스트

5단계. Policy(정책) > Policy Sets(정책 집합)로 이동합니다. 생성한 정책 집합에서 Allowed Protocols/Server Sequence(허용되는 프로토콜/서버 시퀀스) 열에서 Default Network Access(기본 네트워크 액세스)를 선택합니다.



정책 집합

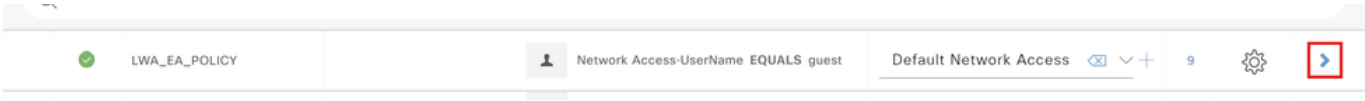
6단계. Save(저장)를 클릭하여 변경 사항을 저장합니다.

권한 부여 규칙 구성

권한 부여 규칙은 클라이언트에 어떤 권한(권한 부여 프로파일) 결과를 적용할지 결정하는 역할을

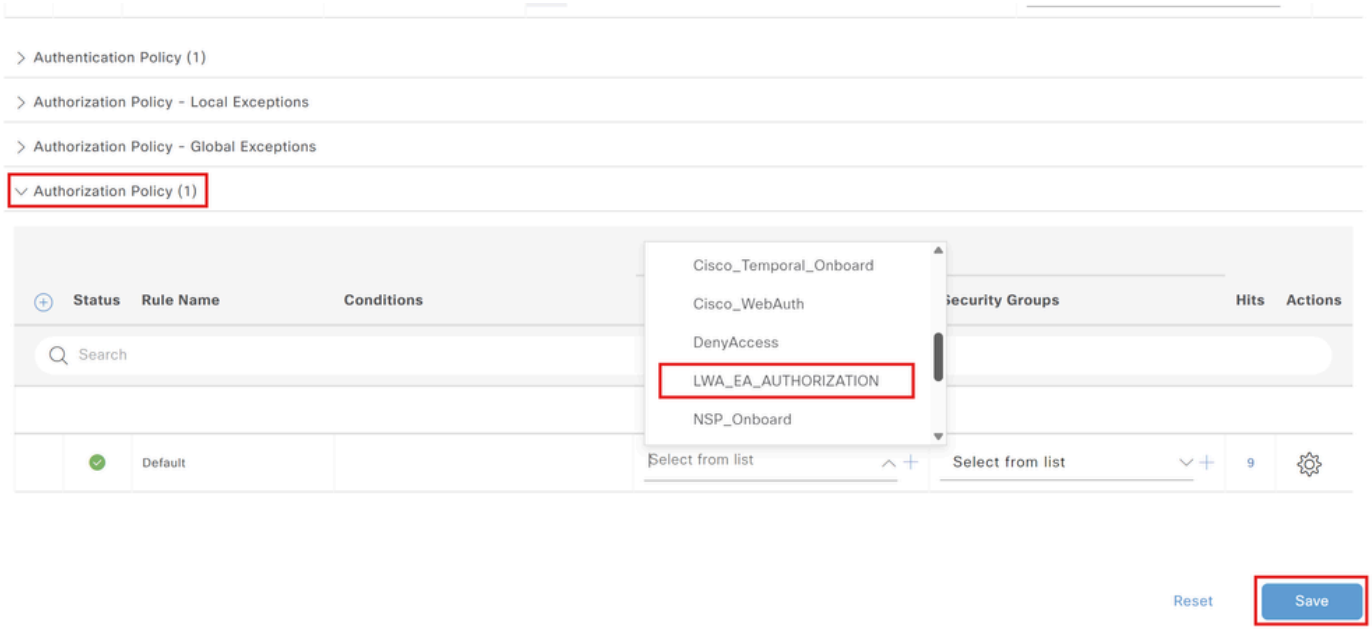
합니다.

1단계. Policy(정책) > Policy Sets(정책 집합)로 이동합니다. 생성한 정책 세트에서 화살표 아이콘을 클릭합니다.



정책 설정 화살표

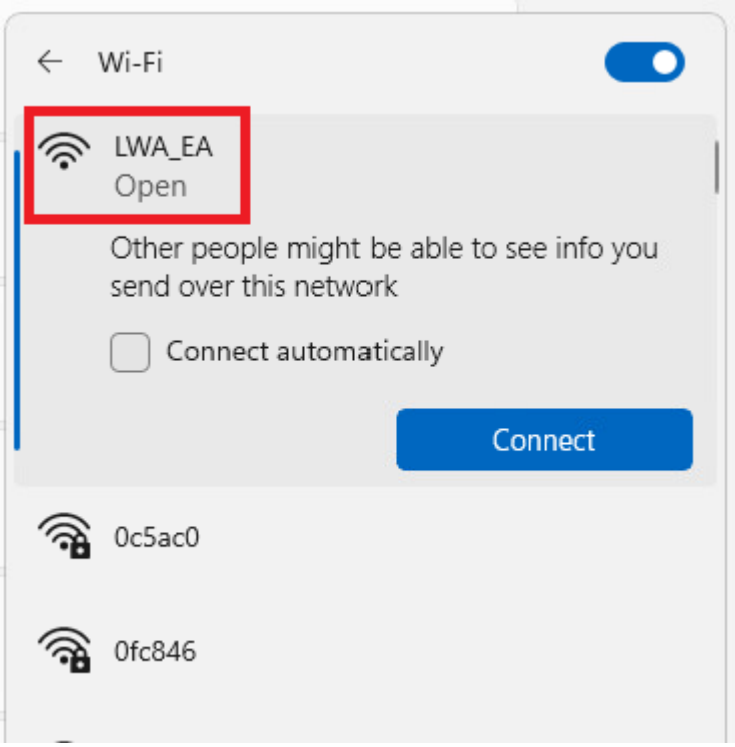
2단계. 동일한 Policy set(정책 설정) 페이지에서 이미지에 표시된 대로 Authorization Policy(권한 부여 정책)를 확장합니다. 프로필 열에서 DenyAccess를 삭제하고 LWA_EA_AUTHORIZATION을 추가합니다. 변경 사항을 저장하려면 저장을 누릅니다.



권한 부여 정책

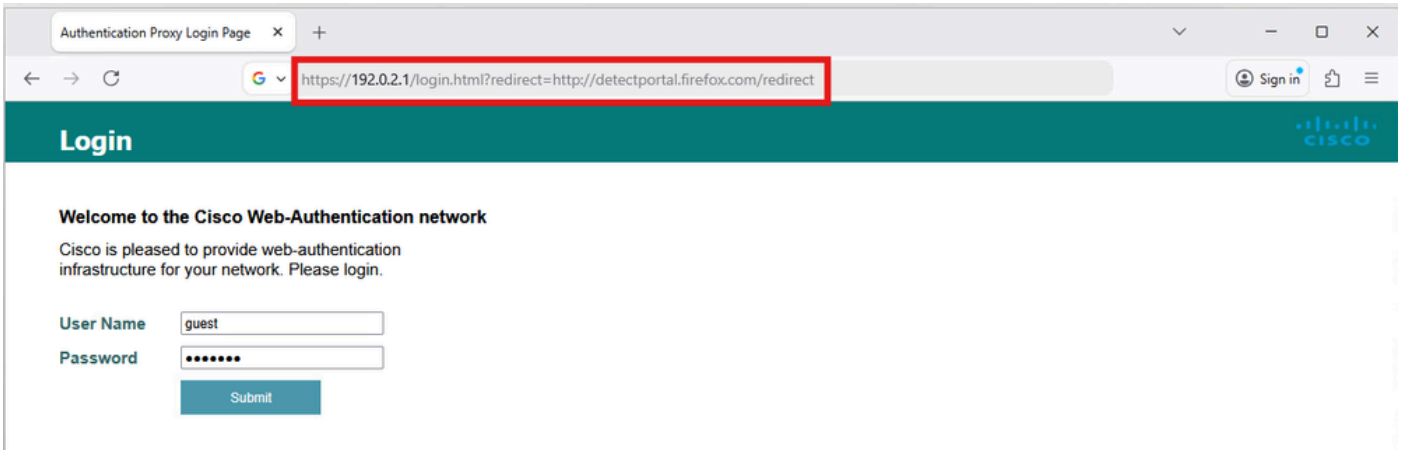
게스트 클라이언트 연결

1단계. 컴퓨터/전화기에서 Wi-Fi 네트워크로 이동하고 SSID LWA_EA를 찾은 후 Connect(연결)를 선택합니다.



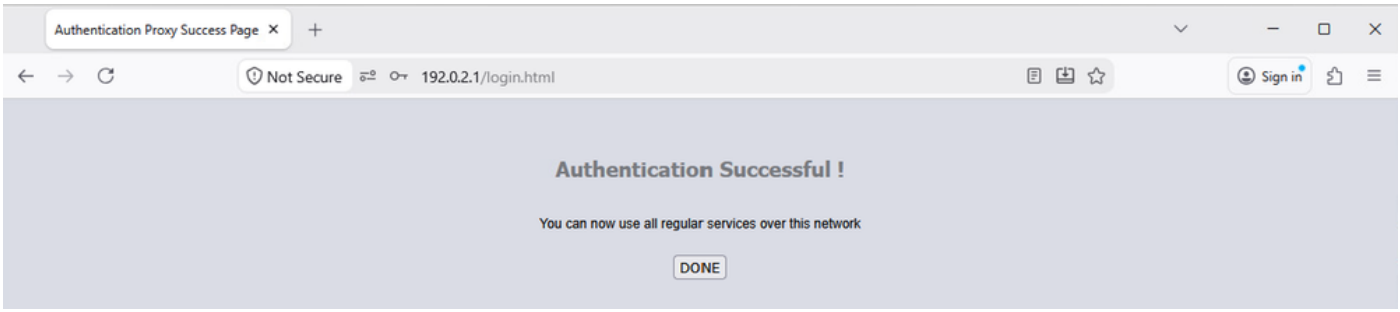
게스트 클라이언트 연결

2단계. 로그인 페이지가 표시된 브라우저 창이 나타납니다. 리디렉션 URL은 URL 상자에 있으며, 네트워크에 액세스하려면 사용자 이름과 비밀번호를 입력해야 합니다. 그런 다음 Submit(제출)을 선택합니다.



리디렉션 URL이 있는 로그인 페이지

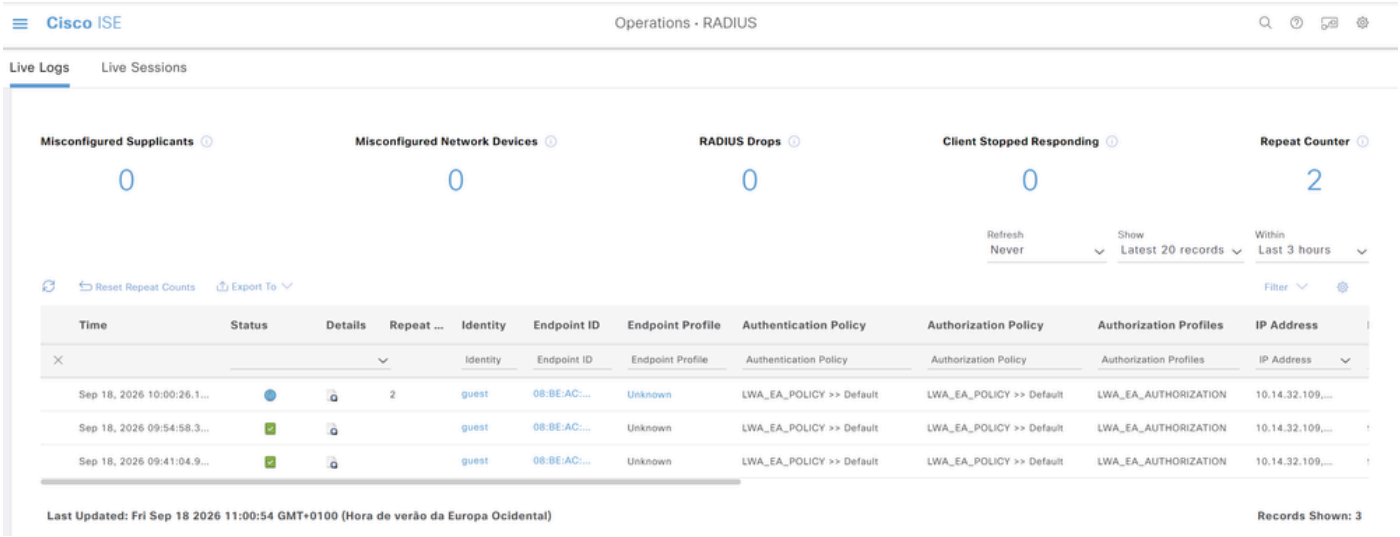
자격 증명이 올바르면 인증 성공 페이지가 나타납니다.



인증 성공 로그인 페이지

참고: 제시된 URL은 WLC에서 제공했습니다. 여기에는 WLC 가상 IP 및 Windows 연결 테스트 URL에 대한 리디렉션이 포함되어 있습니다.

3단계. Operations(운영) > RADIUS > Live Logs(라이브 로그)로 이동합니다. 인증 및 권한 부여 정책과 함께 인증된 클라이언트 디바이스를 볼 수 있습니다.



Radius 라이브 로그

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Show WLAN Summary

<#root>

9800WLC#show wlan summary

```
Number of WLANs: 1
```

```
ID Profile Name SSID Status 2.4GHz/5GHz Security
-----------------------------------------------
```

1 LWA_EA LWA_EA UP [open],[Web Auth]

```
9800WLC#
```

show wlan name LWA_EA

```
WLAN Profile Name : LWA_EA
==========================================
Identifier : 1
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security
```

Web Based Authentication : Enabled

```
OWE Transition Mode : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
```

Webauth Authentication List Name : LWA_AUTHENTICATION

Webauth Authorization List Name : Disabled

Webauth Parameter Map : global

```
(...)
Security-2.4GHz/5GHz
```

802.11 Authentication : Open System

```
Static WEP Keys : Disabled
```

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

```
OSEN : Disabled
PMF Support : Disabled
(...)
Band Select : Disabled
Load Balancing : Disabled
(...)
```

Show Parameter Map Configuration

9800WLC#show running-config | section parameter-map type webauth global

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint TP-self-signed-123456
```

Show AAA Information

<#root>

9800WLC#show aaa method-lists authentication

```
authen queue=AAA_ML_AUTHEN_LOGIN
```

name=LWA_AUTHENTICATION valid=TRUE id=BD000005 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)
```

9800WLC#show aaa method-lists authorization

```
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
```

name=LWA_AUTHORIZATION valid=TRUE id=90000006 :state=ALIVE : SERVER_GROUP RADIUSGROUP

```
author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)
```

9800WLC#show aaa servers

RADIUS: id 2, priority 1, host 192.0.2.30, auth-port 1812, acct-port 1813, hostname RADIUS

```
State: current UP, duration 8421s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 8421s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCD (0) : current UP
(...)
```

문제 해결

일반적인 문제

다음은 웹 인증 문제를 해결하는 방법에 대한 몇 가지 안내서입니다.

- 사용자는 인증할 수 없습니다.
- 인증서 문제.
- 리디렉션 URL이 작동하지 않습니다.
- 게스트 사용자는 게스트 WLAN에 연결할 수 없습니다.
- 사용자가 IP 주소를 가져오지 않습니다.
- Web Authentication Log in(웹 인증 로그인) 페이지로 리디렉션하지 못했습니다.
- 인증에 성공한 후 게스트 사용자는 인터넷에 액세스할 수 없습니다.

다음 가이드에서는 문제 해결 단계에 대해 자세히 설명합니다.

- 웹 인증에 대한 일반적인 문제 해결
- 트러블슈팅할 기타 상황

조건부 디버그 및 무선 활성 추적 및 포함된 패킷 캡처

조건부 디버그를 활성화하고 RA(Radio Active) 추적을 캡처할 수 있습니다. 그러면 지정된 조건(이 경우 클라이언트 mac 주소)과 상호 작용하는 모든 프로세스에 대한 디버그 레벨 추적이 제공됩니다. 조건부 디버그를 활성화하려면 가이드, 조건부 디버그 및 RadioActive 추적의 단계를 사용합니다.

EPC(Embedded Packet Capture)를 수집할 수도 있습니다. EPC는 Catalyst 9800 WLC로 향하는 패킷, 소스 패킷, LWA의 DHCP, DNS, HTTP GET 패킷을 볼 수 있는 패킷 캡처 기능입니다. 이러한 캡처는 Wireshark를 사용하여 오프라인 분석을 위해 내보낼 수 있습니다. 이 방법에 대한 자세한 단계는 Embedded Packet Capture를 참조하십시오.

성공한 시도의 예

RADIUS 서버를 사용하는 게스트 SSID에 연결된 상태에서 연결/인증 프로세스 시 각 단계를 성공적으로 식별하기 위한 RA_traces의 출력입니다.

802.11 연결/인증:

[client-orch-sm] [17062]: (참고): MAC: 08be.ac3f 연결을 받았습니다. BSSID cc70.edcf.552f, WLAN LWA_EA, 슬롯 1 AP 2ce3.8eb4, CW9172I-LAB
[client-orch-sm] [17062]: (디버그): MAC: 08be.ac3f Dot11 연결 요청을 받았습니다. 처리가 시작되었습니다 .SSID: LWA_EA, 정책 프로필: 정책 프로필, AP 이름: CW9172I-LAB, Ap Mac 주소: 2ce3.8eb4BSSID MAC000.0000.0000wlan ID: 1RSSI: -49, SNR: 46
[client-orch-state] [17062]: (참고): MAC: 08be.ac3f 클라이언트 상태 전환: S_CO_INIT -> S_CO_연결
[dot11-validate] [17062]: (정보): MAC: 08be.ac3f Dot11 ie는 ext/supp 속도를 확인합니다. 지원되는 속도 (radio_type 2)에 대한 검증 통과
[dot11-validate] [17062]: (정보): MAC: 08be.ac3f WiFi 다이렉트: Dot11은 P2P IE를 확인합니다. P2P IE가 없습니다.
[dot11] [17062]: (디버그): MAC: 08be.ac3f dot11에서 연결 응답을 보냅니다. resp_status_code를 사용한 프레이밍 연결 응답: 0
[dot11] [17062]: (디버그): MAC: 08be.ac3f Dot11 기능 정보 바이트1 1, 바이트2: 11
[dot11-frame] [17062]: (정보): MAC: 08be.ac3f WiFi 다이렉트: P2P IE를 사용하여 Assoc Resp 빌드 건너뛰기: Wifi 직접 정책 사용 안 함
[dot11] [17062]: (정보): MAC: 08be.ac3f dot11에서 연결 응답을 보냅니다. 연결 응답(길이) 보내기: 130(resp_status_code 포함): 0, DOT11_상태: DOT11_상태_성공
[dot11] [17062]: (참고): MAC: 08be.ac3f 연결 성공. AID 1, 로밍 = False, WGB = False, 11r = False, 11w = False 빠른 로밍 = False
[dot11] [17062]: (정보): MAC: 08be.ac3f DOT11 상태 전환: S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (디버그): MAC: 08be.ac3f Station Dot11 연결에 성공했습니다.

IP 학습 프로세스:

[client-orch-state] [17062]: (참고): MAC: 08be.ac3f 클라이언트 상태 전환: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: (정보): MAC: 08be.ac3f IP-learn 상태 전환: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (정보): MAC: 08be.ac3f 클라이언트 인증 인터페이스 상태 전환: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: (참고): MAC: 08be.ac3f 클라이언트 IP에 대해 알아보았습니다. 방법: DHCP IP: 10.14.32.109
[client-iplearn] [17062]: (정보): MAC: 08be.ac3f IP-learn 상태 전환: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
[client-orch-sm] [17062]: (디버그): MAC: 08be.ac3f ip learn 응답을 받았습니다. 방법: IPLEARN_METHOD_DHCP

레이어 3 인증:

[client-orch-sm] [17062]: (디버그): MAC: 08be.ac3f 트리거된 L3 인증. 상태 = 0x0, 성공
[client-orch-state] [17062]: (참고): MAC: 08be.ac3f 클라이언트 상태 전환: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: (참고): MAC: 08be.ac3f L3 인증이 시작되었습니다. LWA
[client-auth] [17062]: (정보): MAC: 08be.ac3f 클라이언트 인증 인터페이스 상태 전환: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING

[webauth-httpd] [17062] (정보): capwap_90000004[08be.ac3f][10.14.32.109]로그인 상태일 때 수신 요청
[webauth-httpd] [17062] (정보): capwap_90000004[08be.ac3f][10.14.32.109]HTTP GET 요청

[webauth-httpd] [17062] (정보): capwap_90000004[08be.ac3f][10.14.32.109]구문 분석 GET, src [10.14.32.109] dst [10.107.221.82] url [http://firefox detect portal/]
[webauth-httpd] [17062] (정보): capwap_90000004[08be.ac3f][10.14.32.109]읽기 완료: parse_request 반환 8
[webauth-io] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO 상태 읽기 -> 쓰기
[webauth-io] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]56538/219 IO 상태 쓰기 -> 읽기
[webauth-io] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO 상태 새 -> 읽기
[webauth-io] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 읽기 이벤트, 메시지 준비됨
[webauth-httpd] [17062] (정보): capwap_90000004[08be.ac3f][10.14.32.109]로그인 상태일 때 POST 수신

레이어 3 인증에 성공하면 클라이언트를 RUN 상태로 이동합니다.

[인증 관리자] [17062]: (정보): [08be.ac3f:capwap_90000004] 08be.ac3f 클라이언트에 대한 사용자 이름 게스트를 받았습니다.
[인증 관리자] [17062]: (정보): [08be.ac3f:capwap_90000004] auth mgr attr 추가/변경 알림이 attr auth-domain(954)에 대해 수신되었습니다.
[인증 관리자] [17062]: (정보): [08be.ac3f:capwap_90000004] 메서드 webauth가 상태를 'Running'에서 'Authc Success'로 변경합니다.
[인증 관리자] [17062]: (정보): [08be.ac3f:capwap_90000004] 컨텍스트 변경 상태가 '실행 중'에서 '인증 성공'으로
[인증 관리자] [17062]: (정보): [08be.ac3f:capwap_90000004] auth mgr attr 추가/변경 알림이 attr 메서드에 대해 수신됨(757)
[인증 관리자] [17062]: (정보): [08be.ac3f:capwap_90000004] 이벤트 AUTHZ_SUCCESS (11)
[인증 관리자] [17062]: (정보): [08be.ac3f:capwap_90000004] 컨텍스트 변경 상태가 '인증 성공'에서 '인증 성공'으로
[웹 인증 acl] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]SVM을 통해 IPv4 로그아웃 ACL 적용, 이름: IP-Adm-V4-LOGOUT-ACL, 우선 순위: 51, IIF-ID: 0
[webauth-sess] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]Param-map 사용: 글로벌
[webauth-state] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]Param-map 사용: 글로벌
[webauth-state] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]상태 AUTHC_SUCCESS -> AUTHZ
[웹 인증 페이지] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]Webauth 성공 페이지 보내기
[webauth-io] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO 상태 인증 -> 쓰기
[webauth-io] [17062]: (정보): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO 상태 쓰기 -> 끝
[webauth-httpd] [17062] (정보): capwap_90000004[08be.ac3f][10.14.32.109]56539/218 IO ctx를 제거하고 소켓, id [99000029] 닫기
[client-auth] [17062]: (참고): MAC: 08be.ac3f L3 인증 성공 ACL:[]
[client-auth] [17062]: (정보): MAC: 08be.ac3f 클라이언트 인증 인터페이스 상태 전환: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[webauth-httpd] [17062] (정보): capwap_90000004[08be.ac3f][10.48.39.243]56538/219 IO ctx를 제거하고 소켓, id [D7000028]를 닫습니다.
[오류 메시지] [17062]: (정보): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0 wncd: MAC이 있는 디바이스의 ssid(LWA_EA)에 연결된 사용자 이름 항목(게스트): 08be.ac3f
[aaa-attr-inf] [17062]: (정보): [적용된 특성: bsn-vlan-interface-name 0 " VLAN0039"]
[aaa-attr-inf] [17062]: (정보): [적용된 특성: 시간 초과 0 1800(0x708)]
[aaa-attr-inf] [17062]: (정보): [적용된 특성: url-redirect-acl 0 " IP-Adm-V4-LOGOUT-ACL"]
[ewlc-qos-client] [17062]: (정보): MAC: 08be.ac3f 클라이언트 QoS 실행 상태 처리기

[rog-proxy-capwap] [17062]: (디버그): 관리되는 클라이언트 RUN 상태 알림: 08be.ac3f
[client-orch-state] [17062]: (참고): MAC: 08be.ac3f 클라이언트 상태 전환: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

관련 정보

- Cisco 기술 지원 및 다운로드

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.