# ISE와 CSM TACACS 통합

## 목차



## 소개

이 문서에서는 TACACS+ 프로토콜로 관리자 사용자 인증을 위해 Cisco CSM(Security Manager)을 ISE(Identity Services Engine)와 통합하는 절차에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CSM(Cisco Security Manager).
- ISE(Identity Services Engine).
- TACACS 프로토콜.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CSM Server 버전 4.22
- ISE 버전 3.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 배경 정보

기본적으로 Cisco CSM(Security Manager)은 CiscoWorks라는 인증 모드를 사용하여 사용자를 로컬에서 인증하고 권한을 부여하여 TACACS 프로토콜을 통해 Cisco Identity Service Engine을 사용할 수 있는 중앙 집중식 인증 방법을 제공합니다.

# 구성

## 네트워크 다이어그램


## 인증 절차

1단계. 관리자 사용자의 자격 증명을 사용하여 CSM 애플리케이션에 로그인합니다.

2단계. 인증 프로세스가 트리거되고 ISE는 로컬 또는 Active Directory를 통해 자격 증명을 검증합니다.

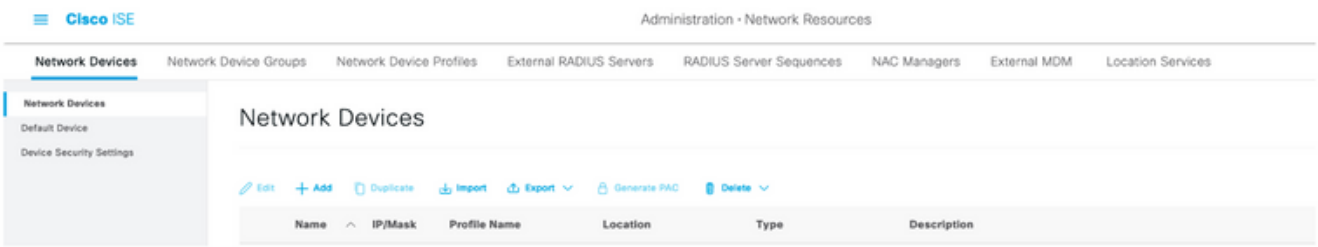
3단계. 인증이 성공적으로 완료되면 ISE는 CSM에 대한 액세스를 권한 부여하기 위해 허용 패킷을 전송합니다.

4단계. CSM은 사용자 이름을 로컬 사용자 역할 할당과 매핑합니다.

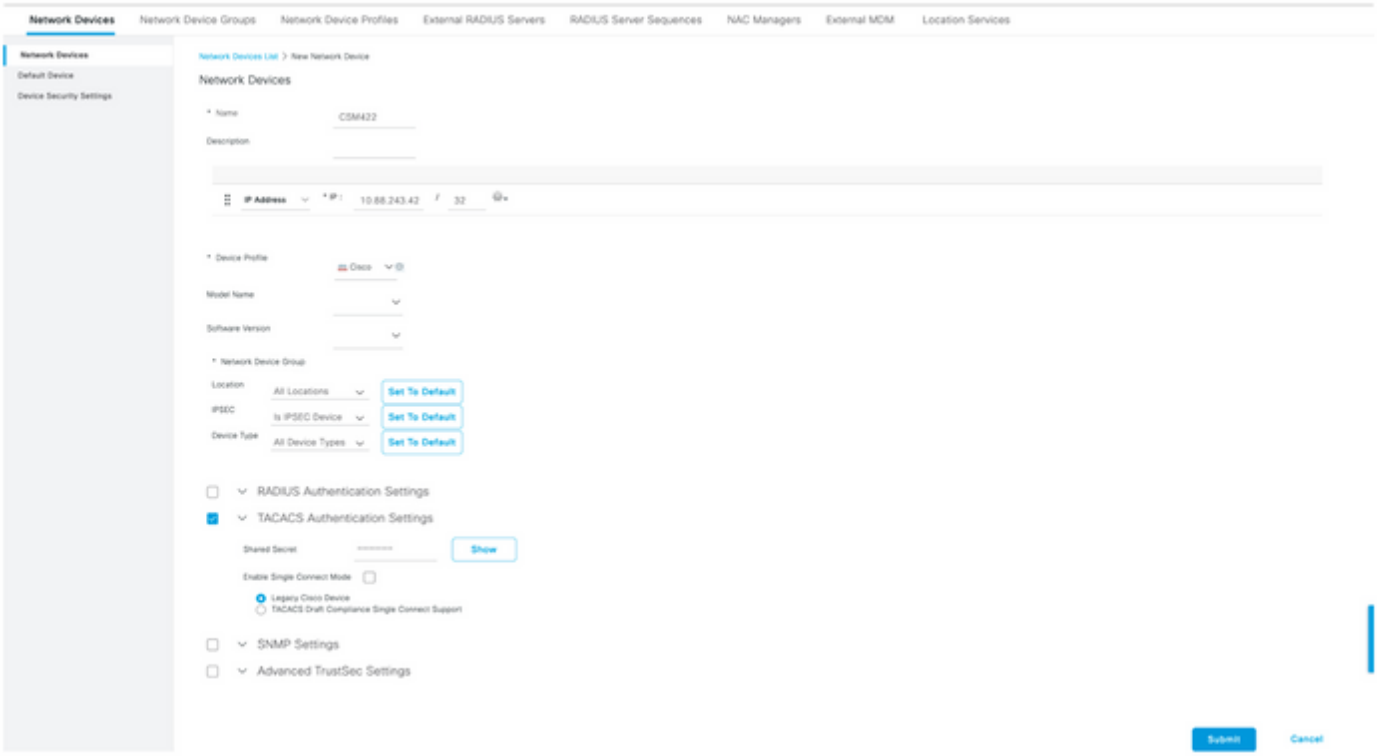
5단계. ISE는 성공적인 인증 라이브 로그를 표시합니다.

## ISE 컨피그레이션

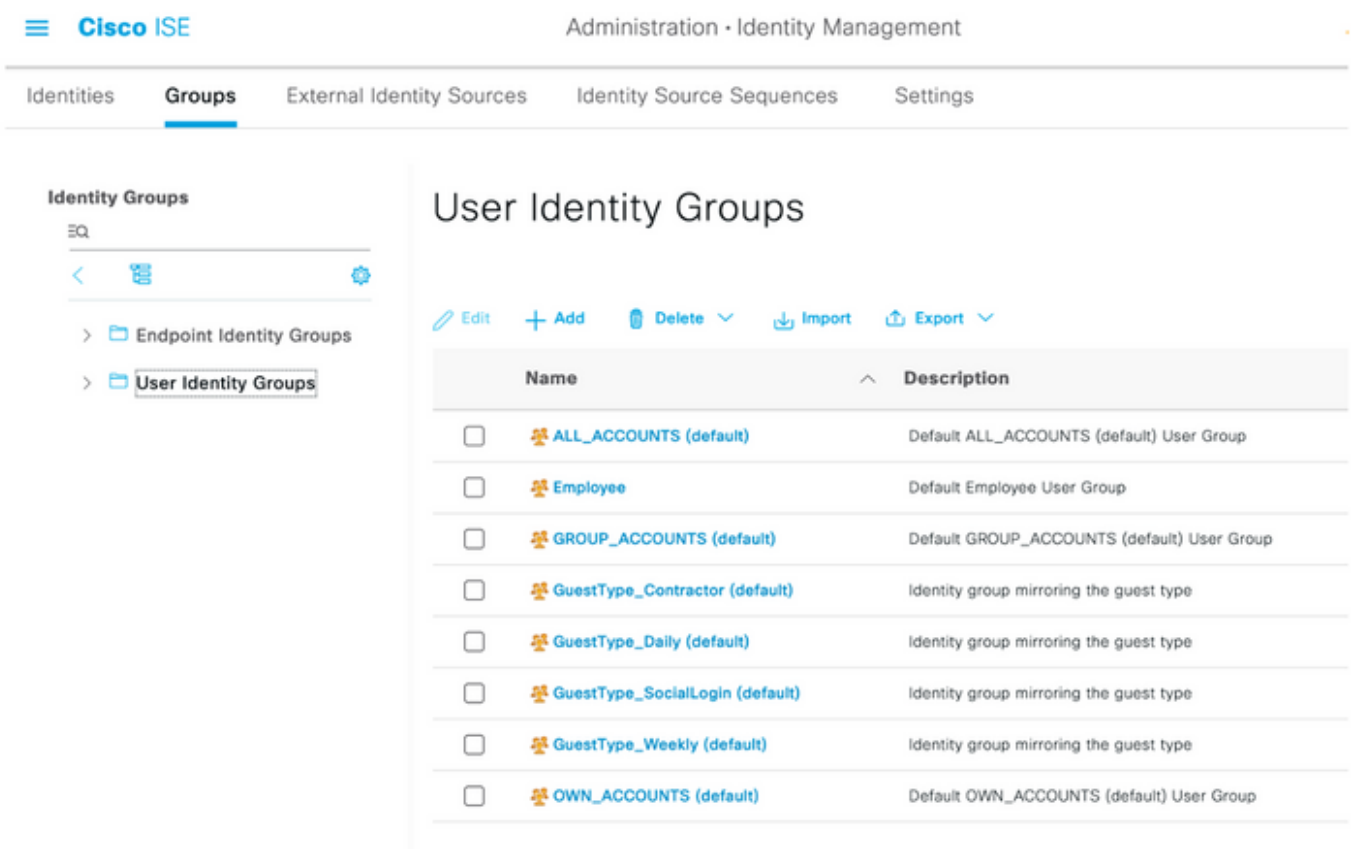
**1단계.** 세 개의 라인 아이콘을 선택합니다. 왼쪽 상단 모서리에 있는 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.



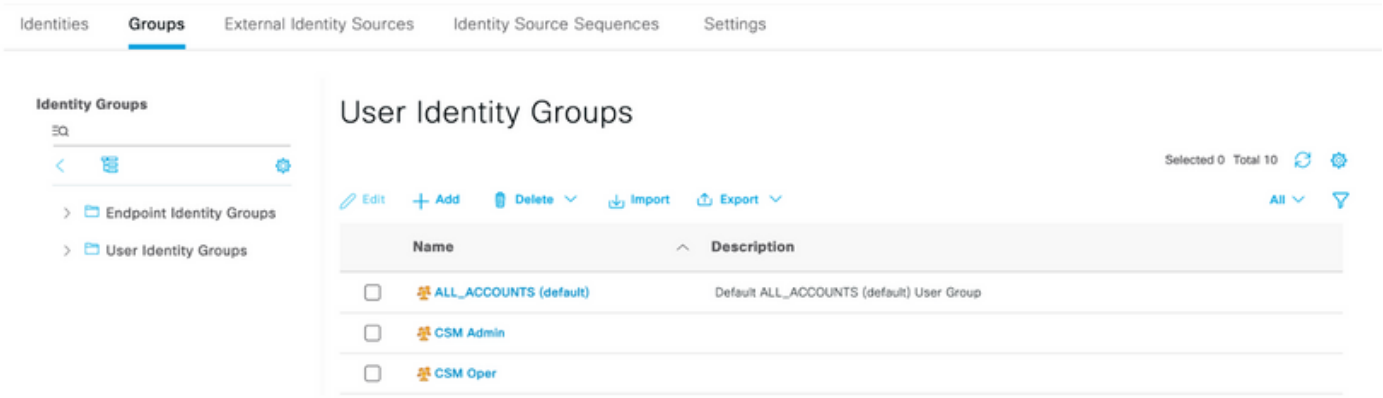

**2단계. +Add** 버튼을 선택하고 Network Access Device Name and IP Address(네트워크 액세스 디바이스 이름 및 IP 주소)에 적절한 값을 입력한 다음 **TACACS Authentication Settings(TACACS 인증 설정)** 확인란을 확인하고 공유 암호를 정의합니다.제출 버튼을 선택합니다.




**3단계.** 세 개의 라인 아이콘을 선택합니다. 의 왼쪽 위 모서리에 있는 Administration(관리) > Identity **Management(ID 관리) > Groups(그룹)로 이동합니다.**

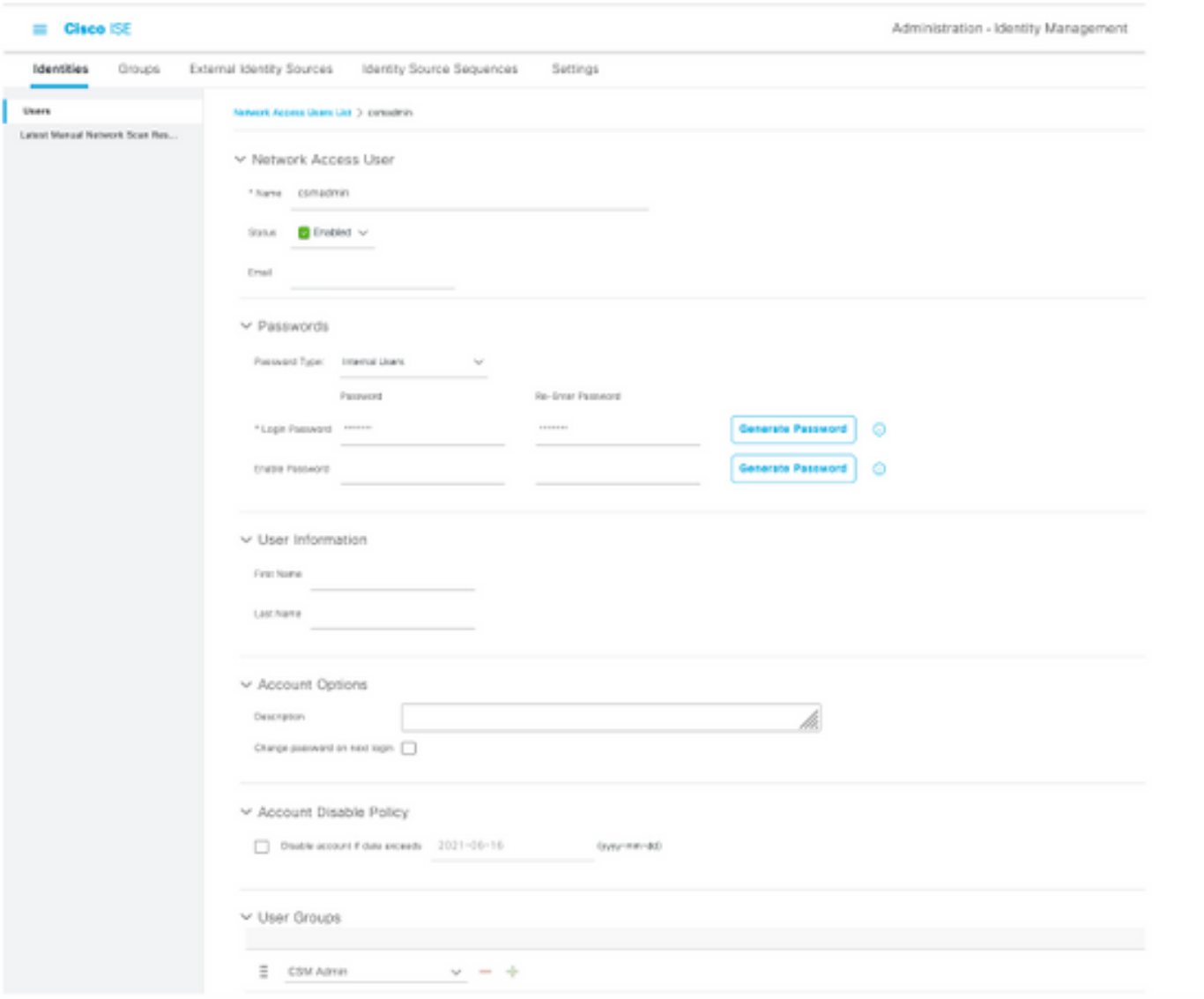


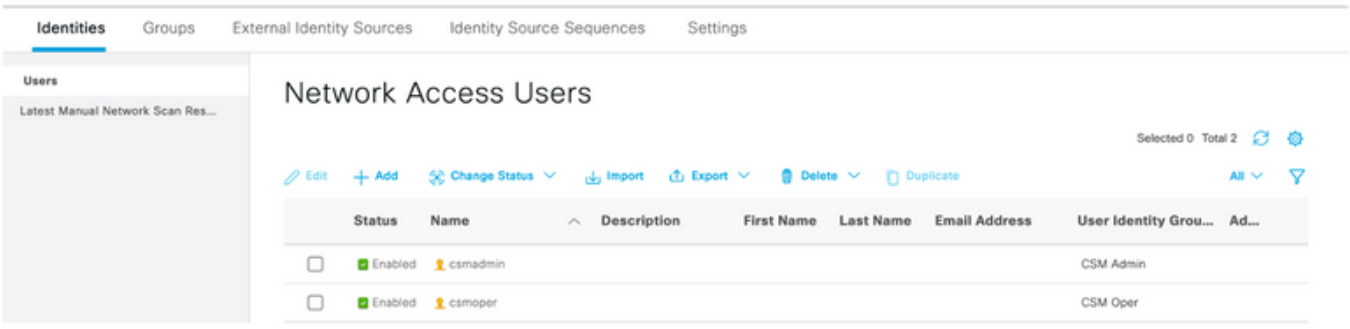
**4단계. User Identity Groups(사용자 ID 그룹)** 폴더로 이동하고 **+Add(추가)** 버튼을 선택합니다.이름을 정의하고 **실행** 버튼을 선택합니다.



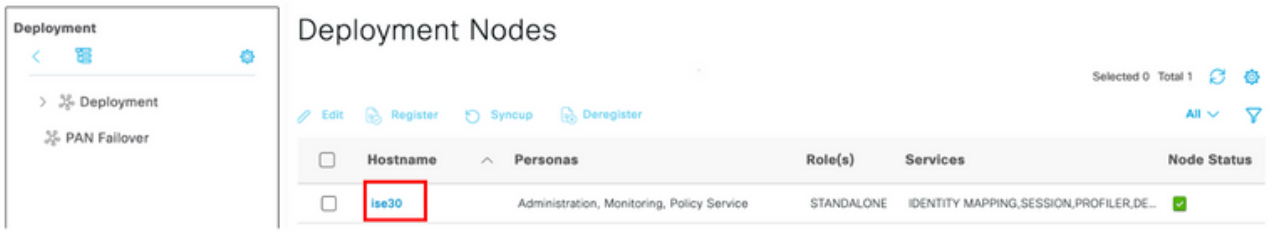

**참고:**이 예에서는 CSM Admin 및 CSM Oper Identity 그룹을 생성합니다.CSM의 각 관리자 사용자 유형에 대해 4단계를 반복할 수 있습니다.

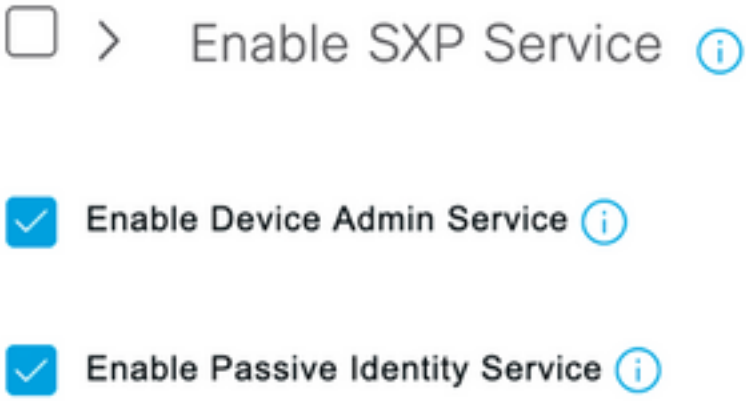
**5단계.** 3개 라인 아이콘 선택 Administration(관리) > Identity **Management(ID 관리) >Identities(ID)로 이동합니다.+**Add 버튼을 선택하고 사용자 이름과 비밀번호를 정의한 다음 사용자가 속한 그룹을 선택합니다.이 예에서는 csmadmin **및** Cosmoper 사용자**를** 생성하고 각각 CSM Admin 및 CSM Oper 그룹에 할당합니다.



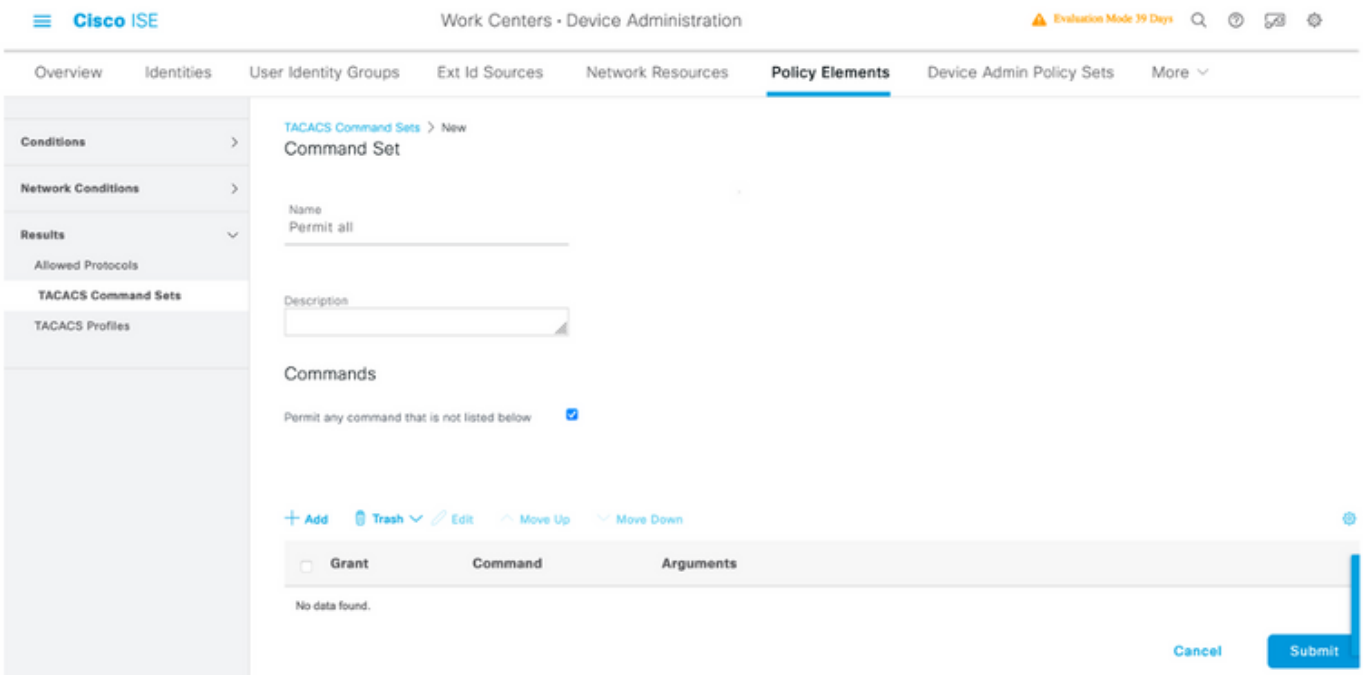

**6단계.** 선택 Administration(관리) **> System(시스템) > Deployment(구축)로 이동합니다.**호스트 이름 노드를 선택하고 **Device Admin Service를 활성화합니다.**



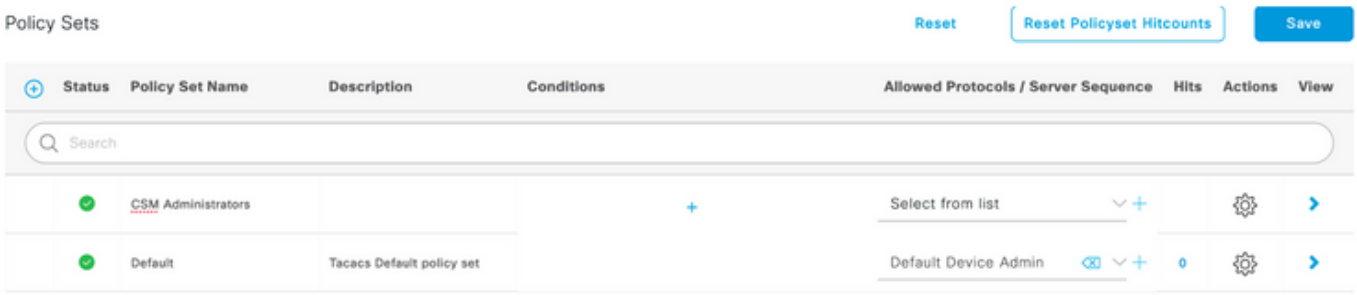

**참고:**분산 구축의 경우 TACACS 요청을 처리하는 PSN 노드를 선택합니다.

**7단계**. 3개 행 아이콘을 선택하고 Administration(관리) **> Device Administration(디바이스 관리) > Policy Elements(정책 요소)로 이동합니다.**Results(결과) **> TACACS Command Sets(TACACS 명령 세트)로 이동합니다.+추가** 버튼**을** 선택하고 명령 세트의 이름을 정의한 다음 **확인란 아래에 나열되지 않은 명령 허용**을 활성화합니다.제출을 **선택합니다.**

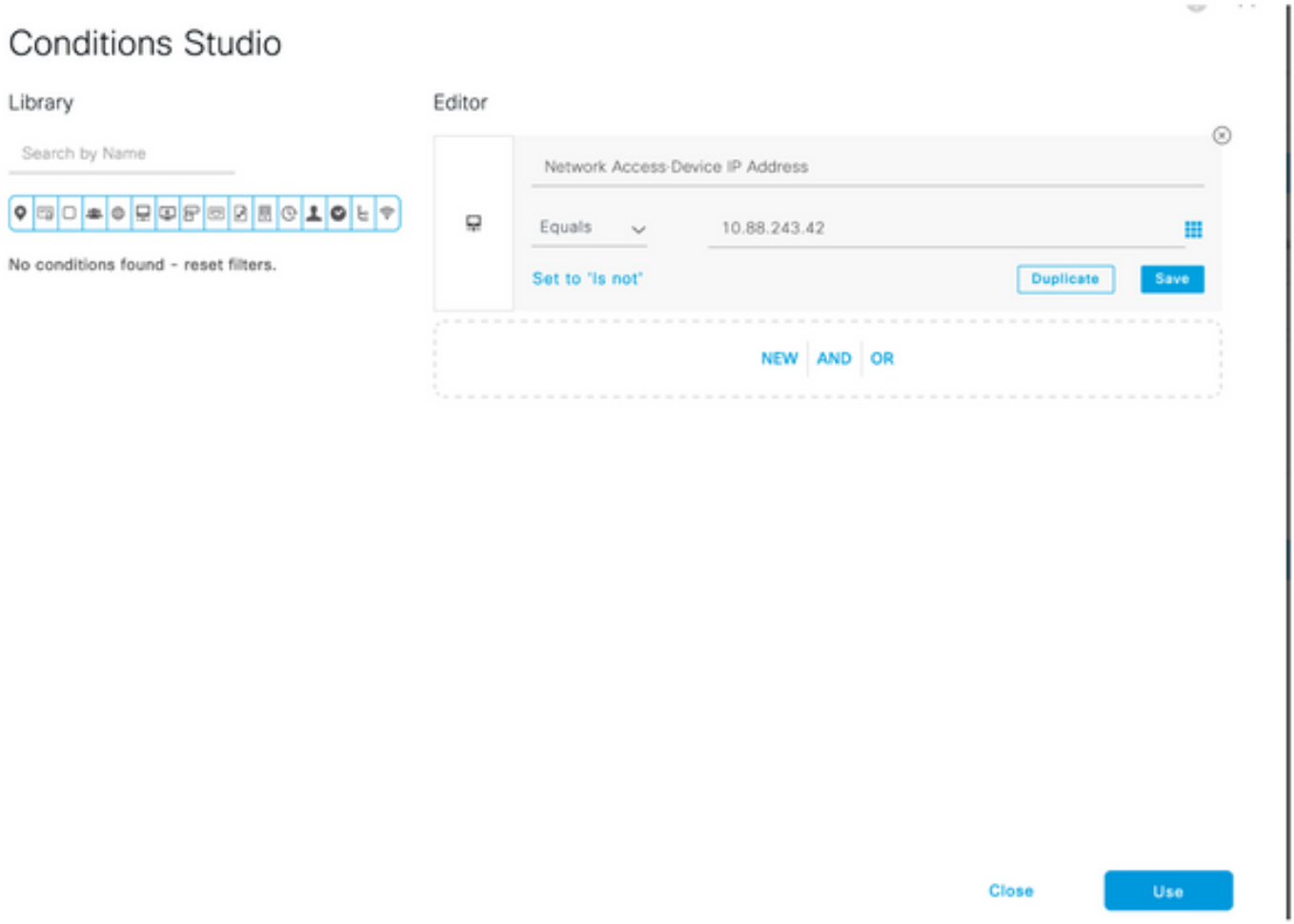



**8단계.** 왼쪽 상단 모서리에 있는 세 개의 회선 아이콘을 선택하고 Administration(관리) **->Device Administration(디바이스 관리)->Device Admin Policy Sets(디바이스 관리 정책 세트)로 이동합니다**

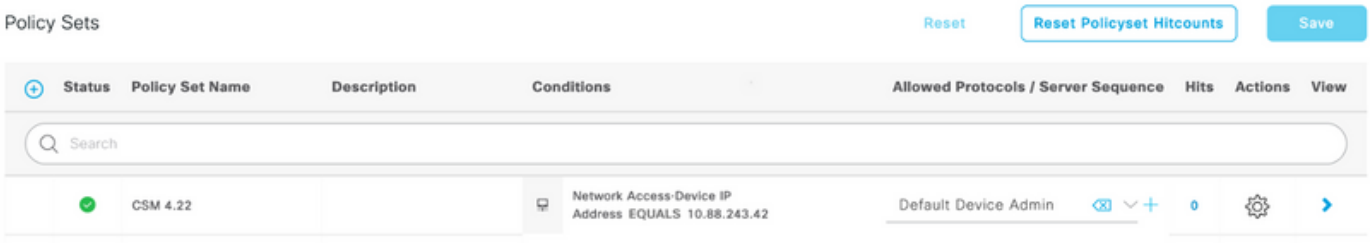
.선택  Policy Sets(정책 집합) 제목 아래에 있는 이름을 정의하고 가운데의+ 버튼을 선택하여 새 조건을 추가합니다.




**9단계.** Condition(조건) 창에서 특성 추가를 선택한 다음 Network Device Icon(**네트워크 디바이스** 아이콘)을 선택하고 Network access device IP address(네트워크 액세스 디바이스 IP 주소)를 선택합니다. Attribute **Value(특성 값)**를 선택하고 CSM IP 주소를 추가합니다.Use once done을 선택합니다.




**10단계.** Allow protocols(허용 프로토콜) 섹션에서 Device Default **Admin(디바이스 기본 관리자)을** 선택합니다.저장 **선택**



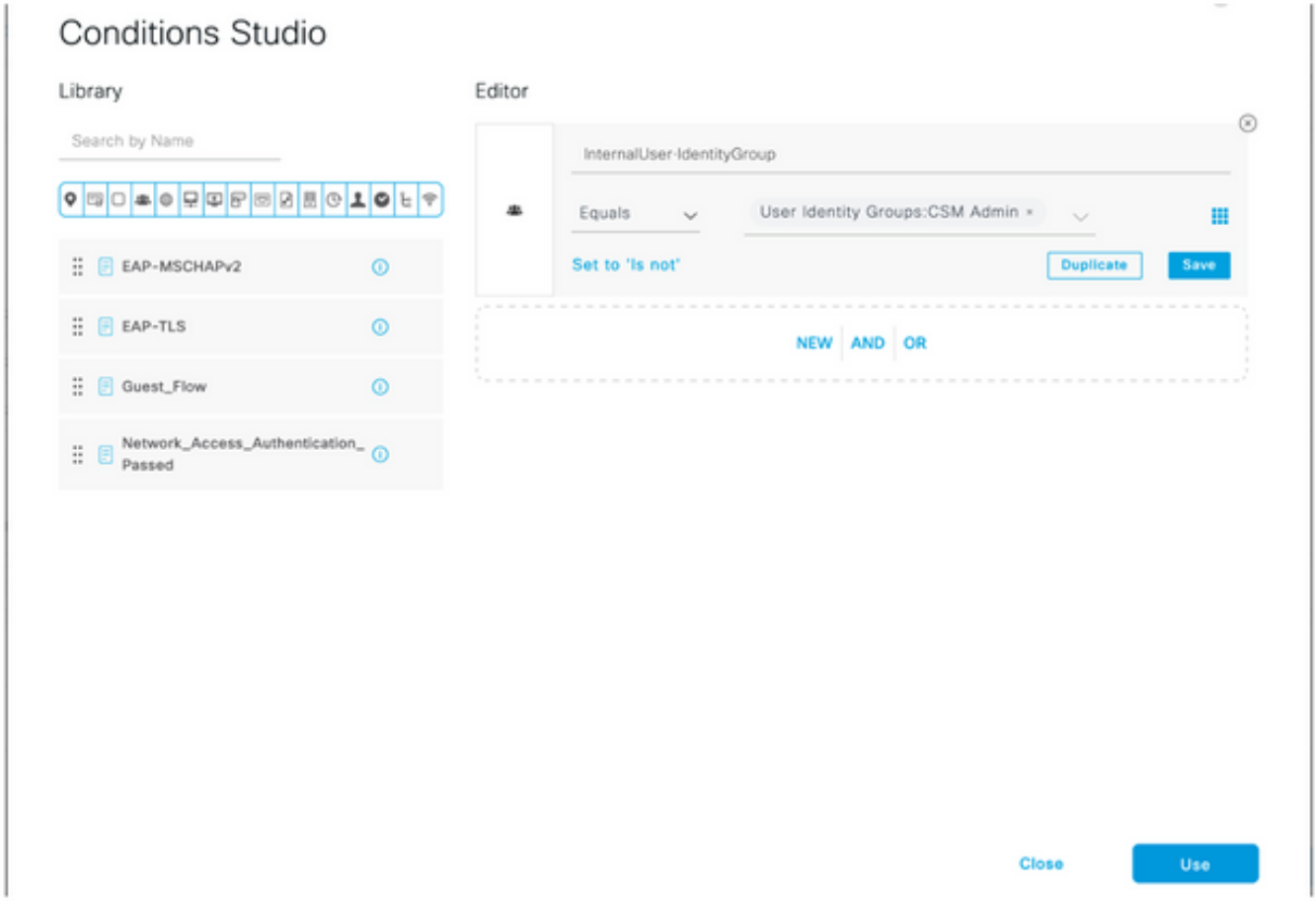

**11단계.** 오른쪽 화살표를 선택합니다. 인증 및 권한 부여 정책을 정의하도록 설정된 정책의 아이콘

**12단계.** 선택 인증 정책 제목 아래에 있는 이름을 정의하고 중간에 있는 +를 선택하여 새 조건을 추가합니다.Condition(조건) 창에서 특성 추가를 선택한 다음 **Network Device Icon(네트워크 디바이스** 아이콘)과 Network access device IP address(네트워크 액세스 디바이스 IP 주소)를 차례로 선택합니다. Attribute **Value(특성 값**)를 선택하고 CSM IP 주소를 추가합니다.Use once 완료 를 선택합니다.

**13단계.** ID 저장소에서 내부 사용자를 선택하고 **저장 선택**

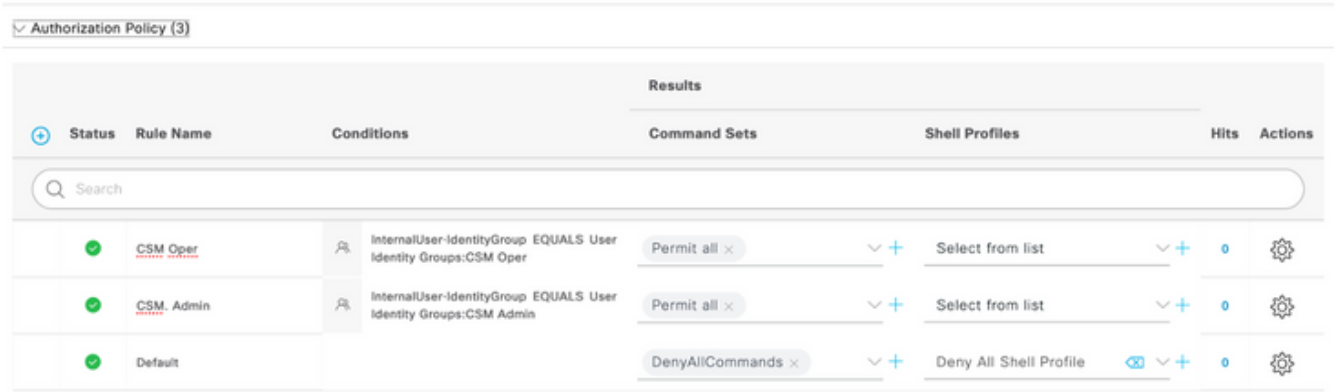

**참고:**ISE가 Active Directory에 조인된 경우 ID 저장소를 AD 저장소로 변경할 수 있습니다.

**14단계.** 선택 Authorization Policy(권한 부여 정책) 제목 아래에 있는 이름을 정의하고 가운데에서**+** 버튼을 선택하여 새 조건을 추가합니다.조건 창에서 속성 추가를 선택한 다음 ID 그룹 아이콘**과 내부 사용자**를 차례로 선택합니다.**ID 그룹**.CSM Admin Group(CSM 관리 그룹)을 선택하고 Use(사용)를 **선택합니다**.



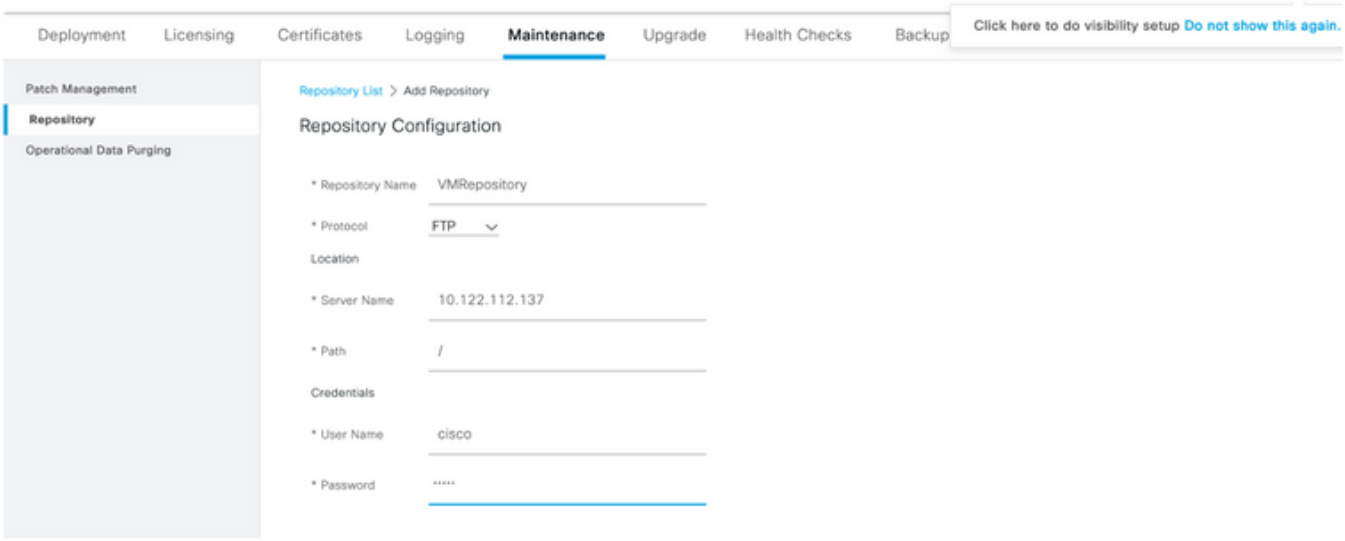

**15단계.** Command Set(명령 집합)에서 Permit all command set created in Step 7(7단계에서 생성한 모든 명령 집합 허용)을 선택한 다음 Save(저장)를 선택합니다.

CSM Oper 그룹에 대해 14단계 및 15단계를 반복합니다.



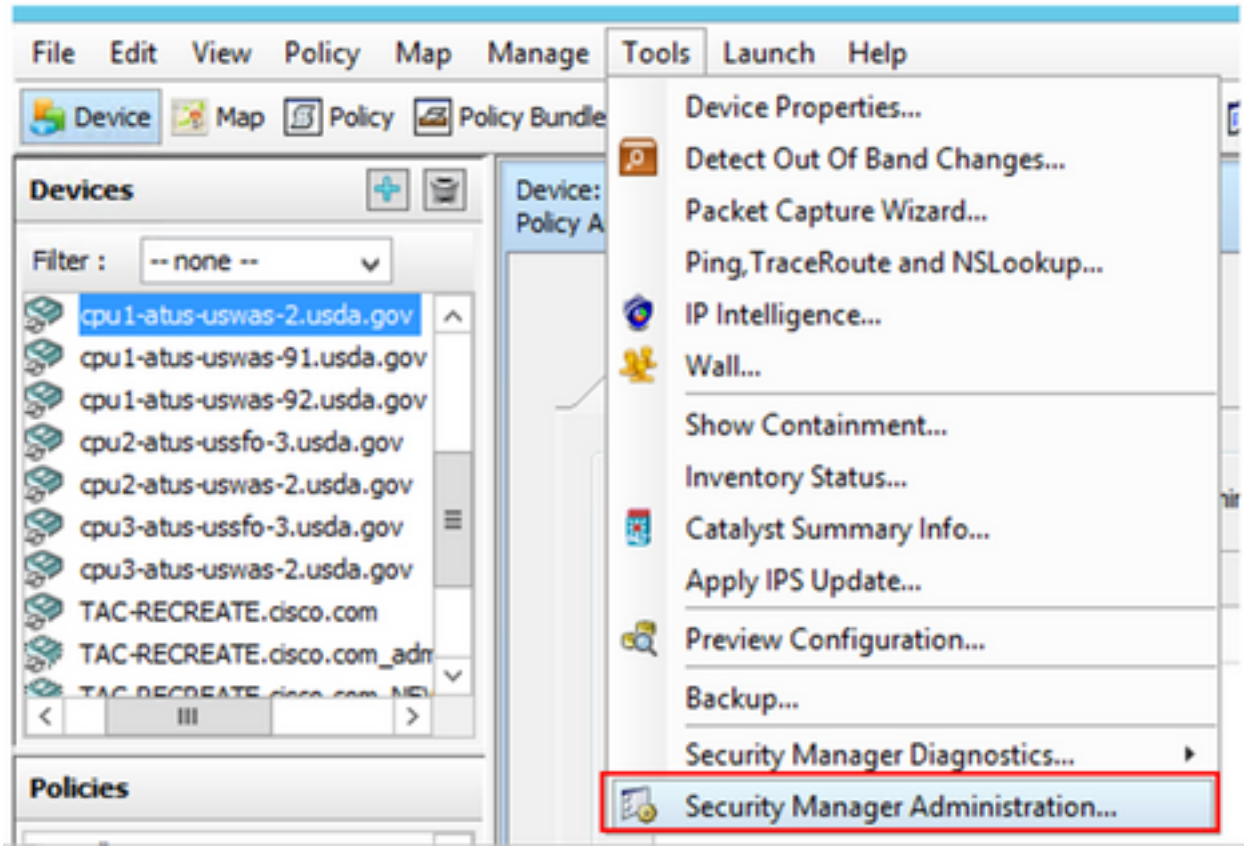

**16단계(선택 사항).** 왼쪽 상단 모서리에 있는 세 개의 회선 아이콘을 선택하고 **Administration>System>Maintenance>Repository**를 선택한 다음 **+Add**를 선택하여 문제 해결을 위해 TCP 덤프 파일을 저장하는 데 사용되는 저장소를 추가합니다.

**17단계(선택 사항).** 저장소 이름, 프로토콜, 서버 이름, 경로 및 자격 증명을 정의합니다.완료되면 **Submit(제출)**을 선택합니다.

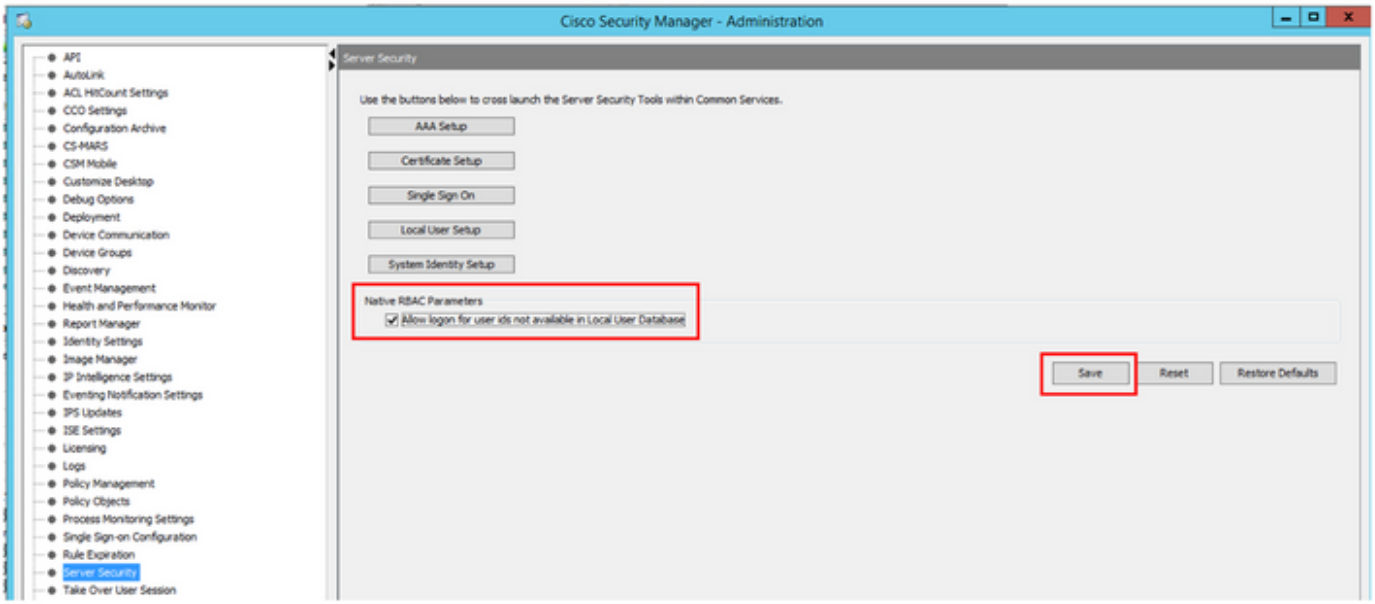



## CSM 컨피그레이션

**1단계.** 로컬 관리자 계정으로 Cisco Security Manager Client 애플리케이션에 로그인합니다.메뉴에서 **Tools > Security Manager Administration으로 이동합니다.**



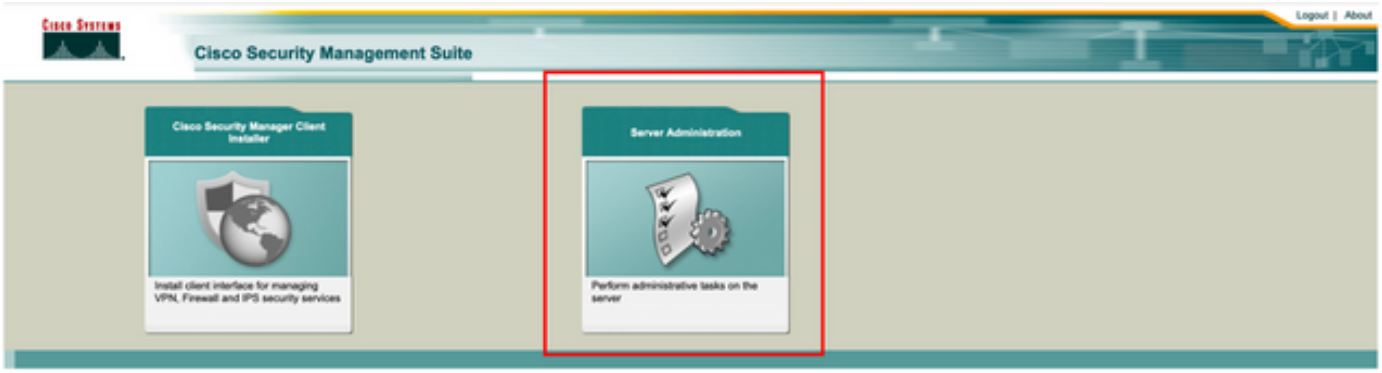

**2단계.** Native RBAC Parameters(기본 RBAC 매개변수) **아래의 확인란을 선택합니다.**저장 및 **닫기 선택**




**3단계.** 메뉴에서 파일 **> 실행을 선택합니다.파일 > 전송.**

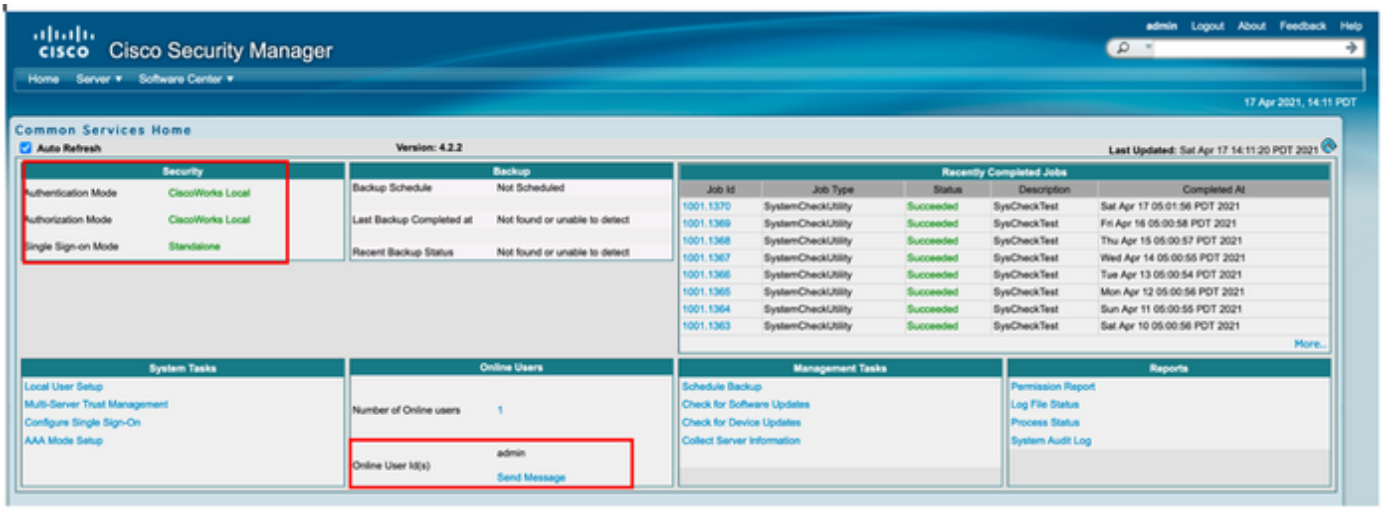
**참고:**컨피그레이션 변경이 제출되어 구축해야 하는 경우 모든 변경 사항을 저장해야 합니다.

**4단계.** CSM Management UI로 이동하고 https://<enter_CSM_IP_Address를 입력하고 **Server Administration(서버 관리)을 선택합니다.**



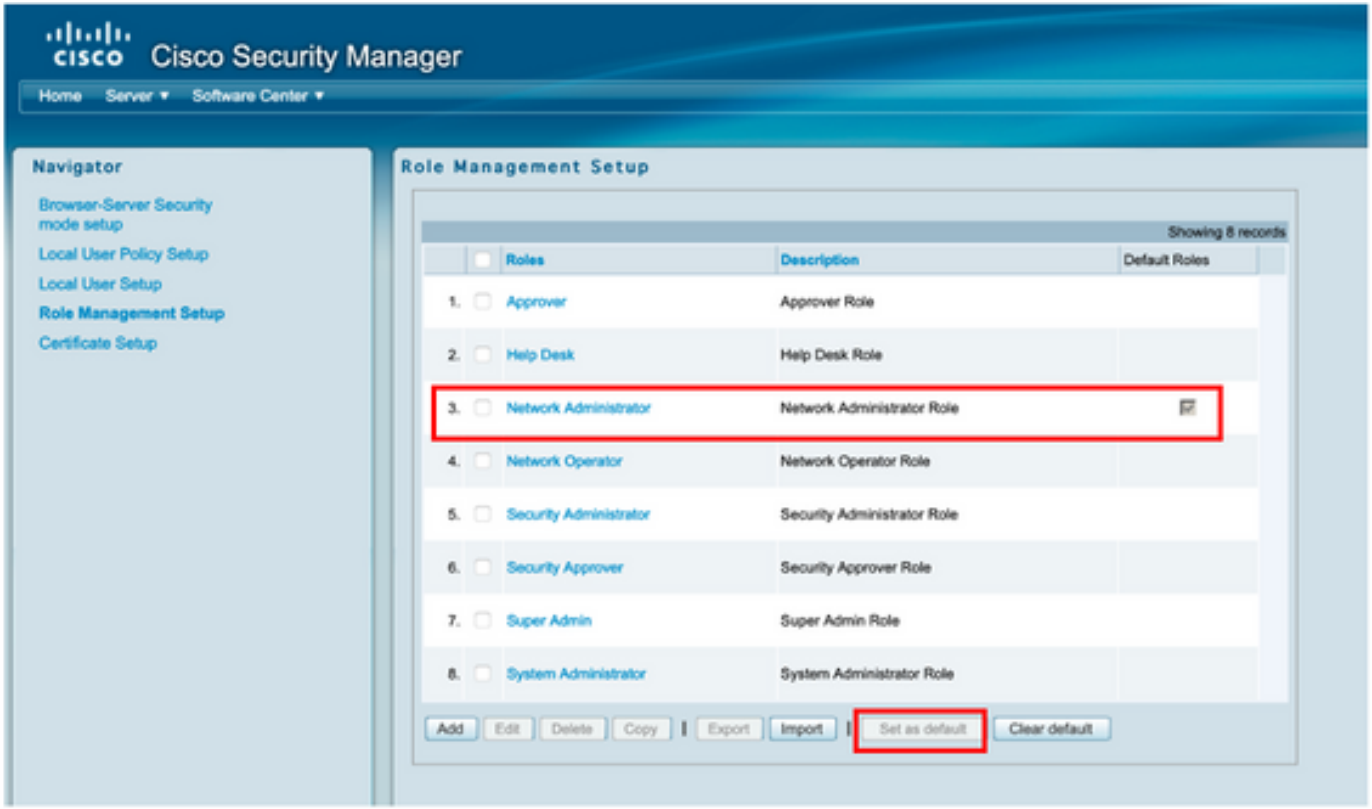

**참고:**4~7단계에서는 ISE에 정의되지 않은 모든 관리자에 대한 기본 역할을 정의하는 절차를 보여줍니다.이러한 단계는 선택 사항입니다.

**5단계.** 인증 모드가 **CiscoWorks Local**로 설정되었는지 확인하고 **Online** userID는 CSM에서 생성된 로컬 관리자 계정입니다.



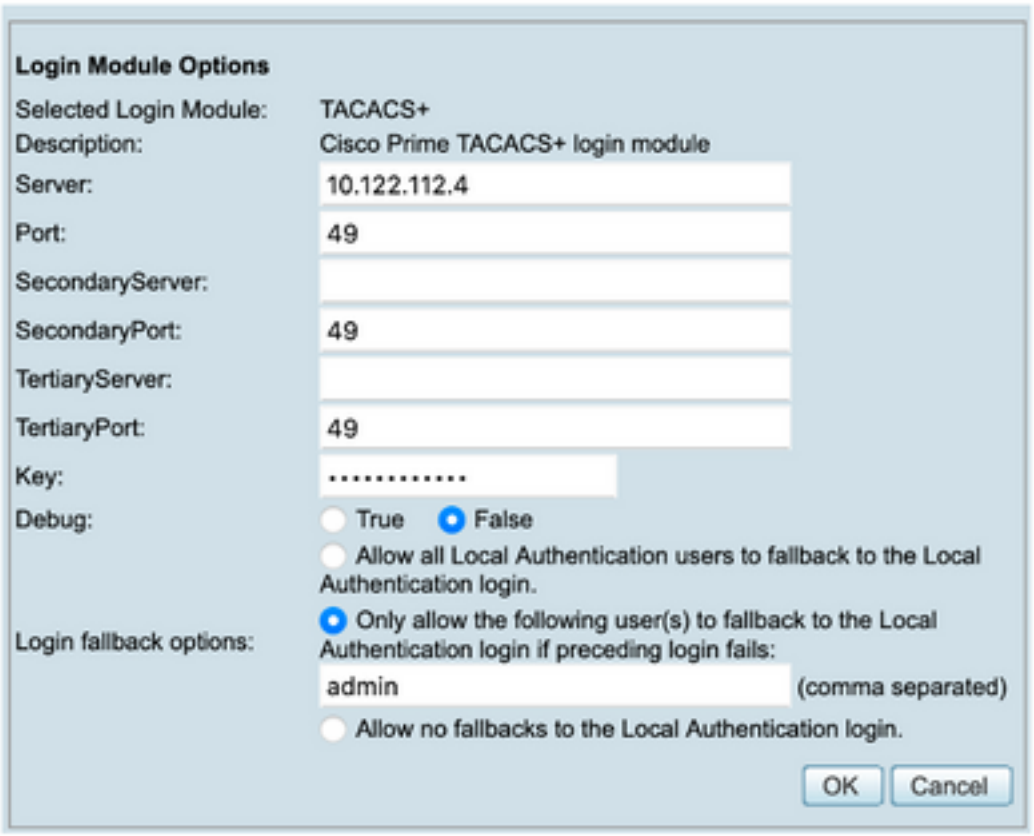

**6단계. 서버**로 **이동하고 단일 서버 관리**를 선택합니다.

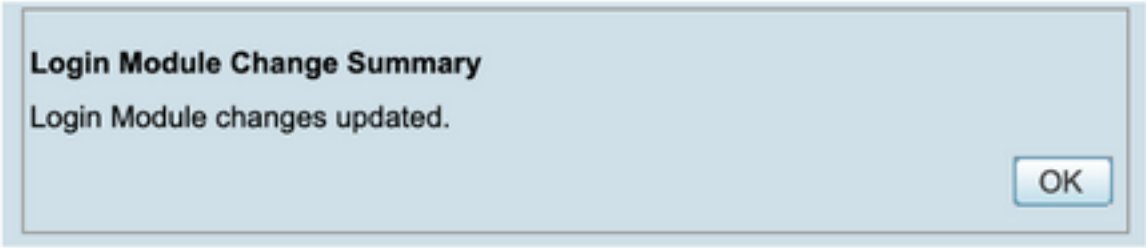

**7단계.** Role Management Setup(역할 관리 설정)을 선택하고 인증 시 모든 관리자 사용자가 받는 기본 권한을 선택합니다.이 예에서는 네트워크 관리자가 사용됩니다.선택한 후 **기본값으로 설정을** 선택합니다.



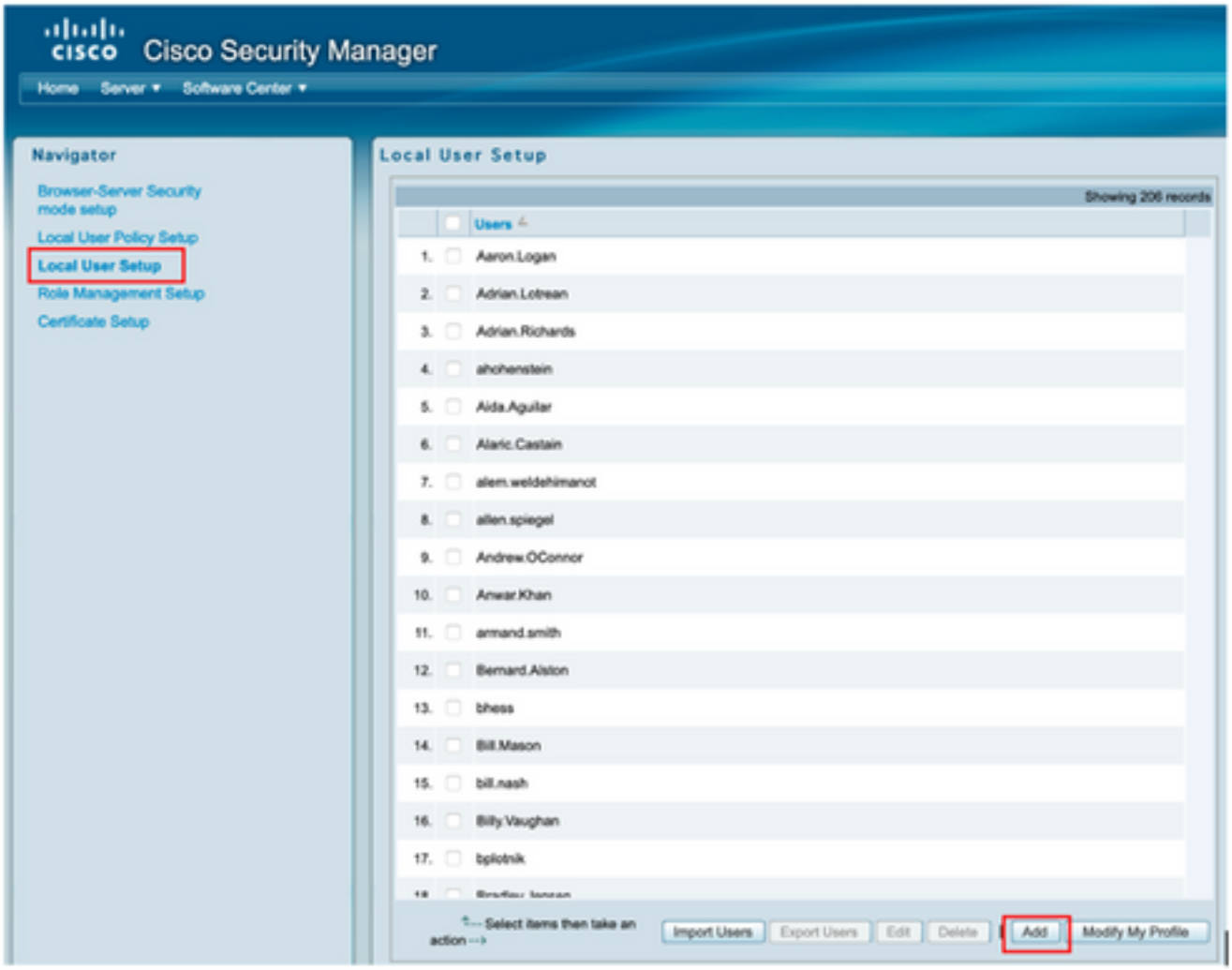

**8단계.** Server(서버) **>AAA Mode Setup Role(AAA 모드 설정 역할)을** 선택한 다음 **TACACS+** 옵션을 선택하고 마지막으로 변경**을 선택하여** ISE 정보를 추가합니다.


**9단계.** ISE IP 주소 및 키를 정의합니다. 선택적으로 모든 로컬 인증 사용자를 허용하는 옵션을 선택하거나 로그인이 실패한 경우 한 명의 사용자만을 허용할 수 있습니다.이 예에서는 Only admin 사용자가 대체 방법으로 허용됩니다.**확인**을 선택하여 변경 사항을 저장합니다.

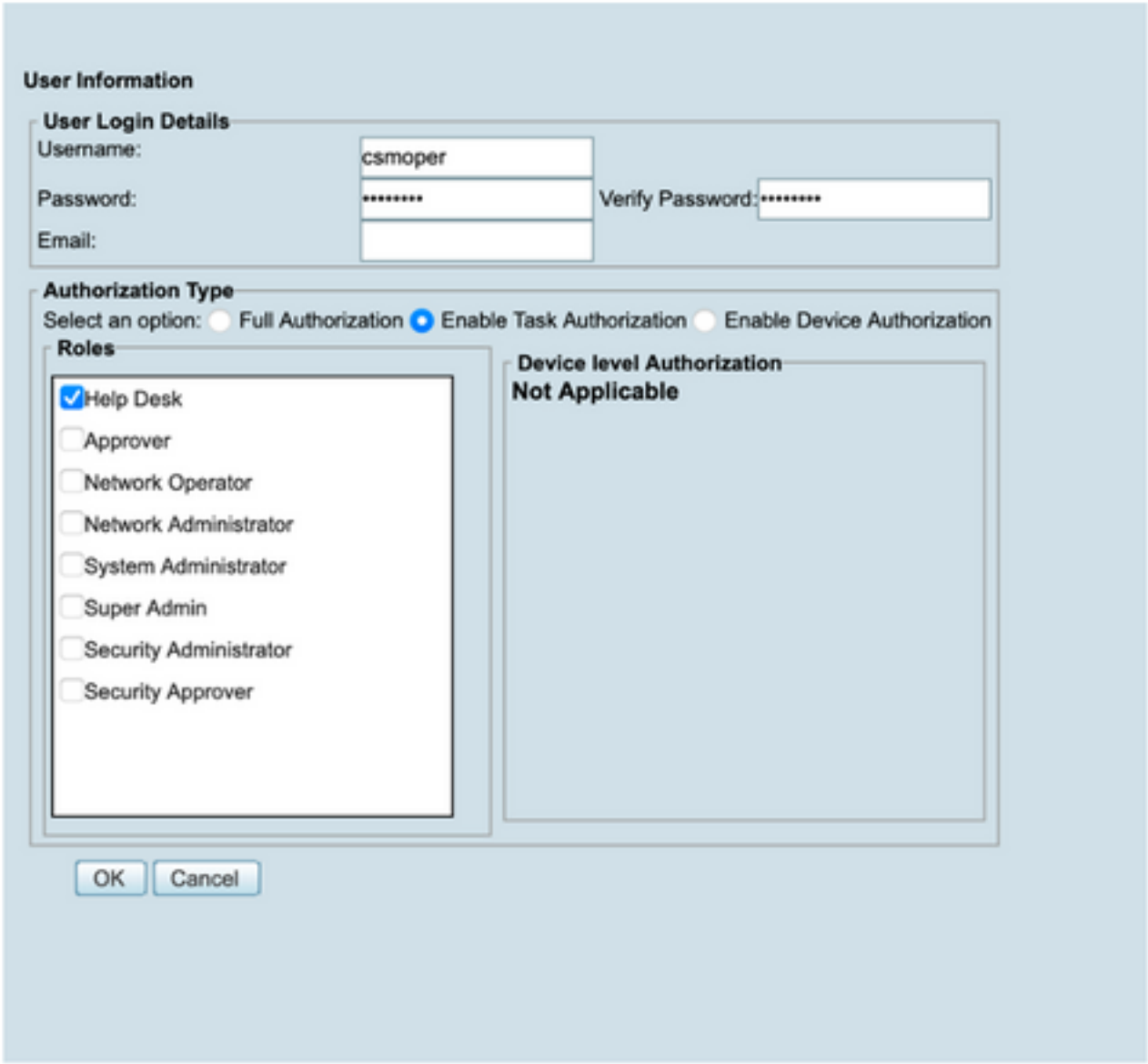





**10단계.** Server(**서버**) **> Single Server Management(단일 서버 관리)**를 선택한 다음 **Local User Setup(로컬 사용자 설정)**을 선택하고 **Add(추가)**를 선택합니다.



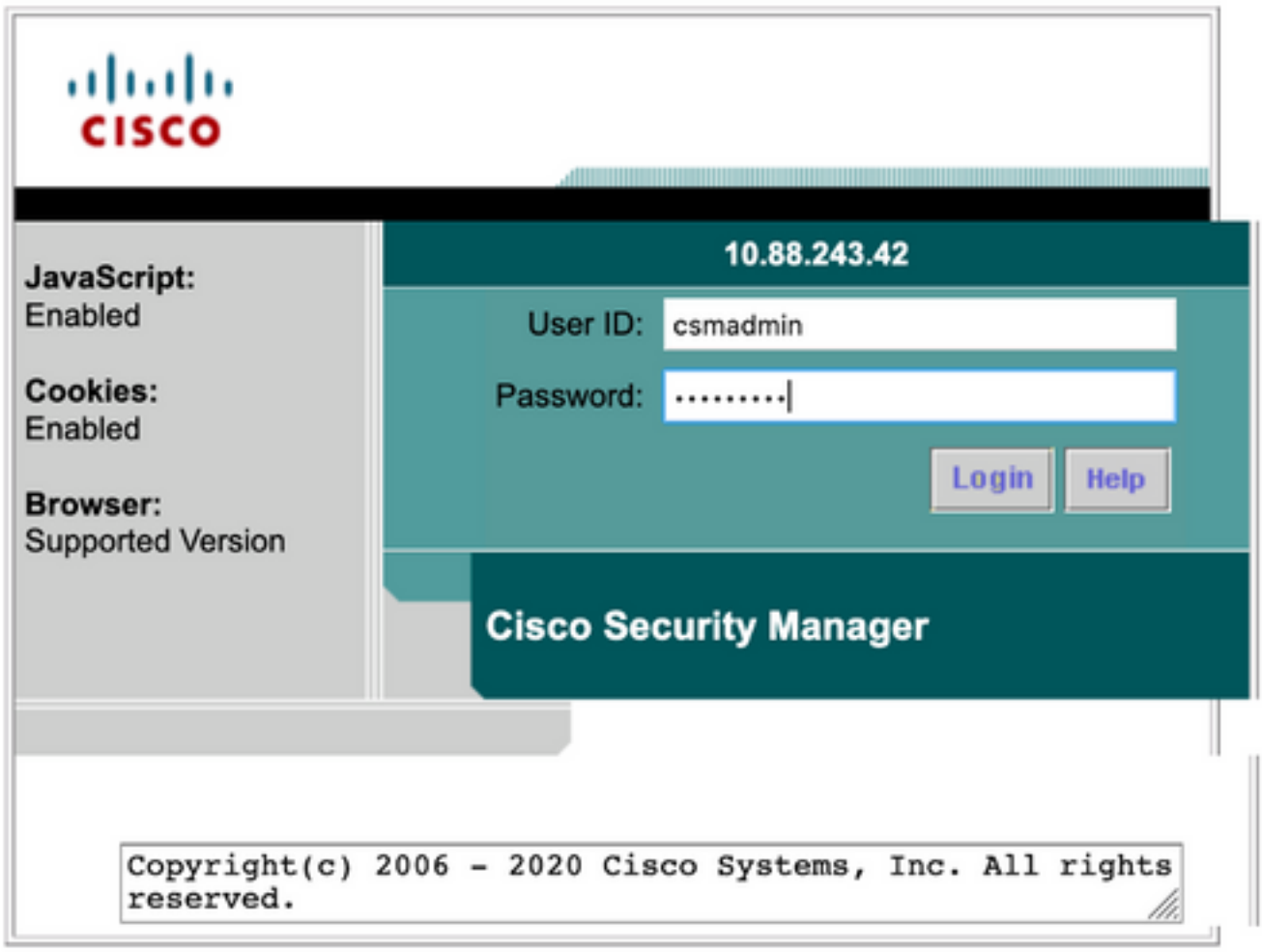

**11단계.** ISE 컨피그레이션 섹션, **관리자** 및 **헬프 데스크 작업 권한 부여 역할**이 이 이 예에서 사용되는 단계 5의 ISE에 생성된 동일한 사용자 이름 및 비밀번호를 정의합니다.관리자 사용자를 저장하려면 확인을 선택합니다.



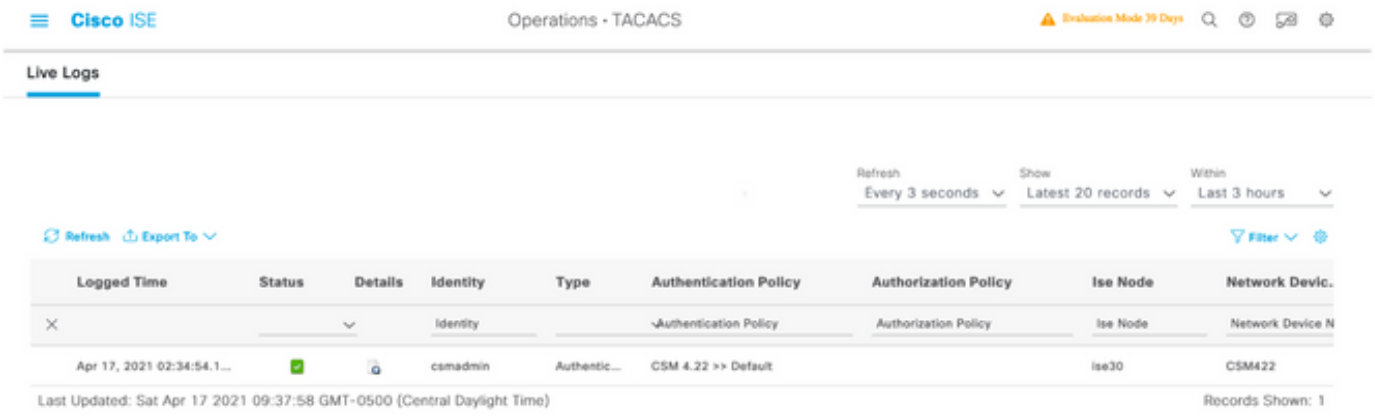

# 다음을 확인합니다.

### Cisco Security Manager 클라이언트 UI

**1단계.** 새 창 브라우저를 열고 https://<enter_CSM_IP_Address, ISE 컨피그레이션 섹션**의** 5단계에서 생성된 csmadmin 사용자 이름 및 비밀번호를 사용합니다.



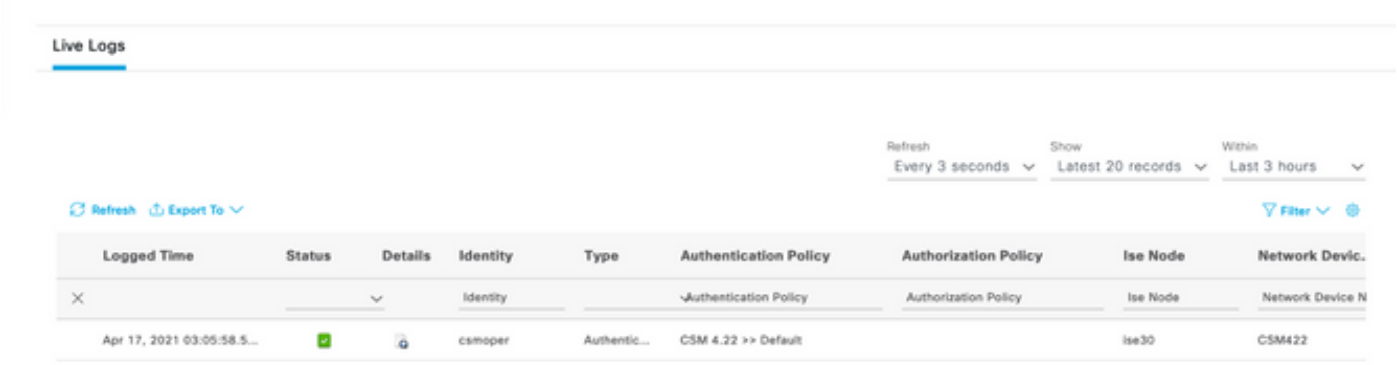

ISE TACACS 라이브 로그에서 시도 로그인 성공 확인 가능



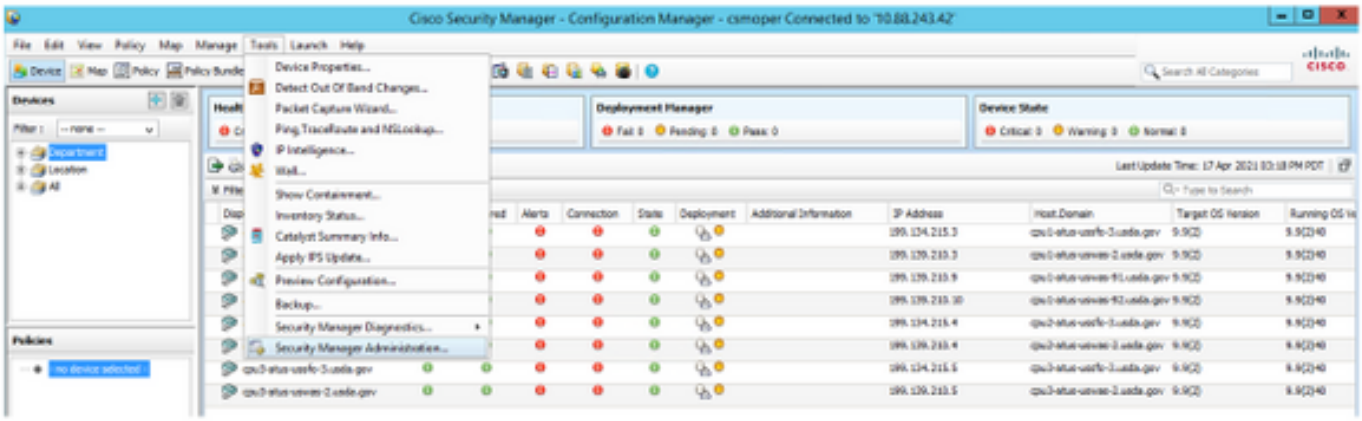

### Cisco Security Manager 클라이언트 애플리케이션

**1단계.** 헬프데스크 관리자 계정으로 Cisco Security Manager Client 애플리케이션에 로그인합니다.


ISE TACACS 라이브 로그에서 시도 로그인 성공 확인 가능




**2단계.** CSM 클라이언트 애플리케이션 메뉴에서 **Tools > Security Manager Administration**을 선택합니다. 오류 메시지는 권한이 없음을 나타냅니다.




**3단계.** csmadmin 계정과 함께 1~3단계를 반복하여 이 사용자에게 적절한 권한이 제공되었는지 확인합니다.

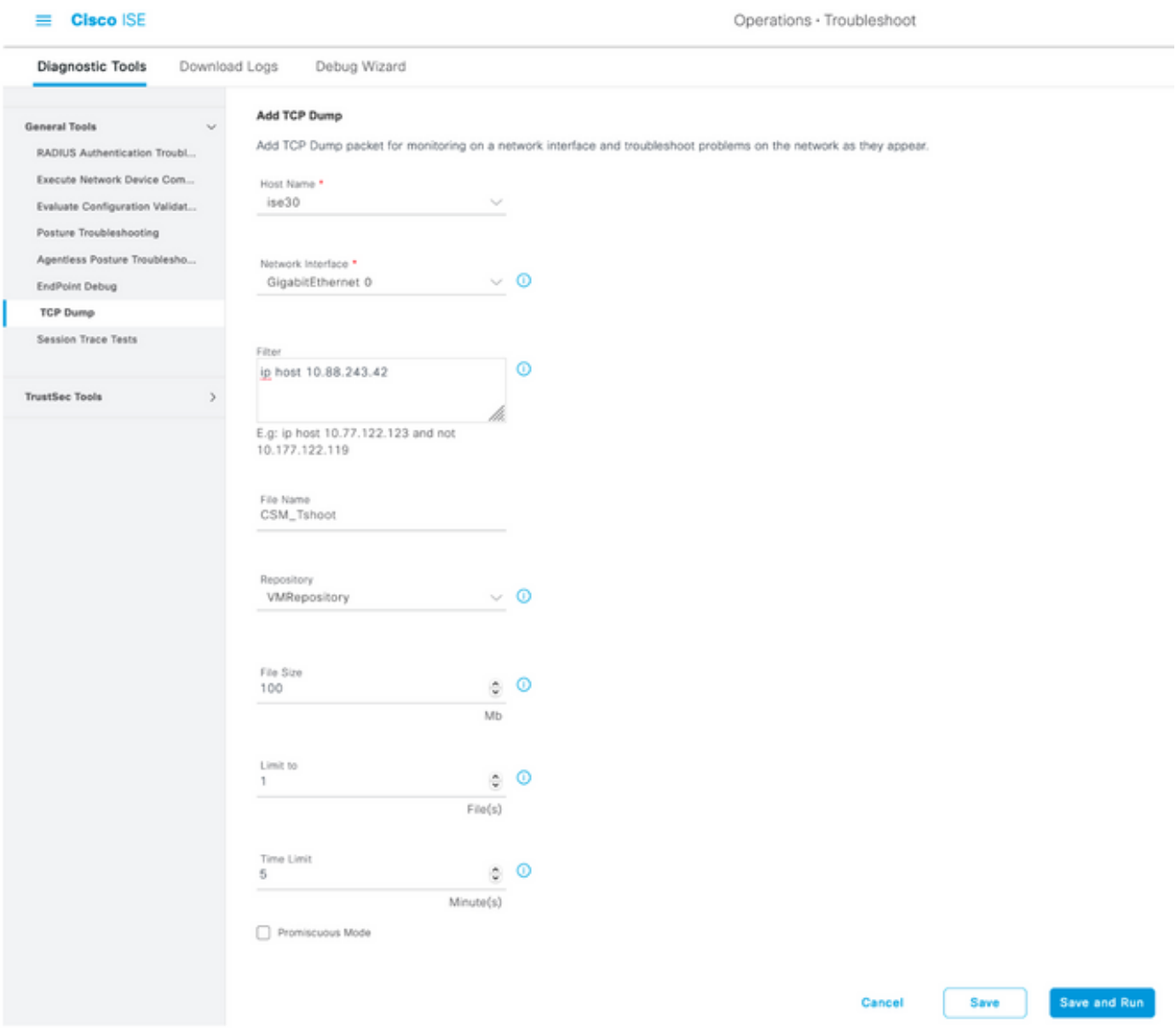
# 문제 해결

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

### ISE의 TCP 덤프 툴과의 통신 검증

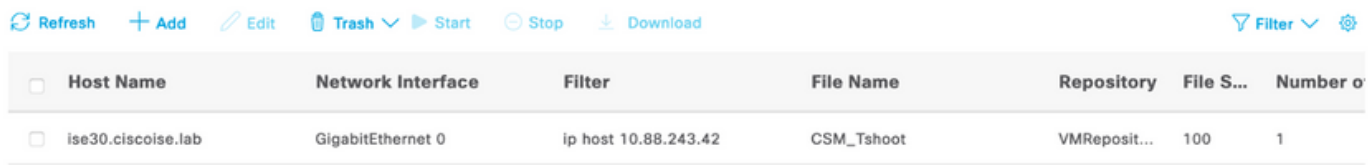
**1단계.**ISE에 로그인하고 왼쪽 상단 모서리에 있는 세 개의 회선 아이콘으로 이동한 다음 Operations(작업) **>Troubleshoot(문제 해결)>Diagnostic Tools(진단 도구)를** 선택합니다.

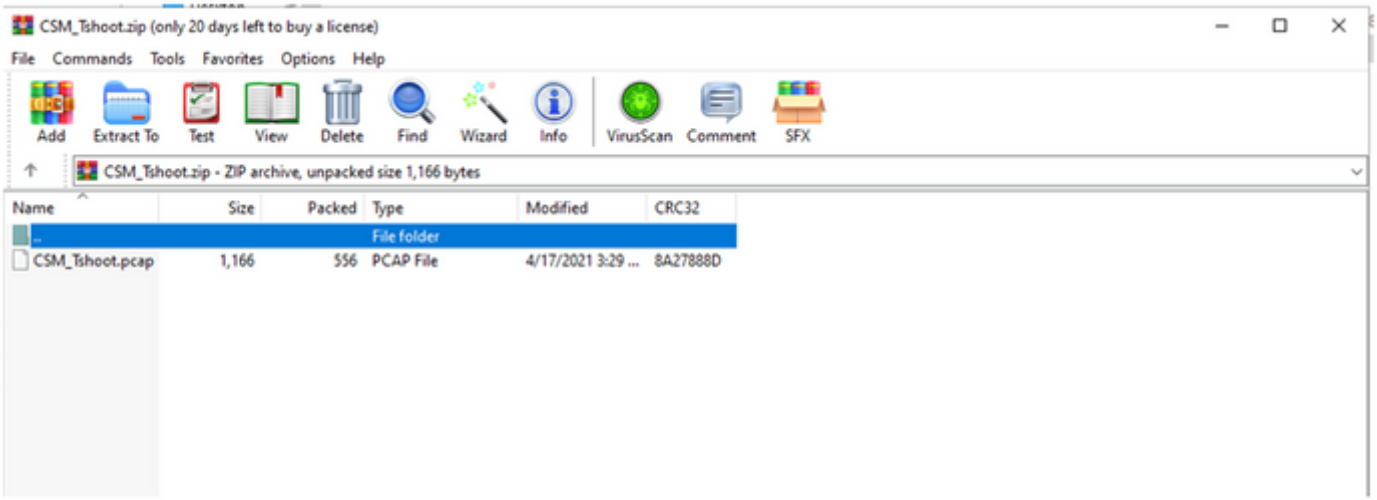
**2단계.** General(**일반) 도구**에서 **TCP Dumps(TCP 덤프)를** 선택한 다음 **Add+(추가+)를 선택합니다** .Hostname(호스트 이름), Network Interface File Name(네트워크 인터페이스 파일 이름), Repository(리포지토리) 및 선택적으로 CSM IP 주소 통신 흐름만 수집하도록 필터를 선택합니다 .저장 **및 실행 선택**



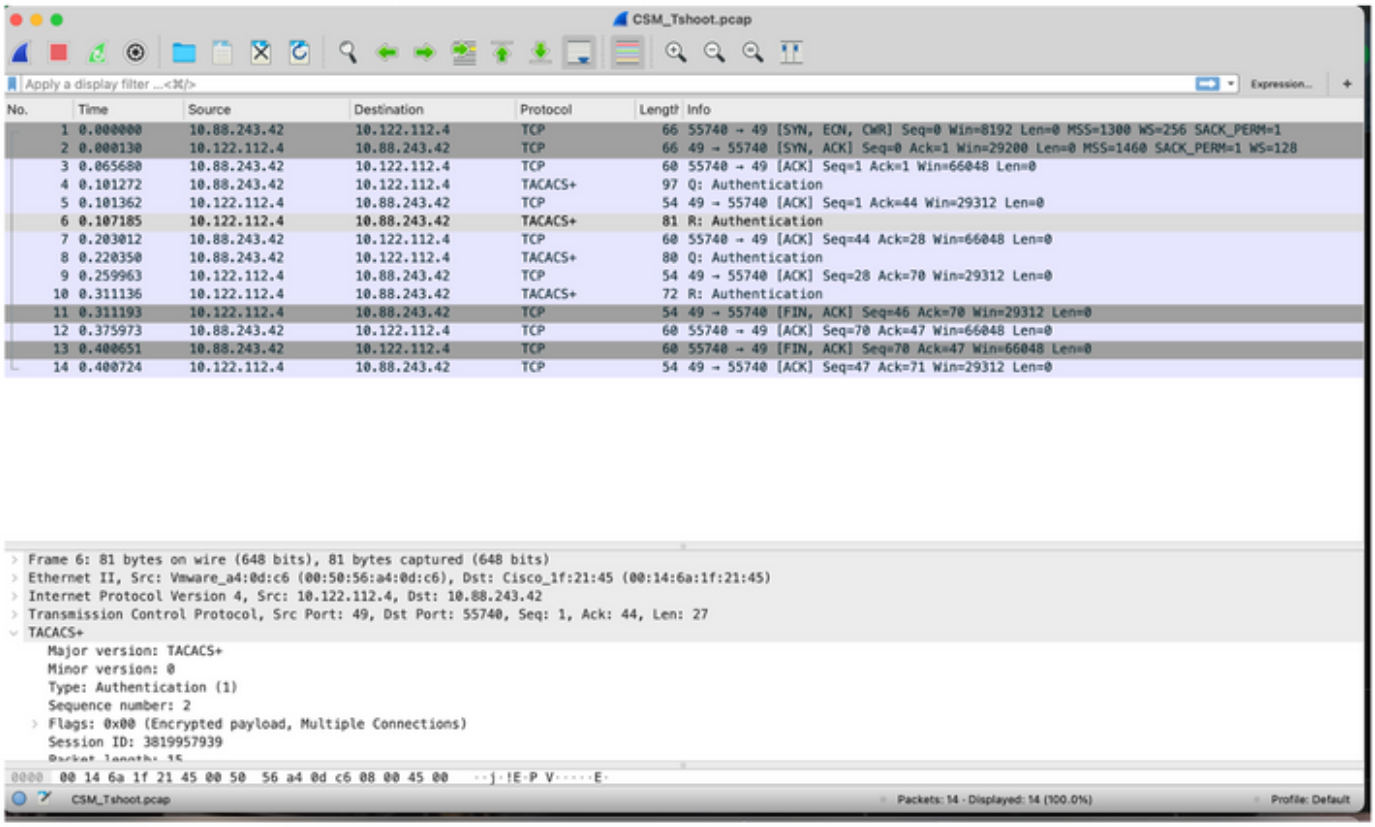

**3단계.** CSM 클라이언트 애플리케이션 또는 클라이언트 UI에 로그인하고 관리자 자격 증명을 입력합니다.

**4단계.** ISE에서 **Stop** 버튼을 선택하고 pcap 파일이 정의된 저장소로 전송되었는지 확인합니다.






**5단계.** pcap 파일을 열어 CSM과 ISE 간의 성공적인 통신을 검증합니다.




pcap 파일에 항목이 표시되지 않으면 다음을 검증합니다.

1. 디바이스 관리 서비스가 ISE 노드에서 활성화됨
2. CSM 컨피그레이션에 올바른 ISE IP 주소가 추가되었습니다.
3. 방화벽이 중간 확인 포트 49(TACACS)에 있는 경우 허용됩니다.