Cisco Identity Services Engine 2.4를 사용하여 ASR9K TACACS 구성

목차

소개

이 문서에서는 Cisco Identity Services Engine 2.4 서버에서 TACACS+를 통해 인증하고 권한을 부여하기 위한 ASR 9000 Series ASR(Aggregation Services Router)의 컨피그레이션에 대해 설명합니다.

배경 정보

Cisco IOS® XR 소프트웨어 시스템에서 사용자 액세스를 제어하기 위해 사용되는 작업 기반 권한 부여의 관리 모델을 예로 들 수 있습니다.작업 기반 권한 부여를 구현하는 데 필요한 주요 작업에는 사용자 그룹 및 작업 그룹을 구성하는 방법이 포함됩니다.사용자 그룹 및 작업 그룹은 AAA(Authentication, Authorization and Accounting) 서비스에 사용되는 Cisco IOS® XR 소프트웨어 명령 세트를 통해 구성됩니다.인증 명령은 사용자 또는 주도자의 ID를 확인하는 데 사용됩니다.권한 부여 명령은 특정 작업을 수행하기 위해 인증된 사용자(또는 주도자)에게 권한이 부여되었는지 확인하는 데 사용됩니다.어카운팅 명령은 세션 로깅 및 특정 사용자 또는 시스템에서 생성한 작업을 기록하여 감사 추적을 생성하는 데 사용됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASR 9000 구축 및 기본 구성
- TACACS+ 프로토콜
- ISE 2.4 구축 및 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASR 9000 with Cisco IOS® XR Software, 버전 5.3.4
- Cisco ISE 2.4

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성됩니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우, 모든 컨피그레이션 변경의 잠재적 영향을 완전히 파악해야 합니다.

구성

IOS® XR의 사전 정의 구성 요소

IOS® XR에는 사전 정의된 사용자 그룹 및 작업 그룹이 있습니다.관리자는 이러한 사전 정의된 그룹을 사용하거나 요구 사항에 따라 사용자 지정 그룹을 정의할 수 있습니다.

사전 정의 사용자 그룹

이러한 사용자 그룹은 IOS® XR에 미리 정의되어 있습니다.

사용자 그룹	권한
cisco 지원	기능 디버그 및 문제 해결(일반적으로 Cisco 기술 지원 담당자가 사용)
netadmin	OSPF(Open Shortest Path First)와 같은 네트워크 프로토콜을 구성합니다(일반적으로 네트 관리자가 사용).
연산자	일상적인 모니터링 작업을 수행하고 구성 권한이 제한됩니다.
루트 lr	단일 RP 내에서 모든 명령을 표시하고 실행합니다.
루트 시스템	시스템의 모든 RP에 대해 모든 명령을 표시하고 실행합니다.
sysadmin	코어 덤프가 저장되는 위치를 유지 관리하거나 NTP(Network Time Protocol) 시계를 설정하 라우터에 대한 시스템 관리 작업을 수행합니다.
서비스관리자	SBC(Session Border Controller)와 같은 서비스 관리 작업을 수행합니다.

사전 정의된 각 사용자 그룹에는 특정 작업 그룹이 매핑되어 있으므로 수정할 수 없습니다.사전 정의된 사용자 그룹을 확인하려면 다음 명령을 사용합니다.

```
RP/0/RSP0/CPU0:ASR9k#sh aaa usergroup ?

  |              Output Modifiers
 root-lr         Name of the usergroup
 netadmin        Name of the usergroup
 operator        Name of the usergroup
 sysadmin        Name of the usergroup
 retrieval       Name of the usergroup
 maintenance     Name of the usergroup
 root-system     Name of the usergroup
```

```
 provisioning   Name of the usergroup
 read-only-tg   Name of the usergroup
 serviceadmin   Name of the usergroup
 cisco-support  Name of the usergroup
 WORD           Name of the usergroup
 <cr>
```

미리 정의된 작업 그룹

관리자는 이러한 사전 정의 작업 그룹을 사용할 수 있습니다. 일반적으로 초기 컨피그레이션에 사용됩니다.

- cisco 지원:Cisco 지원 인력 작업
- netadmin:네트워크 관리자 작업
- 연산자:운영자 일상적인 작업(데모용)
- root-lr:보안 도메인 라우터 관리자 작업
- 루트 시스템:시스템 차원의 관리자 작업
- sysadmin:시스템 관리자 작업
- 서비스 관리자:서비스 관리 작업

미리 정의된 작업 그룹을 확인하려면 다음 명령을 사용합니다.

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup ?

|              Output Modifiers
root-lr        Name of the taskgroup
netadmin       Name of the taskgroup
operator       Name of the taskgroup
sysadmin       Name of the taskgroup
root-system    Name of the taskgroup
serviceadmin   Name of the taskgroup
cisco-support  Name of the taskgroup
WORD           Name of the taskgroup
<cr>
```

.

```
RP/0/RSP1/CPU0:ASR9k#show aaa task supported
```

.

aaa	ACL	관리자	안cp	ATM	기본 서비스	BCDL	BFD	bgp
부팅	번들	콜 홈	CDP	세프	CGN	cisco 지원	config-mgmt	구성 서
암호화	디그	허용 안 함	드라이버	DWDM	에임	Eigrp	이더넷 서비스	외부 액
패브릭	결함 관리자	파일 시스템	방화벽	대상	HDLC	호스트 서비스	HSRP	인터페
인벤토리	ip 서비스	IPv4	IPv6	이시스	L2vpn	리	리스프	로깅
길이	모니터	mpls ldp	mpls-static	mpls-te	멀티캐스트	Netflow	네트워크	nps
OSPF	우니	PBR	pkg-mgmt	pos dpt	PPP	Qos	rcmd	리브
립	루트 lr	루트 시스템	경로 맵	경로 정책	SBC	SNMP	소넷 sdh	정적
Sysmgr	시스템	전송	tty 액세스	터널	범용	VLAN	VPDN	vrp

이러한 각 작업은 다음 권한 중 하나 또는 네 가지 권한 모두로 지정할 수 있습니다.

읽기 읽기 작업만 허용하는 지정을 지정합니다.
쓰기 변경 작업을 허용하고 암시적으로 읽기 작업을 허용하는 지정을 지정합니다.
실행 액세스 작업을 허용하는 지정을 지정합니다.예를 들어, ping 및 telnet이 있습니다.
디버그 디버그 작업을 허용하는 지정을 지정합니다.

사용자 정의 작업 그룹

관리자는 특정 요구 사항을 충족하도록 사용자 지정 작업 그룹을 구성할 수 있습니다. 구성 예는 다음과 같습니다.

```
RP/0/RSP1/CPU0:ASR9k(config)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-tg)#task ?
  debug    Specify a debug-type task ID
  execute  Specify a execute-type task ID
  read     Specify a read-type task ID
  write    Specify a read-write-type task ID

RP/0/RSP1/CPU0:ASR9k(config-tg)#task read aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task debug aaa
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute acl
RP/0/RSP1/CPU0:ASR9k(config-tg)#commit

RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup TAC-Defined-TASK
Task group 'TAC-Defined-TASK'

Task IDs included directly by this group:
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE

Task group 'TAC-Defined-TASK' has the following combined set
  of task IDs (including all inherited groups):
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE
```

describe 명령을 사용하여 특정 명령에 필요한 작업 그룹 및 권한을 찾을 수 있습니다.

예 1.

```
RP/0/RSP1/CPU0:ASR9k#describe show aaa usergroup
Package:
.....
User needs ALL of the following taskids:

aaa (READ)
RP/0/RSP1/CPU0:ASR9k#
```

사용자가 commandshow aaa **usergroup**을 실행하도록 허용하려면 작업 그룹: **작업 읽기 aaa**를 사용자 그룹에 할당해야 합니다.

예 2.

```
RP/0/RSP1/CPU0:ASR9k(config)#describe aaa authentication login default group tacacs+
Package:
.....
User needs ALL of the following taskids:
```

```
aaa (READ WRITE)
RP/0/RSP1/CPU0:ASR9k(config)#
```

사용자가 컨피그레이션 모드에서 명령 **인증 로그인 기본 그룹 tacacs+를** 실행하도록 허용하려면 작업 그룹: **작업 읽기 쓰기 aaa**를 사용자 그룹에 할당해야 합니다.

관리자는 여러 작업 그룹을 상속할 수 있는 사용자 그룹을 정의할 수 있습니다.구성 예는 다음과 같습니다.

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:50:56.799 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'

User group 'TAC-Defined' has the following combined set
  of task IDs (including all inherited groups):
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ

RP/0/RSP1/CPU0:ASR9k#conf t
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit

RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:51:31.494 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'
  Inherits from task group 'TAC-Defined-TASK'

User group 'TAC-Defined' has the following combined set
  of task IDs (including all inherited groups):
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

라우터의 AAA 컨피그레이션

사용할 IP 주소 및 공유 암호로 ASR 라우터의 TACACS 서버를 구성합니다.

```
RP/0/RSP1/CPU0:ASR9k(config)#tacacs-server host 10.106.73.233 port 49
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#key 0 cisco
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#commit

!
tacacs-server host 10.127.196.160 port 49
key 7 14141B180F0B
!
```

구성된 TACACS 서버를 사용하도록 인증 및 권한 부여를 구성합니다.

```
#aaa authentication login default group tacacs+ local
#aaa authorization exec default group tacacs+ local
```

구성된 TACACS 서버를 사용하도록 명령 권한 부여를 구성합니다(선택 사항).

> **참고:**인증 및 권한 부여가 예상대로 작동하는지 확인하고 명령 권한 부여를 활성화하기 전에 명령 집합도 올바르게 구성되었는지 확인합니다.제대로 구성되지 않은 경우 사용자가 디바이스에 명령을 입력할 수 없을 수 있습니다.

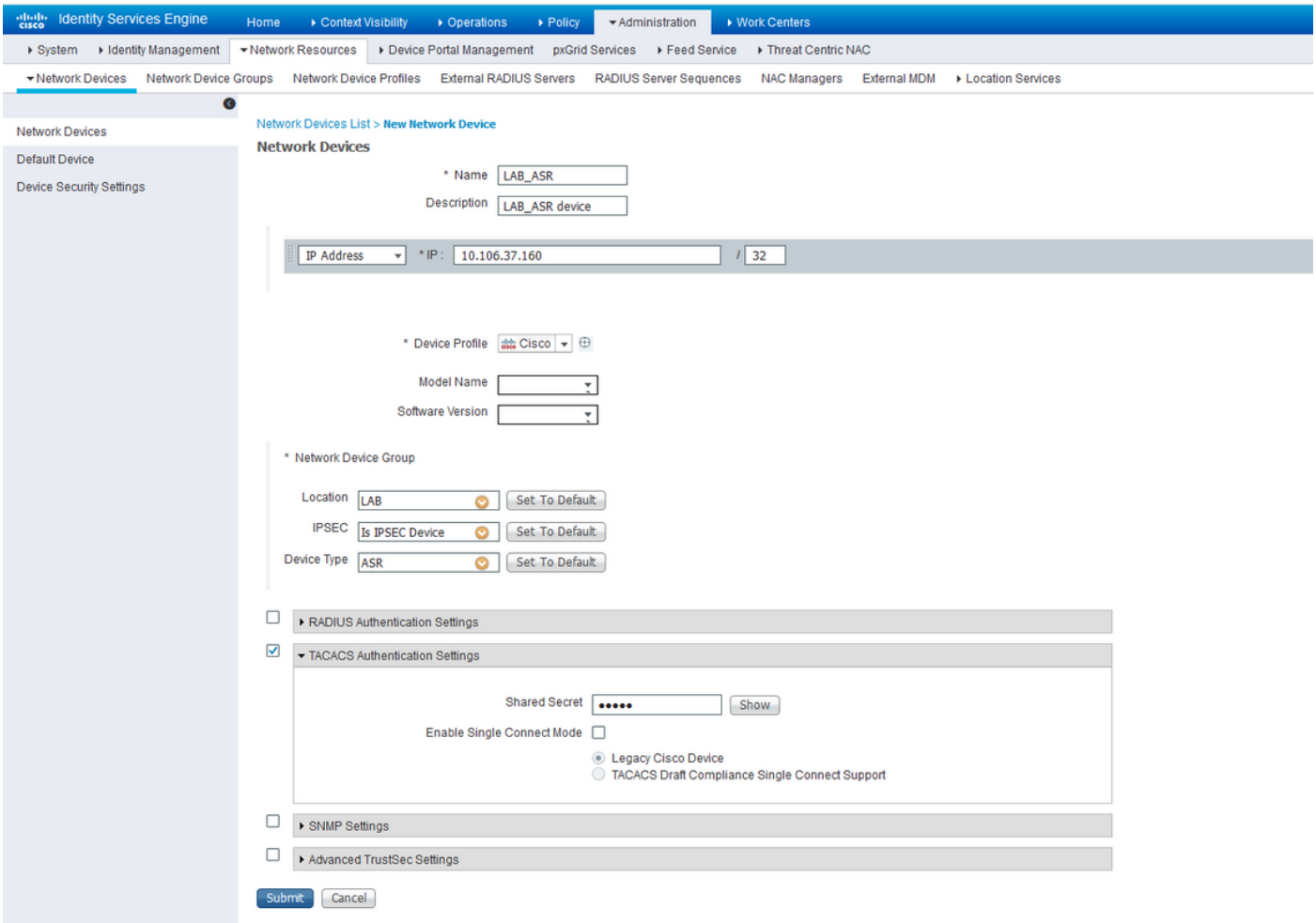
```
#aaa authorization commands default group tacacs+
```

구성된 TACACS 서버를 사용하도록 명령 어카운팅을 구성합니다(선택 사항).

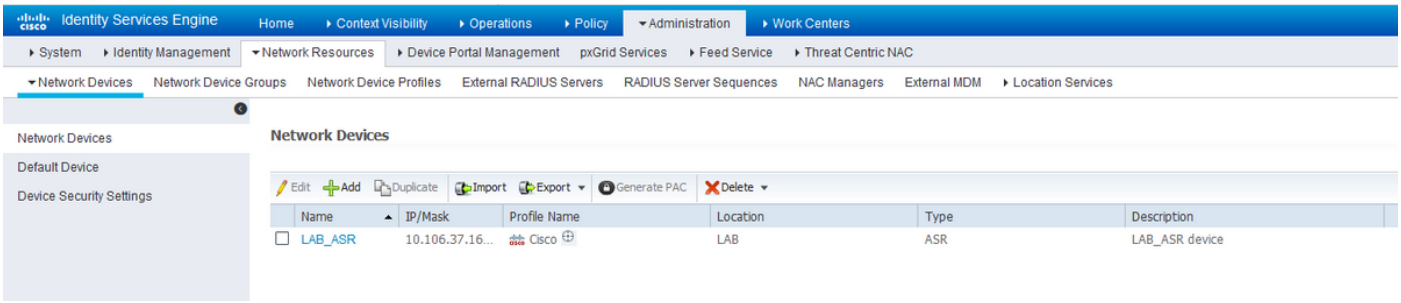
```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

ISE 서버 컨피그레이션

1단계. ISE 서버의 AAA 클라이언트 목록에서 라우터 IP를 정의하려면 **Administration > N으로** 이동합니다.**네트워크 리소스 > 네트워크 디바이스** 이미지에 표시된 것과 같습니다. 공유 암호는 이미지에 표시된 것과 같이 ASR 라우터에 구성된 것과 동일해야 합니다.



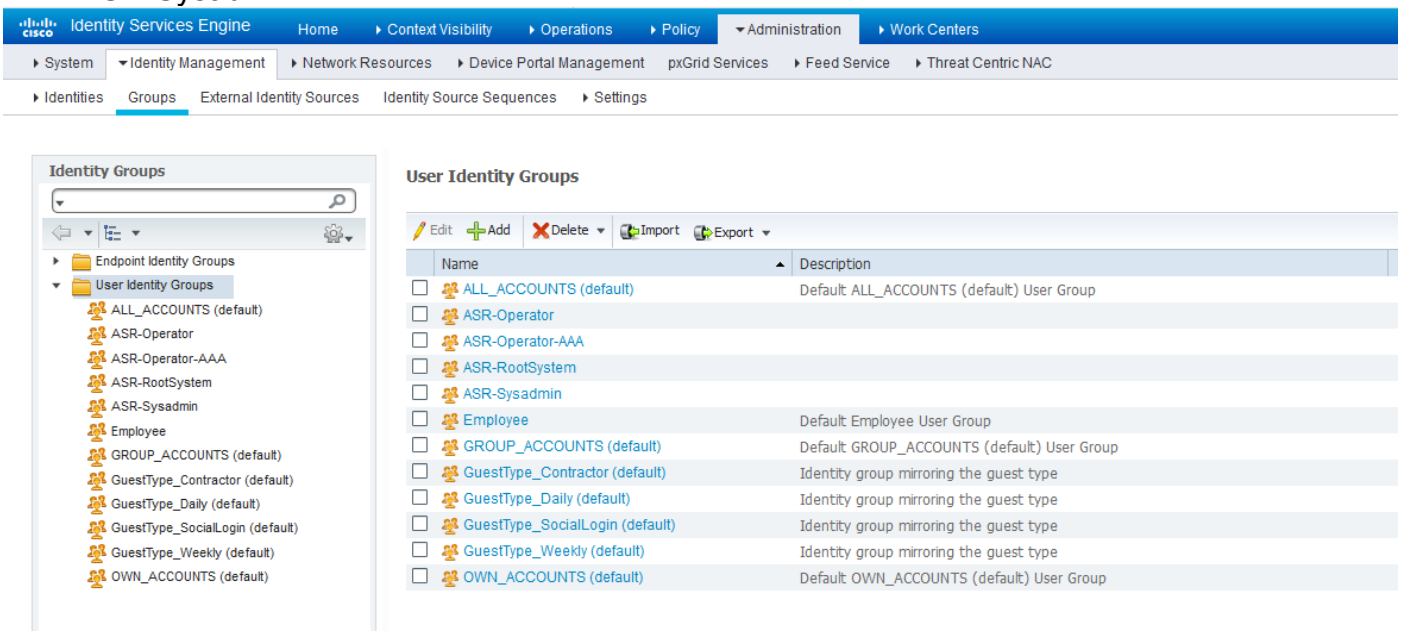
네트워크 디바이스 컨피그레이션



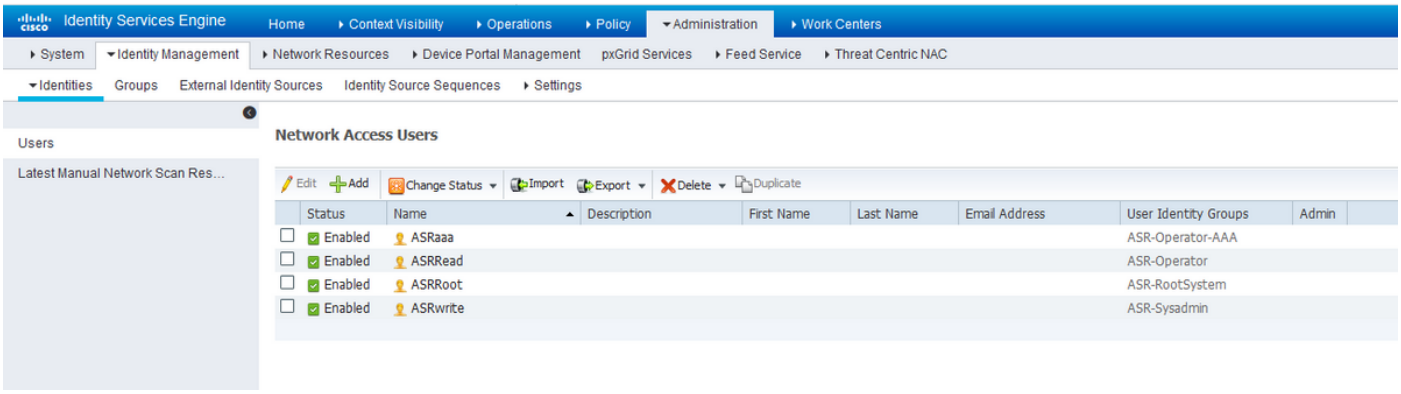
네트워크 디바이스 컨피그레이션

2단계. 사용자 그룹을 요구 사항에 따라 정의합니다. 예를 들어, 이 이미지에 표시된 것처럼 네 개의 그룹을 사용합니다.Administration(관리) > Identity **Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹)** 아래에서 그룹을 정의할 수 있습니다.이 예에서 생성된 그룹은 다음과 같습니다.

1. ASR 운영자
2. ASR-운영자-AAA
3. ASR 루트 시스템
4. ASR-Sysadmin



ID 그룹3단계. 이미지에 표시된 대로 사용자를 생성하고 이전에 생성한 각 사용자 그룹에 매핑합니다.



ID/사용자

참고:이 예에서는 ISE 내부 사용자가 인증 및 권한 부여에 사용됩니다.외부 ID 소스를 사용한 인증 및 권한 부여는 이 문서의 범위를 벗어납니다.

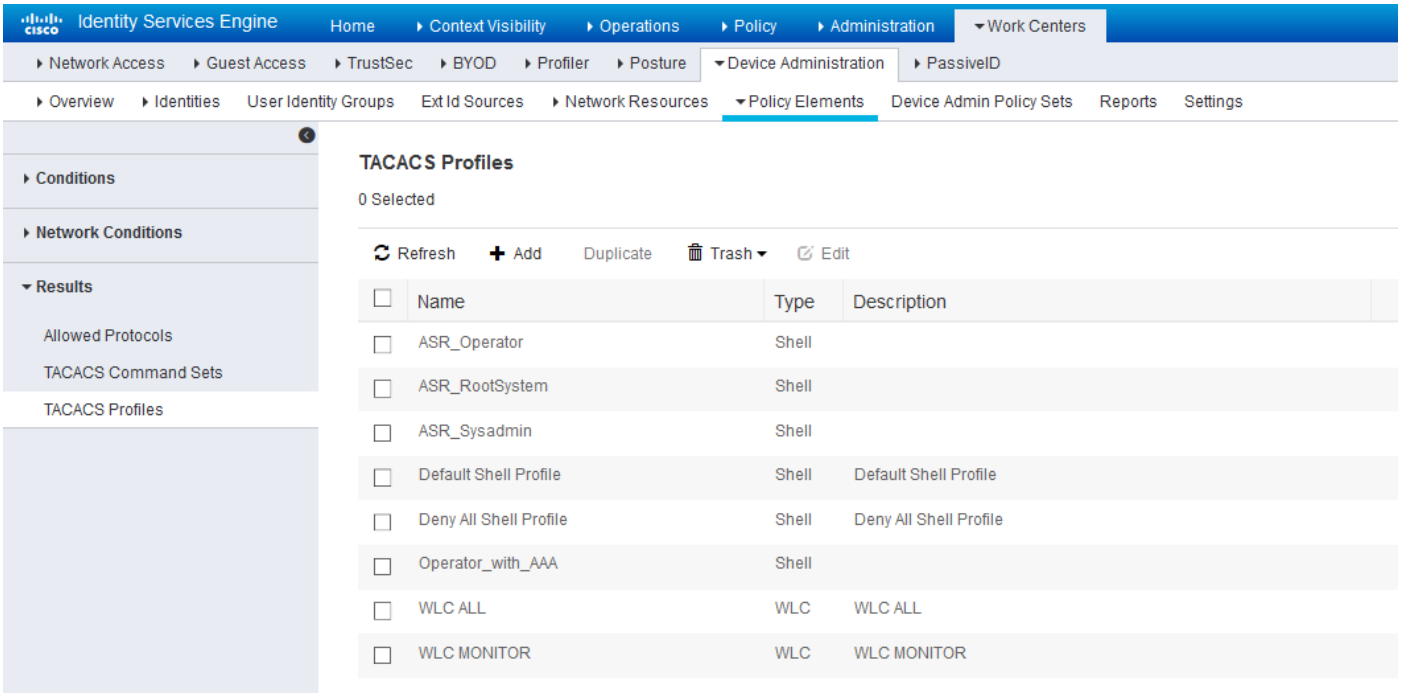
4단계. 각 사용자에 대해 푸시할 셸 프로파일을 정의합니다.이렇게 하려면 Work Centers(작업 센터) > Device Administration(디바이스 관리) **> Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로파일)로 이동합니다**.이미지 및 이전 버전의 ISE에 표시된 대로 새 셸 프로필을 구성할 수 있습니다.이 예제에 정의된 셸 프로파일은 다음과 같습니다.

1. ASR_운영자

2. ASR_RootSystem

3. asr_sysadmin

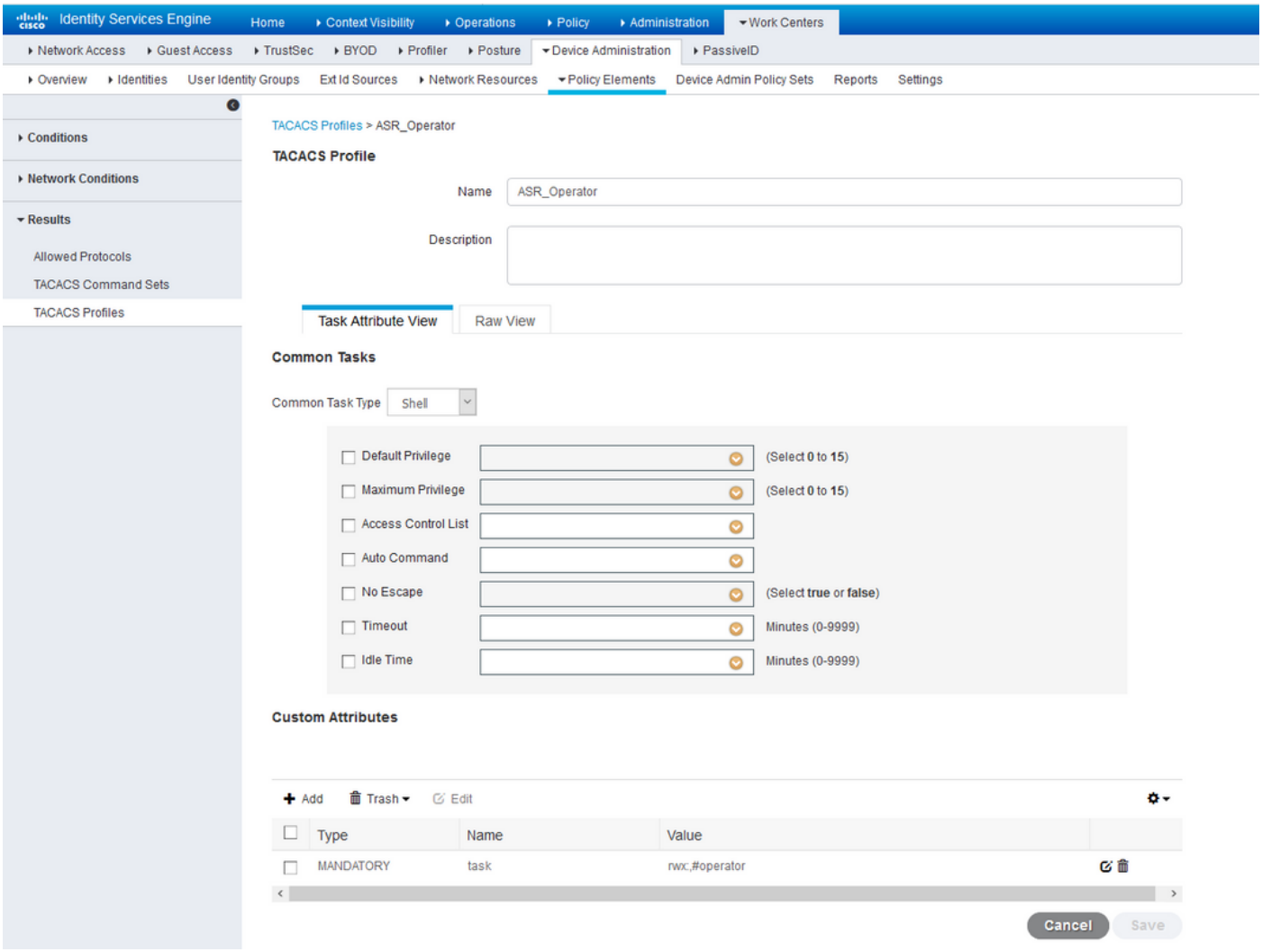
4. Operator_with_AAA



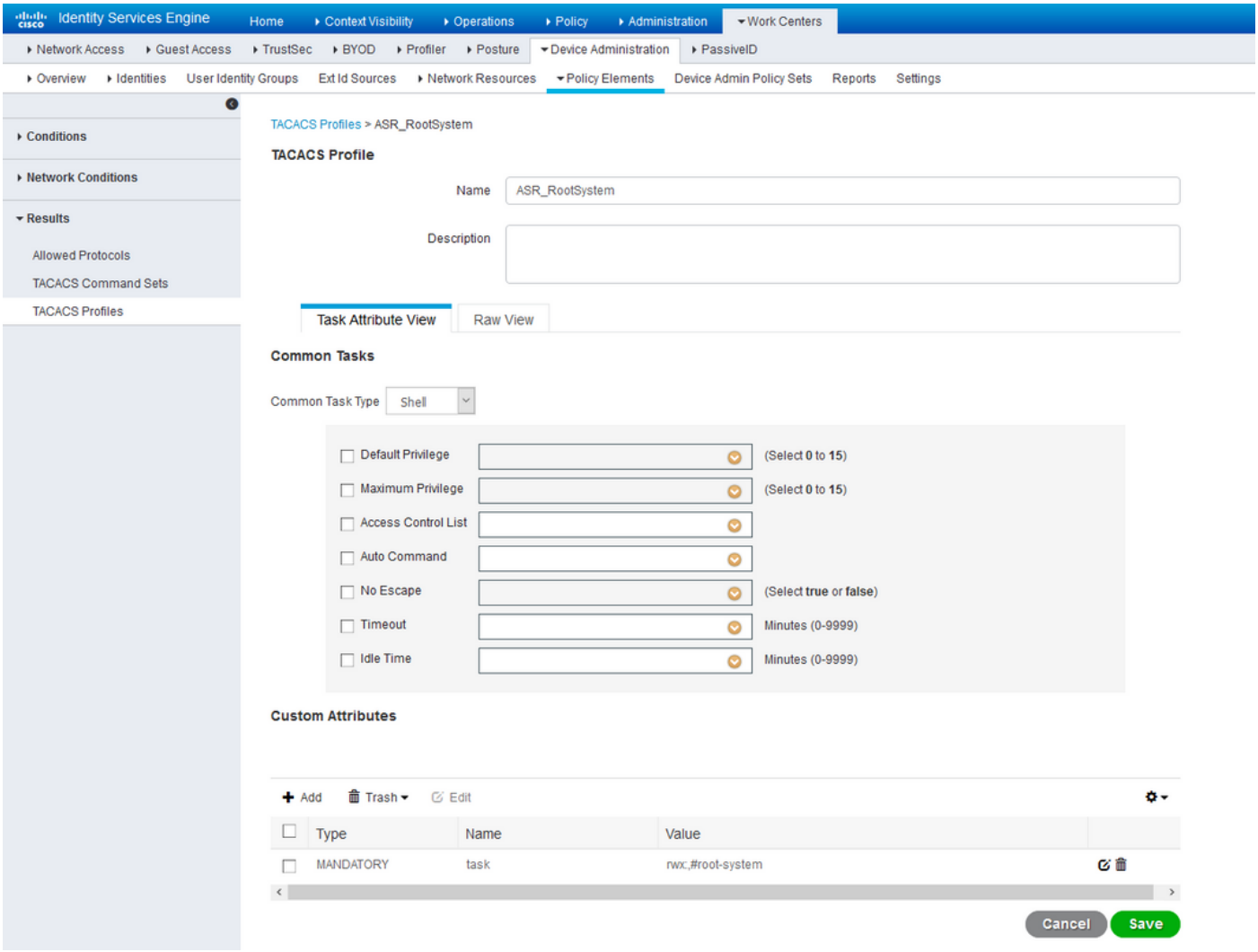
TACACS용 셸 프로파일

Add(추가) 버튼을 클릭하여 **Custom Attributes(맞춤형 특성)** 섹션 아래 이미지에 표시된 대로 Type(유형), Name(이름) 및 Value(값) 필드를 입력할 수 있습니다.

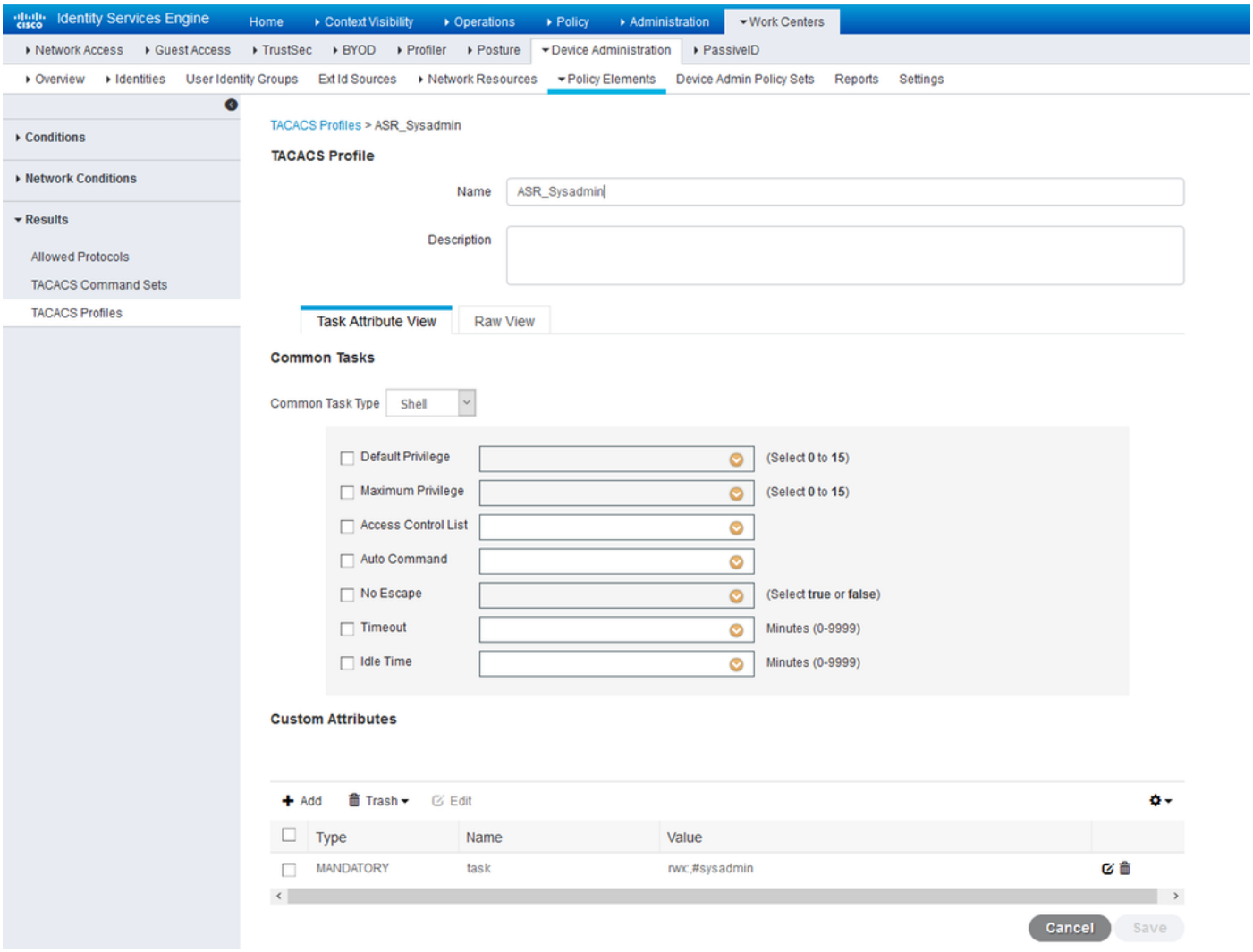
운영자 역할의 경우:



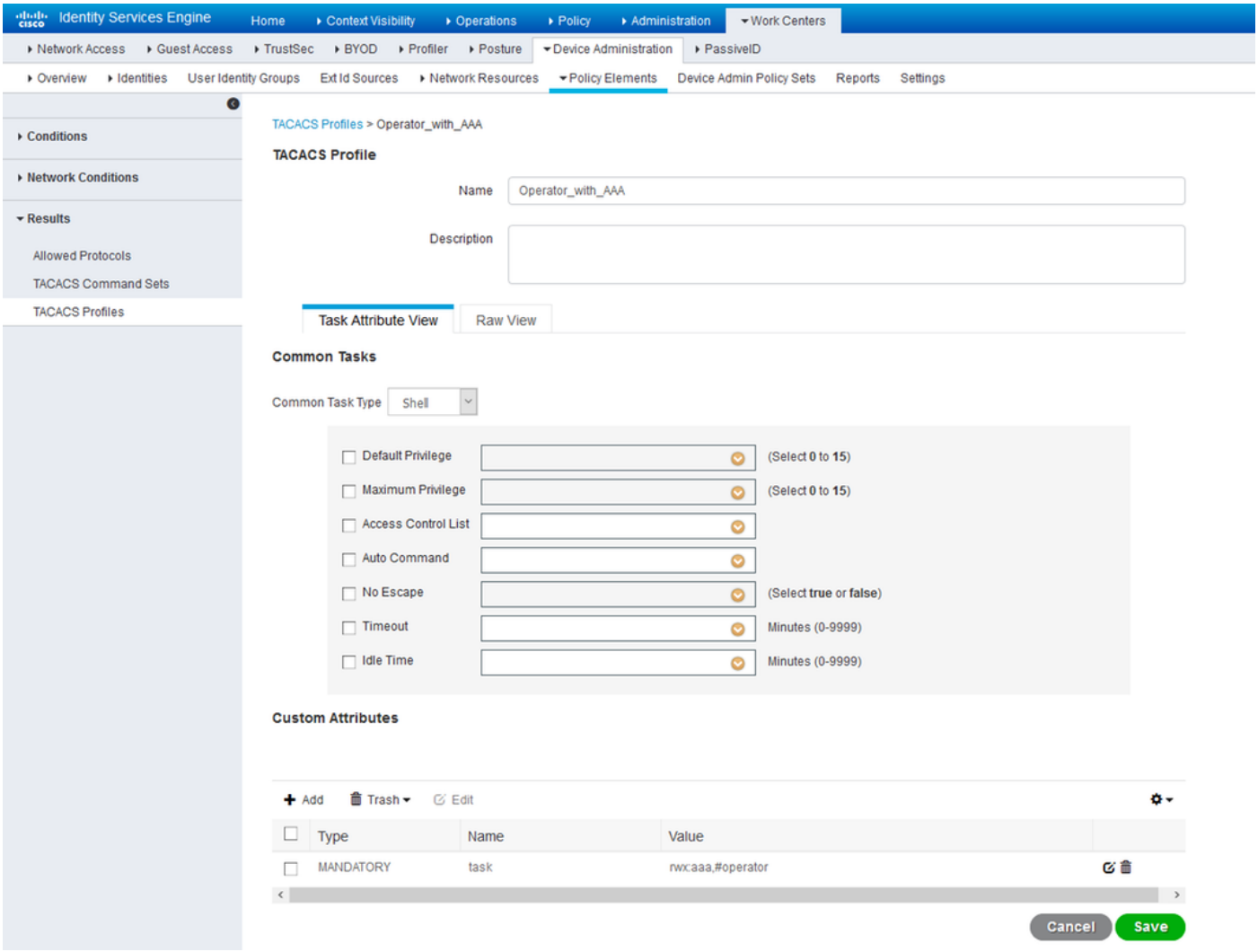
ASR Operator 셸 프로파일루트 시스템 역할의 경우:



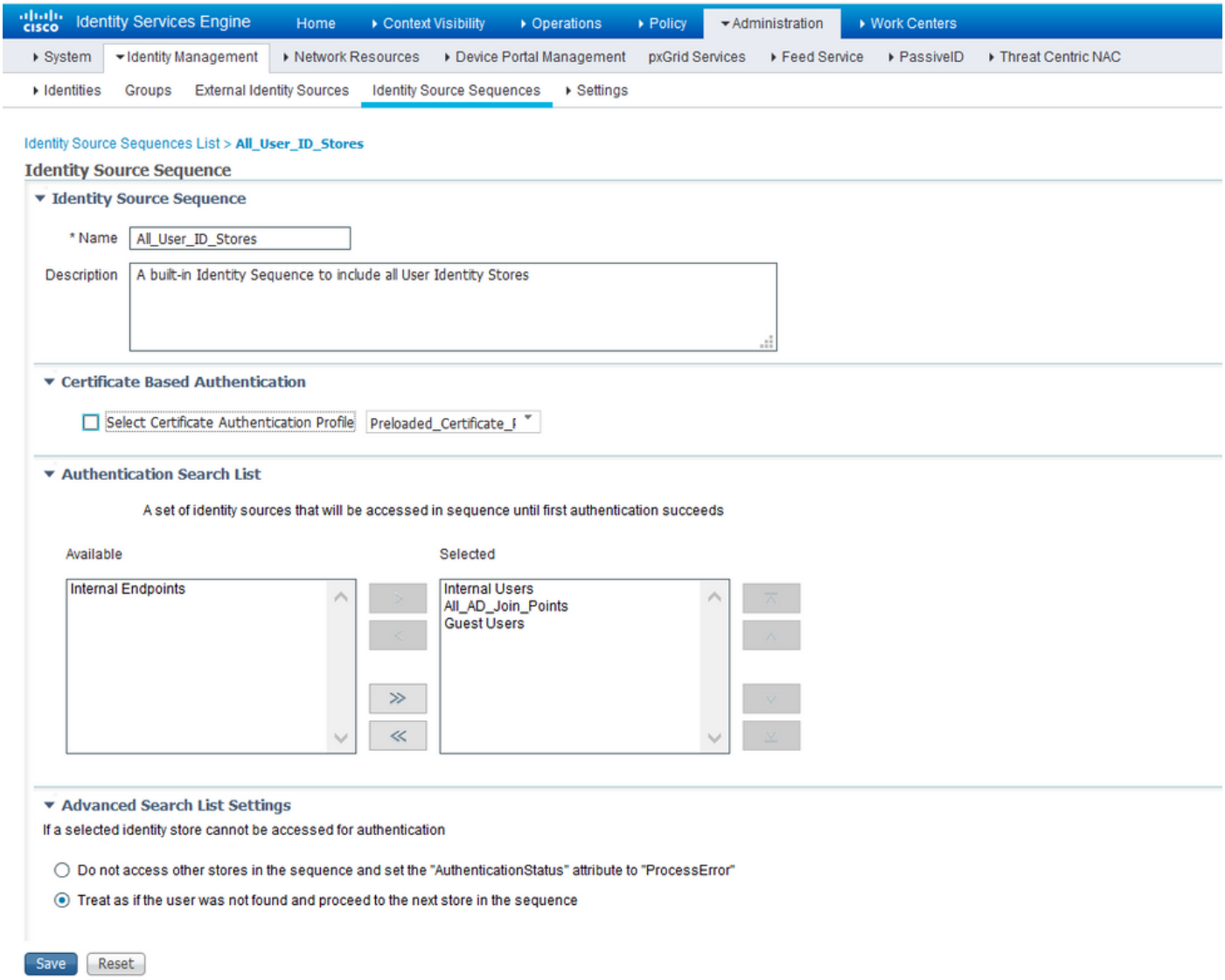
ASR 루트 시스템 셸 프로파일sysadmin 역할의 경우:



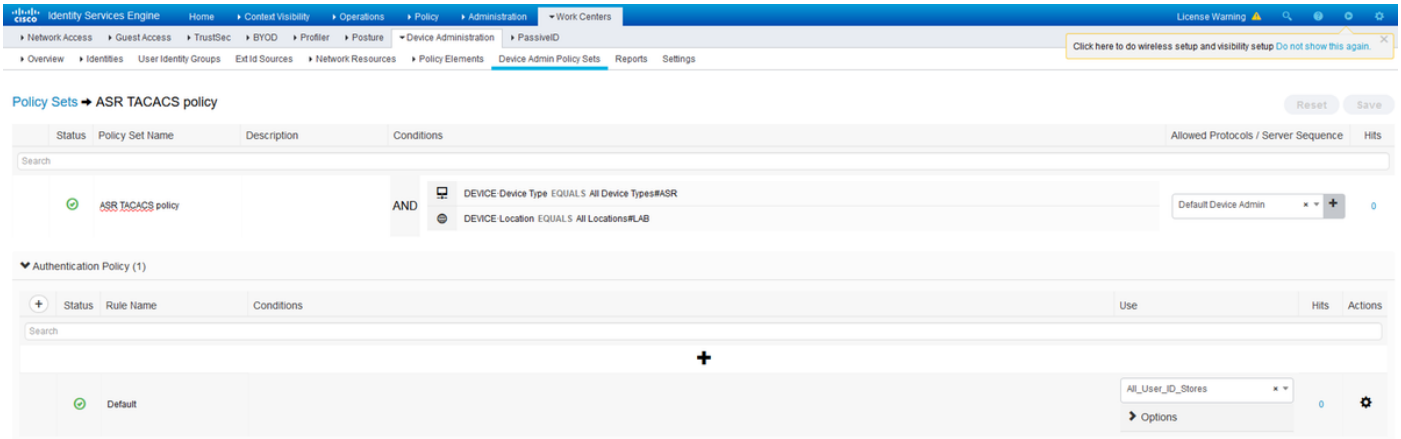
ASR Sysadmin 셸 프로파일운영자 및 AAA 역할의 경우:



AAA 셸 프로파일이 있는 연산자5단계. ID 소스 시퀀스를 구성하여 **관리 > ID 관리 > ID 소스 시퀀스**의 내부 사용자를 사용합니다. 새 ID 소스 시퀀스를 추가하거나 사용 가능한 시퀀스를 편집할 수 있습니다.

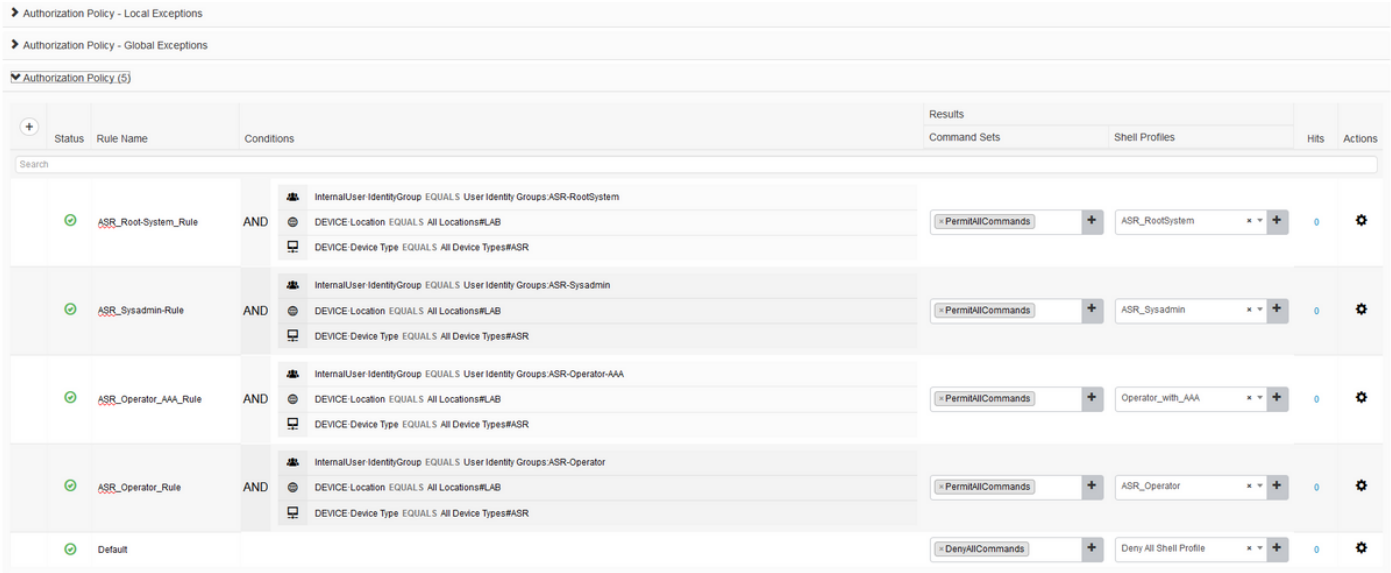


6단계. 내부 사용자가 포함된 ID 스토어 시퀀스를 사용하려면 **Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) > [Choose Policy Set](정책 집합 선택)**에서 인증 정책을 구성합니다.이전에 생성한 사용자 ID 그룹을 사용하여 요구 사항에 따라 권한 부여를 구성하고 이미지에 표시된 대로 각 셸 프로파일을 매핑합니다.



인증 정책

권한 부여 정책은 요구 사항에 따라 다양한 방식으로 구성할 수 있습니다.이미지에 표시된 규칙은 디바이스 위치, 유형 및 특정 내부 사용자 ID 그룹을 기반으로 합니다.선택한 셸 프로파일은 권한 부여 시 명령 집합과 함께 푸시됩니다.



권한 부여 정책

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

연산자

사용자가 라우터에 로그인할 **때** 할당된 사용자 그룹 및 작업 그룹을 확인합니다.

```
username: ASRread
password:

RP/0/RSP1/CPU0:ASR9k#show user
ASRread

RP/0/RSP1/CPU0:ASR9k#show user group
operator

RP/0/RSP1/CPU0:ASR9k#show user tasks
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

AAA가 있는 연산자

다음 경우에 할당된 사용자 그룹 및 작업 그룹 확인**아사라** 사용자가 라우터에 로그인합니다.

> **참고**:AAA 작업 읽기, 쓰기 및 실행 권한과 함께 TACACS 서버에서 푸시된 운영자 작업을 설명합니다.

```
username: asraaa
password:

RP/0/RSP1/CPU0:ASR9k#sh user
```

```
asraaa

RP/0/RSP1/CPU0:ASR9k#sh user group
operator

RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:                  aaa  : READ    WRITE    EXECUTE
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

시스템 관리자

다음 경우에 할당된 사용자 그룹 및 작업 그룹 확인**쓰기** 사용자가 라우터에 로그인합니다.

```
username: asrwrite
password:

RP/0/RSP1/CPU0:ASR9k#sh user
asrwrite

RP/0/RSP1/CPU0:ASR9k#sh user group
sysadmin

RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:                  aaa  : READ
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ
Task:                 ancp  : READ
Task:                  atm  : READ
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ
Task:                  bfd  : READ
Task:                  bgp  : READ
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ
Task:           call-home  : READ
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ
Task:                  cgn  : READ
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ
Task:                 dwdm  : READ
Task:                  eem  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ
Task:    ethernet-services  : READ
--More--
(output omitted )
```

루트 시스템

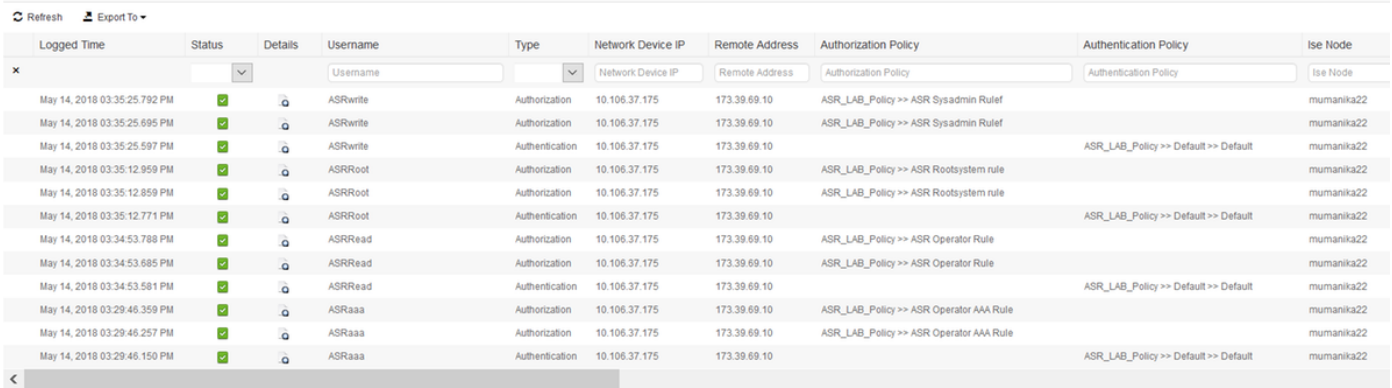
다음 경우에 할당된 사용자 그룹 및 작업 그룹 확인**asrroot** 사용자가 라우터에 로그인합니다.

```
username: asrroot
password:

RP/0/RSP1/CPU0:ASR9k#show user
asrroot

RP/0/RSP1/CPU0:ASR9k#show user group
root-system

RP/0/RSP1/CPU0:ios#show user tasks
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ    WRITE    EXECUTE    DEBUG
Task:                 ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:            call-home  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:                  cgn  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:                 dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                  eem  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
--More--
(output omitted )
```

문제 해결

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

Operations(작업) **> TACACS > Live Logs(라이브 로그)**에서 ISE 보고서**를 확인합니다**.자세한 보고서를 보려면 돋보기 기호를 클릭합니다.



다음은 ASR에서 문제를 해결하기 위한 몇 가지 유용한 명령입니다.

- **사용자 표시**
- **사용자 그룹 표시**

- 사용자 작업 표시
- 사용자 모두 표시