Configure ISE as an External Authentication for Catalyst SD-WAN GUI

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Before You Begin

Configure - Using TACACS+

- Configure Catalyst SD-WAN Using TACACS+
- Configure ISE for TACACS+
- Verify TACACS+ Configuration

Troubleshoot

References

Introduction

This document describes how to configure Cisco Identity Services Engine(ISE) as an external authentication for Cisco Catalyst SD-WAN GUI administration.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- TACACS+ protocol
- Cisco ISE Device Administration
- Cisco Catalyst SD-WAN Administration
- Cisco ISE Policy Evaluation

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine (ISE) Version 3.4 Patch2
- Cisco Catalyst SD-WAN Version 20.15.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Before You Begin

Starting from Cisco vManage Release 20.9.1, new tags are used in authentication:

- Viptela-User-Group: for user group definitions instead of Viptela-Group-Name.
- Viptela-Resource-Group: for resource group definitions.

Configure - Using TACACS+

Configure Catalyst SD-WAN Using TACACS+

Procedure

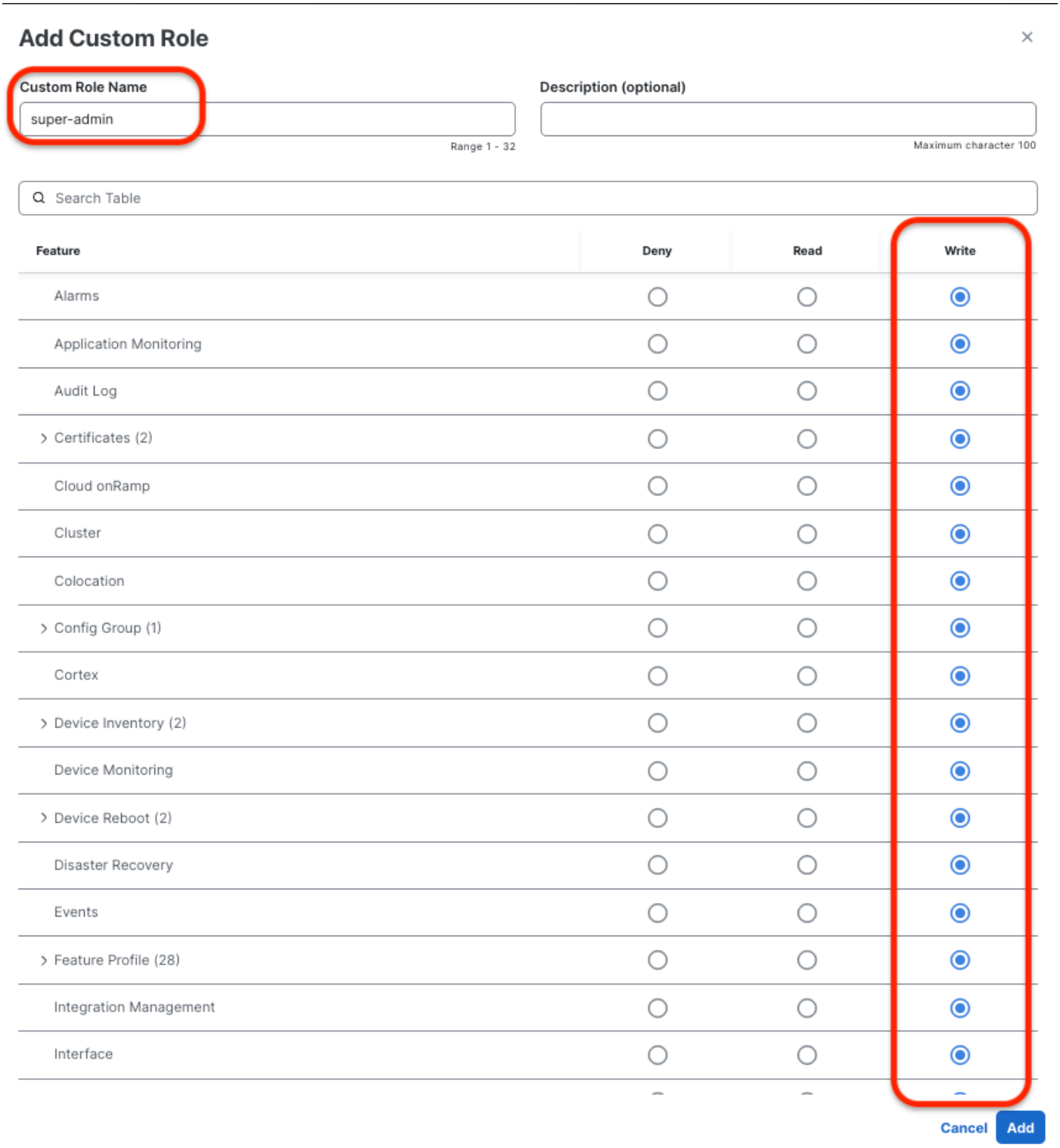
Step 1. (Optional) Define Custom Roles.

Configure your custom roles that fulfils your requirement, instead, you can use the default User Roles. This can be done from the tab **Catalyst SD-WAN: Administration > Users and Access > Roles**.

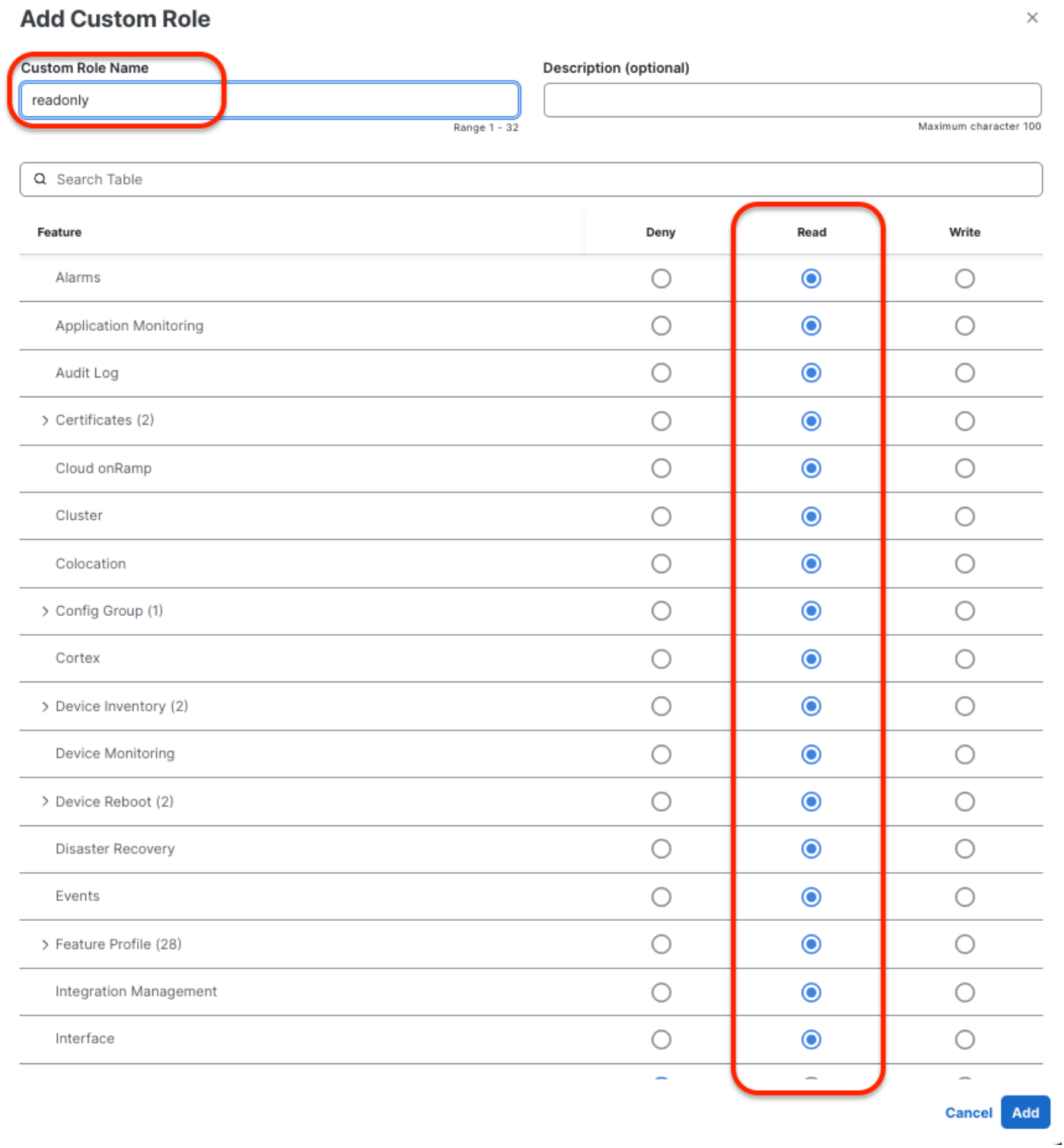
Create two Custom Roles:

1. Admin Role: **super-admin**
2. Read Only Role: **readonly**

This can be done from the tab **Catalyst SD-WAN: Administration > Users and Access > Roles > Click > Add Role**.



Admin Role (super-admin)



Read -Only Role (readonly)

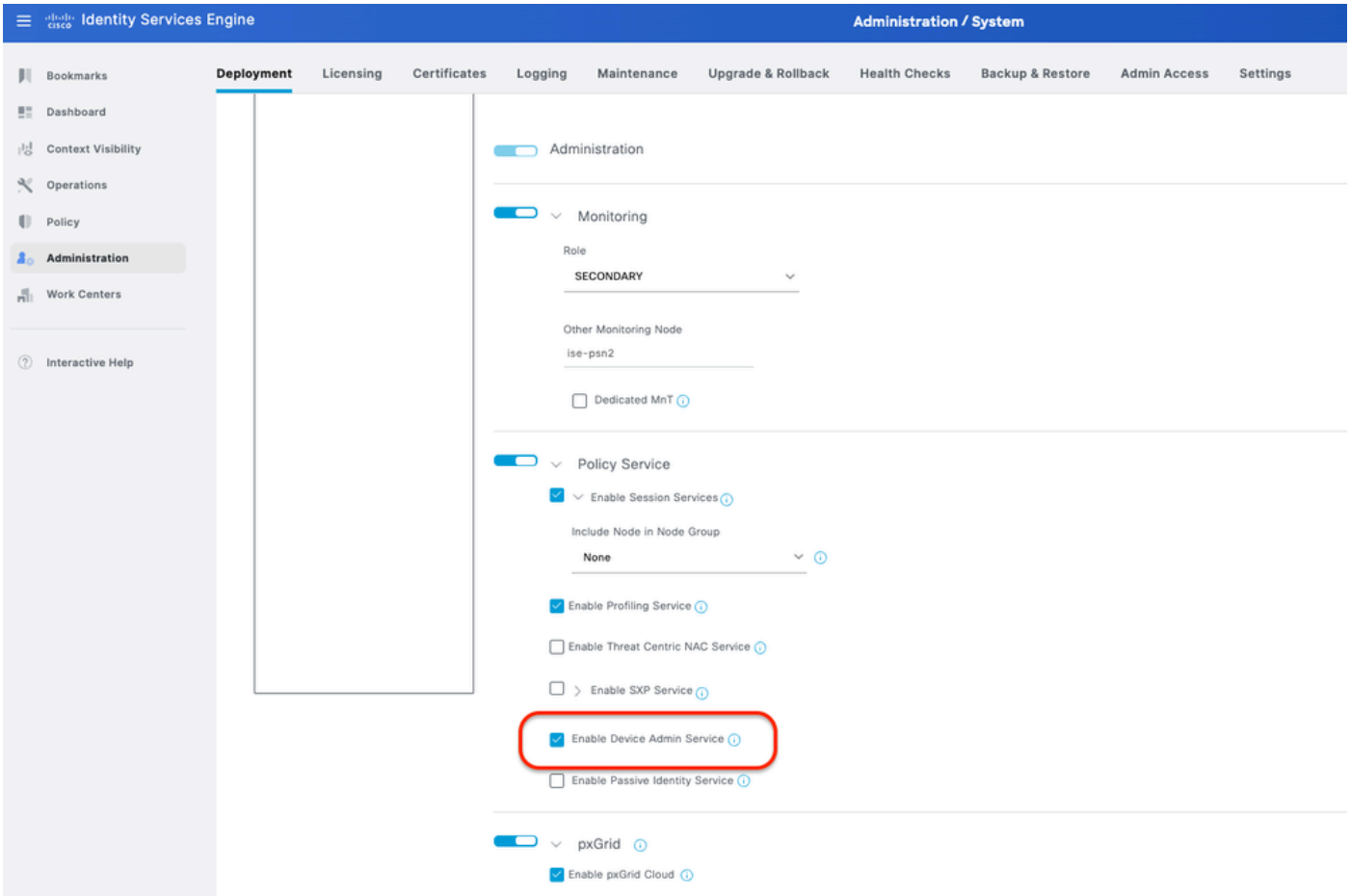
Step 2. Configure **External Authentication** using TACACS+ (CLI).

```
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+ Configuration

Configure ISE for TACACS+

Step 1. Enable Device Admin Service.
This can be done from the tab **Administration > System > Deployment >Edit (ISE PSN Node)>Check Enable Device Admin Service**.



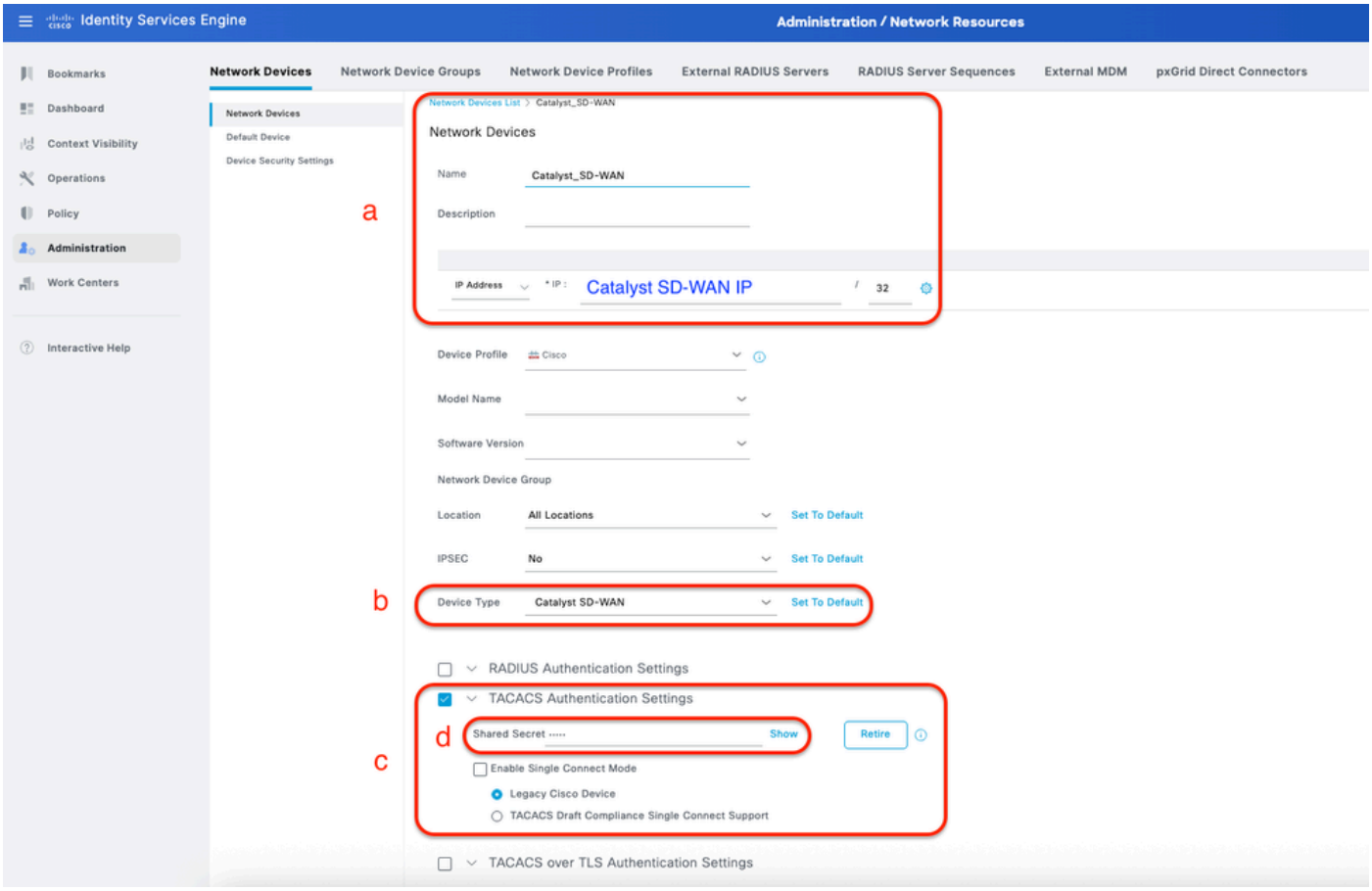
Enable Device Admin Service

Step 2. Add **Catalyst SD-WAN** as a Network Device on ISE.

This can be done from the tab **Administration > Network Resources > Network Devices**.

Procedure

a. Define (Catalyst SD-WAN) **Network Device** name and **IP**.
b. (Optional) Classify **Device Type** for Policy Set condition.
c. Enable **TACACS+ Authentication Settings**.
d. Set **TACACS+ Shared Secret**.



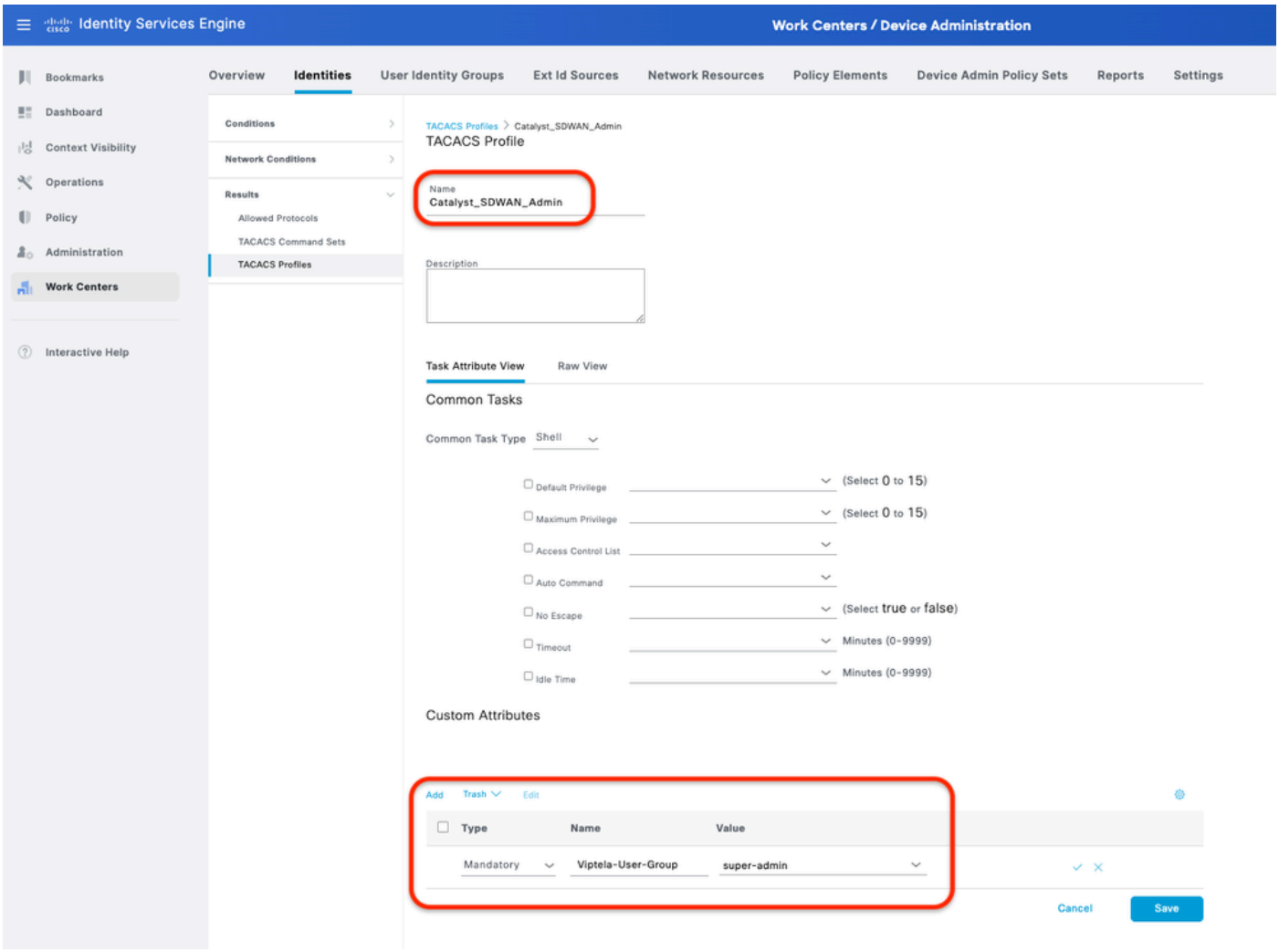
ISE Network Device (Catalyst SD-WAN) for TACACS+

Step 3. Create **TACACS+ Profile** for each Catalyst SD-WAN role.

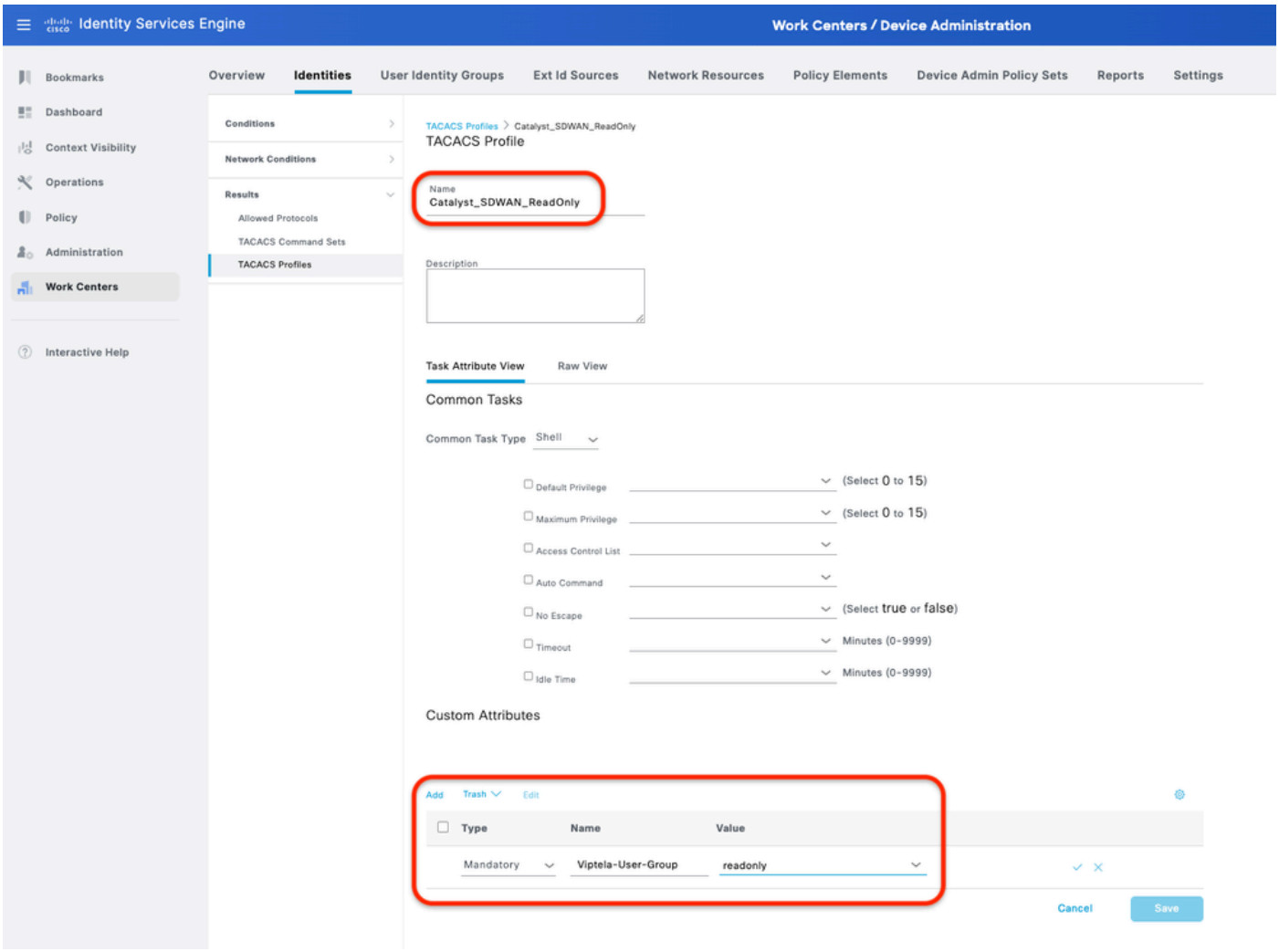
Create TACACS+ Profiles:

1. Catalyst_SDWAN_Admin: For Super Admin Users.
2. Catalyst_SDWAN_ReadOnly: For Read Only Users.

This can be done from the tab **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles > Add**.



TACACS+ Profile - (Catalyst_SDWAN_Admin)



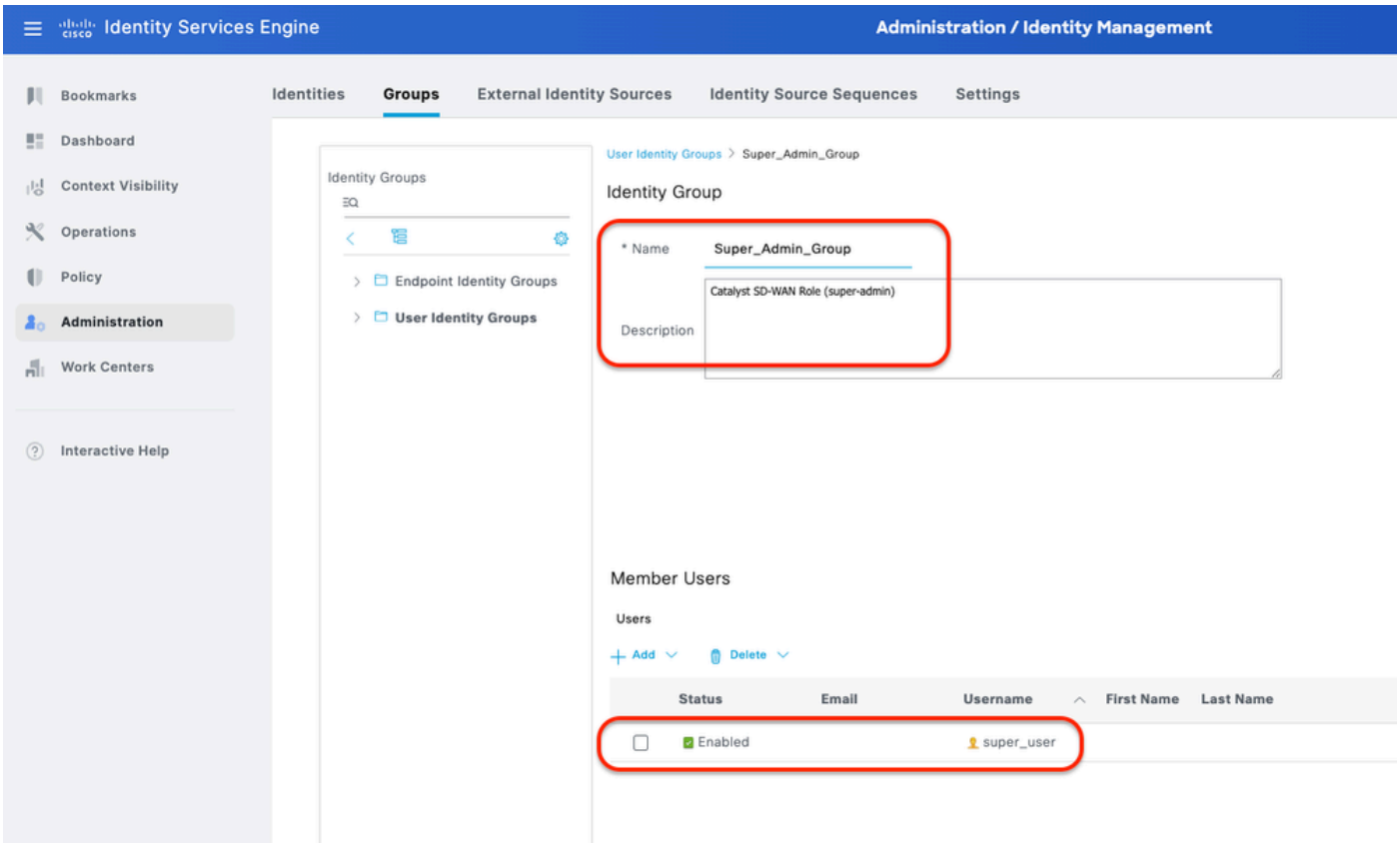
TACACS+ Profile - (Catalyst_SDWAN_ReadOnly)

Step 4. Create **User Group** add **Local Users** as a member.

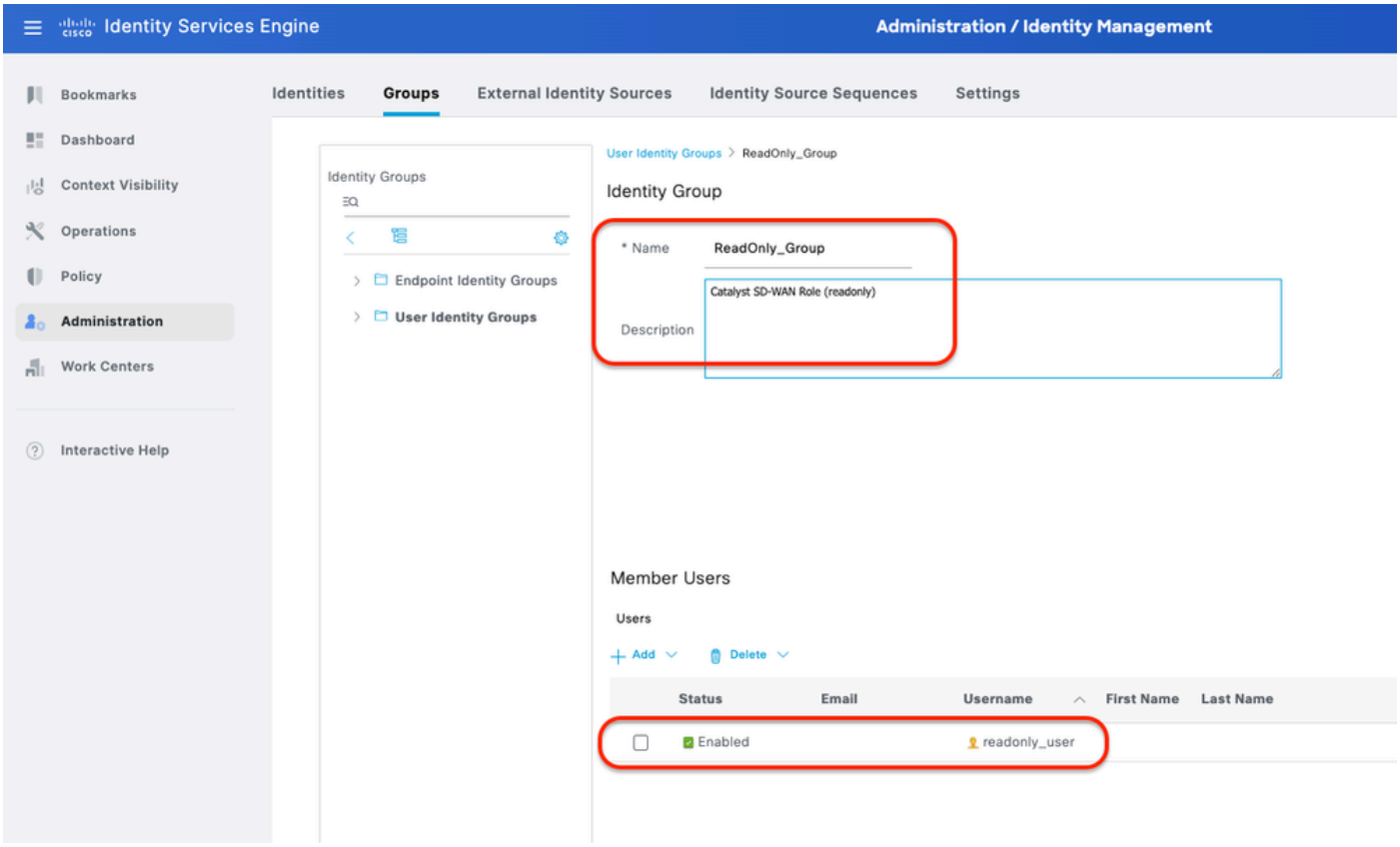
This can be done from the tab **Work Centers > Device Administration > User Identity Groups**.

Create two **User Identity Groups**:

1. Super_Admin_Group
2. ReadOnly_Group



User Identity Group - (Super_Admin_Group)



User Identity Group - (ReadOnly_Group)

Step 5. (Optional) Add **TACACS+ Policy Set**.

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets**.

Procedure

a. Click **Actions** and **choose** (**Insert new row above**).

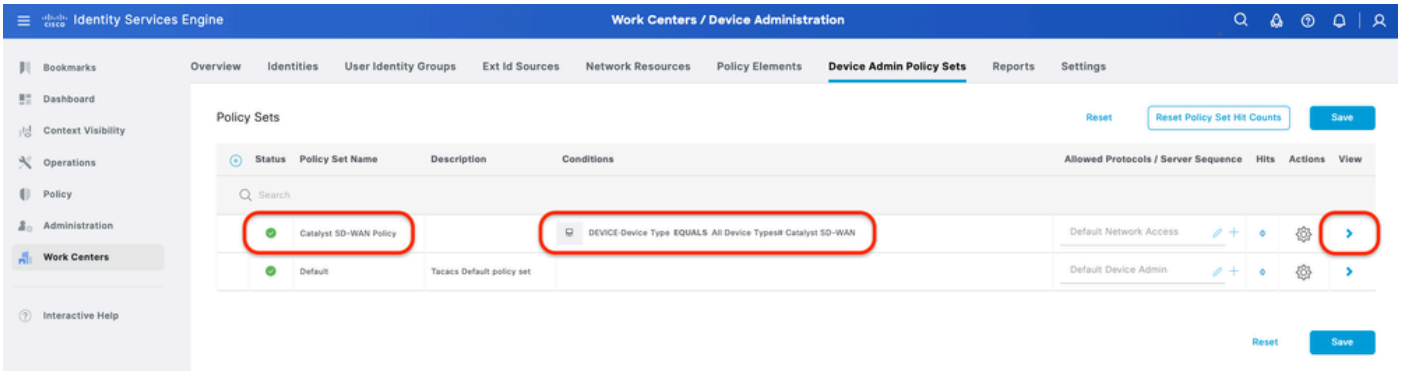
b. Define the **Policy Set name**.

c. Set the Policy Set **Condition** to **Select** Device Type you created previously on (Step 2 > b).

d. Set the **Allowed protocols**.

e. Click **Save.**

f. Click (>) **Policy Set View** to configure authentication and authorization rules.



ISE Policy Set

Step 6. Configure TACACS+ Authentication Policy.

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets > Click (>)**.

Procedure

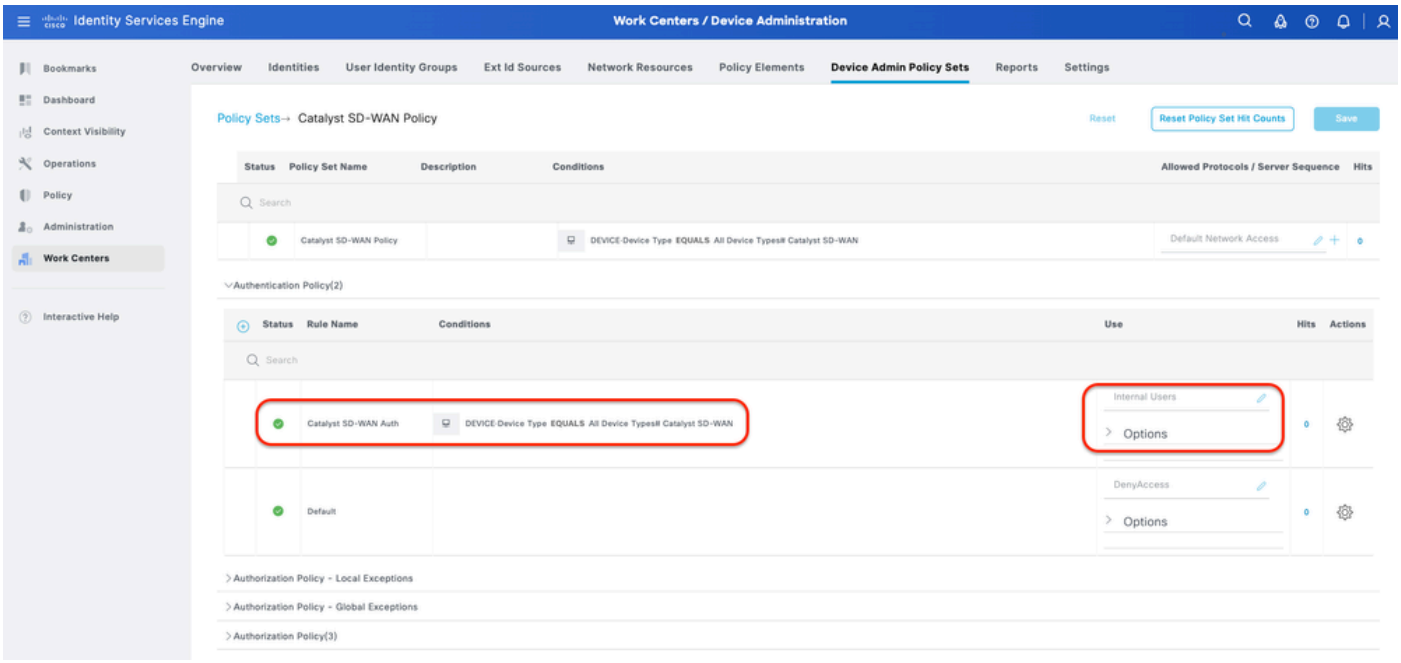
a. Click **Actions** and **choose** (**Insert new row above**).

b. Define the **Authentication Policy name**.

c. Set the Authentication Policy **Condition** and select **Device Type** you created previously on (Step 2 > b).

d. Set the Authentication Policy **Use** for Identity source.

e. Click **Save.**



Authentication Policy

Step 7. Configure TACACS+ Authorization Policy.

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets > Click (>)**.

This step to create Authorization Policy for each Catalyst SD-WAN Role:

- Catalyst SD-WAN Authz (super-admin): super-admin
- Catalyst SD-WAN Authz (readonly): readonly

Procedure

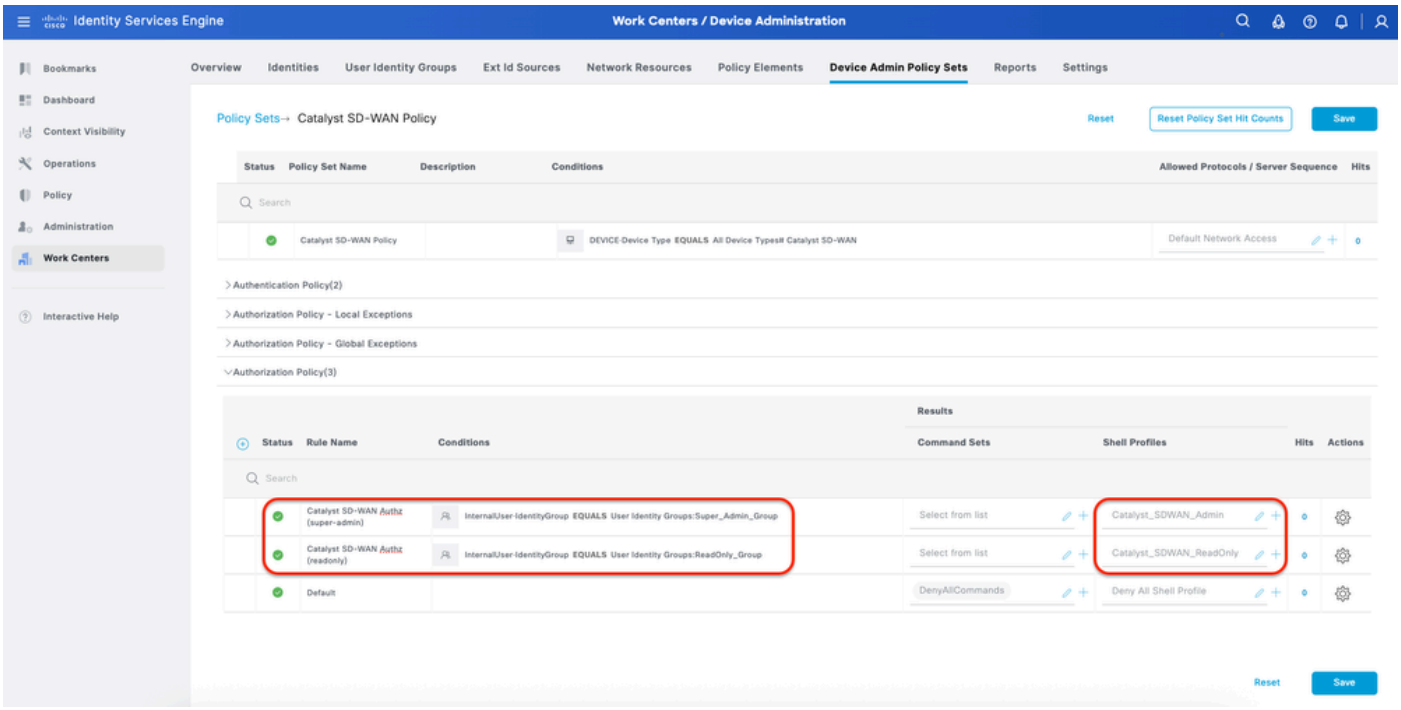
a. Click **Actions** and **choose** (**Insert new row above**).

b. Define the **Authorization Policy name**.

c. Set the Authorization Policy **Condition** and select **User Group** that you created in (Step 4).

d. Set the Authorization Policy**Shell Profiles**and select **TACACS Profile**that you created in (Step 3).

e. Click **Save**.

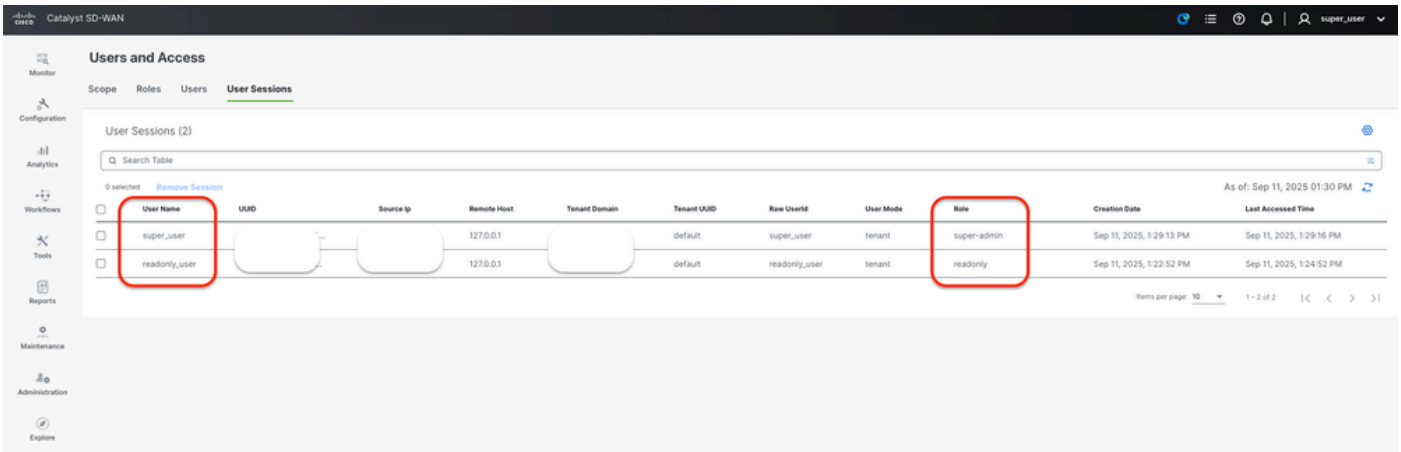


Authorization Policy

Verify TACACS+ Configuration

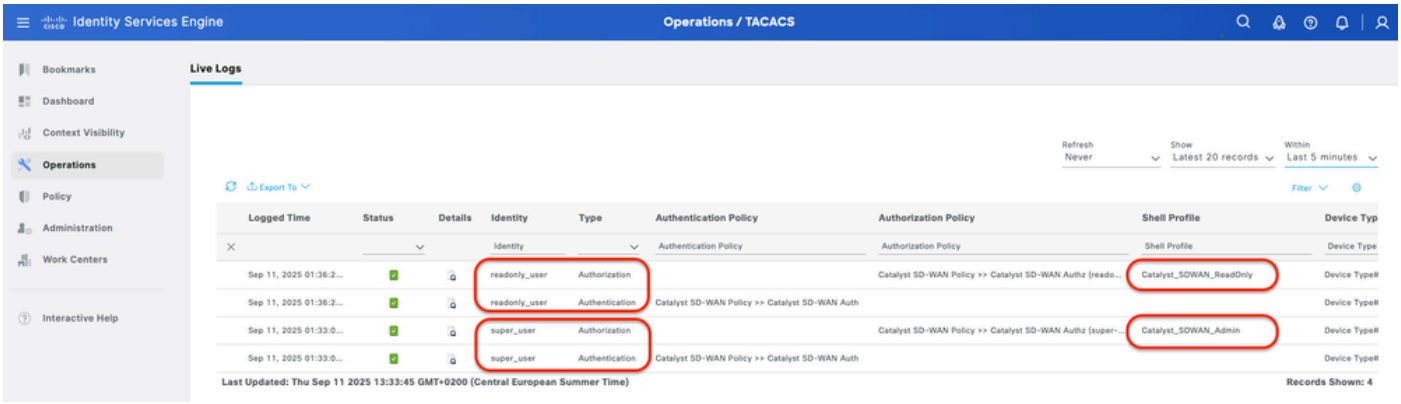
1- Display Catalyst SD-WAS User Sessions **Catalyst SD-WAN: Administration > Users and Access > User Sessions**.

You can view the list of external users who have logged in through RADIUS for the first time. The information that is displayed includes their usernames and roles.



Catalyst SD-WAS User Sessions

2- ISE - TACACS Live-Logs **Operations > TACACS > Live-Logs.**


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

Live-Logs

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; }

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; }

Troubleshoot

There is currently no specific diagnostic information available for this configuration.

References

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