将ISE配置为Catalyst SD-WAN GUI的外部身份验证

目录

简介

先决条件

- 要求
- 使用的组件
- 开始使用前

配置 — 使用TACACS+

- 使用TACACS+配置Catalyst SD-WAN
- 为TACACS+配置ISE
- 检验TACACS+配置

故障排除

参考

简介

本文档介绍如何将思科身份服务引擎(ISE)配置为Cisco Catalyst SD-WAN GUI管理的外部身份验证。

先决条件

要求

思科建议您了解以下主题：

- TACACS+协议
- Cisco ISE设备管理
- Cisco Catalyst SD-WAN管理
- 思科ISE策略评估

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎(ISE)版本3.4补丁2
- 思科Catalyst SD-WAN版本20.15.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

开始使用前

从Cisco vManage版本20.9.1开始，在身份验证中使用新标签：

- Viptela用户组：用于用户组定义而不是Viptela-Group-Name。
- Viptela资源组：用于资源组定义。

配置 — 使用TACACS+

使用TACACS+配置Catalyst SD-WAN

步骤

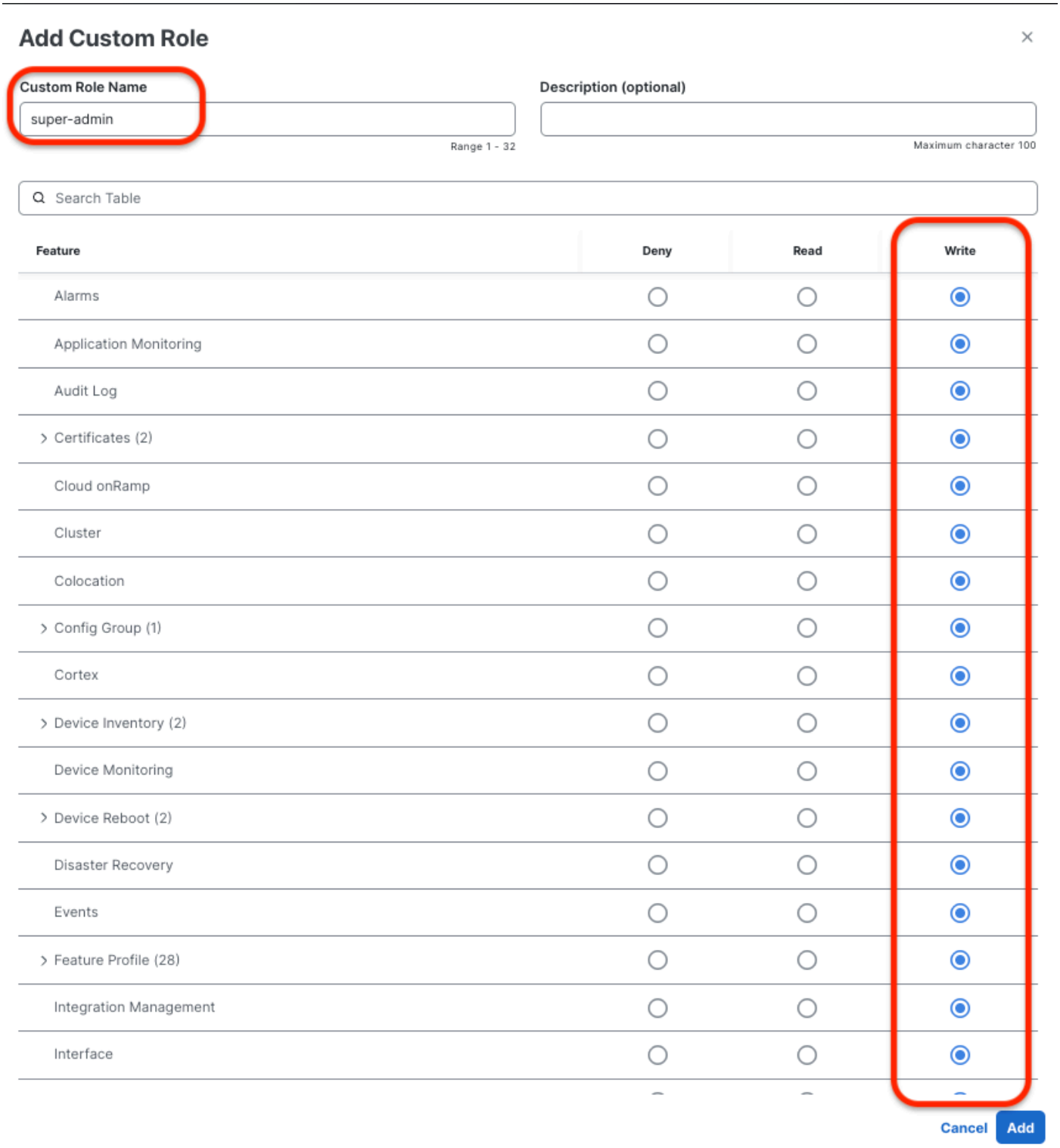
步骤1.（可选）定义自定义角色。

配置满足要求的自定义角色，您可以使用默认用户角色。这可以通过Catalyst SD-WAN选项卡完成：Administration > Users and Access > Roles。

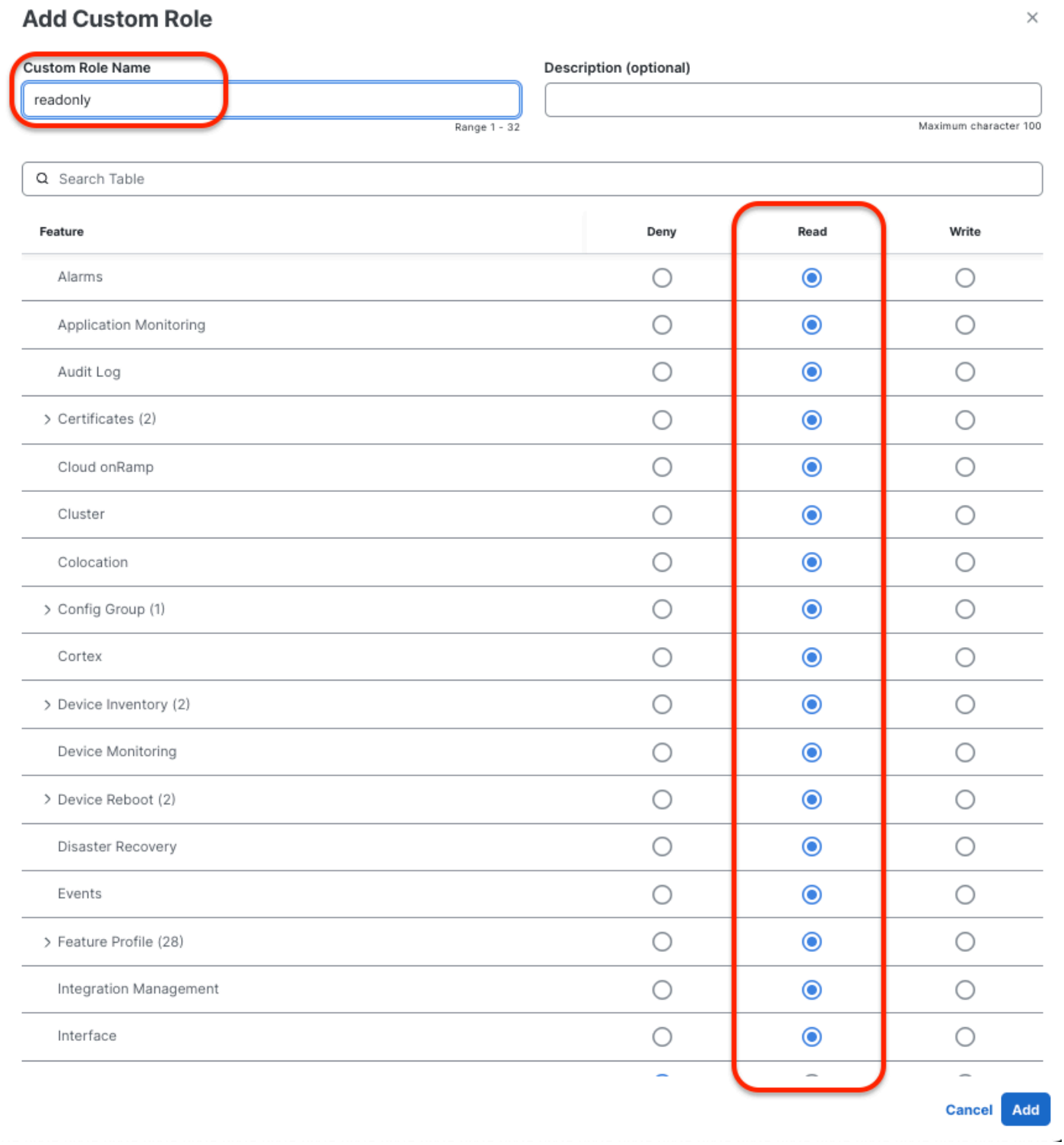
创建两个自定义角色：

1. 管理员角色：超级管理员
2. 只读角色：只读

这可以通过Catalyst SD-WAN选项卡完成：Administration > Users and Access > Roles > Click > Add Role。


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

管理员角色（超级管理员）



只读角色（只读）

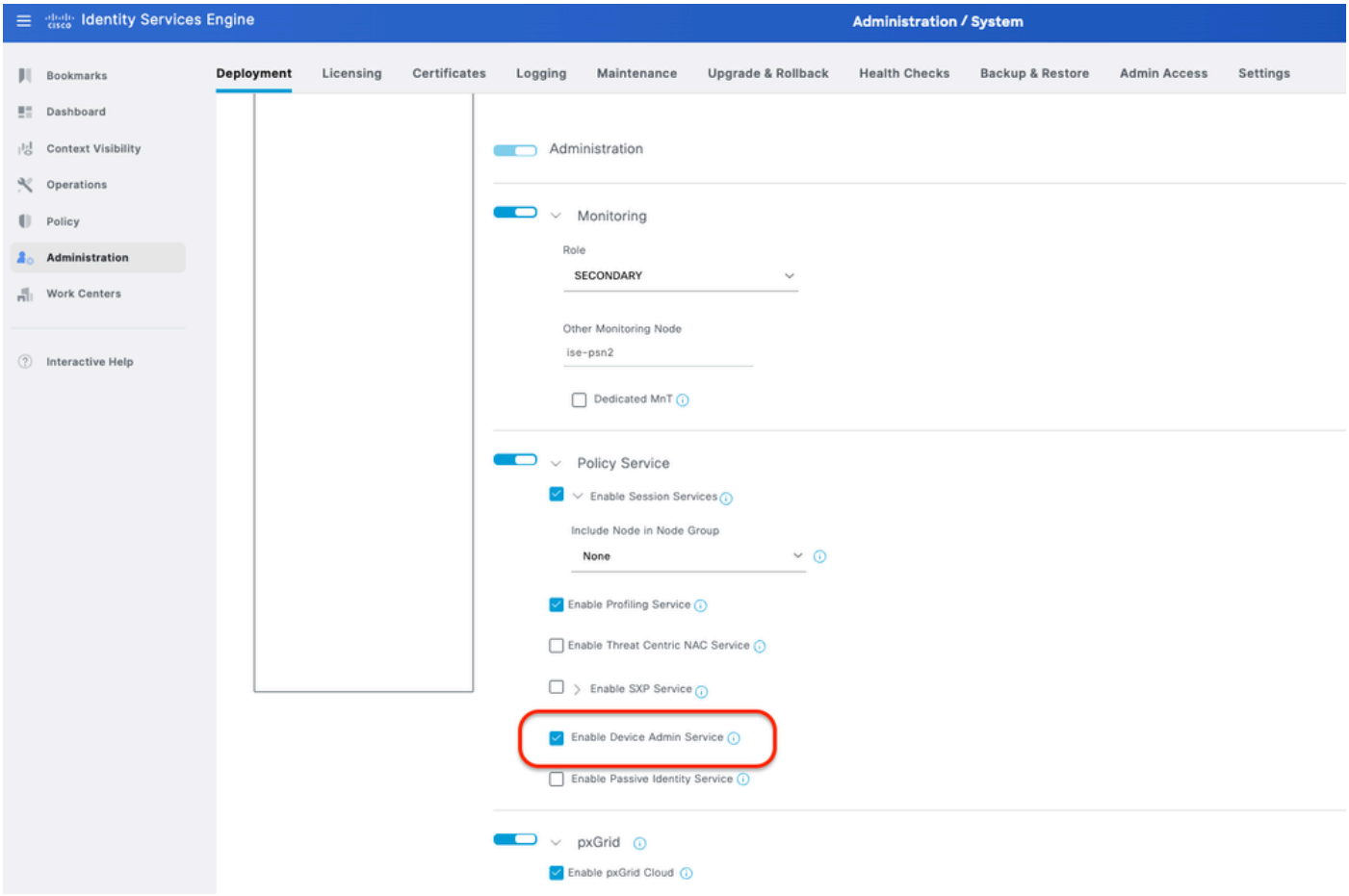
步骤2.使用TACACS+(CLI)配置外部身份验证。

```
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+配置

为TACACS+配置ISE

步骤1.启用设备管理服务。
这可以从选项卡Administration > System > Deployment > Edit(ISE PSN Node)>选中Enable Device Admin Service中完成。



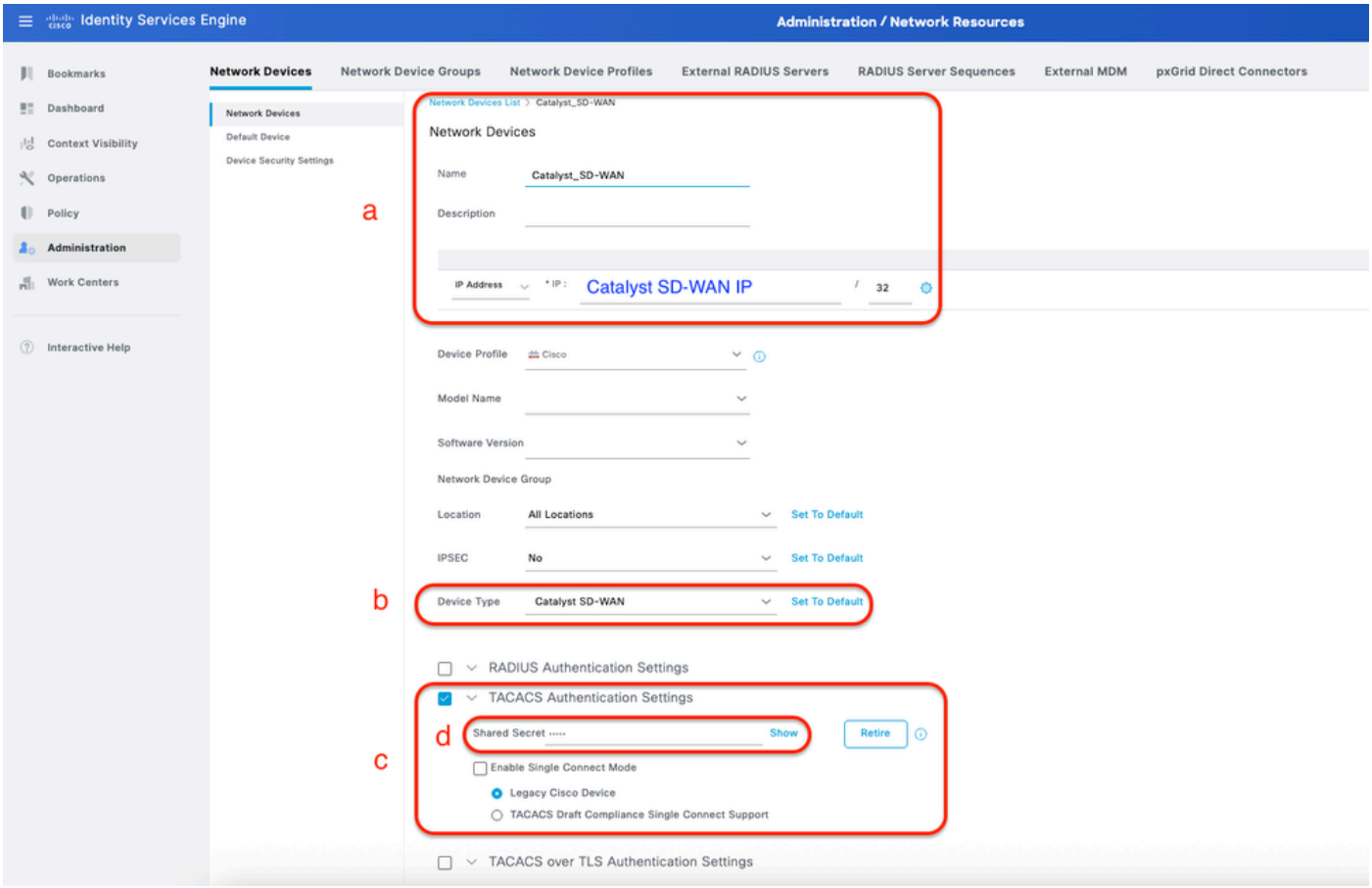
启用设备管理服务

步骤2.在ISE上将Catalyst SD-WAN添加为网络设备。

这可以通过管理>网络资源>网络设备选项卡完成。

步骤

a.定义(Catalyst SD-WAN)网络设备名称和IP。
b.（可选）为策略集条件分类设备类型。
c.启用TACACS+身份验证设置。
d.设置TACACS+共享密钥。



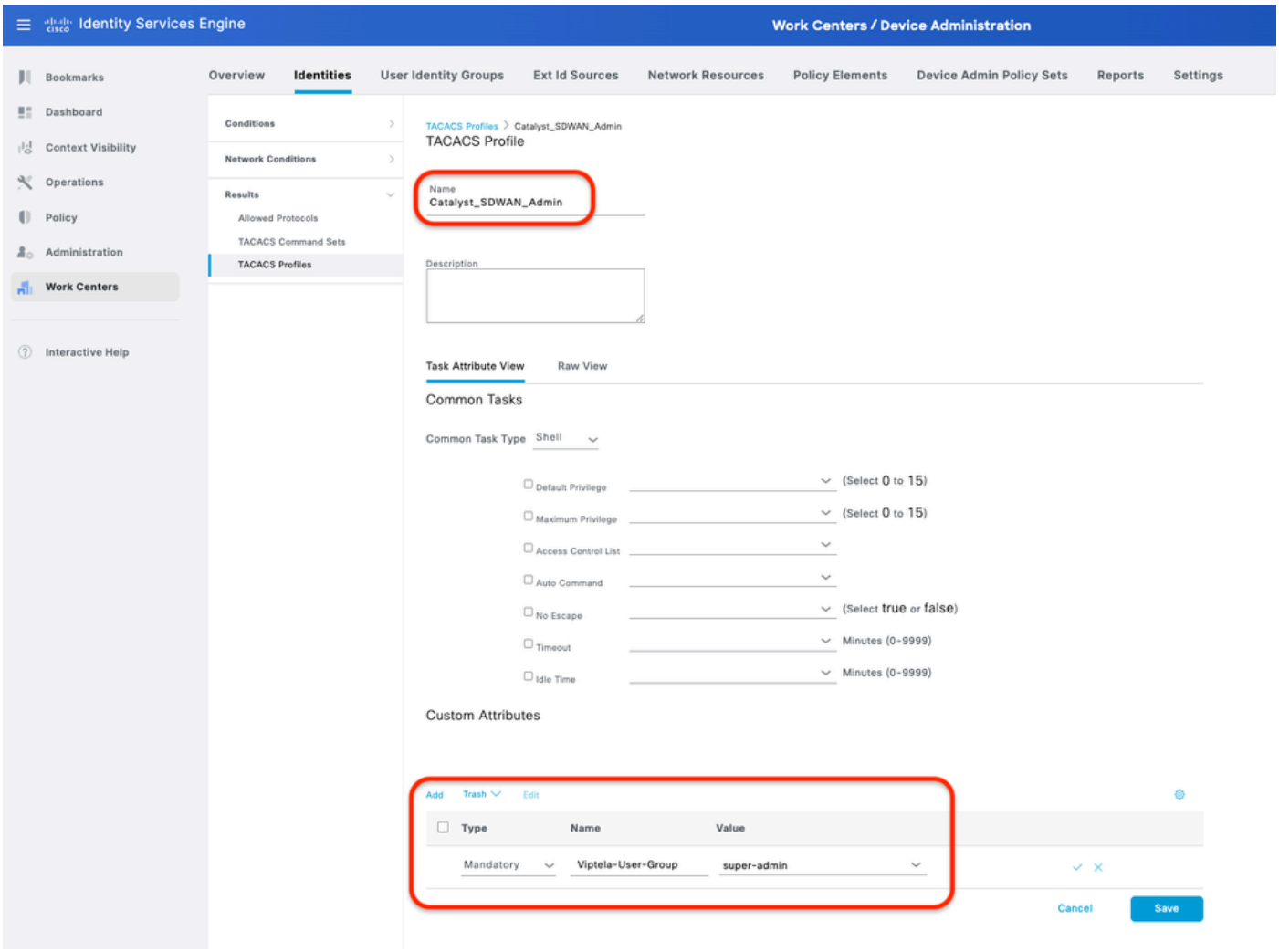
用于TACACS+的ISE网络设备(Catalyst SD-WAN)

步骤3.为每个Catalyst SD-WAN角色创建TACACS+配置文件。

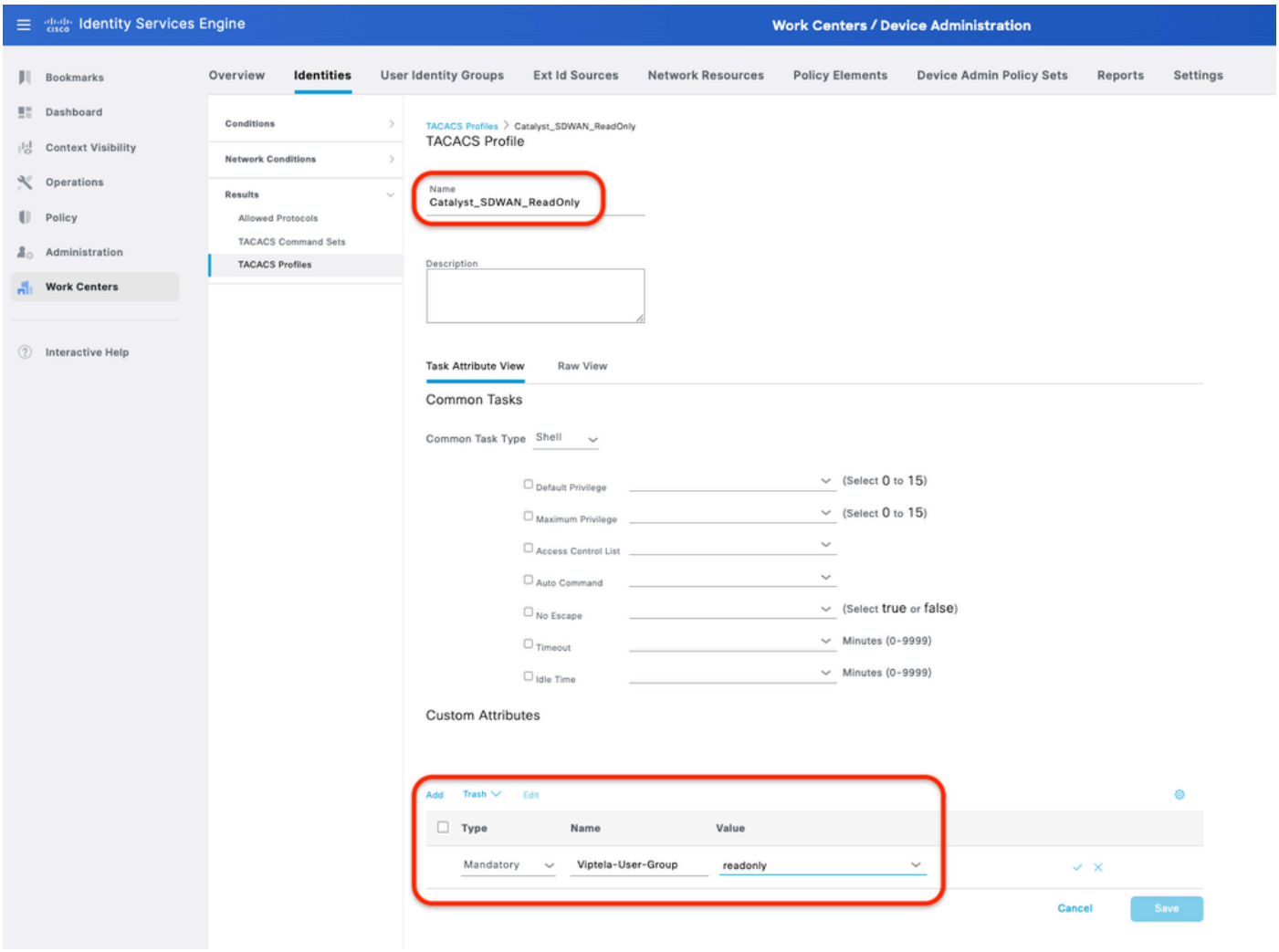
创建TACACS+配置文件：

1. Catalyst_SDWAN_Admin:对于超级管理员用户。
2. Catalyst_SDWAN_ReadOnly:对于只读用户。

这可以从工作中心>设备管理>策略元素>结果> TACACS配置文件>添加选项卡完成。



TACACS+配置文件 — (Catalyst_SDWAN_Admin)



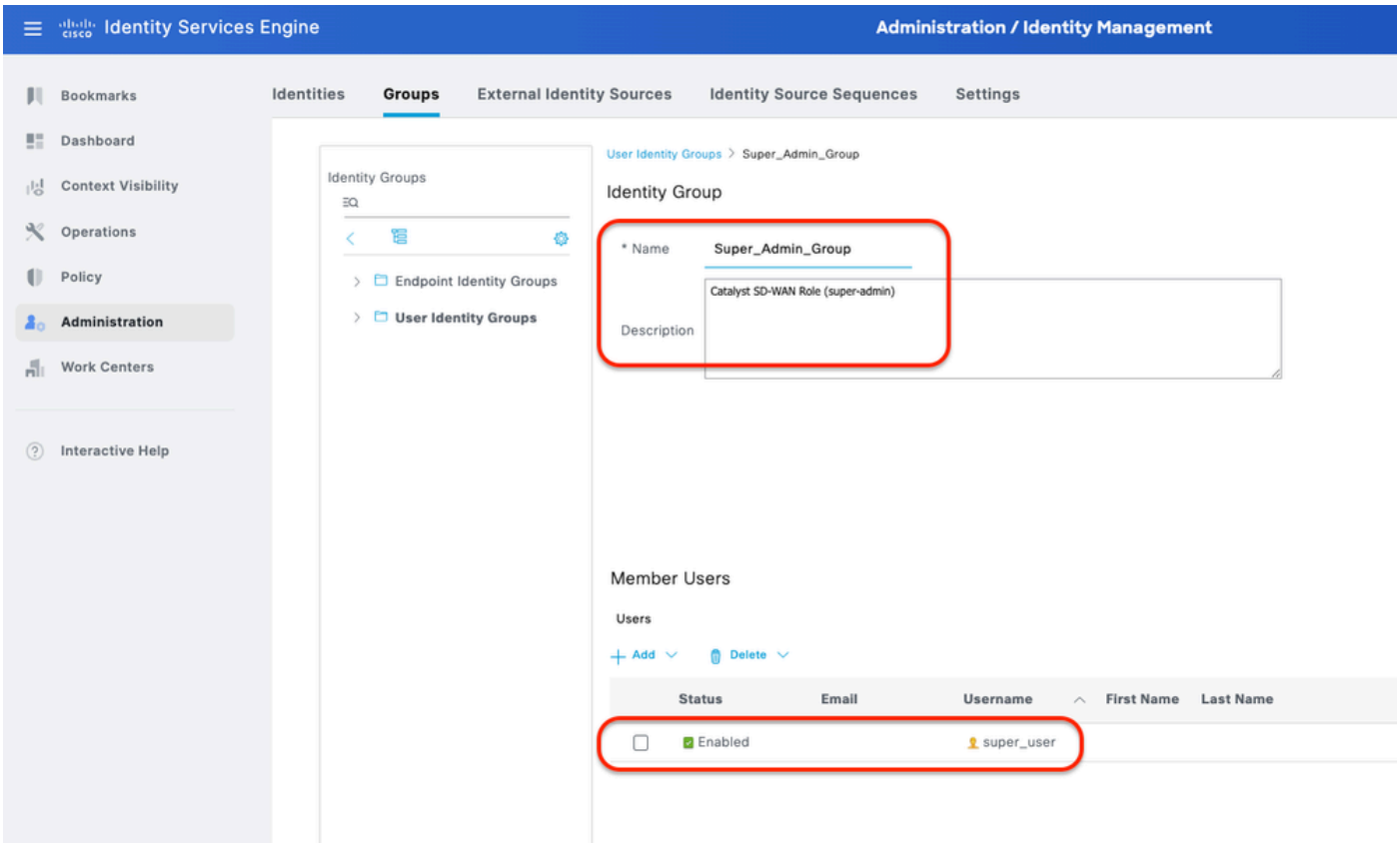
TACACS+配置文件 — (Catalyst_SDWAN_ReadOnly)

步骤4.创建用户组将本地用户添加为成员。

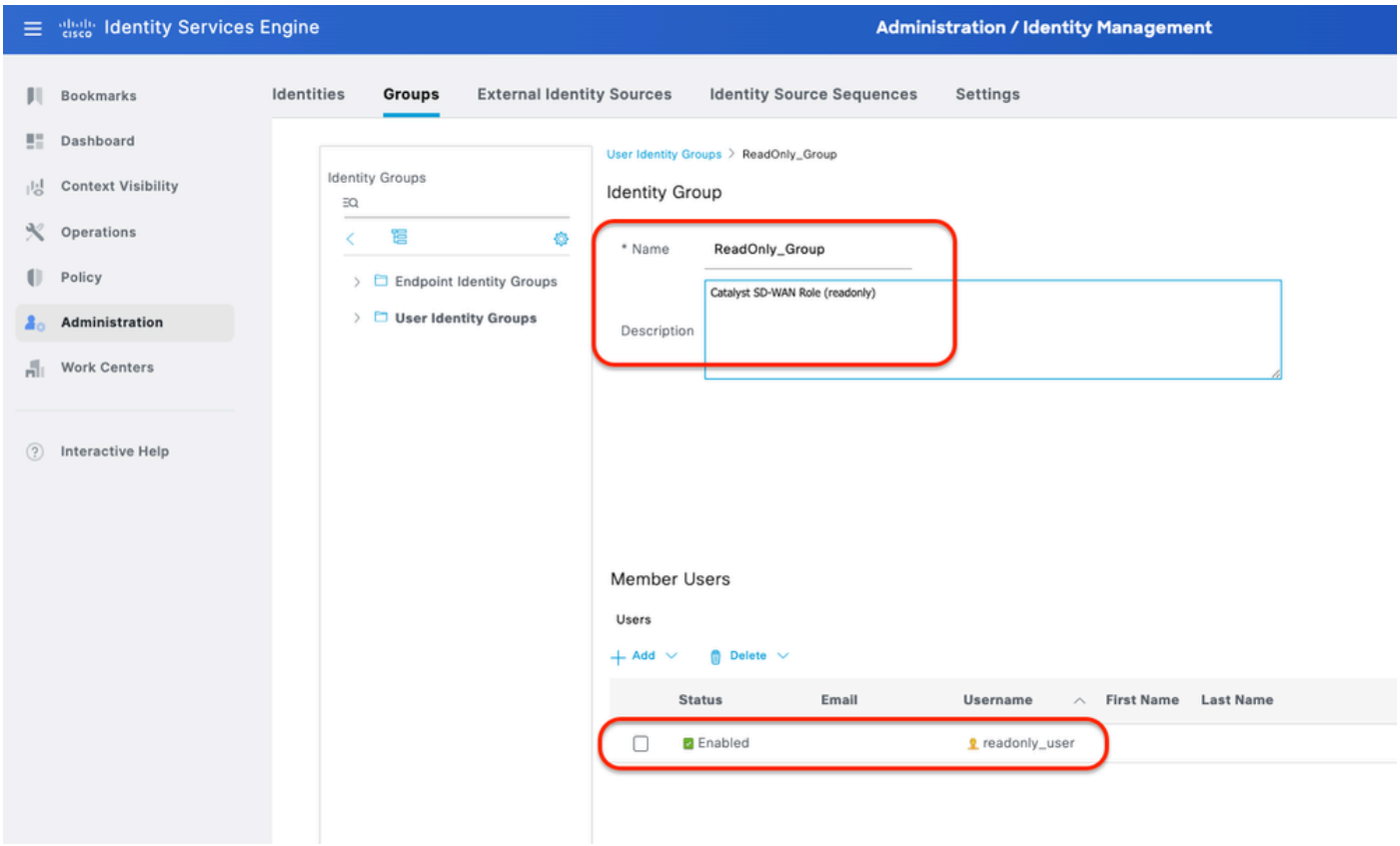
这可以通过工作中心>设备管理>用户身份组选项卡完成。

创建两个用户身份组:

1. Super_Admin_Group
2. 只读组



用户身份组 — (Super_Admin_Group)



用户身份组 — (ReadOnly_Group)

步骤5.（可选）添加TACACS+策略集。

这可以通过工作中心>设备管理>设备管理策略集选项卡完成。

步骤

a.单击Actions并选择(上面插入新行)。

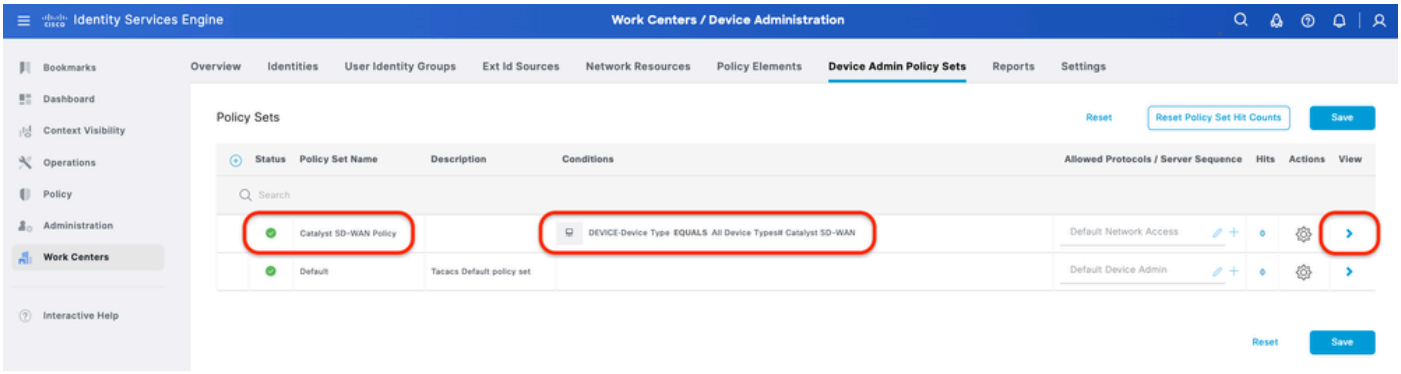
b.定义策略集名称。

c.将Policy Set Condition设置为Select Device Type you previous created on（步骤2 > b）。

d.设置Allowed protocols。

e.Click Save.

f.单击(>)Policy Set View配置身份验证和授权规则。



ISE策略集

步骤6.配置TACACS+身份验证策略。

这可以从工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略集(Device Admin Policy Sets)>点击(>)完成。

步骤

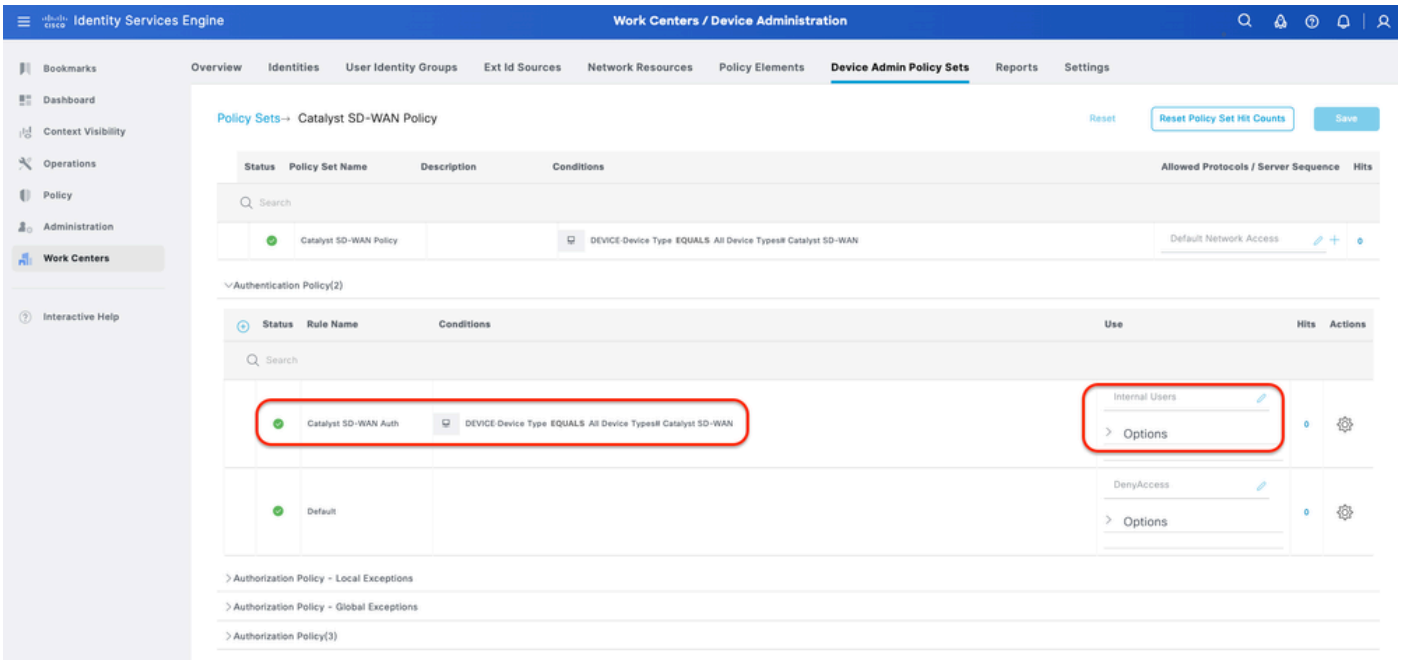
a.单击Actions并选择(上面插入新行)。

b.定义身份验证策略名称。

c.设置Authentication Policy Condition并选择Device Type（之前在上创建的设备）（步骤2 > b）。

d.为身份源设置Authentication Policy Use。

e.Click Save.



验证策略

步骤7.配置TACACS+授权策略。

这可以从工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略集(Device Admin Policy Sets)>点击(>)中完成。

此步骤用于为每个Catalyst SD-WAN角色创建授权策略：

- Catalyst SD-WAN身份验证（超级管理员）：超级管理员
- Catalyst SD-WAN身份验证（只读）：只读

步骤

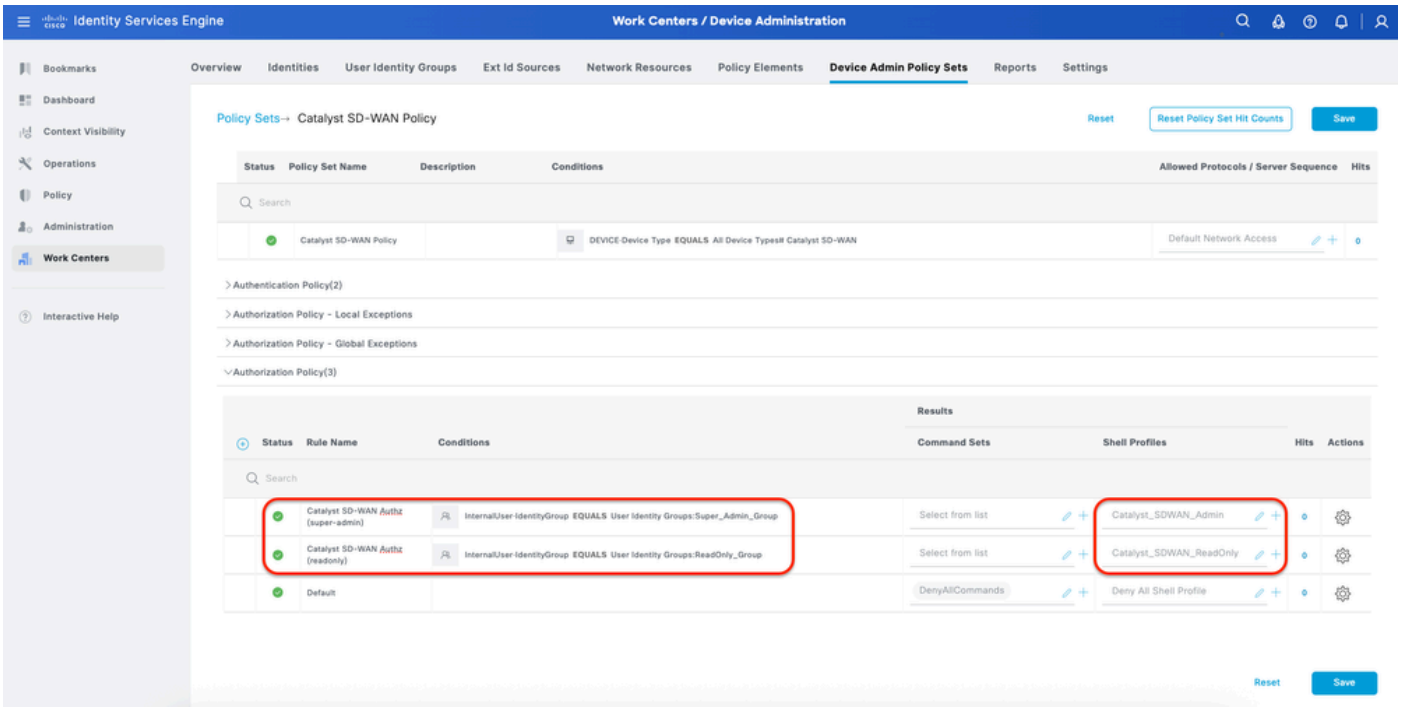
a.单击Actions并选择(上面插入新行)。

b.定义授权策略名称。

c.设置Authorization Policy Condition并选择User Group（步骤4）。

d.设置Authorization PolicyShell Profileses并选择您在中创建的TACACS Profileing（第3步）。

e.Click Save.

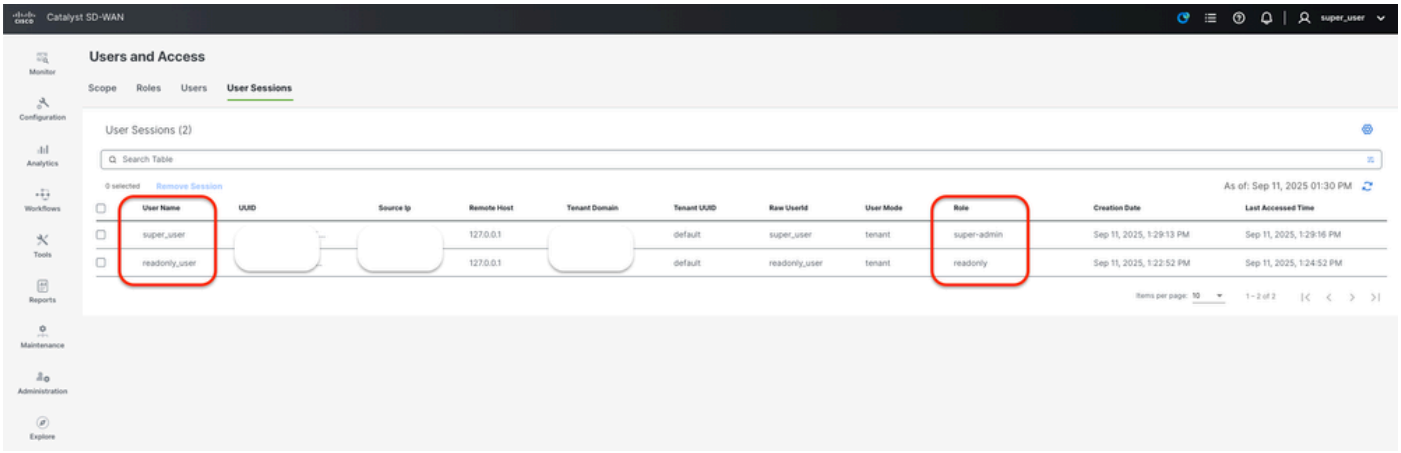


授权策略

检验TACACS+配置

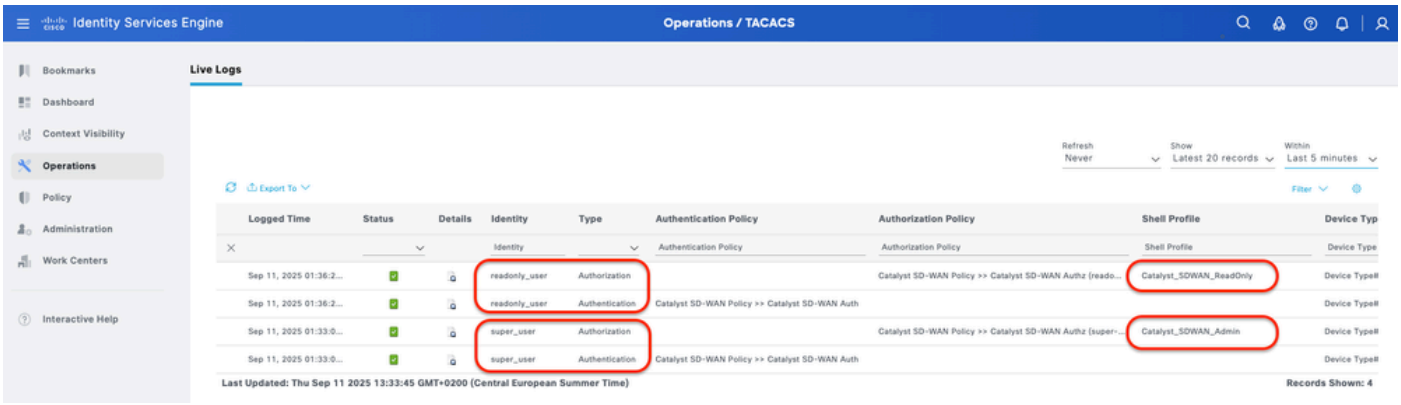
1 — 显示Catalyst SD-WAS用户会话Catalyst SD-WAN:Administration > Users and Access > User Sessions。

您可以查看首次通过RADIUS登录的外部用户的列表。显示的信息包括他们的用户名和角色。



Catalyst SD-WAS用户会话

2 - ISE - TACACS实时日志操作> TACACS >实时日志。


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

实时日志

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; }

详细实时日志 — （只读）

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; }

故障排除

当前没有可用于此配置的特定诊断信息。

参考

- 思科身份服务引擎管理员指南，版本3.4
- Cisco Catalyst SD-WAN系统和接口配置指南，Cisco IOS XE Catalyst SD-WAN版本17.x

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。