Catalyst 9800 Wireless Controller에서 MAC 인증 SSID 구성

목차

소개

이 문서에서는 Cisco Catalyst 9800 WLC에서 MAC 인증 보안을 사용하여 WLAN(Wireless Local Area Network)을 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요건

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- MAC 주소
- Cisco Catalyst 9800 Series 무선 컨트롤러
- ISE(Identity Service Engine)

사용되는 구성 요소

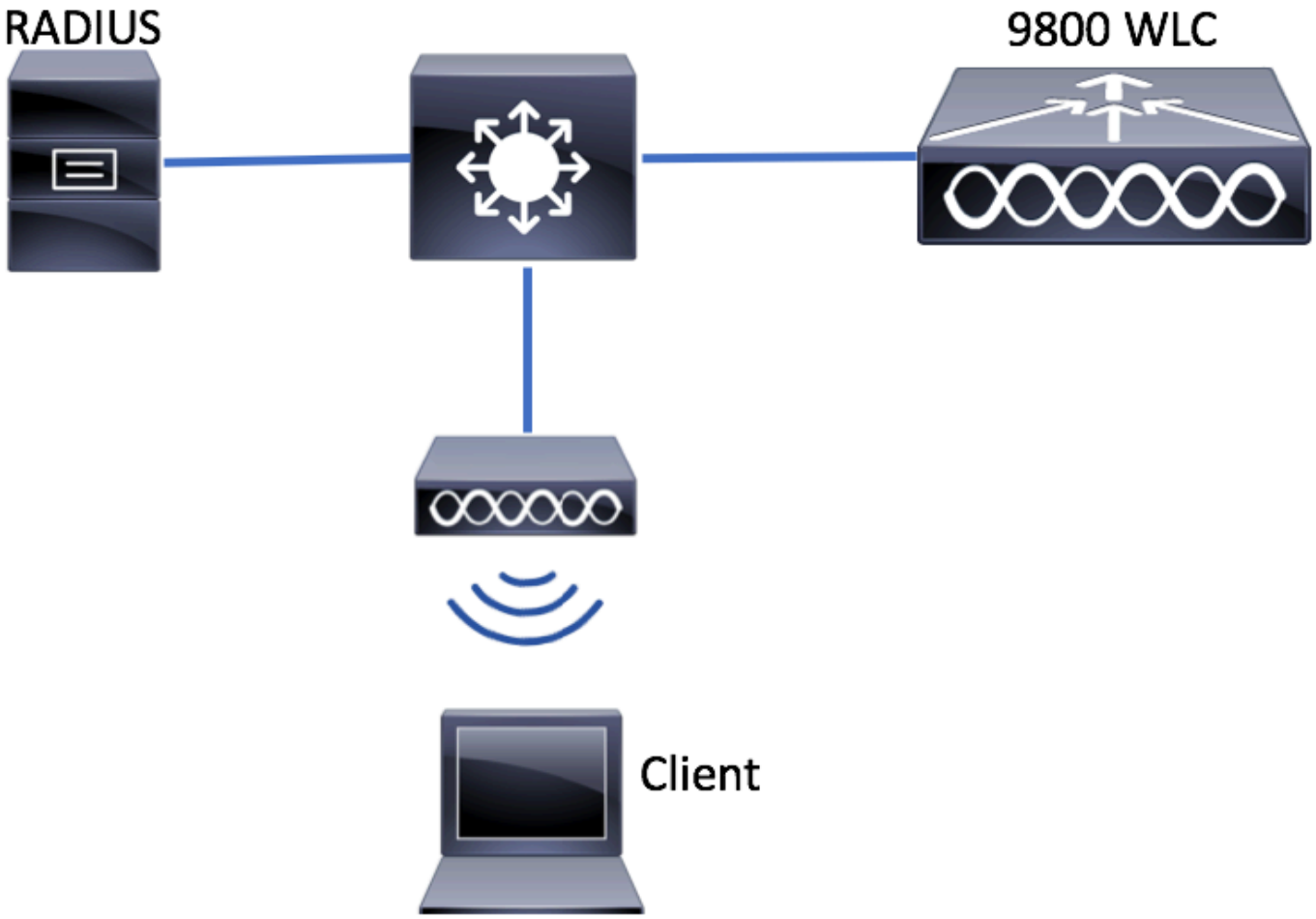
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® XE 지브롤터 v16.12
- ISE v2.2

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



9800 WLC의 AAA 구성

외부 서버로 클라이언트 인증

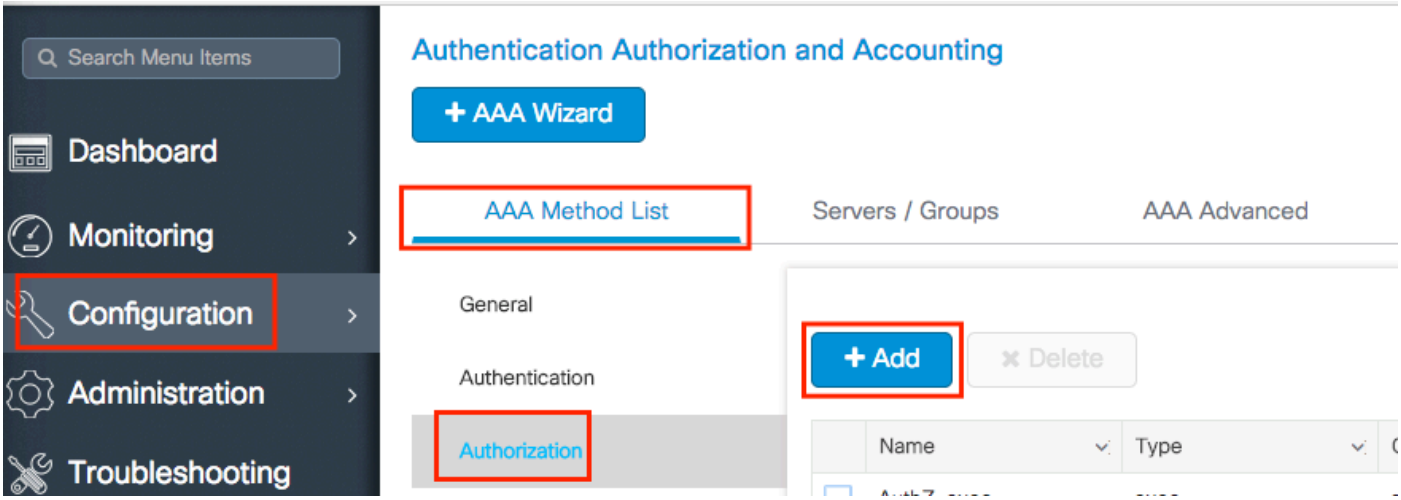
GUI:

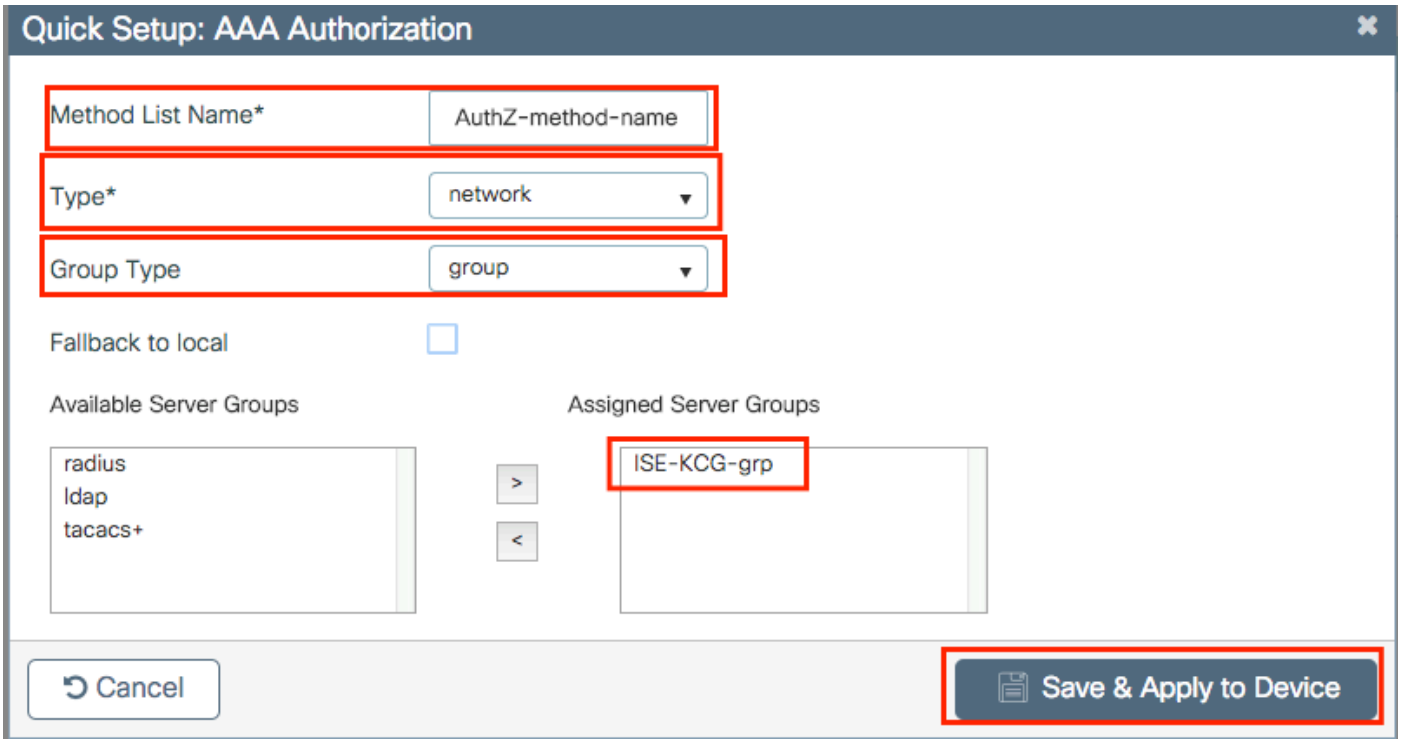
이 링크에서 '9800 WLC에 대한 AAA 컨피그레이션' 섹션의 1-3단계를 읽어보십시오.

9800 Series WLC의 AAA 컨피그레이션

4단계. 권한 부여 네트워크 방법을 만듭니다.

탐색 Configuration > Security > AAA > AAA Method List > Authorization > + Add 만들 수 있습니다.





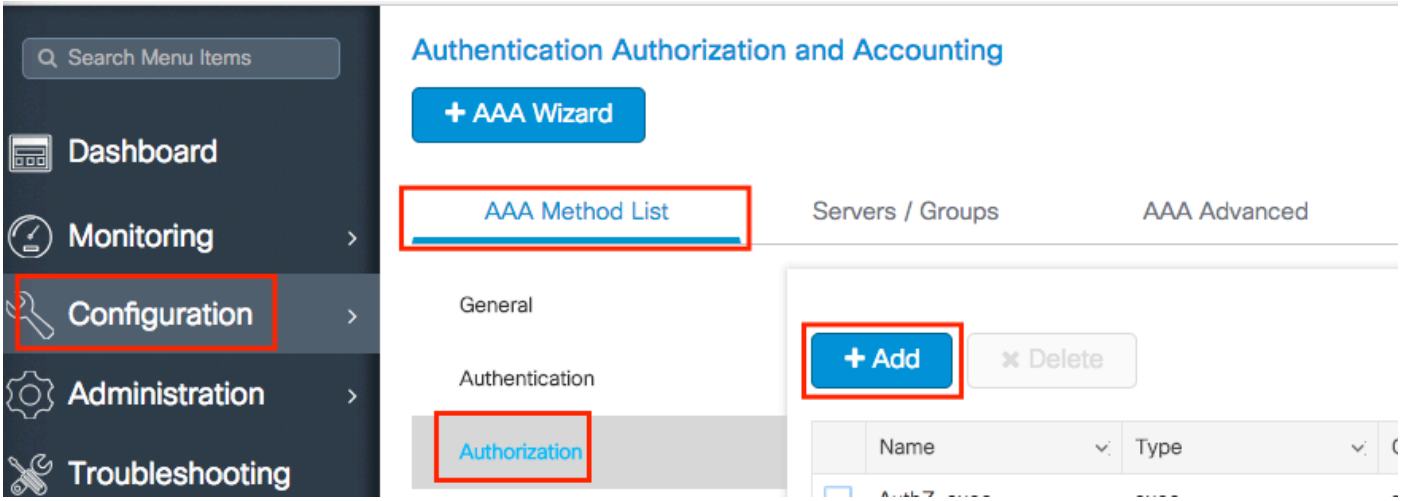
CLI:

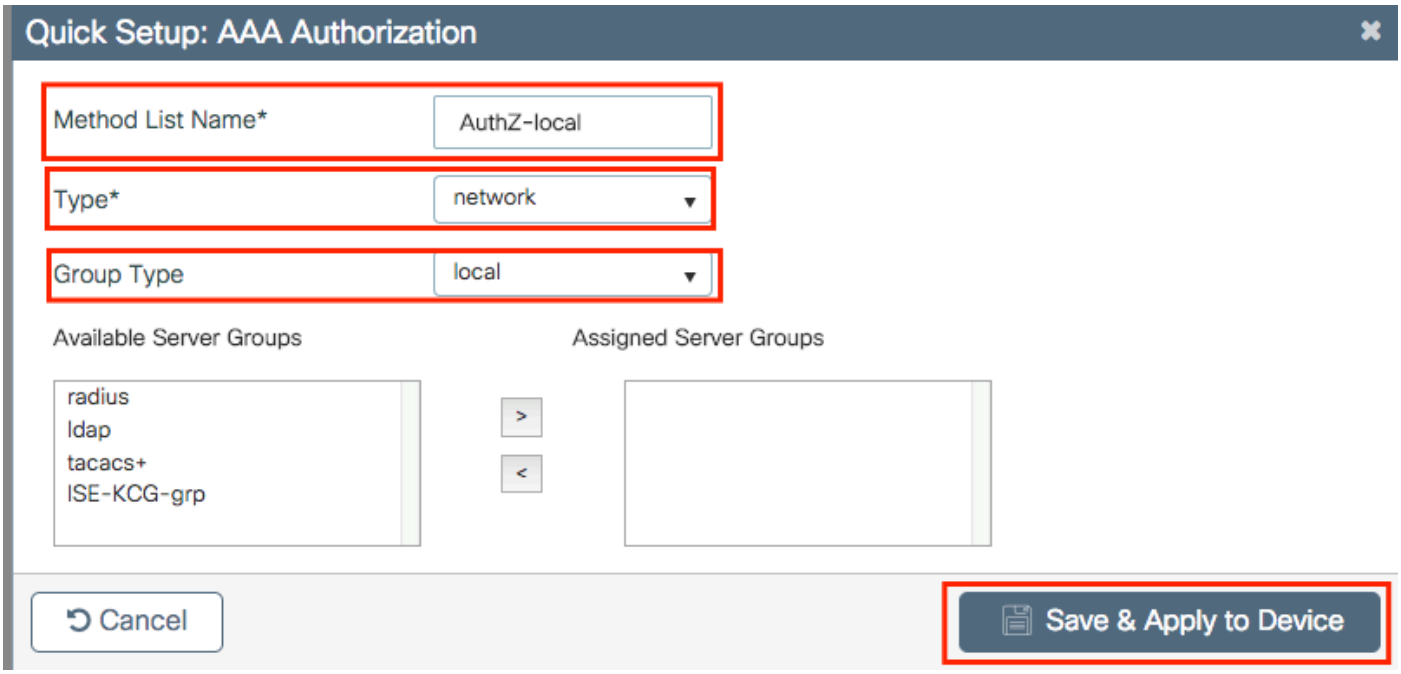
```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authorization network <AuthZ-method-name> group <radius-grp-name>
```

로컬에서 클라이언트 인증

로컬 권한 부여 네트워크 방법을 만듭니다.

탐색 Configuration > Security > AAA > AAA Method List > Authorization > + Add 만들 수 있습니다.





CLI:

```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

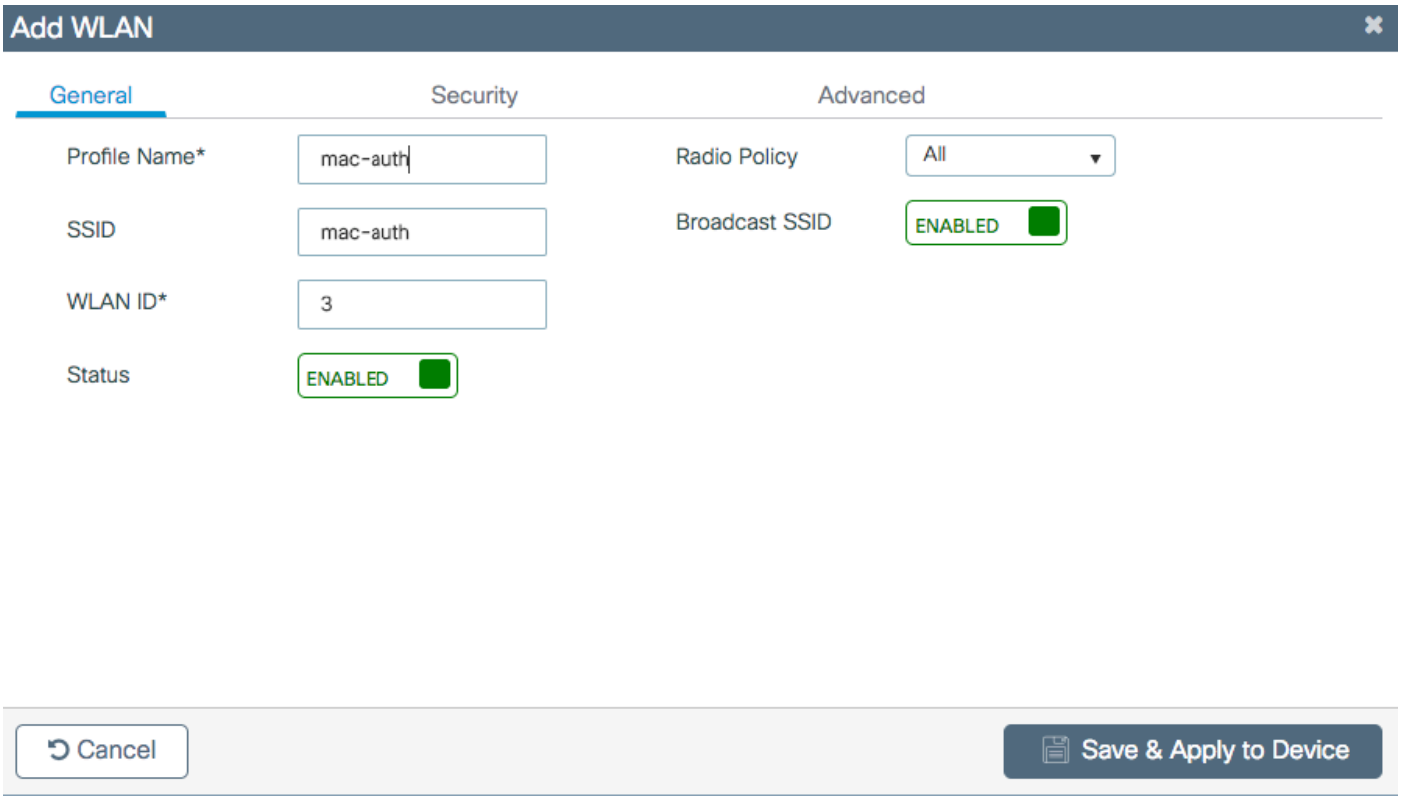
WLAN 구성

GUI:

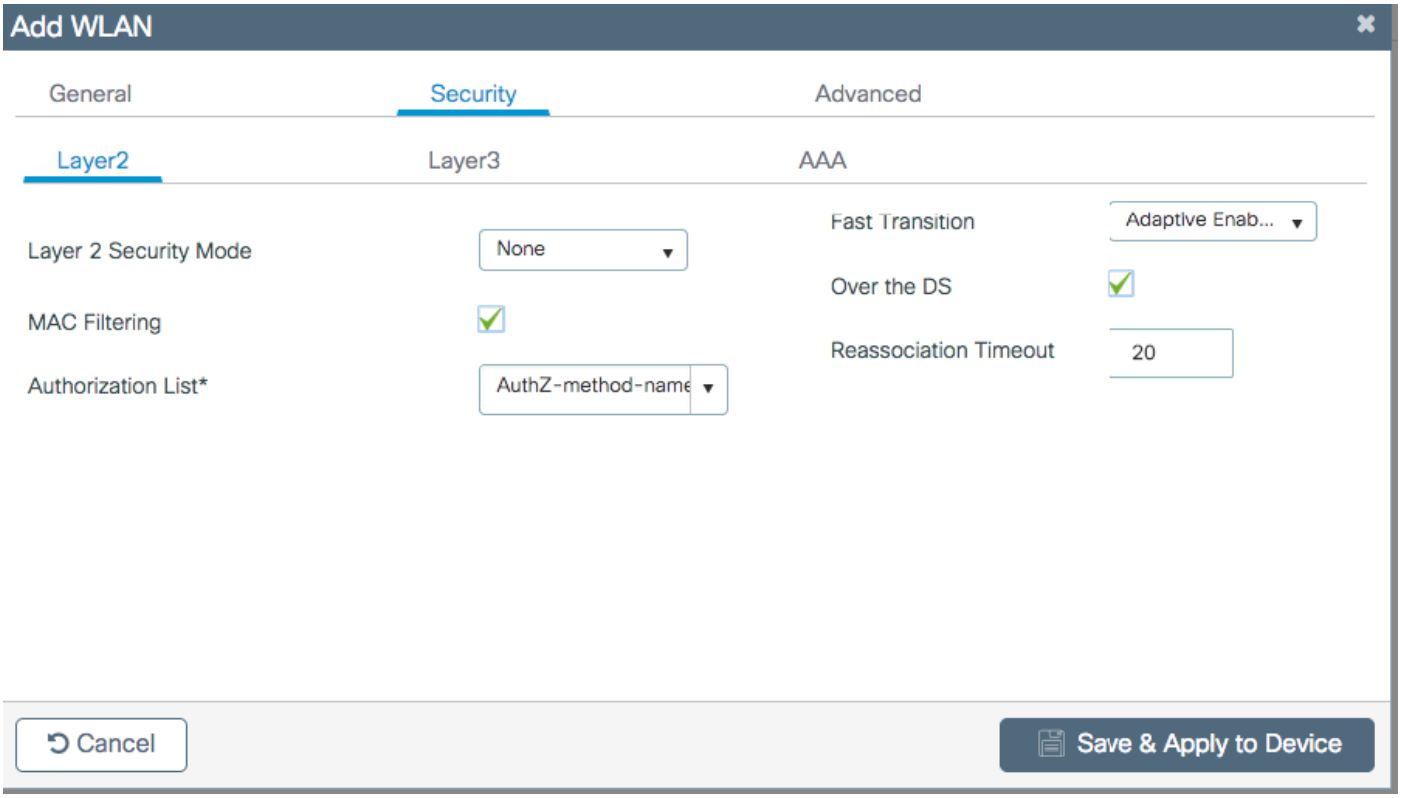
1단계. WLAN을 생성합니다.

탐색 Configuration > Wireless > WLANs > + Add 필요에 따라 네트워크를 구성합니다.

2단계. WLAN 정보를 입력합니다.



3단계. 탐색: Security tab 및 disable Layer 2 Security Mode 및 활성화 MAC Filtering. 발신 Authorization List에서 이전 단계에서 생성한 권한 부여 방법을 선택합니다. 그런 다음 Save & Apply to Device.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

정책 프로파일 구성

다음을 활성화해야 합니다. aaa-override 정책 프로필에서 SSID당 mac-filtering이 제대로 작동하는지 확인합니다.

9800 WLC의 정책 프로파일 컨피그레이션

정책 태그 구성

9800 WLC의 정책 태그

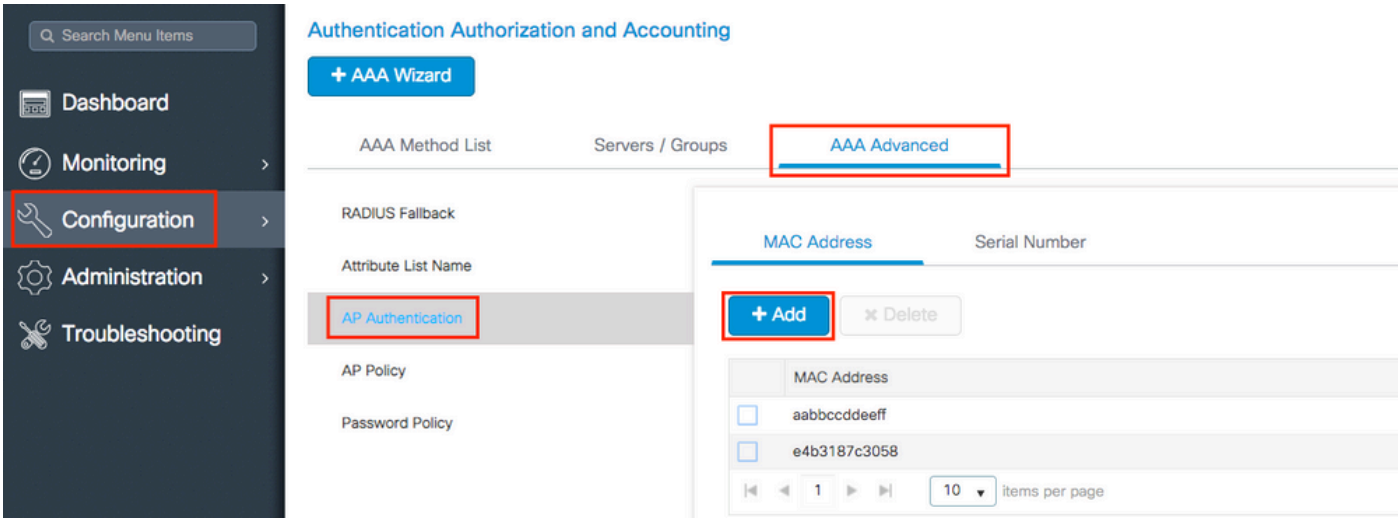
정책 태그 할당

9800 WLC의 정책 태그 할당

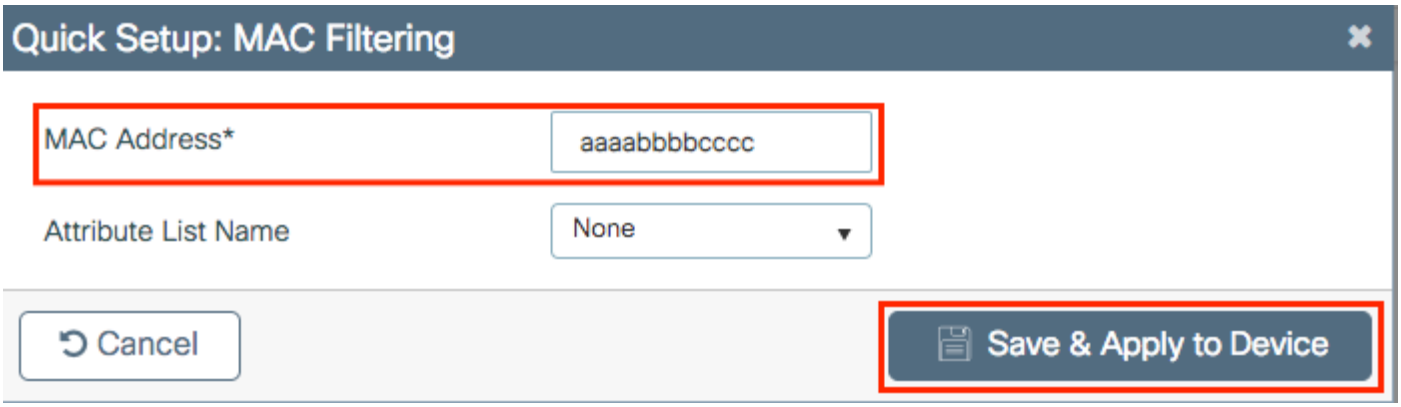
허용된 MAC 주소를 등록합니다.

로컬 인증을 위해 WLC에 MAC 주소를 로컬로 등록

탐색 Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add.



구분 기호 없이 모든 소문자로 mac 주소를 쓰고 Save & Apply to Device.



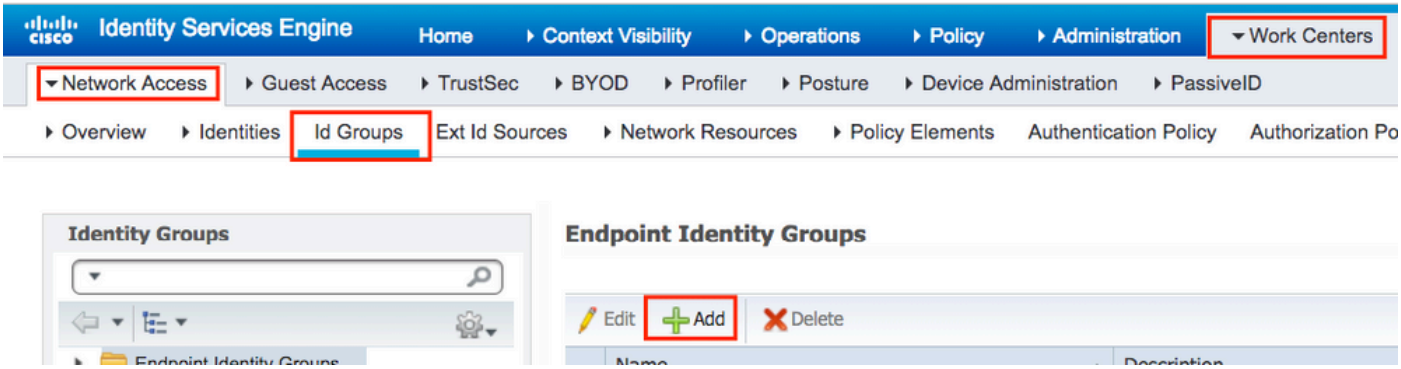
> **참고**: 17.3 이전 버전에서는 웹 UI가 사용자가 입력한 MAC 형식을 그림에 표시된 '구분 기호 없음' 형식으로 변경했습니다. 17.3 이상에서는 웹 UI가 사용자가 입력한 디자인을 존중하므로 구분 기호를 입력하지 않는 것이 중요합니다. 개선 버그 Cisco 버그 ID CSCv43870은 MAC 인증을 위한 여러 형식의 지원을 추적합니다.

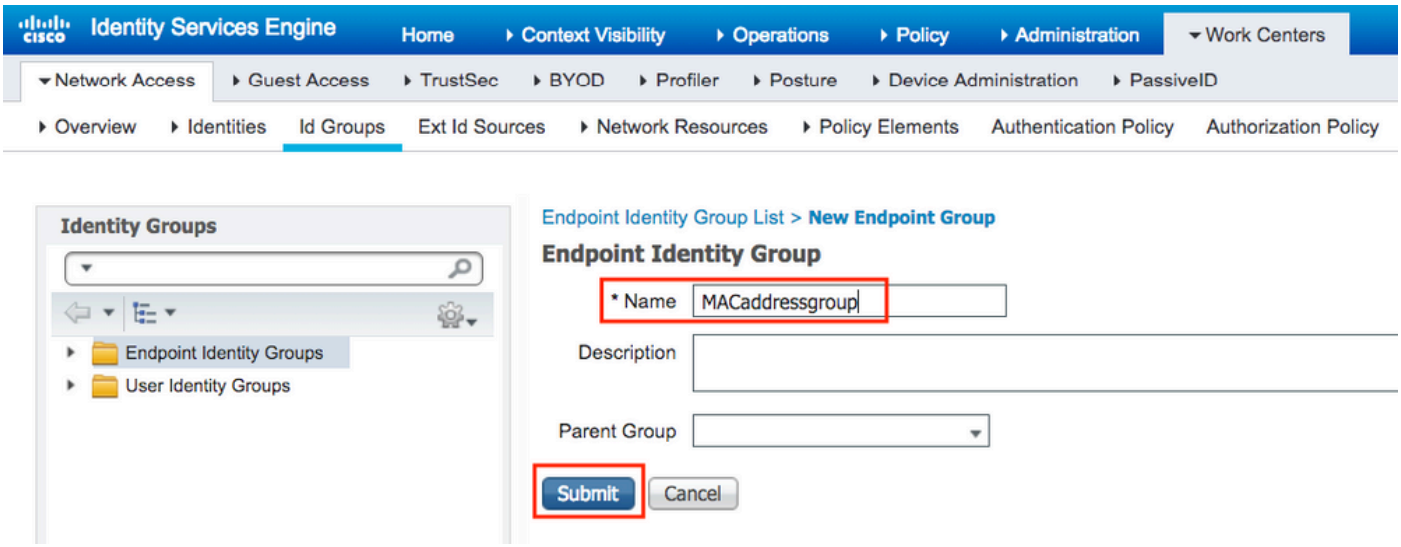
CLI:

```
# config t
# username <aabbccddeeff> mac
```

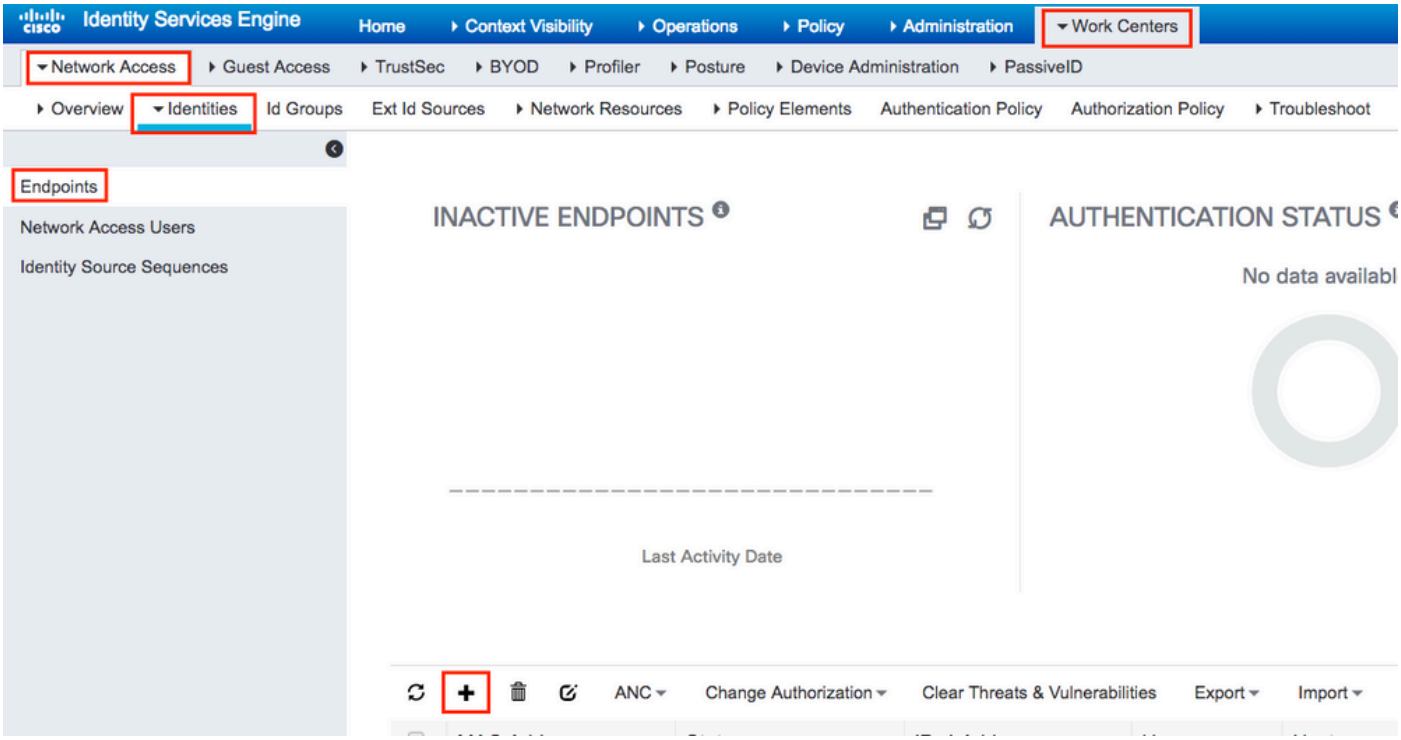
ISE 엔드포인트 데이터베이스의 MAC 주소 입력

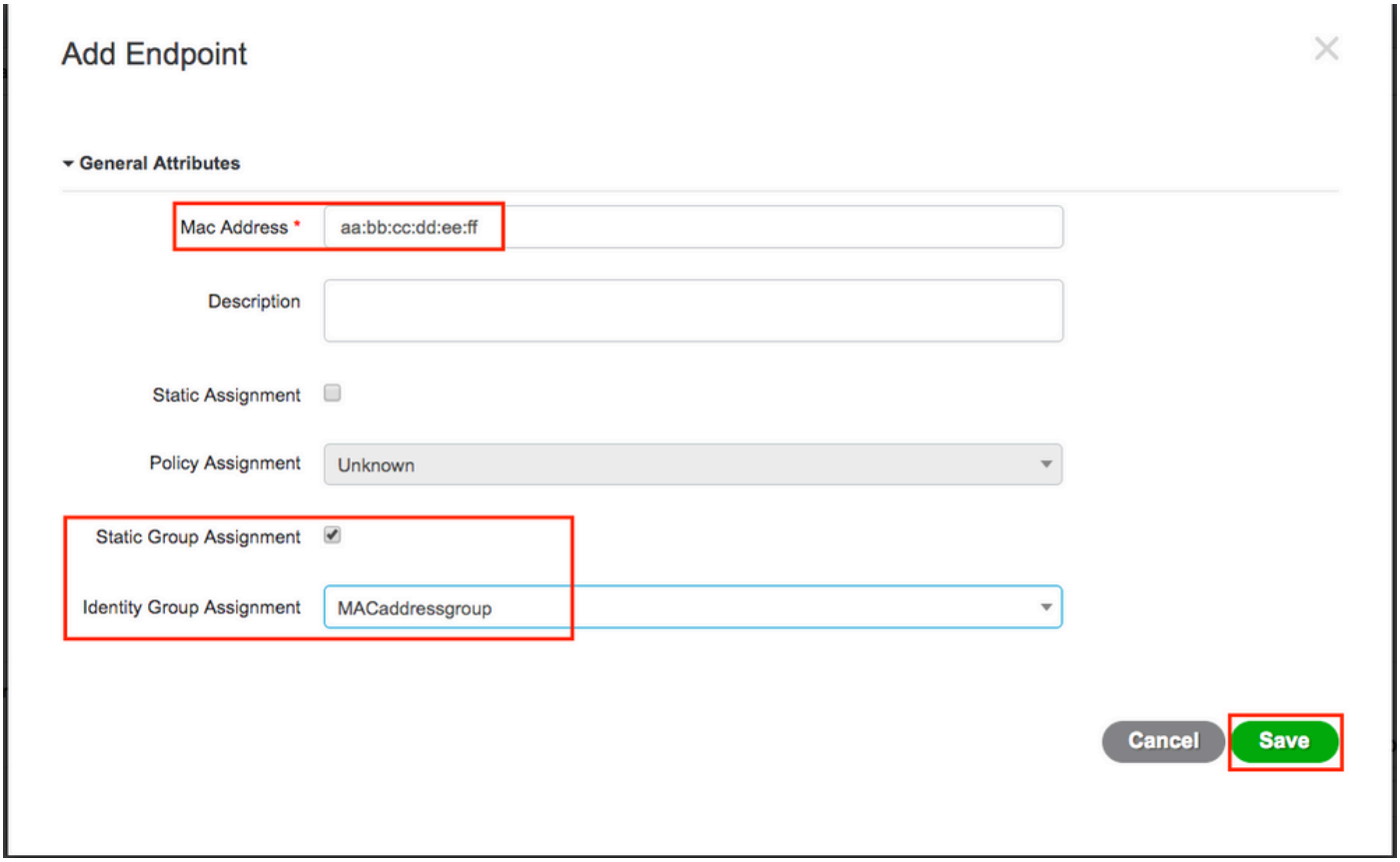
1단계. (선택 사항) 새 엔드포인트 그룹을 생성합니다.
탐색 Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add.





2단계. 탐색 Work Centers > Network Access > Identities > Endpoints > +Add.





ISE 구성

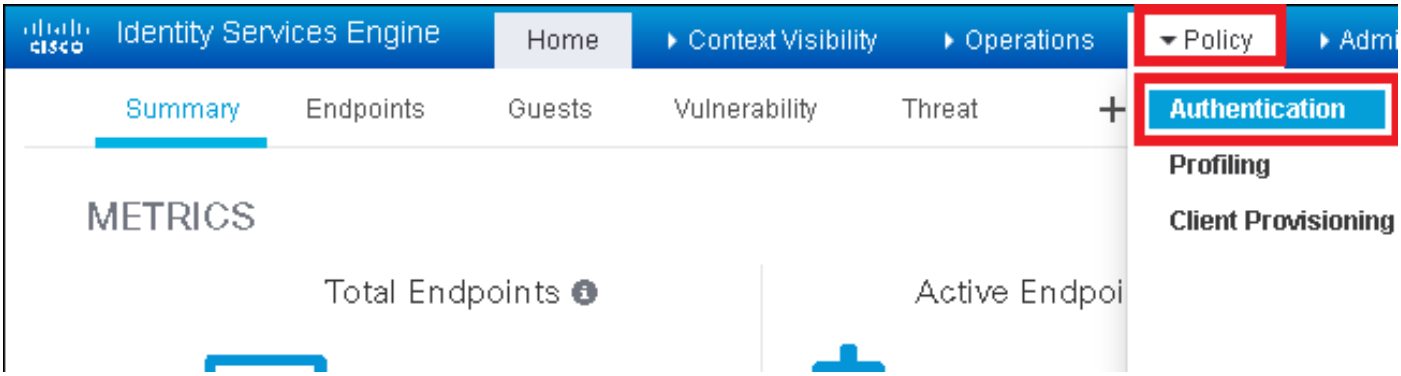
ISE에 9800 WLC 추가.

이 링크의 지침을 읽으십시오. Declare WLC to [ISE(ISE에 WLC 선언)](#) .

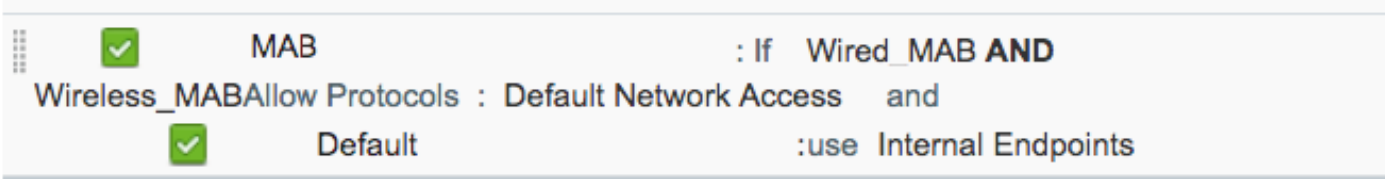
인증 규칙 생성

인증 규칙은 사용자의 자격 증명이 올바른지 확인하고(사용자가 실제로 올바른 사용자인지 확인) 사용자가 사용하도록 허용된 인증 방법을 제한하는 데 사용됩니다.

1단계. 탐색 Policy > Authentication 그림에 표시된 것과 같습니다.
기본 MAB 규칙이 ISE에 있는지 확인합니다.



2단계. MAB에 대한 기본 인증 규칙이 이미 있는지 확인합니다.

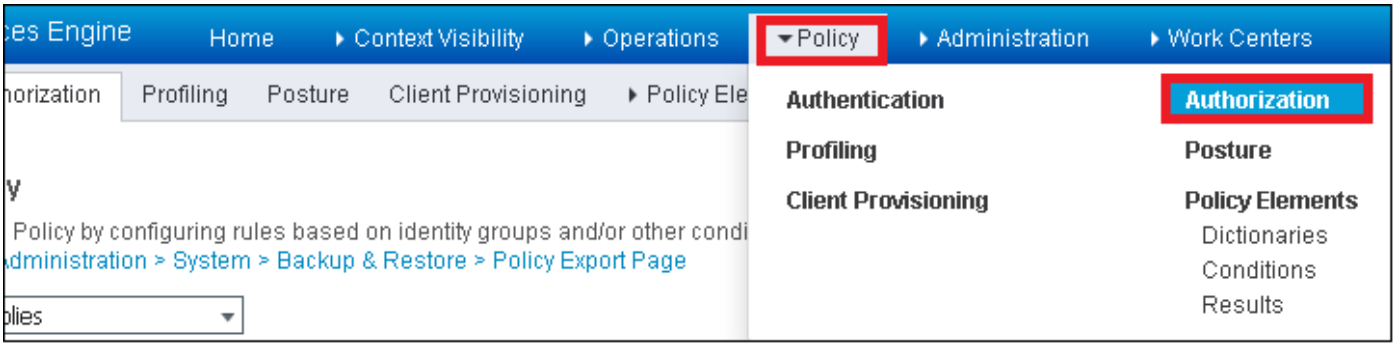


그렇지 않은 경우 를 클릭하면 새 를 추가할 수 있습니다. Insert new row above.

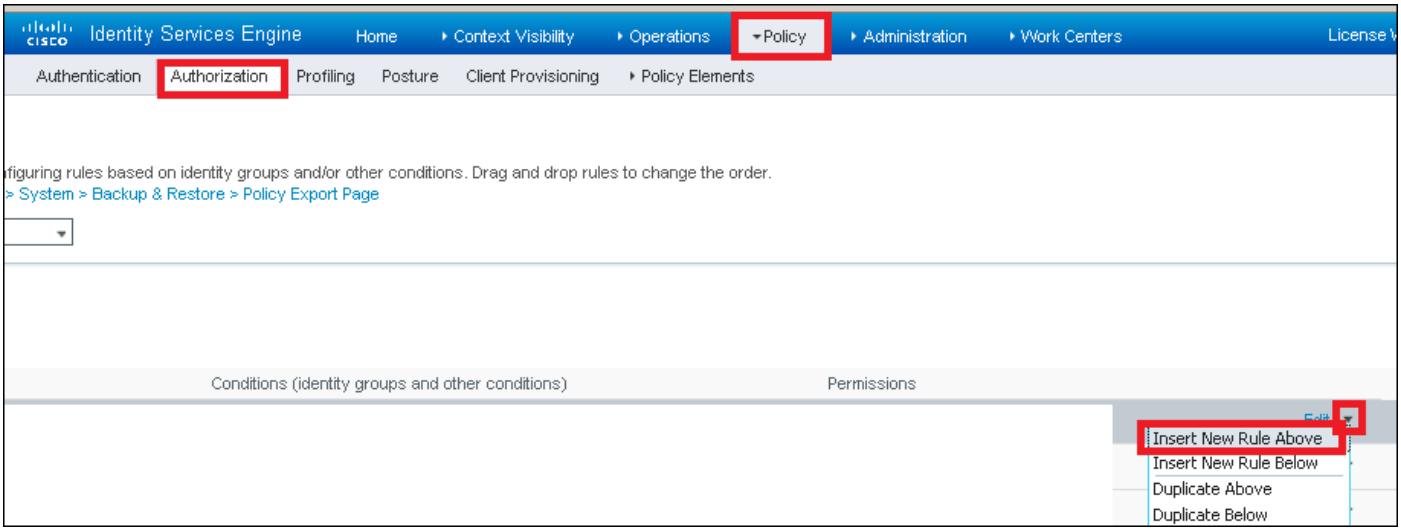
권한 부여 규칙 생성

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

1단계. 탐색 Policy > Authorization 그림에 표시된 것과 같습니다.

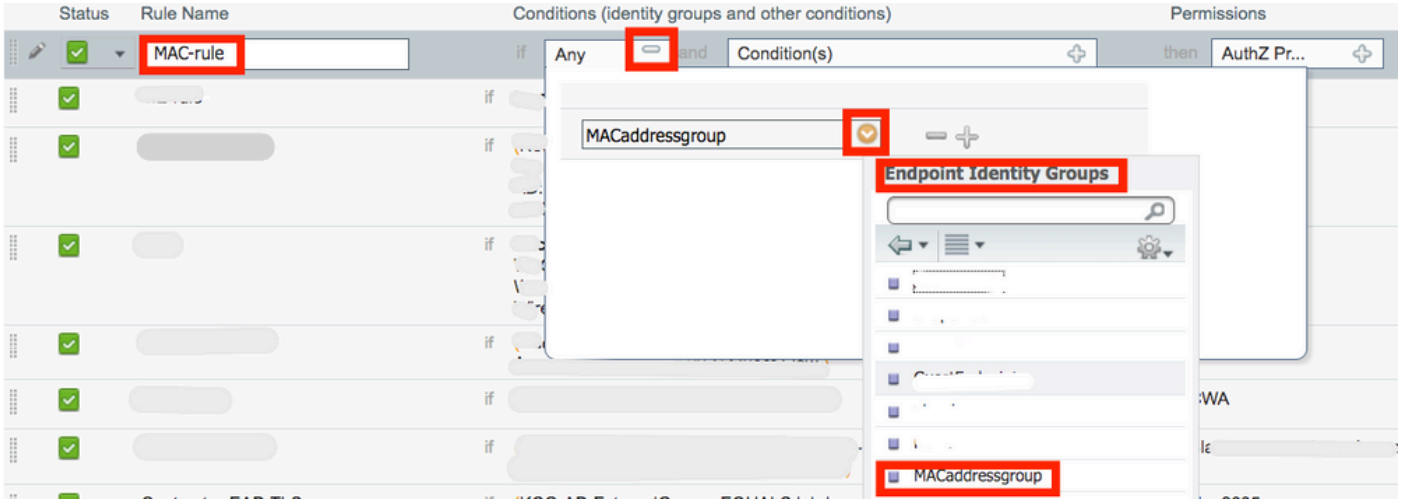


2단계. 이미지에 표시된 대로 새 규칙을 삽입합니다.

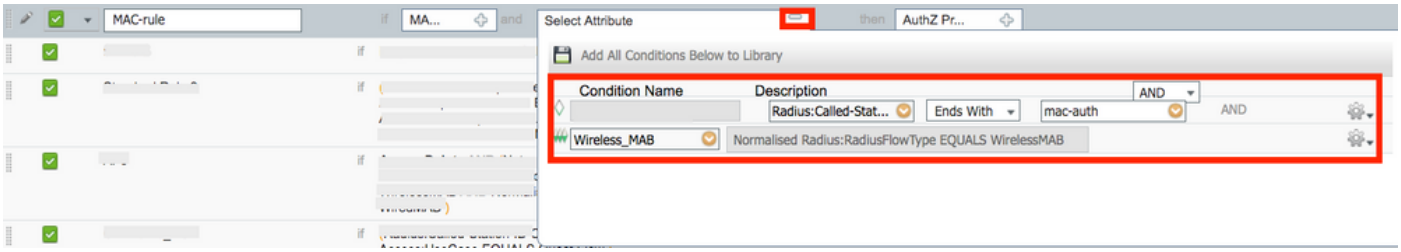


3단계. 값을 입력합니다.

먼저, 엔드 포인트가 저장 되는 ID 그룹 및 규칙의 이름을 선택 합니다.**MACaddressgroup**)를 참조하십시오.



그런 다음 이 규칙에 속하기 위해 권한 부여 프로세스를 수행하는 다른 조건을 선택합니다. 이 예에서는 권한 부여 프로세스가 무선 MAB를 사용하고 해당 호출된 스테이션 ID(SSID의 이름)가 다음으로 끝나는 경우 이 규칙에 도달합니다 mac-auth 그림에 표시된 것과 같습니다.



마지막으로, 할당된 권한 부여 프로파일을 선택합니다(이 경우). PermitAccess 해당 규칙에 도달한 클라이언트에 적용됩니다. 클릭 Done 저장하십시오.

다음을 확인합니다.

이러한 명령을 사용하여 현재 구성을 확인할 수 있습니다:

```
# show wlan { summary | id | name | all }
# 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, 사고 또는 장애 발생 후 상황에 대한 로그를 볼 수 있습니다.

> **참고**: 생성된 로그의 양에 따라 다르지만 몇 시간에서 며칠로 돌아갈 수 있습니다.

기본적으로 9800 WLC가 수집한 추적을 보려면 SSH/텔넷을 통해 9800 WLC에 연결하고 다음 단계를 읽을 수 있습니다(세션을 텍스트 파일에 로깅해야 함).

1단계. 문제가 발생한 시점까지의 로그를 추적할 수 있도록 컨트롤러의 현재 시간을 확인합니다.

```
# show clock
```

2단계. 시스템 컨피그레이션에 따라 컨트롤러 버퍼 또는 외부 syslog에서 syslog를 수집합니다. 이렇게 하면 시스템의 상태 및 오류(있는 경우)를 빠르게 확인할 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**: 조건을 나열하면, 활성화된 조건(mac 주소, IP 주소 등)이 발생하는 모든 프로세스의 디버그 레벨에 추적이 로깅됨을 의미합니다. 이렇게 하면 로그의 볼륨이 증가합니다. 따라서 능동적으로 디버깅하지 않을 때는 모든 조건을 지우는 것이 좋습니다.

4단계. 테스트 중인 MAC 주소가 3단계의 조건으로 나열되지 않은 경우, 특정 MAC 주소에 대한 always-on 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 콘텐츠를 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 활성 추적

Always-on 추적을 통해 조사 중인 문제의 트리거를 확인할 수 있는 충분한 정보가 제공되지 않을 경우, 조건부 디버깅을 활성화하고 RA(Radio Active) 추적을 캡처할 수 있습니다. 그러면 지정된 조건(이 경우 클라이언트 mac 주소)과 상호 작용하는 모든 프로세스에 대해 디버그 레벨 추적을 제공합니다. 조건부 디버깅을 활성화하려면 다음 단계를 읽으십시오.

5단계. 활성화된 디버그 조건이 없는지 확인합니다.

```
# clear platform condition all
```

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

이 명령은 30분(1,800초) 동안 제공된 MAC 주소를 모니터링하기 시작합니다. 선택적으로 이 시간을 최대 2,085,978,494초까지 늘릴 수 있습니다.

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

> **참고:** 한 번에 둘 이상의 클라이언트를 모니터링하려면 debug wireless mac을 실행합니다 mac 주소당 명령입니다.

> **참고**: 모든 것이 나중에 볼 수 있도록 내부적으로 버퍼링되므로 터미널 세션에서 클라이언트 활동의 출력이 표시되지 않습니다.

7단계. 모니터링할 문제나 동작을 재현합니다.

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

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

모니터 시간이 경과하거나 디버그 무선이 중지되면 9800 WLC는 다음과 같은 이름의 로컬 파일을 생성합니다. ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

9단계. MAC 주소 활동의 파일을 수집합니다. 다음 중 하나를 복사하거나 ra trace .log 외부 서버에 연결하거나 화면에 출력을 직접 표시합니다.

RA 추적 파일의 이름을 확인합니다:

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

파일을 외부 서버에 복사:

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

콘텐츠 표시:

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

10단계. 근본 원인이 아직 명확하지 않은 경우 디버그 레벨 로그를 더 자세히 보여주는 내부 로그를 수집합니다. 이미 수집되어 내부적으로 저장된 디버그 로그만 자세히 살펴볼 것이므로 클라이언트를 다시 디버깅할 필요는 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 상당히 방대합니다. 이러한 추적을 분석하도록 Cisco TAC와 협력하십시오.

다음 중 하나를 복사하거나 ra-internal-FILENAME.txt 외부 서버에 연결하거나 화면에 출력을 직접 표시합니다.

파일을 외부 서버에 복사:

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

콘텐츠 표시:

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

11단계. 디버그 조건을 제거합니다.

```
# clear platform condition all
```

참고: 트러블슈팅 세션 후에는 항상 디버그 조건을 제거해야 합니다.

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.