

# Configuration de l'authentification externe RADIUS sur DNA Center et ISE 3.1

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Vérifier](#)

[Plus de rôles](#)

---

## Introduction

Ce document décrit comment configurer l'authentification externe RADIUS sur Cisco DNA Center à l'aide d'un serveur Cisco ISE exécutant la version 3.1.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco DNA Center et Cisco ISE sont déjà intégrés et l'intégration est en cours.

### Composants utilisés

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

- Cisco DNA Center 2.3.5.x.
- Cisco ISE version 3.1.

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.

## Configurer

Étape 1. Connectez-vous à l'interface utilisateur graphique de Cisco DNA Center et accédez à System > Settings > Authentication and Policy Servers.

Vérifiez que le protocole RADIUS est configuré et que l'état d'ISE est Actif pour le serveur de type ISE.

Settings / External Services

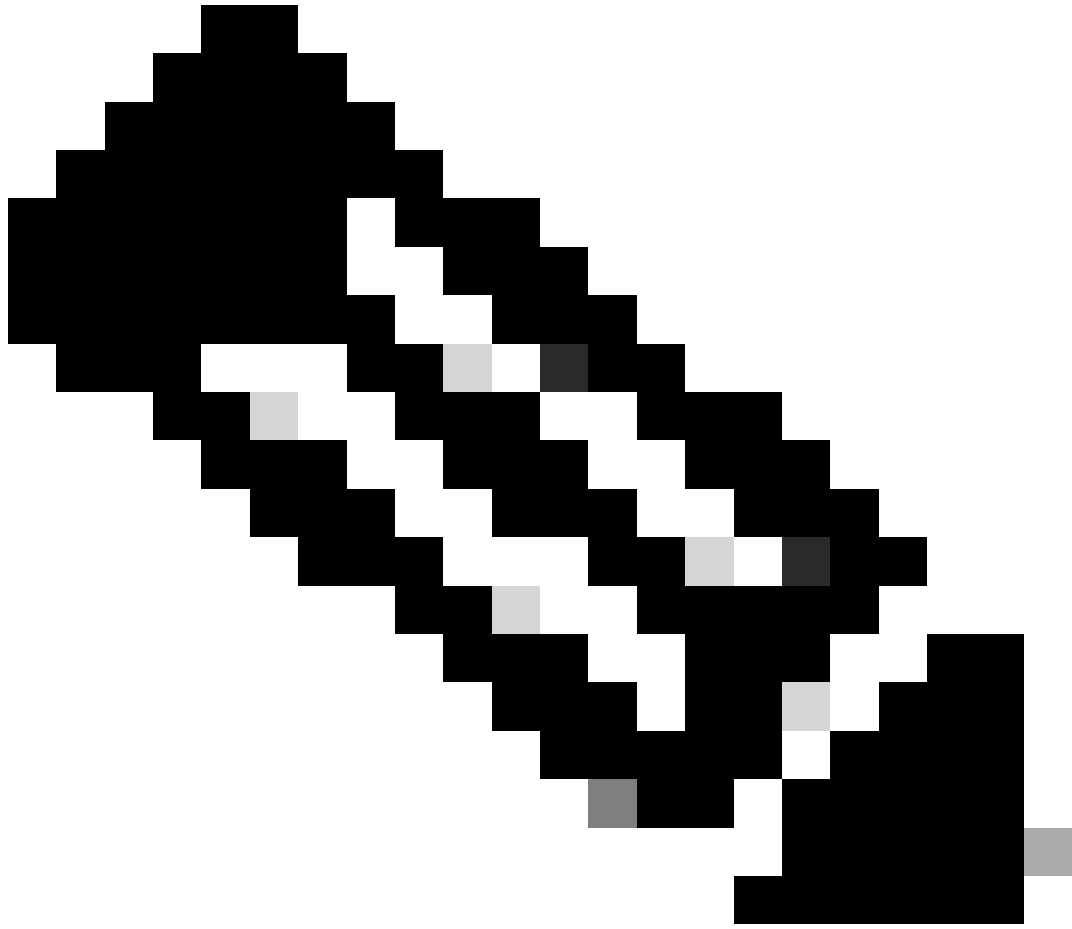
## Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[Add](#) [Export](#)

As of: Jul 19, 2023 4:38 PM [Refresh](#)

IP Address	Protocol	Type	Status	Actions
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...
[REDACTED]	<b>RADIUS</b>	<b>ISE</b>	<b>ACTIVE</b>	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS	AAA	ACTIVE	...
[REDACTED]	RADIUS_TACACS	AAA	ACTIVE	...



Remarque : le type de protocole RADIUS\_TACACS fonctionne pour ce document.

---












Avertissement : si le serveur ISE n'est pas à l'état Actif, vous devez d'abord corriger l'intégration.


Étape 2. Sur le serveur ISE, accédez à Administration > Network Resources > Network Devices, cliquez sur l'icône Filter, écrivez l'adresse IP Cisco DNA Center et confirmez si une entrée existe. Si c'est le cas, passez à l'étape 3.

Si l'entrée est manquante, vous devez voir le message No data available.

### Network Devices

Selected 0 Total 0  

 Edit  Add  Duplicate  Import  Export  Generate PAC  Delete

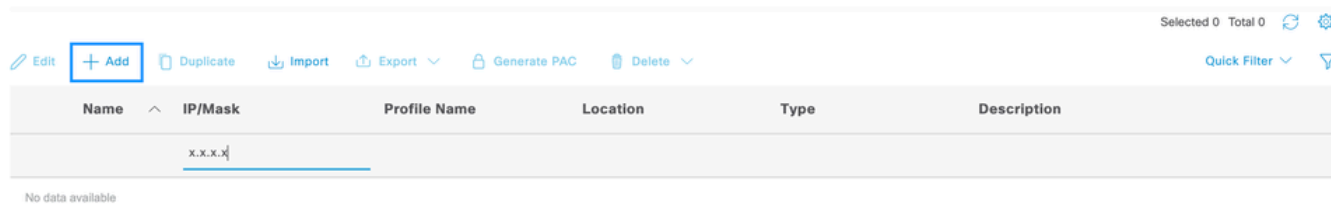
Quick Filter 

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

Dans ce cas, vous devez créer un périphérique réseau pour Cisco DNA Center, alors cliquez sur le bouton Add.

## Network Devices



Selected 0 Total 0

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

Name	IP/Mask	Profile Name	Location	Type	Description
	x.x.x.x				

No data available

Configurez le nom, la description et l'adresse IP (ou les adresses) à partir de Cisco DNA Center. Tous les autres paramètres sont définis sur les valeurs par défaut et ne sont pas nécessaires dans le cadre de ce document.

## Network Devices

\* Name

Description

IP Address <input type="text" value="* IP :"/>		/ 32	
--	--	------	--

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

[Set To Default](#)

IPSEC

[Set To Default](#)

Device Type

[Set To Default](#)

Faites défiler vers le bas et activez les paramètres d'authentification RADIUS en cliquant sur sa case à cocher et configurez un secret partagé.



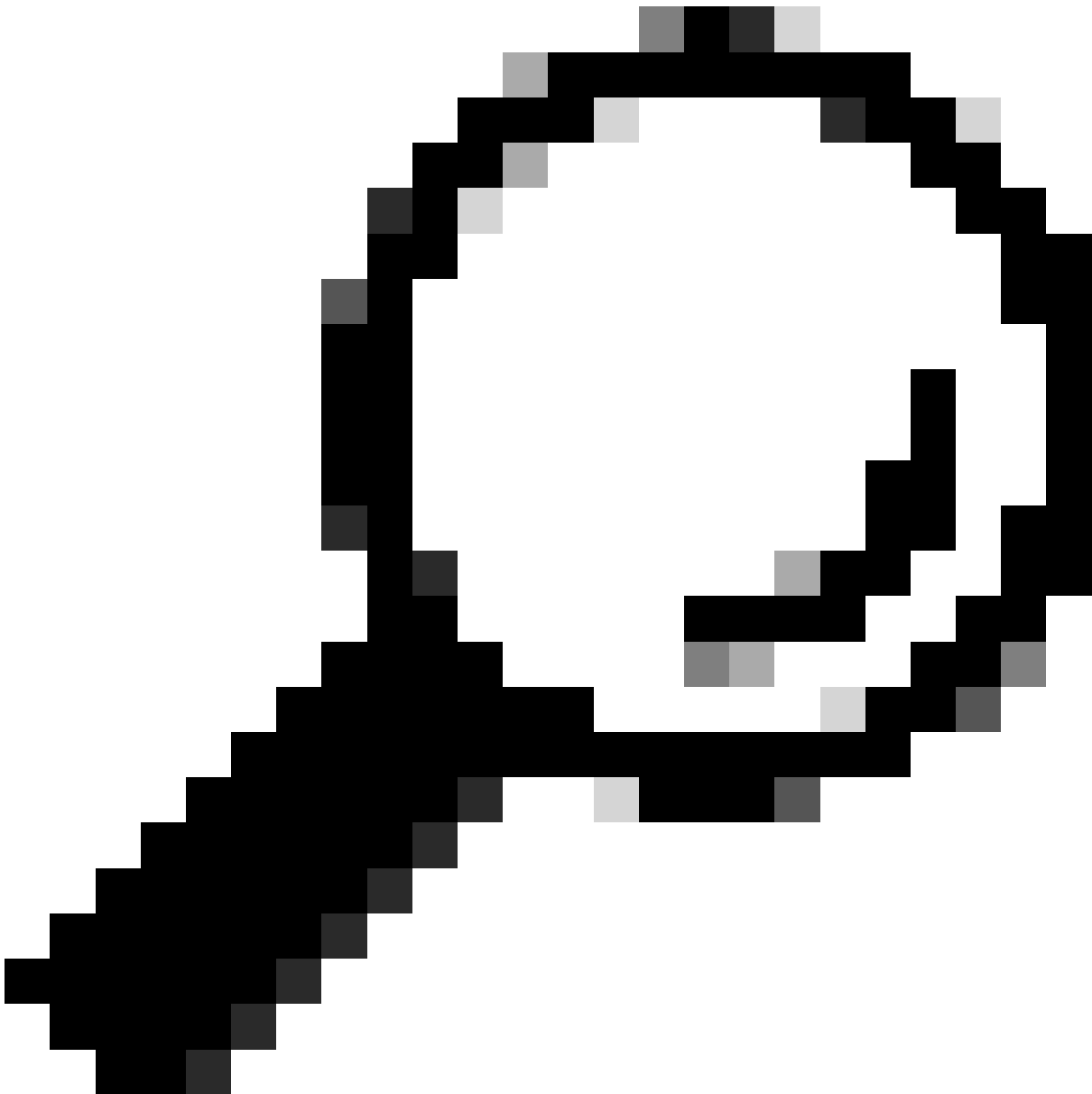
## ✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

\* Shared Secret .....

Show

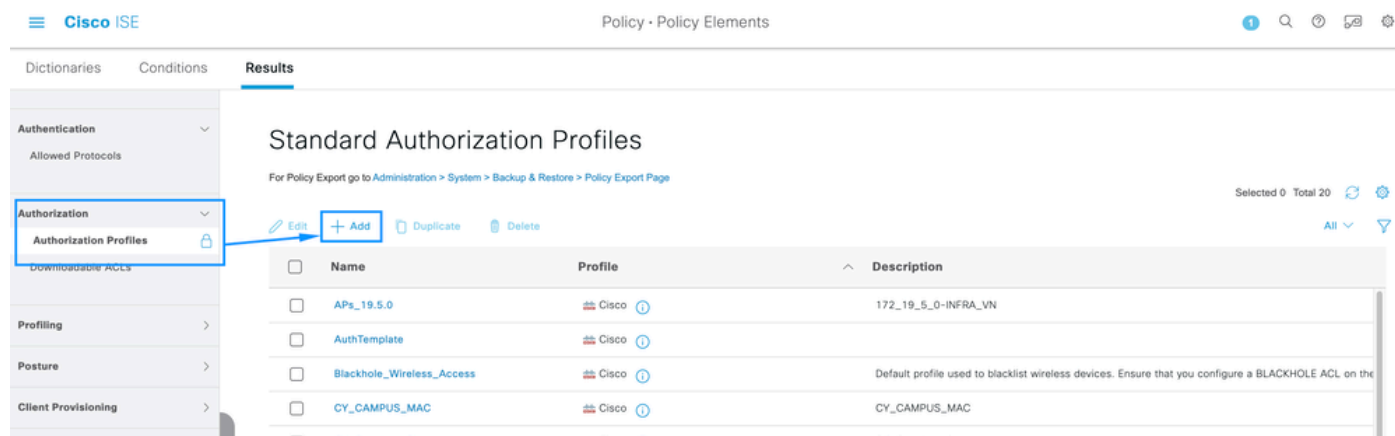


Conseil : ce secret partagé sera nécessaire plus tard. Enregistrez-le ailleurs.

Ensuite, cliquez sur Submit.

Étape 3. Sur le serveur ISE, accédez à Policy > Policy Elements > Results, pour créer le profil d'autorisation.

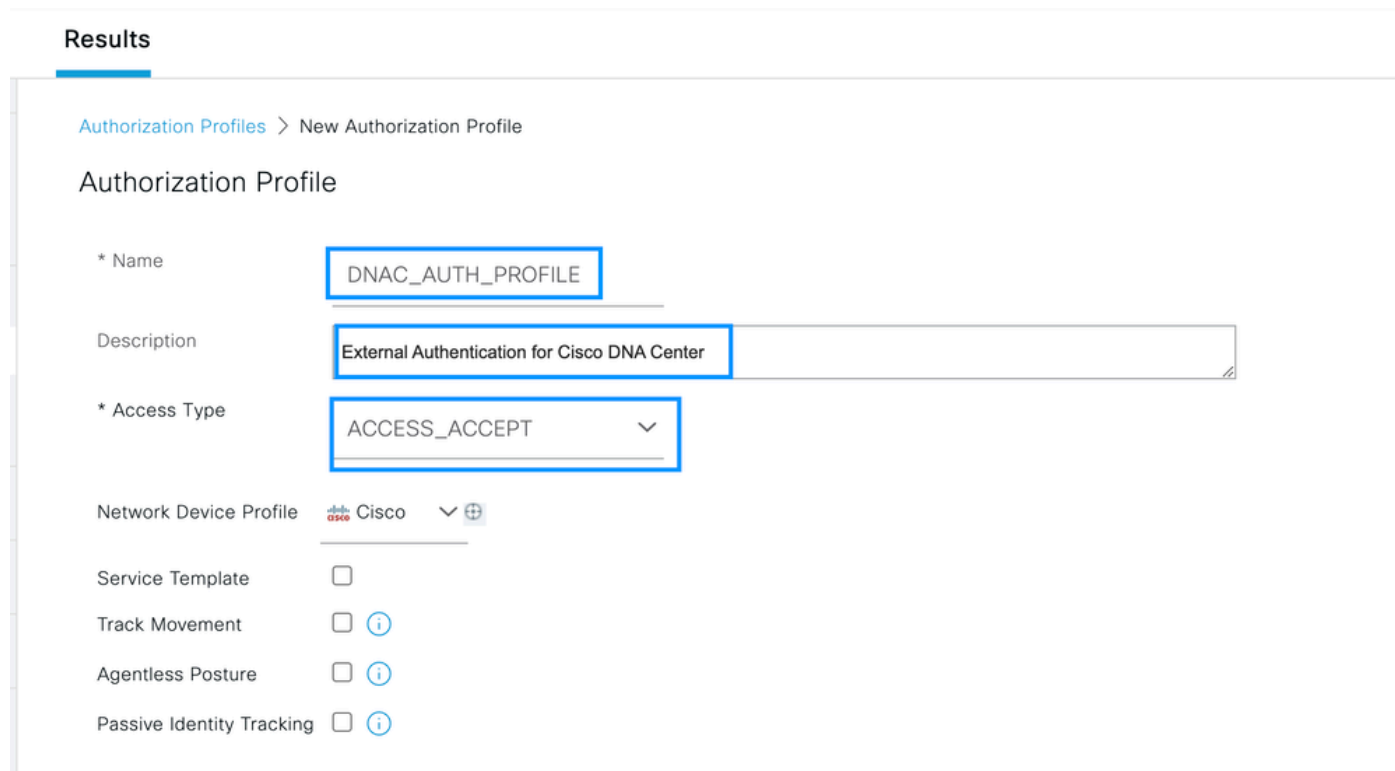
Assurez-vous que vous êtes sous Authorization > Authorization Profiles, puis sélectionnez l'option Add.



The screenshot shows the Cisco ISE interface for 'Policy - Policy Elements' under the 'Results' tab. The left sidebar shows a navigation menu with 'Authorization' selected. The main area displays 'Standard Authorization Profiles' with a table of existing profiles. A blue box highlights the '+ Add' button, and a blue arrow points to it from the 'Authorization Profiles' menu item.

Name	Profile	Description
APs_19.5.0	Cisco	172_19_5_0-INFRA_VN
AuthTemplate	Cisco	
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the
CY_CAMPUS_MAC	Cisco	CY_CAMPUS_MAC
CY Guest profile	Cisco	CY Guest profile

Configurez Name, ajoutez une Description juste pour garder un enregistrement du nouveau Profile et assurez-vous que le Access Type est défini sur ACCES\_ACCEPT.



The screenshot shows the 'New Authorization Profile' configuration page in Cisco ISE. The 'Name' field is 'DNAC\_AUTH\_PROFILE', the 'Description' is 'External Authentication for Cisco DNA Center', and the 'Access Type' is 'ACCESS\_ACCEPT'. These fields are highlighted with blue boxes.

Authorization Profile

\* Name: DNAC\_AUTH\_PROFILE

Description: External Authentication for Cisco DNA Center

\* Access Type: ACCESS\_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:  (i)

Agentless Posture:  (i)

Passive Identity Tracking:  (i)



Faites défiler vers le bas et configurez les paramètres d'attributs avancés.

Dans la colonne de gauche, recherchez l'option cisco-av-pair et sélectionnez-la.

Dans la colonne de droite, tapez manuellement Role=SUPER-ADMIN-ROLE.

Une fois qu'il ressemble à l'image ci-dessous, cliquez sur Submit.

### Advanced Attributes Settings

Cisco:cisco-av-pair = Role=SUPER-ADMIN-ROLE

### Attributes Details

Access Type = ACCESS\_ACCEPT  
cisco-av-pair = Role=SUPER-ADMIN-ROLE

Étape 4. Sur le serveur ISE, accédez à Work Centers > Profiler > Policy Sets, pour configurer la politique d'authentification et d'autorisation.

Identifiez la stratégie par défaut et cliquez sur la flèche bleue pour la configurer.

The screenshot shows the Cisco ISE interface for configuring Policy Sets. The 'Default' policy set is selected, and a blue arrow points to the configuration icon (gear) for this policy set.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
⊗	Wire-dot1x		Wired_802.1X	internal_user	0	⚙️	➔
⊗	MAB		Wired_MAB	Default Network Access	0	⚙️	➔
✅	Default	Default policy set		Default Network Access	180517	⚙️	➔

Dans l'ensemble de stratégies par défaut, développez la stratégie d'authentification et sous la section Default, développez les options et assurez-vous qu'elles correspondent à la configuration ci-dessous.

**Cisco ISE** Work Centers - Profiler

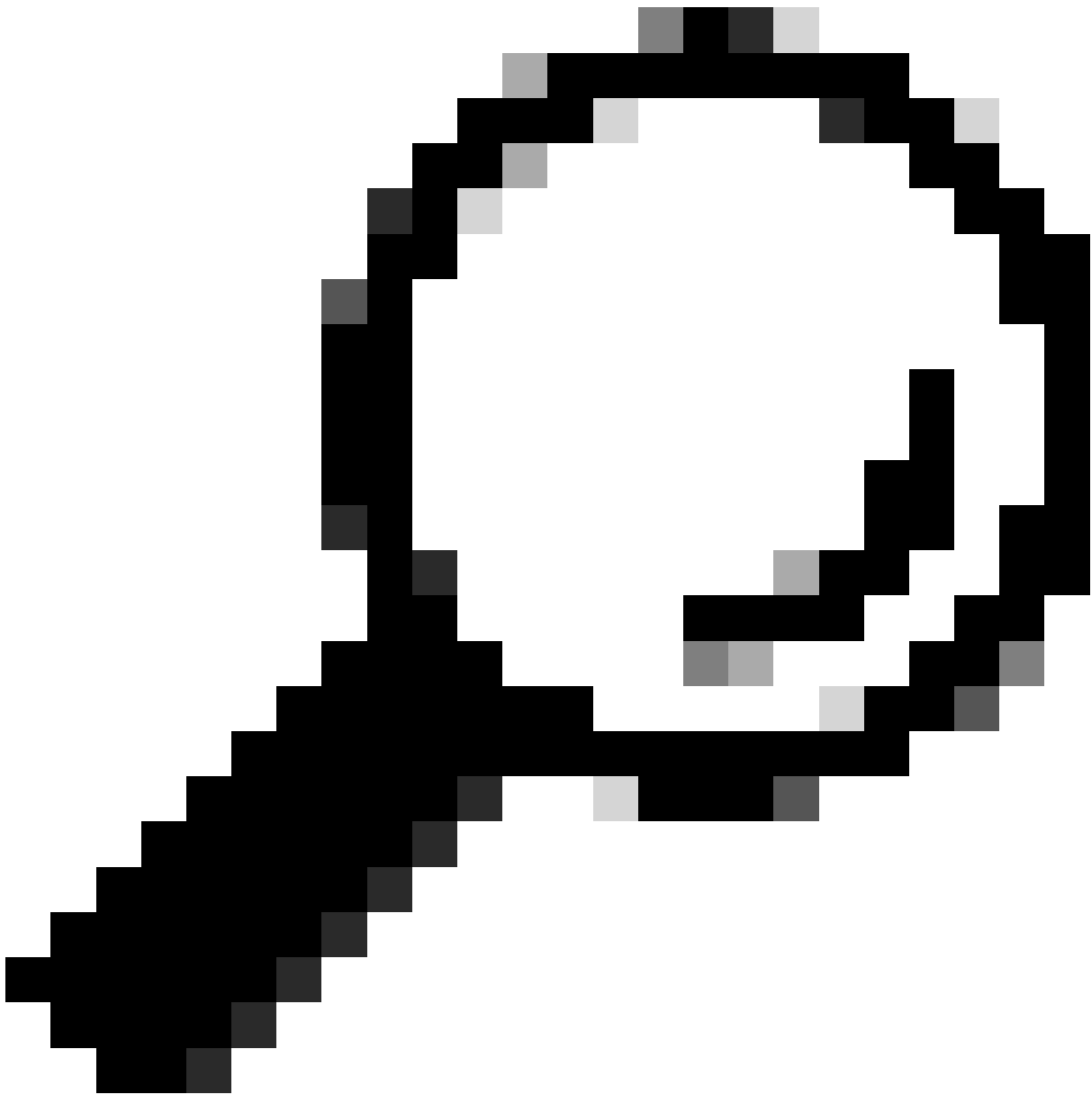
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies **More**

Policy Sets -> Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	4556	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	0	⚙️
✓	Default		All_User_ID_Stores Options If Auth fail REJECT If User not found REJECT If Process fail DROP	62816	⚙️



Conseil : REJECT configuré sur les 3 options fonctionne également

---

Dans l'ensemble de stratégies par défaut, développez la stratégie d'autorisation et sélectionnez l'icône Ajouter pour créer une nouvelle condition d'autorisation.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies **More**

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

⌵ Authorization Policy (25)

⊕ Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
⊕						

Configurez un nom de règle, puis cliquez sur l'icône Ajouter pour configurer la condition.

Cisco ISE Work Centers - Profiler

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies **More**

Policy Sets → Default Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	180617

> Authentication Policy (3)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

⌵ Authorization Policy (26)

⊕ Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
✓	DNAC-SUPER-ADMIN-ROLE					

Dans le cadre de la condition, associez-la à l'adresse IP du périphérique réseau configurée à l'étape 2.

# Conditions Studio

## Library

Search by Name



- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- CY\_Campus
- CY\_CAMPUS\_MAC
- CY\_Campus\_voice
- CY\_Guest
- EAP-MSCHAPv2
- ...

## Editor

Network Access-Device IP Address

Equals 10.88.244.151

Set to 'Is not'

Duplicate Save

NEW | AND | OR

Close

Use

Cliquez sur Enregistrer.

Enregistrez-le en tant que nouvelle condition de bibliothèque, et nommez-le comme vous le souhaitez, dans ce cas, il est nommé comme DNAC.



# Save condition

Save as existing Library Condition (replaces current version and impact all policies that use this condition)

Select from list



Save as a new Library Condition

DNAC

Description (optional)

Condition Description

Close

Save

Enfin, configurez le profil créé à l'étape 3.

The screenshot shows the Cisco ISE Profiler interface. At the top, there's a navigation bar with 'Cisco ISE' and 'Work Centers - Profiler'. Below that, a breadcrumb trail shows 'Policy Sets -> Default'. There are buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. A table lists policy sets with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. The 'Default' policy set is highlighted. Below this, there are expandable sections for 'Authentication Policy (3)', 'Authorization Policy - Local Exceptions', 'Authorization Policy - Global Exceptions', and 'Authorization Policy (25)'. The 'Authorization Policy (25)' section is expanded, showing a table with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. The 'DNAC-SUPER-ADMIN-ROLE' rule is selected, and its 'Profiles' column shows 'DNAC\_AUTH\_PROFILE' with a dropdown arrow.

Cliquez sur Enregistrer.

Étape 5. Connectez-vous à l'interface utilisateur graphique de Cisco DNA Center et accédez à Système > Utilisateurs et rôles > Authentification externe.

Cliquez sur l'option Enable External User et définissez l'attribut AAA comme Cisco-AVPair.

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 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 choo 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 cisc 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".

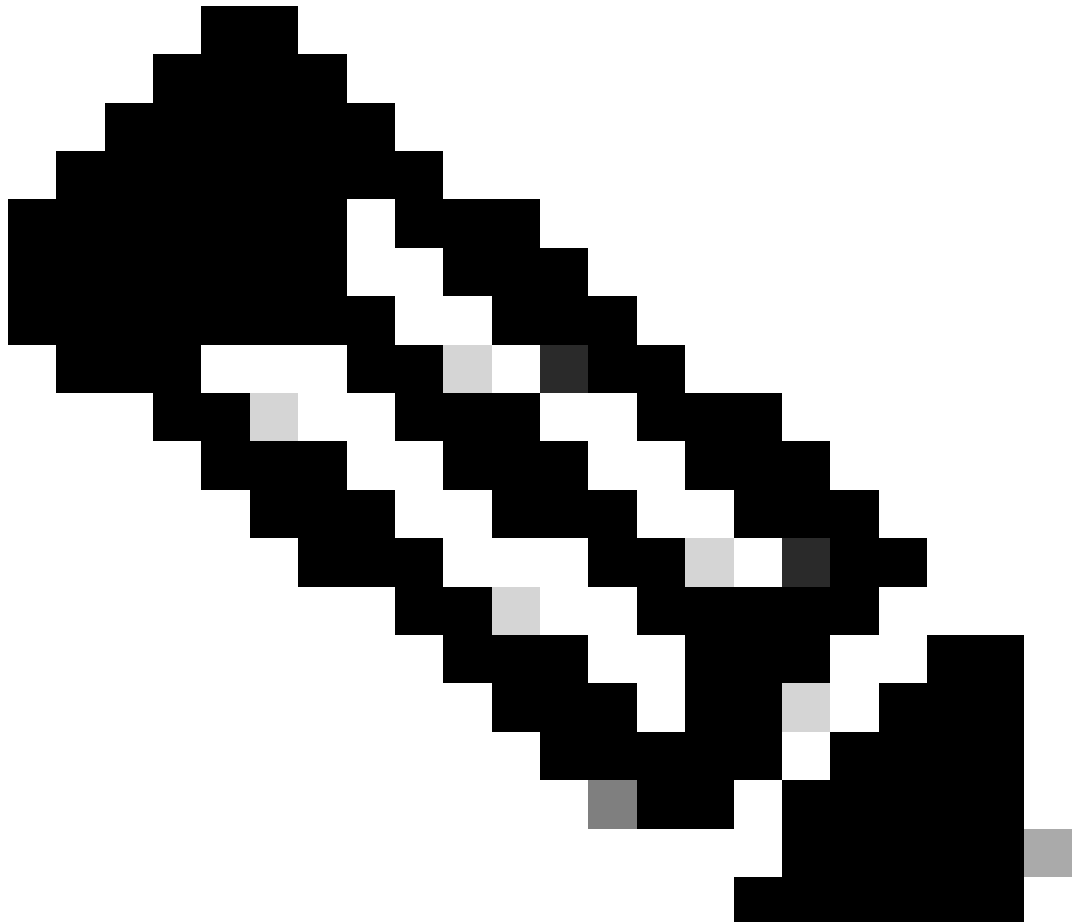
Enable External User ?

AAA Attribute

AAA Attribute  
Cisco-AVPair

Reset to Default

Update



Remarque : le serveur ISE utilise l'attribut Cisco-AVPair sur le serveur principal, de sorte

---

que la configuration de l'étape 3 est valide.

---

Faites défiler vers le bas pour afficher la section AAA Server(s) configuration. Configurez l'adresse IP du serveur ISE à l'étape 1 et le secret partagé configuré à l'étape 3.

Cliquez ensuite sur Afficher les paramètres avancés.

▼ AAA Server(s)

### Primary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

[View Advanced Settings](#)

Update

### Secondary AAA Server

IP Address

10.10.10.10



Shared Secret

\*\*\*\*\*

SHOW

Info

[View Advanced Settings](#)

Update

Vérifiez que l'option RADIUS est sélectionnée et cliquez sur le bouton Update sur les deux serveurs.



▼ AAA Server(s)

### Primary AAA Server

IP Address

██████████



Shared Secret

\*\*\*\*\*

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

Timeout (seconds)

4

### Secondary AAA Server

IP Address

██████████



Shared Secret

\*\*\*\*\*

SHOW

Info

Hide Advanced Settings

RADIUS

TACACS

Authentication Port

1812

Accounting Port

1813

Retries

3

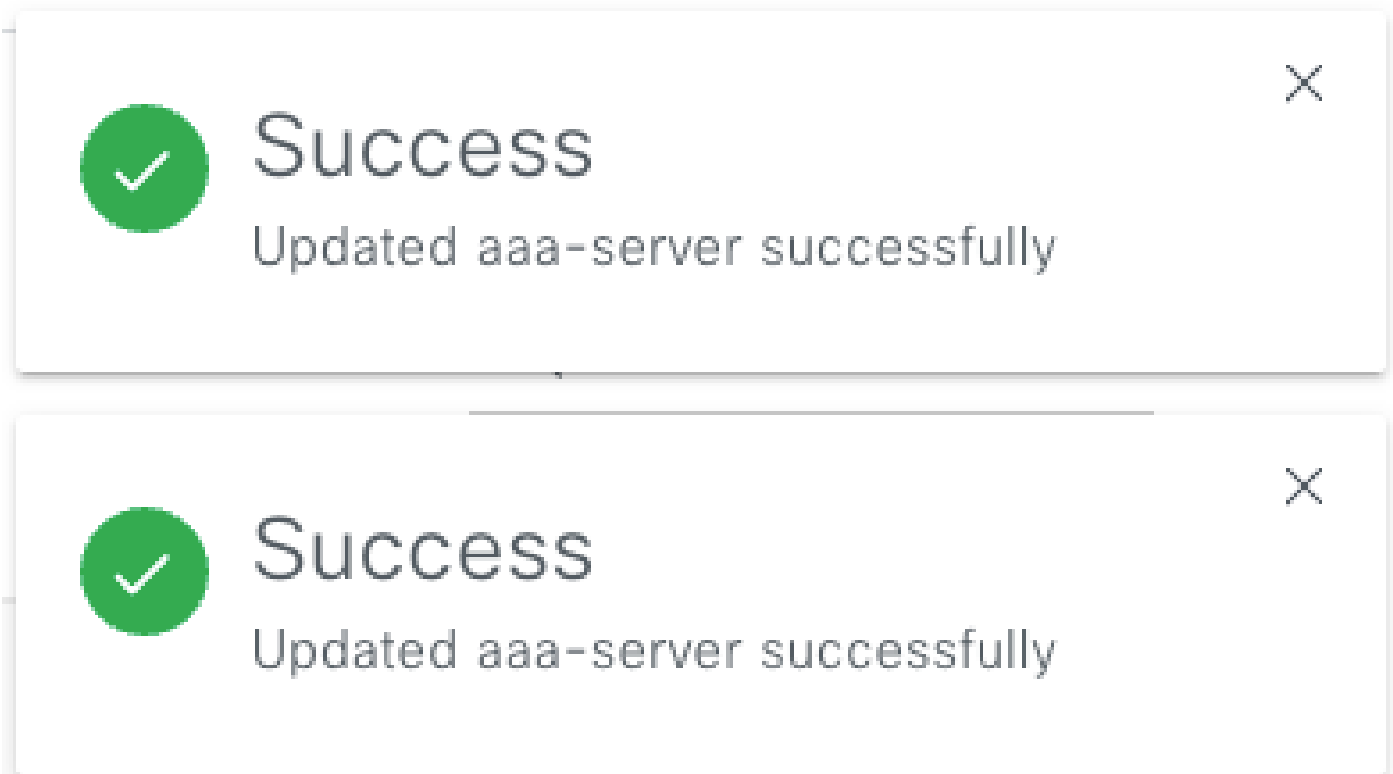
Timeout (seconds)

4

Update

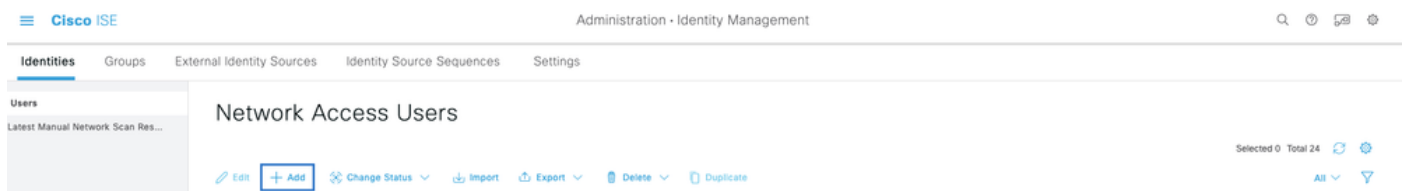
Update

Vous devez voir un message de réussite pour chaque.



Vous pouvez désormais vous connecter avec n'importe quelle identité ISE créée dans le menu ISE > Administration > Identity Management > Identities > Users.

Si aucun utilisateur n'est créé, connectez-vous à ISE, accédez au chemin ci-dessus et ajoutez un nouvel utilisateur d'accès au réseau.



## Vérifier

Chargement de l'interface graphique Cisco DNA Center et connectez-vous avec un utilisateur à partir d'identités ISE.



# Cisco DNA Center

The bridge to possible

✓ Success!

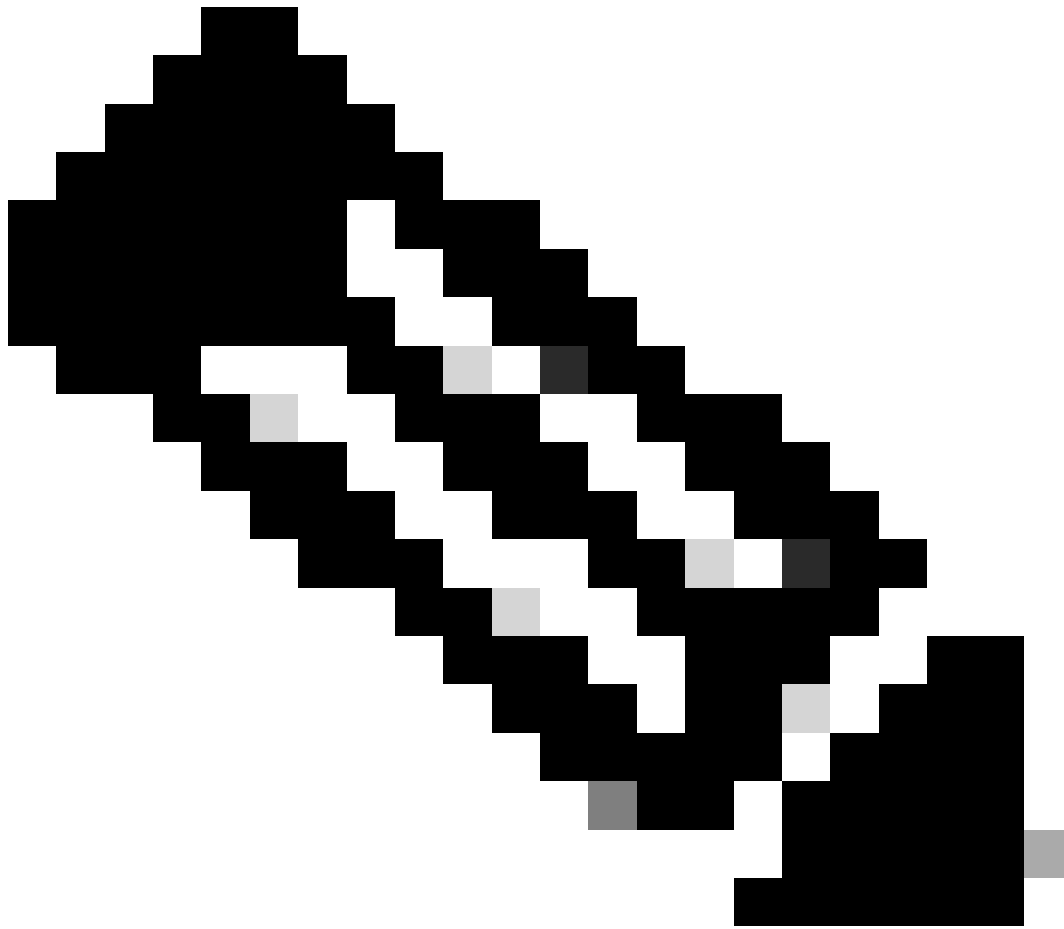
Username

test

Password

.....

Log In



Remarque : tout utilisateur disposant d'identités ISE peut se connecter maintenant. Vous pouvez ajouter plus de granularité aux règles d'authentification sur le serveur ISE.

---

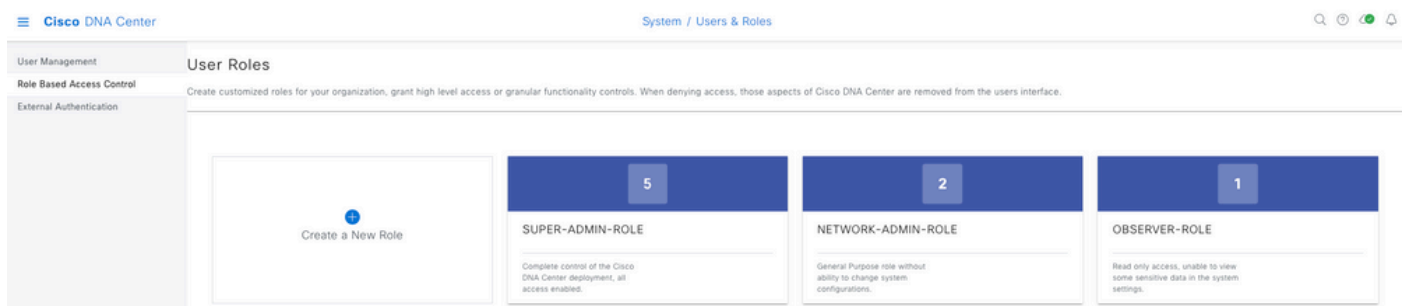
Une fois la connexion établie, le nom d'utilisateur s'affiche sur l'interface utilisateur graphique de Cisco DNA Center

## Welcome, test

Écran de bienvenue

## Plus de rôles

Vous pouvez répéter ces étapes pour chaque rôle sur Cisco DNA Center, comme par défaut, nous avons : SUPER-ADMIN-ROLE, NETWORK-ADMIN-ROLE et OBSERVER-ROLE.



Dans ce document, nous utilisons l'exemple de rôle SUPER-ADMIN-ROLE, néanmoins, vous pouvez configurer un profil d'autorisation sur ISE pour chaque rôle sur Cisco DNA Center, la seule considération est que le rôle configuré à l'étape 3 doit correspondre exactement (sensible à la casse) au nom du rôle sur Cisco DNA Center.

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.