Configurar Autorização Cert RAVPN e Autorização ISE no FMC

Contents

Introdução

Este documento descreve a configuração das políticas de autorização do servidor ISE para autenticação de certificado em conexões RAVPN gerenciadas por CSF no FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall (CSF)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Identity Services Engine (ISE)
- Noções básicas de Registro de Certificado e SSL.
- autoridade de certificado (CA)

Componentes Utilizados

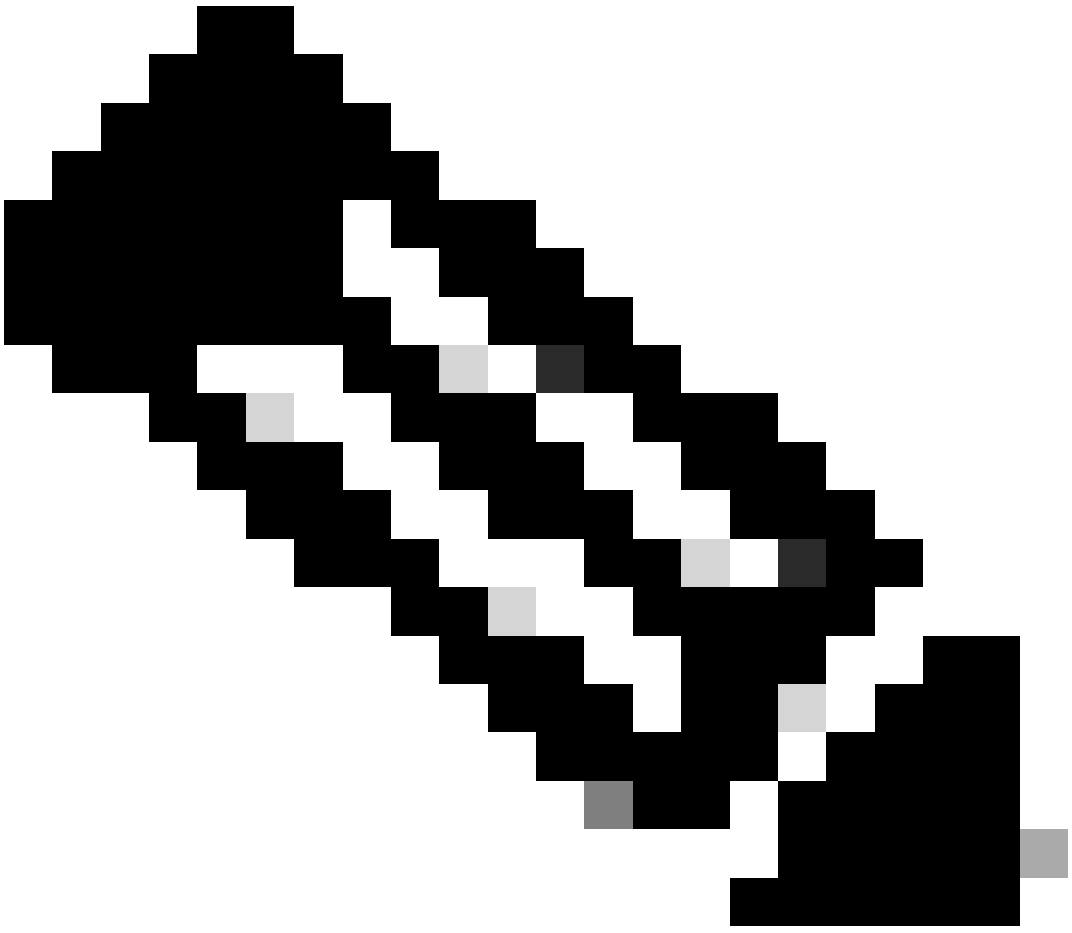
O conteúdo deste documento é baseado nessas versões de software e hardware.

- Cisco Secure Client Versão 5.1.6
- Cisco Secure Firewall versão 7.2.8
- Cisco Secure Firewall Management Center versão 7.2.8

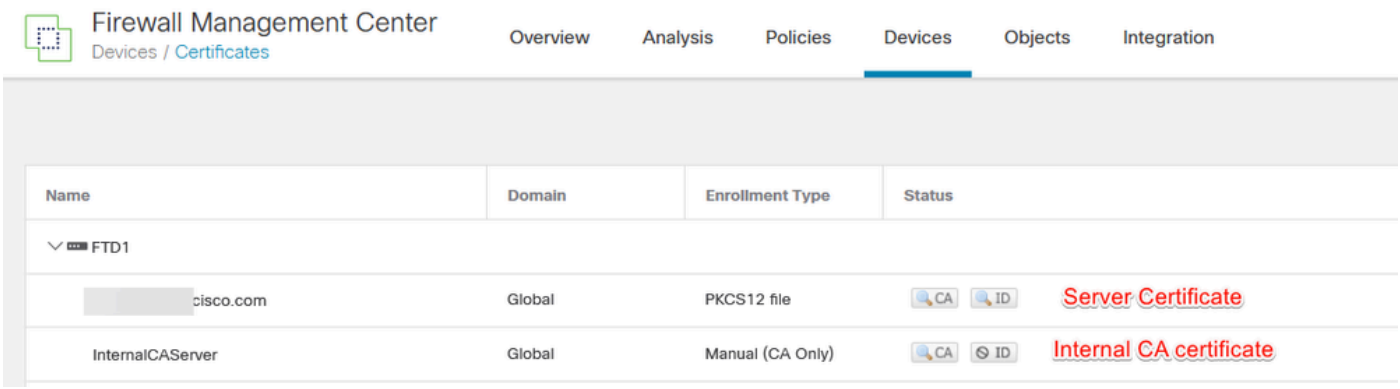
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configurar

Etapa 1: Instalar um Certificado de CA Confiável



Observação: esta etapa precisará ser seguida se o certificado CA for diferente daquele usado para a autenticação do servidor. Se o mesmo servidor de CA emitir os certificados dos usuários, não será necessário importar o mesmo certificado de CA novamente.

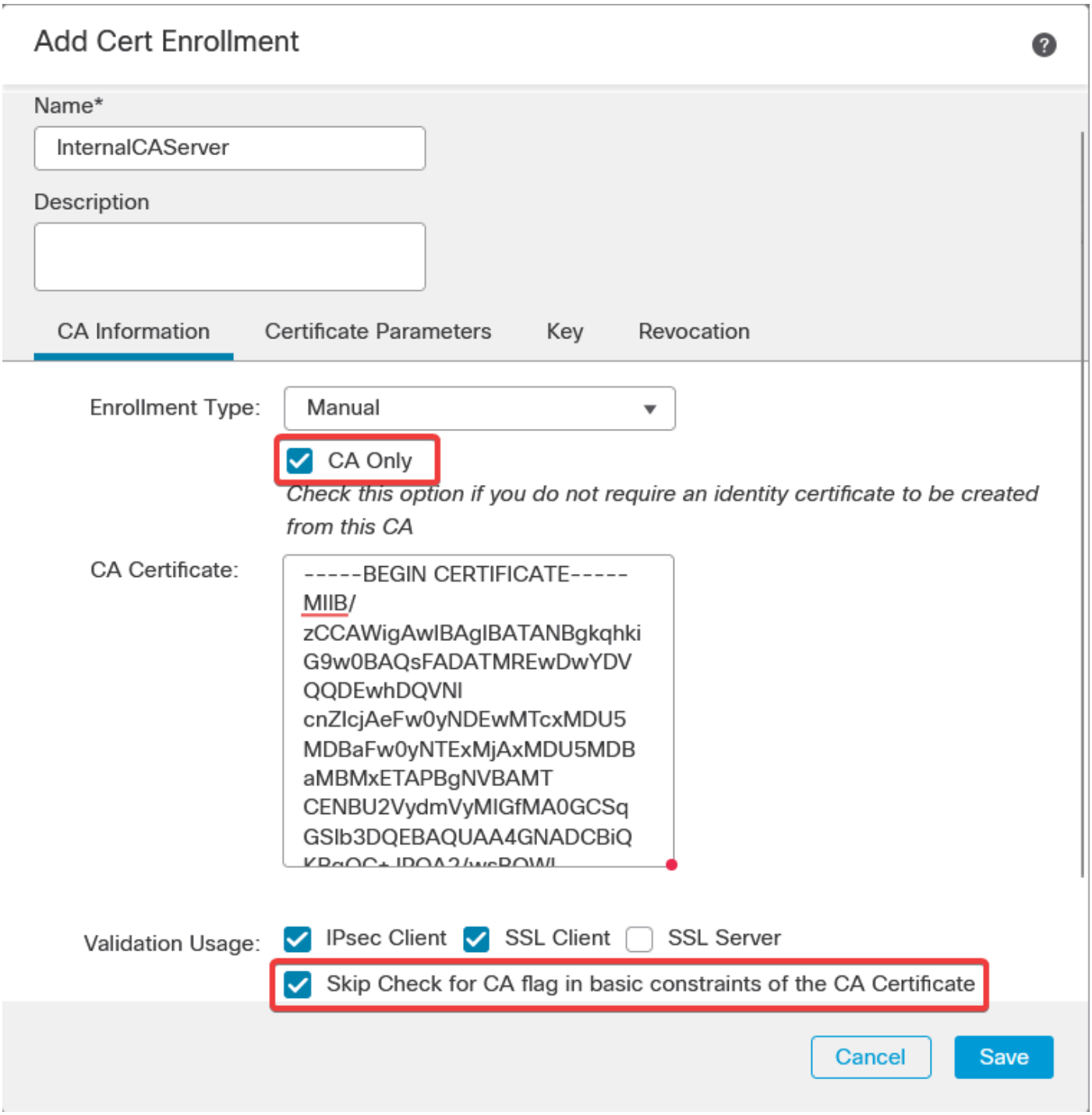


a. Navegue atéDevices > Certificatese clique em **Add**.

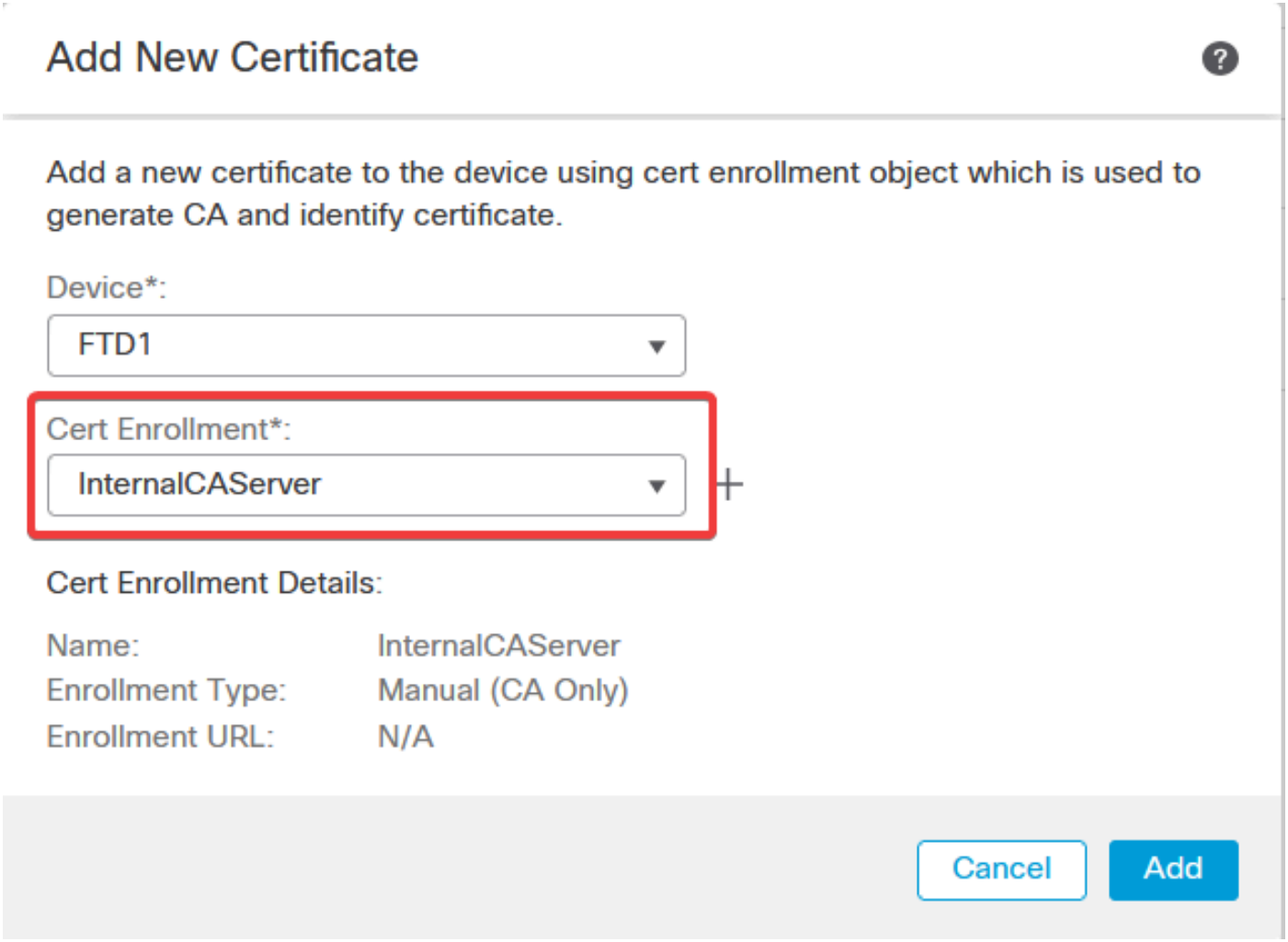
b. Informe um **trustpoint name** e selecione Manual como o tipo de inscrição em Informações da CA.

c. VerifiqueCA Onlye cole o certificado CA confiável/interno no formato pem.

d. Marque **Skip Check for CA flag in basic constraints of the CA Certificate** e clique em **Save**.

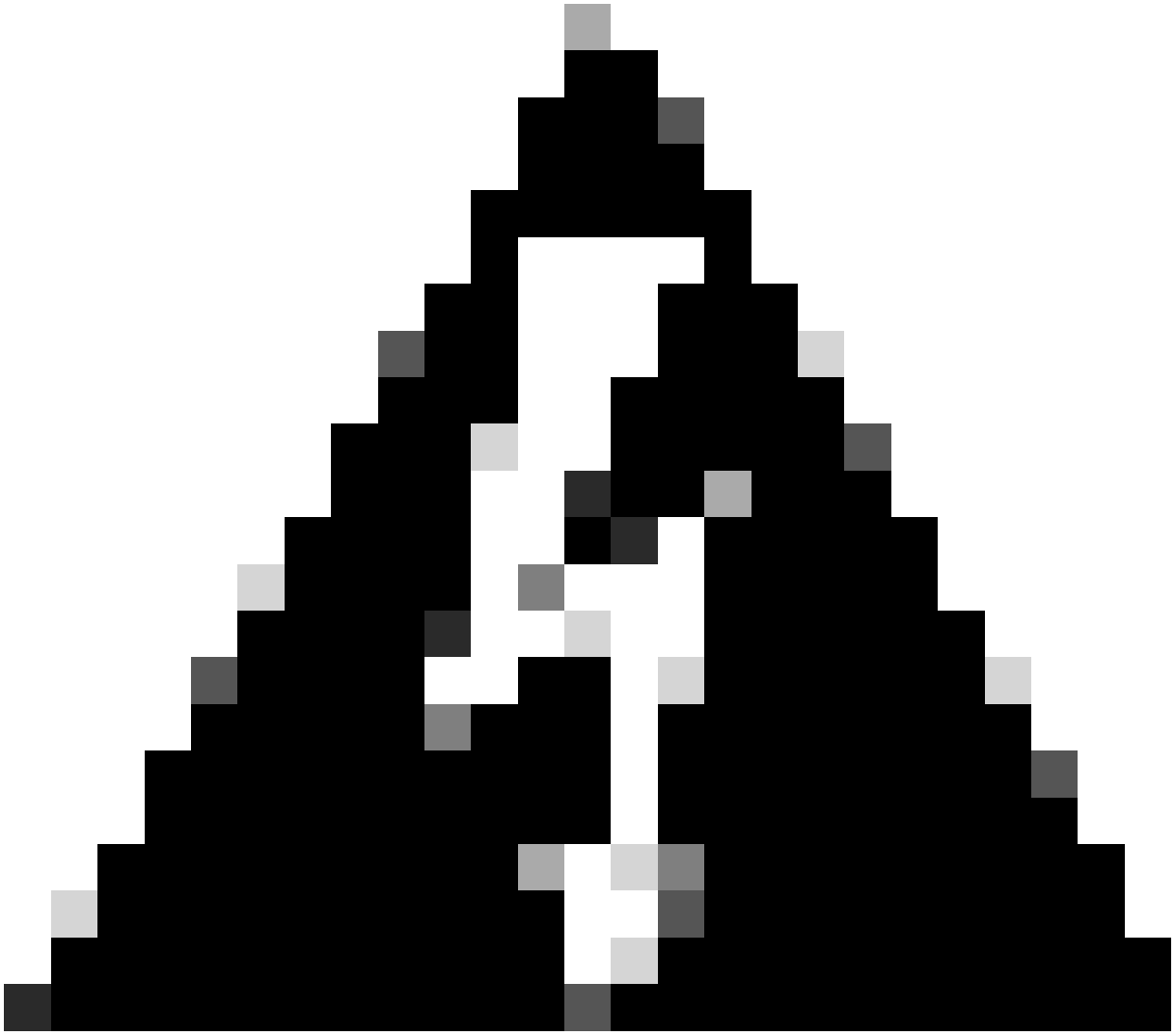


e. Em **Cert Enrollment**, selecione o **trustpoint** na lista suspensa que acabou de ser criada e clique em **Add.**

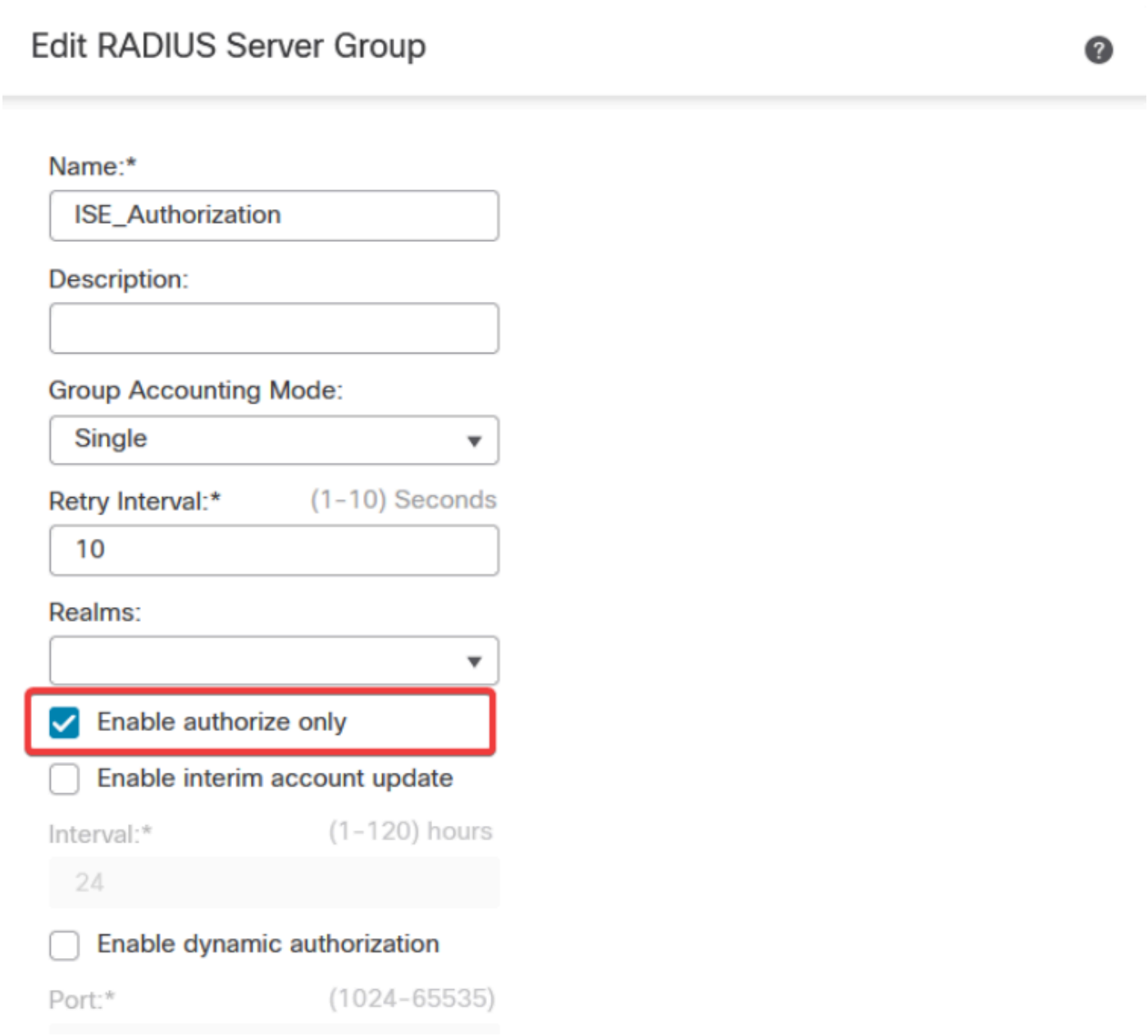


Etapa 2: Configurar o grupo de servidores ISE/Radius e o perfil de conexão

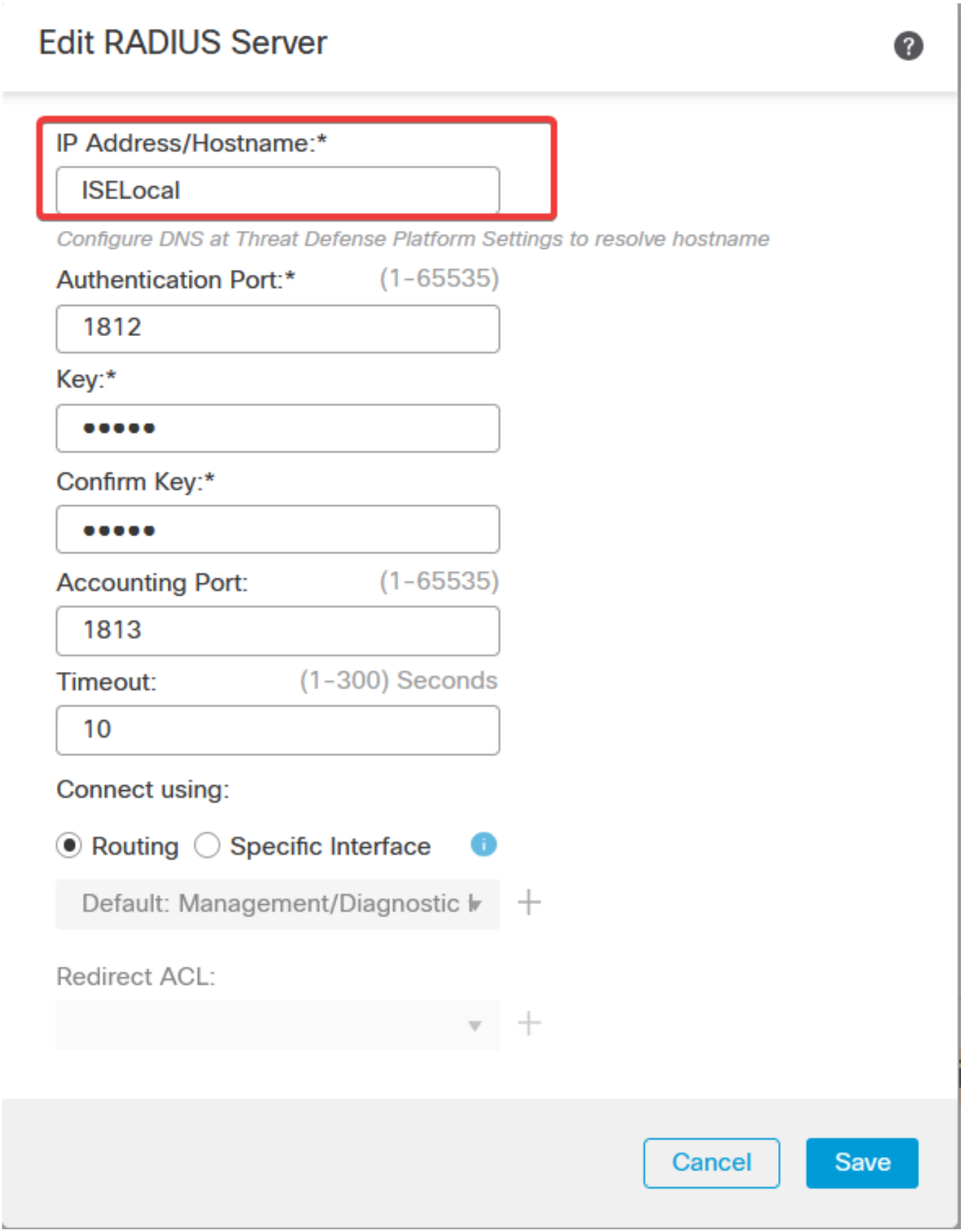
a. Navegue até **Objects > AAA Server > RADIUS Server Group** e clique em **Add RADIUS Server Group**. Opção de verificação**Enable authorize only**.



Aviso: se a opção Ativar somente autorização não estiver marcada, o firewall enviará uma solicitação de autenticação. No entanto, o ISE espera receber um nome de usuário e uma senha com essa solicitação, e uma senha não é usada em certificados. Como resultado, o ISE marca a solicitação como falha de autenticação.

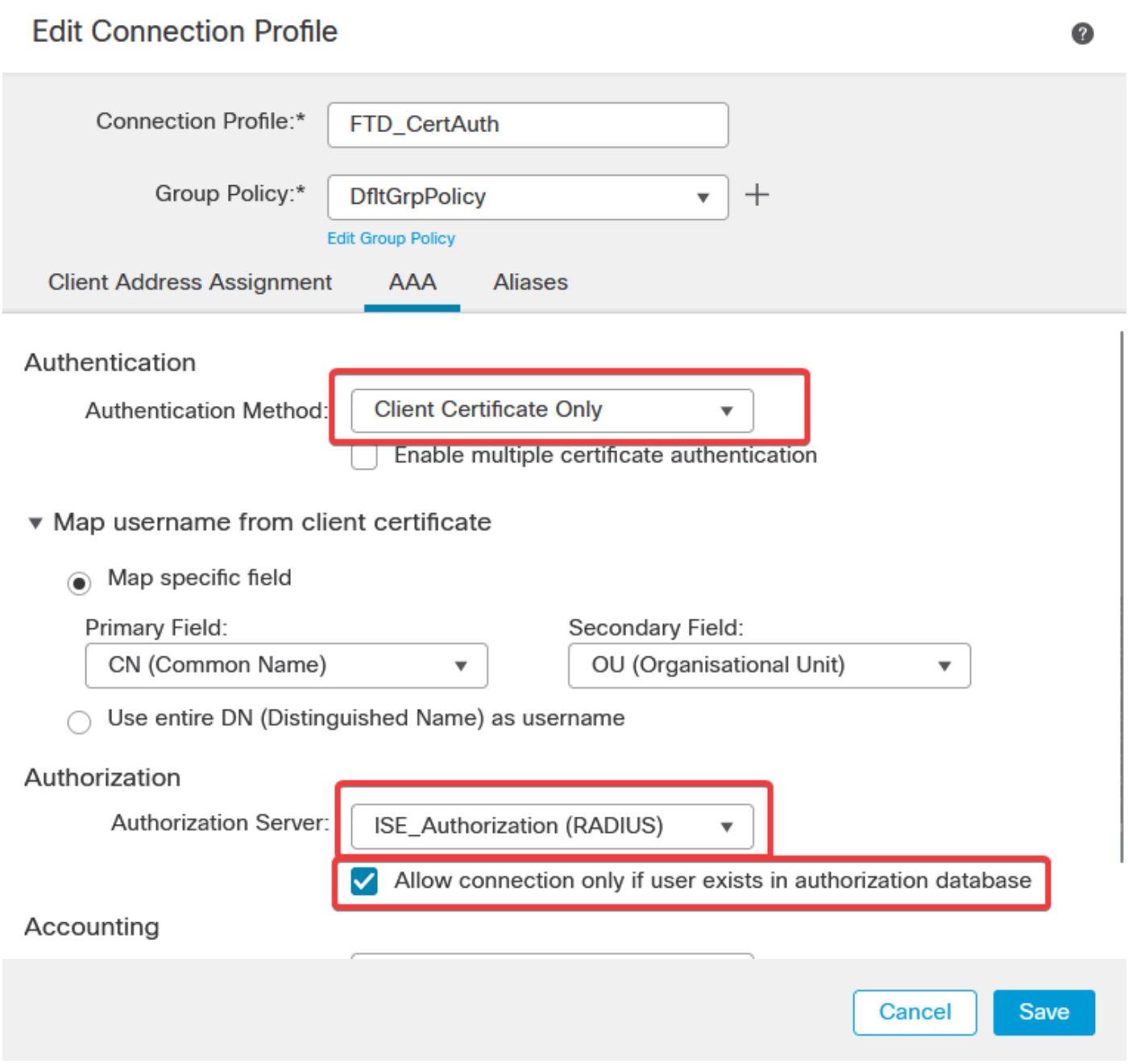


b. Clique **Add (+)** no ícone e adicione oRadius server/ISE serverusando o endereço IP ou um nome de host.



c. Navegue até **Devices** > **Remote Access configuration** . Crie umnew connection profilee defina o método de autenticação comoClient Certificate Only. Para o Servidor de Autorização, escolha aquele que foi criado nas etapas anteriores.

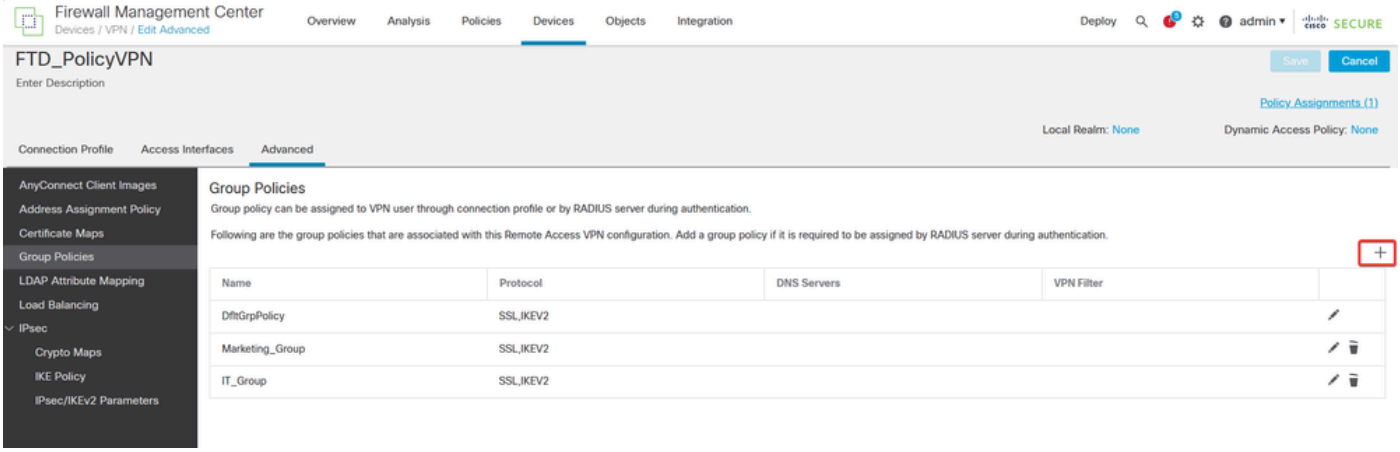
Certifique-se de marcar a **Allow connection only if user exists in authorization database** opção. Esta configuração garante que a conexão ao RAVPN seja concluída somente se a autorização for permitida.



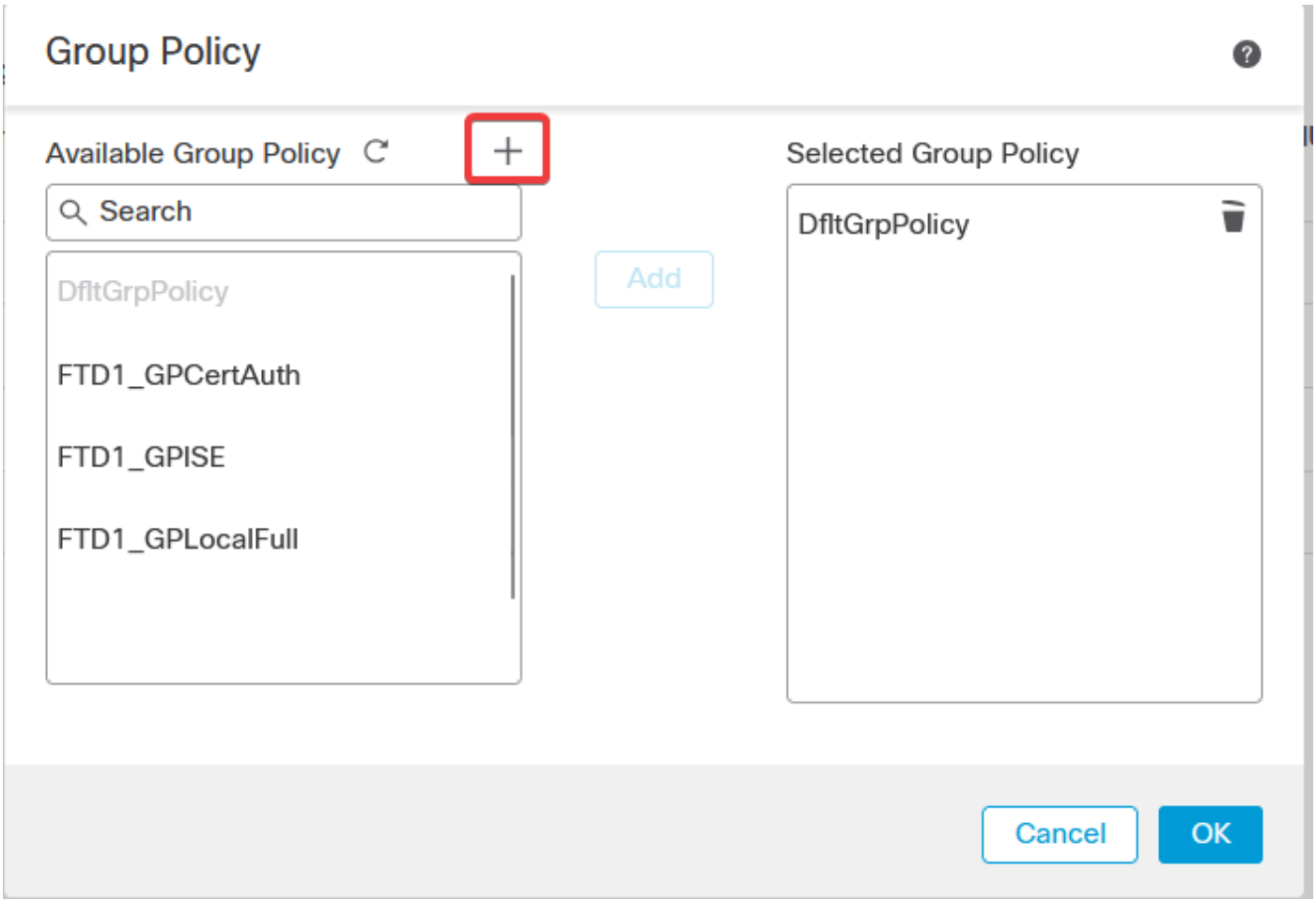
Mapear Nome de Usuário do certificado do cliente se refere às informações obtidas do certificado para identificar o usuário. Neste exemplo, você mantém a configuração padrão, mas ela pode ser alterada dependendo de quais informações são usadas para identificar os usuários.

Clique em **.Save**

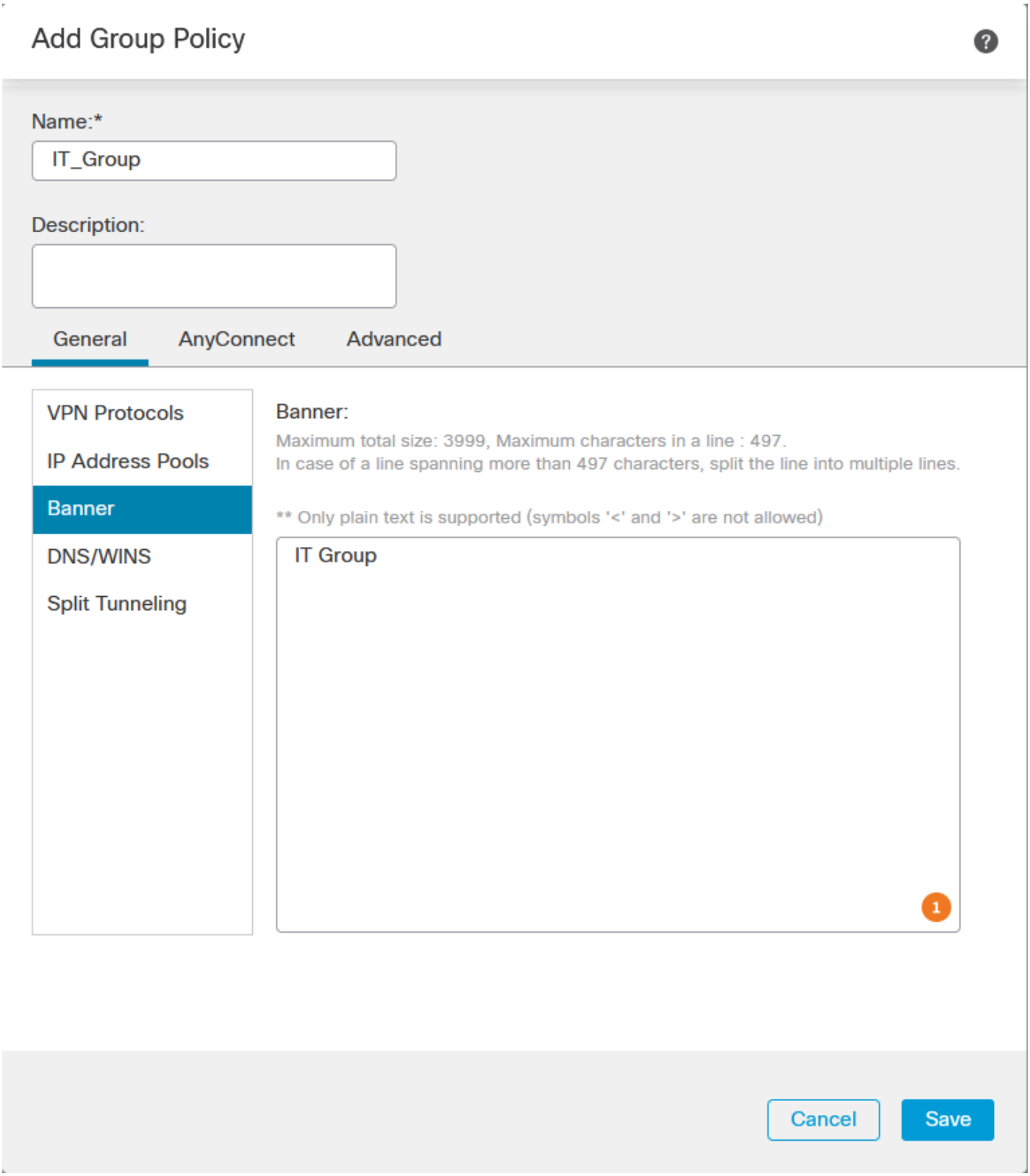
d. Navegue até **Advanced** > **Group Policies**. Clique **Add (+)** no ícone do lado direito.



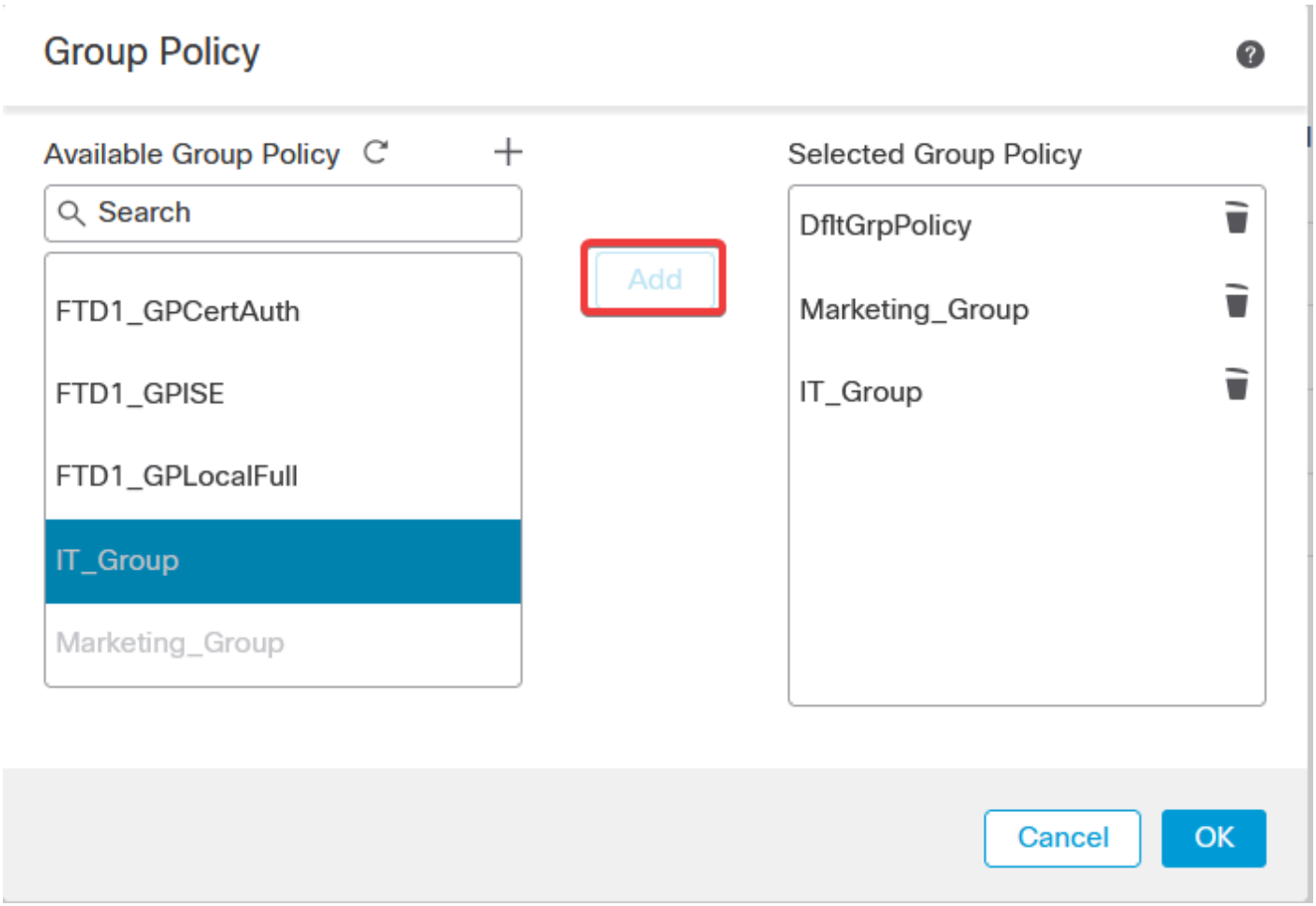
e. Crie o **group policies**. Cada política de grupo é configurada com base nos grupos da organização e nas redes que cada grupo pode acessar.



f. Na política de grupo, execute as configurações específicas de cada grupo. Uma mensagem de banner pode ser adicionada para ser exibida após uma conexão bem-sucedida.



g. Selecione o **group policies** no lado esquerdo e cliqueAddpara movê-lo para o lado direito. Isso especifica quais políticas de grupo estão sendo usadas na configuração.

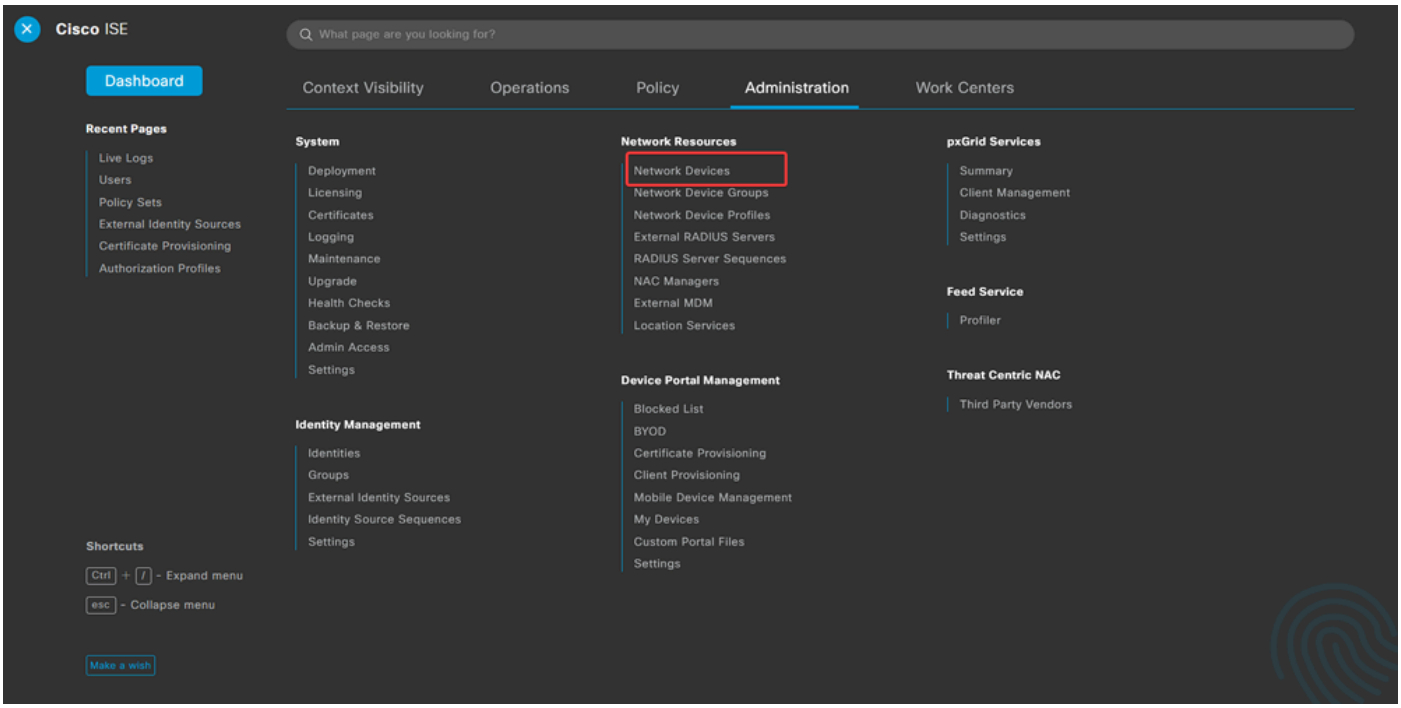


e. Implante as alterações.

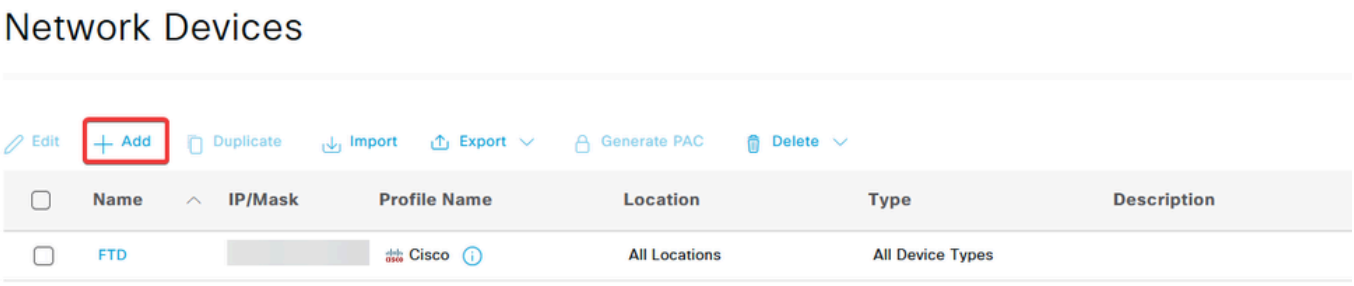
Etapa 3: Configurar o ISE

Etapa 3.1: Criar usuários, grupos e perfil de autenticação de certificado

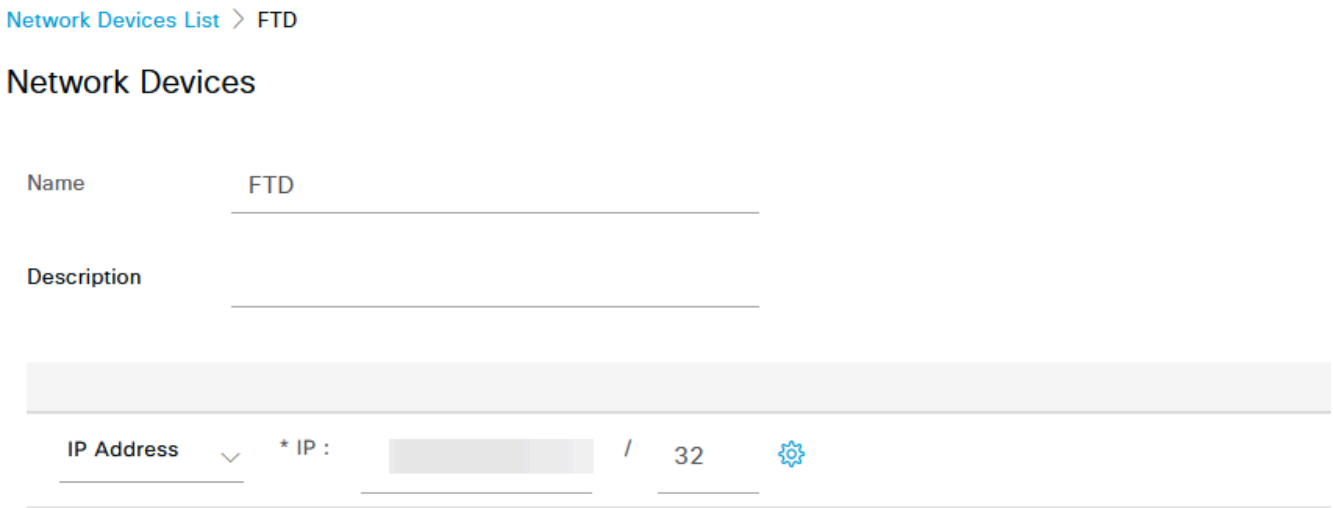
a. Faça login no servidor ISE e navegue até **Administration** > **Network Resources** > **Network Devices**.

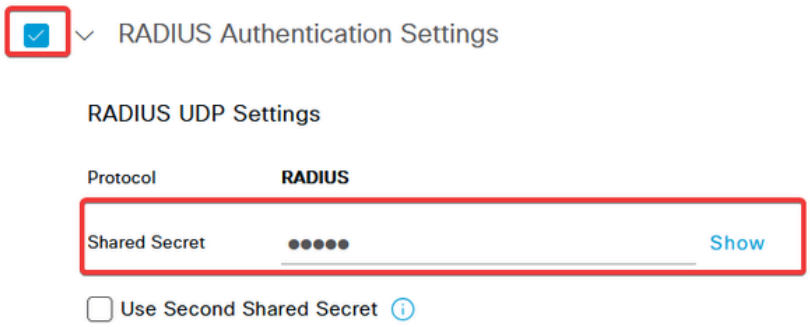


b. Clique **Add** para configurar o Firewall como um cliente AAA.

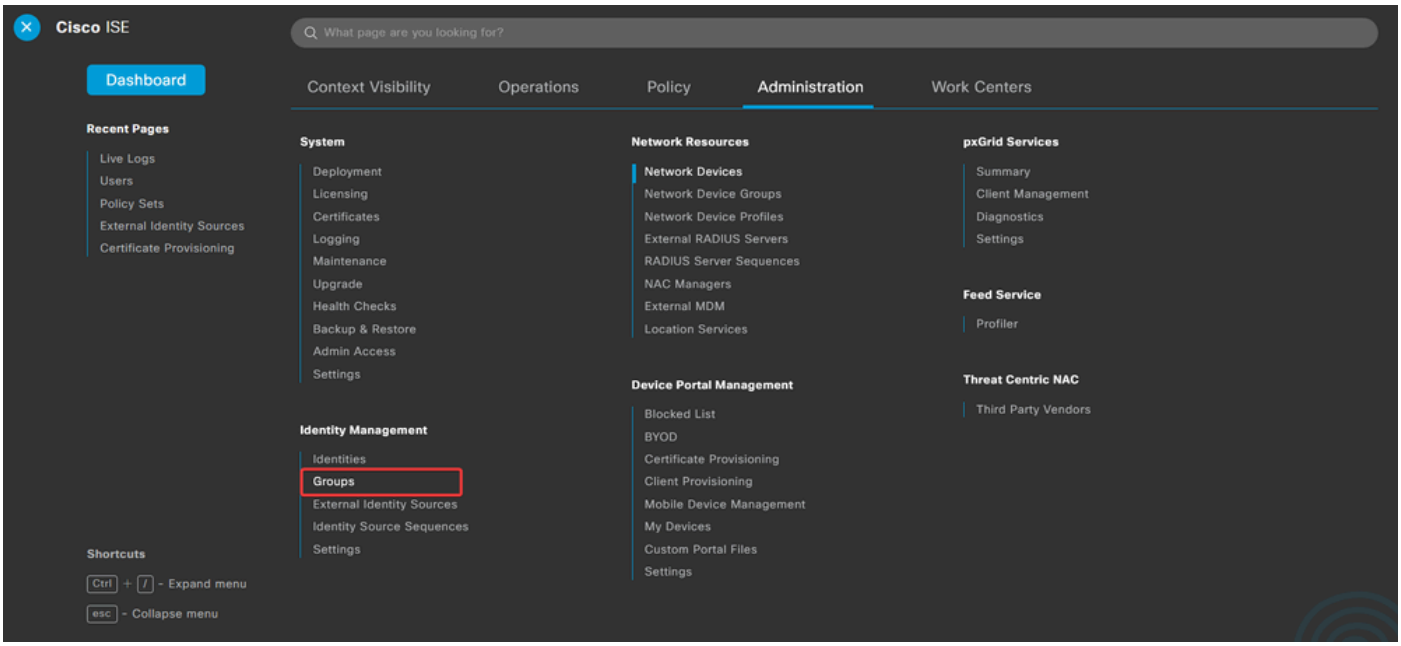


c. Insira os campos Network device Name e IP Address e marque **RADIUS Authentication Settings** a caixa de seleção e adicione **Shared Secret**. This value deve ser o mesmo que foi usado quando o objeto RADIUS Server no FMC foi criado. Clique em .Save



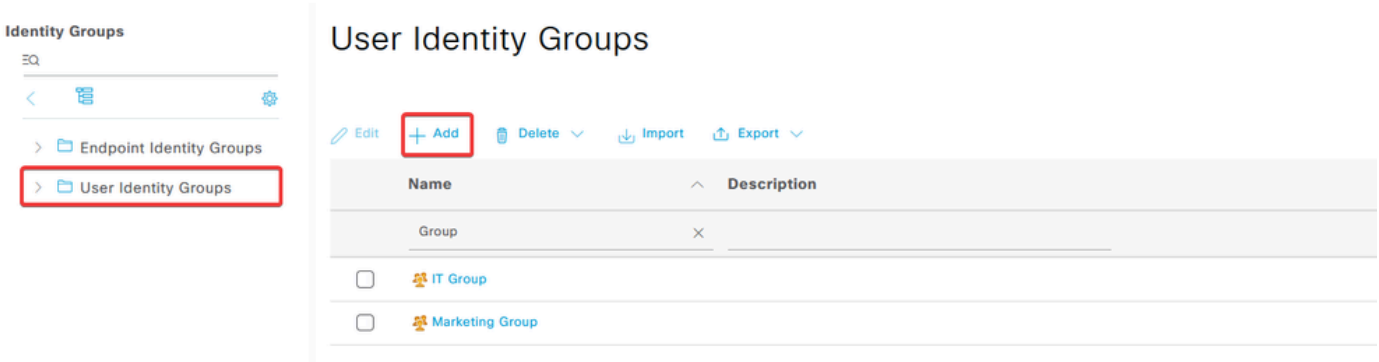


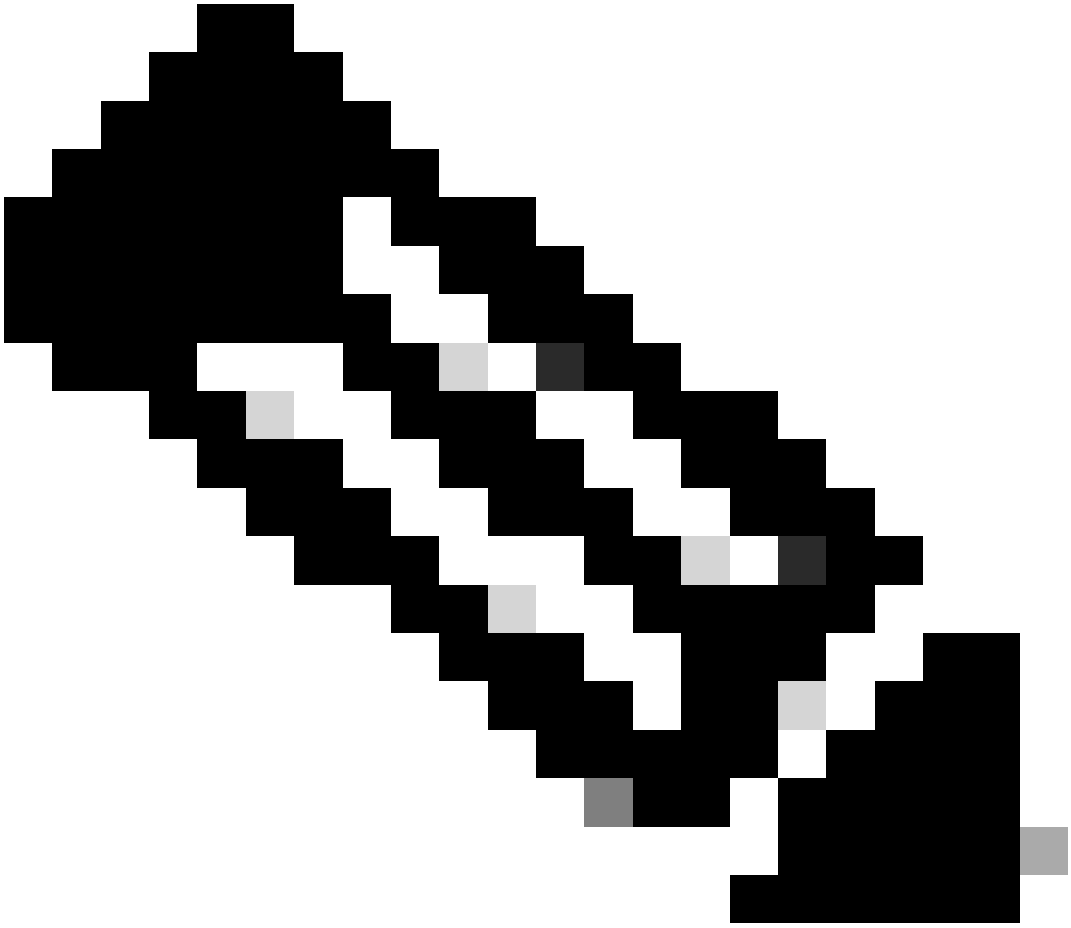
d. Navegue atéAdministration > Identity Management > Groups.



e. Clique emUser Identity Groupse em **Add**.

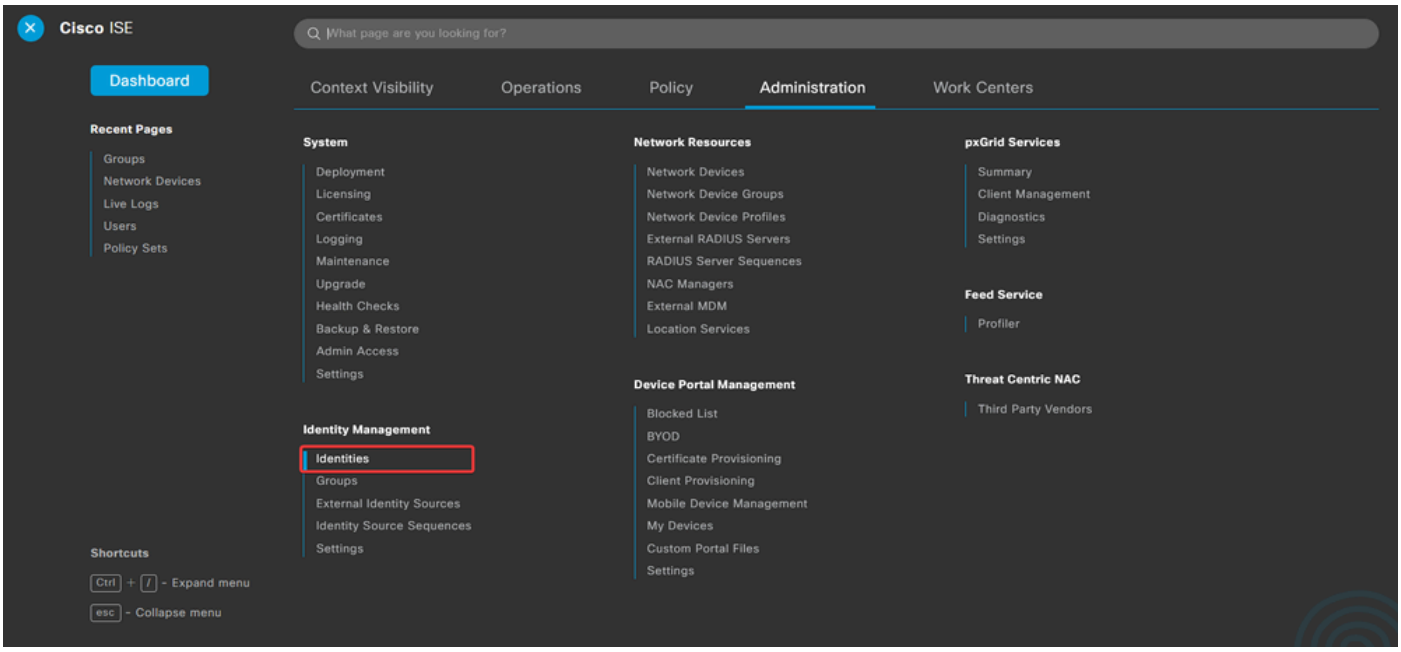
Insira o nome do grupoe clique emSubmit.





Observação: repita para criar quantos grupos forem necessários.

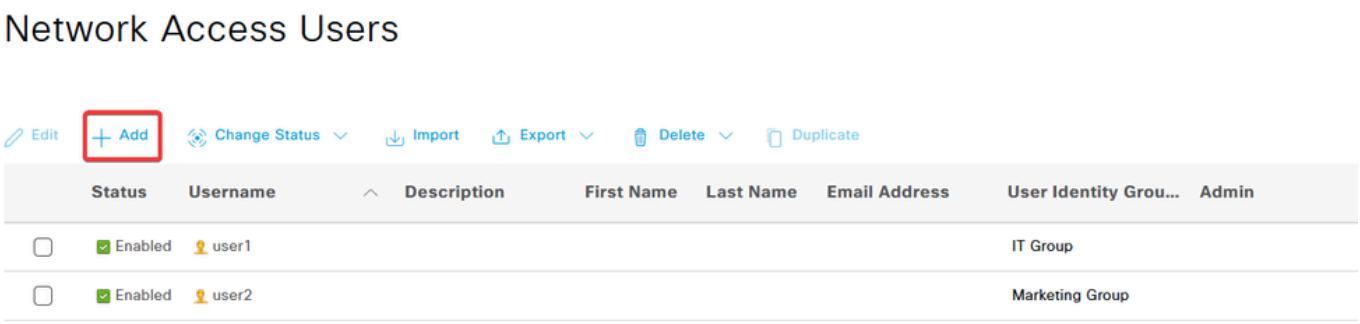
d. Navegue até **Administration > Identity Management > Identities.**

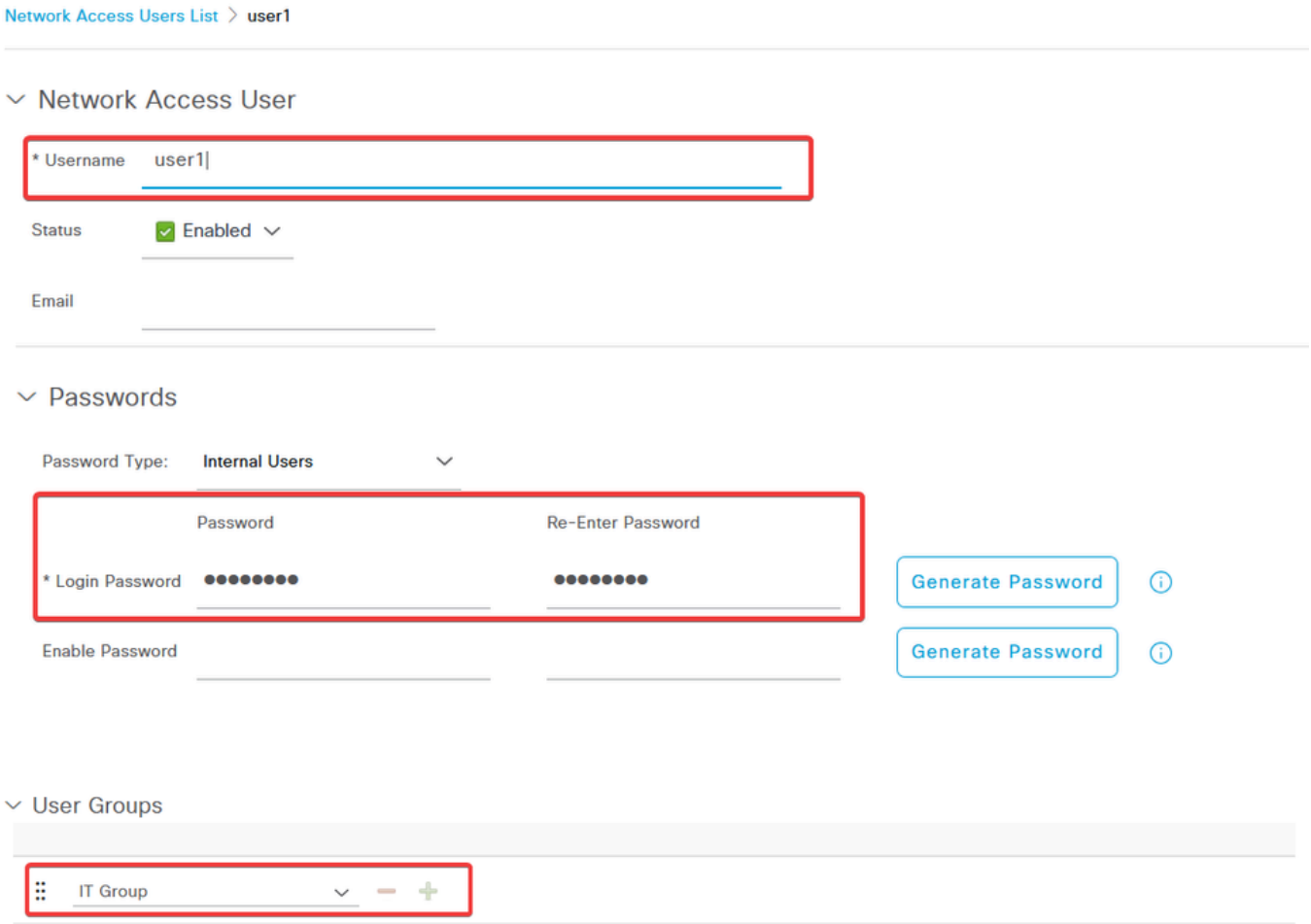


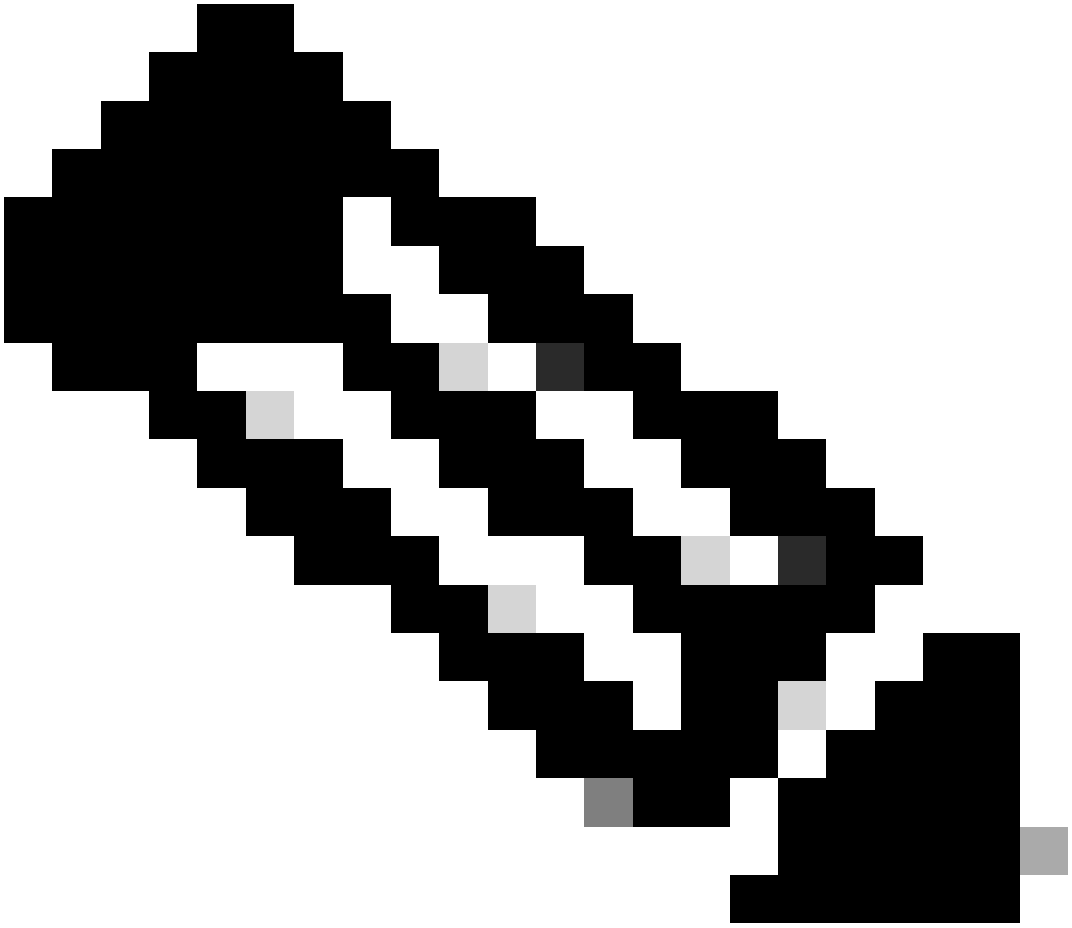
e. CliqueAddpara criar um novo usuário no banco de dados local do servidor.

Insira oUsernamee **Login Password**. Em seguida, navegue até o final desta página e selecione oUser Group.

Clique em .**Save**

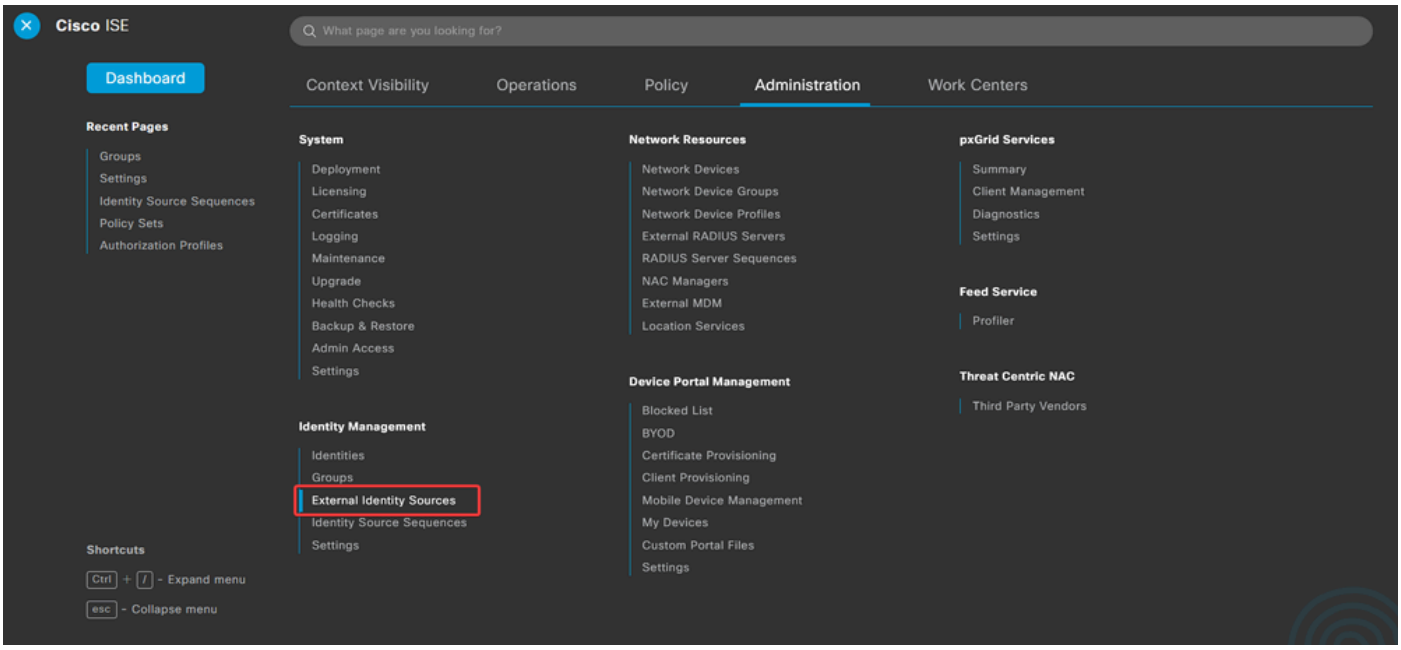



Network Access Users List
user1
Network Access User
* Username
user1
Status
Enabled
Email
Passwords
Password Type:
Internal Users
Password
Re-Enter Password
* Login Password
Generate Password
Enable Password
Generate Password
User Groups
IT Group



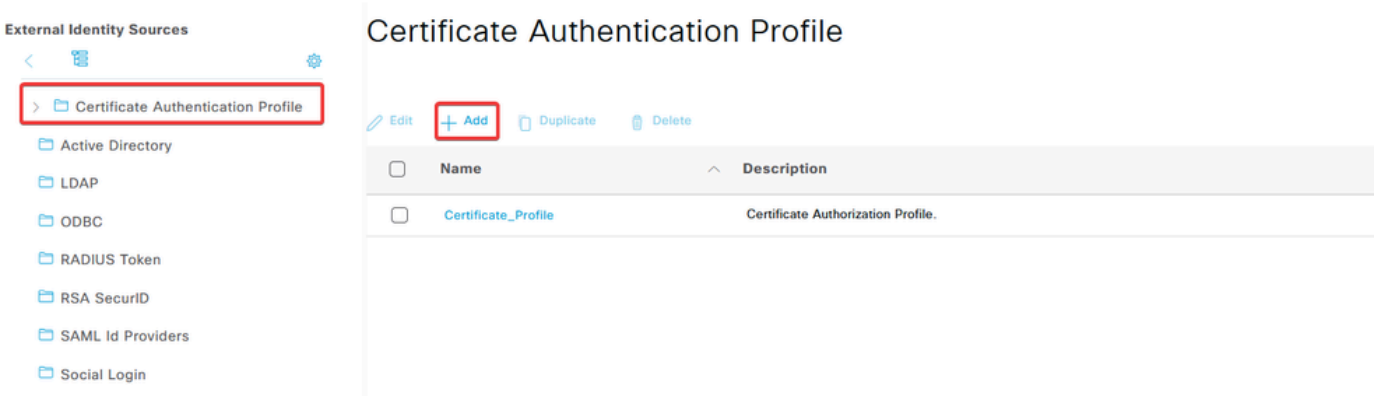
Observação: é necessário configurar um nome de usuário e uma senha para criar usuários internos. Mesmo que não seja necessário para a autenticação RAVPN, que é executada usando certificados, esses usuários podem ser usados para outros serviços internos que exigem uma senha. Portanto, certifique-se de usar uma senha forte.

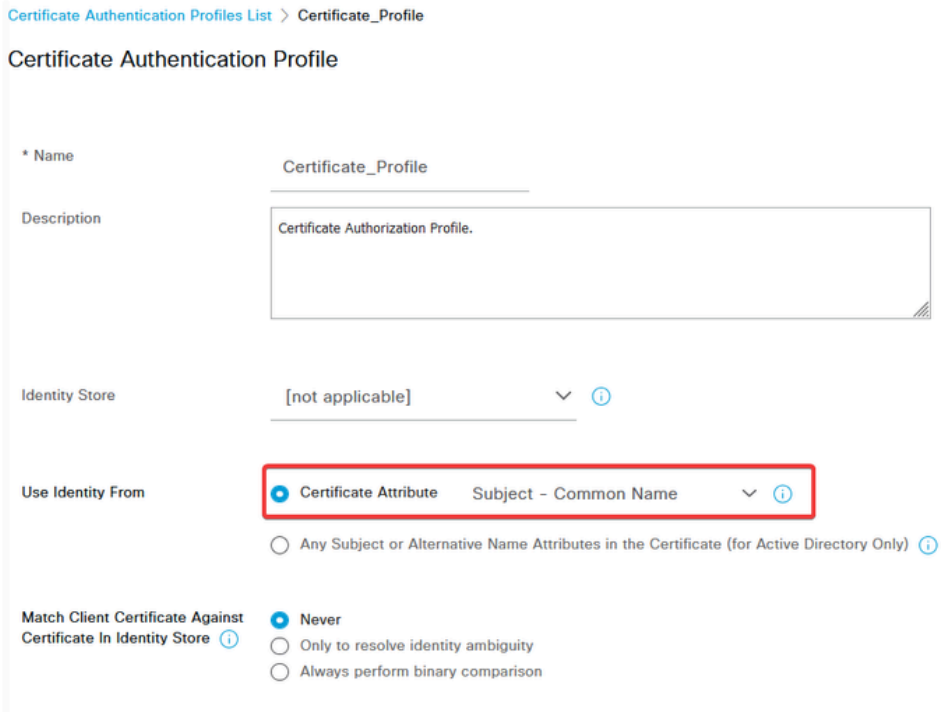
f. Navegue até **Administration > Identity Management > External Identify Sources.**



g. CliqueAddpara criar um **Certificate Authentication Profile.**

O perfil de autenticação de certificado especifica como os certificados de cliente são validados, incluindo quais campos no certificado podem ser verificados (nome alternativo do assunto, nome comum, etc.).

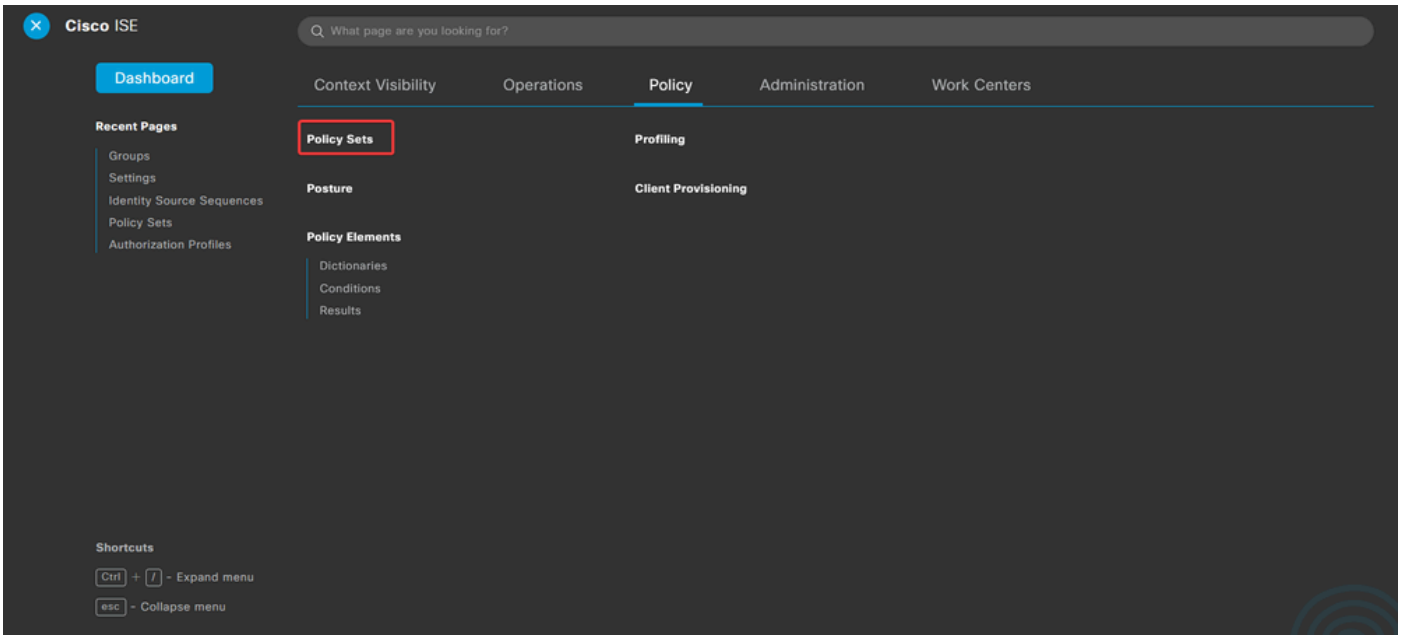




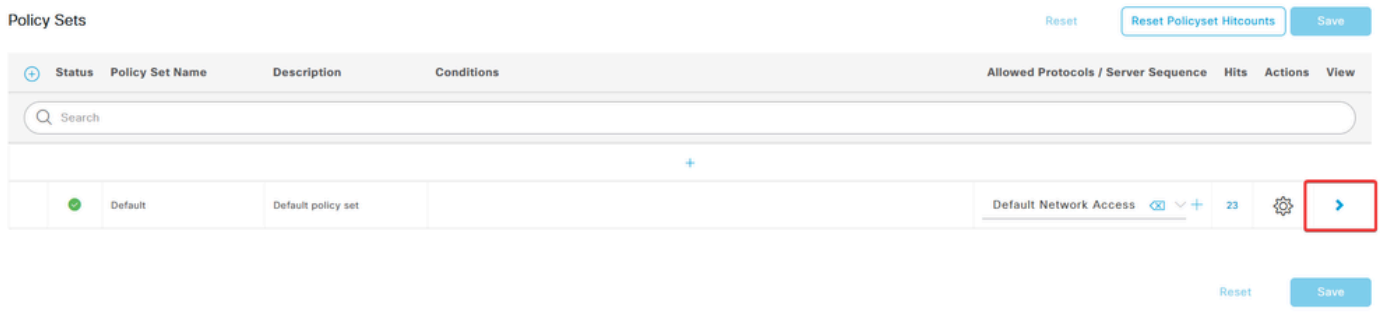
Etapa 3.2: Configurar a política de autenticação

A política de autenticação é usada para autenticar se a solicitação foi originada no firewall e no Perfil de Conexão específico.

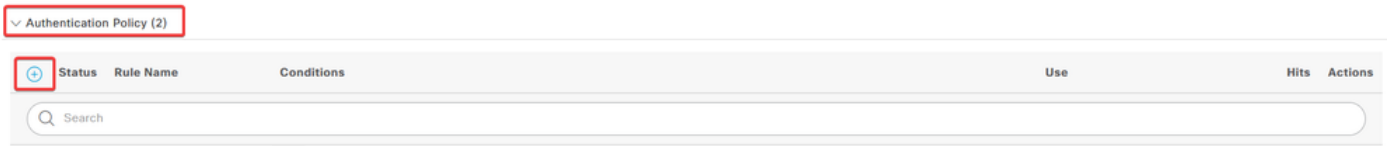
a. Navegue até **Policy** > **Policy Sets**.



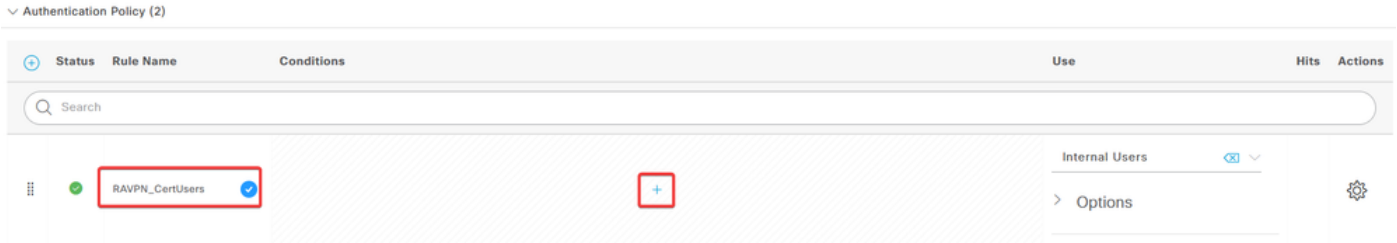
Selecione a política de autorização padrão clicando na seta no lado direito da tela:



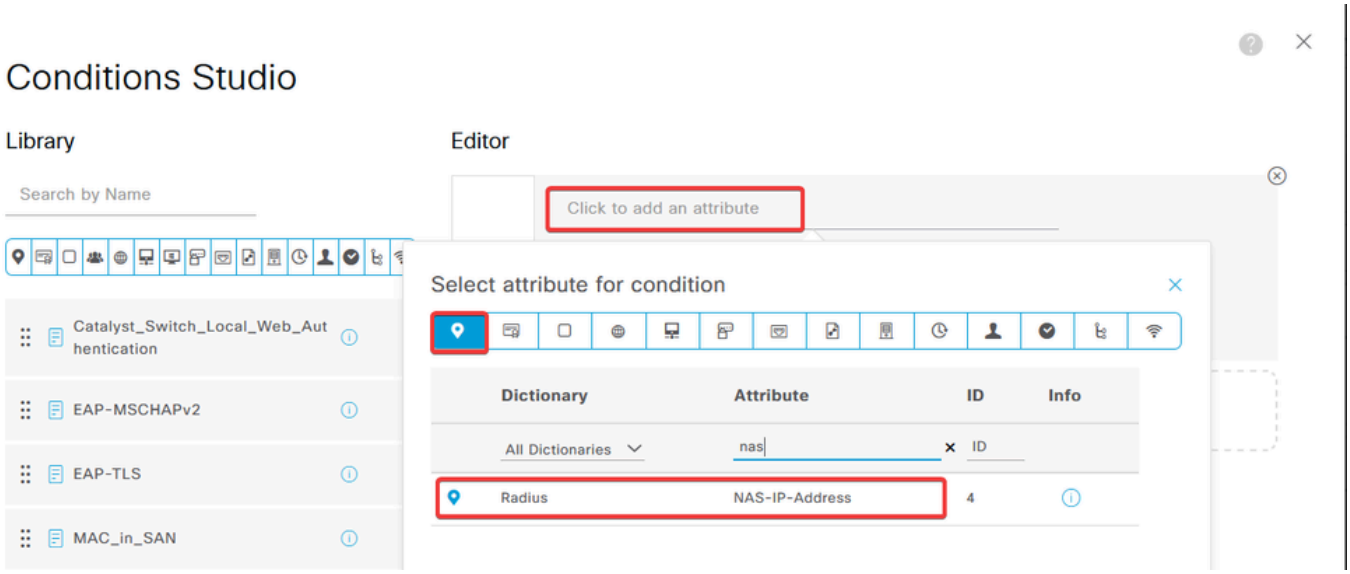
b. Clique na seta do menu suspenso ao lado de Authentication Policy para expandi-lo. Em seguida, clique no ícone **add (+)** para adicionar uma nova regra.



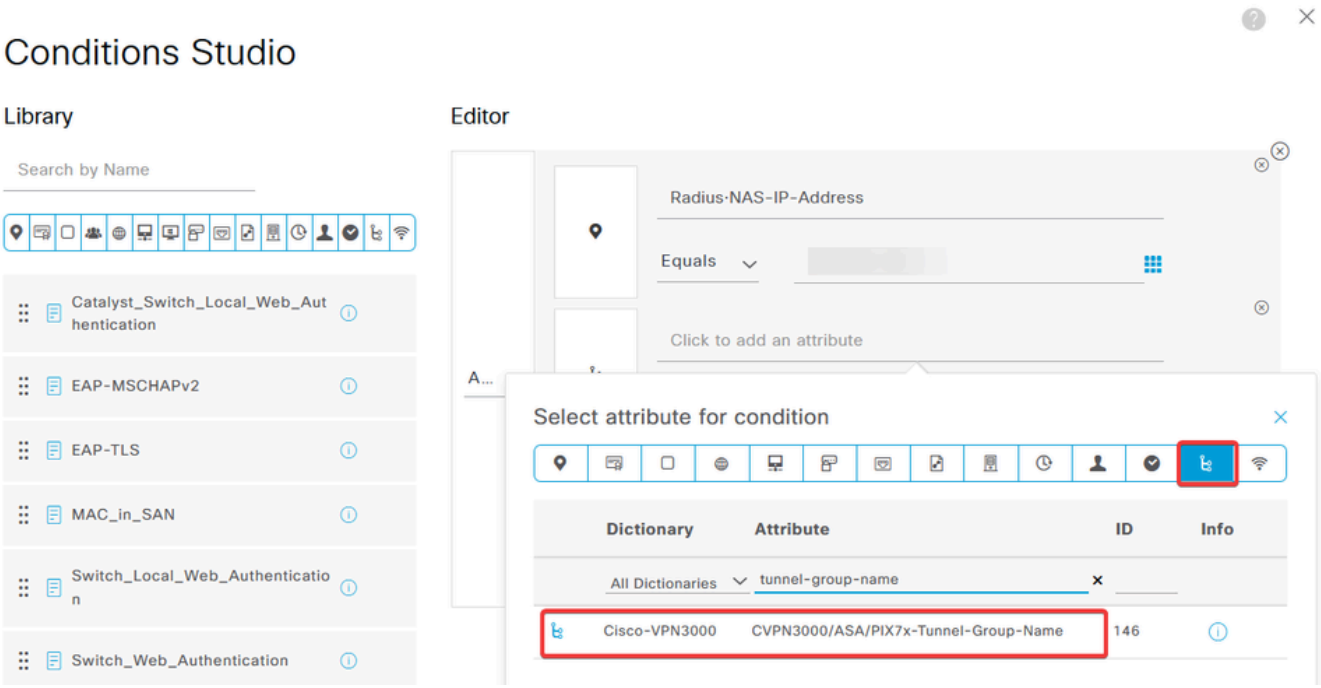
Insira o nome da regra e selecione o ícone add (+) na coluna Condições.

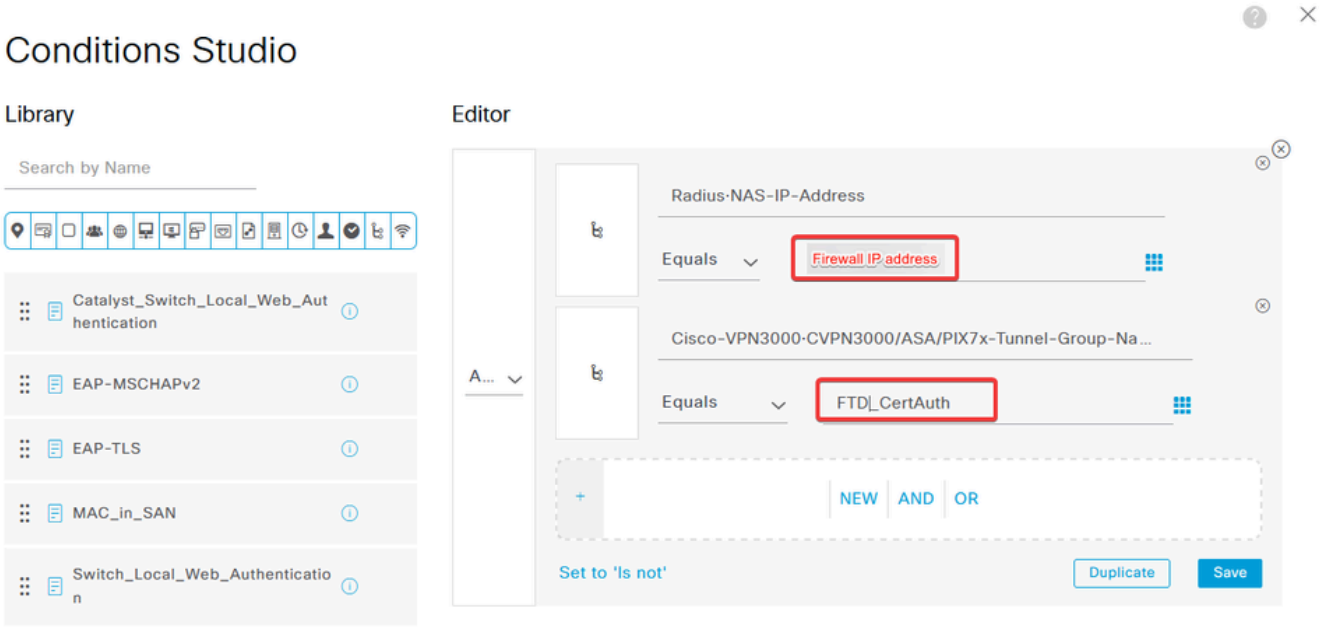


c. Clique na caixa de texto Editor de atributos e clique no NAS-IP-Address ícone. Insira o endereço IP do firewall.

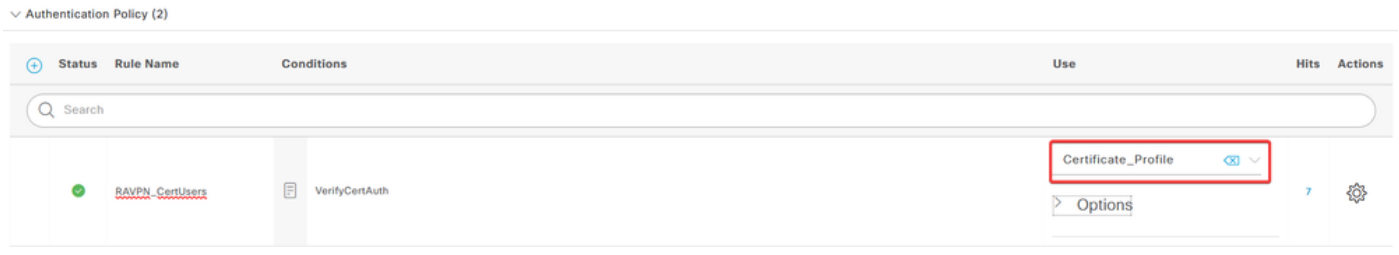


d. Clique em **New** e adicione o outro atributo Tunnel-Group-name. Insira o Connection Profile nome que foi configurado no FMC.





e. Na coluna Usar, selecione o **Certificate Authentication Profile** que foi criado. Ao fazer isso, ele especifica as informações definidas no perfil que são usadas para identificar os usuários.

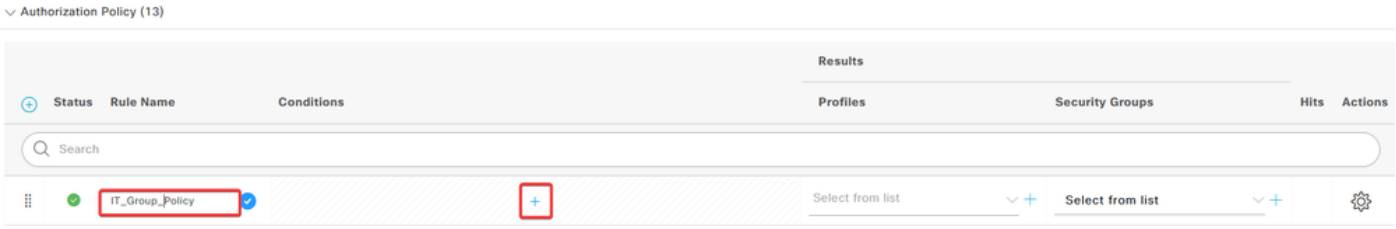


Clique em .Save

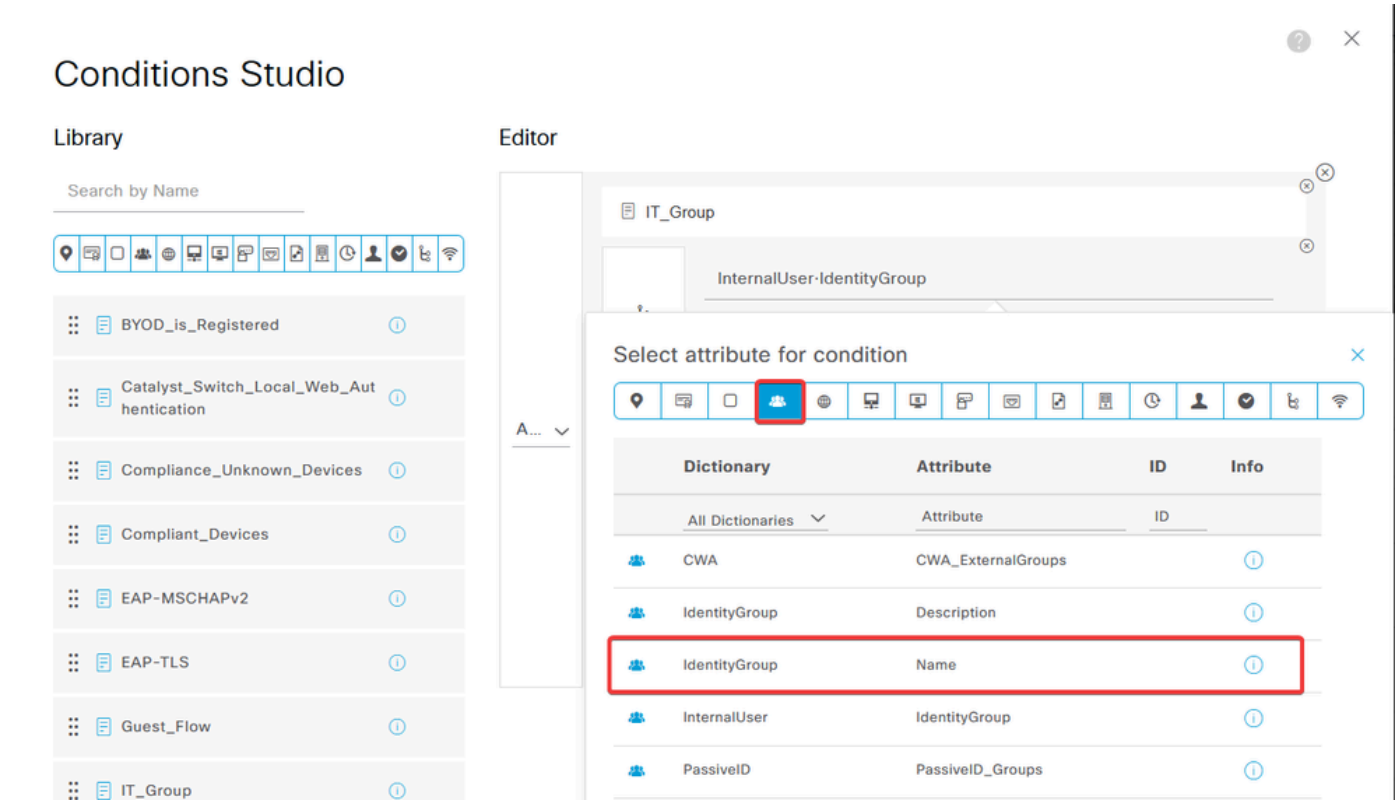
Etapa 3.3: Configurar a política de autorização

a. Clique na seta do menu suspenso ao lado deAuthorization Policypara expandi-lo. Em seguida, clique no ícone para adicionar uma nova regra**add (+)**.

Insira o nome da regra e selecione o ícone **add (+)** na coluna Condições.

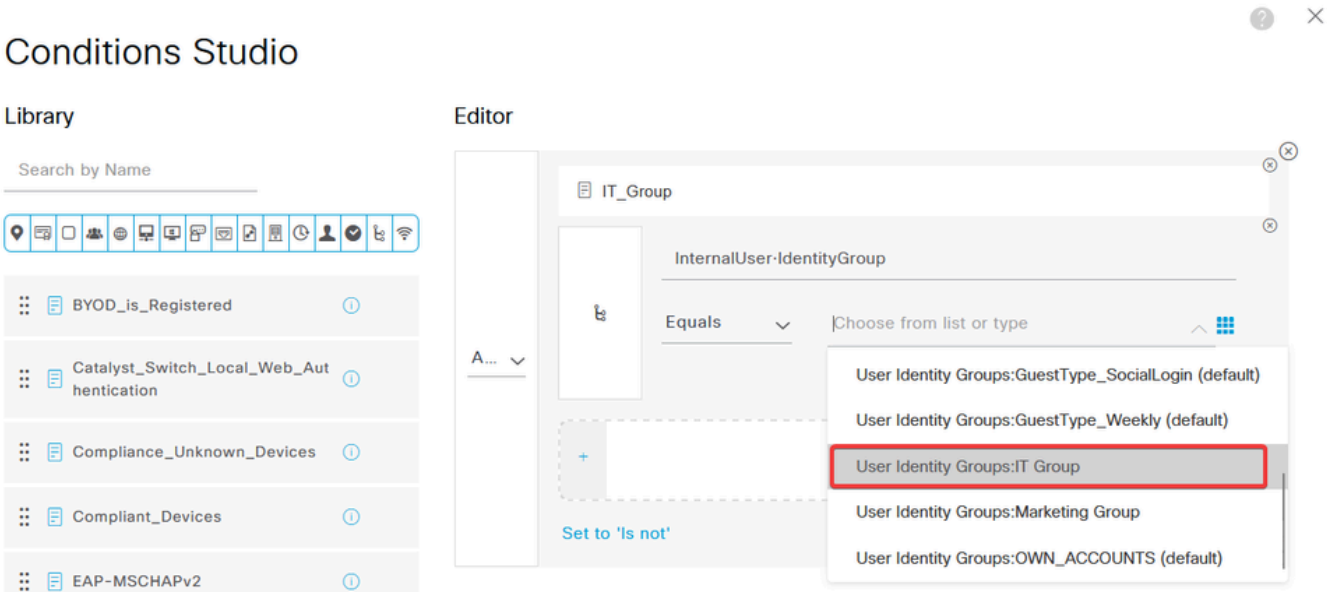


b. Clique na caixa de texto Editor de atributos e clique no ícone Identity group. Selecione o **Identity group - Name** atributo.

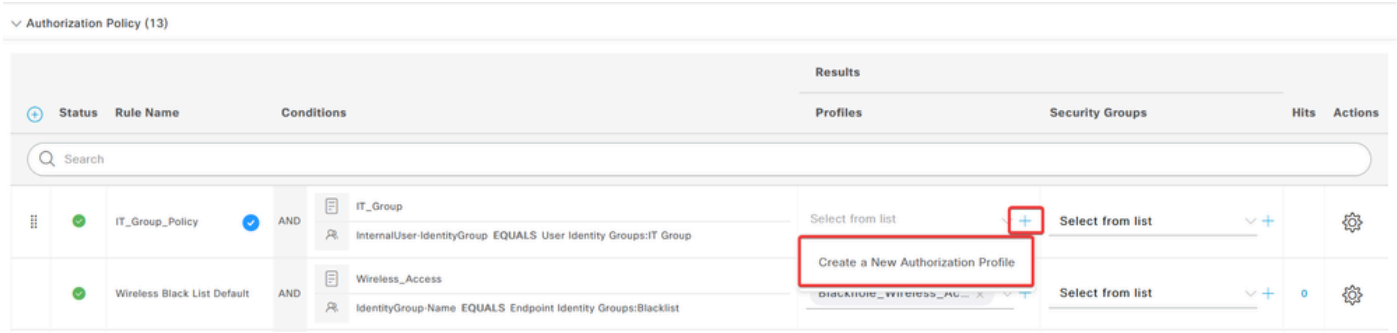


SelecioneEqualscomo o operador e clique na seta do menu suspenso para mostrar as opções disponíveis e selecione **User Identity Groups:**

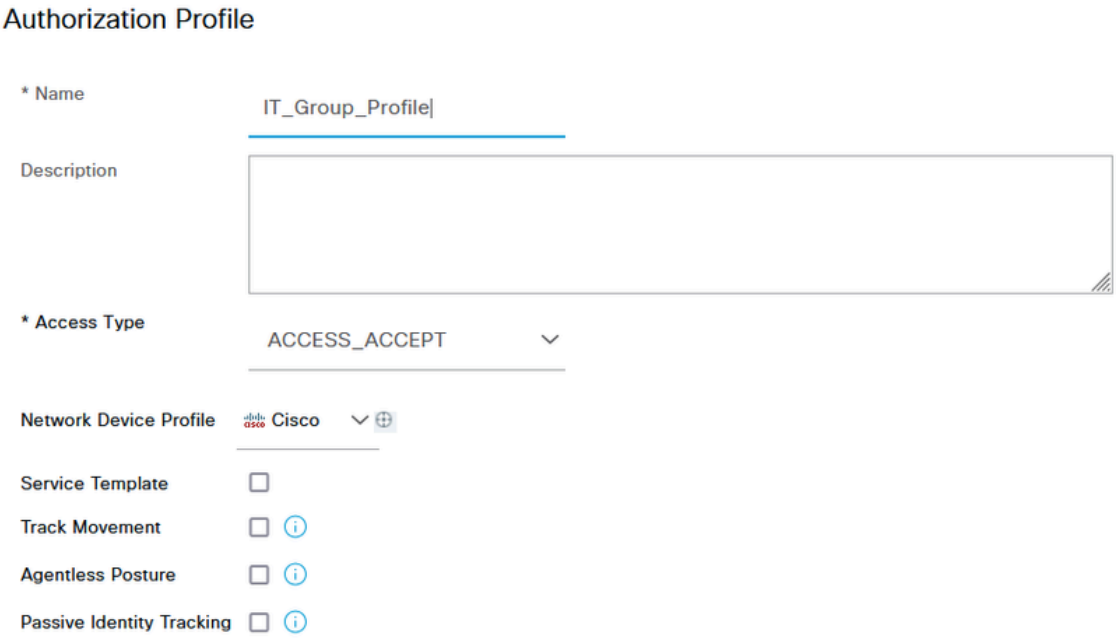
.



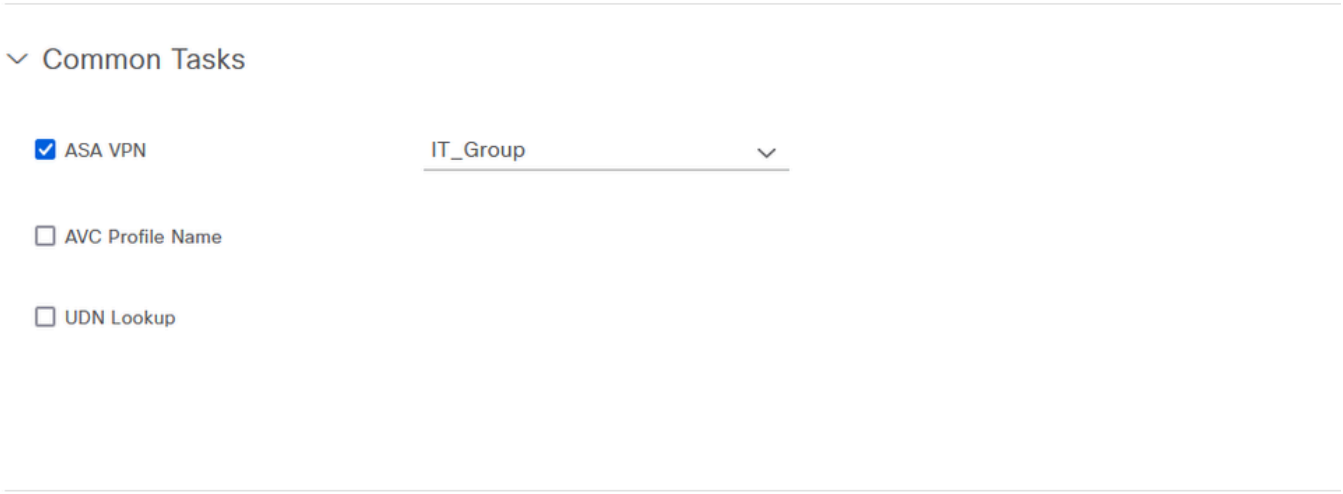
c. Na coluna Profiles, clique noadd (+)ícone e escolha **Create a New Authorization Profile.**



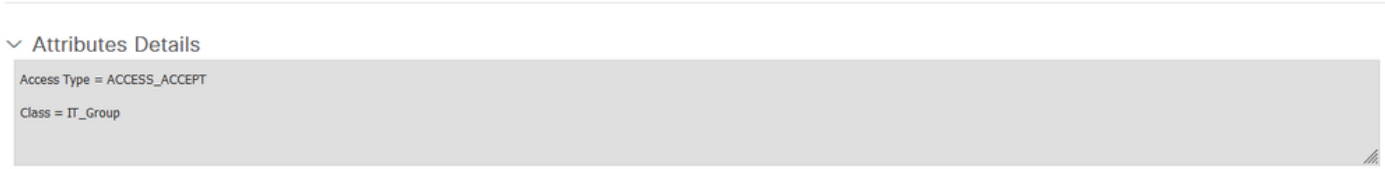
Digite o perfil**Name.**



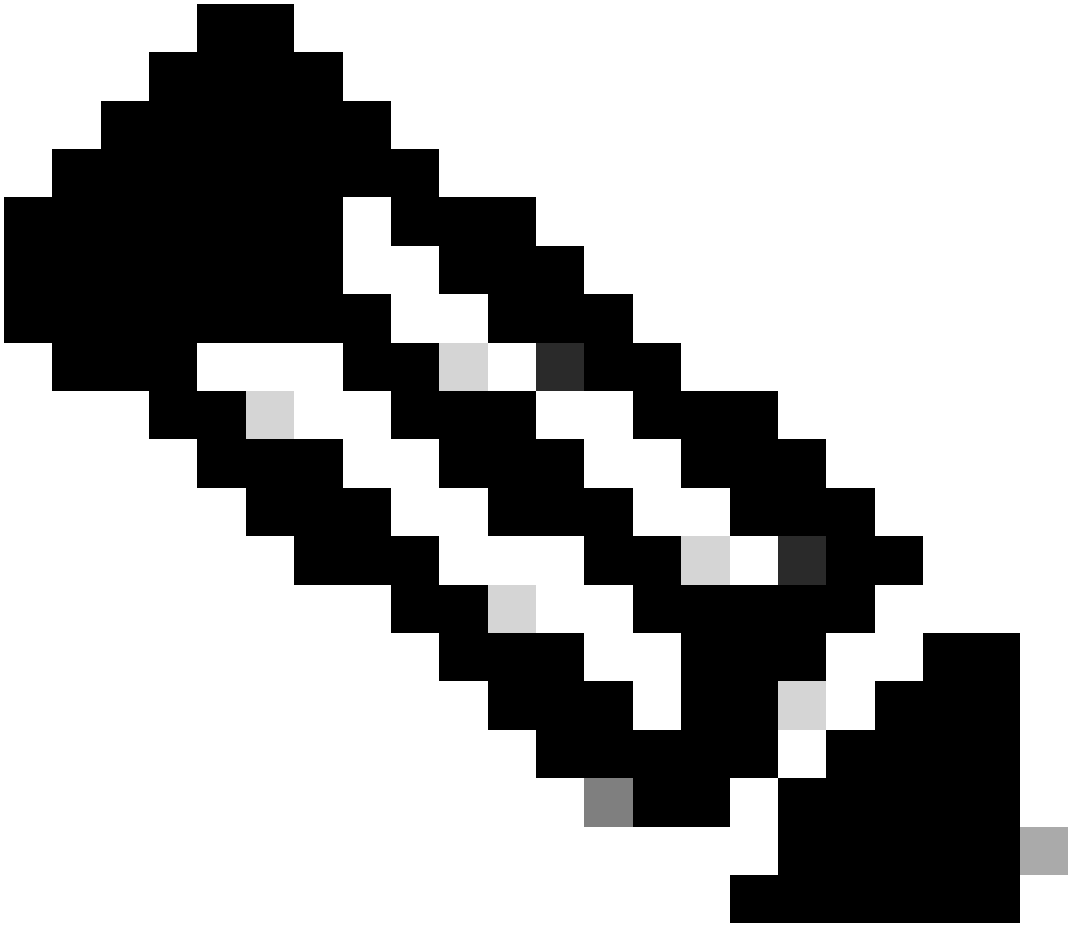
Navegue até **Common Tasks** e marque **ASA VPN**. Em seguida, digite o **group policy name**, que precisa ser o mesmo que o criado no FMC.



Os atributos que vêm em seguida foram atribuídos a cada grupo:



Click Save.



Observação: repita a Etapa 3.3: Configure a política de autorização para cada grupo criado.

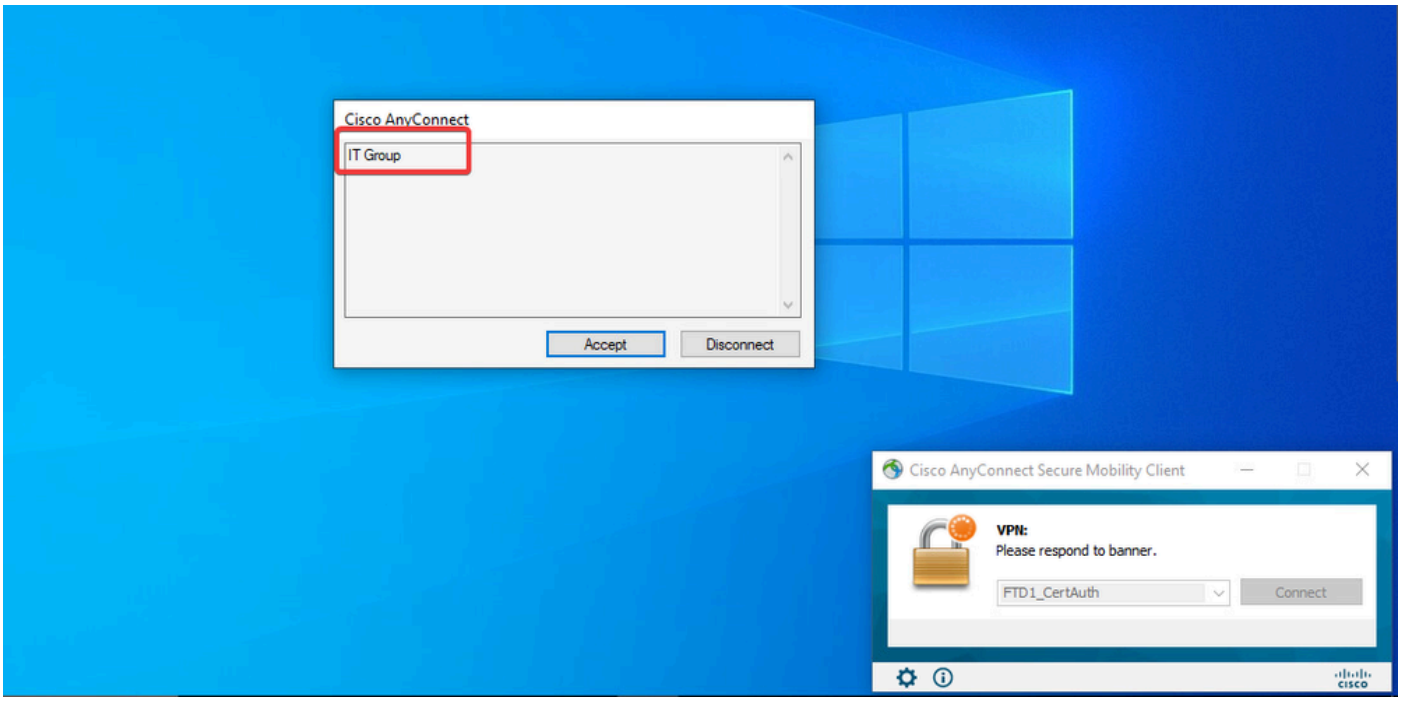
Verificar

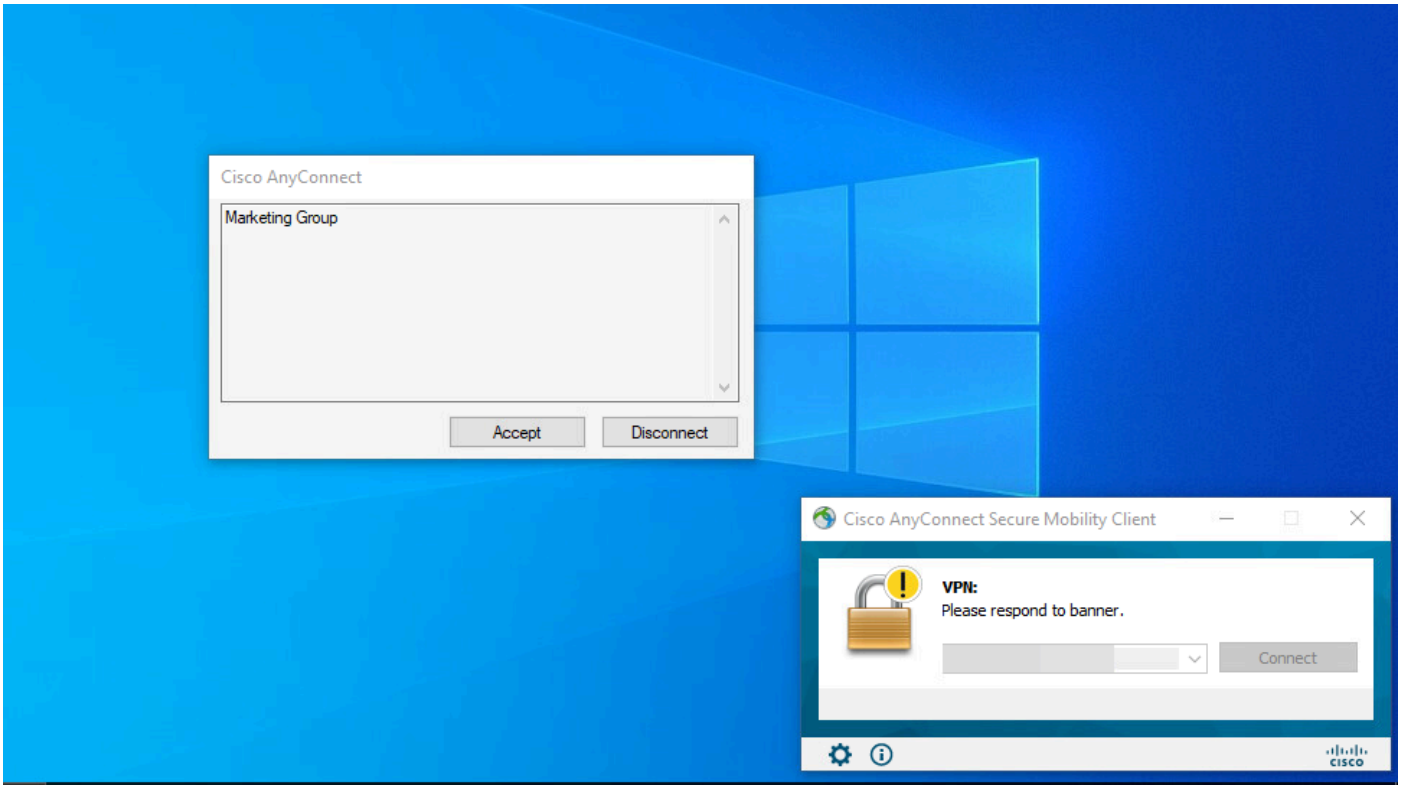
1. Execute o comando`show vpn-sessiondb anyconnect`e verifique se o usuário está usando a política de grupo correta.

```
<#root>

firepower#

show vpn-sessiondb anyconnect


Session Type : AnyConnect

Username     : user1
```

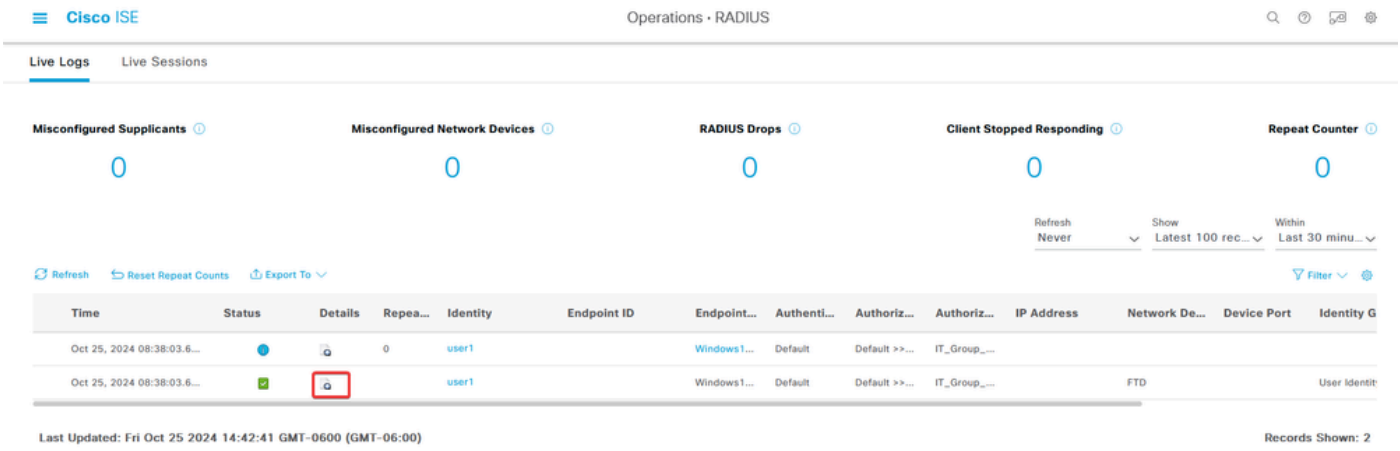
```
                Index        : 64
Assigned IP   : 192.168.55.2           Public IP    :
Protocol      : AnyConnect-Parent
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none
Hashing       : AnyConnect-Parent: (1)none
Bytes Tx      : 15084                   Bytes Rx     : 99611

Group Policy  : IT_Group                Tunnel Group : FTD_CertAuth


Login Time    : 22:21:43 UTC Tue Oct 22 2024
Duration      : 3h:03m:50s
Inactivity    : 0h:41m:44s
VLAN Mapping  : N/A                     VLAN         : none
Audt Sess ID  : 96130a0f0004000067182577
Security Grp  : none                    Tunnel Zone  : 0


Username      : User2

                  Index        : 70
Assigned IP   : 192.168.55.3           Public IP    :
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 15112                   Bytes Rx     : 19738

Group Policy  : Marketing_Group         Tunnel Group : FTD_CertAuth


Login Time    : 01:23:08 UTC Wed Oct 23 2024
Duration      : 0h:02m:25s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                     VLAN         : none
Audt Sess ID  : 96130a0f0004600067184ffc
Security Grp  : none                    Tunnel Zone  : 0

firepower#
```

2. Na política de grupo, você pode configurar uma mensagem de banner que é exibida quando o usuário se conecta com êxito. Cada banner pode ser usado para identificar o grupo que tem autorização.





3. Em logs dinâmicos, verifique se a conexão está usando a política de autorização apropriada. Clique emDetailse mostre o Relatório de autenticação.



Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

1. As depurações podem ser executadas a partir da CLI de diagnóstico do CSF para Autenticação de Certificado.

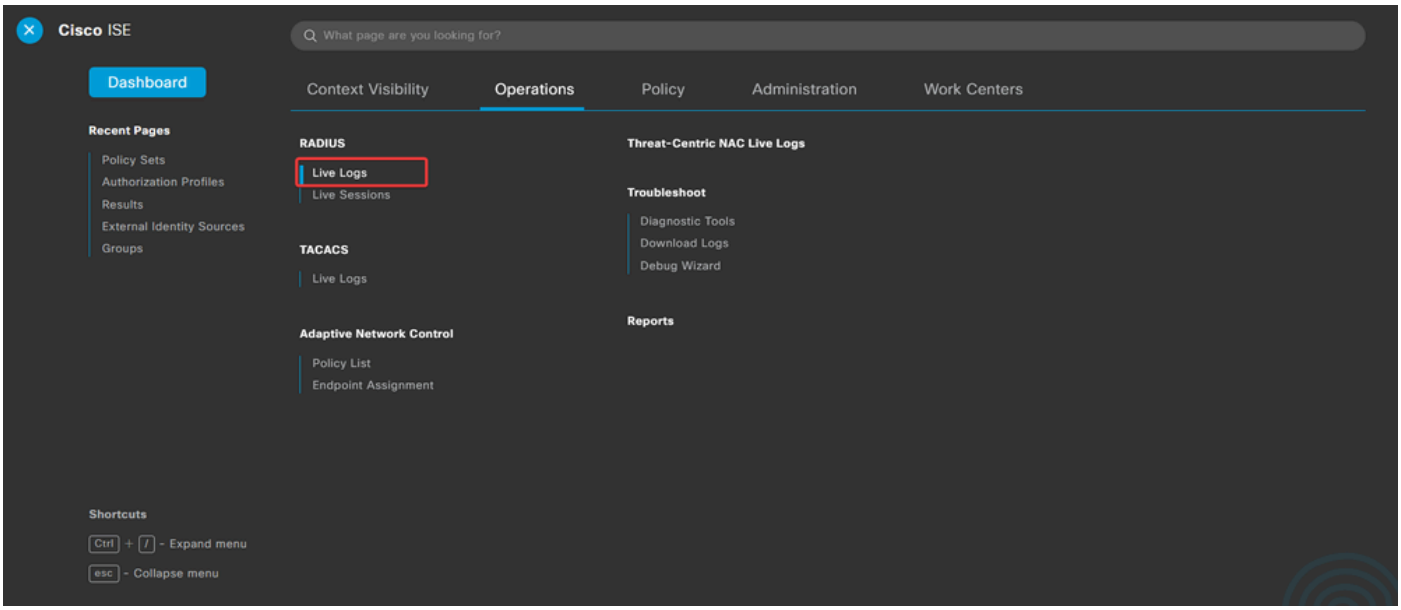
```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

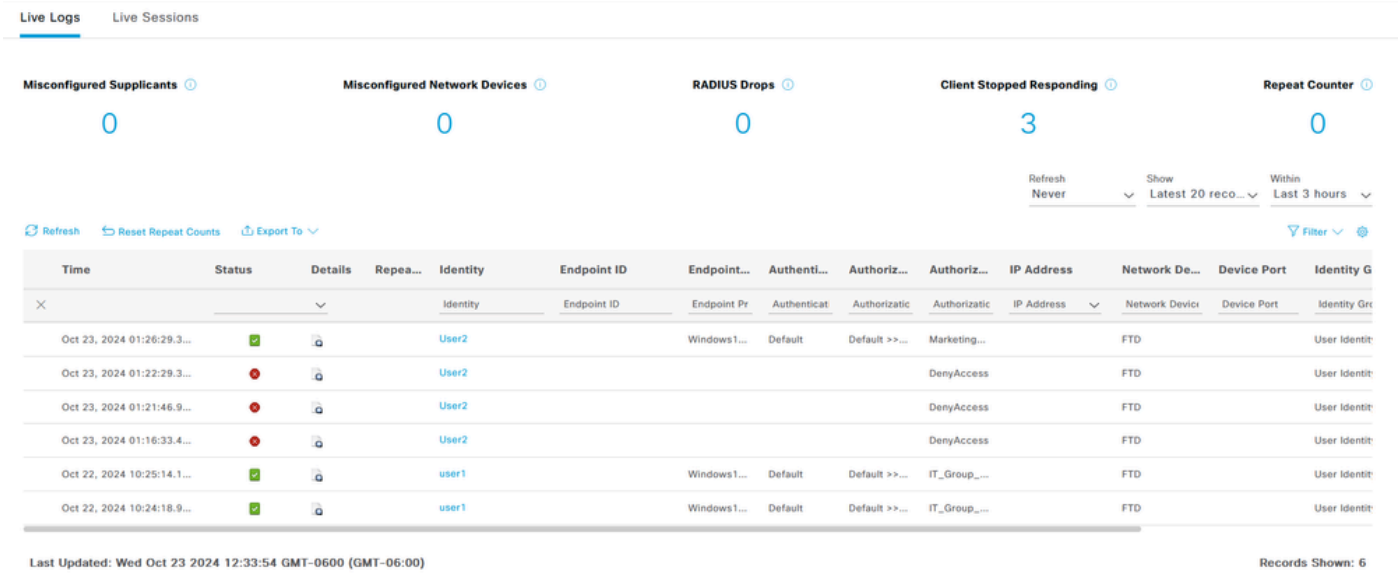
2. Use depurações AAA para verificar a atribuição de atributos locais e/ou remotos.

```
debug aaa common 255
debug aaa shim 255
debug aaa authentication
debug aaa authorization
debug radius all
```

No ISE:

1. Navegue atéOperations > RADIUS > Live Logs.


Cisco ISE
What page are you looking for?
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Recent Pages
Policy Sets
Authorization Profiles
Results
External Identity Sources
Groups
RADIUS
Live Logs
Live Sessions
TACACS
Live Logs
Adaptive Network Control
Policy List
Endpoint Assignment
Threat-Centric NAC Live Logs
Troubleshoot
Diagnostic Tools
Download Logs
Debug Wizard
Reports
Shortcuts
Ctrl + / - Expand menu
esc - Collapse menu


Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
3
Repeat Counter
0
Refresh
Never
Show
Latest 20 reco...
Within
Last 3 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authenti...
Authoriz...
Authoriz...
IP Address
Network De...
Device Port
Identity G
Oct 23, 2024 01:26:29.3... User2 Windows1... Default Default >>... Marketing... FTD User Identit
Oct 23, 2024 01:22:29.3... User2 DenyAccess FTD User Identit
Oct 23, 2024 01:21:46.9... User2 DenyAccess FTD User Identit
Oct 23, 2024 01:16:33.4... User2 DenyAccess FTD User Identit
Oct 22, 2024 10:25:14.1... user1 Windows1... Default Default >>... IT_Group_... FTD User Identit
Oct 22, 2024 10:24:18.9... user1 Windows1... Default Default >>... IT_Group_... FTD User Identit
Last Updated: Wed Oct 23 2024 12:33:54 GMT-0600 (GMT-06:00)
Records Shown: 6

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.