9800 컨트롤러를 사용하여 액세스 포인트에 대한 802.1X 신청자 구성

목차

소개

이 문서에서는 Cisco AP(액세스 포인트)를 802.1x 신청자로 구성하여 RADIUS 서버에 대한 스위치 포트에서 권한을 부여하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC(Wireless Lan Controller) 및 LAP(Lightweight Access Point)
- 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.

- WS-C3560CX, Cisco IOS® XE,15.2(3r)E2

- C9800-CL-K9, Cisco IOS® XE,17.6.1
- ISE 3.0
- AIR-CAP3702
- AIR-AP3802

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.

배경 정보

이 설정에서는 액세스 포인트(AP)가 802.1x 신청자 역할을 하며 EAP 방법 EAP-FAST를 사용하여 ISE에 대해 스위치에 의해 인증됩니다.

포트가 802.1X 인증을 위해 구성되면, 스위치에 포트에 연결된 디바이스가 성공적으로 인증될 때까지 802.1X 트래픽 이외의 트래픽은 포트를 통과할 수 없습니다.

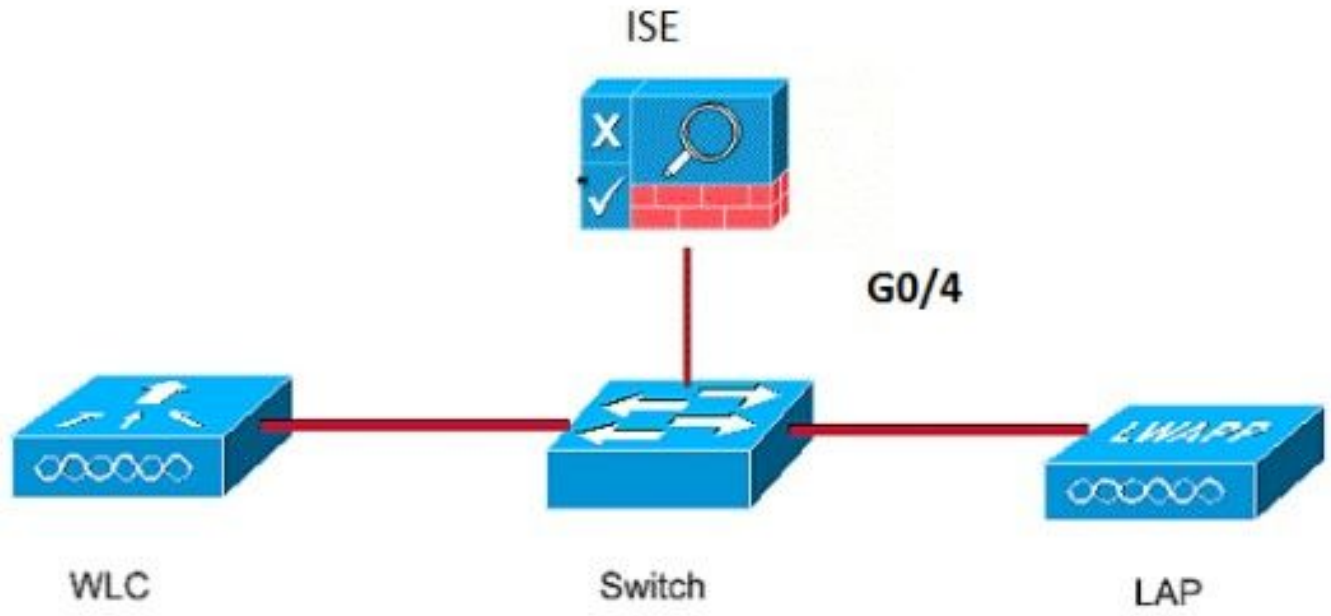
AP가 WLC에 연결되기 전 또는 WLC에 연결된 후 AP를 인증할 수 있습니다. 이 경우 LAP가 WLC에 연결된 후 스위치에 802.1X를 구성합니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.

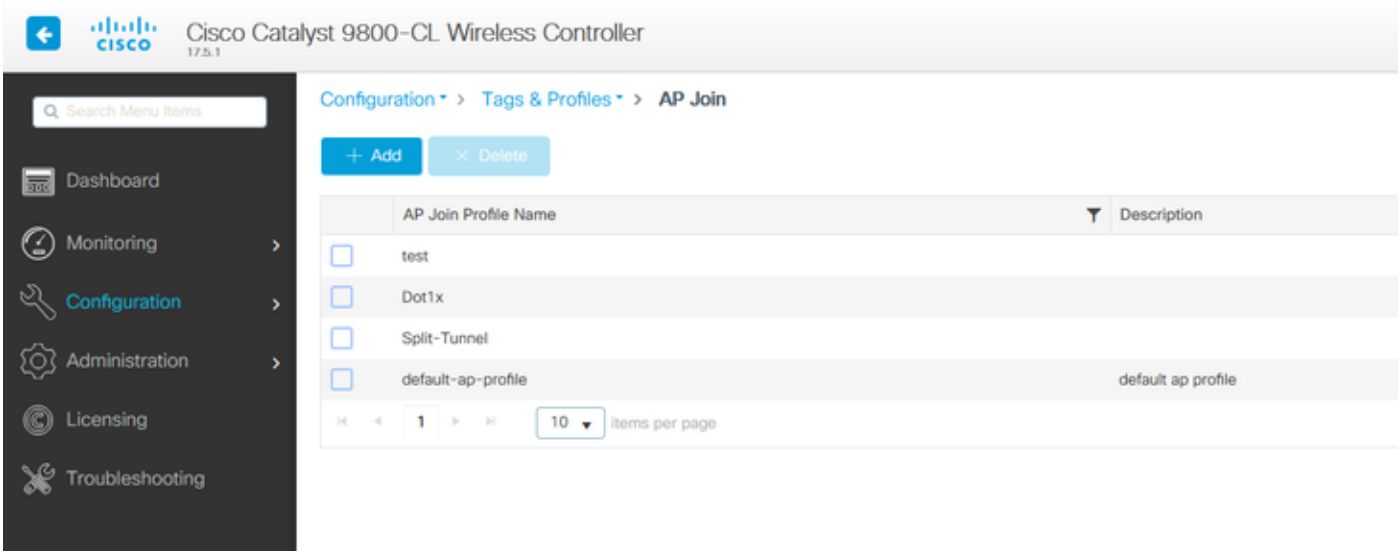


LAP를 802.1x 서플리컨트로 구성

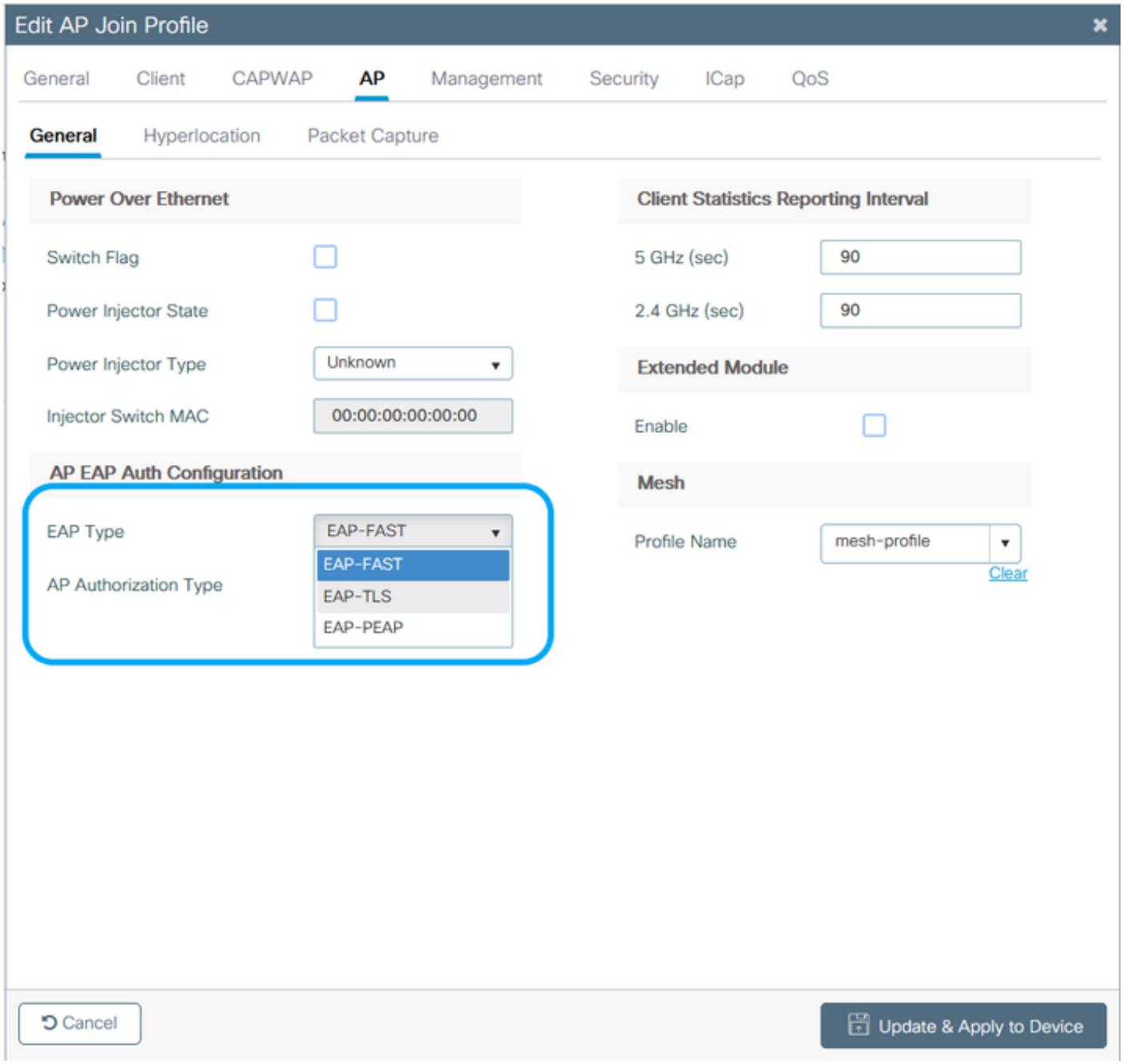
Ap가 이미 Wlc에 조인된 경우:

802.1x 인증 유형 및 LSC(Locally Significant Certificate) AP 인증 유형을 구성합니다.

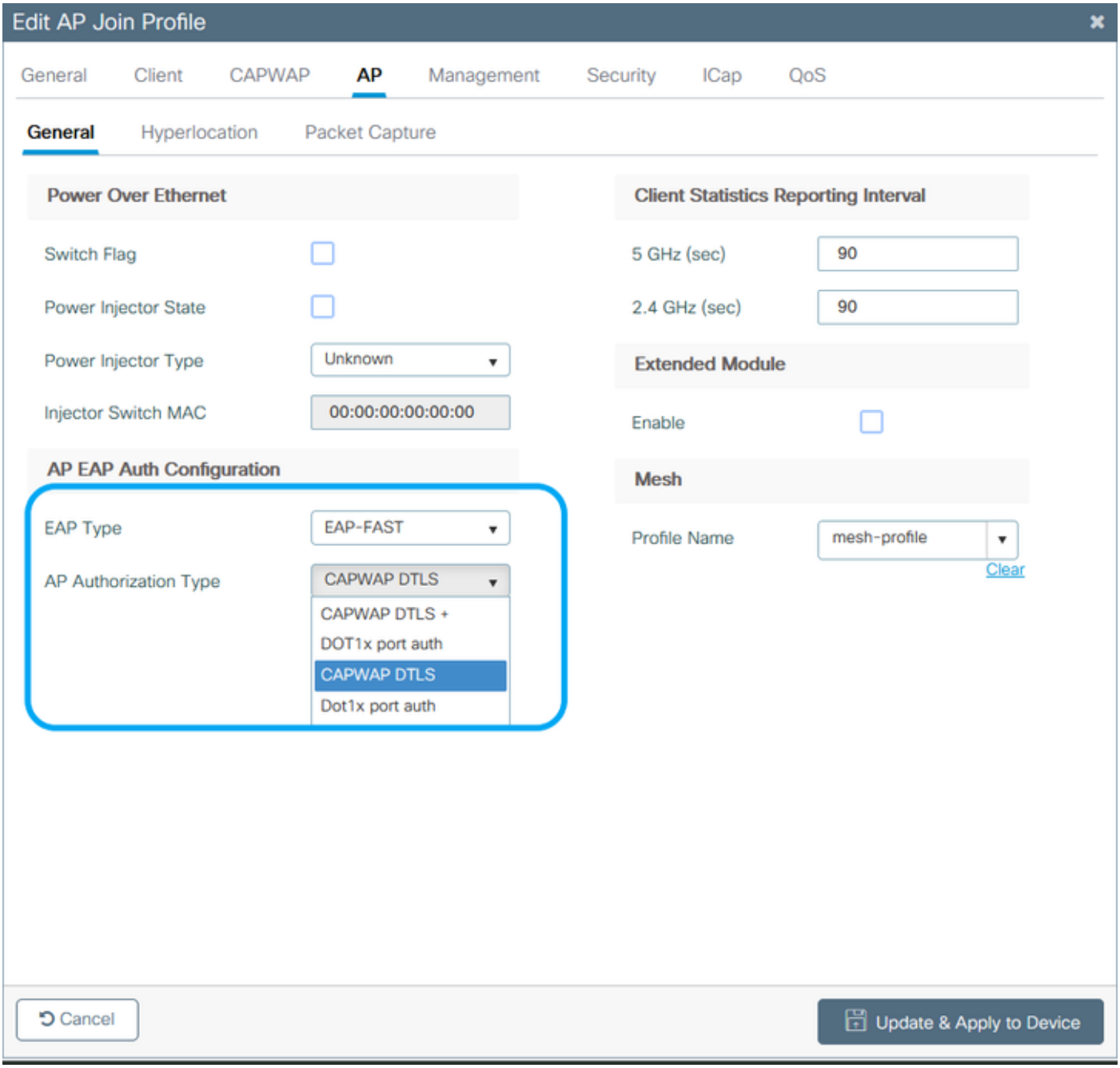
1단계. Configuration(컨피그레이션) > **Tags & Profiles(태그 및 프로필) > AP Join(AP 조인) > AP Join Profile(AP 조인 프로필) 페이지**에서 Add(추가)를 클릭하여**새 조인 프로필을 추가하거나 AP 조인 프로필을 수정할 때 해당 이름을 클릭합니다.**



2단계. AP Join Profile(AP 조인 프로파일) 페이지의 **AP > General(일반)**에서 **AP EAP Auth Configuration(AP EAP 인증 컨피그레이션) 섹션으로** 이동합니다. EAP **Type** 드롭다운 목록에서 EAP 유형을 EAP-FAST, EAP-TLS 또는 EAP-PEAP로 선택하여 dot1x 인증 유형을 구성합니다.

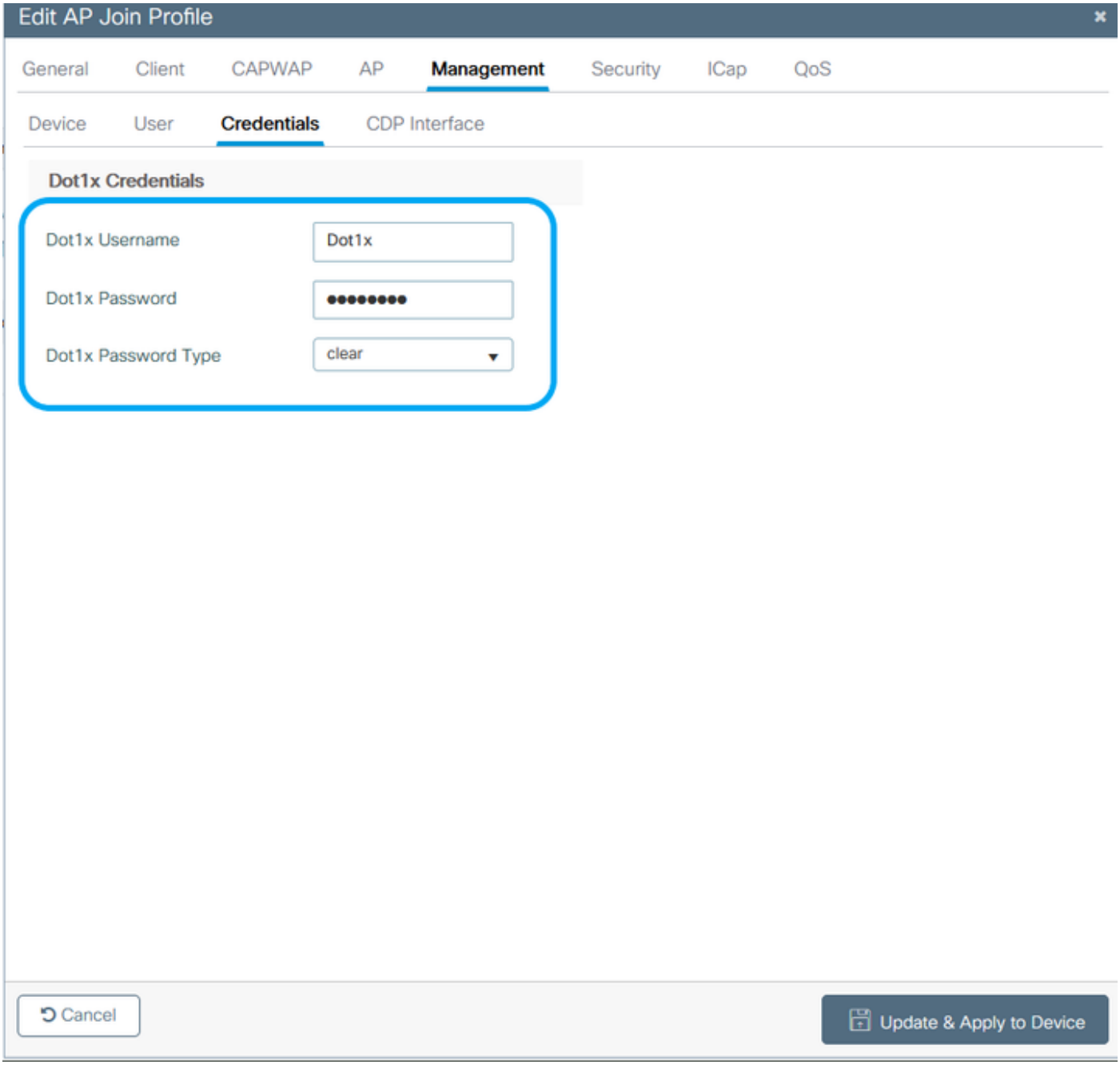


3단계. **AP Authorization Type(AP 권한 부여 유형)** 드롭다운 목록에서 유형을 CAPWAP DTLS + 또는 CAPWAP DTLS로 선택하고 Update **& Apply to Device(디바이스에 업데이트 및 적용)를 클릭합니다**.



802.1x 사용자 이름 및 비밀번호를 구성합니다.

1단계. **Management(관리) > Credentials(자격 증명) > Dot1x username and password details(Dot1x 사용자 이름 및 비밀번호 세부사항 입력)** > 적절한 802.1x 비밀번호 유형을 선택하고 > Update & Apply to Device(디바이스에 **업데이트 및 적용)를 클릭합니다**



Ap가 아직 WLC에 조인하지 않은 경우:

자격 증명을 설정하고 다음 CLI 명령을 사용하려면 LAP로 콘솔링해야 합니다(Cheetah OS 및 Cisco IOS® AP).

CLI:

```
LAP# debug capwap console cli
LAP# capwap ap dot1x username
```

AP에서 Dot1x 자격 증명을 지우려면(필요한 경우)

Cisco IOS® AP의 경우 AP를 다시 로드한 후 다음을 수행합니다.

CLI:

```
LAP# clear capwap ap dot1x
```

Cisco COS AP의 경우 AP를 다시 로드한 후 다음을 수행합니다.

CLI:

```
LAP# capwap ap dot1x disable
```

스위치 구성

스위치에서 전역적으로 dot1x를 활성화하고 ISE 서버를 스위치에 추가합니다.

CLI:

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

AP 스위치 포트를 구성합니다.

CLI:

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

AP가 **Flex Connect 모드(로컬 스위칭**)인 경우, 클라이언트 트래픽이 AP 레벨에서 릴리스되므로 포트에 여러 MAC 주소를 허용하도록 스위치 인터페이스에 추가 컨피그레이션을 수행해야 합니다.

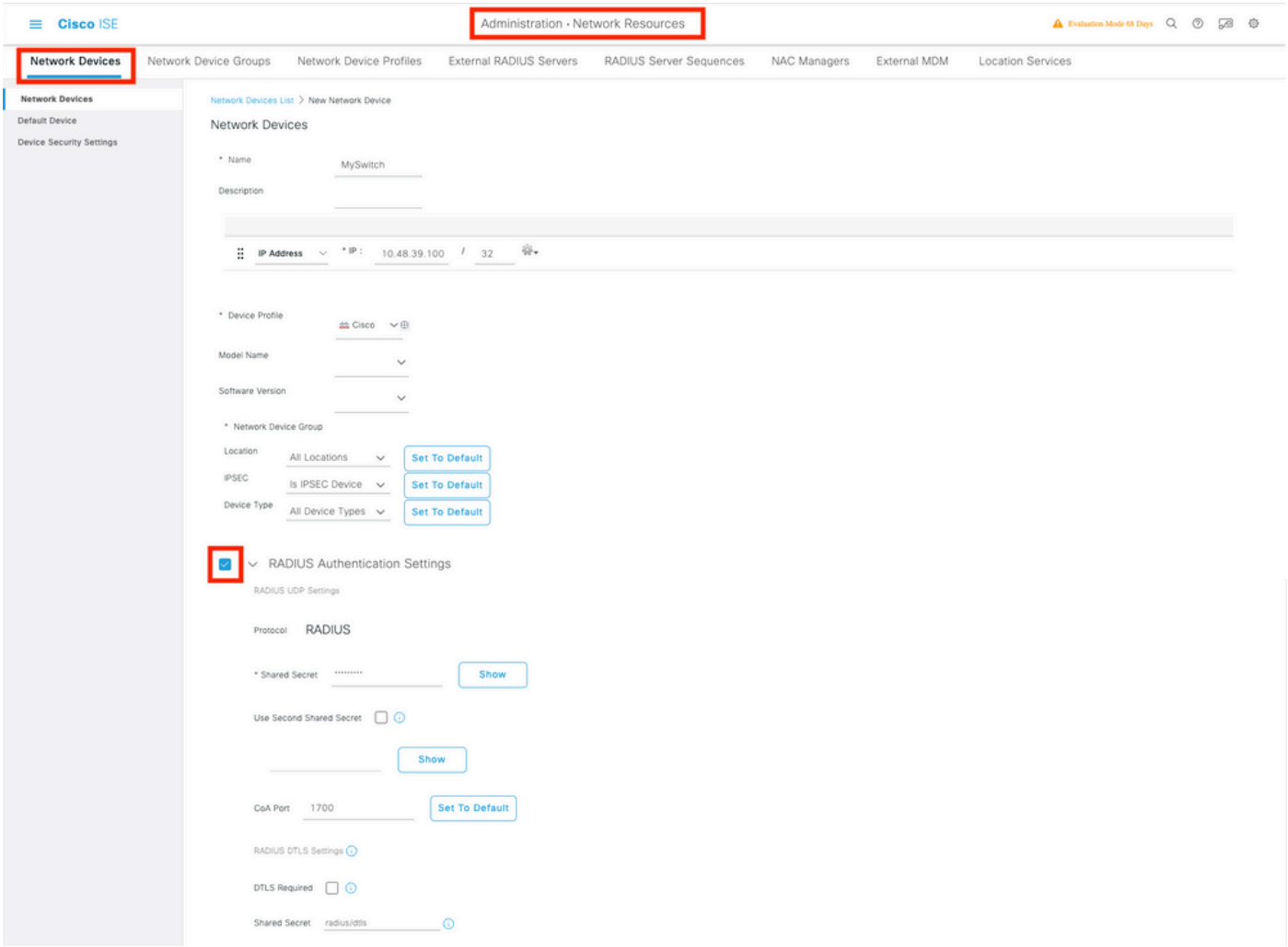
```
authentication host-mode multi-host
```

참고: 독자가 메모해야 함을 의미합니다. 참고에는 유용한 제안이나 문서에서 다루지 않는 자료에 대한 참조가 포함되어 있습니다.

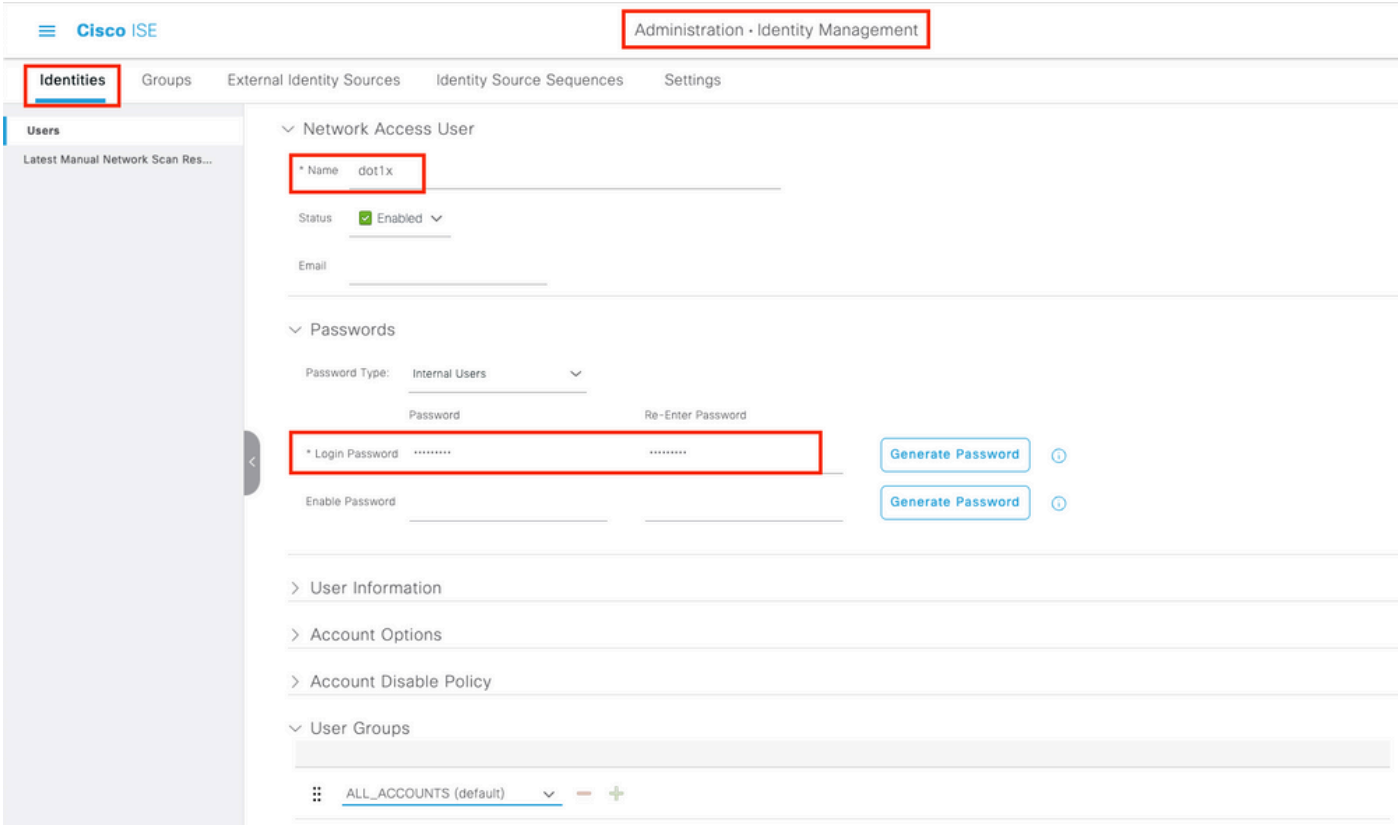
> **참고**: 멀티호스트 모드에서 첫 번째 MAC 주소를 인증한 다음 다른 MAC 주소를 무제한으로 허용합니다. 연결된 AP가 로컬 스위칭 모드로 구성된 경우 스위치 포트에서 호스트 모드를 활성화합니다. 클라이언트의 트래픽이 스위치 포트를 통과하도록 허용합니다. 보안 트래픽 경로를 원하는 경우 WLAN에서 dot1x를 활성화하여 클라이언트 데이터를 보호합니다

ISE 서버 구성

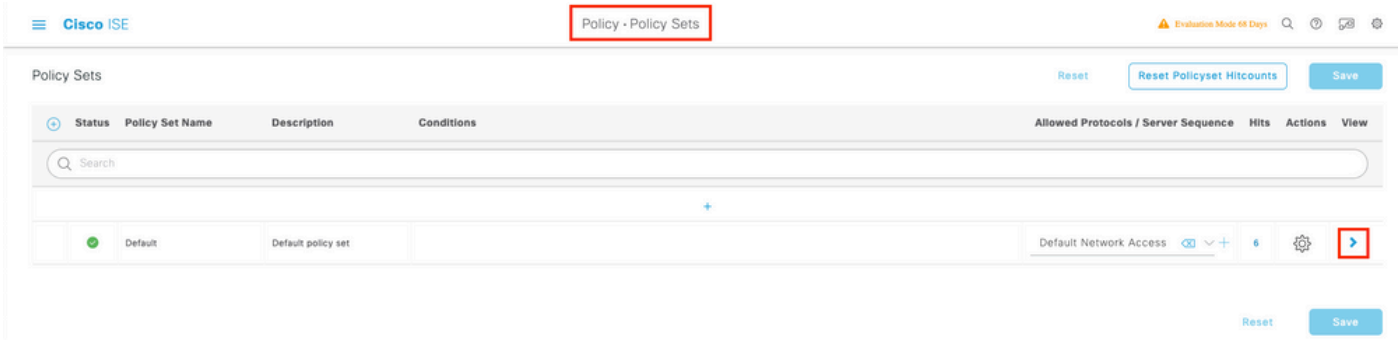
1단계. **스위치를 ISE 서버의 네트워크 디바이스로 추가합니다.** Administration(관리) > **Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > Add(추가)** > Enter Device name, IP address(디바이스 이름, IP 주소 입력), enable RADIUS Authentication Settings(RADIUS 인증 설정 활성화), Specify Shared Secret Value(공유 암호 값 지정), COA port(COA 포트를 기본값으로 유지) > Submit(제출)로 이동합니다.



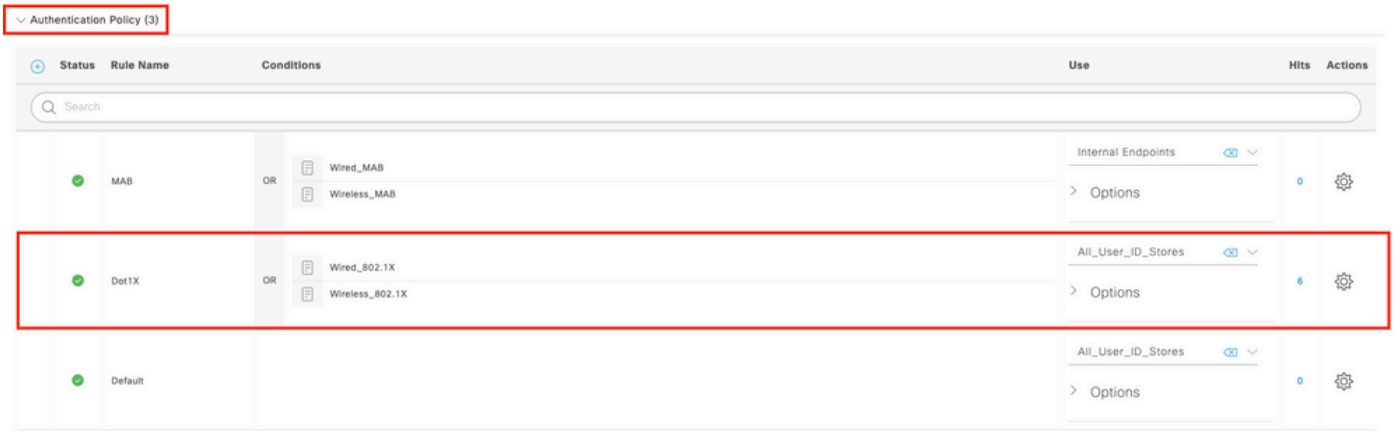
2단계. **ISE에 AP 자격 증명을 추가합니다**. Administration(관리) > **Identity Management(ID 관리) > Identities(ID) > Users(사용자)**로 이동하고 **Add(추가)** 버튼을 클릭하여 사용자를 추가합니다. 여기서 WLC의 AP 가입 프로필에 구성한 자격 증명을 입력해야 합니다. 사용자는 여기에서 기본 그룹에 포함되지만 요구 사항에 따라 이 그룹을 조정할 수 있습니다.

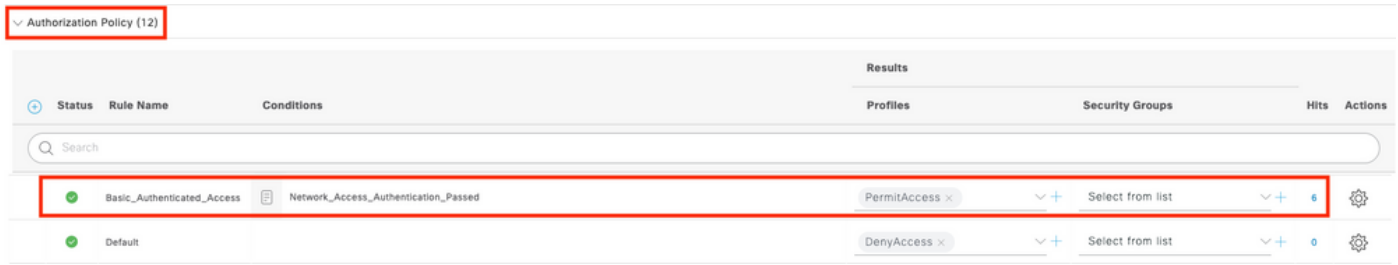


3단계. ISE에서 **인증 정책** 및 **권한 부여** 정책을 **구성합니다**. Policy(**정책**) > **Policy Sets(정책** 집합)로 이동하여 구성하려는 정책 집합과 오른쪽에 있는 파란색 화살표를 선택합니다. 이 경우 기본 정책 집합이 사용되지만 요구 사항에 따라 사용자 지정할 수 있습니다.

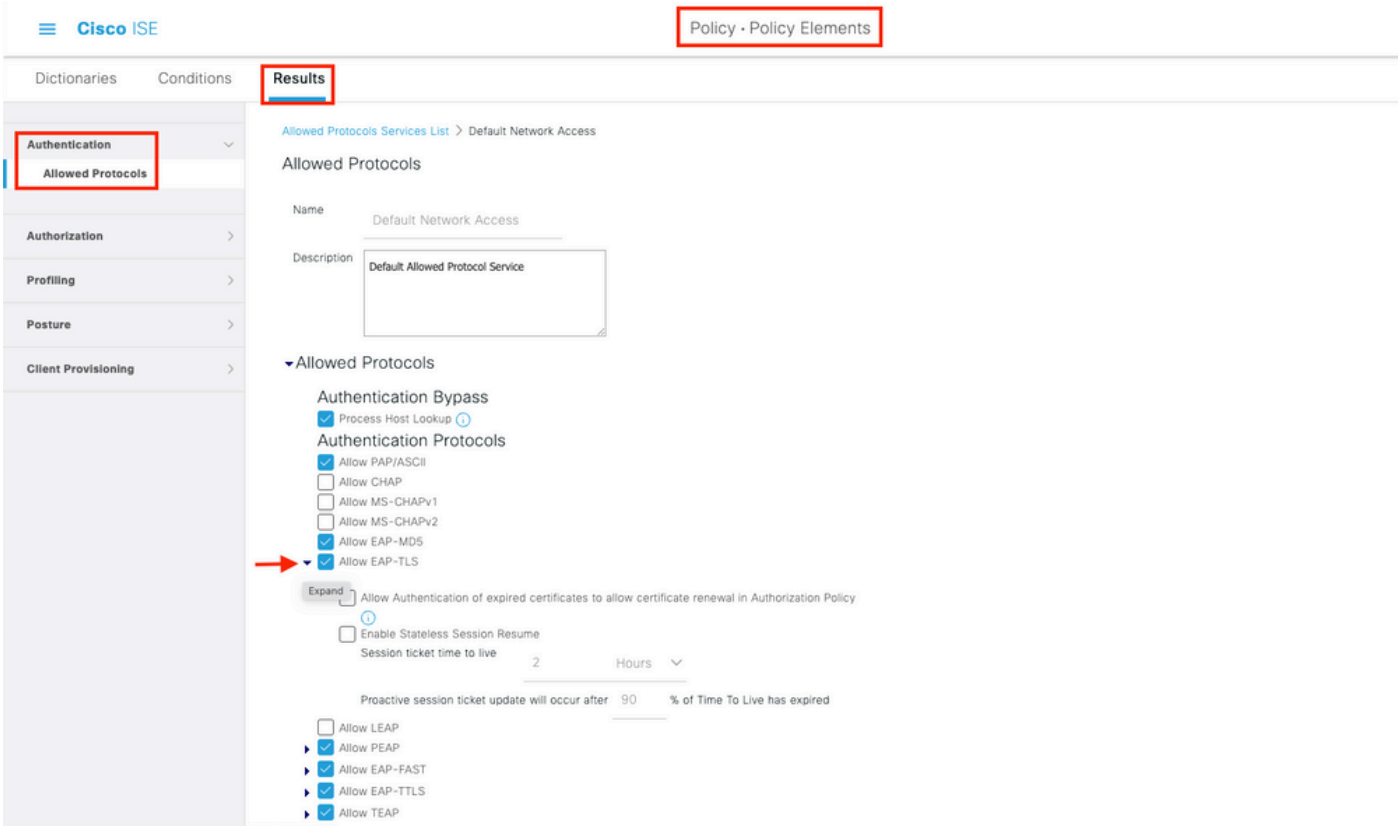


그런 다음 **인증 정책 및 권한 부여 정책을 구성합니다**. 여기에 표시된 정책은 ISE 서버에서 생성된 기본 정책이지만 요구 사항에 따라 수정하고 사용자 지정할 수 있습니다.
이 예에서 컨피그레이션은 "유선 802.1X가 사용되고 사용자가 ISE 서버에서 알려진 경우 인증에 성공한 사용자에 대한 액세스를 허용합니다."로 변환될 수 있습니다. 그러면 AP가 ISE 서버에 대해 인증됩니다.





4단계. 허용되는 프로토콜에서 Default Network Access(기본 네트워크 액세스)가 허용되는지 확인합니다. Policy(정책) > Policy Elements(정책 요소) > Authentication(인증) > Results(결과) > Allowed Protocols(허용되는 프로토콜) > Default Network Access(기본 네트워크 액세스) > Enable Allow EAP-TLS(EAP-TLS 허용) > Save(저장)**로 이동합니다.**



다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

인증 유형 확인

show 명령은 AP 프로필의 인증 정보를 표시합니다.

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

예:

```
9800WLC#show ap profile name default-ap-profile detailed
```

```
 AP Profile Name        : Dot1x
 …
 Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
 LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

스위치 포트에서 802.1x 확인

show 명령은 스위치 포트에서 802.1x의 인증 상태를 표시합니다.

CLI:

```
Switch# show dot1x all
```

출력 예:

```
Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for GigabitEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

포트가 인증되었는지 확인

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

출력 예:

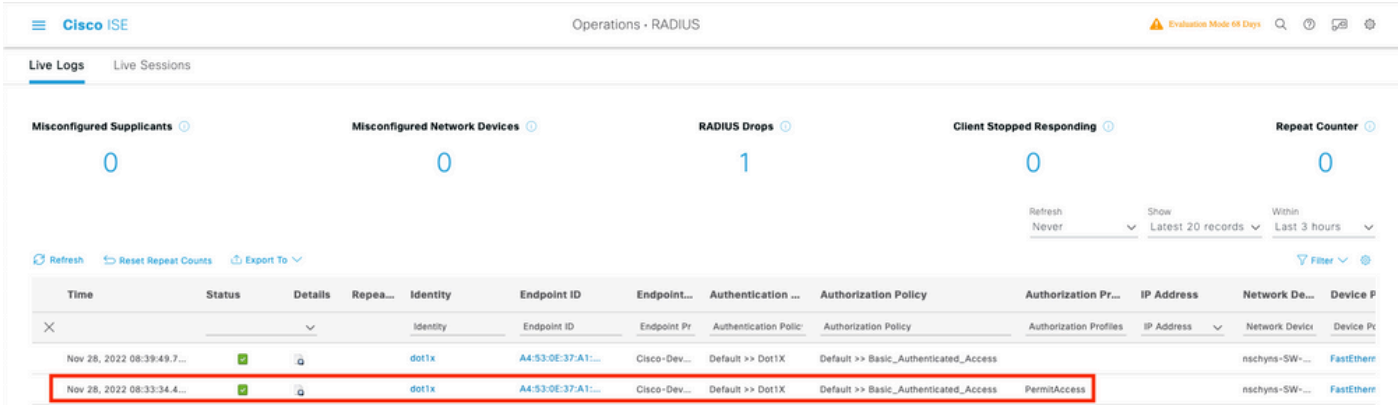
```
Dot1x Info for GigabitEthernet0/8
----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
EAP Method                = FAST
Supplicant                = f4db.e67e.dd16
Session ID                = 0A30279E00000BB7411A6BC4
   Auth SM State         = AUTHENTICATED
   Auth BEND SM State    = IDLE
ED
Auth BEND SM State = IDLE
```

CLI에서:

```
Switch#show authentication sessions
```
출력 예:

```
Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi0/8        f4db.e67e.dd16 dot1x   DATA    Auth      0A30279E00000BB7411A6BC4
```
ISE에서 Operations(**작업) > Radius Livelogs(Radius Livelogs)**를 선택하고 인증이 성공적이며 올바른 Authorization(권한 부여) 프로파일이 푸시되는지 확인합니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

1. ISE 서버가 **스위치**에서 연결 가능한지 확인하려면 ping 명령을 입력합니다.
2. 스위치가 ISE 서버에서 AAA 클라이언트로 구성되어 있는지 확인합니다.
3. 공유 암호가 스위치와 ISE 서버 간에 동일한지 확인합니다.
4. ISE 서버에서 EAP-FAST가 활성화되었는지 확인합니다.
5. 802.1x 자격 증명이 LAP에 대해 구성되어 있고 ISE 서버에서 동일한지 확인합니다.
   참고: 사용자 이름과 비밀번호는 대/소문자를 구분합니다.
6. 인증에 실패하면 스위치에 debug dot1x 및 debug **authentication 명령을 입력합니다**.

Cisco IOS 기반 액세스 포인트(802.11ac wave 1)는 TLS 버전 1.1 및 1.2를 지원하지 않습니다. 이 경우 ISE 또는 RADIUS 서버가 802.1X 내의 TLS 1.2만 허용하도록 구성된 경우 문제가 발생할 수 있습니다.

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.