

Configurer ISE en tant qu'authentification externe pour l'interface utilisateur DNAC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Avant de commencer](#)

[Configurer](#)

[\(Option 1\) Configurez l'authentification externe DNAC à l'aide de RADIUS](#)

[\(Option 1\) Configuration d'ISE pour RADIUS](#)

[\(Option 2\) Configurez l'authentification externe DNAC à l'aide de TACACS+](#)

[\(Option 2\) Configuration d'ISE pour TACACS+](#)

[Vérifier](#)

[Vérification de la configuration RADIUS](#)

[Vérification de la configuration TACACS+](#)

[Dépannage](#)

[Références](#)

Introduction

Ce document décrit comment configurer Cisco Identity Services Engine (ISE) en tant qu'authentification externe pour l'administration de l'interface utilisateur graphique de Cisco DNA Center.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- Protocoles TACACS+ et RADIUS.
- Intégration de Cisco ISE avec Cisco DNA Center.
- Évaluation de la politique Cisco ISE.

Composants utilisés


Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine (ISE) Version 3.4 Patch1.
- Cisco DNA Center version 2.3.5.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Avant de commencer

- Assurez-vous qu'au moins un serveur d'authentification RADIUS est configuré sur System > Settings > External Services > Authentication and Policy Servers.
- Seul un utilisateur avec des autorisations SUPER-ADMIN-ROLE sur DNAC peut effectuer cette procédure.
- Activez le fallback d'authentification externe.

 Mise en garde : Dans les versions antérieures à 2.1.x, lorsque l'authentification externe est activée, Cisco DNA Center revient aux utilisateurs locaux si le serveur AAA est inaccessible ou si le serveur AAA rejette un nom d'utilisateur inconnu. Dans la version actuelle, Cisco DNA Center ne reviendra pas aux utilisateurs locaux si le serveur AAA est inaccessible ou si le serveur AAA rejette un nom d'utilisateur inconnu. Lorsque le secours d'authentification externe est activé, les utilisateurs externes et les administrateurs locaux peuvent se connecter à Cisco DNA Center.

Pour activer la reprise d'authentification externe, établissez une connexion SSH avec l'instance Cisco DNA Center et entrez la commande this CLI (`magctl rbac external_auth_fallback enable`).

Configurer

(Option 1) Configurez l'authentification externe DNAC à l'aide de RADIUS

Étape 1. (Facultatif) Définissez des rôles personnalisés.

Configurez vos rôles personnalisés en fonction de vos besoins. Vous pouvez utiliser les rôles d'utilisateurs par défaut. Pour ce faire, accédez à l'onglet System > Users & Roles > Role Based Access Control.

Procédure

- a. Créer un nouveau rôle.

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

Nom du rôle DevOps

b. Définissez l'accès.

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

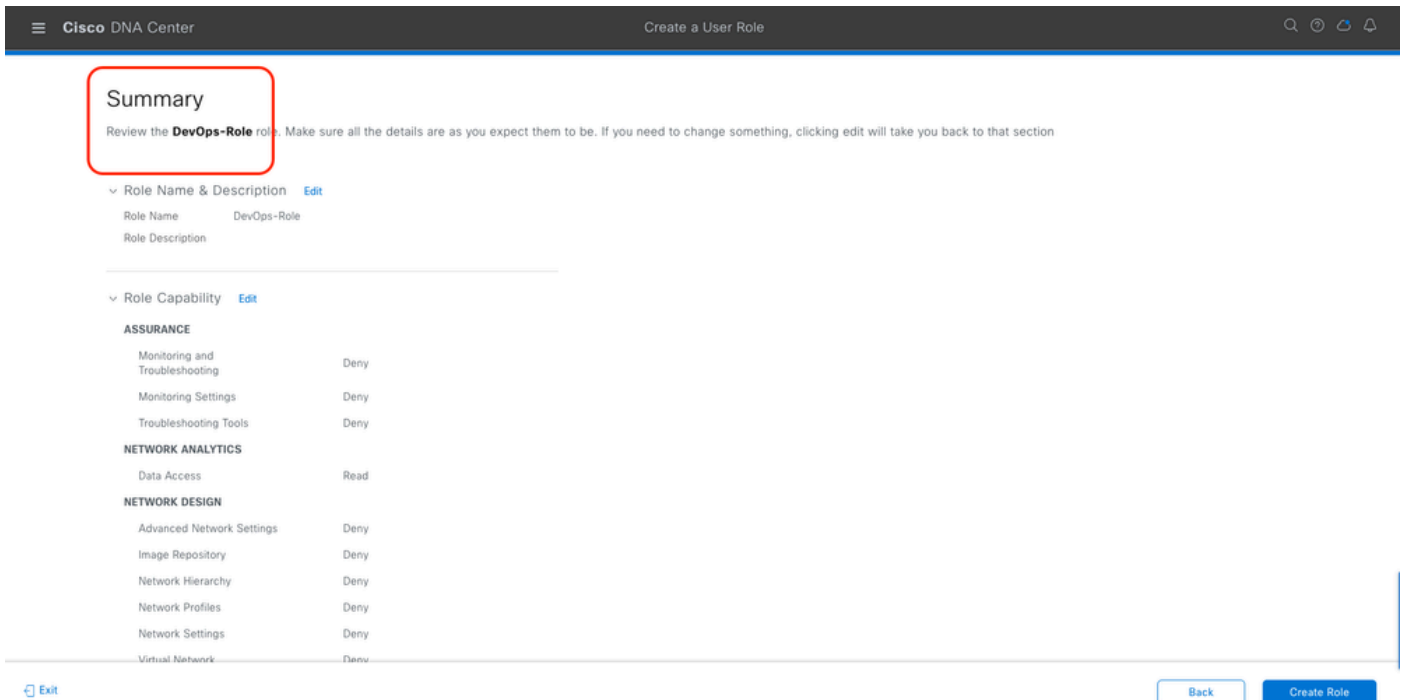
Access	Permission	Description
> Assurance	<input checked="" type="radio"/> Deny <input type="radio"/> Read <input type="radio"/> Write	Assure consistent service levels with complete visibility across all aspects of your network.
> Network Analytics	<input type="radio"/> Deny <input checked="" type="radio"/>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

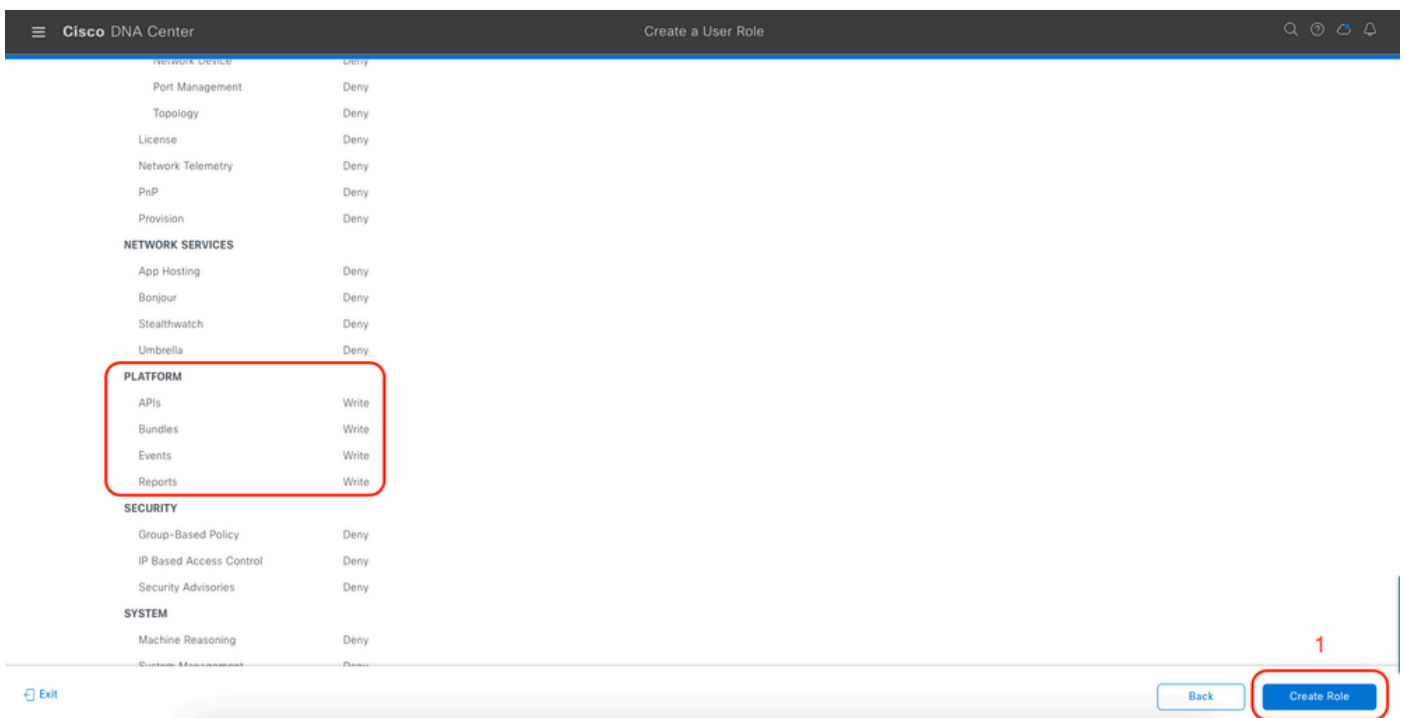
Next

Accès au rôle DevOps

c. Créez le nouveau rôle.



Récapitulatif des rôles DevOps



Vérifier et créer un rôle DevOps

Étape 2 : configuration de l'authentification externe à l'aide de RADIUS

Pour ce faire, accédez à l'onglet System > Users & Roles > External Authentication.

Procédure

a. Pour activer l'authentification externe dans Cisco DNA Center, cochez la case Enable External User.

b. Définissez les attributs AAA.

Saisissez Cisco-AVPair dans le champ AAA attributes.

c. (Facultatif) Configurez les serveurs AAA principal et secondaire.

Assurez-vous que le protocole RADIUS est activé sur le serveur AAA principal au moins, ou sur les serveurs principal et secondaire.

The screenshot shows the 'External Authentication' configuration page in Cisco DNA Center. The page is titled 'System / Users & Roles' and has a search icon in the top right. The left sidebar shows 'User Management', 'Role Based Access Control', and 'External Authentication'. The main content area is titled 'External Authentication' and contains the following configuration options:

- Enable External User:** A checkbox that is checked, highlighted with a red box labeled 'a'.
- AAA Attribute:** A dropdown menu set to 'Cisco-AVPair', highlighted with a red box labeled 'b'.
- AAA Server(s):** A section with two columns for 'Primary AAA Server' and 'Secondary AAA Server', highlighted with a red box labeled 'c'. Each column has the following fields:
 - IP Address:** 'ISE Server 1 IP' for Primary and 'ISE Server 2 IP' for Secondary.
 - Shared Secret:** Masked with '*****'.
 - Authentication Port:** '1812' for both.
 - Protocol:** 'RADIUS' is selected for both, with 'TACACS' as an alternative.

Étapes de configuration de l'authentification externe (RADIUS)

(Option 1) Configuration d'ISE pour RADIUS

Étape 1 : ajout d'un serveur DNAC en tant que périphérique réseau sur ISE

Pour ce faire, accédez à l'onglet Administration > Network Resources > Network Devices.

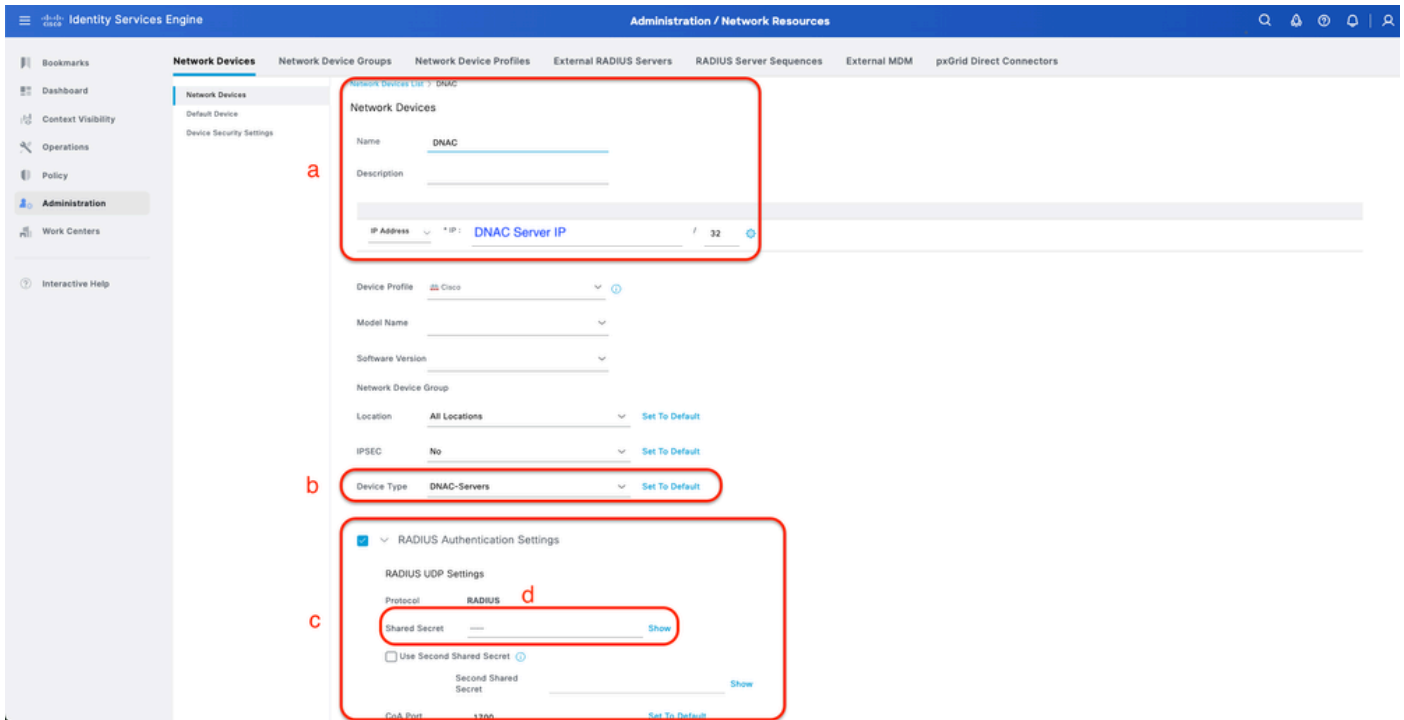
Procédure

a. Définissez le nom et l'adresse IP du périphérique réseau (DNAC).

b. (Facultatif) Classez le type de périphérique pour la condition Jeu de stratégies.

c. Activez les paramètres d'authentification RADIUS.

d. Définissez le secret partagé RADIUS.



Périphérique réseau ISE (DNAC) pour RADIUS

Étape 2 : création de profils d'autorisation RADIUS

Vous pouvez le faire à partir de l'onglet Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation.

 Remarque : Créez trois profils d'autorisation RADIUS, un pour chaque rôle d'utilisateur.

Procédure

- Cliquez sur Add et définissez le nom du profil d'autorisation RADIUS.
- Saisissez la paire Cisco : cisco-av-dans les paramètres d'attributs avancés et remplissez le rôle d'utilisateur approprié.
 - Pour le rôle d'utilisateur (DecOps-Role), entrez ROLE=DevOps-Role.
 - Pour le rôle d'utilisateur (NETWORK-ADMIN-ROLE), entrez ROLE=NETWORK-ADMIN-ROLE.
 - Pour le rôle d'utilisateur (SUPER-ADMIN-ROLE), entrez ROLE=SUPER-ADMIN-ROLE.
- Consultez les détails des attributs.
- Cliquez sur Save.

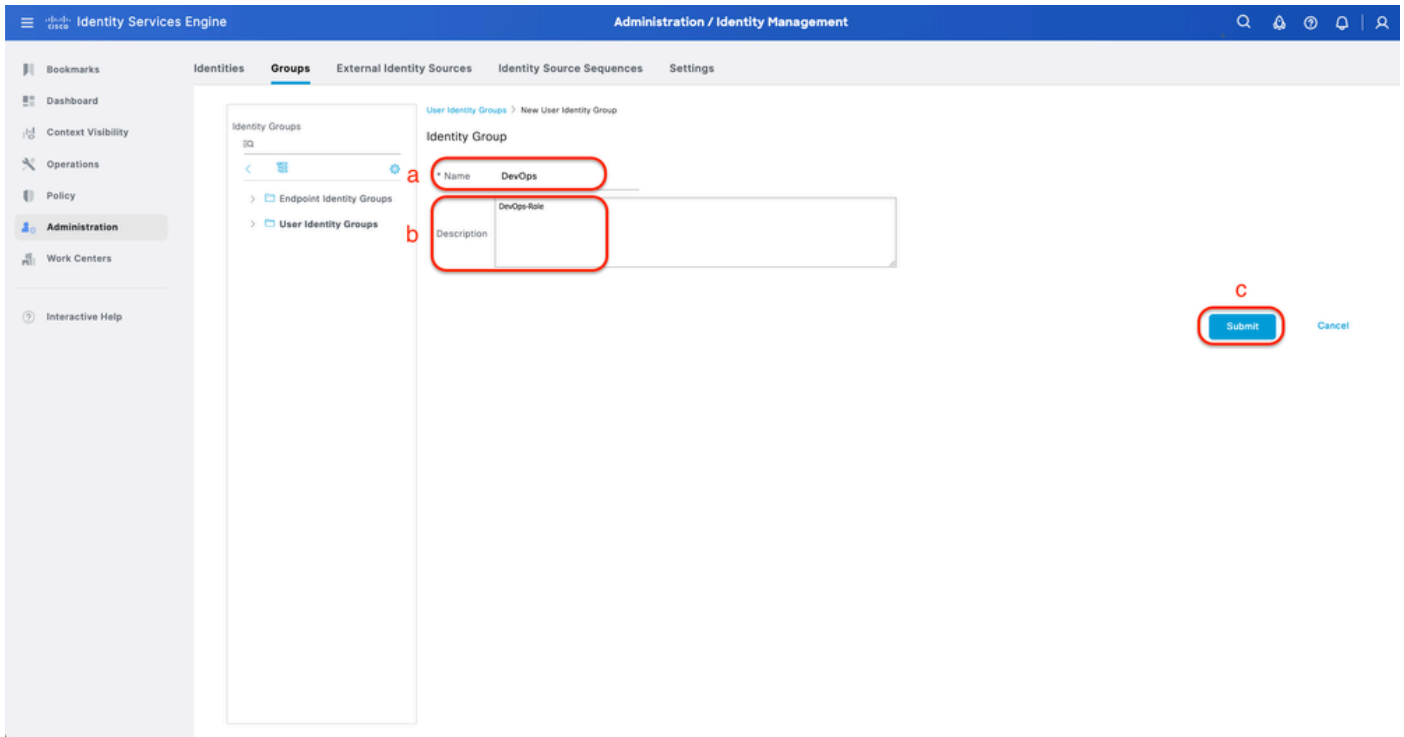
Créer un profil d'autorisation

Étape 3 : création d'un groupe d'utilisateurs

Pour ce faire, accédez à l'onglet Administration > Identity Management > Groups > User Identity Groups.

Procédure

- a. Cliquez sur Add et définissez le nom du groupe d'identités
- b. (Facultatif) Définissez la description.
- c. Cliquez sur Envoyer.



Créer un groupe d'identités utilisateur

Étape 4 : création d'un utilisateur local

Pour ce faire, accédez à l'onglet Administration > Identity Management > Identities > Users.

Procédure

- a. Cliquez sur Add et définissez le nom d'utilisateur.
- b. Définissez le mot de passe de connexion.
- c. Ajoutez l'utilisateur au groupe d'utilisateurs associé.
- d. Cliquez sur Submit.

Identity Services Engine Administration / Identity Management

Network Access Users List > New Network Access User

Network Access User

* Username **DevOps_User**

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

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

Never Expires

* Login Password Re-Enter Password

Generate Password

Enable Password

User Information

First Name

Last Name

Créer un utilisateur local 1-2

Identity Services Engine Administration / Identity Management

* Login Password Re-Enter 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 2025-03-20 (yyyy-mm-dd)

User Groups

DevOps

Submit

Cancel

Créer un utilisateur local 2-2

Étape 5. (Facultatif) Ajouter un jeu de stratégies RADIUS.

Pour ce faire, accédez à l'onglet Policy > Policy Sets.

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

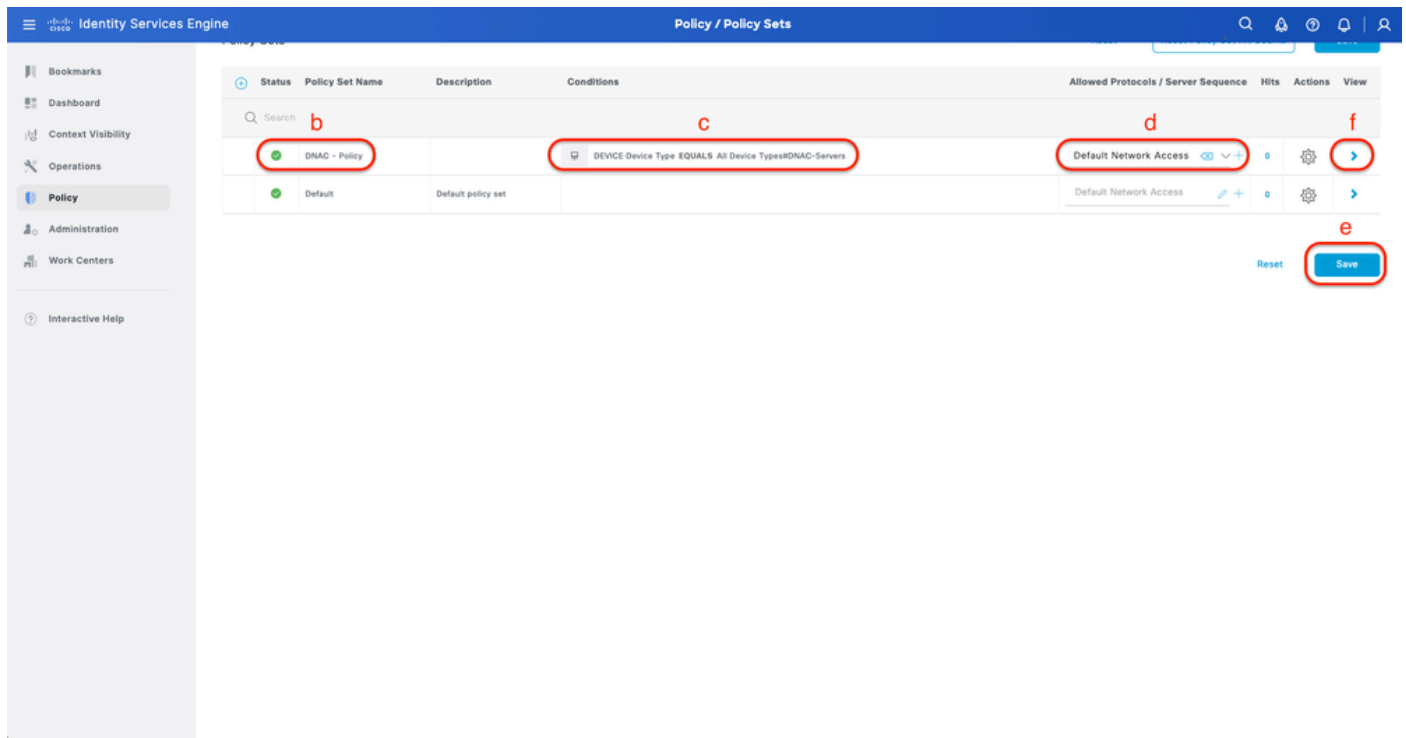
b. Définissez le nom du jeu de stratégies.

c. Définissez la condition du jeu de stratégies sur Sélectionner le type de périphérique précédemment créé (Étape 1 > b).

d. Définissez les protocoles autorisés.

e. Cliquez sur Save.

f. Cliquez sur (>) Policy Set View pour configurer les règles d'authentification et d'autorisation.



Ajouter un ensemble de stratégies RADIUS

Étape 6 : configuration de la stratégie d'authentification RADIUS

Pour ce faire, sélectionnez l'onglet Policy > Policy Sets > Click (>).

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'authentification.

c. Définissez la condition de stratégie d'authentification et sélectionnez le type de périphérique que vous avez créé précédemment (Étape 1 > b).

d. Définissez l'option Authentication Policy Use for Identity source.

e. Cliquez sur Save.

The screenshot displays the Cisco ISE Policy / Policy Sets configuration interface. 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 red letters: 'b' for the 'DNAC - Authentication' rule name, 'c' for the condition, and 'd' for the 'Internal Users' user group selection.

Ajouter une stratégie d'authentification RADIUS

Étape 7 : configuration de la stratégie d'autorisation RADIUS

Pour ce faire, accédez à l'onglet Policy > Policy Sets > Click (>).

Cette étape permet de créer une stratégie d'autorisation pour chaque rôle d'utilisateur :

- RÔLE DE SUPER-ADMINISTRATEUR
- RÔLE-ADMINISTRATEUR-RÉSEAU
- Rôle DevOps

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'autorisation.

c. Définissez la condition de stratégie d'autorisation et sélectionnez le groupe d'utilisateurs que vous avez créé à l' (étape 3).

d. Définissez les résultats/profils de stratégie d'autorisation et sélectionnez le profil d'autorisation que vous avez créé à l' (étape 2).

e. Cliquez sur Save.

The screenshot displays the Cisco ISE Policy / Policy Sets interface. The main table shows the following data:

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

Below the table, the configuration for a specific rule is shown:

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	⚙️

At the bottom right, there are buttons for 'Reset' and 'Save'.

Ajouter une stratégie d'autorisation

(Option 2) Configurer l'authentification externe DNAC à l'aide de TACACS+

Étape 1. (Facultatif) Définissez des rôles personnalisés.

Configurez vos rôles personnalisés en fonction de vos besoins. Vous pouvez utiliser les rôles d'utilisateurs par défaut. Pour ce faire, accédez à l'onglet System > Users & Roles > Role Based Access Control.

Procédure

a. Créer un nouveau rôle.

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](#)

Nom du rôle SecOps

b. Définissez l'accès.

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 checked="" 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 checked="" 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](#)

Accès au rôle SecOps

c. Créez le nouveau rôle.

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](#)

Résumé du rôle 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](#)

Vérifier et créer un rôle SecOps

Étape 2 : configuration de l'authentification externe à l'aide de TACACS+
 Pour ce faire, accédez à l'onglet System > Users & Roles > External Authentication.

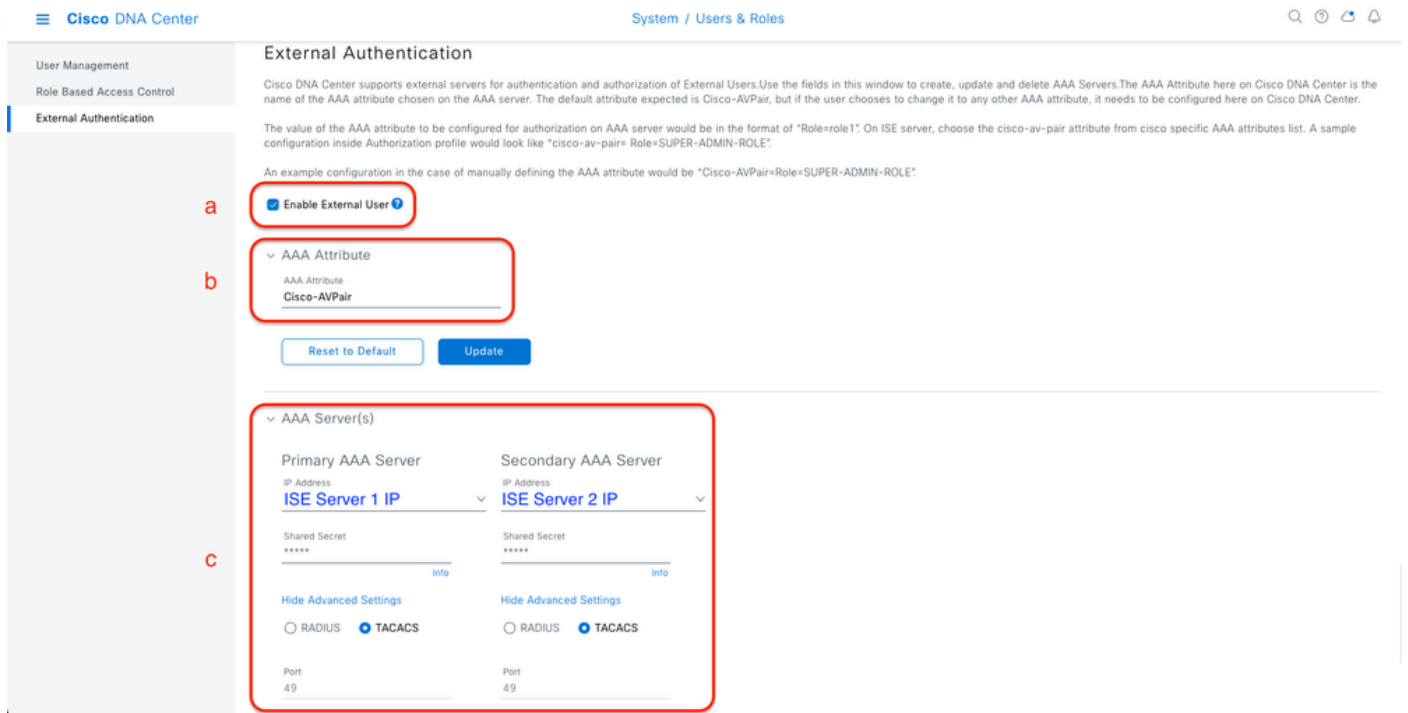
a. Pour activer l'authentification externe dans Cisco DNA Center, cochez la case Enable External User.

b. Définissez les attributs AAA.

Saisissez Cisco-AVPair dans le champ AAA attributes.

c. (Facultatif) Configurez les serveurs AAA principal et secondaire.

Assurez-vous que le protocole TACACS+ est activé sur le serveur AAA principal au moins, ou sur les serveurs principal et secondaire.

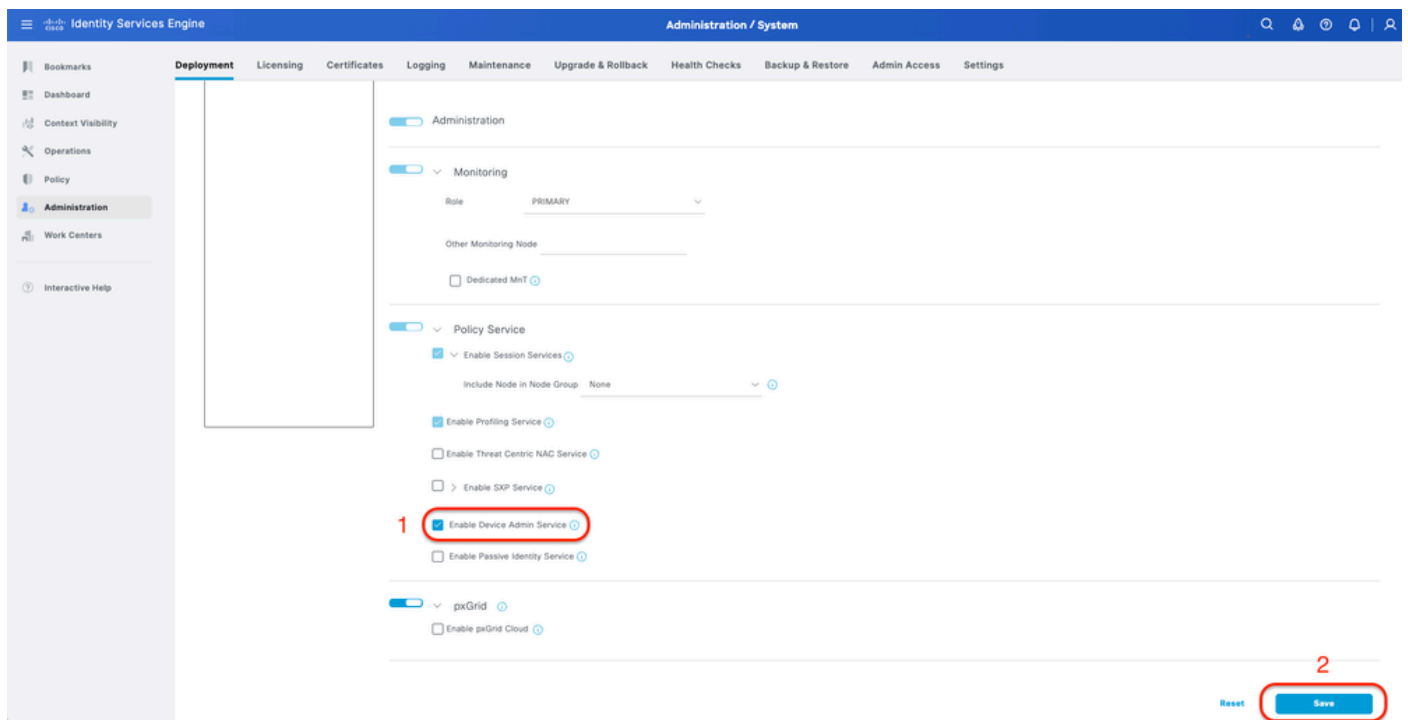


(TACACS+) Étapes de configuration de l'authentification externe

(Option 2) Configuration d'ISE pour TACACS+

Étape 1 : activation du service d'administration des périphériques

Pour ce faire, accédez à l'onglet Administration > System > Deployment > Edit (ISE PSN Node) > Check Enable Device Admin Service.



Activer le service d'administration des périphériques

Étape 2 : ajout d'un serveur DNAC en tant que périphérique réseau sur ISE

Pour ce faire, accédez à l'onglet Administration > Network Resources > Network Devices.

Procédure

- Définissez le nom et l'adresse IP du périphérique réseau (DNAC).
- (Facultatif) Classez le type de périphérique pour la condition Jeu de stratégies.
- Activez les paramètres d'authentification TACACS+.
- Définissez le secret partagé TACACS+.

The screenshot shows the 'Network Devices' configuration page in the ISE Administration console. The form is for adding a new device named 'DNAC'. The IP address is 'DNAC Server IP'. The device profile is 'Cisco'. The device type is 'DNAC-Servers'. Under 'RADIUS Authentication Settings', 'TACACS Authentication Settings' is checked, and the 'Shared Secret' field is highlighted with a red box. The 'Retire' button is also visible.

Périphérique réseau ISE (DNAC) pour TACACS+

Étape 3 : création de profils TACACS+ pour chaque rôle DNAC

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles.




Remarque : Créez 3 profils TACACS+, un pour chaque rôle d'utilisateur.

Procédure

- Cliquez sur Add et définissez le nom du profil TACACS.
- Cliquez sur l'onglet Affichage brut.
- Saisissez Cisco-AVPair=ROLE= et remplissez le rôle d'utilisateur approprié.
 - Pour le rôle d'utilisateur (SecOps-Role), saisissez Cisco-AVPair=ROLE=SecOps-Role.

- Pour le rôle d'utilisateur (NETWORK-ADMIN-ROLE), entrez Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE.
- Pour le rôle d'utilisateur (SUPER-ADMIN-ROLE), saisissez Cisco-AVPair=ROLE=SUPER-ADMIN-ROLE.

 Remarque : Souvenez-vous que la valeur AVPair (Cisco-AVPair=ROLE=) est sensible à la casse et assurez-vous qu'elle correspond au rôle d'utilisateur DNAC.

d. Cliquez sur Save.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a TACACS Profile. The main configuration area is titled 'TACACS Profile' and includes the following fields and options:

- Name:** SecOps_Role (labeled 'a')
- Description:** (labeled 'b')
- Task Attribute View:** Raw View (labeled 'b')
- Profile Attributes:** Cisco-AVPair=ROLE=SecOps-Role (labeled 'c')
- Buttons:** Cancel and Save (labeled 'd')

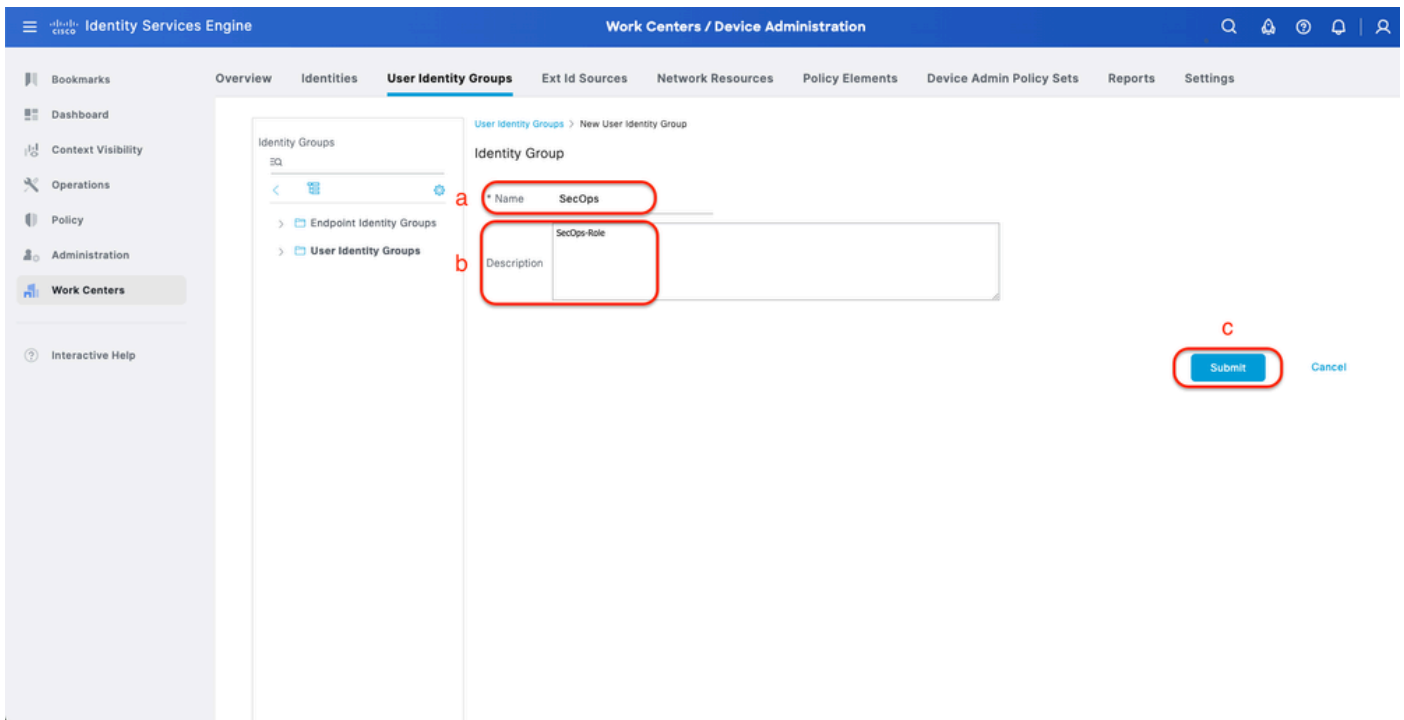
Créer un profil TACACS (SecOps_Role)

Étape 4 : création d'un groupe d'utilisateurs

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > User Identity Groups.

Procédure

- Cliquez sur Add et définissez le nom du groupe d'identités.
- (Facultatif) Définissez la description.
- Cliquez sur Envoyer.



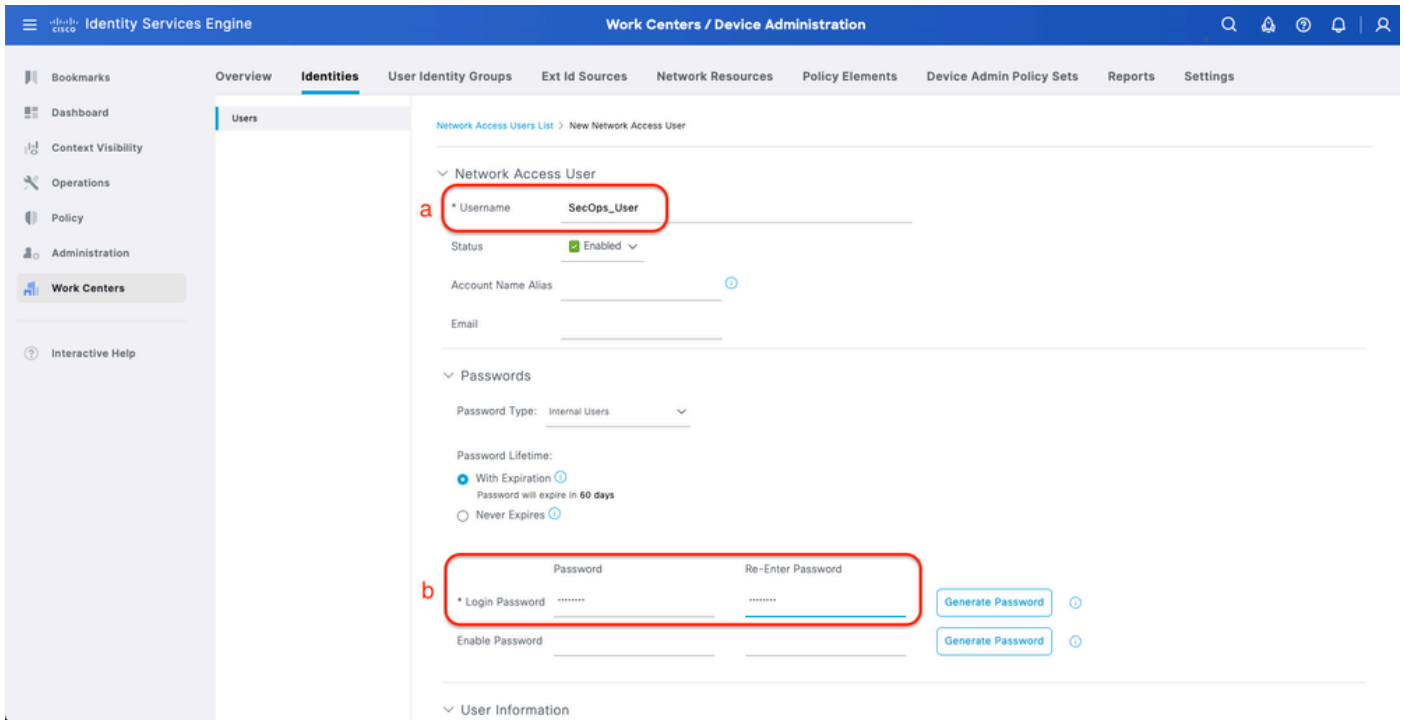
Créer un groupe d'identités utilisateur

Étape 5 : création d'un utilisateur local

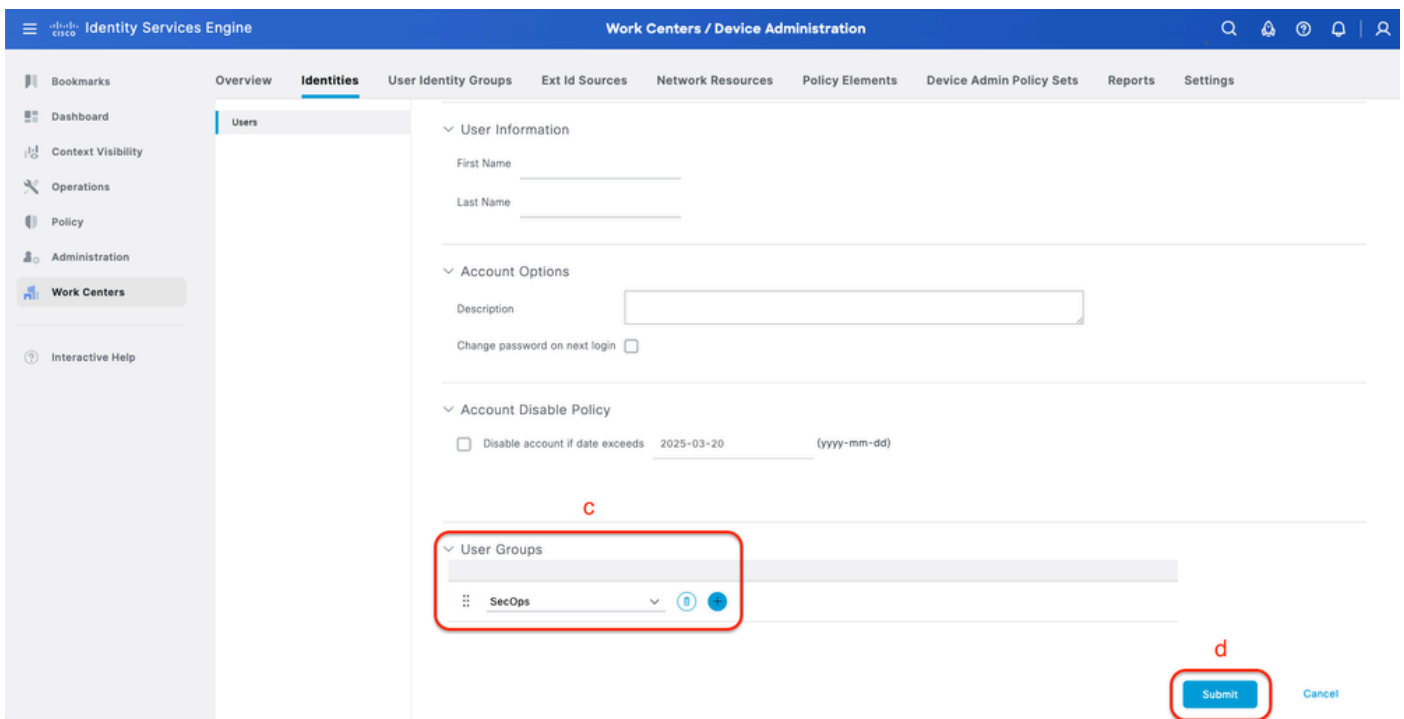
Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Identities > Users.

Procédure

- a. Cliquez sur Add et définissez le nom d'utilisateur.
- b. Définissez le mot de passe de connexion.
- c. Ajoutez l'utilisateur au groupe d'utilisateurs associé.
- d. Cliquez sur Submit.



Créer un utilisateur local 1-2



Créer un utilisateur local 2-2

Étape 6. (Facultatif) Ajoutez un jeu de stratégies TACACS+.

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets.

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

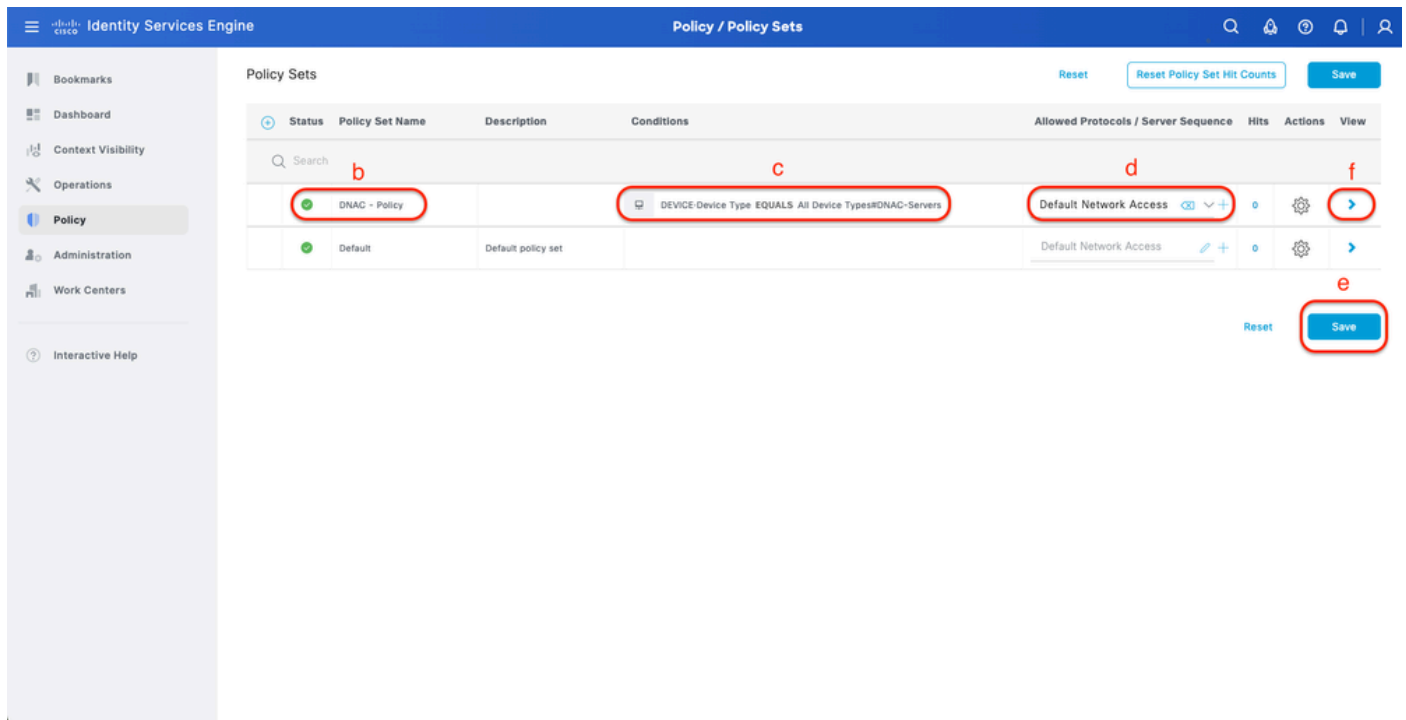
b. Définissez le nom du jeu de stratégies.

c. Définissez la condition Jeu de stratégies sur Sélectionner le type de périphérique précédemment créé (Étape 2 > b).

d. Définissez les protocoles autorisés.

e. Cliquez sur Save.

f. Cliquez sur (>) Policy Set View pour configurer les règles d'authentification et d'autorisation.



Ajouter un ensemble de stratégies TACACS+

Étape 7 : configuration de la stratégie d'authentification TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'authentification.

c. Définissez la condition de stratégie d'authentification et sélectionnez le type de périphérique que vous avez créé précédemment (Étape 2 > b).

d. Définissez l'option Authentication Policy Use for Identity source.

e. Cliquez sur Save.

Ajouter une stratégie d'authentification TACACS+

Étape 8 : configuration de la stratégie d'autorisation TACACS+

Pour ce faire, accédez à l'onglet Work Centers > Device Administration > Device Admin Policy Sets > Cliquez sur (>).

Cette étape permet de créer une stratégie d'autorisation pour chaque rôle d'utilisateur :

- RÔLE DE SUPER-ADMINISTRATEUR
- RÔLE-ADMINISTRATEUR-RÉSEAU
- Rôle SecOps

Procédure

a. Cliquez sur Actions et choisissez (Insérer une nouvelle ligne ci-dessus).

b. Définissez le nom de la stratégie d'autorisation.

c. Définissez la condition de stratégie d'autorisation et sélectionnez le groupe d'utilisateurs que vous avez créé à l' (étape 4).

d. Définissez les profils Shell de stratégie d'autorisation et sélectionnez le profil TACACS que vous avez créé à l' (étape 3).

e. Cliquez sur 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

Ajouter une stratégie d'autorisation

Vérifier

Vérification de la configuration RADIUS

1- DNAC - Afficher les utilisateurs externes Système > Utilisateurs et rôles > Authentification externe > Utilisateurs externes.

Vous pouvez afficher la liste des utilisateurs externes qui se sont connectés via RADIUS pour la première fois. Les informations affichées incluent leurs noms d'utilisateur et leurs rôles.

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)

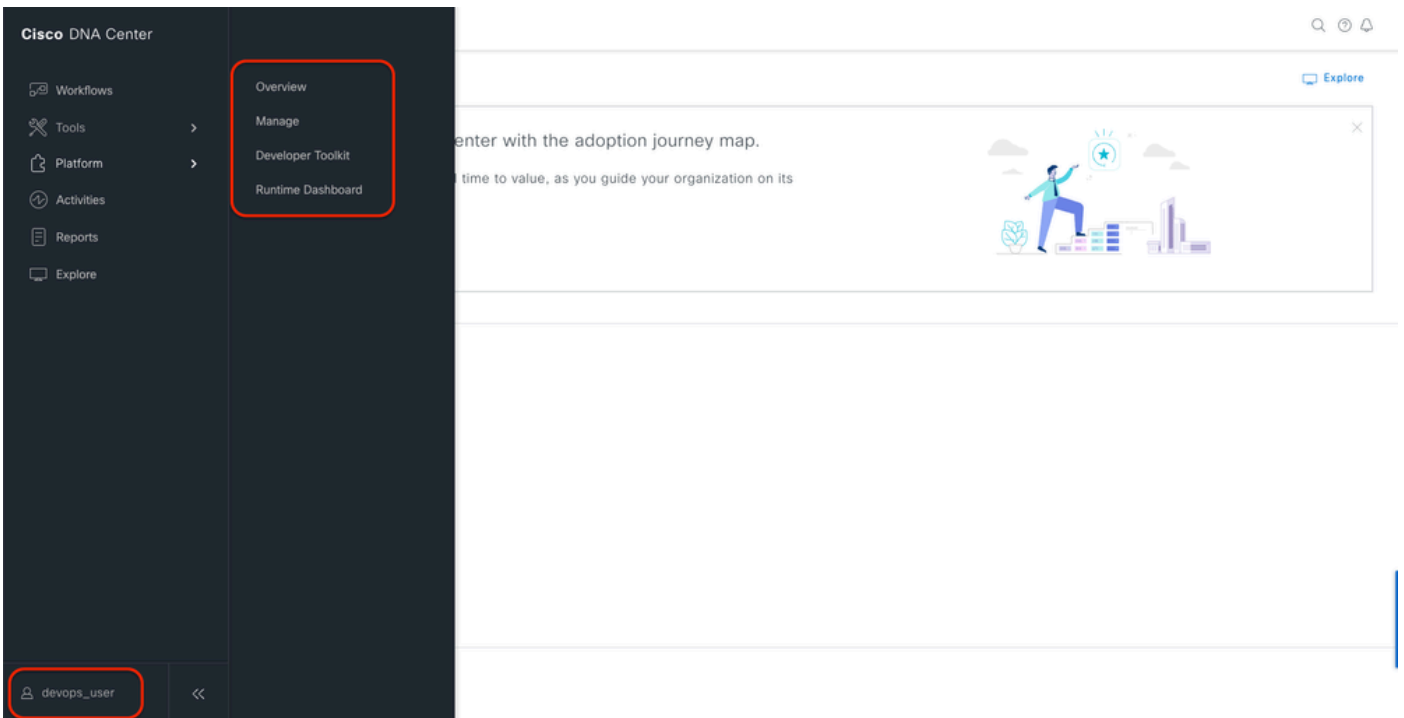
External Users

Username	Role	Action
devops_user	DevOps-Role	Delete

Showing 1 of 1

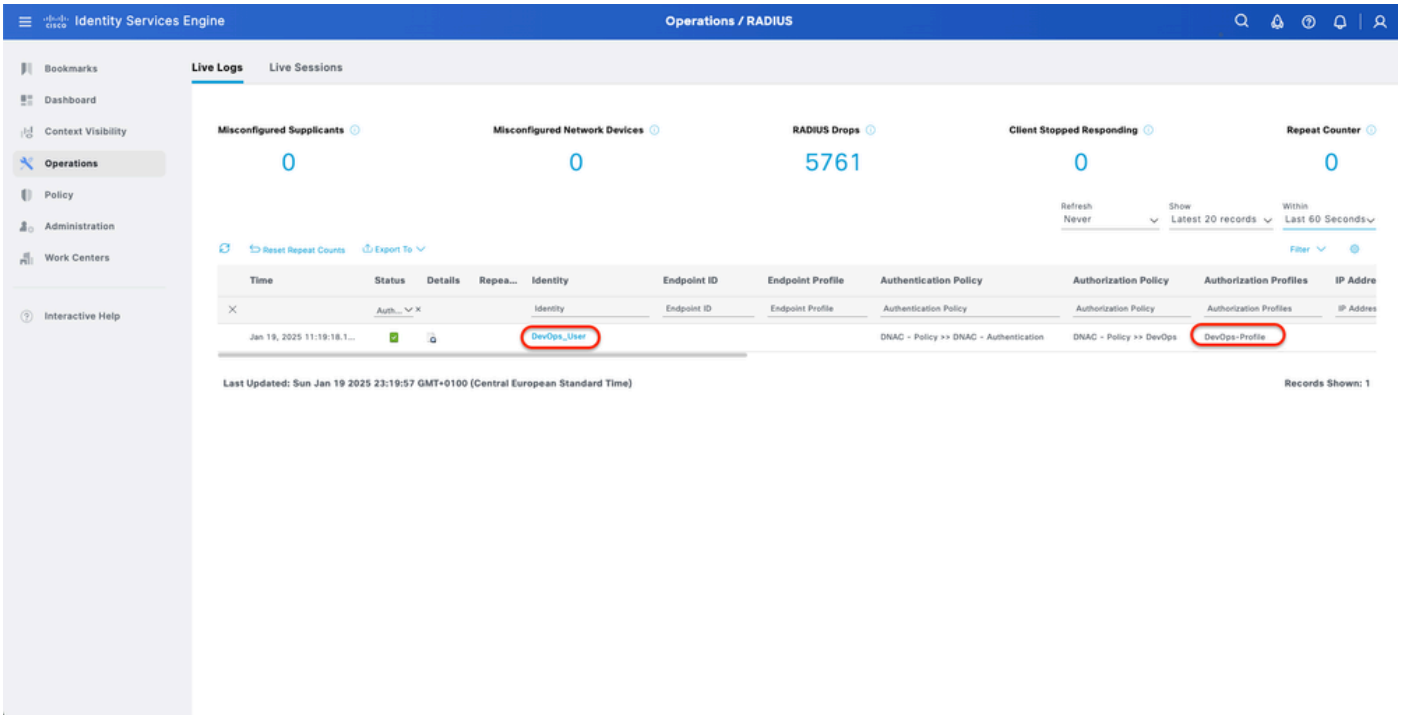
Utilisateurs externes

2. DNAC - Confirmez l'accès utilisateur.



Accès utilisateur limité

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



Journaux en direct RADIUS

3.b ISE - RADIUS Live-Logs Operations > RADIUS > Live-Logs > Click (Details) for Authorization log.

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

Journaux en direct détaillés 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

Journaux en direct détaillés RADIUS 2-2

Vérification de la configuration TACACS+

1- DNAC - Afficher les utilisateurs externes Système > Utilisateurs et rôles > Authentification externe > Utilisateurs externes.

Vous pouvez afficher la liste des utilisateurs externes qui se sont connectés via TACACS+ pour la première fois. Les informations affichées incluent leurs noms d'utilisateur et leurs rôles.

Cisco DNA Center System / Users & Roles

User Management
Role Based Access Control
External Authentication

AAA Attribute
Cisco-AVPair

Reset to Default Update

AAA Server(s)

Primary AAA Server Secondary AAA Server

IP Address IP Address

Shared Secret Shared Secret

View Advanced Settings View Advanced Settings

Update Update

External Users

Filter EQ Find

Username	Role	Action
secops_user	SecOps-Role	Delete

Showing 1 of 1

Utilisateurs externes

2. DNAC - Confirmez l'accès utilisateur.

Cisco DNA Center

Policy Workflows Tools Platform Activities Explore

Group-Based Access Control
IP & URL Based Access Control

center with the adoption journey map.

time to value, as you guide your organization on its

Network Bug Identifier
Identify bugs in the network

secops_user

Accès utilisateur limité

3.a ISE - Centres de travail TACACS+ Live-Logs > Administration des périphériques > Présentation > TACACS Livelllog.

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

Journaux TACACS en direct

3.b ISE - détails TACACS+ Live-Logs Work Centers > Device Administration > Overview > TACACS Livelog > Click (Details) for Authorization log.

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

Journaux en direct détaillés 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
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; }

Journaux en direct détaillés TACACS+ 2-2

Dépannage

Aucune information de diagnostic spécifique n'est actuellement disponible pour cette configuration.

Références

- [Guide d'administration de Cisco Identity Services Engine, version 3.4 > Device Administration](#)
- [Guide de l'administrateur de Cisco DNA Center, version 2.3.5](#)
- [Cisco DNA Center: Contrôle d'accès basé sur les rôles avec authentification externe](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.