Wireless LAN Controller에서 유선 게스트 확인 및 문제 해결 구성

목차

소개

이 문서에서는 외부 웹 인증을 사용하여 9800 및 IRCM에서 유선 게스트 액세스를 구성, 확인 및 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

9800 WLC

아이레OS WLC

모빌리티 터널

ISE

유선 게스트 액세스를 구성하기 전에 두 WLC 간의 모빌리티 터널이 설정된 것으로 가정합니다.

이 측면은 이 컨피그레이션 예의 범위를 벗어납니다. 자세한 지침은 Configuring Mobility Topologies on 9800이라는 제목의 첨부 문서를 참조하십시오

사용되는 구성 요소

9800 WLC 버전 17.12.1

5520 WLC 버전 8.10.185.0

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.

다른 catalyst 9800에 고정된 catalyst 9800에서 유선 게스트 구성

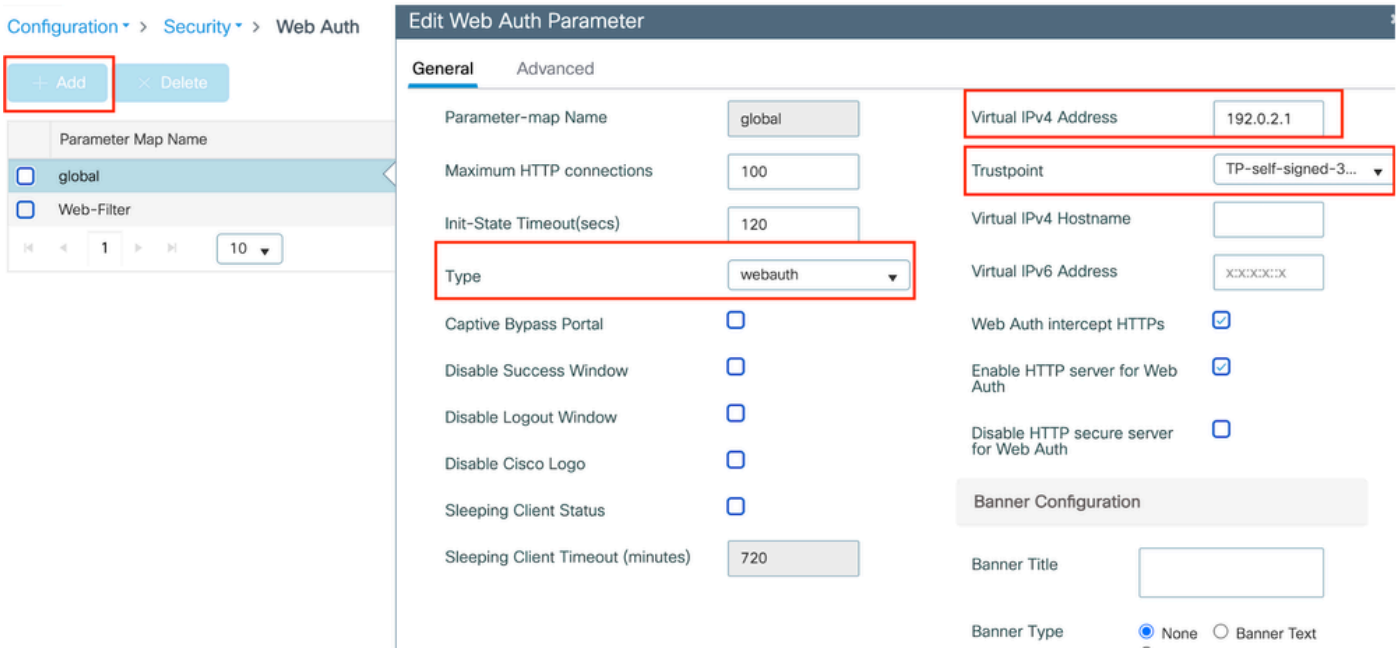
네트워크 다이어그램

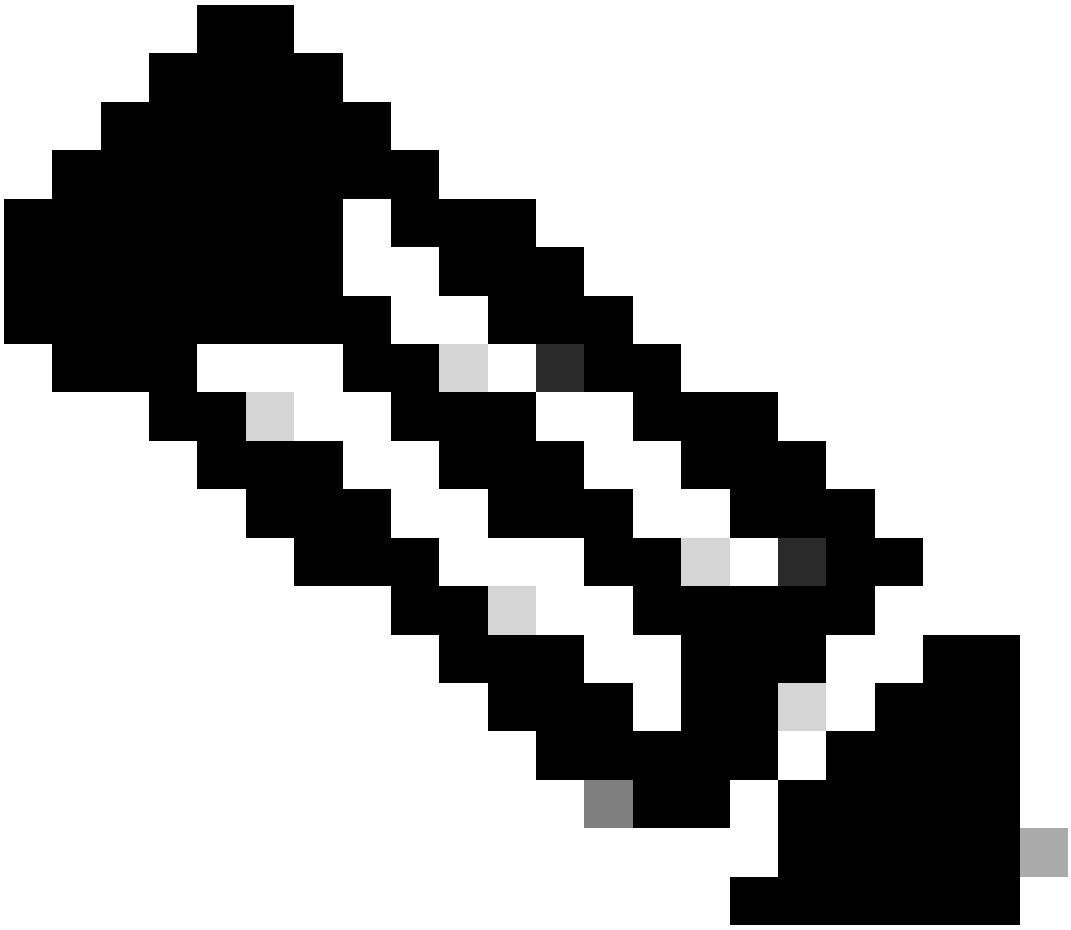
네트워크 토폴로지

외부 9800 WLC의 컨피그레이션

웹 매개 변수 맵 구성

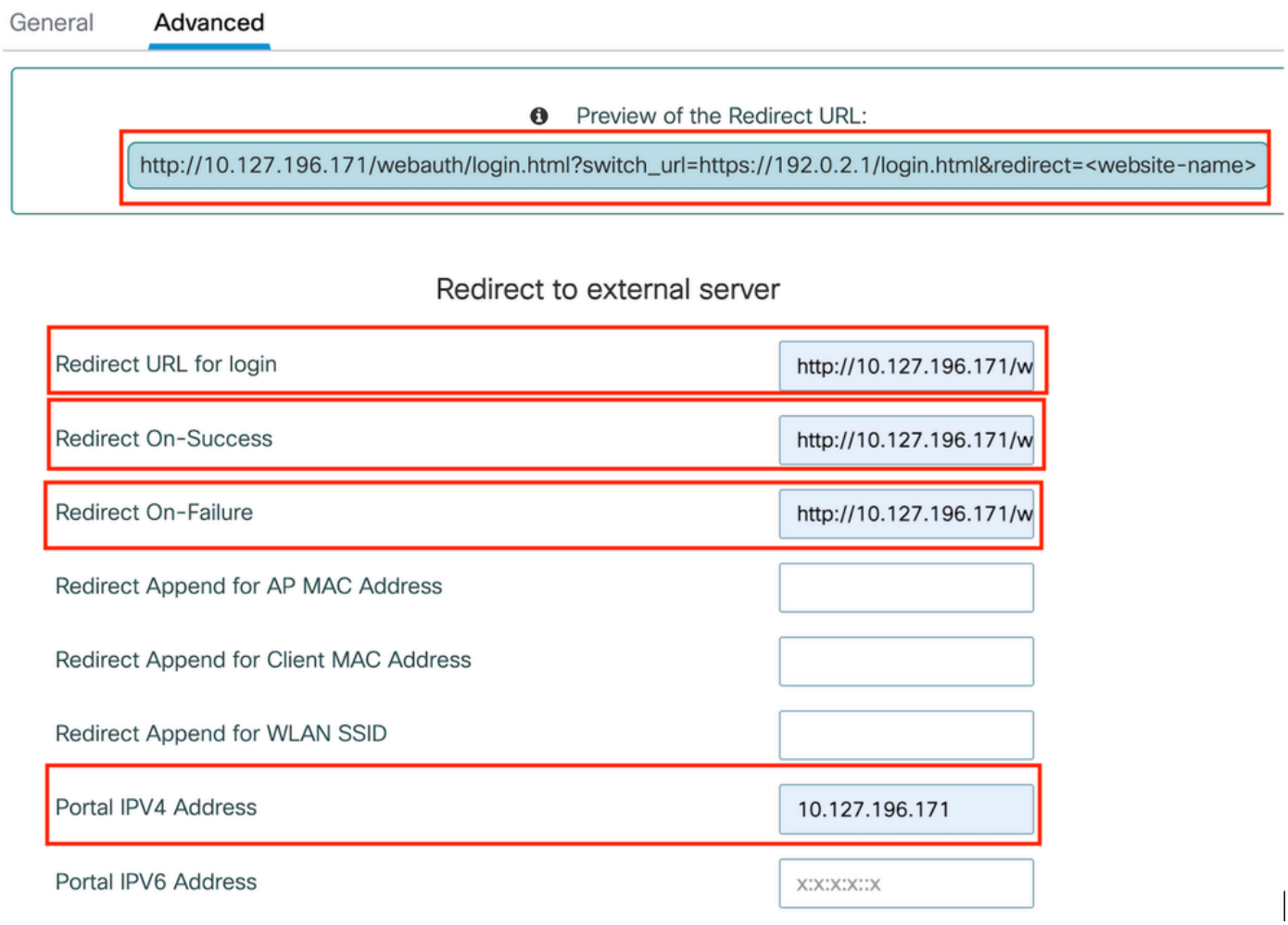
1단계: Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고, Global(전역)을 선택하고, 컨트롤러 및 신뢰 지점 매핑의 가상 IP 주소를 확인하고, 유형이 webauth로 설정되어 있는지 확인합니다.





참고: 웹 인증 가로채기 HTTP는 선택적 설정입니다. HTTPS 리디렉션이 필요한 경우 Web Auth intercept HTTPS 옵션을 활성화해야 합니다. 그러나 이 컨피그레이션은 CPU 사용량을 증가시키므로 권장되지 않습니다.

2단계: Advanced(고급) 탭에서 클라이언트 리디렉션을 위한 외부 웹 페이지 URL을 구성합니다. "Redirect URL for Login(로그인을 위한 리디렉션 URL)" 및 "Redirect On-Failure(장애 시 리디렉션)"를 설정합니다. "Redirect On-Success(성공 시 리디렉션)"는 선택 사항입니다. 구성된 리디렉션 URL의 미리 보기는 웹 인증 프로파일에 표시됩니다.



고급 탭

CLI 컨피그레이션

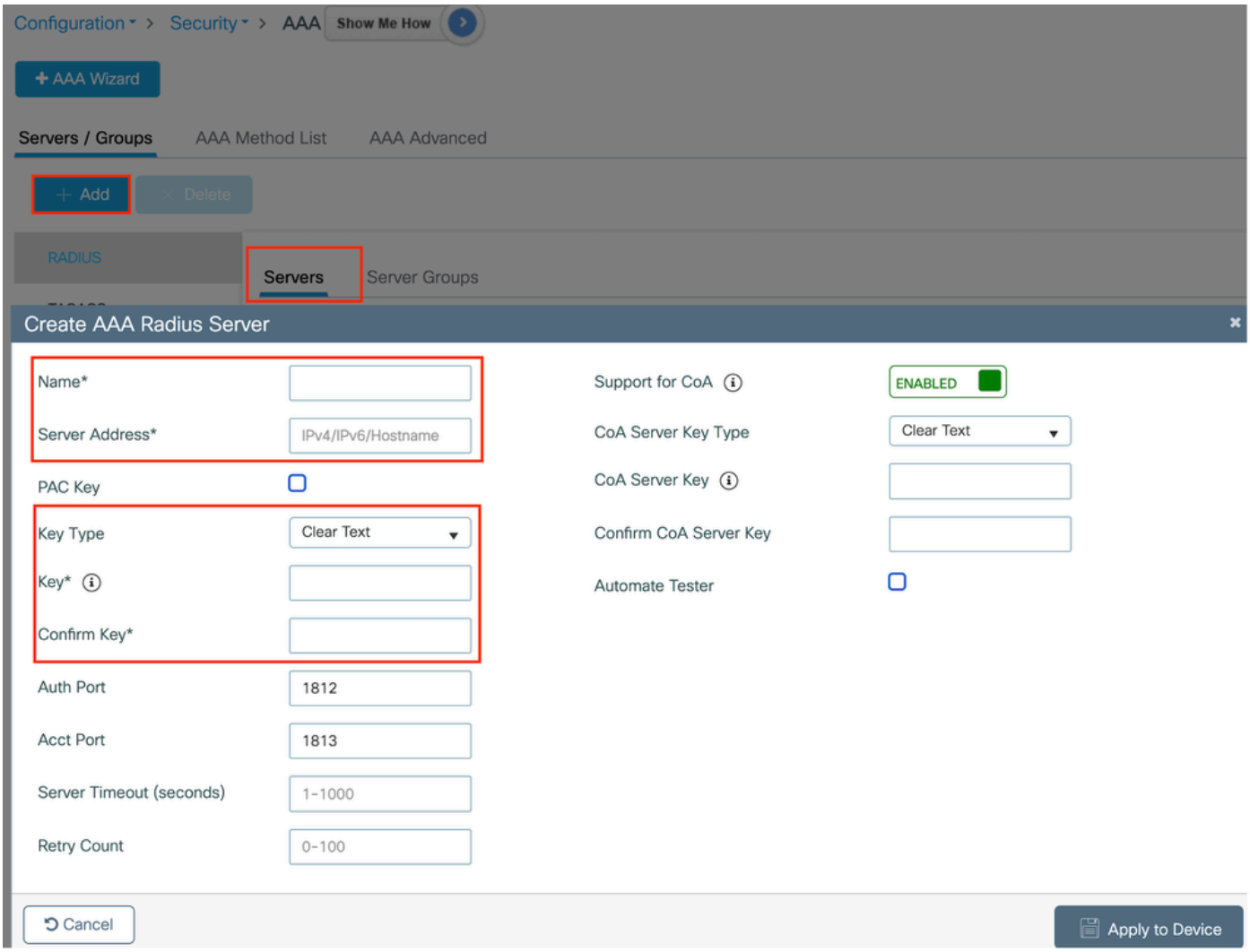
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

주: 이 시나리오에서는 글로벌 매개변수 맵이 사용됩니다. 요구 사항에 따라 Add(추가)를 선택하여 사용자 지정 웹 매개변수 맵을 구성하고 Advanced(고급) 탭 아래에서 리디렉션 URL을 설정합니다. 신뢰 지점 및 가상 IP 설정은 전역 프로필에서 상속됩니다.

AAA 설정:

1단계: Radius 서버 생성:

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



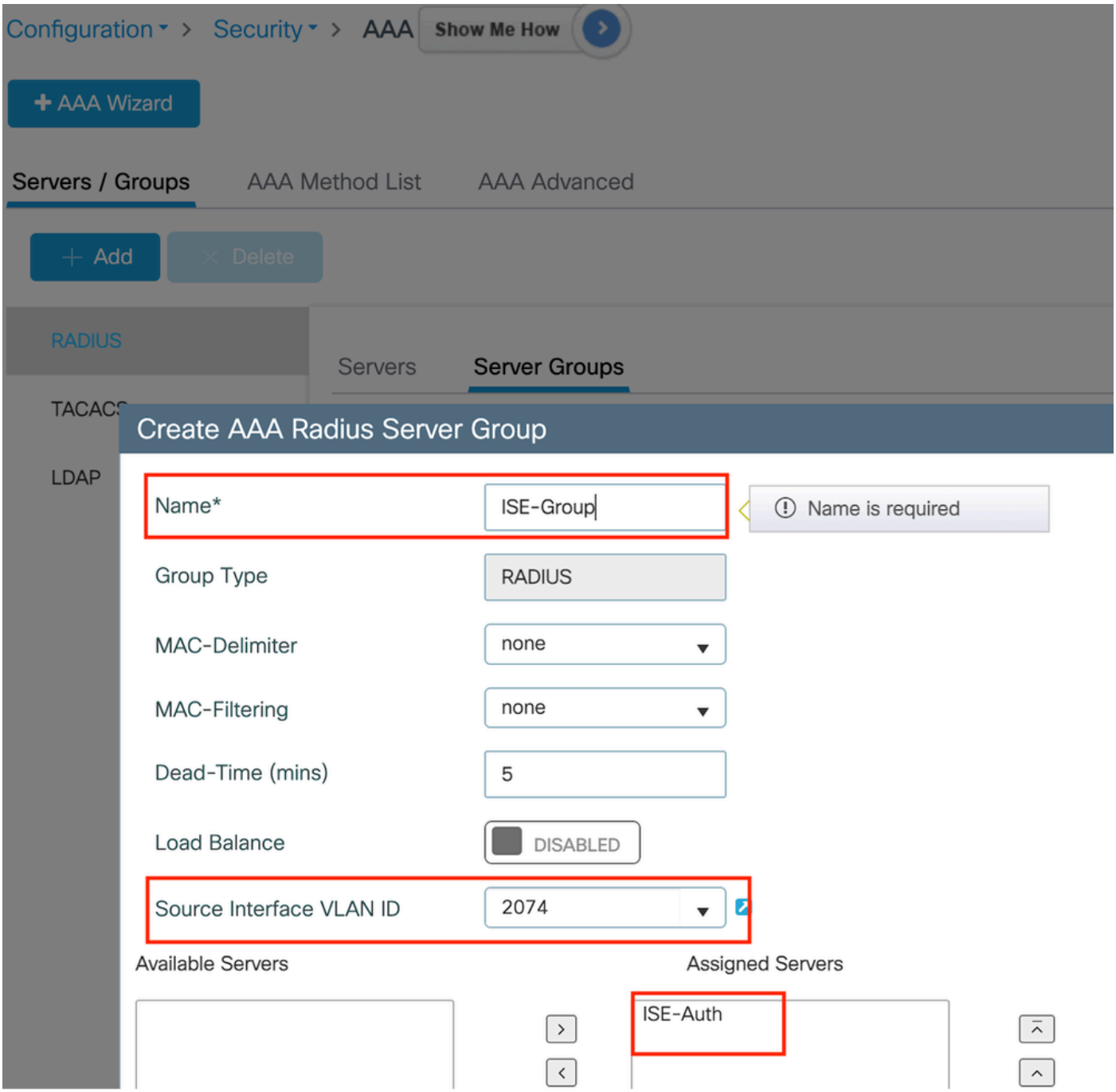
Radius 서버 컨피그레이션

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 그룹 생성:

Server Groups(서버 그룹) 섹션에서 "Add(추가)"를 선택하여 서버 그룹을 정의하고 그룹 컨피그레이션에 포함할 서버를 전환합니다.



Radius 서버 그룹

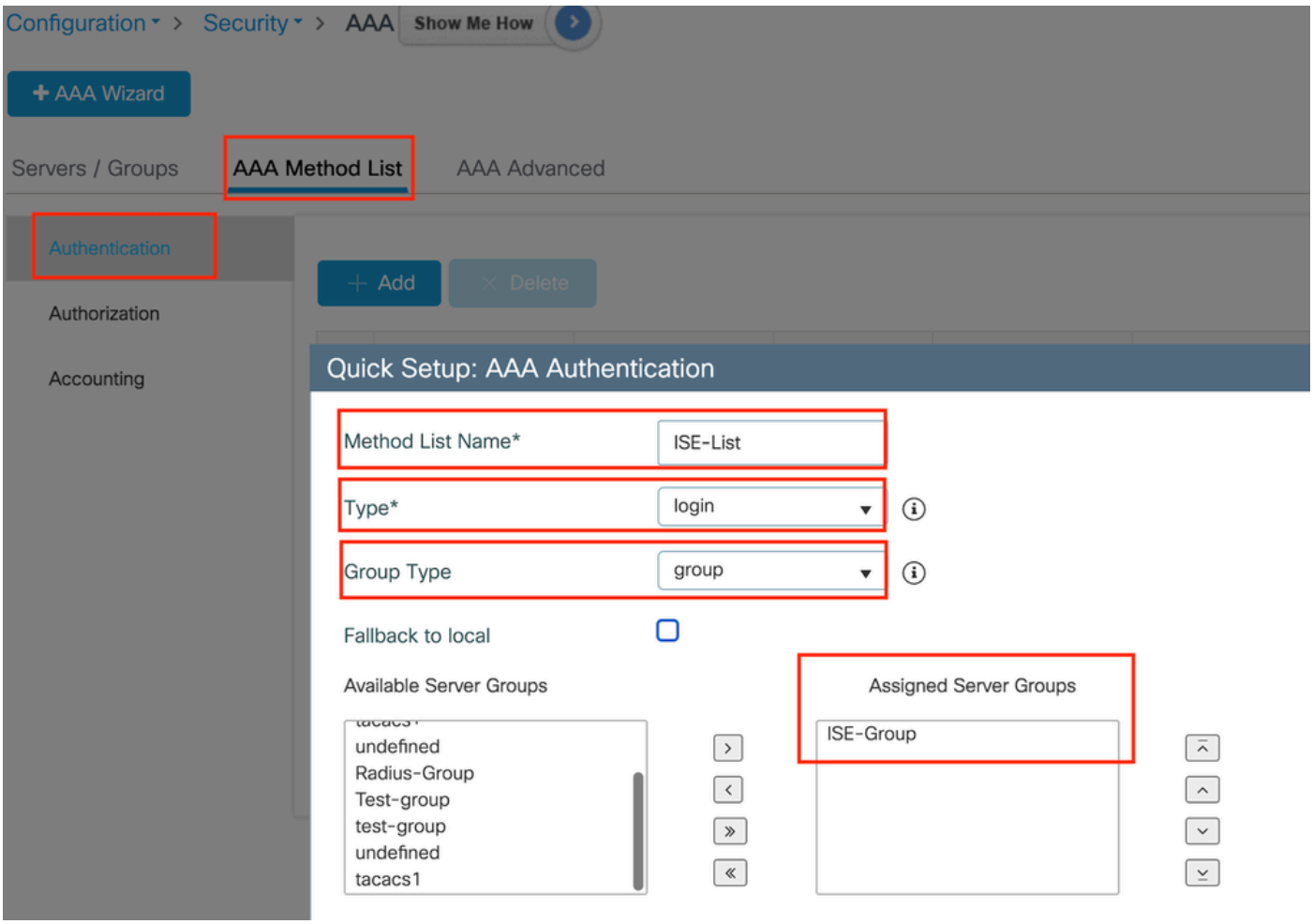
CLI 컨피그레이션

```
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 방법 목록) 탭으로 이동하여 Authentication(인증)에서 Add(추가)를 선택하고

Type(유형)을 "login(로그인)"으로, Group type(그룹 유형)을 "Group(그룹)"으로 지정하여 방법 목록 이름을 정의하고 Assigned Server Group(할당된 서버 그룹) 섹션 아래에서 구성된 인증 서버 그룹을 매핑합니다.



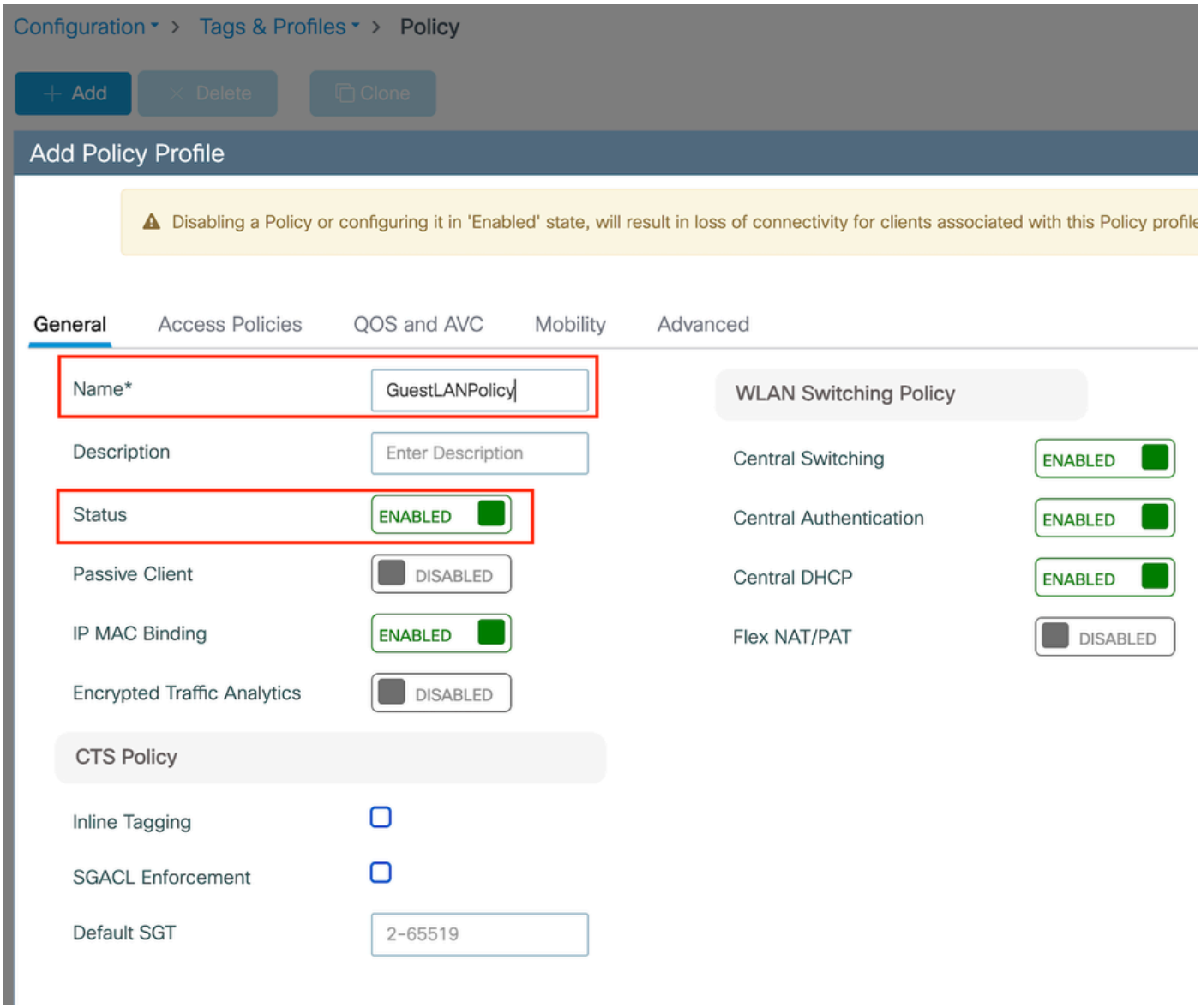
인증 방법 목록

CLI 컨피그레이션

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

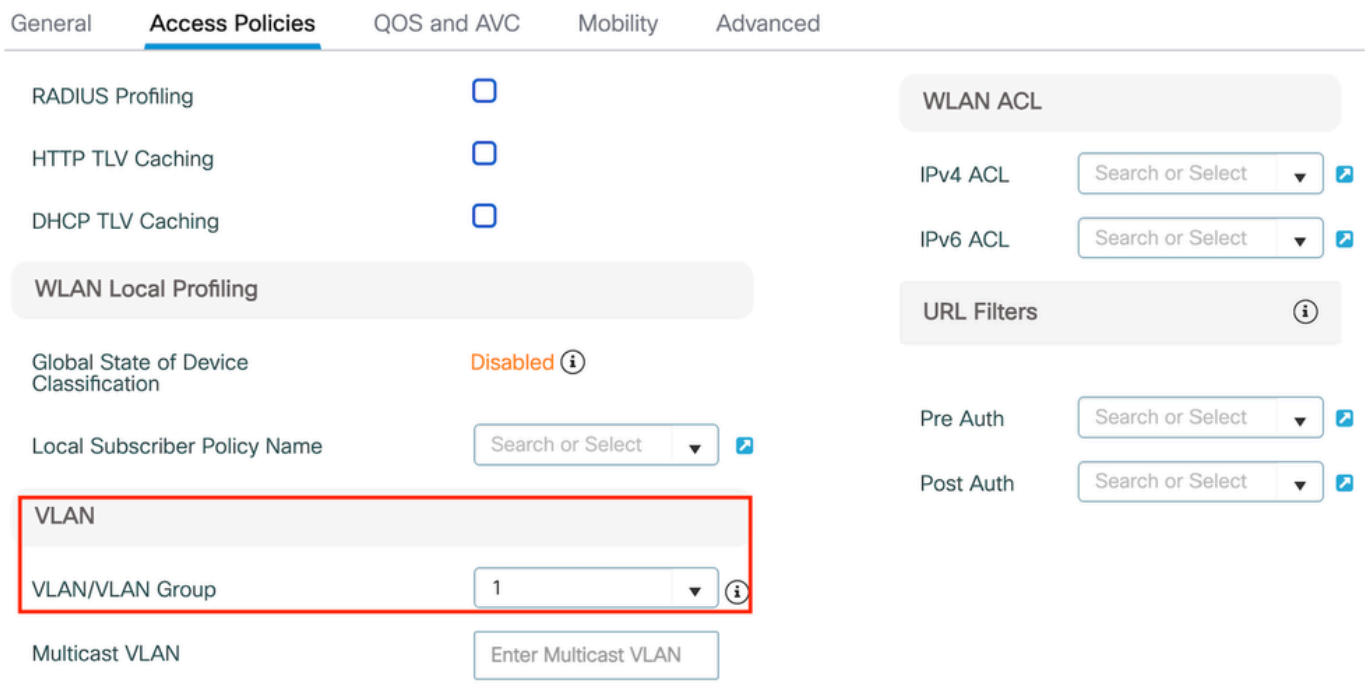
정책 프로필 구성

1단계: Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동하고 General(일반) 탭에서 새 프로필의 이름을 지정한 다음 상태 토글을 사용하여 활성화합니다.



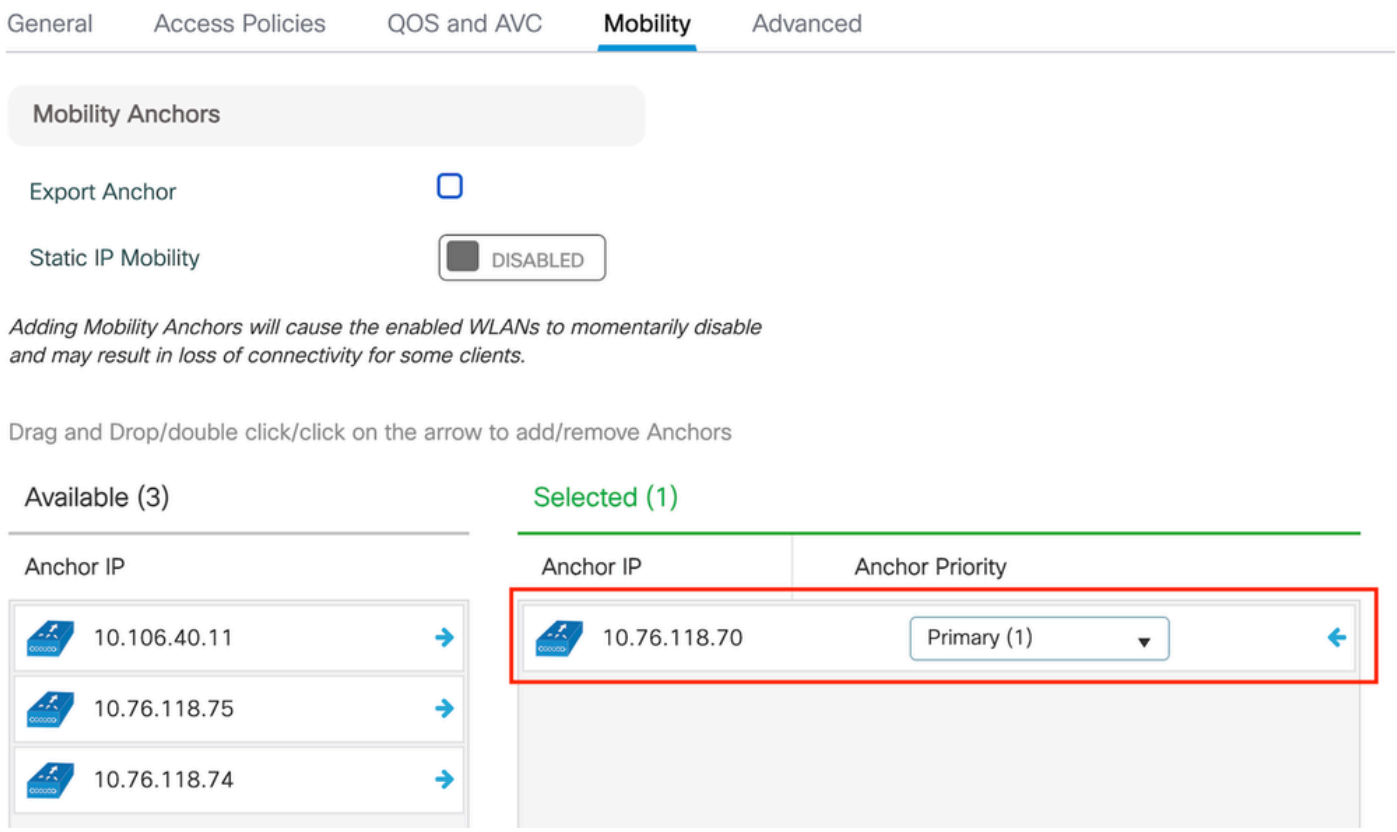
정책 프로파일

2단계: Access Policies(액세스 정책) 탭 아래에서 anchor controller(앵커 컨트롤러)에서 vlan 매핑이 완료될 때 임의의 vlan을 할당합니다. 이 예에서는 vlan 1이 구성됩니다



액세스 정책 탭

3단계: Mobility(모빌리티) 탭 아래에서 Anchor(앵커) 컨트롤러를 Primary(1)로 전환하고 선택적으로 이중화 요구 사항을 위한 Secondary 및 Tertiary 모빌리티 터널을 구성합니다



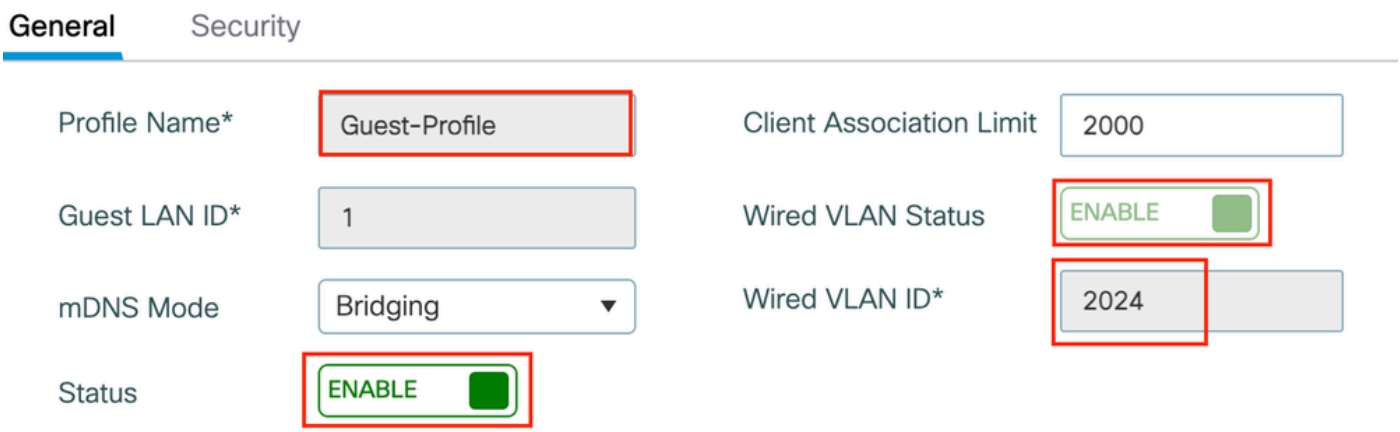
모빌리티 맵

CLI 컨피그레이션

```
wireless profile policy GuestLANPolicy
 mobility anchor 10.76.118.70 priority 1
 no shutdown
```

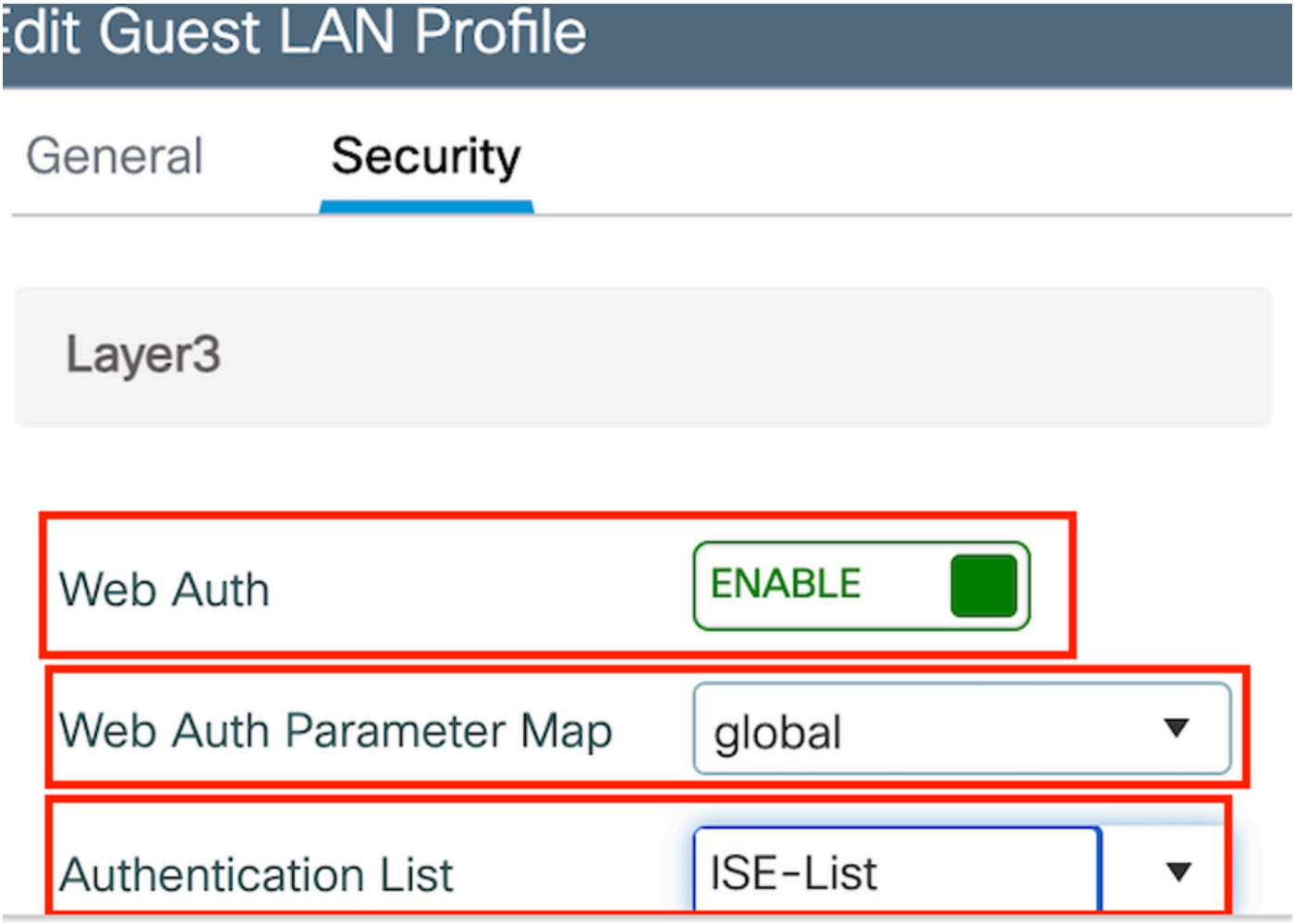
게스트 LAN 프로필 구성

1단계: Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동하고 Add(추가)를 선택하고, 고유한 프로파일 이름을 구성하고, Wired VLAN을 활성화하고, 유선 게스트 사용자의 VLAN ID를 입력하고, 프로파일 상태를 Enabled(활성화됨)로 전환합니다.



게스트 LAN 프로필

2단계: Security(보안) 탭에서 Web Auth(웹 인증)를 활성화하고 Web Auth(웹 인증) 매개변수 맵을 매핑한 다음 Authentication(인증) 드롭다운 목록에서 Radius 서버를 선택합니다.



Guest LAN security(게스트 LAN 보안) 탭

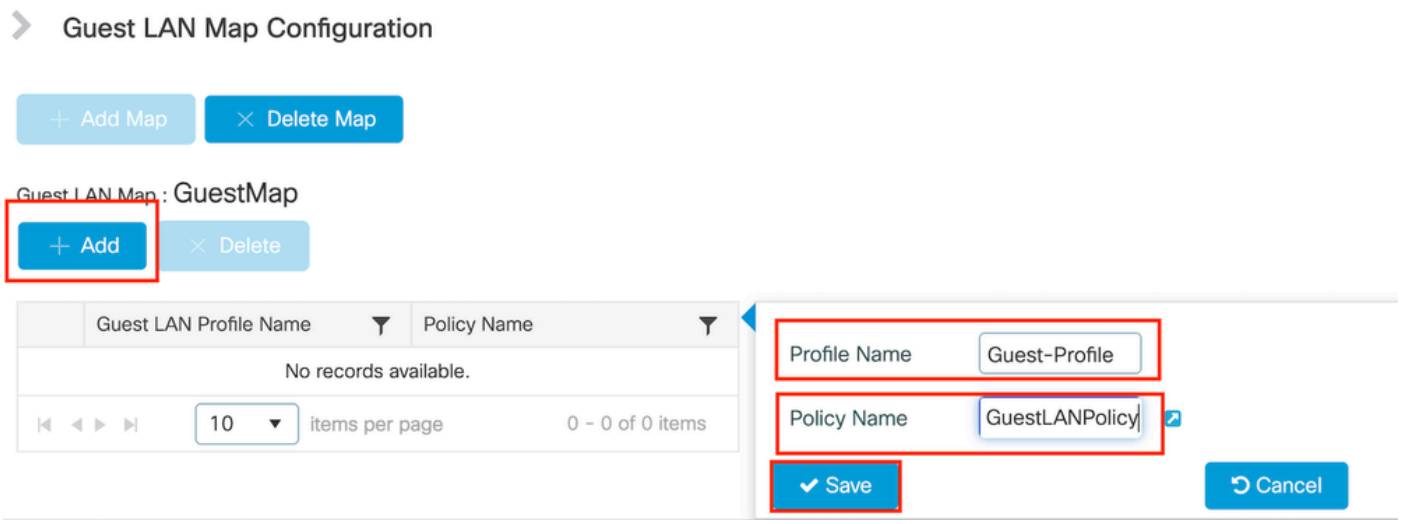
CLI 컨피그레이션

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024
 security web-auth authentication-list ISE-List
 security web-auth parameter-map global
```

게스트 LAN 맵

Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동합니다.

Guest LAN MAP configuration(게스트 LAN 맵 컨피그레이션) 섹션에서 Add(추가)를 선택하고 Policy profile(정책 프로필) 및 Guest LAN profile(게스트 LAN 프로필)을 매핑합니다



게스트 LAN 맵

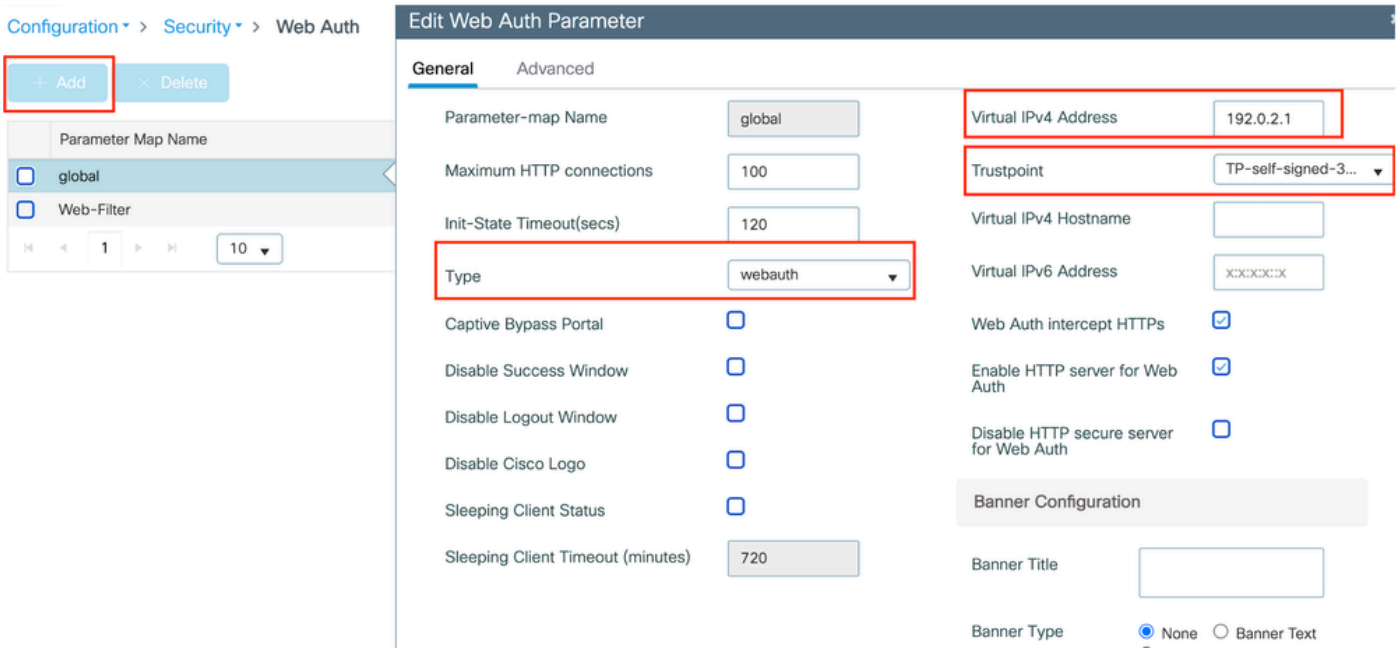
CLI 컨피그레이션

```
wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy
```

앵커 9800 WLC의 컨피그레이션

웹 매개 변수 맵 구성

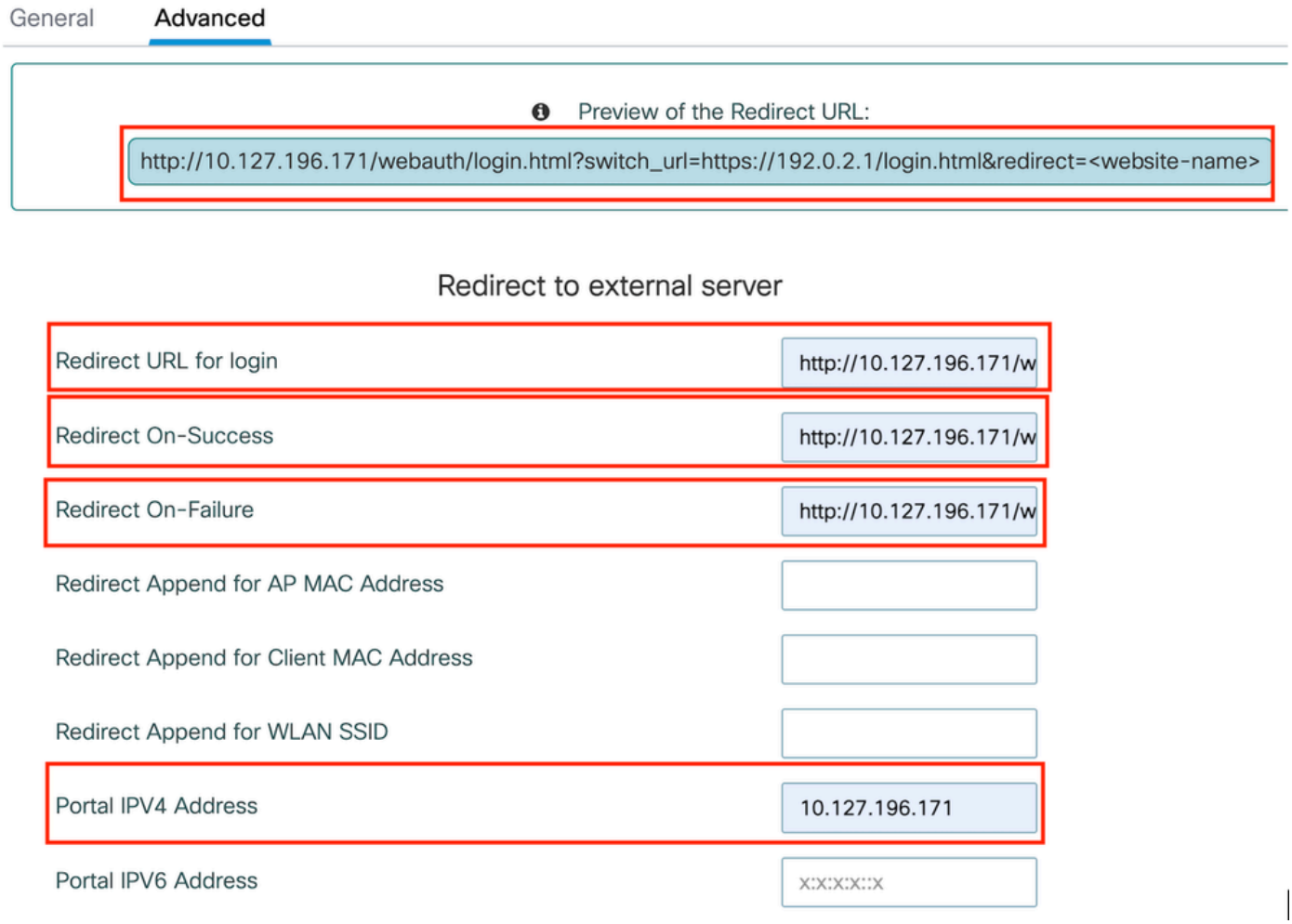
1단계: Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고, Global(전역)을 선택하고, 컨트롤러 및 신뢰 지점 매핑의 가상 IP 주소를 확인하고, 유형이 webauth로 설정되어 있는지 확인합니다.



전역 매개변수 맵

2단계: Advanced(고급) 탭에서 클라이언트 리디렉션을 위한 외부 웹 페이지 URL을 구성합니다. "Redirect URL for Login(로그인을 위한 리디렉션 URL)" 및 "Redirect On-Failure(장애 시 리디렉션)"를 설정합니다. "Redirect On-Success(성공 시 리디렉션)"는 선택 사항입니다.

구성된 리디렉션 URL의 미리 보기는 웹 인증 프로파일에 표시됩니다.



고급 탭

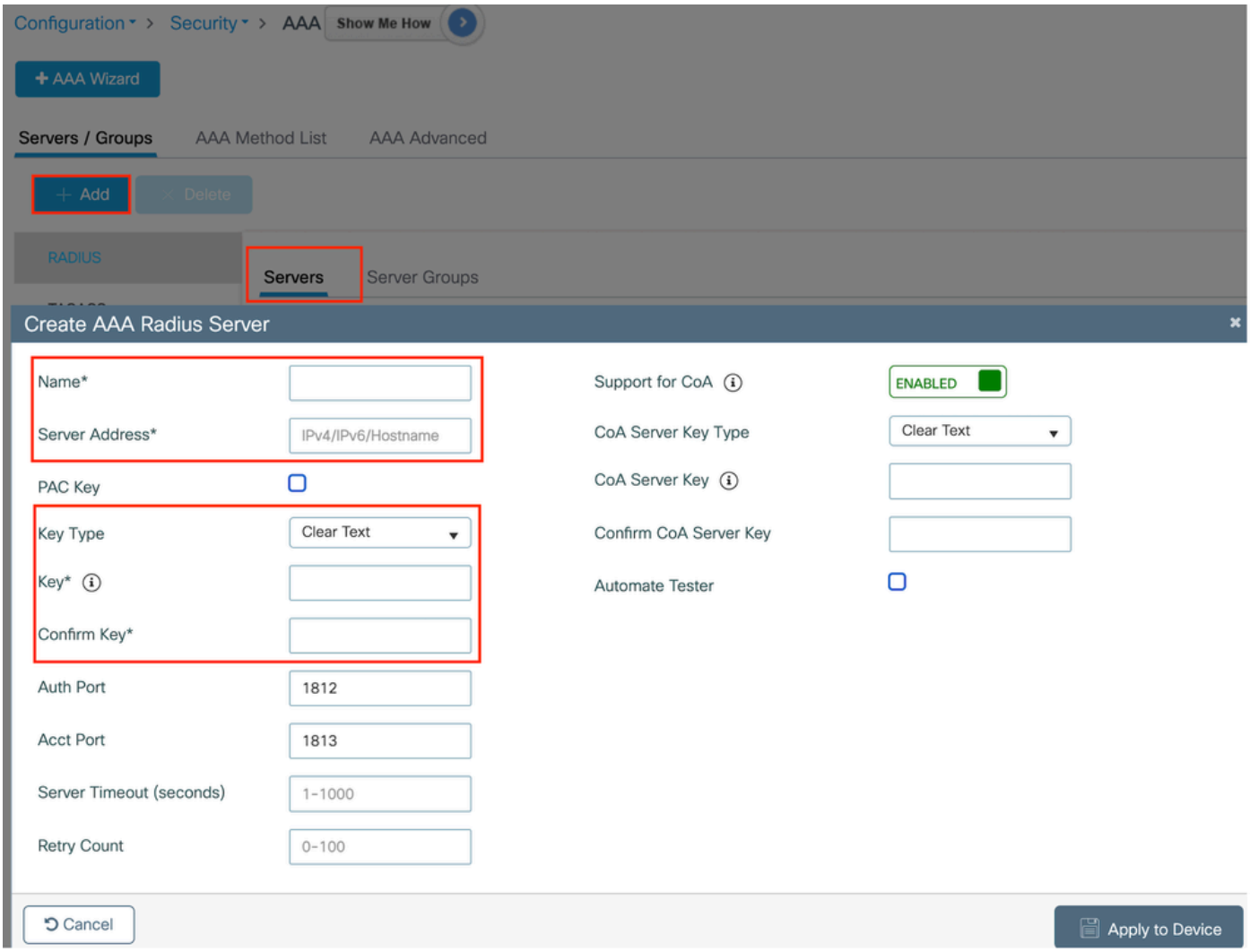
CLI 컨피그레이션

```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable.
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

AAA 설정:

1단계: Radius 서버 생성:

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



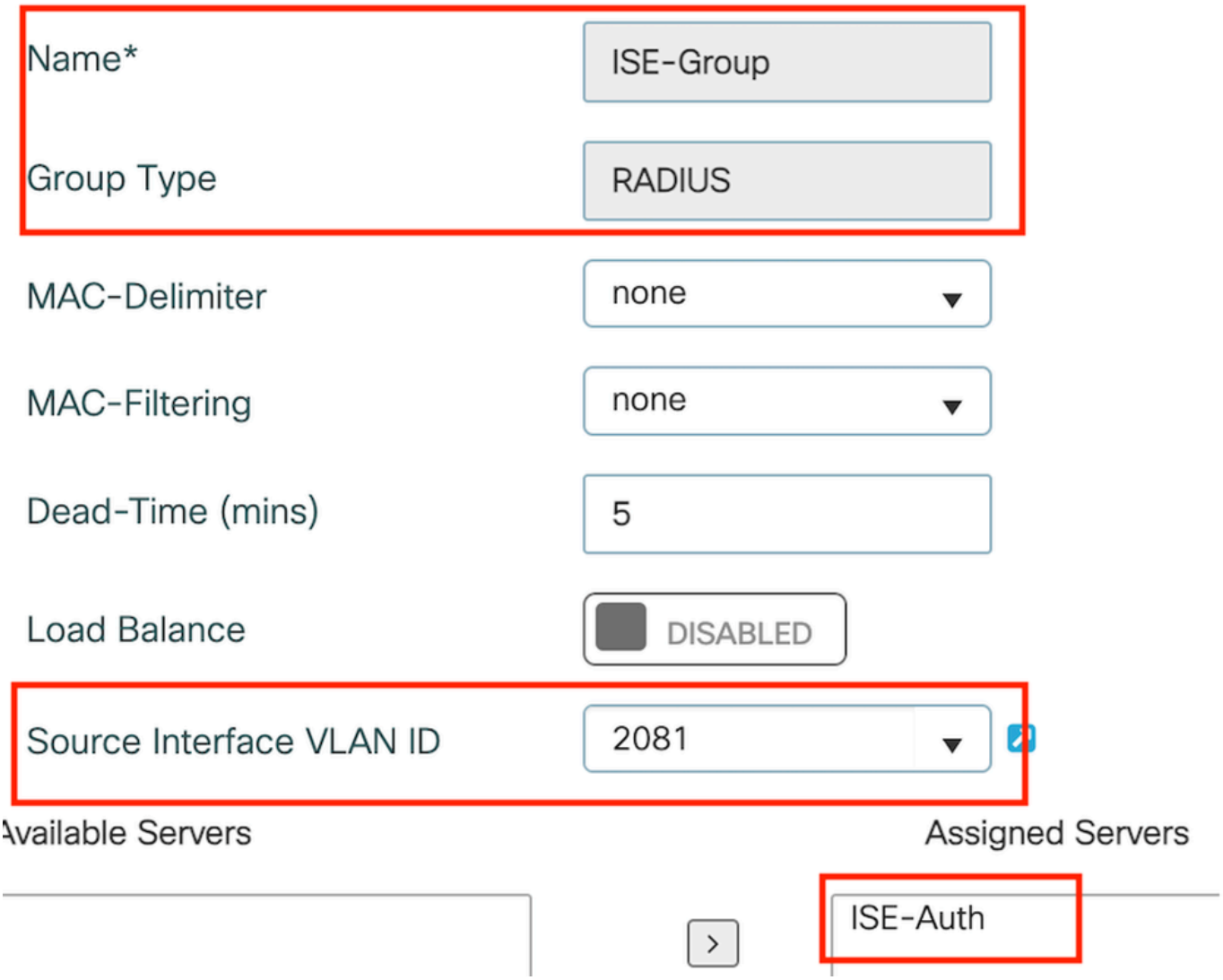
Radius 서버 컨피그레이션

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 그룹 생성:

서버 그룹 섹션에서 추가를 선택하여 서버 그룹을 정의하고 그룹 컨피그레이션에 포함할 서버를 전환합니다.



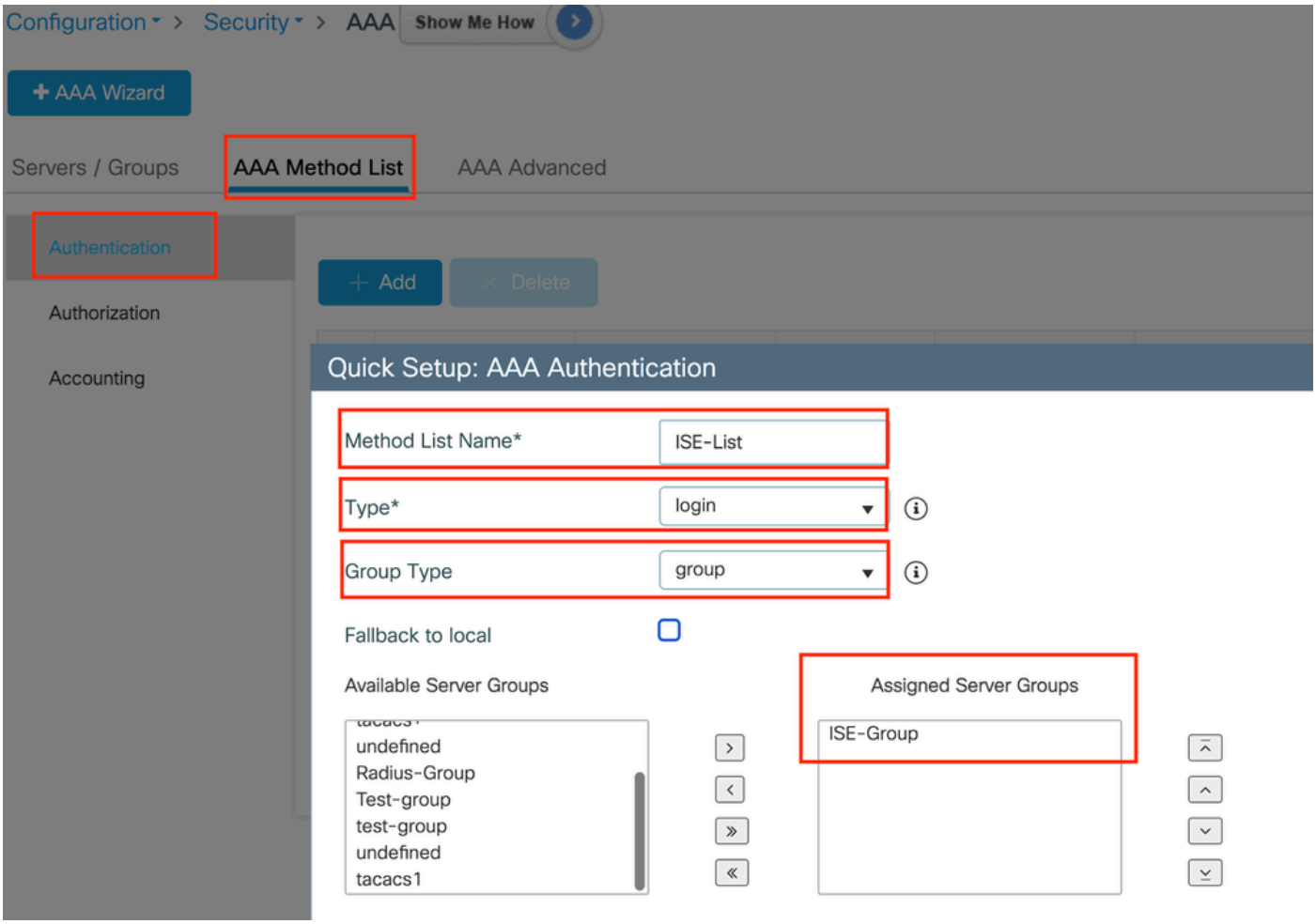
앵커 반경 그룹

CLI 컨피그레이션

```
aaa group server radius ISE-Group
 server name ISE-Auth
 ip radius source-interface Vlan2081
 deadtime 5
```

3단계: AAA 메서드 목록 구성:

AAA Method List(AAA 방법 목록) 탭으로 이동하여 Authentication(인증)에서 Add(추가)를 선택하고, Type(유형)을 "login(로그인)"으로, Group type(그룹 유형)을 "Group(그룹)"으로 지정하여 방법 목록 이름을 정의하고, Assigned Server Group(할당된 서버 그룹) 섹션 아래에서 구성된 인증 서버 그룹을 매핑합니다.



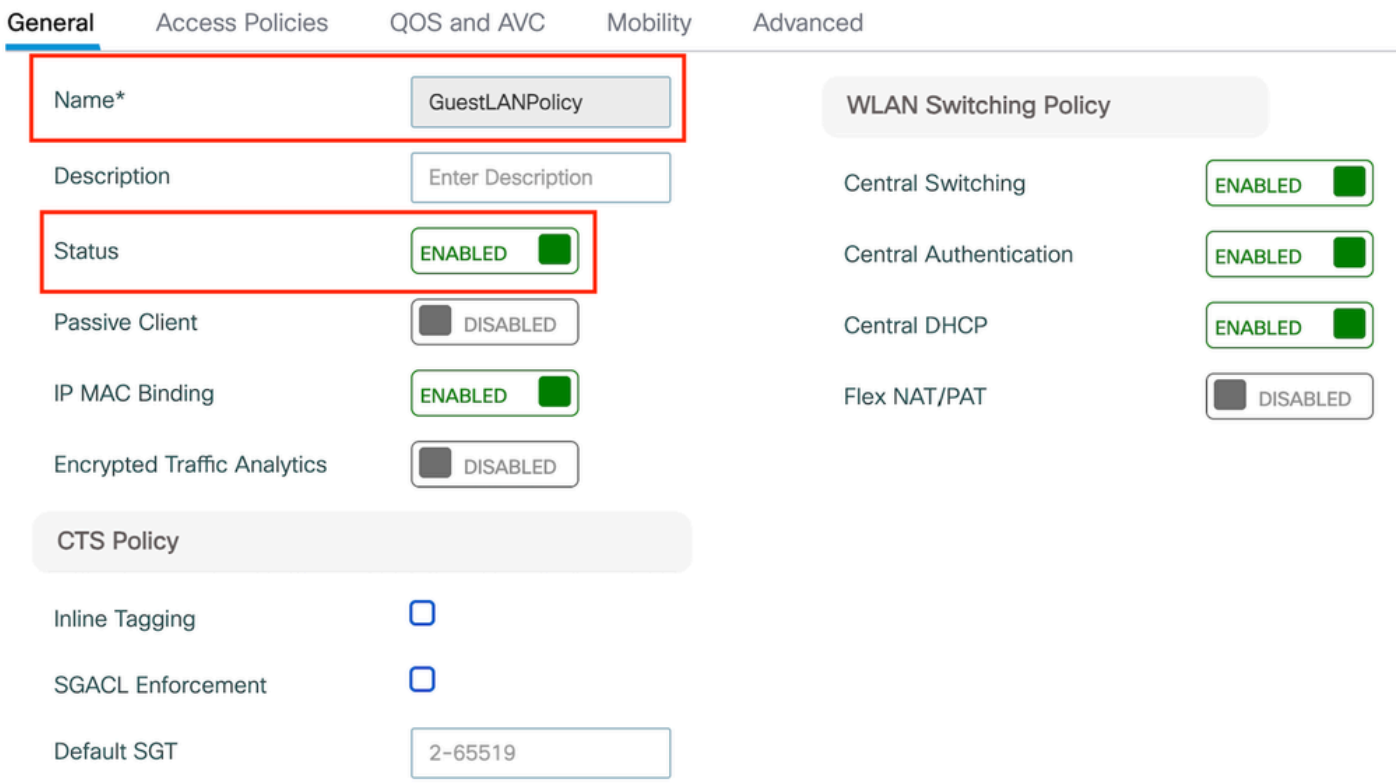
인증 방법 목록

CLI 컨피그레이션

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

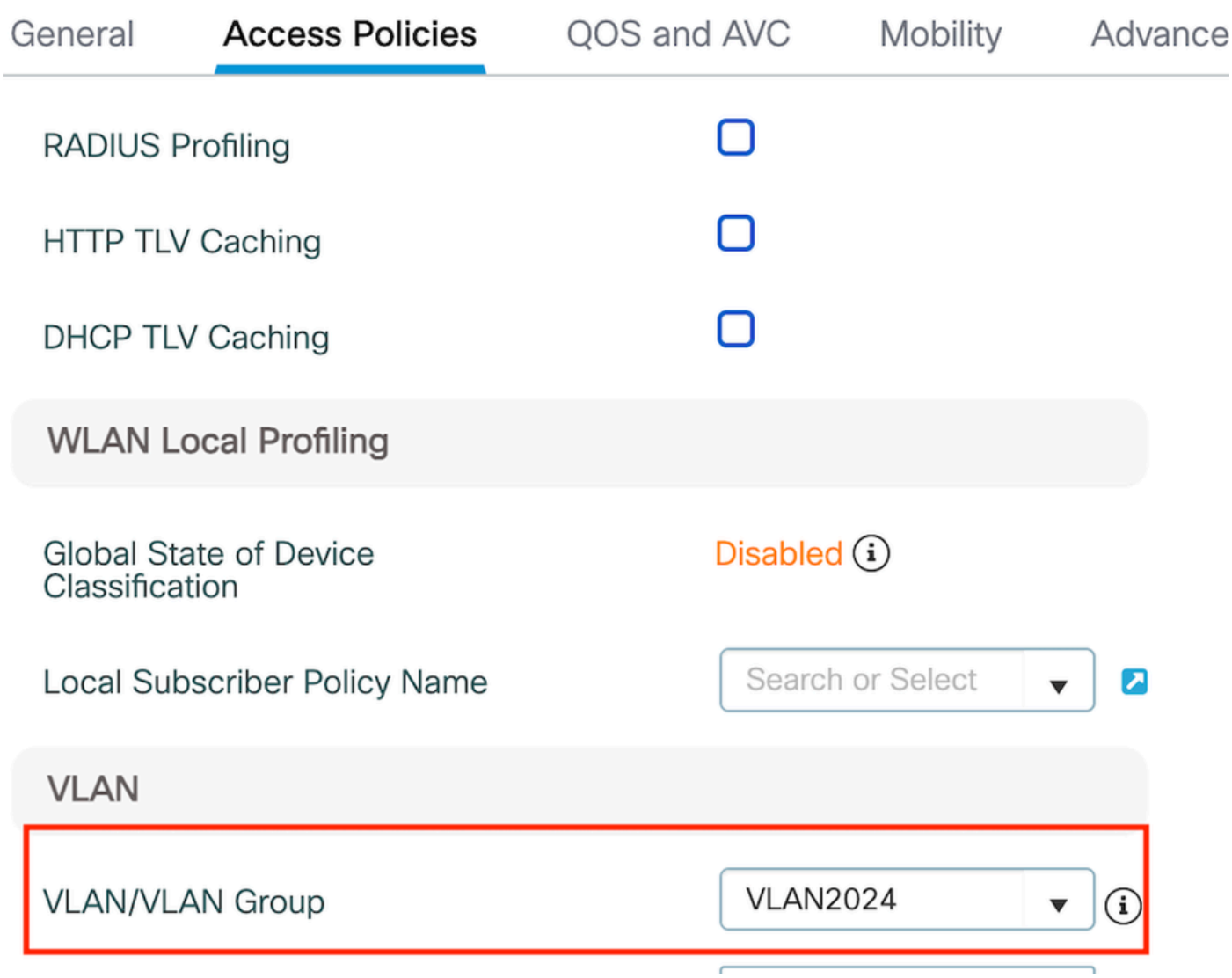
정책 프로필 구성

1단계: Configuration(컨피그레이션) > Tag & Profiles(태그 및 프로필) > Policy(정책)로 이동하여 외부 컨트롤러와 동일한 이름으로 정책 프로필을 구성하고 프로필을 활성화합니다.

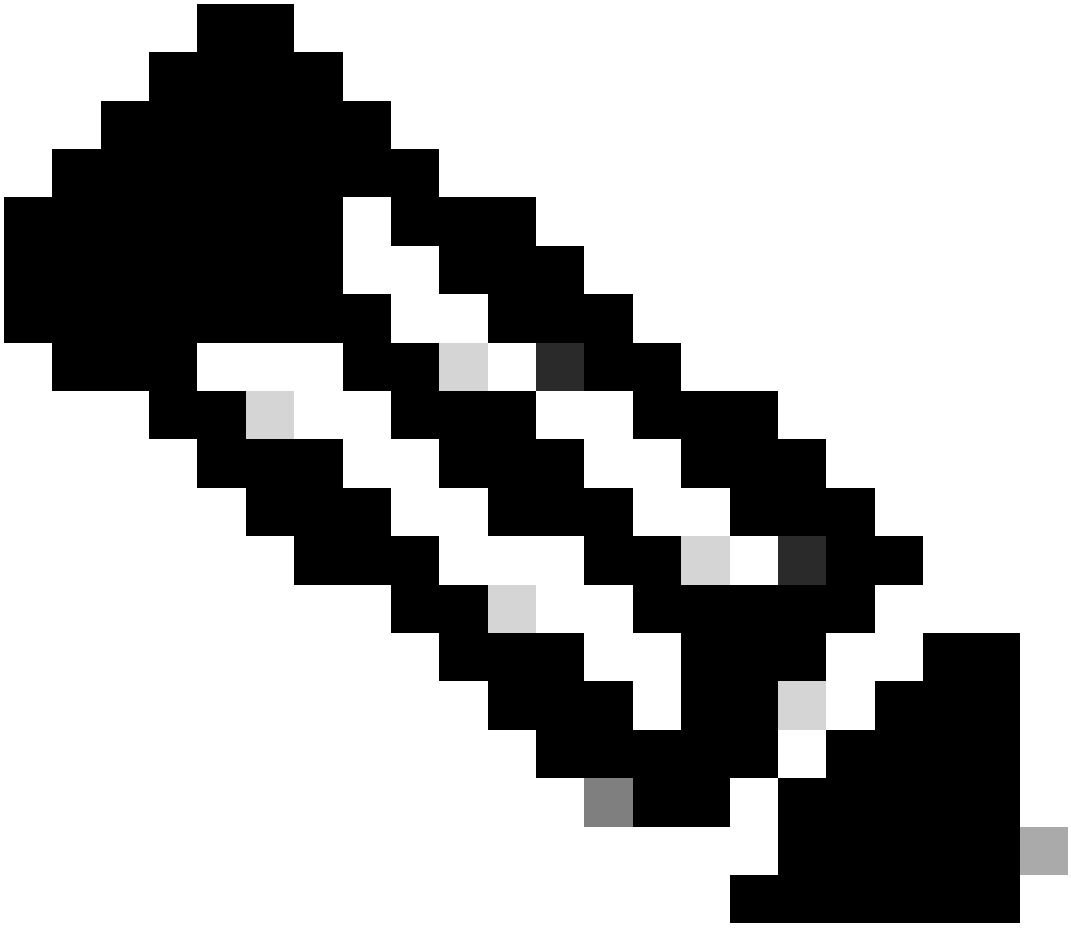


앵커 정책 프로필

2단계: Access Policies(액세스 정책) 아래의 드롭다운 목록에서 유선 클라이언트 vlan을 매핑합니다

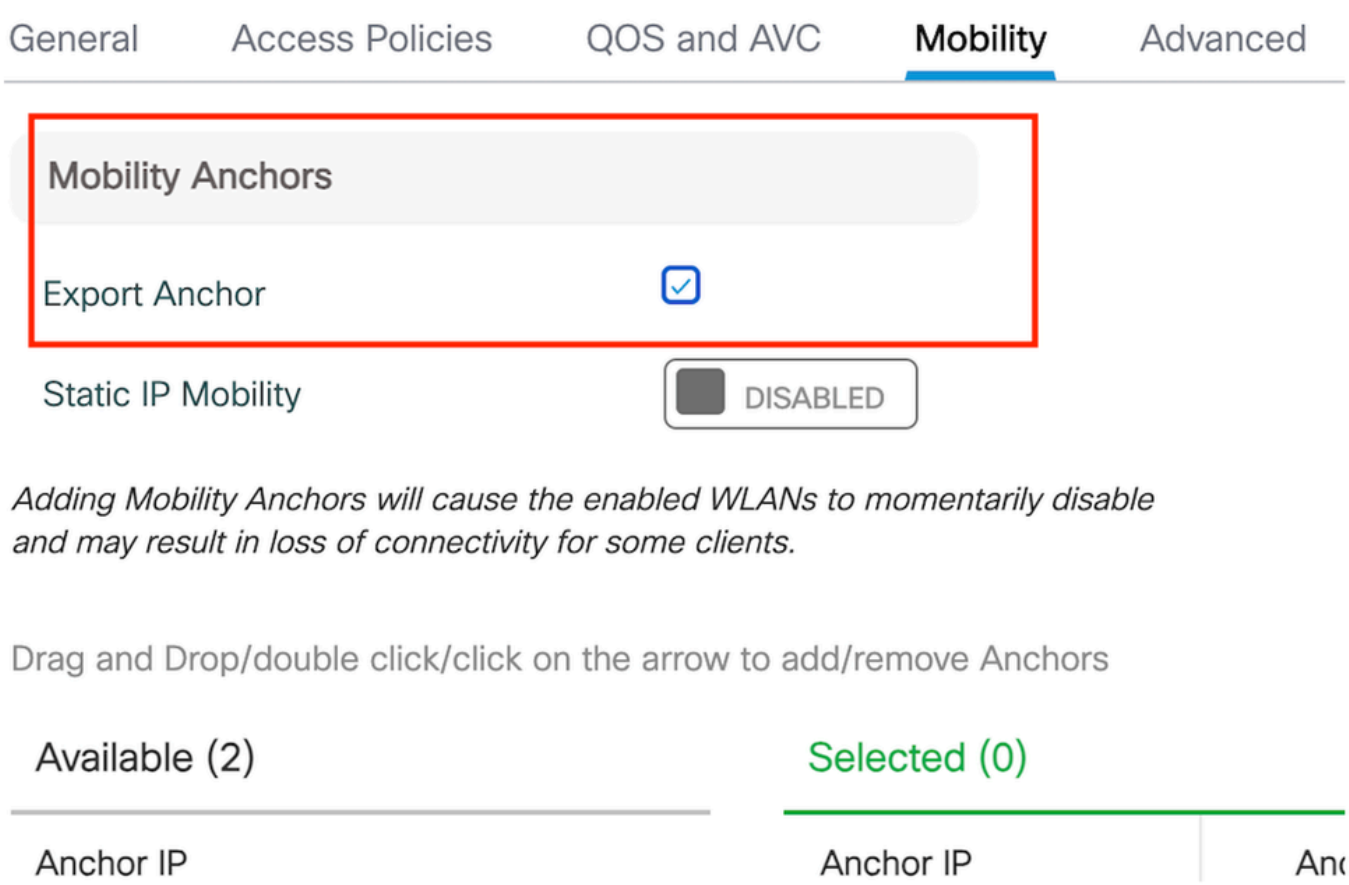

General
Access Policies
QOS and AVC
Mobility
Advance
RADIUS Profiling
HTTP TLV Caching
DHCP TLV Caching
WLAN Local Profiling
Global State of Device Classification
Disabled
Local Subscriber Policy Name
Search or Select
VLAN
VLAN/VLAN Group
VLAN2024

액세스 정책 탭

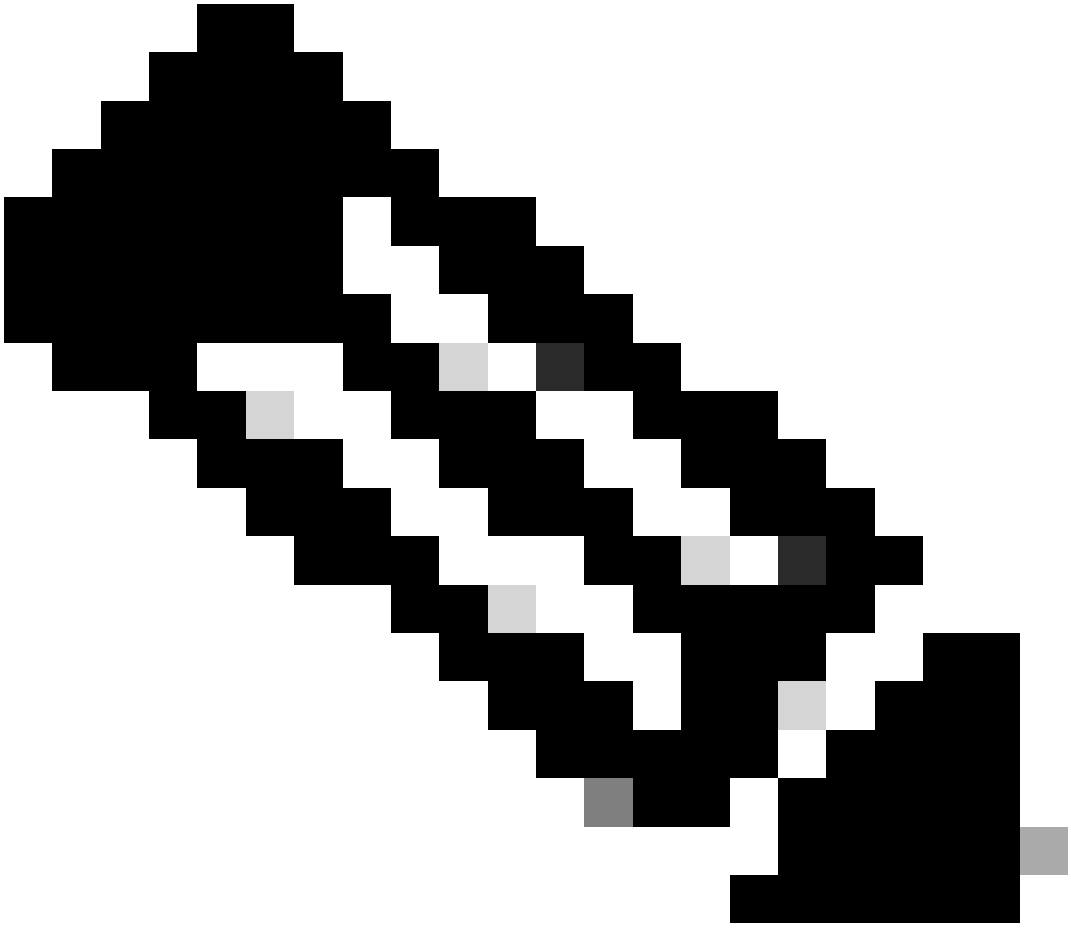


참고: 정책 프로필의 컨피그레이션은 VLAN을 제외하고 외부 컨트롤러와 앵커 컨트롤러 모두에서 일치해야 합니다.

3단계: Mobility(모빌리티) 탭 아래에서 Export Anchor(앵커 내보내기)를 선택합니다.


General
Access Policies
QOS and AVC
Mobility
Advanced
Mobility Anchors
Export Anchor
Static IP Mobility
DISABLED
Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.
Drag and Drop/double click/click on the arrow to add/remove Anchors
Available (2)
Selected (0)
Anchor IP
Anchor IP
Anc

내보내기 앵커



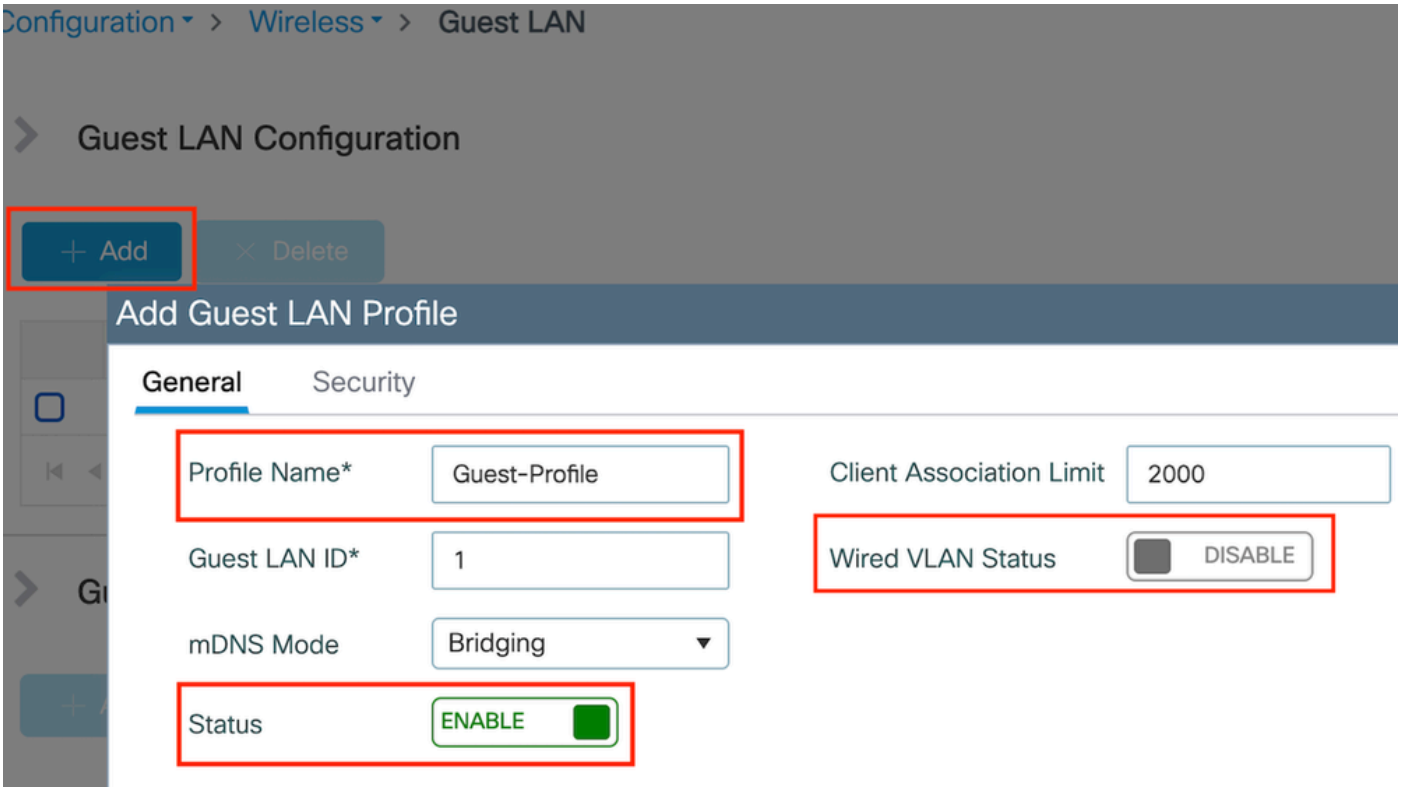
참고: 이 컨피그레이션은 9800 WLC(Wireless LAN Controller)를 지정된 정책 프로파일과 연결된 WLAN에 대한 앵커 WLC로 지정합니다. 외부 9800 WLC가 클라이언트를 앵커 WLC로 리디렉션하면 클라이언트에 할당된 WLAN 및 정책 프로필에 대한 세부 정보가 제공됩니다. 이렇게 하면 앵커 WLC가 수신된 정보를 기반으로 적절한 로컬 정책 프로필을 적용할 수 있습니다.

CLI 컨피그레이션

```
wireless profile policy GuestLANPolicy
 mobility anchor
 vlan VLAN2024
 no shutdown
```

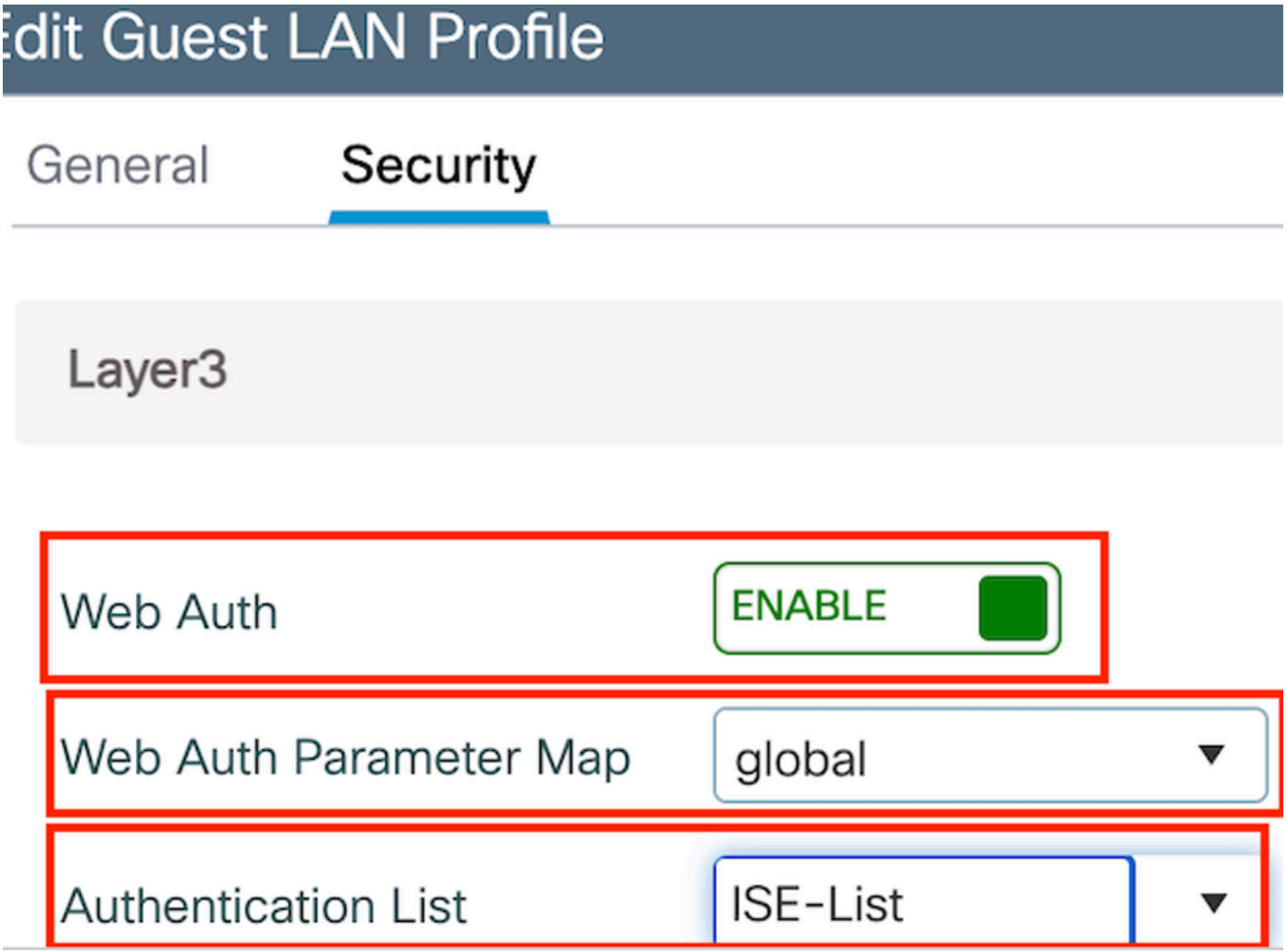
게스트 LAN 프로필 구성

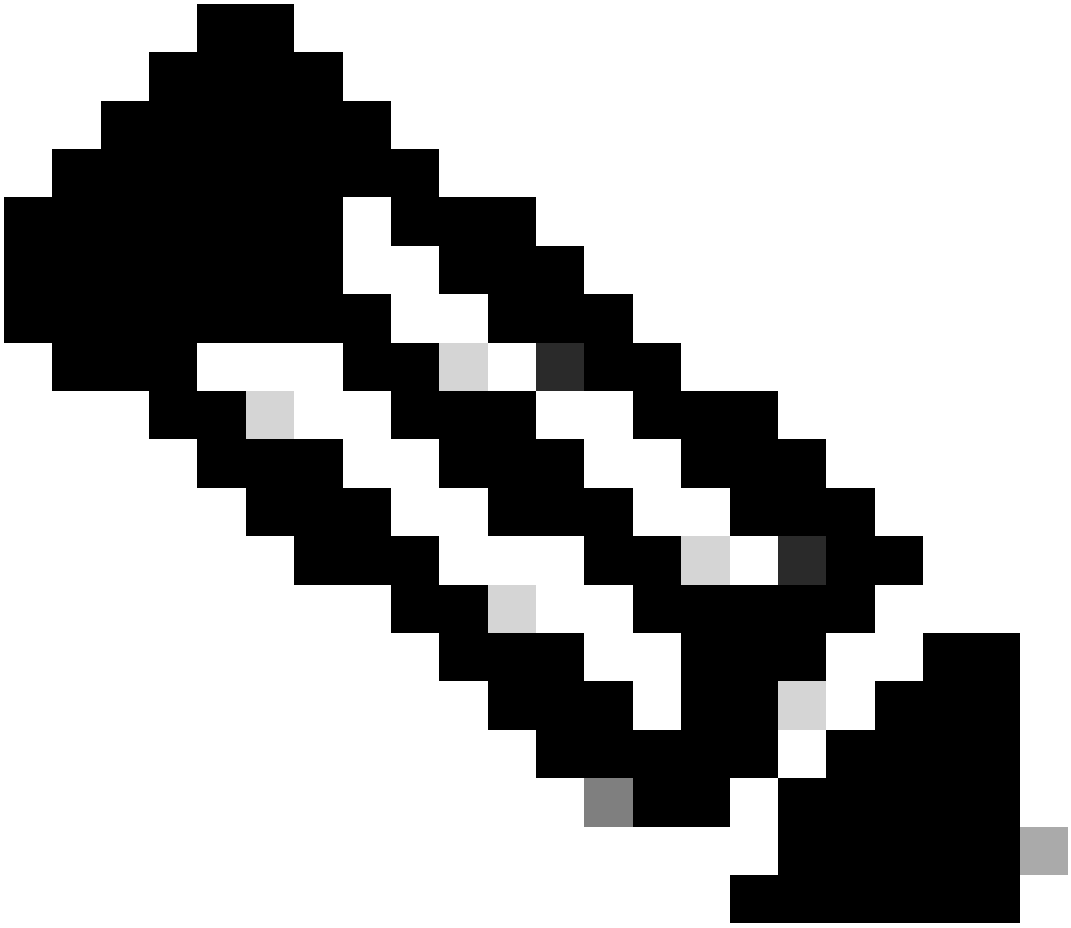
1단계: Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동한 다음 Add(추가)를 선택하여 게스트 LAN 프로필을 생성하고 구성합니다. 프로파일 이름이 외부 컨트롤러의 이름과 일치하는지 확인합니다. 앵커 컨트롤러에서 유선 VLAN을 비활성화해야 합니다.



게스트 LAN 프로필

2단계: 보안 설정에서 웹 인증을 활성화한 다음 웹 인증 매개변수 맵과 인증 목록을 구성합니다.


Edit Guest LAN Profile
General
Security
Layer3
Web Auth
ENABLE
Web Auth Parameter Map
global
Authentication List
ISE-List



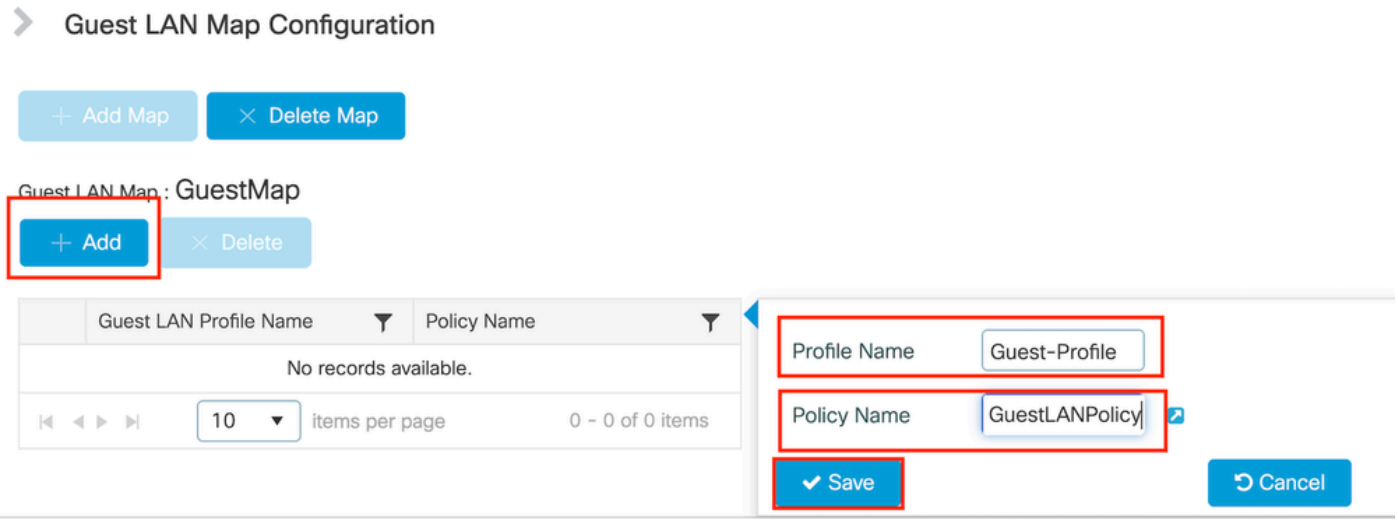
참고: 게스트 LAN 프로필 컨피그레이션은 유선 VLAN 상태를 제외하고 외부 컨트롤러와 앵커 컨트롤러 간에 동일해야 합니다

CLI 컨피그레이션

```
guest-lan profile-name Guest-Profile 1
 security web-auth authentication-list ISE-List
 security web-auth parameter-map global
```

게스트 LAN 맵

1단계: Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동합니다. Guest LAN MAP configuration(게스트 LAN 맵 컨피그레이션) 섹션에서 Add(추가)를 선택하고 Policy Profile(정책 프로파일)을 게스트 LAN 프로파일에 매핑합니다.



게스트 LAN 맵

```
wireless guest-lan map GuestMap
guest-lan Guest-Profile policy GuestLANPolicy
```

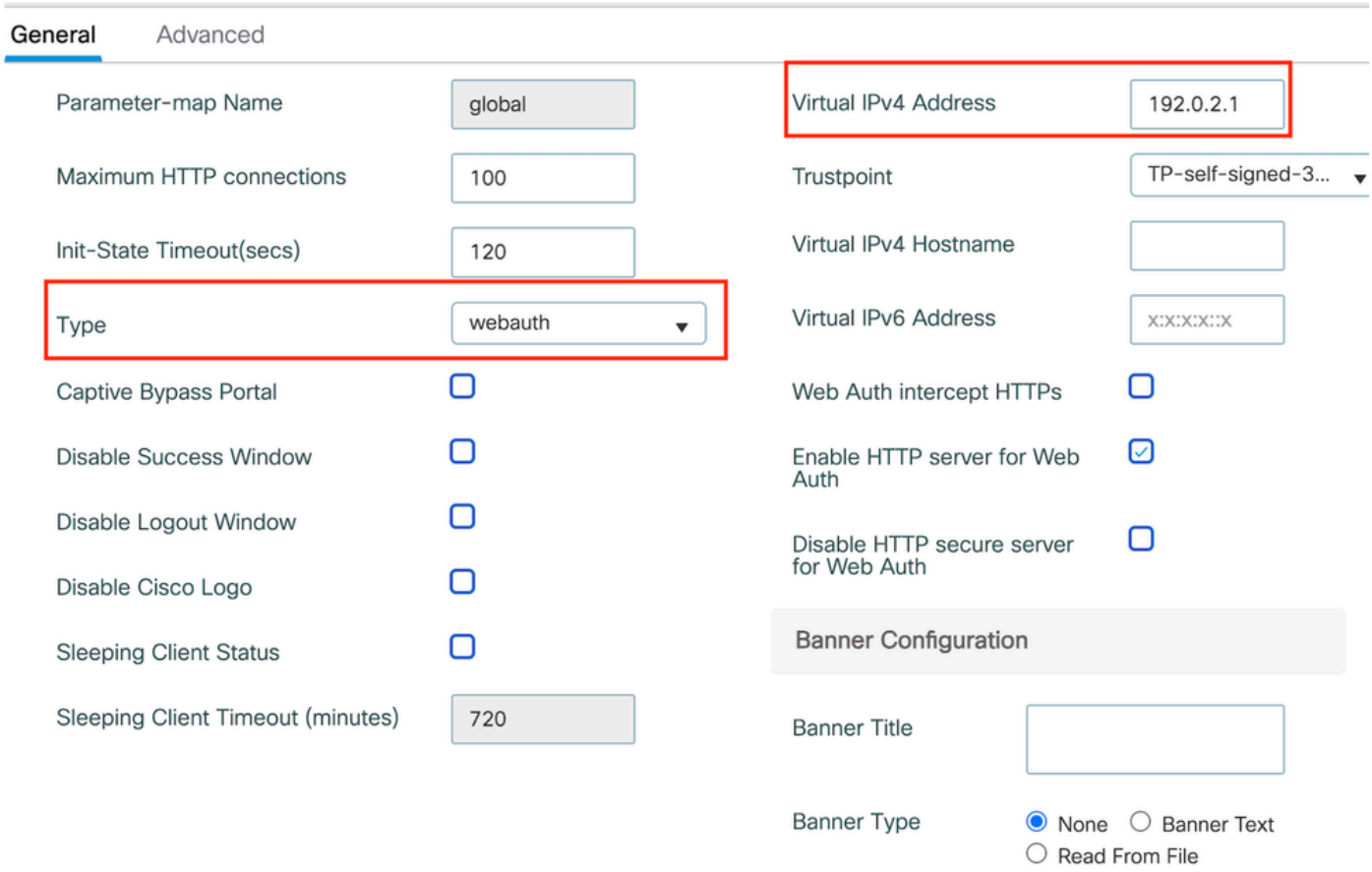
AireOS 5520 컨트롤러에 고정된 catalyst 9800에서 유선 게스트 구성

네트워크 토폴로지

외부 9800 WLC의 컨피그레이션

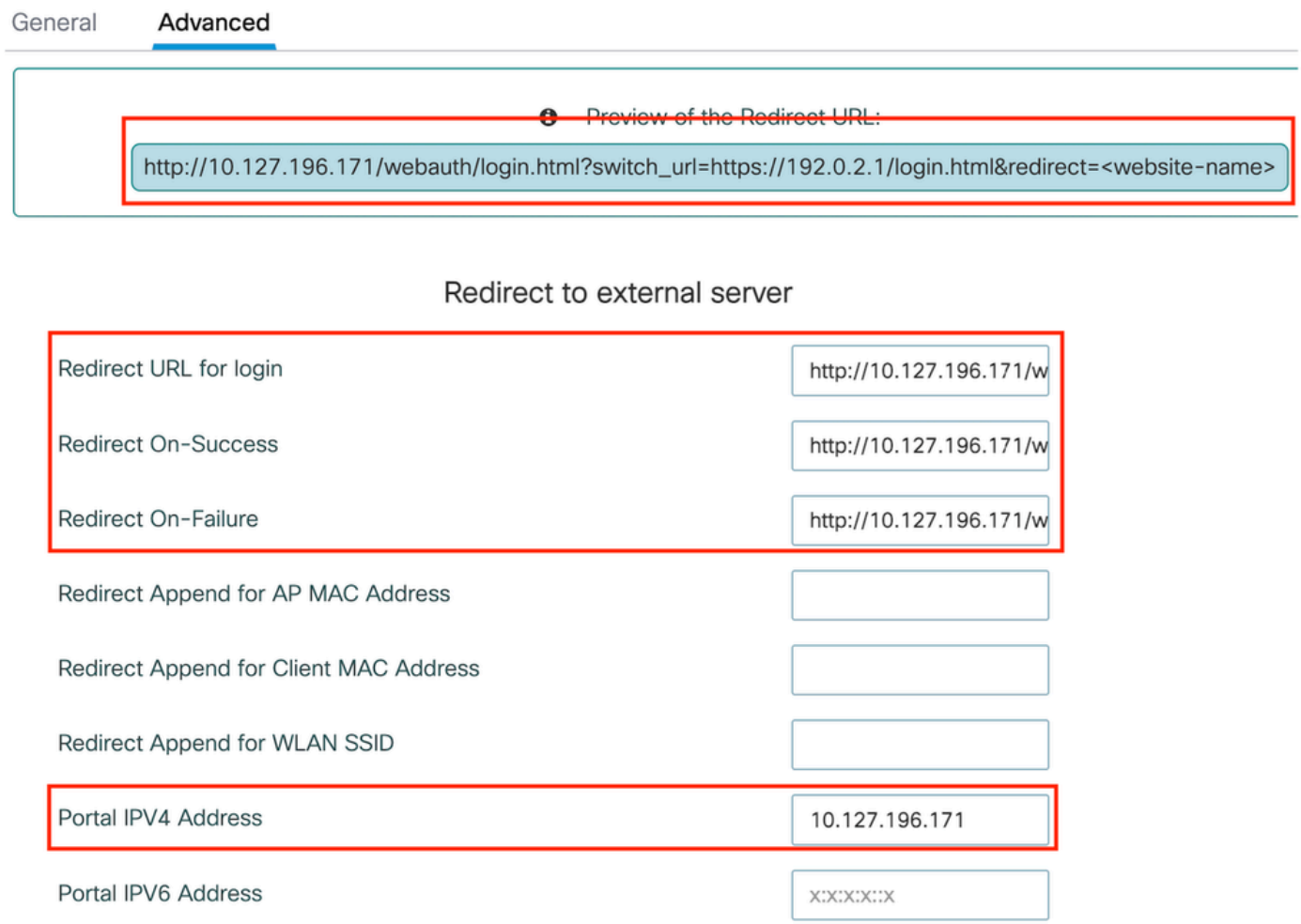
웹 매개 변수 맵 구성

1단계: Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고 Global(전역)을 선택합니다. 컨트롤러 및 신뢰 지점의 가상 IP 주소가 프로필에 올바르게 매핑되었는지, 유형이 webauth로 설정되어 있는지 확인합니다.



웹 매개 변수 맵

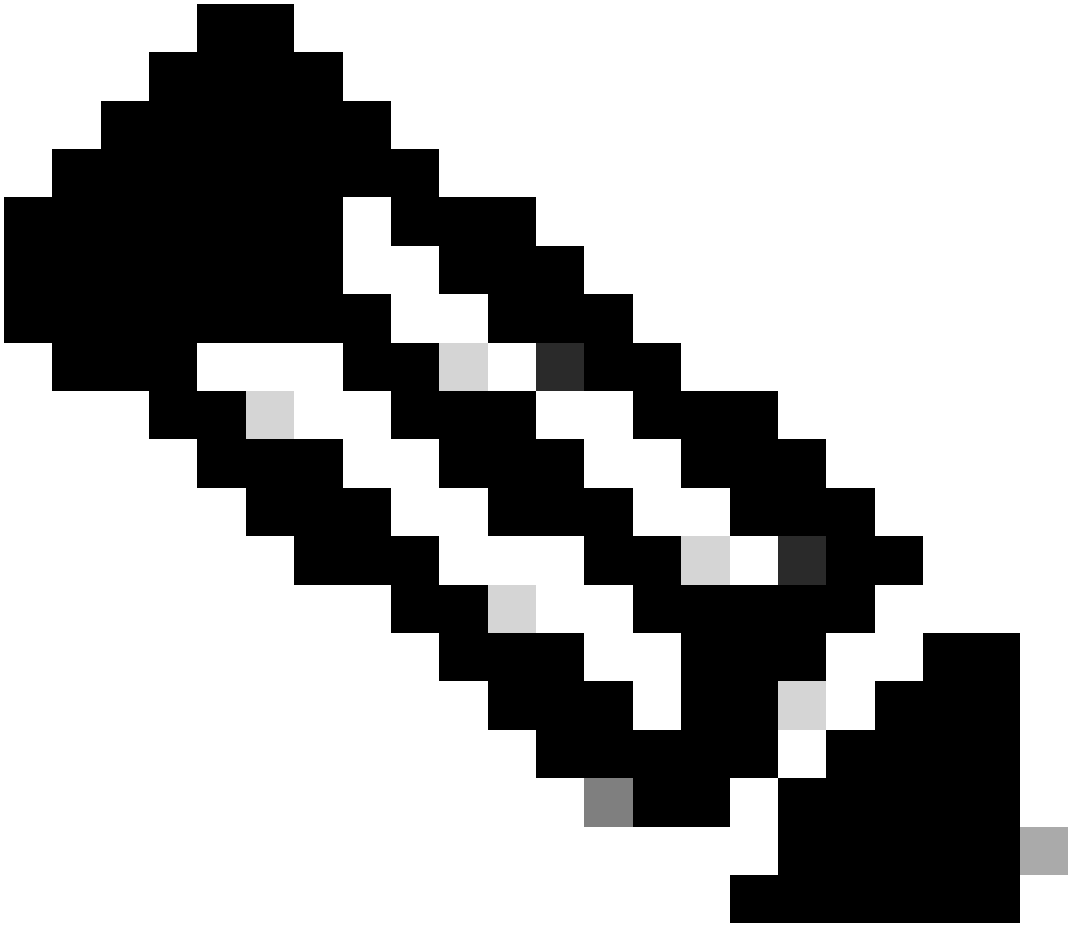
2단계: Advanced(고급) 탭에서 클라이언트를 리디렉션해야 하는 외부 웹 페이지 URL을 지정합니다. 로그인 및 실패 시 리디렉션을 위한 리디렉션 URL을 구성합니다. Redirect On-Success 설정은 선택적 컨피그레이션입니다.



고급 탭

CLI 컨피그레이션

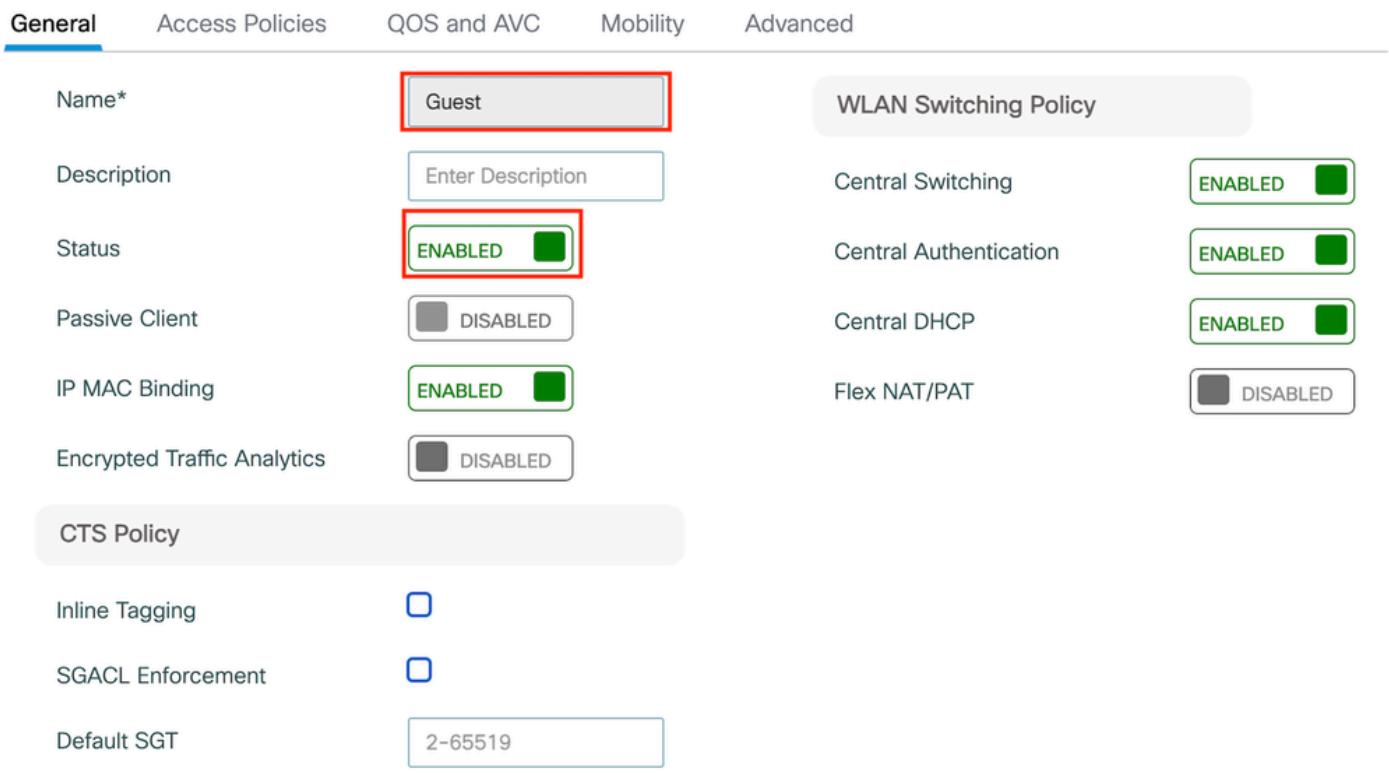
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 trustpoint TP-self-signed-3010594951
 webauth-http-enable
```



참고: AAA 컨피그레이션의 경우 Foreign 9800 WLC의 "" 섹션에 제공된 컨피그레이션 세부 사항을 참조하십시오.

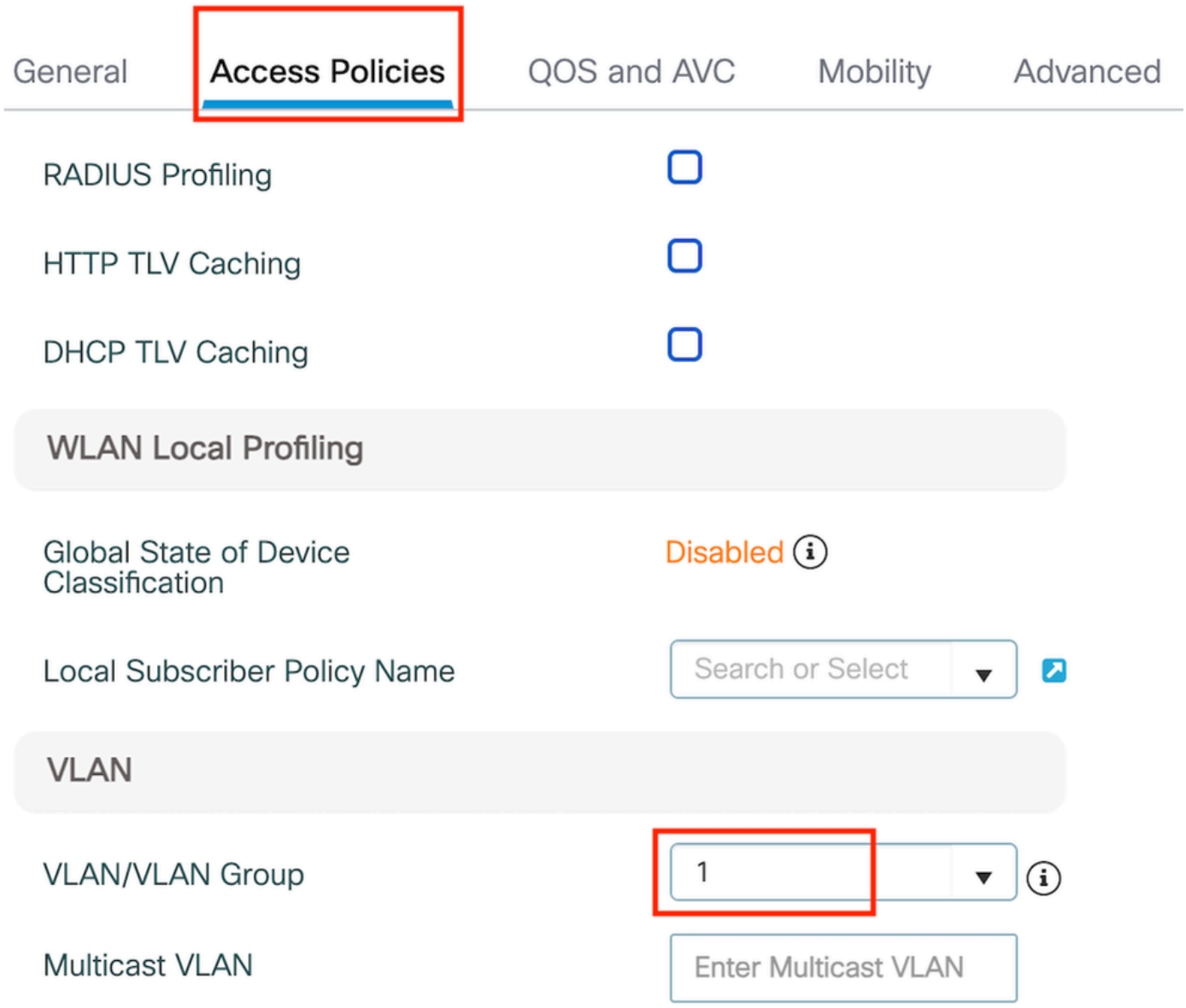
정책 프로필 구성

1단계: Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다. Add(추가)를 선택하고 General(일반) 탭에서 프로파일의 이름을 입력하고 상태 토글을 활성화합니다.



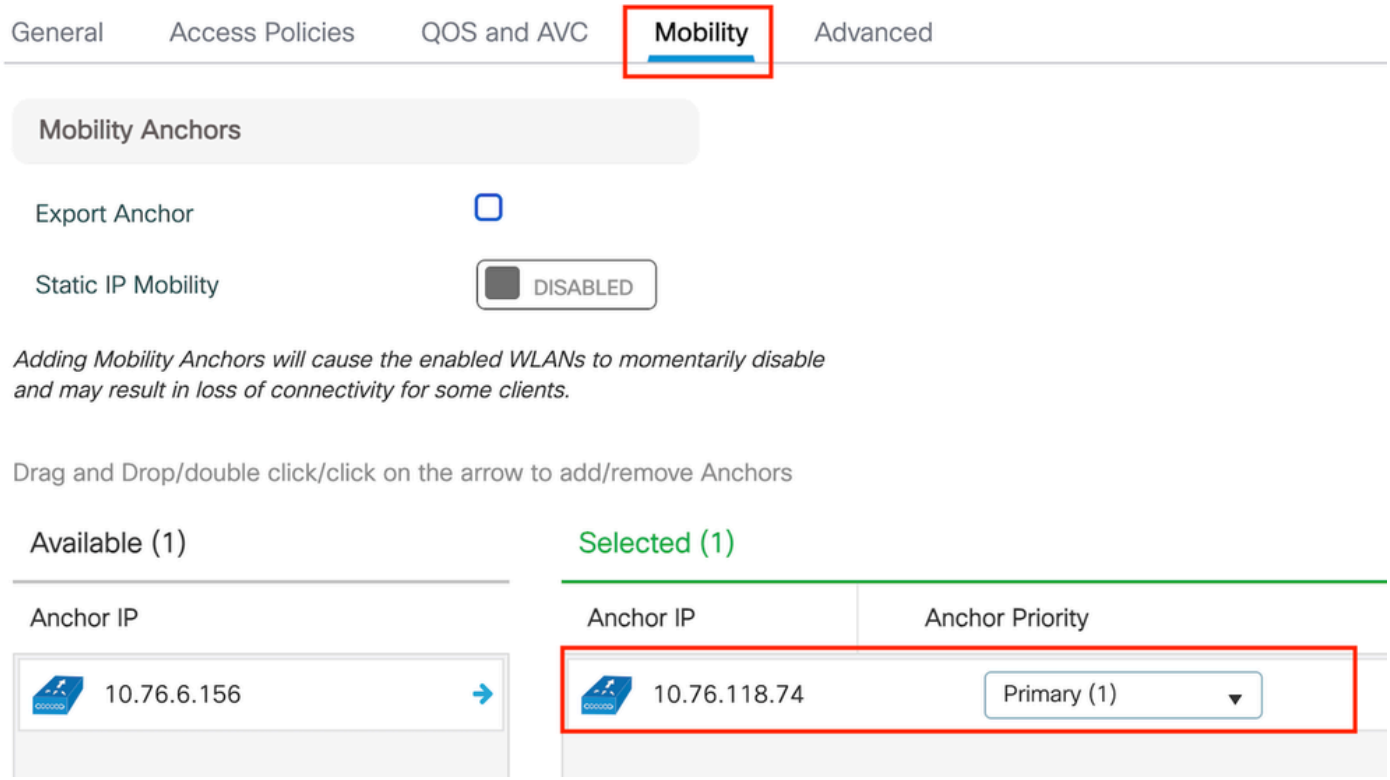
정책 프로파일

2단계: Access Policies(액세스 정책) 탭에서 임의의 VLAN을 할당합니다.

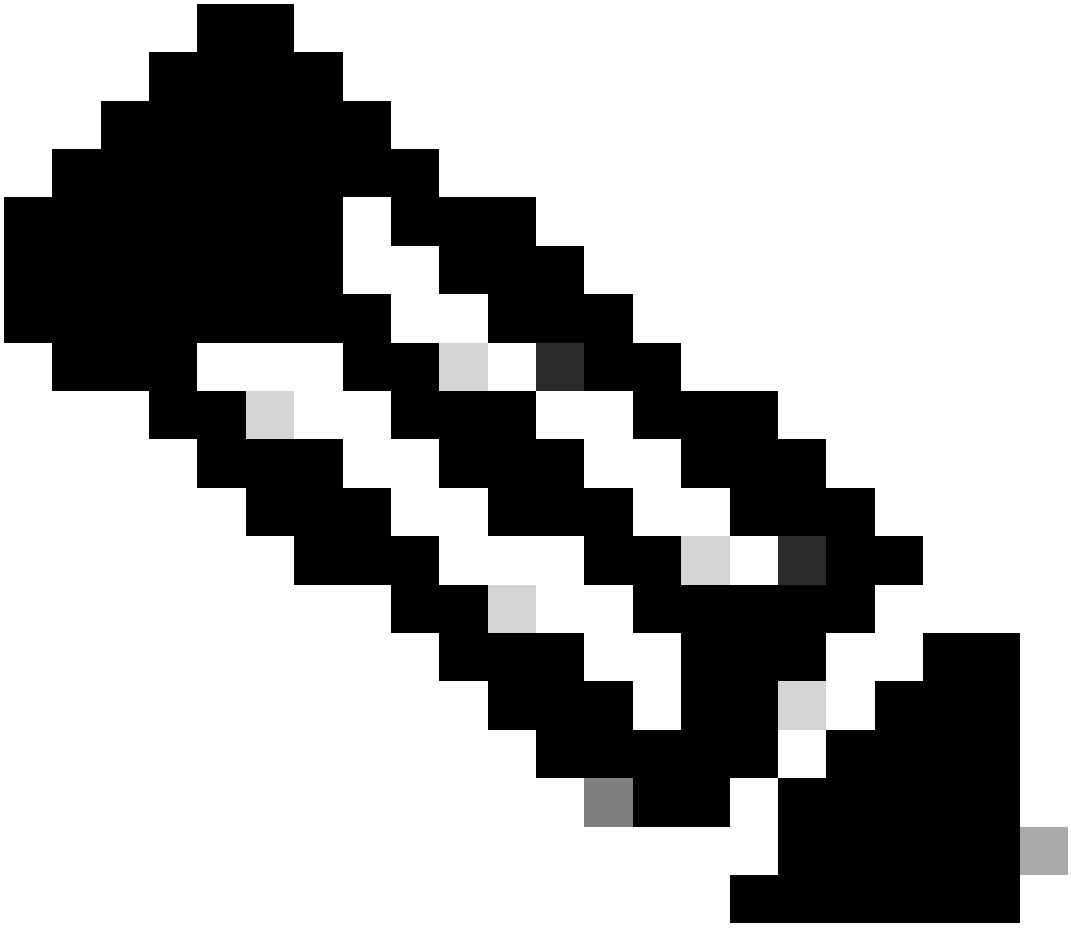


액세스 정책

3단계: Mobility(모빌리티) 탭에서 Anchor(앵커) 컨트롤러를 토글하고 우선순위를 Primary(1)로 설정합니다


General
Access Policies
QOS and AVC
Mobility
Advanced
Mobility Anchors
Export Anchor
Static IP Mobility
DISABLED
Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.
Drag and Drop/double click/click on the arrow to add/remove Anchors
Available (1)
Anchor IP
10.76.6.156
Selected (1)
Anchor IP
Anchor Priority
10.76.118.74
Primary (1)

모빌리티 탭



참고: 9800 외부 WLC의 정책 프로필은 vlan 컨피그레이션을 제외하고 5520 앵커 WLC의 게스트 LAN 프로필과 일치해야 합니다

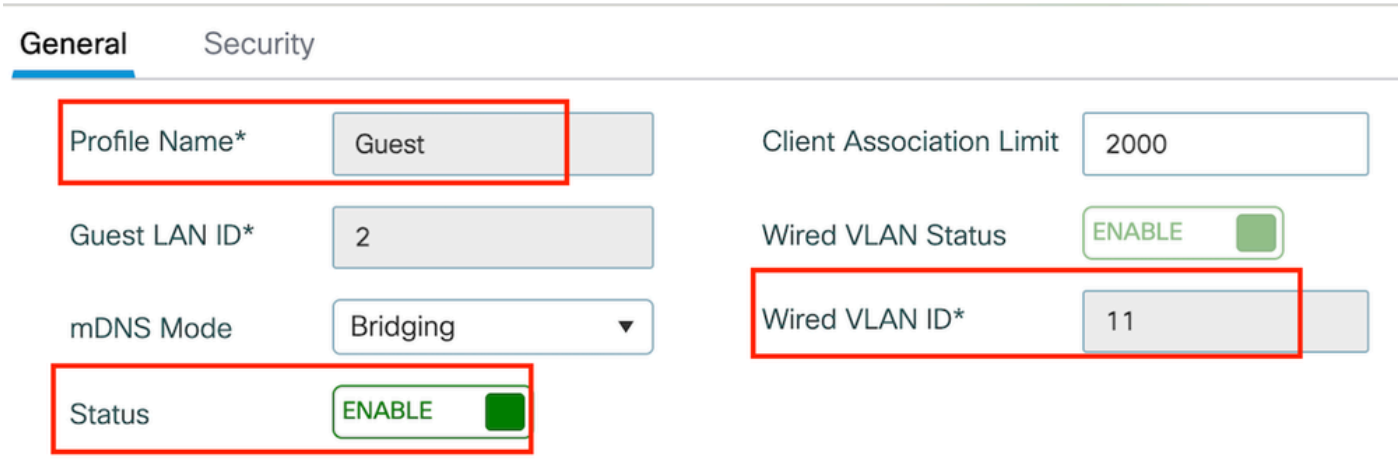
CLI 컨피그레이션

```
wireless profile policy Guest
 no accounting-interim
 exclusionlist timeout 180
 no flex umbrella dhcp-dns-option
 mobility anchor 10.76.118.74 priority 1
 no shutdown
```

게스트 LAN 프로필 구성

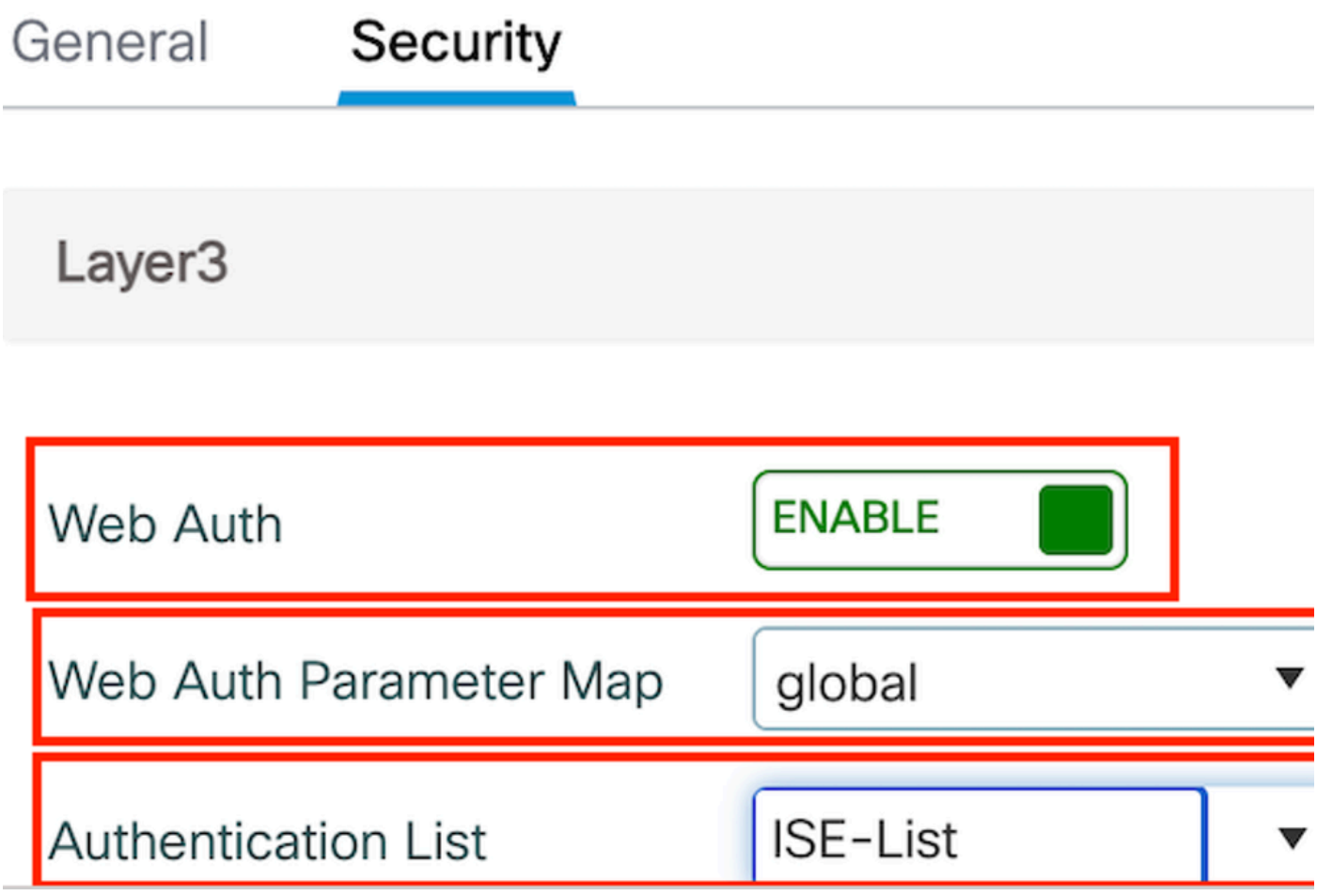
1단계: Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동하고

Add(추가)를 선택합니다. 고유한 프로파일 이름을 구성하고 유선 VLAN을 활성화하며, 유선 게스트 사용자 전용 VLAN ID를 지정합니다. 마지막으로 프로파일 상태를 Enabled(활성화됨)로 전환합니다.

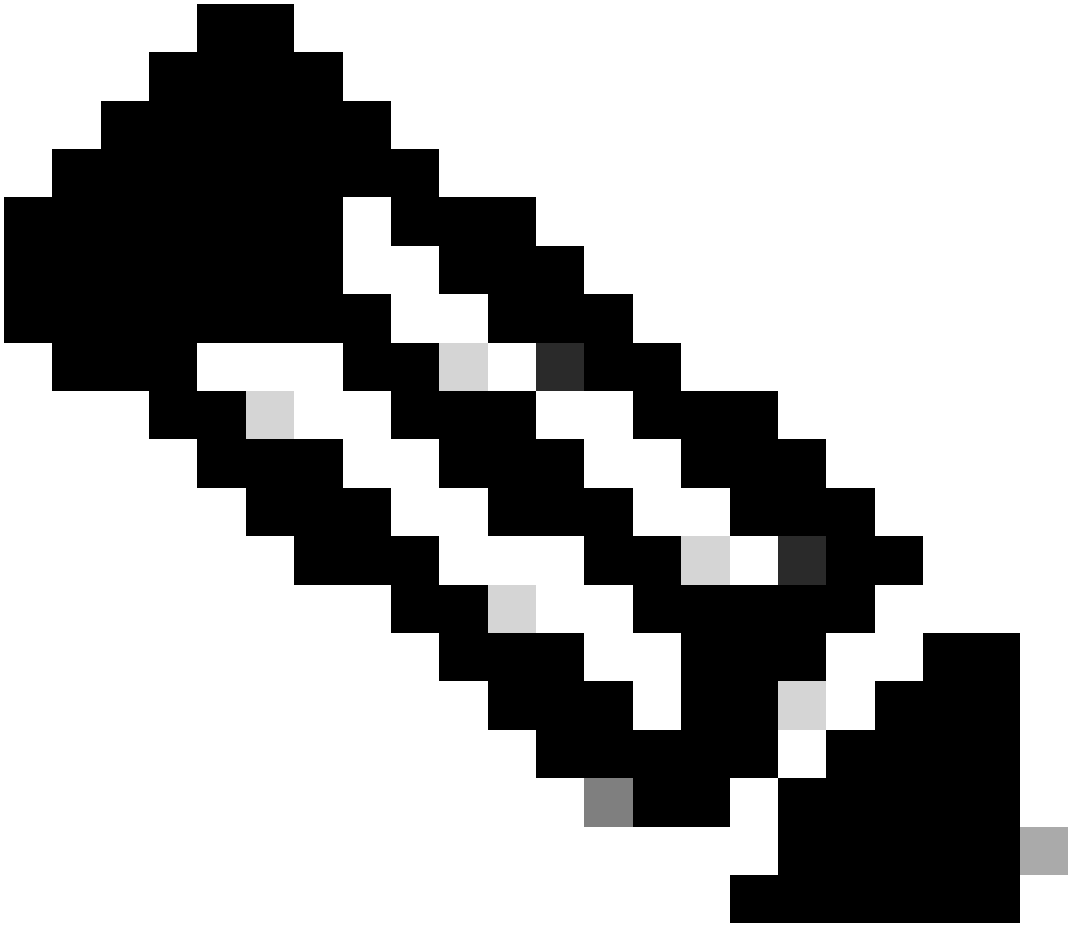


게스트 LAN 정책

2단계: Security(보안) 탭 아래에서 Web Auth(웹 인증)를 활성화하고 Web Auth 매개변수 맵을 매핑한 다음 Authentication(인증) 드롭다운 목록에서 RADIUS 서버를 선택합니다.



보안 탭



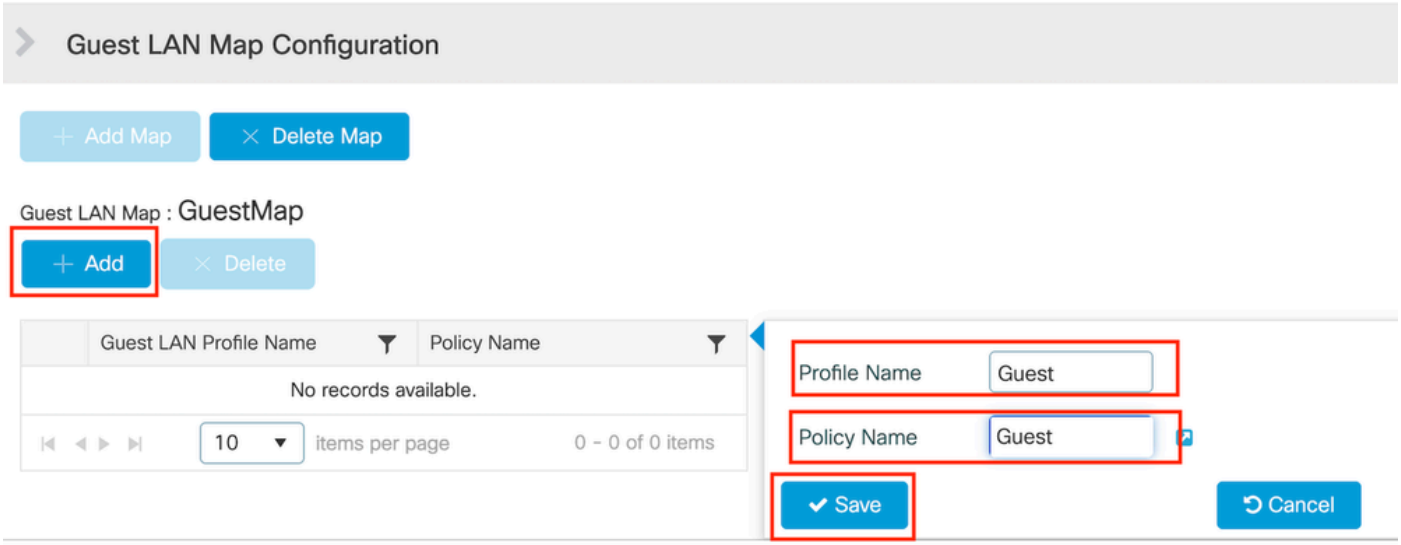
참고: 9800 Foreign 및 5520 Anchor 컨트롤러의 게스트 LAN 프로필 이름은 동일해야 합니다

CLI 컨피그레이션

```
guest-lan profile-name Guest 2 wired-vlan 11
 security web-auth authentication-list ISE-List
 security web-auth parameter-map global
```

게스트 LAN 맵

1단계: Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동합니다. Guest LAN MAP 컨피그레이션 섹션에서 Add(추가)를 선택하고 Policy Profile(정책 프로필)을 Guest LAN 프로필에 매핑합니다.



게스트 LAN 맵

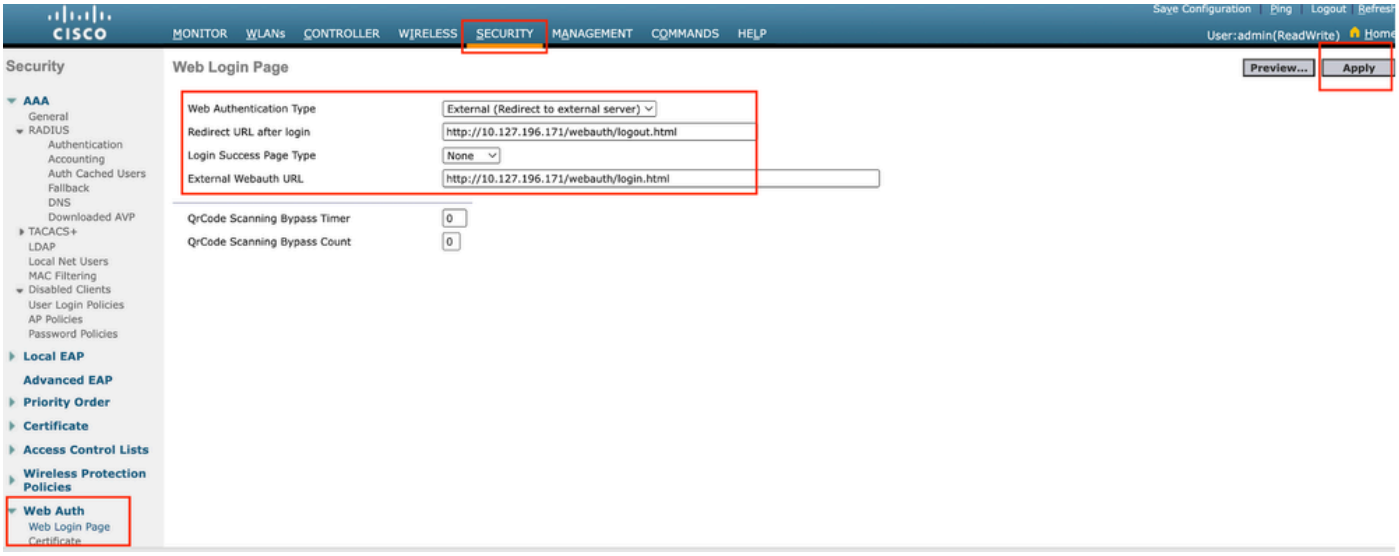
CLI 컨피그레이션

```
wireless guest-lan map GuestMap
 guest-lan Guest policy Guest
```

앵커 5520 WLC의 컨피그레이션

웹 인증 구성

1단계: Security(보안) > Web Auth(웹 인증) > Web Login Page(웹 로그인 페이지)로 이동합니다. 웹 인증 유형을 외부(외부 서버로 리디렉션)로 설정하고 외부 웹 인증 URL을 구성합니다. 로그인 후 리디렉션 URL은 선택 사항이며 인증에 성공한 후 클라이언트를 전용 페이지로 리디렉션해야 하는 경우 구성할 수 있습니다.

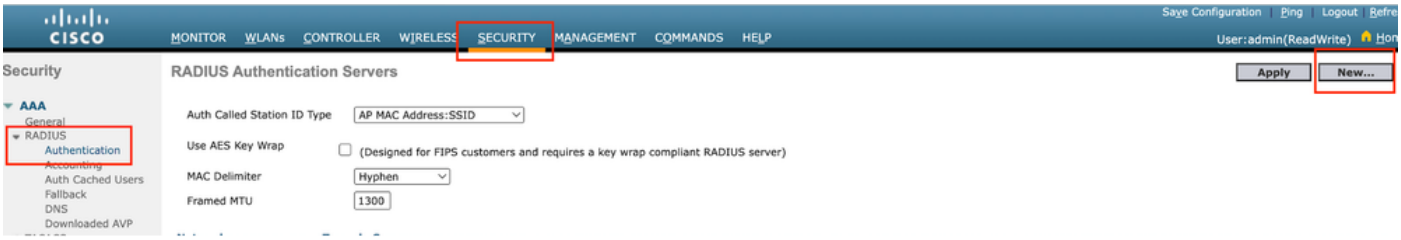


웹 인증 설정

AAA 설정:

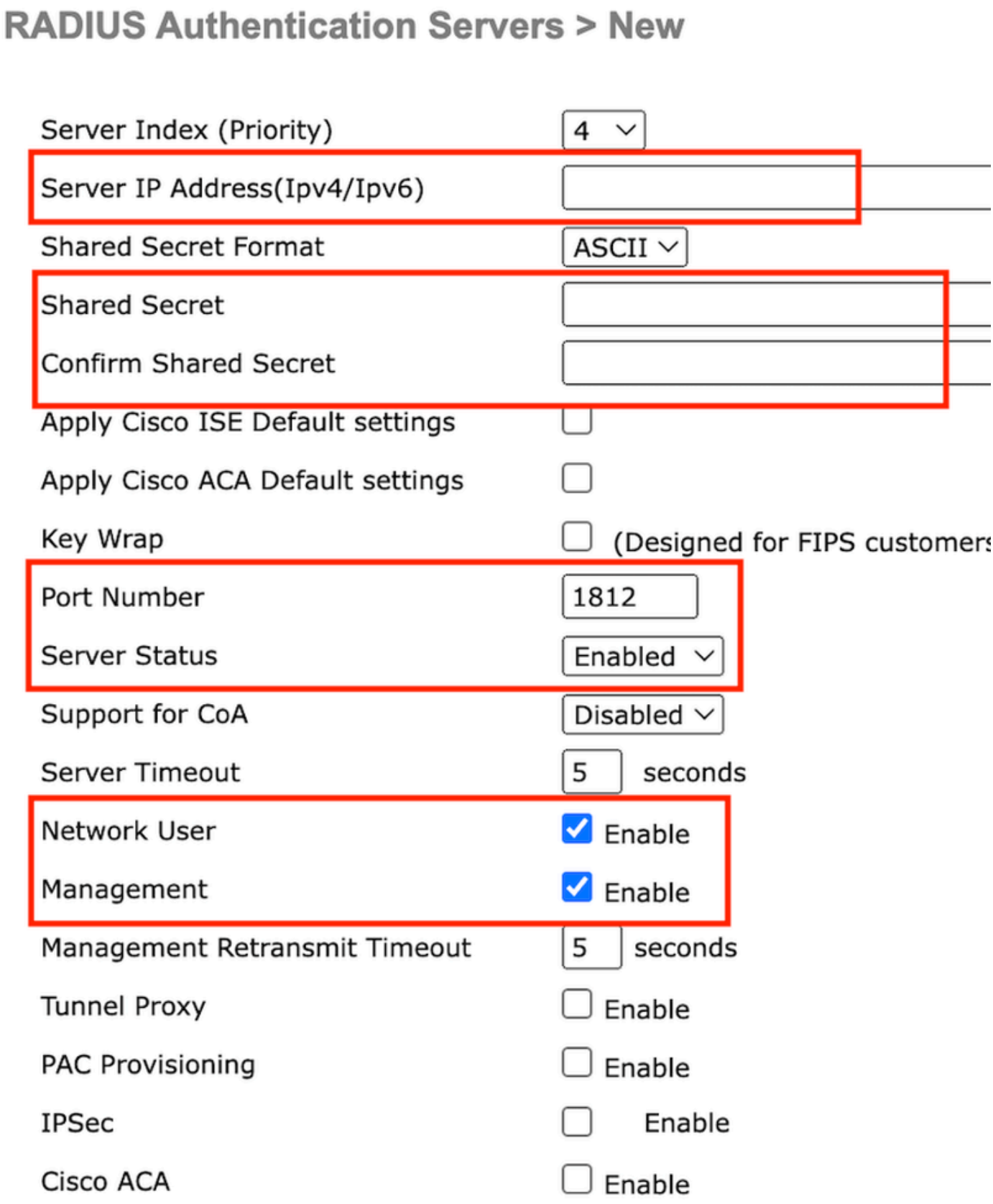
1단계: radius 서버 구성

Security(보안) > Radius > Authentication(인증) > New(새로 만들기)로 이동합니다.



Radius 서버

2단계: 컨트롤러에서 RADIUS 서버 IP 및 공유 암호를 구성합니다. 서버 상태를 Enabled(활성화됨)로 전환하고 Network User(네트워크 사용자) 확인란을 선택합니다.

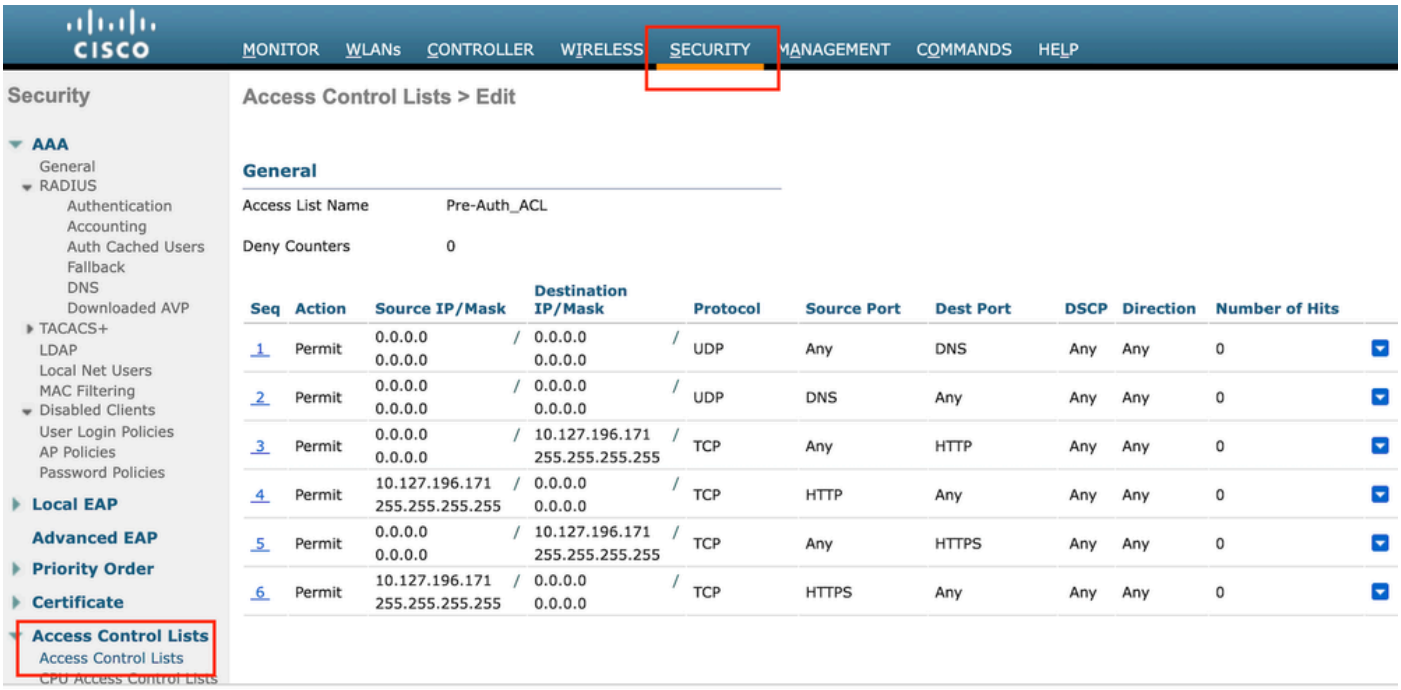


서버 컨피그레이션

액세스 제어 목록 구성

1단계: Security(보안) > Access Control List(액세스 제어 목록)로 이동하고 New(새로 만들기)를 선

택합니다. DNS 및 외부 웹 서버에 대한 트래픽을 허용하는 사전 인증 ACL을 생성합니다.



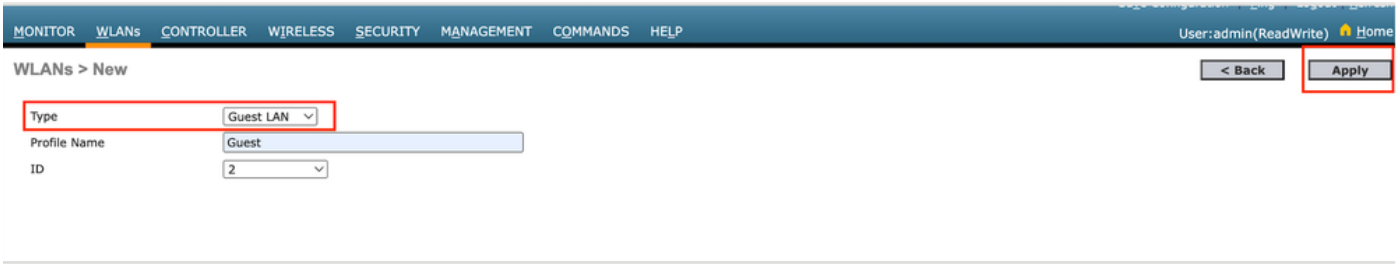
웹 서버에 대한 트래픽을 허용하는 액세스 목록

게스트 LAN 프로필 구성

1단계: WLANs(WLAN)로 이동하고 Create New(새로 만들기)를 선택합니다.

Type as Guest LAN(게스트 LAN으로 유형)을 선택하고 9800 Foreign Controller의 정책 프로파일과 동일한 이름을 구성합니다.

게스트 LAN 생성



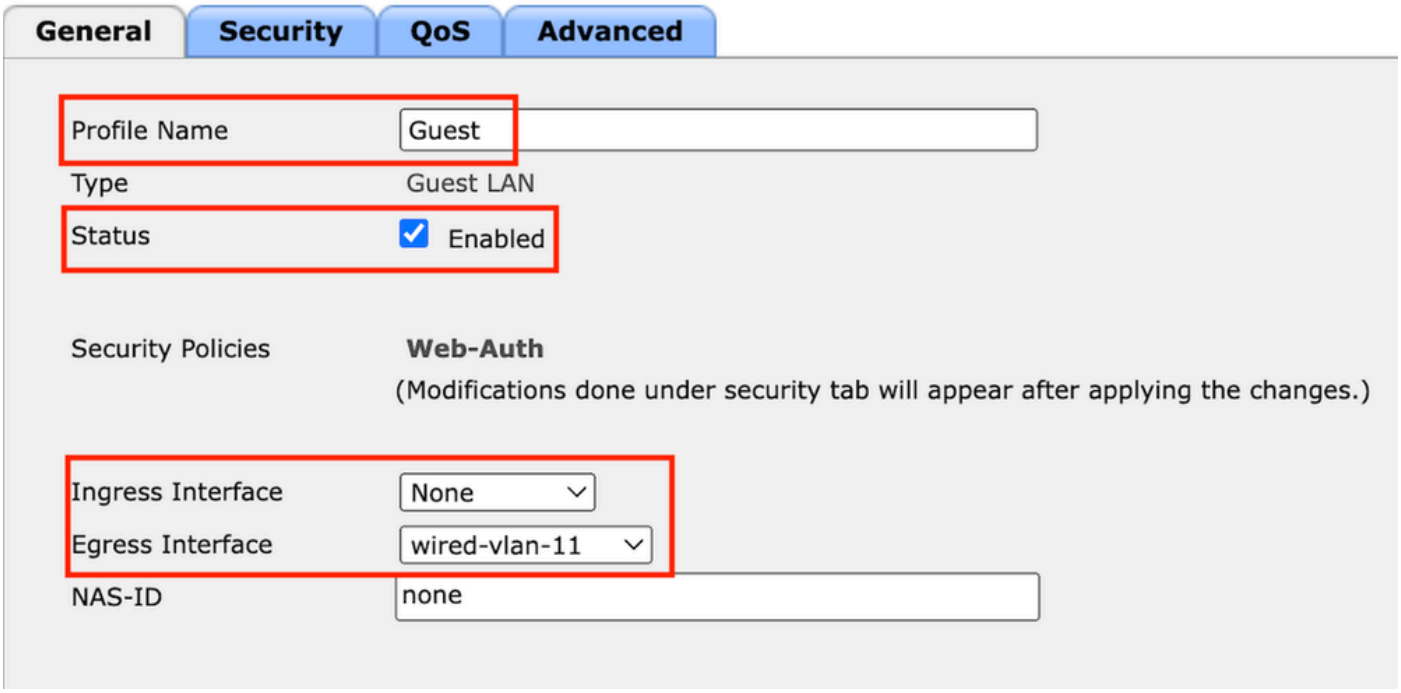
게스트 LAN 프로필

2단계: 게스트 LAN 프로필에 인그레스 및 이그레스 인터페이스를 매핑합니다.

이 경우 인그레스 인터페이스는 외부 컨트롤러의 EoIP 터널이므로 인그레스 인터페이스가 없습니

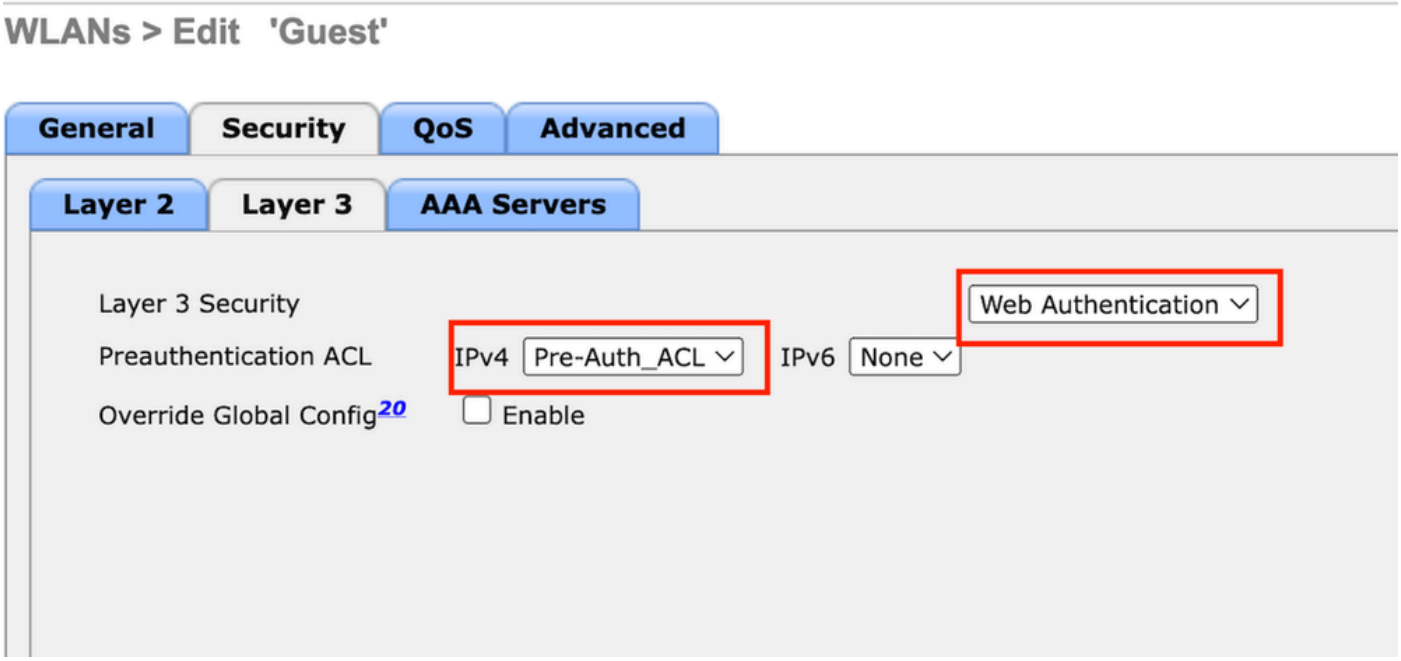
다.

이그레스 인터페이스는 유선 클라이언트가 물리적으로 연결하는 VLAN입니다.



게스트 LAN 프로필

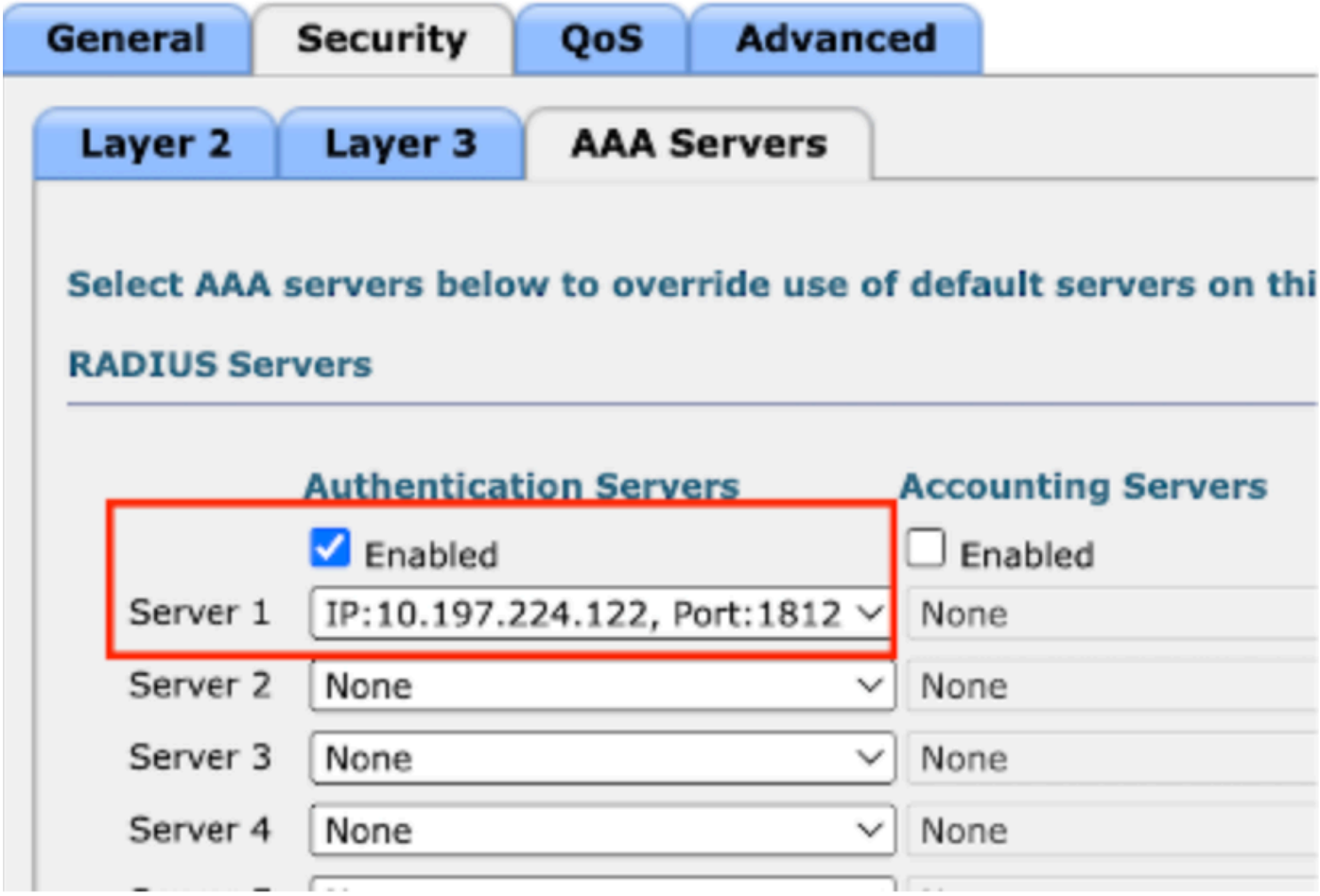
3단계: Security(보안) 탭에서 Layer 3 security as Web Authentication(웹 인증)을 선택하고 사전 인증 ACL을 매핑합니다.



Guest LAN security(게스트 LAN 보안) 탭

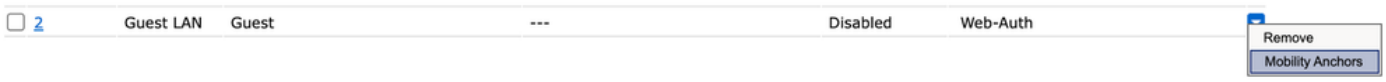
4단계: Security(보안) > AAA Server(AAA 서버)로 이동합니다.

드롭다운을 선택하고 게스트 LAN 프로필에 RADIUS 서버를 매핑합니다.



게스트 LAN 프로필에 RADIUS 서버 매핑

5단계: WLAN으로 이동합니다. 게스트 LAN 프로필의 드롭다운 아이콘 위에 마우스 커서를 올려 놓고 Mobility Anchors를 선택합니다.



6단계: Mobility Anchor Create(모빌리티 앵커 생성)를 선택하여 컨트롤러를 이 게스트 LAN 프로파일의 내보내기 앵커로 구성합니다.

모빌리티 앵커 만들기

Catalyst 9800에 고정된 AireOS 5520에서 유선 게스트 구성

네트워크 토폴로지

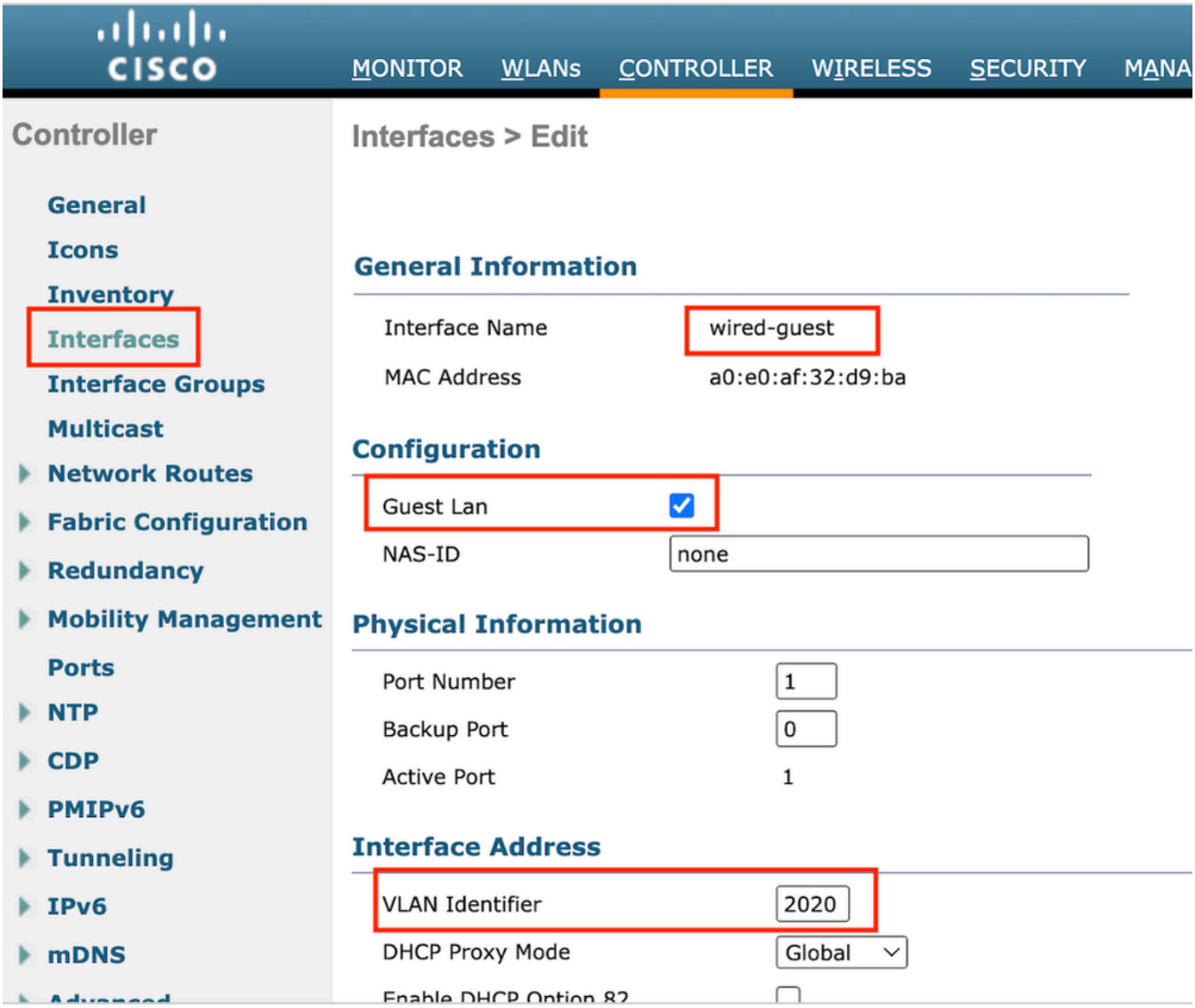
외부 5520 WLC의 컨피그레이션

컨트롤러 인터페이스 컨피그레이션

1단계: Controller(컨트롤러) > Interfaces(인터페이스) > New(새로 만들기)로 이동합니다. 인터페이스 이름, VLAN ID를 구성하고 게스트 LAN을 활성화합니다.

유선 게스트에는 2개의 동적 인터페이스가 필요합니다.

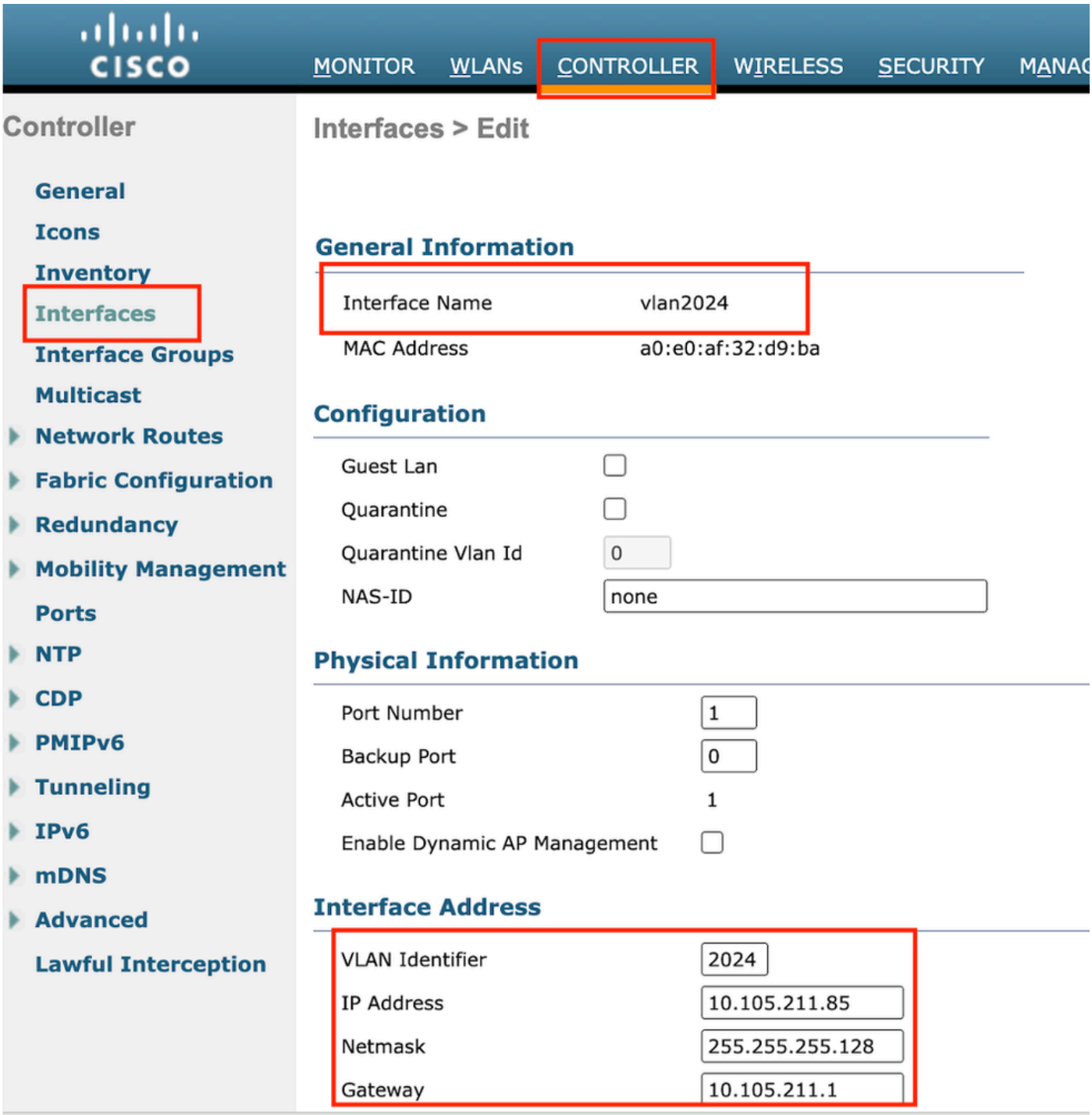
먼저 레이어 2 동적 인터페이스를 생성하고 이를 게스트 LAN으로 지정합니다. 이 인터페이스는 유선 클라이언트가 물리적으로 연결되는 게스트 LAN의 인그레스 인터페이스 역할을 합니다.



인그레스 인터페이스

2단계: Controller(컨트롤러) > Interfaces(인터페이스) > New(새로 만들기)로 이동합니다. 인터페이스 이름, VLAN ID를 구성합니다.

두 번째 동적 인터페이스는 컨트롤러의 레이어 3 인터페이스여야 하며 유선 클라이언트는 이 VLAN 서브넷에서 IP 주소를 수신합니다. 이 인터페이스는 게스트 LAN 프로파일에 대한 이그레스 인터페이스 역할을 합니다.



이그레스 인터페이스

스위치 포트 컨피그레이션

유선 게스트 사용자는 액세스 레이어 스위치에 연결, 이러한 지정 된 포트는 컨트롤러에서 게스트 LAN 이 활성화 된 VLAN으로 구성 되어야 합니다

액세스 레이어 스위치 포트 컨피그레이션

인터페이스 기가비트 이더넷 <x/x/x>

설명 유선 게스트 액세스

switchport access vlan 2020

스위치포트 모드 액세스

끝

외부 컨트롤러 업링크 포트 컨피그레이션

인터페이스 TenGigabitEthernet<x/x/x>

설명 외부 WLC에 대한 트렁크 포트

switchport 모드 트렁크

switchport trunk 네이티브 vlan 2081

switchport trunk 허용 vlan 2081,2020

끝

앵커 컨트롤러 업링크 포트 컨피그레이션

인터페이스 TenGigabitEthernet<x/x/x>

설명 앵커 WLC에 대한 트렁크 포트

switchport 모드 트렁크

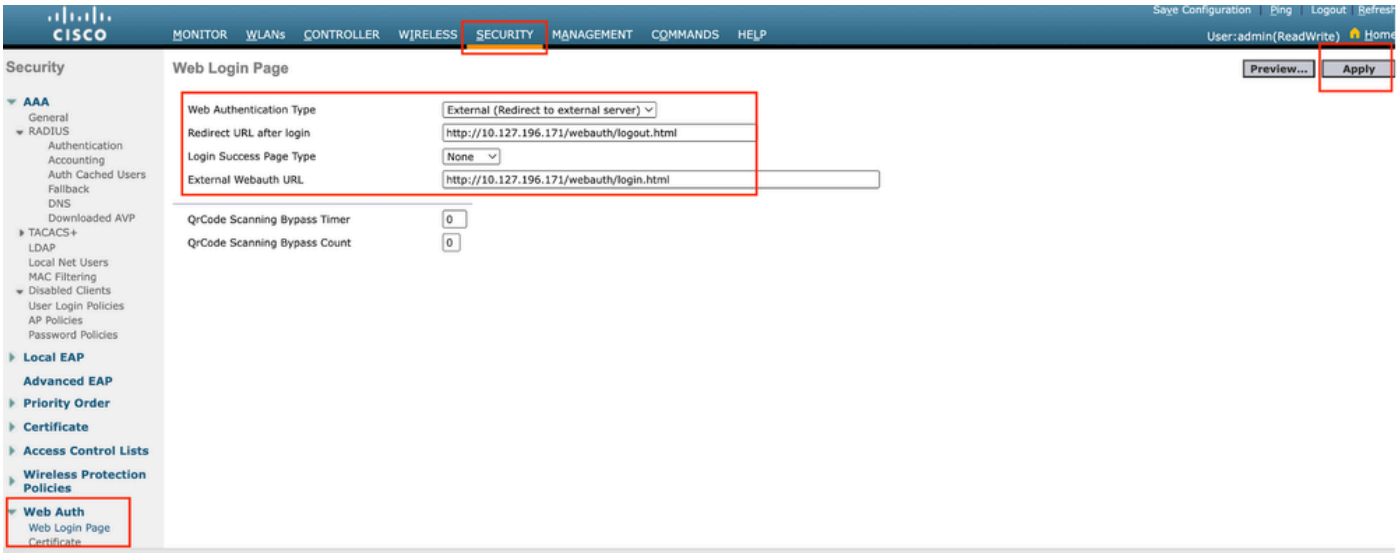
switchport trunk 네이티브 vlan 2081

switchport trunk allowed vlan 2081,2024

끝

웹 인증 구성

1단계: Security(보안) > Web Auth(웹 인증) > Web Login Page(웹 로그인 페이지)로 이동합니다. 웹 인증 유형을 외부(외부 서버로 리디렉션)로 설정하고 외부 웹 인증 URL을 구성합니다. 로그인 후 리디렉션 URL은 선택 사항이며 인증에 성공한 후 클라이언트를 전용 페이지로 리디렉션해야 하는 경우 구성할 수 있습니다.

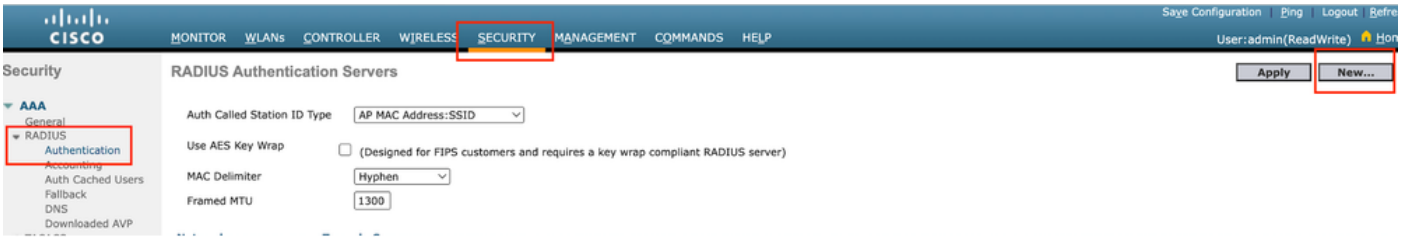


웹 인증 설정

AAA 설정:

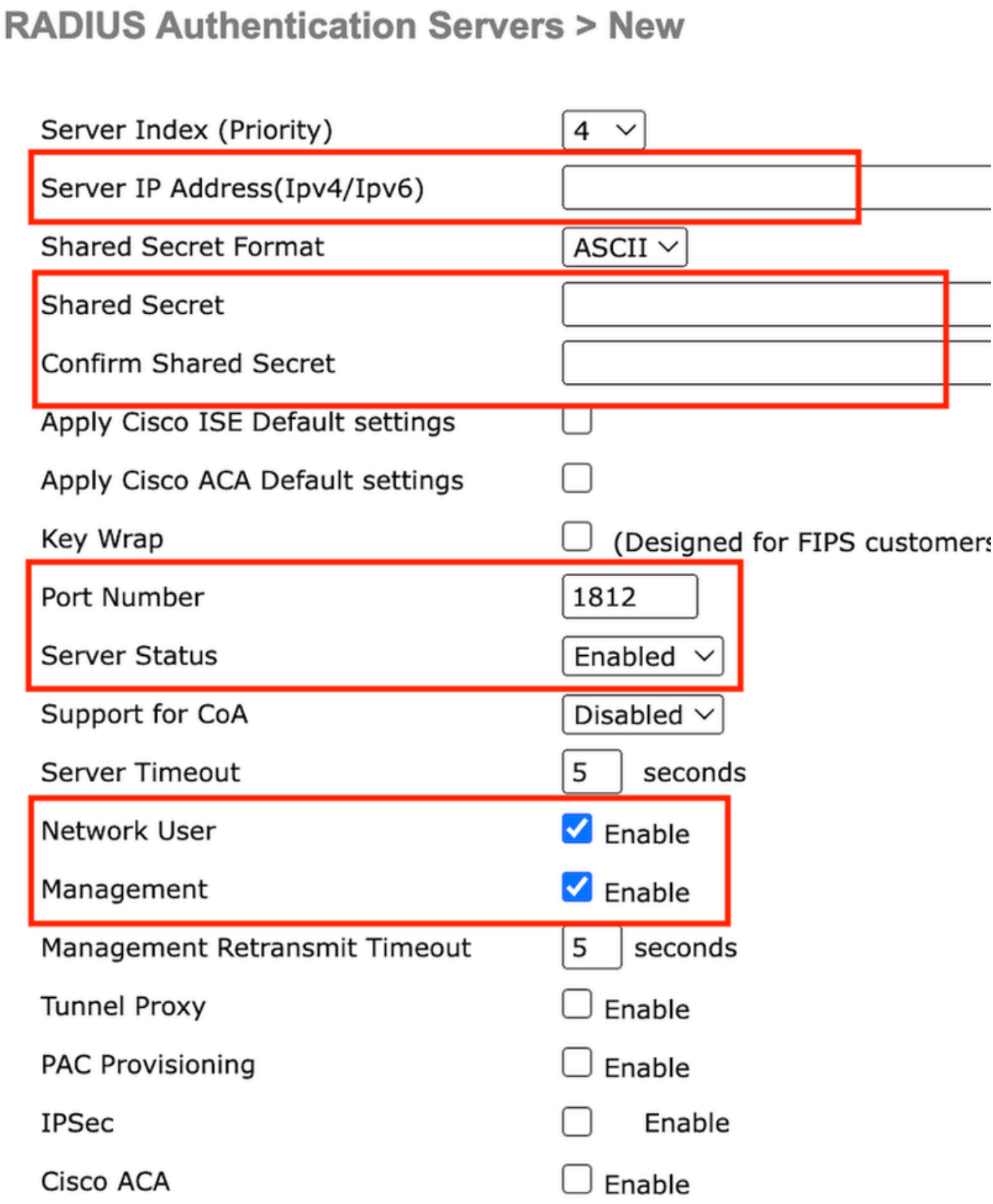
1단계: radius 서버 구성

Security(보안) > Radius > Authentication(인증) > New(새로 만들기)로 이동합니다.



Radius 서버

2단계: 컨트롤러에서 RADIUS 서버 IP 및 공유 암호를 구성합니다. 서버 상태를 Enabled(활성화됨)로 전환하고 Network User(네트워크 사용자) 확인란을 선택합니다.

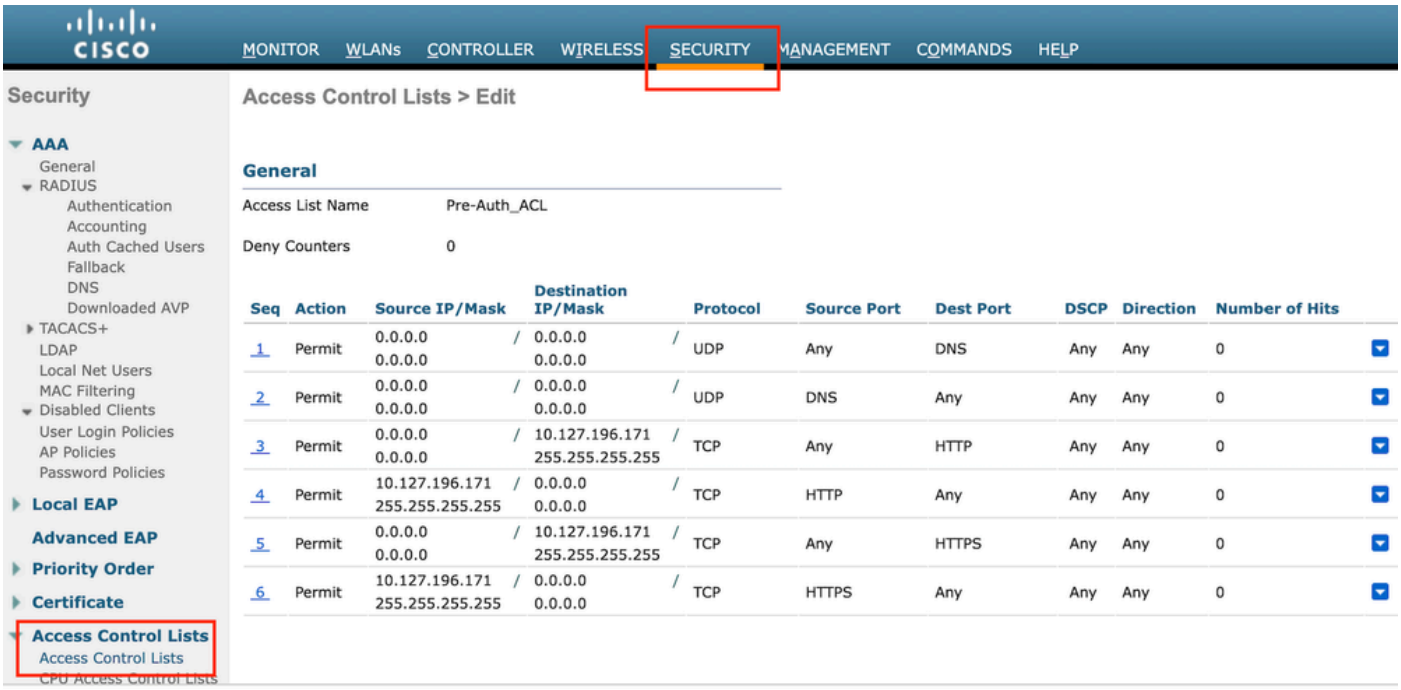


서버 컨피그레이션

액세스 제어 목록 구성

1단계: Security(보안) > Access Control List(액세스 제어 목록)로 이동하고 New(새로 만들기)를 선

택합니다. DNS 및 외부 웹 서버에 대한 트래픽을 허용하는 사전 인증 ACL을 생성합니다.



웹 서버에 대한 트래픽을 허용하는 액세스 목록

게스트 LAN 프로필 구성

1단계: WLAN(WLAN) > Create New(새로 만들기) > Go(이동)로 이동합니다.

게스트 LAN 프로필

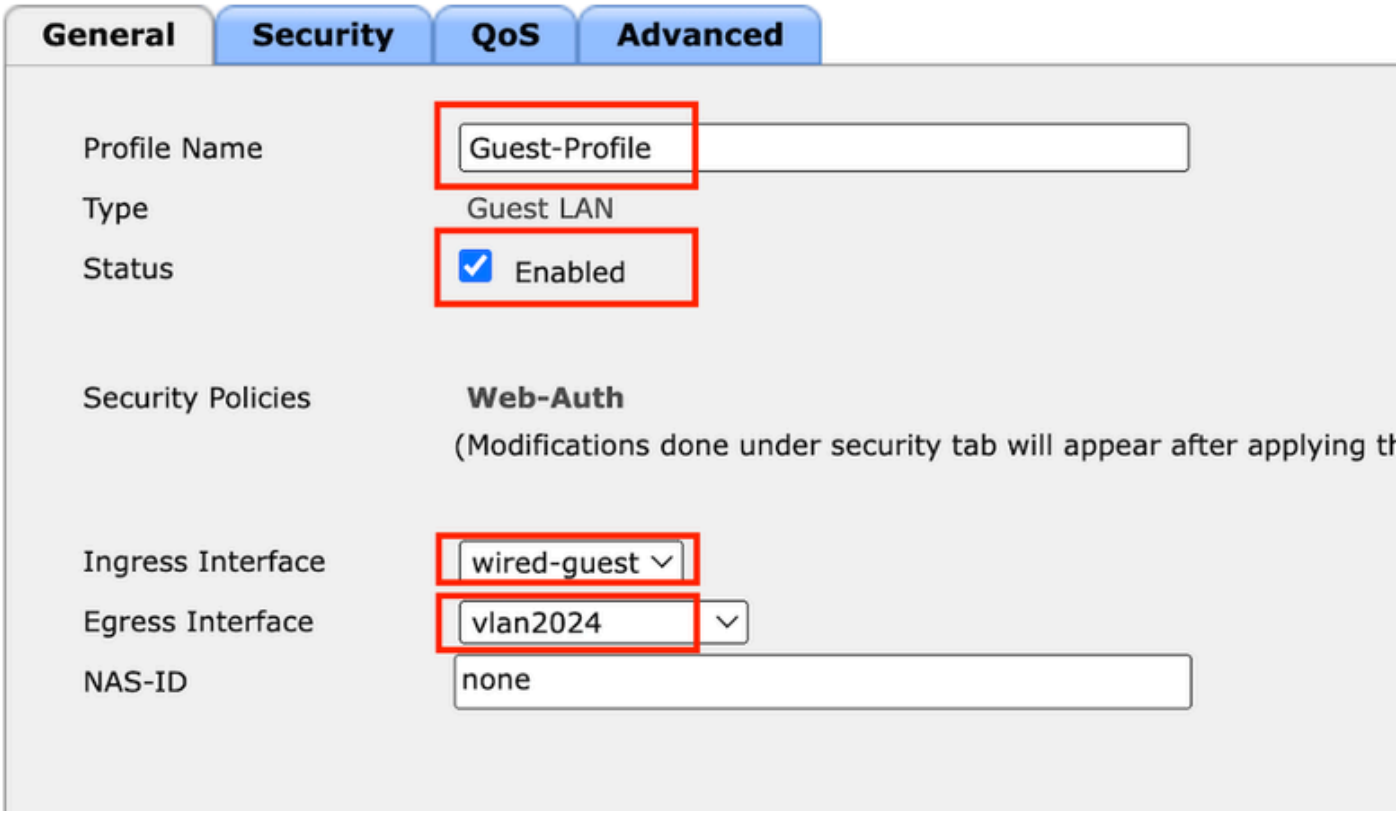
Type as Guest LAN(게스트 LAN으로 유형)을 선택하고 프로파일 이름을 구성합니다. 9800 Anchor 컨트롤러의 정책 프로파일과 게스트 LAN 프로파일에서 동일한 이름을 구성해야 합니다.

게스트 LAN 프로필

2단계: General(일반) 탭에서 게스트 LAN 프로필의 Ingress(인그레스) 및 Egress(이그레스) 인터페이스를 매핑합니다.

인그레스 인터페이스는 유선 클라이언트가 물리적으로 연결하는 VLAN입니다.

이그레스 인터페이스는 클라이언트가 IP 주소에 대해 요청하는 VLAN 서브넷입니다.

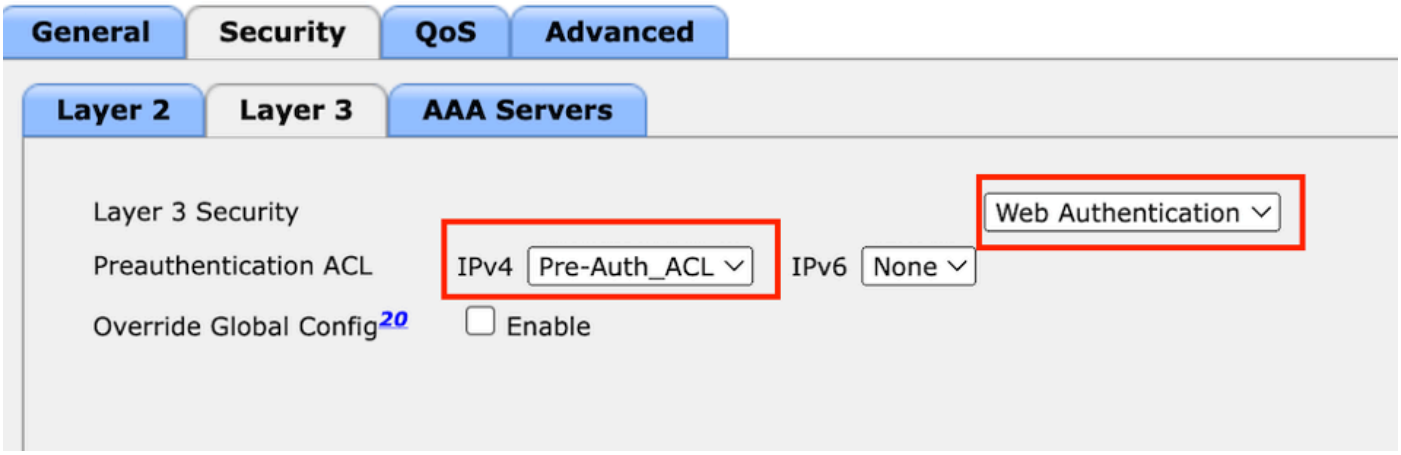


게스트 LAN 프로필

3단계: Security(보안) > Layer 3(레이어 3)으로 이동합니다.

Layer 3 Security as Web Authentication(웹 인증으로 레이어 3 보안)을 선택하고 사전 인증 ACL을

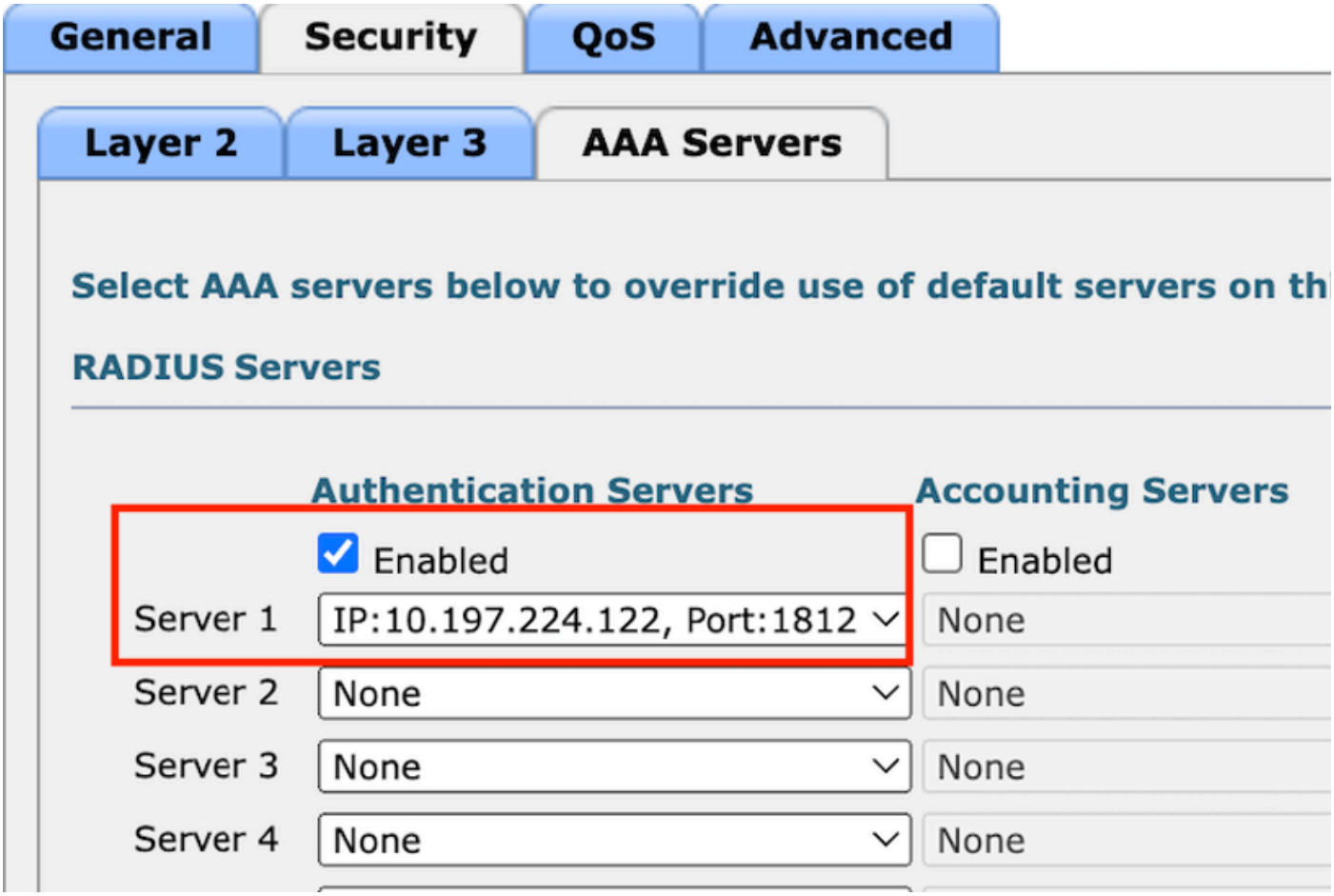
매핑합니다.



레이어 3 보안 탭

4단계:

AAA servers(AAA 서버) 탭에서 Radius 서버를 매핑하고 Enabled(활성화됨) 확인란을 선택합니다.



게스트 LAN 프로필에 RADIUS 서버 매핑

5단계: WLAN 페이지로 이동하고 게스트 LAN 프로필의 드롭다운 아이콘 위에 마우스 커서를 올려 놓고 Mobility Anchors(모빌리티 앵커)를 선택합니다.

모빌리티 앵커

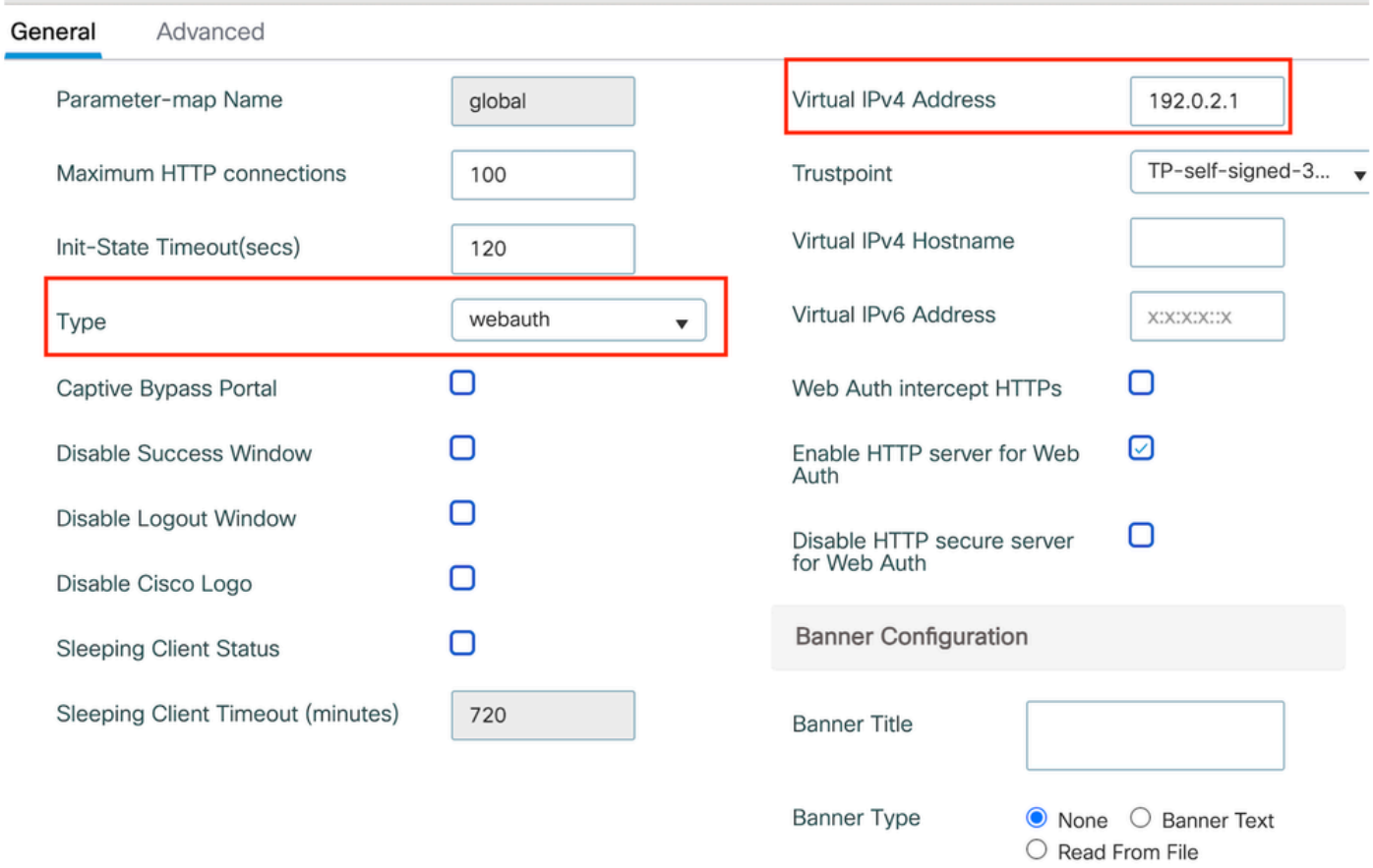
6단계: 드롭다운 목록의 모빌리티 앵커를 게스트 LAN 프로필에 매핑합니다.

게스트 LAN에 모빌리티 앵커 매핑

앵커 9800 WLC의 컨피그레이션

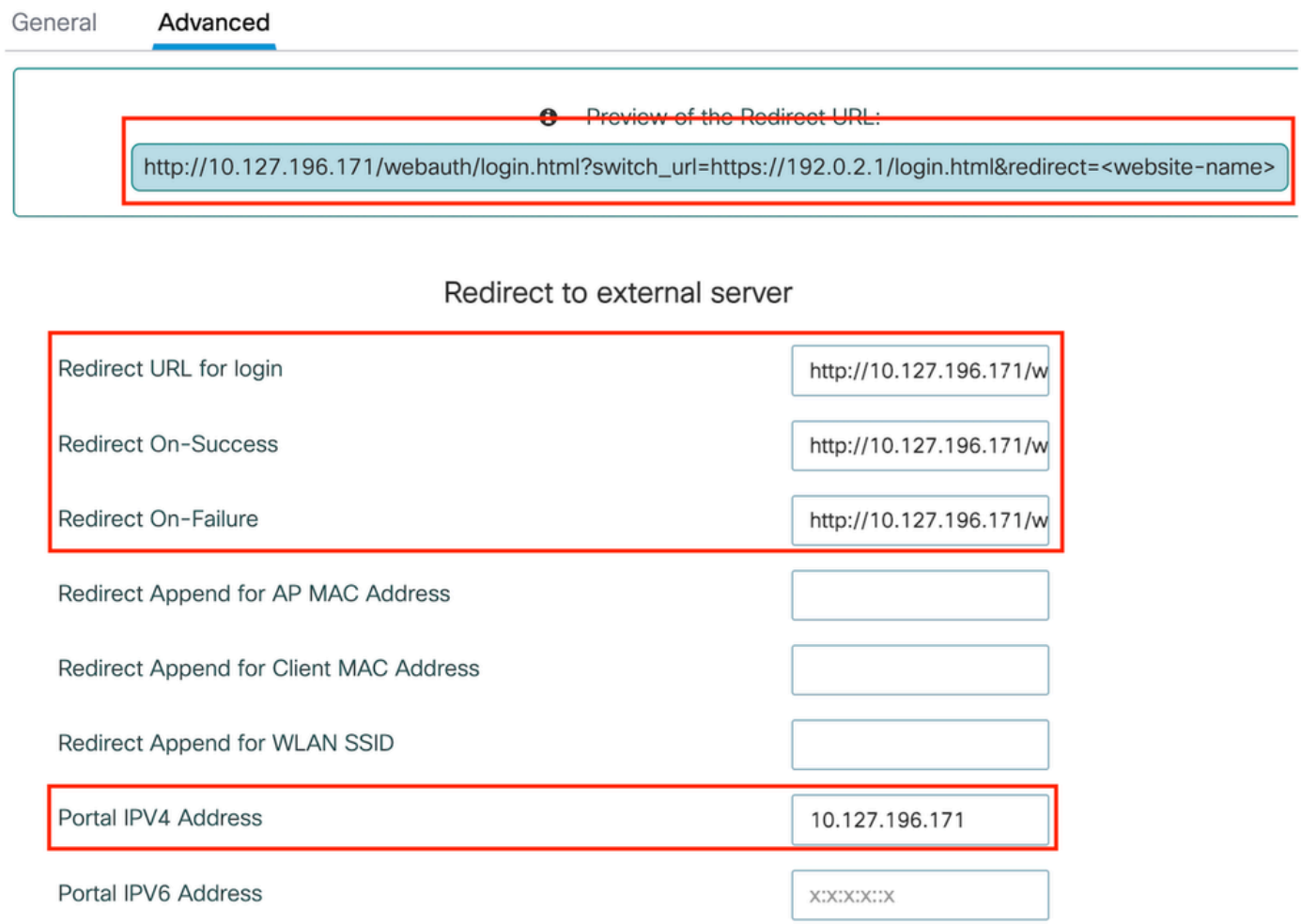
웹 매개 변수 맵 구성

1단계: Configuration(컨피그레이션) > Security(보안) > Web Auth(웹 인증)로 이동하고 Global(전역)을 선택합니다. 컨트롤러 및 신뢰 지점의 가상 IP 주소가 프로필에 올바르게 매핑되었는지, 유형이 webauth로 설정되어 있는지 확인합니다.



웹 매개 변수 맵

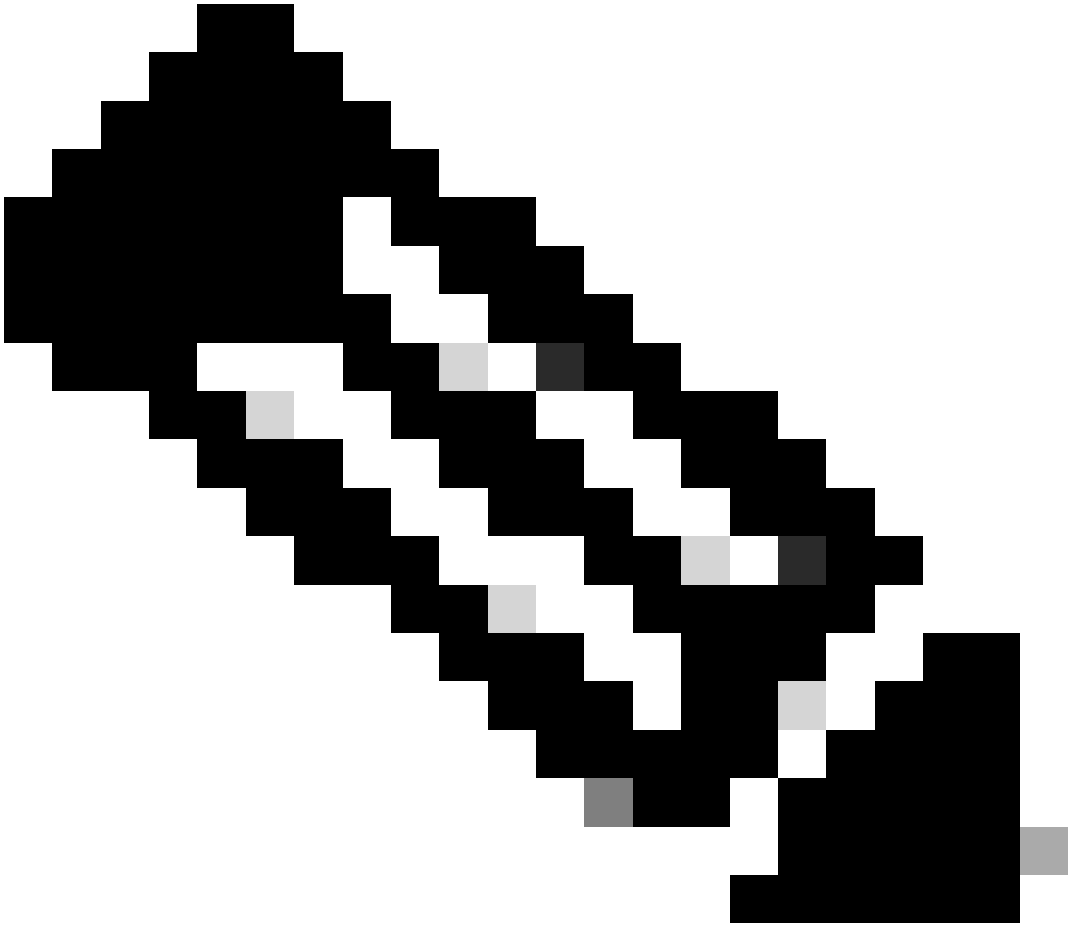
2단계: Advanced(고급) 탭에서 클라이언트를 리디렉션해야 하는 외부 웹 페이지 URL을 지정합니다. 로그인 및 실패 시 리디렉션을 위한 리디렉션 URL을 구성합니다. Redirect On-Success 설정은 선택적 컨피그레이션입니다.



고급 탭

CLI 컨피그레이션

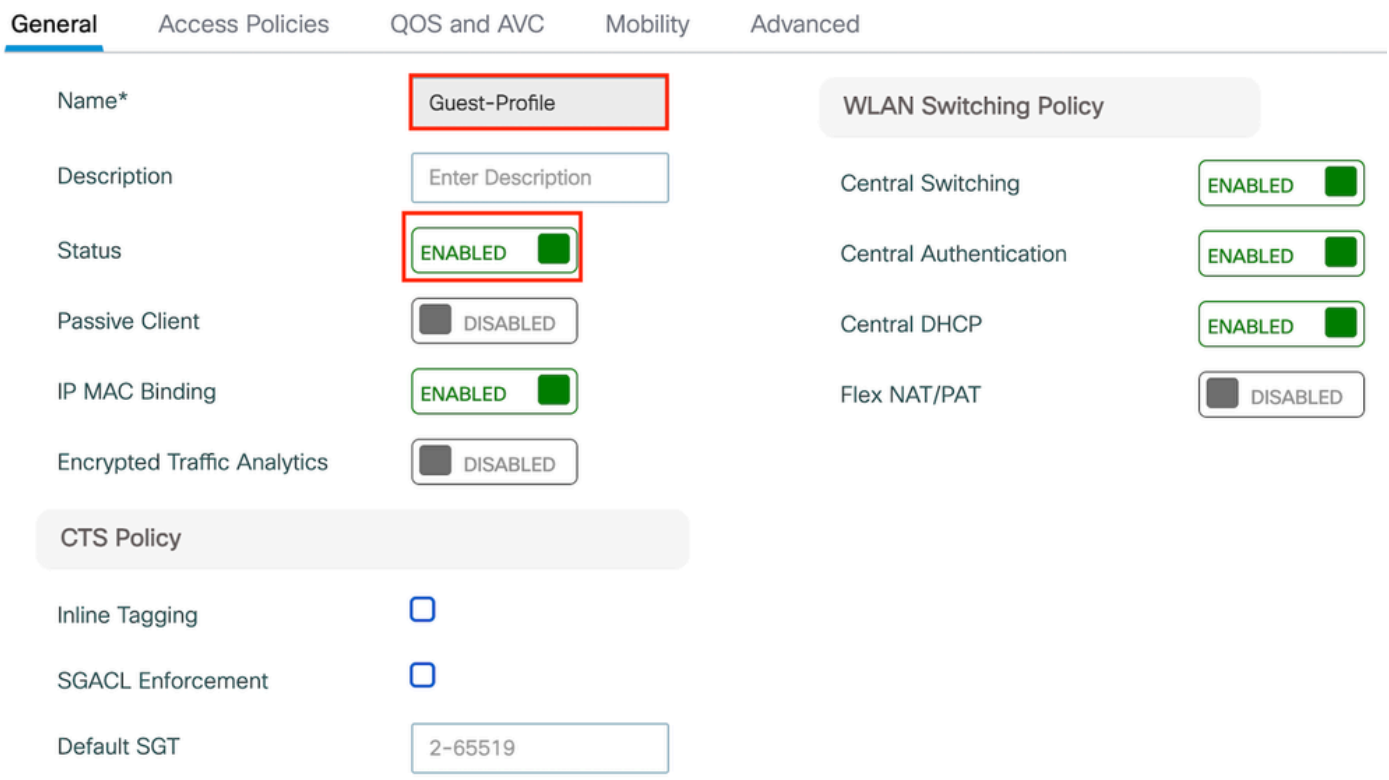
```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 trustpoint TP-self-signed-3010594951
 webauth-http-enable
```



참고: AAA 컨피그레이션의 경우 Foreign 9800 WLC의 "Configure Wired Guest on catalyst 9800 anchored to another catalyst 9800" 섹션에 제공된 컨피그레이션 세부사항을 참조하십시오.

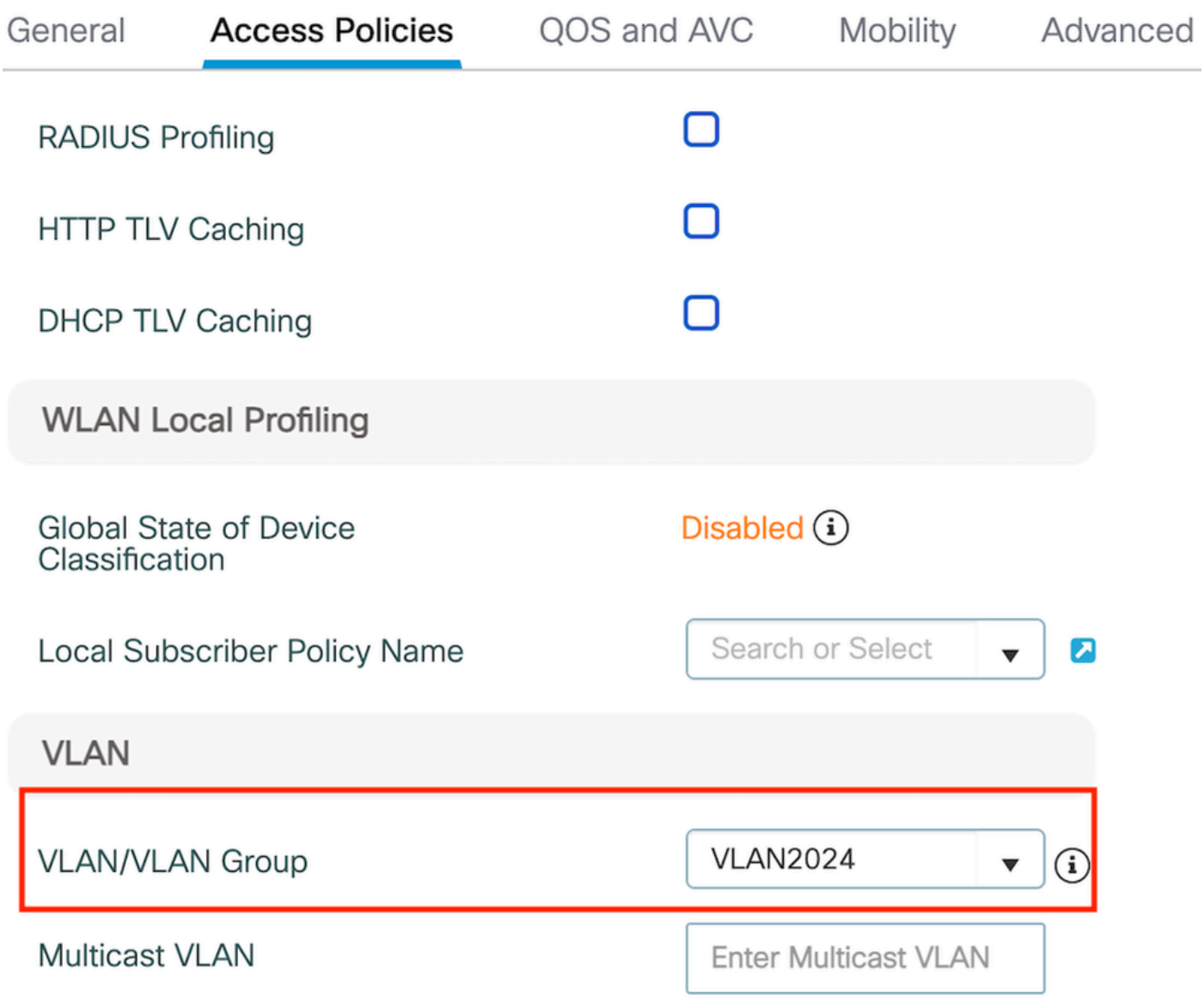
정책 프로필 구성

1단계: Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동합니다. 외부 컨트롤러의 게스트 LAN 프로필에 사용되는 것과 동일한 이름으로 정책 프로필을 구성합니다.



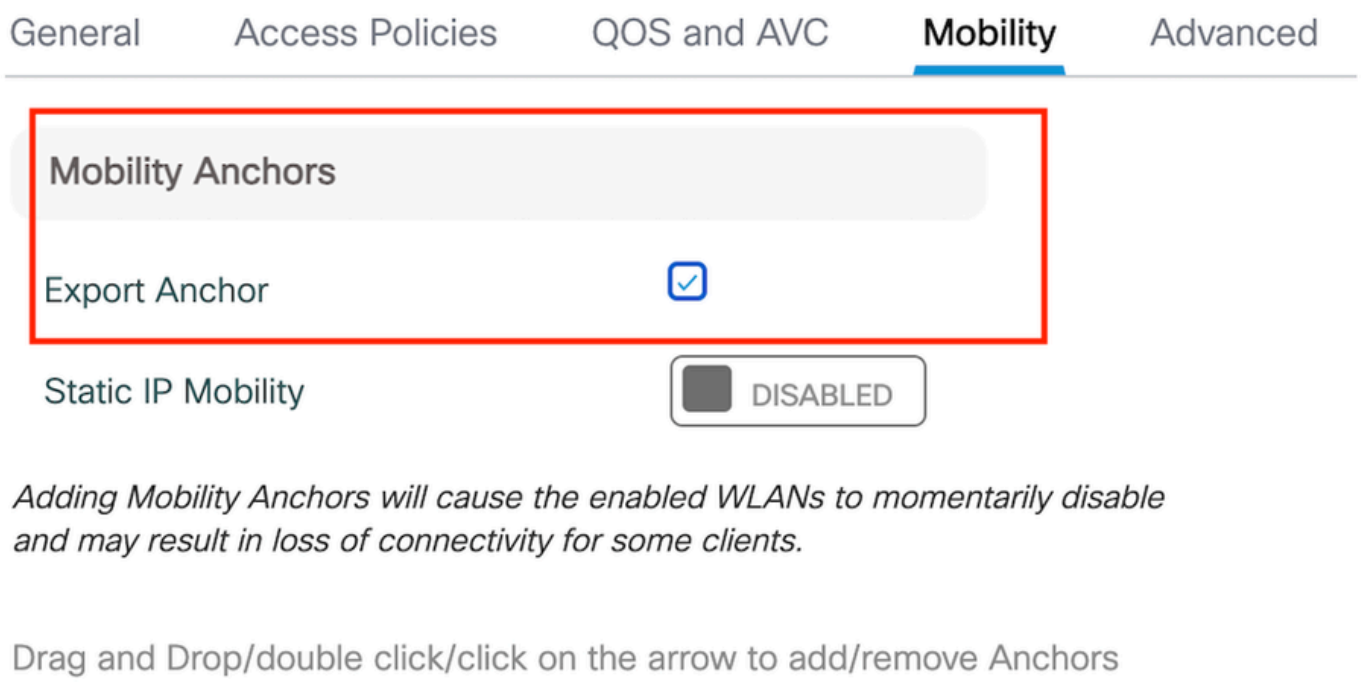
정책 프로파일

2단계: Access Policies(액세스 정책) 탭의 드롭다운 목록에서 유선 클라이언트 vlan을 매핑합니다



액세스 정책

3단계: Mobility(모빌리티) 탭 아래에서 Export Anchor(앵커 내보내기)를 선택합니다.



모빌리티 탭

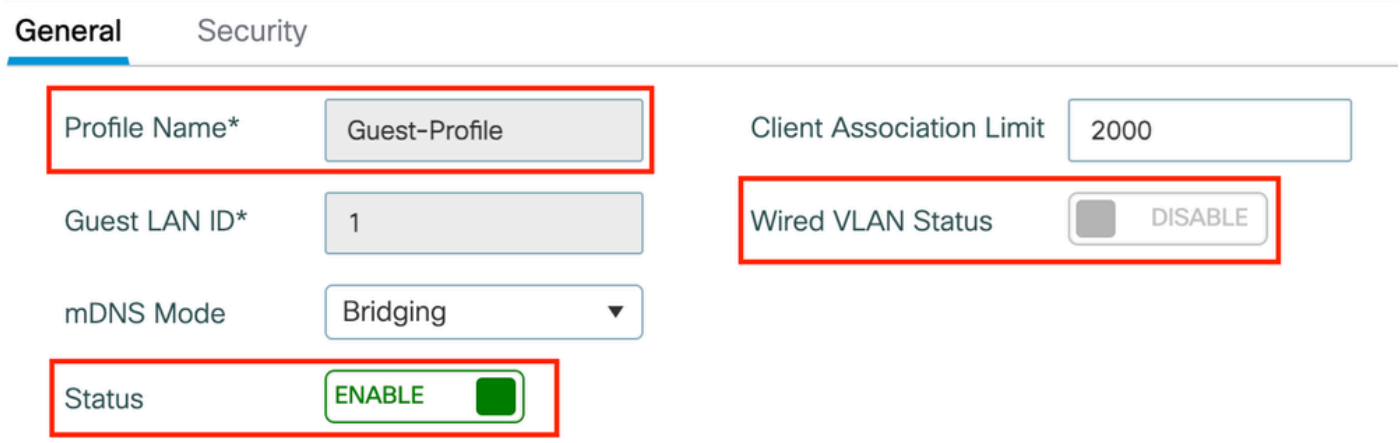
CLI 컨피그레이션

```
wireless profile policy Guest-Profile
 no accounting-interim
 exclusionlist timeout 180
 no flex umbrella dhcp-dns-option
 mobility anchor
 vlan VLAN2024
 no shutdown
```

게스트 LAN 프로필 구성

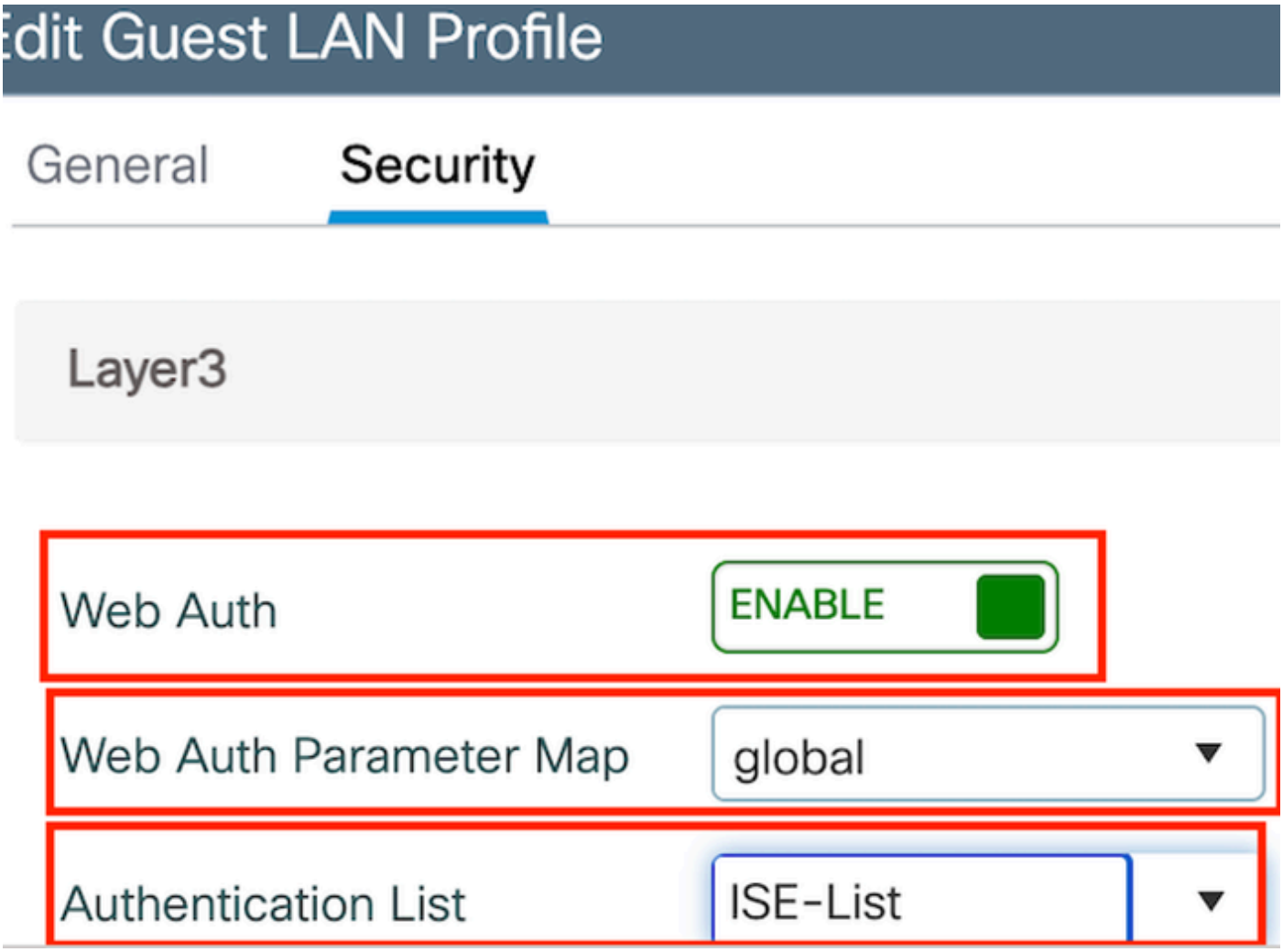
1단계: Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동하고 Add(추가)를 선택하여 게스트 LAN 프로필을 구성하고 유선 VLAN 상태를 비활성화합니다.

앵커의 게스트 LAN 프로파일 이름은 외부 WLC의 게스트 LAN 프로파일과 같아야 합니다.



게스트 LAN 프로필

2단계: Security(보안) 탭 아래에서 Web Auth(웹 인증)를 활성화합니다. 드롭다운 목록에서 Web Auth(웹 인증) 매개변수 맵 및 Authentication List(인증 목록)를 선택합니다



게스트 LAN 보안 탭

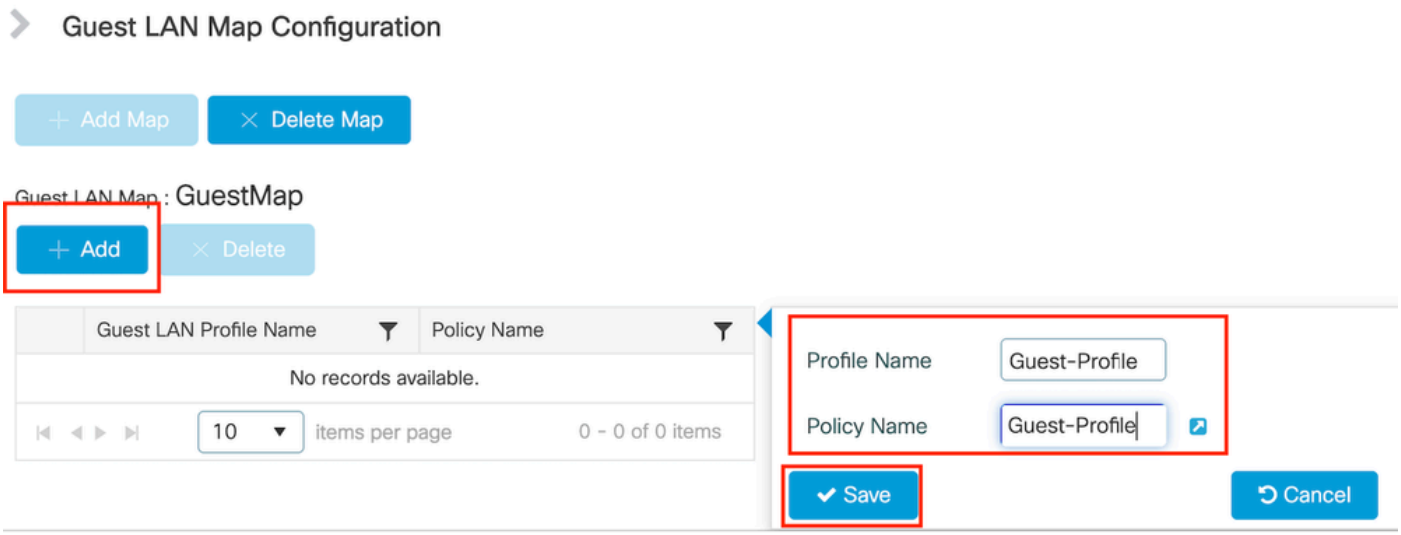
CLI 컨피그레이션

```
guest-lan profile-name Guest-Profile 1
```

```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

게스트 LAN 맵

1단계: Configuration(컨피그레이션) > Wireless(무선) > Guest LAN(게스트 LAN)으로 이동합니다. Guest LAN MAP 컨피그레이션 섹션에서 Add(추가)를 선택하고 Policy Profile(정책 프로필)을 Guest LAN 프로필에 매핑합니다.



게스트 LAN 맵

다음을 확인합니다.

컨트롤러 컨피그레이션 확인

#show-lan 요약

```
GLAN  GLAN Profile Name                  Status
-----------------------------------------------
1     Guest-Profile                      UP
2     Guest                              UP
```

#show-lan id 1 사용

<#root>

```
Guest-LAN Profile Name     : Guest
================================================
Guest-LAN ID                                  : 2
Wired-Vlan                                    :
```

```
Status                                          :

Enabled

Number of Active Clients                        : 0
Max Associated Clients                          : 2000
Security
    WebAuth                                     :

Enabled

    Webauth Parameter Map                       : global
    Webauth Authentication List                 :

ISE-List

    Webauth Authorization List                  : Not configured
mDNS Gateway Status                             : Bridge
```

#show 매개변수 맵 유형 webauth 전역

<#root>

```
Parameter Map Name              : global
  Type                          :

webauth

  Redirect:
    For Login                   :

http://10.127.196.171/webauth/login.html

    On Success                  :

http://10.127.196.171/webauth/logout.html

    On Failure                  :

http://10.127.196.171/webauth/failed.html

    Portal ipv4                 :

10.127.196.171

        Virtual-ipv4                :

192.0.2.1
```

#show-map type webauth name <profile name> (사용자 지정 웹 매개 변수 프로필을 사용하는 경우)

#show guest-lan-map 요약

```
GLAN Profile Name                   Policy Name
------------------------------------------------------------------------------
Guest                               Guest
```

#show 무선 모빌리티 요약

```
IP                                          Public Ip                                       MAC Address
-------------------------------------------------------------------------------------------------------
10.76.118.70                                10.76.118.70                                    f4bd.9e59.314b
```

#show http 서버 상태 확인

```
HTTP server status: Enabled
HTTP server port: 80
HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local

HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server trustpoint: TP-self-signed-3010594951
```

>게스트 LAN 요약 표시

```
Number of Guest LANs.............................. 1

GLAN ID  GLAN Profile Name                     Status    Interface Name
-------  -------------------------------------  --------  --------------------
2        Guest                                 Enabled  wired-vlan-11
```

>show guest-lan 2

```
Guest LAN Identifier.............................. 2
Profile Name...................................... Guest
Status............................................ Enabled
Interface......................................... wired-vlan-11
Radius Servers
   Authentication................................. 10.197.224.122 1812 *
    Web Based Authentication...................... Enabled
   Web Authentication Timeout..................... 300
        IPv4 ACL.................................... Pre-Auth_ACL
               Mobility Anchor List
 GLAN ID     IP Address            Status
 -------     ---------------       ------
 2           10.76.118.74          Up
```

>사용자 지정 웹 모두 표시

```
Radius Authentication Method..................... PAP
Cisco Logo....................................... Enabled
CustomLogo....................................... None
Custom Title..................................... None
Custom Message................................... None
Custom Redirect URL.............................. http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode....... None
Web Authentication Type.......................... External
Logout-popup..................................... Enabled
External Web Authentication URL.................. http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer.................... 0
QR Code Scanning Bypass Count.................... 0
```

>show custom-web guest-lan 2

```
Guest LAN Status............................... Enabled
Web Security Policy............................ Web Based Authentication
WebAuth Type................................... External
Global Status.................................. Enabled
```

클라이언트 정책 상태 검증

외국에서

#show 무선 클라이언트 요약

클라이언트가 성공적으로 연결되면 외부 컨트롤러의 클라이언트 정책 관리자 상태가 RUN입니다.

<#root>

```
MAC Address    AP Name                                          Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------
a0ce.c8c3.a9b5 N/A

GLAN 1

    Run

802.3

    Web Auth

Export Foreign
```

>show client detail a0ce.c8c3.a9b5

<#root>

```
Client MAC Address.............................. a0:ce:c8:c3:a9:b5
Client Username ................................ N/A
Client Webauth Username ........................ N/A
Client State.................................... Associated
User Authenticated by .......................... None
Client User Group.............................
Client NAC OOB State............................ Access
guest-lan....................................... 1
Wireless LAN Profile Name....................... Guest-Profile
Mobility State..................................

Export Foreign

Mobility Anchor IP Address.....................

10.76.118.70

Security Policy Completed.......................

Yes

Policy Manager State............................

RUN

Pre-auth IPv4 ACL Name.......................... Pre-Auth_ACL
EAP Type........................................ Unknown
Interface.......................................

wired-guest-egress

VLAN............................................ 2024
Quarantine VLAN................................. 0
```

앵커에서

클라이언트 상태 전송은 앵커 컨트롤러에서 모니터링해야 합니다.

클라이언트 정책 관리자 상태가 웹 인증 보류 중입니다.

<#root>

```
MAC Address    AP Name                                          Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------
a0ce.c8c3.a9b5 10.76.6.156

GLAN 1

    Webauth Pending

802.3

    Web Auth

Export Anchor
```

클라이언트가 인증되면 정책 관리자 상태가 RUN 상태로 전환됩니다.

```
MAC Address    AP Name                                             Type ID   State             Protocol Meth
-------------------------------------------------------------------------------------------------------------
a0ce.c8c3.a9b5 10.76.6.156                                         GLAN 1    Run               802.3    Web A
```

#show 무선 클라이언트 mac-address a0ce.c8c3.a9b5 세부 정보

<#root>

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
```

10.105.211.69

```
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
  GLAN Id: 1
  GLAN Name: Guest-Profile

Mobility:
  Foreign IP Address          :
```

10.76.118.74

```
  Point of Attachment         : 0xA0000003
  Point of Presence           : 0
  Move Count                  : 1
  Mobility Role               :
```

Export Anchor

```
  Mobility Roam Type          :
```

L3 Requested

```
Policy Manager State:
```

Webauth Pending

```
Last Policy Manager State :
```

IP Learn Complete

```
Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:
  Point of Attachment : mobility_a0000003
  IIF ID              : 0xA0000003
  Authorized          : FALSE
  Session timeout     : 28800
  Common Session ID: 4a764c0a0000008ea0285466
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : Web Auth
```

```
                Webauth State    :
```

Login

```
                Webauth Method   :
```

Webauth

```
Server Policies:
  Resultant Policies:
                URL Redirect ACL :
```

WA-v4-int-10.127.196.171

```
                Preauth ACL      :
```

WA-sec-10.127.196.171

```
                VLAN Name        : VLAN2024
                VLAN             :
```

2024

```
                Absolute-Timer   : 28800
```

웹 인증에 성공하면 클라이언트가 RUN 상태로 전환됩니다.

show wireless client mac-address a0ce.c8c3.a9b5 detail

<#root>

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
```

10.105.211.69

```
Client Username :
```

testuser

```
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile : N/A
Guest Lan:
  GLAN Id: 1
  GLAN Name: Guest-Profile
Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 81 seconds
Protocol : 802.3

Policy Manager State:
```

Run

```
Last Policy Manager State :
```

Webauth Pending

Client Entry Create Time : 81 seconds
VLAN : VLAN2024

Last Tried Aaa Server Details:
Server IP :

10.197.224.122

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

Resultant Policies:
URL Redirect ACL :

IP-Adm-V4-LOGOUT-ACL

VLAN Name : VLAN2024
VLAN :

2024

Absolute-Timer : 28800

>show client detail a0:ce:c8:c3:a9:b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username ..... N/A
Client Webauth Username ..... N/A
Client State..... Associated
Wireless LAN Profile Name..... Guest
WLAN Profile check for roaming..... Disabled
Hotspot (802.11u)..... Not Supported
Connected For ..... 90 secs
IP Address..... 10.105.211.75
Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....

Export Anchor

Mobility Foreign IP Address.....

10.76.118.70

Security Policy Completed..... No
Policy Manager State.....

WEBAUTH_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth_ACLPre-auth

IPv4 ACL Applied Status..... Yes
Pre-auth IPv4 ACL Applied Status.....

Yes

인증 후 클라이언트가 RUN 상태로 전환됩니다.

<#root>

```
show client detail a0:ce:c8:c3:a9:b5
Client MAC Address.............................. a0:ce:c8:c3:a9:b5
Client Username ..............................

testuser

Client Webauth Username ......................

testuser

Client State..................................

Associated


User Authenticated by ........................

RADIUS Server

Client User Group.............................. testuser
Client NAC OOB State........................... Access
Connected For ................................. 37 secs
IP Address.....................................

10.105.211.75

Gateway Address................................ 10.105.211.1
Netmask........................................ 255.255.255.128
Mobility State..............................

Export Anchor

Mobility Foreign IP Address..................... 10.76.118.70
Security Policy Completed...................... Yes
Policy Manager State..........................

RUN

Pre-auth IPv4 ACL Name......................... Pre-Auth_ACL
Pre-auth IPv4 ACL Applied Status............... Yes
EAP Type....................................... Unknown
Interface.....................................

wired-vlan-11

VLAN.........................................

11

Quarantine VLAN................................ 0
```

문제 해결

AireOS 컨트롤러 디버그

클라이언트 디버그 사용

>debug 클라이언트 <H.H.H>

디버깅이 활성화되었는지 확인하려면

>디버깅 표시

디버그를 비활성화하려면

모두 디버그 비활성화

9800 방사능 흔적

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

Radioactive Tracing 활성화 단계:

모든 조건부 디버그가 비활성화되어 있는지 확인합니다.

```
clear platform condition all
```

지정된 mac 주소에 대해 디버그를 활성화합니다.

```
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 컨트롤러의 bootflash에서 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
```

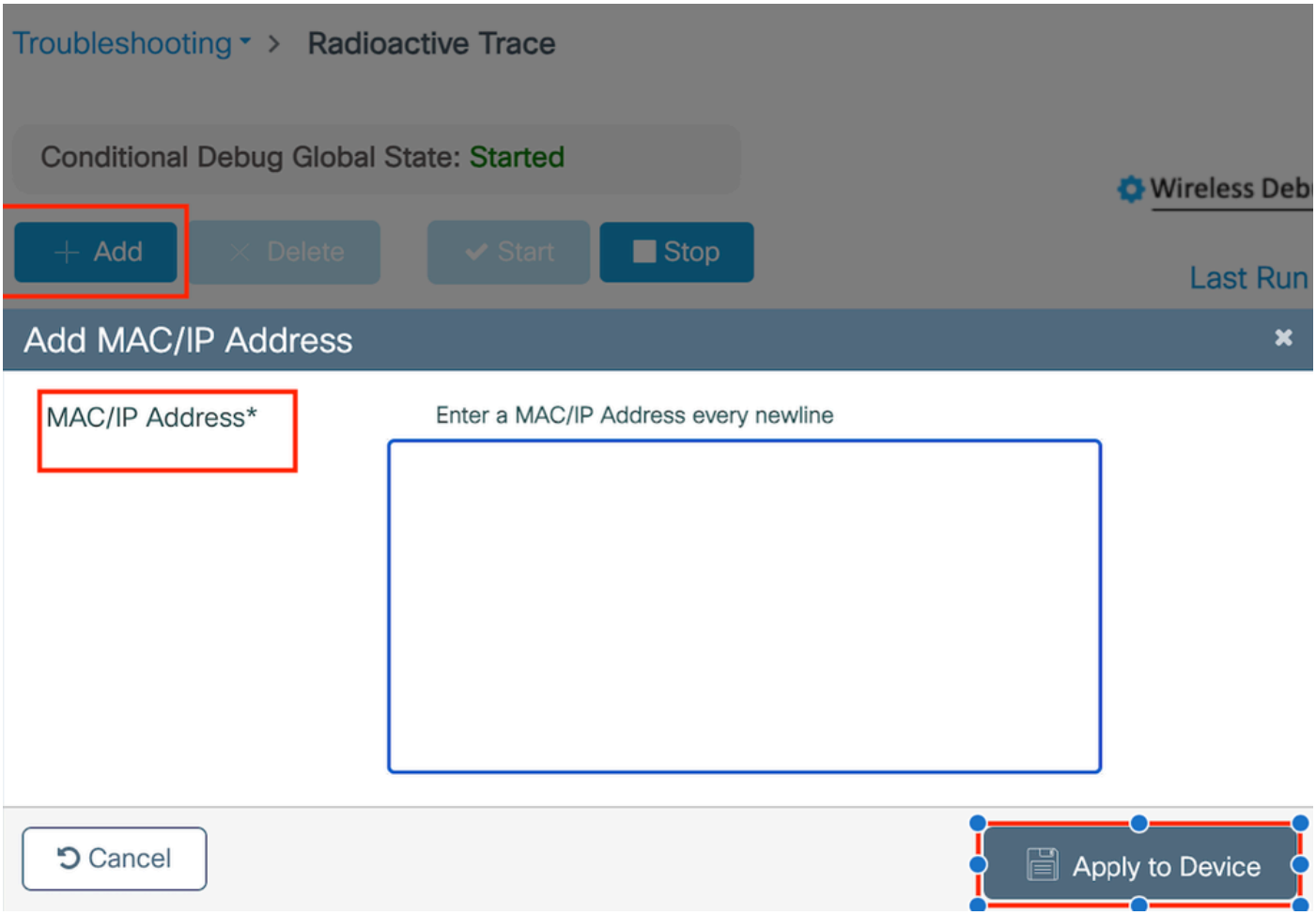
파일을 외부 서버에 복사.

```
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
```

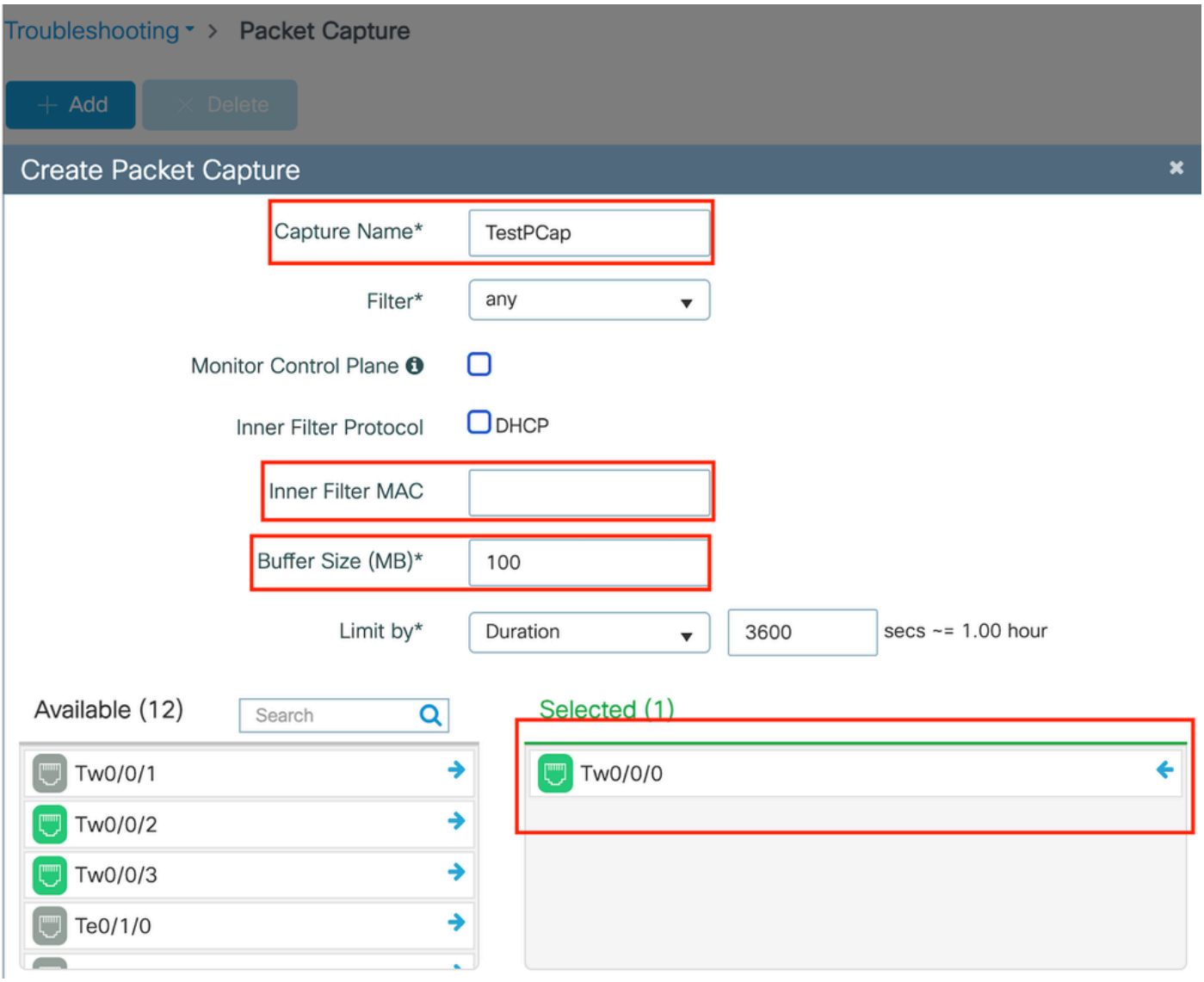
GUI에서 RA 추적 활성화



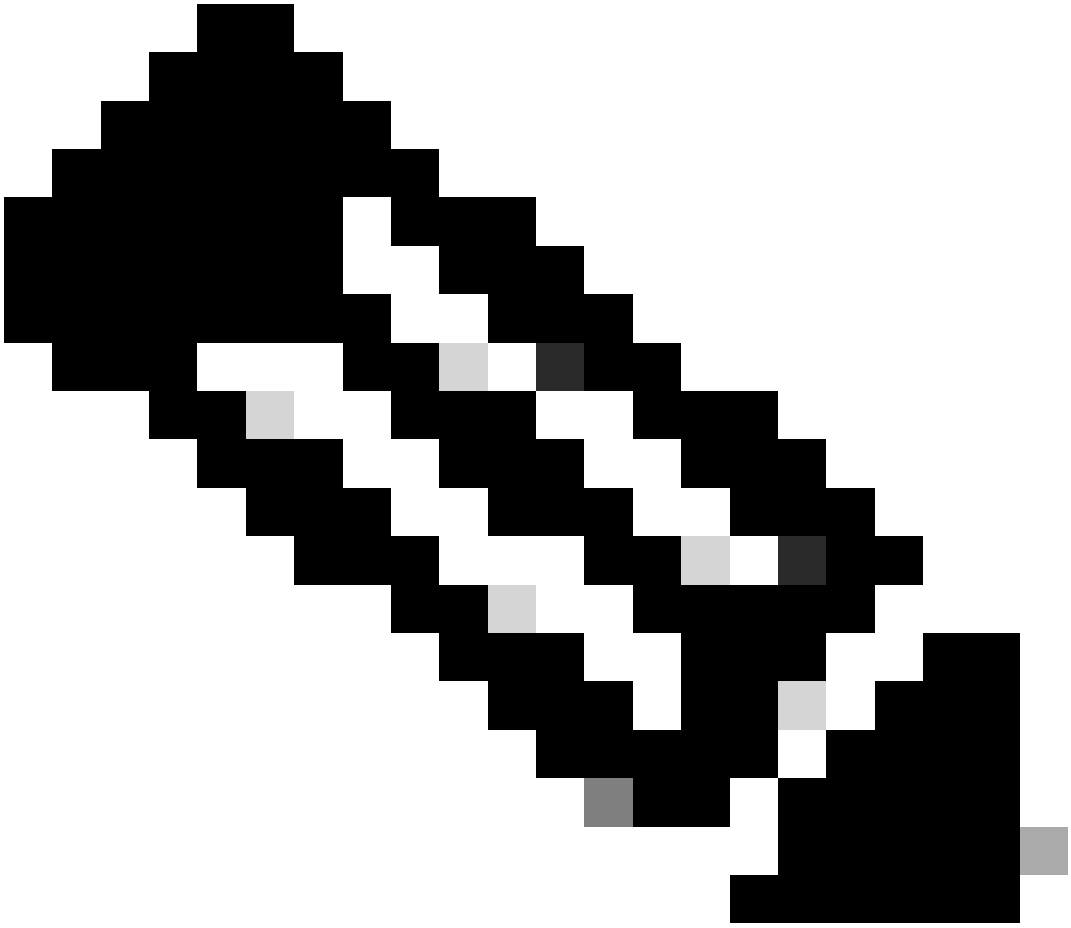
WebUI에서 RA 추적 사용

임베디드 패킷 캡처

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

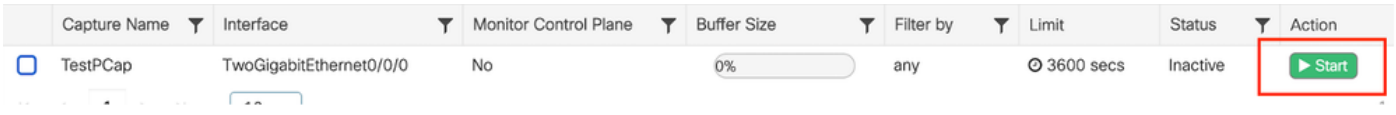

Troubleshooting
Packet Capture
Add
Delete
Create Packet Capture
Capture Name*
TestPCap
Filter*
any
Monitor Control Plane
Inner Filter Protocol
DHCP
Inner Filter MAC
Buffer Size (MB)*
100
Limit by*
Duration
3600
secs ~= 1.00 hour
Available (12)
Search
Tw0/0/1
Tw0/0/2
Tw0/0/3
Te0/1/0
Selected (1)
Tw0/0/0

임베디드 패킷 캡처



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

Troubleshooting(트러블슈팅) > Packet Capture(패킷 캡처)로 이동하고 Start(시작)를 선택하여 패킷을 캡처합니다.



패킷 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
```

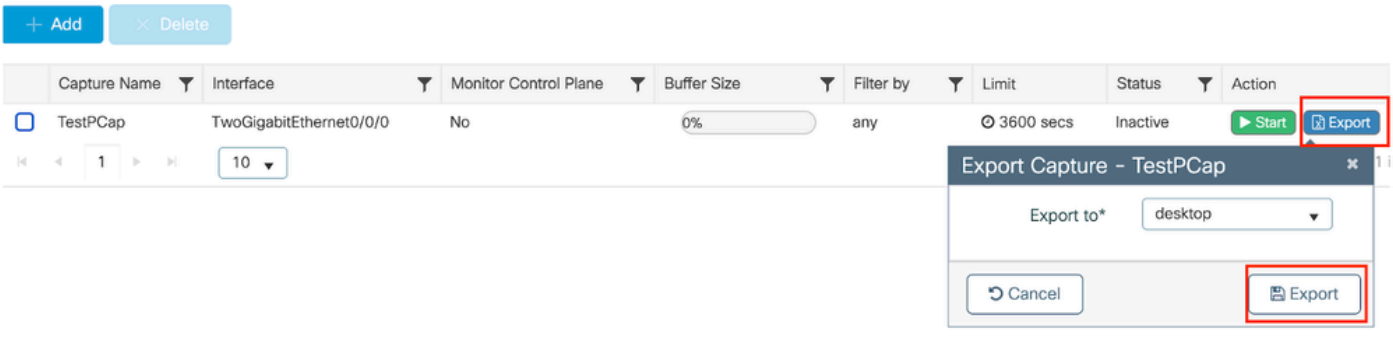
```
show monitor capture TestPCap

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)
```

패킷 캡처를 외부 TFTP 서버로 내보냅니다.

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

Troubleshooting(트러블슈팅) > Packet Capture(패킷 캡처)로 이동하고 Export(내보내기)를 선택하여 로컬 시스템에 캡처 파일을 다운로드합니다.



EPC 다운로드

작업 로그 조각

AireOS 외부 컨트롤러 클라이언트 디버그 로그

유선 클라이언트에서 유선 패킷을 받았습니다.

```
*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5  Wired Guest packet from 10.105.211.69 on mobil
```

외부 컨트롤러 빌딩 내보내기 앵커 요청

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0
```

외부 컨트롤러가 앵커 컨트롤러로 앵커 내보내기 요청을 보냅니다.

```
*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70
```

앵커 컨트롤러가 클라이언트에 대한 앵커 요청에 대한 확인을 보냅니다.

```
*Dot1x_NW_MsgTask_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile  a0:ce:c8:c
```

외래 컨트롤러의 클라이언트에 대한 모빌리티 역할이 외래를 내보내도록 업데이트됩니다.

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) mobility role update requ
  Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70
```

클라이언트가 RUN 상태로 전환되었습니다.

```
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mobilit
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:
*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800 Foreign Controller 방사능 흔적

클라이언트가 컨트롤러에 연결합니다.

```
2024/07/15 04:10:29.087608331 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

연결 후 모빌리티 검색이 진행 중입니다.

```
2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

모빌리티 검색이 처리되면 클라이언트 로밍 유형이 요청된 L3에 대한 업데이트입니다.

```
2024/07/15 04:10:29.091664605 {wncd_x_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM
2024/07/15 04:10:29.091693445 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t
```

외부 컨트롤러가 앵커 WLC에 내보내기 앵커 요청을 보내고 있습니다.

```
2024/07/15 04:10:32.093245394 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 04:10:32.093253788 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo
2024/07/15 04:10:32.093274405 {mobilityd_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For
```

앵커 컨트롤러에서 앵커 내보내기 응답을 수신하고 사용자 프로필에서 vlan을 적용합니다.

```
2024/07/15 04:10:32.106775213 {mobilityd_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 04:10:32.106811183 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 04:10:32.107183692 {wncd_x_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An
2024/07/15 04:10:32.107247304 {wncd_x_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr
2024/07/15 04:10:32.107250258 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:
```

Export Anchor(앵커 내보내기) 요청이 처리되면 클라이언트 이동성 역할이 Export Foreign(외부 내보내기)으로 업데이트됩니다.

```
2024/07/15 04:10:32.107490972 {wncd_x_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce
2024/07/15 04:10:32.107502336 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili
2024/07/15 04:10:32.107533732 {wncd_x_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20
2024/07/15 04:10:32.107592251 {wncd_x_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

클라이언트가 IP learn 상태로 전환됩니다.

```
2024/07/15 04:10:32.108210365 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 04:10:32.108293096 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5
```

IP 학습 후 클라이언트는 외부 WLC에서 RUN 상태로 전환됩니다.

```
2024/07/15 04:10:32.108521618 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

AireOS Anchor 컨트롤러 클라이언트 디버그 로그

외부 컨트롤러에서 수신된 내보내기 앵커 요청입니다.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv  Ssid=Guest  useProfileNa
```

로컬 브리징 VLAN이 클라이언트에 적용됩니다.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol
```

모빌리티 역할이 Export Anchor(내보내기 앵커) 및 Client State(클라이언트 상태)가 Associated(연결됨)로 변환됩니다.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ
  Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74
Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
                                                    add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5
                                                    Sent message to add a0:ce:c8:c3:a9:b5 on me
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi
```

모빌리티가 완료되었습니다. 클라이언트 상태가 연결되었으며 모빌리티 역할은 Export Anchor(내보내기 앵커)입니다.

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

클라이언트 IP 주소는 컨트롤러에서 학습되며 상태는 DHCP에서 웹 인증 필수로 변환됩니다.

```
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

Webauth URL은 외부 리디렉션 URL 및 컨트롤러 가상 IP 주소를 추가하여 공식화됩니다.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```

URL에 클라이언트 mac 주소 및 WLAN을 추가했습니다.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http:/
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127
```

호스트 10.105.211.1에 대한 HTTP GET의 구문 분석 후 최종 URL

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-  parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

리디렉션 URL은 200 OK 응답 패킷에서 클라이언트로 전송됩니다.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

클라이언트가 리디렉션 url 호스트와의 TCP 연결을 설정합니다. 클라이언트가 포털에서 로그인 사용자 이름 및 비밀번호를 제출하면 컨트롤러가 radius 서버로 radius 요청을 보냅니다

컨트롤러가 Access-Accept를 수신하면 클라이언트가 TCP 세션을 닫았다가 RUN 상태로 전환됩니다.

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
```

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe

*aaaQueueReader: May 28 10:46:59:077:         AVP[01] User-Name.............................testuser
*aaaQueueReader: May 28 10:46:59:077:         AVP[03] Calling-Station-Id....................a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077:         AVP[04] Nas-Port..............................0x000000
*aaaQueueReader: May 28 10:46:59:077:         AVP[05] Nas-Ip-Address........................0x0a4c76
*aaaQueueReader: May 28 10:46:59:077:         AVP[06] NAS-Identifier........................POD1586-

*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5  Access-Accept received from RADIUS serv

*Dot1x_NW_MsgTask_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c

*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state
```

9800 앵커 컨트롤러 방사능 흔적

외부 컨트롤러에서 클라이언트에 대한 모빌리티 알림 메시지

```
2024/07/15 15:10:20.614677358 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re
```

외부 컨트롤러 RA 추적에서 확인할 수 있는 앵커 컨트롤러에서 보낸 내보내기 앵커 응답을 클라이언트가 연결할 때 외부 컨트롤러에서 내보내기 앵커 요청을 받았습니다.

```
2024/07/15 15:10:22.615246594 {mobilityd_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5
```

클라이언트가 연결 상태로 이동되고 모빌리티 역할이 내보내기 앵커로 전환됩니다.

```
2024/07/15 15:10:22.616156811 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 15:10:22.627358367 {wncd_x_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

```
2024/07/15 15:10:22.627462963 {wncd_x_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5  Client da
2024/07/15 15:10:22.627490485 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 15:10:22.627494963 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo
```

IP 학습이 완료되었으며 클라이언트 IP가 ARP를 통해 학습되었습니다.

```
2024/07/15 15:10:22.628124206 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:23.627064171 {wncd_x_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m
```

```
2024/07/15 15:10:24.469704913 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470527056 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470587596 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470613094 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
```

클라이언트 정책 상태가 웹 인증 보류 중입니다.

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5  Cli
```

TCP 핸드셰이크는 컨트롤러에 의해 스푸핑됩니다. 클라이언트가 HTTP GET을 전송할 때 리디렉션 URL을 포함하는 200 OK 응답 프레임이 전송됩니다.

클라이언트는 리디렉션 URL과 TCP 핸드셰이크를 설정하고 페이지를 로드해야 합니다.

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wnc2024/07/15 15:12:04.280574375 {wncd_x_R0-0}{1}: [webauth-httpd] [1470
```

클라이언트가 웹 포털 페이지에서 로그인 자격 증명을 제출하면 Access-Request 패킷이 인증을 위해 RADIUS 서버로 전송됩니다.

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:   Cisco AVpair
```

Access-Accept가 RADIUS 서버에서 수신되면 webauth가 성공합니다.

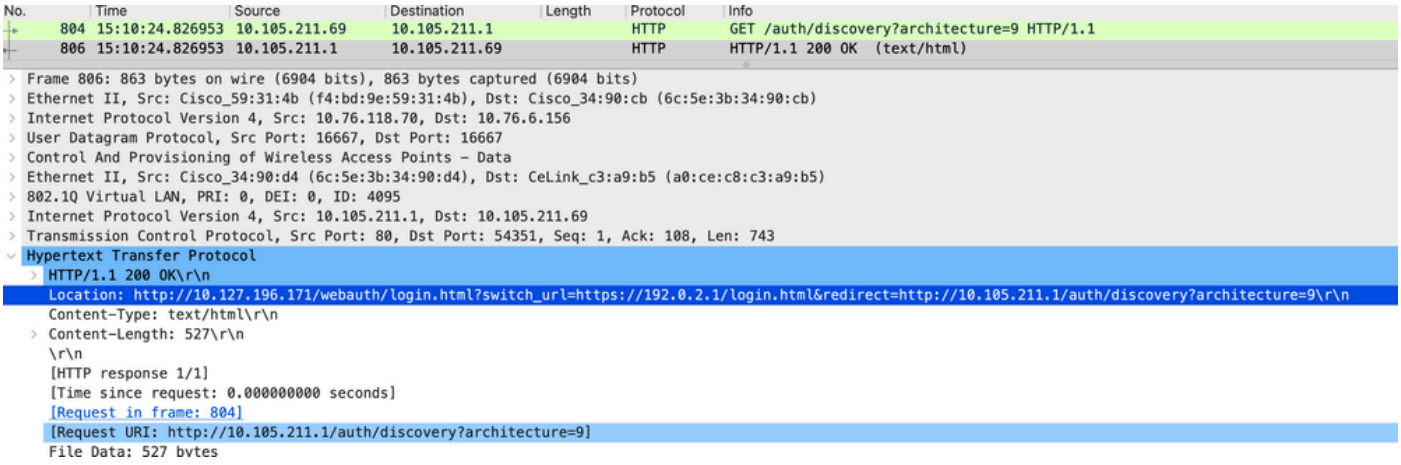
```
2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  authenticator 52 3e
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS:  User-Name
```

인증에 성공했으며 클라이언트 정책 상태가 RUN입니다.

```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
```

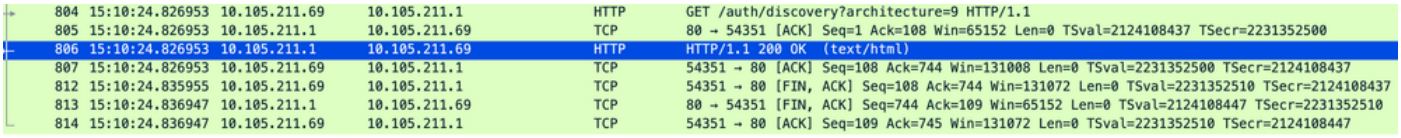
```
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
```

내장형 패킷 캡처 분석



클라이언트가 포털 페이지로 리디렉션됩니다.

리디렉션 URL을 받은 후 세션이 닫힙니다.

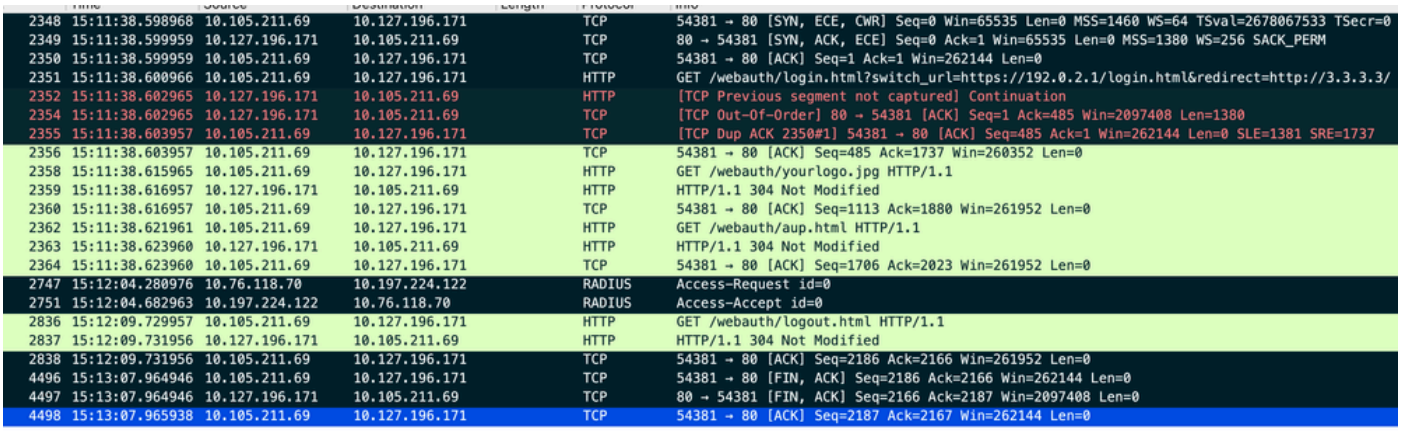


리디렉션 URL을 수신한 후 TCP 세션이 닫힘

클라이언트는 리디렉션 URL 호스트로 TCP 3 way 핸드셰이크를 시작하고 HTTP GET 요청을 보냅니다.

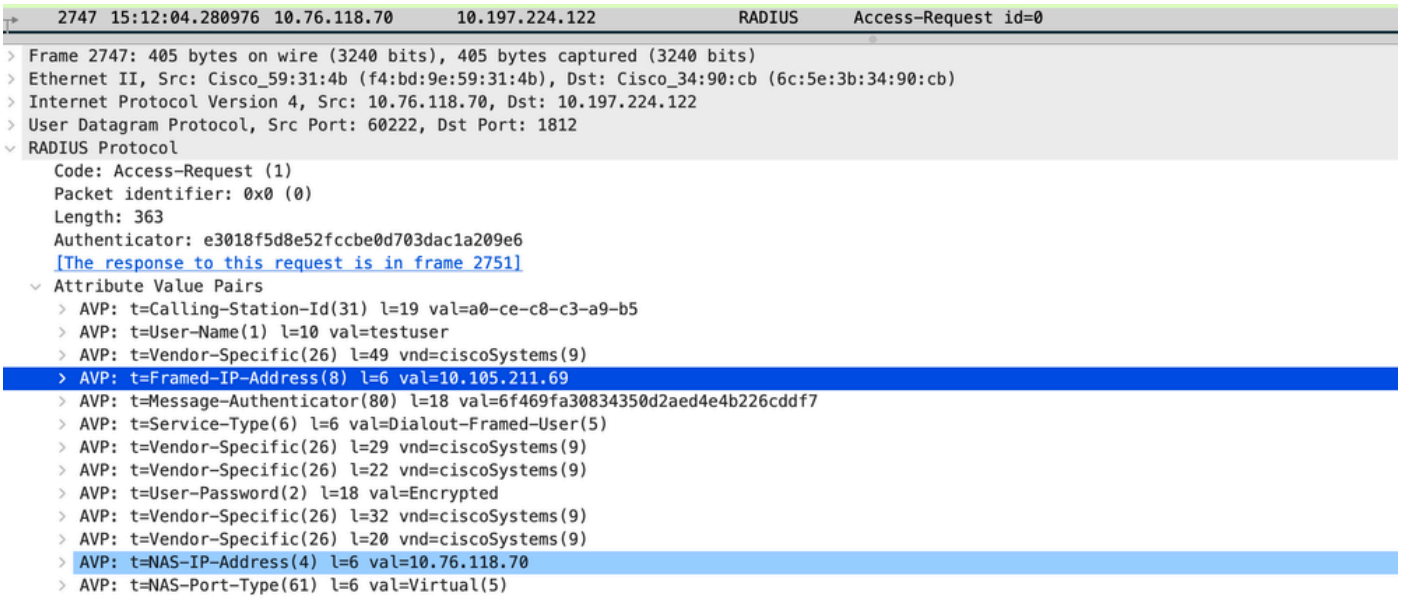
페이지가 로드되고 로그인 자격 증명이 포털에 제출되면 컨트롤러는 클라이언트를 인증하기 위해 RADIUS 서버에 액세스 요청을 보냅니다.

인증에 성공하면 웹 서버에 대한 TCP 세션이 닫히고 컨트롤러에서 클라이언트 정책 관리자 상태가 RUN으로 전환됩니다.



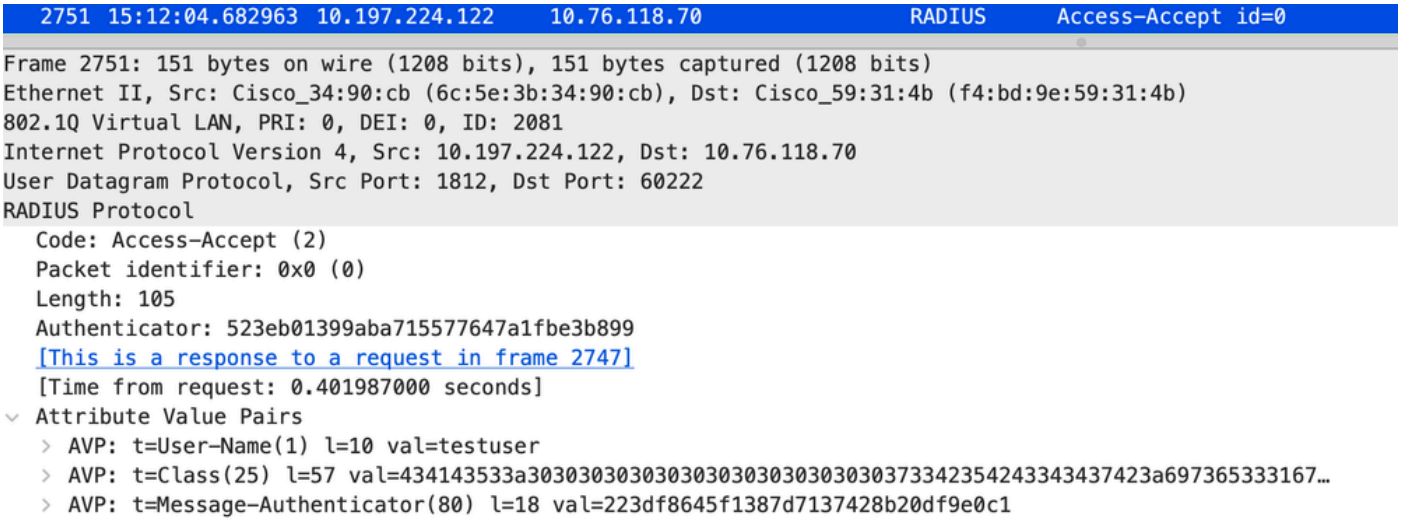
클라이언트가 포털 페이지에 HTTP GET 요청을 전송하고 인증을 성공적으로 완료합니다.

Radius 액세스 요청 패킷



액세스 요청 패킷

Radius 액세스 수락 패킷



액세스 수락 패킷

관련 기사

[Catalyst 9800에서 WLAN Anchor Mobility 기능 구성]

[AireOS 컨트롤러를 사용한 유선 게스트 액세스 컨피그레이션 예]

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.