Integração do sistema de FireSIGHT com o ISE para a autenticação de usuário RADIUS

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Configuração ISE
Configurando dispositivos de rede e grupos de dispositivo de rede
Configurando a política de autenticação ISE:
Adicionando um usuário local ao ISE
Configurando a política da autorização ISE
Configuração da política de sistema de Sourcefire
Permita a autenticação externa
Verificar
Troubleshooting
Informações Relacionadas

Introdução

Este documento descreve as etapas de configuração exigidas para integrar um dispositivo gerenciado do centro de gerenciamento (FMC) ou da potência de fogo de Cisco FireSIGHT com Cisco Identity Services Engine (ISE) para a autenticação de usuário do Remote Authentication Dial In User Service (RAIO).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração inicial do sistema e do dispositivo gerenciado de FireSIGHT através do GUI e/ou do shell
- Configurando políticas da authentication e autorização no ISE
- Conhecimento do raio básico

Componentes Utilizados

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

- Cisco ASA v9.2.1
- Módulo v5.3.1 da potência de fogo ASA
- ISE 1.2

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Configuração ISE

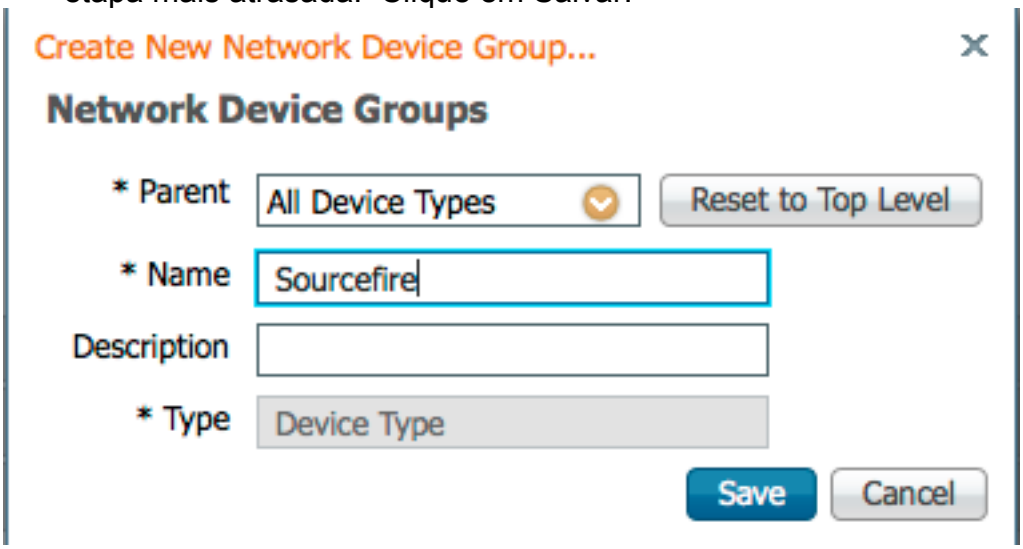
> Dica: Há umas formas múltiplas configurar políticas da authentication e autorização ISE para apoiar a integração com dispositivos do acesso de rede (NAD) como Sourcefire. O exemplo abaixo é uma maneira de configurar o intregration. A configuração de exemplo é um ponto de referência e pode ser adaptada para serir as necessidades do desenvolvimento específico. Note que a configuração de autorização é um processo em duas etapas. Umas ou várias políticas da autorização serão definidas no ISE com pares de retorno do valor de atributo RADIUS ISE (AV-pares) ao FMC ou ao dispositivo gerenciado. Estes AV-pares são traçados então a um grupo de usuário local definido na configuração da política de sistema FMC.

Configurando dispositivos de rede e grupos de dispositivo de rede

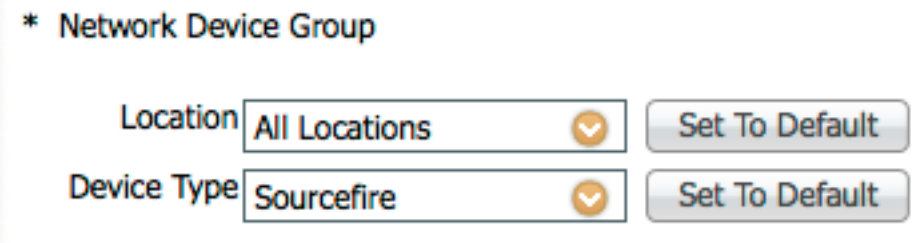
- Do ISE GUI, navegue à **administração > aos recursos de rede > aos dispositivos de rede**. Clique **+Add** para adicionar um dispositivo novo do acesso de rede (NAD). Forneça um nome e um endereço IP de Um ou Mais Servidores Cisco ICM NT descritivos do dispositivo. O FMC é definido no exemplo abaixo.

- Sob o **grupo de dispositivo de rede**, clique sobre a seta alaranjada ao lado de **todos os tipos de dispositivo.** Clique sobre  o ícone e seleto **crie o grupo de dispositivo de rede novo**. No tiro de tela do exemplo que segue, o tipo de dispositivo Sourcefire foi configurado. Este tipo de dispositivo será provido na definição da regra da política da autorização em uma

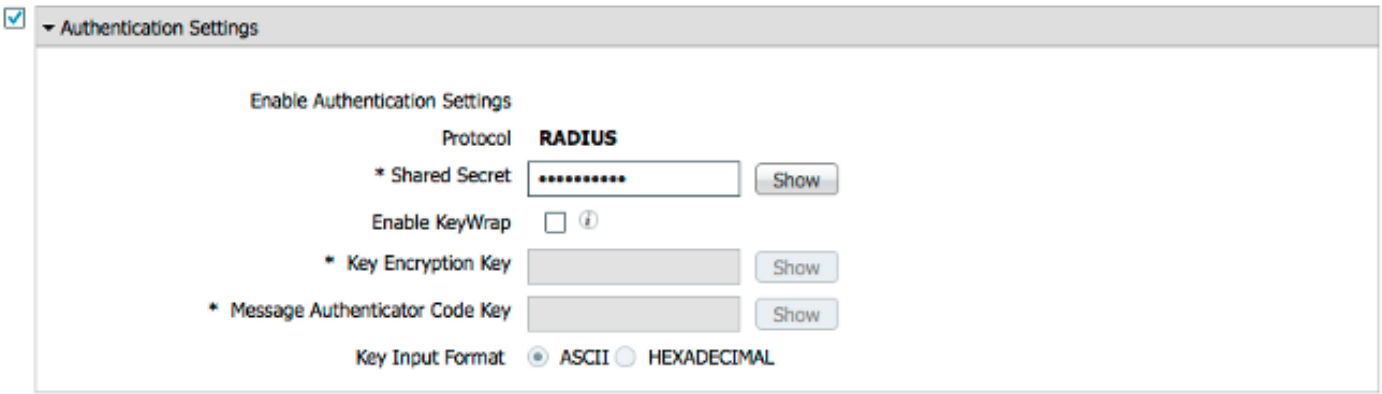
etapa mais atrasada. Clique em Salvar.



- Clique a seta alaranjada outra vez e selecione o grupo de dispositivo de rede configurado na etapa acima



- Verifique a caixa ao lado dos **ajustes da autenticação**. Incorpore a chave secreta compartilhada RAIO que será usada para este NAD. Note a mesma chave secreta compartilhada será usado outra vez mais tarde ao configurar o servidor Radius no FireSIGHT MC. Para rever o valor chave do texto simples, clique o botão da **mostra**. Clique em Salvar.

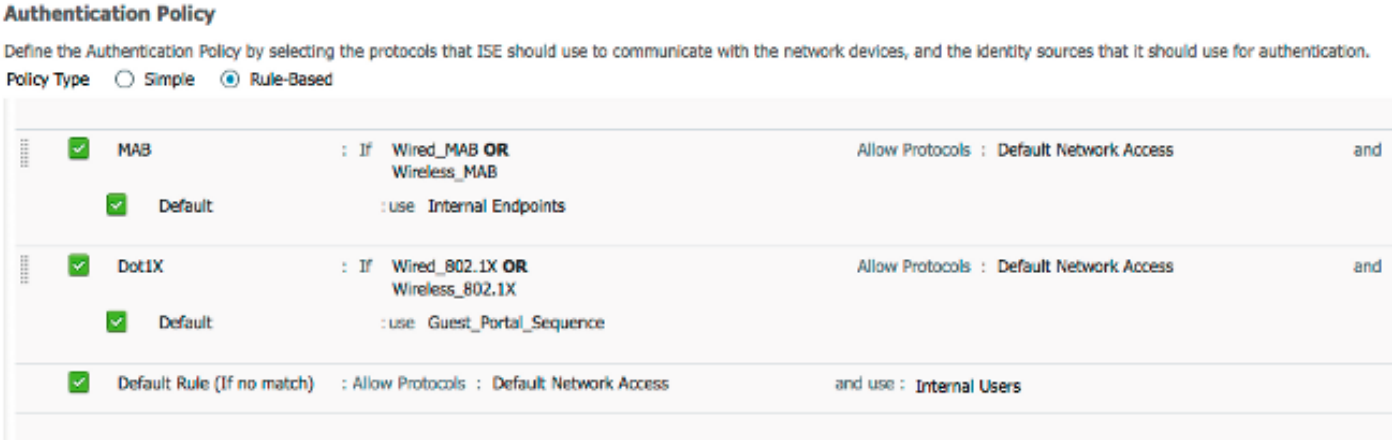


- Repita as etapas acima para todo o FireSIGHT os MC e os dispositivos gerenciado que exigirão a autenticação de usuário RADIUS/autorização para o GUI e/ou descascarão o acesso.

Configurando a política de autenticação ISE:

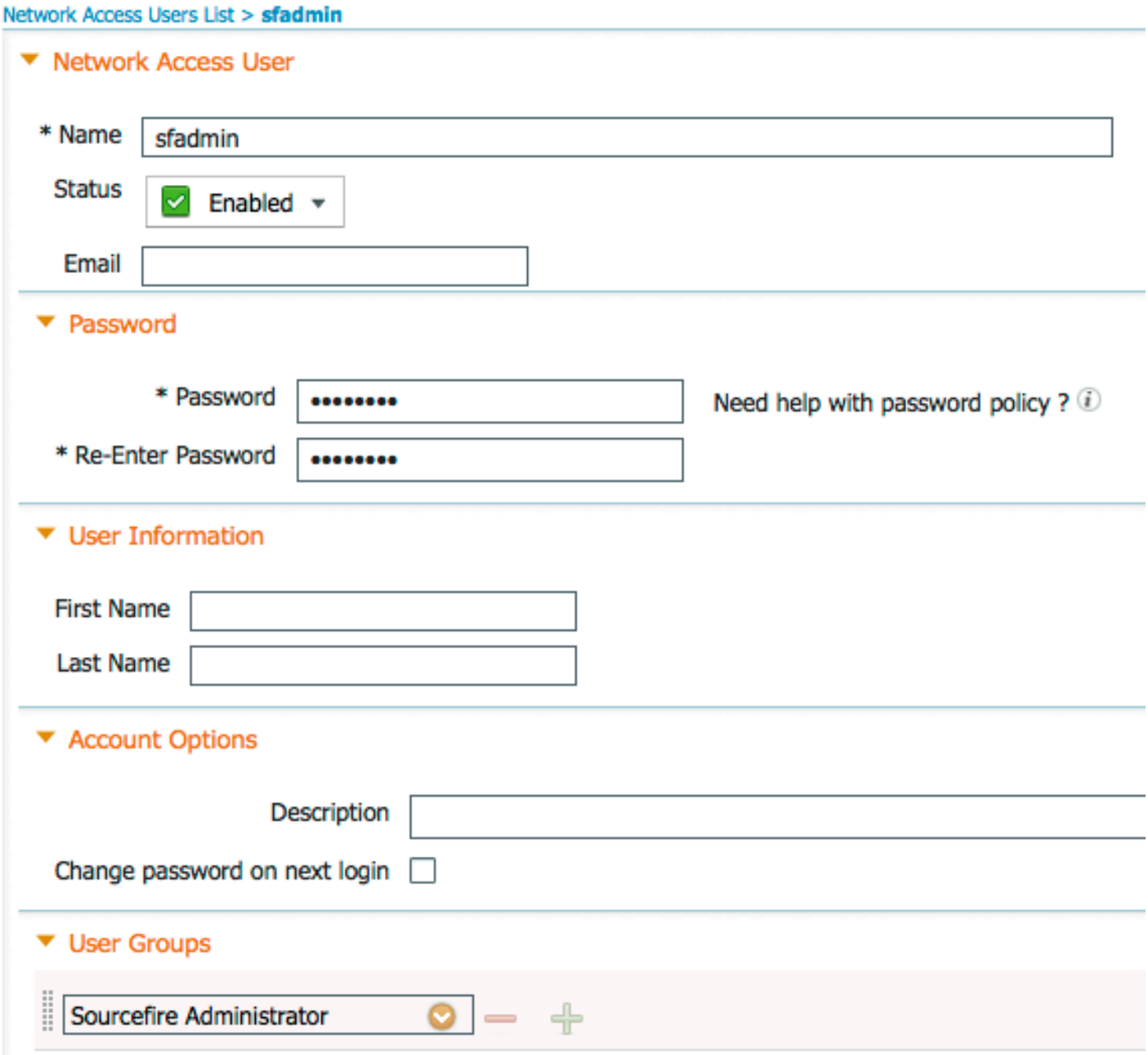
- Do ISE GUI, navegue à **política > à autenticação**. Se usando grupos da política, navegue à **política > aos grupos da política**. O exemplo abaixo é tomado de um desenvolvimento ISE que use as interfaces de política da autenticação padrão e da autorização. A lógica da regra da authentication e autorização é a mesma apesar da aproximação da configuração.

- **A regra de padrão (se nenhum fósforo)** será usada autenticar requisições RADIUS de NADs onde o método no uso não é o desvio da autenticação de MAC (MAB) ou o 802.1X. Como configurado à revelia, esta regra procurará contas de usuário na fonte local da identidade dos **usuários internos do** ISE. Esta configuração pode ser alterada para referir uma fonte externo da identidade tal como o diretório ativo, o LDAP, etc. como definida sob a **administração > o Gerenciamento de identidades > fontes externos da identidade**. Para a causa do simplciity, este exemplo definirá contas de usuário localmente no ISE assim que nenhuma alteração mais adicional à política de autenticação é exigida.



Adicionando um usuário local ao ISE

- Navegue à **administração > ao Gerenciamento de identidades > às identidades > aos usuários**. Clique em Add. Incorpore um nome de usuário e senha significativo. Sob a seleção de **grupos de usuário**, selecione um nome de grupo existente ou clique o verde + sinal adicionar um grupo novo. Neste exemplo, o usuário “sfadmin” é atribuído ao grupo feito sob encomenda de “administrador Sourcefire”. Este grupo de usuário será ligado ao perfil da autorização definido na etapa **configurando da política da autorização ISE** abaixo. Clique em Salvar.



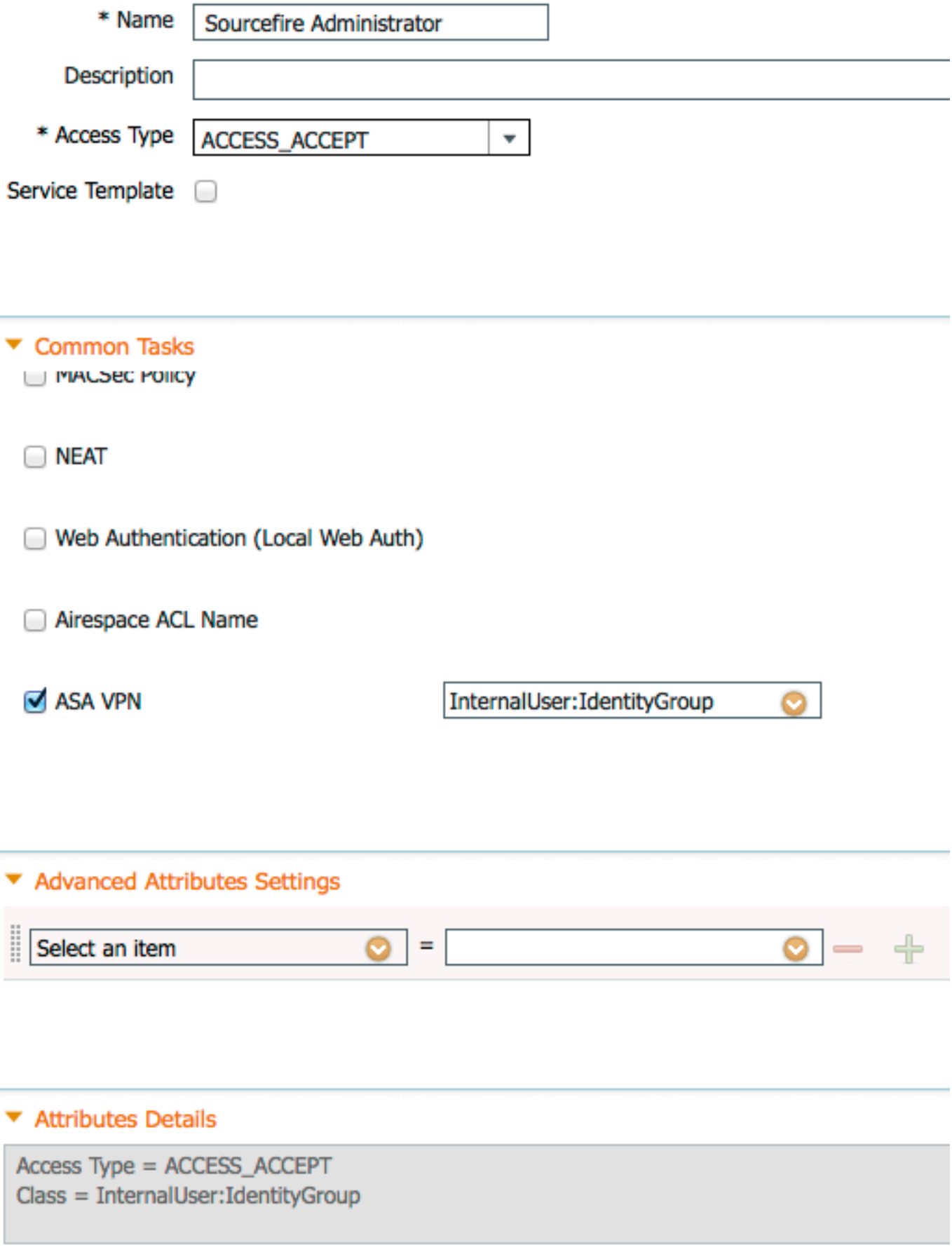
Configurando a política da autorização ISE

- Navegue à **política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização**. Clique o verde + sinal adicionar um perfil novo da autorização.
- Forneça um nome descritivo tal como o administrador de Sourcefire. Selecione **ACCESS_ACCEPT** para o **tipo de acesso**. Sob **tarefas comuns**, enrole a parte inferior e verifique a caixa ao lado de **ASA VPN**. Clique a seta alaranjada e selecione **InternalUser: IdentityGroup**. Clique em Salvar.

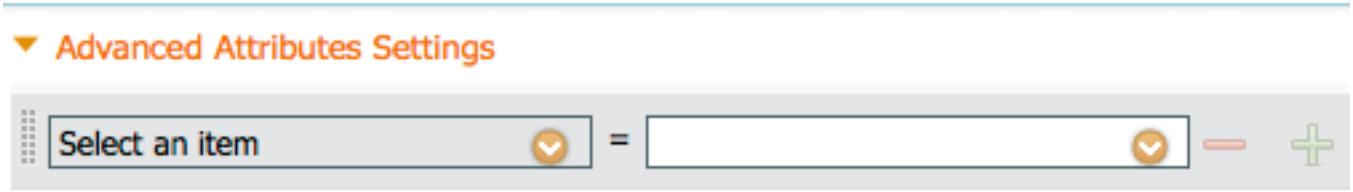
  Dica: Porque este exemplo usa a loja da identidade do usuário local ISE, o InternalUser: A opção do grupo de IdentityGroup é usada para simplificar a configuração. Se usando uma loja externo da identidade, o atributo da autorização ASA VPN é usado ainda, contudo, o valor a ser retornado ao dispositivo de Sourcefire está configurado manualmente. Por exemplo, o administrador manualmente de datilografia no ASA VPN deixa cair para baixo a caixa conduzirá a um valor dos AV-pares Class-25 da classe = do administrador que estão sendo enviados ao dispositivo de Sourcefire. Este valor pode então ser traçado a um grupo de usuário do sourcefire como parte da configuração da política de sistema. Para usuários

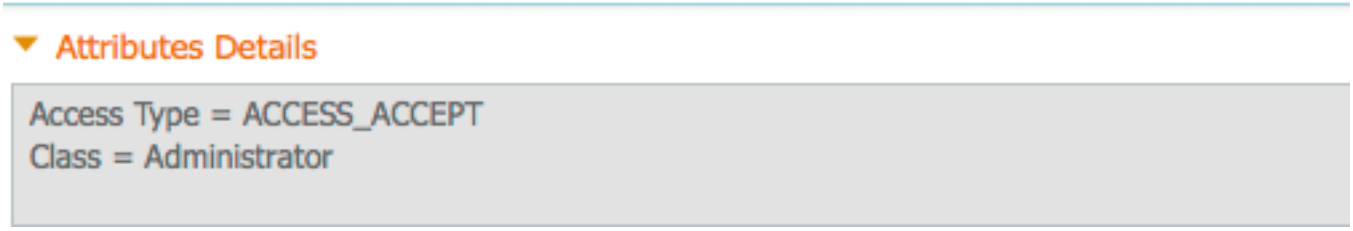
internos, um ou outro método de configuração é aceitável.

Exemplo do usuário interno



Exemplo do usuário externo





- Navegue à **política > à autorização** e configurar uma política nova da autorização para as sessões da administração de Sourcefire. O exemplo abaixo usa o **DISPOSITIVO:** Condição do **tipo de dispositivo** para combinar o tipo de dispositivo configurado no **Configurando a** seção dos **dispositivos de rede e dos grupos de dispositivo de rede** acima. Esta política é associada então com o perfil da autorização do administrador de Sourcefire configurado acima. Clique em Salvar.

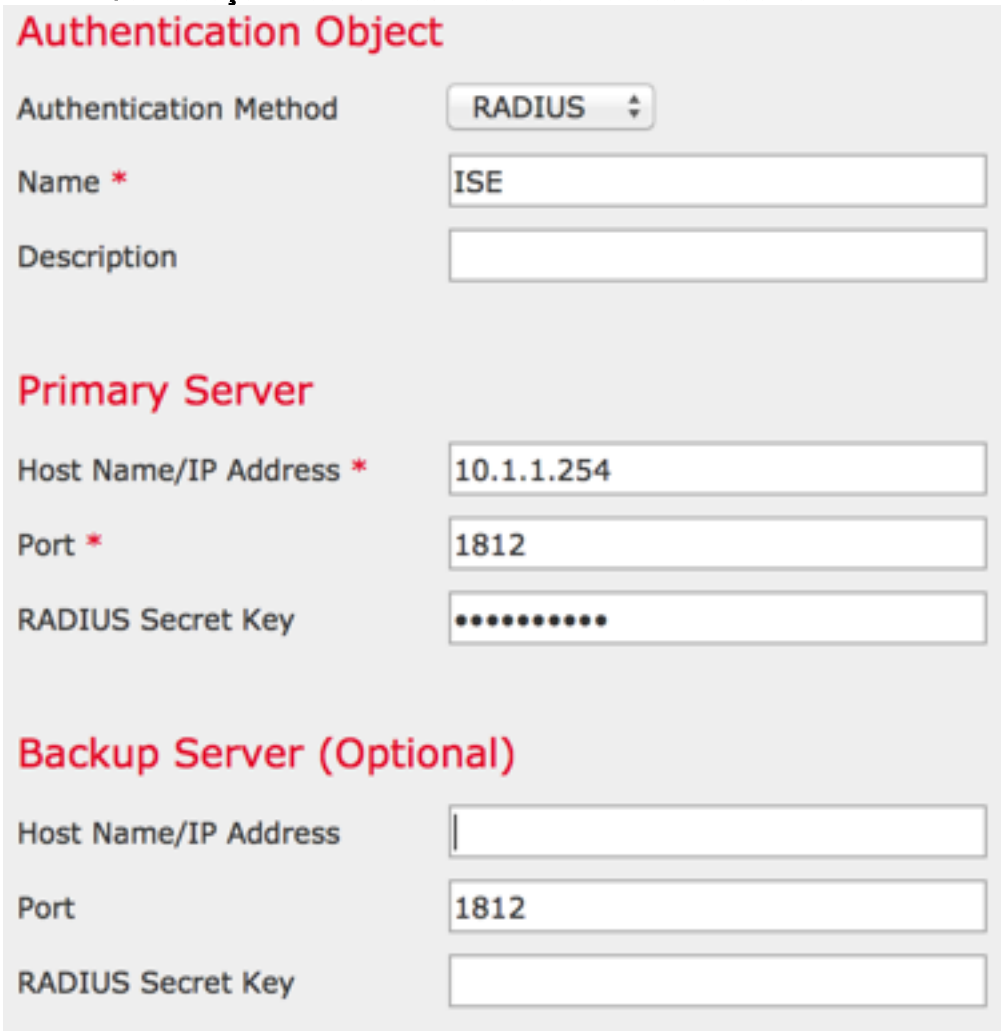
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	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 da política de sistema de Sourcefire

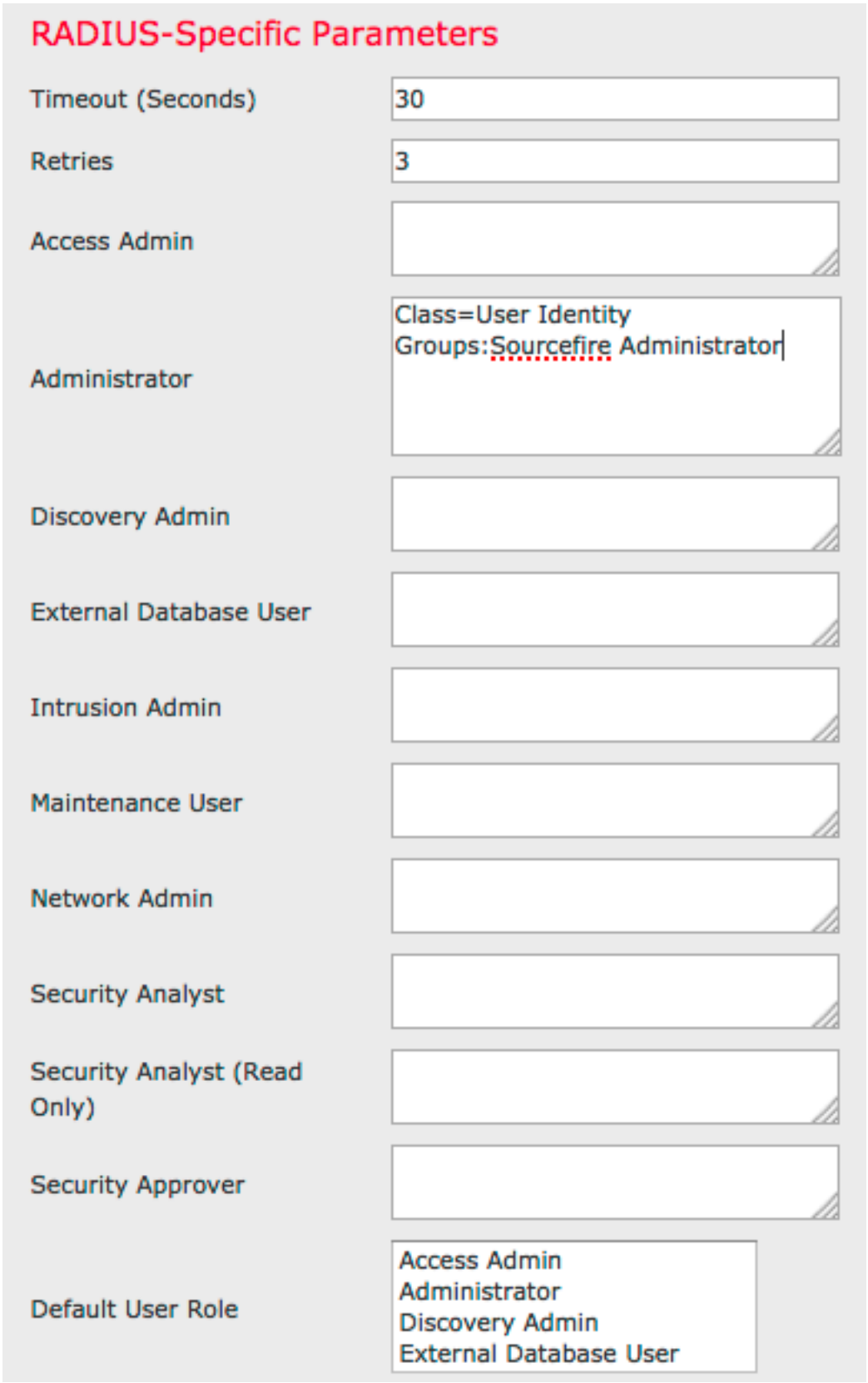
- Entre ao FireSIGHT MC e navegue ao **sistema > ao Local > ao gerenciamento de usuário**. Clique sobre a aba da **autenticação de login**. Clique **+ criam o** botão do **objeto da autenticação** para adicionar um servidor Radius novo para a autenticação de

usuário/autorização.

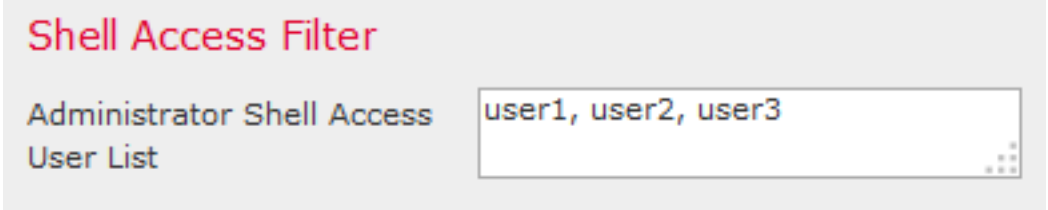
- Selecione o **RAIO** para o **método de autenticação**. Dê entrada com um nome descritivo para o servidor Radius. Incorpore o **nome de host/endereço IP de Um ou Mais Servidores Cisco ICM NT** e a **chave secreta do RAIO**. A chave secreta deve combinar a chave configurada previamente no ISE. Incorpore opcionalmente um **nome de** host de servidor do backup ISE**/endereço IP de Um ou Mais Servidores Cisco ICM NT** se um existe.



- Sob os **parâmetros Raio-específicos** secione, inscreva a corda dos AV-pares Class-25 na caixa de texto ao lado do nome de grupo local de Sourcefire a ser combinado para o acesso de GUI. Neste exemplo, a identidade de Class=User agrupa: O valor do administrador de Sourcefire é traçado ao grupo de administrador de Sourcefire. Este é o valor que o ISE retorna como parte da ACEITAÇÃO DE ACESSO. Opcionalmente, selecione um **papel de usuário padrão** para os usuários autenticados que não têm os grupos Class-25 atribuídos. Clique a **salvaguarda** para salvar a configuração ou para continuar à seção da verificação abaixo à autenticação de teste com ISE.



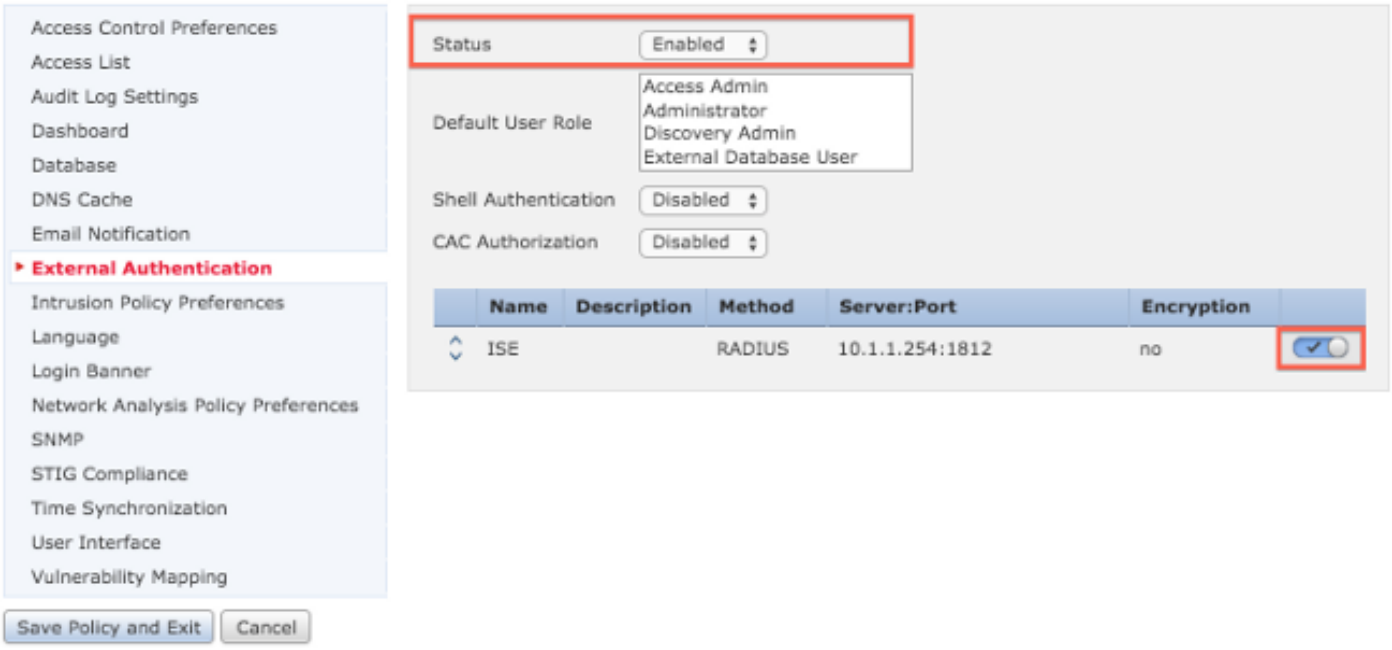
- Sob o **filtro do acesso do shell**, incorpore uma lista separada vírgula de usuários para restringir sessões shell/SSH.



Permita a autenticação externa

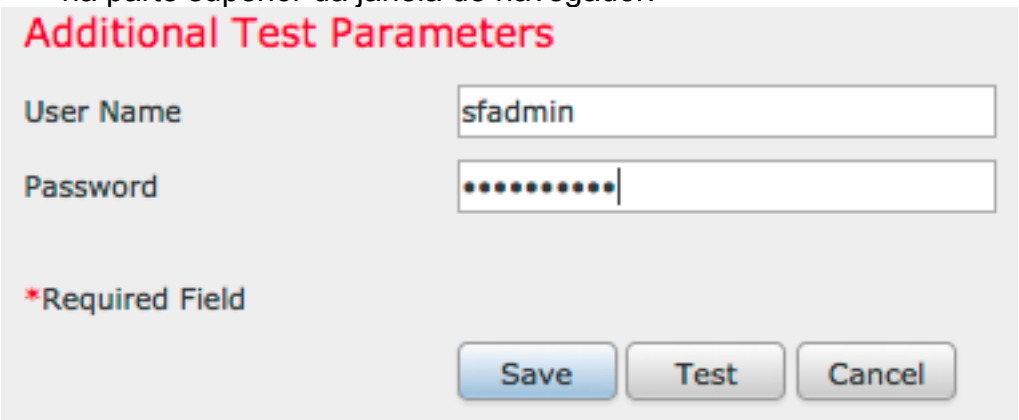
Finalmente, termine estas etapas a fim permitir a autenticação externa no FMC:

1. Navegue ao **sistema** > ao **Local** > à **política de sistema**.
2. Selecione a **autenticação externa no** painel esquerdo.
3. Mude o *estado ao* **permitido** (desabilitado à revelia).
4. Permita o servidor Radius adicionado ISE.
5. Salvar a política e reaplique a política no dispositivo.



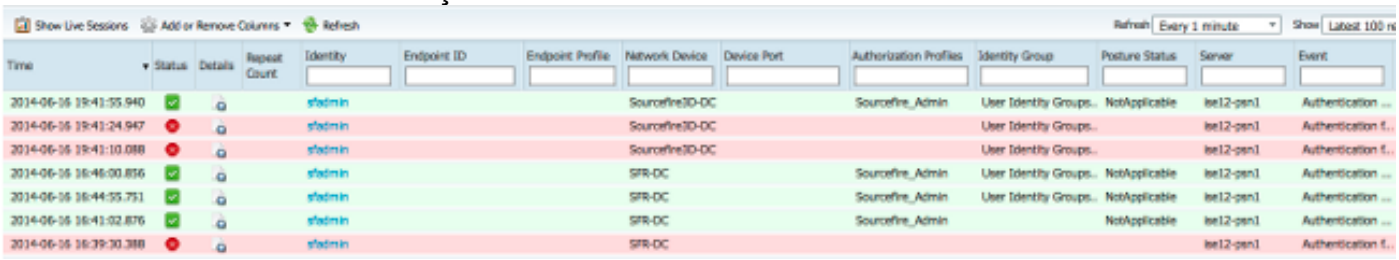
Verificar

- Àautenticação de usuário de teste contra o ISE, enrole para baixo a seção **adicional dos parâmetros de teste** e incorpore um nome de usuário e senha para o usuário ISE. Clique o **teste.** Um teste bem-sucedido conduzirá a um sucesso verde: Teste o mensagem completa na parte superior da janela de navegador.



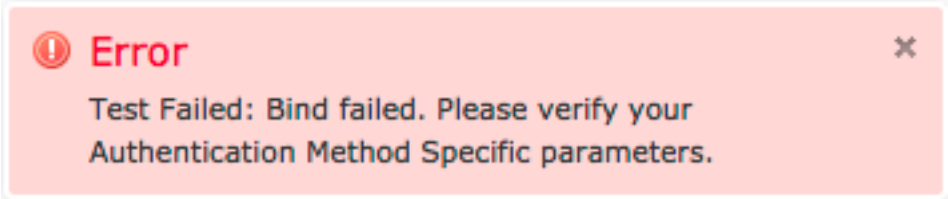
- Para ver os resultados da autenticação de teste, ir à **seção de emissor do teste** e clicar a seta **preta** ao lado dos **detalhes da mostra**. No tiro de tela do exemplo abaixo, note o “radiusauth - resposta: |Grupos da identidade de Class=User: Administrador de Sourcefire|” valor recebido do ISE. Isto deve combinar o valor de classe associado com o grupo local de Sourcefire configurado no FireSIGHT MC acima. Clique em Salvar.

- Do ISE Admin GUI, navegue às **operações > às autenticações** para verificar o sucesso ou a falha do teste da autenticação de usuário.

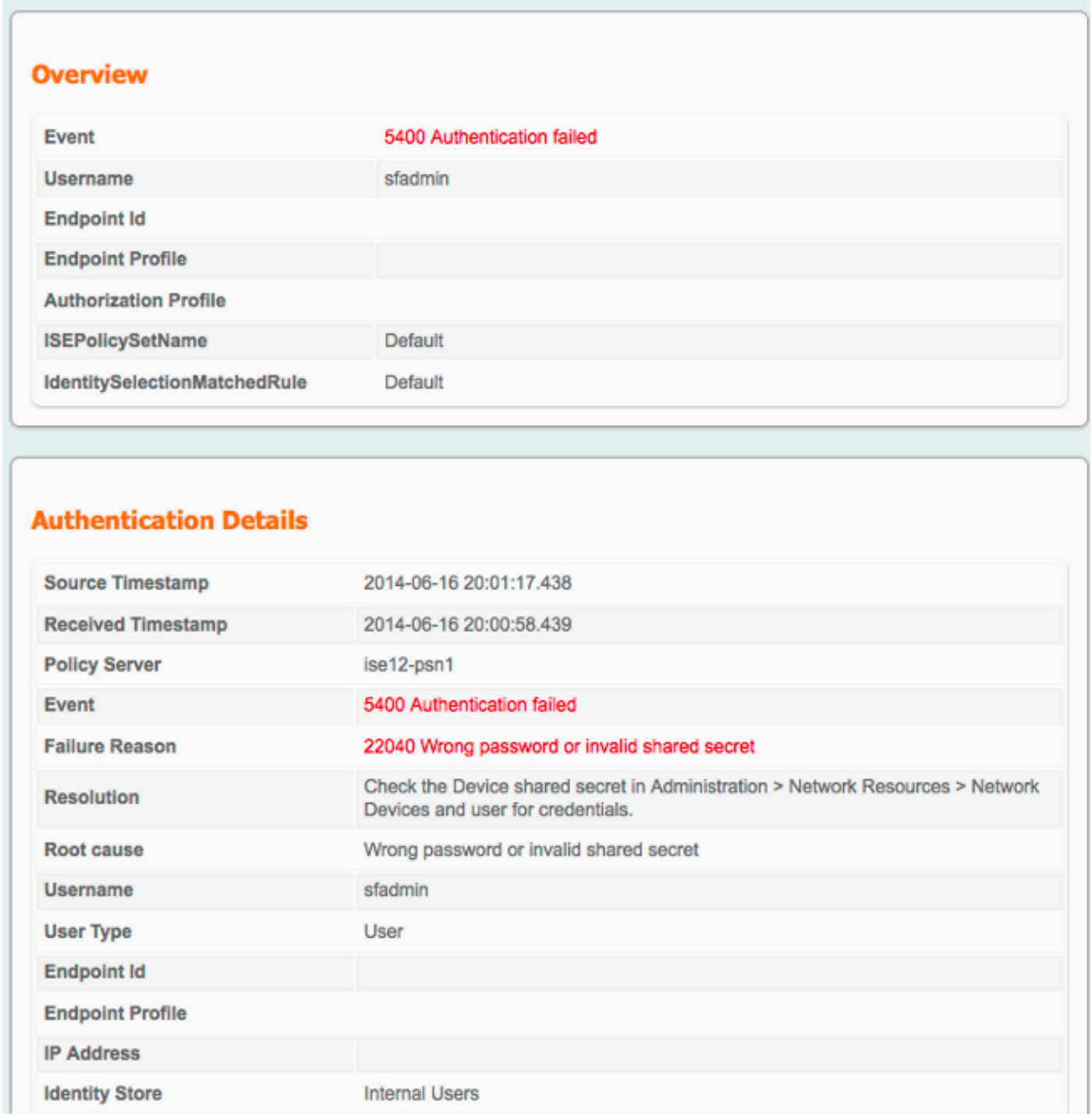


Troubleshooting

- Ao testar a autenticação de usuário contra o ISE, o seguinte erro é indicativo de uma má combinação de chave secreta do RAIO ou de um nome de usuário incorreto/senha.



- Do ISE admin GUI, navegue às **operações > às autenticações**. Um evento **vermelho** é indicativo de uma falha quando um evento **verde** for indicativo de uma autenticação bem sucedida/autorização/mudança da autorização. Clique sobre  o ícone para rever os detalhes do evento da 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]