Integração do sistema de FireSIGHT com ACS 5.x para a autenticação de usuário RADIUS

Índice

Introdução

Este documento descreve as etapas de configuração exigidas para integrar um centro de gerenciamento de Cisco FireSIGHT (FMC) ou o dispositivo gerenciado de FirePOWER com Cisco Secure Access Control System 5.x (ACS) 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 em ACS 5.x
- Conhecimento do raio básico

Componentes Utilizados

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

- Cisco Secure Access Control System 5.7 (ACS 5.7)

- Centro 5.4.1 do gerente de Cisco FireSIGHT

Acima das versões são as versões as mais atrasadas disponíveis atualmente. A característica é apoiada em todas as versões ACS 5.x e em versões FMC 5.x.

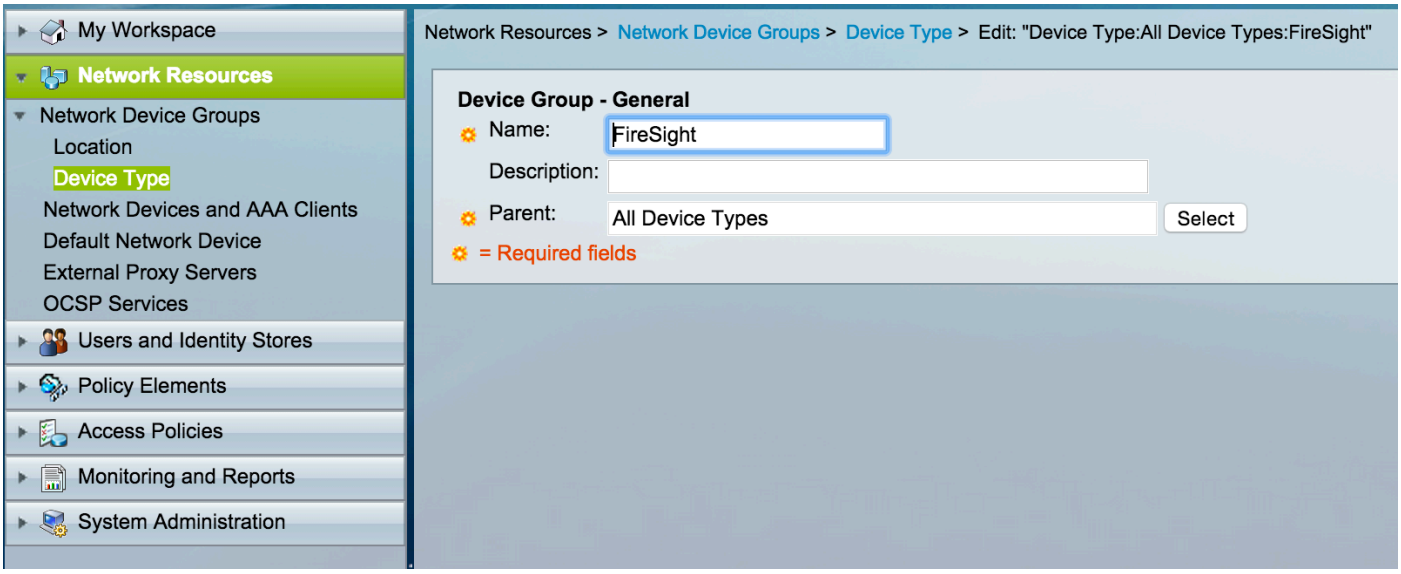
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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

Configuração

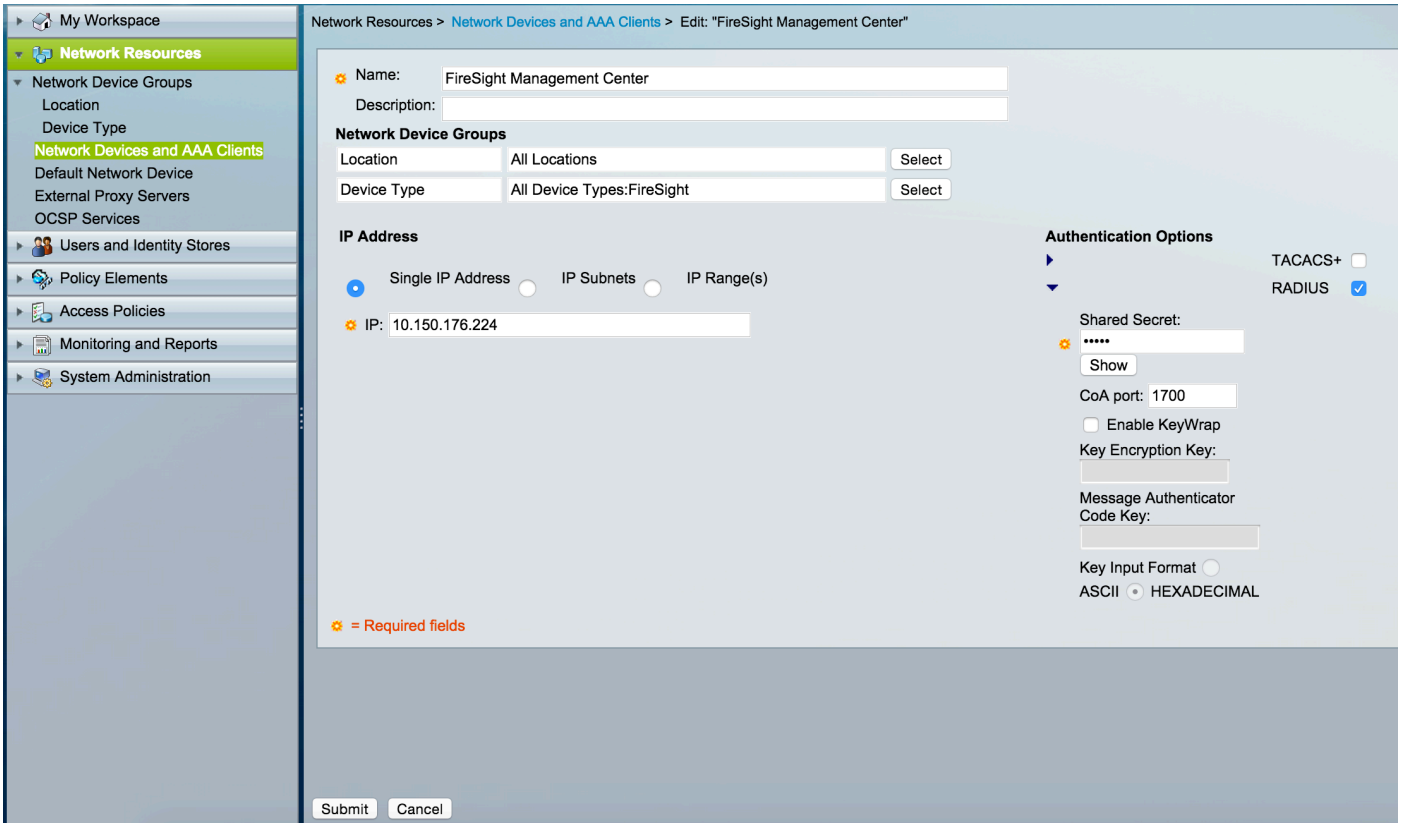
Configuração ACS 5.x

Configurando dispositivos de rede e grupos de dispositivo de rede

- Do ACS GUI, navegue ao **grupo de dispositivo de rede**, clique sobre o **tipo de dispositivo** e crie um grupo do dispositivo. No tiro de tela do exemplo que segue, o tipo de dispositivo FireSIGHT foi configurado. Este tipo de dispositivo será provido na definição da regra da política da autorização em uma etapa mais atrasada. Click **Save**.



- Do ACS GUI, navegue ao **grupo de dispositivo de rede**, clique sobre **NetwokDevices e clientes de AAA** e adicionar um dispositivo. Forneça um nome e um endereço IP de Um ou Mais Servidores Cisco ICM NT descritivos do dispositivo. O centro de gerenciamento de FireSIGHT é definido no exemplo abaixo.



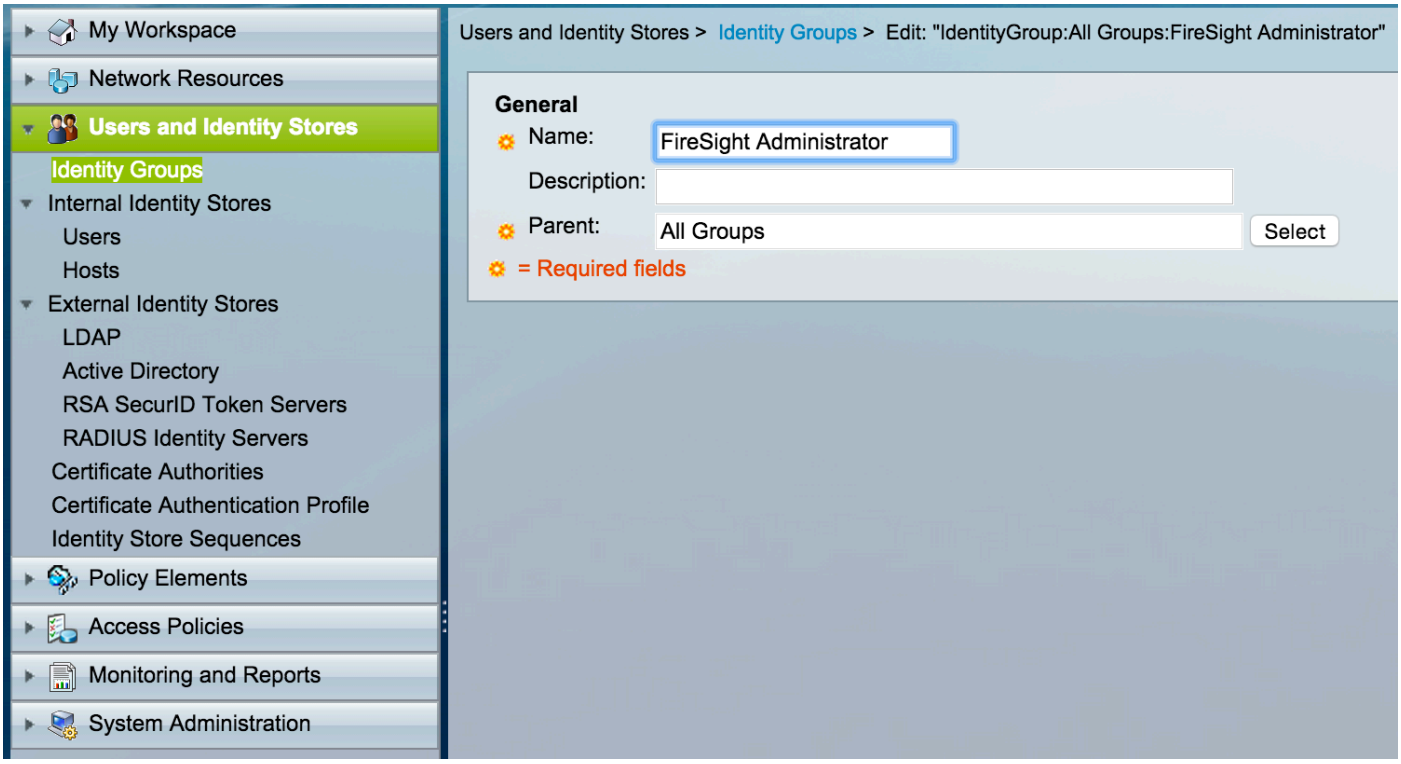
- **Nos grupos de dispositivo de rede,** configurar o **tipo de dispositivo** mesmos que o grupo do dispositivo criado na etapa acima.

- Verifique a caixa ao lado das **opções de autenticação,** selecione a caixa de verificação do RAIO e incorpore a **chave secreta compartilhada** que será usada para este NAD. Note a mesma chave secreta compartilhada será usado outra vez mais tarde ao configurar o servidor Radius no centro de gerenciamento de FireSIGHT. Para rever o valor chave do texto simples, clique o botão da **mostra**. Clique em Submit.

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

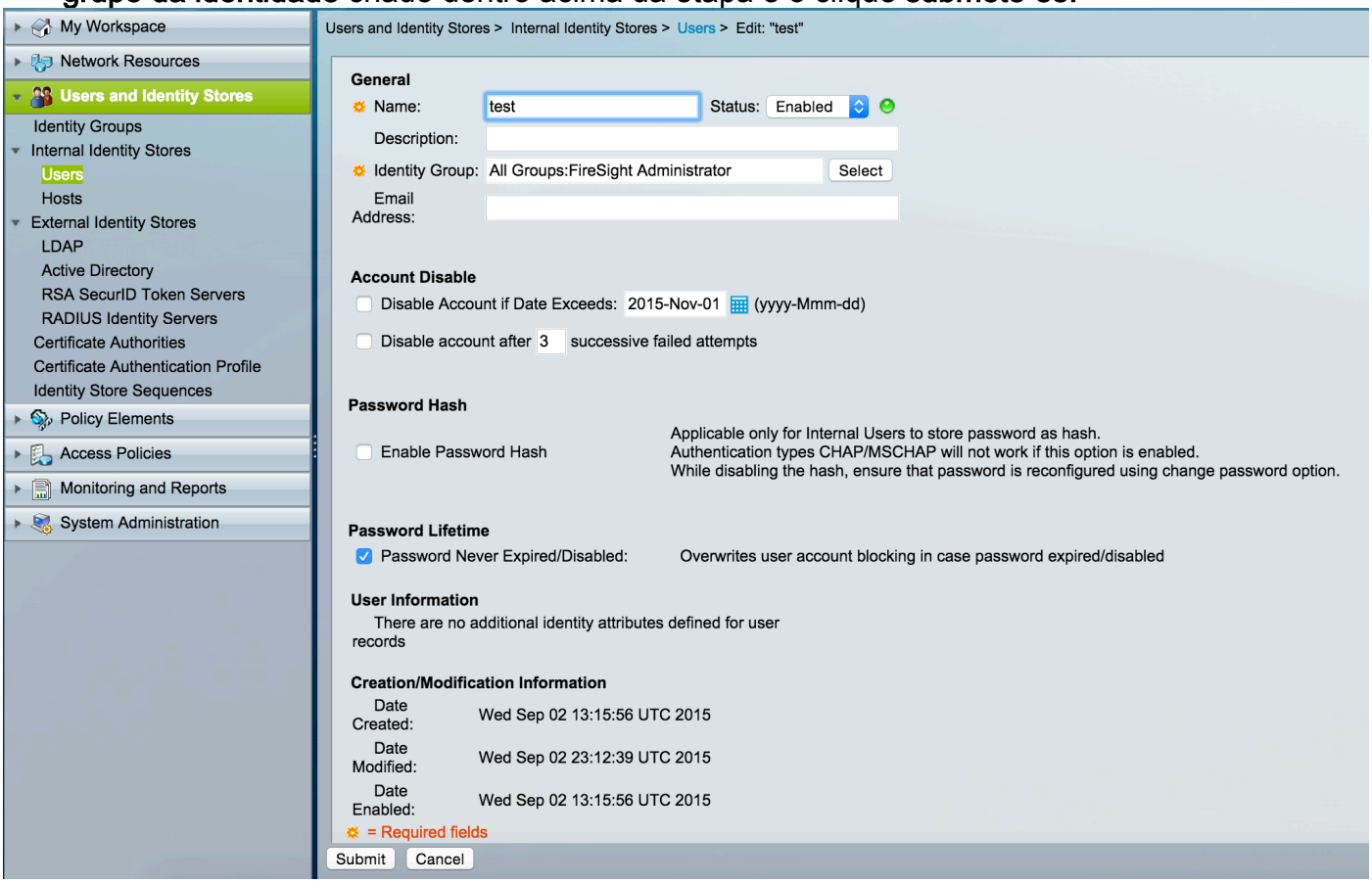
Adicionando um grupo de Idenity no ACS

- Navegue aos **usuários e as lojas da identidade,** configuram o **grupo da identidade**. Neste exemplo, o grupo da identidade criado é de “administrador FireSIGHT”. Este grupo será ligado ao perfil da autorização definido nas etapas abaixo.



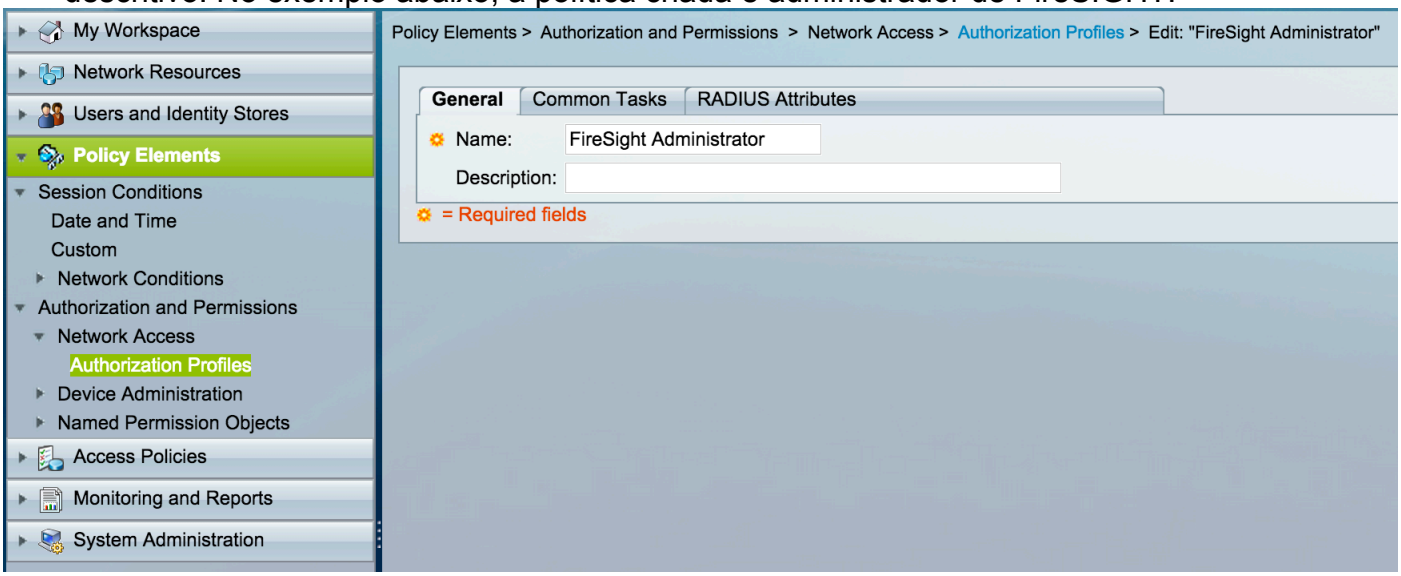
Adicionando um usuário local ao ACS

- Navegue aos **usuários e as lojas da identidade,** configuram **usuários na** seção **interna das lojas da identidade**. Enter requried a informação para a criação do usuário local, seleciona o **grupo da identidade** criado dentro acima da etapa e o clique **submete-se.**

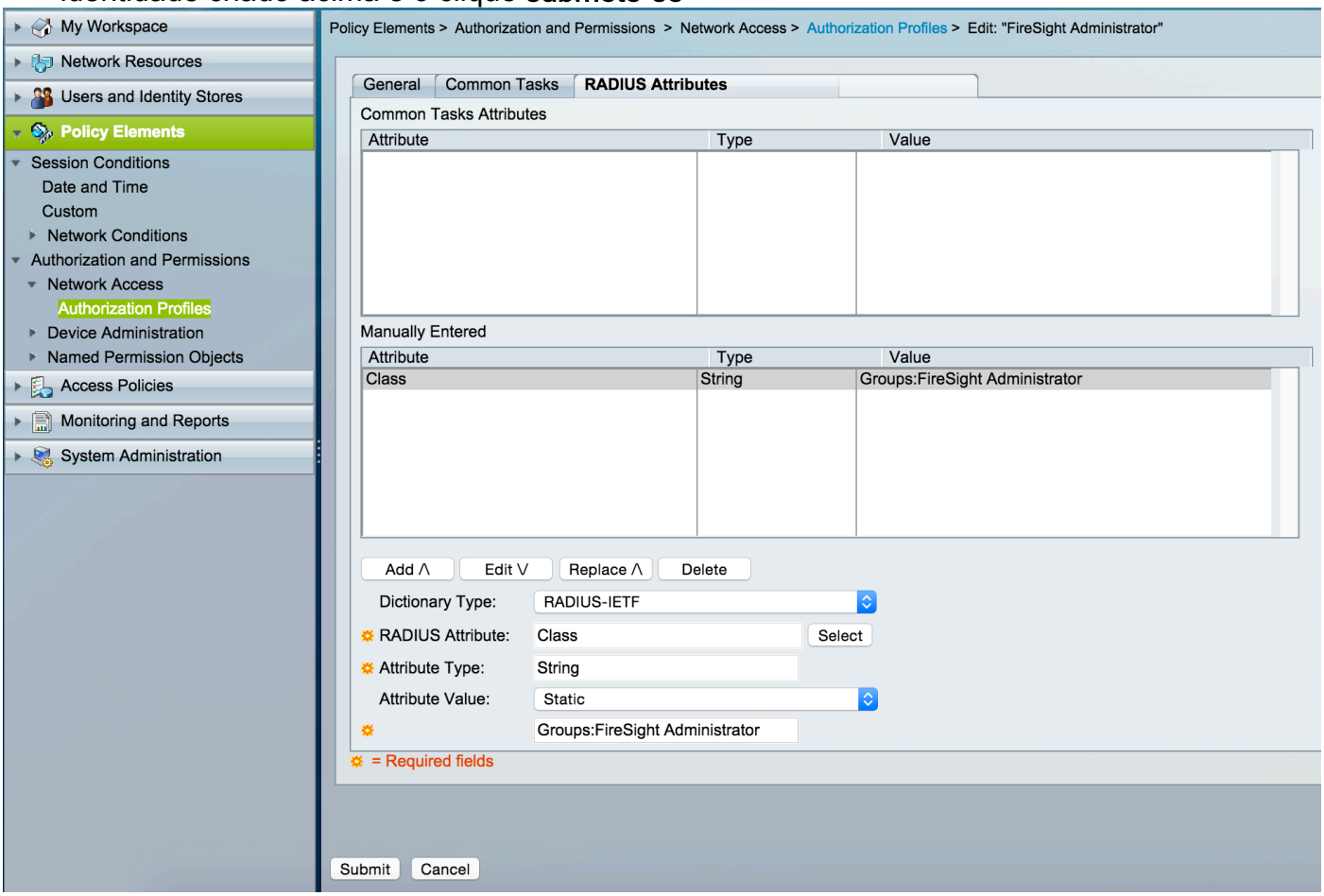


Configurando a política ACS

- No ACS GUI, navegue aos **elementos da política > à autorização e às permissões > aos perfis do acesso de rede > da autorização**. Crie um perfil novo da autorização com um nome descritivo. No exemplo abaixo, a política criada é administrador de FireSIGHT.

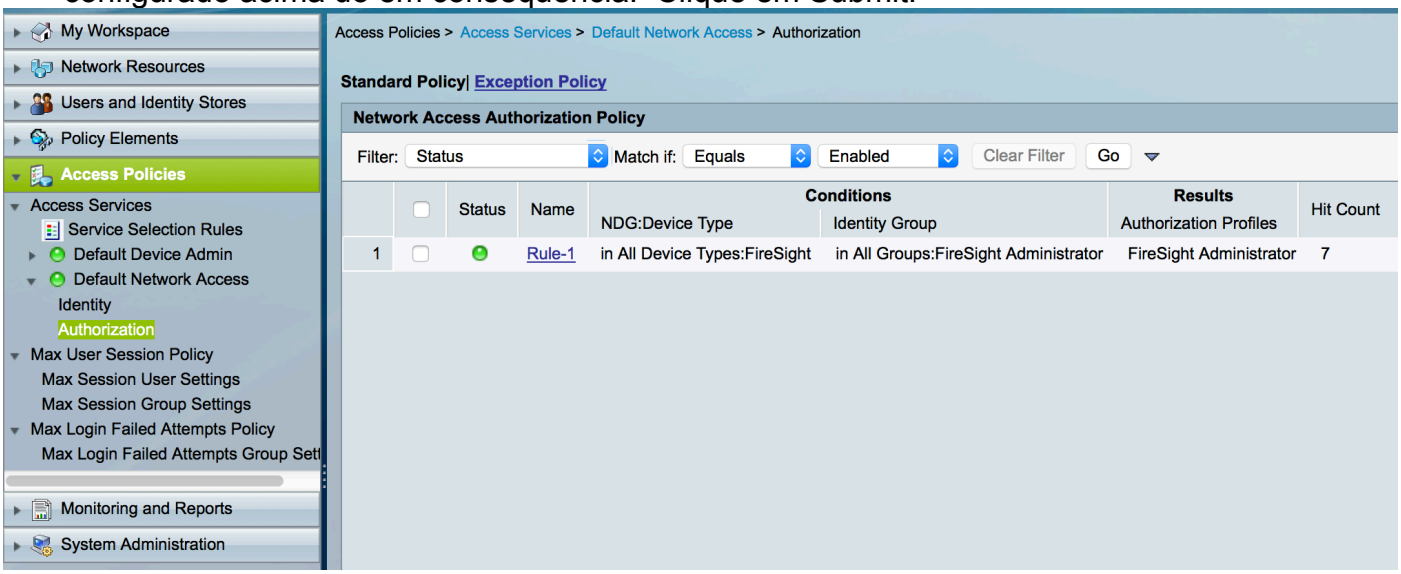


- **Nos atributos RADIUS** catalogue, adicionar o atributo manual para autorizar o grupo da identidade criado acima e o clique **submete-se**



- Navegue às **políticas de acesso > ao acesso presta serviços de manutenção > acesso > autorização de rede padrão** e configuram uma política nova da autorização para as sessões da administração do centro de gerenciamento de FireSIGHT. O exemplo abaixo usa o **NDG:** Condição do **grupo do tipo de dispositivo** & da **identidade** para combinar o grupo do tipo de dispositivo e da identidade configurado nas etapas acima.
- Esta política é associada então com o perfil da autorização do administrador de FireSIGHT

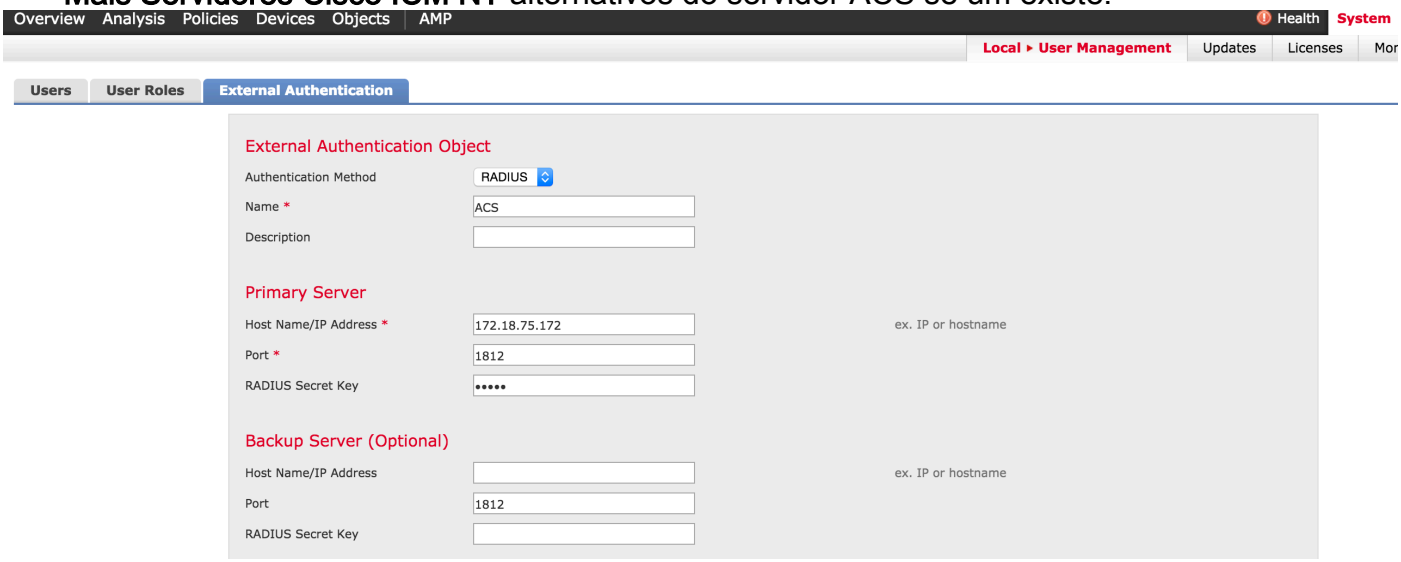
configurado acima do em consequência. Clique em Submit.



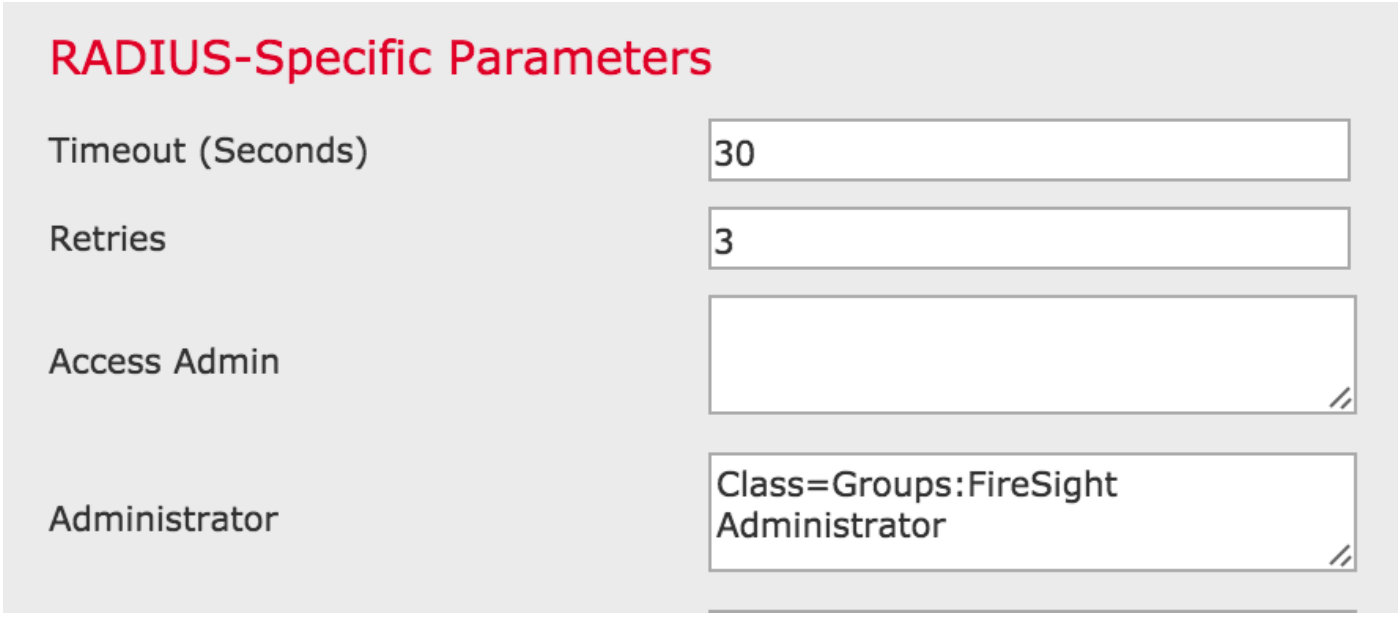
Configuração do centro de gerenciamento de FireSIGHT

Configuração da política de sistema do gerente de FireSIGHT

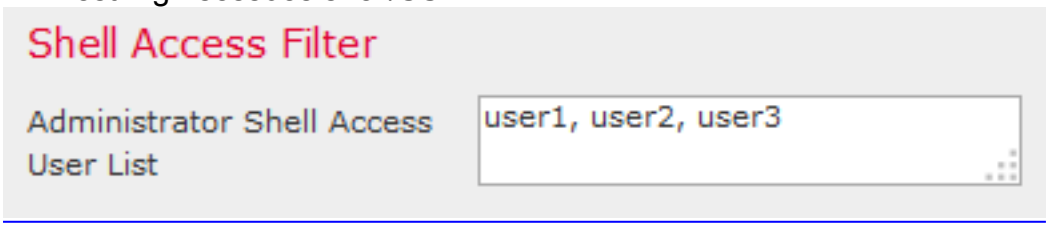
- Entre a FireSIGHT MC e navegue ao **sistema > ao Local > ao gerenciamento de usuário**. Clique sobre a aba da **autenticação externa**. Clique **+ criam o** botão do **objeto da autenticação** para adicionar um servidor Radius novo para a autenticação de usuário/autorização.
- Selecione o **RAIO** 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 ACS. Incorpore opcionalmente um **nome de host/endereço IP de Um ou Mais Servidores Cisco ICM NT** alternativos do servidor ACS se um existe.



- Sob a seção Raio-**específica dos parâmetros**, neste exemplo, o Class=Groups: O valor do administrador de FireSIGHT é traçado ao grupo de administrador de FireSIGHT. Este é o valor que o ACS retorna como parte da ACEITAÇÃO DE ACESSO. Clique a **salvaguarda** para salvar a configuração ou para continuar à seção da verificação abaixo à autenticação de teste com ACS.



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



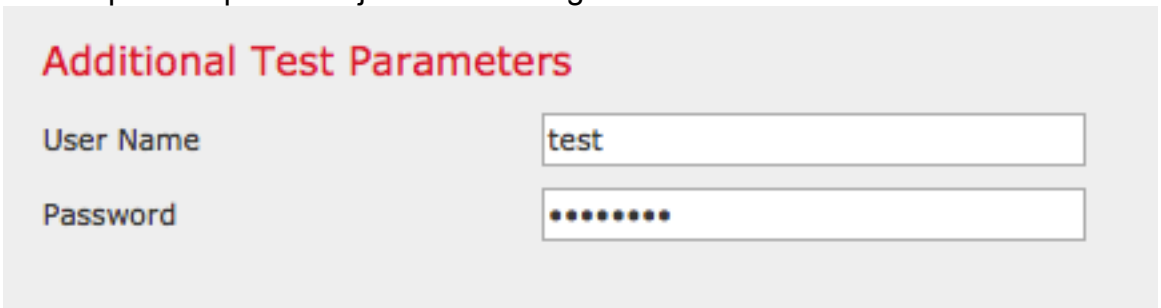
Permita a autenticação externa

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 ACS.
5. Salvar a política e reaplique a política no dispositivo.

Verificação

- Àautenticação de usuário de teste contra o ACS, enrole para baixo a seção **adicional dos parâmetros de teste** e incorpore um nome de usuário e senha para o usuário ACS. 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: |Class=Groups: Administrador de FireSIGHT|” valor recebido do ACS. Isto deve combinar o valor de classe associado com o grupo local de FireSIGHT configurado em FireSIGHT MC acima. Click **Save**.