

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.

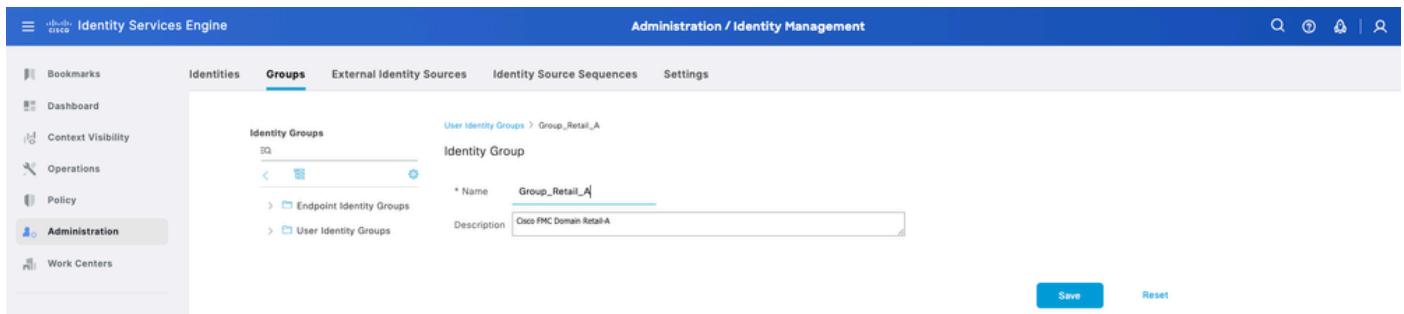
Etapa 2. Atribua um Name ao objeto do dispositivo de rede e insira o endereço IP do FMC.

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.

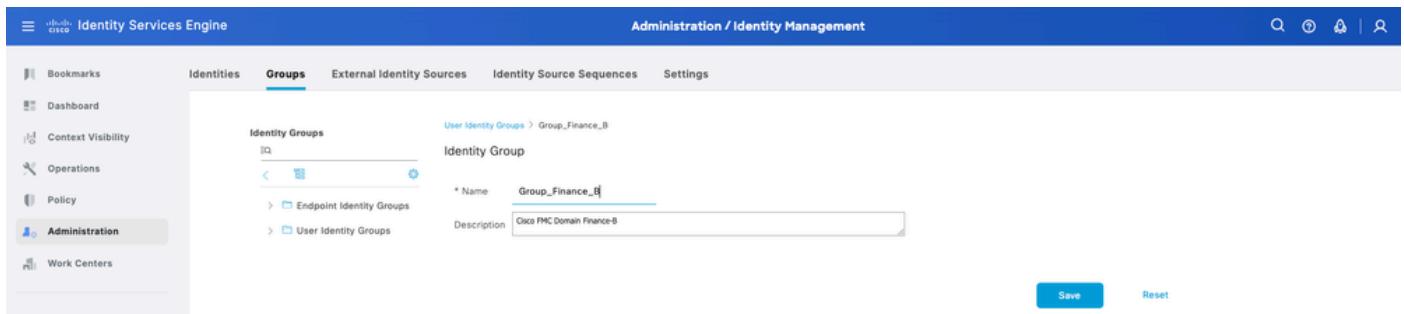
Criar os grupos de identidade e usuários locais

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.

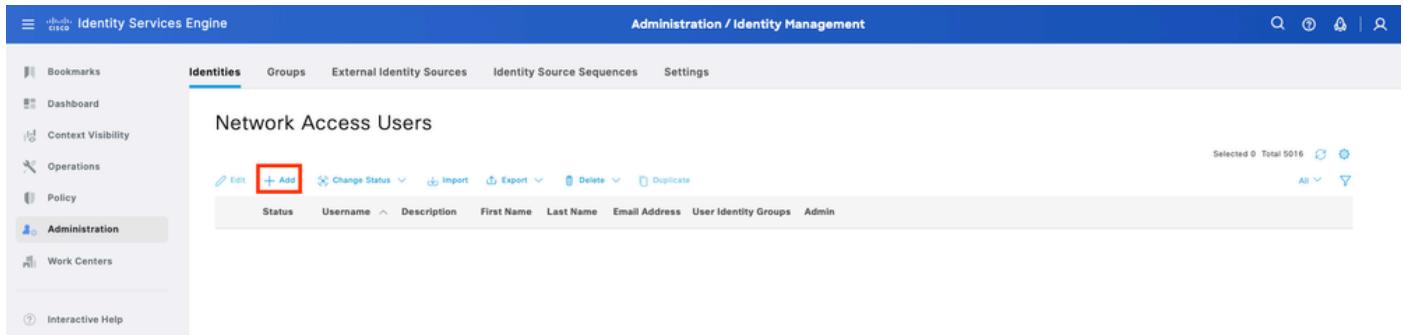


The screenshot shows the 'Groups' tab selected in the navigation bar. Under 'Identity Groups', a new group is being created with the name 'Group_Retail_A' and a description 'Cisco FMC Domain Retail-A'. The 'Save' button is highlighted.



The screenshot shows the 'Groups' tab selected in the navigation bar. Under 'Identity Groups', a new group is being created with the name 'Group_Finance_B' and a description 'Cisco FMC Domain Finance-B'. The 'Save' button is highlighted.

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



The screenshot shows the 'Identidades' tab selected in the navigation bar. Under 'Network Access Users', a new user is being created with the 'Add' button highlighted. The user will be assigned to the 'Group_Retail_A' group.

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.

Identity Services Engine Administration / Identity Management

Identities

* Username: admin_retail

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime:

- With Expiration
- Never Expires

Password: Login Password: Re-Enter Password:

Enable Password:

User Information

Account Options

Account Disable Policy

User Groups

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.

Identity Services Engine Administration / Identity Management

Identities

* Username: admin_finance

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime:

- With Expiration
- Never Expires

Password: Login Password: Re-Enter Password:

Enable Password:

User Information

Account Options

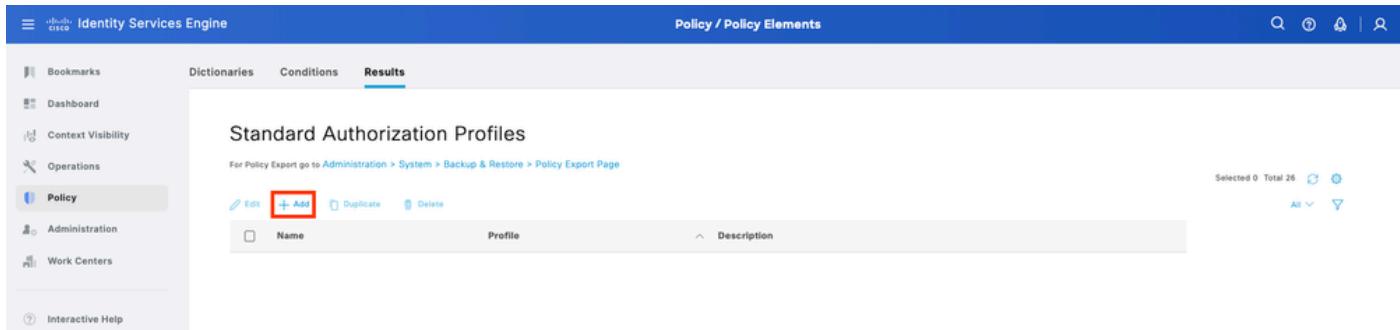
Account Disable Policy

User Groups

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.



Identity Services Engine

Policy / Policy Elements

Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 26

Profile

Description

Name

Profile

Description

Selected 0 Total 26

All

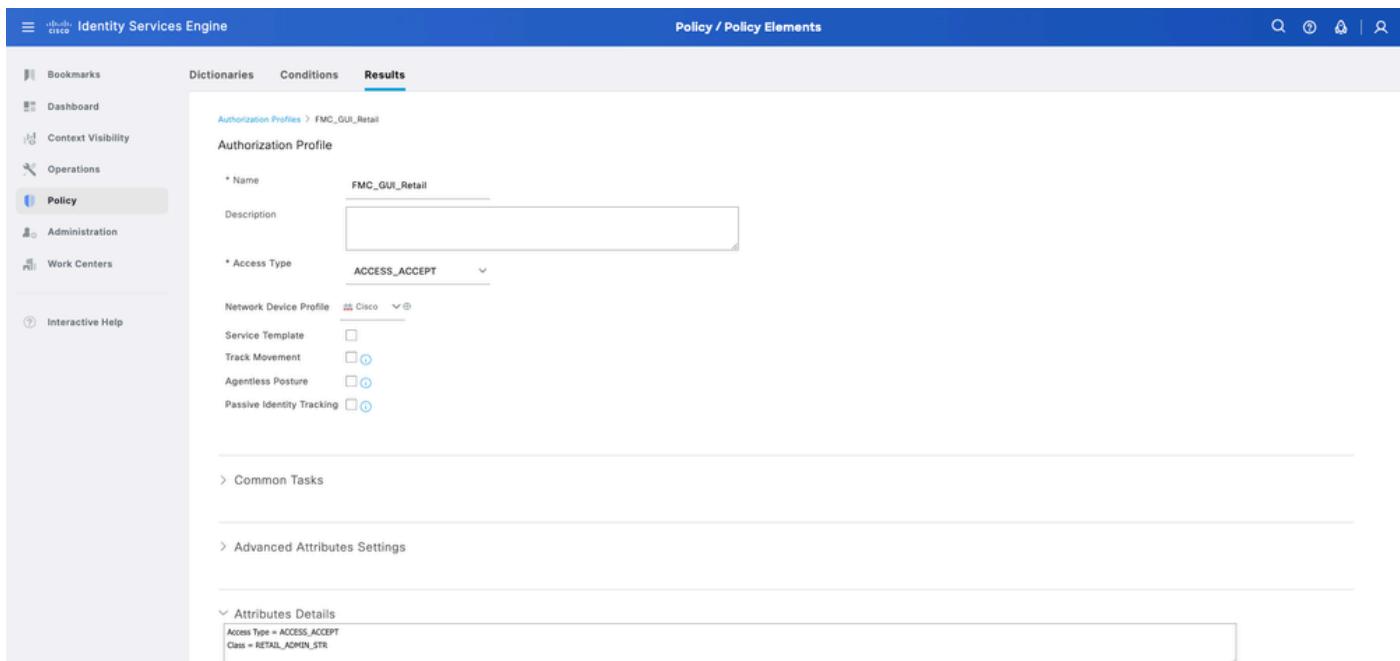
Defina um nome para o Perfil de Autorização, deixe Tipo de Acesso como ACCESS_ACCEPT.

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.



Identity Services Engine

Policy / Policy Elements

Authorization Profiles > FMC_GUI_Retail

Authorization Profile

* Name: FMC_GUI_Retail

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Agentless Posture:

Passive Identity Tracking:

Common Tasks

Advanced Attributes Settings

Attributes Details

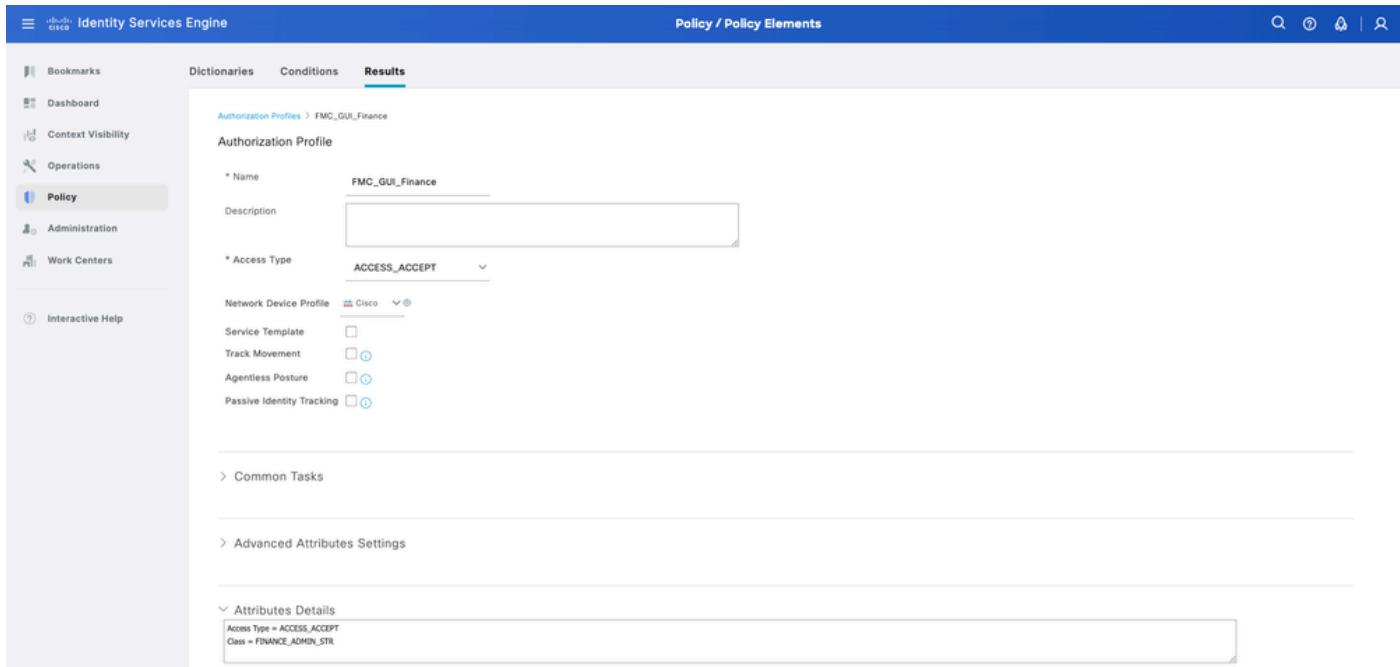
Access Type = ACCESS_ACCEPT

Class = RETAIL_ADMIN_STR

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



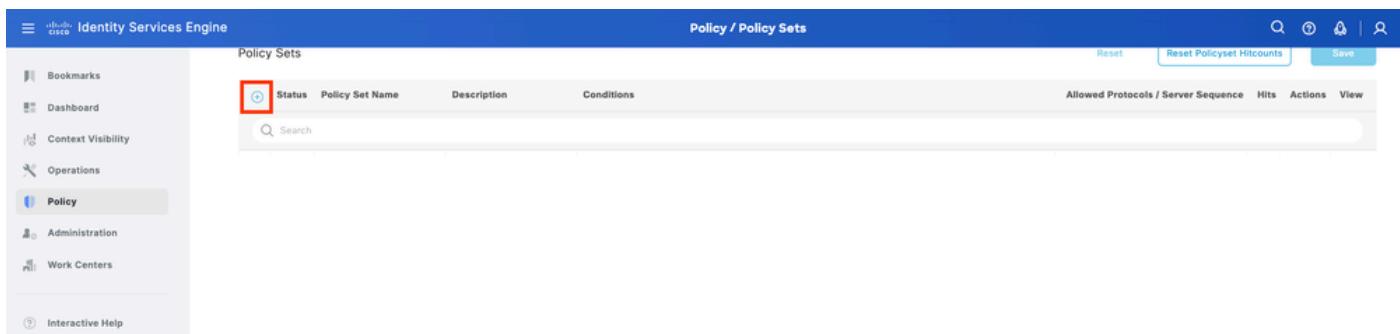
Tip: Aqui FINANCE_ADMIN_STR pode ser qualquer coisa; certifique-se de que o mesmo valor também seja colocado no lado do FMC.



The screenshot shows the 'Policy / Policy Elements' section of the Cisco Identity Services Engine. On the left, a sidebar includes 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy' (which is selected and highlighted in grey), 'Administration', 'Work Centers', and 'Interactive Help'. The main content area is titled 'Authorization Profiles > FMC_GUI_Finance' and shows an 'Authorization Profile' configuration. It includes fields for 'Name' (FMC_GUI_Finance), 'Description' (empty), 'Access Type' (ACCESS_ACCEPT), and a 'Network Device Profile' dropdown set to 'Cisco'. Below these are checkboxes for 'Service Template', 'Track Movement', 'Agentless Posture', and 'Passive Identity Tracking', all of which are checked. A 'Common Tasks' section and an 'Advanced Attributes Settings' section are also present. At the bottom, an 'Attributes Details' section shows 'Access Type = ACCESS_ACCEPT' and 'Class = FINANCE_ADMINISTRATOR'.

Adicionar um novo conjunto de políticas

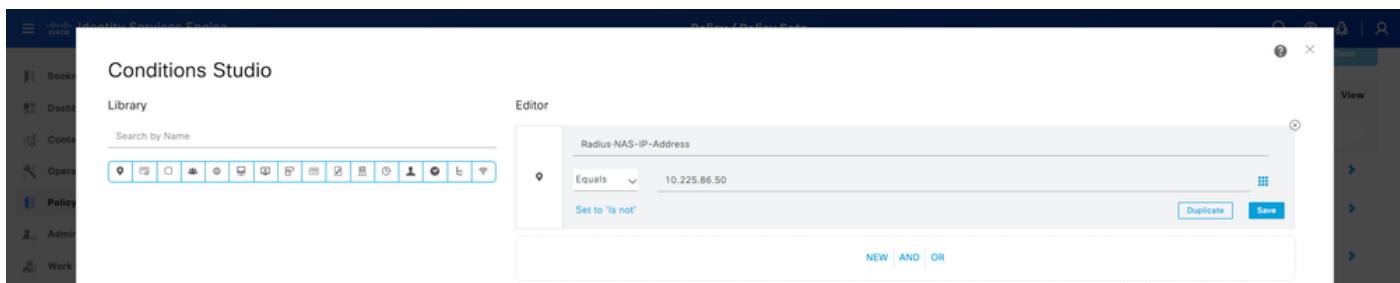
Etapa 7. Criar um conjunto de políticas correspondente ao endereço IP do FMC. Isso evita que outros dispositivos concedam acesso aos usuários. Navegue para Política > Conjuntos de políticas > ícone do sinal de adição no canto superior esquerdo.



The screenshot shows the 'Policy / Policy Sets' section of the Cisco Identity Services Engine. The left sidebar is identical to the previous screenshot. The main area is titled 'Policy Sets' and shows a table with columns for 'Status' (highlighted with a red box), 'Policy Set Name', 'Description', and 'Conditions'. A 'Search' bar is at the top of the table. To the right, there are buttons for 'Reset', 'Reset Policyset Hitcounts', 'Save', and 'Allowed Protocols / Server Sequence Hits Actions View'. The table is currently empty.

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.



The screenshot shows the 'Conditions Studio' interface. The left sidebar includes 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy' (selected), 'Administration', 'Work Centers', and 'Interactive Help'. The main area has a 'Library' section with a search bar and a 'Editor' section. The 'Editor' section shows a condition for 'Radius-NAS-IP-Address' with the operator 'Equals' and the value '10.225.86.50'. Below this, there is a link to 'Set to "Is not"'. At the bottom of the editor, there are buttons for 'Duplicate' and 'Save'. The status bar at the bottom of the window shows 'Conditions Studio' and 'Conditions Studio'.

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.

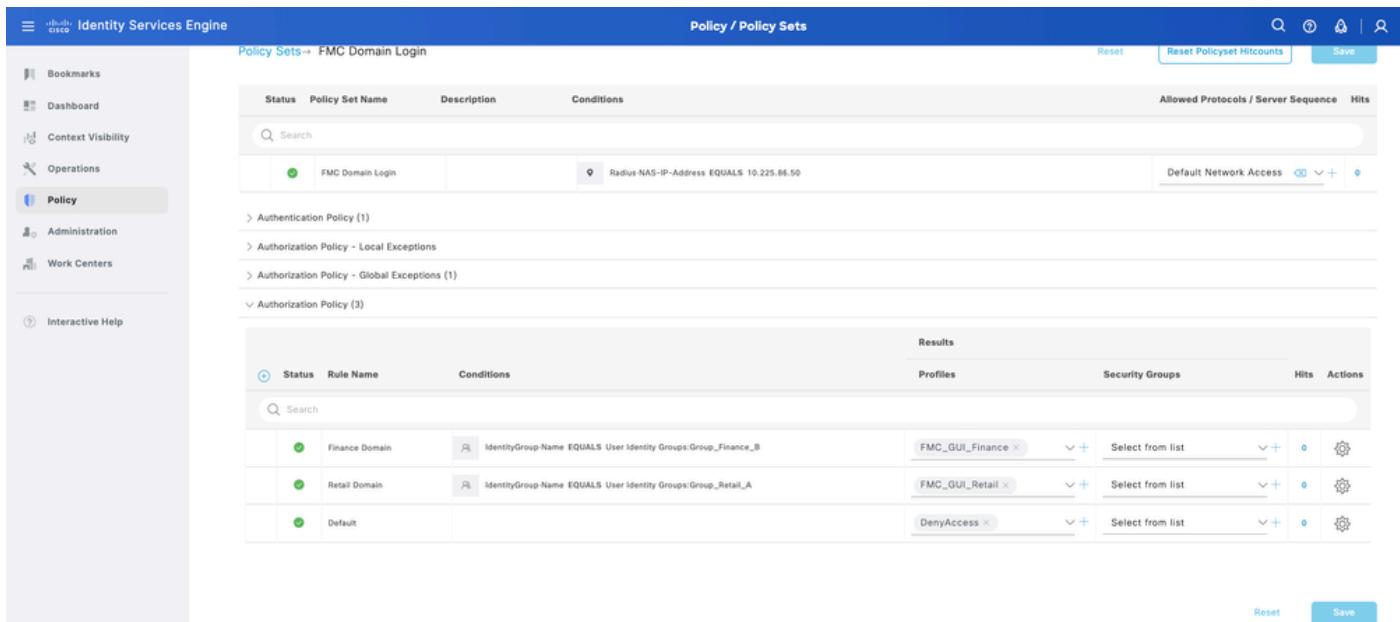
Expanda o menu Authorization Policy e pressione o ícone do sinal de adição para adicionar uma nova regra para permitir o acesso ao usuário com direitos administrativos. Dê-lhe um nome.



The screenshot shows the 'Policy / Policy Sets' page. On the left, a sidebar includes 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy' (which is selected and highlighted in blue), 'Administration', 'Work Centers', and 'Interactive Help'. The main area is titled 'Policy Sets' and shows a table with columns: Status, Policy Set Name, Description, and Conditions. A search bar is at the top of the table. The 'Conditions' section contains a single row with a green status icon, 'FMC Domain Login', and a condition 'Radius-NAS-IP-Address EQUALS 10.225.86.50'. To the right of the table are buttons for 'Allowed Protocols / Server Sequence', 'Hits', 'Actions', and 'View'. At the bottom right of the table is a 'Save' button, which is highlighted with a red box.

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.



The screenshot shows the 'Policy / Policy Sets' page with the 'FMC Domain Login' policy set selected. The left sidebar is identical to the previous screenshot. The main area shows the expanded 'Conditions' section. Under 'Conditions', there are three sections: 'Authentication Policy (1)', 'Authorization Policy - Local Exceptions', and 'Authorization Policy - Global Exceptions (1)'. Below these is a expanded 'Authorization Policy (3)' section. The 'Results' table shows three rules: 'Finance Domain' (Profile: FMC_GUI_Finance, Security Group: Select from list), 'Retail Domain' (Profile: FMC_GUI_Retail, Security Group: Select from list), and 'Default' (Profile: DenyAccess, Security Group: Select from list). The 'Save' button is highlighted with a red box at the bottom right of the table.

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.

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

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.

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=RETAIL_ADMIN_STR

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.

Firewall Management Center

System / Domains

Domain configuration is used in this session

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

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_financial. 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.

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_igO13NsO1DZN6QciDbrc0cwlaYWHMto:eagle/556377151/553|
"admin_financial" RADIUS Authentication OK
check_is_radius_member attrib match found: |Class=FINANCE_ADMIN_STR| ~ |Class=FINANCE_ADMIN_STR| *****
role_kee2eb18-e129-11df-a04a-42c66f0a3b36:

```

*Required Field

Cancel Test Save

Registros ativos do ISE

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

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint Pr	Authentication	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 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_igO13NsO1DZN6QciDbrc0cwl aYWHMto: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.