

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

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration](#)

[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](#)

[Vérification](#)

[Test de connexion interdomaine](#)

[Tests internes FMC](#)

[Journaux en direct ISE](#)

[Informations connexes](#)

---

## Introduction

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

## Conditions préalables

### Exigences

Il est recommandé de connaître les sujets suivants :

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

## Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

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

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

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

## Configuration

### Configuration ISE

Ajouter vos périphériques réseau

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

The screenshot shows the 'Network Devices' section of the Cisco Identity Services Engine. The top navigation bar includes 'Administration / Network Resources'. The left sidebar has 'Administration' selected. The main table header includes columns for Name, IP/Mask, Profile Name, Location, Type, and Description. A toolbar at the top provides options like Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete.

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.

This screenshot shows the configuration of a new network device. The 'Name' field is set to 'fmc\_10.225.86.50'. Under 'Device Profile', 'Cisco' is selected. The 'Device Type' is set to 'FMC'. The 'RADIUS Authentication Settings' checkbox is checked. The 'Protocol' is set to 'RADIUS' and the 'Shared Secret' field contains a shared secret key.

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

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

The screenshot shows the 'Groups' section of the Administration / Identity Management interface. The 'User Identity Groups' section is displayed. The 'Add' button in the toolbar is highlighted with a red box.

Étape 4. Attribuez un nom à chaque groupe et enregistrez-le individuellement. Dans cet exemple, vous créez un groupe pour les utilisateurs Administrateur. Créez deux groupes : Group\_Retail\_A et Group\_Finance\_B.

The screenshot shows the 'Groups' tab selected in the navigation bar. A new identity group is being created under 'User Identity Groups'. The 'Name' field contains 'Group\_Retail\_A' and the 'Description' field contains 'Cisco FMC Domain Retail-A'. The 'Save' button is visible at the bottom right.

The screenshot shows the 'Groups' tab selected in the navigation bar. A new identity group is being created under 'User Identity Groups'. The 'Name' field contains 'Group\_Finance\_B' and the 'Description' field contains 'Cisco FMC Domain Finance-B'. The 'Save' button is visible at the bottom right.

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

The screenshot shows the 'Identities' tab selected in the navigation bar. The 'Network Access Users' section is displayed. The '+ Add' button is highlighted with a red box. The table headers include Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin.

Étape 5.1. Commencez par créer l'utilisateur avec des droits d'administrateur. Attribuez-lui un nom admin\_retail, un mot de passe et le groupe Group\_Retail\_A.

Identity Services Engine Administration / Identity Management

**Identities**

Bookmarks	Groups	External Identity Sources	Identity Source Sequences	Settings
-----------	--------	---------------------------	---------------------------	----------

\* Username: admin\_retail

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	.....

**User Information**

**Account Options**

**Account Disable Policy**

**User Groups**

Group\_Retail\_A

Étape 5.2. Commencez par créer l'utilisateur avec des droits d'administrateur. Attribuez un nom à admin\_financial, password et au groupe Group\_Finance\_B.

Identity Services Engine Administration / Identity Management

**Identities**

Bookmarks	Groups	External Identity Sources	Identity Source Sequences	Settings
-----------	--------	---------------------------	---------------------------	----------

\* Username: admin\_financial

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	.....

**User Information**

**Account Options**

**Account Disable Policy**

**User Groups**

Group\_Finance\_B

## Créer les profils d'autorisation

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

The screenshot shows the Cisco Identity Services Engine interface. The top navigation bar includes 'Identity Services Engine', 'Policy / Policy Elements', and search/filter icons. On the left, a sidebar lists 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy' (which is selected), 'Administration', 'Work Centers', and 'Interactive Help'. The main content area is titled 'Standard Authorization Profiles' and displays a table with columns 'Name', 'Profile', and 'Description'. At the top of the table, there are buttons for 'Edit', '+ Add' (which is highlighted with a red box), 'Duplicate', and 'Delete'. The status bar at the bottom right shows 'Selected 0 Total 26'.

Définissez un nom pour le profil d'autorisation, laissez le type d'accès ACCESS\_ACCEPT.

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

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



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

The screenshot shows the configuration of an Authorization Profile named 'FMC\_GUI\_Retail'. The profile details include:

- Name:** FMC\_GUI\_Retail
- Description:** (empty)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (checkbox)
- Track Movement:** (checkbox)
- Agentless Posture:** (checkbox)
- Passive Identity Tracking:** (checkbox)

Below the profile details, there are sections for 'Common Tasks' and 'Advanced Attributes Settings'. Under 'Attributes Details', it shows:  
Access Type = ACCESS\_ACCEPT  
Class = RETAIL\_ADMIN\_STR

Étape 6.2. Financement par profil : Sous Advanced Attributes Settings, ajoutez Radius : Class avec la valeur FINANCE\_ADMIN\_STR.



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

The screenshot shows the 'Policy / Policy Elements' section of the Cisco Identity Services Engine. On the left, there's a navigation bar with links like Bookmarks, Dashboard, Context Visibility, Operations, Policy (which is selected), Administration, and Work Centers. The main area is titled 'Authorization Profiles > FMC\_GUI\_Finance'. It shows an 'Authorization Profile' with a name 'FMC\_GUI\_Finance' and an 'Access Type' set to 'ACCESS\_ACCEPT'. Under 'Network Device Profile', it says 'Cisco'. There are sections for 'Service Template', 'Track Movement', 'Agentless Posture', and 'Passive Identity Tracking', each with a checkbox and a help icon. Below these are 'Common Tasks' and 'Advanced Attributes Settings'. At the bottom, under 'Attributes Details', it shows 'Access Type = ACCESS\_ACCEPT' and 'Class = FINANCE\_ADMINISTRATOR'.

## Ajouter un nouvel ensemble de stratégies

Étape 7 : création d'un ensemble de stratégies correspondant à l'adresse IP FMC Cela permet d'empêcher d'autres périphériques d'accorder l'accès aux utilisateurs. Accédez à Policy > Policy Sets > icône de signe Plus placée dans l'angle supérieur gauche.

The screenshot shows the 'Policy / Policy Sets' section. The left sidebar includes links for Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, and Work Centers. The main area displays a table of 'Policy Sets' with columns for Status, Policy Set Name, Description, and Conditions. A search bar is at the top of the table. To the right of the table are buttons for Reset, Save, and a link to 'Reset Policyset Hitcounts'. A red box highlights the 'Add' button (a plus sign icon) in the top right corner of the table header.

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

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

The screenshot shows the 'Conditions Studio' interface. On the left, there's a 'Library' with various condition icons. The main area is the 'Editor' where a condition is being defined. The condition 'Radius-NAS-IP-Address' is set to 'Equals' with the value '10.225.86.50'. Below this, there's an option 'Set to "Is not"' and buttons for 'Duplicate' and 'Save'. At the bottom of the editor, there are buttons for 'NEW', 'AND', and 'OR'.

## Étape 8.2. Une fois terminé, appuyez sur Save.

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

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

The screenshot shows the 'Policy / Policy Sets' section of the Cisco Identity Services Engine. On the left, there's a navigation bar with links like Bookmarks, Dashboard, Context Visibility, Operations, Policy (which is selected), Administration, Work Centers, and Interactive Help. The main area displays a table for 'Policy Sets'. One row is visible: 'FMC Domain Login' with a status of 'OK', a condition 'Radius-NAS-IP-Address EQUALS 10.225.86.50', and an action 'Default Network Access'. At the bottom right of this row, there's a red box around a small square icon with a plus sign, which is the 'More' or 'Edit' icon.

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

- Règle 1 : Si Groupe d'identités utilisateur est égal à Groupe\_Détail\_A, affectez le profil Détail.
- Règle 2 : Si Groupe d'identités d'utilisateur est égal à Group\_Finance\_B, affectez le financement de profil.

The screenshot shows the 'Policy / Policy Sets' page with the 'FMC Domain Login' rule expanded. Under the 'Conditions' section, there are three entries under 'Authorization Policy': 'Authentication Policy (1)', 'Authorization Policy - Local Exceptions', and 'Authorization Policy - Global Exceptions (1)'. Below this, the 'Results' section shows three rules:

- 'Finance Domain' with profile 'FMC\_GUI\_Finance' and security group 'Select from list'.
- 'Retail Domain' with profile 'FMC\_GUI\_Retail' and security group 'Select from list'.
- 'Default' with profile 'DenyAccess' and security group 'Select from list'.

A red box highlights the 'Save' button at the bottom right of the page.

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

## Configuration FMC

Ajouter votre serveur RADIUS ISE pour l'authentification FMC

## Étape 1. Établir la structure du domaine :

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

Firewall Management Center  
System / Domains

Overview Analysis Policies Devices Objects Integration Deploy Global \ admin SECURE

Domain configuration is up to date. Save Cancel Add Domain

Name	Description	Devices
Global		
Finance-B		
Retail-A		 1 Device*

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

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



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

Firewall Management Center  
System / Domains

Overview Analysis Policies Devices Objects Integration Deploy Global \ admin SECURE

Domain configuration is up to date

Filter domains

Global

Finance-B

Retail-A

User Preferences

Theme Light Dusk Classic

Log Out

Last login from 10.227.192.57 on 2026-02-11 02:17:27

External Authentication Object

Authentication Method: RADIUS

Name: ISE-RADIUS-FMC

Description: RADIUS Auth for FMC

**Primary Server**

Host Name/IP Address: 10.197.243.183  
ex. IP or hostname

Port: 1812

RADIUS Secret Key: \*\*\*\*

**Backup Server (Optional)**

Host Name/IP Address:

Port: 1812  
ex. IP or hostname

RADIUS Secret Key:

**RADIUS-Specific Parameters**

Timeout (Seconds): 30

Retries: 3

Access Admin:

Administrator: Class=RETAIL\_ADMIN\_STR

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

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



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

Firewall Management Center

System / Domains

Overview Analysis Policies Devices Objects Integration Deploy

Domain configuration is u

Name	Description
Global	
Finance-B	
Retail-A	

Filter domains

Global

Finance-B

Retail-A

User Preferences

Theme: Light

Last login from 10.227.192.57 on 2026-02-11 02:17:27

Firewall Management Center  
System / Users / Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ Finance-B \ admin SECURE

Users User Roles External Authentication

**External Authentication Object**

Authentication Method: RADIUS  
Name: ISE-RADIUS-FMC  
Description: RADIUS Auth for FMC

**Primary Server**  
Host Name/IP Address: 10.197.243.183  
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:  
Administrator: Class=FINANCE\_ADMIN\_STR

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

## Vérification

### Test de connexion interdomaine

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



Conseil : Lorsque vous vous connectez à un domaine spécifique, utilisez le format nom\_utilisateur nom\_domaine\radius\_utilisateur\_mappé\_avec\_ce\_domaine.

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

Firewall Management Center  
Overview / Dashboards / Dashboard

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ Retail-A \ admin\_retail SECURE

Summary Dashboard (switch\_dashboard)  
Provides a summary of activity on the appliance

Network Threats Intrusion Events Status Geolocation QoS Zero Trust +

Unique Applications over Time  
Top Web Applications Seen  
Top Client Applications Seen

Last updated 3 minutes ago

Filter domains  
Global  
Retail-A  
User Preferences  
Theme: Light, Dusk, Classic  
Log Out  
Last login from 10.110.212.51 on 2026-02-11 10:03:51

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

## Tests internes FMC

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

Additional Test Parameters

User Name	admin_financial
Password	*****

Test Output

Show Details ▾

```

check_auth_radius: szUser: admin_financial
RADIUS config file: /var/tmp/roCPmVujOv/radiusclient_0.conf
radiusauth - response: |User-Name=admin_financial|
radiusauth - response: |Class=FINANCE_ADMIN_STR|
User Test
radiusauth - response: |Class=CACS:0ac5f3b7m0vFormvHHyC_lgO13NsO1DZN6QciDbrc0cwlaYWHMto:eagle/556377151/553|
"admin_financial" RADIUS Authentication OK
check_is_radius_member attrib match found: |Class=FINANCE_ADMIN_STR| ~ |Class=FINANCE_ADMIN_STR| *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:

```

\*Required Field

Cancel Test Save

## Journaux en direct ISE

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

Time	Status	Details	Repeat...	Identity	Endpoint ID	Endpoint...	Authentica...	Authorization Policy	Authorization Profiles	IP Address
Feb 11, 2026 10:10:43.2...	Success	0	0	admin_financial	FMC Domain ...	FMC Domain Login >> Finance Domain		FMC_GUI_Finance		
Feb 11, 2026 10:09:38.3...	Success	0	0	admin_financial	FMC Domain ...	FMC Domain Login >> Finance Domain		FMC_GUI_Finance		
Feb 11, 2026 10:08:12.9...	Success	0	0	admin_retail	FMC Domain ...	FMC Domain Login >> Retail Domain		FMC_GUI_Retail		

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

## Overview

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

## Authentication Details

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

## Result

Class	FINANCE_ADMIN_STR
Class	CACS:0ac5f3b7m0vFomvHHyC_igO13NsO1DZN6QciDbrc0cwl aYWHMto:eagle/556377151/553

## Informations connexes

[Configurer l'authentification externe FMC et FTD avec ISE en tant que serveur RADIUS](#)

## À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.