

# Integração do sistema FireSIGHT com ISE para autenticação de usuário RADIUS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração do ISE](#)

[Configurando dispositivos de rede e grupos de dispositivos de rede](#)

[Configurando a política de autenticação do ISE:](#)

[Adicionando um usuário local ao ISE](#)

[Configurando a política de autorização do ISE](#)

[Configuração de política do sistema Sourcefire](#)

[Ativar autenticação externa](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve as etapas de configuração necessárias para integrar uma autenticação de usuário do Cisco FireSIGHT Management Center (FMC) ou Firepower Managed Device com o Cisco Identity Services Engine (ISE) para Remote Authentication Dial In User Service (RADIUS).

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração inicial do FireSIGHT System e do dispositivo gerenciado via GUI e/ou shell
- Configuração de políticas de autenticação e autorização no ISE
- Conhecimento RADIUS básico

### Componentes Utilizados

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

- Cisco ASA v9.2.1
- Módulo ASA FirePOWER v5.3.1
- ISE 1.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

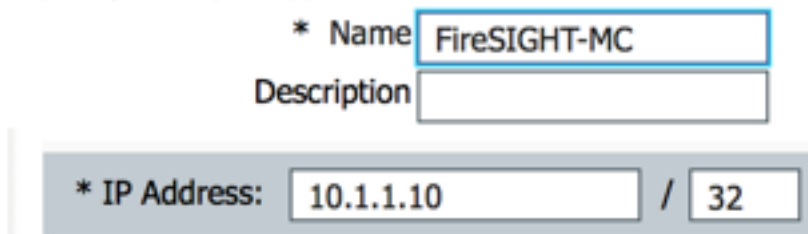
### Configuração do ISE

**Tip:** Há várias maneiras de configurar as políticas de autenticação e autorização do ISE para suportar a integração com os NAD (Network Access Devices, dispositivos de acesso à rede), como a Sourcefire. O exemplo abaixo é uma forma de configurar a integração. A configuração de exemplo é um ponto de referência e pode ser adaptada de acordo com as necessidades da implantação específica. Observe que a configuração de autorização é um processo de duas etapas. Uma ou mais políticas de autorização serão definidas no ISE com o ISE retornando pares de valores de atributos RADIUS (pares av) ao FMC ou dispositivo gerenciado. Esses pares av são mapeados para um grupo de usuários local definido na configuração da política do sistema FMC.

### Configurando dispositivos de rede e grupos de dispositivos de rede

- Na GUI do ISE, navegue para **Administration > Network Resources > Network Devices**. Clique em **+Adicionar** para adicionar um novo NAD (Network Access Device, dispositivo de acesso à rede). Forneça um nome descritivo e um endereço IP do dispositivo. O FMC é definido no exemplo abaixo.


#### Network Devices



\* Name

Description

\* IP Address:  /

- Em **Network Device Group**, clique na **seta laranja** ao lado de **All Device Types**. Clique no  ícone e selecione **Create New Network Device Group**. No exemplo de captura de tela a seguir, o Tipo de dispositivo Sourcefire foi configurado. Este tipo de dispositivo será referenciado na definição da regra de política de autorização em uma etapa posterior. Click **Save**.

Create New Network Device Group... ✕

### Network Device Groups

\* Parent

\* Name

Description

\* Type

- Clique na **seta laranja** novamente e selecione o grupo de dispositivos de rede configurado na etapa acima

\* Network Device Group

Location

Device Type

- Marque a caixa ao lado de **Configurações de autenticação**. Insira a chave secreta compartilhada RADIUS que será usada para este NAD. Observe que a mesma chave secreta compartilhada será usada novamente mais tarde ao configurar o servidor RADIUS no FireSIGHT MC. Para revisar o valor da chave de texto simples, clique no botão **Mostrar**.  
Click **Save**.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  ⓘ

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

- Repita as etapas acima para todos os FireSIGHT MCs e dispositivos gerenciados que exigirão autenticação/autorização de usuário RADIUS para acesso à GUI e/ou shell.

### Configurando a política de autenticação do ISE:

- Na GUI do ISE, navegue até **Policy > Authentication**. Se estiver usando Conjuntos de políticas, navegue para **Política > Conjuntos de políticas**. O exemplo abaixo é extraído de uma implantação do ISE que usa as interfaces de política de autenticação e autorização padrão. A lógica da regra de autenticação e autorização é a mesma independentemente da abordagem de configuração.

- A **regra padrão (se não houver correspondência)** será usada para autenticar solicitações RADIUS de NADs onde o método em uso não é MAC Authentication Bypass (MAB) ou 802.1X. Conforme configurado por padrão, essa regra procurará contas de usuário na fonte de identidade **interna do ISE**. Essa configuração pode ser modificada para se referir a uma fonte de identidade externa, como Active Directory, LDAP, etc, conforme definido em **Administração > Gerenciamento de identidade > Fontes de identidade externas**. Por uma questão de simplicidade, este exemplo definirá as contas de usuário localmente no ISE para que nenhuma modificação adicional na política de autenticação seja necessária.

#### Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type  Simple  Rule-Based

<input checked="" type="checkbox"/>	MAB	: If	Wired_MAB OR Wireless_MAB	Allow Protocols :	Default Network Access	and
<input checked="" type="checkbox"/>	Default	: use	Internal Endpoints			
<input checked="" type="checkbox"/>	Dot1X	: If	Wired_802.1X OR Wireless_802.1X	Allow Protocols :	Default Network Access	and
<input checked="" type="checkbox"/>	Default	: use	Guest_Portal_Sequence			
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols :	Default Network Access	and use :	Internal Users	

#### Adicionando um usuário local ao ISE

- Navegue até **Administração > Gerenciamento de identidades > Identidades > Usuários**. Clique em Add. Insira um nome de usuário e uma senha significativos. Na seleção **Grupos de usuários**, selecione um nome de grupo existente ou clique no  **sinal verde +** para adicionar um novo grupo. Neste exemplo, o usuário "sfadmin" é atribuído ao grupo personalizado "Sourcefire Administrator". Este grupo de usuários será vinculado ao perfil de autorização definido na etapa **Configuração da política de autorização do ISE** abaixo. Click **Save**.

▼ Network Access User

\* Name

Status  Enabled ▼

Email

---

▼ Password

\* Password  Need help with password policy ? ⓘ

\* Re-Enter Password

---

▼ User Information

First Name

Last Name

---

▼ Account Options

Description

Change password on next login

---

▼ User Groups

▼ - +

## Configurando a política de autorização do ISE

- Navegue até **Política > Elementos de política > Resultados > Autorização > Perfis de autorização**. Clique no  **sinal verde +**  para adicionar um novo perfil de autorização.
- Forneça um nome descritivo, como Sourcefire Administrator. Selecione **ACCESS\_ACCEPT** para o **Tipo de acesso**. Em **Tarefas comuns**, role até a parte inferior e marque a caixa ao lado de **ASA VPN**. Clique na **seta laranja** e selecione **InternalUser:IdentityGroup**. Click **Save**.

**Tip:** Como este exemplo usa o repositório de identidade de usuário local do ISE, a opção de grupo InternalUser:IdentityGroup é usada para simplificar a configuração. Se estiver usando um repositório de identidade externo, o atributo de autorização de VPN ASA ainda será usado, no entanto, o valor a ser devolvido ao dispositivo Sourcefire será configurado manualmente. Por exemplo, digitar manualmente Administrador na caixa suspensa VPN ASA resultará em um valor de par av classe 25 de Class = Administrador enviado ao dispositivo Sourcefire. Esse valor pode ser mapeado para um grupo de usuários do sourcefire como parte da configuração da política do sistema. Para usuários internos, qualquer método de configuração é aceitável.

## Exemplo de usuário interno

\* Name

Description

\* Access Type

Service Template

### ▼ Common Tasks

MACSEC Policy

NEAT

Web Authentication (Local Web Auth)

Airespace ACL Name

ASA VPN

### ▼ Advanced Attributes Settings

=  - +

### ▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = InternalUser:IdentityGroup

## Exemplo de usuário externo

Advanced Attributes Settings

Select an item = [ ] - +

Attributes Details

Access Type = ACCESS\_ACCEPT  
Class = Administrator

- Navegue até **Política > Autorização** e configure uma nova política de autorização para as sessões de administração do Sourcefire. O exemplo abaixo usa a condição **DEVICE:Device Type** para corresponder ao tipo de dispositivo configurado na Seção **Configuração de Dispositivos de Rede e Grupos de Dispositivos de Rede** acima. Essa política é então associada ao perfil de autorização do Sourcefire Administrator configurado acima. Click **Save**.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
✓	Sourcefire Administrator	if DEVICE:Device Type EQUALS All Device Types#Sourcefire	then Sourcefire Administrator
✓	CWA-PSN1	if Network Access:ISE Host Name EQUALS ise12-psn1	then CWA-PSN1
✓	CWA-PSN2	if Network Access:ISE Host Name EQUALS ise12-psn2	then CWA-PSN2

### Configuração de política do sistema Sourcefire

- Faça login no FireSIGHT MC e navegue para **System > Local > User Management**. Clique na guia **Autenticação de login**. Clique no botão **+ Create Authentication Object (Criar objeto de autenticação)** para adicionar um novo servidor RADIUS para autenticação/autorização do usuário.
- Selecione **RADIUS** para o **Método de autenticação**. Digite um nome descritivo para o servidor RADIUS. Insira o **Host Name/IP Address** e **RADIUS Secret Key**. A chave secreta deve corresponder à chave previamente configurada no ISE. Opcionalmente, insira um

servidor ISE de backup **Nome do host/endereço IP**, se houver.

## Authentication Object

Authentication Method	<input type="text" value="RADIUS"/>
Name *	<input type="text" value="ISE"/>
Description	<input type="text"/>

## Primary Server

Host Name/IP Address *	<input type="text" value="10.1.1.254"/>
Port *	<input type="text" value="1812"/>
RADIUS Secret Key	<input type="password" value="....."/>

## Backup Server (Optional)

Host Name/IP Address	<input type="text"/>
Port	<input type="text" value="1812"/>
RADIUS Secret Key	<input type="password"/>

- Na seção **RADIUS-Specific Parameters**, digite a string de par av Class-25 na caixa de texto ao lado do nome do grupo local Sourcefire a ser correspondido para acesso à GUI. Neste exemplo, o valor Class=User Identity Groups:Sourcefire Administrator é mapeado para o grupo Sourcefire Administrator. Esse é o valor que o ISE retorna como parte do ACCESS-ACCEPT. Opcionalmente, selecione uma **Função de Usuário Padrão** para usuários autenticados que não têm grupos de Classe 25 atribuídos. Clique em **Save** para salvar a configuração ou continue na seção Verify (Verificar) abaixo para testar a autenticação com o ISE.



## 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=User Identity&lt;br/&gt;Groups:Sourcefire 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"/>
Security Approver	<input type="text"/>
Default User Role	<input type="text" value="Access Admin&lt;br/&gt;Administrator&lt;br/&gt;Discovery Admin&lt;br/&gt;External Database User"/>

- Em **Filtro de Acesso Shell**, insira uma lista separada por vírgulas de usuários para restringir sessões shell/SSH.

## Shell Access Filter

Administrator Shell Access User List	<input type="text" value="user1, user2, user3"/>
--------------------------------------	--

## Ativar autenticação externa

Finalmente, conclua estes passos para habilitar a autenticação externa no FMC:

1. Navegar para **Sistema > Local > Política do sistema**.
2. Selecionar **Autenticação externa** no painel esquerdo.
3. Alterar o *status* para **Habilitado** (desabilitado por padrão).
4. Ative o servidor RADIUS ISE adicionado.
5. Salve a diretiva e reaplique-a no dispositivo.

Access Control Preferences

Access List

Audit Log Settings

Dashboard

Database

DNS Cache

Email Notification

► **External Authentication**

Intrusion Policy Preferences

Language

Login Banner

Network Analysis Policy Preferences

SNMP

STIG Compliance

Time Synchronization

User Interface

Vulnerability Mapping

Save Policy and Exit Cancel

Status Enabled

Default User Role

Access Admin  
Administrator  
Discovery Admin  
External Database User

Shell Authentication Disabled

CAC Authorization Disabled

Name	Description	Method	Server:Port	Encryption	
ISE		RADIUS	10.1.1.254:1812	no	<input checked="" type="checkbox"/>

## Verificar

- Para testar a autenticação do usuário em relação ao ISE, role para baixo até a seção **Additional Test Parameters** e insira um nome de usuário e uma senha para o usuário do ISE. Clique em **Testar**. Um teste bem-sucedido resultará em uma mensagem verde **Êxito: Teste concluído** na parte superior da janela do navegador.

**Additional Test Parameters**

User Name sfadmin

Password .....

\*Required Field

Save Test Cancel

- Para ver os resultados da autenticação de teste, vá para a seção **Saída de teste** e clique na seta **preta** ao lado de **Mostrar detalhes**. Na captura de tela do exemplo abaixo, observe o "radiusauth - response: |Class=User Identity Groups:Sourcefire Administrator|" valor recebido do ISE. Isso deve corresponder ao valor Class associado ao grupo local Sourcefire configurado no FireSIGHT MC acima. Clique **Save**.

## Test Output

Show Details

```
check_auth_radius: szUser: sfadmin
RADIUS config file: /var/tmp/OPMTH1T3qLx/radiusclient_0.conf
radiusauth - response: [User-Name=sfadmin]
radiusauth - response: [State=ReauthSession:0ac9e8cb0000006539F4896]
radiusauth - response: [Class=User Identity Groups:Sourcefire Administrator]
radiusauth - response: [Class=CACS:0ac9e8cb0000006539F4896:ise12-psn1/191969386/7]
"sfadmin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=User Identity Groups:Sourcefire Administrator] - [Class=User Identity Groups:Sourcefire Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

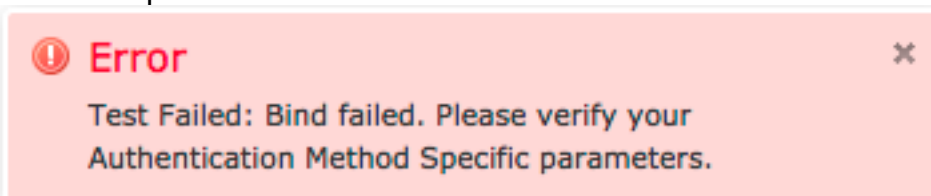
User Test


- Na GUI do ISE Admin, navegue até **Operations > Authentications** para verificar o sucesso ou a falha do teste de autenticação do usuário.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server	Event
2014-06-16 18:41:55.940	✓		0	sfadmin			Sourcefire3D-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:41:24.947	✗		0	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:41:10.088	✗		0	sfadmin			Sourcefire3D-DC			User Identity Groups...		ise12-psn1	Authentication f...
2014-06-16 18:46:00.856	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:44:55.751	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:41:02.876	✓		0	sfadmin			SFR-DC		Sourcefire_Admin	User Identity Groups...	NotApplicable	ise12-psn1	Authentication ...
2014-06-16 18:39:30.388	✗		0	sfadmin			SFR-DC					ise12-psn1	Authentication f...

## Troubleshoot

- Ao testar a autenticação do usuário em relação ao ISE, o erro a seguir é indicativo de uma incompatibilidade de chave secreta RADIUS ou de um nome de usuário/senha incorretos.



- Na GUI do administrador do ISE, navegue para **Operations > Authentications**. Um evento **vermelho** indica uma falha, enquanto um evento **verde** indica uma autenticação/autorização/alteração de autorização bem-sucedida. Clique no  ícone para revisar os detalhes do evento de autenticação.

## Overview

Event	5400 Authentication failed
Username	sfadmin
Endpoint Id	
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

## Authentication Details

Source Timestamp	2014-06-16 20:01:17.438
Received Timestamp	2014-06-16 20:00:58.439
Policy Server	ise12-psn1
Event	5400 Authentication failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	sfadmin
User Type	User
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	Internal Users

## Informações Relacionadas

[Suporte Técnico e Documentação - Cisco Systems](#)