ISE 2.0:ASA CLI TACACS+ 인증 및 명령 권한 부여 컨피그레이션 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램](#)
[구성](#)
[인증 및 권한 부여를 위한 ISE 구성](#)
[네트워크 장치 추가](#)
[사용자 ID 그룹 구성](#)
[사용자 구성](#)
[장치 관리 서비스 사용](#)
[TACACS 명령 세트 구성](#)
[TACACS 프로파일 구성](#)
[TACACS 권한 부여 정책 구성](#)
[인증 및 권한 부여를 위해 Cisco ASA 방화벽 구성](#)
[다음을 확인합니다.](#)
[Cisco ASA 방화벽 확인](#)
[ISE 2.0 확인](#)
[문제 해결](#)
[관련 정보](#)
[관련 Cisco 지원 커뮤니티 토론](#)

소개

이 문서에서는 ISE(Identity Service Engine) 2.0 이상에서 Cisco ASA(Adaptive Security Appliance)에서 TACACS+ 인증 및 명령 권한 부여를 구성하는 방법에 대해 설명합니다.ISE는 로컬 ID 저장소를 사용하여 사용자, 그룹 및 엔드포인트와 같은 리소스를 저장합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA 방화벽이 완벽하게 작동
- ASA와 ISE 간의 연결
- ISE 서버 부트스트랩

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 2.0
- Cisco ASA 소프트웨어 릴리스 9.5(1)

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.

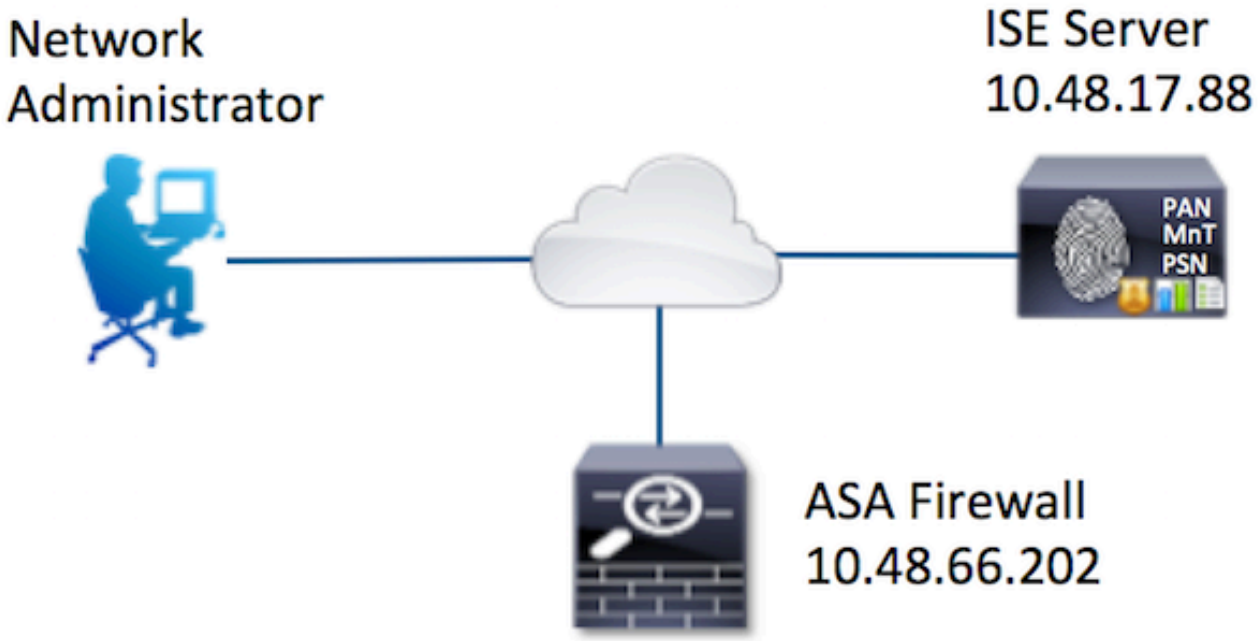
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

구성

구성의 목적은 다음과 같습니다.

- 내부 ID 저장소를 통해 ssh 사용자 인증
- 로그인 후 특별 권한 EXEC 모드로 전환되도록 ssh 사용자 권한 부여
- 확인을 위해 실행된 모든 명령을 ISE에 확인 및 전송

네트워크 다이어그램



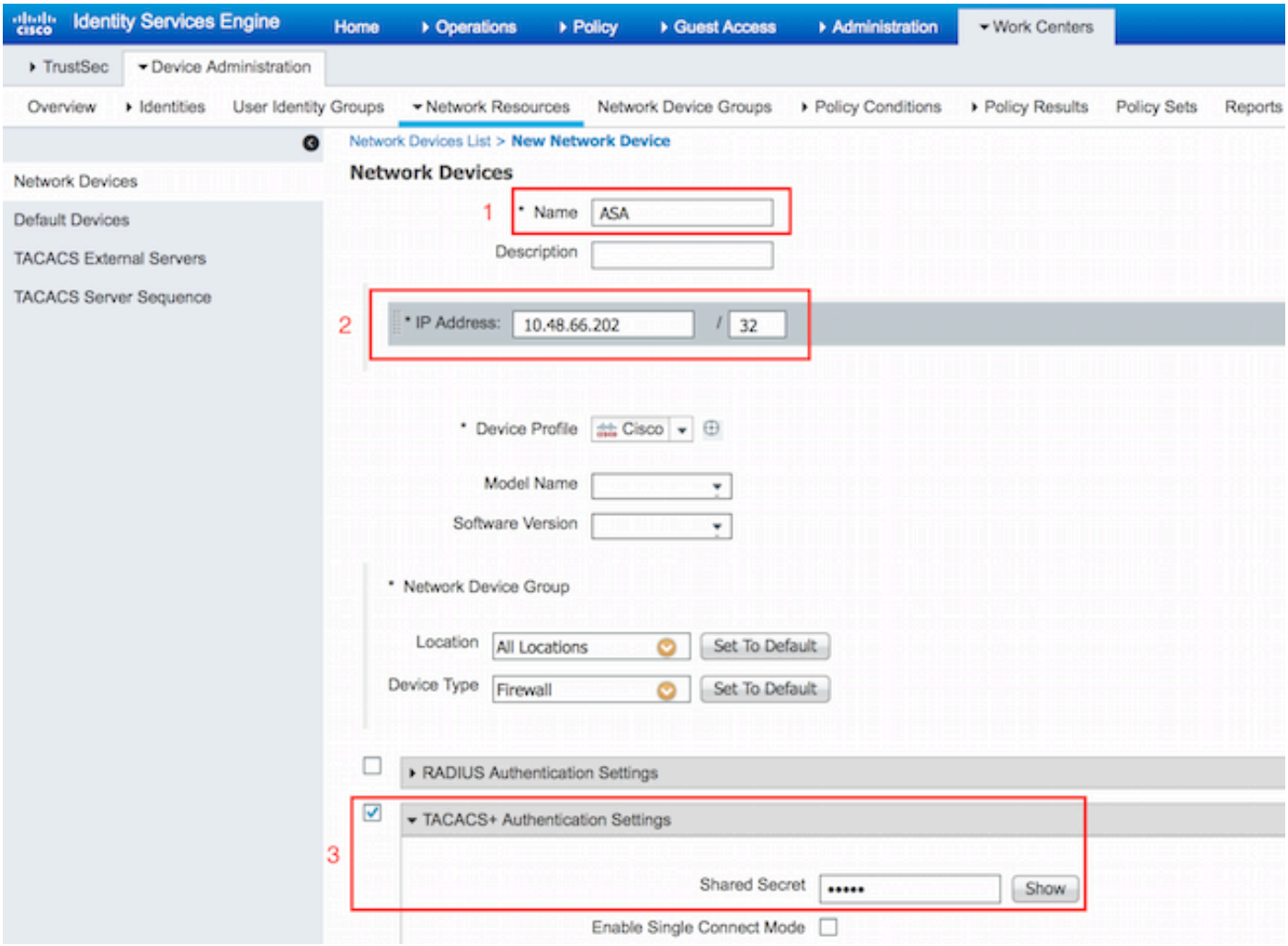
구성

인증 및 권한 부여를 위한 ISE 구성

두 명의 사용자가 생성됩니다.사용자 **관리자**는 ISE에서 **Network Admins** 로컬 ID 그룹의 일부입니다.이 사용자는 전체 CLI 권한을 갖습니다.사용자 **사용자**는 ISE에서 **네트워크 유지 관리 팀** 로컬 ID 그룹의 일부입니다.이 사용자는 show 명령과 ping만 수행할 수 있습니다.

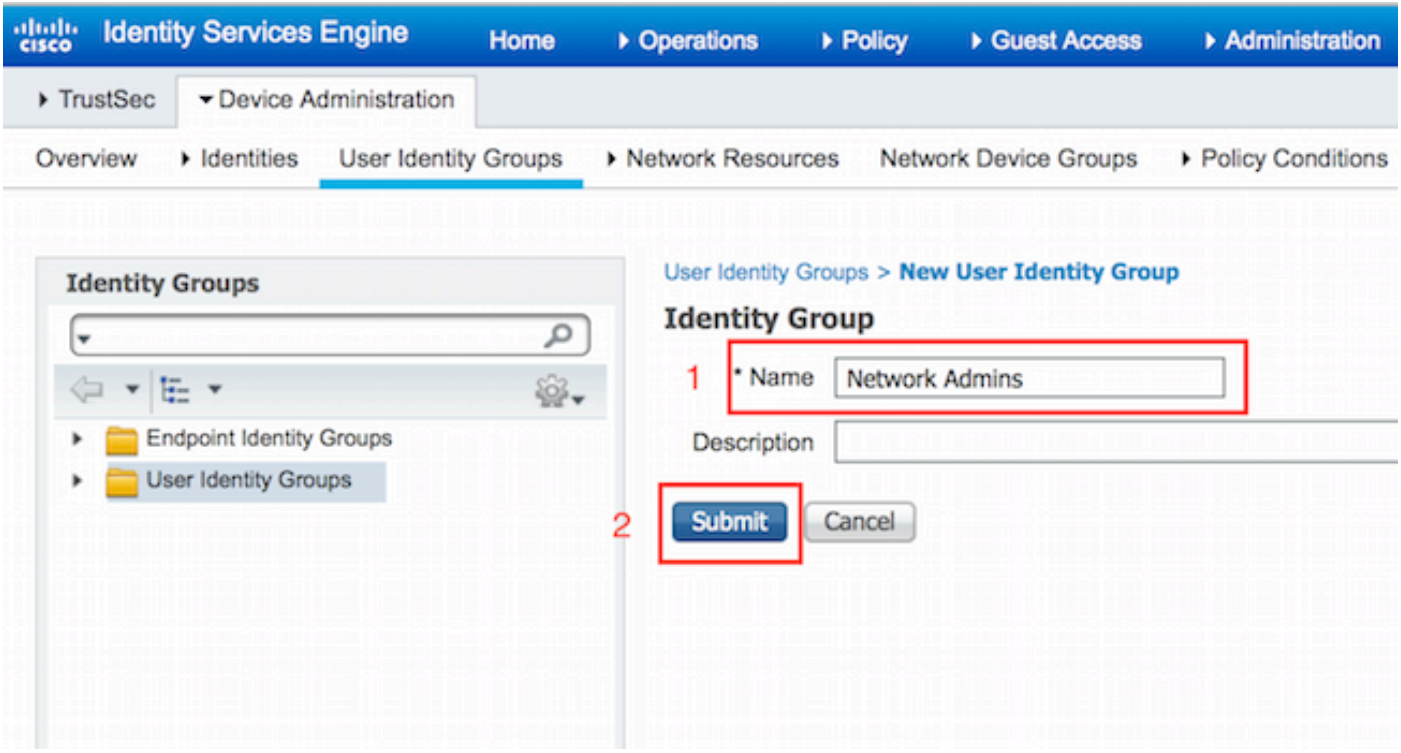
네트워크 장치 추가

Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다.**Add(**추가)를 클릭합니다.**이름, IP 주소를 입력하고 TACACS **+ 인증 설정** 확인란을 선택하고 **공유 암호** 키**를** 제공합니다.선택적으로 장치 유형/위치를 지정할 수 있습니다.



사용자 ID 그룹 구성

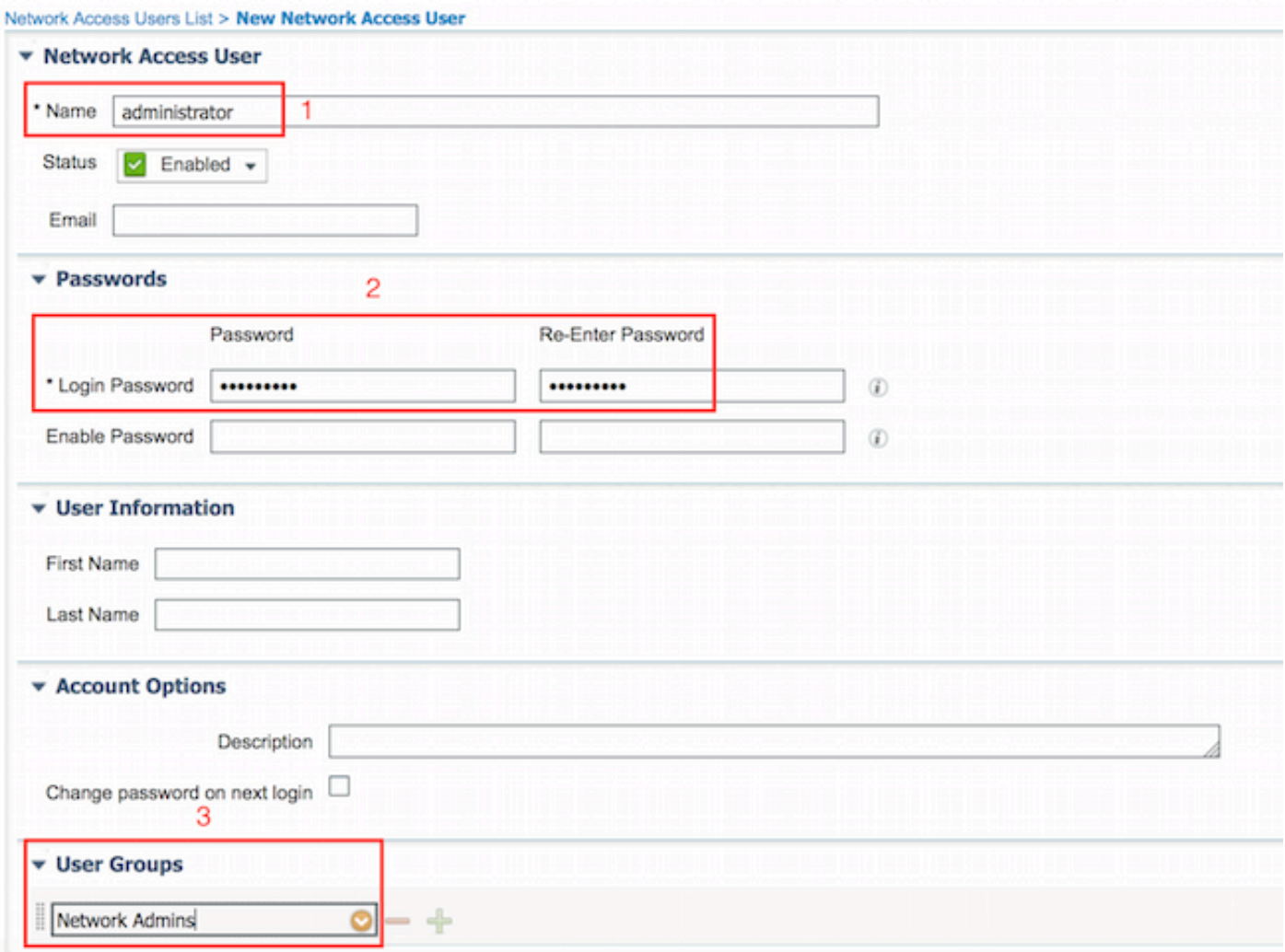
Work Centers(**작업 센터) > Device Administration(디바이스 관리) > User Identity Groups(사용자 ID 그룹)로 이동합니다.**Add(**추가)를 클릭합니다.**이름을 입력하고 제출을 **클릭합니다.**



동일한 단계를 반복하여 **네트워크 유지 관리 팀** 사용자 ID 그룹을 구성합니다.

사용자 구성

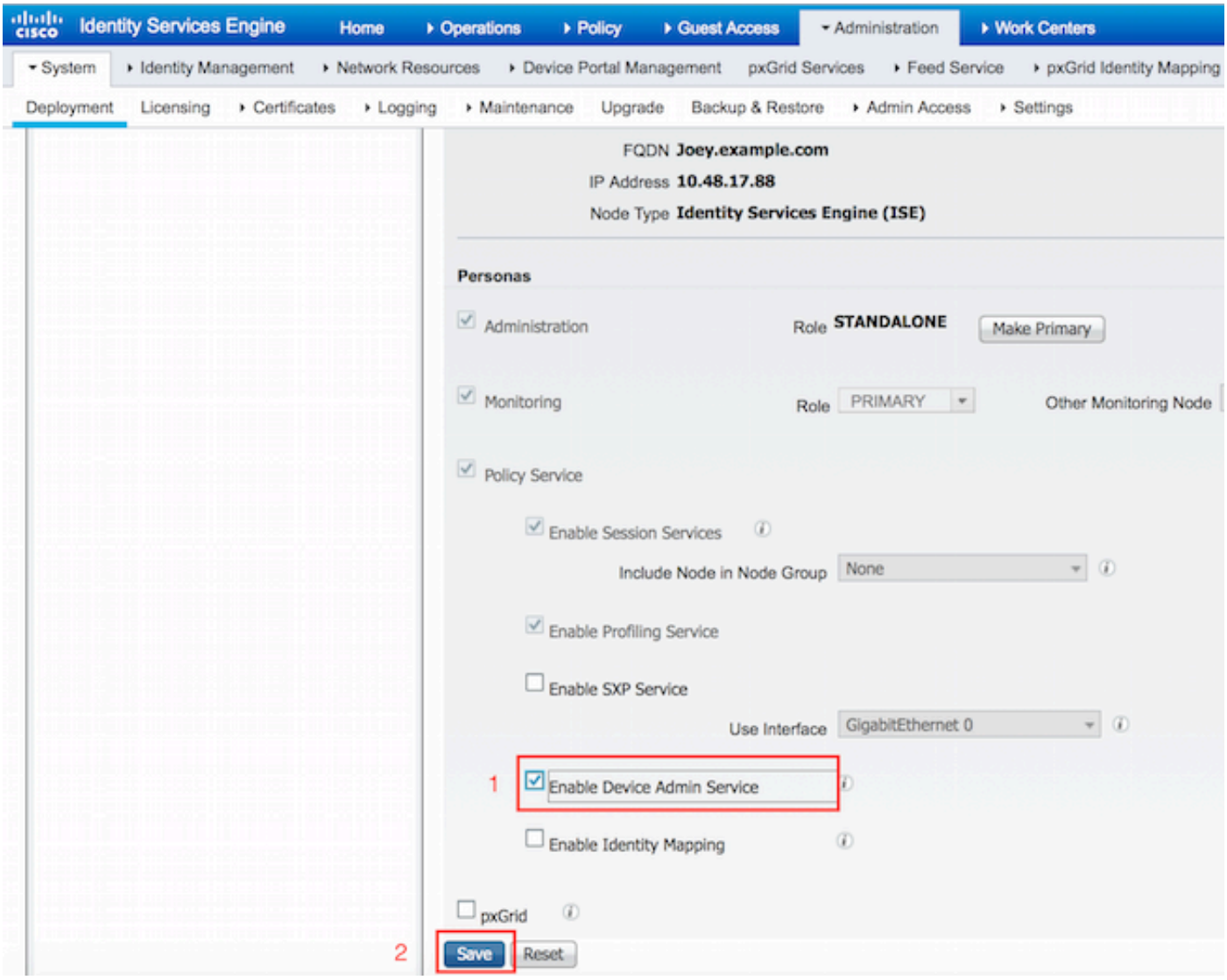
Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Identities(ID) > Users(사용자)로 이동합니다.**Add(**추가)를 클릭합니다.**이름, 로그인 비밀번호는 사용자 그룹을 지정하고 제출을 **클릭합니다**.



사용자 **사용자**를 구성하고 **네트워크 유지 관리 팀** 사용자 ID 그룹**을 할당하려면** 단계를 반복합니다 .

장치 관리 서비스 사용

Administration(관리) **> System(시스템) > Deployment(구축)로 이동합니다.**필수 노드를 선택합니다 .Enable **Device Admin Service(디바이스 관리 서비스 활성화)** 확인란을 선택하고 Save(저장)를 **클릭합니다.**

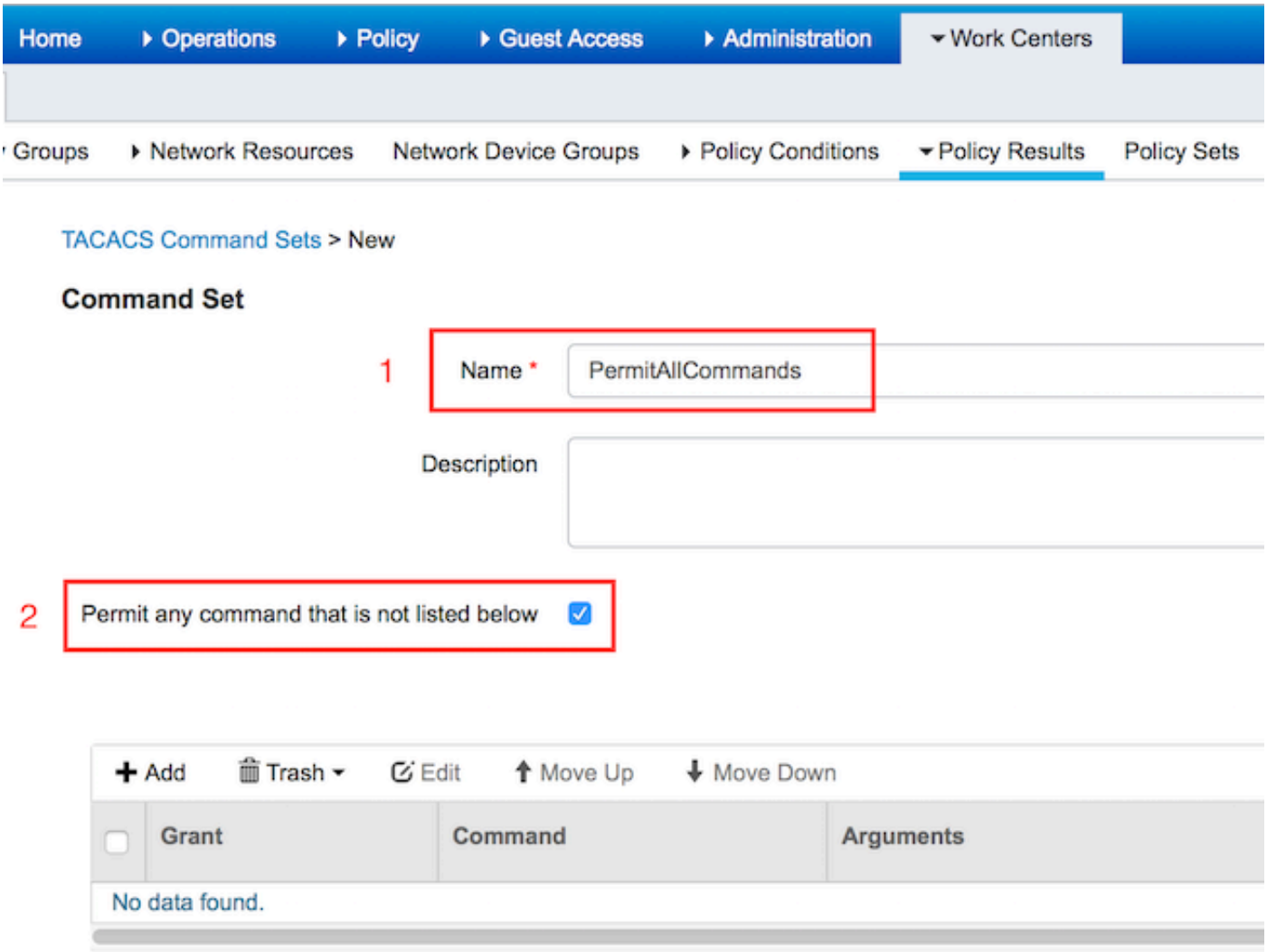


참고:TACACS의 경우 별도의 라이센스를 설치해야 합니다.

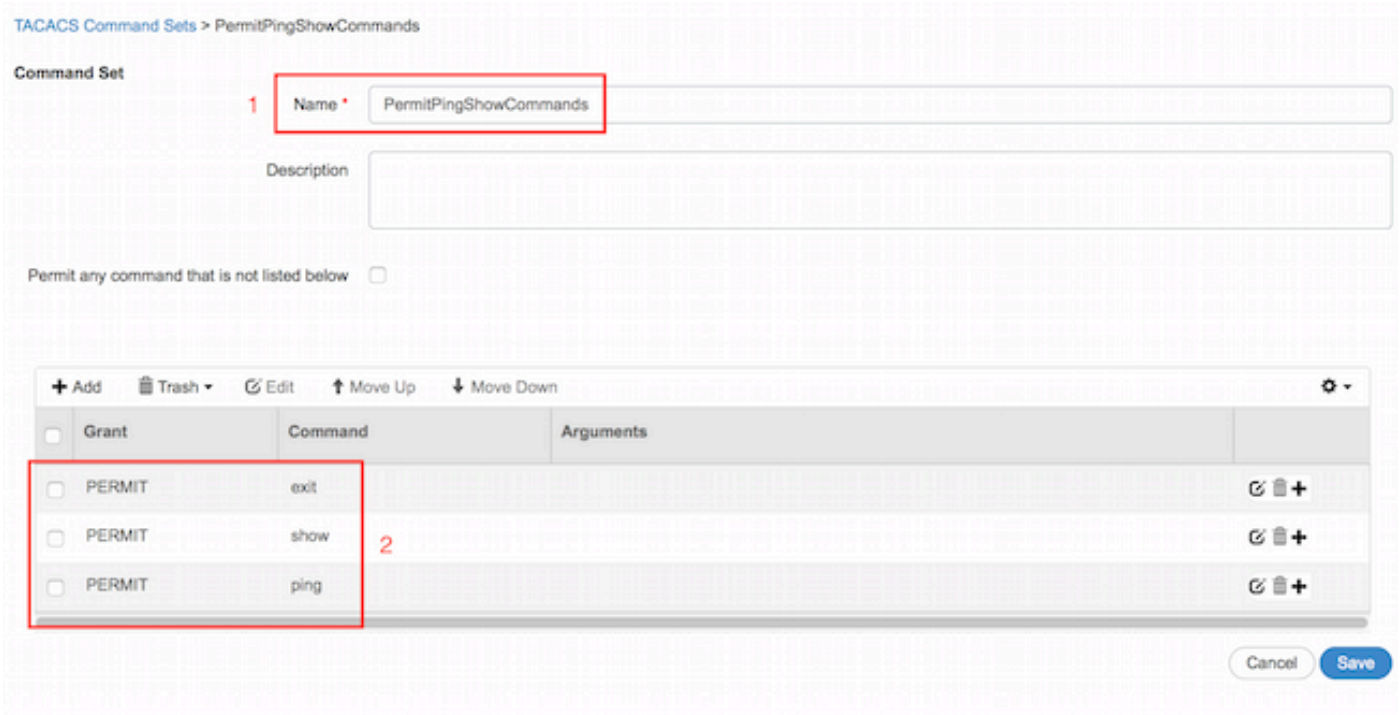
TACACS 명령 세트 구성

두 개의 명령 집합이 구성됩니다.디바이스의 모든 명령을 허용하는 관리자 사용자의 첫 번째 PermitAllCommands입니다.show **및 ping 명령만** 허용하는 사용자의 두 번째 PermitPingShowCommands입니다.

1. **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 세트)로 이동합니다.**Add(**추가)를 클릭합니다.**Name PermitAllCommands를 **제공하고 아래 목록에 없는 명령 허용** 확인란을 선택하고 **제출**을 클릭합니다.

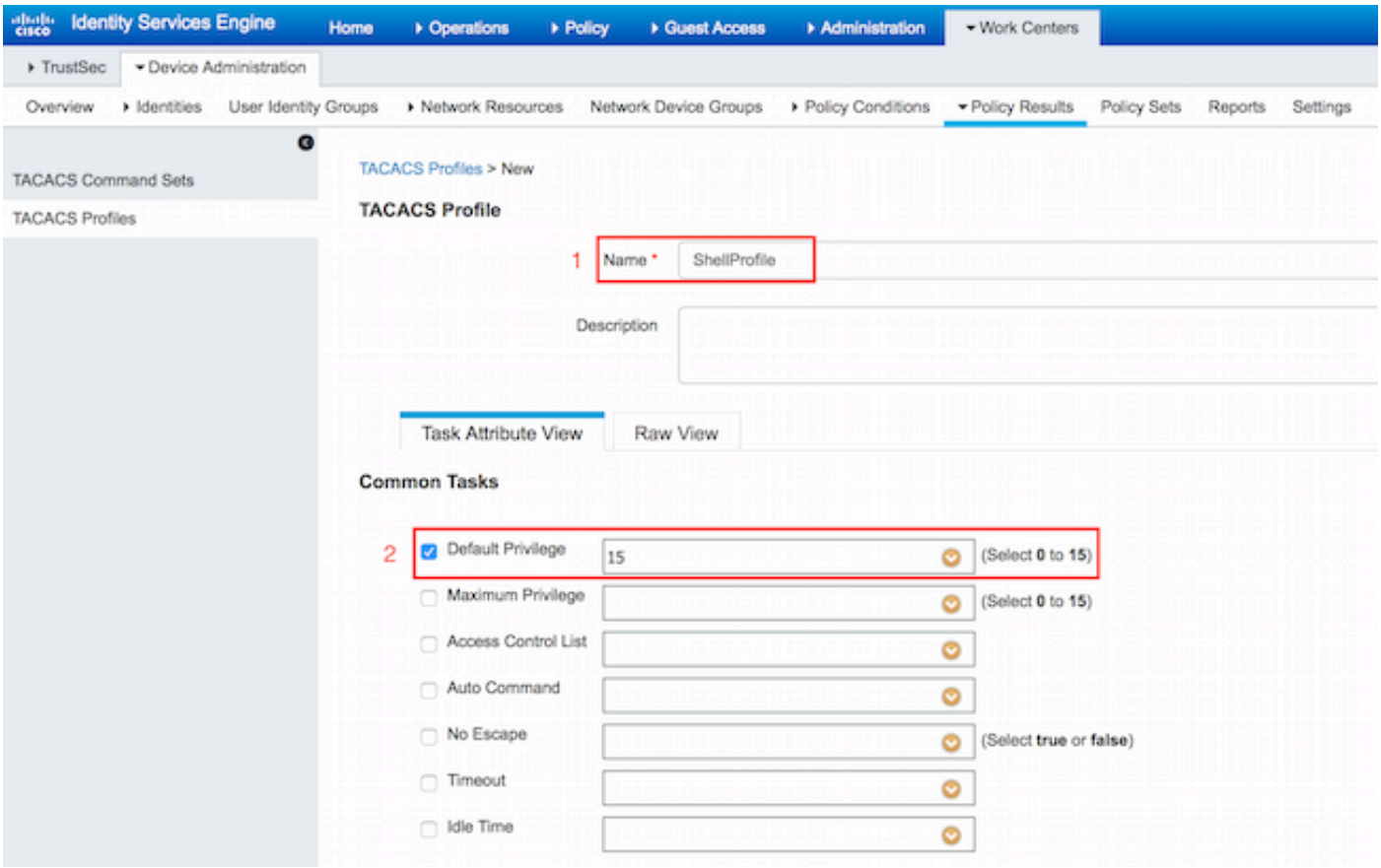


2. **작업 센터 > 디바이스 관리 > 정책 결과 > TACACS 명령 세트로 이동합니다.**Add(**추가)를 클릭합니다.**Name PermitPingShowCommands를 **제공하고 Add** and permit **show,** ping 및 exit 명령을 **클릭합니다.**기본적으로 인수가 비어 있으면 모든 인수가 포함됩니다.제출을 **클릭합니다.**



TACACS 프로파일 구성

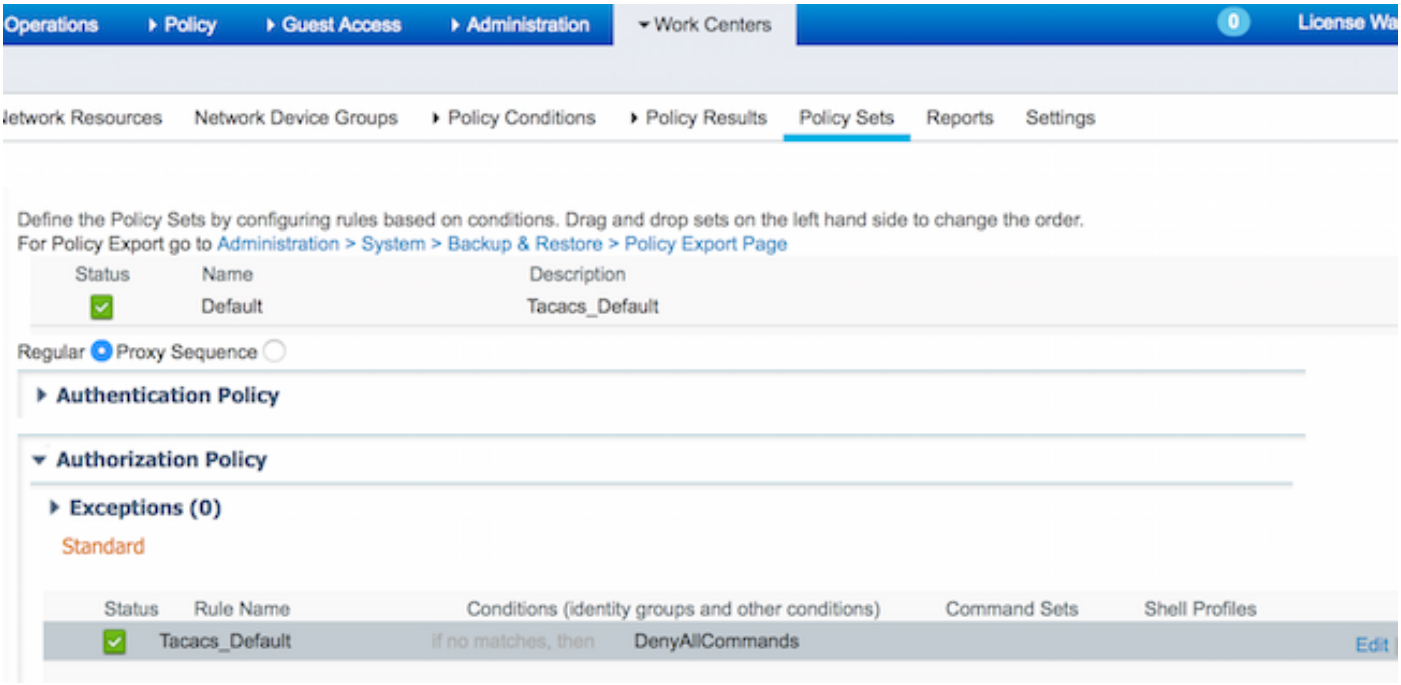
단일 TACACS 프로파일이 구성됩니다.실제 명령 시행은 명령 집합을 통해 수행됩니다.Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Profiles(TACACS 프로파일)로 이동합니다.**Add(**추가)를 클릭합니다.**Name ShellProfile**을** 제공하고 Default **Privilege** 확인란을 선택하고 값 15를 입력합니다. Submit을 **클릭합니다**.



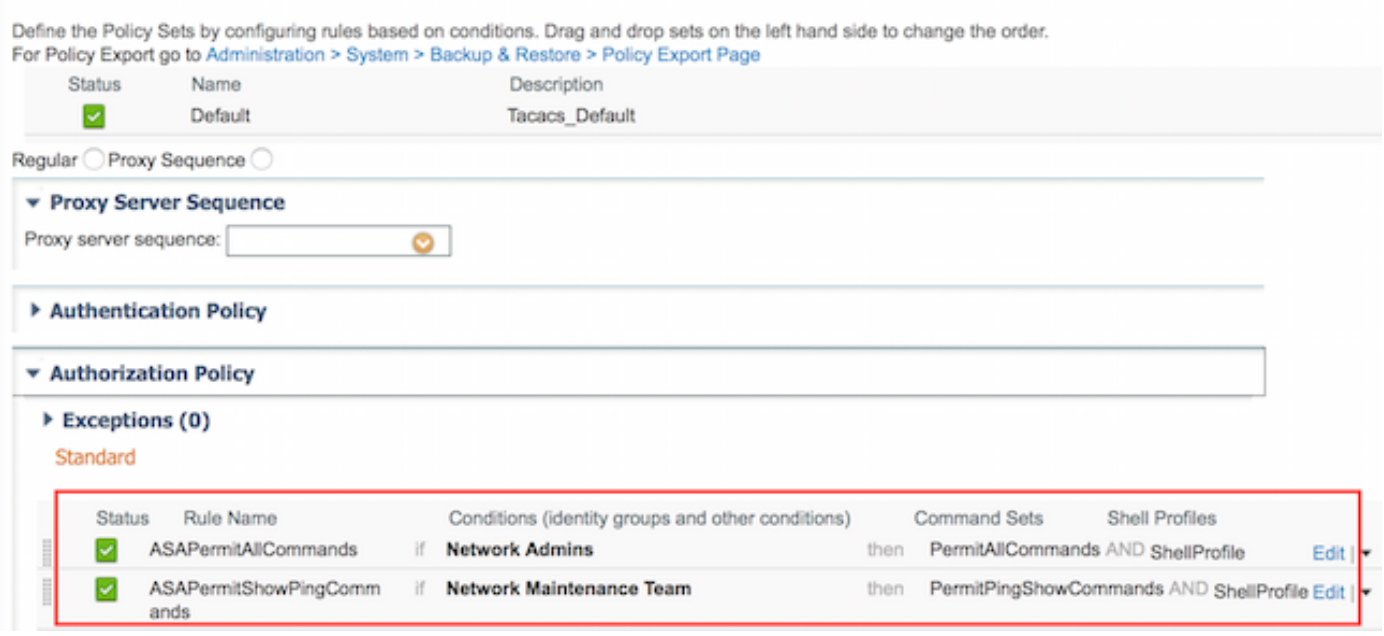
TACACS 권한 부여 정책 구성

인증 정책은 기본적으로 All_User_ID_Stores를 가리키므로 로컬 저장소도 포함되므로 변경되지 않습니다.

Work Centers(**작업 센터) > Device Administration(디바이스 관리) > Policy Sets(정책 집합) > Default(기본값) > Authorization Policy(권한 부여 정책) > Edit(편집) > Insert New Rule Above(위에 새 규칙 삽입)로 이동합니다.**



두 가지 권한 부여 규칙이 구성되며, 첫 번째 규칙은 TACACS 프로필 ShellProfile 및 **Network Admins** User Identity Group 구성원 자격을 기반으로 명령 Set **PermitAllCommands**를 할당합니다 .두 번째 규칙은 TACACS 프로필 ShellProfile 및 **네트워크 유지 관리 팀** 사용자 ID 그룹 구성원 자격을 **기반으로** 명령 Set **PermitPingShowCommands**를 할당합니다.



인증 및 권한 부여를 위해 Cisco ASA 방화벽 구성

1. 여기와 같이 username 명령을 사용하여 대체하기 위한 전체 권한을 가진 로컬 사용자를 생성합니다.

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. TACACS 서버 ISE를 정의하고 인터페이스, 프로토콜 IP 주소 및 **tacacs** 키를 지정합니다.

```
aaa-server ISE protocol tacacs+
aaa-server ISE (mgmt) host 10.48.17.88
```

```
key cisco
```

참고:서버 키는 이전에 ISE 서버에 정의된 것과 일치해야 합니다.

3. 표시된 대로 test **aaa** 명령을 사용하여 TACACS 서버 연결성을 테스트합니다.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

이전 명령의 출력에서는 TACACS 서버에 연결할 수 있으며 사용자가 성공적으로 인증되었음을 보여줍니다.

4. 아래와 같이 ssh, exec authorization 및 명령 권한 부여에 대한 인증을 구성합니다.**aaa authorization exec authentication-server auto-enable을 사용하면** 자동으로 특별 권한 EXEC 모드가 됩니다.

```
aaa authentication ssh console ISE
aaa authorization command ISE
aaa authorization exec authentication-server auto-enable
```

참고:위의 명령을 사용하여 ISE에서 인증이 수행되고 사용자가 권한 모드에 직접 배치되고 명령 권한 부여가 수행됩니다.

5. 관리 인터페이스에서 쉬를 허용합니다.

```
ssh 0.0.0.0 0.0.0.0 mgmt
```

다음을 확인합니다.

Cisco ASA 방화벽 확인

1. 전체 액세스 사용자 ID 그룹에 속하는 **관리자**로 ASA 방화벽에 SSH를 적용합니다.**Network Admins 그룹은 ISE의 ShellProfile** 및 **PermitAllCommands** 명령 집합에 매핑됩니다.모든 명령을 실행하여 전체 액세스를 보장합니다.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

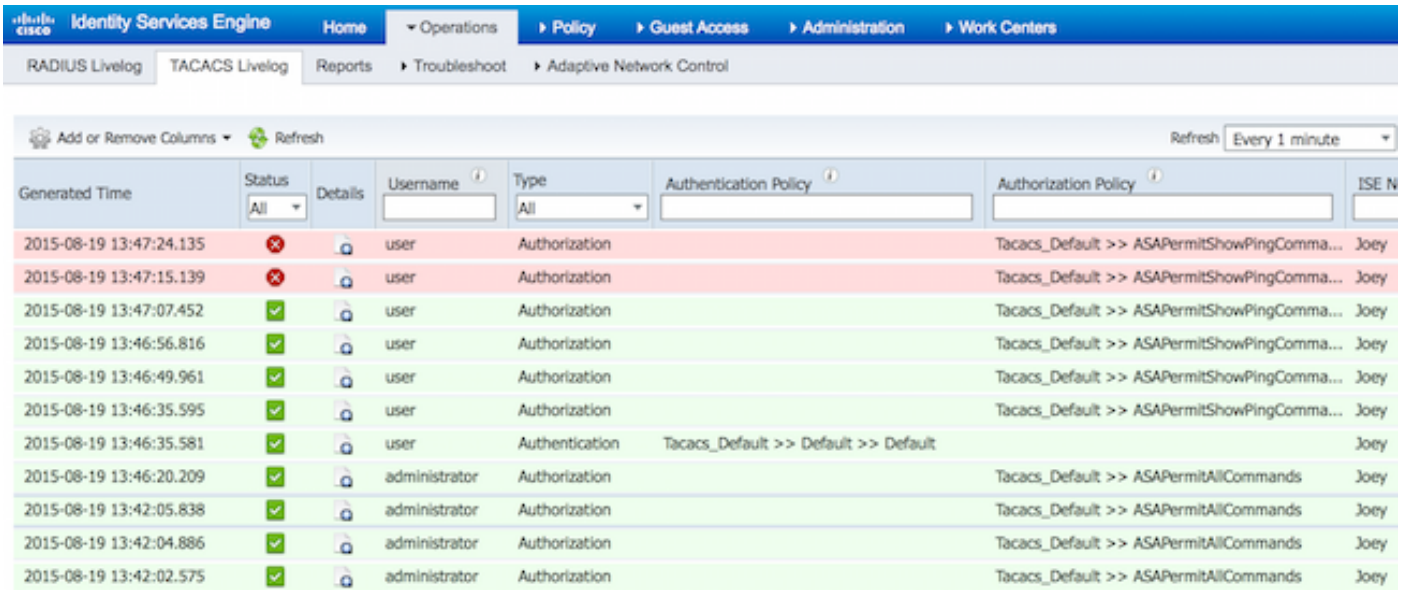
2. ASA 방화벽에 대한 SSH를 제한된 액세스 사용자 ID 그룹에 속하는 **사용자**로 설정합니다.**네트워크 유지 관리** 그룹은 **ISE**의 **ShellProfile** 및 **PermitPingShowCommands** 명령 집합에 매핑됩니다.show 및 ping 명령만 실행할 수 있도록 명령을 실행해 보십시오.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
```

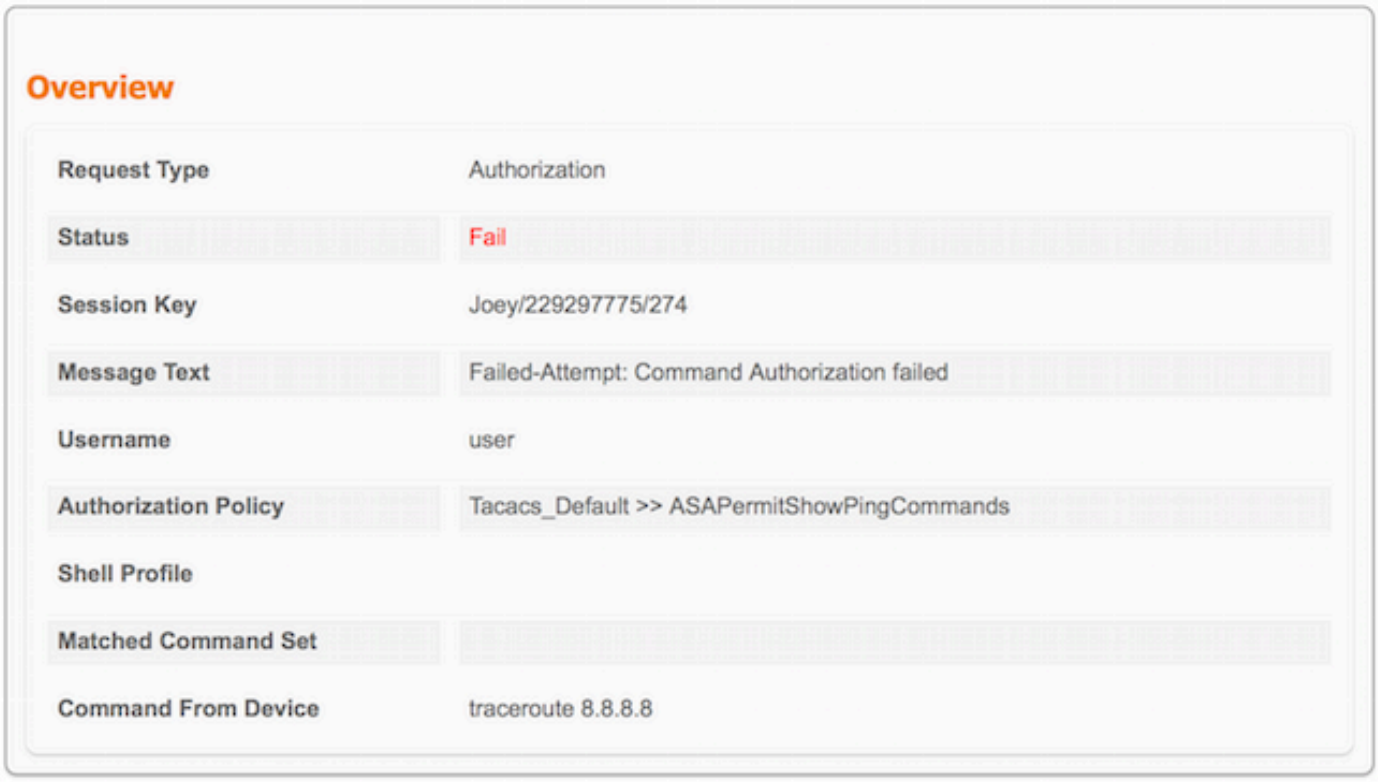
```
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

ISE 2.0 확인

1. Operations(운영) **> TACACS Livelog로 이동합니다.**위에서 수행한 시도가 표시되는지 확인합니다.



2. 앞에서 실행된 빨간색 보고서 중 하나의 세부 정보를 클릭합니다.



문제 해결

오류:실패 시도:명령 권한 부여 실패

SelectedCommandSet 특성을 검사하여 필요한 명령 집합이 권한 부여 정책에 의해 선택되었는지 확인합니다.

관련 정보

[기술 지원 및 문서 – Cisco Systems]

[ISE 2.0 릴리스 정보]

[ISE 2.0 하드웨어 설치 가이드]

[ISE 2.0 업그레이드 가이드]

[ACS에서 ISE로 마이그레이션 툴 가이드]

[ISE 2.0 Active Directory 통합 가이드]

[ISE 2.0 엔진 관리자 가이드]