

# Configure Authorization Flow for Passive ID Sessions in ISE 3.2

## Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes how to configure Authorization rules for Passive ID events to assign SGTs to the sessions.

## Background Information

Passive identity services (Passive ID) do not authenticate users directly, but gather user identities and IP addresses from external authentication servers such as Active Directory (AD), known as providers, and then share that information with subscribers.

ISE 3.2 introduces a new feature that allows you to configure an authorization policy to assign a Security Group Tag (SGT) to a user based on the Active Directory group membership.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ISE 3.X
- Passive ID integration with any provider
- Active Directory (AD) administration
- Segmentation (Trustsec)
- PxGrid (Platform Exchange Grid)

### Components Used

- Identity Service Engine (ISE) software version 3.2
- Microsoft Active directory
- Syslogs

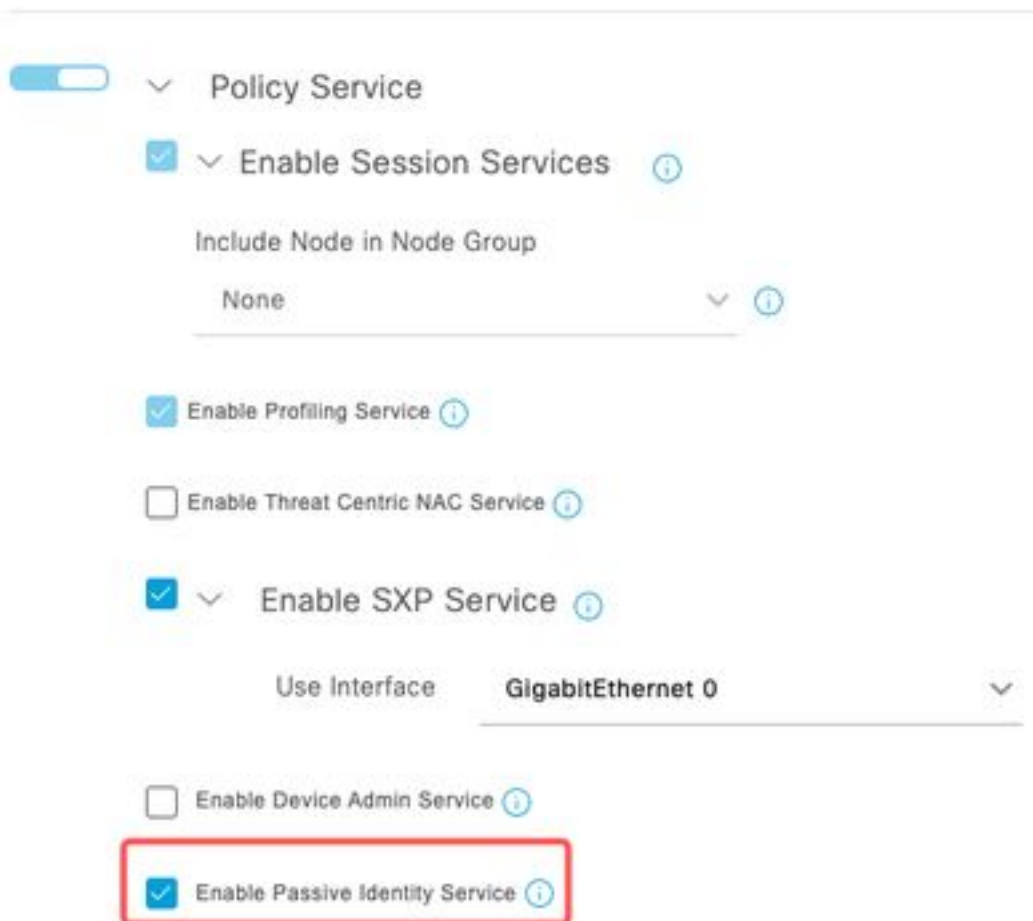
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Configuration

Step 1. Enable ISE Services.

1. On ISE, navigate to **Administration > Deployment**, choose the ISE node and click **Edit**, enable **Policy Service** and choose **Enable Passive Identity Service**. Optional, you can enable SXP and PxGrid if the passive id sessions need to be published through each one. Click **Save**.

**Warning:** SGT details of the PassiveID login users that are authenticated by API provider cannot be published into SXP. However, the SGT details of these users can be published through pxGrid and pxGrid Cloud.



*Services Enabled*

Step 2. Configure the Active Directory.

1. Navigate to **Administration > Identity Management > External Identity Sources** and choose **Active directory** then click the **Add** button.
2. Enter the **Join Point Name** and **Active Directory Domain**. Click **Submit**.

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

---

**External Identity Sources**

<   [Icon]   [Icon]

> [Folder] Certificate Authentication F

[Folder] Active Directory

**Connection**

\* Join Point Name   **aaamexrub**

\* Active Directory Domain   **aaamexrub.com**

*Add Active Directory*

3. A pop up appears to join ISE to the AD. Click **Yes**. Enter the **Username** and **Password**. Click **OK**.

**i**

## Information

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

No   **Yes**

*Continue to join*

## Join Domain

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

\* AD User Name ⓘ **user**

\* Password \*\*\*\*\*

Specify Organizational Unit ⓘ

Store Credentials ⓘ

Cancel   **OK**

*ISE*   *Join Active Directory*

4. Retrieve AD groups. Navigate to **Groups**, click **Add**, then click **Retrieve Groups** and choose all the interested groups and click **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

Retrieve AD groups

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

Retrieved Groups

5. Enable Authorization flow. Navigate to **Advance Settings** and in the section **PassiveID Settings** check the **Authorization Flow** checkbox. 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 ⓘ

*Enable Authorization Flow*

Step 3. Configure Syslog provider.

1. Navigate to **Work Centers > PassiveID > Providers**, choose **Syslog Providers**, click **Add** and complete the information. Click **Save**

**Caution:** In this case, ISE receives the syslog message from a successful VPN connection in an ASA, but this document does not describe that configuration.

## Syslog Providers

Name\*  
ASA

Description


Status\*  
Enabled

Host FQDN\*  
asa-rudelave.aaamexrub.com

Connection Type\*  
UDP - Port 40514

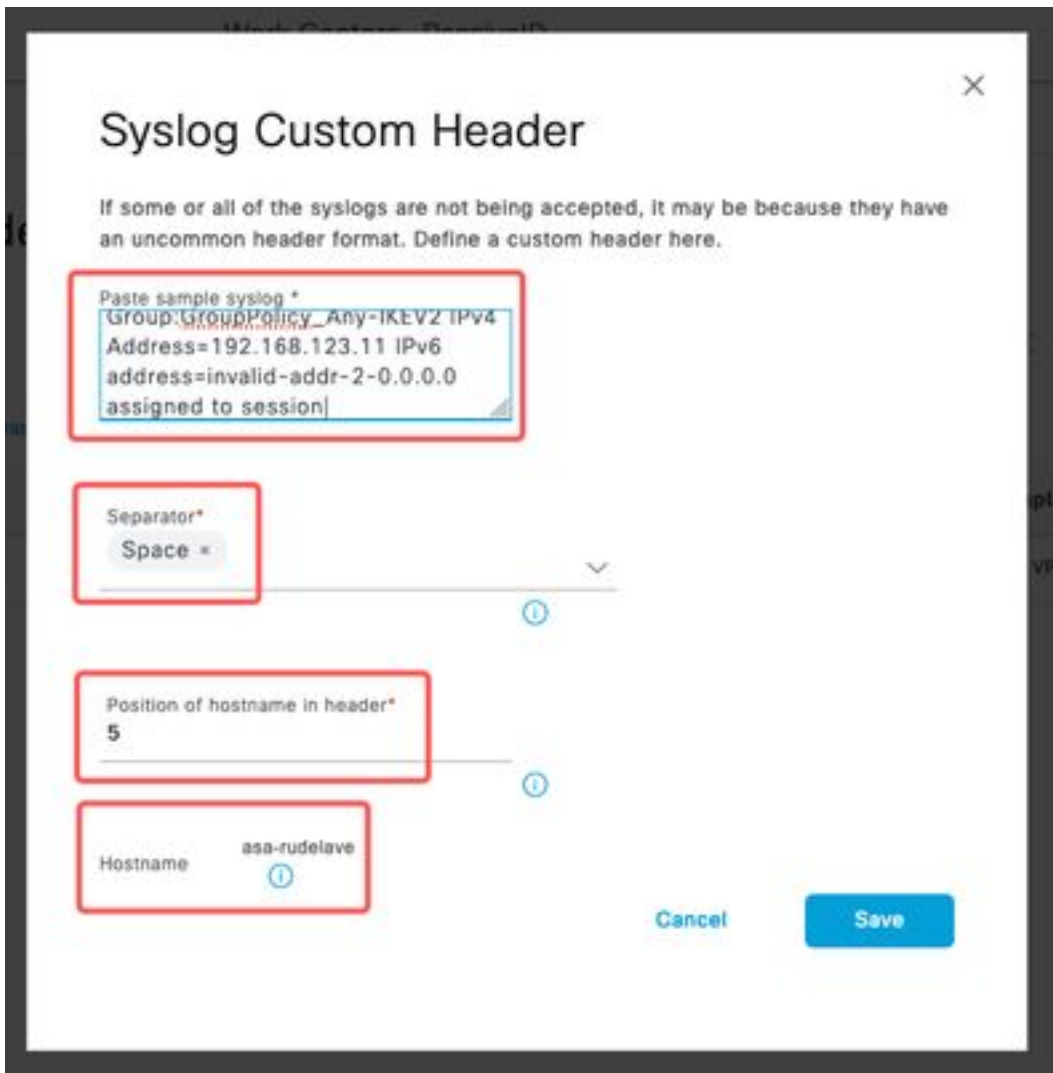
Template\* ASA VPN [View](#) [New](#)

Default Domain  
aaamexrub.com



*Configure Syslog provider*

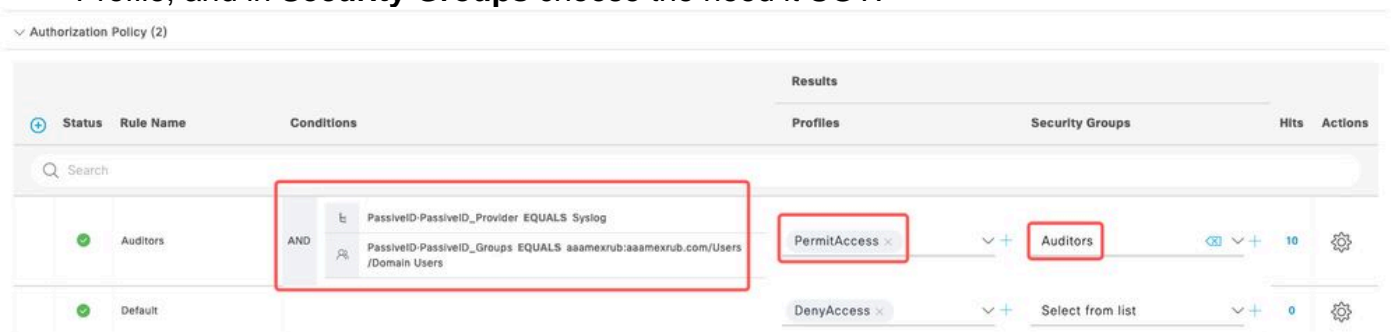
2. Click **Custom Header**. Paste the sample syslog and use a Separator or Tab to find the device hostname. If it is correct, the Hostname appears. Click **Save**



Configure Custom Header

#### Step 4. Configure Authorization rules

1. Navigate to **Policy > Policy Sets**. For this case, it uses the Default policy. Click the **Default** policy. In the **Authorization Policy**, add a new rule. In the PassivID policies, ISE has all the providers. You can combine this one with a PassivID group. Choose **Permit Access** as Profile, and in **Security Groups** choose the need it SGT.



Configure Authorization Rules

## Verify

Once ISE receives the Syslog, you can check the Radius Live Logs to see Authorization Flow. Navigate to **Operations > Radius > Live logs**.

In the logs you can see the Authorization event. This one contains the Username, Authorization

Policy and Security Group Tag associated with it.

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

Radius Live Log

To check more details, click the **Detail Report**. Here you can see the Authorize-Only flow that evaluates the Policies to assign the 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

Radius Live log Report

## Troubleshoot

For this case, it uses two flows; the passiveID sessions and the Authoriation flow. To enable the debugs, navigate to **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**, then choose the ISE node.

For the PassiveID, enable the next components to **DEBUG** level:

- PassiveID

To check the logs, based on the Passive ID provider, the file to check for this scenario, you need to review the **file** passiveid-syslog.log, for the other providers:

- passiveid-agent.log
- passiveid-api.log



- passiveid-endpoint.log
- passiveid-span.log
- passiveid-wmilog

For the Authorization Flow, enable the next components to **DEBUG** level:

- policy-engine
- prrt-JNI

Example:

The screenshot shows the 'Debug Wizard' interface for a node named 'asc-ise32-726.aaamexrub.com'. The main section is titled 'Debug Level Configuration'. Below the title, there are 'Edit' and 'Reset to Default' buttons. A table lists the configuration for three components, all set to the 'debug' log level. The 'Log file Name' column for each component is highlighted with a red box.

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

*Debugs enabled*