Catalyst SD-WAN GUI에 대한 외부 인증으로 ISE 구성

목차

소개

이 문서에서는 Cisco Catalyst SD-WAN GUI 관리를 위한 외부 인증으로 Cisco ISE(Identity Services Engine)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- TACACS+ 프로토콜
- Cisco ISE 장치 관리
- Cisco Catalyst SD-WAN 관리
- Cisco ISE 정책 평가

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE(Identity Services Engine) 버전 3.4 패치 2
- Cisco Catalyst SD-WAN 버전 20.15.3

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.

시작하기 전에

Cisco vManage Release 20.9.1부터 새로운 태그가 인증에 사용됩니다.

- 비디오 사용자 그룹: Viptela-Group-Name 대신 사용자 그룹 정의를 사용합니다.
- Viptela-Resource-Group: 리소스 그룹 정의를 참조하십시오.

구성 - TACACS+ 사용

TACACS+를 사용하여 Catalyst SD-WAN 구성

절차

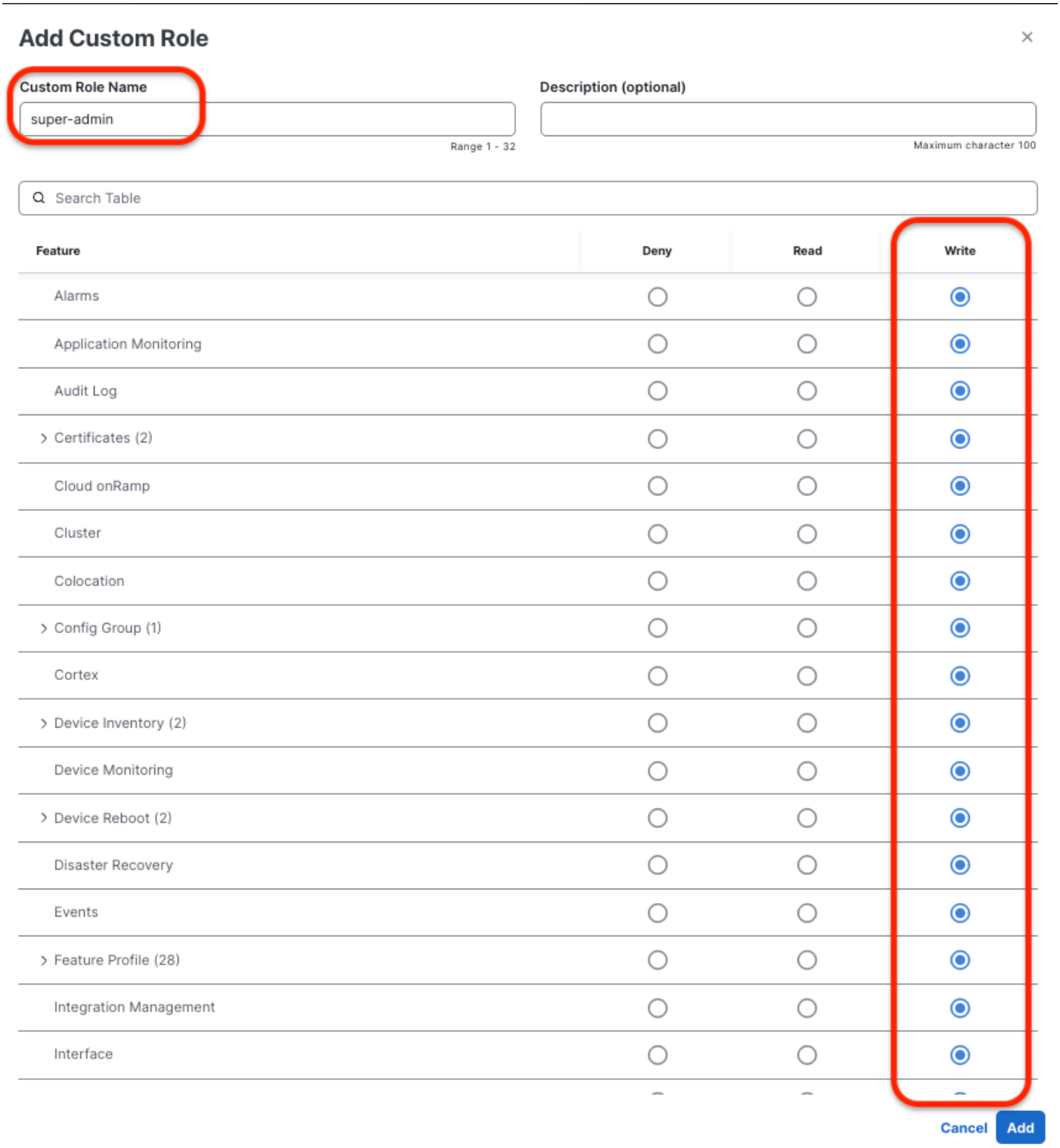
단계 1. (선택 사항) 사용자 지정 역할을 정의합니다.

요구 사항을 충족하는 사용자 지정 역할을 구성합니다. 대신 기본 사용자 역할을 사용할 수 있습니다. 이 작업은 Catalyst SD-WAN 탭에서 수행할 수 있습니다. Administration(관리) > Users and Access(사용자 및 액세스) > Roles(역할).

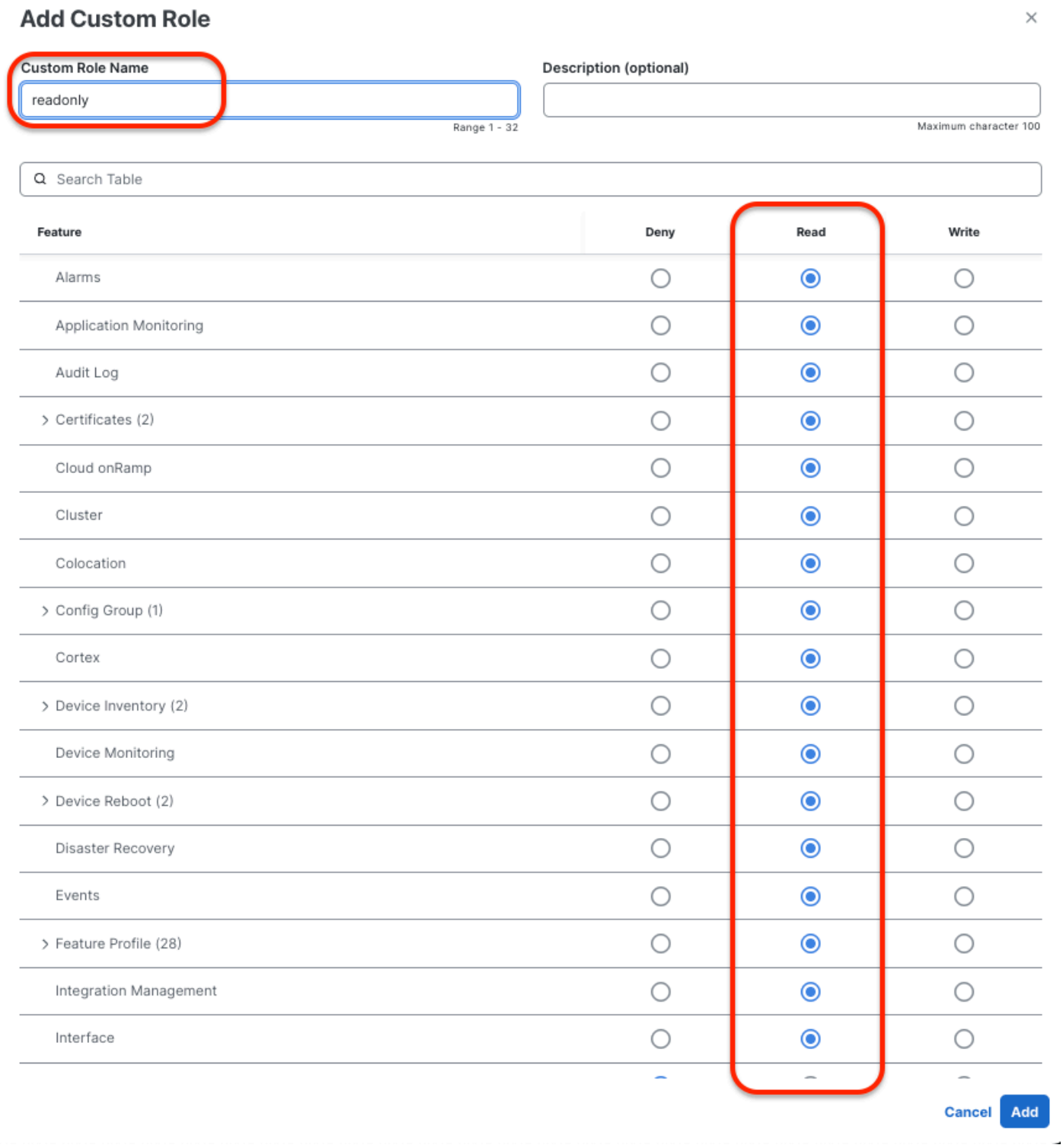
두 가지 사용자 지정 역할 생성:

1. 관리자 역할: 수퍼 관리자
2. 읽기 전용 역할: 읽기 전용

이 작업은 Catalyst SD-WAN 탭에서 수행할 수 있습니다. Administration(관리) > Users and Access(사용자 및 액세스) > Roles(역할) > Add Role(역할 추가)을 클릭합니다.


Add Custom Role
Custom Role Name
super-admin
Range 1 - 32
Description (optional)
Maximum character 100
Search Table
Feature
Deny
Read
Write
Alarms
Application Monitoring
Audit Log
Certificates (2)
Cloud onRamp
Cluster
Colocation
Config Group (1)
Cortex
Device Inventory (2)
Device Monitoring
Device Reboot (2)
Disaster Recovery
Events
Feature Profile (28)
Integration Management
Interface
Cancel
Add

관리자 역할(수퍼 관리자)



읽기 전용 역할(읽기 전용)

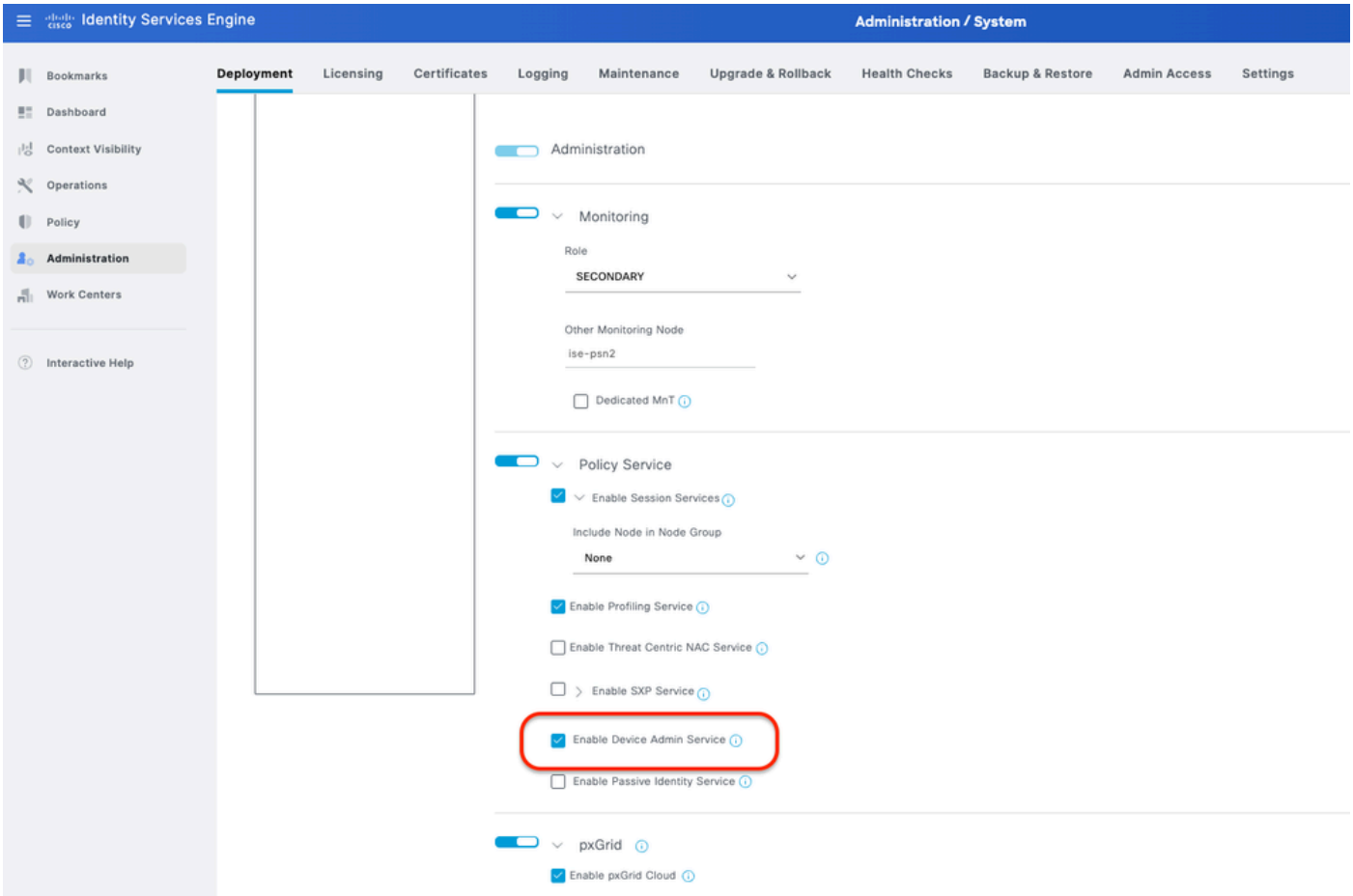
2단계. TACACS+(CLI)를 사용하여 외부 인증을 구성합니다.

```
Entering configuration mode terminal
vmanage(config)#
vmanage(config)#
vmanage(config)# system
vmanage(config-system)# aaa
vmanage(config-aaa)# auth-order tacacs radius local
vmanage(config-aaa)# auth-fallback
vmanage(config-aaa)# commit and-quit
Commit complete.
```

vManger CLI - TACACS+ 컨피그레이션

TACACS+용 ISE 구성

1단계. Device Admin Service를 활성화합니다.
이 작업은 Administration(관리) > System(시스템) > Deployment(구축) > Edit (ISE PSN Node)(편집(ISE PSN 노드)>Enable Device Admin Service(디바이스 관리 서비스 활성화)에서 수행할 수 있습니다.



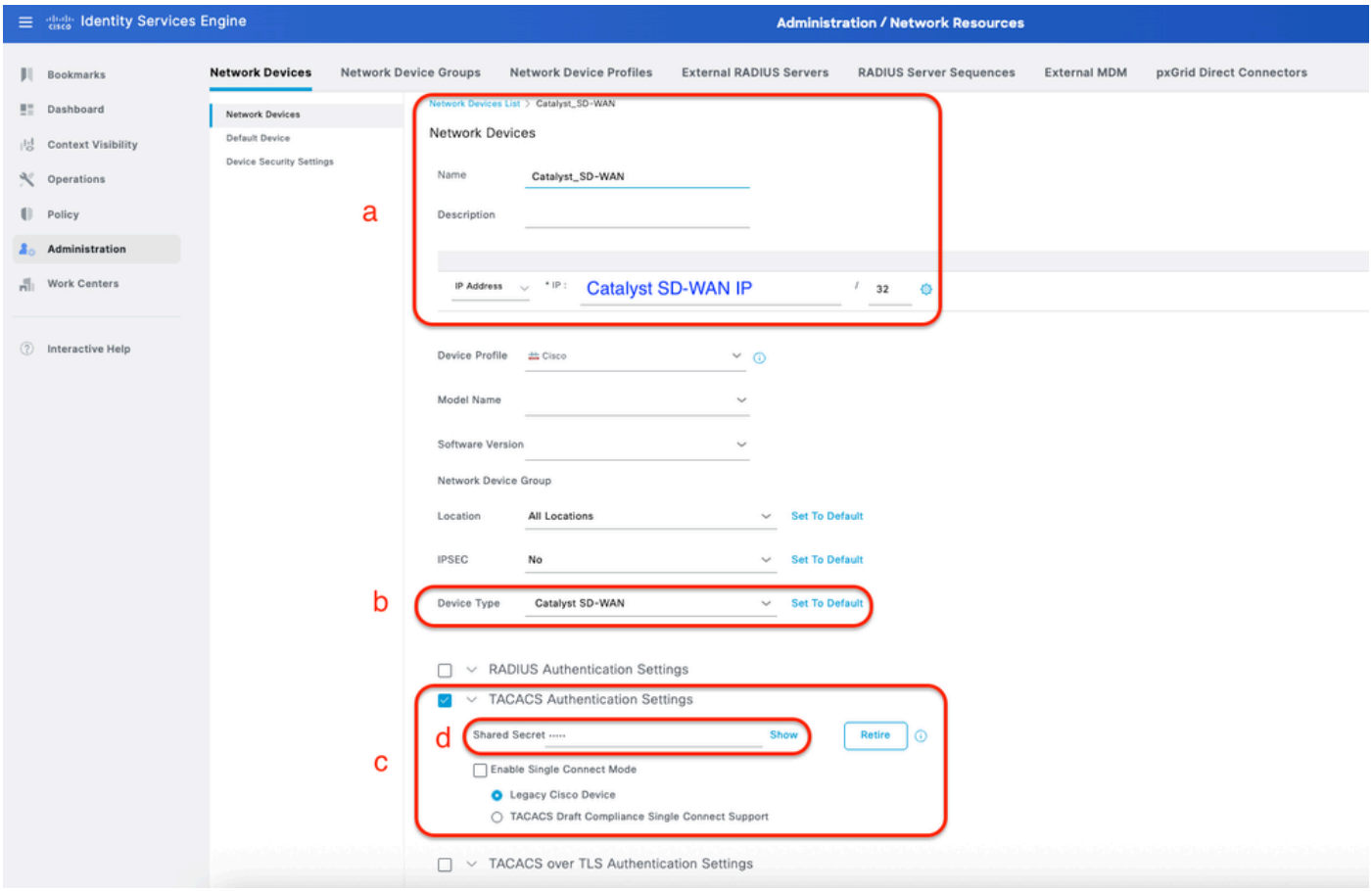
장치 관리 서비스 사용

2단계. Catalyst SD-WAN을 ISE의 네트워크 디바이스로 추가합니다.

이 작업은 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) 탭에서 수행할 수 있습니다.

절차

a. (Catalyst SD-WAN) 네트워크 디바이스 이름 및 IP를 정의합니다.
b. (선택 사항) 정책 집합 조건에 대해 디바이스 유형을 분류합니다.
c. TACACS+ 인증 설정을 활성화합니다.
d. TACACS+ 공유 암호를 설정합니다.



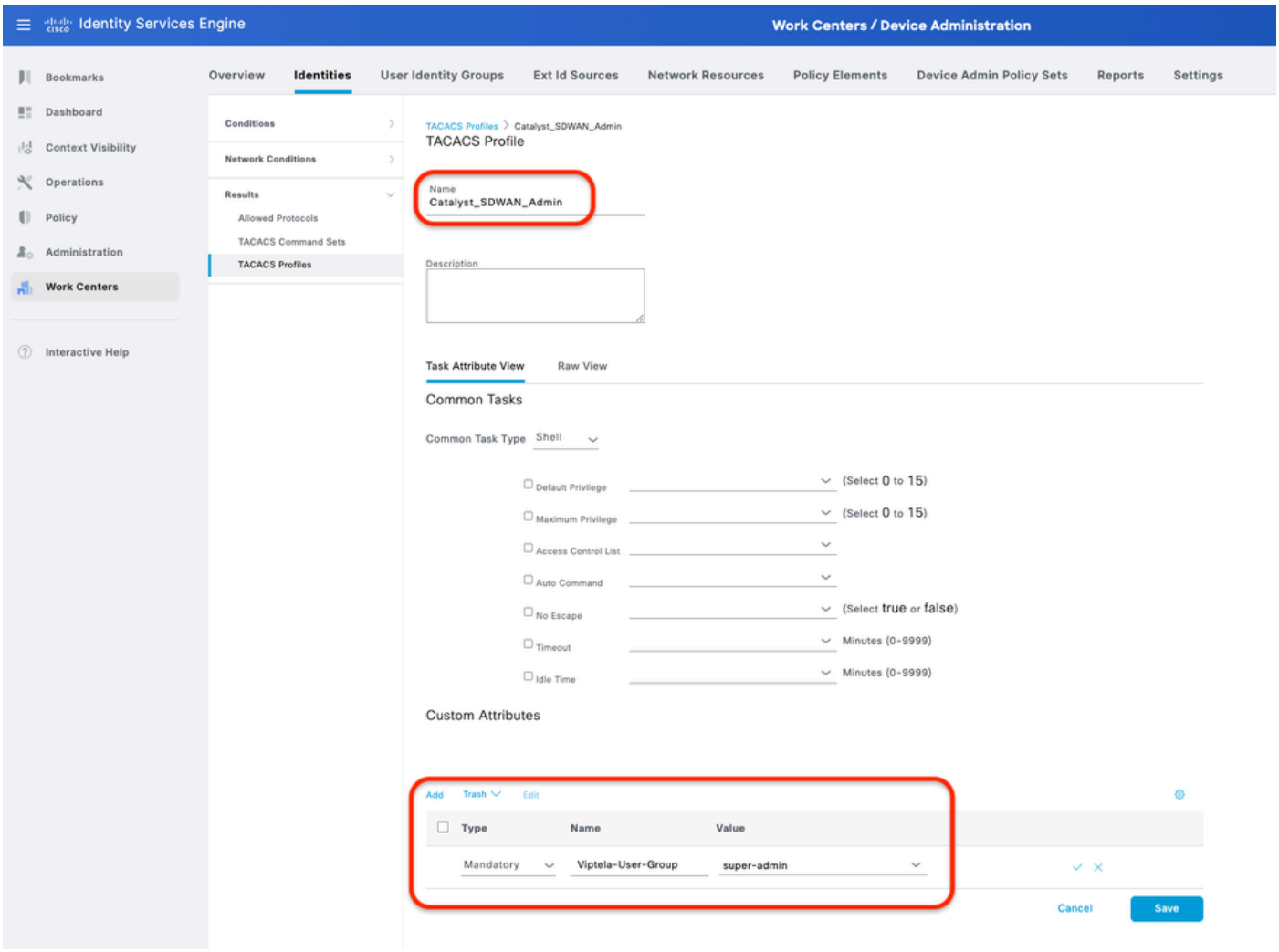
TACACS+용 ISE 네트워크 디바이스(Catalyst SD-WAN)

3단계. 각 Catalyst SD-WAN 역할에 대한 TACACS+ 프로파일을 생성합니다.

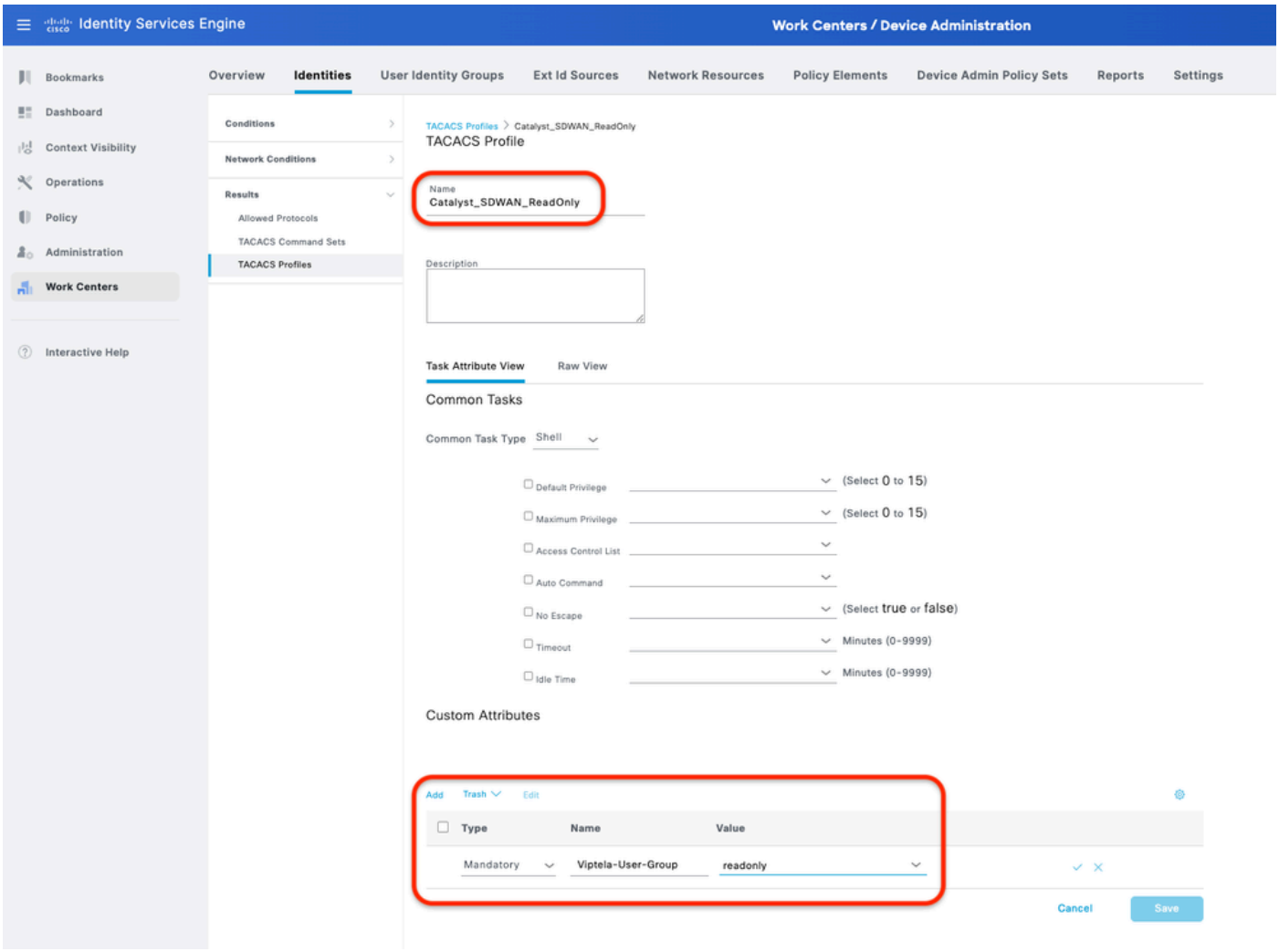
TACACS+ 프로파일 생성:

1. Catalyst_SDWAN_Admin: 수퍼 관리자 사용자의 경우
2. Catalyst_SDWAN_ReadOnly 읽기 전용 사용자용

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로필) > Add(추가) 탭에서 수행할 수 있습니다.



TACACS+ 프로파일 - (Catalyst_SDWAN_Admin)



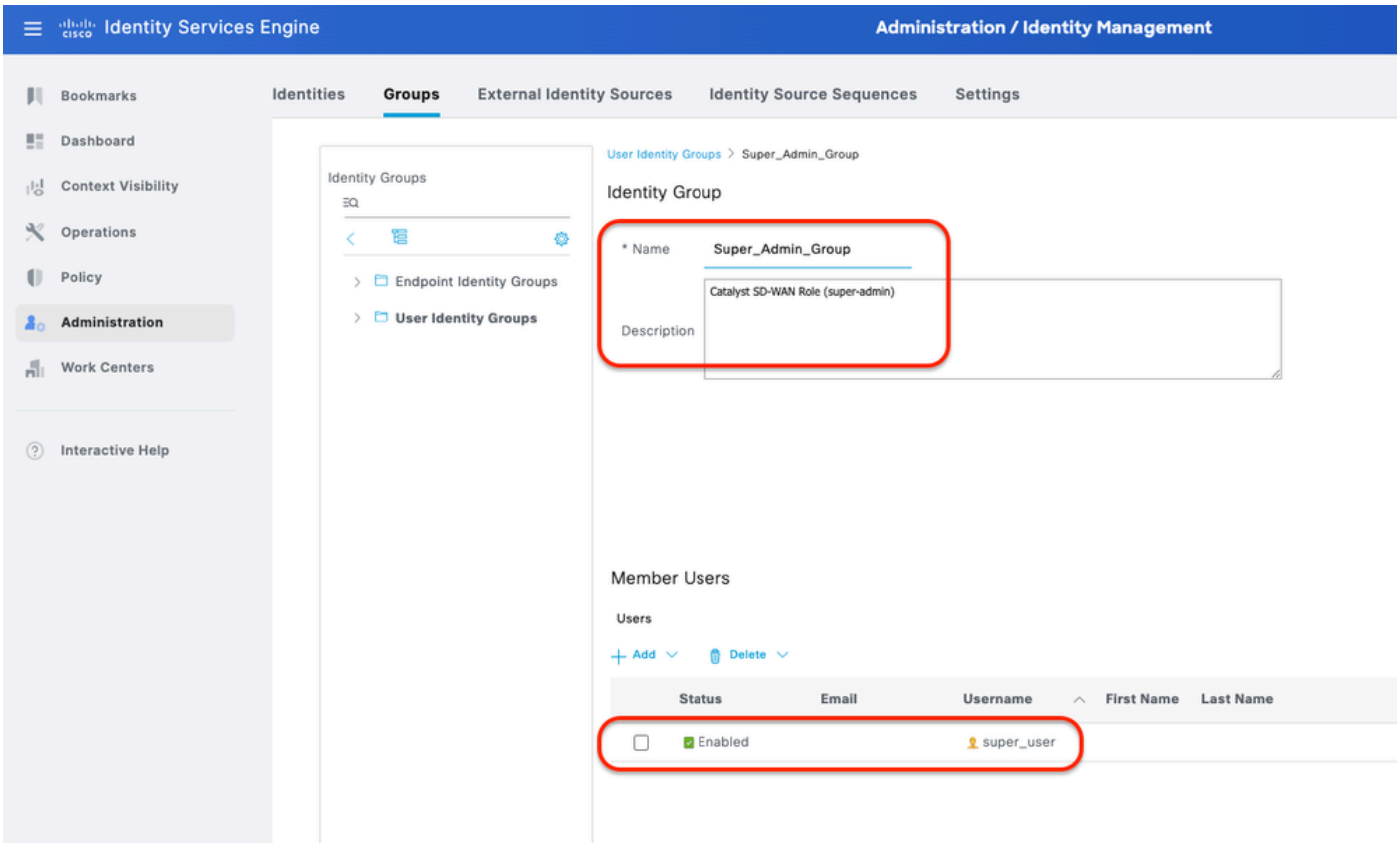
TACACS+ 프로파일 - (Catalyst_SDWAN_ReadOnly)

4단계. 사용자 그룹 생성 로컬 사용자를 구성원으로 추가합니다.

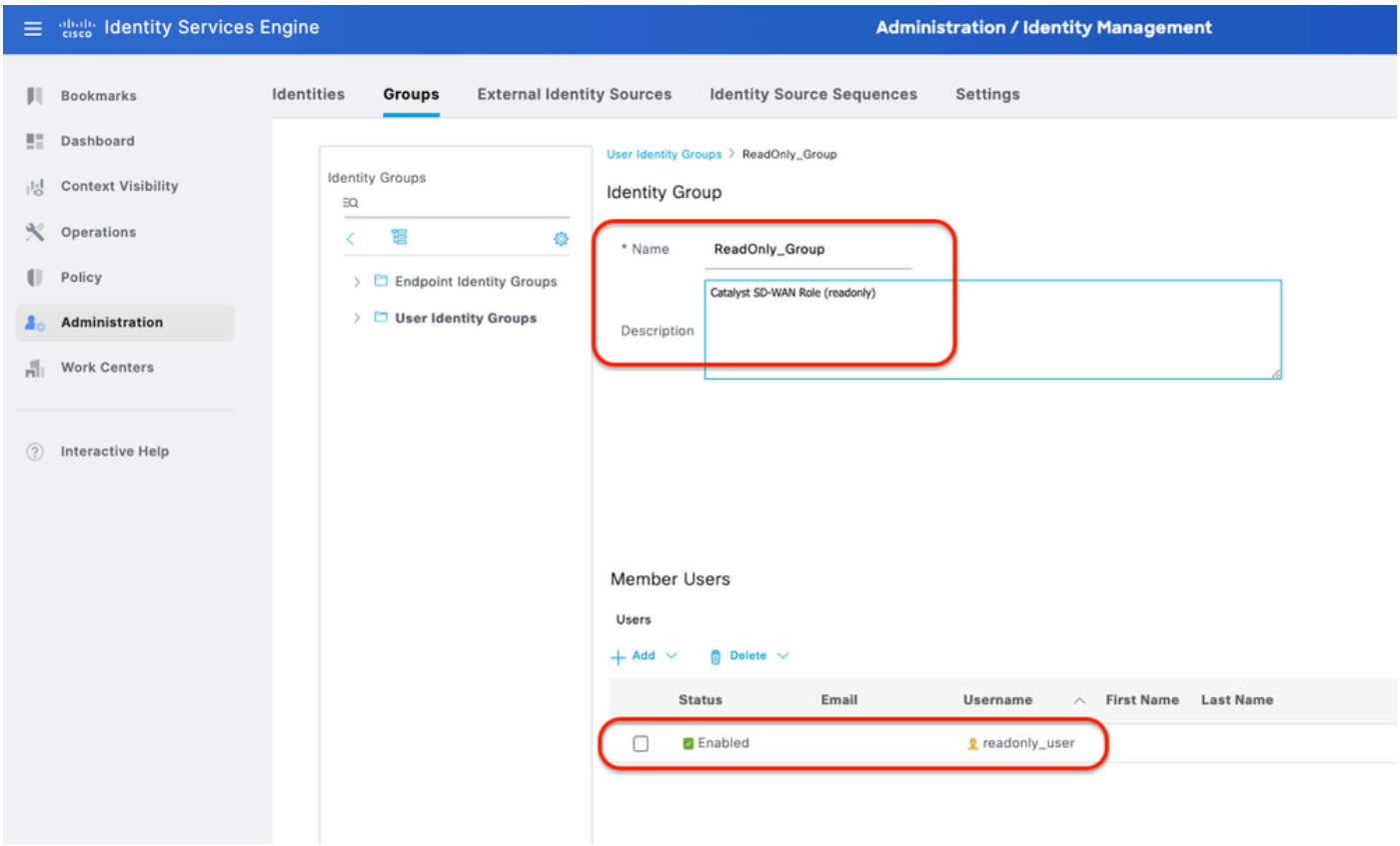
이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > User Identity Groups(사용자 ID 그룹) 탭에서 수행할 수 있습니다.

두 개의 사용자 ID 그룹 생성:

1. Super_Admin_Group
2. 읽기 전용_그룹



사용자 ID 그룹 - (Super_Admin_Group)



사용자 ID 그룹 - (ReadOnly_Group)

5단계. (선택 사항) TACACS+ 정책 세트를 추가합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) 탭에서 수행할 수 있습니다.

절차

a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

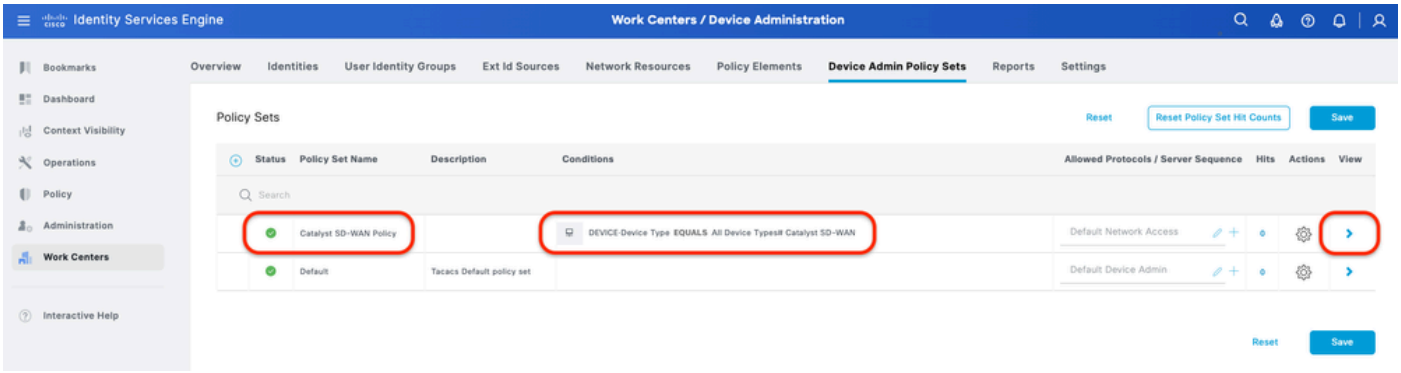
b. 정책 집합 이름을 정의합니다.

c. 이전에 생성한 Select Device Type(디바이스 유형 선택)으로 Policy Set Condition(정책 설정 조건)을 설정합니다(2단계 > b).

d. Allowed 프로토콜을 설정합니다.

e. 저장을 클릭합니다.

f. 인증 및 권한 부여 규칙을 구성하려면 (>) Policy Set View를 클릭합니다.



ISE 정책 집합

6단계. TACACS+ 인증 정책을 구성합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) > Click(>) 탭에서 수행할 수 있습니다.

절차

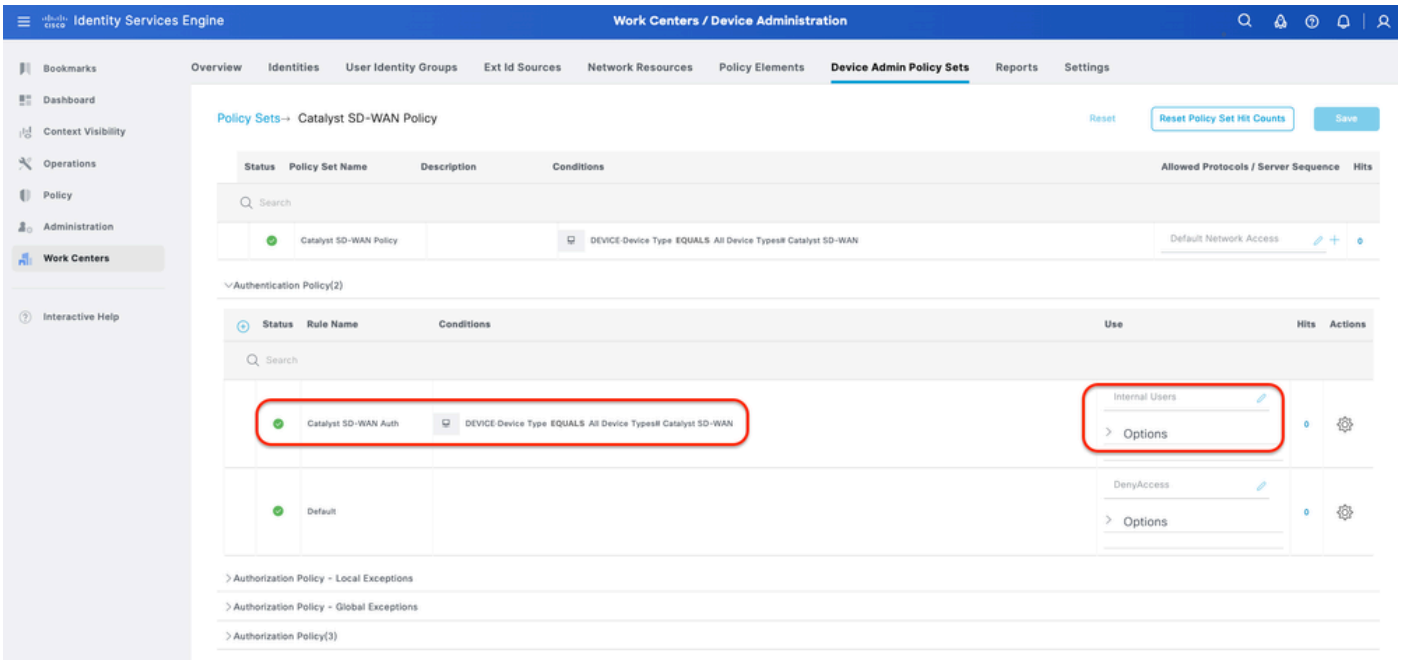
a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

b. 인증 정책 이름을 정의 합니다.

c. Authentication Policy Condition(인증 정책 조건)을 설정하고 이전에 생성한 Device Type(디바이스 유형)을 선택합니다(2단계 > b).

d. ID 소스에 대한 인증 정책 사용을 설정합니다.

e. 저장을 클릭합니다.



인증 정책

7단계. TACACS+ 권한 부여 정책을 구성합니다.

이 작업은 Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합) > Click (>)(클릭) 탭에서 수행할 수 있습니다.

각 Catalyst SD-WAN 역할에 대한 권한 부여 정책을 생성하려면 이 단계를 수행합니다.

- Catalyst SD-WAN Authz(수퍼 관리자): 수퍼 관리자
- Catalyst SD-WAN 인증(읽기 전용): 읽기 전용

절차

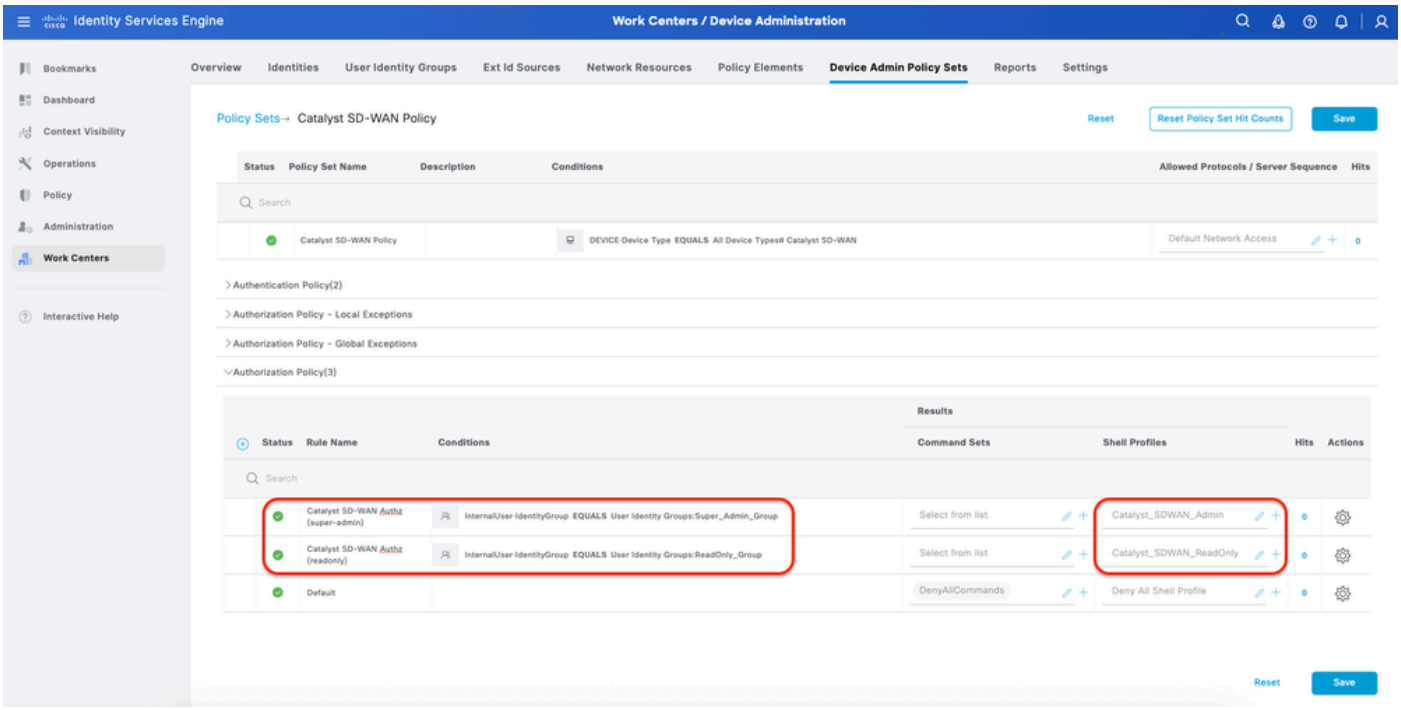
a. Actions(작업)를 클릭하고 선택합니다(위에 새 행 삽입).

b. 권한 부여 정책 이름을 정의합니다.

c. Authorization Policy Condition(권한 부여 정책 조건)을 설정하고 (4단계)에서 생성한 User Group(사용자 그룹)을 선택합니다.

d. Authorization Policy(권한 부여 정책)Shell Profiles(셸 프로파일)를 설정하고 3단계에서 생성한 TACACS Profile(TACACS 프로파일)을 선택합니다.

e. 저장을 클릭합니다.

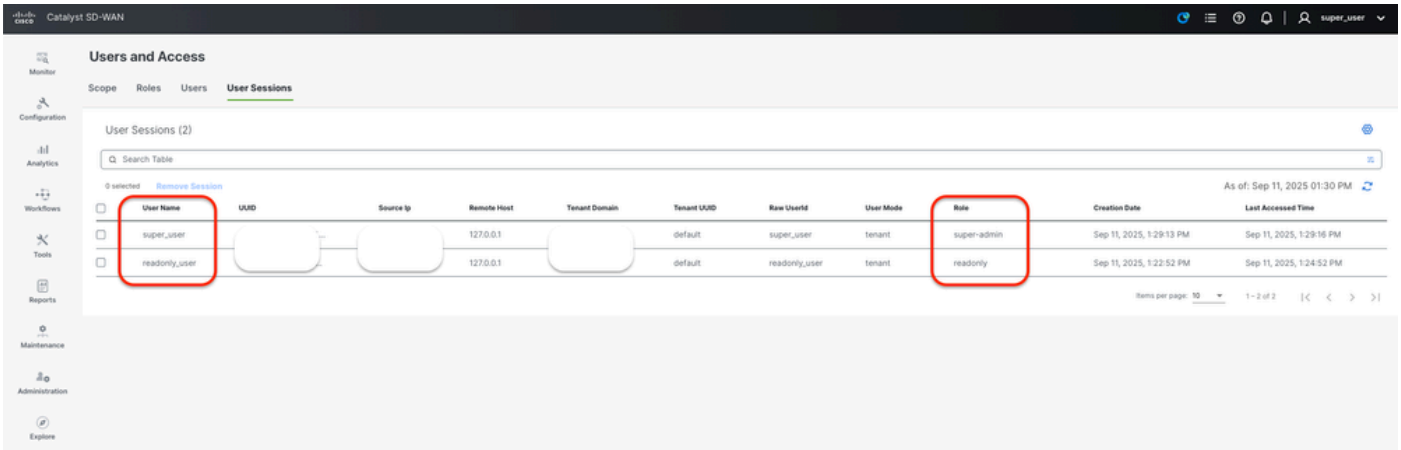


권한 부여 정책

TACACS+ 컨피그레이션 확인

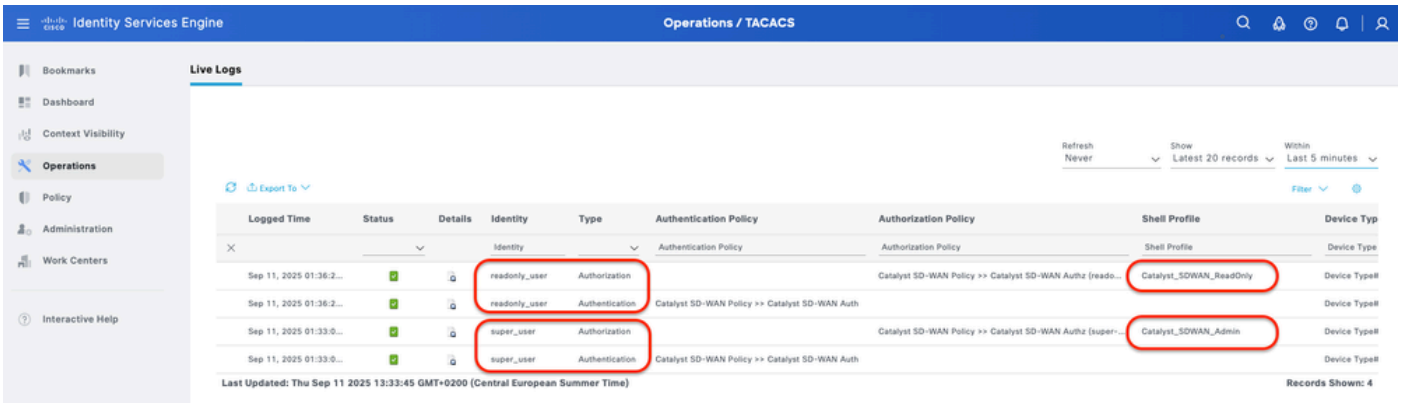
1- Catalyst SD-WAS 사용자 세션 표시 Catalyst SD-WAN: Administration(관리) > Users and Access(사용자 및 액세스) > User Sessions(사용자 세션).

RADIUS를 통해 처음 로그인한 외부 사용자 목록을 볼 수 있습니다. 표시되는 정보에는 사용자 이름 및 역할이 포함됩니다.



Catalyst SD-WAS 사용자 세션

2- ISE - TACACS Live-Logs Operations(TACACS 라이브 로그 작업) > TACACS > Live-Logs(라이브 로그)


Identity Services Engine
Operations / TACACS
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Live Logs
Refresh
Never
Show
Latest 20 records
Within
Last 5 minutes
Export To
Filter
Logged Time
Status
Details
Identity
Type
Authentication Policy
Authorization Policy
Shell Profile
Device Typ
Sep 11, 2025 01:36:2...
readonly_user
Authorization
Catalyst SD-WAN Policy >> Catalyst SD-WAN Authz (reado...
Catalyst_SDWAN_ReadOnly
Device Type#
Sep 11, 2025 01:36:2...
readonly_user
Authentication
Catalyst SD-WAN Policy >> Catalyst SD-WAN Auth
Device Type#
Sep 11, 2025 01:33:0...
super_user
Authorization
Catalyst SD-WAN Policy >> Catalyst SD-WAN Authz (super-...
Catalyst_SDWAN_Admin
Device Type#
Sep 11, 2025 01:33:0...
super_user
Authentication
Catalyst SD-WAN Policy >> Catalyst SD-WAN Auth
Device Type#
Last Updated: Thu Sep 11 2025 13:33:45 GMT+0200 (Central European Summer Time)
Records Shown: 4

라이브 로그

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	27
IdentityGroup	User Identity Groups:ReadOnly_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	316584755210.127.198.7438561Authorization3165847552
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=0;2=0;3=4;4=3;5=4;6=0;7=2;8=1;9=0;10=8;11=2;12=3;13=0;14=0;15=0
TotalAuthenLatency	27
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=readonly; }

자세한 라이브 로그 - (읽기 전용)

Protocol	Tacacs
Type	Authorization
Service-Argument	ppp
Protocol-Argument	ip
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Network Access
RequestLatency	30
IdentityGroup	User Identity Groups:Super_Admin_Group
SelectedAuthenticationIdentityStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	354536652810.127.198.7460535Authorization3545366528
IdentitySelectionMatchedRule	Catalyst SD-WAN Auth
StepLatency	1=1;2=0;3=3;4=3;5=3;6=0;7=2;8=0;9=0;10=10;11=4;12=4;13=0;14=1;15=0
TotalAuthenLatency	30
ClientLatency	0
TacacsPlusTLS	false
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Viptela-User-Group=super-admin; }

문제 해결

현재 이 구성에 사용할 수 있는 특정 진단 정보가 없습니다.

참조

- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.4
- Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN 릴리스 17.x

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.