# 통합 무선 네트워크에서 액세스 포인트 권한 부여 구성

## 목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 경량 AP 권한 부여 구성 WLC의 내부 권한 부여 목록을 사용한 컨피그레이션 다음을 확인합니다. AAA 서버에 대한 AP 권한 부여 Cisco ISE가 AP를 인증하도록 구성 MAB에 NAS-Port-Type 특성이 필요하지 않은 새 디바이스 프로파일 구성 Cisco ISE에서 WLC를 AAA 클라이언트로 구성 Cisco ISE의 엔드포인트 데이터베이스에 AP MAC 주소 추가 Cisco ISE의 사용자 데이터베이스에 AP MAC 주소 추가(선택 사항) 정책 집합 정의 다음을 확인합니다. 문제 해결

## 소개

이 문서에서는 AP의 MAC 주소를 기반으로 액세스 포인트(AP)에 권한을 부여하도록 WLC를 구성 하는 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 디바 이스는 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 이후 에 제조된 모든 Cisco AP에는 MIC가 있습니다.

등록 프로세스 중에 발생하는 이러한 상호 인증 외에도, WLC는 AP의 MAC 주소를 기반으로 등록 하는 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 인 증이 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

،،ا،،،ا،، cısco	MONITOR WLANS (	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	Sa <u>v</u> e Configuration <u>F</u> EEDBACK	<u>P</u> ing	Logou	it <u>R</u> efresh
Security	AP Policies								Apply		Add
▼ AAA General ▼ RADIUS	Policy Configuration							-			
Authentication Accounting	Accept Self Signed Cert	tificate (SSC)									
Auth Cached Users Fallback	Accept Manufactured In	nstalled Certificat	te (MIC)								
DNS Developded AVP	Accept Local Significant	t Certificate (LSC	:)								
▶ TACACS+	Authorize MIC APs agai	inst auth-list or A	AAA								
LDAP Local Net Users MAC Filtering	Authorize LSC APs agai	inst auth-list									
<ul> <li>Disabled Clients</li> <li>User Login Policies</li> </ul>	AP Authorization List				Ent	ries 1 - 5 of 5					
AP Policies Password Policies	Search by MAC		Searc	h							
Local EAP											
Advanced EAD	MAC address / Serial N	Number	Certificate	Type Si	IA1 Key Hash						

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

									Save	comguration	End	Logour Meiresn
CISCO	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK			🔒 <u>H</u> ome
Security	AP Policie	es										Apply
▼ AAA General ▼ RADIUS	Policy Conf	figuration										
Authentication Accounting Auth Cached Users	Accept Self	f Signed Ce	ertificate (SSC)									
Fallback	Accept Mar	nufactured	Installed Certifica	ate (MIC)								
DNS Downloaded AVP	Accept Loc	al Significa	nt Certificate (LS	C)								
TACACS+	Authorize M	MIC APs ag	ainst auth-list or	AAA								
Local Net Users MAC Filtering Disabled Clients	Authorize L	LSC APs ag	ainst auth-list									
Lises Login Policies	Add AP to A	Authoriza	tion List									
AP Policies Password Policies	MAC Addre	:55	4	4c:77:6d:9e:61	:62							
Local EAP	Certificate	Туре	C	MIC	۲							
Advanced EAP				Add			J					
Priority Order     Certificate	AP Authoriz	zation Lis	st			Er	ntries 0 - 0 of 0					
Access Control Lists				Contra								
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>	Search by M	AC	ificate	Searc	n							
Web Auth	Serial Num	ber Type	SHA1 K	ey Hash								
TrustSec												
Local Policies												
Umbrella												
Advanced												

AP가 AP 권한 부여 목록에 추가되고 AP Authorization List.

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

ahaha						Sa <u>v</u> e Conf	iguration <u>P</u> ing Logout <u>R</u> el
CISCO	MONITOR WLANS CONTROLLER	R WIRELESS SECU	RITY M <u>A</u> NAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK	<u>н</u> н
ecurity	AP Policies						Apply Ad
AAA General ▼ RADIUS	Policy Configuration						$\square$
Authentication Accounting	Accept Self Signed Certificate (SSC)						
Auth Cached Users Fallback	Accept Manufactured Installed Certifi	icate (MIC)					
DNS Developed at the	Accept Local Significant Certificate (I	.SC)					
▶ TACACS+	Authorize MIC APs against auth-list	or AAA					
LDAP	Authorize LSC APs papiest auth-list						
MAC Filtering	Authorize LSC APS against auth-list						
Disabled Clients	AD Authorization List		En	tries 1 - 5 of 5			
AP Policies	AP Autionzation List				e.		
Password Policies	Search by MAC	Search					
Local EAP							
Advanced EAP	MAC address / Serial Number	Certificate Type	SHA1 Key Hash				-
Priority Order	40:77:60:90:61:62	MIC					
Certificate	70:03:79:26:39:68	MIC					
torres Control Lints	88:r0:31:7e:e0:38	MIC					
Access Control Lists	F4:00:e6:43:c4:02	MIC					
Wireless Protection Policies	10:20:23:67:50:20	MIC					M
Web Auth							
TrustSec							

### 다음을 확인합니다.

이 컨피그레이션을 확인하려면 MAC 주소로 AP를 연결해야 합니다 4c:77:6d:9e:61:62 네트워크 및 모 니터에 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 4000001 \*aaaQueueReader: Feb 27 10:15:25.593: AuthenticationRequest: 0x7f01b4083638 \*aaaQueueReader: Feb 27 10:15:25.593: Callback..... \*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) 51-4e-c0 (17 bytes) 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-\*aaaQueueReader: Feb 27 10:15:25.593: AVP[06] NAS-Identifier......0x6e6f (28271) (2 bytes) \*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: protocolUsed..... \*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 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: 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: 0x36 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 사용합니 다. 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 매개변수 를 선택하면 WLC가 먼저 로컬 권한 부여 목록을 확인합니다. AP MAC가 없는 경우 RADIUS 서버를 확인합니다.

սիսիս						Sa <u>v</u> e Config	juration <u>P</u> ing Logout	Refresh
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECU	RITY MANAGEMENT	C <u>O</u> MMANDS	HELP	<b>FEEDBACK</b>		🔒 <u>H</u> ome
Security	AP Policies						Apply	Add
▼ AAA General ▼ RADIUS	Policy Configuration						$\square$	
Authentication Accounting Auth Cached Users	Accept Self Signed Certificate (SSC)							
Fallback DNS	Accept Manufactured Installed Certifi	cate (MIC)	×					
Downloaded AVP	Accept Local Significant Certificate (L	SC)						
LDAP Local Net Users	Authorize LSC APs against auth-list	r aaa						
MAC Filtering Disabled Clients Disabled Clients	AP Authorization List		En	tries 1 - 5 of 5				
Password Policies	Search by MAC	Search						
Local EAP		C						
Advanced EAP	MAC address / Serial Number	Certificate Type	SHA1 Key Hash				-	
Priority Order	40:77:00:96:01:02	MIC						
Certificate	88:f0:31:7e:e0:38	MIC						
Access Control Lists	f4:db:e6:43:c4:b2	MIC						
Wireless Protection     Policies	fc:5b:39:e7:2b:30	MIC						
▶ Web Auth								
▶ TrustSec								

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

ahaha										Sa <u>v</u> e Configu	uration Ping Logout	<u>R</u> efresh
cisco	MONITOR	R <u>W</u> LANS <u>C</u>	ONTROLLER	R WIRELES	S SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK			<u>H</u> ome
Security	RADIUS	S Authentica	tion Serv	ers	1110						Apply Nev	N
AAA     General     RADIUS     Authentication	Auth C Use AE	alled Station ID T S Key Wrap	ype AP	MAC Address:	SSID	d requires a key wr	an compliant RADI		4			
Accounting Auth Cached Users Fallback DNS	MAC De	elimiter 3 MTO	No	Delimiter 🔻	D	a requires a key mit			,			
Downloaded AVP TACACS+ LDAP	Network User	k Management	Tunne Hyp Proxy	ohen ale Hyphen	Server Addres	is(Ipv4/Ipv6)			Port	IPSec	Admin Status	
MAC Filtering				gie Hypiteli	10.48.39.100				1812	Disabled	Enabled	
Disabled Citerits     User Login Policies     AP Policies     Password Policies		×.	NO NO	Demniter	10.40.39.120				1012	Disabled	Enabled	
P LOCALEAP												
Advanced EAP												
Priority Order												
Certificate												
Access Control Lists												
Wireless Protection     Policies												
Web Auth												
TrustSec												
Local Policies												

4. 그런 다음 New RADIUS 서버를 정의합니다.

adaadaa			Sage Configuration Ping Logout Refresh
cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	A Home
Security	RADIUS Authentication Serve	ers > New	< Back Apply
<ul> <li>AAA         <ul> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Auth Cached Users</li> <li>Fallback</li> <li>DNS</li> <li>Downloaded AVP</li> </ul> </li> <li>TACACS+         <ul> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>Password Policies</li> </ul> </li> <li>Local EAP         <ul> <li>Advanced EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection             <ul> <li>Policies</li> <li>Web Auth</li> <li>TrustSec</li> </ul> </li> </ul></li></ul>	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Apply Cisco ACA Default settings Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeout Turnel Proxy PAC Provisioning IPSec Cisco ACA	3	
Local Policies			

5. 에서 RADIUS 서버 매개변수를 정의합니다. RADIUS Authentication Servers > New 페이지. 이러한 매 개변수에는 RADIUS가 포함됩니다 Server IP Address, Shared Secret, Port Number및 Server Status. 완 료되면 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 전송 하지 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. 기 존 Cisco 프로필에서 다른 설정을 복사할 수 있지만 유선 MAB 워크플로에 'Nas-port-type' 특성이 필요하지 않습니다.



Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers
* Name	Ciscotemp		
Description			<i>i</i>
Icon	change icon	Default (i)	
Vendor	Cisco		
Supported Protoc	cols		
RADIUS			
TACACS+			
TrustSec			
RADIUS Dictionaries			
Templates			
Expand All / Collapse All			
$\vee$ Authentication	/Authorization		
$\checkmark$ Flow Type Co	onditions		
Wired MAB deter	cted if the following condition(s) are m	net :	
Radius:Se	ervice-Type 🗸 =	Call Check 🗸	_  +

### Cisco ISE에서 WLC를 AAA 클라이언트로 구성

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

	Identity Servi	ces Engine	Home	Context Visibil	ity ► Operations	► Policy ▼A	dministration	Work Centers		License Warning 🔺	<u> </u>	
+ Sys	stem 🕨 Identi	ty Management	• Networl	k Resources D	evice Portal Manageme	ent pxGrid Service	s Feed Service	Threat Centric	NAC			
- Net	twork Devices	Network Device G	roups	Network Device Pro	files External RADIU	JS Servers RADIL	IS Server Sequence	s NAC Managers	External MDM	Location Services		
		0	Netv	work Devices								
etwor	rk Devices			* Nam	e WLC5520							
efault	t Device			Descriptio	n							
evice	Security Setting	S										
				IP Address	▼ * IP : 10.48.71.	20		/ 32			容.	
			<b>0</b> #	Pv6 is supported on! * Device Profil Model Nam Software Versic * Network Device Gi Location LAB	y for TACACS, At least e <u>the Cisco</u> • e <u>•</u> • n <u>•</u> oup	one IPv4 must be de	fined when RADIUS	is selected				
			ſ	IPSEC No Device Type WLC-I	ab 📀	Set To Default						
					tication Settings							
				RADIUS Authen     RADIUS UDP	tication Settings Settings							
				<ul> <li>▼ RADIUS Auther.</li> <li>RADIUS UDP :</li> </ul>	tication Settings Settings	Protocol	RADIUS					
			2		tication Settings Settings	Protocol * Shared Secret	RADIUS	Shov				
					tication Settings Settings	Protocol * Shared Secret CoA Port	RADIUS 1700	Shov	o Default			
			V	▼ RADIUS Auther RADIUS UDP : RADIUS DTL S	tication Settings Settings Settings (j)	Protocol * Shared Secret CoA Port	RADIUS 1700	Show	o Default			
			V	RADIUS Auther     RADIUS UDP     RADIUS DTL S	tication Settings Settings Settings (j)	Protocol * Shared Secret CoA Port DTLS Required	RADIUS 1700	Shov	o Default			

3. 클릭 Submit.

Cisco ISE의 엔드포인트 데이터베이스에 AP MAC 주소 추가

탐색 Administration > Identity Management > Identities 엔드포인트 데이터베이스에 MAC 주소를 추가합니 다.

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 필 요하지 않습니다. 탐색 Settings > User Authentication Settings > Password Policy:

cisco Identity Services Engine	Home   Context Visibility   Operations   Policy   Administration   Work Centers  Lic	ense Warning 🔺	0	0	0	- 0
System      Identity Management	Network Resources     Device Portal Management     pxGrid Services     Feed Service     Threat Centric NAC					
Identities Groups External Iden	entity Sources Identity Source Sequences - Settings					
•	•					
User Custom Attributes	Password Policy Account Disable Policy					_
User Authentication Settings	Password Policy					
Endpoint Purge	* Minimum Length: 4 characters (Valid Range 4 to 127)					
Endpoint Custom Attributes	Password must not contain:					
	User name or its characters in reverse order					
	"cisco" or its characters in reverse order					
	This word or its characters in reverse order.					
	Repeated characters four or more times consecutively					
	Dictionary words, their characters in reverse order or their letters replaced with other characters (j)					
	Default Dictionary					
	Custom Dictionary () Choose File No file chosen					
	The newly added custom dictionary file will replace the existing custom dictionary file.					
	Password must contain at least one character of each of the selected types:					
	Lowercase alphabetic characters					
	Uppercase alphabetic characters					
	Vumeric characters					
	Non-alphanumeric characters					
	Password History					

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 필 드입니다.

비밀번호는 AP MAC 주소여야 합니다. 이 예에서는 4c776d9e6162.

dentity Services Engine	Home  Context Visibility  Operations  Policy  Administration  Work Centers	License Warning 🔺 🔍 🥥 📀
System - Identity Management	Network Resources	
Identities Groups External Identit	/ Sources Identity Source Sequences + Settings	
	Network Access Users List > New Network Access User	
est Manual Network Scan Recults	▼ Network Access User	
est manual Network Scan Nesults	* Name 4c776d9e6162	
	Status Enabled -	
	Email	
	▼ Passwords	
	Password Type: Internal Lisere	
	Password Re-Enter Password	
	* Login Password Generate Password	
	Enable Password Generate Password (i)	
	▼ User Information	
	First Name	
	Last Name	
	* Account Ontions	
	Description Artificial	
	Description Description Description	A
	Change password on next login	
	▼ Account Disable Policy	
	Disable account if date exceeds 2019-04-28 (yyyy-mm-dd)	
	w Heav Crowns	
	• user droups	
	APs 📀 —	+
	Submit	

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 > Conditions및 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.

cisco Identity Services Engine	Home	▼ Policy → Administration	Work Centers Lic	ense Warning 🔺 🔍 🎯 🔿 🔅	
Policy Sets Profiling Posture (	Client Provisioning - Policy Elements	<u> </u>			
Dictionaries Conditions + Resu	ults				
Library Conditions	Library	Editor			
Smart Conditions	Search by Name			© <sup>®</sup> *	
Time and Date		1212123	Radius Service-Type		
Profiling	♀▫□▰◉异♀₽▨ੋੋੋੋ©↓	. O b 🕈	Equals Y Call Check		
▶ Posture	AP_Auth	0	cituas		
<ul> <li>Network Conditions</li> </ul>	Condition for authe/authz of APs.	AND T	LAB_WLC		
Endstation Network Conditions Device Network Conditions Device Port Network Conditions	BYOD_is_Registered Default condition for BYOD flow for any device that has passed the NSP process	0	+ (New) (AND	OR	
	Catalyst_Switch_Local_Web_Authe	Se	t to 'Is not'	Duplicate Save	
	Default condition used to match authentication requests for Local Web Authentication from Cisco Catalyst Switches	0			

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

cisco Identity Services Engine	Home ▶ Co	ontext Visibility	Operations	▼Policy	Administration	Work Centers	License Warning 🔺	Q,	0	0	ø
Policy Sets Profiling Posture (	Client Provisioning	· Policy Element	nts								
Dictionaries Conditions Resu	ilts										
- Authentication	Allowed Protoco Allowed Protoco	ols Services List : tocols	AP_authenticat	ion							
Allowed Protocols	Name	AP_authenticat	ion								
Authorization	Description			5%	-						
Profiling					h						
Posture		otocols									
Client Provisioning	Auth	entication Bypas Process Host Loo	is kup (j)								
	Auth	entication Proto Allow PAP/ASCII	cols								
		Allow CHAP									
		Allow MS-CHAPv	1								
	□,	Allow MS-CHAPv	2								
		Allow EAP-MD5									
	, 🗆 ,	Allow EAP-TLS									
	Ξ,	Allow LEAP									
	, 🗆 ,	Allow PEAP									

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/비 밀번호를 검색하도록 합니다.

cy Sets						F	Reset	Save
Status Policy Set Name	Description	Conditions	Allowed P	rotocols / Serve	er Sequence	Hits	Actions	Viev
arch		$\frown$						
Policy4APsAuth		AP_Auth	AP_authe	ntication	× • +	19	¢	2
O Default	Default policy set		Default Ne	etwork Access	× • +	591	¢	>
							Reset	Save
V Sets Profiling Posture Client Prov	Context Visibility     O	perations    Policy   Administration	Work Centers	Lice	nse Warning 🔏	<u> </u>	8	•
Data + Dallaud A Da Auth						6	Reset	Sav
cy Sets - Policy4APSAuth								-
Status Policy Set Name	Description	Conditions		Allow	ed Protocols	/ Server S	equence	Hit
Status Policy Set Name	Description	Conditions		Allow	ed Protocols	/ Server S	equence	Hit
Status Policy Set Name arch  Policy4APsAuth  Policy4APsAuth	Description	Conditions		Allow	ed Protocols authentication	/ Server S	equence	Hit
Cy Sets  Policy APSAuth  Status Policy Set Name  Policy4APSAuth  Authentication Policy (1)	Description	Conditions		Allow	ed Protocols authentication	/ Server S	× • +	Hit
Cy Sets - Policy4APSAuth  Status Policy Set Name  arch  Policy4APsAuth  Authentication Policy (1)  + Status Rule Name	Description	Conditions AP_Auth	U	Allow	ed Protocols	/ Server S	equence	Hit 15 Action
Cy Sets - Policy APSAuth Status Policy Set Name arch Policy4APSAuth Authentication Policy (1) + Status Rule Name earch	Description	Conditions	U	Allow	ed Protocols	/ Server S	× • + Hits	Hit 19 Action
Cy Sets - Policy4APSAuth  Status Policy Set Name  arch  Policy4APSAuth  Authentication Policy (1)  Status Rule Name  rearch	Description	Conditions	U	Allow	ed Protocols	/ Server S	+ + +	Hit 19 Action
Cy Sets - Policy4APSAuth  Status Policy Set Name  arch  Policy4APsAuth  Authentication Policy (1)  + Status Rule Name  rearch	Description	Conditions AP_Auth	U	Allow AP_ se	ed Protocols	/ Server S	+ + +	Hit 19 Action
Cy Sets - Policy 4AP SAuth Status Policy Set Name arch Policy 4AP SAuth Policy 4AP SAuth Policy 4AP SAuth Authentication Policy (1) + Status Rule Name earch Default	Description	Conditions AP_Auth +	U	Allow AP_ se internal Users > Options	ed Protocols	/ Server S	Hits	Hit 19 Action
Status       Policy4APSAuth         Status       Policy4APSAuth         Image: Policy4APSAuth       Image: Policy4APSAuth         Image: Policy4APSAuth       Image: Policy4APSAuth         Authentication Policy (1)       Image: Policy4APSAuth         +       Status       Rule Name         rearch       Image: Policy4APSAuth       Image: Policy4APSAuth         •       Default       Image: Policy4APSAuth         Authentication Policy - Local Exceptions       Image: Policy4APSAuth	Description	Conditions AP_Auth +	U	Allow AP_ se internal Users > Options	ed Protocols	/ Server S	Hits	Hiti 15 Action
Cy Sets - Policy 4APSAuth  Status Policy Set Name  arch  Policy4APSAuth  Authentication Policy (1)  Status Rule Name  rearch  Default  Authorization Policy - Local Exceptions  Authorization Policy - Global Exceptions	Description	Conditions AP_Auth +	U	Allow AP_ se internal Users > Options	ed Protocols	/ Server S	Hits	Hitt Hitt

#### 5. 클릭 Save.

#### 다음을 확인합니다.

이 컨피그레이션을 확인하려면 MAC 주소 4c:77:6d:9e:61:62의 AP를 네트워크 및 모니터에 연결해 야 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 서버 는 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..... \*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: \*aaaOueueReader: Feb 27 14:58:07.566: AVP[02] Called-Station-\*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) (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) \*aaaOueueReader: 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 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 0a ZW"[A..a.l.... \*aaaQueueReader: Feb 27 14:58:07.566: 0000080: 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, vTd=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: 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:0a302780bNEx79SKIFosJ2ioAmIYNOiRe2iDSY3dr cFsHuYpChs (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 기록되 는 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 않 는 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 번 역 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.