Catalyst 9800 WLC에서 로컬 EAP 인증 구성

목차

소개

이 문서에서는 Catalyst 9800 WLC(Wireless LAN Controller)의 로컬 EAP 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에서는 Catalyst 9800 WLC의 로컬 EAP(Extensible Authentication Protocol) 컨피그레이션, 즉 WLC가 무선 클라이언트에 대해 RADIUS 인증 서버로 수행하는 것에 대해 설명합니다.

이 문서에서는 9800 WLC의 WLAN에 대한 기본 컨피그레이션을 잘 알고 있다고 가정하고, 무선 클라이언트에 대한 로컬 EAP 서버로 작동하는 WLC에만 중점을 둡니다.

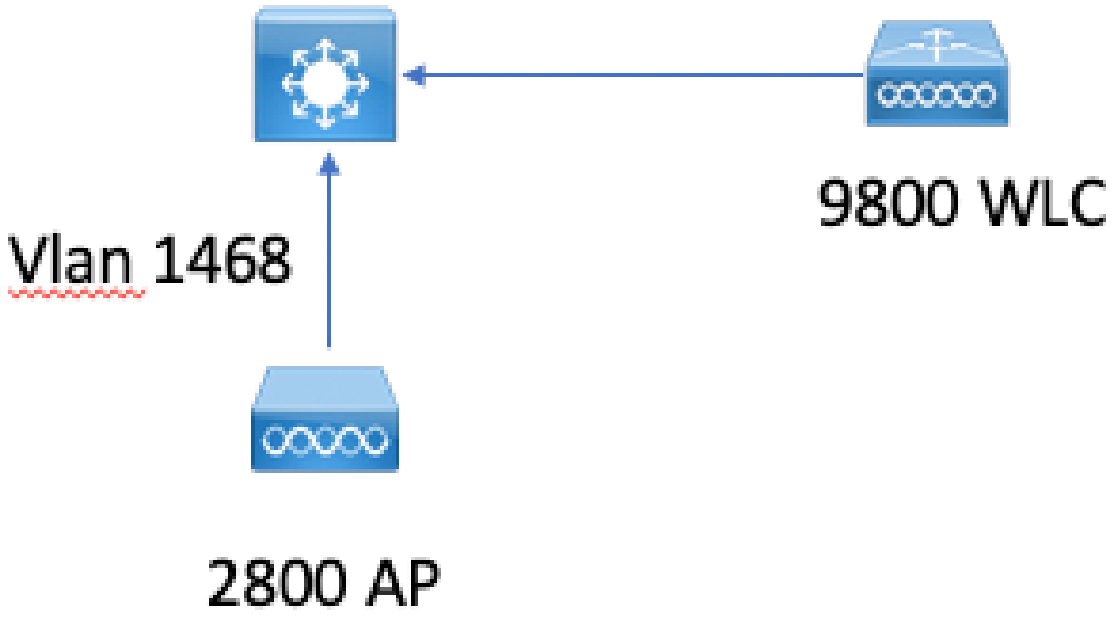
사용되는 구성 요소

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.

버전 16.12.1s의 Catalyst 9800

구성

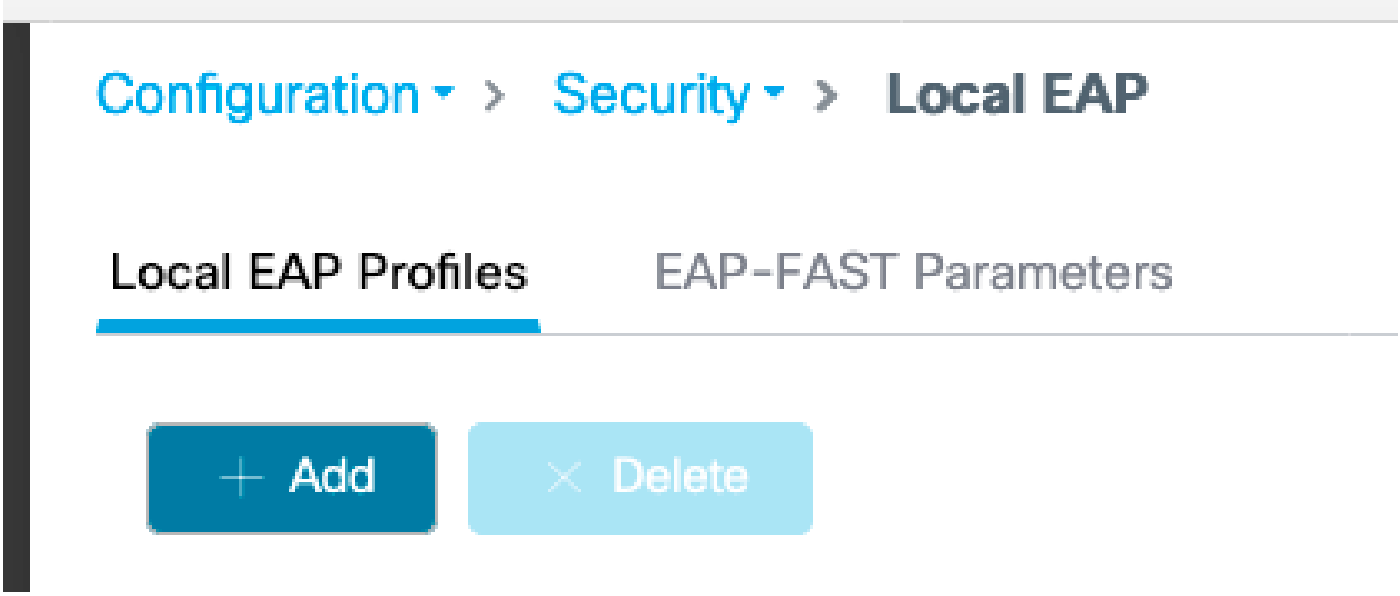
네트워크 다이어그램



기본 로컬 EAP 컨피그레이션

1단계. 로컬 EAP 프로파일

9800 웹 UI에서 Configuration(컨피그레이션) > Security(보안) > Local EAP(로컬 EAP)로 이동합니다.

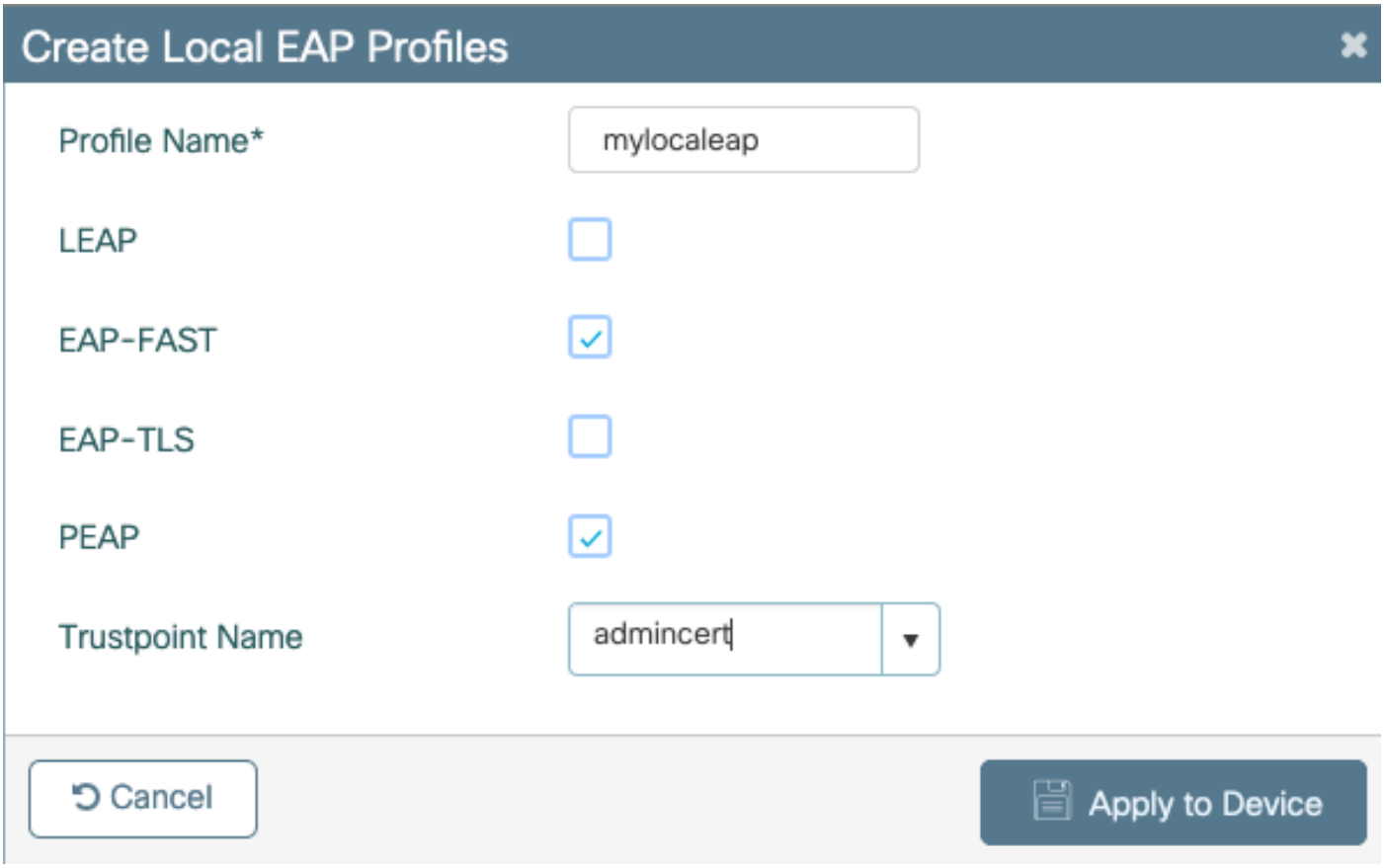


Add(추가)를 선택합니다.

프로파일 이름을 입력합니다.

보안이 취약해 LEAP를 전혀 사용하는 것은 권고되지 않는다. 다른 3가지 EAP 방법 중 하나를 사용하려면 신뢰 지점을 구성해야 합니다. 인증자 역할을 하는 9800은 클라이언트가 인증서를 신뢰하도록 인증서를 보내야 하기 때문입니다.

클라이언트는 WLC 기본 인증서를 신뢰하지 않으므로 클라이언트측에서 서버 인증서 검증을 비활성화하거나(권장 사항 없음) 클라이언트가 신뢰하는 9800 WLC에 인증서 신뢰 지점을 설치해야 합니다(또는 클라이언트 신뢰 저장소에서 수동으로 가져와야 함).



CLI:

```
(config)#eap profile mylocapeap
(config-eap-profile)#method peap
(config-eap-profile)#pki-trustpoint admincert
```

2단계. AAA 인증 방법

사용자의 로컬 데이터베이스를 사용하려면 로컬을 가리키는 AAA dot1x 메서드를 구성해야 합니다(예: 외부 LDAP 조회를 사용할 수 있음).

Configuration(컨피그레이션) > Security(보안) > AAA로 이동하고 Authentication(인증)에 대한 AAA method list(AAA 방법 목록) 탭으로 이동합니다. Add를 선택합니다.

"dot1x" 유형 및 로컬 그룹 유형을 선택합니다.

3단계. AAA 권한 부여 방법 구성

Authorization(권한 부여) 하위 탭으로 이동하여 type credential-download(자격 증명 다운로드 유형)에 대한 새 방법을 만들고 이를 local(로컬)로 가리킵니다.

네트워크 권한 부여 유형에 대해 동일한 작업을 수행합니다.

CLI:

```
(config)#aaa new-model
(config)#aaa authentication dot1x default local
(config)#aaa authorization credential-download default local
(config)#aaa local authentication default authorization default
(config)#aaa authorization network default local
```

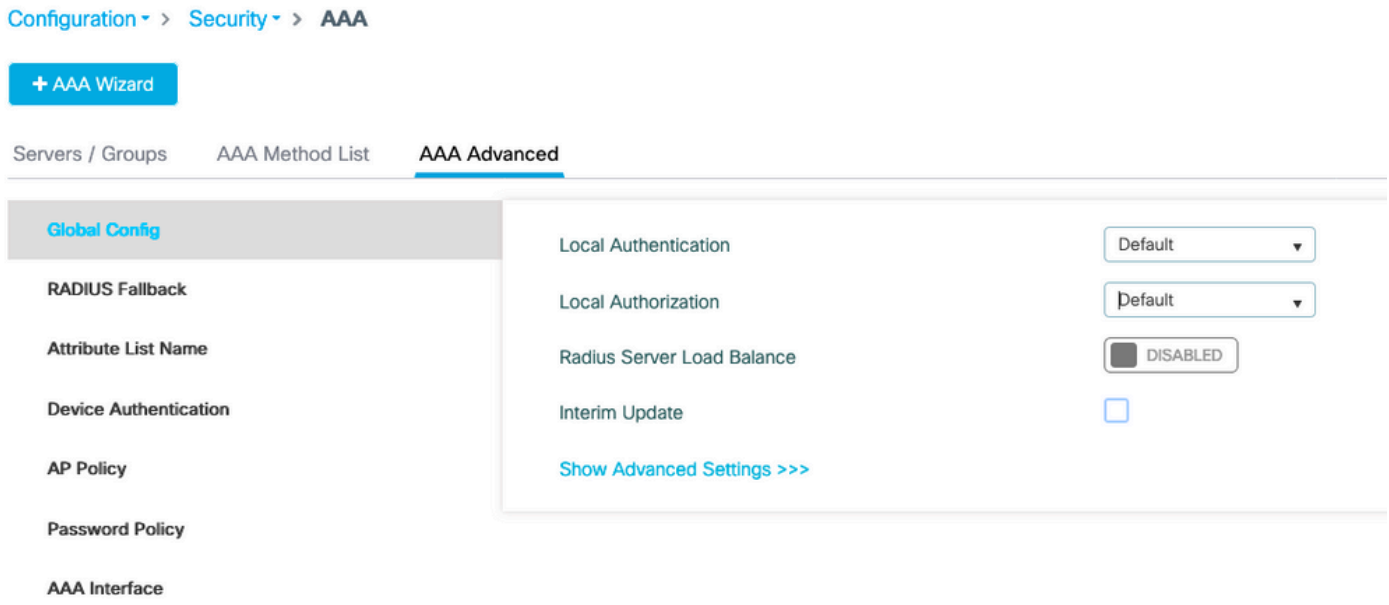
4단계. 로컬 고급 방법 구성

AAA 고급 탭으로 이동합니다.

로컬 인증 및 권한 부여 방법을 정의합니다. 이 예에서는 "default" credential-download 및 "Default"

dot1x 메서드를 사용했으므로 여기에 있는 로컬 인증 및 권한 부여 드롭다운 상자에 모두 default를 설정해야 합니다.

명명된 메서드를 정의한 경우 드롭다운에서 "method list"를 선택하면 다른 필드에서 메서드 이름을 입력할 수 있습니다.



CLI:

```
aaa local authentication default authorization default
```

5단계. WLAN 구성

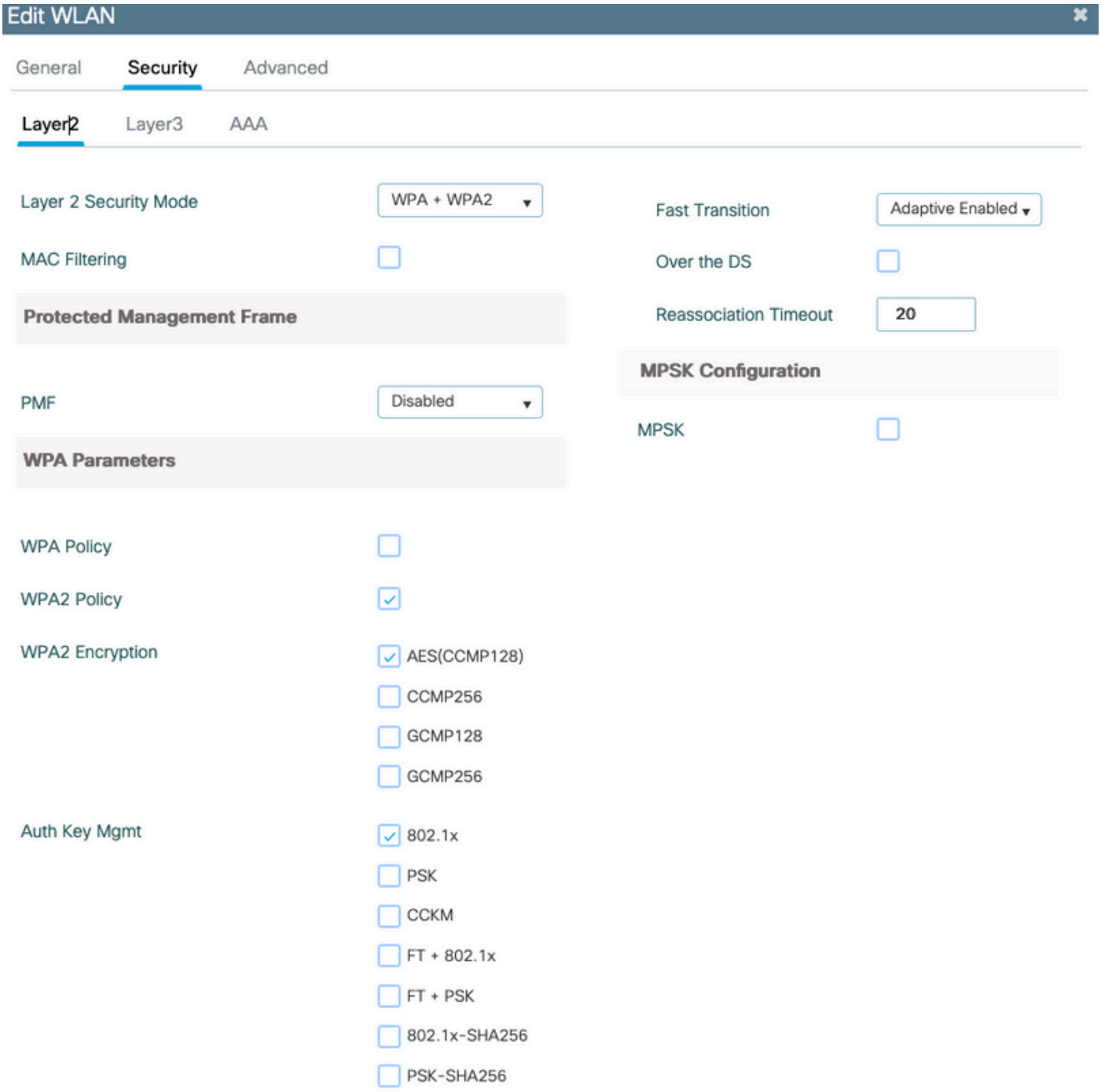
그런 다음 이전 단계에서 정의한 로컬 EAP 프로파일 및 AAA 인증 방법에 대해 802.1x 보안을 위해 WLAN을 구성할 수 있습니다.

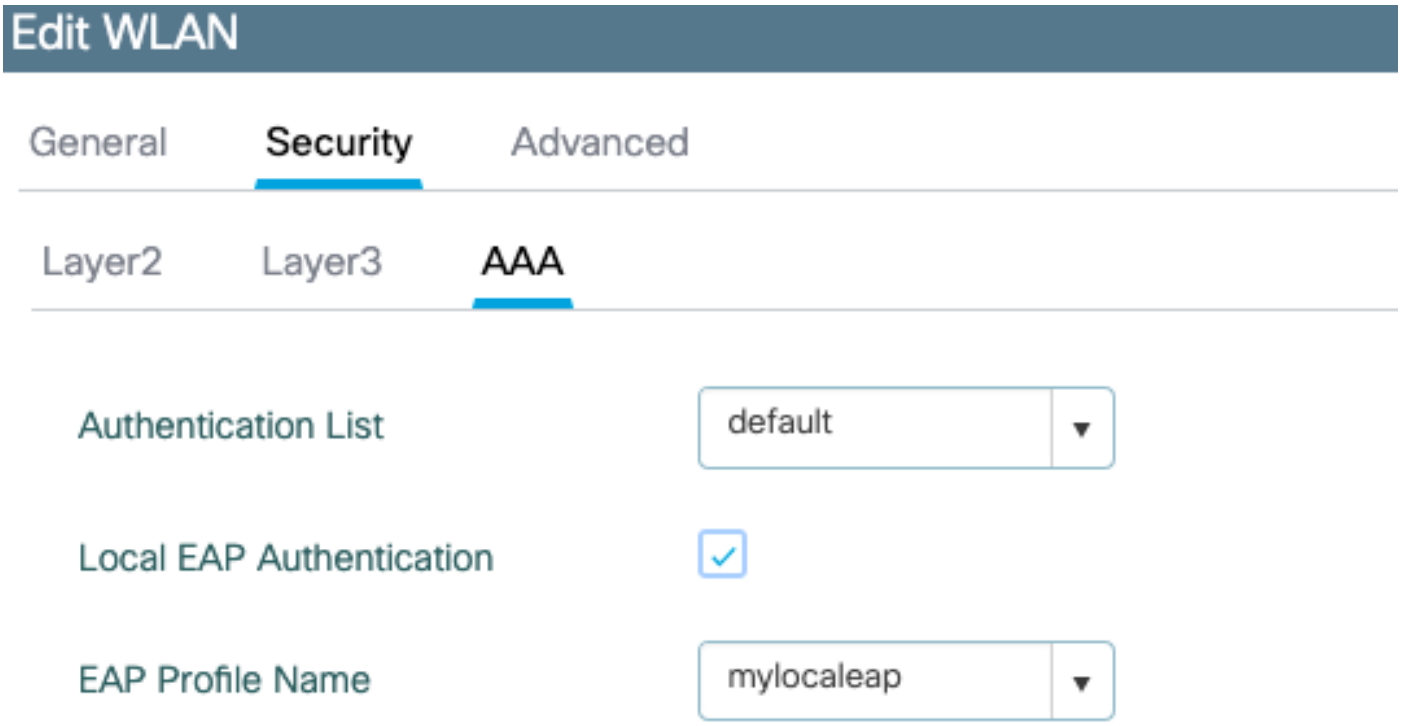
Configuration(컨피그레이션) > Tags and Profiles(태그 및 프로필) > WLANs(WLAN) > + Add(추가) >

SSID 및 프로파일 이름을 제공합니다.

레이어 2 아래에서 Dot1x 보안이 기본적으로 선택됩니다.

AAA 아래에서 Local EAP Authentication(로컬 EAP 인증)을 선택하고 드롭다운 목록에서 Local EAP profile and AAA Authentication list(로컬 EAP 프로필 및 AAA 인증 목록)을 선택합니다.


Edit WLAN
General
Security
Advanced
Layer2
Layer3
AAA
Layer 2 Security Mode
WPA + WPA2
MAC Filtering
Protected Management Frame
PMF
Disabled
WPA Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Auth Key Mgmt
802.1x
PSK
CCKM
FT + 802.1x
FT + PSK
802.1x-SHA256
PSK-SHA256
Fast Transition
Adaptive Enabled
Over the DS
Reassociation Timeout
20
MPSK Configuration
MPSK




```
(config)#wlan localpeapssid 1 localpeapssid
(config-wlan)#security dot1x authentication-list default
(config-wlan)#local-auth mylocaleap
```

6단계. 하나 이상의 사용자 생성

CLI에서 사용자는 network-user 유형이어야 합니다. 다음은 CLI에서 만든 사용자 예입니다.

```
(config)#user-name 1xuser
 creation-time 1572730075
 description 1xuser
 password 0 Cisco123
 type network-user description 1xuser
```

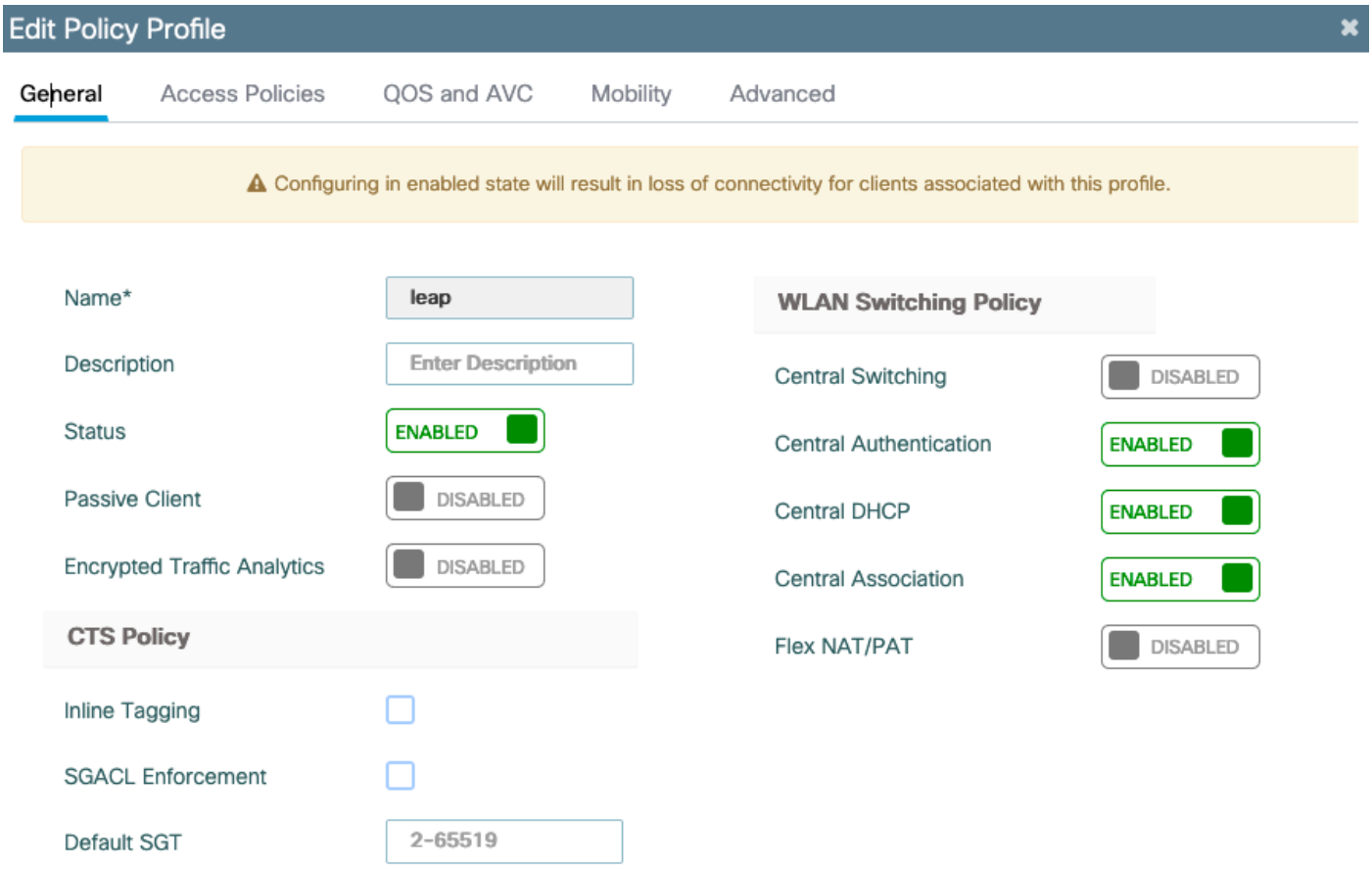
CLI에서 생성된 사용자는 웹 UI에 표시되지만 웹 UI에서 생성된 경우 16.12부터 네트워크 사용자로 만들 방법은 없습니다

7단계. 정책 프로필을 생성합니다. 이 WLAN 프로필을 정책 프로필에 매핑할 정책 태그 만들기

Configuration(컨피그레이션) > Tags and profiles(태그 및 프로필) > Policy(정책)로 이동합니다.

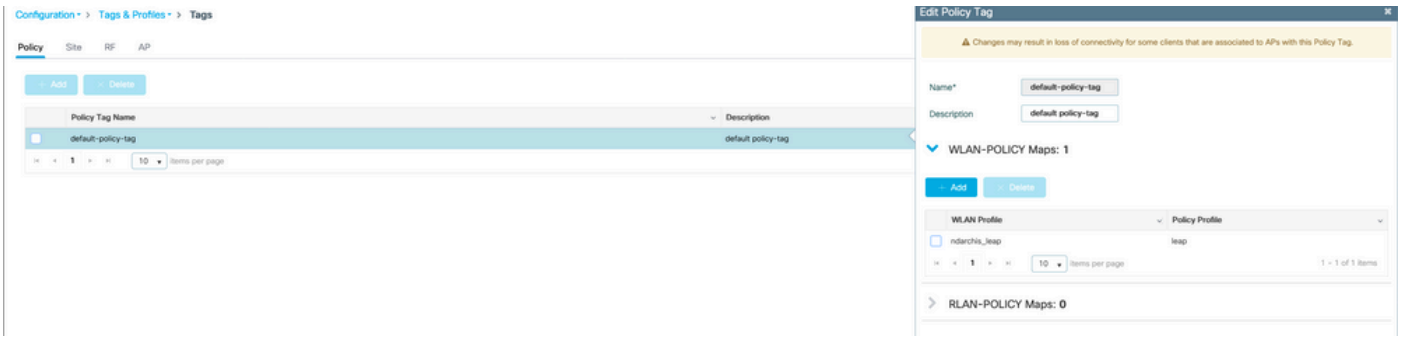
WLAN에 대한 정책 프로필을 생성합니다.

이 예에서는 flexconnect 로컬 스위칭이지만 vlan 1468의 중앙 인증 시나리오를 보여주지만 이는 네트워크에 따라 다릅니다.



Configuration(컨피그레이션) > Tags and profiles(태그 및 프로필) > Tags(태그)로 이동합니다.

태그 내의 정책 프로필에 WLAN을 할당합니다.



8단계. 액세스 포인트에 정책 태그를 구축합니다.

이 경우 단일 AP의 경우 AP에 직접 태그를 할당할 수 있습니다.

Configuration(컨피그레이션) > Wireless(무선) >Access points(액세스 포인트)로 이동하여 구성할 AP를 선택합니다.

할당된 태그가 사용자가 구성한 태그인지 확인합니다.

다음을 확인합니다.

기본 컨피그레이션 행은 다음과 같습니다.

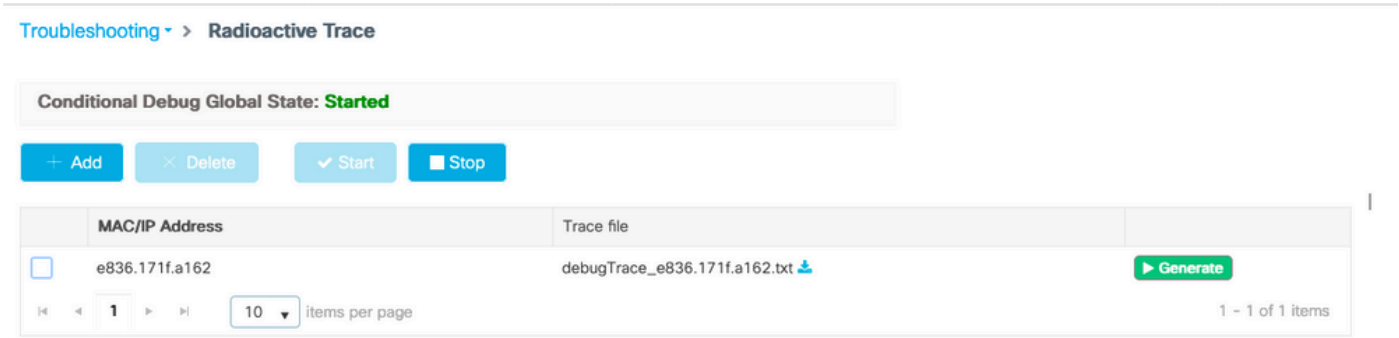
```
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download default local
aaa local authentication default authorization default
eap profile mylocaleap
method peap
pki-trustpoint admincert
user-name 1xuser
creation-time 1572730075 description 1xuser
password 0 Cisco123
type network-user description 1xuser
wlan ndarchis_leap 1 ndarchis_leap
local-auth mylocaleap
security dot1x authentication-list default
no shutdown
```

문제 해결

Cisco IOS® XE 16.12 및 이전 릴리스는 로컬 eap 인증을 위해 TLS 1.0만 지원하는데, 이 경우 클라이언트에서 TLS 1.2만 지원하는 경우가 더 일반적입니다. Cisco IOS® XE 17.1 이상에서는 TLS 1.2 및 TLS 1.0을 지원합니다.

연결에 문제가 있는 특정 클라이언트의 문제를 해결하려면 RadioActive Tracing을 사용합니다. Troubleshooting(트러블슈팅) > RadioActive Trace(RadioActive 추적)로 이동하여 클라이언트 mac 주소를 추가합니다.

해당 클라이언트에 대한 추적을 활성화하려면 시작을 선택합니다.



문제가 재현되면 Generate(생성) 버튼을 선택하여 디버깅 출력이 포함된 파일을 생성할 수 있습니다.

잘못된 암호로 인해 연결하지 못한 클라이언트의 예

```
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.781 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.784 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.785 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.788 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.791 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.792 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.795 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.796 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.804 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.805 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [eap] [23294]: (info): FAST:EAP_FAIL from inner method MSCHAP
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Sen
2019/10/30 14:54:00.808 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rec
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] EAP
2019/10/30 14:54:00.811 {wncd_x_R0-0}{2}: [caaa-authen] [23294]: (info): [CAAA:AUTHEN:66000006] DEBUG: r
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [eap-auth] [23294]: (info): FAIL for EAP method name: EAP-FAS
2019/10/30 14:54:00.812 {wncd_x_R0-0}{2}: [dot1x] [23294]: (info): [e836.171f.a162:capwap_90000004] Rai
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [errmsg] [23294]: (note): %DOT1X-5-FAIL: Authentication faile
2019/10/30 14:54:00.813 {wncd_x_R0-0}{2}: [auth-mgr] [23294]: (info): [e836.171f.a162:capwap_90000004] A
```

실패 시 추적

디버그가 활성화되지 않은 경우에도 trace-on-failure 명령을 사용하여 지정된 mac 주소에 대한 실패 이벤트 목록을 확인할 수 있습니다.

다음 예에서는 AAA 메서드가 처음에 없는 경우(AAA 서버 중단 이벤트) 몇 분 후에 클라이언트가 잘못된 자격 증명을 사용했습니다.

이 명령은 릴리스 16.12 이전의 show logging trace-on-failure summary이며, Cisco IOS® XE 17.1 이상의 show logging profile wireless (filter mac <mac>) trace-on-failure입니다. 17.1 이상에서는 클라이언트 mac 주소를 필터링할 수 있다는 점과 기술적인 차이가 없습니다.

```
Nico9800#show logging profile wireless filter mac e836.171f.a162 trace-on-failure
Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
```

```
executing cmd on chassis 2 ...
sending cmd to chassis 1 ...
Collecting files on current[1] chassis.
# of files collected = 30
Collecting files on current[2] chassis.
# of files collected = 30
Collecting files from chassis 1.
Time                        UUID                Log

--------------------------------------------------------------------------------------------------


2019/10/30 14:51:04.438     0x0      SANET_AUTHC_FAILURE - AAA Server Down username , audit session id
2019/10/30 14:58:04.424     0x0      e836.171f.a162 CLIENT_STAGE_TIMEOUT State = AUTHENTICATING, WLAN p
```

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.