

Configuración de ISE como autenticación externa para la GUI de DNAC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antes de comenzar](#)

[Configurar](#)

[\(Opción 1\) Configuración de la autenticación externa de DNAC mediante RADIUS](#)

[\(Opción 1\) Configuración de ISE para RADIUS](#)

[\(Opción 2\) Configuración de la autenticación externa de DNAC mediante TACACS+](#)

[\(Opción 2\) Configuración de ISE para TACACS+](#)

[Verificación](#)

[Verificar configuración RADIUS](#)

[Verificar configuración de TACACS+](#)

[Troubleshoot](#)

[Referencias](#)

Introducción

Este documento describe cómo configurar Cisco Identity Services Engine (ISE) como una autenticación externa para la administración GUI de Cisco DNA Center.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Protocolos TACACS+ y RADIUS.
- Integración de Cisco ISE con Cisco DNA Center.
- Evaluación de políticas de Cisco ISE.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.


- Parche 1 de Cisco Identity Services Engine (ISE) versión 3.4.

- Cisco DNA Center versión 2.3.5.5.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de comenzar

- Asegúrese de tener al menos un servidor de autenticación RADIUS configurado en System > Settings > External Services > Authentication and Policy Servers.
- Solo un usuario con permisos SUPER-ADMIN-ROLE en DNAC puede realizar este procedimiento.
- Active la reserva de autenticación externa.

 **Precaución:** En las versiones anteriores a la 2.1.x, cuando se habilita la autenticación externa, Cisco DNA Center recurre a los usuarios locales si el servidor AAA es inalcanzable o el servidor AAA rechaza un nombre de usuario desconocido. En la versión actual, Cisco DNA Center no recurre a los usuarios locales si el servidor AAA es inalcanzable o el servidor AAA rechaza un nombre de usuario desconocido. Cuando la reserva de autenticación externa está habilitada, los usuarios externos y los administradores locales pueden iniciar sesión en Cisco DNA Center.

Para habilitar la reserva de autenticación externa, conecte SSH a la instancia del Cisco DNA Center e ingrese el comando this CLI (`magctl rbac external_auth_fallback enable`).

Configurar

(Opción 1) Configuración de la autenticación externa de DNAC mediante RADIUS

Paso 1. (Opcional) Definir un rol personalizado.

Configure las funciones personalizadas que satisfagan sus requisitos; en su lugar, puede utilizar las funciones de usuario predeterminadas. Esto se puede hacer desde la pestaña System > Users & Roles > Role Based Access Control.

Procedimiento

- a. Crear un nuevo rol.

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)

2

Next

Nombre de rol de DevOps

b. Defina el acceso.

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

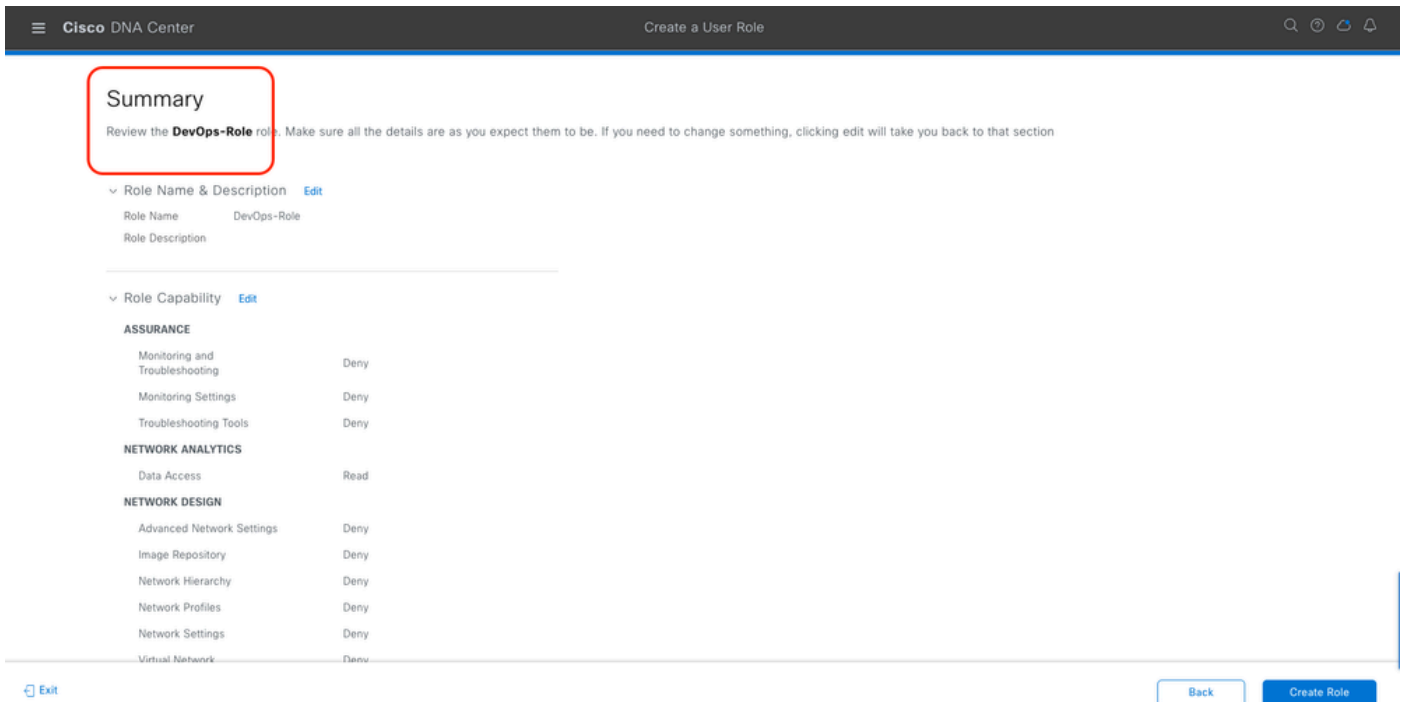
Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/> 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.

2

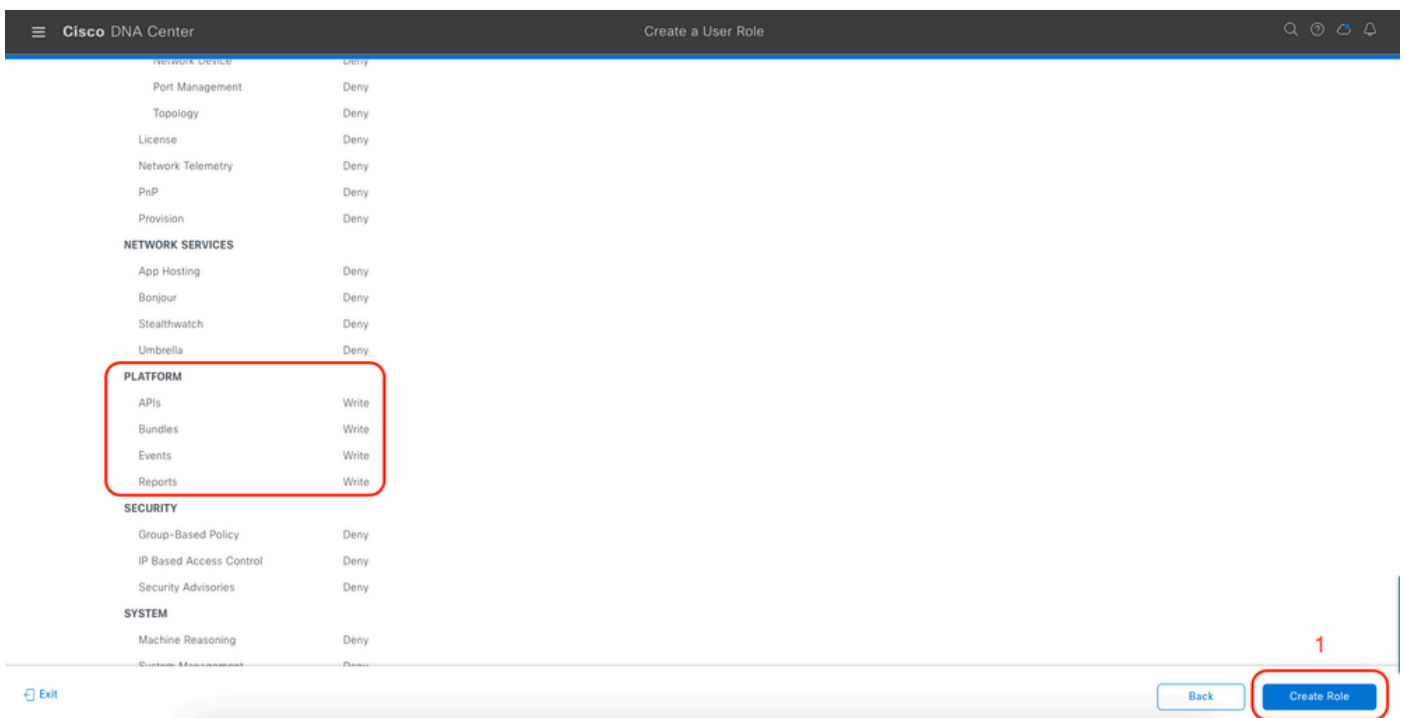
Next

Acceso a roles de DevOps

c. Cree el nuevo rol.



Resumen de funciones de DevOps



Revisar y crear rol de DevOps

Paso 2. Configure la autenticación externa usando RADIUS.
Esto se puede hacer desde la pestaña System > Users & Roles > External Authentication.

Procedimiento

a. Para habilitar la autenticación externa en Cisco DNA Center, marque la casilla de verificación Enable External User.

b. Establezca los atributos AAA.

Ingrese Cisco-AVPair en el campo AAA attributes.

c. (Opcional) Configure el Servidor AAA Principal y Secundario.

Asegúrese de que el protocolo RADIUS esté habilitado en el Servidor AAA Primario al menos, o en ambos servidores, el Primario y el Secundario.

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles' and 'External Authentication'. The left sidebar shows 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area has a heading 'External Authentication' and a sub-heading 'External Authentication'. Below the heading, there is a paragraph of text explaining the purpose of the page. Below the text, there are three main sections: 1. 'Enable External User' checkbox, which is checked and highlighted with a red box and labeled 'a'. 2. 'AAA Attribute' dropdown menu, which is set to 'Cisco-AVPair' and highlighted with a red box and labeled 'b'. 3. 'AAA Server(s)' section, which is highlighted with a red box and labeled 'c'. This section contains two columns: 'Primary AAA Server' and 'Secondary AAA Server'. Each column has fields for 'IP Address', 'Shared Secret', and 'Authentication Port'. The 'IP Address' fields are set to 'ISE Server 1 IP' and 'ISE Server 2 IP'. The 'Shared Secret' fields are masked with '*****'. The 'Authentication Port' fields are set to '1812'. Below each column, there are radio buttons for 'RADIUS' (selected) and 'TACACS'. There are also 'Reset to Default' and 'Update' buttons.

(RADIUS) Pasos de Configuración de Autenticación Externa

(Opción 1) Configuración de ISE para RADIUS

Paso 1. Agregue el servidor DNAC como dispositivo de red en ISE.

Esto se puede hacer desde la pestaña Administration > Network Resources > Network Devices.

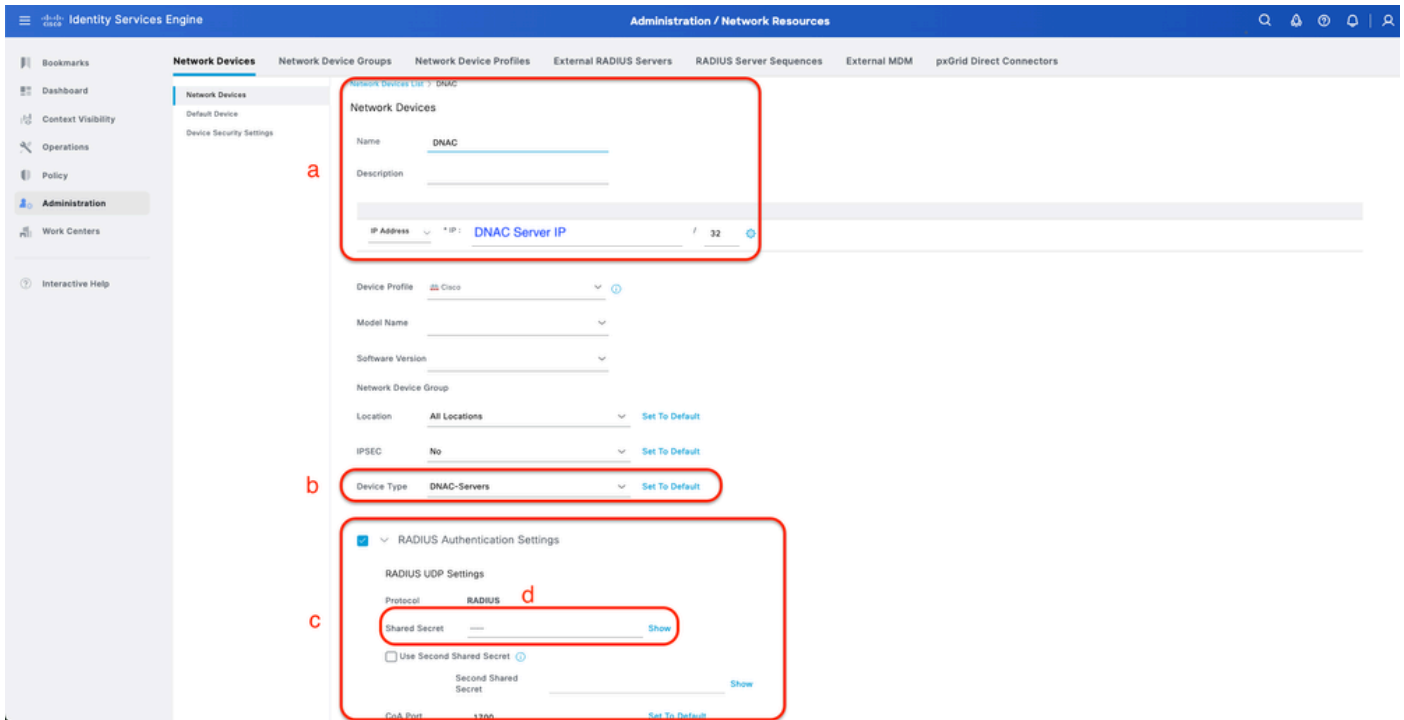
Procedimiento

a. Definir (DNAC) nombre del dispositivo de red e IP.

b. (Opcional) Clasifique el tipo de dispositivo para la condición del conjunto de políticas.

c. Active la configuración de autenticación RADIUS.

d. Establezca la clave secreta compartida RADIUS.



Dispositivo de red ISE (DNAC) para RADIUS

Paso 2. Crear perfiles de autorización RADIUS.

Esto se puede hacer desde la pestaña Política > Elementos de Política > Resultados > Autorización > Perfiles de autorización.



Nota: Cree tres perfiles de autorización RADIUS, uno para cada función de usuario.

Procedimiento

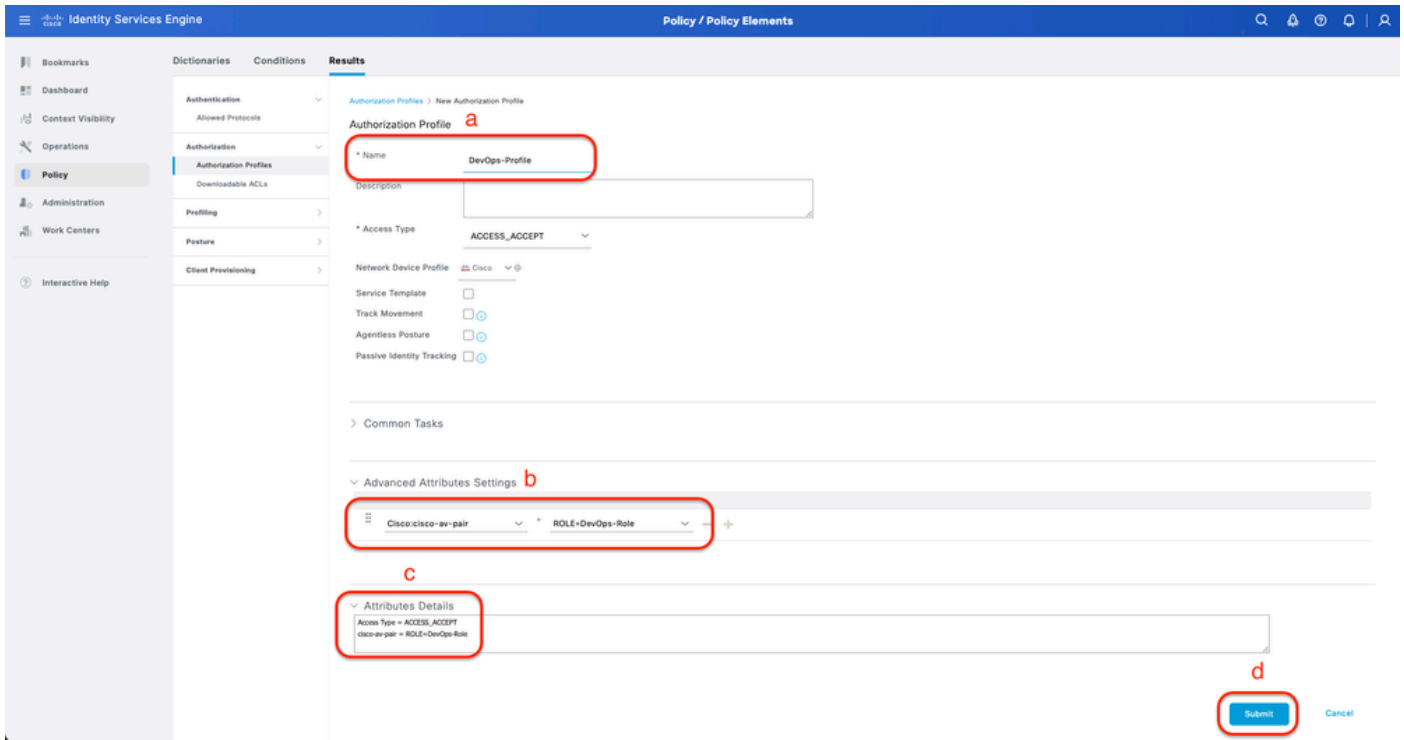
a. Haga clic en Agregar y defina el nombre del perfil de autorización RADIUS.

b. Ingrese el Cisco:cisco-av-pair en Advanced Attributes Settings y complete el rol de usuario correcto.

- Para la función de usuario (DecOps-Role), introduzca ROLE=DevOps-Role.
- Para el rol de usuario (NETWORK-ADMIN-ROLE), introduzca ROLE=NETWORK-ADMIN-ROLE.
- Para el rol de usuario (SUPER-ADMIN-ROLE), introduzca ROLE=SUPER-ADMIN-ROLE.

c. Revise los detalles del atributo.

d. Click Save.



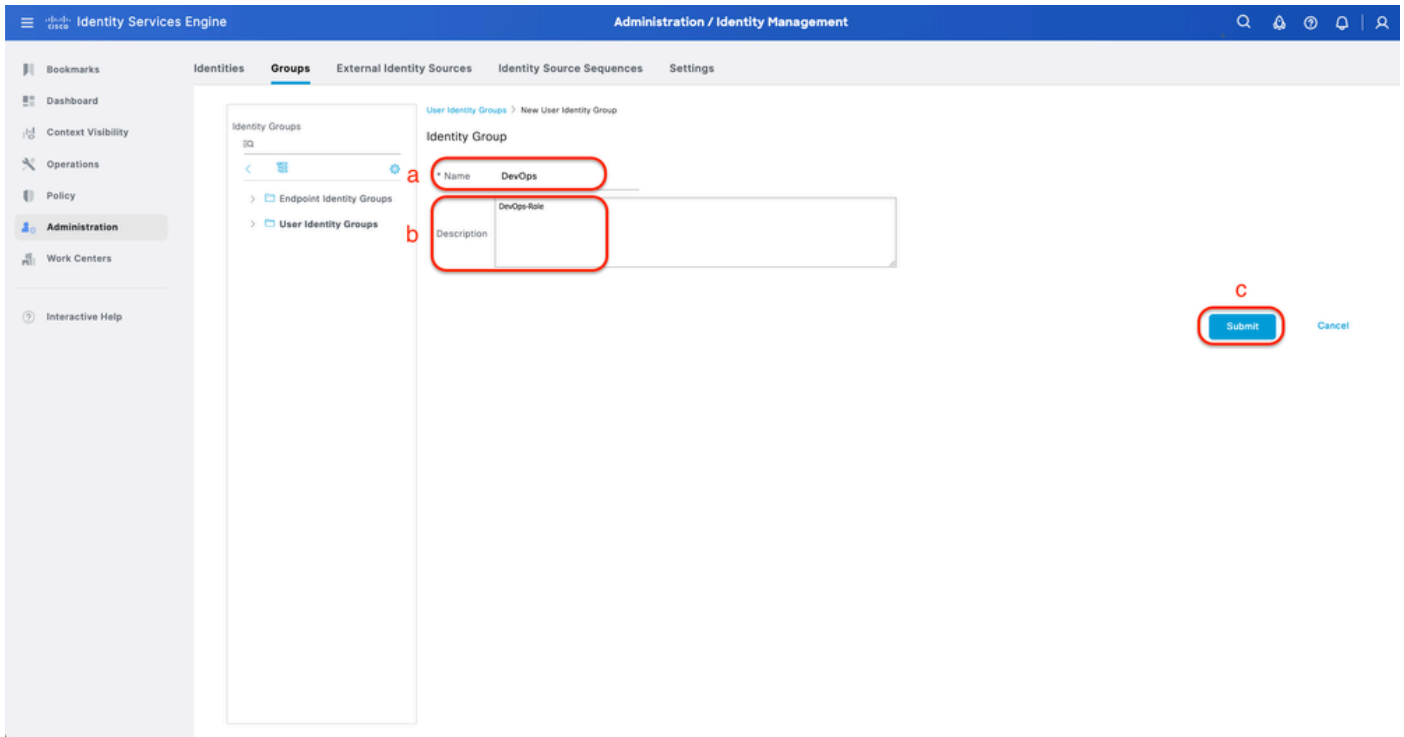
Creación del perfil de autorización

Paso 3. Crear grupo de usuarios.

Esto se puede hacer desde la pestaña Administration > Identity Management > Groups > User Identity Groups.

Procedimiento

- a. Haga clic en Agregar y defina el nombre del grupo de identidad
- b. (Opcional) Defina la descripción.
- c. Haga clic en Enviar.



Crear grupo de identidad de usuario

Paso 4. Crear usuario local.

Esto se puede hacer desde la pestaña Administration > Identity Management > Identities > Users.

Procedimiento

- a. Haga clic en Agregar y defina el nombre de usuario.
- b. Establezca la contraseña de inicio de sesión.
- c. Agregue el usuario al grupo de usuarios relacionado.
- d. Haga clic en Submit (Enviar).

Identity Services Engine Administration / Identity Management

Network Access Users List > New Network Access User

a * Username **DevOps_User**

Status Enabled

Account Name Alias

Email

b Password Re-Enter Password

* Login Password

Generate Password

Enable Password

Generate Password

Password Type: Internal Users

Password Lifetime:

With Expiration
Password will expire in **60 days**

Never Expires

User Information

First Name

Last Name

Crear usuario local 1-2

Identity Services Engine Administration / Identity Management

* Login Password

Generate Password

Enable Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

Change password on next login

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

c User Groups

DevOps

d Submit Cancel

Crear usuario local 2-2

Paso 5. (Opcional) Agregar conjunto de políticas RADIUS.

Esto se puede hacer desde la pestaña Policy > Policy Sets.

Procedimiento

a. Haga clic en Acciones y elija (Insertar nueva fila encima).

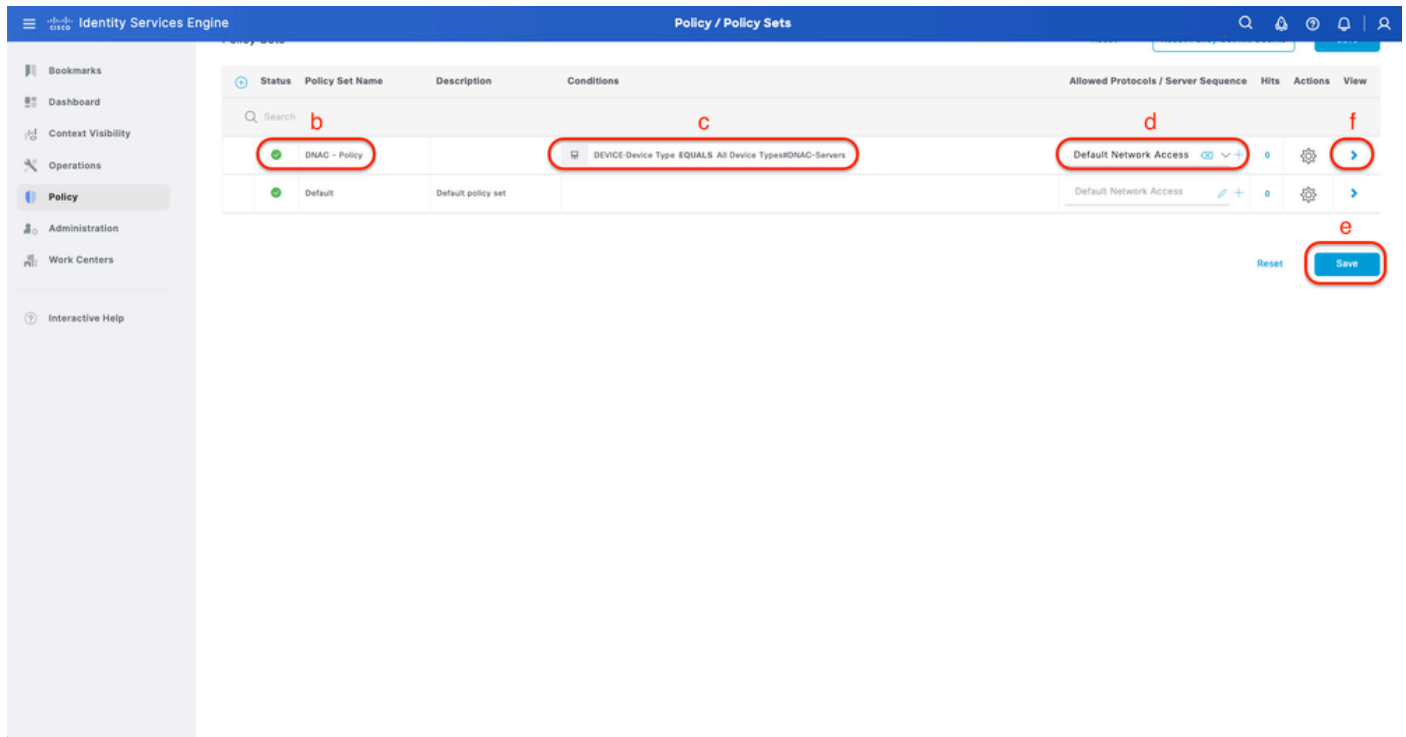
b. Defina el nombre del conjunto de políticas.

c. Establezca la Condición de Conjunto de Políticas en Seleccionar Tipo de Dispositivo que creó anteriormente en (Paso 1 > b).

d. Establezca los protocolos permitidos.

e. Click Save.

f. Haga clic en (>) Vista de conjunto de políticas para configurar las reglas de autenticación y autorización.



Agregar conjunto de directivas RADIUS

Paso 6. Configure la Política de Autenticación RADIUS.

Esto se puede hacer desde la pestaña Policy > Policy Sets > Click (>).

Procedimiento

a. Haga clic en Acciones y elija (Insertar nueva fila encima).

b. Defina el nombre de la política de autenticación.

c. Establezca la Condición de la Política de Autenticación y Seleccione el Tipo de Dispositivo que creó anteriormente en (Paso 1 > b).

d. Establezca el Uso de la política de autenticación para el origen de identidad.

e. Click Save.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The main content area shows a table of Policy Sets under the 'Authentication Policy(2)' section. The table has columns for Status, Rule Name, Conditions, Use, Hits, and Actions. The first row is 'DNAC - Authentication' with a condition 'DEVICE Device Type EQUALS All Device Types#DNAC-Servers'. The 'Use' column for this row shows 'Internal Users'. The 'Save' button at the bottom right is highlighted with a red circle labeled 'e'. Other elements are labeled with letters: 'b' on the 'DNAC - Authentication' status, 'c' on the condition, and 'd' on the 'Internal Users' dropdown.

Agregar política de autenticación RADIUS

Paso 7. Configure la Política de Autorización RADIUS.

Esto se puede hacer desde la pestaña Policy > Policy Sets> Haga clic en (>).

Siga este paso para crear una directiva de autorización para cada rol de usuario:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- DevOps-Role

Procedimiento

a. Haga clic en Acciones y elija (Insertar nueva fila encima).

b. Defina el nombre de la directiva de autorización.

c. Establezca la Condición de directiva de autorización y Seleccione el grupo de usuarios que creó en (Paso 3).

d. Establezca los Perfiles/Resultados de la Política de Autorización y Seleccione el Perfil de Autorización que creó en (Paso 2).

e. Click Save.

The screenshot displays the 'Policy / Policy Sets' configuration interface. At the top, there's a navigation bar with 'Identity Services Engine' and 'Policy / Policy Sets'. Below this, a table lists policy sets, with 'DNAC - Policy' selected. The main area shows a detailed view of an authorization policy with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. Red annotations highlight: 'b' (green status), 'c' (condition: IdentityGroup-Name EQUALS User Identity Groups:SUPER-ADMIN), 'd' (role selection dropdown: Super-Admin_Role_Pr...), 'a' (gear icon for configuration), and 'e' (Save button).

Agregar política de autorización

(Opción 2) Configuración de la autenticación externa de DNAC mediante TACACS+

Paso 1. (Opcional) Definir un rol personalizado.

Configure las funciones personalizadas que satisfagan sus requisitos; en su lugar, puede utilizar las funciones de usuario predeterminadas. Esto se puede hacer desde la pestaña System > Users & Roles > Role Based Access Control.

Procedimiento

a. Crear un nuevo rol.

Cisco DNA Center 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.

1

Role Name*

Describe the role (optional)

2

[Exit](#) [Next](#)

Nombre del rol SecOps

b. Defina el acceso.

Cisco DNA Center Create a User Role

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 **SecOps-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.

> Network Analytics	<input type="radio"/> Deny <input type="radio"/> Read <input checked="" 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 checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Open platform for accessible intent-based workflows, data exchange, notifications, and third-party app integrations.
> Security	<input type="radio"/> Deny <input type="radio"/> Read <input checked="" type="radio"/> Write	Manage and control secure access to the network.
> System	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Centralized administration of your Cisco DNA Center, which includes configuration management, network connectivity, software upgrades, and more.
> Utilities	<input checked="" type="radio"/> Deny <input checked="" type="radio"/> Read <input checked="" type="radio"/> Write	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.

2

[Exit](#) [Review](#) [Back](#) [Next](#)

Acceso a roles de SecOps

c. Cree el nuevo rol.

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](#)

Resumen de roles de 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 y crear rol de SecOps

Paso 2. Configure la autenticación externa mediante TACACS+.

Esto se puede hacer desde la pestaña System > Users & Roles > External Authentication.

a. Para habilitar la autenticación externa en Cisco DNA Center, marque la casilla de verificación Enable External User.

b. Establezca los atributos AAA.

Ingrese Cisco-AVPair en el campo AAA attributes.

c. (Opcional) Configure el Servidor AAA Principal y Secundario.

Asegúrese de que el protocolo TACACS+ esté habilitado en el Servidor AAA Primario al menos, o en ambos servidores, el Primario y el Secundario.

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, also circled in red and 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 'Port' set to '49'. The 'TACACS+' radio button is selected in both columns, circled in red and labeled 'c'. There are 'Reset to Default' and 'Update' buttons at the bottom of the configuration area.

Pasos de Configuración de Autenticación Externa (TACACS+)

(Opción 2) Configuración de ISE para TACACS+

Paso 1. Habilite Device Admin Service.

Esto se puede hacer desde la pestaña Administration > System > Deployment > Edit (ISE PSN Node) > Check Enable Device Admin Service.

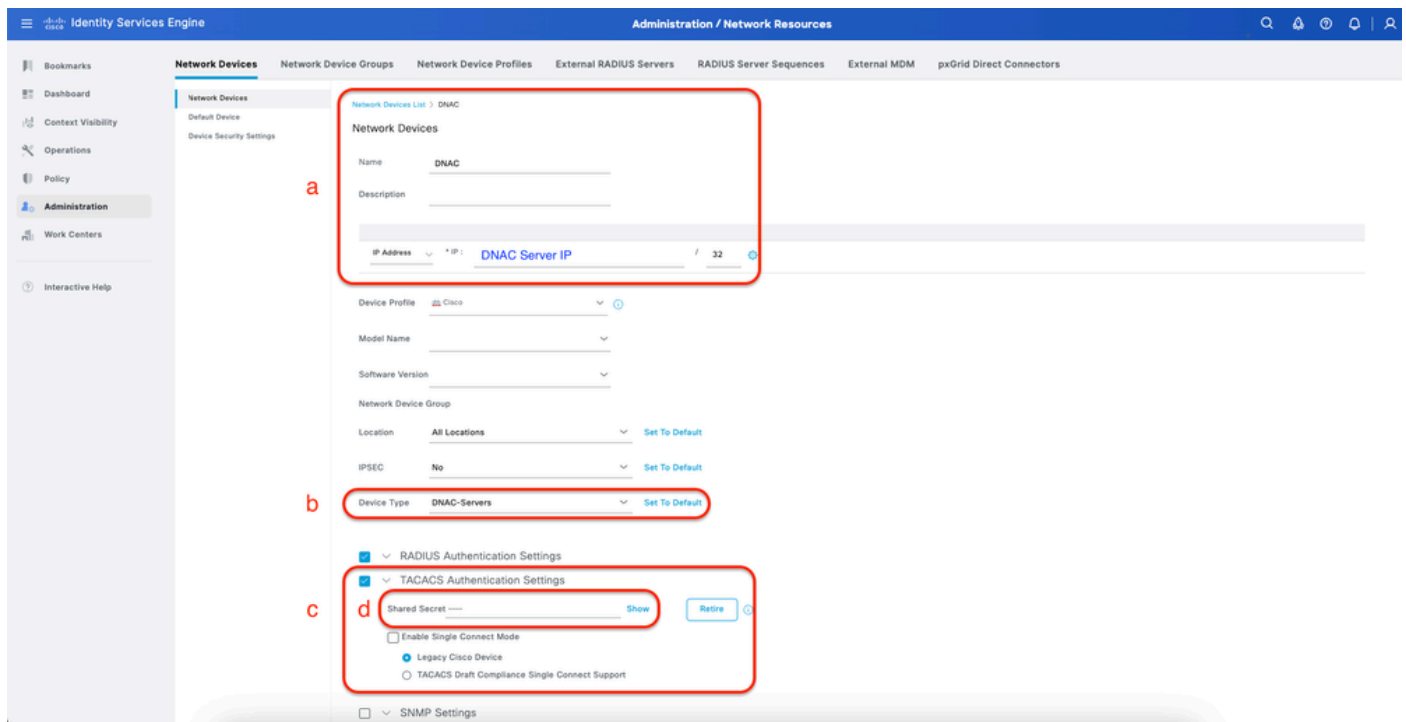
The screenshot shows the 'Administration / System' page in Identity Services Engine. The 'Deployment' tab is selected. The page displays various service configurations. The 'Administration' section is expanded, showing 'Monitoring' and 'Policy Service' sections. In the 'Policy Service' section, the 'Enable 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 'Save' button is located at the bottom right of the page, next to a 'Reset' button.

Paso 2. Agregue el servidor DNAC como dispositivo de red en ISE.

Esto se puede hacer desde la pestaña Administration > Network Resources > Network Devices.

Procedimiento

- Definir (DNAC) nombre del dispositivo de red e IP.
- (Opcional) Clasifique el tipo de dispositivo para la condición del conjunto de políticas.
- Habilitar configuración de autenticación TACACS+.
- Establecer secreto compartido TACACS+.



Dispositivo de red ISE (DNAC) para TACACS+

Paso 3. Crear perfiles TACACS+ para cada función DNAC.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS.




Nota: Cree 3 perfiles TACACS+, uno para cada función de usuario.

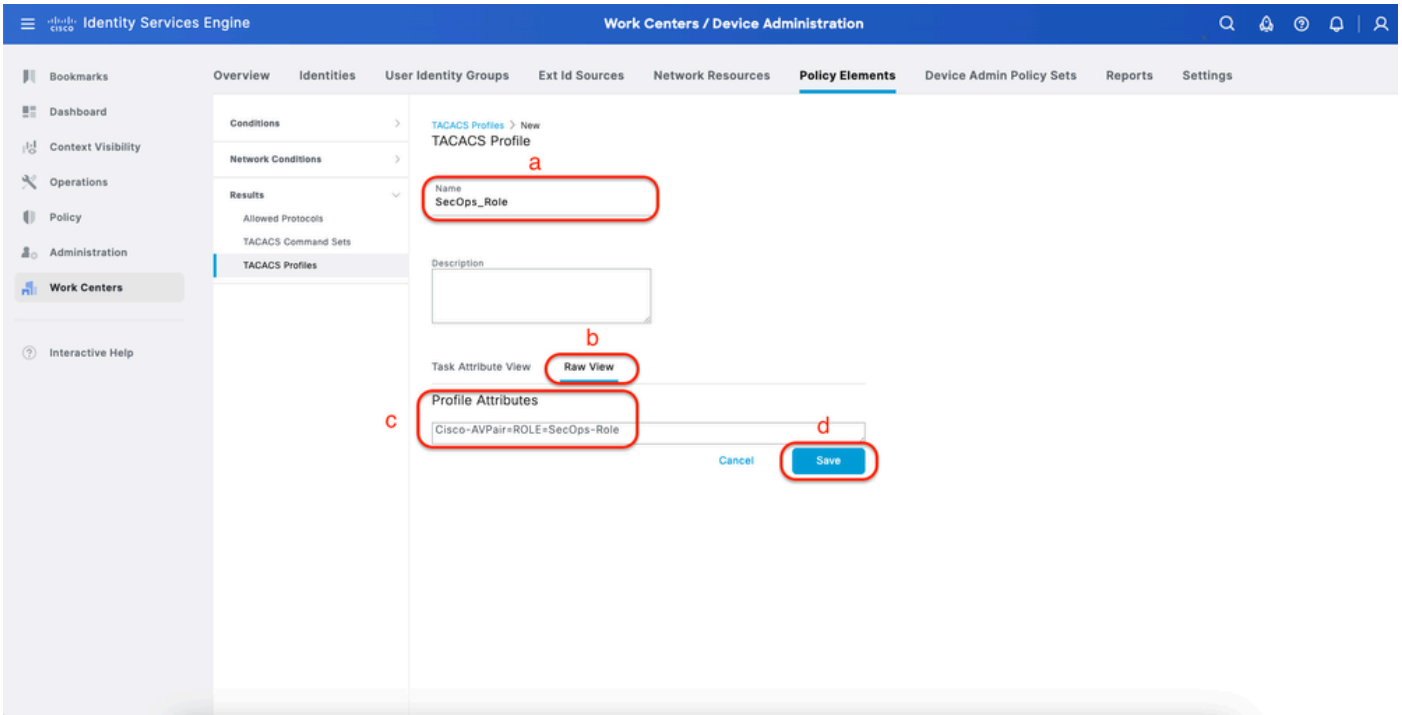
Procedimiento

- Haga clic en Agregar y defina el nombre del perfil TACACS.
- Haga clic en la pestaña Vista sin procesar.
- Ingrese Cisco-AVPair=ROLE= y complete el rol de usuario correcto.
 - Para la función de usuario (SecOps-Role), introduzca Cisco-AVPair=ROLE=SecOps-Role.

- Para el rol de usuario (NETWORK-ADMIN-ROLE), introduzca Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE.
- Para el rol de usuario (SUPER-ADMIN-ROLE), introduzca Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE.

 Nota: Recuerde que el valor de AVPair (Cisco-AVPair=ROLE=) distingue entre mayúsculas y minúsculas y asegúrese de que coincide con el rol de usuario de DNAC.

d. Click Save.



The screenshot shows the 'TACACS Profile' configuration page in the Identity Services Engine. The page is titled 'TACACS Profile' and has a breadcrumb trail 'TACACS Profiles > New'. The main content area contains the following fields and controls:

- Name:** SecOps_Role (highlighted with a red box 'a')
- Description:** (empty text box)
- Task Attribute View:** Raw View (highlighted with a red box 'b')
- Profile Attributes:** Cisco-AVPair=ROLE=SecOps-Role (highlighted with a red box 'c')
- Buttons:** Cancel and Save (the Save button is highlighted with a red box 'd')

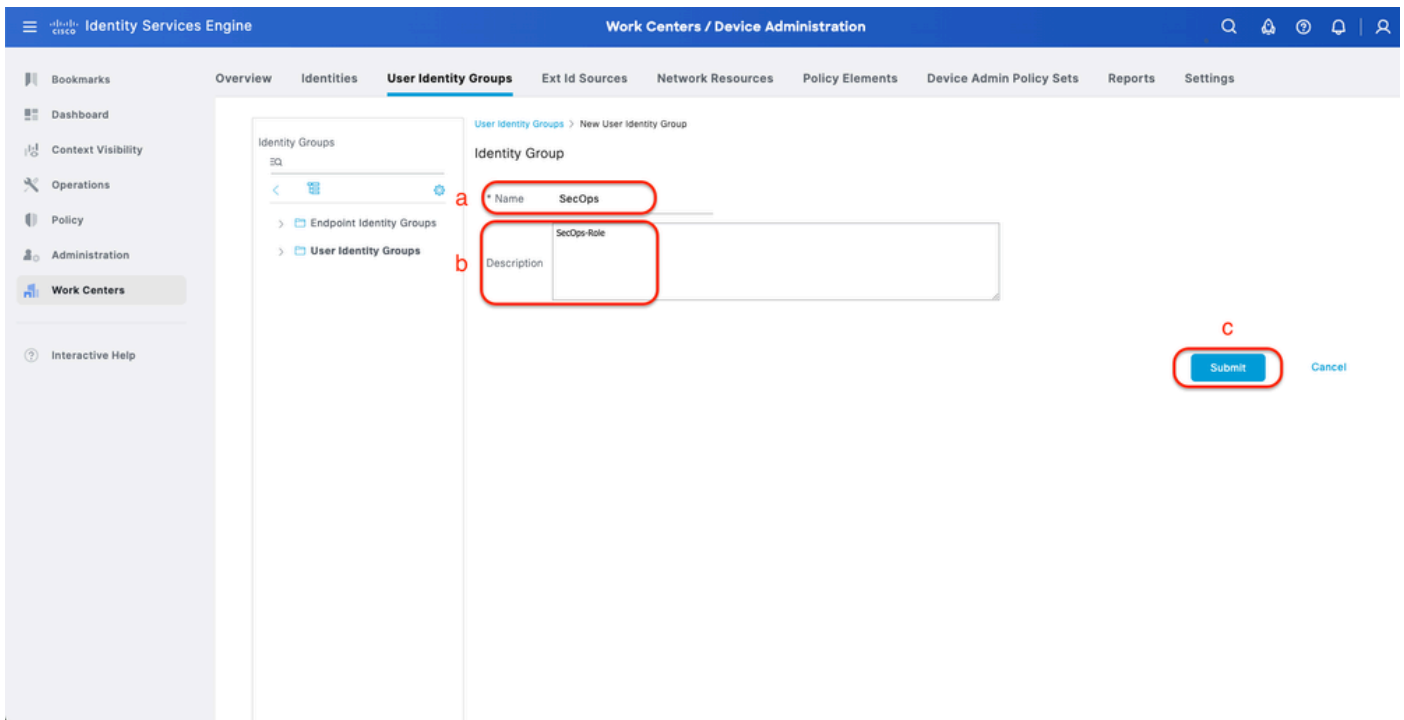
Crear perfil TACACS (SecOps_Role)

Paso 4. Crear grupo de usuarios.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Grupos de identidades de usuarios.

Procedimiento

- Haga clic en Agregar y defina el nombre del grupo de identidad.
- (Opcional) Defina la descripción.
- Haga clic en Enviar.



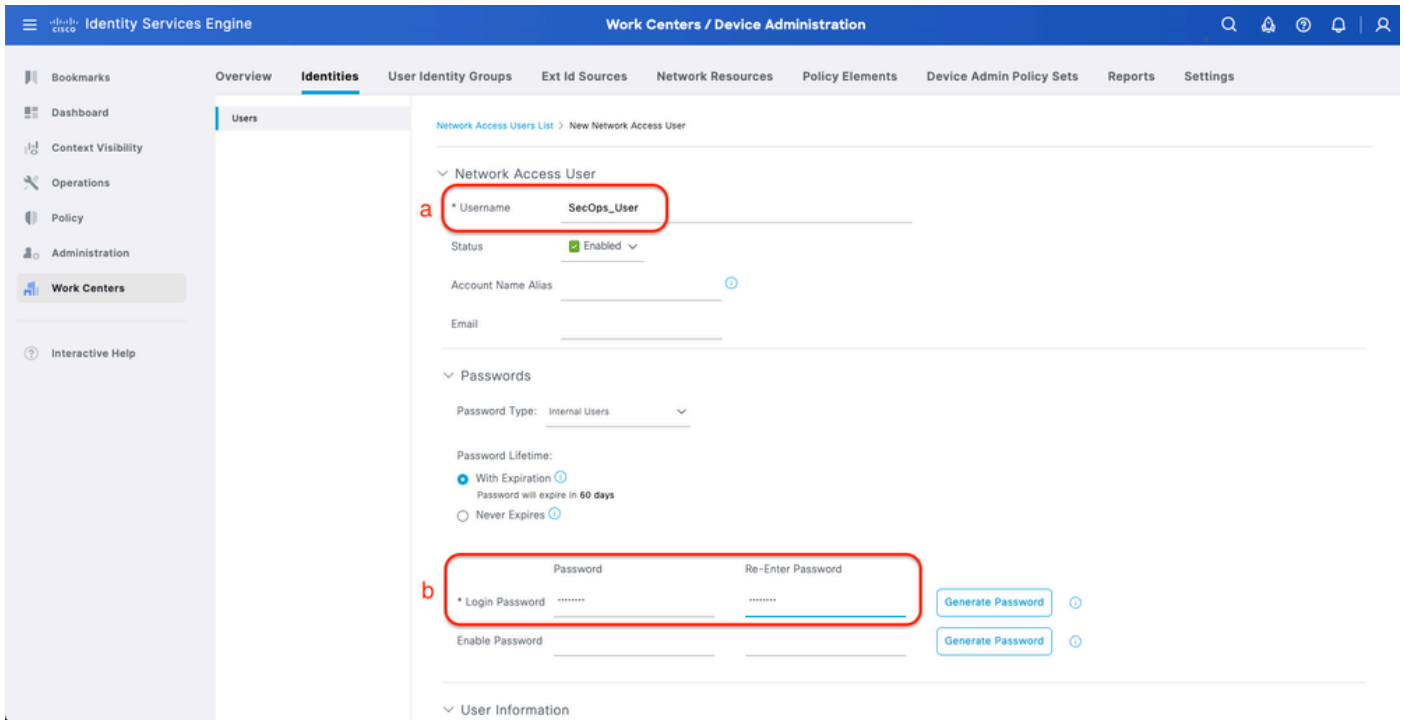
Crear grupo de identidad de usuario

Paso 5. Crear usuario local.

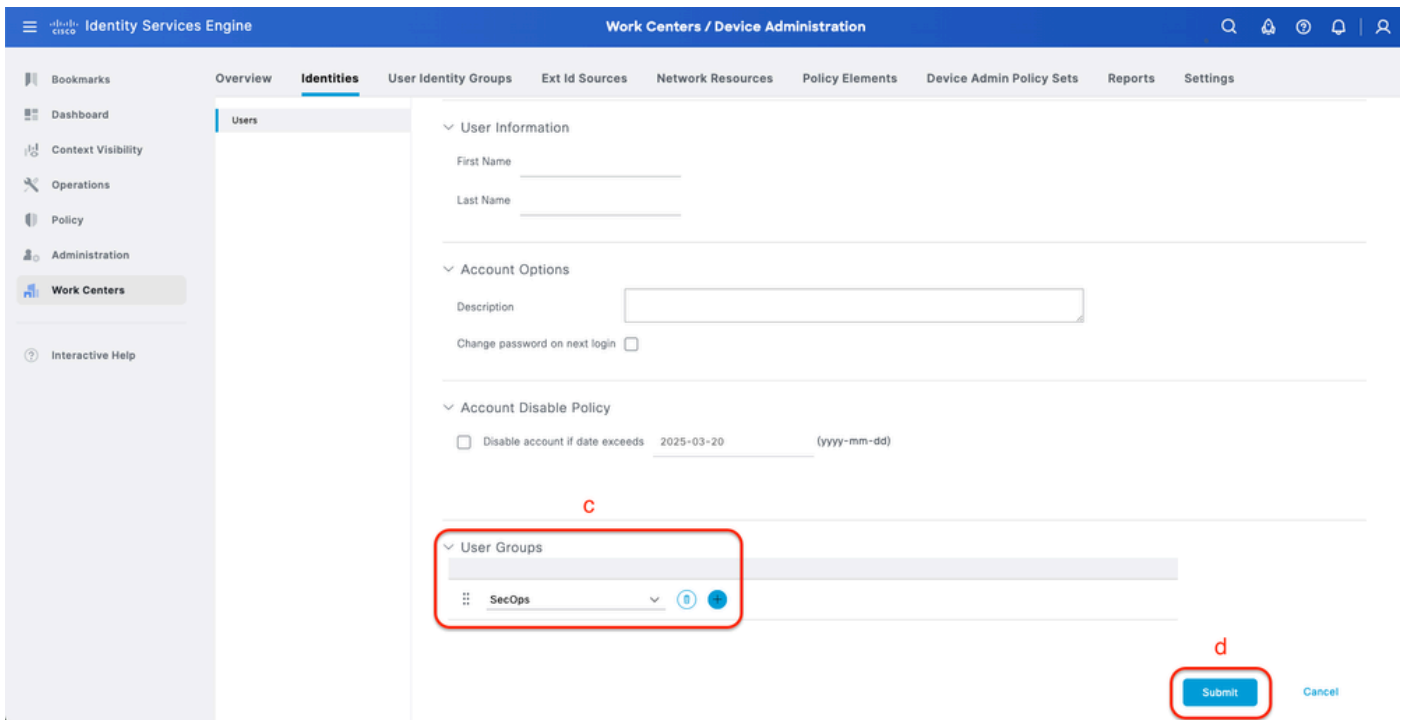
Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Identidades > Usuarios.

Procedimiento

- a. Haga clic en Agregar y defina el nombre de usuario.
- b. Establezca la contraseña de inicio de sesión.
- c. Agregue el usuario al grupo de usuarios relacionado.
- d. Haga clic en Submit (Enviar).



Crear usuario local 1-2



Crear usuario local 2-2

Paso 6. (Opcional) Agregar conjunto de políticas TACACS+.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos.

Procedimiento

a. Haga clic en Acciones y elija (Insertar nueva fila encima).

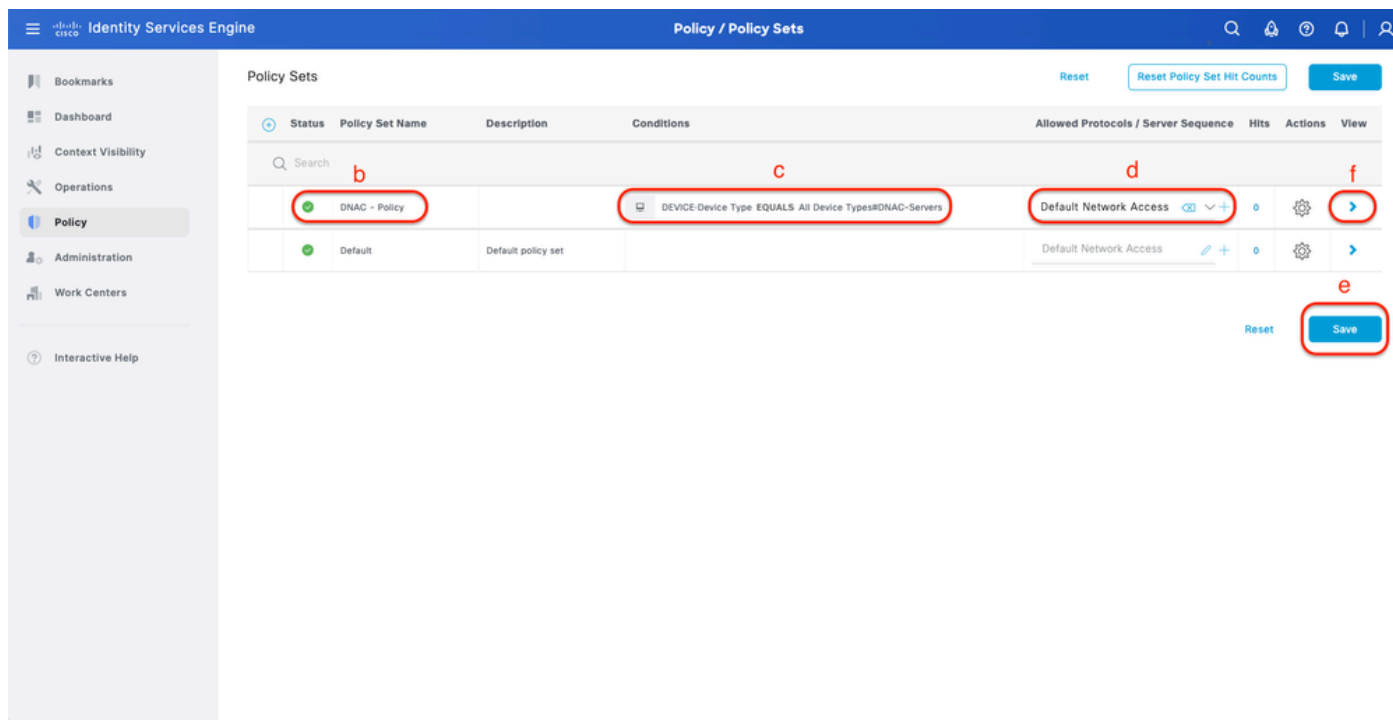
b. Defina el nombre del conjunto de políticas.

c. Establezca la Condición de Conjunto de Políticas en Seleccionar Tipo de Dispositivo que creó anteriormente en (Paso 2 > b).

d. Establezca los protocolos permitidos.

e. Click Save.

f. Haga clic en (>) Vista de conjunto de políticas para configurar las reglas de autenticación y autorización.



Agregar conjunto de políticas TACACS+

Paso 7. Configure la Política de Autenticación de TACACS+.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos > Haga clic en (>).

Procedimiento

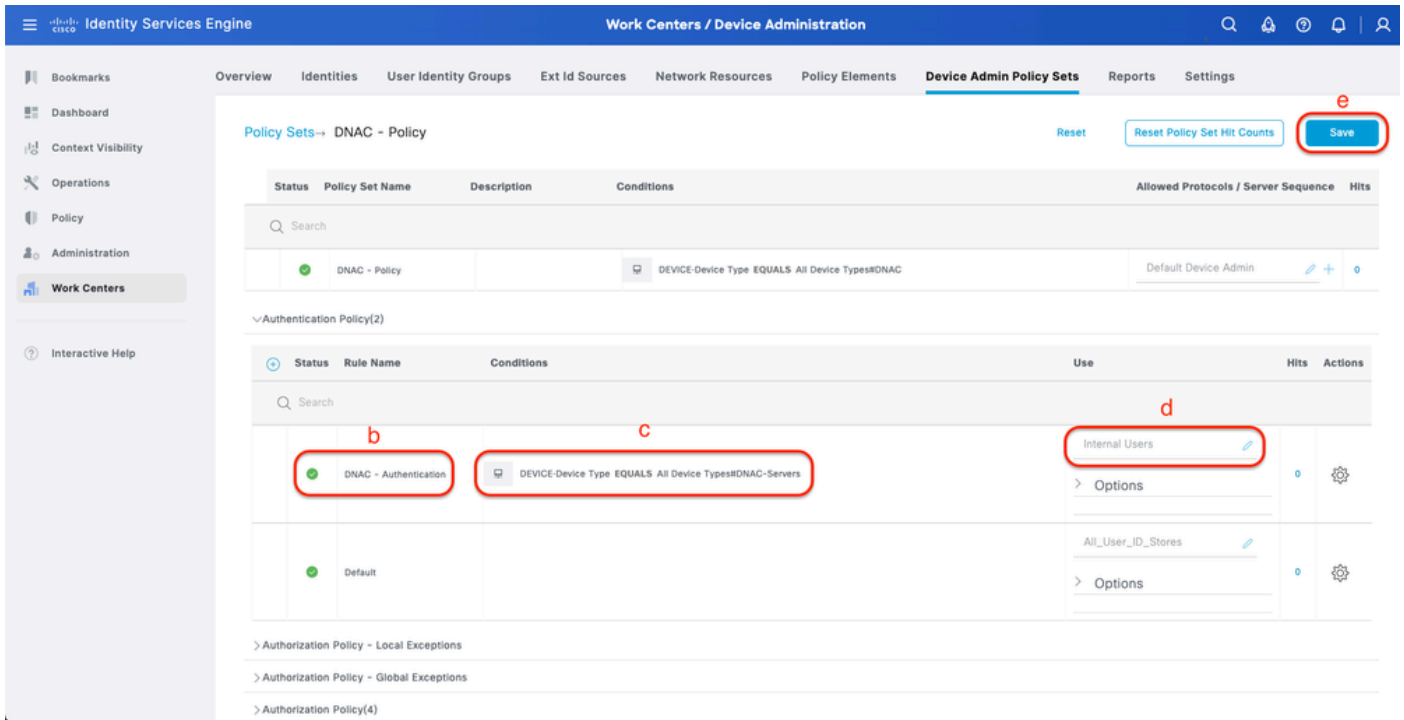
a. Haga clic en Acciones y elija (Insertar nueva fila encima).

b. Defina el nombre de la política de autenticación.

c. Establezca la Condición de Política de Autenticación y Seleccione el Tipo de Dispositivo que creó anteriormente en (Paso 2 > b).

d. Establezca el Uso de la política de autenticación para el origen de identidad.

e. Click Save.



Agregar política de autenticación TACACS+

Paso 8. Configure la Política de Autorización de TACACS+.

Esto se puede hacer desde la pestaña Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos > Haga clic en (>).

Siga este paso para crear una directiva de autorización para cada rol de usuario:

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- SecOps-Role

Procedimiento

a. Haga clic en Acciones y elija (Insertar nueva fila encima).

b. Defina el nombre de la directiva de autorización.

c. Establezca la Condición de Política de Autorización y Seleccione el Grupo de Usuarios que creó en (Paso 4).

d. Establezca los perfiles de shell de política de autorización y seleccione el perfil TACACS que creó en (Paso 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**

Agregar política de autorización

Verificación

Verificar configuración RADIUS

1- DNAC - Mostrar usuarios externos Sistema > Usuarios y funciones > Autenticación externa > Usuarios externos.

Puede ver la lista de usuarios externos que han iniciado sesión a través de RADIUS por primera vez. La información que se muestra incluye sus nombres de usuario y roles.

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)

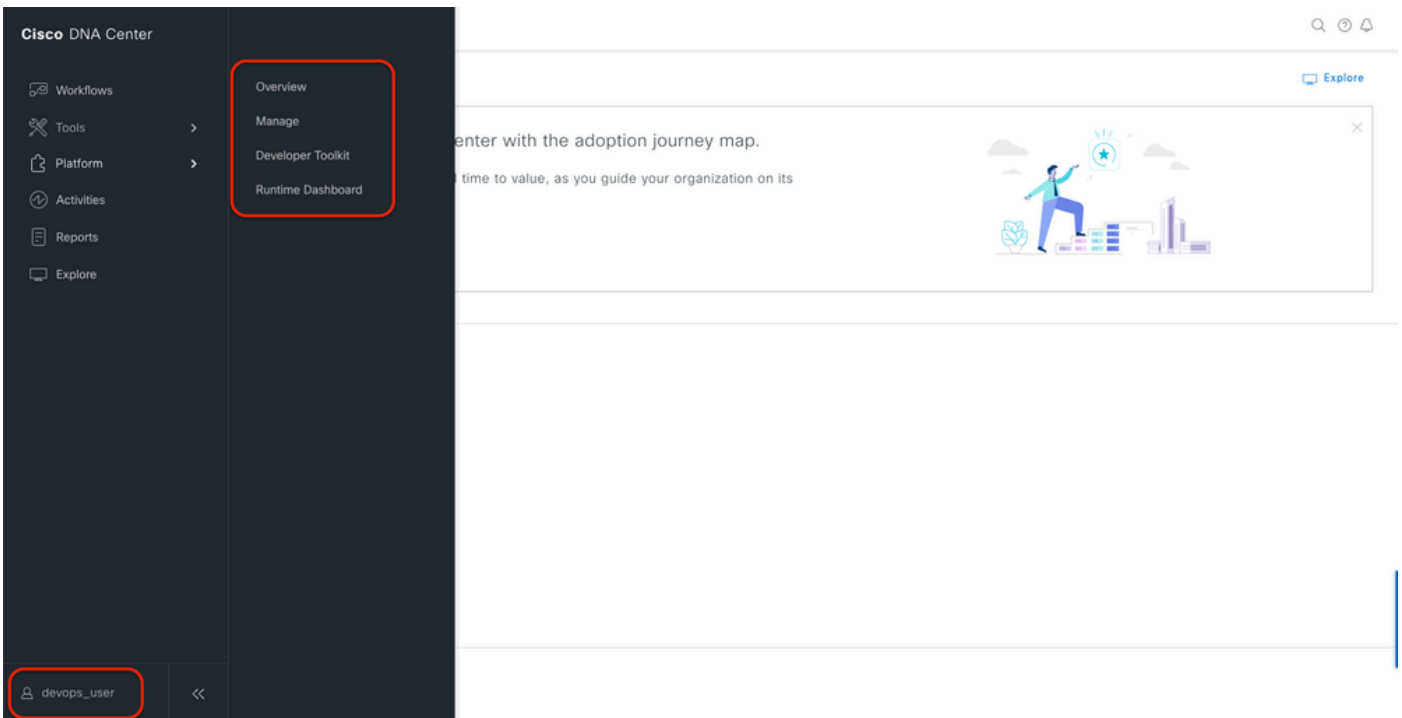
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

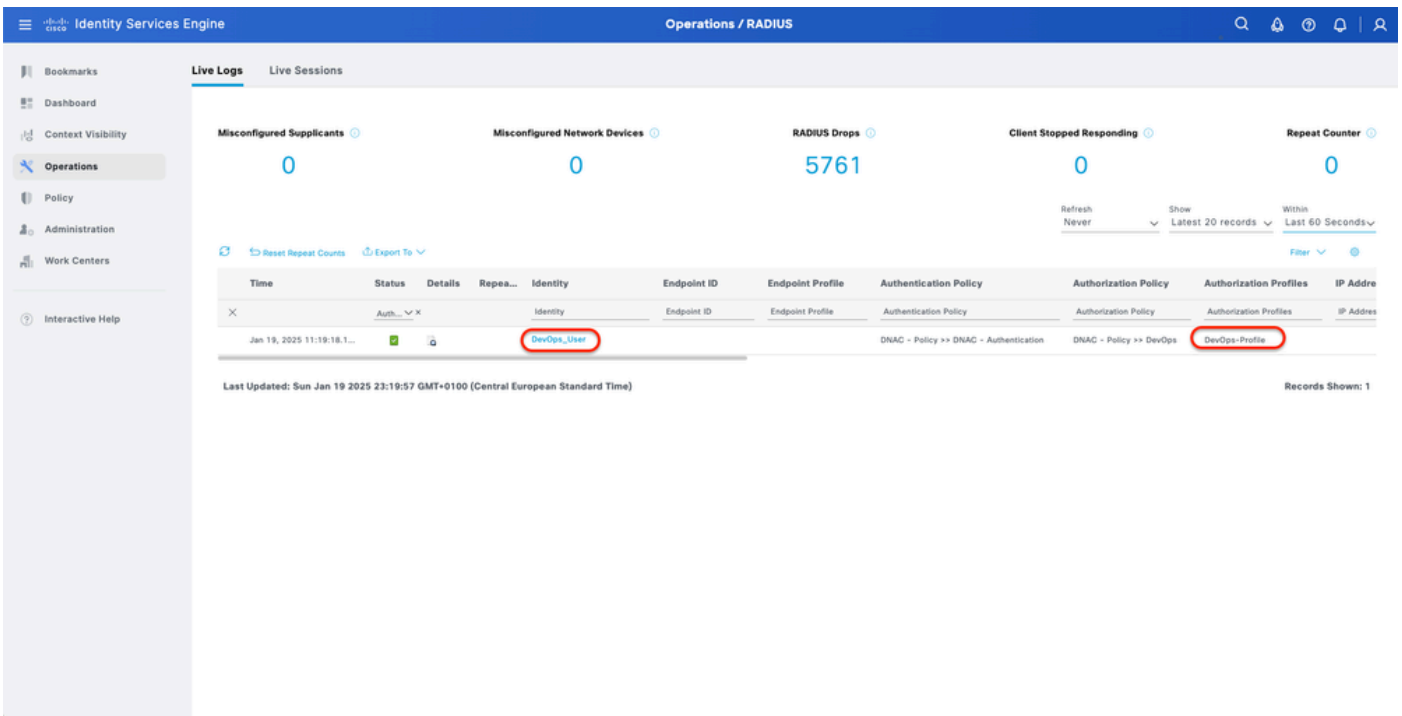
Usuarios externos

2. DNAC - Confirmar el acceso del usuario.



Acceso de usuario limitado

3.a ISE - Operaciones de Live-Logs de RADIUS > RADIUS > Live-Logs.



Registros en directo de RADIUS

3.b ISE - Operaciones de Live-Logs de RADIUS > RADIUS > Live-Logs > Haga clic (Detalles) para el registro de autorización.

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 en directo detallados de 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: 0a301105o95d4kCbv7kMBCoFkesRrFcdXec0uEqPP8RtG/WY

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

Result

Class: CACS:0a301105o95d4kCbv7kMBCoFkesRrFcdXec0uEqPP8RtG/WY:ise34/528427220/15433

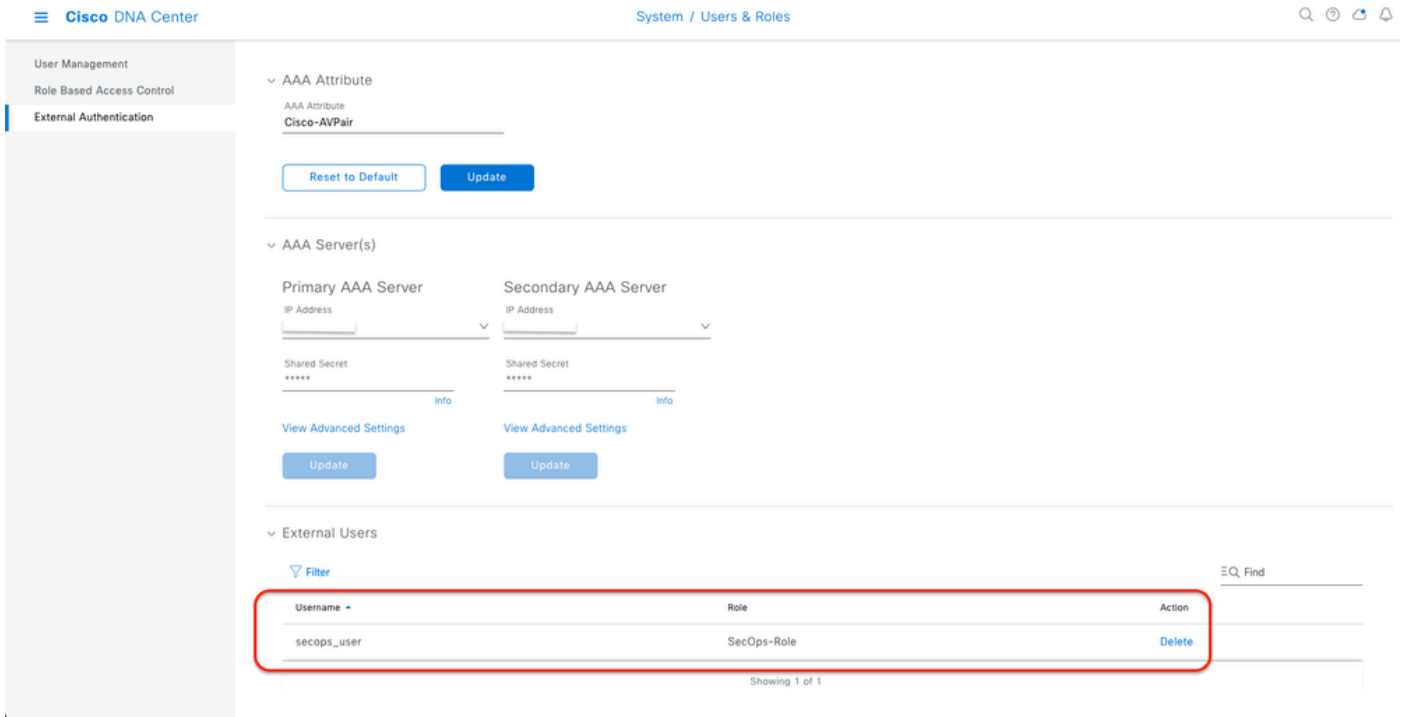
cisco-av-pair: ROLE=DevOps-Role

Registros en directo detallados de RADIUS 2-2

Verificar configuración de TACACS+

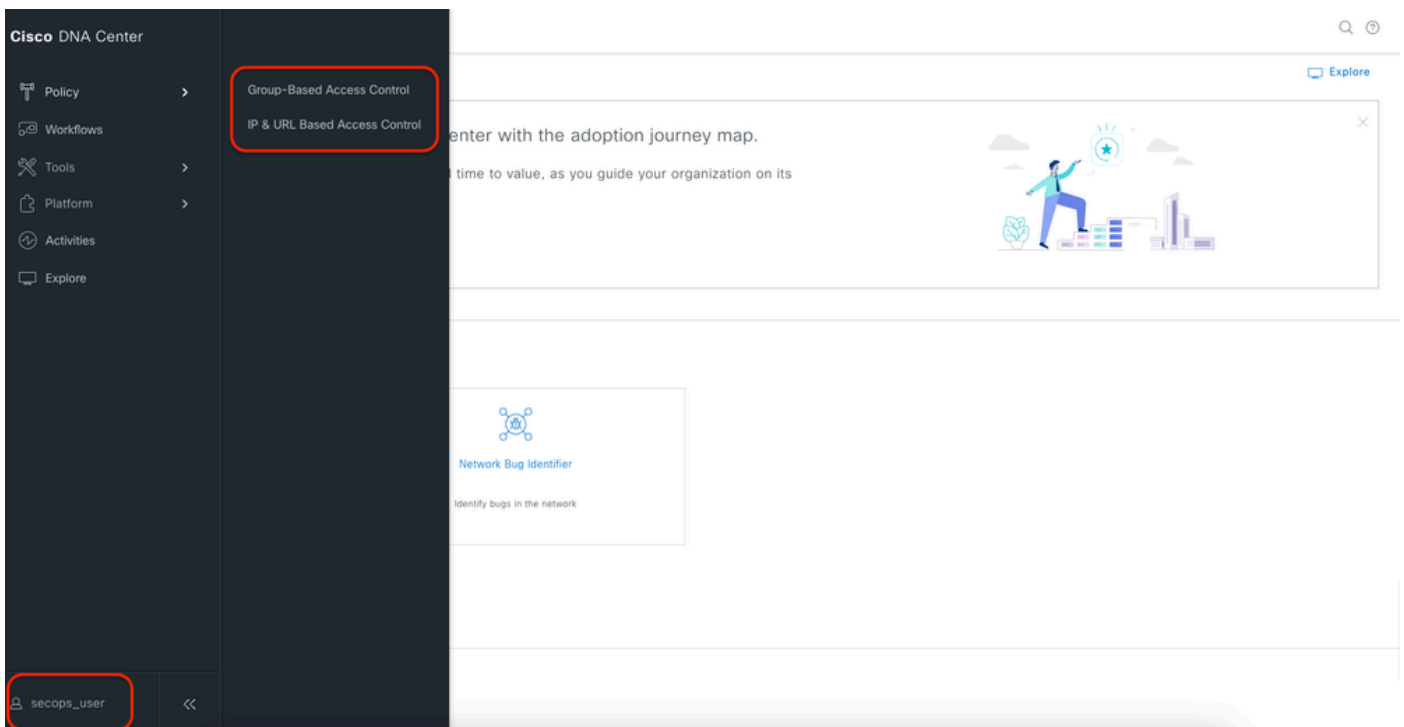
1- DNAC - Mostrar usuarios externos Sistema > Usuarios y funciones > Autenticación externa > Usuarios externos.

Puede ver la lista de usuarios externos que han iniciado sesión mediante TACACS+ por primera vez. La información que se muestra incluye sus nombres de usuario y roles.



Usuarios externos

2. DNAC - Confirmar el acceso del usuario.



Acceso de usuario limitado

3.a ISE - Centros de trabajo de Live-Logs de TACACS+ > Administración de dispositivos > Descripción general > Livellog de TACACS.

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#All Device Types#DNAC...	Lo
Jan 19, 2025 05:12:4...	✓		SecOps_User	Authentication	DNAC - Policy >> DNAC - Authentication			Device Type#All Device Types#DNAC...	Lo

Last Updated: Sun Jan 19 2025 17:16:38 GMT+0100 (Central European Standard Time) Records Shown: 2

Live-Logs de TACACS

3.b ISE - Centros de trabajo detallados de Live-Logs de TACACS+ > Administración de dispositivos > Descripción general > Livelog de TACACS > Haga clic (Detalles) para acceder al registro de autorización.

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

Live-Logs detallados de 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; }

Live-Logs detallados de TACACS+ 2-2

Troubleshoot

Actualmente no hay información de diagnóstico específica disponible para esta configuración.

Referencias

- [Guía del administrador de Cisco Identity Services Engine, versión 3.4 > Administración de dispositivos](#)
- [Guía del administrador de Cisco DNA Center, versión 2.3.5](#)
- [Cisco DNA Center: Control de acceso basado en roles con autenticación externa](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).