Mac 필터 실패에서 웹 인증 구성 및 문제 해결

목차

소개

이 문서에서는 외부 인증을 위해 ISE를 사용하여 "Mac Filter Failure" 기능에 대한 로컬 웹 인증을 구성, 트러블슈팅 및 확인하는 방법을 설명합니다.

사전 요구 사항

MAC 인증을 위한 ISE 구성

ISE/Active Directory에 구성된 유효한 사용자 자격 증명

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

컨트롤러 웹 UI를 탐색하기 위한 기본 이해

정책, WLAN 프로필 및 정책 태그 컨피그레이션

ISE의 서비스 정책 컨피그레이션

사용되는 구성 요소

9800 WLC 버전 17.12.2

C9120 AXI AP

9300 스위치

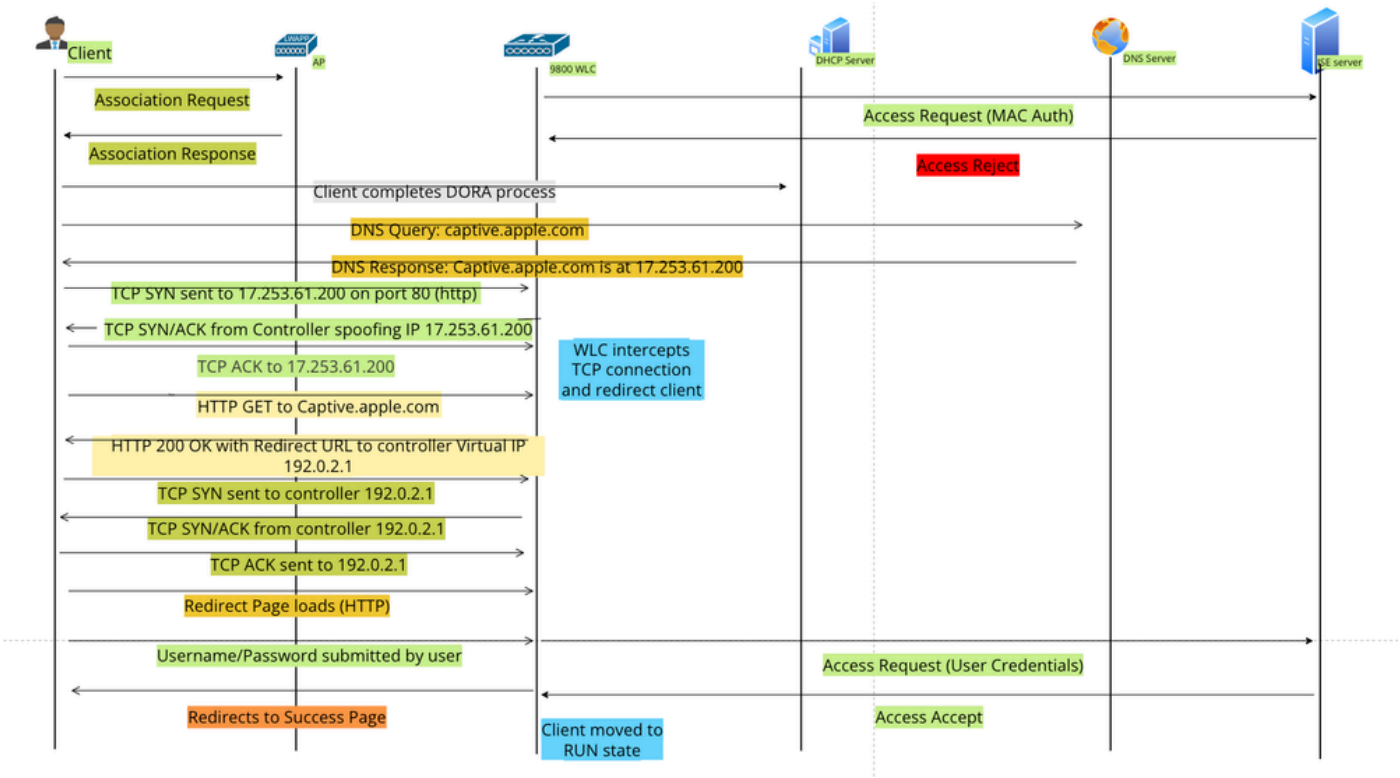
ISE 버전 3.1.0.518

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

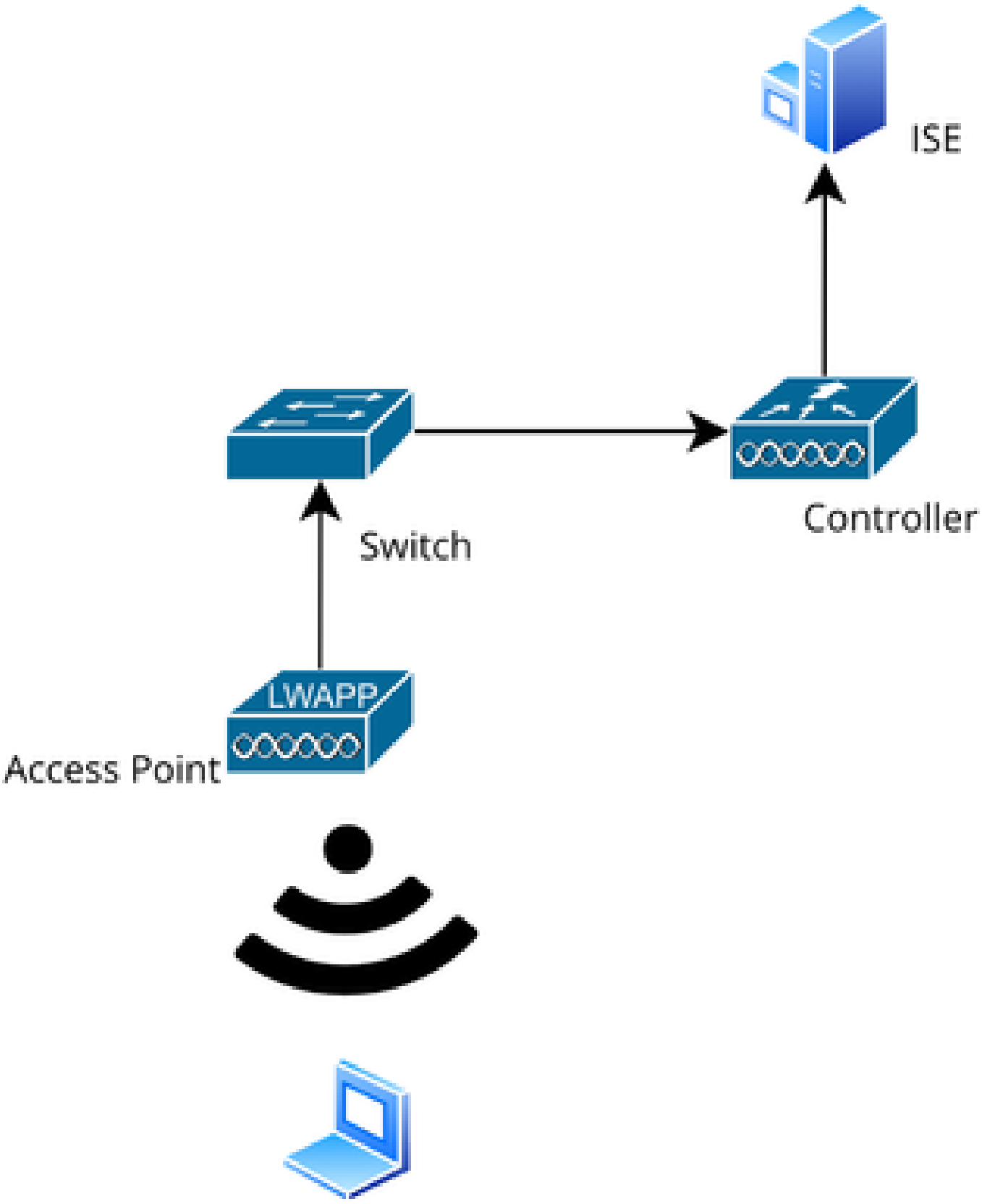
웹 인증 "On Mac Failure Filter" 기능은 MAC 인증과 웹 인증을 모두 사용하는 WLAN 환경에서 폴백 메커니즘으로 사용됩니다.

- 폴백 메커니즘: 클라이언트가 외부 RADIUS 서버(ISE) 또는 로컬 서버에 대해 MAC 필터를 사용하여 WLAN에 연결하려고 시도했으나 인증에 실패하면 이 기능은 레이어 3 웹 인증을 자동으로 시작합니다.
- 성공적인 인증: 클라이언트가 MAC 필터를 통해 성공적으로 인증되면 웹 인증이 우회되므로 클라이언트가 WLAN에 직접 연결할 수 있습니다.
- 연결 해제 방지: 이 기능은 MAC 필터 인증 실패로 인해 발생할 수 있는 연결 해제를 방지하는 데 도움이 됩니다.



구성

네트워크 다이어그램



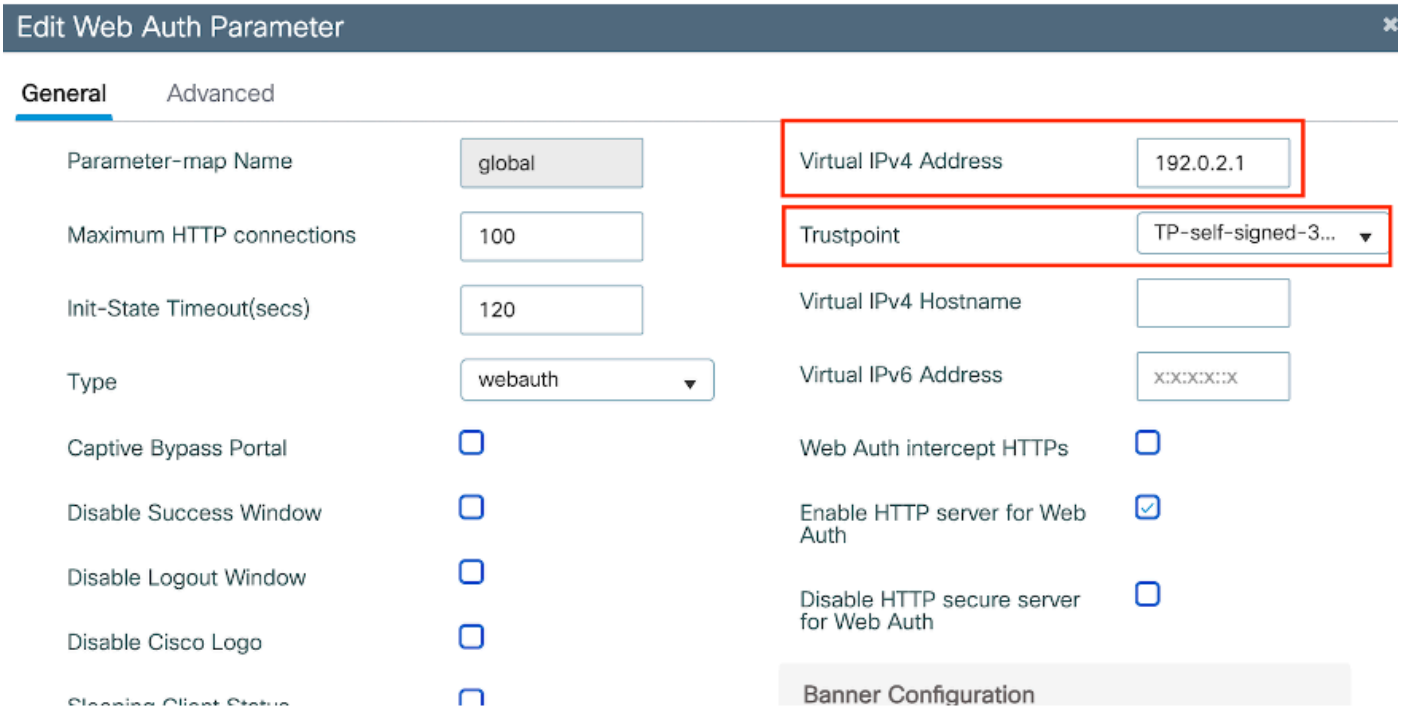
네트워크 토폴로지

설정

웹 매개변수 구성

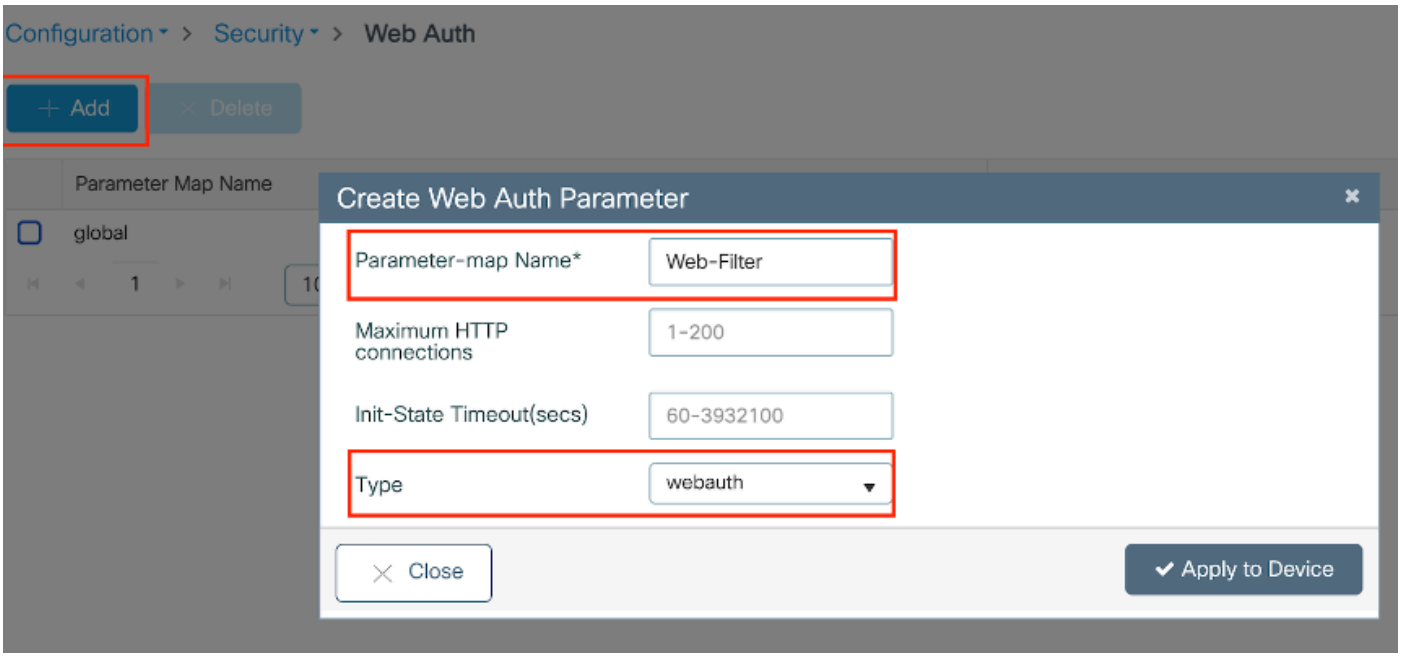
Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고 Global parameter map(전역 매개변수 맵)을 선택합니다

전역 매개변수 맵에서 가상 IP 및 신뢰 지점 컨피그레이션을 확인합니다. 모든 사용자 지정 웹 인증 매개변수 프로파일은 전역 매개변수 맵에서 가상 IP 및 신뢰 지점 컨피그레이션을 상속합니다.



전역 웹 인증 매개변수 프로파일

1단계: "Add(추가)"를 선택하여 사용자 지정 웹 인증 매개변수 맵을 만듭니다. 프로파일 이름을 입력하고 유형을 "Webauth"로 선택합니다.



웹 인증 매개변수 프로파일

클라이언트에서 IPv6 주소도 가져오는 경우 매개변수 맵에 가상 IPv6 주소도 추가해야 합니다. 설명서 범위 2001:db8::/32에서 IP 사용

클라이언트가 IPv6 주소를 얻은 경우 V4가 아닌 V6에서 HTTP 웹 인증 리디렉션을 가져오려고 시도할 가능성이 높습니다. 따라서 가상 IPv6도 설정해야 합니다.

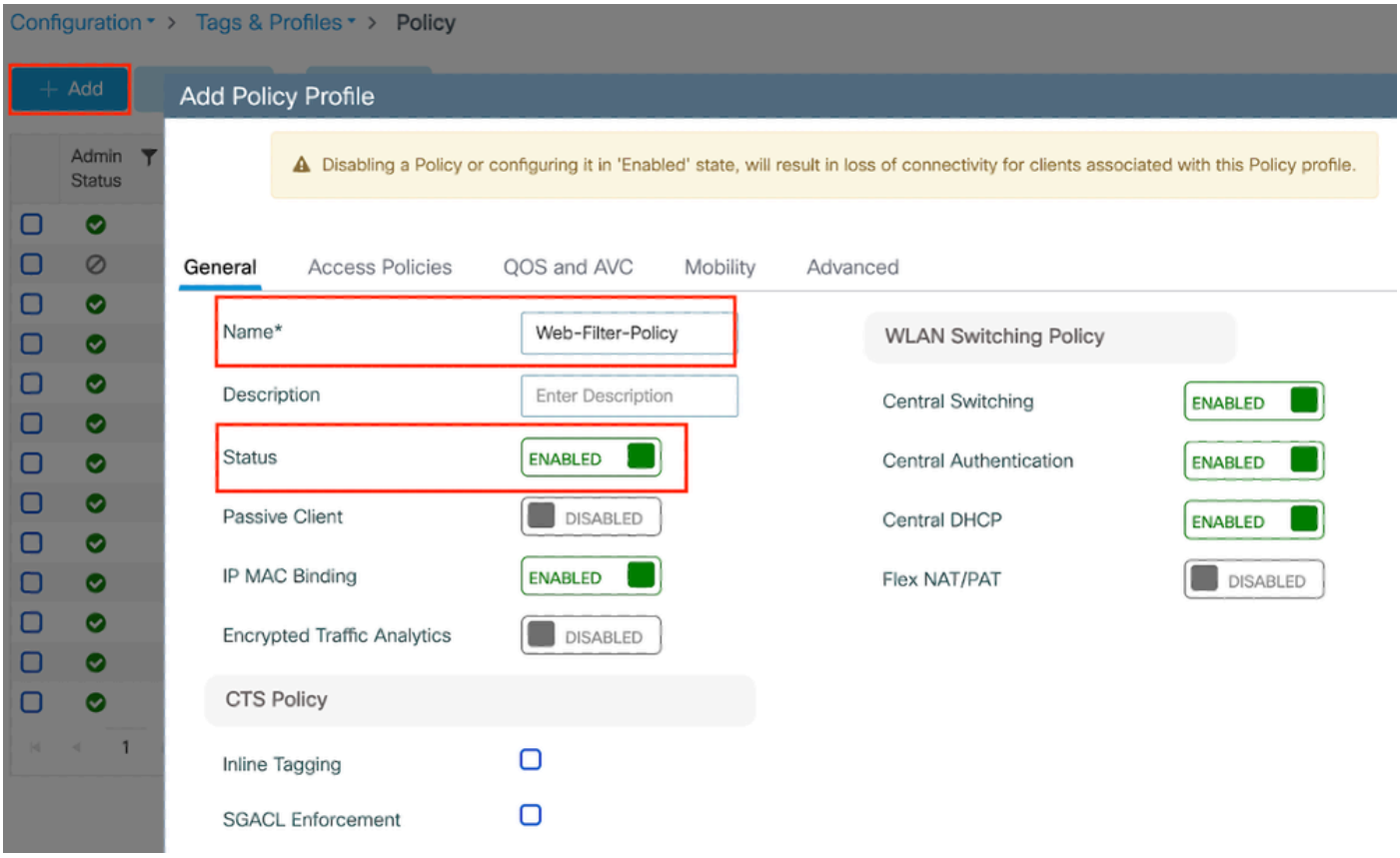
CLI 구성:

```
parameter-map type webauth Web-Filter
 type webauth
```

정책 프로필 구성

1단계: 정책 프로필 생성

Configuration > Tags & Profiles > Policy로 이동합니다. "추가"를 선택합니다. General(일반) 탭에서 프로파일의 이름을 지정하고 상태 토글을 활성화합니다.

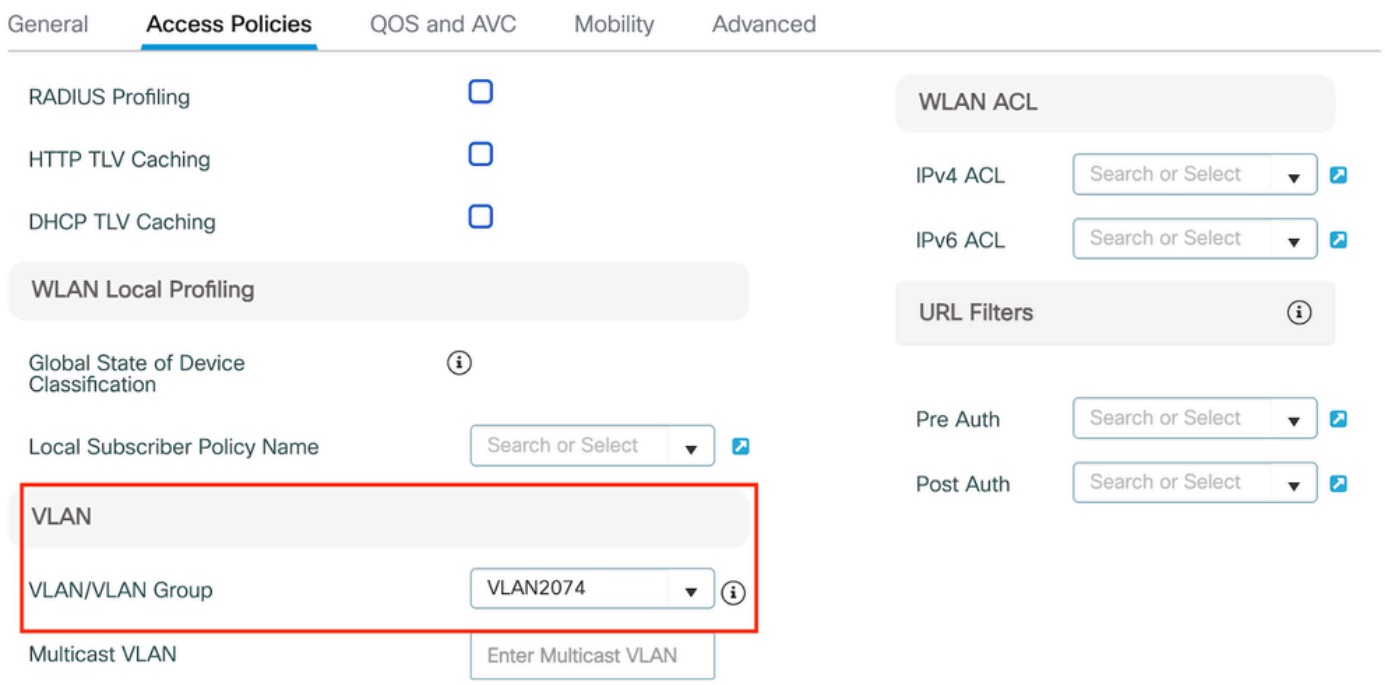


정책 프로파일

2단계:

Access Policies(액세스 정책) 탭의 VLAN 섹션 드롭다운 목록에서 클라이언트 VLAN을 선택합니다

.



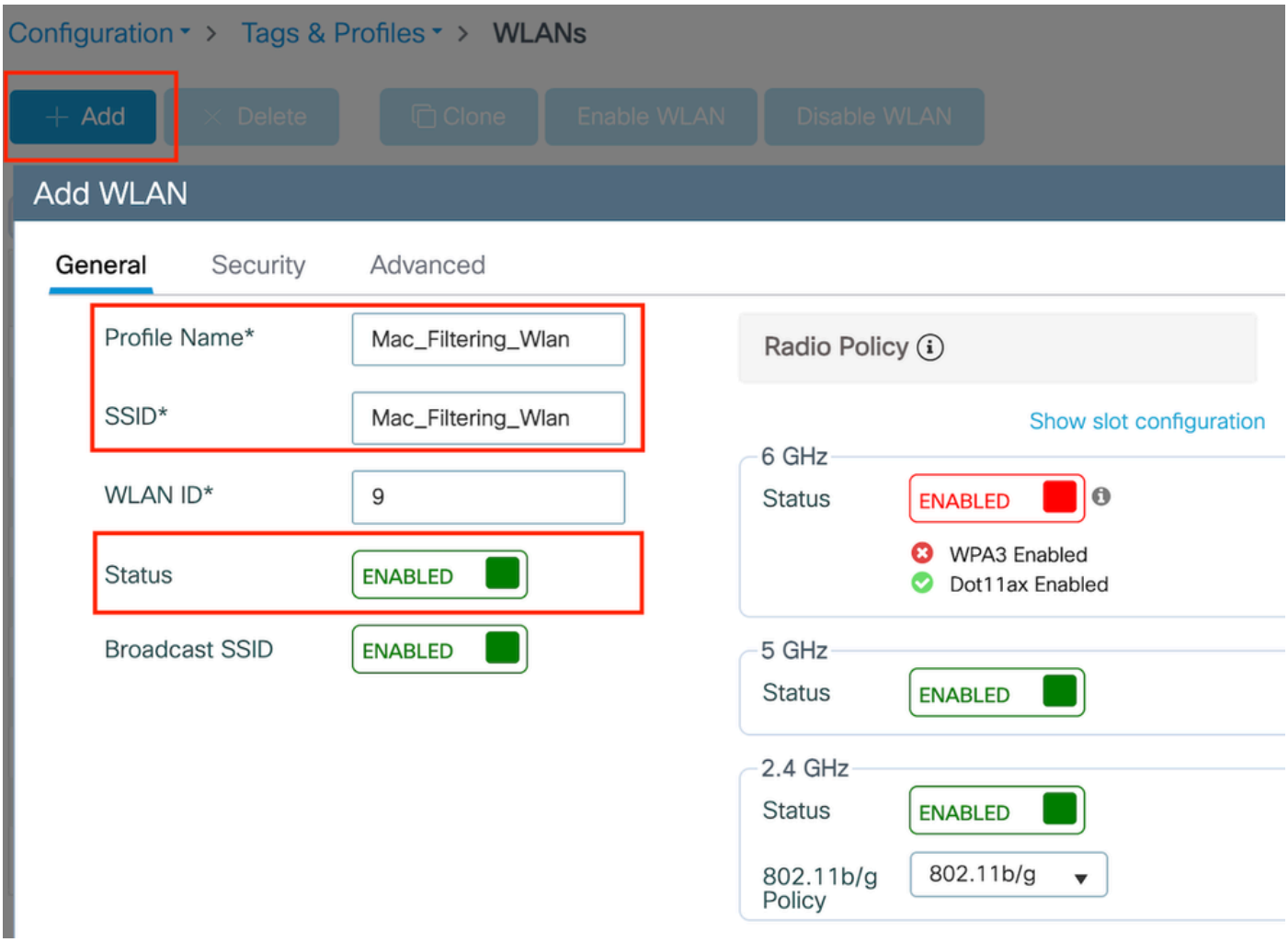
액세스 정책 탭

CLI 구성:

```
wireless profile policy Web-Filter-Policy
 vlan VLAN2074
 no shutdown
```

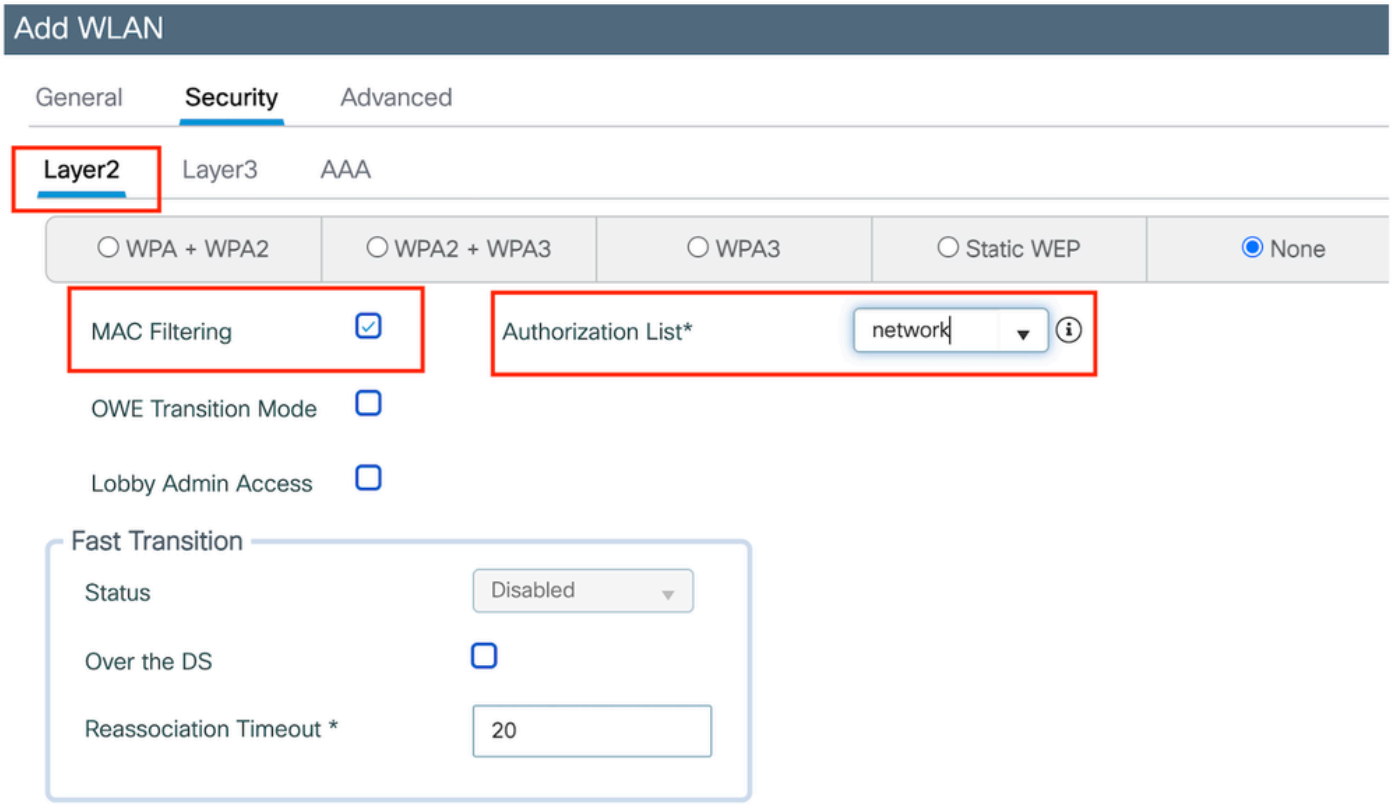
WLAN 프로필 구성

1단계: Configuration(컨피그레이션) > Tags and Profiles(태그 및 프로필) > WLANs(WLAN)로 이동합니다. "추가"를 선택하여 새 프로필을 만듭니다. 프로파일 이름 및 SSID 이름을 정의하고 상태 필드를 활성화합니다.



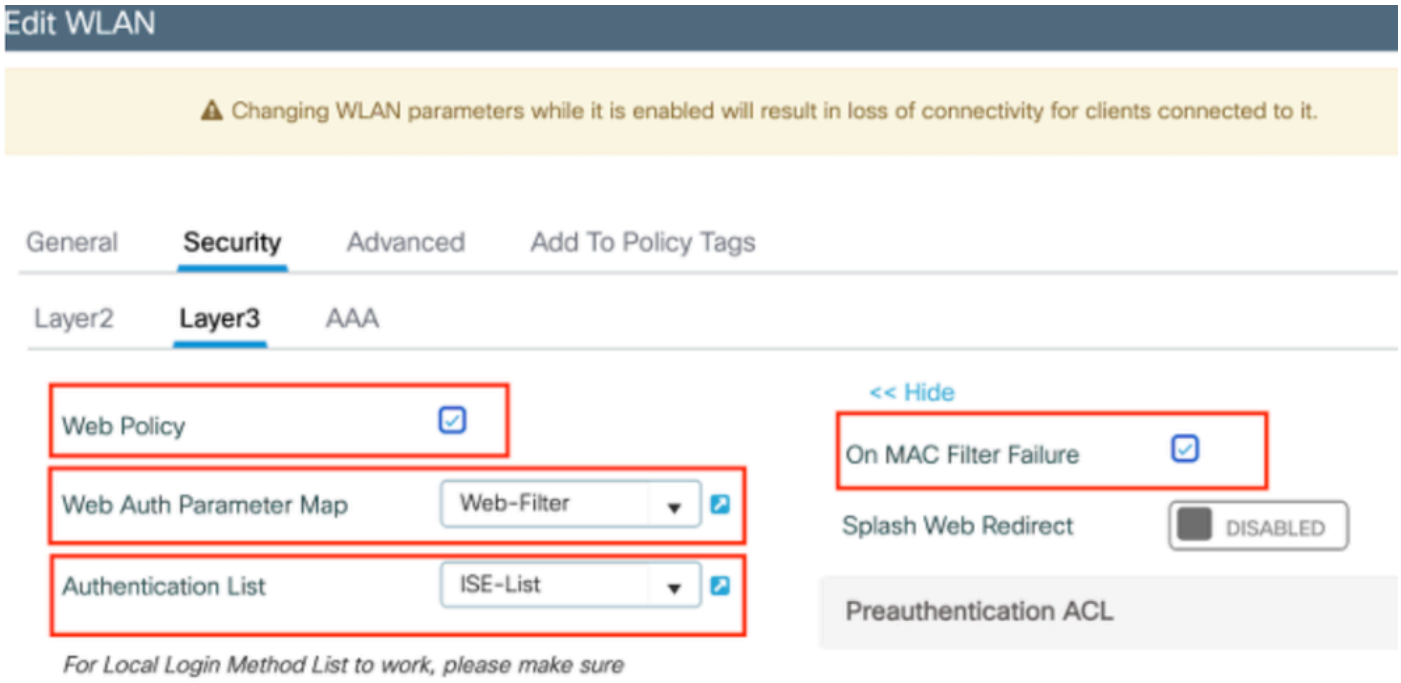
WLAN 프로파일

2단계: Security(보안) 탭에서 "Mac Filtering(Mac 필터링)" 확인란을 활성화하고 Authorization List(권한 부여 목록)(ISE 또는 로컬 서버)에서 RADIUS 서버를 구성합니다. 이 설정에서는 Mac 인증 및 웹 인증 모두에 ISE를 사용합니다.



WLAN 레이어 2 보안

3단계: Security(보안) > Layer3로 이동합니다. 웹 정책을 활성화하고 웹 인증 매개변수 맵 프로파일과 연결합니다. "On Mac Filter Failure(Mac 필터 실패 시)" 확인란을 선택하고 Authentication(인증) 목록 드롭다운에서 RADIUS 서버를 선택합니다.



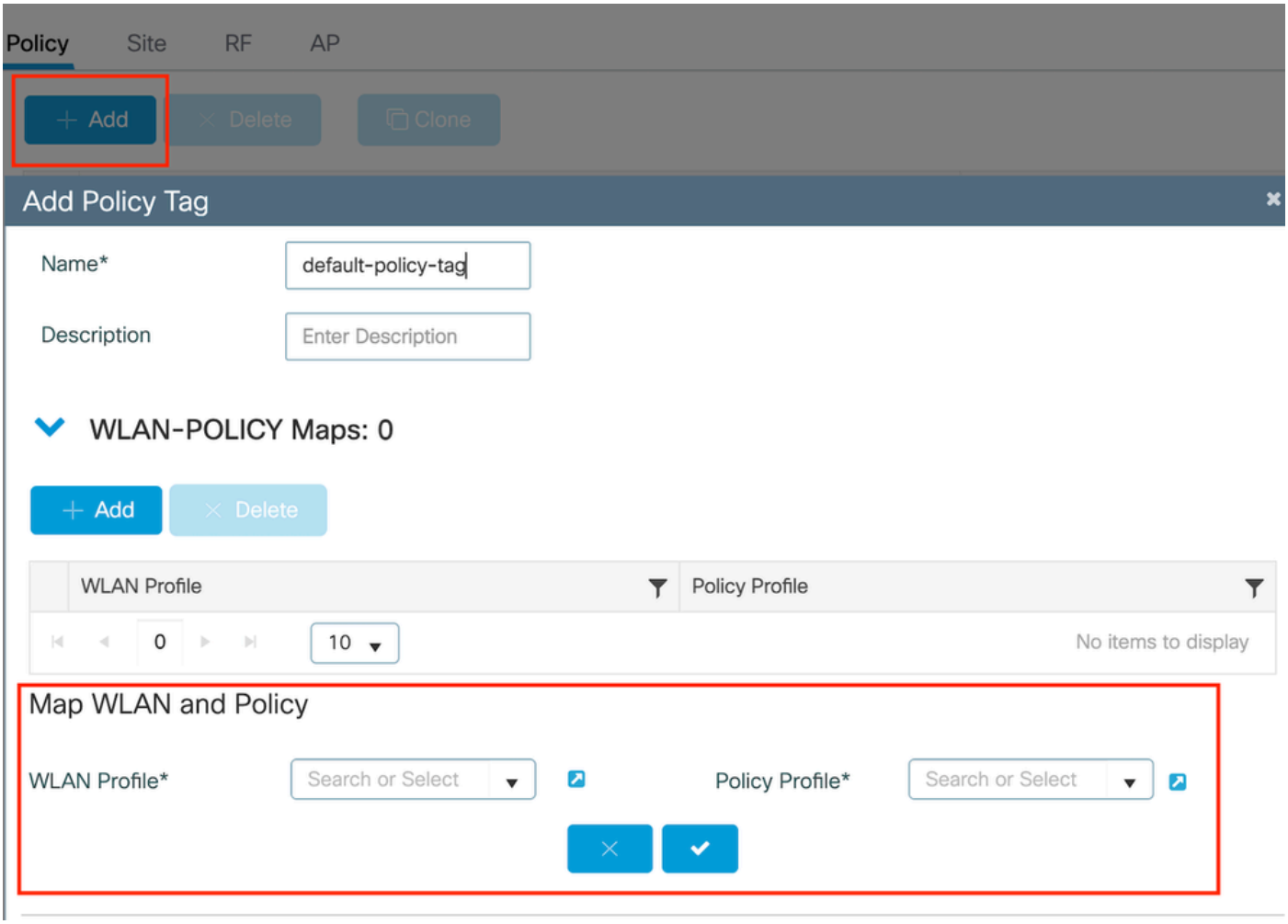
WLAN Layer3 보안 탭

CLI 컨피그레이션

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
 mac-filtering network
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 security web-auth
 security web-auth authentication-list ISE-List
 security web-auth on-macfilter-failure
 security web-auth parameter-map Web-Filter
 no shutdown
```

4단계: 정책 태그 구성, WLAN 프로필 생성, 정책 프로필 매핑

Configuration > Tags & Profiles > Tags > Policy로 이동합니다. 정책 태그의 이름을 정의하려면 "Add(추가)"를 클릭합니다. WLAN-Policy Maps(WLAN-정책 맵)에서 "Add(추가)"를 선택하여 이전에 생성한 WLAN 및 정책 프로필을 매핑합니다.

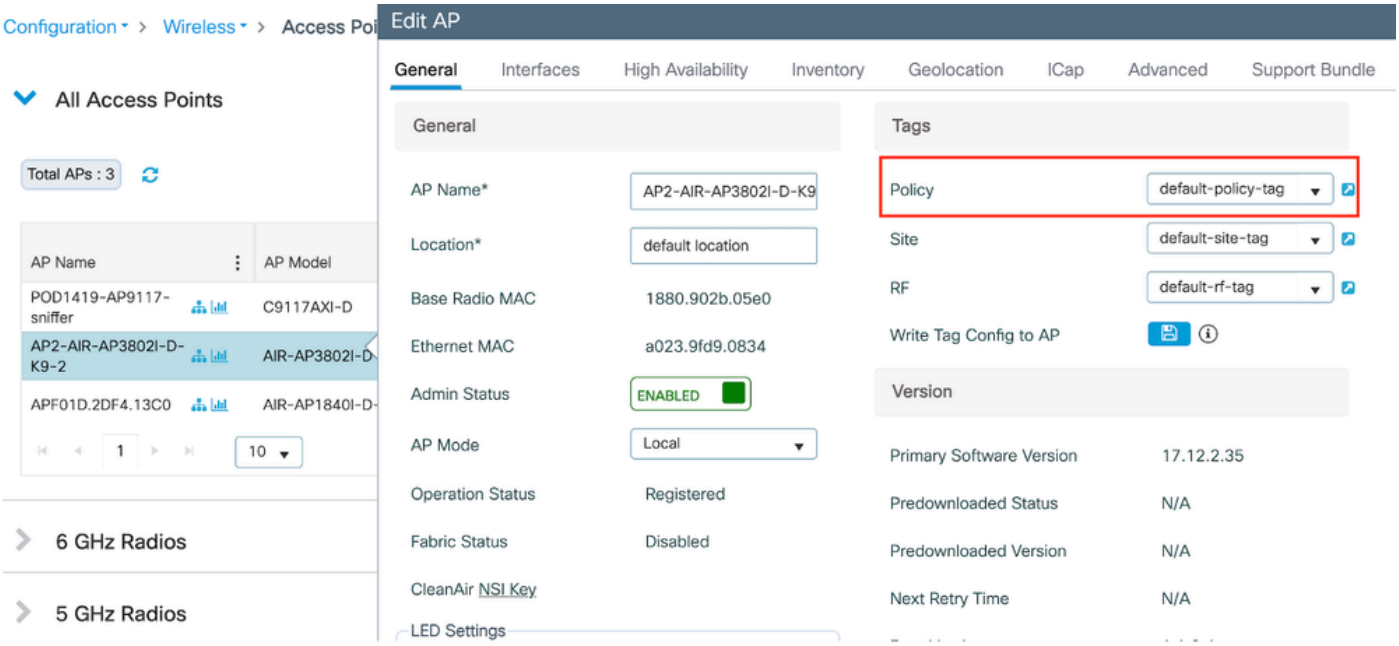


정책 태그 맵

CLI 구성:

```
wireless tag policy default-policy-tag
 description "default policy-tag"
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

5단계: Configuration(컨피그레이션) > Wireless(무선) > Access Point(액세스 포인트)로 이동합니다. 이 SSID를 브로드캐스트하는 액세스 포인트를 선택합니다. Edit AP(AP 수정) 메뉴에서 생성된 정책 태그를 할당합니다.

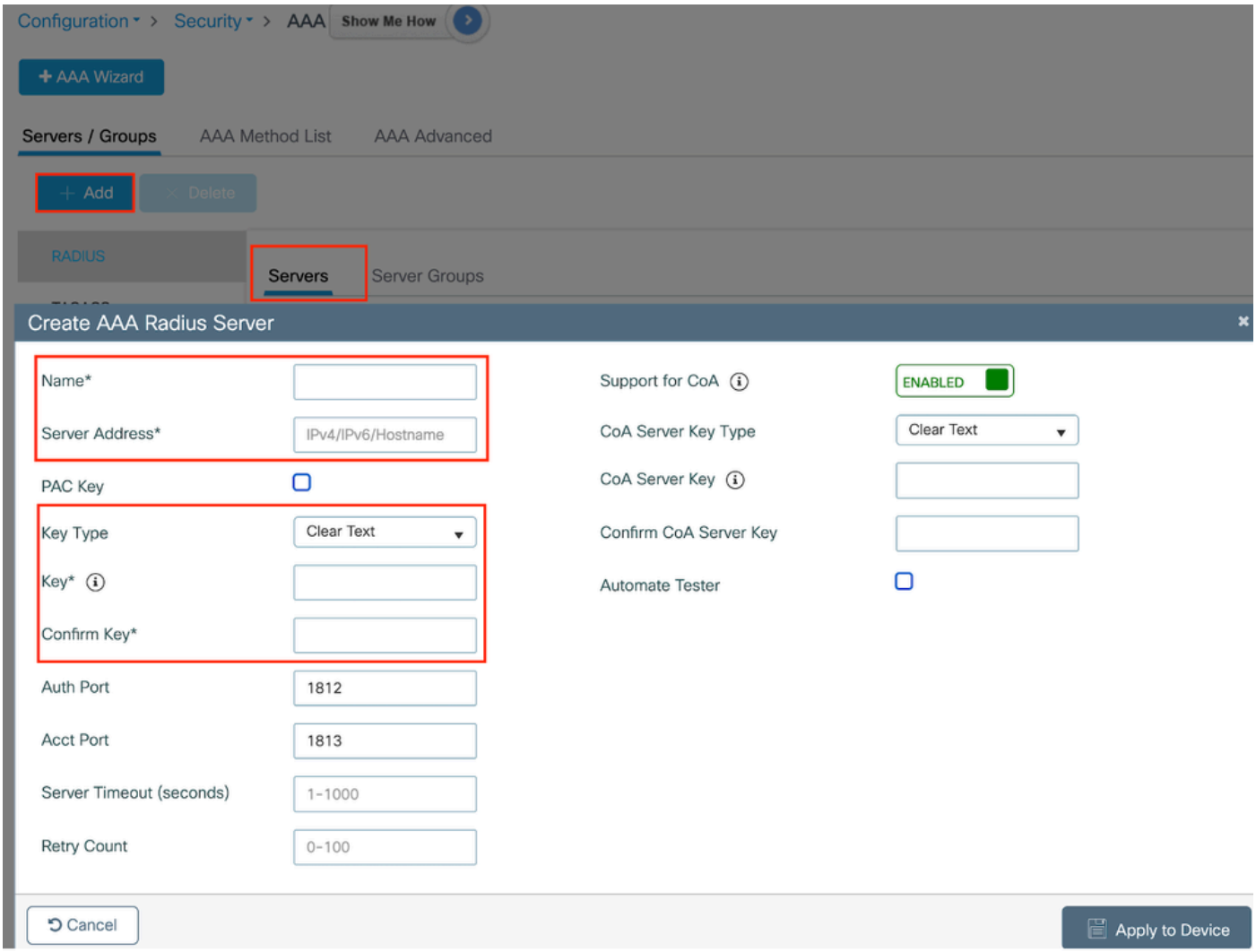


AP에 정책 태그 매핑

AAA 설정을 구성합니다.

1단계: Radius 서버 생성:

Configuration(컨피그레이션) > Security(보안) > AAA로 이동합니다. Server/Group(서버/그룹) 섹션에서 "Add(추가)" 옵션을 클릭합니다. "Create AAA Radius Server(AAA Radius 서버 생성)" 페이지에서 서버 이름, IP 주소 및 공유 암호를 입력합니다.



서버 컨피그레이션

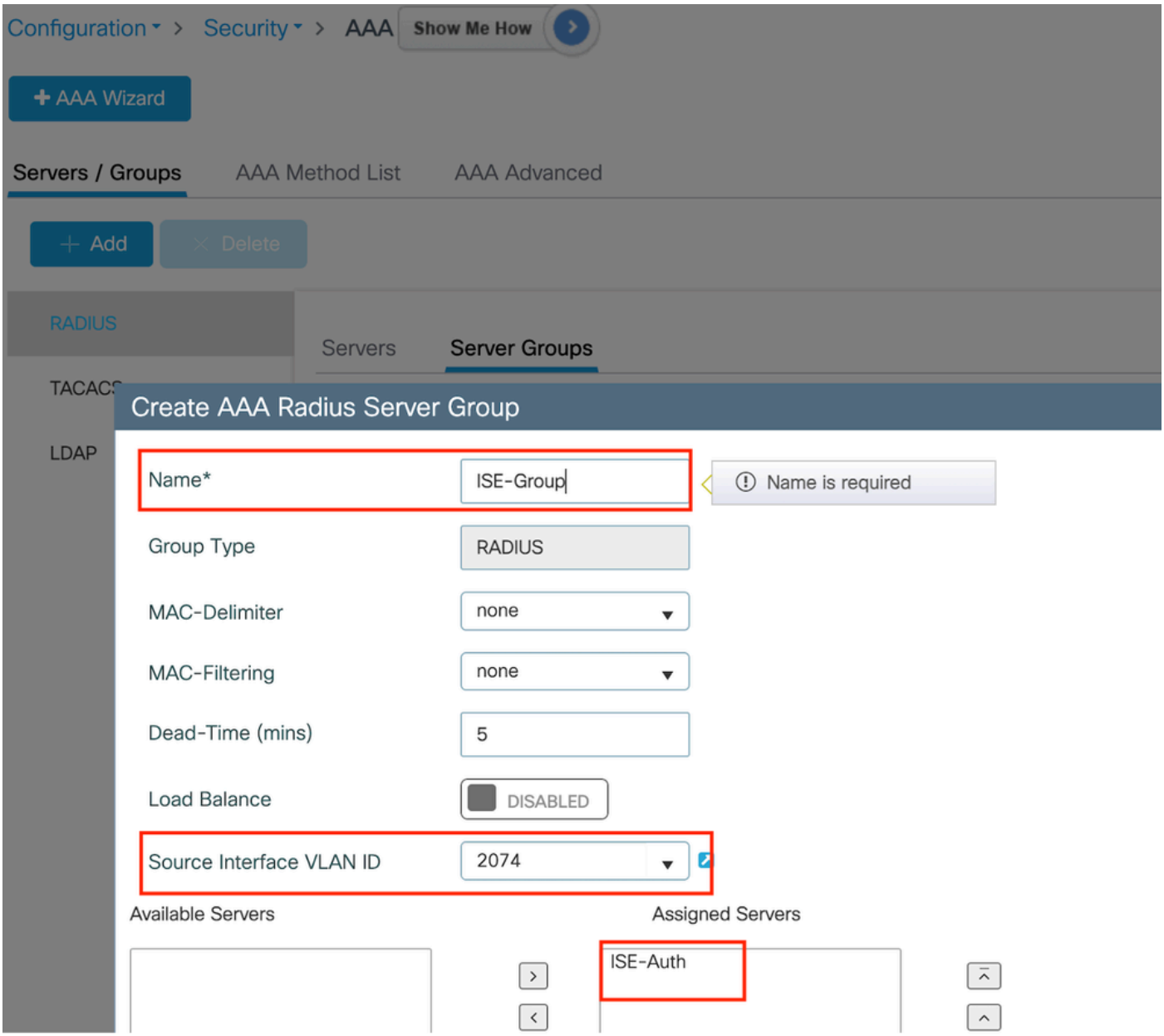
CLI 컨피그레이션

```
radius server ISE-Auth
 address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
 key *****
 server name ISE-Auth
```

2단계: Radius 서버 그룹을 생성합니다.

Server Groups(서버 그룹) 섹션에서 "Add(추가)" 옵션을 선택하여 서버 그룹을 정의합니다. 동일한 그룹 컨피그레이션에 포함할 서버를 토글합니다.

소스 인터페이스를 설정할 필요는 없습니다. 기본적으로 9800은 라우팅 테이블을 사용하여 RADIUS 서버에 연결하는 데 사용할 인터페이스를 계산하며 일반적으로 기본 게이트웨이를 사용합니다.



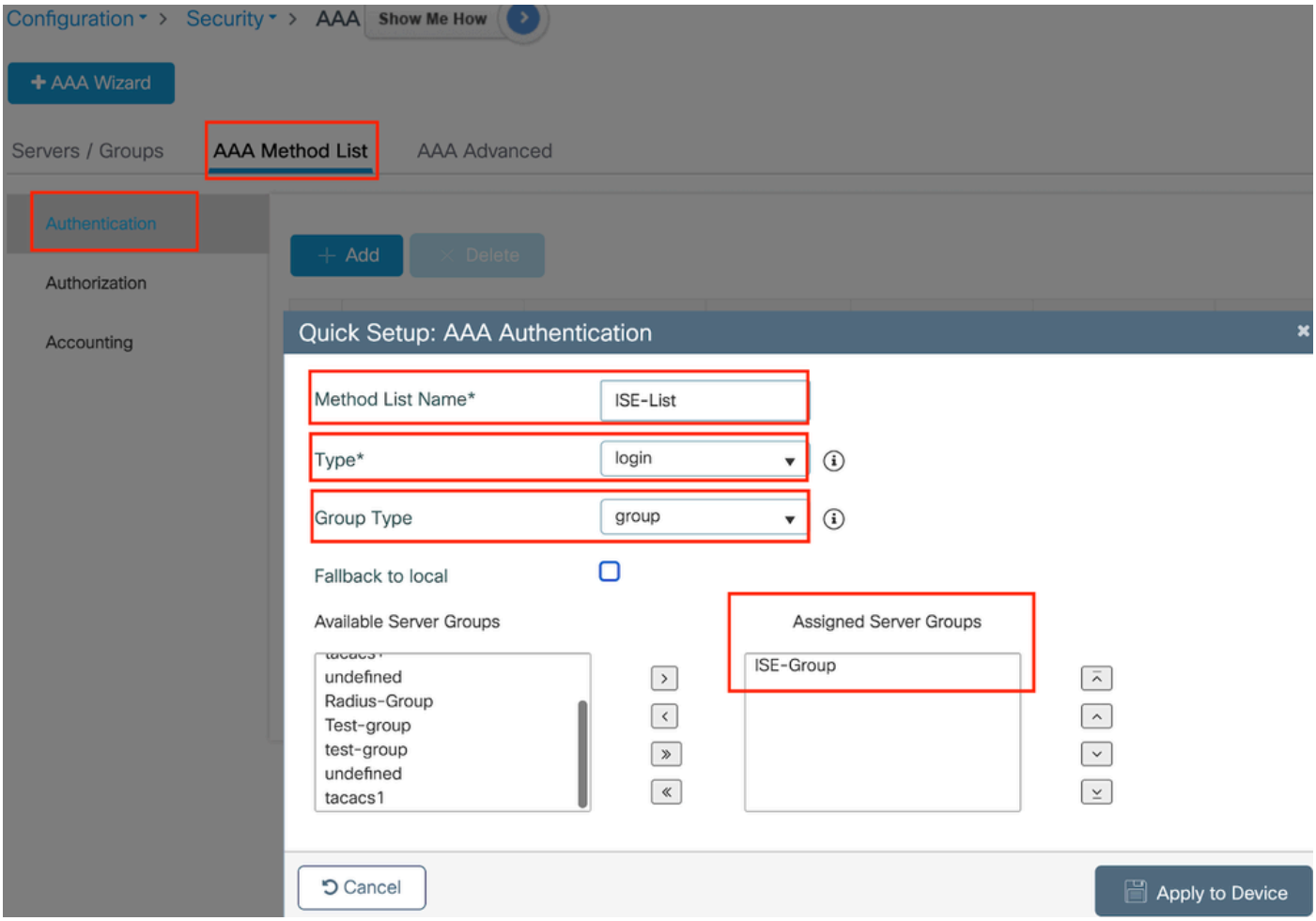
서버 그룹

CLI 컨피그레이션

```
aaa group server radius ISE-Group
 server name ISE-Auth
 ip radius source-interface Vlan2074
 deadtime 5
```

3단계: AAA 메서드 목록 구성:

AAA Method List(AAA 메소드 목록) 탭으로 이동합니다. Authentication(인증)에서 Add(추가)를 클릭합니다. Type을 "login"으로, Group type을 "Group"으로 메서드 목록 이름을 정의합니다. Assigned Server Group(할당된 서버 그룹) 섹션 아래에 구성된 인증 서버 그룹을 매핑합니다.

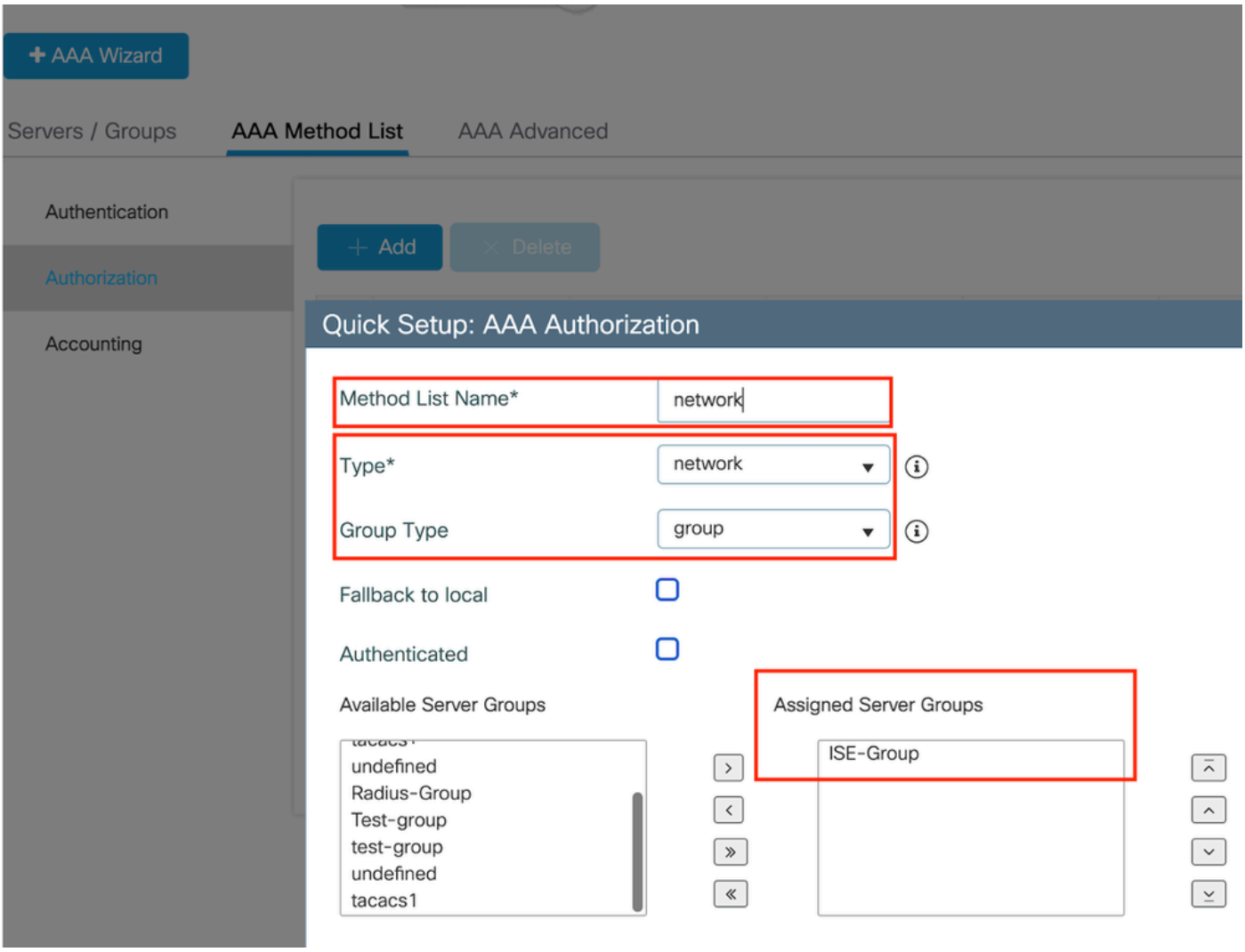


인증 방법 목록

CLI 컨피그레이션

```
aaa authentication login ISE-List group ISE-Group
```

Authorization Method List(권한 부여 방법 목록) 섹션으로 이동하고 "Add(추가)"를 클릭합니다. 메서드 목록 이름을 정의하고 Group type(그룹 유형)을 "Group(그룹)"으로 지정하여 유형을 "network(네트워크)"로 설정합니다. 구성된 RADIUS 서버를 Assigned Server Groups(할당된 서버 그룹) 섹션으로 전환합니다.



권한 부여 방법 목록

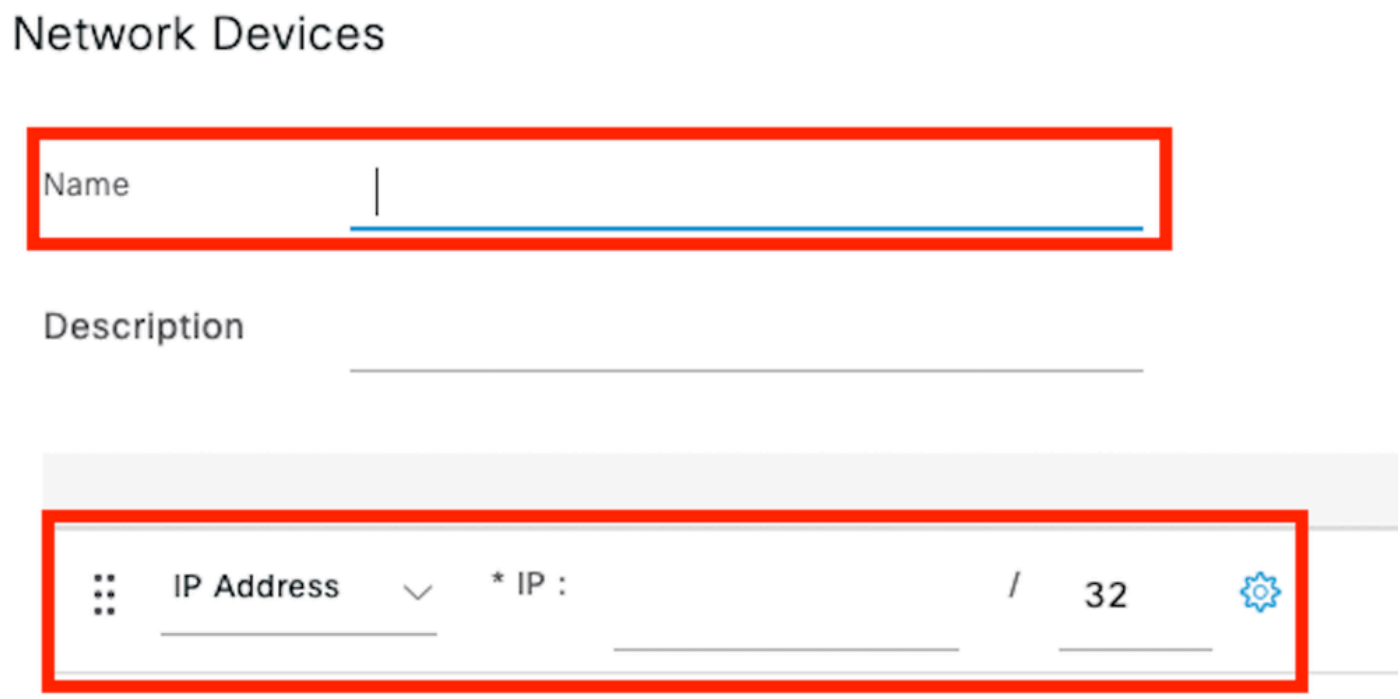
CLI 컨피그레이션

```
aaa authorization network network group ISE-Group
```

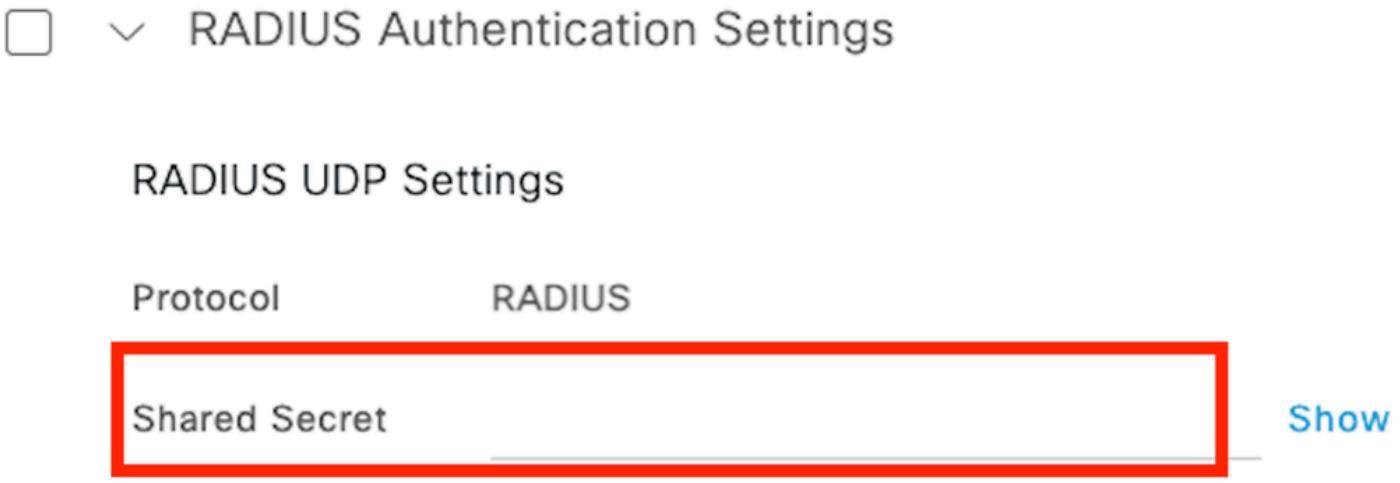
ISE 구성:

ISE에서 네트워크 디바이스로 WLC 추가

1단계: Administration(관리) > Network Devices(네트워크 디바이스)로 이동하고 Add(추가)를 클릭합니다. Radius 인증 설정 아래에 컨트롤러 IP 주소, 호스트 이름 및 공유 암호를 입력 합니다



네트워크 디바이스 추가

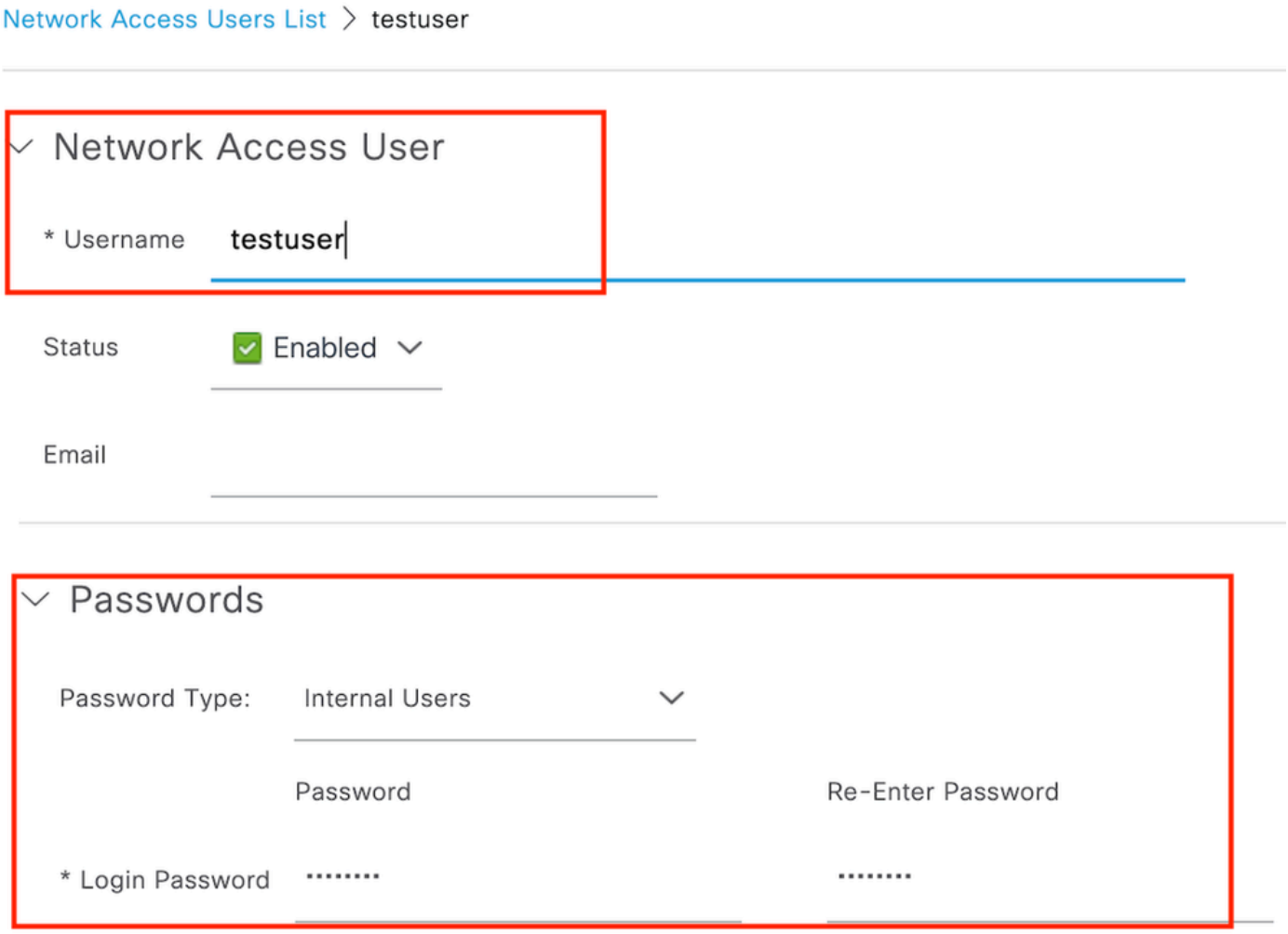


공유 암호

2단계: 사용자 항목 생성

Identity Management(ID 관리) > Identities(ID)에서 Add(추가) 옵션을 선택합니다.

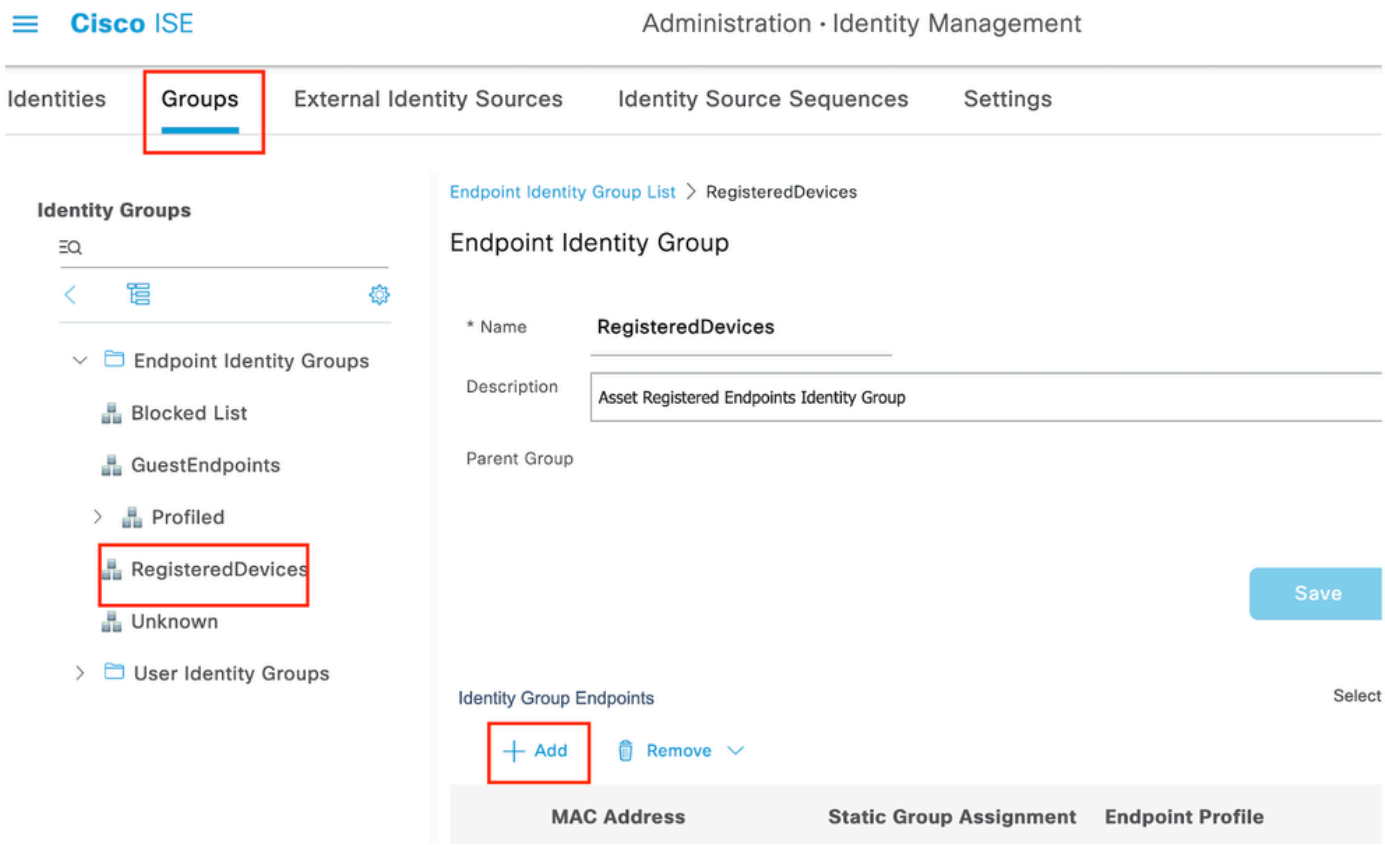
클라이언트가 웹 인증에 사용해야 하는 사용자 이름 및 비밀번호를 구성합니다



사용자 자격 증명 추가

3단계: Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > Registered Devices(등록된 디바이스)로 이동하고 Add(추가)를 클릭합니다.

디바이스 mac 주소를 입력하여 서버에 항목을 생성합니다.

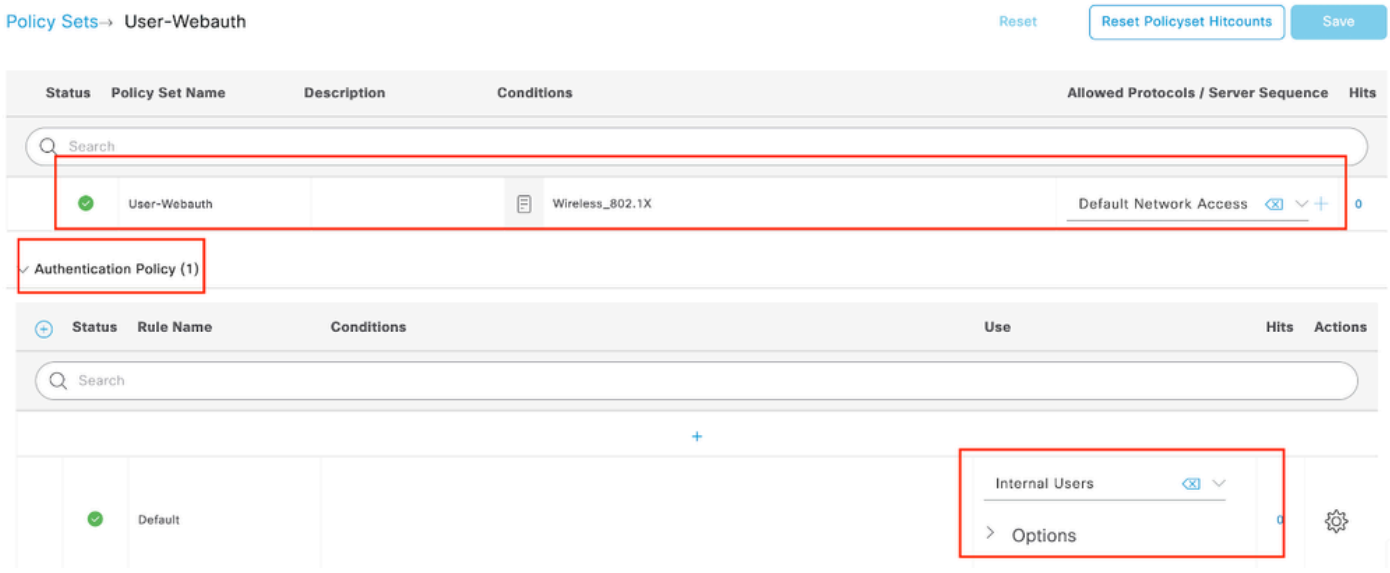


디바이스 MAC 주소 추가

4단계: 서비스 정책 생성

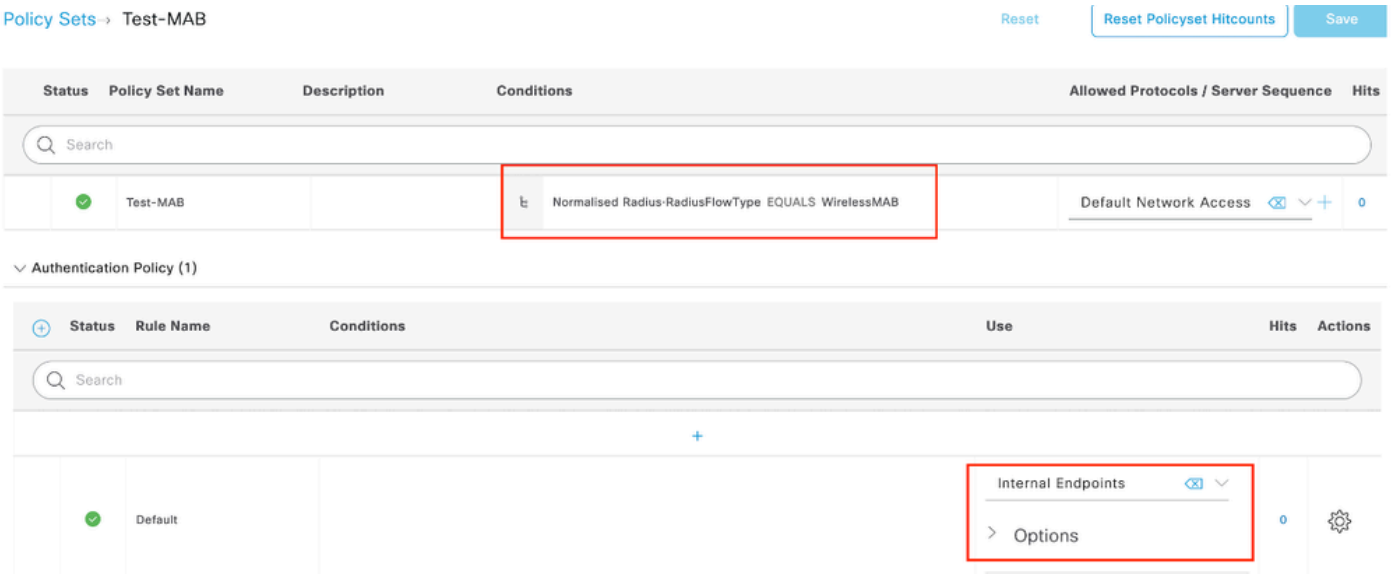
Policy(정책) > Policy sets(정책 집합)로 이동하고 "+" 기호를 선택하여 새 정책 집합을 생성합니다

이 정책 설정은 사용자 웹 인증을 위한 것이며, 여기서 클라이언트의 사용자 이름 및 비밀번호는 ID 관리에서 생성됩니다



웹 인증 서비스 정책

마찬가지로 MAB 서비스 정책을 생성하고 인증 정책 아래에서 내부 엔드포인트를 매핑합니다.



MAB 인증 서비스 정책

다음을 확인합니다.

컨트롤러 컨피그레이션

<#root>

```
show wireless tag policy detailed
```

default-policy-tag

```
Policy Tag Name : default-policy-tag
Description     : default policy-tag
Number of WLAN-POLICY maps: 1
WLAN Profile Name                Policy Name
------------------------------------------------------------------------
```

Mac_Filtering_Wlan

Web-Filter-Policy

<#root>

```
show wireless profile policy detailed
```

Web-Filter-Policy

```
Policy Profile Name                :
```

Web-Filter-Policy

```
Description                        :
```

```
Status                              :
```

ENABLED

```
VLAN                                :
```

2074

```
Multicast VLAN                      : 0
```

<#root>

```
show wlan name
```

Mac_Filtering_Wlan

```
WLAN Profile Name     :
```

Mac_Filtering_Wlan

```
================================================
Identifier                                : 9
Description                               :
Network Name (SSID)                       :
```

Mac_Filtering_Wlan

```
Status                                    :
```

Enabled

```
Broadcast SSID                            :
```

Enabled

```
Mac Filter Authorization list name        :
```

network

```
Webauth On-mac-filter Failure             :
```

Enabled

```
    Webauth Authentication List Name      :
```

ISE-List

```
    Webauth Authorization List Name       : Disabled
    Webauth Parameter Map                 :
```

Web-Filter

<#root>

```
show parameter-map type webauth name Web-Filter
Parameter Map Name              :
```

Web-Filter

```
  Type                          :
```

webauth

```
  Auth-proxy Init State time     : 120 sec
  Webauth max-http connection    : 100
  Webauth logout-window          :
```

Enabled

```
  Webauth success-window         :
```

Enabled

```
  Consent Email                  : Disabled
  Activation Mode                : Replace
  Sleeping-Client                : Disabled
  Webauth login-auth-bypass:
```

<#root>

```
show ip http server status

HTTP server status:
```

Enabled

```
HTTP server port:
```

80

```
HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:
```

Enabled

```
HTTP secure server port:
```

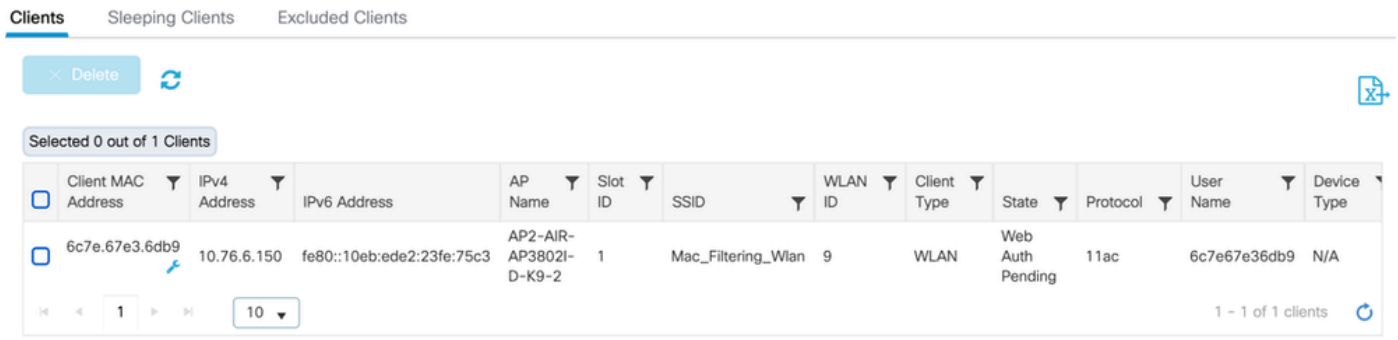
443

```
show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping
------------------
```

```
WLAN Profile Name                Policy Name                    VLAN                          Flex
-------------------------------------------------------------------------------------------------
Mac_Filtering_Wlan               Web-Filter-Policy              2074                          ENAB
```

컨트롤러의 클라이언트 정책 상태

Dashboard(대시보드) > Clients(클라이언트) 섹션으로 이동하여 연결된 클라이언트의 상태를 확인합니다.
클라이언트가 현재 웹 인증 보류 중 상태입니다.



클라이언트 세부사항

```
show wireless client summary
Number of Clients: 1
MAC Address    AP Name                                    Type ID   State              Protocol Meth
-------------------------------------------------------------------------------------------------
6c7e.67e3.6db9 AP2-AIR-AP3802I-D-K9-2                     WLAN 9    Webauth Pending    11ac     Web
```

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail
Client MAC Address :
```

6c7e.67e3.6db9

```
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
```

10.76.6.150

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
Client Username :
```

6c7e67e36db9

```
AP MAC Address : 1880.902b.05e0
AP Name: AP2-AIR-AP3802I-D-K9-2
AP slot : 1
Client State : Associated
Policy Profile :
```

Web-Filter-Policy

```
Flex Profile : N/A
Wireless LAN Id: 9
WLAN Profile Name:
```

Mac_Filtering_Wlan

```
Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :
```

Failed

```
Policy Manager State:
```

Webauth Pending

```
Last Policy Manager State :
```

IP Learn Complete

```
Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List
        Method : Web Auth
                Webauth State    :
```

Get Redirect

```
                Webauth Method   :
```

Webauth

웹 인증에 성공하면 클라이언트 정책 관리자 상태가 RUN으로 전환됩니다

<#root>

```
show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:
```

Run

```
Last Policy Manager State :
```

Webauth Pending

```
Client Entry Create Time : 131 seconds
Policy Type : N/A
```

문제 해결

MAC 장애 시 웹 인증 기능의 기능은 MAB 장애 시 웹 인증을 트리거하는 컨트롤러 기능에 의존합니

다. Cisco의 주된 목표는 트러블슈팅 및 분석을 위해 컨트롤러에서 RA 추적을 효율적으로 수집하는 것입니다.

방사능 흔적 수집

Radio Active Tracing을 활성화하여 CLI에서 지정된 MAC 주소에 대한 클라이언트 디버그 추적을 생성합니다.

Radioactive Tracing 활성화 단계:

모든 조건부 디버그가 비활성화되었는지 확인합니다.

```
clear platform condition all
```

지정된 MAC 주소에 대해 디버그 활성화

```
debug wireless mac <H.H.H> monitor-time <Time is seconds>
```

문제를 재현한 후 디버깅을 비활성화하여 RA 추적 수집을 중지합니다.

```
no debug wireless mac <H.H.H>
```

RA 추적이 중지되면 컨트롤러 부트플래시에서 디버그 파일이 생성됩니다.

```
show bootflash: | include ra_trace
2728        179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

파일을 외부 서버에 복사.

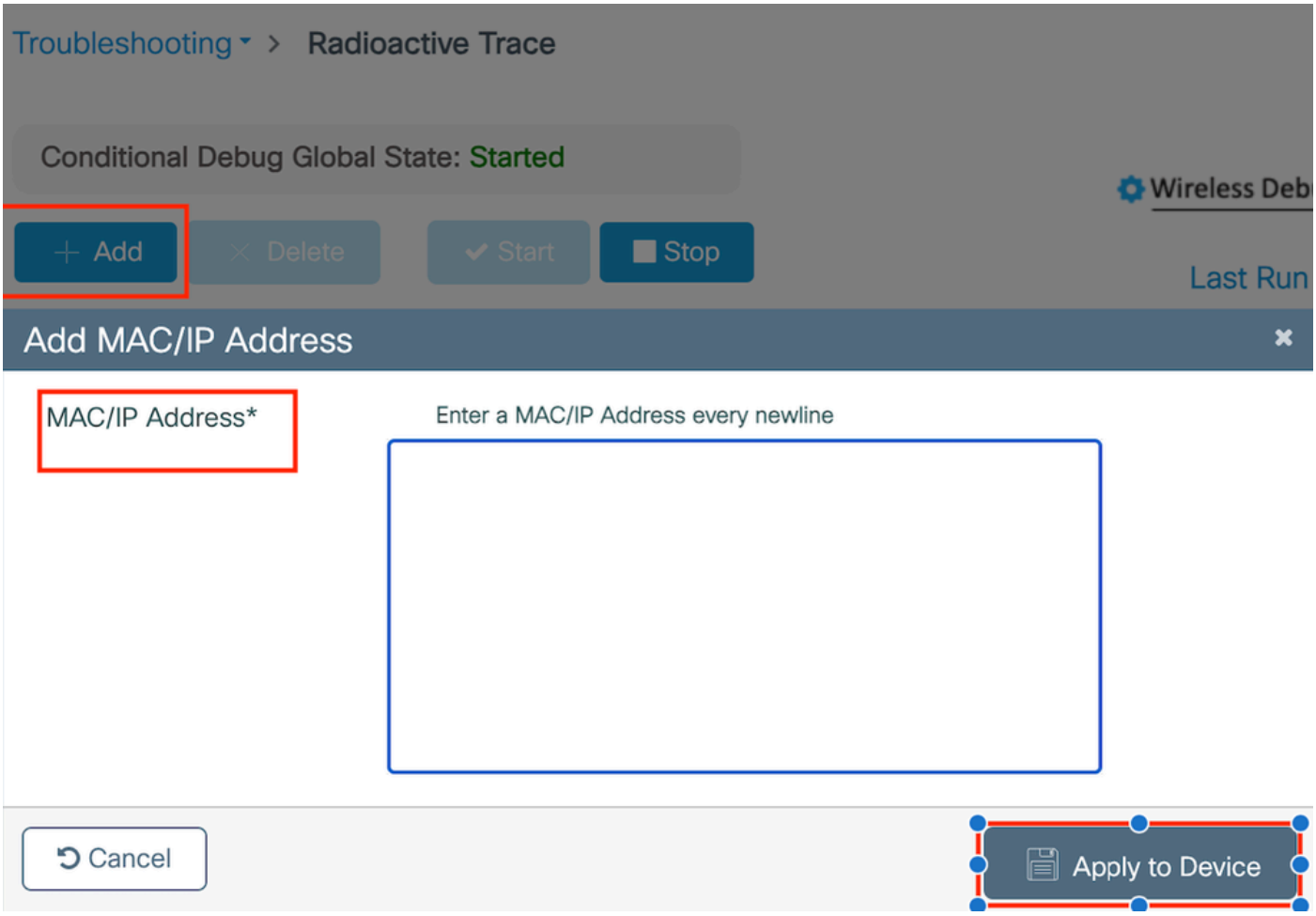
```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP addr
```

디버그 로그를 표시합니다.

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

GUI에서 RA 추적 활성화

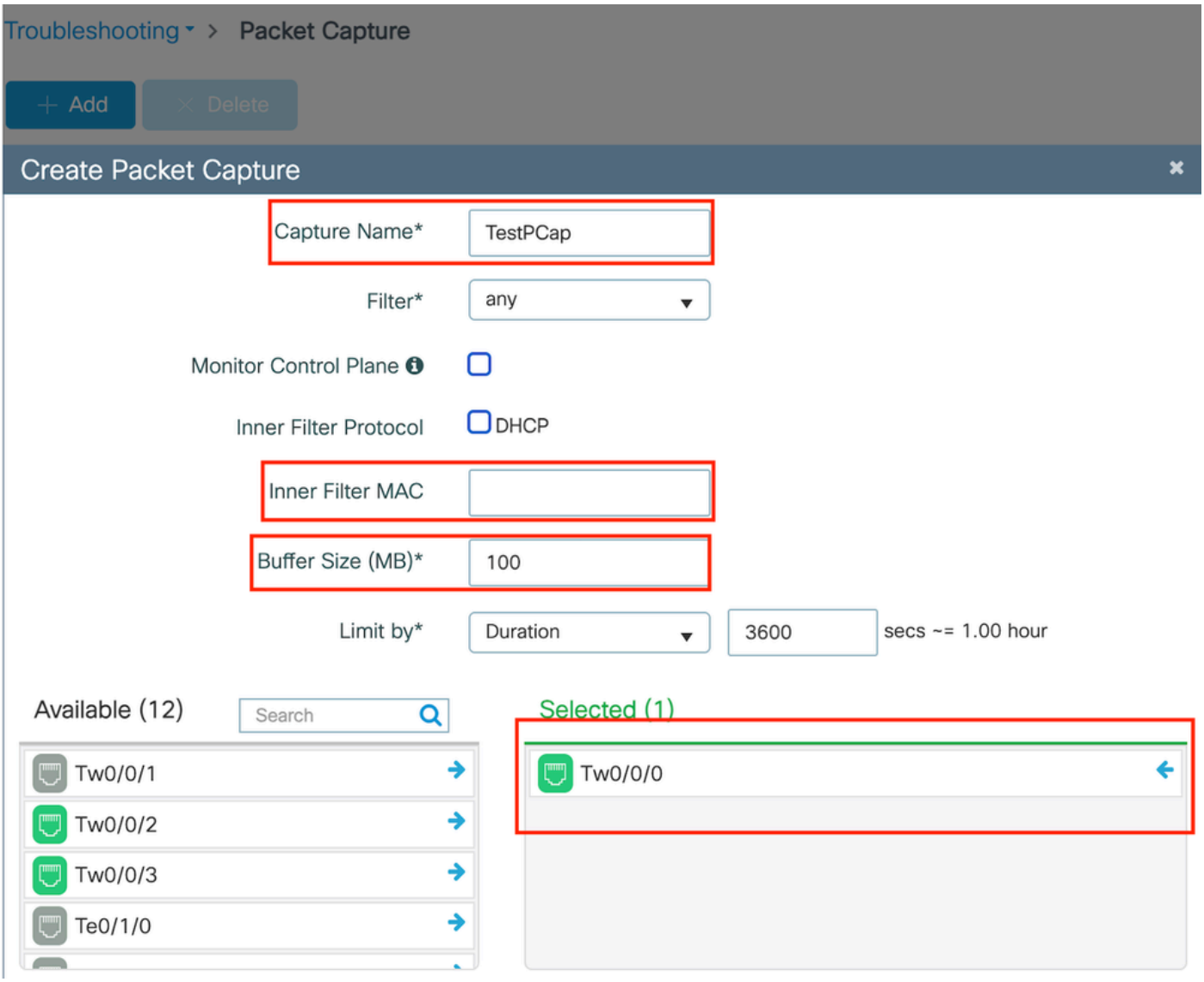
1단계: Troubleshooting(트러블슈팅) > Radioactive Trace(방사능 추적)로 이동합니다. 새 항목을 추가하는 옵션을 선택한 다음 지정된 Add MAC/IP Address(MAC/IP 주소 추가) 탭에 클라이언트 MAC 주소를 입력합니다.



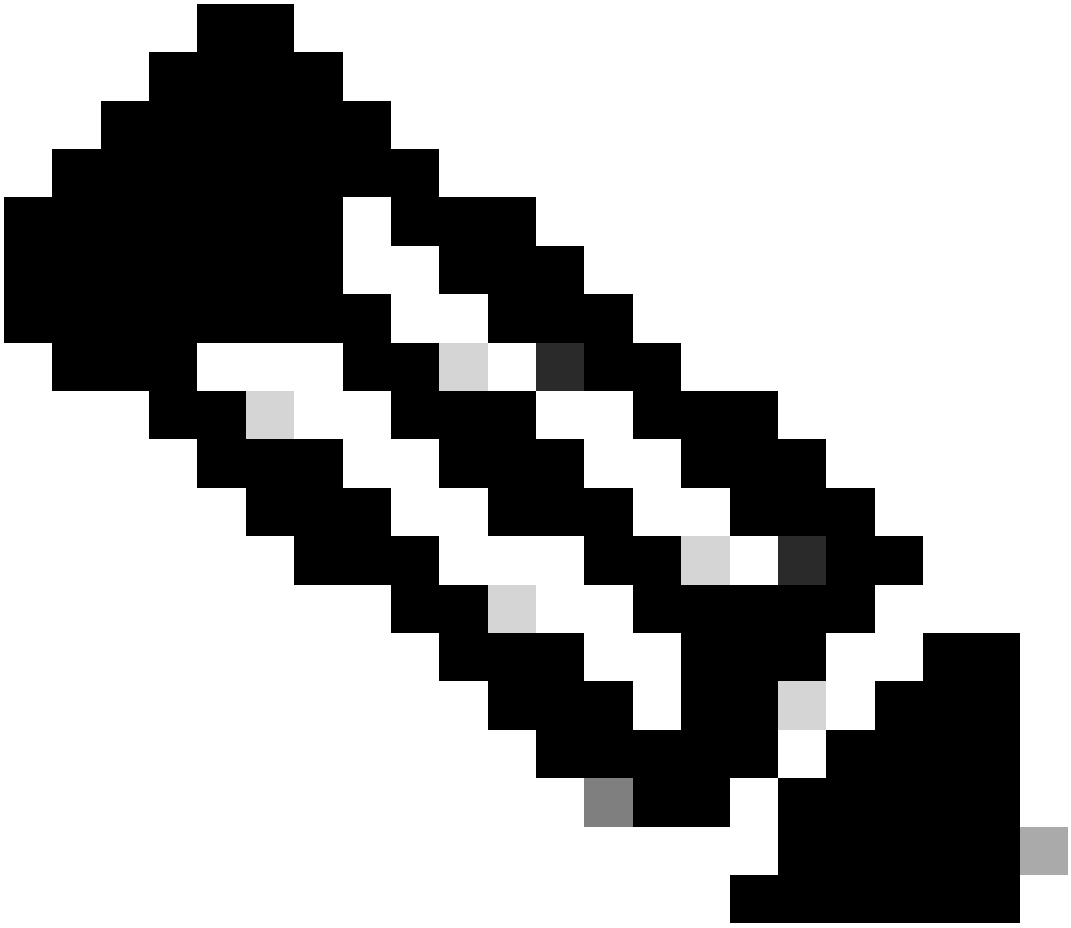
무선 활성 추적

임베디드 패킷 캡처:

Troubleshooting(트러블슈팅) > Packet Capture(패킷 캡처)로 이동합니다. 캡처 이름을 입력하고 클라이언트 MAC 주소를 내부 필터 MAC으로 지정합니다. 버퍼 크기를 100으로 설정하고 업링크 인터페이스를 선택하여 수신 및 발신 패킷을 모니터링합니다.

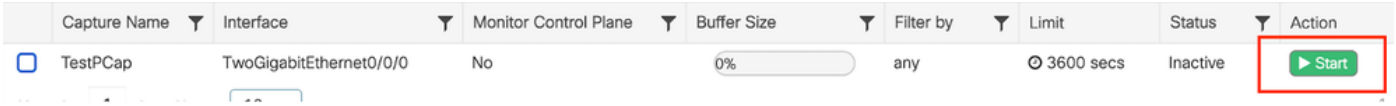

Troubleshooting
Packet Capture
Add
Delete
Create Packet Capture
Capture Name*
TestPCap
Filter*
any
Monitor Control Plane
Inner Filter Protocol
DHCP
Inner Filter MAC
Buffer Size (MB)*
100
Limit by*
Duration
3600
secs ~= 1.00 hour
Available (12)
Search
Tw0/0/1
Tw0/0/2
Tw0/0/3
Te0/1/0
Selected (1)
Tw0/0/0

내장형 패킷 캡처



참고: 시스템 CPU로 리디렉션되고 데이터 플레인으로 재전송된 트래픽을 보려면 "Monitor Control Traffic(제어 트래픽 모니터링)" 옵션을 선택합니다.

Start(시작)를 선택하여 패킷을 캡처합니다.



캡처 시작

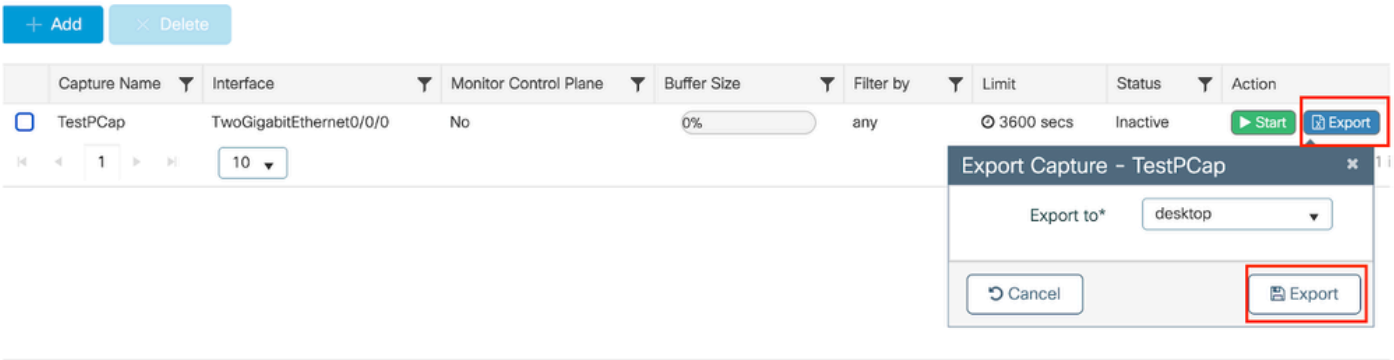
CLI 컨피그레이션

```
monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start
```

```
<Reporduce the issue>

monitor capture TestPCap stop



show monitor capture TestPCap

Status Information for Capture TestPCap
  Target Type:
 Interface: TwoGigabitEthernet0/0/0, Direction: BOTH
  Status : Inactive
  Filter Details:
  Capture all packets
  Inner Filter Details:
  Mac: 6c7e.67e3.6db9
  Continuous capture: disabled
  Buffer Details:
  Buffer Type: LINEAR (default)
  Buffer Size (in MB): 100
  Limit Details:
  Number of Packets to capture: 0 (no limit)
  Packet Capture duration: 3600
  Packet Size to capture: 0 (no limit)
  Maximum number of packets to capture per second: 1000
  Packet sampling rate: 0 (no sampling)
```

외부 TFTP 서버로 패킷 캡처 내보내기

monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap



패킷 캡처 내보내기

MAC 인증이 성공하는 동안 클라이언트 디바이스가 네트워크에 연결하는 시나리오 예를 들어, 클라이언트 디바이스의 MAC 주소는 구성된 정책을 통해 RADIUS 서버에 의해 검증되며, 검증되면 네트워크 액세스 디바이스에 의해 액세스가 부여되어 네트워크 연결이 허용됩니다.

클라이언트가 연결되면 컨트롤러는 ISE 서버에 Access-Request를 보냅니다.

사용자 이름은 MAB 인증이므로 클라이언트의 mac 주소입니다

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:   Cisco AVpair
```

유효한 사용자 항목이 있는 경우 ISE에서 Access-Accept를 보냅니다.

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

Mac 인증으로 전환된 클라이언트 정책 상태 완료

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29  Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

클라이언트가 MAB 인증에 성공한 후 IP 학습 상태에 있습니다.

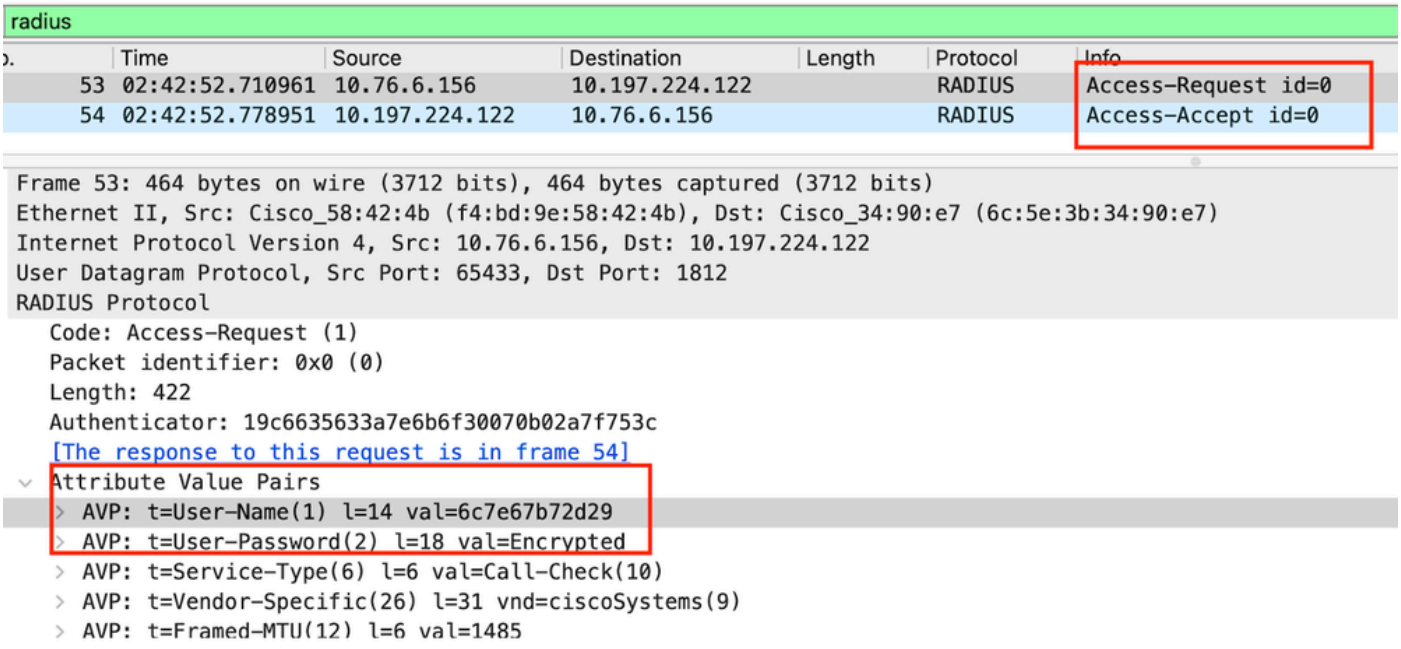
```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d2
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

클라이언트 정책 관리자 상태가 RUN으로 업데이트됨, MAB 인증을 완료하는 클라이언트에 대해 웹 인증을 건너뜁니다.

```
2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
```

임베디드 패킷 캡처를 사용한 확인



Radius 패킷

클라이언트 디바이스에 대한 MAC 인증 실패의 예

연결에 성공한 후 클라이언트에 대해 시작된 Mac 인증

```
2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Succes
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
```

이 디바이스 항목이 ISE에 없으므로 ISE에서 Access-Reject(액세스 거부)를 보냅니다.

```
2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000
```

MAB로 클라이언트 장치에 대해 시작된 웹 인증 실패

```
2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9  Cli
```

클라이언트가 HTTP GET 요청을 시작하면 컨트롤러에 의해 해당 TCP 세션이 스푸핑될 때 리디렉션 URL이 클라이언트 디바이스에 푸시됩니다.

```
2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6
```

클라이언트는 리디렉션 URL에 대한 HTTP Get을 시작하고 페이지가 로드되면 로그인 자격 증명이 제출됩니다.

컨트롤러가 ISE에 액세스 요청을 보냅니다.

이는 Access-Accept 패킷에서 유효한 사용자 이름이 관찰되었으므로 웹 인증입니다

```
2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Vendor, Cisco
```

ISE에서 Access-Accept 수신

```
2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS:  Message-Authenticato
```

웹 인증에 성공했으며 클라이언트 상태가 RUN 상태로 전환되었습니다.

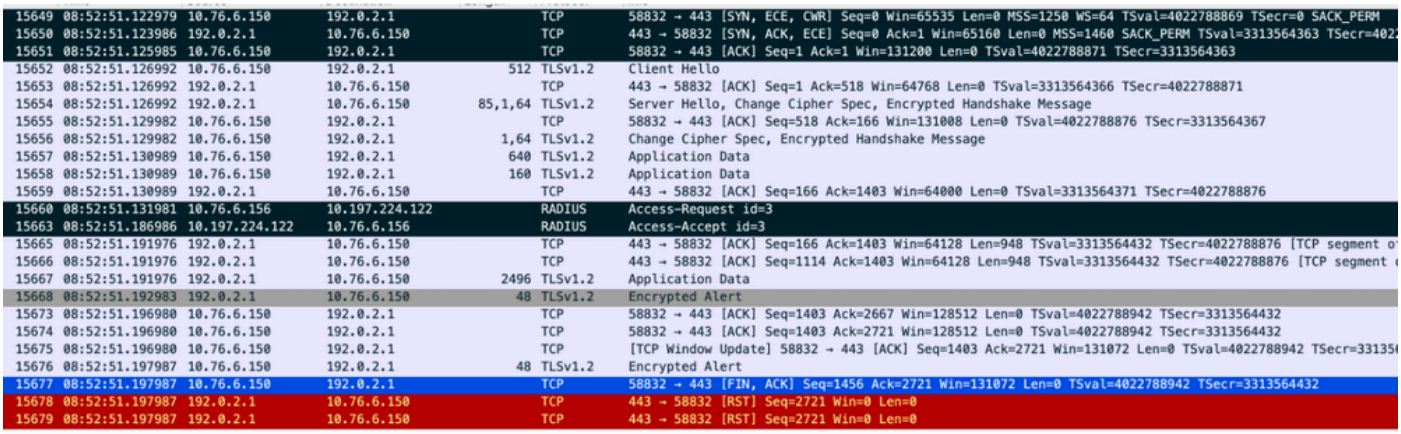
```
2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db
```

EPC 캡처를 통한 확인

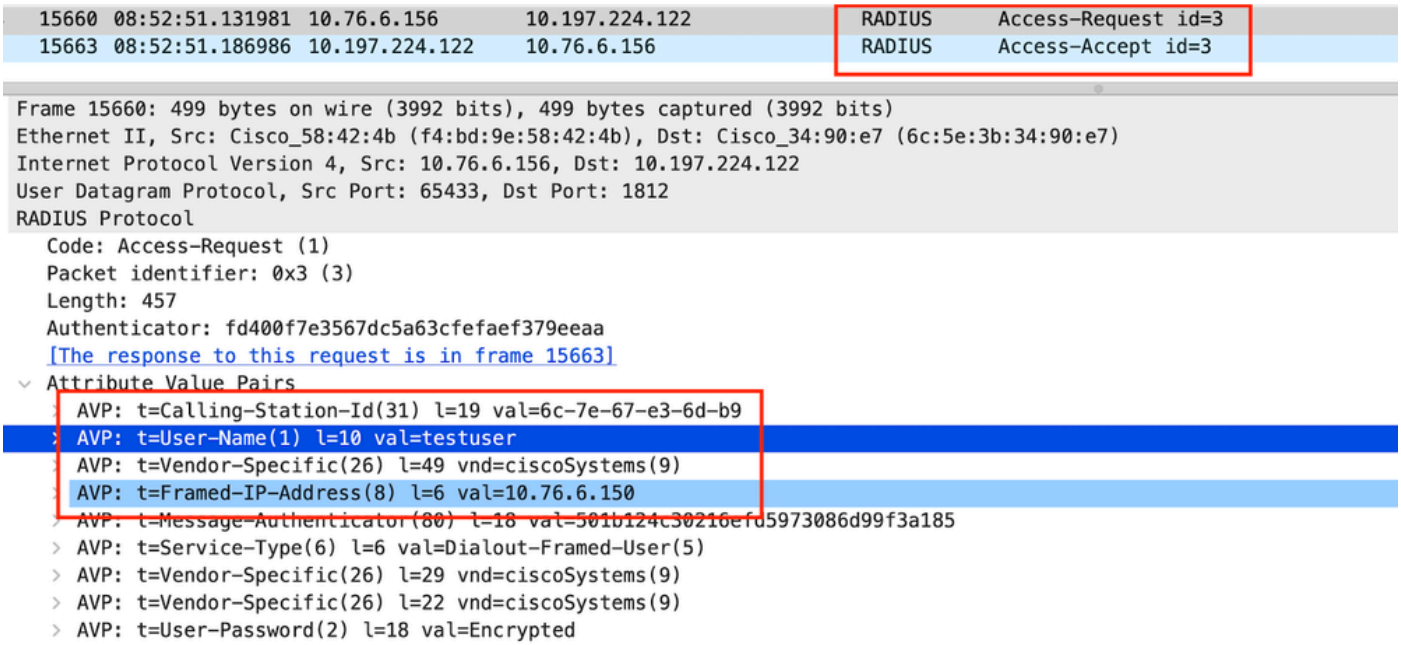
클라이언트는 컨트롤러 가상 IP 주소로 TCP 핸드셰이크를 완료하고 클라이언트는 리디렉션 포털 페이지를 로드합니다. 사용자가 사용자 이름 및 비밀번호를 제출하면 컨트롤러 관리 IP 주소에서 radius access-request를 관찰할 수 있습니다.

인증에 성공하면 클라이언트 TCP 세션이 닫히고 컨트롤러에서 클라이언트가 RUN 상태로 전환됩

니다.

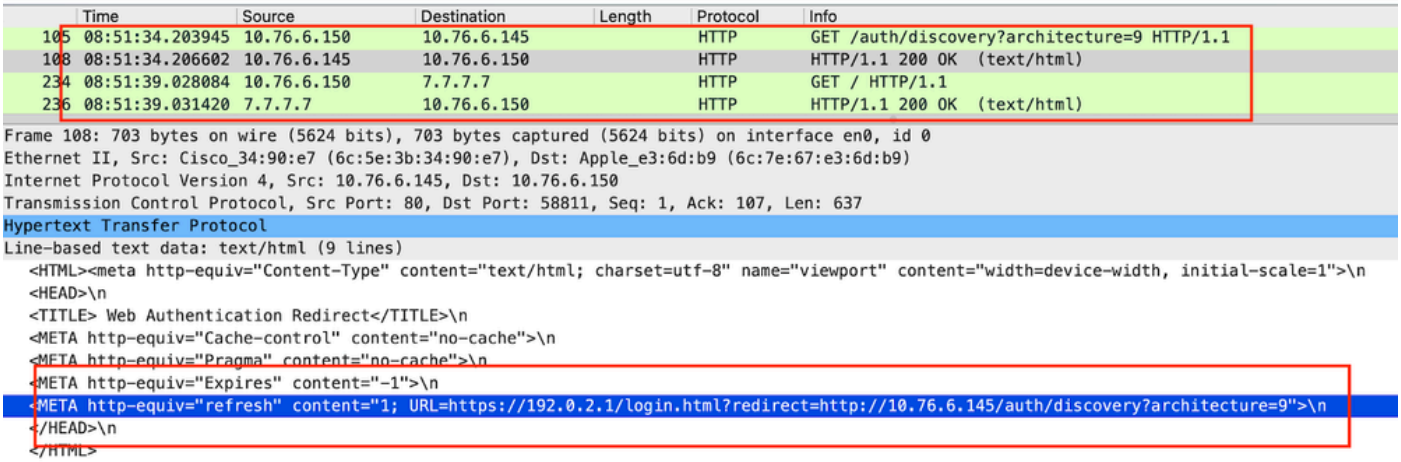


RADIUS 패킷을 사용하는 TCP 흐름



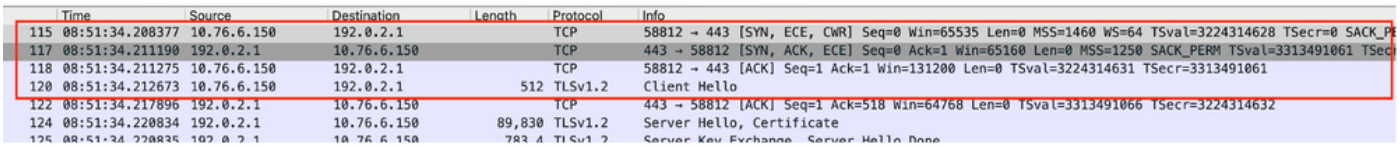
사용자 자격 증명과 함께 ISE로 전송된 RADIUS 패킷

클라이언트 트래픽을 검증하기 위한 클라이언트 측 wireshark 캡처는 포털 페이지로 리디렉션되고 컨트롤러 가상 ip 주소/웹 서버에 대한 TCP 핸드셰이크를 검증합니다.



리디렉션 URL을 검증하기 위한 클라이언트측 캡처

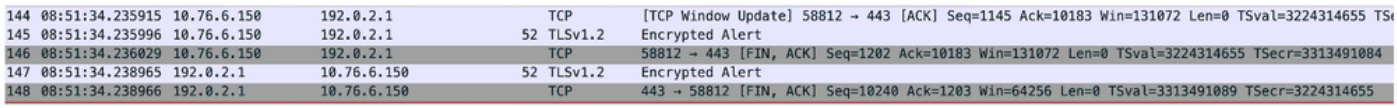
클라이언트가 컨트롤러의 가상 IP 주소에 대한 TCP 핸드셰이크를 설정합니다



	Time	Source	Destination	Length	Protocol	Info
115	08:51:34.208377	10.76.6.150	192.0.2.1		TCP	58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PE
117	08:51:34.211190	192.0.2.1	10.76.6.150		TCP	443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr
118	08:51:34.211275	10.76.6.150	192.0.2.1		TCP	58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120	08:51:34.212673	10.76.6.150	192.0.2.1	512	TLSv1.2	Client Hello
122	08:51:34.217896	192.0.2.1	10.76.6.150		TCP	443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124	08:51:34.220834	192.0.2.1	10.76.6.150	89,830	TLSv1.2	Server Hello, Certificate
125	08:51:34.220835	192.0.2.1	10.76.6.150	783	TLSv1.2	Server Key Exchange, Server Hello Done

클라이언트와 웹 서버 간의 TCP 핸드셰이크

웹 인증에 성공한 후 세션이 닫힙니다.



144	08:51:34.235915	10.76.6.150	192.0.2.1		TCP	[TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSe
145	08:51:34.235996	10.76.6.150	192.0.2.1	52	TLSv1.2	Encrypted Alert
146	08:51:34.236029	10.76.6.150	192.0.2.1		TCP	58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147	08:51:34.238965	192.0.2.1	10.76.6.150	52	TLSv1.2	Encrypted Alert
148	08:51:34.238966	192.0.2.1	10.76.6.150		TCP	443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655

클라이언트가 웹 인증을 완료한 후 TCP 세션이 닫힘

관련 기사

Catalyst 9800 Wireless LAN Controller의 무선 디버깅 및 로그 수집 이해

9800의 웹 기반 인증

9800에서 로컬 웹 인증 구성

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.