통합 무선 네트워크에서 액세스 포인트 권한 부여 구성

목차

소개

이 문서에서는 AP의 MAC 주소를 기반으로 액세스 포인트(AP)에 권한을 부여하도록 WLC를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE(Identity Services Engine) 구성 방법에 대한 기본 지식
- Cisco AP 및 Cisco WLC 컨피그레이션에 대한 지식
- Cisco Unified Wireless Security 솔루션에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AireOS 8.8.111.0 소프트웨어를 실행하는 WLC1차 AP: 1700/2700/3700 및

3500(1600/2600/3600은 계속 지원되지만 AireOS 지원은 버전 8.5.x에서 끝남)Wave2 AP: 1800/2800/3800/4800, 1540 및 1560 ISE 버전 2.3.0.298

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.

경량 AP 권한 부여

AP 등록 프로세스 중에 AP와 WLC는 X.509 인증서를 사용하여 상호 인증합니다. X.509 인증서는 Cisco에서 공장에서 AP 및 WLC의 보호된 플래시에 번들로 구성합니다.

AP에서 공장 출하 시 설치된 인증서를 MIC(제조 설치 인증서)라고 합니다. 2005년 7월 18일 이후에 제조된 모든 Cisco AP에는 MIC가 있습니다.

등록 프로세스 중에 발생하는 이러한 상호 인증 외에도, WLC는 AP의 MAC 주소를 기반으로 등록하는 AP를 제한할 수도 있습니다.

컨트롤러가 RADIUS 서버를 통해 AP를 승인하기 전에 MIC를 사용하여 AP를 인증하므로 AP MAC 주소를 사용할 때 강력한 비밀번호가 없는 것은 문제가 되지 않습니다. MIC를 사용하면 강력한 인증이 제공됩니다.

AP 권한 부여는 두 가지 방법으로 수행할 수 있습니다.

- WLC에서 내부 권한 부여 목록 사용
- AAA 서버에서 MAC 주소 데이터베이스 사용

AP의 동작은 사용된 인증서에 따라 다릅니다.

- SSC가 있는 AP - WLC는 내부 권한 부여 목록만 사용하며 이러한 AP에 대한 요청을 RADIUS 서버에 전달하지 않습니다
- MIC가 있는 AP - WLC는 WLC에 구성된 내부 권한 부여 목록을 사용하거나 RADIUS 서버를 사용하여 AP에 권한을 부여할 수 있습니다

이 문서에서는 내부 권한 부여 목록 및 AAA 서버를 모두 사용하는 AP 권한 부여에 대해 설명합니다
.

구성

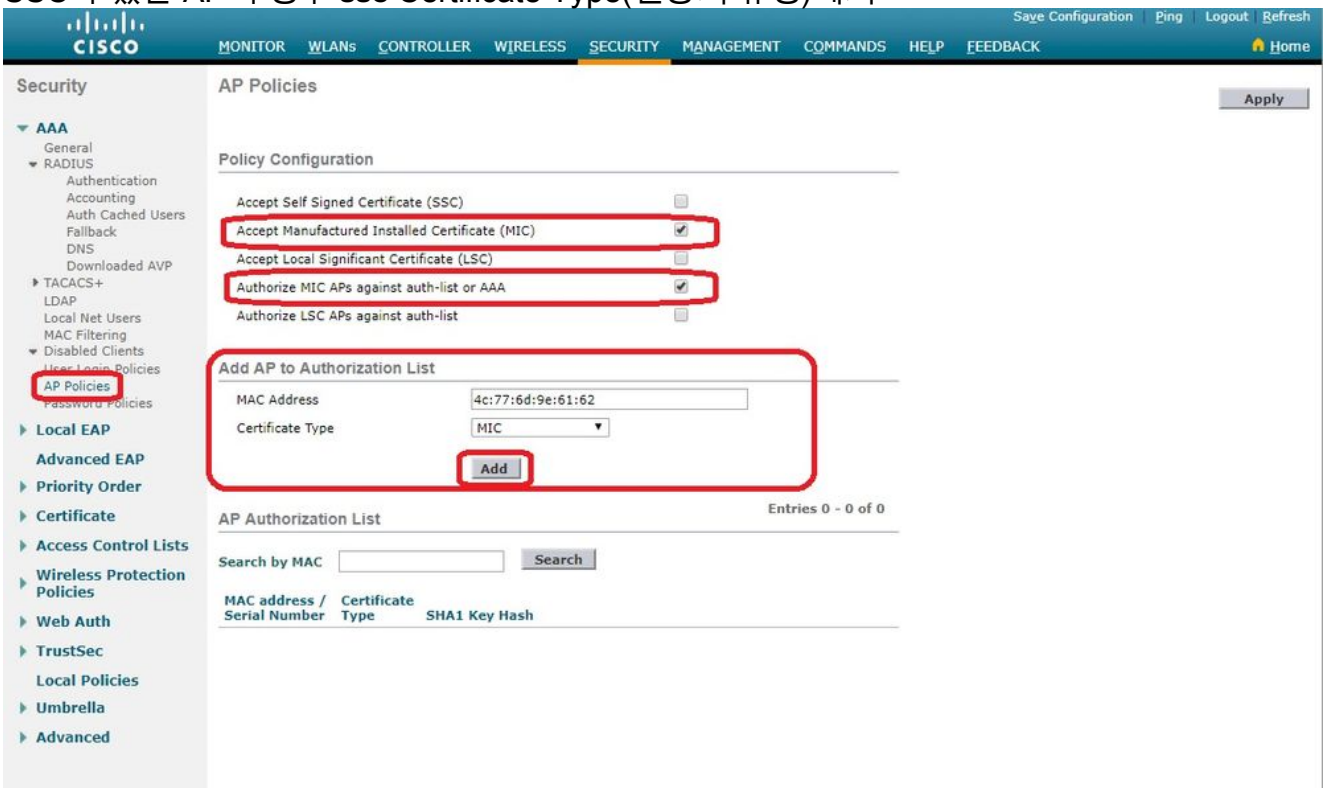
WLC의 내부 권한 부여 목록을 사용한 컨피그레이션

WLC에서 MAC 주소를 기반으로 AP를 제한하려면 AP 권한 부여 목록을 사용합니다. AP 권한 부여 목록은 **Security > AP Policies** 있습니다.

이 예에서는 MAC 주소가 있는 AP를 추가하는 방법을 보여 줍니다 **4c:77:6d:9e:61:62.**

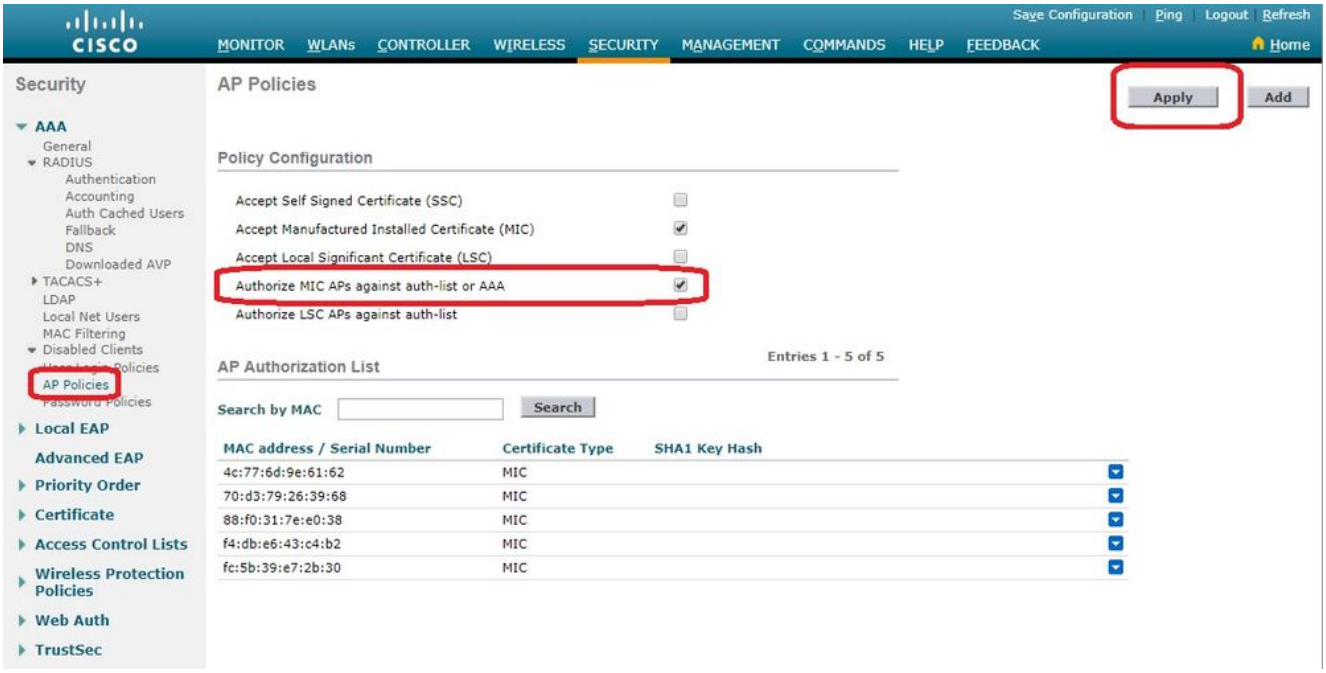
1. WLC 컨트롤러 GUI에서 **Security > AP Policies** AP Policies 페이지가 나타납니다.
2. 다음을 클릭합니다. **Add** 화면의 오른쪽에 있는 버튼

3. 아래 **Add AP to Authorization List**를 입력합니다. **AP MAC** 주소(AP 무선 mac 주소가 아님). 그런 다음 인증서 유형을 선택하고 **Add**.이 예에서는 MIC 인증서가 있는 AP가 추가됩니다.**참고:** SSC가 있는 AP의 경우 ssc Certificate Type(인증서 유형)에서



AP가 AP 권한 부여 목록에 추가되고 **AP Authorization List.**

4. Policy Configuration(정책 컨피그레이션)에서 **Authorize MIC APs against auth-list or AAA.**이 매개변수를 선택하면 WLC가 먼저 로컬 권한 부여 목록을 확인합니다. AP MAC가 없는 경우 RADIUS 서버를 확인합니다.



다음을 확인합니다.

이 컨피그레이션을 확인하려면 MAC 주소로 AP를 연결해야 합니다 **4c:77:6d:9e:61:62** 네트워크 및 모니터에 연결합니다. 이 **debug capwap events/errors enable** 및 **debug aaa all enable** 명령을 사용합니다.

이 출력은 AP MAC 주소가 AP 권한 부여 목록에 없는 경우 디버그를 표시합니다.

참고: 공간 제약 조건으로 인해 출력의 일부 행이 두 번째 행으로 이동되었습니다.

```
(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 Allocate database entry for AP
192.168.79.151:5256, already allocated index 277

*spamApTask4: Feb 27 10:15:25.592: 70:69:5a:51:4e:c0 AP Allocate request at index 277 (reserved)
*spamApTask4: Feb 27 10:15:25.593: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Dropping request or response packet to AP
:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP
70:69:5a:51:4e:c0
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Request failed!
```

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5256

*aaaQueueReader: Feb 27 10:15:25.593: **Unable to find requested user entry for 4c776d9e6162**
*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9
*aaaQueueReader: Feb 27 10:15:25.593: ReProcessAuthentication previous proto 8, next proto 40000001
*aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638

*aaaQueueReader: Feb 27 10:15:25.593: Callback.....0xd6cef02166

*aaaQueueReader: Feb 27 10:15:25.593: protocolType.....0x40000001

*aaaQueueReader: Feb 27 10:15:25.593:
proxyState.....70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 9 AVPs:

*aaaQueueReader: Feb 27 10:15:25.593: AVP[01] User-Name.....4c776d9e6162 (12 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[02] Called-Station-Id.....70-69-5a-51-4e-c0 (17 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[03] Calling-Station-Id.....4c-77-6d-9e-61-62 (17 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[06] NAS-Identifier.....0x6e6f (28271) (2 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[07] User-Password.....[...]

*aaaQueueReader: Feb 27 10:15:25.593: AVP[08] Service-Type.....0x0000000a (10) (4 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: AVP[09] Message-Authenticator.....DATA (16 bytes)

*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Error Response code for AAA Authentication : -7
*aaaQueueReader: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Returning AAA Error 'No Server' (-7) for mobile 70:69:5a:51:4e:c0 serverIdx 0
*aaaQueueReader: Feb 27 10:15:25.593: AuthorizationResponse: 0x7f017adf5770

*aaaQueueReader: Feb 27 10:15:25.593: RadiusIndexSet(0), Index(0)
*aaaQueueReader: Feb 27 10:15:25.593: resultCode.....-7

*aaaQueueReader: Feb 27 10:15:25.593: protocolUsed.....0xffffffff

*aaaQueueReader: Feb 27 10:15:25.593:
proxyState.....70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 10:15:25.593: Packet contains 0 AVPs:

*aaaQueueReader: Feb 27 10:15:25.593: **70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.**

```
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 10:15:25.593: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Join Failure Response sent to 0.0.0.0:5256

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Radius Authentication failed. Closing dtls
Connection.
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Disconnecting DTLS Capwap-Ctrl session
0xd6f0724fd8 for AP (192:168:79:151/5256). Notify(true)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 CAPWAP State: Dtls tear down

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 acDtlsPlumbControlPlaneKeys:
lrad:192.168.79.151(5256) mwar:10.48.71.20(5246)

*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS keys for Control Plane deleted
successfully for AP 192.168.79.151

*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 DTLS connection closed event receivedserver
(10.48.71.20/5246) client (192.168.79.151/5256)
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Entry exists for AP (192.168.79.151/5256)
*spamApTask0: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 AP Delete request
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 Unable to find AP 70:69:5a:51:4e:c0
*spamApTask4: Feb 27 10:15:25.593: 70:69:5a:51:4e:c0 No AP entry exist in temporary database for
192.168.79.151:5256
```

이 출력은 LAP MAC 주소가 AP 권한 부여 목록에 추가될 때의 디버그를 보여줍니다.

참고: 공간 제약 조건으로 인해 출력의 일부 행이 두 번째 행으로 이동되었습니다.

```
(Cisco Controller) >debug capwap events enable
(Cisco Controller) >debug capwap errors enable
(Cisco Controller) >debug aaa all enable

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5256

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 using already alloced index 274
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Allocate database entry for AP
192.168.79.151:5256, already allocated index 274

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP Allocate request at index 274 (reserved)
*spamApTask4: Feb 27 09:50:25.393: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5256 from
temporary database.
*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 AP group received default-group is found in
ap group configured in wlc.

*spamApTask4: Feb 27 09:50:25.393: 70:69:5a:51:4e:c0 Dropping request or response packet to AP
:192.168.79.151 (5256) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response,
state Capwap_no_state

*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is
not allowed to send in state Capwap_no_state for AP 192.168.79.151
```

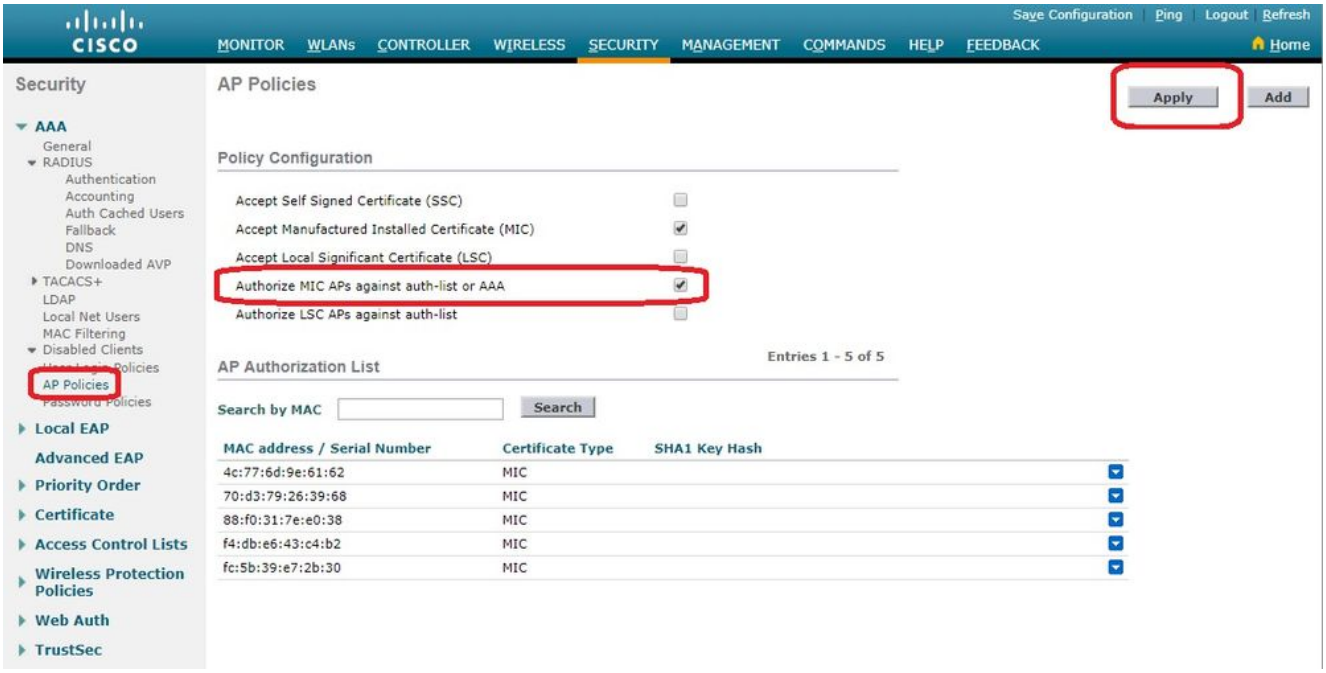
```
*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 In AAA state 'Idle' for AP
70:69:5a:51:4e:c0
*spamApTask4: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Request failed!


*aaaQueueReader: Feb 27 09:50:25.394: User 4c776d9e6162 authenticated
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Normal Response code for AAA
Authentication : 0
*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Returning AAA Success for mobile
70:69:5a:51:4e:c0
*aaaQueueReader: Feb 27 09:50:25.394: AuthorizationResponse: 0x7f0288a66408


*aaaQueueReader: Feb 27 09:50:25.394: structureSize.............................194

*aaaQueueReader: Feb 27 09:50:25.394: resultCode.................................0

*aaaQueueReader: Feb 27 09:50:25.394:
proxyState.................................70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 09:50:25.394: Packet contains 2 AVPs:

*aaaQueueReader: Feb 27 09:50:25.394: AVP[01] Service-
Type.........................0x00000065 (101) (4 bytes)

*aaaQueueReader: Feb 27 09:50:25.394: AVP[02] Airespace / WLAN-
Identifier.............0x00000000 (0) (4 bytes)

*aaaQueueReader: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 User authentication Success with File DB
on WLAN ID :0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 09:50:25.394: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5256

*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 CAPWAP State: Join

*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 capwap_ac_platform.c:2095 - Operation State
0 ===> 4
*spamApTask0: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Capwap State Change Event (Reg) from
capwap_ac_platform.c 2136

*apfReceiveTask: Feb 27 09:50:25.394: 70:69:5a:51:4e:c0 Register LWAPP event for AP
70:69:5a:51:4e:c0 slot 0
```

AAA 서버에 대한 AP 권한 부여

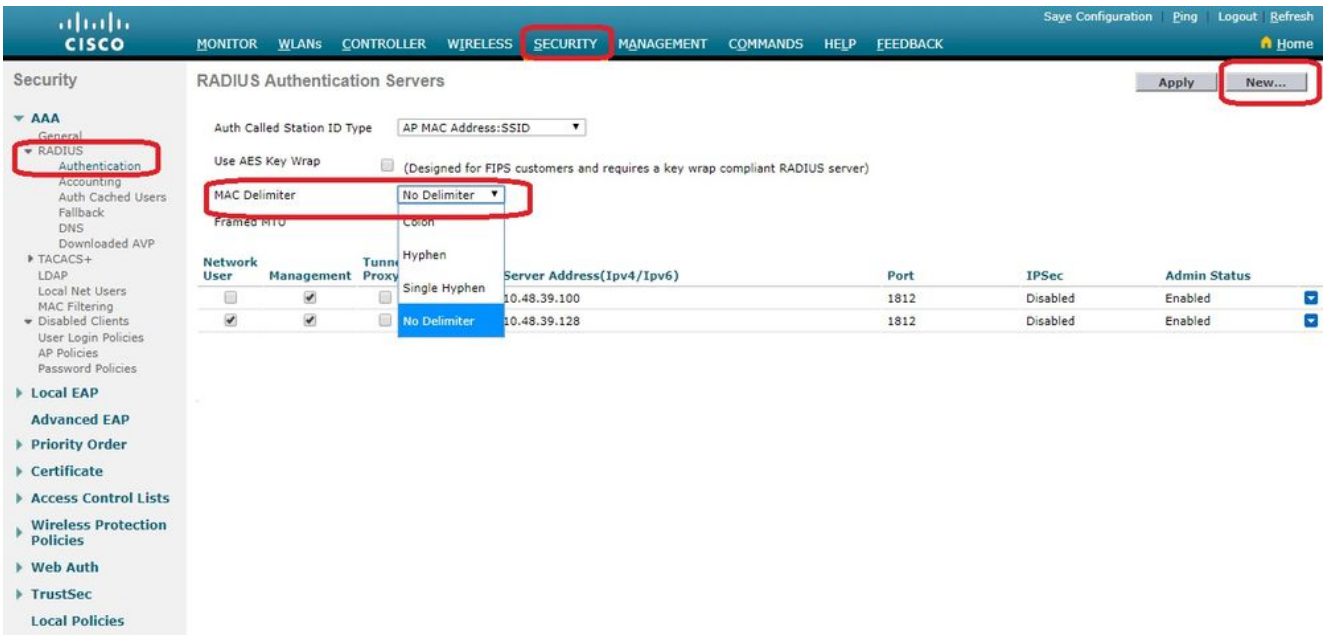
RADIUS 서버를 사용하여 MIC를 사용하는 AP에 권한을 부여하도록 WLC를 구성할 수도 있습니다. WLC는 RADIUS 서버에 정보를 보낼 때 AP MAC 주소를 사용자 이름과 비밀번호로 모두 사용합니다. 예를 들어 AP의 MAC 주소가 **4c:77:6d:9e:61:62**, 컨트롤러에서 AP에 권한을 부여하는 데 사용하는 사용자 이름과 비밀번호는 모두 정의된 delimeter를 사용하는 mac 주소입니다.

이 예에서는 Cisco ISE를 사용하여 AP에 권한을 부여하도록 WLC를 구성하는 방법을 보여줍니다.

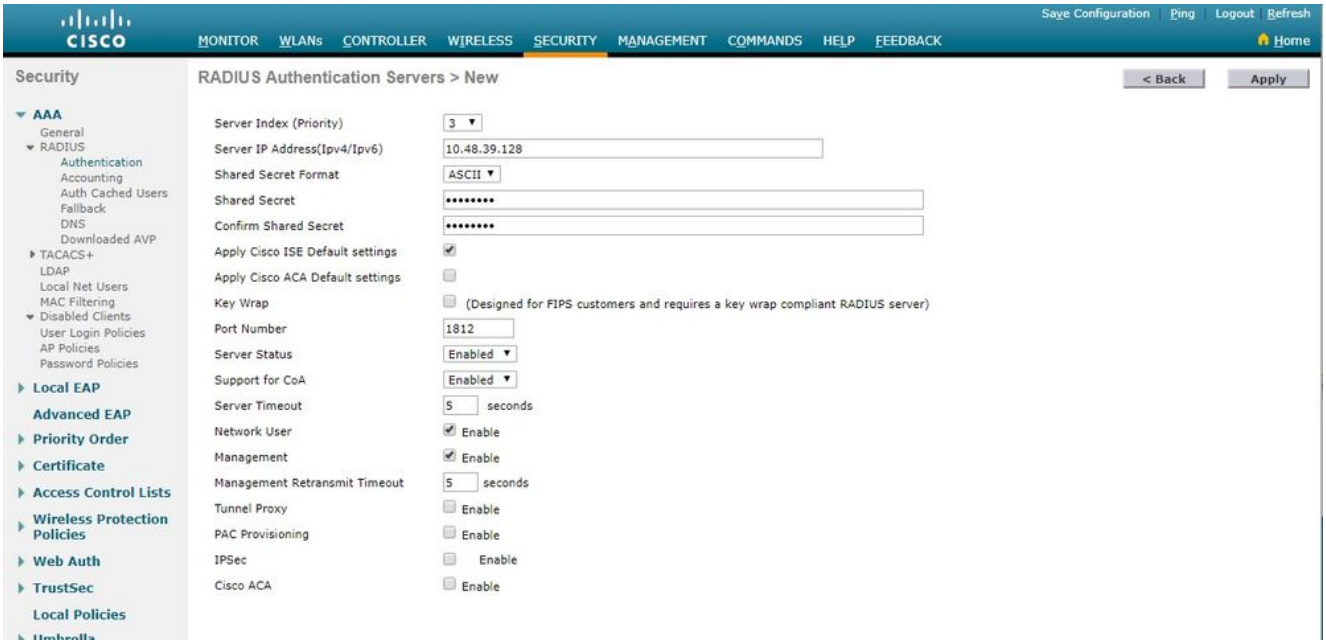
1. WLC 컨트롤러 GUI에서 **Security > AP Policies**. AP Policies 페이지가 나타납니다.
2. Policy Configuration(정책 컨피그레이션)에서 **Authorize MIC APs against auth-list or AAA**.이 매개변수를 선택하면 WLC가 먼저 로컬 권한 부여 목록을 확인합니다. AP MAC가 없는 경우 RADIUS 서버를 확인합니다.



3. 탐색 **Security > RADIUS Authentication** 컨트롤러 GUI에서 **RADIUS Authentication Servers** 페이지. 이 페이지에서 **MAC** 구분 기호를 정의할 수 **있습니다**. WLC는 AP Mac 주소를 가져온 다음 여기에 정의된 구분 기호를 사용하여 Radius 서버로 전송합니다. 사용자 이름이 Radius 서버에 구성된 것과 일치해야 합니다. 이 예에서는 **No Delimiter** 사용자 이름이 **4c776d9e6162.**



4. 그런 다음 **New** RADIUS 서버를 정의합니다.



5. 에서 RADIUS 서버 매개변수를 정의합니다. **RADIUS Authentication Servers > New** 페이지. 이러한 매개변수에는 RADIUS가 포함됩니다 **Server IP Address**, **Shared Secret**, **Port Number**및 **Server Status**. 완료되면 **Apply**. 이 예에서는 IP 주소가 10.48.39.128인 RADIUS 서버로 Cisco ISE를 사용합니다 .

Cisco ISE가 AP를 인증하도록 구성

Cisco ISE가 AP를 인증하도록 하려면 다음 단계를 완료해야 합니다.

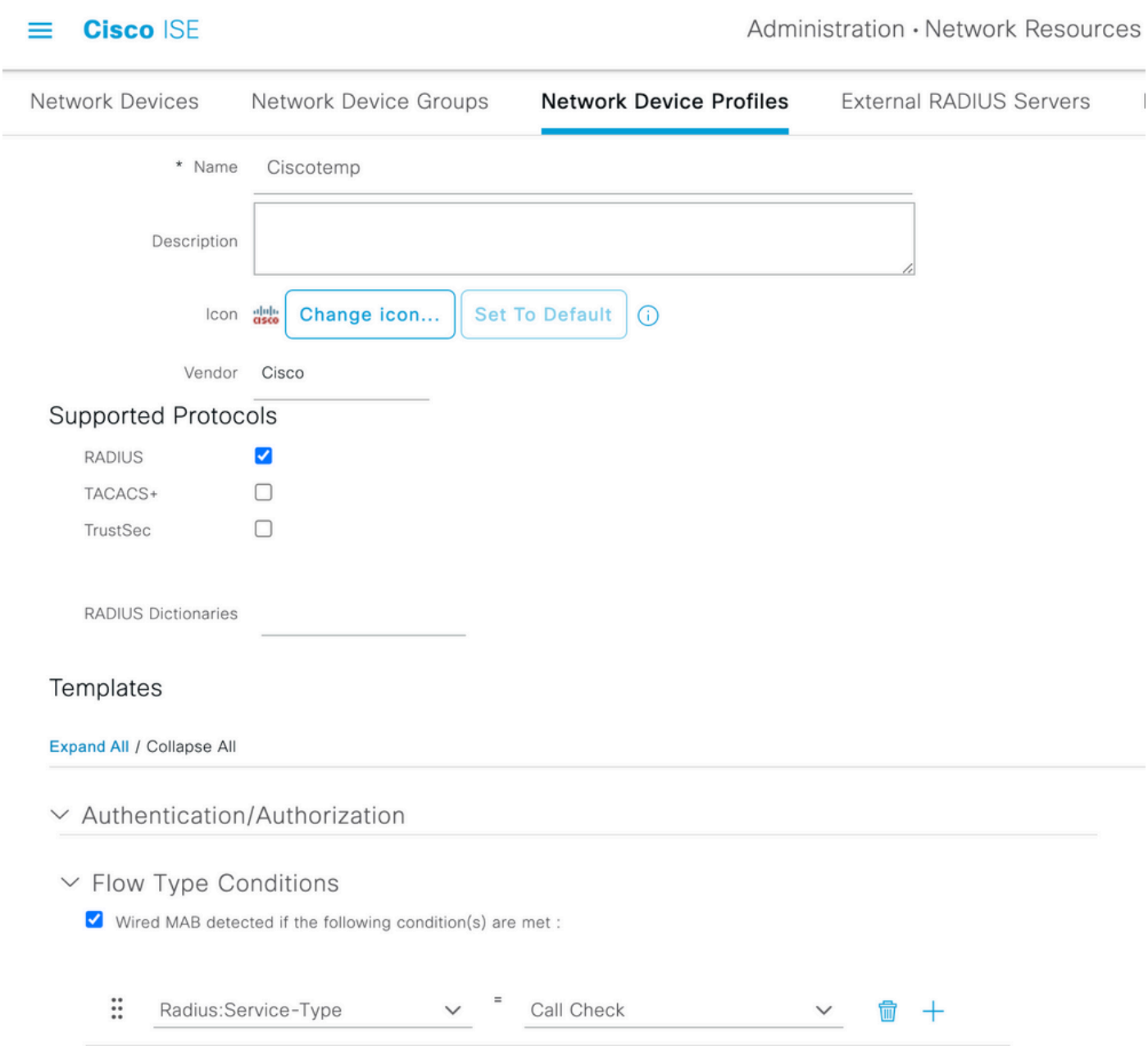
1. Cisco ISE에서 WLC를 AAA 클라이언트로 구성합니다.
2. Cisco ISE의 데이터베이스에 AP MAC 주소를 추가합니다.

그러나 AP MAC 주소를 엔드포인트(최상의 방법) 또는 사용자(비밀번호가 MAC 주소인 사용자)로 추가할 수 있지만, 이 경우 비밀번호 보안 정책 요구 사항을 줄여야 합니다.

WLC가 MAB(Mac 주소 인증) 워크플로와 일치하는 ISE의 요구 사항인 NAS-Port-Type 특성을 전송하지 않기 때문에 이를 조정해야 합니다.

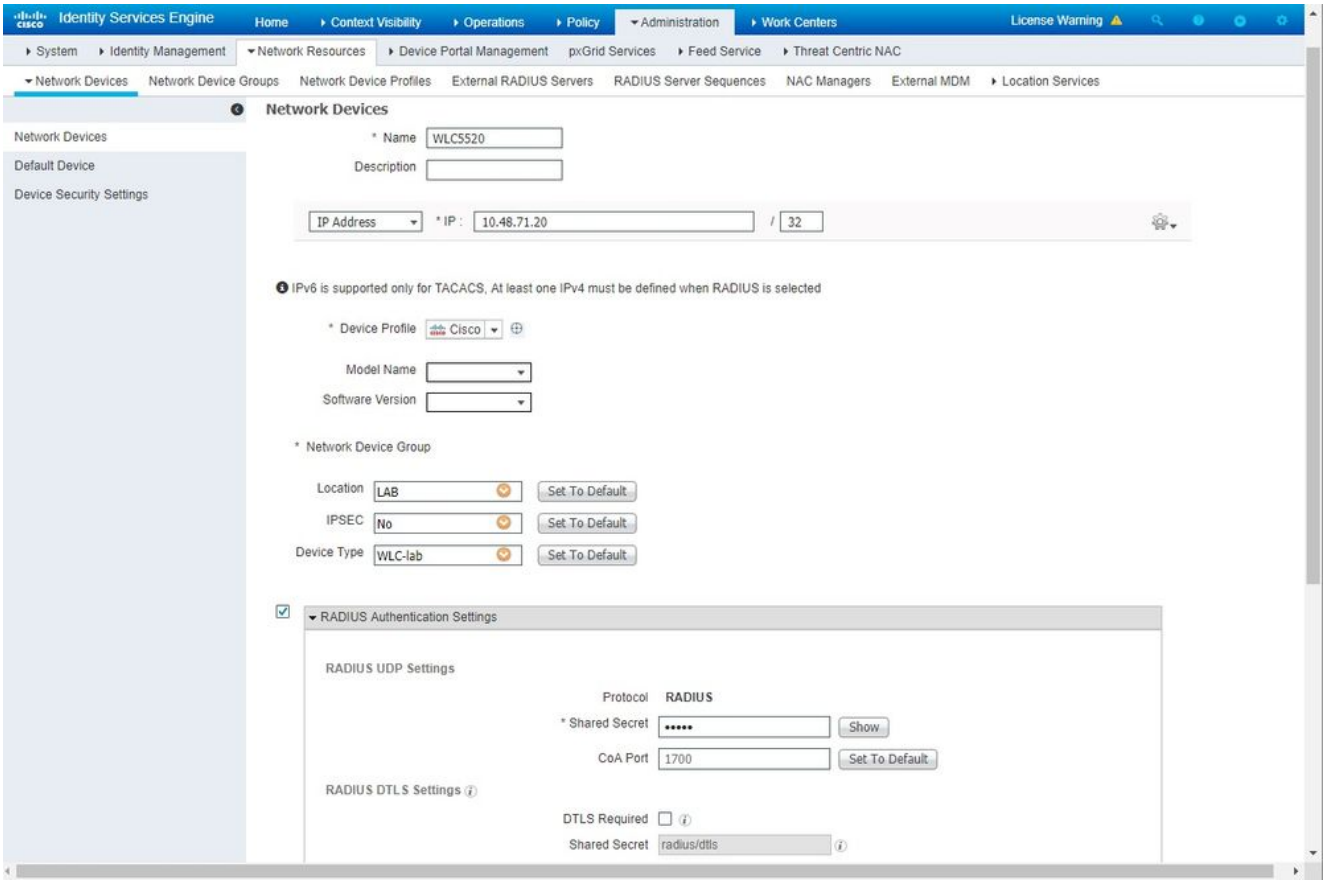
MAB에 NAS-Port-Type 특성이 필요하지 않은 새 디바이스 프로파일 구성

탐색 **Administration > Network device profile** 새 디바이스 프로필을 생성합니다. 이미지에 표시된 대로 RADIUS를 활성화하고 유선 MAB 플로우를 service-type=Call-check가 필요하도록 설정합니다. 기존 Cisco 프로필에서 다른 설정을 복사할 수 있지만 유선 MAB 워크플로에 'Nas-port-type' 특성이 필요하지 않습니다.



Cisco ISE에서 WLC를 AAA 클라이언트로 구성

1. 이동 **Administration > Network Resources > Network Devices > Add**. New Network Device 페이지가 나타납니다.
2. 이 페이지에서 WLC를 정의합니다 **Name**, 관리 인터페이스 **IP Address** 및 **Radius Authentications Settings** 좋아요 **Shared Secret**. AP MAC 주소를 엔드포인트로 입력할 계획이라면 기본 Cisco 프로필이 아닌 이전에 구성된 맞춤형 디바이스 프로필을 사용해야 합니다.



3. 클릭 **Submit**.

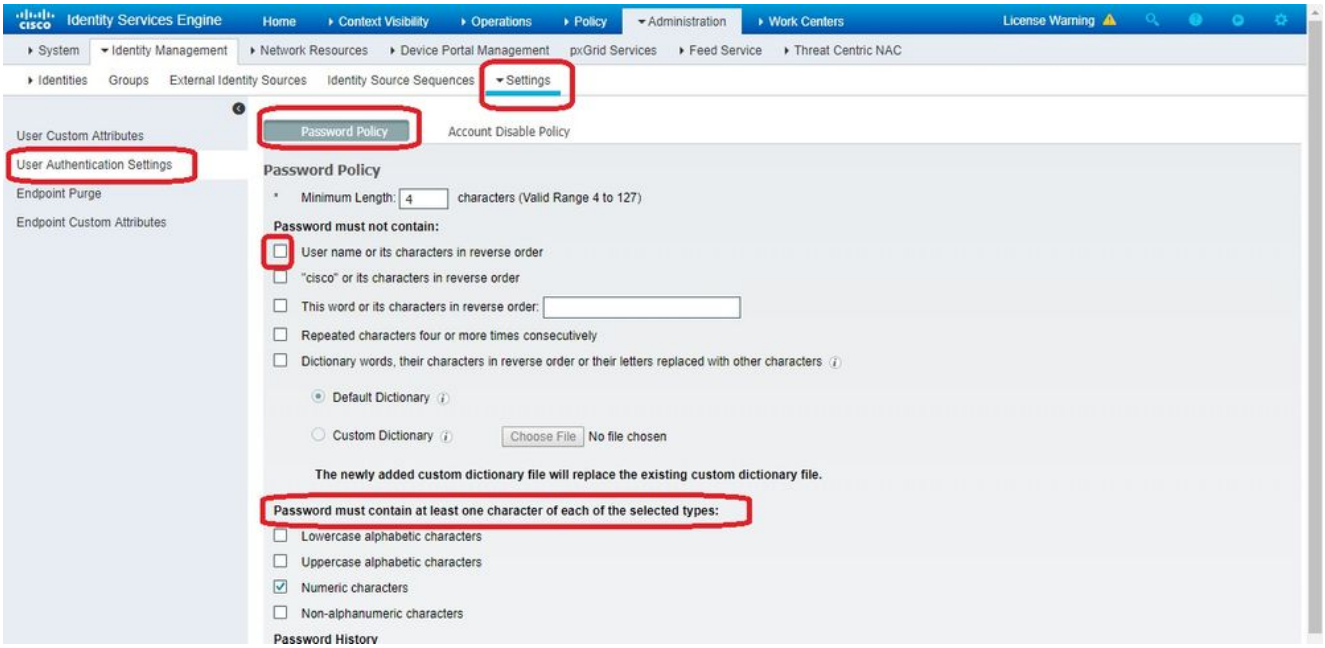
Cisco ISE의 엔드포인트 데이터베이스에 AP MAC 주소 추가

탐색 **Administration > Identity Management > Identities** 엔드포인트 데이터베이스에 MAC 주소를 추가합니다.

Cisco ISE의 사용자 데이터베이스에 AP MAC 주소 추가(선택 사항)

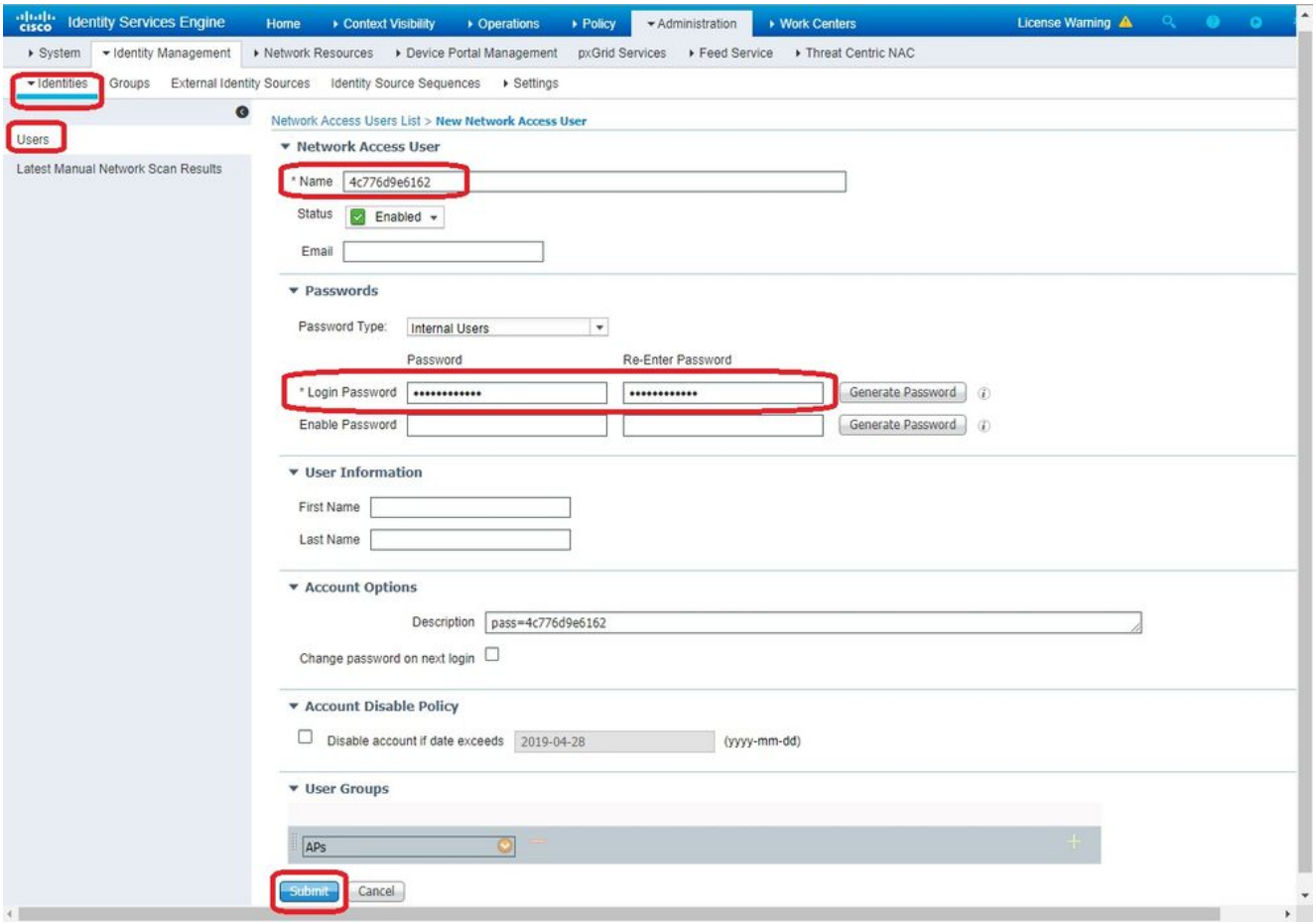
유선 MAB 프로파일을 수정하지 않고 AP MAC 주소를 사용자로 추가하도록 선택한 경우 비밀번호 정책 요구 사항을 낮춰야 합니다.

1. 탐색 **Administration > Identity Management**. 여기서는 비밀번호 정책이 사용자 이름을 비밀번호로 사용하도록 허용하고 정책이 mac 주소 문자를 사용하도록 허용해야 하며 다른 유형의 문자가 필요하지 않습니다. 탐색 **Settings > User Authentication Settings > Password Policy**:



2. 다음으로 이동 **Identities > Users** 및 **Add**. User Setup 페이지가 나타나면 표시된 대로 이 AP의 사용자 이름 및 비밀번호를 정의합니다.

팁: 이 **Description** 비밀번호로 정의된 내용을 나중에 쉽게 알 수 있도록 비밀번호를 입력하는 필드입니다.
비밀번호는 AP MAC 주소여야 합니다. 이 예에서는 **4c776d9e6162**.

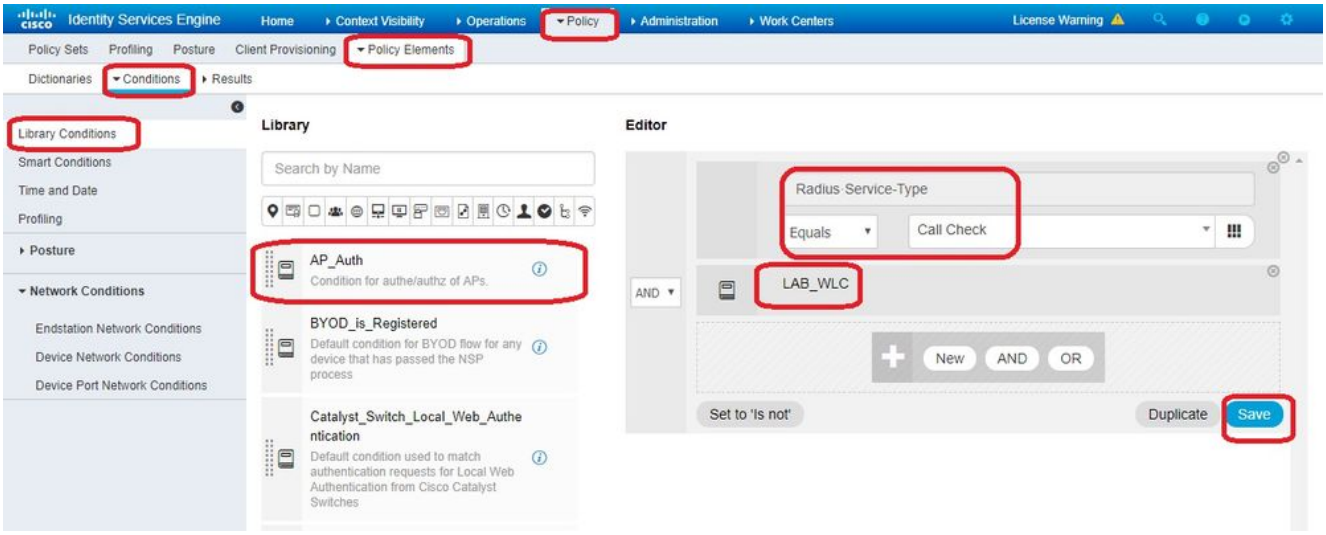


3. 클릭 **Submit**.

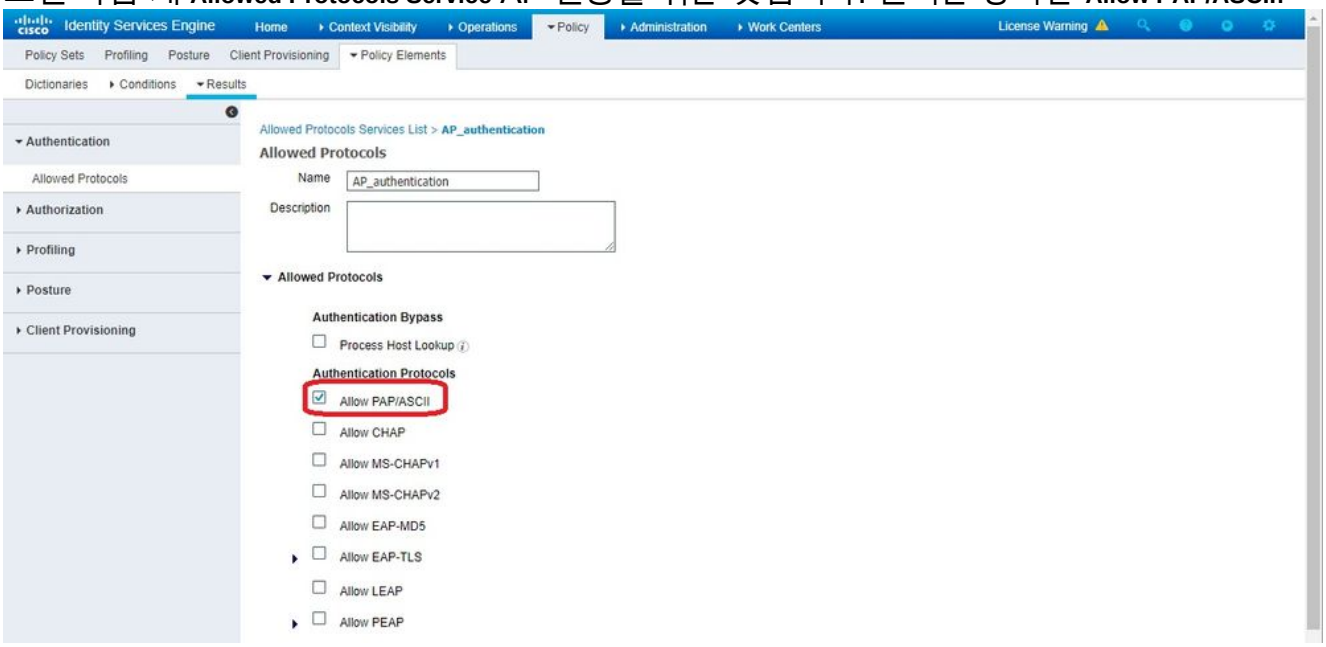
정책 집합 정의

1. 다음을 정의해야 합니다. **Policy Set** WLC에서 오는 인증 요청과 일치시킵니다. 먼저 다음 사이

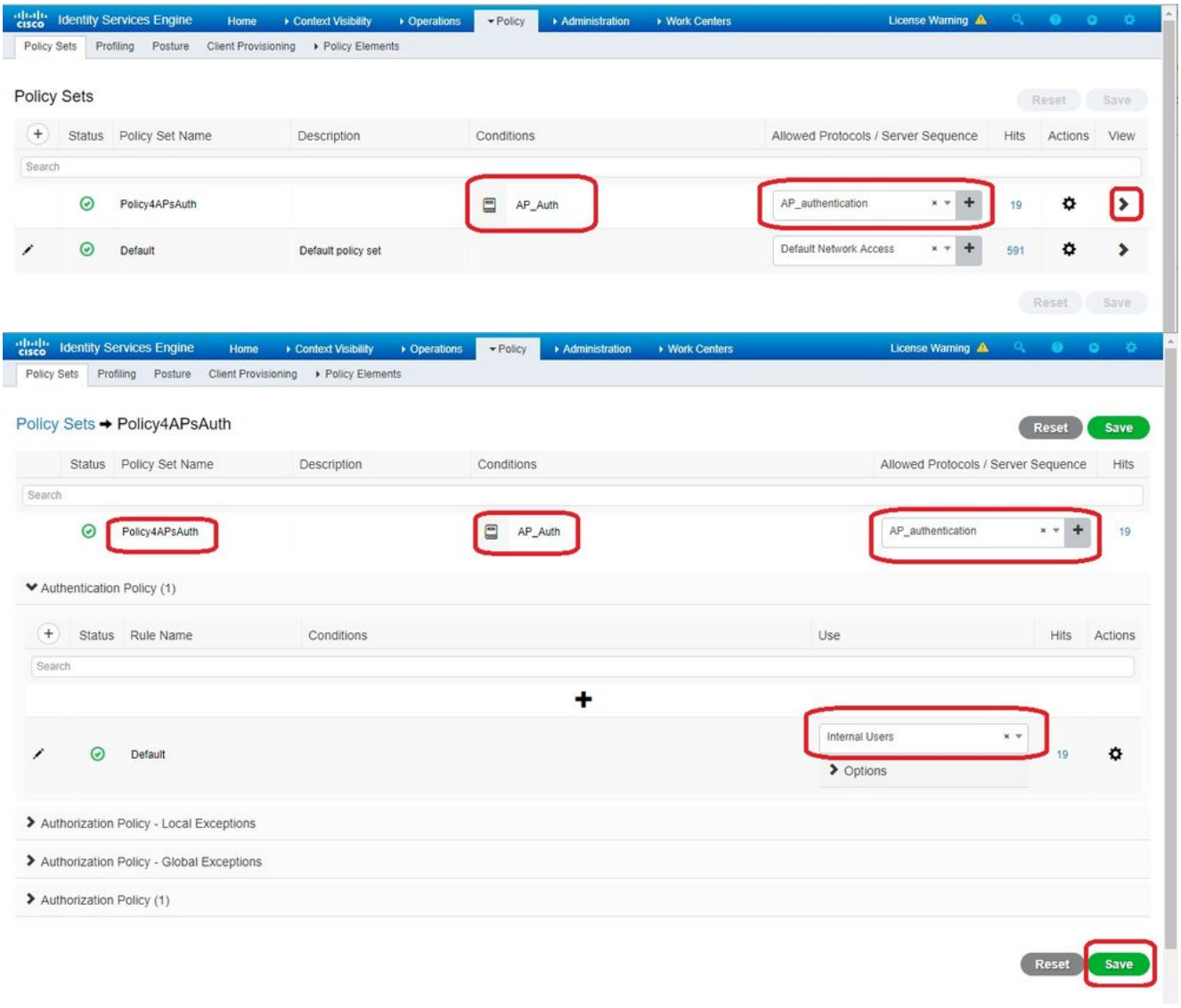
트로 이동하여 조건을 작성합니다. **Policy > Policy Elements > Conditions**및 WLC 위치와 일치하는 새 조건 만들기(이 예에서는 'LAB_WLC') **Radius:Service-Type Equals Call Check** Mac 인증에 사용됩니다. 여기서 조건의 이름은 'AP_Auth'입니다.



2. 클릭 **Save.**
3. 그런 다음 새 **Allowed Protocols Service** AP 인증을 위한 것입니다. 선택한 항목만 **Allow PAP/ASCII**:



4. 에서 이전에 생성한 서비스를 선택합니다. **Allowed Protocols/Server Sequence.** 를 확장합니다 . **View** 및 아래에 **Authentication Policy > Use > Internal Users** ISE가 내부 DB에서 AP의 사용자 이름/비밀번호를 검색하도록 합니다.



5. 클릭 **Save**.

다음을 확인합니다.

이 컨피그레이션을 확인하려면 MAC 주소 4c:77:6d:9e:61:62의 AP를 네트워크 및 모니터에 연결해야 합니다. 이 **debug capwap events/errors enable** 및 **debug aaa all enable** 명령을 사용합니다.

디버그에서 볼 수 있듯이, WLC는 AP MAC 주소를 RADIUS 서버 10.48.39.128로 전달했으며 서버는 AP를 성공적으로 인증했습니다. 그러면 AP가 컨트롤러에 등록됩니다.

참고: 공간 제약 조건으로 인해 출력의 일부 행이 두 번째 행으로 이동되었습니다.

```
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request from 192.168.79.151:5248

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 using already alloced index 437
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Unable to get Ap mode in Join request

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Allocate database entry for AP
192.168.79.151:5248, already allocated index 437

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP Allocate request at index 437 (reserved)
*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Deleting AP entry 192.168.79.151:5248 from
```

temporary database.
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 AP group received default-group is found in ap group configured in wlc.

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Dropping request or response packet to AP :192.168.79.151 (5248) by Controller: 10.48.71.20 (5246), message Capwap_wtp_event_response, state Capwap_no_state

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Message type Capwap_wtp_event_response is not allowed to send in state Capwap_no_state for AP 192.168.79.151

*spamApTask4: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 In AAA state 'Idle' for AP 70:69:5a:51:4e:c0**
*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Join Request failed!

*spamApTask4: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 State machine handler: Failed to process msg type = 3 state = 0 from 192.168.79.151:5248

*spamApTask4: Feb 27 14:58:07.566: 24:7e:12:19:41:ef Failed to parse CAPWAP packet from 192.168.79.151:5248

*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 Normal Response code for AAA Authentication : -9**
*aaaQueueReader: Feb 27 14:58:07.566: ReProcessAuthentication previous proto 8, next proto 40000001
*aaaQueueReader: Feb 27 14:58:07.566: AuthenticationRequest: 0x7f01b404f0f8

*aaaQueueReader: Feb 27 14:58:07.566: Callback.....0xd6cef02166

*aaaQueueReader: Feb 27 14:58:07.566: protocolType.....0x40000001

*aaaQueueReader: Feb 27 14:58:07.566: proxyState.....70:69:5A:51:4E:C0-00:00

*aaaQueueReader: Feb 27 14:58:07.566: Packet contains 9 AVPs:

*aaaQueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-Id.....70:69:5a:51:4e:c0 (17 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[03] Calling-Station-Id.....4c:77:6d:9e:61:62 (17 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[04] Nas-Port.....0x00000001 (1) (4 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[05] Nas-Ip-Address.....0x0a304714 (170936084) (4 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[06] NAS-Identifier.....0x6e6f (28271) (2 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[08] Service-Type.....0x0000000a (10) (4 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: AVP[09] Message-Authenticator.....DATA (16 bytes)

*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 radiusServerFallbackPassiveStateUpdate: **RADIUS server is ready 10.48.39.128 port 1812** index 1 active 1
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 NAI-Realm not enabled on Wlan, radius servers will be selected as usual
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Found the radius server : 10.48.39.128 from the global server list

*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Send Radius Auth Request with pktId:185 into qid:0 of server at index:1
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 Sending the packet to v4 host 10.48.39.128:1812 of length 130
*aaaQueueReader: Feb 27 14:58:07.566: 70:69:5a:51:4e:c0 **Successful transmission of Authentication Packet (pktId 185) to 10.48.39.128:1812** from server queue 0, proxy state 70:69:5a:51:4e:c0-00:00
*aaaQueueReader: Feb 27 14:58:07.566: 00000000: 01 b9 00 82 d9 c2 ef 27 f1 bb e4 9f a8 88 5a 6d ....'......Zm
*aaaQueueReader: Feb 27 14:58:07.566: 00000010: 4b 38 1a a6 01 0e 34 63 37 37 36 64 39 65 36 31 K8....4c776d9e61
*aaaQueueReader: Feb 27 14:58:07.566: 00000020: 36 32 1e 13 37 30 3a 36 39 3a 35 61 3a 35 31 3a 62..70:69:5a:51:
*aaaQueueReader: Feb 27 14:58:07.566: 00000030: 34 65 3a 63 30 1f 13 34 63 3a 37 37 3a 36 64 3a 4e:c0..4c:77:6d:
*aaaQueueReader: Feb 27 14:58:07.566: 00000040: 39 65 3a 36 31 3a 36 32 05 06 00 00 00 01 04 06 9e:61:62........
*aaaQueueReader: Feb 27 14:58:07.566: 00000050: 0a 30 47 14 20 04 6e 6f 02 12 54 46 96 61 2a 38 .0G...no..TF.a*8
*aaaQueueReader: Feb 27 14:58:07.566: 00000060: 5a 57 22 5b 41 c8 13 61 97 6c 06 06 00 00 00 0a ZW"[A..a.l......
*aaaQueueReader: Feb 27 14:58:07.566: 00000080: 15 f9 ..
*aaaQueueReader: Feb 27 14:58:07.566: **70:69:5a:51:4e:c0 User entry not found in the Local FileDB for the client.**
*radiusTransportThread: Feb 27 14:58:07.587: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9)
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 *** Counted VSA 150994944 AVP of length 28, code 1 atrlen 22)
*radiusTransportThread: Feb 27 14:58:07.588: Vendor Specif Radius Attribute(code=26, avp_len=28, vId=9)
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 AVP: VendorId: 9, vendorType: 1, vendorLen: 22

*radiusTransportThread: Feb 27 14:58:07.588: 00000000: 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 55 6e 6b profile-name=Unk
*radiusTransportThread: Feb 27 14:58:07.588: 00000010: 6e 6f 77 6e nown
*radiusTransportThread: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Processed VSA 9, type 1, raw bytes 22, copied 0 bytes
*radiusTransportThread: Feb 27 14:58:07.588: **70:69:5a:51:4e:c0 Access-Accept received from RADIUS server 10.48.39.128** (qid:0) with port:1812, pktId:185
*radiusTransportThread: Feb 27 14:58:07.588: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Feb 27 14:58:07.588: structureSize.....................................432

*radiusTransportThread: Feb 27 14:58:07.588: protocolUsed.....................................0x00000001

*radiusTransportThread: Feb 27 14:58:07.588: proxyState.....................................70:69:5A:51:4E:C0-00:00

*radiusTransportThread: Feb 27 14:58:07.588: Packet contains 4 AVPs:

*radiusTransportThread: Feb 27 14:58:07.588: **AVP[01] User-Name.....................................4c776d9e6162** (12 bytes)

*radiusTransportThread: Feb 27 14:58:07.588: AVP[02] State.....................................ReauthSession:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3drcFsHuYpChs (65 bytes)

*radiusTransportThread: Feb 27 14:58:07.588: AVP[03] Class.....................................DATA (83 bytes)

*radiusTransportThread: Feb 27 14:58:07.588: AVP[04] Message-Authenticator.....................DATA (16 bytes)

```
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Version: = 134770432

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType = 54 apModel: AIR-AP4800-E-K

*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 apType: Ox36 bundleApImageVer: 8.8.111.0
*spamApTask0: Feb 27 14:58:07.588: 00:00:00:00:00:00 version:8 release:8 maint:111 build:0
*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join resp: CAPWAP Maximum Msg element len =
79

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 Join Response sent to 0.0.0.0:5248

*spamApTask0: Feb 27 14:58:07.588: 70:69:5a:51:4e:c0 CAPWAP State: Join
```

문제 해결

컨피그레이션의 문제를 해결하려면 다음 명령을 사용합니다.

- debug capwap events enable- LWAPP 이벤트의 디버그를 구성합니다
- debug capwap packet enable- LWAPP 패킷 추적의 디버그를 구성합니다
- debug capwap errors enable- LWAPP 패킷 오류의 디버그를 구성합니다
- debug aaa all enable- 모든 AAA 메시지의 디버그를 구성합니다

ISE에서 RADIUS 라이브 로그에 AP가 ISE에 대해 권한 부여될 때 사용자 이름 'INVALID'가 기록되는 경우, 이는 엔드포인트 데이터베이스에 대해 인증이 확인되고 사용자가 이 문서에 설명된 대로 유선 MAB 프로파일을 수정하지 않았음을 의미합니다. ISE는 유선/무선 MAB 프로파일과 일치하지 않을 경우 MAC 주소 인증이 잘못된 것으로 간주합니다. 이 경우 기본적으로 WLC에서 전송하지 않는 NAS 포트 유형 특성이 필요합니다.

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.