

Catalyst 9800 Wireless Controller에서 802.1x AAA 재정의가 포함된 FlexConnect WLAN

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[구성](#)

[9800 WLC의 AAA 컨피그레이션](#)

[WLAN 컨피그레이션](#)

[AP를 FlexConnect 모드로 설정](#)

[스위치 구성](#)

[정책 프로파일 컨피그레이션](#)

[정책 태그 컨피그레이션](#)

[정책 태그 할당](#)

[ISE 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 FlexConnect 모드 액세스 포인트(AP)와 VLAN(Virtual Local Area Network) 인증, 권한 부여 및 계정 관리(AAA) 재지정을 사용하여 로컬로 스위칭되는 802.1x WLAN(Wireless Local Area Network)을 사용하여 Elastic Wireless LAN 컨트롤러(9800 WLC)를 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC 컨피그레이션 모드
- FlexConnect

사용되는 구성 요소

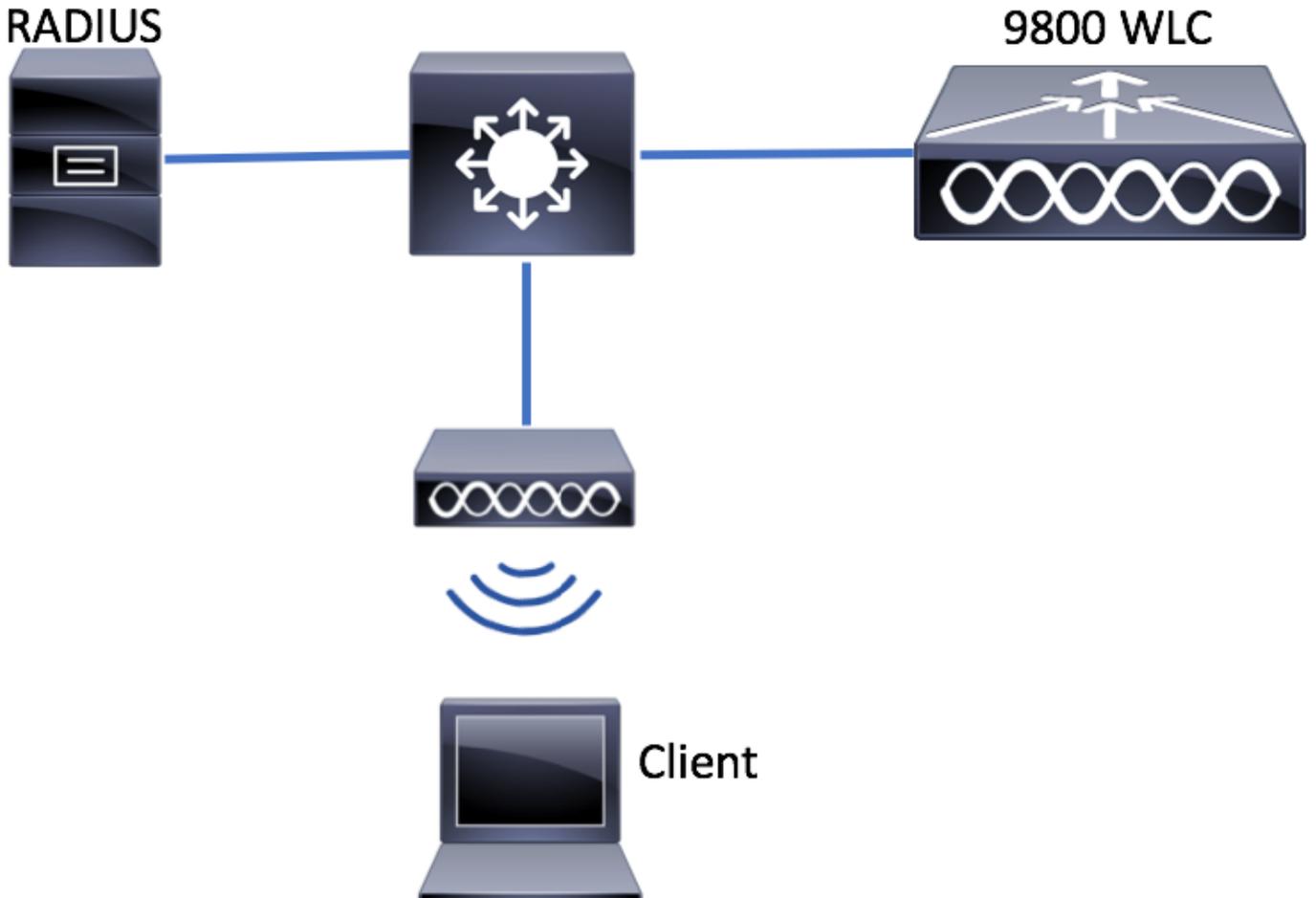
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800 WLC v16.10

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

구성

네트워크 다이어그램



구성

9800 WLC의 AAA 컨피그레이션

이 링크의 지침을 따를 수 있습니다.

[9800 WLC의 AAA 컨피그레이션](#)

WLAN 컨피그레이션

이 링크의 지침을 따를 수 있습니다.

[WLAN 컨피그레이션](#)

AP를 FlexConnect 모드로 설정

AireOS 컨피그레이션과 달리 9800 WLC에서는 AP에서 직접 AP 로컬 또는 flexconnect 모드를 구성할 수 없습니다. FlexConnect 모드에서 AP를 구성하려면 다음 단계를 수행합니다.

GUI

1단계. Flex 프로파일을 구성합니다.

다음으로 이동 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Flex default-flex-profile을 수정하거나 +Add를 클릭하여 새 프로필을 만듭니다.

Flex Profile

+ Add x Delete

Flex Profile Name	Description
default-flex-profile	default profile

10 items per page

Add Flex Profile

General Local Authentication Policy ACL VLAN

Name* new-flex-profile Multicast Overridden Interface

Description New flex profile Fallback Radio Shut

Native VLAN ID 2601 ARP Caching

HTTP Proxy Port 0 Efficient Image Upgrade

HTTP-Proxy IP Address 0.0.0.0 CTS Inline Tagging

Office Extend AP

Join Minimum Latency

Cancel Save & Apply to Device

2단계. 필요한 VLAN을 추가합니다(기본 WLAN의 VLAN 또는 ISE에서 푸시된 VLAN 모두).

참고: Policy Profile Configuration(정책 프로파일 컨피그레이션) 섹션 3단계에서 SSID에 할당된 기본 VLAN을 선택합니다. 해당 단계에서 VLAN 이름을 사용하는 경우 Flex Profile 컨피그레이션에서 동일한 VLAN 이름을 사용해야 합니다. 그렇지 않으면 클라이언트가 WLAN에 연결할 수 없습니다.

Edit Flex Profile

General

Local Authentication

Policy ACL

VLAN

+ Add

✕ Delete

VLAN Name	ID	ACL Name
◀ 0 ▶ 10 items per page		
No items to display		

VLAN당 특정 ACL을 선택적으로 추가할 수 있습니다.

VLAN Name*

vlan2602

VLAN Id*

2602

ACL Name

Select ACL

✓ Save

↺ Cancel

선택적으로, FlexConnect AP가 로컬 인증을 수행할 수 있도록 Radius 서버 그룹을 할당합니다.

Edit Flex Profile

General **Local Authentication** Policy ACL VLAN

Radius Server Group **ISE-kcg-grp** LEAP

EAP Fast Profile Select Profile PEAP

TLS

RADIUS

Users

+ Add

Username

0 10 items per page

No items to display

3단계. 사이트 태그를 구성합니다.

구성 > 태그 및 프로파일 > 태그 > 사이트로 이동합니다. 기본 사이트 태그(모든 AP에 기본적으로 지정된 태그)를 수정하거나 새 태그를 생성합니다(새 태그를 생성하려면+추가를 누릅니다).

Q Search Menu Items

Dashboard

Monitoring >

Configuration >

Administration >

Troubleshooting

Manage Tags

Policy **Site** RF AP

+ Add

Site Tag Name

default-site-tag

1 10 items per page

Enable Local Site(로컬 사이트 활성화) 옵션을 비활성화해야 합니다. 비활성화하지 않으면 Flex Profile(플렉스 프로파일) 옵션을 사용할 수 없습니다.

참고: Enable Local Site(로컬 사이트 활성화)가 활성화된 사이트 태그를 가져오는 모든 AP는 로컬 모드로 구성됩니다. 마찬가지로 Enable Local Site(로컬 사이트 활성화)가 비활성화된 사이트 태그를 가져오는 모든 AP는 flexconnect 모드로 구성됩니다.

4단계. AP를 9800 WLC에 연결하고 2단계에서 구성한 사이트 태그를 할당합니다.

Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트) > AP name(AP 이름)으로 이동하고 Site(사이트 태그)을 설정합니다. 그런 다음 Update & Apply to Device(업데이트 및 디바이스에 적용)를 클릭하여 변경 사항을 설정합니다.

참고: AP에서 태그를 변경하면 9800 WLC와의 연결이 끊기고 약 1분 내에 다시 가입됩니다.

5단계. AP가 다시 연결되면 AP 모드가 Flex임을 확인합니다.

The screenshot shows the 'Access Points' management interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main area displays a table of APs. One AP, 'AP1702-05', is highlighted, and its 'AP Mode' is 'Flex'. Below the table are expandable sections for 'Radios 802.11a/n/ac', 'Radios 802.11b/g/n', and 'Dual-Band Radios'. On the right, the 'Edit AP' sidebar is open to the 'General' tab, showing various configuration fields. The 'AP Mode' dropdown menu is set to 'Flex' and is highlighted with a red box.

CLI

```
# config t
# wireless profile flex new-flex-profile
# arp-caching
# description "New flex profile"
# native-vlan-id 2601

# config t
# wireless tag site new-flex-site
# flex-profile new-flex-profile
# no local-site
# site-tag new-flex-site

# config t
# ap <eth-mac-address>
# site-tag new-flex-site
Associating site-tag will cause associated AP to reconnect
# exit

#show ap name <ap-name> config general | inc AP Mode
AP Mode                               : FlexConnect
```

스위치 구성

AP가 연결된 스위치의 인터페이스를 구성합니다.

```
# config t
# interface <int-id>
# switchport trunk native vlan 2601
# switchport mode trunk
# spanning-tree portfast trunk
# end
```

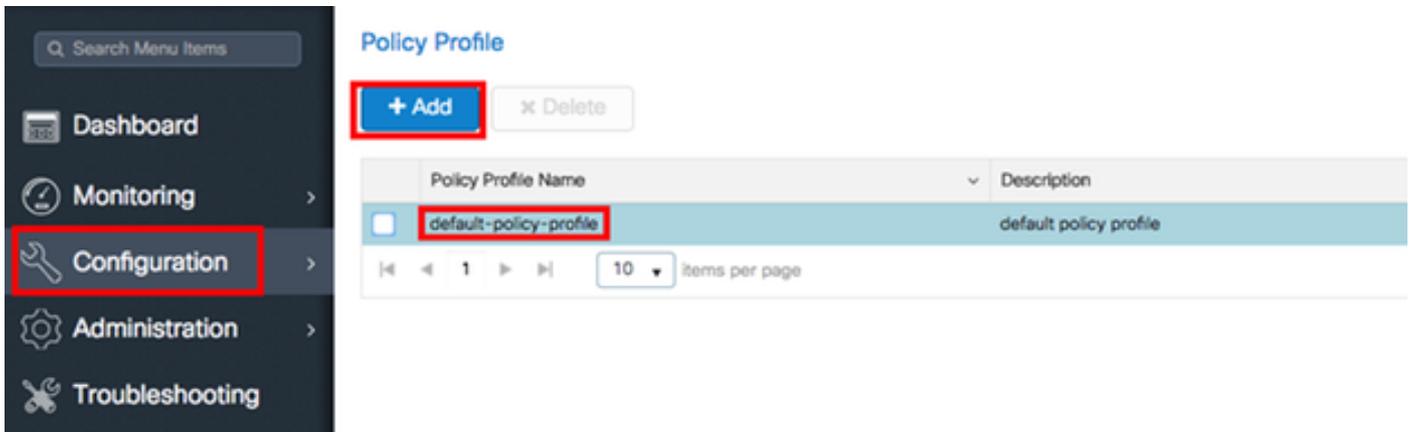
정책 프로파일 컨피그레이션

정책 프로파일 내에서 클라이언트를 할당할 VLAN을 ACL(Access Controls List), QoS(Quality of Service), 모빌리티 앵커, 타이머 등의 다른 설정 중에서 결정할 수 있습니다.

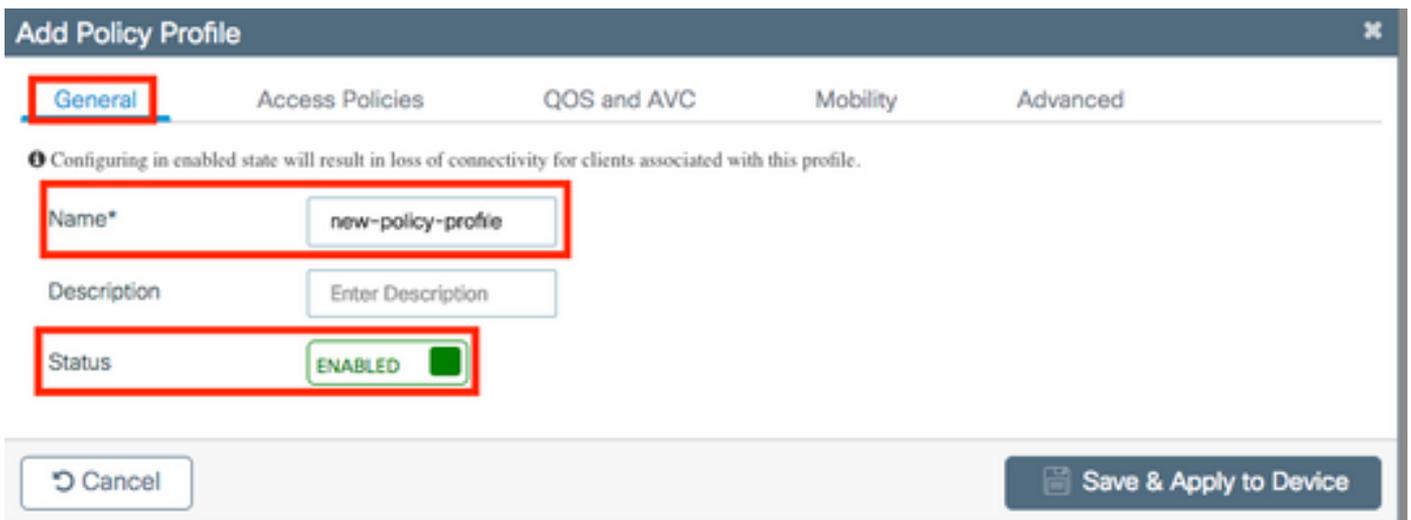
GUI

1단계. WLAN에 할당할 정책 프로필을 구성합니다.

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Policy(정책)로 이동하고 새 프로파일을 생성하거나 default-policy-profile을 수정합니다.



2단계. **General(일반)** 탭에서 Policy Profile(정책 프로파일)에 이름을 지정하고 상태를 ENABLED(활성화됨)로 변경합니다.



3단계. **Access Policies(액세스 정책)** 탭에서 무선 클라이언트가 기본적으로 이 WLAN에 연결할 때 할당할 VLAN을 할당합니다.

드롭다운에서 VLAN 이름 하나를 선택하거나 수동으로 vlan id를 입력할 수 있습니다.

참고: 드롭다운에서 vlan 이름을 선택하는 경우 Set AP as FlexConnect mode(AP를 FlexConnect 모드로 설정) 섹션 2에서 사용되는 vlan 이름과 일치하는지 확인합니다.

Add Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

WLAN Local Profiling

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

WLAN ACL

IPv4 ACL

IPv6 ACL

VLAN

VLAN/VLAN Group

또는

Edit Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

WLAN Local Profiling

Local HTTP Profiling

Radius HTTP Profiling

Local DHCP Profiling

Local Subscriber Policy Name

WLAN ACL

IPv4 ACL

IPv6 ACL

VLAN

VLAN/VLAN Group

4단계. **Advanced(고급)** 탭으로 이동하고 **Central Authentication Enable(중앙 인증 활성화)** 및 **Allow AAA Override(AAA 재정의 허용)** 옵션을 활성화합니다. **중앙 스위칭을 비활성화**해야 합니다.

인증 프로세스를 9800 WLC에서 중앙 집중식으로 수행하려면 **중앙 인증**을 활성화해야 합니다. FlexConnect AP가 무선 클라이언트를 인증하도록 하려면 비활성화합니다.

Edit Policy Profile



General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)*

Idle Timeout (sec)*

Idle Threshold (bytes)*

Client Exclusion Timeout (sec)*

DHCP

DHCP Enable

DHCP Server IP Address

DHCP Opt82 Enable

DHCP Opt82 Ascii

DHCP Opt82 RID

DHCP Opt82 Format

DHCP AP MAC

DHCP SSID

DHCP AP ETH MAC

DHCP AP NAME

DHCP Policy Tag

DHCP AP Location

DHCP VLAN ID

AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Cancel

Update & Apply to Device

CLI

```
# config t
# wireless profile policy new-policy-profile # central association # vlan <vlan-id or vlan-name>
```

no shutdown

정책 태그 컨피그레이션

정책 태그는 SSID를 정책 프로파일과 연결하는 데 사용됩니다. 새 정책 태그를 만들거나 기본 정책 태그를 사용할 수 있습니다.

참고: default-policy-tag는 WLAN ID가 1~16인 모든 SSID를 기본 정책 프로파일에 자동으로 매핑합니다. 수정하거나 삭제할 수 없습니다. ID가 17 이상인 WLAN이 있는 경우 default-policy-tag를 사용할 수 없습니다.

GUI:

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Tags(태그) > Policy(정책)로 이동하고 필요한 경우 새 정책을 추가합니다.

The screenshot shows the 'Manage Tags' interface. On the left is a navigation menu with 'Configuration' selected. The main area has tabs for 'Policy', 'Site', 'RF', and 'AP', with 'Policy' selected. Below the tabs are '+ Add' and 'x Delete' buttons. A table lists existing tags:

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

At the bottom, there are pagination controls showing '1' items per page.

WLAN 프로필을 원하는 정책 프로파일에 연결합니다.

The 'Add Policy Tag' dialog box is shown. It has a close button (x) in the top right. The 'Name*' field contains 'PolicyTagName'. The 'Description' field contains 'Enter Description'. Below are '+ Add' and 'x Delete' buttons. At the bottom, there are dropdowns for 'WLAN Profile' and 'Policy Profile', and a 'No items to display' message. At the very bottom are 'Cancel' and 'Save & Apply to Device' buttons.

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ▶ 0 ▶ ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

✕
✓

↶ Cancel
📄 Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
◀ ▶ 1 ▶ ▶ 10 items per page 1 - 1 of 1 items	

↶ Cancel
📄 Save & Apply to Device

CLI:

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

정책 태그 할당

AP에 정책 태그 할당

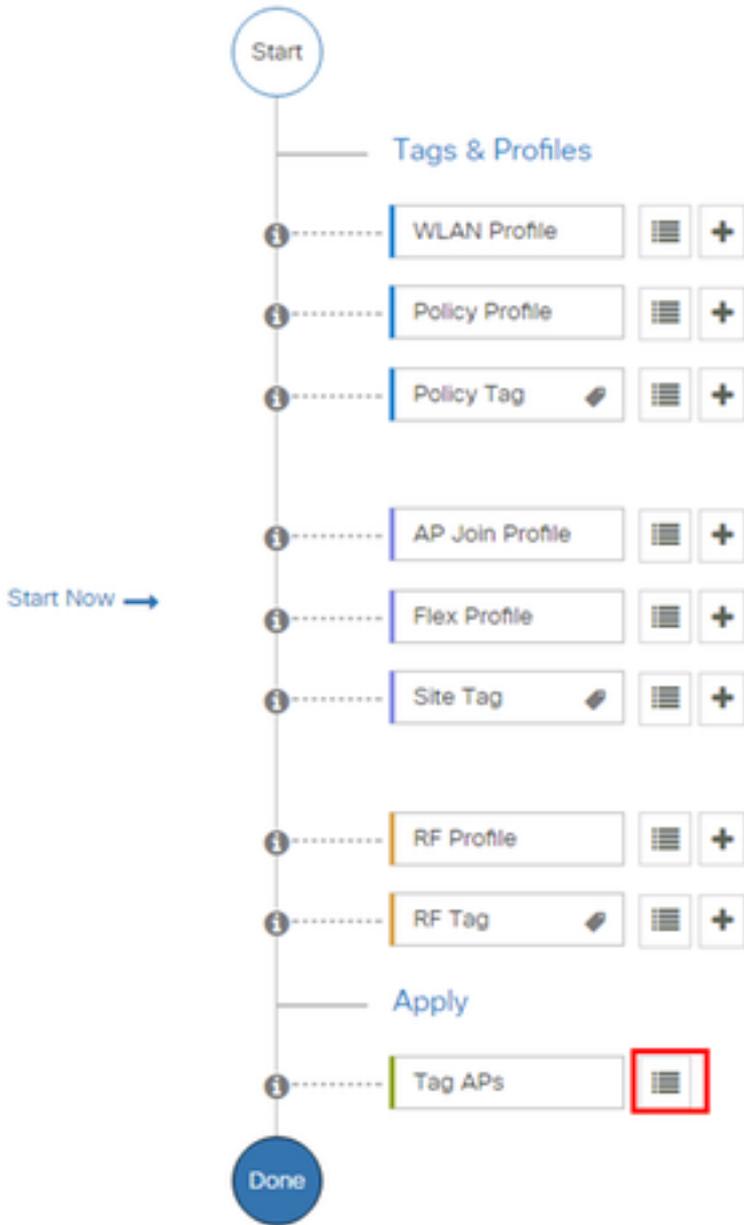
GUI

하나의 AP에 태그를 할당하려면 Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트) > AP Name(AP 이름) > General Tags(일반 태그)로 이동하여 필요한 할당을 설정한 다음 Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

General	Version
AP Name*	Primary Software Version
Location*	Predownloaded Status
Base Radio MAC	Predownloaded Version
Ethernet MAC	Next Retry Time
Admin Status	Boot Version
AP Mode	IOS Version
Operation Status	Mini IOS Version
Fabric Status	IP Config
Tags	IP Address
Policy	Static IP
Site	Time Statistics
RF	Up Time
	Controller Associated Time
	Controller Association Latency

참고: AP에서 정책 태그를 변경하면 9800 WLC와의 연결이 끊어지고 약 1분 내에 다시 가입됩니다.

여러 AP에 동일한 정책 태그를 할당하려면 Configuration(컨피그레이션) > Wireless(무선) > Wireless Setup(무선 설정) > Start Now(지금 시작) > Apply(적용)로 이동합니다.



태그를 할당할 AP를 선택하고 + Tag APs를 클릭합니다.

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

<input checked="" type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag
<input checked="" type="checkbox"/>	AP3802-02-WS	AIR-AP3802I-A-K9	C0-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-01	AIR-AP3802I-B-K9	20-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag
<input checked="" type="checkbox"/>	AP3802-02	AIR-AP3802I-B-K9	40-40-00-10-11-00	Local	Enabled	Registered	default-policy-tag	default-site-tag

10 items per page 1 - 3 of 3 items

표시된 태그를 선택하고 **Save & Apply to Device**(저장 및 장치에 적용)를 클릭합니다.

Tag APs [X]

Tags

Policy: default-policy-tag ▼

Site: SiteTag1 ▼

RF: default-rf-tag ▼

Cancel **Save & Apply to Device**

CLI

```
# config t
# ap <ethernet-mac-addr>
# policy-tag <policy-tag-name>
# end
```

ISE 컨피그레이션

ISE v1.2 컨피그레이션의 경우 이 링크를 선택합니다.

[ISE 컨피그레이션](#)

다음을 확인합니다.

이 명령을 사용하여 현재 컨피그레이션을 확인할 수 있습니다

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | name | all }
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
```

문제 해결

WLC 9800은 ALWAYS-ON 추적 기능을 제공합니다.이렇게 하면 모든 클라이언트 연결 관련 오류, 경고 및 알림 수준 메시지가 지속적으로 로깅되며, 발생 후 장애 또는 장애 상태에 대한 로그를 볼 수 있습니다.

참고:생성되는 로그 볼륨에 따라 몇 시간에서 며칠로 돌아갈 수 있습니다.

기본적으로 수집된 9800 WLC의 추적을 보려면 SSH/텔넷을 통해 9800 WLC에 연결하고 다음 단계를 수행하십시오(텍스트 파일에 세션을 로깅하는지 확인).

1단계. 컨트롤러의 현재 시간을 확인하여 문제가 발생한 시점으로 돌아가 로그를 추적할 수 있습니다.

```
# show clock
```

2단계. 시스템 컨피그레이션에 따라 컨트롤러의 버퍼 또는 외부 syslog에서 syslog를 수집합니다. 시스템 상태 및 오류(있는 경우)를 빠르게 볼 수 있습니다.

```
# show logging
```

3단계. 디버그 조건이 활성화되었는지 확인합니다.

```
# show debugging
```

IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:

Packet Infra debugs:

Ip Address

Port

-----|-----

참고:나열된 조건이 있는 경우, 활성화된 조건(mac 주소, ip 주소 등)이 발생하는 모든 프로세스의 디버그 레벨로 추적이 로깅되고 있음을 의미합니다. 이렇게 하면 로그 볼륨이 증가합니다.따라서 능동적으로 디버깅하지 않을 때는 모든 조건을 지우는 것이 좋습니다

4단계. 테스트 중인 mac 주소가 3단계에서 조건으로 나열되지 않았다고 가정하면 특정 mac 주소에 대한 상시 알림 레벨 추적을 수집합니다.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file  
always-on-<FILENAME.txt>
```

세션의 내용을 표시하거나 파일을 외부 TFTP 서버에 복사할 수 있습니다.

```
# more bootflash:always-on-<FILENAME.txt>  
or  
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

조건부 디버깅 및 무선 활성화 추적

Always-On 추적이 조사 중인 문제의 트리거를 확인할 수 있는 충분한 정보를 제공하지 않는 경우 조건부 디버깅을 활성화하고 RA(Radio Active) 추적을 캡처할 수 있습니다. 그러면 지정된 조건과 상호 작용하는 모든 프로세스(이 경우 클라이언트 MAC 주소)에 대한 디버그 수준 추적을 제공할 수 있습니다. 조건부 디버깅을 활성화하려면 다음 단계를 수행합니다.

5단계. 활성화된 디버그 조건이 없는지 확인합니다.

```
# clear platform condition all
```

6단계. 모니터링할 무선 클라이언트 MAC 주소에 대한 디버그 조건을 활성화합니다.

이 명령은 제공된 mac 주소를 30분(1800초) 동안 모니터링하기 시작합니다. 선택적으로 이 시간을 최대 2085978494초로 늘릴 수 있습니다.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

참고: 한 번에 두 개 이상의 클라이언트를 모니터링하려면 mac 주소당 디버그 무선 mac <aaaa.bbbb.cccc> 명령을 실행합니다.

참고: 모든 항목이 내부적으로 버퍼링되어 나중에 볼 수 있으므로 터미널 세션에서 클라이언트 활동의 출력이 표시되지 않습니다.

7단계. 모니터링할 문제 또는 동작을 재현합니다.

8단계. 기본 또는 구성된 모니터 시간이 시작되기 전에 문제가 재현되는 경우 디버그를 중지합니다.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

모니터 시간이 경과하거나 디버그 무선이 중지되면 9800 WLC는 이름이 다음과 같은 로컬 파일을 생성합니다.

```
ra_trace_MAC_aaabbcccc_HHMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

9단계. mac 주소 활동의 파일을 수집합니다. ra trace .log를 외부 서버에 복사하거나 화면에 직접 출력을 표시할 수 있습니다.

RA 추적 파일의 이름 확인

```
# dir bootflash: | inc ra_trace
```

파일을 외부 서버에 복사합니다.

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

내용 표시:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

10단계. 근본 원인이 아직 명확하지 않은 경우 디버그 수준 로그를 보다 자세히 볼 수 있는 내부 로그를 수집합니다. 이미 수집 및 내부적으로 저장된 디버그 로그만 자세히 살펴보기 때문에 클라이언트를 다시 디버깅할 필요가 없습니다.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }  
to-file ra-internal-<FILENAME>.txt
```

참고:이 명령 출력은 모든 프로세스의 모든 로깅 레벨에 대한 추적을 반환하며 상당한 양의 데이터를 제공합니다. Cisco TAC에 문의하여 이러한 추적을 분석하십시오.

ra-internal-FILENAME.txt를 외부 서버에 복사하거나 화면에 직접 출력을 표시할 수 있습니다.

파일을 외부 서버에 복사합니다.

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

내용 표시:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

11단계. 디버그 조건을 제거합니다.

```
# clear platform condition all
```

참고:문제 해결 세션 후에 항상 디버그 조건을 제거해야 합니다.