

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[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 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.

1

Role Name*
DevOps-Role

Describe the role (optional)

Nome da Função DevOps

b. Defina o Acesso.

Define the Access

1

These permissions enable different capabilities in Cisco DNA Center, some of which are inter-dependent. Before making the selections, please ensure you understand the details of what each of these permissions allow. Click here to [Learn More](#).

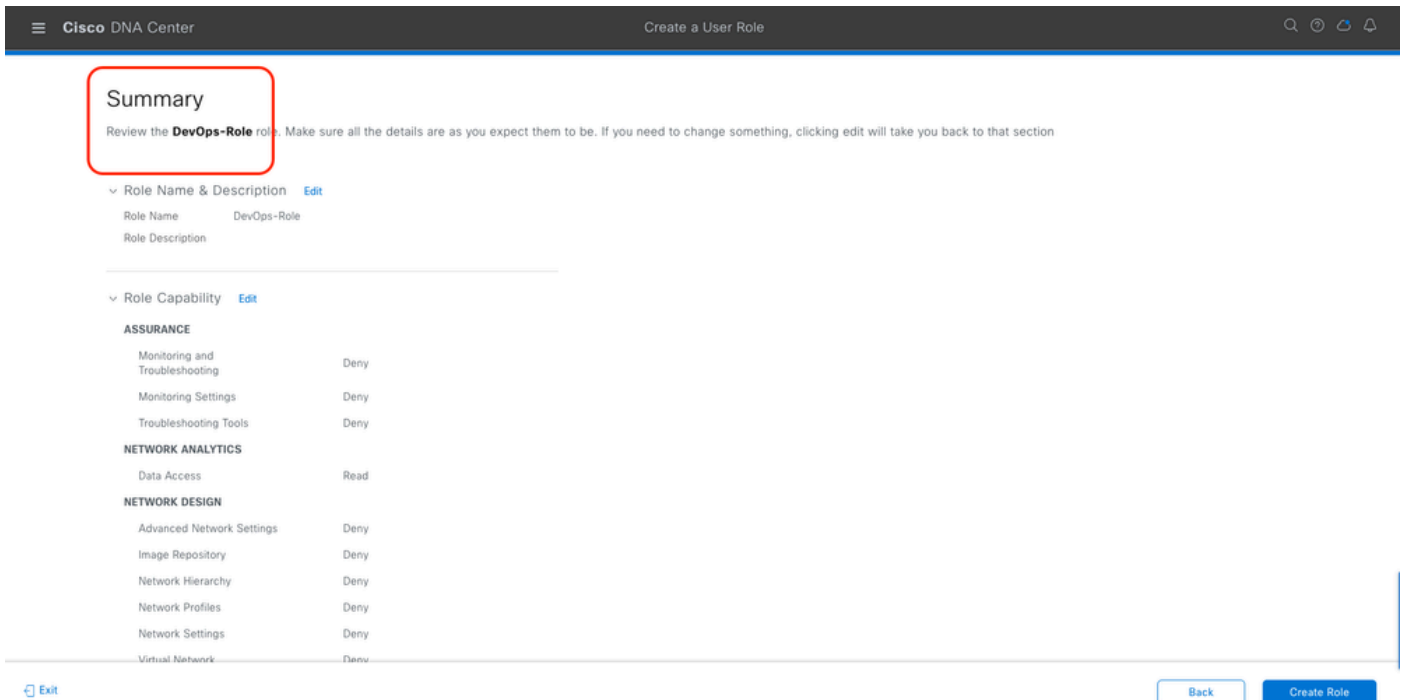
Define the **DevOps-Role** role. Custom roles permit or restrict user access to certain Cisco DNA Center functions. By default, roles are configured with Read permission, which is an Observer role. If a role is configured with Deny permission, all related content for that capability is removed from the GUI.

1

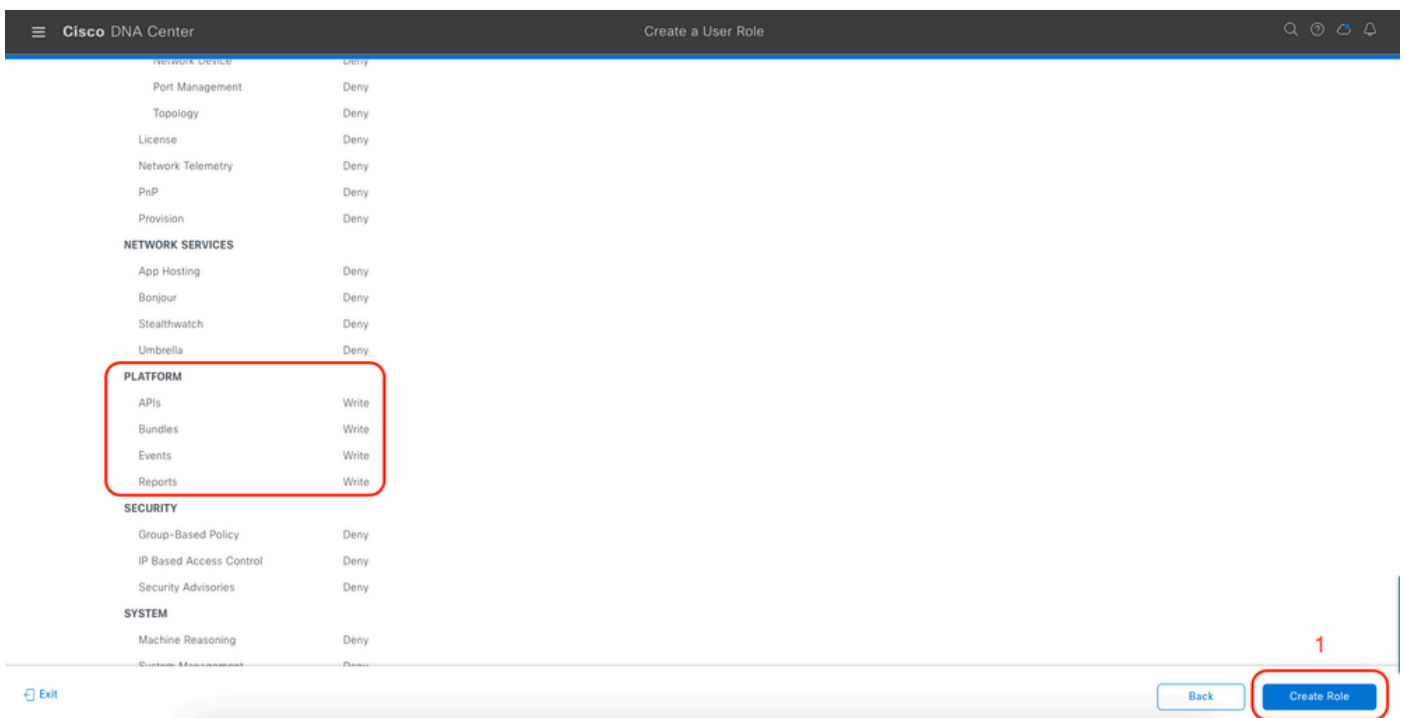
Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Access to Network Analytics related components.
> Network Design	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> 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	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure, upgrade, provision and manage your network devices.
> Network Services	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Configure additional capabilities on the network beyond basic network connectivity and access.
> Platform	<input type="radio"/> Deny <input checked="" type="radio"/> Read <input type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Manage and control secure access to the network.

Acesso à Função DevOps

c. Crie a Nova Função.



Resumo da função DevOps



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.

The screenshot displays the 'External Authentication' configuration interface in Cisco DNA Center. It includes a sidebar with navigation options like 'User Management' and 'External Authentication'. The main content area contains instructions and configuration fields. Three specific areas are highlighted with red boxes and labeled 'a', 'b', and 'c':

- a:** A red box highlights the 'Enable External User' checkbox, which is checked.
- b:** A red box highlights the 'AAA Attribute' dropdown menu, which is set to 'Cisco-AVPair'.
- c:** A red box highlights the 'AAA Server(s)' section, which is configured with two servers: 'Primary AAA Server' and 'Secondary AAA Server'. Both are set to use 'RADIUS' and have an 'Authentication Port' of '1812'.

(RADIUS) Etapas de configuração da autenticação externa

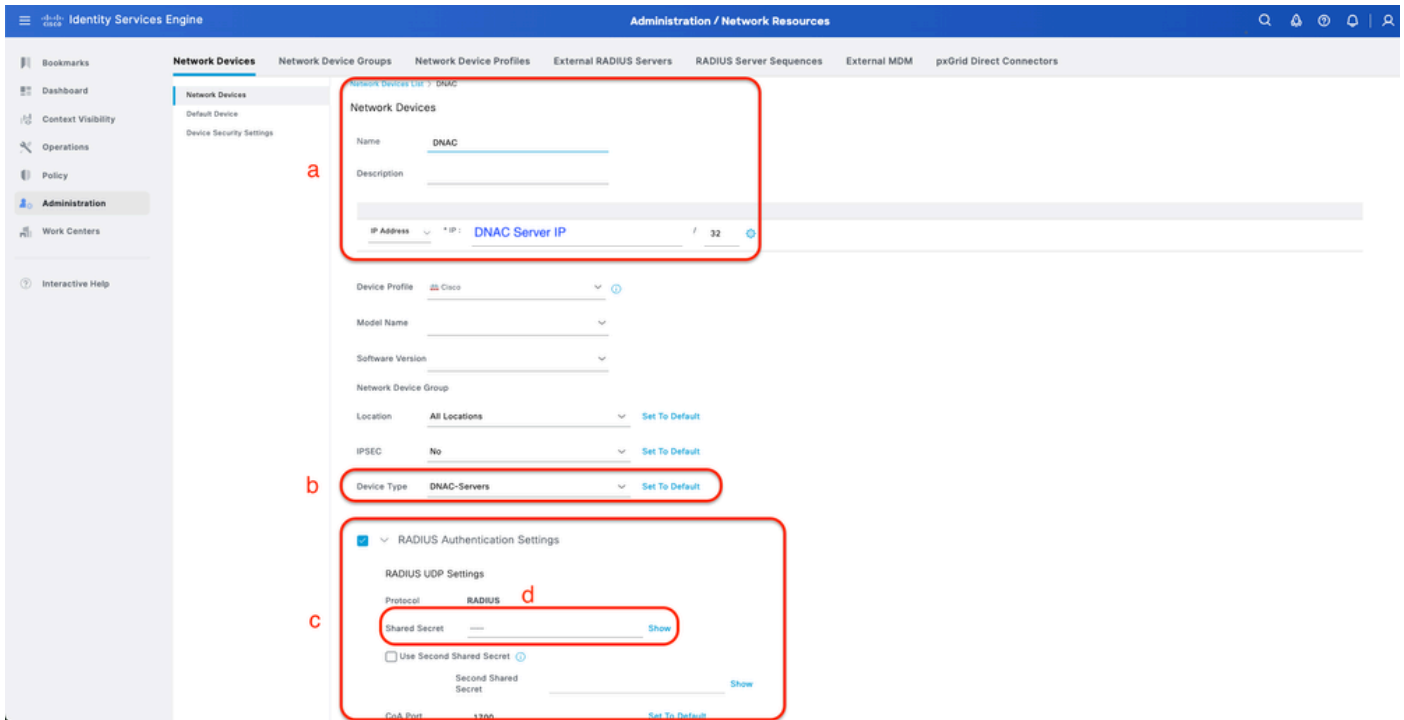
(Opção 1) Configurar ISE para RADIUS

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

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

Procedimento

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



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

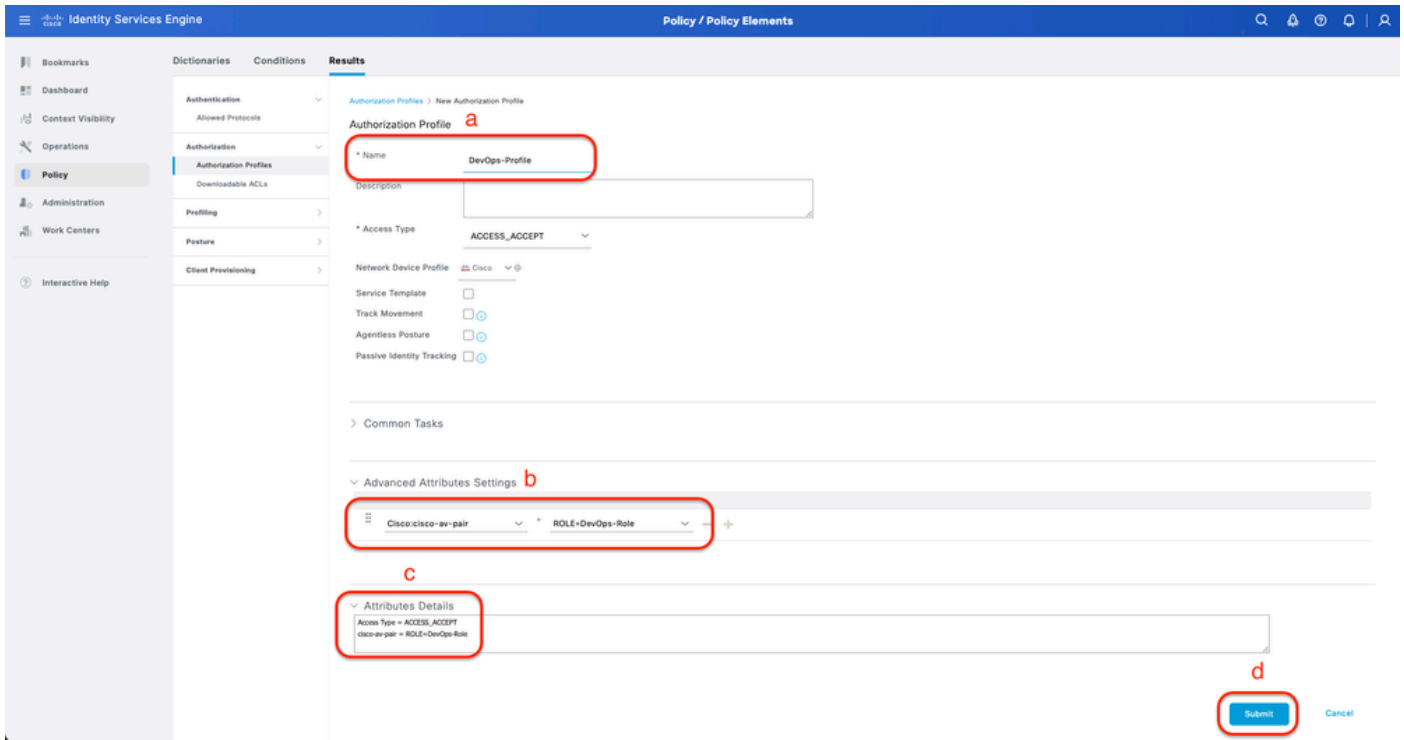
a. Clique em Add e defina o nome do Perfil de Autorização RADIUS.

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.



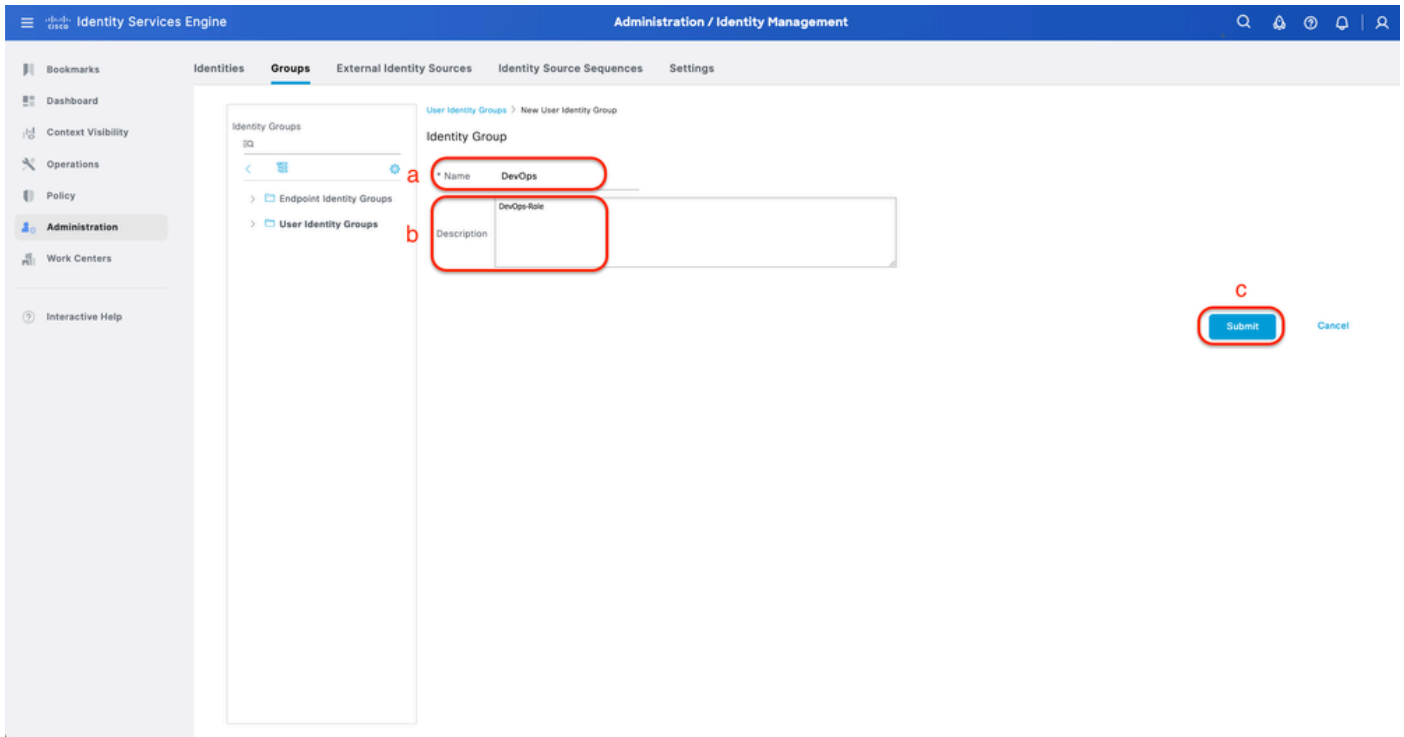
Criar perfil de autorização

Etapa 3. Criar Grupo de Usuários.

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

Procedimento

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

Procedimento

- 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.

Criar usuário local 1-2

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).

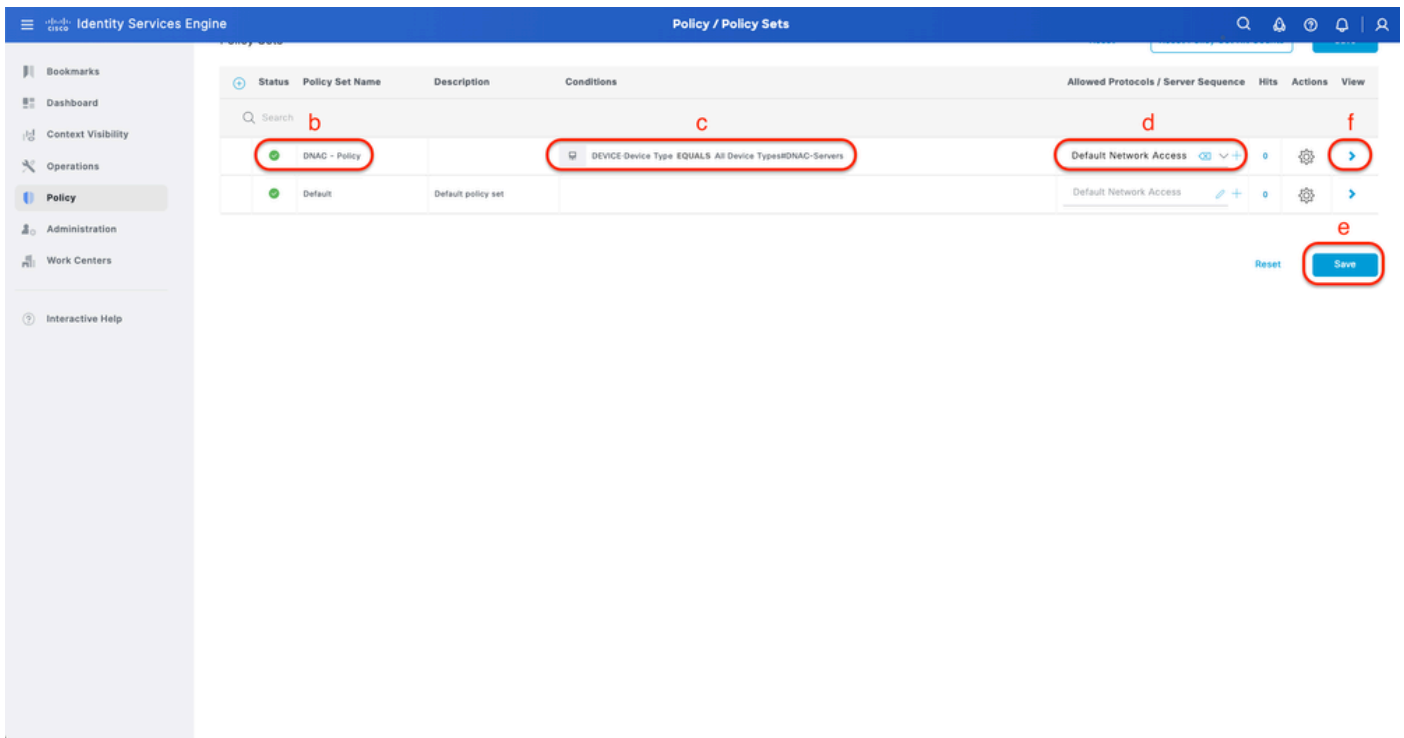
b. Defina o nome do Conjunto de políticas.

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.

Identity Services Engine Policy / Policy Sets

Policy Sets -> DNAC - Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	DNAC - Policy		DEVICE Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0

Authentication Policy(2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	DNAC - Authentication	DEVICE Device Type EQUALS All Device Types#DNAC-Servers	Internal Users	0	⚙️
●	Default		All_User_ID_Stores	2	⚙️

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy(1)

Reset 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.

Identity Services Engine Policy / Policy Sets

Policy Sets -> DNAC - Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	DNAC - Policy		DEVICE-Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0

> Authentication Policy(2)
 > Authorization Policy - Local Exceptions
 > Authorization Policy - Global Exceptions
 < Authorization Policy(4)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Super-Admin_Role_Pr...	Select from list	0	⚙️
●	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Network-Admin_Role_...	Select from list	0	⚙️
●	DevOps	IdentityGroup-Name EQUALS User Identity Groups:DevOps	DevOps-Profile	Select from list	0	⚙️
●	Default		DenyAccess	Select from list	0	⚙️

Reset Save

Adicionar Política de Autorização

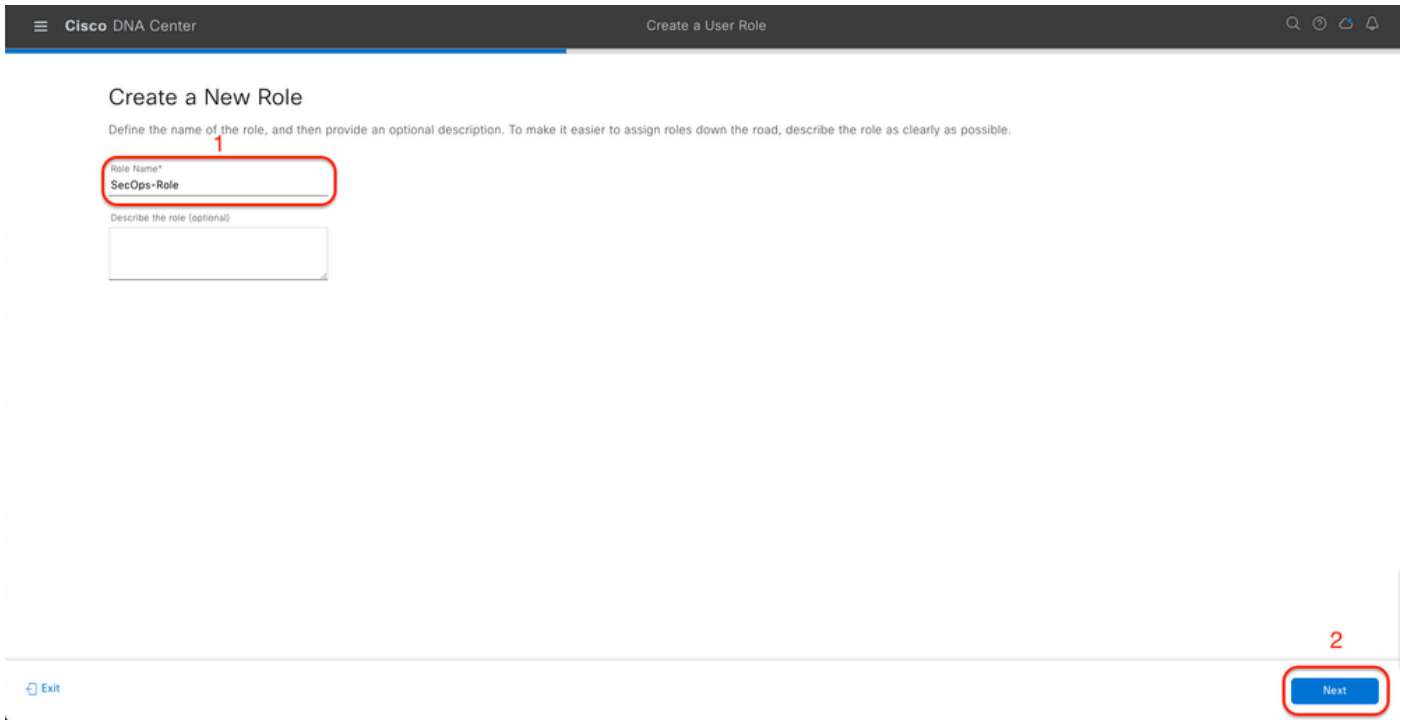
(Opção 2) Configurar a autenticação externa de DNAC usando TACACS+

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.

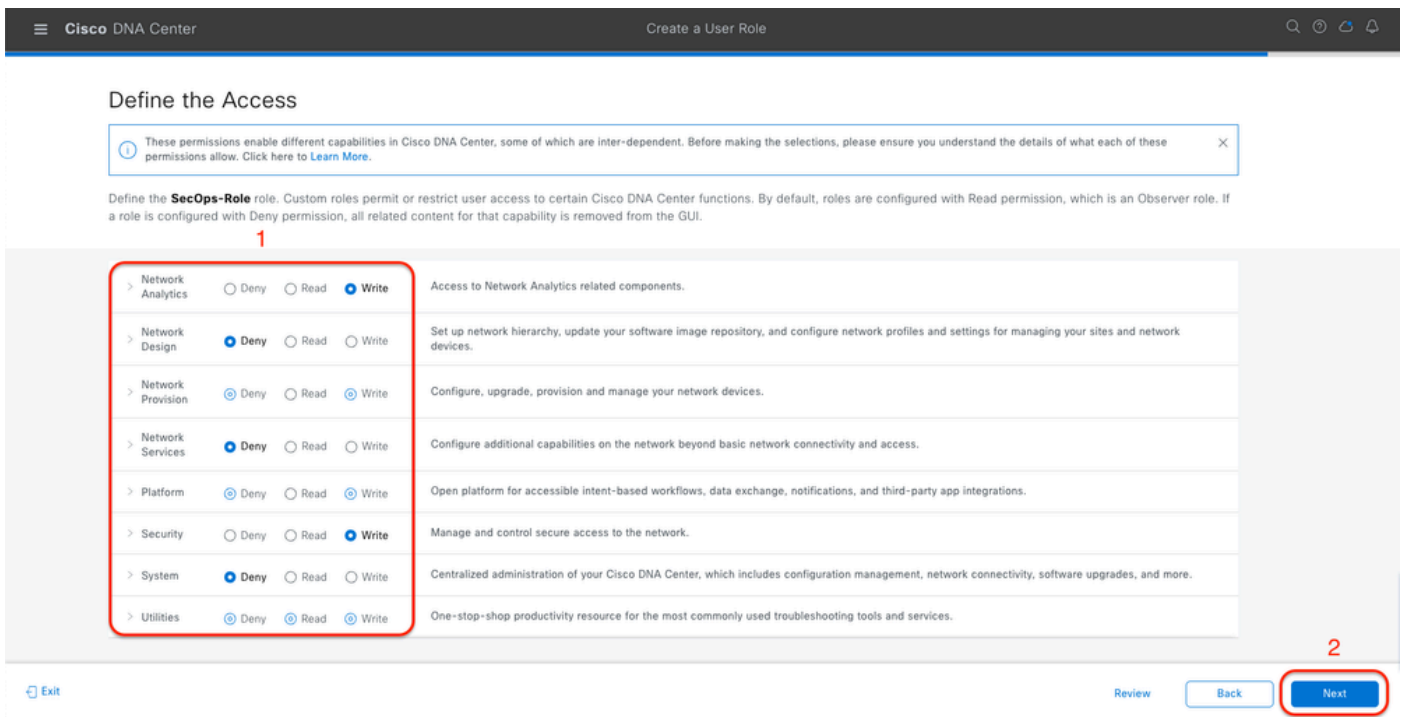
Procedimento

a. Crie uma nova função.



Nome da Função SecOps

b. Defina o Acesso.



Acesso à função SecOps

c. Crie a Nova Função.

Cisco DNA Center Create a User Role

Summary

Review the **SecOps-Role** role. Make sure all the details are as you expect them to be. If you need to change something, clicking edit will take you back to that section.

Role Name & Description [Edit](#)

Role Name	SecOps-Role
Role Description	

Role Capability [Edit](#)

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	Deny

[Exit](#) [Back](#) [Create Role](#)

Resumo da função SecOps

Cisco DNA Center Create a User Role

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

[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.

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles'. On the left, there is a navigation menu with 'External Authentication' selected. The main content area has a header 'External Authentication' and a sub-header 'External Authentication'. Below this, there is a section 'Enable External User' with a checkbox that is checked and circled in red, labeled 'a'. Below that is a section 'AAA Attribute' with a dropdown menu showing 'Cisco-AVPair' selected, circled in red, labeled 'b'. At the bottom, there is a section 'AAA Server(s)' with two columns: 'Primary AAA Server' and 'Secondary AAA Server'. Both columns have 'IP Address' set to 'ISE Server 1 IP' and 'ISE Server 2 IP' respectively, and 'Shared Secret' set to '*****'. The 'TACACS+' radio button is selected in both columns, circled in red, labeled 'c'. There are 'Reset to Default' and 'Update' buttons at the bottom of the configuration area.

(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.

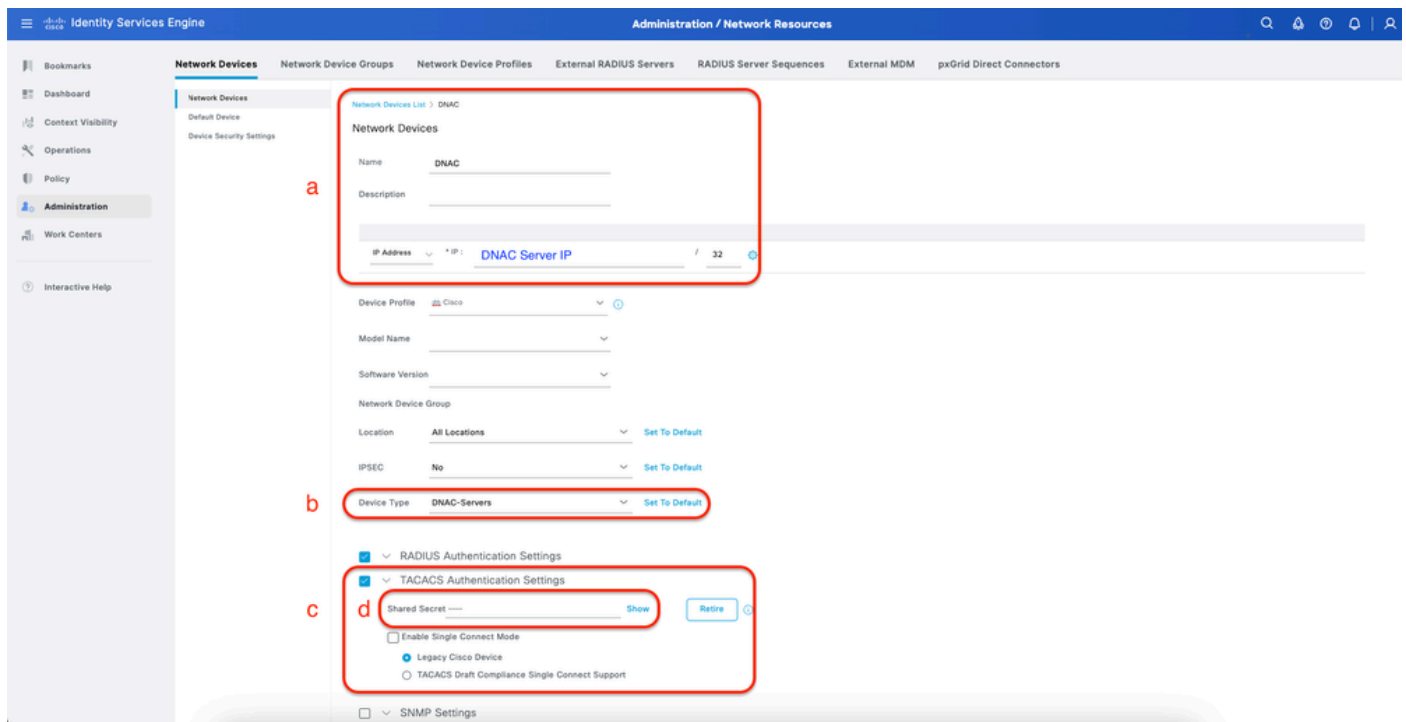
The screenshot shows the 'Administration / System' page in Identity Services Engine. The 'Deployment' tab is selected. The page displays various configuration options for the system. The 'Administration' section is expanded, showing 'Monitoring' and 'Policy Service' sections. In the 'Policy Service' section, the 'Enable Device Admin Service' checkbox is checked and circled in red, labeled '1'. At the bottom right, there is a 'Save' button circled in red, labeled '2'. The page also includes a navigation menu on the left and a top navigation bar with 'Administration / System' and search, refresh, and help icons.

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


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



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.

Procedimento

- Clique em Add e defina o nome do Perfil TACACS.
- Clique na guia Visualização bruta.
- 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.

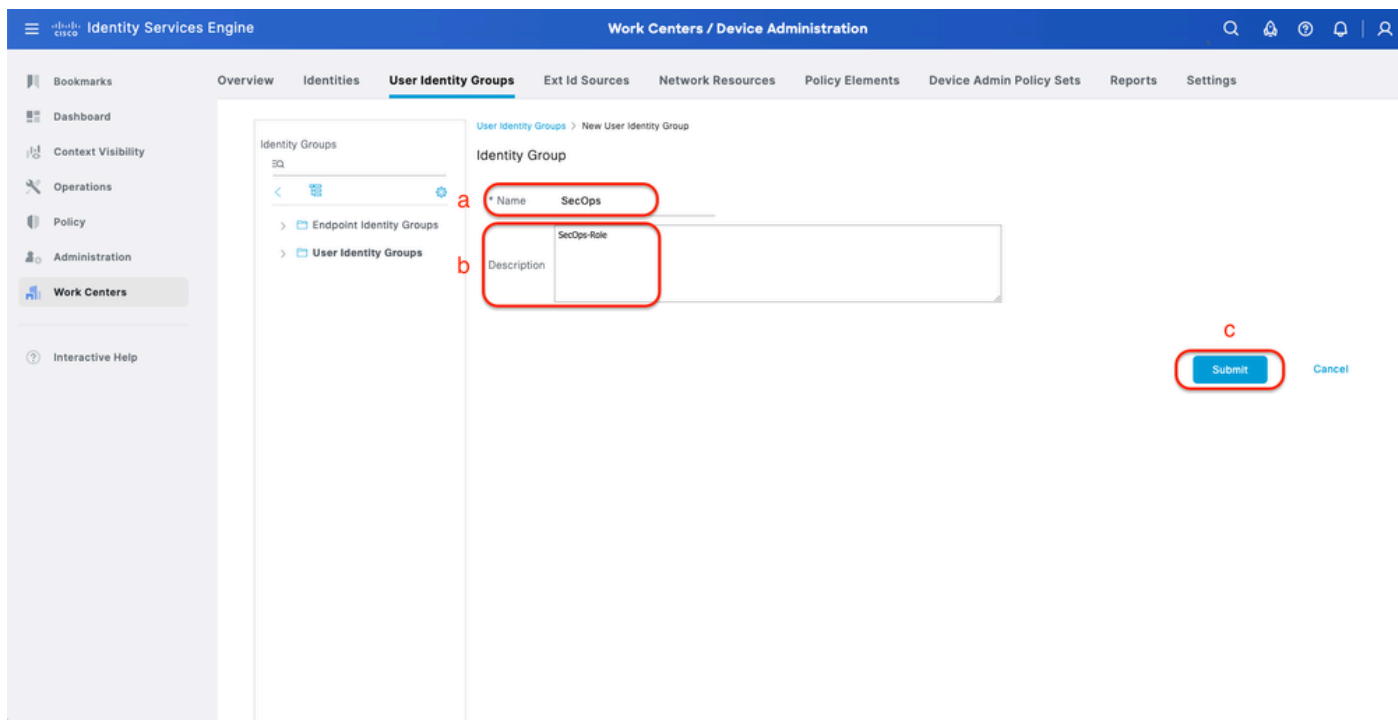
Criar perfil TACACS (SecOps_Role)

Etapa 4. Criar Grupo de Usuários.

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

Procedimento

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



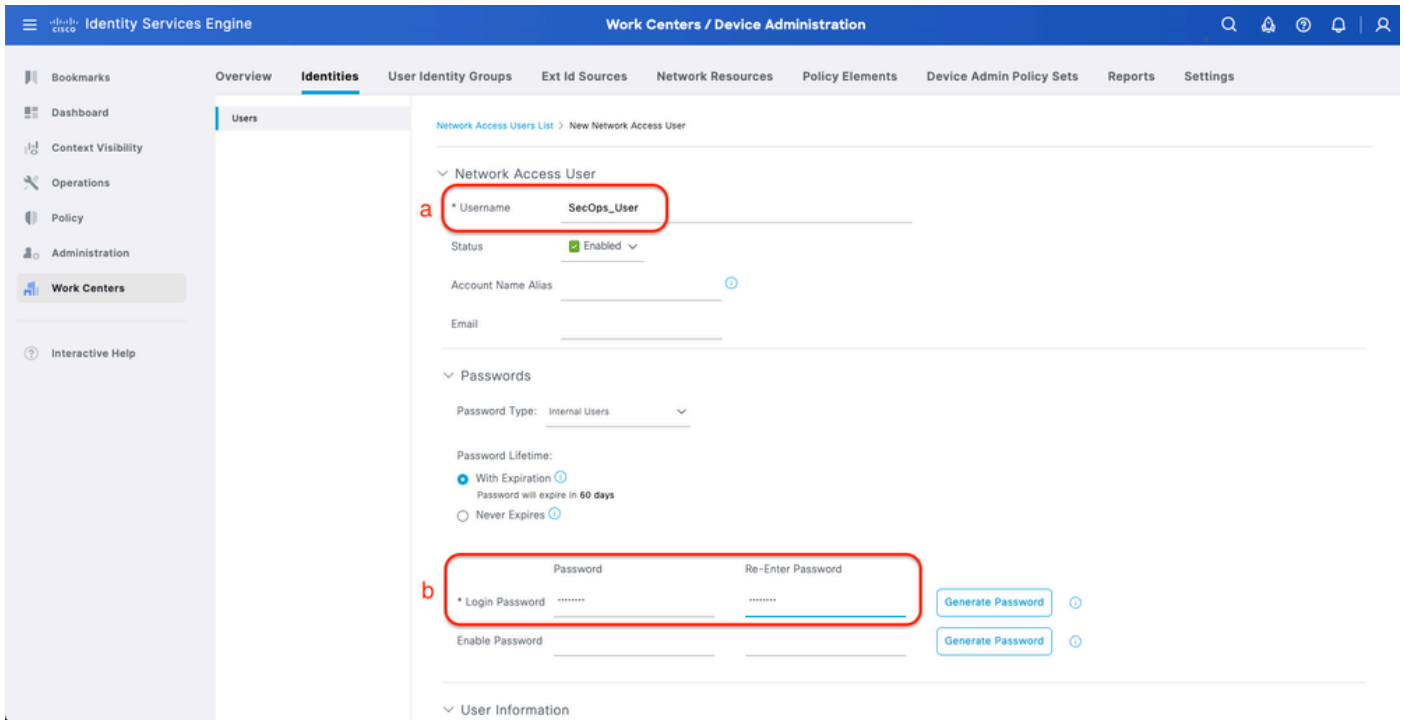
Criar Grupo de Identidades de Usuário

Etapa 5. Criar Usuário Local.

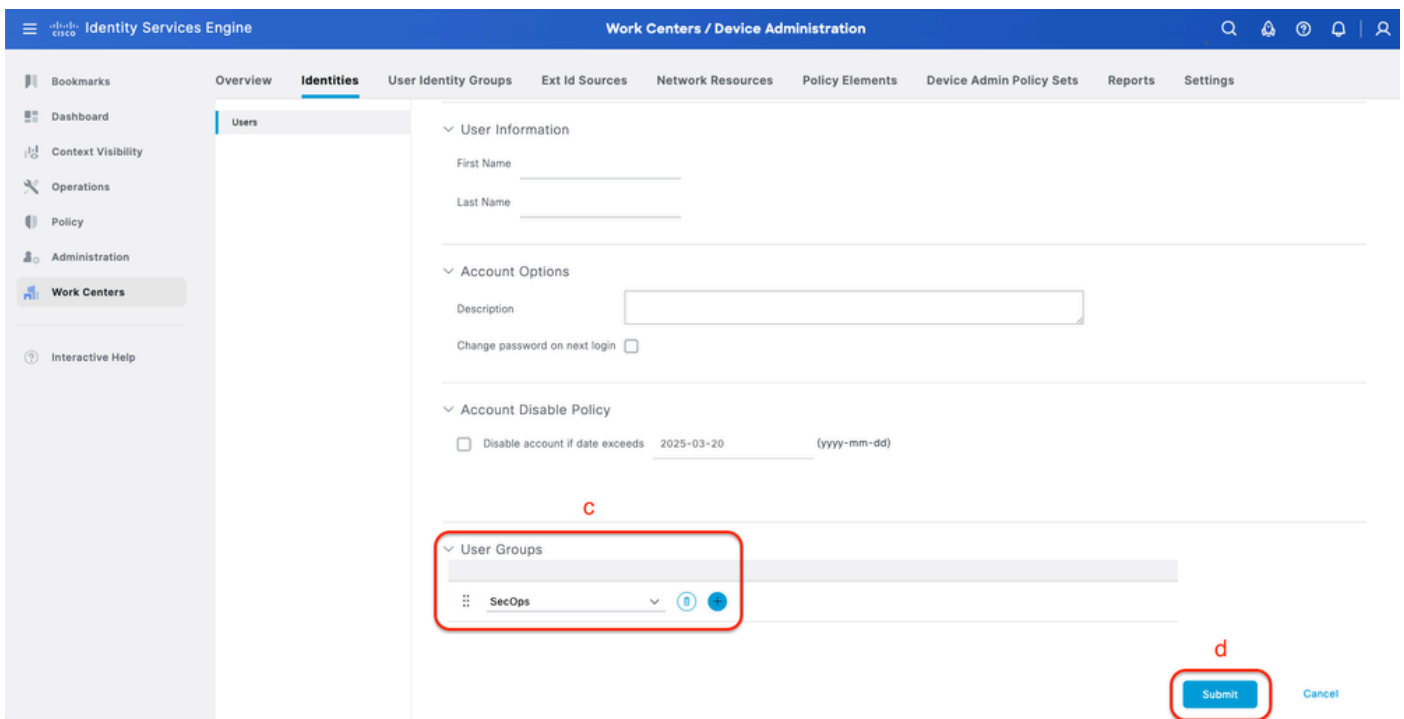
Isso pode ser feito na guia Centros de trabalho > Administração de dispositivo > Identidades > Usuários.

Procedimento

- 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.



Criar usuário local 1-2



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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for managing Policy Sets. The table below represents the data shown in the interface:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	DNAC - Policy		DEVICE Device Type EQUALS All Device Types#DNAC-Servers	Default Network Access	0		>
●	Default	Default policy set		Default Network Access	0		>

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.

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.

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

Search

DNAC - Policy DEVICE Device Type EQUALS All Device Types#DNAC Default Device Admin

> Authentication Policy(2)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
v Authorization Policy(1)

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
+	Super Admin	IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN	Select from list	SUPER_ADMIN_ROLE	0	+
+	Network Admin	IdentityGroup-Name EQUALS User Identity Groups:NETWORK-ADMIN	Select from list	NETWORK_ADMIN_ROLE	0	+
+	SecOps	IdentityGroup-Name EQUALS User Identity Groups:SecOps	Select from list	SecOps_Role	0	+
+	Default		DenyAllCommands	Deny All Shell Profile	0	+

Reset 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 System / Users & Roles

User Management
Role Based Access Control
External Authentication

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 DNA Center is the 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 DNA Center.

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 list. A sample configuration 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".

Enable External User

AAA Attribute
Cisco-AVPair

Reset to Default Update

AAA Server(s)

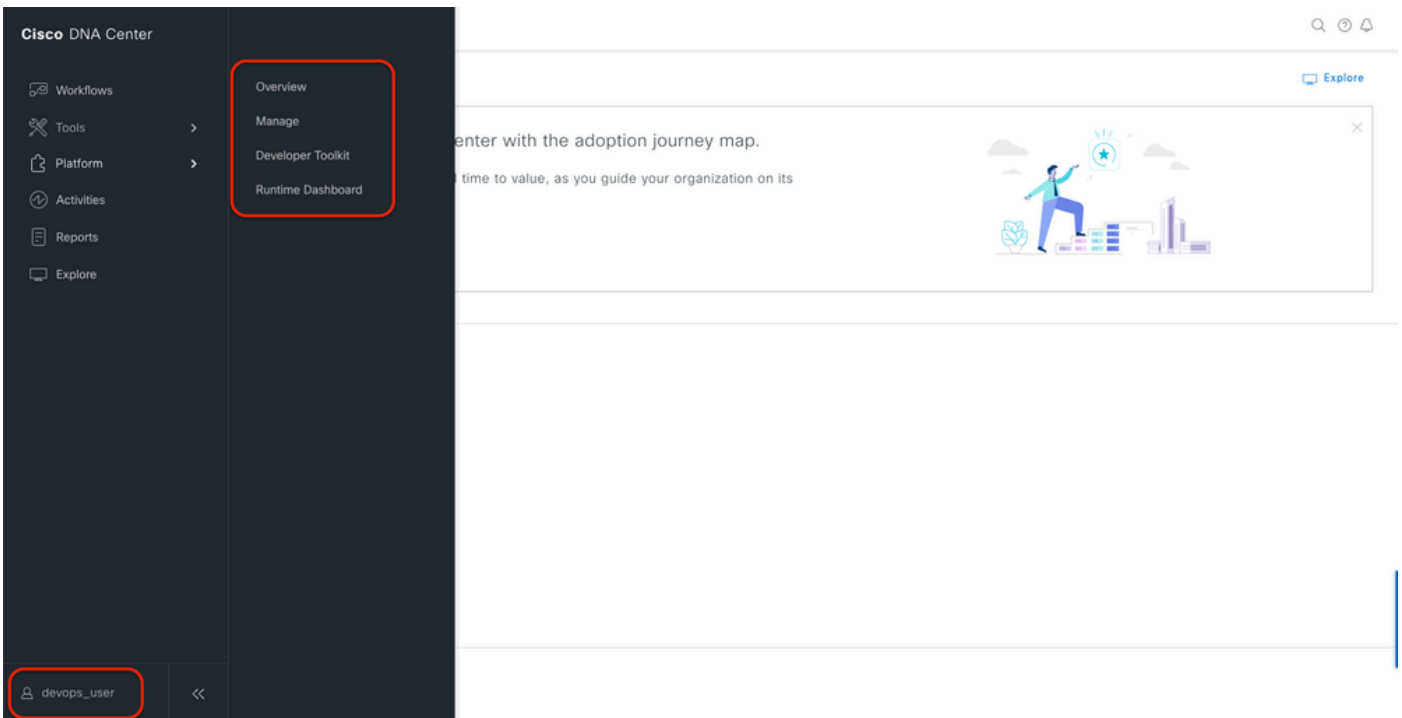
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

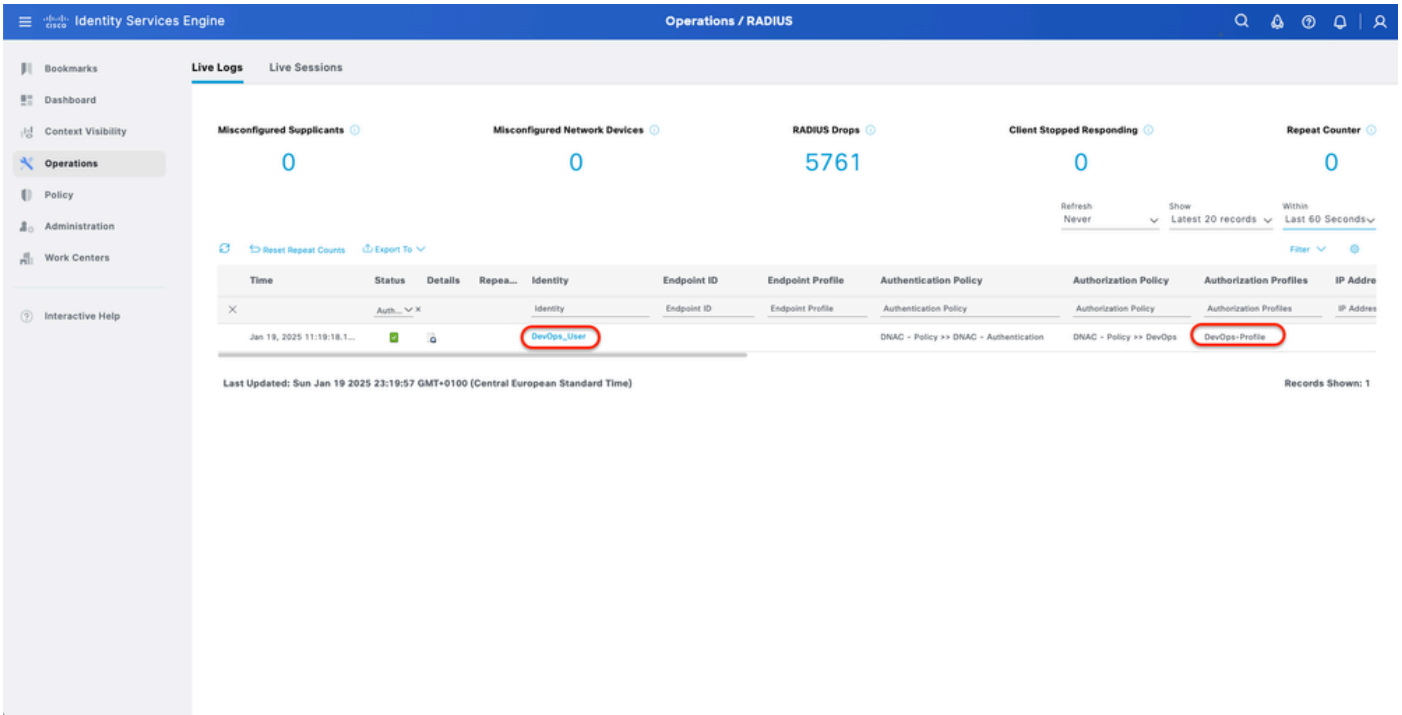
Usuários externos

2. DNAC - Confirmar acesso do usuário.



Acesso de usuário limitado

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



Registros ao vivo RADIUS

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

Cisco ISE

Overview

Event: 5200 Authentication succeeded

Username: DevOps_User

Endpoint Id:

Endpoint Profile:

Authentication Policy: DNAC - Policy >> DNAC - Authentication

Authorization Policy: DNAC - Policy >> DevOps

Authorization Result: DevOps-Profile

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

Authentication Details

Source Timestamp: 2025-01-19 23:19:18.156

Received Timestamp: 2025-01-19 23:19:18.156

Policy Server: ise34

Event: 5200 Authentication succeeded

Username: DevOps_User

User Type: User

Authentication Identity Store: Internal Users

Identity Group: User Identity Groups:DevOps

Authentication Method: PAP_ASCII

Authentication Protocol: PAP_ASCII

Network Device: DNAC

Device Type: All Device Types#DNAC-Servers

Location: All Locations

Registros ao vivo detalhados do RADIUS 1-2

Cisco ISE

IdentityPolicyMatchedRule: DNAC - Authentication

AuthorizationPolicyMatchedRule: DevOps

ISEPolicySetName: DNAC - Policy

IdentitySelectionMatchedRule: DNAC - Authentication

TotalAuthnLatency: 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: 0a301105095d4kCbV7kMBCoFkesRrFcdXec0uEqPP8RtG/WY

CiscoAVPair: AuthenticationIdentityStore=Internal Users, FQSubjectName=92731e30-8c01-11e6-996c-525400b48521#devops_user, UniqueSubjectID=9b4d28083db66a1f8bcc98565c8f5eaa5dedf467

Result

Class: CACS:0a301105095d4kCbV7kMBCoFkesRrFcdXec0uEqPP8RtG/WY:ise34/528427220/15433

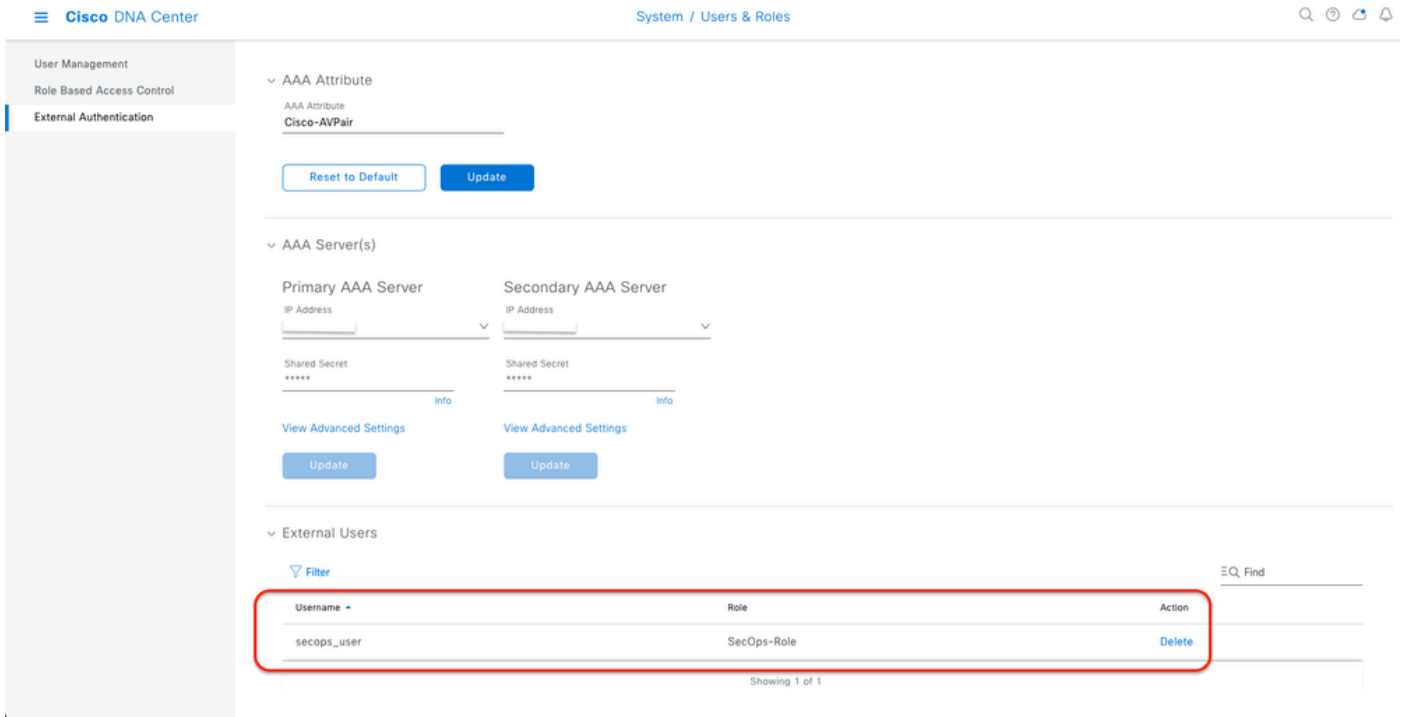
cisco-av-pair ROLE=DevOps-Role

Registros ao vivo detalhados do RADIUS 2-2

Verificar a configuração TACACS+

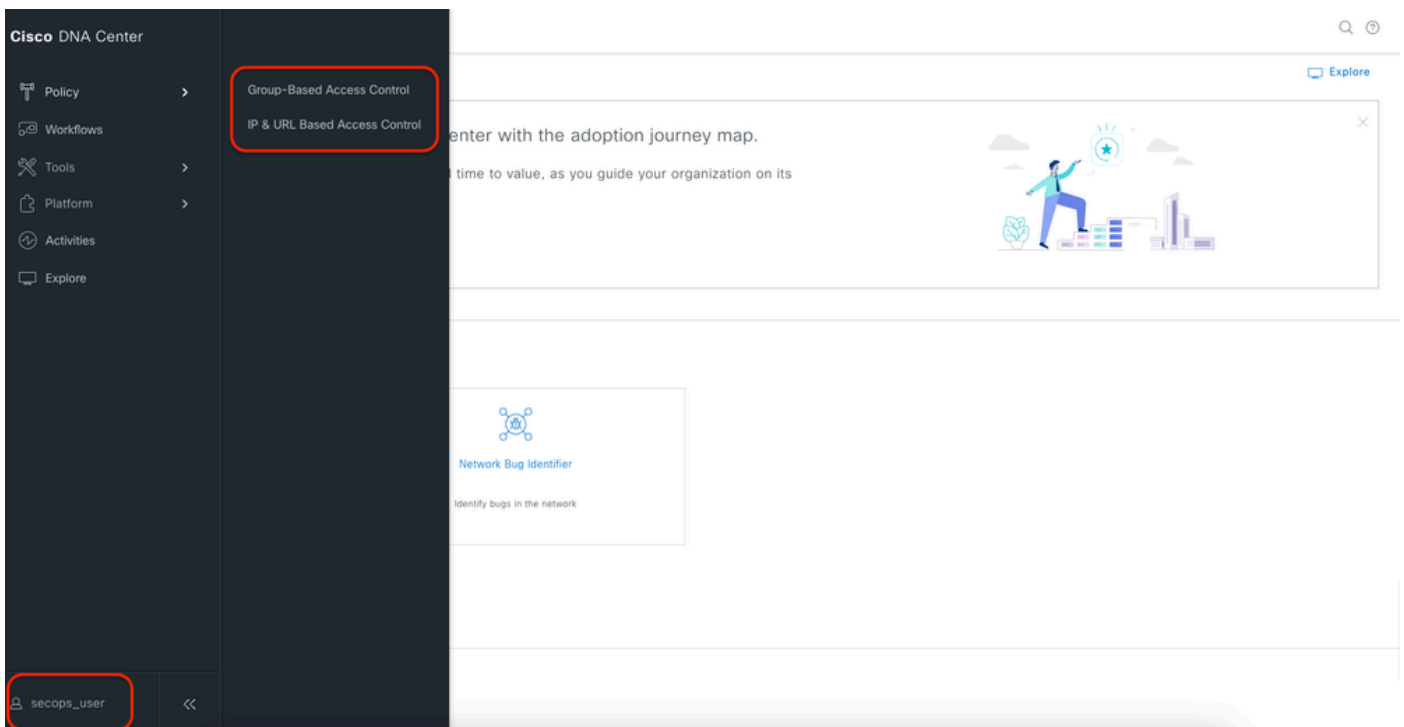
1- DNAC - Exibir Sistema de Usuários Externos > Usuários e Funções > Autenticação Externa > Usuários Externos.

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.



Usuários externos

2. DNAC - Confirmar acesso do usuário.



Acesso de usuário limitado

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

Identity Services Engine Operations / TACACS

Live Logs

Refresh Never Show Latest 20 records Within Last 60 Seconds

Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Shell Profile	Device Type	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authorization		DNAC - Policy >> SecOps	SecOps_Role	Device Type#AII Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#AII Device Types#DNAC...	Lo

Last Updated: Sun Jan 19 2025 17:16:38 GMT+0100 (Central European Standard Time) Records Shown: 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

Overview

Request Type: Authorization

Status: Pass

Session Key: ise34/526427220/13958

Message Text: Device-Administration: Session Authorization succeeded

Username: SecOps_User

Authorization Policy: DNAC - Policy >> SecOps

Shell Profile: SecOps_Role

Matched Command Set

Command From Device

Steps

Step ID	Description	Latency (ms)
13005	Received TACACS+ Authorization Request	
15049	Evaluating Policy Group	1
15008	Evaluating Service Selection Policy	1
15048	Queried PIP - DEVICE.Device Type	4
15041	Evaluating Identity Policy	7
15013	Selected Identity Source - Internal Users	5
24210	Looking up User in Internal Users IDStore	1
24212	Found User in Internal Users IDStore	4
22037	Authentication Passed	0
15036	Evaluating Authorization Policy	0
15048	Queried PIP - Network Access.UserName	10
15048	Queried PIP - IdentityGroup.Name	2
15017	Selected Shell Profile	2
22081	Max sessions policy passed	1
22080	New accounting session created in Session cache	0
13034	Returned TACACS+ Authorization Reply	0

Authorization Details

Generated Time: 2025-01-19 17:12:43.368 +1:00

Logged Time: 2025-01-19 17:12:43.368

Epoch Time (sec): 1737303163

ISE 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

Type	Value
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
SelectedAuthenticationIdentityStores	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;13=1;14=0;15=0
TotalAuthnLatency	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

- [Guia do Administrador do Cisco Identity Services Engine, Versão 3.4 > Administração de Dispositivos](#)
- [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.