IBNS 2.0 및 인터페이스 템플릿으로 유선 802.1X AP 인증 표준화

목차

소개

이 문서에서는 IBNS 2.0 인터페이스 템플릿을 사용하는 802.1X 컨피그레이션에 대해 설명합니다.

문제 설명

포트 보안에 IEEE 802.1X를 사용하는 것이 일반적인 모범 사례입니다. 네트워크 보안을 개선하는 것 외에도, 네트워크 전반에 표준화된 액세스 포트 구성을 허용하여 스위치 구축을 간소화합니다.

이 설명서에서는 표준화된 단일 스위치 포트 컨피그레이션을 엔드 디바이스와 Cisco AP(Access Point) 모두에 사용하는 방법에 대해 설명합니다. 모든 스위치 포트가 처음에는 표준 액세스 포트로

작동하며 IEEE 802.1X 인증을 수행하지만, 인증된 AP는 구축 시나리오에 따라 다른 작동 모드를 필요로 할 수 있습니다.

특히 여러 SSID의 클라이언트 트래픽이 로컬로 브리지되기 때문에 FlexConnect 로컬 스위칭 모드에서 작동하는 AP는 트렁크 포트에서 작동해야 합니다. 따라서 스위치 인터페이스는 인증 성공 후 액세스 포트에서 트렁크 포트로 동적으로 전환되어야 합니다.

단순한 엔드 디바이스가 아닌 인프라 디바이스를 연결하는 액세스 포트에는 기본 액세스 포트 동작과 다른 인터페이스 컨피그레이션이 필요한 경우가 많습니다.

따라서 인증 프로세스 중에 스위치 인터페이스 컨피그레이션을 동적으로 수정해야 합니다. 지난 몇 년간 Auto SmartPorts 및 EEM(Embedded Event Manager) 애플릿을 비롯한 몇 가지 접근 방식이 이 동작을 달성하는 데 사용되었습니다. 현재 권장되는 솔루션은 인터페이스 템플릿과 함께 IBNS 2.0[1]이며, 인증 성공 후 인터페이스 구성을 동적으로 변경할 수 있는 확장 가능하고 일관된 방법을 제공합니다.

접근 방식

정상적으로 작동하는 설정을 위해서는 다양한 구성 요소가 올바르게 구성되어 있어야 합니다.

- Radius 서버(Identity Service Engine)
- 스위치
- 액세스 포인트/무선 LAN 컨트롤러

기존 문서(마지막에 있는 참조 참조)가 있으므로 이 문서의 특정 시나리오에 중점을 두고 기존 문서를 지원 자료로 참조합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC(Wireless Lan Controller) 및 LAP(Lightweight AP)
- Cisco 스위치 및 ISE의 802.1x
- EAP(Extensible Authentication Protocol)
- RADIUS(Remote Authentication Dial-In User Service)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

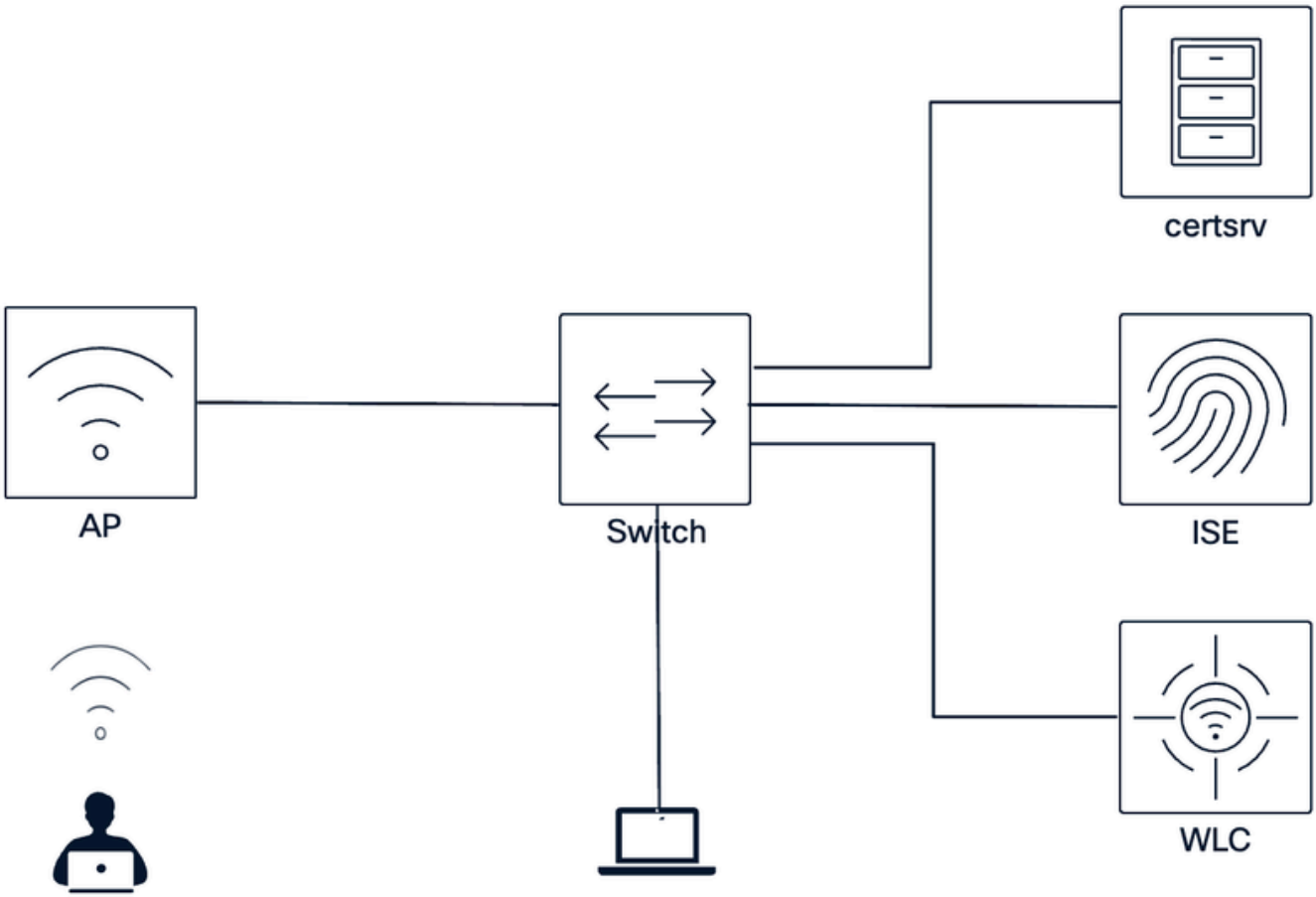
- Cisco C9350 - IOS XE 26.1.1a
- Cisco C9800-40 WLC - IOS XE 26.1.1
- ISE 버전 3.5 패치 1
- AP CW917x, CW916x

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.

컨피그레이션은 또한 netascode.cisco.com에 설명되어 있습니다. 스위칭 및 ISE의 데이터 모델을 통해 설정을 쉽게 복제할 수 있습니다.

설정

네트워크 다이어그램



샘플 설정

여기서는 단일 시나리오에 초점을 맞추고 구성 조각 및 단계별 지침을 제공합니다. 여러 가지 다양한 변형이 있으므로 이를 지적하고 이를 위해 기존 문서를 참조합니다.

이 가이드에서 다루는 시나리오는 다음과 같습니다.

- EAP-FAST 인증을 사용하는 AP 유선 Dot1X
- C9800 WLC를 통해 프로비저닝된 Dot1X 자격 증명
- Flex Connect 로컬 스위칭 모드의 AP

이 설계에서 switchport는 초기에 MAB 폴백과 함께 공통 폐쇄 모드 802.1X 컨피그레이션을 사용합니다. 첫 번째 온보딩 중에는 AP에 아직 802.1X 자격 증명이 없을 수 있으므로 ISE는 WLC 또는 Catalyst Center에 연결할 수 있는 제한된 액세스로 MAB를 통해 AP에 권한을 부여할 수 있습니다. 자격 증명 또는 인증서가 프로비저닝되면 AP는 유선 802.1X 인증을 수행합니다. 그런 다음 ISE는 AP_FLEX_TRUNK 인터페이스 템플릿에 적용되는 권한 부여 결과를 반환하여 포트를 필요한 FlexConnect 트렁크 컨피그레이션으로 변환합니다.

Variations				
Auth Types	MAB	EAP-FAST	EAP-PEAP	EAP-TLS
Provisioning of AP Dot1x supplicant	Wireless LAN Controller	Catalyst Center		
Certificate Rollout method	SCEP	EST		

표 1: 개요의 추가 변형 및 옵션

AP 설정

유선 Dot1x 인증을 AP와 함께 사용하려면 먼저 선택한 인증 방법에 따라 자격 증명 및/또는 인증서를 AP에 롤아웃해야 합니다.

일반적으로 Cisco Catalyst AP Dot1x 서 플리 컨 트는 EAP-FAST, EAP-PEAP 또는 EAP-TLS를 지원 합니다. 또한 MAB는 옵션일 수도 있습니다. 특히 AP가 EAP 유형 인증을 실행할 수 있도록 자격 증명 또는 인증서를 먼저 수집해야 하기 때문입니다.

- MAB:
  - AP측 설정 불필요
  - 하드웨어 MAC 주소를 관리하려면 툴링이 필요합니다.
  - 쉽게 스푸핑할 수 있음
  - 공통 포트 컨피그레이션 허용

- EAP-FAST:
  - 사용자 이름/비밀번호 기반
  - 간편한 배포
  - ISE에서 활성화된 익명 대역 내 PAC 프로비저닝 필요

- EAP-PEAP:
  - 사용자 이름/비밀번호 기반
  - 서버 검증을 위한 인증서 필요
  - 그에 따라 인증서 갱신을 계획해야 합니다.

- EAP-TLS:
  - 인증서 기반
  - 그에 따라 인증서 갱신을 계획해야 합니다.

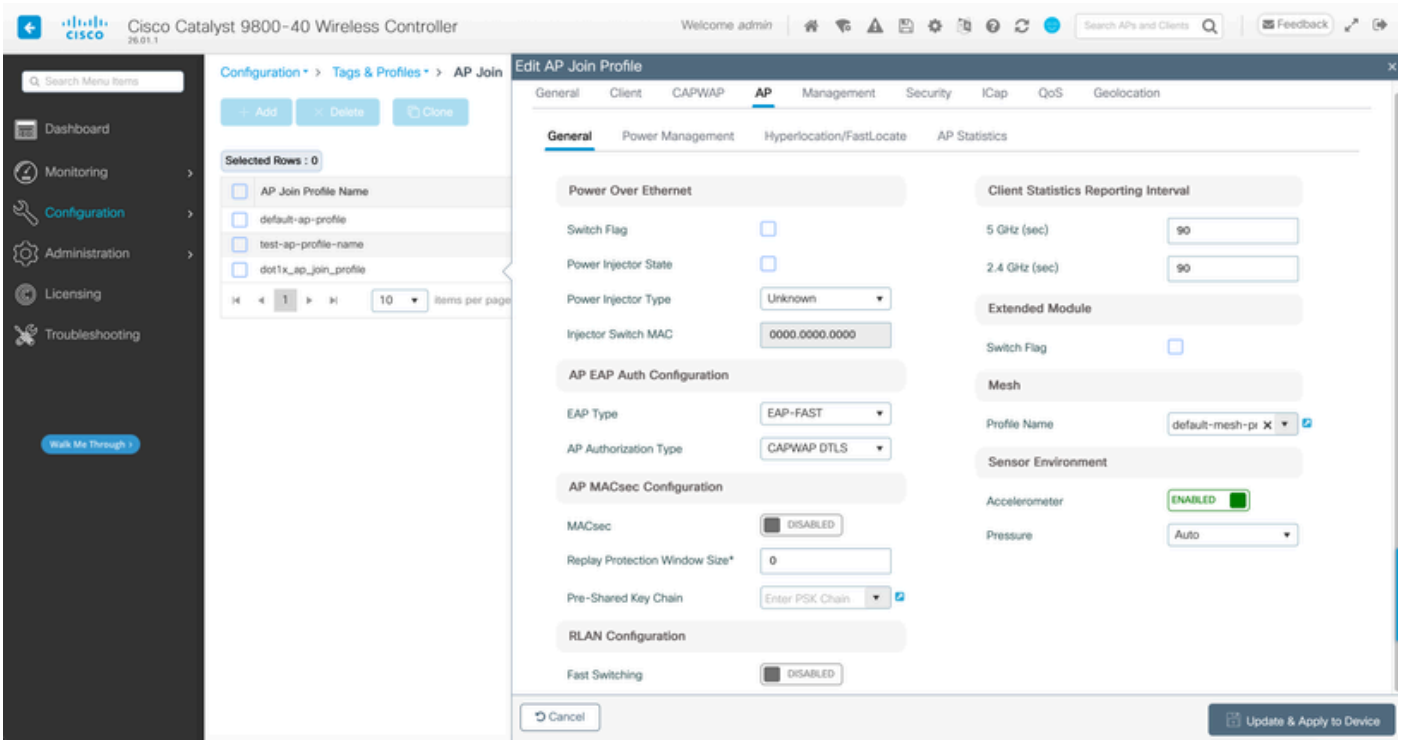
AP 유선 Dot1X 서플리컨트를 구성하려면 Wireless LAN Controller 또는 Catalyst Center를 통한 두 가지 방법이 있습니다. 이에 대해서는 여기에서 설명합니다. 이러한 세부 정보로 들어가기 전에 사용할 인증 유형을 미리 선택해야 합니다.

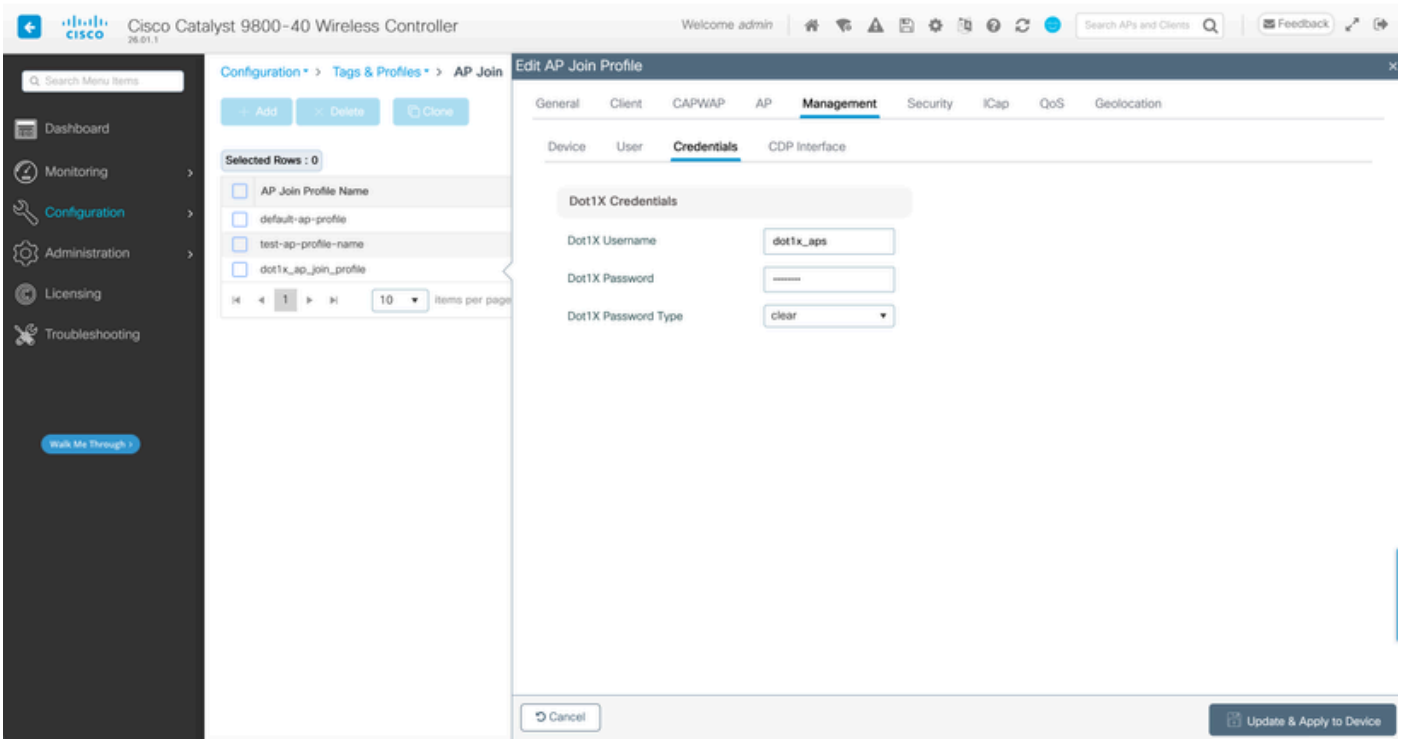
Cisco 9800 Wireless LAN Controller를 통해 유선 Dot1X 설정

인증서 기반 인증(EAP-PEAP 또는 EAP-TLS[1])을 선택한 경우 다음 단계로 SCEP[2] 또는 EST[3]을 통해 LSC(Locally Significant AP Certificates)를 발급할 방법을 결정해야 합니다.

이 시나리오와 같이 EAP-FAST를 사용할 경우 AP 조인 프로필을 생성하면 됩니다. 여기서 Dot1X 사용자 및 비밀번호를 입력하고 해당 조인 프로필을 사이트 태그에 바인딩한 다음 AP에 할당합니다.

GUI 구성





CLI 구성

```
ap profile dot1x_ap_join_profile
 country DE
description dot1x_ap_join_profile
 dot1x eap-type eap-fast
 dot1x username <DOT1X_USER> password 0 <DOT1X_PASSWORD>
```

Catalyst Center Plug and Play를 통해 유선 Dot1X 설정

PnP [4]가 작동하려면 Catalyst Center를 ISE와 통합해야 합니다. 이는 ISE와의 EAP 인증을 위해 AP측에서 서버 검증을 수행하는 데 필요한 인증서 때문에 부분적으로 필요합니다. 디바이스측 인증서의 경우 AP는 기본적으로 자체 내장 또는 해당 CA의 SubCA/SCEP에 의해 구성된 경우 Catalyst Center CA에서 발급한 인증서를 가져옵니다.

PnP를 통한 설정 프로세스에서는 디바이스가 WLC에 조인하기 전에 인증서 및/또는 크리덴셜을 프로비저닝할 수 있습니다.

스위치 구성

인증이 보안 메커니즘인 것 외에도, 이것은 또한 스위치 포트 구성을 표준화하는 방법입니다. 따라서 이들 부분에서는 이를 달성하기 위해 필요한 요소를 기술하고 있다. 이는 샘플 컨피그레이션이므로 반드시 검토하고 설정에 맞게 수정해야 합니다. 일반적으로 이 컨피그레이션은 Dot1x 및 대체 MAB가 데드 Radius 시나리오, 재인증 등의 적절한 처리를 수행하도록 허용합니다.

전역 Radius 특성:

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Radius 서버 그룹:

```
!
radius server client-radius-server01
 address ipv4 <ISE01-PSN-IP> auth-port 1812 acct-port 1813
 timeout 10
 retransmit 1
 automate-tester username dummy ignore-acct-port probe-on key 6 <RADIUS-SECRET>
!
!
aaa group server radius client-radius-group
 server name client-radius-server01
```

```
 ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

AAA 구성:

```
!
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group client-radius-group
aaa authorization network default group client-radius-group
aaa accounting Identity default start-stop group client-radius-group
aaa accounting update newinfo periodic 2880
!
aaa server radius dynamic-author
 client <ISE01-PSN-IP> server-key 6 <RADIUS-SECRET>
!
```

IBNS2.0 클래스 맵 및 서비스 템플릿:

```
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template CRITICAL_AUTH_VLAN
 vlan <CRITICAL-AUTH-VLAN>
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
```

```
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
```

IBNS 2.0 서비스 정책:

```
!
policy-map type control subscriber WiredDot1xClosedAuth_1X_MAB
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 20
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 50 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 60 class DOT1X_TIMEOUT do-until-failure
  10 authenticate using mab priority 20
 70 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
```

```
  30 authentication-restart 60
!
```

인터페이스 템플릿:

```
!
template AP_FLEX_TRUNK
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport trunk native vlan <TRUNK-NATIVE-VLAN>
 switchport trunk allowed vlan <TRUNK-ALLOWED-VLANS>
 switchport mode trunk
 mab
 access-session host-mode multi-host peer
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
template DEFAULT-ACCESS-PORT
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 mab
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
```

인터페이스 구성:

```
!
interface TenGigabitEthernet1/0/1
 switchport access vlan <DEFAULT-ACCESS-VLAN>
 switchport mode access
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DEFAULT-ACCESS-PORT
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

글로벌 필수:

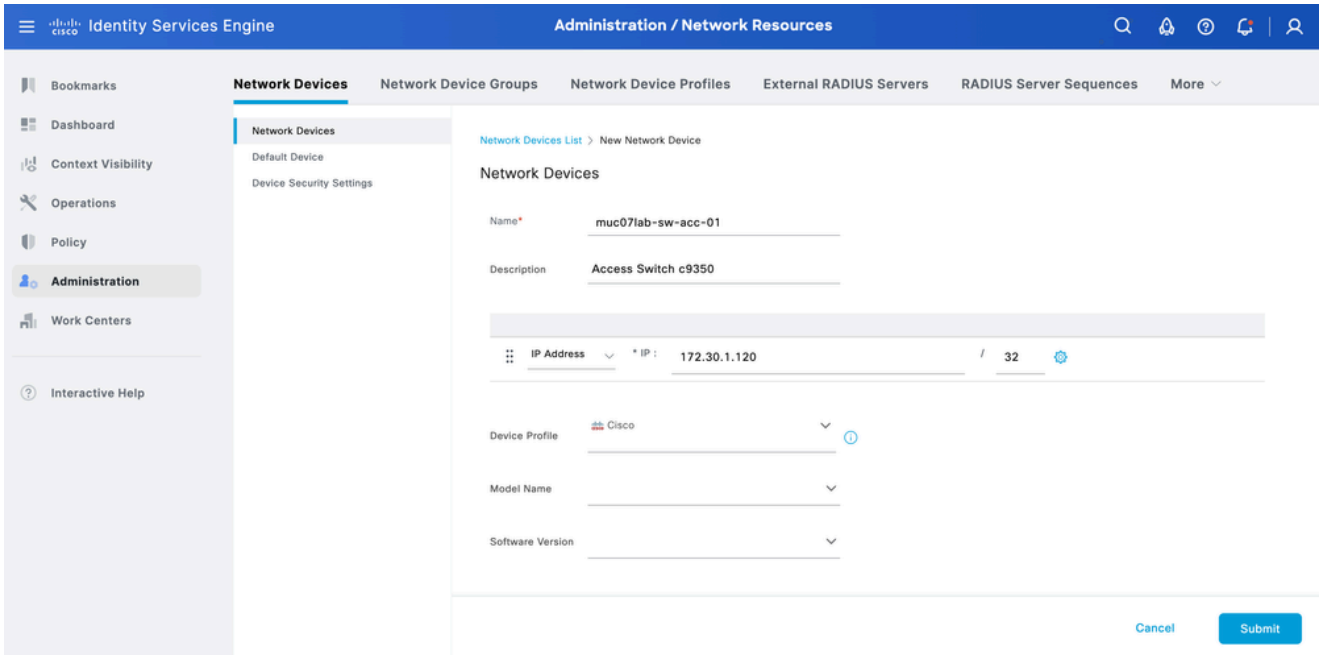
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

참고: CW9178을 사용할 경우 AP는 인증 중에 두 개의 MAC 주소를 나타냅니다. switchport가 err-disabled 상태가 되지 않도록 하려면 호스트 모드 다중 인증에 대해 포트를 초기에 구성해야 합니다. 802.1X 인증에 성공하면 포트 컨피그레이션을 호스트 모드 멀티 호스트로 동적으로 변경하는 것이 좋습니다.

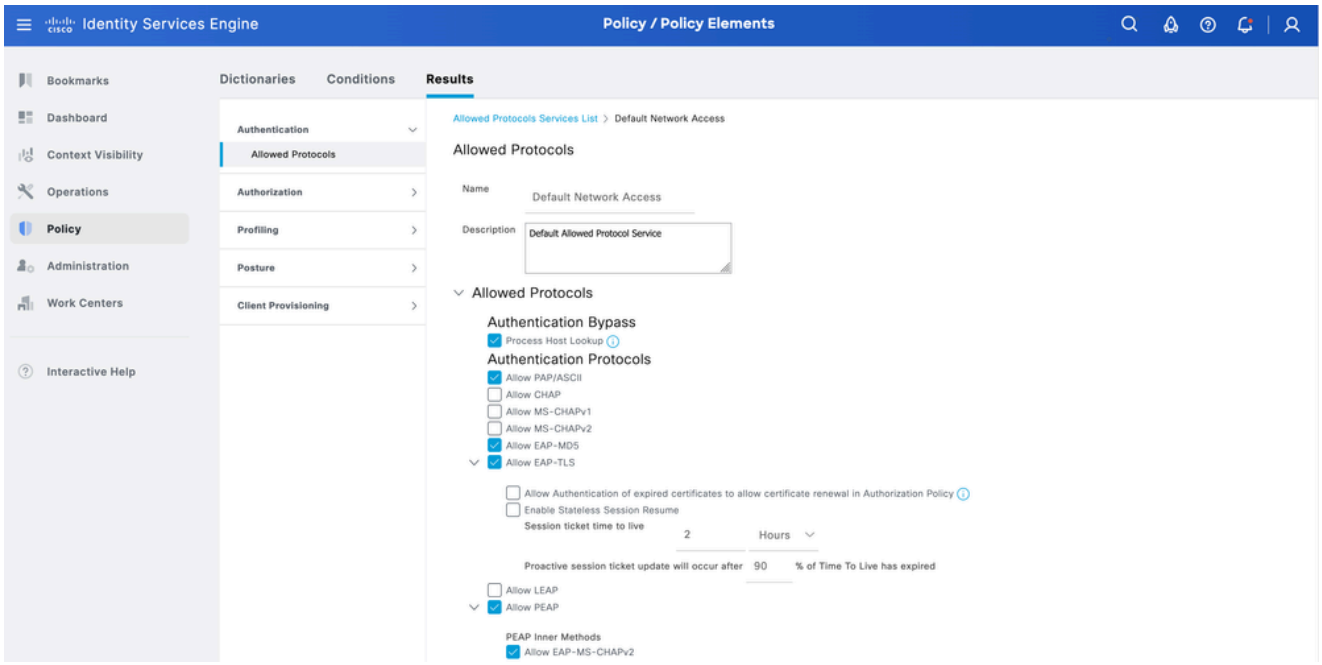
Identity Services Engine 구성

마지막으로, RADIUS 서버도 인증을 허용하도록 구성해야 합니다. 유선 Dot1x의 경우 광범위한 가이드[5]이 있으므로 이 경우 관련 부분에만 중점을 둡니다.

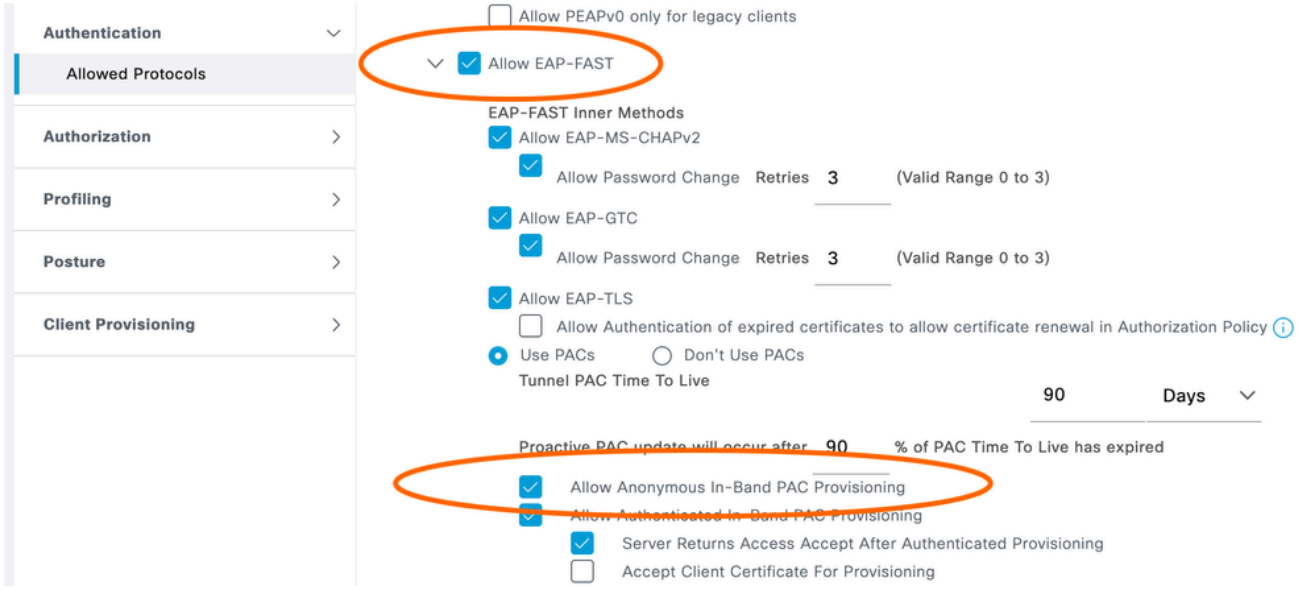
1. 스위치를 네트워크 액세스 디바이스로 추가합니다.
   > 관리 > 네트워크 리소스 > 네트워크 장치 > 추가



2. 사용 중인 EAP 프로토콜을 활성화합니다.
   > 정책 > 정책 구성 요소 > 결과 > 인증 > 허용 된 프로토콜



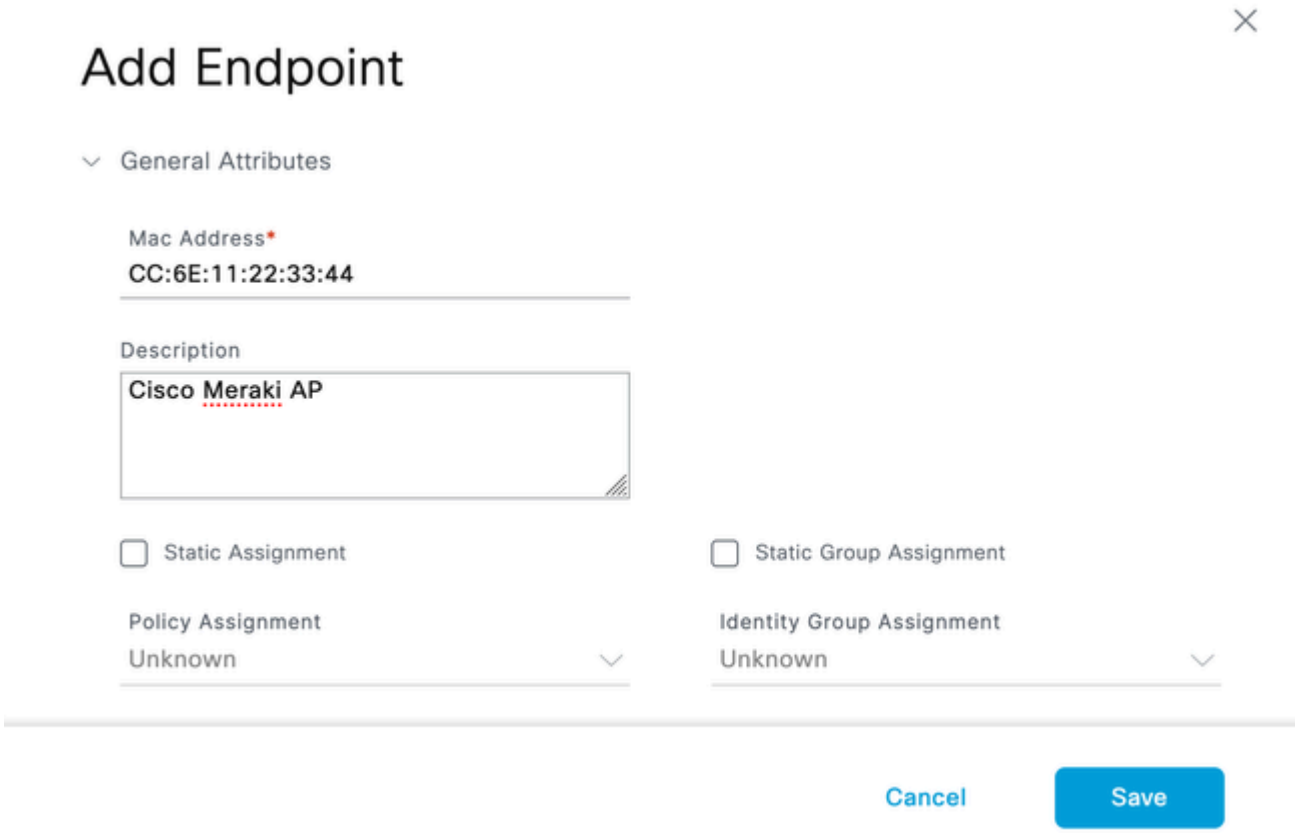
3. EAP-FAST를 사용하는 시나리오에서는 "익명 대역 내 PAC 프로비저닝"을 활성화해야 합니다.



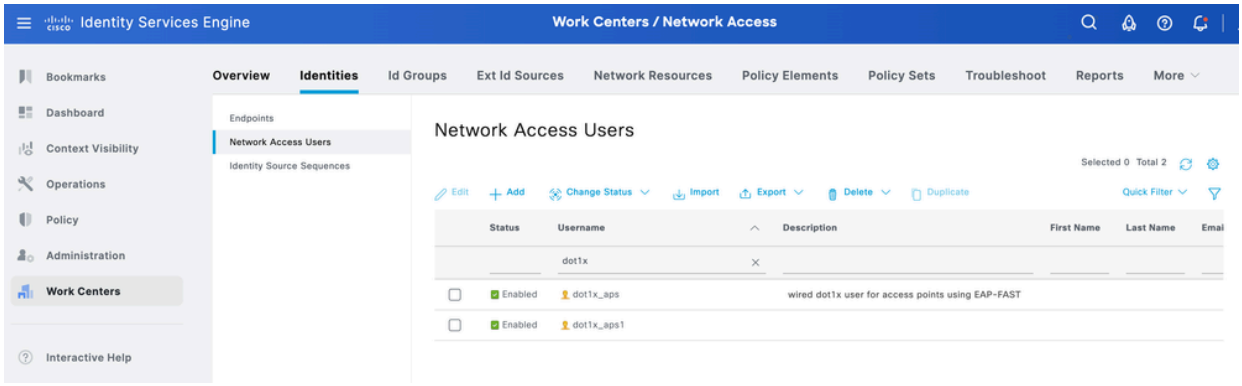
4. ID 추가

> Work Centers(작업 센터) > Network Access(네트워크 액세스) > Identity(ID)

a. 성공적인 작업을 위해 프로세스는 일반적으로 두 단계로 구성됩니다. 처음에는 AP에 자격 증명이 없으므로 EAP 인증에 응답할 수 없습니다. 따라서 스위치 포트는 먼저 MAB를 사용하여 AP를 인증해야 합니다. 이는 일반 권한 부여 정책, 위치 기반 정책 또는 디바이스 프로파일링을 기반으로 할 수 있습니다. 사용된 정책에 관계없이 초기 MAB 인증에 성공하여 AP가 CAPWAP를 통해 WLC에서 또는 PnP(Cisco Catalyst Center)를 통해 자격 증명을 얻을 수 있도록 해야 합니다.

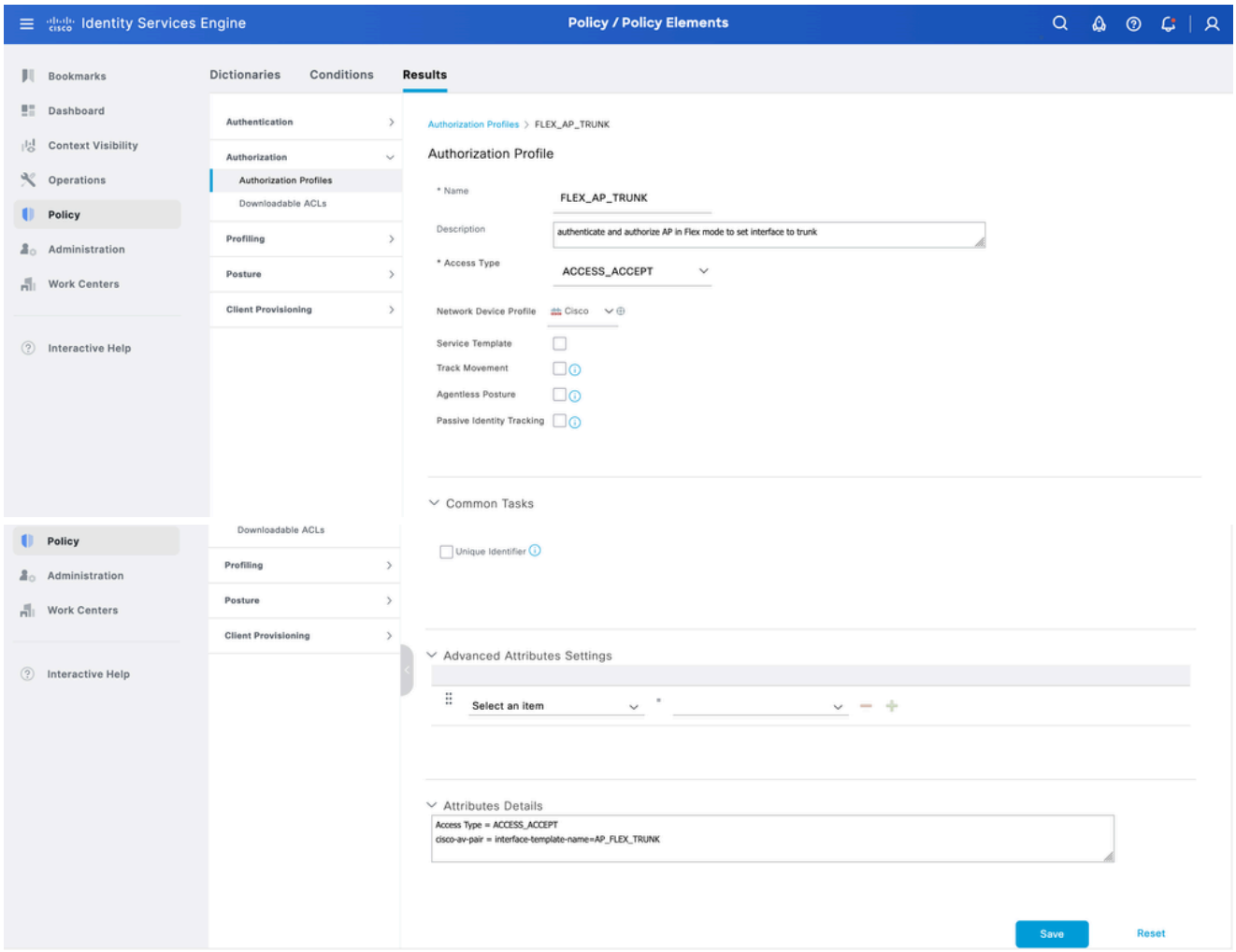


b. AP가 자격 증명/인증서를 수집한 후 AP 유선 Dot1X 신청자는 EAPoL에 응답하고 Dot1X는 전체 액세스를 위해 AP를 활성화하는 인증을 위한 후속 방법입니다.
이 시나리오에서는 사용자 이름/비밀번호를 추가해야 합니다.

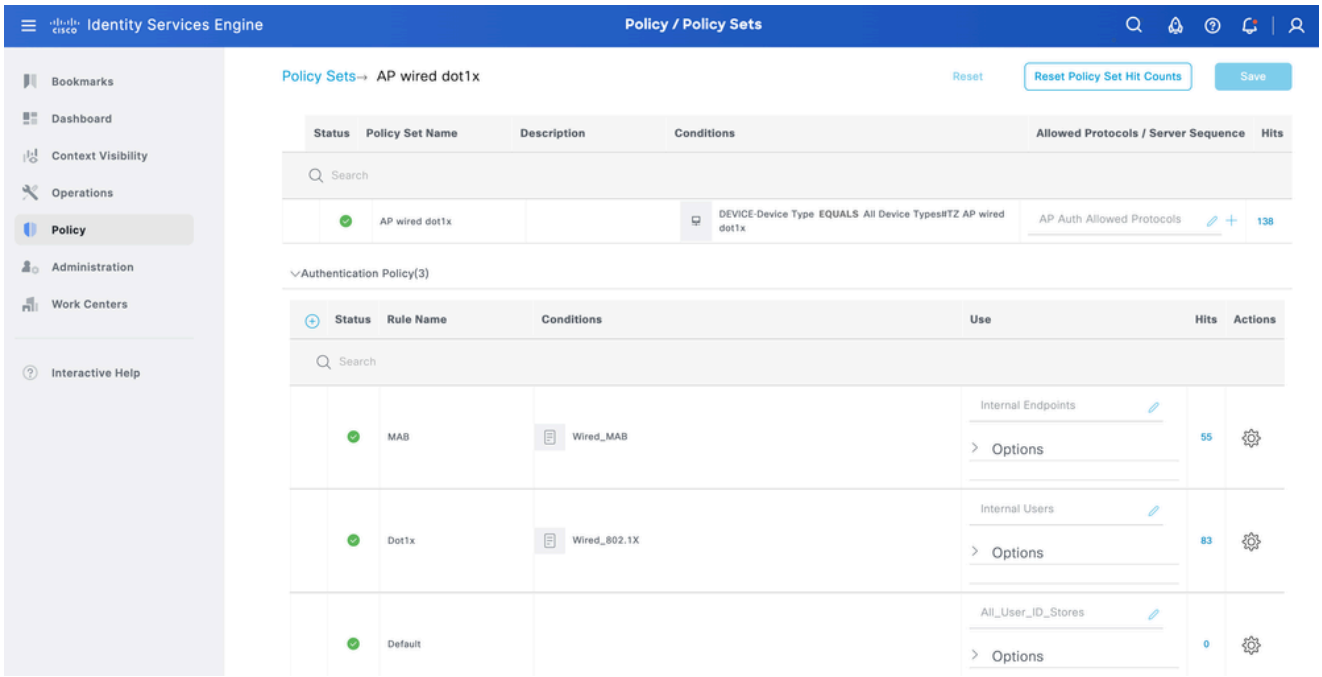


5. 권한 부여 프로파일 생성
권한 부여 프로파일은 필수 av 쌍으로 응답합니다. 여기서는 switchport를 동적으로 수정하므로 interface-template을 구성해야 합니다.
> 정책 > 정책 구성 요소 > 결과 > 인증 > 인증 프로파일

이름: FLEX_AP_TRUNK
액세스 유형: 액세스_수락
인터페이스 템플릿: AP_FLEX_TRUNK

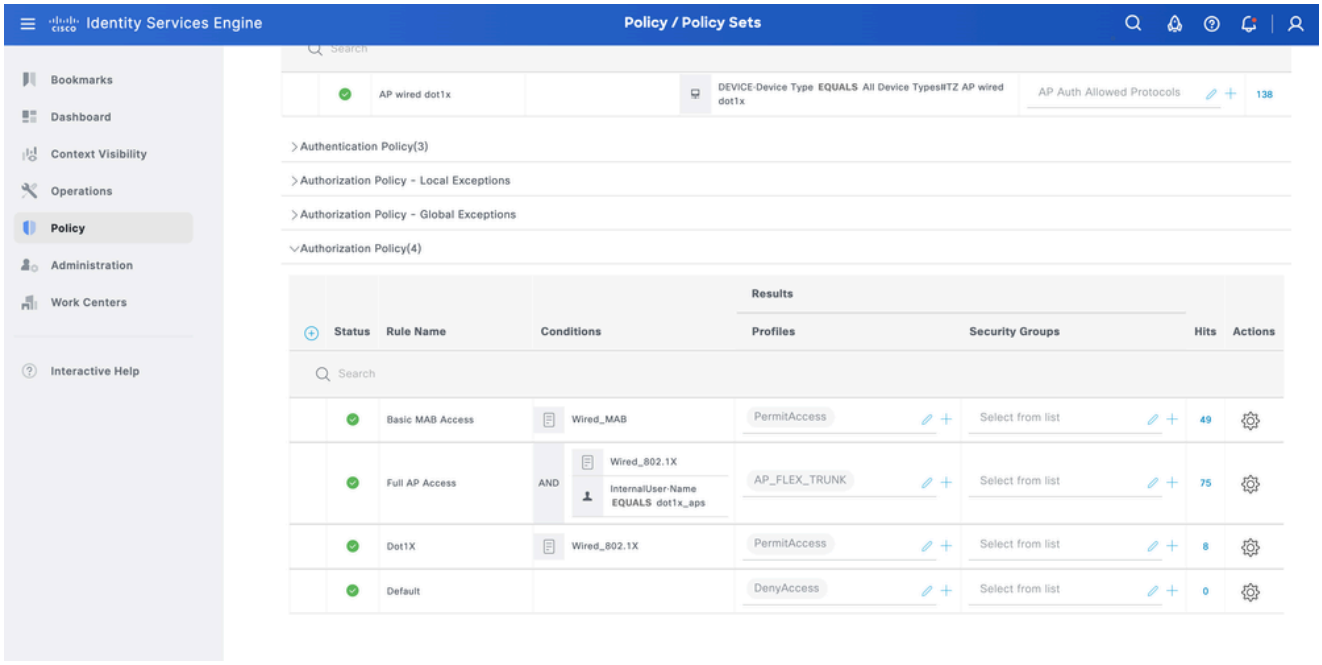


6. 권한 부여 정책 생성
   MAB 및 유선 Dot1X를 허용 하고 적절 한 ID 저장소에서 엔드 포인트/사용자를 검색 하는 인증 정책을 만듭니다.



MAB에 대한 요구 사항에 따라 제한된 액세스 권한 부여 결과를 입력하고 Dot1x에 대한 참조

된 인터페이스 템플릿 av 쌍을 포함하는 전체 AP 액세스를 입력합니다.



다음을 확인합니다.

이 컨피그레이션이 적용되면 AP를 스위치에 연결합니다. 전제 조건으로는 기본 네트워크 설정, 이 경우 WLC를 가리키는 옵션 43이 있는 액세스 VLAN의 DHCP 풀이 AP와 WLC의 통신을 가능하게 해야 합니다.

AP 명령

```
show ap authentication status
show crypto
show crypto pki trustpool
```

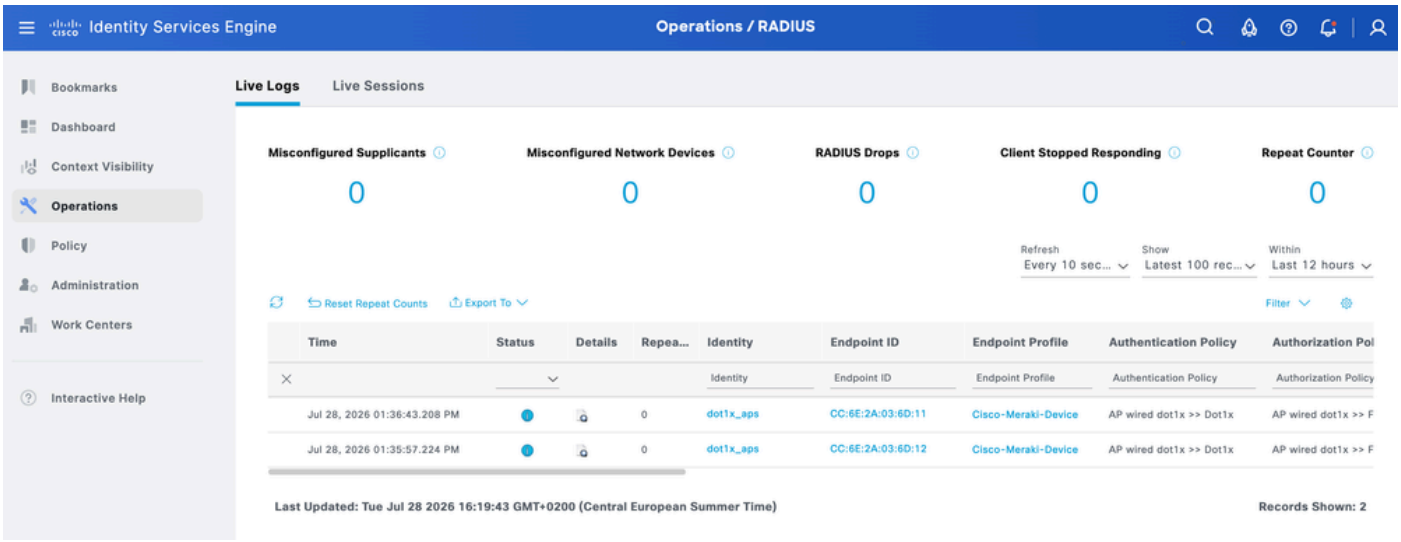
스위치 명령

```
show access-session
show aaa servers
show access-session interface <INTERFACE> details
show template interface binding target <INTERFACE>
show derived-config interface <INTERFACE>

Sample output:
!
C9350-02-R11#show access-session interface te1/0/1
Interface MAC Address Method Domain Status Fg Session ID
-----------------------------------------------------------------------------------------
```

```
Te1/0/1 6cef.1122.3344 dot1x DATA Auth 09FE1FAC000000948FF60A2F
```

ISE



약어 목록

약어	확장
AAA	인증, 권한 부여 및 계정 관리(aaa)
AP	액세스 포인트
인증C	인증
인증Z	Ahthorization(권한 부여)
캐나다	인증 기관
CISP	클라이언트 정보 시그널링 프로토콜
점1x	IEEE 802.1X
EAP	확장 가능 한 인증 프로토콜
동부	보안 전송을 통한 등록
빠름	보안 터널링을 통한 유연한 인증
IBNS	ID 기반 네트워킹 서비스
ISE	ISE(Identity Services Engine)
MAB	MAC 인증 우회
NAD	네트워크 액세스 장치
PEAP	보호 된 확장 가능 한 인증 프로토콜

SCEP	단순 인증서 등록 프로토콜
TLS	전송 계층 보안
WLC	무선 LAN 컨트롤러

참조

[1] LSC를 사용하는 PEAP 또는 EAP-TLS에 대해 AP에 802.1X 구성

[2] 9800 WLC에서 SCEP(Locally Significant Certificate Provisioning) 구성

[3] Cisco Wireless EST 온프레미스 구축 설명서

[4] 보안 AP 온보딩 - 향상된 네트워크 보안 소개

[5] ISE Secure Wired Access 규범적 구축 설명서

LSC용 [6] 컨피그레이션 가이드 섹션

[7] 9800 컨트롤러를 사용하여 액세스 포인트에 대한 802.1X 신청자 구성

[8] Dot1x를 사용하여 Flexconnect AP Switchport를 보호합니다.

[9] Cisco Catalyst 9800 Series Wireless Controller 소프트웨어 컨피그레이션 가이드, Cisco IOS XE 17.18.x - 802.1x

[11] Cisco Catalyst Center 사용 설명서, 릴리스 3.2.x - Cisco IOS XE 장치의 AP 프로필에 대한 관리 설정 구성

[12] 기본 switchport 컨피그레이션에 IBNS 2.0 및 인터페이스 템플릿 사용

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.