

Configuration de l'authentification ISE Radius pour Secure Firewall Chassis Manager (FCM)

Table des matières

Introduction

Ce document décrit le processus de configuration de l'accès d'autorisation/authentification Radius pour Secure Firewall Chassis Manager avec ISE.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Gestionnaire de châssis de pare-feu sécurisé (FCM)
- Cisco Identity Services Engine (ISE)
- Authentification RADIUS

Composants utilisés

- Appareil de sécurité Cisco Firepower 4110 FXOS v2.12
- Correctif 4 de Cisco Identity Services Engine (ISE) v3.2

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

Configurations

Gestionnaire de châssis de pare-feu sécurisé

- Étape 1. Connectez-vous à l'interface utilisateur graphique du Firepower Chassis Manager.
- Étape 2. Accéder aux paramètres de la plate-forme

Overview Interfaces Logical Devices Security Engine **Platform Settings** System Tools Help admin

FPR4K-1-029A78B 172.16.0.130
 Model: Cisco Firepower 4110 Security Appliance | Version: 2.12(0.8) | Operational State: Operable | Chassis Uptime 00:06:02:19

CONSOLE MGMT USB
 Power 1 - Running | Power 2 - Removed

Network Module 1: 1, 3, 5, 7, 2, 4, 6, 8
 Network Module 2 : Empty
 Network Module 3 : Empty

FAULTS 3(3) CRITICAL | 0(0) MAJOR
INTERFACES 3 DOWN | 5 UP
INSTANCES 0 DOWN | 1 UP
LICENSE Smart Agent UNREGISTERED
INVENTORY 1(1) Security Engine | 6(6) Fans | 1(2) Power Supplies

Severity	Description	Cause	Occurrence	Time	Acknowledged
CRITICAL	FPGA version lower than 2.00 is detected. A critical upgrade from the firmwar...	fpga-upgrade-required	1	2022-02-20T22:32:45.641	no
CRITICAL	Network Module 3 removed when in online state. It is recommended to set m...	module-surprise-removal	1	2022-11-07T09:03:02.022	no

8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Étape 3. Dans le menu de gauche, cliquez sur AAA. Sélectionnez Radius et ajoutez un nouveau fournisseur RADIUS.

Overview Interfaces Logical Devices Security Engine **Platform Settings** System Tools Help admin

NTP
 SSH
 SNMP
 HTTPS
AAA
 Syslog
 DNS
 FIPS and Common Criteria
 Access List
 MAC Pool
 Resource Profiles
 Network Control Policy
 Chassis URL

LDAP **RADIUS** TACACS

Properties
 Timeout:* 5 Secs
 Retries:* 1

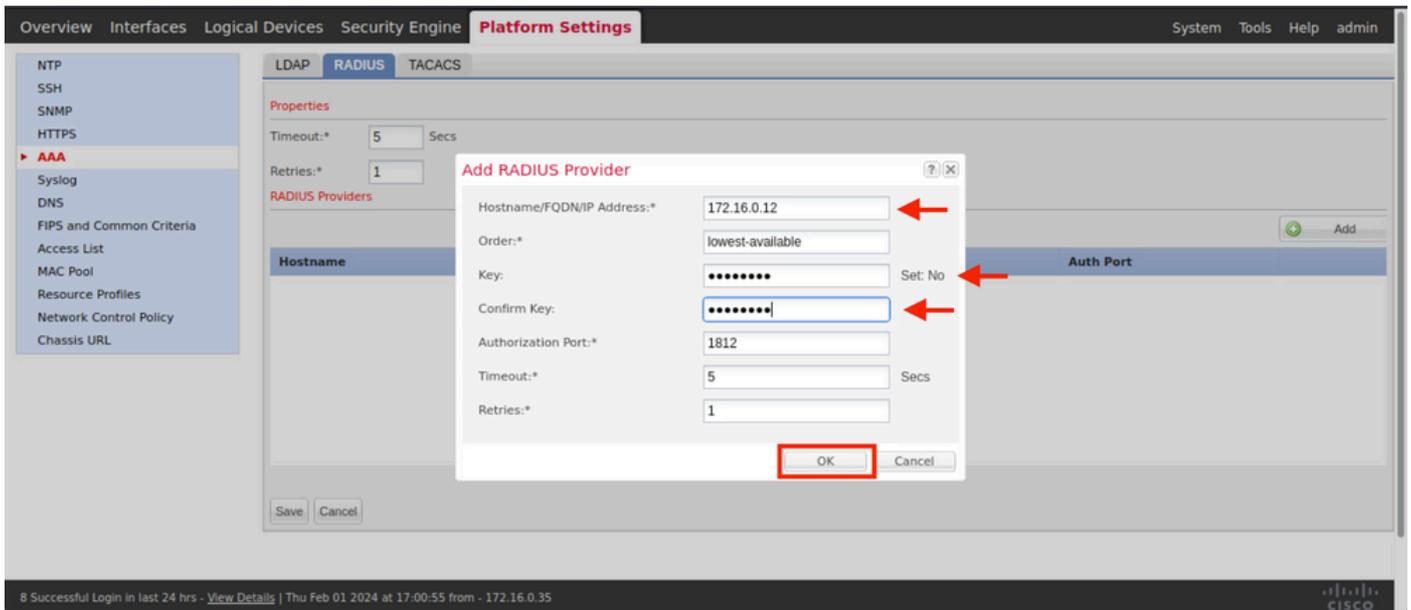
RADIUS Providers + Add

Hostname	Order	Service	Auth Port
----------	-------	---------	-----------

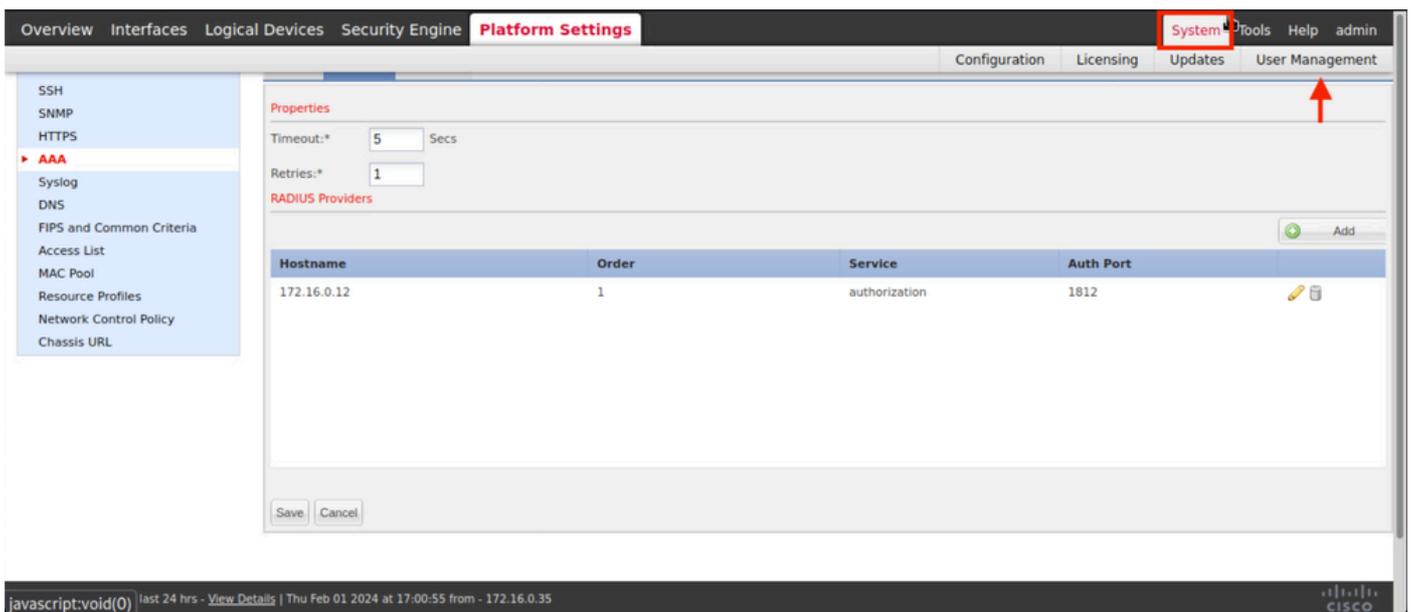
Save Cancel

8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Étape 4. Remplissez le menu d'invite avec les informations demandées du fournisseur Radius. Click OK.



Étape 5. Accédez à Système > Gestion des utilisateurs



Étape 6. Cliquez sur l'onglet Paramètres et définissez l'authentification par défaut dans le menu déroulant sur Radius, puis faites défiler vers le bas et enregistrez la configuration.

Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help admin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication

Local *Local is fallback authentication method

Local
RADIUS 
LDAP
TACACS
None
No-Login

Console Authentication

Remote User Settings

Remote User Role Policy

Local User Settings

Password Strength Check Enable

History Count (0-disabled,1-15)

Change Interval (1-730 hours)

Change Count (1-10)

No Change Interval (1-730 hours)

Days until Password Expiration (0-never,1-9999 days)

Password Expiration Warning Period (0-9999 days)

Expiration Grace Period (0-9999 days)

Password Reuse Interval (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet) (0-never,3600 seconds)

8 Successful Login in last 24 hrs - [View Details](#) | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

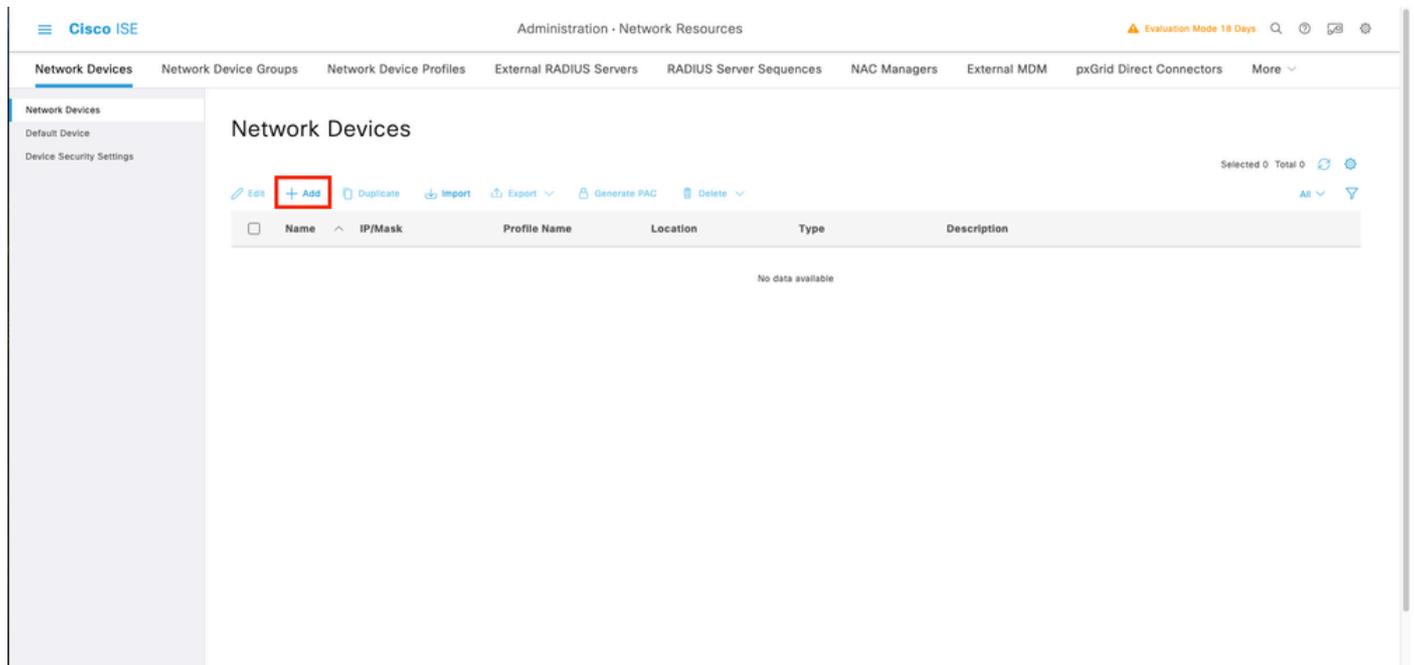
CISCO

Remarque : la configuration de FCM est terminée à ce stade.

Identity Service Engine

Étape 1. Ajoutez un nouveau périphérique réseau.

Accédez à l'icône Burger ≡ située dans l'angle supérieur gauche > Administration > Network Resources > Network Devices > +Add.

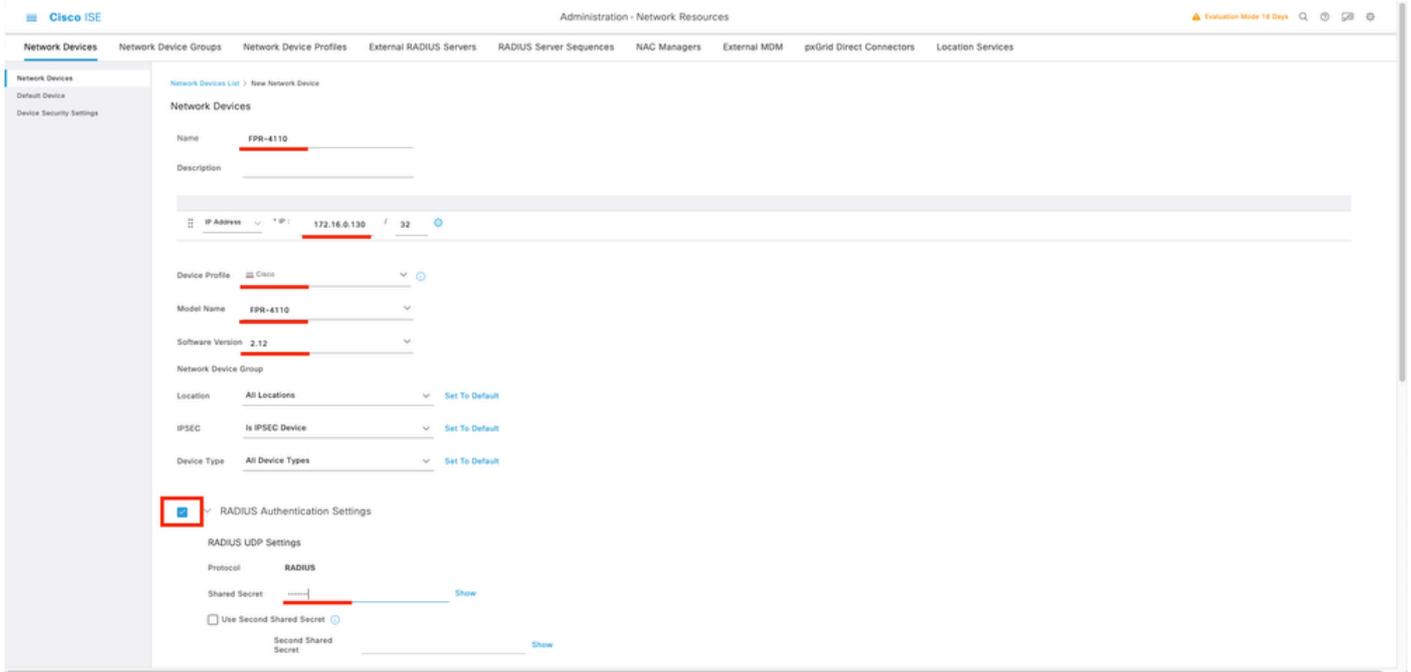


Étape 2. Renseignez les paramètres demandés sur les informations relatives aux nouveaux périphériques réseau.

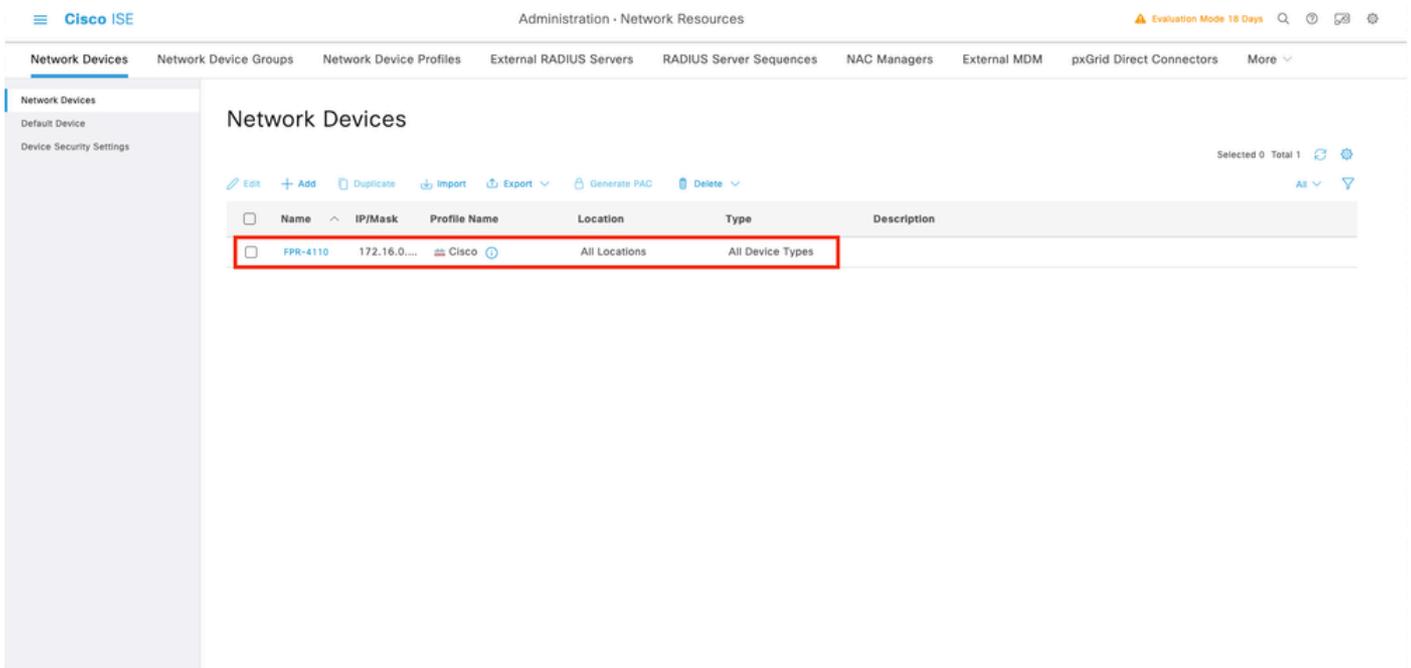
2.1 Cochez la case RADIUS

2.2 Configurez la même clé secrète partagée que dans la configuration FCM Radius.

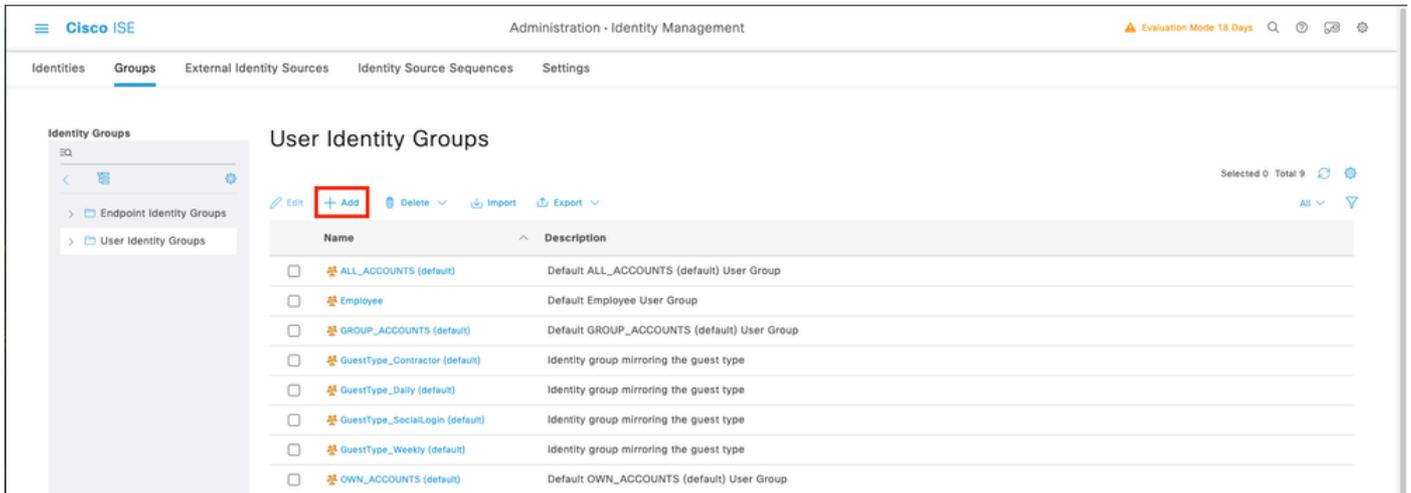
2.1 Faites défiler la page vers le bas et cliquez sur Submit.



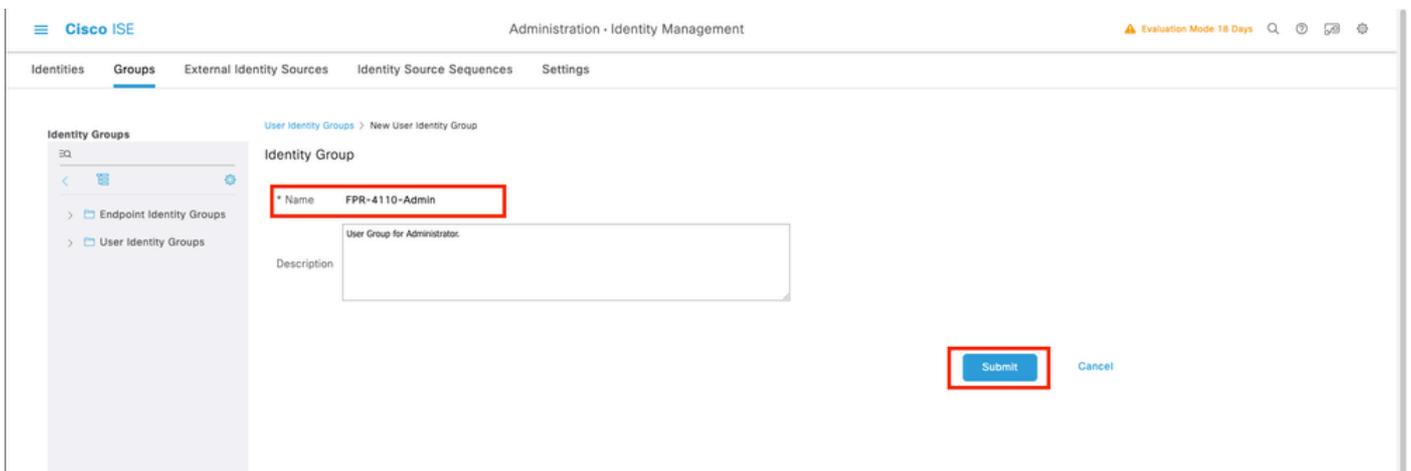
Étape 3. Vérifiez que le nouveau périphérique figure sous Network Devices (Périphériques réseau).



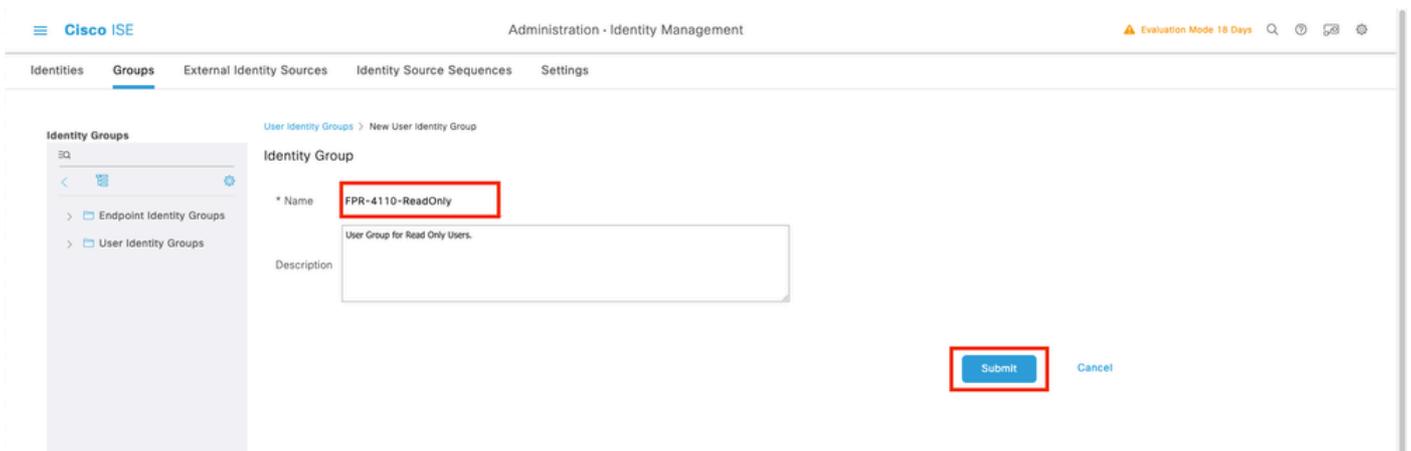
Étape 4. Créez les groupes d'identités utilisateur requis. Accédez à l'icône Burger ≡ située dans l'angle supérieur gauche > Administration > Identity Management > Groups > User Identity Groups > + Add



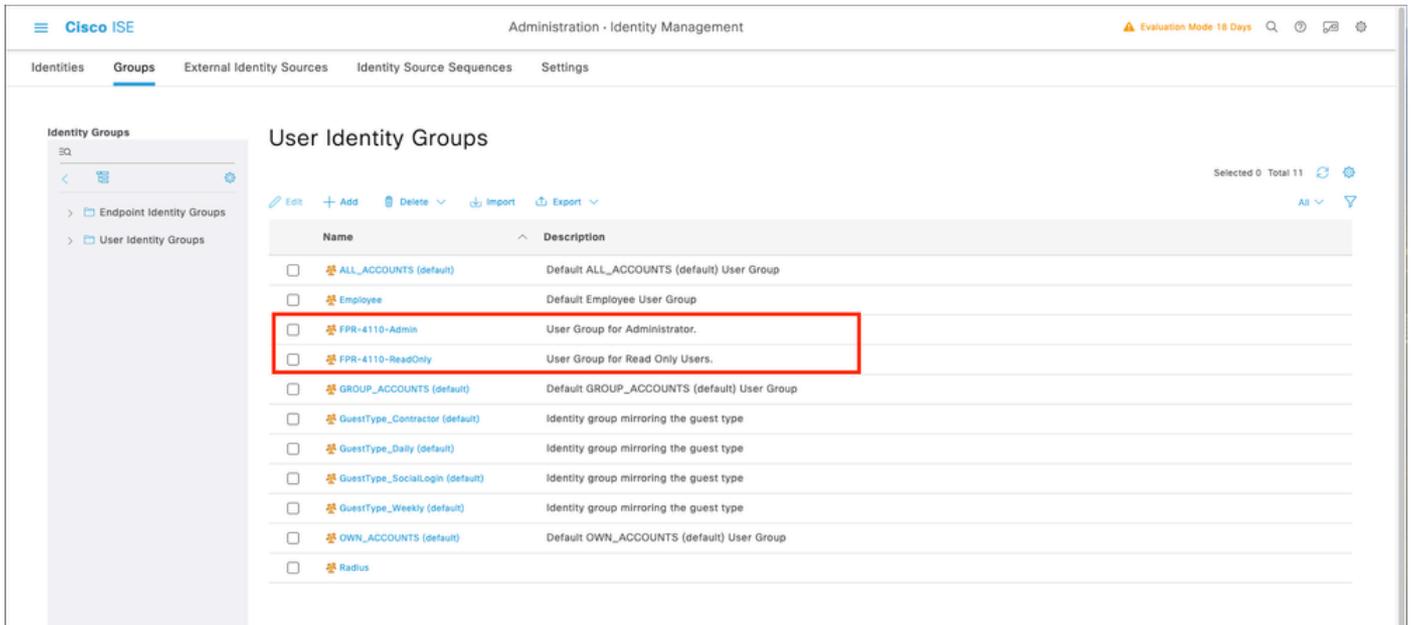
Étape 5. Définissez un nom pour le groupe d'identités d'utilisateur Admin et cliquez sur Submit afin d'enregistrer la configuration.



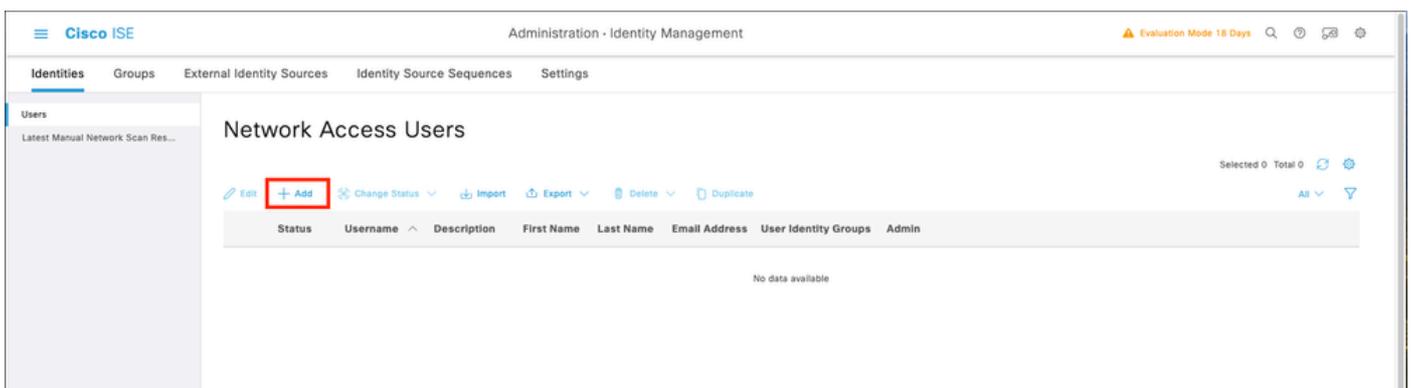
5.1 Répétez la même procédure pour les utilisateurs ReadOnly.



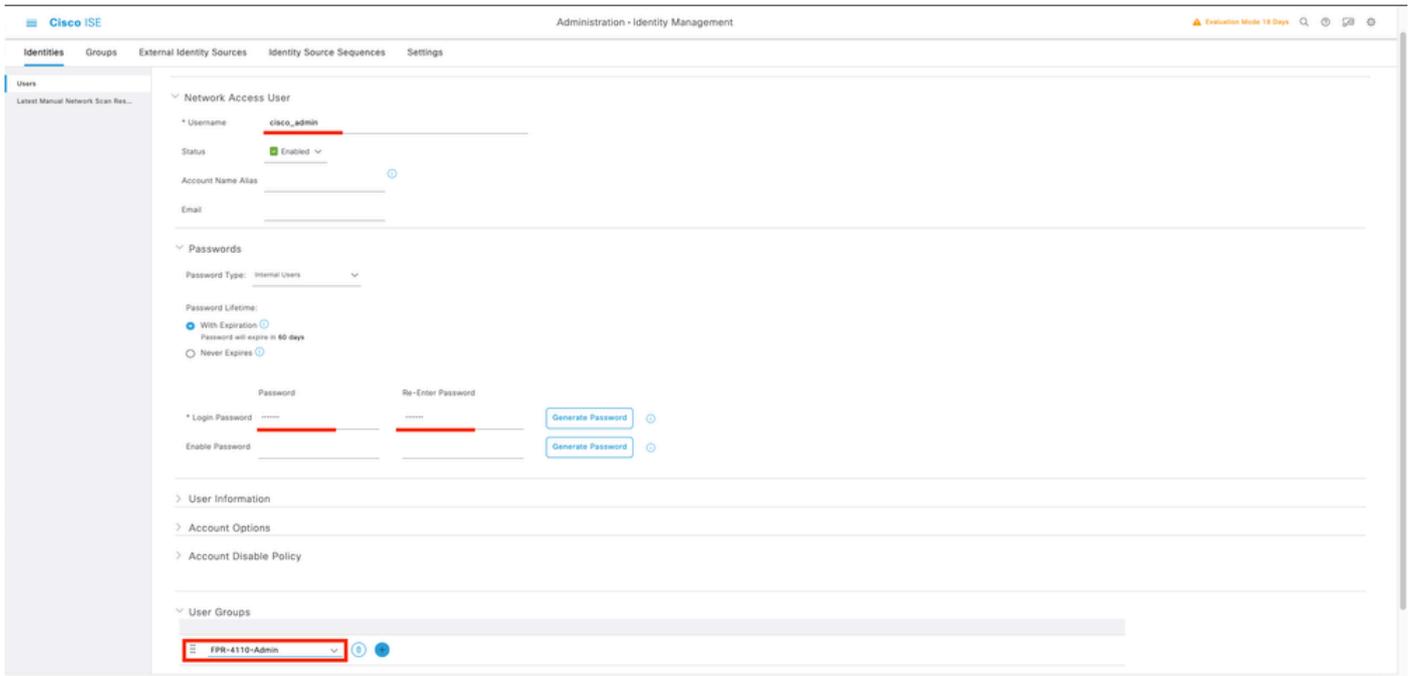
Étape 6. Vérifiez que les nouveaux groupes d'utilisateurs s'affichent sous Groupes d'identités d'utilisateurs.



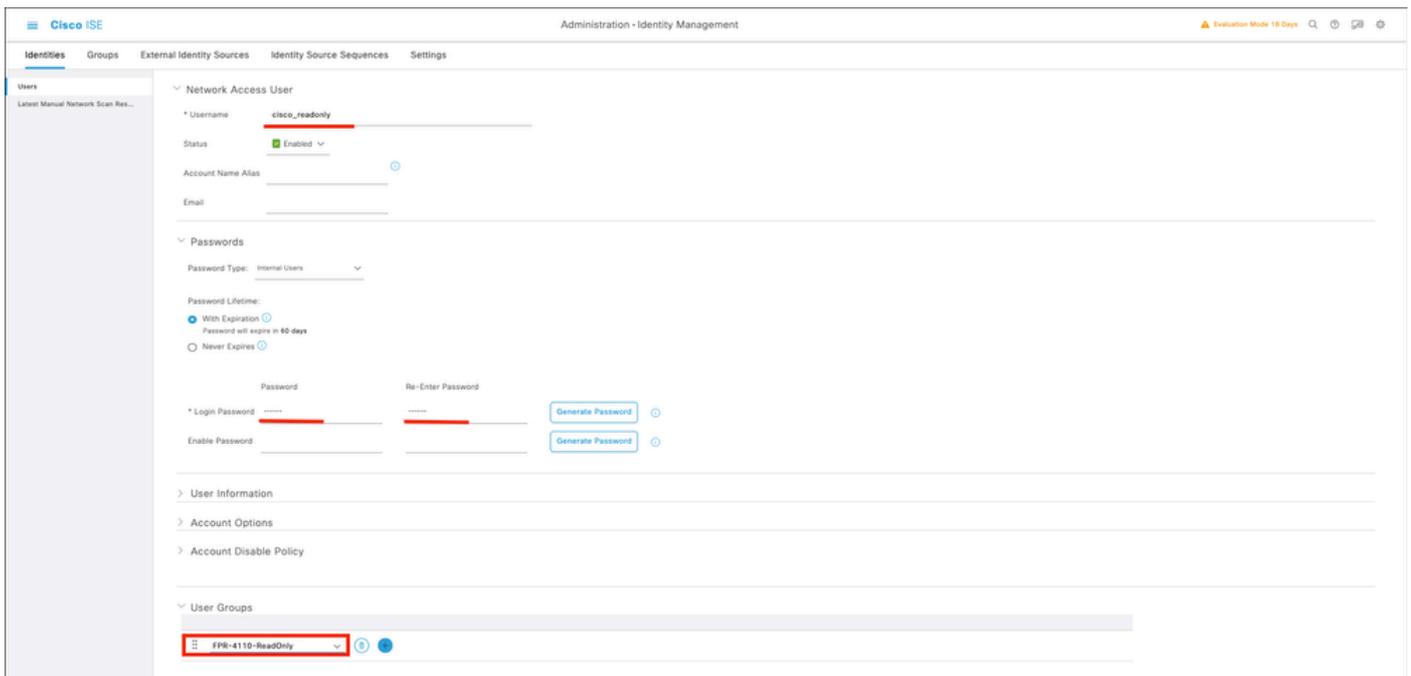
Étape 7. Créez les utilisateurs locaux et ajoutez-les à leur groupe correspondant. Accédez à l'icône burger ≡ > Administration > Identity Management > Identities > + Add.



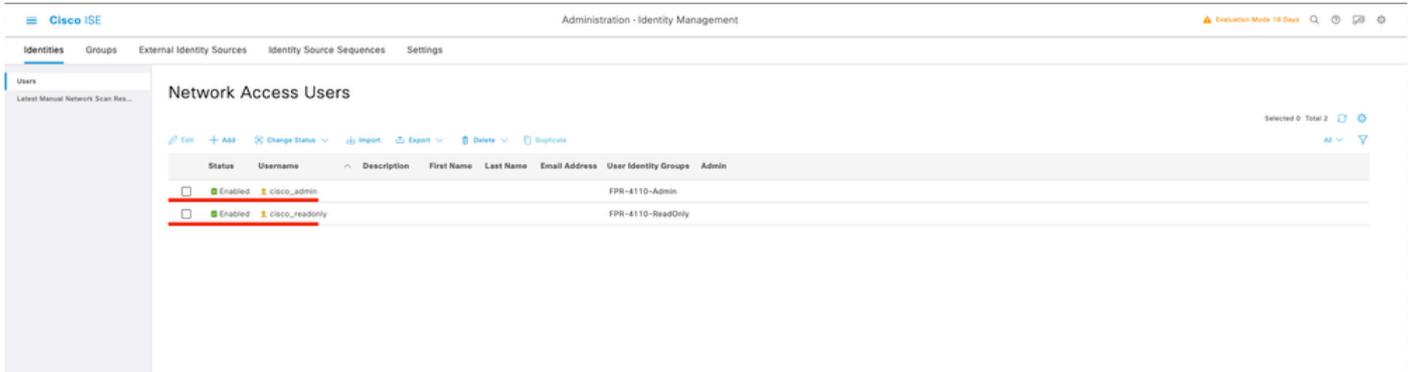
7.1 Ajout de l'utilisateur avec des droits d'administrateur Définissez un nom, un mot de passe et attribuez-le à FPR-4110-Admin, faites défiler vers le bas et cliquez sur Submit pour enregistrer les modifications.



7.2 Ajouter l'utilisateur avec des droits ReadOnly. Définissez un nom, un mot de passe et attribuez-le à FPR-4110-ReadOnly, faites défiler vers le bas et cliquez sur Submit pour enregistrer les modifications.



7.3 Vérifier que les utilisateurs se trouvent sous Network Access Users.



Étape 8. Créez le profil d'autorisation pour l'utilisateur Admin.

Le châssis FXOS comprend les rôles d'utilisateur suivants :

- Administrateur - Accès complet en lecture et en écriture à l'ensemble du système. Ce rôle est attribué par défaut au compte d'administrateur par défaut et ne peut pas être modifié.
- Lecture seule : accès en lecture seule à la configuration du système sans privilèges permettant de modifier l'état du système.
- Opérations : accès en lecture et écriture à la configuration NTP, à la configuration Smart Call Home pour Smart Licensing et aux journaux système, y compris les serveurs et les pannes syslog. Accès en lecture au reste du système.
- AAA : accès en lecture-écriture aux utilisateurs, aux rôles et à la configuration AAA. Accès en lecture au reste du système

Attributs pour chaque rôle :

cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operations"

cisco-av-pair=shell : roles="lecture seule"



Remarque : cette documentation définit uniquement les attributs admin et lecture seule.

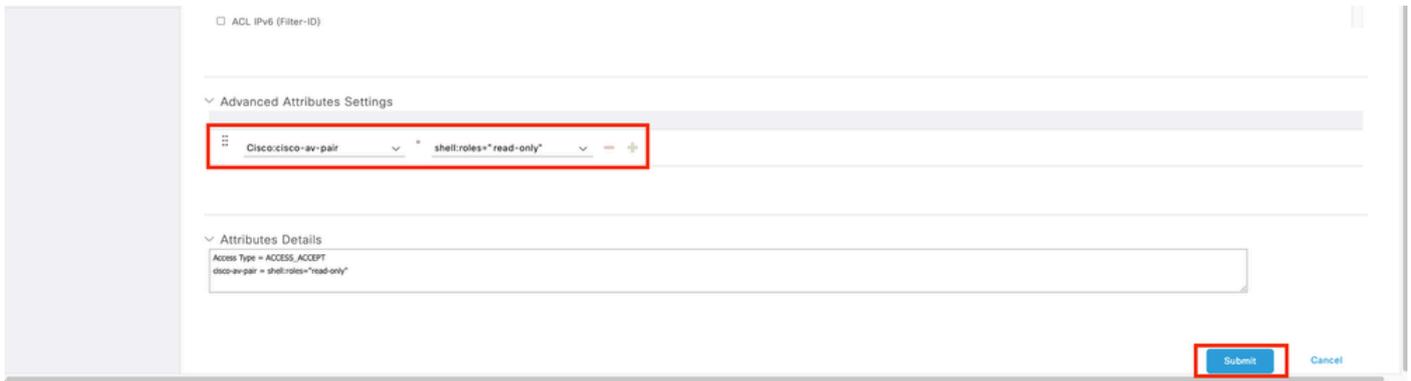
Accédez à l'icône Burger ≡ > Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

Définissez un nom pour le profil d'autorisation, laissez le type d'accès comme ACCESS_ACCEPT et sous Advanced Attributes Settings ajoutez cisco-av-pair=shell : roles="admin" avec et cliquez sur Submit.

The screenshot shows the Cisco ISE Policy Elements configuration interface. The left sidebar contains navigation options: Dictionaries, Conditions, Results, Authentication, Authorization, Authorization Profiles, Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profile' and shows the configuration for 'FPR-4110-Admins'. The 'Name' field is 'FPR-4110-Admins' and the 'Access Type' is 'ACCESS_ACCEPT'. The 'Advanced Attributes Settings' section contains a configuration entry: 'Cisco:cisco-av-pair' with the value 'shell:roles=*admin*'. The 'Attributes Details' section shows the resulting configuration: 'Access Type = ACCESS_ACCEPT' and 'cisco-av-pair = shell:roles=*admin*'. A 'Submit' button is visible at the bottom right.

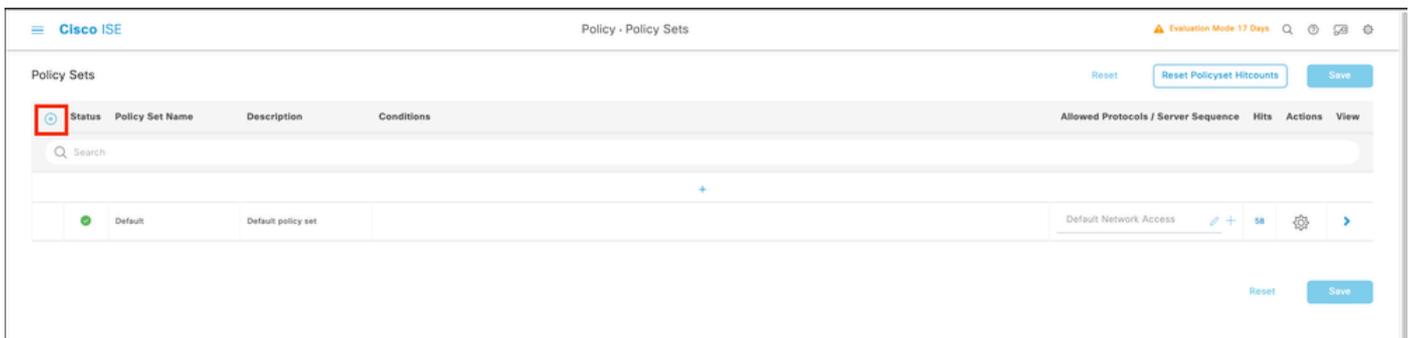
8.1 Répétez l'étape précédente pour créer le profil d'autorisation pour l'utilisateur ReadOnly. Cette fois, créez la classe Radius avec la valeur read-only Administrator.

The screenshot shows the Cisco ISE Policy Elements configuration interface for a new Authorization Profile. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Authorization Profile' and shows the configuration for 'FPR-4110-ReadOnly'. The 'Name' field is 'FPR-4110-ReadOnly' and the 'Access Type' is 'ACCESS_ACCEPT'. The 'Advanced Attributes Settings' section is empty. The 'Attributes Details' section shows the resulting configuration: 'Access Type = ACCESS_ACCEPT'.



Étape 9. Créez un ensemble de stratégies correspondant à l'adresse IP FMC. Cela permet d'empêcher d'autres périphériques d'accorder l'accès aux utilisateurs.

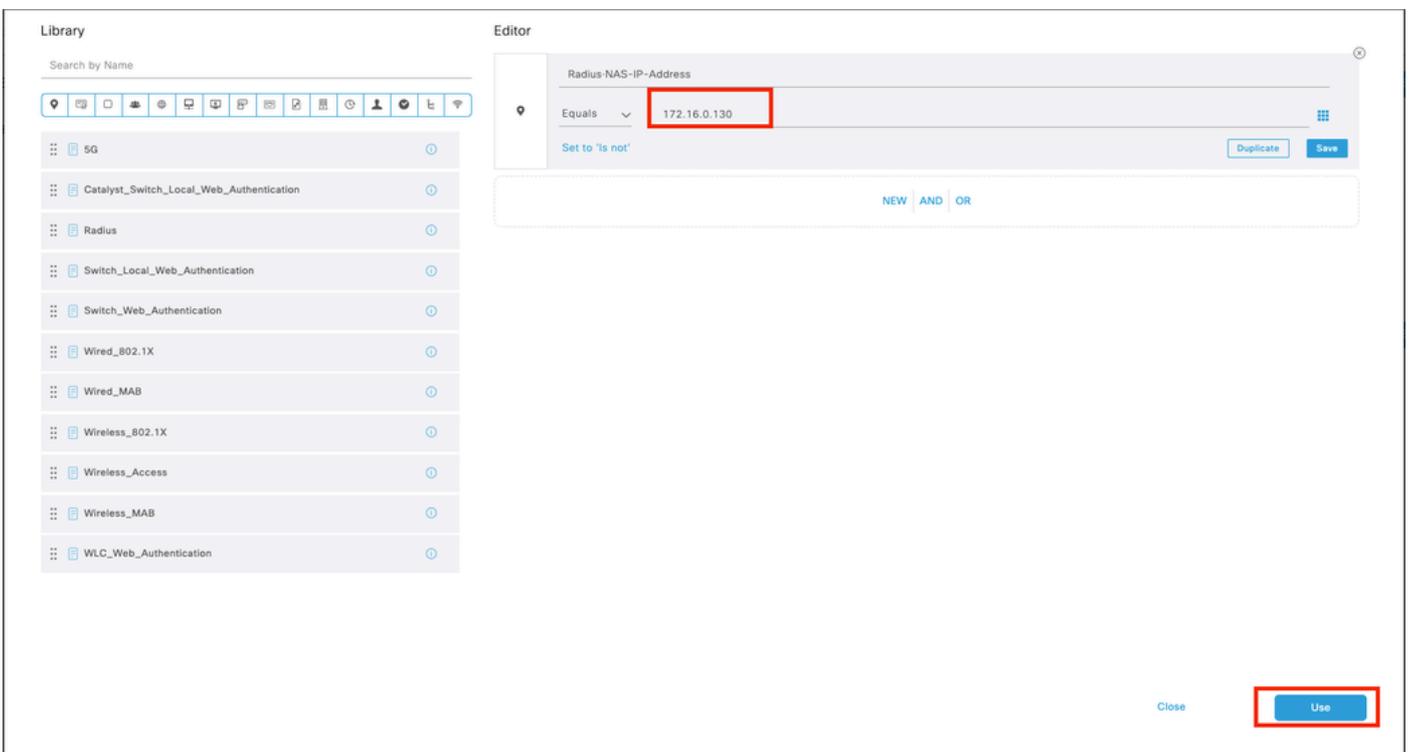
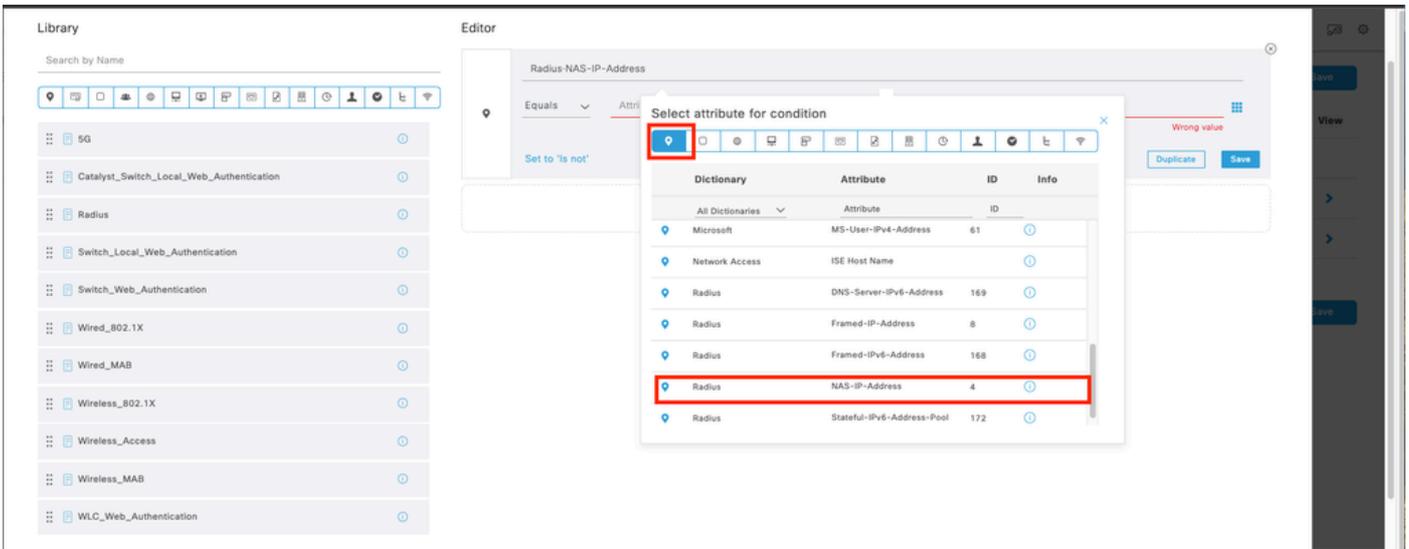
Accédez à ≡ > Policy > Policy Sets > Add icon sign dans l'angle supérieur gauche.



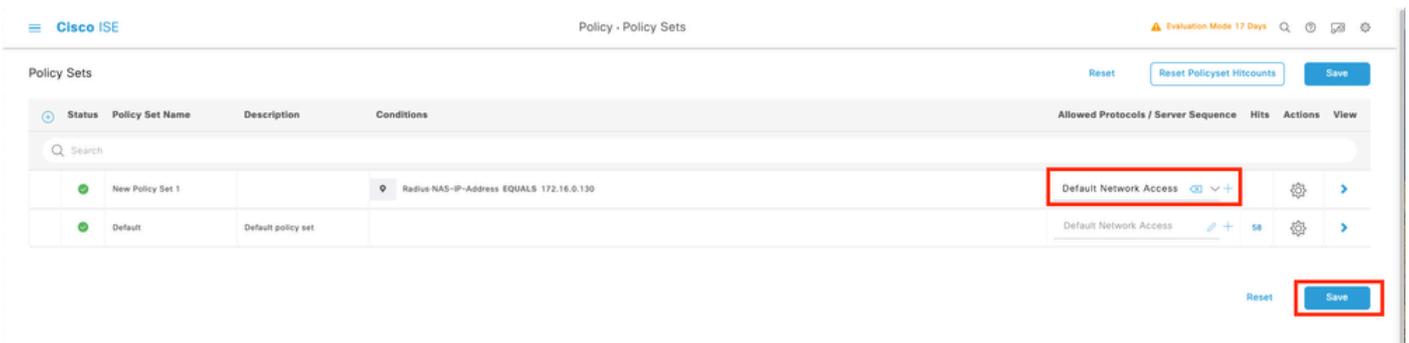
9.1 Une nouvelle ligne est placée en haut de vos ensembles de stratégies. Cliquez sur l'icône Ajouter pour configurer une nouvelle condition.

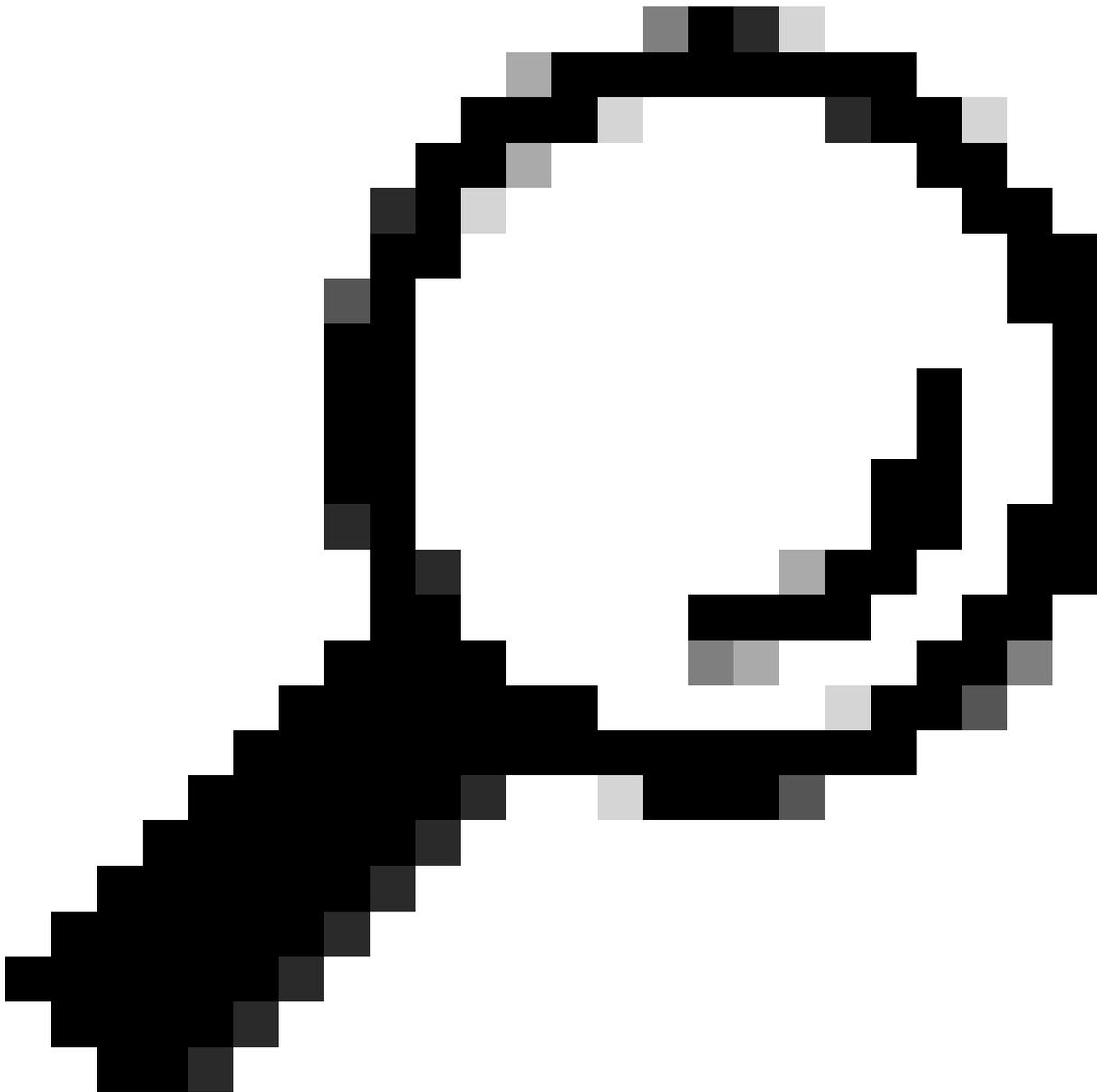


9.2 Ajoutez une condition supérieure pour l'attribut RADIUS NAS-IP-Address correspondant à l'adresse IP FCM, puis cliquez sur Use.



9.3 Une fois terminé, cliquez sur Enregistrer.





Conseil : pour cet exercice, nous avons autorisé la liste des protocoles d'accès réseau par défaut. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

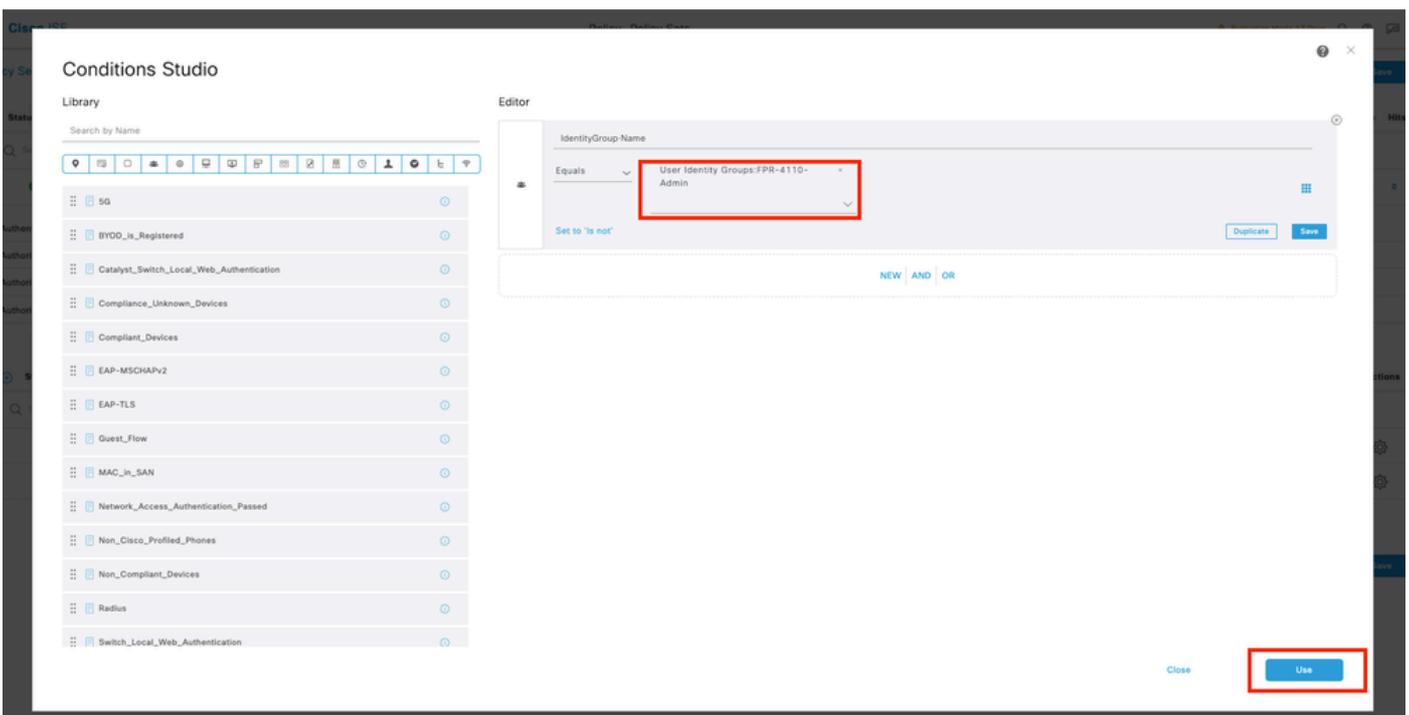
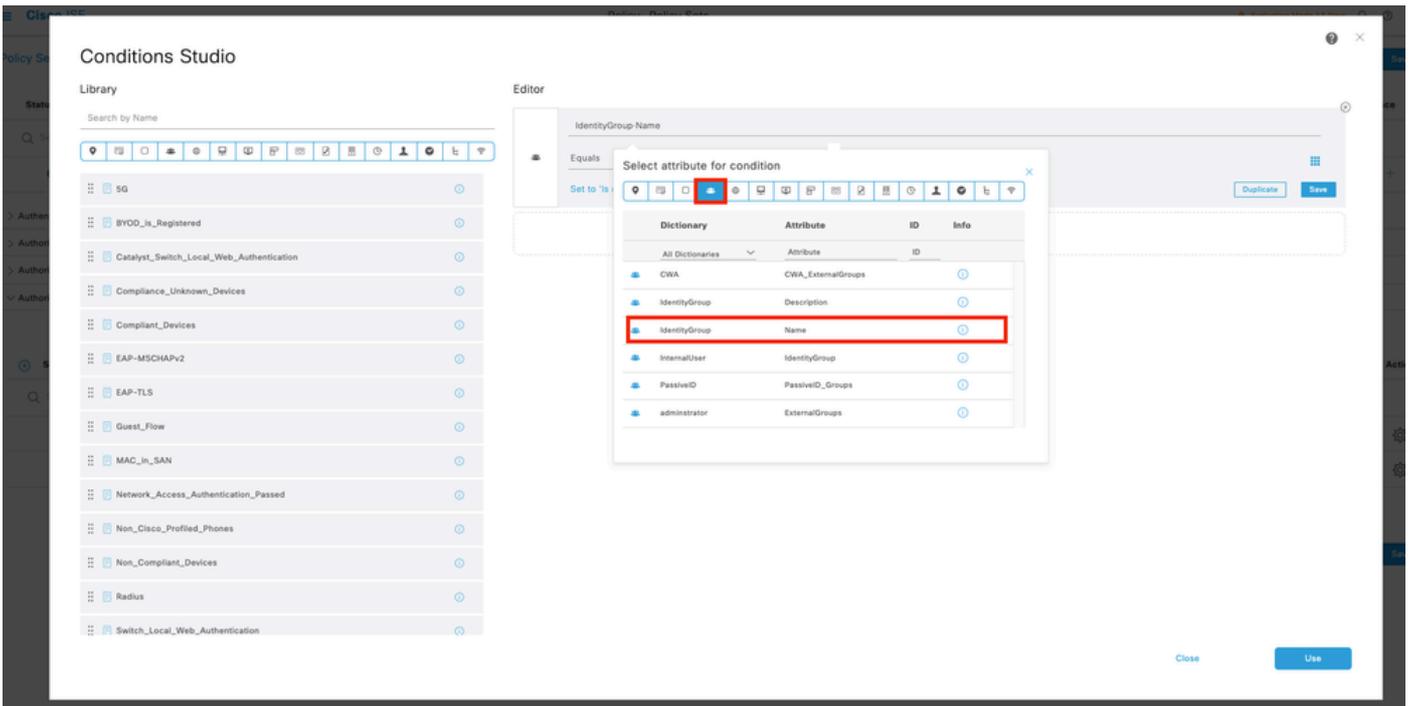
Étape 10. Affichez le nouvel ensemble de règles en cliquant sur l'icône > située à la fin de la ligne.



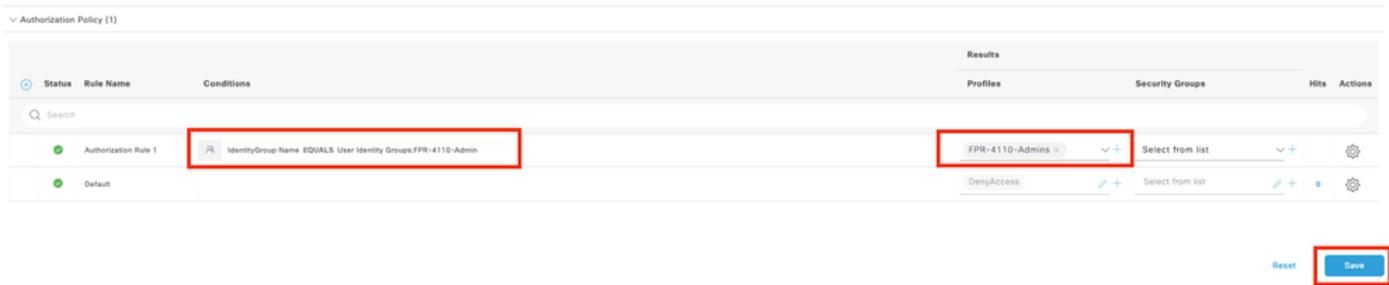
10.1 Développez le menu Stratégie d'autorisation et cliquez sur (+) pour ajouter une nouvelle condition.



10.2 Définissez les conditions pour faire correspondre le groupe DictionaryIdentity avec AttributeName Equals User Identity Groups : FPR-4110-Admins(le nom de groupe créé à l'étape 7) et cliquez sur Use.



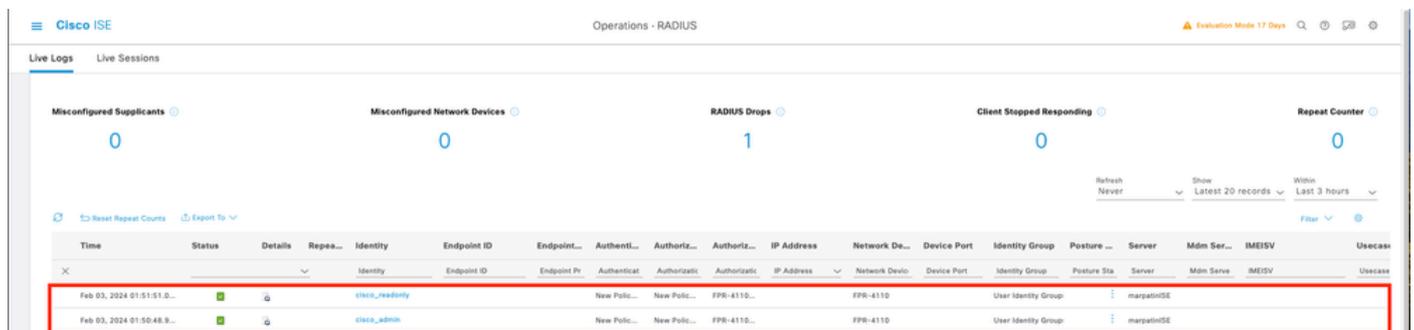
Étape 10.3 Validez la nouvelle condition configurée dans la stratégie d'autorisation, puis ajoutez un profil utilisateur sous Profils.



Étape 11. Répétez le même processus à l'étape 9 pour les utilisateurs en lecture seule et cliquez sur Enregistrer.

Vérifier

1. Essayez de vous connecter à l'interface utilisateur graphique de FCM à l'aide des nouvelles informations d'identification Radius
2. Accédez à l'icône Burger ≡ > Operations > Radius > Live logs.
3. Les informations affichées indiquent si un utilisateur s'est connecté avec succès.



4. Validez le rôle d'utilisateur connecté à partir de l'interface de ligne de commande Secure Firewall Chassis.

```

FPR4K-1-029A78B# scope se
security          server          service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
  Description:
  User Roles:
    Name: admin
    Name: read-only
FPR4K-1-029A78B /security #

```

Dépannage

1. Sur l'interface utilisateur graphique d'ISE , accédez à l'icône burger ≡ > Operations > Radius > Live logs.

1.1 Vérifier si la demande de session de journalisation atteint le noeud ISE.

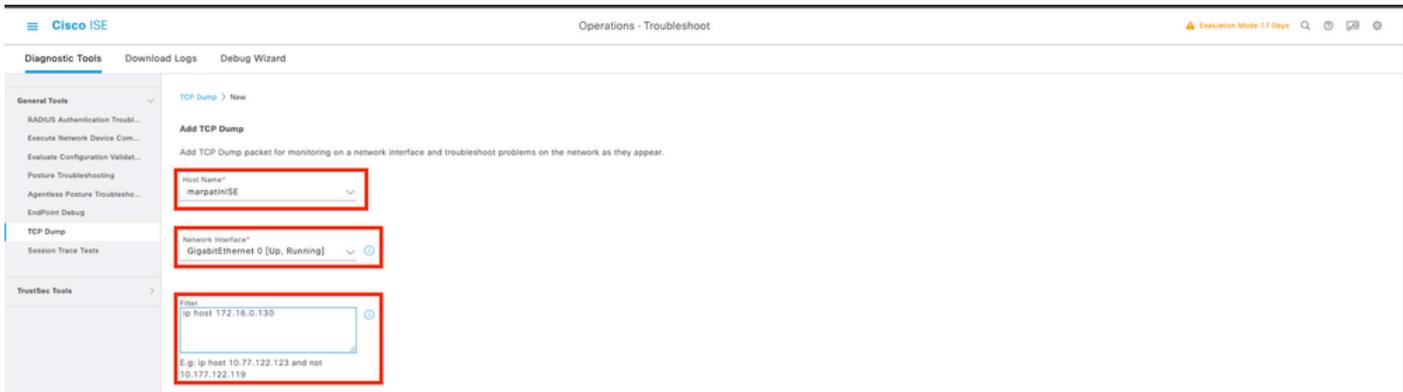
1.2 Pour connaître l'état d'échec, consultez les détails de la session.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authent...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Se
Feb 02, 2024 07:32:18.8...	❌	🔍		cisco_admin	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network Device	Device Port	User Identity Group	Posture Sta	Server	Mdm Sen
Feb 02, 2024 07:23:20.1...	✅	🔍		cisco_readonly			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group		marpat@ISE	
Feb 02, 2024 07:15:32.2...	✅	🔍		cisco_admin			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group		marpat@ISE	

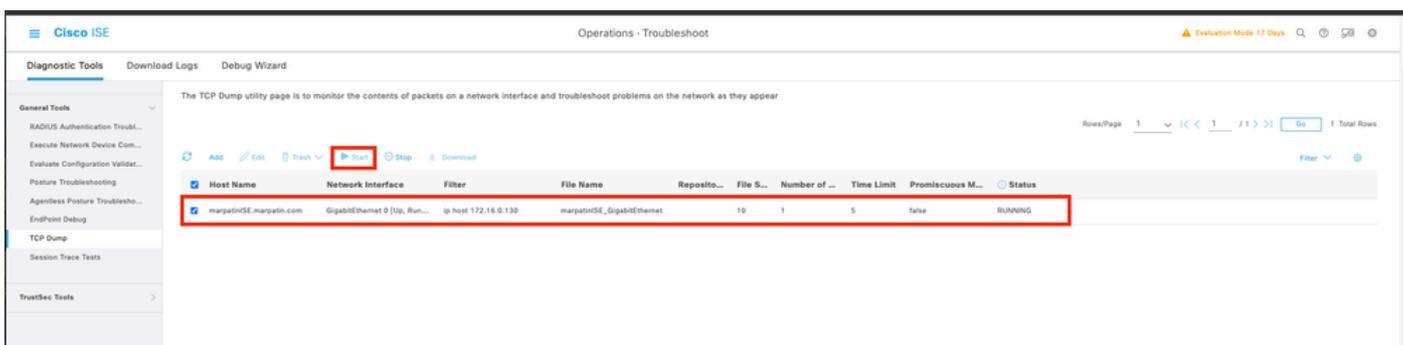
2. Pour les demandes qui n'apparaissent pas dans les journaux Radius Live , vérifiez si la demande UDP atteint le noeud ISE par le biais d'une capture de paquets.

Accédez à l'icône Burger ≡ > Operations > Troubleshoot > Diagnostic Tools > TCP dump. Ajoutez une nouvelle capture et téléchargez le fichier sur votre machine locale afin de vérifier si les paquets UDP arrivent sur le noeud ISE.

2.1 Remplissez les informations demandées, faites défiler la page vers le bas et cliquez sur Save.



2.2 Sélection et démarrage de la capture



2.3 Tentative de connexion au châssis du pare-feu sécurisé pendant l'exécution de la capture ISE

2.4 Arrêtez le vidage TCP dans ISE et téléchargez le fichier sur un ordinateur local.

2.5 Analyse du trafic généré.

Résultat attendu :

Paquet n° 1. Requête du pare-feu sécurisé au serveur ISE via le port 1812 (RADIUS)

Paquet n° 2. Réponse du serveur ISE acceptant la requête initiale.

No.	Time	Source	Destination	Length	Protocol	Message Transaction ID	Info
1	2024-02-02 20:21:52.999276	172.16.0.130	172.16.0.12	128	RADIUS		Access-Request id=22
2	2024-02-02 20:21:53.090894	172.16.0.12	172.16.0.130	186	RADIUS		Access-Accept id=22

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.