

Configurar o ISE como uma autenticação externa para a GUI do Catalyst SD-WAN

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antes de Começar](#)

[Configurar - Usando TACACS+](#)

[Configurar o Catalyst SD-WAN usando TACACS+](#)

[Configurar ISE para TACACS+](#)

[Verificar a configuração TACACS+](#)

[Troubleshooting](#)

[Referências](#)

Introdução

Este documento descreve como configurar o Cisco Identity Services Engine(ISE) como uma autenticação externa para a administração da GUI do Cisco Catalyst SD-WAN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha o conhecimento destes tópicos:

- protocolo TACACS+
- Administração de dispositivos do Cisco ISE
- Administração do Cisco Catalyst SD-WAN
- Avaliação de política do Cisco ISE

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Antes de Começar

A partir do Cisco vManage versão 20.9.1, novas marcas são usadas na autenticação:

- Viptela-User-Group: para definições de grupo de usuários em vez de Viptela-Group-Name.
- Viptela-Resource-Group: para definições de grupos de recursos.

Configurar - Usando TACACS+

Configurar o Catalyst SD-WAN usando TACACS+

Procedimento

Etapa 1. (Opcional) Definir Funções Personalizadas.

Configure suas funções personalizadas que atendam a seus requisitos. Em vez disso, você pode usar as funções de usuário padrão. Isso pode ser feito na guia Catalyst SD-WAN: Administração > Usuários e Acesso > Funções.

Crie duas funções personalizadas:

1. Função do administrador: super-admin
2. Função somente leitura: somente leitura

Isso pode ser feito na guia Catalyst SD-WAN: Administração > Usuários e Acesso > Funções > Clique > Adicionar Função.

Add Custom Role



Custom Role Name

super-admin

Description (optional)

Range 1 - 32

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

Função do administrador (superadministrador)

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

Função somente leitura (somente leitura)

Etapa 2. Configurar a autenticação externa usando TACACS+ (CLI).

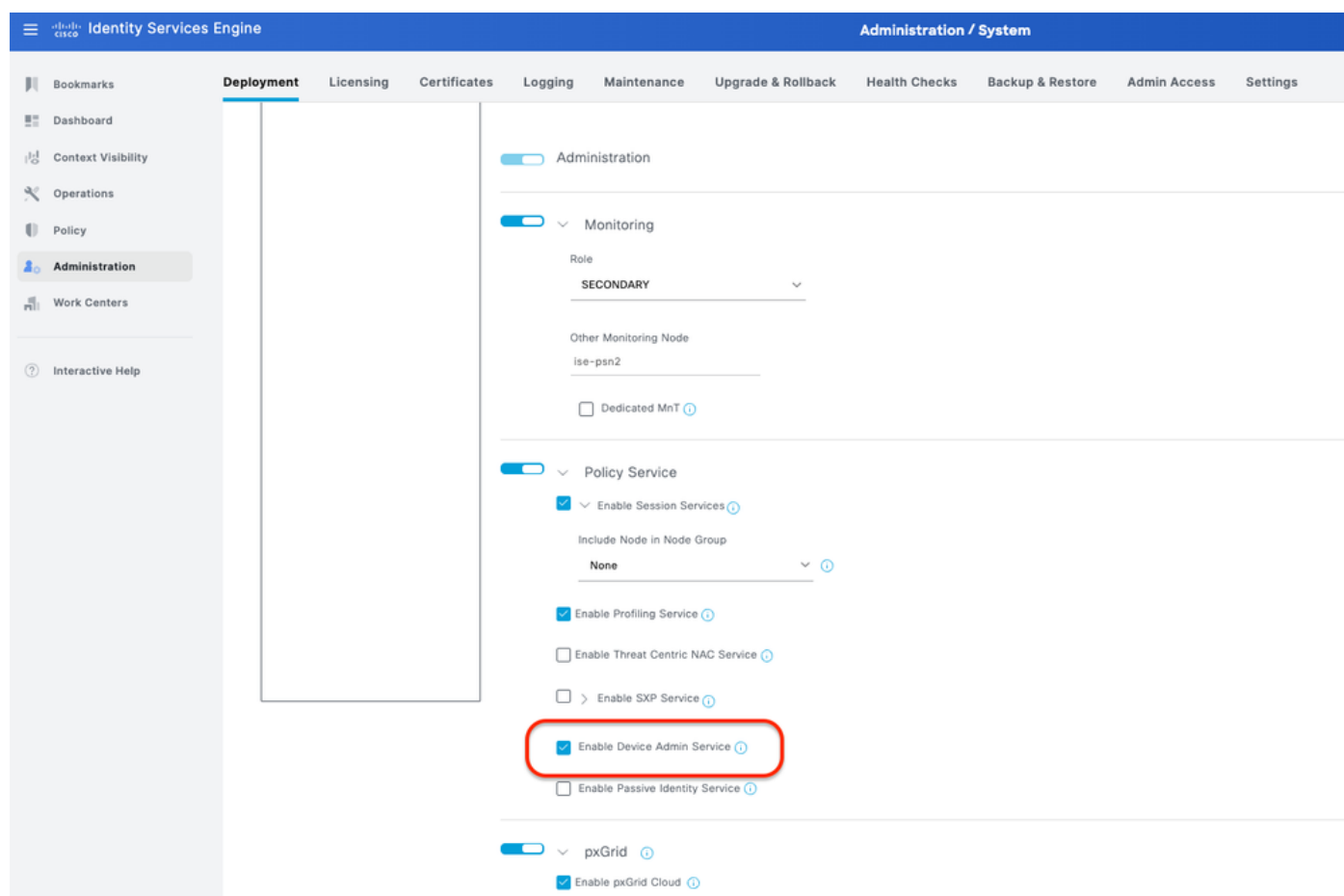
```
Entering configuration mode terminal
vmanage(config)#
vmanage(config)#
vmanage(config)# system
vmanage(config-system)# aaa
vmanage(config-aaa)# auth-order tacacs radius local
vmanage(config-aaa)# auth-fallback
vmanage(config-aaa)# commit and-quit
Commit complete.
```

vManager CLI - Configuração TACACS+

Configurar ISE para TACACS+

Etapa 1. Ativar o Device Admin Service.

Isso pode ser feito na guia Administration > System > Deployment > Edit (ISE PSN Node) > Check Enable Device Admin Service.



Habilitar Serviço de Administração de Dispositivo

Etapa 2. Adicionar o Catalyst SD-WAN como um dispositivo de rede no ISE.

Isso pode ser feito na guia Administration > Network Resources > Network Devices.

Procedimento

- Defina o nome (Catalyst SD-WAN) do dispositivo de rede e o IP.
- (Opcional) Classifique o tipo de dispositivo para a condição do conjunto de políticas.
- Ative TACACS+ Authentication Settings.
- Defina TACACS+ Shared Secret.

Dispositivo de rede ISE (Catalyst SD-WAN) para TACACS+

Etapa 3. Criar Perfil TACACS+ para cada função do Catalyst SD-WAN.

Criar perfis TACACS+:

- Catalyst_SDWAN_Admin: Para usuários Super Admin.
- Catalyst_SDWAN_ReadOnly: Para usuários somente leitura.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS > Adicionar.

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

Perfil 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

Add Trash Edit

Type	Name	Value
Mandatory	Viptela-User-Group	readonly

Cancel Save

Perfil TACACS+ - (Catalyst_SDWAN_ReadOnly)

Etapa 4. Criar Grupo de Usuários adicionar Usuários Locais como membro.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Grupos de identidade de usuário.

Crie dois grupos de identidade de usuário:

1. Super_Admin_Group
2. ReadOnly_Group

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
☐	Enabled	super_user		

Grupo de Identidade de Usuário - (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
☐	Enabled	readonly_user		

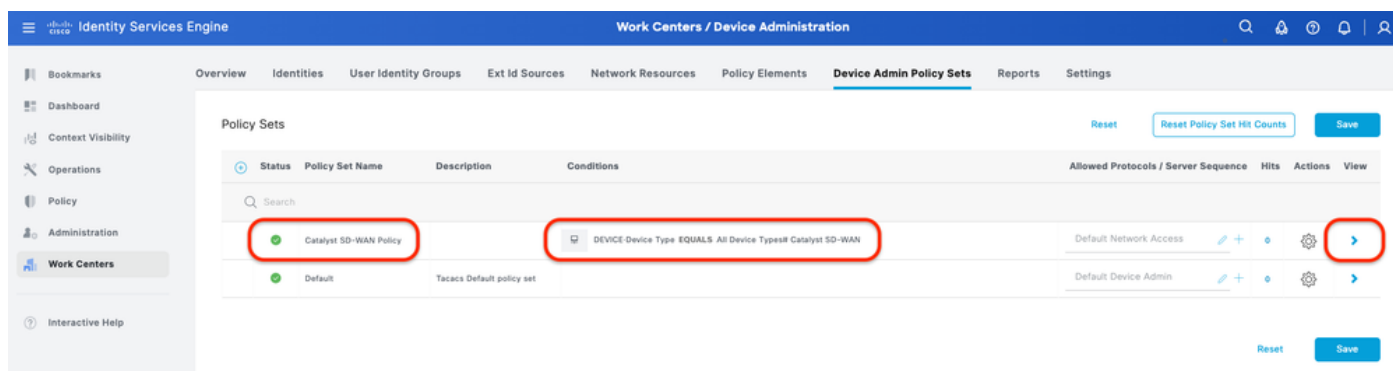
Grupo de Identidade de Usuário - (ReadOnly_Group)

Etapa 5. (Opcional) Adicione o conjunto de políticas TACACS+.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Conjuntos de diretivas de administração de dispositivo.

Procedimento

- Clique em Ações e escolha (Inserir nova linha acima).
- Defina o nome do Conjunto de políticas.
- Defina a condição de definição de política para Selecionar tipo de dispositivo criado anteriormente em (Etapa 2 > b).
- Defina os protocolos permitidos.
- Click Save.
- Clique em (>) Exibição do conjunto de políticas para configurar as regras de autenticação e autorização.



Conjunto de políticas do ISE

Etapa 6. Configurar a política de autenticação TACACS+.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Conjuntos de diretivas de administração de dispositivo > Clique em (>).

Procedimento

- Clique em Ações e escolha (Inserir nova linha acima).
- Defina o nome da política de autenticação.
- Defina Authentication Policy Condition e selecione Device Type criado anteriormente em (Etapa 2 > b).
- Defina a Política de autenticação Usar para a origem da Identidade.
- Click Save.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is active. The 'Catalyst SD-WAN Policy' is selected. The 'Authentication Policy(2)' section shows two rules: 'Catalyst SD-WAN Auth' and 'Default'. The 'Catalyst SD-WAN Auth' rule is highlighted with a red box. The 'Internal Users' group is selected for the 'Catalyst SD-WAN Auth' rule, and the 'Options' button is also highlighted with a red box.

Política de autenticação

Etapa 7. Configurar a política de autorização TACACS+.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Conjuntos de diretivas de administração de dispositivo > Clique em (>).

Esta etapa para criar a Política de Autorização para cada Função do Catalyst SD-WAN:

- Catalyst SD-WAN Authz (superadministrador): super-admin
- Catalyst SD-WAN Authz (somente leitura): somente leitura

Procedimento

- Clique em Ações e escolha (Inserir nova linha acima).
- Defina o nome da Diretiva de Autorização.
- Defina a Condição da diretiva de autorização e selecione o Grupo de usuários criado em (Etapa 4).
- Defina os perfis do Authorization PolicyShell e selecione TACACS Profile que você criou em (Etapa 3).
- Click Save.

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

Política de Autorização

Verificar a configuração TACACS+

1- Exibir sessões de usuário do Catalyst SD-WAS Catalyst SD-WAN: Administração > Usuários e Acesso > Sessões de Usuário.

Você pode exibir a lista de usuários externos que fizeram login através do RADIUS pela primeira vez. As informações exibidas incluem seus nomes de usuário e funções.

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 Username	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

Sessões de usuário do Catalyst SD-WAS

2- ISE - TACACS Live-Logs Operações > 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

Logs ao vivo

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; }

Registros ao vivo detalhados - (somente leitura)

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; }

Troubleshooting

No momento, não há informações de diagnóstico específicas disponíveis para esta configuração.

Referências

- [Guia do Administrador do Cisco Identity Services Engine, Versão 3.4](#)
- [Guia de configuração de sistemas e interfaces Cisco Catalyst SD-WAN, Cisco IOS XE Catalyst SD-WAN versão 17.x](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.