將ISE配置為Catalyst SD-WAN GUI的外部身份驗證

目錄

簡介

本文檔介紹如何將Cisco Identity Services Engine(ISE)配置為用於Cisco Catalyst SD-WAN GUI管理的外部身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- TACACS+通訊協定
- Cisco ISE裝置管理
- Cisco Catalyst SD-WAN管理
- Cisco ISE策略評估

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎(ISE)版本3.4補丁2
- Cisco Catalyst SD-WAN版本20.15.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

開始之前

從Cisco vManage 20.9.1版開始，新的標籤用於身份驗證：

- Viptela-User-Group:用於使用者組定義，而不是Viptela-Group-Name。
- Viptela-Resource-Group:用於資源組定義。

設定 — 使用TACACS+

使用TACACS+配置Catalyst SD-WAN

程式

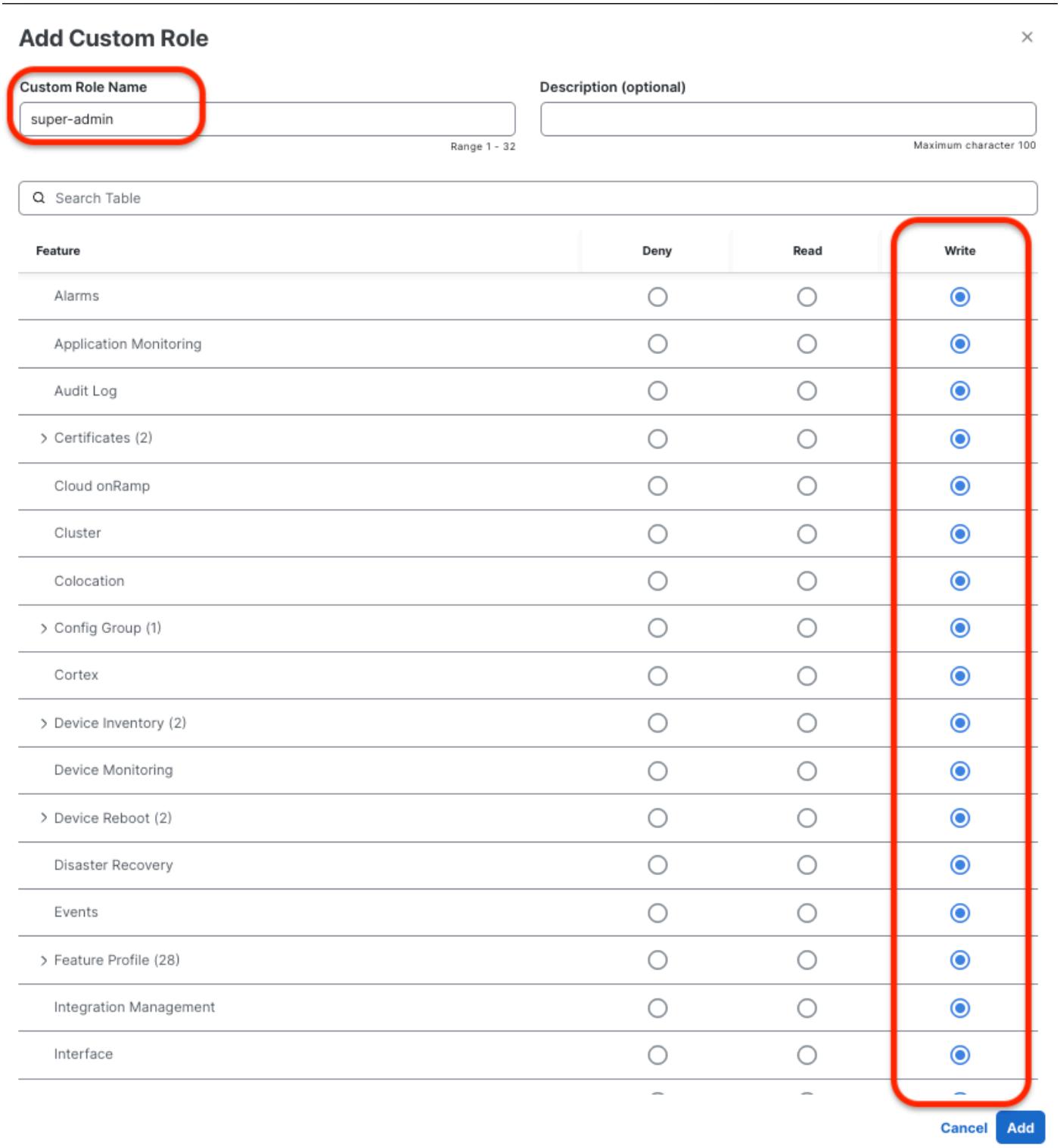
步驟1.（可選）定義自定義角色。

配置滿足要求的自定義角色，而您可以使用預設的使用者角色。可從Catalyst SD-WAN: 索引標籤中執行以下操作：Administration > Users and Access > Roles。

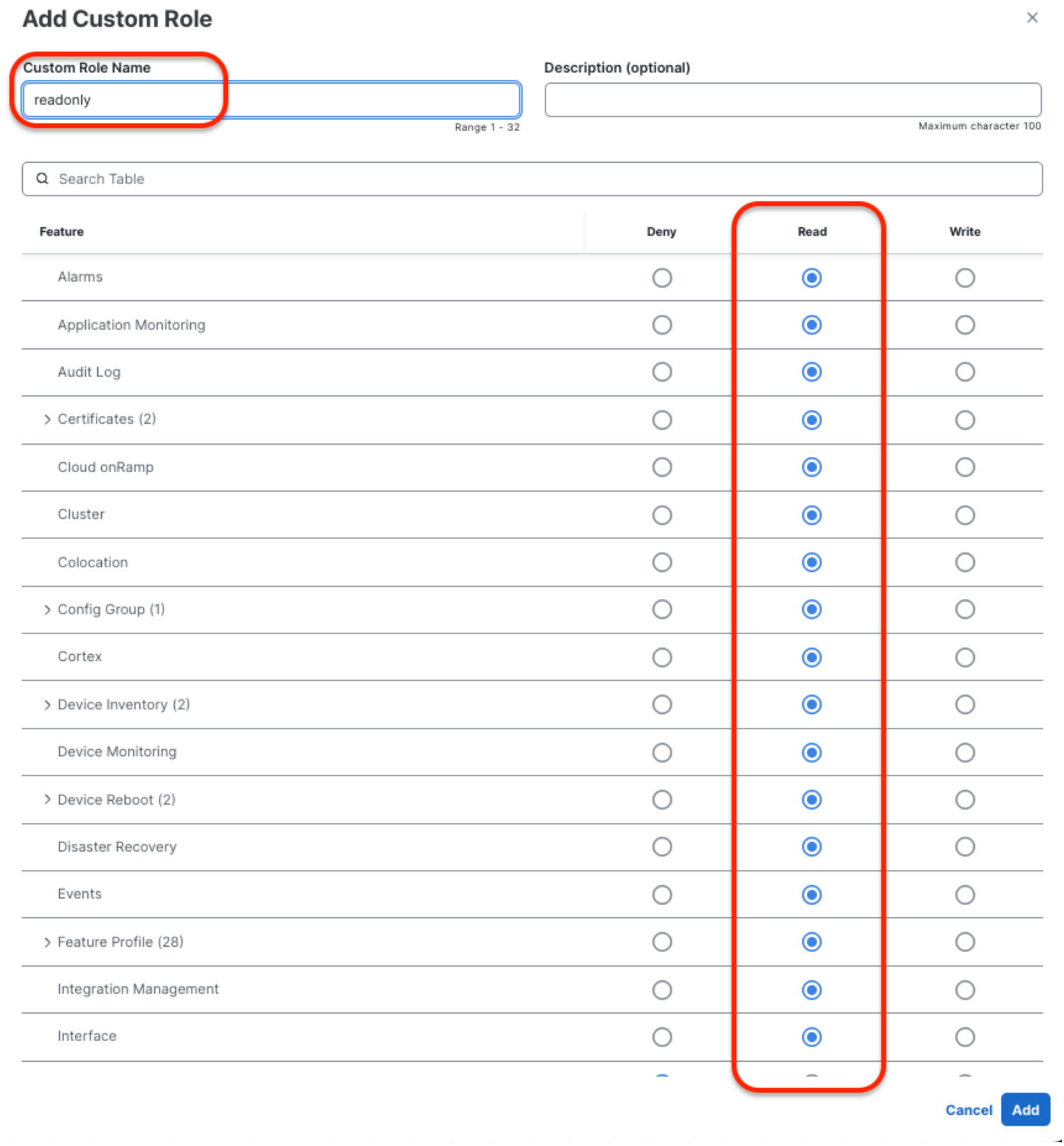
建立兩個自定義角色：

1. 管理員角色：超級管理員
2. 只讀角色：只讀

可從Catalyst SD-WAN: 索引標籤中執行以下操作：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

管理員角色（超級管理員）



只讀角色（只讀）

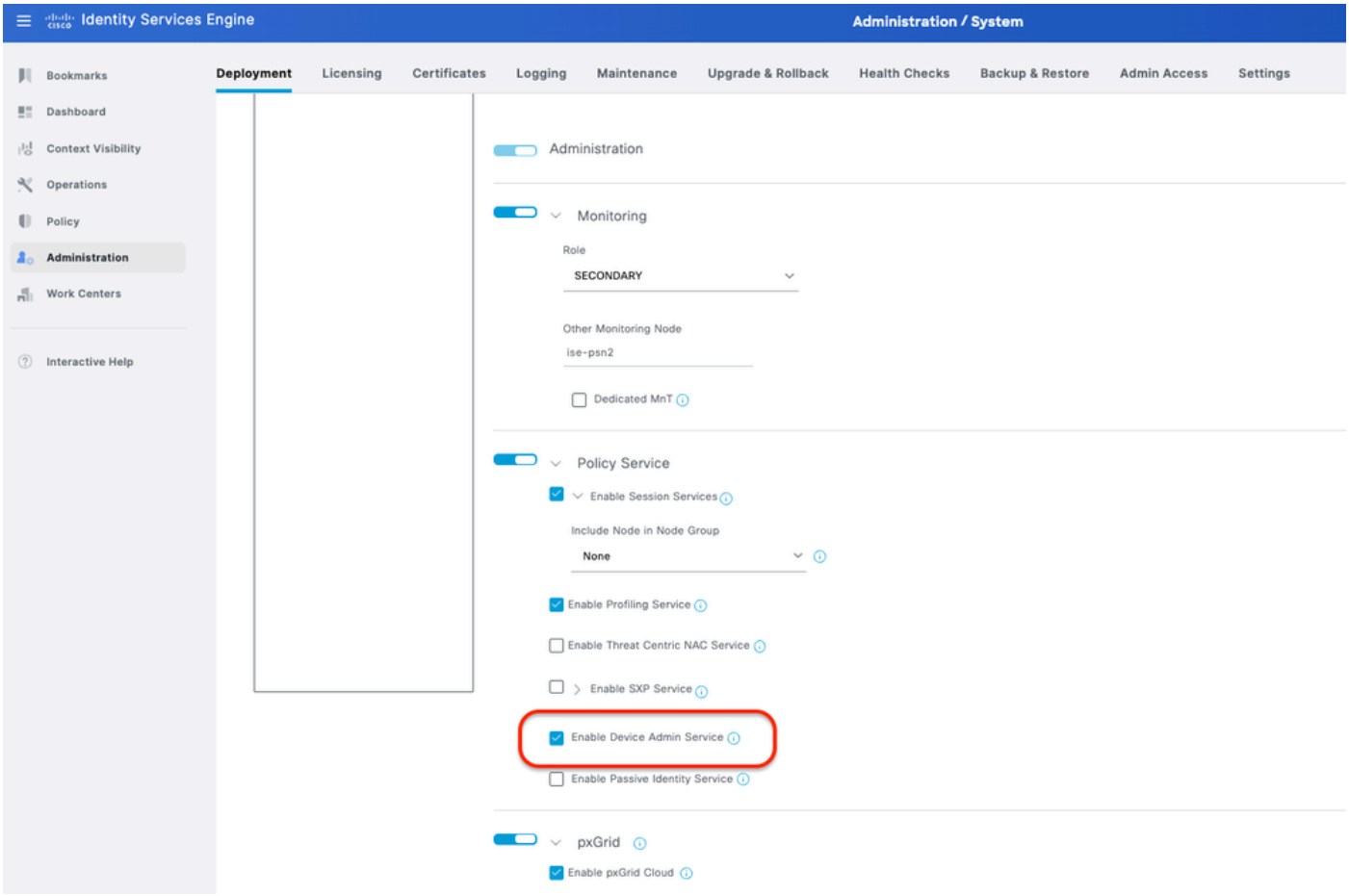
步驟2.使用TACACS+(CLI)設定外部驗證。

```
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 - TACACS+組態

為TACACS+配置ISE

步驟1.啟用Device Admin Service。
可從Administration > System > Deployment > Edit(ISE PSN Node)>Check Enable Device Admin Service頁籤完成此操作。



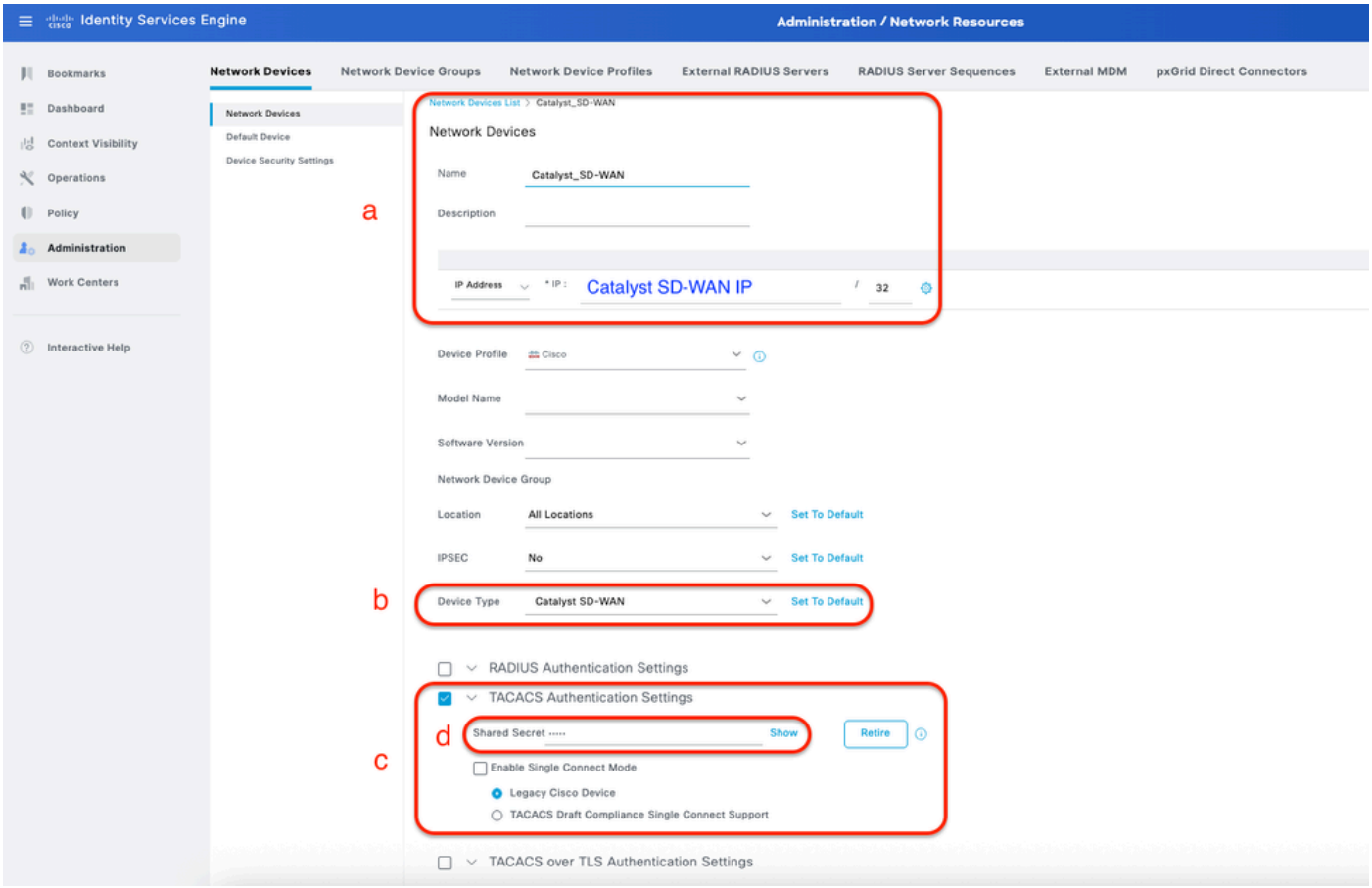
啟用裝置管理服務

步驟2.在ISE上將Catalyst SD-WAN新增為網路裝置。

可從管理>網路資源>網路裝置索引標籤完成此操作。

程式

a.定義(Catalyst SD-WAN)網路裝置名稱和IP。
b.（可選）為策略集條件分類裝置型別。
c.啟用TACACS+身份驗證設定。
d.設定TACACS+共用密碼。



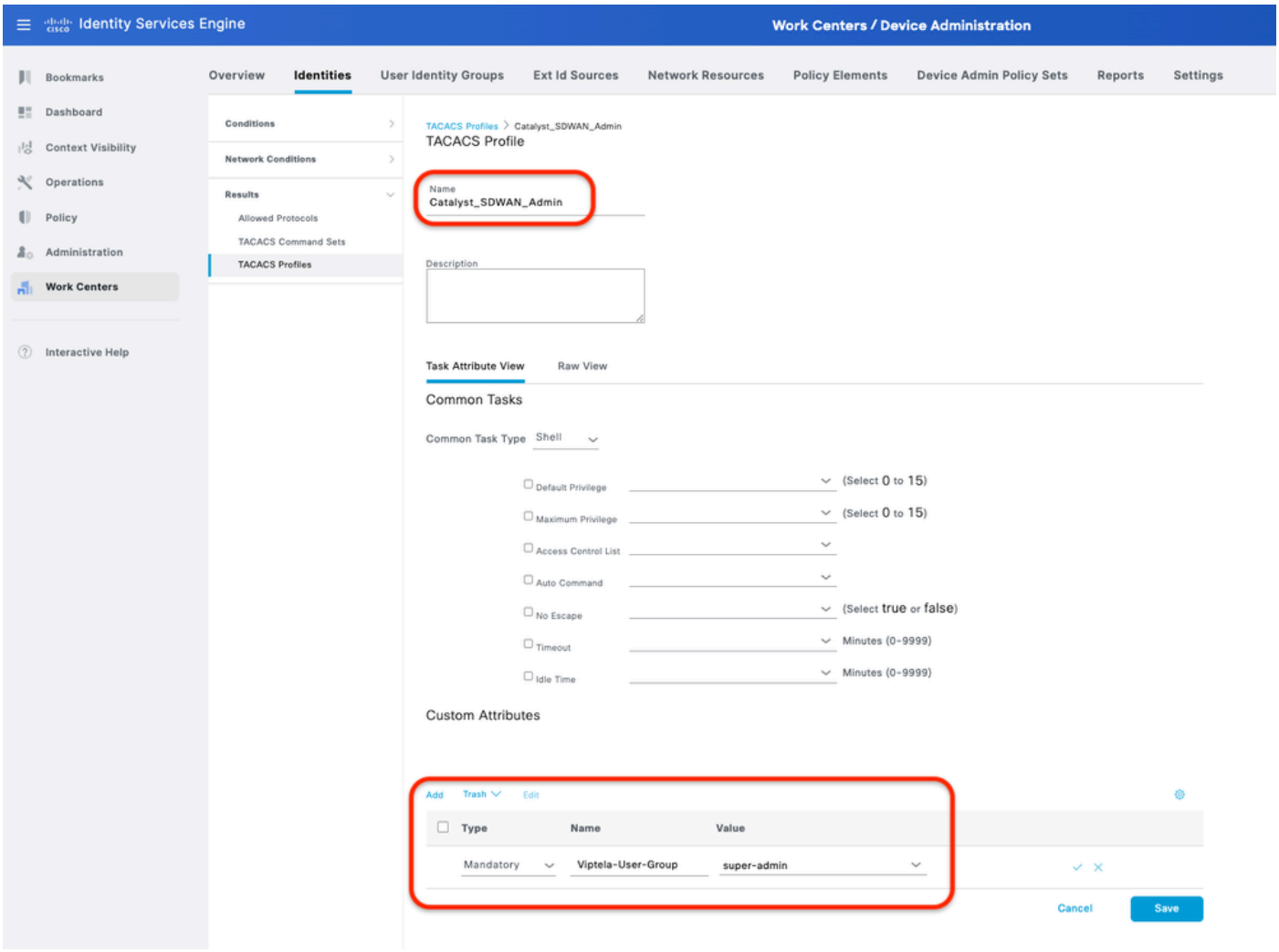
適用於TACACS+的ISE網路裝置(Catalyst SD-WAN)

步驟3.為每個Catalyst SD-WAN角色建立TACACS+配置檔案。

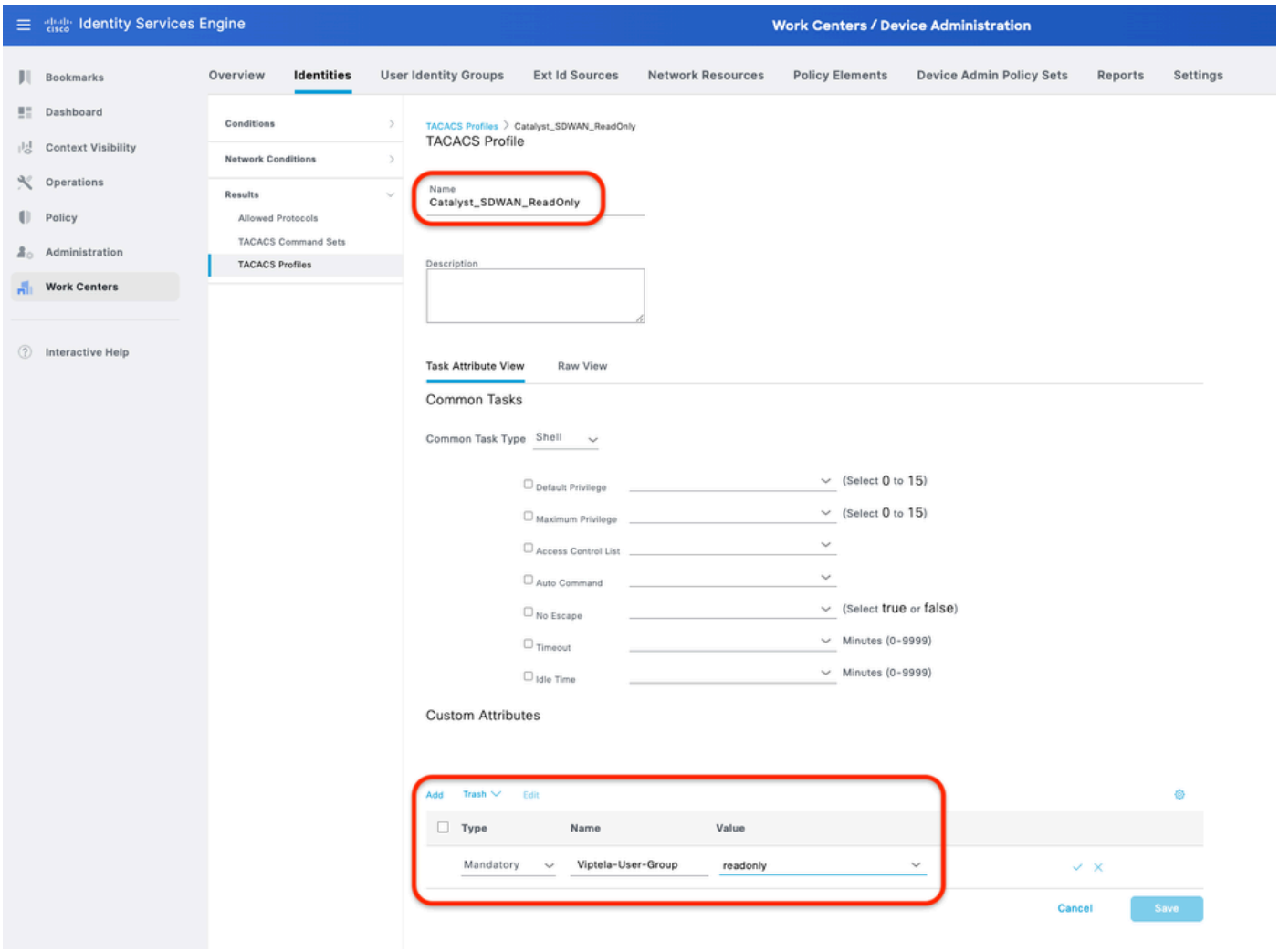
建立TACACS+設定檔：

1. Catalyst_SDWAN_Admin:對於超級管理員使用者。
2. Catalyst_SDWAN_ReadOnly:對於只讀使用者。

可從工作中心>裝置管理>策略元素>結果> TACACS配置檔案>新增頁籤完成此操作。



TACACS+設定檔 — (Catalyst_SDWAN_Admin)



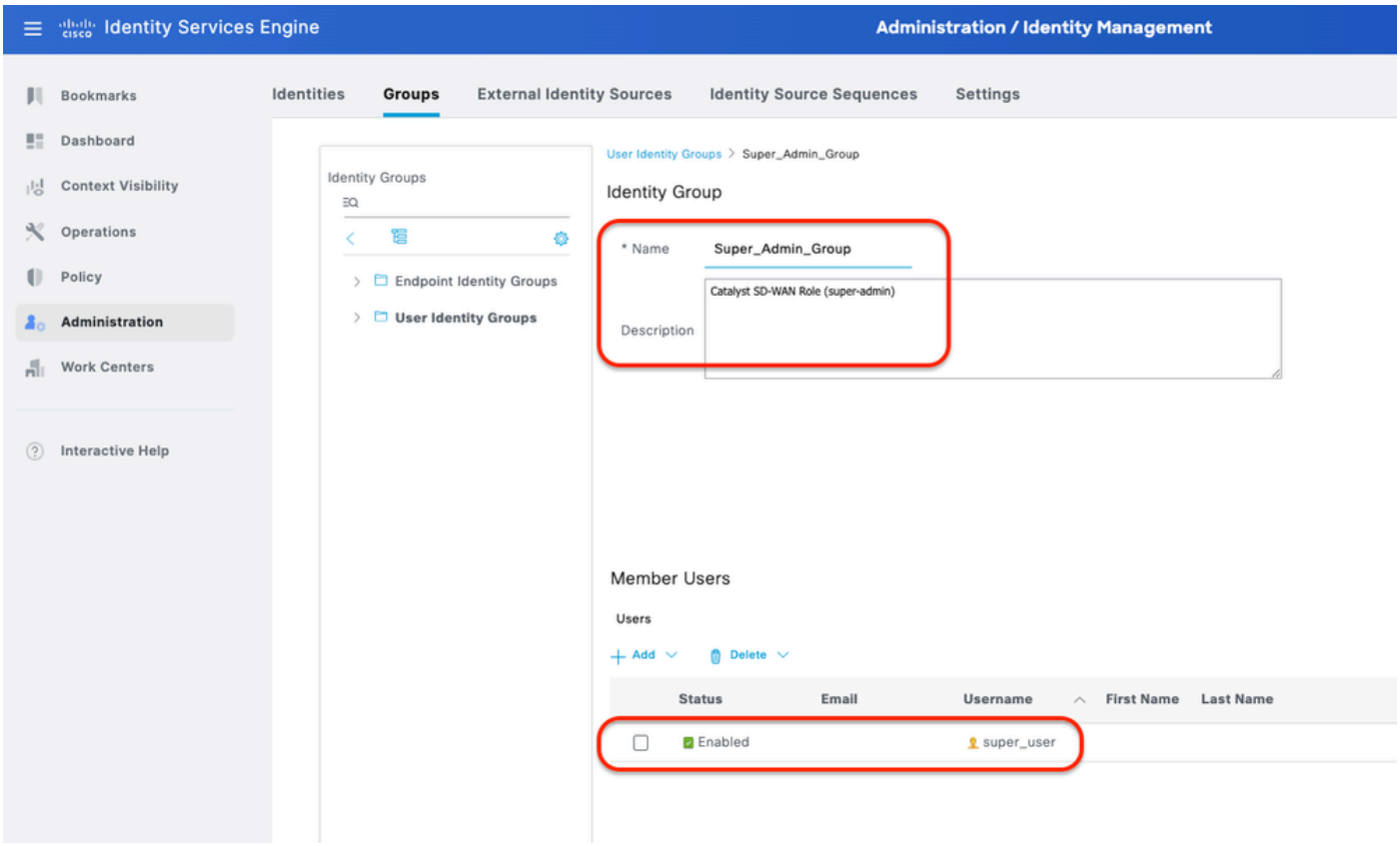
TACACS+設定檔 — (Catalyst_SDWAN_ReadOnly)

步驟4.建立使用者組將Local Users新增為成員。

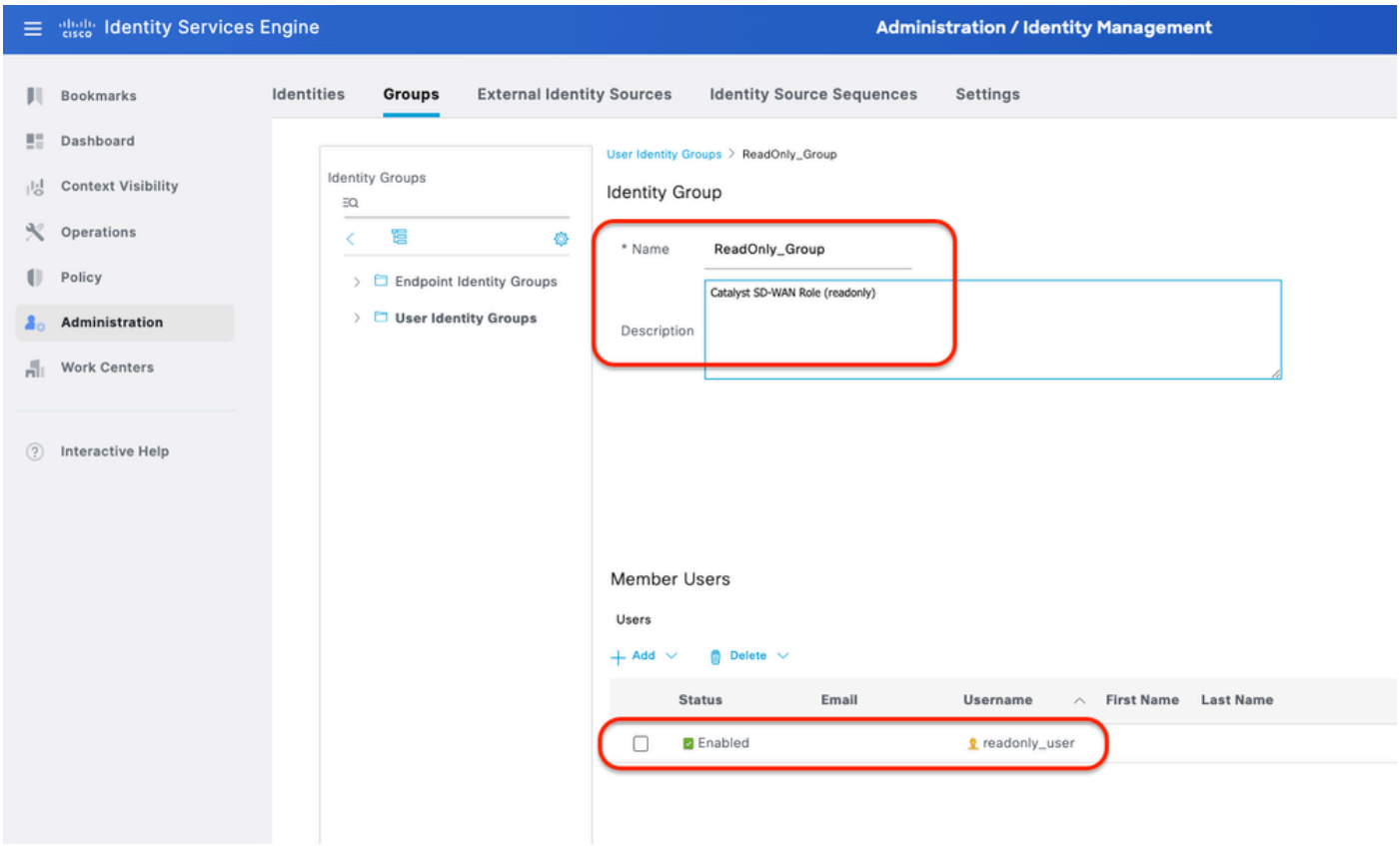
可從工作中心>裝置管理>使用者身份組頁籤完成此操作。

建立兩個使用者身份組:

1. Super_Admin_Group
2. 只讀組



使用者身份組 — (Super_Admin_Group)



使用者身份組 — (ReadOnly_Group)

步驟5.（可選）添加TACACS+策略集。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)頁籤完成此操作。

程式

a.按一下Actions並選擇(在上面插入新行)。

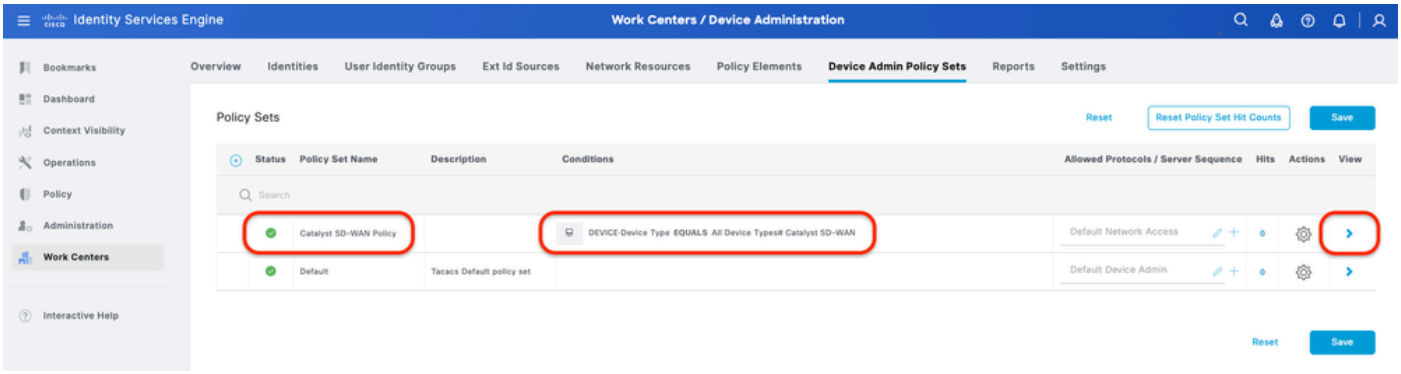
b.定義策略集名稱。

c.將Policy Set Condition設定為Select Device Type you previous created on（步驟2 > b）。

d.設定Allowed protocols。

e.按一下「Save」。

f.按一下(>)Policy Set View配置身份驗證和授權規則。



ISE策略集

步驟6.配置TACACS+身份驗證策略。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)>按一下(>)頁籤完成此操作。

程式

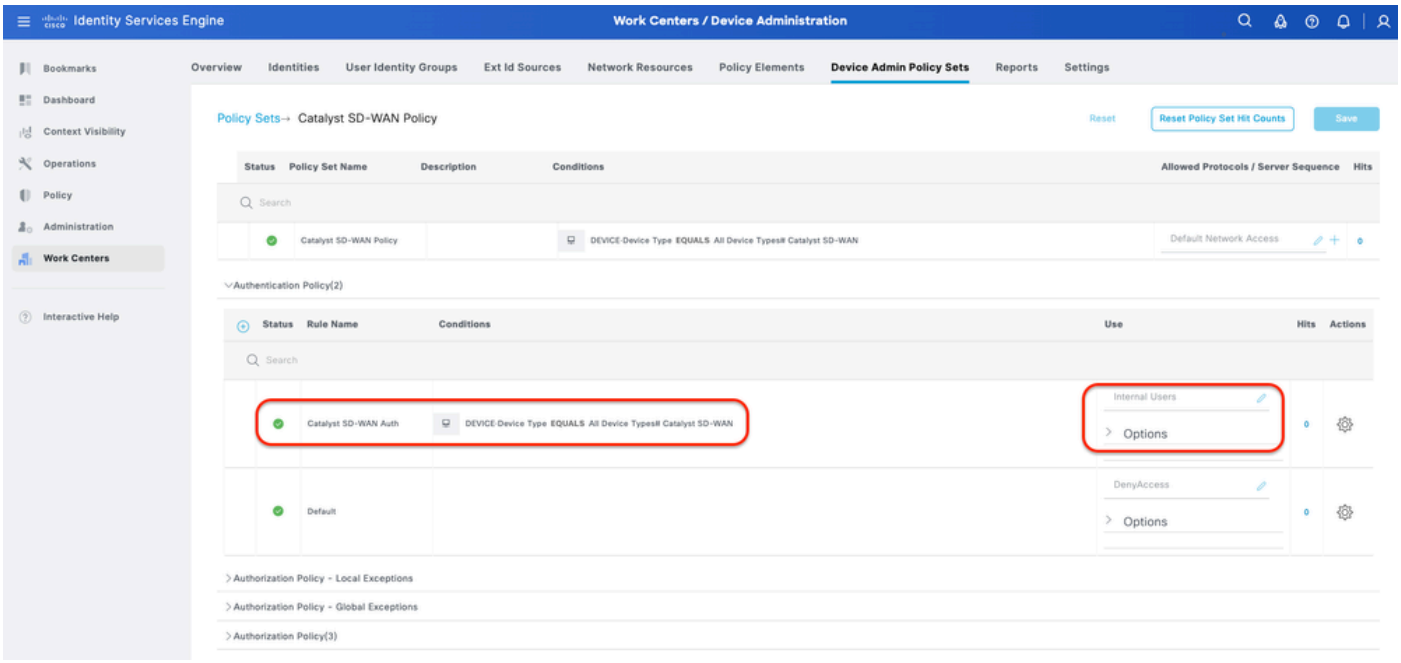
a.按一下Actions並選擇(在上面插入新行)。

b.定義身份驗證策略名稱。

c.設定Authentication Policy Condition，並選擇您之前在上建立的Device Type（步驟2 > b）。

d.設定Authentication Policy Use for Identity源。

e.按一下「Save」。



身份驗證策略

步驟7.配置TACACS+授權策略。

可從工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)>按一下(>)頁籤完成此操作。

此步驟用於為每個Catalyst SD-WAN角色建立授權策略：

- Catalyst SD-WAN授權（超級管理員）：超級管理員
- Catalyst SD-WAN授權（只讀）：只讀

程式

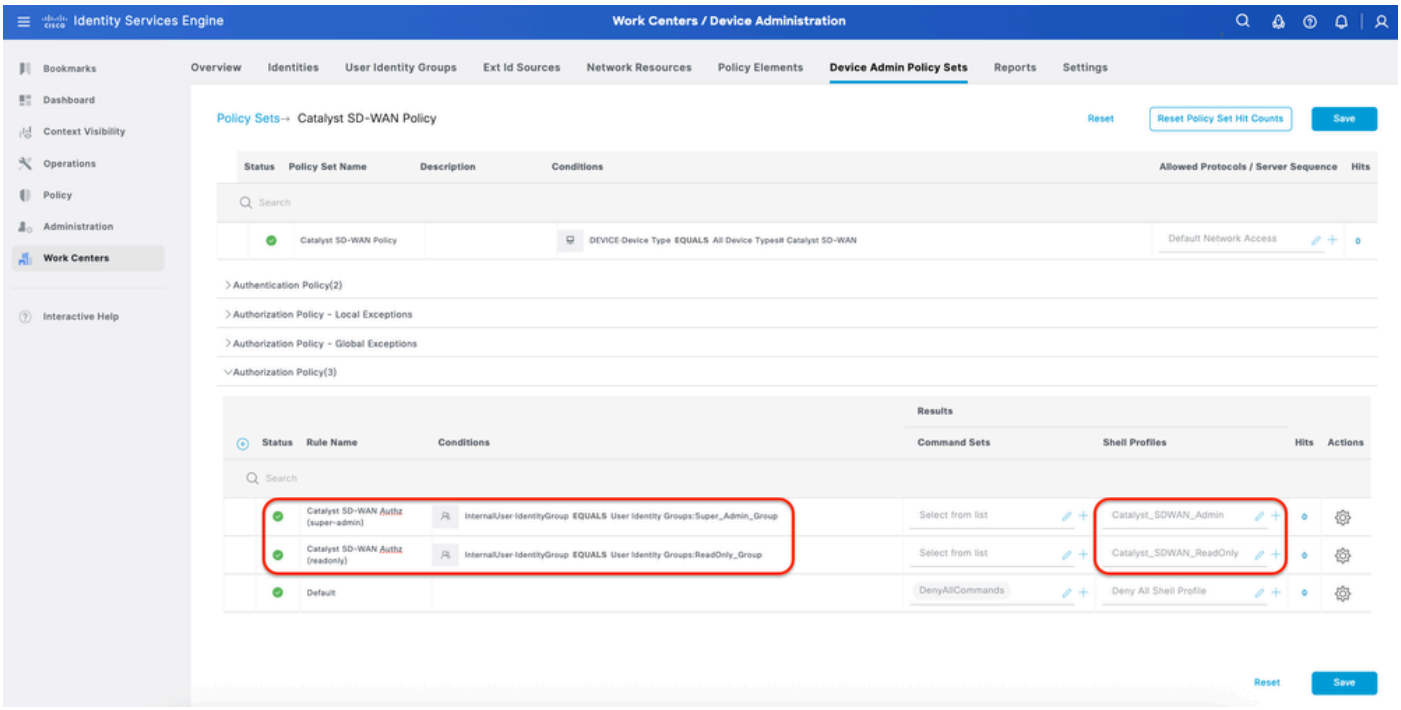
a.按一下Actions並選擇(在上面插入新行)。

b.定義授權策略名稱。

c.設定Authorization Policy Condition並選擇User Group（步驟4）。

d.設定授權PolicyShell配置檔案並選擇您在中建立的TACACS配置檔案（步驟3）。

e.按一下「Save」。

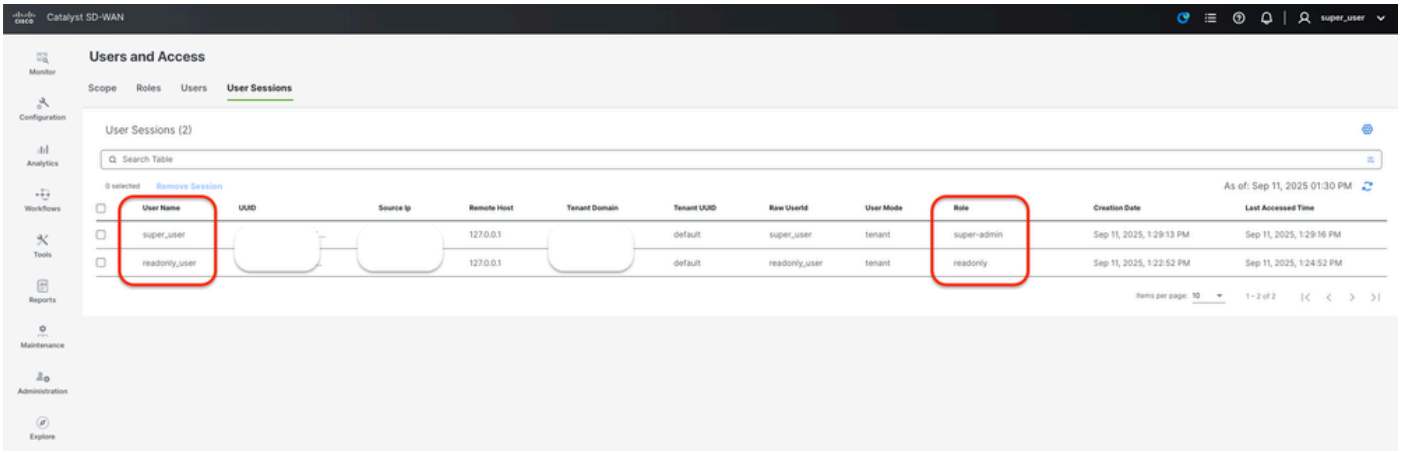


授權策略

驗證TACACS+配置

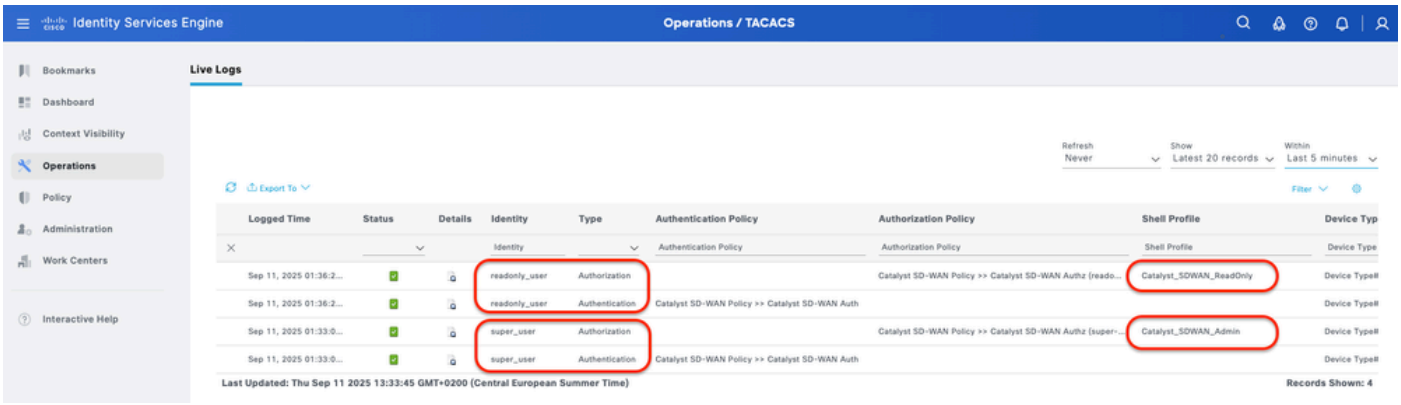
1 — 顯示Catalyst SD-WAS使用者會話Catalyst SD-WAN:Administration > Users and Access > User Sessions。

您可以檢視首次透過RADIUS登入的外部使用者清單。顯示的資訊包括他們的使用者名稱和角色。



Catalyst SD-WAS使用者會話

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

即時日誌

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; }

詳細即時日誌 — (只讀)

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; }

疑難排解

目前尚無適用於此組態的具體診斷資訊。

參考資料

- 思科身份服務引擎管理員指南3.4版
- Cisco Catalyst SD-WAN系統和介面配置指南，Cisco IOS XE Catalyst SD-WAN版本17.x

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。