

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Autenticação externa para FMC](#)

[Autenticação externa para FTD](#)

[Topologia de rede](#)

[Configurar](#)

[Configuração do ISE](#)

[Configuração do FMC](#)

[Configuração de FTD](#)

[Verificar](#)

Introdução

Este documento descreve um exemplo de configuração de autenticação externa para Secure Firewall Management Center e Firewall Threat Defense.

Pré-requisitos

Requisitos

Recomenda-se ter conhecimento destes tópicos:

- Configuração inicial do Cisco Secure Firewall Management Center via GUI e/ou shell.
- Configurando políticas de autenticação e autorização no ISE.
- Conhecimento RADIUS básico.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- vFMC 7.2.5
- vFTD 7.2.5.
- ISE 3.2

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

Quando você habilita a autenticação externa para usuários administrativos e de gerenciamento do sistema do Firewall Seguro, o dispositivo verifica as credenciais do usuário com um servidor LDAP ou RADIUS, conforme especificado em um objeto de autenticação externa.

Os objetos de autenticação externa podem ser utilizados pelos dispositivos FMC e FTD. Você pode compartilhar o mesmo objeto entre diferentes tipos de dispositivo/dispositivo ou criar objetos separados.

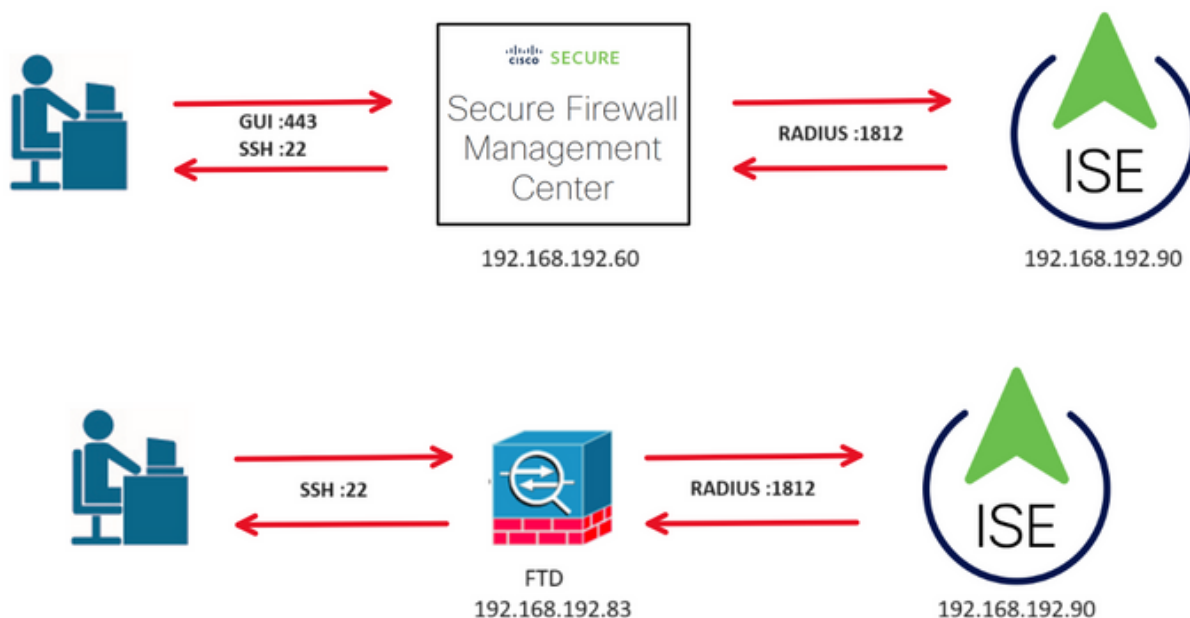
Autenticação externa para FMC

Você pode configurar vários objetos de autenticação externa para acesso à interface da Web. Somente um objeto de autenticação externa pode ser usado para acesso CLI ou shell.

Autenticação externa para FTD

Para o FTD, você pode ativar apenas um objeto de autenticação externa.

Topologia de rede



Configurar

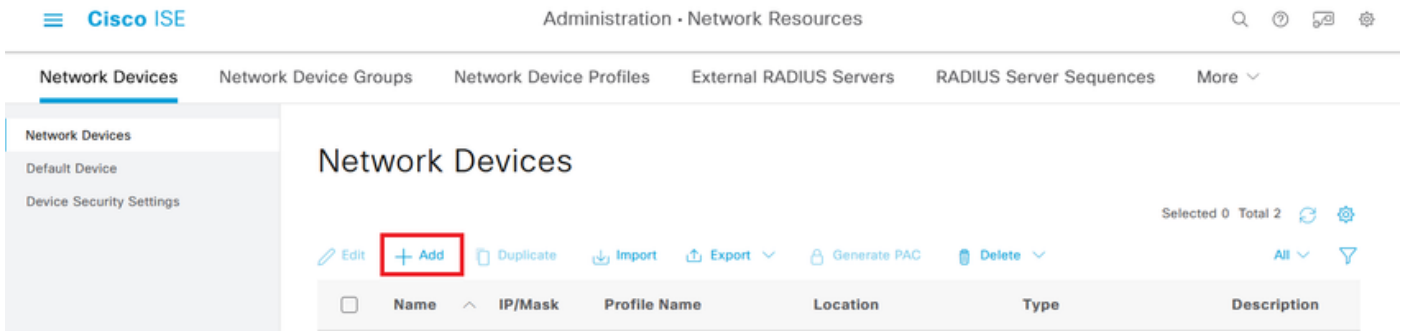
Configuração do ISE



Observação: há várias maneiras de configurar a autenticação do ISE e as políticas de autorização para dispositivos de acesso à rede (NAD), como o FMC. O exemplo descrito neste documento é um ponto de referência no qual criamos dois perfis (um com direitos de administrador e outro somente leitura) e pode ser adaptado para atender às linhas de base para acessar sua rede. Uma ou mais políticas de autorização podem ser definidas no ISE com valores de atributo RADIUS retornados ao FMC que são mapeados para um grupo de usuários local definido na configuração de política do sistema do FMC.



Etapa 1. Adicione um novo dispositivo de rede. Navegue até o ícone de hambúrguer localizado no canto superior esquerdo >Administração > Recursos de rede > Dispositivos de rede > +Adicionar.

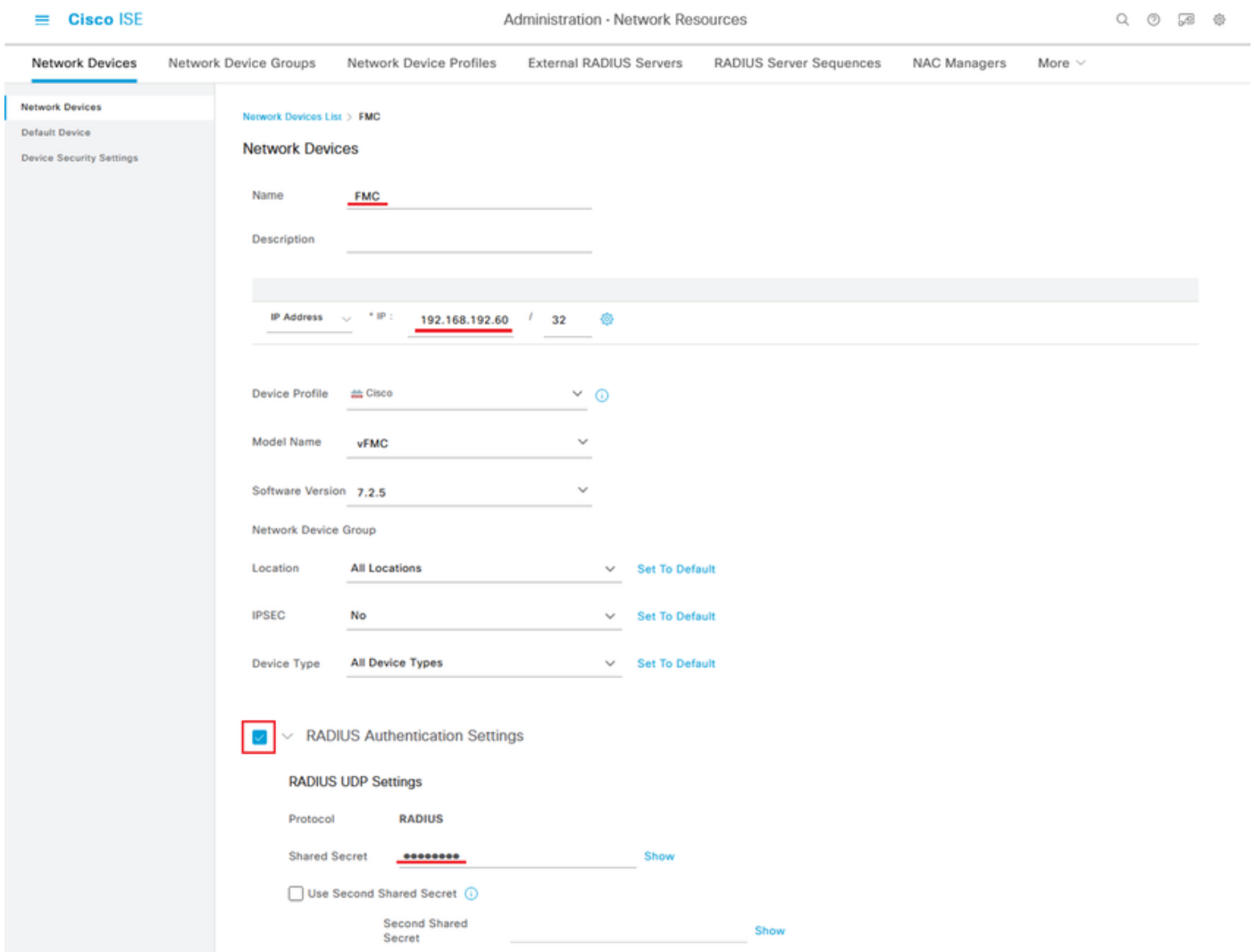


Etapa 2. Atribua um Name ao objeto do dispositivo de rede e insira o endereço IP do FMC.

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.



Etapa 2.1. Repita o mesmo procedimento para adicionar o FTD.

Atribua um Name ao objeto do dispositivo de rede e insira o endereço IP do FTD.

Marque a caixa de seleção RADIUS e defina um segredo compartilhado.

Quando terminar, clique em Salvar.

The screenshot shows the Cisco ISE Administration interface for configuring a Network Device. The device name is 'FTD' and its IP address is '192.168.192.83/32'. The configuration includes a Device Profile of 'Cisco', Model Name 'vFTD', and Software Version '7.2.5'. The RADIUS Authentication Settings are expanded, showing the RADIUS UDP Settings with the Protocol set to 'RADIUS' and a Shared Secret field. A red box highlights the checked checkbox for 'RADIUS Authentication Settings'.

Etapa 2.3. A opção Validate both devices é mostrada em Network Devices.

The screenshot shows the Cisco ISE Administration interface for a list of Network Devices. The table below shows the details of the devices:

Name	IP/Mask	Profile Name	Location	Type	Description
FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

Etapa 3. Crie os Grupos de Identidade de Usuário necessários. Navegue até o ícone de hambúrguer localizado no canto superior esquerdo > Administração > Gerenciamento de

Identities > Grupos > Grupos de Identidades de Usuário > + Adicionar

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is 'Identities > Grupos > Grupos de Identidades de Usuário > + Adicionar'. The main page is titled 'User Identity Groups'. On the left, there is a sidebar with 'Identity Groups' and a search bar. Below it, there are two expandable sections: 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area shows a table with columns 'Name' and 'Description'. Above the table, there are action buttons: 'Edit', '+ Add' (highlighted with a red box), 'Delete', 'Import', and 'Export'. The top right corner shows 'Selected 0 Total 11' and some utility icons.

Etapa 4. Dê um nome a cada grupo e clique em Salvar individualmente. Neste exemplo, estamos criando um grupo para usuários Administradores e outro para usuários Somente leitura. Primeiro, crie o grupo para o usuário com direitos de Administrador.

The screenshot shows the 'Identity Group' configuration page for 'FMC and FTD admins'. The breadcrumb navigation is 'User Identity Groups > FMC and FTD admins'. The page title is 'Identity Group'. There are two input fields: '* Name' with the value 'FMC and FTD admins' (underlined in red) and 'Description' with the value 'FMC and FTD admins ISE local.'. At the bottom, there are two buttons: 'Save' (highlighted with a red box) and 'Reset'.


Etapa 4.1. Crie o segundo grupo para o usuário ReadOnly.

The screenshot shows the 'Identity Group' configuration page for 'FMC and FTD ReadOnly'. The breadcrumb navigation is 'User Identity Groups > FMC and FTD ReadOnly'. The page title is 'Identity Group'. There are two input fields: '* Name' with the value 'FMC and FTD ReadOnly' (underlined in red) and 'Description' with the value 'FMC and FTD ReadOnly.'. At the bottom, there are two buttons: 'Save' (highlighted with a red box) and 'Reset'.

Etapa 4.2. Validar ambos os grupos são mostrados na Lista de grupos de identidade do usuário. Use o filtro para localizá-los facilmente.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The navigation menu includes Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'Groups' section is active, showing a sidebar with 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups' and displays a table with two entries: 'fmc' and 'FMC and FTD admins ISE local'. The '+ Add' button is highlighted with a red box.

Name	Description
fmc	
<input type="checkbox"/> FMC and FTD ReadOnly	FMC and FTD ReadOnly
<input type="checkbox"/> FMC and FTD admins	FMC and FTD admins ISE local.

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 Cisco ISE Administration interface for Identity Management. The navigation menu includes Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'Identities' section is active, showing a sidebar with 'Users' and 'Latest Manual Network Scan Res...'. The main content area is titled 'Network Access Users' and displays a table with columns: Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Adn. The '+ Add' button is highlighted with a red box.

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Adn
No data available							

Etapa 5.1. Primeiro, crie o usuário com direitos de Administrador. Atribuir-lhe um nome, uma senha e os administradores do FMC e do FTD do grupo.

Users
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_admin

Status Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration

Never Expires

Password Re-Enter Password

* Login Password ●●●●●●●● ●●●●●●●● [Generate Password](#)

Enable Password [Generate Password](#)

Users
Latest Manual Network Scan Res...

User Groups

FMC and FTD admins [+](#)

[Submit](#) [Cancel](#)

Etapa 5.2. Adicione o usuário com direitos ReadOnly. Atribua um nome, uma senha e o grupo FMC e FTD ReadOnly.

Identities Groups External Identity Sources Identity Source Sequences Settings

Users
Latest Manual Network Scan Res...

Network Access Users List > New Network Access User

Network Access User

* Username firewall_readuser

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 ⓘ

Identities Groups External Identity Sources Identity Source Sequences Settings

Users
Latest Manual Network Scan Res...

User Groups

FMC and FTD ReadOnly ⓘ +

Etapa 6. Crie o perfil de autorização para o usuário Admin.

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 e, em Configurações avançadas de atributos, adicione um Raio > Classe—[25] com o valor Administrador e clique em Enviar.

The screenshot shows the Cisco ISE web interface for configuring a Policy Element. The breadcrumb trail is: Policy > Policy Elements > Results > Authorization Profiles > FMC and FTD Admins. The left sidebar contains a navigation menu with categories: Authentication (Allowed Protocols), Authorization (Authorization Profiles, Downloadable ACLs), Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profile' and contains the following configuration fields:

- Name:** FMC and FTD Admins
- Description:** (Empty text box)
- Access Type:** ACCESS_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (Empty dropdown)

Dictionaryes Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Advanced Attributes Settings

⋮ Radius:Class = Administrator - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

Passo 7. Repita a etapa anterior para criar o perfil de autorização para o usuário somente leitura. Desta vez, crie a classe Radius com o valor ReadUser em vez de Administrator.

Dictionaryes Conditions **Results**

Authentication >

Allowed Protocols

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name FMC and FTD ReadUser

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Navigation tabs: Dictionaries, Conditions, **Results**

Left sidebar menu:

- Authentication >
- Authorization ▾
 - Authorization Profiles**
 - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Main content area:

Advanced Attributes Settings

⋮ Radius:Class ▾ = ReadUser ▾ - +

Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

Buttons: **Submit** (highlighted with a red box), Cancel

Etapa 8. Crie um conjunto de políticas correspondente ao endereço IP do FMC. Isso evita que outros dispositivos concedam acesso aos usuários.









Navegue até
> Policy > Policy Sets >



ícone colocado no canto superior esquerdo.

Cisco ISE Policy - Policy Sets

Policy Sets Reset Reset Policyset Hitcounts Save

 Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	Default	Default policy set		Default Network Access  	45	 	

Reset Save

Etapa 8.1. Uma nova linha é colocada na parte superior dos 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.

Adicione uma segunda condição com a conjunção OR para incluir o endereço IP do FTD.

Clique em Usar para manter as alterações e sair do editor.

Conditions Studio

Library

Search by Name

5G
Catalyst_Switch_Local_Web_Authentication
Source FMC
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access

Editor

Radius-NAS-IP-Address
Equals 192.168.192.60

OR

Radius-NAS-IP-Address
Equals 192.168.192.83

NEW AND OR

Set to 'is not'

Duplicate Save

Close Use

Etapa 8.2. Depois de concluído, pressione Salvar.

Cisco ISE

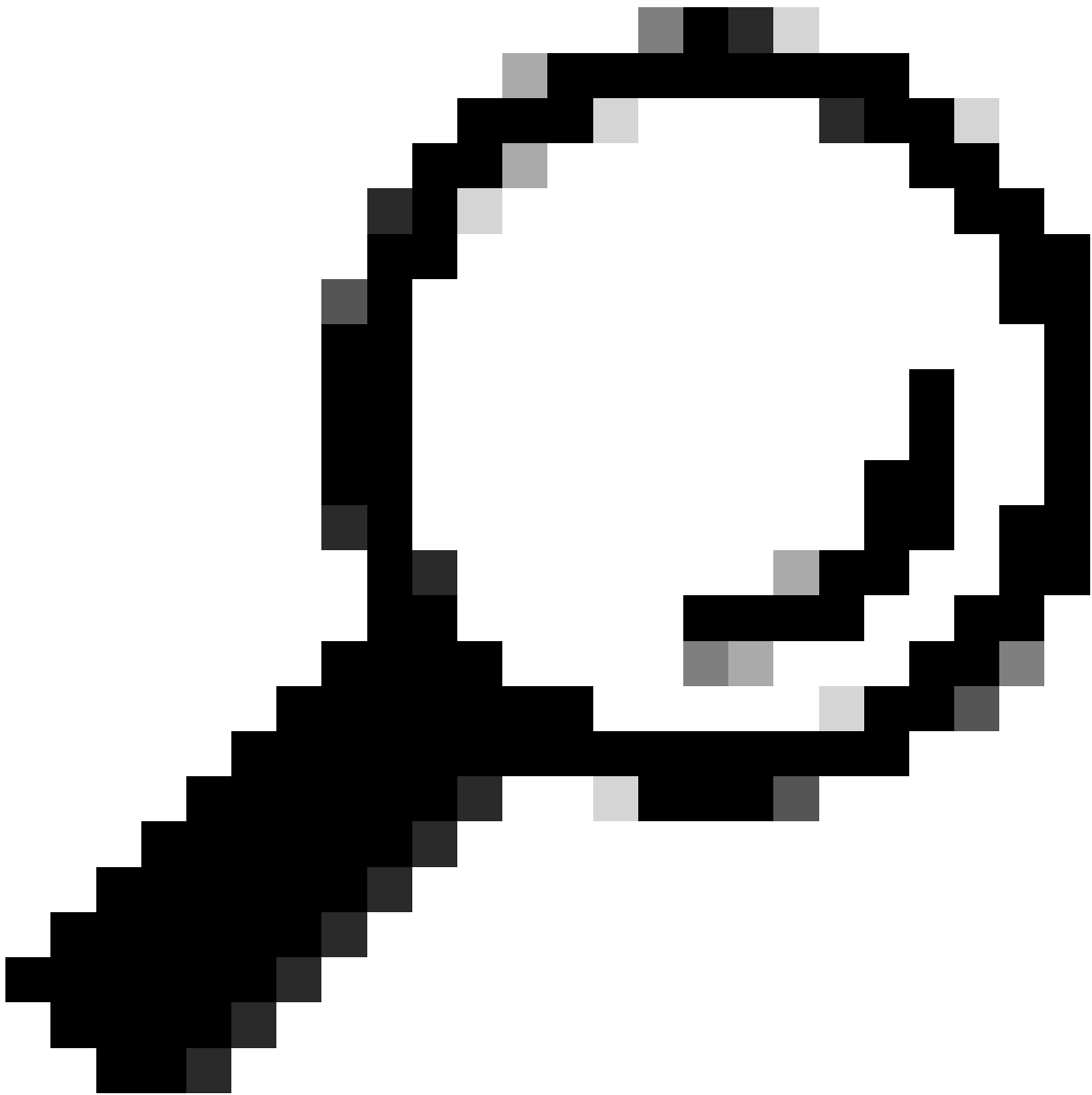
Policy · Policy Sets

Policy Sets

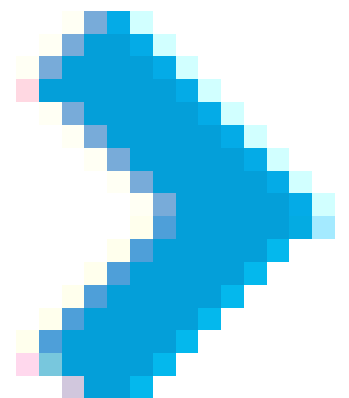
Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access 0	0	⚙️ ➔	➔
✓	Default	Default policy set		Default Network Access 0	0	⚙️ ➔	➔

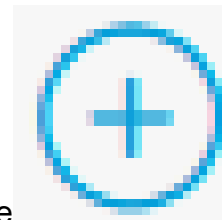
Reset Save



Dica: para este exercício, permitimos a lista Default Network Access Protocols. Você pode criar uma nova lista e restringi-la conforme necessário.



Etapa 9. Visualize o novo conjunto de políticas, pressionando o ícone colocado no final da linha.



Expanda o menu Authorization Policy (Diretiva de autorização) e pressione o ícone para adicionar uma nova regra para permitir o acesso ao usuário com direitos administrativos.

Dê-lhe um nome.

Defina as condições para que correspondam ao Grupo de Identidade de Dicionário com Nome de Atributo Igual a Grupos de Identidade de Usuário: administradores FMC e FTD (o nome do grupo criado na Etapa 4) e clique em Usar.

The screenshot shows the 'Conditions Studio' application. On the left is the 'Library' pane with a search bar and a list of conditions. The 'Editor' pane on the right is active, showing a configuration for 'IdentityGroup-Name'. The condition 'User Identity Groups:FMC and FTD admins' is selected. Below the editor, there are buttons for 'NEW', 'AND', and 'OR'. At the bottom right, there is a 'Close' button and a 'Use' button, which is highlighted with a red rectangular box.

Etapa 10. Clique no ícone



para adicionar uma segunda regra para permitir o acesso ao usuário com direitos somente leitura.

Dê-lhe um nome.

Defina as condições para que correspondam ao Grupo de Identidade de Dicionário com Nome de Atributo Igual a Grupos de Identidade de Usuário: FMC e FTD ReadOnly (o nome do grupo criado na Etapa 4) e clique em Usar.

Conditions Studio

Library

Search by Name



- 5G
- BYOD_Is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices

Editor

IdentityGroup-Name

Equals User Identity Groups:FMC and FTD
ReadOnly

Set to 'Is not'

Duplicate Save

NEW AND OR

Close



Etapa 11. Defina os Perfis de autorização para cada regra e pressione Salvar.

Cisco ISE Policy - Policy Sets

Policy Sets--> FMC and FTD Access

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	FMC and FTD Access	Management Access	OR Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83	Default Network Access	0

> Authentication Policy (1)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
v Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Profiles	Security Groups			
✓	FMC and FTD read user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD ReadOnly	FMC and FTD ReadUser	Select from list	0	⚙️	
✓	FMC and FTD admin user access	IdentityGroup-Name EQUALS User Identity Groups:FMC and FTD admins	FMC and FTD Admins	Select from list	0	⚙️	
✓	Default		DenyAccess	Select from list	0	⚙️	

Reset

Configuração do FMC

Etapa 1. Crie o Objeto de Autenticação Externa em System > Users > External Authentication > + Add External Authentication Object.

Etapa 2. Selecione RADIUS como Método de Autenticação.

Em External Authentication Object, forneça um Name para o novo objeto.

Em seguida, na configuração Primary Server, insira o endereço IP do ISE e a mesma chave secreta RADIUS usada na etapa 2 da configuração do ISE.

Etapa 3. Insira os valores dos atributos RADIUS Class que foram configurados nas Etapas 6 e 7 da Configuração do ISE: Administrator e ReadUser para firewall_admin e firewall_readuser, respectivamente.

RADIUS-Specific Parameters

Timeout (Seconds)	<input type="text" value="30"/>
Retries	<input type="text" value="3"/>
Access Admin	<input type="text"/>
Administrator	<input type="text" value="Class=Administrator"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text"/>
Network Admin	<input type="text"/>
Security Analyst	<input type="text"/>
Security Analyst (Read Only)	<input type="text" value="Class=ReadUser"/>
Security Approver	<input type="text"/>
Threat Intelligence Director (TID) User	<input type="text"/>
Default User Role	<input type="text" value="Access Admin
Administrator
Discovery Admin
External Database User"/>

To specify the default user role if user is not found in any group



Observação: o intervalo de tempo limite é diferente para o FTD e o FMC, portanto, se você compartilhar um objeto e alterar o valor padrão de 30 segundos, certifique-se de não exceder um intervalo de tempo limite menor (1 a 300 segundos) para dispositivos FTD. Se você definir o tempo limite para um valor mais alto, a configuração do RADIUS de defesa contra ameaças não funcionará.

Etapa 4. Preencha a Administrator CLI Access User List em CLI Access Filter com os nomes de usuário com permissão para obter acesso à CLI.

Clique em Salvar quando terminar.

CLI Access Filter
 (For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

Etapa 5. Ative o novo objeto. Defina-o como o método de autenticação Shell para FMC e clique em Save and Apply (Salvar e aplicar).

Firewall Management Center
 System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ ⓘ admin ▾ 🔒 **SECURE**

Users User Roles External Authentication Single Sign-On (SSO)

Default User Role: **None** Shell Authentication Enabled (ISE_Radius) + Add External Authentication Object

Name	Method	Enabled	
1. ISE_Radius	RADIUS	<input checked="" type="checkbox"/>	

Configuração de FTD

Etapa 1. Na GUI do FMC, navegue para Devices > Platform Settings. Edite sua política atual ou crie uma nova se não tiver nenhuma atribuída ao FTD ao qual você precisa acessar. Ative o servidor RADIUS em External Authentication e clique em Save.

Firewall Management Center
 Devices / Platform Settings Editor

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ ⓘ admin ▾ 🔒 **SECURE**

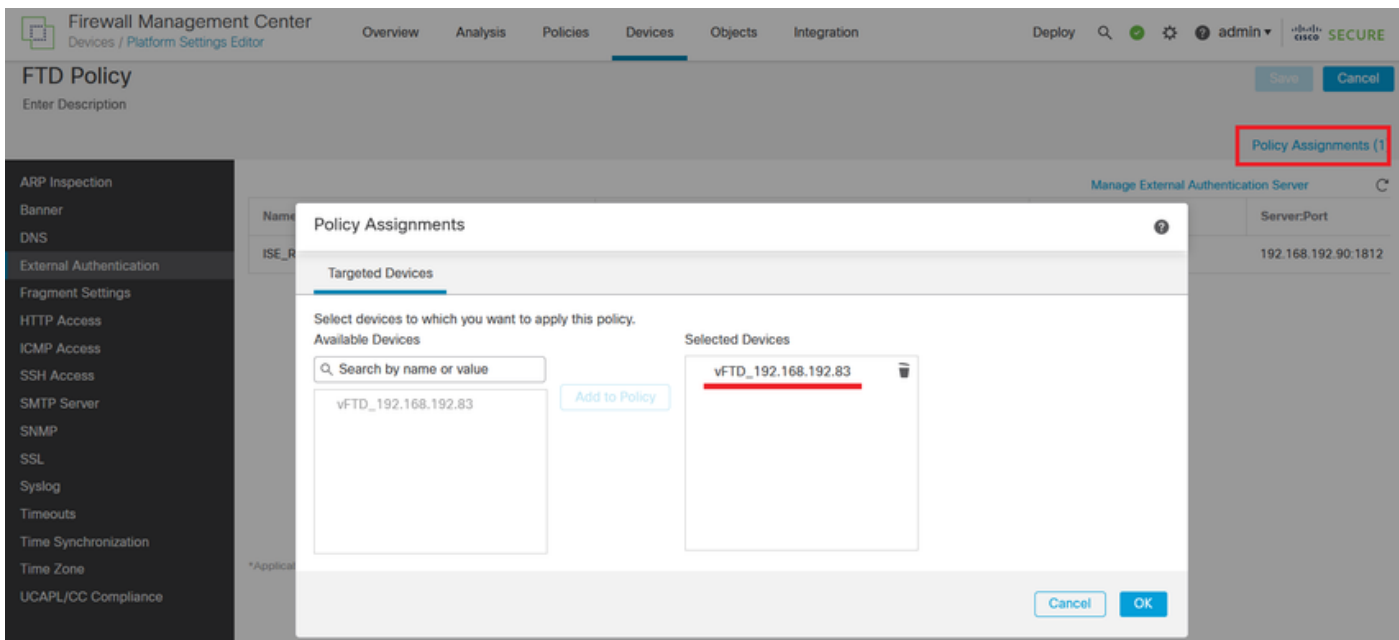
FTD Policy
 Enter Description

You have unsaved changes

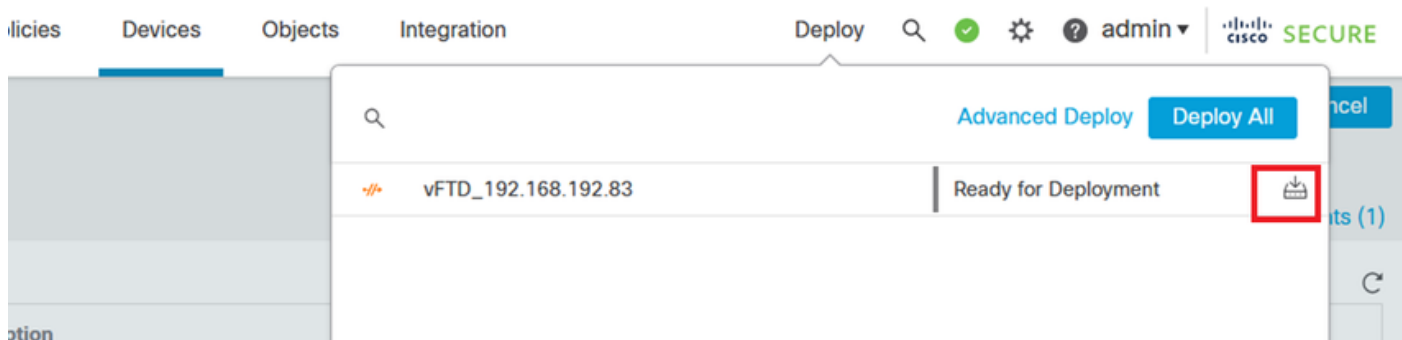
Policy Assignments (1)

Name	Description	Method	Server/Port	Encryption	Enabled
ISE_Radius		RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

Etapa 2. Verifique se o FTD ao qual você precisa obter acesso está listado em Atribuições de política como um dispositivo selecionado.



Etapa 3. Implante as alterações.



Verificar

- Teste se a nova implantação está funcionando corretamente.
- Na GUI do FMC, navegue até as configurações do servidor RADIUS e vá até a seção Additional Test Parameters.
- Insira um nome de usuário e uma senha para o usuário do ISE e clique em Testar.



- Um teste bem-sucedido mostra uma mensagem verde Teste de êxito concluído na parte superior da janela do navegador.



Success
Test Complete.

External Authentication Object

Authentication Method

Name *

- Você pode expandir Details na Test Output para obter mais informações.

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

Test Output

Show Details

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQqxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_cNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

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.