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

Table des matières

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 7.2.5
- vFTD 7.2.5.

- ISE 3.2.

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.

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.

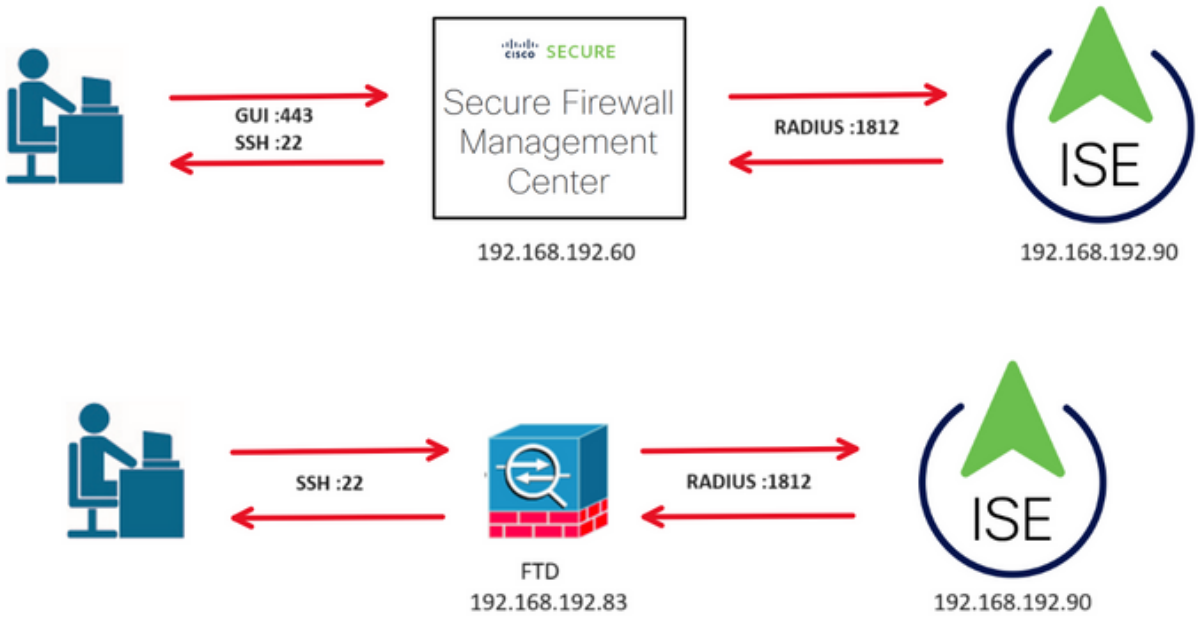
Authentification externe pour FMC

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

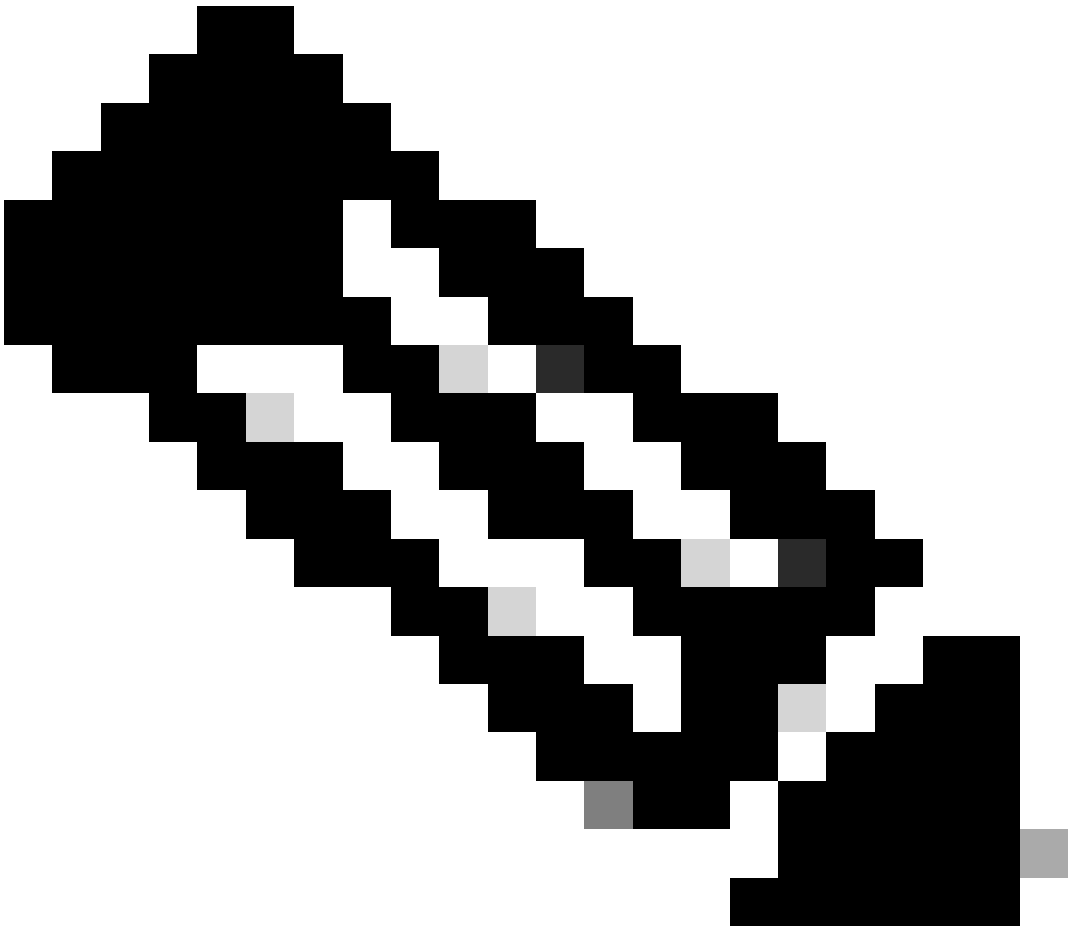
Pour le FTD, vous ne pouvez activer qu'un seul objet d'authentification externe.

Topologie du réseau



Configurer

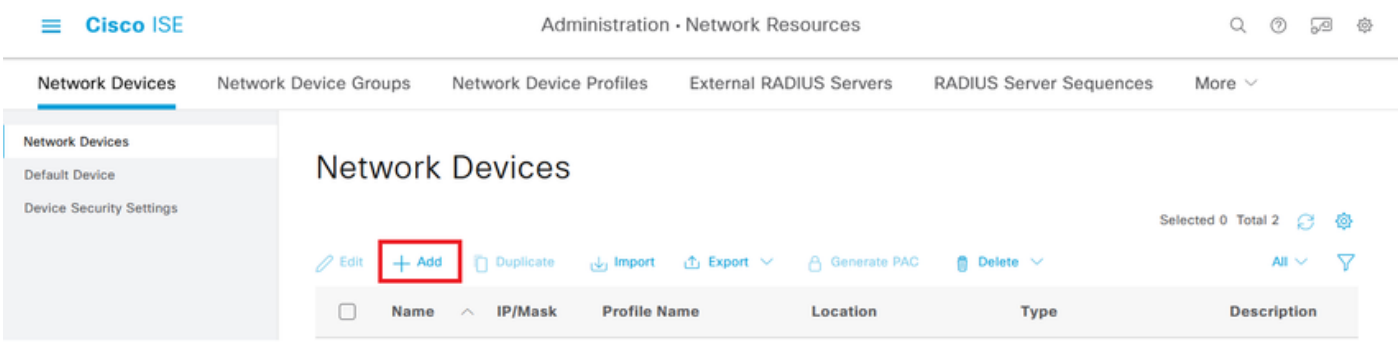
Configuration ISE



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.

Étape 1. Ajoutez un nouveau périphérique réseau. Accédez à l'icône Burger située dans l'angle supérieur gauche >Administration > Network Resources > Network Devices >

+Add.

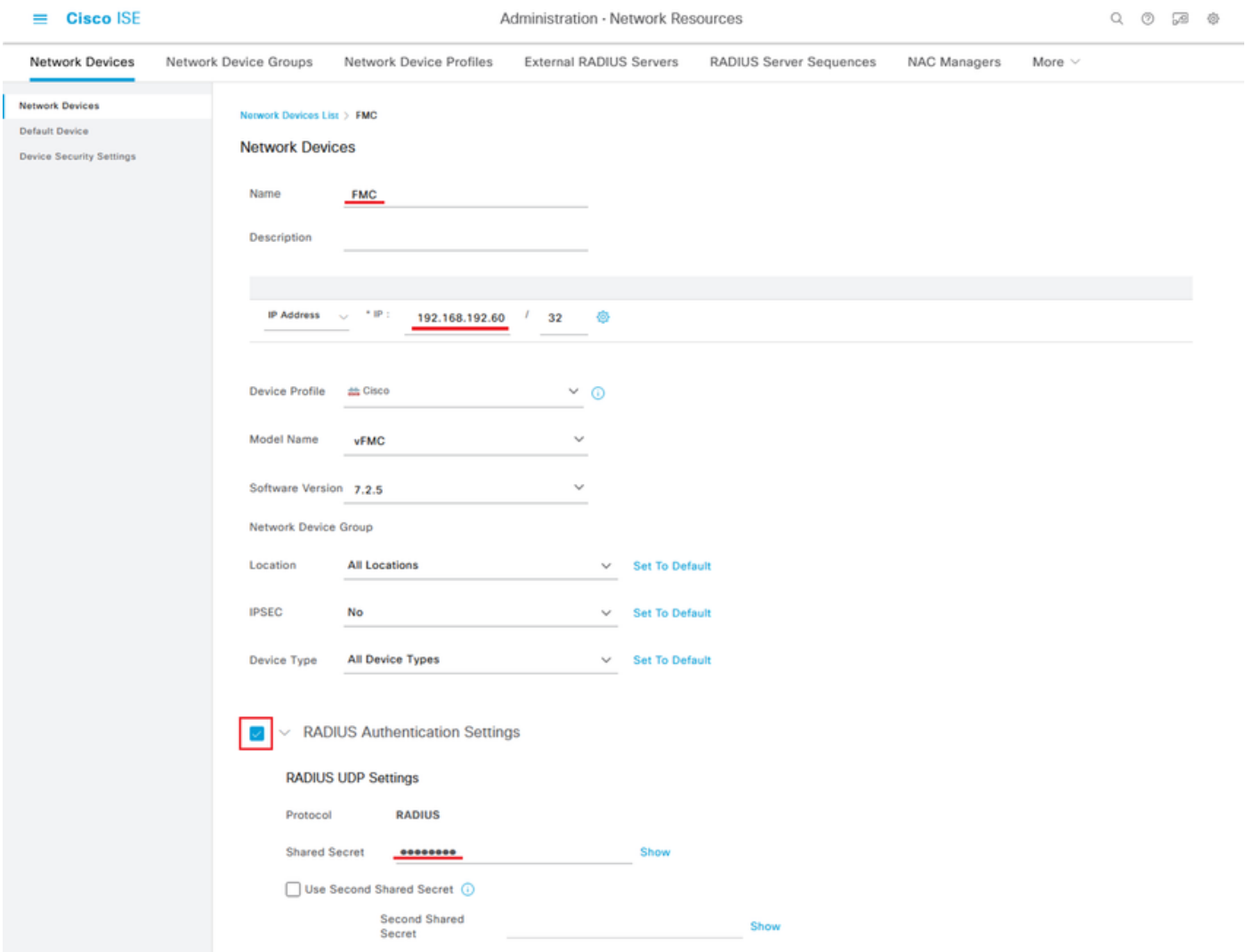


Étape 2. Attribuez un nom à l'objet périphérique réseau et insérez l'adresse IP FMC.

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.

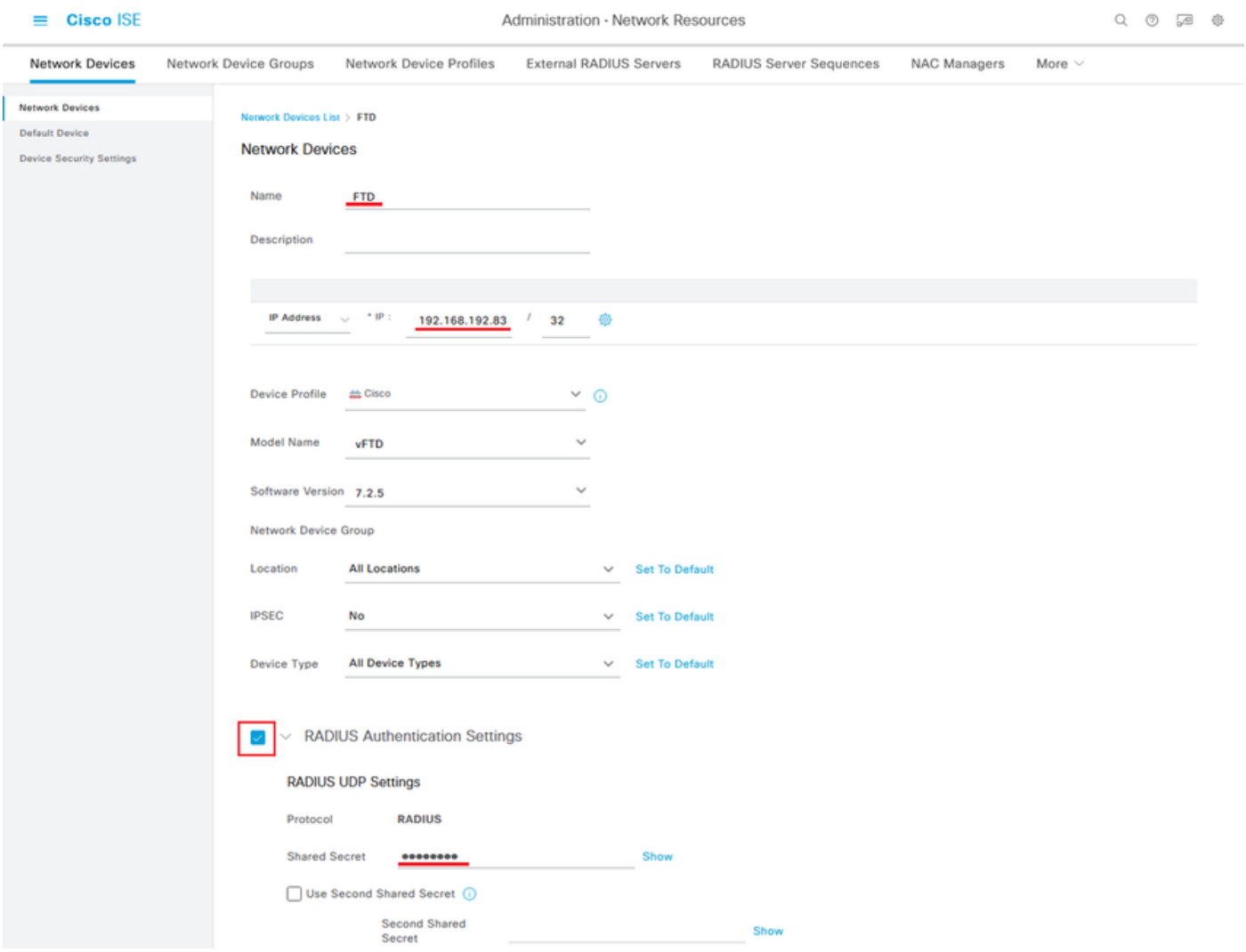


Étape 2.1. Répétez la même procédure pour ajouter le FTD.

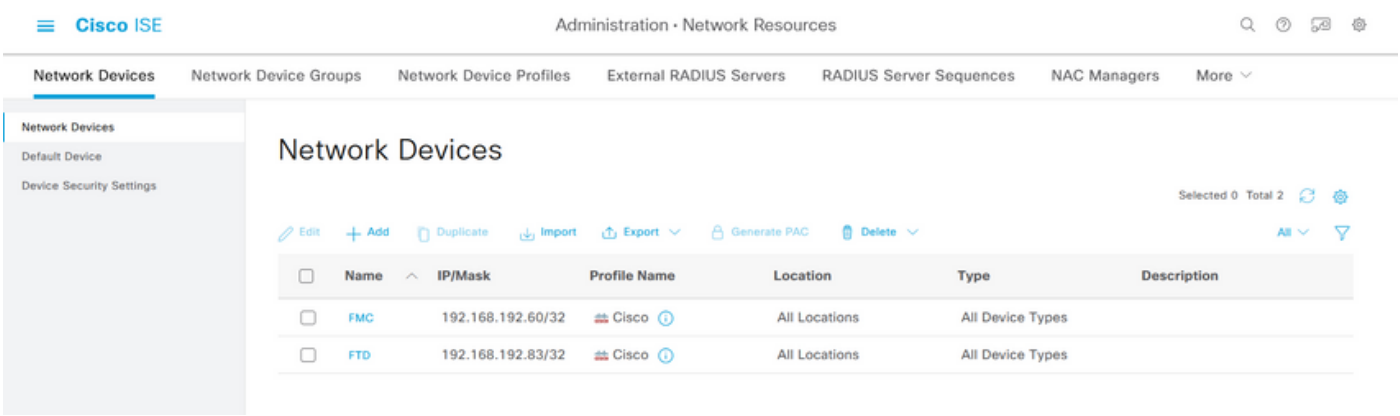
Attribuez un nom à l'objet périphérique réseau et insérez l'adresse IP FTD.

Cochez la case RADIUS et définissez un secret partagé.

Une fois terminé, cliquez sur Enregistrer.

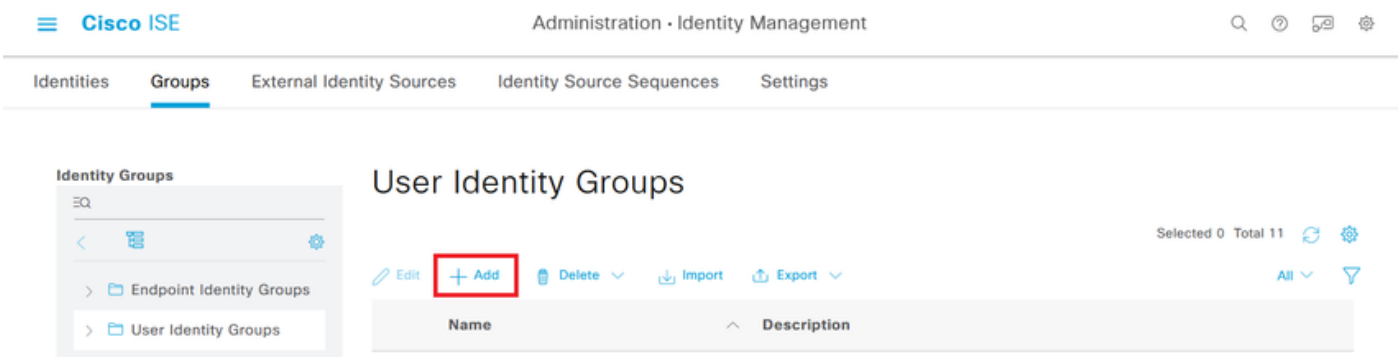


Étape 2.3. Vérifiez que les deux périphériques sont répertoriés sous Network Devices.

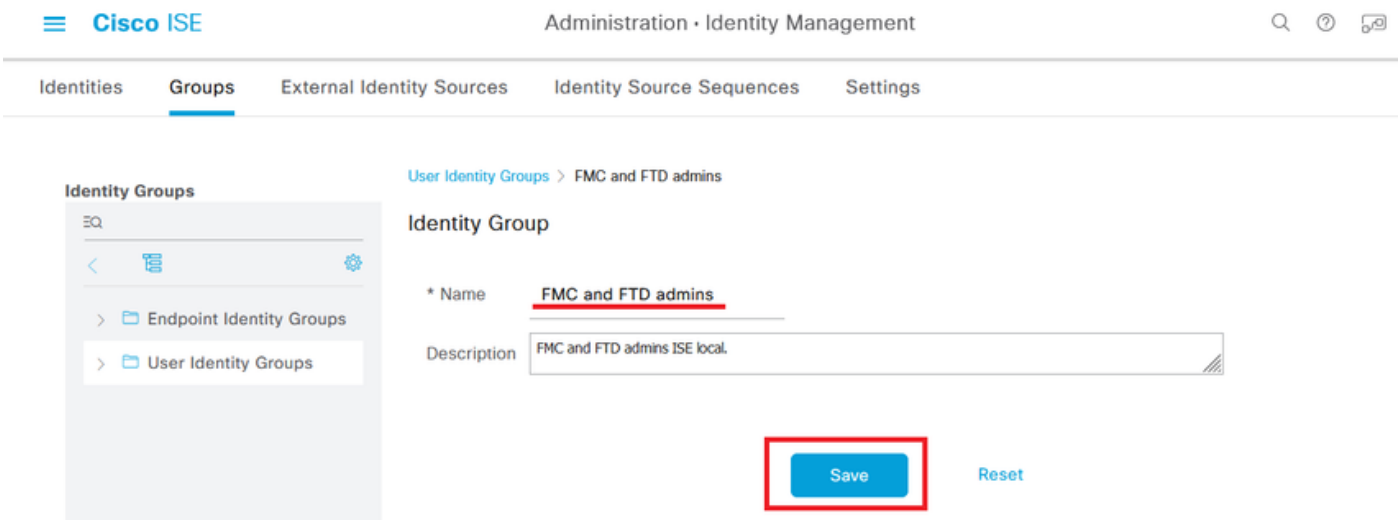


Étape 3. Créez les groupes d'identités utilisateur requis. Accédez à l'icône du hamburger

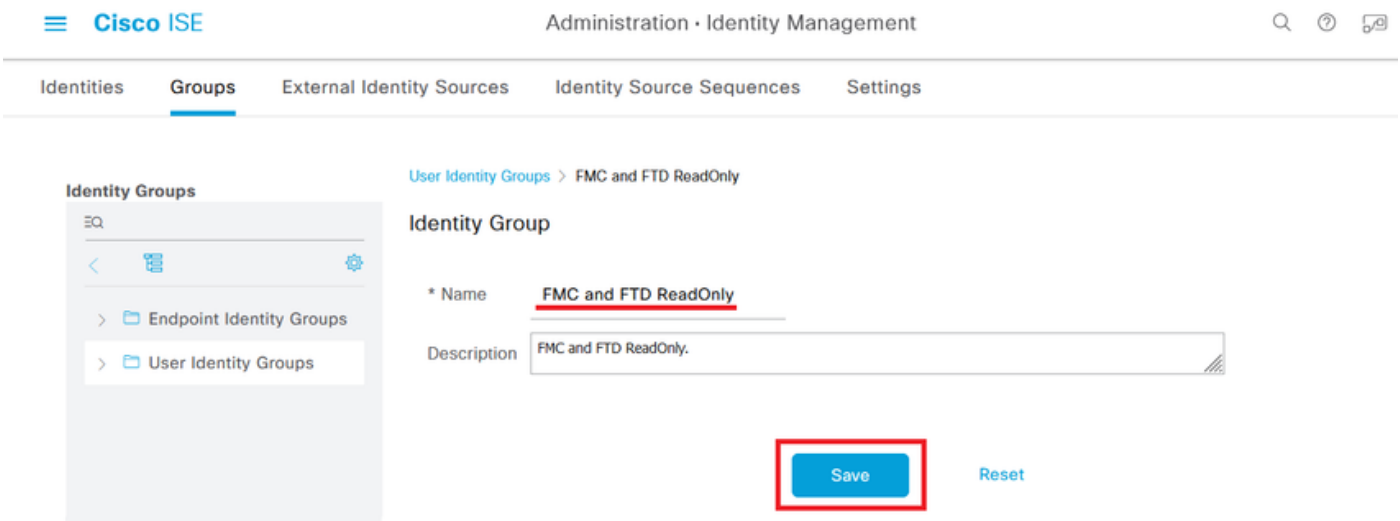
située dans l'angle supérieur gauche > Administration > Identity Management > Groups > User Identity Groups > + Add



Étape 4. Attribuez un nom à chaque groupe et cliquez sur Enregistrer 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.

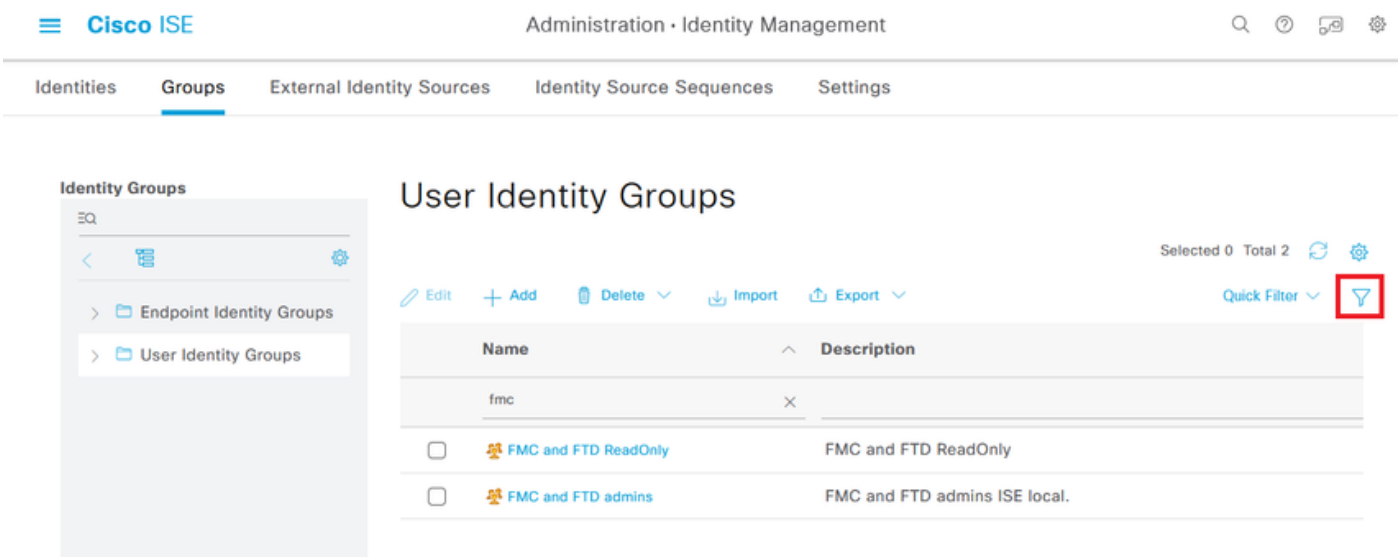


Étape 4.1. Créez le deuxième groupe pour l'utilisateur ReadOnly.



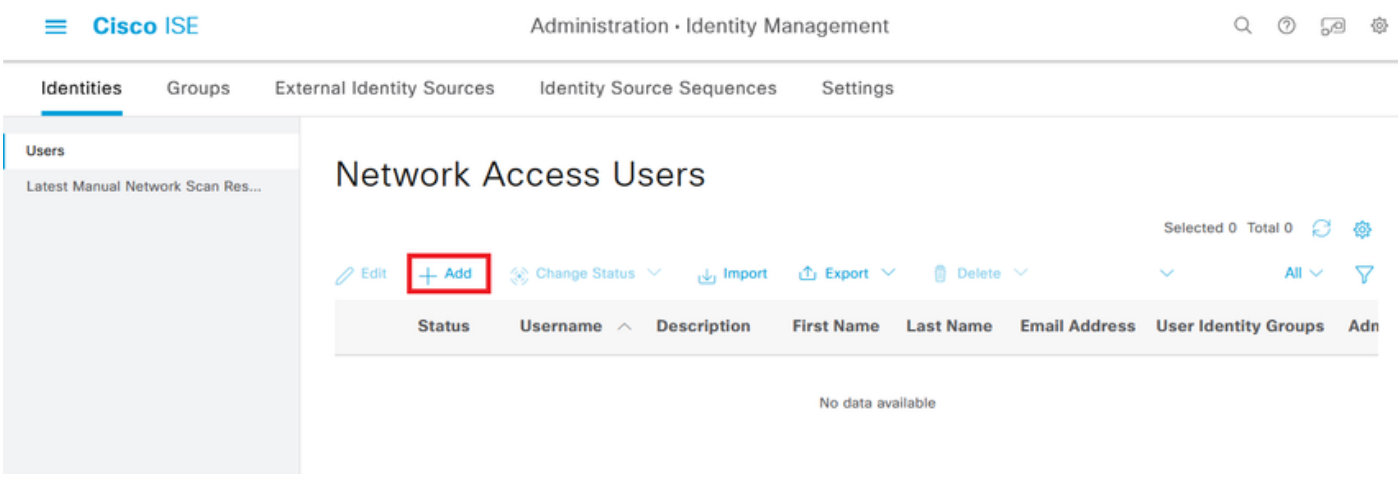
Étape 4.2. Validez que les deux groupes sont affichés dans la liste des groupes d'identité

utilisateur. Utilisez le filtre pour les trouver facilement.

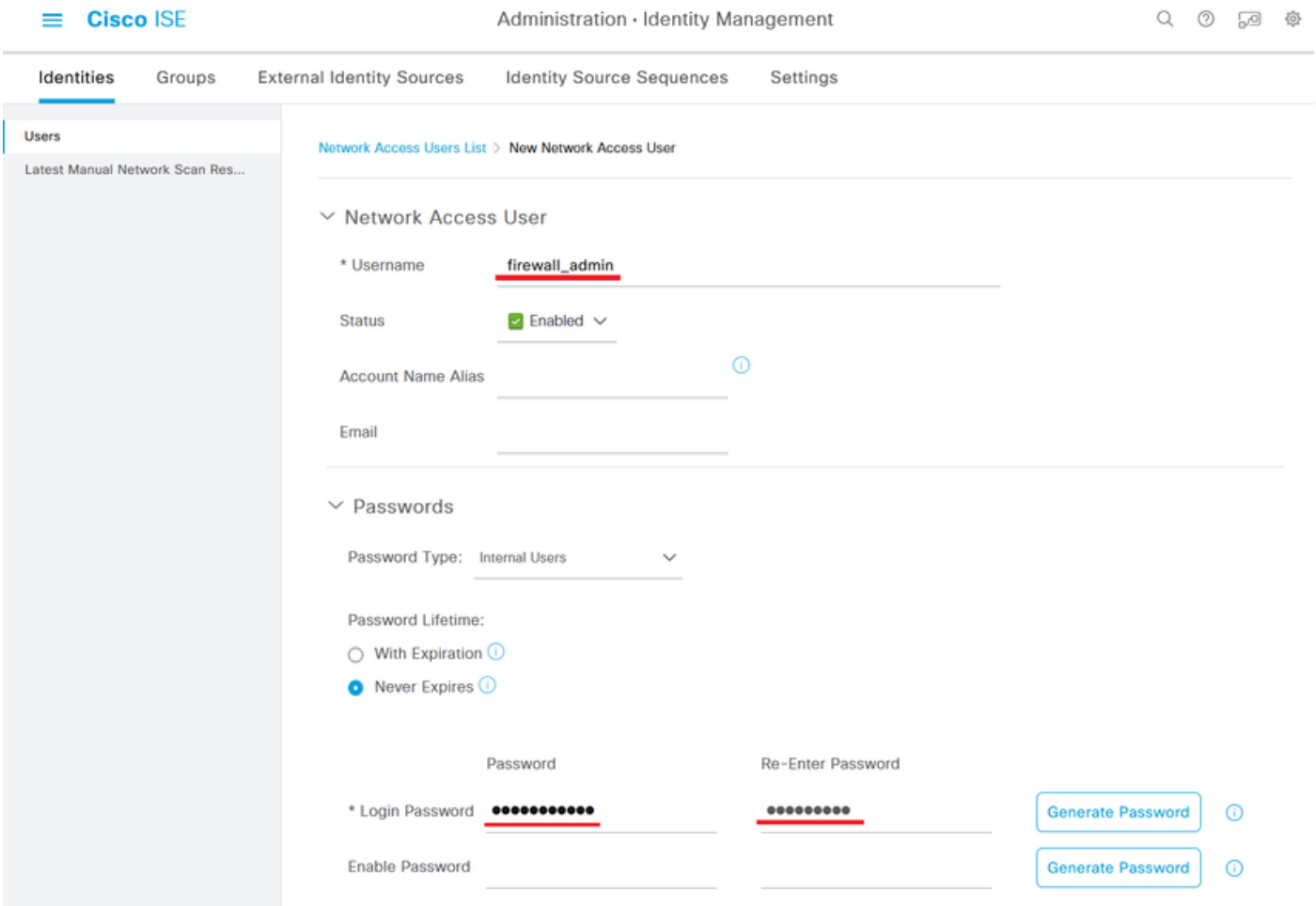


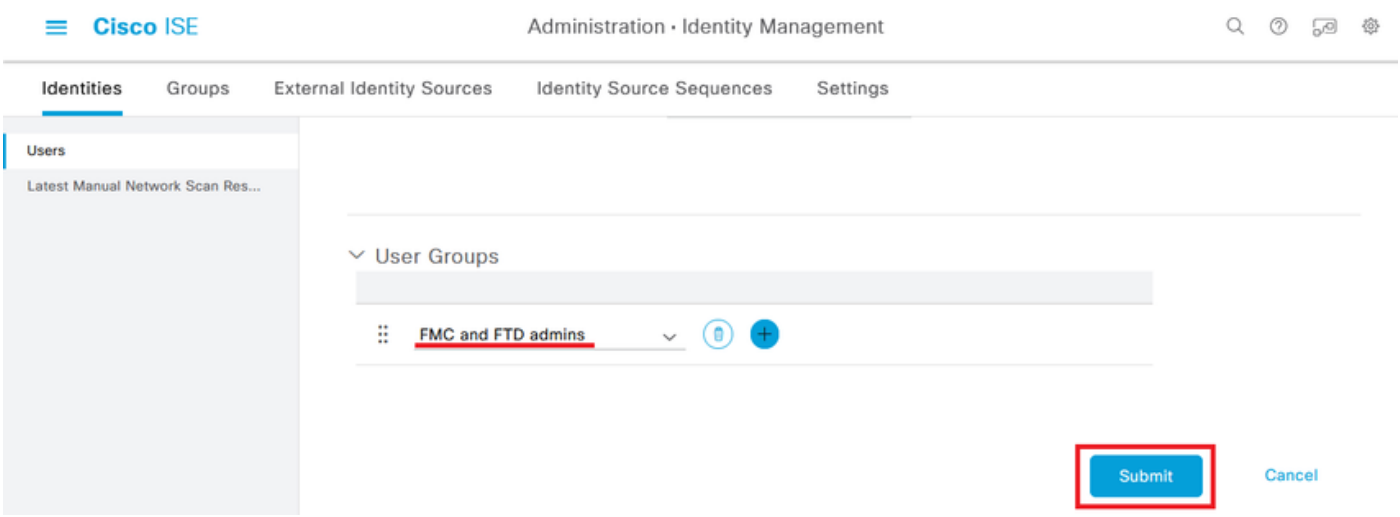
Étape 5. Créez les utilisateurs locaux et ajoutez-les à leur groupe correspondant. Naviguez

jusqu'à
> Administration > Identity Management > Identities > + Add.

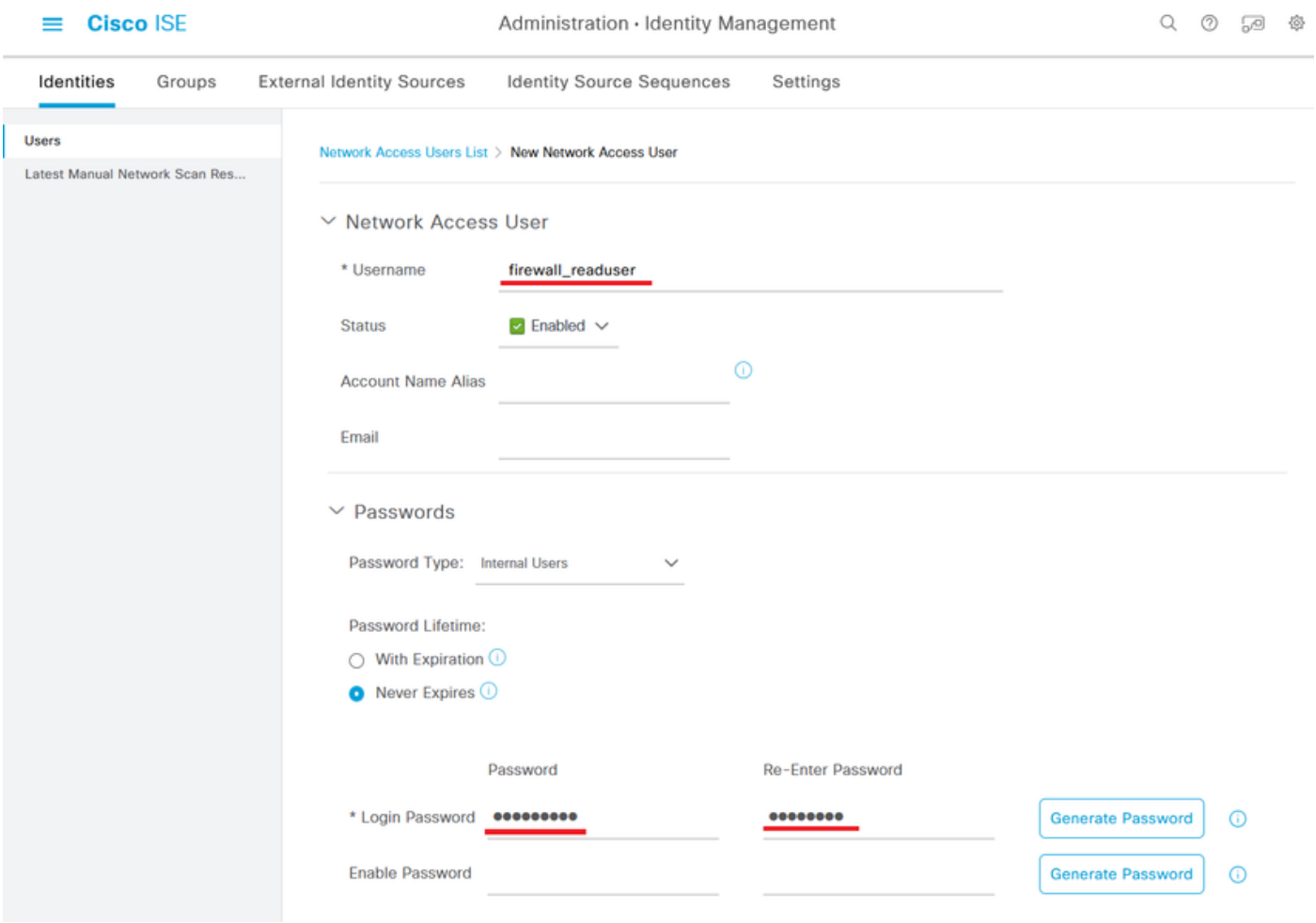


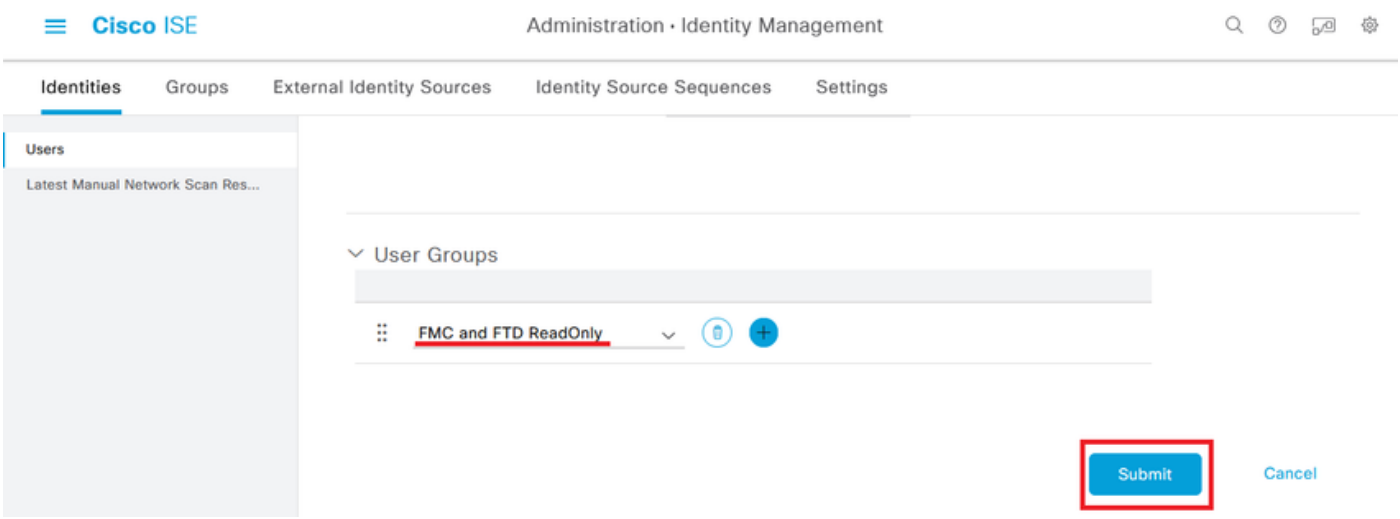
Étape 5.1. Commencez par créer l'utilisateur avec des droits d'administrateur. Attribuez-lui un nom, un mot de passe et le groupe FMC et FTD admins.





Étape 5.2. Ajoutez l'utilisateur avec des droits en lecture seule. Attribuez un nom, un mot de passe et le groupe FMC et FTD ReadOnly.

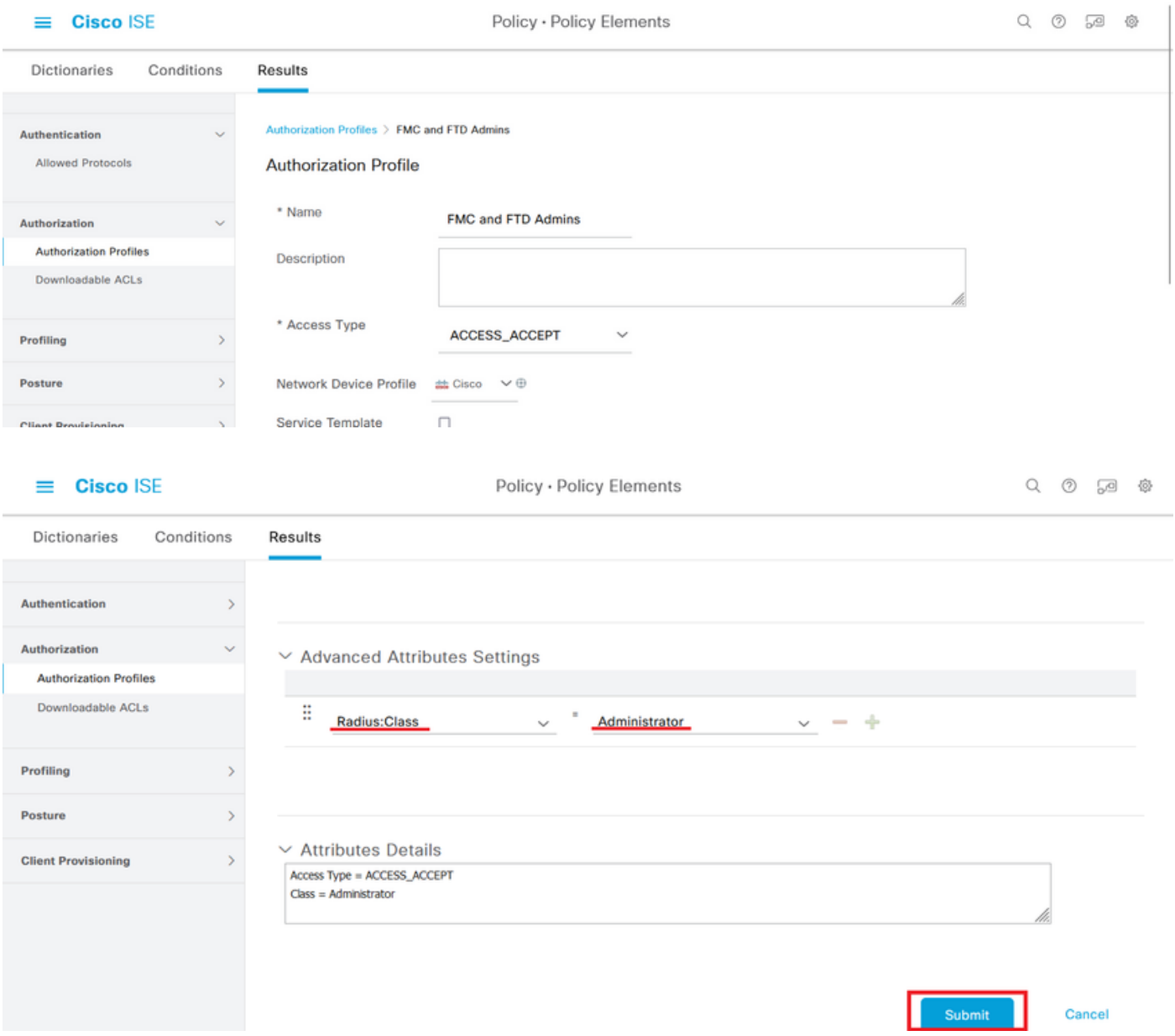




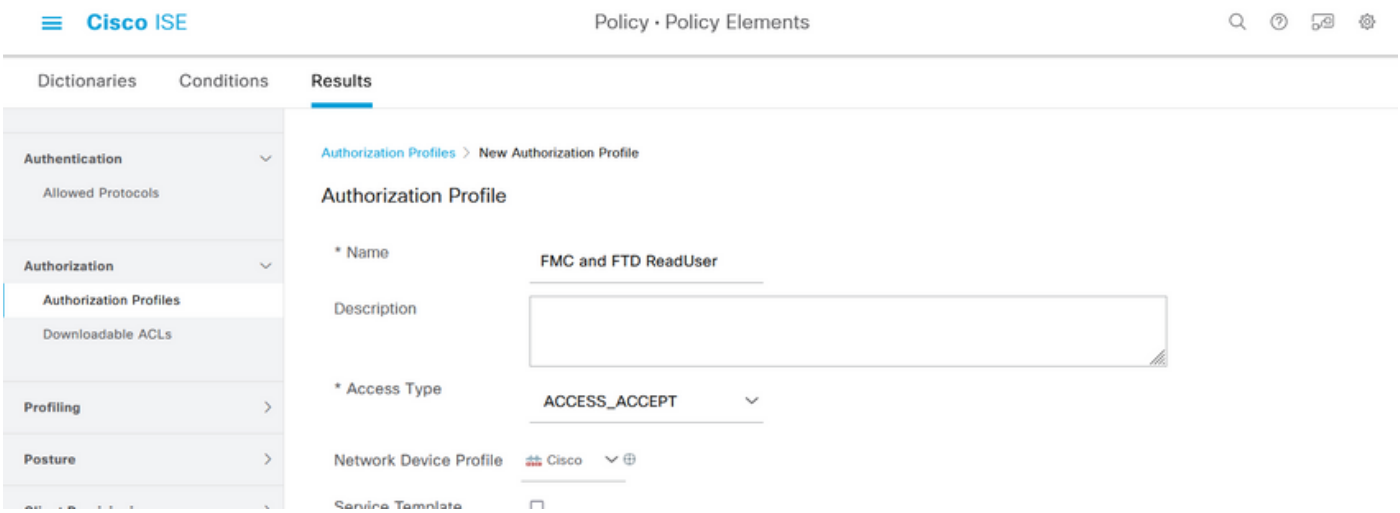
Étape 6. Créez le profil d'autorisation pour l'utilisateur Admin.

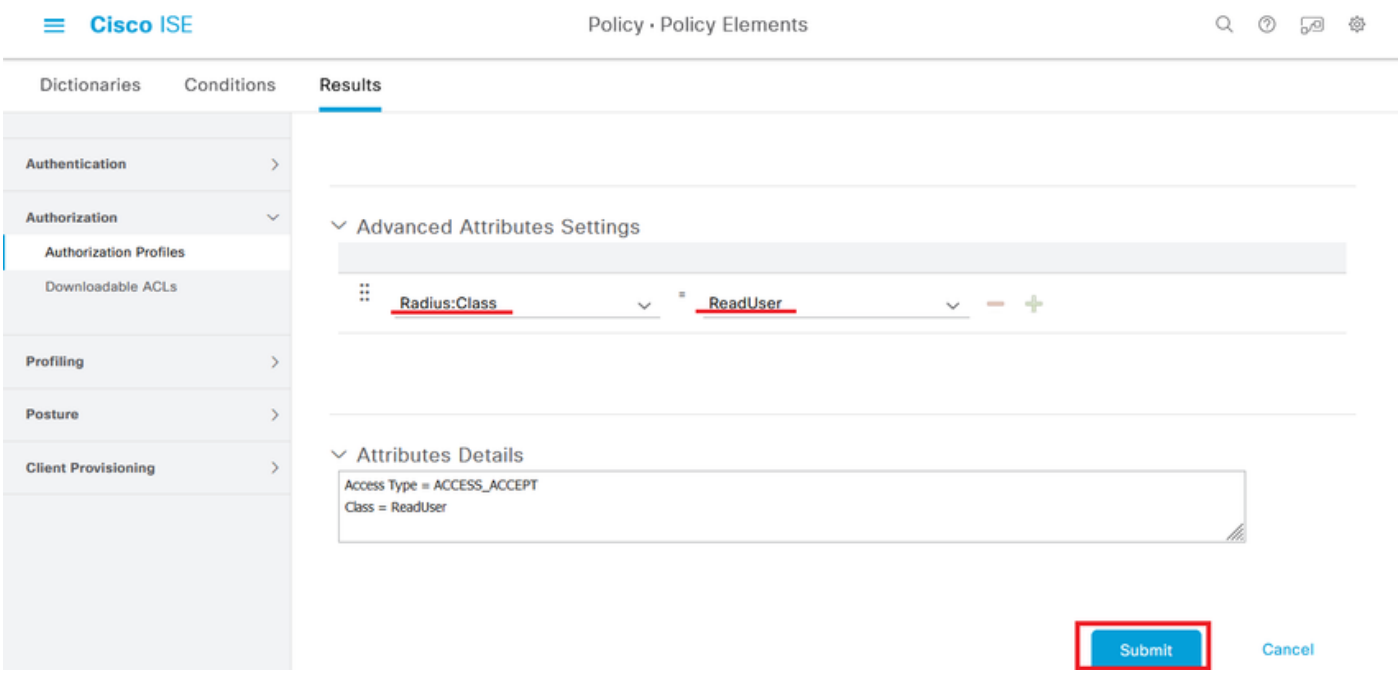
Accédez à
> Règle > Éléments de règle > Résultats > Autorisation > Profils d'autorisation > +Ajouter.

Définissez un nom pour le profil d'autorisation, laissez le type d'accès comme ACCESS_ACCEPT et sous Paramètres d'attributs avancés ajoutez un Rayon > Classe—[25] avec la valeur Administrateur et cliquez sur Envoyer.



Étape 7. Répétez l'étape précédente pour créer le profil d'autorisation pour l'utilisateur ReadOnly. Cette fois, créez la classe Radius avec la valeur ReadUser au lieu de Administrator.

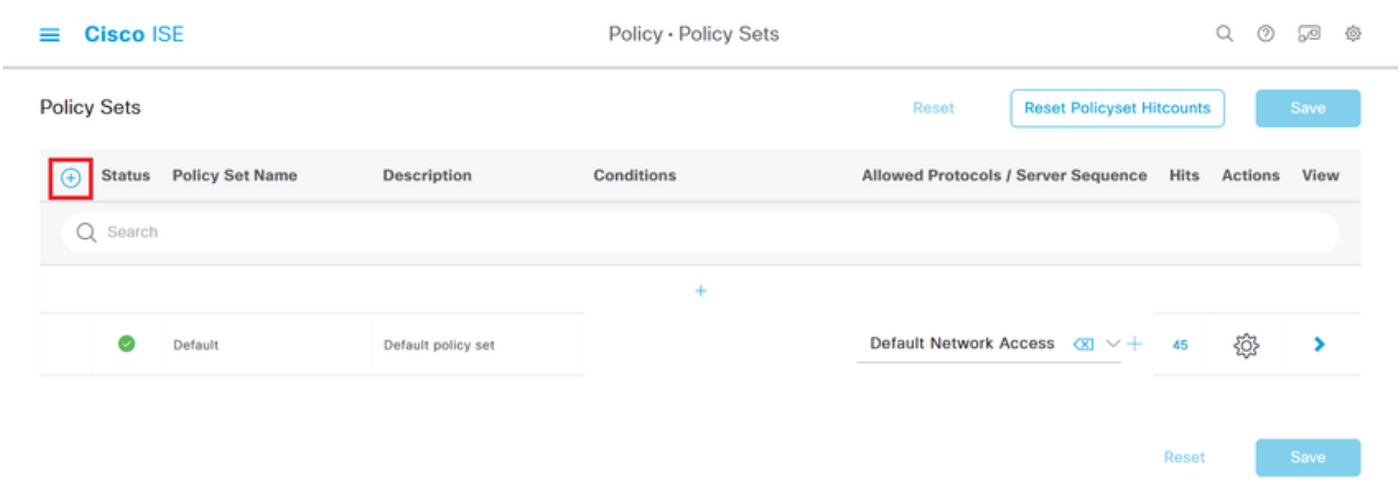




Étape 8. Créez un ensemble de stratégies correspondant à l'adresse IP FMC. Cela permet d'empêcher d'autres périphériques d'accorder l'accès aux utilisateurs.

Accédez à
> Policy > Policy Sets >

icône placée dans l'angle supérieur gauche.

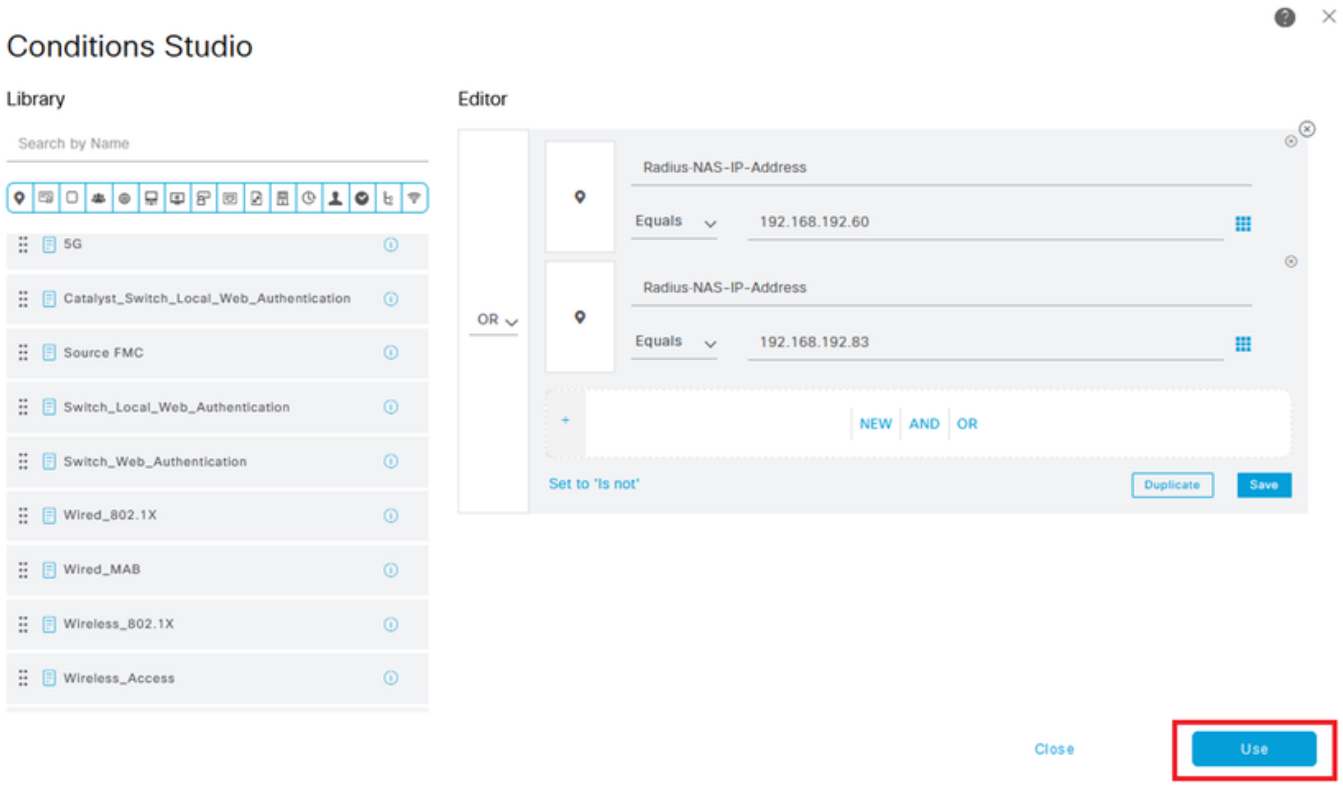


Étape 8.1. Une nouvelle ligne est placée en haut de vos ensembles de stratégies.

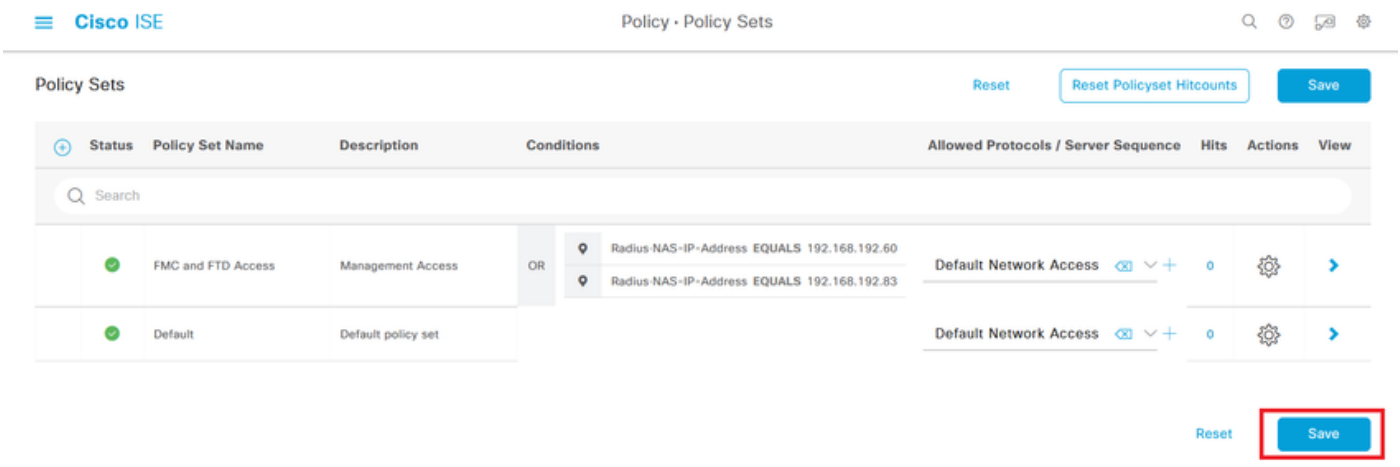
Nommez la nouvelle stratégie et ajoutez une condition supérieure pour l'attribut RADIUS NAS-IP-Address correspondant à l'adresse IP FMC.

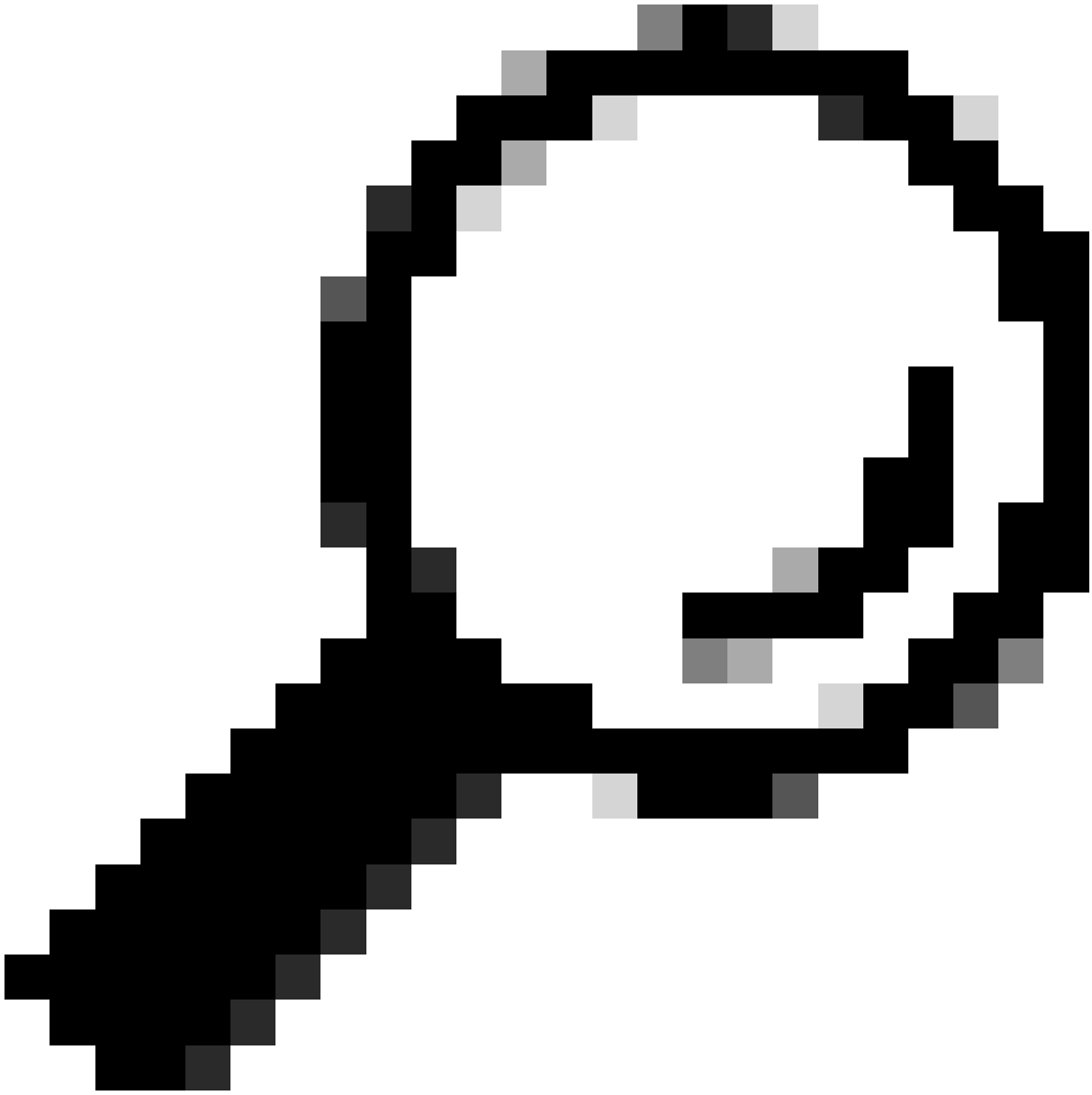
Ajoutez une deuxième condition avec la conjonction OR pour inclure l'adresse IP du FTD.

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



Étape 8.2. Une fois terminé, appuyez sur Enregistrer.

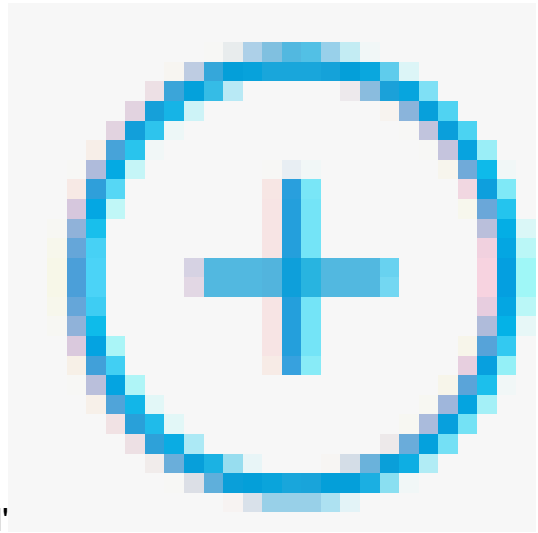




Conseil : pour cet exercice, nous avons autorisé la liste des protocoles d'accès réseau par défaut. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

Étape 9. Affichez le nouvel ensemble de stratégies en cliquant sur l'

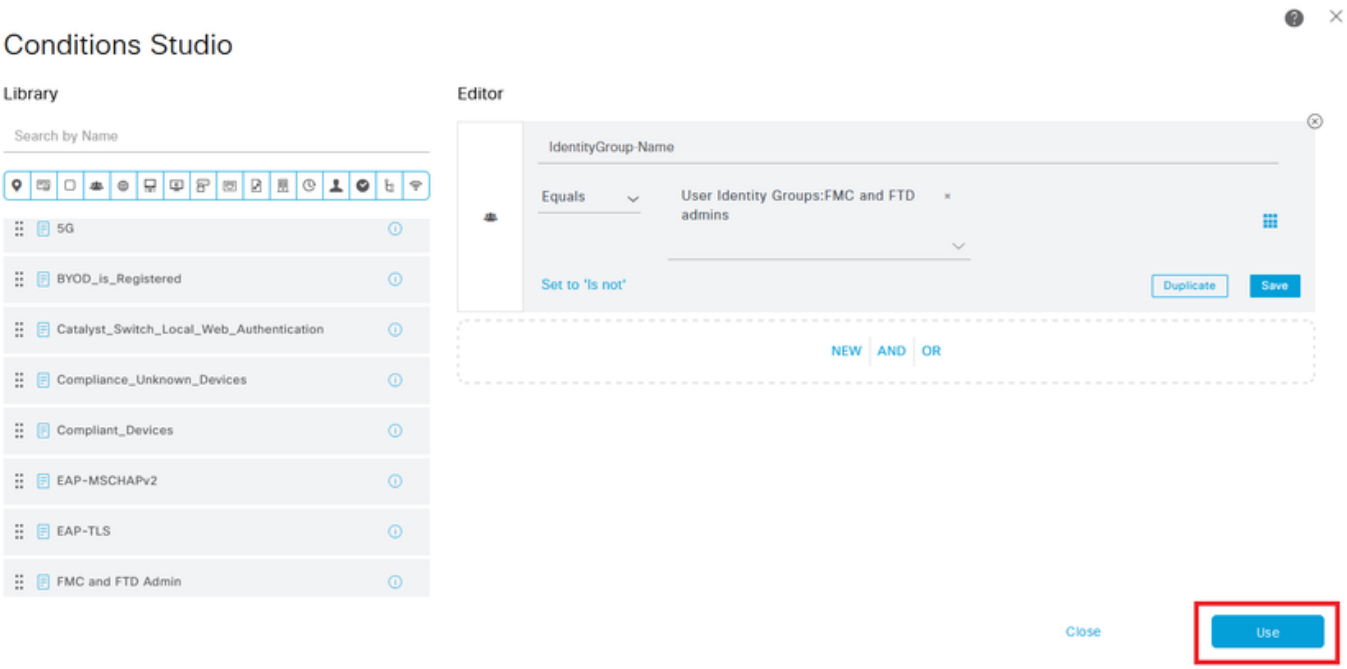
icône située à la fin de la ligne.



Développez le menu Stratégie d'autorisation et appuyez sur l' icône pour ajouter une nouvelle règle permettant 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 est égal à Groupes d'identités d'utilisateurs : administrateurs FMC et FTD (le nom de groupe créé à l'étape 4) et cliquez sur Utiliser.

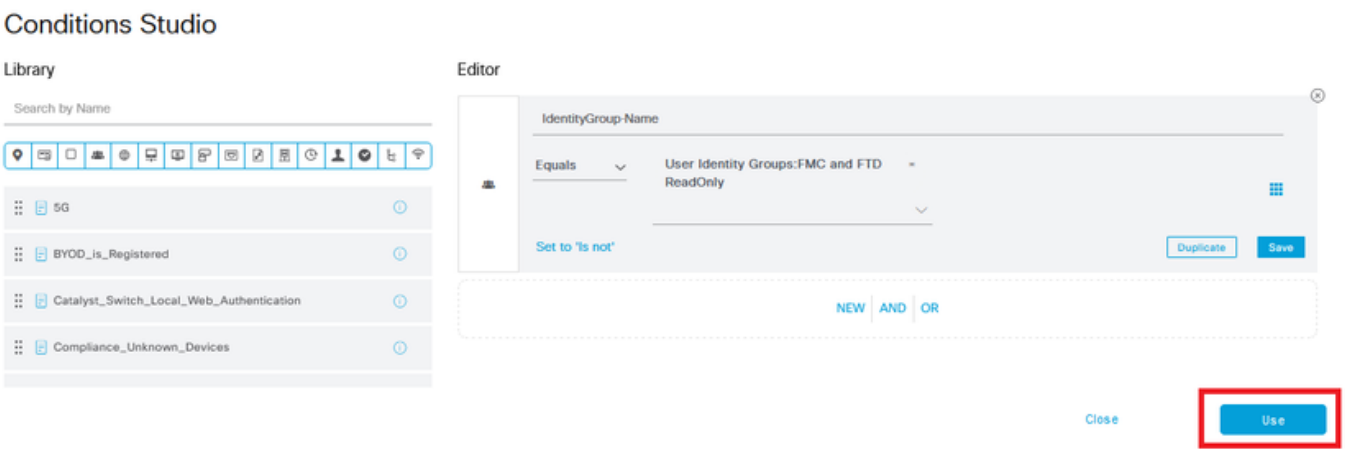


Étape 10. Cliquez sur l'

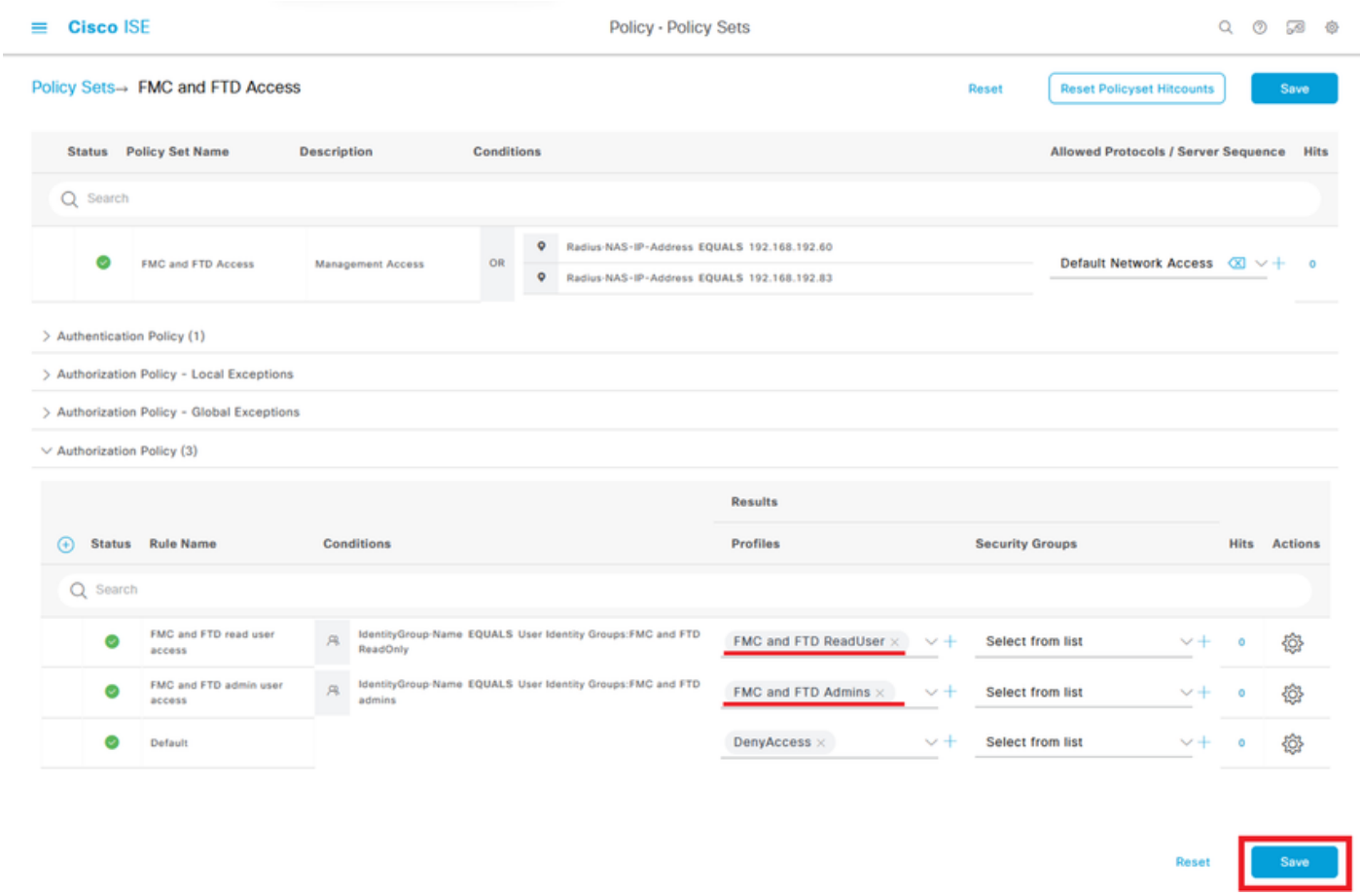
icône pour ajouter une deuxième règle autorisant l'accès à l'utilisateur disposant de droits en lecture seule.

Donnez-lui un nom.

Définissez les conditions pour faire correspondre le groupe d'identités de dictionnaire avec le nom d'attribut est égal aux groupes d'identités d'utilisateurs : FMC et FTD en lecture seule (le nom de groupe créé à l'étape 4) et cliquez sur Utiliser.

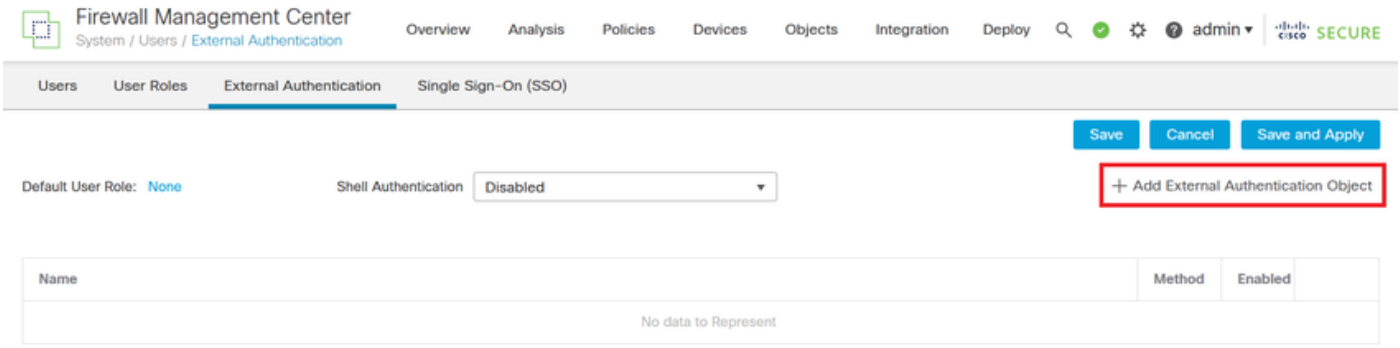


Étape 11. Définissez les profils d'autorisation respectivement pour chaque règle et cliquez sur Enregistrer.



Configuration FMC

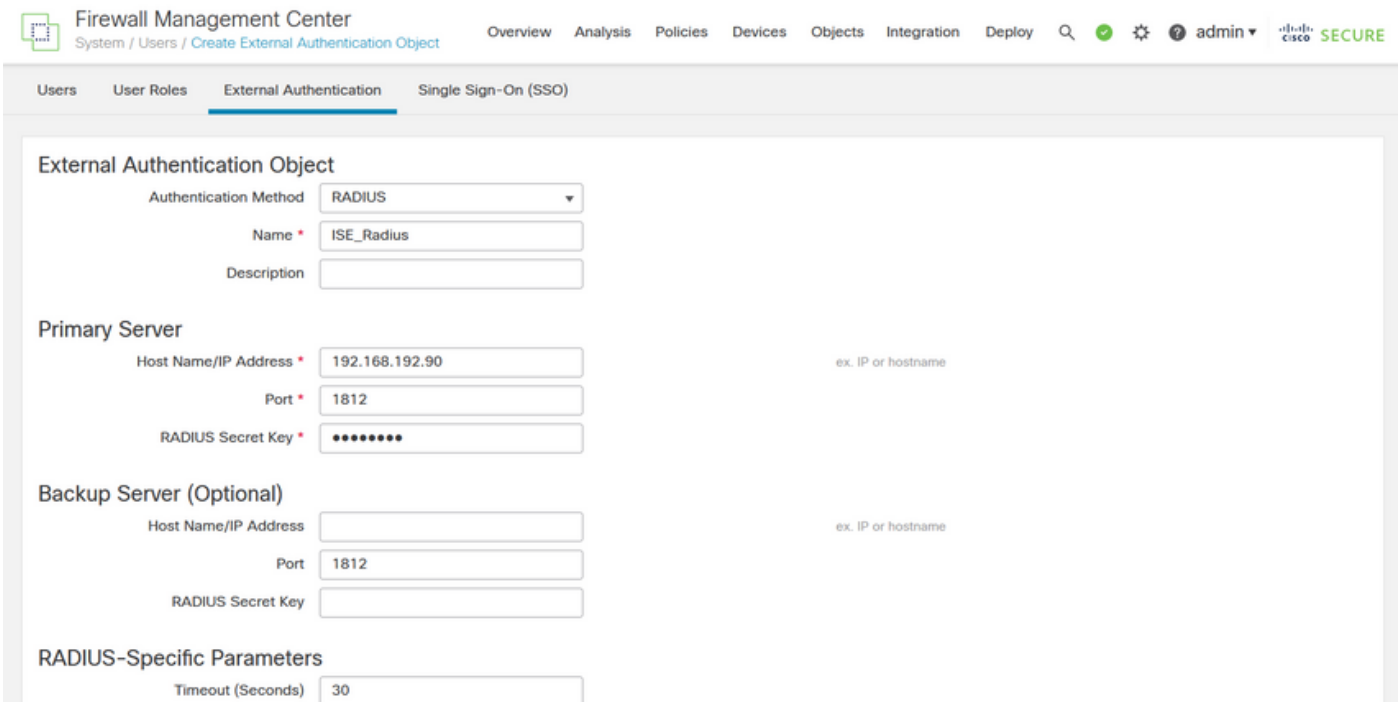
Étape 1. Créez l'objet d'authentification externe sous Système > Utilisateurs > Authentification externe > + Ajouter un objet d'authentification externe.



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.

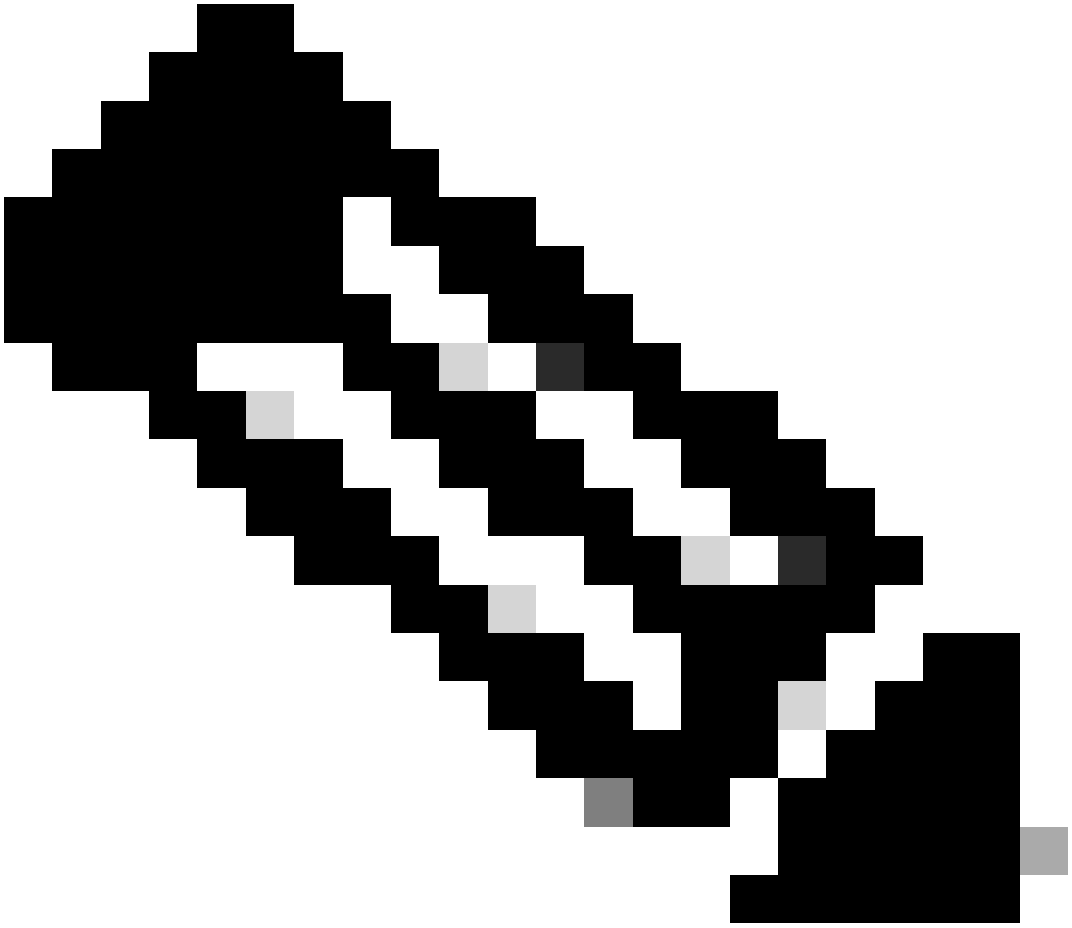


Étape 3. Insérez les valeurs d'attributs de classe RADIUS qui ont été configurées aux étapes 6 et 7 de Configuration ISE : Administrator et ReadUser pour firewall_admin et firewall_readuser respectivement.

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Administrator
Discovery Admin	
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Security Analyst	
Security Analyst (Read Only)	Class=ReadUser
Security Approver	
Threat Intelligence Director (TID) User	
Default User Role	Access Admin Administrator Discovery Admin External Database User

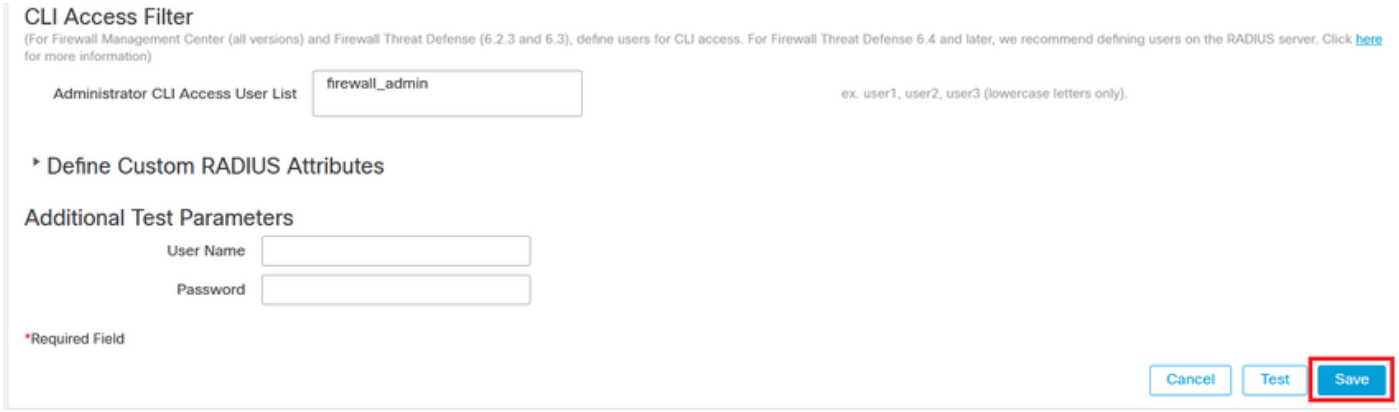
To specify the default user role if user is not found in any group



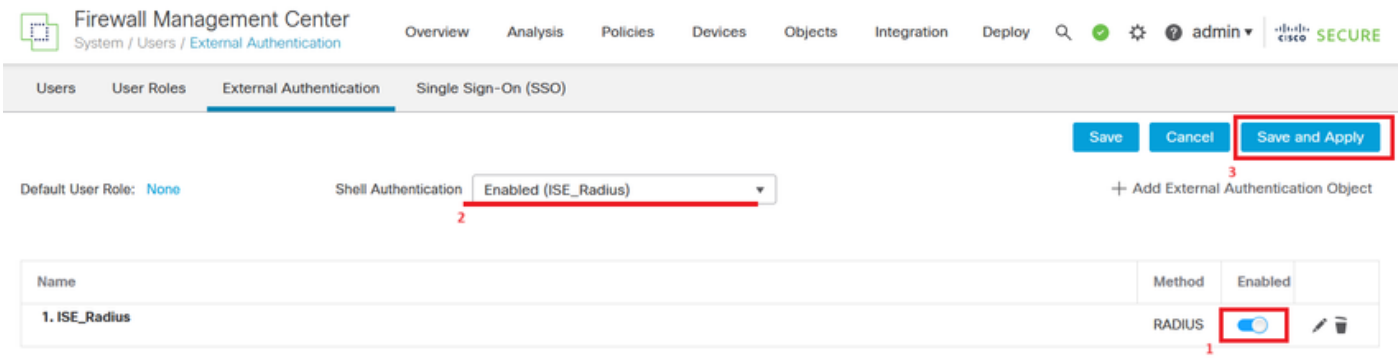
Remarque : la plage de temporisation est différente pour le FTD et le FMC. Par conséquent, si vous partagez un objet et modifiez la valeur par défaut de 30 secondes, veillez à ne pas dépasser une plage de temporisation plus petite (1 à 300 secondes) pour les périphériques FTD. Si vous définissez le délai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

Étape 4. Renseignez la Liste des utilisateurs d'accès à l'interface de ligne de commande de l'administrateur sous Filtre d'accès à l'interface de ligne de commande avec les noms autorisés pour accéder à l'interface.

Cliquez sur Save une fois terminé.

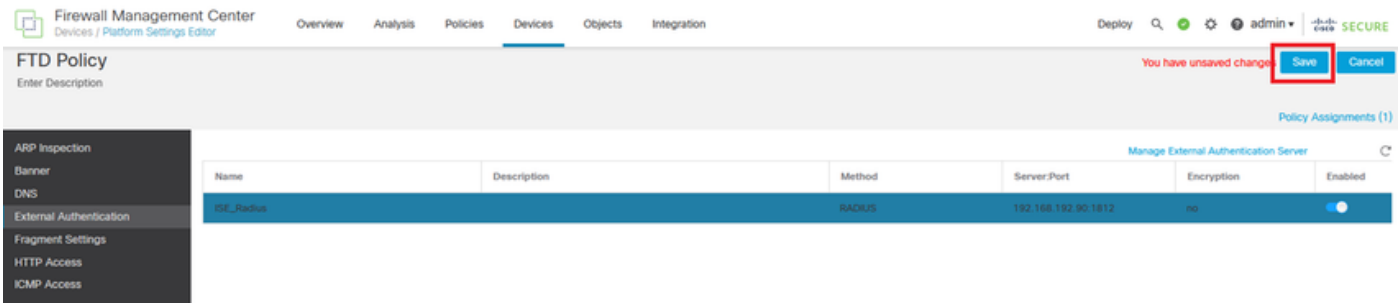


Étape 5. Activez le nouvel objet. Définissez-la comme méthode d'authentification Shell pour FMC et cliquez sur Enregistrer et appliquer.

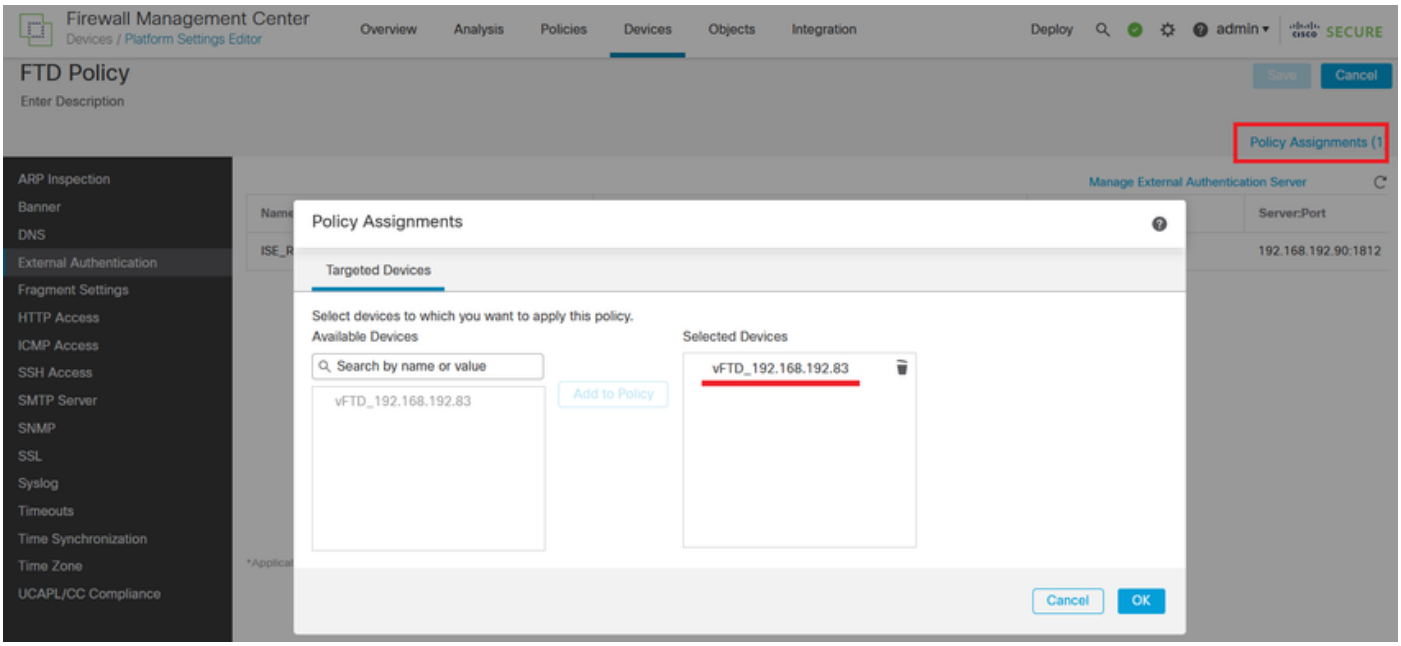


Configuration FTD

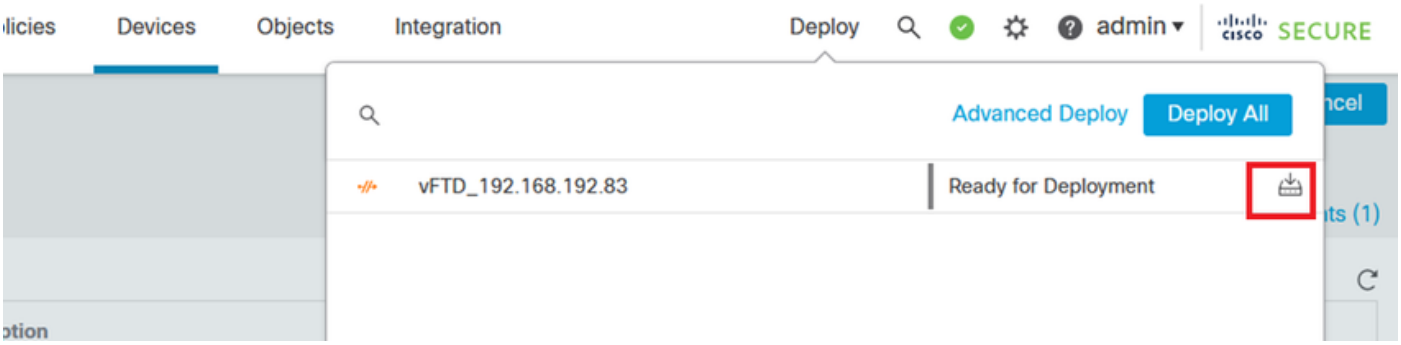
Étape 1. Dans l'interface utilisateur graphique de FMC, accédez à Devices > Platform Settings. Modifiez votre stratégie actuelle ou créez-en une nouvelle si aucune n'est affectée au FTD auquel vous avez besoin d'accéder. Activez le serveur RADIUS sous External Authentication et cliquez sur Save.



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

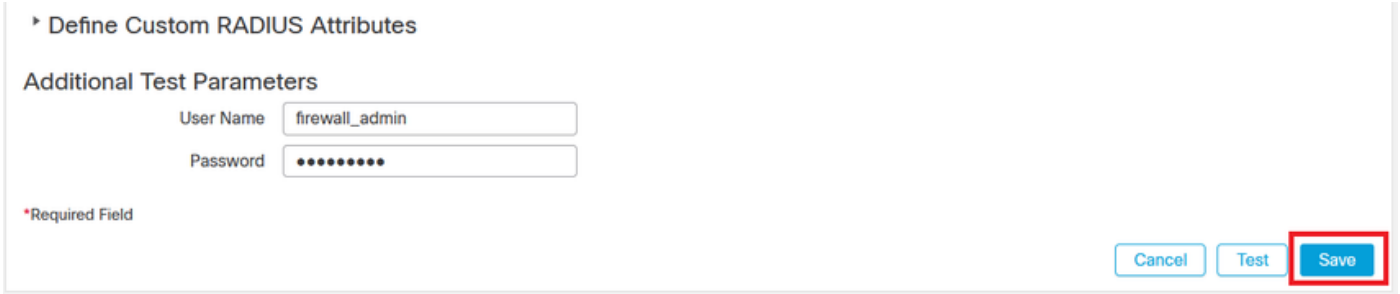


Étape 3. Déployez les modifications.

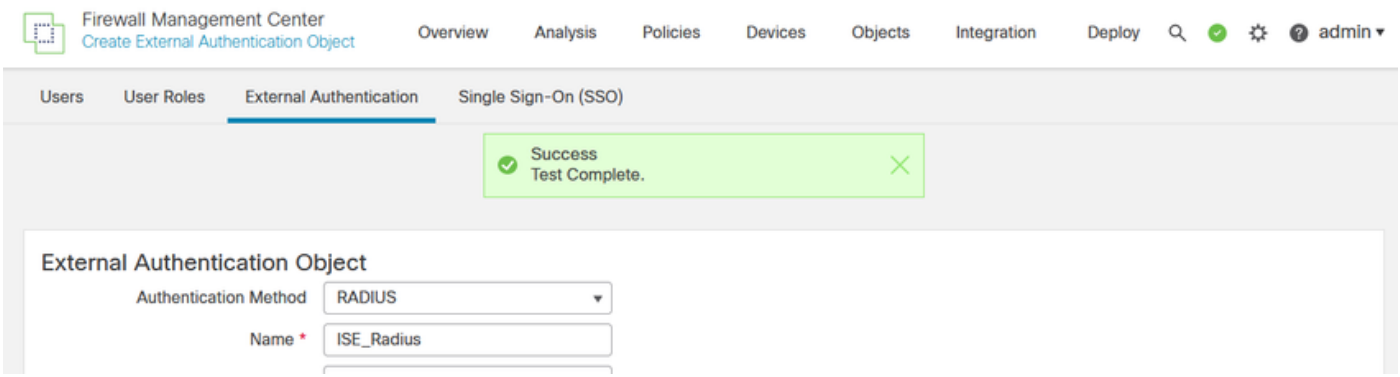


Vérifier

- 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.

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.