

ISE 2.0 TACACS+ 인증 명령 권한 부여 구성

목차

- [소개](#)
- [배경 정보](#)
- [사전 요구 사항](#)
- [요구 사항](#)
- [사용되는 구성 요소](#)
- [구성](#)
- [네트워크 다이어그램](#)
- [설정](#)
- [인증 및 권한 부여를 위한 ISE 구성](#)
- [Active Directory에 ISE 2.0 조인](#)
- [네트워크 디바이스 추가](#)
- [장치 관리 서비스 사용](#)
- [TACACS 명령 집합 구성](#)
- [TACACS 프로파일 구성](#)
- [TACACS 권한 부여 정책 구성](#)
- [인증 및 권한 부여를 위해 Cisco IOS 라우터 구성](#)
- [다음을 확인합니다.](#)
- [Cisco IOS 라우터 확인](#)
- [ISE 2.0 확인](#)
- [문제 해결](#)
- [관련 정보](#)

소개

이 문서에서는 Microsoft AD(Active Directory) 그룹 멤버십을 기반으로 TACACS+ 인증 및 명령 권한 부여를 구성하는 방법에 대해 설명합니다.

배경 정보

ISE(Identity Service Engine) 2.0 이상을 사용하는 사용자의 Microsoft AD(Active Directory) 그룹 멤버십을 기반으로 TACACS+ 인증 및 명령 권한 부여를 구성하려면 ISE는 AD를 외부 ID 저장소로 사용하여 사용자, 머신, 그룹 및 특성과 같은 리소스를 저장합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS Router는 완벽하게 작동함

- 라우터와 ISE 간의 연결
- ISE 서버가 부트스트랩되고 Microsoft AD에 연결됨

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 2.0
- Cisco IOS[®] Software 릴리스 15.4(3)M3
- Microsoft Windows Server 2012 R2

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.

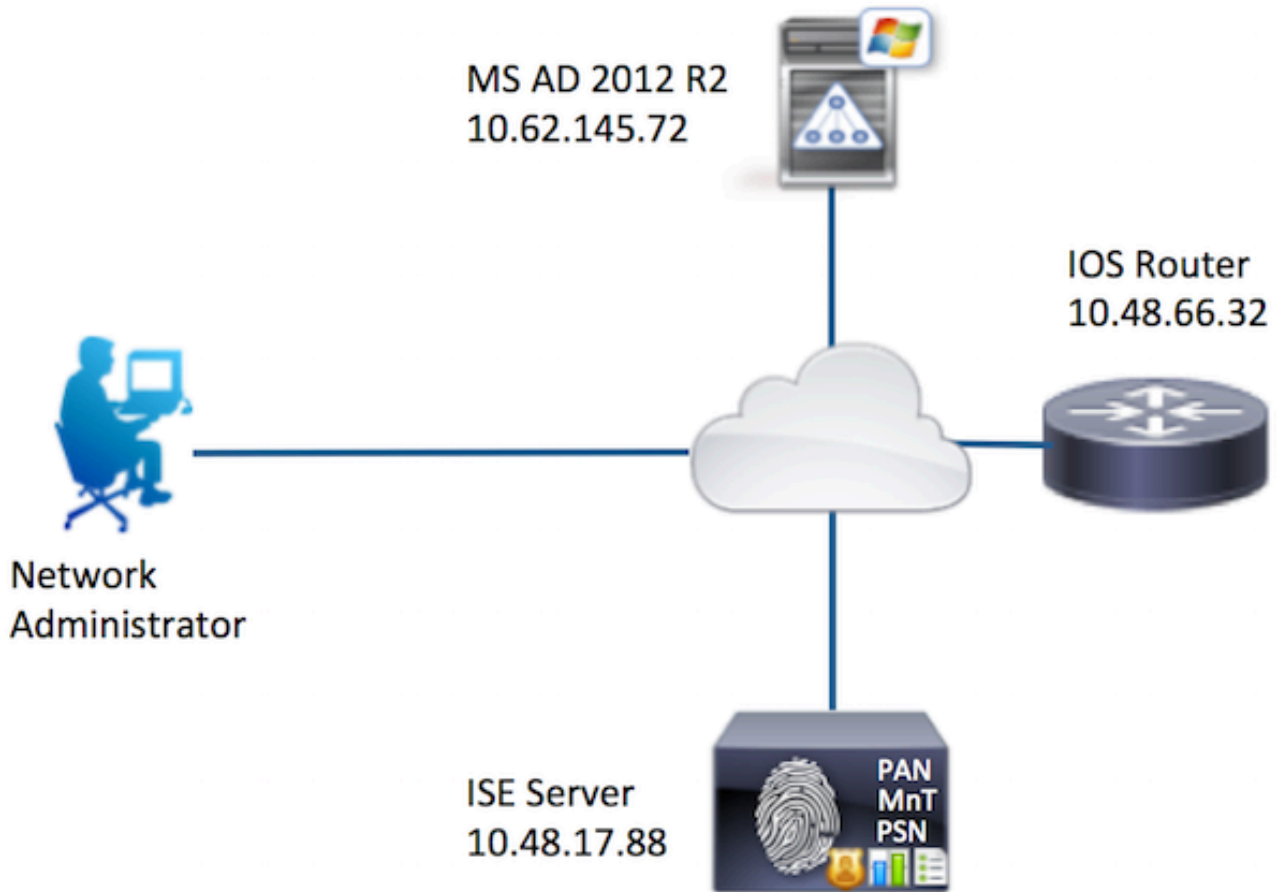
문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 포기 규칙을 참고하십시오.](#)

구성

이 구성의 목표는 다음과 같습니다.

- AD를 통해 텔넷 사용자 인증
- 로그인 후 특별 권한 EXEC 모드로 들어가도록 텔넷 사용자에게 권한 부여
- 확인을 위해 실행된 모든 명령을 확인하고 ISE에 보냅니다.

네트워크 다이어그램



설정

인증 및 권한 부여를 위한 ISE 구성

Active Directory에 ISE 2.0 조인

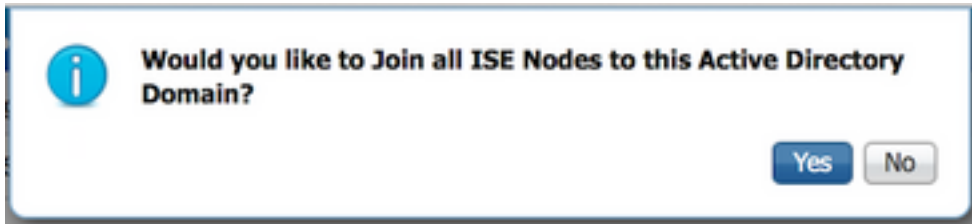
1. Administration(관리) > Identity Management(ID 관리) > External Identity Stores(외부 ID 저장소) > Active Directory > Add(추가)로 이동합니다. 가입 포인트 이름, Active Directory 도메인을 제공하고 제출을 클릭합니다.

The screenshot shows the ISE Administration console interface. The navigation menu includes: Operations, Policy, Guest Access, Administration (selected), and Work Centers. Below the menu, there are links for sources, Device Portal Management, pxGrid Services, Feed Service, and pxGrid Identity Mapping. The main content area is titled 'Identity Source Sequences' and 'Settings'. A 'Connection' tab is active, showing a form with two input fields:

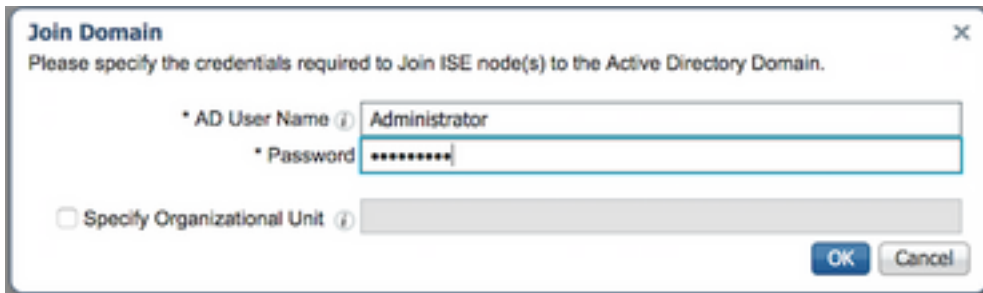
- Join Point Name:** AD
- Active Directory Domain:** example.com

At the bottom of the form, there are 'Submit' and 'Cancel' buttons.

2. 모든 ISE 노드를 이 Active Directory 도메인에 가입시키라는 메시지가 표시되면 **Yes(예)**를 클릭합니다.



3. AD 사용자 이름 및 암호를 입력하고 확인을 **클릭**합니다.

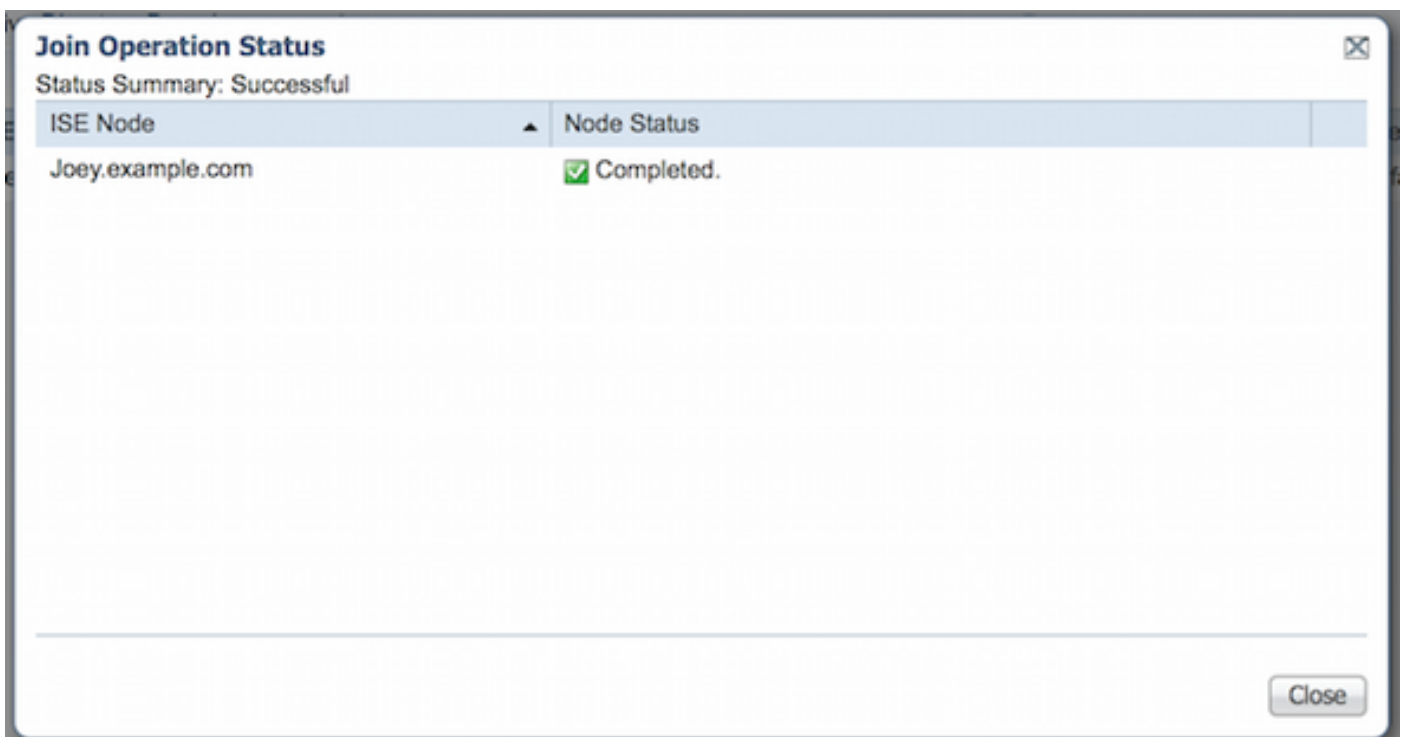


ISE에서 도메인 액세스에 필요한 AD 계정은 다음 중 하나를 가질 수 있습니다.

- 각 도메인의 도메인 사용자 권한에 워크스테이션 추가
- ISE 시스템의 계정이 ISE 시스템을 도메인에 조인하기 전에 생성된 각 컴퓨터 컨테이너에서 컴퓨터 개체 만들기 또는 컴퓨터 개체 삭제 권한

참고: Cisco에서는 ISE 계정에 대한 잠금 정책을 비활성화하고 해당 계정에 잘못된 비밀번호가 사용되는 경우 관리자에게 알림을 전송하도록 AD 인프라를 구성하는 것을 권장합니다. 잘못된 비밀번호를 입력하면 ISE는 필요한 경우 머신 계정을 생성하거나 수정하지 않으므로 모든 인증을 거부할 수 있습니다.

4. 운영 상태 검토 노드 상태는 완료로 표시되어야 합니다. 닫기를 **클릭**합니다.



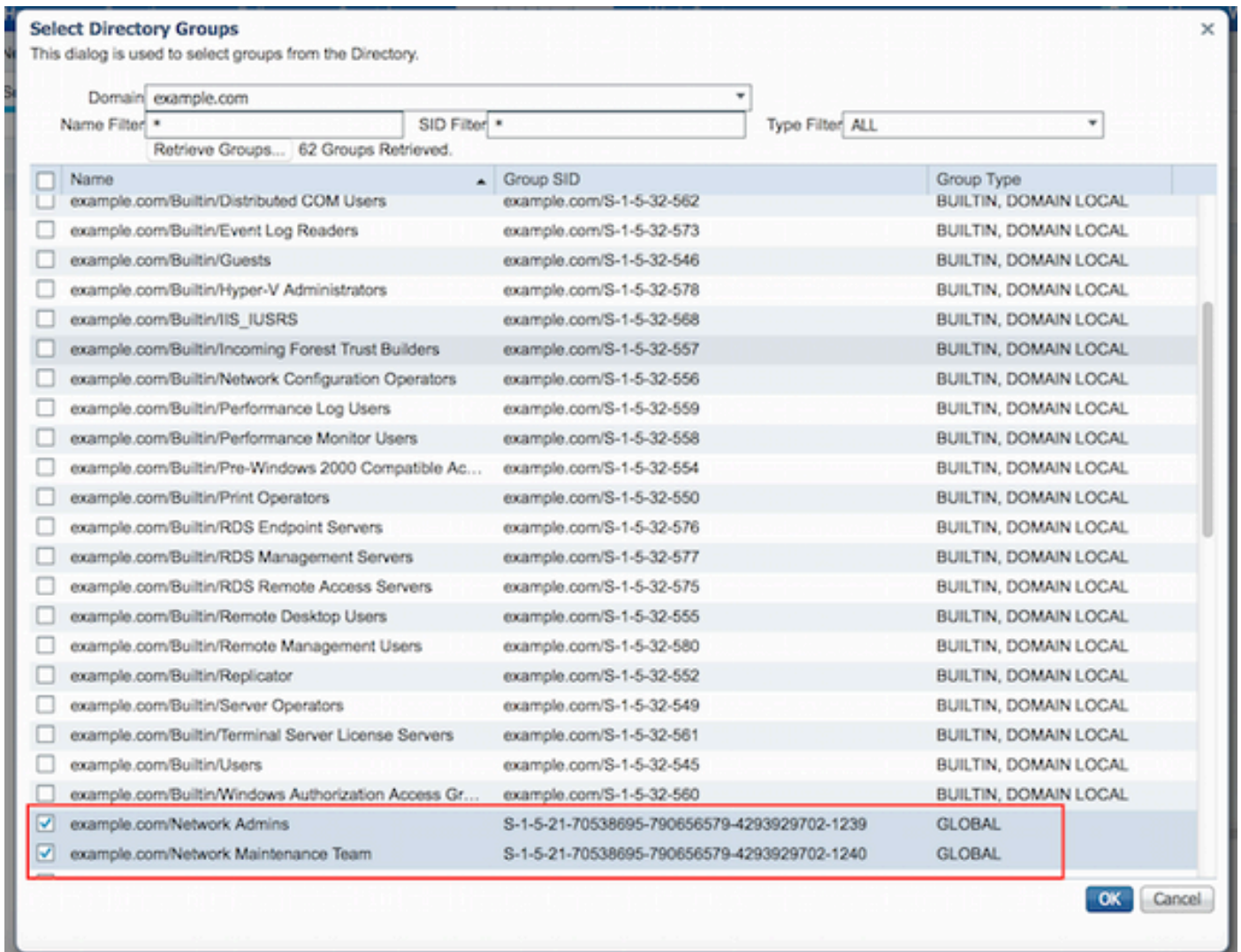
5. AD 작동 상태

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below this, there are sub-menus for 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'pxGrid Identity Source Sequences'. The main content area is titled 'Settings' and has tabs for 'Connection', 'Authentication Domains', 'Groups', and 'Attributes'. The 'Connection' tab is active, showing the configuration for an AD connection. The 'Join Point Name' is 'AD' and the 'Active Directory Domain' is 'example.com'. Below the configuration fields are buttons for 'Join', 'Leave', 'Test User', 'Diagnostic Tool', and 'Refresh Table'. A table below shows the status of the ISE nodes:

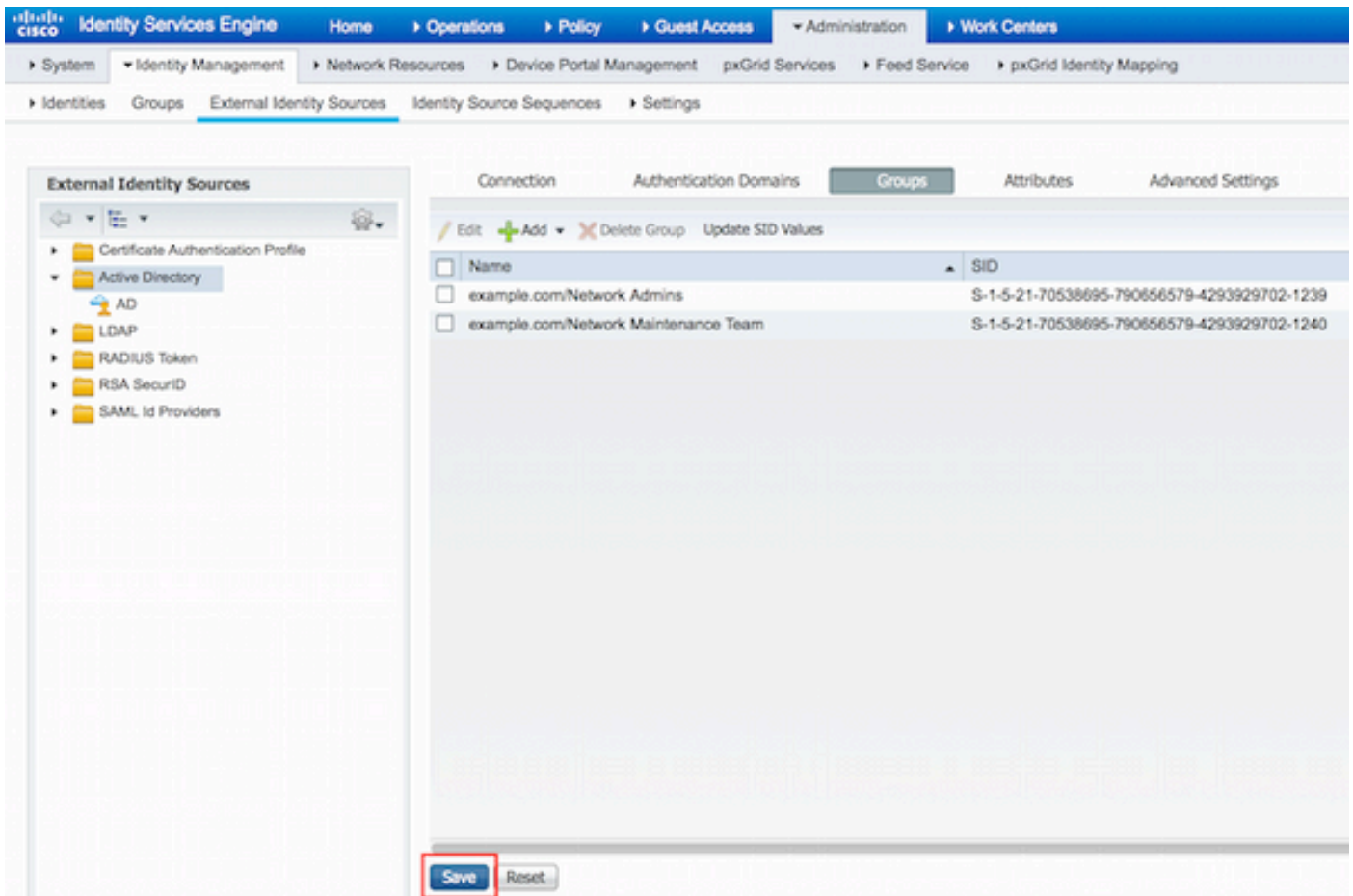
ISE Node	ISE Node Role	Status
<input type="checkbox"/> Joey.example.com	STANDALONE	<input checked="" type="checkbox"/> Operational

6. 그룹 > 추가 > 디렉토리에서 그룹 선택 > 그룹 검색으로 이동합니다. 이 이미지에 표시된 대로 **Network Admins AD Group**(네트워크 관리자 AD 그룹) 및 **Network Maintenance Team AD Group**(네트워크 유지 관리 팀 AD 그룹) 확인란을 선택합니다.

참고: 사용자 관리자가 Network Admins AD 그룹의 구성원입니다. 이 사용자는 전체 액세스 권한을 가집니다. 이 사용자는 네트워크 유지 관리 팀 AD 그룹의 구성원입니다. 이 사용자는 show 명령만 실행할 수 있습니다.

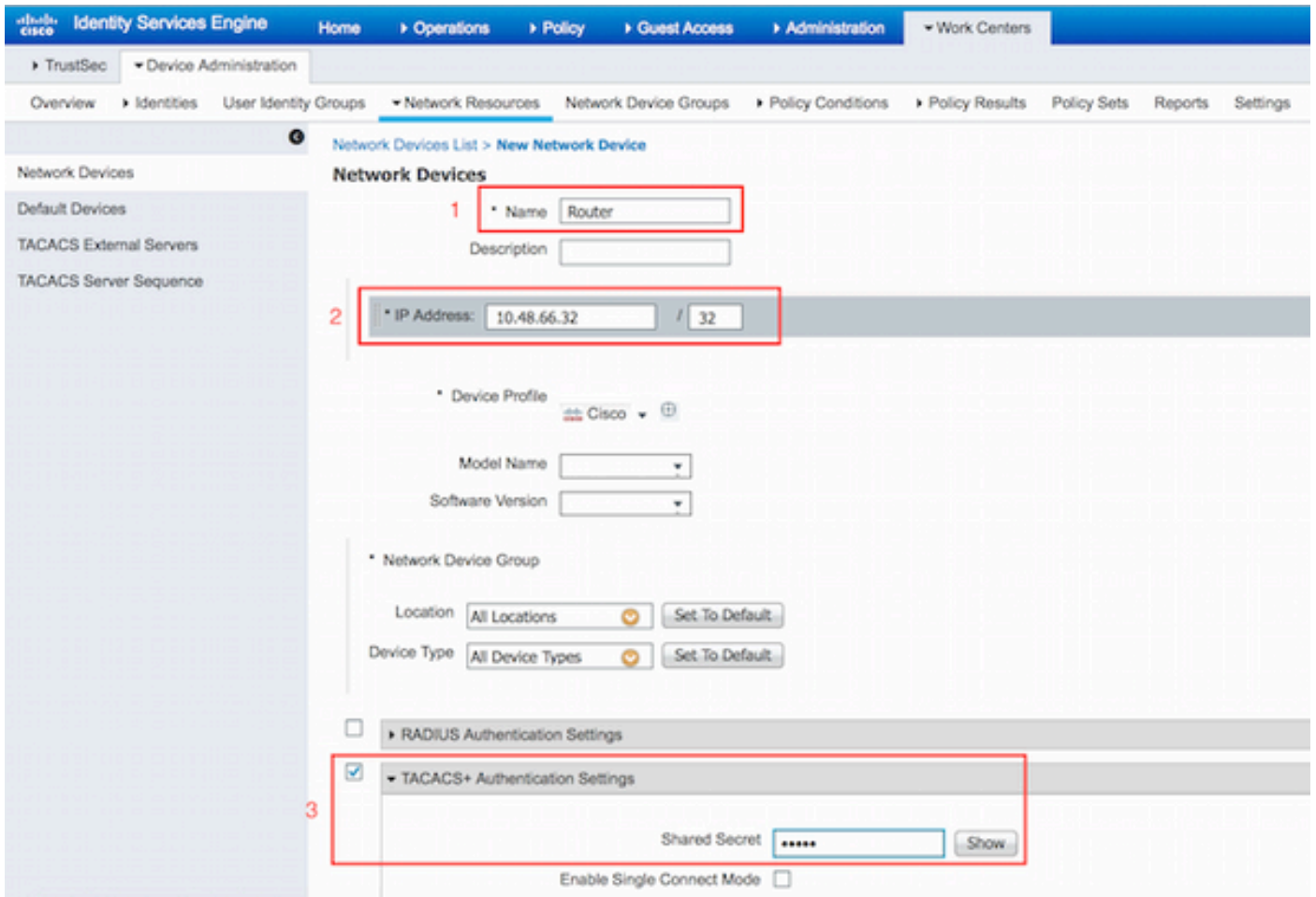


7. 저장을 눌러 검색된 AD 그룹을 저장합니다.



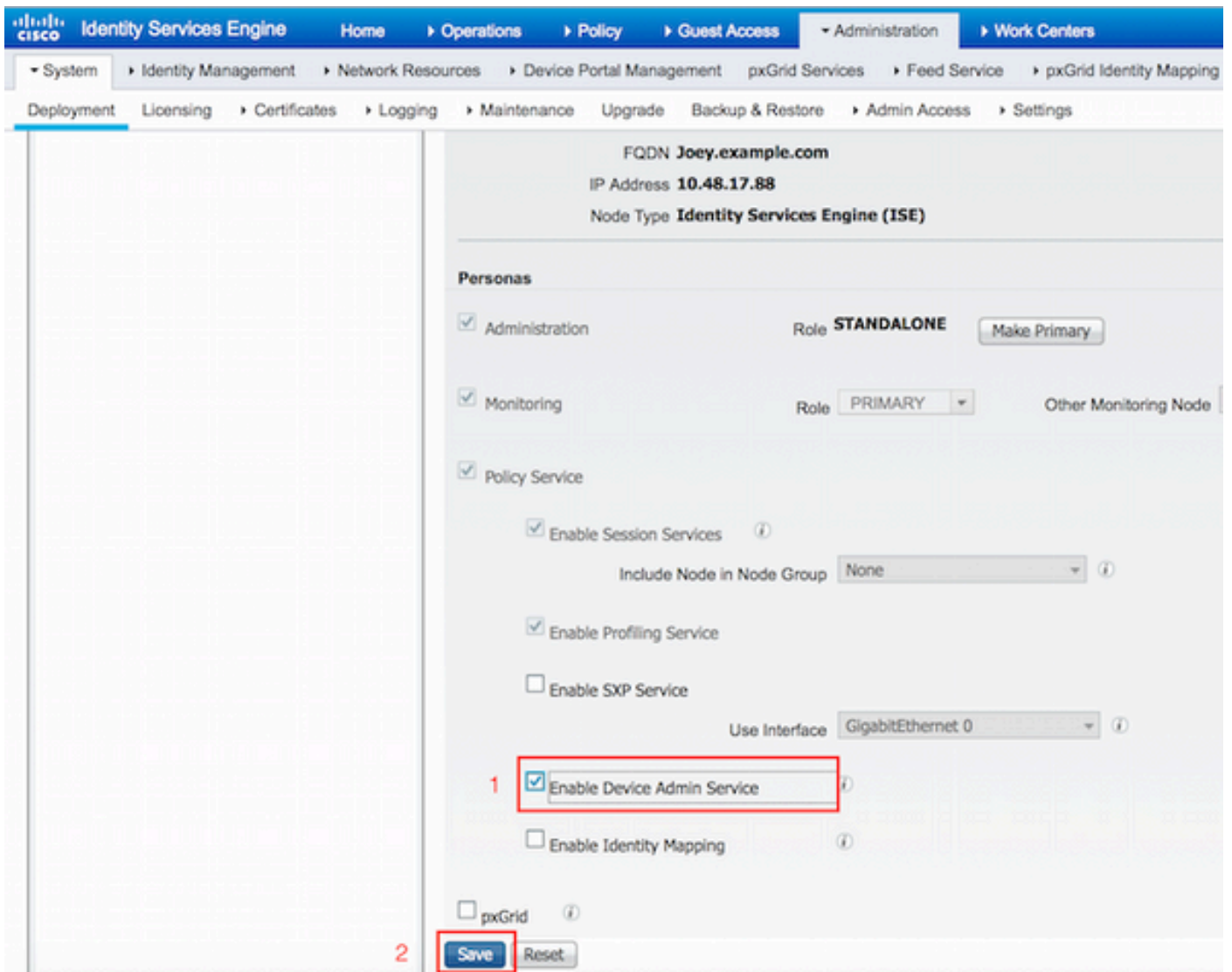
네트워크 디바이스 추가

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. Add(추가)를 클릭합니다. Name(이름), IP Address(IP 주소)를 입력하고 TACACS+ Authentication Settings(TACACS+ 인증 설정) 확인란을 선택한 다음 Shared Secret key(공유 비밀 키)를 입력합니다.



장치 관리 서비스 사용

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



참고: TACACS의 경우 별도의 라이선스를 설치해야 합니다.

TACACS 명령 집합 구성

두 개의 명령 집합이 구성됩니다. 첫 번째 **PermitAllCommands** - 사용자 admin을 위한 것으로 디바이스의 모든 명령을 허용합니다. show 명령만 허용하는 사용자 사용자를 위한 두 번째 **PermitShowCommands**.

1. **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 집합)**로 이동합니다. Add(추가)를 클릭합니다. 이름 **PermitAllCommands**를 제공하고, 나열되지 않은 모든 명령 허용 확인란을 선택하고 **Submit(제출)**을 클릭합니다.

TACACS Command Sets > New

Command Set

1

Name *

Description

2

Permit any command that is not listed below

<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

2. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Command Sets(TACACS 명령 집합)로 이동합니다. Add(추가)를 클릭합니다. Name PermitShowCommands를 입력하고 Add(추가)를 클릭한 후 permit show and exit commands(표시 및 종료 명령 허용)를 클릭합니다. 기본적으로 인수를 비워 둘 경우 모든 인수가 포함됩니다. Submit(제출)을 클릭합니다.

Home ▶ Operations ▶ Policy ▶ Guest Access ▶ Administration ▶ Work Centers

Groups ▶ Network Resources ▶ Network Device Groups ▶ Policy Conditions ▶ Policy Results ▶ Policy Sets

TACACS Command Sets > New

Command Set

1 Name * PermitShowCommands

Description

Permit any command that is not listed below

0 Selected

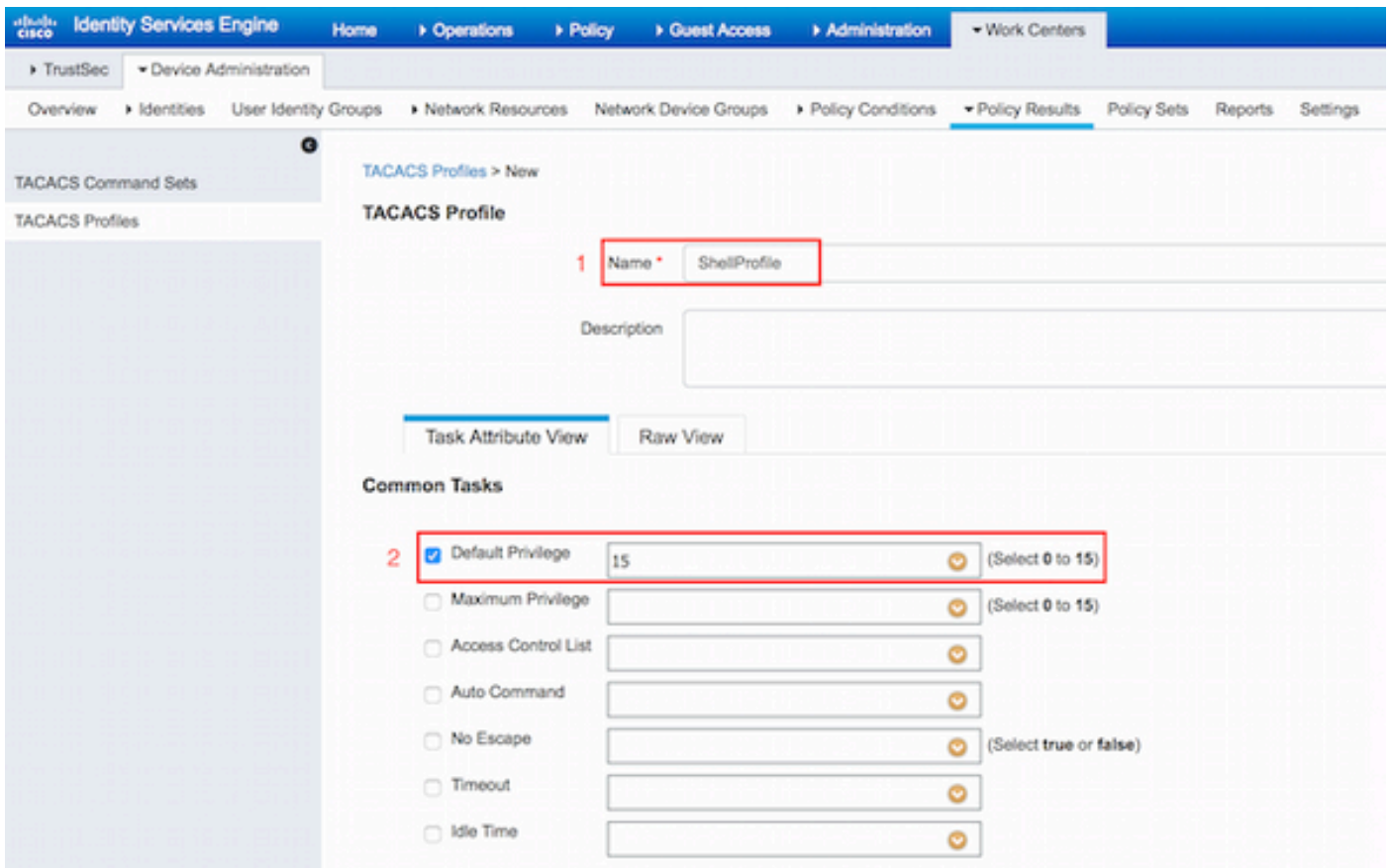
2 + Add Trash Edit Move Up Move Down

<input type="checkbox"/>	Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	show	
<input type="checkbox"/>	PERMIT	exit	

3

TACACS 프로파일 구성

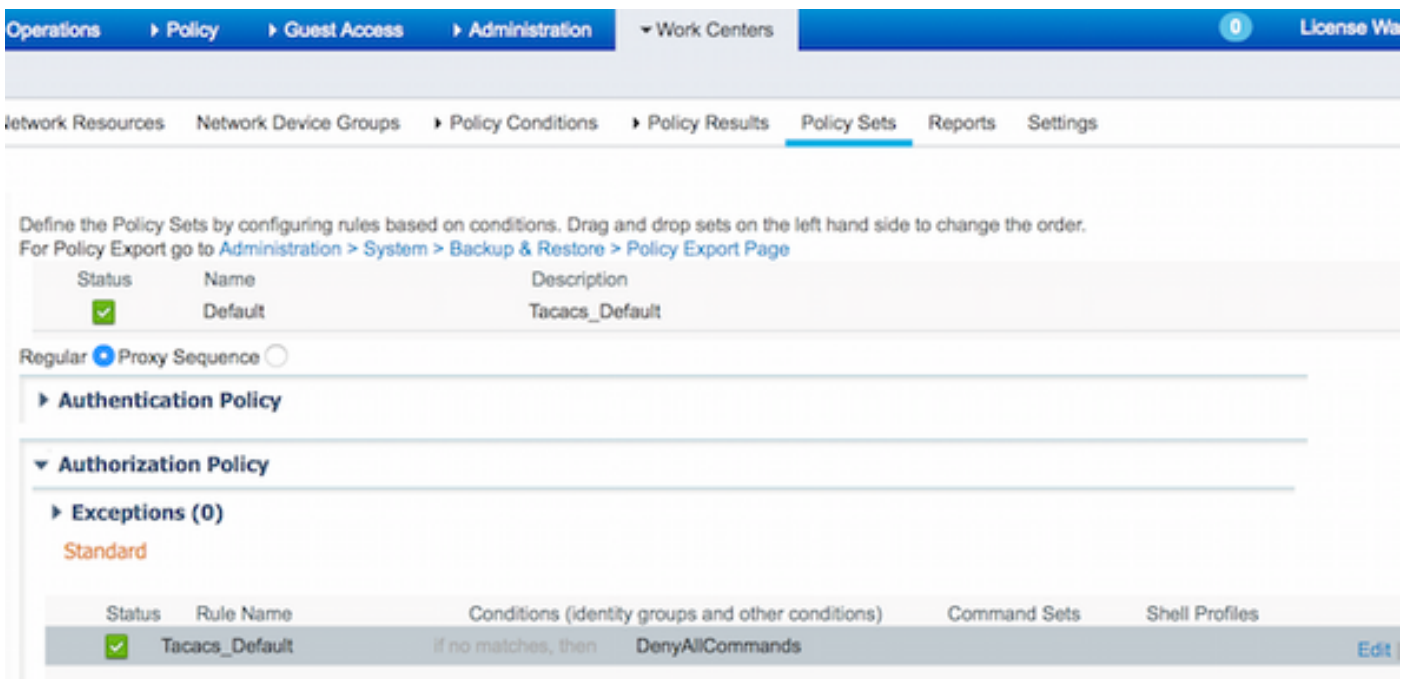
단일 TACACS 프로파일이 구성됩니다. TACACS 프로파일은 ACS의 셸 프로파일과 동일한 개념입니다. 실제 명령 적용은 명령 집합을 통해 수행됩니다. Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Results(정책 결과) > TACACS Profiles(TACACS 프로필)로 이동합니다. Add(추가)를 클릭합니다. Name ShellProfile을 제공하고 Default Privilege 확인란을 선택하고 값 15를 입력합니다. Submit을 클릭합니다.



TACACS 권한 부여 정책 구성

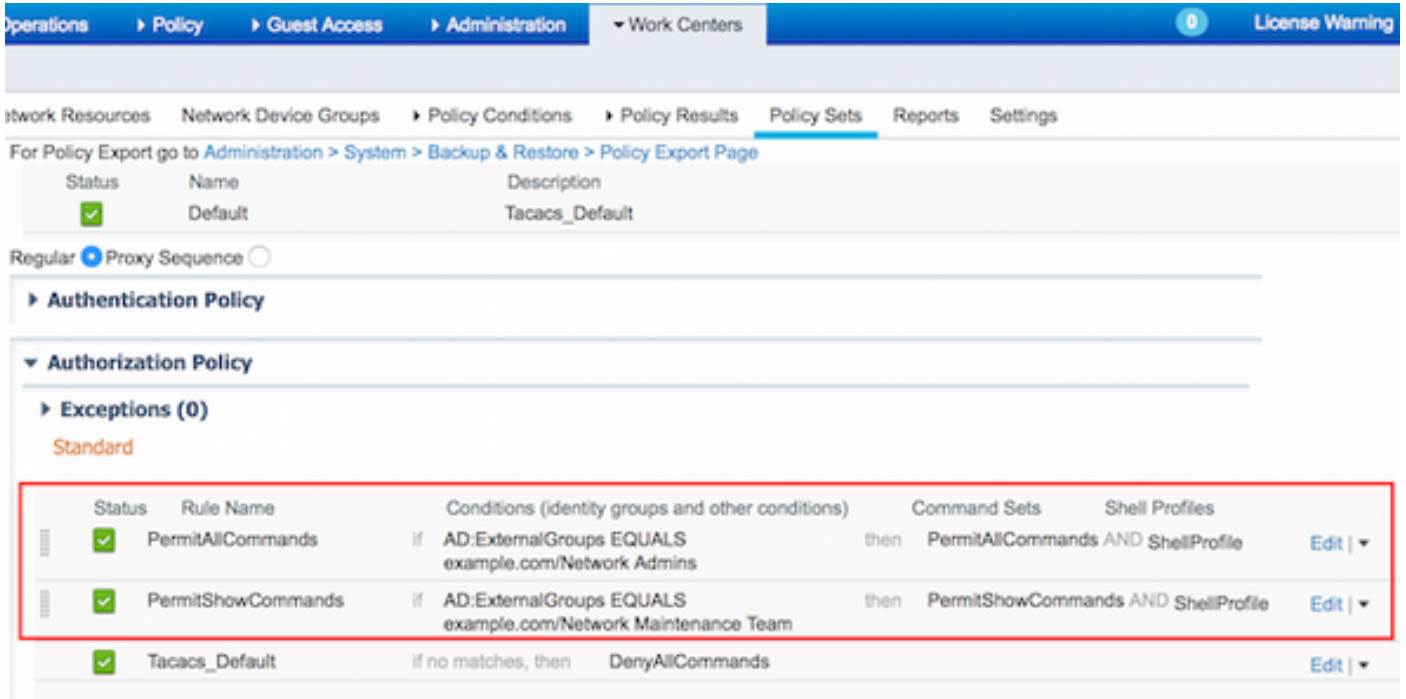
인증 정책은 기본적으로 AD를 포함하는 All_User_ID_Stores를 가리키므로 변경되지 않습니다.

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(위에서 규칙 삽입)로 이동합니다.



두 가지 권한 부여 규칙이 구성됩니다. 첫 번째 규칙은 Network Admins AD 그룹 구성원 자격을 기반으로 TACACS 프로파일 ShellProfile 및 Set PermitAllCommands 명령을 할당합니다. 두 번째 규칙

은 네트워크 유지 관리 팀 AD 그룹 멤버십을 기반으로 TACACS 프로파일 ShellProfile 및 명령 집합 PermitShowCommands를 할당합니다.



인증 및 권한 부여를 위해 Cisco IOS 라우터 구성

인증 및 권한 부여를 위해 Cisco IOS 라우터를 구성하려면 다음 단계를 완료하십시오.

1. 여기 표시된 대로 username 명령으로 풀백할 수 있는 전체 권한을 가진 로컬 사용자를 생성합니다.

```
username cisco privilege 15 password cisco
```

2. aaa 새 모델을 활성화합니다. TACACS 서버 ISE를 정의하고 그룹 ISE_GROUP에 배치합니다.

```
aaa new-model

tacacs server ISE
  address ipv4 10.48.17.88
  key cisco
aaa group server tacacs+ ISE_GROUP
  server name ISE
```

참고: 서버 키는 이전에 ISE 서버에 정의된 것과 일치합니다.

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

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

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

4. 로그인을 구성하고 인증을 활성화한 다음 표시된 대로 exec 및 명령 권한 부여를 사용합니다.

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

참고: 생성된 메서드 목록의 이름은 AAA이며, 나중에 이 목록이 행 vty에 할당될 때 사용됩니다.

5. 방법 목록을 라인 vty 0 4에 지정합니다.

```
line vty 0 4
  authorization commands 0 AAA
  authorization commands 1 AAA
  authorization commands 15 AAA
  authorization exec AAA
  login authentication AAA
```

다음을 확인합니다.

Cisco IOS 라우터 확인

1. AD의 전체 액세스 그룹에 속하는 관리자로 Cisco IOS 라우터에 텔넷 연결합니다. Network Admins 그룹은 ISE에 설정된 ShellProfile 및 PermitAllCommands 명령에 매핑된 AD의 그룹입니다. 모든 명령을 실행하여 전체 액세스를 확인합니다.

```
Username:admin
Password:
```

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

2. AD의 제한된 액세스 그룹에 속하는 사용자로 Cisco IOS 라우터에 텔넷 연결합니다. Network Maintenance Team 그룹은 ISE에서 설정된 ShellProfile 및 PermitShowCommands 명령에 매핑되는 AD의 그룹입니다. show 명령만 실행할 수 있도록 명령을 실행해 보십시오.

```
Username:user
Password:
```

```
Router#show ip interface brief | exclude unassigned
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0      10.48.66.32    YES NVRAM  up              up
```

```
Router#ping 8.8.8.8
Command authorization failed.
```

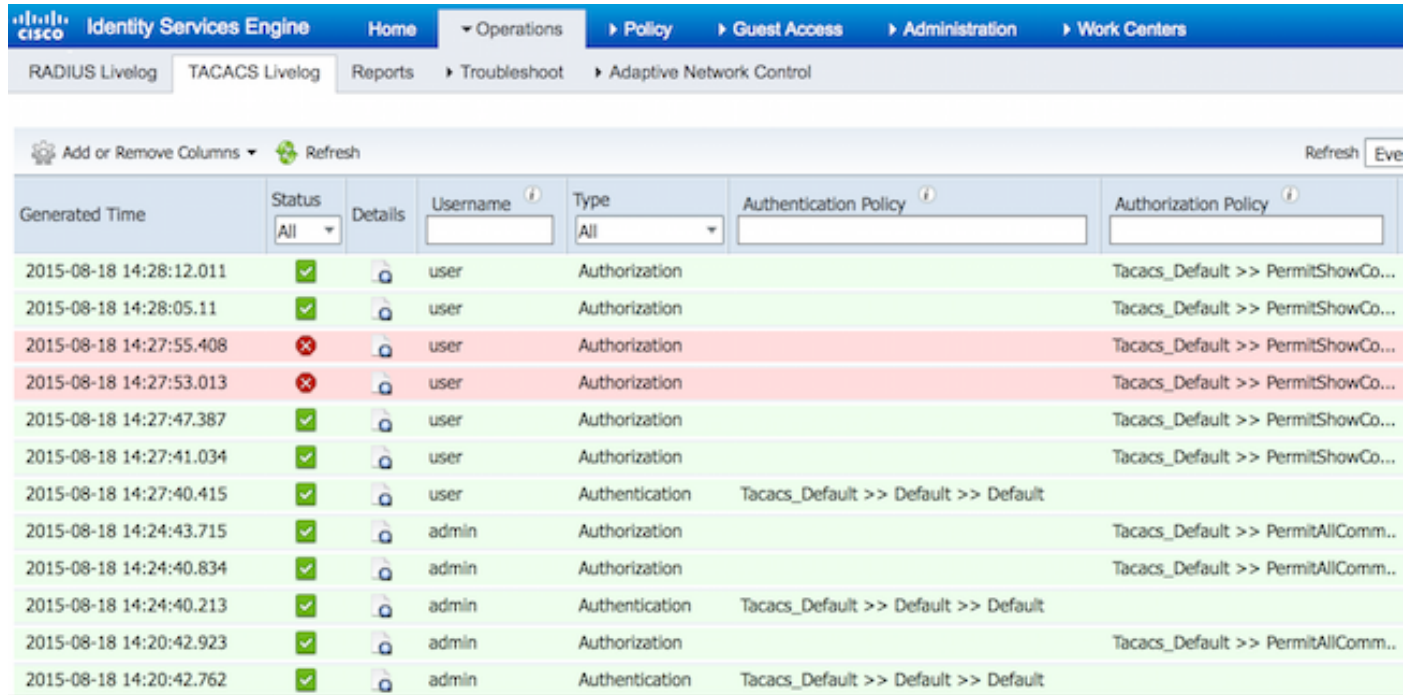
```
Router#configure terminal
Command authorization failed.
```



```
Router#show running-config | include hostname
hostname Router
Router#
```

ISE 2.0 확인

1. Operations(운영) > TACACS Livelog(TACACS 라이브 로그)로 이동합니다. 시도한 내용이 표시되는지 확인합니다.



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below this, there are tabs for 'RADIUS Livelog' and 'TACACS Livelog'. The main content area displays a table of TACACS Livelog entries. The table has columns for 'Generated Time', 'Status', 'Details', 'Username', 'Type', 'Authentication Policy', and 'Authorization Policy'. The 'Status' column contains green checkmarks for successful operations and red crosses for failed operations. The 'Username' column shows 'user' and 'admin'. The 'Type' column shows 'Authorization' and 'Authentication'. The 'Authentication Policy' and 'Authorization Policy' columns show the policy names used for each operation.

Generated Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy
2015-08-18 14:28:12.011	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:28:05.11	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:55.408	✗		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:53.013	✗		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:47.387	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:41.034	✓		user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:40.415	✓		user	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:24:43.715	✓		admin	Authorization		Tacacs_Default >> PermitAllComm...
2015-08-18 14:24:40.834	✓		admin	Authorization		Tacacs_Default >> PermitAllComm...
2015-08-18 14:24:40.213	✓		admin	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:20:42.923	✓		admin	Authorization		Tacacs_Default >> PermitAllComm...
2015-08-18 14:20:42.762	✓		admin	Authentication	Tacacs_Default >> Default >> Default	

2. 빨간색 보고서 중 하나의 상세내역을 클릭합니다. 이전에 실행된 실패한 명령을 볼 수 있습니다.

Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

문제 해결

오류: 13025 명령이 허용 규칙을 매칭하지 못했습니다.

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 ISE로의 마이그레이션 툴 가이드](#)

[ISE 2.0 Active Directory 통합 가이드](#)

[ISE 2.0 엔진 관리자 설명서](#)

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.