# Configurar o ISE como uma autenticação externa para a GUI do DNAC

# Contents

Introdução							
<u>Pré-requisitos</u>							
Requisitos							
Componentes Utilizados							
Antes de Começar							
Configurar							
(Opção1) Configurar a autenticação externa do DNAC usando RADIUS							
(Opção 1) Configurar ISE para RADIUS							
(Opção 2) Configurar a autenticação externa de DNAC usando TACACS+							
(Opção 2) Configurar o ISE para TACACS+							
Verificar							
Verificar a configuração do RADIUS							
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 DNA Center.

# Pré-requisitos

## Requisitos

A Cisco recomenda que você tenha o conhecimento destes tópicos:

- protocolos TACACS+ e RADIUS.
- Integração do Cisco ISE com o Cisco DNA Center.
- 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 Patch1.
- Cisco DNA Center versão 2.3.5.5.

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

- Verifique se você tem pelo menos um servidor de autenticação RADIUS configurado em System > Settings > External Services > Authentication and Policy Servers.
- Somente um usuário com permissões SUPER-ADMIN-ROLE no DNAC pode executar este procedimento.
- Habilitar fallback de autenticação externa.

Caution: Em versões anteriores à 2.1.x, quando a autenticação externa é habilitada, o Cisco DNA Center retorna aos usuários locais se o servidor AAA estiver inacessível ou se o servidor AAA rejeitar um nome de usuário desconhecido. Na versão atual, o Cisco DNA Center não retornará aos usuários locais se o servidor AAA estiver inacessível ou se o servidor AAA rejeitar um nome de usuário desconhecido. Quando o fallback de autenticação externa está habilitado, os usuários externos e os administradores locais podem fazer logon no Cisco DNA Center.

Para habilitar o fallback de autenticação externa, use SSH para acessar a instância do Cisco DNA Center e insira este comando CLI (magctl rbac external\_auth\_fallback enable).

# Configurar

(Opção1) Configurar a autenticação externa do DNAC usando RADIUS

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 System > Users & Roles > Role Based Access Control.

Procedimento

a. Crie uma nova função.

Create a User Role

2

#### Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

Role Name* DevOps-Role	)
Describe the role (optional)	_

Exit

Nome da Função DevOps

### b. Defina o Acesso.

⊟ Cisc	o DNA Center				Create a User Role	Q @ @ 4
	Define the These permissions Define the DevOy a role is configure	e Acce issions enabl allow. Click ps-Role role ed with Den 1	e different c here to Lear e. Custom r y permissio	apabilities in Cie n More. roles permit or on, all related c	co DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If ontent for that capability is removed from the GUI.	
	Access -	Permission			Description	
	> Assurance	O Deny	O Read	O Write	Assure consistent service levels with complete visibility across all aspects of your network.	
	> Network Analytics	O Deny	O Read	O Write	Access to Network Analytics related components.	
	> Network Design	O Deny	O Read	O Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.	
	> Network Provision	O Deny	⊖ Read	O Write	Configure, upgrade, provision and manage your network devices.	
	> Network Services	O Deny	O Read	O Write	Configure additional capabilities on the network beyond basic network connectivity and access.	
	> Platform	O Deny	<ul> <li>Read</li> </ul>	O Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.	
	> Security	O Deny	O Read	O Write	Manage and control secure access to the network.	
			_			2
Exit					Review Back	Next

Acesso à Função DevOps

#### c. Crie a Nova Função.

	Create a User Role		Q @ @ 4
Summary Review the DevOps-Role role. Make sur	all the details are as you expect them to be. If you need to change something, clicking ed	it will take you back to that section	
<ul> <li>Role Name &amp; Description Edit</li> </ul>			
Role Name DevOps-Role			
Role Description			
<ul> <li>Role Capability Edit</li> </ul>			
ASSURANCE			
Monitoring and Troubleshooting	Deny		
Monitoring Settings	Deny		
Troubleshooting Tools	Deny		
NETWORK ANALYTICS			
Data Access	Read		
NETWORK DESIGN			
Advanced Network Settings	Deny		
Image Repository	Deny		
Network Hierarchy	Deny		
Network Profiles	Deny		
Network Settings	Deny		
Virtual Network	Denv		
Exit		Back	Create Role

Resumo da função DevOps

■ Cisco DNA Center		Create a User Role	Q @ C A
Network Device	Deny		
Port Management	Deny		
Topology	Deny		
License	Deny		
Network Telemetry	Deny		
PnP	Deny		
Provision	Deny		
NETWORK SERVICES			
App Hosting	Deny		
Bonjour	Deny		
Stealthwatch	Deny		
Umbrella	Deny		
PLATFORM			
APIs	Write		
Bundles	Write		
Events	Write		
Reports	Write		
SECURITY			
Group-Based Policy	Deny		
IP Based Access Control	Deny		
Security Advisories	Deny		1
SYSTEM			
Machine Reasoning	Deny		1
Suntam Management	Doou		
<) Exit		Back	Create Role

Revisar e Criar Função DevOps

Etapa 2. Configurar a autenticação externa usando o RADIUS. Isso pode ser feito na guia System > Users & Roles > External Authentication.

#### Procedimento

a. Para habilitar a autenticação externa no Cisco DNA Center, marque a caixa de seleção Habilitar usuário externo.

b. Defina os atributos AAA.

Insira Cisco-AVPair no campo AAA attributes.

c. (Opcional) Configure o servidor AAA primário e secundário.

Certifique-se de que o protocolo RADIUS esteja habilitado no Primary AAA Server pelo menos, ou nos servidores Primary e Secondary.

E Cisco DNA Center	System / Users & Roles	Q @ & 4
User Management Role Based Access Control External Authentication	External Authentication Gisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute h name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Rele=role1". On ISE server, choose the cisco-av-pair attribute from cisco specific A	tere on Cisco DNA Center is the d here on Cisco DNA Center. AAA attributes list. A sample
a b	configuration inside Authorization profile would look like "cisco-av-pairs Role=SUPER-ADMIN-ROLE". An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPairsRole=SUPER-ADMIN-ROLE". Enable External User AAA Attribute AAA Attribute Cisco-AVPair	
c	Reset to Default     Update <ul> <li>AAA Server(s)</li> <li>Primary AAA Server</li> <li>Secondary AAA Server</li> <li>P Address</li> <li>ISE Server 1 IP</li> <li>ISE Server 2 IP</li> <li>Shared Secret</li> <li>Shared Secret</li> <li>Shared Secret</li> <li>Shared Secret</li> <li>Shared Secret</li> <li>Shared Secret</li> <li>Titte</li> <li>Info</li> <li>Info</li></ul>	

(RADIUS) Etapas de configuração da autenticação externa

# (Opção 1) Configurar ISE para RADIUS

Etapa 1. Adicionar o servidor DNAC como um dispositivo de rede no ISE.

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

- a. Defina o IP e o nome do dispositivo de rede (DNAC).
- b. (Opcional) Classifique o tipo de dispositivo para a condição do conjunto de políticas.
- c. Ative as configurações de autenticação RADIUS.
- d. Definir segredo compartilhado RADIUS.

=	dealer Identity Services I	Ingine				Administ	ration / Network Resources			۹	۵ ۵	0 Q   A
н	Bookmarks	Network Devices	Network De	vice Groups N	etwork Device Profiles	External RADIUS Servers	RADIUS Server Sequences	External MDM	pxGrid Direct Connectors			
111  11   11   11   11   11   11   11	Dashbeard Context Visibility Operations Policy Administration Work Centers Interactive Help	Network Device Default Device Device Security Setting	а	Network Device Cit Network Device Name Description IP Address Device Profile Model Name Software Version		ər IP 	<u>' 32</u> Ø					
			b c	Network Device Location IPSEC Device Type RADIUS Protocol Shared S Code Port	Group All Locations No DNAC-Servers US Authentication Settin UOP Settings RADRUS d ecret second Shared Secret Second Shared Secret 3200	Set To D     Set To D	sfault sfault sfault Show					

Dispositivo de rede (DNAC) ISE para RADIUS

Etapa 2. Criar perfis de autorização RADIUS.

Isso pode ser feito na guia Política > Elementos de Política > Resultados > Autorização > Perfis de autorização.

Note: Crie 3 perfis de autorização RADIUS, um para cada função de usuário.

#### Procedimento

a. Clique em Add e defina o nome do Perfil de Autorização RADIUS.

b. Insira Cisco:cisco-av-pair nas Advanced Attributes Settings e preencha a função de usuário correta.

- Para a função de usuário (DecOps-Role), digite ROLE=DevOps-Role.
- Para a função de usuário (NETWORK-ADMIN-ROLE), digite ROLE=NETWORK-ADMIN-ROLE.
- Para a função de usuário (SUPER-ADMIN-ROLE), digite ROLE=SUPER-ADMIN-ROLE.
- c. Revise os Detalhes do Atributo.
- d. Click Save.

$\equiv \frac{\mathrm{ded}}{\mathrm{osce}}$ Identity Services	s Engine	Policy / Policy Elements	
JI Bookmarks	Dictionaries Conditions	(esults	
E Dashboard	Authentication $\vee$	Autorization Profiles 3 New Autorization Profile	
16 Context Visibility	Allowed Protocols	Authorization Profile a	
% Operations	Authorization 🖂	* Name DevDex Berlin	
Policy	Authorization Profiles Downloadable ACLs	Description	
Administration	Profiling		
H Work Centers	Posture >	* Access Type ACCESS_ACCEPT V	
	Client Previsioning	Network Device Profile # Cisco V 0	
③ Interactive Help		Service Template	
		Track Movement	
		Agentiess Posture	
		Passive identity Tracking 🗌 💍	
		> Common Tasks	
		Advanced Attributes Settings b	
		E     Ciscoxisco-av-pair      *     ROLE+DevOps-Role      +	
		C	
		Attributes Details     More #CESS#ACCOP     disce exper = KOLF-Dodge-Main	
			d
			Submit Cancel

Criar perfil de autorização

Etapa 3. Criar Grupo de Usuários.

Isso pode ser feito na guia Administration > Identity Management > Groups > User Identity Groups.

- a. Clique em Add e defina o nome do grupo de identidade
- b. (Opcional) Defina a Descrição.
- c. Clique em Submit.



Criar Grupo de Identidades de Usuário

Etapa 4. Criar Usuário Local.

Isso pode ser feito na guia Administração > Gerenciamento de identidades > Identidades > Usuários.

- a. Clique em Add e defina o nome de usuário.
- b. Defina a Senha de login.
- c. Adicione o usuário ao grupo de usuários relacionado.
- d. Clique em Submit.

=	deale Identity Services E	Ingine				Admi	nistration / Identity	Manager	nent		, Q	<b>\$</b> 0	Q   2	٩
рі E	Bookmarks Dashboard	Identities Users	Groups E	xternal Id	lentity Sources Id	dentity Source Sequences	Settings							
18 X	Context Visibility Operations	Latest Manual I Results	Network Scan		Vetwork Access Users List >	> New Network Access User								
0	Policy Administration			a	* Username Status	DevOps_User								
ก็	Work Centers				Account Name Alias		0							
٢	Interactive Help				Password Type: Inte Password Type: Inte Password Lifetime: With Expiration () Password will expire Never Expires ()	ernal Users 👻								
				b	Pa * Login Password Enable Password V User Information First Name Last Name	essword	Re-Enter Password	)	Generate Password	0				

Criar usuário local 1-2

= -deade-	Identity Services E	Engine			Admini	istration / Identity Manageme	ent			, Q	۵	0	٥	A
III     Bookm       Bill     Dashb       Idi     Context       V     Operating       III     Policy       III     Policy       IIII     Work C       Interact	aarks ooard xt Viaibility tions istration Centers ctive Help	Users Latest Mara Results	Groups aal Network Scan	External Identity Sources	Identity Source Sequences	Settings ne-Cites reasonau	Generate Password	<ul> <li>○</li> <li>○</li> </ul>						
				<ul> <li>✓ Account Disal</li> <li>Disable account</li> <li>✓ User Groups</li> <li>※ DevOps</li> </ul>	ble Policy unt if date exceeds 2025-03-20 C	(yyyy-mm-dd)			(	d		Canc	cel	

Criar usuário local 2-2

Etapa 5. (Opcional) Adicione o conjunto de políticas RADIUS.

Isso pode ser feito na guia Política > Conjuntos de políticas.

#### Procedimento

a. Clique em Ações e escolha (Inserir nova linha acima).

b. Defina o nome do Conjunto de políticas.

c. Defina a condição de definição de política para Selecionar tipo de dispositivo criado anteriormente em (Etapa1 > b).

d. Defina os protocolos permitidos.

e. Click Save.

f. Clique em (>) Policy Set View para configurar as regras de autenticação e autorização.

Adicionar Conjunto de Políticas RADIUS

Etapa 6. Configurar a política de autenticação RADIUS.

Isso pode ser feito na guia Política > Conjuntos de políticas > Clique em (>).

Procedimento

- a. Clique em Ações e escolha (Inserir nova linha acima).
- b. Defina o nome da Diretiva de Autenticação.

c. Defina Authentication Policy Condition e Select Device Type criado anteriormente em (Etapa1 > b).

- d. Defina a Política de autenticação Usar para a origem da Identidade.
- e. Click Save.

≡	dentity Services Eng	ine Policy / Policy Sets		۵ ۵	0	Q   8	٩
Щ	Bookmarks	Policy Sets-+ DNAC - Policy	Reset	Reset Policy Set Hit Counts		Save	
	Dashboard	Status Policy Set Name Description Conditions		Allowed Protocols / Serve	r Seque	nce Hits	
명	Context Visibility	Q Search					
×	Operations	DIALC - Pullov     DIALC - Pullov     DIALC - Pullov     DIALC - Pullov		Default Network Access		+ 0	
્ણ	Policy						
20	Administration	VAuthentication Policy(2)					
ri.	Work Centers	Status Rule Name Conditions	Use		Hits	Actions	
(?)	Interactive Help	Q, Search		d			
		DINAC - Authentication C DINAC - Authentication DEVICE Device Type EQUALS All Device TypesROMAC-Servers	> Opt	l Users	0	ø	
		Defauit	AI_Us	ons	2	ø	
		>Authorization Policy - Local Exceptions					
		>Authorization Policy - Global Exceptions					
		>Authorization Policy(1)					
				Reset	(	e Save	)

Adicionar Política de Autenticação RADIUS

Etapa 7. Configurar a Política de Autorização RADIUS.

Isso pode ser feito na guia Política > Conjuntos de políticas> Clique em (>).

Esta etapa para criar a Política de Autorização para cada Função de Usuário:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- DevOps-Função

#### Procedimento

- a. Clique em Ações e escolha (Inserir nova linha acima).
- b. Defina o nome da Política de Autorização.

c. Defina a Condição de Política de Autorização e Selecione o Grupo de Usuários criado em (Etapa 3).

d. Defina os Resultados/Perfis da Política de Autorização e Selecionar Perfil de Autorização que você criou em (Etapa 2).

e. Click Save.

≡ deade Identity Services I	Engine	Policy / Policy Sets		
Bookmarks	Policy Sets -> DNAC - Policy		Reset	Reset Policy Set Hit Counts Save
E Dashboard	Status Policy Set Name	Description Conditions		Allowed Protocols / Server Sequence Hits
No context visibility	Q Search			
Operations	ONAC - Policy	DEVICE-Device Type EQUALS All Device TypesHDNAC-See	rvers	Default Network Access 🥜 🕂 o
2. Administration	> Authentication Policy(2)			
HI Work Centers	> Authorization Policy - Local Exception			
	> Authorization Policy - Global Exception	a		
Interactive Help	~Authorization Policy(4)			
			Results	
	🕂 Status Rule Name	Conditions	Profiles Security	Groups Hits Actions
	Q Search <b>b</b>	С	d	a
	Super Admin	R IdentityGroup Name EQUALS User Identity Groups:SUPER-ADMIN	(Super-Admin_Role_Pr ×) v+ Select	from list: 🖉 + 🔹 🚳
	Network Admin	R. IdentityGroup Name EQUALS User Identity Groups:NETWORK-ADMIN	(Network-Admin_Role ×) v + Select	from list 🥒 + 🔹 🚳
	O DevOps	R IdentityGroup Name EQUALS User Identity Groups:DevOps	DevOps-Profile 0 + Select	from list 🥒 + 🔹 🚳
	O Default		DenyAccess 🖉 + Select	from list 🥒 + 🔹 🚱
				Ő
				Reset Save

(Opção 2) Configurar a autenticação externa de DNAC usando TACACS+

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 System > Users & Roles > Role Based Access Control.

Procedimento

a. Crie uma nova função.

Adicionar Política de Autorização

Create a User Role

#### Create a New Role

Define the name of the role, and then provide an optional description. To make it easier to assign roles down the road, describe the role as clearly as possible.

Role Name*				
SecOps-Role	]			
Describe the role (optional	i()			
	A			
				0
				2
				Next

Nome da Função SecOps

.

#### b. Defina o Acesso.

≡ Cisco	DNA Center				Create a User Role	Q @ 🛆 🗘
	Define the	Acce	SS			
	These permiss     permissions al	sions enable Illow. Click h	e different c ere to Lear	apabilities in C n More.	sco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these 🛛 🗙	
	Define the SecOps a role is configured	<b>-Role</b> role d with Deny 1	. Custom r / permissio	roles permit o on, all related	r restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If content for that capability is removed from the GUI.	
	> Network Analytics	O Deny	O Read	O Write	Access to Network Analytics related components.	
	> Network Design	O Deny	○ Read	O Write	Set up network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.	
	> Network Provision	O Deny	○ Read	Write	Configure, upgrade, provision and manage your network devices.	
	> Network Services	O Deny	⊖ Read	O Write	Configure additional capabilities on the network beyond basic network connectivity and access,	
	> Platform	O Deny	() Read	<ul> <li>Write</li> </ul>	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.	
	> Security	O Deny	○ Read	O Write	Manage and control secure access to the network.	
	> System	O Deny	O Read	O Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.	
	> Utilities	Deny	Read	⊚ Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.	_
						2
€ Exit					Review Back	Next

Acesso à função SecOps

c. Crie a Nova Função.

■ Cisco DNA Center		Create a User Role	
Summary Review the SecOps-Role role Make s	ure all the details are as you expect them t	to be. If you need to change something, clicking edit will take you back to that section	
V Role Name & Description Edit			
Role Name SecOps-Role			
Role Description			
<ul> <li>Kole Gapability Edit</li> </ul>			
ASSURANCE			
Monitoring and Troubleshooting	Deny		
Monitoring Settings	Deny		
Troubleshooting Tools	Deny		
NETWORK ANALYTICS			
Data Access	Write		
NETWORK DESIGN			
Advanced Network Settings	Deny		
Image Repository	Deny		
Network Hierarchy	Deny		
Network Profiles	Deny		
Network Settings	Deny		
Virtual Network	Denv		
- Exit			Back Create Role

Resumo da função SecOps

■ Cisco DNA Center		Create a User Role	ରେ ତ ଦ
PnP	Deny		
Provision	Deny		
NETWORK SERVICES			
App Hosting	Deny		
Bonjour	Deny		
Stealthwatch	Deny		
Umbrella	Deny		
PLATFORM			
APIs	Write		
Bundles	Deny		
Events	Deny		
Reports	Deny		
SECURITY			
Group-Based Policy	Write		
IP Based Access Control	Write		
Security Advisories	Write		
SYSTEM			
Machine Reasoning	Deny		
System Management	Deny		
UTILITIES			
Audit Log	Deny		
Event Viewer	Read		
Network Reasoner	Read		1
- Exit			Back Create Role

Revisar e criar a função SecOps

Etapa 2. Configurar a autenticação externa usando TACACS+. Isso pode ser feito na guia System > Users & Roles > External Authentication.

a. Para habilitar a autenticação externa no Cisco DNA Center, marque a caixa de seleção Habilitar usuário externo.

b. Defina os atributos AAA.

Insira Cisco-AVPair no campo AAA attributes.

c. (Opcional) Configure o servidor AAA primário e secundário.

Certifique-se de que o protocolo TACACS+ esteja habilitado no Primary AAA Server pelo menos, ou nos servidores Primary e Secondary.

E Cisco DNA Center	System / Users & Roles C	20	0	4
User Management Role Based Access Control External Authentication a b	External Authentication  Cisco DNA Center supports external servers for authentication and authorization of External Users. Use the fields in this window to create, update and delete AAA Servers. The AAA Attribute here on Cisco D name of the AAA attribute chosen on the AAA server. The default attribute expected is Cisco-AVPair, but if the user chooses to change it to any other AAA attribute, it needs to be configured here on Cisco D. The value of the AAA attribute to be configured for authorization on AAA server would be in the format of "Role=role1." On ISE server, choose the cisco-av-pair attribute from cisco specific AAA attributes liconfiguration inside Authorization profile would look like "cisco-av-pair" Role=SUPER-ADMIN-ROLE:  An example configuration in the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".  An example configuration is the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".  An example configuration is the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".  An example configuration is the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".  An example configuration is the case of manually defining the AAA attribute would be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".  AAA Attribute  AAA Attribute  Reset to Default Update	NA Cent DNA Ce st. A sar	er is th enter. mple	10
C	✓ AAA Server(s)       Primary AAA Server     Secondary AAA Server       IP Address     IP Address       ISE Server 1 IP     ISE Server 2 IP       Shared Secret     Shared Secret       Imfe     Infe       Hide Advanced Settings     Hide Advanced Settings       O RADIUS     TACACS       Port     49			

(TACACS+) Etapas de configuração da autenticação externa

## (Opção 2) Configurar o 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.

=	dealer Identity Services	Engine						Administration /	System			a	۵ ۵	0 0 0
н	Bookmarks	Deployn	nent Licensing	Certificate	s Logging	Maintenance	Upgrade & Rollback	Health Checks	Backup & Restore	Admin Access	Settings			
53	Dashboard													
15	Context Visibility				Adm	nistration								
*	Operations					de a la cale a								
0	Policy					vionitoring								
20	Administration				Ro	e P	OMARY	×						
ñ	Work Centers				Ot	her Monitoring Node								
٢	Interactive Help				0	Dedicated MnT 🕡								
					<b>—</b> • 1	olicy Service								
					<b>2</b> ~	Enable Session Ser	vices 🕕							
						Include Node in No	de Group None		~ O					
						ship Drofiling Sandra								
						auto Provinsing Gervice								
					L) En	able Threat Centric N	IAC Service 🕡							
						Enable SXP Service	0							
					1 🔳	able Device Admin 5	Service 🕡							
					0.6	able Passive Identity	Service 🕡							
					<b>—</b> ~ ,	xGrid ()								
					En	able pxGrid Cloud 🤅	)							
													2	
												Reset (	Sin	•

Etapa 2. Adicionar o servidor DNAC como um dispositivo de rede no ISE.

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

Procedimento

- a. Defina o IP e o nome do dispositivo de rede (DNAC).
- b. (Opcional) Classifique o tipo de dispositivo para a condição do conjunto de políticas.
- c. Ative as configurações de autenticação TACACS+.
- d. Definir segredo compartilhado TACACS+.

≡ deale Identity Services	Engine		Administration / Network Resources								0   A
JI Bookmarks	Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	External MDM	pxGrid Direct Connectors				
<ul> <li>Enableard</li> <li>Context Visibility</li> <li>Operations</li> <li>Policy</li> <li>Administration</li> <li>Work Centers</li> <li>Interactive Help</li> </ul>	Vetench Device Darland Device Device Security Settings	a Descriptio Descriptio Device Pri Model Nar Software 1 Network D	es List 3 DMAC Devices n n free <u>m</u> Class me evice Group	ver IP	- <sup>/</sup> <u>32</u>						
L		Location UPSEC Device Tyr C C	All Locations No DRAC-Servers DRAC-Servers ADUUS Authentication Set TACACS Authentication Set TACACS Authentication Set TaCACS Data English English Single Connect Mode Legacy Clace Drvice D Legacy Clace Drvice D TaCACS Draft Cengliance Si SNMP Settlings	Set To D      Set To D      Show  ngle Connect Support	rfault rfault Retire						

Dispositivo de rede (DNAC) ISE para TACACS+

Etapa 3. Criar perfis TACACS+ para cada função DNAC.

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

Note: Crie 3x perfis TACACS+, um para cada função de usuário.

- a. Clique em Add e defina o nome do Perfil TACACS.
- b. Clique na guia Visualização bruta.
- c. Insira Cisco-AVPair=ROLE= e preencha a função de usuário correta.
  - Para a função de usuário (SecOps-Role), digite Cisco-AVPair=ROLE=SecOps-Role.

- Para a função de usuário (NETWORK-ADMIN-ROLE), digite Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE.
- Para a função de usuário (SUPER-ADMIN-ROLE), digite Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE.

Note: Lembre-se de que o valor AVPair (Cisco-AVPair=ROLE=) diferencia maiúsculas de minúsculas e garante que ele corresponda à função de usuário DNAC.

d. Click Save.

≡	dentity Services	Engine	Work Centers / Device Administration							q	۵	9 Ç	A   A
н	Bookmarks	Overview Identities	User Iden	itity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
	Dashboard	Conditions	> та	ACACS Profiles > N	ew								
1d	Context Visibility	Network Conditions	> T/	ACACS Profile	a								
*	Operations	Results	v (N	lame									
- 0	Policy	Allowed Protocols	C	ecups_Role		)							
8.	Administration	TACACS Command Sets	De	escription									
តា	Work Centers	TACACS Profiles		a composition		7							
•	Interactive Help		C C	ask Attribute View rofile Attribute Cisco-AVPair=RO	B Raw View IS LE=SecOps-Role	Cancel	d Save						

Criar perfil TACACS (SecOps\_Role)

Etapa 4. Criar Grupo de Usuários.

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

- a. Clique em Add e defina o nome do grupo de identidade.
- b. (Opcional) Defina a Descrição.
- c. Clique em Submit.

≡ dentity Services	s Engine		Work Centers / Device Administration						9 Q	9   A
II Bookmarks	Overview Identities	User Identity Groups	Ext Id Sources Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
Dashboard		User identity (	Groups > New User Identity Group							
$ {}^{I:I}_{O}$ Context Visibility	Identity Groups	Identity G	roup							
X Operations	< 18	a Name	SecOps							
Policy	> 🛅 Endpoint Ide	entity Groups	SecOps-Role							
2 Administration	> 🛅 User Identif	b Description	an i							
							С			
Interactive Help							Submit	D	Cance	ы

Criar Grupo de Identidades de Usuário

#### Etapa 5. Criar Usuário Local.

Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Identidades > Usuários.

- a. Clique em Add e defina o nome de usuário.
- b. Defina a Senha de login.
- c. Adicione o usuário ao grupo de usuários relacionado.
- d. Clique em Submit.

≡	dentity Services I	Engine		Work Centers / Device Administration							٩	۵ ۵	0 Q   A	
н	Bookmarks	Overview	Identities	User Identity G	roups	Ext Id Sources	Network Re	sources	Policy Elements	Device Admin Policy	Sets Reports	Settings		
5	Dashboard	Users		Network	Access Users L	List > New Network Ad	cess User							
망	Context Visibility													
*	Operations			~ Net	work Acc	ess User								
-0	Policy			a 🕛	rname	SecOps_User								
8.	Administration			Statu	8	Z Enabled 🗸								
đ	Work Centers			Acco	unt Name Ali	ias		0						
				Emai										
?	Interactive Help													
				∨ Pa	sswords									
				Pas	word Type:	Internal Users	~							
				Pas	word Lifetim	ne:								
				•	With Expiration	on 🕕								
				0	Vever Expire:	expire in 60 days is 🕕								
						Password		Re-Enter	r Password					
				D Lo	gin Password	d				Generate Password	0			
				Enal	ele Password	đ				Generate Password	0			
				∨ Us	er Informa	ation								

```
Criar usuário local 1-2
```

≡	alada Identity Services	Engine			Work			Q	ۍ ک	Q	۹		
н	Bookmarks	Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	Reports	Settings			
	Dashboard	Users		✓ User Inform	mation								
1d	Context Visibility			First Name									
*	Operations			Last Name									
-0	Policy												
2.	Administration			✓ Account C	otions								
đ	Work Centers			Description	,								
?	Interactive Help			Change passv	rord on next login								
				✓ Account D	isable Policy								
				Disable a	ccount if date exceed	s 2025-03-20	(yyyy-mm-dd)						
					С								
				<ul> <li>✓ User Grou</li> <li>∷ SecOpe</li> </ul>	ps	~ (i) 😁							
										d			
										<u> </u>			
										Submit	J °	ancel	

Criar usuário local 2-2

Etapa 6. (Opcional) Adicionar conjunto de políticas TACACS+.

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

#### Procedimento

a. Clique em Ações e escolha (Inserir nova linha acima).

- b. Defina o nome do Conjunto de políticas.
- c. Defina Policy Set Condition como Select Device Type criado anteriormente em (Etapa2 > b).
- d. Defina os protocolos permitidos.
- e. Click Save.

f. Clique em (>) Policy Set View para configurar as regras de autenticação e autorização.

≡	dentity Services E	ngine		Policy / Policy Sets	Q & @ Q   A
н	Bookmarks	Policy Sets			Reset Reset Policy Set Hit Counts Save
	Dashboard	Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
15	Context Visibility	Q Search		C	d f
*	Operations				
0	Policy	Unixe - Policy		Rear and the second sec	
8.	Administration	O Default	Default policy set		Default Network Access 🥜 🕂 o 🍪 🕻
-file	Work Centers				e
					Reset
?	Interactive Help				

Adicionar conjunto de políticas TACACS+

Etapa 7. 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

- a. Clique em Ações e escolha (Inserir nova linha acima).
- b. Defina o nome da Diretiva de Autenticação.

c. Defina Authentication Policy Condition e Select Device Type criado anteriormente em (Etapa2 > b).

d. Defina a Política de autenticação Usar para a origem da Identidade.

e. Click Save.

≡	diade Identity Services I	ingine Work Centers / Device Administration	Q 4	0	Q	A
Л	Bookmarks	Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements	ce Admin Policy Sets Reports Settings			
	Dashboard	Policy Sets→ DNAC - Policy	Reset Reset Policy Set Hit Count		e Save	ה
18 X	Operations	Status Policy Set Name Description Conditions	Allowed Protocols / Servi	er Seque	ice Hit	ts
0	Policy	Q Search				
2.0	Administration	DNAC - Policy     DEVICE Oevice Type EQUALS All Device TypestDNAC	Default Device Admin	0	+ 0	
-		~Authentication Policy(2)				
?	Interactive Help	Status Rule Name Conditions	Use	Hits	Actions	
		Q. Search	d			
		DNAC - Authentication     DEVICE Device Type EQUALS All Device TypesIIDNAC-Servers	Internal Users     Options	0	曫	
			All_User_ID_Stores		eôn	
		Cersuit	> Options	0	ф	
		> Authorization Policy - Local Exceptions				
		> Authorization Policy - Global Exceptions				
		> Authorization Policy(4)				

Adicionar política de autenticação TACACS+

Etapa 8. 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 de Usuário:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- SecOps-Função

#### Procedimento

- a. Clique em Ações e escolha (Inserir nova linha acima).
- b. Defina o nome da Política de Autorização.

c. Defina a Condição de Política de Autorização e Selecione o Grupo de Usuários criado em (Etapa 4).

d. Defina os perfis do shell da política de autorização e selecione o perfil TACACS que você criou em (Etapa 3).

e. Click Save.

≡	dentity Services I	Engine				We	ork Centers /	/ Device Adı	ministratio	on no				Q (	<b>4</b> 0	Q	A
Щ	Bookmarks	Overview	Identi	ties User Identity	Groups	Ext Id Sources	Network	Resources	Policy Ele	ements Devi	ce Admin Policy Se	ts Repo	rts Setti	ngs			
	Dashboard	0	Search														
망	Context Visibility		0	DNAC - Policy			DEVICE-Dev	vice Type EQUAL	S All Device Typ	pes#DNAC			Default Devic	e Admin		+	0
- %	Operations																
-0	Policy	> Aut	hentication	Policy(2)													
8.	Administration	> Aut	horization F	folicy - Local Exceptions													
đ	Work Centers	> Aut	horization F	folicy - Global Exceptions													
		VAUD	norization F	oncy(1)													
?	Interactive Help									Results							
		•	Status	Rule Name	Condit	ions				Command Sets		Shell Profile	5		Hits	Action	15
		(	Q Search					1									
	SUPER-ADMIN	I-ROLE	0	Super Admin	8.4	SentityGroup-Name EQ	UALS User Identity	y Groups:SUPER-/	ADMIN	Select from list	0 +	SUPER_AD	MIN_ROLE		•)	   	
	NETWORK-ADM	IN-ROLE	0	Network Admin	8 1	dentityGroup-Name EQ	UALS User Identity	y Groups:NETWOR	K-ADMIN	Select from list	0 +	NETWORK	_ADMIN_ROLE	<b>@</b> ~	•)		
	SecOps-Rol	le	0	SecOps	8.1	dentityGroup-Name EQ	UALS User identity	y Groups:SecOps		Select from list	0 +	SecOps_R	ole	@ ~	•)	(2)	
			۲	Default						DenyAllComman	ds 🖉 +	Deny All Si	ell Profile	0	+ •	   	
																2	
															6	2	
														Resi	R U	Save	

Adicionar Política de Autorização

# Verificar

# Verificar a configuração do RADIUS

1- DNAC - Exibir Sistema de Usuários Externos > Usuários e Funções > Autenticação Externa > Usuários Externos.

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.

	■ Cisco DNA Center	Sys	tem / Users & Roles		Q @ C Q
	User Management	External Authentication			
Ē	External Authentication	Cisco DNA Center supports external servers for authentication and authorizat name of the AAA attribute chosen on the AAA server. The default attribute ex	on of External Users.Use the fields in this window to create, updat pected is Cisco-AVPair, but if the user chooses to change it to any	e and delete AAA Servers. The AAA Attribute here on Cis other AAA attribute, it needs to be configured here on C	co DNA Center is the Cisco DNA Center.
		The value of the AAA attribute to be configured for authorization on AAA ser- configuration inside Authorization profile would look like "cisco-av-pair= Role	er would be in the format of "Role=role1". On ISE server, choose th =SUPER-ADMIN-ROLE".	e cisco-av-pair attribute from cisco specific AAA attribu	tes list. A sample
		An example configuration in the case of manually defining the AAA attribute	rould be "Cisco-AVPair=Role=SUPER-ADMIN-ROLE".		
		🕑 Enable External User 😗			
		<ul> <li>AAA Attribute</li> <li>AAA Attribute</li> <li>Cisco-AVPair</li> <li>Reset to Default</li> <li>Update</li> <li>AAA Server(s)</li> <li>External Users</li> </ul>			
		√ Filter		EQ, Find	
		Username *	Role	Action	
		devops_user	DevOps-Role	Delete	
			Showing 1 of 1		

2. DNAC - Confirmar acesso do usuário.

Cisco DNA Center			Q @ D
Cisco DNA Center	Overview Manage Developer Toolkit Runtime Dashboard	enter with the adoption journey map. time to value, as you guide your organization on its	C O C
A devops_user ≪			

Acesso de usuário limitado

## 3.a ISE - RADIUS Live-Logs Operações > RADIUS > Live-Logs.

=	dealer Identity Services I	Ingine	Operations	/ RADIUS		Q & @ Q   A
Л	Bookmarks	Live Logs Live Sessions				
- 53	Dashboard					
15	Context Visibility	Misconfigured Supplicants 🕕	Misconfigured Network Devices 🕕	RADIUS Drops	Client Stopped Responding ()	Repeat Counter ()
*	Operations	0	0	5761	0	0
- 0	Policy				Refresh Show	Within
8.	Administration				Never V Latest 20	) records 🗸 Last 60 Seconds
d.	Work Centers	Ø     ⇔ Reset Repeat Counts				Filter 🗸 🔘
		Time Status Details	Repea Identity Endpoint ID	Endpoint Profile Authentication Pol	licy Authorization Policy A	uthorization Profiles IP Addre
?	Interactive Help	X Auth	DevOns User	Endpoint Profile Authentication Policy	Authorization Policy A	v/horization Profiles IP Addres
		Last Updated: Sun Jan 19 2025 23:19:57 GMT+0100	(Central European Standard Time)			Records Shown: 1

Registros ao vivo RADIUS

3.b ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs > Click (Details) for Authorization log (Detalhes do registro de autorização).



Steps		
Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
11015	An Access-Request MUST contain at least a NAS-IP- Address, NAS-IPv6-Address, or a NAS-Identifier; Continue processing	1
11117	Generated a new session ID	2
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	2
15041	Evaluating Identity Policy	3
15048	Queried PIP - DEVICE.Device Type	4
15013	Selected Identity Source - Internal Users	3
24210	Looking up User in Internal Users IDStore - DevOps_User	0
24212	Found User in Internal Users IDStore	8
22037	Authentication Passed	1
15036	Evaluating Authorization Policy	1
15016	Selected Authorization Profile - DevOps-Profile	5
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	1
11002	Returned RADIUS Access-Accept	0

Registros ao vivo detalhados do RADIUS 1-2

Cisco ISE	
IdentityPolicyMatchedRule	DNAC - Authentication
AuthorizationPolicyMatchedR ule	DevOps
ISEPolicySetName	DNAC - Policy
IdentitySelectionMatchedRule	DNAC - Authentication
TotalAuthenLatency	35
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#DNAC-Servers
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:DevOps
EnableFlag	Enabled
RADIUS Username	DevOps_User
Device IP Address	
CPMSessionID	0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8RtG/ WY
CiscoAVPair	AuthenticationidentityStore-internal Users, FQSkipterkhame+92731830-8c01-11e6-996c- 525400048514640905,user, UniqueSubjectID-994d28083db66a1f8bcc98565c8f5eaa5de df467
Result	
Class	CACS:0a301105o95d4kCbV7kMBCoFkesRirFcDiXec0uEqPPr8R G/WY:ise34/526427220/15433
cisco-av-pair R	ROLE=DevOps-Role

Registros ao vivo detalhados do RADIUS 2-2

## Verificar a configuração TACACS+

1- DNAC - Exibir Sistema de Usuários Externos > Usuários e Funções > Autenticação Externa > Usuários Externos.

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

■ Cisco DNA Center		System / Users & Roles		Q @ @ 4
User Management Role Based Access Control External Authentication	<ul> <li>AAA Attribute</li> <li>AAA Attribute</li> <li>Cisco-AVPair</li> <li>Reset to Default</li> <li>Upd</li> </ul>			
	<ul> <li>AAA Server(s)</li> <li>Primary AAA Server</li> <li>P Address</li> <li>Shared Secret</li> <li>*****</li> <li>info</li> <li>View Advanced Settings</li> <li>Update</li> </ul>	Secondary AAA Server		
	<ul> <li>✓ External Users</li> <li>✓ Filter</li> <li>Username =</li> <li>secops_user</li> </ul>	Role SecOps-Role	EQ Fil Action Delete	nd
		Showing 1 of 1		

Usuários externos

## 2. DNAC - Confirmar acesso do usuário.

Cisco DNA Center			Q ()
<sup>0</sup> ∏ <sup>0</sup> Policy	Group-Based Access Control		C Explore
- Workflows	IP & URL Based Access Control	enter with the adoption journey map.	×
% Tools		time to value, as you guide your organization on its	
Platform			
Activities			
Explore			
		Retwork Bug Identifier Identify bugs in the network	
요 secops_user			

Acesso de usuário limitado

3.a ISE - TACACS+ Live-Logs Centros de trabalho > Administração de dispositivos > Visão geral > TACACS Livelog.

≡	dentity Services	Engine		Opera	ations / TACACS			Q & @	Q   A
н	Bookmarks	Live Logs							
	Dashboard								
명	Context Visibility					Defeath	Chow	Within	
*	Operations					Never	✓ Latest 2	0 records 🗸 Last 60 S	leconds√
0	Policy	🖉 🏦 Export To 🗸						Filter 🗸	۲
20	Administration	Logged Time	Status Details I	dentity Type	Authentication Policy	Authorization Policy	Shell Profile Dev	ісе Туре	Lo
đ	Work Centers	×	`	Identity ~	Authentication Policy	Authorization Policy	Shell Profile Dev	се Туре	Lo
		Jan 19, 2025 05:12:4		SecOps_User Authorization		DNAC - Policy >> SecOps	SecOps_Role Devi	e Type#All Device Types#DNA	NC Loc
?	Interactive Help	Jan 19, 2025 05:12:4		SecOps_User Authentication	DNAC - Policy >> DNAC - Authentication		Devi	e TypeIIAII Device TypesIIDNA	C Loc
		Last updated: Sun Jan 19 2	025 17:16:38 GM1+0100 (Ce	entral European Standard Time	)			Records 3	snown: 2

Registros ao vivo TACACS

3.b ISE - TACACS+ Live-Logs Work Centers > Device Administration > Overview > TACACS Livelog > Click (Details) para log de autorização.

Cisco ISE				
Verview		Steps		
Request Type	Authorization	Step ID	Description	Latency (ms)
Status	Pase	13005	Received TACACS+ Authorization Request	
010/03	F 633	15049	Evaluating Policy Group	1
Session Key	ise34/526427220/13958	15008	Evaluating Service Selection Policy	1
Message Text	Device-Administration: Session Authorization succeeded	15048	Queried PIP - DEVICE.Device Type	4
Username	SecOps_User	15041	Evaluating Identity Policy	7
		15013	Selected Identity Source - Internal Users	5
Authorization Policy	DNAC - Policy >> SecUps	24210	Looking up User in Internal Users IDStore	1
Shell Profile	SecOps_Role	24212	Found User in Internal Users IDStore	4
Matched Command Set		22037	Authentication Passed	0
Command From Device		15036	Evaluating Authorization Policy	0
Command From Device		15048	Queried PIP - Network Access.UserName	10
		15048	Queried PIP - IdentityGroup.Name	2
		15017	Selected Shell Profile	2
uthorization Details		22081	Max sessions policy passed	1
Generated Time	2025-01-19 17:12:43.368 +1:00	22080	New accounting session created in Session cache	0
Logged Time	2025-01-19 17:12:43.368	13034	Returned TACACS+ Authorization Reply	
poch Time (sec)	1737303163			
SE Node	ise34			
Message Text	Device-Administration: Session Authorization succeeded			
Failure Reason				
Resolution				
Root Cause				
Username	SecOps_User			
Network Device Name	DNAC			

Registros ao vivo detalhados do TACACS+ 1-2

Cisco ISE	
1380	riteriorization
Service-Argument	cas-service
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
RequestLatency	38
IdentityGroup	User Identity Groups:SecOps
SelectedAuthenticationIdentit yStores	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	13004827410.62.150.14628131Authorization130048274
IdentitySelectionMatchedRule	DNAC - Authentication
StepLatency	1=1;2=1;3=4;4=7;5=5;6=1;7=4;8=0;9=0;10=10;11=2;12=2;1 3+1;14+0;15+0
TotalAuthenLatency	38
ClientLatency	0
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
Name	User Identity Groups:SecOps
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=Cisco- AVPair=ROLE=SecOps-Role; }

Registros ao vivo detalhados do TACACS+ 2-2

# Troubleshooting

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

# Referências

- <u>Guia do Administrador do Cisco Identity Services Engine, Versão 3.4 > Administração de</u> <u>Dispositivos</u>
- Guia do administrador do Cisco DNA Center, versão 2.3.5
- Cisco DNA Center: Controle de Acesso Baseado em Função com Autenticação Externa

#### 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.