Configurar o fluxo de autorização para sessões de ID passiva no ISE 3.2

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Configuração](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar regras de autorização para eventos de ID Passivo para atribuir SGTs às sessões.

Informações de Apoio

Os serviços de identidade passiva (ID passiva) não autenticam os usuários diretamente, mas coletam identidades de usuário e endereços IP de servidores de autenticação externos, como o Ative Diretory (AD), conhecidos como provedores, e compartilham essas informações com os assinantes.

O ISE 3.2 apresenta um novo recurso que permite configurar uma política de autorização para atribuir uma SGT (Security Group Tag, tag de grupo de segurança) a um usuário com base na associação de grupo do Ative Diretory.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ISE 3.X
- Integração de ID passiva com qualquer provedor
- Administração do Ative Diretory (AD)
- Segmentação (Trustsec)
- PxGrid (grade de intercâmbio de plataforma)

Componentes Utilizados

- Software Identity Service Engine (ISE) versão 3.2
- Microsoft Ative Diretory
- Syslogs

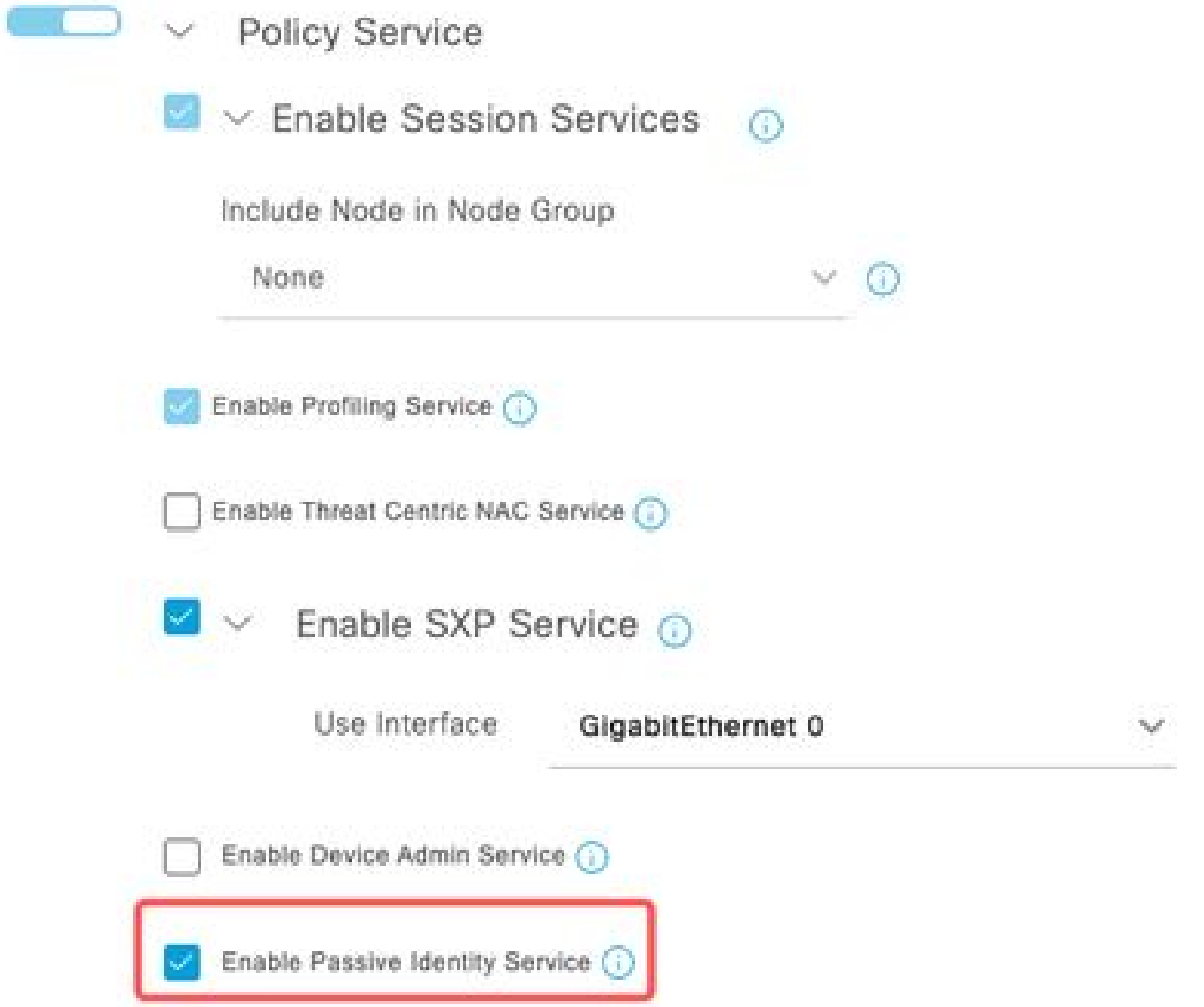
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configuração

Etapa 1. Ative os serviços do ISE.

1. No ISE, navegue até Administração > Implantação, escolha o nó do ISE e clique em Editar, habilitar Serviço de política e escolha Habilitar serviço de identidade passiva. Opcional, você pode habilitar o SXP e o PxGrid se as sessões de id passiva precisarem ser publicadas por meio de cada uma. Click Save.

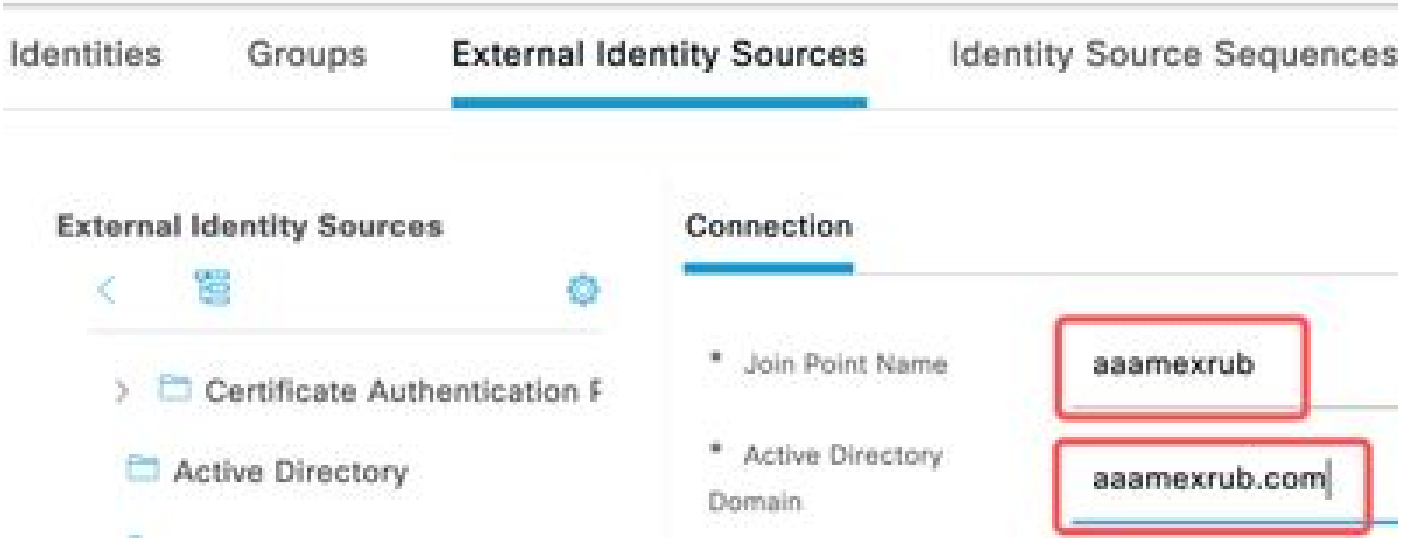
Aviso: os detalhes SGT dos usuários de login PassiveID autenticados pelo provedor de API não podem ser publicados no SXP. No entanto, os detalhes do SGT desses usuários podem ser publicados por meio do pxGrid e do pxGrid Cloud.



Serviços habilitados

Etapa 2. Configure o Ative Diretory.

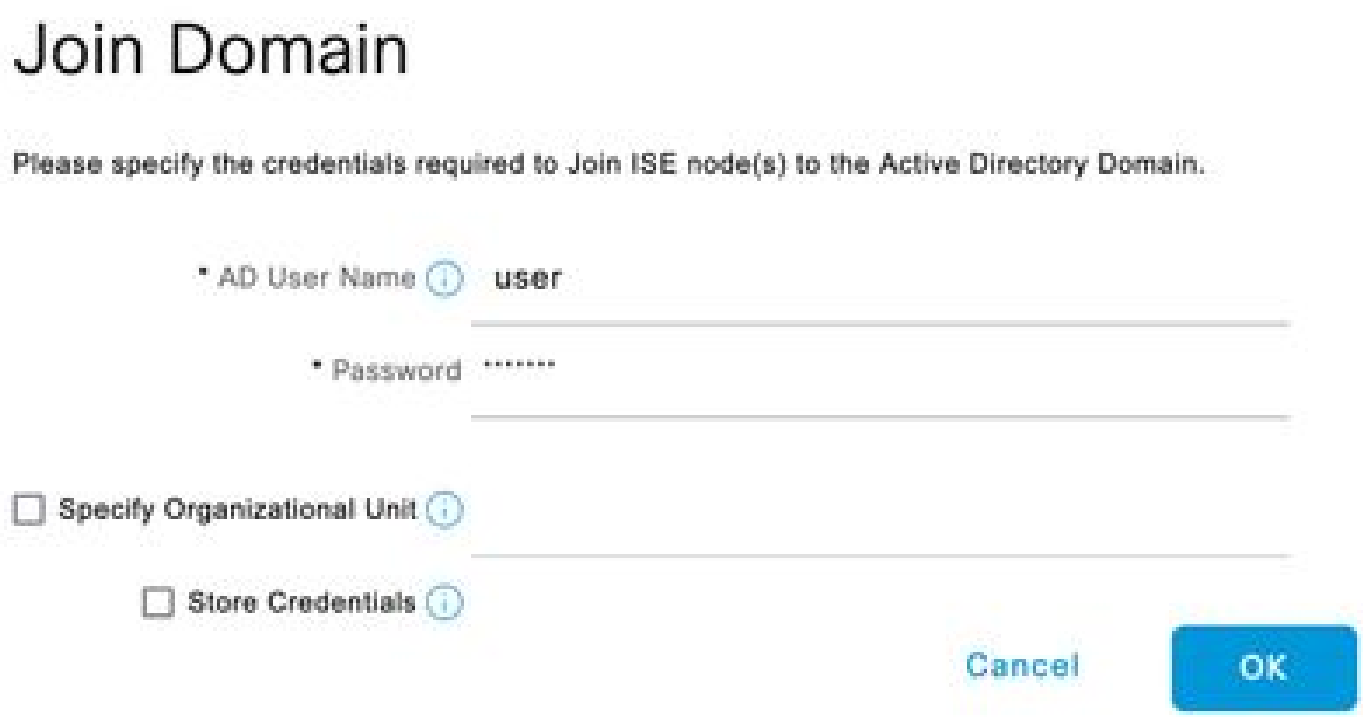
1. Navegue para Administração > Gerenciamento de identidades > Fontes de identidade externas e escolha Ative Diretory e clique no botão Adicionar.
2. Insira o Join Point Name e o Ative Diretory Domain. Clique em Submit.



Adicionar Ative Diretory

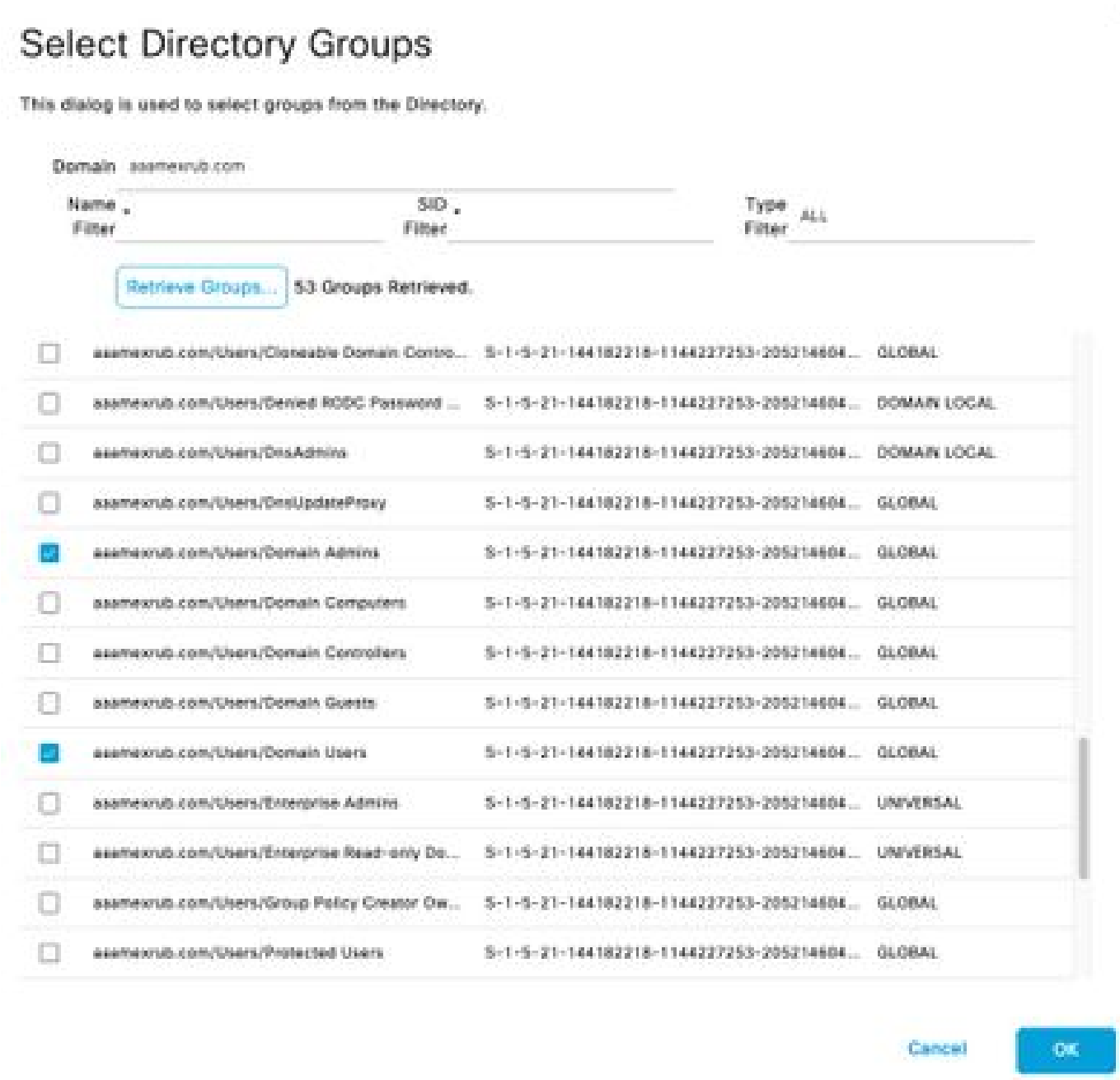
3. Uma janela pop-up aparece para que o ISE seja adicionado ao AD. Clique em Sim. Digite o nome de usuário e a senha. Click OK.

Continuar a ingressar no ISE

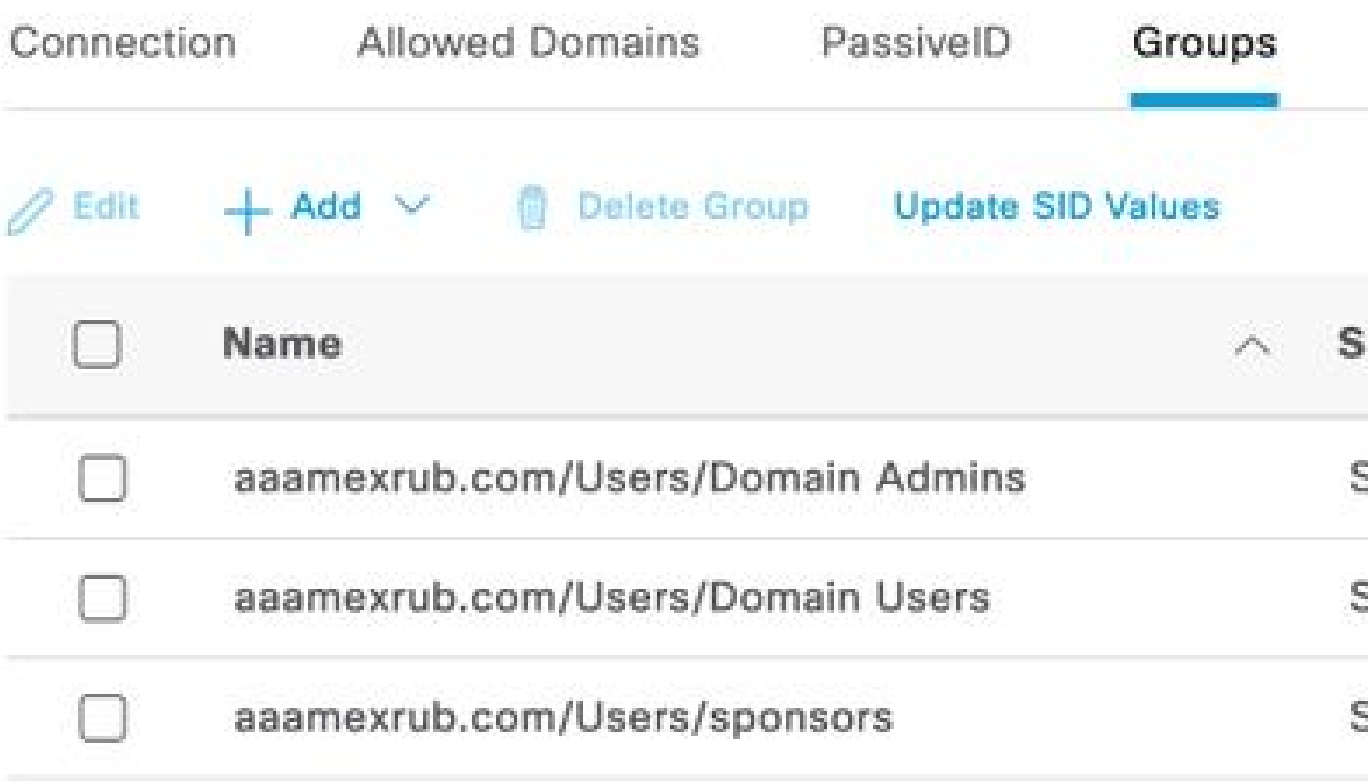


Ingressar no Ative Diretory

4. Recupere grupos do AD. Navegue até Grupos, clique em Adicionar, clique em Recuperar grupos, escolha todos os grupos interessados e clique em OK.

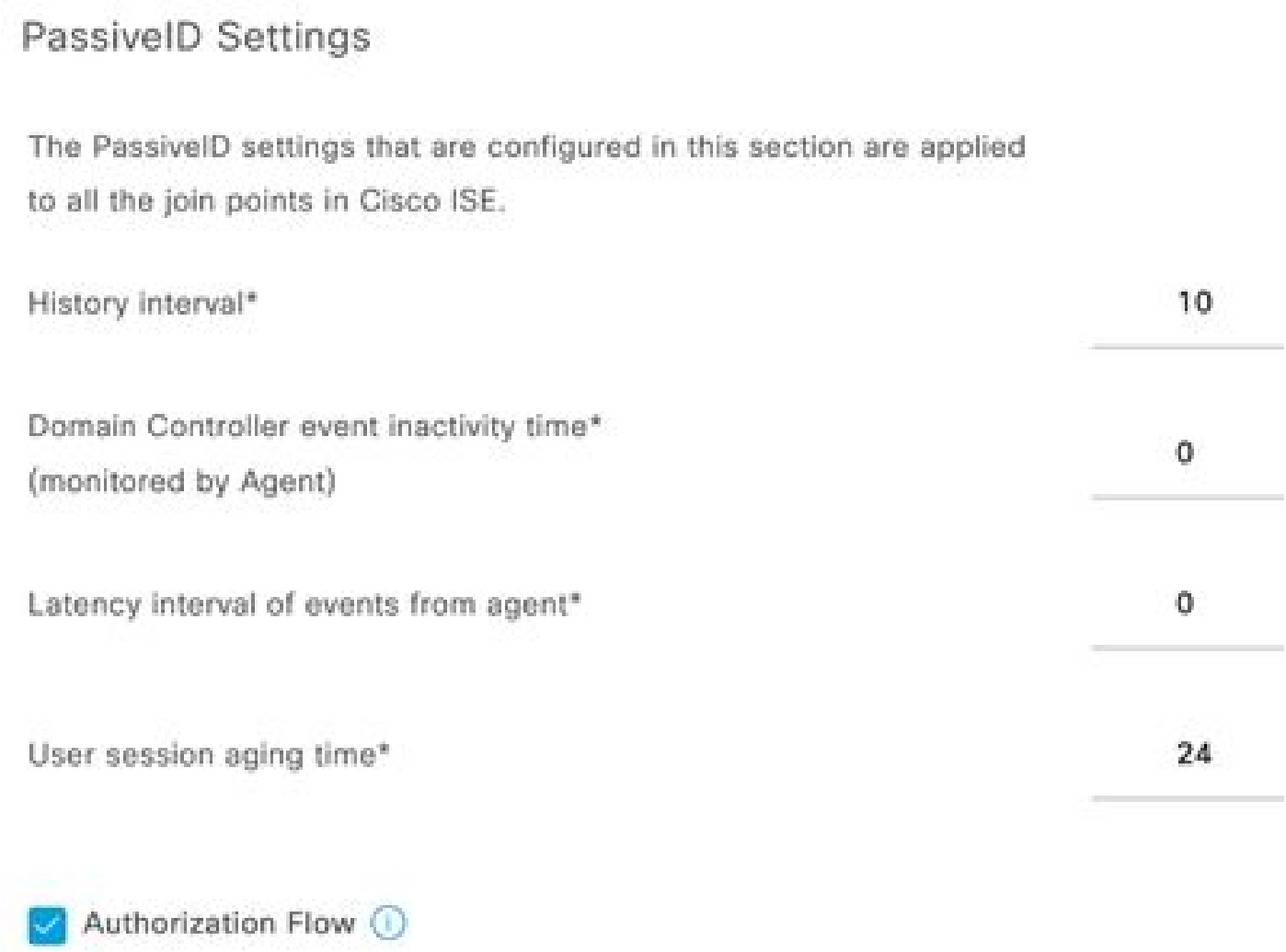


Recuperar grupos do AD



Grupos Recuperados

5. Ative o fluxo de Autorização. Navegue para Configurações avançadas e, na seção Configurações de ID passiva, marque a caixa de seleção Fluxo de autorização. Click Save.

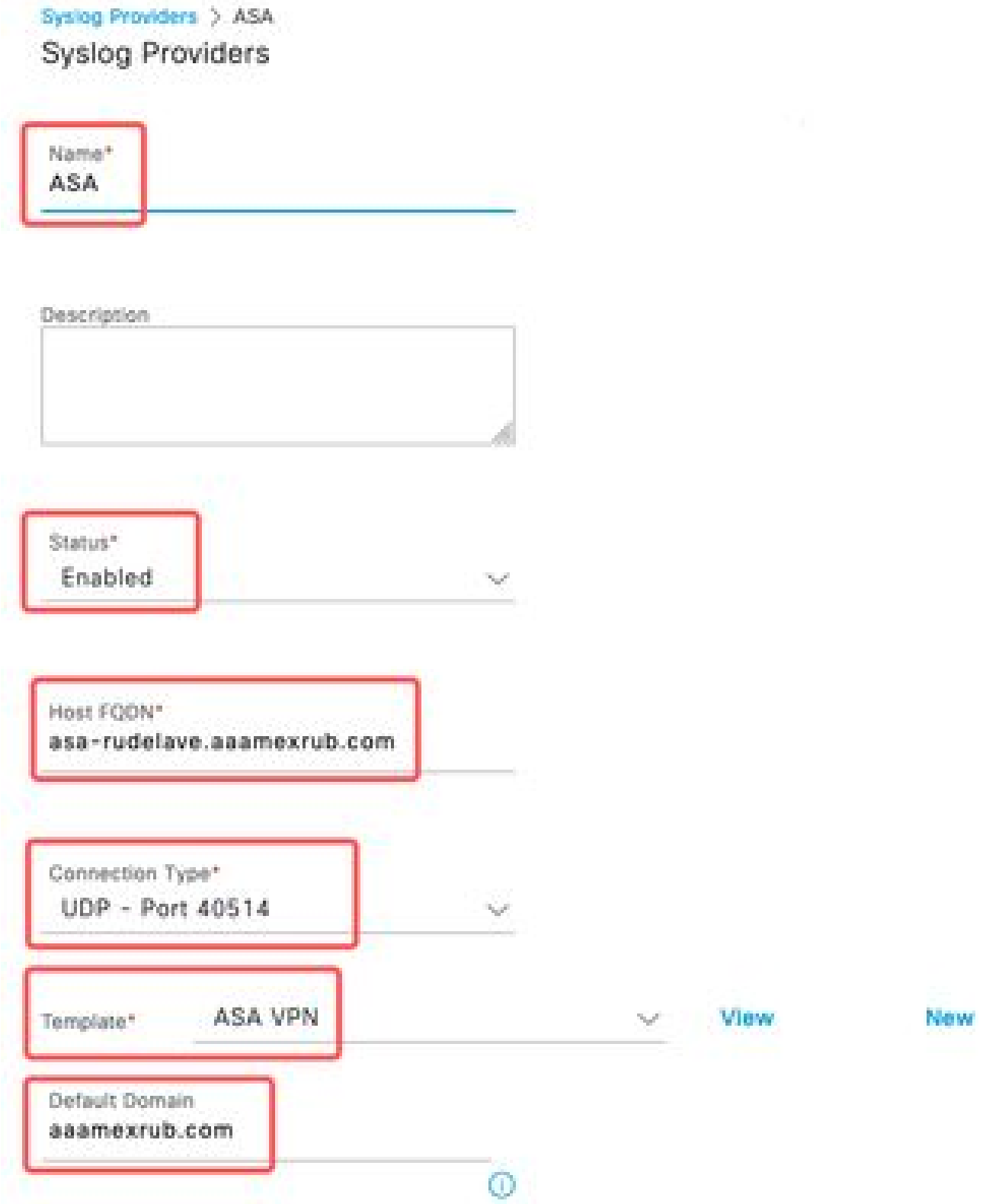


Habilitar Fluxo de Autorização

Etapa 3. Configure o provedor de Syslog.

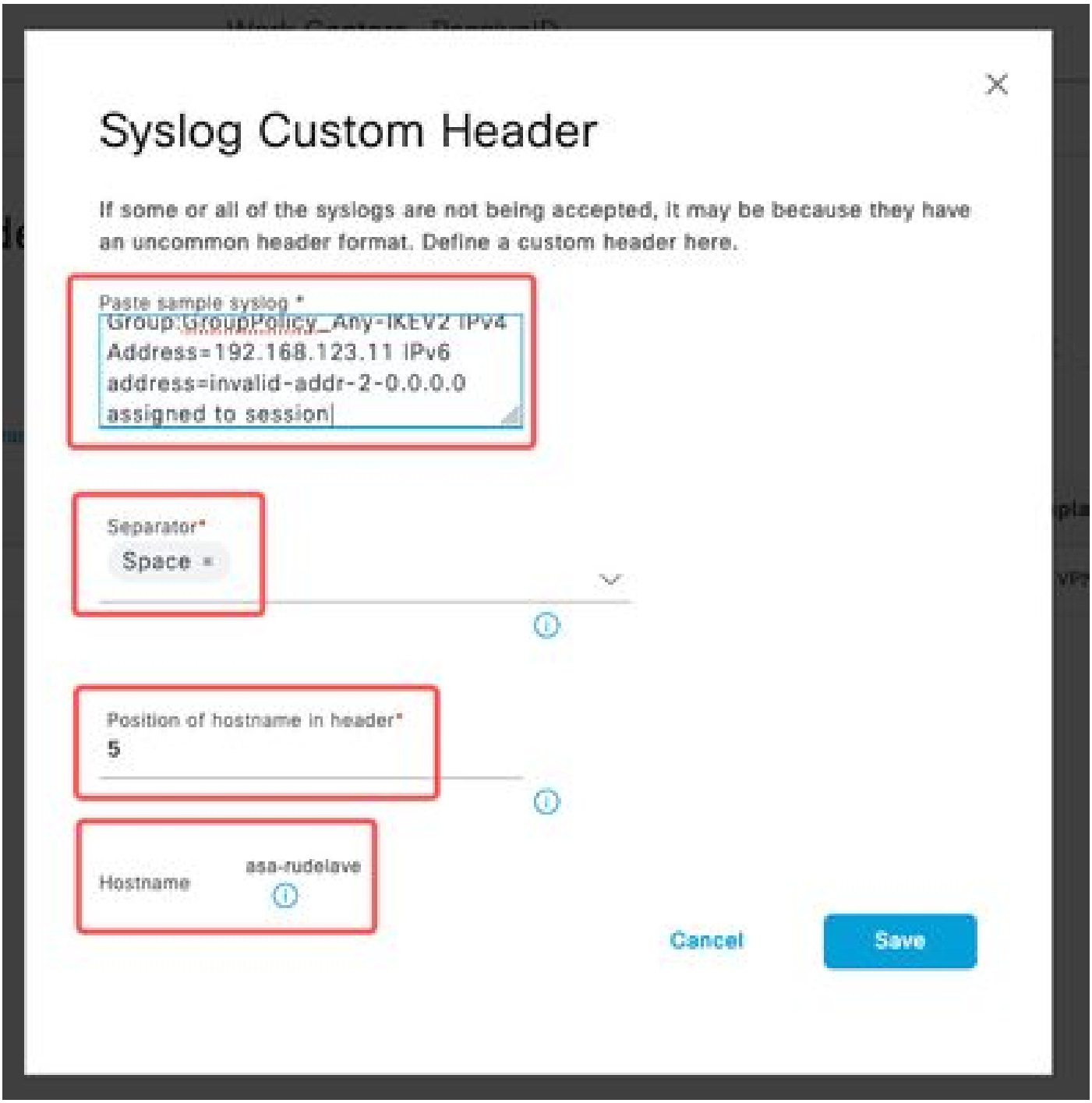
1. Navegue até Centros de trabalho > PassiveID > Provedores, escolha Provedores de Syslog, clique em Adicionar e complete as informações. Clique em Salvar

⚠ Cuidado: Neste caso, o ISE recebe a mensagem de syslog de uma conexão VPN bem-sucedida em um ASA, mas este documento não descreve essa configuração.



Configurar provedor de Syslog

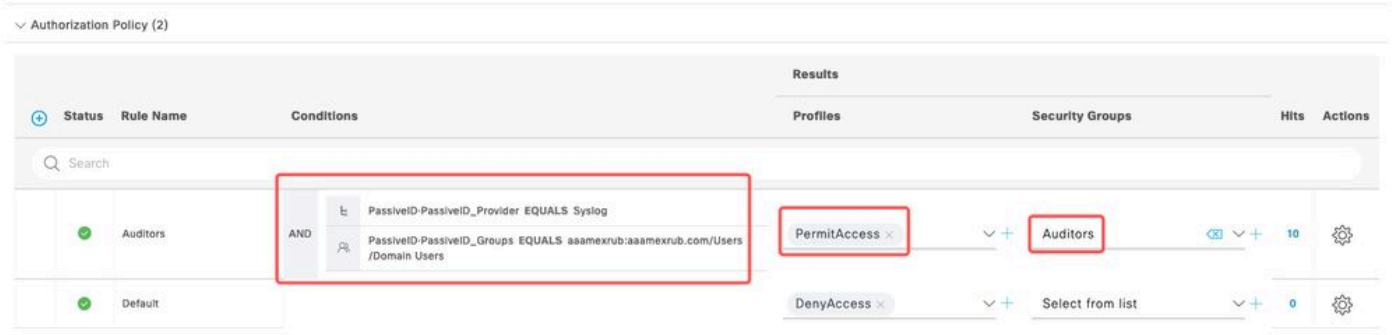
2. Clique em Custom Header. Cole o syslog de exemplo e use um Separador ou uma Guia para localizar o nome de host do dispositivo. Se estiver correto, o nome do host será exibido. Clique em Salvar



Configurar cabeçalho personalizado

Etapa 4. Configurar regras de autorização

1. Navegue até Política > Conjuntos de política. Para esse caso, ele usa a política padrão. Clique na opção Default policy. Na Política de autorização, adicione uma nova regra. Nas políticas PassiveID, o ISE tem todos os provedores. Você pode combinar este com um grupo PassiveID. Escolha Permit Access como Profile e, em Security Groups, escolha a necessidade de SGT.

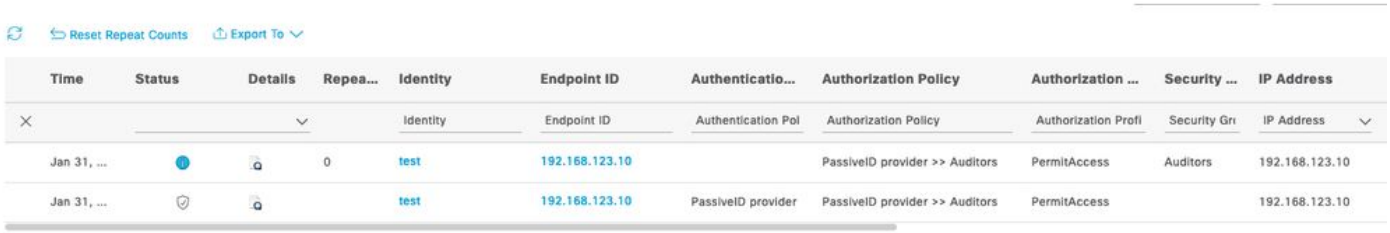


Configurar regras de autorização

Verificar

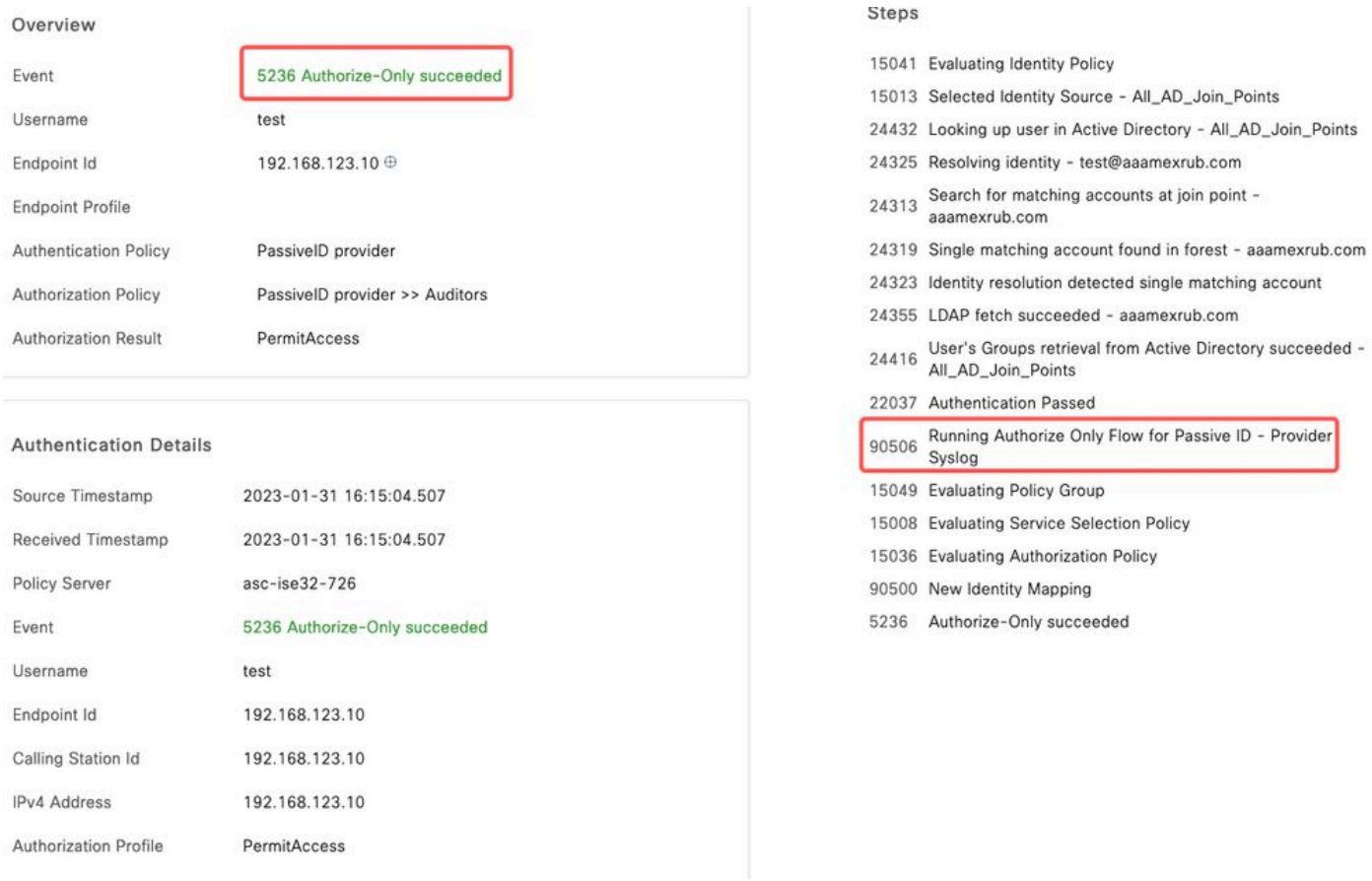
Depois que o ISE receber o Syslog, você poderá verificar os registros em tempo real do Radius para ver o fluxo de autorização. Navegue até Operations > Radius > Live logs.

Nos logs, você pode ver o evento de autorização. Este contém o Nome de usuário, a Política de autorização e a Tag do grupo de segurança associados a ele.



Log ao vivo do Radius

Para verificar mais detalhes, clique no Relatório de detalhes. Aqui você pode ver o fluxo Somente Autorização que avalia as Políticas para atribuir o SGT.



Relatório de Live log do Radius

Troubleshooting

Para esse caso, ele usa dois fluxos: as sessões passiveID e o fluxo de Autorização. Para habilitar as depurações, navegue para Operations > Troubleshoot > Debug Wizard > Debug Log Configuration e escolha o nó do ISE.

Para PassiveID, habilite os próximos componentes para o nível DEBUG:

- IDpassiva

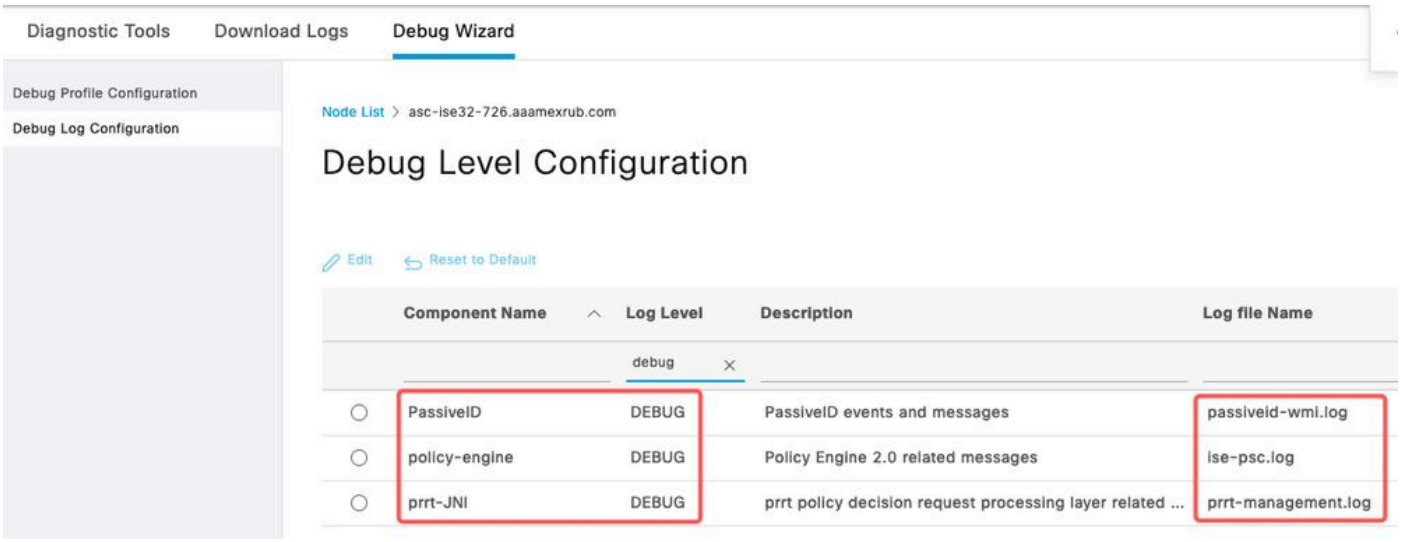
Para verificar os logs, com base no provedor Passive ID, o arquivo a ser verificado para este cenário, você precisa revisar o arquivo passiveid-syslog.log, para os outros provedores:

- passiveid-agent.log
- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- passiveid-wmilog

Para o fluxo de autorização, ative os próximos componentes no nível DEBUG:

- mecanismo de política
- prrt-JNI

Exemplo:



Depurações habilitadas

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.