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

Contenido

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.

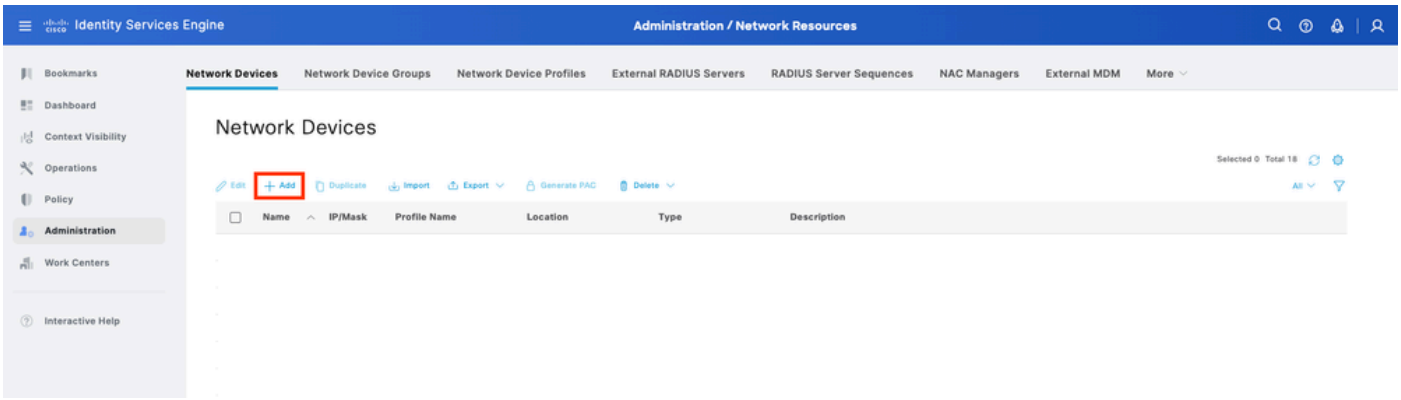
- Jerarquía de dominio: La jerarquía comienza en el dominio global. Puede crear hasta 100 subdominios en una estructura de dos o tres niveles.
- Dominios de hoja: Estos son dominios en la parte inferior de la jerarquía sin más subdominios. Y lo que es más importante, cada dispositivo FTD gestionado debe 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

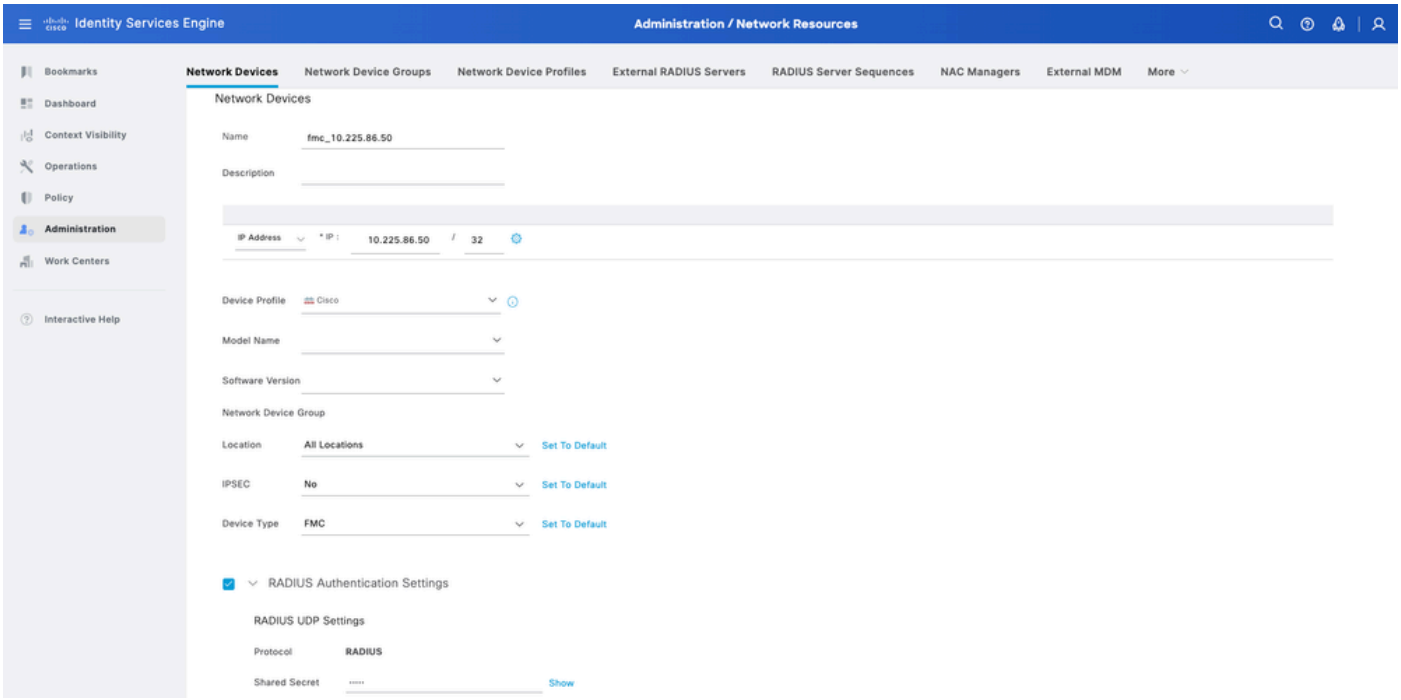
Agregue sus dispositivos de red

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



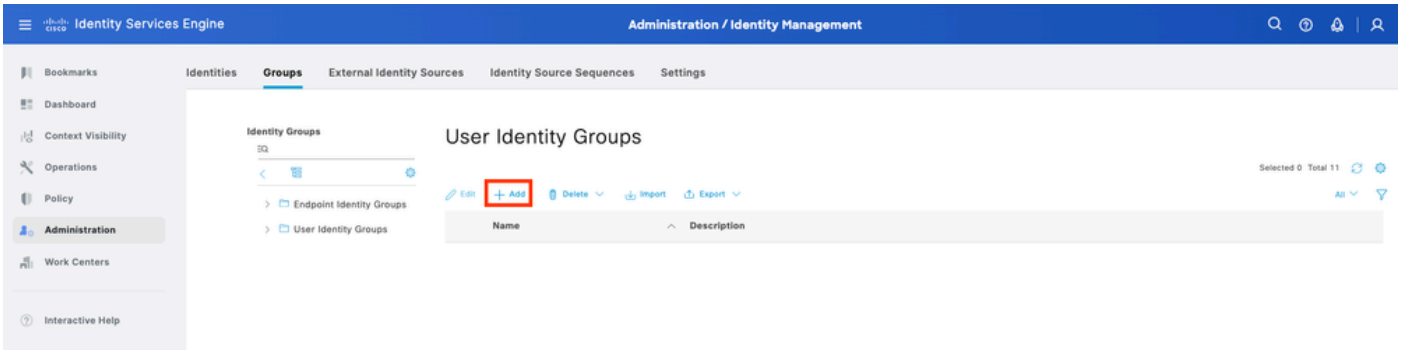
Paso 2. Asigne un nombre al objeto del dispositivo de red e inserte la dirección IP del CSP.

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.

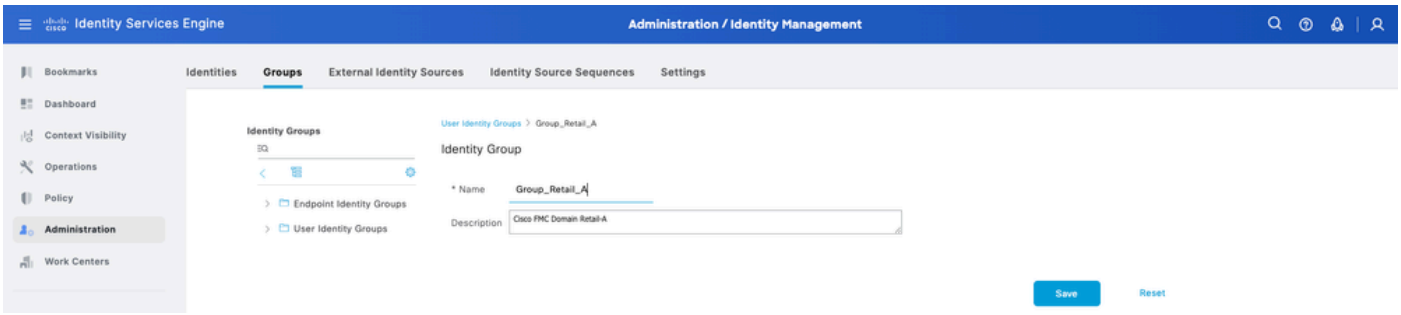


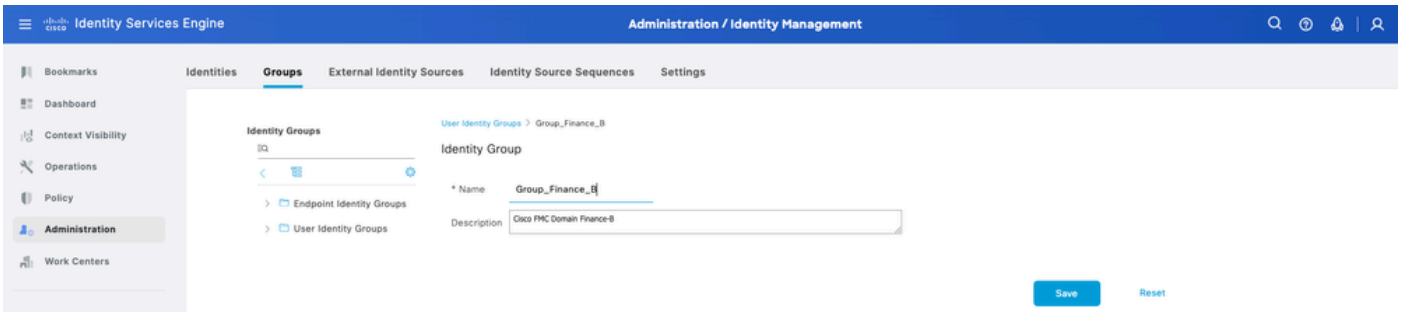
Crear los grupos de identidad de usuarios locales y los usuarios

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

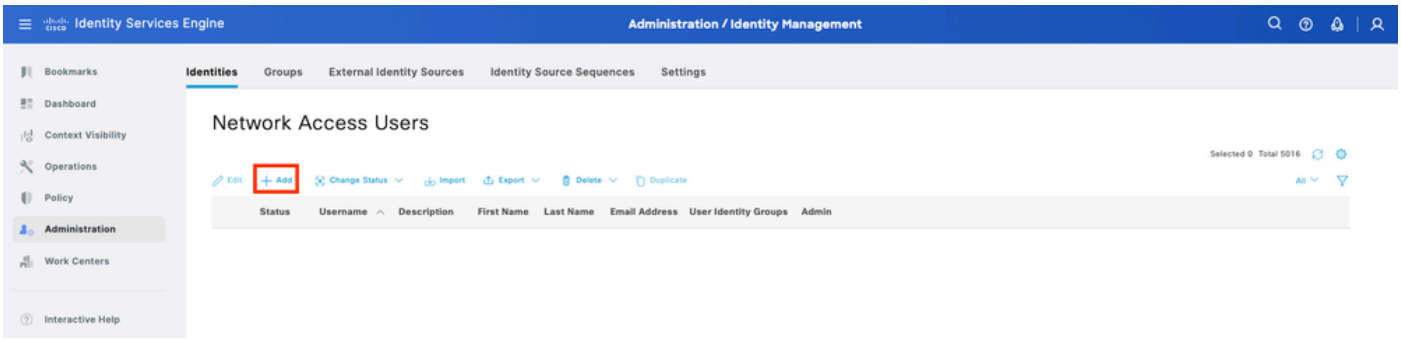


Paso 4. Dé a cada grupo un nombre y Guardar individualmente. En este ejemplo, está creando un grupo para usuarios de Administrator. Cree dos grupos: Group_Retail_A y Group_Finance_B.

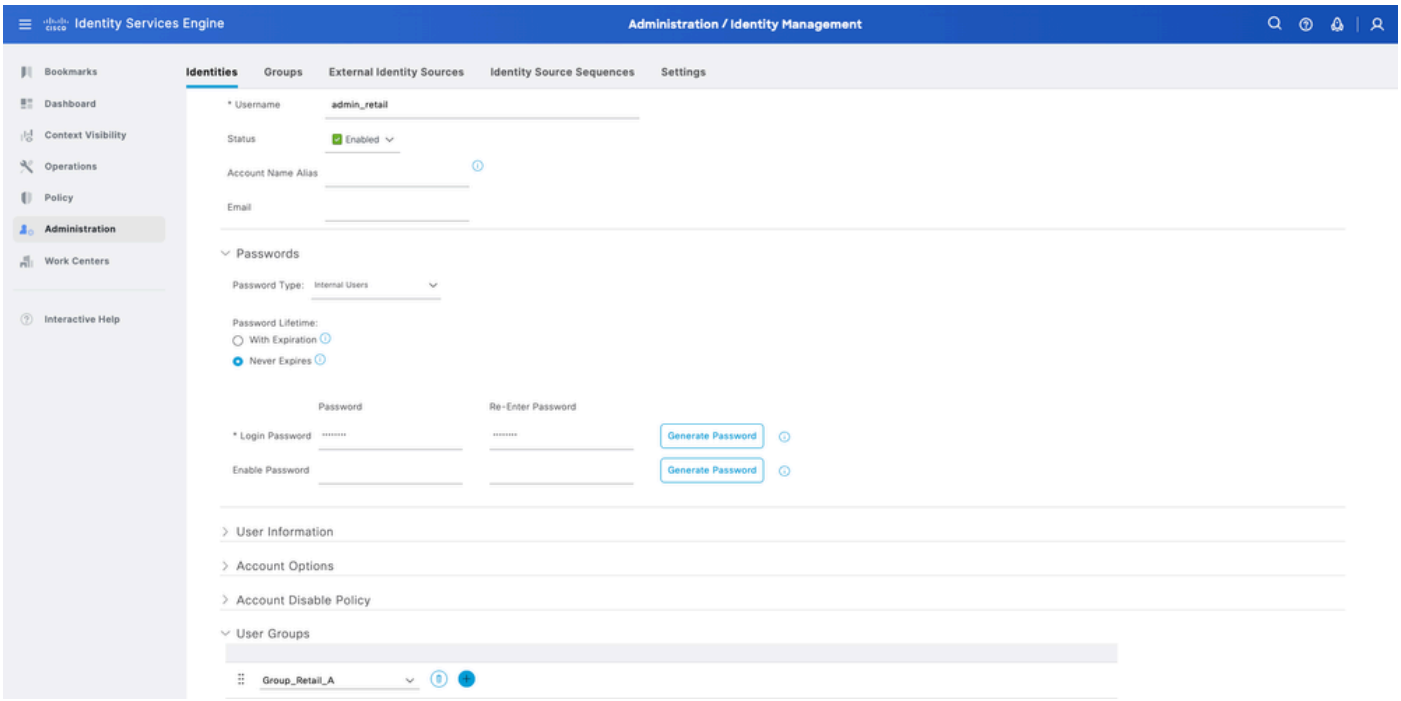




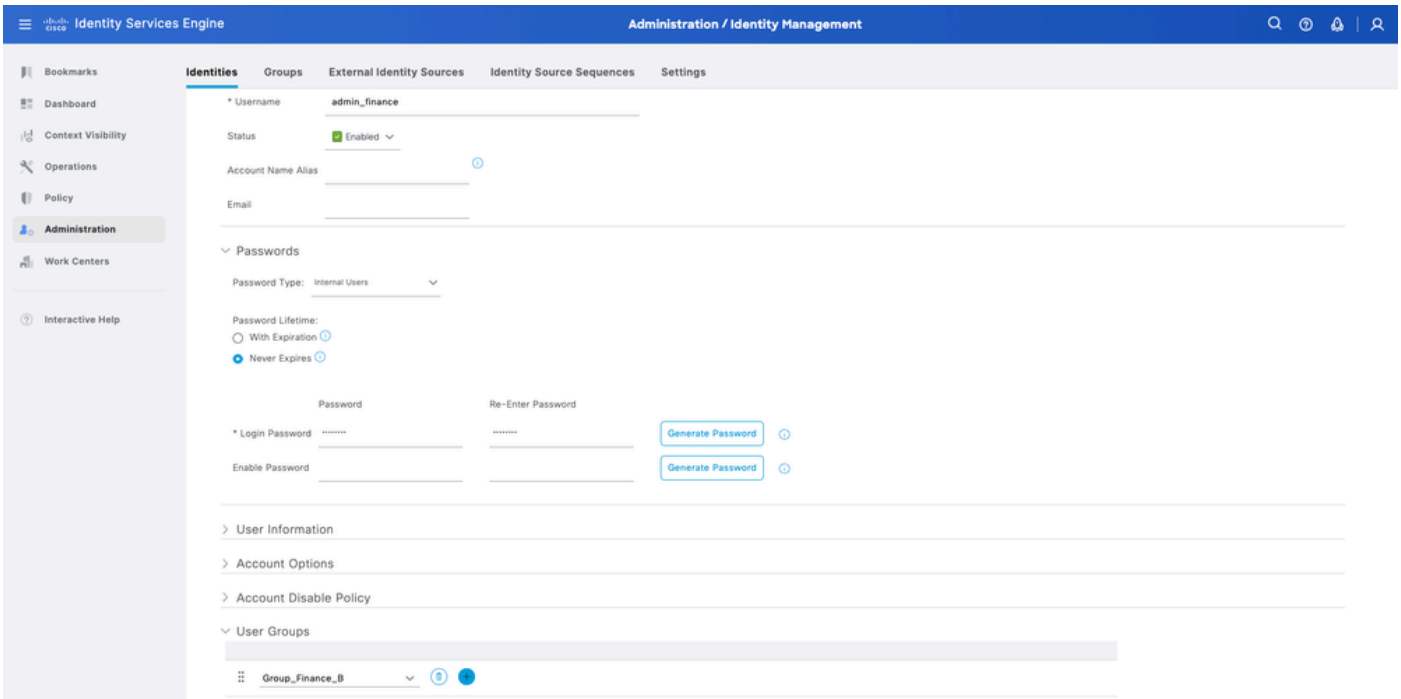
Paso 5. Cree los usuarios locales y agréguelos a su grupo correspondiente. Vaya a Administration > Identity Management > Identities > Add.



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.

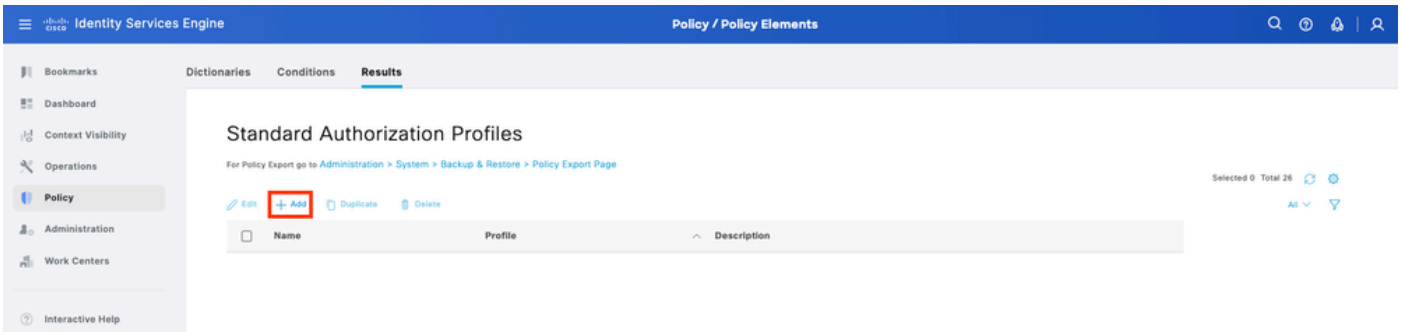


Paso 5.2. Cree primero el usuario con derechos de administrador. Asigne un nombre al grupo admin_finance, password y al grupo Group_Finance_B.



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.

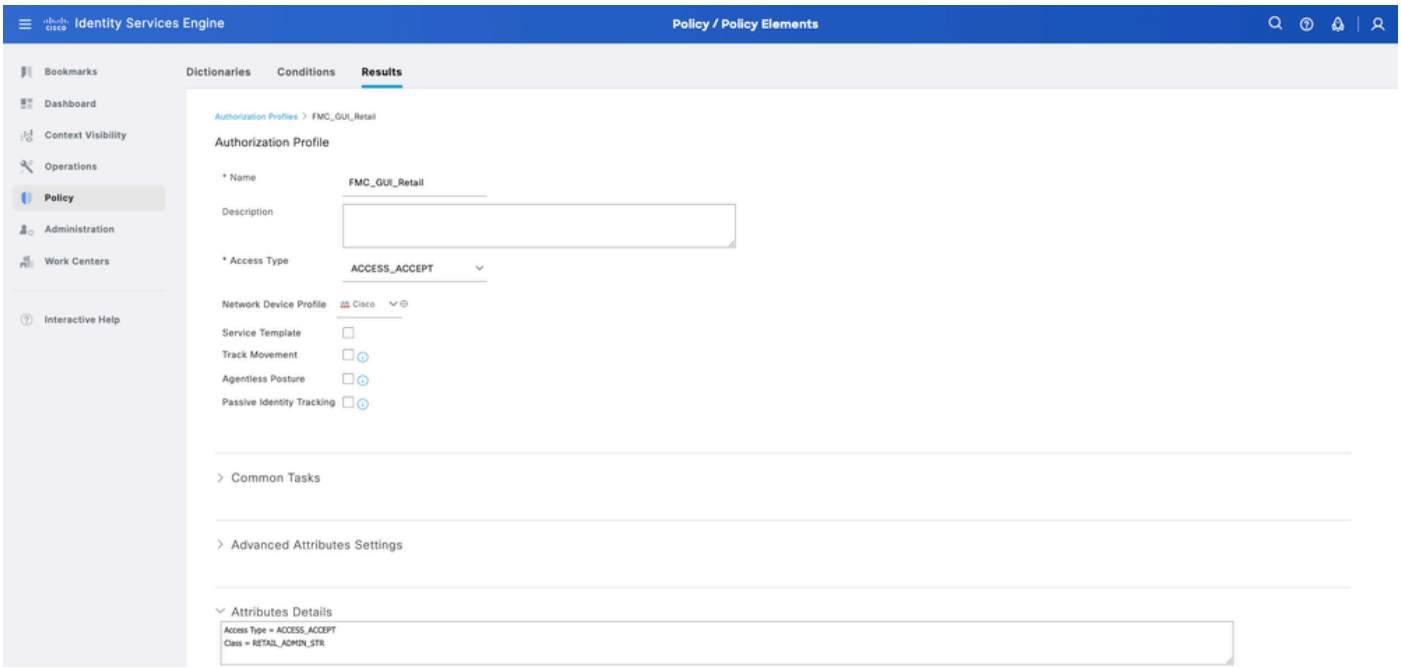


Defina un nombre para el perfil de autorización, deje Tipo de acceso como ACCESS_ACCEPT.

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

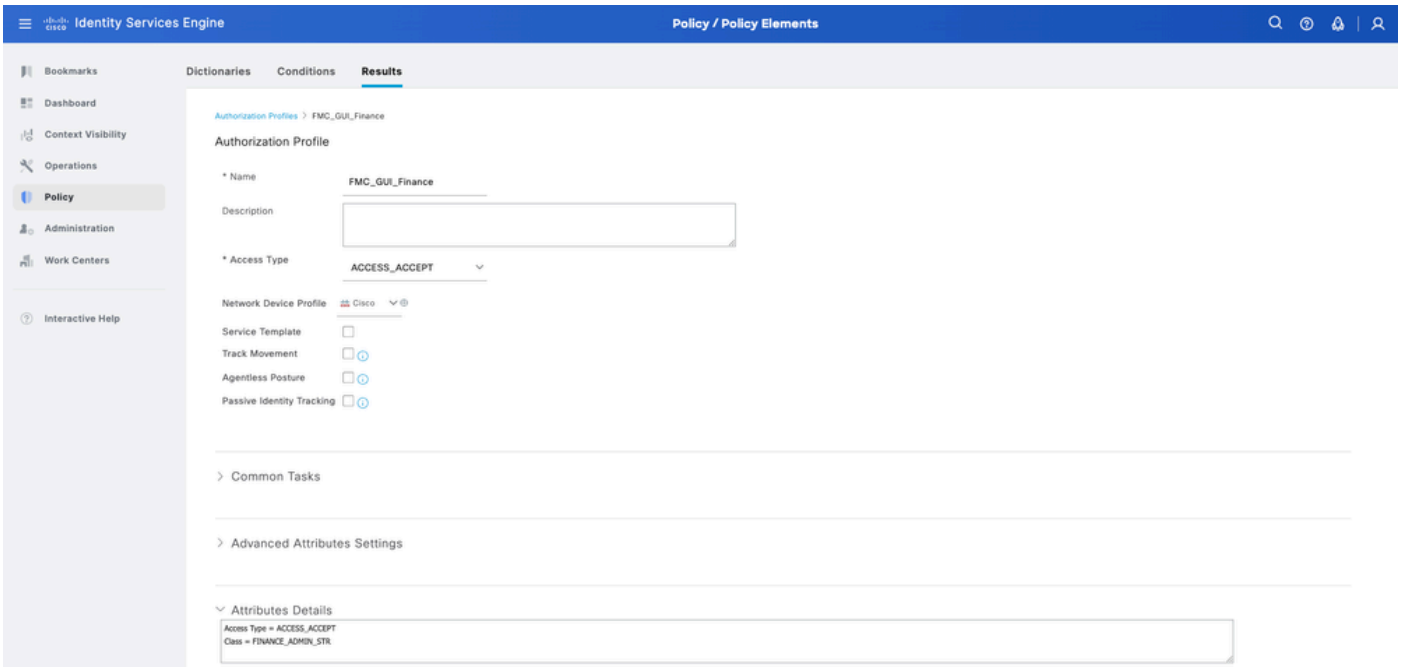
Paso 6.1. Venta al por menor del perfil: En Advanced Attributes Settings, agregue Radius:Class con el valor RETAIL_ADMIN_STR.

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.



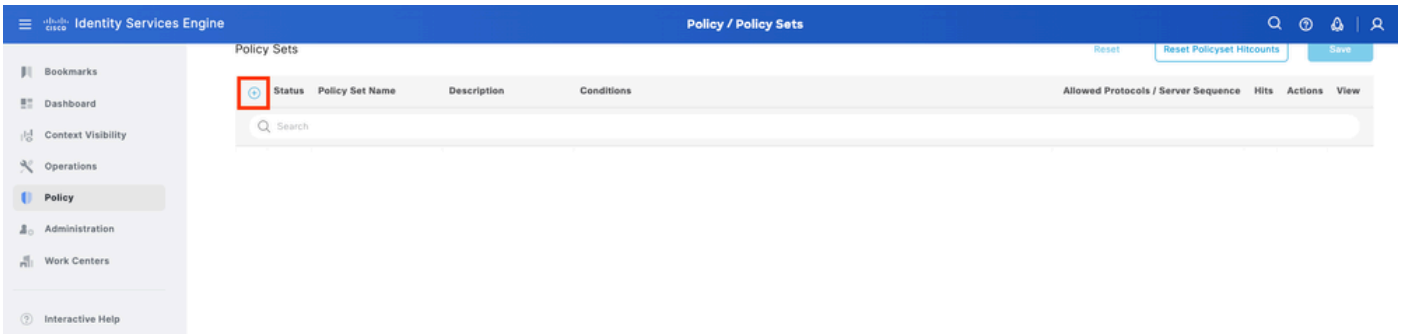
Paso 6.2. Perfil de financiación: En Advanced Attributes Settings, agregue Radius:Class con el valor FINANCE_ADMIN_STR.

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



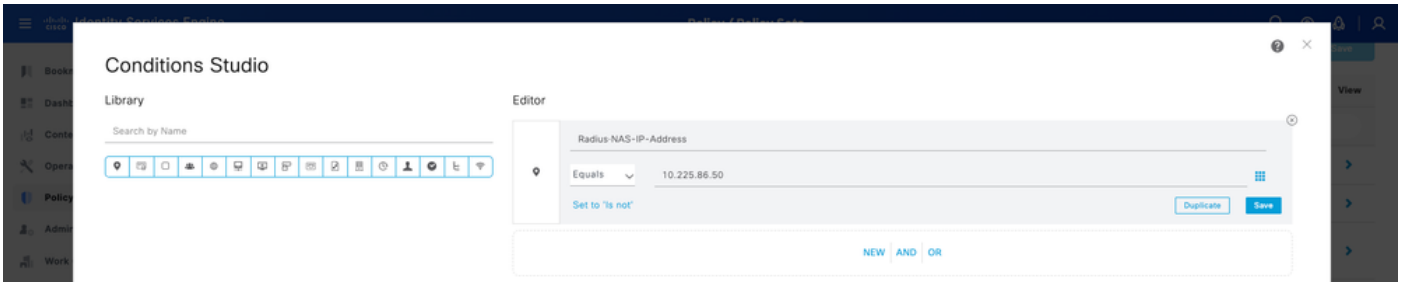
Agregar un nuevo conjunto de políticas

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.



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 coincida con la dirección IP de FMC. Haga clic en Utilizar para mantener los cambios y salir del editor.



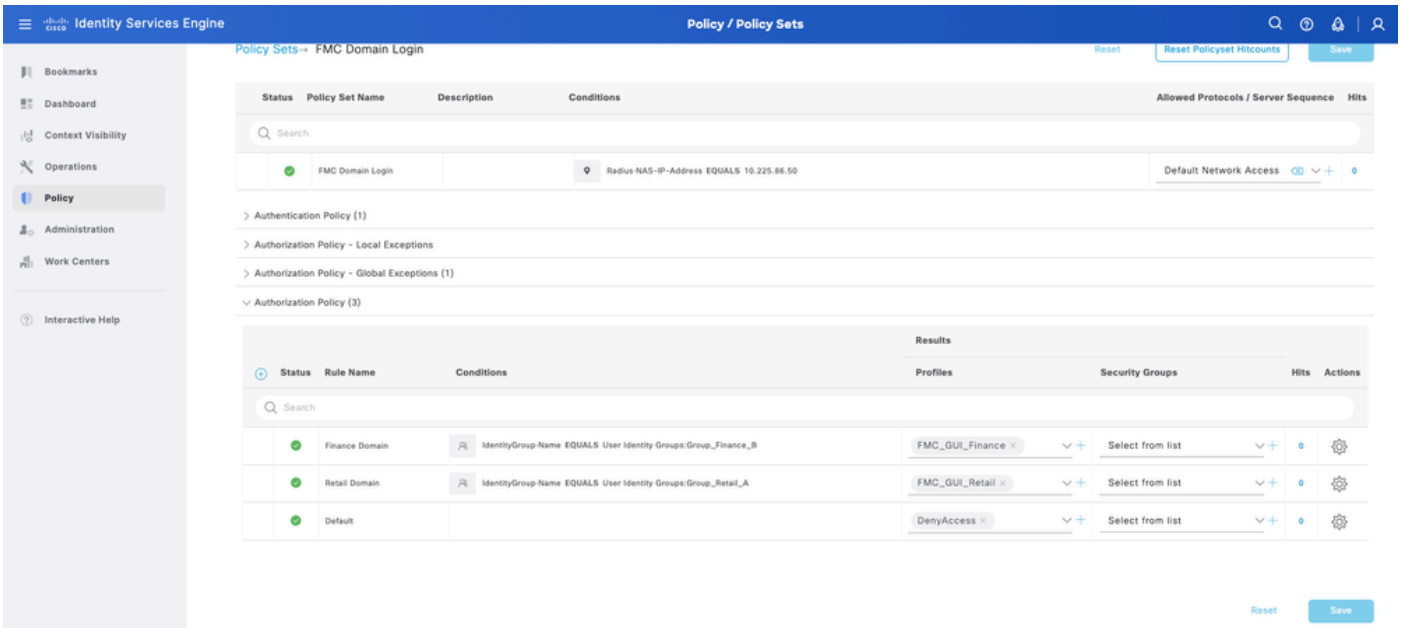
Paso 8.2. Una vez completado, presione Guardar.

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.

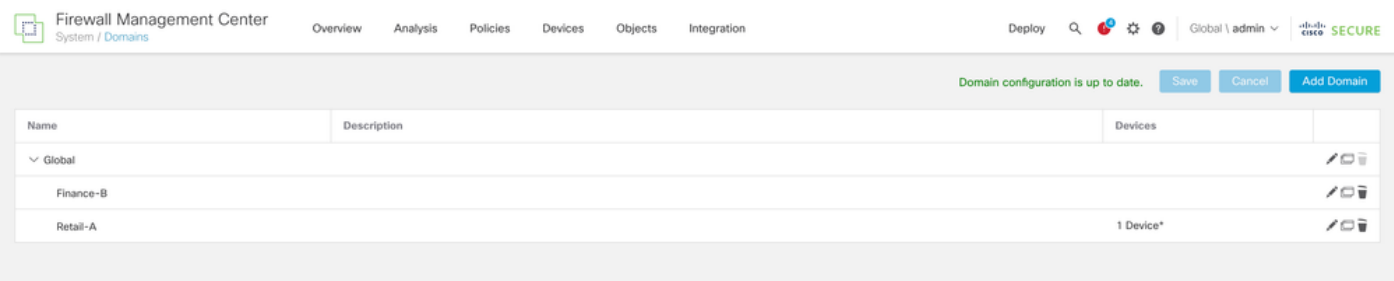
Configuración de FMC

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.

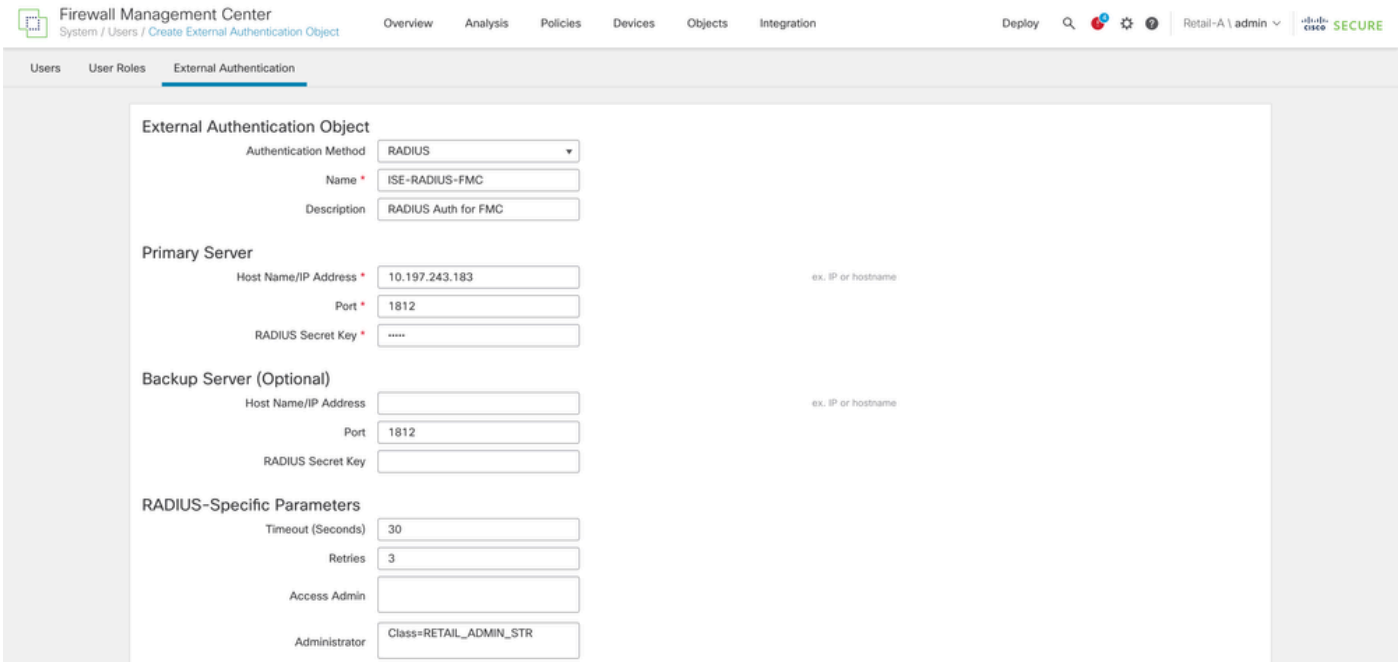
- Vaya a Administration > Domains.
- Haga clic en Agregar dominio para crear Retail-A y Finance-B como subdominios de Global.



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

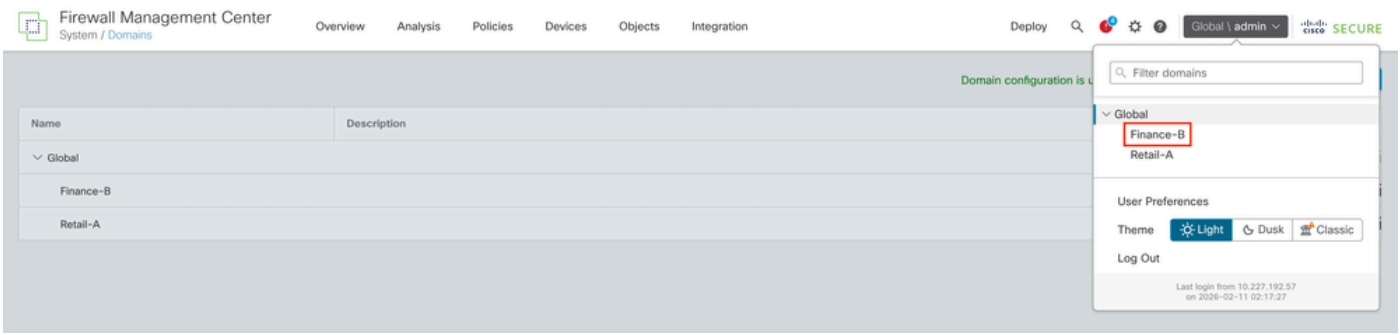
Consejo: Utilice el mismo valor de clase que el configurado en Perfiles de autorización de ISE.

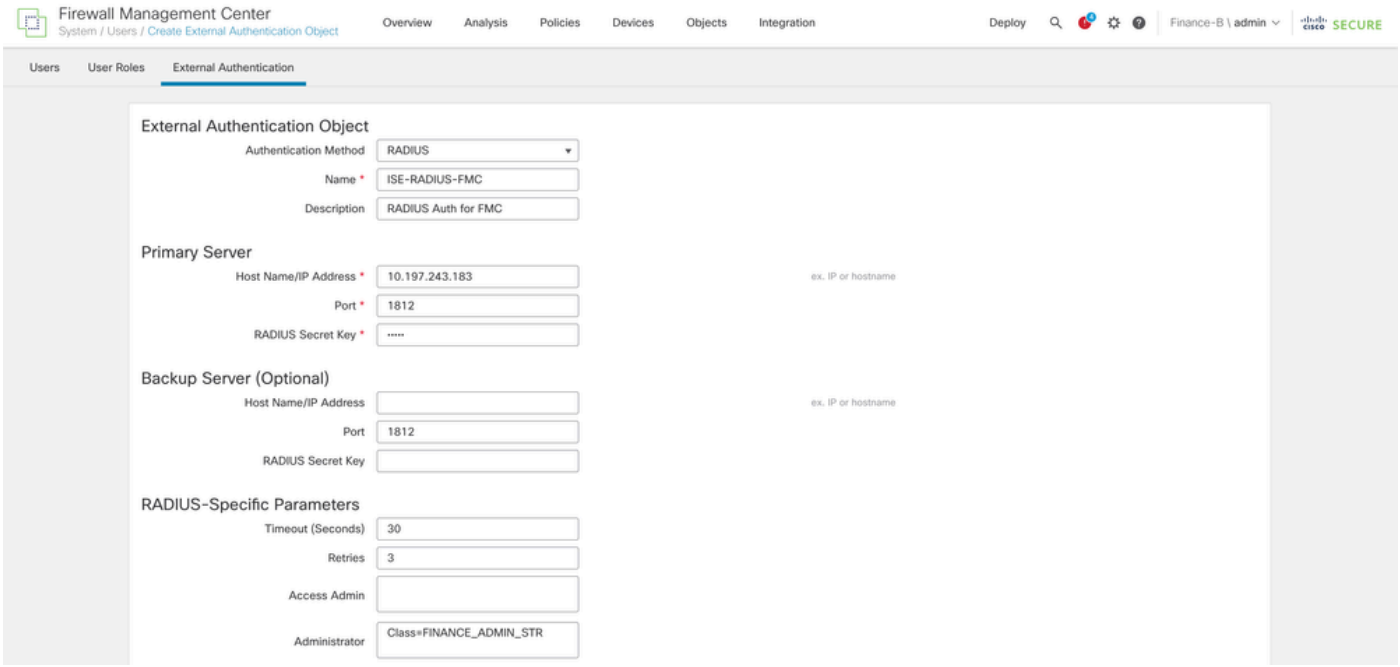


Paso 2.2. Configure el Objeto de Autenticación Externa en Dominio para Finance-B

- 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.





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

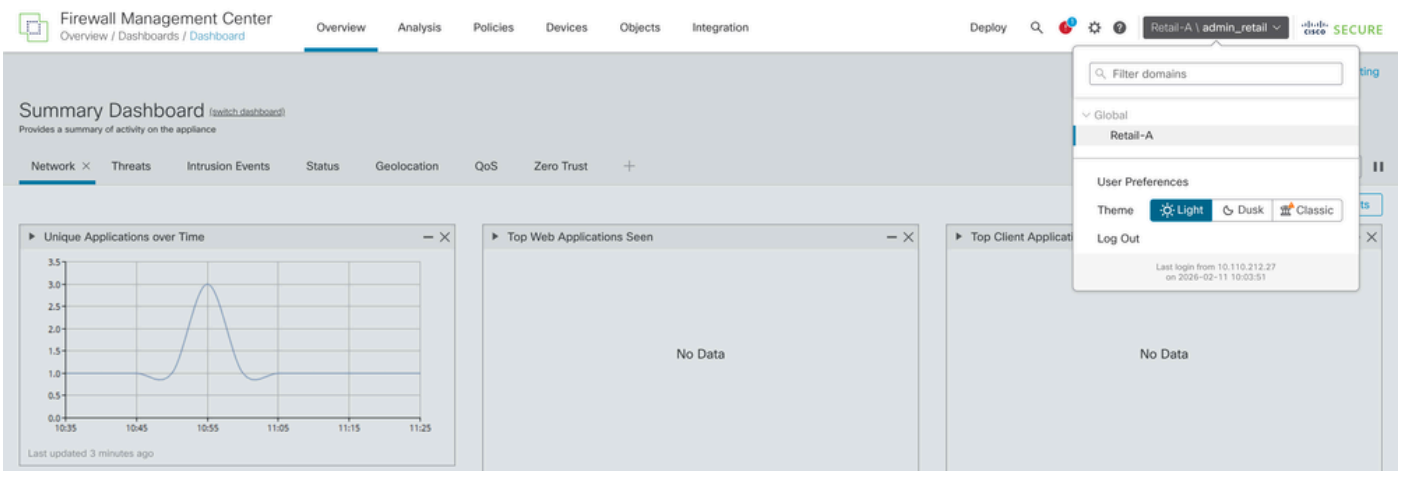
Verificación

Prueba de conexión entre dominios

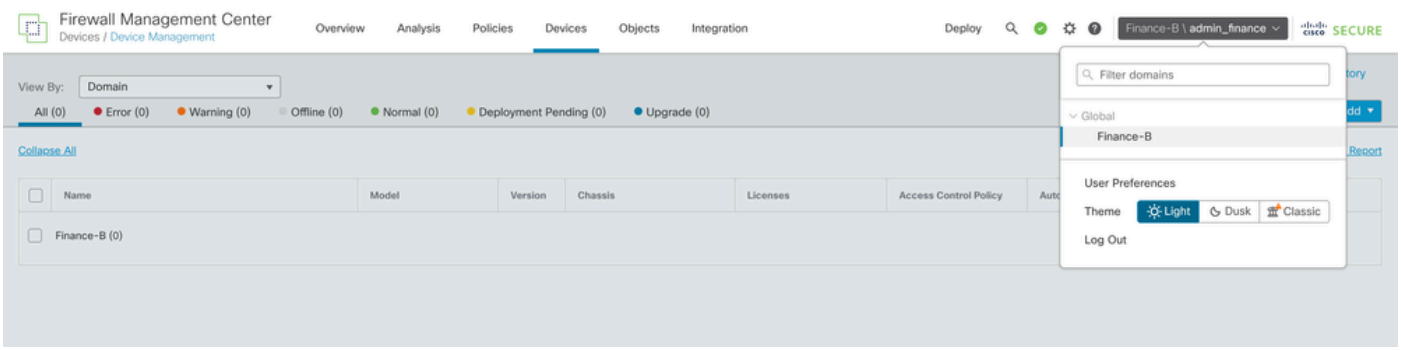
- Intente iniciar sesión en la interfaz web de FMC con admin_retail. Verifique que el Dominio actual que se muestra en la parte superior derecha de la interfaz de usuario sea Retail-A.

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



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

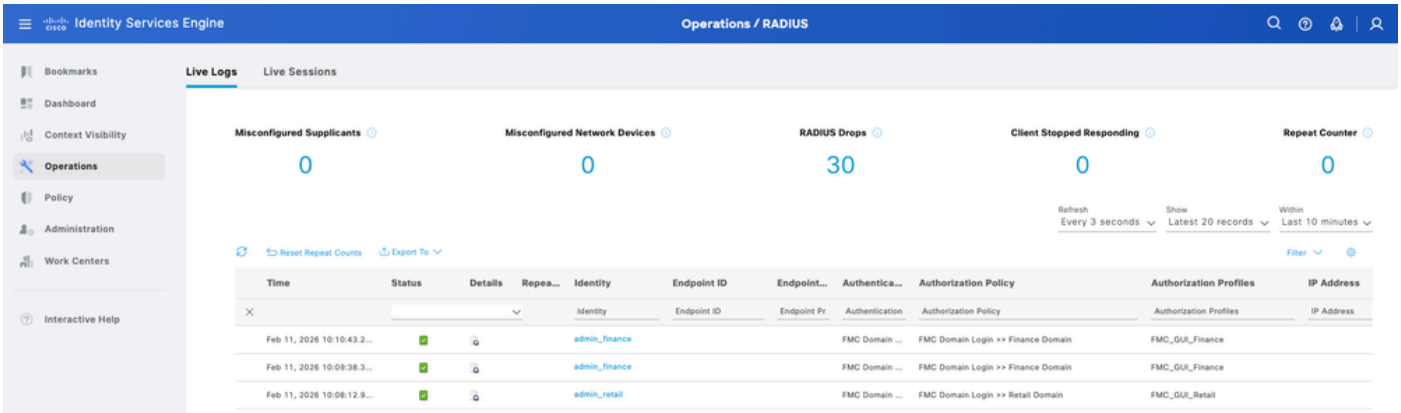


Pruebas internas de FMC

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.

registros en vivo de ISE

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



- 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_igO13NsO1DZN6QciDbrc0cwlaYWHMto: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).