

Configurazione di ISE come autenticazione esterna per l'interfaccia GUI Catalyst SD-WAN

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Operazioni preliminari](#)

[Configurazione - Uso di TACACS+](#)

[Configurazione di Catalyst SD-WAN con TACACS+](#)

[Configurare ISE per TACACS+](#)

[Verifica configurazione TACACS+](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

Introduzione

Questo documento descrive come configurare Cisco Identity Services Engine (ISE) come autenticazione esterna per l'amministrazione della GUI di Cisco Catalyst SD-WAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Patch2 di Cisco Identity Services Engine (ISE) versione 3.4
- Cisco Catalyst SD-WAN versione 20.15.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Operazioni preliminari

A partire da Cisco vManage release 20.9.1, i nuovi tag vengono utilizzati nell'autenticazione:

- Viptela-User-Group: per le definizioni dei gruppi di utenti invece di Viptela-Group-Name.
- Viptela-Resource-Group: per le definizioni dei gruppi di risorse.

Configurazione - Uso di TACACS+

Configurazione di Catalyst SD-WAN con TACACS+

Procedura

Passaggio 1. (Facoltativo) Definire Ruoli Personalizzati.

Configurare i ruoli personalizzati che soddisfano i requisiti, è possibile utilizzare i ruoli utente predefiniti. A tal fine, è possibile usare la scheda Catalyst SD-WAN: Amministrazione > Utenti e Accesso > Ruoli.

Creare due ruoli personalizzati:

1. Ruolo amministratore: amministratore privilegiato
2. Ruolo di sola lettura: sola lettura

A tal fine, è possibile usare la scheda Catalyst SD-WAN: Amministrazione > Utenti e accesso > Ruoli > Fare clic > Aggiungi ruolo.

Add Custom Role



Custom Role Name

super-admin

Range 1 - 32

Description (optional)

Maximum character 100

Q 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**

Ruolo di amministratore (amministratore privilegiato)

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

Ruolo di sola lettura (sola lettura)

Passaggio 2. Configurare l'autenticazione esterna utilizzando TACACS+ (CLI).

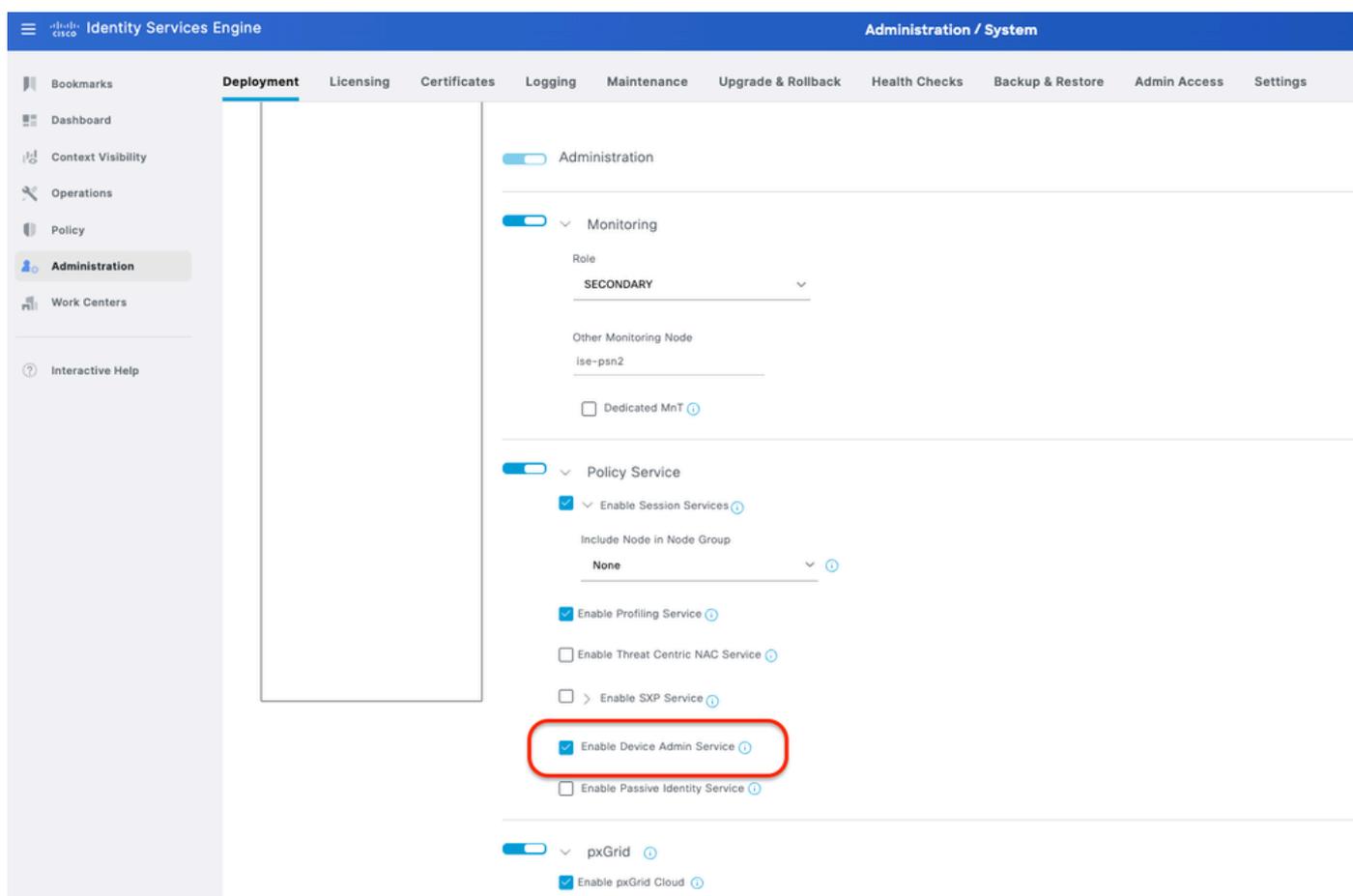
```
Entering configuration mode terminal
vmanage(config)#
vmanage(config)#
vmanage(config)# system
vmanage(config-system)# aaa
vmanage(config-aaa)# auth-order tacacs radius local
vmanage(config-aaa)# auth-fallback
vmanage(config-aaa)# commit and-quit
Commit complete.
```

CLI vManager - Configurazione TACACS+

Configurare ISE per TACACS+

Passaggio 1. Abilitare il servizio Amministrazione dispositivi.

A tale scopo, selezionare la scheda Amministrazione > Sistema > Distribuzione > Modifica (ISE PSN Node)>Selezionare Abilita servizio di amministrazione dispositivi.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System configuration page. The 'Administration' section is expanded, and the 'Enable Device Admin Service' checkbox is checked and highlighted with a red circle. The page also shows other configuration options like 'Administration', 'Monitoring', 'Policy Service', and 'pxGrid'.

Abilita servizio di amministrazione dispositivi

Passaggio 2. Aggiungere Catalyst SD-WAN come dispositivo di rete su ISE.

A tale scopo, selezionare la scheda Amministrazione > Risorse di rete > Dispositivi di rete.

Procedura

- r. Definire (Catalyst SD-WAN) il nome e l'IP del dispositivo di rete.
- b. (Facoltativo) Classificare il tipo di dispositivo per la condizione Set di criteri.
- c. Abilita le impostazioni di autenticazione TACACS+.
- d. Impostare TACACS+ Shared Secret.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main content area is titled "Administration / Network Resources" and displays the configuration for a Network Device named "Catalyst_SD-WAN". The configuration fields are:

- Name: Catalyst_SD-WAN
- Description: (empty)
- IP Address: Catalyst SD-WAN IP / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations
- IPSEC: No
- Device Type: Catalyst SD-WAN
- RADIUS Authentication Settings: (unchecked)
- TACACS Authentication Settings: (checked)
- Shared Secret: (masked with dots)
- Enable Single Connect Mode: (unchecked)
- Legacy Cisco Device: (selected)
- TACACS Draft Compliance Single Connect Support: (unchecked)
- TACACS over TLS Authentication Settings: (unchecked)

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

Passaggio 3. Creare il profilo TACACS+ per ciascun ruolo Catalyst SD-WAN.

Crea profili TACACS+:

1. Catalyst_SDWAN_Admin: Per utenti con privilegi di amministratore privilegiato.
2. Catalyst_SDWAN_ReadOnly: Per gli utenti di sola lettura.

A tale scopo, selezionare la scheda Work Center > Device Administration > Policy Elements > Results > TACACS Profiles > Add.

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

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

Type	Name	Value
Mandatory	Viptela-User-Group	super-admin

Cancel Save

Perfil TACACS+ - (Catalyst_SDWAN_Admin)

Profilo TACACS+ - (Catalyst_SDWAN_ReadOnly)

Passaggio 4. Creazione di un gruppo di utenti aggiunta di utenti locali come membro.

A tale scopo, è possibile utilizzare la scheda Centri di lavoro > Amministrazione dispositivi > Gruppi di identità utente.

Creare due gruppi di identità utente:

1. Gruppo_Amministratore_Privilegiato
2. Gruppo_solaLettura

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
<input type="checkbox"/> Enabled		super_user		

Gruppo di identità utente - (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
<input type="checkbox"/> Enabled		readonly_user		

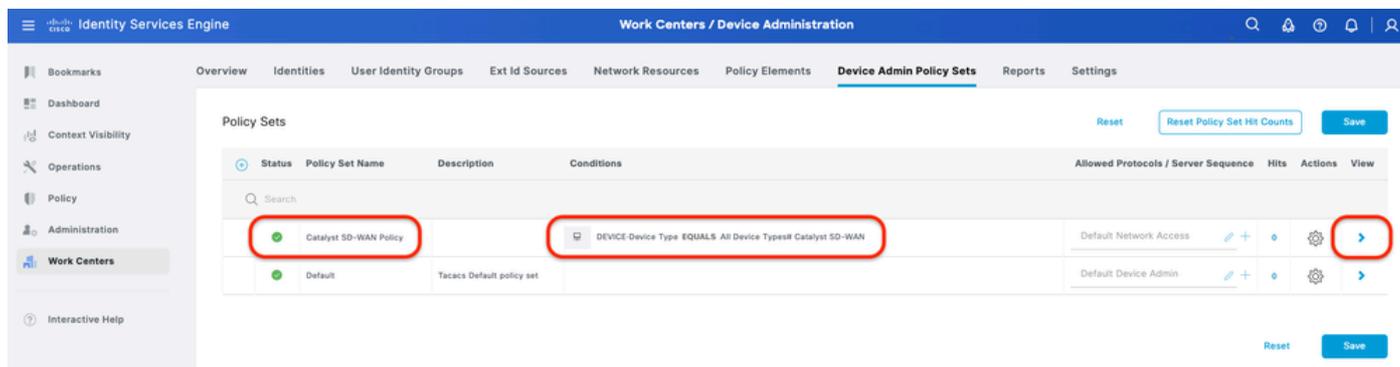
Gruppo di identità utente - (ReadOnly_Group)

Passaggio 5. (Facoltativo) Aggiungere il set di criteri TACACS+.

A tale scopo, è possibile utilizzare la scheda Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi.

Procedura

- r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).
- b. Definire il nome del set di criteri.
- c. Impostare Policy Set Condition su Select Device Type (Seleziona tipo di dispositivo) creato in precedenza (Passo 2 > b).
- d. Impostare i protocolli consentiti.
- e. Fare clic su Save (Salva).
- f. Fare clic su (>) Visualizzazione set di criteri per configurare le regole di autenticazione e autorizzazione.



ISE Policy Set

Passaggio 6. Configurare il criterio di autenticazione TACACS+.

A tale scopo, è possibile utilizzare la scheda Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi > Fare clic su (>).

Procedura

- r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).
- b. Definire il nome del criterio di autenticazione.
- c. Impostare la condizione del criterio di autenticazione e selezionare il tipo di dispositivo creato in precedenza (passo 2 > b).
- d. Impostare l'utilizzo dei criteri di autenticazione per l'origine identità.
- e. Fare clic su Save (Salva).

Criterio di autenticazione

Passaggio 7. Configurare i criteri di autorizzazione TACACS+.

A tale scopo, selezionare la scheda Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi > Fare clic su (>).

Questo passaggio consente di creare criteri di autorizzazione per ciascun ruolo Catalyst SD-WAN:

- Catalyst SD-WAN Authz (superamministratore): amministratore privilegiato
- Catalyst SD-WAN Authz (sola lettura): sola lettura

Procedura

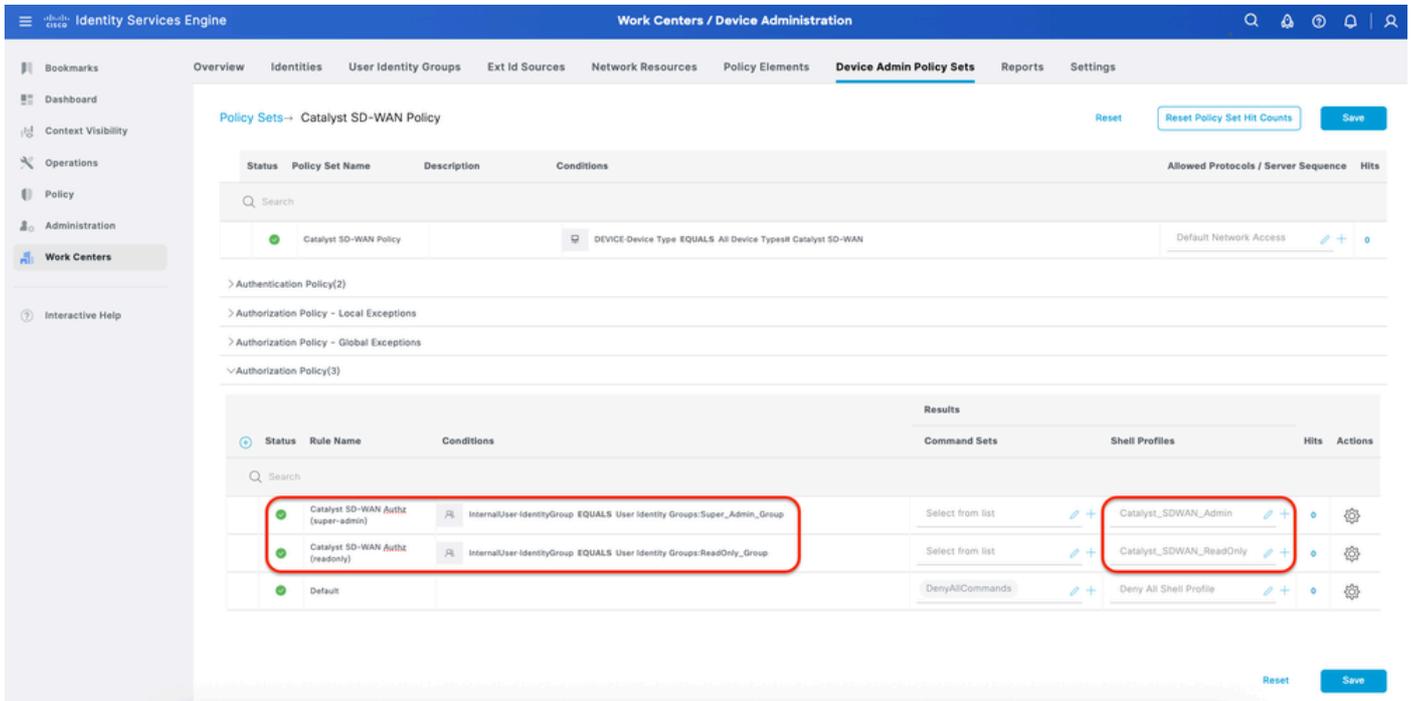
r. Fare clic su Azioni e scegliere (Inserisci nuova riga sopra).

b. Definire il nome del criterio di autorizzazione.

c. Impostare la condizione del criterio di autorizzazione e selezionare il gruppo di utenti creato in (Passaggio 4).

d. Impostare i profili della shell dei criteri di autorizzazione e selezionare il profilo TACACS creato in (Passaggio 3).

e. Fare clic su Save (Salva).

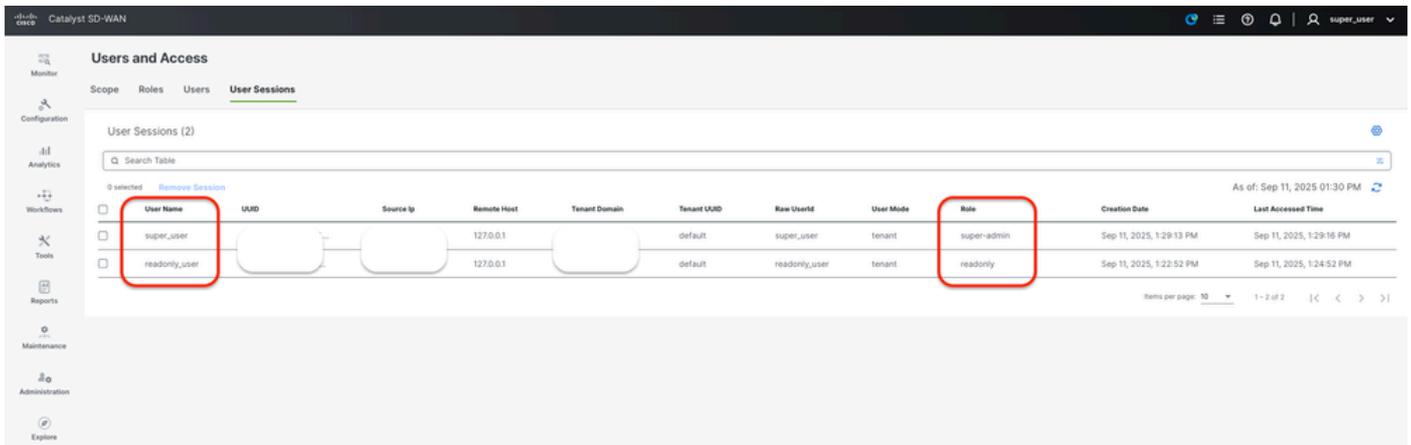


Criteri di autorizzazione

Verifica configurazione TACACS+

1- Visualizzazione delle sessioni utente Catalyst SD-WAS Catalyst SD-WAN: Amministrazione > Utenti e accesso > Sessioni utente.

È possibile visualizzare l'elenco degli utenti esterni che hanno eseguito il login tramite RADIUS per la prima volta. Le informazioni visualizzate includono i relativi nomi utente e ruoli.



Sessioni utente Catalyst SD-WAS

2- ISE - TACACS Live-Log Operazioni > TACACS > Live-Log.

Identity Services Engine Operations / TACACS

Live Logs

Refresh: Never | Show: Latest 20 records | Within: Last 5 minutes

Export To

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 Policy >> Catalyst SD-WAN Authz (reado...	Catalyst_SDWAN_ReadOnly	Device Type#
Sep 11, 2025 01:36:2...	✔		readonly_user	Authorization	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 Policy >> Catalyst SD-WAN Authz (super...	Catalyst_SDWAN_Admin	Device Type#
Sep 11, 2025 01:33:0...	✔		super_user	Authorization	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-Log

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; }

Log dettagliati in tempo reale - (sola lettura)

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; }

Risoluzione dei problemi

Non sono attualmente disponibili informazioni di diagnostica specifiche per questa configurazione.

Riferimenti

- [Guida dell'amministratore di Cisco Identity Services Engine, versione 3.4](#)
- [Guida alla configurazione di sistemi e interfacce Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN release 17.x](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).