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

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Authentification externe pour FMC
  - Authentification externe pour FTD
  - Topologie du réseau
- Configurer
  - Configuration ISE
    - Ajouter vos périphériques réseau
    - Créer les groupes et utilisateurs d'identités d'utilisateurs locaux
    - Créer les profils d'autorisation
    - Ajouter un nouvel ensemble de stratégies
  - Configuration FMC
    - Ajouter votre serveur RADIUS ISE pour l'authentification FMC
  - Configuration FTD
    - Ajouter votre serveur RADIUS ISE pour l'authentification FTD
    - Activer le serveur RADIUS
- Vérifier

Introduction

Ce document décrit un exemple de configuration d'authentification externe pour Secure Firewall Management Center et Firewall Threat Defense.

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.
- Configuration des stratégies d'authentification et d'autorisation sur ISE.
- Connaissances de base de RADIUS.

Composants utilisés

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

- vFMC 7.4.2
- vFTD 7.4.2
- 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

Lorsque vous activez l'authentification externe pour les utilisateurs de gestion et d'administration de votre système Secure Firewall, le périphérique vérifie les informations d'identification de l'utilisateur à l'aide d'un serveur LDAP (Lightweight Directory Access Protocol) ou RADIUS comme spécifié dans un objet d'authentification externe.

Les objets d'authentification externes peuvent être utilisés par les périphériques FMC et FTD. Vous pouvez partager le même objet entre les différents types d'appareils ou de périphériques, ou créer des objets distincts.

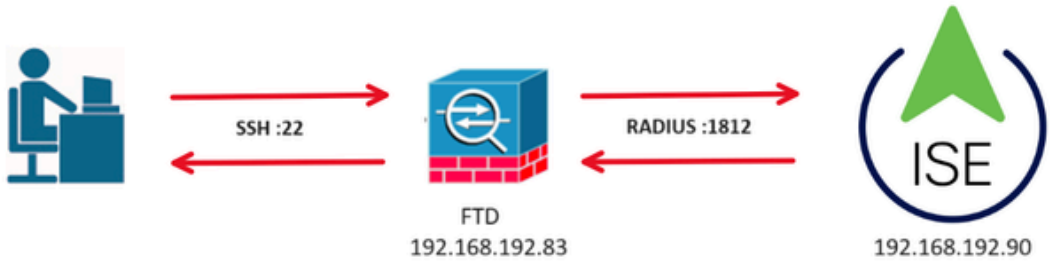
Authentification externe pour FMC

Vous pouvez configurer plusieurs objets d'authentification externes pour l'accès à l'interface Web. Un seul objet d'authentification externe peut être utilisé pour l'accès CLI ou shell.

Authentification externe pour FTD

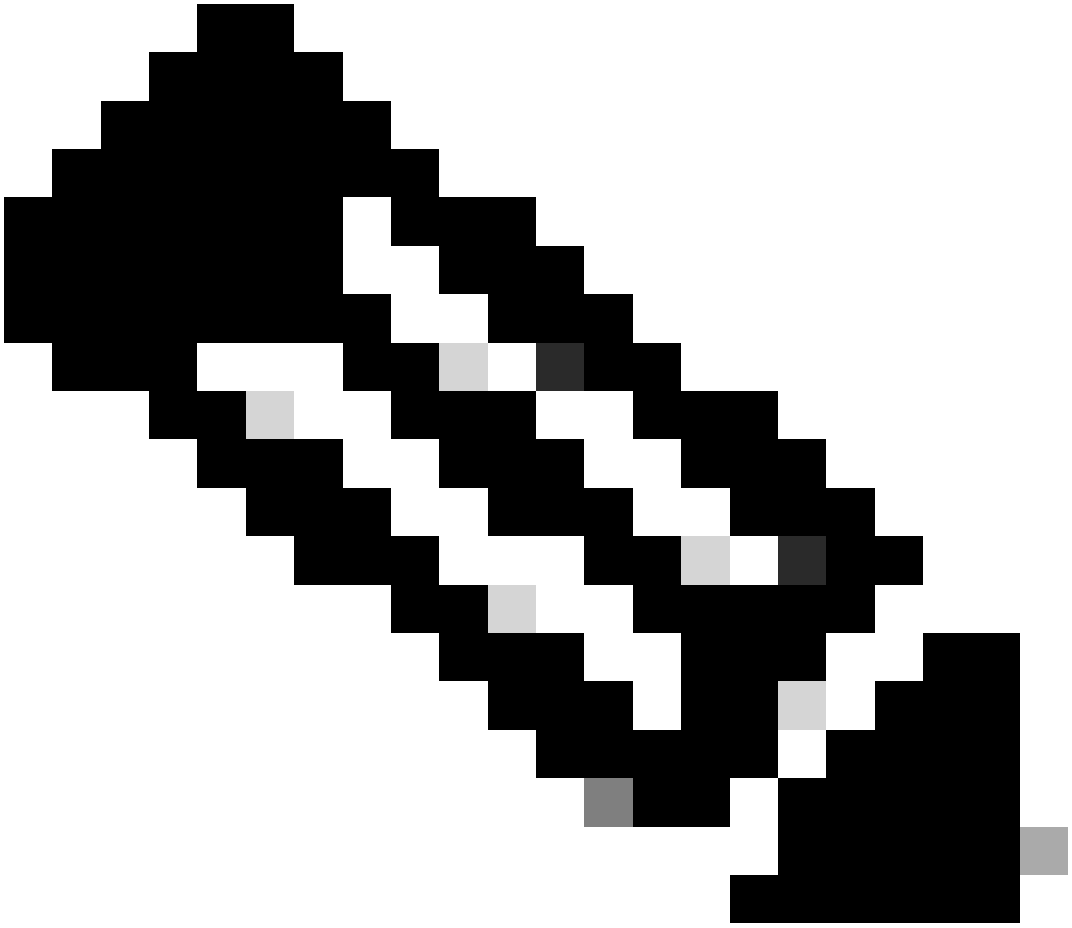
Pour le FTD, vous ne pouvez activer qu'un seul objet d'authentification externe.

Topologie du réseau



Configurer

Configuration ISE

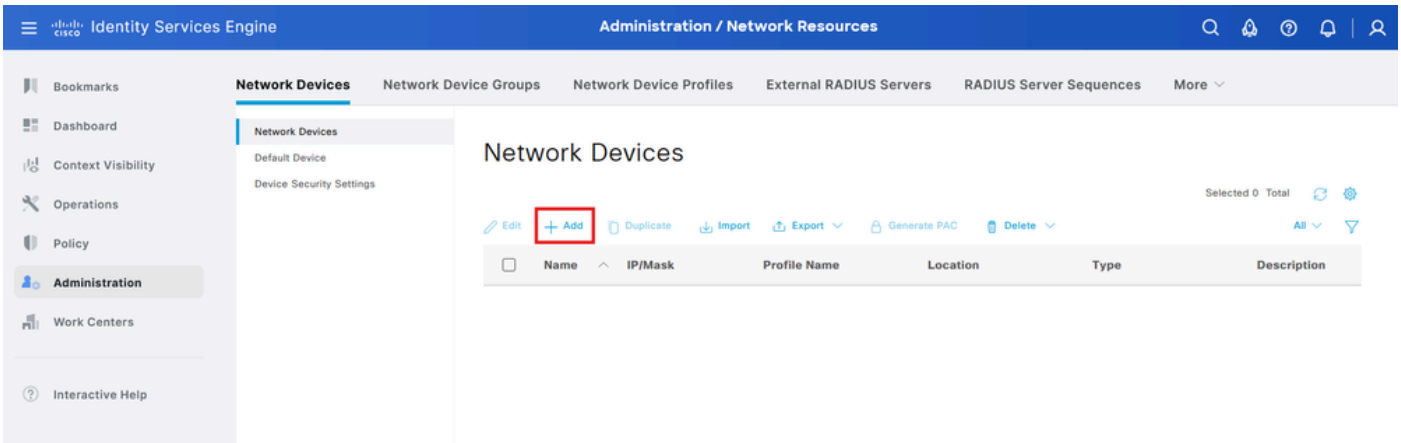


Remarque : Il existe plusieurs façons de configurer les stratégies d'authentification et d'autorisation ISE pour les périphériques d'accès réseau (NAD) tels que FMC. L'exemple décrit dans ce document est un point de référence dans lequel nous créons deux profils (l'un avec des droits d'administrateur et l'autre en lecture seule) et peut être adapté pour répondre aux lignes de base pour accéder à votre réseau. Une ou plusieurs stratégies d'autorisation peuvent être définies sur ISE avec le renvoi de valeurs d'attribut RADIUS au FMC qui sont ensuite mappées à un groupe d'utilisateurs local défini dans la configuration de stratégie système FMC.

Ajouter vos périphériques réseau

Étape 1. Accédez à l'icône Burger

situé dans le coin supérieur gauche >Administration > Network Resources > Network Devices > +Add.

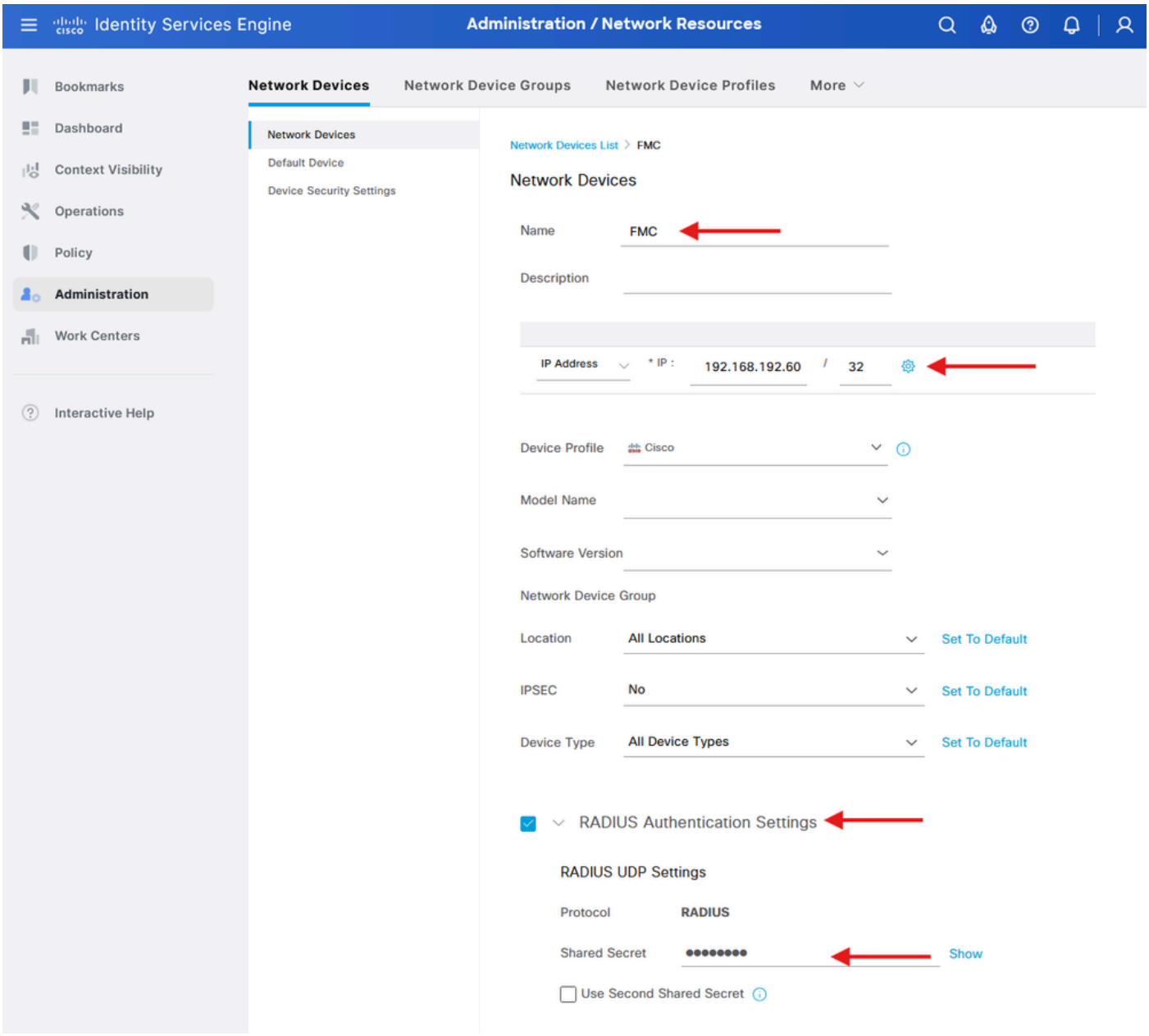


Étape 2 : attribution d'un nom à l'objet périphérique réseau et insertion de l'adresse IP FMC.

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.

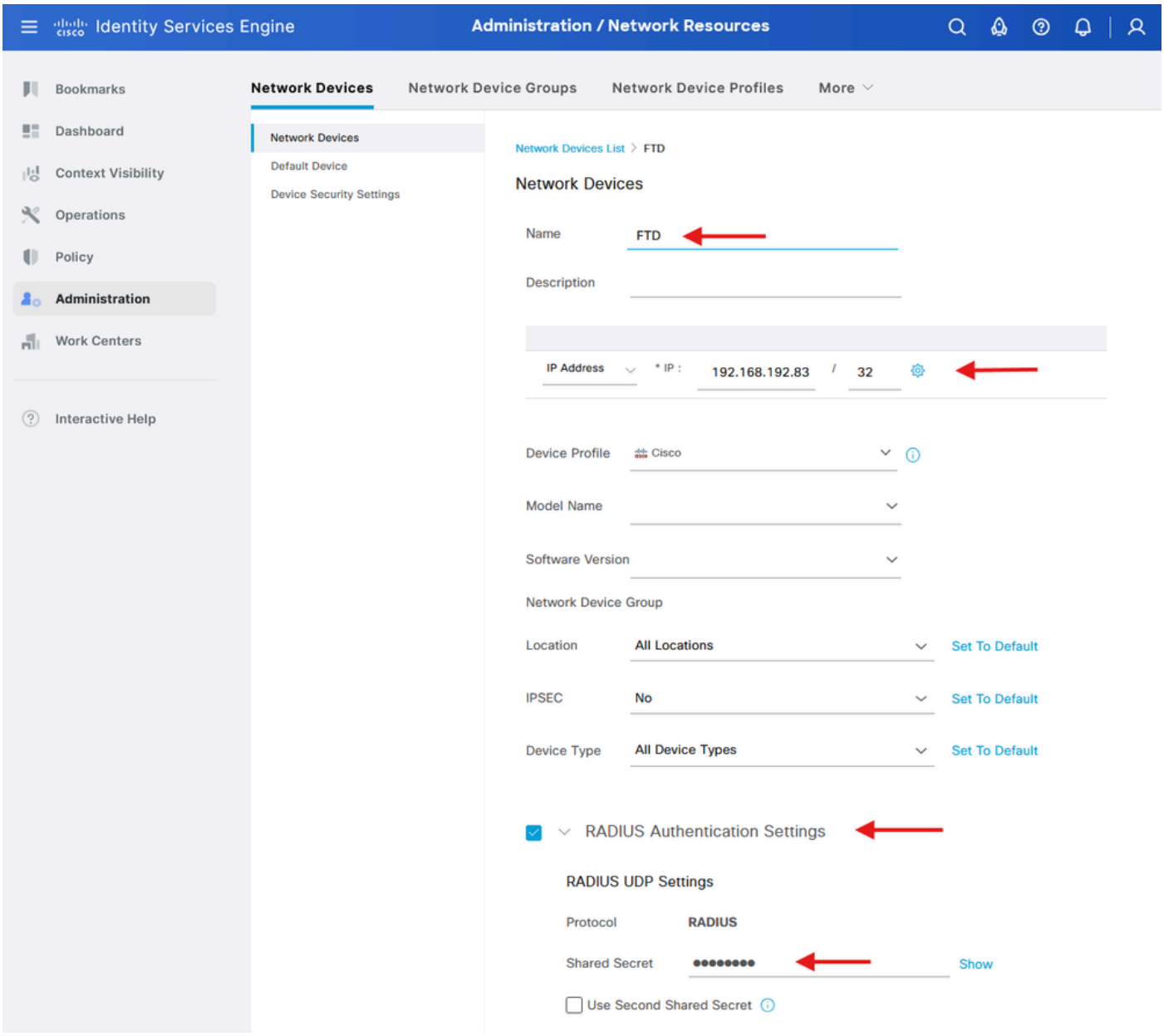


Étape 2.1. Répétez la même procédure pour ajouter le FTD.

Attribuez un nom à l'objet périphérique réseau et insérez l'adresse IP FTD.

Cochez la case RADIUS et définissez un secret partagé.

Une fois terminé, cliquez sur Enregistrer.

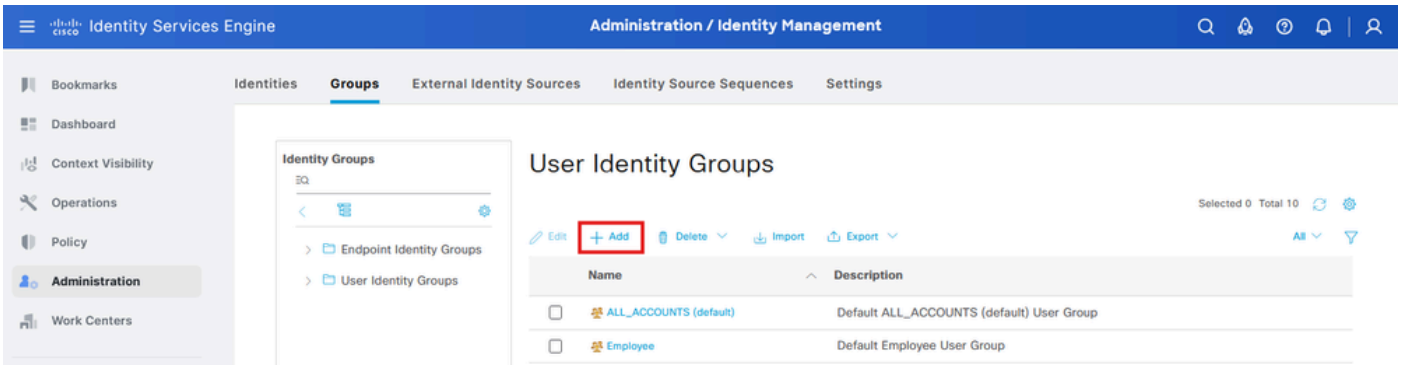


Étape 2.3. Validez que les deux périphériques sont affichés sous Périphériques réseau.

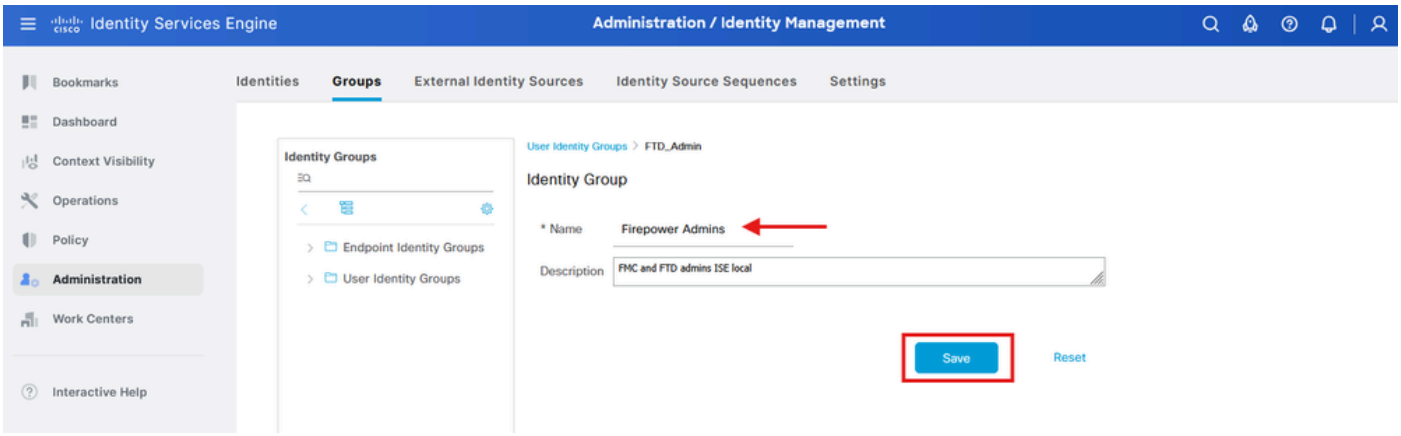
Créer les groupes et utilisateurs d'identités d'utilisateurs locaux

Étape 3 : création des groupes d'identités utilisateur requis Accédez à l'icône Burger

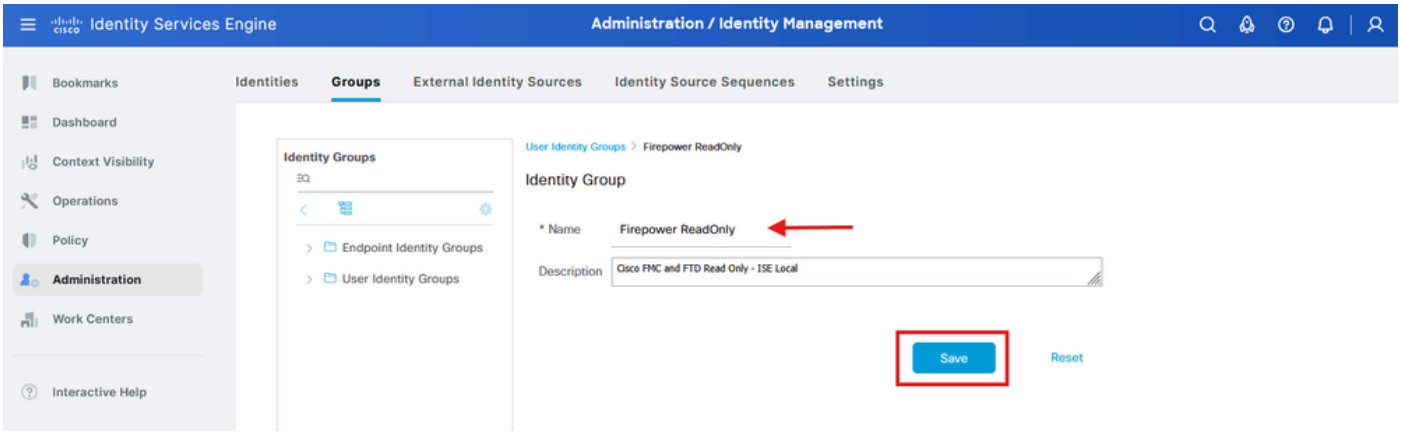
situé dans le coin supérieur gauche > Administration > Identity Management > Groups > User Identity Groups > + Add



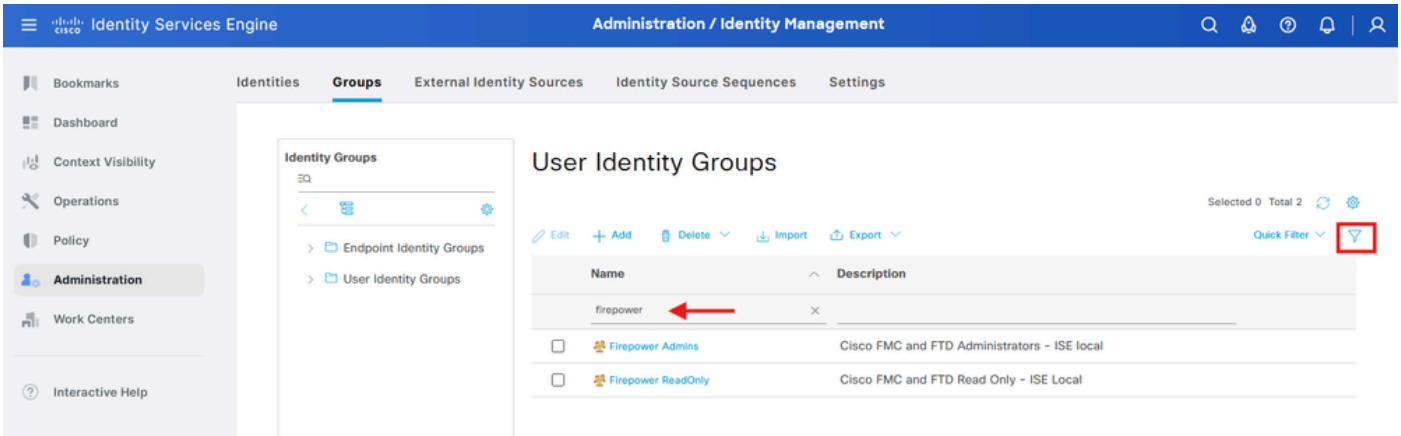
Étape 4. Attribuez un nom à chaque groupe et enregistrez-le individuellement. Dans cet exemple, nous créons un groupe pour les administrateurs et un autre pour les utilisateurs en lecture seule. Commencez par créer le groupe pour l'utilisateur disposant de droits d'administrateur.



Étape 4.1. Créez le deuxième groupe pour l'utilisateur ReadOnly.

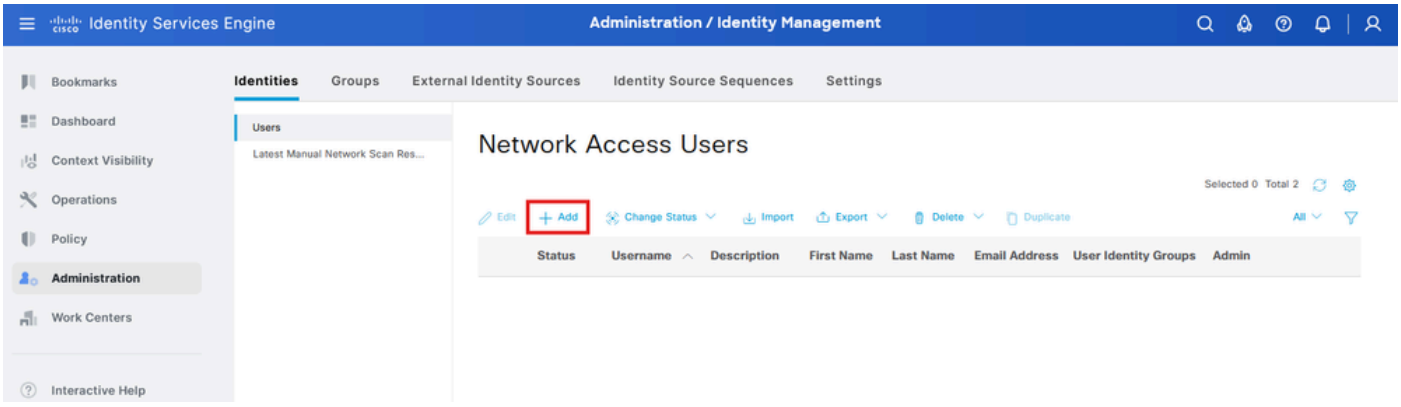


Étape 4.2. Validez que les deux groupes sont affichés dans la liste des groupes d'identité d'utilisateur. Utilisez le filtre pour les trouver facilement.

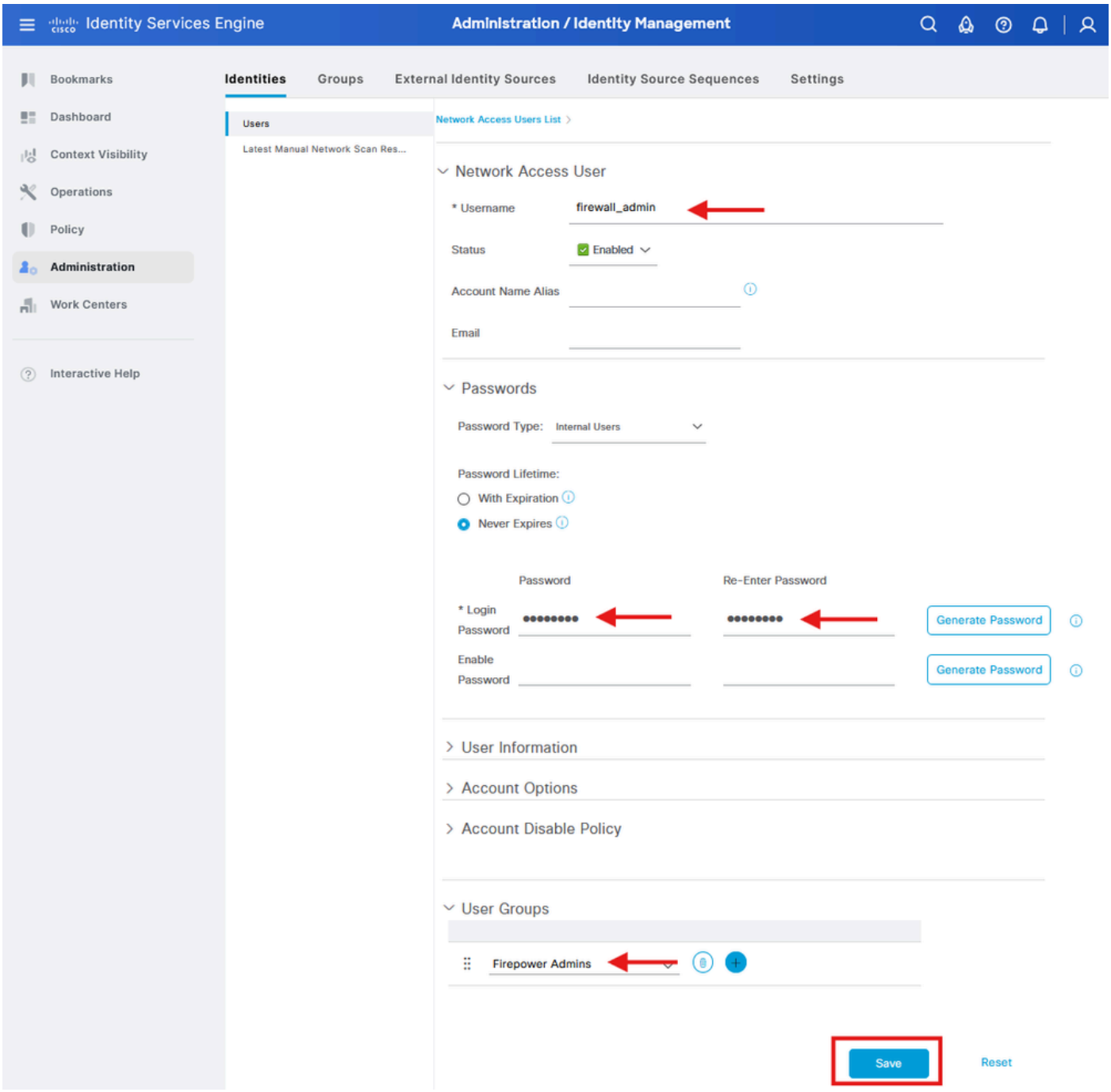


Étape 5. Créez les utilisateurs locaux et ajoutez-les à leur groupe de correspondants. Naviguez jusqu'à

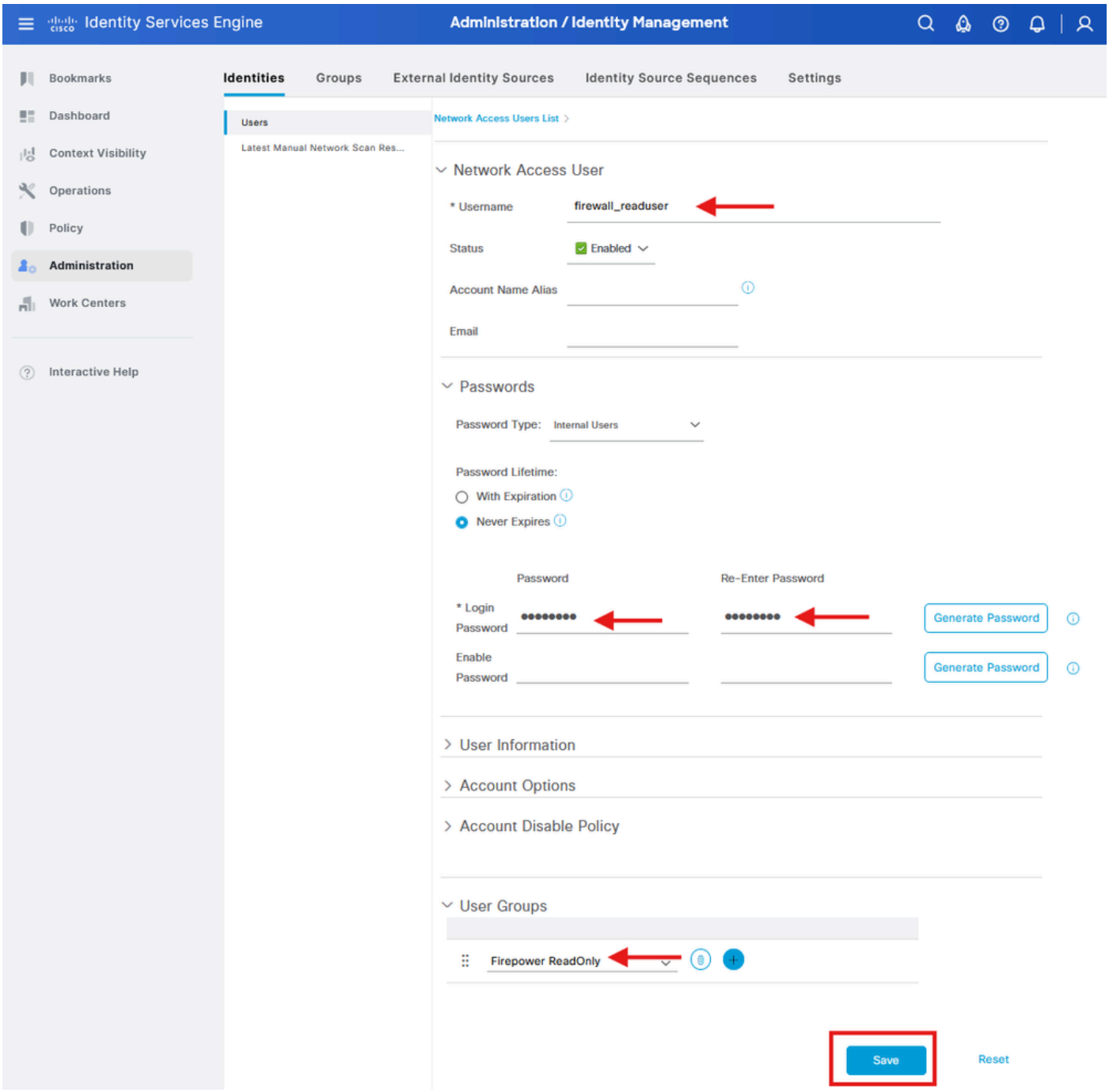
> Administration > Gestion des identités > Identités > + Ajouter.



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



Étape 5.2. Ajouter l'utilisateur avec des droits ReadOnly Attribuez un nom, un mot de passe et le groupe Firepower ReadOnly.



Créer les profils d'autorisation

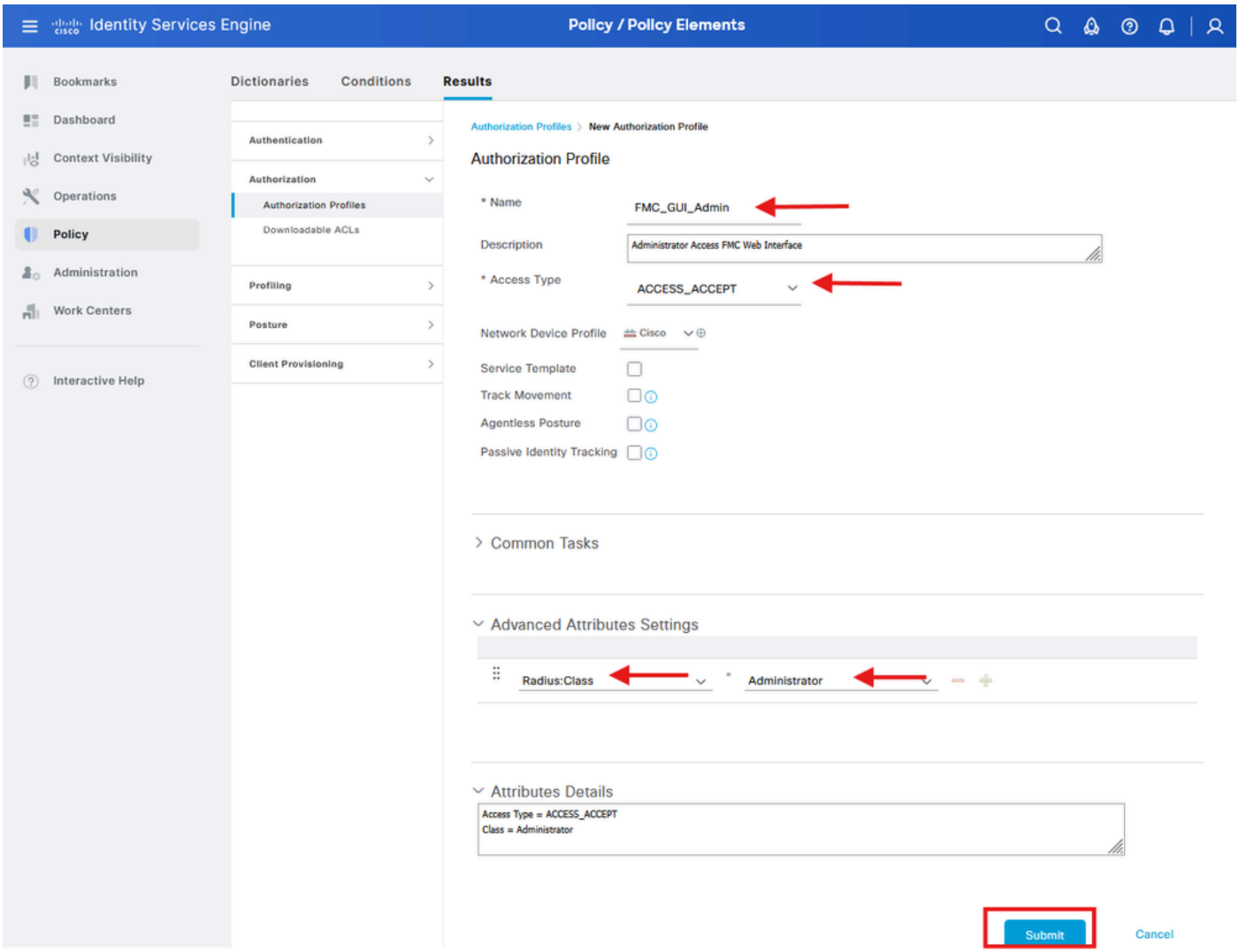
Étape 6 : création du profil d’autorisation pour l’utilisateur Administrateur de l’interface Web FMC

Naviguez jusqu'à

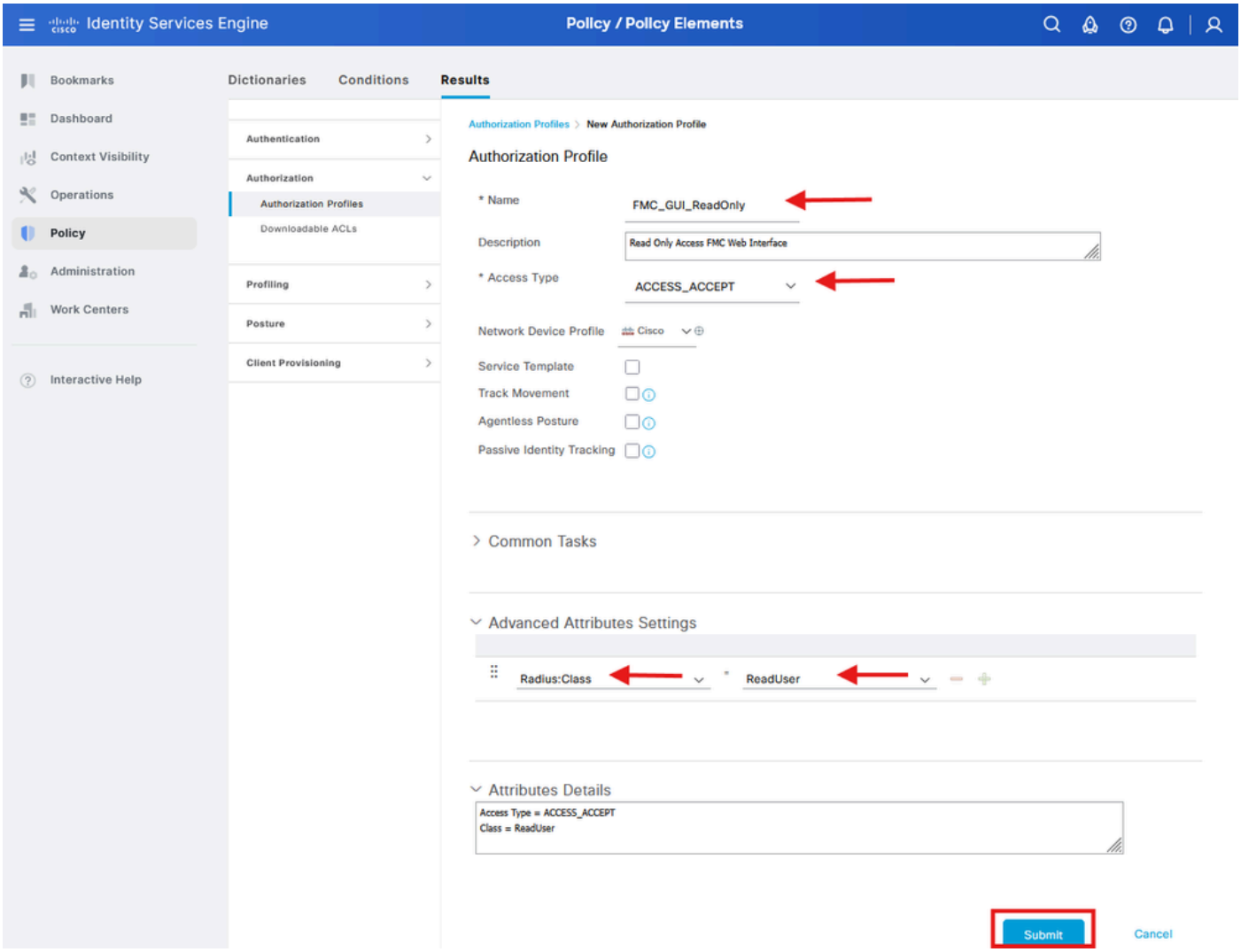
> Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation > +Ajouter.

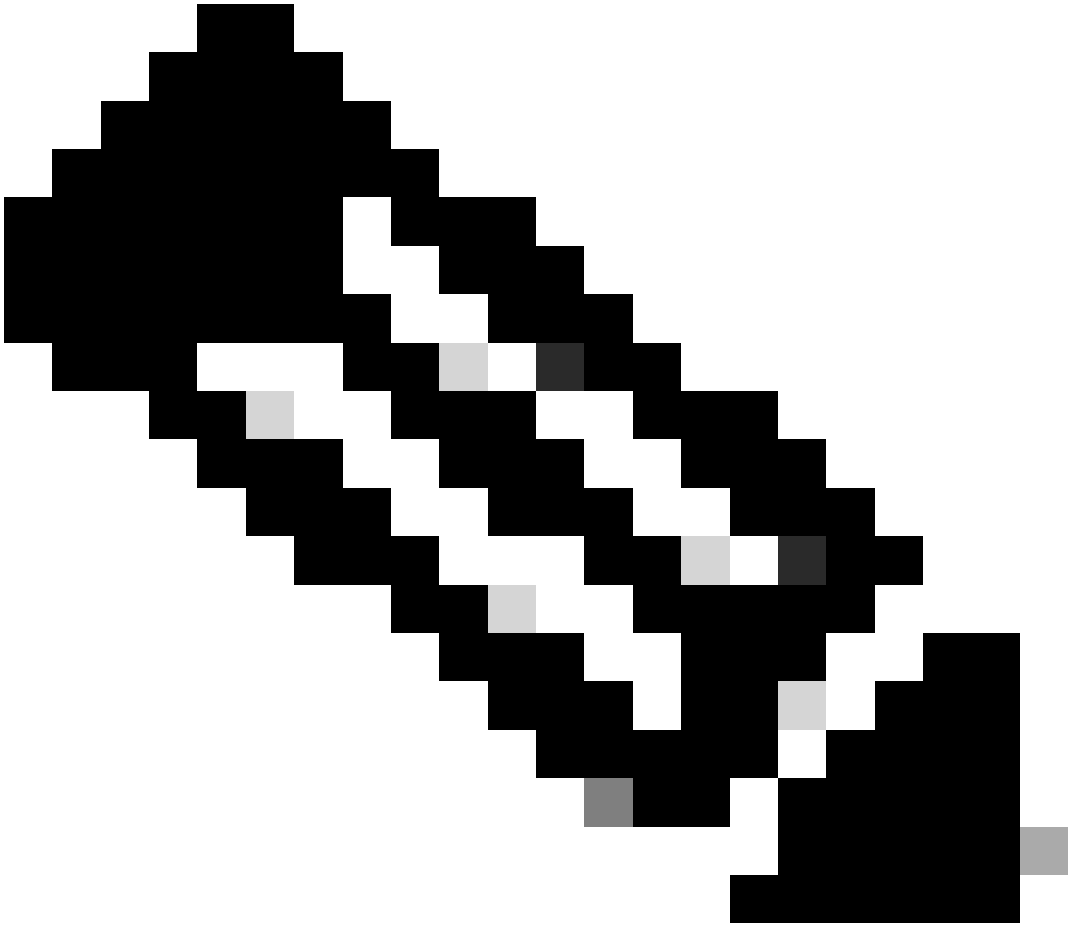
Définissez un nom pour le profil d'autorisation, laissez le type d'accès ACCESS_ACCEPT.

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



Étape 6.1. Répétez l'étape précédente pour créer le profil d'autorisation pour l'utilisateur ReadOnly de l'interface Web FMC. Cette fois, créez la classe Radius avec la valeur ReadUser au lieu de Administrator.


Identity Services Engine
Policy / Policy Elements
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
FMC_GUI_ReadOnly
Description
Read Only Access FMC Web Interface
* Access Type
ACCESS_ACCEPT
Network Device Profile
Cisco
Service Template
Track Movement
Agentless Posture
Passive Identity Tracking
Common Tasks
Advanced Attributes Settings
Radius:Class
ReadUser
Attributes Details
Access Type = ACCESS_ACCEPT
Class = ReadUser
Submit
Cancel



Remarque : Pour FMC (toutes versions) et FTD (6.2.3 et 6.3), vous devez définir des utilisateurs pour l'accès à l'interface de ligne de commande (CLI) dans l'objet d'authentification externe FMC, que j'affiche à l'étape 4 de la procédure de configuration FMC. Pour FTD 6.4 et versions ultérieures, nous vous recommandons de définir des utilisateurs sur le serveur RADIUS comme je vous le montre à l'étape suivante.

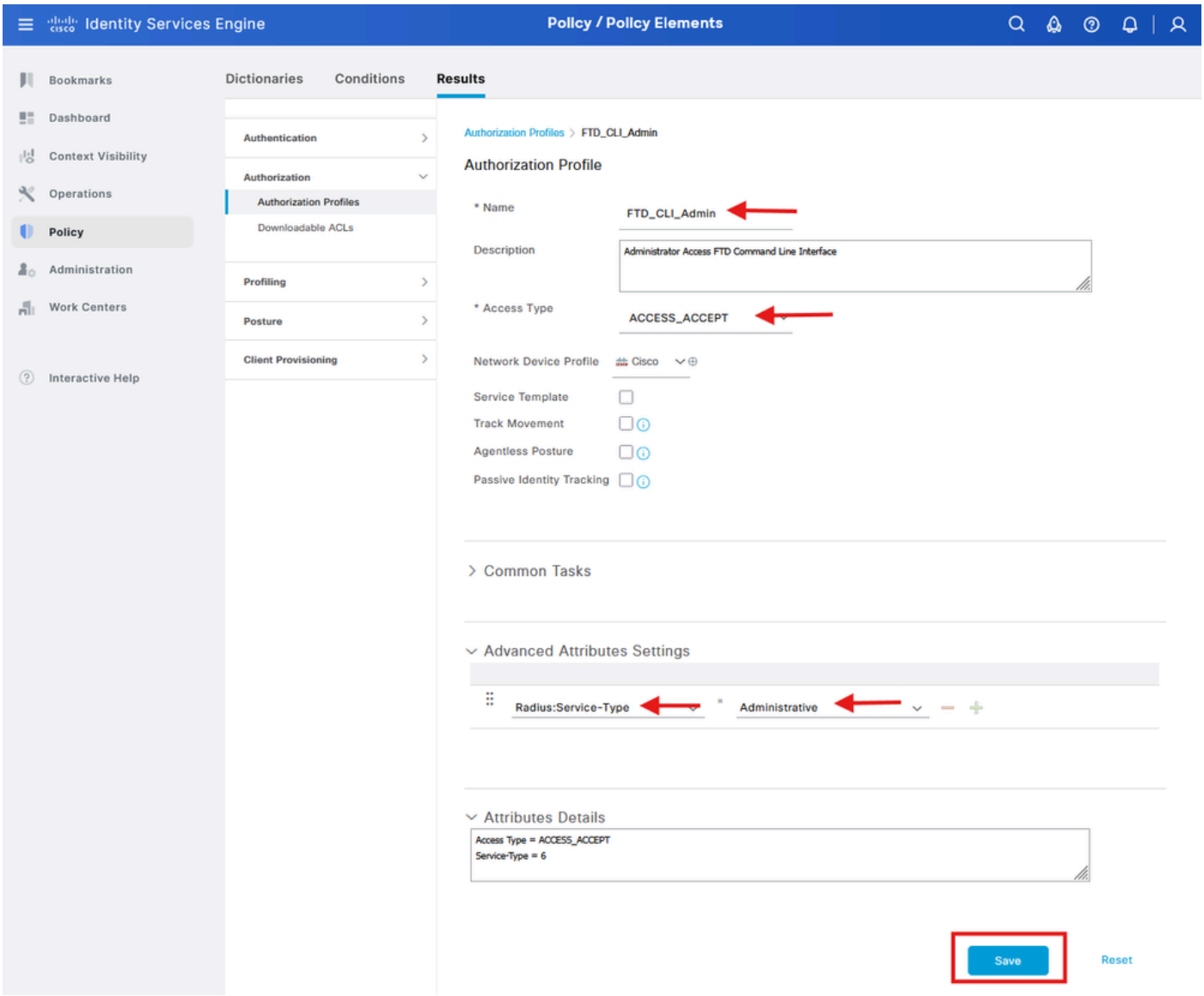
Étape 7. Créez le profil d'autorisation pour l'utilisateur CLI FTD disposant de droits d'administrateur.

Naviguez jusqu'à

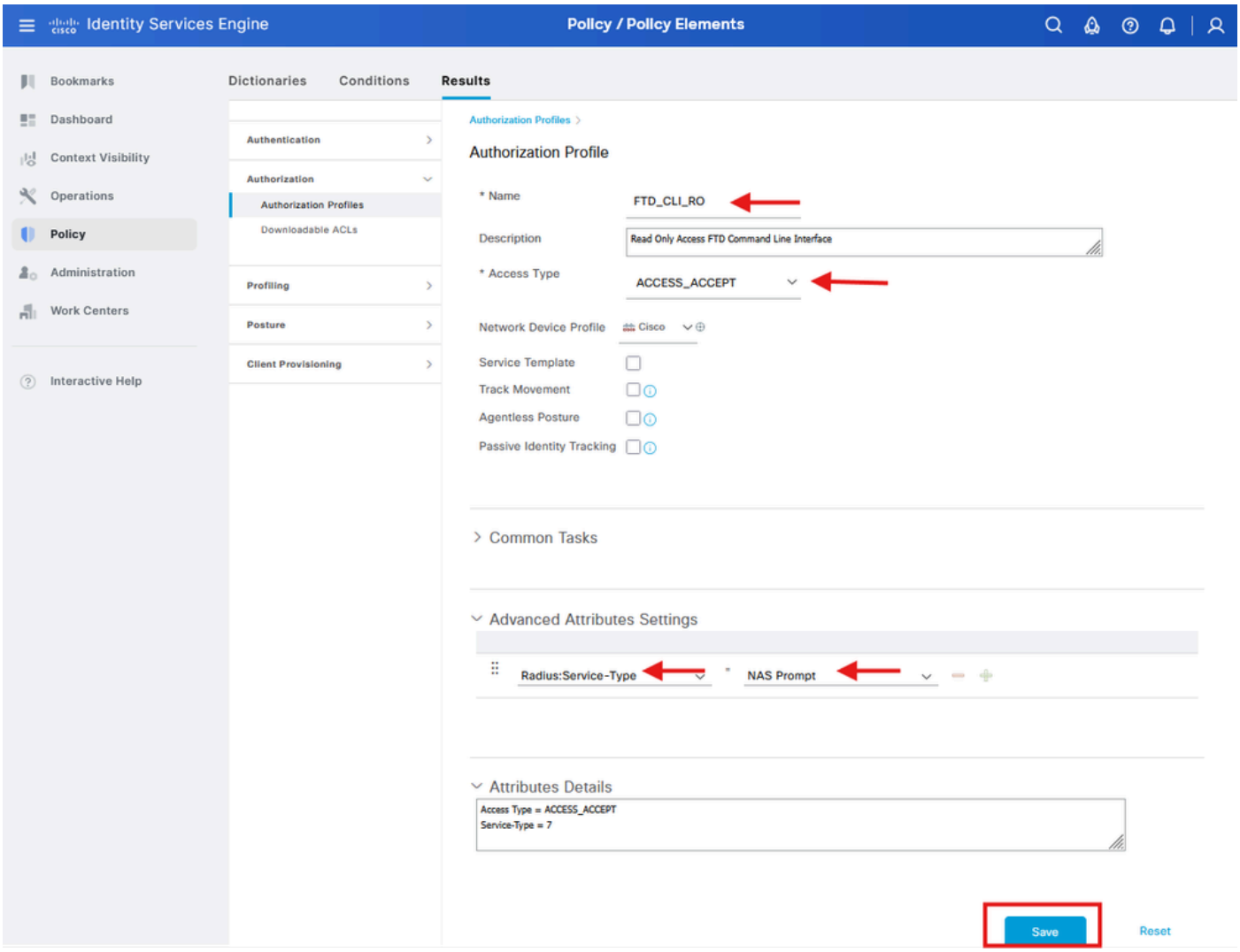
> Stratégie > Éléments de stratégie > Résultats > Autorisation > Profils d'autorisation > +Ajouter.

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

Sous Advanced Attributes Settings, ajoutez un Radius > Service-Type—[6] avec la valeur Administrative et cliquez sur Submit.



Étape 7.1. Répétez l'étape précédente pour créer le profil d'autorisation pour l'utilisateur FTD CLI ReadOnly. Cette fois, créez Radius > Service-Type—[6] avec la valeur NAS Prompt à la place.

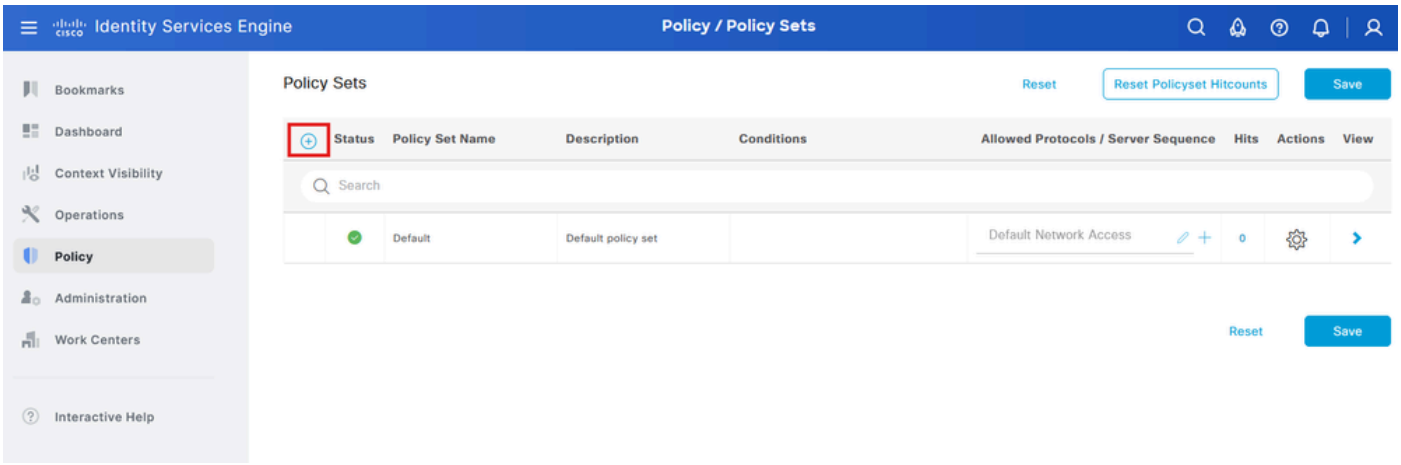


Ajouter un nouvel ensemble de stratégies

Étape 8 : 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.

Naviguez jusqu'à

> Stratégie **>** Ensembles de stratégies **>** placé dans l'angle supérieur gauche.

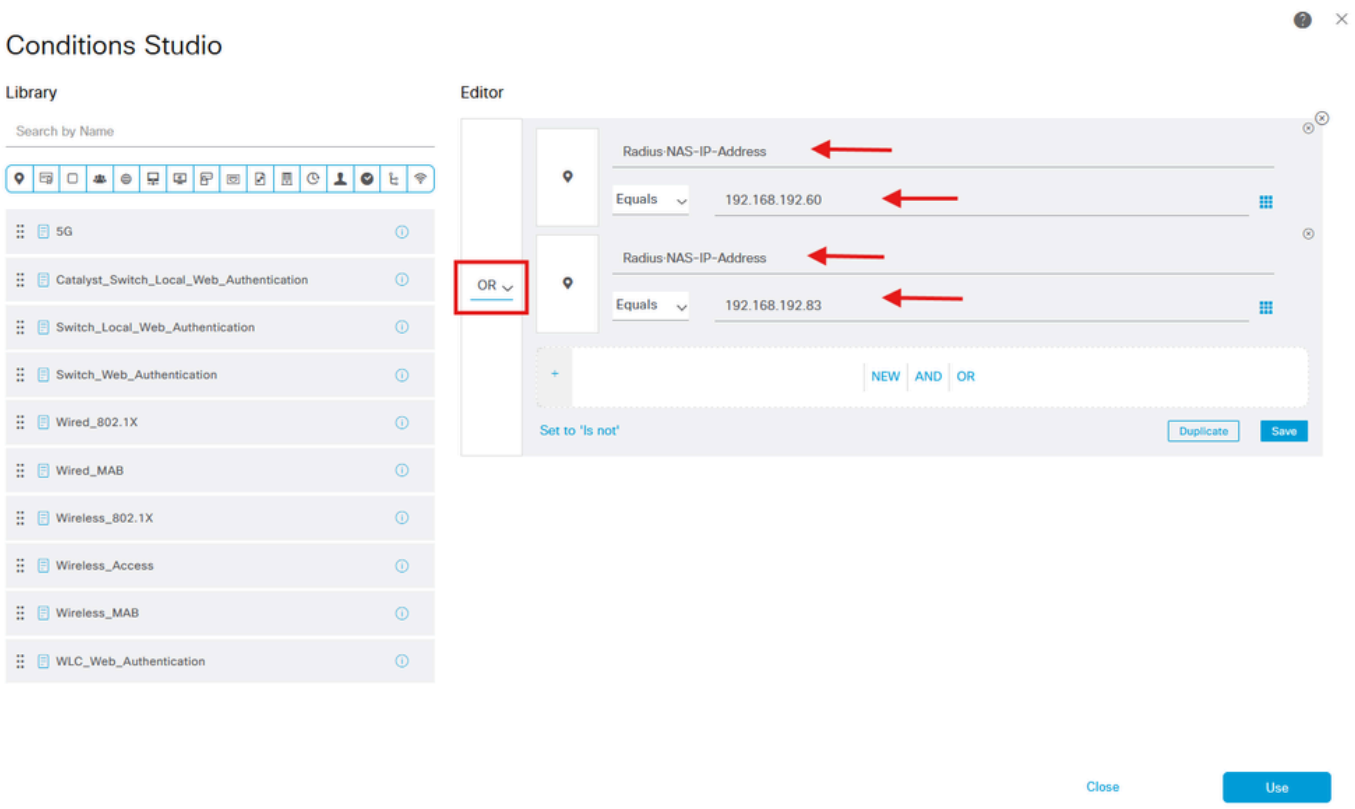


Étape 8.1. Une nouvelle ligne est placée en haut de vos ensembles de stratégies.

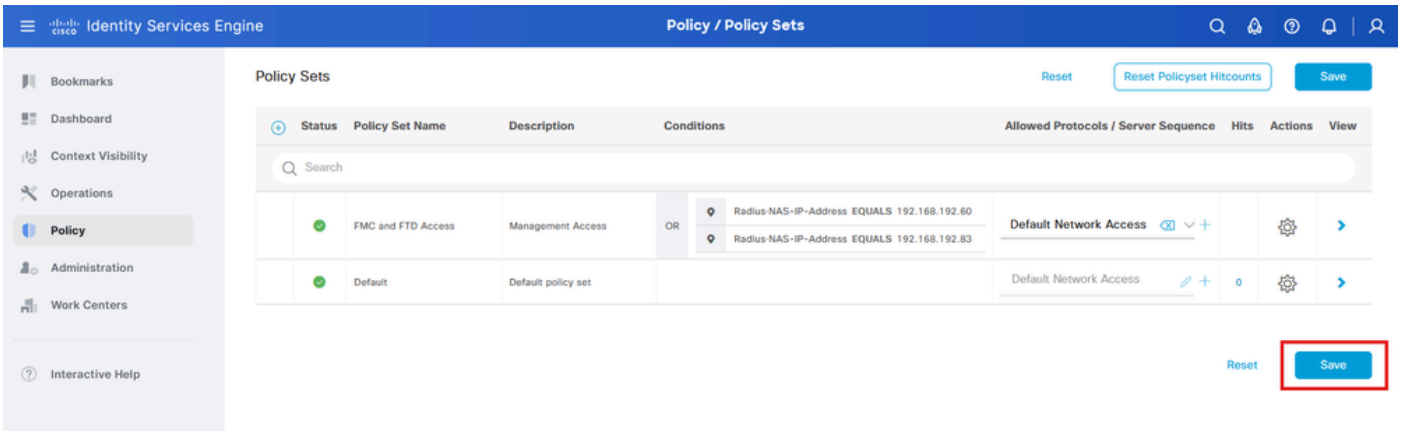
Nommez la nouvelle stratégie et ajoutez une condition supérieure pour l'attribut RADIUS NAS-IP-Address correspondant à l'adresse IP FMC.

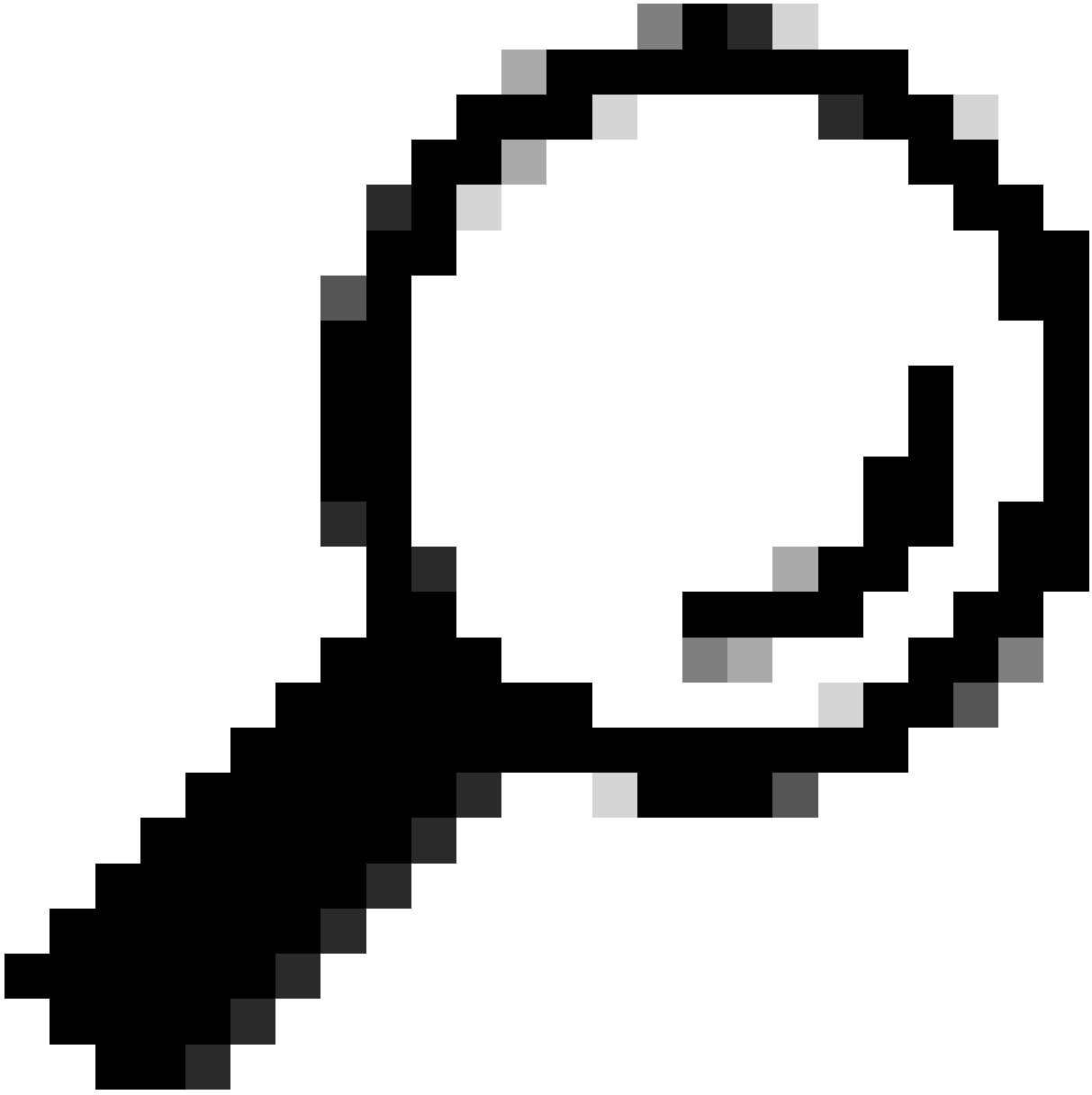
Ajoutez une deuxième condition avec la conjonction OR pour inclure l'adresse IP du FTD.

Cliquez sur Utiliser pour conserver les modifications et quitter l'éditeur.

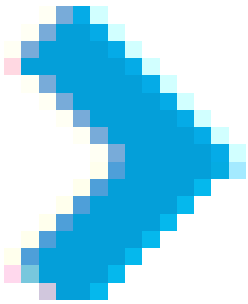


Étape 8.2. Une fois terminé, appuyez sur Enregistrer.

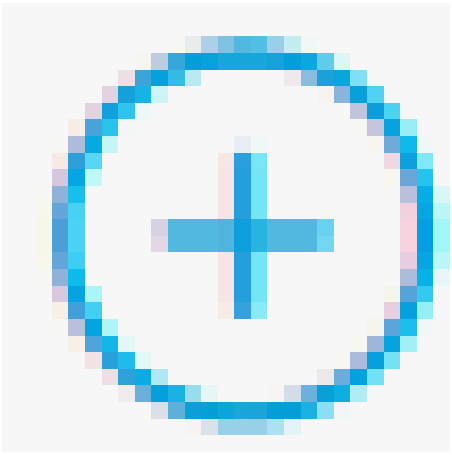




Conseil : Pour cet exercice, nous avons autorisé la liste Default Network Access Protocols. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.



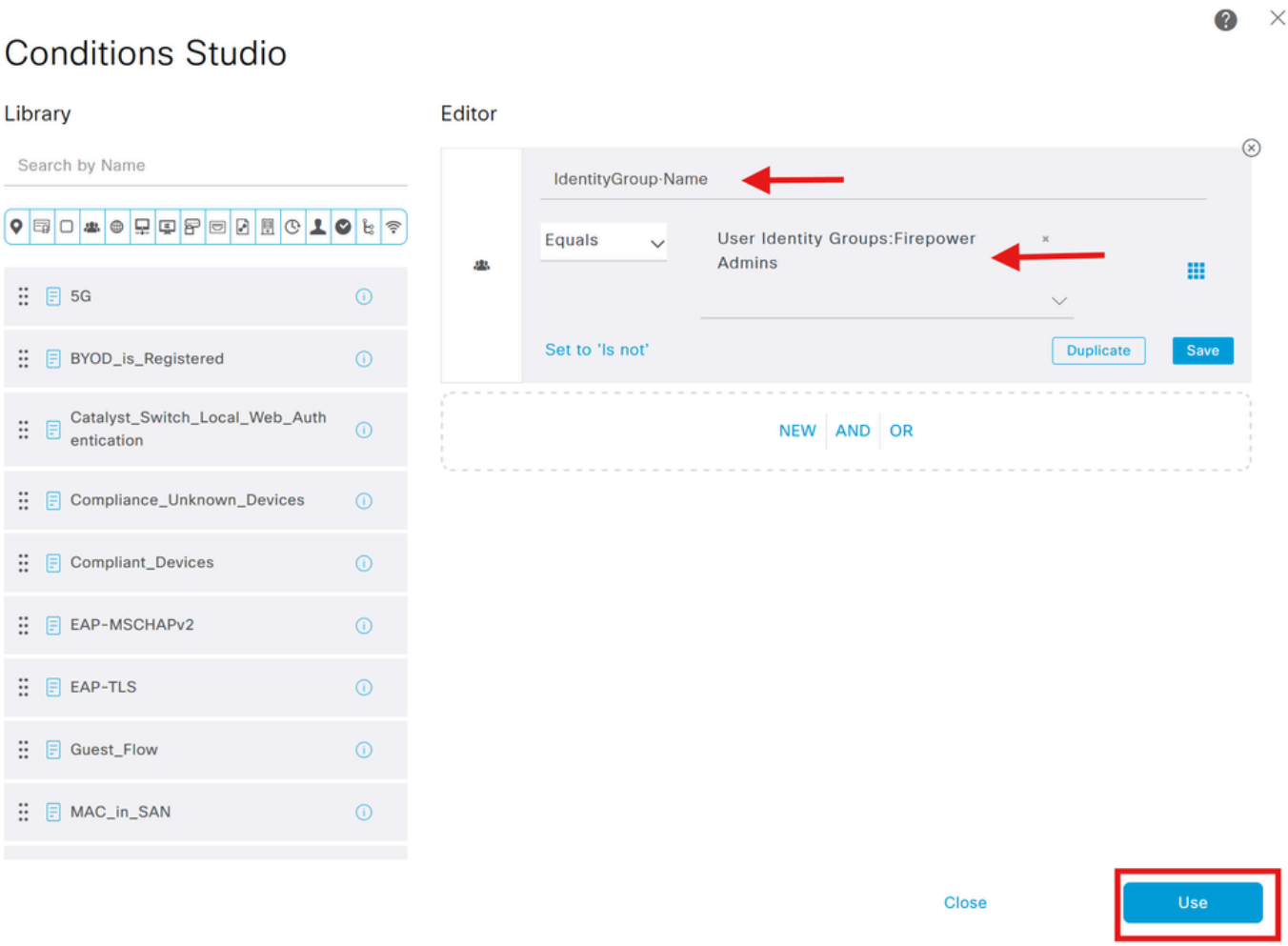
Étape 9. Affichez le nouvel ensemble de stratégies en cliquant sur le bouton placé à la fin de la ligne.



Développez le menu Authorization Policy et appuyez sur la touche pour ajouter une nouvelle règle autorisant l'accès à l'utilisateur disposant de droits d'administrateur.

Donnez-lui un nom.

Définissez les conditions pour faire correspondre le groupe d'identités du dictionnaire avec le nom d'attribut Égal à et choisissez Groupes d'identités d'utilisateurs : Firepower Admins (nom du groupe créé à l'étape 4) et cliquez sur Use.

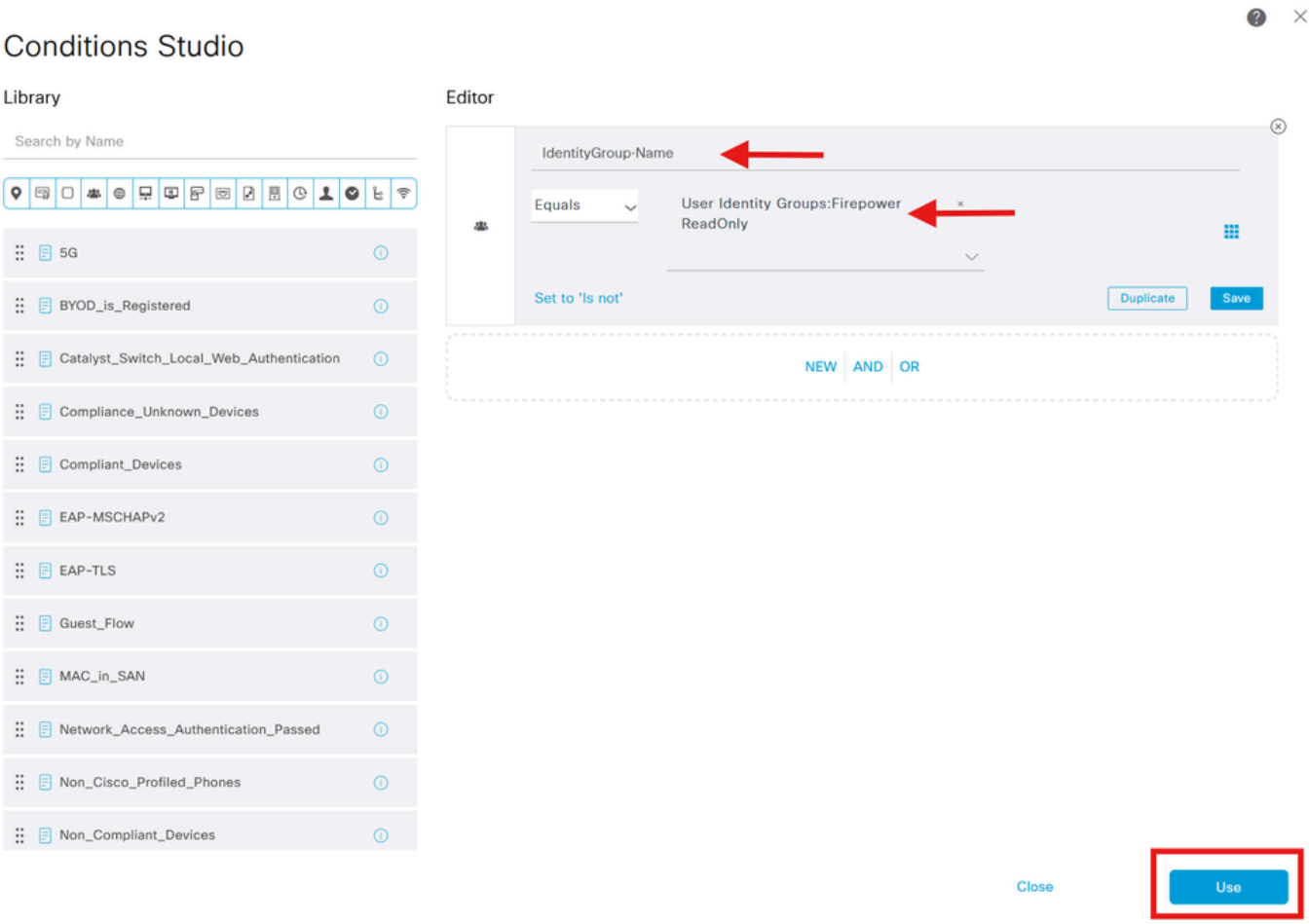


Étape 10. Cliquez sur le bouton

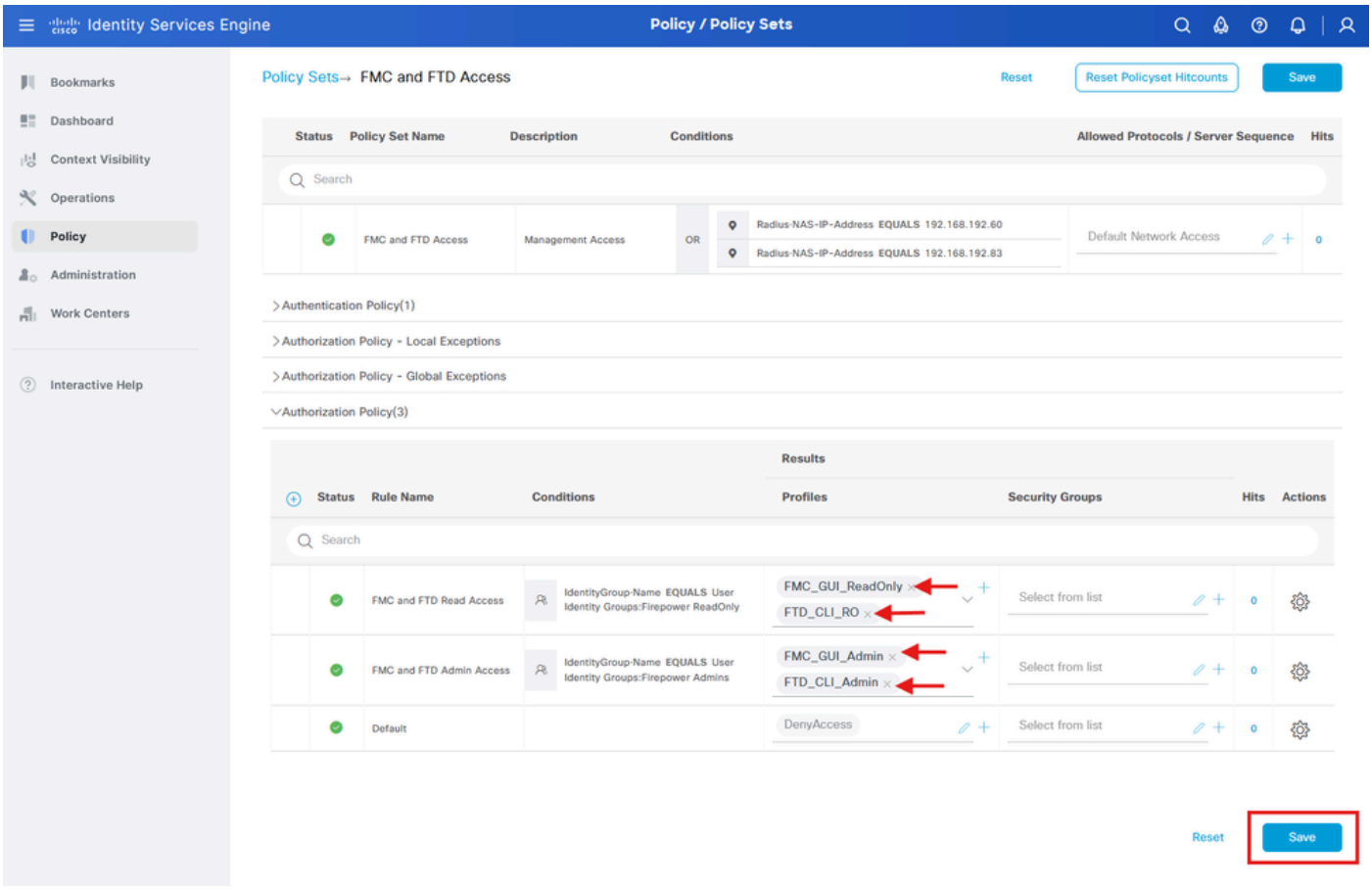
pour ajouter une deuxième règle autorisant l'accès à l'utilisateur avec des droits en lecture seule.

Donnez-lui un nom.

Définissez les conditions pour faire correspondre le groupe d'identités du dictionnaire avec le nom d'attribut et les groupes d'identités de l'utilisateur : Firepower ReadOnly (nom du groupe créé à l'étape 4.1) et cliquez sur Use.



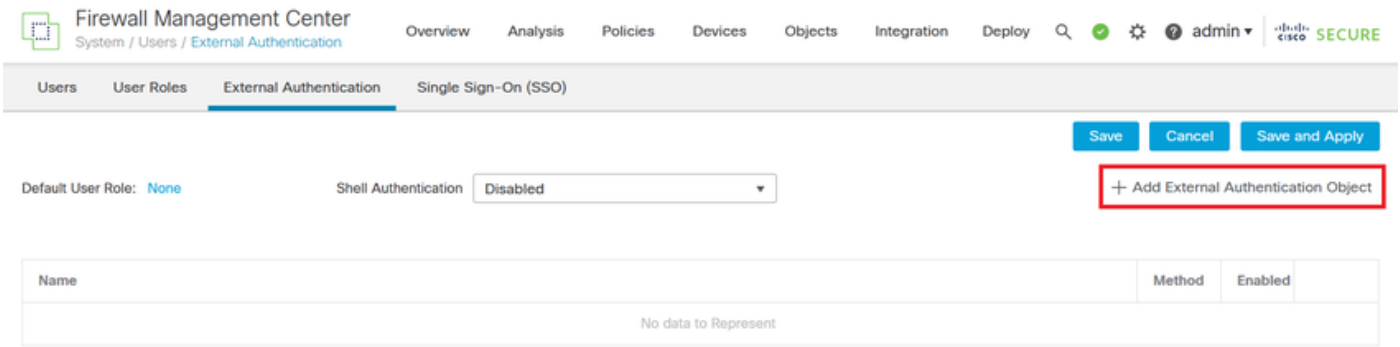
Étape 11. Définissez les profils d’autorisation respectivement pour chaque règle et cliquez sur Enregistrer.



Configuration FMC

Ajouter votre serveur RADIUS ISE pour l'authentification FMC

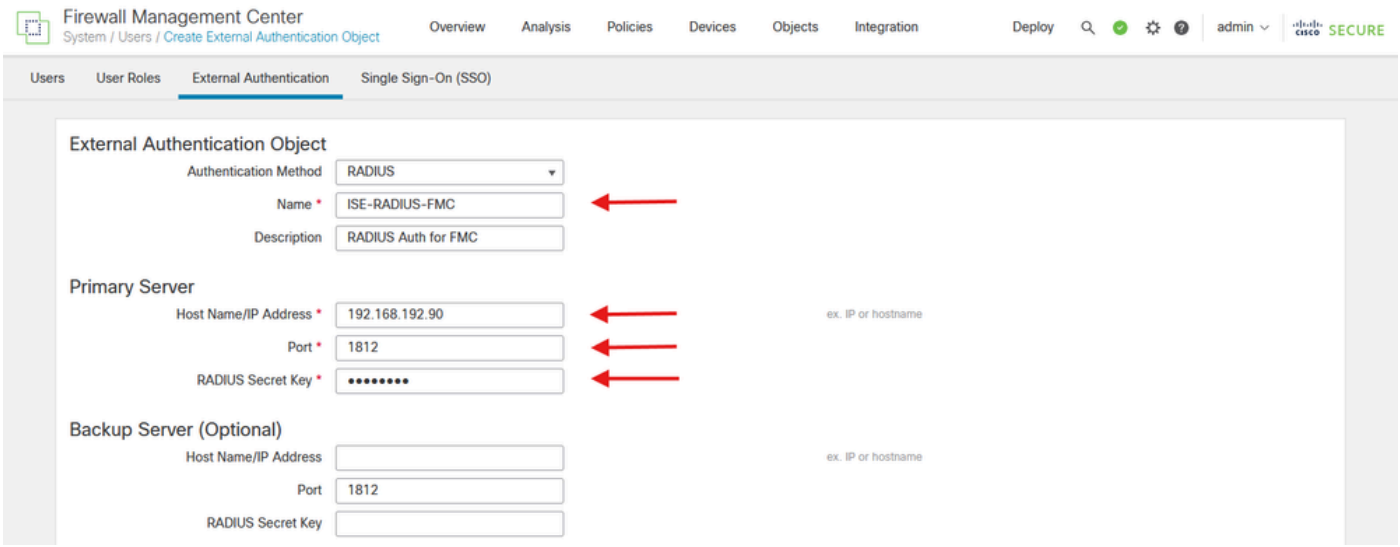
Étape 1. Créez l'objet d'authentification externe sous Système > Utilisateurs > Authentification externe > + Ajouter un objet d'authentification externe.



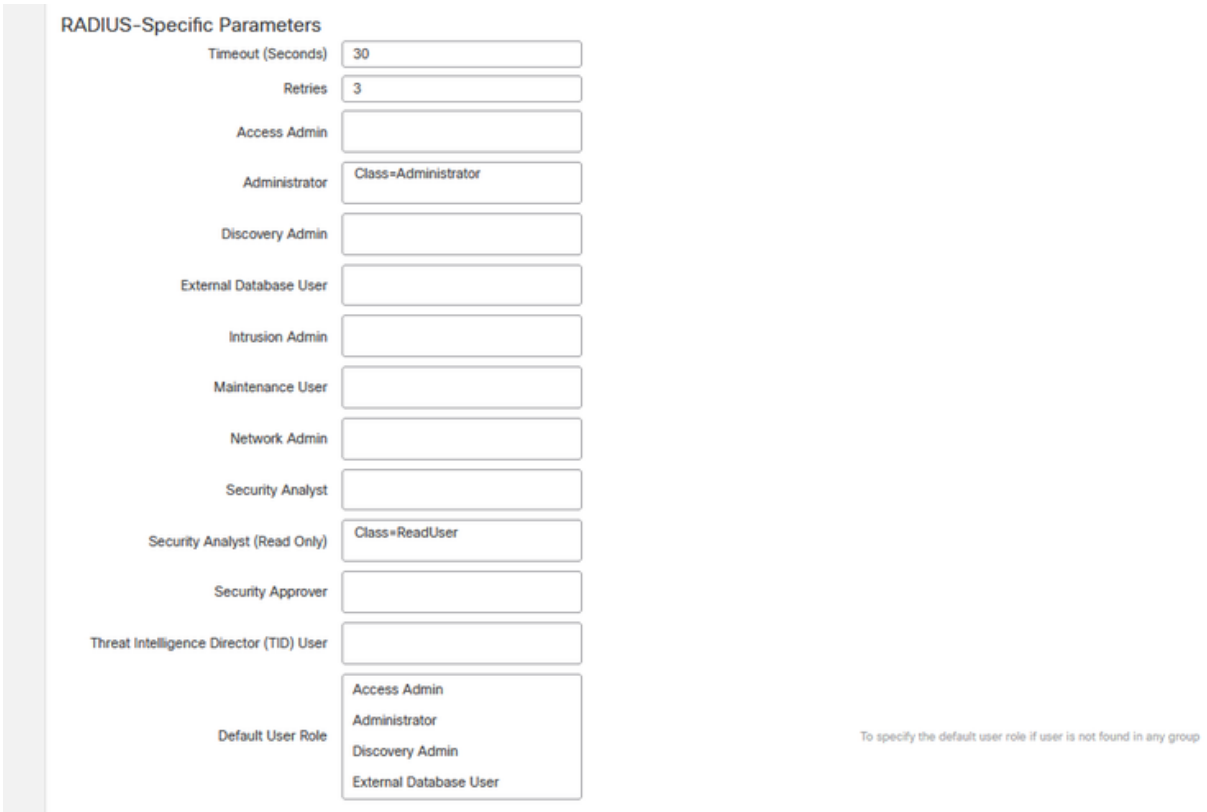
Étape 2 : sélectionnez RADIUS comme méthode d'authentification.

Sous External Authentication Object, attribuez un nom au nouvel objet.

Ensuite, dans le paramètre Primary Server, insérez l'adresse IP ISE et la même clé secrète RADIUS que vous avez utilisée à l'étape 2 de votre configuration ISE.

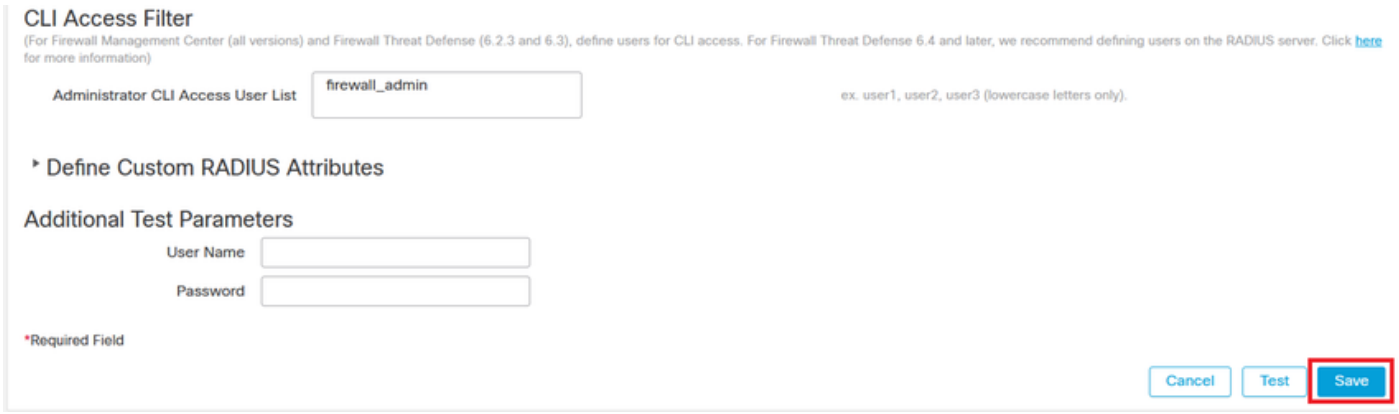


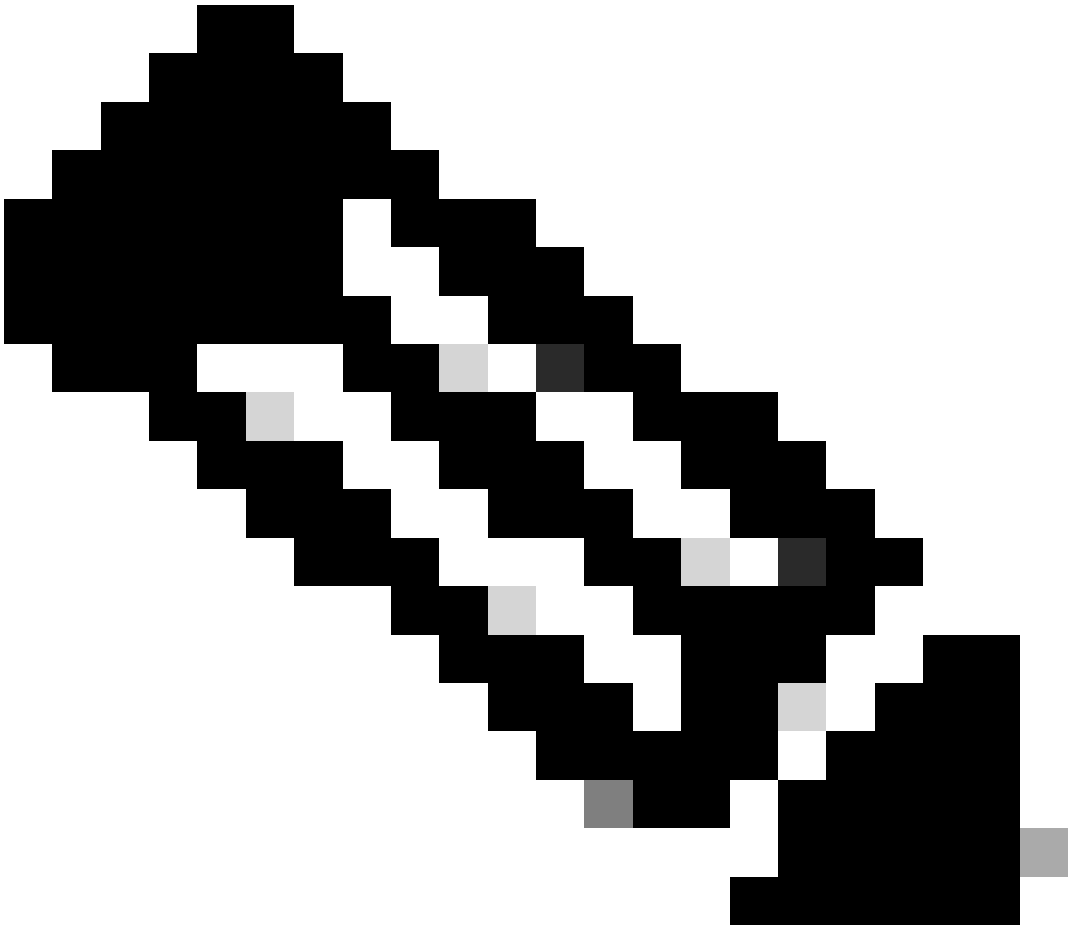
Étape 3. Insérez les valeurs d'attributs de classe RADIUS qui ont été configurées aux étapes 6 et 7 de la configuration ISE : Administrator et ReadUser pour firewall_admin et firewall_readuser respectivement.



Étape 4. Remplissez la liste des utilisateurs d’accès CLI de l’administrateur sous CLI Access Filter avec le nom d’utilisateur qui doit avoir un accès CLI au FMC.

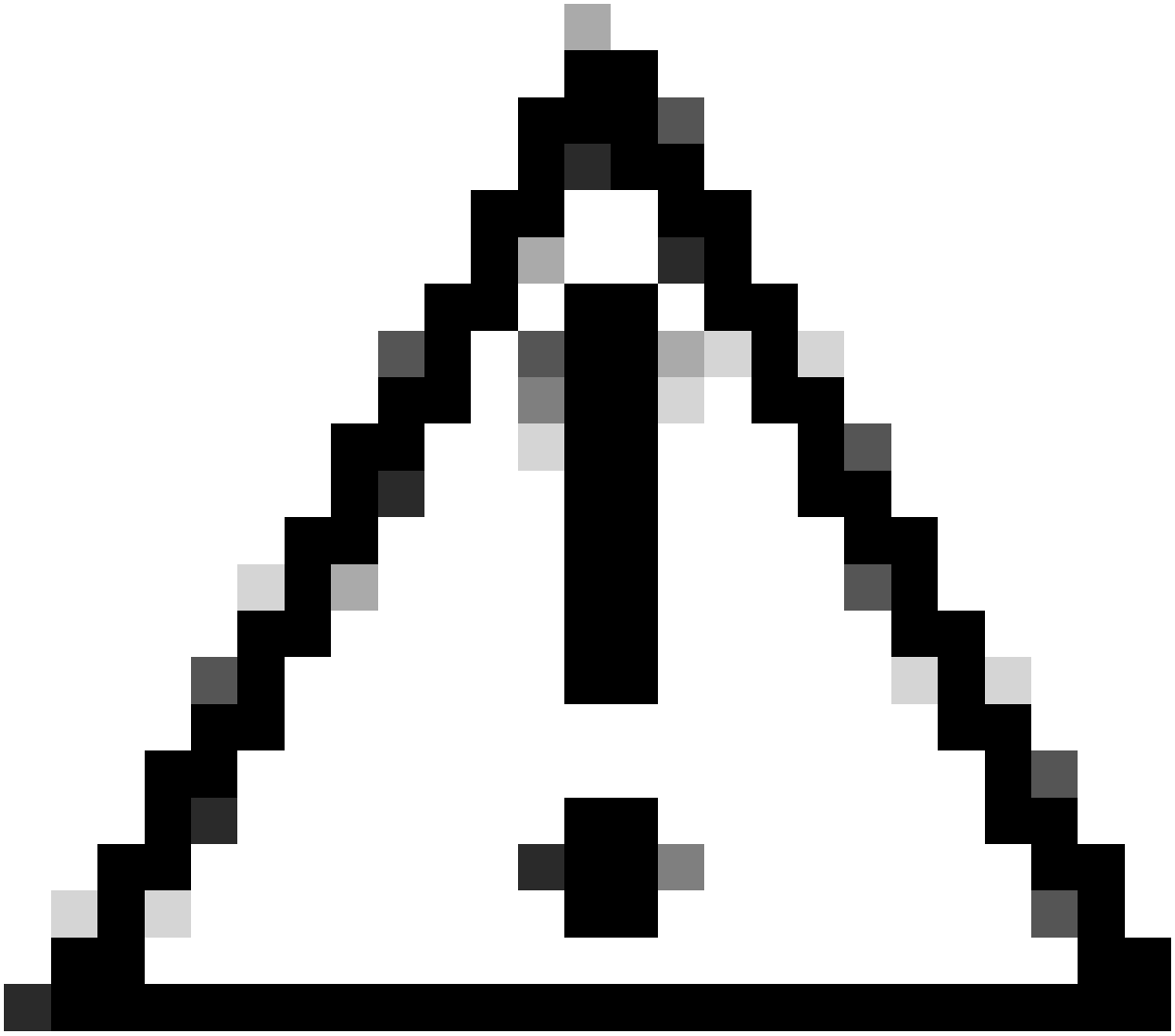
Cliquez sur Save une fois terminé.





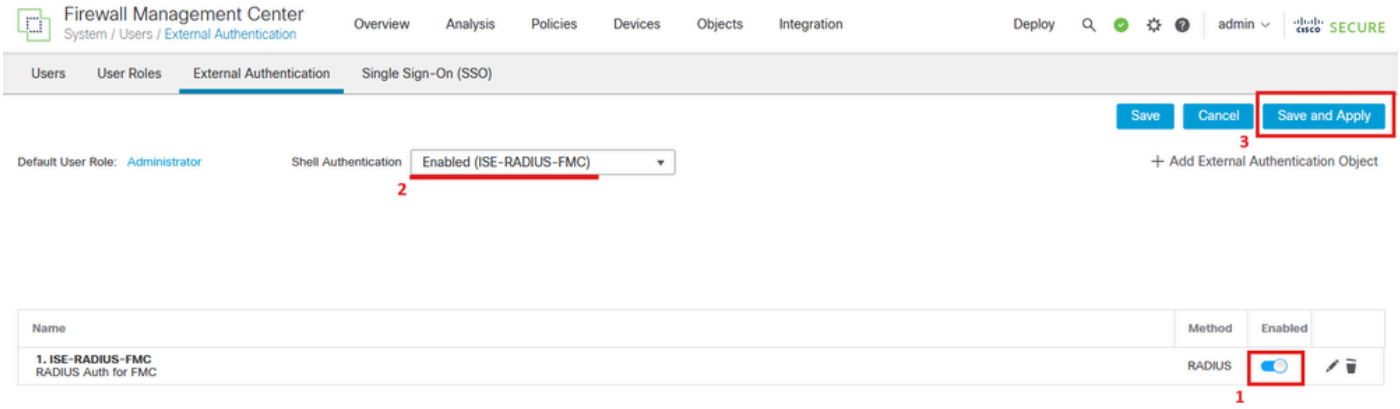
Remarque : Dans cette procédure, nous définissons les utilisateurs sur le serveur RADIUS à l'aide de l'attribut Service-Type pour empêcher les utilisateurs ReadOnly d'obtenir un accès CLI au FTD avec des droits d'expert.

Pour l'accès CLI FMC, vous devez utiliser cette liste d'utilisateurs.



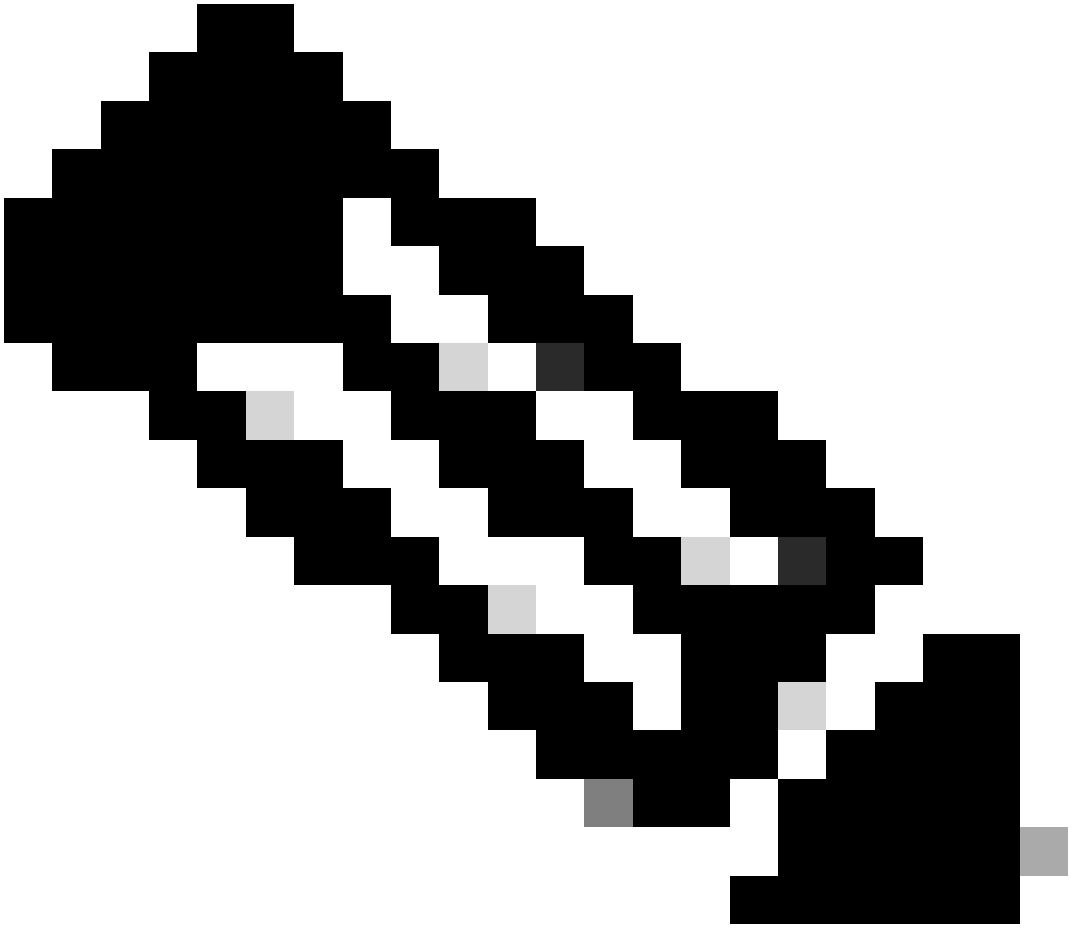
Mise en garde : Tout utilisateur disposant d'un accès CLI au FMC peut obtenir un accès au shell Linux à l'aide de la commande expert. Les utilisateurs du shell Linux peuvent obtenir des privilèges root, ce qui peut présenter un risque pour la sécurité. Veillez à limiter la liste des utilisateurs disposant d'un accès à l'interface de ligne de commande ou au shell Linux.

Étape 5 : activation du nouvel objet Définissez-la comme méthode d'authentification Shell pour FMC et cliquez sur Enregistrer et appliquer.



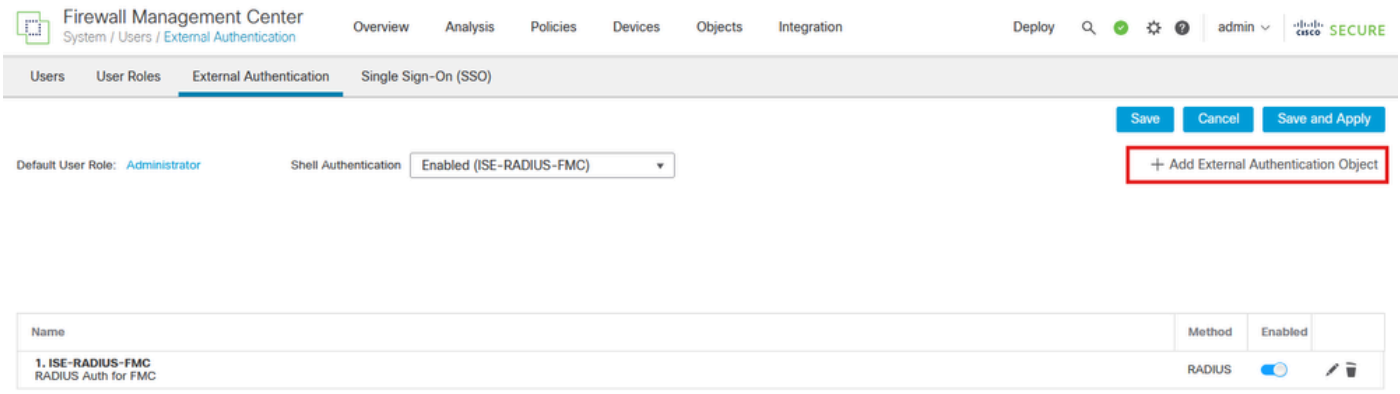
Configuration FTD

Ajouter votre serveur RADIUS ISE pour l'authentification FTD



Remarque : Vous pouvez partager le même objet entre le centre de gestion et les périphériques ou créer des objets distincts selon l'emplacement où vous souhaitez définir vos utilisateurs et le niveau d'autorisation qu'ils doivent posséder. Dans ce scénario, nous définissons nos utilisateurs sur le serveur RADIUS. Nous devons donc créer des objets distincts pour la défense contre les menaces et le centre de gestion.

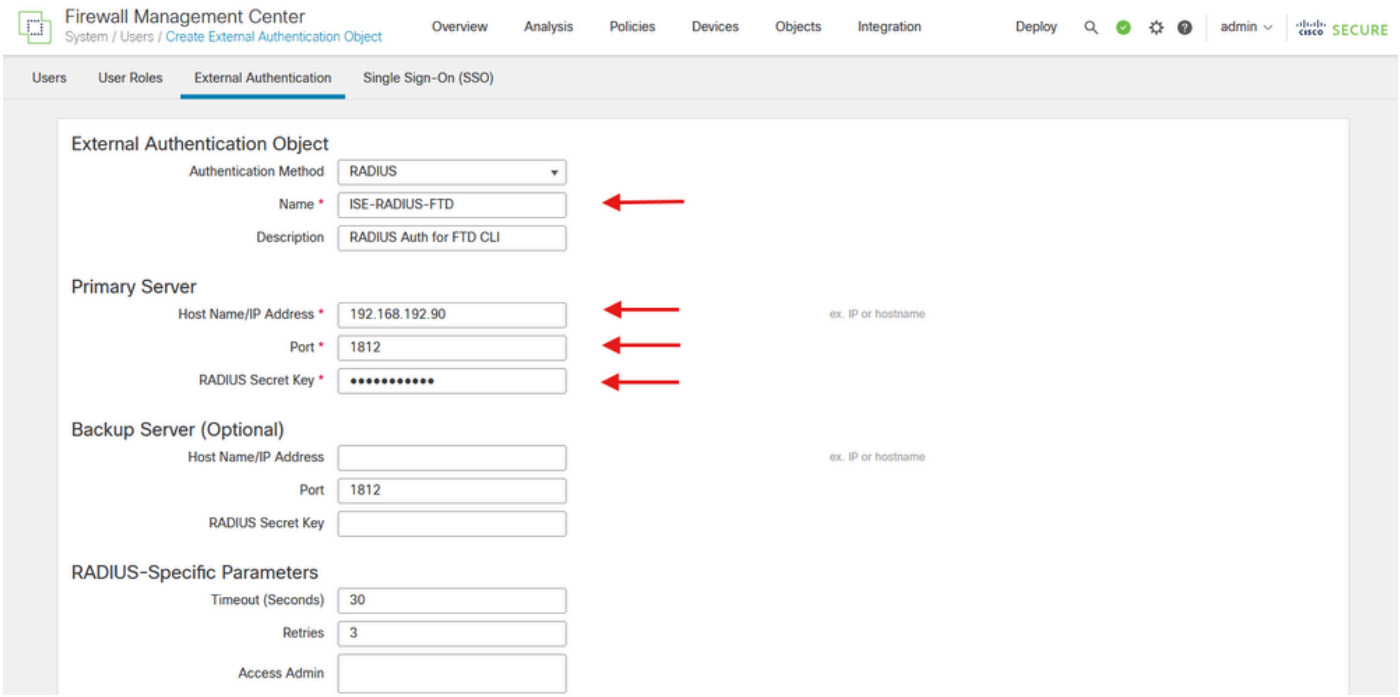
Étape 1 : comme pour FMC, créez l'objet d'authentification externe sous Système > Utilisateurs > Authentification externe > + Ajouter un objet d'authentification externe.

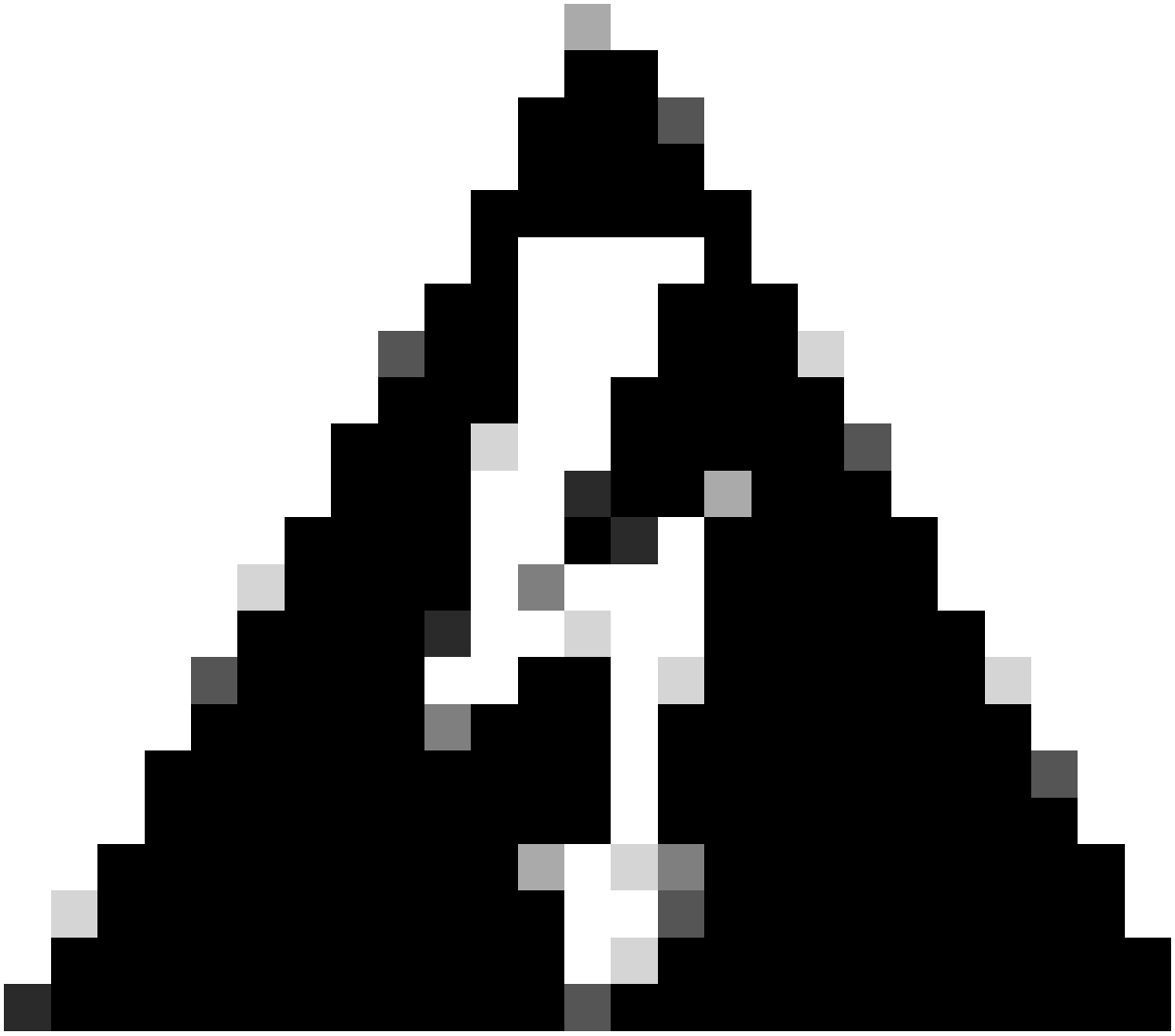


Étape 2 : sélectionnez RADIUS comme méthode d'authentification.

Sous External Authentication Object, attribuez un nom au nouvel objet.

Ensuite, dans le paramètre Primary Server, insérez l'adresse IP ISE et la même clé secrète RADIUS que vous avez utilisée à l'étape 2.1 de votre configuration ISE. Cliquez sur Save (enregistrer)

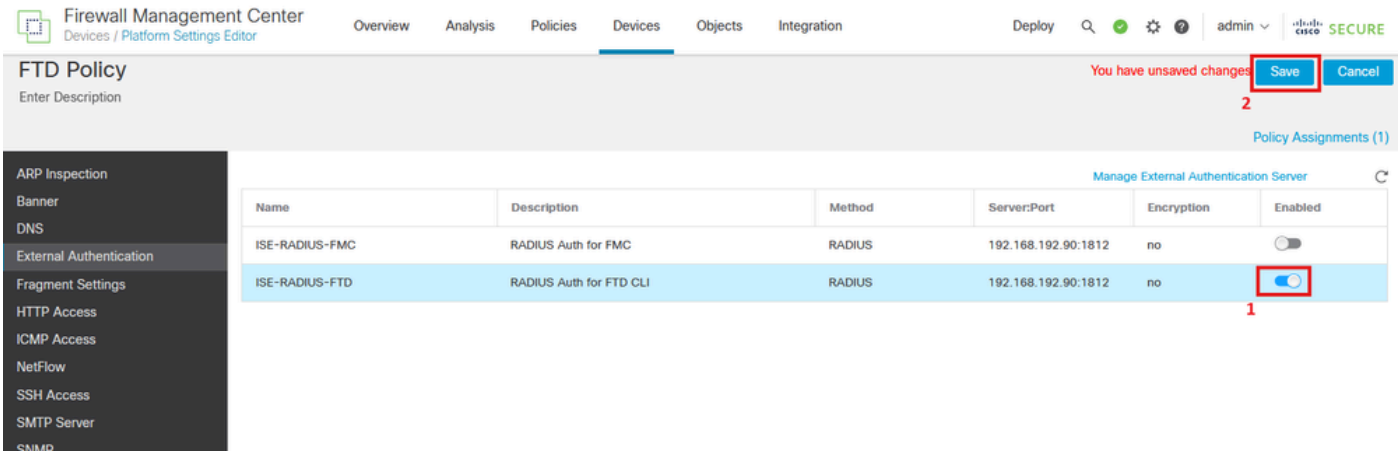




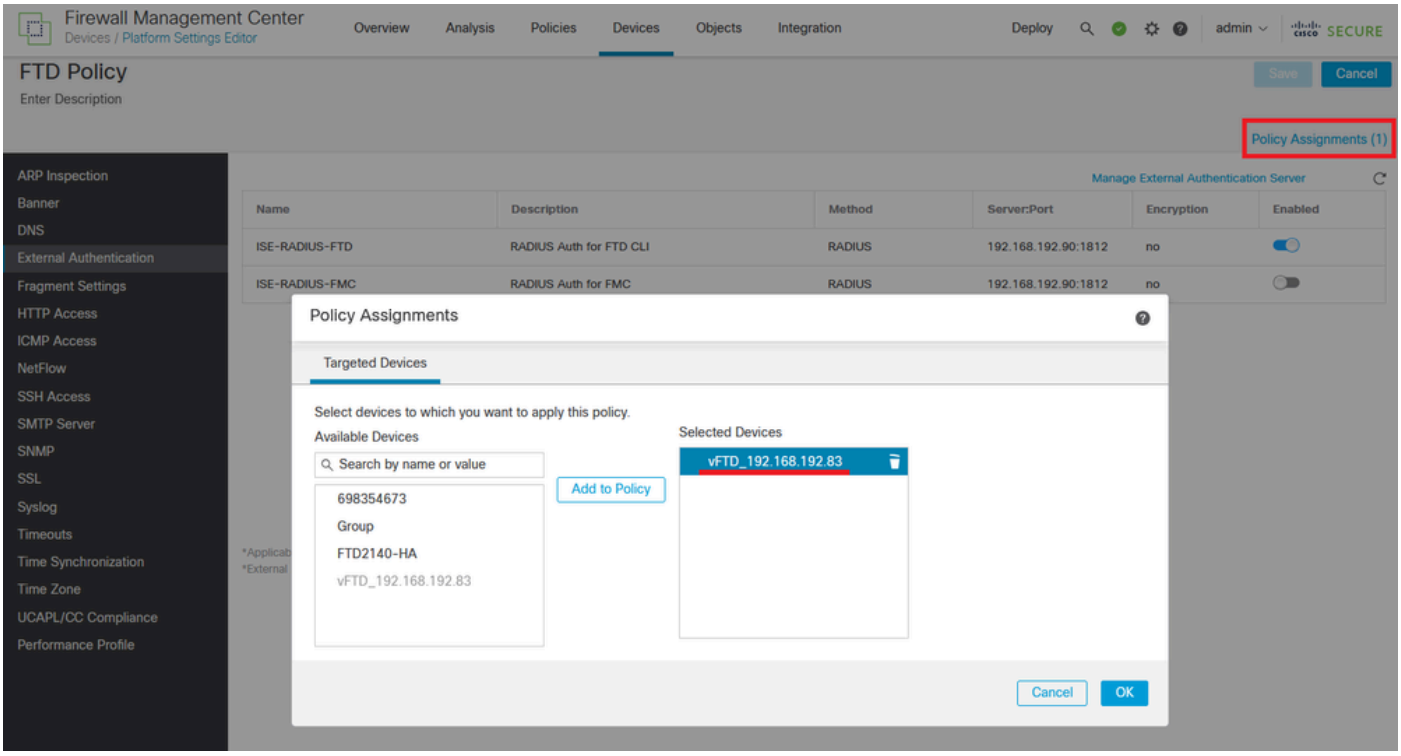
Avertissement : La plage de temporisation est différente pour le FTD et le FMC. Par conséquent, si vous partagez un objet et modifiez la valeur par défaut de 30 secondes, veillez à ne pas dépasser une plage de temporisation plus petite (1 à 300 secondes) pour les périphériques FTD. Si vous définissez le délai d'attente sur une valeur supérieure, la configuration RADIUS de défense contre les menaces ne fonctionne pas.

Activer le serveur RADIUS

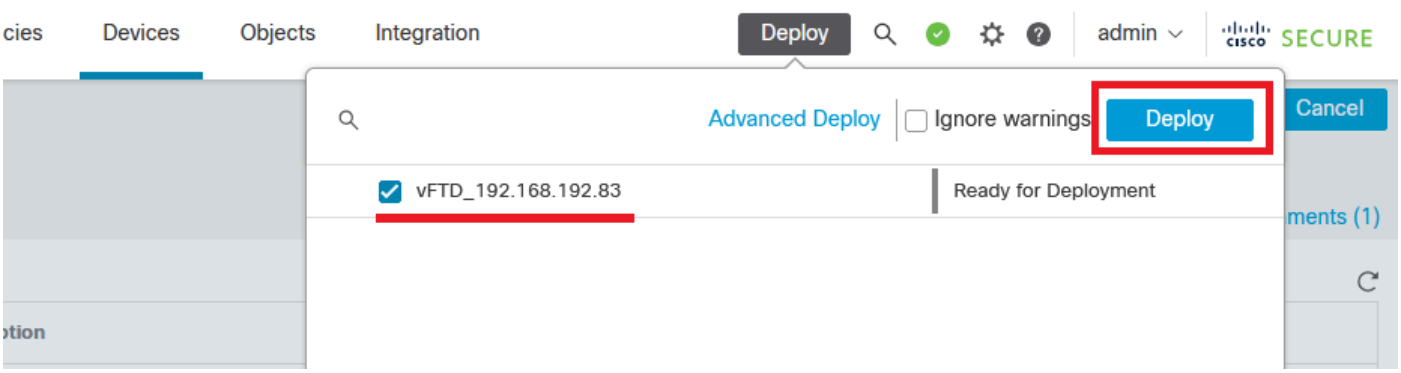
Étape 1. Dans l’interface utilisateur graphique de FMC, accédez à Périphériques > Paramètres de plate-forme. Modifiez votre stratégie actuelle ou créez-en une nouvelle si aucune n'est affectée au FTD auquel vous avez besoin d'accéder. Activez le serveur RADIUS sous External Authentication et cliquez sur Save.

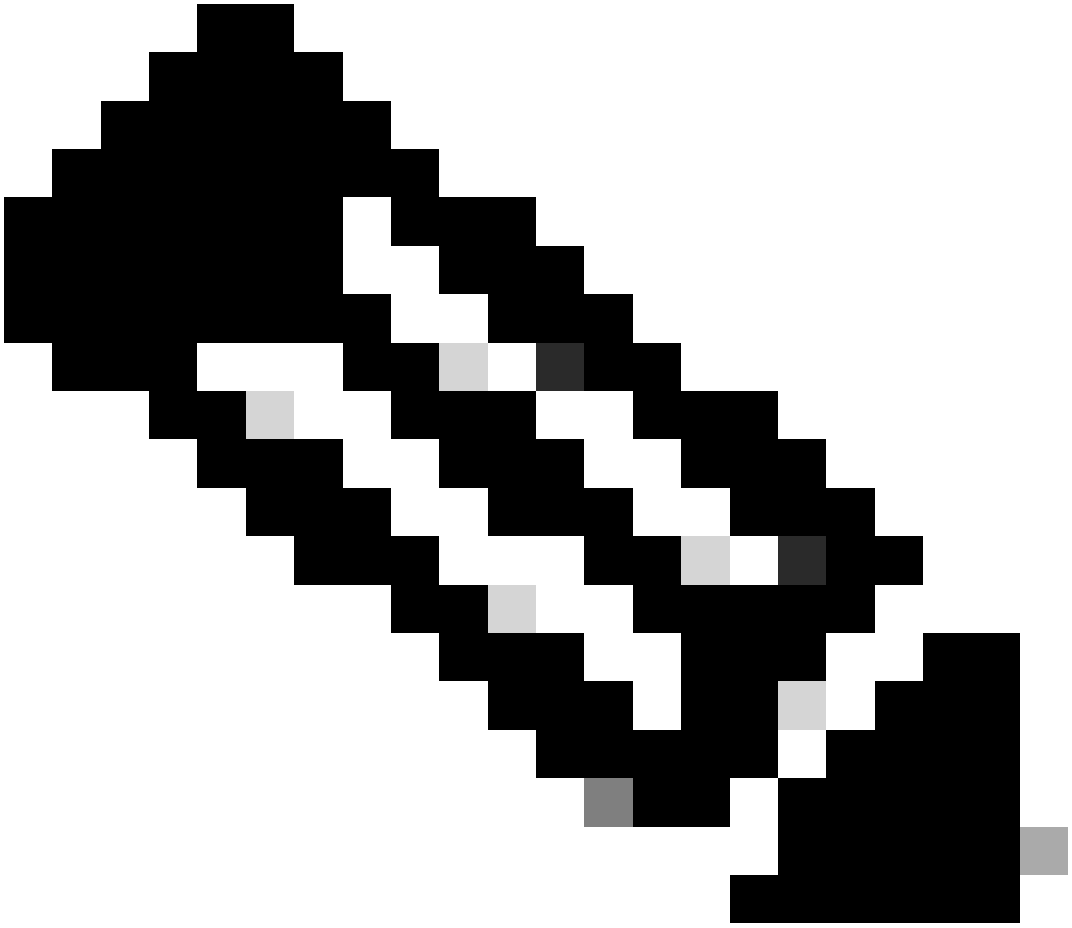


Étape 2. Assurez-vous que le FTD auquel vous devez accéder figure sous Affectations de politiques en tant que périphérique sélectionné.



Étape 3 : déploiement des modifications

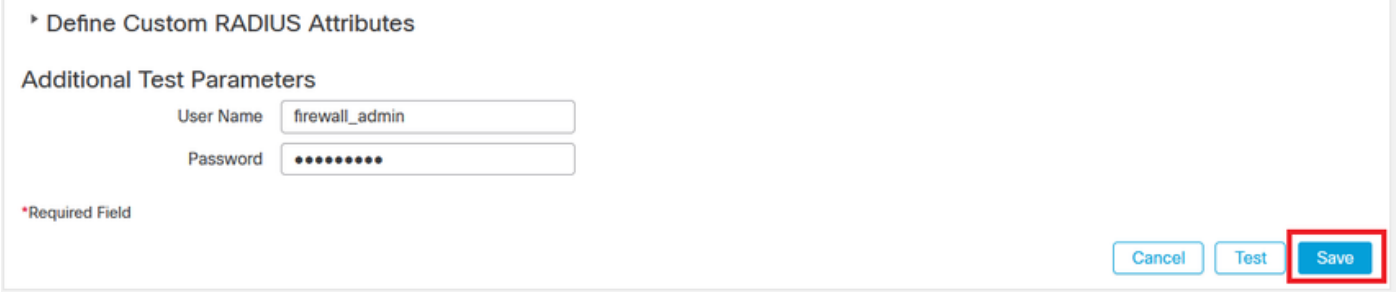




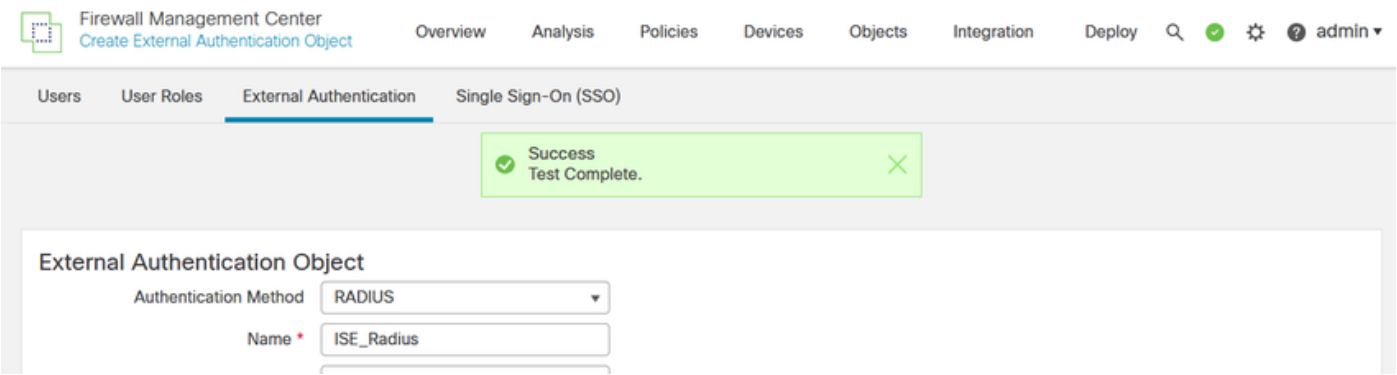
Remarque : Si vous avez précédemment configuré un nom d'utilisateur externe existant en tant qu'utilisateur interne à l'aide de la commande configure user add, la défense contre les menaces vérifie d'abord le mot de passe par rapport à l'utilisateur interne, et si cela échoue, elle vérifie le serveur RADIUS. Notez que vous ne pourrez pas ajouter ultérieurement un utilisateur interne portant le même nom qu'un utilisateur externe car le déploiement échouera ; seuls les utilisateurs internes préexistants sont pris en charge.

Vérifier

- Testez le bon fonctionnement de votre nouveau déploiement.
- Dans l'interface utilisateur graphique de FMC, accédez aux paramètres du serveur RADIUS et faites défiler la page jusqu'à la section Additional Test Parameters.
- Entrez un nom d'utilisateur et un mot de passe pour l'utilisateur ISE et cliquez sur Test.

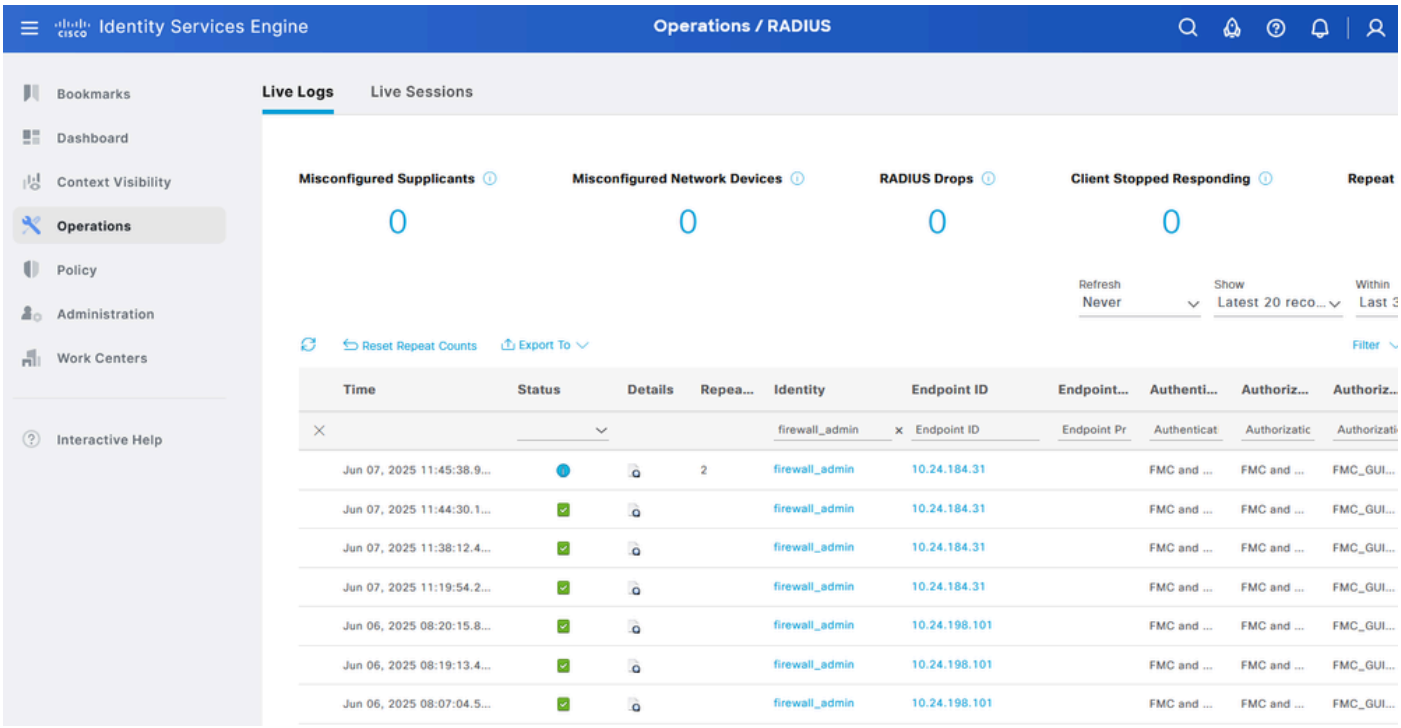


- Un test réussi affiche un message vert Success Test Complete (Test réussi terminé) en haut de la fenêtre du navigateur.



- Pour plus d'informations, développez Détails sous Sortie de test.

- Vérifiez la demande et la réponse d'authentification dans votre ISE RADIUS sous Operations > RADIUS > Live Logs.


Identity Services Engine
Operations / RADIUS
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Repeat
Refresh
Never
Show
Latest 20 reco...
Within
Last 3
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authenti...
Authoriz...
Authoriz...
firewall_admin
Endpoint ID
Endpoint Pr
Authenticat
Authorizatic
Jun 07, 2025 11:45:38.9... 2 firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 07, 2025 11:44:30.1... firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 07, 2025 11:38:12.4... firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 07, 2025 11:19:54.2... firewall_admin 10.24.184.31 FMC and ... FMC and ... FMC_GUI...
Jun 06, 2025 08:20:15.8... firewall_admin 10.24.198.101 FMC and ... FMC and ... FMC_GUI...
Jun 06, 2025 08:19:13.4... firewall_admin 10.24.198.101 FMC and ... FMC and ... FMC_GUI...
Jun 06, 2025 08:07:04.5... firewall_admin 10.24.198.101 FMC and ... FMC and ... FMC_GUI...

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.