Configuración de ISE como autenticación externa para la GUI de Catalyst SD-WAN

Contenido

Introducción

Este documento describe cómo configurar Cisco Identity Services Engine (ISE) como una autenticación externa para la administración de la GUI de Cisco Catalyst SD-WAN.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- protocolo TACACS+
- Administración de dispositivos de Cisco ISE
- Administración de SD-WAN de Cisco Catalyst
- Evaluación de políticas de Cisco ISE

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Parche 2 de Cisco Identity Services Engine (ISE) versión 3.4
- Cisco Catalyst SD-WAN versión 20.15.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de comenzar

A partir de Cisco vManage Release 20.9.1, se utilizan nuevas etiquetas en la autenticación:

- Viptela-User-Group: para definiciones de grupos de usuarios en lugar de Viptela-Group-Name.
- Viptela-Resource-Group: para definiciones de grupos de recursos.

Configurar - Uso de TACACS+

Configuración de Catalyst SD-WAN mediante TACACS+

Procedimiento

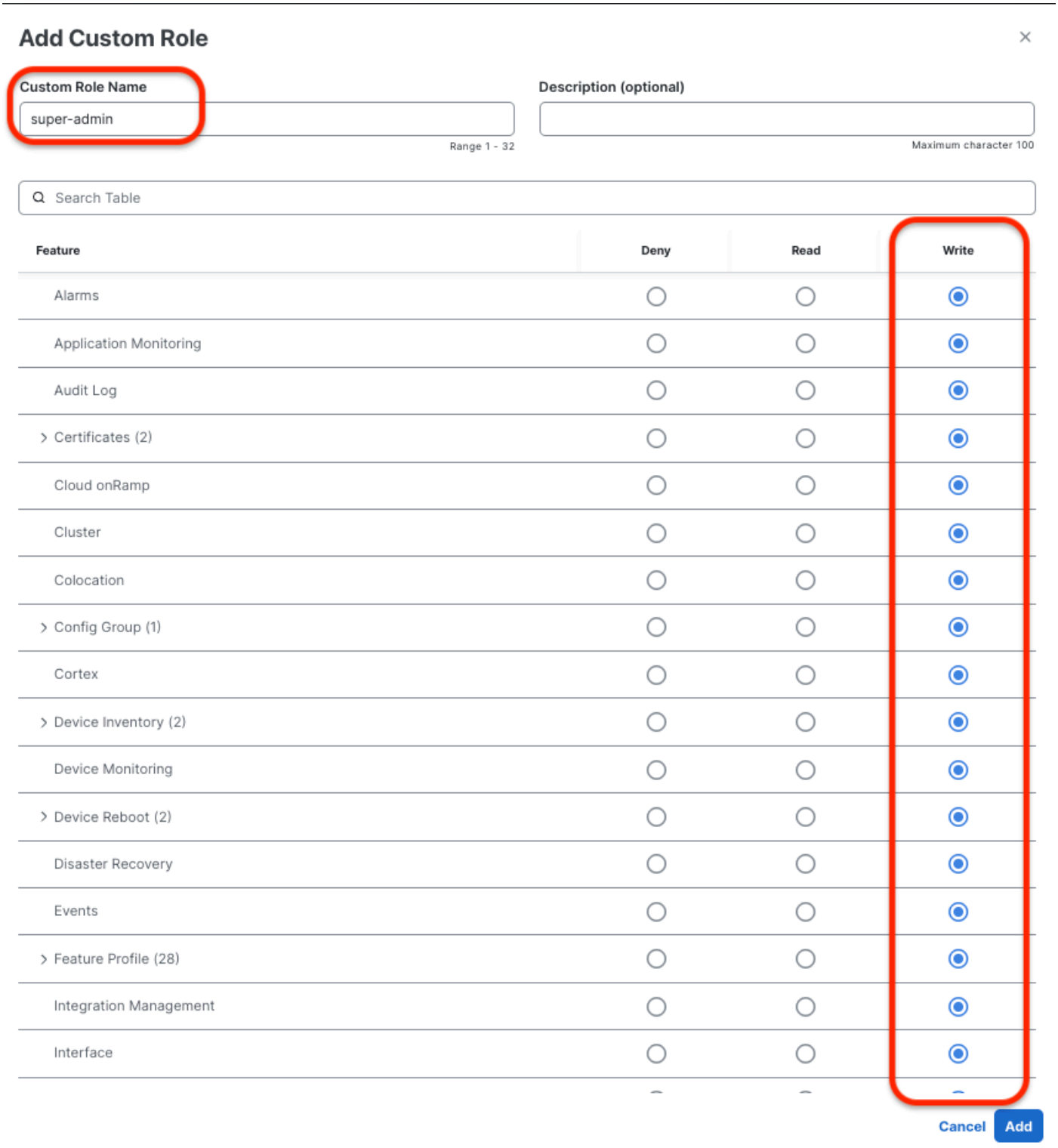
Paso 1. (Opcional) Definir Roles Personalizados.

Configure las funciones personalizadas que satisfagan sus requisitos; en su lugar, puede utilizar las funciones de usuario predeterminadas. Esto se puede hacer desde la pestaña Catalyst SD-WAN: Administration > Users y Access > Roles.

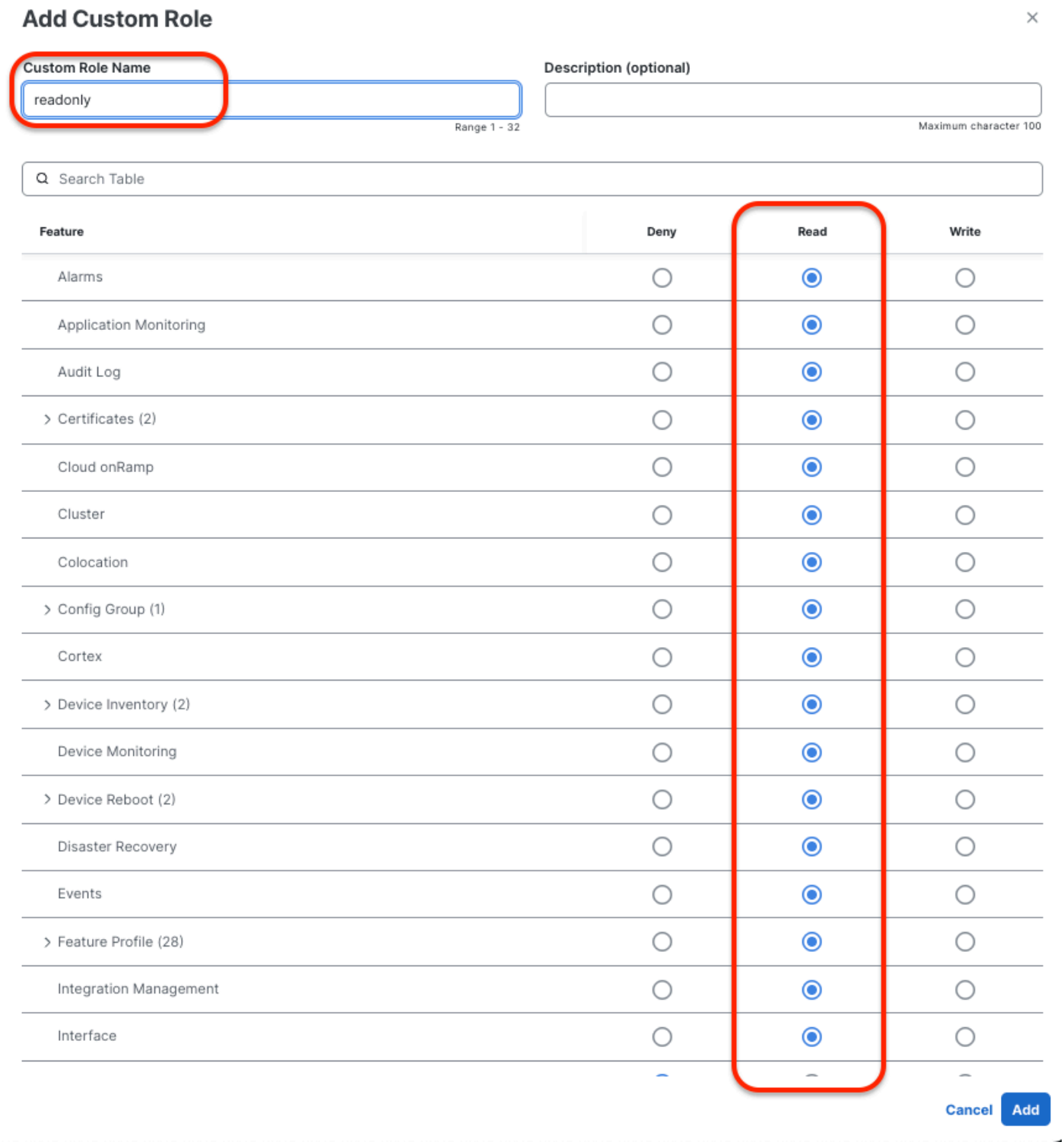
Cree dos funciones personalizadas:

1. Rol de administrador: super-admin
2. Función de sólo lectura: de sólo lectura

Esto se puede hacer desde la pestaña Catalyst SD-WAN: Administration > Users and Access > Roles > Click > Add Role.



Rol de administrador (super-admin)



Función de sólo lectura (sólo lectura)

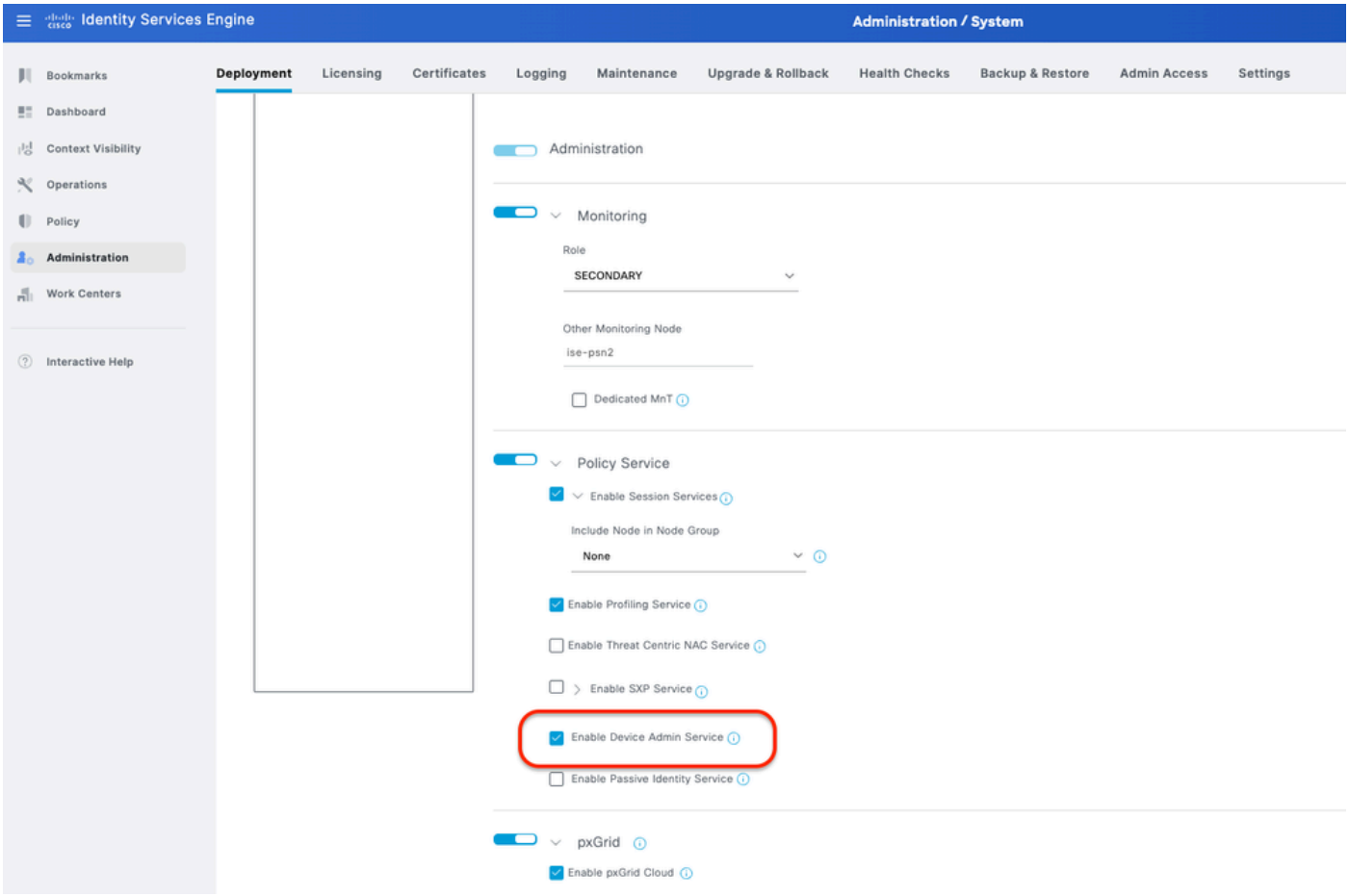
Paso 2. Configure la autenticación externa mediante TACACS+ (CLI).

```
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.
```

CLI de vManager: configuración de TACACS+

Configuración de ISE para TACACS+

Paso 1. Habilite Device Admin Service.
Esto se puede hacer desde la pestaña Administration > System > Deployment >Edit (ISE PSN Node)>Check Enable Device Admin Service.



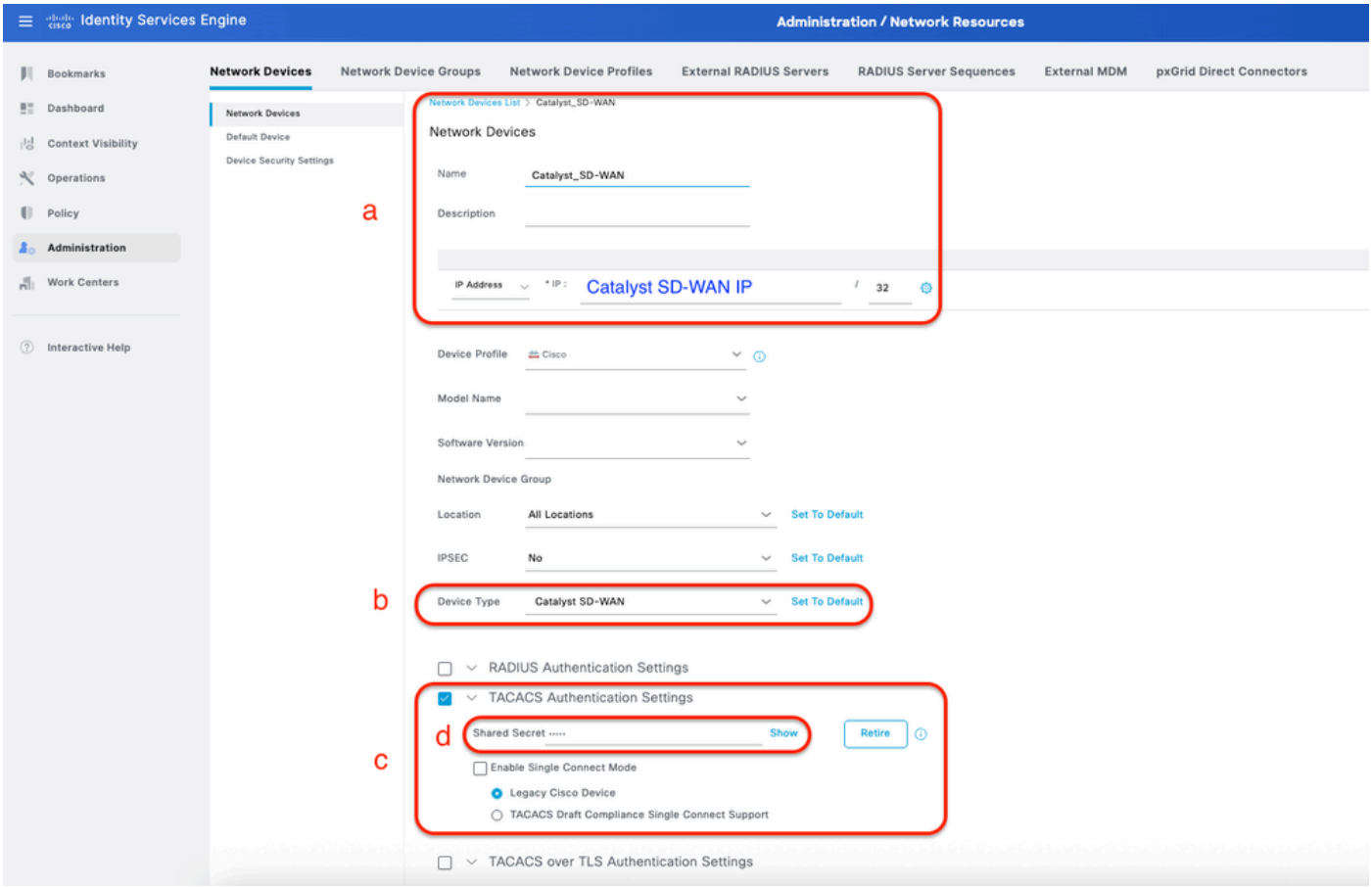
Habilitar servicio de administración de dispositivos

Paso 2. Agregue Catalyst SD-WAN como dispositivo de red en ISE.

Esto se puede hacer desde la pestaña Administration > Network Resources > Network Devices.

Procedimiento

a. Definir (Catalyst SD-WAN) Network Device name e IP.
b. (Opcional) Clasifique el tipo de dispositivo para la condición del conjunto de políticas.
c. Habilite la Configuración de Autenticación de TACACS+.
d. Establezca TACACS+ Shared Secret.



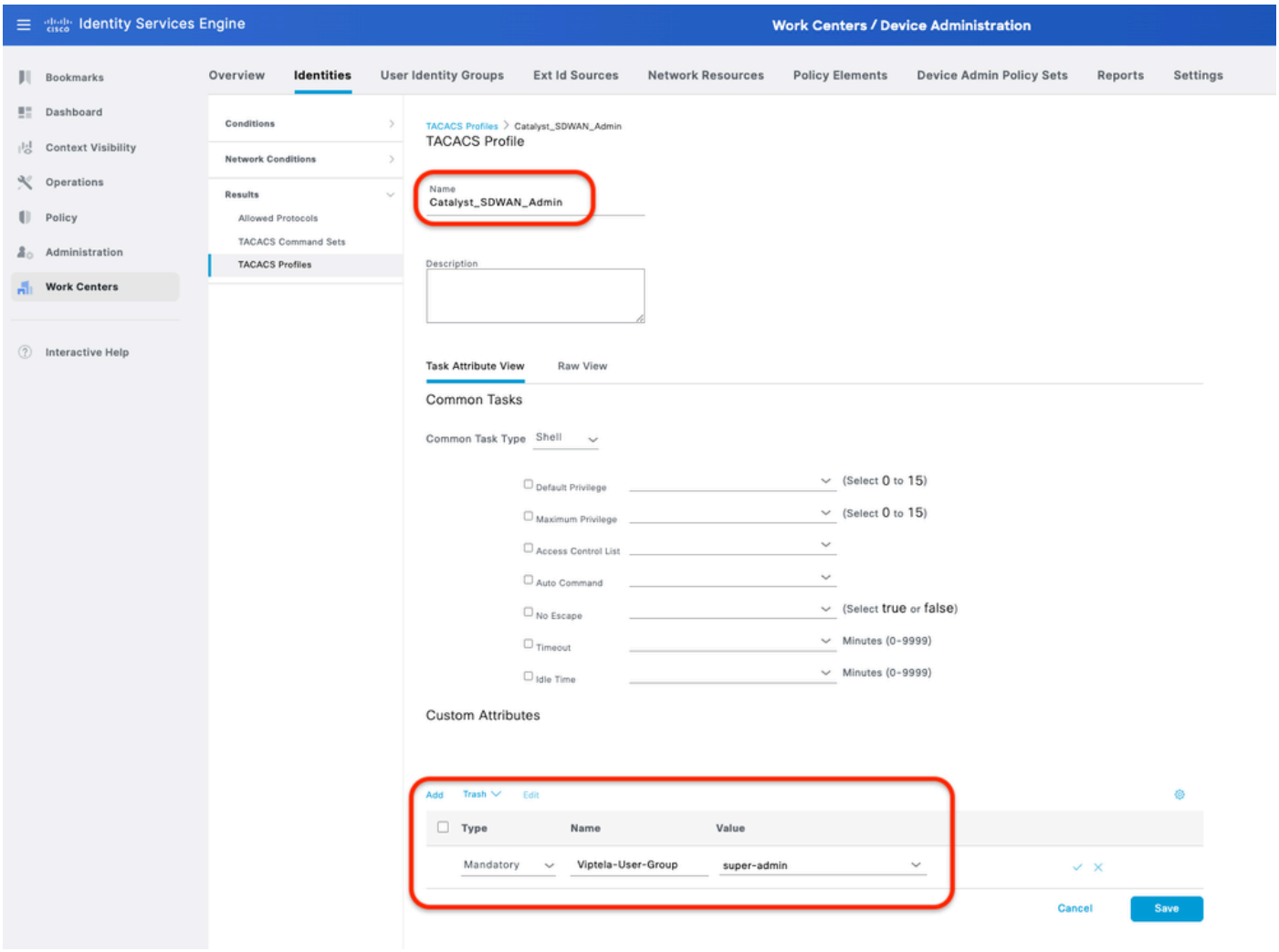
Dispositivo de red ISE (Catalyst SD-WAN) para TACACS+

Paso 3. Crear perfil TACACS+ para cada función de Catalyst SD-WAN.

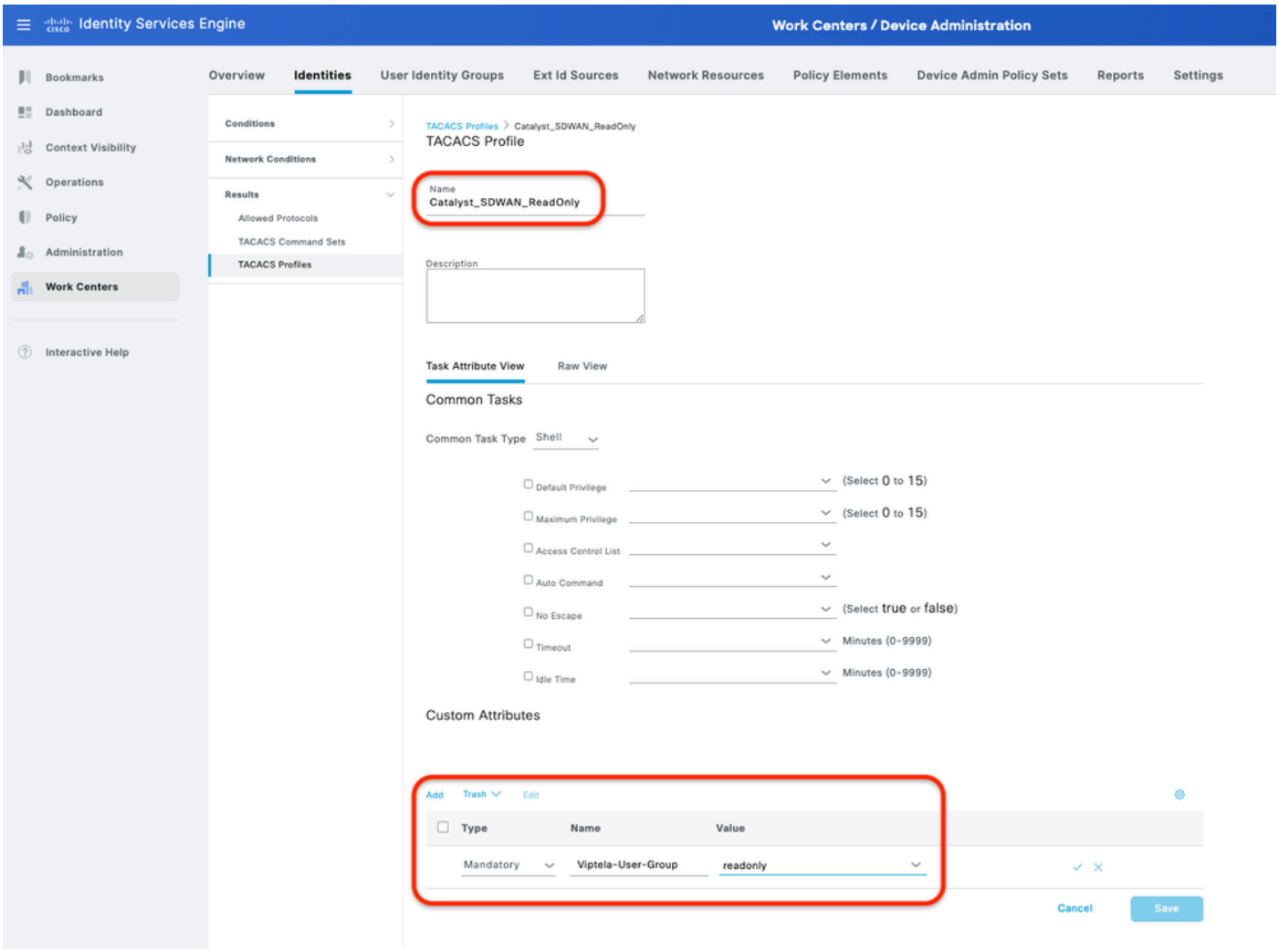
Crear perfiles TACACS+:

1. Catalyst_SDWAN_Admin: Para usuarios superadministradores.
2. Catalyst_SDWAN_ReadOnly: Para usuarios de sólo lectura.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS > Agregar.



Perfil de TACACS+: (Catalyst_SDWAN_Admin)



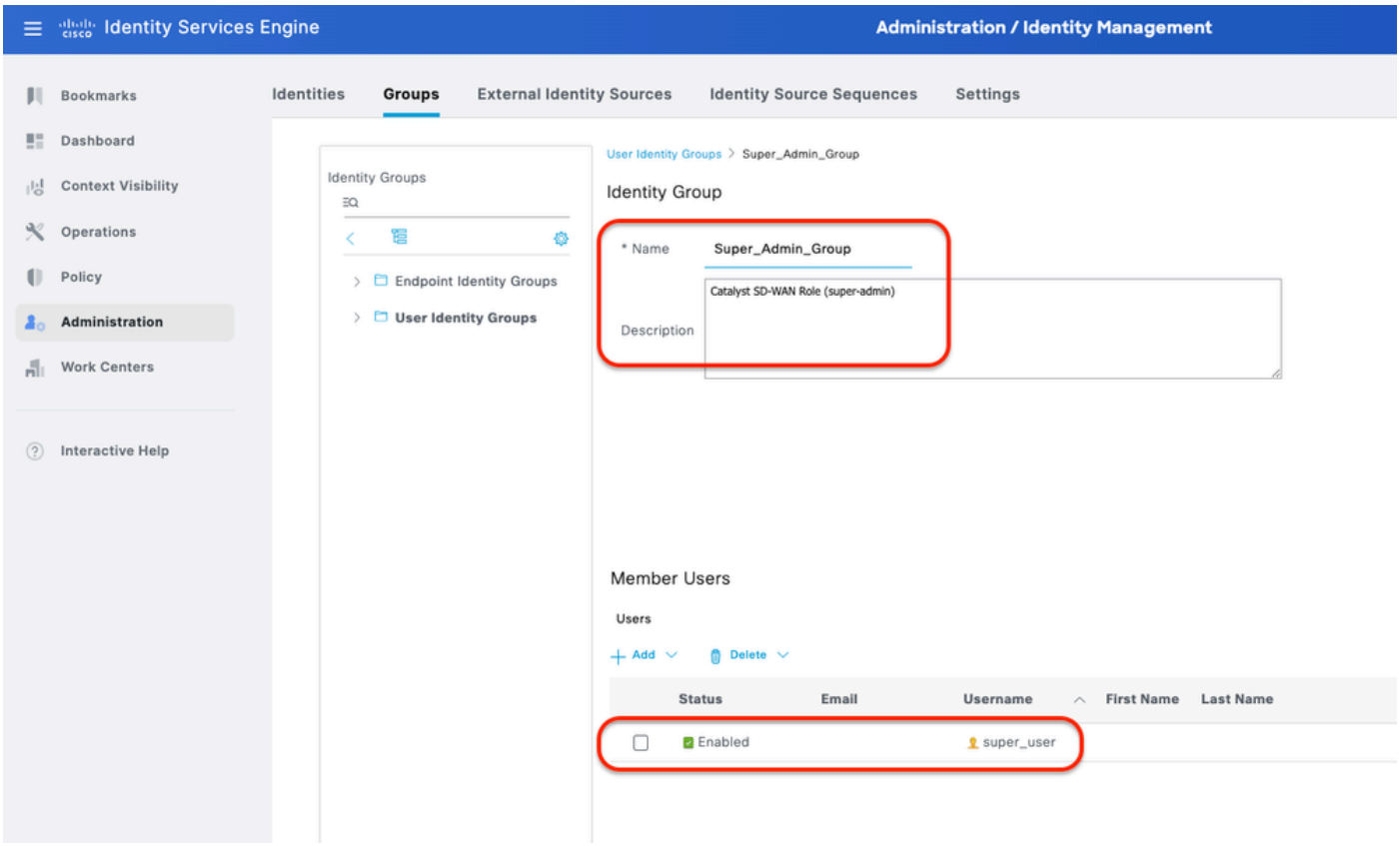
Perfil de TACACS+: (Catalyst_SDWAN_ReadOnly)

Paso 4. Crear grupo de usuarios y agregar usuarios locales como miembro.

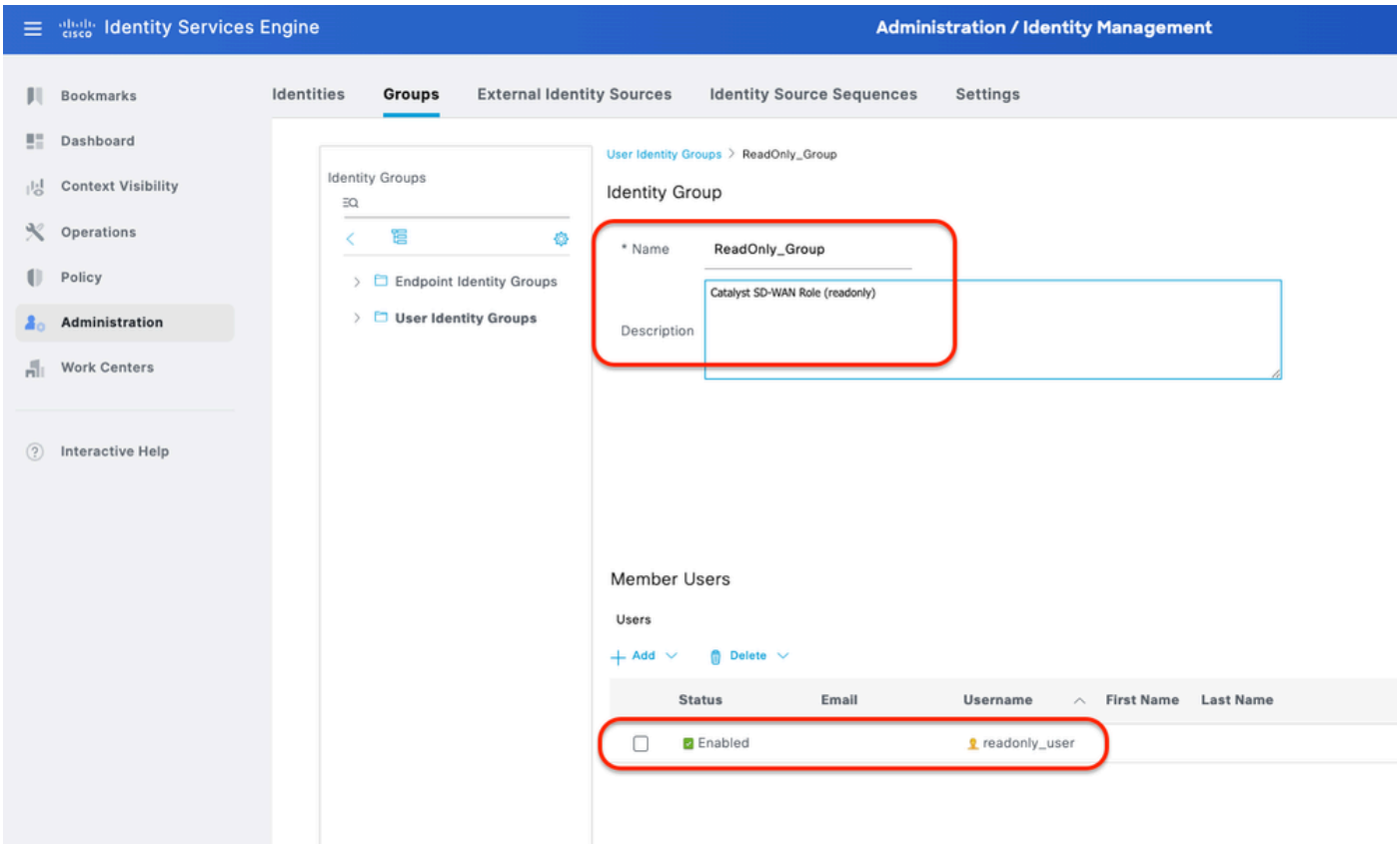
Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Grupos de identidades de usuarios.

Cree dos grupos de identidad de usuario:

1. Super_Admin_Group
2. Grupo_de_sóloLectura



Grupo de identidad de usuario: (Super_Admin_Group)



Grupo de identidades de usuario: (ReadOnly_Group)

Paso 5. (Opcional) Agregar conjunto de políticas TACACS+.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos.

Procedimiento

a. Haga clic en Acciones y elija (Insertar nueva fila encima).

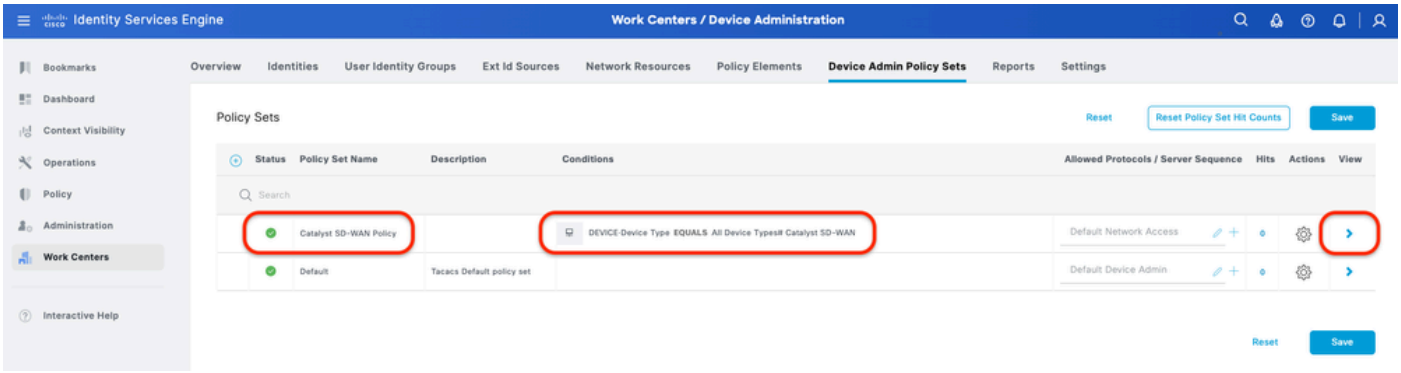
b. Defina el nombre del conjunto de políticas.

c. Establezca la Condición de Conjunto de Políticas en Seleccionar Tipo de Dispositivo que creó anteriormente en (Paso 2 > b).

d. Establezca los protocolos permitidos.

e. Click Save.

f. Haga clic en (>) Vista de conjunto de políticas para configurar las reglas de autenticación y autorización.



Conjunto de políticas de ISE

Paso 6. Configure la Política de Autenticación de TACACS+.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos > Haga clic en (>).

Procedimiento

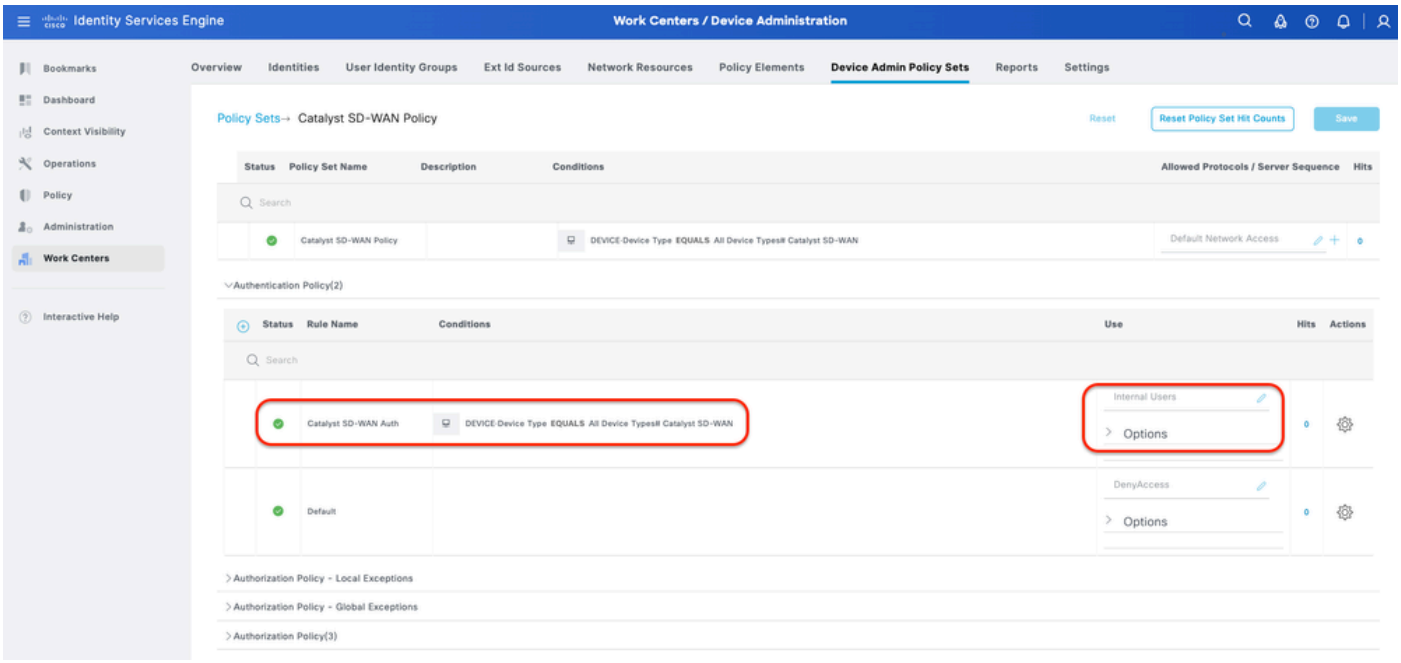
a. Haga clic en Acciones y elija (Insertar nueva fila encima).

b. Defina el nombre de la política de autenticación.

c. Establezca la Condición de la Política de Autenticación y seleccione el Tipo de Dispositivo que creó anteriormente en (Paso 2 > b).

d. Establezca el Uso de la política de autenticación para el origen de identidad.

e. Click Save.



Política de autenticación

Paso 7. Configure la Política de Autorización de TACACS+.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos > Haga clic en (>).

Este paso para crear una política de autorización para cada función de Catalyst SD-WAN:

- Catalyst SD-WAN Authz (super-admin): super-admin
- Catalyst SD-WAN Authz (solo lectura): de sólo lectura

Procedimiento

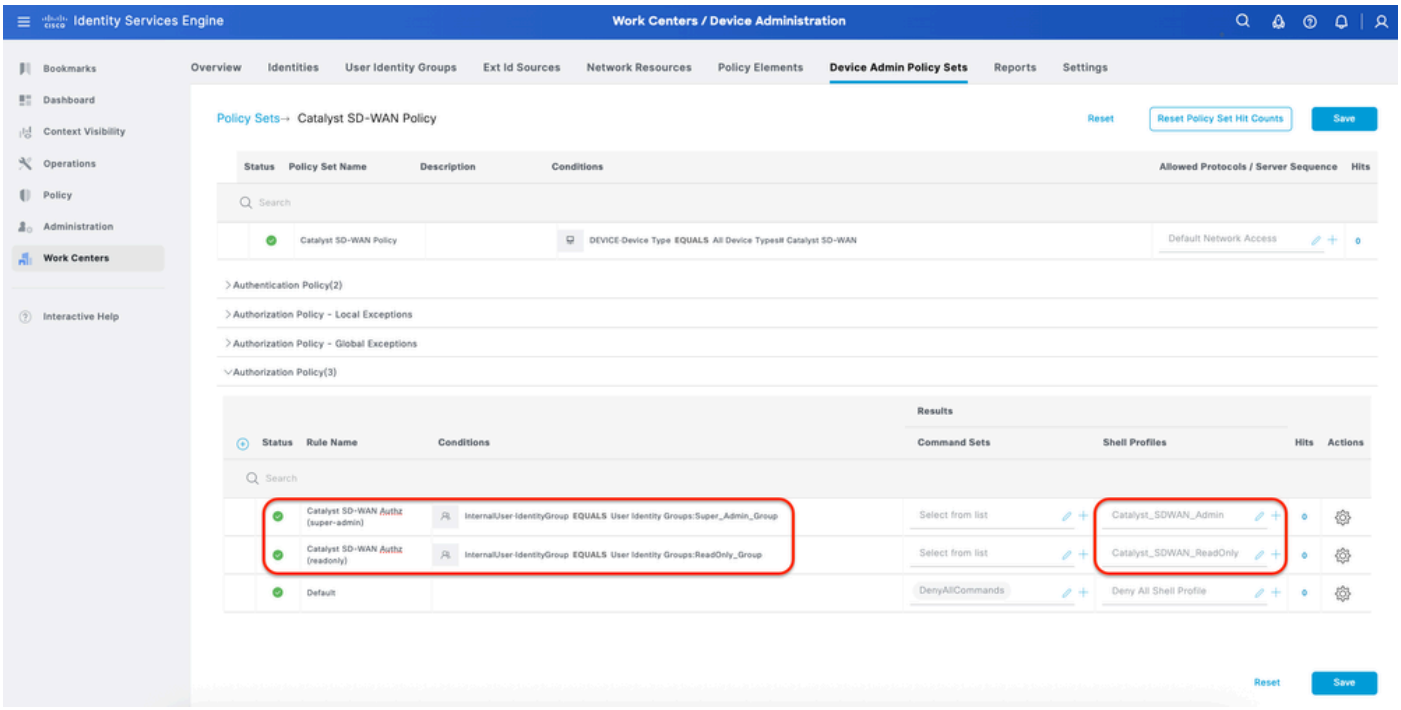
a. Haga clic en Acciones y elija (Insertar nueva fila encima).

b. Defina el nombre de la política de autorización.

c. Establezca la Condición de Política de Autorización y seleccione el Grupo de Usuarios que creó en (Paso 4).

d. Establezca los perfiles de Authorization PolicyShell y seleccione el perfil TACACS que creó en (Paso 3).

e. Click Save.

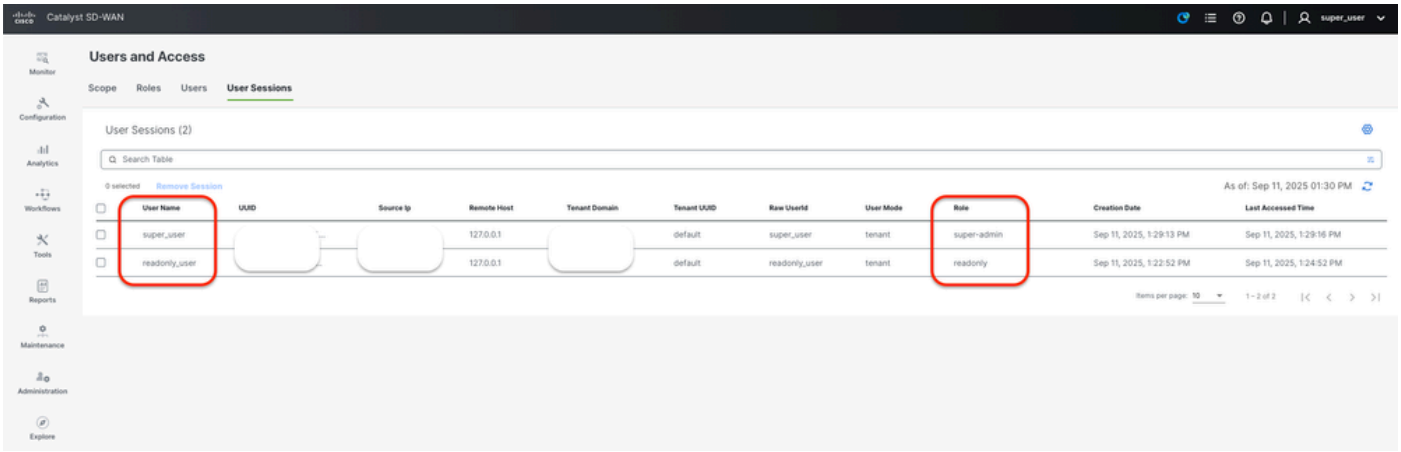


Política de autorización

Verificar configuración de TACACS+

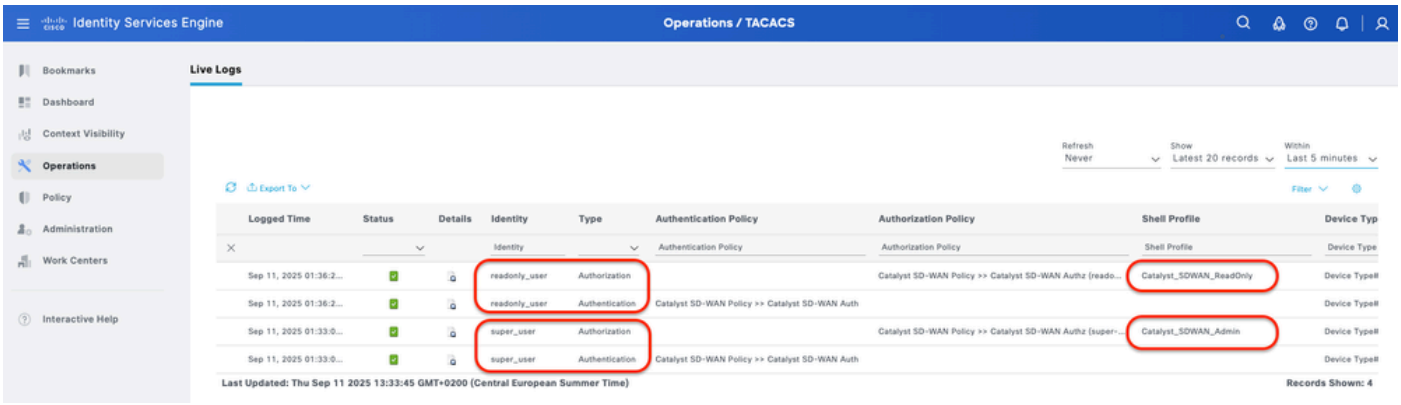
1- Mostrar sesiones de usuario de Catalyst SD-WAS Catalyst SD-WAN: Administration > Users y Access > User Sessions.

Puede ver la lista de usuarios externos que han iniciado sesión a través de RADIUS por primera vez. La información que se muestra incluye sus nombres de usuario y roles.



Sesiones de usuario de Catalyst SD-WAS

2- ISE - Operaciones de Live-Logs de TACACS > 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; }

Live-Logs detallados: (solo lectura)

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

Actualmente no hay información de diagnóstico específica disponible para esta configuración.

Referencias

- Guía del administrador de Cisco Identity Services Engine, versión 3.4
- Guía de Configuración de Interfaces y Sistemas SD-WAN de Cisco Catalyst, Cisco IOS XE Catalyst SD-WAN Release 17.x

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).