경량 액세스 포인트를 802.1x 신청자로 구성

소개

이 문서에서는 ISE(Identity Services Engine) 서버에 대해 인증하기 위해 LAP(Lightweight Access Point)를 802.1x 신청자로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC(Wireless Lan Controller) 및 LAP
- Cisco 스위치에서 802.1x
- ISE
- EAP(Extensible Authentication Protocol) - FAST(Secure Tunneling)를 통한 유연한 인증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- ISE 2.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

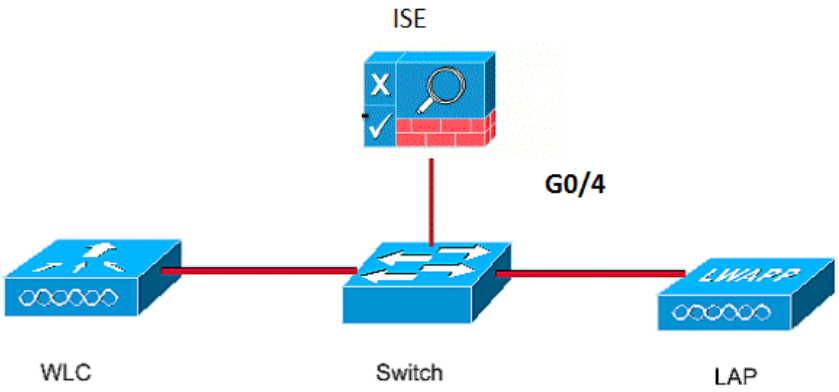
이 설정에서 액세스 포인트(AP)는 802.1x 신청자 역할을 하며 익명 PAC(Protected Access Credentials) 프로비저닝을 사용하여 EAP-FAST를 사용하는 ISE에 대해 스위치에 의해 인증됩니다.포트가 802.1x 인증을 위해 구성되면, 스위치에 연결된 디바이스가 성공적으로 인증될 때까지 스위치는 802.1x 트래픽 이외의 트래픽이 포트를 통과하도록 허용하지 않습니다.AP는 WLC에 가입하기 전이나 WLC에 가입한 후 인증할 수 있습니다. 이 경우 LAP가 WLC에 조인된 후 스위치에 802.1x를 구성합니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

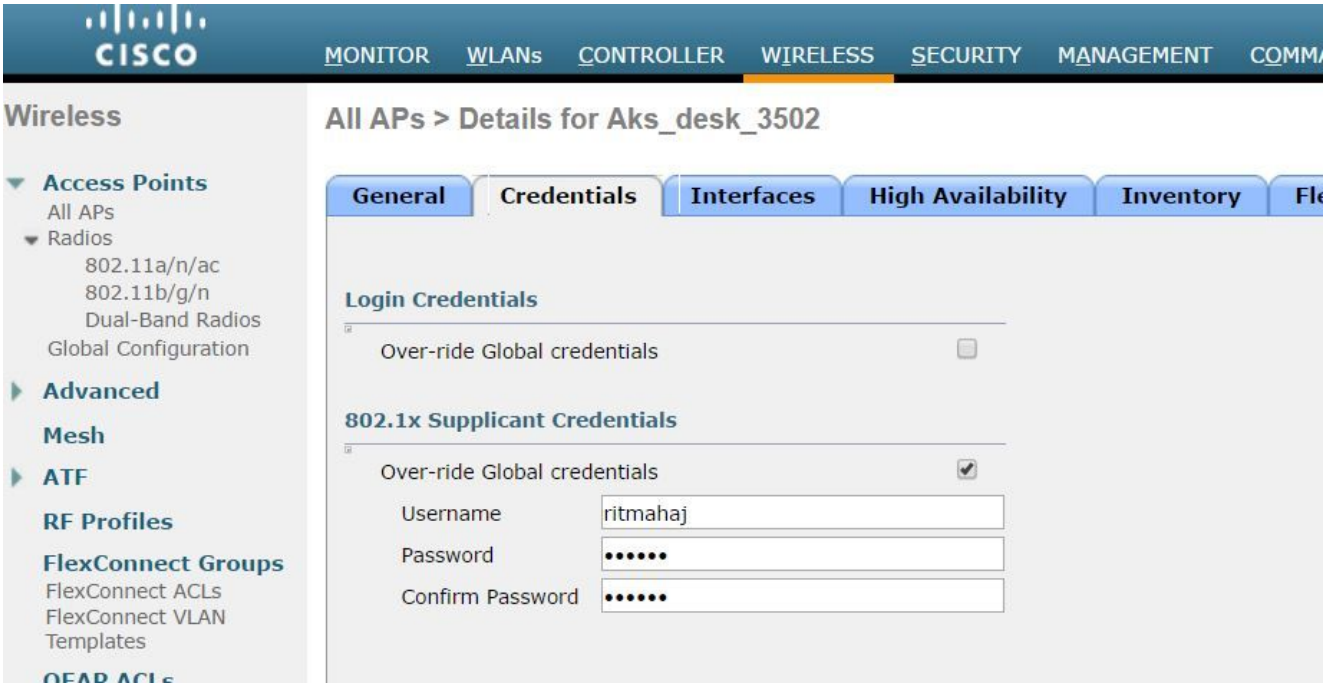
이 문서에서는 다음 IP 주소를 사용합니다.

- 스위치의 IP 주소는 10.48.39.141입니다.
- ISE 서버의 IP 주소는 10.48.39.161입니다.
- WLC의 IP 주소는 10.48.39.142입니다.

LAP 구성

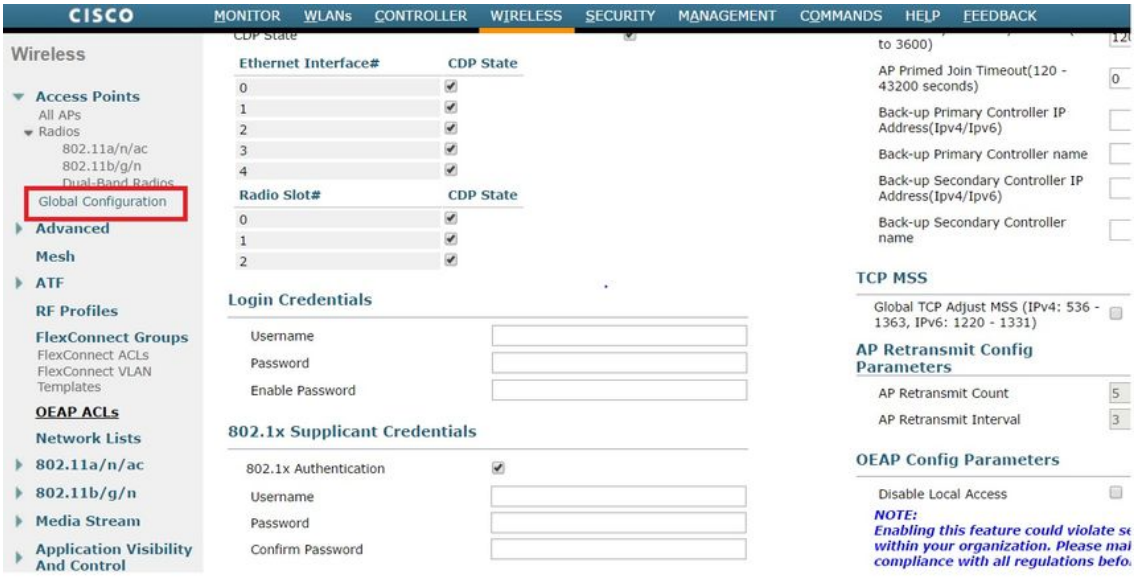
이 섹션에서는 LAP를 802.1x 신청자로 구성하는 정보를 제공합니다.

1. AP가 WLC에 이미 가입되어 있는 경우 Wireless(무선) 탭으로 이동하여 AP를 클릭하고 Credentials(자격 증명) 필드로 이동한 다음 802.1x Supplicant Credentials(802.1x 신청자 자격 증명) 제목 아래에서 이 AP에 대한 802.1x 사용자 이름 및 비밀번호를 설정하려면 Over-ride **Global credentials(Over-Global credentials)**) 확인란을 선택합니다.



Global Configuration(전역 컨피그레이션) 메뉴를 사용하여 WLC에 조인되는 모든 AP에 대해 공통 사용자 이름과 비밀번호를 설정할 수도 있습니다

.



2. AP가 아직 WLC에 가입하지 않은 경우 자격 증명을 설정하고 다음 CLI 명령을 사용하려면 LAP에 로그인해야 합니다.

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

스위치 구성

1. 스위치에서 dot1x를 전역적으로 활성화하고 스위치에 ISE 서버를 추가합니다.

```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
  key 7 123A0C0411045D5679
```

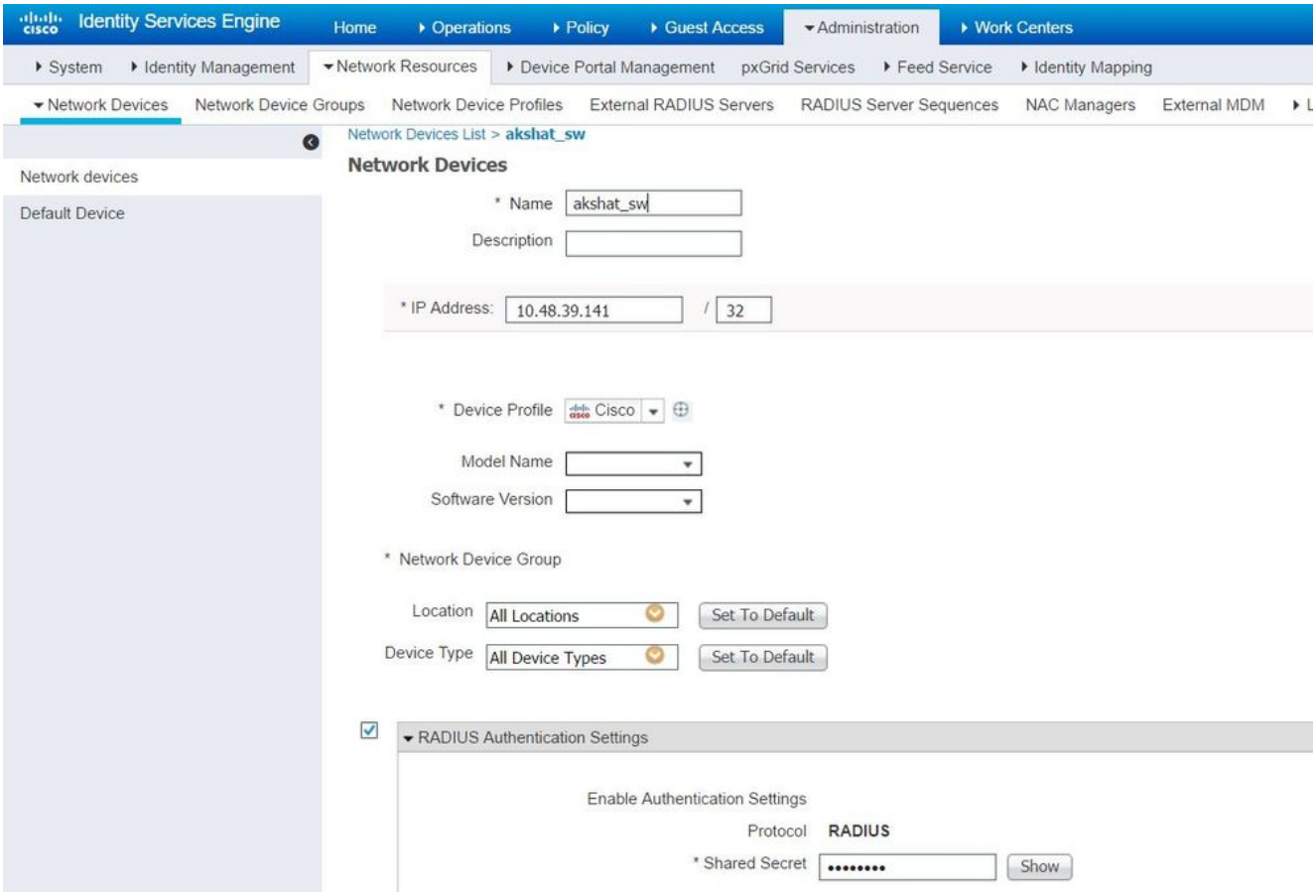
2. 이제 AP 스위치 포트를 구성합니다.

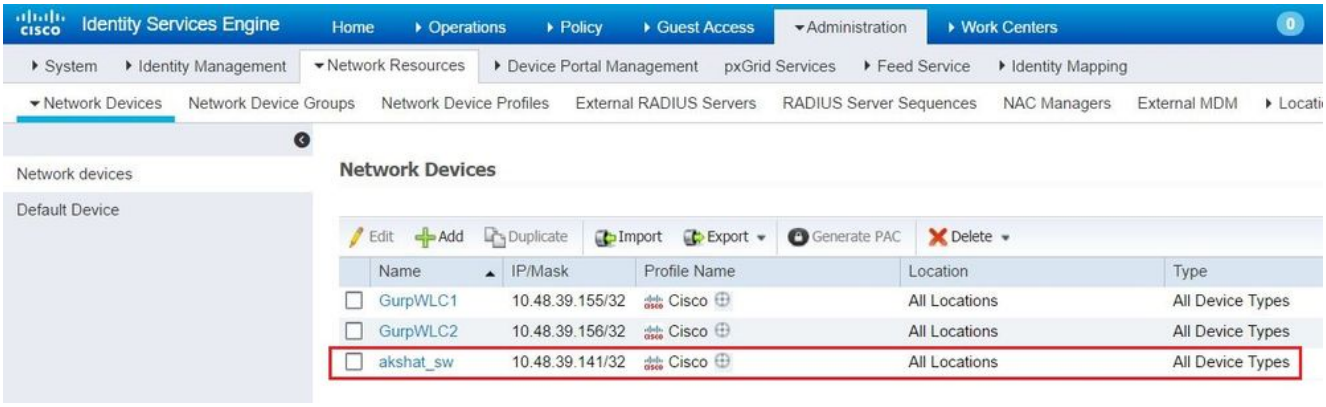
```
interface GigabitEthernet0/4


switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

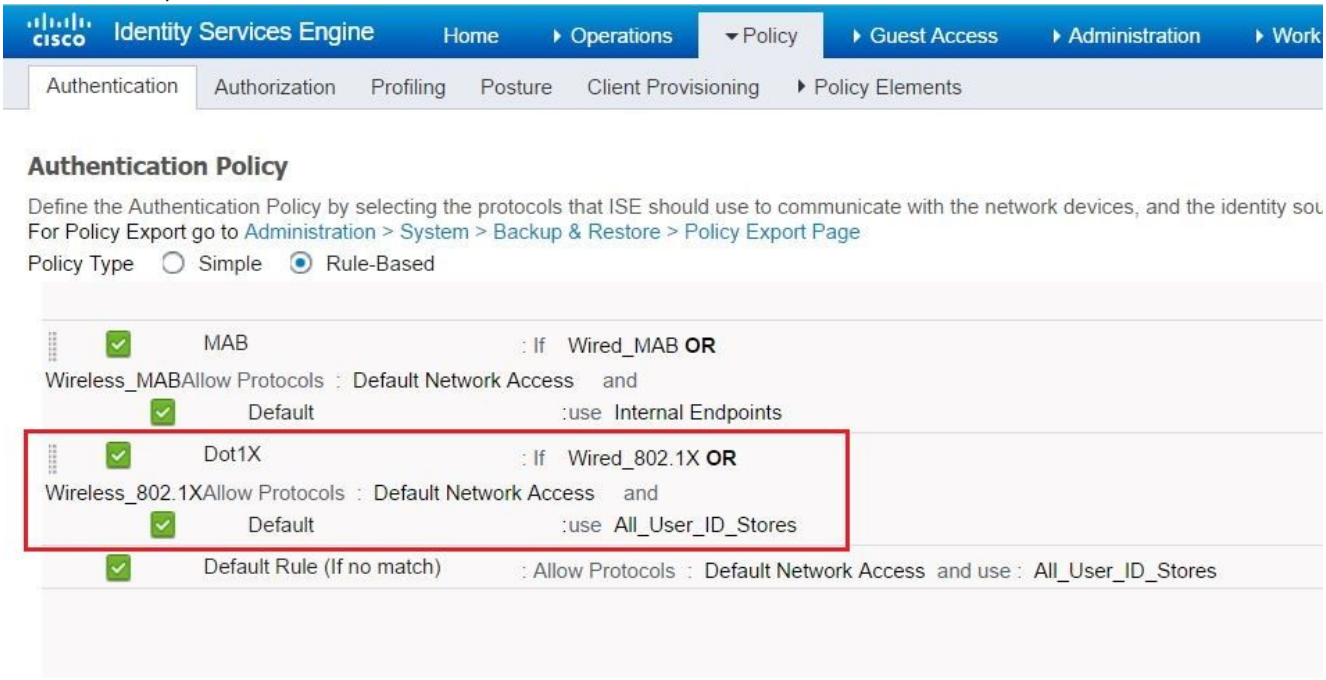
ISE 서버 구성

1. ISE 서버에서 AAA(Authentication, Authorization, and Accounting) 클라이언트로 스위치를 추가합니다.



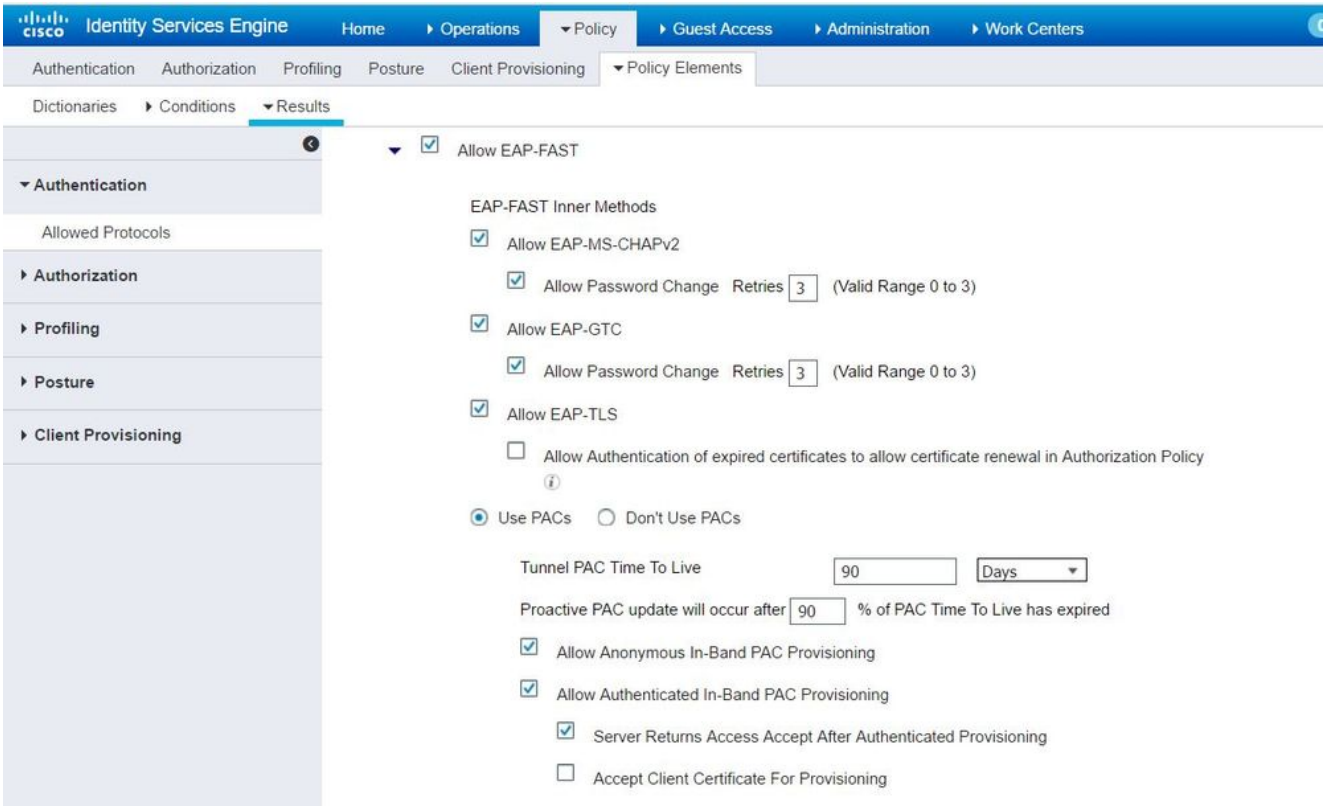


2. ISE에서 인증 정책 및 권한 부여 정책을 구성합니다.이 경우 유선 dot.1x인 기본 인증 규칙이 사용되지만, 사용자는 요구 사항에 따라 이를 사용자 지정할 수 있습니다.



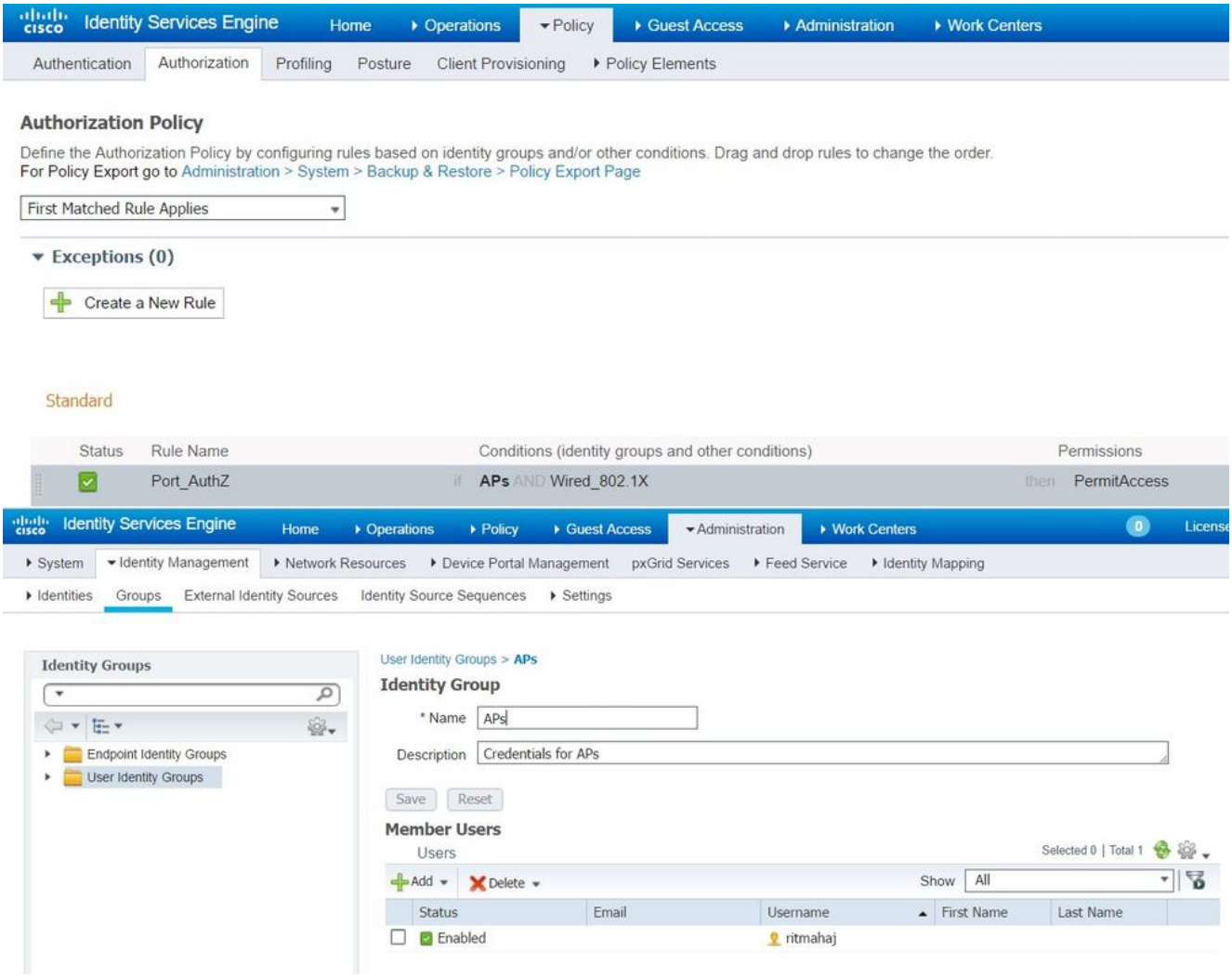
기본 네트워크 액세스를 허용하는 프로토콜에서 EAP-FAST가 허용되는지 확인합니다

.



3. 권한 부여 정책(Port_AuthZ)에 대해 이 경우 AP 자격 증명이 사용자 그룹(AP)에 추가되었습니다. 사용된 조건은 "사용자가 그룹 AP에 속하고 유선 dot1x를 수행한 다음 기본 권한 부여 프로파일 허용 액세스를 푸시합니다."입니다. 또한 요구 사항에 따라 사용자 지정할 수 있습니다

.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

스위치 포트에서 802.1x가 활성화되면 802.1x 트래픽을 제외한 모든 트래픽이 포트를 통해 차단됩니다.WLC에 이미 등록된 LAP는 연결 해제됩니다.성공한 802.1x 인증만 통과하도록 허용된 다른 트래픽입니다.스위치에서 802.1x를 활성화한 후 WLC에 LAP를 성공적으로 등록하면 LAP 인증이 성공했음을 나타냅니다.LAP가 인증되었는지 확인하기 위해 이러한 방법을 사용할 수도 있습니다.

1. 스위치에서 **show** 명령 중 하나를 입력하여 포트가 인증되었는지 확인합니다.

```
akshat_sw#show dot1x interface g0/4

Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30


akshat_sw#show dot1x interface g0/4 details

Dot1x Info for GigabitEthernet0/4
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30


Dot1x Authenticator Client List
-------------------------------
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE


akshat_sw#show authentication sessions

Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. ISE에서 **Operations(작업) > Radius Livelogs(RADIUS 라이브 로그)**를 선택하고 인증이 성공하고 올바른 권한 부여 프로파일이 푸시되는지 확인합니다.

문제 해결

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

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