Configurar o ISE como uma autenticação externa para a GUI do Catalyst SD-WAN

Contents

Introdução

Este documento descreve como configurar o Cisco Identity Services Engine(ISE) como uma autenticação externa para a administração da GUI do Cisco Catalyst SD-WAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha o conhecimento destes tópicos:

- protocolo TACACS+
- Administração de dispositivos do Cisco ISE
- Administração do Cisco Catalyst SD-WAN
- Avaliação de política do Cisco ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Antes de Começar

A partir do Cisco vManage versão 20.9.1, novas marcas são usadas na autenticação:

- Viptela-User-Group: para definições de grupo de usuários em vez de Viptela-Group-Name.
- Viptela-Resource-Group: para definições de grupos de recursos.

Configurar - Usando TACACS+

Configurar o Catalyst SD-WAN usando TACACS+

Procedimento

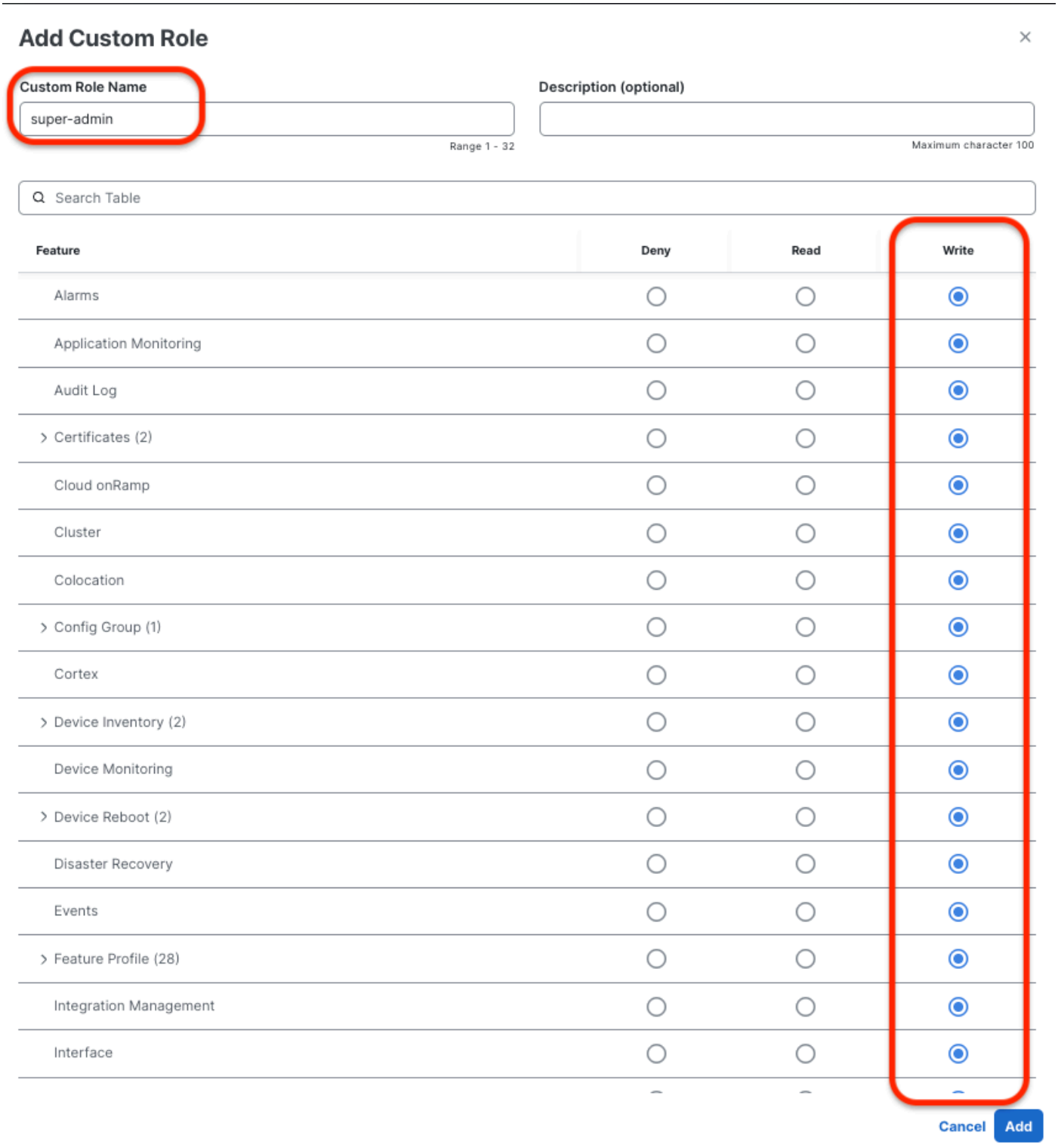
Etapa 1. (Opcional) Definir Funções Personalizadas.

Configure suas funções personalizadas que atendam a seus requisitos. Em vez disso, você pode usar as funções de usuário padrão. Isso pode ser feito na guia Catalyst SD-WAN: Administração > Usuários e Acesso > Funções.

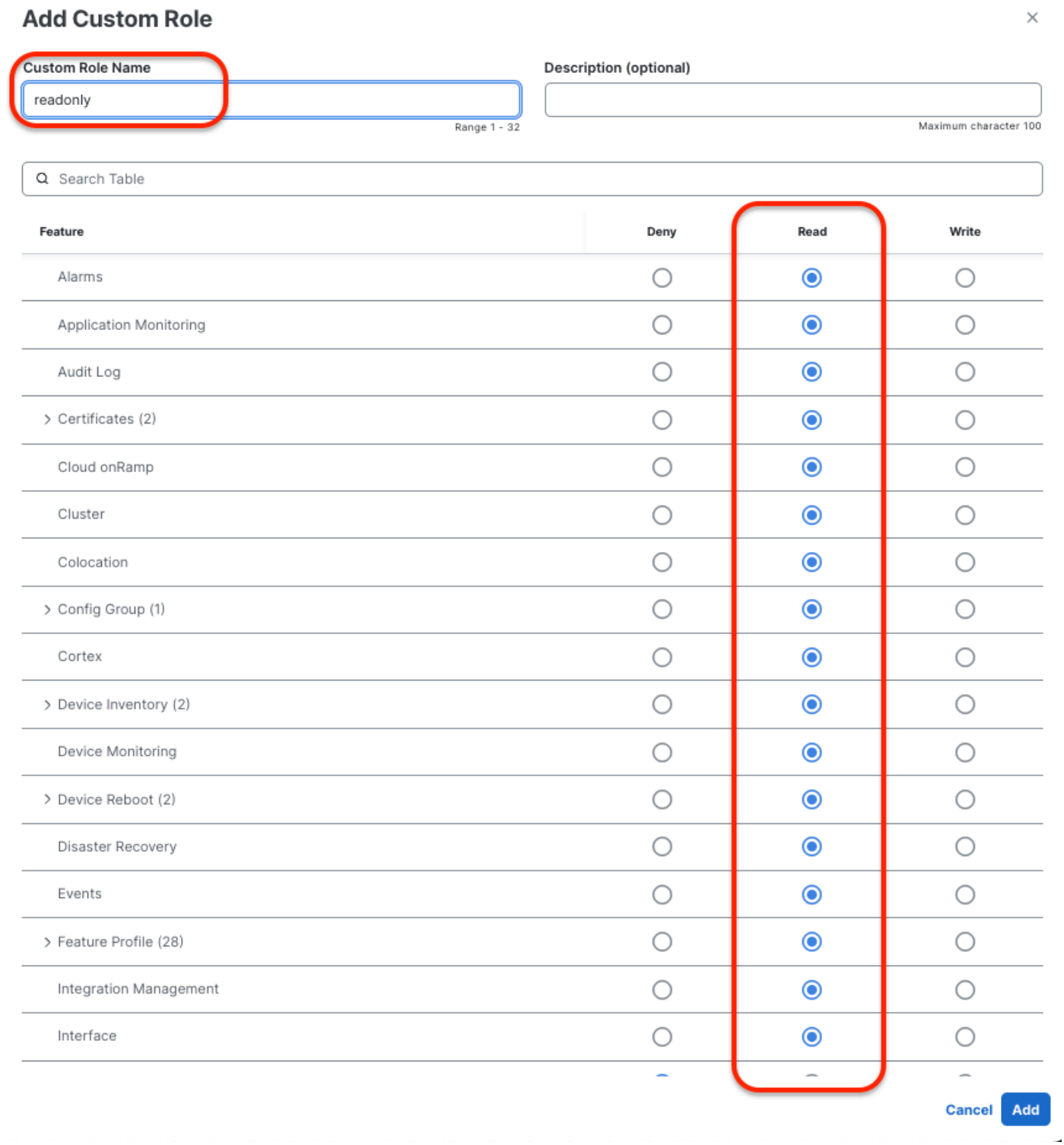
Crie duas funções personalizadas:

1. Função do administrador: super-admin
2. Função somente leitura: somente leitura

Isso pode ser feito na guia Catalyst SD-WAN: Administração > Usuários e Acesso > Funções > Clique > Adicionar Função.



Função do administrador (superadministrador)



Função somente leitura (somente leitura)

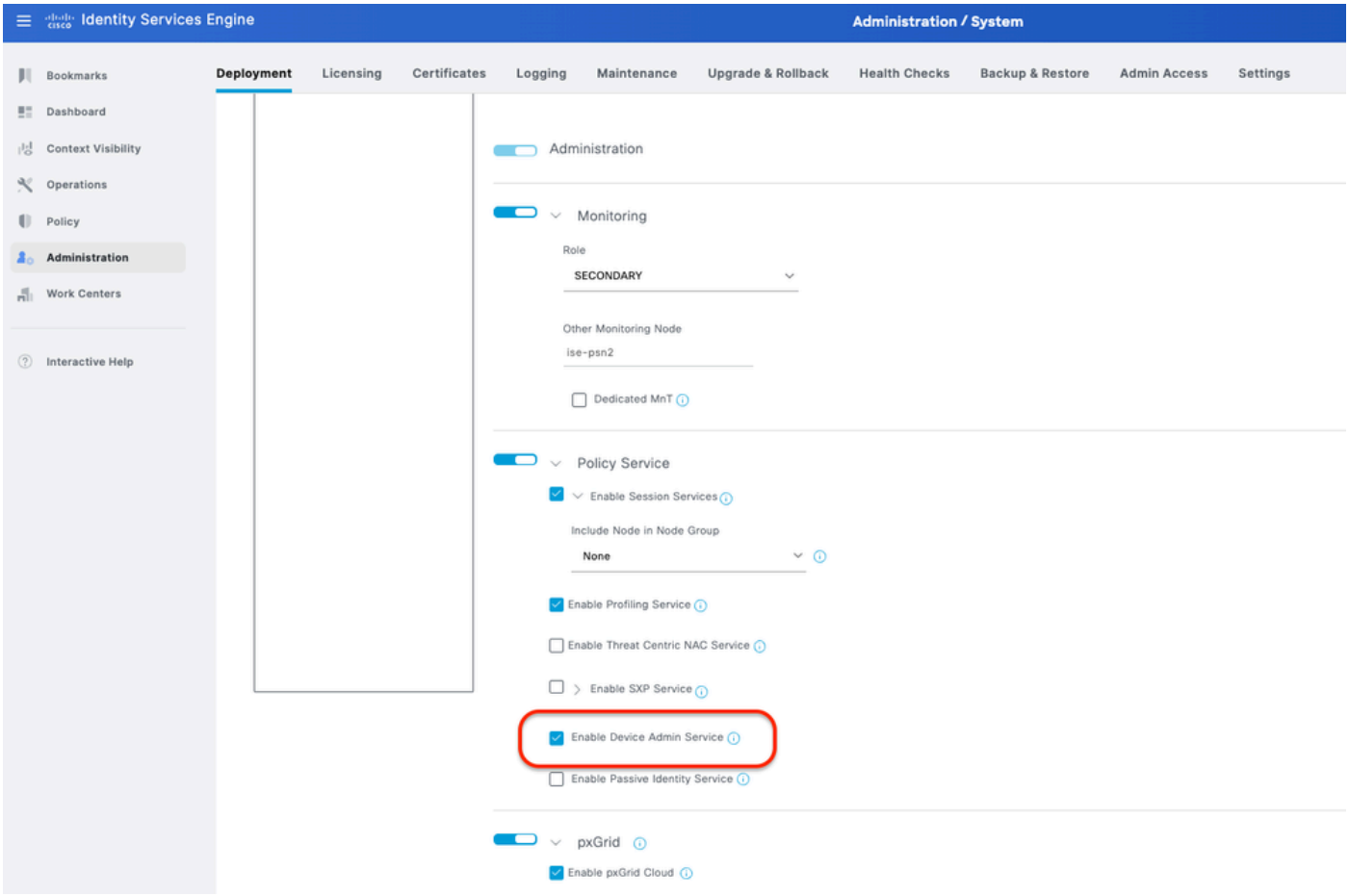
Etapa 2. Configurar a autenticação externa usando TACACS+ (CLI).

```
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.
```

vManager CLI - Configuração TACACS+

Configurar ISE para TACACS+

Etapa 1. Ativar o Device Admin Service.
Isso pode ser feito na guia Administration > System > Deployment >Edit (ISE PSN Node)>Check Enable Device Admin Service.



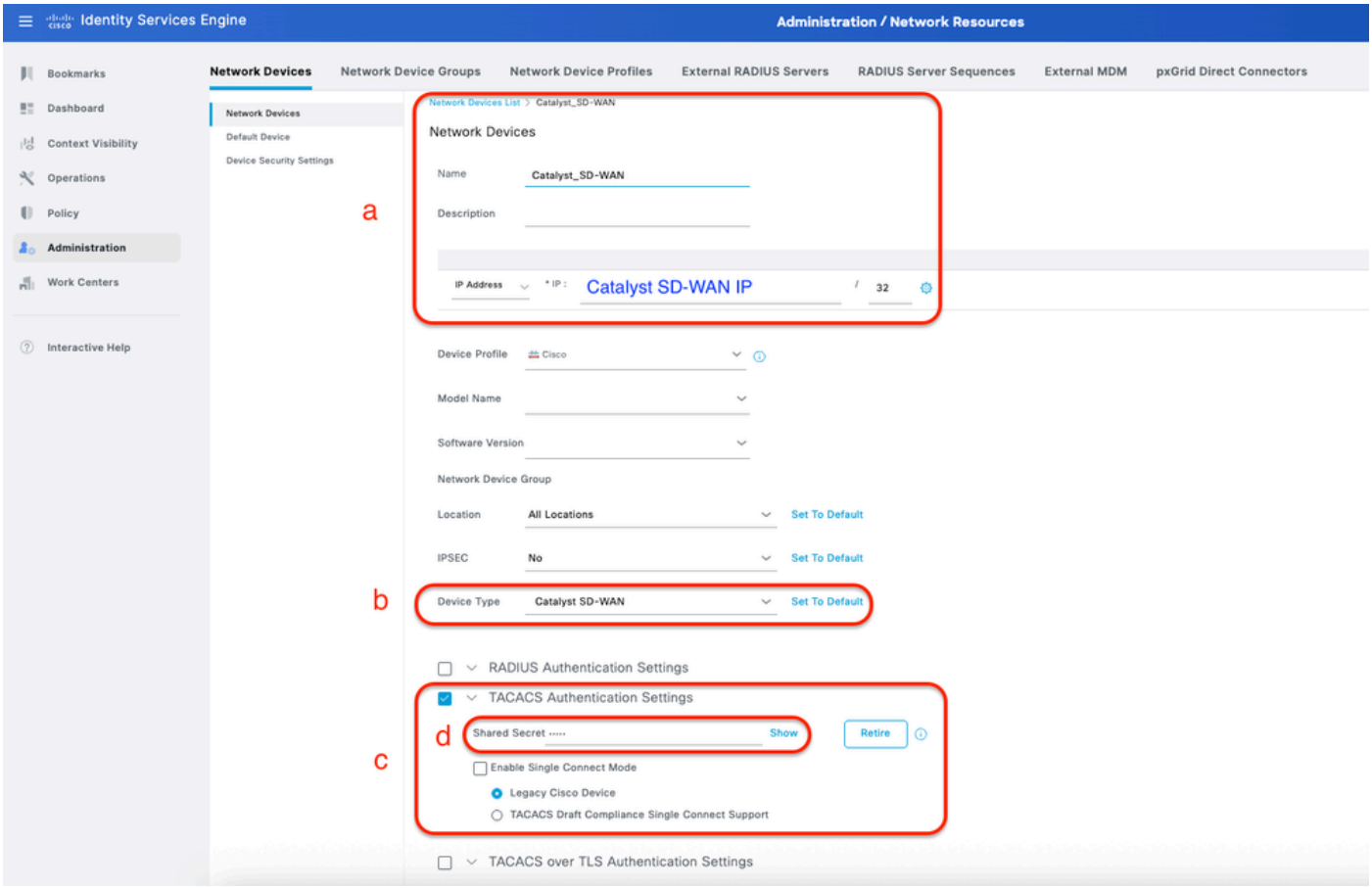
Habilitar Serviço de Administração de Dispositivo

Etapa 2. Adicionar o Catalyst SD-WAN como um dispositivo de rede no ISE.

Isso pode ser feito na guia Administration > Network Resources > Network Devices.

Procedimento

a. Defina o nome (Catalyst SD-WAN) do dispositivo de rede e o IP.
b. (Opcional) Classifique o tipo de dispositivo para a condição do conjunto de políticas.
c. Ative TACACS+ Authentication Settings.
d. Defina TACACS+ Shared Secret.



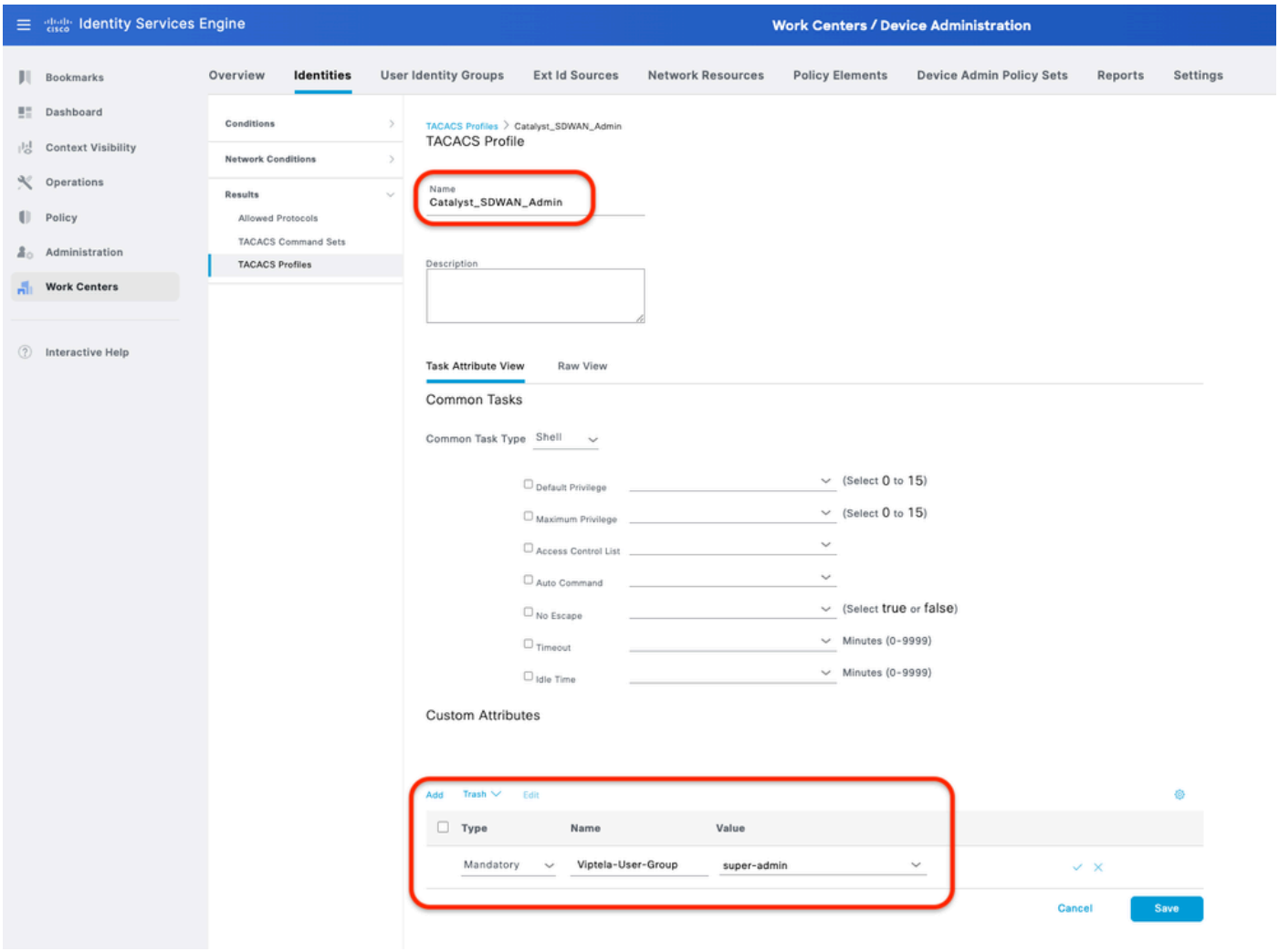
Dispositivo de rede ISE (Catalyst SD-WAN) para TACACS+

Etapa 3. Criar Perfil TACACS+ para cada função do Catalyst SD-WAN.

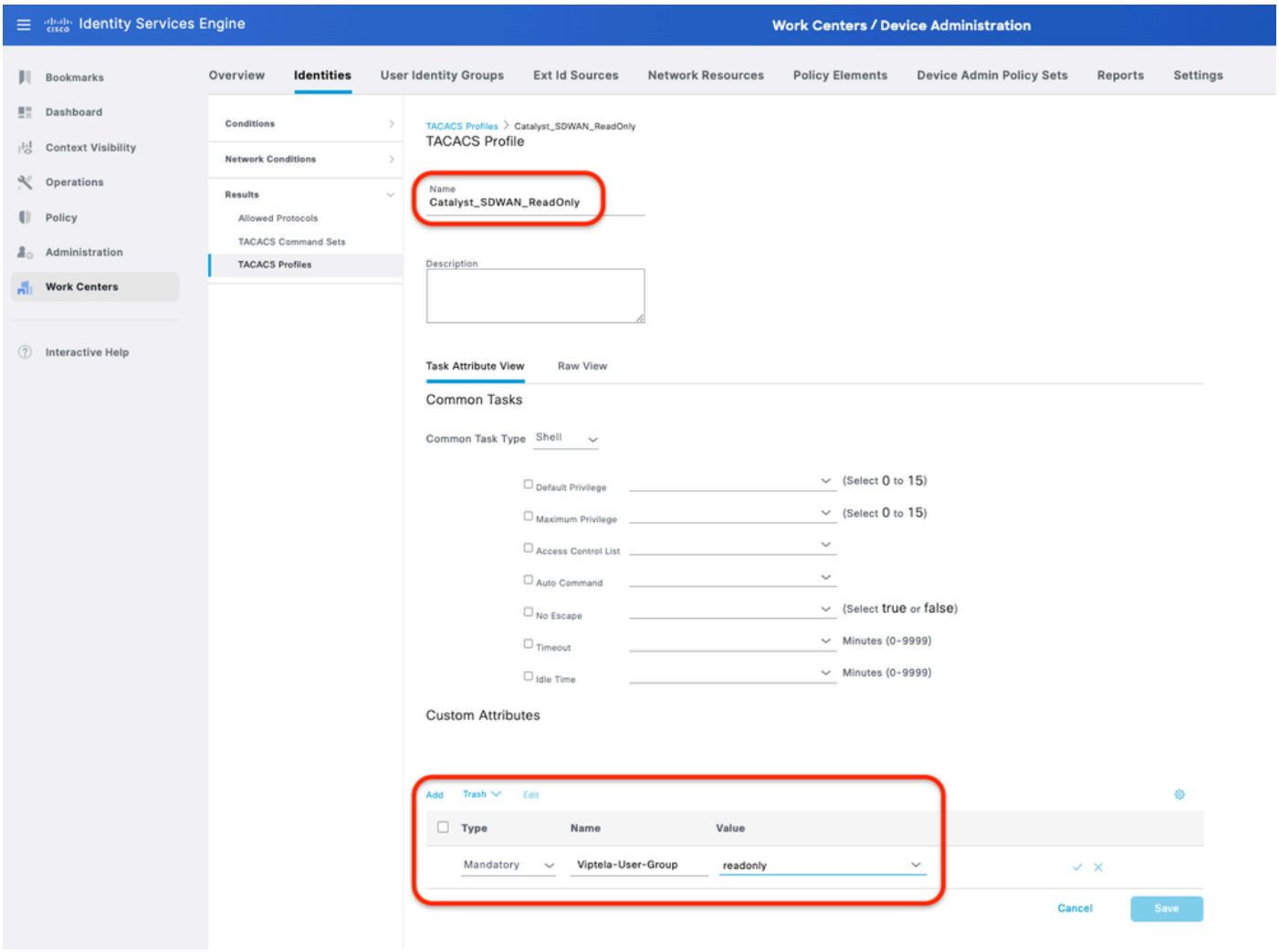
Criar perfis TACACS+:

1. Catalyst_SDWAN_Admin: Para usuários Super Admin.
2. Catalyst_SDWAN_ReadOnly: Para usuários somente leitura.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS > Adicionar.



Perfil TACACS+ - (Catalyst_SDWAN_Admin)



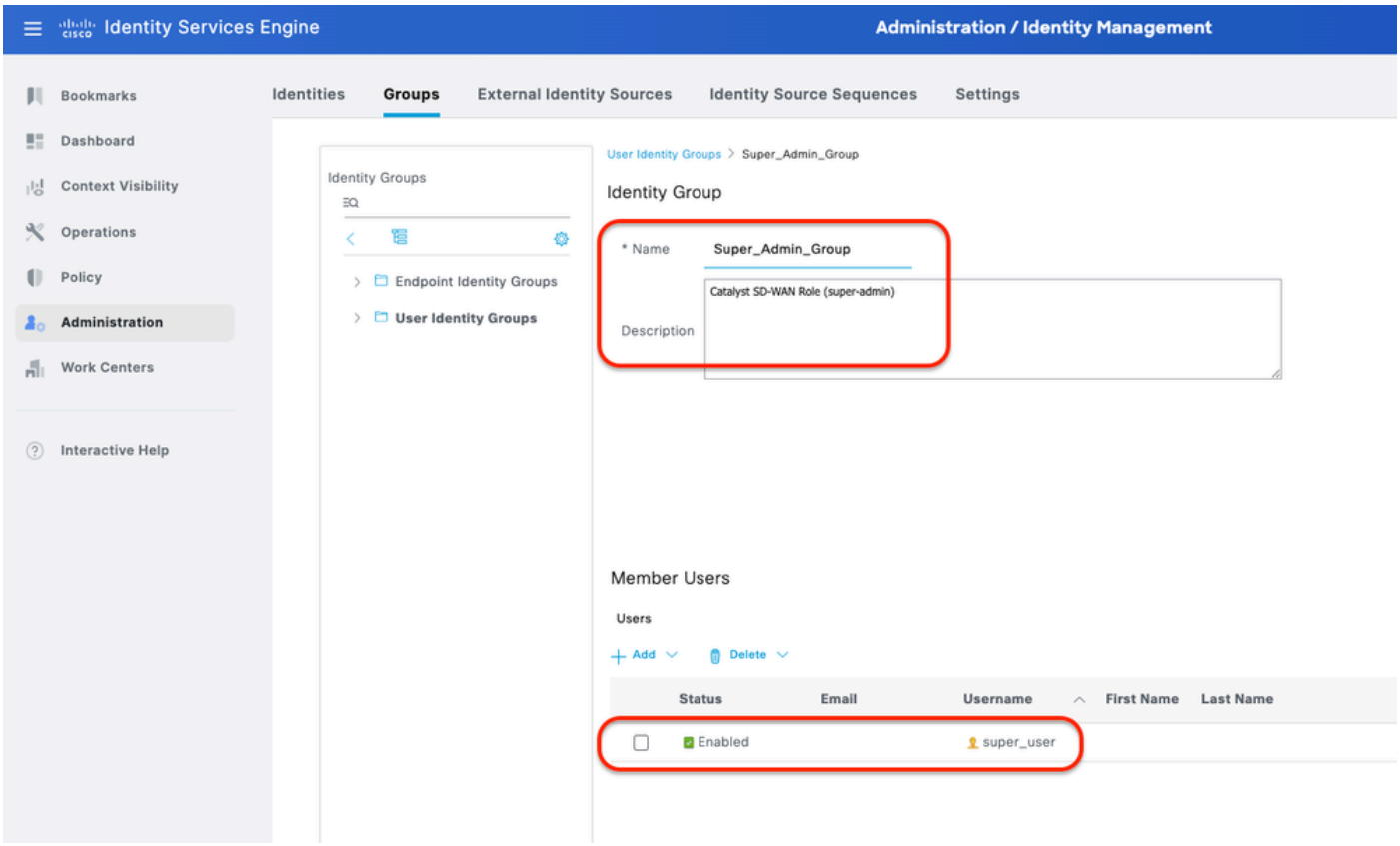
Perfil TACACS+ - (Catalyst_SDWAN_ReadOnly)

Etapa 4. Criar Grupo de Usuários adicionar Usuários Locais como membro.

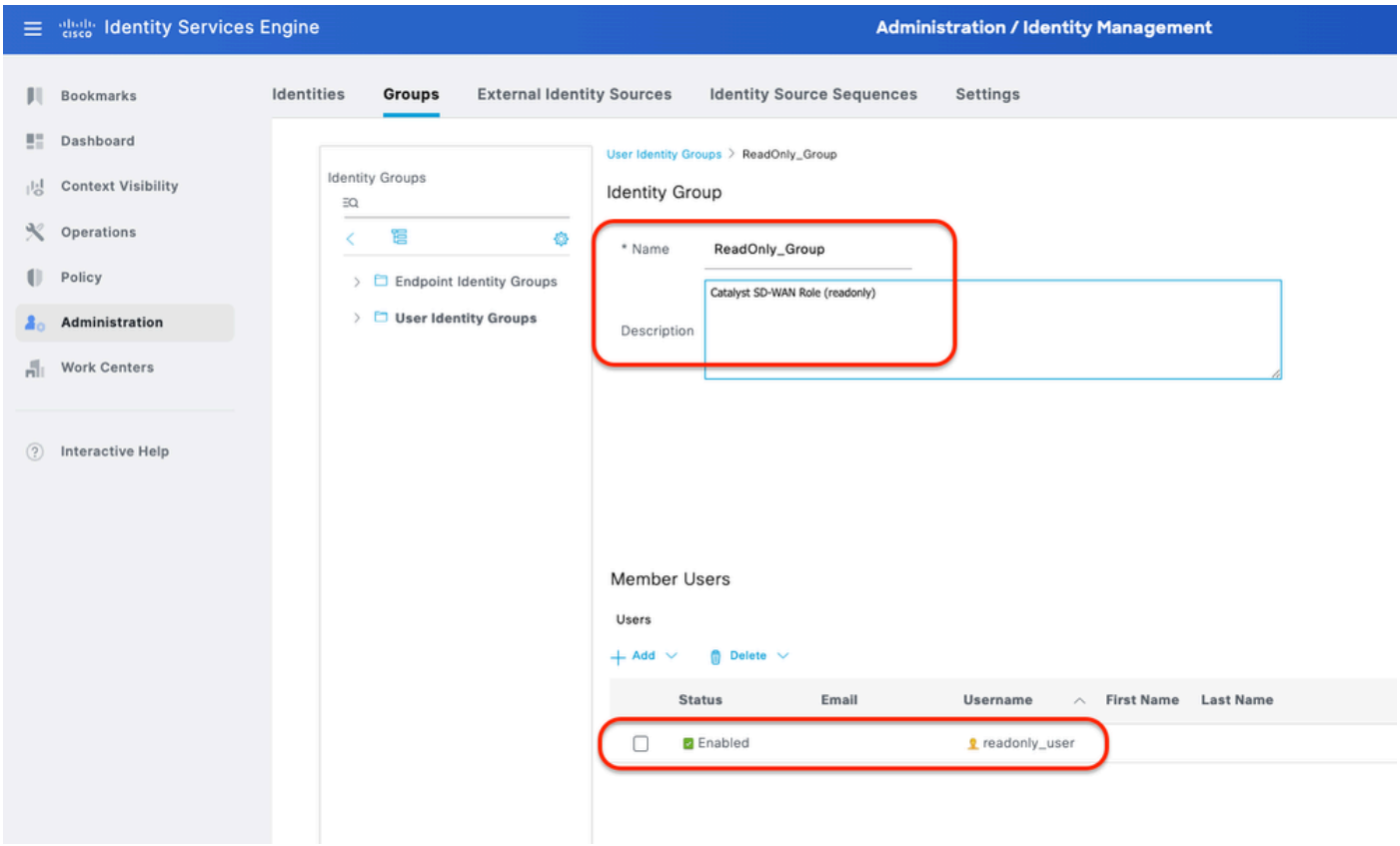
Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Grupos de identidade de usuário.

Crie dois grupos de identidade de usuário:

1. Super_Admin_Group
2. ReadOnly_Group



Grupo de Identidade de Usuário - (Super_Admin_Group)



Grupo de Identidade de Usuário - (ReadOnly_Group)

Etapa 5. (Opcional) Adicione o conjunto de políticas TACACS+.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Conjuntos de diretivas de administração de dispositivo.

Procedimento

a. Clique em Ações e escolha (Inserir nova linha acima).

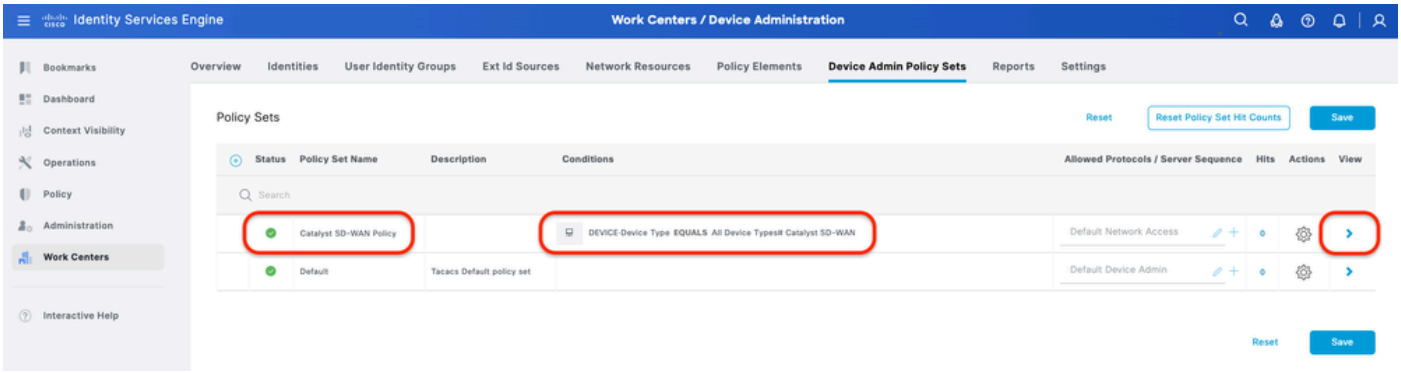
b. Defina o nome do Conjunto de políticas.

c. Defina a condição de definição de política para Selecionar tipo de dispositivo criado anteriormente em (Etapa 2 > b).

d. Defina os protocolos permitidos.

e. Click Save.

f. Clique em (>) Exibição do conjunto de políticas para configurar as regras de autenticação e autorização.



Conjunto de políticas do ISE

Etapa 6. Configurar a política de autenticação TACACS+.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Conjuntos de diretivas de administração de dispositivo > Clique em (>).

Procedimento

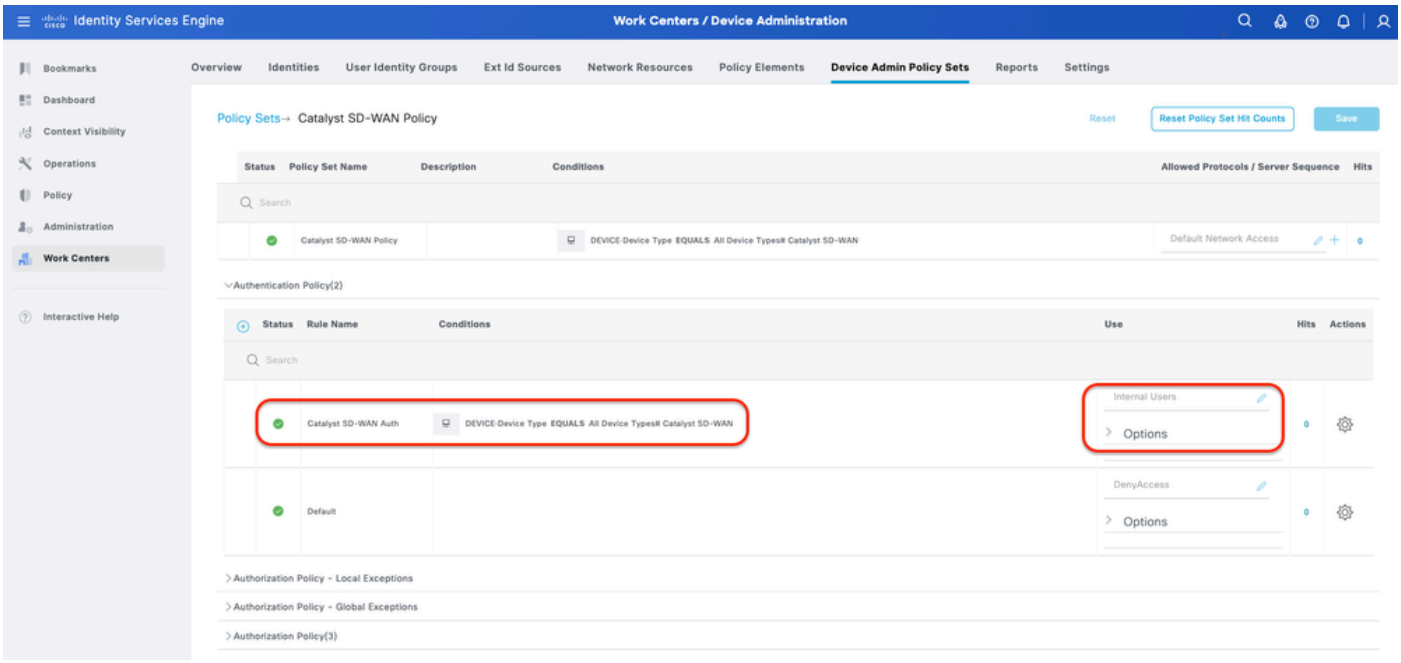
a. Clique em Ações e escolha (Inserir nova linha acima).

b. Defina o nome da política de autenticação.

c. Defina Authentication Policy Condition e selecione Device Type criado anteriormente em (Etapa 2 > b).

d. Defina a Política de autenticação Usar para a origem da Identidade.

e. Click Save.



Política de autenticação

Etapa 7. Configurar a política de autorização TACACS+.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Conjuntos de diretivas de administração de dispositivo > Clique em (>).

Esta etapa para criar a Política de Autorização para cada Função do Catalyst SD-WAN:

- Catalyst SD-WAN Authz (superadministrador): super-admin
- Catalyst SD-WAN Authz (somente leitura): somente leitura

Procedimento

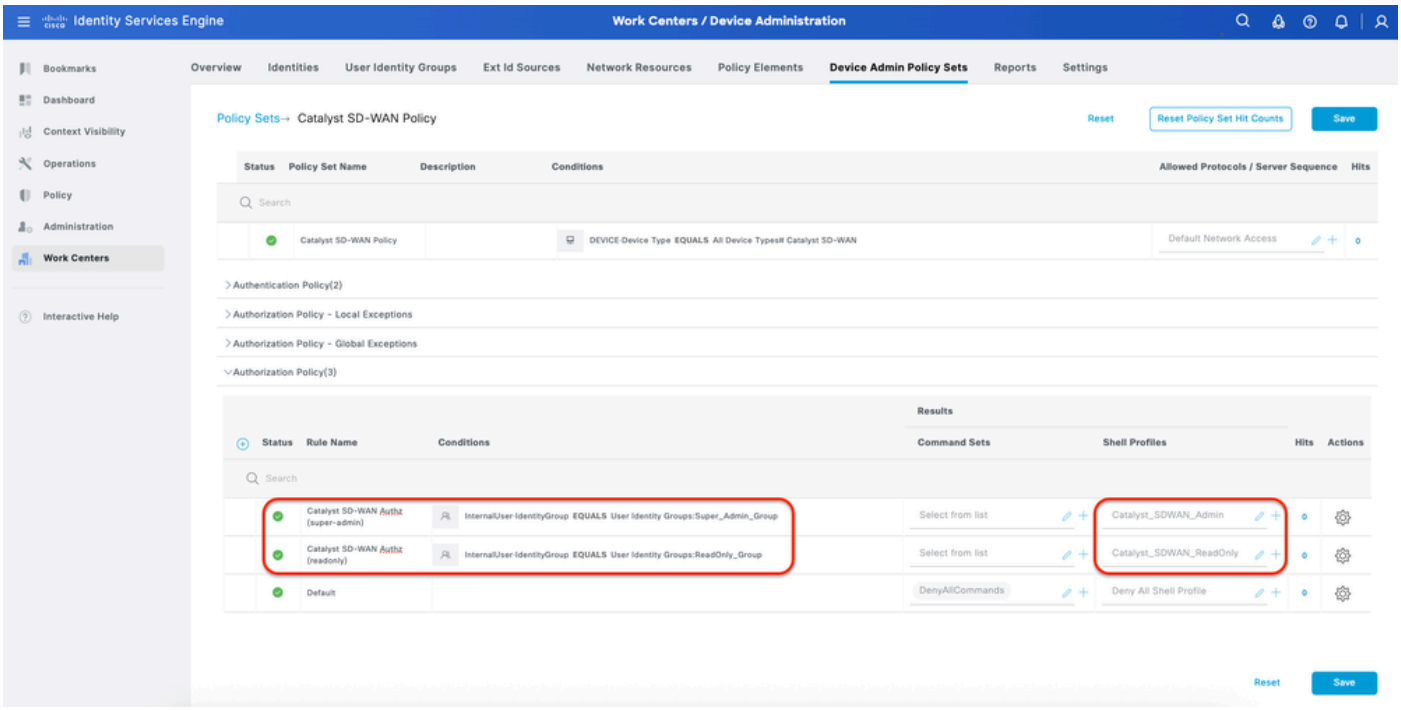
a. Clique em Ações e escolha (Inserir nova linha acima).

b. Defina o nome da Diretiva de Autorização.

c. Defina a Condição da diretiva de autorização e selecione o Grupo de usuários criado em (Etapa 4).

d. Defina os perfis do Authorization PolicyShell e selecione TACACS Profile que você criou em (Etapa 3).

e. Click Save.

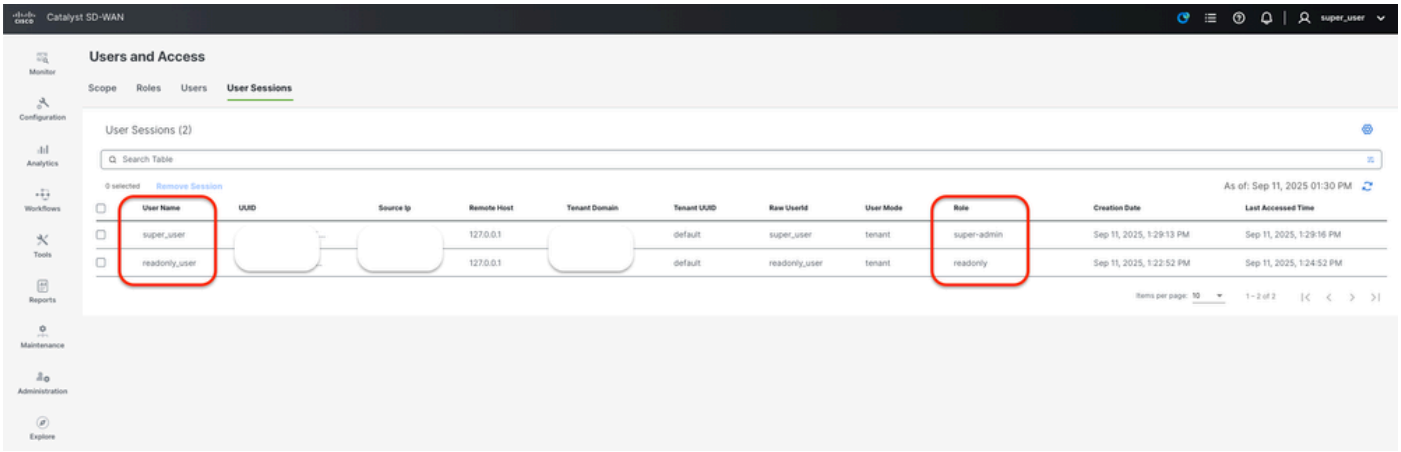


Política de Autorização

Verificar a configuração TACACS+

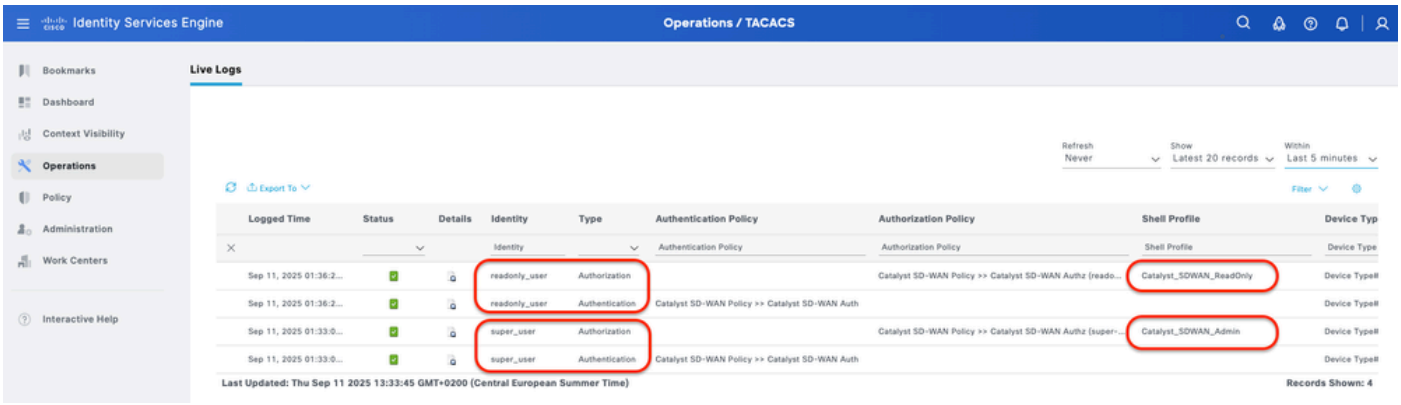
1- Exibir sessões de usuário do Catalyst SD-WAS Catalyst SD-WAN: Administração > Usuários e Acesso > Sessões de Usuário.

Você pode exibir a lista de usuários externos que fizeram login através do RADIUS pela primeira vez. As informações exibidas incluem seus nomes de usuário e funções.



Sessões de usuário do Catalyst SD-WAS

2- ISE - TACACS Live-Logs Operações > 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

Logs ao vivo

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; }

Registros ao vivo detalhados - (somente leitura)

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; }

Troubleshooting

No momento, não há informações de diagnóstico específicas disponíveis para esta configuração.

Referências

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.4
- Guia de configuração de sistemas e interfaces Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN versão 17.x

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.