

Configuración de la Autenticación Externa FMC en el Entorno de Varios Dominios

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración](#)

[Configuración de ISE](#)

[Agregue sus dispositivos de red](#)

[Crear los grupos de identidad de usuarios locales y los usuarios](#)

[Crear los perfiles de autorización](#)

[Agregar un nuevo conjunto de políticas](#)

[Configuración de FMC](#)

[Agregue su servidor RADIUS de ISE para la autenticación FMC](#)

[Verificación](#)

[Prueba de conexión entre dominios](#)

[Pruebas internas de FMC](#)

[registros en vivo de ISE](#)

[Información Relacionada](#)

Introducción

Este documento describe la implementación de varios arrendatarios (multidominio) dentro de Cisco FMC al tiempo que aprovecha Cisco ISE para la autenticación RADIUS centralizada.

Prerequisites

Requirements

Se recomienda tener conocimiento de estos temas:

- Configuración inicial de Cisco Secure Firewall Management Center a través de la GUI o el shell.
- Privilegios de administrador completos en el dominio global de FMC para crear subdominios y objetos de autenticación externos.
- Configuración de políticas de autenticación y autorización en ISE.
- Conocimiento básico de RADIUS

Componentes Utilizados

- Cisco Secure FMC: vFMC 7.4.2 (o posterior recomendado para la estabilidad multidominio)
- Estructura de dominio: Jerarquía de tres niveles (Global > Subdominios de segundo nivel).
- Cisco Identity Services Engine: ISE 3.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En entornos empresariales a gran escala o en escenarios de proveedores de servicios de seguridad gestionados (MSSP), a menudo es necesario segmentar la administración de la red en distintos límites administrativos. Este documento describe cómo configurar el FMC para admitir múltiples dominios, específicamente para un ejemplo real donde un MSSP administra dos clientes: Retail-A y Finance-B. Al utilizar la autenticación RADIUS externa a través de Cisco ISE, los administradores pueden garantizar que los usuarios reciban acceso automáticamente solo a sus respectivos dominios de usuario en función de sus credenciales centralizadas.

El sistema Cisco Secure Firewall utiliza dominios para implementar varios arrendatarios.

- Jerarquía de dominio: La jerarquía comienza en el dominio global. Puede crear hasta 100 subdominios en una estructura de dos o tres niveles.
- Dominios de hoja: Estos son dominios en la parte inferior de la jerarquía sin más subdominios. Y lo que es más importante, cada dispositivo FTD gestionado debe asociarse exactamente a un dominio de hoja.
- Atributo de clase RADIUS (atributo 25): En una configuración de varios dominios, FMC utiliza el atributo de clase RADIUS devuelto por ISE para asignar un usuario autenticado a un dominio y una función de usuario específicos. Esto permite que un único servidor RADIUS asigne usuarios dinámicamente a diferentes segmentos de usuario (por ejemplo, Retail-A frente a Finance-B) al iniciar sesión.

Configuración

Configuración de ISE

Agregue sus dispositivos de red

Paso 1. Navegue hasta Administración > Recursos de red > Dispositivos de red > Agregar.

The screenshot shows the 'Network Devices' section of the Cisco Identity Services Engine. The top navigation bar includes 'Administration / Network Resources'. On the left, there's a sidebar with links like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (which is selected), and Work Centers. The main area has a table header with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. A red box highlights the '+ Add' button in the toolbar above the table.

Paso 2. Asigne un nombre al objeto del dispositivo de red e inserte la dirección IP del CSP.

Marque la casilla de verificación RADIUS y defina un secreto compartido. La misma clave debe utilizarse más adelante para configurar el FMC. Una vez hecho esto, haga clic en Guardar.

The screenshot shows the 'Network Device' creation form. The 'Name' field is filled with 'fmc_10.225.86.50'. The 'Description' field is empty. Below it, the 'IP Address' field contains '10.225.86.50' with a subnet mask of '32'. The 'Device Profile' dropdown is set to 'Cisco'. Other fields include 'Model Name', 'Software Version', 'Network Device Group', 'Location' (set to 'All Locations'), 'IPSEC' (set to 'No'), and 'Device Type' (set to 'FMC'). Under 'RADIUS Authentication Settings', the 'Protocol' is set to 'RADIUS' and the 'Shared Secret' field is populated with a shared secret. A red box highlights the 'RADIUS UDP Settings' section.

Crear los grupos de identidad de usuarios locales y los usuarios

Paso 3. Cree los grupos de identidad de usuario necesarios. Vaya a Administration > Identity Management > Groups > User Identity Groups > Add.

The screenshot shows the 'User Identity Groups' section of the Cisco Identity Services Engine. The top navigation bar includes 'Administration / Identity Management'. On the left, there's a sidebar with links like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main area has a table header with columns: Name and Description. A red box highlights the '+ Add' button in the toolbar above the table.

Paso 4. Dé a cada grupo un nombre y Guardar individualmente. En este ejemplo, está creando un grupo para usuarios de Administrator. Cree dos grupos: Group_Retail_A y Group_Finance_B.

The screenshot shows the 'Groups' tab selected in the navigation bar. On the left sidebar, 'Administration' is highlighted. The main panel displays the 'Identity Groups' section under 'User Identity Groups'. A new group is being created with the name 'Group_Retail_A' and a description 'Cisco FMC Domain Retail-A'. The 'Save' button is visible at the bottom right.

This screenshot shows the continuation of step 4, where a new group 'Group_Finance_B' is being created. The name is 'Group_Finance_B' and the description is 'Cisco FMC Domain Finance-B'. The 'Save' button is visible at the bottom right.

Paso 5. Cree los usuarios locales y agréguelos a su grupo correspondiente. Vaya a Administration > Identity Management > Identities > Add.

The screenshot shows the 'Identities' tab selected in the navigation bar. On the left sidebar, 'Administration' is highlighted. The main panel displays the 'Network Access Users' section. The '+ Add' button is highlighted with a red box. The top right corner shows a status message 'Selected 0 Total 5016' and filter options.

Paso 5.1. Cree primero el usuario con derechos de administrador. Asigne un nombre al grupo admin_retail, password y el grupo 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: Never Expires

Password: Login Password: Re-Enter Password: Generate Password

Enable Password: Generate Password

User Information

Account Options

Account Disable Policy

User Groups

Group_Retail_A

Paso 5.2. Cree primero el usuario con derechos de administrador. Asigne un nombre al grupo admin_finance, password y al grupo Group_Finance_B.

Identity Services Engine Administration / Identity Management

Identities

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

* Username: admin_finance

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime: Never Expires

Password: Login Password: Re-Enter Password: Generate Password

Enable Password: Generate Password

User Information

Account Options

Account Disable Policy

User Groups

Group_Finance_B

Crear los perfiles de autorización

Paso 6. Cree el perfil de autorización para el usuario administrador de la interfaz web de FMC. Vaya a Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización > Agregar.

The screenshot shows the Cisco Identity Services Engine interface. The top navigation bar includes 'Identity Services Engine' and 'Policy / Policy Elements'. The left sidebar has links for 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 contains a table with columns for Name, Profile, and Description. At the top of the table are buttons for Edit, + Add (highlighted with a red box), Duplicate, and Delete. A status bar at the bottom right says 'Selected 0 Total 26'.

Defina un nombre para el perfil de autorización, deje Tipo de acceso como ACCESS_ACCEPT.

En Configuración de atributos avanzados, agregue un Radius > Class—[25] con el valor y haga clic en Enviar.

Paso 6.1. Venta al por menor del perfil: En Advanced Attributes Settings, agregue Radius:Class con el valor RETAIL_ADMIN_STR.



Consejo: Aquí RETAIL_ADMIN_STR puede ser cualquier cosa; asegúrese de que las necesidades con el mismo valor se incluyen también en el lado del CSP.

The screenshot shows the 'Authorization Profile' configuration page for 'FMC_GUI_Retail'. It includes fields for Name (FMC_GUI_Retail), Description, Access Type (set to ACCESS_ACCEPT), Network Device Profile (Cisco), Service Template, Track Movement, Agentless Posture, and Passive Identity Tracking. Below these are sections for Common Tasks and Advanced Attributes Settings. The 'Attributes Details' section at the bottom shows 'Access Type = ACCESS_ACCEPT' and 'Class = RETAIL_ADMIN_STR'.

Paso 6.2. Perfil de financiación: En Advanced Attributes Settings, agregue Radius:Class con el valor FINANCE_ADMIN_STR.



Consejo: Aquí FINANCE_ADMIN_STR puede ser cualquier cosa; asegúrese de que también se asigna el mismo valor al lado del CSP.

The screenshot shows the 'Policy / Policy Elements' section under the 'Policy' tab. A new 'Authorization Profile' is being created with the name 'FMC_GUI_Finance'. The 'Access Type' is set to 'ACCESS_ACCEPT'. Under 'Network Device Profile', 'Cisco' is selected. In the 'Attributes Details' section, it shows 'Access Type = ACCESS_ACCEPT' and 'Class = FINANCE_ADMINISTRATOR'. There are also sections for 'Common Tasks' and 'Advanced Attributes Settings'.

Agregar un nuevo conjunto de políticas

Paso 7. Crear un conjunto de políticas que coincida con la dirección IP del CSP. Esto es para evitar que otros dispositivos concedan acceso a los usuarios. Vaya a Policy > Policy Sets > Plus sign icon situado en la esquina superior izquierda.

The screenshot shows the 'Policy / Policy Sets' section under the 'Policy' tab. A new policy set is being created. The 'Status' field has a plus sign icon highlighted with a red box. The 'Policy Set Name' field is empty. The 'Description' and 'Conditions' fields are also present. At the top right, there are buttons for 'Reset', 'Save', and 'Reset Policyset Hitcounts'.

Paso 8.1. Se coloca una nueva línea en la parte superior de los conjuntos de políticas.

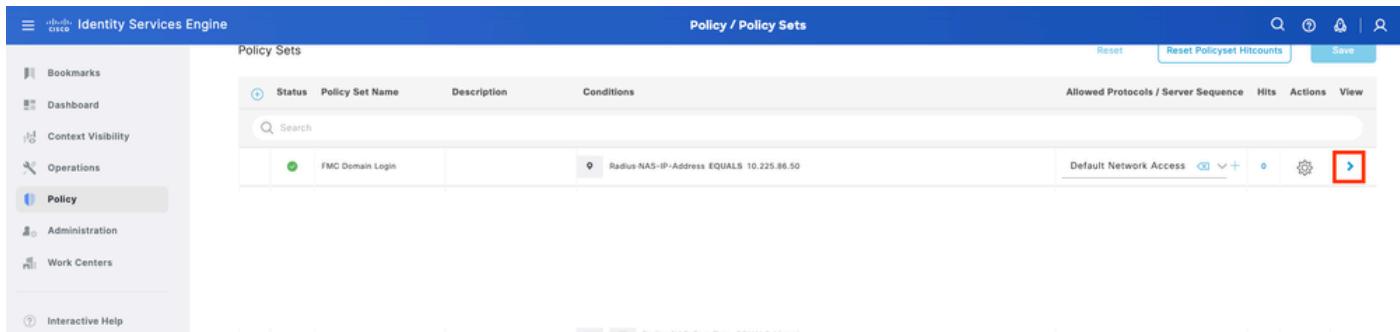
Dé un nombre a la nueva política y agregue una condición superior para el atributo RADIUS NAS-IP-Address que coincide con la dirección IP de FMC. Haga clic en Utilizar para mantener los cambios y salir del editor.

The screenshot shows the 'Conditions Studio' interface. A condition for 'Radius-NAS-IP-Address' is being created with the operator 'Equals' and the value '10.225.86.50'. The 'Set to "Is not"' option is also visible. The 'Editor' pane shows the condition being built, and the 'View' pane on the right shows the current conditions for the policy set.

Paso 8.2. Una vez completado, presione Guardar.

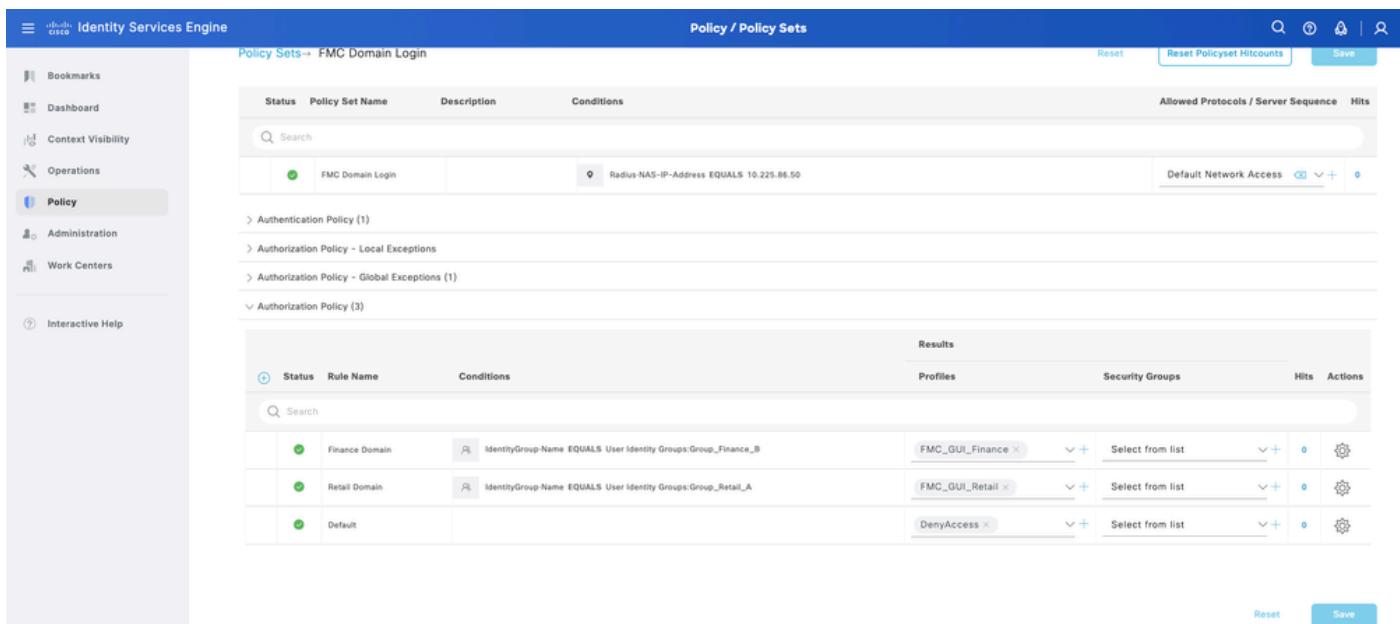
Paso 9. Consulte el nuevo juego de políticas pulsando el icono juego situado al final de la fila.

Expanda el menú Authorization Policy y presione el icono Plus sign para agregar una nueva regla que permita el acceso al usuario con derechos de administrador. Dale un nombre.



Establezca las condiciones para hacer coincidir el Grupo de Identidad de Diccionario con Nombre de Atributo Igual a y elija Grupos de Identidad de Usuario. En Directiva de autorización, cree reglas:

- Regla 1: Si el grupo de identidad de usuario es igual a Group_Retail_A, asigne el perfil Retail.
- Regla 2: Si el grupo de identidad de usuario es igual a Group_Finance_B, asigne Profile Finance.



Paso 10. Establezca los perfiles de autorización para cada regla y haga clic en Guardar.

Configuración de FMC

Agregue su servidor RADIUS de ISE para la autenticación FMC

Paso 1. Establecer la estructura de dominio:

- Inicie sesión en el dominio global de FMC.

- Vaya a Administration > Domains.
- Haga clic en Agregar dominio para crear Retail-A y Finance-B como subdominios de Global.

Firewall Management Center
System / Domains

Overview Analysis Policies Devices Objects Integration Deploy Global \ admin SECURE

Domain configuration is up to date.

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

Paso 2.1. Configure el Objeto de Autenticación Externa en Dominio a Retail-A

- Cambie el dominio a Retail-A.
- Vaya a System > Users > External Authentication.
- Seleccione Add External Authentication Object y elija RADIUS.
- Introduzca la dirección IP de ISE y la clave secreta compartida configuradas anteriormente.
- Ingrese RADIUS-Specific Parameters > Administrator > class=RETAIL_ADMIN_STR



Consejo: Utilice el mismo valor de clase que el configurado en Perfiles de autorización de ISE.

Firewall Management Center
System / Domains

Overview Analysis Policies Devices Objects Integration Deploy Global \ admin SECURE

Domain configuration is up to date.

Name	Description
Global	
Finance-B	
Retail-A	

Filter domains

Global
Finance-B
Retail-A

User Preferences
Theme: Light Dusk Classic
Log Out

Last login from 10.227.192.57 on 2020-02-11 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

Paso 2.2. Configure el Objeto de Autenticación Externa en Dominio para Finance-B

- Cambie el dominio a Finance-B.
- Vaya a System > Users > External Authentication.
- Seleccione Add External Authentication Object y elija RADIUS.
- Introduzca la dirección IP de ISE y la clave secreta compartida configuradas anteriormente.
- Ingrese RADIUS-Specific Parameters > Administrator > class=FINANCE_ADMIN_STR



Consejo: Utilice el mismo valor de clase que el configurado en Perfiles de autorización de ISE.

Name	Description
Global	
Finance-B	
Retail-A	

Domain configuration is used by 0 objects

Filter domains

Global

Finance-B

Retail-A

User Preferences

Theme: Light, Dusk, Classic

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

Log Out

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

Paso 3. Activar autenticación: Habilite el objeto y establézcalo como el método de autenticación de shell. Haga clic en Guardar y Aplicar.

Verificación

Prueba de conexión entre dominios

- Intente iniciar sesión en la interfaz web de FMC con admin_retail. Verifique que el Dominio actual que se muestra en la parte superior derecha de la interfaz de usuario sea Retail-A.



Consejo: Al iniciar sesión en un dominio específico, utilice el formato de nombre de usuario domain_name\radius_user_appended_with_that_domain.

Por ejemplo, si el usuario administrador de Retail necesita iniciar sesión, el nombre de usuario debe ser Retail-A\admin_retail y la contraseña correspondiente.

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

Log Out

Last login from 10.110.212.21 on 2026-02-11 10:03:51

- Cierre sesión e inicie sesión como admin_financial. Compruebe que el usuario está restringido al dominio Finance-B y que no puede ver los dispositivos Retail-A.

Pruebas internas de FMC

Vaya a los parámetros del servidor RADIUS en el FMC. Utilice la sección Parámetros de Prueba Adicionales para ingresar un nombre de usuario y contraseña de prueba. Una prueba correcta debe mostrar un mensaje de confirmación de color verde.

Additional Test Parameters

User Name: admin_financial
Password: *****

Test Output

```
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

registros en vivo de ISE

- En Cisco ISE, vaya a Operations > RADIUS > Live Logs.

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

- Confirme que las solicitudes de autenticación muestren un estado Pass y que se haya enviado el perfil de autorización correcto (y la cadena de clase asociada) en el paquete de aceptación de acceso RADIUS.

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

Información Relacionada

Configuración de la autenticación externa FMC y FTD con ISE como servidor RADIUS

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).