

Configure ISE as an External Authentication for Catalyst SD-WAN GUI

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Before You Begin](#)

[Configure - Using TACACS+](#)

[Configure Catalyst SD-WAN Using TACACS+](#)

[Configure ISE for TACACS+](#)

[Verify TACACS+ Configuration](#)

[Troubleshoot](#)

[References](#)

Introduction

This document describes how to configure Cisco Identity Services Engine(ISE) as an external authentication for Cisco Catalyst SD-WAN GUI administration.

Prerequisites

Requirements

Cisco recommends that you have the knowledge of these topics:

- TACACS+ protocol
- Cisco ISE Device Administration
- Cisco Catalyst SD-WAN Administration
- Cisco ISE Policy Evaluation

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Identity Services Engine (ISE) Version 3.4 Patch2
- 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. If your network is live, ensure that you understand the potential impact of any command.

Before You Begin

Starting from Cisco vManage Release 20.9.1, new tags are used in authentication:

- Viptela-User-Group: for user group definitions instead of Viptela-Group-Name.
- Viptela-Resource-Group: for resource group definitions.

Configure - Using TACACS+

Configure Catalyst SD-WAN Using TACACS+

Procedure

Step 1. (Optional) Define Custom Roles.

Configure your custom roles that fulfils your requirement, instead, you can use the default User Roles. This can be done from the tab **Catalyst SD-WAN: Administration > Users and Access > Roles**.

Create two Custom Roles:

1. Admin Role: **super-admin**
2. Read Only Role: **readonly**

This can be done from the tab **Catalyst SD-WAN: Administration > Users and Access > Roles > Click > Add Role**.

Add Custom Role



Custom Role Name

super-admin

Description (optional)

Range 1 - 32

Maximum character 100

Q 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

Admin Role (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	☐	☒	☐
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

Read -Only Role (readonly)

Step 2. Configure **External Authentication** using 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.

```

vManger CLI - TACACS+ Configuration

Configure ISE for TACACS+

Step 1. Enable Device Admin Service.

This can be done from the tab **Administration** > **System** > **Deployment** > **Edit (ISE PSN Node)** > **Check Enable Device Admin Service**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System tab, specifically the Deployment section. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Help. The main content area displays various configuration options for the ISE PSN Node. The 'Administration' section is expanded, showing 'Administration' (enabled), 'Monitoring' (enabled), and 'Policy Service' (enabled). Under 'Policy Service', the 'Enable Device Admin Service' checkbox is checked and highlighted with a red box. Other options include 'Enable Session Services', 'Include Node in Node Group', 'Enable Profiling Service', 'Enable Threat Centric NAC Service', 'Enable SXP Service', and 'Enable Passive Identity Service'. The 'pxGrid' section is also visible at the bottom, with 'pxGrid' (enabled) and 'Enable pxGrid Cloud' (checked).

Enable Device Admin Service

Step 2. Add **Catalyst SD-WAN** as a Network Device on ISE.

This can be done from the tab **Administration** > **Network Resources** > **Network Devices**.

Procedure

- Define (Catalyst SD-WAN) **Network Device** name and **IP**.
- (Optional) Classify **Device Type** for Policy Set condition.
- Enable **TACACS+ Authentication Settings**.
- Set **TACACS+ Shared Secret**.

ISE Network Device (Catalyst SD-WAN) for TACACS+

ISE Network Device (Catalyst SD-WAN) for TACACS+

Step 3. Create **TACACS+ Profile** for each Catalyst SD-WAN role.

Create TACACS+ Profiles:

- Catalyst_SDWAN_Admin: For Super Admin Users.
- Catalyst_SDWAN_ReadOnly: For Read Only Users.

This can be done from the tab **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

TACACS+ Profile - (Catalyst_SDWAN_Admin)

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_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

Add

Trash

Edit

Type	Name	Value
Mandatory	Viptela-User-Group	readonly

✓

✕

Cancel

Save

TACACS+ Profile - (Catalyst_SDWAN_ReadOnly)

Step 4. Create **User Group** add **Local Users** as a member.

This can be done from the tab **Work Centers > Device Administration > User Identity Groups**.

Create two **User Identity Groups**:

1. Super_Admin_Group
2. ReadOnly_Group

Identity Services Engine Administration / Identity Management

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

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
☐ Enabled		super_user		

User Identity Group - (Super_Admin_Group)

Identity Services Engine Administration / Identity Management

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

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
☐ Enabled		readonly_user		

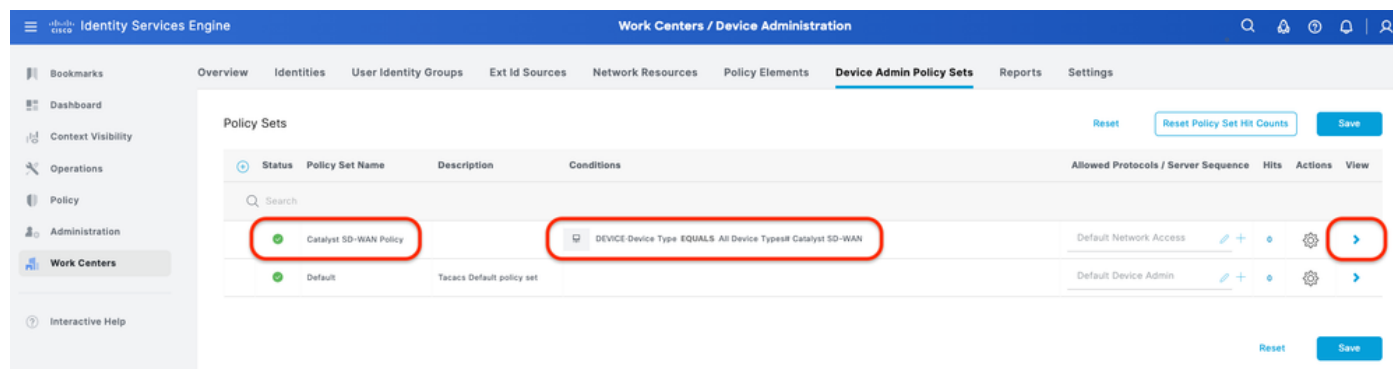
User Identity Group - (ReadOnly_Group)

Step 5. (Optional) Add **TACACS+ Policy Set**.

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets**.

Procedure

- Click **Actions** and choose (**Insert new row above**).
- Define the **Policy Set name**.
- Set the Policy Set **Condition** to **Select Device Type** you created previously on (Step 2 > b).
- Set the **Allowed protocols**.
- Click **Save**.
- Click (>) **Policy Set View** to configure authentication and authorization rules.



ISE Policy Set

Step 6. Configure TACACS+ Authentication Policy.

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets > Click (>)**.

Procedure

- Click **Actions** and choose (**Insert new row above**).
- Define the **Authentication Policy name**.
- Set the Authentication Policy **Condition** and select **Device Type** you created previously on (Step 2 > b).
- Set the Authentication Policy **Use** for Identity source.
- Click **Save**.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is selected. Under the 'Catalyst SD-WAN Policy', the 'Authentication Policy(2)' section is expanded. It lists two policies: 'Catalyst SD-WAN Auth' and 'Default'. The 'Catalyst SD-WAN Auth' policy is highlighted with a red box. The 'Conditions' column for this policy shows 'DEVICE Device Type EQUALS All Device Types Catalyst SD-WAN'. The 'Use' column shows 'Internal Users' and 'Options' are highlighted with a red box. The 'Hits' column shows '0'.

Authentication Policy

Step 7. Configure TACACS+ Authorization Policy.

This can be done from the tab **Work Centers > Device Administration > Device Admin Policy Sets > Click (>).**

This step to create Authorization Policy for each Catalyst SD-WAN Role:

- Catalyst SD-WAN Authz (super-admin): super-admin
- Catalyst SD-WAN Authz (readonly): readonly

Procedure

- Click **Actions** and **choose (Insert new row above).**
- Define the **Authorization Policy name.**
- Set the Authorization Policy **Condition** and select **User Group** that you created in (Step 4).
- Set the Authorization Policy **Shell Profiles** and select **TACACS Profile** that you created in (Step 3).
- Click **Save.**

Policy Sets - Catalyst SD-WAN Policy

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	

Authorization Policy

Verify TACACS+ Configuration

1- Display Catalyst SD-WAS User Sessions **Catalyst SD-WAN: Administration > Users and Access > User Sessions.**

You can view the list of external users who have logged in through RADIUS for the first time. The information that is displayed includes their usernames and roles.

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
☐	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
☐	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

Catalyst SD-WAS User Sessions

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

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
X			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 (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

Live-Logs

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; }

Detailed Live-Logs - (readonly)

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; }

Troubleshoot

There is currently no specific diagnostic information available for this configuration.

References

- [Cisco Identity Services Engine Administrator Guide, Release 3.4](#)
- [Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x](#)