

# 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](#)

[Configuration FMC](#)

[Configuration FTD](#)

[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 7.2.5
- 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.

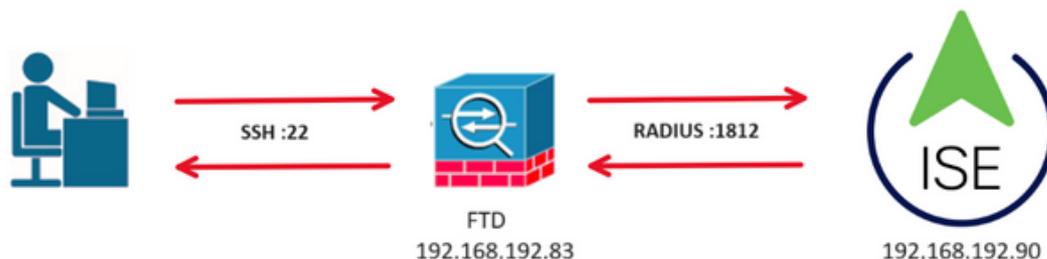
### Authentification externe pour FMC

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.

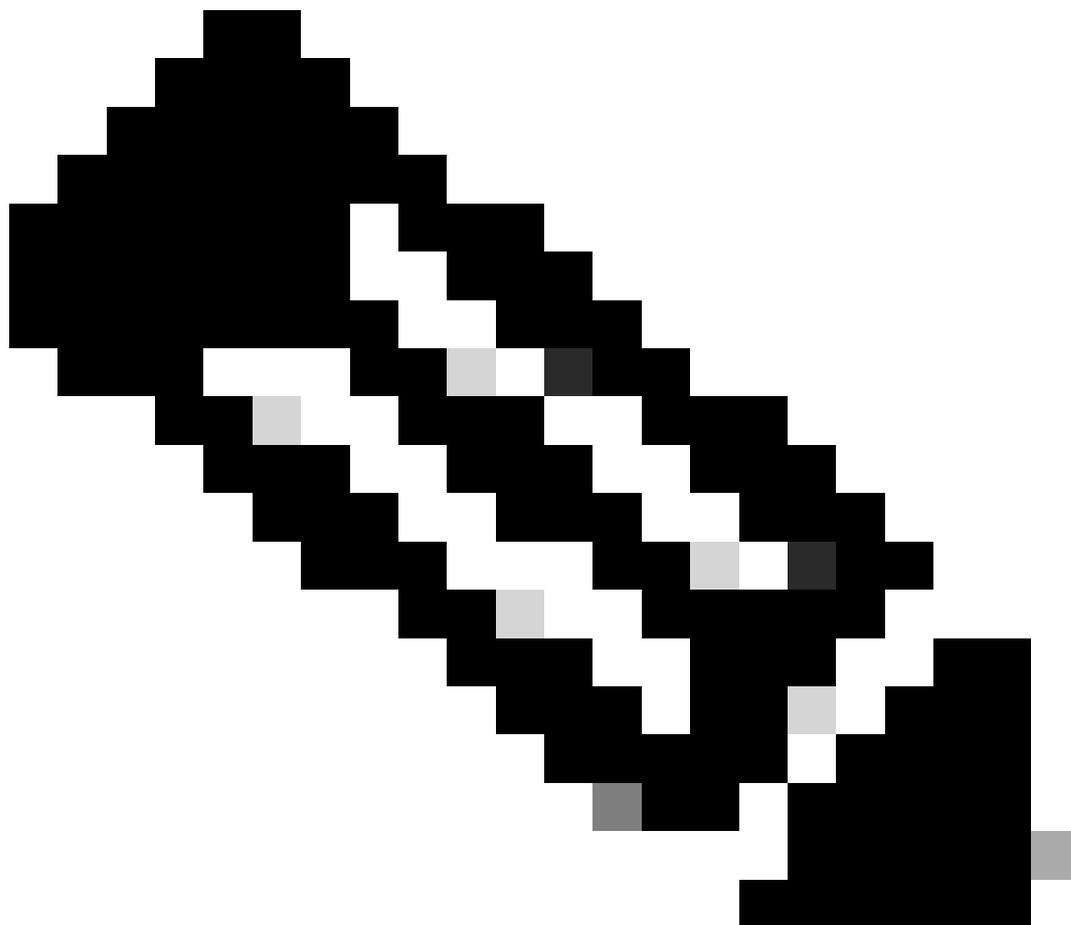
### Authentification externe pour FTD

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

### Topologie du réseau



## Configurer



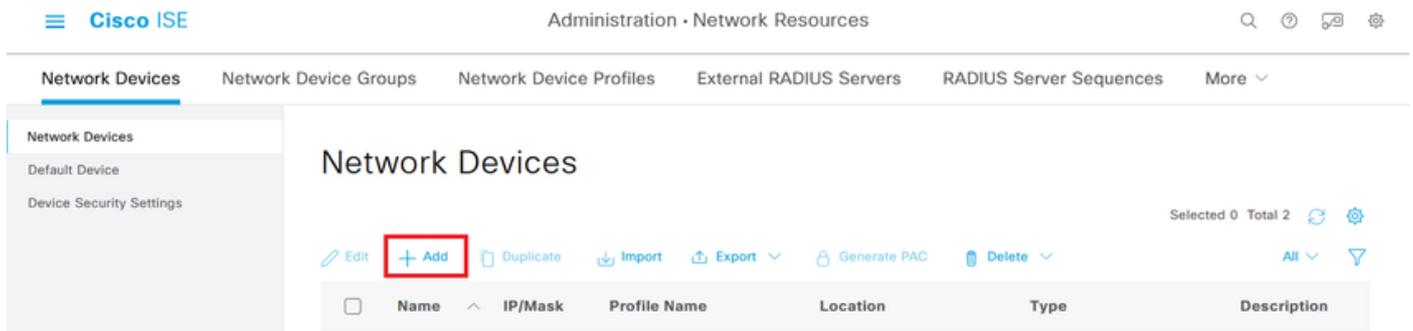
Remarque : il existe plusieurs façons de configurer les stratégies d'authentification et d'autorisation ISE pour les périphériques d'accès réseau (NAD) tels que FMC. L'exemple décrit dans ce document est un point de référence dans lequel nous créons deux profils (l'un avec des droits d'administrateur 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.

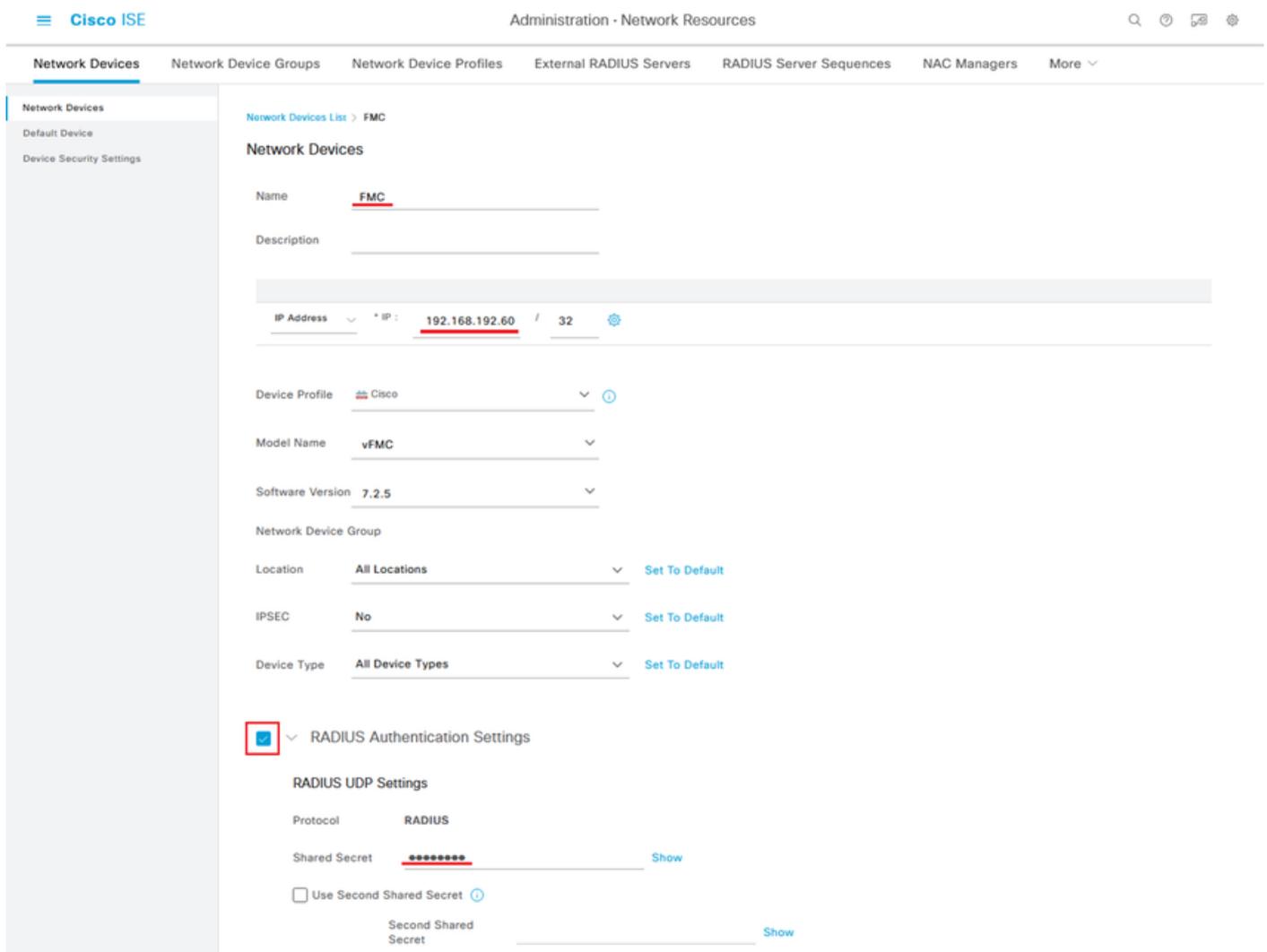


Étape 2. Attribuez un nom à l'objet périphérique réseau et insérez l'adresse IP FMC.

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.

The screenshot shows the configuration page for a Network Device named 'FTD'. The 'RADIUS Authentication Settings' section is highlighted with a red box. The configuration includes:

- Name: **FTD**
- Description: (empty)
- IP Address: **192.168.192.83 / 32**
- Device Profile: **Cisco**
- Model Name: **vFTD**
- Software Version: **7.2.5**
- Network Device Group: (empty)
- Location: **All Locations** (Set To Default)
- IPSEC: **No** (Set To Default)
- Device Type: **All Device Types** (Set To Default)
- RADIUS Authentication Settings**
- RADIUS UDP Settings**
- Protocol: **RADIUS**
- Shared Secret: **\*\*\*\*\*** (Show)
- Use Second Shared Secret (Show)

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

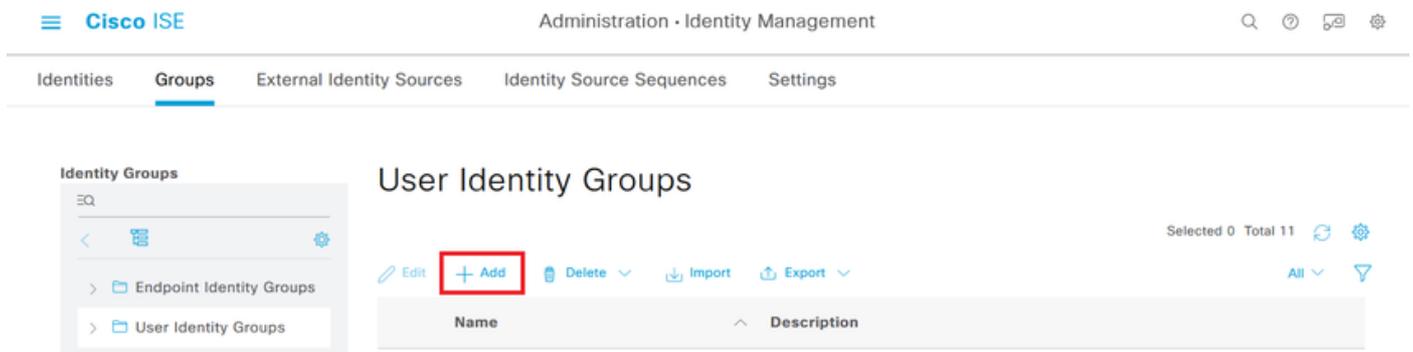
The screenshot shows the 'Network Devices' list in Cisco ISE. The table below lists the devices:

| Name                         | IP/Mask           | Profile Name | Location      | Type             | Description |
|------------------------------|-------------------|--------------|---------------|------------------|-------------|
| <input type="checkbox"/> FMC | 192.168.192.60/32 | Cisco        | All Locations | All Device Types |             |
| <input type="checkbox"/> FTD | 192.168.192.83/32 | Cisco        | All Locations | All Device Types |             |

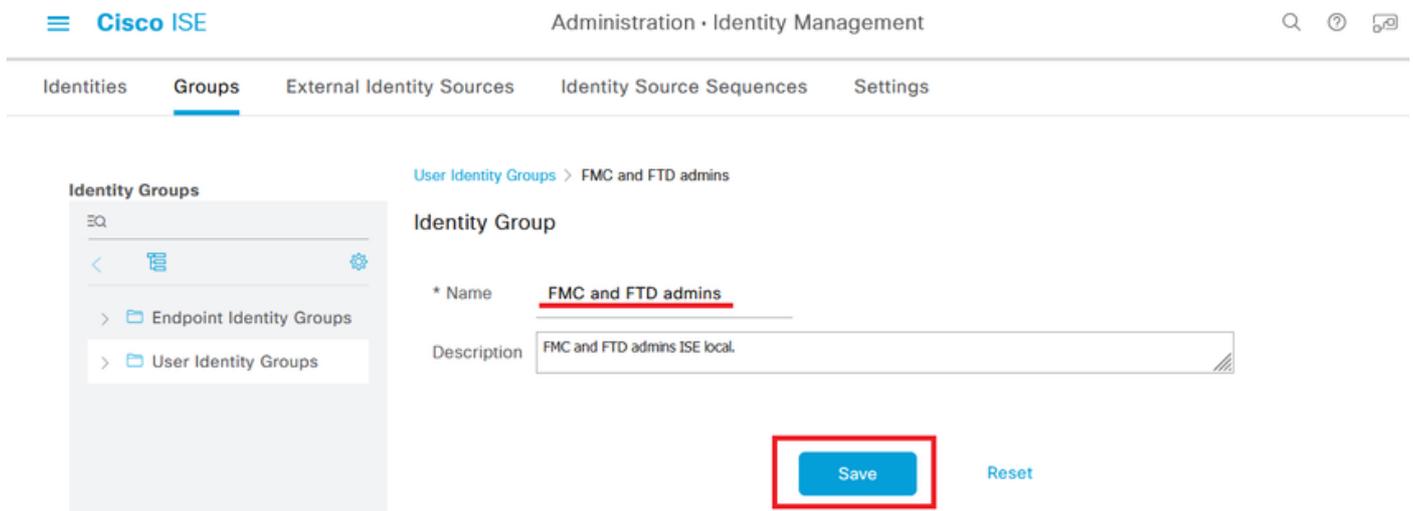
Étape 3. Créez les groupes d'identités utilisateur requis. Accédez à l'icône du hamburger



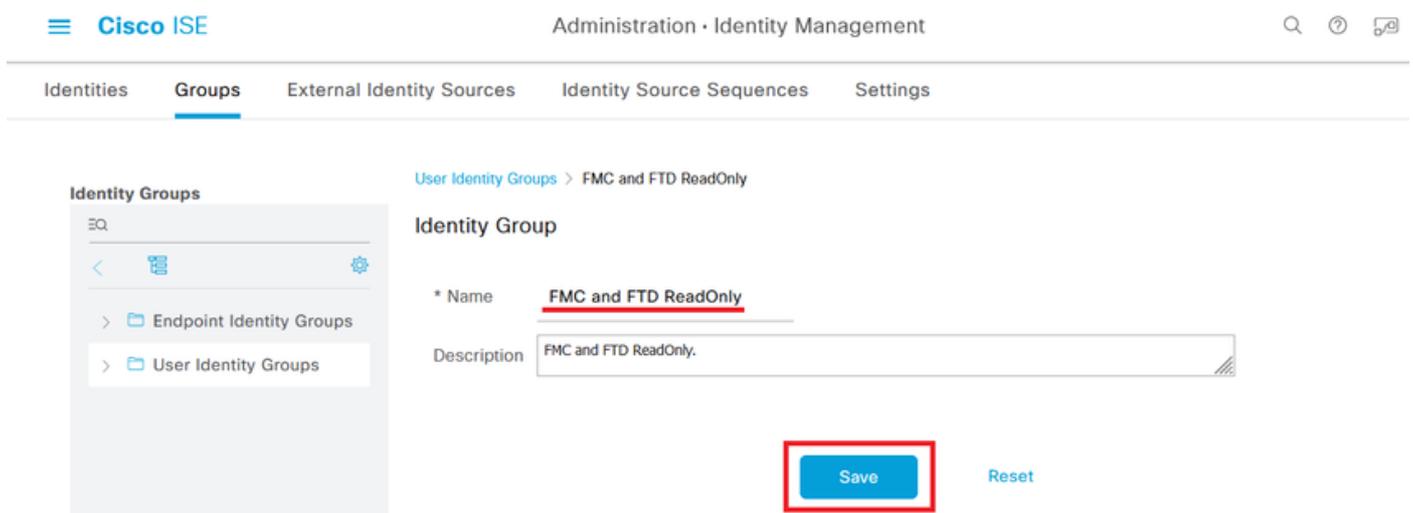
située dans l'angle supérieur gauche > Administration > Identity Management > Groups > User Identity Groups > + Add



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.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE', 'Administration · Identity Management', and search, refresh, and settings icons. Below the navigation bar, the 'Groups' tab is selected. The left sidebar shows 'Identity Groups' with a search bar and a tree view containing 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups' and shows a table with two rows. The first row is 'fmc' with a description 'FMC and FTD ReadOnly'. The second row is 'FMC and FTD admins' with a description 'FMC and FTD admins ISE local.'. Above the table are buttons for 'Edit', 'Add', 'Delete', 'Import', and 'Export'. In the top right corner of the table area, there is a 'Quick Filter' dropdown menu, which is highlighted with a red box.

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



jusqu'à

> Administration > Identity Management > Identities > + Add.

Users

Latest Manual Network Scan Res...

## Network Access Users

Selected 0 Total 0 🔄 ⚙

[Edit](#) **+ Add** [Change Status](#) [Import](#) [Export](#) [Delete](#) [All](#) [Filter](#)

| Status            | Username | Description | First Name | Last Name | Email Address | User Identity Groups | Adm |
|-------------------|----------|-------------|------------|-----------|---------------|----------------------|-----|
| No data available |          |             |            |           |               |                      |     |

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.

Users

Latest Manual Network Scan Res...

[Network Access Users List](#) > [New Network Access User](#)

### Network Access User

\* Username firewall\_admin

Status  Enabled

Account Name Alias ⓘ

Email

### Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

Password Re-Enter Password

\* Login Password ●●●●●●●● ●●●●●●●● [Generate Password](#) ⓘ

Enable Password \_\_\_\_\_ \_\_\_\_\_ [Generate Password](#) ⓘ

Users

Latest Manual Network Scan Res...

## User Groups

FMC and FTD admins

Submit

Cancel

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.

Users

Latest Manual Network Scan Res...

Network Access Users List &gt; New Network Access User

## Network Access User

\* Username firewall\_readuserStatus  Enabled

Account Name Alias

Email

## Passwords

Password Type: Internal Users

Password Lifetime:

 With Expiration ⓘ Never Expires ⓘ

Password

Re-Enter Password

\* Login Password

Re-Enter Password

Generate Password ⓘ

Enable Password

Generate Password ⓘ

Identities   Groups   External Identity Sources   Identity Source Sequences   Settings

Users  
Latest Manual Network Scan Res...

▼ User Groups

⋮ FMC and FTD ReadOnly ▼ ⓘ +

Submit Cancel

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.

Cisco ISE Policy · Policy Elements

Dictionarys Conditions **Results**

Authentication > Allowed Protocols

Authorization > Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > FMC and FTD Admins

### Authorization Profile

\* Name **FMC and FTD Admins**

Description

\* Access Type **ACCESS\_ACCEPT**

Network Device Profile **Cisco**

Service Template

Cisco ISE Policy · Policy Elements

Dictionarys Conditions **Results**

Authentication >

Authorization > Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

**Radius:Class** = **Administrator**

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

**Submit** Cancel

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.

Cisco ISE Policy · Policy Elements

Dictionarys Conditions **Results**

Authentication > Allowed Protocols

Authorization > Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name **FMC and FTD ReadUser**

Description

\* Access Type **ACCESS\_ACCEPT**

Network Device Profile **Cisco**

Service Template

Navigation: Dictionaries | Conditions | **Results**

Left sidebar menu:

- Authentication >
- Authorization ▾
  - Authorization Profiles
  - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Main content area:

Advanced Attributes Settings

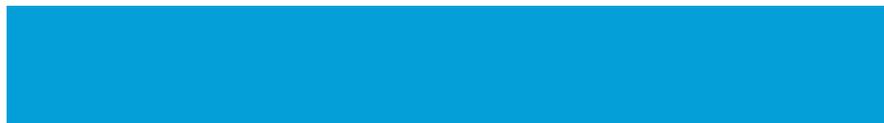
⋮ Radius:Class ▾ = ReadUser ▾ - +

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = ReadUser

Buttons: **Submit** (highlighted with a red box) | Cancel

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.

Cisco ISE Policy - Policy Sets

Policy Sets Reset Reset Policyset Hitcounts Save

|  Status | Policy Set Name | Description        | Conditions | Allowed Protocols / Server Sequence  | Hits | Actions   | View |
|--|-----------------|--------------------|------------|--|------|---|------|
|         | Default         | Default policy set |            | Default Network Access   | 45   |   |      |

Reset Save

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.

Conditions Studio

Library

Search by Name

5G  
Catalyst\_Switch\_Local\_Web\_Authentication  
Source FMC  
Switch\_Local\_Web\_Authentication  
Switch\_Web\_Authentication  
Wired\_802.1X  
Wired\_MAB  
Wireless\_802.1X  
Wireless\_Access

Editor

Radius-NAS-IP-Address  
Equals 192.168.192.60

OR

Radius-NAS-IP-Address  
Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

Étape 8.2. Une fois terminé, appuyez sur Enregistrer.

Cisco ISE

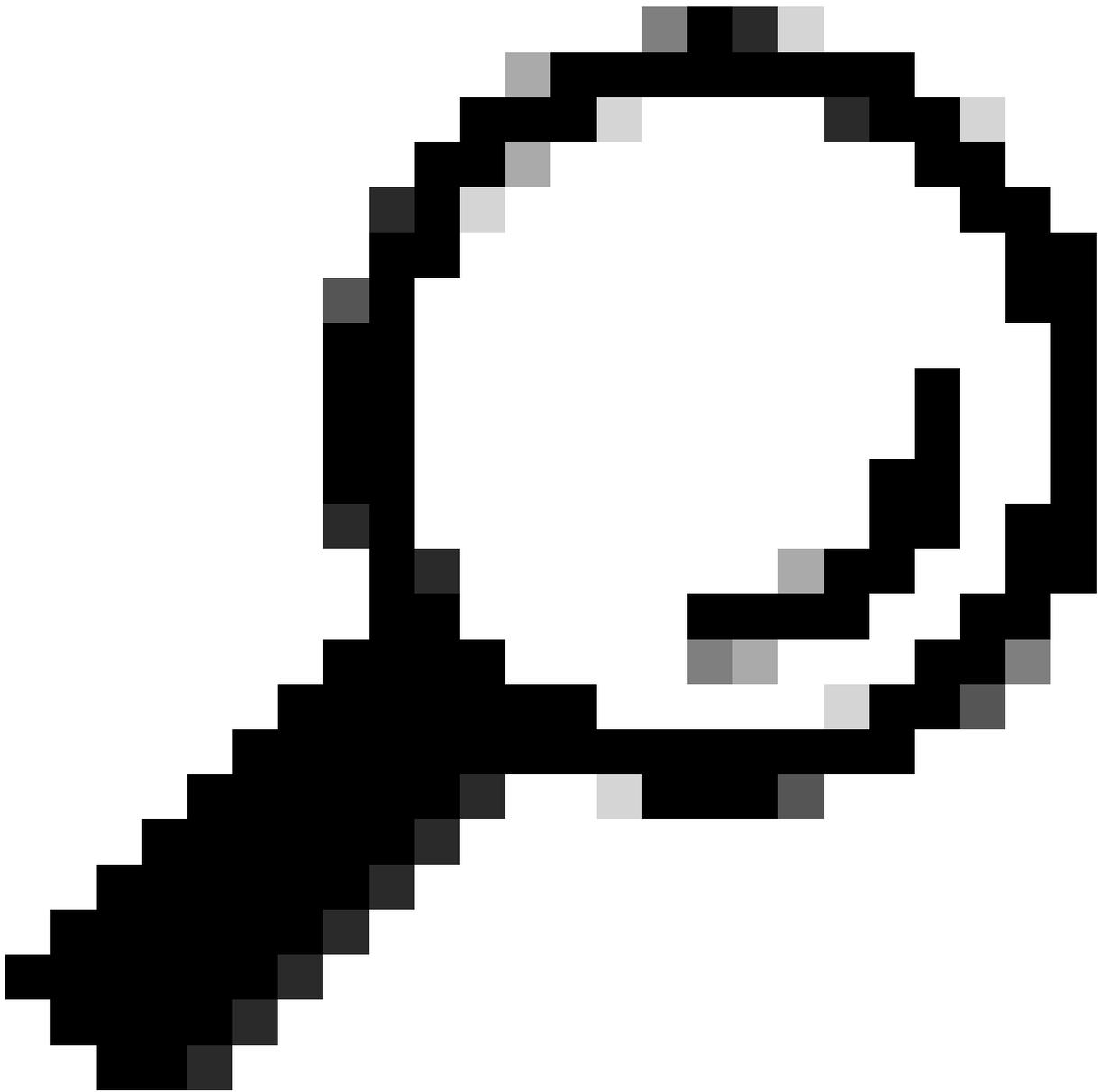
Policy > Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

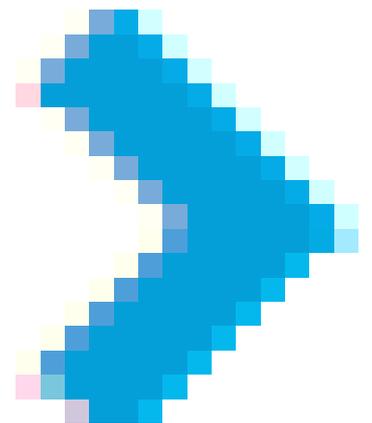
| Status | Policy Set Name    | Description        | Conditions   | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------|--------------------|--------------------|--|-------------------------------------|------|---------|------|
| ✓      | FMC and FTD Access | Management Access  | OR<br>Radius-NAS-IP-Address EQUALS 192.168.192.60<br>Radius-NAS-IP-Address EQUALS 192.168.192.83 | Default Network Access              | 0    | ⚙️      | ➔    |
| ✓      | Default            | Default policy set |  | Default Network Access              | 0    | ⚙️      | ➔    |

Reset Save



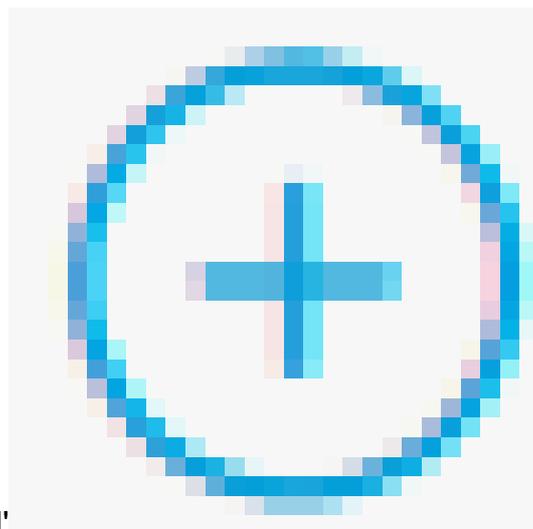
Conseil : pour cet exercice, nous avons autorisé la liste des protocoles d'accès réseau par défaut. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

---



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.

Conditions Studio

Library

Search by Name

- 5G
- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- EAP-MSCHAPv2
- EAP-TLS
- FMC and FTD Admin

Editor

IdentityGroup Name

Equals User Identity Groups:FMC and FTD admins

Set to 'is not'

Duplicate Save

NEW AND OR

Close Use

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.

## Conditions Studio

### Library

Search by Name



- 5G
- BYOD\_Is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices

### Editor

IdentityGroup-Name

Equals User Identity Groups:FMC and FTD  
ReadOnly

Set to 'Is not'

Duplicate Save

NEW AND OR

Close



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

Cisco ISE

Policy - Policy Sets

Policy Sets → FMC and FTD Access

Reset

Reset Policyset Hitcounts

Save

| Status | Policy Set Name    | Description       | Conditions   | Allowed Protocols / Server Sequence | Hits |
|--------|--------------------|-------------------|--|-------------------------------------|------|
| 🟢      | FMC and FTD Access | Management Access | OR<br>• Radius-NAS-IP-Address EQUALS 192.168.192.60<br>• Radius-NAS-IP-Address EQUALS 192.168.192.83 | Default Network Access              | 0    |

> Authentication Policy (1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy (3)

| Status | Rule Name                     | Conditions  | Results              |                  |   | Hits | Actions |
|--------|-------------------------------|---|----------------------|------------------|---|------|---------|
|        |                               |   | Profiles             | Security Groups  |   |      |         |
| 🟢      | FMC and FTD read user access  | IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly | FMC and FTD ReadUser | Select from list | 0 | ⚙️   |         |
| 🟢      | FMC and FTD admin user access | IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins   | FMC and FTD Admins   | Select from list | 0 | ⚙️   |         |
| 🟢      | Default                       |   | DenyAccess           | Select from list | 0 | ⚙️   |         |

Reset



## Configuration FMC

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

Firewall Management Center  
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ 👤 admin | cisco SECURE

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Disabled

Save Cancel Save and Apply

+ Add External Authentication Object

| Name                 | Method | Enabled |
|----------------------|--------|---------|
| No data to Represent |        |         |

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.

Firewall Management Center  
System / Users / Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ 👤 admin | cisco SECURE

Users User Roles External Authentication Single Sign-On (SSO)

### External Authentication Object

Authentication Method: RADIUS

Name: ISE\_Radius

Description:

### Primary Server

Host Name/IP Address: 192.168.192.90 (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: ●●●●●●

### Backup Server (Optional)

Host Name/IP Address: (ex. IP or hostname)

Port: 1812

RADIUS Secret Key:

### RADIUS-Specific Parameters

Timeout (Seconds): 30

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)

Retries

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

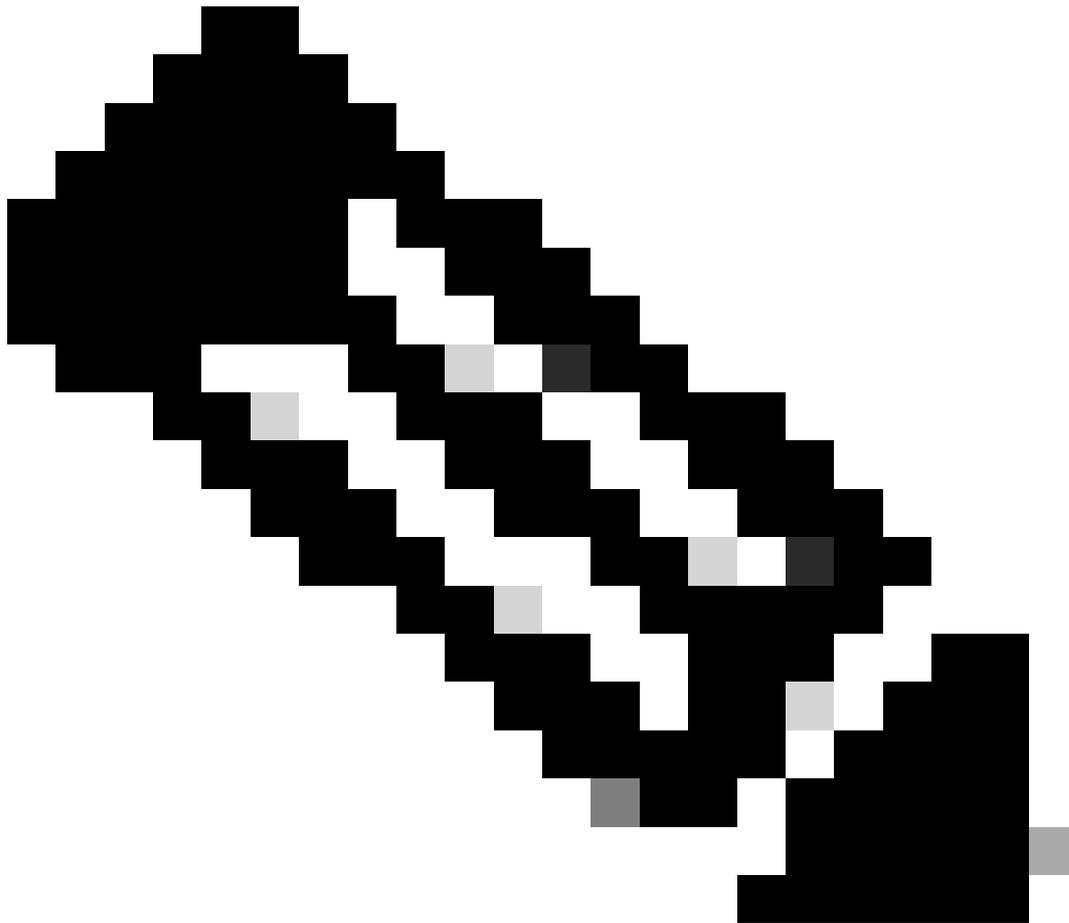
Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Default User Role

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.

### CLI Access Filter

(For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List  ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

\*Required Field

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

Firewall Management Center  
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: None Shell Authentication Enabled (ISE\_Radius) + Add External Authentication Object

| Name          | Method | Enabled                             |
|---------------|--------|-------------------------------------|
| 1. ISE_Radius | RADIUS | <input checked="" type="checkbox"/> |

## 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.

Firewall Management Center  
Devices / Platform Settings Editor

Overview Analysis Policies Devices Objects Integration

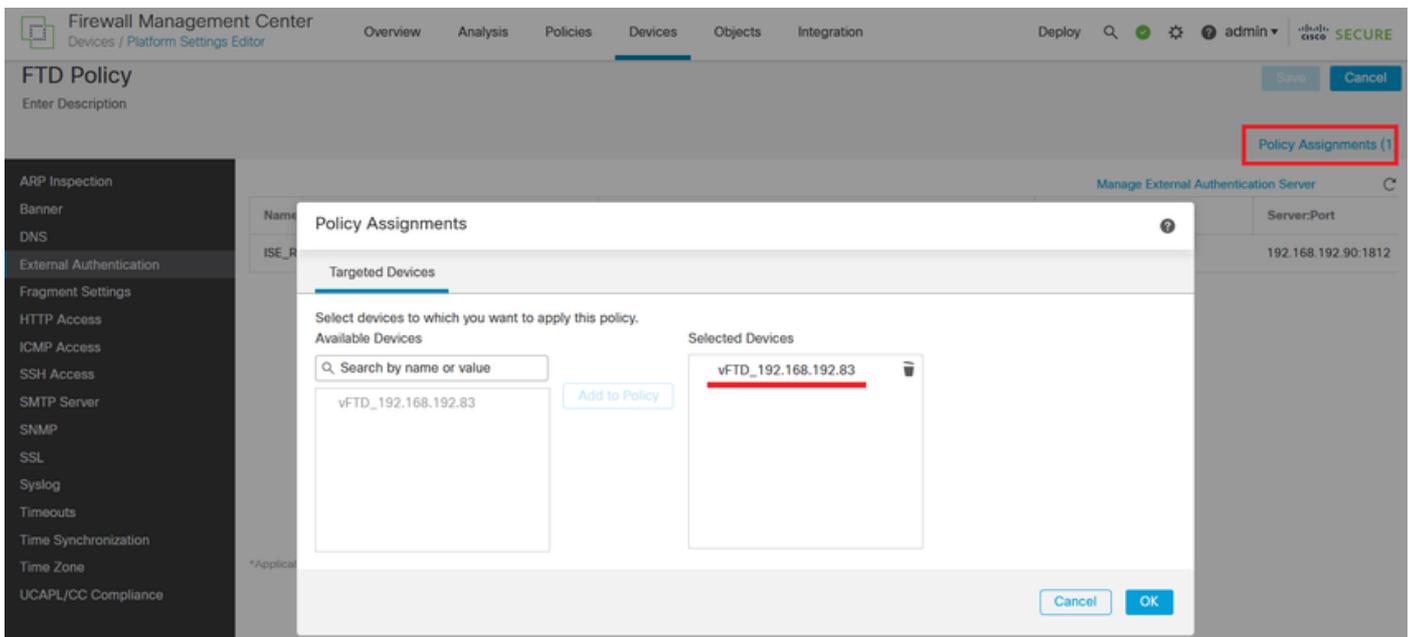
FTD Policy You have unsaved changes

Enter Description

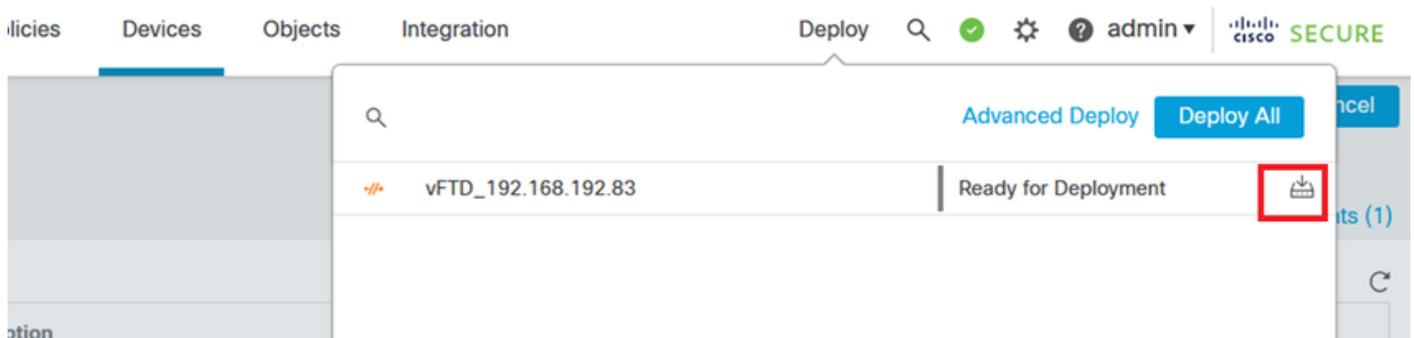
Manage External Authentication Server

| Name       | Description | Method | Server/Port         | Encryption | Enabled                             |
|------------|-------------|--------|---------------------|------------|-------------------------------------|
| ISE_Radius |             | RADIUS | 192.168.192.90:1812 | no         | <input checked="" type="checkbox"/> |

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

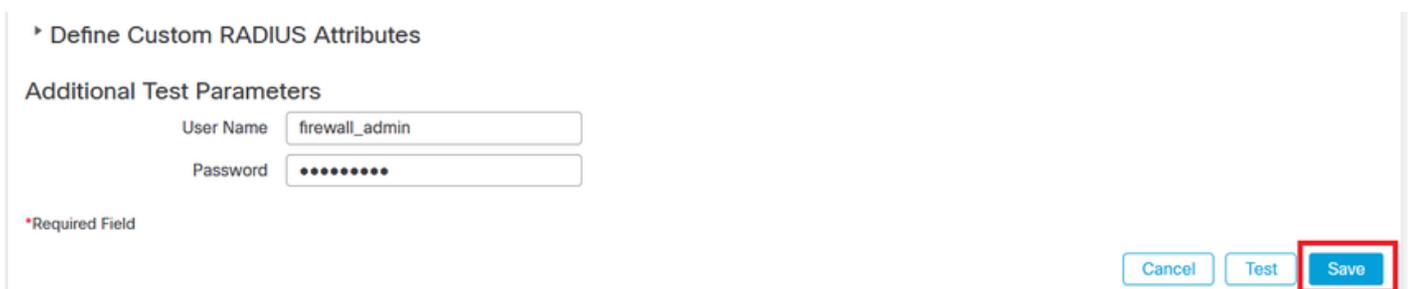


Étape 3. Déployez les modifications.



## 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.

✔ Success  
Test Complete. ✕

### External Authentication Object

Authentication Method

Name \*

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

▸ Define Custom RADIUS Attributes

### Additional Test Parameters

User Name

Password

### Test Output

Show Details ▾

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

\*Required Field

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.