Catalyst 9800 Wireless Controller AP 권한 부여 목록 구성

목차

소개

이 문서에서는 Catalyst 9800 Wireless LAN Controller AP(Access Point) 인증 정책을 구성하는 방법에 대해 설명합니다.

배경 정보

액세스 포인트(AP)에 권한을 부여하려면 9800 Wireless LAN Controller를 사용하는 로컬 데이터베이스 또는 외부 원격 인증 RADIUS(Dial-In User Service) 서버에 대해 AP의 이더넷 MAC 주소를 인증해야 합니다.

이 기능을 사용하면 승인된 액세스 포인트(AP)만 Catalyst 9800 Wireless LAN Controller에 조인할 수 있습니다. 이 문서에서는 컨트롤러에 조인하기 위해 mac 필터 항목이 필요하지만 일반적인 AP 권한 부여 흐름을 추적하지 않는 메시(1500 Series) AP의 경우를 다루지 않습니다(참조).

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC
- 무선 컨트롤러에 대한 CLI(명령줄 인터페이스) 액세스

사용되는 구성 요소

9800 WLC v16.12

AP 1810W

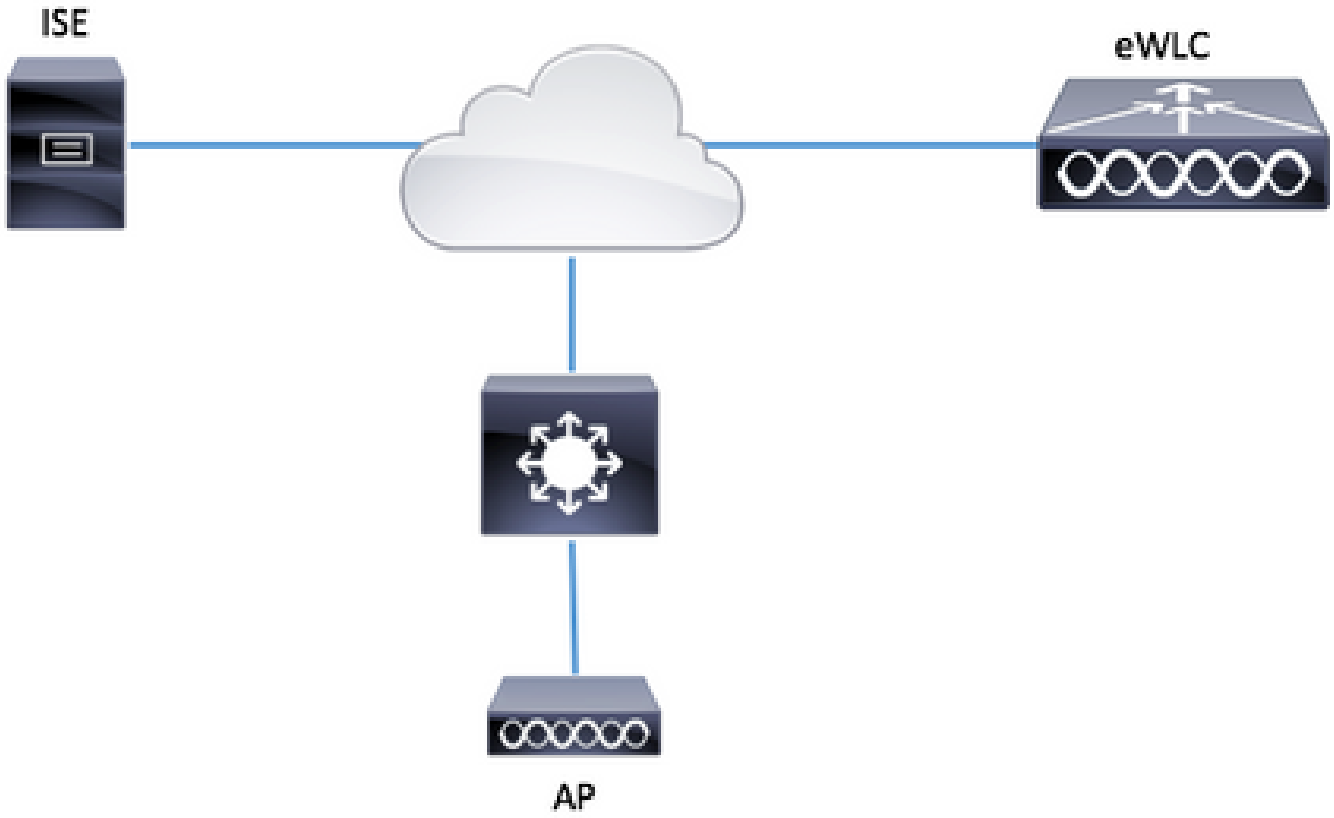
AP 1700

ISE(Identity Service Engine) v2.2

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.

구성

네트워크 다이어그램



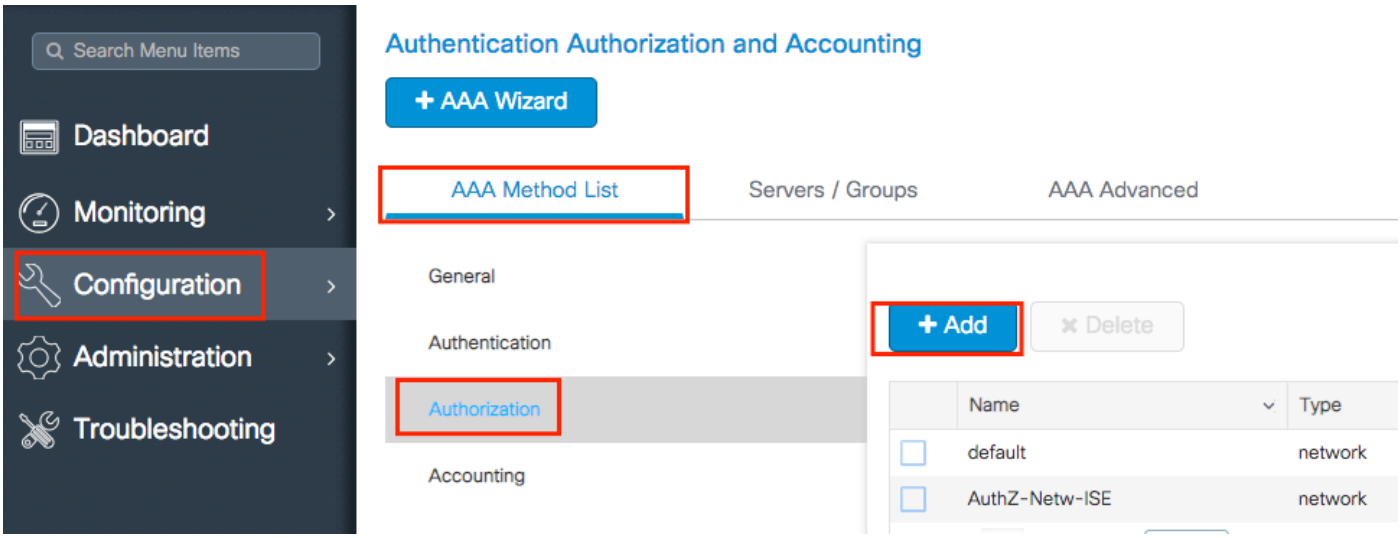
설정

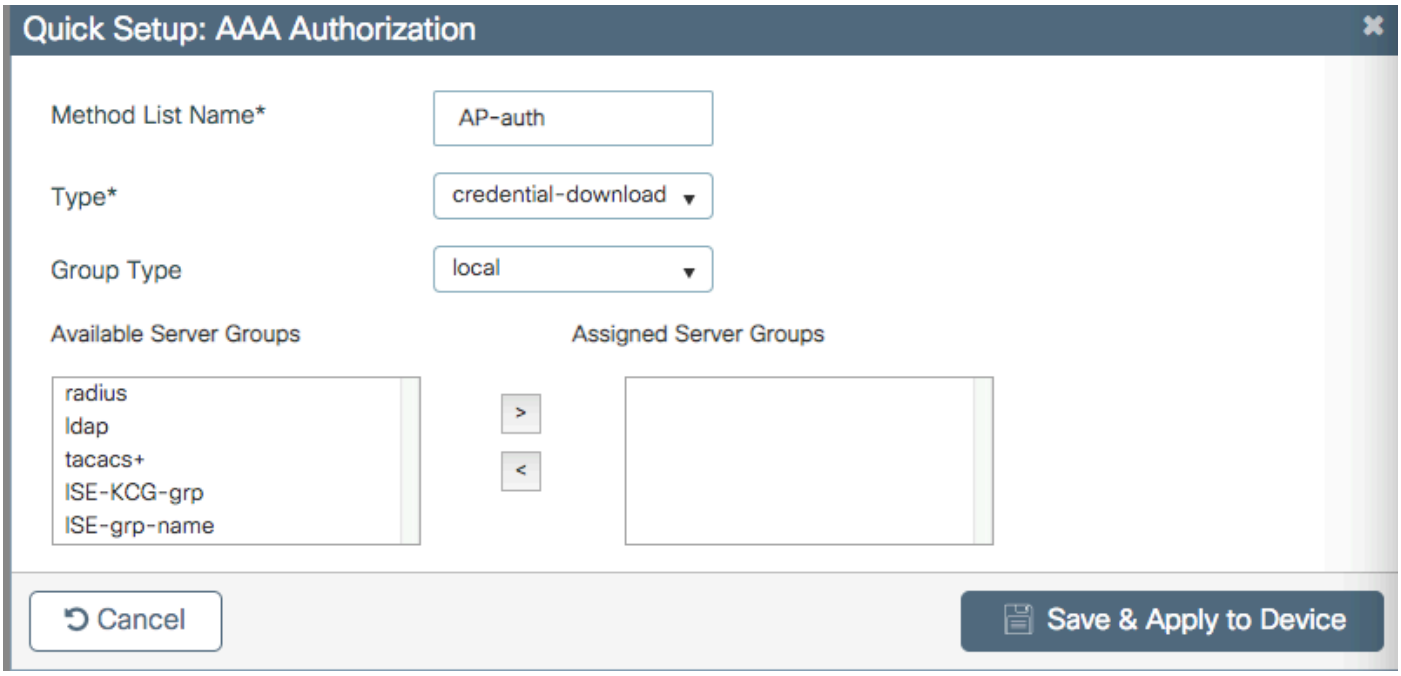
MAC AP 권한 부여 목록 - 로컬

권한 있는 AP의 MAC 주소는 9800 WLC에 로컬로 저장됩니다.

1단계. 로컬 인증 자격 증명 다운로드 방법 목록을 만듭니다.

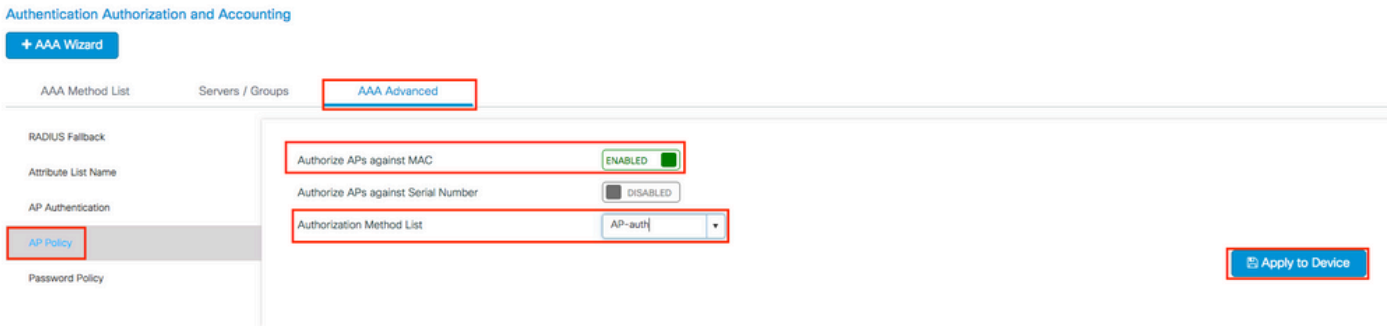
Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여) > + Add(추가)로 이동합니다.





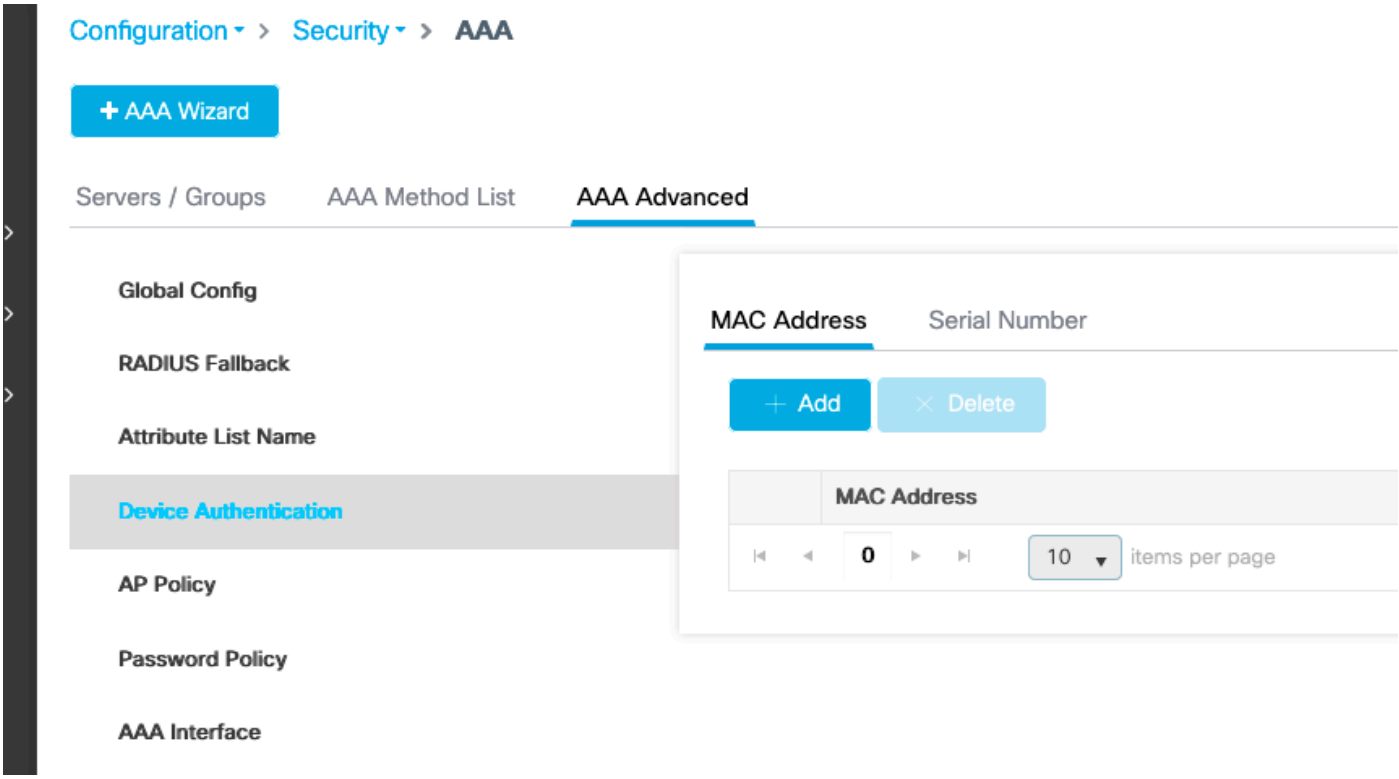
2단계. AP MAC 권한 부여를 활성화합니다.

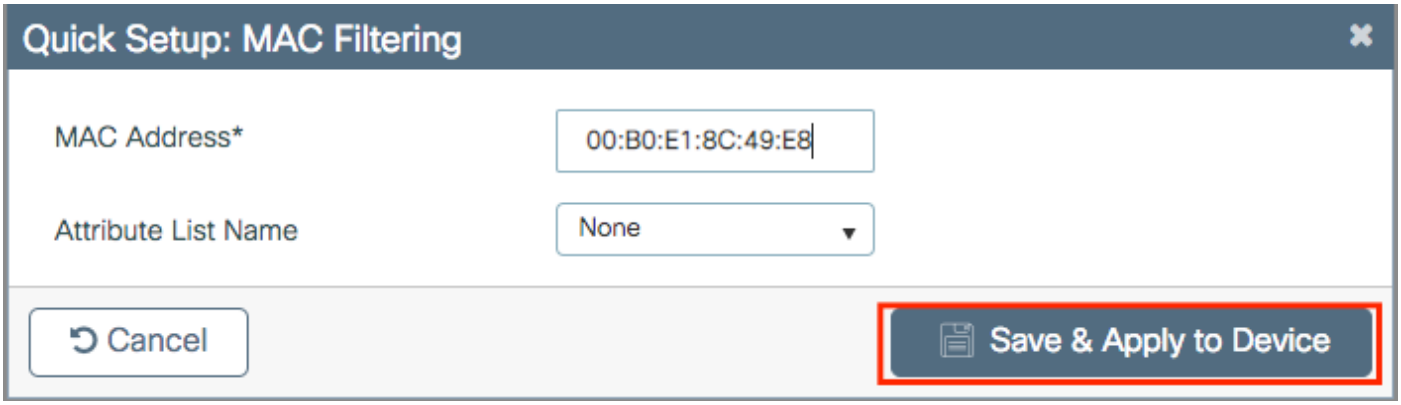
탐색 Configuration(구성) > Security(보안) > AAA > AAA Advanced(AAA 고급) > AP Policy(AP 정책) Authorize APs against MAC(MAC에 대해 권한 부여 AP 활성화)을 활성화하고 1단계에서 생성한 Authorization Method(권한 부여 방법) 목록을 선택합니다.



3단계. AP 이더넷 mac 주소를 추가합니다.

탐색 Configuration(구성) > Security(보안) > AAA > AAA Advanced(AAA 고급) > Device Authentication(디바이스 인증) > MAC Address(MAC 주소) > + Add(추가)





참고: AP 이더넷 mac 주소는 버전 16.12의 웹 UI(xx:xx:xx:xx:xx(또는) xxxx.xxxx.xxxx(또는) xx-xx-xx-xx-xx)에 입력한 경우 이러한 형식 중 하나로 표시됩니다. 버전 17.3에서는 구분 기호가 없는 xxxxxxxxxxx 형식이어야 합니다. CLI 형식은 항상 모든 버전에서 xxxxxxxxxxx입니다(16.12에서는 웹 UI가 컨피그레이션에서 구분 기호를 제거합니다). Cisco 버그 ID CSCvv43870은 이후 릴리스에서 CLI 또는 웹 UI의 모든 형식을 사용할 수 있습니다.

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

MAC AP 권한 부여 목록 - 외부 RADIUS 서버

9800 WLC 구성

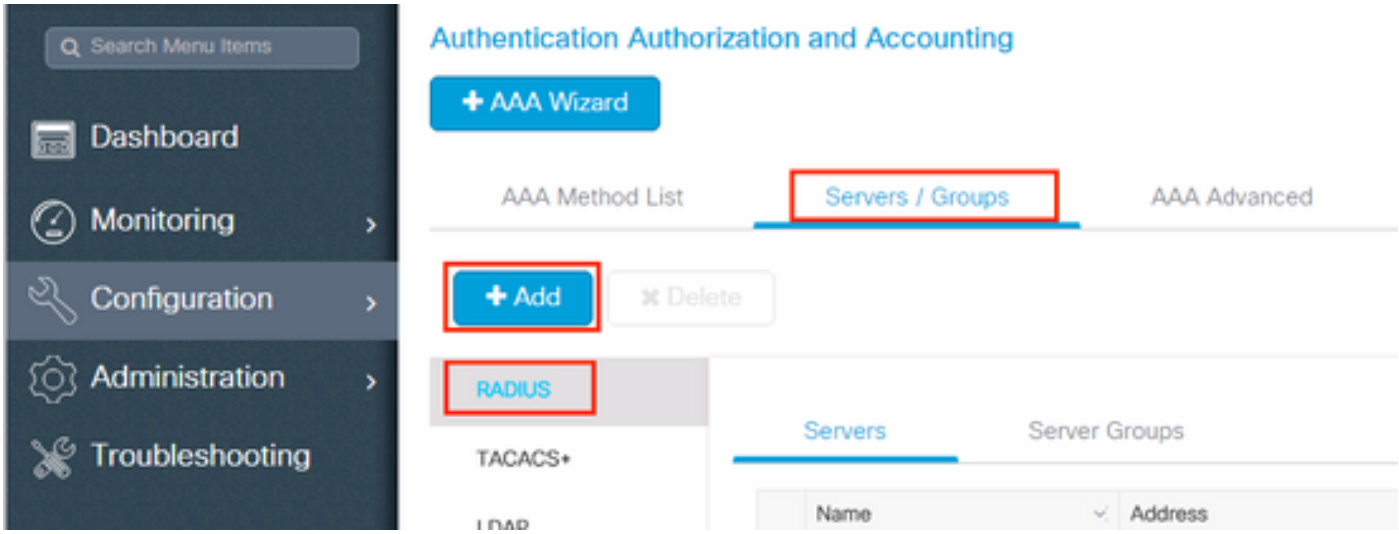
권한 있는 AP의 MAC 주소는 외부 RADIUS 서버(이 예에서는 ISE)에 저장됩니다.

ISE에서 AP의 MAC 주소를 사용자 이름/비밀번호 또는 엔드포인트로 등록할 수 있습니다. 이 단계를 수행하면 한 가지 방법 또는 다른 방법을 사용하도록 선택하는 방법이 표시됩니다.

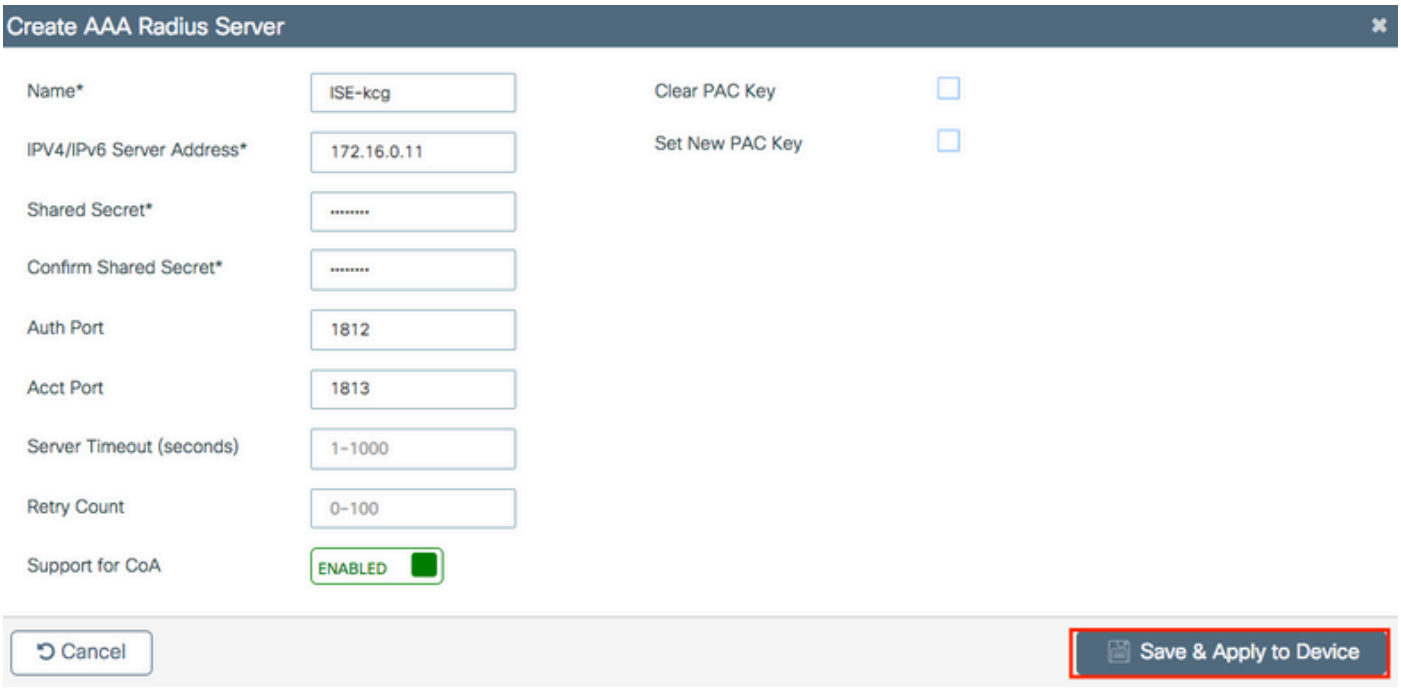
GUI:

1단계. RADIUS 서버 선언

Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Servers(서버) > + Add(추가)로 이동하고 RADIUS 서버 정보를 입력합니다.



나중에 중앙 웹 인증(또는 CoA를 필요로 하는 모든 종류의 보안)을 사용하려는 경우 CoA 지원이 활성화되어 있는지 확인하십시오.

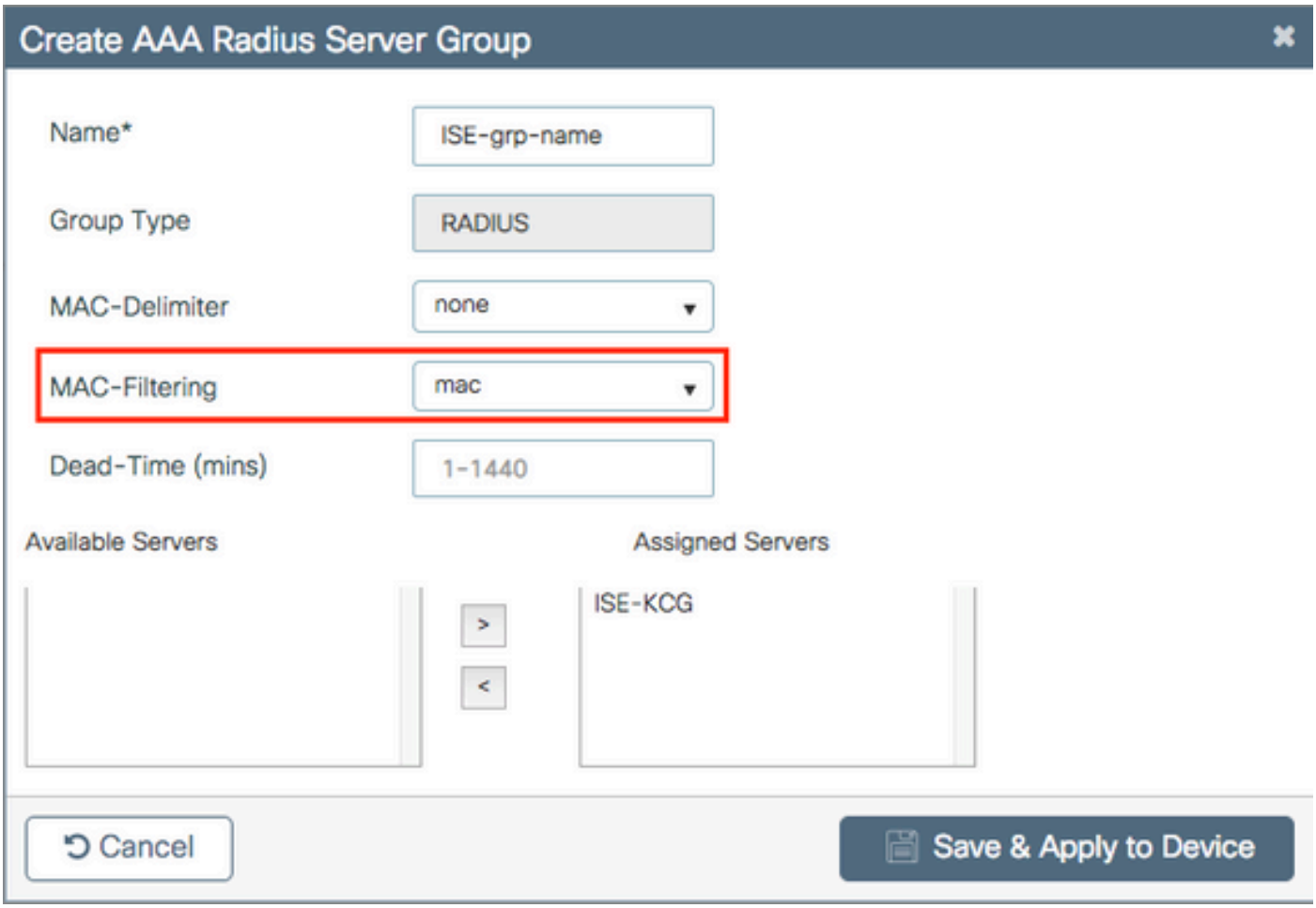


2단계. RADIUS 그룹에 RADIUS 서버 추가

Configuration(컨피그레이션) > Security(보안) > AAA > Servers/Groups(서버/그룹) > RADIUS > Server Groups(서버 그룹) > + Add(추가)로 이동합니다

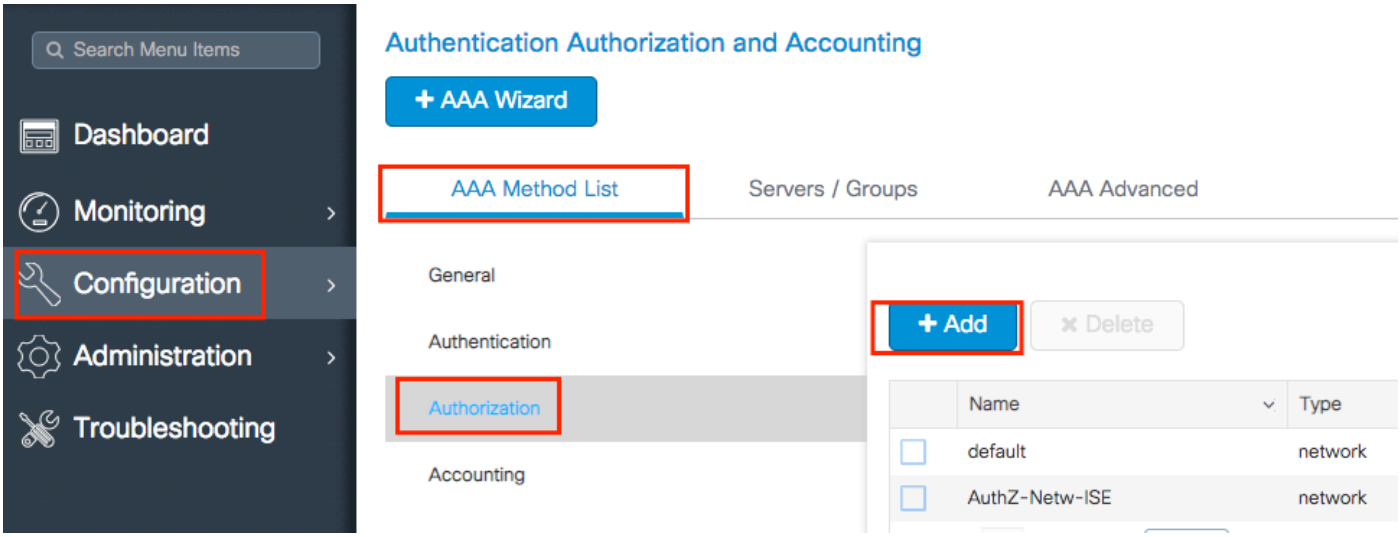
ISE가 AP MAC 주소를 사용자 이름으로 인증하도록 하려면 MAC-Filtering을 none으로 둡니다.

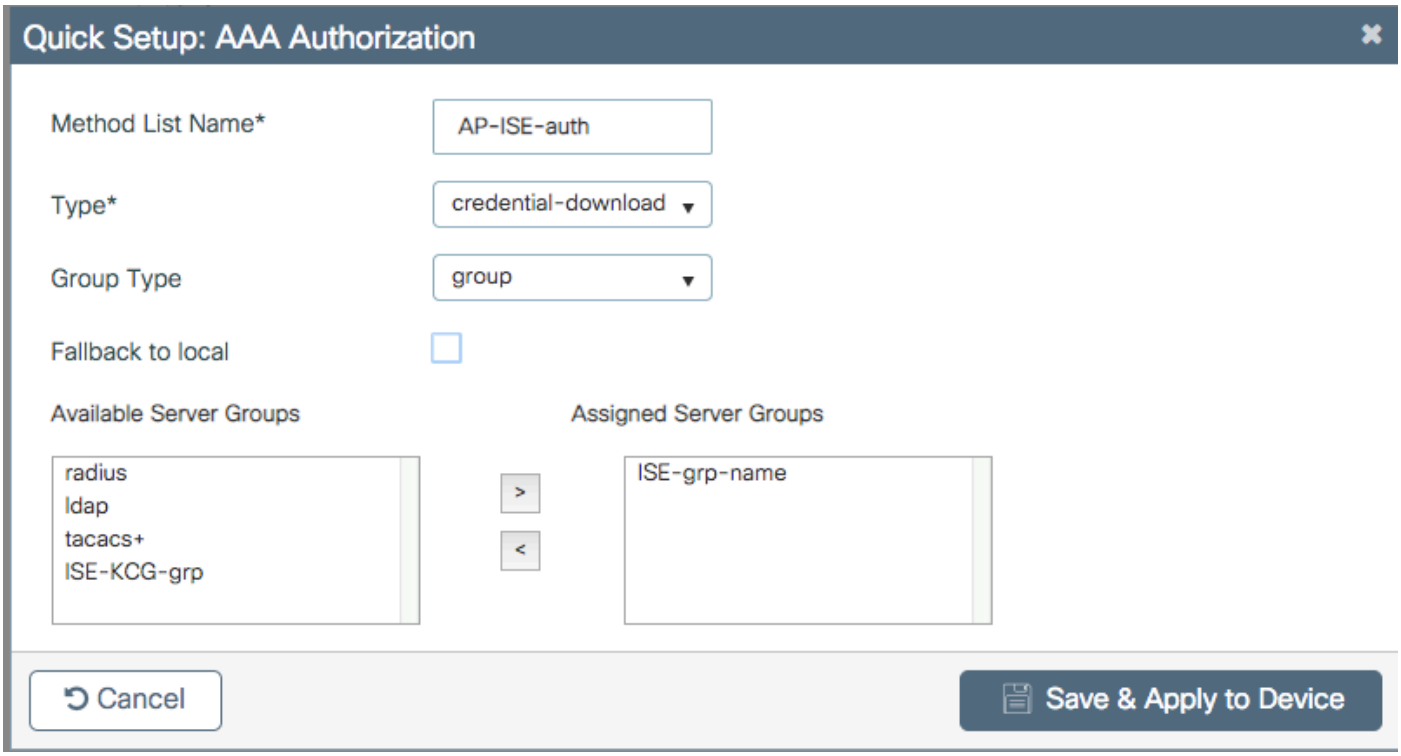
엔드포인트가 MAC-Filtering을 mac으로 변경할 때 ISE가 AP MAC 주소를 인증하도록 하려면



3단계. 권한 부여 자격 증명 다운로드 방법 목록을 만듭니다.

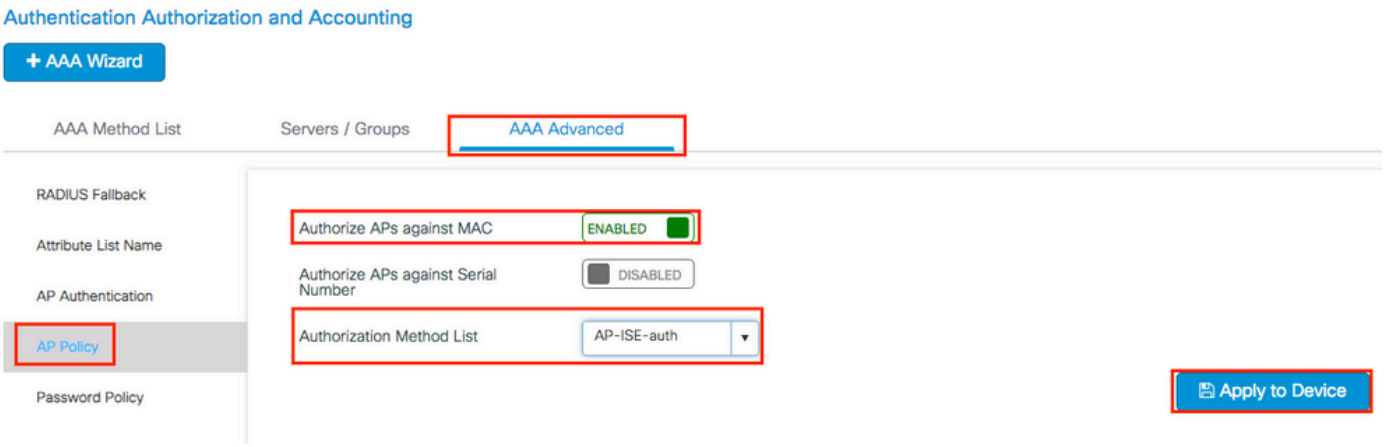
Configuration(컨피그레이션) > Security(보안) > AAA > AAA Method List(AAA 메서드 목록) > Authorization(권한 부여) > + Add(추가)로 이동합니다.





4단계. AP MAC 권한 부여를 활성화합니다.

탐색 Configuration(구성) > Security(보안) > AAA > AAA Advanced(AAA 고급) > AP Policy(AP 정책) Authorize APs against MAC(MAC에 대해 권한 부여 AP)을 활성화하고 3단계에서 생성한 Authorization Method(권한 부여 방법) 목록을 선택합니다.



CLI:

```
# config t
# aaa new-model

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

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

ISE 컨피그레이션

1단계. ISE에 9800 WLC를 추가하려면

ISE에서 9800 WLC 선언

인증을 기반으로 AP의 MAC 주소를 필수 단계로 구성하도록 선택합니다.

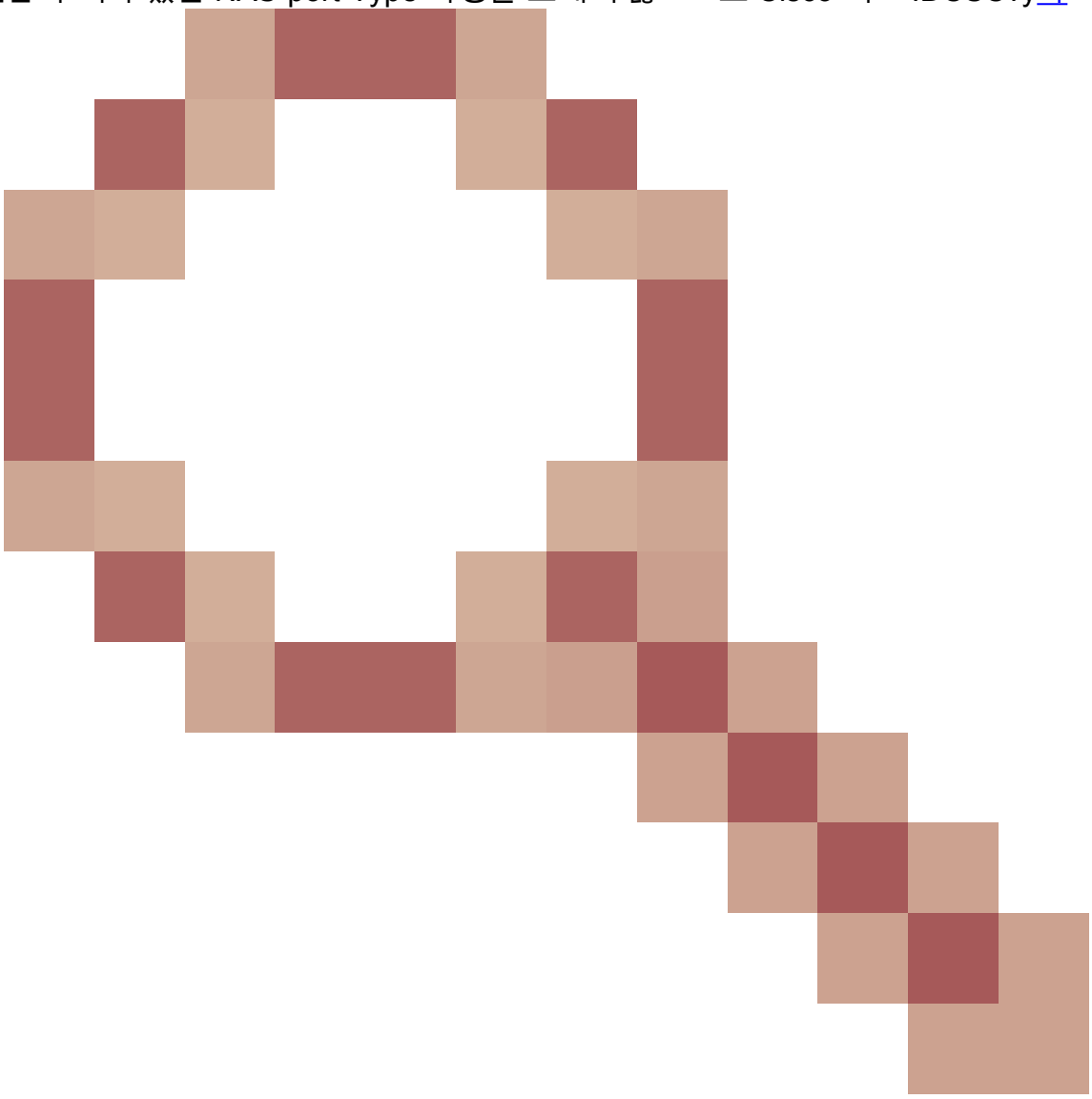
MAC 주소를 엔드포인트로 인증하도록 USE 구성

MAC 주소를 사용자 이름/비밀번호로 인증하도록 ISE 구성

MAC 주소를 엔드포인트로 인증하도록 ISE 구성

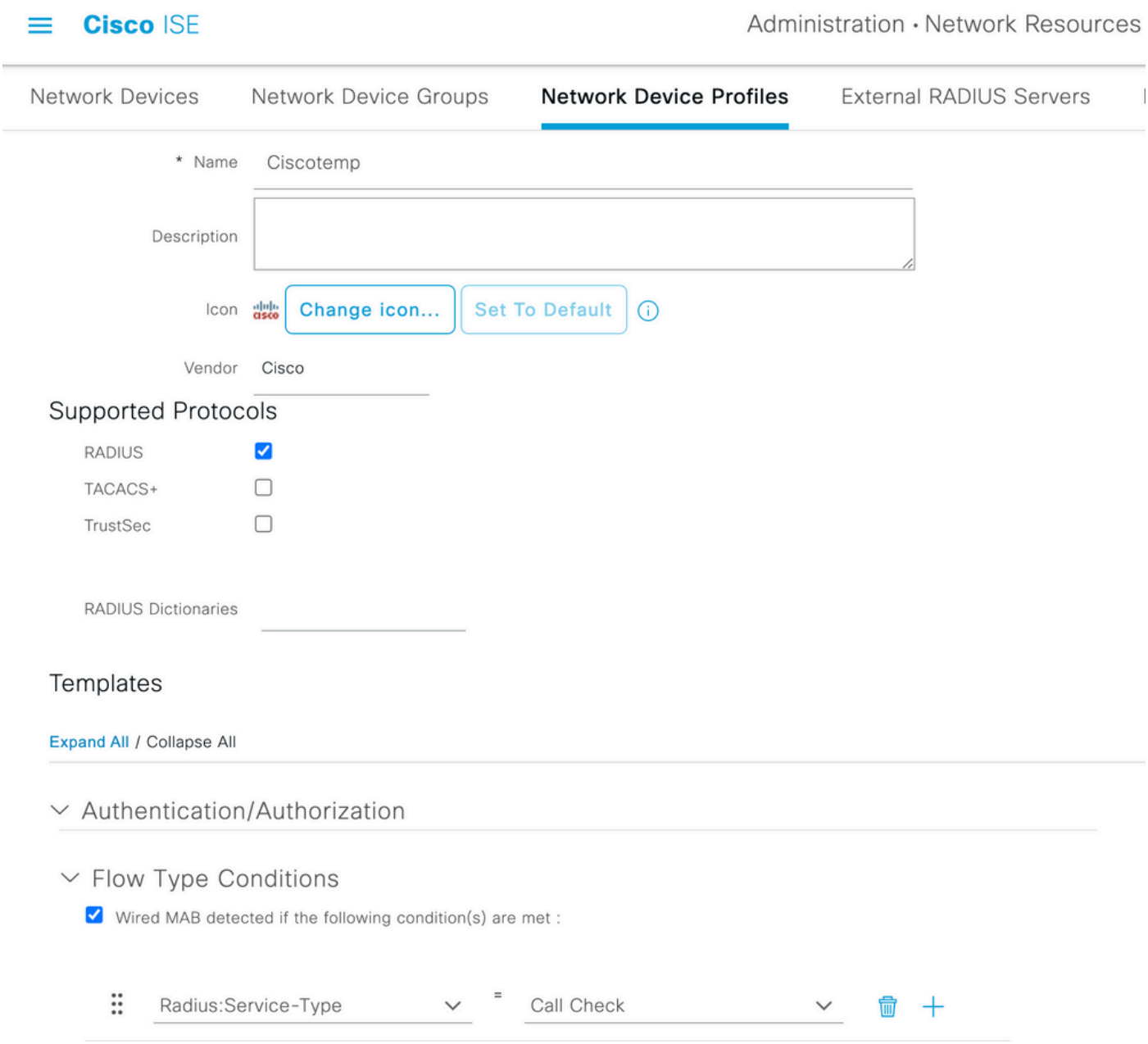
2단계. (선택 사항) 액세스 포인트에 대한 ID 그룹 생성

9800에서는 AP 권한 부여가 있는 NAS-port-Type 특성을 보내지 않으므로 Cisco 버그 IDCSCvy가



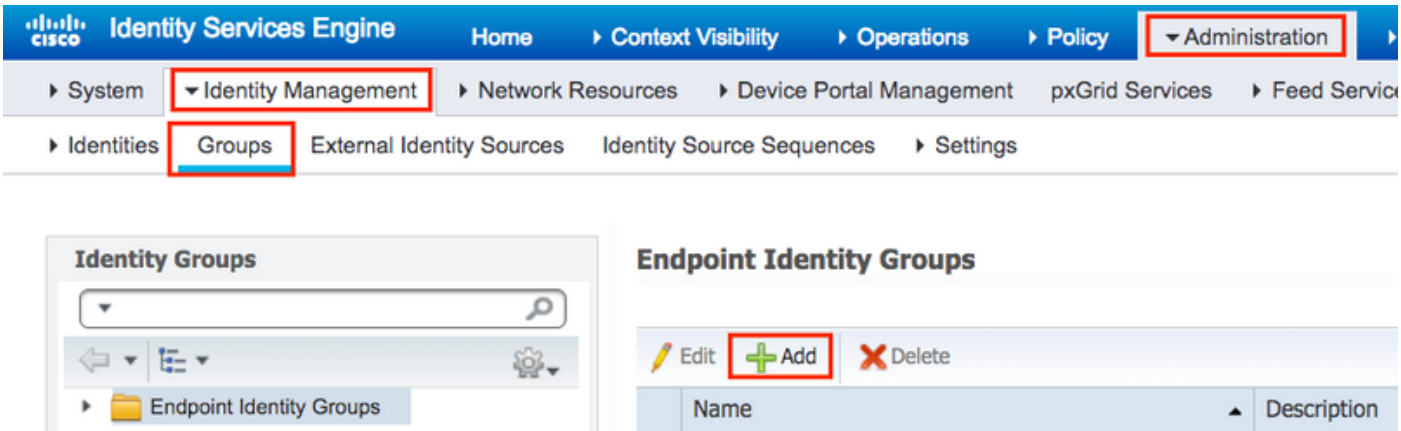
발생합니다74904
) ISE는 AP 권한 부여를 MAB 워크플로로 인식하지 않으므로 AP의 MAC 주소가 엔드포인트 목록에 있으면 AP를 인증할 수 없습니다. 단, MAB 워크플로를 수정하여 ISE의 NAS-PORT-type 특성을 요구하지 않아야 합니다.

Administrator(관리자) > Network device profile(네트워크 디바이스 프로파일)로 이동하여 새 디바이스 프로파일을 생성합니다. RADIUS를 활성화하고 유선 MAB에 대한 service-type=call-check를 추가합니다. 나머지는 Cisco 원래 프로필에서 복사할 수 있습니다. 유선 MAB에 대한 "nas-port-type" 조건이 없는 것이 좋습니다.

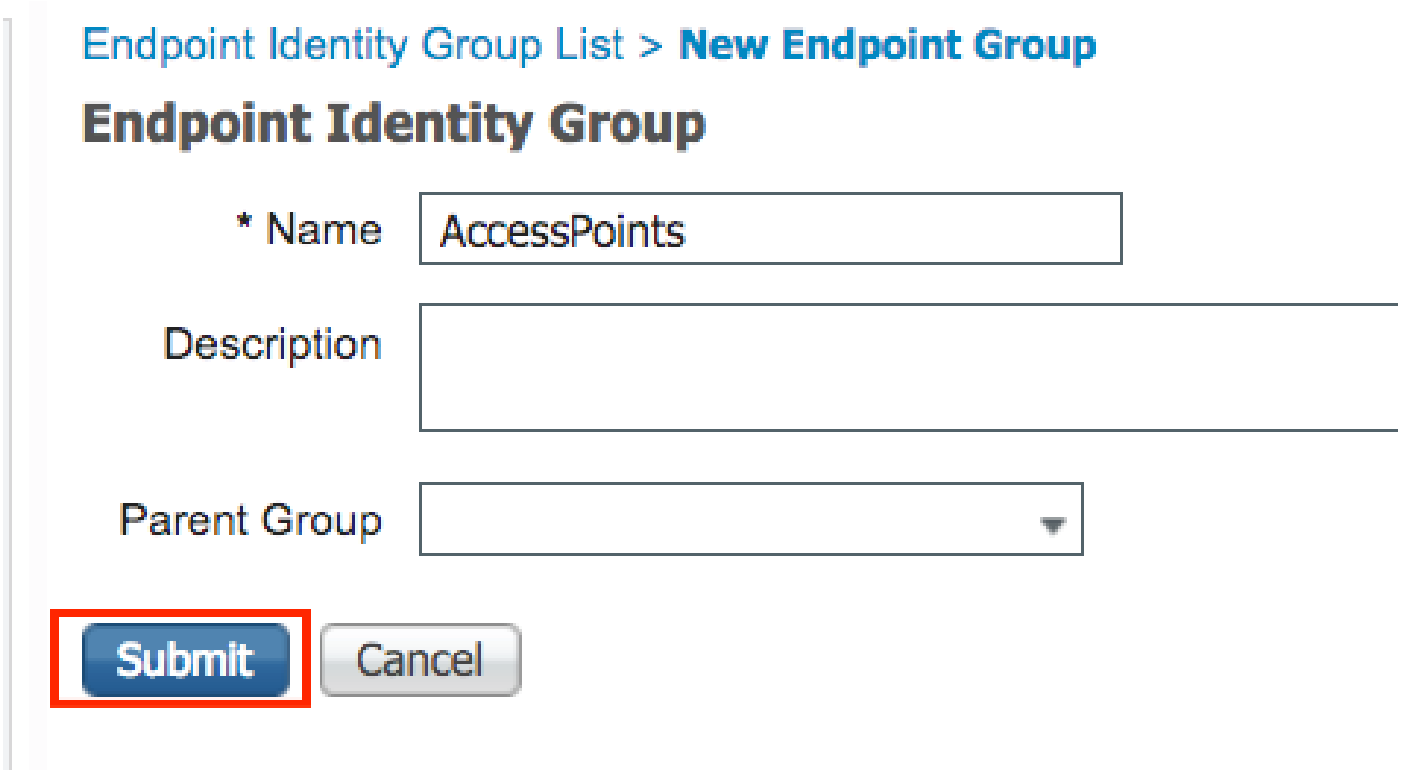


9800의 네트워크 디바이스 항목으로 돌아가 해당 프로필을 새로 생성된 디바이스 프로필로 설정합니다.

Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > Endpoint Identity Groups(엔드포인트 ID 그룹) > + Add(추가)로 이동합니다.

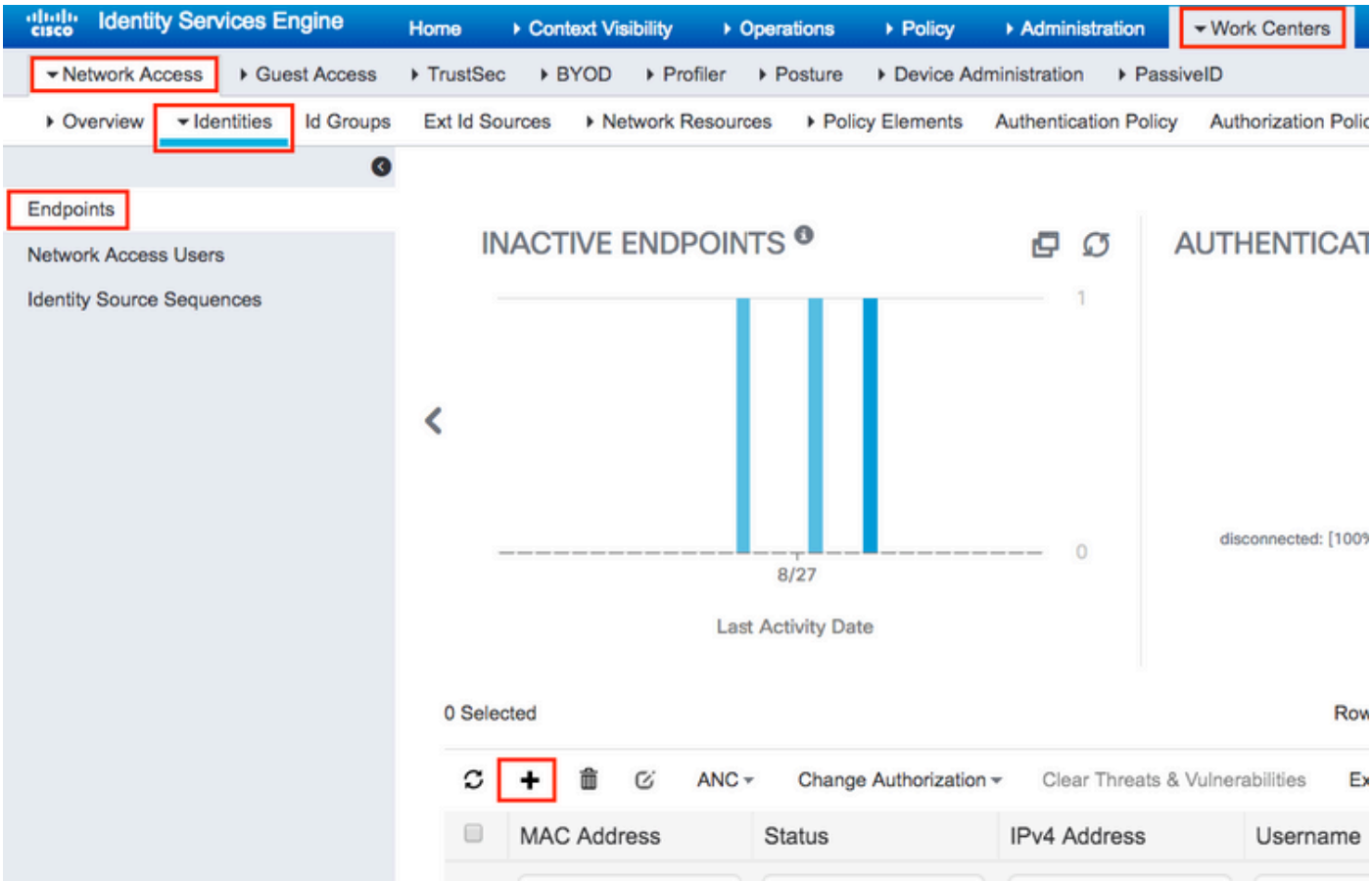


이름을 선택하고 Submit(제출)을 클릭합니다.

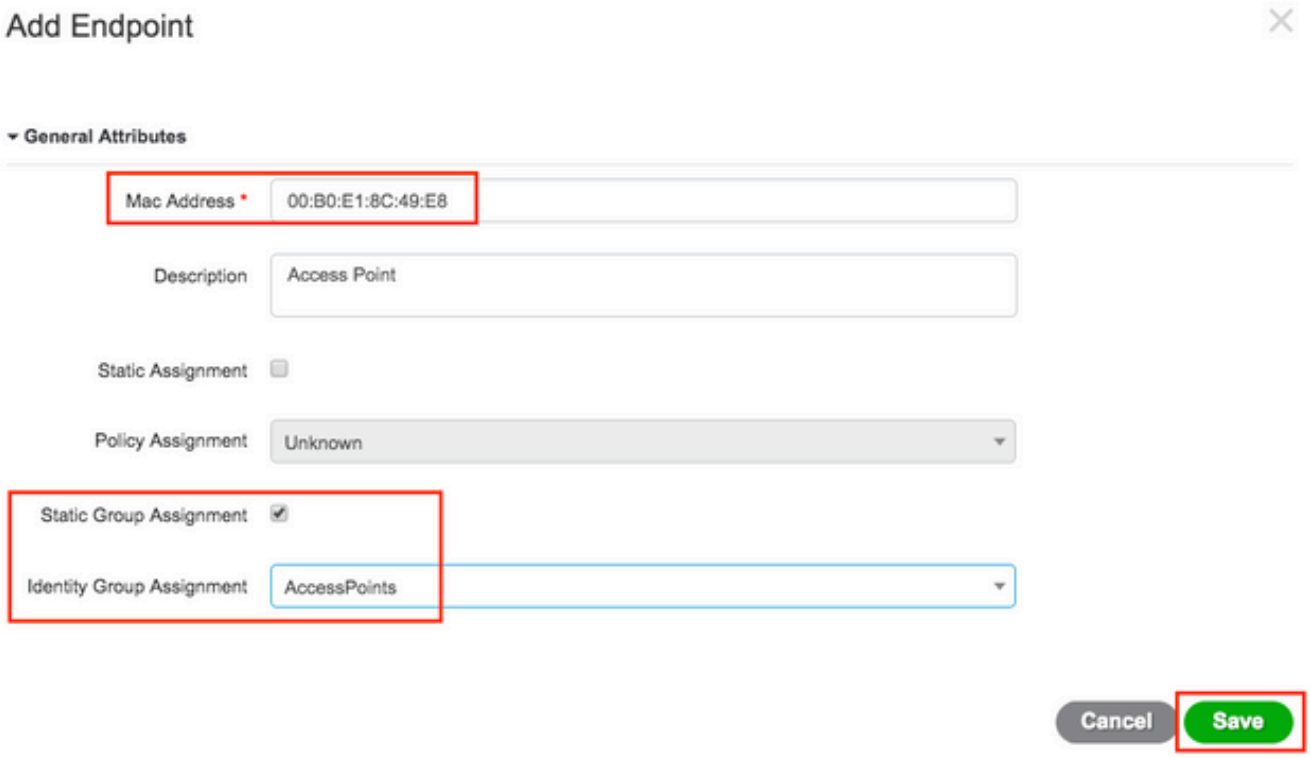


3단계. 엔드포인트 ID 그룹에 AP 이더넷 mac 주소를 추가합니다.

Work Centers(작업 센터) > Network Access(네트워크 액세스) > Identities(ID) > Endpoints(엔드포인트) > +로 이동합니다.

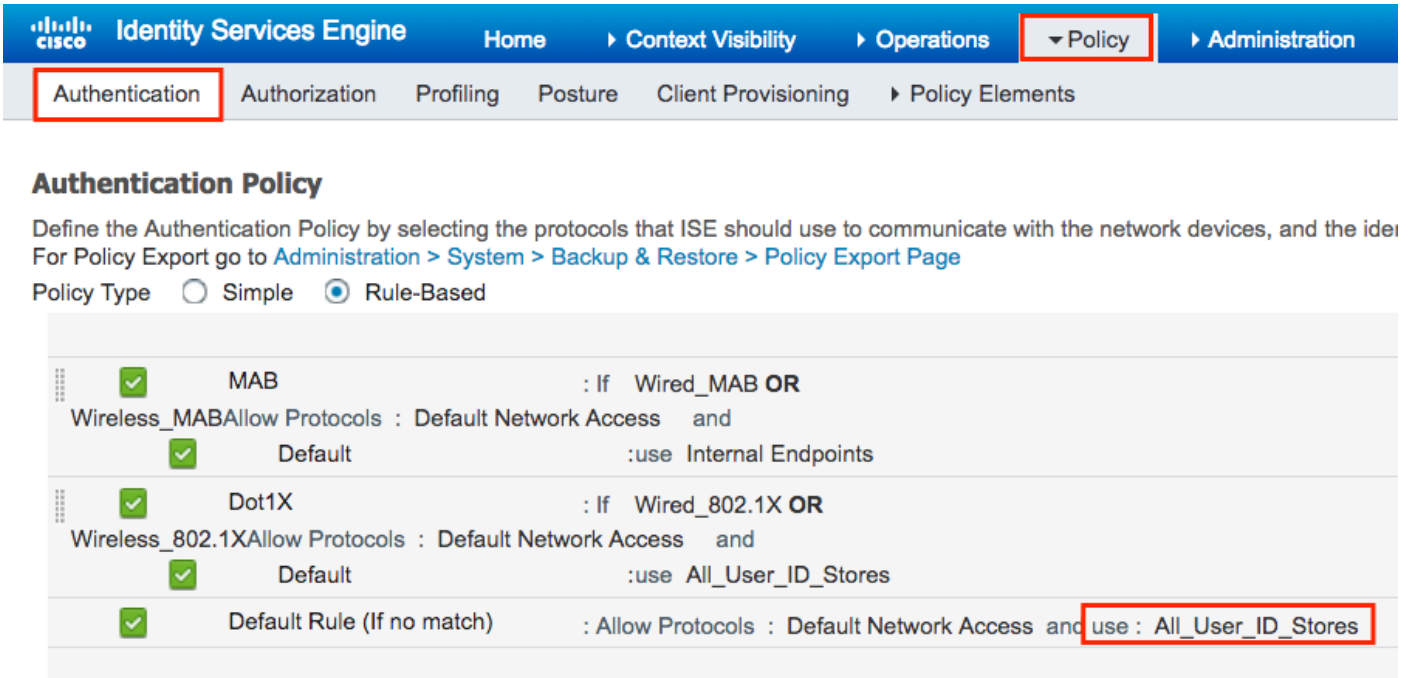


필요한 정보를 입력합니다.

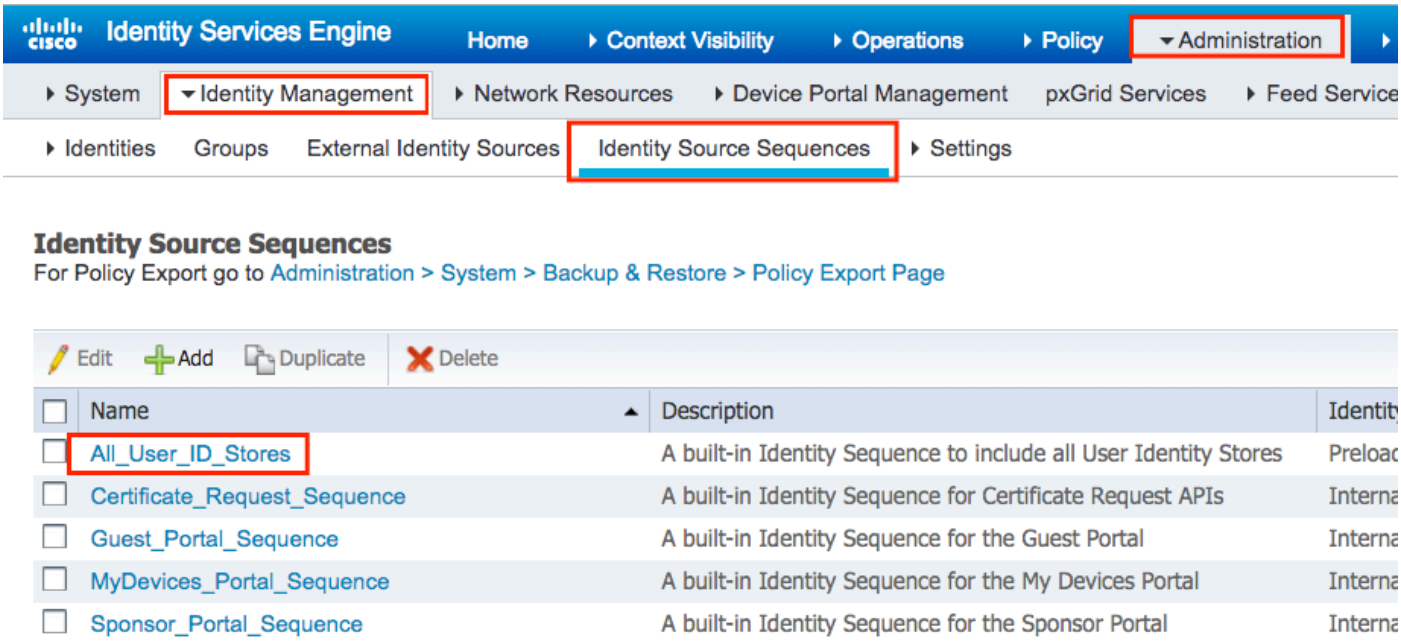


4단계. 기본 인증 규칙에 사용되는 ID 저장소에 내부 엔드포인트가 포함되어 있는지 확인합니다.

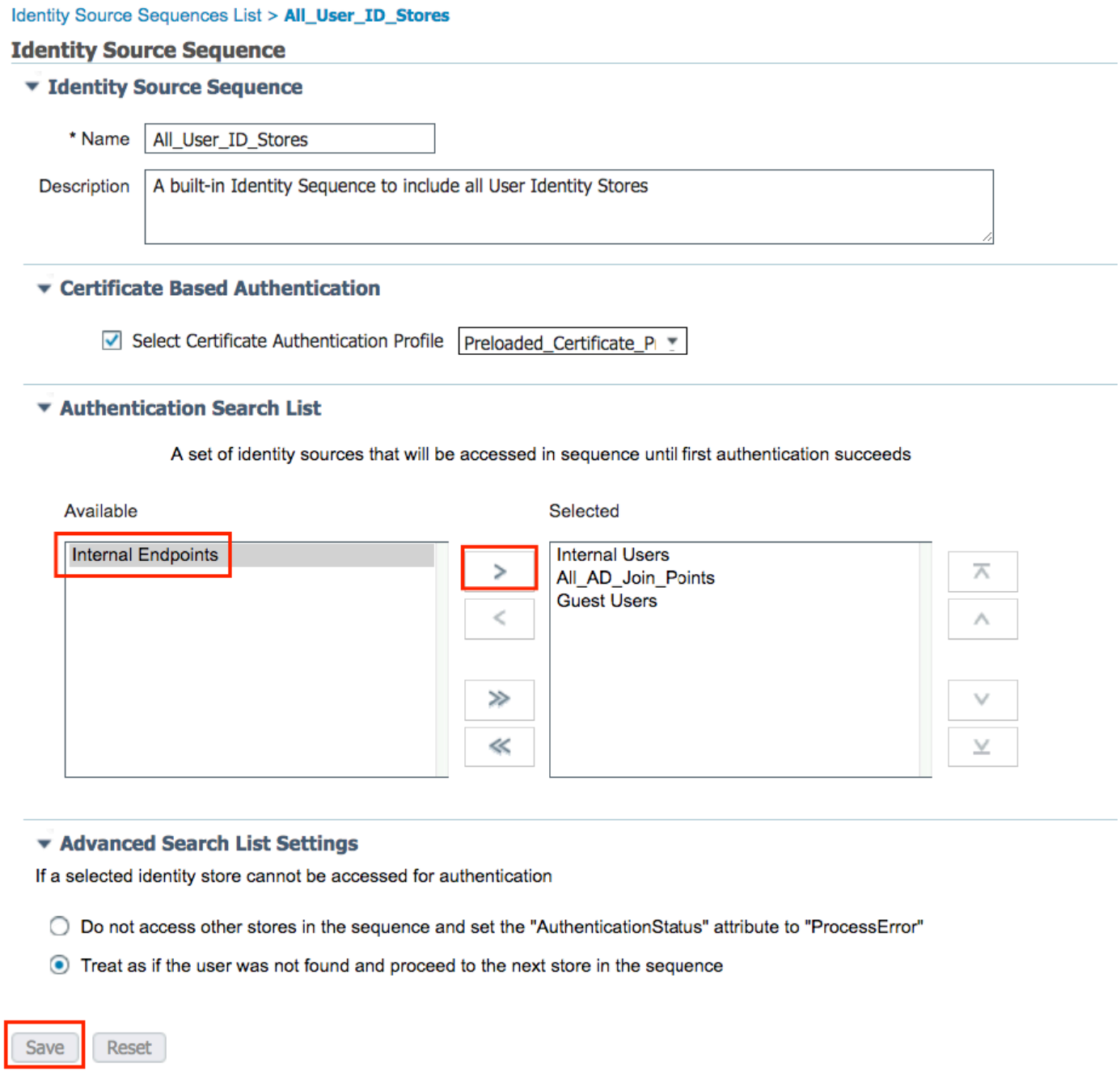
A. Policy(정책) > Authentication(인증)으로 이동하고 Identity store(ID 저장소)를 기록합니다.



B. Administration(관리) > Identity Management(ID 관리) > Identity Source Sequences(ID 소스 시퀀스) > Identity Name(ID 이름)으로 이동합니다.



C. 내부 엔드포인트가 여기에 속하는지 확인합니다(그렇지 않은 경우).



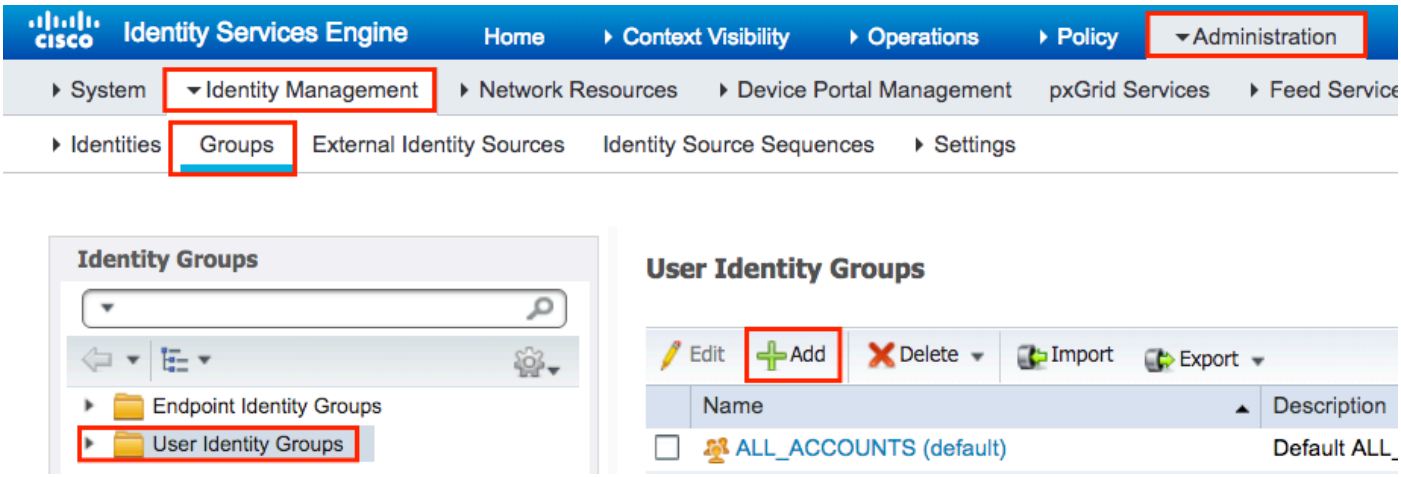
MAC 주소를 사용자 이름/비밀번호로 인증하도록 ISE 구성

이 방법은 사용자 이름과 동일한 비밀번호를 허용하기 위해 더 낮은 비밀번호 정책이 필요하므로 권장되지 않습니다.

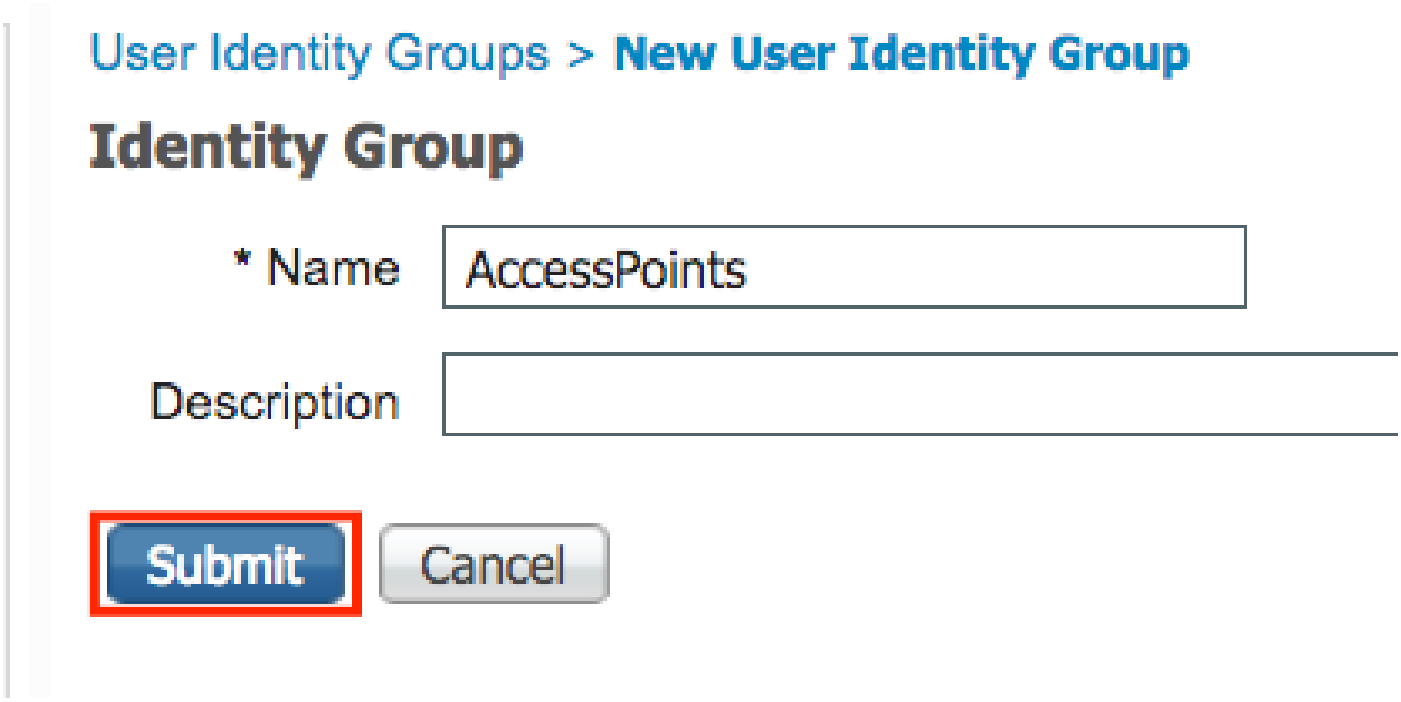
그러나 네트워크 디바이스 프로파일을 수정할 수 없는 경우에는 이 방법을 사용할 수 있습니다

2단계. (선택 사항) 액세스 포인트에 대한 ID 그룹 생성

Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹) > + Add(추가)로 이동합니다.

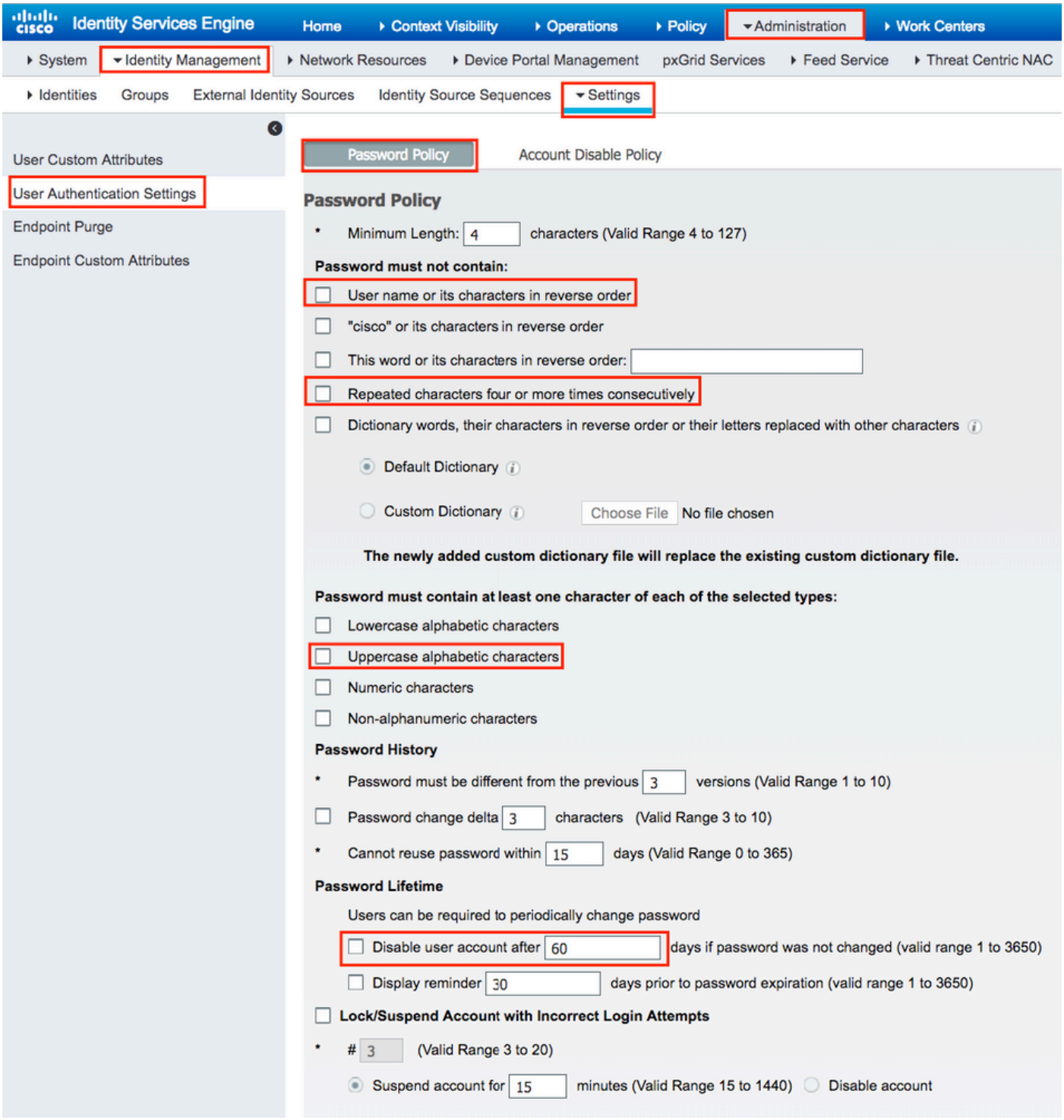


이름을 선택하고 Submit(제출)을 클릭합니다.



3단계. 현재 비밀번호 정책에서 mac 주소를 사용자 이름 및 비밀번호로 추가할 수 있는지 확인합니다.

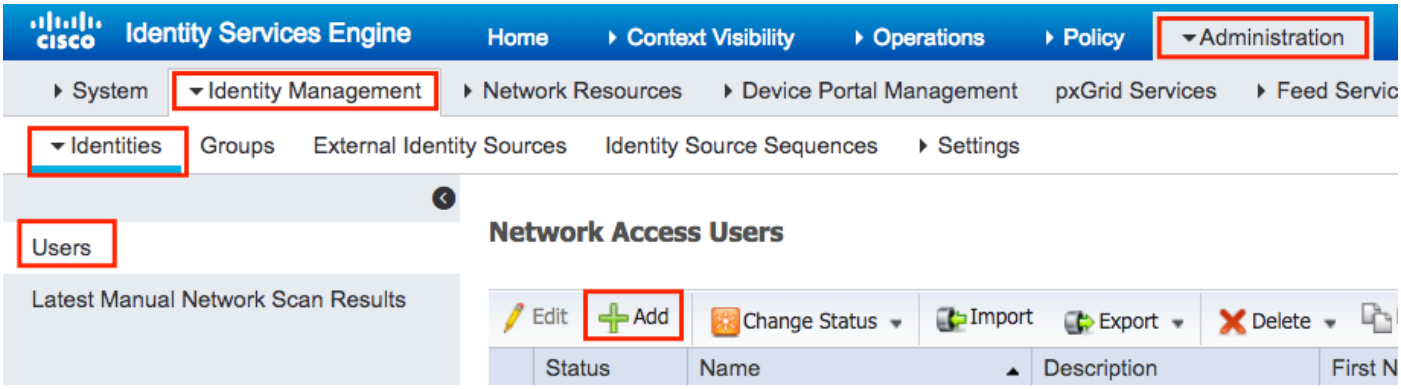
Administration > Identity Management > Settings > User Authentication Settings > Password Policy로 이동하여 다음 옵션 이상이 비활성화되었는지 확인합니다.



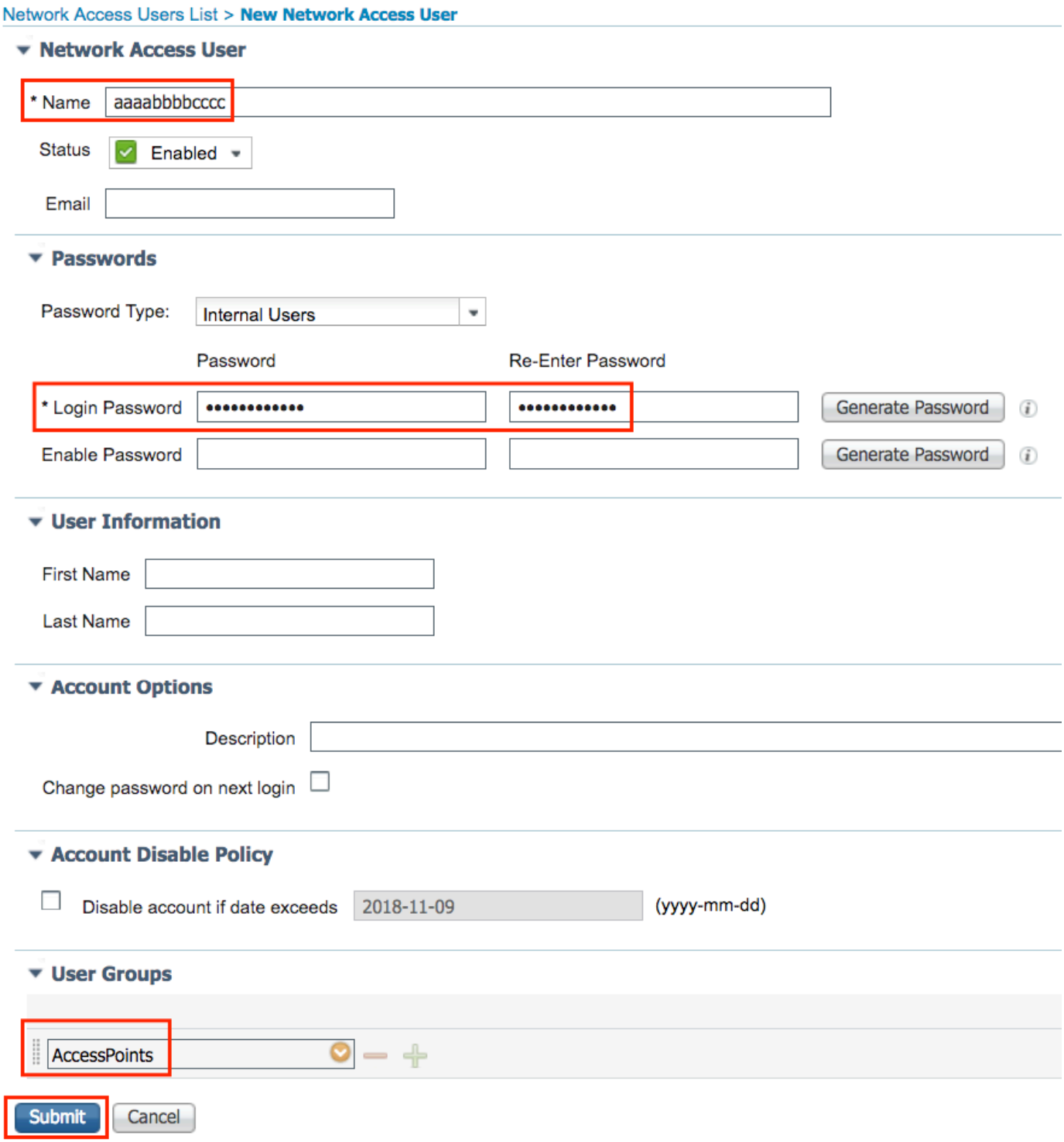
참고: 비밀번호가 변경되지 않은 경우 XX일 후 사용자 계정 비활성화 옵션을 비활성화할 수도 있습니다. mac 주소이므로 비밀번호는 변경되지 않습니다.

4단계. AP 이더넷 mac 주소를 추가합니다.

Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자) > + Add(추가)로 이동합니다.



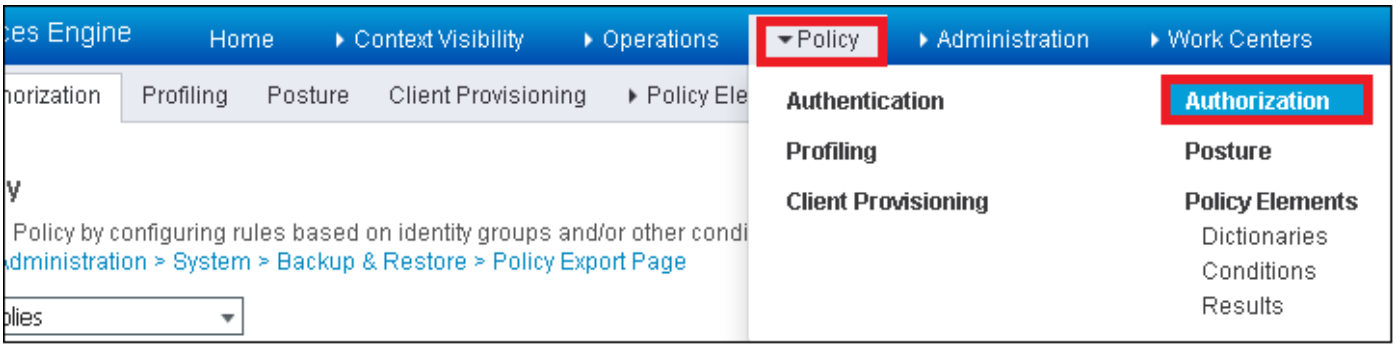
필요한 정보를 입력합니다.



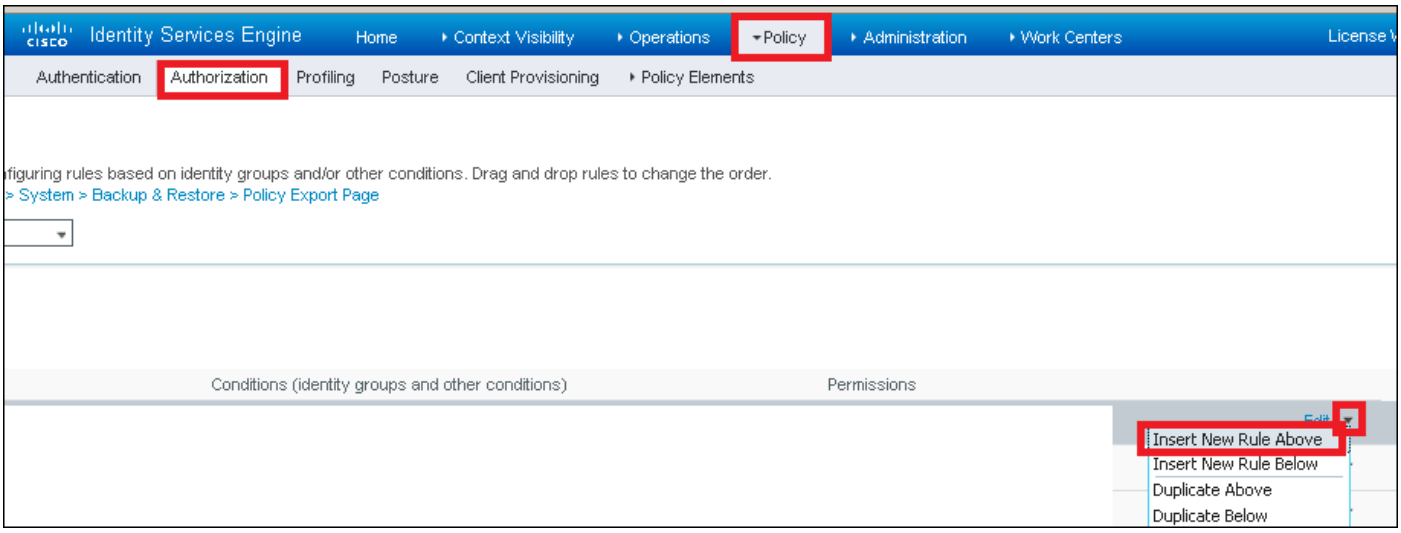
참고: Name and Login Passwordfield는 AP의 이더넷 MAC 주소여야 하며 모든 소문자를 구분하지 않아야 합니다.

AP 인증을 위한 권한 부여 정책

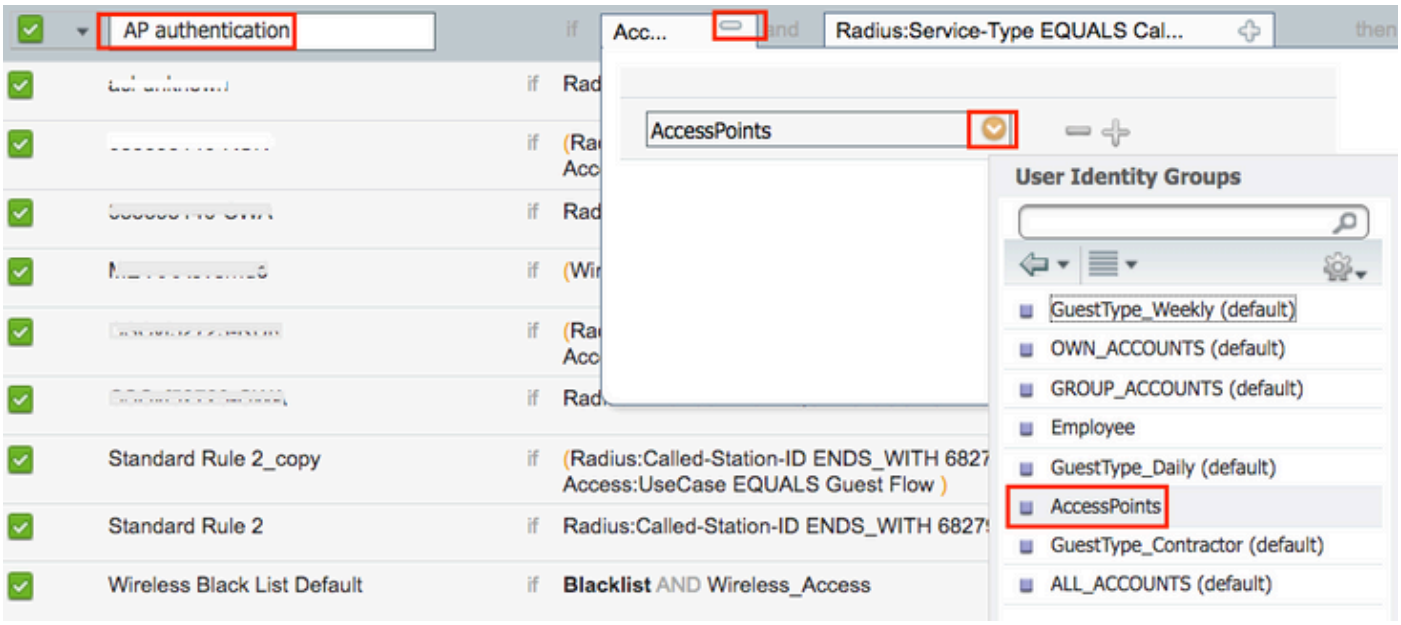
이미지에 표시된 대로 Policy(정책) > Authorization(권한 부여)으로 이동합니다.



이미지에 표시된 대로 새 규칙을 삽입합니다.

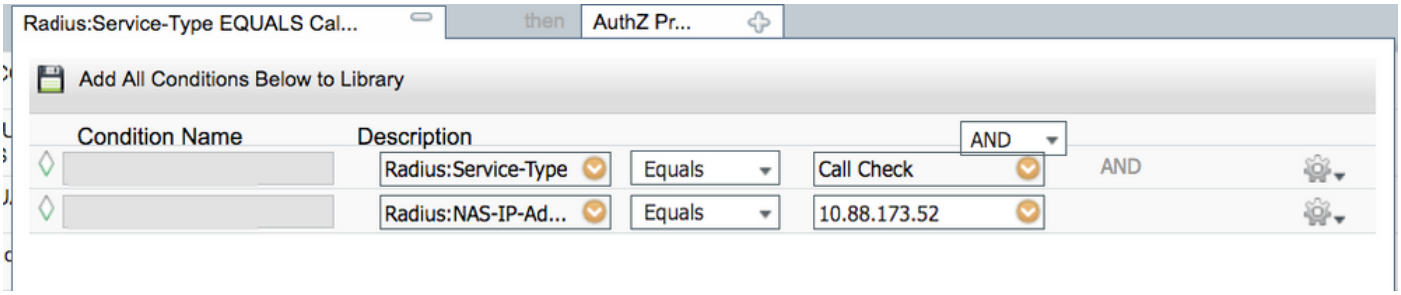


먼저 규칙의 이름과 액세스 포인트가 저장된 ID 그룹(AccessPoints)을 선택합니다. MAC 주소를 사용자 이름 비밀번호로 인증하기로 결정한 경우 User Identity Groups(사용자 ID 그룹)를 선택하고, AP MAC 주소를 엔드포인트로 인증하기로 선택한 경우 Endpoint Identity Groups(엔드포인트 ID 그룹)를 선택합니다.

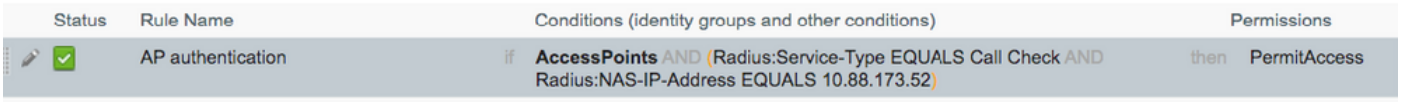


그런 다음 이 규칙에 속하도록 권한 부여 프로세스를 수행하는 다른 조건을 선택합니다. 이 예에서는 권한 부여 프로세스가 서비스 유형 통화 확인을 사용하고 인증 요청이 IP 주소 10.88.173.52에서

오는 경우 이 규칙에 부합합니다.



마지막으로, 해당 규칙에 도달한 클라이언트에 할당된 권한 부여 프로파일을 선택하고 Done을 클릭한 다음 이미지에 표시된 대로 저장합니다.



참고: 컨트롤러에 이미 연결된 AP의 연결이 끊어지지 않습니다. 그러나 권한 부여 목록이 활성화된 후 컨트롤러와의 통신이 끊기고 다시 참가를 시도하면 인증 프로세스가 진행됩니다. 해당 mac 주소가 로컬로 또는 RADIUS 서버에 나열되지 않으면 컨트롤러에 다시 조인할 수 없습니다.

다음을 확인합니다.

9800 WLC에서 ap 인증 목록을 활성화했는지 확인합니다.

<#root>

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

RADIUS 컨피그레이션을 확인합니다.

<#root>

```
#
show run aaa
```

문제 해결

WLC 9800은 ALWAYS-ON 추적 기능을 제공합니다. 이렇게 하면 모든 AP 가입 관련 오류, 경고 및 알림 수준 메시지가 지속적으로 로깅되며, 사고 또는 장애 발생 후 상황에 대한 로그를 볼 수 있습니다.

참고: 생성된 로그의 볼륨은 몇 시간에서 며칠로 거꾸로 바뀝니다.

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

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

```
# show clock
```

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

```
# show logging
```

3단계. 디버그 조건이 활성화되었는지 확인합니다.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Trace Configs:


Packet Infra debugs:

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

참고: 어떤 조건도 나열되어 있으면, 그 추적은 활성화된 조건(mac 주소, ip 주소 등)이 발생하는 모든 프로세스의 디버그 레벨로 로깅됨을 의미합니다. 이로 인해 로그의 볼륨이 증가합니다. 따라서 적극적으로 디버깅하지 않을 때는 모든 조건을 지우는 것이 좋습니다.

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

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

세션의 콘텐츠를 표시하거나 파일을 외부 TFTP 서버에 복사할 수 있습니다.

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

조건부 디버깅 및 무선 활성 추적

Always-on 추적을 통해 조사 중인 문제의 트리거를 확인할 수 있는 충분한 정보가 제공되지 않을 경우, 조건부 디버깅을 활성화하고 RA(Radio Active) 추적을 캡처할 수 있습니다. 그러면 지정된 조건(이 경우 클라이언트 mac 주소)과 상호 작용하는 모든 프로세스에 대한 디버그 레벨 추적이 제공됩니다.

5단계. 활성화된 디버그 조건이 없는지 확인합니다.

```
# clear platform condition all
```

6단계. 모니터링할 무선 클라이언트 mac 주소에 대한 디버그 조건을 활성화합니다.

이 명령은 제공된 mac 주소를 30분(1800초) 동안 모니터링하기 시작합니다. 선택적으로 이 시간을 최대 2,085,978,494초까지 늘릴 수 있습니다.

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

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

참고: 모든 것이 나중에 볼 수 있도록 내부적으로 버퍼링되므로 터미널 세션에서 클라이언트 활동의 출력이 표시되지 않습니다.

7단계. 모니터링할 문제나 동작을 재현합니다.

8단계. 기본 또는 구성된 모니터 시간이 끝나기 전에 문제가 재현되는 경우 디버그를 중지합니다.

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

모니터링 시간이 경과하거나 무선 디버그가 중단되면 9800 WLC는 다음과 같은 이름의 로컬 파일을 생성합니다.

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

9단계. MAC 주소 활동의 파일을 수집합니다. RA 추적 .log를 외부 서버에 복사하거나 출력을 화면에 직접 표시할 수 있습니다.

RA 추적 파일의 이름을 확인합니다

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

파일을 외부 서버에 복사:

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

콘텐츠 표시:

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

10단계. 근본 원인이 아직 명확하지 않은 경우 디버그 레벨 로그를 더 자세히 보여주는 내부 로그를 수집합니다. 이미 수집되어 내부적으로 저장된 디버그 로그만 더 자세히 살펴볼 것이므로 클라이언트를 다시 디버깅할 필요는 없습니다.

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

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

---

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

파일을 외부 서버에 복사:

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

콘텐츠 표시:

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

11단계. 디버그 조건을 제거합니다.

```
# clear platform condition all
```

참고: 트러블슈팅 세션 후에는 항상 디버그 조건을 제거해야 합니다.

참조

메시 AP를 9800 WLC에 연결

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.