TACACS+를 사용하는 Cisco WLC의 디바이스 관리

목차

소개

이 문서에서는 ISE(Identity Service Engine)를 사용하여 Cisco WLC(Wireless LAN Controller)의 디바이스 관리를 위해 TACACS+를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Service Engine)에 대한 기본 지식
- Cisco WLC(Wireless LAN Controller)에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

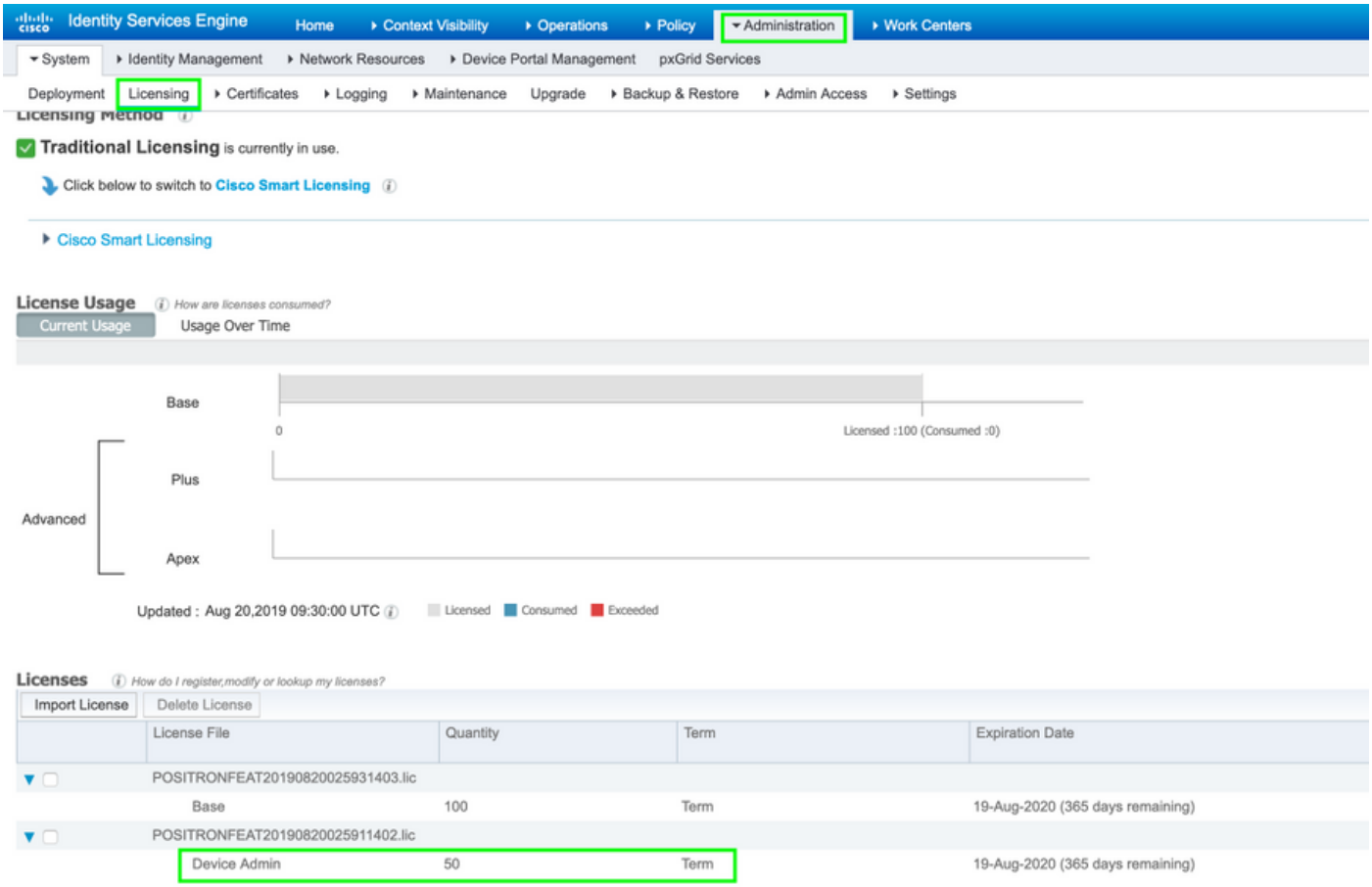
- Cisco Identity Service Engine 2.4
- Cisco Wireless LAN Controller 8.5.135

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.

구성

1단계. 디바이스 관리 라이센스를 확인합니다.

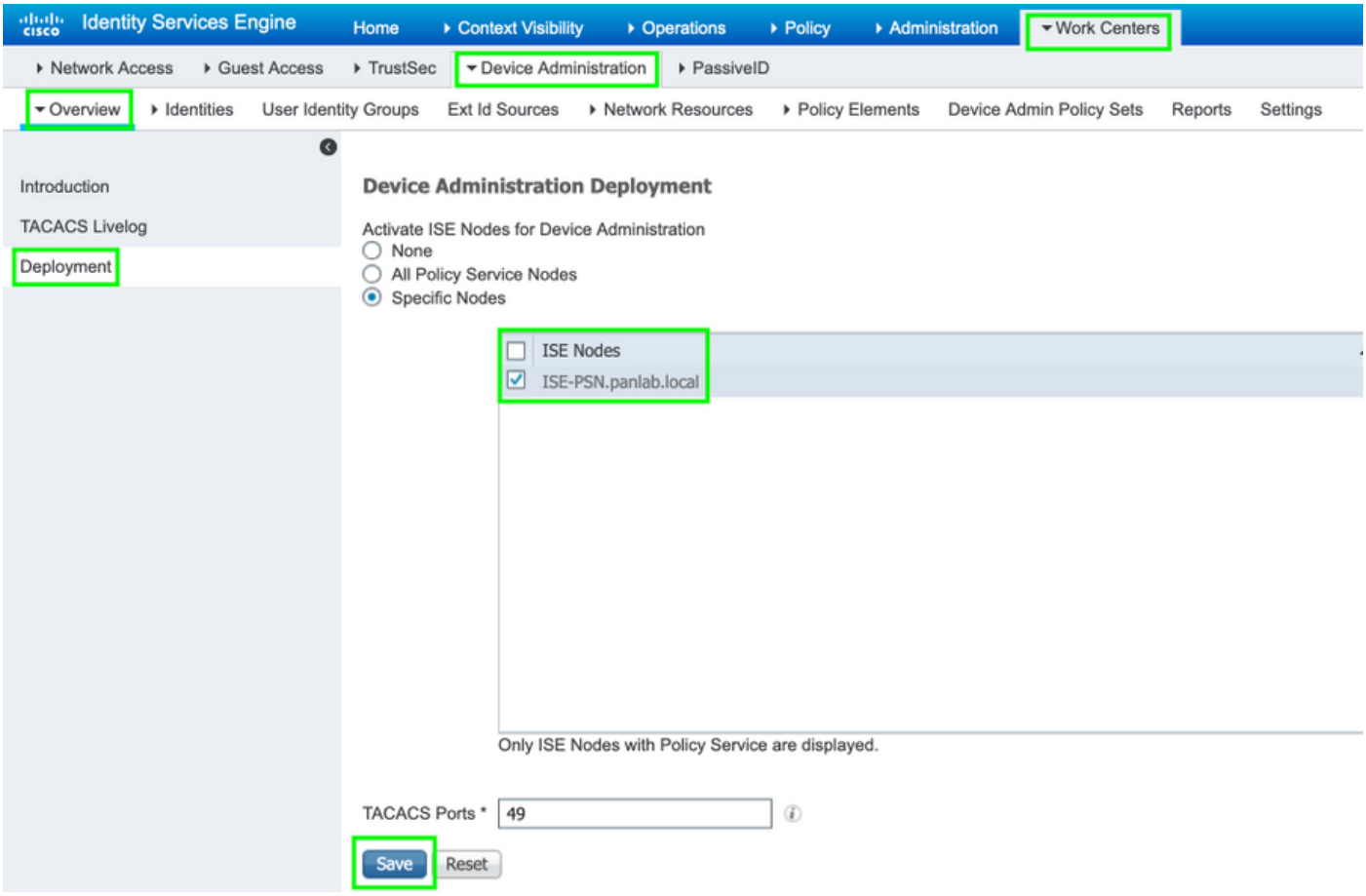
Administration(**관리) > System(시스템) > Licensing(라이센싱**) 탭**으로 이동하고** 이미지에 표시된 대로 Device Admin 라이센스가 설치되었는지 확인합니다.



참고:ISE에서 TACACS+ 기능을 사용하려면 디바이스 관리자 라이센스가 필요합니다.

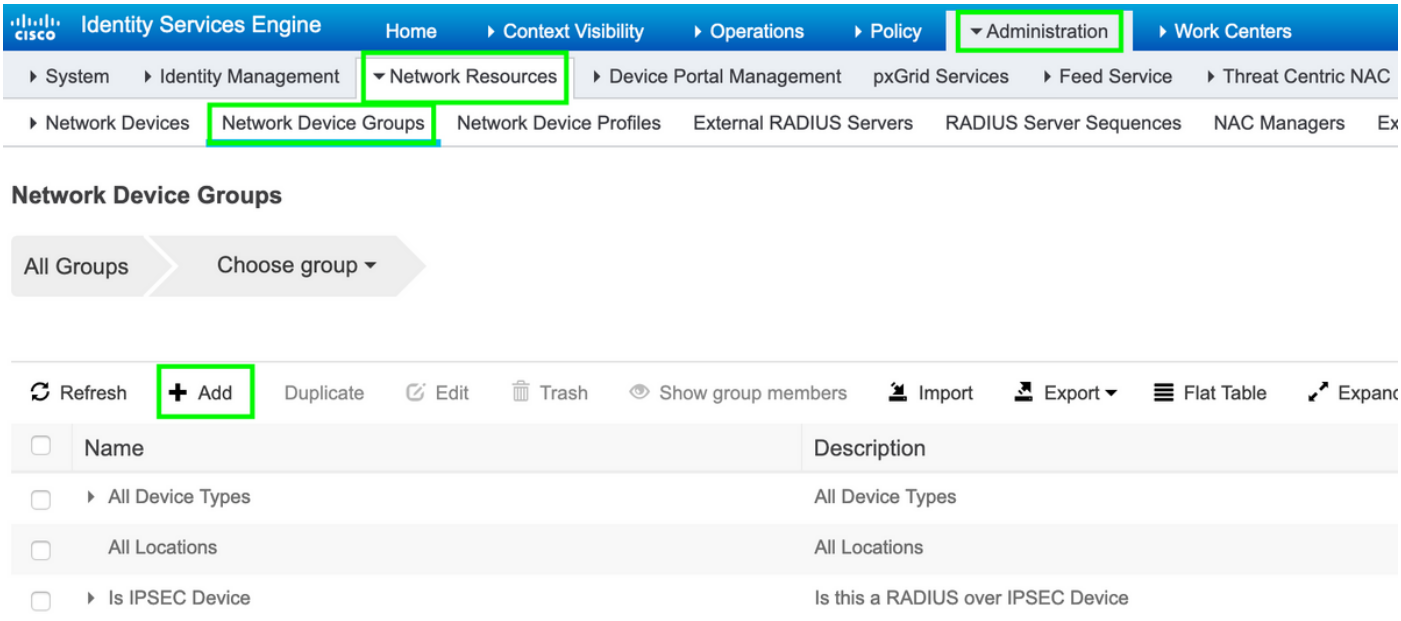
2단계. ISE PSN 노드에서 디바이스 관리를 활성화합니다.

Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Overview(개요)로** 이동하고 **Deployment(구축)** 탭, Select the Specific PSN Node(특정 PSN 노드 선택) 라디오 버튼을 클릭합니다.**ISE** 노드에서 **확인란**을 선택하고 이미지에 표시된 대로 **저장**을 클릭하여 디바이스 관리를 활성화합니다.



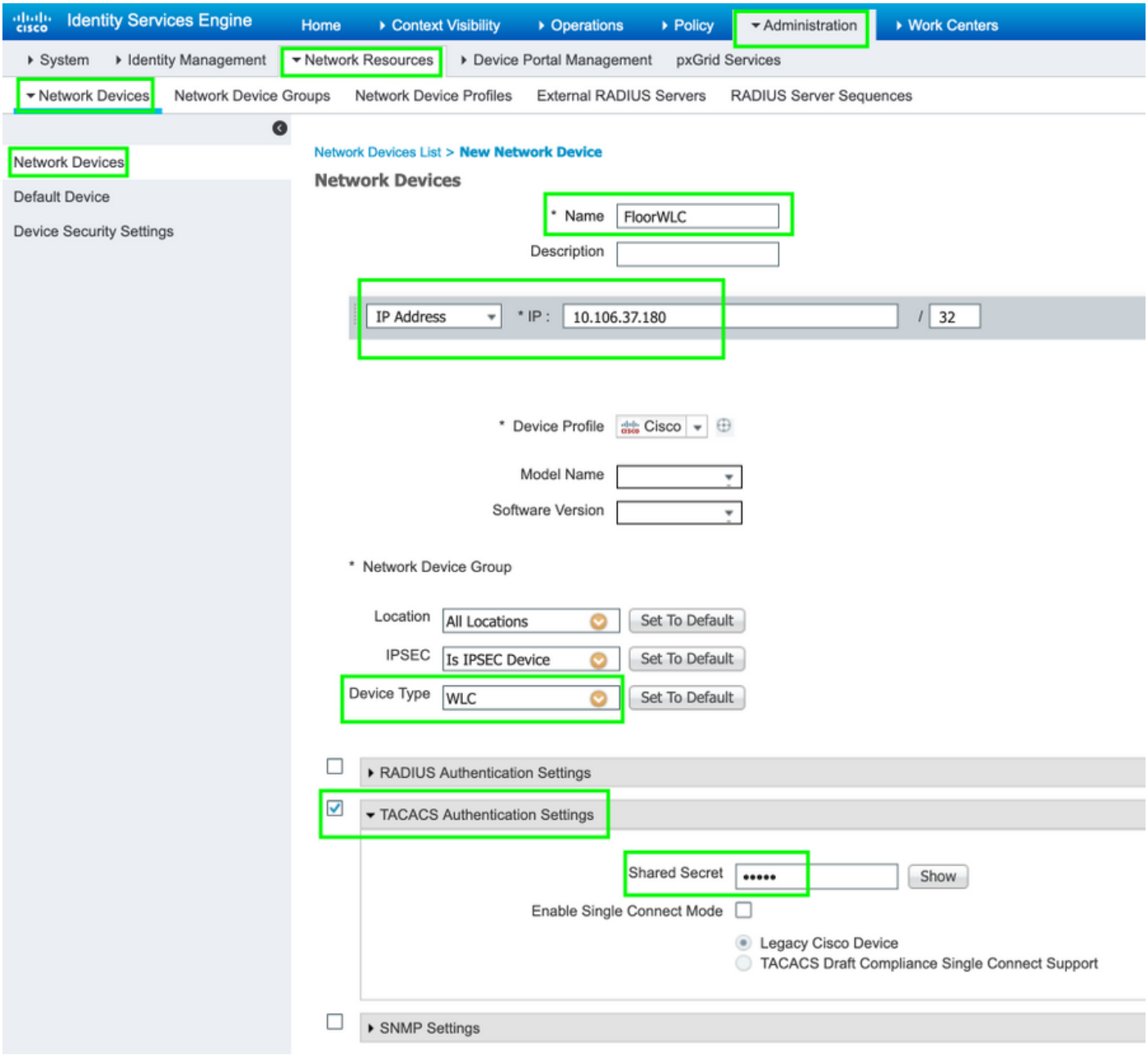
3단계. 네트워크 장치 그룹을 만듭니다.

ISE에서 WLC를 네트워크 디바이스로 추가하려면 다음 이미지에 표시된 대로 **Administration(관리) > Network Resources(네트워크 리소스) > Network Device Groups(네트워크 디바이스 그룹) > All Device Types(모든 디바이스 유형)**로 이동하여 WLC에 **대한 새 그룹**을 생성합니다.



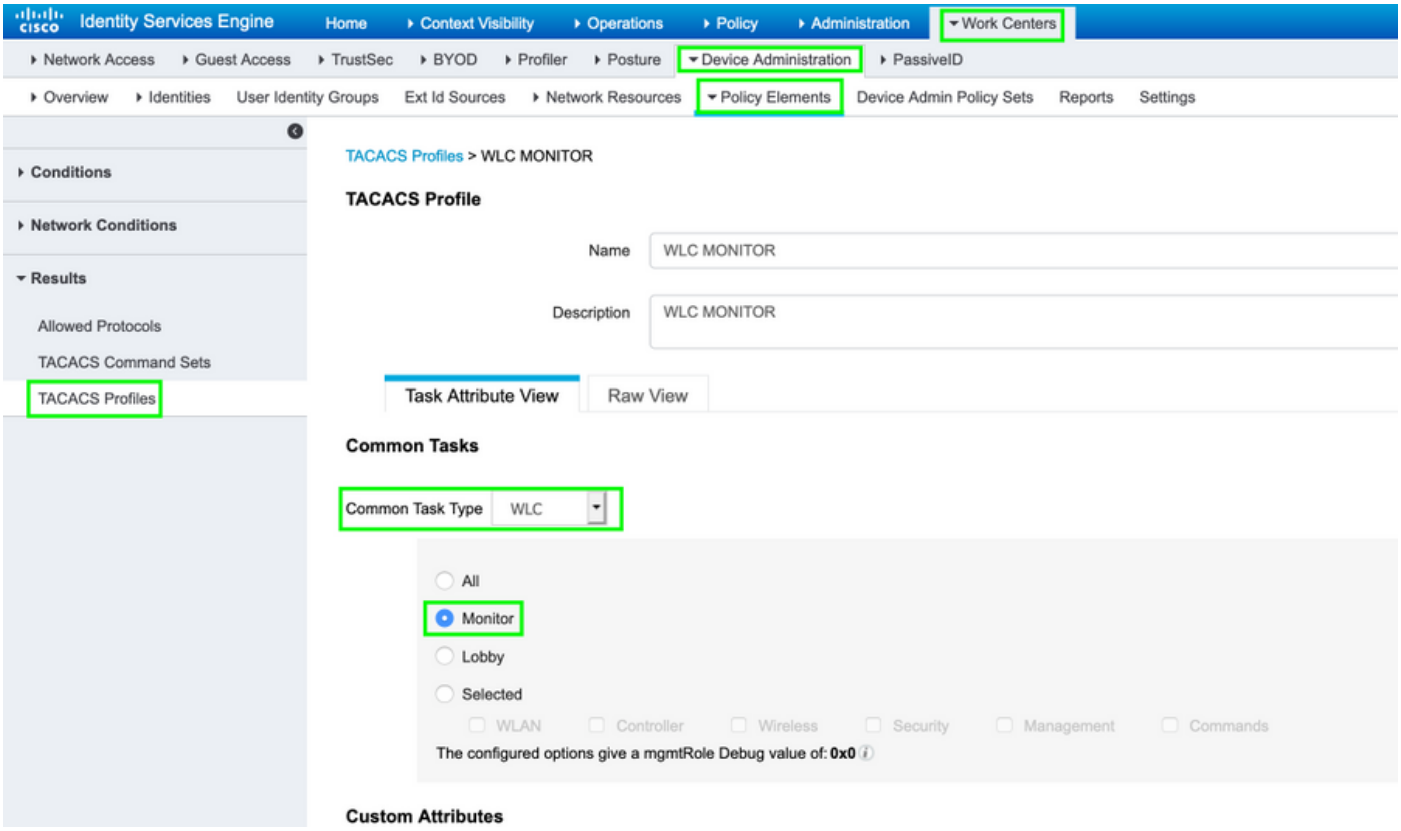
4단계. WLC를 네트워크 디바이스로 추가합니다.

Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다**.Add(**추가**)를 클릭하고 **Name**, **IP Address(이름**, **IP 주소)를** 제공하고 Device type as **WLC(디바이스 유형)를** 선택하고 **TACACS+ Authentication Settings(TACACS+ 인증 설정) 확인란을 선택한 후 이미지에 표시된 대로 Shared Secret(공유 암호) 키를 제공합니다.**

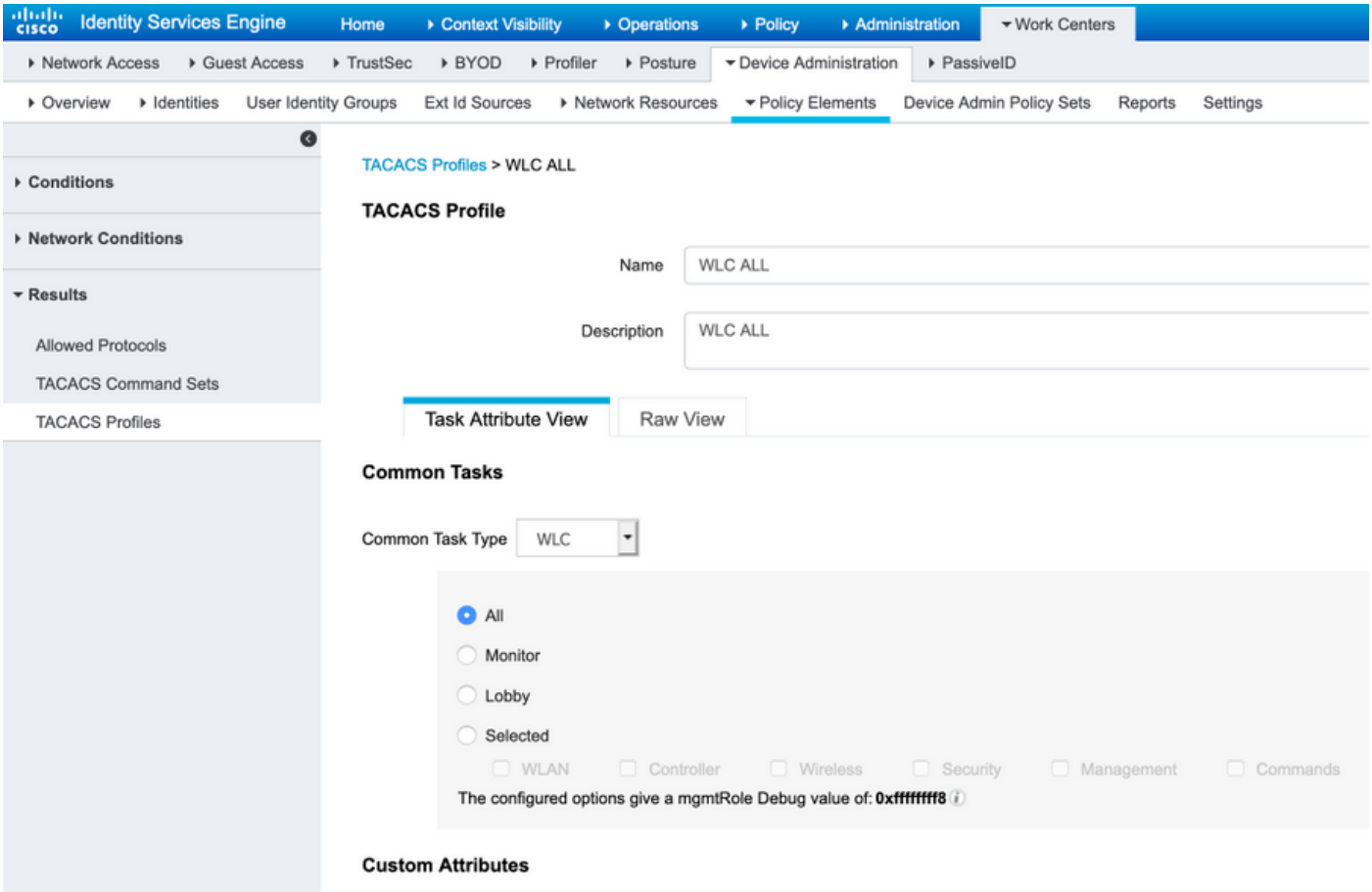


5단계. WLC에 대한 TACACS 프로파일을 생성합니다.

Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로파일)로 이동합니다.**Add(**추가)를 클릭하고 Name(이름)**을 **입력합니다.작업 속성 보기** 탭에서 **공통 작업 유형**에 대해 **WLC**를 선택합니다. 기본 프로파일이 있으며 이 프로파일에서 이미지에 표시된 대로 사용자에 대한 제한적 액세스를 허용하도록 모니터를 선택합니다.

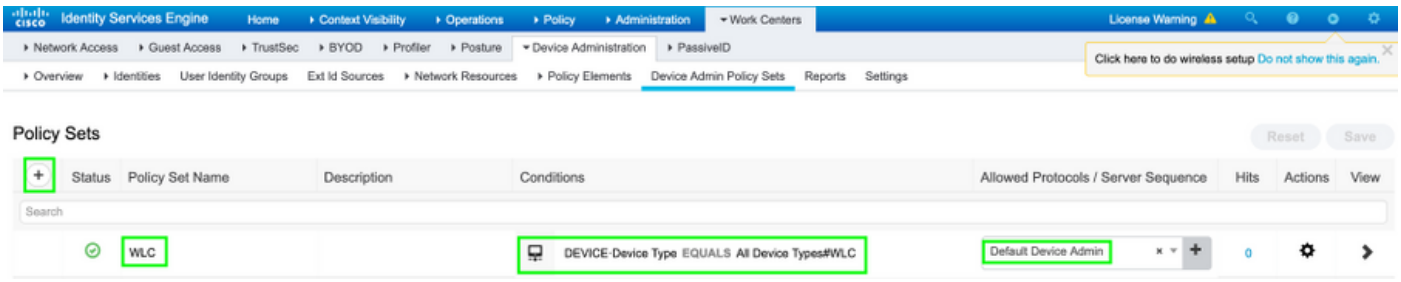


이미지에 표시된 대로 사용자에 대한 전체 액세스를 허용하는 또 다른 기본 프로파일 **All**이 있습니다.



6단계. 정책 세트를 생성합니다.

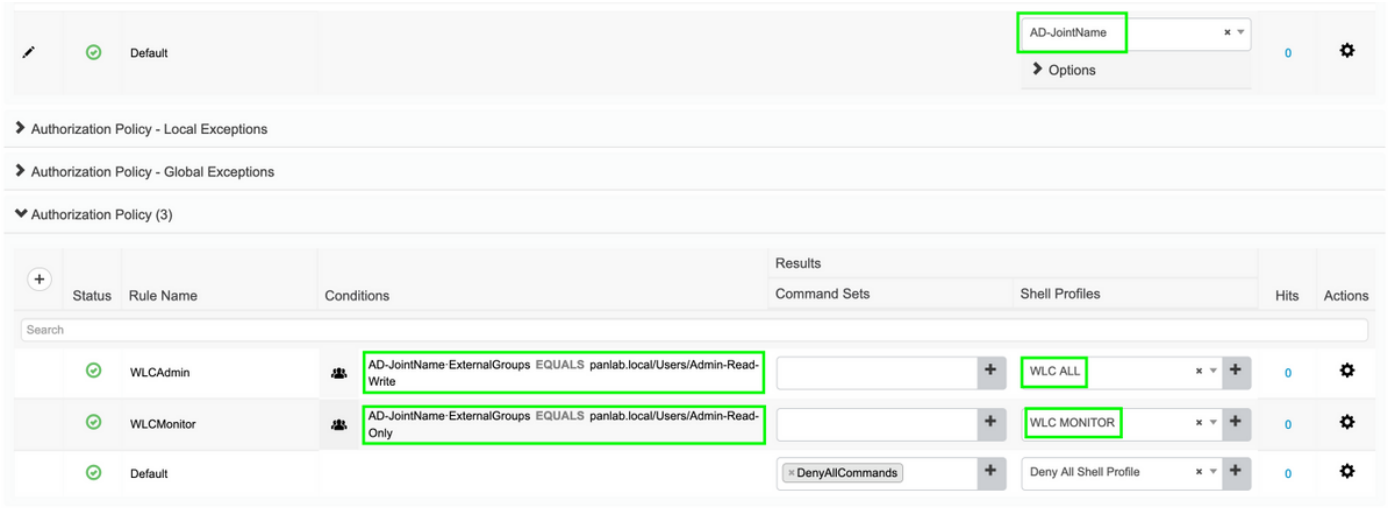
Work centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 세트)로 이동합니다. **(+)를** 클릭하고 정책 세트에 이름을 지정합니다.정책 조건에서 Device **Type(디바이스 유형)**을 WLC로 선택합니다. 허용되는 프로토콜은 이미지에 표시된 대로 **Default Device Admin(기본 디바이스 관리자)**이 될 수 있습니다.



7단계. 인증 및 권한 부여 정책을 생성합니다.

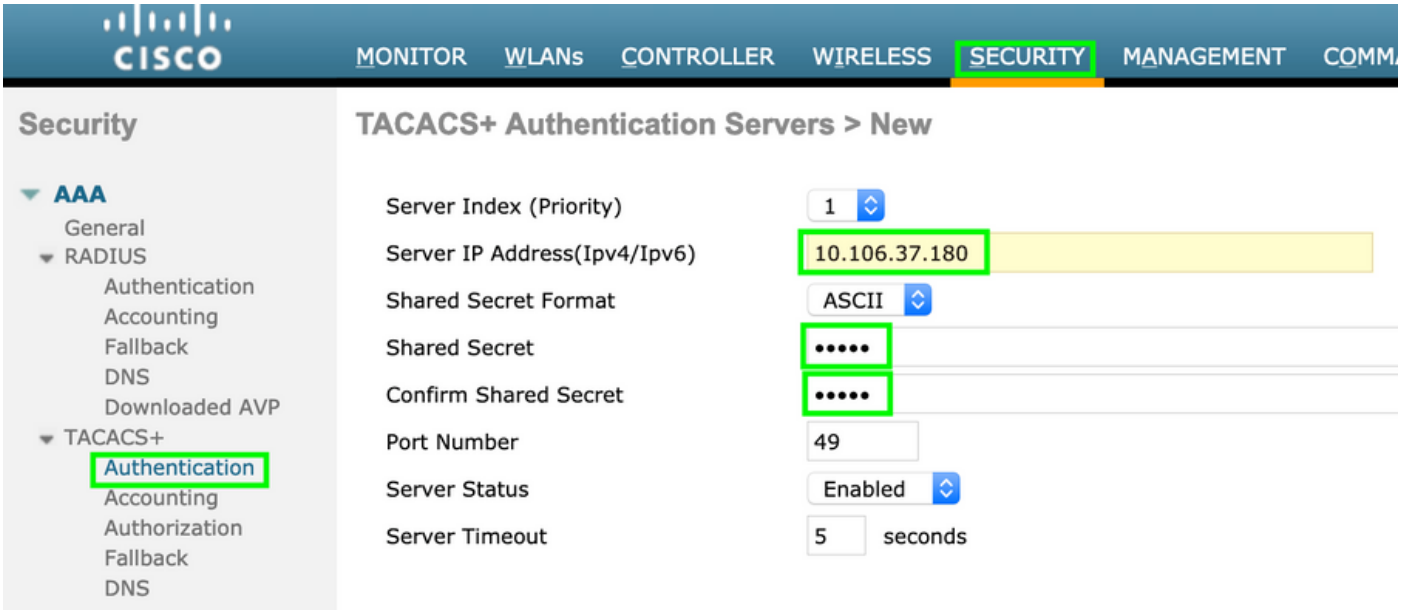
이 문서에서 두 개의 샘플 그룹 **Admin-Read-Write** 및 **Admin-Read-Only가** 각각 Active Directory에 구성되고 각 그룹 **admin1**에 속한 한 사용자**가 admin2**로 **구성됩니다**.Active Directory는 AD-**JointName**이라는 연결점을 통해 ISE와 **통합됩니다.**

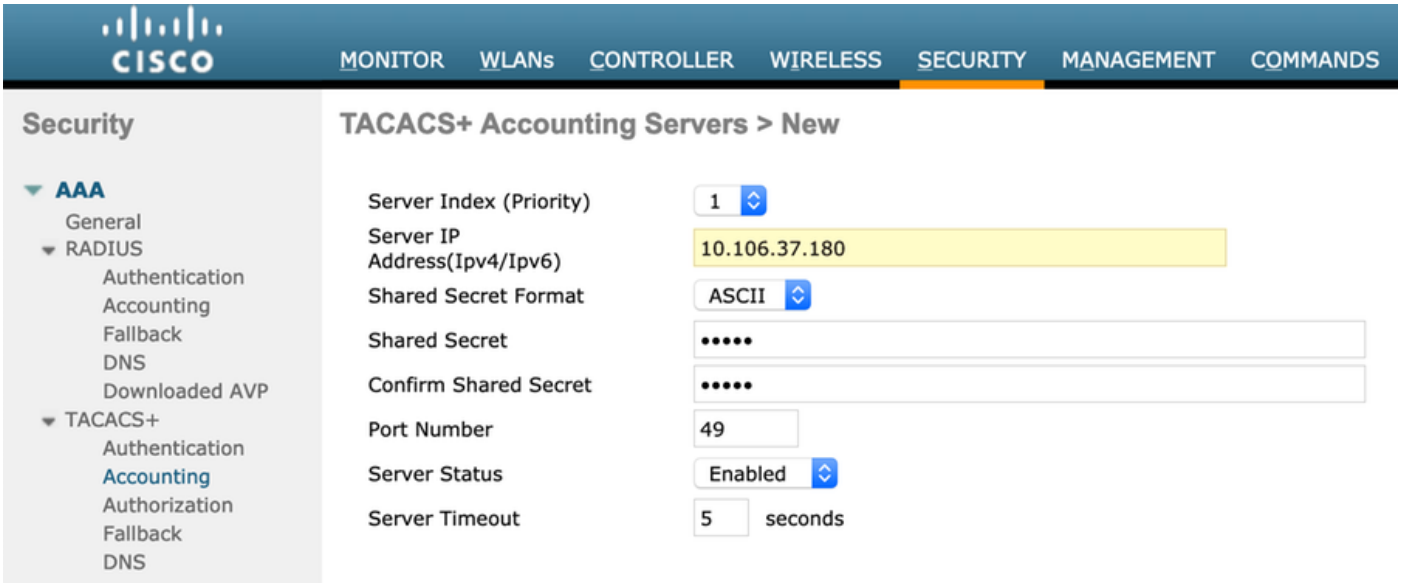
이미지에 표시된 대로 두 개의 권한 부여 정책을 생성합니다.



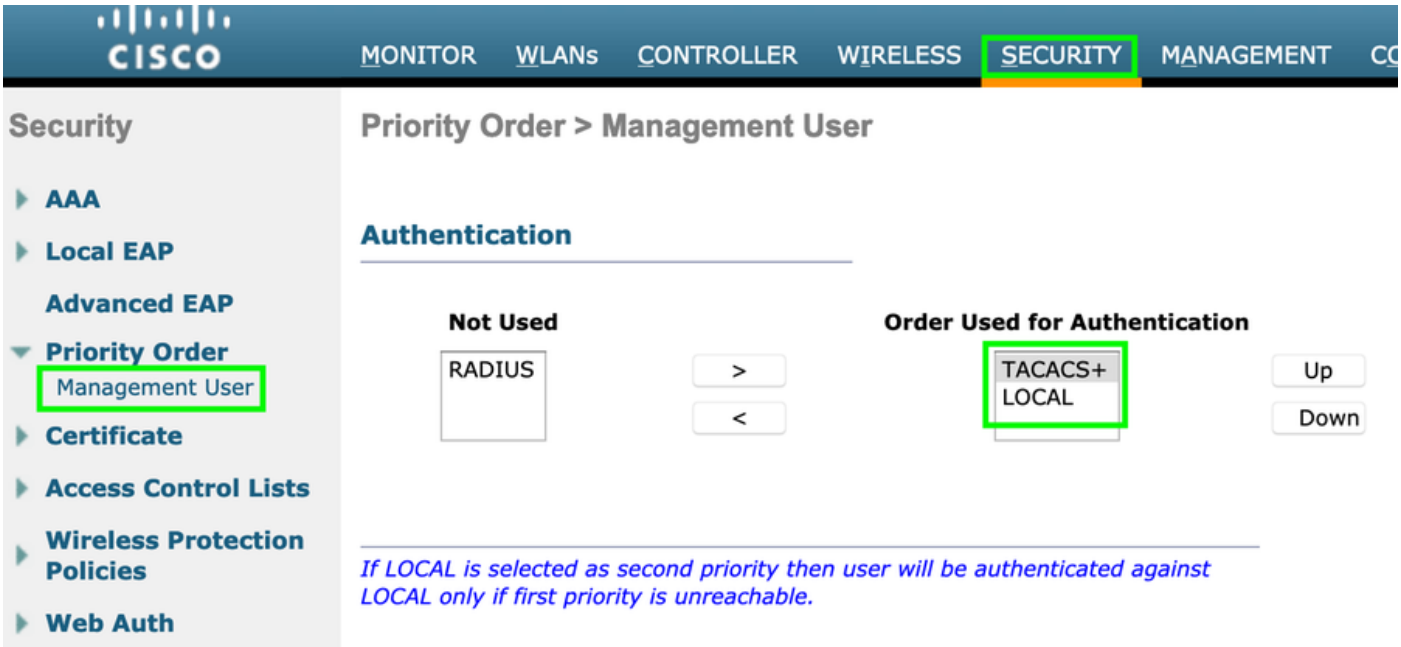
8단계. 디바이스 관리를 위한 WLC를 구성합니다.

Security(**보안) > AAA > TACACS로 이동하고 New(새로 만들기)를** 클릭하고 이미지에 표시된 대로 Authentication, Accounting server(인증, 어카운팅 서버)를 추가합니다.





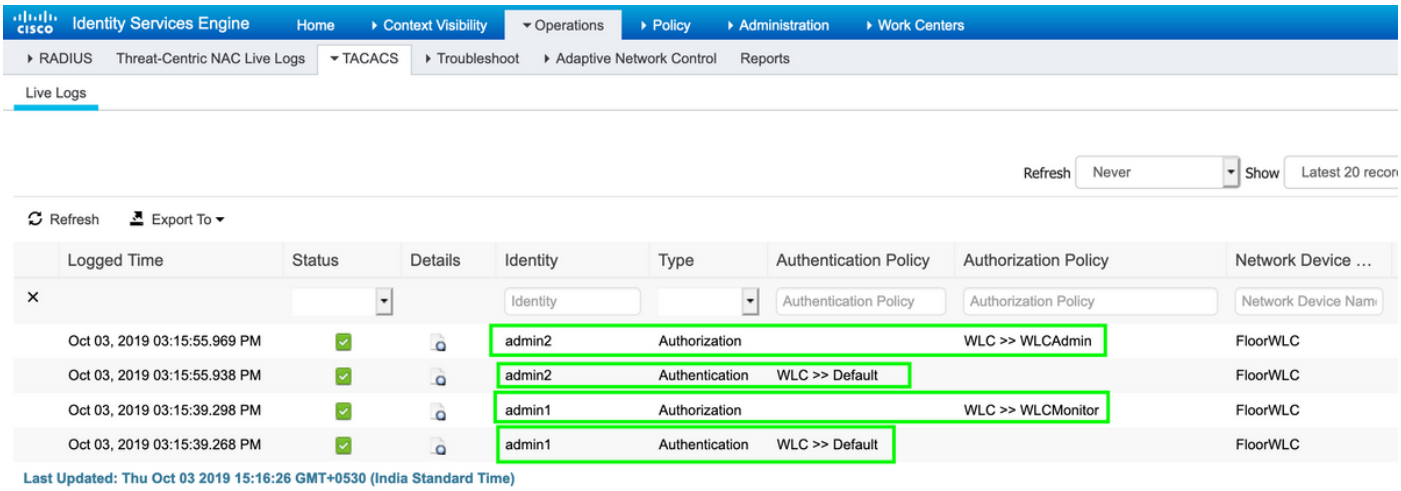
이미지에 표시된 대로 우선 순위 순서를 변경하고 TACACS+를 위쪽에서 아래쪽으로 설정하고 Local을 아래쪽으로 설정합니다.



주의:현재 WLC GUI 세션을 닫지 마십시오.다른 웹 브라우저에서 WLC GUI를 열고 TACACS+ 자격 증명으로 로그인하는지 여부를 확인하는 것이 좋습니다.그렇지 않은 경우 TCP 포트 49에서 ISE 노드에 대한 컨피그레이션 및 연결을 확인합니다.

다음을 확인합니다.

Operations(작업) **> TACACS > Live logs(라이브 로그)로 이동하고 라이브 로그를 모니터링합니다** .이미지에 표시된 대로 WLC GUI를 열고 Active Directory 사용자 자격 증명으로 로그인합니다.



문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.