Configurar a autenticação RADIUS do ISE para o Gerenciador de chassi de firewall seguro (FCM)

Contents

Introdução

Este documento descreve o processo de como configurar o acesso de Autorização/Autenticação Radius para o Secure Firewall Cluster Manager com ISE.

Pré-requisitos

Requisitos

A Cisco recomenda ter conhecimento dos seguintes tópicos:

- Gerenciador de chassi de firewall seguro (FCM)
- Cisco Identity Services Engine (ISE)
- Autenticação RADIUS

Componentes Utilizados

- Dispositivo de segurança Cisco Firepower 4110 FXOS v2.12
- Cisco Identity Services Engine (ISE) v3.2 patch 4

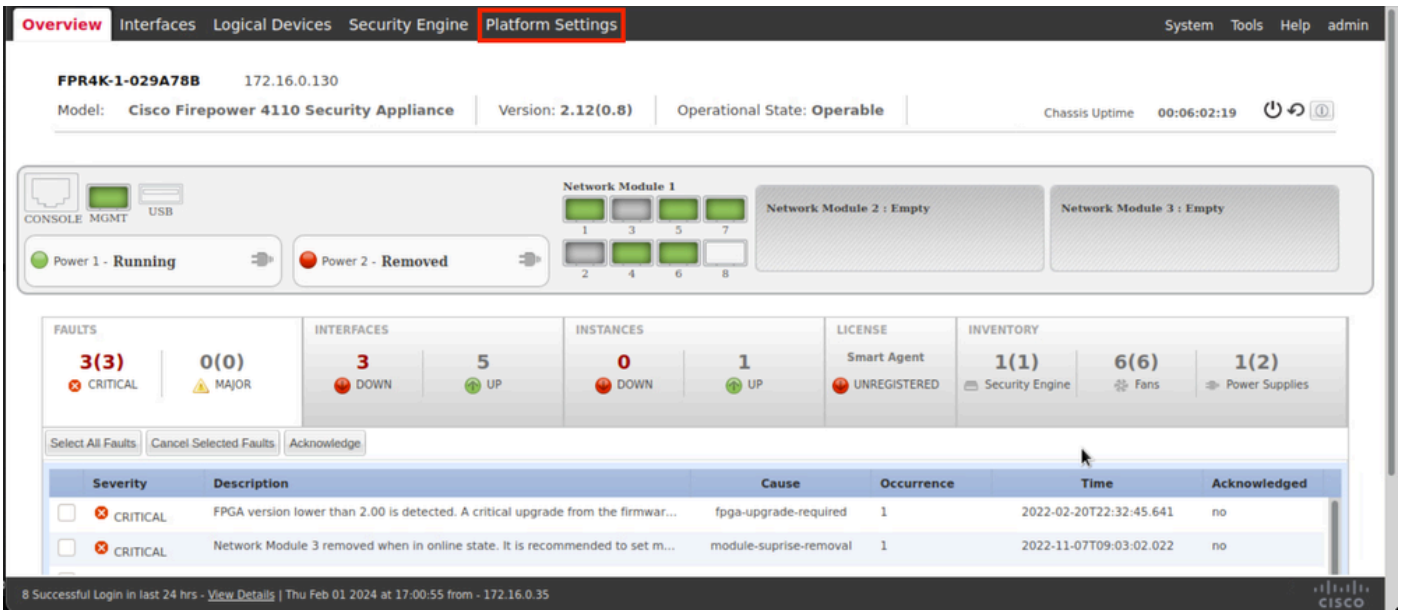
  As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configurar

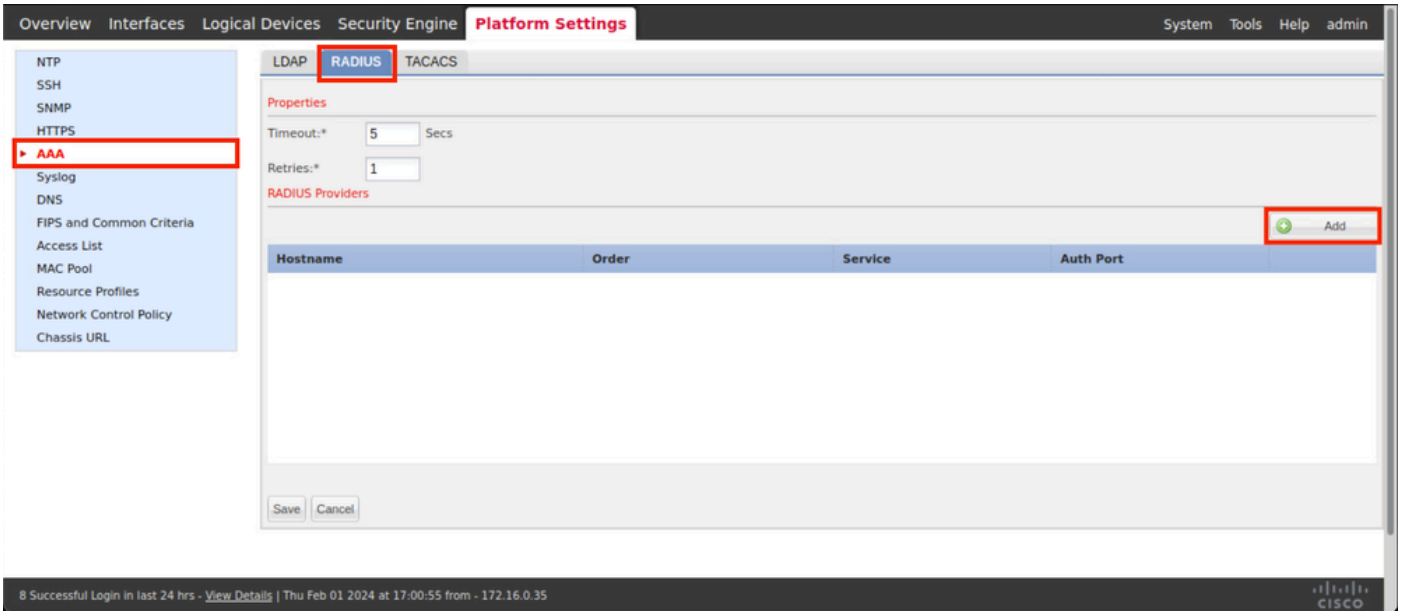
Configurações

Gerenciador de chassi de firewall seguro

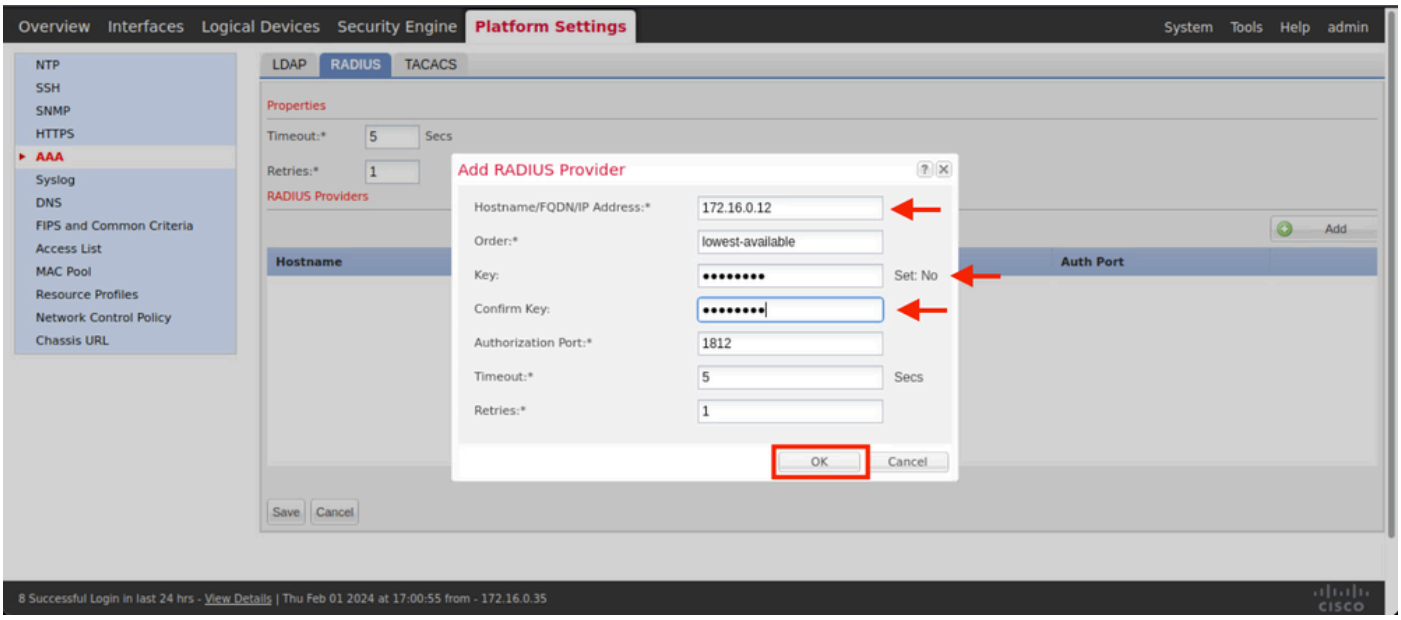
Etapa 1. Faça login na GUI do Firepower Chassis Manager.
Etapa 2. Navegue até Configurações da plataforma



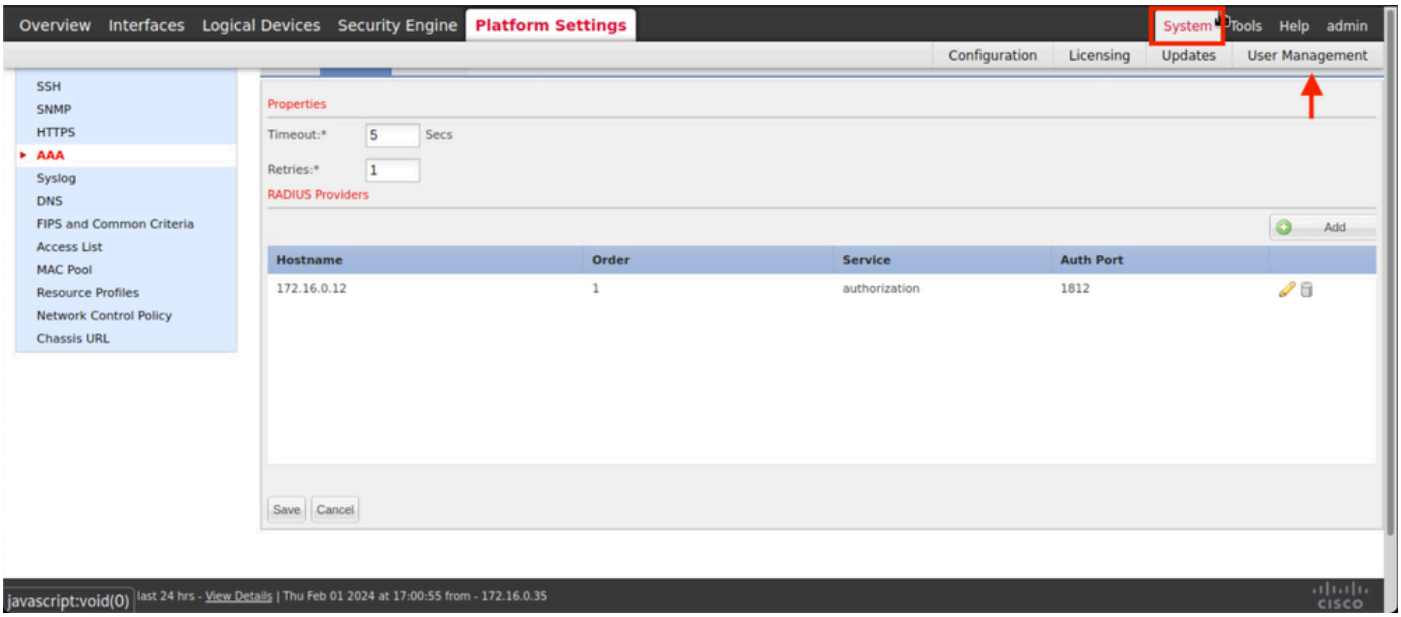
Etapa 3. No menu esquerdo, clique sobre AAA. Selecione Radius e Adicionar um novo provedor RADIUS.



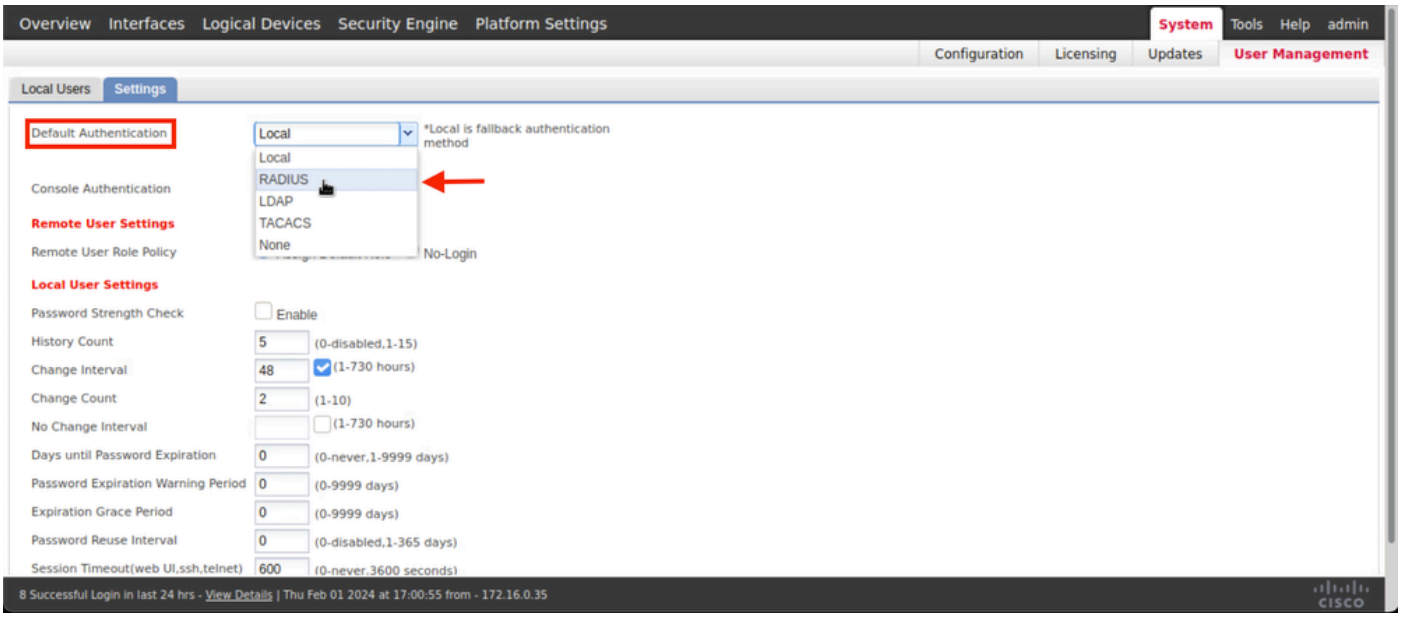
Etapa 4. Preencha o menu do prompt com as informações solicitadas do provedor Radius. Click OK.

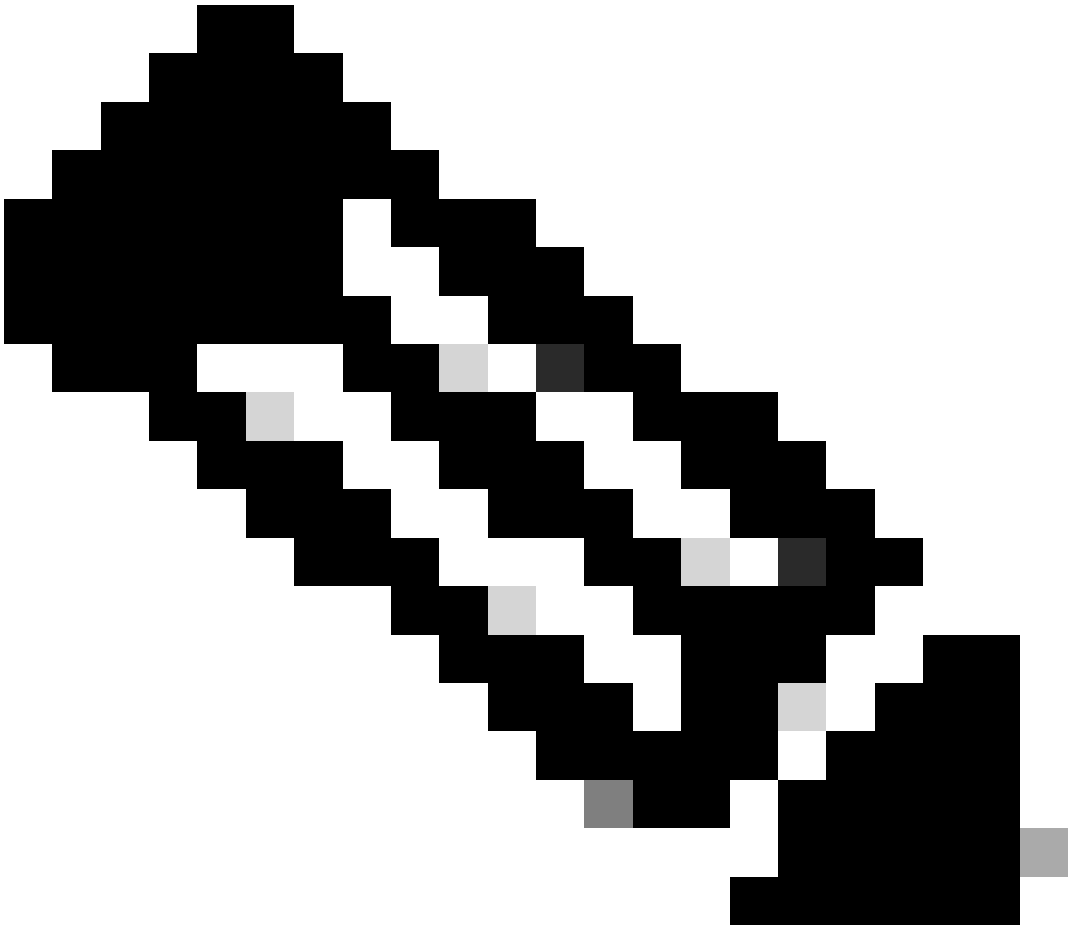


Etapa 5. Navegue até Sistema > Gerenciamento de usuários



Etapa 6. Clique na guia Settings (Configurações) e defina Default Authentication (Autenticação padrão) no menu suspenso para Radius; em seguida, role para baixo e salve a configuração.



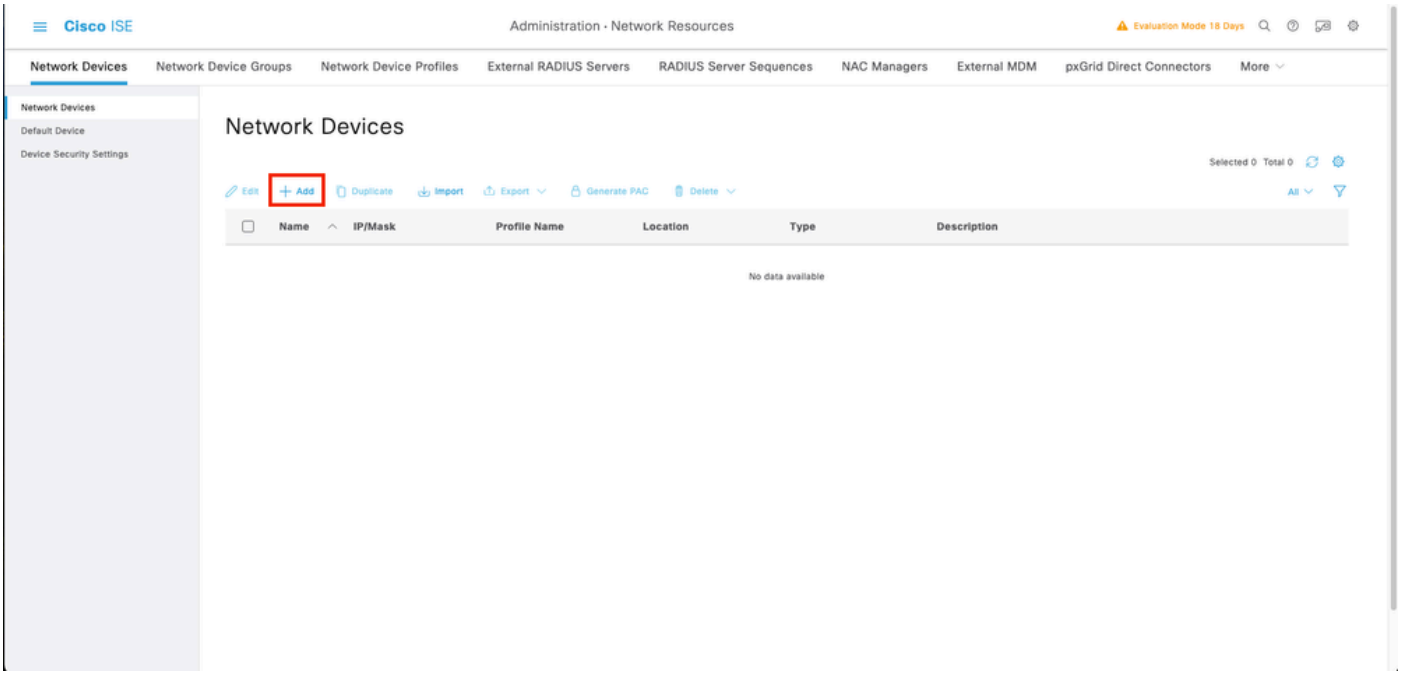


Observação: a configuração do FCM foi concluída neste ponto.

Identity Service Engine

Etapa 1. Adicione um novo dispositivo de rede.

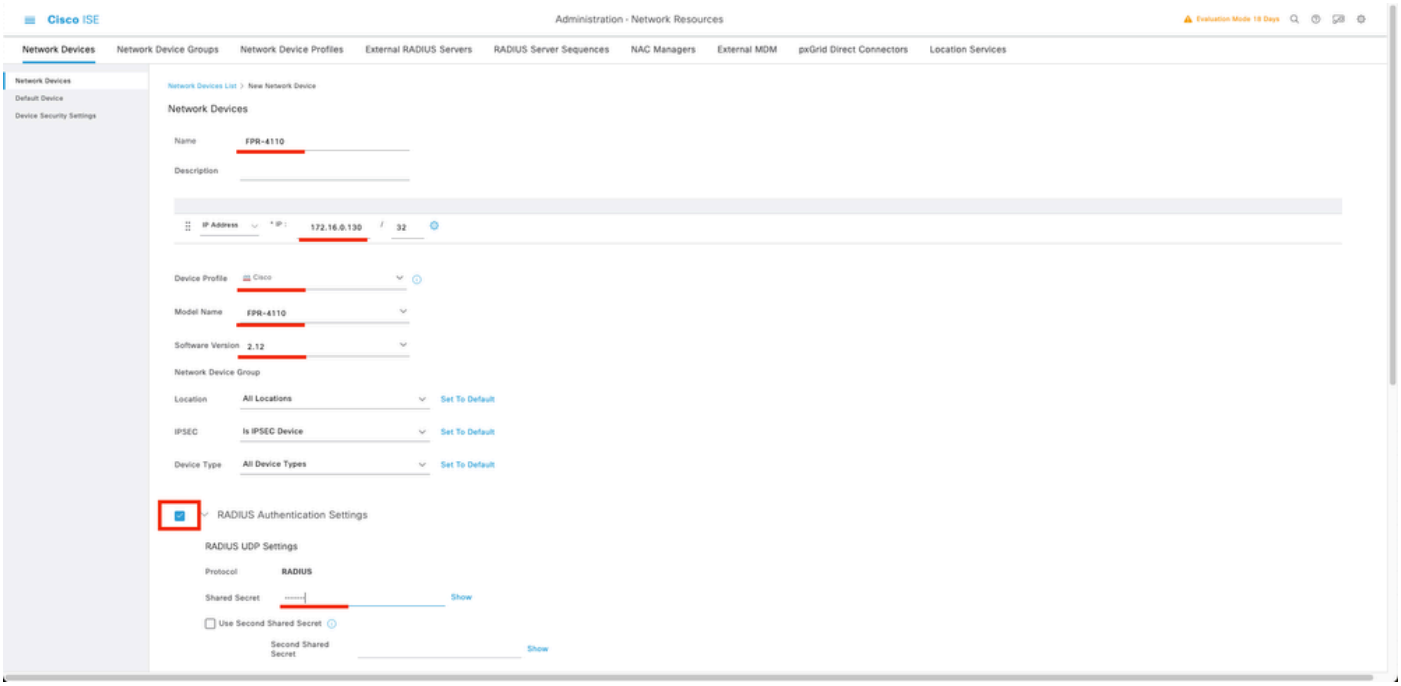
Navegue até o ícone de hambúrguer ≡ localizado no canto superior esquerdo > Administração > Recursos de rede > Dispositivos de rede > +Adicionar.



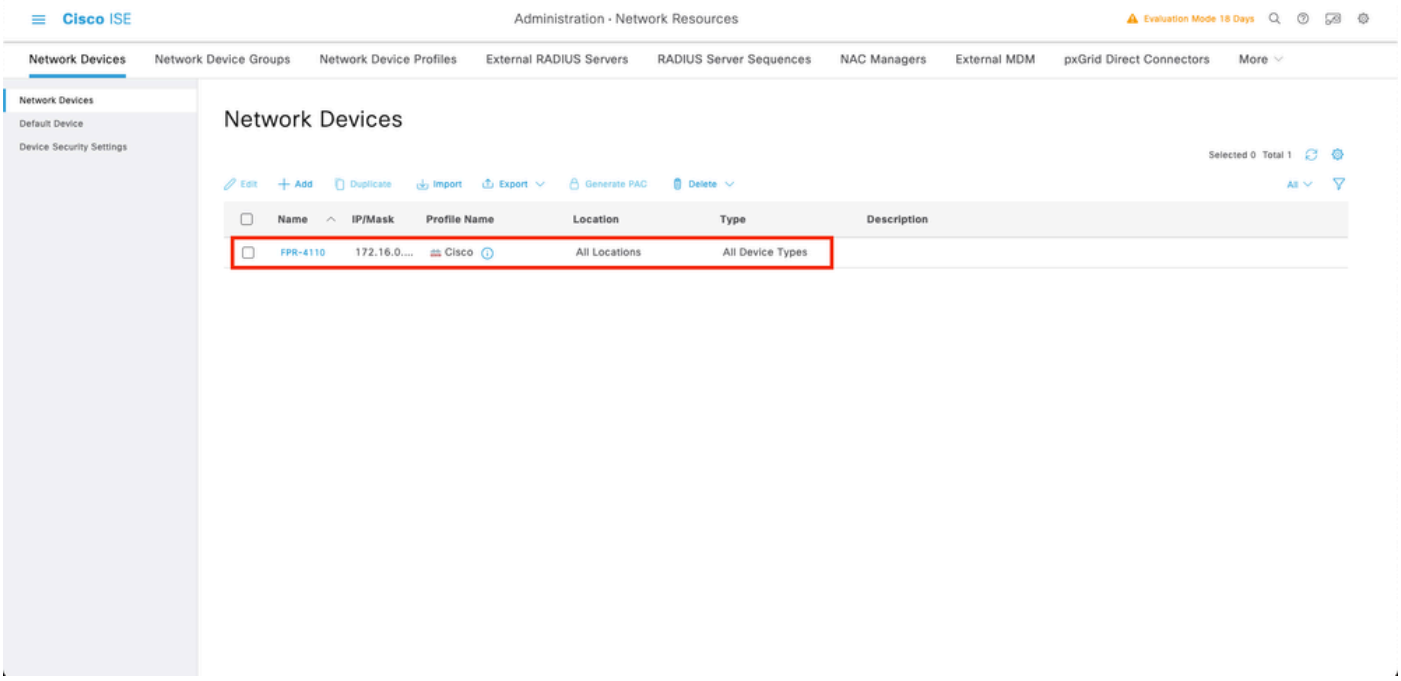
Etapa 2. Preencha os parâmetros solicitados sobre as novas informações de dispositivos de rede.

2.1 Marque a caixa de seleção RADIUS
2.2 Configure a mesma chave secreta compartilhada que consta na configuração FCM Radius.

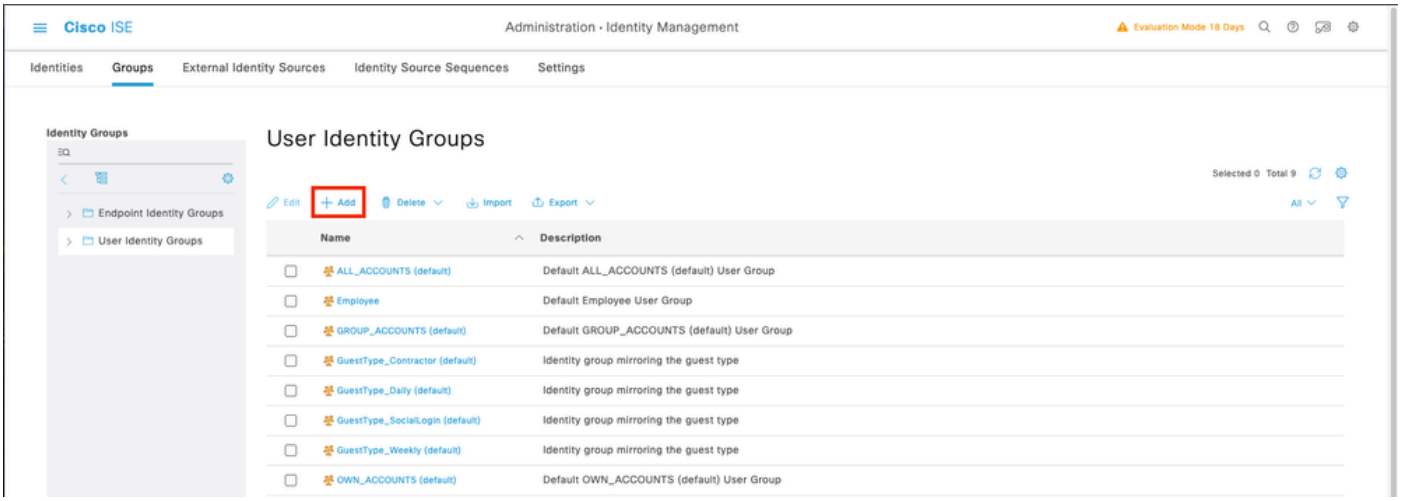
2.1 Role para baixo e clique em Submit (Enviar).



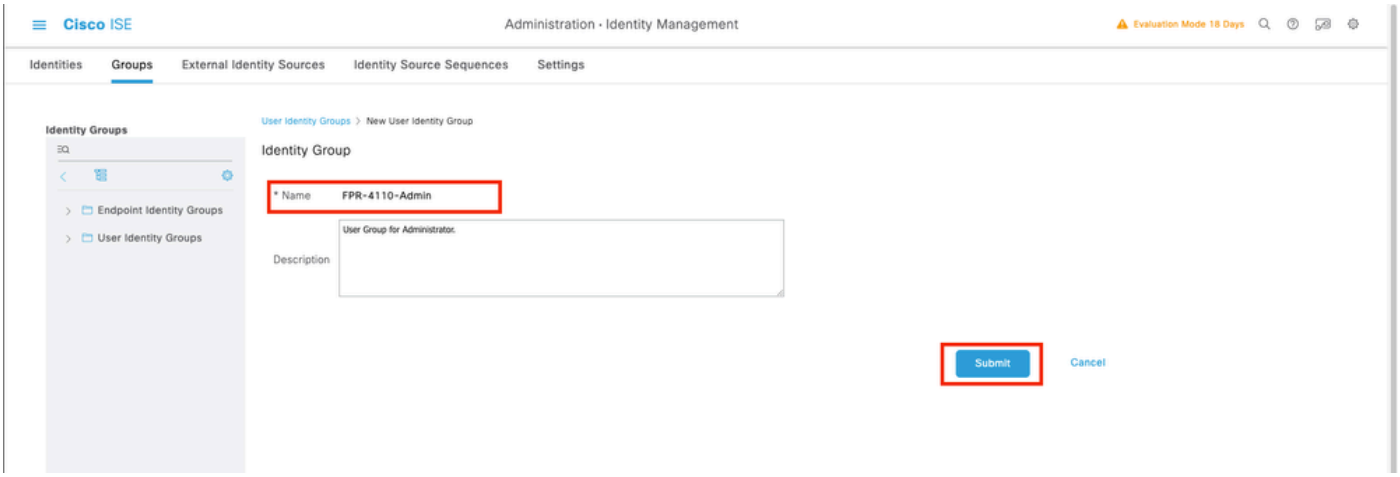
Etapa 3. A opção Validate the new device (Validar o novo dispositivo) é exibida em Network Devices (Dispositivos de rede).



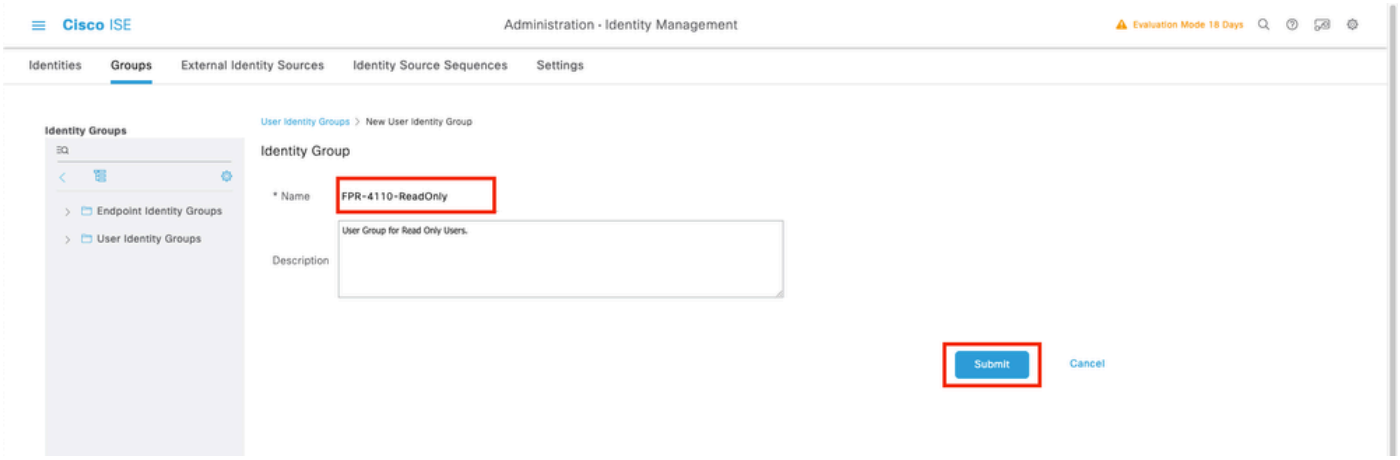
Etapa 4. Crie os Grupos de Identidade de Usuário necessários. Navegue até o ícone de hambúrguer ≡ localizado no canto superior esquerdo > Administração > Gerenciamento de identidade > Grupos > Grupos de identidade do usuário > + Adicionar



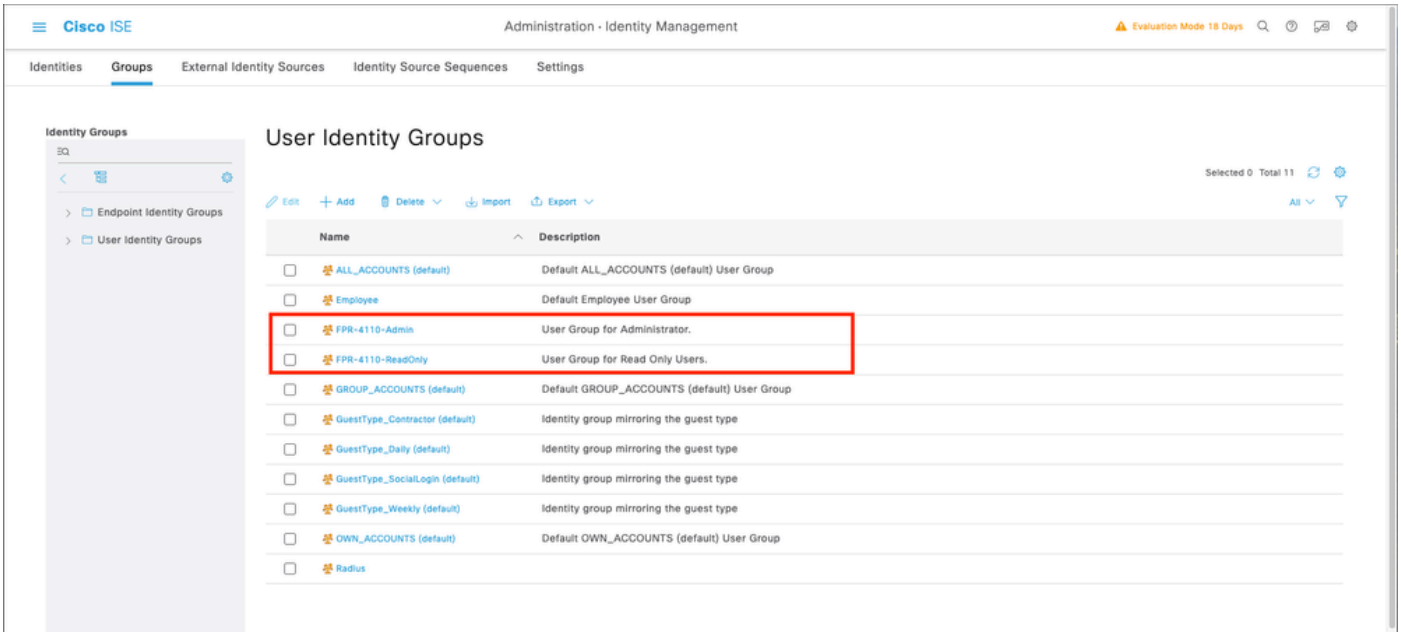
Etapa 5. Defina um nome para o Grupo de Identidade de Usuário Admin e clique em Enviar para salvar a configuração.



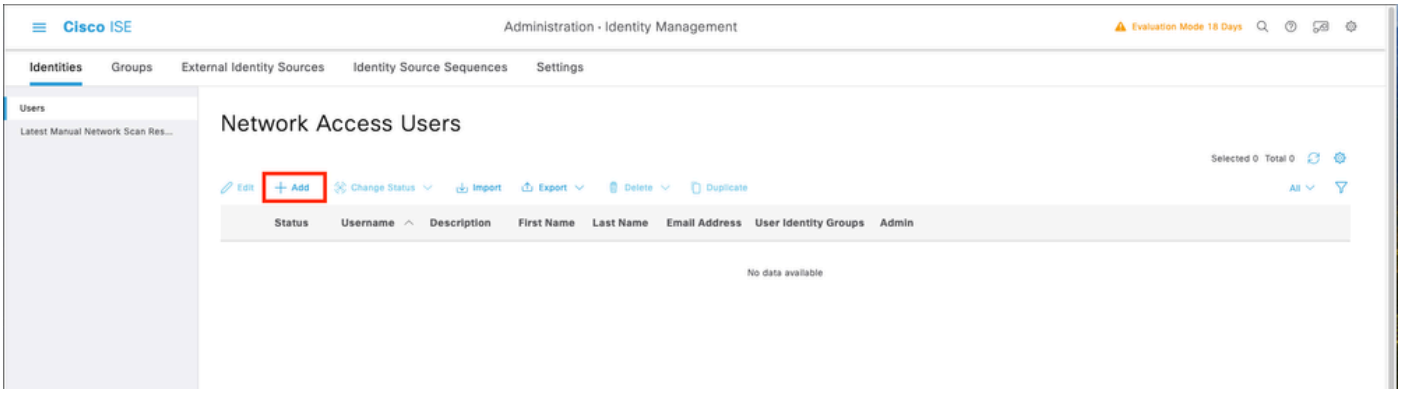
5.1 Repita o mesmo processo para usuários ReadOnly.



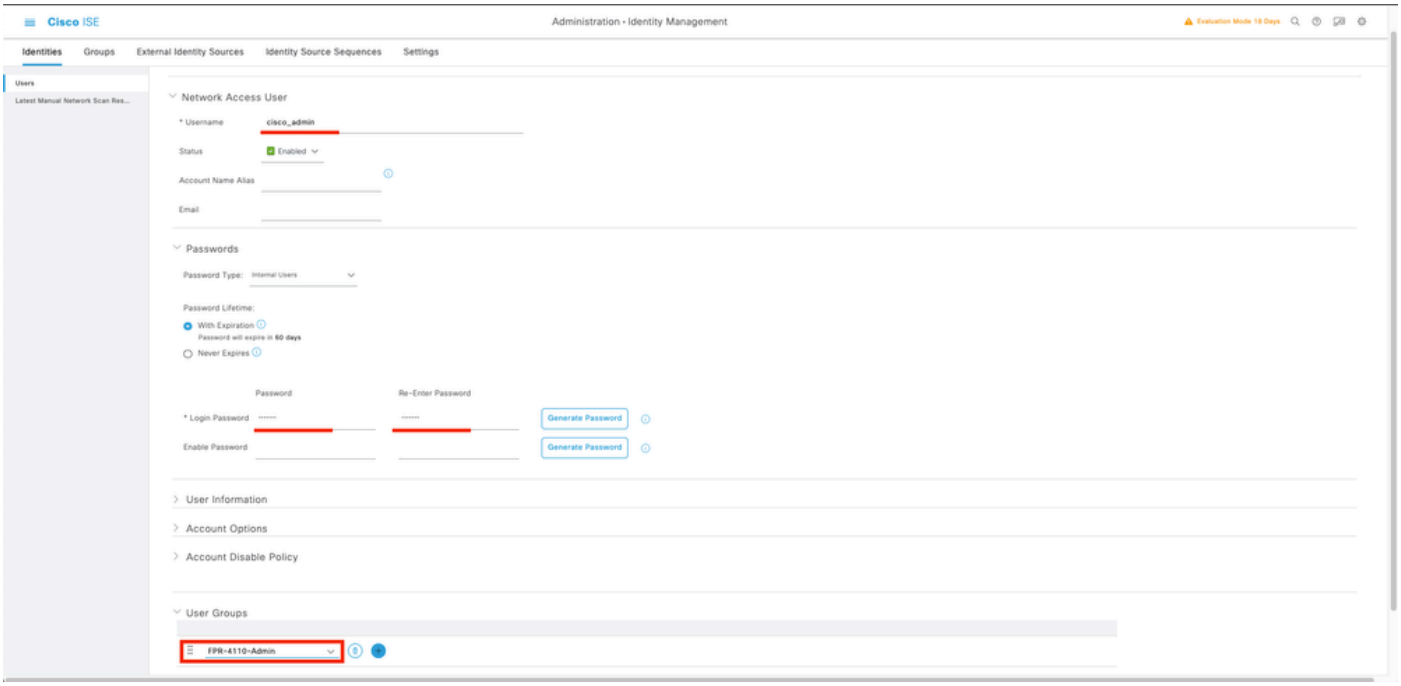
Etapa 6. Valide os novos grupos de usuários que estão sendo exibidos em Grupos de identidade de usuário.



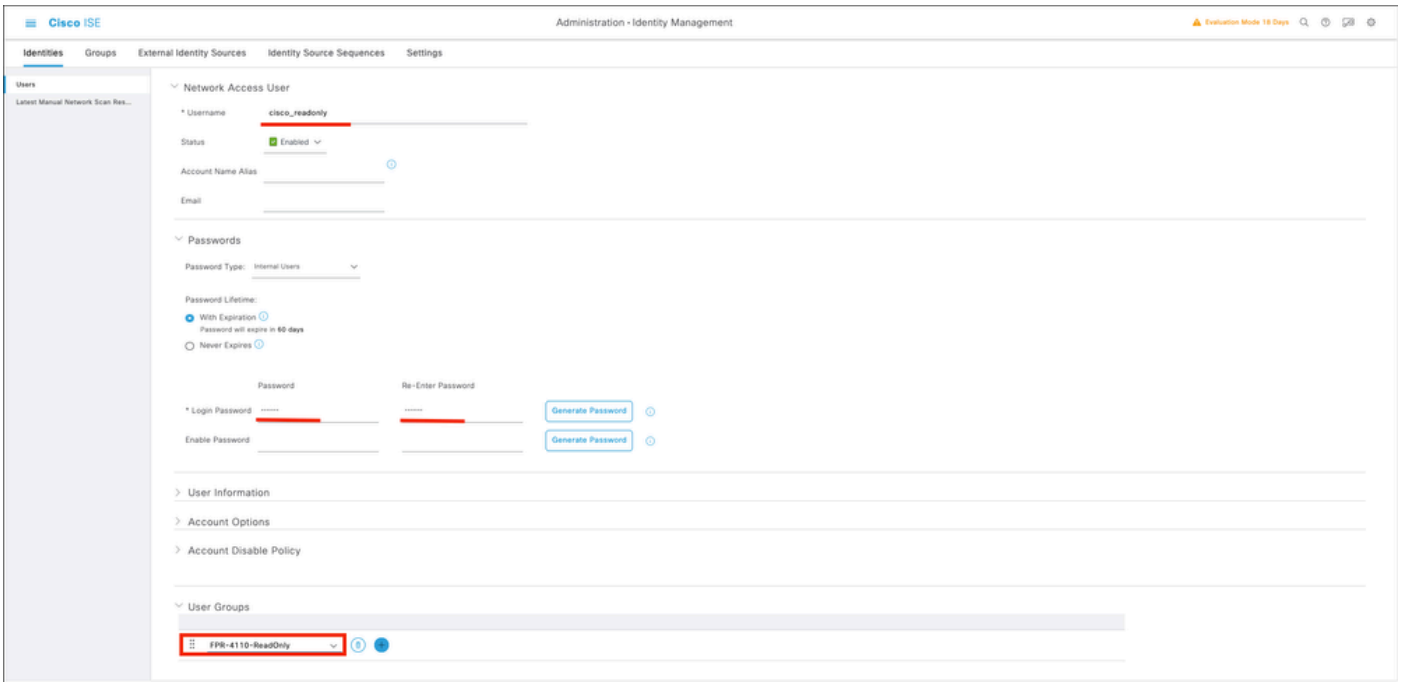
Passo 7. Crie os usuários locais e adicione-os ao seu grupo de correspondentes. Navegue até o ícone de hambúrguer ≡ > Administração > Gerenciamento de Identidades > Identidades > + Adicionar.



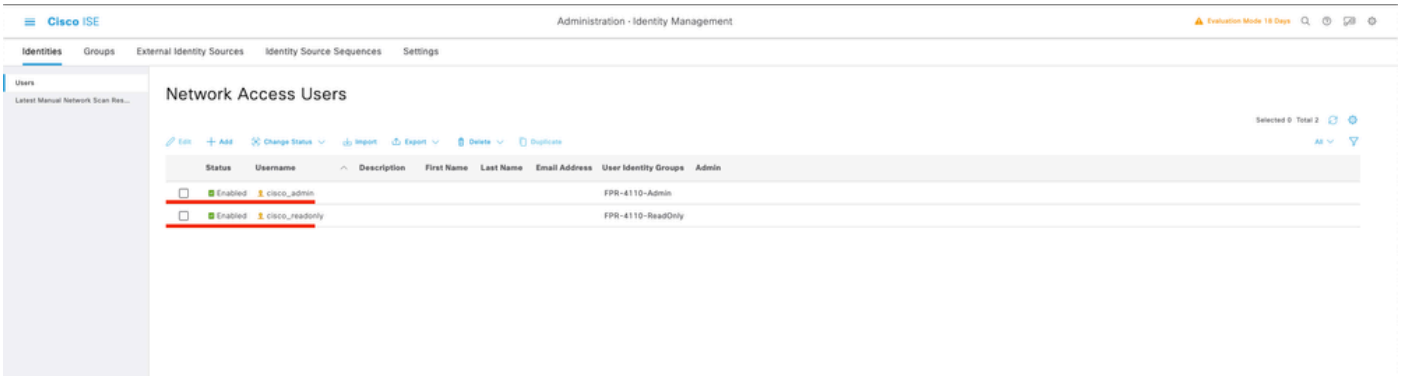
7.1 Adicione o usuário com direitos de Administrador. Defina um nome, uma senha e atribua-os a FPR-4110-Admin, role para baixo e clique em Enviar para salvar as alterações.



7.2 Adicione o usuário com direitos ReadOnly. Defina um nome e uma senha e atribua-os a FPR-4110-ReadOnly, role para baixo e clique em Submit para salvar as alterações.



7.3 Valide se os usuários estão em Network Access Users (Usuários de acesso à rede).



Etapa 8.Crie o perfil de autorização para o usuário Admin.

O chassi FXOS inclui as seguintes funções de usuário:

- Administrador - Acesso completo de leitura e gravação a todo o sistema. A conta de administrador padrão recebe essa função por padrão e não pode ser alterada.
- Somente Leitura - Acesso somente leitura à configuração do sistema sem privilégios para modificar o estado do sistema.
- Operações - Acesso de leitura e gravação à configuração NTP, configuração do Smart Call Home para Smart Licensing e logs do sistema, incluindo servidores e falhas do syslog. Acesso de leitura ao restante do sistema.
- AAA - Acesso de leitura e gravação a usuários, funções e configuração AAA. Acesso de leitura ao restante do sistema

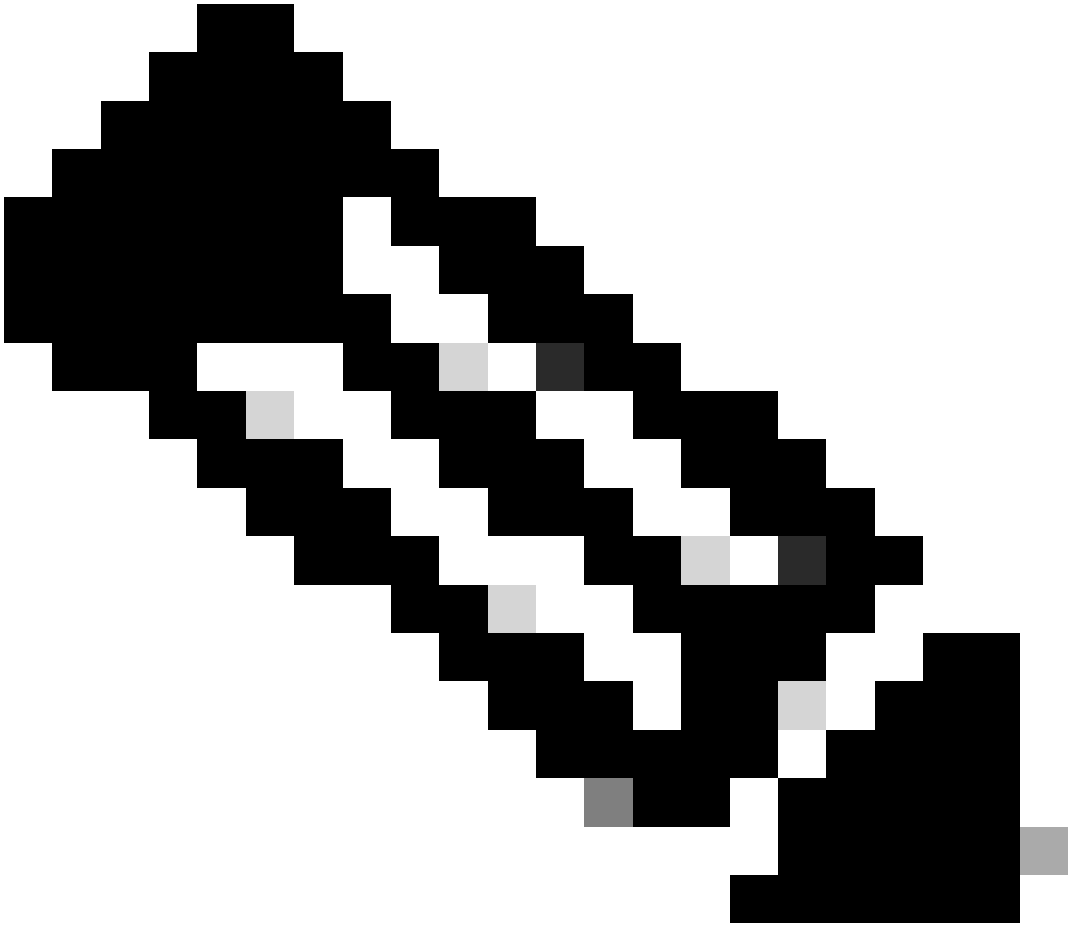
Atribuições para cada função:

cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

cisco-av-pair=shell:roles="operações"

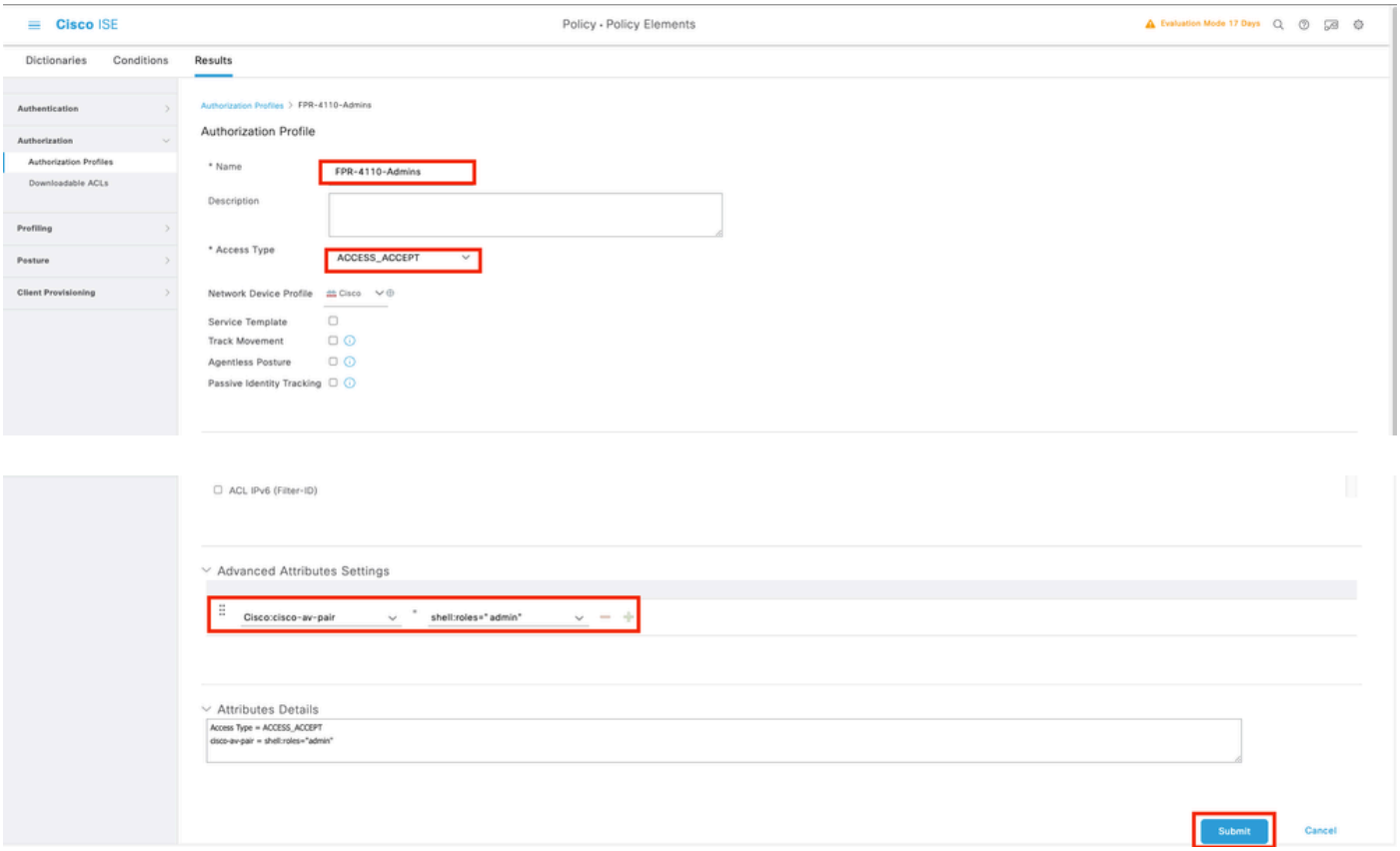
cisco-av-pair=shell:roles="somente leitura"



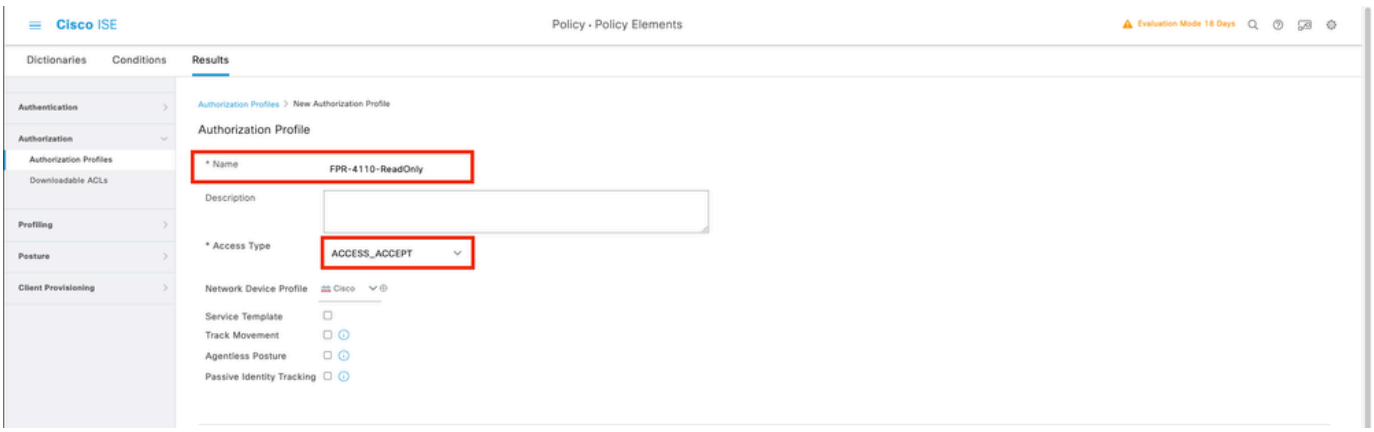
Observação: esta documentação define apenas atributos admin e somente leitura.

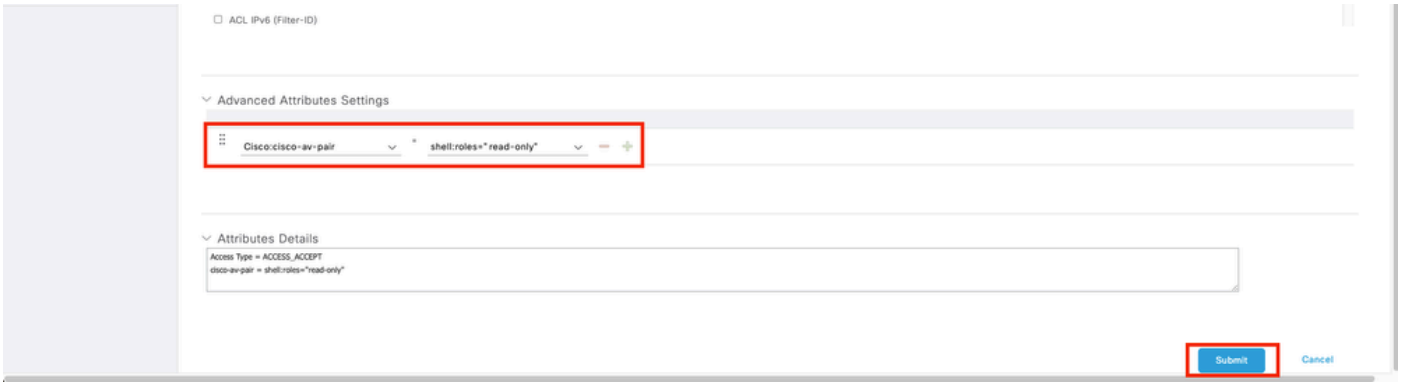
Navegue até o ícone de hambúrguer ≡ > Política > Elementos de Política > Resultados > Autorização > Perfis de Autorização > +Adicionar.

Defina um nome para o perfil de autorização, deixe Tipo de acesso como ACCESS_ACCEPT e em Configurações avançadas de atributos adicione cisco-av-pair=shell:roles="admin" com e clique em Enviar.



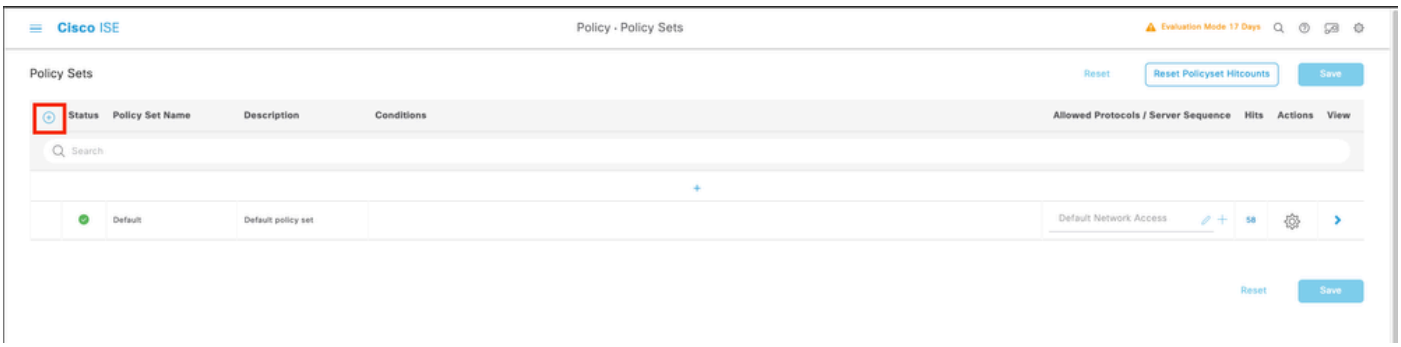
8.1 Repita a etapa anterior para criar o perfil de autorização para o usuário somente leitura. Crie a classe Radius com o valor read-only Administrator desta vez.



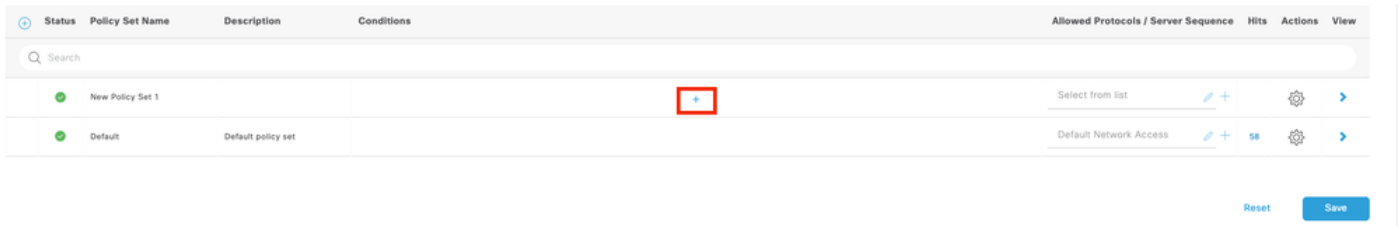


Etapa 9.Crie um conjunto de políticas correspondente ao endereço IP do FMC. Isso evita que outros dispositivos concedam acesso aos usuários.

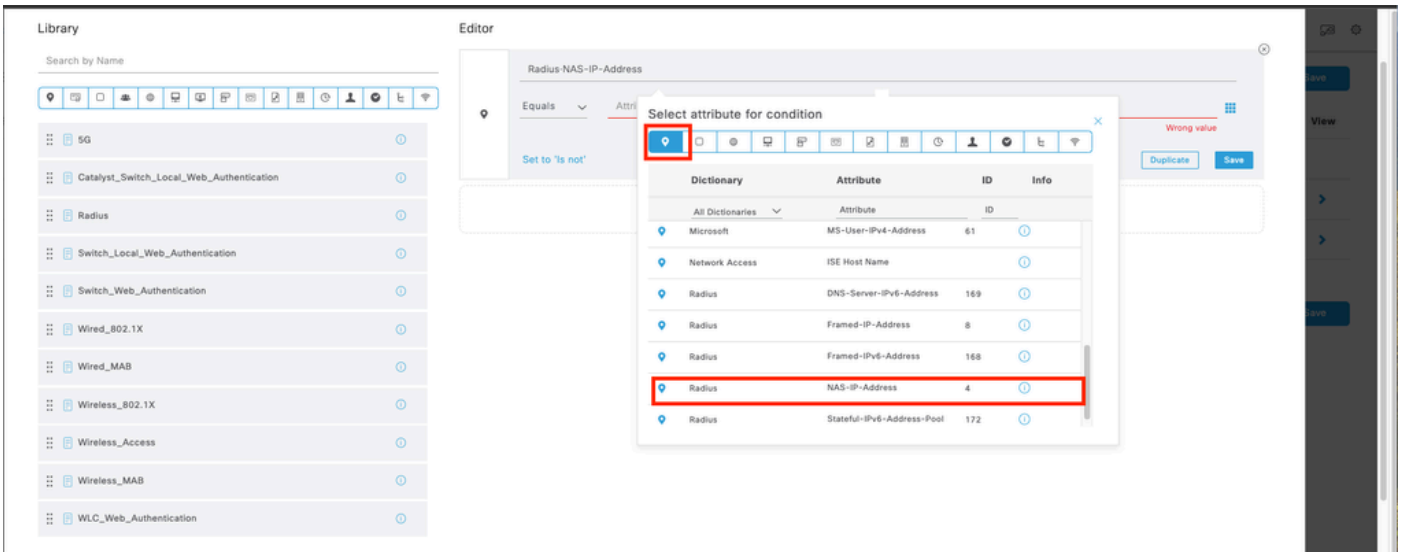
Navegue para ≡ > Política > Conjuntos de políticas >Adicionar sinal de ícone no canto superior esquerdo.

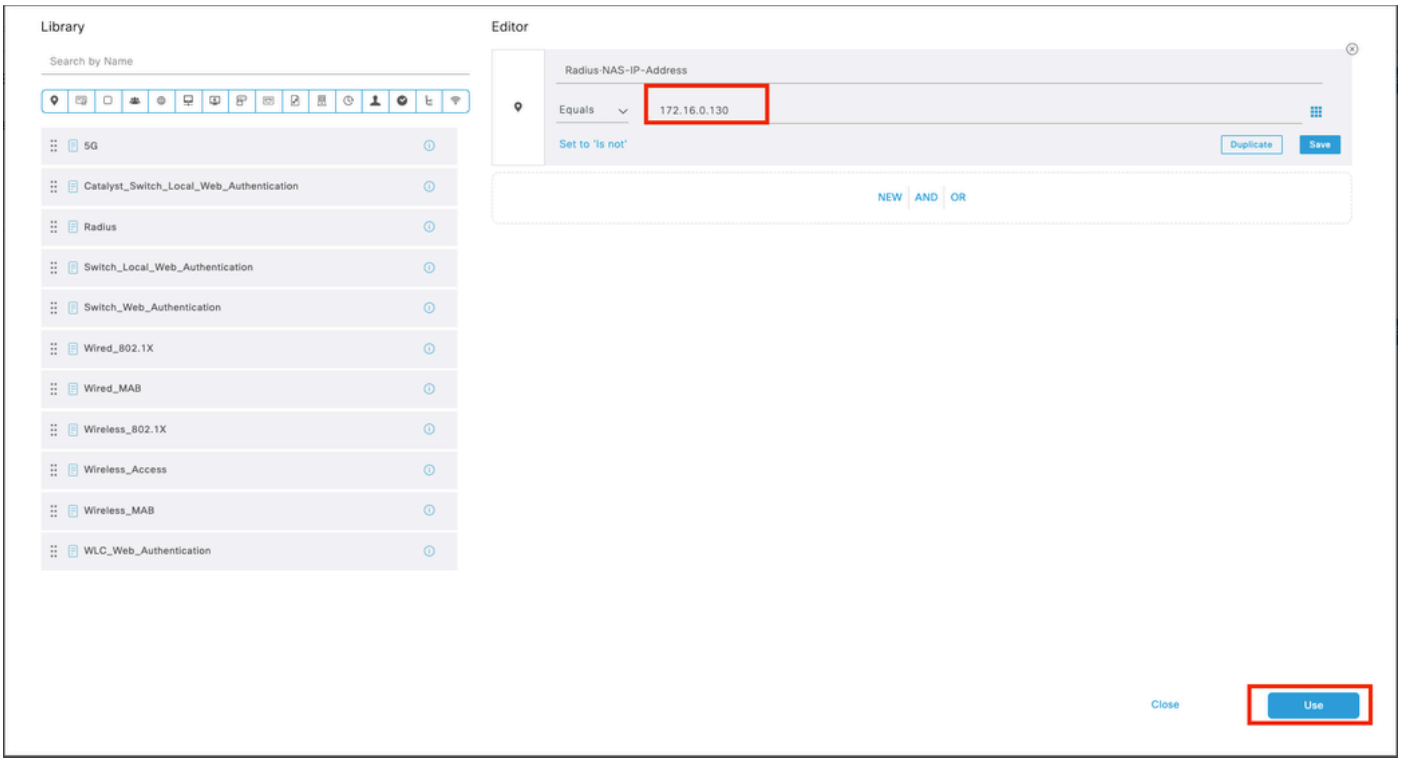


9.1 Uma nova linha é colocada na parte superior de seus conjuntos de políticas. Clique no ícone Adicionar para configurar uma nova condição.

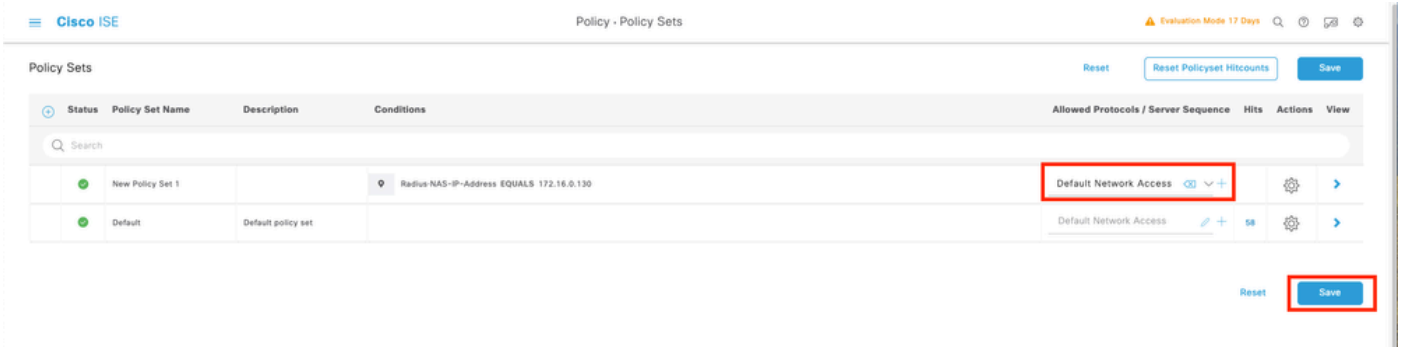


9.2 Adicione uma condição superior para o atributo RADIUS NAS-IP-Addresscorrespondente ao endereço IP do FCM e clique em Usar.





9.3 Depois de concluir, clique em Save.

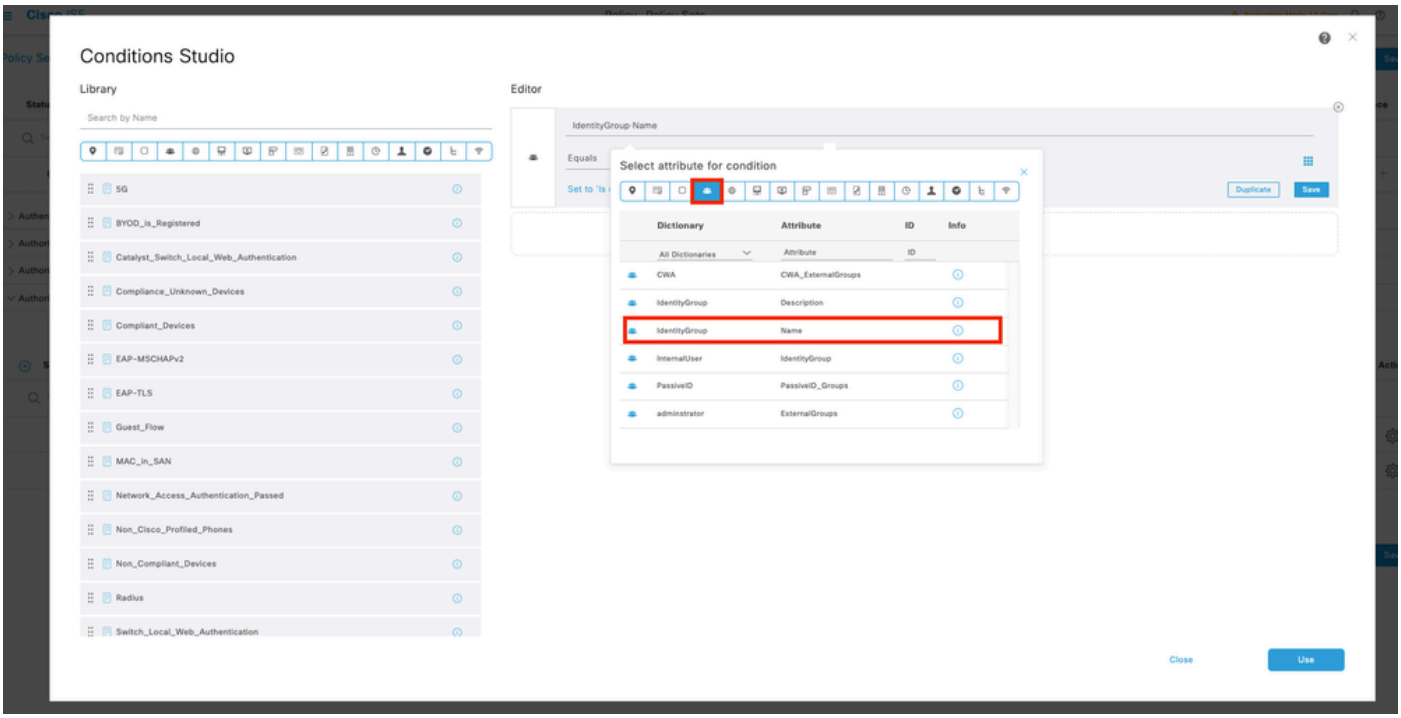


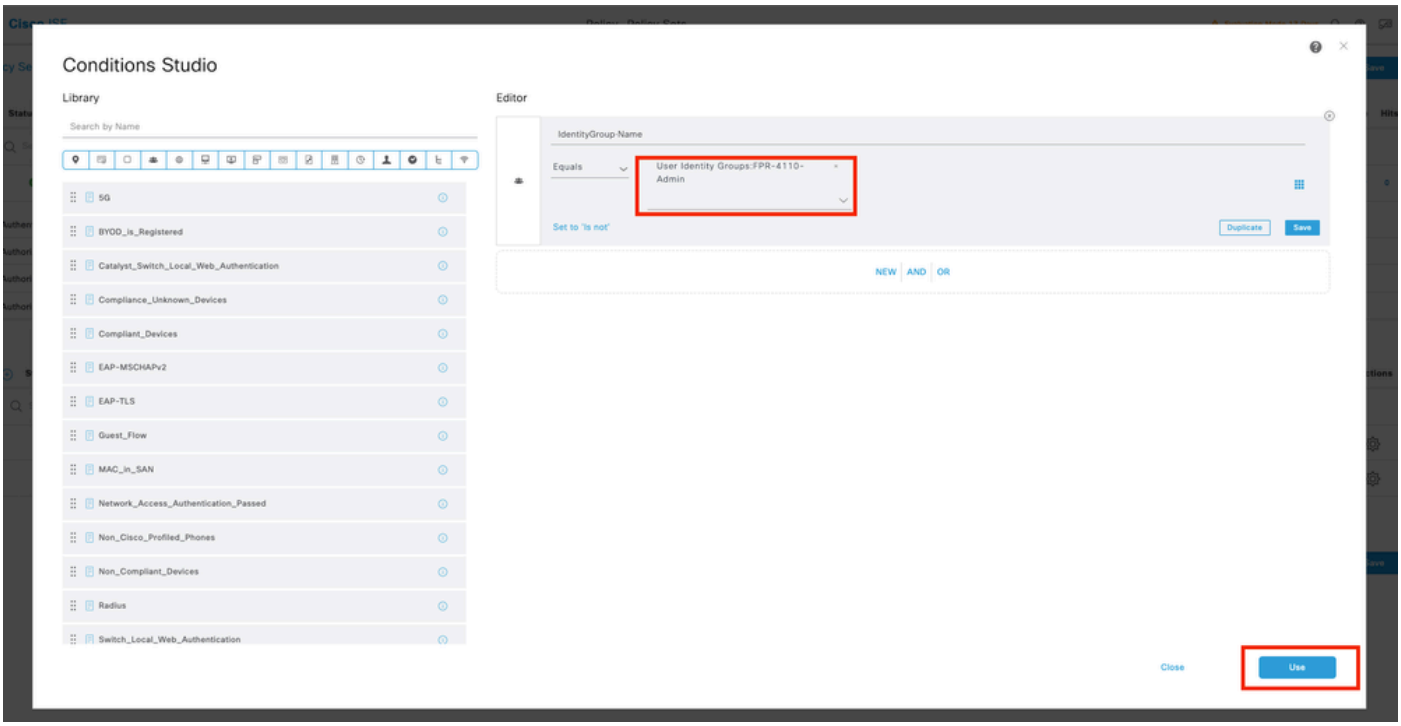
Dica: para este exercício, permitimos a lista Default Network Access Protocols. Você pode criar uma nova lista e restringi-la conforme necessário.

Etapa 10. Visualize o novo conjunto de políticas, pressionando o ícone >colocado no final da linha.

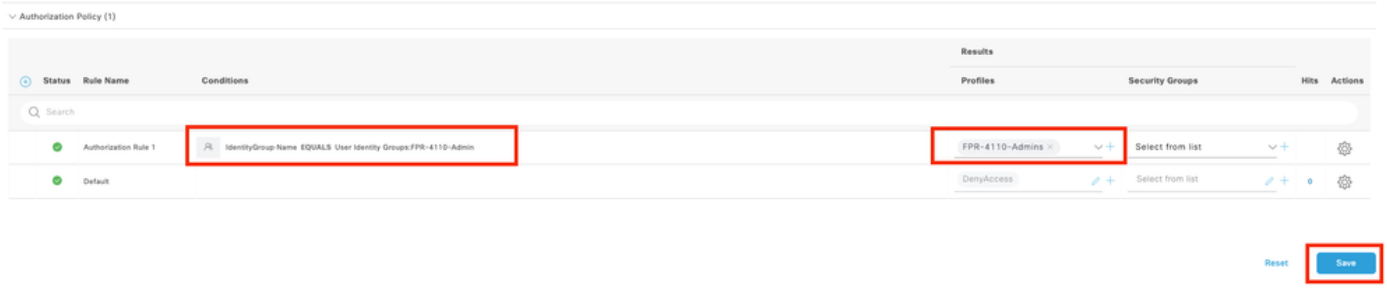
10.1 Expanda o menu Authorization Policy e clique em (+) para adicionar uma nova condição.

10.2 Defina as condições para corresponder ao grupo DictionaryIdentity com AttributeName igual a User Identity Groups: FPR-4110-Admins(o nome do grupo criado na Etapa 7) e clickUse.





Etapa 10.3 Validar que a nova condição está configurada na política de autorização e adicionar um perfil de usuário em Perfis.



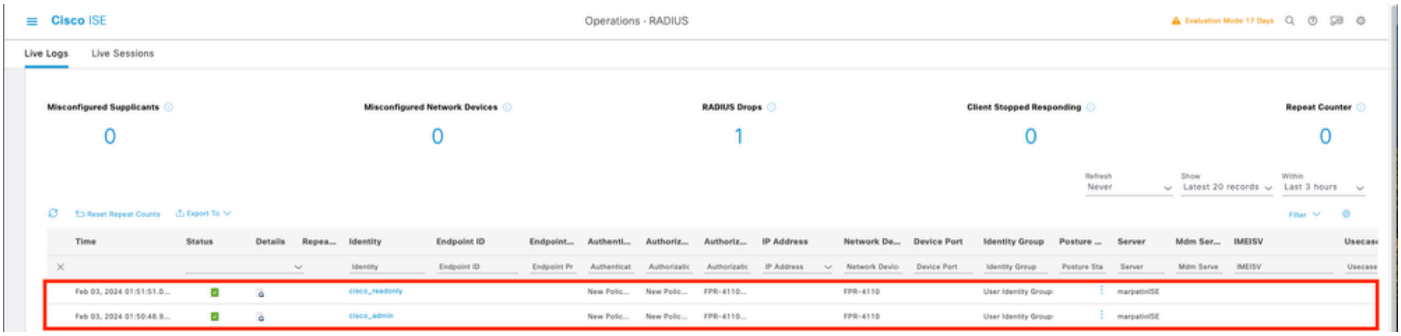
Etapa 11. Repita o mesmo processo na etapa 9 para Read-only Users e clique em Save.

Verificar

1. Tente fazer login na GUI do FCM usando as novas credenciais do Radius

2. Navegue até o ícone do hambúrguer ≡ > Operações > Raio > Registros ao vivo.

3. As informações exibidas mostram se um usuário efetuou login com êxito.



4. Validar a função Usuários registrados na CLI do Chassi do Firewall Seguro.

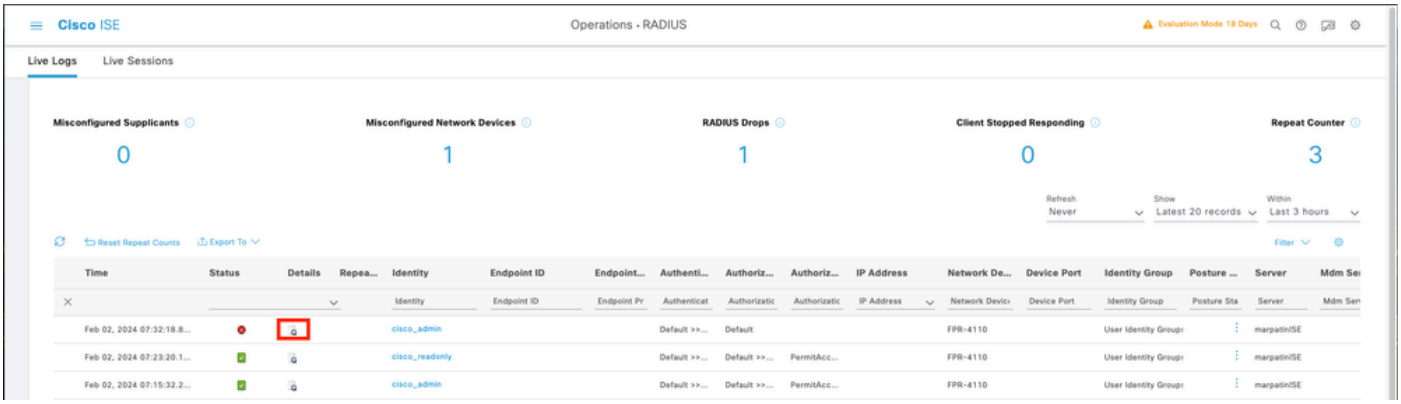
```
FPR4K-1-029A78B# scope se
security         server           service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
    Description:
    User Roles:
        Name: admin
        Name: read-only
FPR4K-1-029A78B /security #
```

Troubleshooting

1. Na GUI do ISE , navegue até o ícone de hambúrguer ≡ > Operações > Radius > Registros ao vivo.

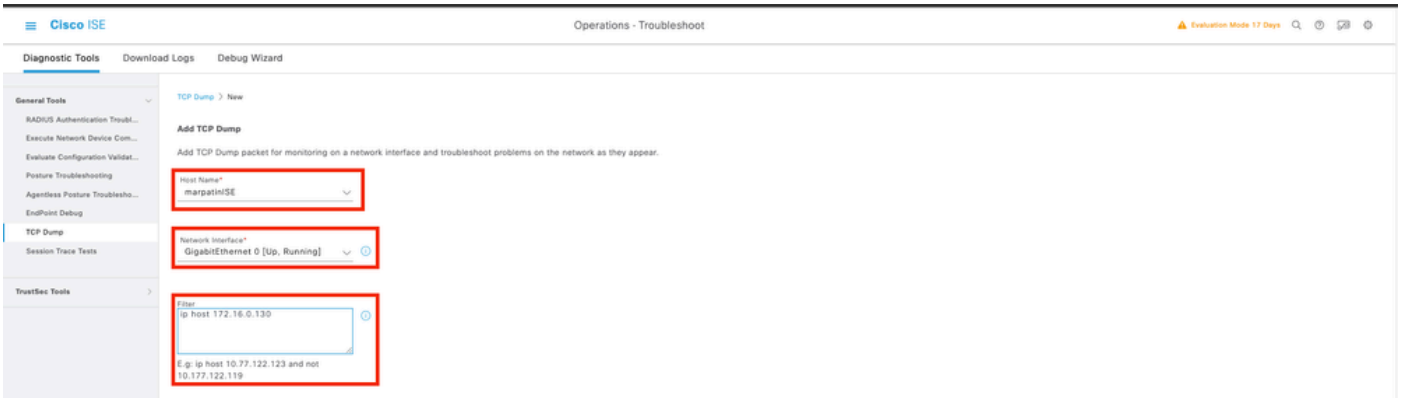
1.1 Valide se a solicitação de sessão de log está alcançando o nó do ISE.
1.2 Para status de falha, revise os detalhes da sessão.



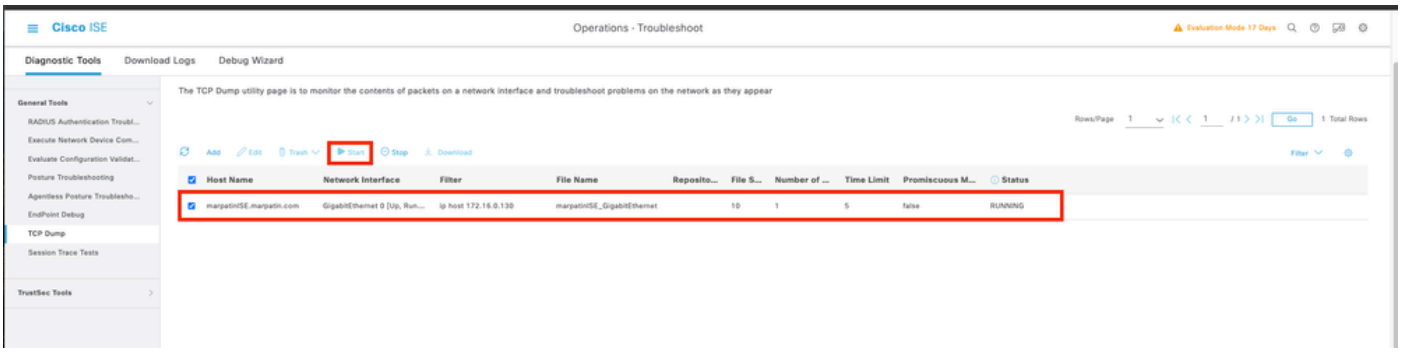
2. Para solicitações que não aparecem nos logs do Radius Live , revise se a solicitação UDP está alcançando o nó ISE por meio de uma captura de pacote.

Navegue até o ícone de hambúrguer ≡ > Operações > Solução de problemas > Ferramentas de diagnóstico > dump TCP. Adicione uma nova captura e baixe o arquivo em sua máquina local para verificar se os pacotes UDP estão chegando ao nó ISE.

2.1 Preencha as informações solicitadas, role para baixo e clique em Save.



2.2 Selecione e inicie a captura.



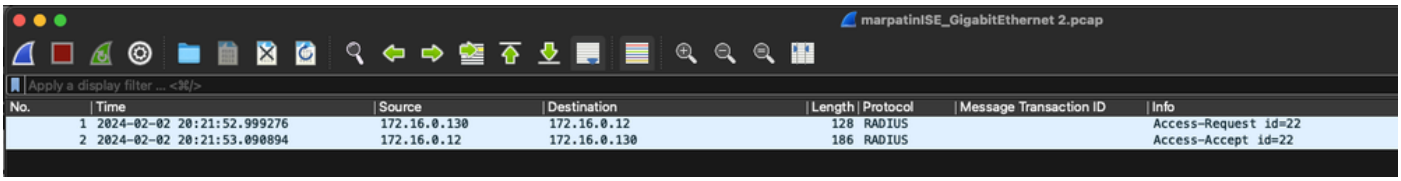
2.3 Tentativa de fazer login no chassi do firewall seguro enquanto a captura do ISE está em execução

2.4 Pare o despejo TCP no ISE e baixe o arquivo para uma máquina local.

2.5 Reveja a saída do tráfego.

Saída esperada:

Pacote No1. Solicitação do firewall seguro para o servidor ISE através da porta 1812 (RADIUS)
Pacote No2. Resposta do servidor ISE aceitando a solicitação inicial.



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.