FlexConnect 모드에서 로컬 인증 구성

목차

소개
- 배경 정보
  - FlexConnect 개요 및 요구 사항
  - 작동 모드
  - 빠른 보안 로밍
  - FlexConnect High Scale 모드
  - Wi-Fi 7 FlexConnect 지원
  - FlexConnect 복원력 시나리오

사전 요구 사항
- 요구 사항
- 사용되는 구성 요소

구성
- 네트워크 다이어그램
- AAA 서버 구성
- 원격 사이트에서 FlexConnect 모드 구성
- 외부 RADIUS 서버를 사용하여 로컬 인증으로 802.1x WLAN 구성
- ISE 구성
- 로컬 인증으로 PSK WLAN 구성

다음을 확인합니다.

문제 해결
- 독립형 시나리오

관련 정보

소개

이 문서에서는 FlexConnect 로컬 인증 작동 방식과 Cisco Catalyst 9800 Series WLC(Wireless Controller)를 사용하여 이를 구성하는 방법에 대해 설명합니다

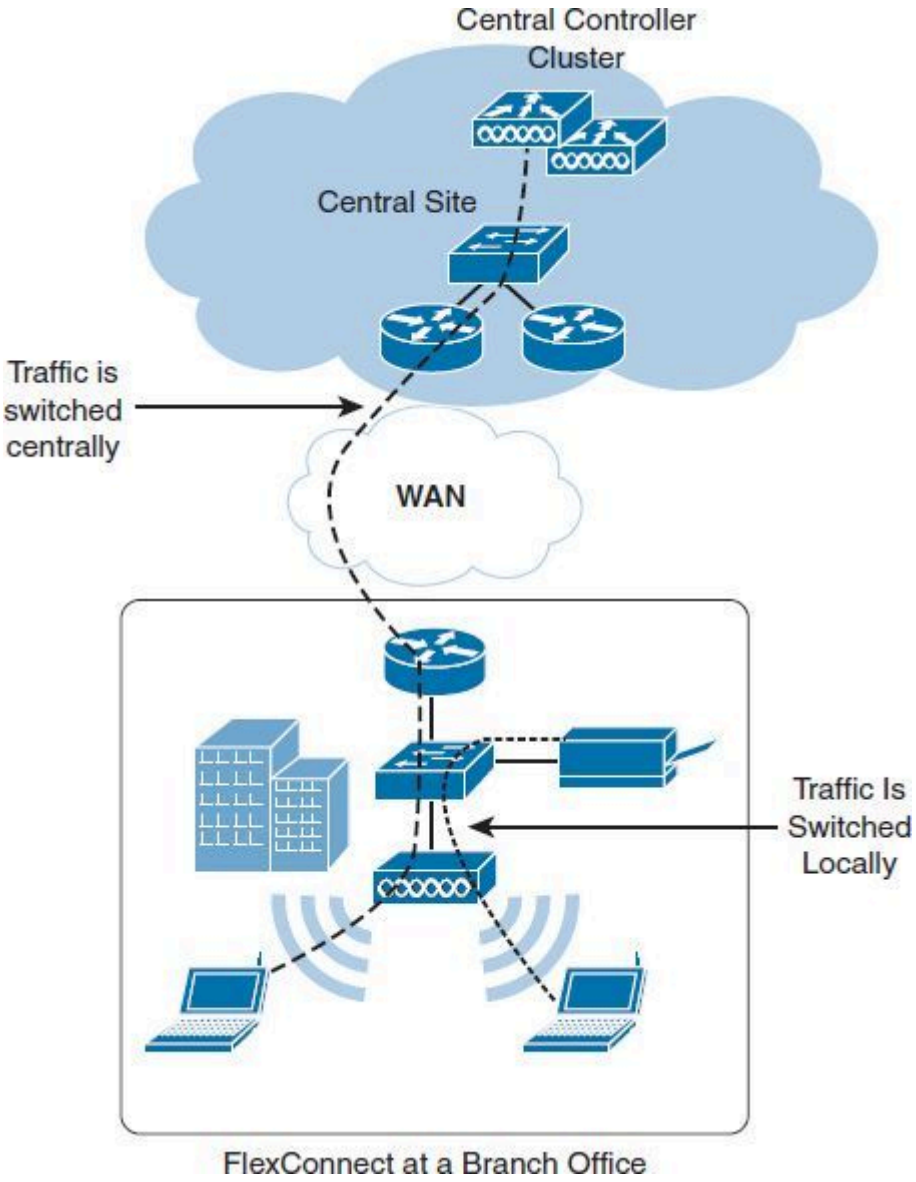
배경 정보

FlexConnect 개요 및 요구 사항

FlexConnect를 사용하면 원격 또는 지사의 AP(Access Point)가 중앙 집중식 컨트롤러에 연결하는 동시에 무선 트래픽의 로컬 처리가 가능합니다. 모든 무선 트래픽이 CAPWAP(Control and Provisioning of Wireless Access Points)를 사용하여 컨트롤러로 터널링되는 기존의 중앙 집중식 무

선 구축과 달리, FlexConnect를 사용하면 트래픽을 로컬로 전환하고 지사 AP에서 직접 처리할 수 있습니다. 이러한 로컬 스위칭은 AP에 어느 정도의 자율성을 제공하여 보안, 로밍, QoS(Quality of Service)와 같은 주요 서비스가 컨트롤러와 독립적으로 작동할 수 있도록 합니다.

FlexConnect는 기본적으로 로컬 트래픽 스위칭을 위해 설계되었지만, 필요할 때 특정 SSID(Service Set Identifier)를 중앙에서 스위칭할 수 있는 유연성도 제공합니다. 예를 들어, 특정 트래픽이 중앙 방화벽을 통과해야 하는 경우 중앙 스위칭을 위해 CAPWAP를 통해 SSID를 컨트롤러로 다시 전송할 수 있습니다. 이 이중 기능을 통해 단일 FlexConnect AP가 로컬과 중앙에서 스위칭하는 WLAN(Wireless Local Area Network)을 동시에 지원할 수 있습니다.



브랜치에 구축된 FlexConnect AP는 로컬로 한 SSID를 스위칭하는 반면 다른 SSID는 중앙에서 스위칭됩니다

작동 모드

FlexConnect AP는 두 가지 모드로 작동합니다. 연결 모드와 독립형 모드.

- 연결 모드에서 AP는 CAPWAP 제어 채널을 통해 컨트롤러에 대한 활성 연결을 유지합니다.
- 독립형 모드는 AP가 컨트롤러에 대한 연결을 끊을 때 발생하는 폴백 상태입니다.

정상 상태에서 FlexConnect AP는 연결 모드에서 작동합니다. 이 모드에서는 컨트롤러가 중앙 집중식 인증, 클라이언트 프로파일링, RRM(Radio Resource Management)과 같은 중요한 서비스를 관리합니다. AP는 대부분의 경우 이 모드를 유지할 것으로 예상되지만, 컨트롤러와의 통신이 끊길 경우 독립형 모드로 자동 전환됩니다. 독립형 모드에서는 AP가 계속 작동하면서 로컬로 트래픽을 전환하고 클라이언트가 연결된 상태를 유지할 수 있습니다. AP는 중앙 컨트롤러에 인증 요청을 전달하지 않고 클라이언트를 독립적으로 인증합니다. 그러나 RRM 및 중앙 집중식 클라이언트 인증과 같은 특정 컨트롤러 종속 서비스는 일시적으로 사용할 수 없게 됩니다.

예를 들어, WAN(Wide Area Network) 중단으로 인해 AP와 컨트롤러 간의 연결이 중단되지만 인터넷 액세스는 활성 상태로 유지되는 경우, AP는 독립형 모드로 전환되고 중단 없이 로컬로 전환된 트래픽을 계속 처리합니다. 기존 클라이언트는 계속 연결되어 있지만 로컬 인증이 구성되어 있지 않으면 중앙 인증이 필요한 새 클라이언트가 네트워크에 참여할 수 없습니다. FlexConnect AP는 WAN 장애 시 로컬 인증을 수행하도록 설정할 수 있으므로 컨트롤러에 연결할 수 없는 경우에도 서비스를 계속 유지할 수 있습니다.

독립형 모드에서는 AP에서 다음 기능을 사용할 수 없습니다.

- 클라이언트 웹 인증
- 게스트 인증(포털 리디렉션)
- 모든 중앙 스위칭 SSID
- RRM
- IPv6 레이어-3 모빌리티
- 네이티브 프로파일링
- 정책 분류
- 서비스 검색 게이트웨이
- 컨피그레이션 업데이트

독립형 모드(로컬 인증)에서 지원되는 기능 및 WLAN 컨피그레이션의 전체 목록은 기능 매트릭스를 참조하십시오. Cisco Wireless Access Points의 기능 매트릭스

일반적인 FlexConnect 장애 시나리오에서는 WAN이 완전히 손실되거나 크게 저하되어 CAPWAP 제어 채널이 중단됩니다. AP가 WAN 문제로 인해 컨트롤러에 대한 연결이 끊기면 즉시 독립형 모드로 전환됩니다.

WAN 장애 시 가장 중요한 목적은 컨트롤러와의 통신을 최대한 신속하게 복원하여 전체 기능을 재개하는 것입니다.

WAN 장애로 인해 FlexConnect AP가 독립형 모드로 진입하면 활성 클라이언트는 연결된 상태를 유지하며 FlexConnect 도메인/사이트 태그 내의 AP 간에 원활하게 로밍할 수 있지만, 서로 다른 FlexConnect 사이트 태그 간의 로밍에는 완전한 재인증이 필요할 수 있습니다. 그러나 중앙 위치의 AAA 서버(Authentication, Authorization, Accounting Server)에 연결할 수 없기 때문에 로컬로 스위칭된 WLAN에 조인하려는 새 클라이언트를 인증할 수 없습니다.

빠른 보안 로밍

EAP(Extensible Authentication Protocol) 인증은 AAA 서버와의 EAP 프레임 교환으로 인해 PSK(Pre-Shared Key) 인증에 비해 레이턴시가 향상됩니다. 그러나 빠른 보안 로밍을 사용하는 경우 클라이언트는 네트워크와의 초기 연결 동안에만 완전한 802.1X/EAP 인증을 거칩니다. 후속 로밍에서 인접 AP로 이동하면 EAP 교환이 우회되어 4방향 핸드셰이크만 남게 됩니다. 이는 AAA 서버와 관련이 없기 때문에 훨씬 빠릅니다. 이 표에서는 로컬 모드 및 FlexConnect 구축 모두에서 9800 WLC가 지원하는 다양한 고속 보안 로밍 방법을 간략하게 설명합니다.

기능	로컬 모드	FlexConnect(연결 모드, 중앙 인증)	FlexConnect(연결 모드 - 로컬 인증)	FlexConnect(독립형)
고정 키 캐싱(SKC)	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음
OKC(Opportunistic Key Caching)	지원	지원	지원	지원(클라이언트 세션이 만료될 때까지)
Cisco CCKM(Centralized Key Management)	지원	지원	지원	지원되지 않음
FT-802.11r/ Adaptive 11r(빠른 전환)(무선)	지원	지원	지원	지원(클라이언트 세션이 만료될 때까지)
FT-802.11r/ Adaptive 11r(빠른 전환)(DS를 통해)	지원	지원	지원되지 않음	지원되지 않음

독립형 모드에서 빠른 로밍은 캐시된 키 자료가 유효한지 여부에 따라 달라집니다. 캐시된 PMK(Pairwise Master Key)/세션이 만료되면, 컨트롤러 연결이 복원될 때까지 AP는 새 컨트롤러에서 파생된 키 정보를 얻을 수 없습니다.

FlexConnect High Scale 모드

Cisco IOS XE 17.8.1 이상에서는 300개의 AP 및 3000개의 802.1x 클라이언트를 수용할 수 있도록 Flex Site 사이트 용량이 확장되었습니다.

PMK 전파를 사용하면 동일한 FlexConnect 사이트 내의 AP가 PMK 정보를 공유할 수 있으므로 로밍 중에 완전한 EAP 교환이 필요하지 않습니다. PMK 전파는 기본적으로 활성화되어 있지 않습니다.

PMK 전파를 확인하고 PMK를 활성화하려면 다음 명령을 사용합니다.

- 무선 통계 표시 pmk-전파
- pmk 전파

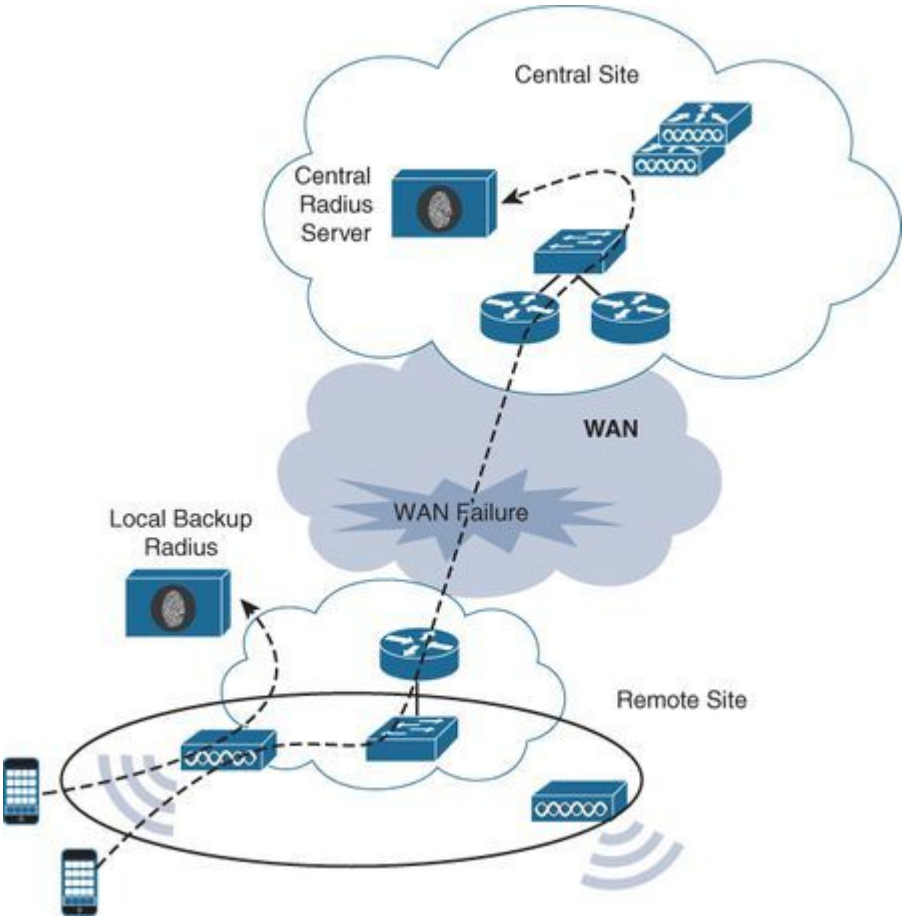
Wi-Fi 7 FlexConnect 지원

이 표에는 CW917x Wi-Fi 7 AP 제품군에서 지원되는 FlexConnect 기능이 요약되어 있습니다.

기능	지원
로컬 스위칭	지원
중앙 스위칭	지원
WLAN-VLAN 매핑	지원
외부 RADIUS를 통한 로컬 인증	지원
WPA3-엔터프라이즈	지원
FT-802.11r 빠른 로밍	지원
MLO(Multi Link Operation)	지원
내부 RADIUS를 통한 로컬 인증	지원되지 않음
WPA3-엔터프라이즈-192	지원되지 않음

FlexConnect 복원력 시나리오

1. N+1 복원력 설정에서 여러 활성 컨트롤러는 활성 컨트롤러에 장애가 발생할 경우 이를 인계하는 공통 백업 컨트롤러를 공유합니다. 기본 컨트롤러가 오프라인 상태가 되면 FlexConnect AP가 즉시 독립형 모드로 전환하고 백업 컨트롤러 검색을 시작합니다. 이 연결 해제 기간 동안 중앙에서 스위칭된 클라이언트는 AP에서 연결이 끊어집니다. AP가 찾아서 백업 컨트롤러와 동기화하면 중앙에서 전환된 SSID에 액세스해야 하는 클라이언트가 다시 연결됩니다. 한편, 로컬로 전환된 클라이언트는 영향을 받지 않으며 서비스 중단을 인식하지 못한 채 계속 작동합니다.
2. FlexConnect 그룹에서 액세스할 수 있는 원격 위치에 백업 AAA 서버를 제공합니다. 로컬 인증이 활성화된 경우, 이 백업 RADIUS 서버는 AP가 독립형 모드로 들어갈 때만 사용됩니다. AP가 연결 모드에 있는 동안에는 비활성 상태로 유지됩니다. FlexConnect AP가 인증에 로컬 백업 AAA 서버를 사용할 경우 중앙 집중식 AAA 서버와 마찬가지로 인증 키가 FlexConnect 그룹의 모든 AP에 분산됩니다. 따라서 백업 RADIUS 서버가 사용 중인 경우에도 새 클라이언트가 재인증 없이 AP 간에 원활하게 로밍할 수 있습니다.
3. 로컬 인증을 허용하는 Cisco Wireless Access Points용 Feature Matrix에 있는 모든 방법.



WAN 장애로 인해 중앙 AAA 서버를 사용할 수 없게 될 때 클라이언트가 로컬 백업 AAA 서버에 대해 인증합니다

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

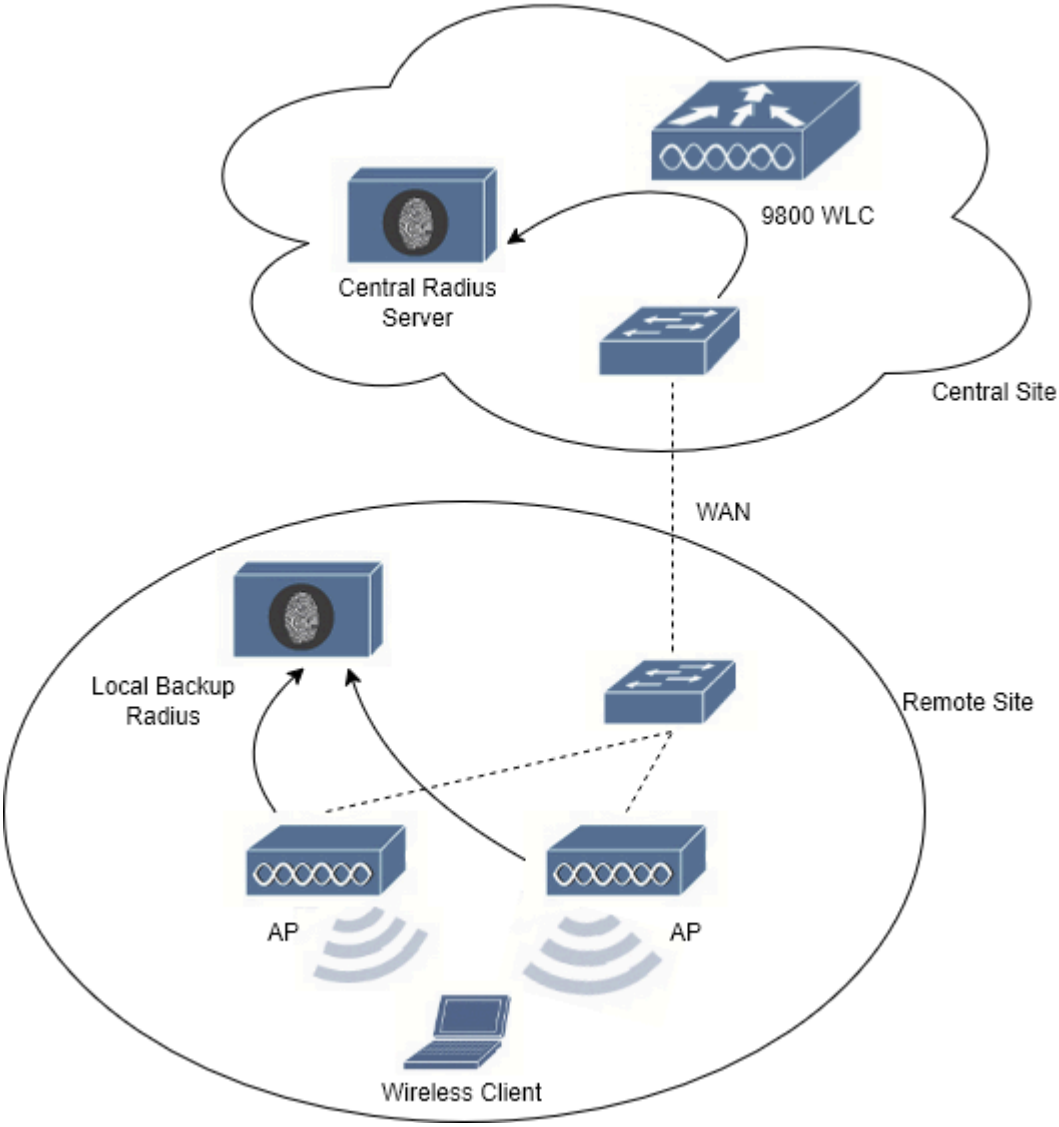
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst C9800-CL Wireless Controller for Cloud with Cisco IOS® XE Dublin 17.18.3
- Catalyst CW9164I-ROW Access Point v17.18.3.18
- Aironet® AIR-AP2802I-E-K9 Access Point v17.18.3.18
- Identity Services Engine v3.2.0.542 2개

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.

구성

네트워크 다이어그램



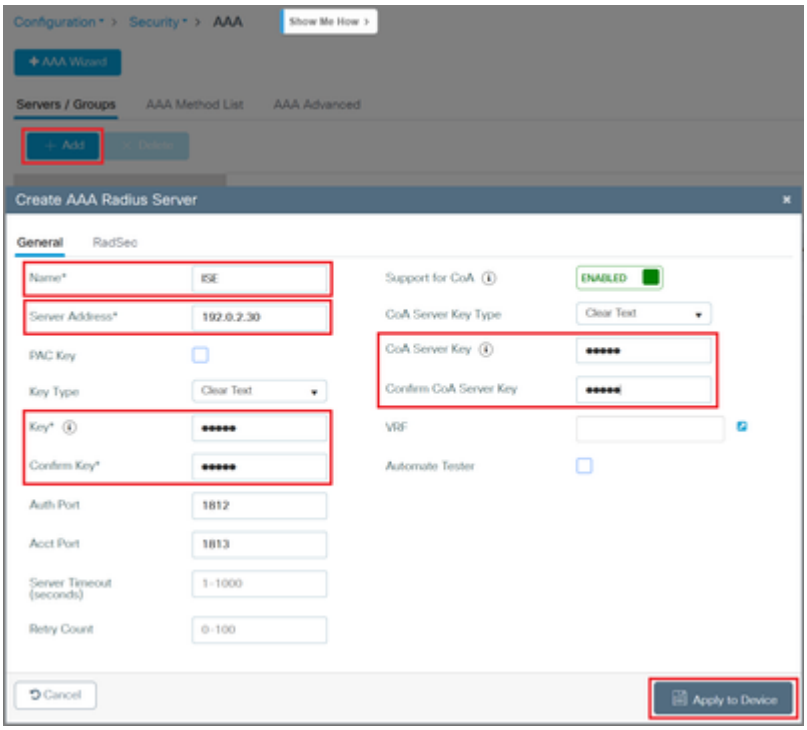
네트워크 다이어그램

AAA 서버 구성

1단계. 802.1x WLAN을 구성하려면 9800 WLC에서 AAA 서버 그룹을 생성해야 합니다.

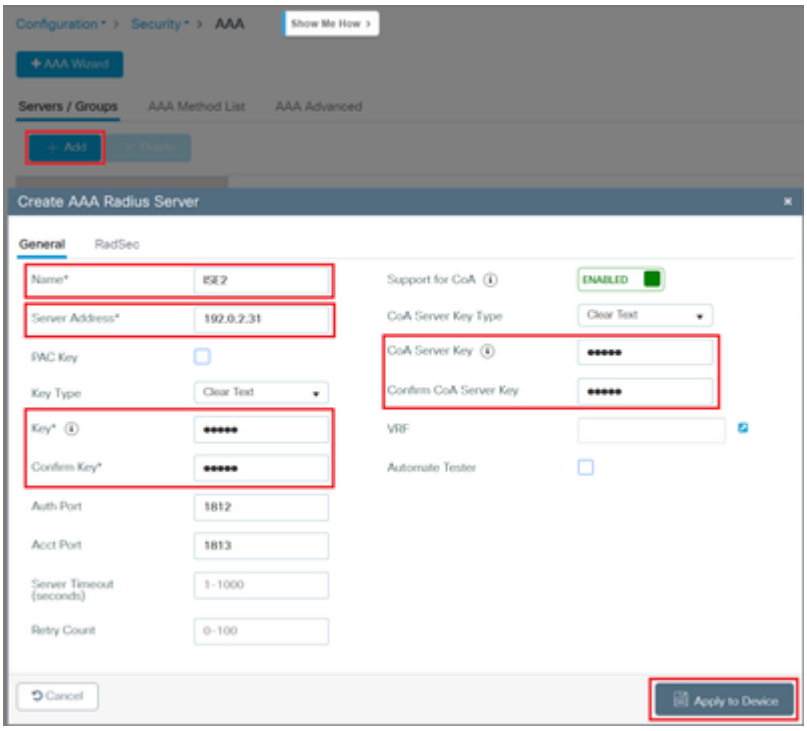
각 사이트에 대해 중앙 사이트와 원격 사이트에 각각 하나씩 AAA 서버를 생성합니다.

Configuration(컨피그레이션) > Security(보안) > AAA > Server/Groups(서버/그룹) > Servers(서버)로 이동하고 +Add(추가)를 선택합니다. 서버의 이름, IP 주소, 키(및 확인 키), CoA(Change of Authorization) 지원을 활성화하고 CoA 서버 키(및 CoA 서버 키 확인)를 입력합니다. 키는 반드시 같아야 합니다.



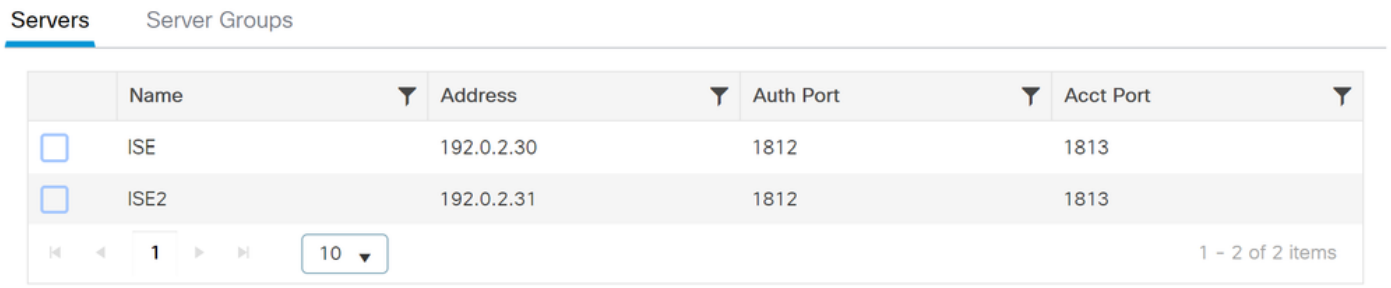
Apply to Device(디바이스에 적용)를 클릭합니다.

2단계. 다른 AAA 서버를 생성합니다.

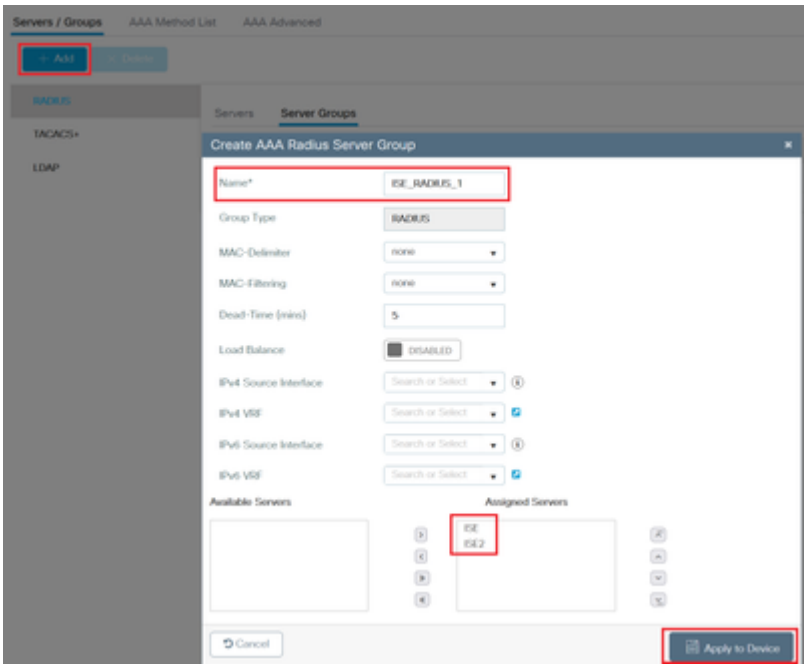


Apply to Device(디바이스에 적용)를 클릭합니다.

이제 AAA 서버가 구성된 것을 볼 수 있습니다.

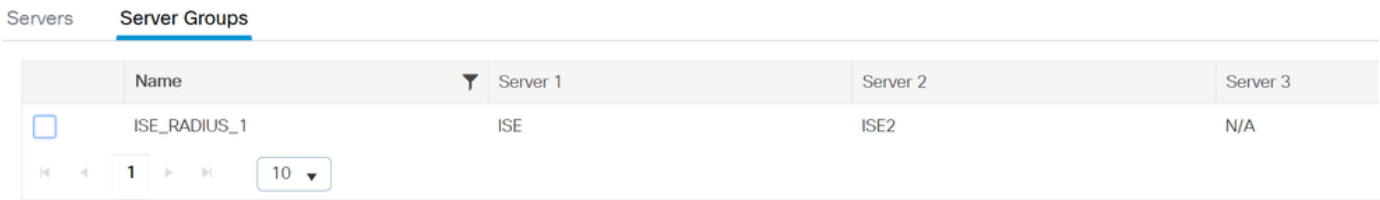


3단계. Configuration(구성) > Security(보안) > AAA > Server/Groups(서버/그룹) > Server Groups(서버 그룹)로 이동하고 +Add(추가)를 선택합니다. 그룹 서버에 이름을 지정하고, 이전에 생성한 AAA 서버를 Assigned Servers(할당된 서버) 열에 추가합니다.



Apply to Device(디바이스에 적용)를 클릭합니다.

그러면 구성된 AAA 서버 그룹이 표시됩니다.



CLI:

```
aaa new-model
```

```
!
radius server ISE
address ipv4 192.0.2.30 auth-port 1812 acct-port 1813
key keystring
!
radius server ISE2
address ipv4 192.0.2.31 auth-port 1812 acct-port 1813
key keystring
!
aaa server radius dynamic-author
client 192.0.2.30 server-key keystring
client 192.0.2.31 server-key keystring
!
aaa group server radius ISE_RADIUS_1
server name ISE
server name ISE2
deadtime 5
```

원격 사이트에서 FlexConnect 모드 구성

1단계. 첫 번째 단계는 원격 사이트에 FlexConnect를 구성하는 것입니다.

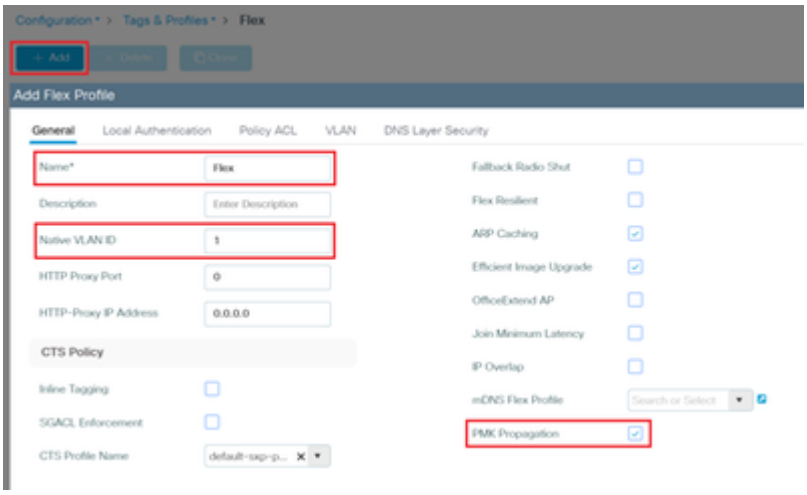
이 가이드를 사용하여 AP 모드를 Flex: FlexConnect on Catalyst 9800 Wireless Controller로 변경할 수 있습니다.

이 가이드/실습의 AP는 동일한 Flex 프로파일을 사용합니다.

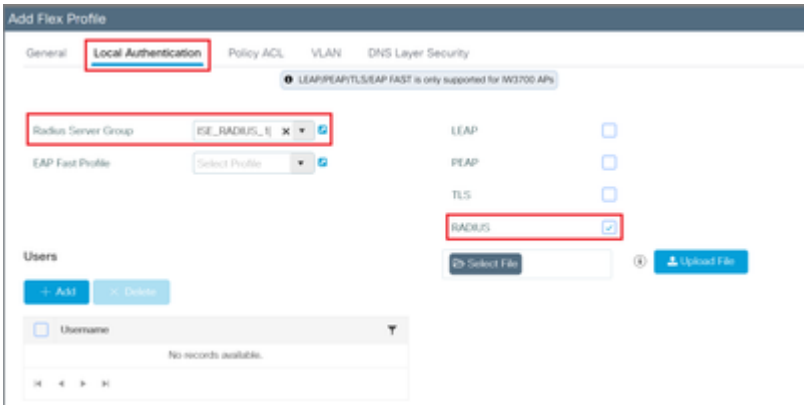
2단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Flex(플렉스)로 이동합니다.

+Add(추가)를 사용하여 새 Flex Profile Name(Flex 프로필 이름)을 생성합니다. General(일반) 탭에서 프로필에 이름을 지정하고 Native VLAN(Virtual Local Area Network) ID를 입력한 다음 PMK 전파를 활성화합니다.

PMK 전파를 활성화하여 단일 사이트 내의 AP 간에 PMK 정보를 공유함으로써 원활한 무선 클라이언트 로밍을 지원합니다.

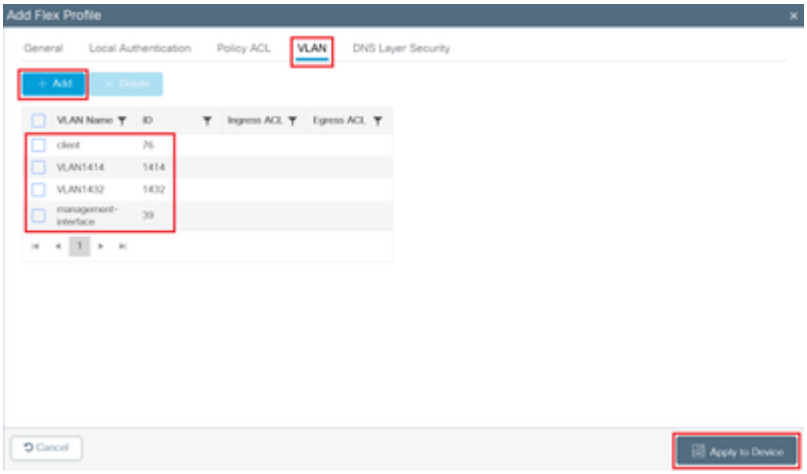


3단계. 802.1x WLAN의 경우 Local Authentication(로컬 인증) 탭에서 Radius Server Group(RADIUS 서버 그룹)을 선택하고 RADIUS를 활성화합니다.



팁: PSK WLAN의 경우 이 탭에 아무것도 추가할 필요가 없습니다.

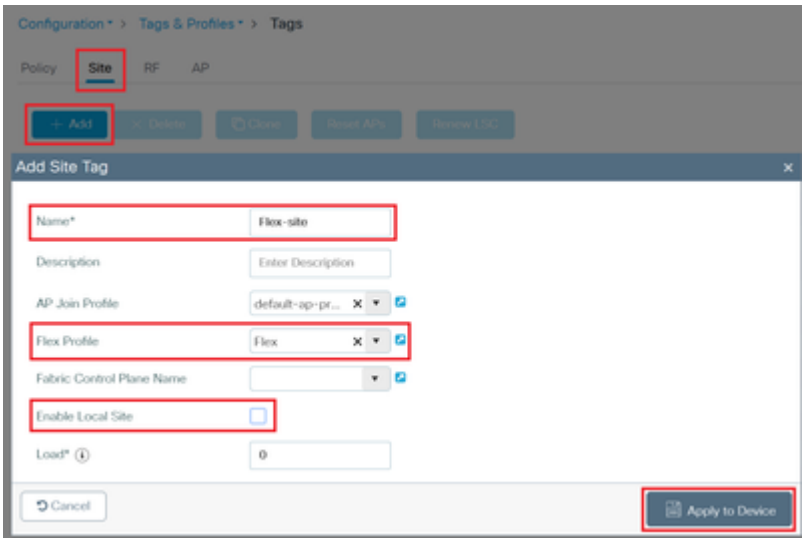
4단계. VLAN 탭에서 클라이언트, AP 및 RADIUS 서버에서 사용하는 모든 VLAN을 추가합니다. 각 VLAN 이름을 올바른 VLAN ID에 올바르게 대응시켜야 합니다.



마지막에 Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

5단계. Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Site(사이트)로 이동하고 +Add(추가)를 선택합니다.

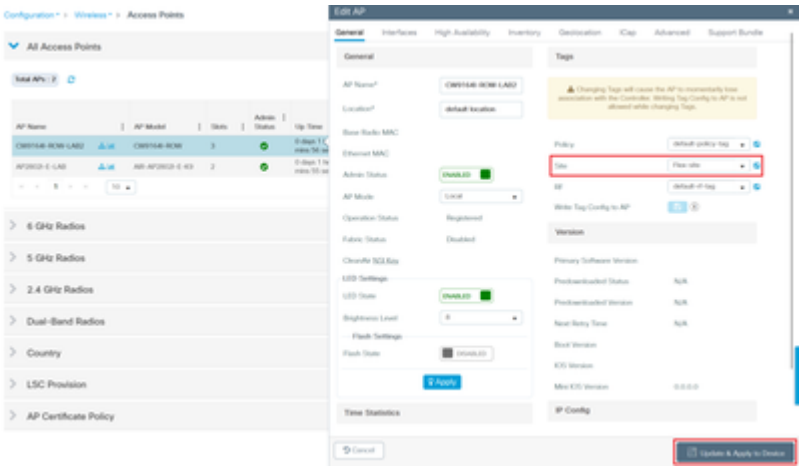
이전에 생성한 Flex Profile로 사이트 태그를 생성합니다. 이름을 지정하고 올바른 Flex Profile을 선택한 다음 Enable Local Site(로컬 사이트 활성화)를 비활성화합니다. AP 조인 프로파일이 올바른지 확인합니다.



Apply to Device(디바이스에 적용)를 클릭합니다.

6단계. Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동합니다.

AP를 선택하고 General(일반) > Tags(태그)에서 Site Tag(사이트 태그)를 이전에 구성한 태그로 변경합니다.



Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

AP가 WLC와의 연결을 끊고 Flex AP 모드로 다시 결합합니다.

동일한 페이지에서 AP가 다시 조인할 때 열 AP 모드에서 AP 모드를 확인할 수 있습니다.

AP를 선택하면 새 사이트 태그가 표시됩니다.



CLI:

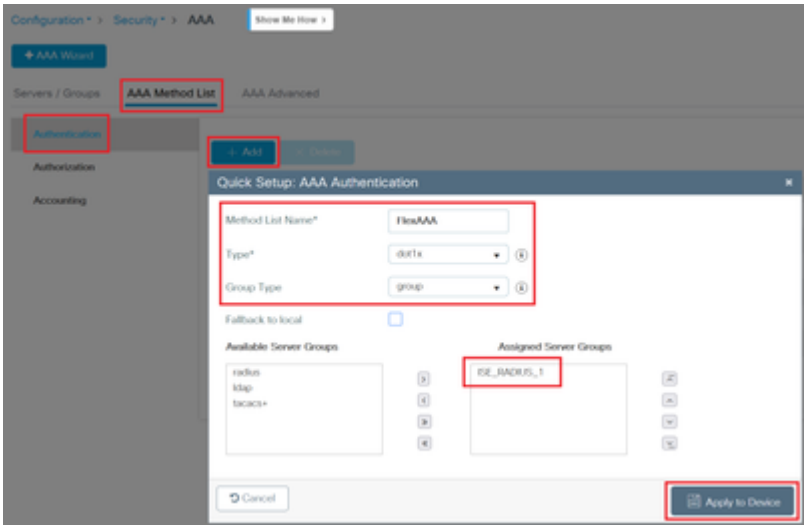
```
wireless profile flex Flex
ip http client proxy 0.0.0.0 0
local-auth radius-server-group ISE_RADIUS_1
vlan-name client
vlan-id 76
vlan-name VLAN1414
vlan-id 1414
vlan-name VLAN1432
vlan-id 1432
vlan-name management-interface
vlan-id 39
pmk propagate
!
wireless tag site Flex-site
ap-profile default-ap-profile
no local-site
flex-profile Flex
!
ap h.h.h (AP Radio MAC address)
policy-tag default-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

외부 RADIUS 서버를 사용하여 로컬 인증으로 802.1x WLAN 구성

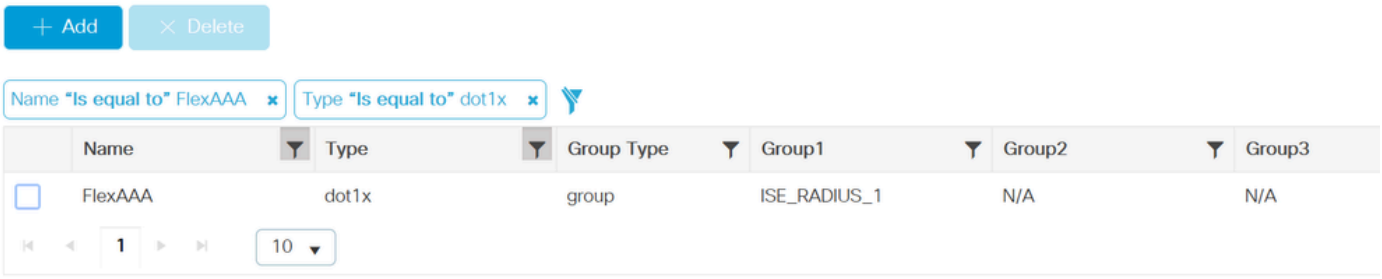
1단계. Authentication Method(인증 방법) 목록을 생성합니다.

AAA Method List(AAA 방법 목록) > Authentication(인증) 탭에서 Configuration(컨피그레이션) > Security(보안) > AAA로 이동합니다.

Assigned +Add(추가)를 선택하고 메소드 목록 이름에 이름을 지정한 후 유형으로 dot1x를 선택하고 그룹 유형으로 그룹을 선택한 후 Assigned Server Groups(할당된 서버 그룹) 열에서 AAA 서버 그룹을 할당합니다.



이제 생성된 AAA 메서드 목록이 표시됩니다.



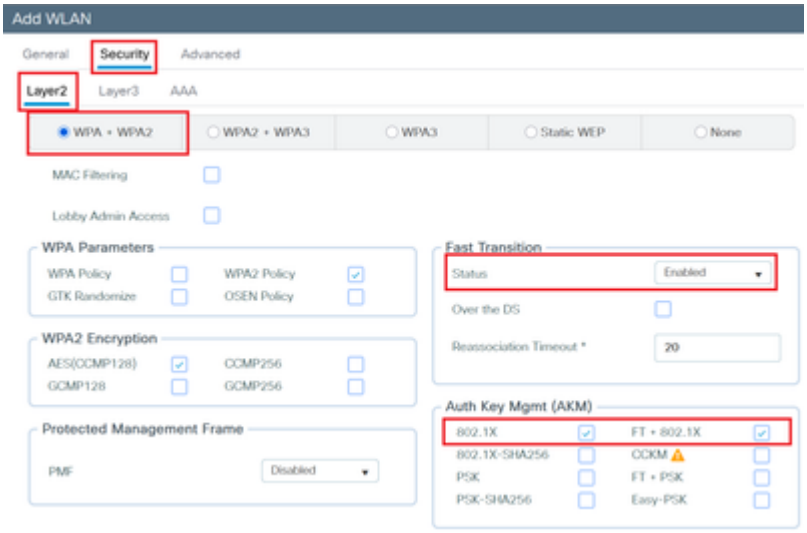
2단계. WLAN 생성.

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동하고 +Add(추가)를 선택합니다.

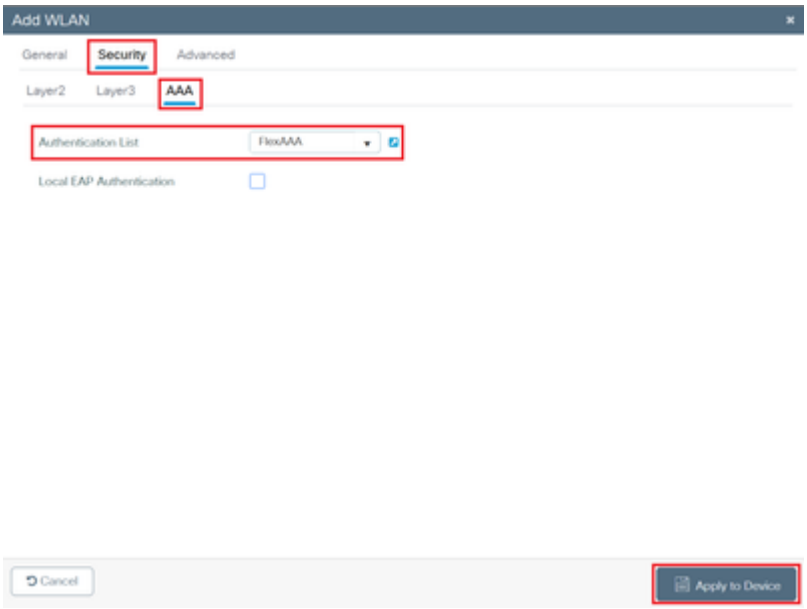
General 태그에서 Profile Name(프로파일 이름), SSID 및 enable Status(상태 활성화)에 대한 이름을 생성합니다.



3단계. Security(보안) > Layer 2(레이어 2) 탭으로 이동하여 WPA+WPA2(Wi-Fi Protected Access)를 선택하고 Fast Transition(빠른 전환)을 Enabled(활성화됨)로 선택한 후 인증 키 관리 802.1X 및 FT+802.1X를 선택합니다.



4단계. Security(보안) > AAA 탭으로 이동하고 Authentication List(인증 목록) 드롭다운 메뉴에서 이전에 생성한 목록을 선택합니다.



Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

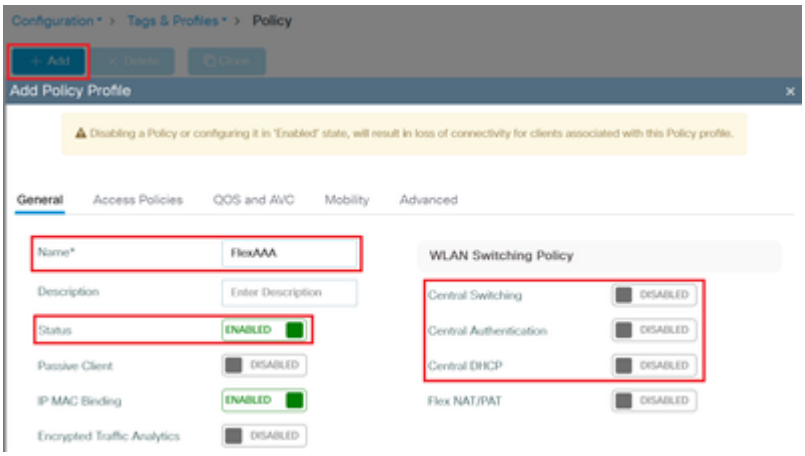
그런 다음 생성된 WLAN이 표시됩니다.



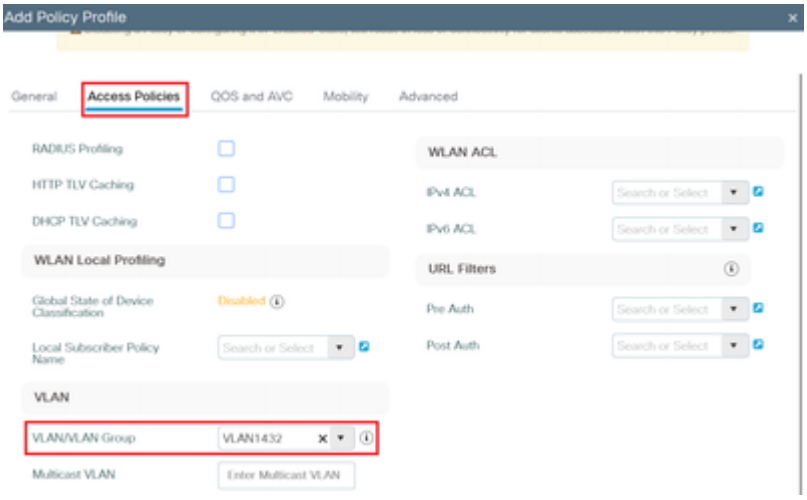
5단계. 정책 프로필을 생성합니다.

Configuration > Tags & Profiles > Policy로 이동합니다.

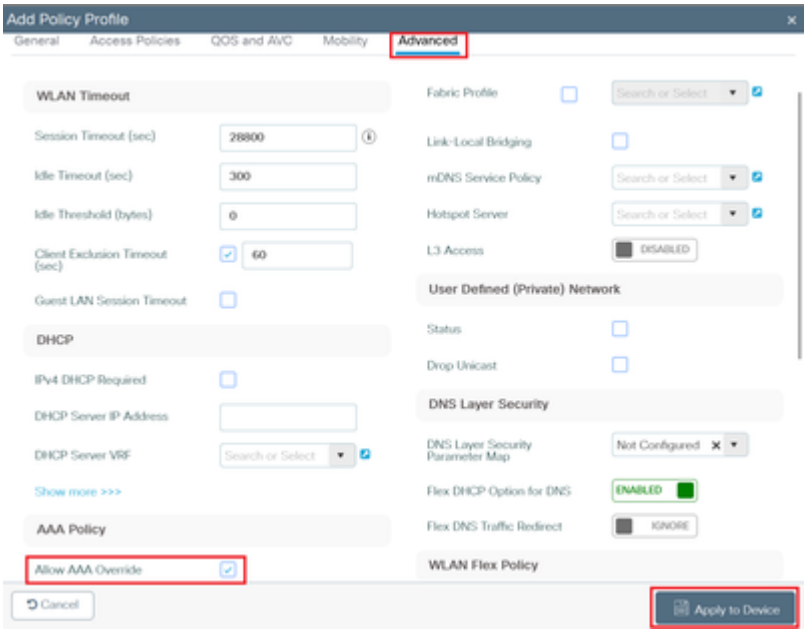
+Add를 선택하고 General 탭에서 정책 프로필의 이름을 지정하고, 상태를 활성화하고, 중앙 스위칭, 중앙 인증 및 중앙 DHCP(Dynamic Host Configuration Protocol)를 비활성화합니다.



6단계. Access Policies(액세스 정책) 탭으로 이동하고 VLAN을 선택합니다.

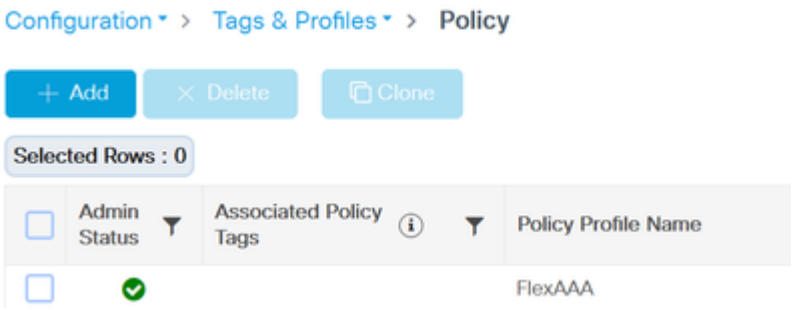


7단계. Advanced(고급) 탭으로 이동하여 Allow AAA Override(AAA 재정의 허용)를 활성화합니다.



Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

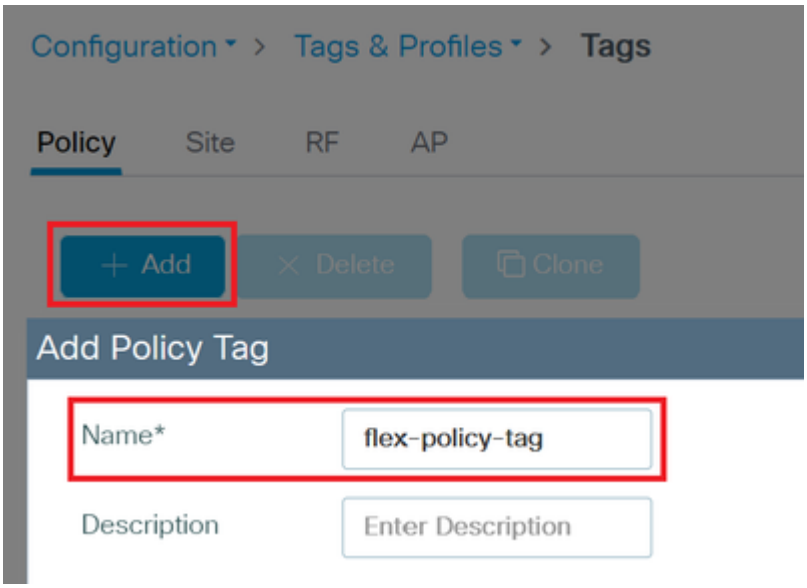
목록에서 정책 프로필을 볼 수 있습니다.



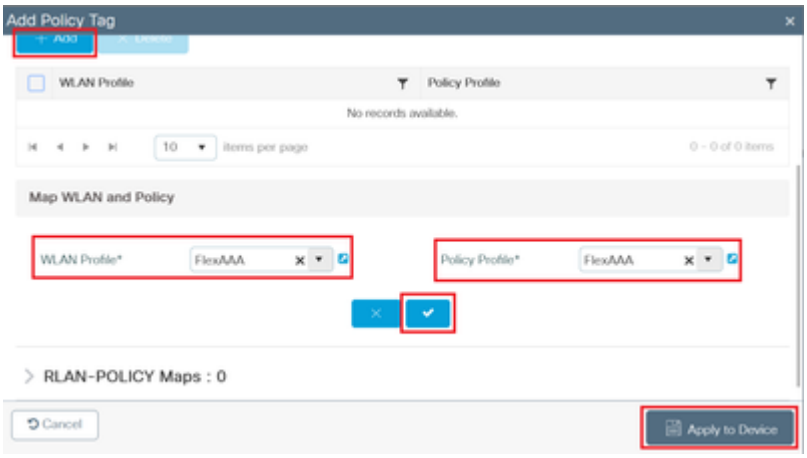
8단계. 정책 태그를 생성합니다.

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그)로 이동합니다.

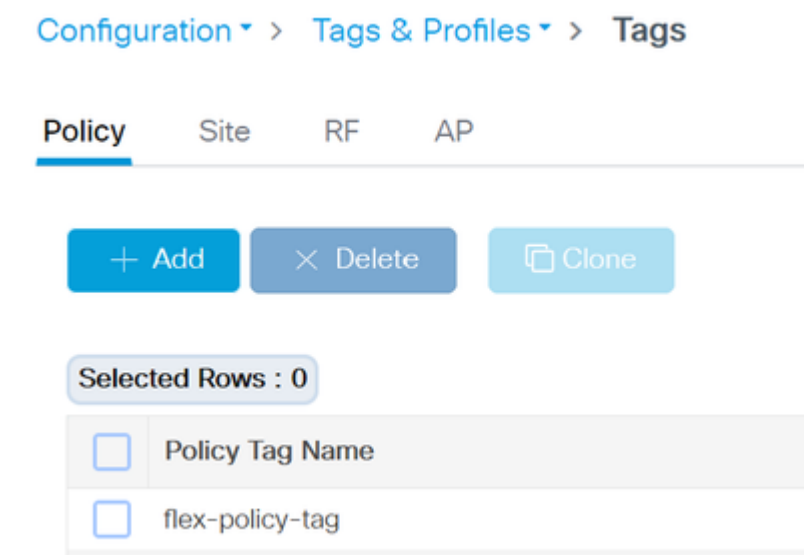
Policy(정책) 탭에서 +Add(추가)를 선택합니다. 정책 태그에 이름 지정:



아래로 스크롤하여 WLAN-POLICY Maps(WLAN-정책 맵) 아래에서 +Add(추가)를 선택합니다. WLAN Profile(WLAN 프로파일)의 드롭다운 메뉴에서 이전에 생성한 WLAN을 선택합니다. Policy Profile(정책 프로필)의 드롭다운 메뉴에서 이전에 생성한 정책 프로필을 선택합니다. 확인 버튼을 클릭한 다음 장치에 적용 을 클릭합니다.

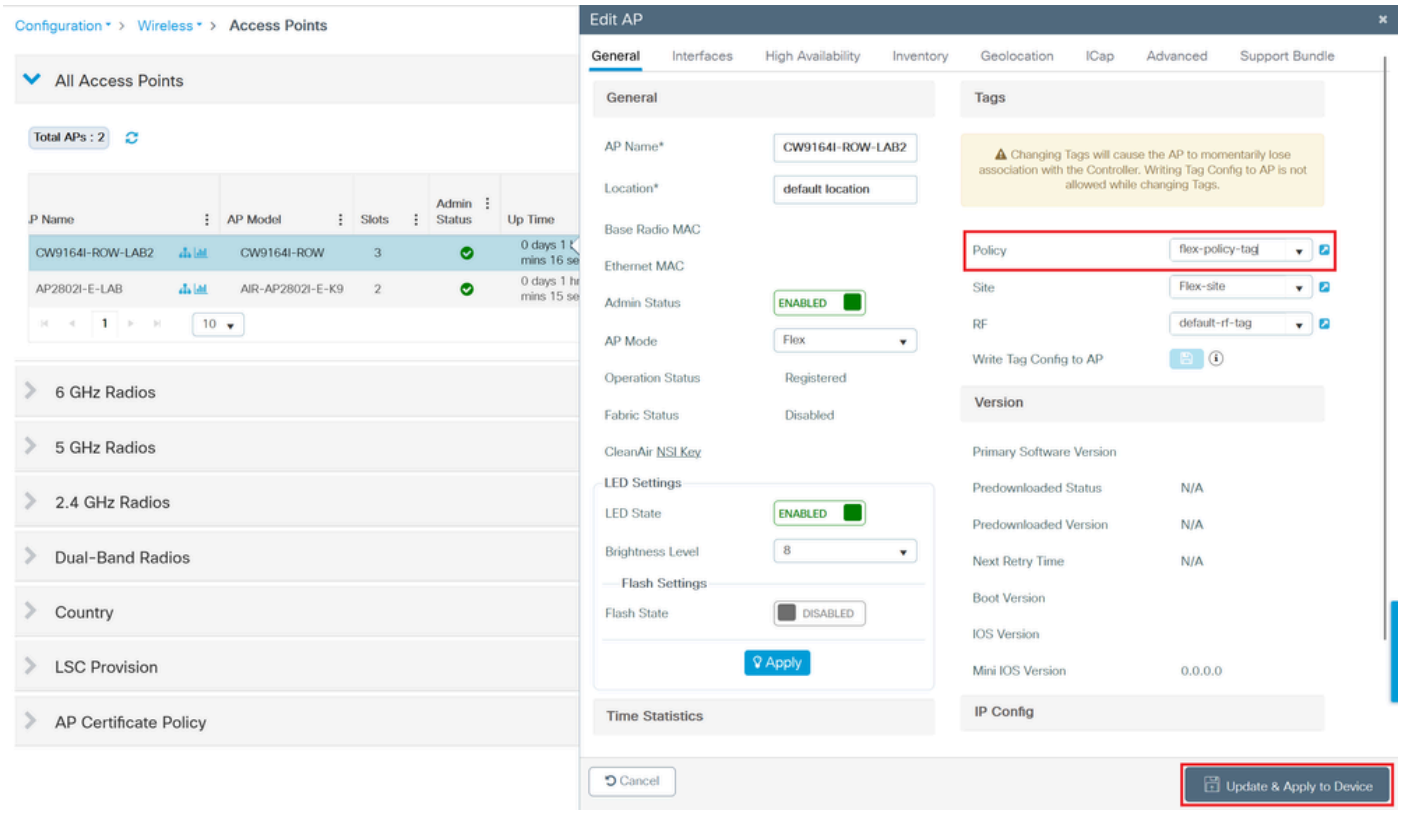


목록에서 정책 태그를 확인할 수 있습니다.



9단계. AP 태그에 정책 태그를 할당합니다.

Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동합니다. 태그를 변경할 AP를 선택합니다.



Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

AP가 연결을 끊고 새 정책 태그로 다시 결합합니다.

AP가 다시 연결되면 Access Points(액세스 포인트) 목록을 확인하고 AP가 Flex 모드인지 확인한 다음 할당된 태그를 확인할 수 있습니다.



CLI:

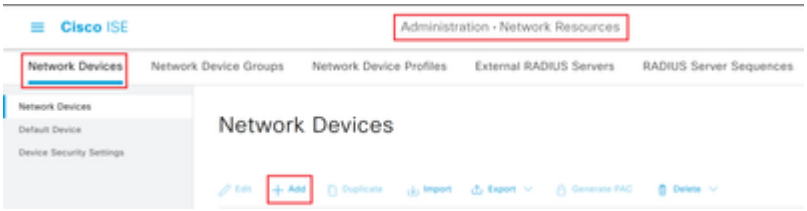
```
aaa authentication dot1x FlexAAA group ISE_RADIUS_1
!
wlan FlexAAA 4 FlexAAA
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa akm ft dot1x
security dot1x authentication-list FlexAAA
no shutdown
```

```
!
wireless profile policy FlexAAA
aaa-override
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

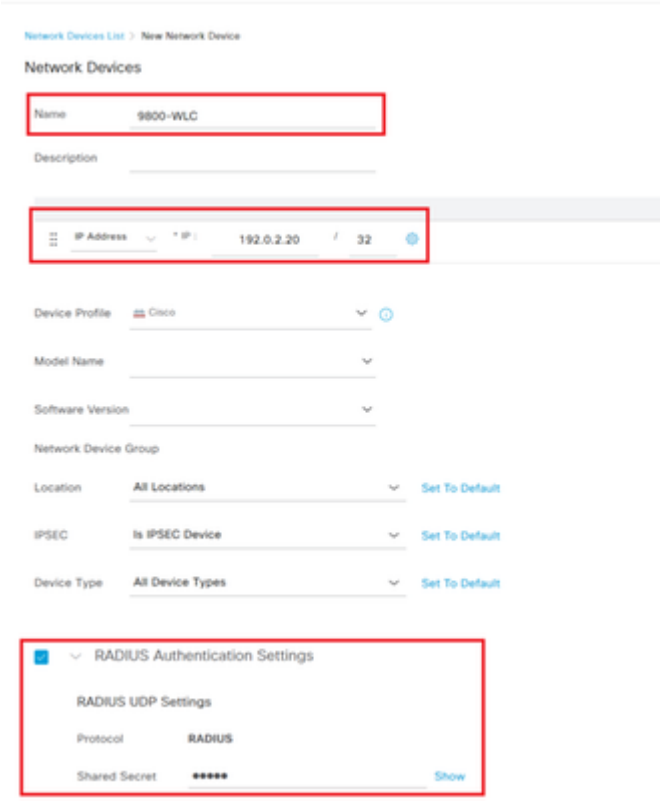
ISE 구성

이제 클라이언트가 로컬 인증에 있을 때 클라이언트를 인증할 수 있도록 ISE를 구성해야 합니다.

1단계. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. +추가를 선택합니다.



2단계. 9800 WLC 추가 이름을 지정하고, IP 주소를 추가하고, RADIUS 인증 설정을 활성화하고, 공유 암호 키를 추가합니다. 이 키는 9800 WLC에서 AAA 서버를 생성할 때 이전에 구성한 키와 동일해야 합니다.



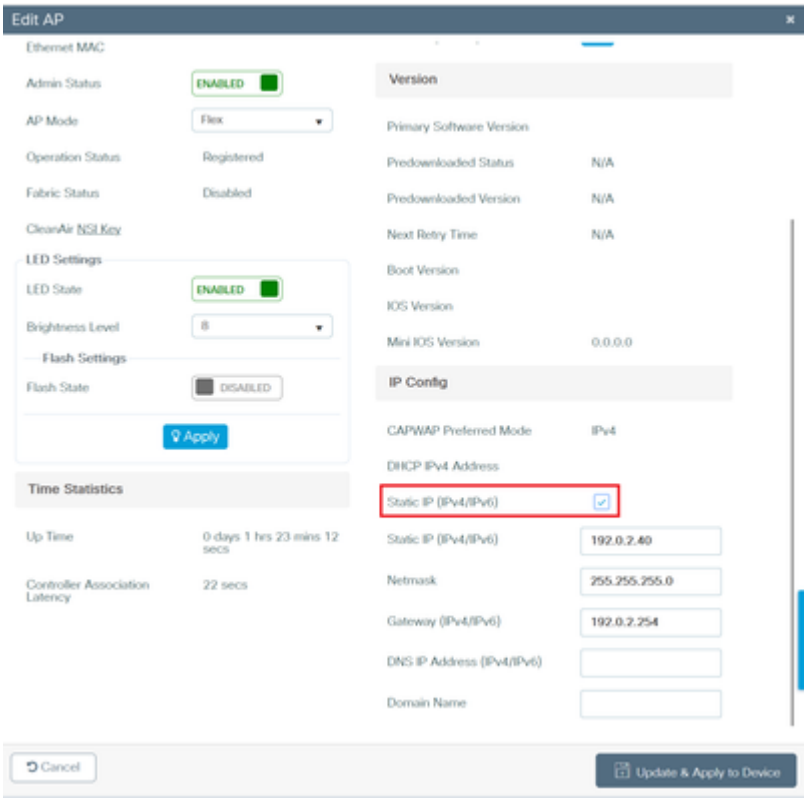
오른쪽 하단 모서리에서 Save(저장)를 클릭합니다.

3단계. 원격 사이트에서 WAN 링크를 해제할 때(그리고 AP가 독립형 모드로 전환할 때) AAA 인증자/전달자 역할을 할 수 있도록 네트워크 디바이스 목록에 AP를 추가해야 합니다.

9800 WLC GUI에서 Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동하고 각 AP IP 주소를 기록해 둡니다.

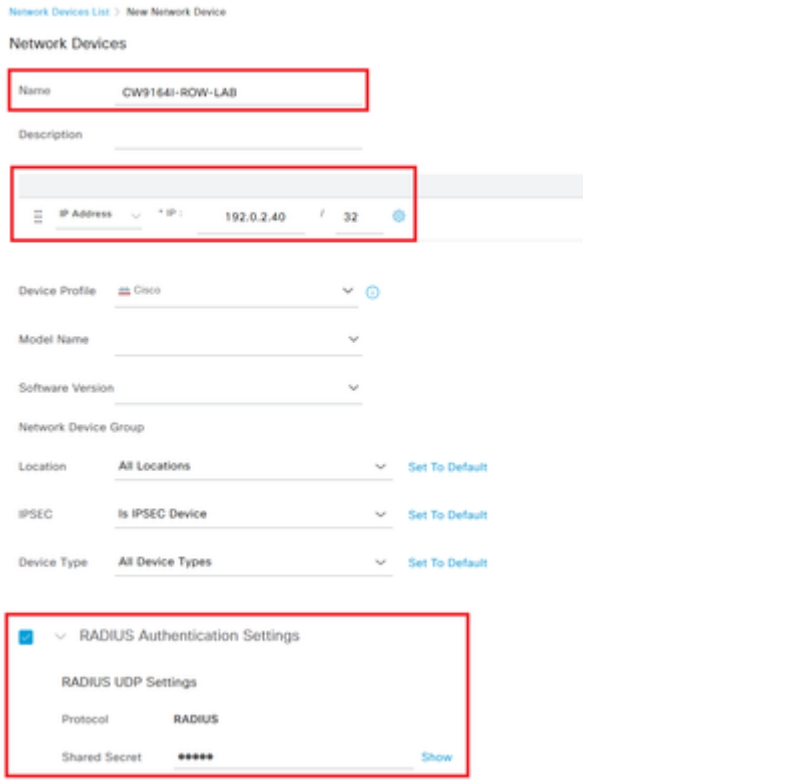
참고: 각 Flex AP의 IP 주소를 Static으로 구성합니다. AP가 느슨해지고 9800 WLC에 다시 연결되면 DHCP의 다른 IP 주소로 다시 돌아올 수 있으므로 ISE와의 통신이 끊어집니다.

고정 IP(IPv4/IPv6)를 활성화합니다. Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.



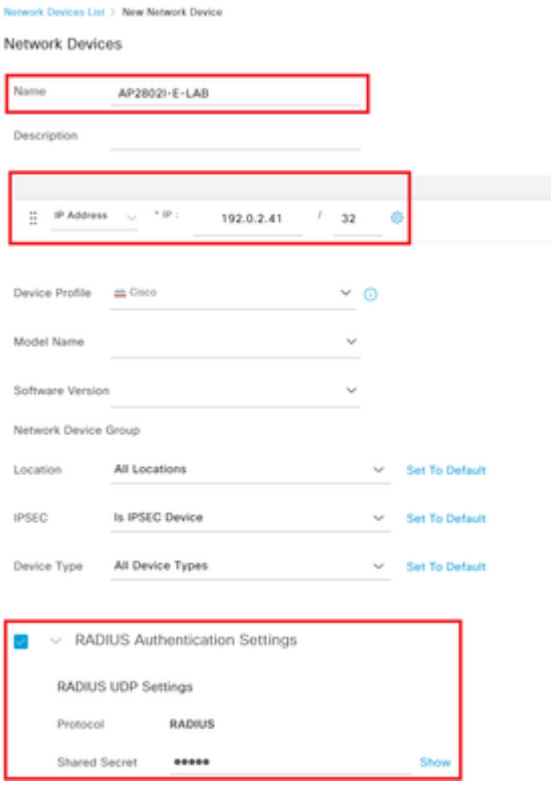
4단계. ISE로 돌아가서 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. +추가를 선택합니다.

AP를 9800 WLC와 동일한 컨피그레이션인 네트워크 디바이스로 추가합니다.



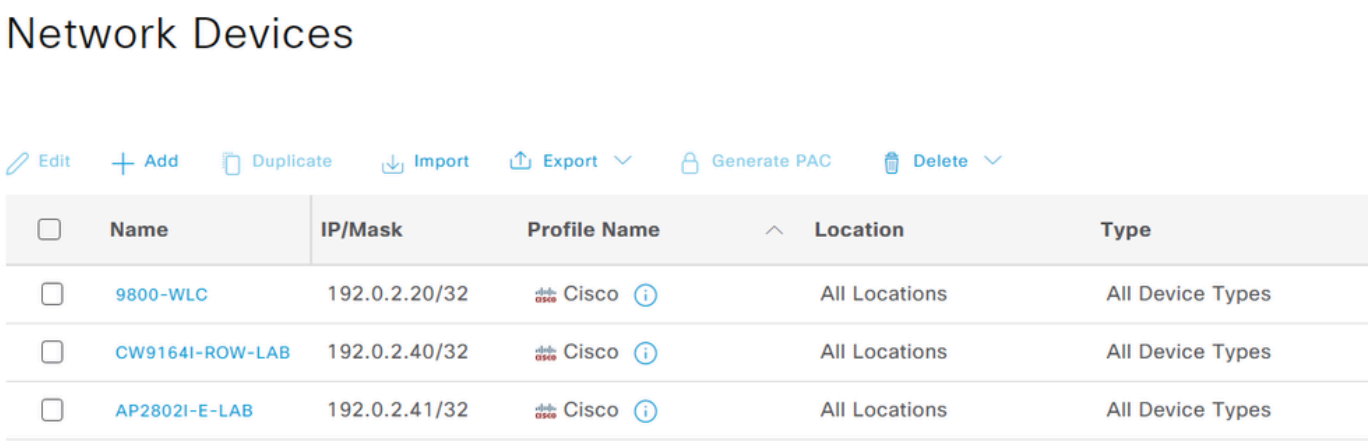
오른쪽 하단 모서리에서 Save(저장)를 클릭합니다.

두 번째 AP의 경우:



오른쪽 하단 모서리에서 Save(저장)를 클릭합니다.

다음과 같은 네트워크 디바이스 목록을 볼 수 있습니다.



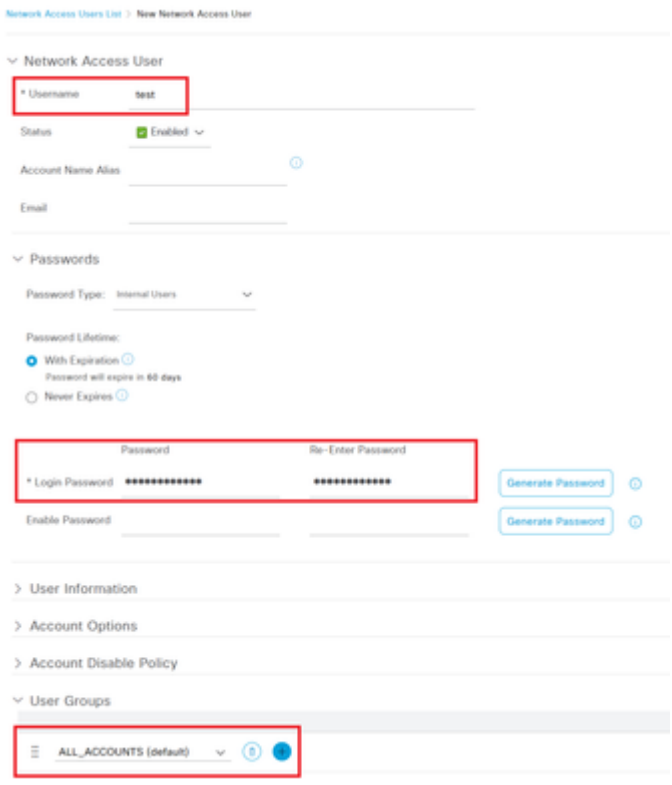
AP가 연속 IP 범위에 있는 경우 마스크 기능을 사용하여 전체 AP 그룹(전부는 아님)에 대한 공유 암호를 정의하는 단일 항목을 구성할 수 있습니다. ISE에서 AP당 하나의 네트워크 디바이스를 구성할

필요가 없습니다. 그러나 와일드카드 및 마스크를 사용하면 비인가 디바이스가 ISE에 전달자 역할을 할 수 있는 여지를 남깁니다.

5단계. Users(사용자) 탭에서 Administration(관리) > Identity Management(ID 관리) > Identities(ID)로 이동하여 802.1x 인증을 위한 사용자를 생성합니다. 선택 +추가:

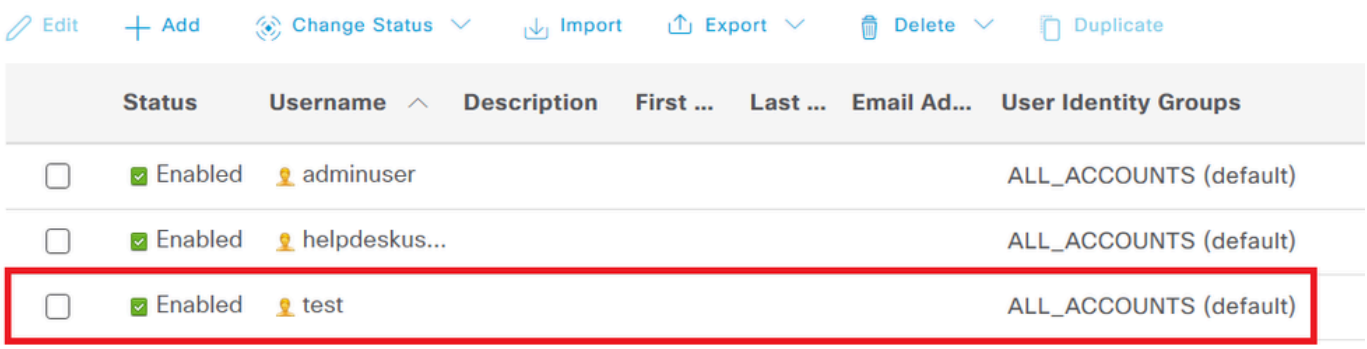


사용자 이름, 비밀번호를 생성하고(비밀번호 재입력 시 동일한 비밀번호 입력), User Groups(사용자 그룹) 드롭다운 메뉴에서 ALL_ACCOUNTS(기본값)를 선택합니다.

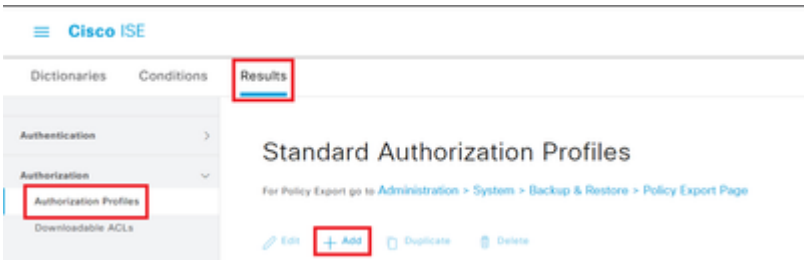


오른쪽 하단에서 Submit(제출)을 클릭합니다.

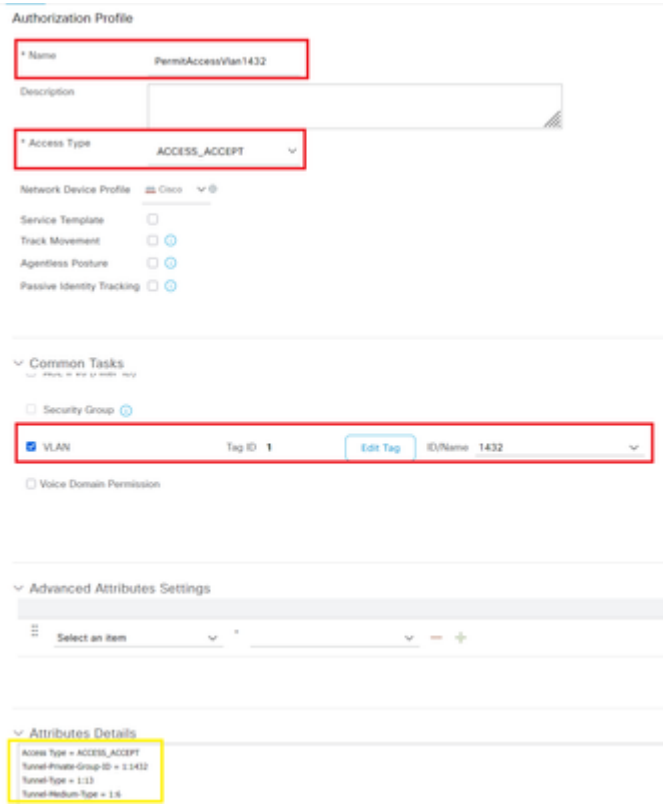
Network Access Users(네트워크 액세스 사용자) 목록에서 사용자를 볼 수 있습니다.



6단계. Policy(정책) > Policy Elements(정책 요소) > Results(결과)로 이동합니다. Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일) 탭에서 +Add(추가)를 선택합니다.



로컬 인증 클라이언트가 할당된 VLAN에 대한 권한 부여 프로파일을 생성합니다.

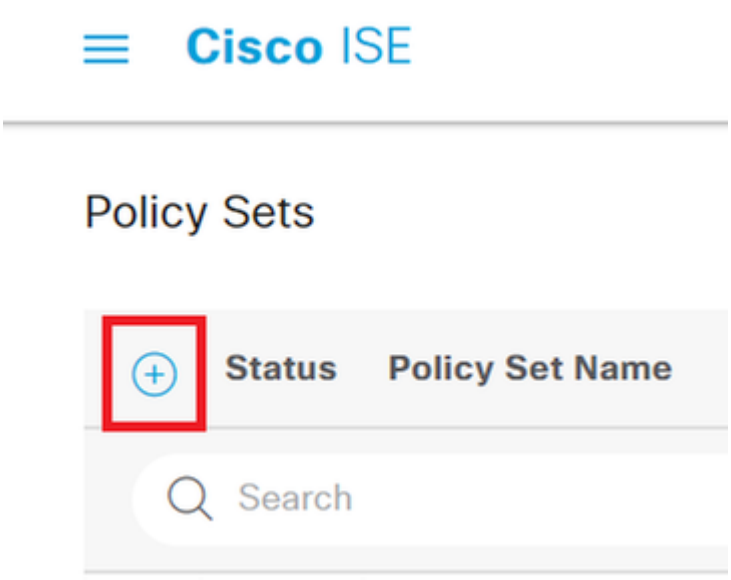


오른쪽 하단에서 Submit(제출)을 클릭합니다.

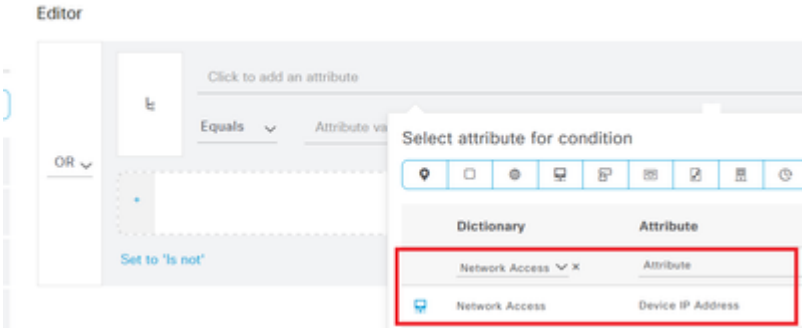
성공 시나리오에서 ISE가 WLC/AP에 전송하는 특성 세부사항을 볼 수 있습니다.

7단계. Policy(정책) > Policy Sets(정책 집합)로 이동합니다. 새 정책 집합을 만듭니다.

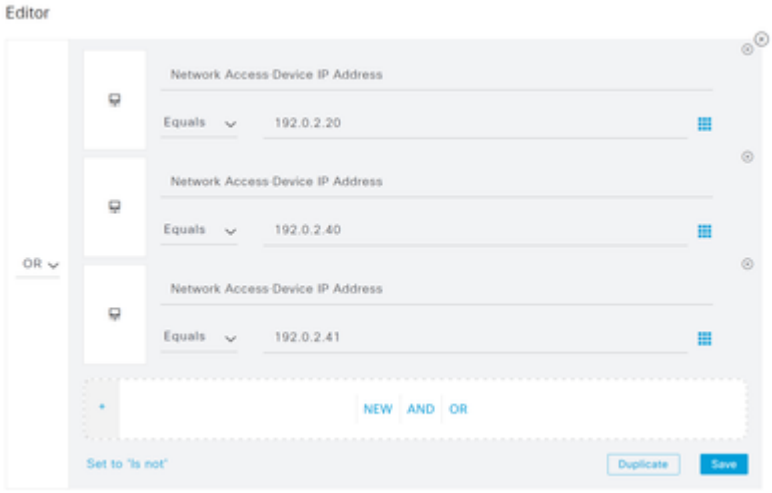
+기호를 클릭합니다.



정책 집합에 이름을 지정합니다. Conditions(조건) 열에서 OR 규칙을 추가하고 Attribute Device IP Address(특성 디바이스 IP 주소)를 사용하여 Dictionary Network Access(사전 네트워크 액세스)를 추가하려면 Equals(같음)를 선택합니다.

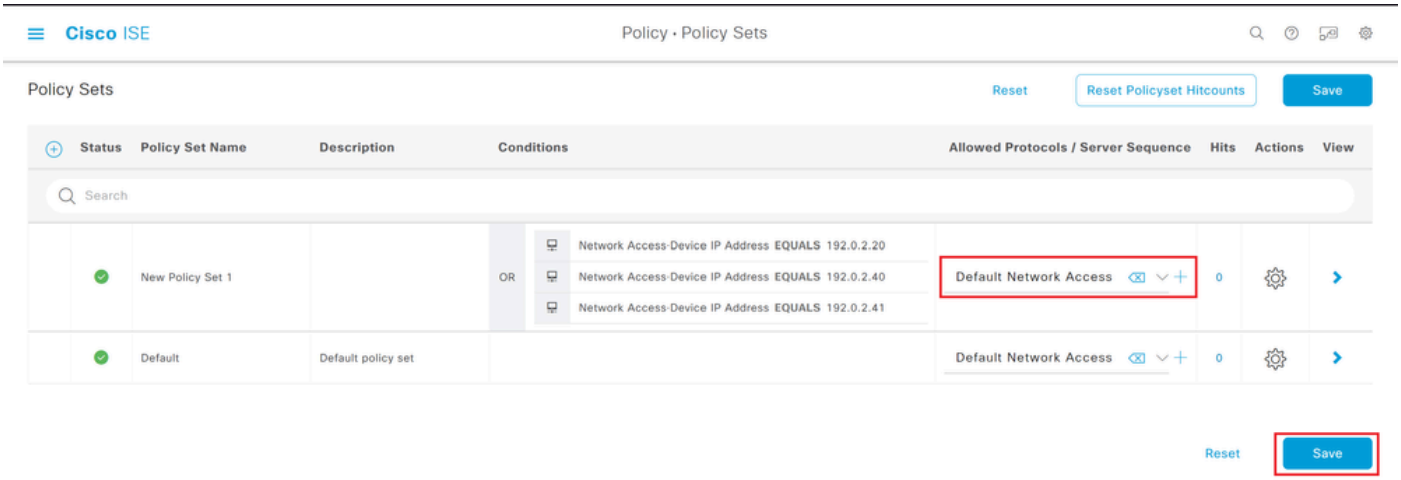


9800 WLC 및 AP IP 주소를 추가합니다.

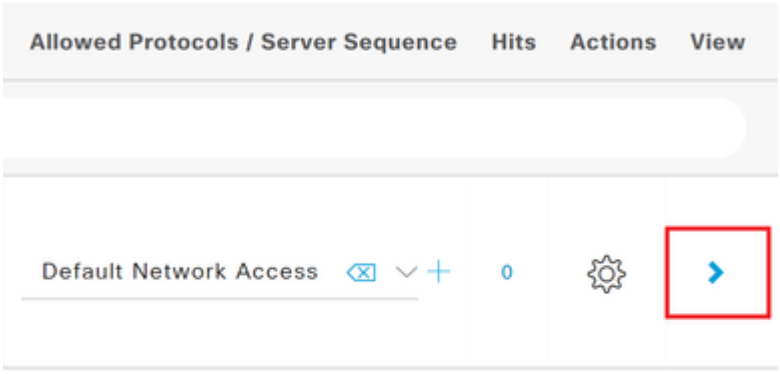


오른쪽 하단에서 Use(사용)를 클릭합니다.

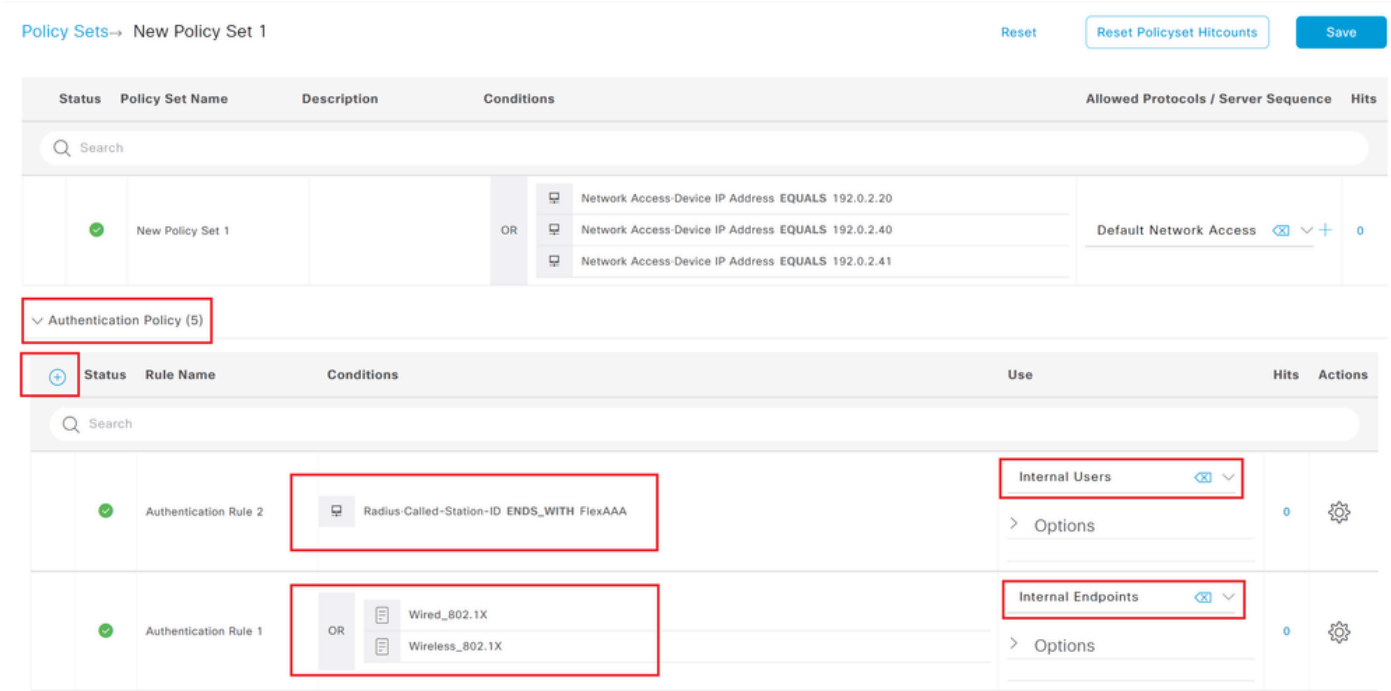
8단계. Allowed Protocols(허용된 프로토콜) 열에서 Default Network Access(기본 네트워크 액세스)를 선택합니다. 마지막에 Save(저장)를 클릭합니다.



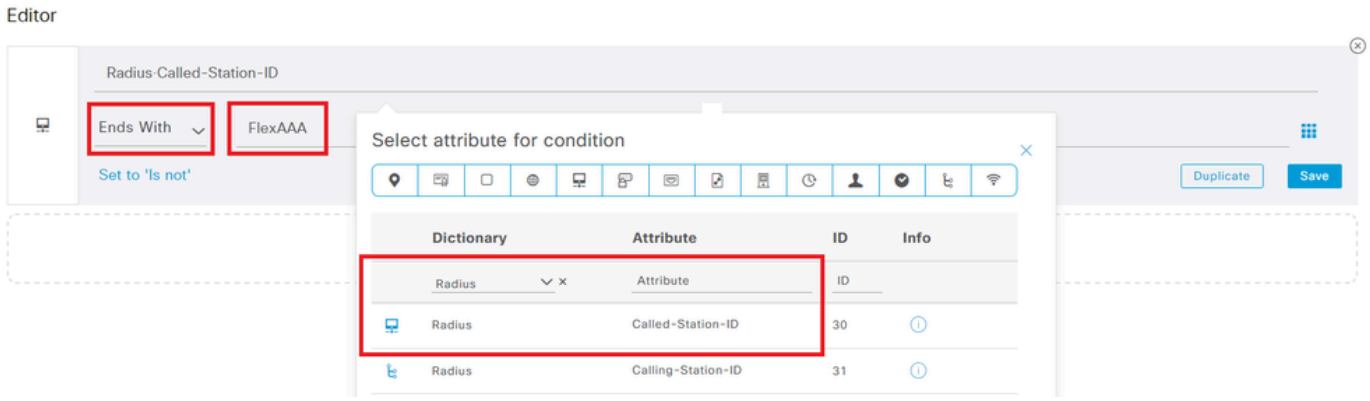
9단계. 열 뷰에서 화살표 기호를 클릭합니다.



10단계. Authentication Policy(인증 정책)를 확장하고 두 개의 새 정책을 생성합니다. 하나는 WLAN 이름용이고 다른 하나는 802.1X 컨피그레이션용입니다.

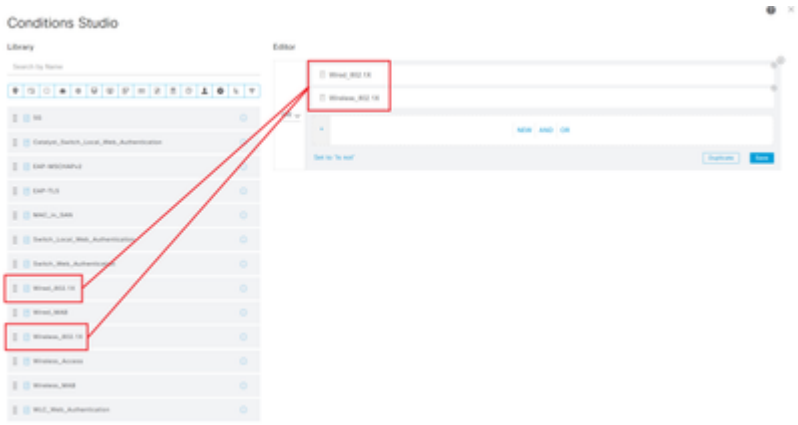


WLAN 이름에서 Radius 및 Attribute Called-Station-ID(Called-Station-ID 특성) 사전을 사용하여 Condition(조건)을 생성합니다. Ends With(다음으로 종료)를 선택하고 WLAN 이름을 입력합니다.



오른쪽 하단에서 Use(사용)를 클릭합니다. 이 정책의 경우 Use(사용) 열에서 Internal Users(내부 사용자)를 선택합니다.

11단계. 802.1X 정책의 경우 ISE에서 사용 가능한 Wired_802.1X 및 Wireless_802.1X 라이브러리로 조건을 생성합니다. 이러한 항목을 끌어서 놓고 조건 또는 을 선택할 수 있습니다.



오른쪽 하단에서 Use(사용)를 클릭합니다. 이 정책의 경우 Use(사용) 열에서 Internal Endpoints(내부 엔드포인트)를 선택합니다.

12단계. 아래로 스크롤하여 Authorization Policy(권한 부여 정책)를 선택하고 새 정책을 생성합니다. 이름을 지정하고 인증 정책에서 WLAN 이름에 대해 생성된 조건과 동일한 조건을 생성합니다.

Profiles(프로파일) 열의 드롭다운 메뉴에서 프로파일 PermitAccessVlan1432를 선택합니다.



오른쪽 하단 모서리에서 Save(저장)를 클릭합니다.

로컬 인증으로 PSK WLAN 구성

1단계. 먼저 원격 사이트에서 FlexConnect 모드 구성 섹션에 설명된 대로 AP를 Flex 모드로 구성합니다.

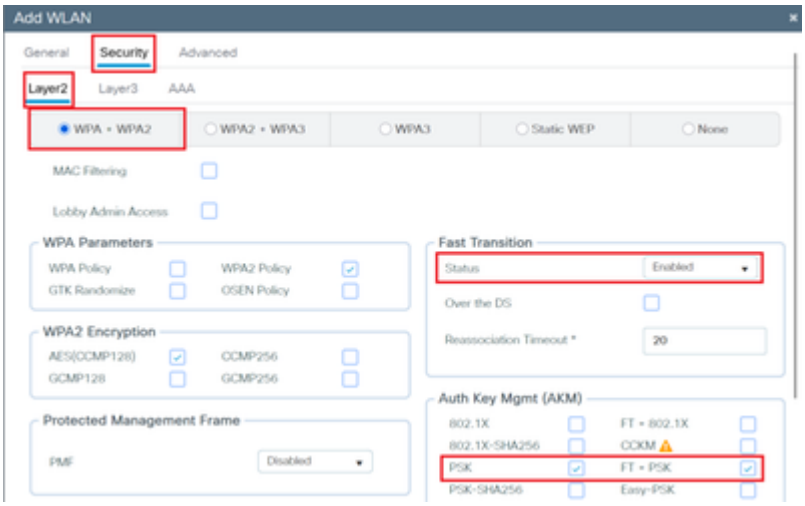
2단계. WLAN 생성.

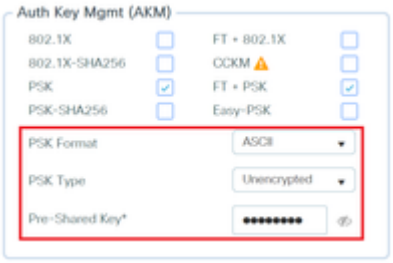
Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동하고 +Add(추가)를 선택합니다.

General 태그에서 Profile Name(프로파일 이름), SSID 및 enable Status(상태 활성화)에 대한 이름을 생성합니다.



3단계. Security(보안) > Layer 2(레이어 2) 탭으로 이동하여 WPA+WPA2, Fast Transition as Enabled(빠른 전환 활성화됨), Auth Key Management PSK(인증 키 관리 PSK) 및 FT+PSK를 선택하고, 원하는 PSK Format(PSK 형식) 및 PSK Type(PSK 유형)을 선택한 다음, 클라이언트에서 사용할 사전 공유 키를 입력합니다.





Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

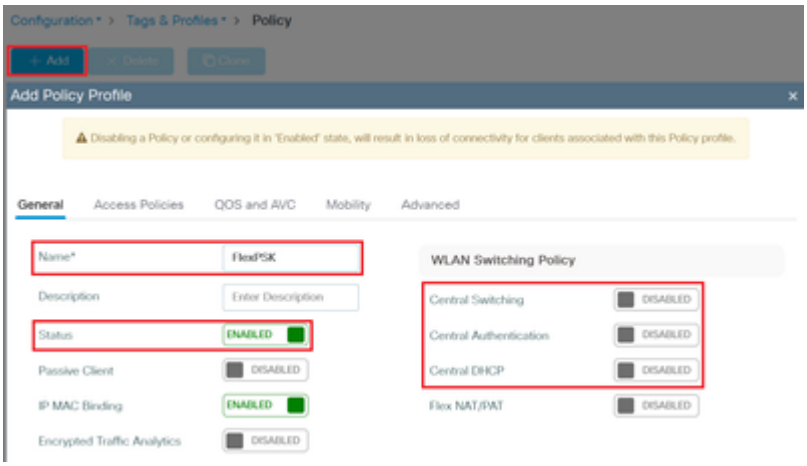
생성된 WLAN을 볼 수 있습니다.



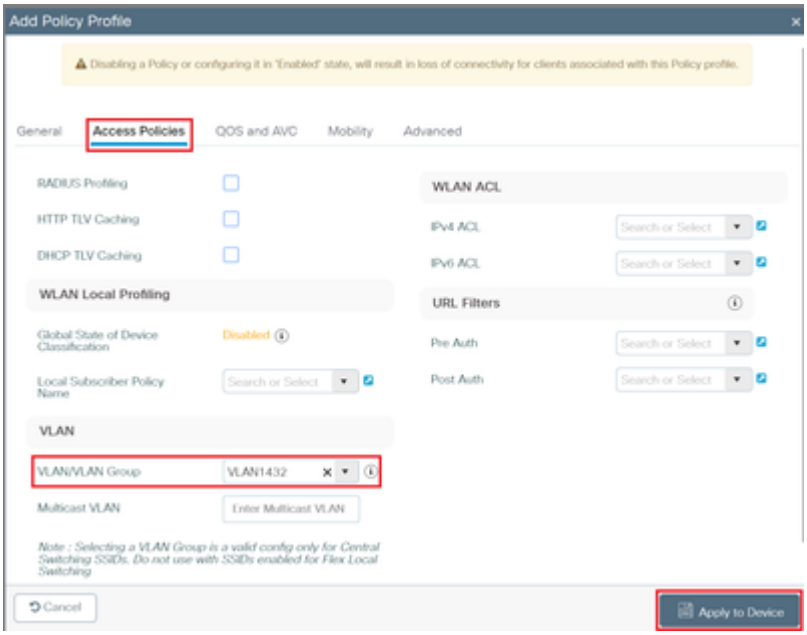
4단계. 정책 프로필을 생성합니다.

Configuration > Tags & Profiles > Policy로 이동합니다.

+Add(추가)를 선택하고 General(일반) 탭에서 정책 프로필의 이름을 지정하고, 상태를 활성화하고, 중앙 스위칭, 중앙 인증 및 중앙 DHCP를 비활성화합니다.

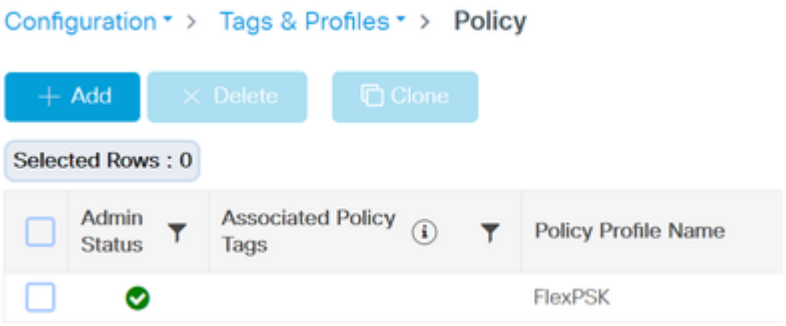


5단계. Access Policies(액세스 정책) 탭으로 이동하여 VLAN을 선택합니다.



Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

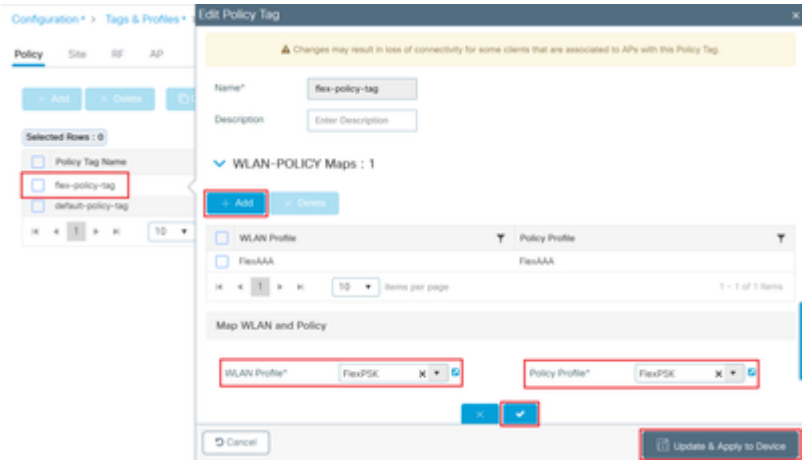
목록에서 정책 프로필을 볼 수 있습니다.



6단계. 새 정책 태그를 생성하거나 기존 태그를 편집할 수 있습니다.

기존 정책 태그를 편집하려면 Configuration > Tags & Profiles > Tags로 이동합니다. 편집할 태그를 선택합니다.

WLAN-POLICY Maps(WLAN-정책 맵)에서 +Add(추가)를 선택합니다. WLAN Profile(WLAN 프로파일)의 드롭다운 메뉴에서 이전에 생성한 WLAN을 선택합니다. Policy Profile(정책 프로필)의 드롭다운 메뉴에서 이전에 생성한 정책 프로필을 선택합니다. 확인 버튼을 클릭한 다음 장치에 적용 을 클릭합니다.



정책 태그가 AP에 이미 할당된 경우 다른 작업을 수행할 필요가 없습니다.

그렇지 않은 경우 AP 태그에 정책 태그를 할당합니다. [구성] > [무선] > [액세스 포인트]로 이동합니다. 정책 태그를 변경할 AP를 선택하고 "Update & Apply to Device"를 클릭합니다.

AP가 분리되고 새 정책 태그로 다시 결합합니다.

AP가 다시 연결되면 Access Points(액세스 포인트) 목록을 확인하고 AP가 Flex 모드이며 올바른 할당된 태그가 있음을 확인할 수 있습니다.

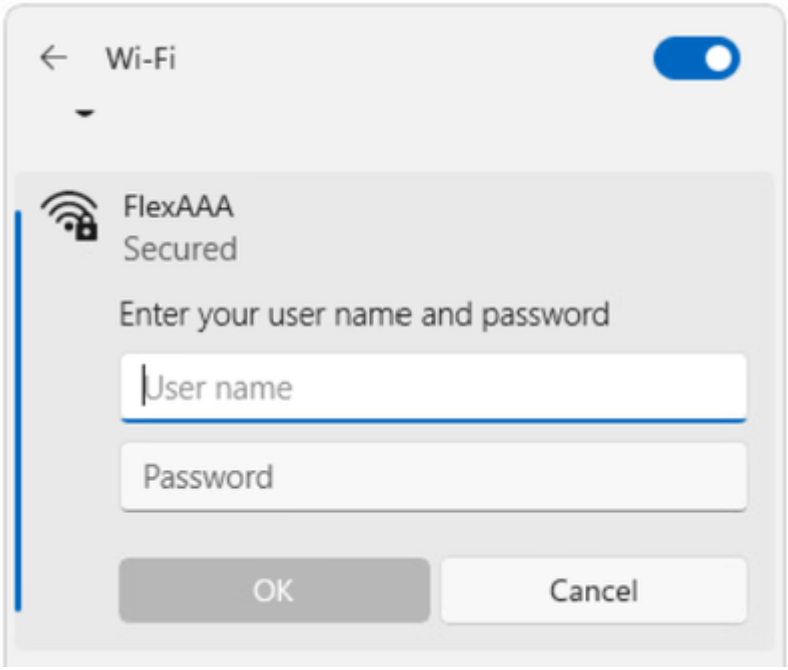
CLI:

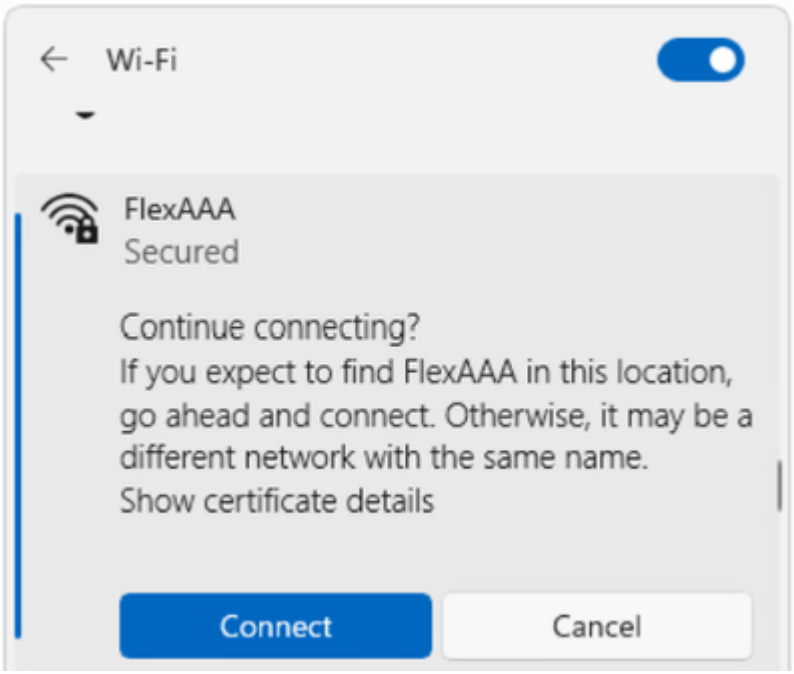
```
wlan FlexPSK 5 FlexPSK
radio policy dot11 24ghz
radio policy dot11 5ghz
security ft
security wpa psk set-key ascii 0 Password123
no security wpa akm dot1x
security wpa akm ft psk
security wpa akm psk
no shutdown
!
```

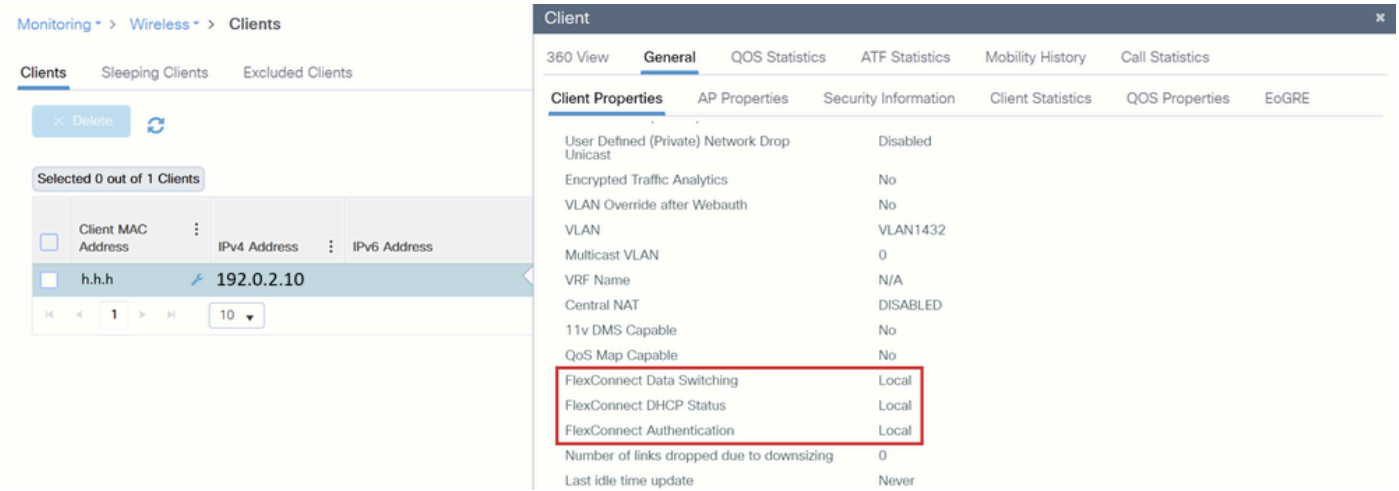
```
wireless profile policy FlexPSK
no central authentication
no central dhcp
no central switching
vlan VLAN1432
no shutdown
!
wireless tag policy flex-policy-tag
wlan FlexAAA policy FlexAAA
wlan FlexPSK policy FlexPSK
!
ap h.h.h (AP Radio MAC address)
policy-tag flex-policy-tag
site-tag Flex-site
rf-tag default-rf-tag
```

다음을 확인합니다.

802.1x WLAN의 경우







CLI:

```
C9800-1#show wireless client mac-address      h.h.h        detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :192.0.2.10
Client IPv6 Addresses :
Client Username : test
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexAAA
Flex Profile : Flex
Wireless LAN Id: 4
WLAN Profile Name: FlexAAA
Wireless LAN Network Name (SSID): FlexAAA
BSSID :
Connected For : 134 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

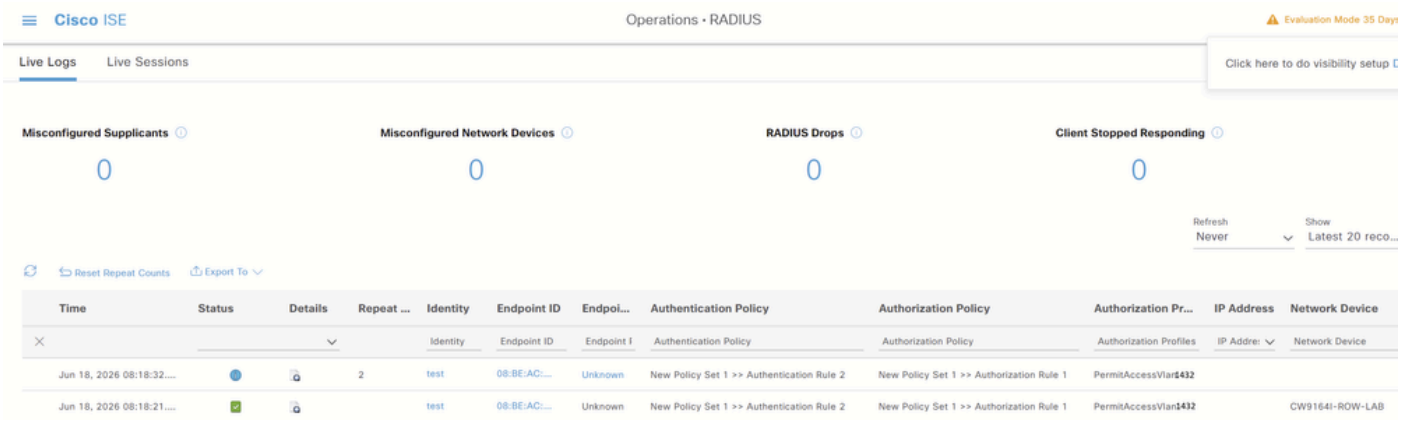
```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

AP CLI에서 다음을 수행합니다.

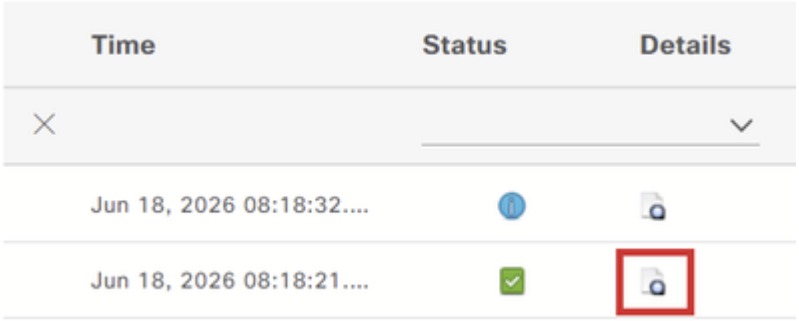
```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC   Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
MM:MM:MM:MM:MM:MM          1       1  33   FlexAAA  -45 MCS9155           No         No
```

ISE에서



IP Address	Network Device	Device Port	Identity Group	Posture ...	Server
IP Addre:	Network Device	Device Port	Identity Group	Posture Sta	Server
		Radio:1Wlan:1			ISE1
	CW9164I-ROW-LAB	Radio:1Wlan:1	User Identity Groups:ALL_ACCOUNTS (default),Unknown		ISE1



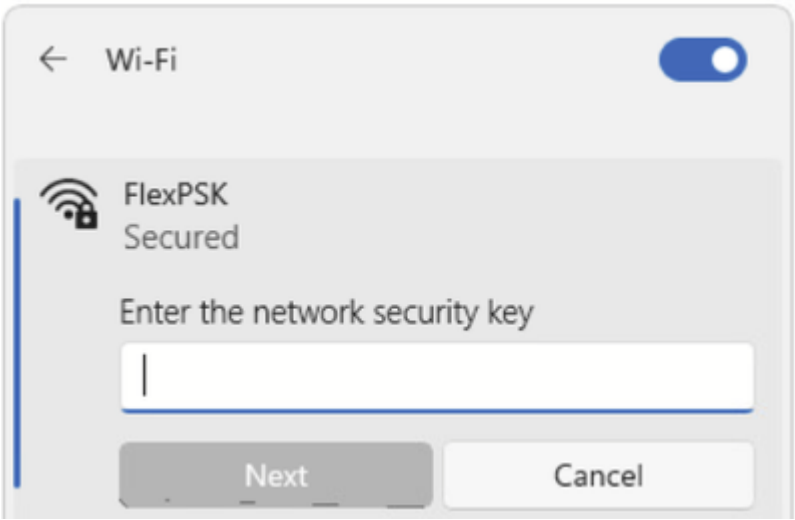
Cisco ISE

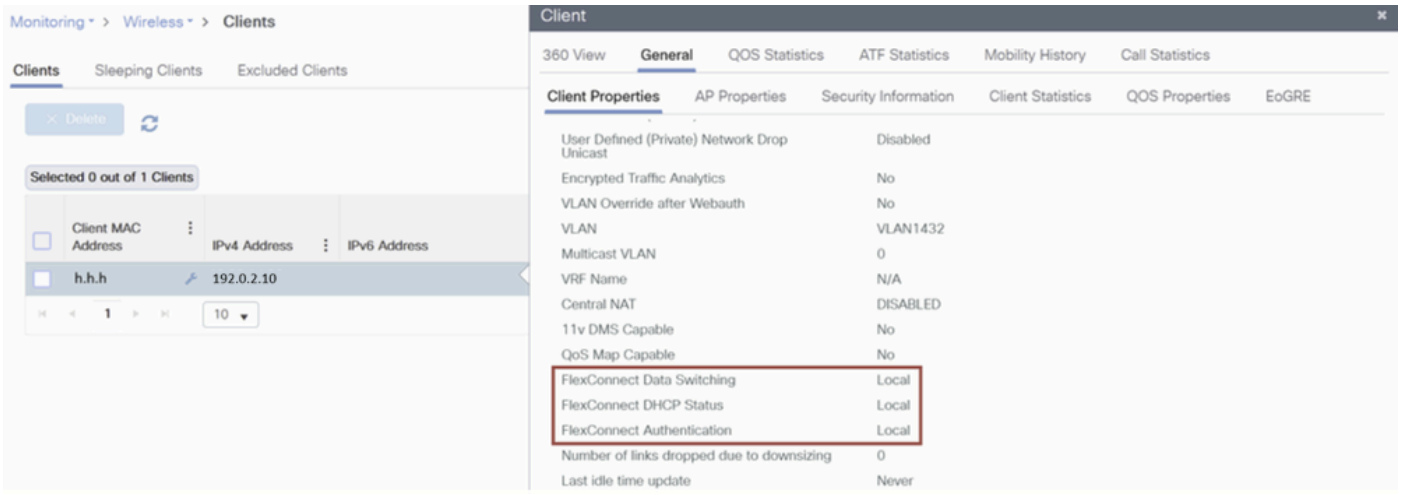
Overview

Event	5200 Authentication succeeded
Username	test
Endpoint Id	HH:HH:HH:HH:HH:HH
Endpoint Profile	Unknown
Authentication Policy	New Policy Set 1 >> Authentication Rule 2
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Authorization Result	PermitAccessVlan1432

Authentication Identity Store	Internal Users
Identity Group	User Identity Groups:ALL_ACCOUNTS (default),Unknown
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	CW9164I-ROW-LAB
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	192.0.2.40
NAS Port Id	Radio:1Wlan:1
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccessVlan1432
Response Time	64 milliseconds

PSK WLAN의 경우





CLI:

```
C9800-1#show wireless client mac-address h.h.h detail

Client MAC Address : h.h.h
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 192.0.2.10
Client IPv6 Addresses :
Client Username: N/A
AP MAC Address :
AP Name: CW9164I-ROW-LAB2
AP slot : 1
Client State : Associated
Policy Profile : FlexPSK
Flex Profile : Flex
Wireless LAN Id: 5
WLAN Profile Name: FlexPSK
Wireless LAN Network Name (SSID): FlexPSK
BSSID :
Connected For : 116 seconds
Protocol : 802.11ac
Channel : 48
Client IIF-ID : 0xa0000001
Association Id : 33
```

```
QoS Map Capable : No
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Local
Client Statistics:
```

AP CLI에서:

```
CW9164I-ROW-LAB#show dot11 clients

Total dot11 clients: 1
      Client MAC    Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
                       1       2  33   FlexPSK  -45 MCS9ISS           No          No
```

문제 해결

동기화된 클라이언트 mac 주소로 AP 디버깅 및 RA 추적을 활성화합니다.

AP에서 다음 디버그를 활성화합니다.

flexconnect 이벤트 디버그
flexconnect pmk 디버그
flexconnect dot11r 디버그
dot11 클라이언트 관리 정보 디버그
dot11 클라이언트 관리 중요 디버그
dot11 클라이언트 관리 오류 디버그
dot11 클라이언트 관리 이벤트 디버그

802.1x WLAN의 경우

AP가 인증에 성공하여 로그를 디버깅합니다.

AP는 802.11 상태 시스템 및 로컬 키 관리를 처리합니다.
AP는 연결을 처리하고 인증을 위해 클라이언트를 준비합니다.

```
[*06/19/2026 06:49:00.1836] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*06/19/2026 06:49:00.1890] wcp/flex_roam_st :: Flexconnect 11r enabled for client HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1908] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
[*06/19/2026 06:49:00.1909] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*06/19/2026 06:49:00.1931] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
```

AP가 권한 부여를 처리하고, VLAN 재정의를 적용하며, 클라이언트를 FWD(Forwarding) 상태로 이동합니다.

```
[*06/19/2026 06:49:20.3601] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*06/19/2026 06:49:20.3601] CLSM[HH:HH:HH:HH:HH:HH]: WCP_EVENT_CLIENT_AUTHORIZE : Plumbing key info to
[*06/19/2026 06:49:20.3612] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*06/19/2026 06:49:20.3625] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*06/19/2026 06:49:20.3627] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Retrieved key for FT+FT_DOT1X algono: 8, vlanId: 1
[*06/19/2026 06:49:20.3627] CLSM[HH:HH:HH:HH:HH:HH]: Local auth (Add) on radio 1 Vap 0 reported to WLC
[*06/19/2026 06:49:20.3701] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*06/19/2026 06:49:20.4313] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr1v0
[*06/19/2026 06:49:20.4317] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 1 Vap 0 IP 192.0.2.10 updatere
[*06/19/2026 06:49:20.4318] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

성공한 동일한 인증에 대한 RA 추적 로그:

RA 추적은 WLC의 세션 오케스트레이션을 로깅합니다. WLC는 클라이언트 ID 및 정책을 확인 합니다.
WLC는 FlexConnect 연결을 인식합니다.

```
2026/06/19 06:49:20.934325580 {wncd_x_R0-1}{1}: [client-orch-sm] [18318]: (note): MAC: hhhh.hhhh.hhhh H
2026/06/19 06:49:20.936543415 {wncd_x_R0-1}{1}: [dot1x] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040000
2026/06/19 06:49:20.936579730 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936600851 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.936654791 {wncd_x_R0-1}{1}: [ewlc-infra-evq] [18318]: (note): Authentication Succes
2026/06/19 06:49:20.936769433 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

WLC가 AP에 정책을 푸시합니다.

```
2026/06/19 06:49:20.937447786 {wncd_x_R0-1}{1}: [svm] [18318]: (info): [hhhh.hhhh.hhhh] Applied User Pr
2026/06/19 06:49:20.937451734 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: c
2026/06/19 06:49:20.937452534 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937455590 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: v
2026/06/19 06:49:20.937456177 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: m
2026/06/19 06:49:20.937458436 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: u
2026/06/19 06:49:20.937462127 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile:tu
2026/06/19 06:49:20.937462755 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937463426 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
2026/06/19 06:49:20.937464035 {wncd_x_R0-1}{1}: [aaa-attr-inf] [18318]: (info): Applied User Profile: t
```

권한 부여가 성공했습니다.

```
2026/06/19 06:49:20.937594042 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
2026/06/19 06:49:20.937597878 {wncd_x_R0-1}{1}: [auth-mgr] [18318]: (info): [hhhh.hhhh.hhhh:capwap_9040
```

클라이언트 매개변수.
2026/06/19 06:49:20.939394217 {wncd_x_R0-1}{1}: [dot11] [18318]: (참고): MAC: hhhh.hhhh.hhhh 클라이언트 데이터 경로 입력 매개 변수 - ssid:FlexAAA,slot_id:1 bssid ifid: 0x0, radio_ifid: 0x90400008, wlan_ifid: 00400004

WLC는 로컬 DHCP/ARP를 통해 IP를 학습합니다.
2026/06/19 06:49:21.001000218 {wncd_x_R0-1}{1}: [client-iplearn] [18318]: (참고): MAC: hhhh.hhhh.hhhh 클라이언트 IP 학습에 성공했습니다. 방법: IP 스누핑 IP: 192.0.2.10

클라이언트가 완전히 연결되었습니다.
2026/06/19 06:49:21.002363496 {wncd_x_R0-1}{1}: [오류 메시지] [18318]: (정보): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/1: wncd: MAC이 있는 디바이스에 대해 ssid(FlexAAA)와 연결된 사용자 이름 항목(테스트): 채널(48)의 hhh.hhh.hhh
2026/06/19 06:49:21.002795009 {wncd_x_R0-1}{1}: [client-orch-state] [18318]: (참고): MAC: hhhh.hhhh.hhhh 클라이언트 상태 전환: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

독립형 시나리오

AP-WLC 연결 손실 및 후속 복구 동안의 동작

AP가 WLC에 조인됩니다. 클라이언트는 성공적인 802.1X 인증을 수행하며 AP는 클라이언트를 FWD(Forwarding) 상태로 전환합니다.

ISE RADIUS Live Logs(RADIUS 라이브 로그)에서 클라이언트 세션이 표시됩니다.

```
[*07/06/2026 20:26:05.8590] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: Local auth on radio 0 Vap 0 IP 192.0.2.10 updatere
[*07/06/2026 20:26:05.9330] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD
```

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```

AP가 WLC에 연결하지 못하고 재전송 횟수를 초과한 후 독립형 모드로 전환합니다. 기존 클라이언트는 로컬로 연결된 상태로 유지됩니다.

```
[*07/06/2026 20:28:47.0840] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=33, NumofPendingMsgs=4
[*07/06/2026 20:28:50.0860] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=34, NumofPendingMsgs=5
[*07/06/2026 20:28:53.0870] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:56.0990] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:28:59.1000] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=35, NumofPendingMsgs=6
[*07/06/2026 20:29:02.1010] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/06/2026 20:29:02.1020] Flexconnect Switching to Standalone Mode!
[*07/06/2026 20:29:02.2170] CAPWAP State: DTLS Teardown
```

그러나 클라이언트는 여전히 연결되어 있습니다.

CW9164I-ROW-LAB2#show dot11 client

총 dot11 클라이언트 수: 1
클라이언트 MAC 슬롯 ID WLAN ID AID WLAN 이름 RSSI 최대 속도 is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 아니오

클라이언트가 독립형 모드에서 다른 AP로 로밍하면 RADIUS 서버에 연결할 수 없어 EAP 핸드셰이크가 실패합니다. 클라이언트가 권한 부여가 취소되고 AP에서 제거됩니다.

```
[*07/06/2026 20:34:44.7240] CLSM[HH:HH:HH:HH:HH:HH]: Session timeout
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-RETRANSMIT hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2670] hostapd:apr0v0: CTRL-EVENT-EAP-TIMEOUT-FAILURE hh:hh:hh:hh:hh:hh
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: Received UNAUTHORIZE for hh:hh:hh:h
[*07/06/2026 20:36:15.2680] wcp/flex_roam_st :: Flexconnect hapdev: recv'd UNAUTH with DISCONNECT REQUE
[*07/06/2026 20:36:15.2680] CLSM[HH:HH:HH:HH:HH:HH]: Client delete initiated with timeout of 10 seconds
[*07/06/2026 20:36:15.2770] CLSM[HH:HH:HH:HH:HH:HH]: Remove success from ClientIPTable on apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Not sending DELETE to cont, reason CLIENT_DEL_EAP_
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: Deauthorize succeeded to radio intf apr0v0
[*07/06/2026 20:36:15.2780] CLSM[HH:HH:HH:HH:HH:HH]: client moved from FWD to DELETE_PENDING
[*07/06/2026 20:36:15.2880] CLSM[HH:HH:HH:HH:HH:HH]: Send Deauth with reason 2 force 1 - Radio 0 Vap 0
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete timeout
[*07/06/2026 20:36:25.0830] CLSM[HH:HH:HH:HH:HH:HH]: Delete client reassoc 0 succeeded to radio intf ap
```

AP가 백업 RADIUS 서버에 클라이언트 세션을 보냅니다.

AP가 WLC에 다시 연결합니다. AP가 다시 연결 모드로 전환되고 로컬 클라이언트 세션 정보를 WLC와 동기화합니다.

클라이언트 세션은 AP 연결 상태에 따라 기본 및 백업 ISE 노드 간에 전환됩니다.

AP와 클라이언트는 WLC에 연결된 것으로 표시되며, 클라이언트는 AP와 WLC 간의 연결이 끊어질 때 어떤 연결 끊김이나 플랩도 감지하지 못했습니다.

```
CW9164I-ROW-LAB2#show dot11 clients

Total dot11 clients: 0


Upon roaming back, the client undergoes local authentication. The AP processes the association and move

[*07/06/2026 20:48:49.2830] CLSM[HH:HH:HH:HH:HH:HH]: US Auth(b0) seq 2653 IF 23 slot 0 vap 0 len 30 sta
[*07/06/2026 20:48:49.2840] CLSM[HH:HH:HH:HH:HH:HH]: DS Auth len 30 slot 0 vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2850] CLSM[HH:HH:HH:HH:HH:HH]: client moved from UNASSOC to AUTH
[*07/06/2026 20:48:49.2920] CLSM[HH:HH:HH:HH:HH:HH]: US Reassoc Req(20) seq 2654 IF 23 slot 0 vap 0 len
[*07/06/2026 20:48:49.2930] CLSM[HH:HH:HH:HH:HH:HH]: AUTH TYPE RSNIE DOT1X
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: Populate client capability: cap_from_click=true, m
[*07/06/2026 20:48:49.2940] Flexconnect local_auth 1 local_assoc 1 frame subtype 32
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio id: 0, vap id: 0, max clients for this wlan:
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: radio state: 1, client state: 1, max_client_per_ra
[*07/06/2026 20:48:49.2940] Adding RM Capable IE - Len = 5, RRM[0] = 73, RRM[1] = c0
[*07/06/2026 20:48:49.2940] DS [re]Assoc 1 req_len=201 resp_len=146 11r_len=0 cckm 0 qos_flag 1 status
[*07/06/2026 20:48:49.2940] CLSM[HH:HH:HH:HH:HH:HH]: DS Reassoc Resp(30) IF 0 slot 0 vap 0 state AUTH,
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: Driver send mgmt frame success Radio 0 Vap 0
[*07/06/2026 20:48:49.2950] CLSM[HH:HH:HH:HH:HH:HH]: client moved from AUTH to ASSOC
```

```
[*07/06/2026 20:48:49.2950] Sending ADD MOBILE to client SM for local auth client mac HH:HH:HH:HH:HH:HH
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.2960] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Driver Add Client success AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2960] CLSM[HH:HH:HH:HH:HH:HH]: Added to ClientIPTable on apr0v0
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: client moved from ASSOC to 8021X
[*07/06/2026 20:48:49.2970] CLSM[HH:HH:HH:HH:HH:HH]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*07/06/2026 20:48:49.2980] wcp/flex_roam_st :: Flexconnect hapdev: client WCP_EVENT_CLIENT_ASSOC/REASS
[*07/06/2026 20:48:49.6360] received WCP_EVENT_CLIENT_AUTHORIZE (non) roaming case clearing roam flags
[*07/06/2026 20:48:49.6360] wcp/flex_roam_st :: Flexconnect (AUTHORIZE) received PTK thru wcp_event
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect HH:HH:HH:HH:HH:HH client ACL , Qos Profile:
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect AAA Override Vlan with WLAN mapping: 1432 f
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect Sending ADD_MOBILE_PAYLOAD (v4-client-acl-n
[*07/06/2026 20:48:49.6370] wcp/flex_roam_st :: Flexconnect encode_and_send_add_mobile_to_dott11_client
[*07/06/2026 20:48:49.6370] CLSM[HH:HH:HH:HH:HH:HH]: ADD_MOBILE AID 1
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: check vlan override vlan 1432
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*07/06/2026 20:48:49.6380] CLSM[HH:HH:HH:HH:HH:HH]: client moved from 8021X to IPLEARN_PENDING
[*07/06/2026 20:48:49.6390] wcp/flex_roam_st :: Flexconnect Sending HREAP_APAUTH_CLIENT_ADD
[*07/06/2026 20:48:49.6900] CLSM[HH:HH:HH:HH:HH:HH]: Authorize succeeded to radio intf apr0v0
[*07/06/2026 20:48:49.6910] CLSM[HH:HH:HH:HH:HH:HH]: client moved from IPLEARN_PENDING to FWD


CW9164I-ROW-LAB2#show dot11 clients

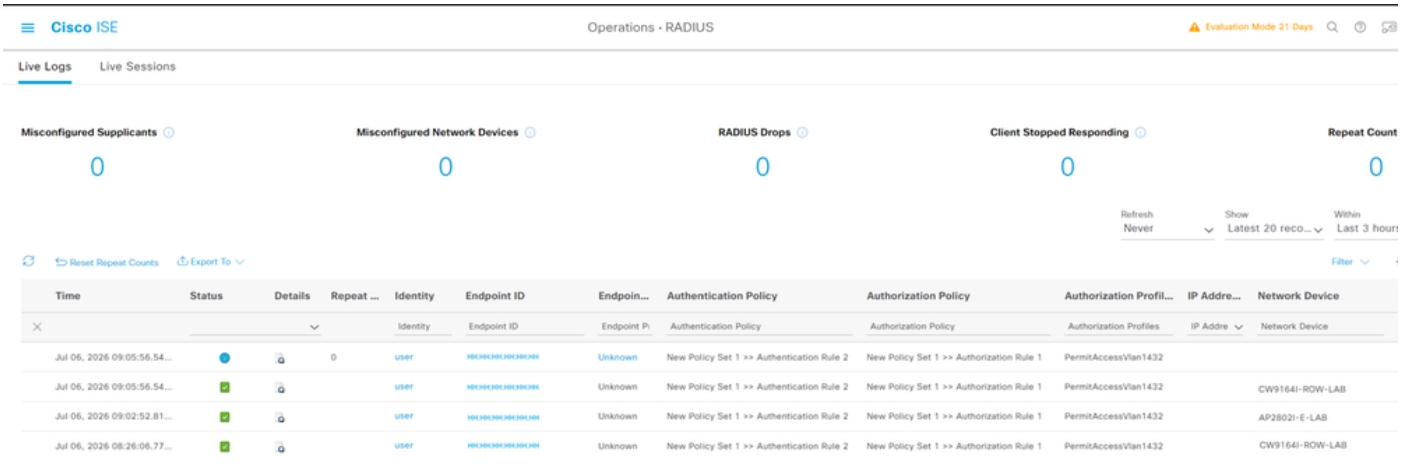
Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -39 M7 No No



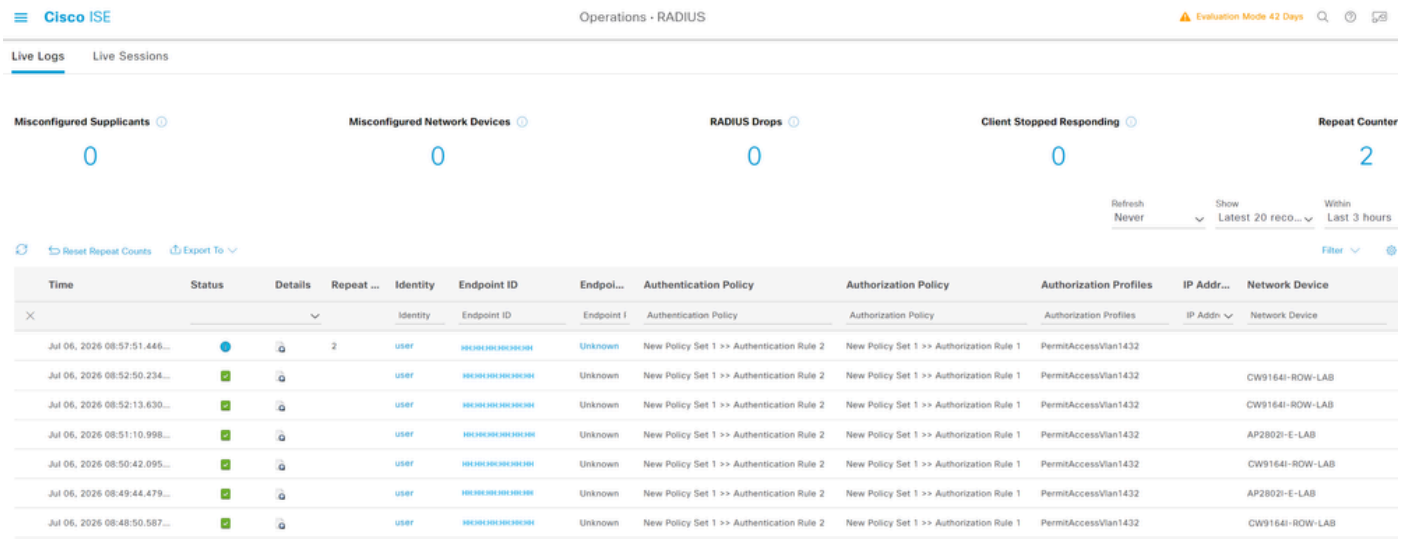

*07/06/2026 20:59:57.7690] Discovery Response from 192.0.2.20
[*07/06/2026 21:00:08.0080] CAPWAP State: DTLS Setup
[*07/06/2026 21:00:08.4820] CAPWAP State: Join
[*07/06/2026 21:00:09.3740] Sending Join request to 192.0.2.20 through port 5253, packet size 1376
[*07/06/2026 21:00:09.3780] Join Response from 192.0.2.20, packet size 1397
[*07/06/2026 21:00:09.4040] CAPWAP State: Image Data
[*07/06/2026 21:00:09.5020] CAPWAP State: Configure
[*07/06/2026 21:00:12.5510] CAPWAP State: Run
[*07/06/2026 21:00:12.6480] AP has joined controller C9800-1
[*07/06/2026 21:00:12.6490] Flexconnect Switching to Connected Mode!
[*07/06/2026 21:00:12.6520] CLSM[HH:HH:HH:HH:HH:HH]: AP_REAP_CLIENT_INFO_PAYLOAD Client MAC HH:HH:HH:HH
[*07/06/2026 21:00:12.6520] AssocTimeAtAP 1783371169 clientBitmap=0x13
[*07/06/2026 21:00:12.6520] CLSM[00:00:00:00:00:00]: Numbers of Local Switching clients to report : 1
[*07/06/2026 21:00:14.8270] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8270] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716
[*07/06/2026 21:00:14.8280] chatter: pmk_tracker :: PMKTracker: add dot11r entry for client HH:HH:HH:HH
[*07/06/2026 21:00:14.8280] chatter: bssid BB:BB:BB:BB:BB:BB, life_time 1783371774, created_at 17833716


CW9164I-ROW-LAB2# show dot11 clients

Total dot11 clients: 1
Client MAC Slot ID WLAN ID AID WLAN Name RSSI Maxrate is_wgb_wired is_mld_sta
HH:HH:HH:HH:HH:HH 0 1 1 FlexAAA -40 M7 No No
```



기본 ISE: 초기 세션(08:26:06) 및 WLC 연결 복원 후 재개된 세션(09:02:52)을 기록합니다.



백업 ISE: AP가 독립형 모드로 작동하는 동안 세션 활동(08:48:50 - 08:57:51)을 캡처합니다.

첫 번째 세션은 08:26:06에 있었으며, 그 후 AP는 WLC에 대한 연결이 끊어지고 독립형 모드로 전환되었습니다.

세션 09:02:52는 AP가 WLC와의 연결을 재설정한 후 첫 번째 세션입니다.

관련 정보

- CCNP Enterprise Wireless Design ENWLSD 300-425 및 구현 ENWLSI 300-430 공식 인증서 가이드, 2판
- [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE 17.8.x - 장: FlexConnect]
- [Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Cupertino 릴리스 17.8.x 릴리

스 정보
- Cisco Wireless Access Points의 기능 매트릭스
- 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.