

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.

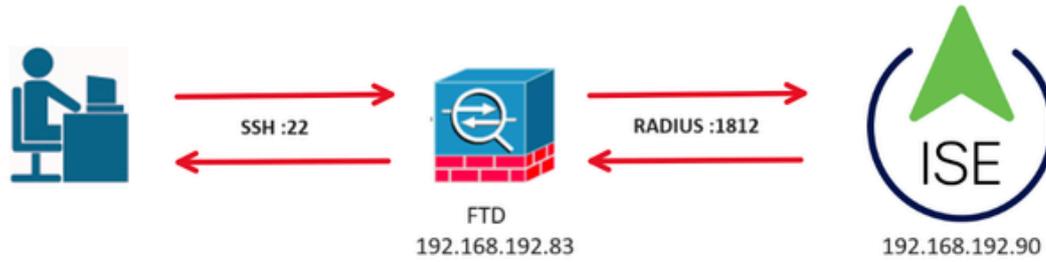
Authentification externe pour FMC

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



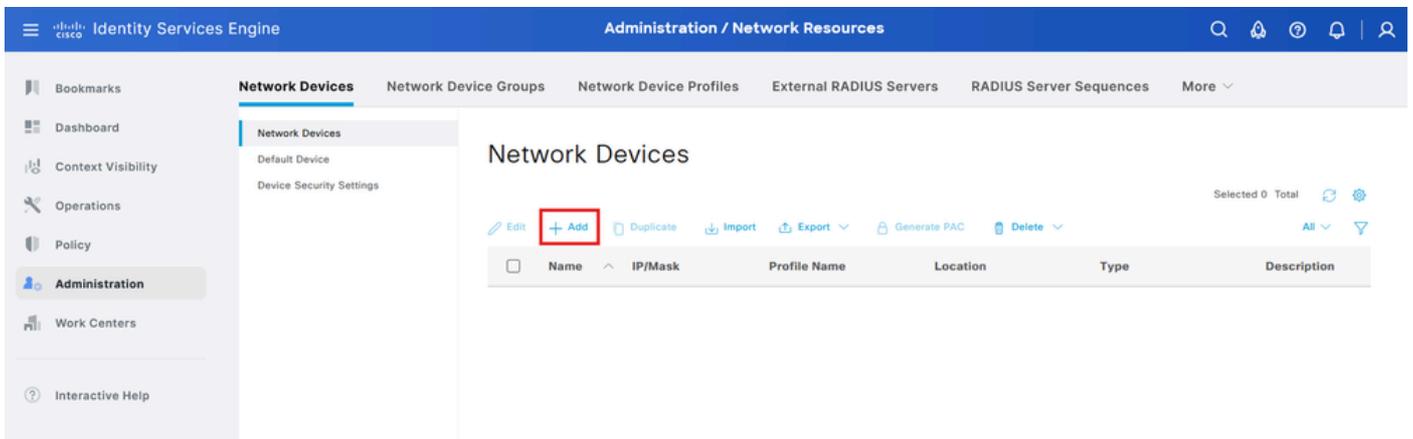
Remarque : Il existe plusieurs façons de configurer les stratégies d'authentification et d'autorisation ISE pour les périphériques d'accès réseau (NAD) tels que FMC. L'exemple décrit dans ce document est un point de référence dans lequel nous créons deux profils (l'un avec des droits d'administrateur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

The screenshot displays the Cisco Identity Services Engine Administration interface. The top navigation bar shows 'Administration / Network Resources'. The left sidebar contains various navigation options, with 'Administration' highlighted. The main content area is titled 'Network Devices' and shows the configuration for a device named 'FMC'. The configuration includes fields for Name, Description, IP Address (192.168.192.60 / 32), Device Profile (Cisco), Model Name, Software Version, Network Device Group, Location (All Locations), IPSEC (No), and Device Type (All Device Types). The RADIUS Authentication Settings are checked, and the RADIUS UDP Settings are visible, including the Protocol (RADIUS) and the Shared Secret (masked with dots). A 'Show' button is next to the Shared Secret field. Red arrows point to the Name field, the IP address field, the RADIUS Authentication Settings checkbox, and the Shared Secret field.

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.

Network Devices

Network Devices List > FTD

Network Devices

Name FTD

Description _____

IP Address * IP : 192.168.192.83 / 32

Device Profile Cisco

Model Name _____

Software Version _____

Network Device Group _____

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

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

Network Devices

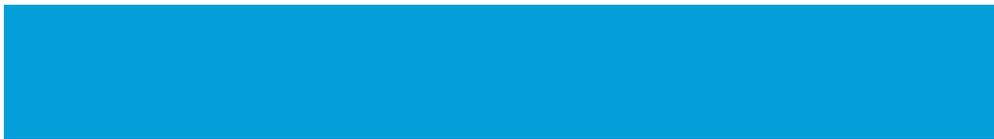
Selected 0 Total 2

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Export](#) [Generate PAC](#) [Delete](#)

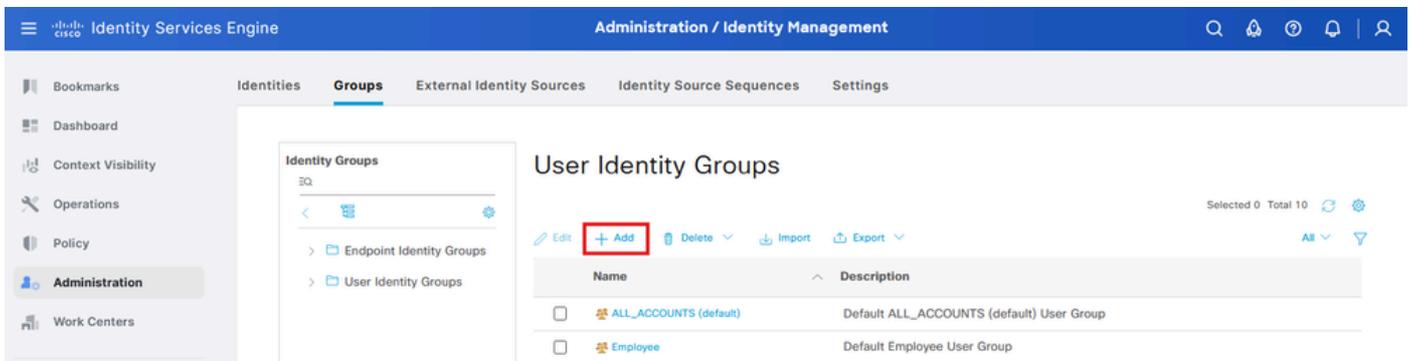
Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/> FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

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

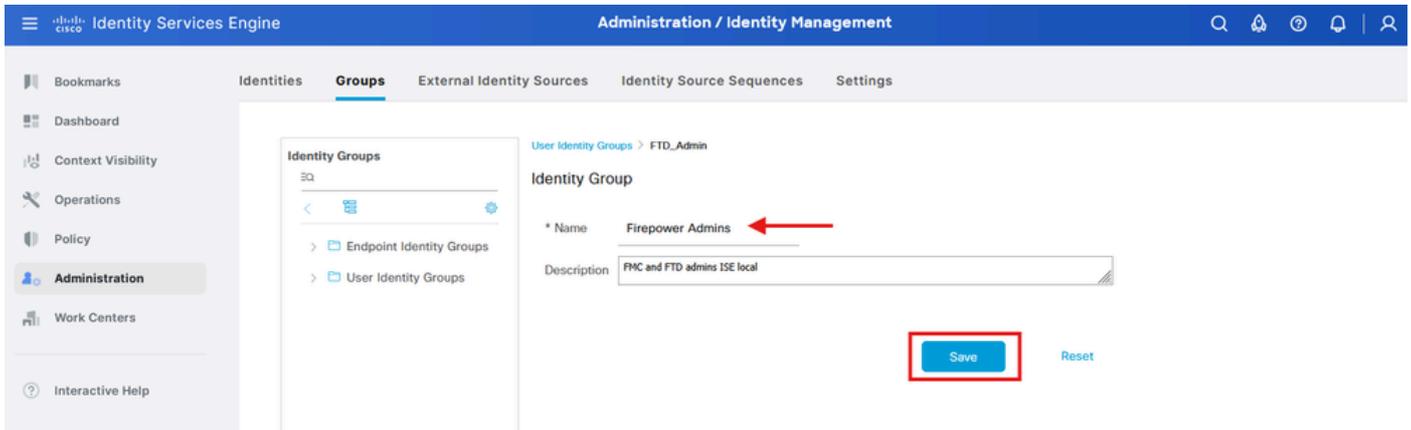
Étape 3 : création des groupes d'identités utilisateur requis Accédez à l'icône Burger



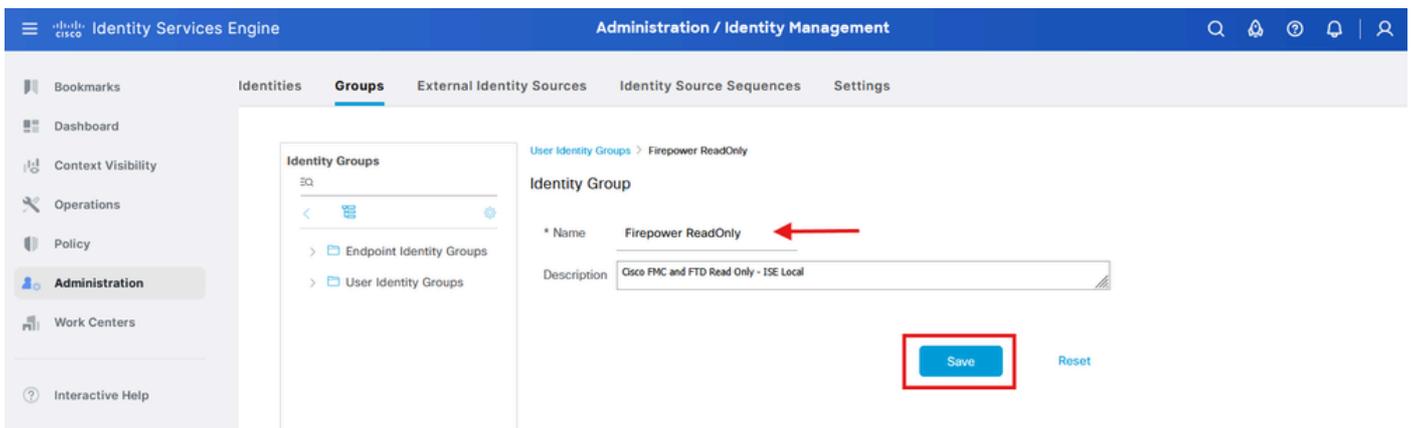
situé dans le coin supérieur gauche > Administration > Identity Management > Groups > User Identity Groups > + Add



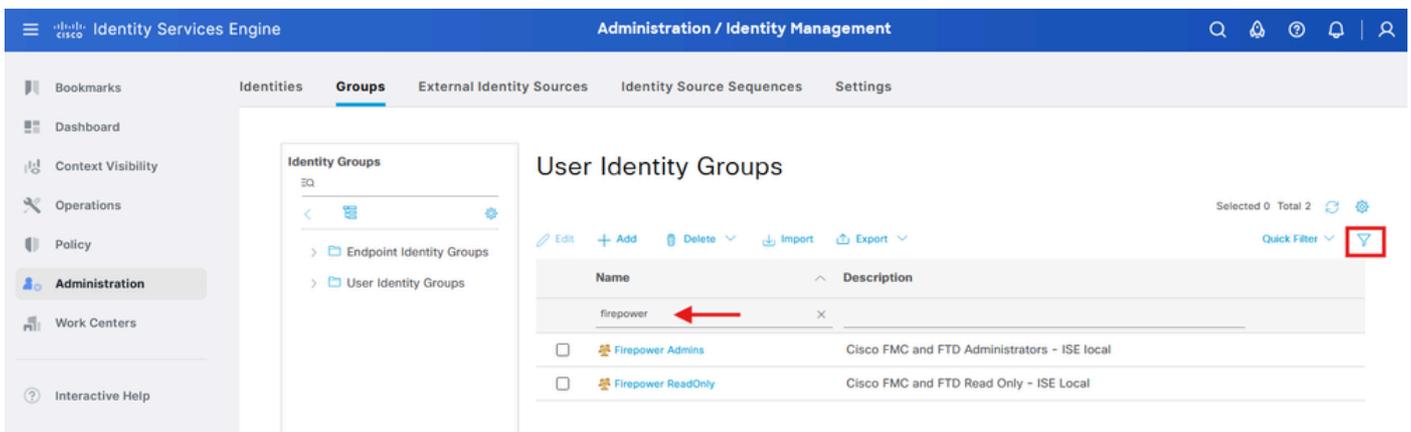
Étape 4. Attribuez un nom à chaque groupe et enregistrez-le individuellement. Dans cet exemple, nous créons un groupe pour les administrateurs et un autre pour les utilisateurs en lecture seule. Commencez par créer le groupe pour l'utilisateur disposant de droits d'administrateur.



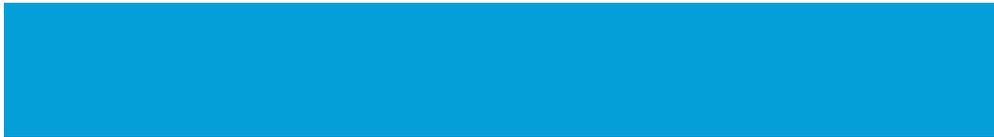
Étape 4.1. Créez le deuxième groupe pour l'utilisateur ReadOnly.



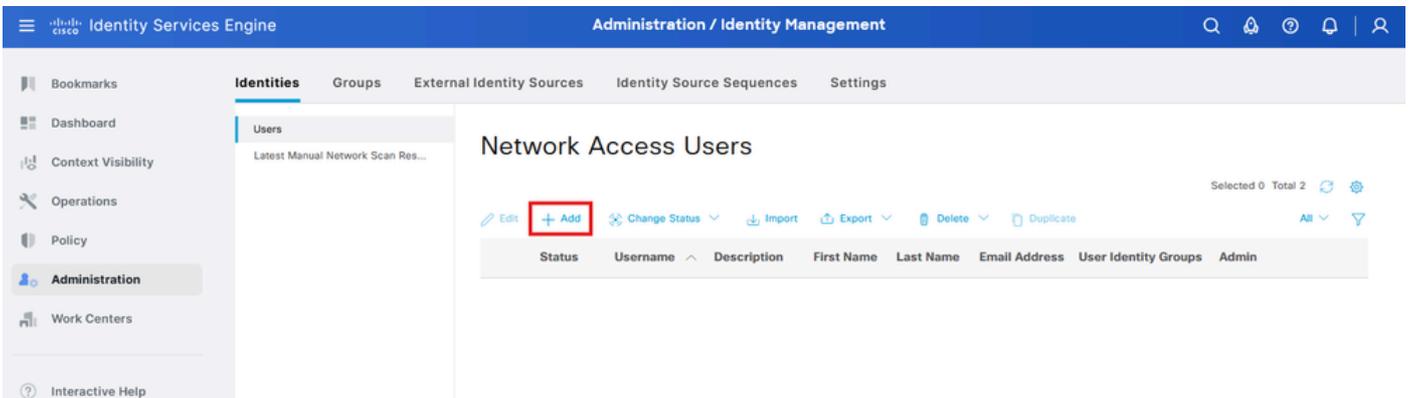
Étape 4.2. Validez que les deux groupes sont affichés dans la liste des groupes d'identité d'utilisateur. Utilisez le filtre pour les trouver facilement.



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.

Identity Services Engine Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users [Network Access Users List >](#)

Latest Manual Network Scan Res...

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 ←

Enable Password ←

Generate Password ⓘ

Generate Password ⓘ

> User Information

> Account Options

> Account Disable Policy

User Groups

Firepower Admins ← ⓘ ⓘ

Save Reset

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

Identity Services Engine Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Network Access Users List >

Latest Manual Network Scan Res...

Network Access User

* Username **firewall_readuser**

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration

Never Expires

Password Re-Enter Password

* Login Password

Enable Password

Generate Password

Generate Password

> User Information

> Account Options

> Account Disable Policy

User Groups

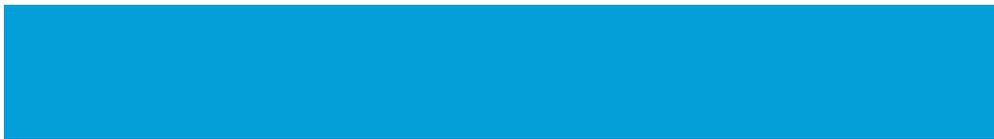
Firepower ReadOnly

Save Reset

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.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a new authorization profile. The page title is "Policy / Policy Elements". The left sidebar shows the navigation menu with "Policy" selected. The main content area is titled "Authorization Profile" and shows the configuration for a new profile named "FMC_GUI_Admin". The "Description" is "Administrator Access FMC Web Interface" and the "Access Type" is "ACCESS_ACCEPT". The "Advanced Attributes Settings" section shows a rule for "Radius:Class" with a value of "Administrator". The "Submit" button is highlighted with a red box.

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.

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy**
- Administration
- Work Centers
- Interactive Help

- Authentication
- Authorization
- Downloadable ACLs
- Profiling
- Posture
- Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: ←

Description:

* Access Type: ←

Network Device Profile: Cisco

Service Template:

Track Movement:

Agentless Posture:

Passive Identity Tracking:

> Common Tasks

Advanced Attributes Settings

Radius:Class ← * ReadUser ←

Attributes Details

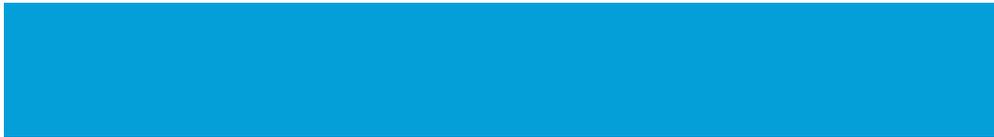
Access Type = ACCESS_ACCEPT
Class = ReadUser



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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Profile. The page is titled "Policy / Policy Elements" and is in the "Results" tab. The left sidebar shows the navigation menu with "Policy" selected. The main content area is titled "Authorization Profile" and shows the configuration for the profile named "FTD_CLI_Admin".

Key configuration details include:

- Name:** FTD_CLI_Admin (indicated by a red arrow)
- Description:** Administrator Access FTD Command Line Interface
- Access Type:** ACCESS_ACCEPT (indicated by a red arrow)
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:** (with a refresh icon)
- Agentless Posture:** (with a refresh icon)
- Passive Identity Tracking:** (with a refresh icon)

Under the "Advanced Attributes Settings" section, there is a list of attributes. One attribute is highlighted with a red arrow: "Radius:Service-Type" with a value of "Administrative".

Under the "Attributes Details" section, the following values are displayed:

```
Access Type = ACCESS_ACCEPT
Service-Type = 6
```

At the bottom right, there is a "Save" button (highlighted with a red box) and a "Reset" button.

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.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a policy. The main content area is titled "Authorization Profile" and shows the following configuration details:

- Name:** FTD_CLI_RO
- Description:** Read Only Access FTD Command Line Interface
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**
- Agentless Posture:**
- Passive Identity Tracking:**

Under the "Advanced Attributes Settings" section, the following attributes are listed:

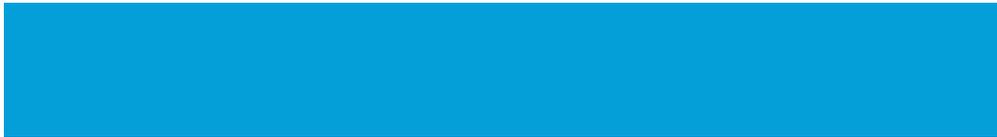
- Radius:Service-Type
- NAS Prompt

At the bottom right of the configuration area, a "Save" button is highlighted with a red box, and a "Reset" button is visible next to it.

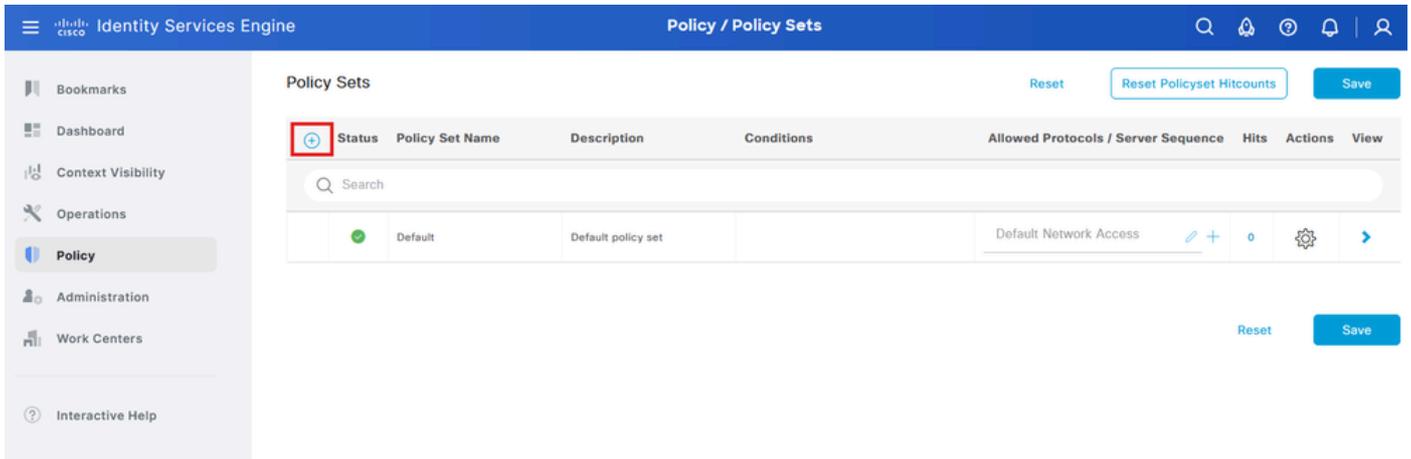
Ajouter un nouvel ensemble de stratégies

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.

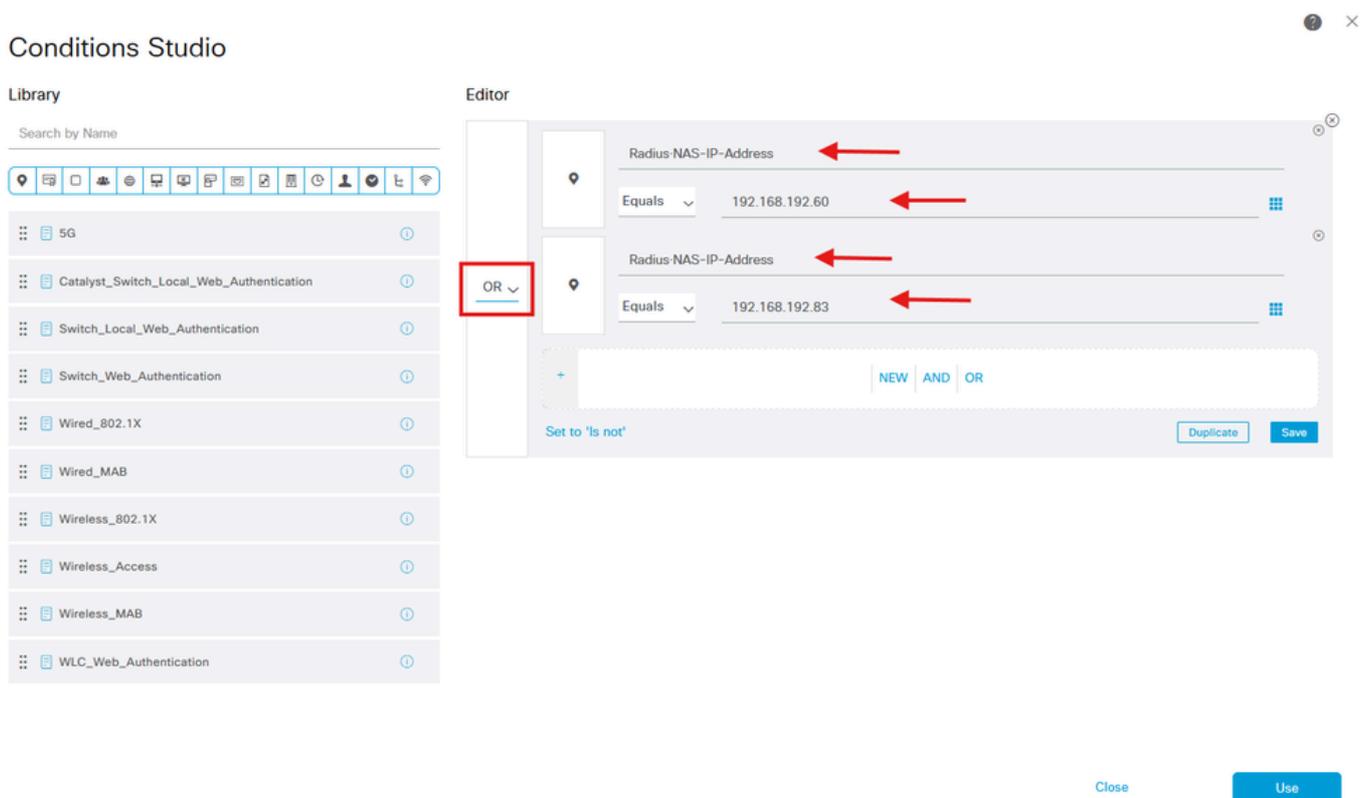


Étape 8.1. Une nouvelle ligne est placée en haut de vos ensembles de stratégies.

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.



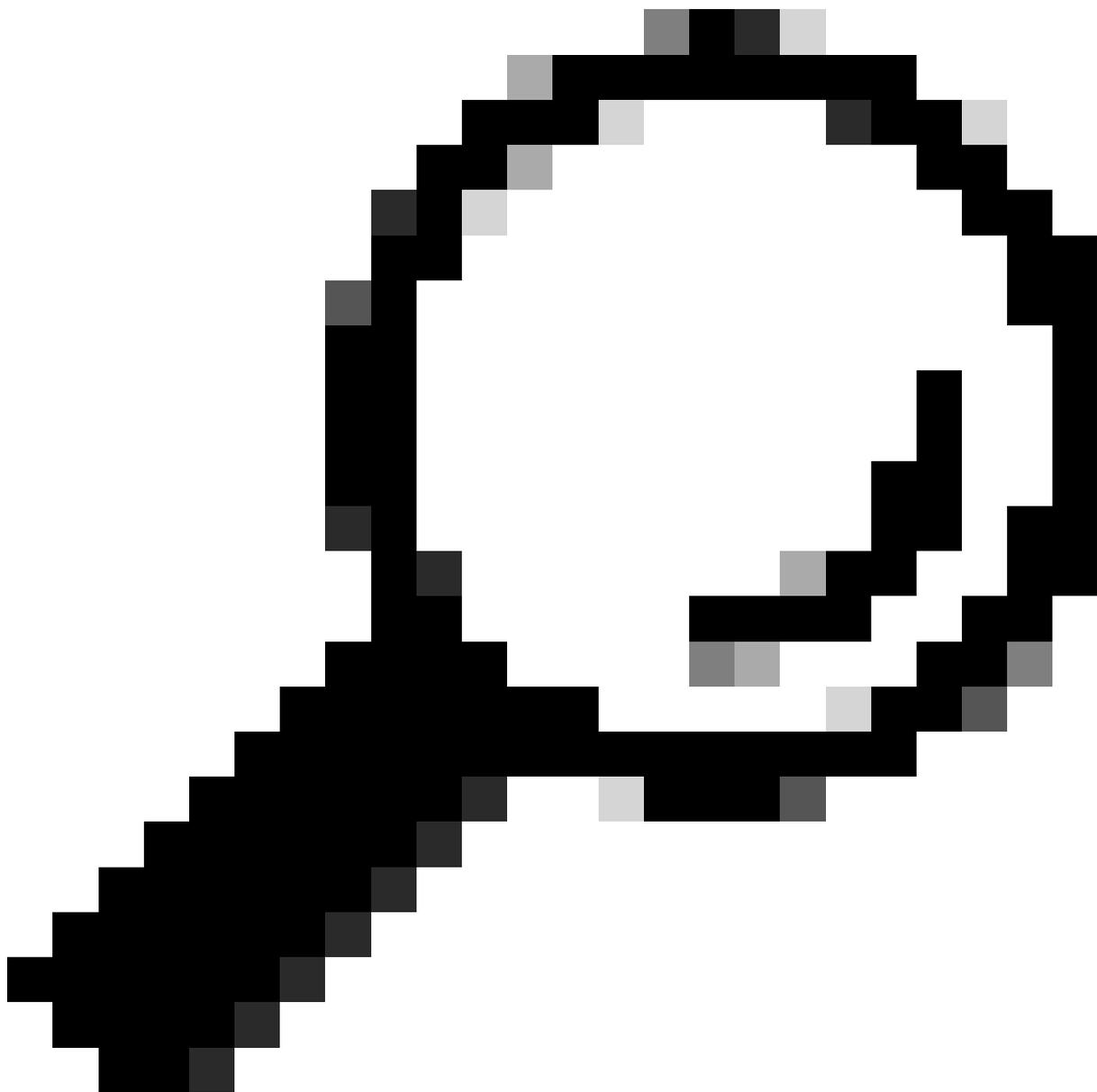
Étape 8.2. Une fois terminé, appuyez sur Enregistrer.

Identity Services Engine Policy / Policy Sets

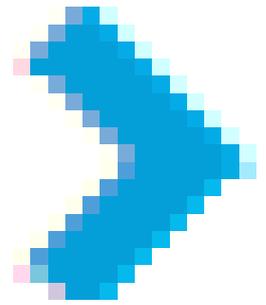
Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	FMC and FTD Access	Management Access	OR • Radius-NAS-IP-Address EQUALS 192.168.192.60 • Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access ⊗ +		⚙️	➔
●	Default	Default policy set		Default Network Access ✎ +	0	⚙️	➔

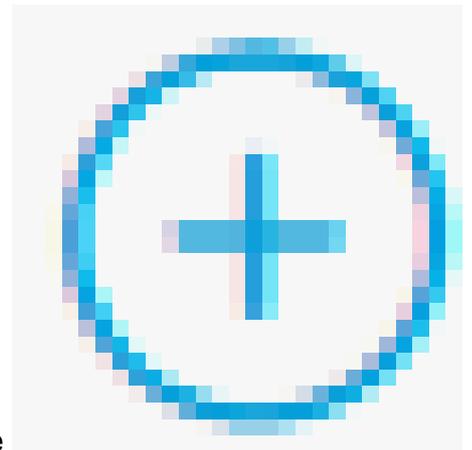
Reset Save



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.

Conditions Studio



Library

Search by Name



- 5G
- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Auth entication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN

Editor

IdentityGroup-Name

Equals User Identity Groups:Firepower Admins

Set to 'Is not'

Duplicate Save

NEW AND OR

Close



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.

Conditions Studio



Library

Search by Name



- 5G
- BYOD_Is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed
- Non_Cisco_Profiled_Phones
- Non_Compliant_Devices

Editor

IdentityGroup-Name

Equals User Identity Groups:Firepower
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.

Identity Services Engine Policy / Policy Sets

Policy Sets → FMC and FTD Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 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	Profiles	Security Groups	Hits	Actions
●	FMC and FTD Read Access	IdentityGroup-Name EQUALS User Identity Groups:Firepower ReadOnly	FMC_GUI_ReadOnly FTD_CLI_RO	Select from list	0	⚙️
●	FMC and FTD Admin Access	IdentityGroup-Name EQUALS User Identity Groups:Firepower Admins	FMC_GUI_Admin FTD_CLI_Admin	Select from list	0	⚙️
●	Default		DenyAccess	Select from list	0	⚙️

Reset **Save**

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.

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 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.

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

External Authentication Object

Authentication Method: RADIUS

Name: ISE-RADIUS-FMC

Description: RADIUS Auth for FMC

Primary Server

Host Name/IP Address: 192.168.192.90

Port: 1812

RADIUS Secret Key: [Redacted]

Backup Server (Optional)

Host Name/IP Address: [Empty]

Port: 1812

RADIUS Secret Key: [Empty]

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.

RADIUS-Specific Parameters

Timeout (Seconds): 30

Retries: 3

Access Admin: [Empty]

Administrator: Class=Administrator

Discovery Admin: [Empty]

External Database User: [Empty]

Intrusion Admin: [Empty]

Maintenance User: [Empty]

Network Admin: [Empty]

Security Analyst: [Empty]

Security Analyst (Read Only): Class=ReadUser

Security Approver: [Empty]

Threat Intelligence Director (TID) User: [Empty]

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

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.

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

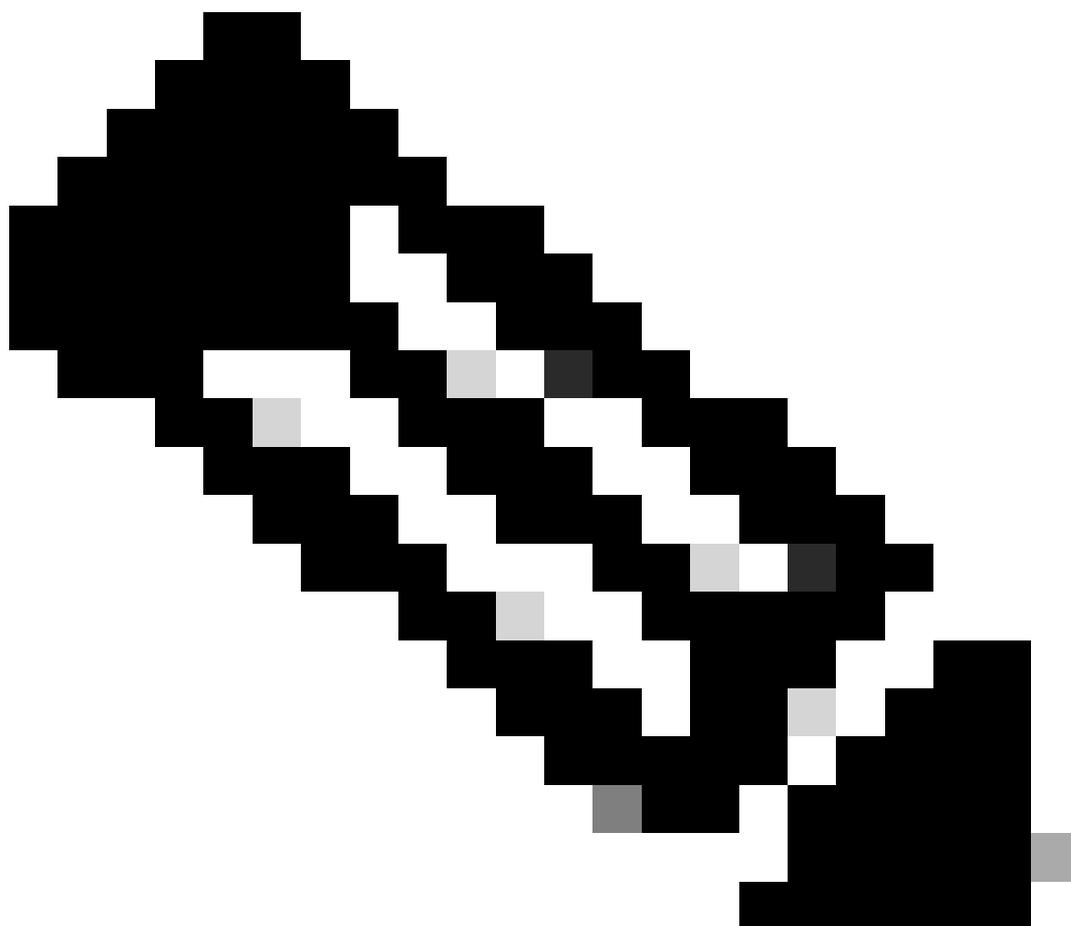
Password

*Required Field

Cancel

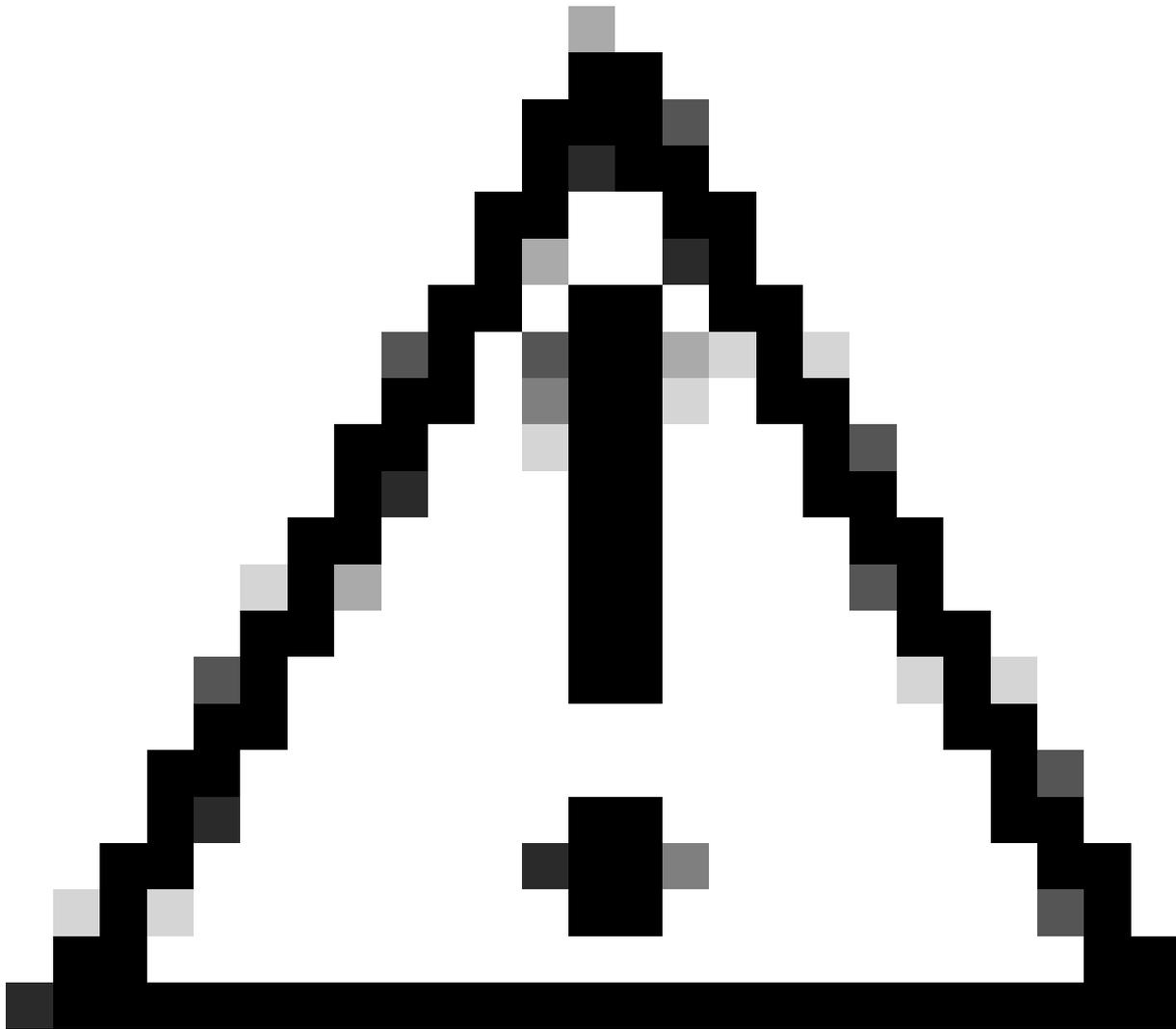
Test

Save



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.

Save Cancel Save and Apply

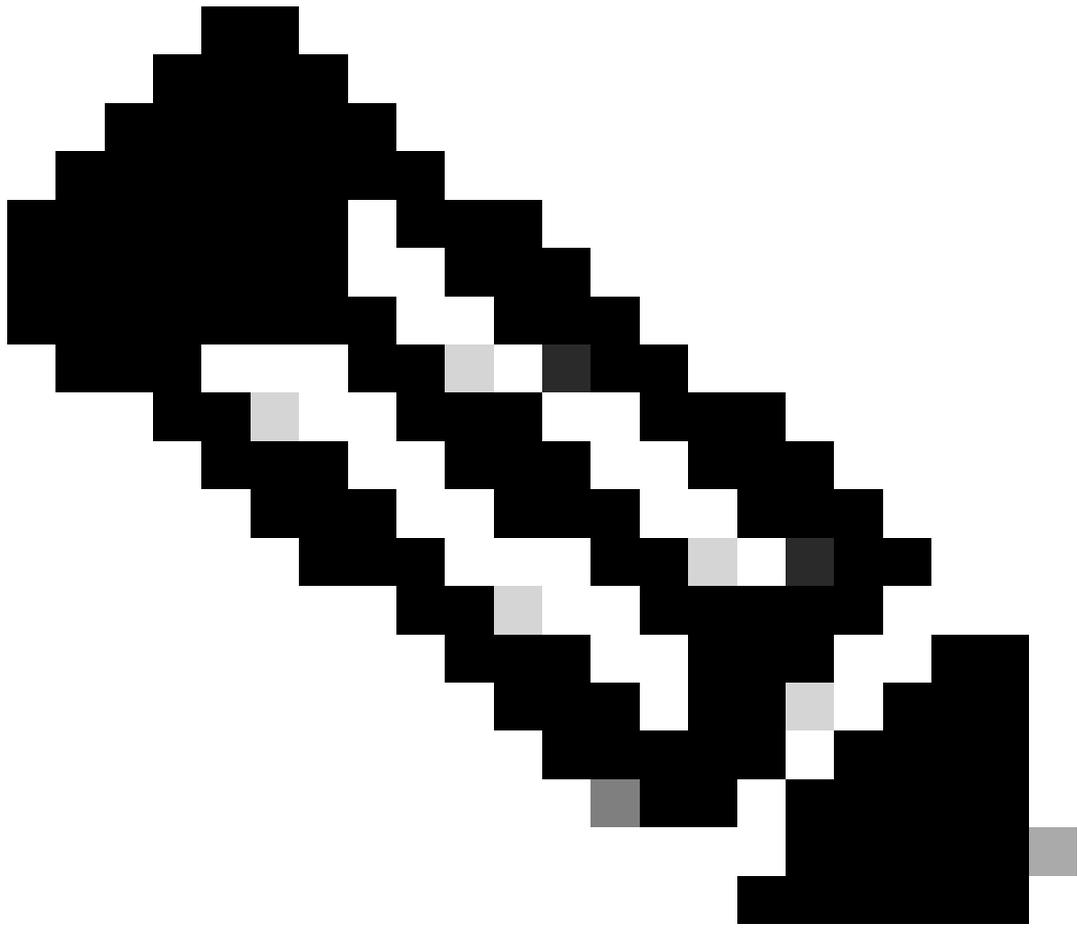
Default User Role: Administrator Shell Authentication Enabled (ISE-RADIUS-FMC)

+ Add External Authentication Object

Name	Method	Enabled	
1. ISE-RADIUS-FMC RADIUS Auth for FMC	RADIUS	<input checked="" type="checkbox"/>	 

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.

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: Administrator Shell Authentication: Enabled (ISE-RADIUS-FMC)

Save Cancel Save and Apply

+ Add External Authentication Object

Name	Method	Enabled
1. ISE-RADIUS-FMC RADIUS Auth for FMC	RADIUS	Enabled

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)

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-FTD

Description: RADIUS Auth for FTD CLI

Primary Server

Host Name/IP Address: 192.168.192.90

Port: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address:

Port: 1812

RADIUS Secret Key:

RADIUS-Specific Parameters

Timeout (Seconds): 30

Retries: 3

Access Admin:



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, veuillez 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.

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🟢 ⚙️ ? admin ▾ CISCO SECURE

FTD Policy
Enter Description

You have unsaved changes **Save** Cancel

2

Policy Assignments (1)

Manage External Authentication Server

Name	Description	Method	Server:Port	Encryption	Enabled
ISE-RADIUS-FMC	RADIUS Auth for FMC	RADIUS	192.168.192.90:1812	no	<input type="checkbox"/>
ISE-RADIUS-FTD	RADIUS Auth for FTD CLI	RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

1

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

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 🟢 ⚙️ ? admin ▾ CISCO SECURE

FTD Policy
Enter Description

Policy Assignments (1)

Manage External Authentication Server

Name	Description	Method	Server:Port	Encryption	Enabled
ISE-RADIUS-FTD	RADIUS Auth for FTD CLI	RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>
ISE-RADIUS-FMC	RADIUS Auth for FMC	RADIUS	192.168.192.90:1812	no	<input type="checkbox"/>

Policy Assignments

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

698354673
Group
FTD2140-HA
vFTD_192.168.192.83

Selected Devices

vFTD_192.168.192.83

Cancel OK

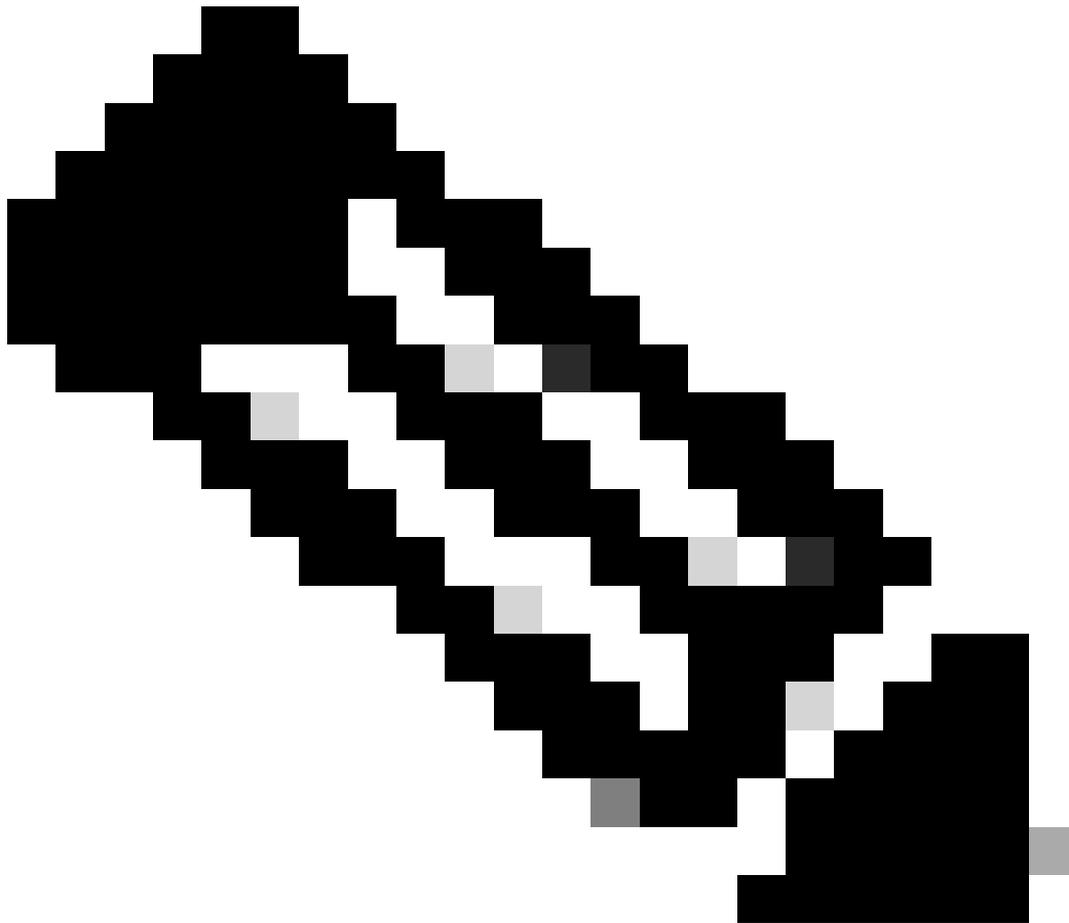
Étape 3 : déploiement des modifications

Devices Objects Integration **Deploy** 🔍 🟢 ⚙️ ? admin ▾ CISCO SECURE

Advanced Deploy Ignore warnings **Deploy** Cancel

vFTD_192.168.192.83 Ready for Deployment

Assignments (1)



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.

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

Cancel Test **Save**

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

Firewall Management Center
Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ ? admin ▾

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

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

Cancel Test **Save**

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

- Bookmarks
- Dashboard
- Context Visibility
- Operations**
- Policy
- Administration
- Work Centers

Live Logs Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat

Refresh: Never | Show: Latest 20 records | Within: Last 3

[Reset Repeat Counts](#) [Export To](#)

[Filter](#)

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...
Jun 07, 2025 11:45:38.9...	●		2	firewall_admin	10.24.184.31	Endpoint Pr	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.