외부 인증으로 로컬 웹 인증 구성

목차

소개

이 문서에서는 9800 WLC(Wireless LAN Controller)에서 로컬 인증을 사용하여 로컬 웹 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

9800 WLC 컨피그레이션 모델에 대한 지식이 있는 것이 좋습니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco WLC 9800 시리즈
- 웹 인증에 대한 포괄적인 지식.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9800-CL WLC Cisco IOS® XE 버전 17.12.5
- Cisco Access Point C9117AXI입니다.

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

LWA(Local Web Authentication)는 WLC에서 구성할 수 있는 WLAN(Wireless Local Area Network) 인증 방법입니다. 사용자가 사용 가능한 네트워크 목록에서 WLAN을 선택하면 웹 포털로 리디렉션됩니다. 이 포털에서는 컨피그레이션에 따라 사용자에게 사용자 이름 및 비밀번호를 입력하거나, AUP(Acceptable Use Policy)를 수락하거나, 두 작업의 조합을 선택하여 연결을 완료하라는 프롬프트가 표시될 수 있습니다.

로그인 프로세스 중에 표시되는 4가지 유형의 웹 인증 페이지에 대한 자세한 내용은 로컬 웹 인증 구성 가이드를 참조하고 웹 인증 유형에 대해 사용 가능한 옵션을 검토하십시오. Types of Authentication(인증 유형) 섹션에서 Configure Local Web Authentication with External Authentication(외부 인증으로 로컬 웹 인증 구성) 가이드를 참조할 수도 있습니다.

매개변수 맵

매개변수 맵은 웹 인증을 활성화하는 WLC의 필수 구성 요소입니다. 인증 유형, 리디렉션 URL, 추가된 매개변수, 시간 제한, 사용자 지정 웹 페이지 등 웹 인증 프로세스의 다양한 측면을 제어하는 설정 집합으로 구성됩니다. 특정 SSID에 대한 웹 기반 인증을 활성화하고 관리하려면 이 맵을 WLAN 프로필에 연결해야 합니다.

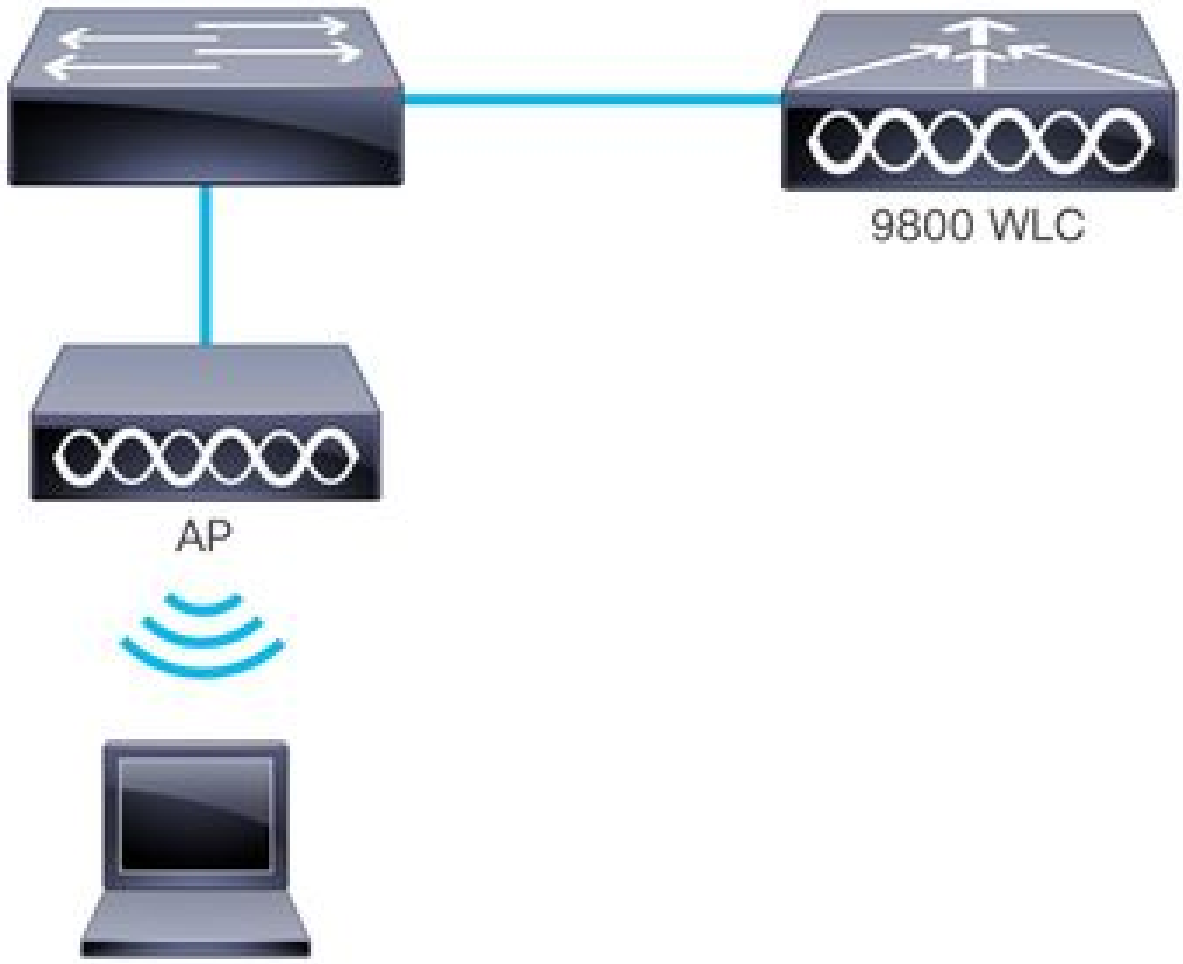
Wireless LAN Controller는 기본 전역 매개변수 맵과 함께 제공되지만 관리자는 특정 요구에 따라 웹 인증 동작을 사용자 지정하기 위해 사용자 지정 매개변수 맵을 만들 수 있습니다.

인증을 위한 데이터베이스

매개변수 맵이 사용자 이름 및 비밀번호를 사용하도록 구성된 경우 WLC에 로컬로 저장되는 인증 자격 증명을 정의해야 합니다. GUI를 통해 게스트 사용자 계정을 생성할 때 게스트 계정당 허용되는 최대 동시 로그인 수를 설정할 수 있습니다. 유효한 값의 범위는 0~64입니다. 여기서 0은 해당 게스트 사용자에 대해 무제한 동시 로그인이 허용됨을 나타냅니다.

LWA는 주로 소규모 구축을 위한 것입니다. 다른 인증 방법과의 통합을 지원합니다. 자세한 내용은 클라이언트의 지원되는 인증 조합을 확인할 수 있습니다.

이 이미지는 LWA의 일반 토폴로지를 나타냅니다.



로컬 인증을 사용하는 LWA의 일반 토폴로지

LWA의 네트워크 토폴로지에 있는 디바이스:

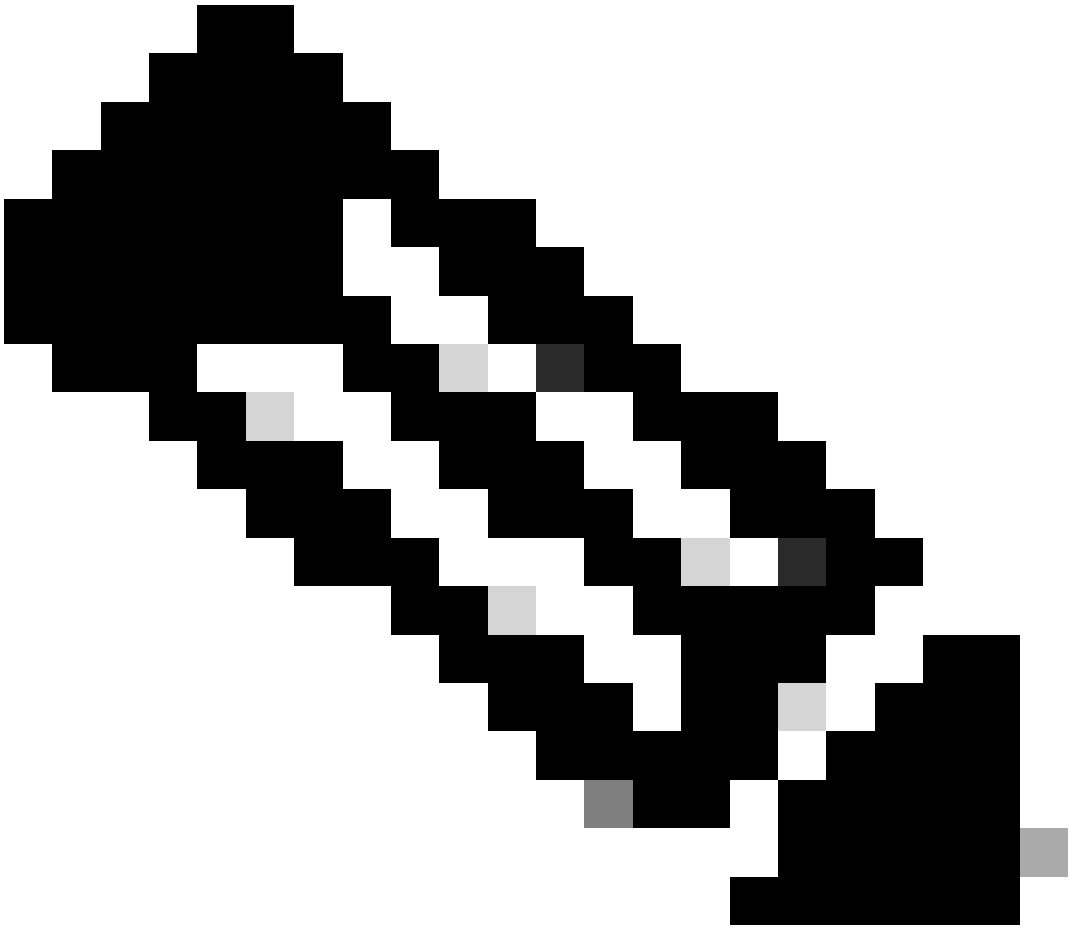
- 클라이언트/서플리컨트: WLAN, 나중에 DHCP 및 DNS 서버에 대한 연결 요청을 시작하고 WLC로부터의 통신에 응답합니다.
- 액세스 포인트: 스위치에 연결되어 게스트 WLAN을 브로드캐스트하고 게스트 디바이스에 무선 연결을 제공합니다. 게스트 사용자가 유효한 자격 증명을 입력하여 인증을 완료하기 전에 DHCP 및 DNS 트래픽을 허용하거나, AUP를 수락하거나, 두 작업의 조합을 허용합니다.
- WLC/인증자: AP 및 클라이언트 디바이스를 관리합니다. WLC는 리디렉션 URL을 호스팅하며 매개변수 맵을 구성할 때 기본적으로 생성되는 트래픽 및 트래픽을 제어하는 ACL(Access Control List)을 적용합니다. 게스트 사용자의 HTTP 요청을 가로채고 사용자가 인증해야 하는 웹 포털(로그인 페이지)로 리디렉션합니다. WLC는 사용자 자격 증명을 캡처하고 게스트를 인증하며 로컬 데이터베이스를 검사하여 자격 증명 유효성을 확인합니다.
- 인증 서버: 이 시나리오에서 WLC는 인증 서버로 작동합니다. 게스트 사용자 자격 증명을 검증하고 그에 따라 네트워크 액세스를 허용하거나 거부합니다.

구성

CLI에서 로컬 인증을 사용하는 로컬 웹 인증

로컬 인증을 위한 방법 목록

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



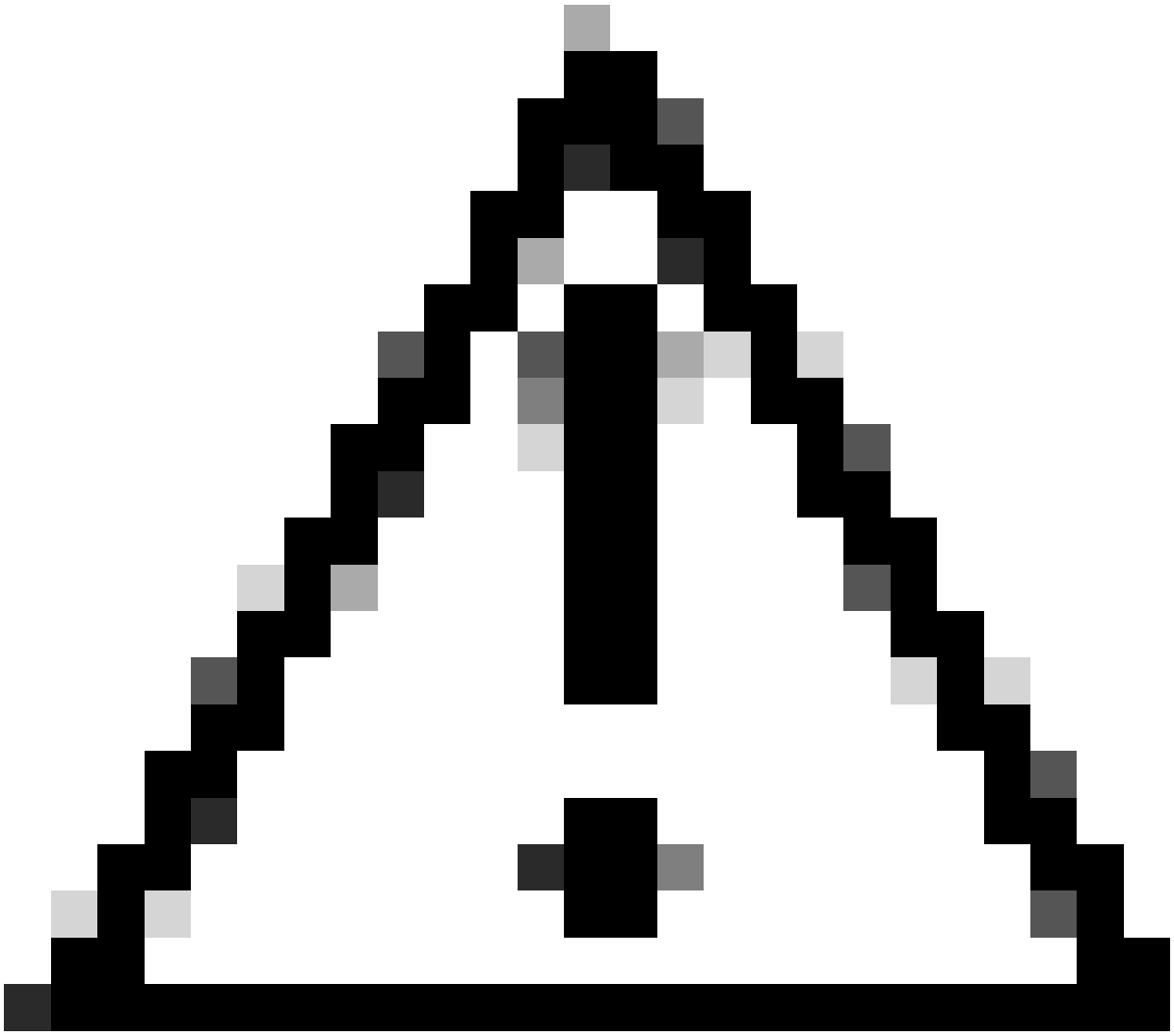
참고: Local Login Method List(로컬 로그인 방법 목록)가 작동하려면 WLC에 aaa

---

authorization network default local(aaa 권한 부여 네트워크 기본 로컬) 컨피그레이션이 있는지 확인합니다. 이는 WLC가 네트워크에 사용자를 인증하기 때문에 필요합니다.

매개변수 맵

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint



9800WLC(config-params-parameter-map)#webauth-http-enable


9800WLC(config-params-parameter-map)#end
```



주의: 가상 IP는 RFC 5737에 제안된 라우팅 불가 주소여야 합니다. 기본적으로 IP 192.0.2.1이 설정됩니다. Cisco Catalyst 9800 Series 구성 모범 사례의 가상 IP 주소에 대한 자세한 내용을 참조하십시오. AireOs에서는 IP가 1.1.1.1을 사용하는 경우가 대부분이었습니다. 이는 공용 IP가 되었기 때문에 더 이상 권장되지 않습니다.

여러 매개 변수 맵을 만드는 기능을 통해 맞춤형 플로우를 구현할 수 있습니다. 각 WLAN에 대한 맞춤형 웹 페이지 및 특정 프레젠테이션 매개변수 전역 매개변수 맵은 신뢰 지점 및 따라서 WLC가 리디렉션 포털의 클라이언트에 제공하는 인증서를 결정합니다. 또한 리디렉션 포털의 HTTP/HTTPS, 가상 IP 주소의 도메인 또는 호스트 이름 확인 등 가로채기된 클라이언트 트래픽의 유형을 제어합니다. 이러한 분리를 통해 전역 맵은 인증서 표시 및 트래픽 가로채기와 같은 주요 설정을 처리하는 반면, 사용자 정의 매개변수 맵은 WLAN당 세분화된 환경을 제공합니다.

WLAN 보안 매개변수

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

정책 프로필 생성

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

정책 태그 생성

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless tag policy
```

```
9800WLC(config-policy-tag)#wlan LWA_LA policy
```

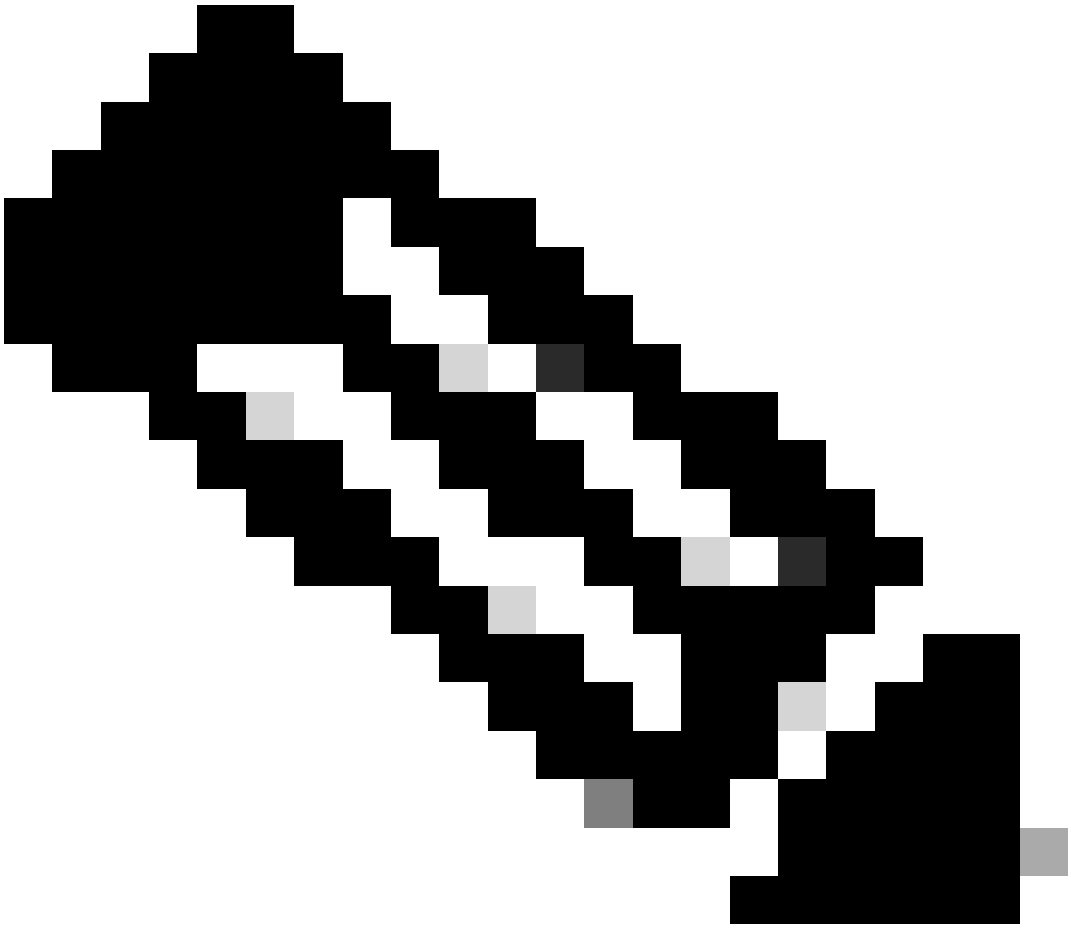
```
9800WLC(config-policy-tag)# end
```

AP에 정책 태그 할당

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap


       >


9800WLC(config-ap-tag)#policy-tag POLICY_TAG


9800WLC(config-ap-tag)#end
```

게스트 사용자 이름 생성

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description


        guest-user lifetime year 0 month 11 day 30 hour 23


9800WLC(config-user-name)#end
```

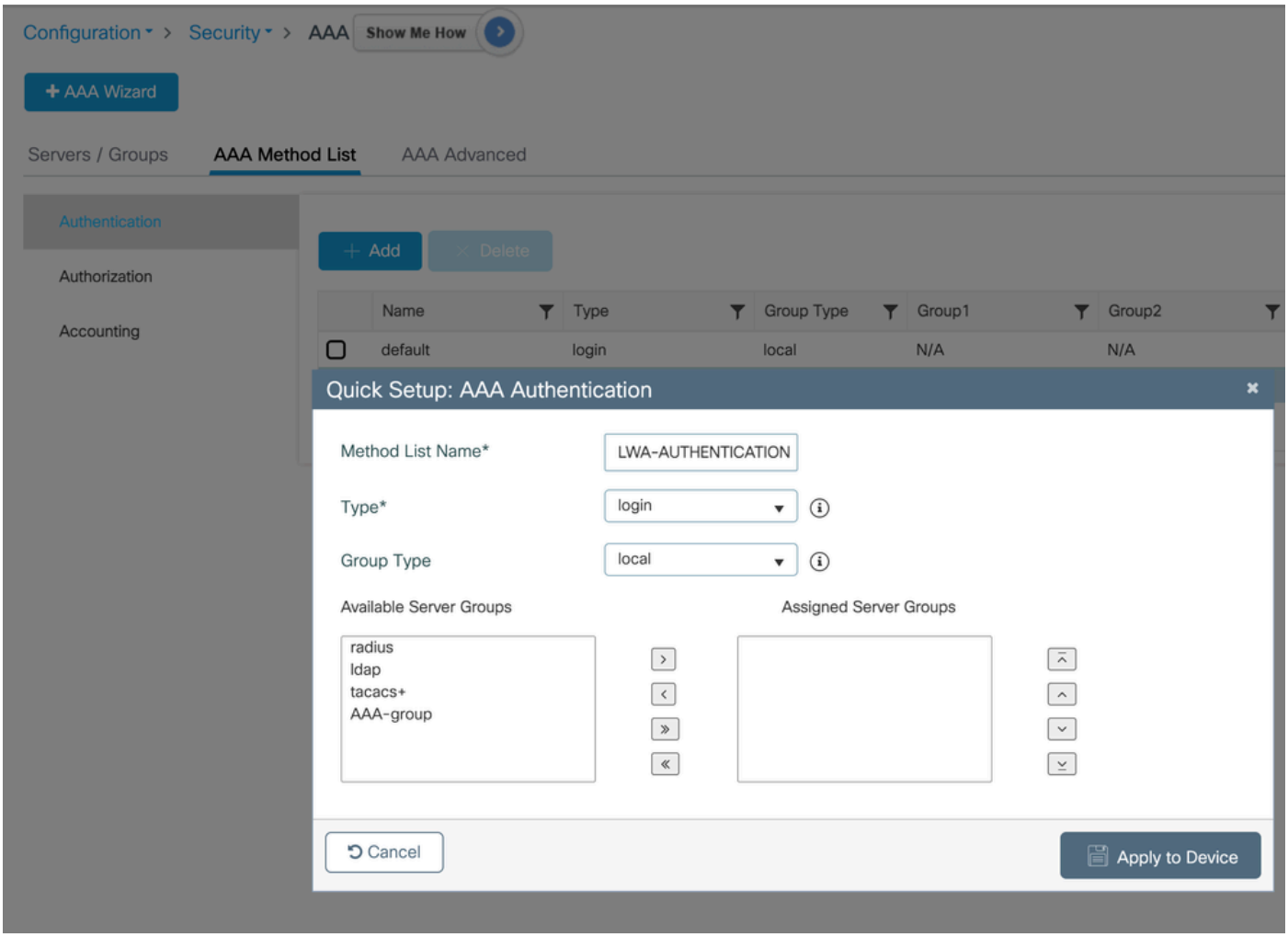


참고: 게스트 사용자의 수명을 설정할 때 연도를 1로 설정하면 최대 수명이 1년이므로 이후의 매개변수(월, 일, 시간 및 분)를 지정할 수 없습니다.

WebUI를 통한 로컬 인증을 통한 로컬 웹 인증

로컬 인증을 위한 방법 목록

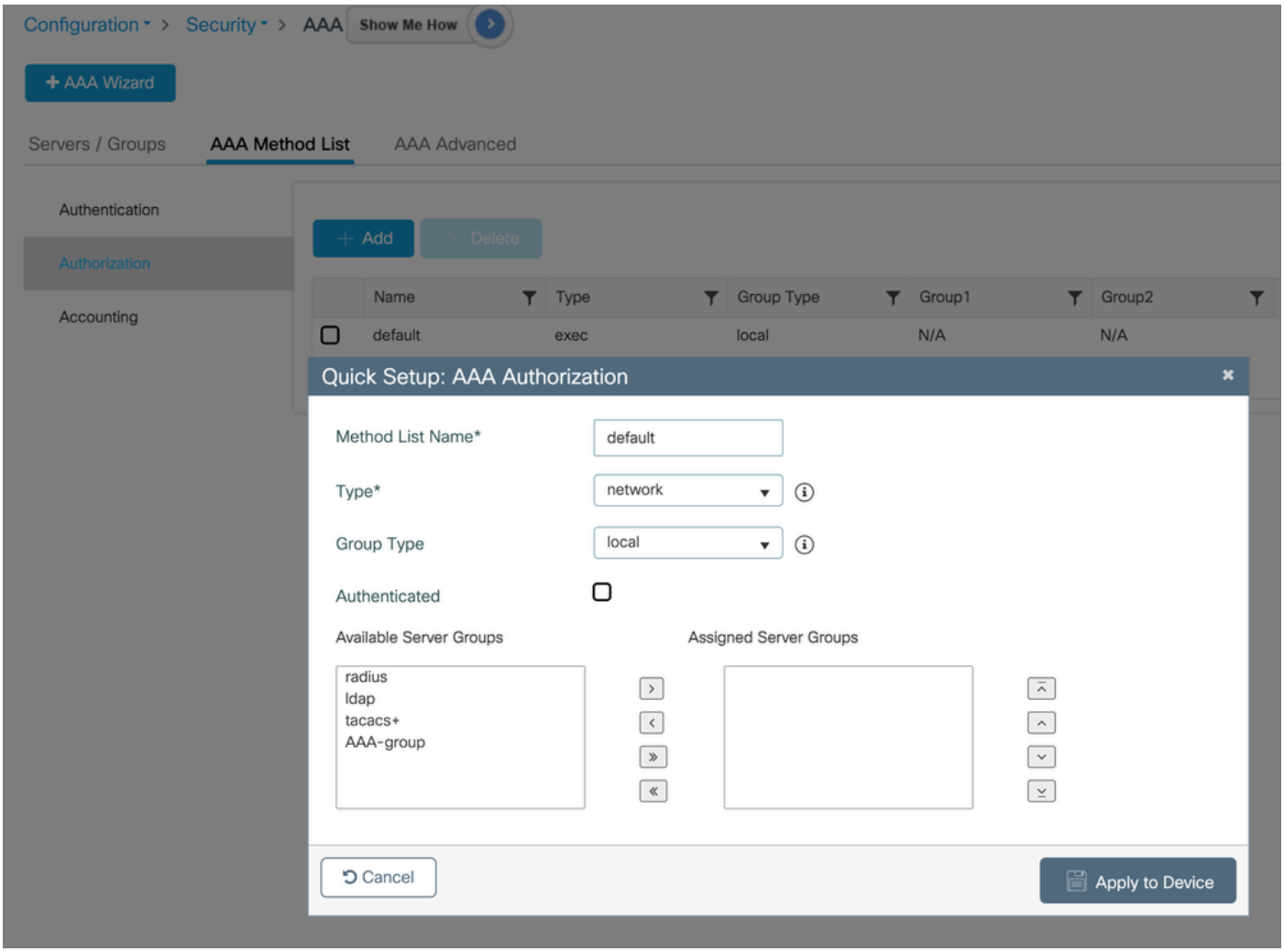
Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 방법 목록) > Authentication(인증) > Add(추가)로 이동하여 나중에 WLAN 컨피그레이션에서 사용할 방법 목록을 생성합니다.



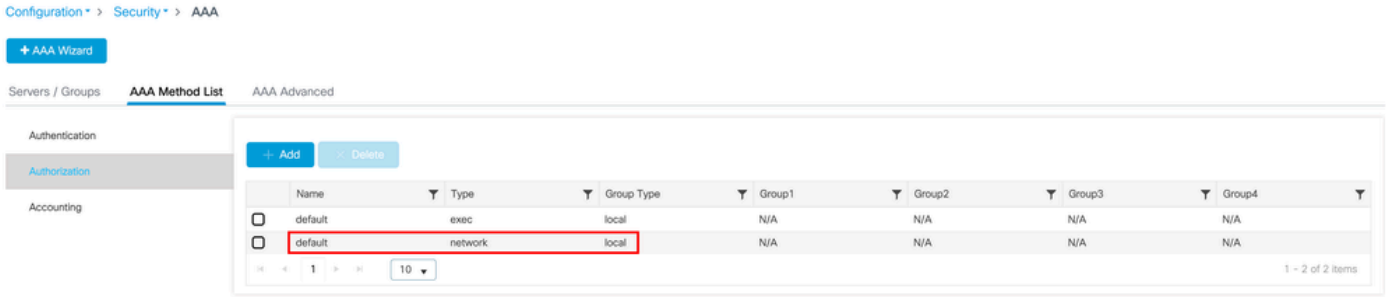
Apply to Device(디바이스에 적용)를 클릭한 후 AAA 메서드 목록 생성을 확인합니다. 

로컬 인증 방법 목록이 있는지 확인합니다. 이 목록은 생성된 로컬 로그인 방법 목록이 작동하기 위한 요구 사항입니다.

Configuration(구성) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여) > Add(추가)

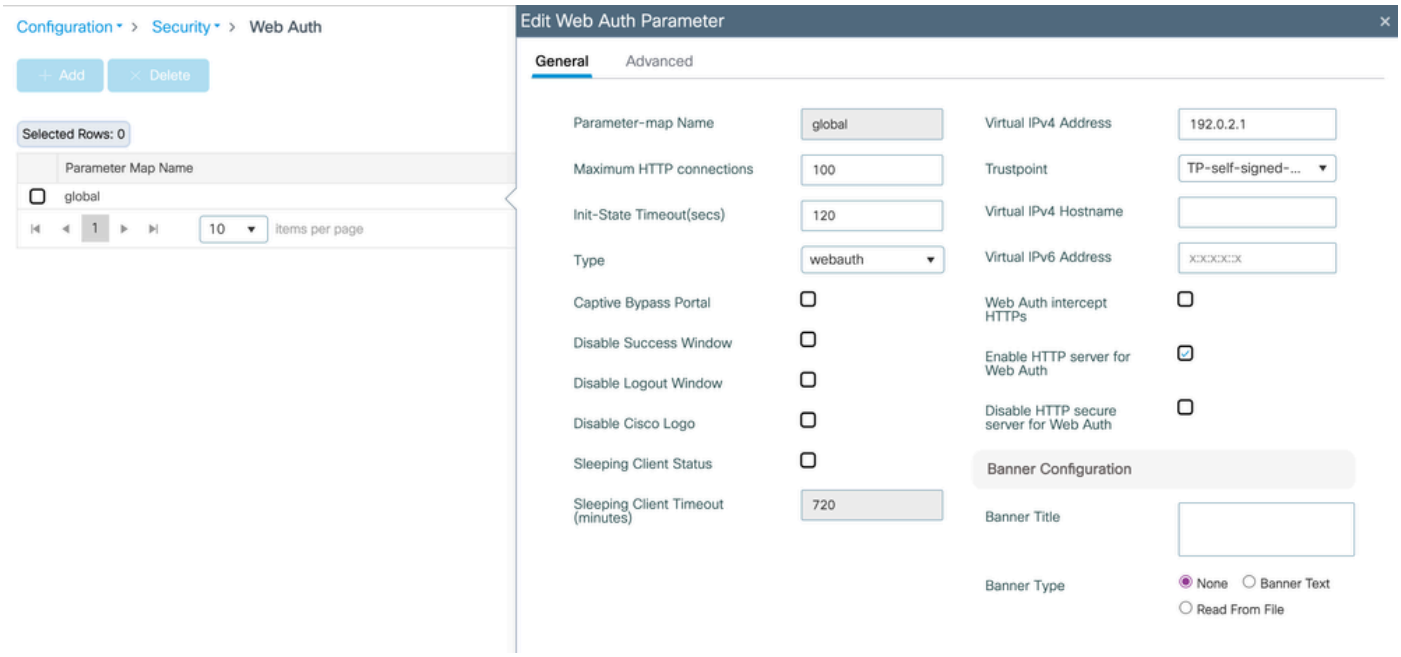


Apply to Device(디바이스에 적용)를 클릭한 후 AAA 메서드 목록 생성을 확인합니다.

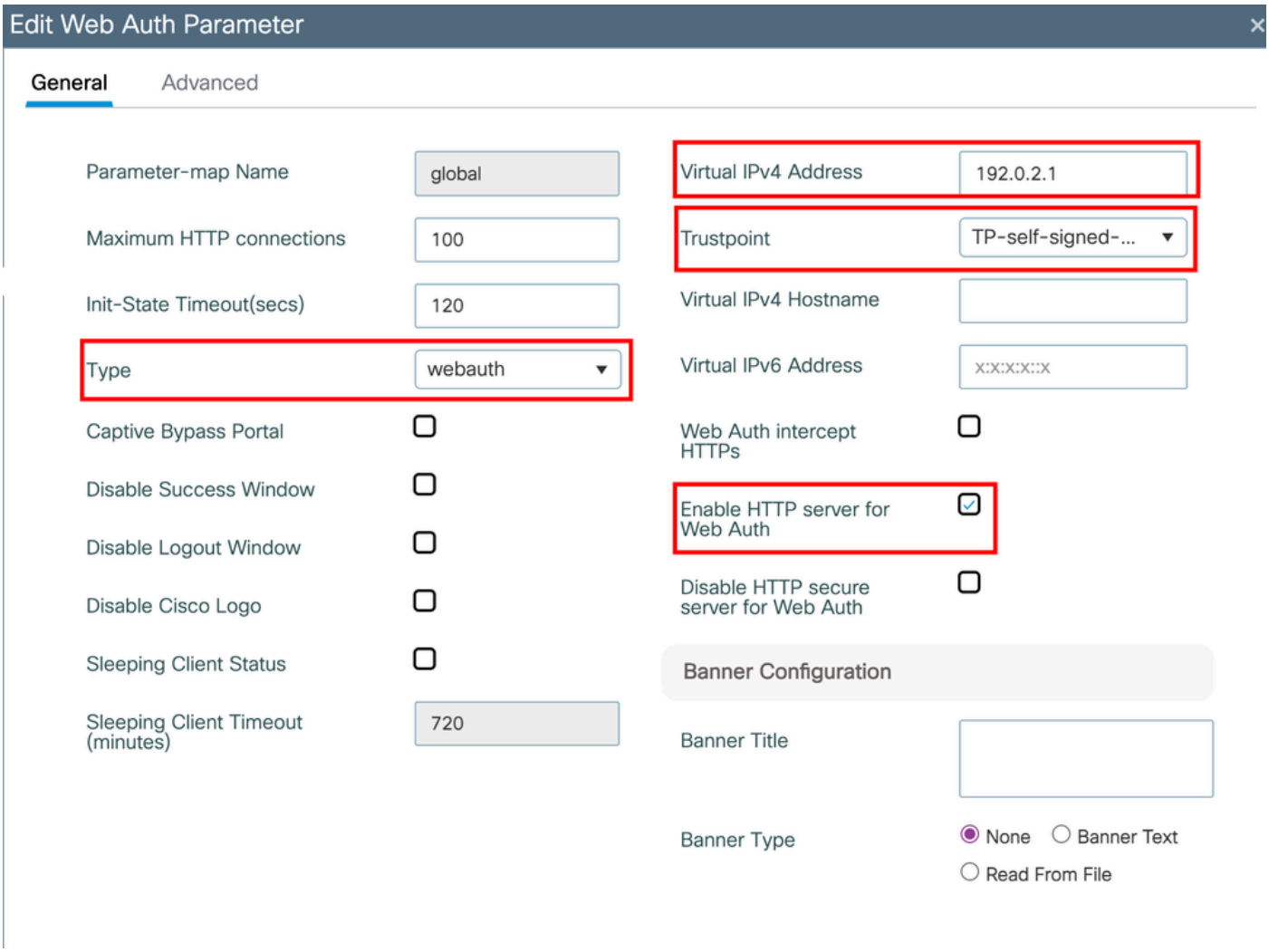


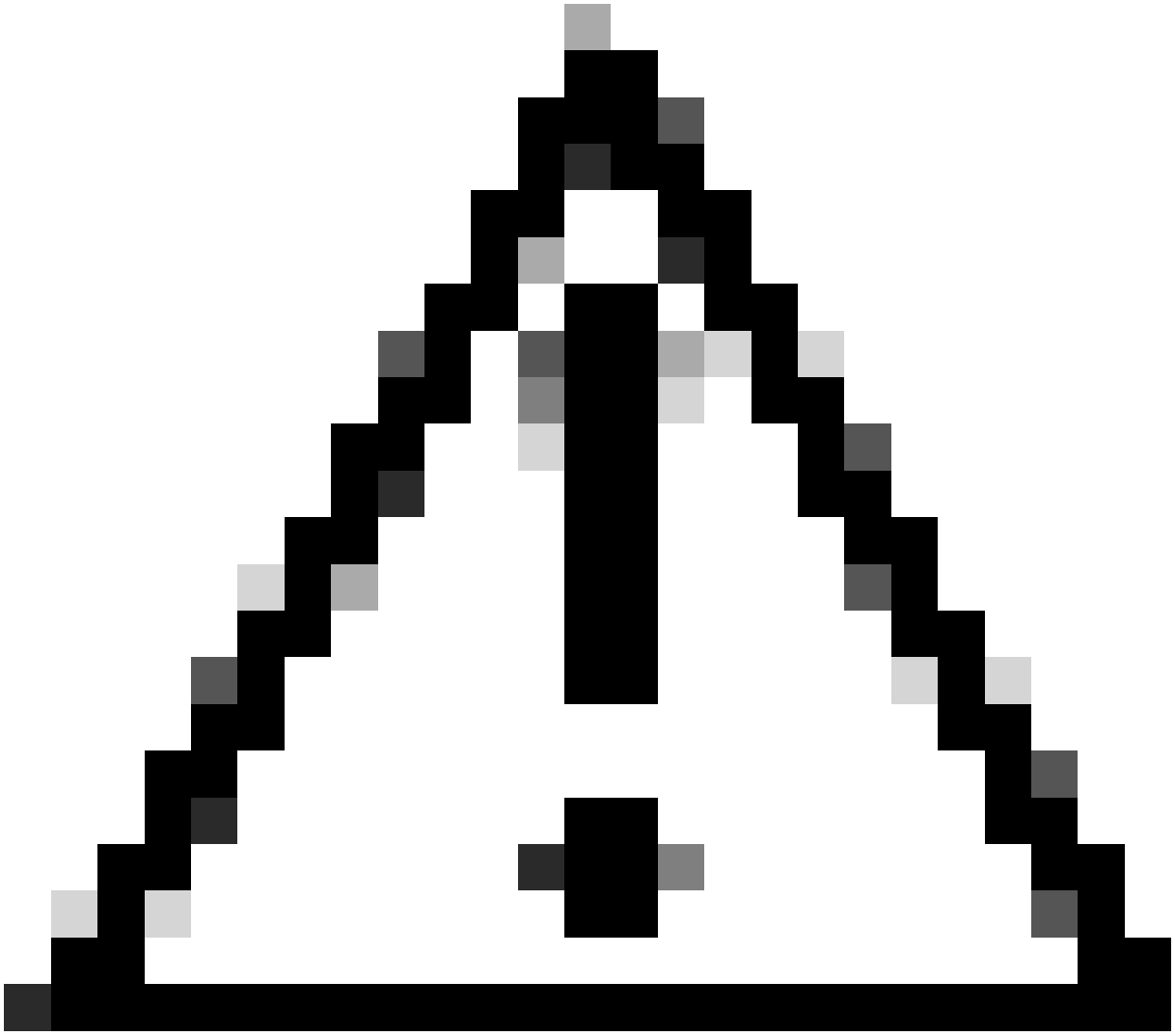
매개변수 맵

Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)에서 전역 매개변수 맵을 편집합니다.



사용할 웹 인증 유형, 가상 IP 및 WLC가 웹 포털에 제공하는 신뢰 지점을 선택합니다. 이 경우 자체 서명 인증서가 선택되어 있으며, 이는 LSC(Locally Significant Certificate)이며 인터넷에서 인식 가능한 CA가 서명하지 않기 때문에 "사용자 연결이 사설 네트워크가 아닙니다 ::ERR_CERT_AUTHORITY_INVALID" 종류의 면책조항이 발생할 수 있습니다. 이를 수정하려면 서명한 타사 인증서를 사용하십시오. 자세한 내용은 Catalyst 9800 WLC에서 CSR 인증서 생성 및 다운로드를 참조하거나, Cisco 9800 WLC에서 WebAuth 및 WebAdmin용 업로드 및 트러스포인트 생성 Renew Certificates를 설명하는 비디오 옵션이 있습니다 | 보안 무선 LAN 컨트롤러 설정.

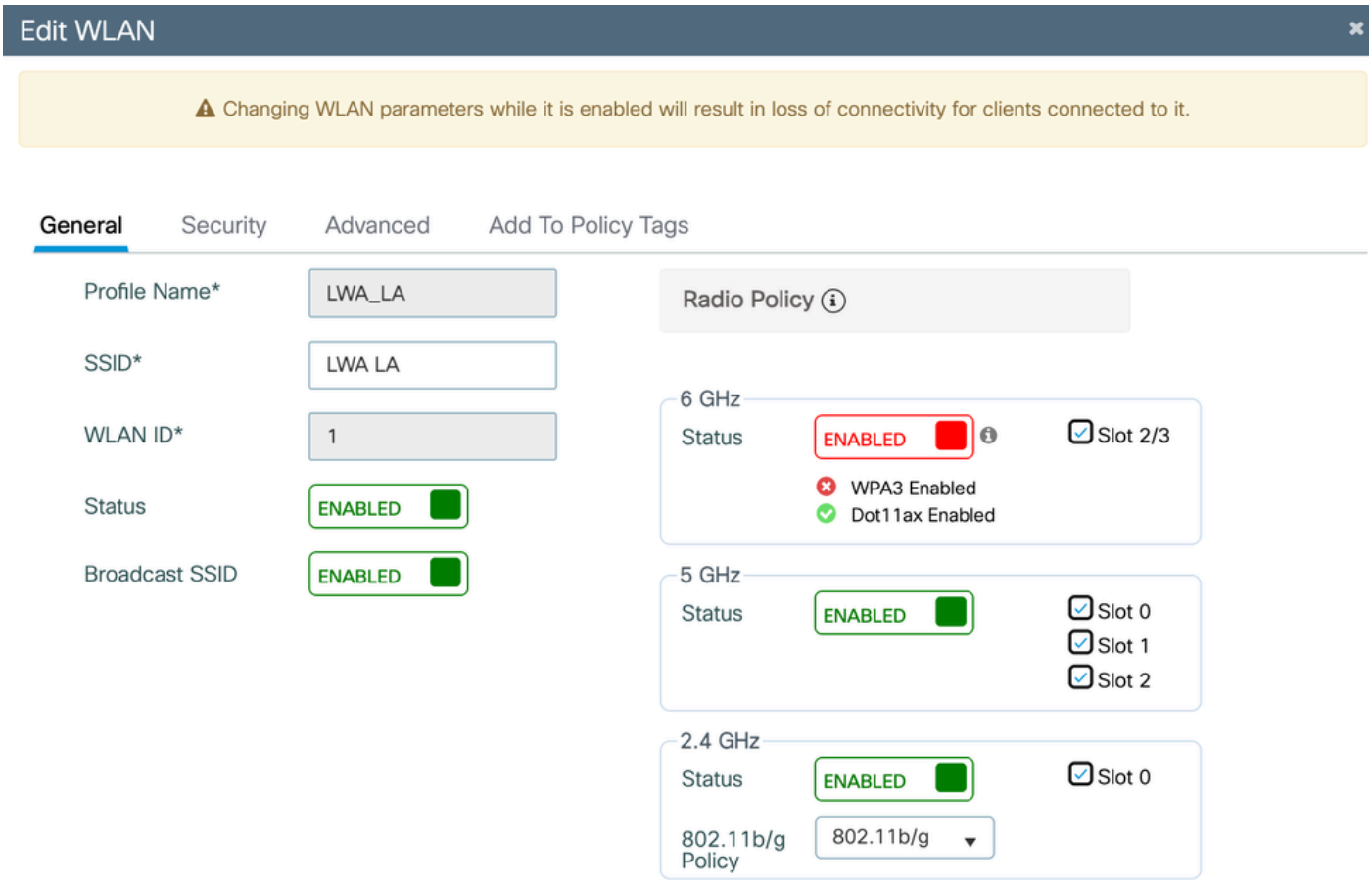

Edit Web Auth Parameter
General
Advanced
Parameter-map Name
global
Maximum HTTP connections
100
Init-State Timeout(secs)
120
Type
webauth
Captive Bypass Portal
Disable Success Window
Disable Logout Window
Disable Cisco Logo
Sleeping Client Status
Sleeping Client Timeout (minutes)
720
Virtual IPv4 Address
192.0.2.1
Trustpoint
TP-self-signed-...
Virtual IPv4 Hostname
Virtual IPv6 Address
x:x:x:x::x
Web Auth intercept HTTPs
Enable HTTP server for Web Auth
Disable HTTP secure server for Web Auth
Banner Configuration
Banner Title
Banner Type
None
Banner Text
Read From File



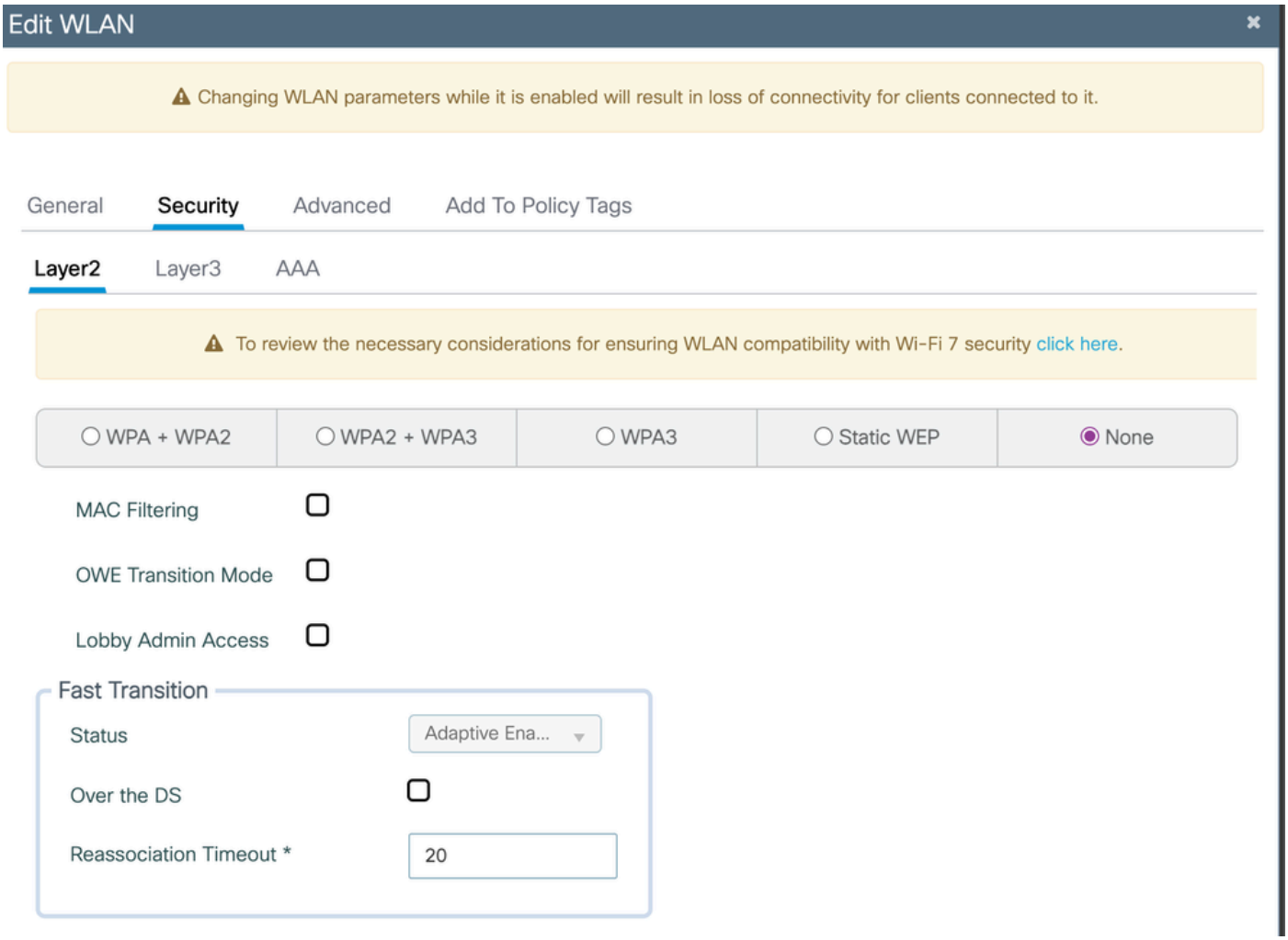
주의: 9800에서 HTTP를 전역적으로 비활성화한 경우 Cisco에서 이러한 프로세스의 종속성을 분리한 후 Enable HTTP server for Web Auth(웹 인증에 HTTP 서버 활성화)를 선택했는지 확인합니다. 클라이언트 또는 서 플리 컨 트가 HTTP 연결 프로세스를 시작 해야 하고 웹 포털을 제시 하는 컨트롤러에 의해 세션 이 차단 됩니다. 따라서 대부분의 구축에서 이 설정이 불필요하고 컨트롤러 CPU 사용률을 증가시켜 성능에 영향을 미칠 수 있으므로 반드시 필요한 경우가 아니면 웹 인증 가로채기 HTTPS를 활성화하지 않는 것이 좋습니다.

WLAN 보안 매개변수

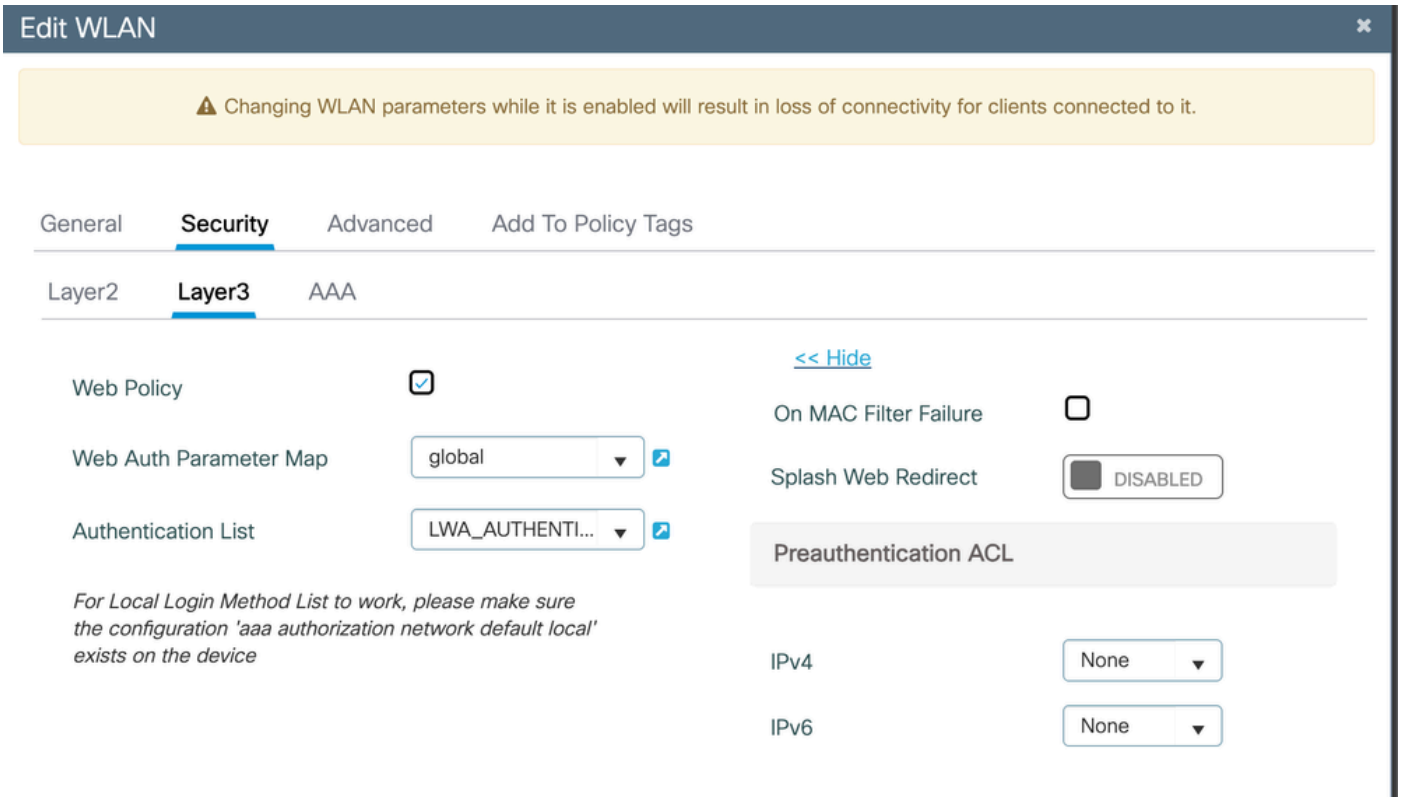
Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLANs(WLAN)로 이동하고 Add(추가)를 클릭합니다.



Security(보안) 탭에서 Layer2에 대해 None(없음)을 선택합니다.

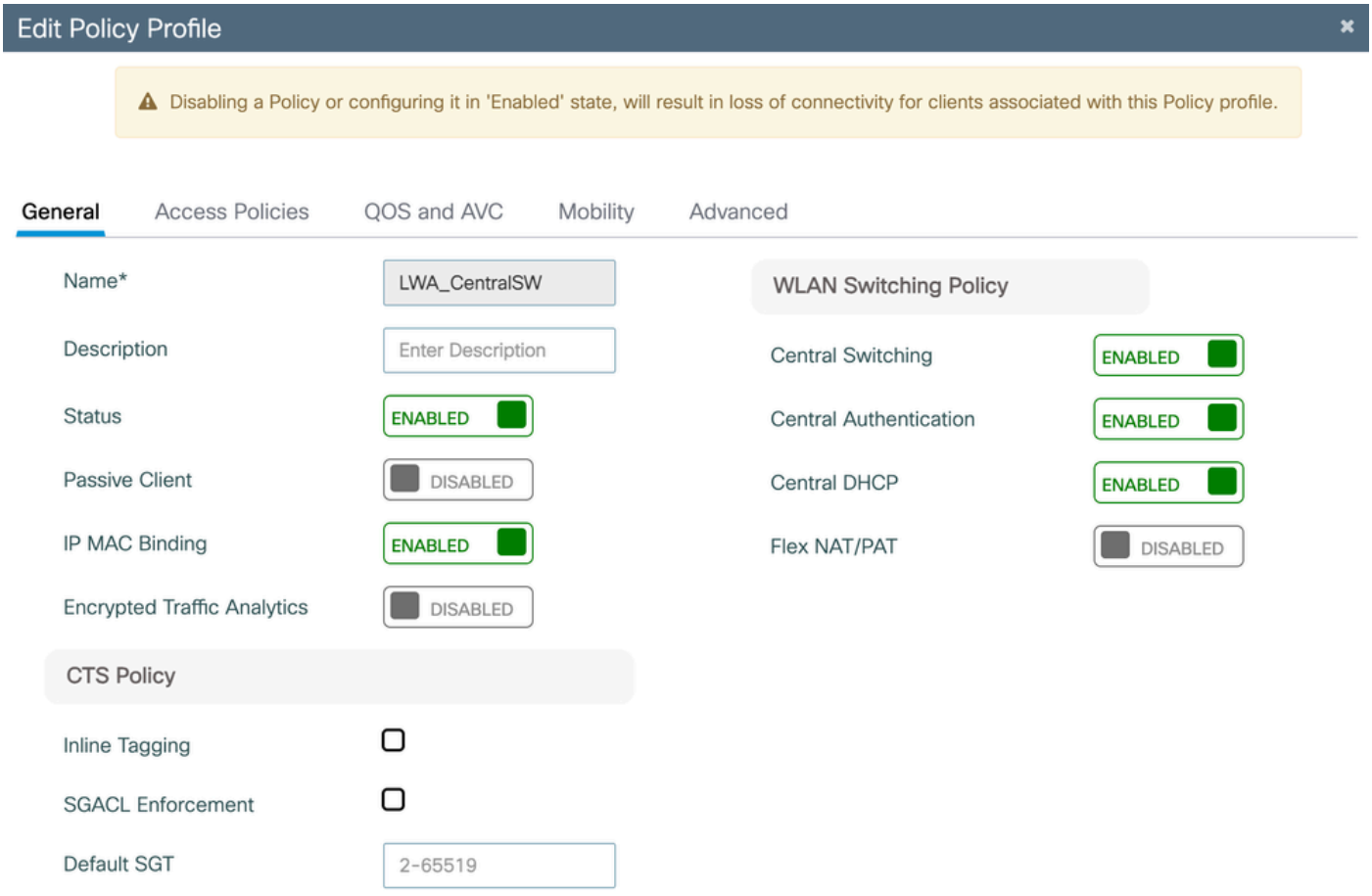


Security(보안) 탭의 Layer3(레이어 3)에서 Web Policy(웹 정책) 상자를 선택합니다. 드롭다운 메뉴와 Authentication List(인증 목록)에서 이전에 구성한 매개변수 맵을 선택합니다.

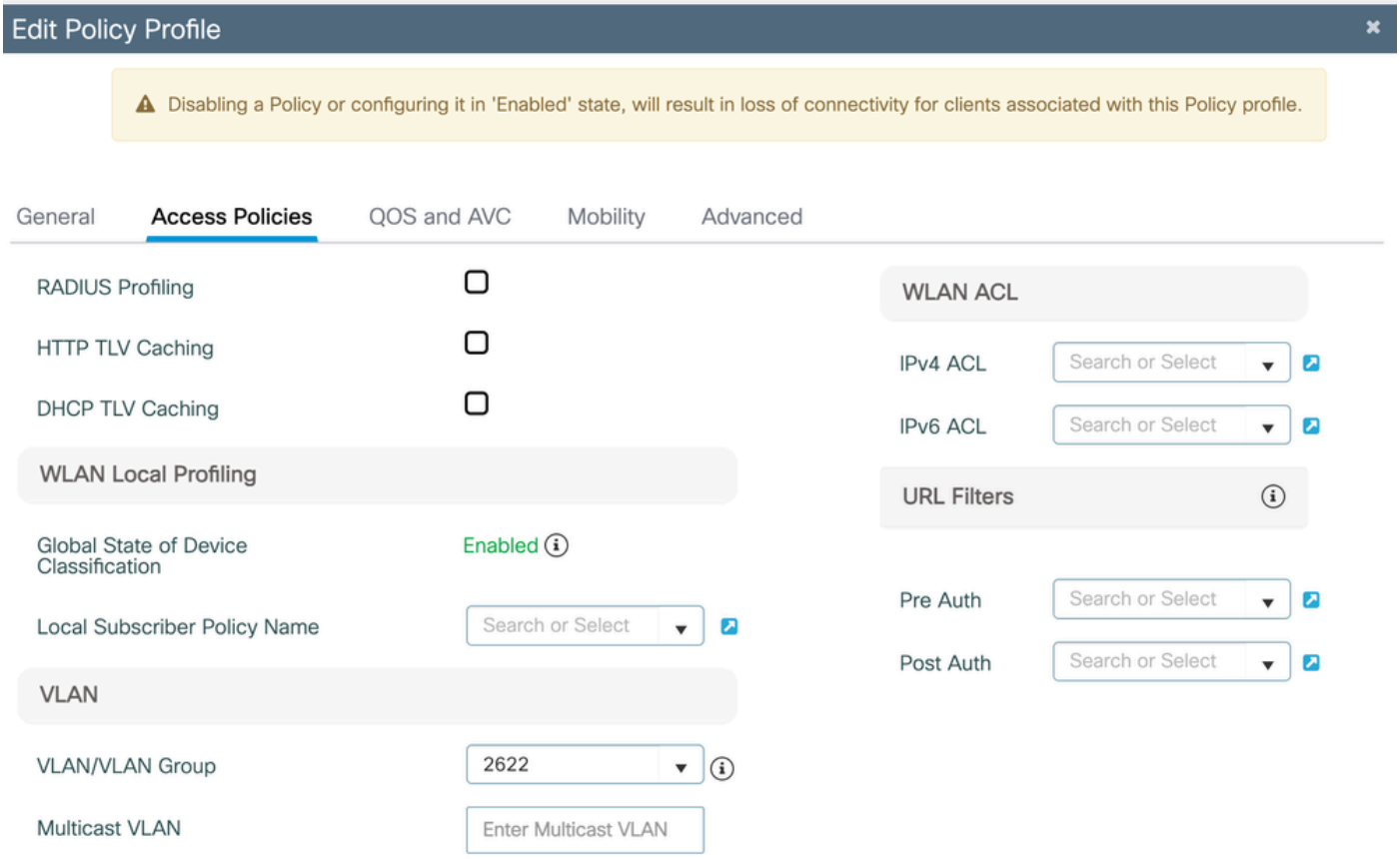


정책 프로필 생성

WLAN 프로필에 연결할 정책 프로필을 생성하려면 Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다.

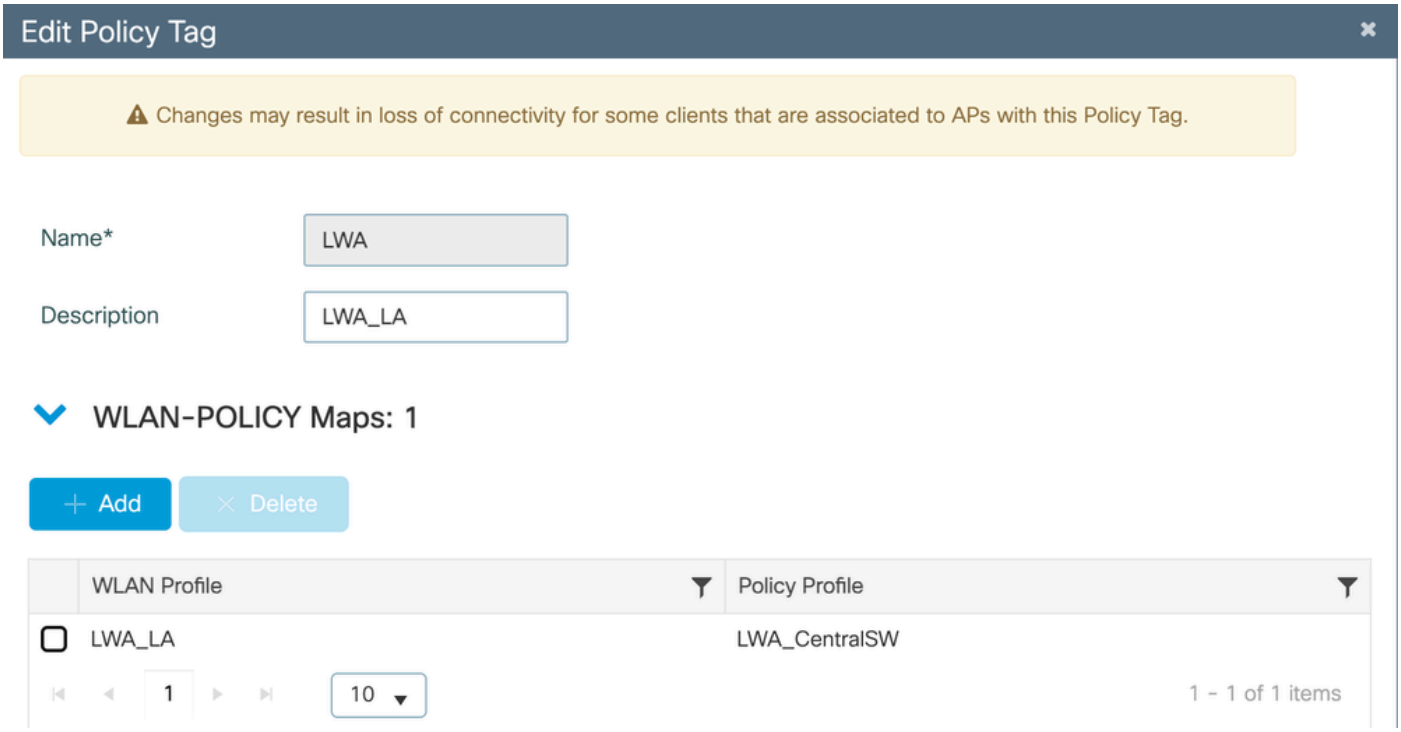


Access Policies(액세스 정책) 탭에서 클라이언트/신청자가 IP를 요청할 VLAN을 선택합니다.



정책 태그 생성

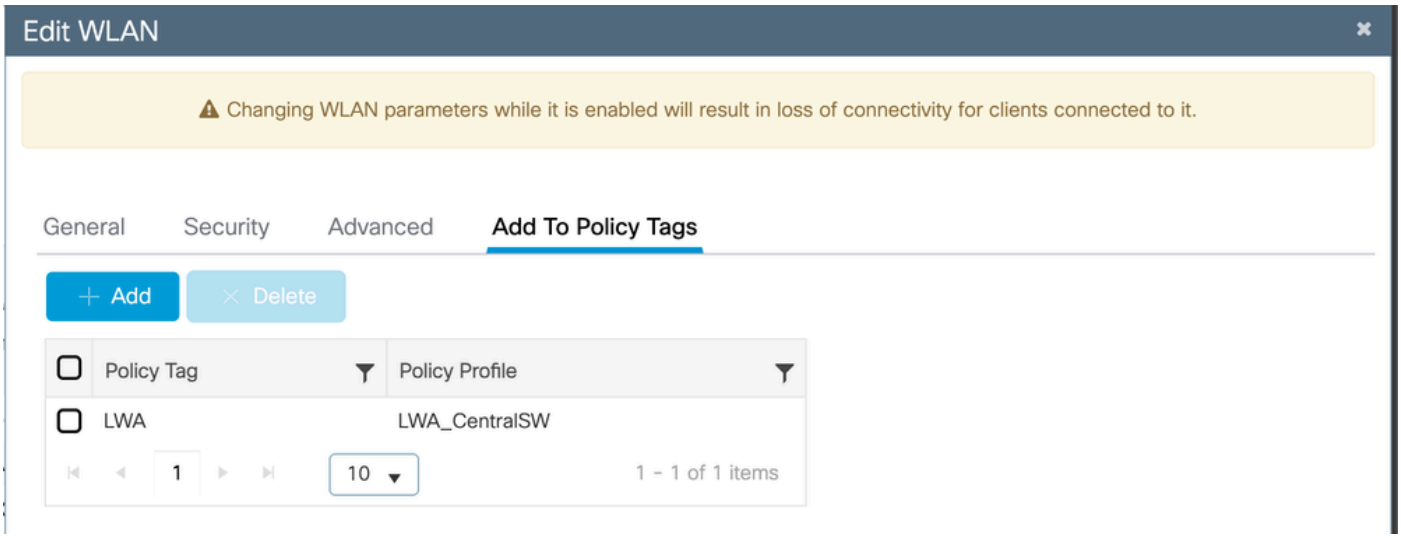
이 컨피그레이션 가이드에서는 LWA라는 사용자 지정 정책 태그를 생성했습니다.



WLAN 및 정책 프로필 연결

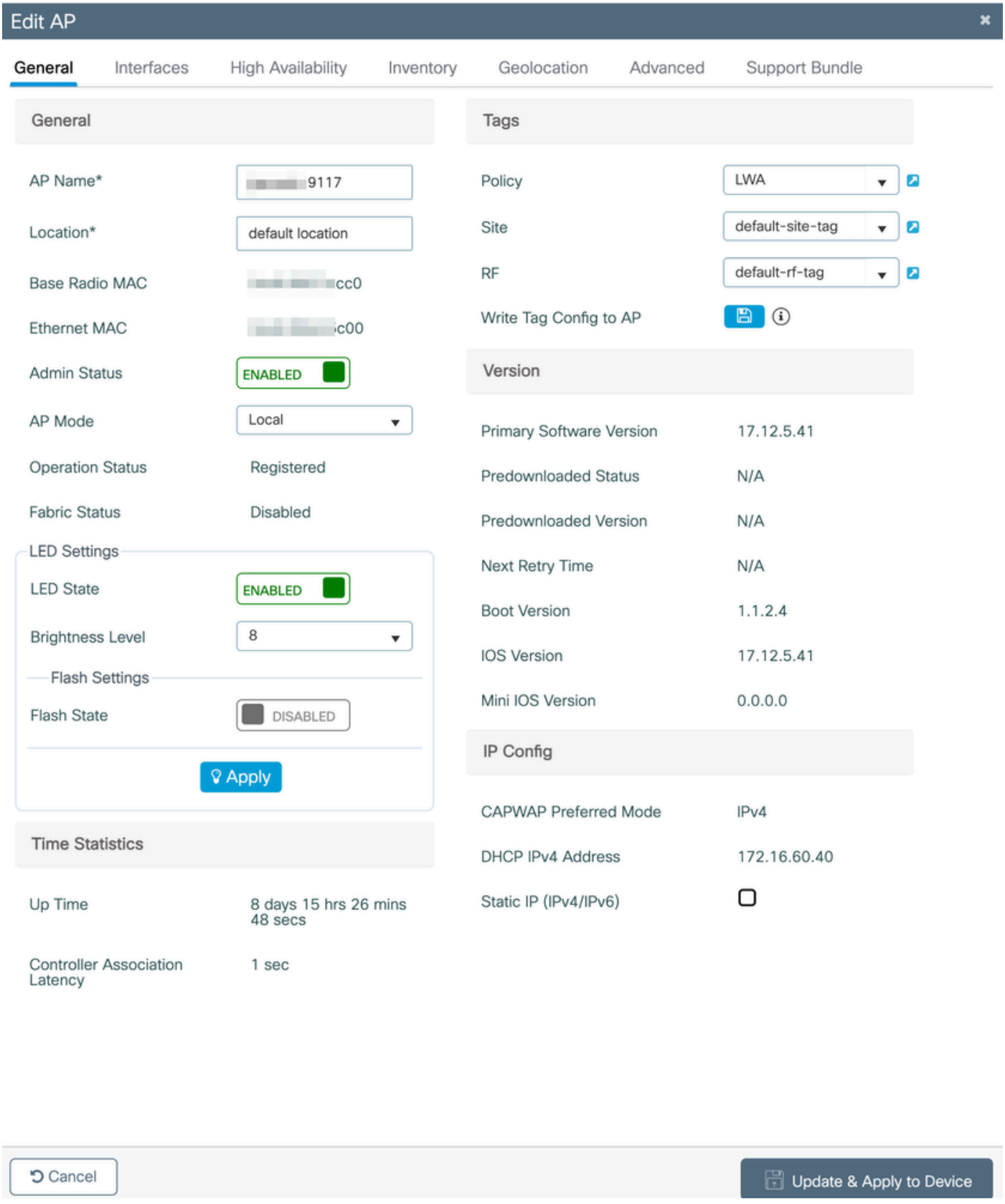
정책 프로파일과 WLAN에서 스위칭 정책을 연결하려면 Configuration(컨피그레이션) > Tags &

Profiles(태그 및 프로파일) > WLANs(WLAN)로 이동하고, WLAN Profile(WLAN 프로파일)을 선택한 후 Add to Policy Tags(정책 태그에 추가)를 클릭합니다.



AP에 정책 태그 할당

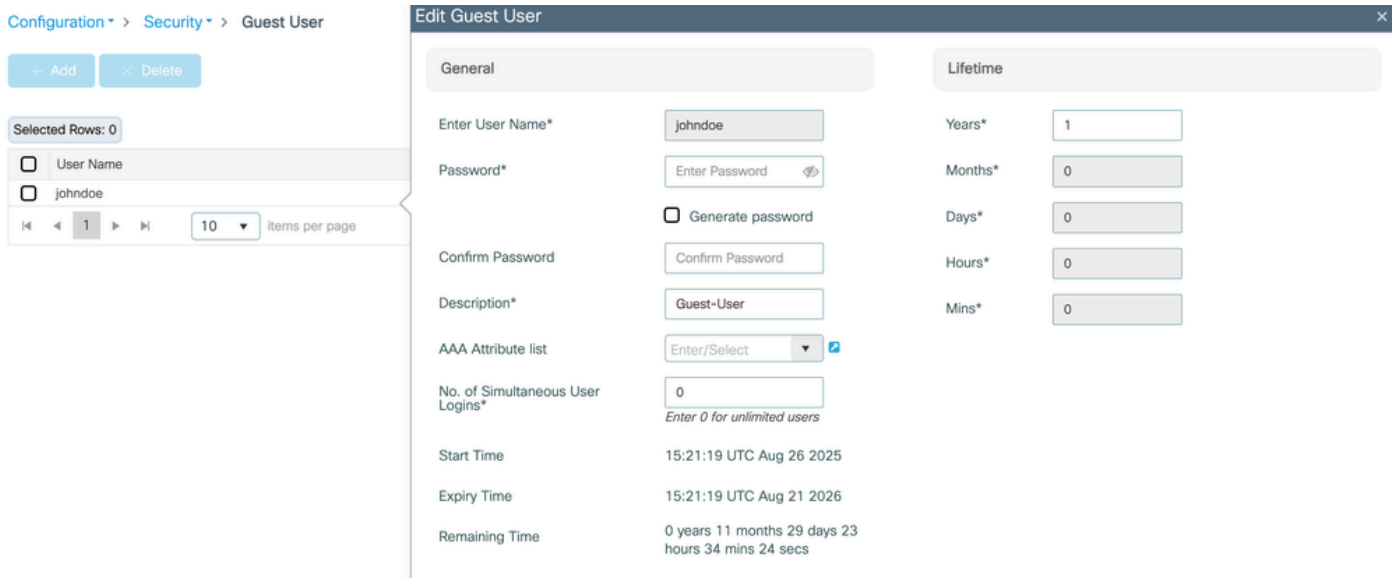
정책 태그가 생성된 AP에 태그를 지정하려면 Configuration(구성) > Wireless(무선) > Access Points(액세스 포인트)로 이동하여 AP를 선택하고 General(일반) 탭의 오른쪽에 AP에서 사용하는 태그가 있습니다.



게스트 사용자 이름 생성

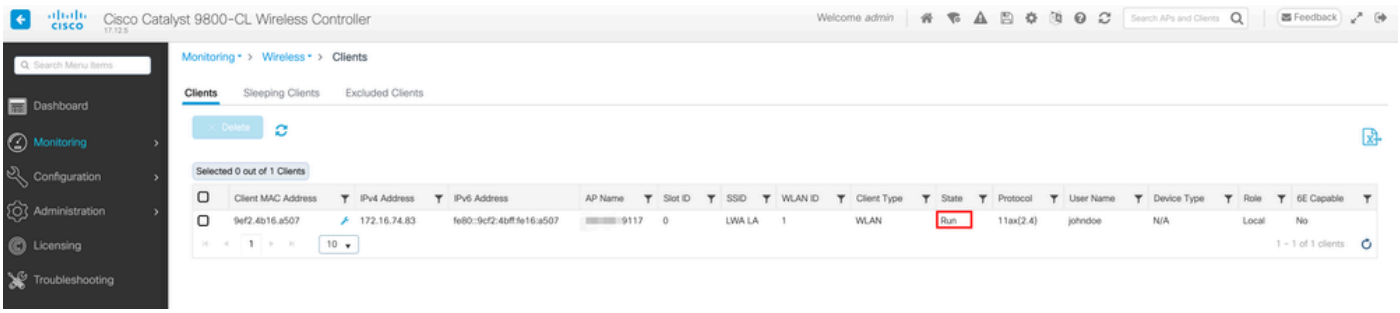
매개변수 맵에서 webauth 유형을 선택한 경우 Guest User-Name을 생성하려면 Configuration(컨피그레이션) > Security(보안) > Guest User(게스트 사용자)로 이동해야 합니다.

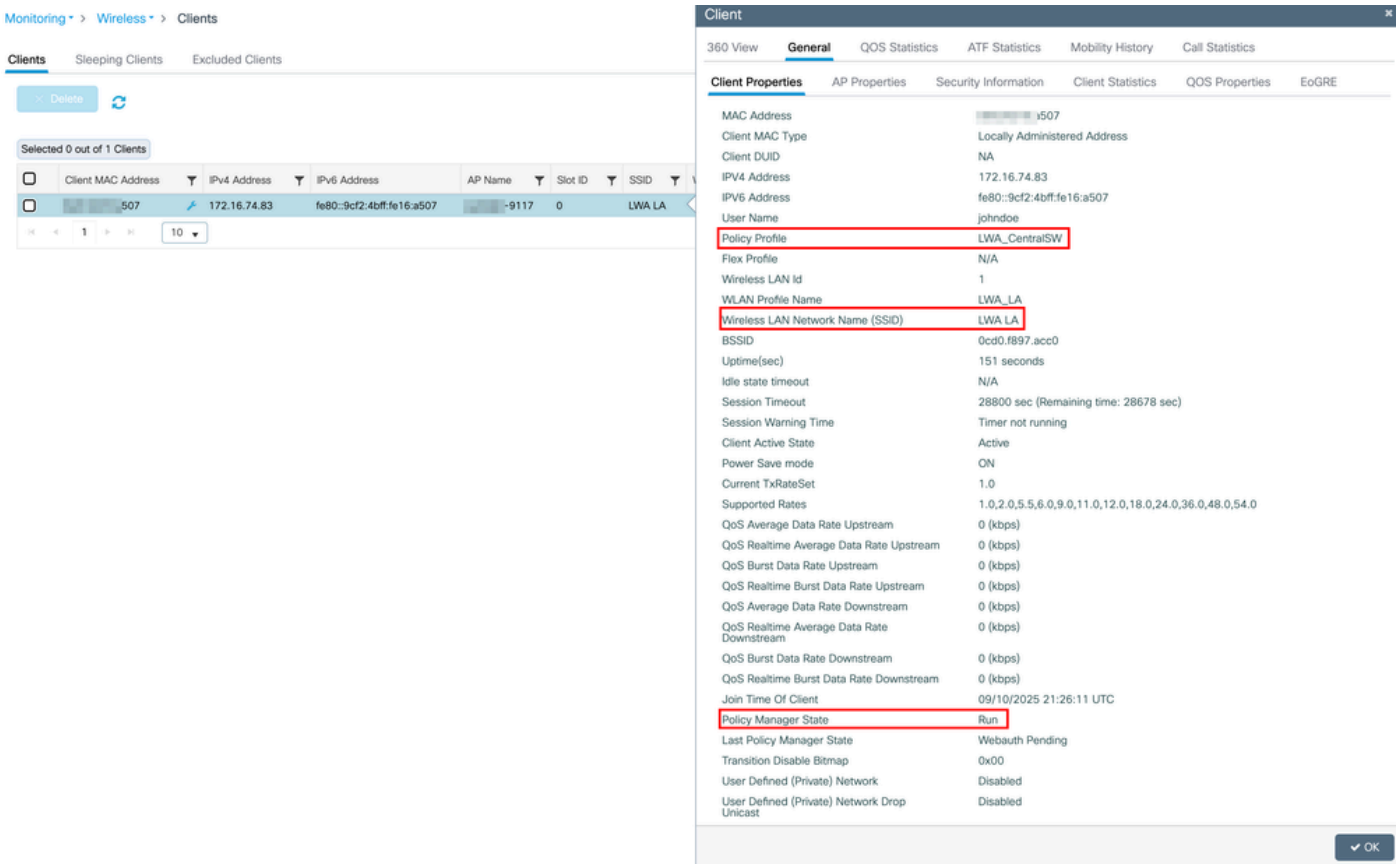
사용자의 최대 수명은 1년입니다. 사용 가능한 옵션으로 다르게 지정할 수 있습니다.



다음을 확인합니다.

GUI 사용





CLI를 통해

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name       Type ID State Protocol  Method    Role
-----------------------------------------------------------------------------------------------------------------
9ef2.4b16.a507   xxxxx-9117 WLAN 1  Run   11ax(2.4) Web Auth  Local
9800WLC#show wireless client mac-address


        detail


Client MAC Address : 9ef2.4b16.a507


Client MAC Type : Locally Administered Address


Client DUID: NA


Client IPv4 Address : 172.16.74.83


Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507


Client Username : johndoe
```

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

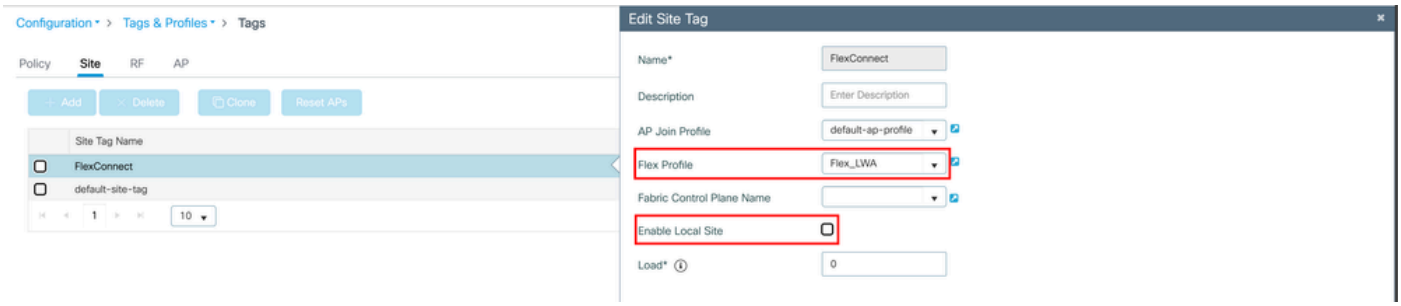
Signal to Noise Ratio : 4 dB

Fabric status : Disabled

```
Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED
```

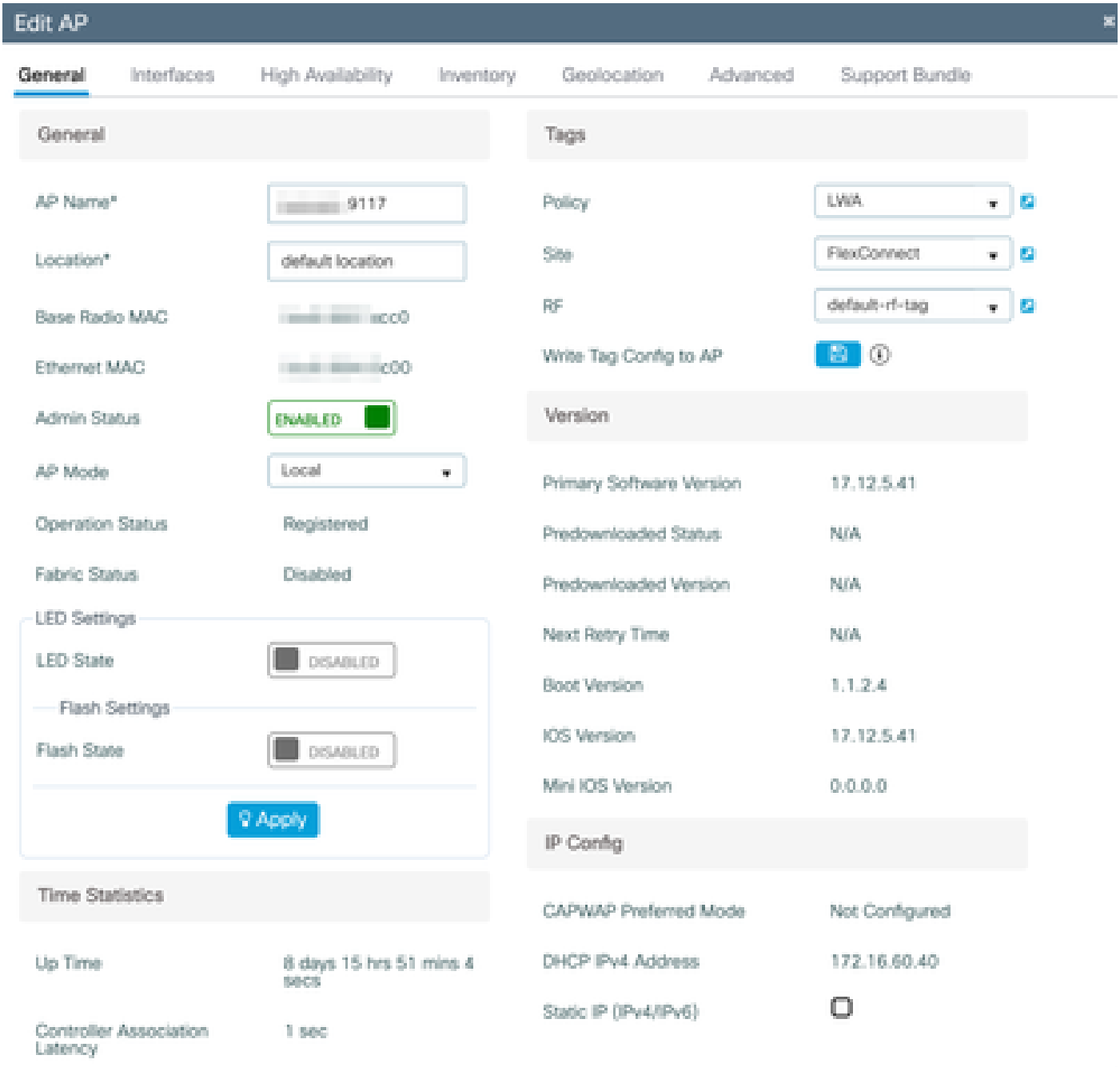
FlexConnect 로컬 스위칭의 로컬 웹 인증

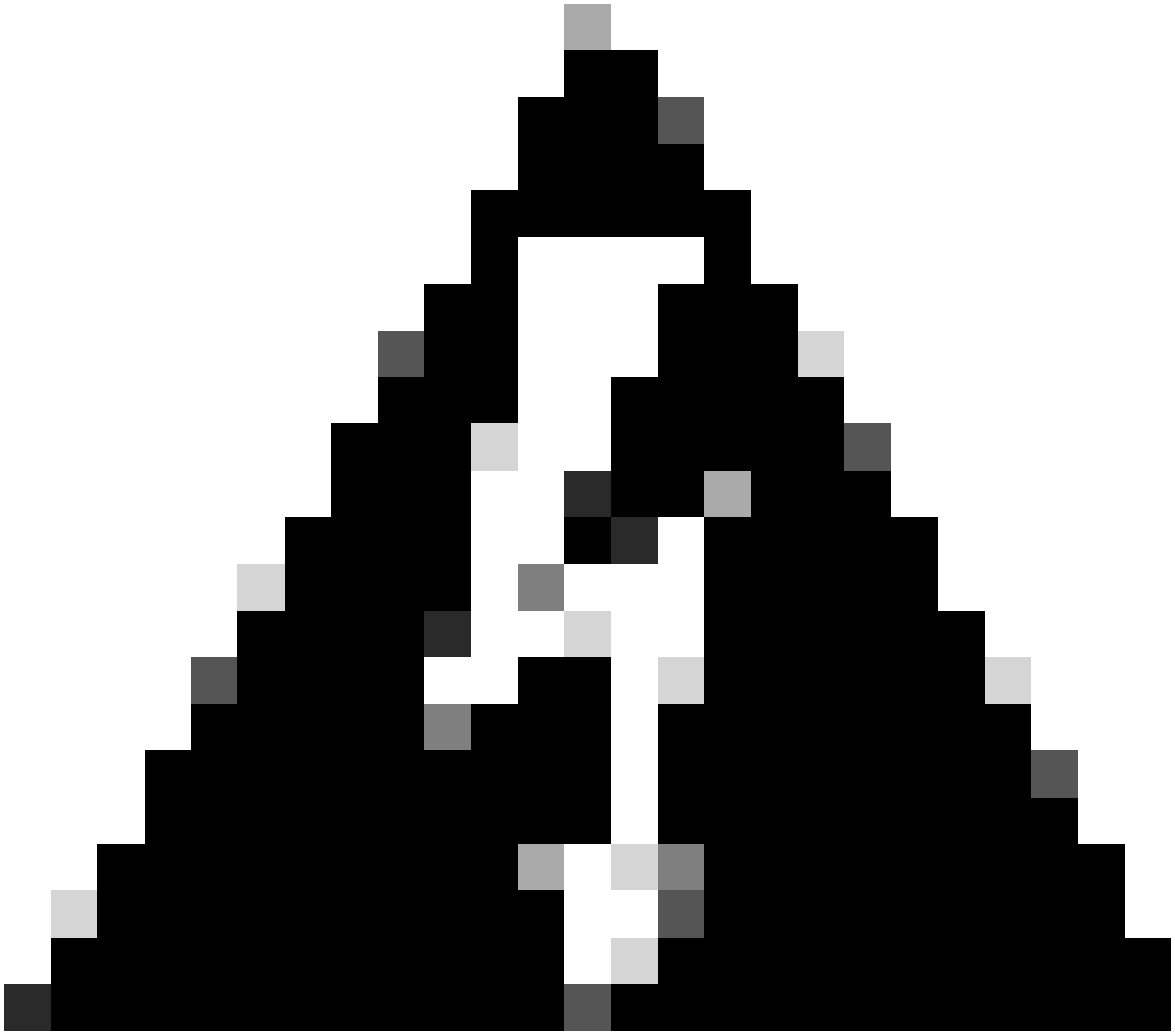
이 시나리오에서는 AP가 FlexConnect 모드라고 가정합니다. AP가 FlexConnect 모드에 있으려면 SiteTag에 연결된 Flex 프로필이 필요합니다. 여기서 Enable Local Site(로컬 사이트 활성화) 확인란이 비활성화됩니다. 이 사이트 태그는 default-ap-join 및 사용자 지정 Flex 프로필 이름 Flex_LWA를 사용합니다.



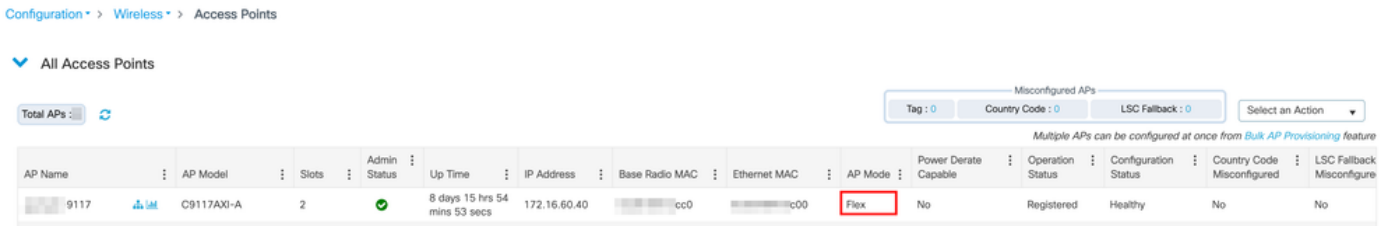
AP에 정책 태그 할당

Configuration(컨피그레이션) > Wireless(무선) > Access Points(액세스 포인트)로 이동하여 AP를 선택하고 General(일반) 탭의 오른쪽에는 AP에서 사용하는 태그가 있습니다.

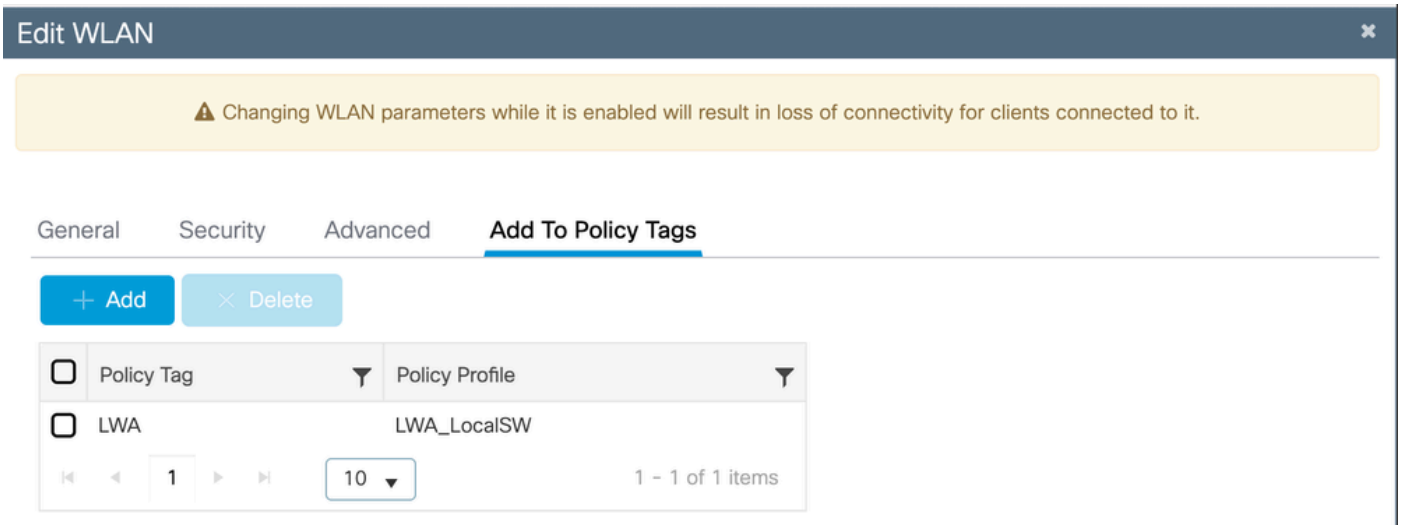


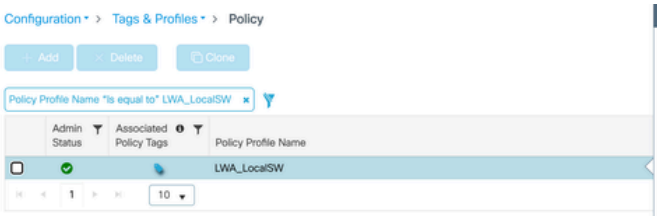


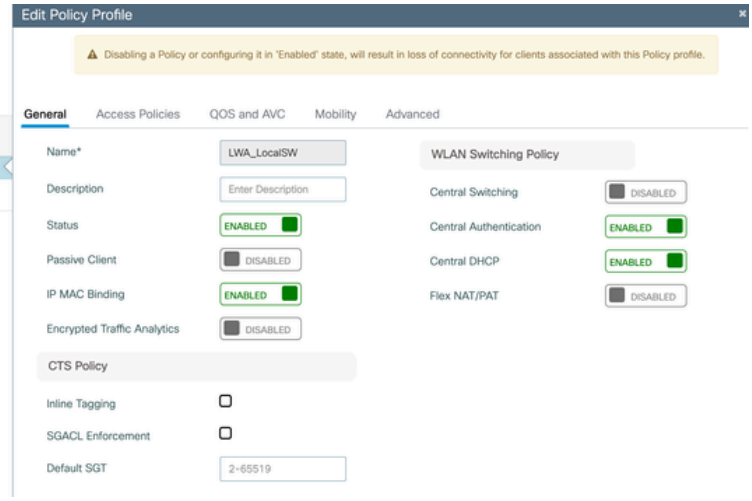
경고: 태그를 변경하면 AP가 WLC의 연결을 끊습니다.



WLAN과 연결된 정책 프로필은 로컬 스위칭입니다







다음을 확인합니다.

```
9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name        Type ID  State Protocol  Method    Role
-----------------------------------------------------------------------------------------------
9ef2.4b16.a507 xxxxx-9117 WLAN 1 Run 11ax(2.4) Web Auth Local

9800WLC#show wireless client mac-address


        detail


Client MAC Address :



Client MAC Type : Locally Administered Address


Client DUID: NA
```

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

```
Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0
```

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failured Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

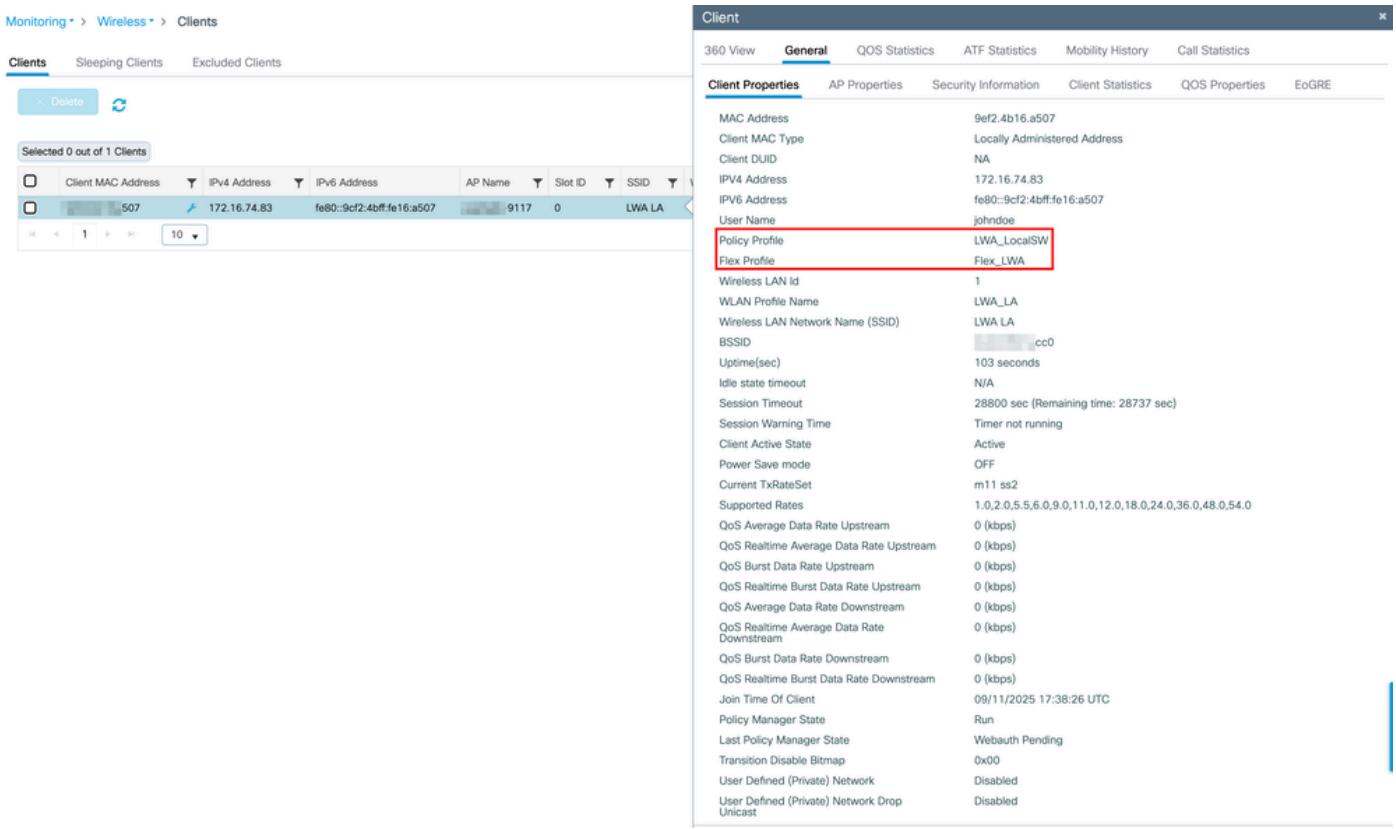
WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED



문제 해결

"Web Auth Pending(웹 인증 보류 중)" 상태는 클라이언트가 액세스 포인트에 연결되었지만 아직 웹 인증 프로세스를 완료하지 않았음을 나타냅니다. 이 상태에서 컨트롤러는 클라이언트 HTTP 트래픽을 인터셉트하고 사용자 로그인 또는 약관 수락을 위해 웹 인증 포털로 리디렉션합니다. 클라이언트는 성공적인 웹 인증이 완료될 때까지 이 상태를 유지하며, 그 후 클라이언트 정책 관리자 상태가 "Run"으로 전환되고 전체 네트워크 액세스가 부여됩니다.

클라이언트 연결의 흐름을 시각적으로 보려면 Configure Local Web Authentication with External Authentication에서 LWA Flow를 확인합니다.

클라이언트가 클라이언트 관점에서 거치는 단계는 9800 WLC에서 LWA와 관련된 일반적인 문제 해결에 나와 있습니다.

- 기술 지원 및 문서 – Cisco Systems

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.