# Configuration de l'authentification externe FMC dans un environnement multidomaine

## Table des matières



## Introduction

Ce document décrit la mise en oeuvre de la mutualisation (multidomaine) au sein de Cisco FMC tout en exploitant Cisco ISE pour l'authentification RADIUS centralisée.

## Conditions préalables

### Exigences

Il est recommandé de connaître les sujets suivants :

- Configuration initiale de Cisco Secure Firewall Management Center via une interface utilisateur graphique et/ou un shell.
- Privilèges d'administration complets dans le domaine global de FMC pour créer des sous-domaines et des objets d'authentification externes.
- Configuration des stratégies d'authentification et d'autorisation sur ISE.
- Connaissances de base de RADIUS

### Composants utilisés

- Cisco Secure FMC : vFMC 7.4.2 (ou version ultérieure recommandée pour la stabilité multidomaine)
- Structure du domaine : Une hiérarchie à trois niveaux (Global > Sous-domaines de second niveau).
- Cisco Identity Services Engine : ISE 3.3

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.

## Informations générales

Dans les environnements d'entreprise à grande échelle ou les scénarios de fournisseurs de services de sécurité gérés (MSSP), il est souvent nécessaire de segmenter la gestion du réseau en frontières administratives distinctes. Ce document décrit comment configurer le FMC pour prendre en charge plusieurs domaines, en particulier pour un exemple réel où un MSSP gère deux clients : Retail-A et Finance-B. En utilisant l'authentification RADIUS externe via Cisco ISE, les administrateurs peuvent s'assurer que les utilisateurs ne disposent automatiquement d'un accès qu'à leurs domaines d'utilisateurs respectifs en fonction de leurs informations d'identification centralisées.

Le système Cisco Secure Firewall utilise des domaines pour mettre en oeuvre la mutualisation.

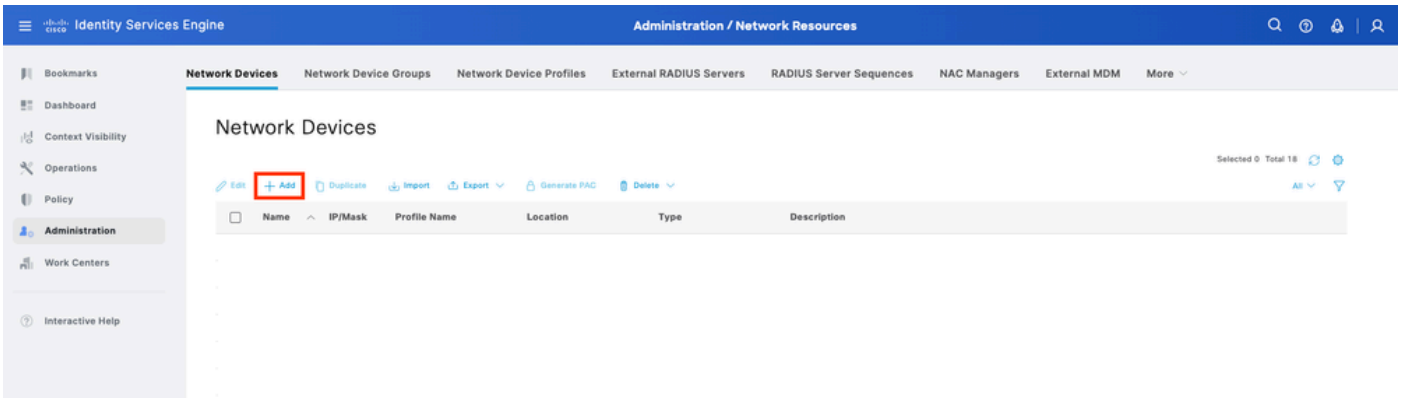
- Hiérarchie des domaines : La hiérarchie commence au niveau du domaine global. Vous pouvez créer jusqu'à 100 sous-domaines dans une structure à deux ou trois niveaux.
- Domaines leaf : Il s'agit de domaines situés au bas de la hiérarchie, sans autre sous-domaine. Il est essentiel que chaque périphérique FTD géré soit associé à exactement un domaine leaf.
- Attribut de classe RADIUS (Attribut 25) : Dans une configuration multidomaine, le FMC utilise l'attribut de classe RADIUS renvoyé par ISE pour mapper un utilisateur authentifié à un domaine et un rôle d'utilisateur spécifiques. Cela permet à un seul serveur RADIUS d'attribuer dynamiquement des utilisateurs à différents segments d'utilisateurs (par exemple, Retail-A ou Finance-B) lors de la connexion.

## Configuration

### Configuration ISE

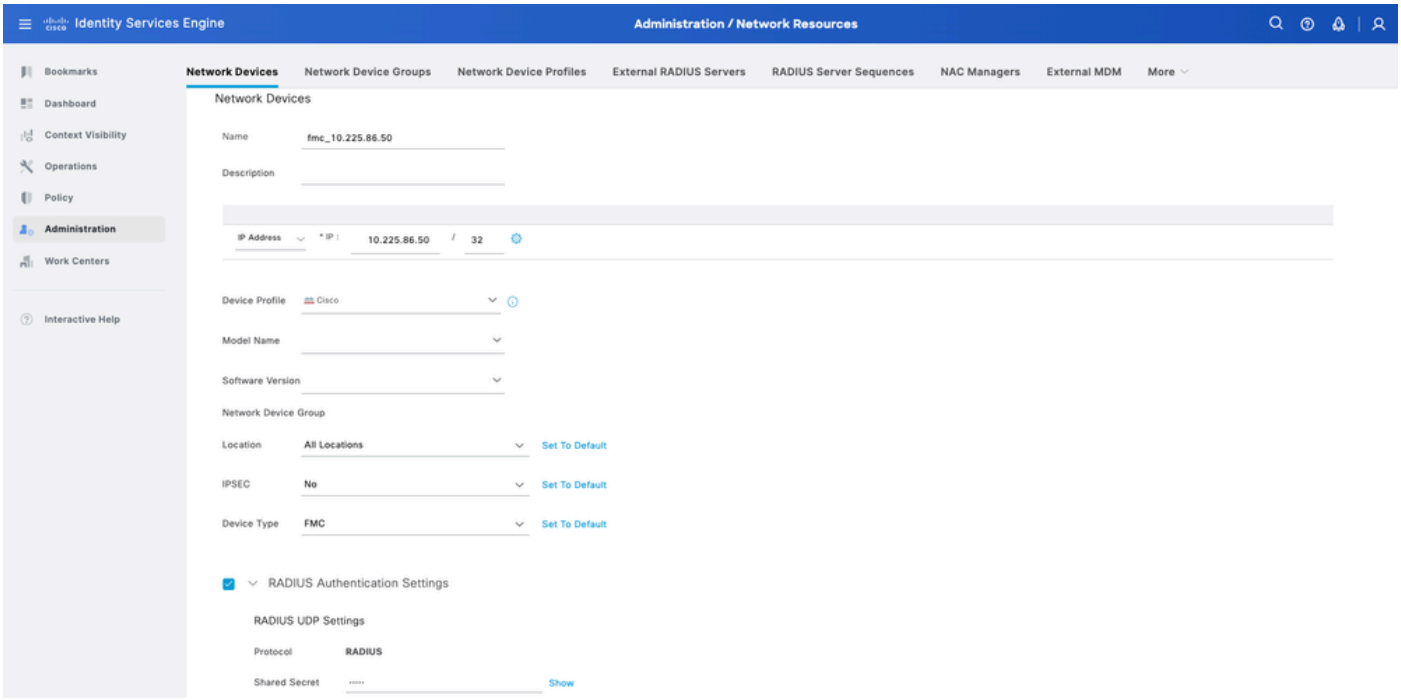
Ajouter vos périphériques réseau

Étape 1. Accédez à Administration > Network Resources > Network Devices > Add.



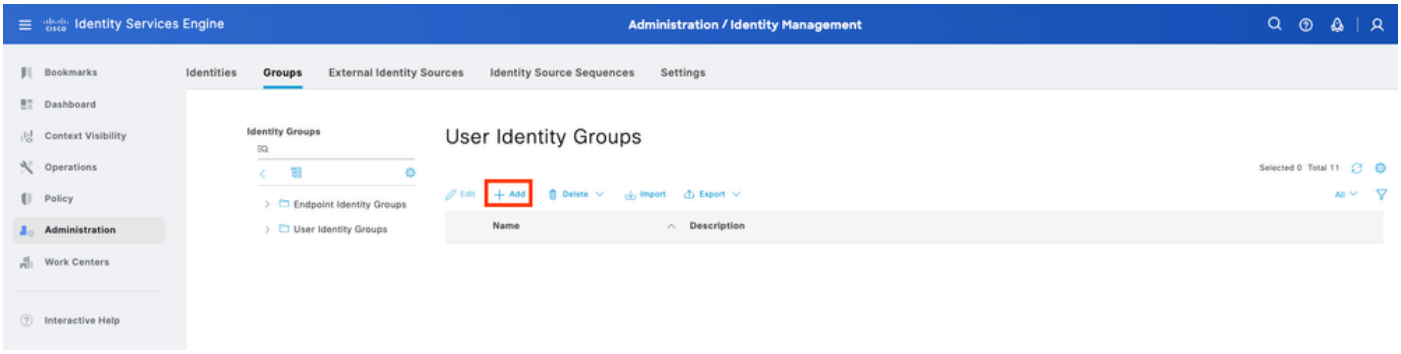

Étape 2. Attribuez un nom à l'objet périphérique réseau et insérez l'adresse IP FMC.

Cochez la case RADIUS et définissez un secret partagé. La même clé doit être utilisée ultérieurement pour configurer le FMC. Une fois terminé, cliquez sur Enregistrer.

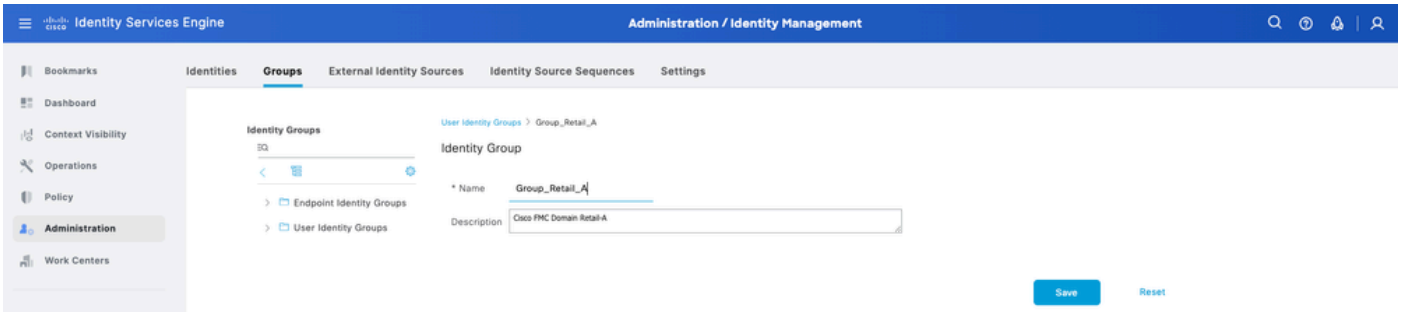


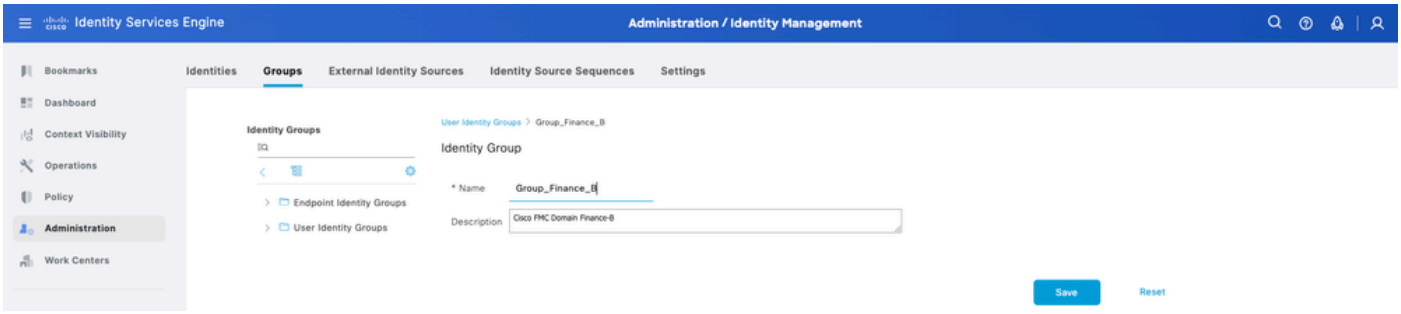

Créer les groupes et utilisateurs d'identités d'utilisateurs locaux

Étape 3 : création des groupes d'identités utilisateur requis Accédez à Administration > Identity Management > Groups > User Identity Groups > Add.

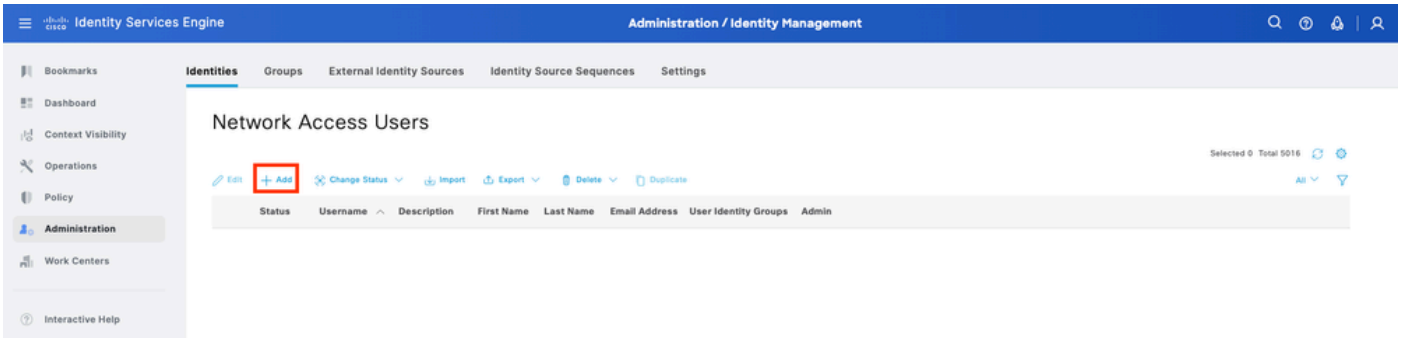


Étape 4. Attribuez un nom à chaque groupe et enregistrez-le individuellement. Dans cet exemple, vous créez un groupe pour les utilisateurs Administrateur. Créez deux groupes : Group_Retail_A et Group_Finance_B.

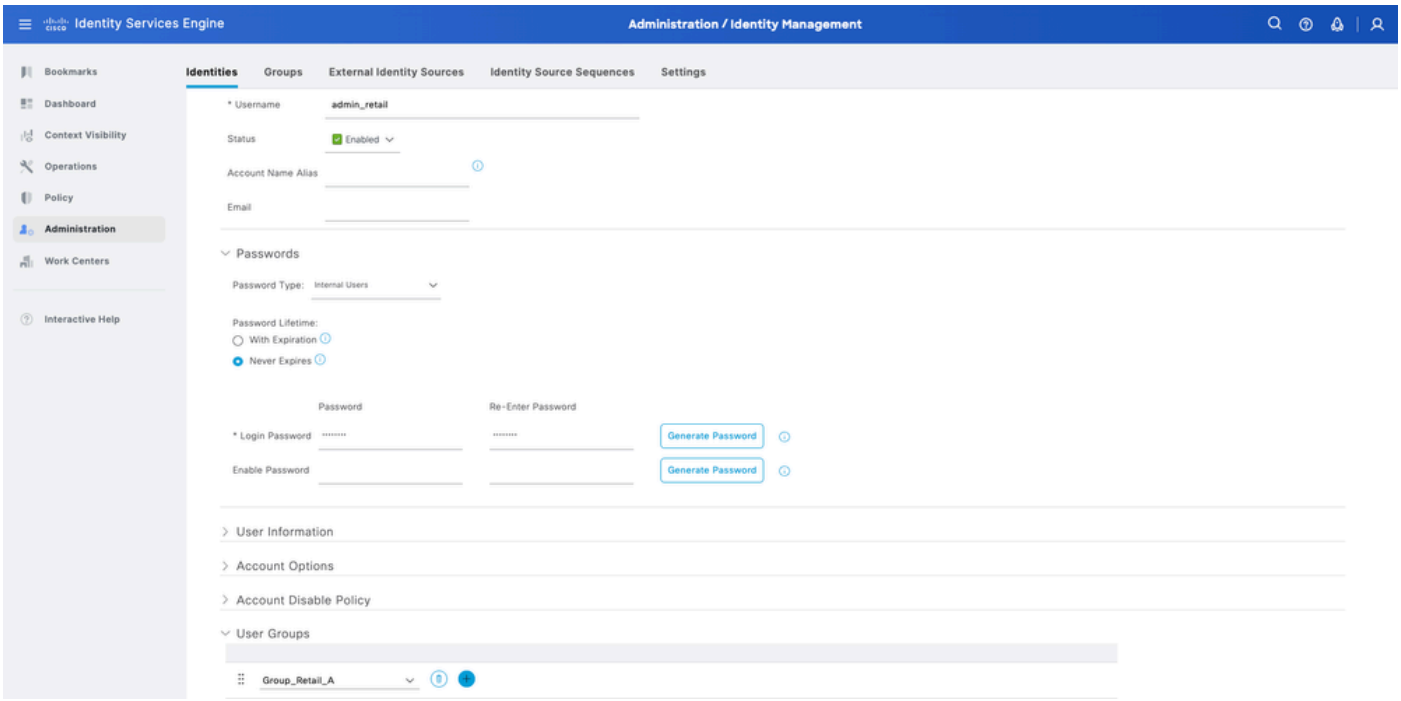


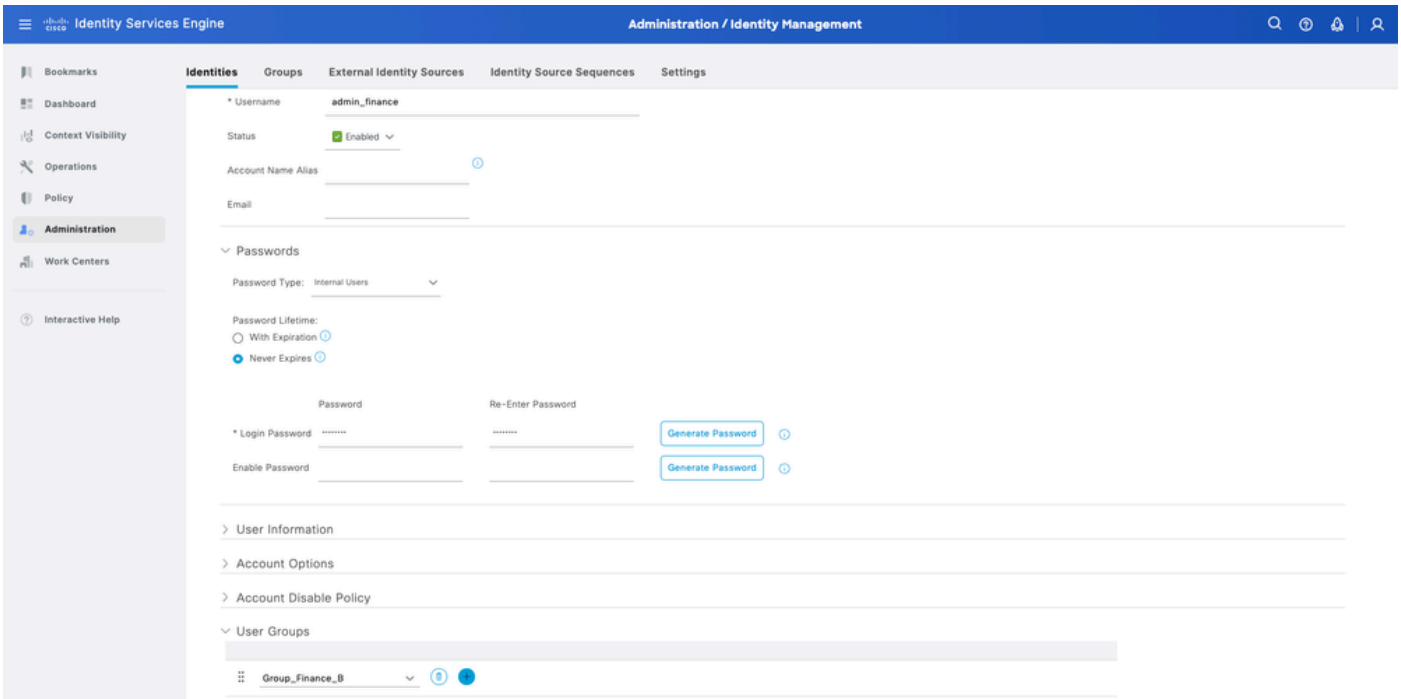

Étape 5. Créez les utilisateurs locaux et ajoutez-les à leur groupe correspondant. Accédez à Administration > Identity Management > Identities > Add.




Étape 5.1. Commencez par créer l'utilisateur avec des droits d'administrateur. Attribuez-lui un nom admin_retail, un mot de passe et le groupe Group_Retail_A.

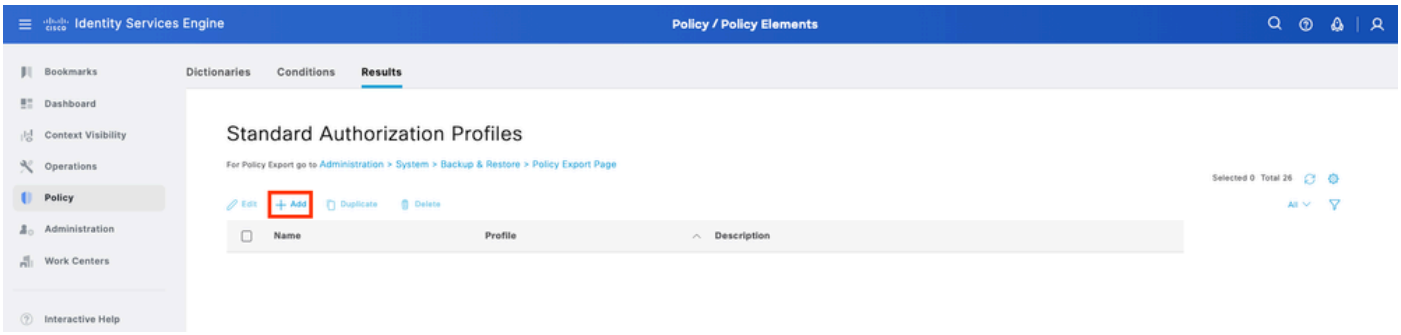



Étape 5.2. Commencez par créer l'utilisateur avec des droits d'administrateur. Attribuez un nom à admin_finance, password et au groupe Group_Finance_B.




Créer les profils d'autorisation

Étape 6. Créer le profil d'autorisation pour l'utilisateur Administrateur de l'interface Web FMC
Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add.




Définissez un nom pour le profil d'autorisation, laissez le type d'accès ACCESS_ACCEPT.

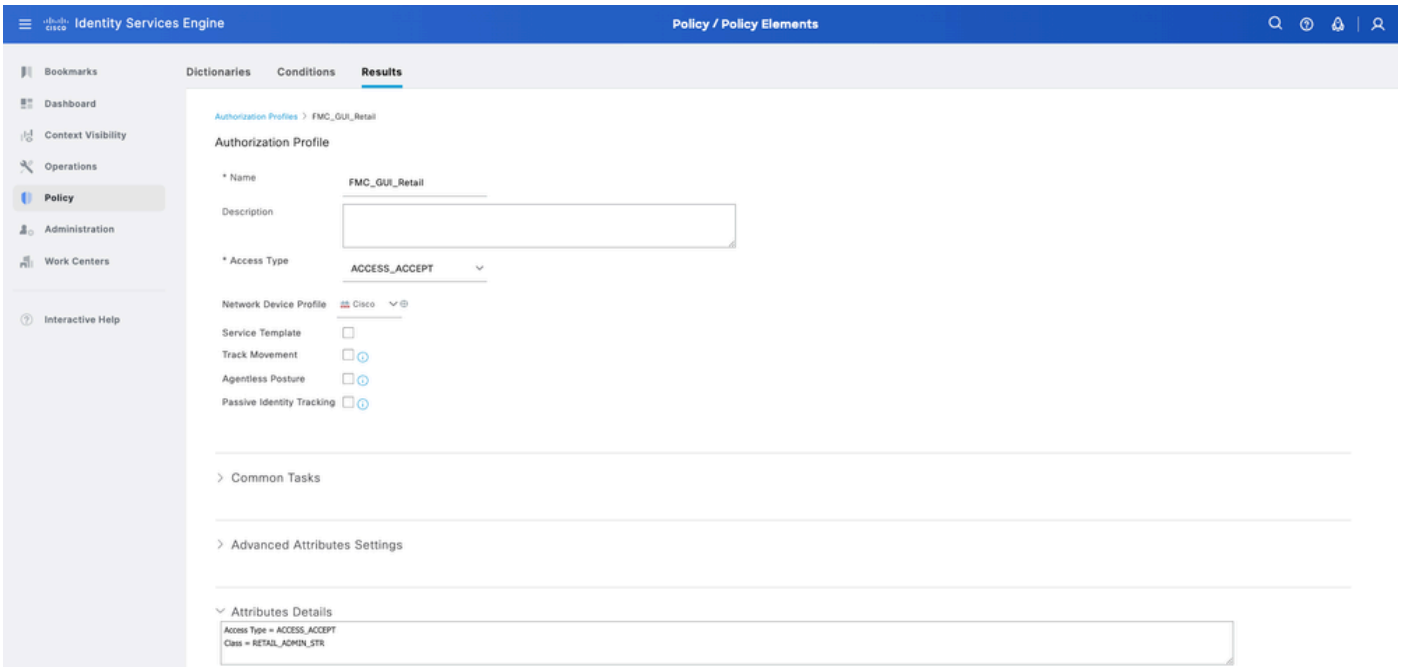
Sous Advanced Attributes Settings, ajoutez un Radius > Class—[25] avec la valeur et cliquez sur Submit.

Étape 6.1. Vente au détail de profils : Sous Advanced Attributes Settings, ajoutez Radius : Class avec la valeur RETAIL_ADMIN_STR.

---

Conseil : Ici RETAIL_ADMIN_STR peut être n'importe quoi ; assurez-vous que les mêmes besoins de valeur sont également mis du côté du FMC.

---

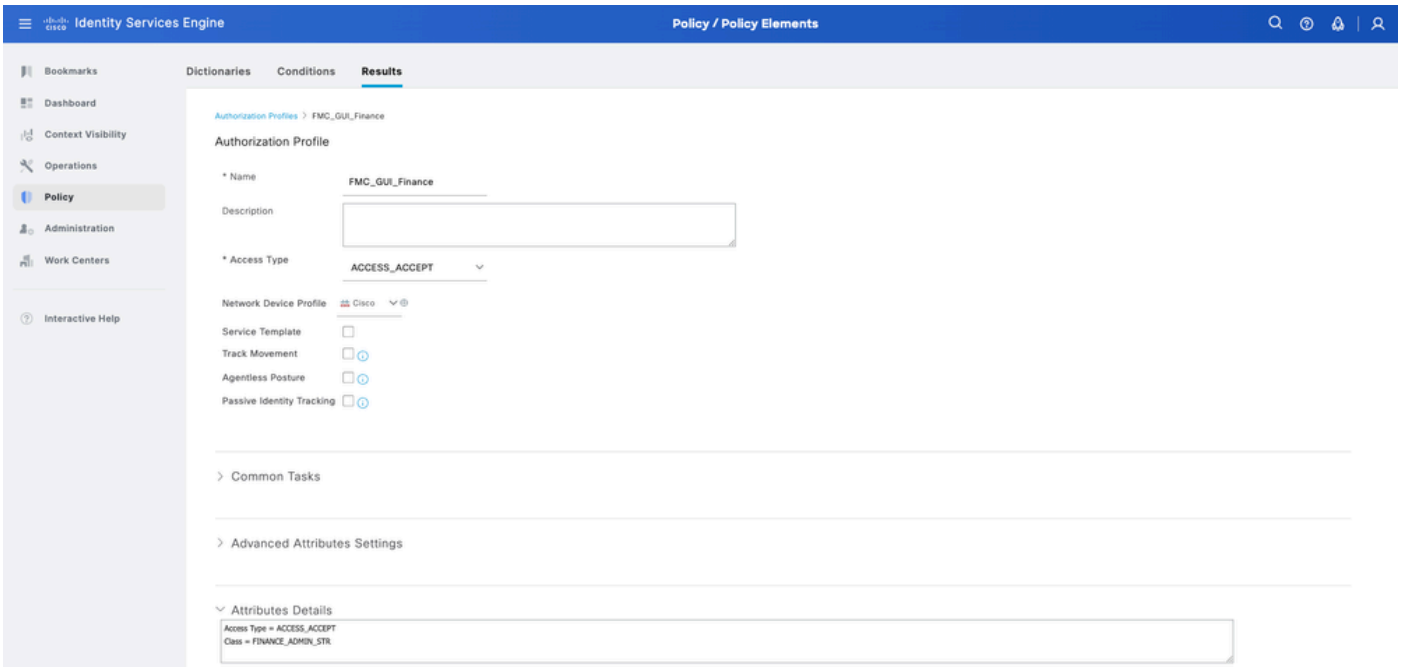



Étape 6.2. Financement par profil : Sous Advanced Attributes Settings, ajoutez Radius : Class avec la valeur FINANCE_ADMIN_STR.

---

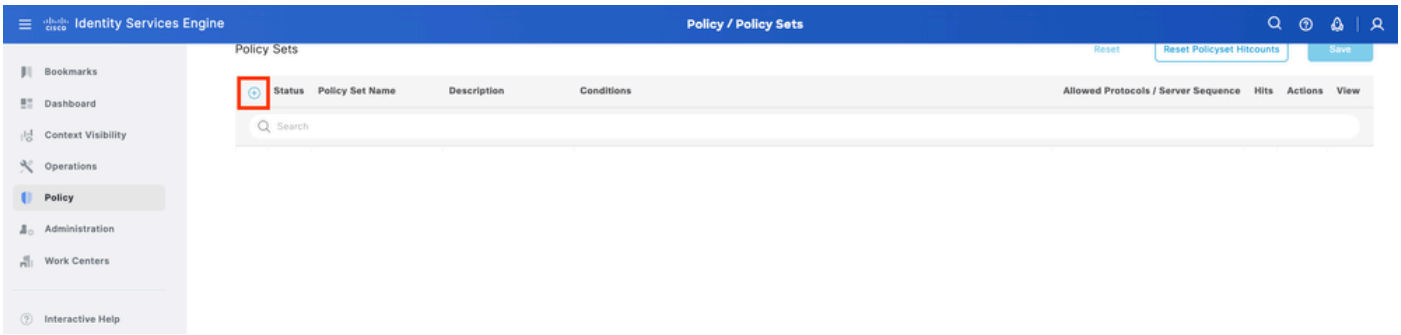
Conseil : Ici FINANCE_ADMIN_STR peut être n'importe quoi ; assurez-vous que la même valeur est également attribuée au FMC.

---



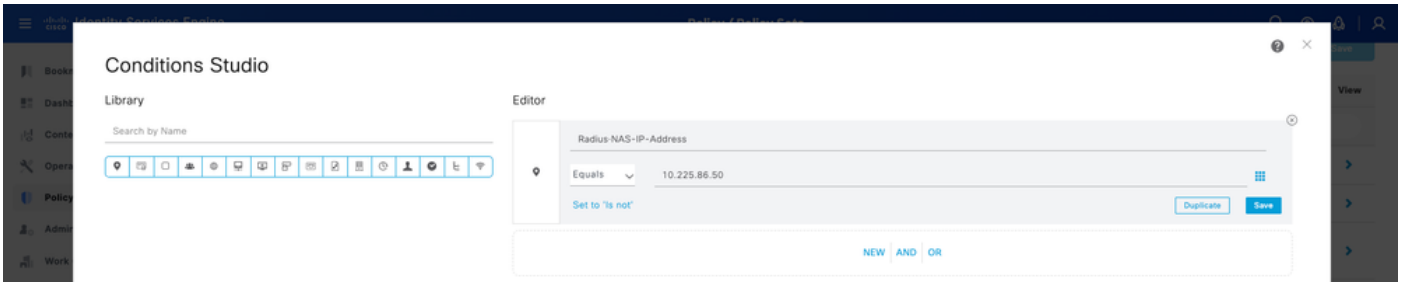

Ajouter un nouvel ensemble de stratégies

Étape 7 : création d'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 > icône de signe Plus placée dans l'angle supérieur gauche.




Étape 8.1. Une nouvelle ligne est placée en haut de vos ensembles de stratégies.

Nommez la nouvelle stratégie et ajoutez une condition supérieure pour l'attribut RADIUS NAS-IP-Address correspondant à l'adresse IP FMC. Cliquez sur Utiliser pour conserver les modifications et quitter l'éditeur.



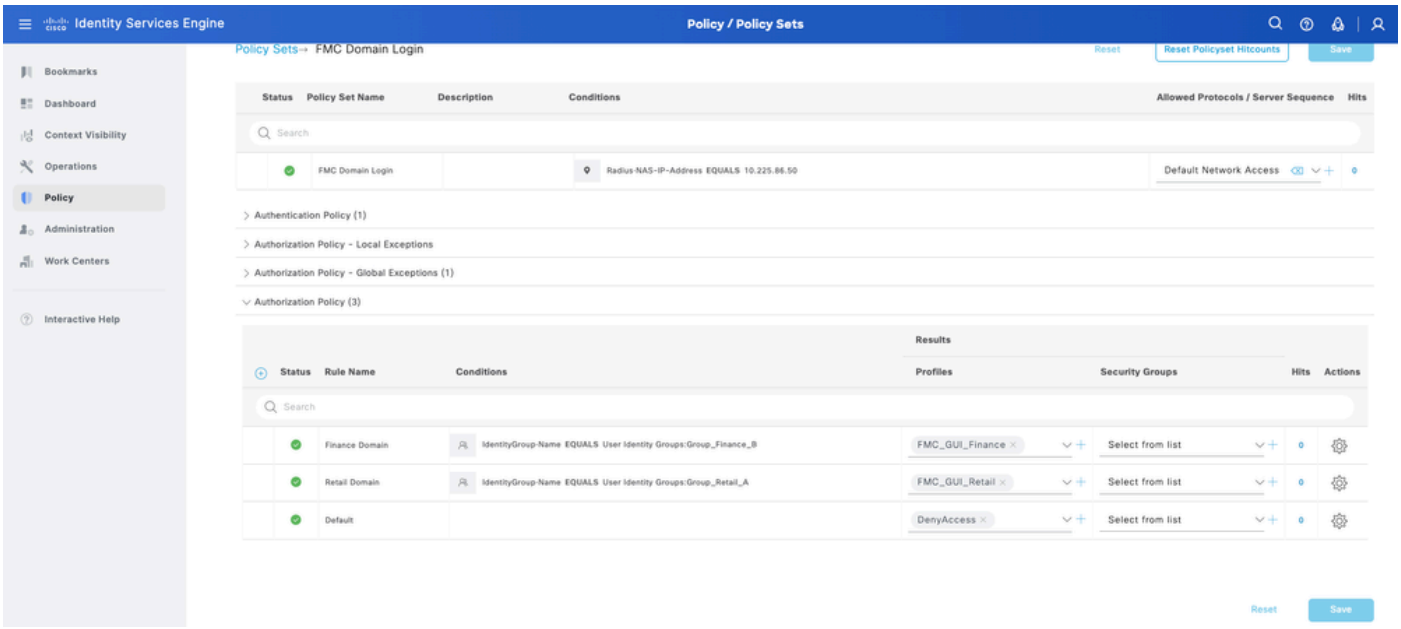

Étape 8.2. Une fois terminé, appuyez sur Save.

Étape 9. Affichez le nouvel ensemble de règles en cliquant sur l'icône d'ensemble placée à la fin de la ligne.

Développez le menu Authorization Policy et appuyez sur l'icône Plus sign pour ajouter une nouvelle règle permettant l'accès à l'utilisateur avec des droits d'administrateur. Donnez-lui un nom.


Définissez les conditions pour faire correspondre le groupe d'identités du dictionnaire avec Nom d'attribut égal et choisissez Groupes d'identités d'utilisateurs. Sous la stratégie d'autorisation, créez des règles :

- Règle 1 : Si Groupe d'identités utilisateur est égal à Groupe_Détail_A, affectez le profil Détail.
- Règle 2 : Si Groupe d'identités d'utilisateur est égal à Group_Finance_B, affectez le financement de profil.



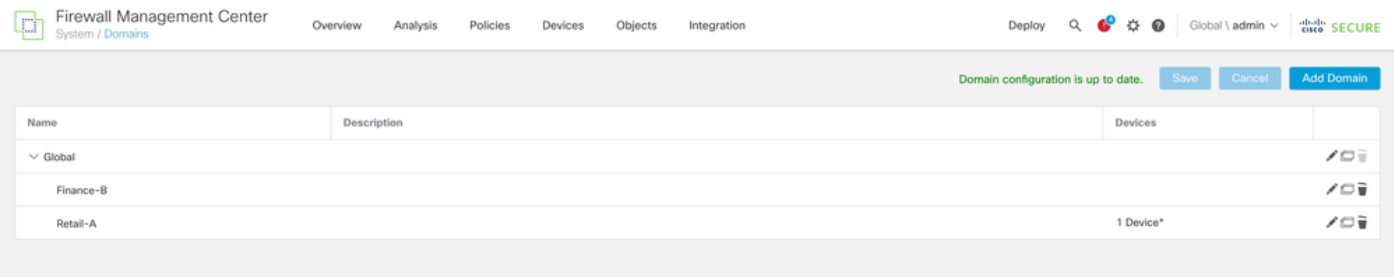

Étape 10. Définissez les profils d’autorisation respectivement pour chaque règle et cliquez sur Enregistrer.

## Configuration FMC

Ajouter votre serveur RADIUS ISE pour l'authentification FMC

Étape 1. Établir la structure du domaine :

- Connectez-vous au domaine global FMC.
- Accédez à Administration > Domains.
- Cliquez sur Add Domain pour créer Retail-A et Finance-B en tant que sous-domaines de Global.



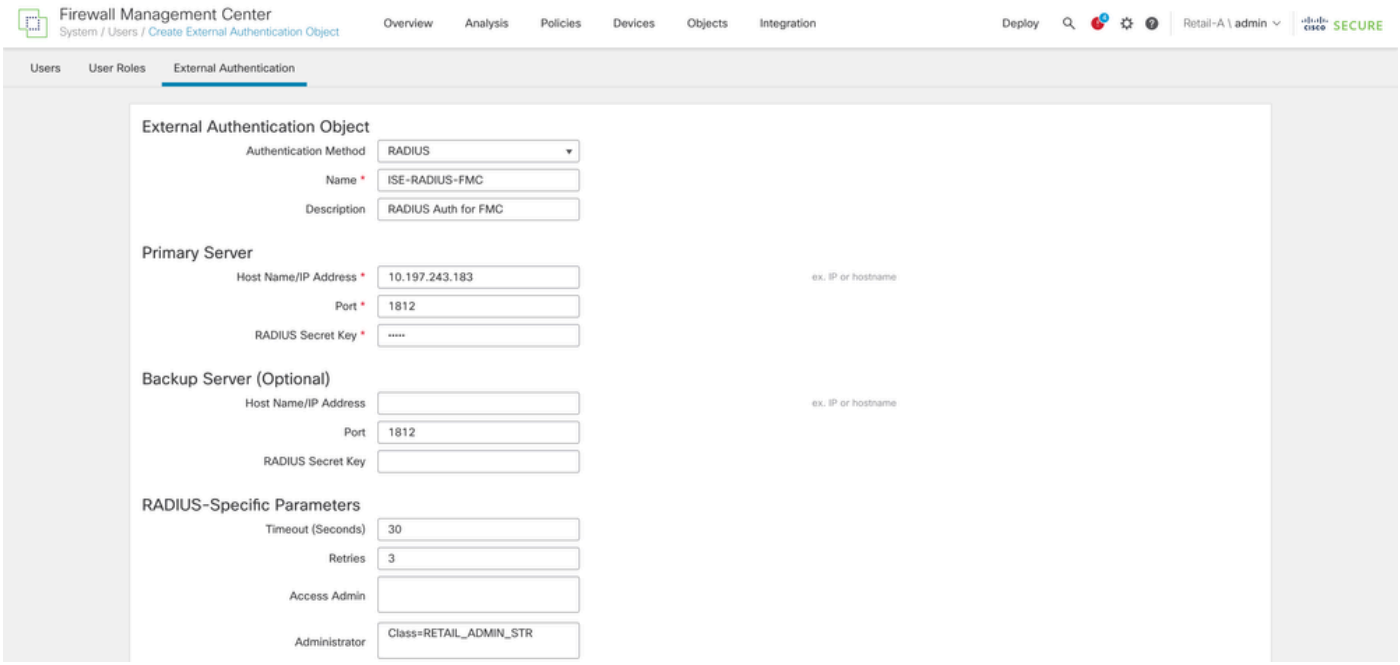

Étape 2.1. Configurez l'objet d'authentification externe sous Domain to Retail-A

- Basculez le domaine vers Retail-A.
- Accédez à System > Users > External Authentication.
- Sélectionnez Add External Authentication Object et choisissez RADIUS.
- Saisissez l'adresse IP ISE et le secret partagé configurés précédemment.
- Saisissez les paramètres spécifiques à RADIUS > Administrator > class=RETAIL_ADMIN_STR

---

Conseil : Utilisez la même valeur pour class que celle configurée sous Profils d'autorisation ISE.

---



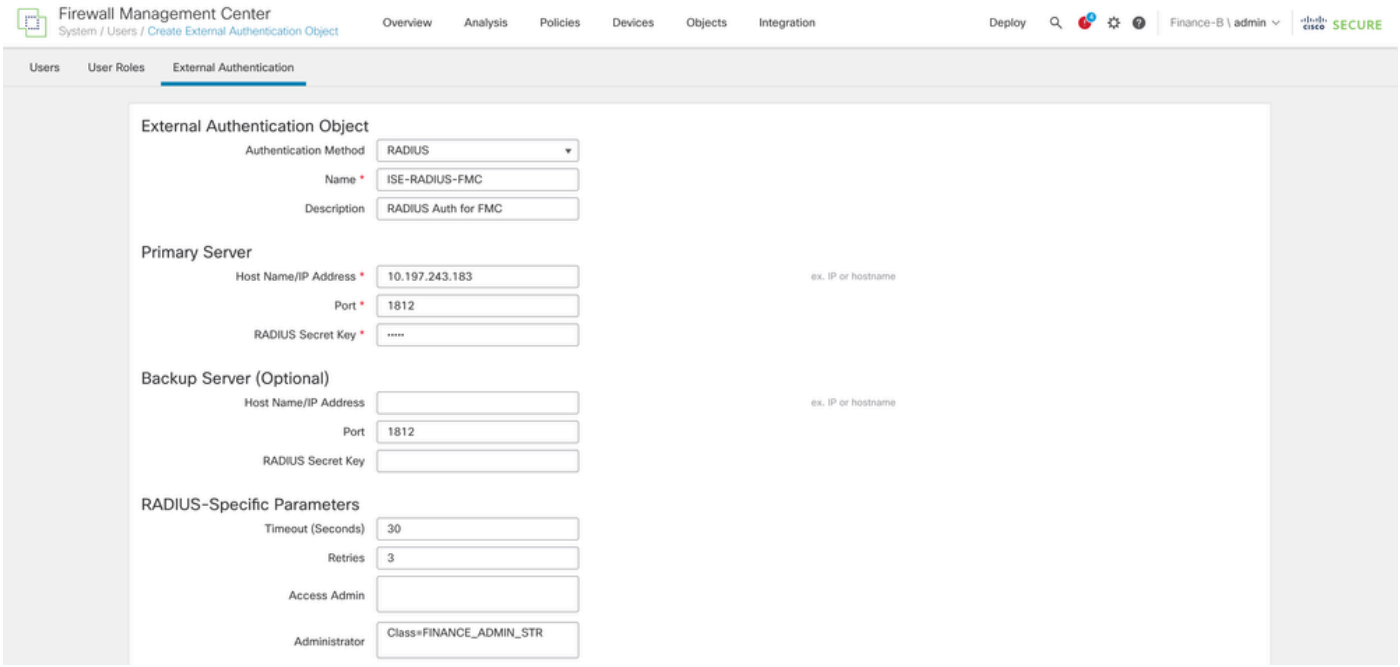

Étape 2.2. Configurez l'objet d'authentification externe sous Domaine sur Finance-B

- Basculer le domaine vers Finance-B.
- Accédez à System > Users > External Authentication.
- Sélectionnez Add External Authentication Object et choisissez RADIUS.
- Entrez l'adresse IP ISE et le secret partagé configurés précédemment.
- Saisissez les paramètres spécifiques à RADIUS > Administrator > class=FINANCE_ADMIN_STR

---

Conseil : Utilisez la même valeur pour class que celle configurée sous Profils d'autorisation ISE.

---




Étape 3. Activer l'authentification : Activez l'objet et définissez-le en tant que méthode d'authentification Shell. Cliquez sur Enregistrer et appliquer.

# Vérification

## Test de connexion interdomaine

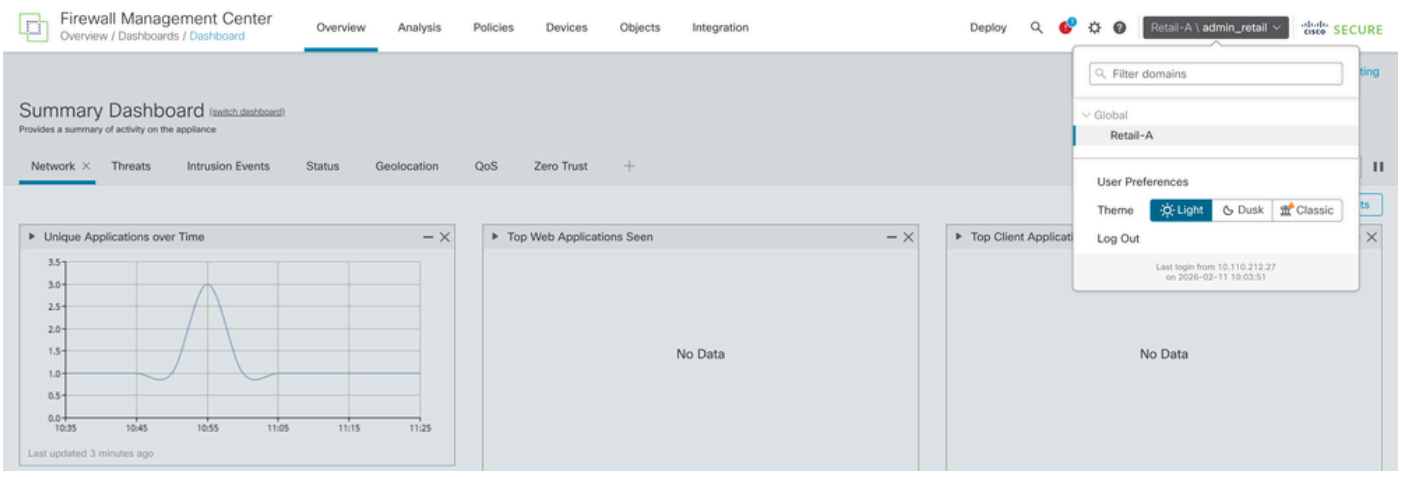
- Essayez de vous connecter à l'interface Web FMC en utilisant admin_retail. Vérifiez que le domaine actuel affiché en haut à droite de l'interface utilisateur est Retail-A.

---

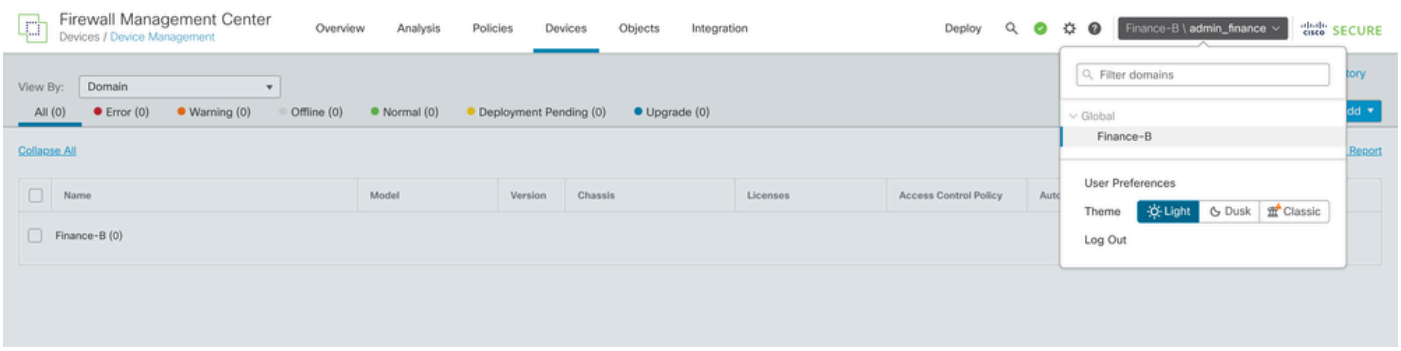
Conseil : Lorsque vous vous connectez à un domaine spécifique, utilisez le format nom_utilisateur nom_domaine\radius_utilisateur_mappé_avec_ce_domaine.

Par exemple, si l'utilisateur Retail admin doit se connecter, le nom d'utilisateur doit être Retail-A\admin_retail et le mot de passe correspondant.

---



- Déconnectez-vous et connectez-vous en tant qu'admin_finance. Vérifiez que l'utilisateur est limité au domaine Finance-B et qu'il ne peut pas voir les périphériques Retail-A.

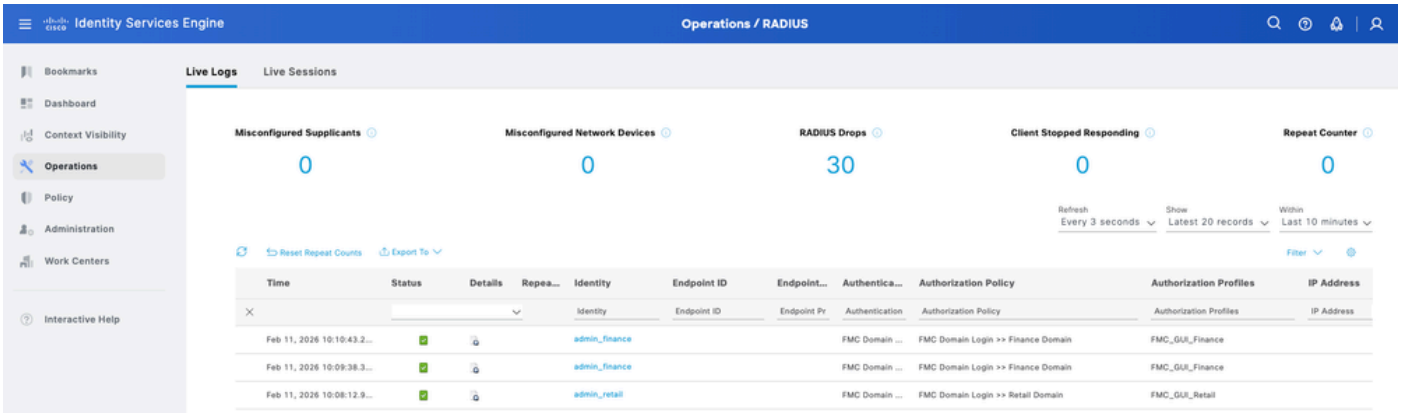



## Tests internes FMC

Accédez aux paramètres du serveur RADIUS dans le FMC. Utilisez la section Additional Test Parameters pour entrer un nom d'utilisateur et un mot de passe de test. Un test réussi doit afficher un message de réussite vert.


## Journaux en direct ISE

- Dans Cisco ISE, accédez à Operations > RADIUS > Live Logs.




- Vérifiez que les demandes d'authentification présentent un état de réussite et que le profil d'autorisation correct (et la chaîne de classe associée) a été envoyé dans le paquet RADIUS Access-Accept.

### Overview

| | |
|---|---|
| Event | 5200 Authentication succeeded |
| Username | admin_finance |
| Endpoint Id | |
| Endpoint Profile | |
| Authentication Policy | FMC Domain Login >> Default |
| Authorization Policy | FMC Domain Login >> Finance Domain |
| Authorization Result | FMC_GUI_Finance |

### Authentication Details

| | |
|---|---|
| Source Timestamp | 2026-02-11 16:40:43.275 |
| Received Timestamp | 2026-02-11 22:10:43.275 |
| Policy Server | eagle |
| Event | 5200 Authentication succeeded |
| Username | admin_finance |
| User Type | User |
| Authentication Identity Store | Internal Users |
| Identity Group | User Identity Groups:Group_Finance_B |

### Result

| | |
|---|---|
| Class | FINANCE_ADMIN_STR |
| Class | CACS:0ac5f3b7m0vFomvHHyC_igO13NsO1DZN6QciDbrc0cwlaYWHMto:eagle/556377151/553 |

## Informations connexes

Configurer l'authentification externe FMC et FTD avec ISE en tant que serveur RADIUS

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.