Catalyst 9800 WLC에서 인증으로 FlexConnect 구성

목차

소개

이 문서에서는 Catalyst 9800 Wireless LAN Controller에서 중앙 또는 로컬 인증으로 FlexConnect를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst Wireless 9800 구성 모델
- FlexConnect
- 802.1x

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C9800-CL, Cisco IOS-XE® 17.3.4

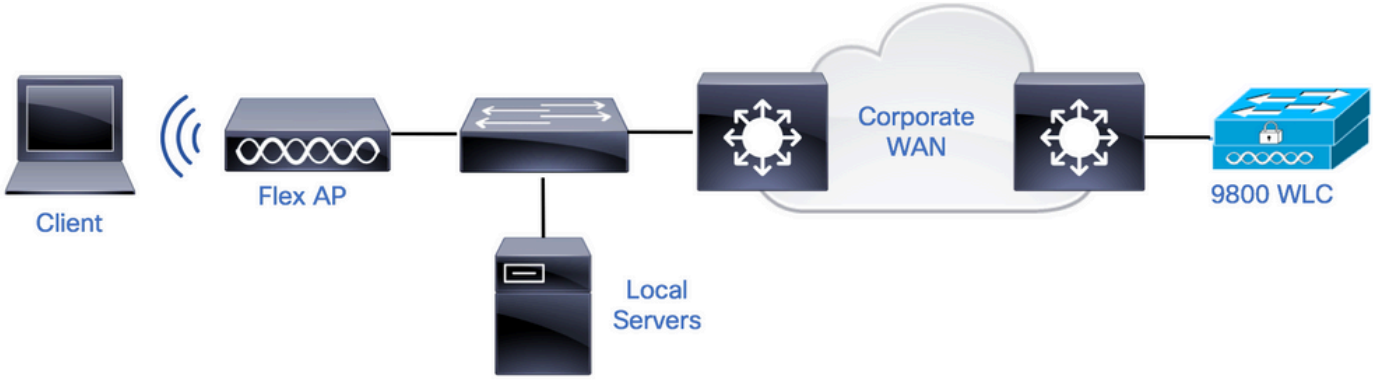
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FlexConnect는 원격 사무실 구축을 위한 무선 솔루션입니다. 각 위치에 컨트롤러를 구축할 필요 없이 WAN(Wide Area Network) 링크를 통해 기업 사무실의 원격 위치에 AP(Access Point)를 구성할 수 있습니다. FlexConnect AP는 클라이언트 데이터 트래픽을 로컬로 전환하고 컨트롤러에 대한 연결이 끊길 경우 클라이언트 인증을 로컬로 수행할 수 있습니다. 연결 모드에서는 FlexConnect AP가 로컬 인증도 수행할 수 있습니다.

구성

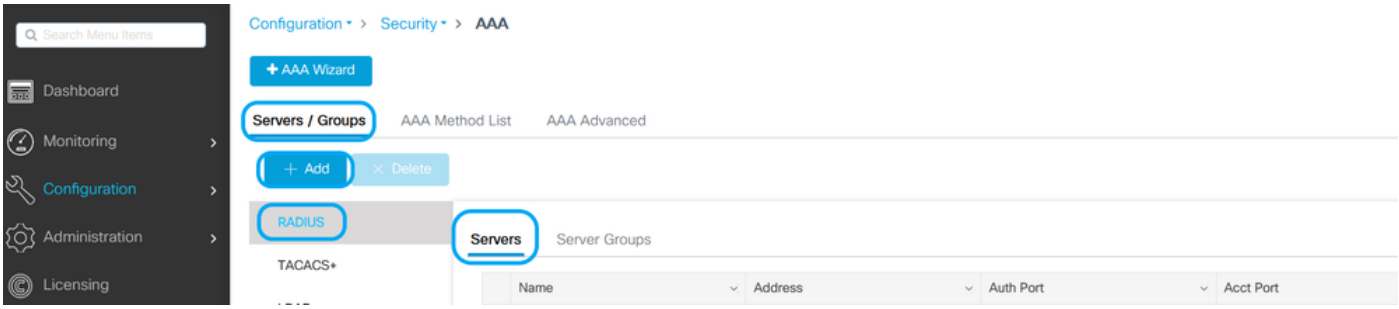
네트워크 다이어그램



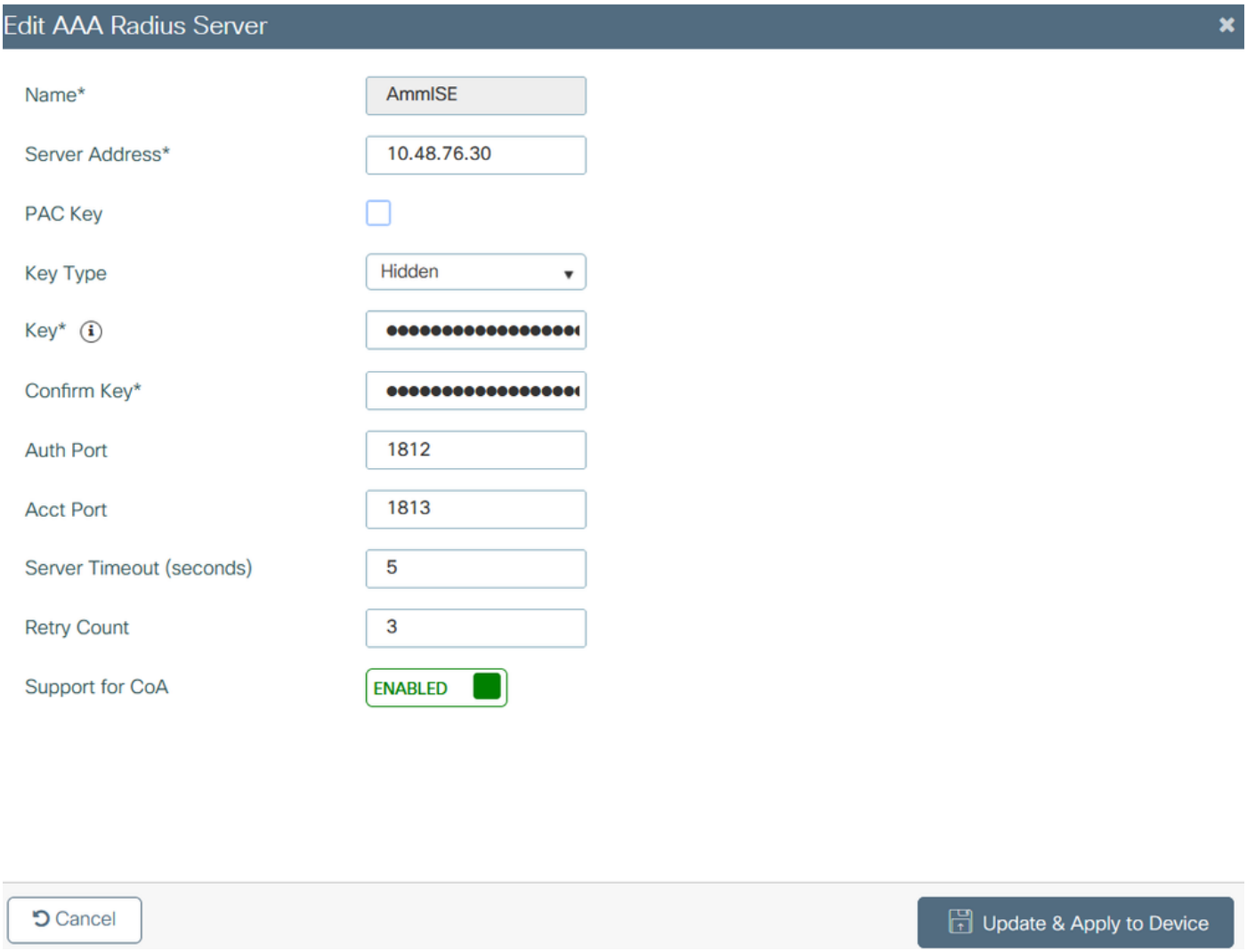
설정

9800 WLC의 AAA 컨피그레이션

1단계. RADIUS 서버를 선언합니다. **GUI에서:** Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Servers(서버) > + Add(추가)로 이동하고 RADIUS 서버 정보를 입력합니다.

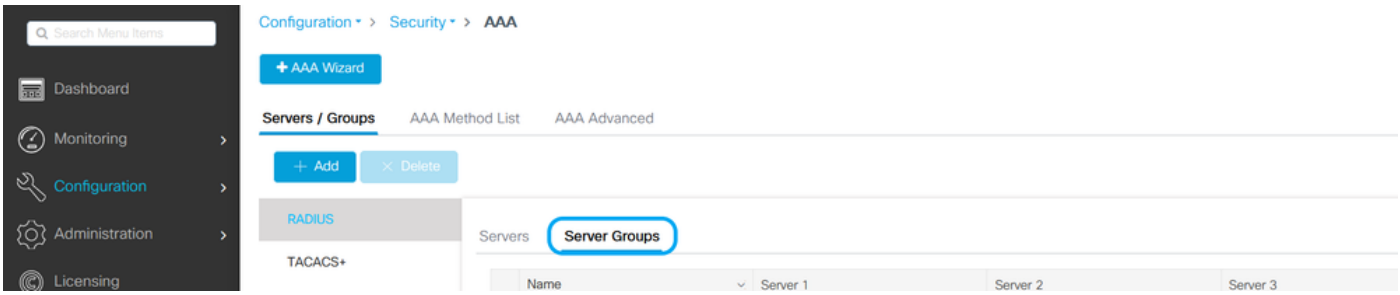


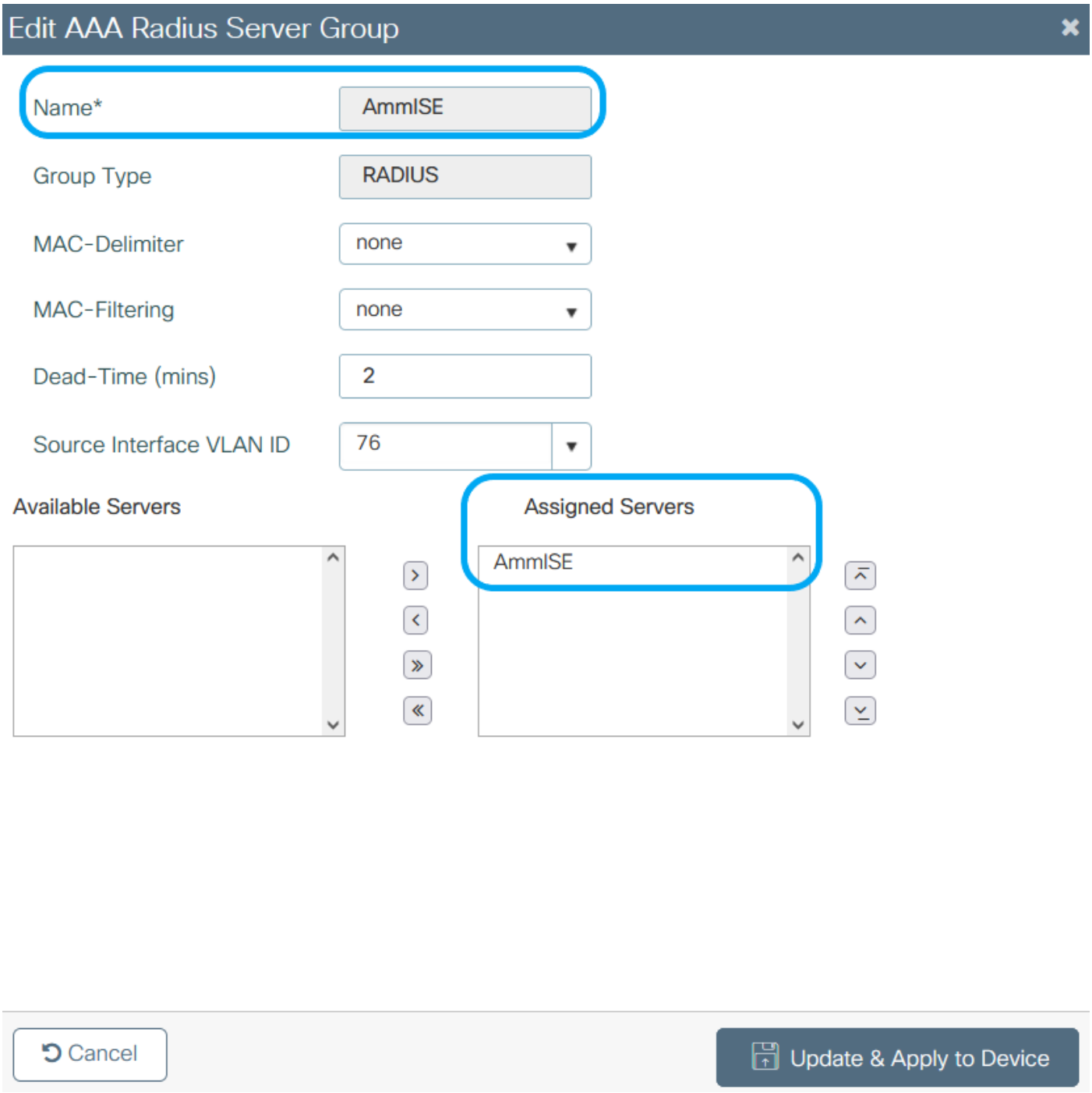
향후 CoA가 필요한 보안 유형을 사용하려는 경우 CoA 지원을 활성화해야 합니다.



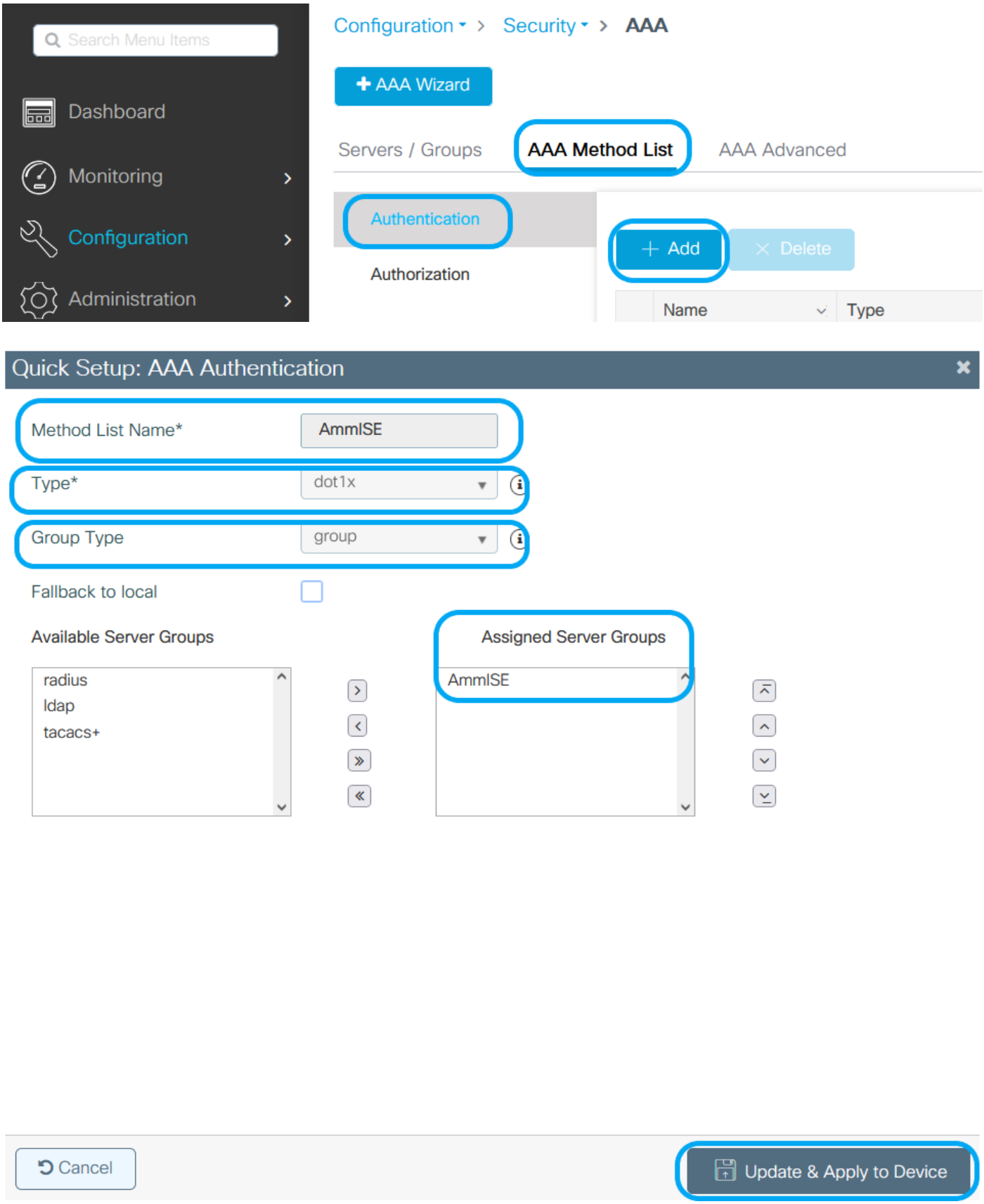
참고: 참고: Radius CoA는 Flex Connect 로컬 인증 구축에서 지원되지 않습니다. .

2단계. RADIUS 그룹에 RADIUS 서버를 추가합니다. **GUI에서:** Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Server Groups(서버 그룹) > + Add(추가)로 이동합니다.





3단계. 인증 방법 목록을 만듭니다. **GUI에서:** Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 방법 목록) > Authentication(인증) > + Add(추가)로 이동합니다.



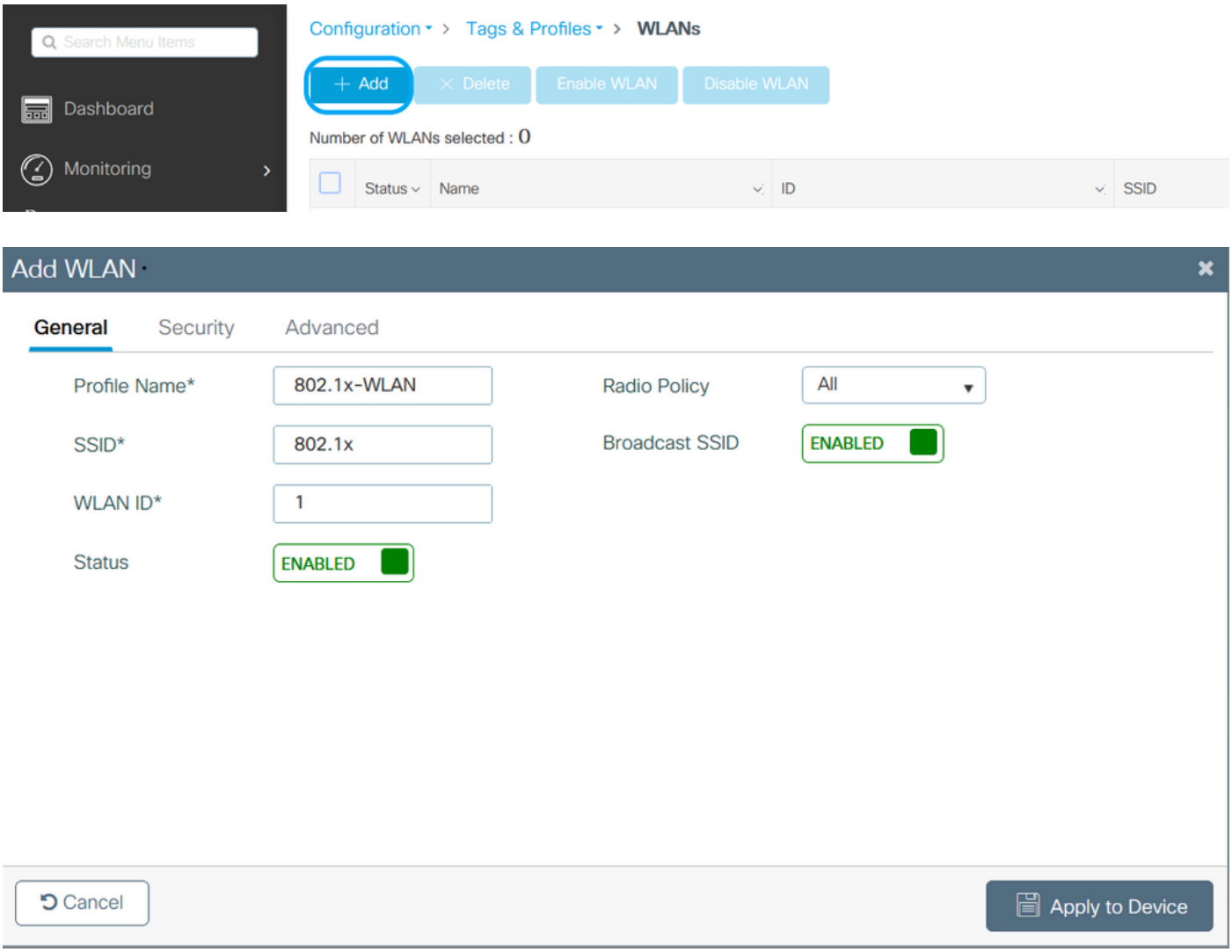
CLI에서:

```
# config t
# aaa new-model
```

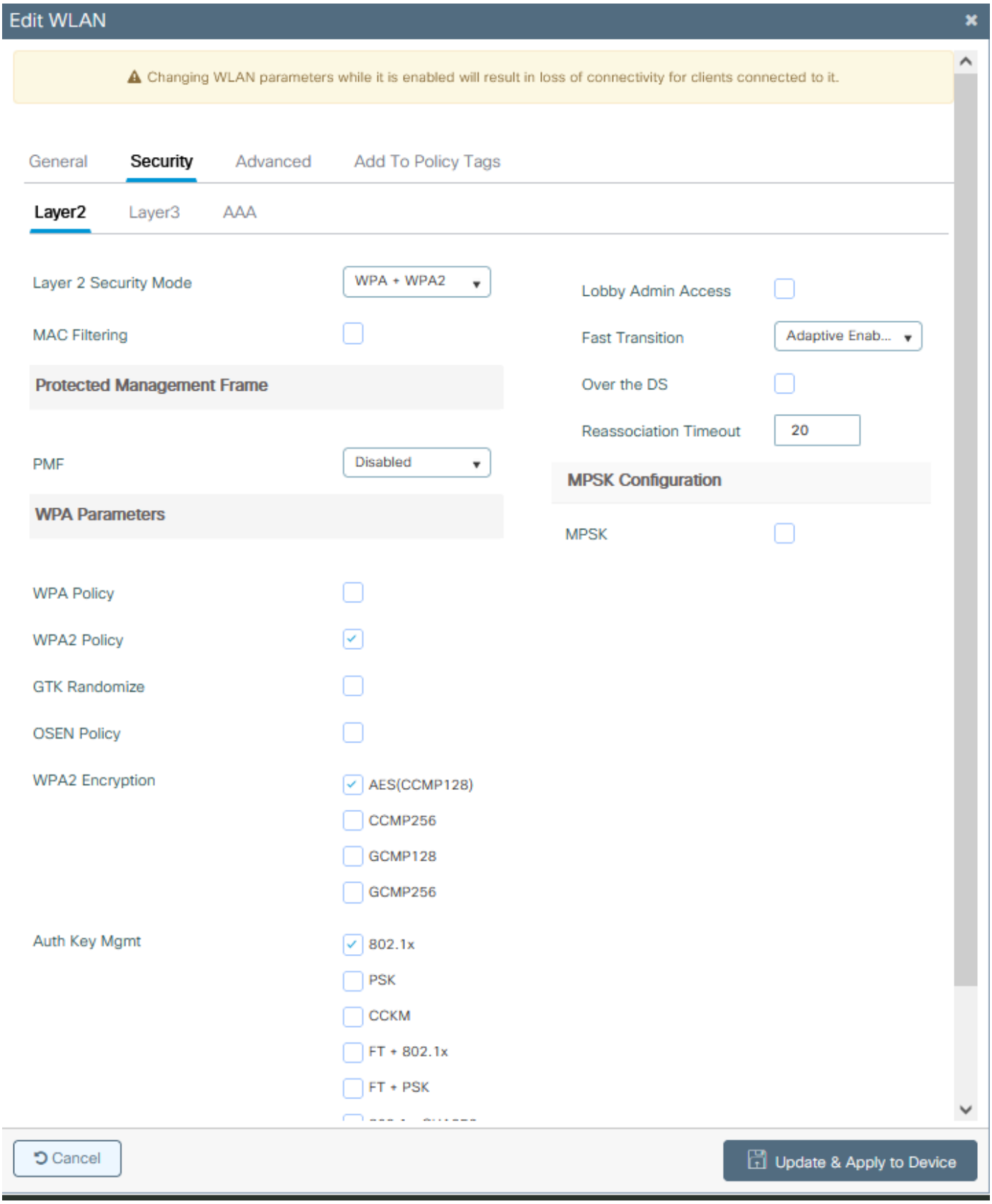
```
# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# 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>
```

WLAN 구성

1단계. **GUI에서:** Configuration(컨피그레이션) > Wireless(무선) > WLANs(WLAN)로 이동하고 +Add(추가)를 클릭하여 새 WLAN을 생성하고 WLAN 정보를 입력합니다. 그런 다음 Apply to Device(디바이스에 적용)를 클릭합니다.

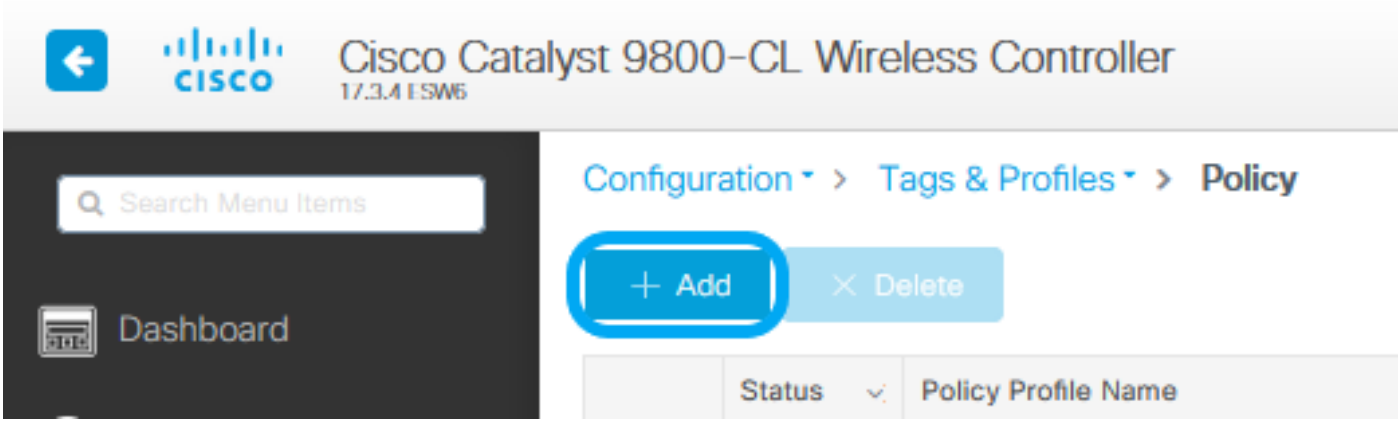


2단계. **GUI에서:** 암호화 방법 및 802.1x가 사용 중인 경우 Authentication List(인증 목록)를 사용하는 동안 Layer2/Layer3 보안 모드를 구성하려면 Security(보안) 탭으로 이동합니다. 그런 다음 Update & Apply to Device를 클릭합니다.

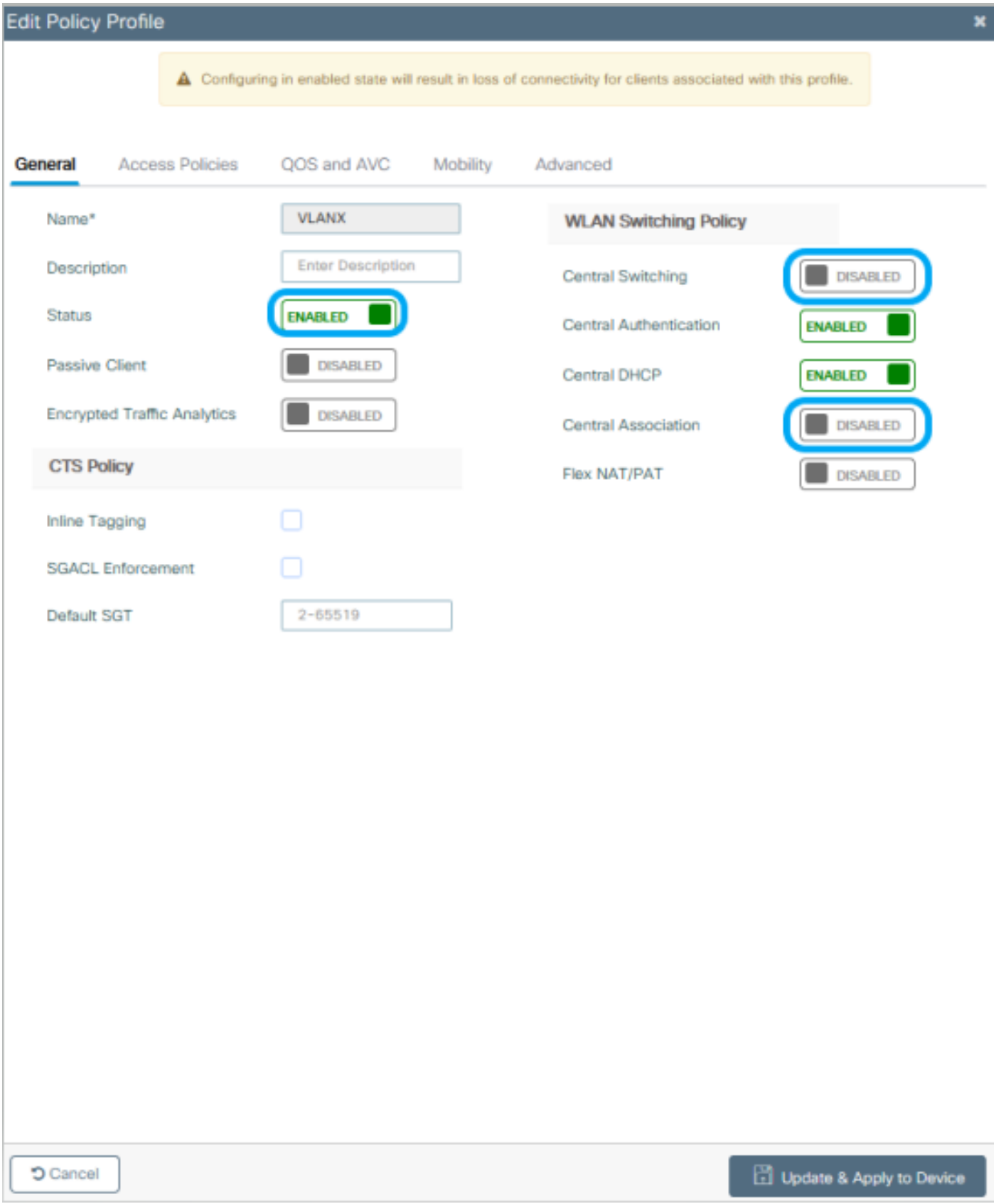


정책 프로파일 구성

1단계. **GUI에서:** Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동하고 +Add(추가)를 클릭하여 정책 프로필을 생성합니다.

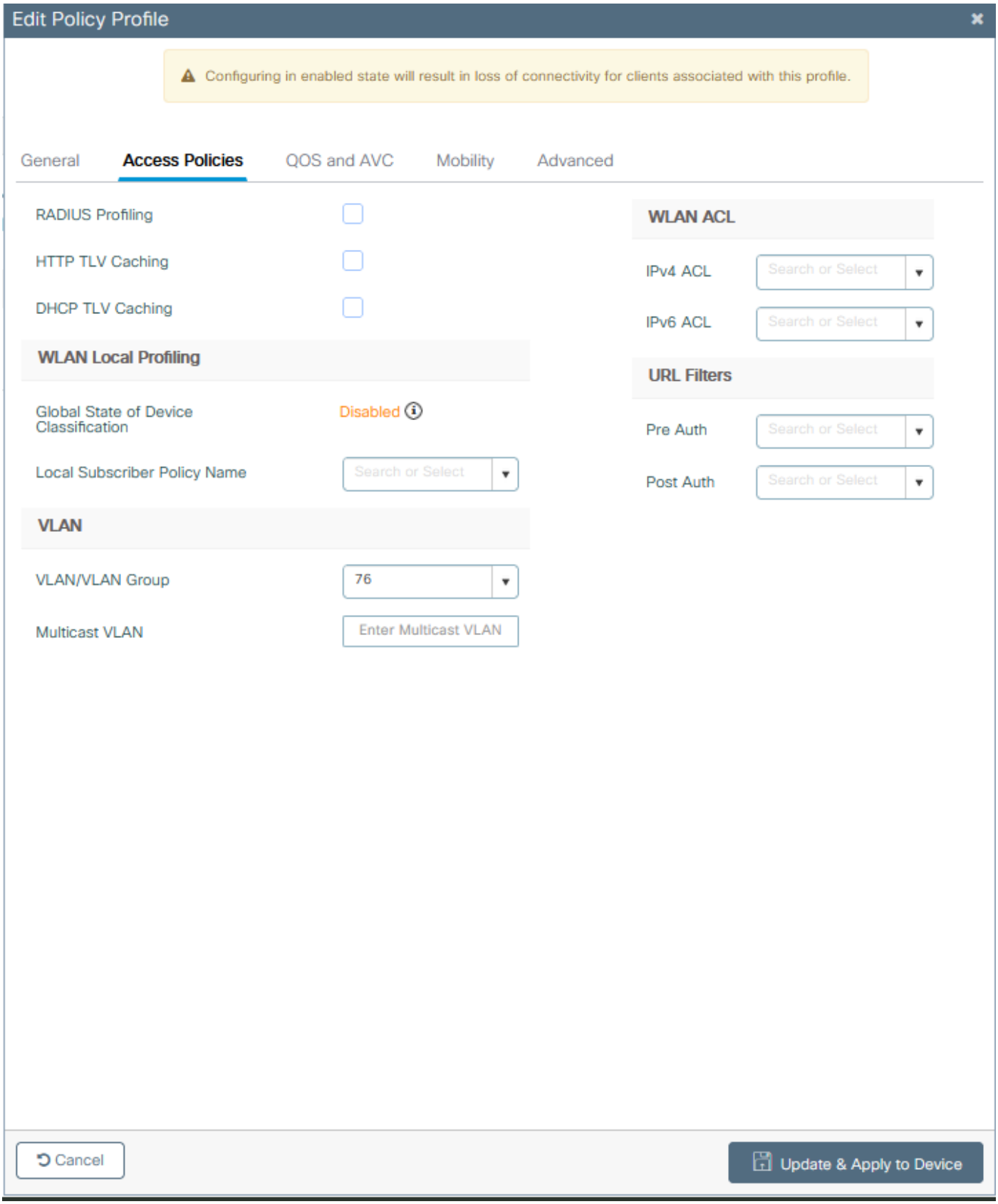


2단계. 이름을 추가하고 Central Switching(중앙 스위칭) 상자의 선택을 취소합니다. 이 설정을 통해 컨트롤러는 클라이언트 인증을 처리하고 FlexConnect 액세스 포인트는 클라이언트 데이터 패킷을 로컬로 전환합니다.

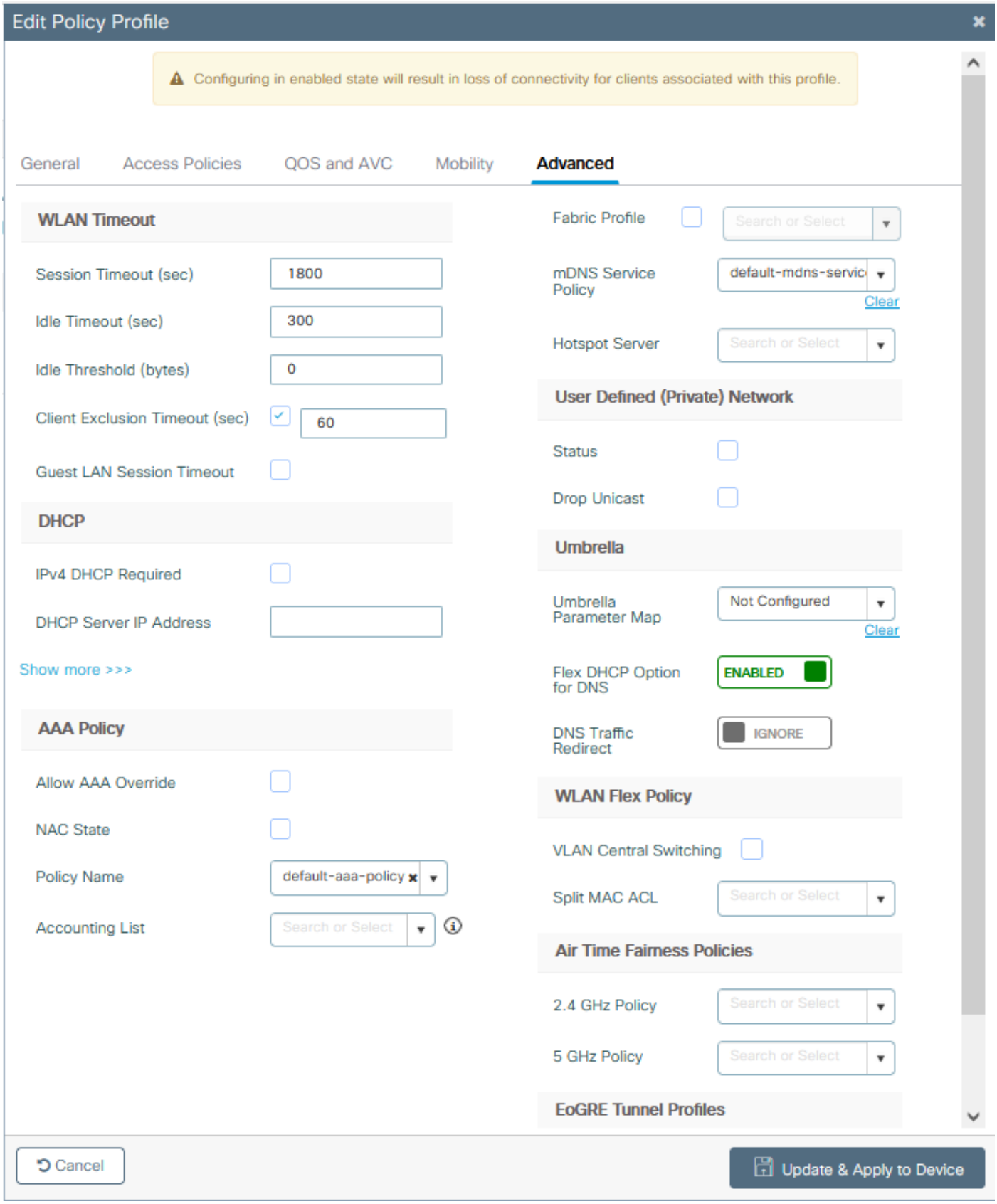


참고: Flexconnect AP가 사용될 때 중앙 스위칭이 비활성화된 경우 중앙 연결은 모든 정책 프로파일에서 비활성화되어야 하며, 연결과 스위칭은 항상 페어링되어야 합니다.

3단계. **GUI**에서**:** Access Policies(액세스 정책) 탭으로 이동하여 무선 클라이언트가 기본적으로 이 WLAN에 연결할 때 할당할 수 있는 VLAN을 할당합니다.
드롭다운에서 하나의 VLAN 이름을 선택하거나, 모범 사례로서 VLAN ID를 수동으로 입력할 수 있습니다.

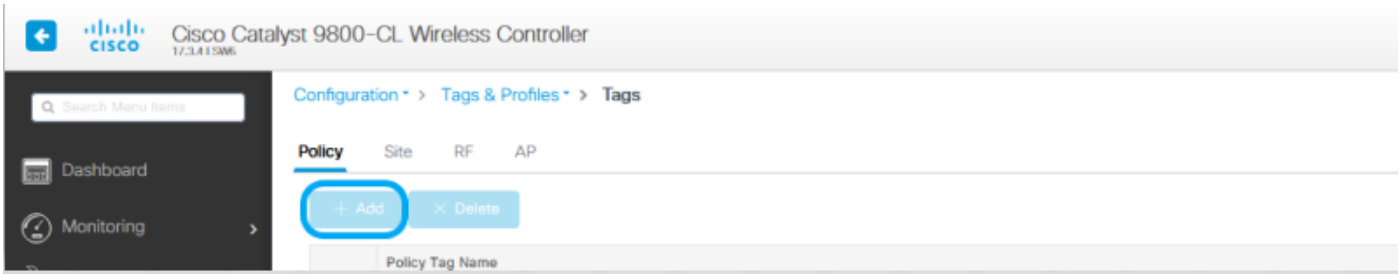


4단계. **GUI**에서**:** Advanced(고급) 탭으로 이동하여 사용 중인 WLAN 시간 제한, DHCP, WLAN Flex Policy 및 AAA 정책을 구성합니다. 그런 다음 Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

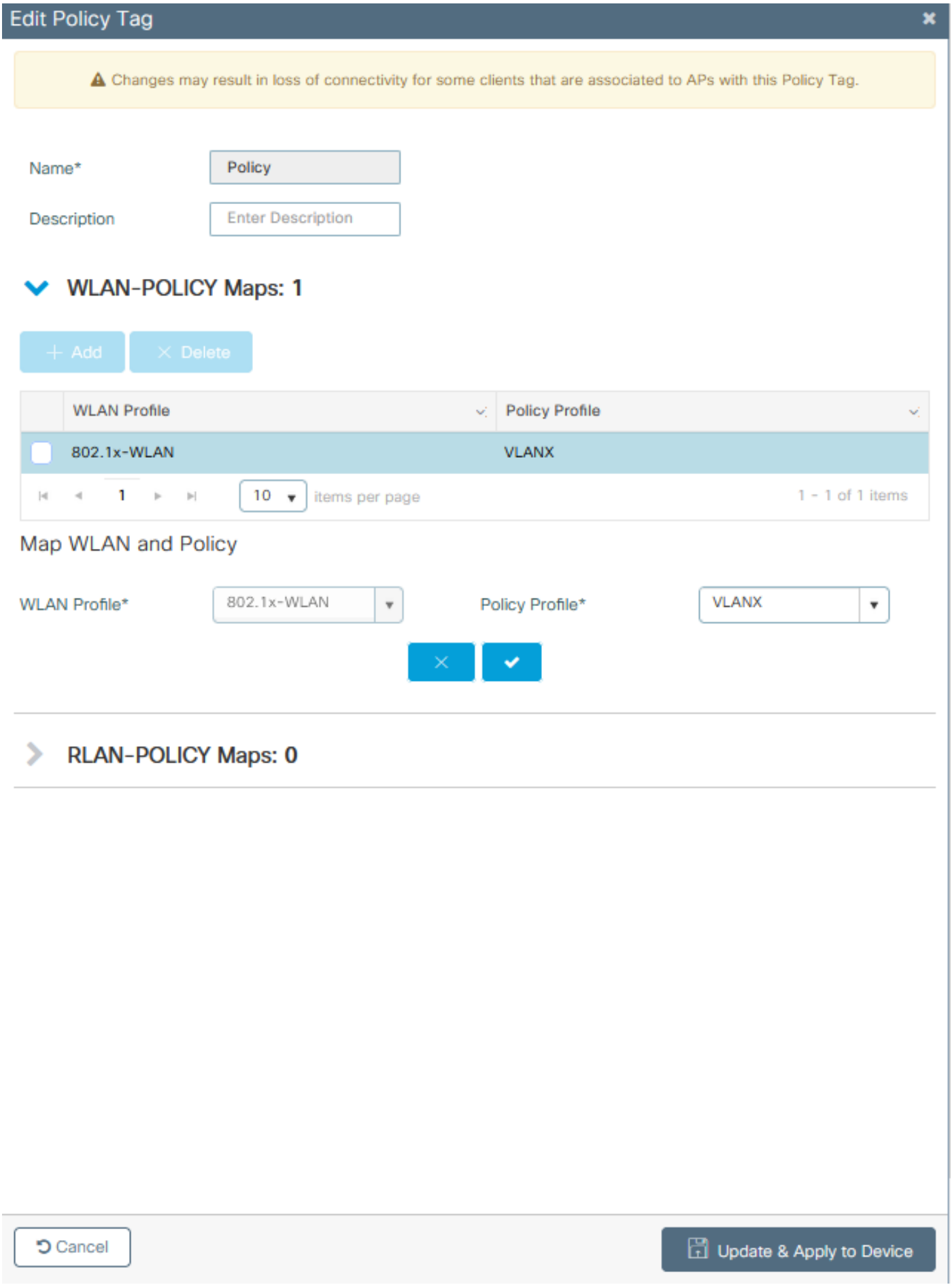


정책 태그 구성

1단계. **GUI에서:** Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Policy(정책) > +Add(추가)로 이동합니다.

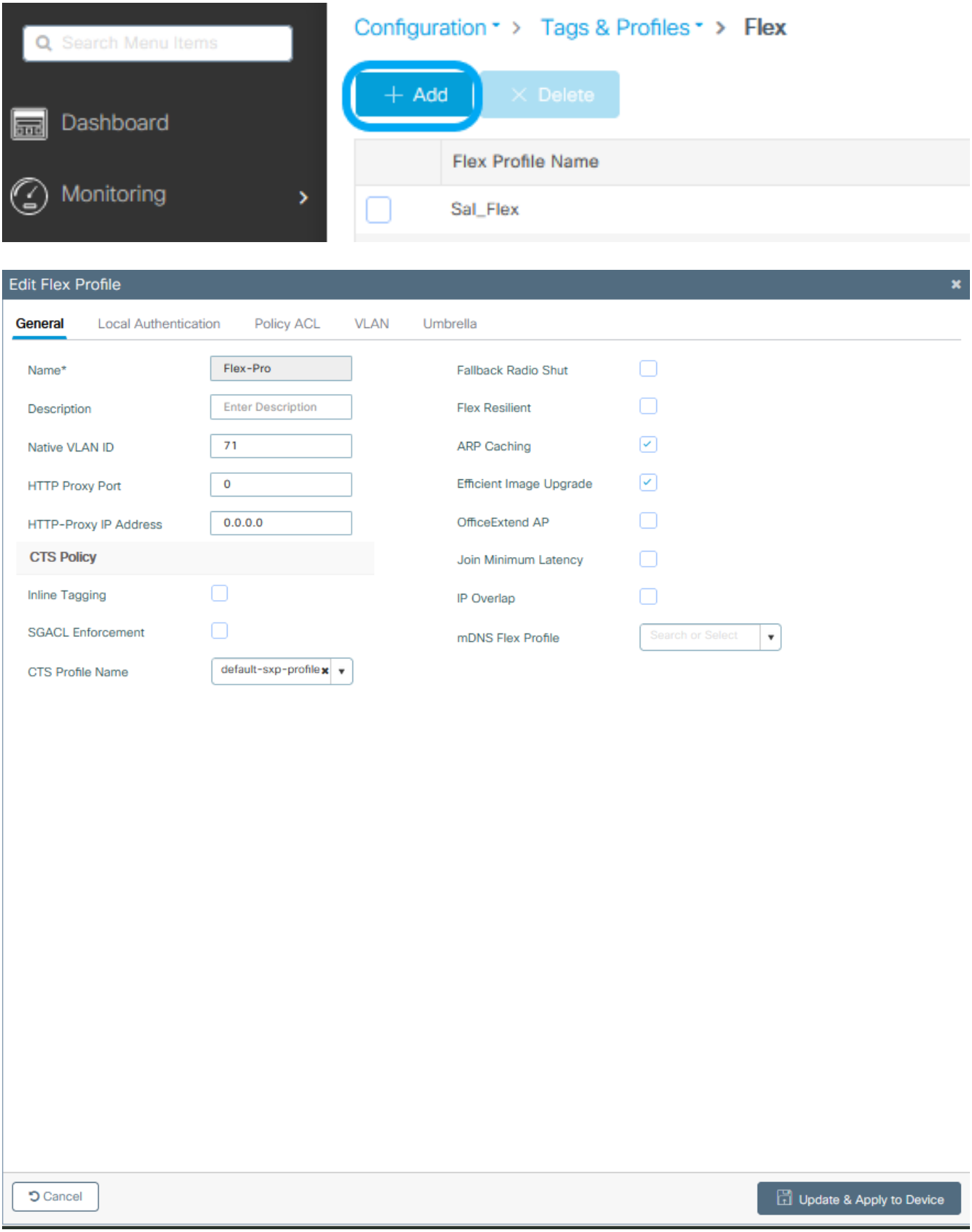


2단계. 이름을 지정하고 전에 생성한 정책 프로필 및 WLAN 프로필을 매핑합니다.



Flex 프로파일 컨피그레이션

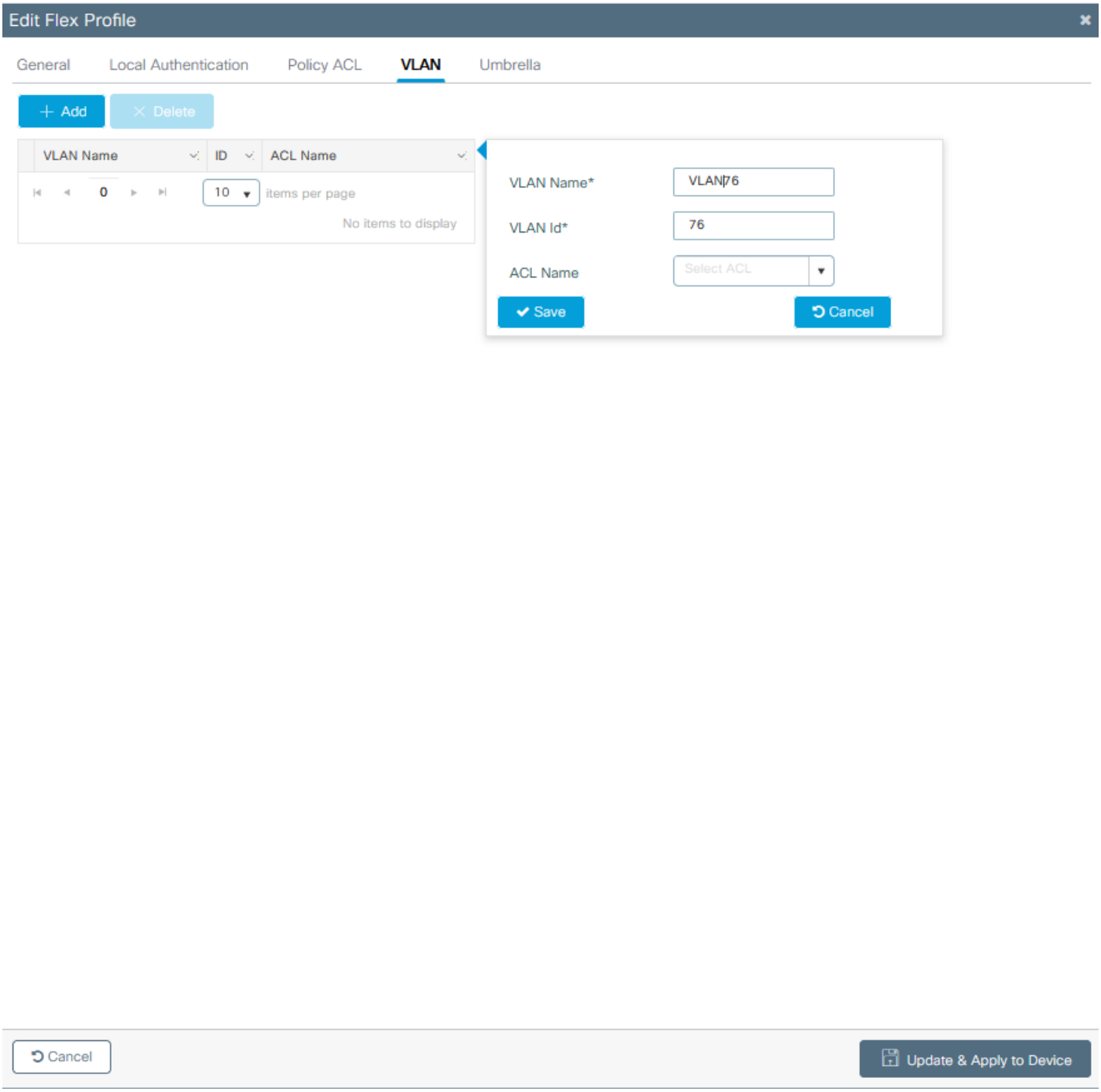
1단계. **GUI에서** Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Flex로 이동하고 +Add(추가)를 클릭하여 새 프로파일을 생성합니다.



참고: Native VLAN ID는 이 Flex Profile을 할당할 수 있는 AP에서 사용하는 VLAN을 의미하며

, AP가 연결된 스위치 포트에서 native로 구성된 VLAN ID와 같아야 합니다.

2단계. VLAN 탭에서 필요한 VLAN, 정책 프로필을 통해 WLAN에 기본적으로 할당된 VLAN 또는 RADIUS 서버에서 푸시한 VLAN을 추가합니다. 그런 다음 Update & Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다.

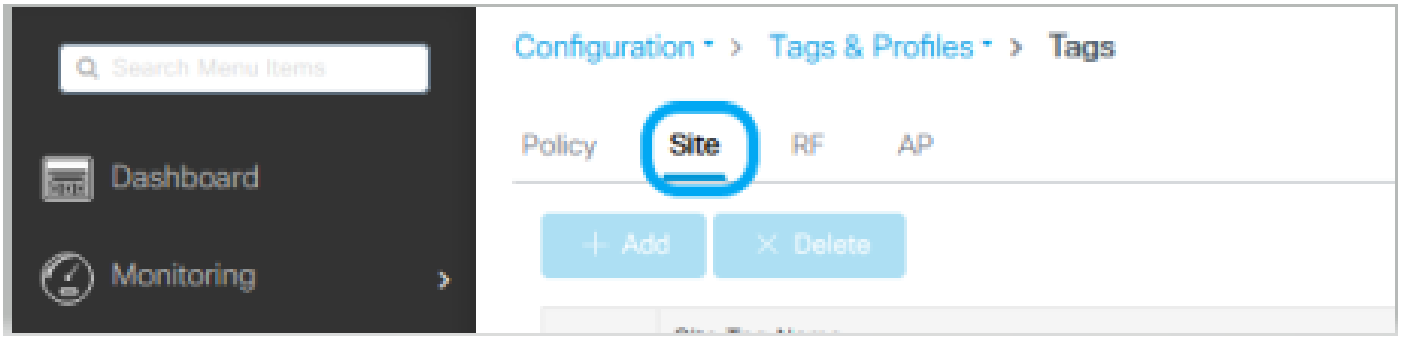


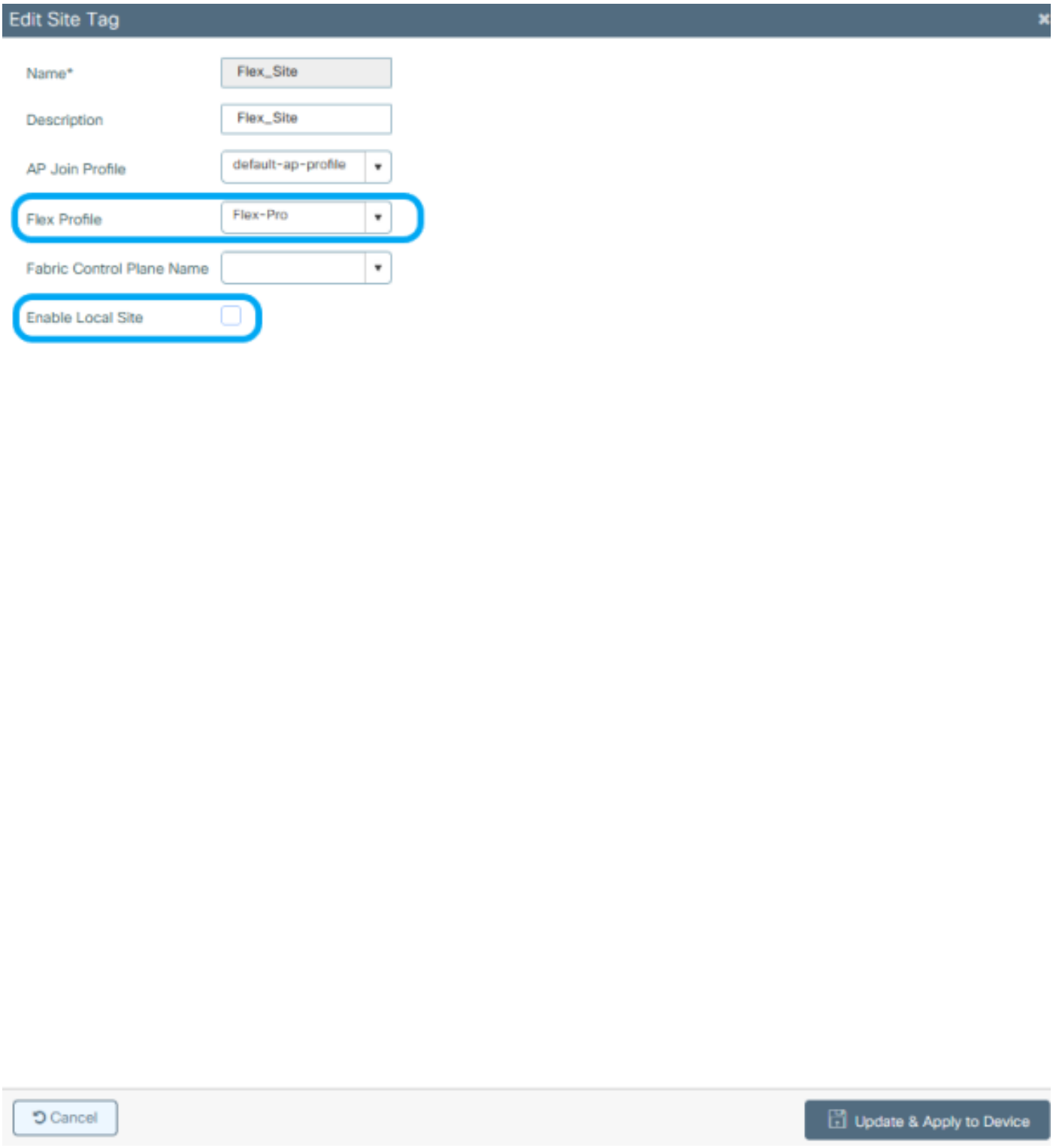
참고: Policy Profile(정책 프로파일)에서 SSID에 할당된 기본 VLAN을 선택합니다. 해당 단계에서 VLAN 이름을 사용하는 경우 Flex Profile 컨피그레이션에서 동일한 VLAN 이름을 사용해야 합니다. 그렇지 않으면 클라이언트가 WLAN에 연결할 수 없습니다.

참고: AAA 재정의로 flexConnect에 대한 ACL을 구성하려면 "policy ACL"에서만 ACL을 구성하십시오. ACL이 특정 VLAN에 할당된 경우 VLAN을 추가할 때 ACL을 추가한 다음 "policy ACL"에서 ACL을 추가하십시오.

사이트 태그 구성

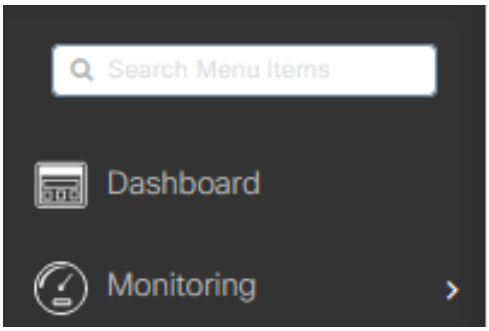
1단계. **GUI에서:** Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Tags(태그) > Site(사이트)로 이동하고 +Add(추가)를 클릭하여 새 사이트 태그를 생성합니다. AP가 클라이언트 데이터 트래픽을 로컬로 전환하도록 허용하려면 Enable Local Site(로컬 사이트 활성화) 상자의 선택을 취소하고 이전에 생성한 Flex Profile을 추가합니다.





참고: Enable Local Site(로컬 사이트 활성화)가 비활성화되면 이 사이트 태그를 할당받는 AP를 FlexConnect 모드로 구성할 수 있습니다.

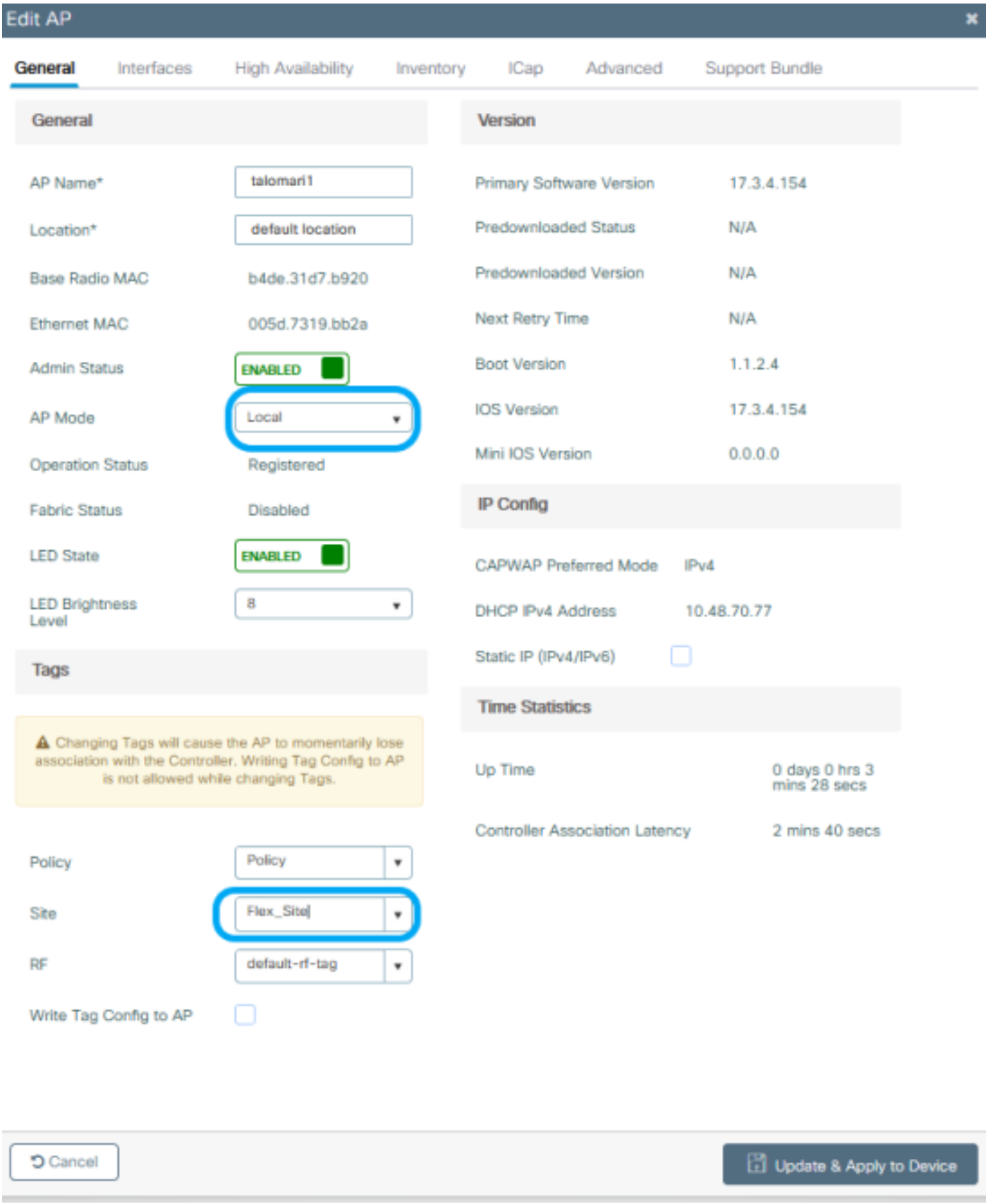
2단계. **GUI에서** Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트) > AP name(AP 이름)으로 이동하여 Site Tag(사이트 태그) 및 Policy Tag(정책 태그)를 연결된 AP에 추가합니다. 이로 인해 AP가 CAPWAP 터널을 다시 시작하고 9800 WLC에 다시 조인할 수 있습니다.



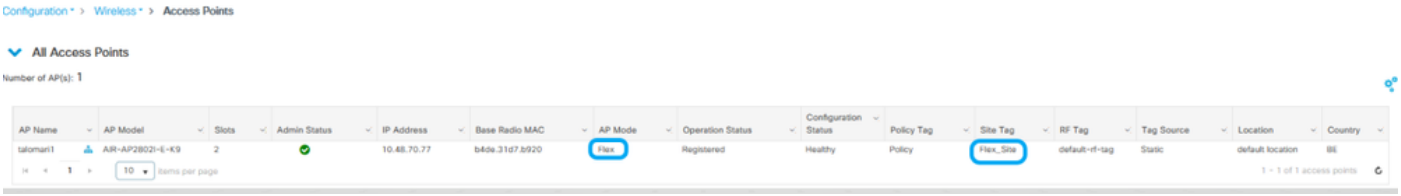
Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

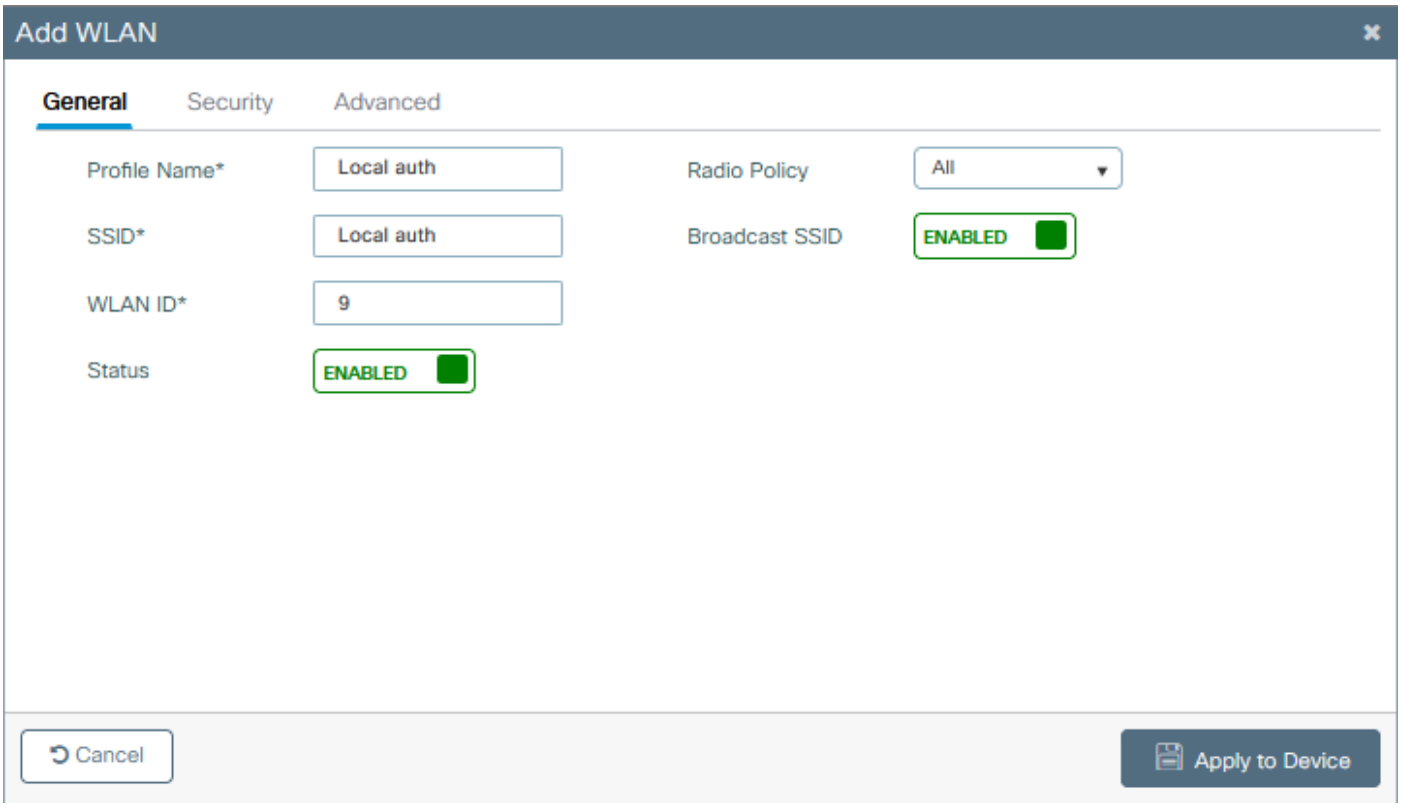


AP가 다시 연결되면 AP가 현재 FlexConnect 모드에 있음을 알 수 있습니다.

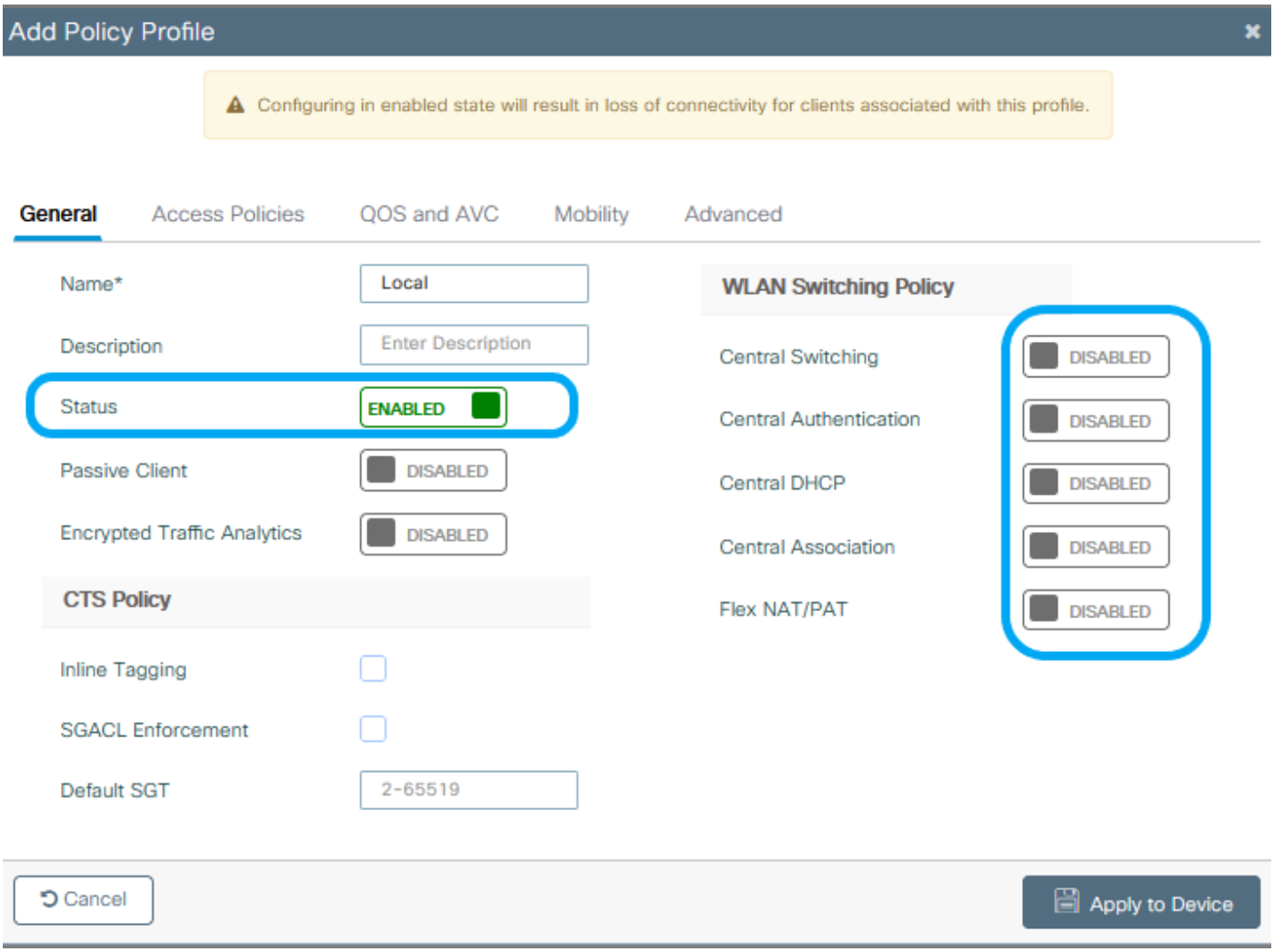


외부 RADIUS 서버에 대한 로컬 인증

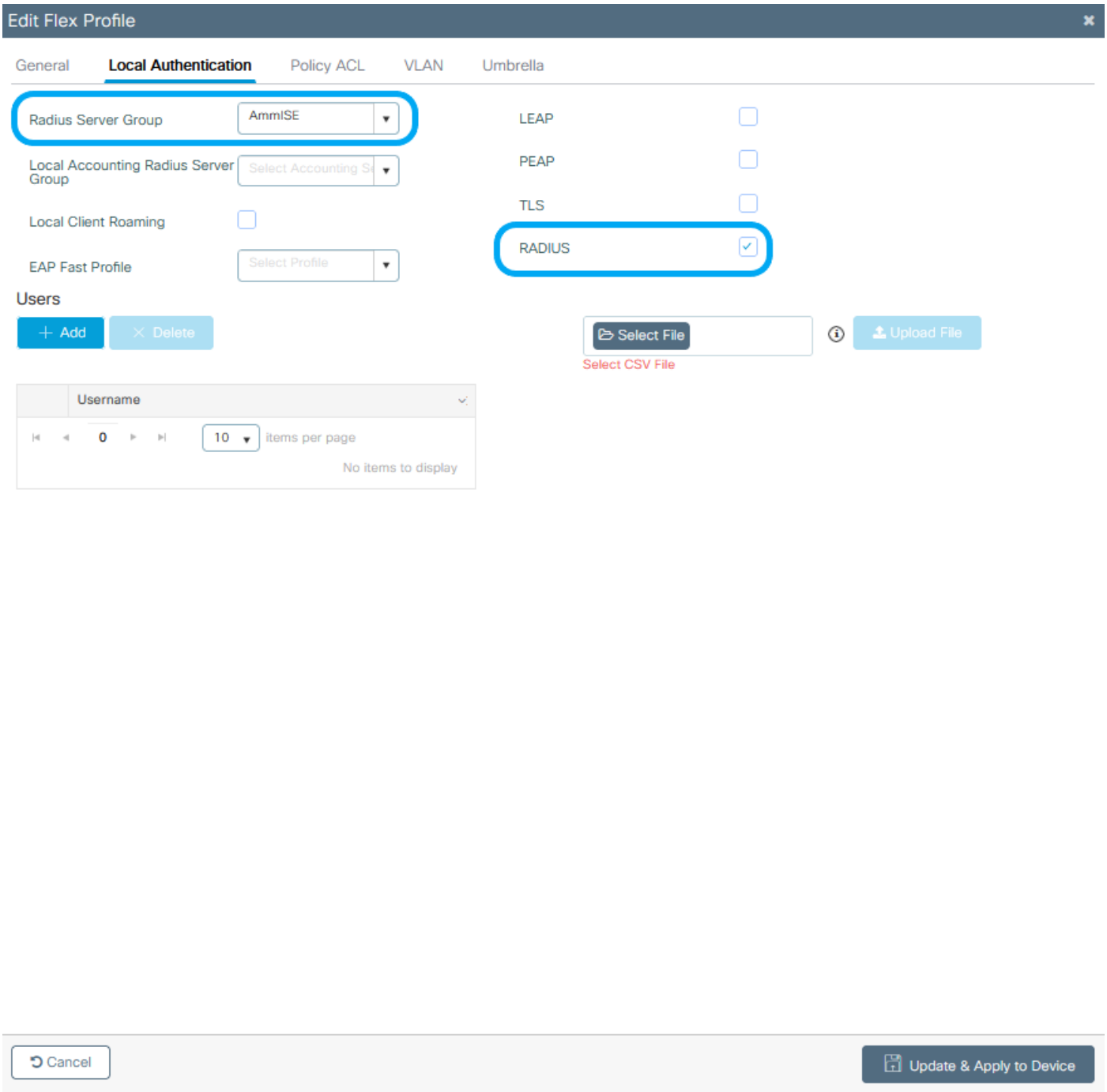
1단계. AP를 RADIUS 서버에 네트워크 디바이스로 추가합니다. 예는 ISE(Identity Service Engine)를 RADIUS 서버로 사용하는 방법을 참조하십시오
2단계. WLAN을 생성합니다.
컨피그레이션은 이전에 구성한 컨피그레이션과 동일할 수 있습니다.



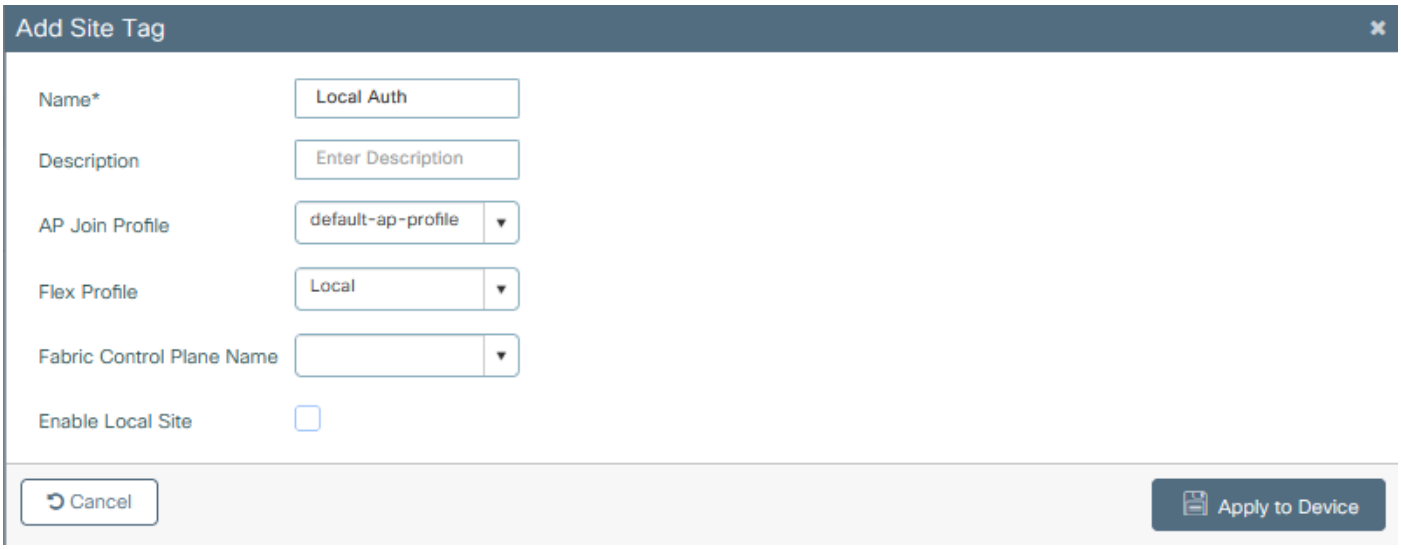
3단계. 정책 프로파일 구성.
새 를 만들거나 이전에 구성한 를 사용할 수 있습니다. 이번에는 Central Switching, Central Authentication, Central DHCP, Central Association Enable(중앙 스위칭, 중앙 DHCP, 중앙 연결 활성화) 상자의 선택을 취소합니다.



4단계. 정책 태그 구성.
구성된 WLAN과 생성된 정책 프로필을 연결합니다.
5단계. Flex Profile 컨피그레이션
Flex Profile을 생성하고 Local Authentication(로컬 인증) 탭으로 이동하여 Radius Server Group(RADIUS 서버 그룹)을 구성하고 RADIUS 상자를 선택합니다.



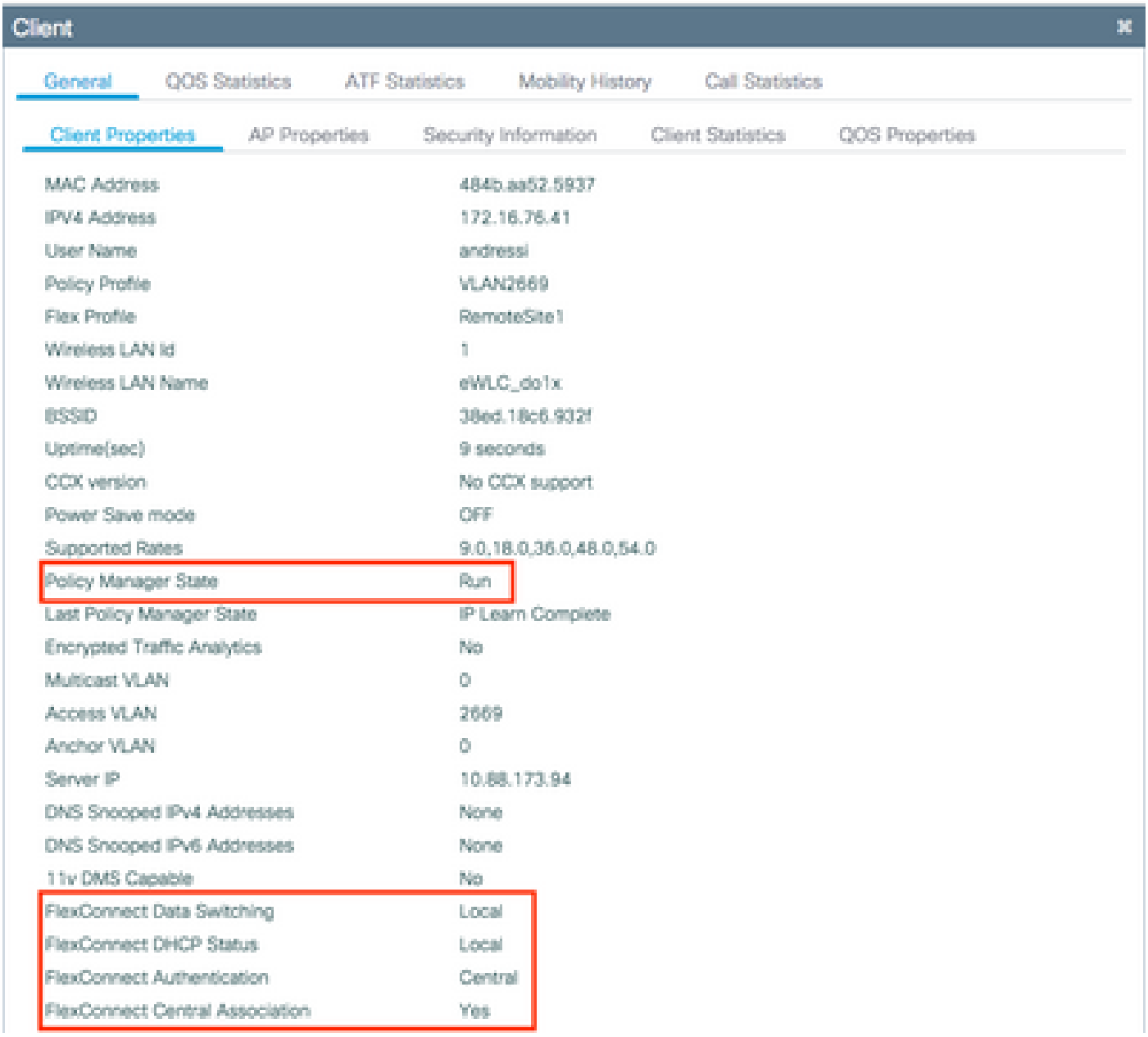
6단계. 사이트 태그 구성.
5단계에서 구성된 Flex Profile을 구성하고 Enable Local Site(로컬 사이트 활성화) 상자의 선택을 취소합니다.



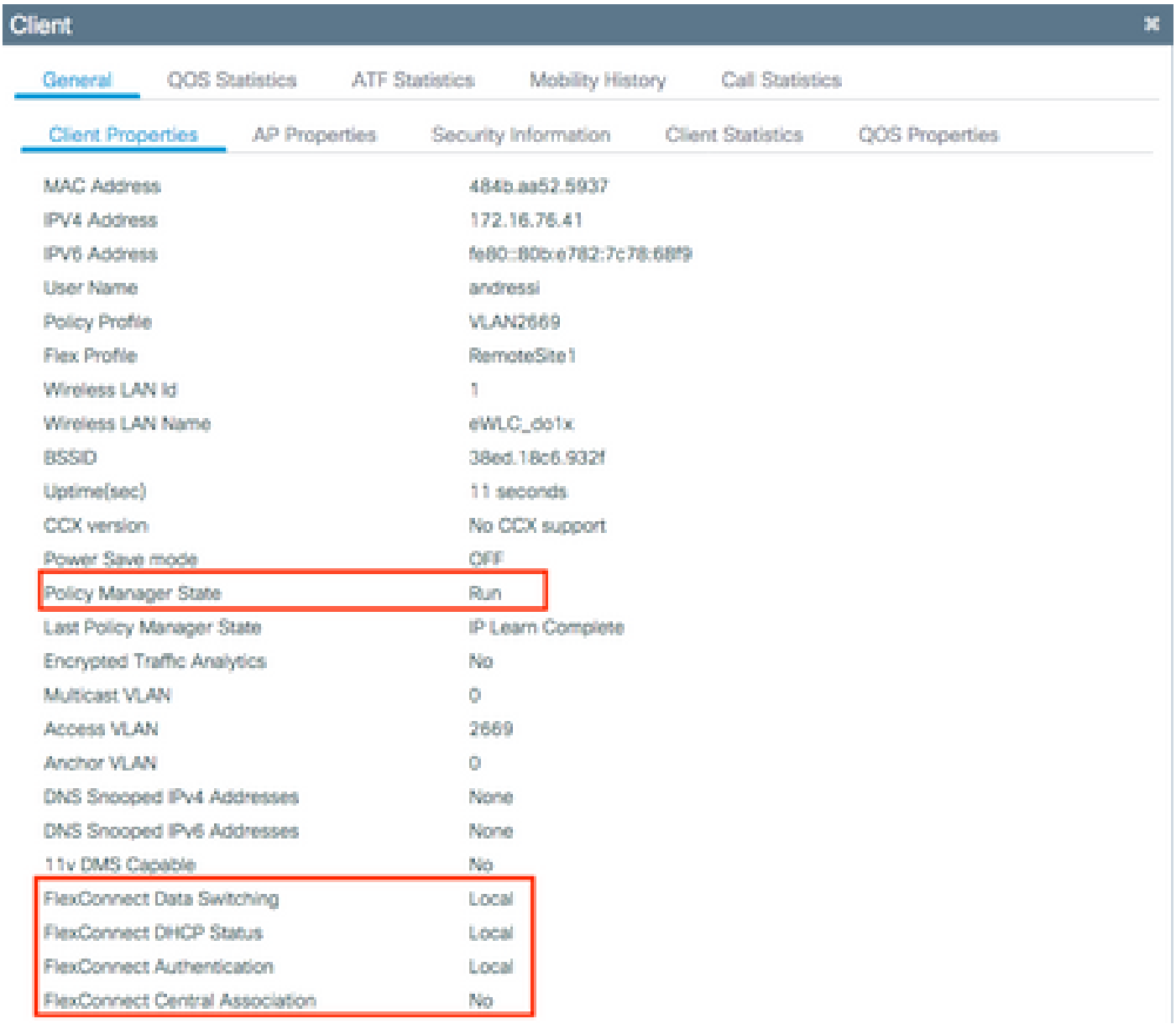
다음을 확인합니다.

GUI에서 Monitoring(모니터링) > Wireless(무선) > Clients(클라이언트)로 이동하고 Policy Manager State(정책 관리자 상태)와 FlexConnect 매개변수를 확인합니다.

중앙 인증:


Client
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
Client Properties
AP Properties
Security Information
Client Statistics
QOS Properties
MAC Address 484b.aa52.5937
IPV4 Address 172.16.76.41
User Name andressi
Policy Profile VLAN2669
Flex Profile RemoteSite1
Wireless LAN Id 1
Wireless LAN Name eWLC_dot1x
BSSID 38ed.18c6.932f
Uptime(sec) 9 seconds
CCX version No CCX support
Power Save mode OFF
Supported Rates 9.0,18.0,36.0,48.0,54.0
Policy Manager State Run
Last Policy Manager State IP Learn Complete
Encrypted Traffic Analytics No
Multicast VLAN 0
Access VLAN 2669
Anchor VLAN 0
Server IP 10.88.173.94
DNS Snooped IPv4 Addresses None
DNS Snooped IPv6 Addresses None
11v DMS Capable No
FlexConnect Data Switching Local
FlexConnect DHCP Status Local
FlexConnect Authentication Central
FlexConnect Central Association Yes

로컬 인증:



이러한 명령을 사용하여 현재 구성을 확인할 수 있습니다:

CLI에서:

```
# 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 볼륨을 기반으로 몇 시간에서 며칠로 돌아갈 수 있습니다.

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

1단계. 문제가 발생했을 때까지의 시간에 로그를 추적할 수 있도록 컨트롤러 현재 시간을 확인합니다.

CLI에서:

```
# show clock
```

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

CLI에서:

```
# show logging
```

3단계. 디버그 조건이 활성화되었는지 확인합니다.

CLI에서:

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

참고: 나열된 조건을 찾을 경우, 이는 활성화된 조건(mac 주소, ip 주소 등)이 발생하는 모든 프로세스의 디버그 레벨에 추적이 로깅됨을 의미합니다. 이로 인해 로그의 볼륨이 증가합니다. 따라서 적극적으로 디버깅하지 않을 때는 모든 조건을 지우는 것이 좋습니다.

4단계. 테스트 중인 mac 주소가 3단계의 조건으로 나열되지 않았다고 가정할 경우, 특정 mac 주소에 대한 always-on 알림 레벨 추적을 수집합니다.

CLI에서:

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

세션의 콘텐츠를 표시하거나 파일을 외부 TFTP 서버에 복사할 수 있습니다.

CLI에서:

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

조건부 디버그 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 상호작용하는 모든 프로세스에 대해 디버그 레벨 추적을 제공할 수 있습니다. 조건부 디버깅을 활성화하려면 다음 단계를 수행합니다.

5단계. 활성화된 디버그 조건이 없는지 확인합니다.

CLI에서:

```
# 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 2,085,978,494초까지 늘릴 수 있습니다.

CLI에서:

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

참고: 한 번에 둘 이상의 클라이언트를 모니터링하려면 mac 주소당 debug wireless mac <aaaa.bbb.cccc> 명령을 실행합니다.

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.

CLI에서:

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

모니터링 시간이 경과하거나 무선 디버그가 중단되면 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. RA 추적 .log를 외부 서버에 복사하거나 출력을 화면에 직접 표시할 수 있습니다.

RA 추적 파일의 이름을 확인합니다

CLI에서:

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

파일을 외부 서버에 복사:

CLI에서:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

콘텐츠 표시:

CLI에서:

```
# 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 로그를 자세히 살펴보았으므로 클라이언트를 다시 디버깅할 필요가 없습니다.

CLI에서:

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

참고: 이 명령 출력은 모든 프로세스의 모든 로깅 레벨에 대한 추적을 반환하며 상당히 방대합니다. 이러한 추적을 구문 분석하는 데 도움이 되도록 Cisco TAC를 활성화하십시오.

---

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

파일을 외부 서버에 복사:

CLI에서:

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

콘텐츠 표시:

CLI에서:

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

11단계. 디버그 조건을 제거합니다.

CLI에서:

```
# 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.