

# Configurer ISE en tant qu'authentification externe pour l'interface utilisateur graphique SD-WAN de Catalyst

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Avant de commencer](#)

[Configuration - Utilisation de TACACS+](#)

[Configuration du SD-WAN Catalyst à l'aide de TACACS+](#)

[Configurer ISE pour TACACS+](#)

[Vérification de la configuration TACACS+](#)

[Dépannage](#)

[Références](#)

---

## Introduction

Ce document décrit comment configurer Cisco Identity Services Engine(ISE) en tant qu'authentification externe pour l'administration de l'interface utilisateur graphique Cisco Catalyst SD-WAN.

## Conditions préalables

### Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- protocole TACACS+
- Administration des périphériques Cisco ISE
- Administration SD-WAN de Cisco Catalyst
- Évaluation de la politique Cisco ISE

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif2 de Cisco Identity Services Engine (ISE) version 3.4

- Cisco Catalyst SD-WAN version 20.15.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Avant de commencer

À partir de la version 20.9.1 de Cisco vManage, de nouvelles balises sont utilisées dans l'authentification :

- Viptela-User-Group : pour les définitions de groupes d'utilisateurs au lieu de Viptela-Group-Name.
- Viptela-Resource-Group : pour les définitions de groupes de ressources.

## Configuration - Utilisation de TACACS+

### Configuration du SD-WAN Catalyst à l'aide de TACACS+

#### Procédure

Étape 1. (Facultatif) Définissez des rôles personnalisés.

Configurez vos rôles personnalisés en fonction de vos besoins. Vous pouvez utiliser les rôles d'utilisateurs par défaut. Vous pouvez effectuer cette opération à partir de l'onglet Catalyst SD-WAN : Administration > Utilisateurs et accès > Rôles.

Créez deux rôles personnalisés :

1. Rôle Admin : super-administrateur
2. Rôle en lecture seule : en lecture seule

Vous pouvez effectuer cette opération à partir de l'onglet Catalyst SD-WAN : Administration > Utilisateurs et accès > Rôles > Cliquez sur > Ajouter un rôle.

Add Custom Role



Custom Role Name

super-admin

Range 1 - 32

Description (optional)

Maximum character 100

Search Table

| Feature                | Deny                  | Read                  | Write                            |
|------------------------|-----------------------|-----------------------|----------------------------------|
| Alarms                 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Application Monitoring | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Audit Log              | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| > Certificates (2)     | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Cloud onRamp           | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Cluster                | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Colocation             | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| > Config Group (1)     | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Cortex                 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| > Device Inventory (2) | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Device Monitoring      | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| > Device Reboot (2)    | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Disaster Recovery      | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Events                 | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| > Feature Profile (28) | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Integration Management | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |
| Interface              | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> |

Cancel Add

Rôle admin (super-admin)

## Add Custom Role



Custom Role Name

readonly

Range 1 - 32

Description (optional)

Maximum character 100

Q Search Table

| Feature                | Deny                  | Read                             | Write                 |
|------------------------|-----------------------|----------------------------------|-----------------------|
| Alarms                 | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Application Monitoring | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Audit Log              | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| > Certificates (2)     | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Cloud onRamp           | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Cluster                | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Colocation             | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| > Config Group (1)     | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Cortex                 | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| > Device Inventory (2) | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Device Monitoring      | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| > Device Reboot (2)    | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Disaster Recovery      | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Events                 | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| > Feature Profile (28) | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Integration Management | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |
| Interface              | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> |

Cancel

Add

Rôle en lecture seule (lecture seule)

Étape 2 : configuration de l'authentification externe à l'aide de TACACS+ (CLI)

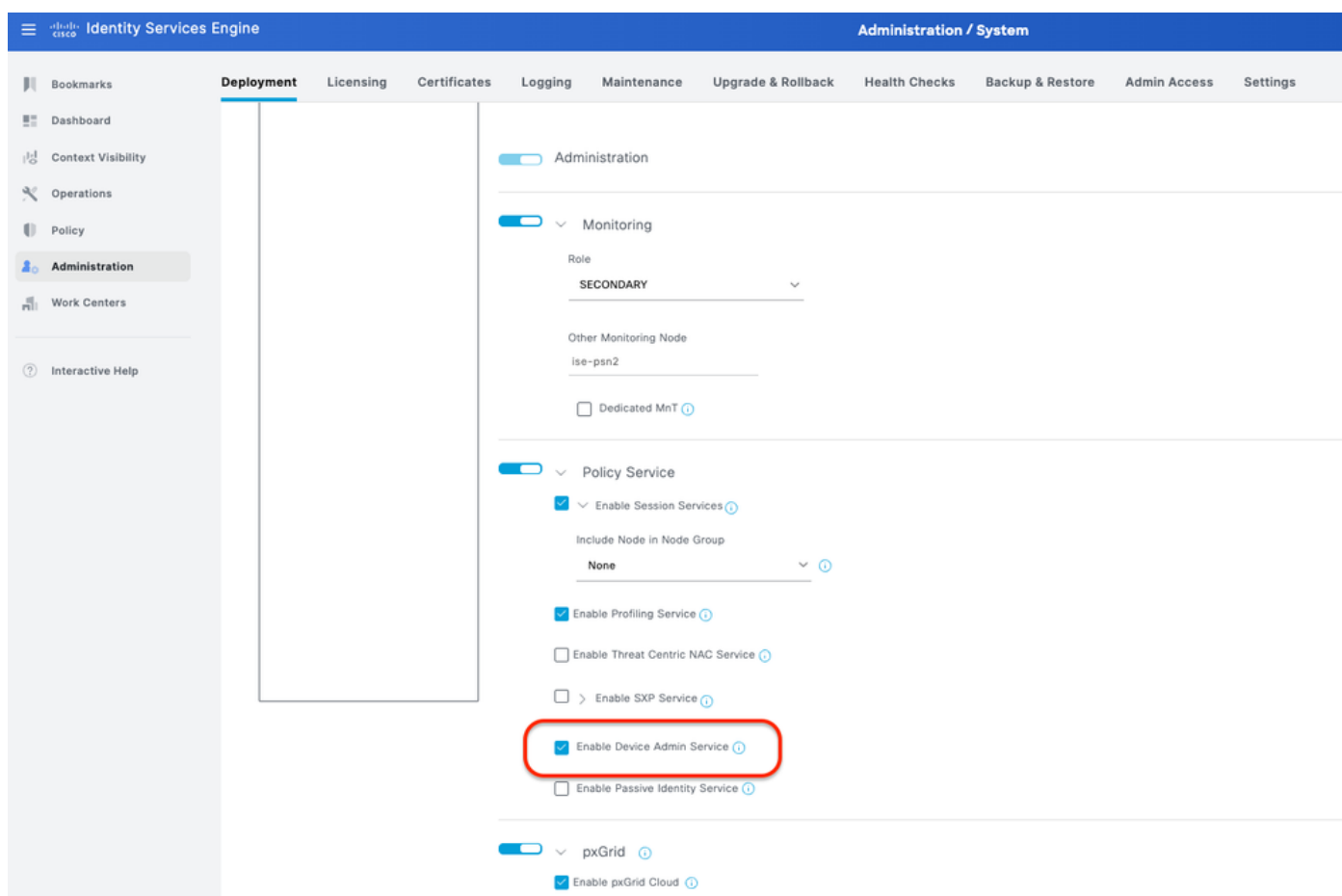
```
Entering configuration mode terminal
vmanage(config)#
vmanage(config)#
vmanage(config)# system
vmanage(config-system)# aaa
vmanage(config-aaa)# auth-order tacacs radius local
vmanage(config-aaa)# auth-fallback
vmanage(config-aaa)# commit and-quit
Commit complete.
```

CLI vManager - Configuration de TACACS+

## Configurer ISE pour TACACS+

Étape 1 : activation du service d'administration des périphériques

Pour ce faire, accédez à l'onglet Administration > System > Deployment > Edit (ISE PSN Node)>Check Enable Device Admin Service.



Activer le service d'administration des périphériques

Étape 2. Ajout du SD-WAN Catalyst en tant que périphérique réseau sur ISE

Pour ce faire, accédez à l'onglet Administration > Network Resources > Network Devices.

## Procédure

- Définissez le nom et l'IP du périphérique réseau (Catalyst SD-WAN).
- (Facultatif) Classez le type de périphérique pour la condition Jeu de stratégies.
- Activez les paramètres d'authentification TACACS+.
- Définissez le secret partagé TACACS+.

Network Devices List > Catalyst\_SD-WAN

**Network Devices**

Name: Catalyst\_SD-WAN

Description: \_\_\_\_\_

IP Address: \* IP: Catalyst SD-WAN IP / 32

Device Profile: Cisco

Model Name: \_\_\_\_\_

Software Version: \_\_\_\_\_

Network Device Group: \_\_\_\_\_

Location: All Locations [Set To Default](#)

IPSEC: No [Set To Default](#)

Device Type: Catalyst SD-WAN [Set To Default](#)

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

Shared Secret: \_\_\_\_\_ [Show](#) [Retire](#)

☐ Enable Single Connect Mode

☒ Legacy Cisco Device

☐ TACACS Draft Compliance Single Connect Support

☐ TACACS over TLS Authentication Settings

Périphérique réseau ISE (Catalyst SD-WAN) pour TACACS+

### Étape 3 : création du profil TACACS+ pour chaque rôle SD-WAN Catalyst

Créer des profils TACACS+ :

- Catalyst\_SDWAN\_Admin : Pour les super administrateurs.
- Catalyst\_SDWAN\_ReadOnly : Pour les utilisateurs en lecture seule.

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles > Add.

Identity Services Engine

Work Centers / Device Administration

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Overview

Identities

User Identity Groups

Ext Id Sources

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Settings

Conditions

Network Conditions

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles > Catalyst\_SDWAN\_Admin

TACACS Profile

Name

Catalyst\_SDWAN\_Admin

Description

Task Attribute View

Raw View

Common Tasks

Common Task Type

Shell

☐

Default Privilege

(Select 0 to 15)

☐

Maximum Privilege

(Select 0 to 15)

☐

Access Control List

☐

Auto Command

☐

No Escape

(Select true or false)

☐

Timeout

Minutes (0-9999)

☐

Idle Time

Minutes (0-9999)

Custom Attributes

Add

Trash

Edit

☐

Type

Name

Value

Mandatory

Viptela-User-Group

super-admin

✓

✕

Cancel

Save

Profil TACACS+ - (Catalyst\_SDWAN\_Admin)

Identity Services Engine Work Centers / Device Administration

Overview **Identities** User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Bookmarks Dashboard Context Visibility Operations Policy Administration **Work Centers** Interactive Help

Conditions > Network Conditions > Results > Allowed Protocols > TACACS Command Sets > **TACACS Profiles**

TACACS Profiles > Catalyst\_SDWAN\_ReadOnly

**TACACS Profile**

Name: Catalyst\_SDWAN\_ReadOnly

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

☐ Default Privilege (Select 0 to 15)  
☐ Maximum Privilege (Select 0 to 15)  
☐ Access Control List  
☐ Auto Command  
☐ No Escape (Select true or false)  
☐ Timeout (Minutes (0-9999))  
☐ Idle Time (Minutes (0-9999))

Custom Attributes

| Type      | Name               | Value    |
|-----------|--------------------|----------|
| Mandatory | Viptela-User-Group | readonly |

Cancel Save

Profil TACACS+ - (Catalyst\_SDWAN\_ReadOnly)

Étape 4. Créer un groupe d'utilisateurs ajouter des utilisateurs locaux en tant que membre

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > User Identity Groups.

Créez deux groupes d'identités utilisateur :

1. Groupe\_Admin\_Supérieur
2. Groupe\_LectureSeule

Identity Services Engine Administration / Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > Super\_Admin\_Group

Identity Group

\* Name Super\_Admin\_Group

Description Catalyst SD-WAN Role (super-admin)

Member Users

Users

+ Add - Delete

| Status                   | Email   | Username   | First Name | Last Name |
|--------------------------|---------|------------|------------|-----------|
| <input type="checkbox"/> | Enabled | super_user |            |           |

Groupe d'identités utilisateur - (Super\_Admin\_Group)

Identity Services Engine Administration / Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > ReadOnly\_Group

Identity Group

\* Name ReadOnly\_Group

Description Catalyst SD-WAN Role (readonly)

Member Users

Users

+ Add - Delete

| Status                   | Email   | Username      | First Name | Last Name |
|--------------------------|---------|---------------|------------|-----------|
| <input type="checkbox"/> | Enabled | readonly_user |            |           |

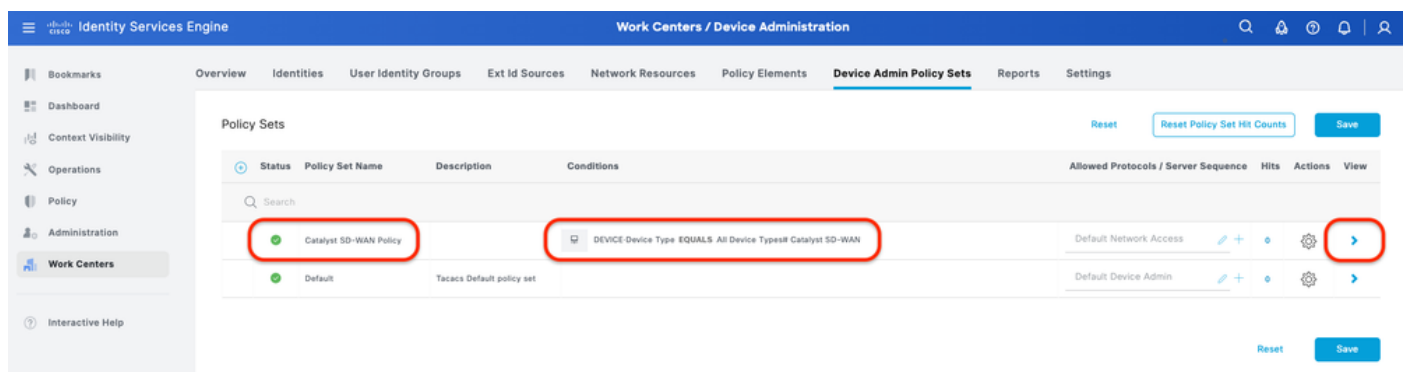
Groupe d'identités utilisateur - (ReadOnly\_Group)

Étape 5. (Facultatif) Ajouter un jeu de stratégies TACACS+.

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets.

### Procédure

- Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).
- Définissez le nom du jeu de stratégies.
- Définissez la condition du jeu de stratégies sur Sélectionner le type de périphérique précédemment créé (Étape 2 > b).
- Définissez les protocoles autorisés.
- Cliquez sur Save.
- Cliquez sur (>) Policy Set View pour configurer les règles d'authentification et d'autorisation.



Ensemble de stratégies ISE

### Étape 6 : configuration de la stratégie d'authentification TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

### Procédure

- Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).
- Définissez le nom de la stratégie d'authentification.
- Définissez la condition de stratégie d'authentification et sélectionnez le type de périphérique que vous avez créé précédemment (Étape 2 > b).
- Définissez l'option Authentication Policy Use for Identity source.
- Cliquez sur Save.

Stratégie d'authentification

## Étape 7 : configuration de la stratégie d'autorisation TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

Cette étape de création d'une politique d'autorisation pour chaque rôle SD-WAN Catalyst :

- Catalyst SD-WAN Authz (super-admin) : super-administrateur
- Catalyst SD-WAN Authz (lecture seule) : en lecture seule

### Procédure

- Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).
- Définissez le nom de la stratégie d'autorisation.
- Définissez la condition de stratégie d'autorisation et sélectionnez le groupe d'utilisateurs que vous avez créé à l' (étape 4).
- Définissez les profils PolicyShell d'autorisation et sélectionnez le profil TACACS que vous avez créé à l' (étape 3).
- Cliquez sur Save.

Identity Services Engine Work Centers / Device Administration

Policy Sets - Catalyst SD-WAN Policy

Reset Reset Policy Set Hit Counts Save

| Status | Policy Set Name        | Description | Conditions                                                 | Allowed Protocols / Server Sequence | Hits |
|--------|------------------------|-------------|------------------------------------------------------------|-------------------------------------|------|
| ●      | Catalyst SD-WAN Policy |             | DEVICE Device Type EQUALS All Device Types Catalyst SD-WAN | Default Network Access              | 0    |

> Authentication Policy(2)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

< Authorization Policy(3)

| Status | Rule Name                           | Conditions                                                               | Results         | Command Sets           | Shell Profiles          | Hits | Actions |
|--------|-------------------------------------|--------------------------------------------------------------------------|-----------------|------------------------|-------------------------|------|---------|
| ●      | Catalyst SD-WAN Authz (super-admin) | InternalUser IdentityGroup EQUALS User Identity Groups:Super_Admin_Group |                 | Select from list       | Catalyst_SDWAN_Admin    | 0    |         |
| ●      | Catalyst SD-WAN Authz (readonly)    | InternalUser IdentityGroup EQUALS User Identity Groups:ReadOnly_Group    |                 | Select from list       | Catalyst_SDWAN_ReadOnly | 0    |         |
| ●      | Default                             |                                                                          | DenyAllCommands | Deny All Shell Profile | 0                       |      |         |

Reset Save

Politique d'autorisation

## Vérification de la configuration TACACS+

1- Afficher les sessions utilisateur Catalyst SD-WAS Catalyst SD-WAN : Administration > Users and Access > User Sessions.

Vous pouvez afficher la liste des utilisateurs externes qui se sont connectés via RADIUS pour la première fois. Les informations affichées incluent leurs noms d'utilisateur et leurs rôles.

Catalyst SD-WAN

Users and Access

Scope Roles Users User Sessions

User Sessions (2)

Search Table

0 selected Remove Session

|                          | User Name     | UUID | Source Ip | Remote Host | Tenant Domain | Tenant UUID | Raw Userid    | User Mode | Role        | Creation Date            | Last Accessed Time       |
|--------------------------|---------------|------|-----------|-------------|---------------|-------------|---------------|-----------|-------------|--------------------------|--------------------------|
| <input type="checkbox"/> | super_user    |      |           | 127.0.0.1   |               | default     | super_user    | tenant    | super-admin | Sep 11, 2025, 1:29:13 PM | Sep 11, 2025, 1:29:16 PM |
| <input type="checkbox"/> | readonly_user |      |           | 127.0.0.1   |               | default     | readonly_user | tenant    | readonly    | Sep 11, 2025, 1:22:52 PM | Sep 11, 2025, 1:24:52 PM |

Items per page: 10 1 - 2 of 2 < > >>

Sessions utilisateur Catalyst SD-WAS

2- ISE - Opérations TACACS Live-Logs > TACACS > Live-Logs.

Identity Services Engine

Operations / TACACS

Search

Alerts

Help

Logout

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Live Logs

Export To

Refresh Never

Show Latest 20 records

Within Last 5 minutes

Filter

| Logged Time             | Status | Details | Identity      | Type           | Authentication Policy                           | Authorization Policy                                      | Shell Profile           | Device Type  |
|-------------------------|--------|---------|---------------|----------------|-------------------------------------------------|-----------------------------------------------------------|-------------------------|--------------|
| Sep 11, 2025 01:36:2... |        |         | readonly_user | Authorization  | Catalyst SD-WAN Policy >> Catalyst SD-WAN Authz | 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 | 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

Journaux en direct

|                                      |                                                                     |
|--------------------------------------|---------------------------------------------------------------------|
| 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; } |

Journaux en direct détaillés - (lecture seule)

|                                      |                                                                        |
|--------------------------------------|------------------------------------------------------------------------|
| 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; } |

## Dépannage

Aucune information de diagnostic spécifique n'est actuellement disponible pour cette configuration.

## Références

- [Guide de l'administrateur de Cisco Identity Services Engine, version 3.4](#)
- [Guide de configuration des interfaces et systèmes SD-WAN de Cisco Catalyst, Cisco IOS XE Catalyst SD-WAN version 17.x](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.