Catalyst SD-WAN GUIの外部認証としてのISEの設定

内容

はじめに

このドキュメントでは、Cisco Catalyst SD-WAN GUI管理の外部認証としてCisco Identity Services Engine(ISE)を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- TACACS+プロトコル
- Cisco ISEデバイス管理
- Cisco Catalyst SD-WANの管理
- Cisco ISEポリシーの評価

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine(ISE)バージョン3.4パッチ2
- Cisco Catalyst SD-WANバージョン20.15.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

はじめる前に

Cisco vManageリリース20.9.1以降では、認証に新しいタグが使用されます。

- Viptela-User-Group:Viptela-Group-Nameの代わりにユーザグループ定義に使用されます。
- Viptela-Resource-Group：リソースグループ定義用。

設定：TACACS+の使用

TACACS+を使用したCatalyst SD-WANの設定

手順

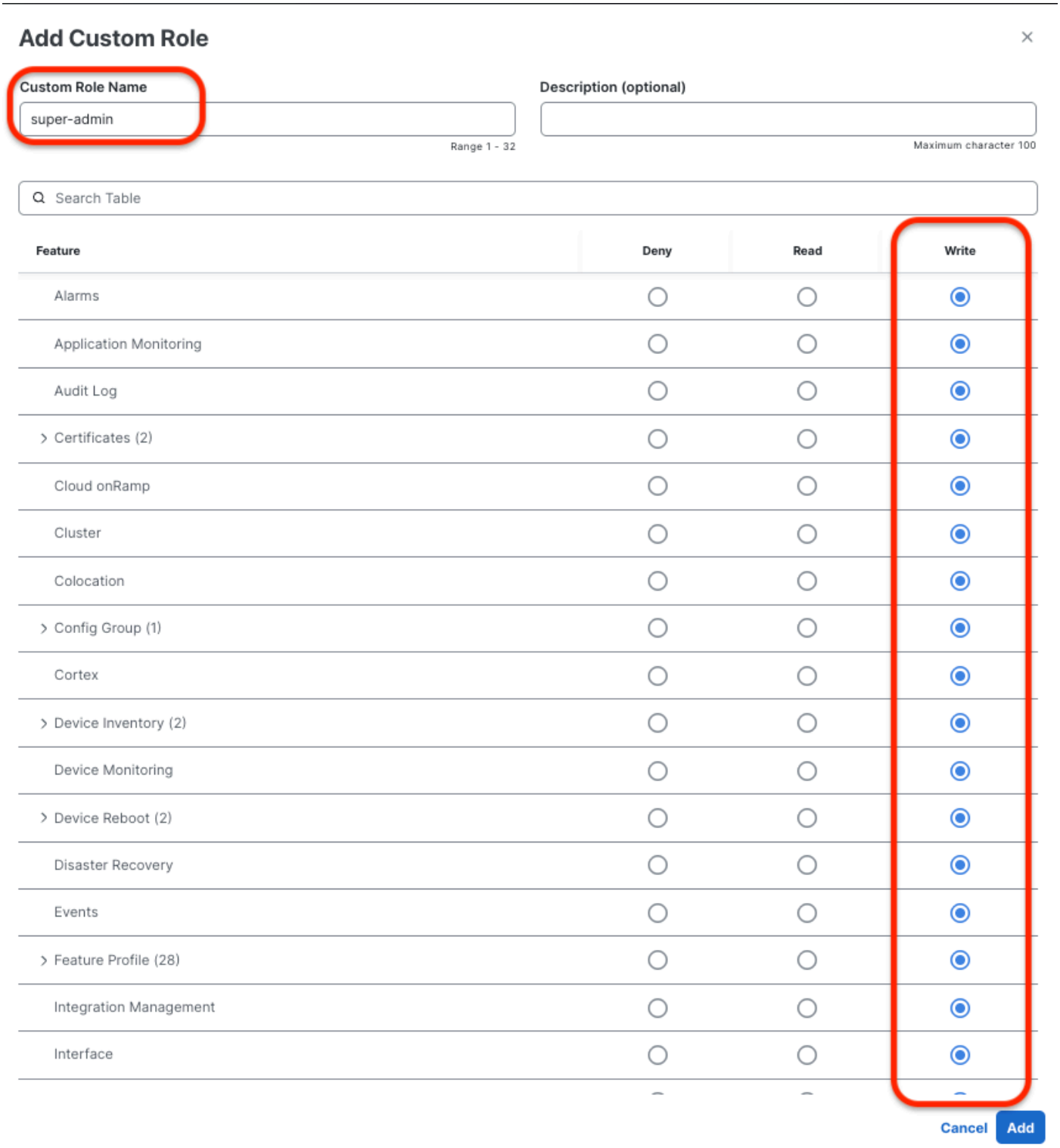
ステップ1:（オプション）カスタムロールを定義します。

要件を満たすカスタムロールを設定する代わりに、デフォルトのユーザロールを使用できます。これは、Catalyst SD-WAN: Administration > Users and Access > Rolesの順に選択して実行できます。

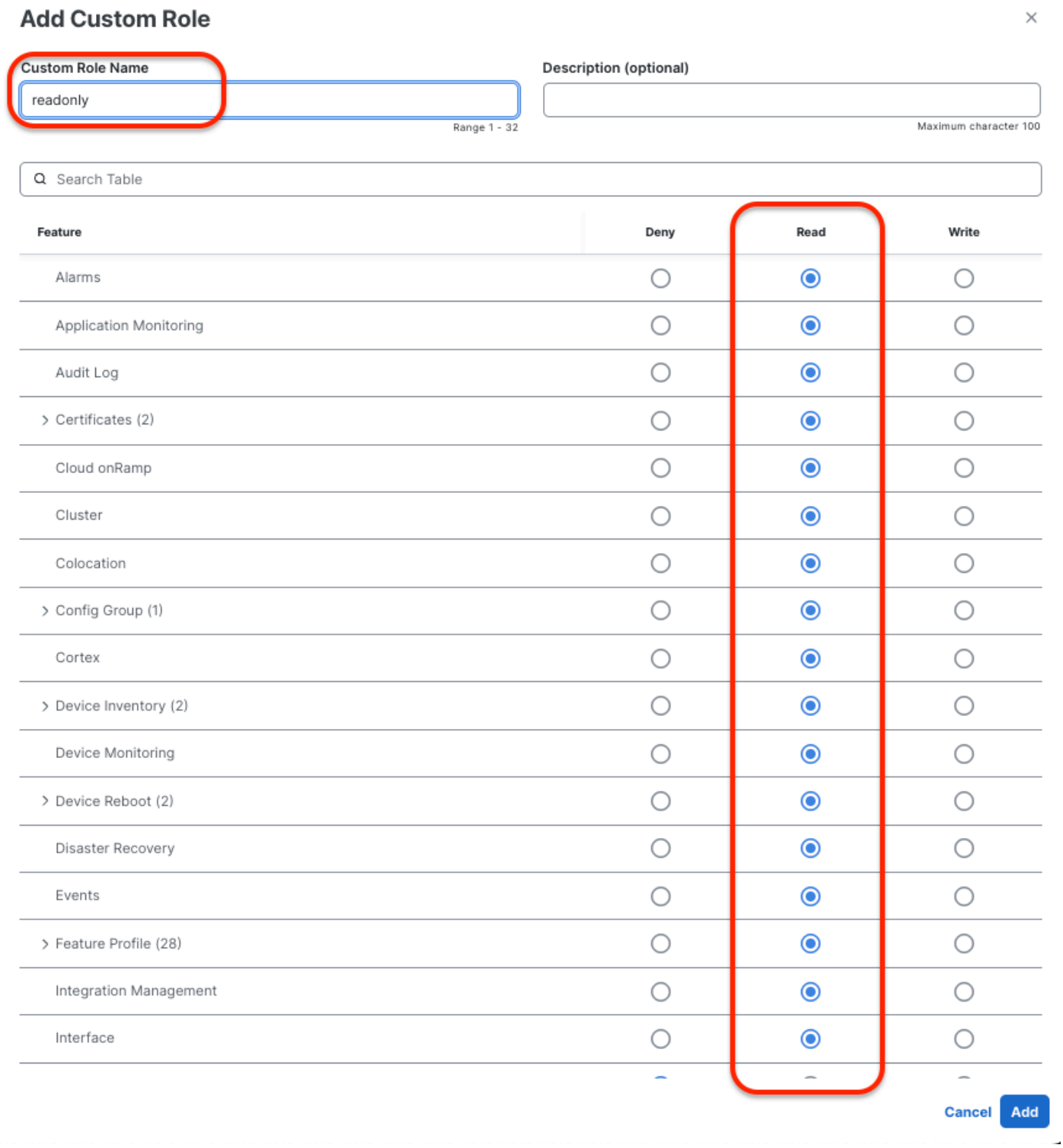
2つのカスタムロールを作成します。

1. 管理者ロール：super-admin
2. 読み取り専用ロール：読み取り専用

これは、Catalyst SD-WAN: Administration > Users and Access > Roles > Click > Add Roleの順にタブから実行できます。



管理者ロール（スーパー管理者）



読み取り専用ロール（読み取り専用）

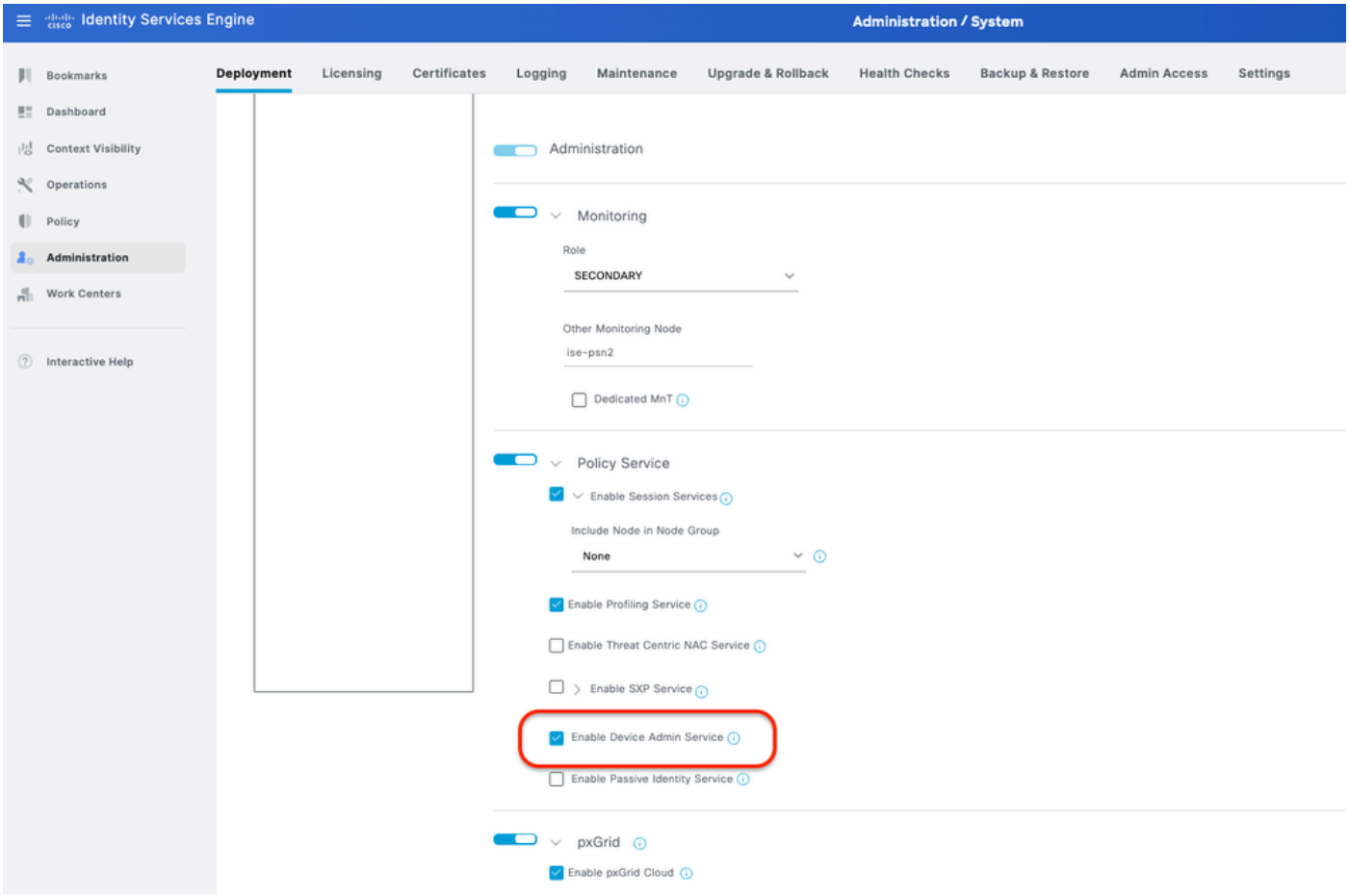
ステップ 2：TACACS+(CLI)を使用して外部認証を設定します。

```
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+の設定

TACACS+用のISEの設定

ステップ 1：Enable Device Admin Service.
これは、タブAdministration > System > Deployment >Edit (ISE PSN Node)> Check Enable Device Admin Serviceから実行できます。



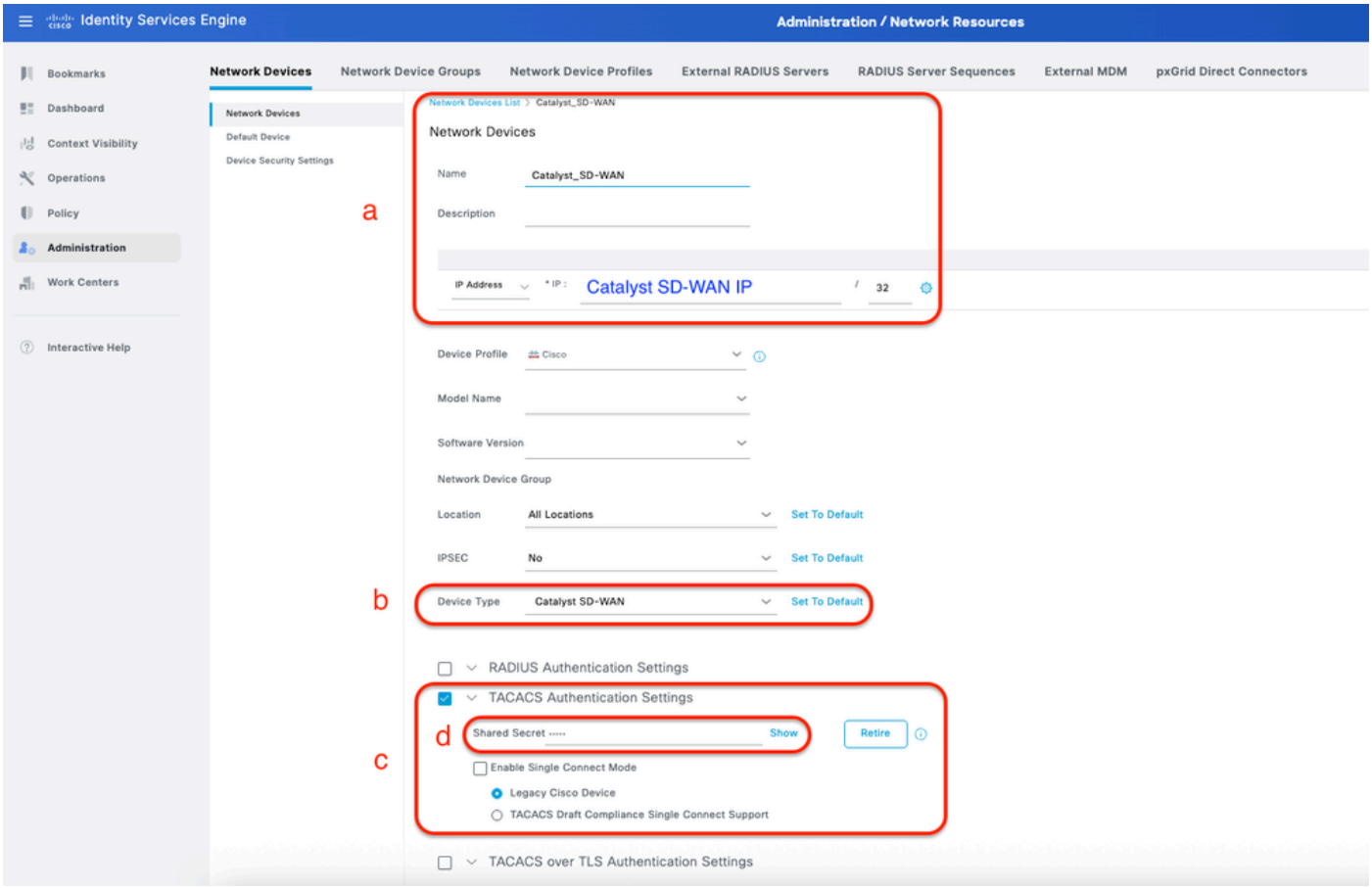
[デバイス管理サービスを有効にする（Enable Device Admin Service）]

ステップ 2：ISEのネットワークデバイスとしてCatalyst SD-WANを追加します。

これは、タブAdministration > Network Resources > Network Devicesから実行できます。

手順

a. (Catalyst SD-WAN)ネットワークデバイスの名前とIPを定義します。
b. （オプション）ポリシーセット条件のデバイスタイプを分類します。
c. TACACS+認証設定を有効にします。
d. TACACS+共有秘密を設定します。



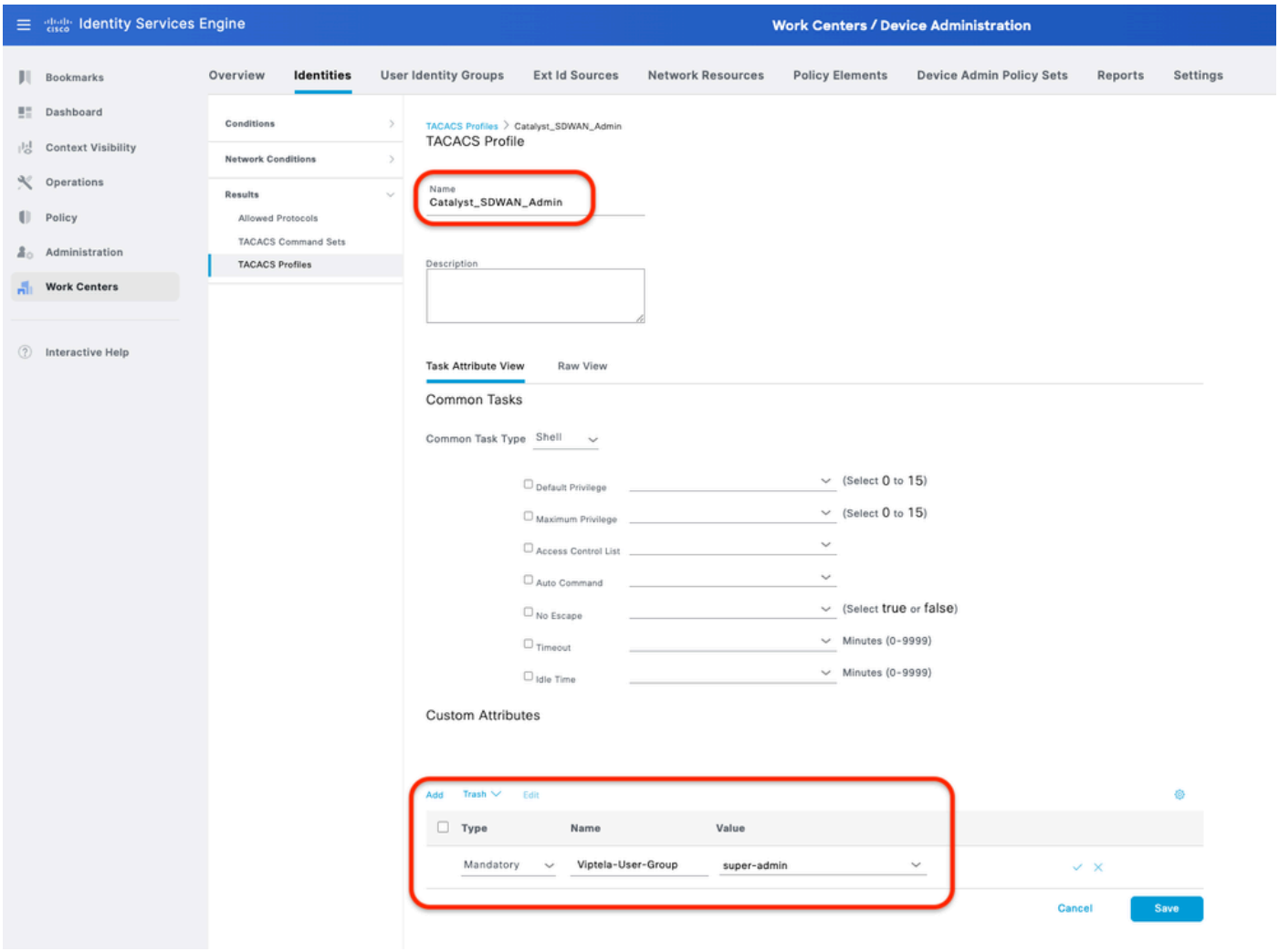
TACACS+用ISEネットワークデバイス(Catalyst SD-WAN)

ステップ 3：Catalyst SD-WANのロールごとにTACACS+プロファイルを作成します。

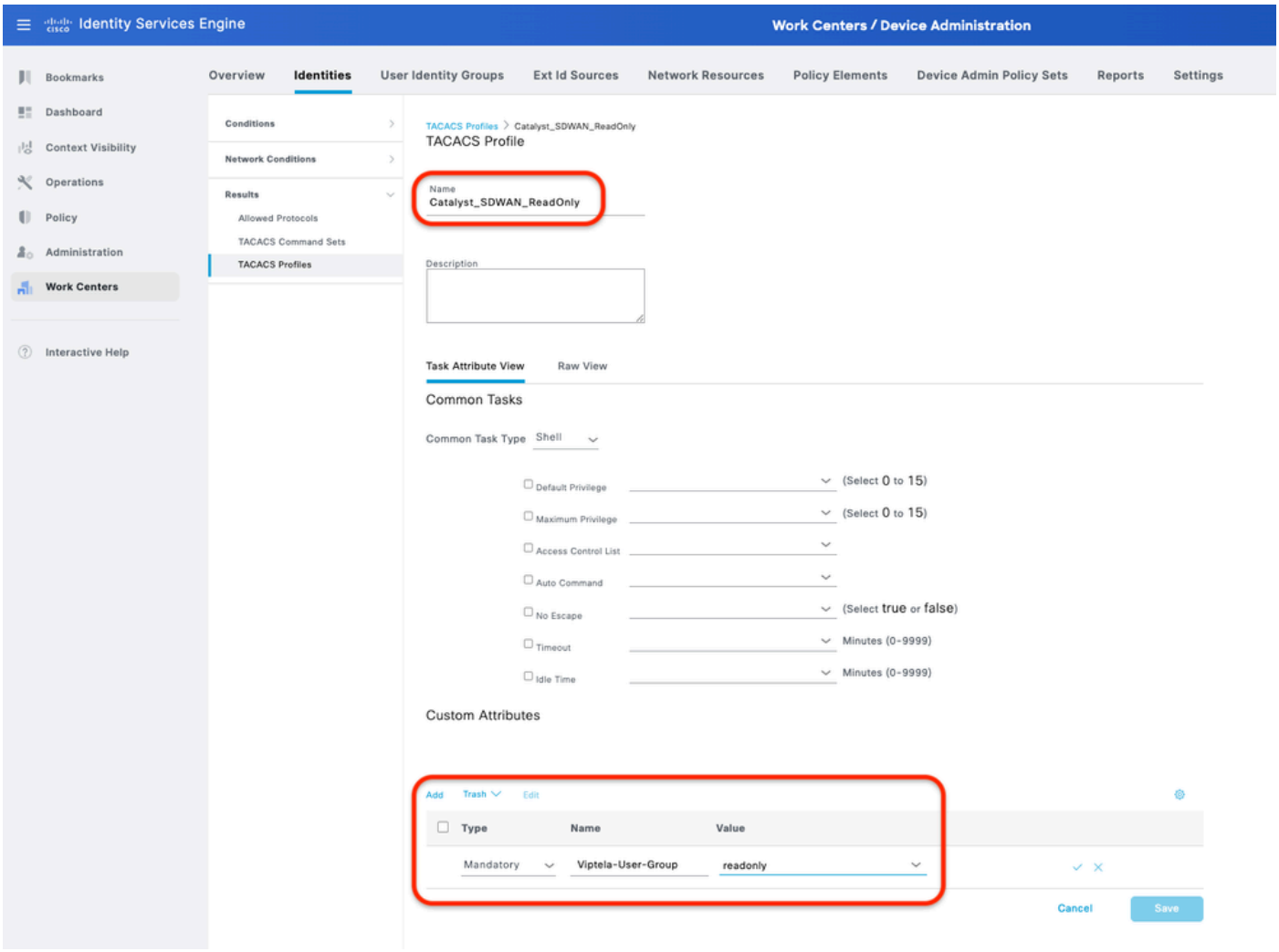
TACACS+プロファイルを作成します。

1. Catalyst_SDWAN_Admin：スーパー管理者ユーザ用。
2. Catalyst_SDWAN_ReadOnly：読み取り専用ユーザ用。

これは、タブWork Centers > Device Administration > Policy Elements > Results > TACACS Profiles > Addから実行できます。



TACACS+プロファイル(Catalyst_SDWAN_Admin)



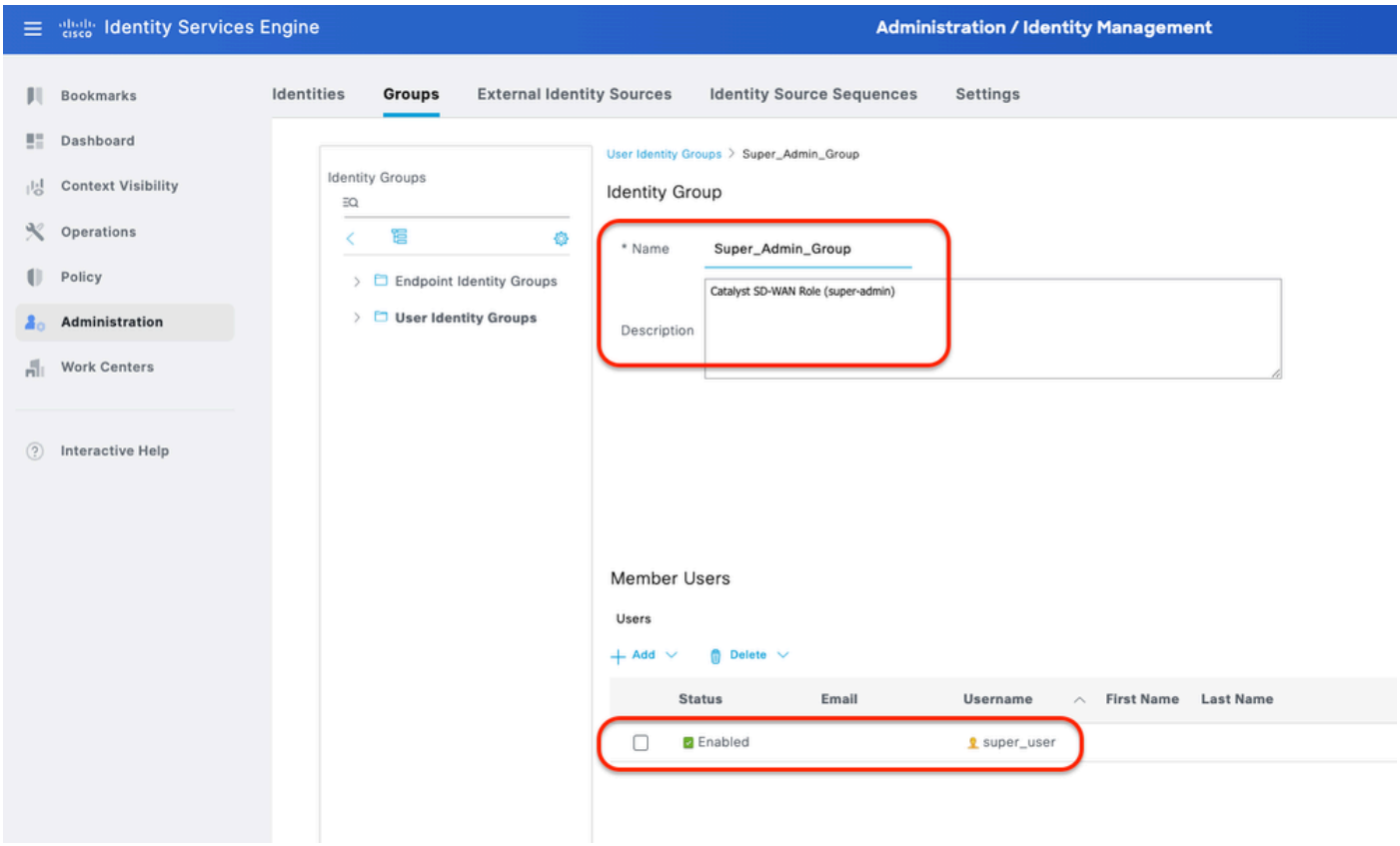
TACACS+プロファイル(Catalyst_SDWAN_ReadOnly)

ステップ 4：ユーザグループを作成し、メンバとしてローカルユーザを追加します。

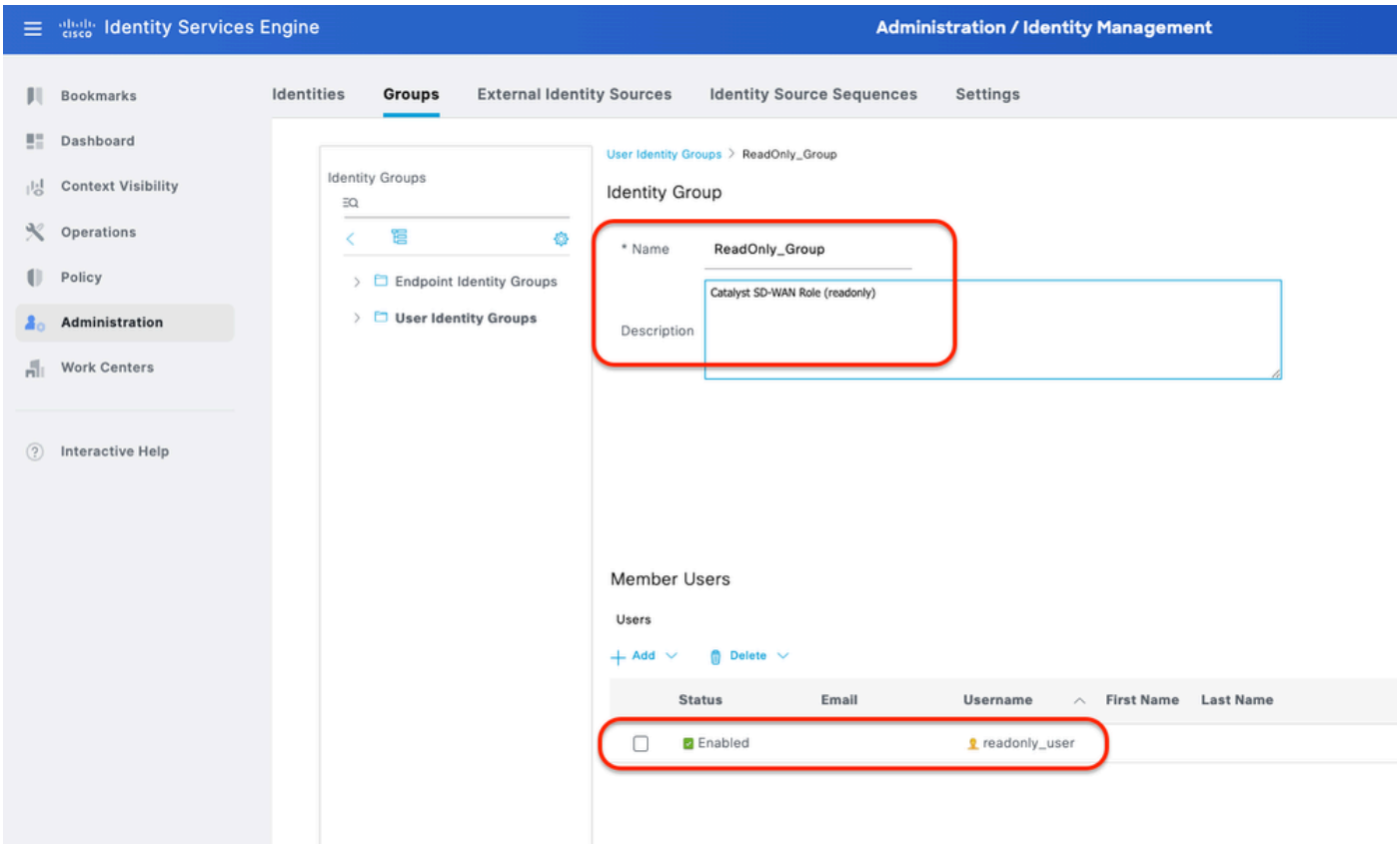
これは、タブWork Centers > Device Administration > User Identity Groupsから実行できます。

2つのユーザIDグループを作成します。

1. スーパー管理者グループ
2. 読み取り専用グループ



ユーザーIDグループ – (Super_Admin_Group)



ユーザーIDグループ – (ReadOnly_Group)

ステップ5: (オプション) TACACS+ポリシーセットを追加します。

これは、タブWork Centers > Device Administration > Device Admin Policy Setsから実行できます。

手順

a. Actionsをクリックし、選択(上に新しい行を挿入)します。

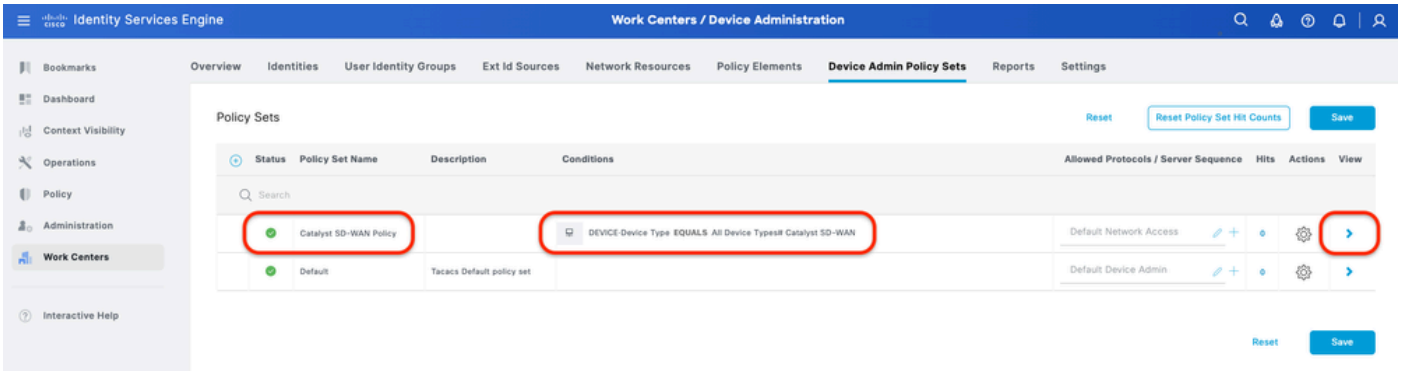
b. ポリシーセット名を定義します。

c.ポリシーセットConditionを、先ほど作成したSelect Device Type（ステップ2 > b）に設定します。

d. Allowed protocolsを設定します。

e. Saveをクリックします。

f. (>)Policy Set Viewをクリックして、認証および認可ルールを設定します。



ISEポリシーセット

手順 6：TACACS+認証ポリシーを設定します。

これを行うには、タブWork Centers > Device Administration > Device Admin Policy Sets >(>)をクリックします。

手順

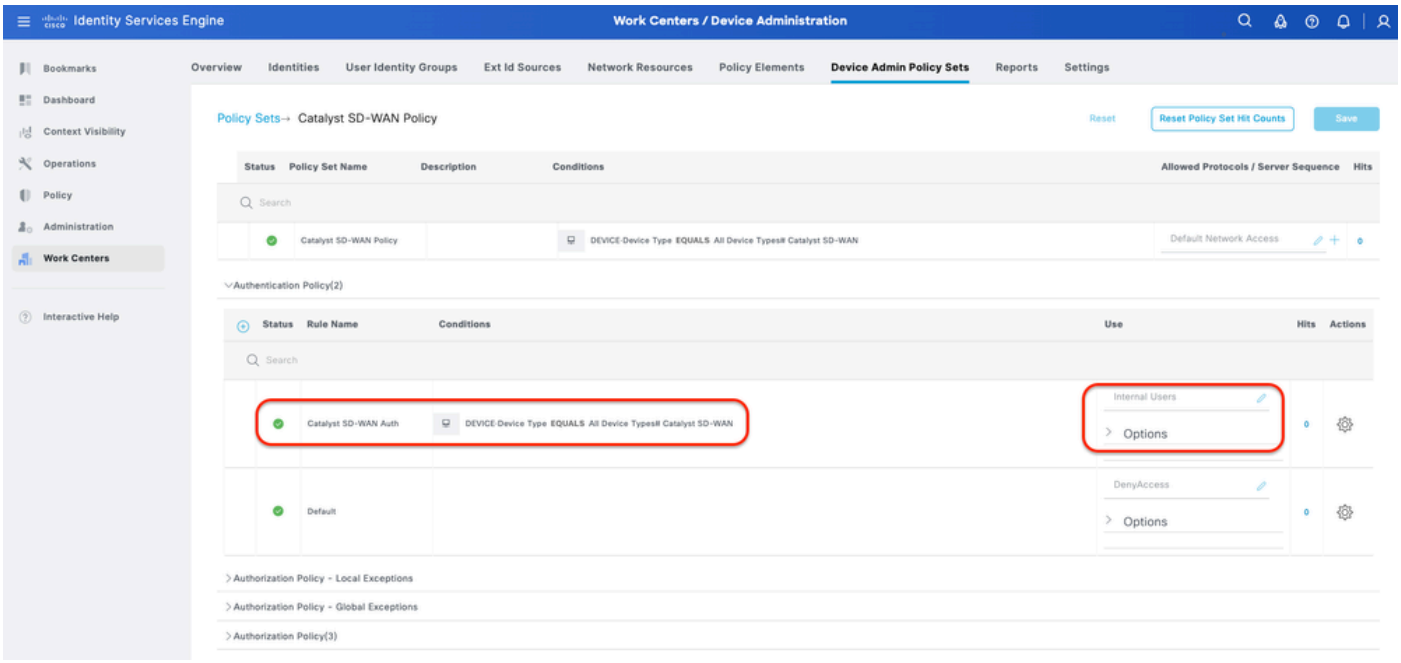
a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b. 認証ポリシー名を定義します。

c.認証ポリシーConditionを設定し、前に作成したDevice Type（ステップ2 > b）を選択します。

d.アイデンティティソースの認証ポリシーUseを設定します。

e. Saveをクリックします。



認証ポリシー

手順 7：TACACS+認可ポリシーを設定します。

これを行うには、タブWork Centers > Device Administration > Device Admin Policy Sets >(>)の順にクリックします。

各Catalyst SD-WANロールの許可ポリシーを作成するには、次の手順に従います。

- Catalyst SD-WAN認証（スーパー管理者）：スーパー管理者
- Catalyst SD-WAN認証（読み取り専用）：読み取り専用

手順

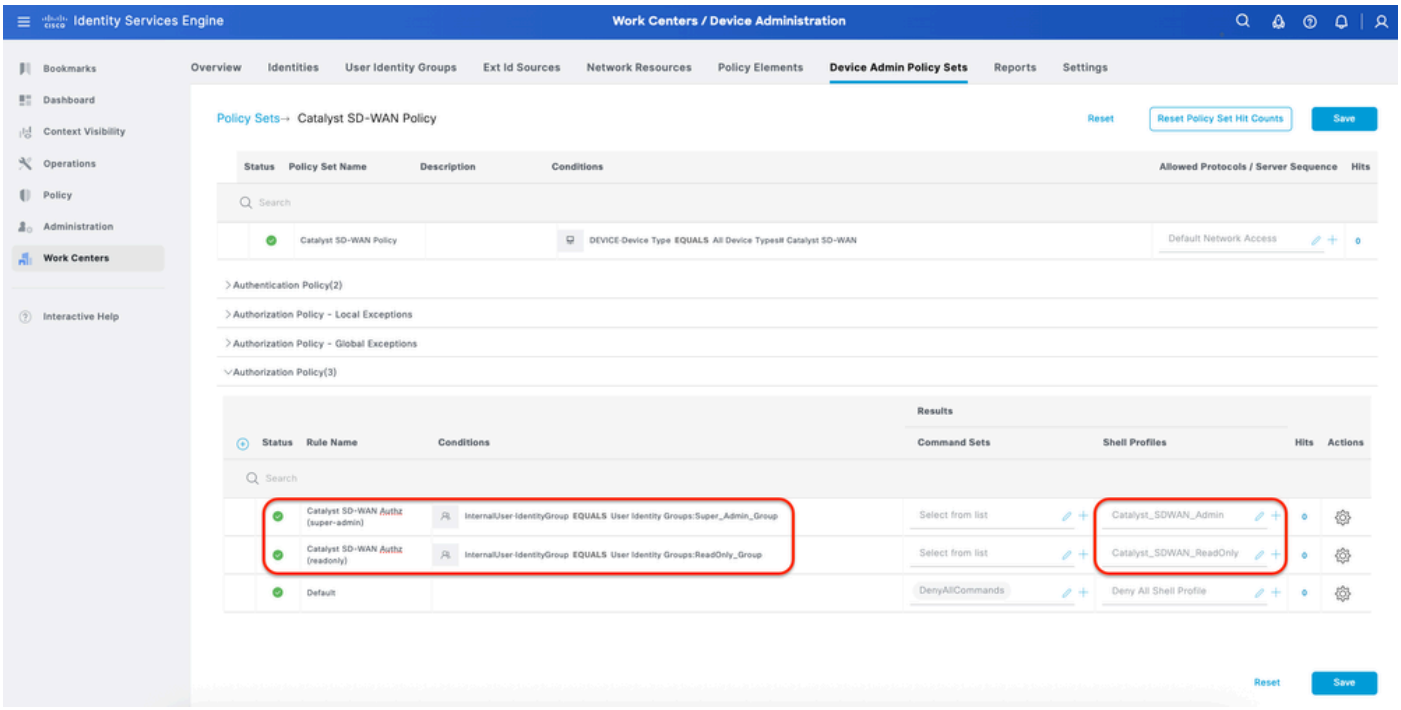
a. Actionsをクリックし、選択(上に新しい行を挿入)します。

b. 許可ポリシー名を定義します。

c.許可ポリシー条件を設定し、（ステップ4）で作成したユーザグループを選択します。

d.許可PolicyShellプロファイルを設定し、（ステップ3）で作成したTACACSプロファイルを選択します。

e. Saveをクリックします。

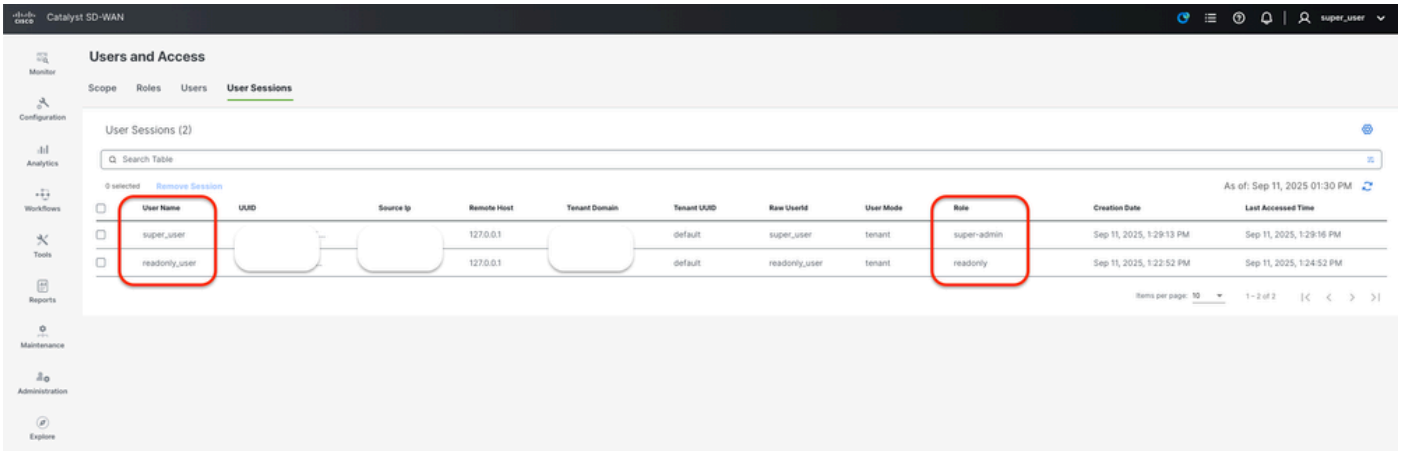


認可ポリシー

TACACS+設定の確認

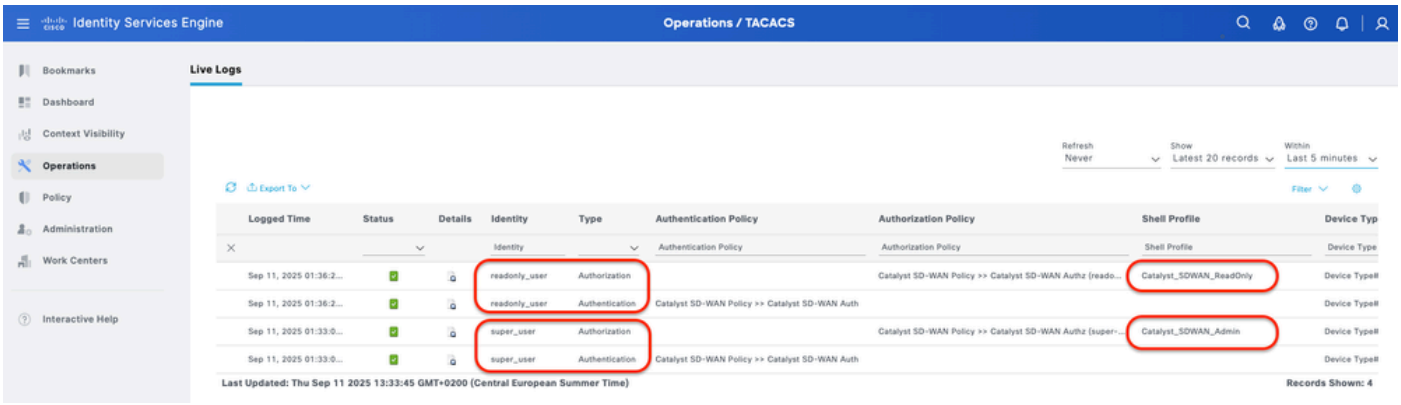
1- Catalyst SD-WASユーザセッションの表示Catalyst SD-WAN:Administration > Users and Access > User Sessions

RADIUSから初めてログインした外部ユーザのリストを表示できます。表示される情報には、ユーザ名とロールが含まれます。



Catalyst SD-WASユーザセッション

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

ライブログ

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; }

詳細なライブログ (読み取り専用)

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; }

トラブルシュート

現在のところ、この設定に関する特定の診断情報はありません。

参考資料

- Cisco Identity Services Engine 管理者ガイド リリース 3.4
- Cisco Catalyst SD-WANシステムおよびインターフェイスコンフィギュレーションガイド、Cisco IOS XE Catalyst SD-WANリリース17.x

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。