Catalyst 9800 Wireless Controller Series에서 802.1X 인증 구성

목차

소개

이 문서에서는 Cisco Catalyst 9800 Series Wireless Controller에서 802.1X 보안을 사용하여 WLAN을 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 802.1X

사용되는 구성 요소

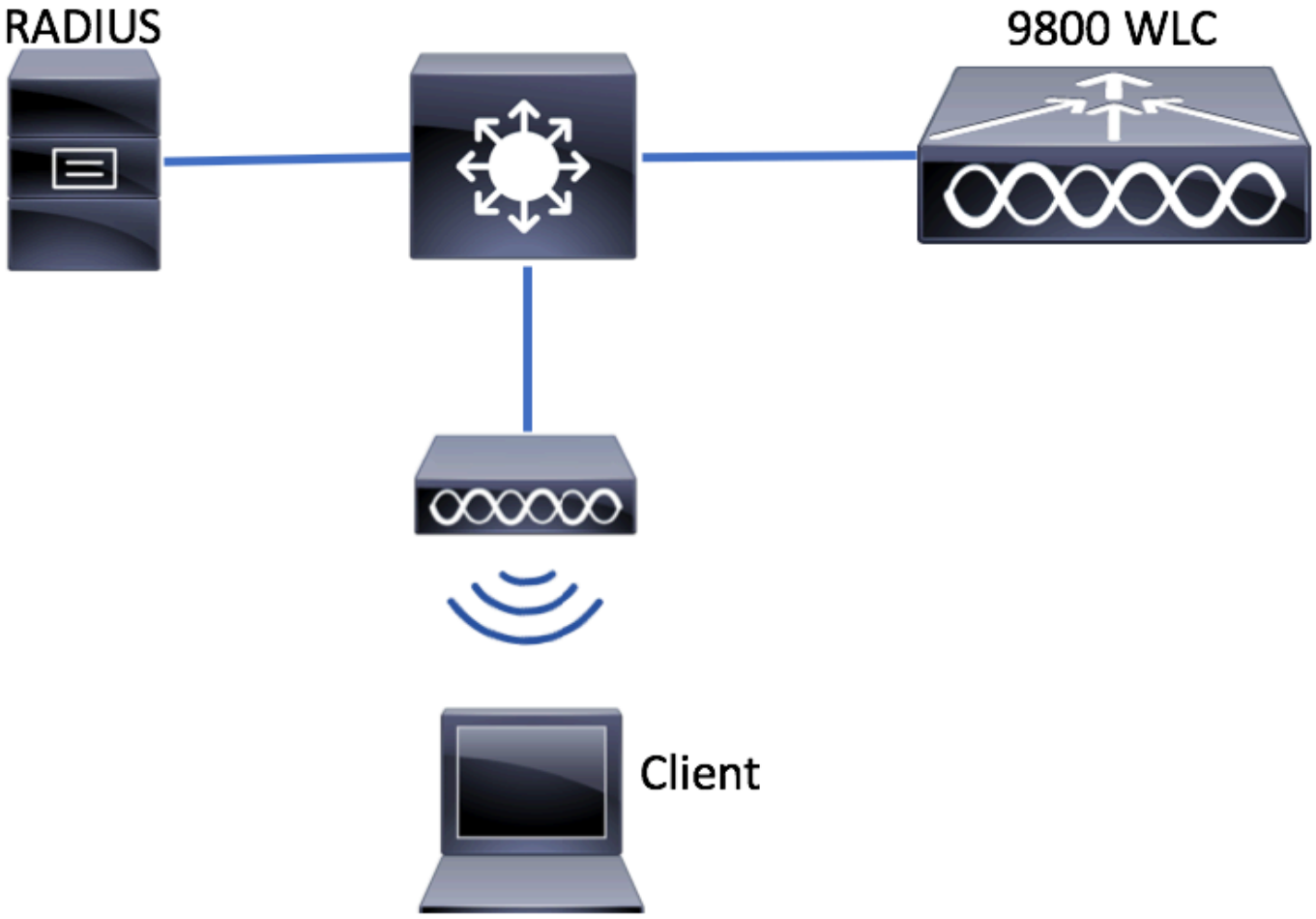
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9800 Wireless Controller Series(Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

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

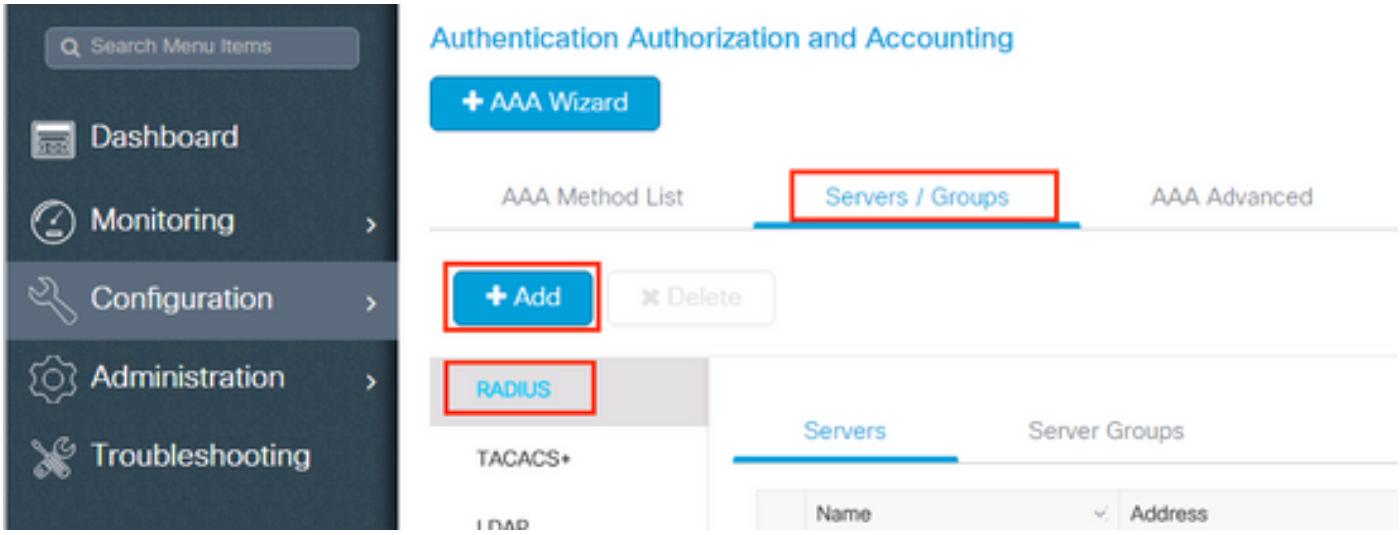


WLC 컨피그레이션

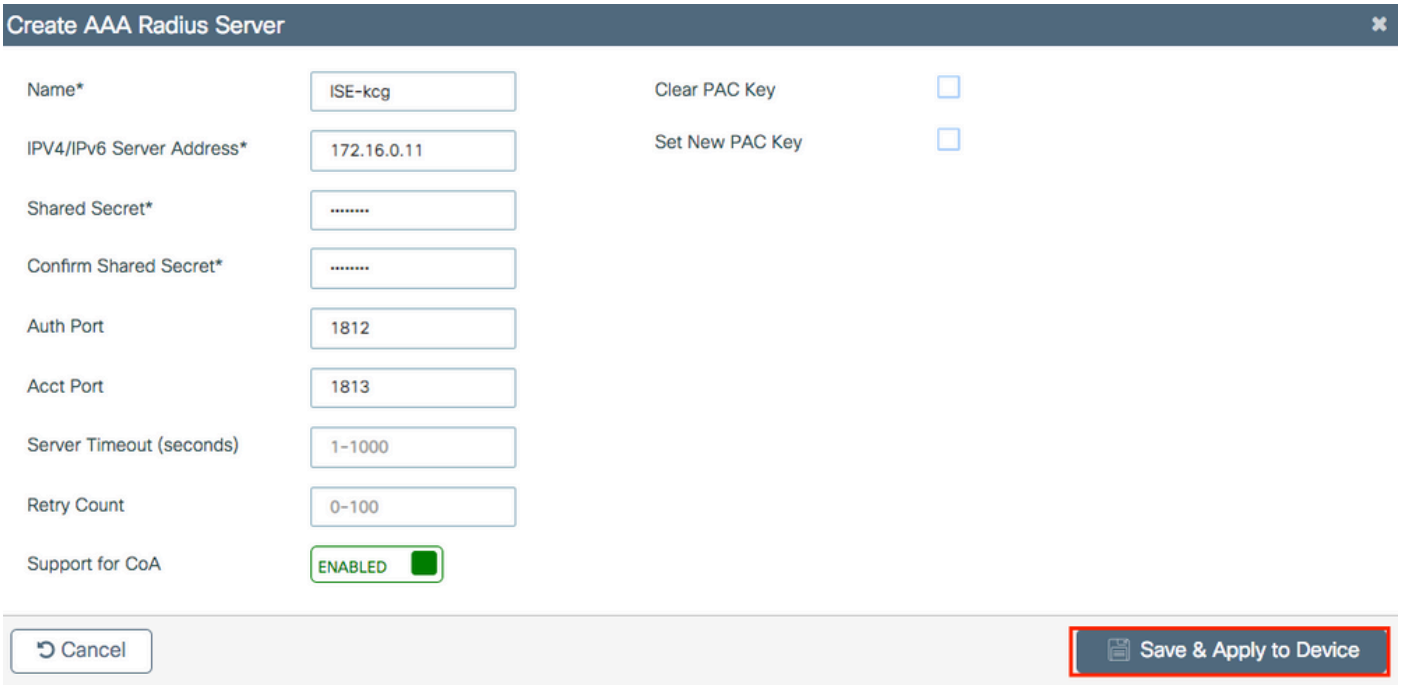
9800 WLC의 AAA 컨피그레이션

GUI:

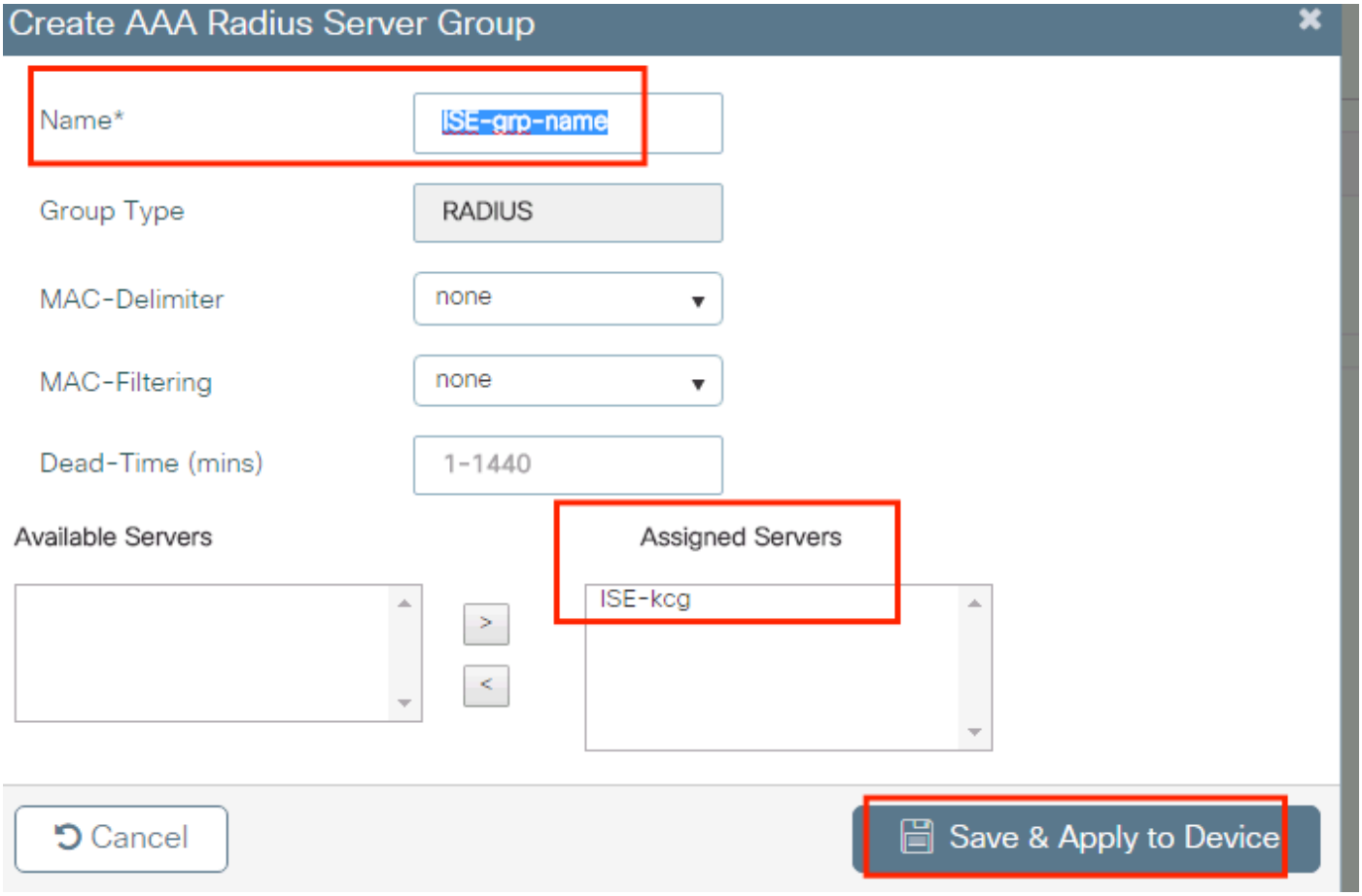
1단계. RADIUS 서버 선언 탐색 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** RADIUS 서버 정보를 입력합니다.



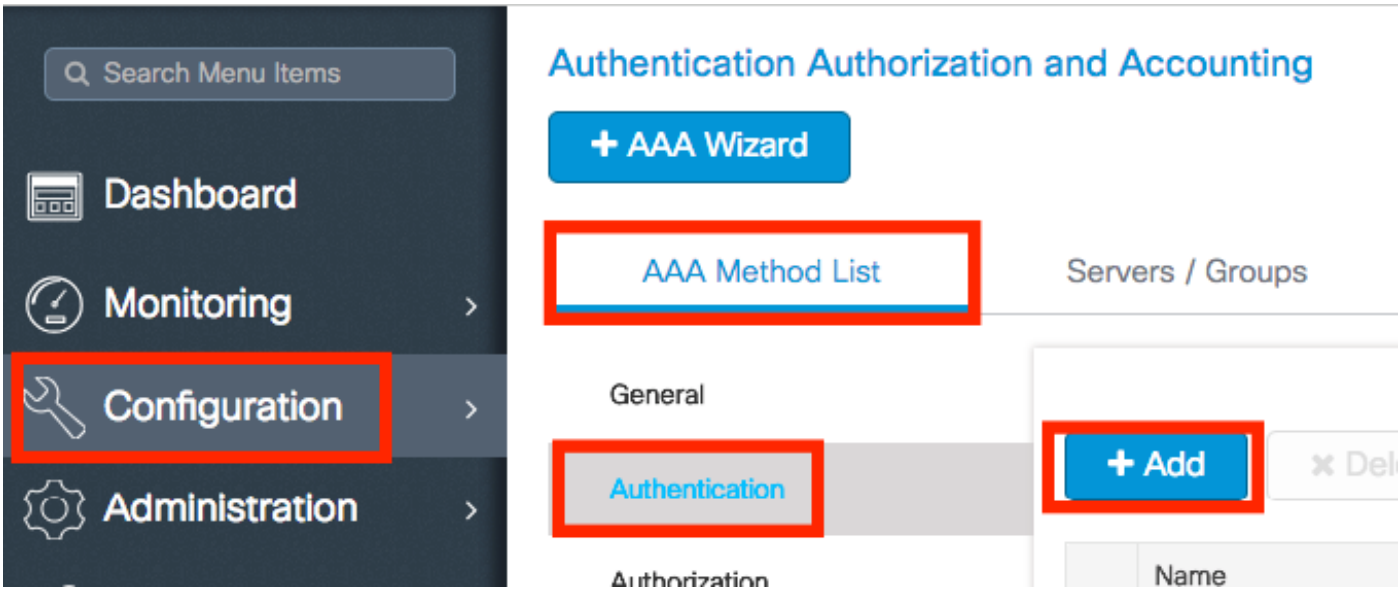
향후 중앙 웹 인증(또는 CoA[Change of Authorization]가 필요한 보안)을 사용하려는 경우 CoA 지원이 활성화되었는지 확인합니다.



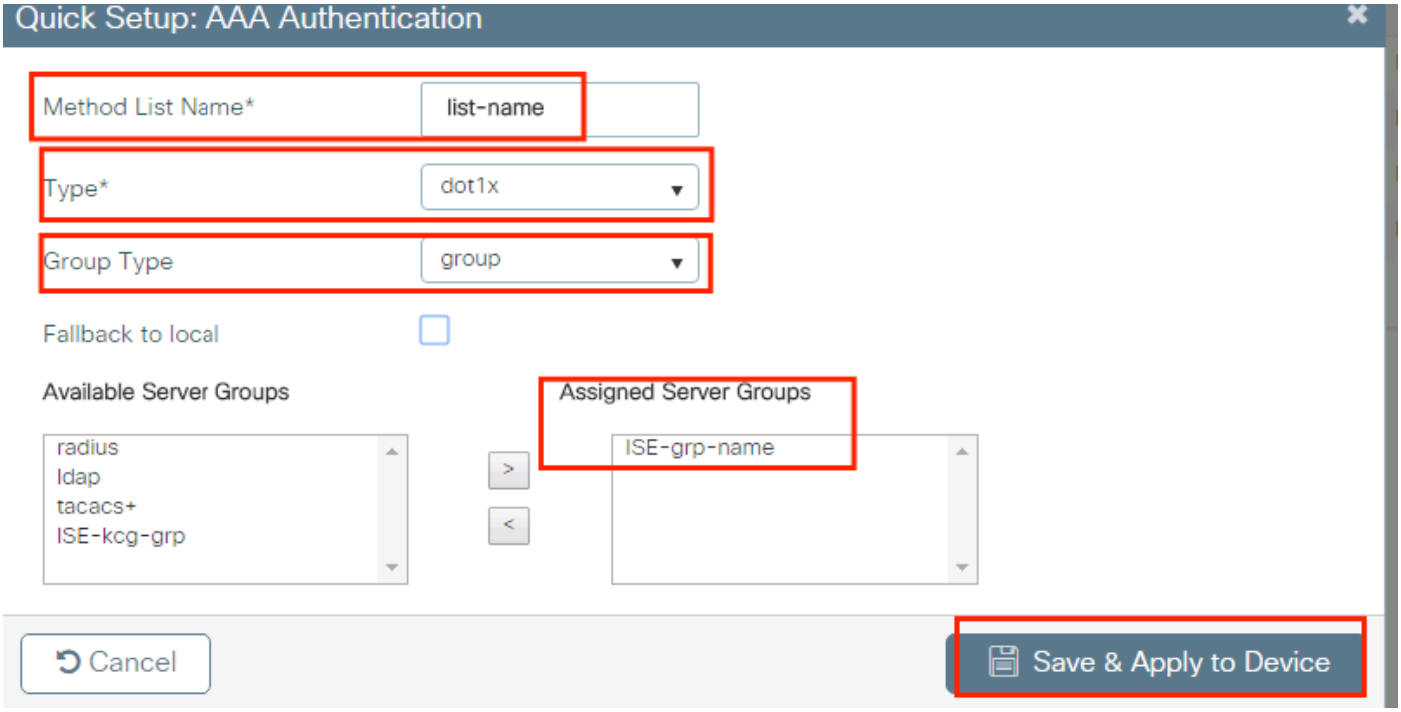
2단계. RADIUS 그룹에 RADIUS 서버를 추가합니다. 탐색 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add.** 그룹의 이름을 지정하고 이전에 만든 서버를 **Assigned Servers**.



3단계. 인증 방법 목록을 만듭니다. 탐색 **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.



다음 정보를 입력합니다.



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 authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

AAA Dead-Server Detection에 대한 참고 사항

RADIUS 서버를 구성한 후 "ALIVE"로 간주되는지 확인할 수 있습니다.

```
#show aaa servers | s WNCD Platform State from WNCD (1) : current UP Platform State from WNCD
(2) : current UP Platform State from WNCD (3) : current UP Platform State from WNCD (4) :
current UP ...
```

다음을 구성할 수 있습니다. **dead criteria**, Firepower Threat Defense **deadtime** WLC에서 특히 여러 RADIUS 서버를 사용하는 경우.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

참고: **dead criteria** 은 RADIUS 서버를 dead로 표시하는 데 사용되는 기준입니다. 1. 컨트롤러가 RADIUS 서버에서 유효한 패킷을 마지막으로 수신한 시간부터 서버가 Dead로 표시된 시간까지 경과해야 하는 시간을 나타내는 시간 제한(초)입니다. 2 . RADIUS 서버가 dead로 표시되

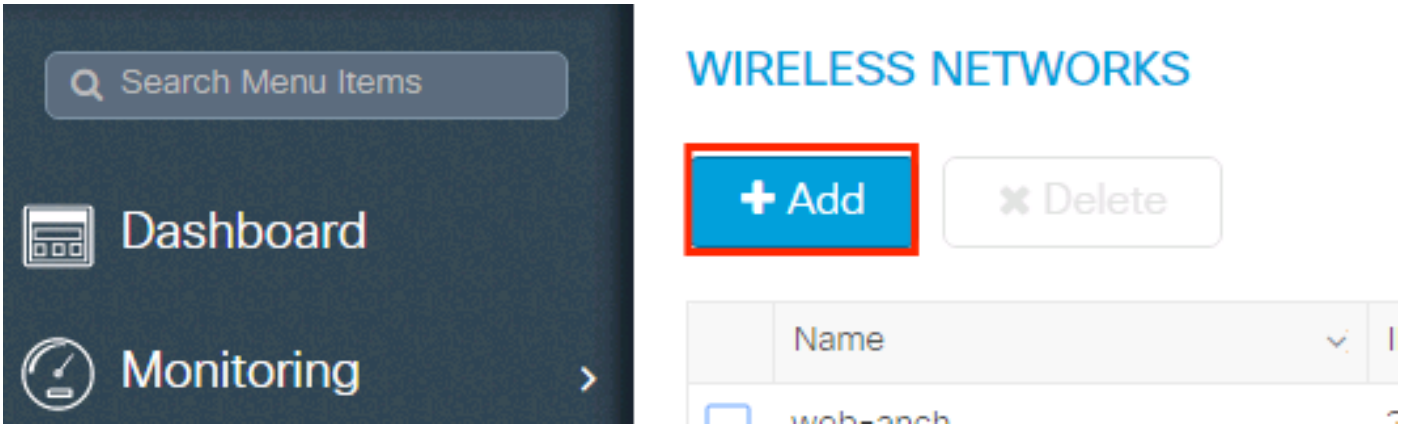
기 전에 컨트롤러에서 발생해야 하는 연속 시간 초과 횟수를 나타내는 카운터.

참고: **deadtime** dead-criteria에서 서버를 dead로 표시한 후 서버가 dead 상태로 유지되는 시간(분)을 지정합니다. 데드타임이 만료되면 컨트롤러는 서버를 UP(ALIVE)로 표시하고 등록된 클라이언트에 상태 변경 사항을 알립니다. 상태가 UP로 표시된 후에도 서버에 계속 연결할 수 없고 dead 기준이 충족되면 dead 시간 간격 동안 서버가 다시 dead로 표시됩니다.

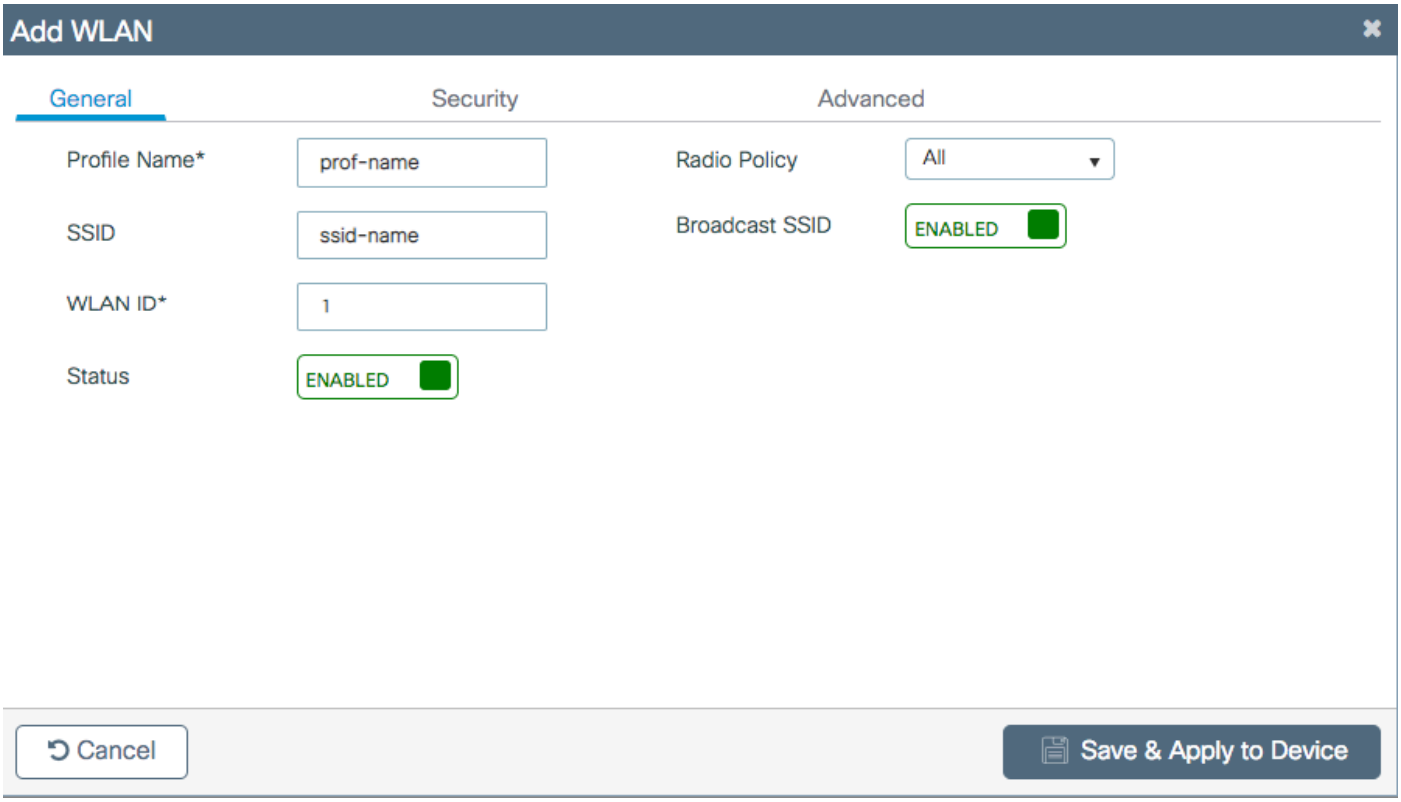
WLAN 프로파일 컨피그레이션

GUI:

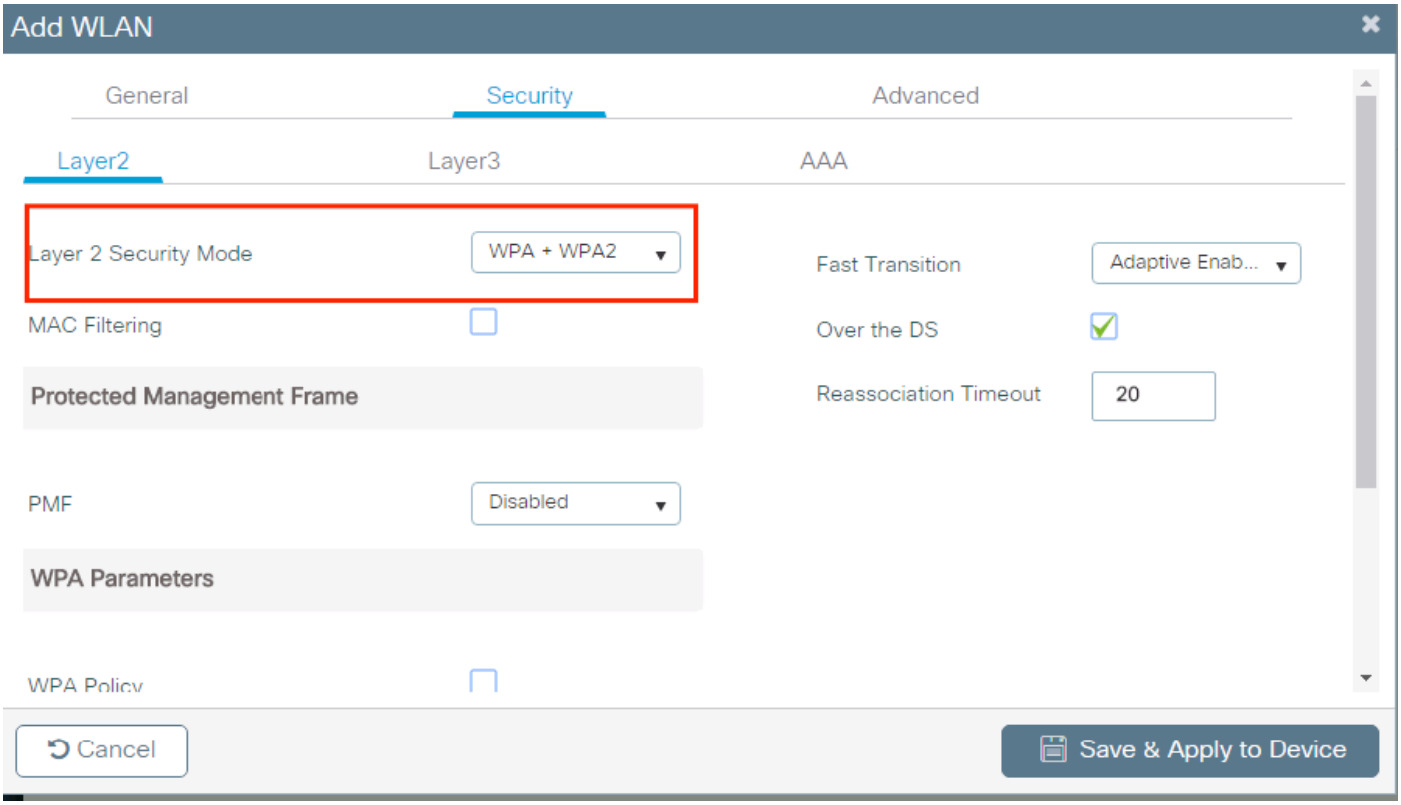
1단계. WLAN을 생성합니다. Configuration(컨피그레이션) **> Wireless(무선) > WLANs(WLANs) > + Add(추가)**로 이동하여 필요에 따라 네트워크를 구성합니다.

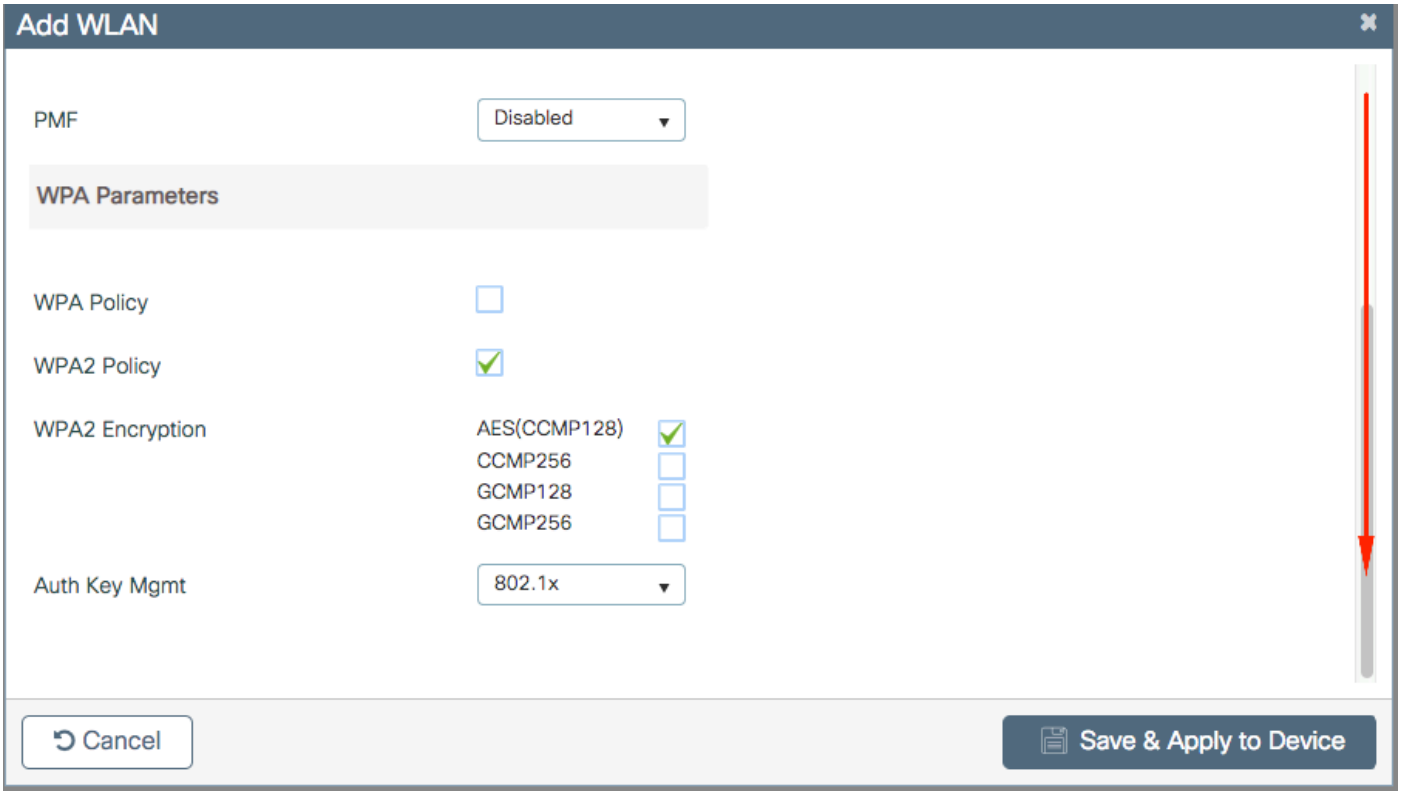


2단계. WLAN 정보를 입력합니다

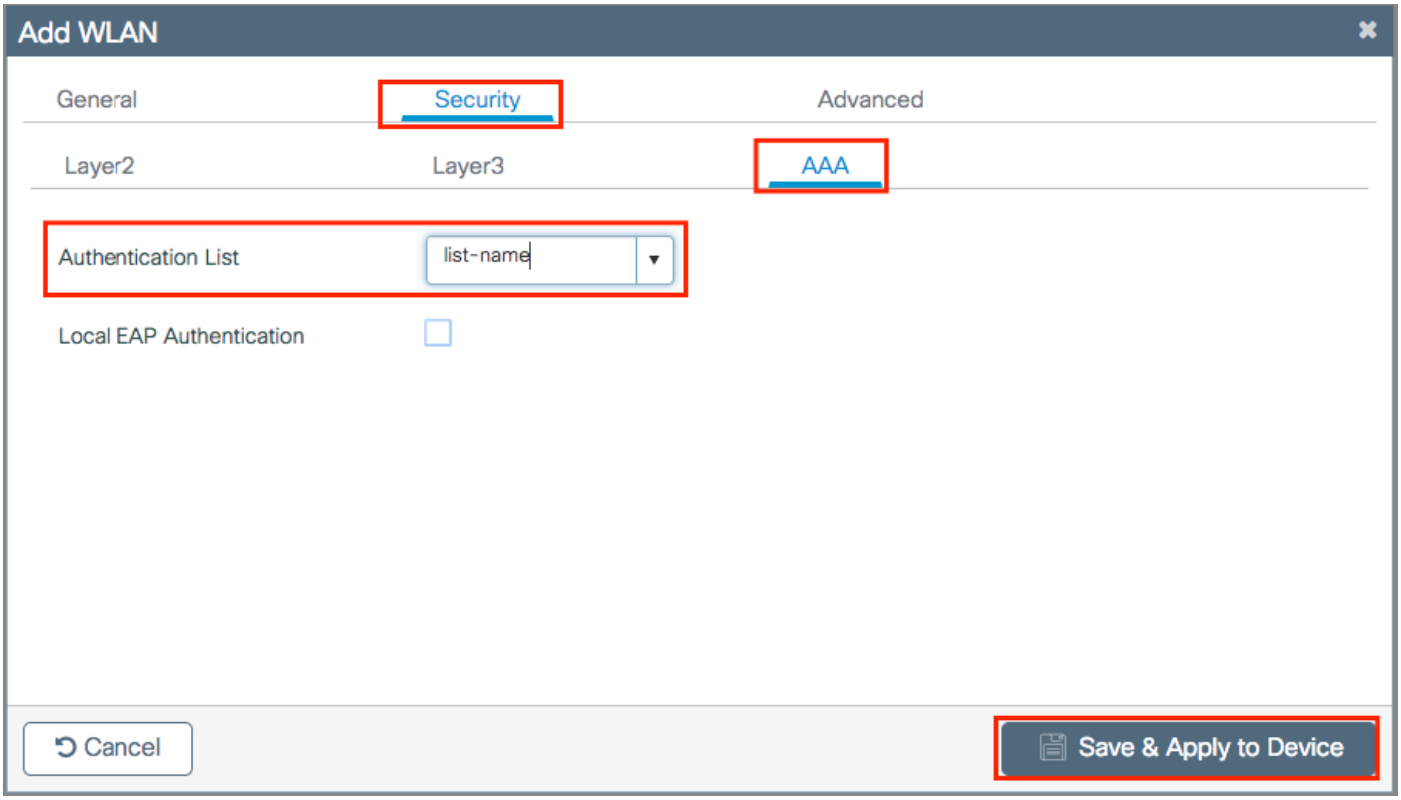


3단계. 탐색: **Security(보안)** 탭에서 필요한 보안 방법을 선택합니다. 이 경우 **WPA2 + 802.1x**.





4단계. 에서 **Security > AAA** 탭에서 AAA Configuration on 9800 WLC(9800 WLC의 AAA 컨피그레이션) 섹션에서 3단계에 생성된 인증 방법을 선택합니다.



CLI:

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

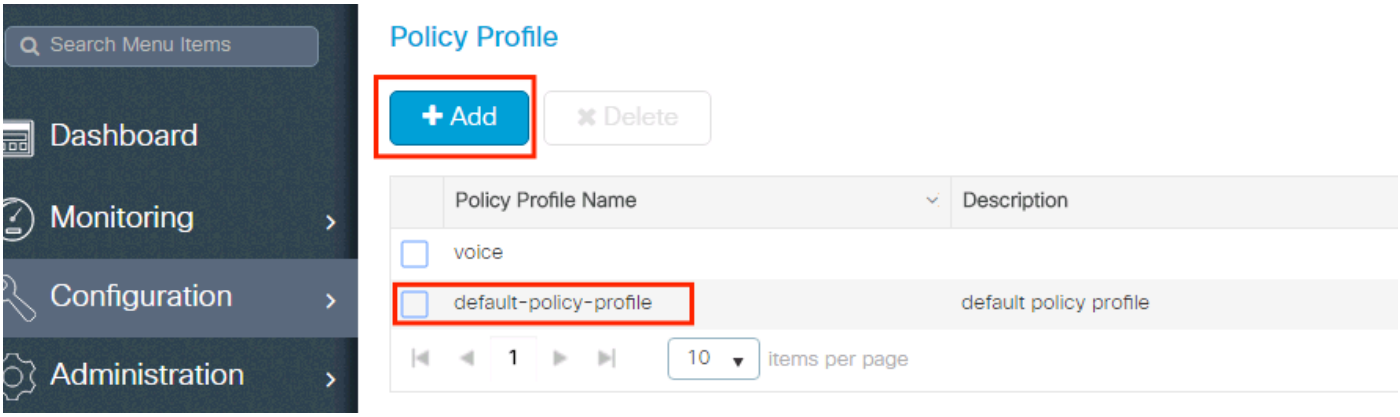
정책 프로파일 구성

정책 프로필 내에서 클라이언트를 할당할 VLAN을 결정할 수 있습니다. ACL(Access Controls List), QoS(Quality of Service), Mobility Anchor, Timers 등과 같은 다른 설정을 지정할 수 있습니다.

기본 정책 프로필을 사용하거나 새 프로필을 생성할 수 있습니다.

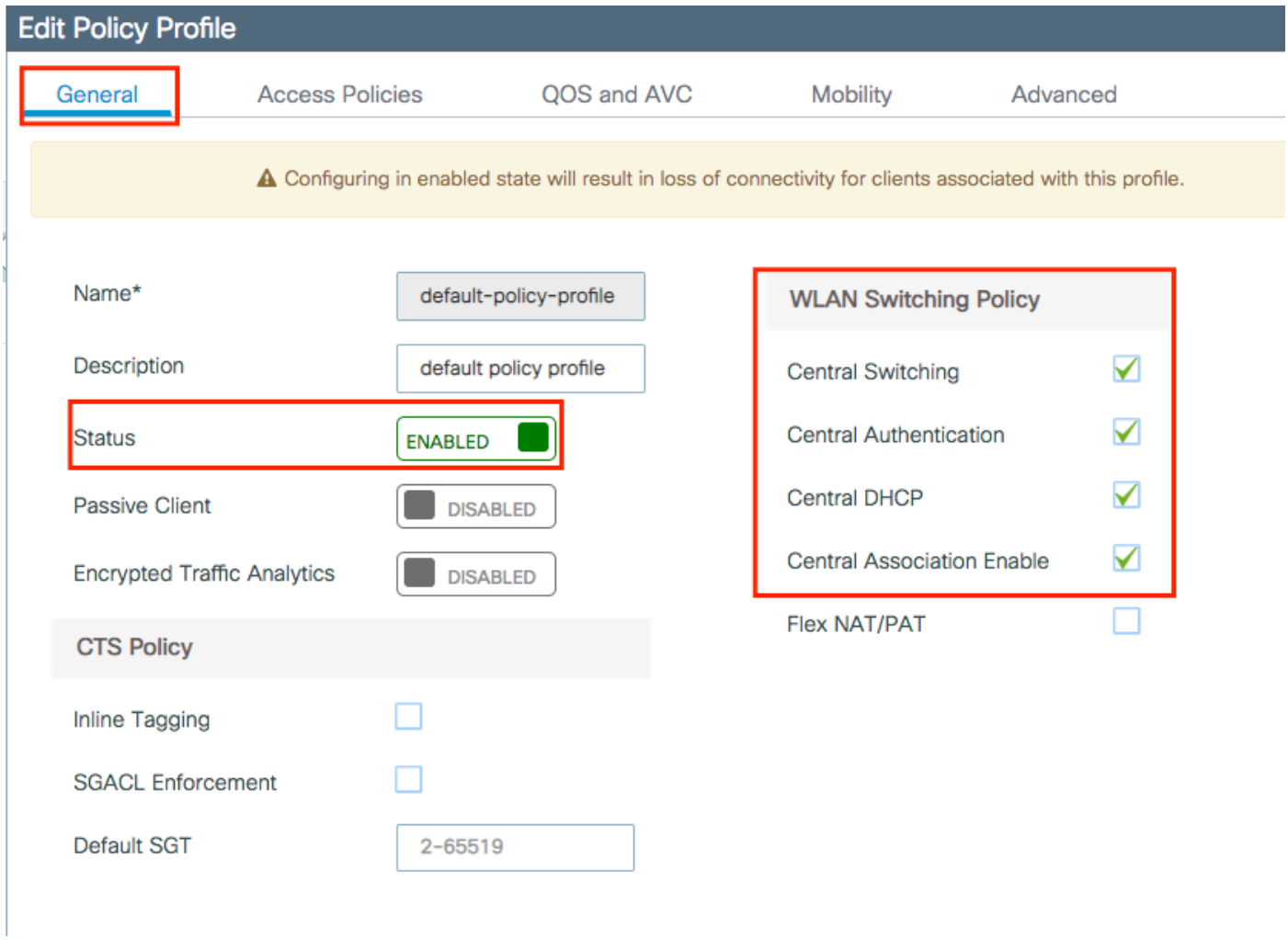
GUI:

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

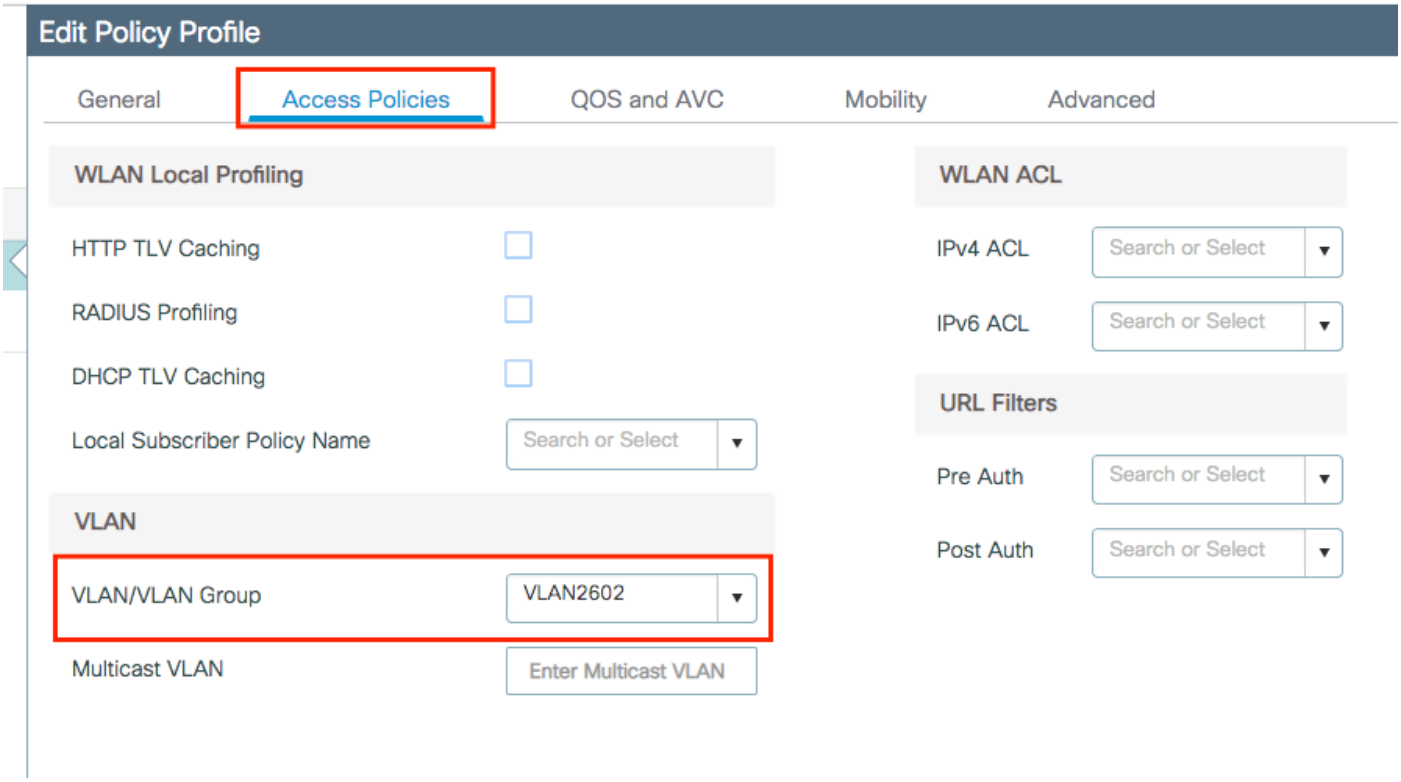


프로파일이 활성화되어야 합니다.

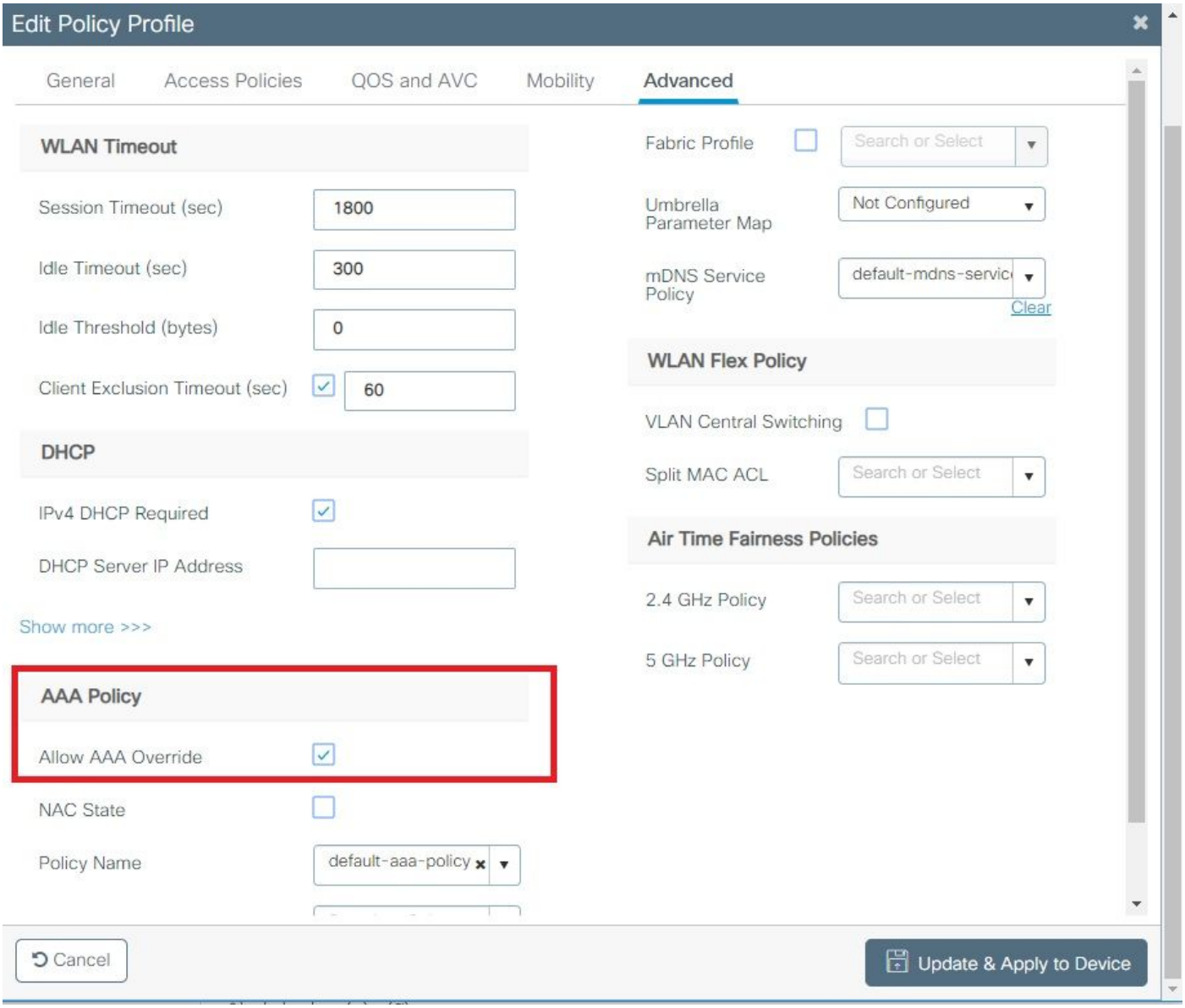
또한 액세스 포인트(AP)가 로컬 모드인 경우 정책 프로필에 **중앙 스위칭** 및 **중앙 인증**이 활성화되어 **있는지** 확인합니다.



Access Policies(액세스 정책) 탭에서 클라이언트를 할당해야 하는 **VLAN을** 선택합니다.



ISE가 VLAN 할당과 같은 Access-Accept에서 특성을 반환하도록 하려면 **Advanced** 탭:



CLI:

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

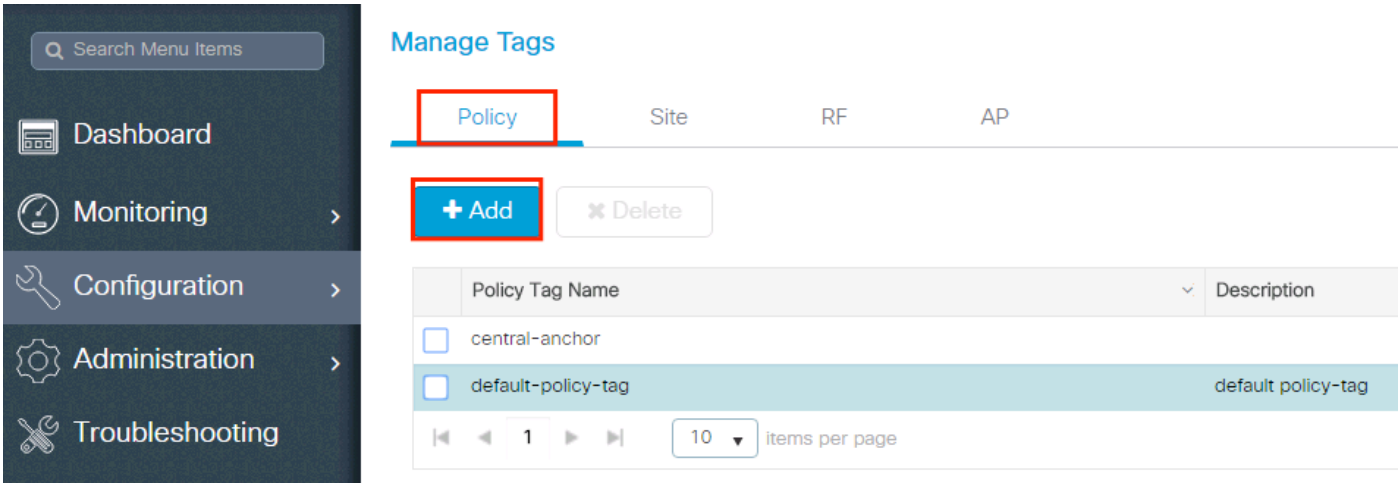
정책 태그 구성

정책 태그는 SSID를 정책 프로파일과 연결하는 데 사용됩니다. 새 정책 태그를 생성하거나 default-policy 태그를 사용할 수 있습니다.

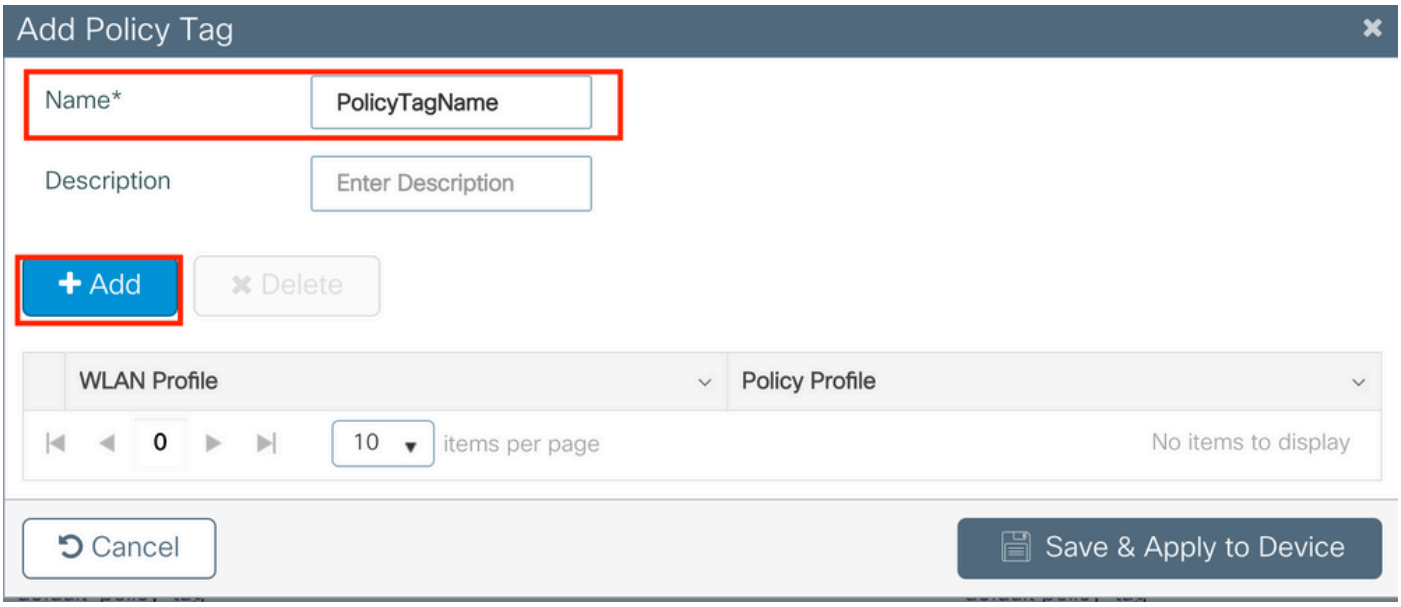
> **참고**: default-policy-tag는 WLAN ID가 1~16인 SSID를 default-policy-profile에 자동으로 매핑합니다. 수정하거나 삭제할 수 없습니다. ID가 17 이상인 WLAN이 있는 경우 default-policy-tag를 사용할 수 없습니다.

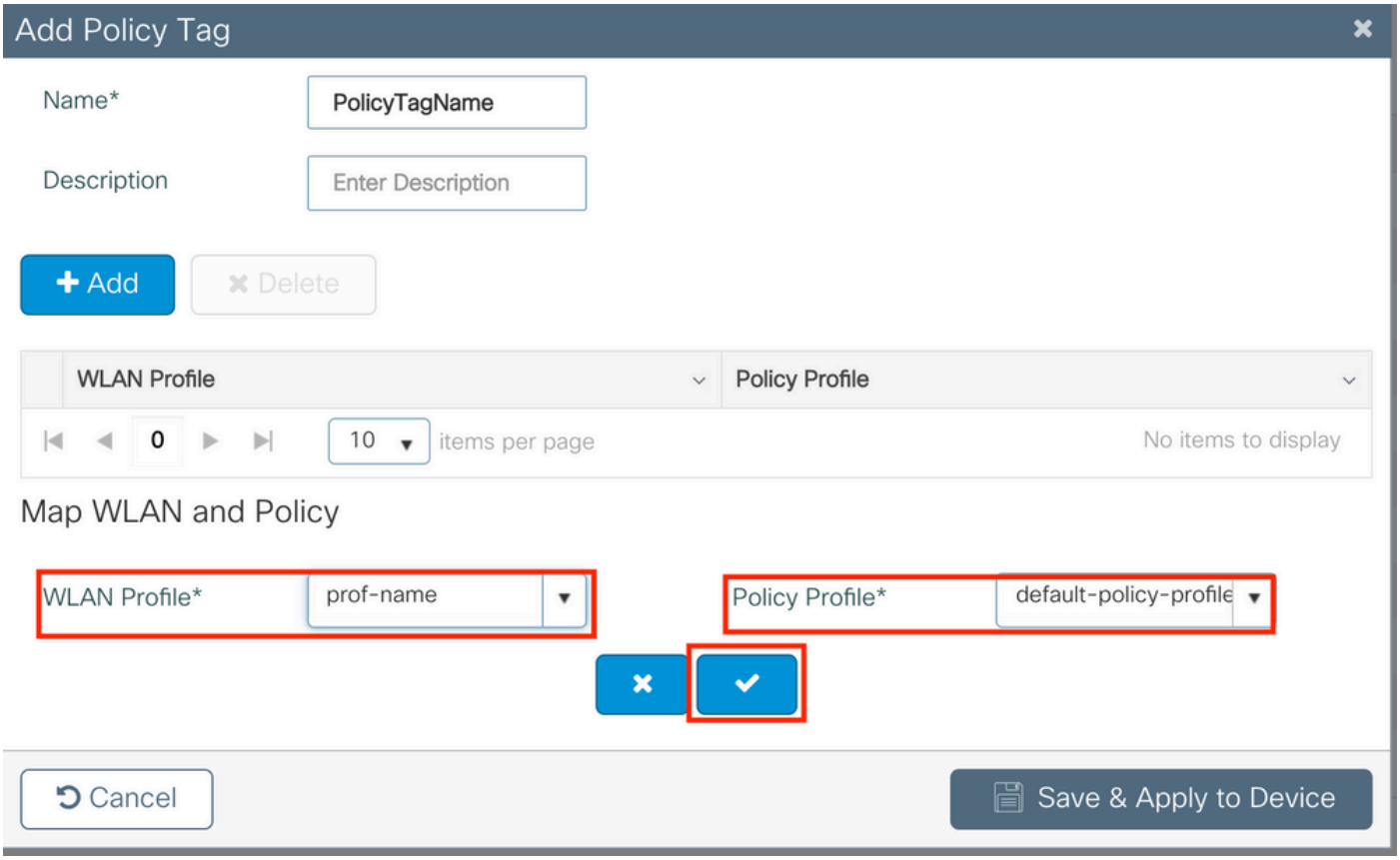
GUI:

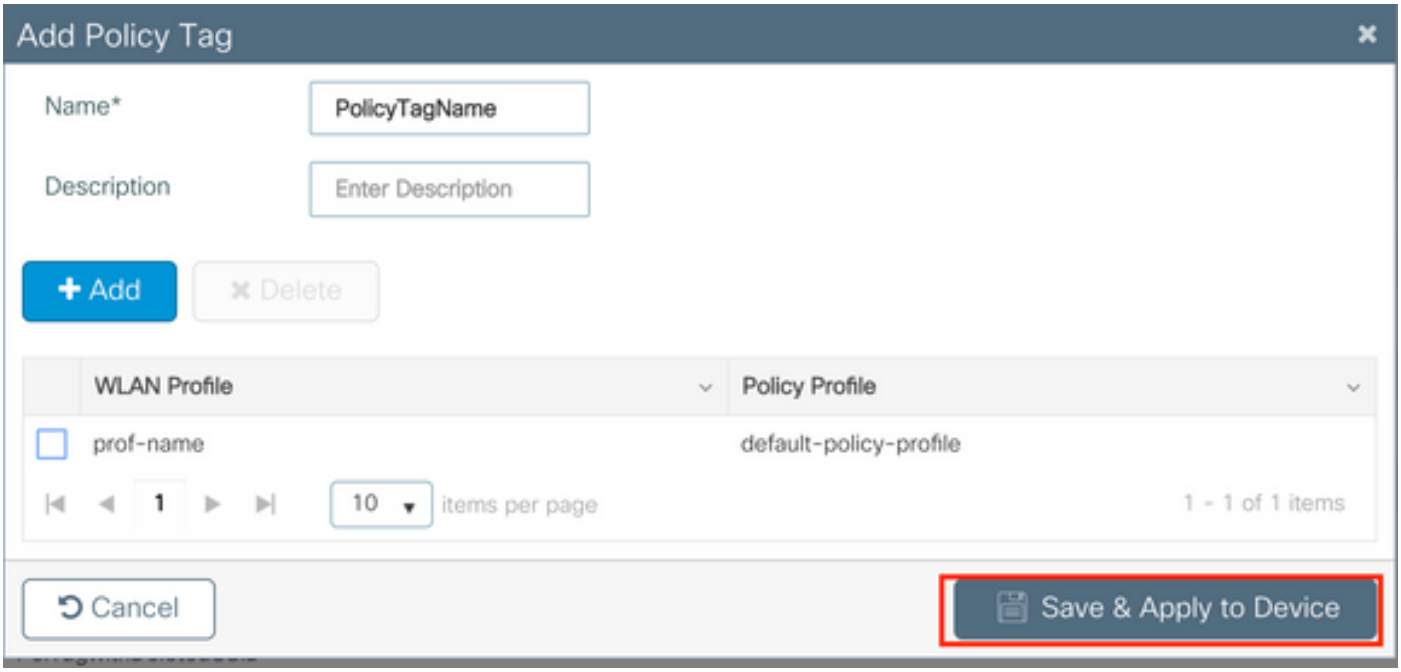
탐색 **Configugation > Tags & Profiles > Tags > Policy** 필요한 경우 새 파일을 추가합니다.



WLAN 프로파일을 원하는 정책 프로파일에 연결합니다.







CLI:

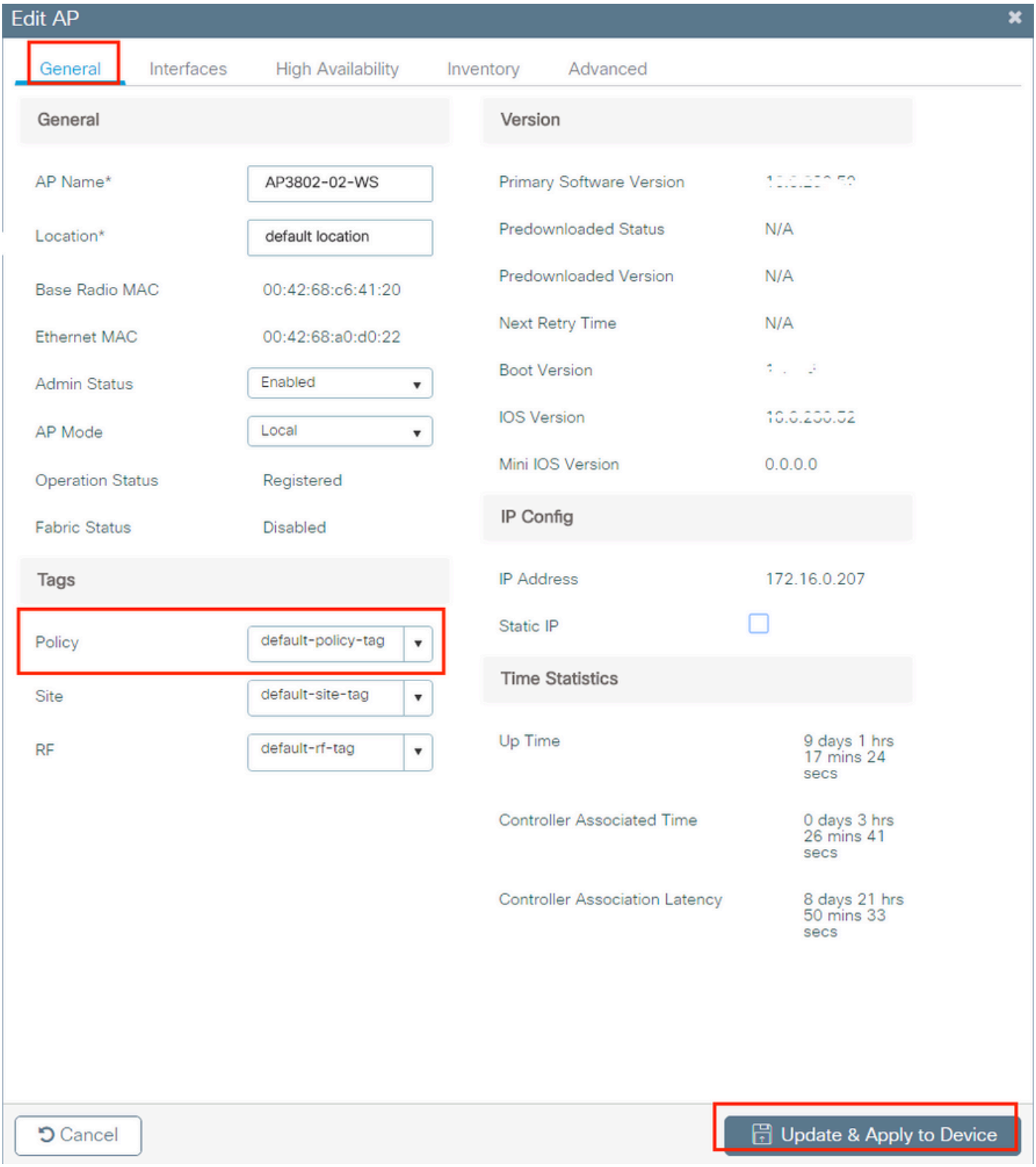
```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

정책 태그 할당

필요한 AP에 정책 태그를 할당합니다.

GUI:

하나의 AP에 태그를 할당하려면 **Configuration > Wireless > Access Points > AP Name > General Tags**, 관련 정책 태그를 할당한 다음 **Update & Apply to Device**.



참고: AP의 정책 태그가 변경되면 9800 WLC와의 연결이 끊어지고 잠시 후 다시 조인됩니다.

동일한 정책 태그를 여러 AP에 할당하려면 **Configuration > Wireless Setup > Advanced > Start Now > Apply**.

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.