Catalyst 9800 및 FlexConnect OEAP 스플릿 터널링 구성

목차

소개

이 문서에서는 실내 액세스 포인트(AP)를 FlexConnect Office Extend(OEAP)로 구성하는 방법 및 홈 오피스에서 로컬로 스위칭할 수 있는 트래픽과 WLC에서 중앙에서 전환해야 하는 트래픽을 정의할 수 있도록 스플릿 터널링을 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서의 컨피그레이션에서는 WLC가 NAT가 활성화된 DMZ에 이미 구성되어 있고 AP가 홈 오피스에서 WLC에 조인할 수 있다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS-XE 17.3.1 소프트웨어를 실행하는 Wireless LAN Controller 9800
- Wave1 AP: 1700/2700/3700 .
- Wave2 AP: 1800/2800/3800/4800 및 Catalyst 9100 시리즈입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

개요

Cisco OfficeExtend Access Point(Cisco OEAP)는 Cisco WLC에서 원격 위치의 Cisco AP로 안전한 통신을 제공하며, 인터넷을 통해 기업 WLAN을 직원의 거주지로 원활하게 확장합니다. 홈 오피스에서 사용하는 사용자의 경험은 기업 사무실에서와 정확히 동일합니다. 액세스 포인트와 컨트롤러 간의 DTLS(Datagram Transport Layer Security) 암호화를 통해 모든 통신에서 최고 수준의 보안을 유지할 수 있습니다. FlexConnect 모드의 모든 실내 AP는 OEAP로 작동할 수 있습니다.

배경 정보

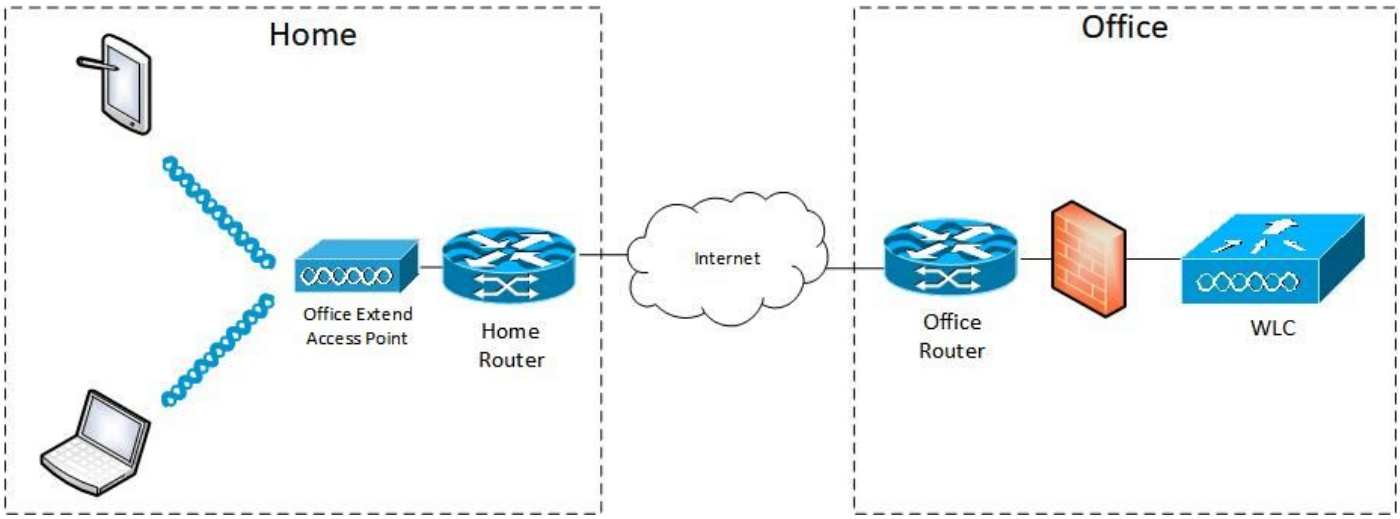
FlexConnect는 WAN을 통해 원격 위치에서 작업하는 동안 무선 클라이언트를 처리하는 액세스 포인트(AP) 기능을 의미합니다. 또한 무선 클라이언트의 트래픽이 AP 레벨(로컬 스위칭)에서 네트워크에 직접 연결되는지 아니면 트래픽이 9800 컨트롤러(중앙 스위칭)로 중앙 집중화되어 WLAN별로 WAN을 통해 다시 전송되는지 결정할 수 있습니다.

FlexConnect에 대한 자세한 내용은 이 문서 Deunderstand FlexConnect on Catalyst 9800 Wireless Controller를 참조하십시오.

OEAP 모드는 FlexConnect AP에서 사용할 수 있는 옵션으로, 예를 들어 홈 액세스를 위한 개인 로컬 SSID와 스플릿 터널링 기능을 제공하여 더 세분화된 방식으로 홈 오피스에서 로컬로 스위칭해야 하는 트래픽과 단일 WLAN을 통해 WLC에서 중앙 집중식으로 전환해야 하는 트래픽을 정의할 수 있습니다

구성

네트워크 다이어그램



구성

스플릿 터널링에 대한 액세스 제어 목록 정의

1단계. Configuration > Security > ACL을 선택합니다. 추가를 선택합니다.

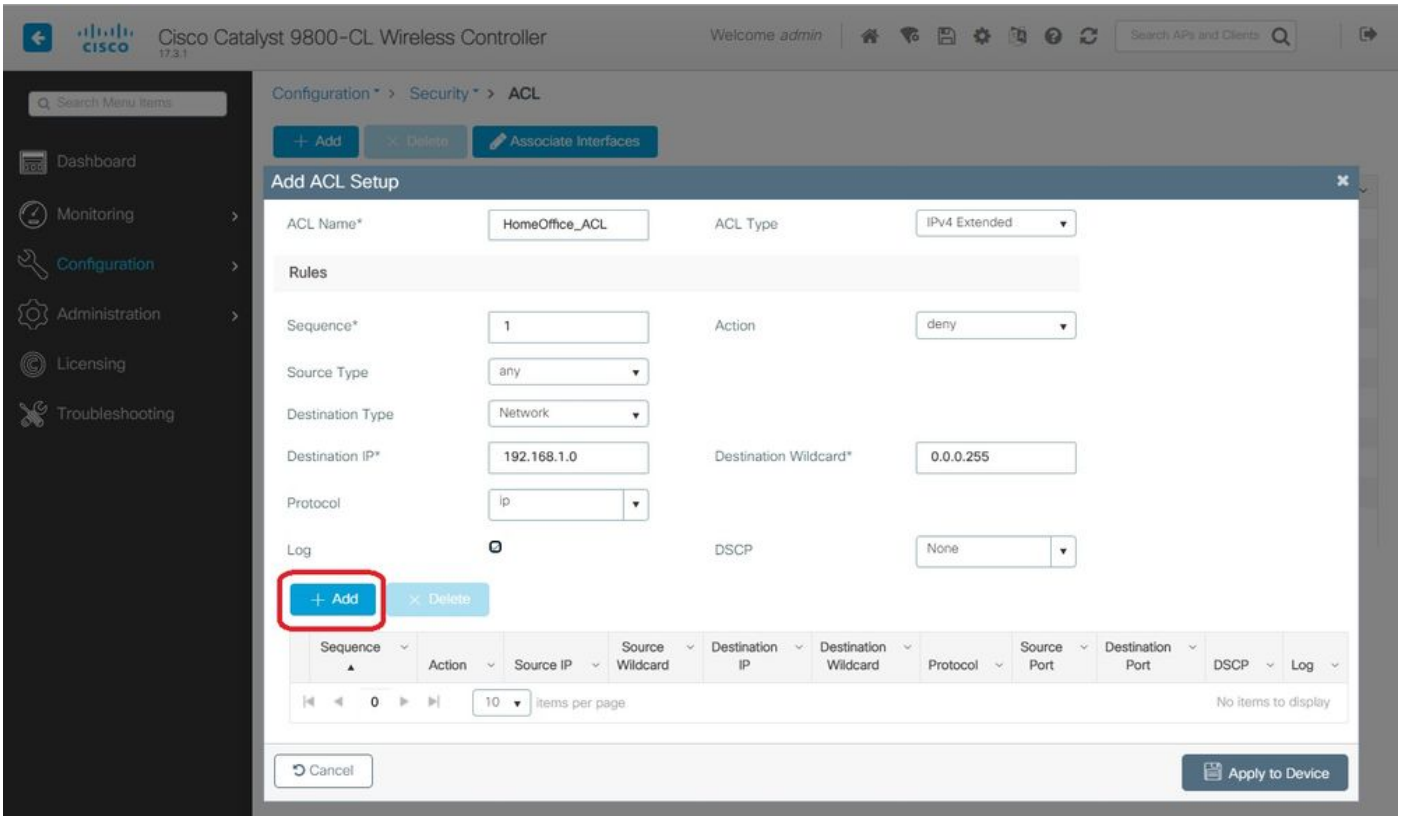
2단계. Add ACL Setup(ACL 설정 추가) 대화 상자에서 ACL Name(ACL 이름)을 입력하고 ACL Type(ACL 유형) 드롭다운 목록에서 ACL 유형을 선택하고 Rules(규칙) 설정에서 Sequence number(시퀀스 번호)를 입력합니다. 그런 다음 작업을 허용 또는 거부로 선택합니다.

3단계. Source Type 드롭다운 목록에서 필요한 소스 유형을 선택합니다.

소스 유형을 Host(호스트)로 선택하는 경우 Host Name/IP를 입력해야 합니다.

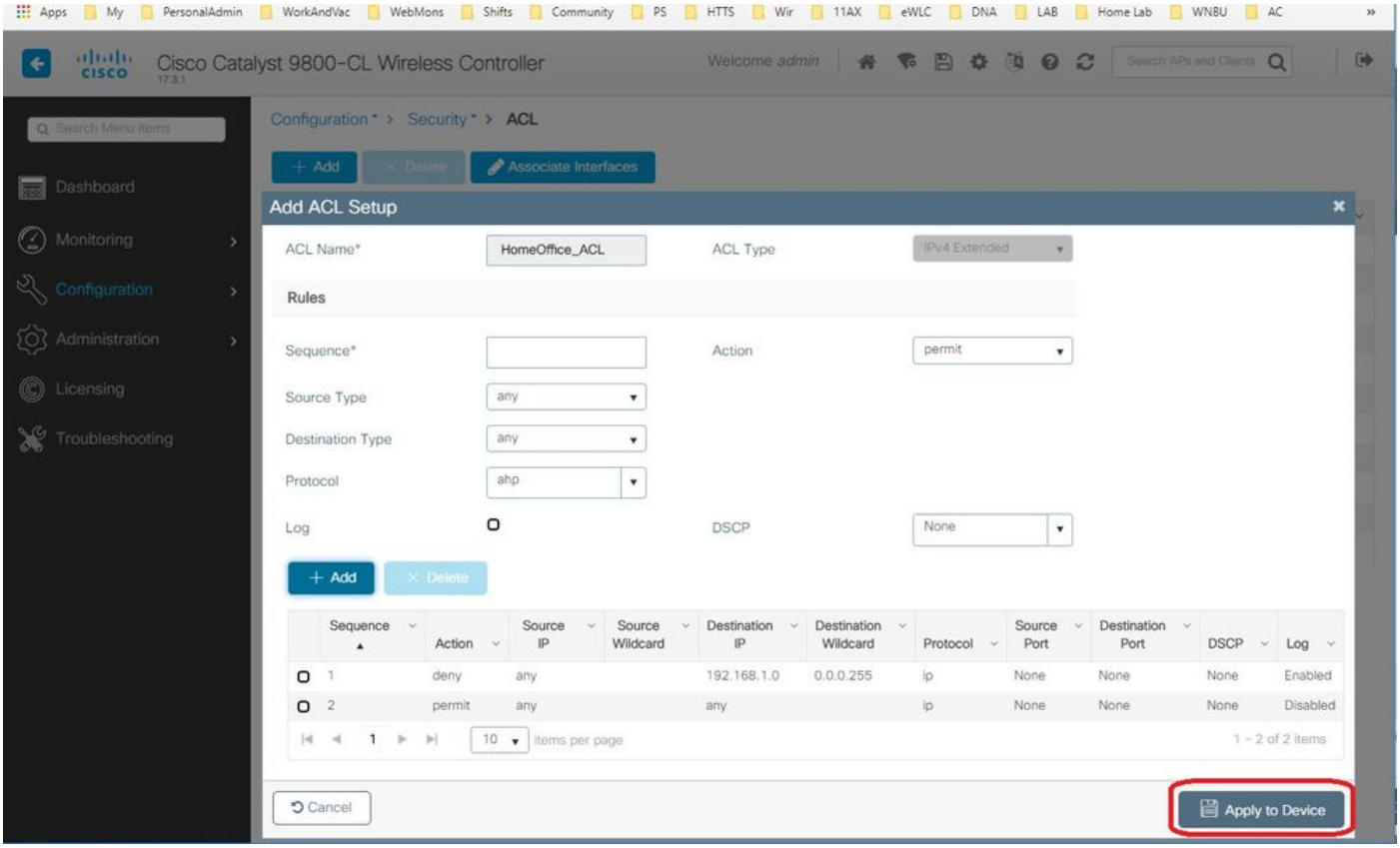
소스 유형을 Network(네트워크)로 선택하는 경우 소스 IP 주소와 소스 와일드카드 마스크를 지정해야 합니다.

이 예에서는 임의의 호스트에서 서브넷 192.168.1.0/24으로 향하는 모든 트래픽이 중앙에서 전환(거부)되고 나머지 트래픽은 모두 로컬로 스위칭됩니다(허용).



4단계. 로그를 원하는 경우 로그 확인란을 선택하고 추가를 선택합니다.

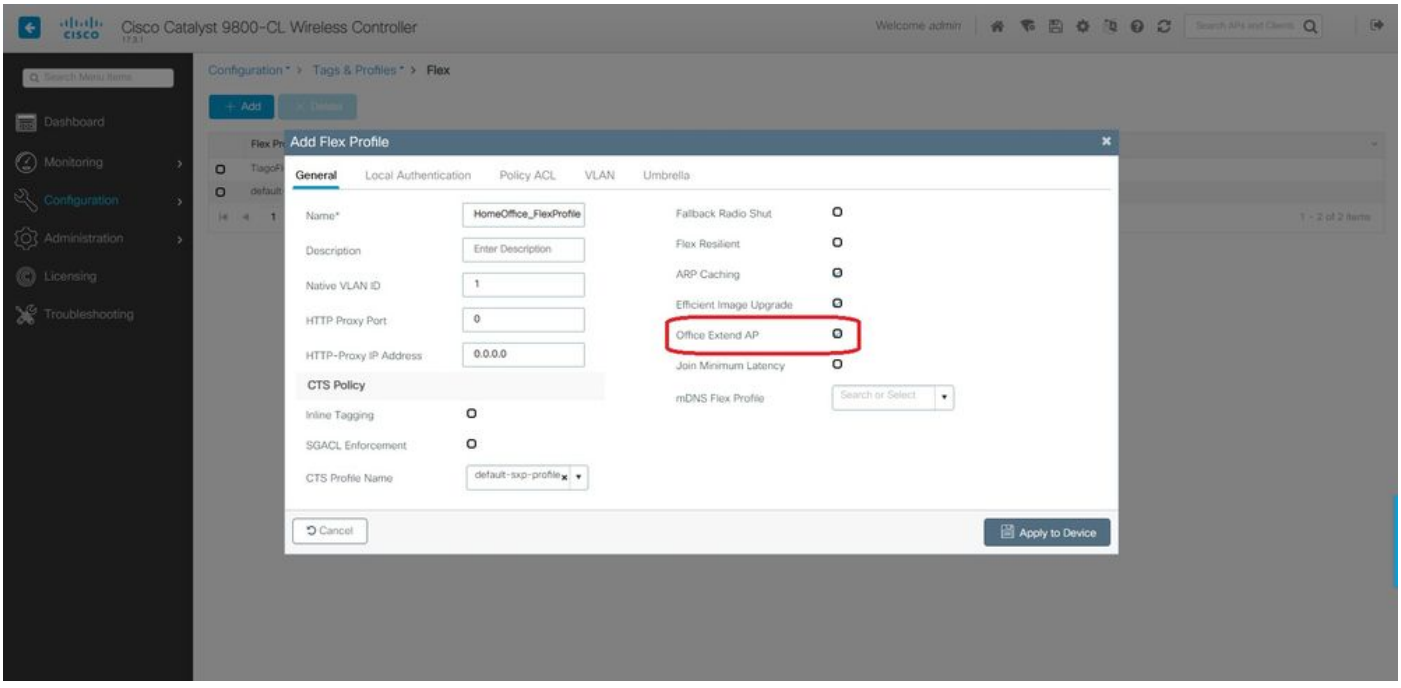
5단계. 나머지 규칙을 추가하고 Apply to Device를 선택합니다.



ACL 정책을 정의된 ACL에 연결

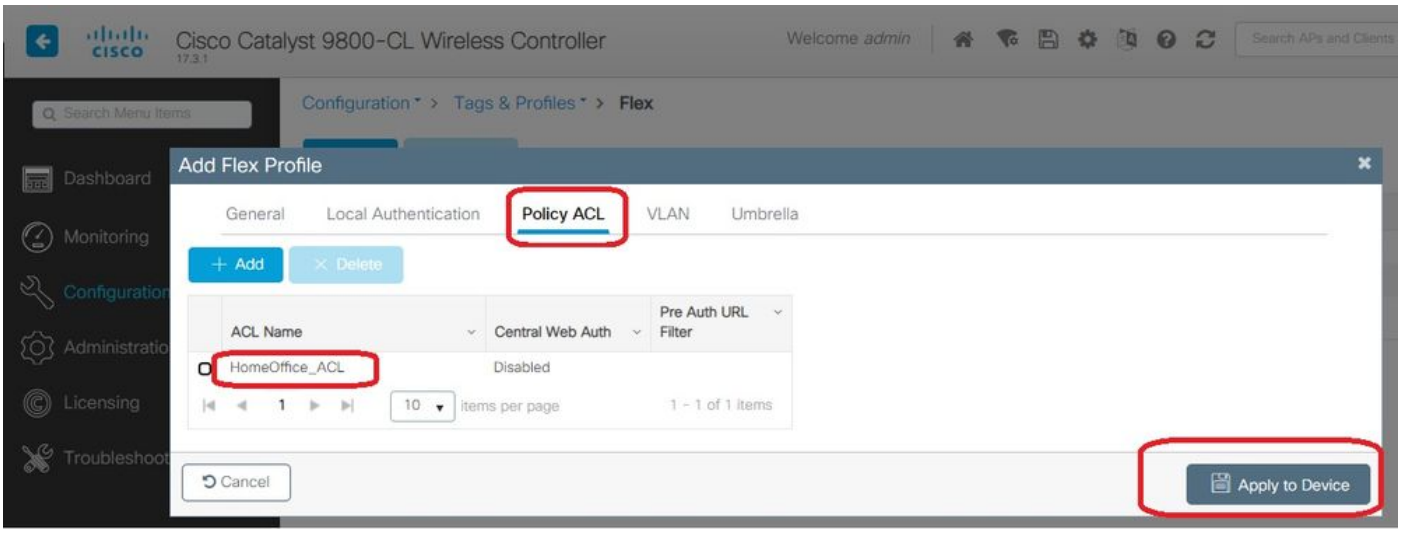
1단계. 새 Flex 프로파일을 생성합니다. Configuration(구성) > Tags & Profiles(태그 및 프로파일) > Flex(플렉스)로 이동합니다. 추가를 선택합니다.

2단계. 이름을 입력하고 OEAP를 활성화합니다. 또한 네이티브 VLAN ID가 AP 스위치 포트의 ID인지 확인합니다.



참고: Office-Extend 모드를 활성화하면 링크 암호화가 기본적으로 활성화되어 있으며 AP 가입 프로필에서 링크 암호화를 비활성화하더라도 변경할 수 없습니다.

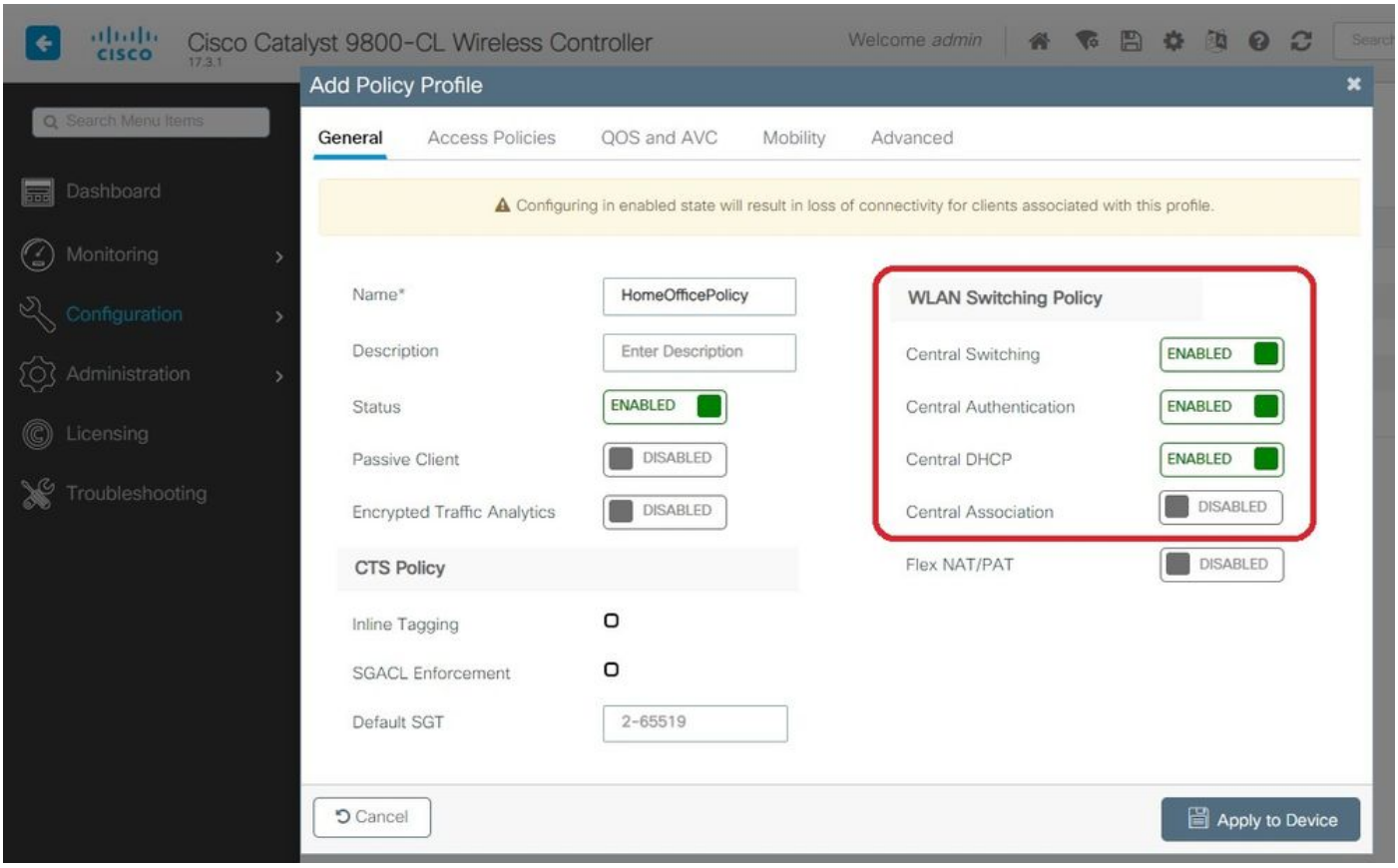
3단계. Policy ACL(정책 ACL) 탭으로 이동하고 Add(추가)를 선택합니다. 여기서 프로파일에 ACL을 추가하고 디바이스에 적용합니다.



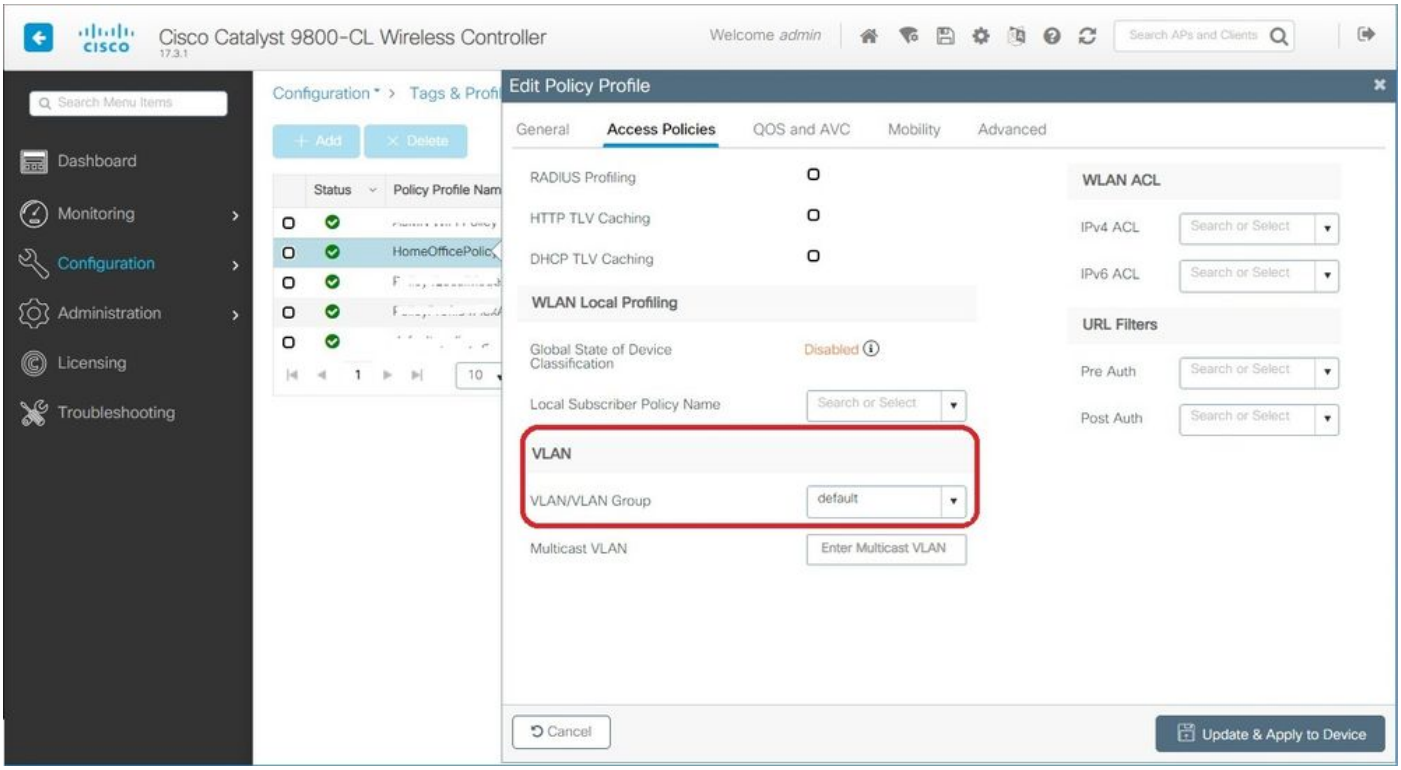
무선 프로파일 정책 및 스플릿 MAC ACL 이름 구성

1단계. WLAN 프로파일을 생성합니다. 이 예에서는 WPA2-PSK 보안이 포함된 HomeOffice라는 SSID를 사용했습니다.

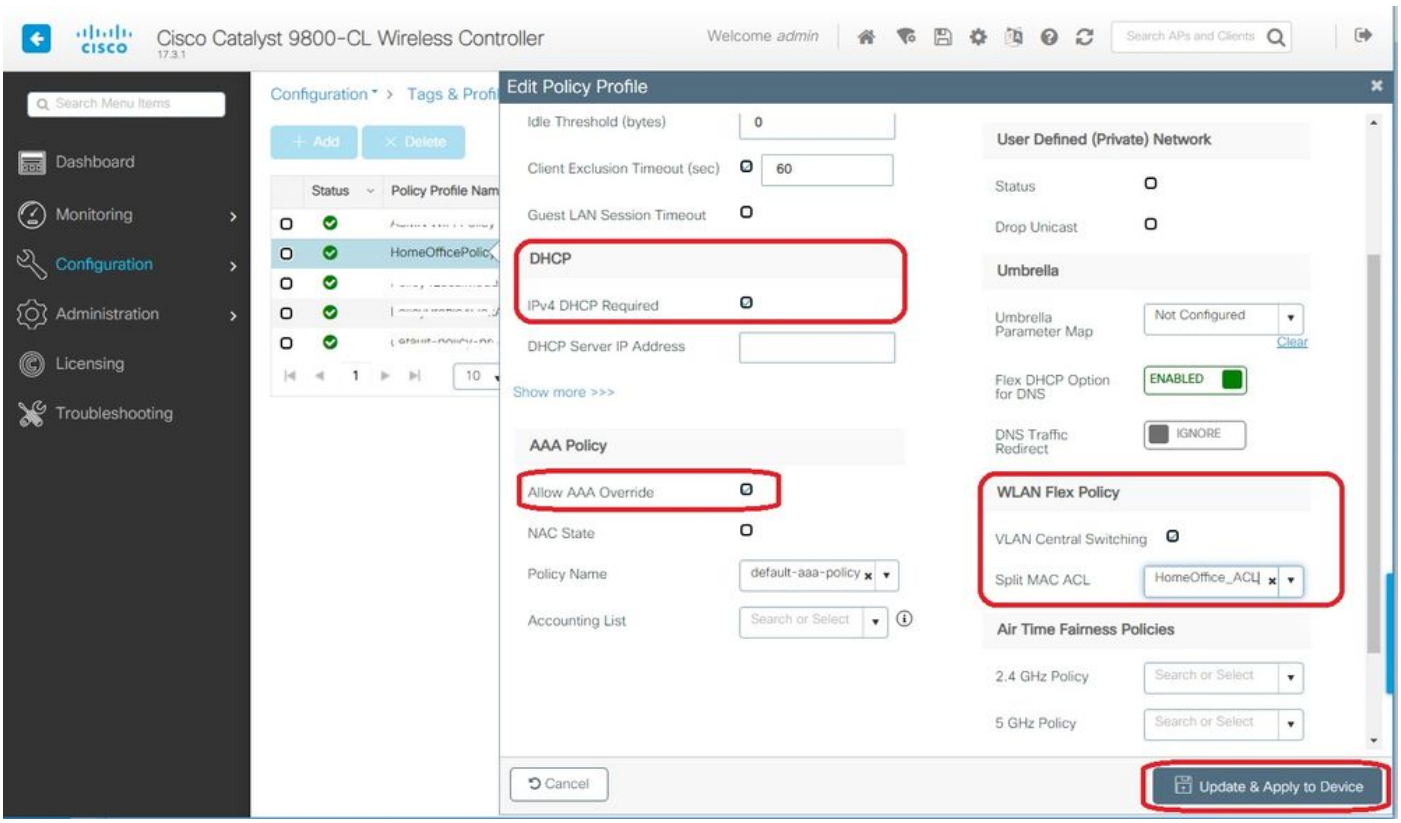
2단계. 정책 프로파일을 생성합니다. [구성] > [태그] > [정책]으로 이동하여 [추가]를 선택합니다. [일반]에서 이 프로파일이 다음 예와 같이 중앙 전환된 정책인지 확인합니다.



3단계. Policy Profile(정책 프로파일) 내에서 Access Policies(액세스 정책)로 이동하여 중앙에서 전환할 트래픽의 VLAN을 정의합니다. 클라이언트는 이 VLAN에 할당된 서브넷에서 IP 주소를 가져옵니다.



4단계. AP에서 로컬 스플릿 터널링을 구성하려면 WLAN에서 DCHP Required를 사용하도록 설정해야 합니다. 이렇게 하면 스플릿 WLAN과 연결된 클라이언트가 DHCP를 수행합니다. Advanced(고급) 탭의 Policy Profile(정책 프로파일)에서 이 옵션을 활성화할 수 있습니다. IPv4 DHCP Required(IPv4 DHCP 필요) 확인란을 활성화합니다. WLAN Flex Policy(WLAN 플렉스 정책) 설정의 Split MAC ACL(MAC ACL 분할) 드롭다운 목록에서 이전에 생성된 분할 MAC ACL을 선택합니다. 장치에 적용 선택:



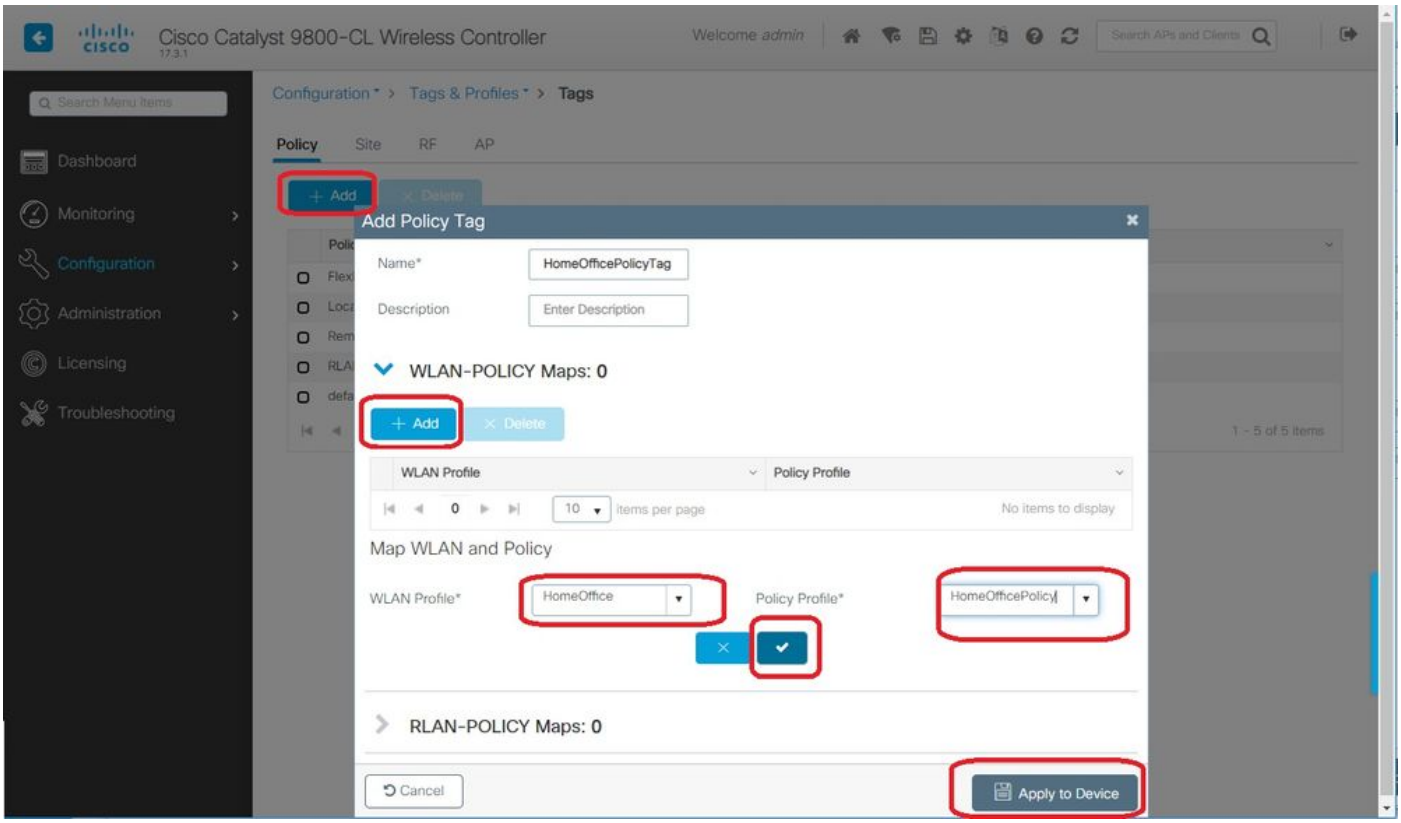
참고: Apple iOS 클라이언트는 분할 터널링이 작동하려면 DHCP 제안에서 옵션 6(DNS)을 설정해야 합니다.

정책 프로필에 WLAN 매핑

1단계. Configuration(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그)를 선택합니다. Policy(정책) 탭에서 Add(추가)를 선택합니다.

2단계. Tag Policy(태그 정책)의 이름을 입력하고 WLAN-POLICY Maps(WLAN-POLICY 맵) 탭에서 Add(추가)를 선택합니다.

3단계. WLAN Profile(WLAN 프로필) 드롭다운 목록에서 WLAN 프로필을 선택하고 Policy Profile(정책 프로필) 드롭다운 목록에서 Policy profile(정책 프로필)을 선택합니다. Tick Icon을 선택한 다음 Apply to Device를 선택합니다.

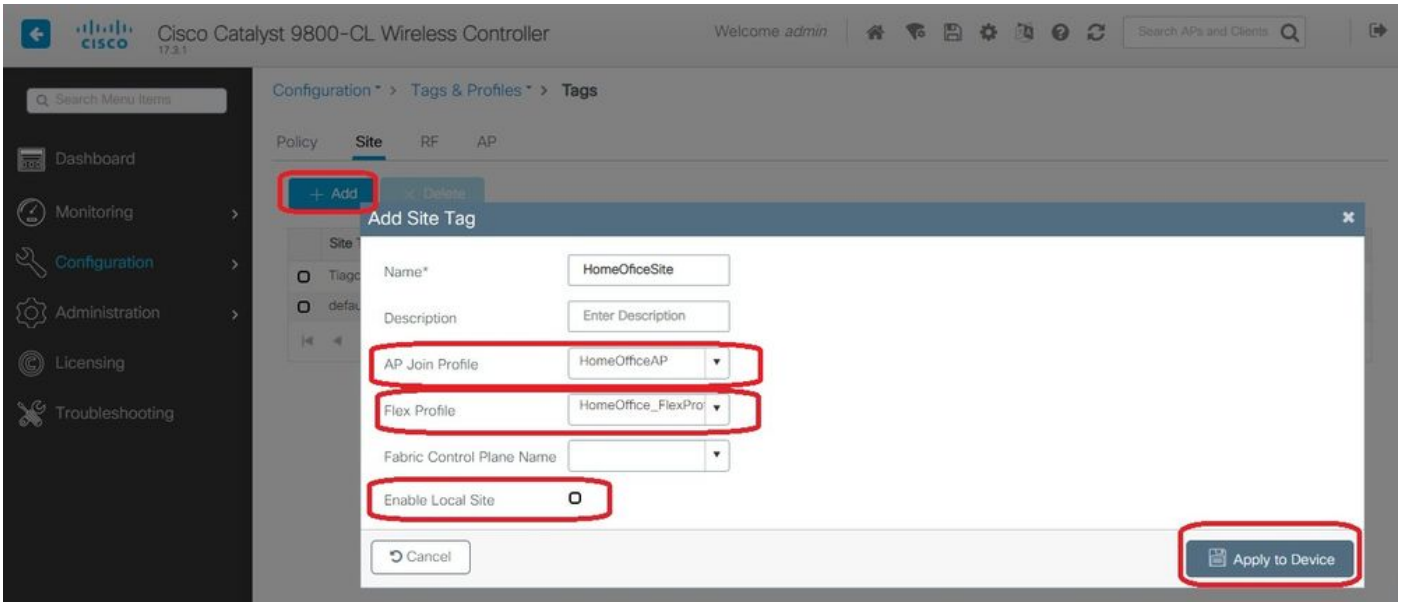


AP 가입 프로필 구성 및 사이트 태그와 연결

1단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > AP Join(AP 조인)으로 이동하고 Add(추가)를 선택합니다. 이름을 입력합니다. 필요에 따라 SSH를 활성화하여 문제 해결을 허용하고 나중에 필요하지 않은 경우 비활성화할 수 있습니다.

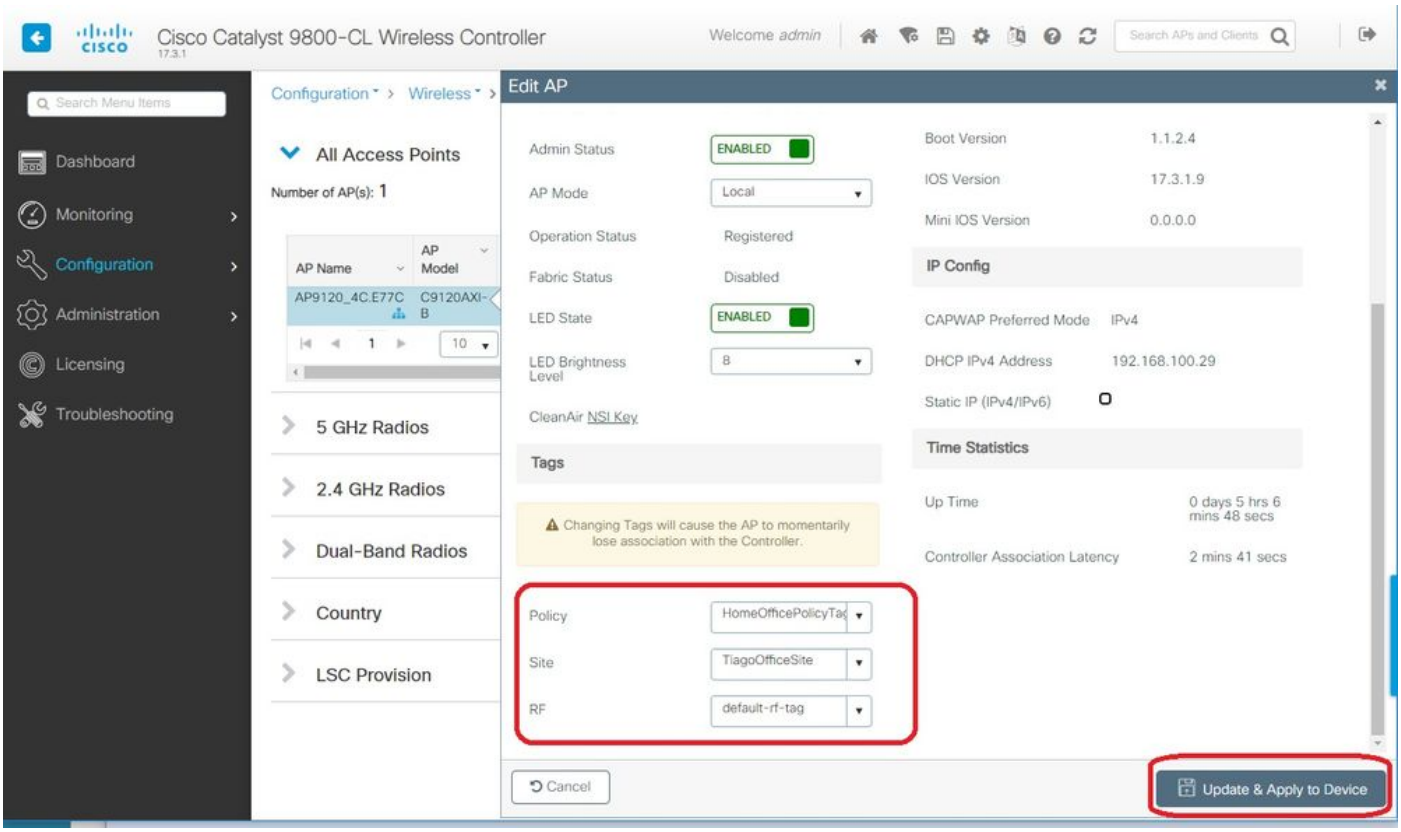
2단계. Configuration(구성) > Tags & Profiles(태그 및 프로파일) > Tags(태그)를 선택합니다. 사이트 탭에서 추가를 선택합니다.

3단계. 사이트 태그의 이름을 입력하고, Enable Local Site(로컬 사이트 활성화)를 선택 취소한 다음, 드롭다운 목록에서 AP Join Profile(AP 가입 프로필) 및 Flex Profile(전에 생성)을 선택합니다. 그런 다음 장치에 적용합니다.

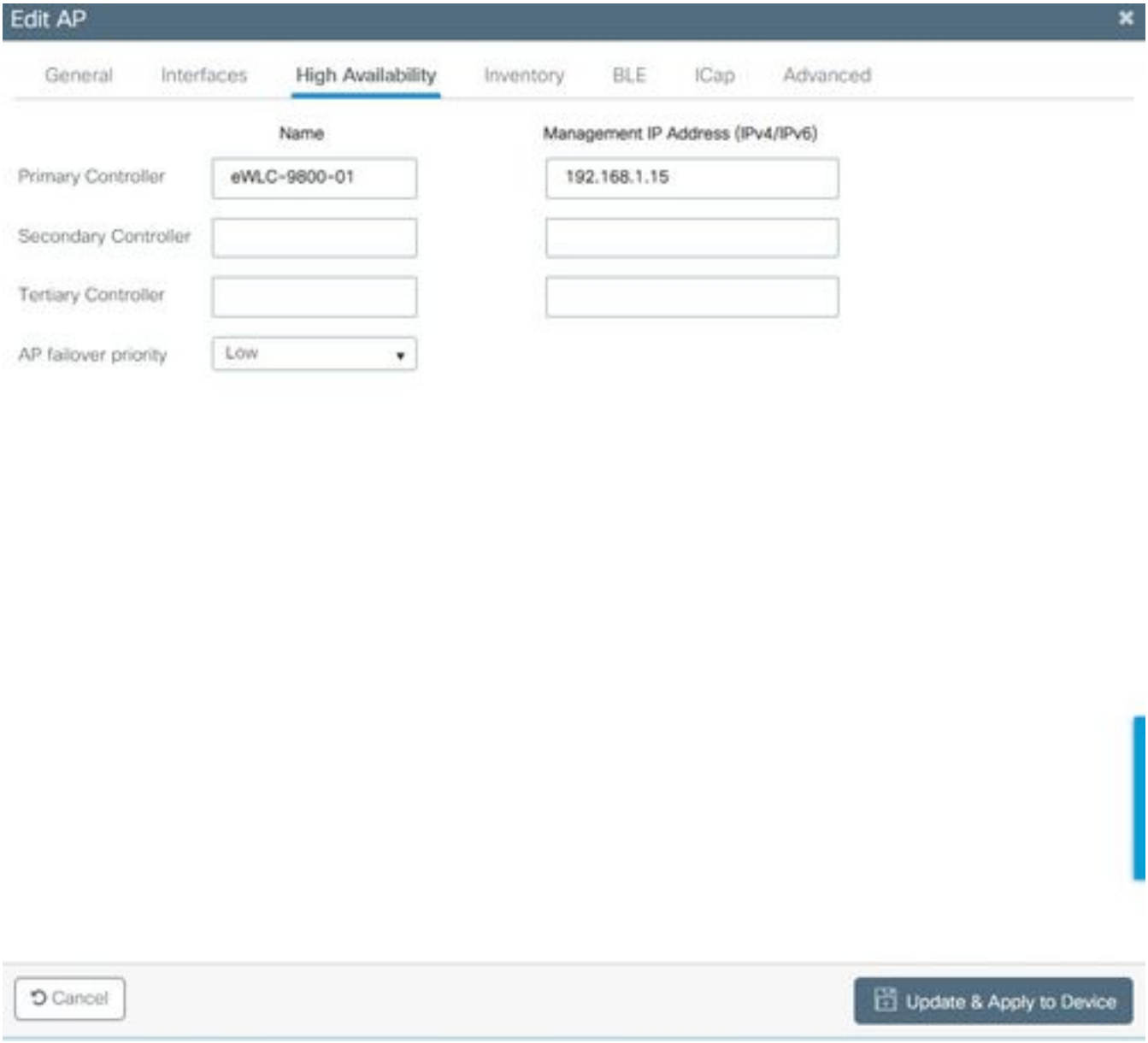


액세스 포인트에 정책 태그 및 사이트 태그 추가

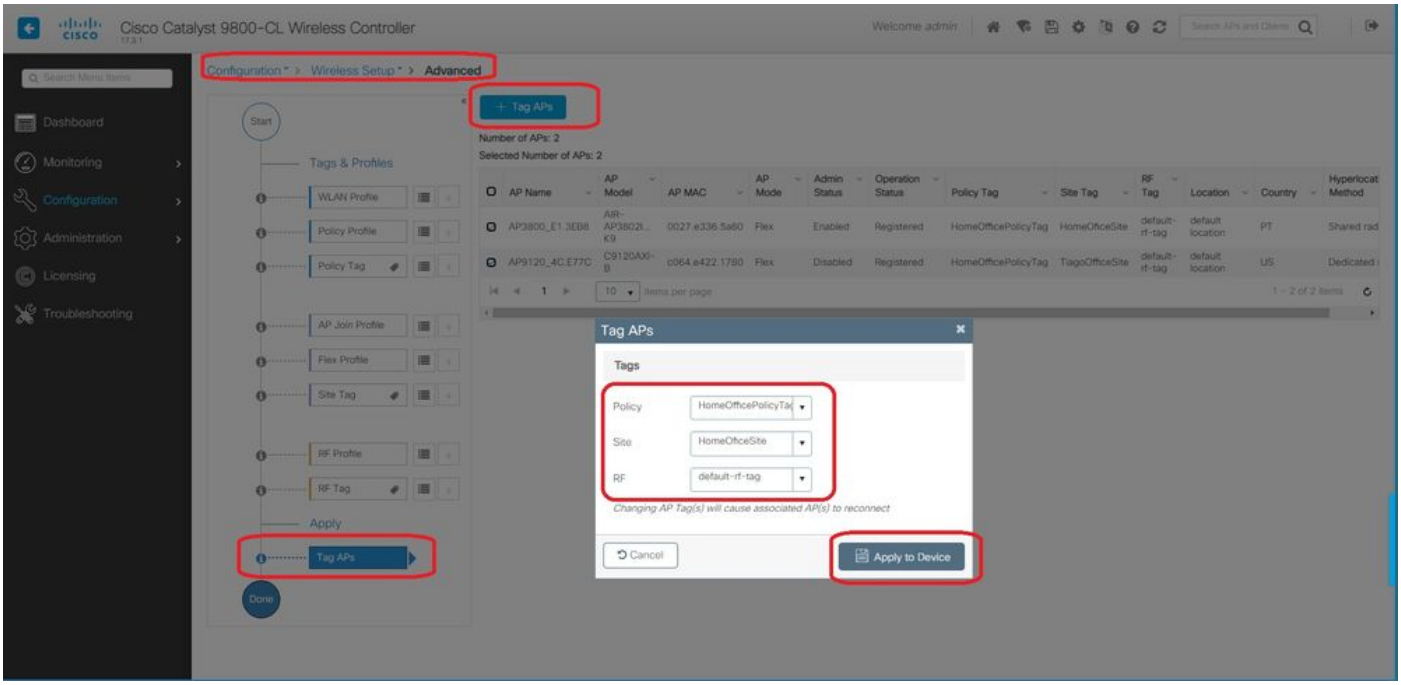
옵션 1. 이 옵션을 사용하려면 한 번에 1개의 AP를 구성해야 합니다. Configuration(구성) > Wireless(무선) > Access Points(액세스 포인트)로 이동합니다. 홈 오피스로 이동할 AP를 선택한 다음 홈 오피스 태그를 선택합니다. 업데이트 및 장치에 적용 선택:



또한 AP가 WLC가 홈 오피스에 구축되면 WLC의 IP/이름을 알 수 있도록 기본 컨트롤러를 구성하는 것이 좋습니다. AP를 High Availability(고가용성) 탭으로 직접 편집할 수 있습니다.



옵션 2. 이 옵션을 사용하면 여러 AP를 동시에 구성할 수 있습니다. Configuration(구성) > Wireless Setup(무선 설정) > Advanced(고급) > Tag APs(태그 AP)로 이동합니다. 이전에 생성한 태그를 선택하고 Apply to Device를 선택합니다.



AP가 재부팅되고 새 설정으로 WLC에 다시 연결됩니다.

다음을 확인합니다.

GUI 또는 CLI를 통해 컨피그레이션을 확인할 수 있습니다. 이것이 CLI에서 생성되는 컨피그레이션입니다.

```
!
ip access-list extended HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255 log
2 permit ip any any log
!
wireless profile flex HomeOffice_FlexProfile
acl-policy HomeOffice_ACL
office-extend
!
wireless profile policy HomeOfficePolicy
no central association
aaa-override
flex split-mac-acl HomeOffice_ACL
flex vlan-central-switching
ipv4 dhcp required
vlan default
no shutdown
!
wireless tag site HomeOficeSite
flex-profile HomeOffice_FlexProfile
no local-site
!
wireless tag policy HomeOfficePolicyTag
wlan HomeOffice policy HomeOfficePolicy
!
wlan HomeOffice 5 HomeOffice
security wpa psk set-key ascii 0 xxxxxxx
no security wpa akm dot1x
security wpa akm psk
no shutdown
!
```

```
ap 70db.98e1.3eb8
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
ap c4f7.d54c.e77c
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
```

AP 컨피그레이션을 확인하는 중:

```
eWLC-9800-01#show ap name AP3800_E1.3EB8 config general

Cisco AP Name : AP3800_E1.3EB8
=====================================================

Cisco AP Identifier : 0027.e336.5a60
...
MAC Address : 70db.98e1.3eb8
IP Address Configuration : DHCP
IP Address : 192.168.1.99
IP Netmask : 255.255.255.0
Gateway IP Address : 192.168.1.254
...
SSH State : Enabled
Cisco AP Location : default location
Site Tag Name : HomeOficeSite
RF Tag Name : default-rf-tag
Policy Tag Name : HomeOfficePolicyTag
AP join Profile : HomeOfficeAP
Flex Profile : HomeOffice_FlexProfile
Primary Cisco Controller Name : eWLC-9800-01
Primary Cisco Controller IP Address : 192.168.1.15
...
AP Mode : FlexConnect
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : IPv4
CAPWAP UDP-Lite : Not Configured
AP Submode : Not Configured
Office Extend Mode : Enabled
...
```

AP에 직접 연결하고 컨피그레이션을 확인할 수도 있습니다.

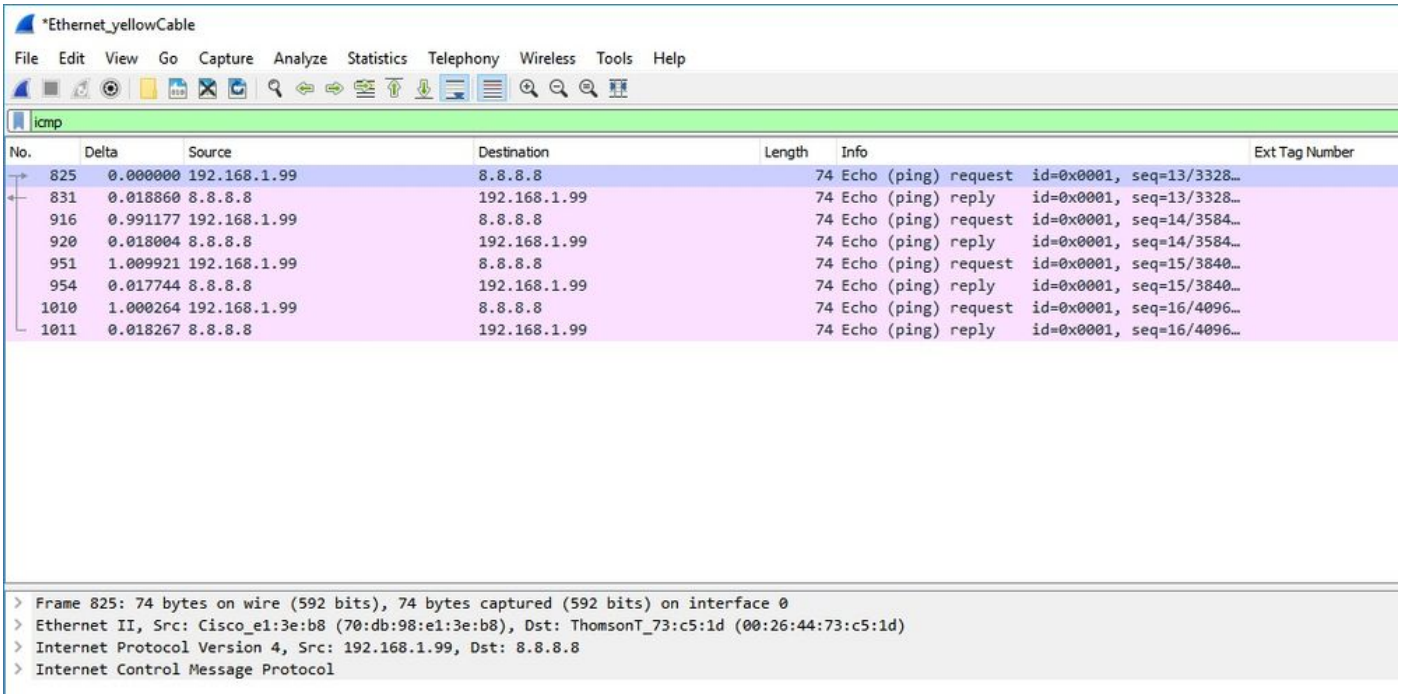
```
AP3800_E1.3EB8#show ip access-lists
Extended IP access list HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255
2 permit ip any any

AP3800_E1.3EB8#show capwap client detailrcb
SLOT 0 Config

SSID : HomeOffice
Vlan Id : 0
Status : Enabled
...
otherFlags : DHCP_REQUIRED VLAN_CENTRAL_SW
...
Profile Name : HomeOffice
...
```

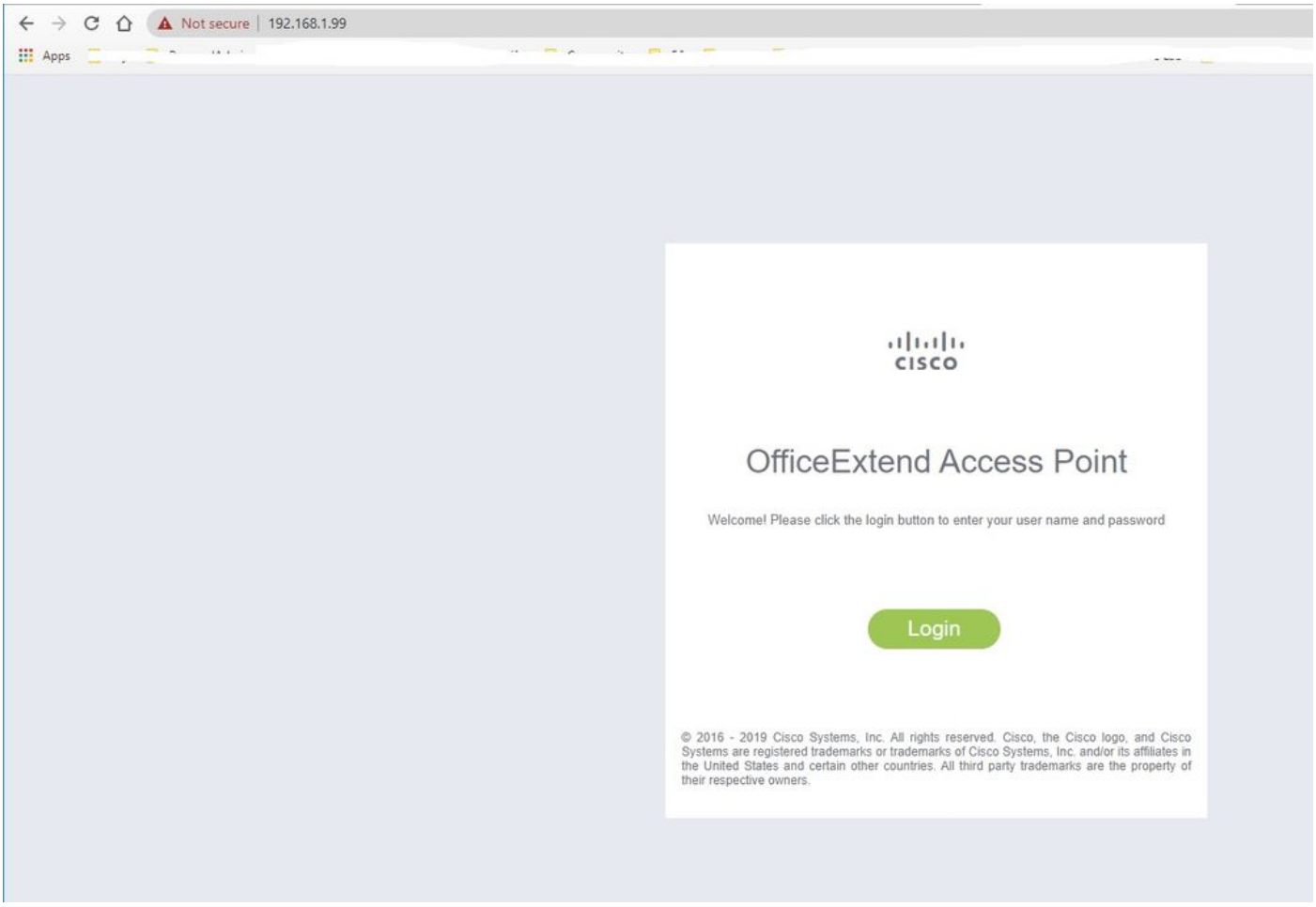
```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name :
ssh status : Enabled
ApMode : FlexConnect
ApSubMode : Not Configured
Link-Encryption : Enabled
OfficeExtend AP : Enabled
Discovery Timer : 10
Heartbeat Timer : 30
...
```

다음은 로컬로 스위칭되는 트래픽을 표시하는 패킷 캡처의 예입니다. 여기서 테스트는 IP 192.168.1.98의 클라이언트에서 Google DNS 서버로, 192.168.1.254으로 "ping"하는 것이었습니다. 트래픽을 로컬에서 AP NAT로 보내는 AP IP 주소 192.168.1.99의 IP를 사용하여 제공된 ICMP를 확인할 수 있습니다. 트래픽이 DTLS 터널에서 암호화되고 애플리케이션 데이터 프레임만 표시되므로 192.168.1.254에 대한 ICMP가 없습니다.

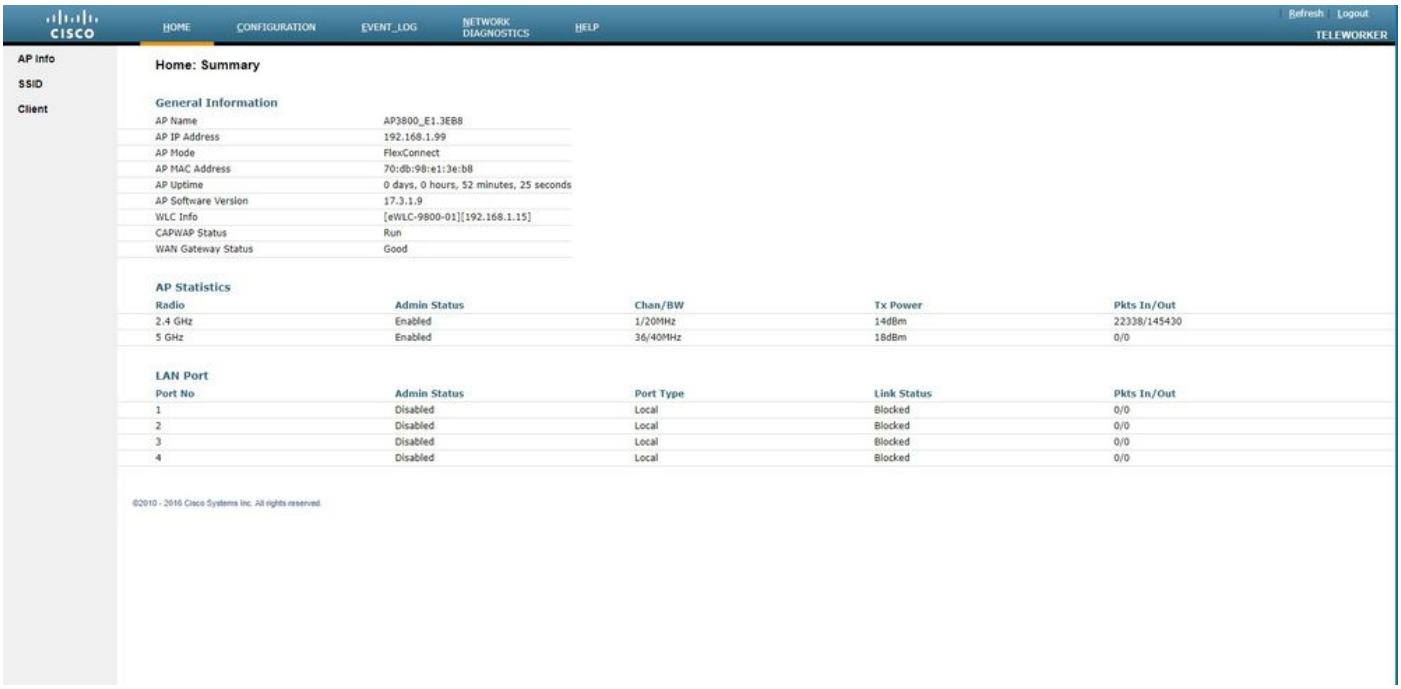


> **참고:** 정상적인 시나리오에서 클라이언트 서브넷은 Office 네트워크에 속하고 홈 오피스의 로컬 장치는 클라이언트 서브넷에 연결하는 방법을 모르기 때문에 로컬에서 스위칭되는 트래픽은 AP에 의해 NAT로 전송됩니다. AP는 로컬 홈 오피스 서브넷에 있는 AP IP 주소를 사용하여 클라이언트 트래픽을 변환합니다.

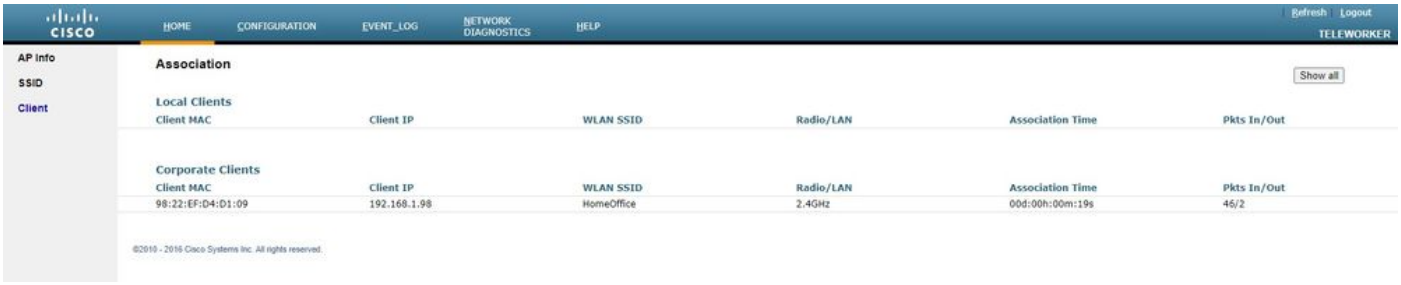
브라우저를 열고 AP IP 주소의 URL을 입력하는 OEAP GUI에 액세스할 수 있습니다. 기본 자격 증명은 admin/admin이며 초기 로그인 시 변경해야 합니다.



로그인하면 GUI에 액세스할 수 있습니다.



AP 정보, SSID 및 연결된 클라이언트와 같은 OEAP의 일반 정보에 액세스할 수 있습니다.



관련 문서

Catalyst 9800 Wireless Controller의 FlexConnect 이해

FlexConnect용 스플릿 터널링

Catalyst 9800 WLC에서 OEAP 및 RLAN 구성