

# Configurar TACACS de Autenticação Externa do Catalyst Center com ISE

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Cisco Identity Services Engine \(ISE\)](#)

[Licenciar e ativar os serviços TACACS+](#)

[Criar usuário administrador e adicionar dispositivo de rede](#)

[Configurar perfil TACACS+](#)

[Configurar políticas TACACS+](#)

[Cisco Catalyst Center](#)

[Configurar o servidor ISE / AAA](#)

[Ative e configure a autenticação externa.](#)

[Verificar](#)

[Troubleshooting](#)

[1. Configuração Incorreta do Atributo](#)

[2. Incompatibilidade de Segredo Compartilhado](#)

---

## Introdução

Este documento descreve as etapas necessárias para integrar o Cisco Identity Services Engine com o Catalyst Center para ativar a autenticação TACACS+.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso de administrador ao Cisco ISE e ao Cisco Catalyst Center.
- Compreensão básica dos conceitos de AAA (Authentication, Authorization, and Accounting).
- Conhecimento prático do protocolo TACACS+.
- Conectividade de rede entre o Catalyst Center e o servidor ISE.

## Componentes Utilizados

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

- Cisco Catalyst Center versão 2.3.7.x
- Cisco Identity Services Engine (ISE) versão 3.x (ou posterior)
- Protocolo TACACS+ para autenticação de usuário externo

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.

## Informações de Apoio

Essa integração permite que usuários externos façam login no Catalyst Center para acesso e gerenciamento administrativos.

## Configurar

### Cisco Identity Services Engine (ISE)

Licenciar e ativar os serviços TACACS+

Antes de começar com a configuração TACACS+ no ISE, você deve confirmar se a licença correta está instalada e se o recurso está habilitado.

1. Verifique se você tem a licença PID L-ISE-TACACS-ND= no portal [Cisco Smart Software Manager](#) ou [Cisco License Central](#).

Habilite a Administração de dispositivo no portal de licenciamento do ISE.

- A licença Device Admin (PID: L-ISE-TACACS-ND=) permite serviços TACACS+ em um Policy Service Node (PSN).

- Navegue até:

Administração > Sistema > Licenciamento

- Marque a caixa Device Admin nas opções de camada.

Tier  Essential  Advantage  Premier  Device Admin

Virtual Appliance  ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

[Reset](#)

[Update](#)

#### Administrador do dispositivo

<input type="checkbox"/>	Premier	Enabled	Released Entitlement	<a href="#">0</a>	-	Dec 27,2024 18:16:00 PM
<input type="checkbox"/>	Device Admin	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM
∨ Virtual Appliance						
	ISE VM License	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM

#### Administrador do dispositivo de licença

### 3. Ative o Device Admin Service no nó ISE que executa o serviço TACACS+.

- Navegue até:

Administração > Sistema > Implantação > Selecionar o nó

- Marque a opção Enable Device Admin Service.

Deployment Nodes List > ise-mxc1

### Edit Node

**General Settings**    Profiling Configuration

Hostname	ise-mxc1
FQDN	ise-mxc1.cisco.com
IP Address	10.88.244.180
Node Type	Identity Services Engine (ISE)

Role: STANDALONE [Make Primary](#)

Administration

> Monitoring

Policy Service

- Enable Session Services ⓘ  
Include Node in Node Group: None ⓘ
- Enable Profiling Service ⓘ
- Enable Threat Centric NAC Service ⓘ
- > Enable SXP Service ⓘ
- Enable Device Admin Service ⓘ
- Enable Passive Identity Service ⓘ

> pxGrid ⓘ

Habilitar Serviço de Administração de Dispositivo

Criar usuário administrador e adicionar dispositivo de rede

### 1. Crie o Usuário Admin.

- Essa conta de usuário é usada para fazer login na IU do Catalyst Center através da autenticação do ISE.
- Navegue até:  
Centros de Trabalho > Acesso à Rede > Identidades > Usuário de Acesso à Rede
- Adicione um novo usuário (por exemplo, catc-user).
- Se o usuário já existir, vá para a próxima etapa.

### 2. Crie o Dispositivo de Rede.

- Navegue até:  
Centros de trabalho > Acesso à rede > Identidades > Recurso de rede

- Adicione o endereço IP do Catalyst Center ou defina a sub-rede onde o IP do Catalyst Center está localizado.
- Se o dispositivo já existir, verifique se ele contém os parâmetros:
  - As configurações de autenticação TACACS estão habilitadas.
  - O segredo compartilhado está configurado e é conhecido (salve esse valor, conforme exigido posteriormente no Catalyst Center).

The screenshot shows the Cisco ISE interface for configuring a network device. The 'Network Resources' tab is active, and the device 'Catalyst-Center\_6' is selected. The configuration page includes fields for Name, Description, IP Address (10.88.244.160 / 32), Device Profile (Cisco), Model Name, Software Version, Network Device Group, Location (All Locations), IPSEC (No), Device Type (All Device Types), and DNAC (DNAC Devices). The 'TACACS Authentication Settings' section is expanded and highlighted with a red box, showing the 'Shared Secret' field, a 'Retire' button, and options for 'Enable Single Connect Mode' (Legacy Cisco Device selected).

Configurações de autenticação TACACS

## Configurar perfil TACACS+

### 1. Crie um novo perfil TACACS+.

- Navegue até:

Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS

- Adicione um nome de perfil.
- Adicione um atributo personalizado da seguinte maneira:

- Digite: Obrigatório
- Nome: Cisco-av-pair
- Valor: Role=FUNÇÃO-SUPERADMIN

- Salve o perfil.

**Cisco ISE** Work Centers - Device Administration

---

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 > CatC\_TACACS\_Profile

**TACACS Profile**

Name  
CatC\_TACACS\_Profile

Description  
Catalyst Center External Authentication

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 ⚙️

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	Role=SUPER-ADMIN-ROLE	✎ 🗑️

[Cancel](#)   [Save](#)

Perfil TACACS+



Note: O Cisco Catalyst Center suporta servidores externos de Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization and Accounting) para controle de acesso. Se estiver usando um servidor externo para autenticação e autorização de usuários externos, você poderá ativar a autenticação externa no Cisco Catalyst Center. A configuração de atributo AAA padrão corresponde ao atributo de perfil de usuário padrão.

O valor do atributo AAA padrão do protocolo TACACS é `cisco-av-pair`.

O valor do atributo AAA padrão do protocolo RADIUS é `Cisco-AVPair`.

A alteração só é necessária se o servidor AAA tiver um atributo personalizado no perfil do usuário. No servidor AAA, o formato do valor do atributo AAA é `Role=role1`. No servidor Cisco Identity Services Engine (Cisco ISE), ao configurar o perfil RADIUS ou TACACS, o usuário pode selecionar ou inserir `cisco av-pair` como atributo AAA.

Por exemplo, você pode selecionar e configurar manualmente o atributo AAA como `cisco-av-pair=Role=SUPER-ADMIN-ROLE` ou `Cisco-AVPair=Role=SUPER-ADMIN-ROLE`.

---

## 2. Crie um Conjunto de Comandos TACACS+.

- Navegue até:

Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Conjuntos de comandos TACACS

- Adicione um nome.
- Marque a opção Permitir qualquer comando que não esteja listado abaixo.
- Salve o conjunto de comandos.

The screenshot shows the Cisco ISE web interface for configuring a TACACS Command Set. The breadcrumb trail is: TACACS Command Sets > PermitAllCommands > Command Set. The page title is "Command Set". The "Name" field is filled with "PermitAllCommands". The "Description" field is empty. Under the "Commands" section, the checkbox "Permit any command that is not listed below" is checked. Below this, there are buttons for "Add", "Trash", "Edit", "Move Up", and "Move Down". A table with columns "Grant", "Command", and "Arguments" is shown, but it is empty with the message "No data found." at the bottom. "Cancel" and "Save" buttons are located at the bottom right of the form.

Conjuntos de comandos TACACS

## Configurar políticas TACACS+

### 1. Crie um Novo Conjunto de Políticas TACACS+.

- Navegue até:

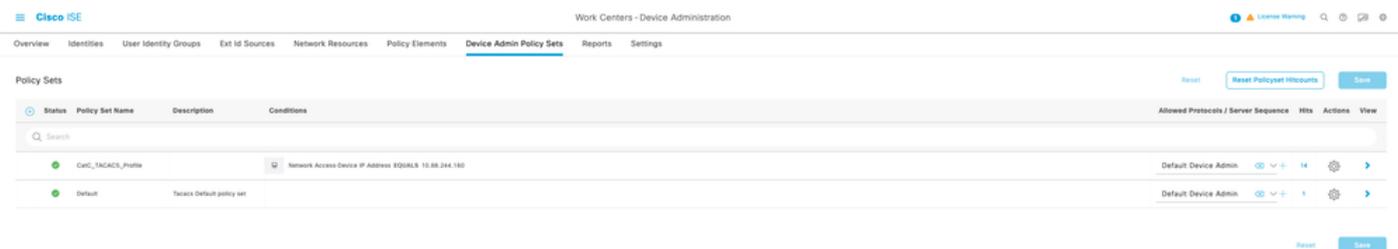
Centros de Trabalho > Administração de Dispositivos > Conjunto de Políticas de Administração de Dispositivos

- Adicione um nome para o conjunto de políticas.
- Configure a condição.
  - Neste exemplo, a condição corresponde ao endereço IP do Catalyst Center.



Endereço IP do Catalyst Center

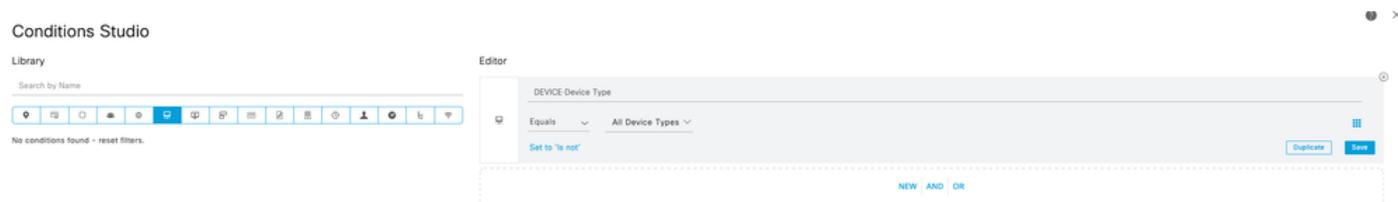
### 1.3 Em Allowed Protocols / Server Sequence, selecione Default Device Admin.



Selecionar administrador de dispositivo padrão

## 2. Configure o Conjunto de Políticas.

- Clique na seta ( > ) à direita para expandir e configurar o conjunto de políticas.
- Adicione uma nova Regra em Política de Autorização.
- Configure a nova regra da seguinte maneira:
  - Nome: Insira um nome de regra descritivo.
  - Condição: Para este exemplo, a condição correspondeu a Todos os tipos de dispositivo.



Todos os tipos de dispositivo

- Conjunto de comandos: Selecione o conjunto de comandos TACACS+ criado anteriormente.
- Perfil do Shell: Selecione o Perfil TACACS+ criado anteriormente.

The screenshot displays the Cisco ISE Device Administration interface. At the top, the navigation menu includes Overview, Identities, User Identity Groups, Ext ID Sources, Network Resources, Policy Elements, Device Admin Policy Sets (selected), Reports, and Settings. The main content area is titled 'Policy Sets - CatC\_TACACS\_Profile'. It features a table with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A search bar is present above the table. Below the main table, there are sections for 'Authorization Policy (1)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (2)'. The 'Authorization Policy (2)' section contains a detailed table with columns for Status, Rule Name, Conditions, Results (Command Sets, Shell Profiles, Hits), and Actions. Two rules are listed: 'Authorization Rule 1' and 'Default'.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Active	CatC_TACACS_Profile		Network Access Device IP Address EQ0AL5 10.88.244.150	Default Device Admin	14

Status	Rule Name	Conditions	Results			Actions
			Command Sets	Shell Profiles	Hits	
Active	Authorization Rule 1	DEVICE Device Type EQ0AL5 All Device Types	PermitAllCommands	CatC_TACACS_Profile	14	Settings
Active	Default		DenyAllCommands	Deny All Shell Profile	6	Settings

Conjunto de comandos TACACS+

## Cisco Catalyst Center

Configurar o servidor ISE / AAA

1. Faça login na interface da Web do Catalyst Center.

- Navegue até:

Menu principal > Sistema > Configurações > Serviços externos > Servidores de autenticação e política

2. Adicione um novo servidor. Você pode selecionar ISE ou AAA.

- Para esta demonstração, a opção AAA server é usada.



Note: Um cluster do Catalyst Center pode ter apenas um cluster do ISE configurado.

---

### 3. Configure estas opções e salve:

- Insira o endereço IP do servidor AAA.
- Adicione o segredo compartilhado (o mesmo segredo configurado no recurso de rede do Cisco ISE).
- Alterne Advanced Settings para On.
- Marque a opção TACACS.

# Add AAA server



Server IP Address\*

10.88.244.180

Shared Secret\*

.....

[SHOW](#)



Advanced Settings

Protocol

RADIUS  TACACS

Enable KeyWrap

Authentication Port\*

1812

Accounting Port\*

1813

Port

49

Retries\*

3

Timeout (seconds)\*

4

## Servidores de autenticação e política

IP Address	Protocol	Type	Status	Actions
192.168.31.228	RADIUS	ISE	INACTIVE	--
10.88.244.180	RADIUS_TACACS	AAA	ACTIVE	--

## Configurações avançadas

Ative e configure a autenticação externa.

1. Navegue até a página Autenticação Externa:

Menu principal > Sistema > Usuário e função > Autenticação externa

2. Adicione o atributo AAA cisco-av-pair e clique em Update para salvar as alterações.



Note: Esta etapa não é obrigatória, pois o atributo padrão para TACACS+ já é cisco-avpair, mas é considerado uma prática recomendada para configurá-lo explicitamente.

---

3. Em Primary AAA Server, selecione o servidor AAA configurado anteriormente.

- Clique em Exibir configurações avançadas para exibir opções adicionais.
- Selecione a opção TACACS+.
- Insira o segredo compartilhado configurado no recurso de rede do Cisco ISE.
- Clique em Atualizar para salvar as alterações.

4. Ative a caixa de seleção Usuário externo.

- Esta ação salva automaticamente a configuração.

The screenshot displays the 'External Authentication' configuration page in Cisco Catalyst Center. The page is titled 'External Authentication' and includes a navigation sidebar on the left with options like 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area contains the following sections:

- Enable External User:** A checkbox labeled 'Enable External User' is checked.
- AAA Attribute:** A dropdown menu is set to 'cisco-av-pair'. Below it are 'Reset to Default' and 'Update' buttons.
- AAA Server(s):** This section is divided into 'Primary AAA Server' and 'Secondary AAA Server'. Both are set to the IP address '10.88.244.180'. Each server has a 'Shared Secret' field with a 'Show' button. The 'Primary AAA Server' has radio buttons for 'RADIUS' (unchecked) and 'TACACS' (checked), with a 'View Advanced Settings' button. Below these are fields for 'Port' (49), 'Retries' (3), and 'Timeout (seconds)' (4), with an 'Update' button.

In the bottom right corner, a green 'Success' notification box states: 'Successfully saved external authentication settings.'

Autenticação externa

## Verificar

1. Abra uma nova sessão do navegador ou use o Modo incógnito e faça login na página da Web do Catalyst Center com a conta de usuário configurada no Cisco ISE.
2. No Catalyst Center, confirme se o login foi bem-sucedido.



Login Configurar o TACACS de Autenticação Externa do Catalyst Center com ISE

3. No Cisco ISE, valide os registros:

Operações > TACACS > Live Logs

- Status de autenticação: Aprovado
- Status da autorização: Aprovado

## Live Logs

Refresh Never Show Latest 20 records Within Last 3 hours Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	ISE Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.851...			isa01-user	Authentication	CatC_TACACS_Profile >> Authn...	CatC_TACACS_Profile >> Authori...	ise-mac1	Catalyst-Centr...	10.88.244.160	Device Type680 D...	LocationM1 Locat...	console		10.189.17.203	Matched Command	CatC_TACACS_P...
Sep 12, 2025 12:12:20.798...			isa01-user	Authentication	CatC_TACACS_Profile >> Default		ise-mac1	Catalyst-Centr...	10.88.244.160	Device Type680 D...	LocationM1 Locat...	console		10.189.17.203		

Last Updated: Thu Sep 11 2025 18:14:58 GMT-0600 (Central Standard Time) Records Shown: 2

Logs ao vivo

#### 4. Em Detalhes da autorização, compare com a próxima saída :

- Texto da mensagem: Administração do dispositivo: Autorização de sessão bem-sucedida
- Todos os atributos de resposta: cisco-av-pair=Role=SUPER-ADMIN-ROLE

### Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No, DNAC#DNAC Devices, Location#All Locations, Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

### Authorization Attributes

All Request Attributes	
All Response Attributes	cisco-av-pair=Role=SUPER-ADMIN-ROLE

cisco-av-pair=Função=SUPER-ADMIN-ROLE

## Troubleshooting

Aqui estão alguns problemas comuns que você pode encontrar durante a integração e como identificá-los:

## 1. Configuração Incorreta do Atributo

Sintoma no Catalyst Center: credenciais de login inválidas



# Cisco Catalyst Center

The bridge to possible

 Invalid Login Credentials

Username

catc-user

Password

.....

[SHOW](#)

Log In

Erro de configuração de atributo

- Sintoma no Cisco ISE (registros TACACS):

- Autenticação: Aprovado
- Autorização: Aprovado

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:25.861...	<span style="color: green;">■</span>		catc-user	Authorization	CatC_TACACS_Profile	CatC_TACACS_Profile >> Authoriz...	ise-mst1	Catalyst-Center_8	10.88.244.180	Device Type:AAA D...	Location:AAA Locat...	console		10.188.17.203		CatC_TACACS_Pt...
Sep 12, 2025 12:12:26.788...	<span style="color: green;">■</span>		catc-user	Authentication	CatC_TACACS_Profile	>> Default	ise-mst1	Catalyst-Center_8	10.88.244.180	Device Type:AAA D...	Location:AAA Locat...	console		10.188.17.203		

Erro de configuração de atributo

- Possíveis causas:
  - Existe um espaço no valor do atributo.

Exemplo:

### Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No, DNAC#DNAC Devices, Location#All Locations, Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

### Authorization Attributes

All Request Attributes

All Response Attributes      cisco-av-pair=Role=SUPER-ADMIN-ROLE

Erro de configuração de atributo

- O atributo está configurado incorretamente, a palavra-chave Role= está ausente.

Exemplo:

### Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No, DNAC#DNAC Devices, Location#All Locations, Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

### Authorization Attributes

All Request Attributes

All Response Attributes      cisco-av-pair=Role=SUPER-ADMIN-ROLE

Erro de configuração de atributo

## 2. Incompatibilidade de Segredo Compartilhado

- Sintoma: Os pacotes de autenticação falham entre o Catalyst Center e o Cisco ISE.

- Possível causa: O segredo compartilhado configurado no recurso de rede do ISE não corresponde ao configurado na página Catalyst Center > Autenticação externa.

Como verificar:

- Verifique a configuração de recurso de rede no ISE.
- Compare o Shared Secret com a configuração em Catalyst Center > External Authentication.

Exemplo:

### Authentication Details

Generated Time 2025-09-11 18:22:24.078000 +00:00

Logged Time 2025-09-11 18:22:24.078

Epoch Time (sec) 1757614944

ISE Node ise-mxc1

Message Text **Failed-Attempt: Authentication failed**

Failure Reason **13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets**

Resolution

Root Cause

Username

Network Device Name Catalyst-Center\_6

Network Device IP 10.88.244.160

Network Device Groups IPSEC#Is IPSEC Device#No, DNAC#DNAC Devices, Location#All Locations, Device Type#All Device Types

Device Type Device Type#All Device Types

Location Location#All Locations

Device Port

Remote Address

Incompatibilidade de Segredo Compartilhado

## 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.