Configurar a autenticação externa do FMC no ambiente de vários domínios

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Configuração
  - Configuração do ISE
    - Adicione seus dispositivos de rede
    - Criar os grupos de identidade e usuários locais
    - Criar os perfis de autorização
    - Adicionar um novo conjunto de políticas
  - Configuração do FMC
    - Adicione seu servidor ISE RADIUS para autenticação FMC
- Verificação
  - Teste de login entre domínios
  - Ensaios internos do FMC
  - Registros ativos do ISE
- Informações Relacionadas

Introdução

Este documento descreve a implementação de multilocação (vários domínios) dentro do Cisco FMC enquanto aproveita o Cisco ISE para autenticação RADIUS centralizada.

Pré-requisitos

Requisitos

Recomenda-se ter conhecimento destes tópicos:

- Configuração inicial do Cisco Secure Firewall Management Center via GUI e/ou shell.
- Privilégios totais de administrador no domínio global do FMC para criar subdomínios e objetos de autenticação externos.
- Configurando políticas de autenticação e autorização no ISE.
- Conhecimento RADIUS básico

Componentes Utilizados

- FMC Cisco Secure: vFMC 7.4.2 (ou posterior recomendado para estabilidade de vários domínios)
- Estrutura do domínio: Uma hierarquia de três níveis (Global > Subdomínios de segundo nível).
- Cisco Identity Services Engine: ISE 3.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Em ambientes corporativos de grande escala ou em cenários de MSSP (Managed Security Service Provider), geralmente é necessário segmentar o gerenciamento de rede em limites administrativos distintos. Este documento descreve como configurar o FMC para suportar vários domínios, especificamente para um exemplo real em que um MSSP gerencia dois clientes: Varejo-A e Finanças-B. Usando a autenticação RADIUS externa via Cisco ISE, os administradores podem garantir que os usuários recebam acesso automaticamente apenas aos respectivos domínios de usuário com base em suas credenciais centralizadas.

O sistema Cisco Secure Firewall usa Domínios para implementar a multilocação.

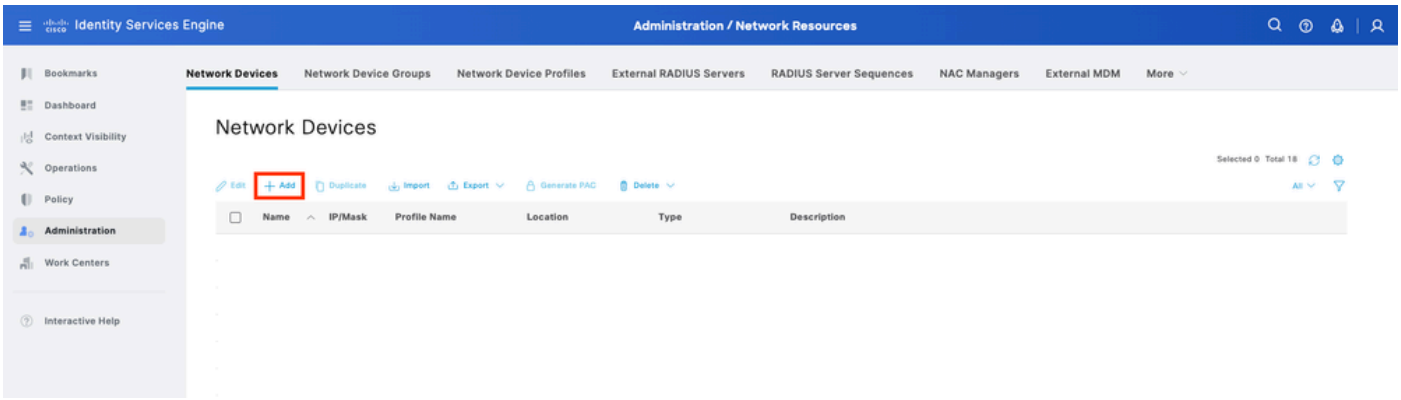
- Hierarquia de domínio: A hierarquia começa no domínio Global. Você pode criar até 100 subdomínios em uma estrutura de dois ou três níveis.
- Domínios Leaf: Esses são domínios na parte inferior da hierarquia sem mais subdomínios. Essencialmente, cada dispositivo FTD gerenciado deve ser associado a exatamente um domínio folha.
- Atributo de classe RADIUS (Atributo 25): Em uma configuração de vários domínios, o FMC usa o atributo de classe RADIUS retornado pelo ISE para mapear um usuário autenticado para um domínio e uma função de usuário específicos. Isso permite que um único servidor RADIUS atribua dinamicamente usuários a diferentes segmentos de usuário (por exemplo, Retail-A vs. Finance-B) no login.

Configuração

Configuração do ISE

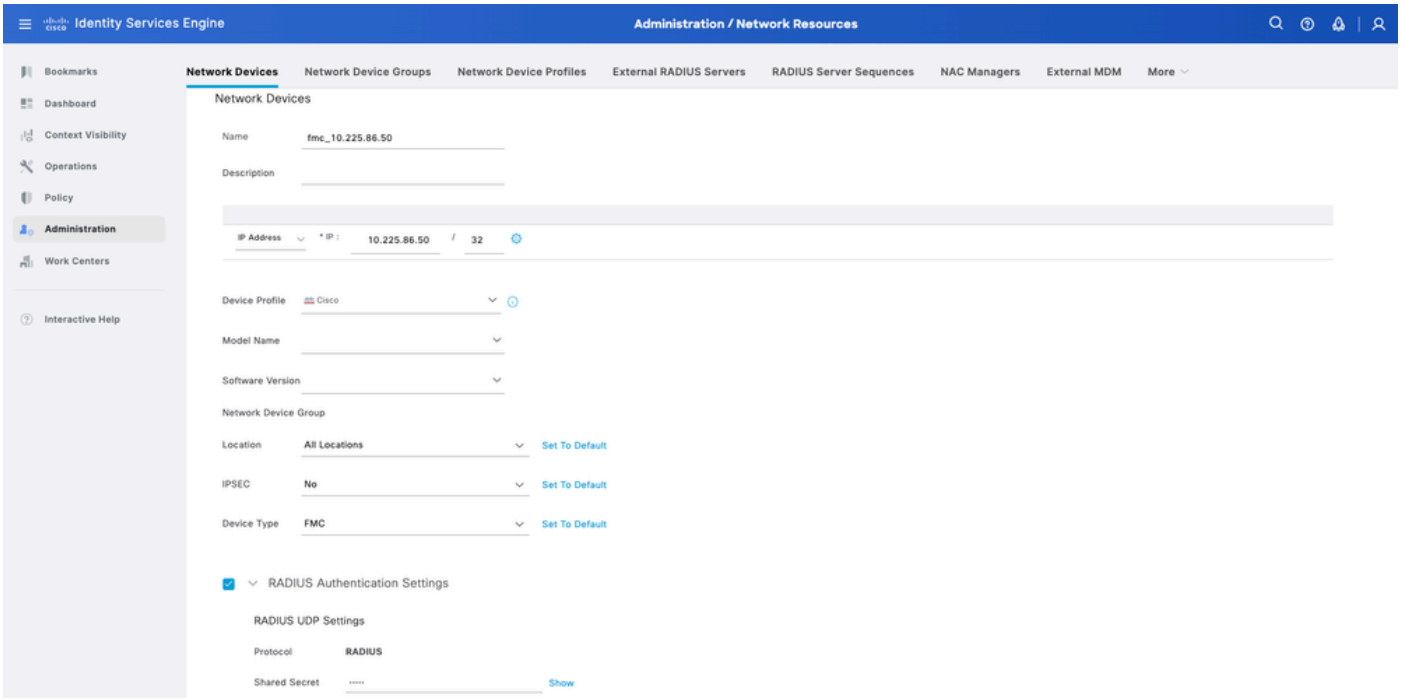
Adicione seus dispositivos de rede

Etapa 1. Navegue até Administração > Recursos de rede > Dispositivos de rede > Adicionar.



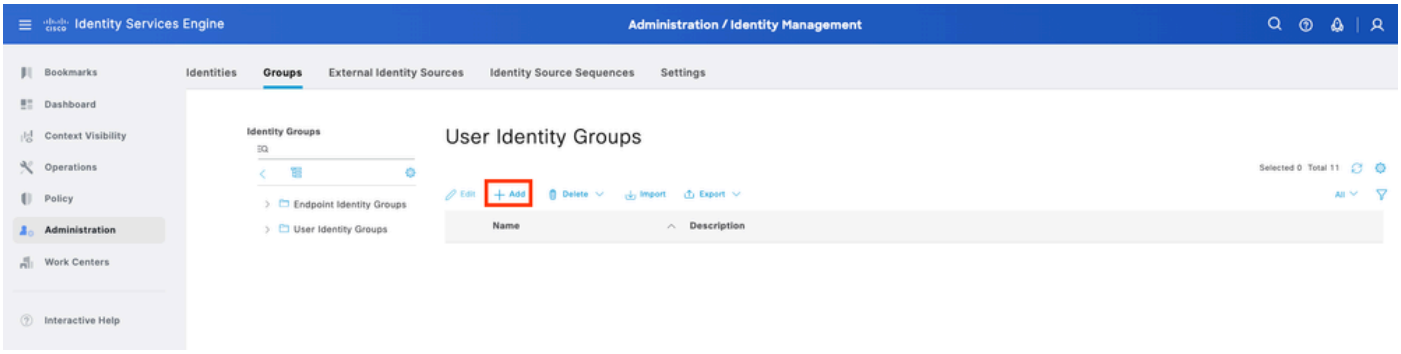
Etapa 2. Atribua um Name ao objeto do dispositivo de rede e insira o endereço IP do FMC.

Marque a caixa de seleção RADIUS e defina um segredo compartilhado. A mesma chave deve ser usada posteriormente para configurar o FMC. Quando terminar, clique em Salvar.

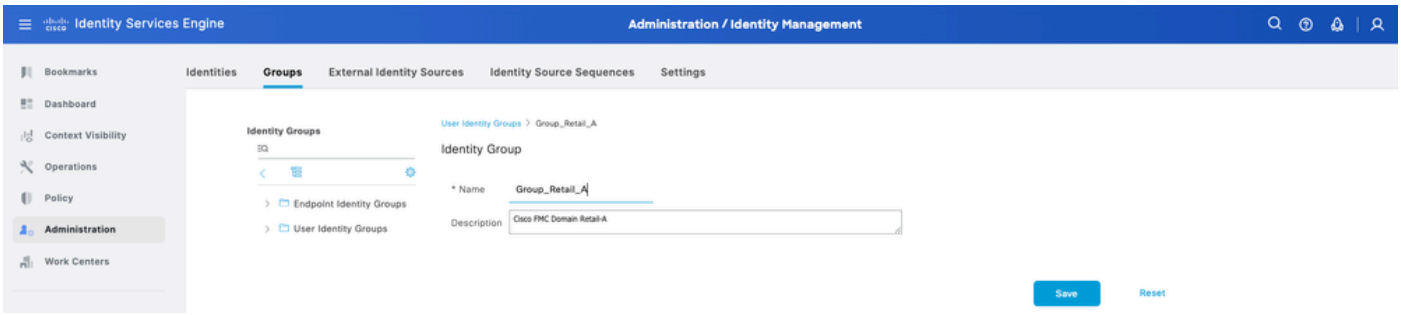


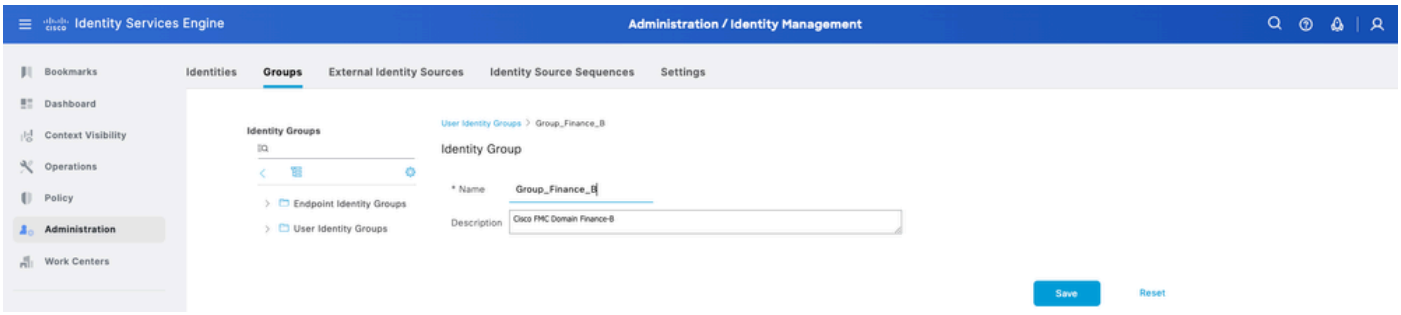
Criar os grupos de identidade e usuários locais

Etapa 3. Criar os Grupos de Identidade de Usuário necessários. Navegue até Administração > Gerenciamento de identidades > Grupos > Grupos de identidades do usuário > Adicionar.

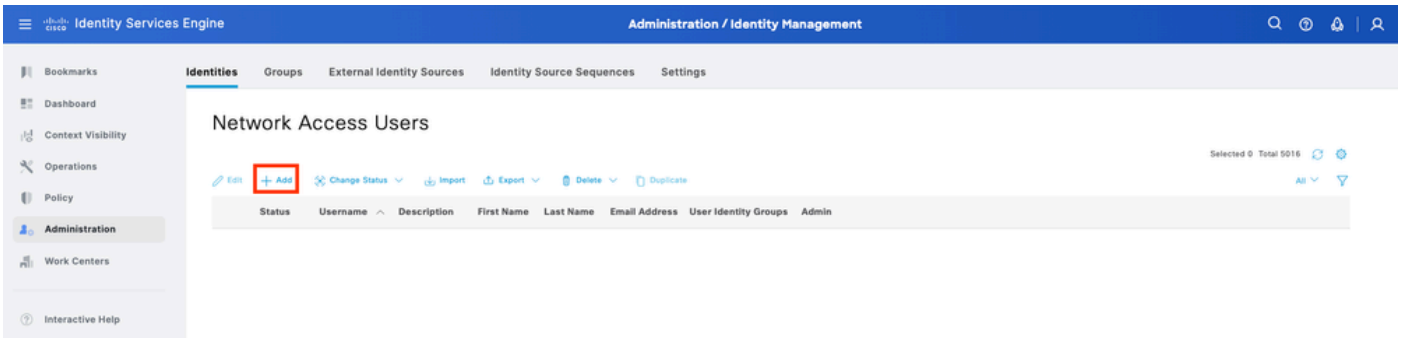


Etapa 4. Dê a cada grupo um nome e Salvar individualmente. Neste exemplo, você está criando um grupo para usuários Administradores. Crie dois grupos: Group_Retail_A e Group_Finance_B.

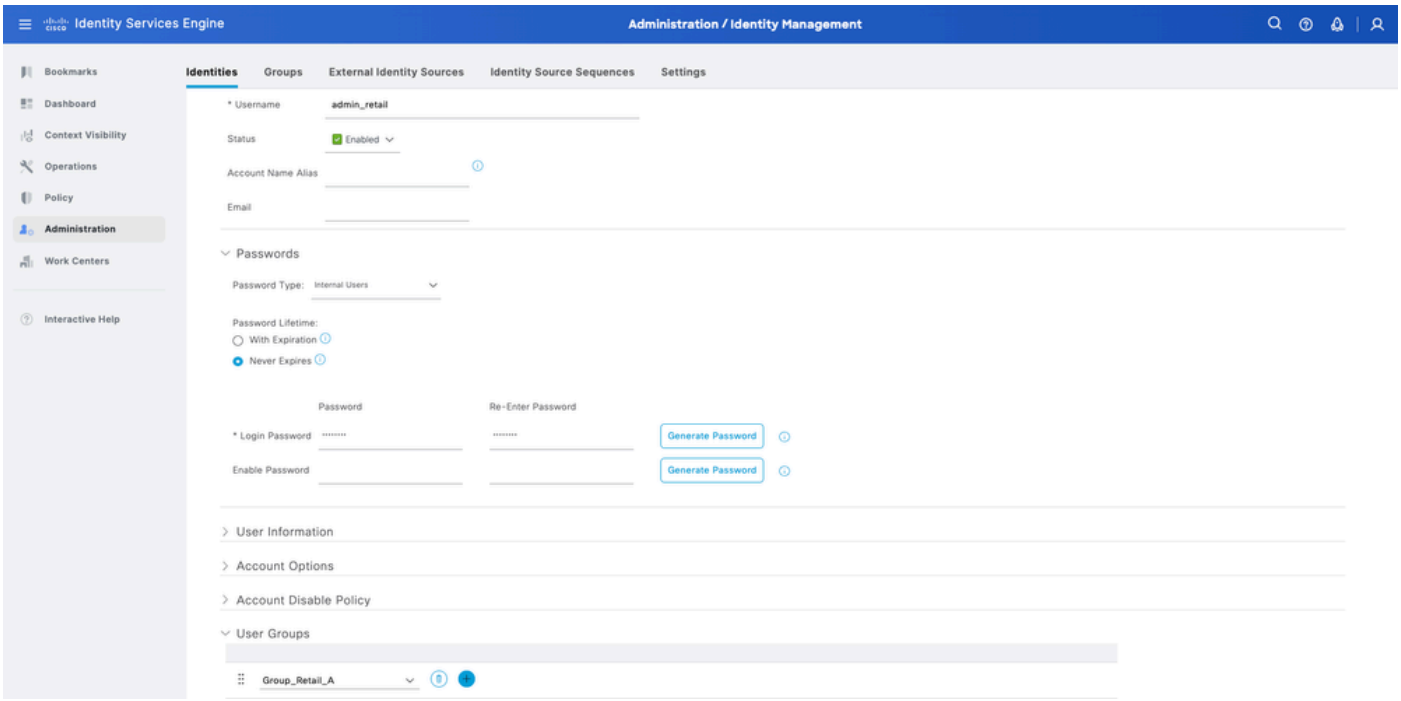




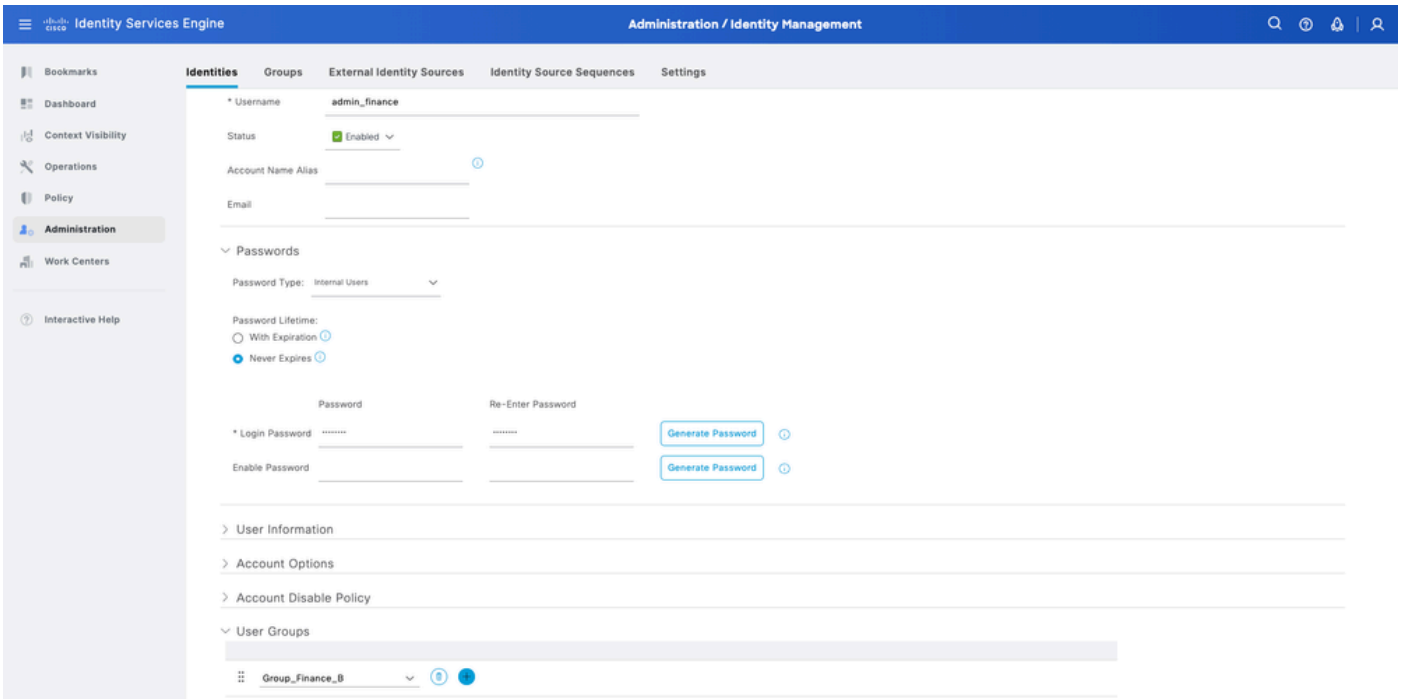
Etapa 5. Crie os usuários locais e adicione-os ao seu grupo de correspondentes. Navegue até Administração > Gerenciamento de identidades > Identidades > Adicionar.



Etapa 5.1. Primeiro crie o usuário com direitos de Administrador. Atribua um nome a ele admin_retail, password e ao grupo Group_Retail_A.

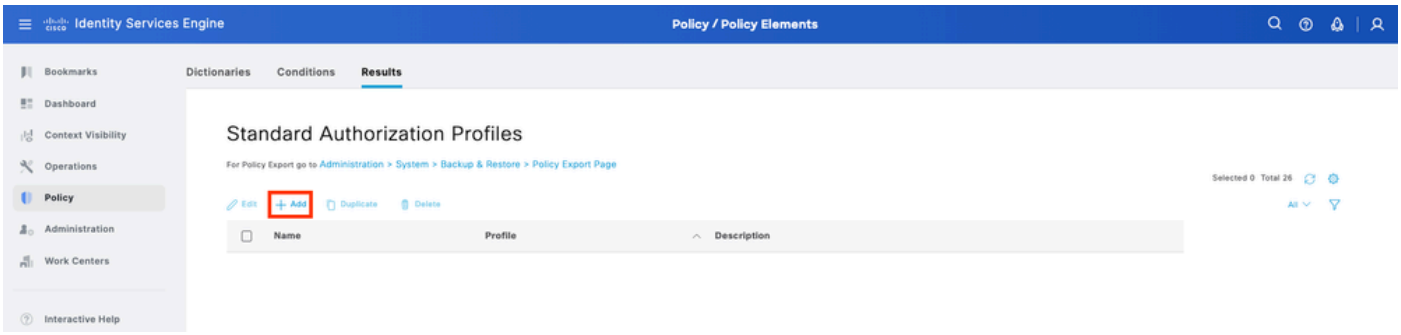


Etapa 5.2. Primeiro crie o usuário com direitos de Administrador. Atribua um nome a ele admin_finance, password e ao grupo Group_Finance_B.



Criar os perfis de autorização

Etapa 6. Criar o perfil de autorização para o usuário administrador da interface da Web do FMC. Navegue até Política > Elementos de política > Resultados > Autorização > Perfis de autorização > Adicionar.

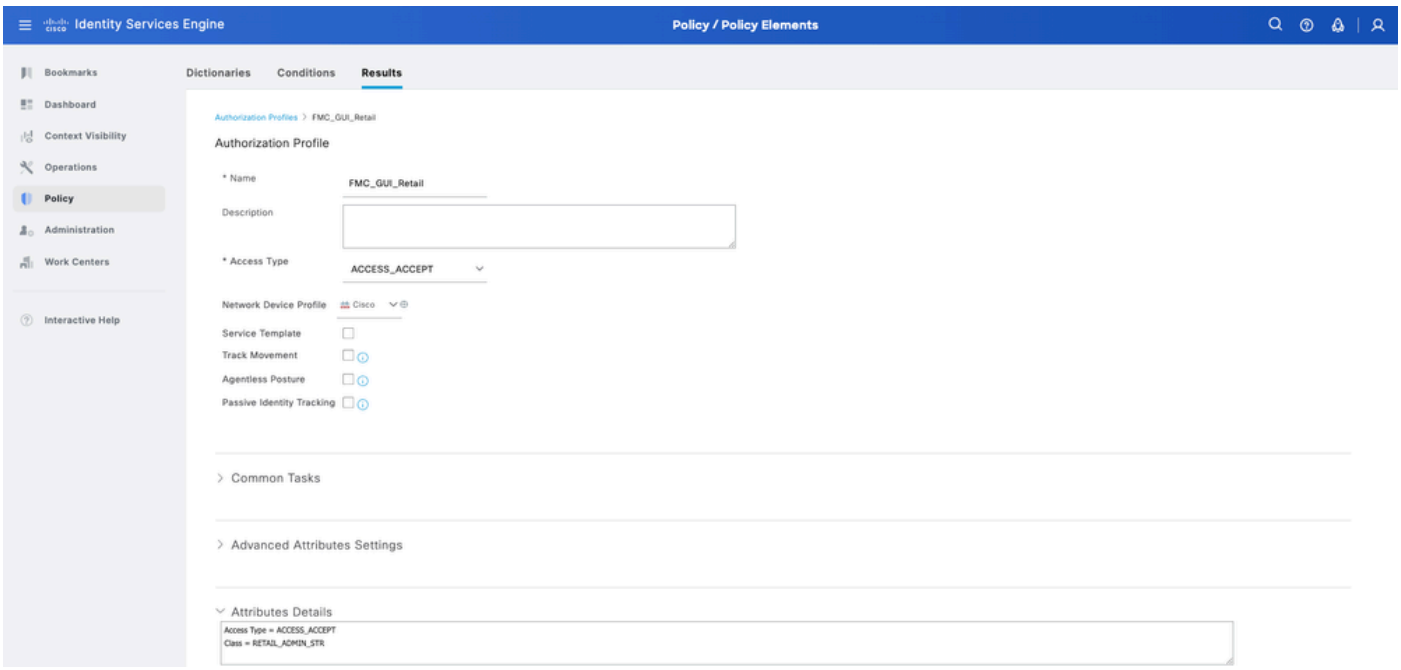


Defina um nome para o Perfil de Autorização, deixe Tipo de Acesso como ACCESS_ACCEPT.

Em Advanced Attributes Settings, adicione Radius > Class—[25] com o valor e clique em Submit.

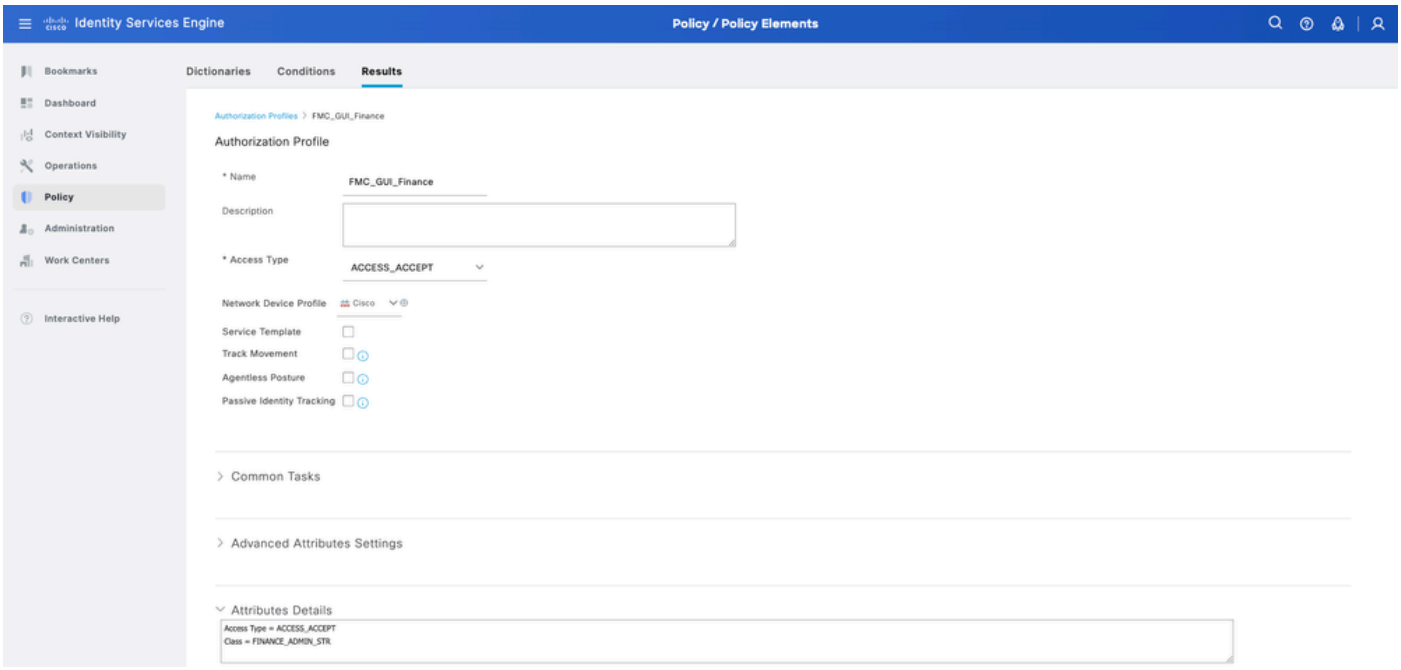
Etapa 6.1. Perfil de varejo: Em Advanced Attributes Settings, adicione Radius:Class com o valor RETAIL_ADMIN_STR.

Tip: Aqui RETAIL_ADMIN_STR pode ser qualquer coisa; certifique-se de que o mesmo valor também seja colocado no lado do FMC.



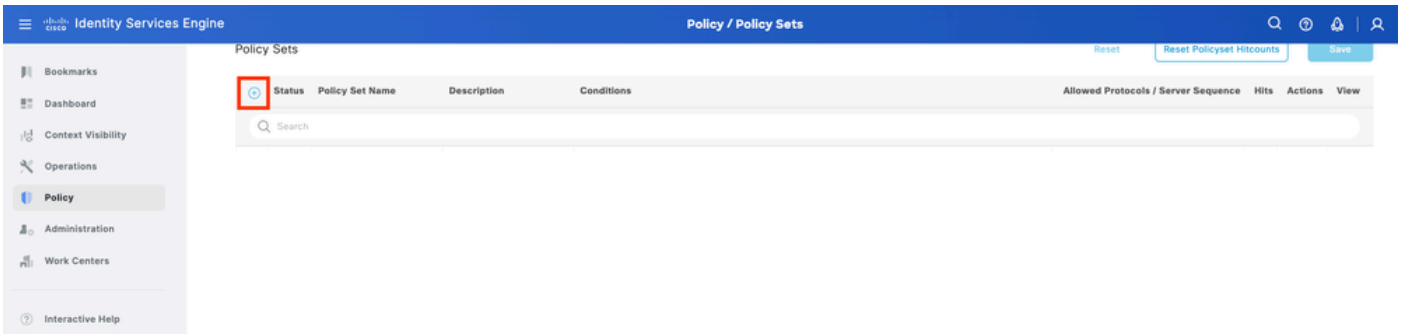
Etapa 6.2. Perfil Financeiro: Em Advanced Attributes Settings, adicione Radius:Class com o valor FINANCE_ADMIN_STR.

Tip: Aqui FINANCE_ADMIN_STR pode ser qualquer coisa; certifique-se de que o mesmo valor também seja colocado no lado do FMC.



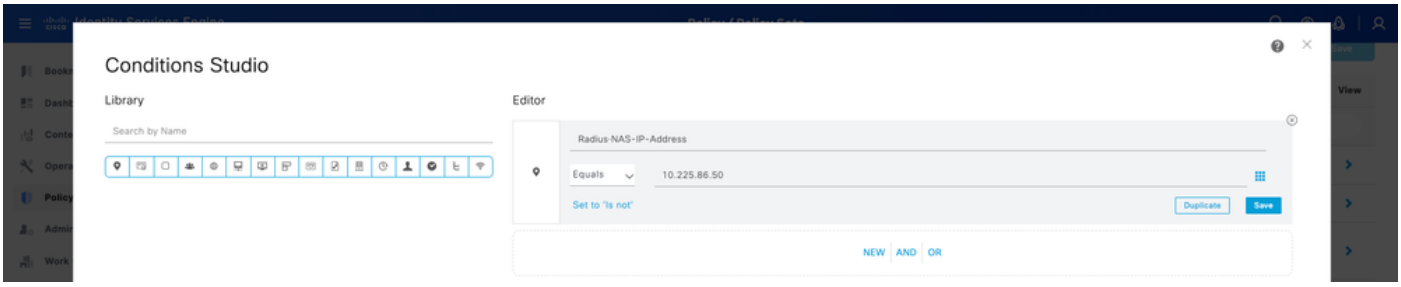
Adicionar um novo conjunto de políticas

Etapa 7. Criar um conjunto de políticas correspondente ao endereço IP do FMC. Isso evita que outros dispositivos concedam acesso aos usuários. Navegue para Política > Conjuntos de políticas > ícone do sinal de adição no canto superior esquerdo.



Etapa 8.1. Uma nova linha é colocada na parte superior de seus conjuntos de políticas.

Nomeie a nova política e adicione uma condição superior para o atributo RADIUS NAS-IP-Address correspondente ao endereço IP do FMC. Clique em Usar para manter as alterações e sair do editor.



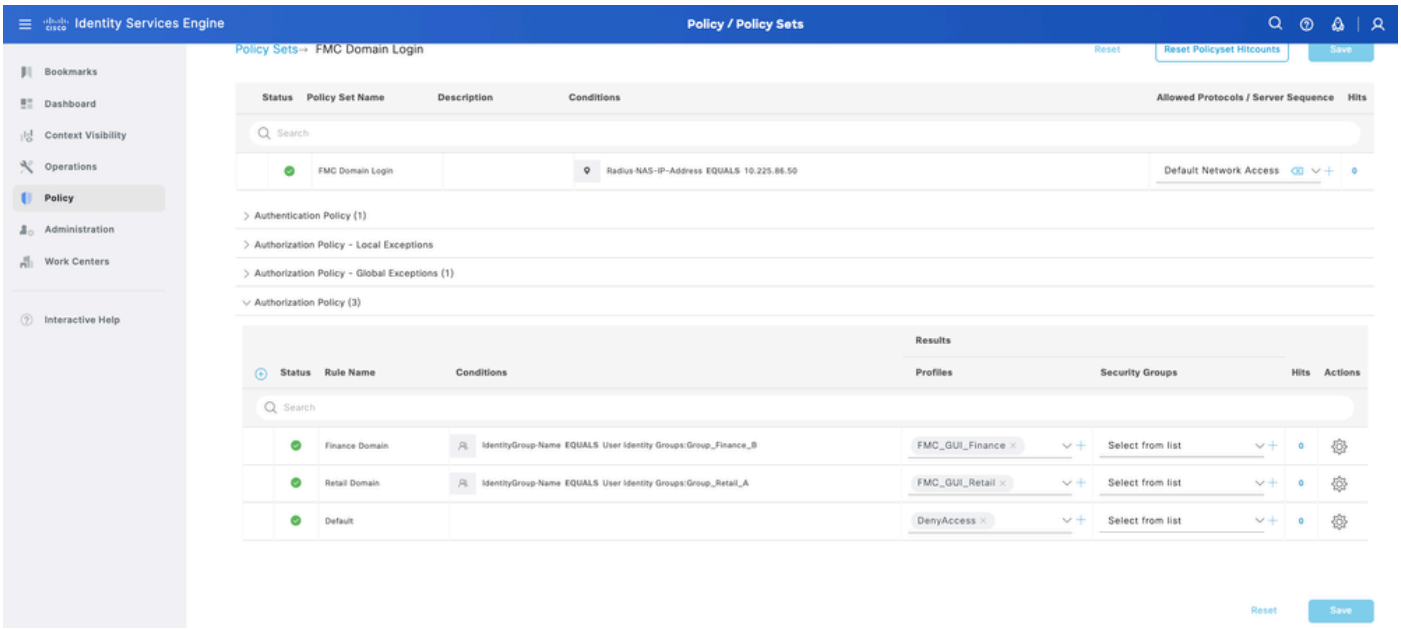
Etapa 8.2. Depois de concluir, clique em Salvar.

Etapa 9. Visualize o novo Conjunto de políticas pressionando o ícone set colocado no final da linha.

Expanda o menu Authorization Policy e pressione o ícone do sinal de adição para adicionar uma nova regra para permitir o acesso ao usuário com direitos administrativos. Dê-lhe um nome.

Defina as condições para corresponder ao Grupo de Identidades do Dicionário com Nome de Atributo Igual a e escolha Grupos de Identidades do Usuário. Em Política de autorização, crie regras:

- Regra 1: Se o Grupo de Identidade do Usuário for igual a Group_Retail_A, atribua o Perfil Varejo.
- Regra 2: Se o Grupo de Identidades do Usuário for igual a Group_Finance_B, atribua o Perfil Financeiro.



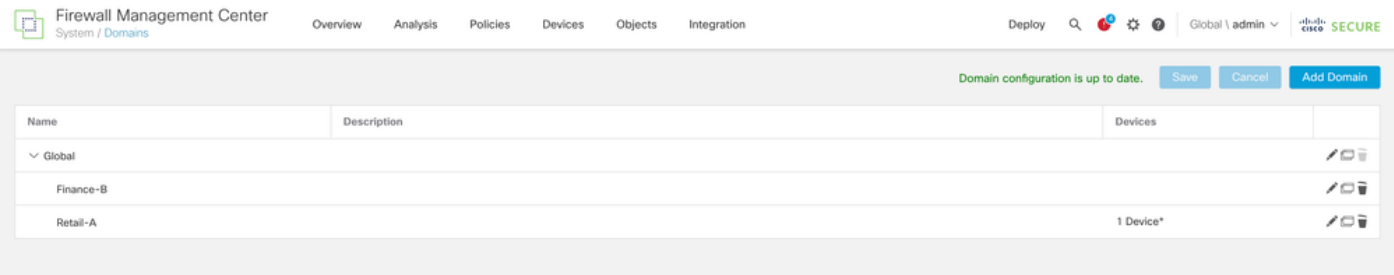
Etapa 10. Defina os Perfis de Autorização para cada regra e pressione Salvar.

Configuração do FMC

Adicione seu servidor ISE RADIUS para autenticação FMC

Etapa 1. Estabeleça a estrutura de domínio:

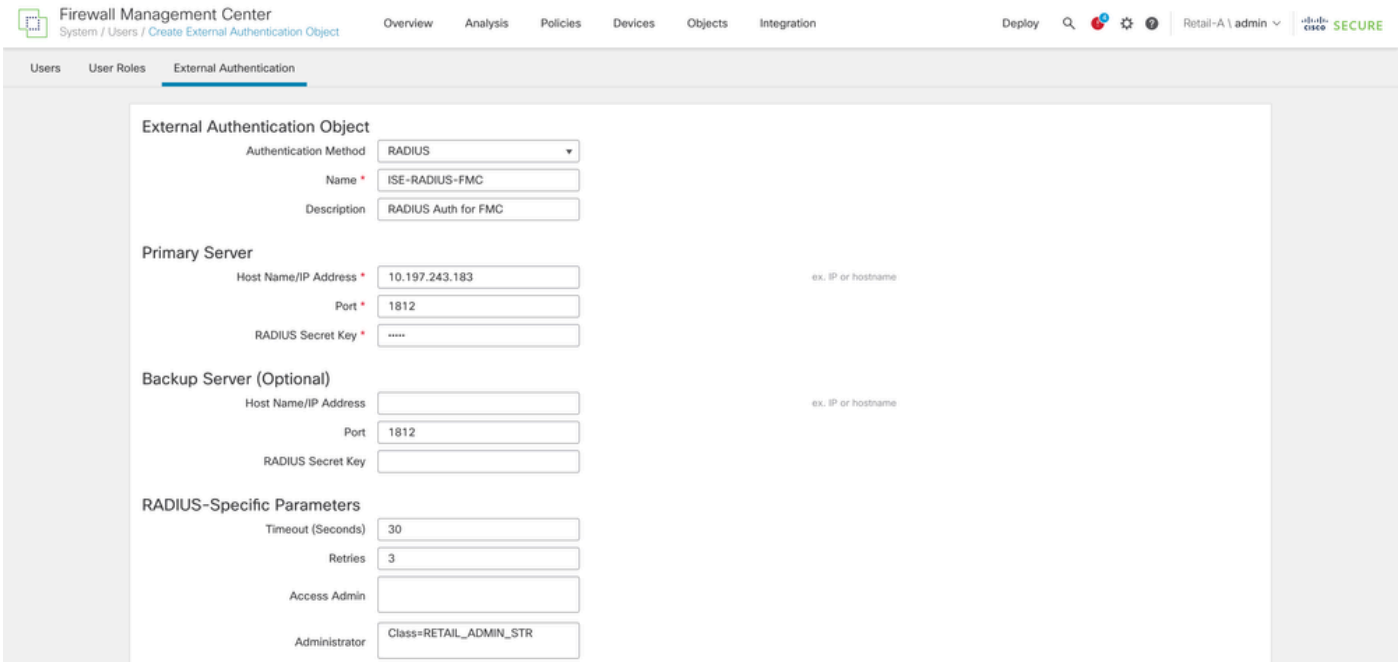
- Faça login no domínio global do FMC.
- Navegue até Administração > Domínios.
- Clique em Adicionar domínio para criar Retail-A e Finance-B como subdomínios de Global.



Etapa 2.1. Configure o Objeto de Autenticação Externa no Domínio para Retail-A

- Mude o domínio para Retail-A.
- Navegue até System > Users > External Authentication.
- Selecione Add External Authentication Object e escolha RADIUS.
- Insira o endereço IP do ISE e o segredo compartilhado configurado anteriormente.
- Informe os Parâmetros Específicos do RADIUS > Administrador > class=RETAIL_ADMIN_STR

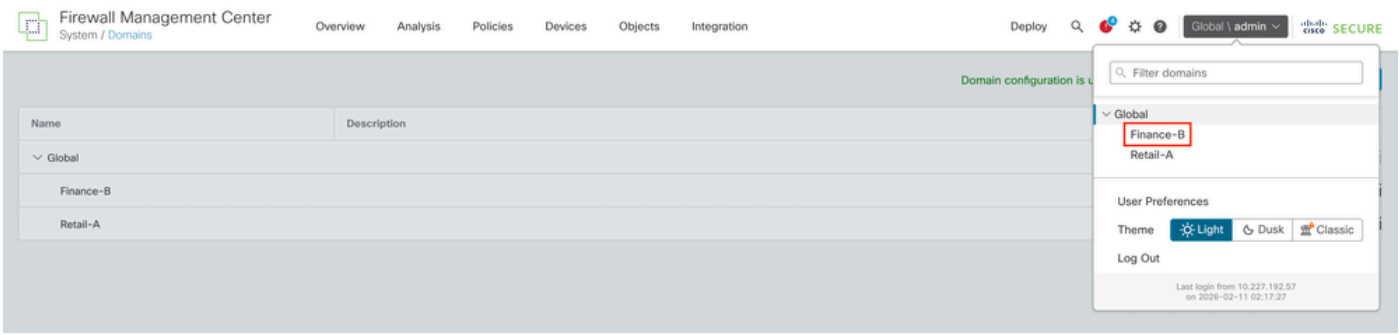
Tip: Use o mesmo valor para a classe como configurado em Perfis de autorização do ISE.

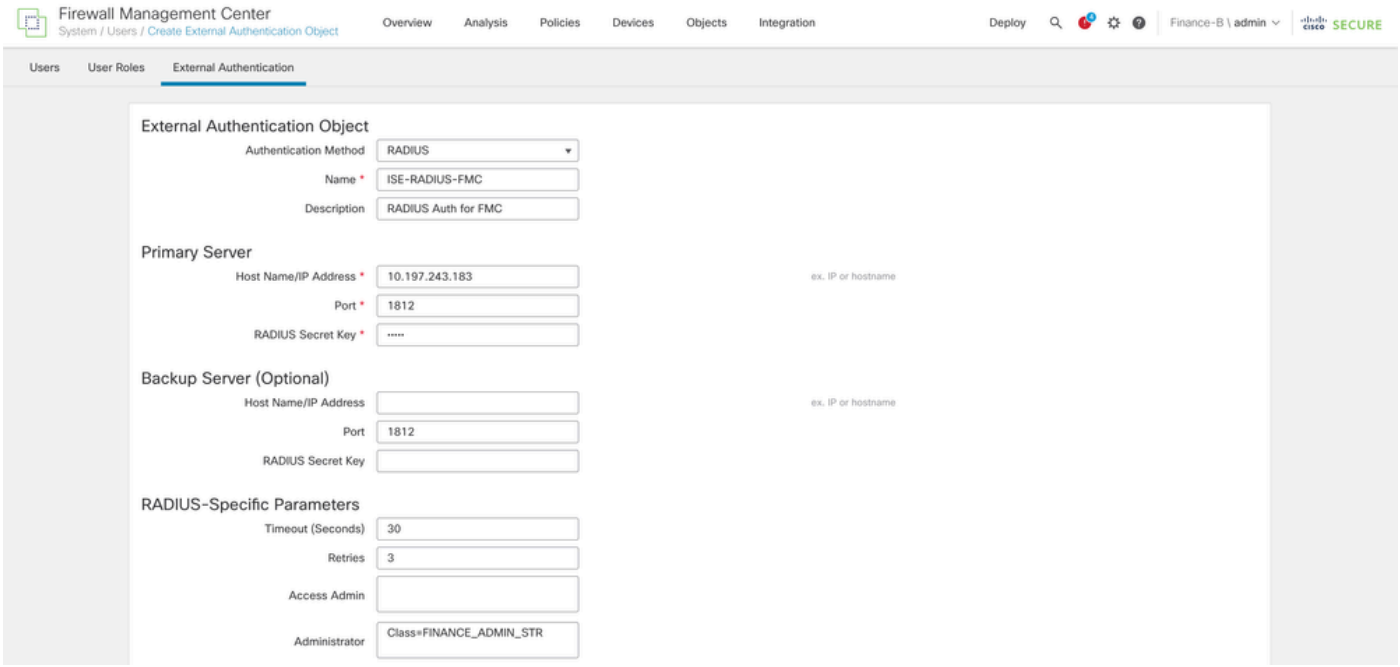


Etapa 2.2. Configure o Objeto de Autenticação Externa no Domínio como Finance-B

- Mude o Domínio para Finance-B.
- Navegue até System > Users > External Authentication.
- Selecione Add External Authentication Object e escolha RADIUS.
- Insira o endereço IP do ISE e o segredo compartilhado configurado anteriormente.
- Informe os Parâmetros Específicos do RADIUS > Administrador > class=FINANCE_ADMIN_STR

Tip: Use o mesmo valor para a classe como configurado em Perfis de autorização do ISE.





Etapa 3. Ativar autenticação: Habilite o objeto e defina-o como o método de autenticação de shell. Clique em Salvar e Aplicar.

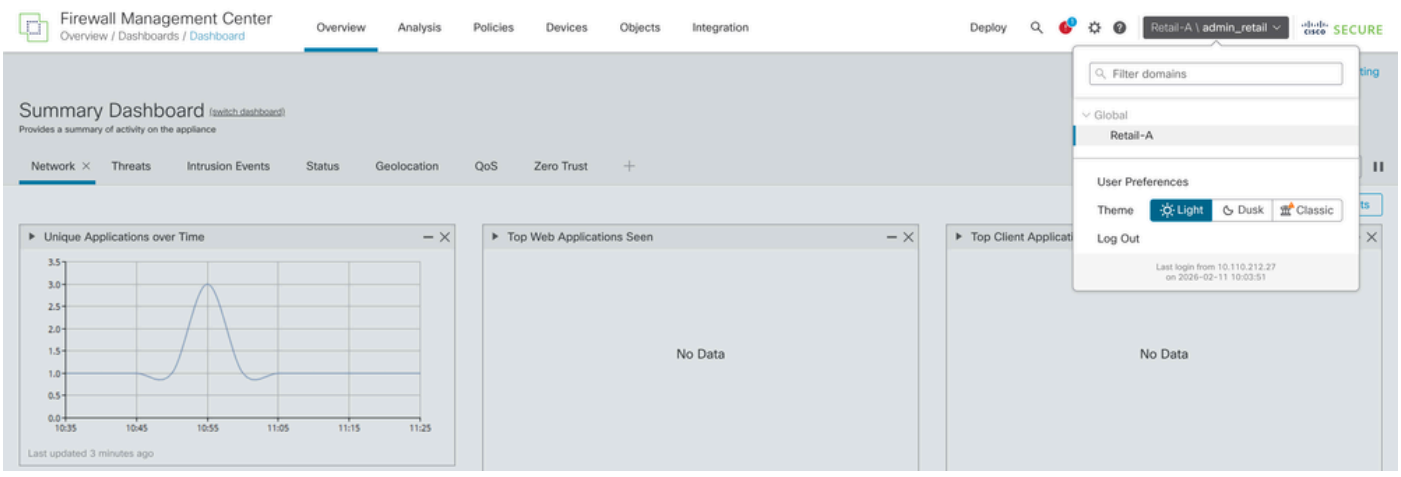
Verificação

Teste de login entre domínios

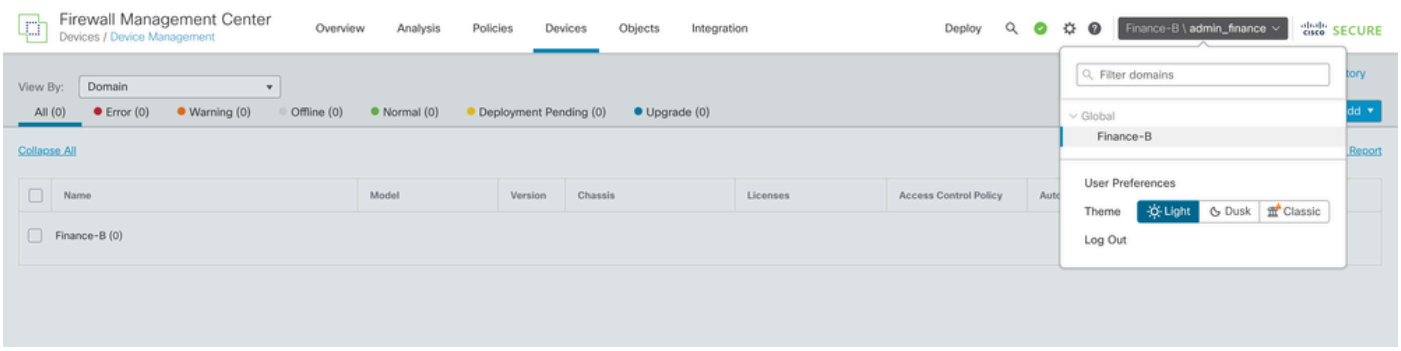
- Tente fazer login na interface da Web do FMC usando admin_retail. Verifique se o Domínio atual exibido na parte superior direita da interface do usuário é Retail-A.

Tip: Ao efetuar login em um domínio específico, use o formato de nome de usuário domain_name\radius_user_mapped_with_that_domain.

Por exemplo, se o usuário administrador de Varejo precisar fazer logon, o nome de usuário deverá ser Retail-A\admin_retail e a senha correspondente.



- Faça logoff e logon como admin_finance. Verifique se o usuário está restrito ao domínio Finance-B e não pode ver dispositivos Retail-A.

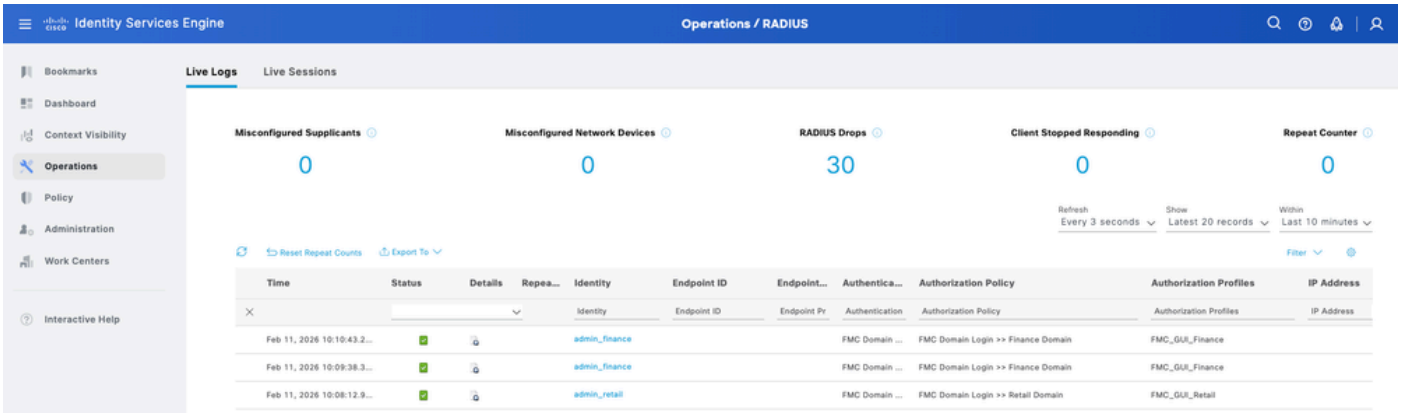


Ensaios internos do FMC

Navegue até as configurações do servidor RADIUS no FMC. Use a seção Parâmetros de Teste Adicionais para informar um nome de usuário e senha de teste. Um teste bem-sucedido deve mostrar uma mensagem verde de êxito.

Registros ativos do ISE

- No Cisco ISE, navegue até Operations > RADIUS > Live Logs.



- Confirme se as solicitações de autenticação mostram um status Pass (Aprovado) e se o Authorization Profile (Perfil de Autorização) correto (e a cadeia de caracteres Class associada) foi enviado no pacote 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_igO13NsO1DZN6QciDbrc0cwlaYWHMto:eagle/556377151/553

Informações Relacionadas

Configurar a autenticação externa de FMC e FTD com ISE como um servidor RADIUS

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.