

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

## Contents

[Introduction](#)

[Informações de Apoio](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuração](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

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 Active Directory (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 Active Directory.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

### Componentes Utilizados

- Software Identity Service Engine (ISE) versão 3.2

- Microsoft Ative Directory
- Syslogs

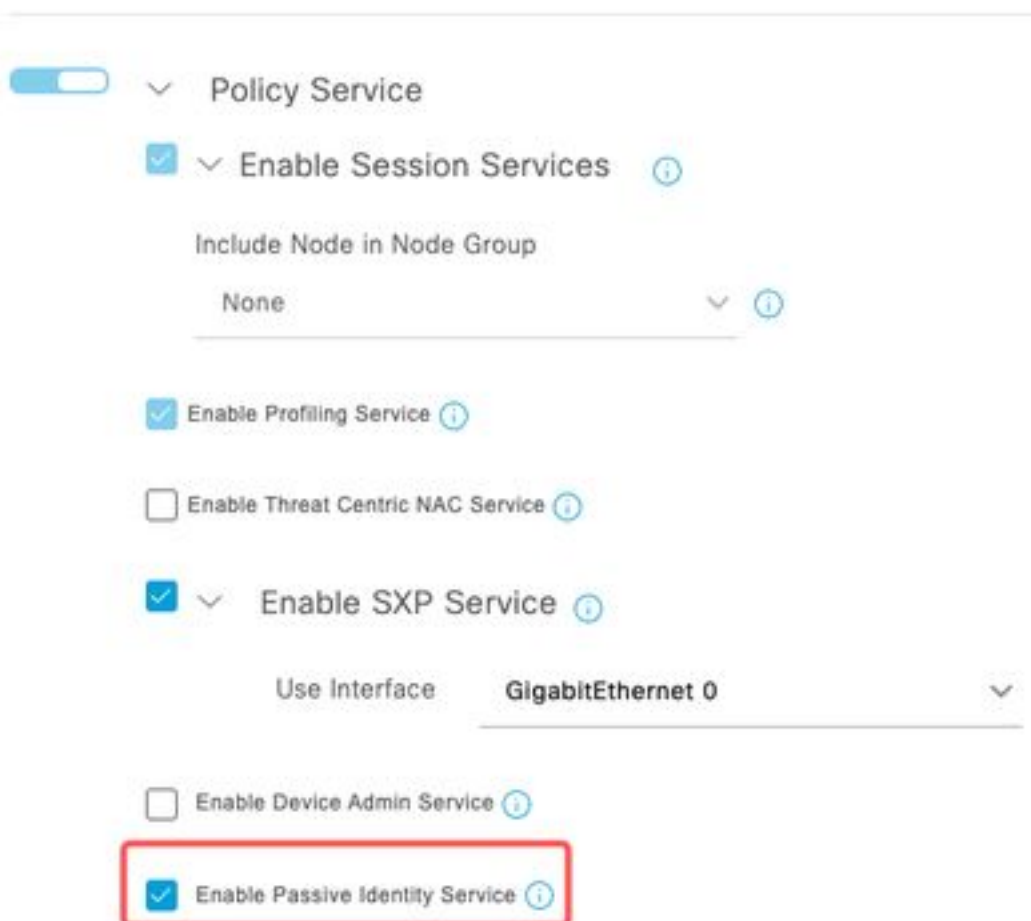
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## 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 PassivelD 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 Directory.


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


Identities   Groups   **External Identity Sources**   Identity Source Sequences

---

**External Identity Sources**

<      

>  Certificate Authentication F

 Active Directory

**Connection**

\* Join Point Name  

\* Active Directory Domain  

*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.



## Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No  

*Continuar ingressando no*

## Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

\* AD User Name 

\* Password

Specify Organizational Unit 

Store Credentials 

Cancel  

*Ingressar no Ative*

ISE  
Directory

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

## Select Directory Groups

This dialog is used to select groups from the Directory.

Domain: aaamexrub.com

Name Filter: \_\_\_\_\_ SID Filter: \_\_\_\_\_ Type Filter: All

53 Groups Retrieved.

<input type="checkbox"/>	aaamexrub.com/Users/Cloneable Domain Contro...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Denied RODC Password ...	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsAdmins	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsUpdateProxy	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Computers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Controllers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Guests	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Admins	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Read-only De...	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Group Policy Creator Ow...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Protected Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL

Recuperar grupos do AD

Connection    Allowed Domains    PassiveID    **Groups**

<input type="checkbox"/>	Name	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Users	S
<input type="checkbox"/>	aaamexrub.com/Users/sponsors	S

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.

## PassiveID Settings

The PassiveID settings that are configured in this section are applied to all the join points in Cisco ISE.

History interval*	10
Domain Controller event inactivity time* (monitored by Agent)	0
Latency interval of events from agent*	0
User session aging time*	24

Authorization Flow ⓘ

*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.

## Syslog Providers

Name\*  
ASA

Description


Status\*  
Enabled

Host FQDN\*  
asa-rudelave.aaamexrub.com

Connection Type\*  
UDP - Port 40514

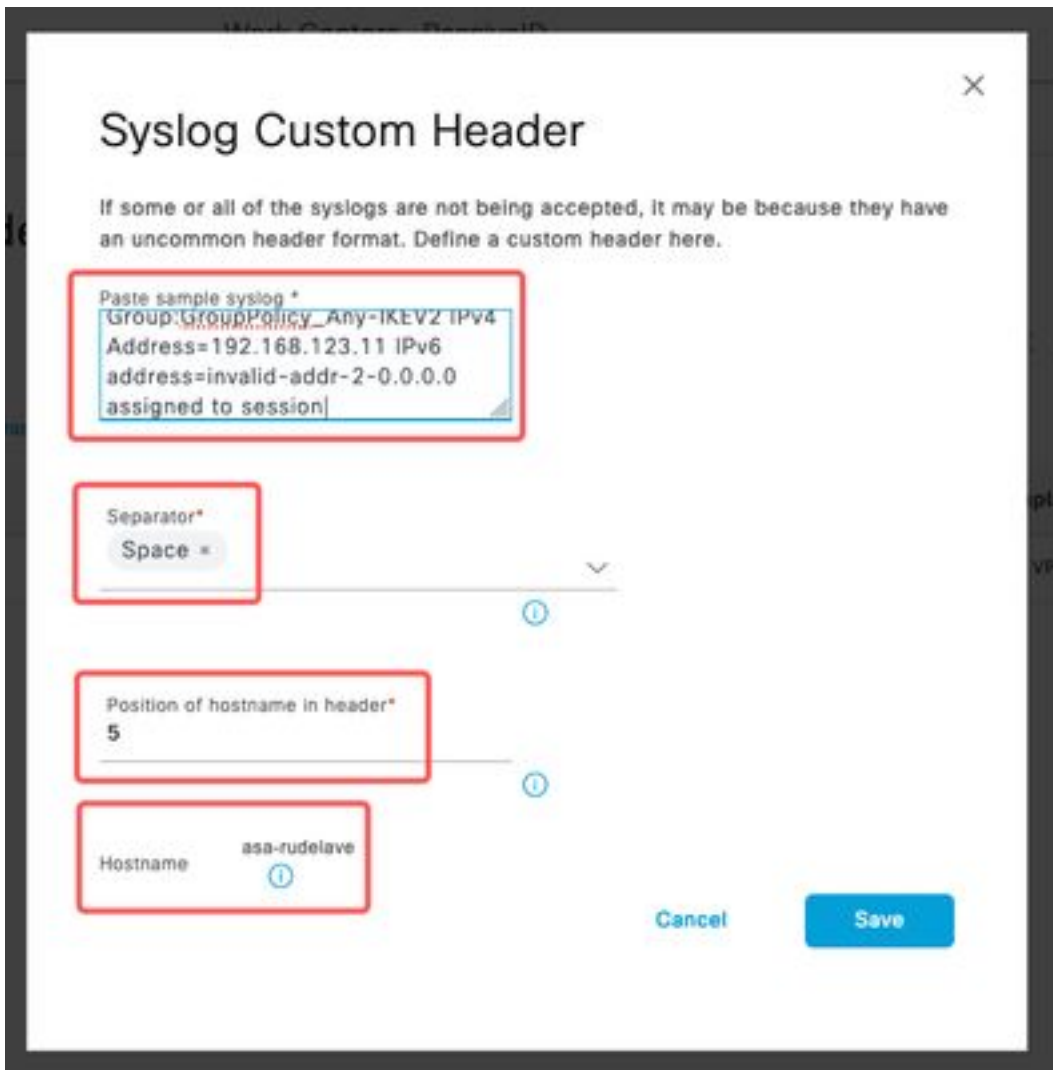
Template\* ASA VPN [View](#) [New](#)

Default Domain  
aaamexrub.com



*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

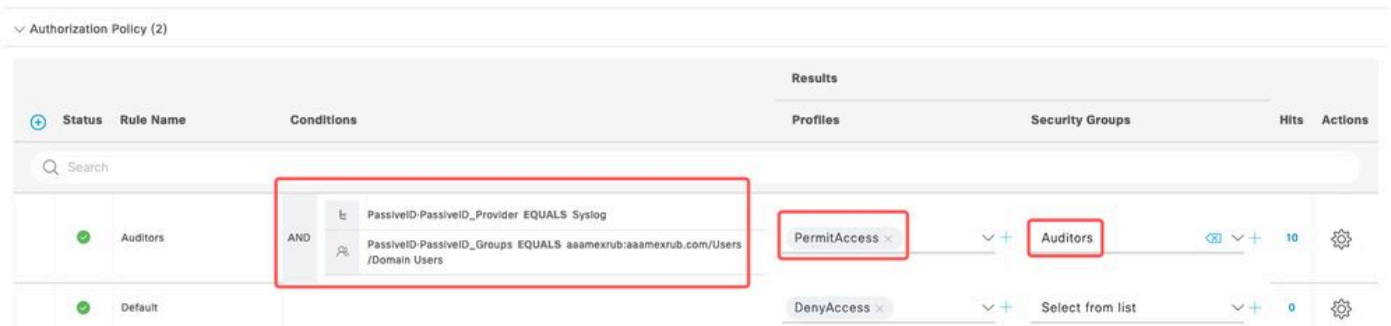


Configurar cabeçalho

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.

Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
Jan 31, ...			0	test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...				test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

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.

### Overview

Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Endpoint Profile	
Authentication Policy	PassiveID provider
Authorization Policy	PassiveID provider >> Auditors
Authorization Result	PermitAccess

### Steps

- 15041 Evaluating Identity Policy
- 15013 Selected Identity Source - All\_AD\_Join\_Points
- 24432 Looking up user in Active Directory - All\_AD\_Join\_Points
- 24325 Resolving identity - test@aaamexrub.com
- 24313 Search for matching accounts at join point - aaamexrub.com
- 24319 Single matching account found in forest - aaamexrub.com
- 24323 Identity resolution detected single matching account
- 24355 LDAP fetch succeeded - aaamexrub.com
- 24416 User's Groups retrieval from Active Directory succeeded - All\_AD\_Join\_Points
- 22037 Authentication Passed
- 90506 Running Authorize Only Flow for Passive ID - Provider Syslog
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15036 Evaluating Authorization Policy
- 90500 New Identity Mapping
- 5236 Authorize-Only succeeded

### Authentication Details

Source Timestamp	2023-01-31 16:15:04.507
Received Timestamp	2023-01-31 16:15:04.507
Policy Server	asc-ise32-726
Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Calling Station Id	192.168.123.10
IPv4 Address	192.168.123.10
Authorization Profile	PermitAccess

Relatório de Live log do Radius

## Troubleshoot

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:

The screenshot shows the 'Debug Wizard' interface for 'asc-ise32-726.aamexrub.com'. The 'Debug Level Configuration' section is active, showing a table of components and their log levels. The log level for all listed components is set to 'DEBUG'. The log file names are also specified for each component.

Component Name	Log Level	Description	Log file Name
<input type="radio"/> PassiveID	DEBUG	PassiveID events and messages	passiveid-wmi.log
<input type="radio"/> policy-engine	DEBUG	Policy Engine 2.0 related messages	ise-psc.log
<input type="radio"/> prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log

*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.