Catalyst 9800에서 Anchor로 중앙 웹 인증 구성

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
다른 Catalyst 9800에 고정된 Catalyst 9800 구성
네트워크 다이어그램
두 9800에서 모두 AAA 구성
WLC에서 WLAN 구성
외부 WLC에 정책 프로필 및 정책 태그 생성
앵커 WLC에 정책 프로파일 생성
두 9800s 모두에서 ACL 컨피그레이션 리디렉션
ISE 구성
AireOS WLC에 고정된 Catalyst 9800 구성
Catalyst 9800 외부 컨피그레이션
앵커 AireOS WLC의 AAA 구성
AireOS WLC의 WLAN 구성
AireOS WLC에서 ACL 리디렉션
ISE 구성
AireOS WLC가 외부, Catalyst 9800이 앵커인 경우 구성의 차이점
다음을 확인합니다.
문제 해결
Catalyst 9800 문제 해결 정보
클라이언트 세부 정보
임베디드 패킷 캡처
RadioActive 추적
AireOS 문제 해결 정보
클라이언트 세부 정보
CLI에서 디버깅
참조

소개

이 문서에서는 AireOS 또는 다른 9800 WLC를 통해 목적지를 다루는 다른 WLC(Wireless LAN Controller)를 모빌리티 앵커로 가리키는 Catalyst 9800에서 CWA(Central Web Authentication)를 구성하고 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

9800 WLC, AireOS WLC 및 Cisco ISE에 대한 기본적인 이해가 있는 것이 좋습니다. CWA 앵커 컨피그레이션을 시작하기 전에 이미 두 WLC 간에 모빌리티 터널을 가동한 것으로 가정합니다. 이 컨피그레이션 예제의 범위를 벗어납니다. 도움이 필요한 경우 "Building Mobility Tunnels on Catalyst 9800 controllers" 문서를 참조하십시오.

사용되는 구성 요소

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

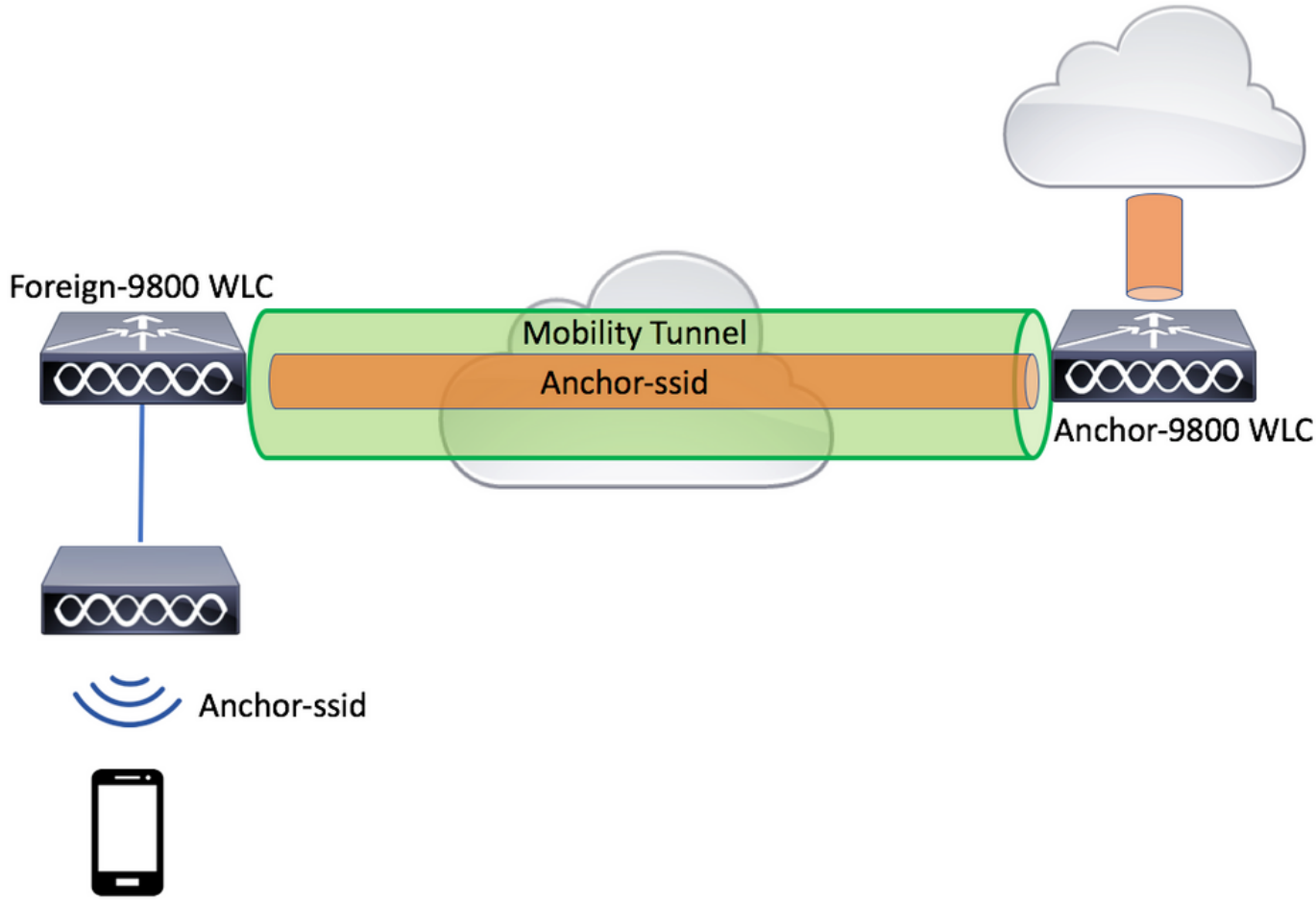
9800 17.2.1

8.5.164IRCM 이미지

ISE 2.4

다른 Catalyst 9800에 고정된 Catalyst 9800 구성

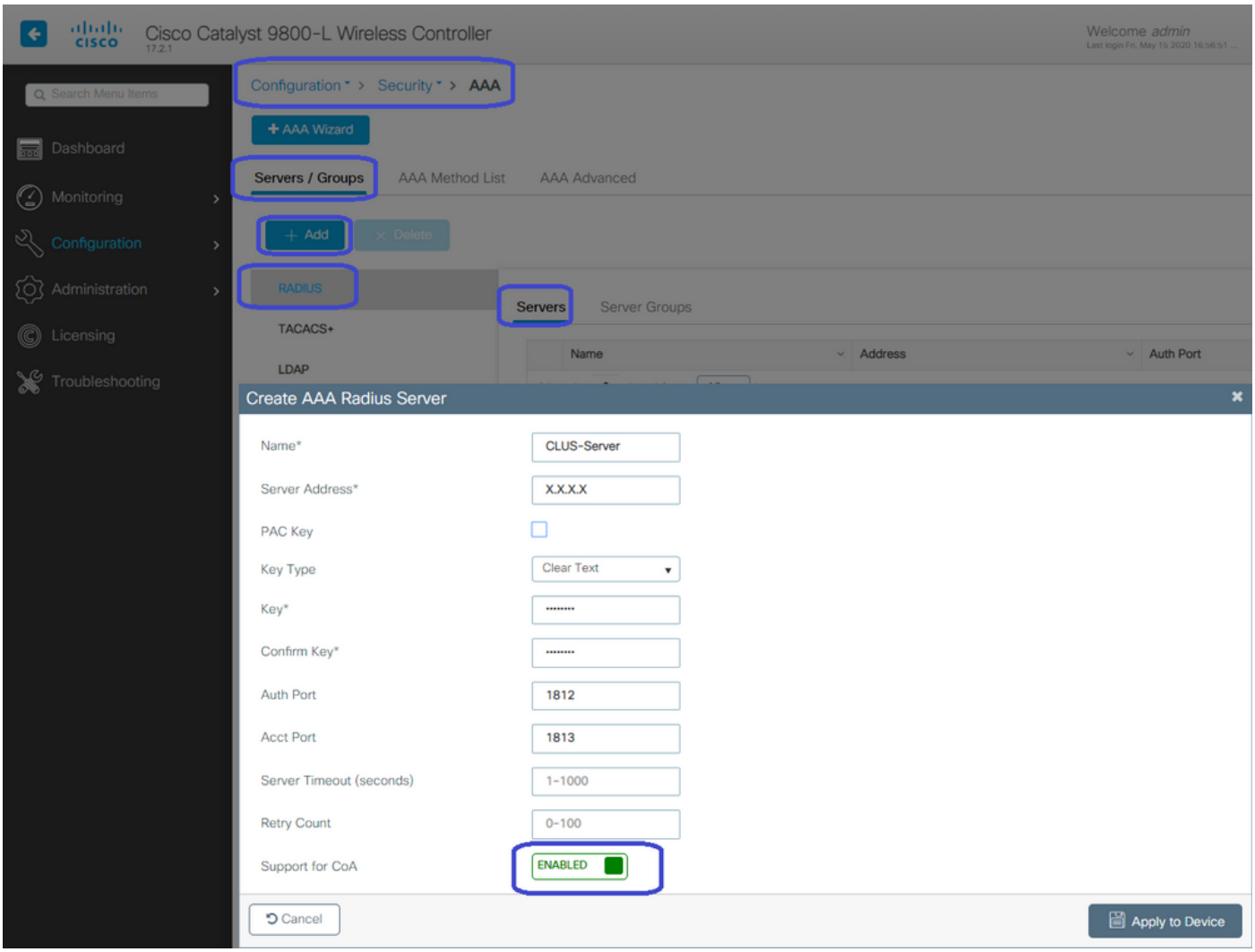
네트워크 다이어그램



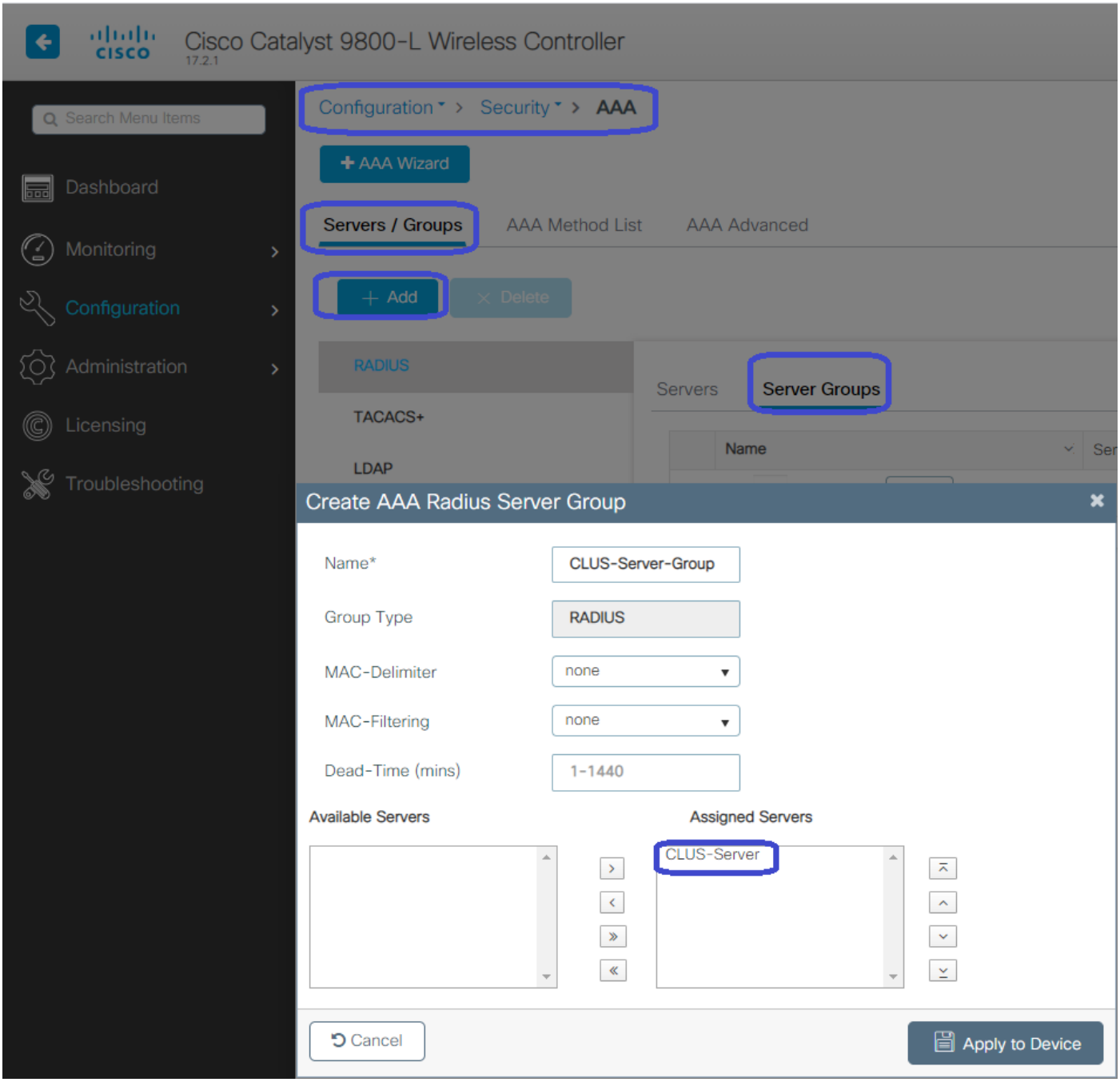
두 9800에서 모두 AAA 구성

앵커와 외부 모두에서 먼저 RADIUS 서버를 추가하고 CoA가 활성화되었는지 확인해야 합니다. 이 작업은 메뉴에서 수행할 수 있습니다.Configuration(구성)>Security(보안)>AAA>Servers/Groups(서버/그룹

)>Servers(서버)> Add(추가) 버튼을 클릭합니다.

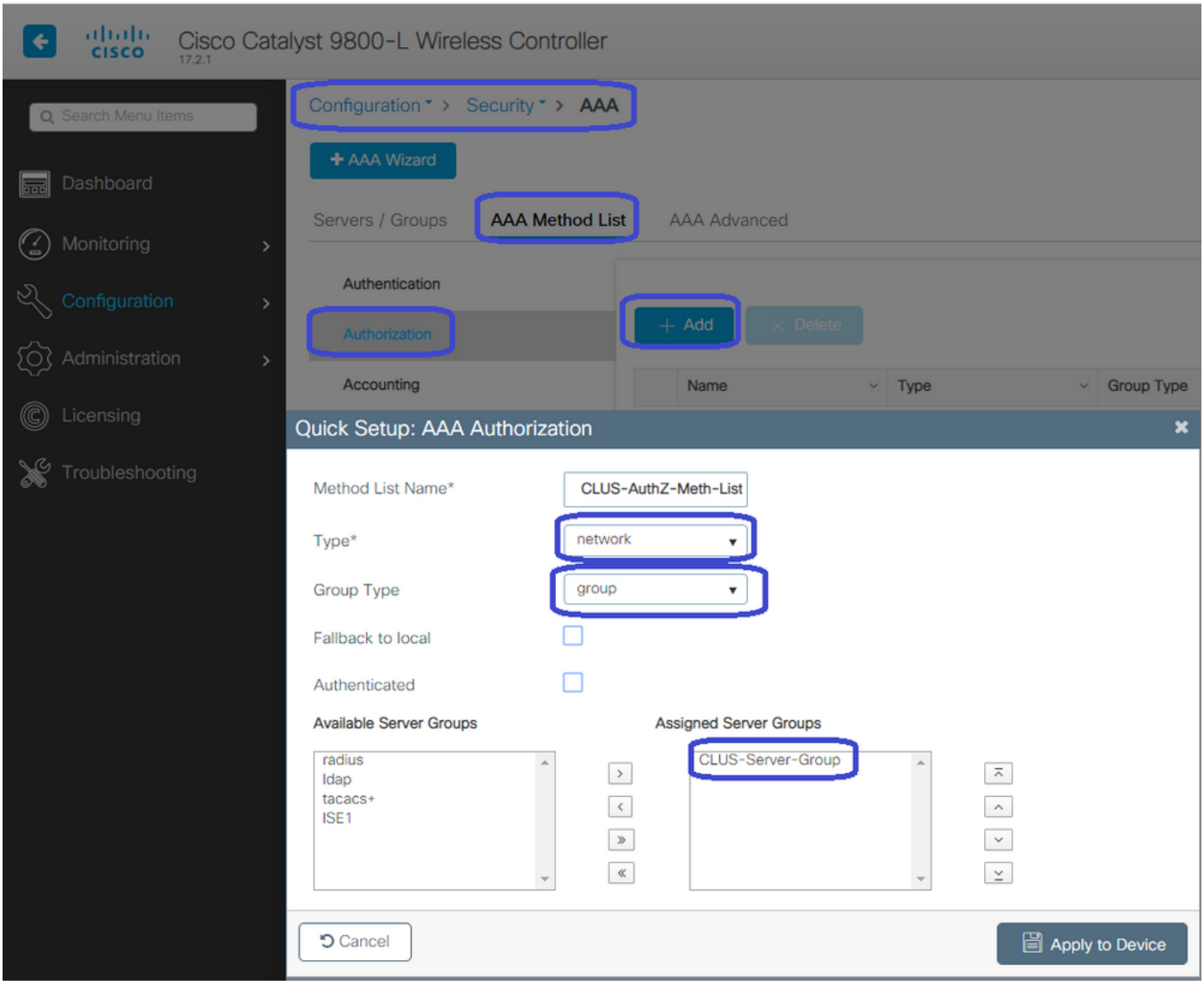


이제 서버 그룹을 생성하고 방금 구성한 서버를 해당 그룹에 배치해야 합니다. 이 작업은 Configuration(구성)>**Security(보안)>AAA>Servers/Groups(서버/그룹)>Server Groups(서버 그룹)>+Add(추가)에서 수행합니다**.

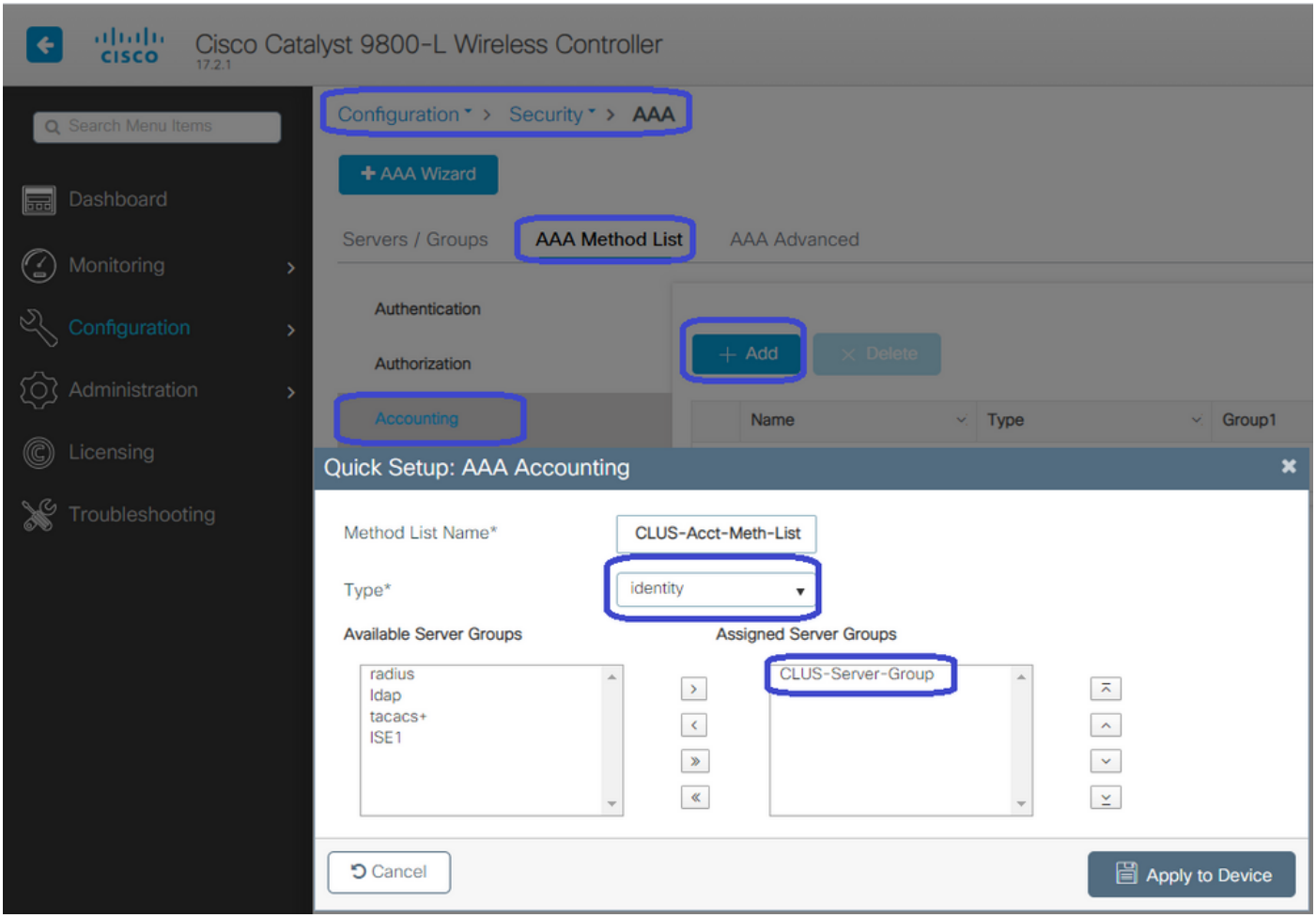


이제 **권한 부여** 방법 목록(CWA에는 인증 방법 목록이 필요하지 않음)을 생성합니다. 여기서 유형은 네트워크이고 그룹 유형은 그룹입니다. 이전 작업에서 이 메서드 목록에 서버 그룹을 추가합니다.

이 컨피그레이션은 Configuration(컨피그레이션)**>Security(보안)>AAA>Servers/AAA Method List(서버/AAA 메서드 목록)>Authorization(권한 부여)>+Add(추가)에서** 수행합니다.

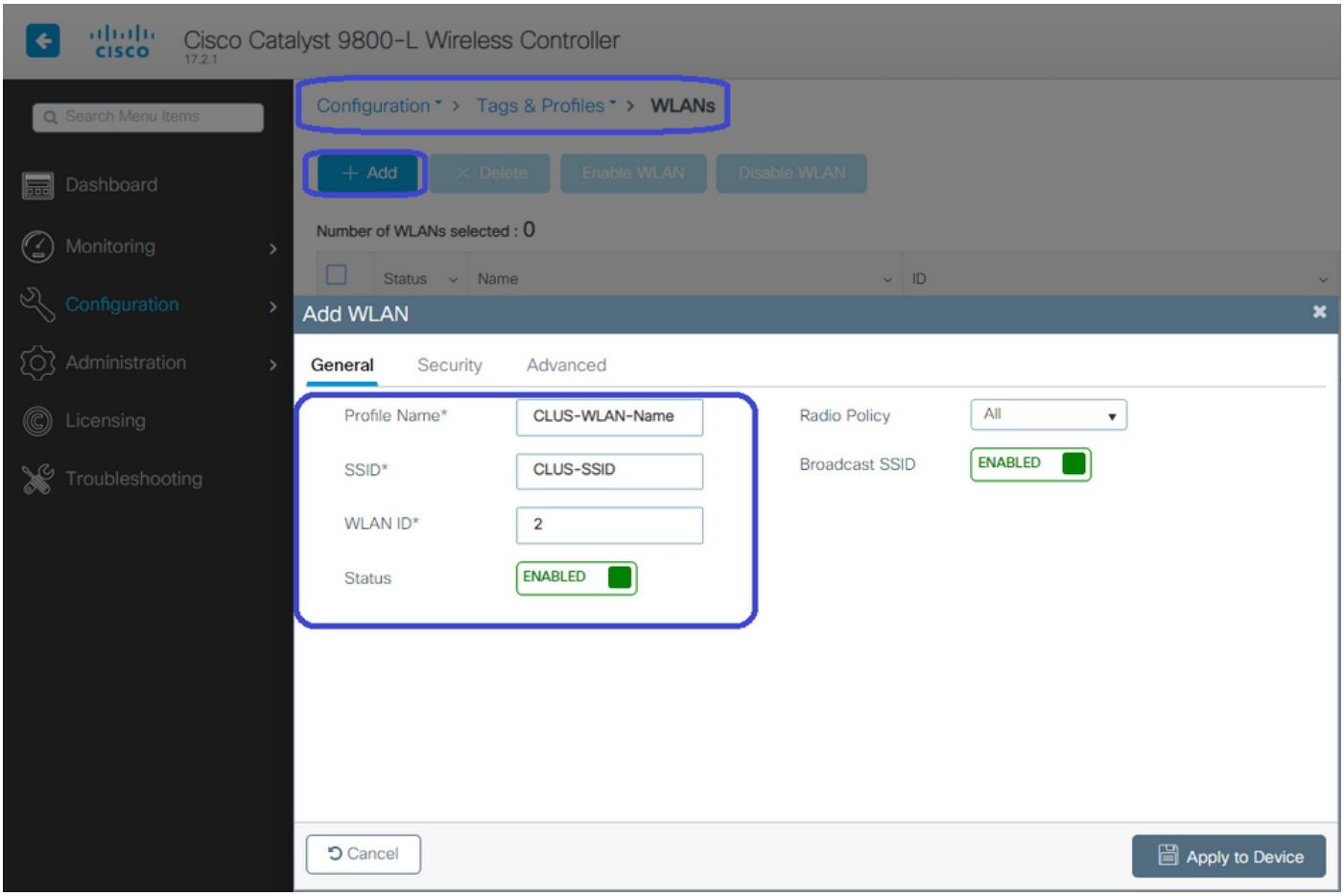


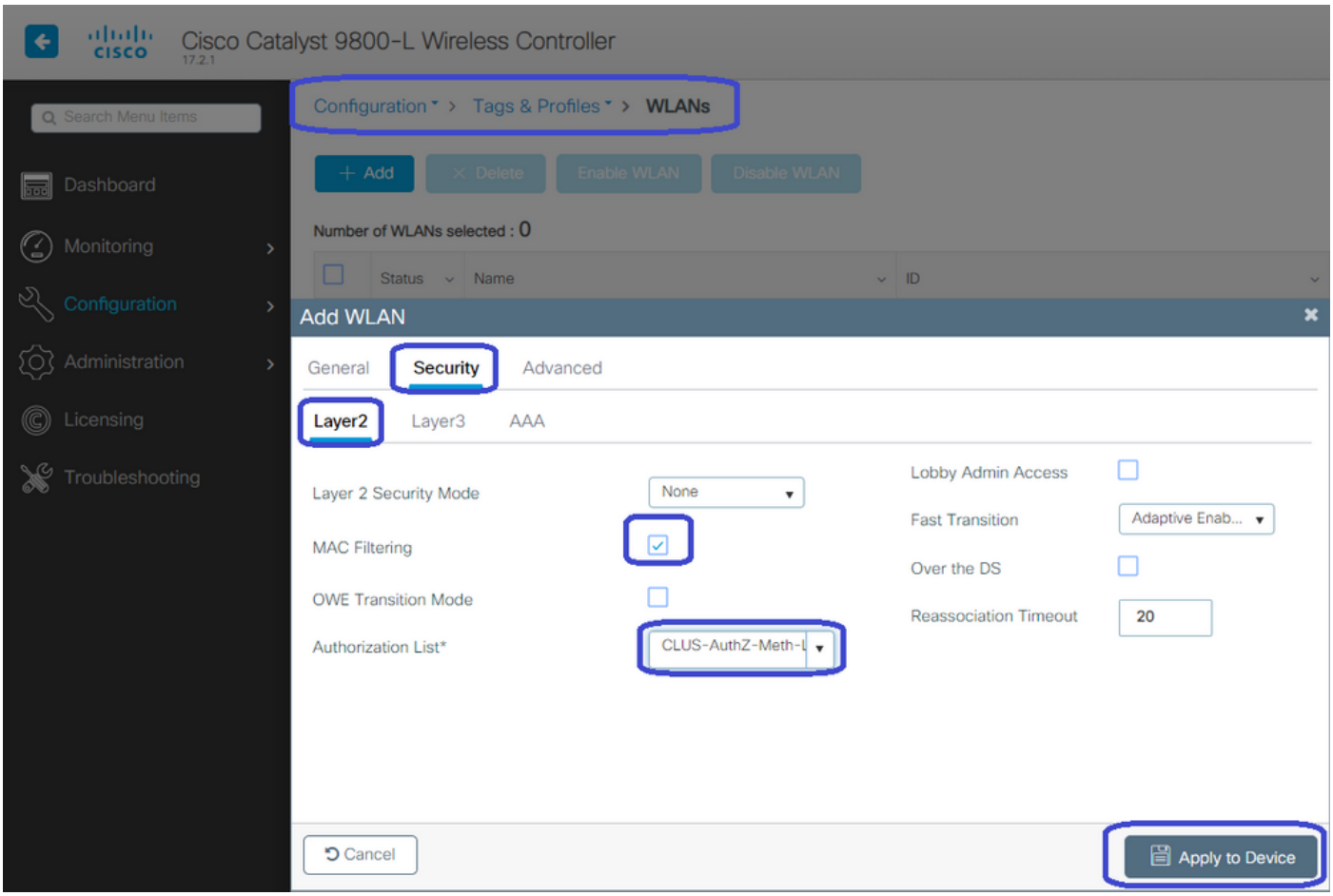
(선택 사항) 권한 부여 방법 목록과 동일한 서버 그룹을 사용하여 계정 관리 방법 목록을 생성합니다. 어카운팅 목록은 Configuration(컨피그레이션)>Security(**보안)>AAA>Servers/AAA Method List(서버/AAA 방법 목록)>Accounting(어카운팅)>+Add(추가)에서 생성할** 수 있습니다.



WLC에서 WLAN 구성

두 WLC에서 WLAN을 생성하고 구성합니다. WLAN이 두 모두에서 일치해야 합니다. 보안 유형은 mac 필터링이어야 하며 이전 단계의 권한 부여 방법 목록을 적용해야 합니다. 이 컨피그레이션은 Configuration(컨피그레이션)>Tags **& Profiles(태그 및 프로파일)>WLANs(WLAN)>+Add(추가)에서** 수행됩니다.



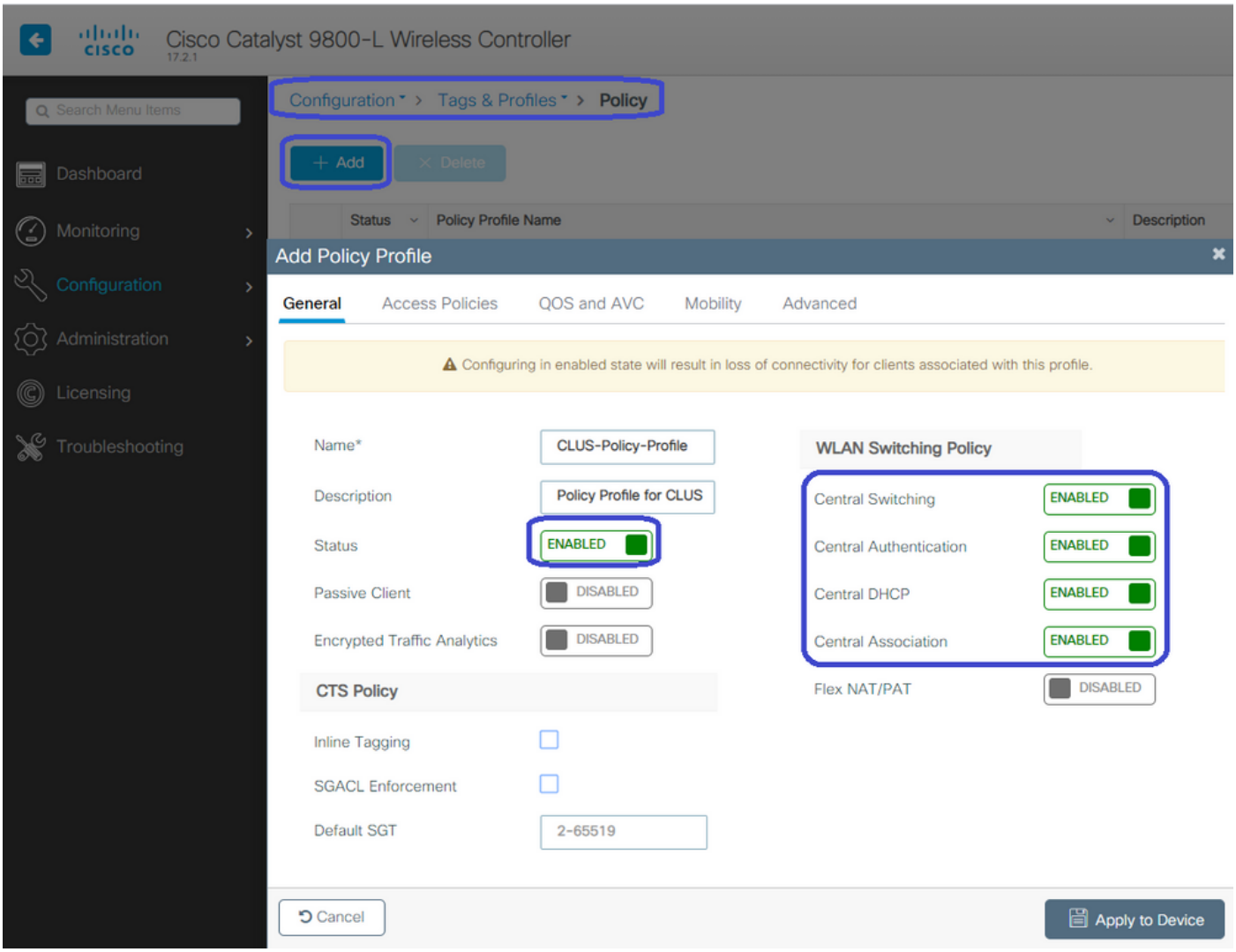


외부 WLC에 정책 프로필 및 정책 태그 생성

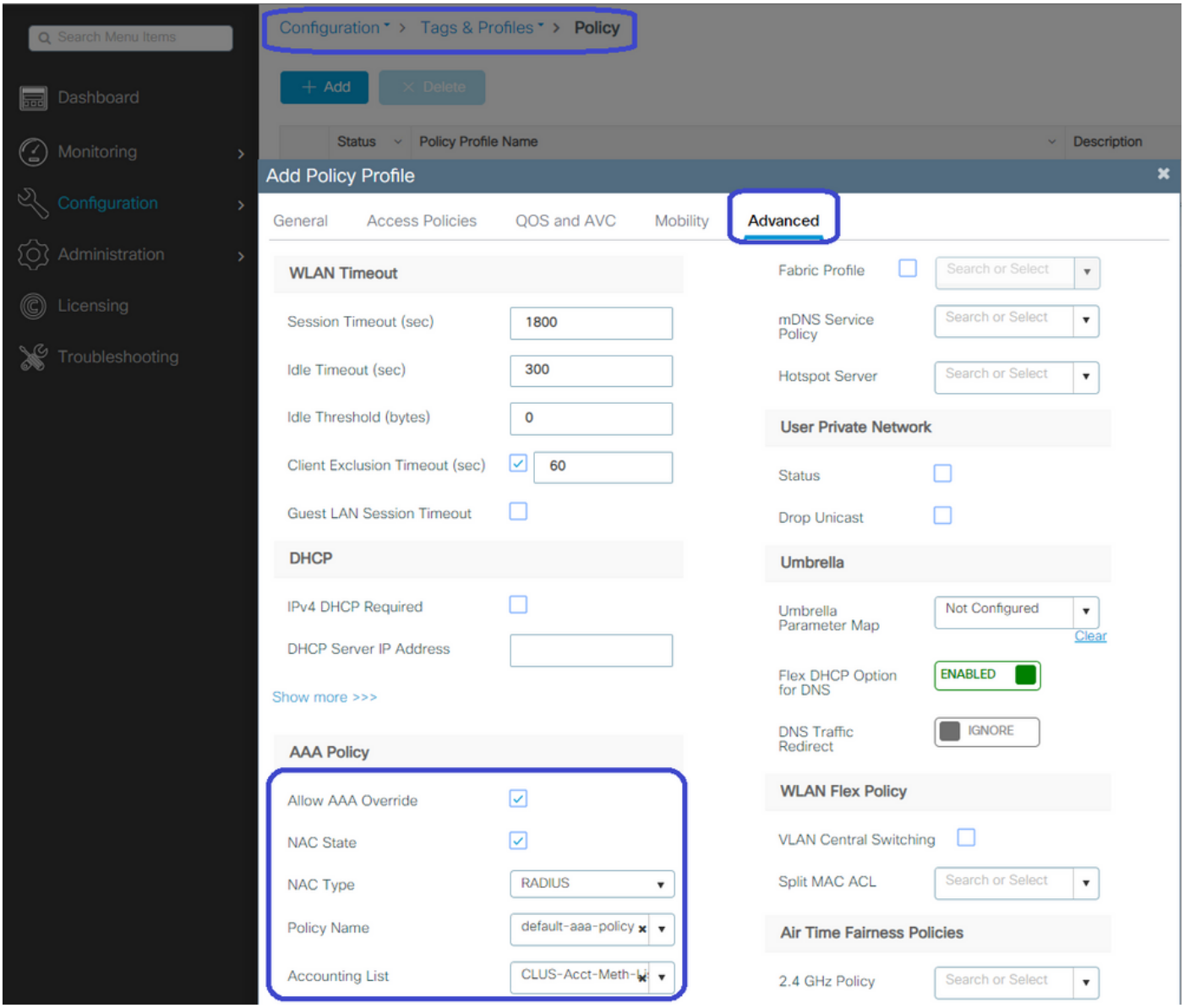
외부 WLC 웹 UI로 이동합니다.

정책 프로필을 생성하려면 Configuration(컨피그레이션)>Tags **& Profiles(태그 및 프로파일)>Policy(정책)>+Add(추가)로** 이동합니다.

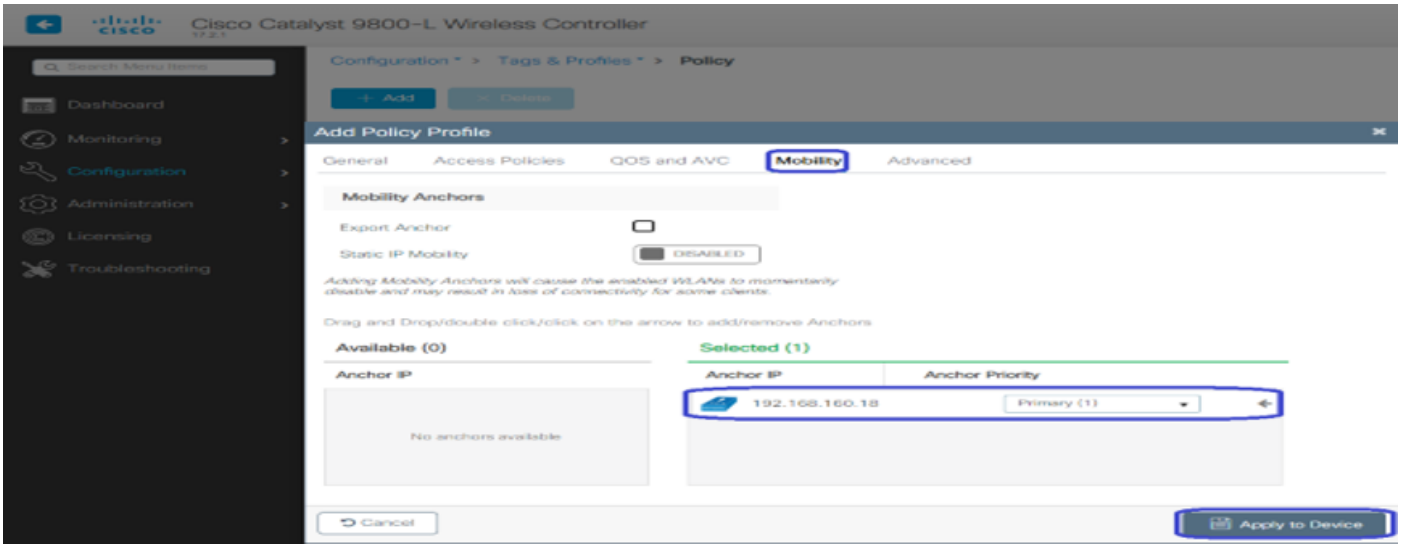
고정할 때는 중앙 스위칭을 사용해야 합니다.



"Advanced(고급)" 탭에서 CWA에 대해 AAA 재정의 및 RADIUS NAC가 필수입니다. 여기에서 어카운팅 방법 목록을 만들도록 선택한 경우에도 적용할 수 있습니다.

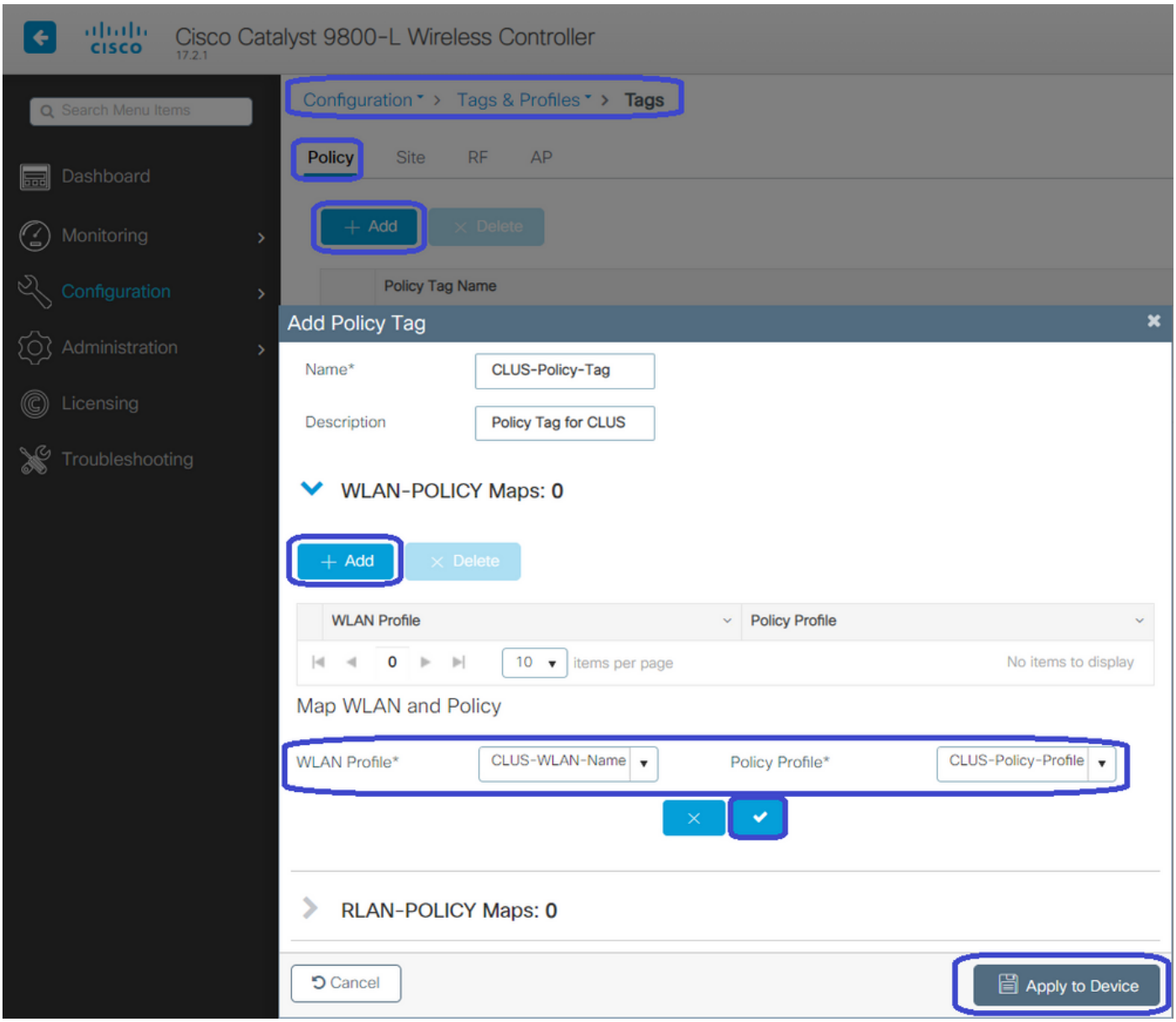


"Mobility(모빌리티)" 탭에서 "앵커 내보내기" 확인란을 선택하지 말고 앵커 목록에 앵커 WLC를 추가합니다. "Apply to Device"를 클릭해야 합니다. 다시 한 번 말씀드리지만, 두 컨트롤러 사이에 모빌리티 터널이 이미 설정되어 있다고 가정합니다

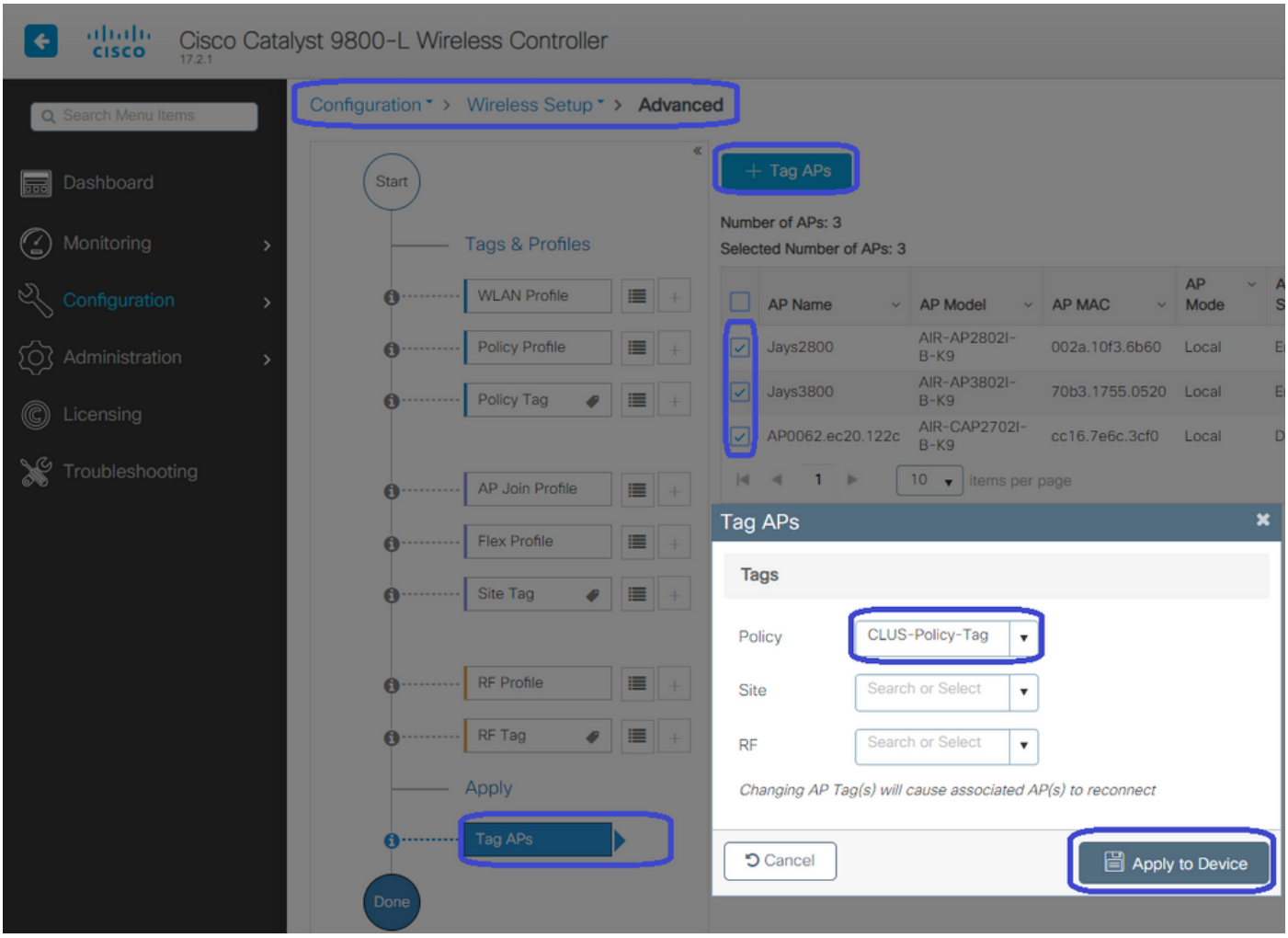


AP에서 이 정책 프로필을 사용하려면 정책 태그를 생성하여 사용하려는 AP에 적용해야 합니다.

정책 태그를 생성하려면 Configuration(구성)>Tags **& Profiles(태그 및 프로파일)>Tags(태그**)?Policy(정책)**>+Add(추가)로** 이동합니다.



여러 AP에 동시에 추가하려면 Configuration(컨피그레이션)>Wireless Setup(무선 설정)**>Advanced(고급)>Start Now(지금 시작)로 이동합니다**. "Tag APs" 옆의 글머리 기호를 클릭하고 선택한 AP에 태그를 추가합니다.

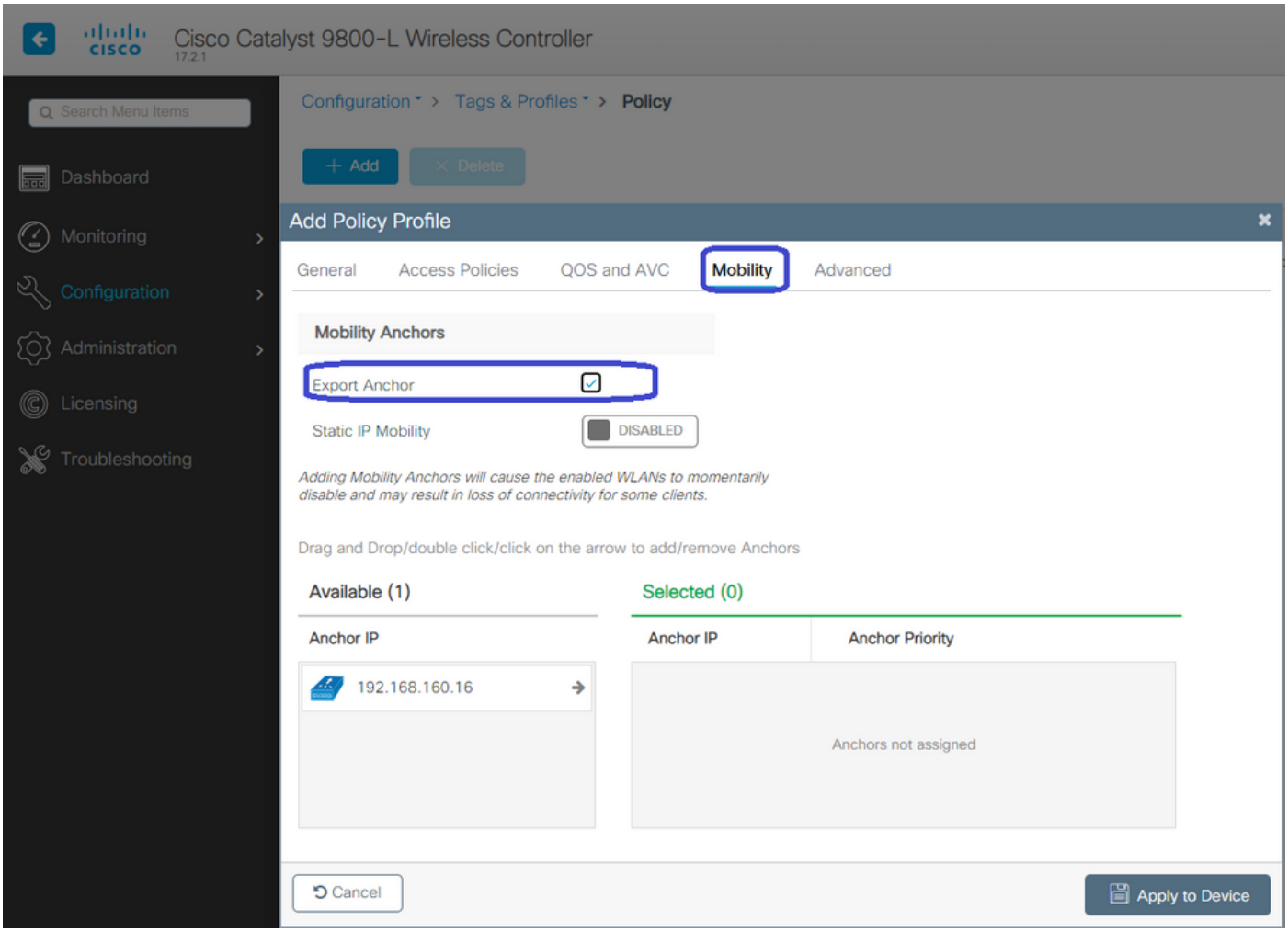


앵커 WLC에 정책 프로파일 생성

앵커 WLC 웹 UI로 이동합니다. 앵커 9800의 Configuration(구성)>Tags & Profiles(태그 및 프로파일)>Tags(태그)>Policy(**정책)>+Add(추가)에서 정책 프로파일을 추가합니다**. 모빌리티 탭 및 어카운팅 목록을 제외하고 이 항목이 외주에서 만든 정책 프로필과 일치하는지 확인합니다.

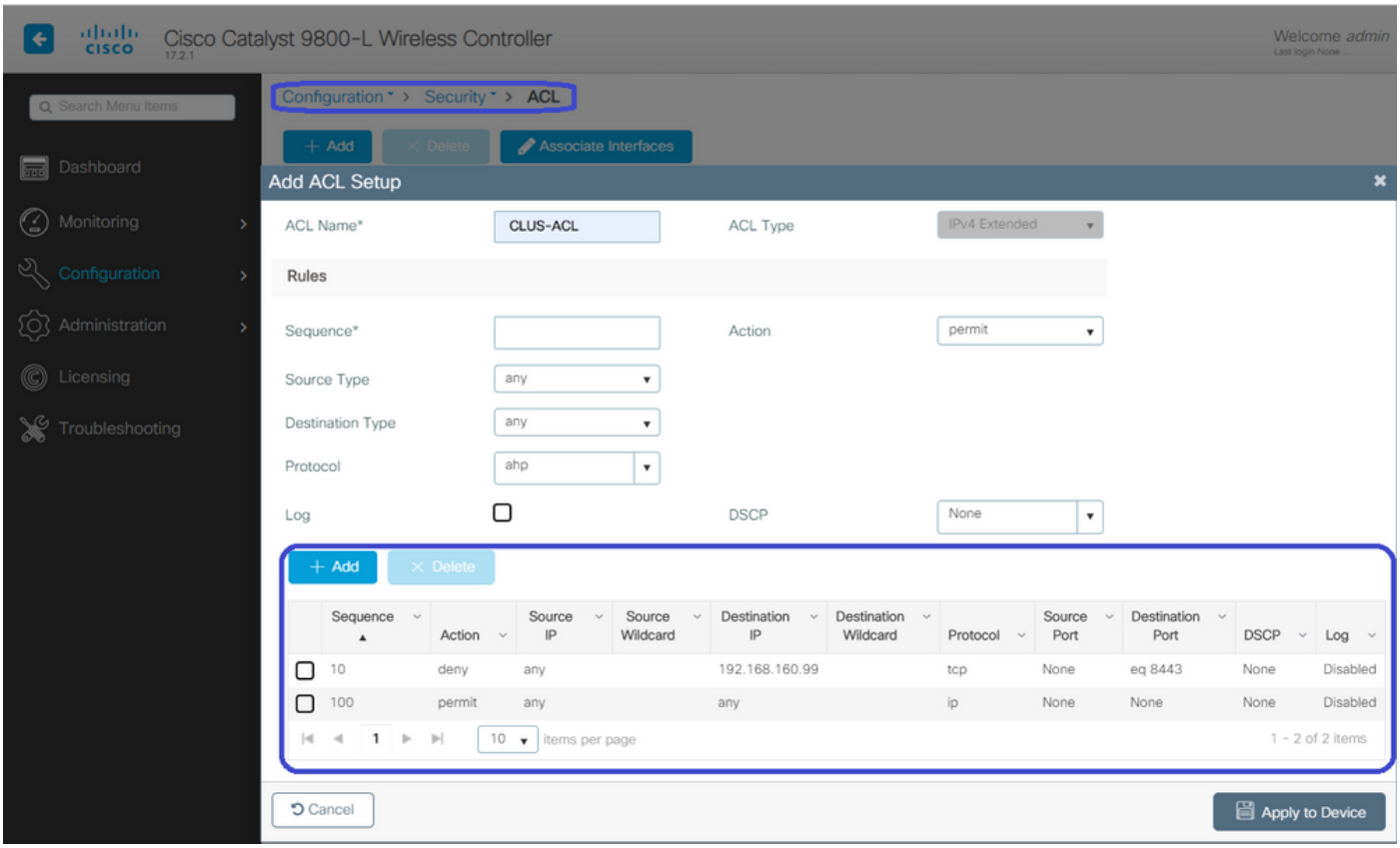
여기서 앵커를 추가하지 않고 "앵커 내보내기" 확인란을 선택합니다. 여기에 계정 목록을 추가하지 마십시오. 다시 한 번 말씀드리지만, 두 컨트롤러 사이에 모빌리티 터널이 이미 설정되어 있다고 가정합니다

참고: 정책 태그의 WLAN에 이 프로파일을 연결할 이유는 없습니다. 이렇게 하면 문제가 발생합니다. 이 WLC의 AP에 동일한 WLAN을 사용하려면 다른 정책 프로파일을 생성합니다.



두 9800s 모두에서 ACL 컨피그레이션 리디렉션

그런 다음 두 9800에서 리디렉션 ACL 컨피그레이션을 생성해야 합니다. 트래픽에 ACL을 적용하는 앵커 WLC가 될 것이므로 외부 항목은 중요하지 않습니다. 유일한 요구 사항은 그것이 그곳에 있고 어떤 입구를 가지고 있다는 것입니다. 앵커의 항목은 포트 8443에서 ISE에 대한 액세스를 "거부"하고 다른 모든 것을 "허용"해야 합니다. 이 ACL은 클라이언트에서 "수신"하는 트래픽에만 적용되므로 반환 트래픽에 대한 규칙이 필요하지 않습니다. DHCP 및 DNS는 ACL의 항목 없이 통과됩니다.

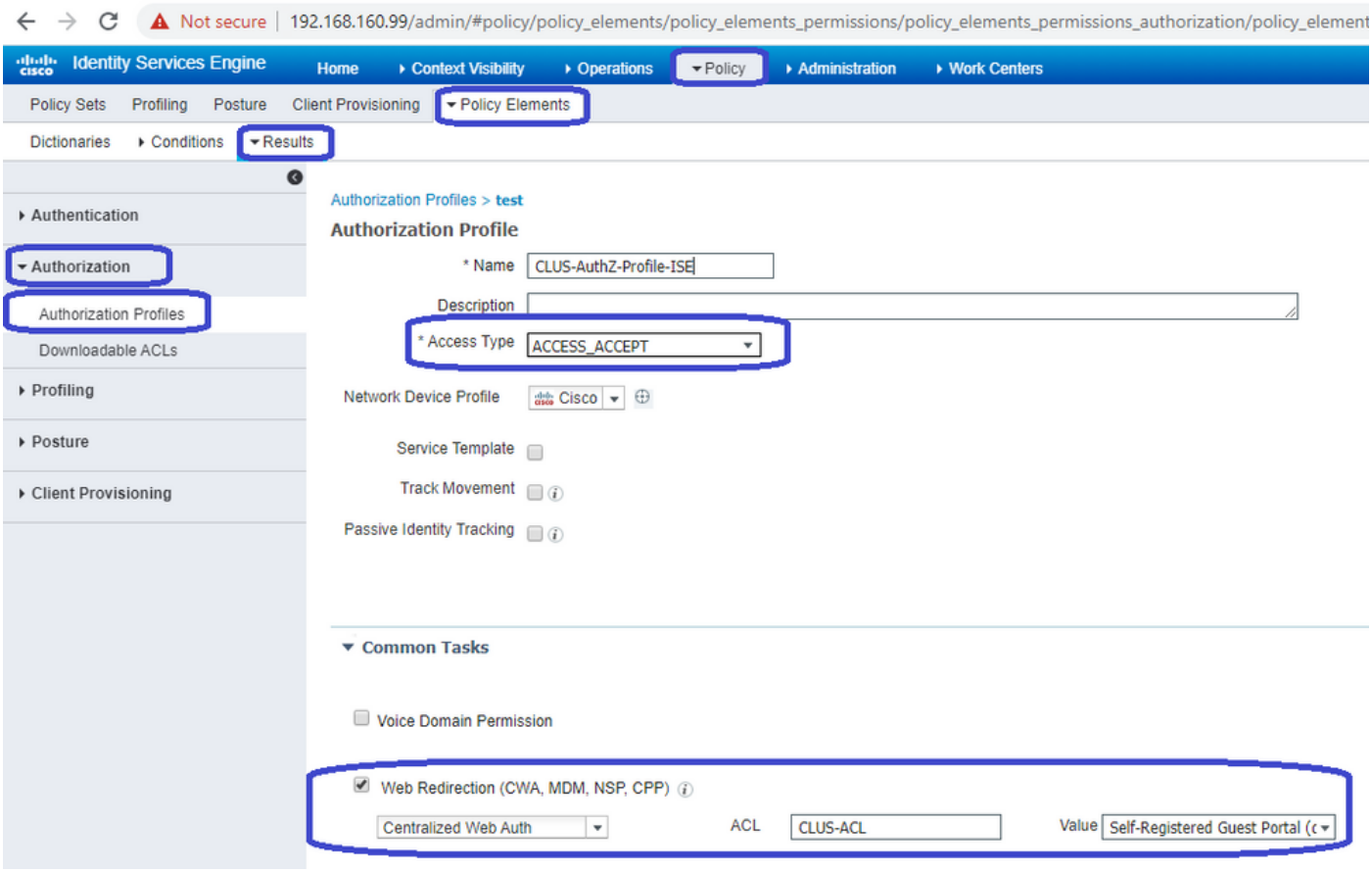


ISE 구성

마지막 단계는 CWA용 ISE를 구성하는 것입니다. 여기에는 수많은 옵션이 있지만 이 예에서는 기본 사항을 고수하며 기본 셀프 등록 게스트 포털을 사용합니다.

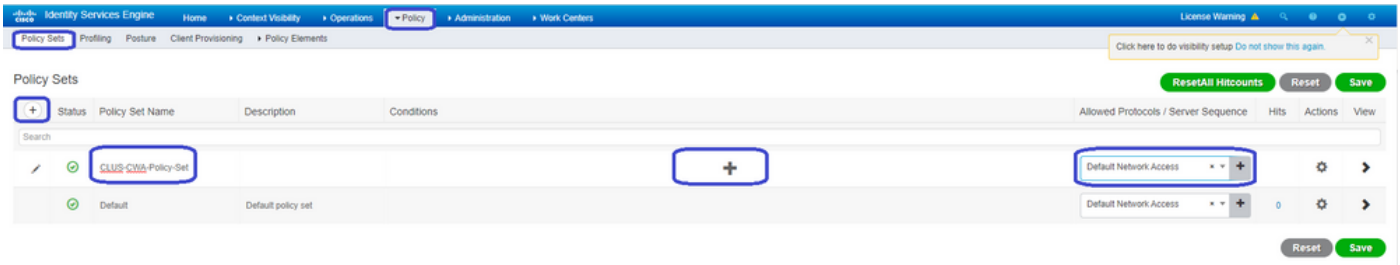
ISE에서 권한 부여 프로파일, 인증 정책 및 권한 부여 프로파일을 사용하는 권한 부여 정책을 가진 정책 집합을 생성하고, 네트워크 디바이스로 ISE에 9800(foreign)을 추가하고, 네트워크에 로그인할 사용자 이름 및 비밀번호를 생성해야 합니다.

권한 부여 프로파일을 생성하려면 Policy(정책)**>Policy Elements(정책 요소)>Authorization(권한 부여)>Results(결과)>Authorization Profiles(권한 부여 프로파일)>**로 이동한 다음 Add(추가)를 **클릭합니다**. 반환된 액세스 유형이 "access_accept"인지 확인한 다음 다시 전송할 AVP(attribute-value 쌍)를 설정합니다. CWA의 경우 리디렉션 ACL 및 리디렉션 URL은 필수 사항이지만 VLAN ID 및 세션 시간 초과 등의 항목을 다시 전송할 수도 있습니다. ACL 이름은 외래 및 앵커 9800에서 리디렉션 ACL의 이름과 일치해야 합니다.

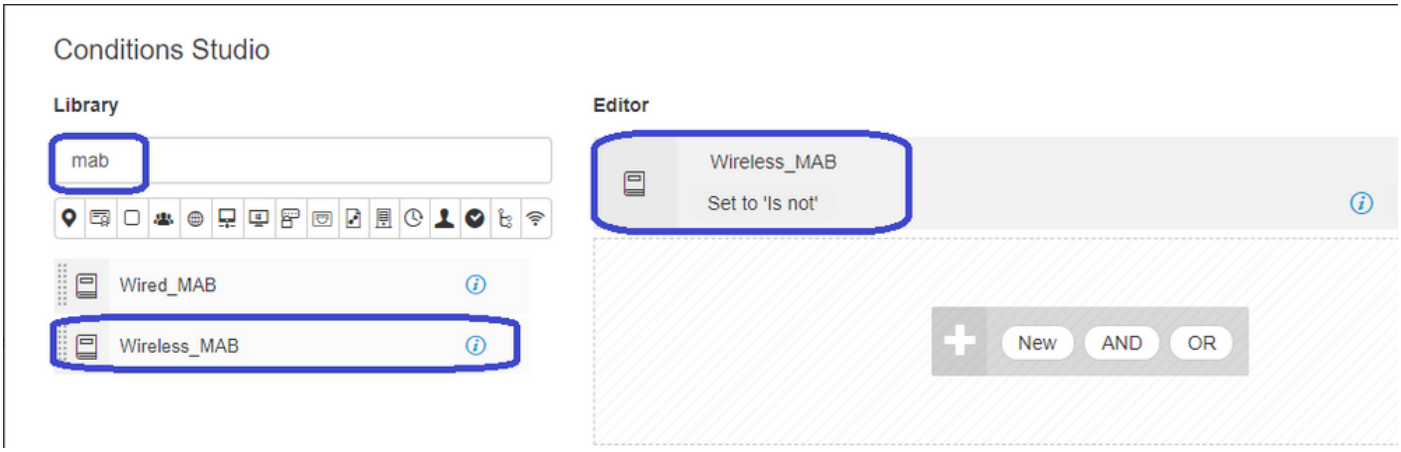


그런 다음 CWA를 통과하는 클라이언트에 방금 생성한 권한 부여 프로파일을 적용하는 방법을 구성해야 합니다. 이를 위해, 한 가지 방법은 MAB를 사용할 때 인증을 우회하는 정책 세트를 만들고, 호출된 스테이션 ID에서 전송된 SSID를 사용할 때 권한 부여 프로파일을 적용하는 것입니다. 다시 한 번 말하지만, 이것을 성취하는 방법에는 많은 것들이 있습니다. 그래서 좀 더 구체적이거나 더 안전한 어떤 것이 필요하다면, 그렇게 하세요. 이것이 바로 가장 간단한 방법입니다.

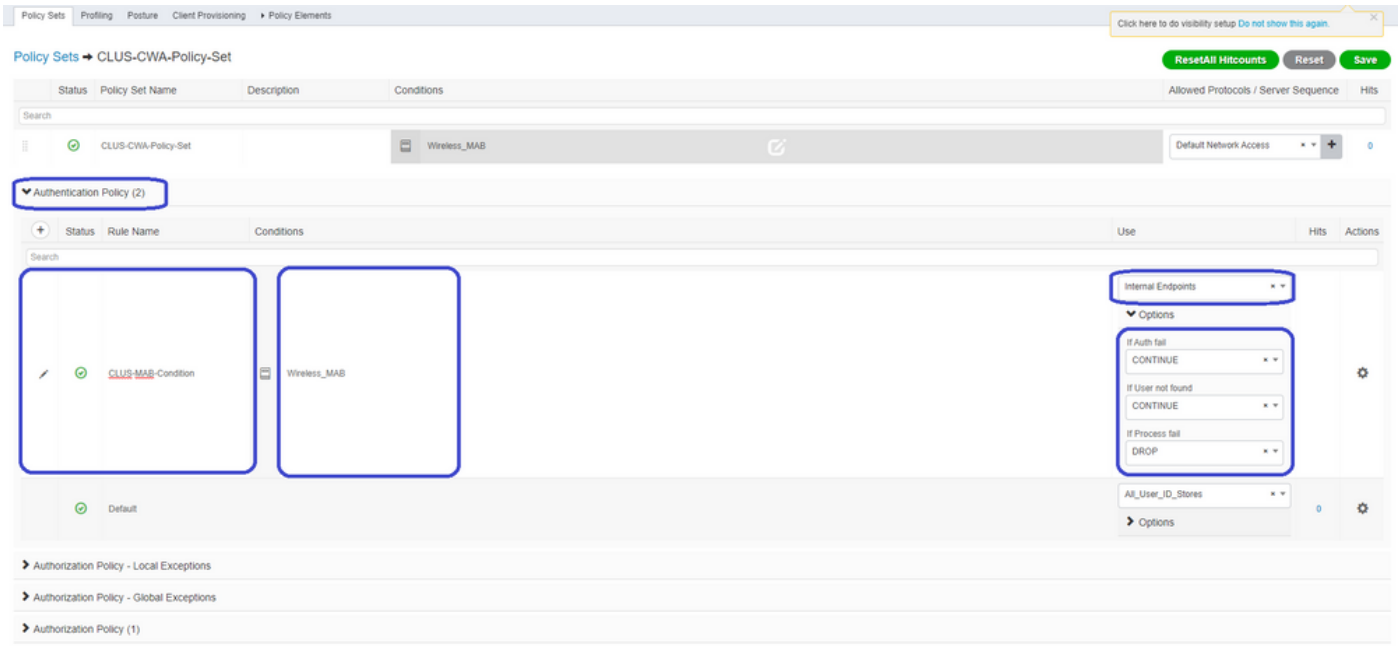
정책 집합을 생성하려면 **Policy(정책)>Policy Sets(정책 집합)**로 이동하여 화면 왼쪽에 있는 + 버튼을 누릅니다. 새 정책 세트의 이름을 지정하고 MAB에 대해 "Process Host Lookup(프로세스 호스트 조회)"을 허용하는 허용된 프로토콜 목록 또는 "기본 네트워크 액세스"로 설정되어 있는지 확인합니다(허용되는 프로토콜 목록을 확인하려면 정책>정책 요소>결과>인증>허용되는 프로토콜)로 이동합니다. 이제 생성한 새 정책 세트의 중간에 + 기호를 누릅니다.



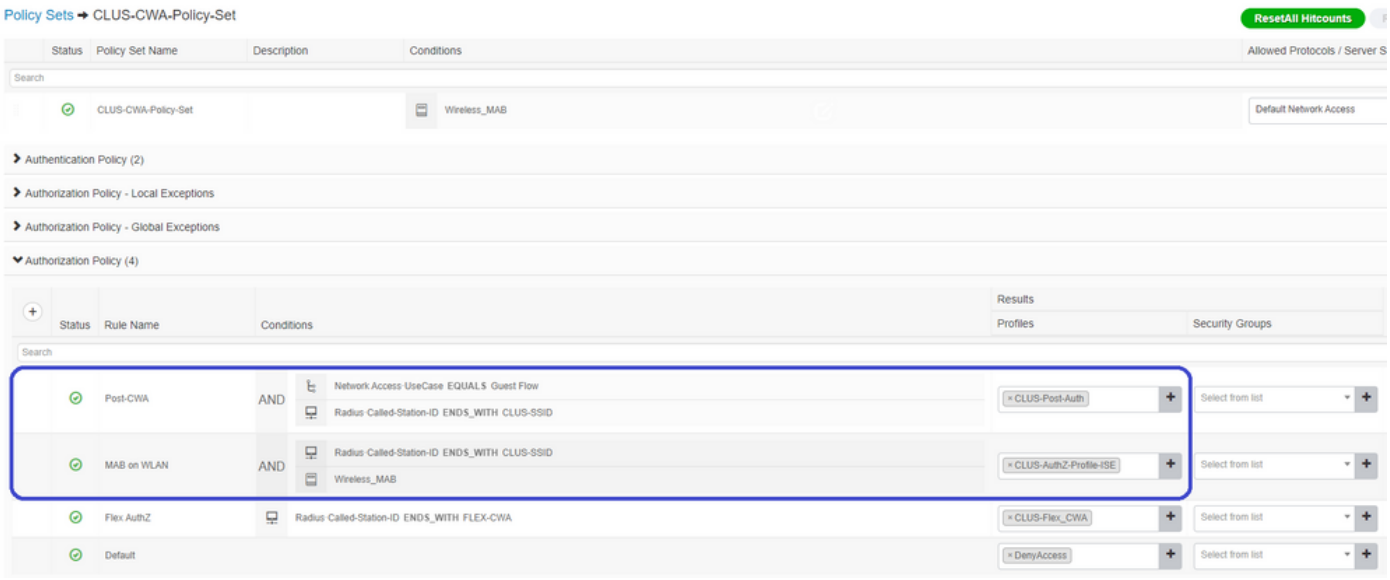
MAB가 ISE에서 사용될 때마다 이 정책 집합에서 실행됩니다. 나중에 사용 중인 WLAN에 따라 다른 결과를 적용할 수 있도록 발신된 스테이션 ID에서 일치하는 권한 부여 정책을 만들 수 있습니다. 이 프로세스는 매칭할 수 있는 많은 것들을 통해 매우 사용자 지정이 가능합니다.



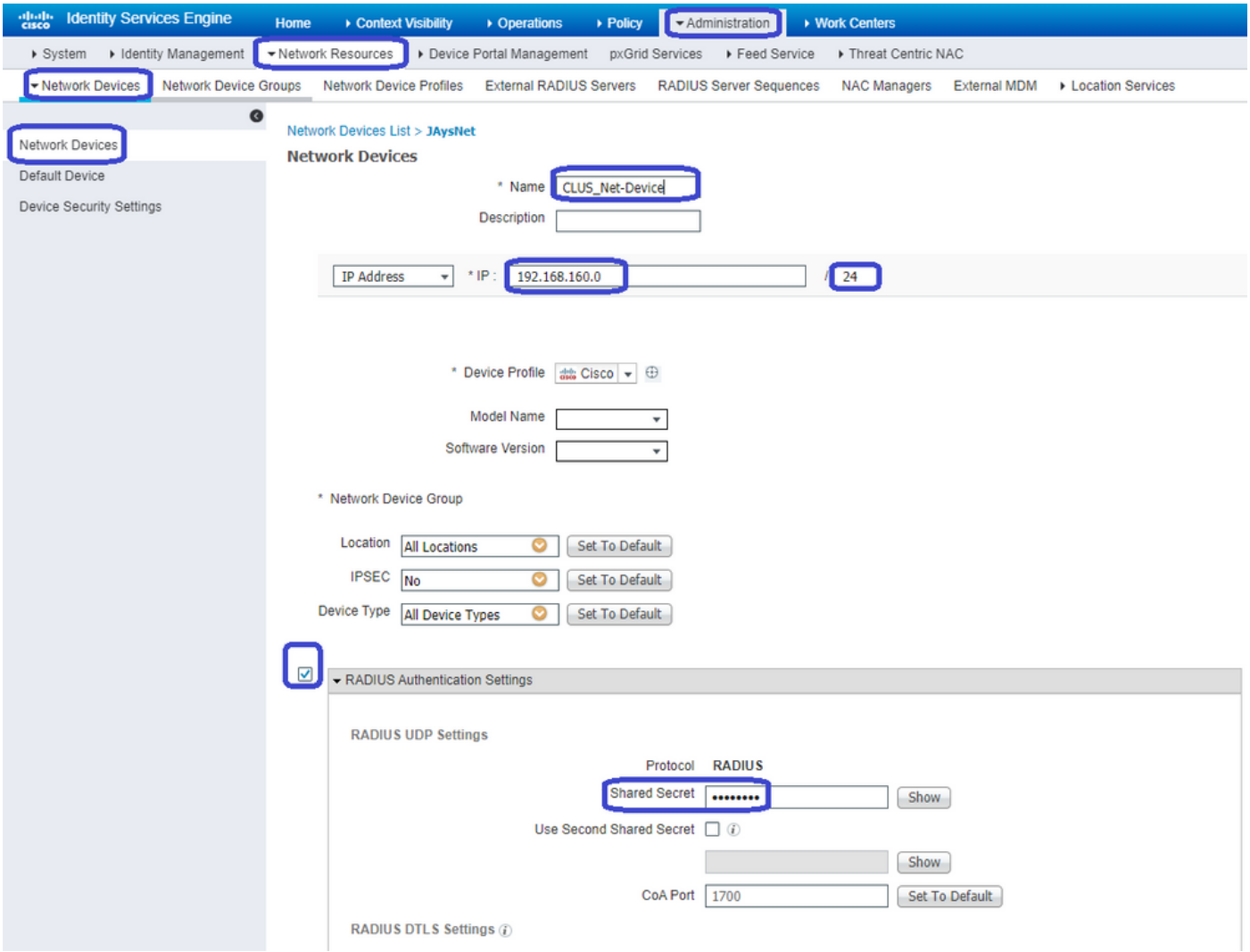
정책 집합 내에서 정책을 생성합니다. 인증 정책은 MAB에서 다시 일치할 수 있지만 "내부 엔드포인트"를 사용하도록 ID 저장소를 변경해야 하며 인증 실패 및 사용자를 찾을 수 없는 경우 계속 옵션을 변경해야 합니다.



인증 정책이 설정되면 권한 부여 정책에서 두 개의 규칙을 생성해야 합니다. 이 정책은 ACL과 같이 읽으므로 주문에 사후 인증 규칙이 맨 위에 있고 맨 아래에 사전 인증 규칙이 있어야 합니다. 사후 인증 규칙은 이미 게스트 플로우를 통과한 사용자와 일치합니다. 이것은 그들이 이미 로그인했다면 그 규칙을 무시하고 거기서 멈춘다는 것을 말하는 것입니다. 로그인하지 않은 경우 목록 아래로 계속 이동하여 사전 인증 규칙을 입력하여 리디렉션을 가져옵니다.권한 부여 정책 규칙을 SSID로 끝나는 호출된 스테이션 ID와 일치시켜 그렇게 구성된 WLAN에 대해서만 적중시키는 것이 좋습니다.

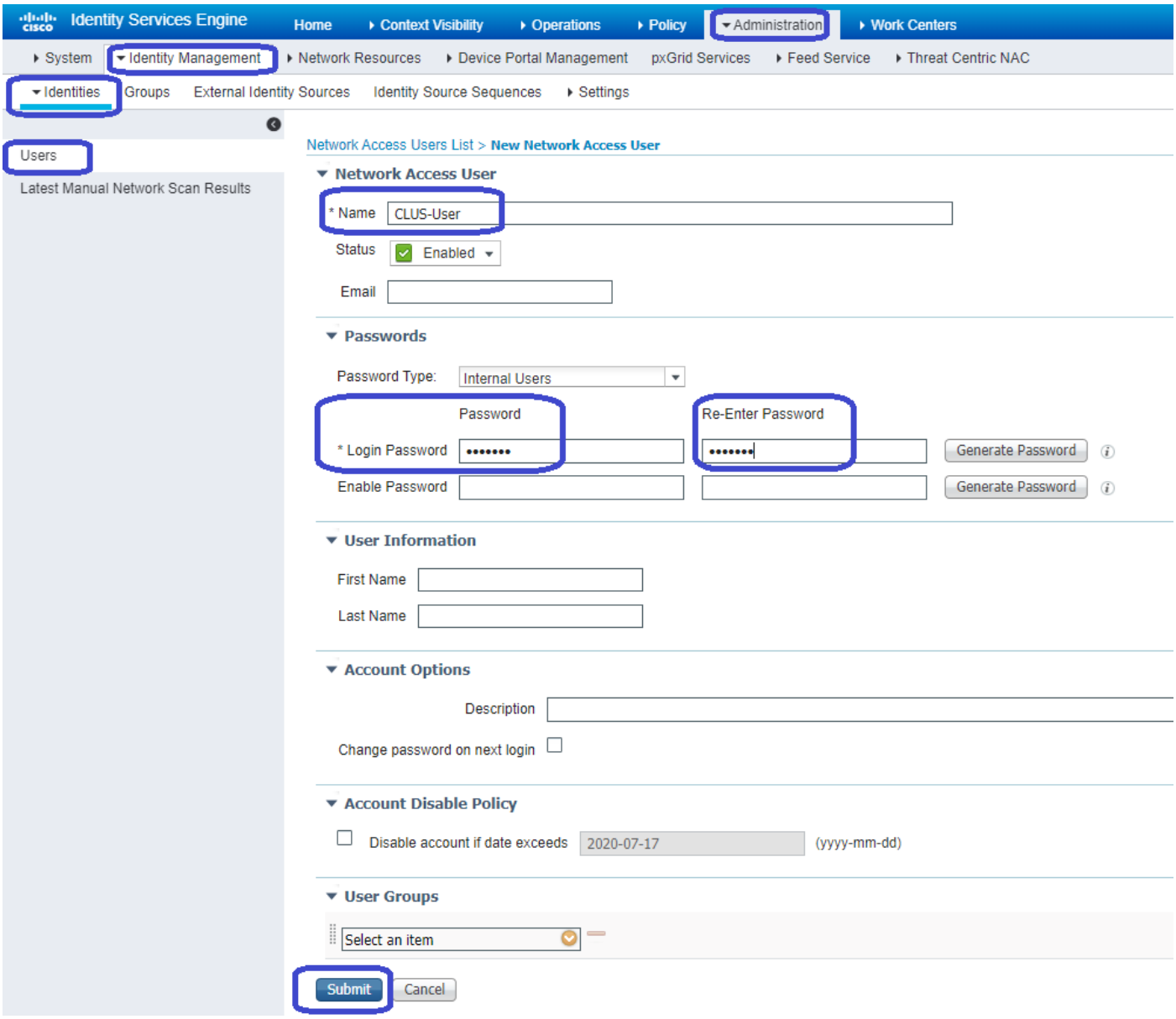


이제 정책 집합이 구성되었으므로 ISE가 인증자로 신뢰하도록 하려면 9800(foreign)에 대해 ISE에 알려야 합니다. 이 작업은 Admin(관리)**>Network Resources(네트워크 리소스)>Network Device(네트워크 디바이스)>+에서** 수행할 수 있습니다. 이름을 지정하고 IP 주소(또는 전체 관리 서브넷)를 설정하고 RADIUS를 활성화하고 공유 암호를 설정해야 합니다. ISE의 공유 암호가 9800의 공유 암호와 일치해야 합니다. 그렇지 않으면 이 프로세스가 실패합니다. 컨피그레이션이 추가된 후 전송 버튼을 눌러 저장합니다.

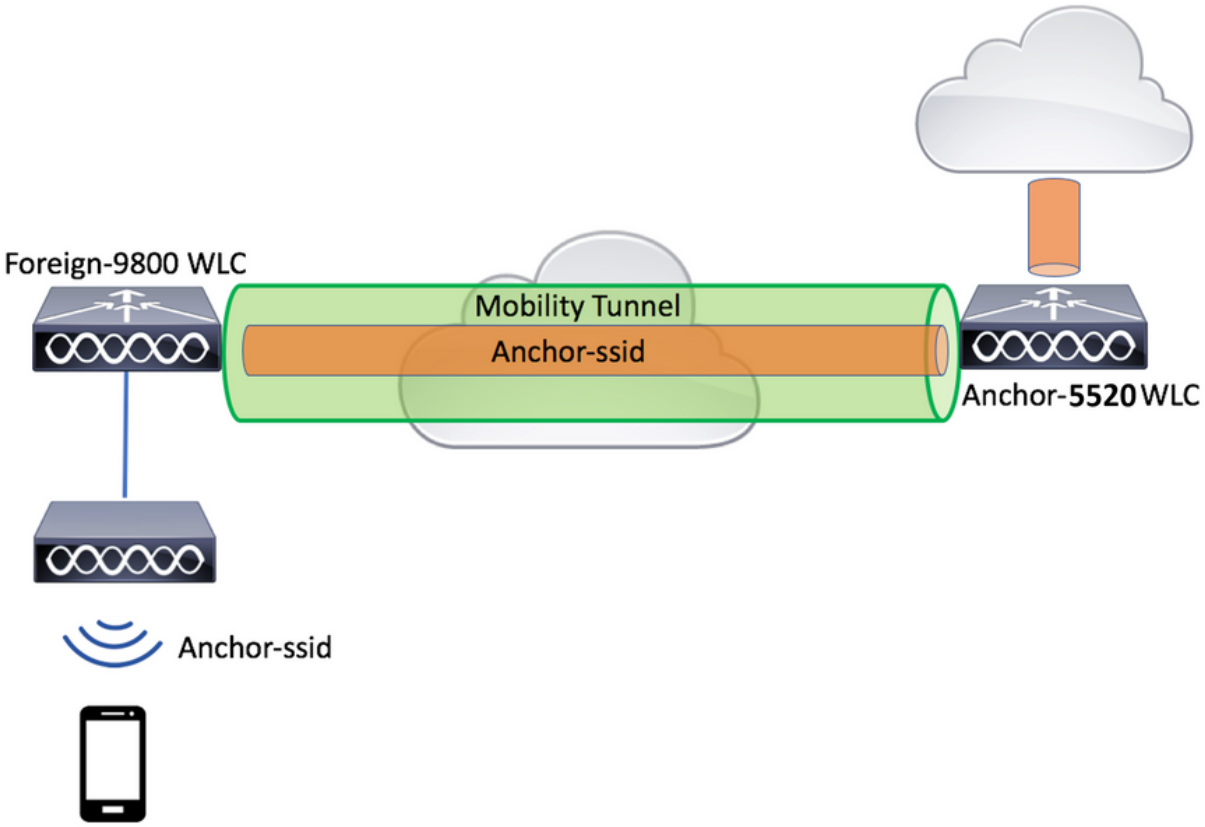


마지막으로, 클라이언트가 네트워크에 액세스할 수 있어야 하는지 확인하기 위해 로그인 페이지에 입력할 사용자 이름과 비밀번호를 추가해야 합니다. 이 작업은 **Admin(관리)>Identity**

Management(ID 관리)>Identity(ID)>Users(사용자)>+Add(추가)에서 수행되며 추가한 후 제출을 누르십시오. ISE의 다른 모든 것과 마찬가지로, 이것은 사용자 지정이 가능하며 로컬에 저장된 사용자가 아니어도 되지만 다시 말해 가장 쉬운 컨피그레이션입니다.



AireOS WLC에 고정된 Catalyst 9800 구성

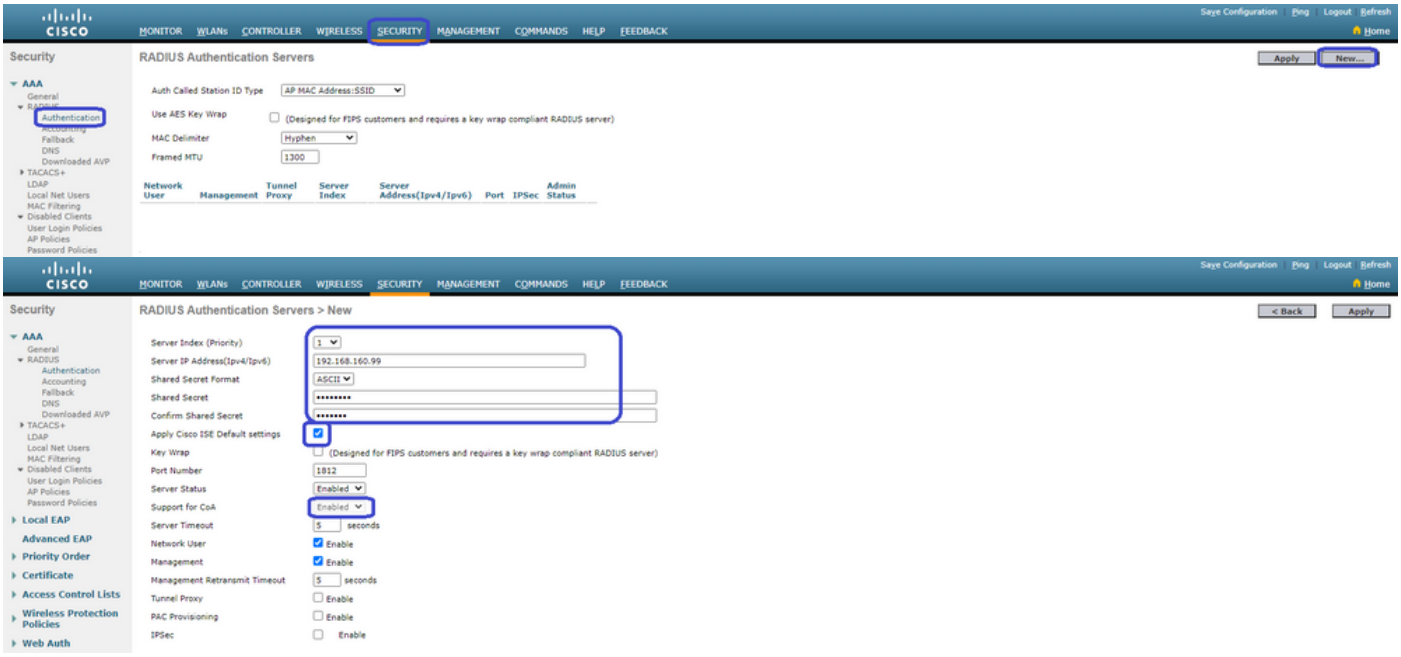


Catalyst 9800 외부 컨피그레이션

앞서 설명한 것과 동일한 단계를 수행하여 "*Create the policy profile on the anchor WLC(앵커 WLC에서 정책 프로필 생성)*" 섹션을 건너뜁니다.

앵커 AireOS WLC의 AAA 구성

Security(보안)>AAA>RADIUS>**Authentication(인증)>New(새로 만들기)**로 이동하여 WLC에 서버**를 추가합니다**. 서버 IP 주소, 공유 암호 및 CoA 지원을 추가합니다.

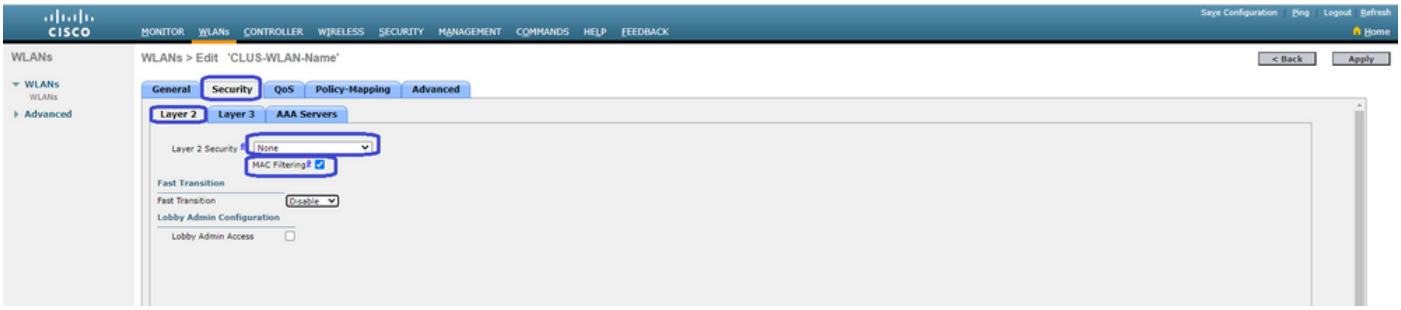


AireOS WLC의 WLAN 구성

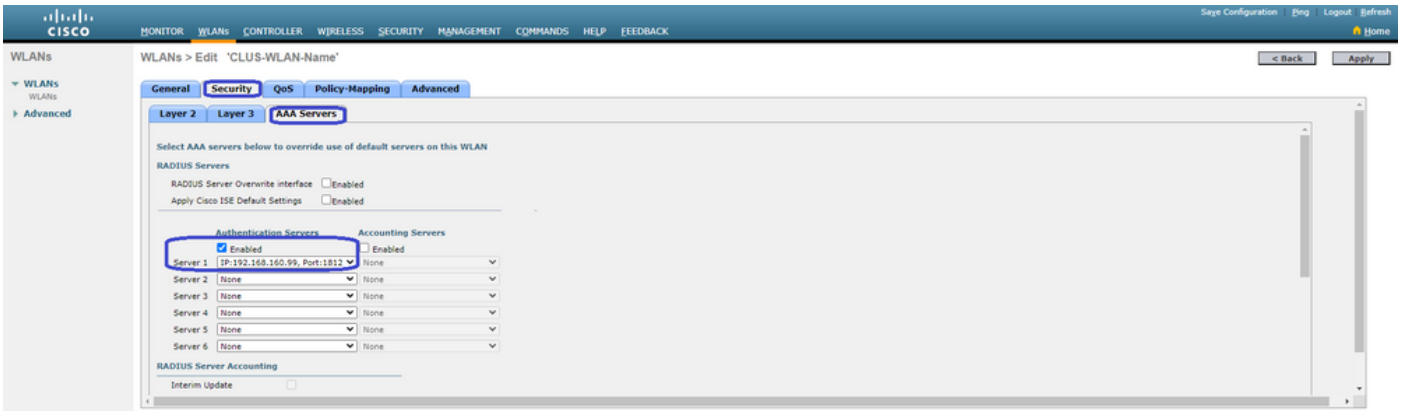
WLAN을 생성하려면 WLANs>Create **New>Go로 이동합니다**.

프로파일 이름, WLAN ID 및 SSID를 구성한 다음 "Apply(적용)"를 누릅니다.

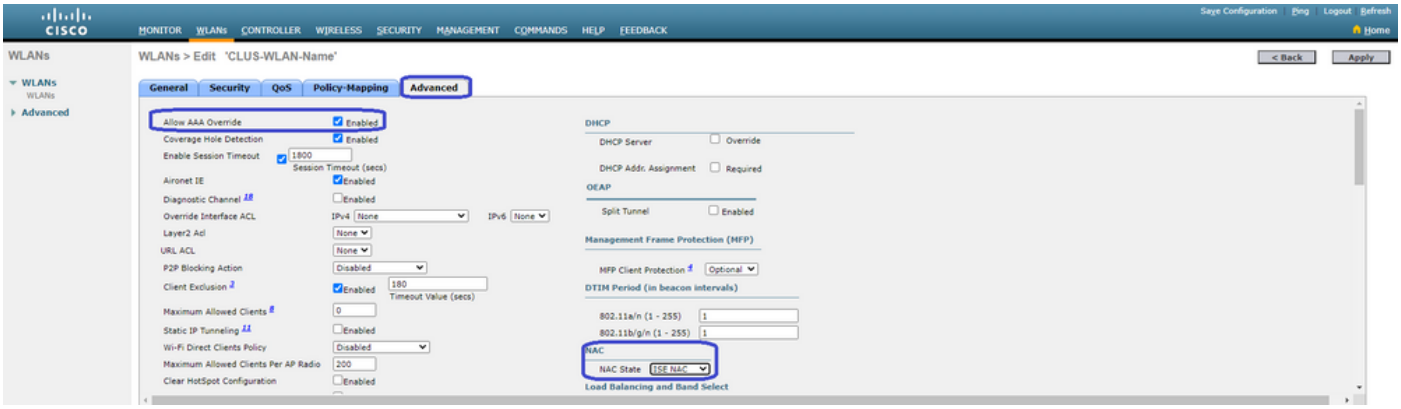
WLAN 컨피그레이션으로 이동해야 합니다. ISE를 AVP에 전송하도록 구성하지 않으려는 경우 "General(일반)" 탭에서 클라이언트가 사용할 인터페이스를 추가할 수 있습니다. 다음으로 **Security>Layer2** 탭으로 이동하여 9800에서 사용한 "Layer 2 Security" 컨피그레이션을 확인하고 "MAC Filtering"을 활성화합니다.



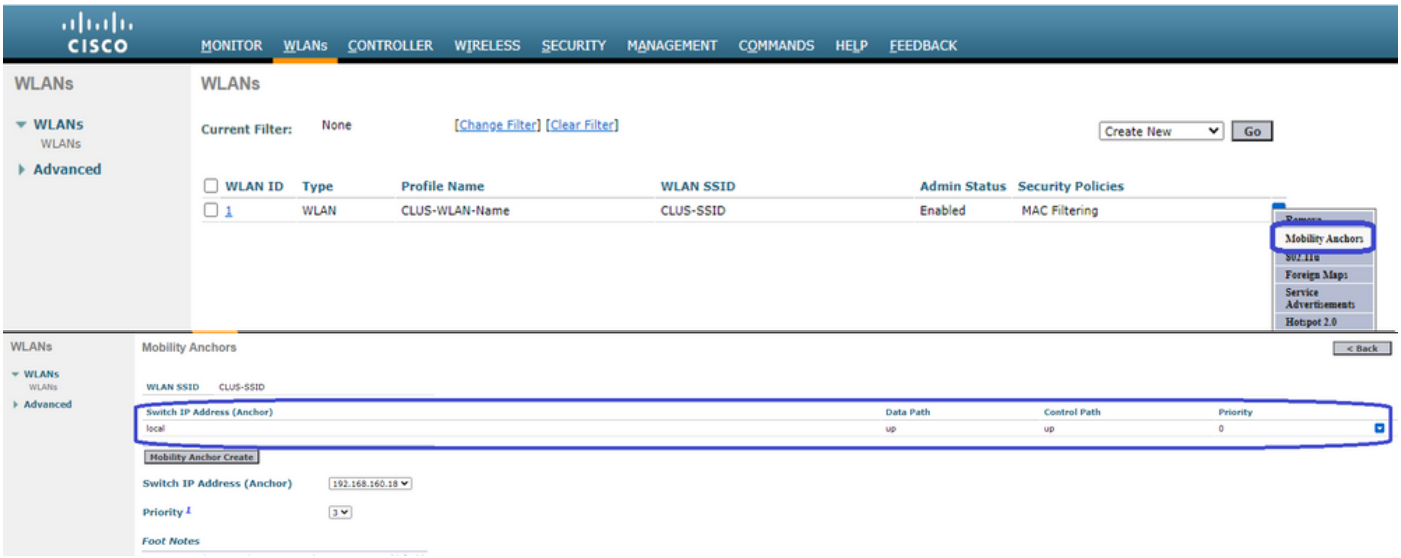
이제 **Security>AAA Servers** 탭으로 이동하고 ISE 서버를 "Authentication Servers"로 설정합니다. **"**Accounting Servers"에 대해 아무것도 설정하지 **마십시오**. 어카운팅에 대해 "Enable(활성화)" 상자의 선택을 취소합니다.



WLAN 컨피그레이션에 있는 동안 "Advanced(고급)" 탭으로 이동하여 "Allow AAA Override(AAA 재정의 허용)"를 활성화하고 "NAC State(NAC 상태)"를 "ISE NAC"로 변경합니다.



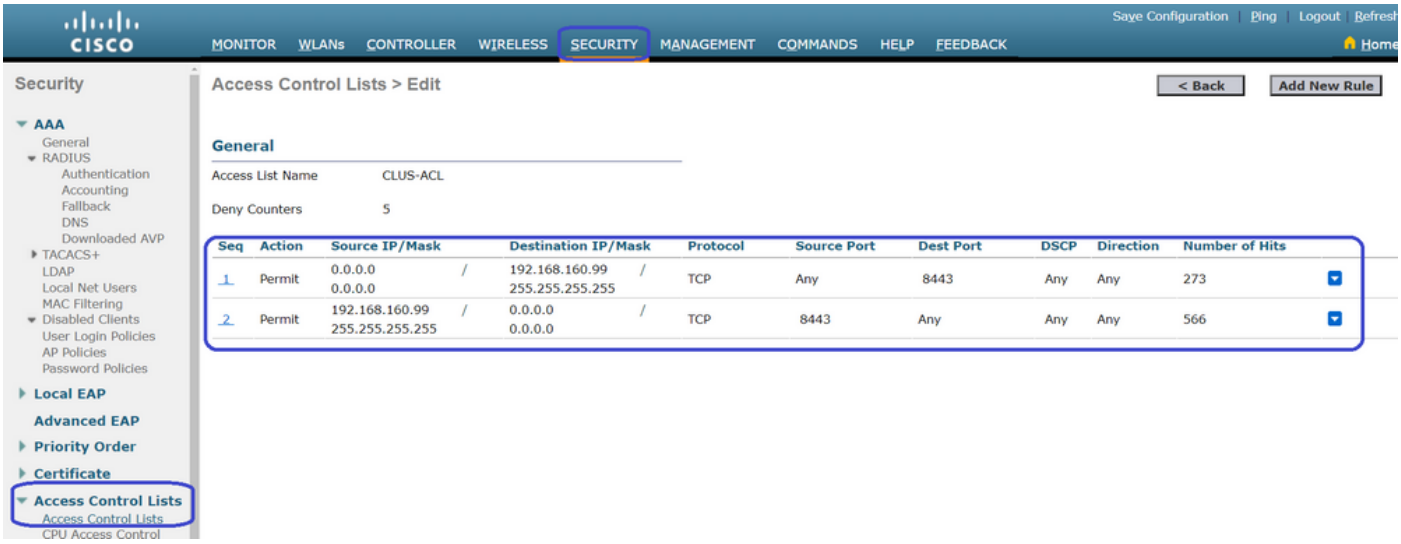
마지막 것은 스스로 고정시키는 것입니다. 이렇게 하려면 **WLANs** 페이지로 돌아가 WLAN>모빌리티 앵커 오른쪽의 파란색 상자 위에 마우스를 놓습니다. "Switch IP Address (Anchor)"를 로컬로 설정하고 "Mobility Anchor Create(모빌리티 앵커 생성)" 버튼을 누릅니다. 그러면 우선순위 0이 고정된 로컬에 표시됩니다.



AireOS WLC에서 ACL 리디렉션

이는 AireOS WLC에 필요한 최종 컨피그레이션입니다. 리디렉션 ACL을 생성하려면 **Security>Access Control Lists>Access Control Lists>New로 이동합니다**. ACL 이름을 입력하고(AVP에서 전송된 것과 일치해야 함) "Apply(적용)"를 누릅니다.

이제 방금 생성한 ACL의 이름을 클릭합니다. "Add New Rule" 버튼을 클릭합니다. 9800 컨트롤러와 달리 AireOS WLC에서는 리디렉션되지 않고 ISE에 연결할 수 있는 트래픽에 대한 permit 문을 구성합니다. DHCP 및 DNS는 기본적으로 허용됩니다.

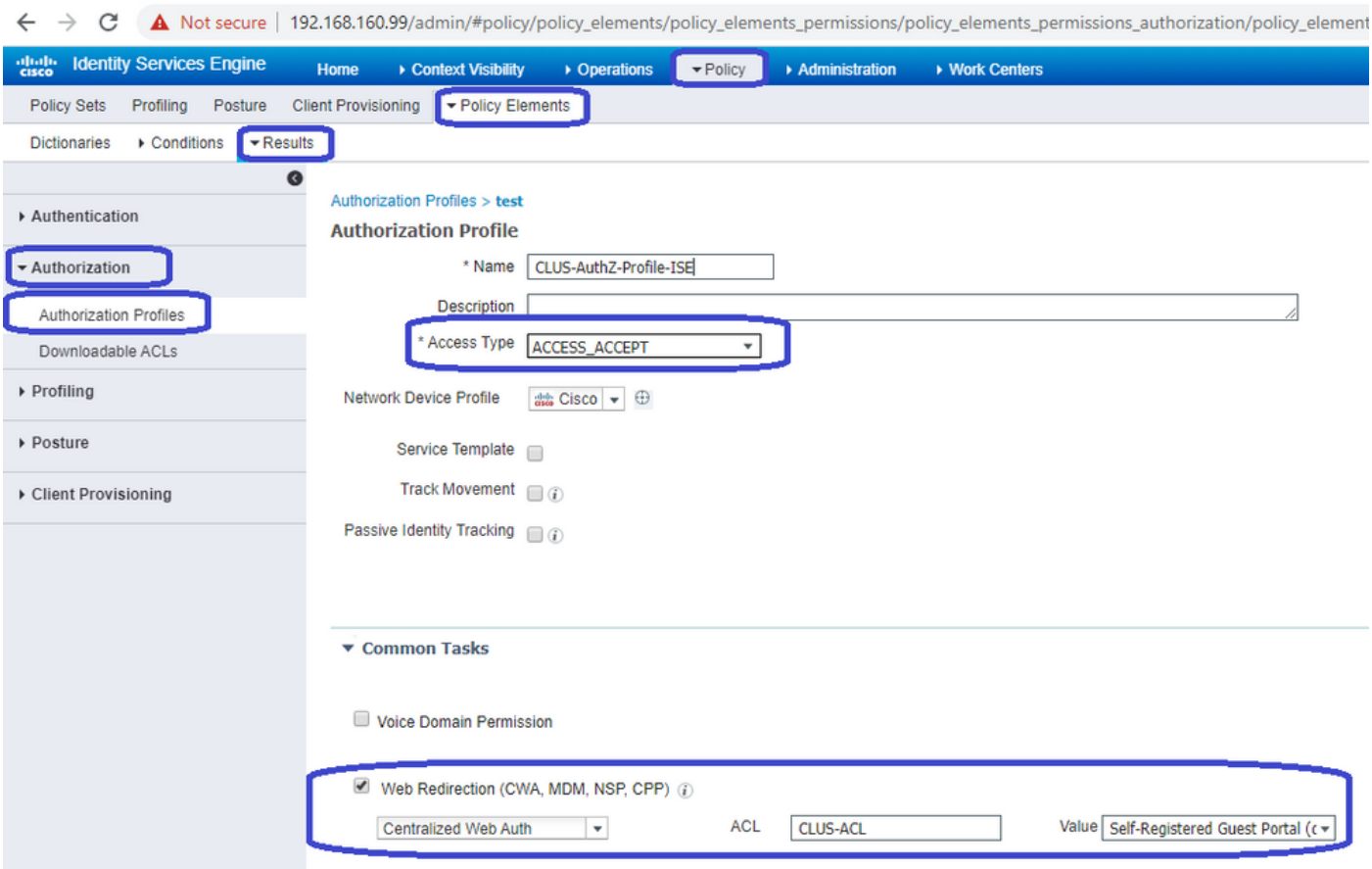


ISE 구성

CWA ISE . .

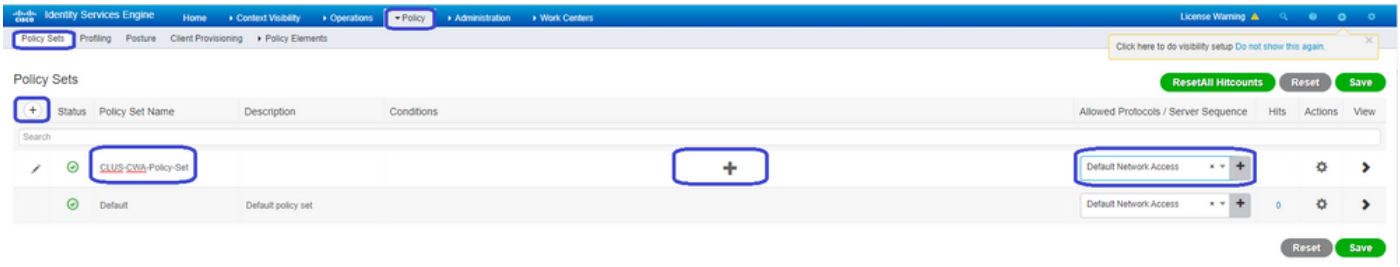
ISE , , ISE 9800(foreign) , .

Policy()>Policy Elements( )>Authorization( )>Results()>Authorization Profiles( )>+Add() . "access_accept" AVP(attribute-value) . CWA ACL URL VLAN ID . ACL WLC ACL .



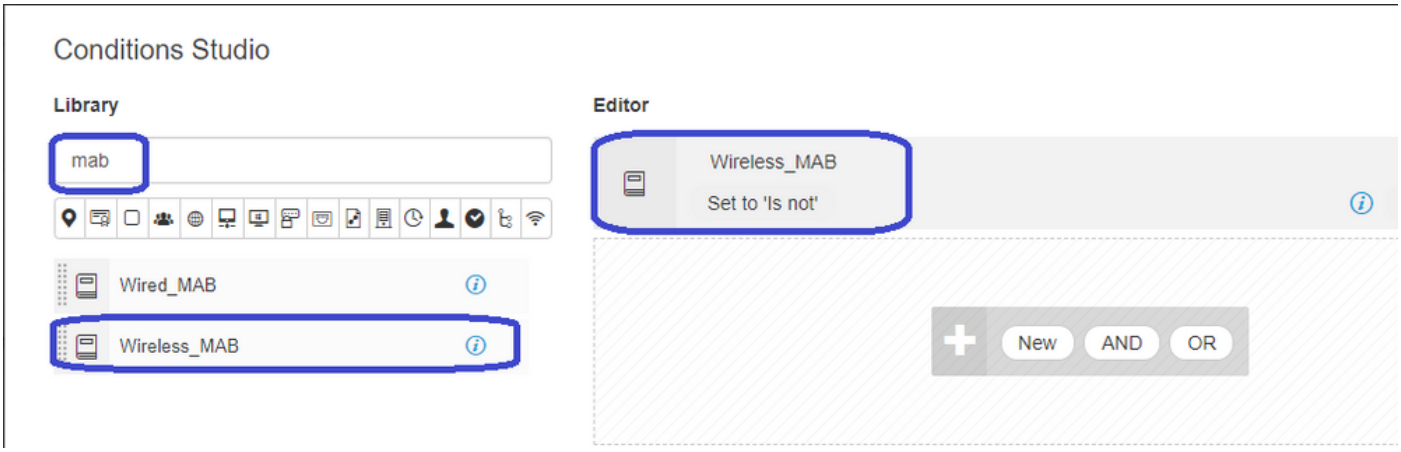
CWA . , MAB , ID SSID . , . , . .

Policy() **>Policy Sets(**) + . MAB "Process Host Lookup( )" " " (> >>>) . + .

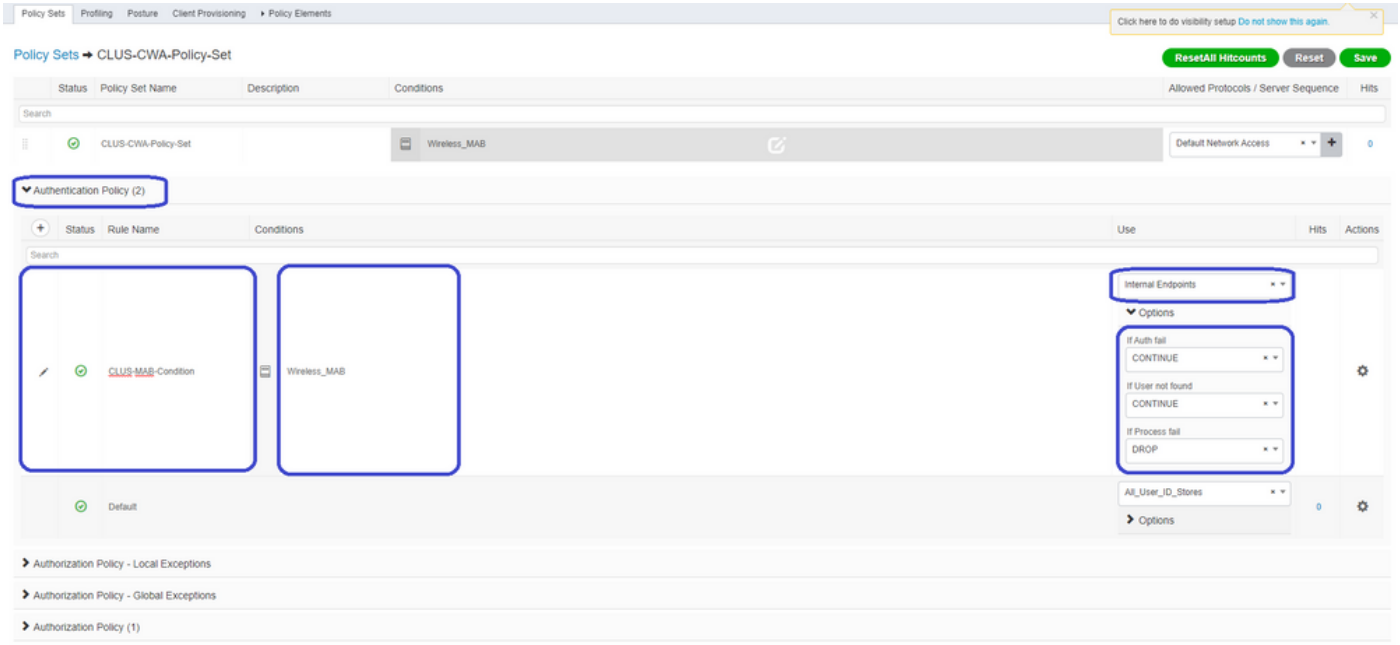


MAB ISE . WLAN ID .

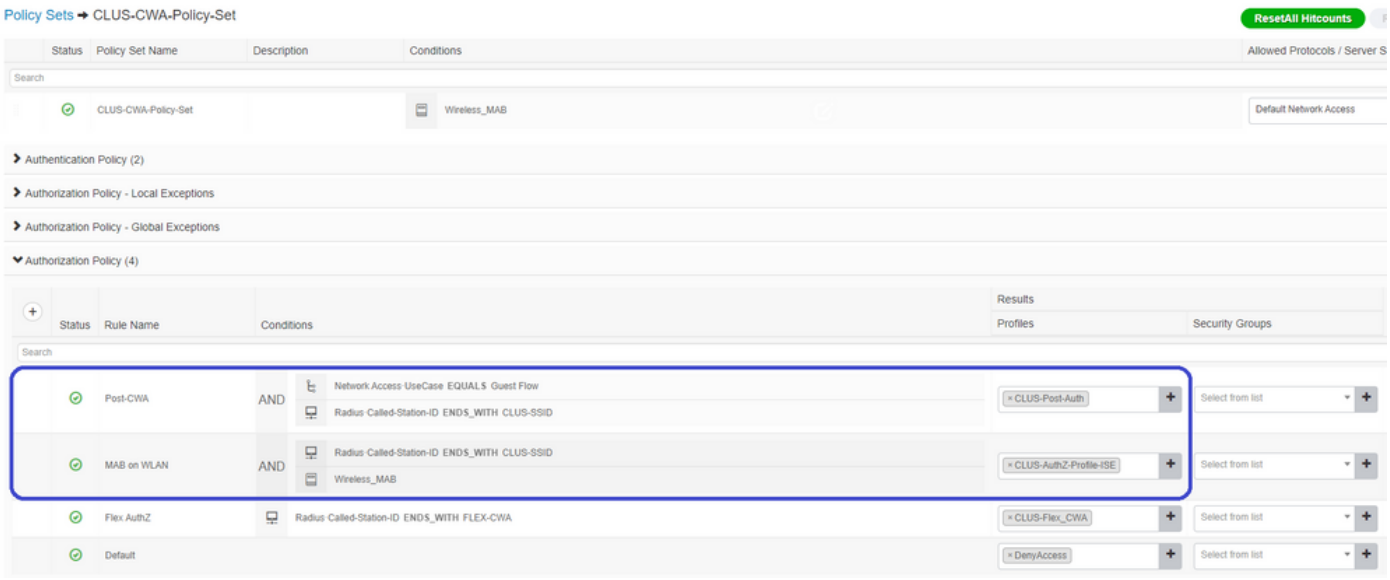
.



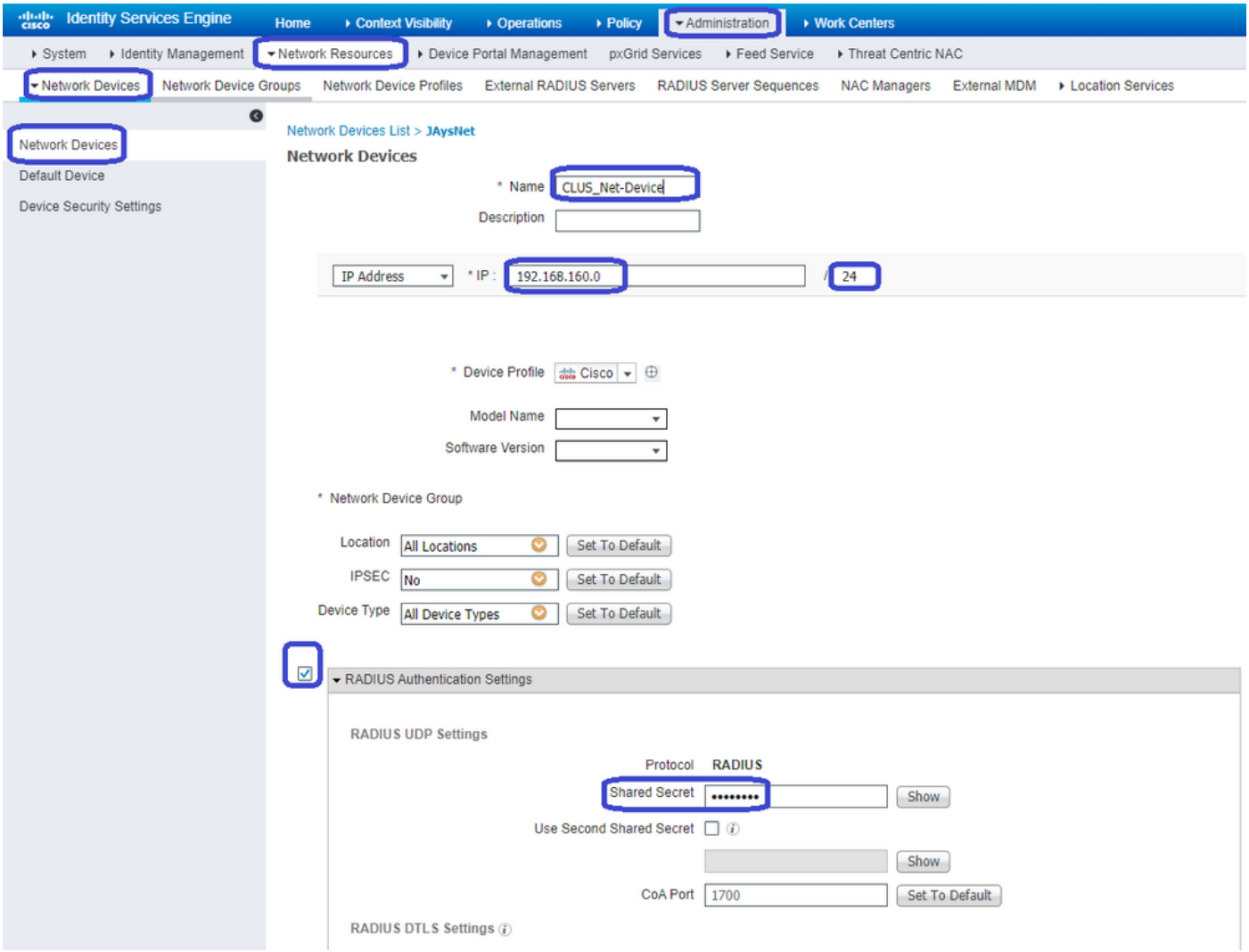
. MAB " " ID .



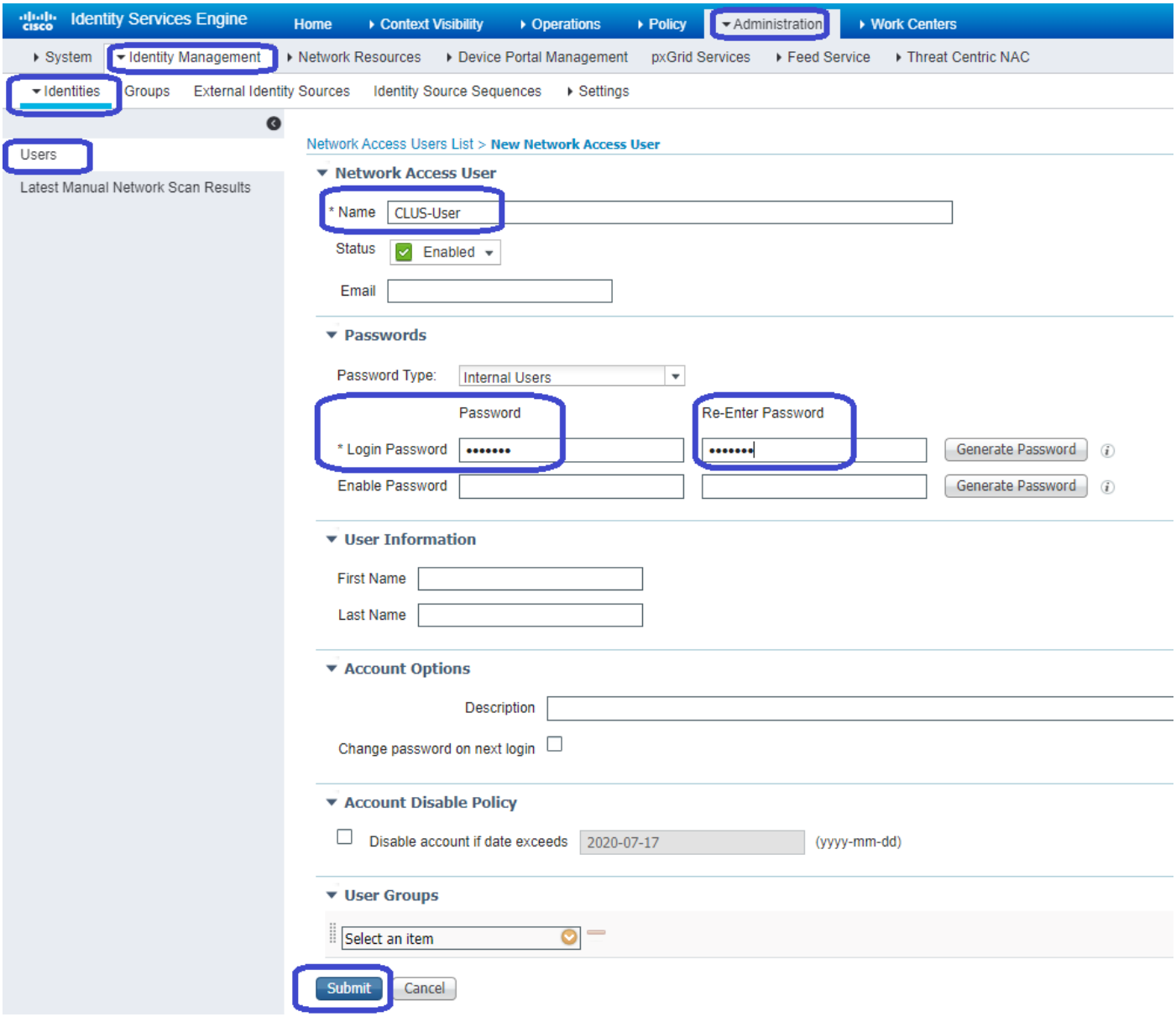
. ACL . . . . SSID ID WLAN .



ISE 9800(foreign) ISE . **Admin()>Network Resources( )>Network Device( )>+**. IP ( ) RADIUS . ISE 9800 . . .



, . **Admin()>Identity Management(ID)>Identity(ID)>Users()>+Add()** submit() . ISE , .



AireOS WLC가 외부, Catalyst 9800이 앵커인 경우 구성의 차이점

AireOs WLC를 외부 컨트롤러로 지정하려면 컨피그레이션은 두 가지 차이만 있는 이전과 동일합니다.

1. AAA 어카운팅은 앵커에서 수행되지 않으므로 9800에는 어카운팅 방법 목록이 없고 AireOS WLC는 어카운팅이 활성화되고 ISE를 가리키도록 합니다.
2. AireOS는 그 자체가 아닌 9800에 고정되어야 합니다. Policy Profile(정책 프로파일)에서 9800에는 앵커가 선택되지 않았지만 "Export Anchor(앵커 내보내기)" 상자가 선택되어 있습니다.
3. AireOS WLC가 클라이언트를 9800으로 내보낼 때 정책 프로파일의 개념이 없으면 WLAN 프로파일 이름만 보냅니다. 따라서 9800은 AireOS에서 전송된 WLAN 프로파일 이름을 WLAN 프로파일 이름 및 정책 프로파일 이름 모두에 적용합니다. AireOS WLC에서 9800 WLC로 고정할 경우 두 WLC의 WLAN 프로파일 이름과 9800의 정책 프로파일 이름이 모두 일치해야 한다는 것입니다.

다음을 확인합니다.

9800 WLC에서 컨피그레이션을 확인하려면 명령을 실행합니다.

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- 정책 프로파일

```
Show wireless profile policy detailed <profile name>
```

- 정책 태그

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- 앵커와 함께 모빌리티가 작동되는지 확인

```
Show wireless mobility summary
```

AireOS WLC의 컨피그레이션을 확인하려면 명령을 실행합니다.

- AAA

```
Show radius summary
```

참고: RFC3576은 CoA 컨피그레이션입니다.

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- 모빌리티가 외부와 일치하는지 확인

```
Show mobility summary
```

문제 해결

문제 해결은 클라이언트가 중지하는 프로세스의 어느 지점에 따라 다르게 나타납니다. 예를 들어 WLC가 MAB에서 ISE로부터 응답을 받지 못하면 클라이언트는 "Policy Manager State:(정책 관리자 상태:): "연결 중"을 선택하고 앵커로 내보내지 않습니다. 이 경우 외부 문제 해결만 수행하며 WLC와 ISE 간의 트래픽에 대한 RA 추적 및 패킷 캡처를 수집할 수 있습니다. 또 다른 예는 MAB가 성공적으로 통과되었지만 클라이언트가 리디렉션을 수신하지 못한다는 것입니다. 이 경우 외주가 AVP에서 리디렉션을 수신하여 클라이언트에 적용했는지 확인해야 합니다. 또한 클라이언트가 올

바른 ACL을 사용하여 있는지 확인하려면 앵커를 확인해야 합니다. 이 트러블슈팅 범위는 이 기술 문서의 설계 외부에 있습니다(일반 클라이언트 트러블슈팅 지침에 대한 참조 확인).

9800 WLC의 CWA 문제 해결에 대한 자세한 내용은 Cisco Live! 프레젠테이션 DGTL-TSCENT-404

Catalyst 9800 문제 해결 정보

클라이언트 세부 정보

show wireless client mac-address
여기서는 "Policy Manager State(정책 관리자 상태)", "Session Manager(세션 관리자)>Auth Method(인증 방법)", "Mobility Role(모빌리티 역할)"을 확인해야 합니다.

Monitoring(모니터링)>Clients(클라이언트) 아래의 GUI에서 이 정보를 찾을 수도 있습니다

임베디드 패킷 캡처

CLI에서 명령은 *capture <capture name>#monitor을* 시작한 다음 옵션이 나타납니다.

GUI에서 Troubleshoot(문제 해결)>Packet Capture(패킷 캡처)>+Add(추가)로 이동합니다.

RadioActive 추적

CLI에서

debug wireless mac|ip
이 명령을 중지하려면 이 명령의 no 형식을 사용합니다. 이 파일은 "ra_trace"라는 bootflash에서 클라이언트의 MAC 또는 IP 주소와 날짜 및 시간에 기록됩니다.

GUI에서 Troubleshoot(문제 해결)>Radial Trace(방사능 추적)>+Add(추가)로 이동합니다. 클라이언트의 mac 또는 ip 주소를 추가하고 Apply를 누른 다음 start를 누릅니다. 프로세스를 몇 번 거친 후 추적을 중지하고 로그를 생성한 다음 디바이스에 다운로드합니다.

AireOS 문제 해결 정보

클라이언트 세부 정보

CLI *show client details <client mac>에서*

GUI Monitor(GUI 모니터)>Clients(클라이언트)에서

CLI에서 디버깅

Debug client

Debug mobility handoff

Debug mobility config

참조

9800 컨트롤러를 사용하여 모빌리티 터널 구축

9800의 무선 디버깅 및 로그 수집