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 :

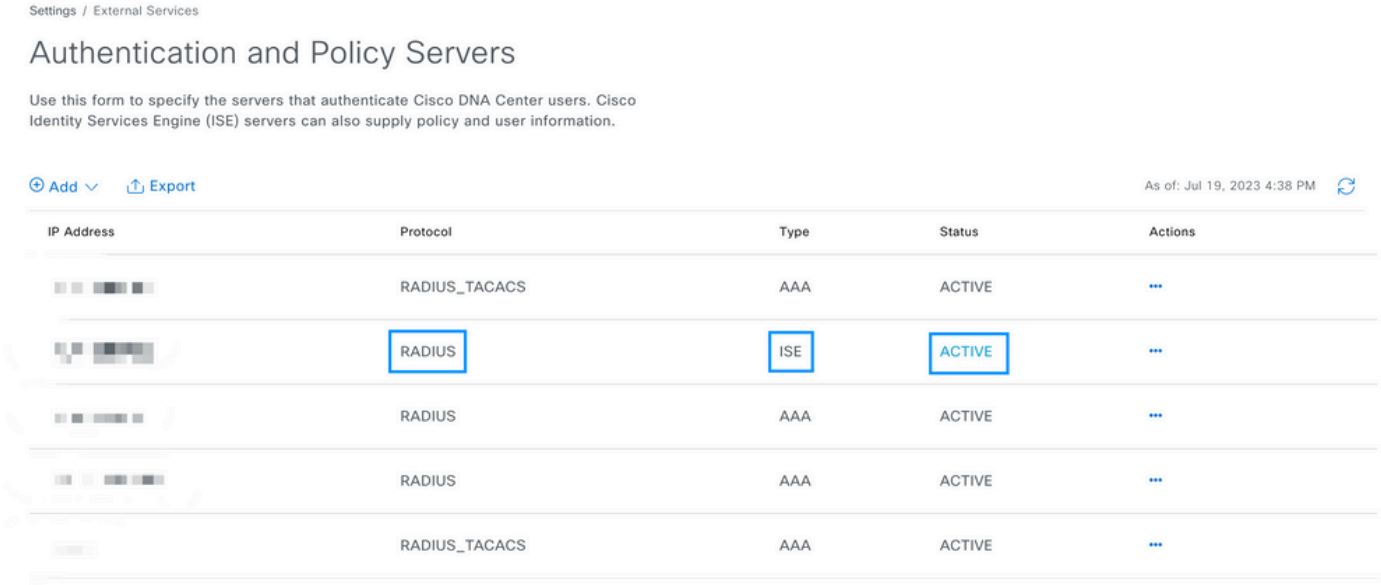
- Cisco DNA Center 2.3.5.x.
- Cisco ISE version 3.1.

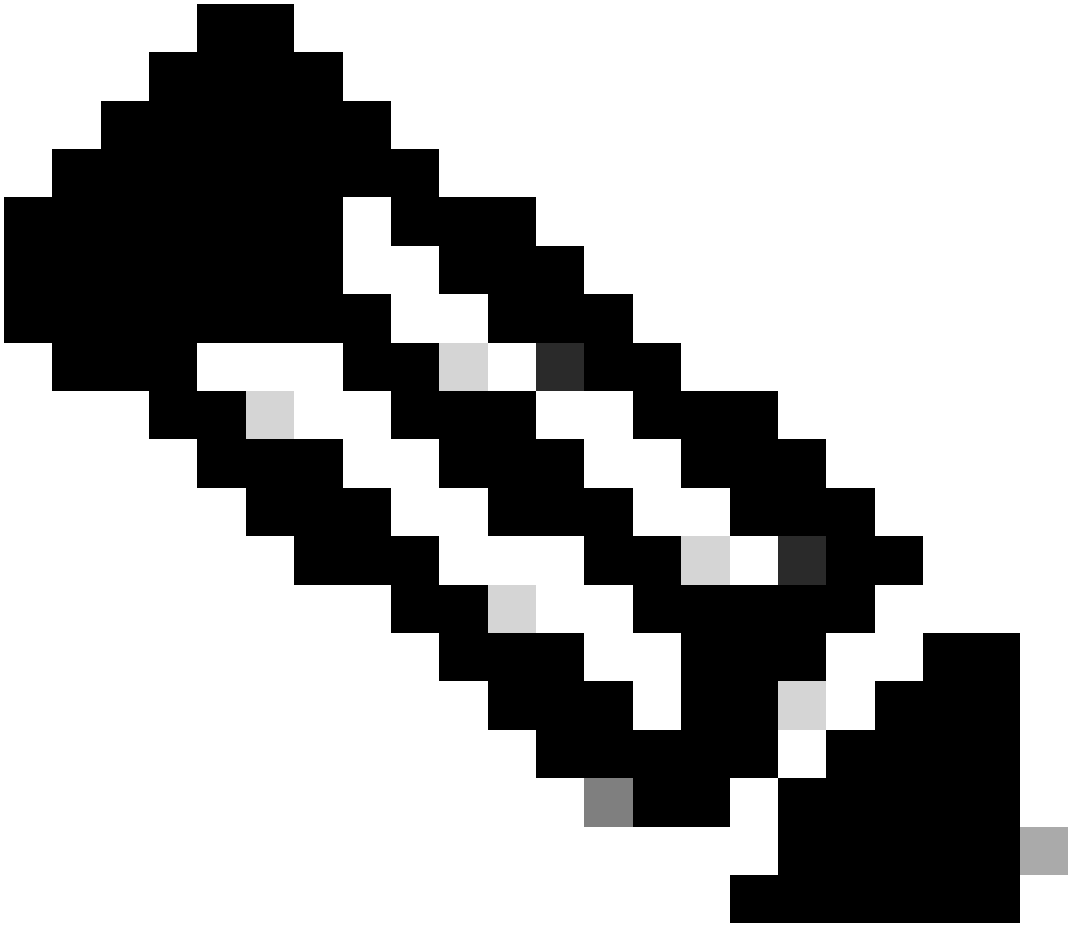
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Étape 1. Connectez-vous à l'interface utilisateur graphique de Cisco DNA Center et accédez àSystème > Paramètres > Serveurs d'authentification et de stratégie.

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



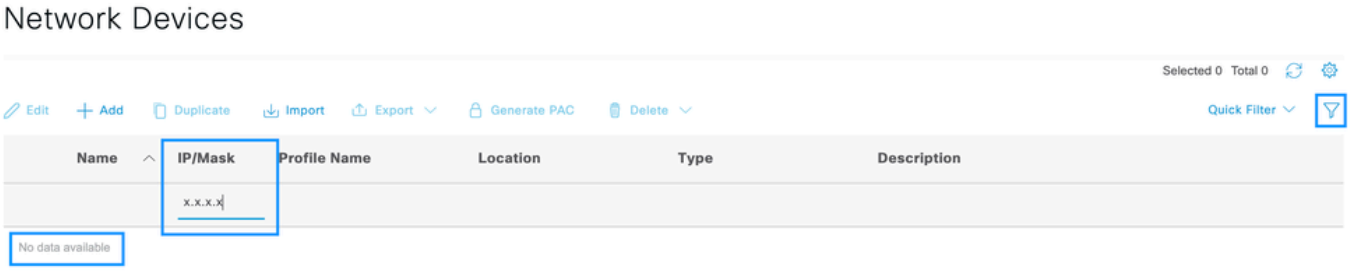


Remarque : Le protocole RADIUS_TACACS fonctionne pour ce document.

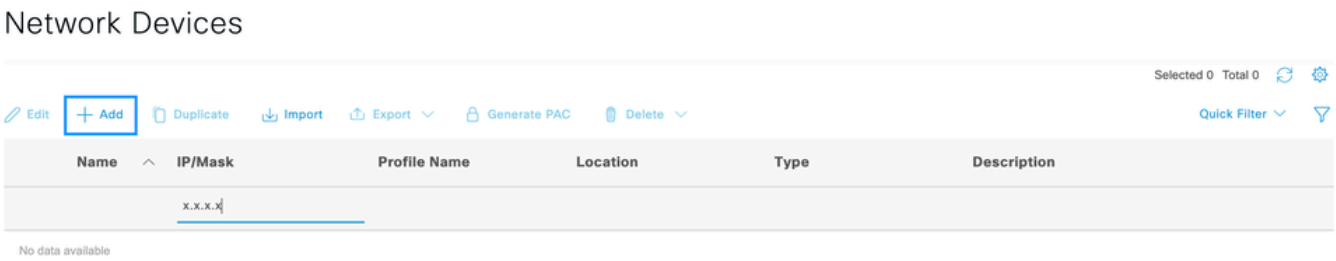
Avertissement : Si le serveur ISE n'est pas à l'état Actif, vous devez d'abord corriger l'intégration.

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

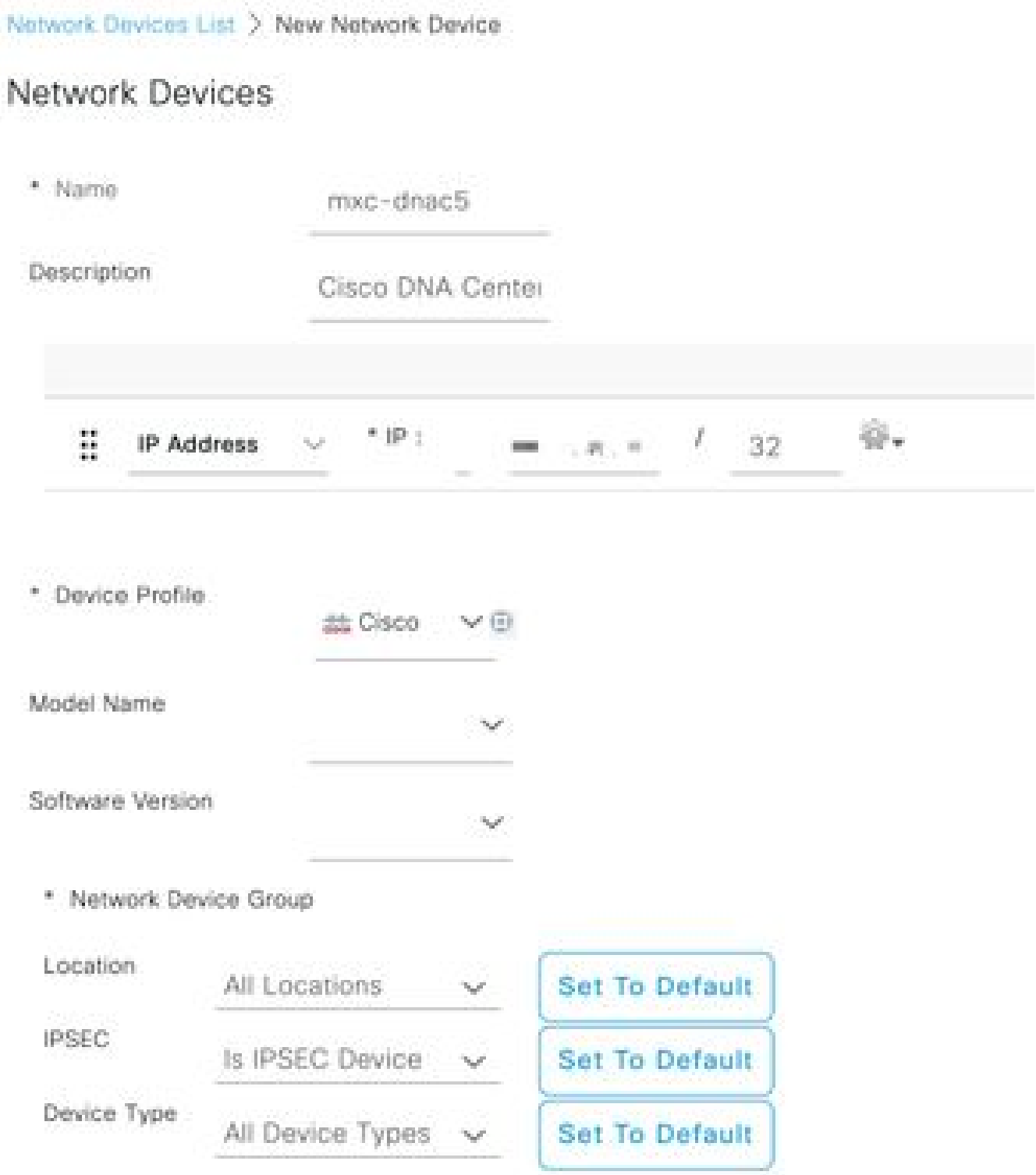
Si l'entrée est manquante, vous devez voir le message No data available.



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



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.



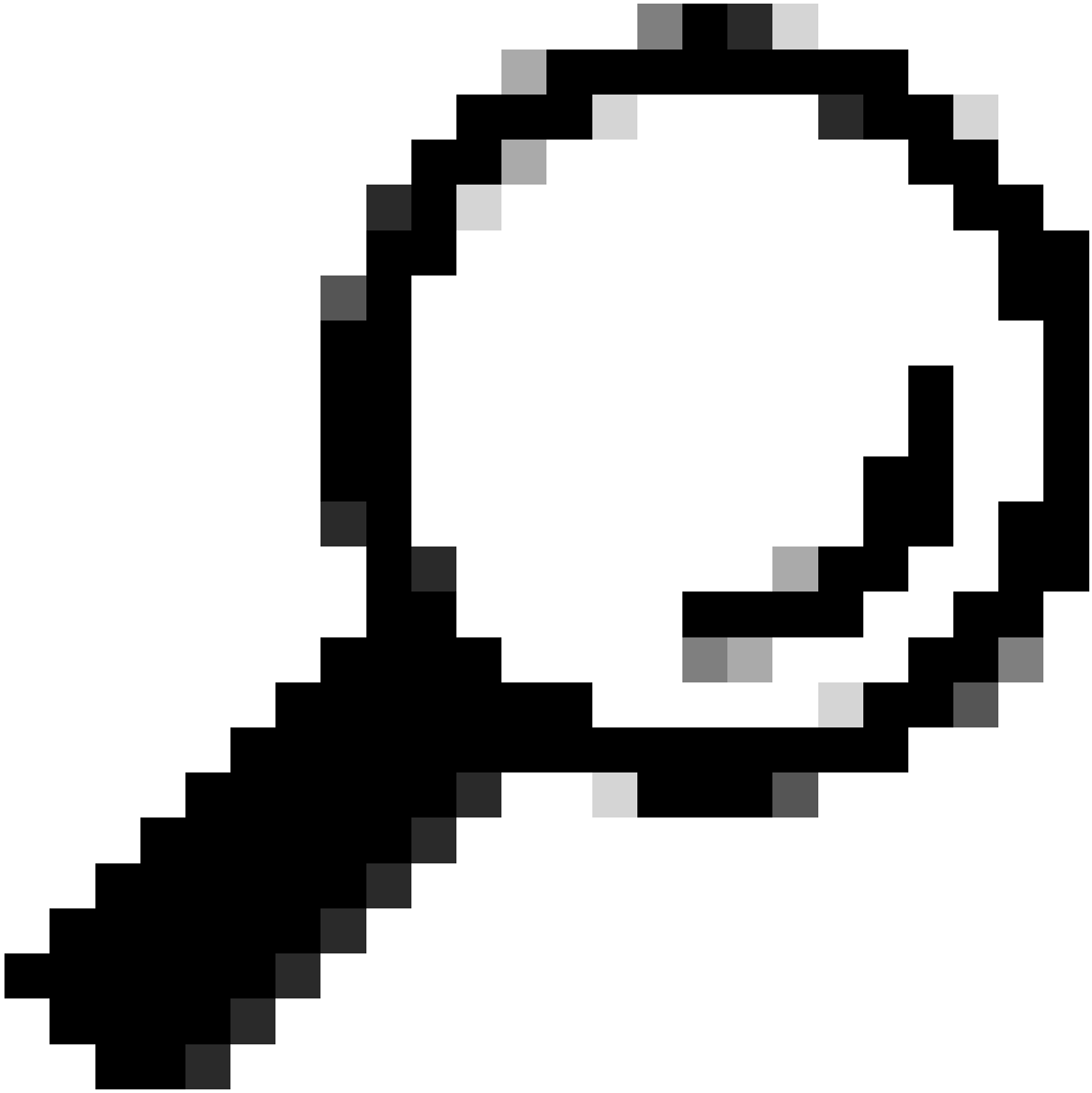
Faites défiler vers le bas et activez les paramètres d'authentification RADIUS en cliquant sur sa case à cocher et configurez un secret partagé.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

* Shared Secret ••••••••• Show

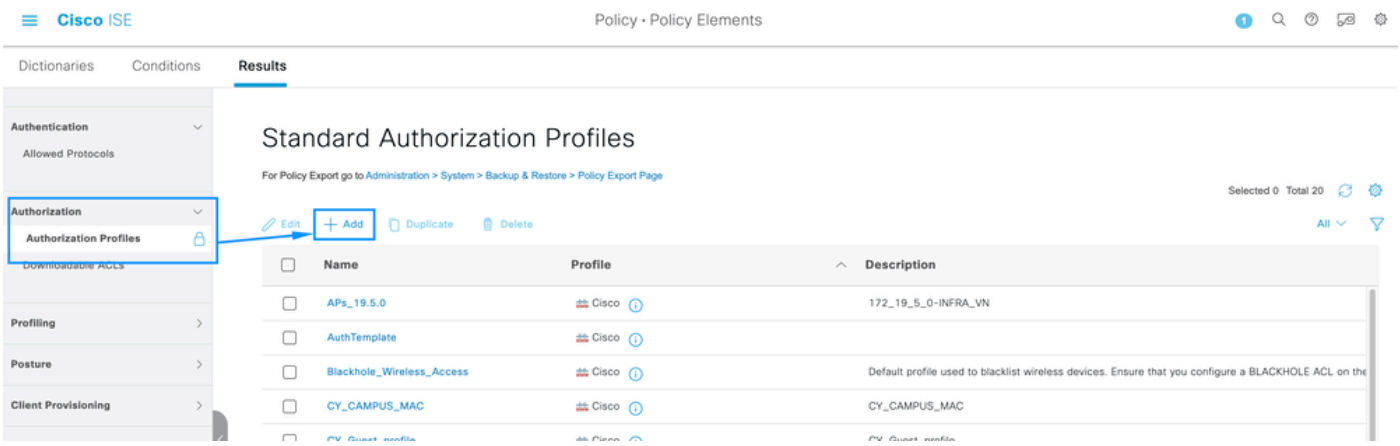


Conseil : Ce secret partagé sera nécessaire plus tard, donc enregistrez-le ailleurs.

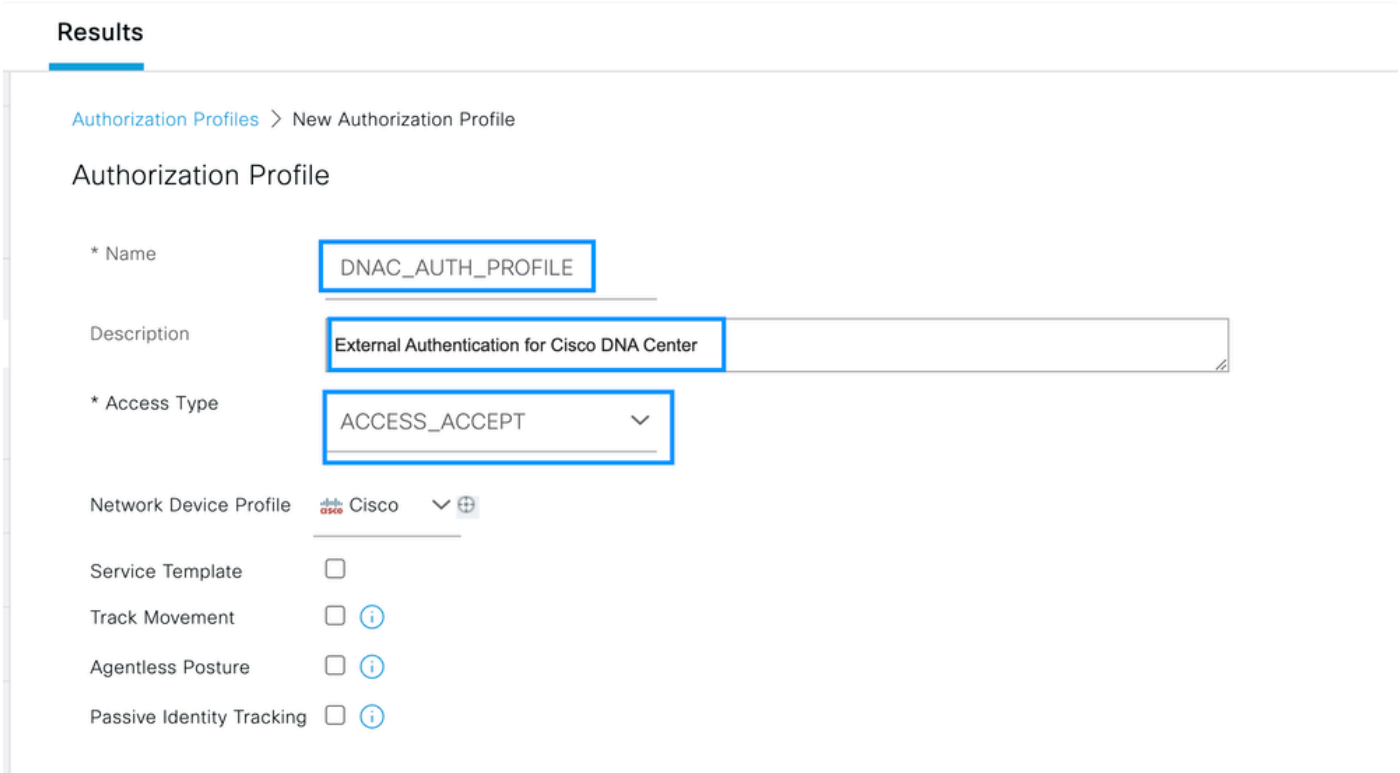
Ensuite, cliquez sur Submit.

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.



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.

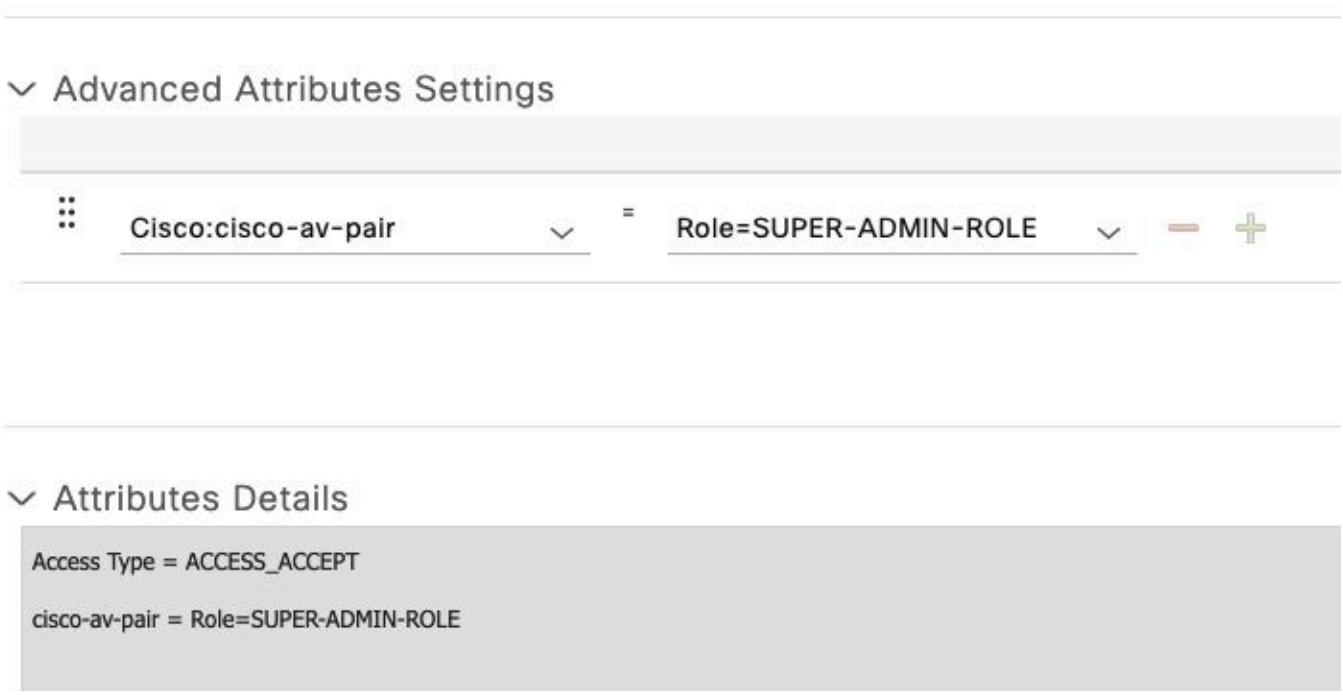


Faites défiler vers le bas et configurez les paramètres d'attributs avancés.

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

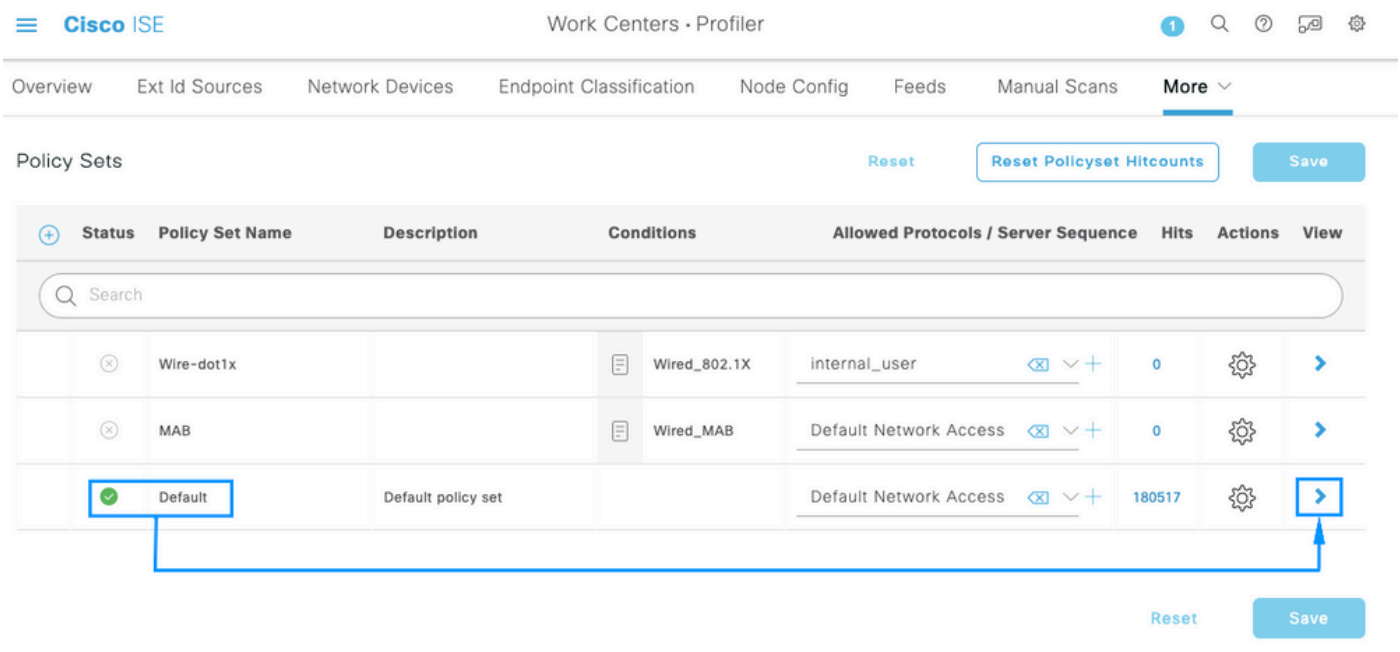
Dans la colonne de droite, tapez manuellement Role=SUPER-ADMIN-ROLE.

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

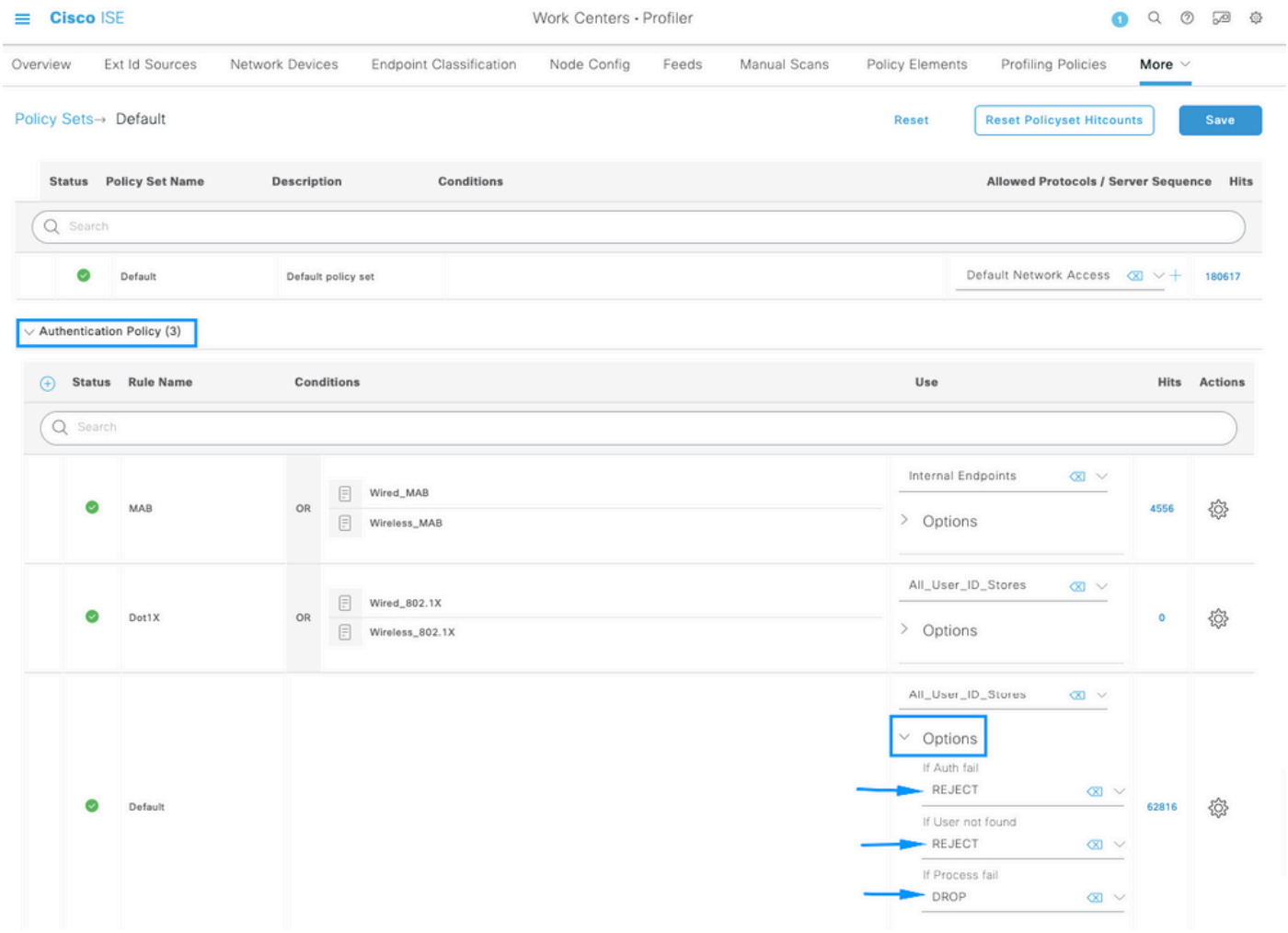


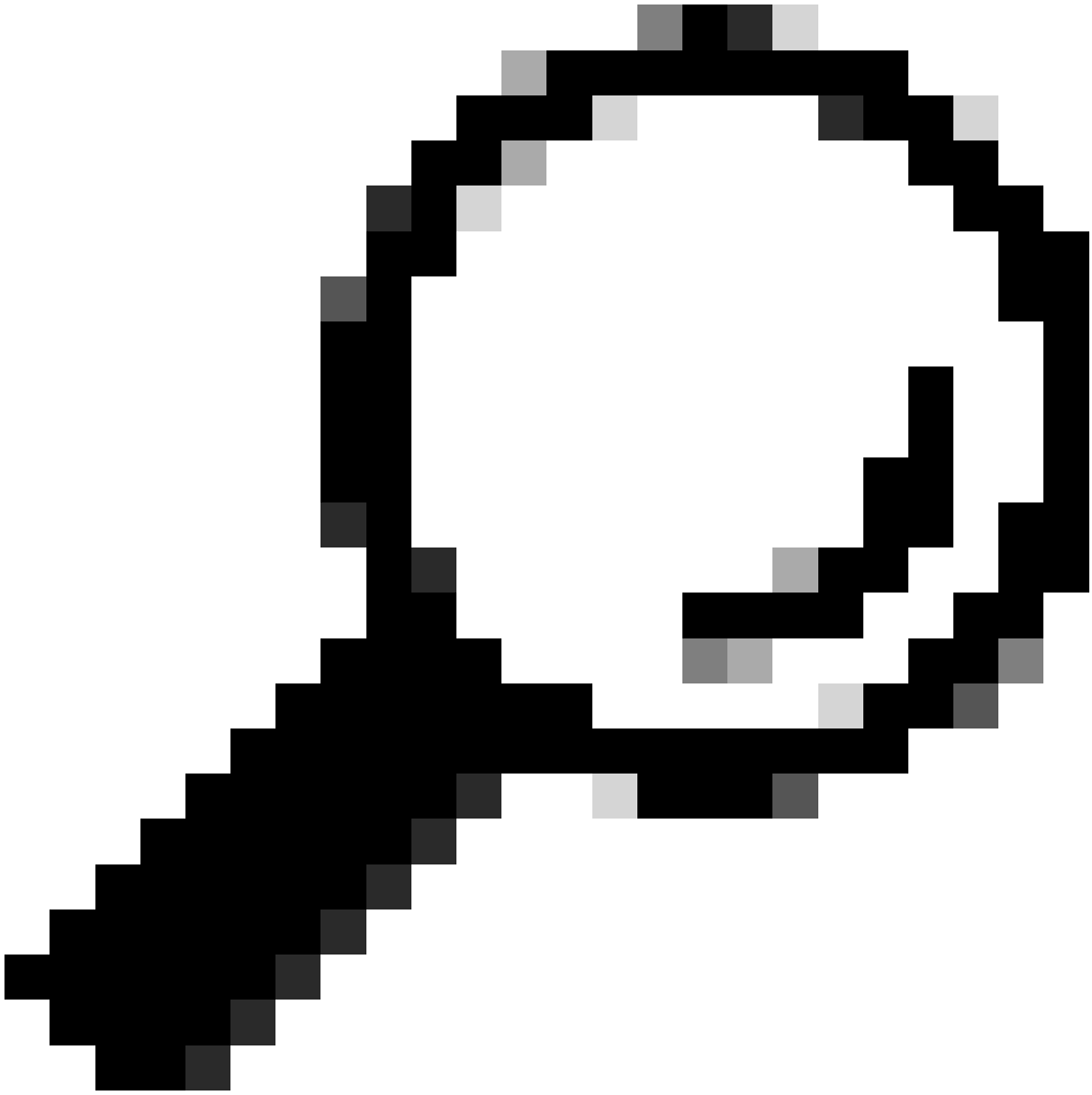
Étape 4. Sur le serveur ISE, accédez à Work Centers > Profiler > Policy Sets, pour configurer la politique d'authentification et d'autorisation.

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



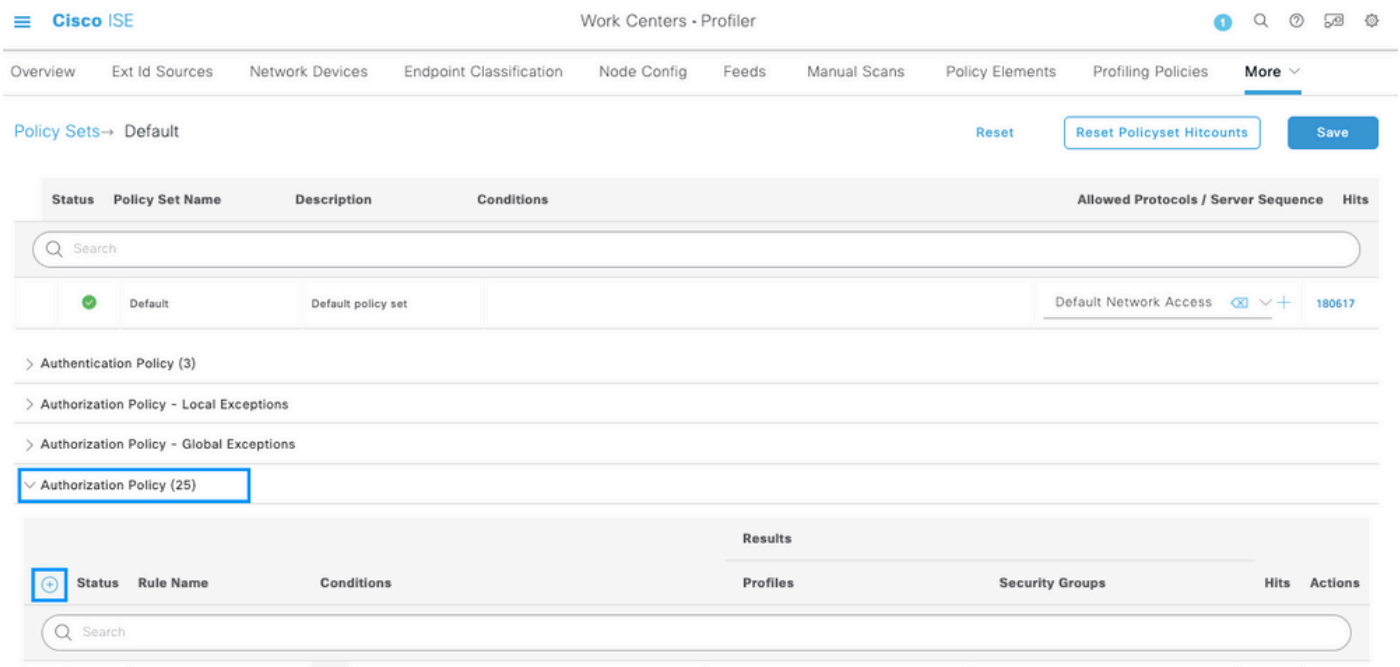
Dans l'ensemble de stratégies par défaut, développez la stratégie d'authentification et sous la section Default, développez les options et assurez-vous qu'elles correspondent à la configuration ci-dessous.



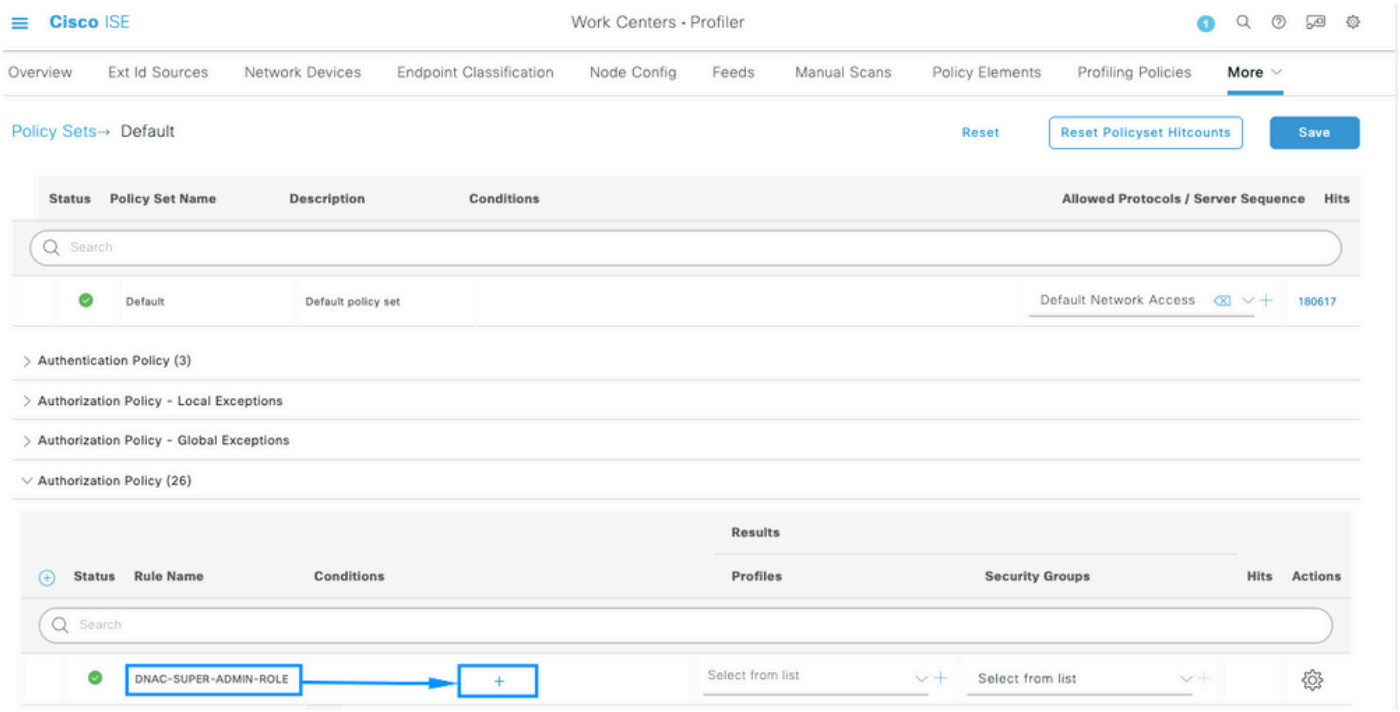


Conseil : REJECT configuré sur les 3 options fonctionne également

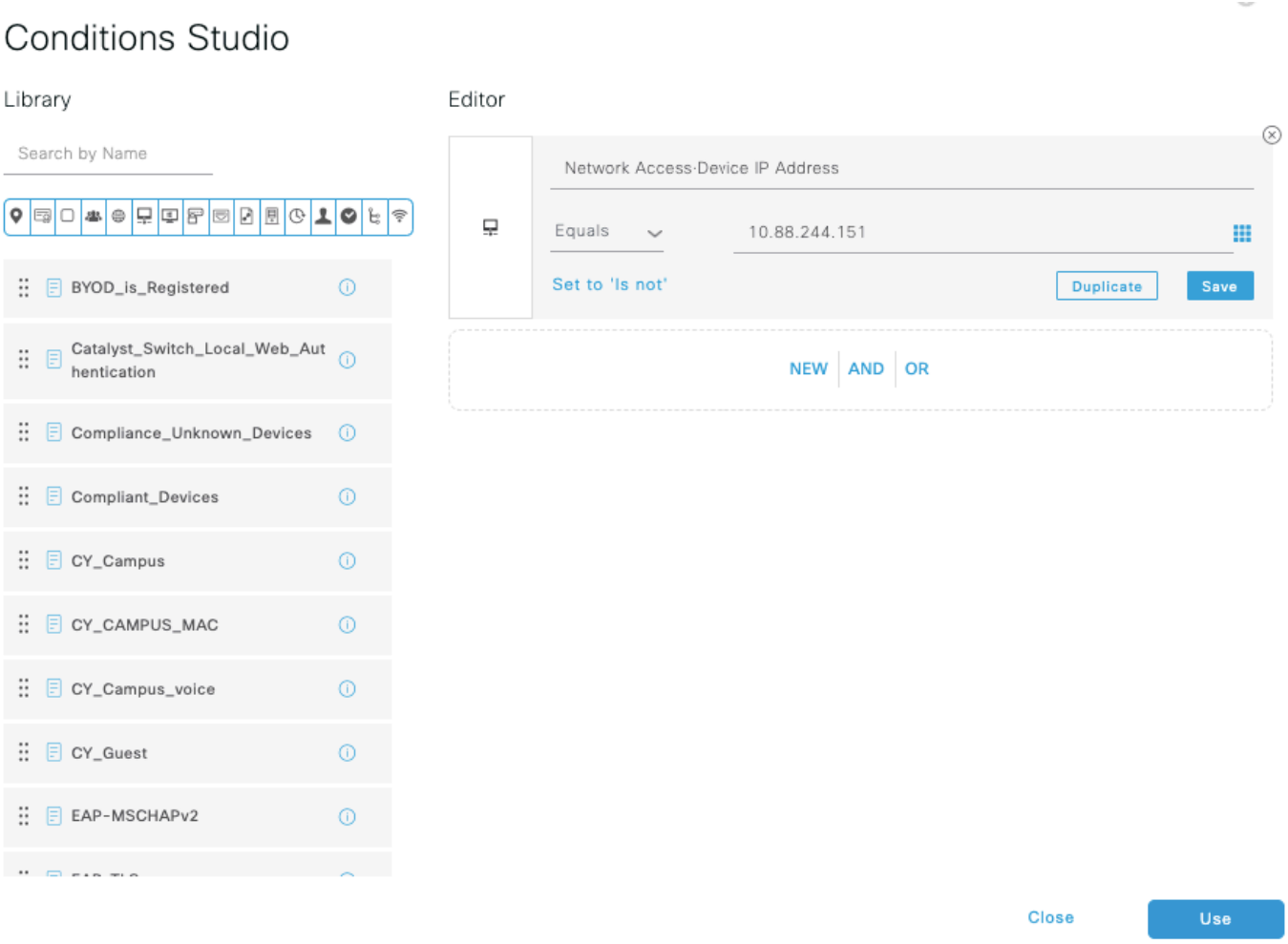
Dans l'ensemble de stratégies par défaut, développez la stratégie d'autorisation et sélectionnez l'icône Ajouter pour créer une nouvelle condition d'autorisation.



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

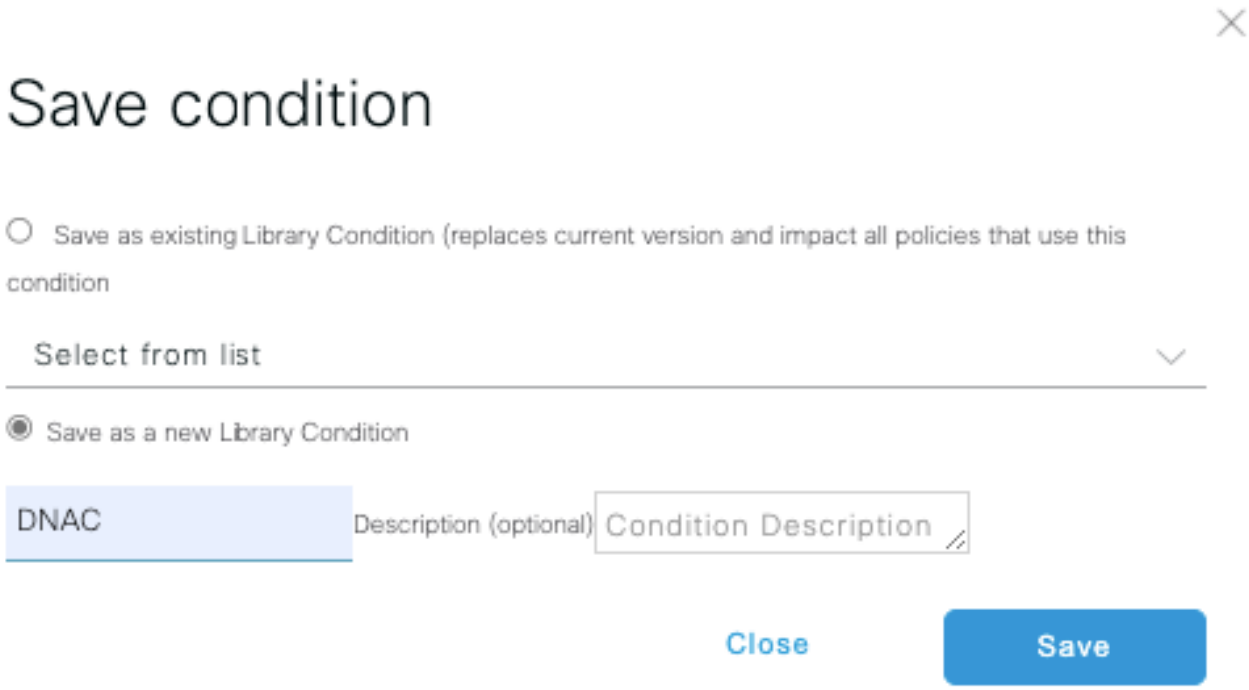


Dans le cadre de la condition, associez-la à l'adresse IP du périphérique réseau configurée à l'étape 2.

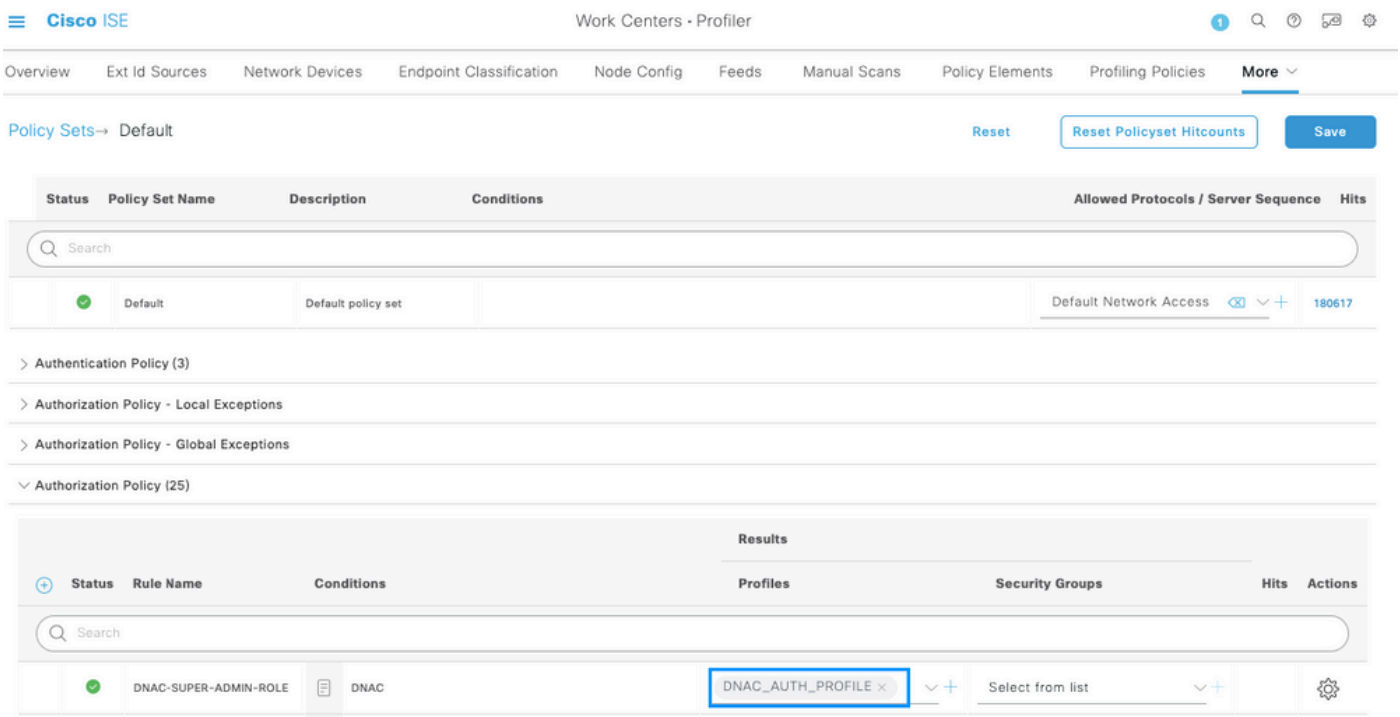


Cliquez sur Enregistrer.

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



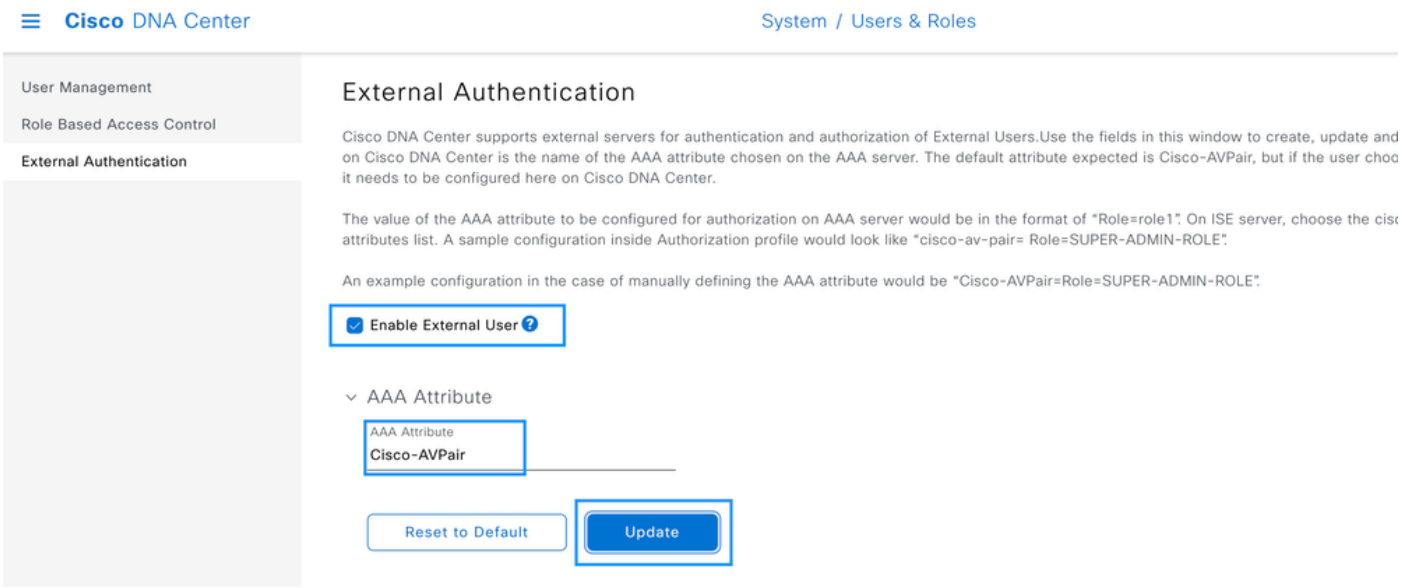
Enfin, configurez le profil créé à l'étape 3.

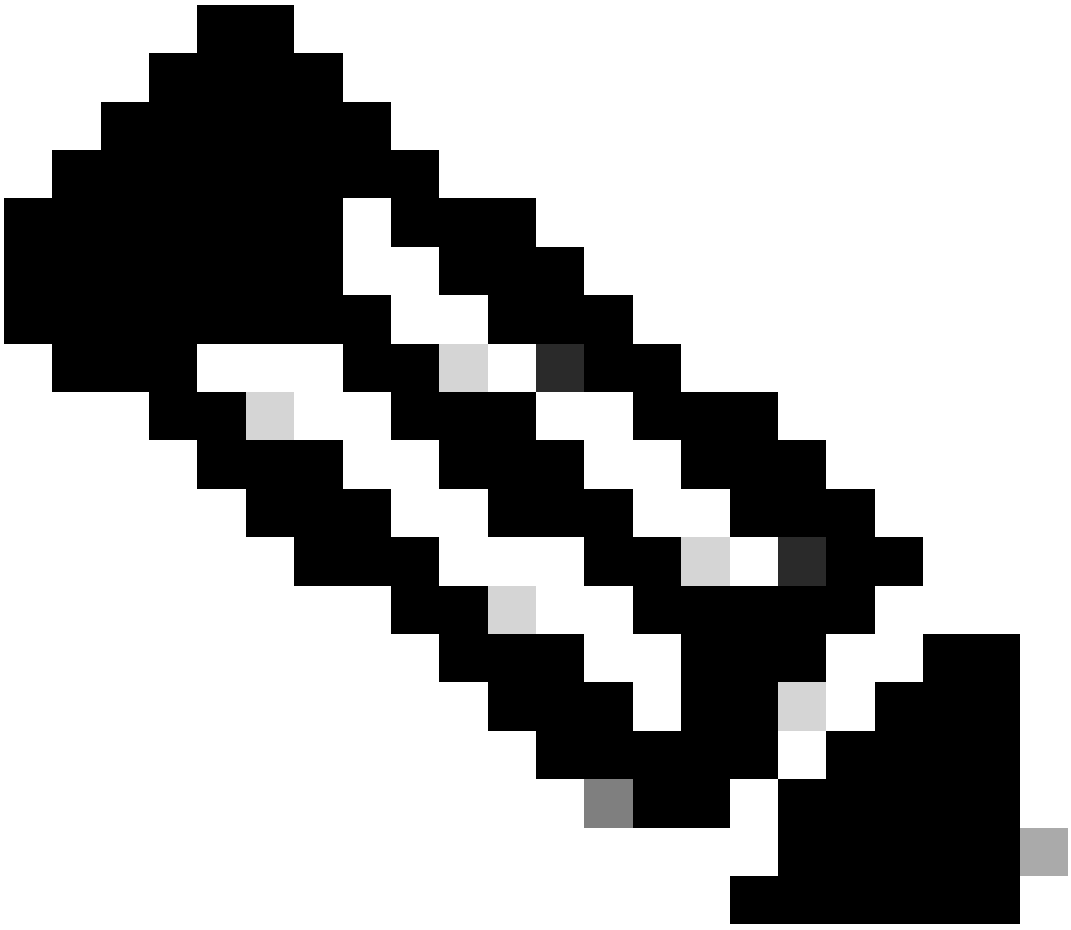


Cliquez sur Enregistrer.

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

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



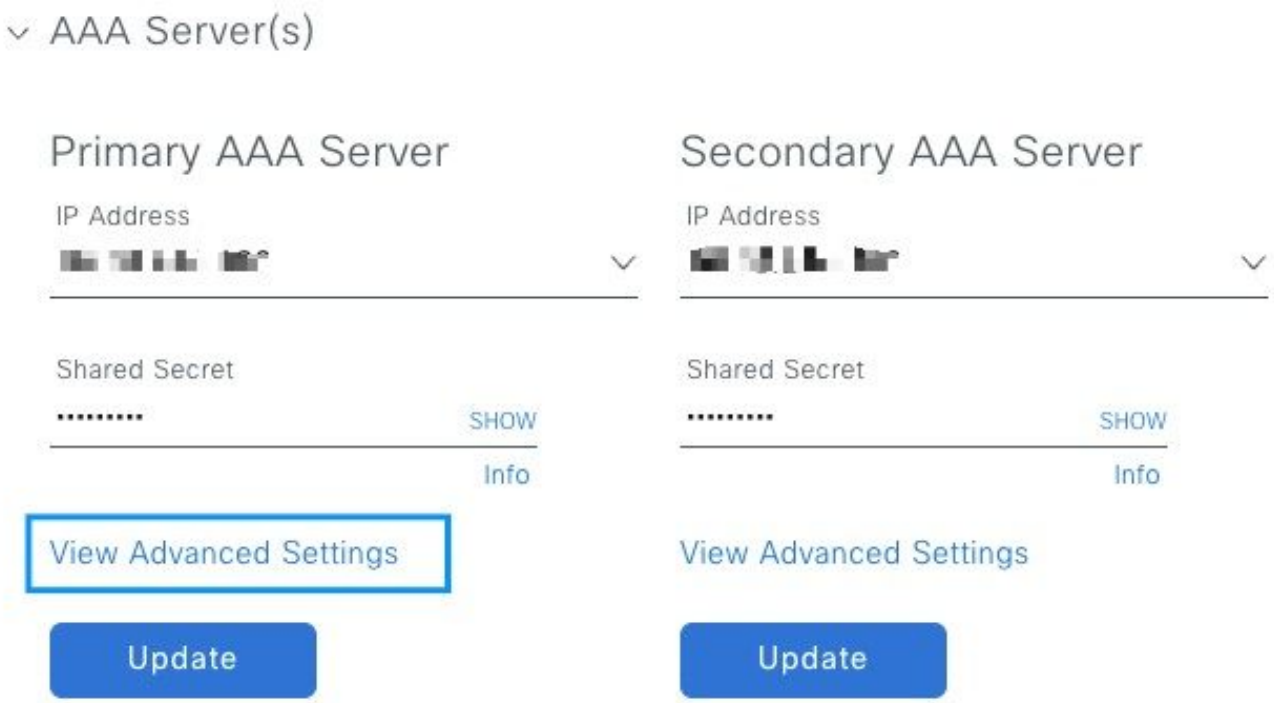


Remarque : Le serveur ISE utilise l'attribut Cisco-AVPair sur le serveur principal, de sorte

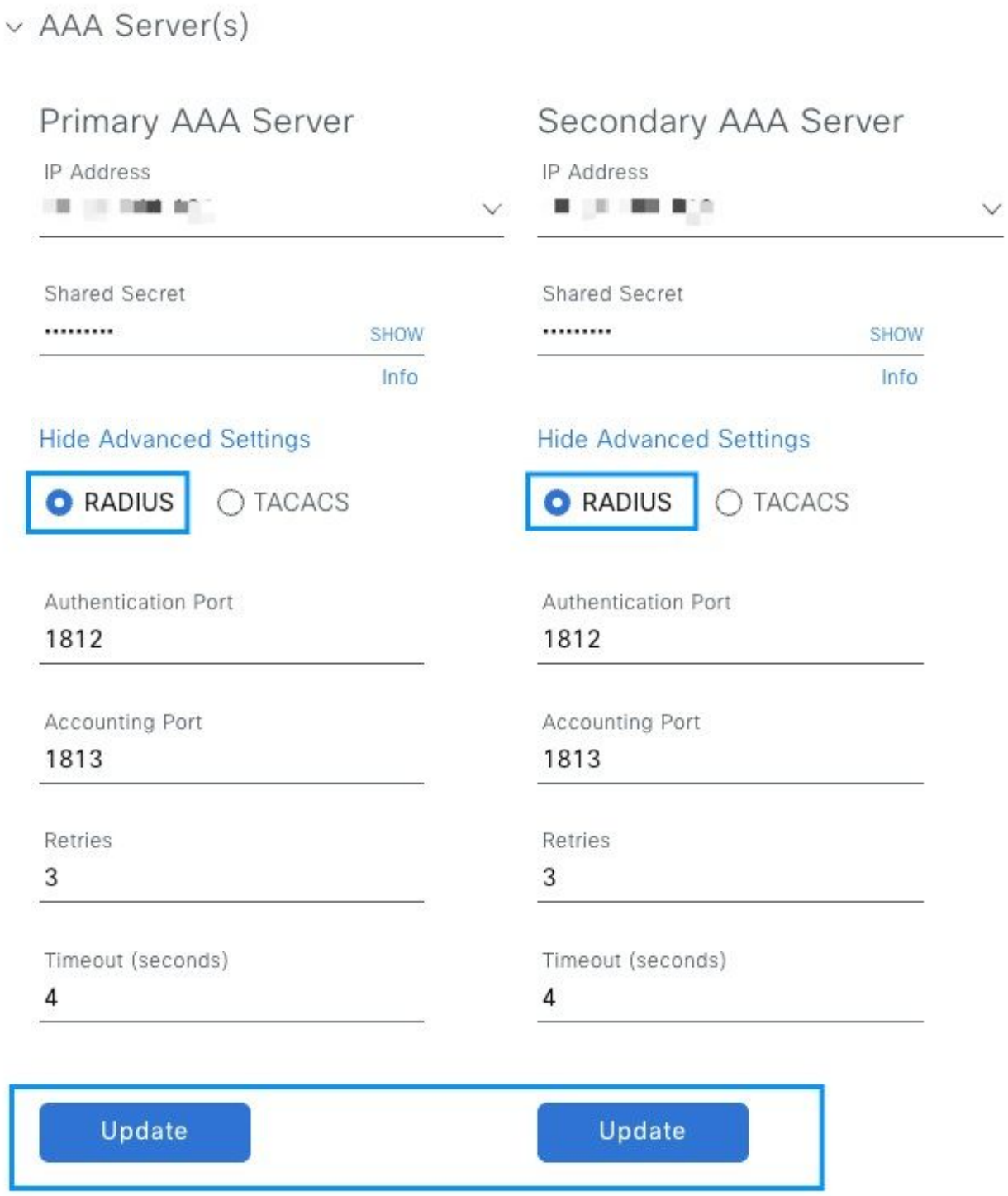
que la configuration de l'étape 3 est valide.

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.

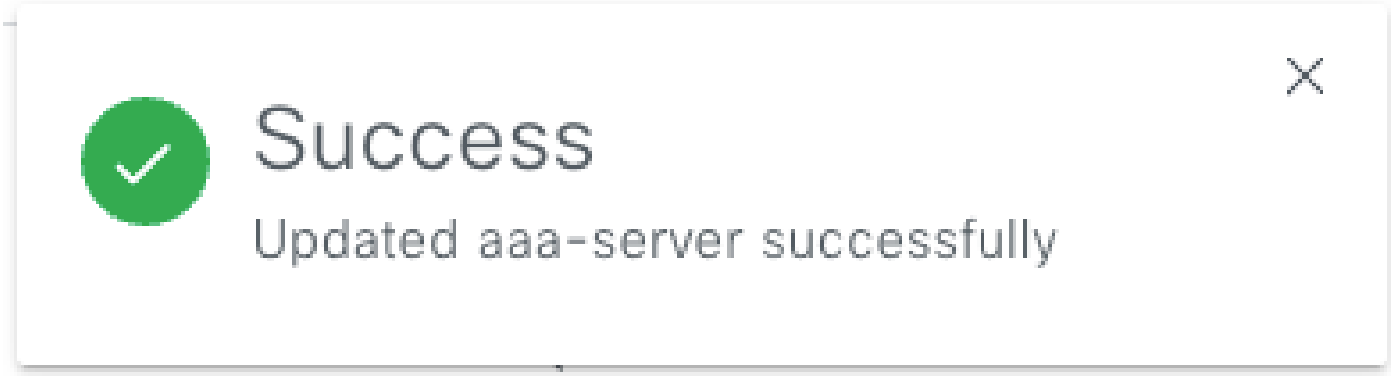
Cliquez ensuite sur Afficher les paramètres avancés.

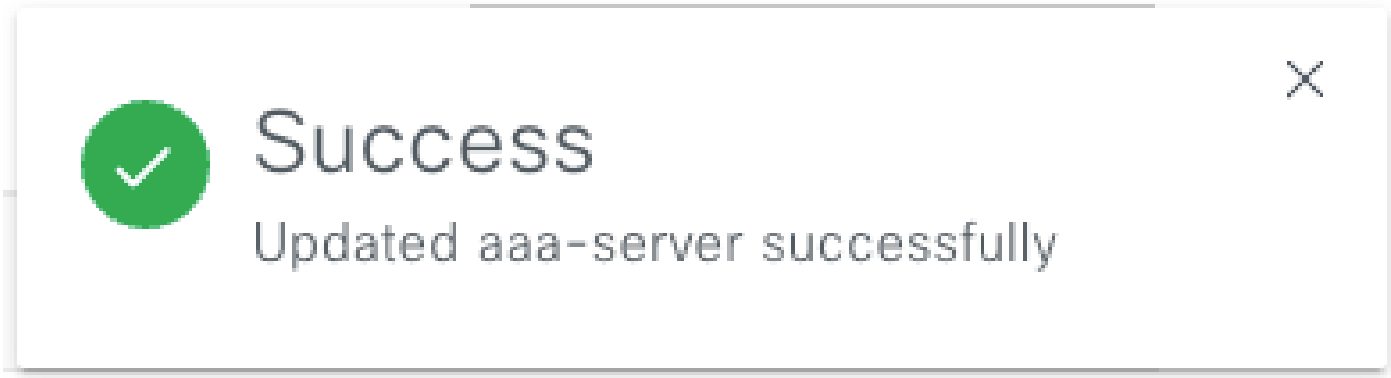


Vérifiez que l'option RADIUS est sélectionnée et cliquez sur le bouton Update sur les deux serveurs.



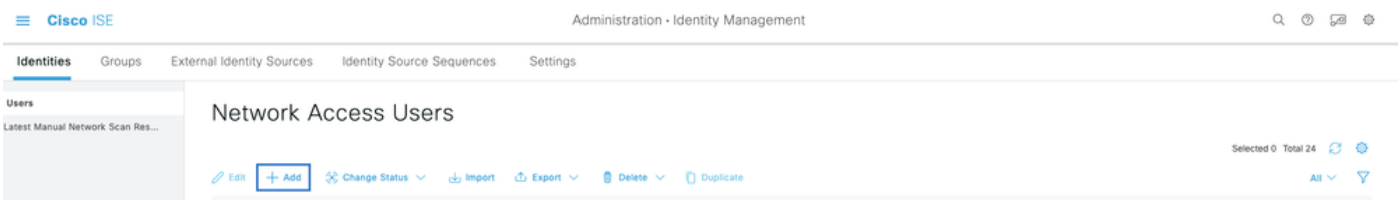
Vous devez voir un message de réussite pour chaque.





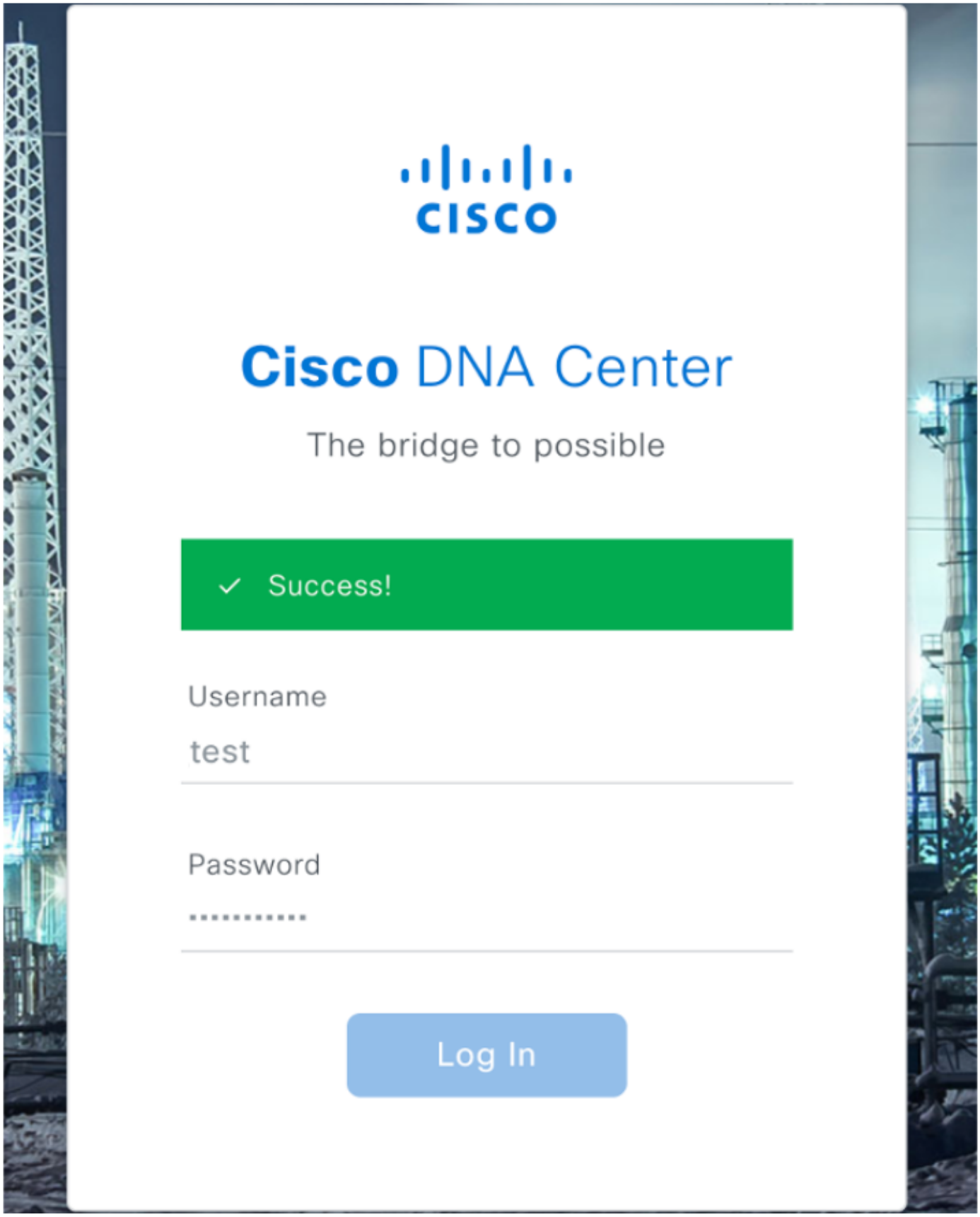
Vous pouvez désormais vous connecter avec n'importe quelle identité ISE créée dans le menu ISE > Administration > Identity Management > Identities > Users.

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

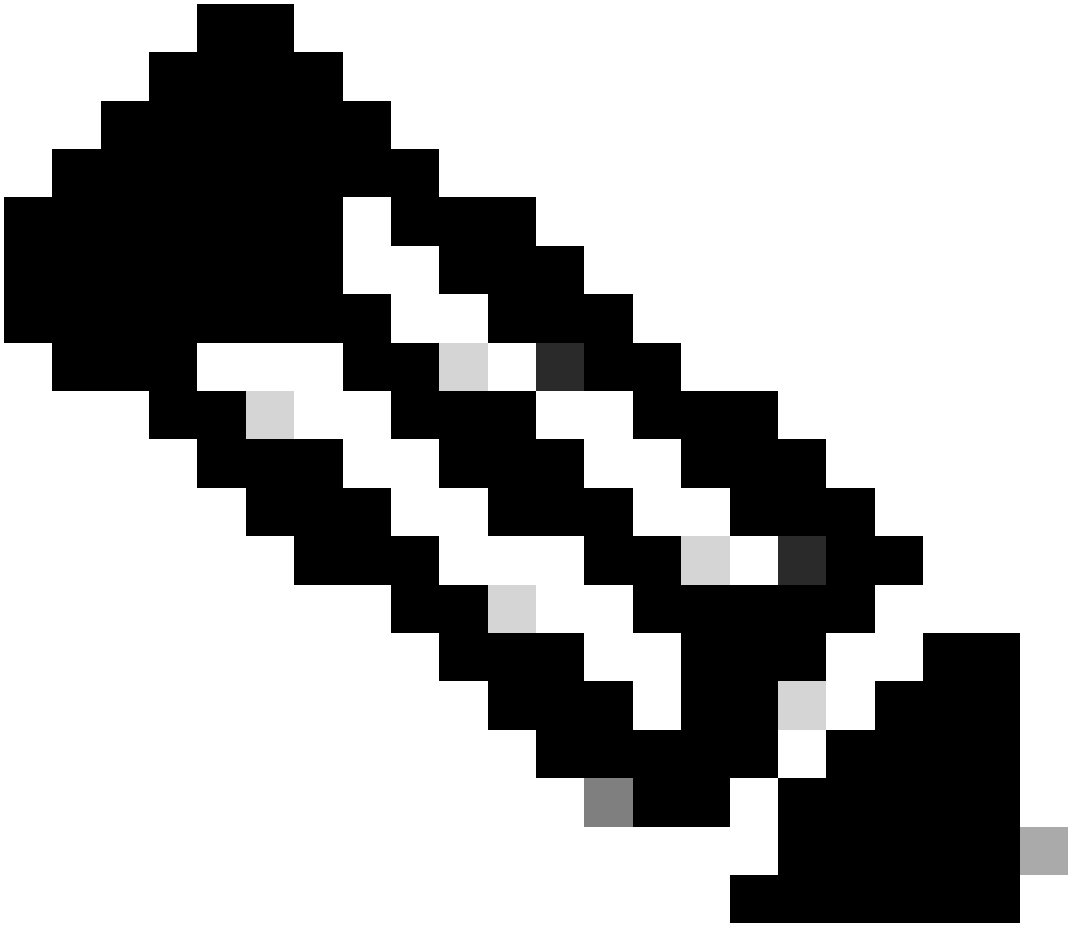


Vérifier

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

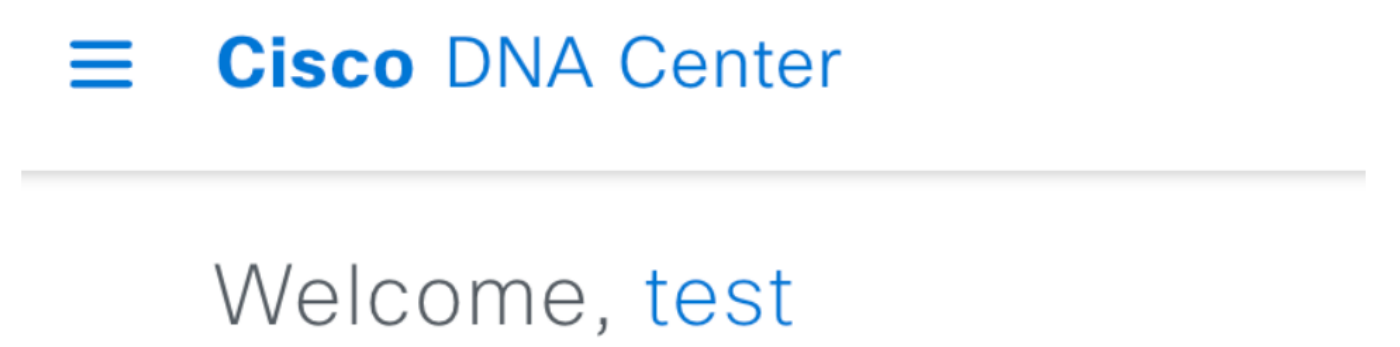


Connexion au centre ADN



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

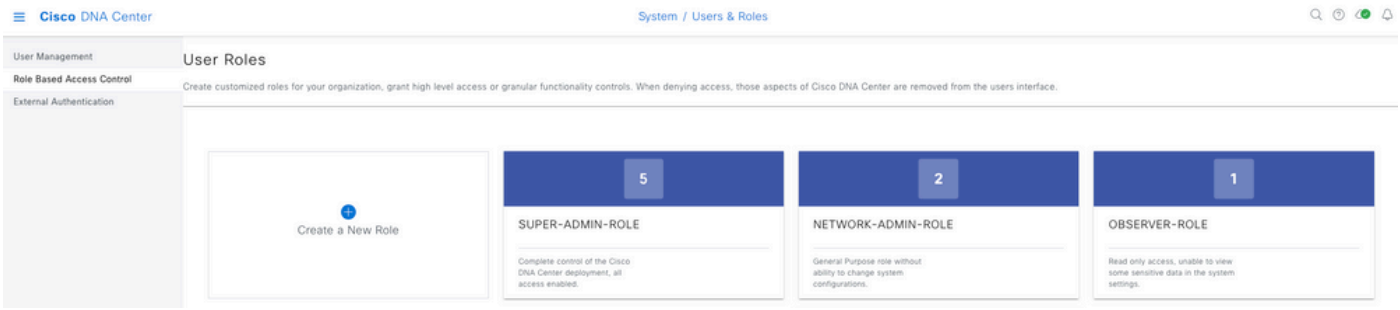
Une fois la connexion établie, le nom d'utilisateur s'affiche sur l'interface utilisateur graphique de Cisco DNA Center



Écran de bienvenue

Plus de rôles

Vous pouvez répéter ces étapes pour chaque rôle sur Cisco DNA Center, comme nous l'avons fait par défaut : 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.