

# Configure ISE 3.2 to Assign Security Group Tags for PassiveID Sessions

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Flow Diagram](#)

[Configurations](#)

[Verify](#)

[ISE Verification](#)

[PxGrid Subscriber Verification](#)

[TrustSec SXP Peer Verification](#)

[Troubleshoot](#)

[Enable Debugs on ISE](#)

[Logs Snippets](#)

## Introduction

This document describes how to configure and assign Security Group Tags (SGTs) to Passive ID sessions via authorization policies in ISE 3.2.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ISE 3.2
- Passive ID, TrustSec, and PxGrid

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P that runs 16.12.1

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.

# Background Information

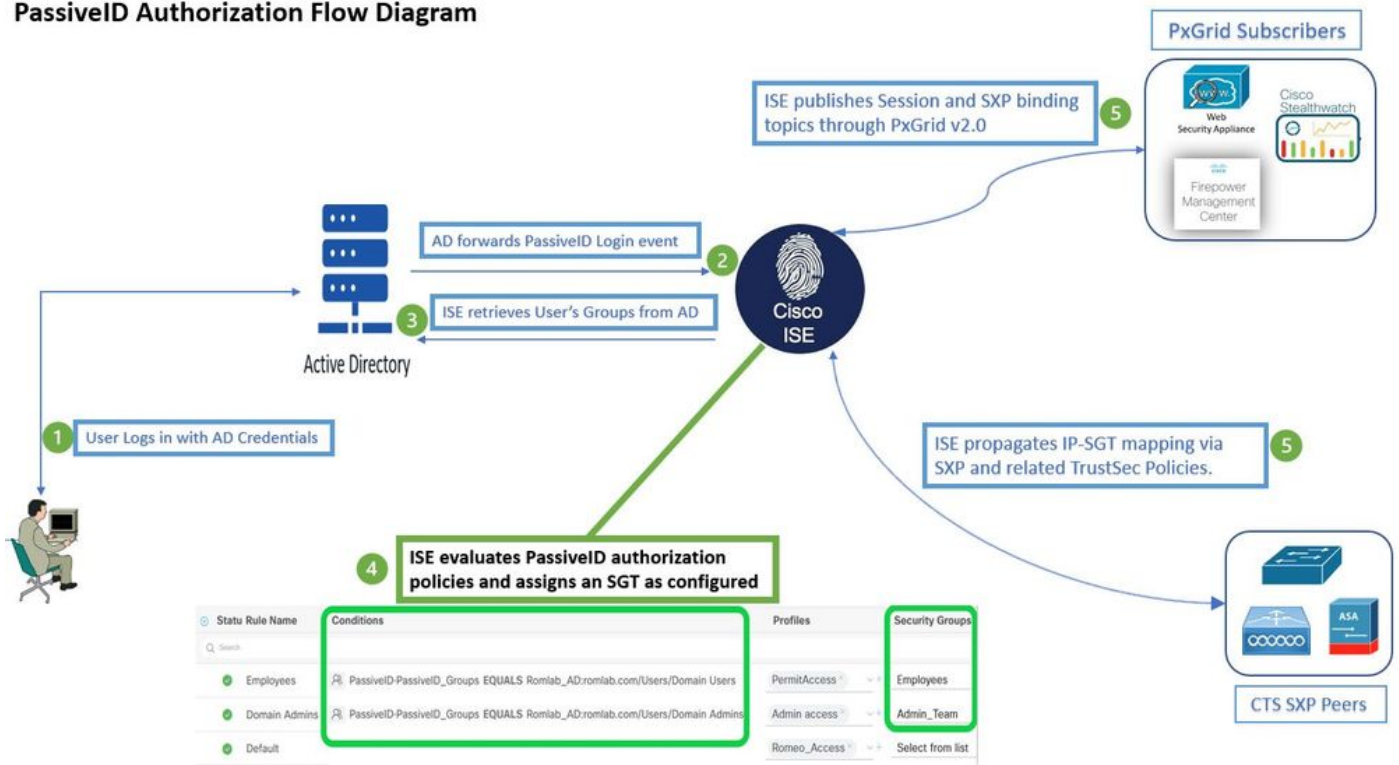
The Cisco Identity Services Engine (ISE) 3.2 is the minimum version that supports this capability. This document does not cover PassiveID, PxGrid, and SXP configuration. For related information, see the [Admin Guide](#).

In ISE 3.1 or older versions, a Security Group Tag (SGT) can only be assigned to Radius session or Active Authentication such as 802.1x and MAB. With ISE 3.2, we can configure authorization policies for PassiveID Sessions such that when Identity Services Engine (ISE) receives user login events from a provider such as Active Directory Domain Controllers (AD DC) WMI or AD Agent, it assigns a Security Group Tag (SGT) to the PassiveID Session based on the user Active Directory (AD) group membership. The IP-SGT mapping and AD group details for the PassiveID can be published to the TrustSec domain via SGT Exchange Protocol (SXP) and/or to Platform Exchange Grid (pxGrid) subscribers such as Cisco Firepower Management Center (FMC) and Cisco Secure Network Analytics (Stealthwatch).

## Configure

### Flow Diagram

PassiveID Authorization Flow Diagram

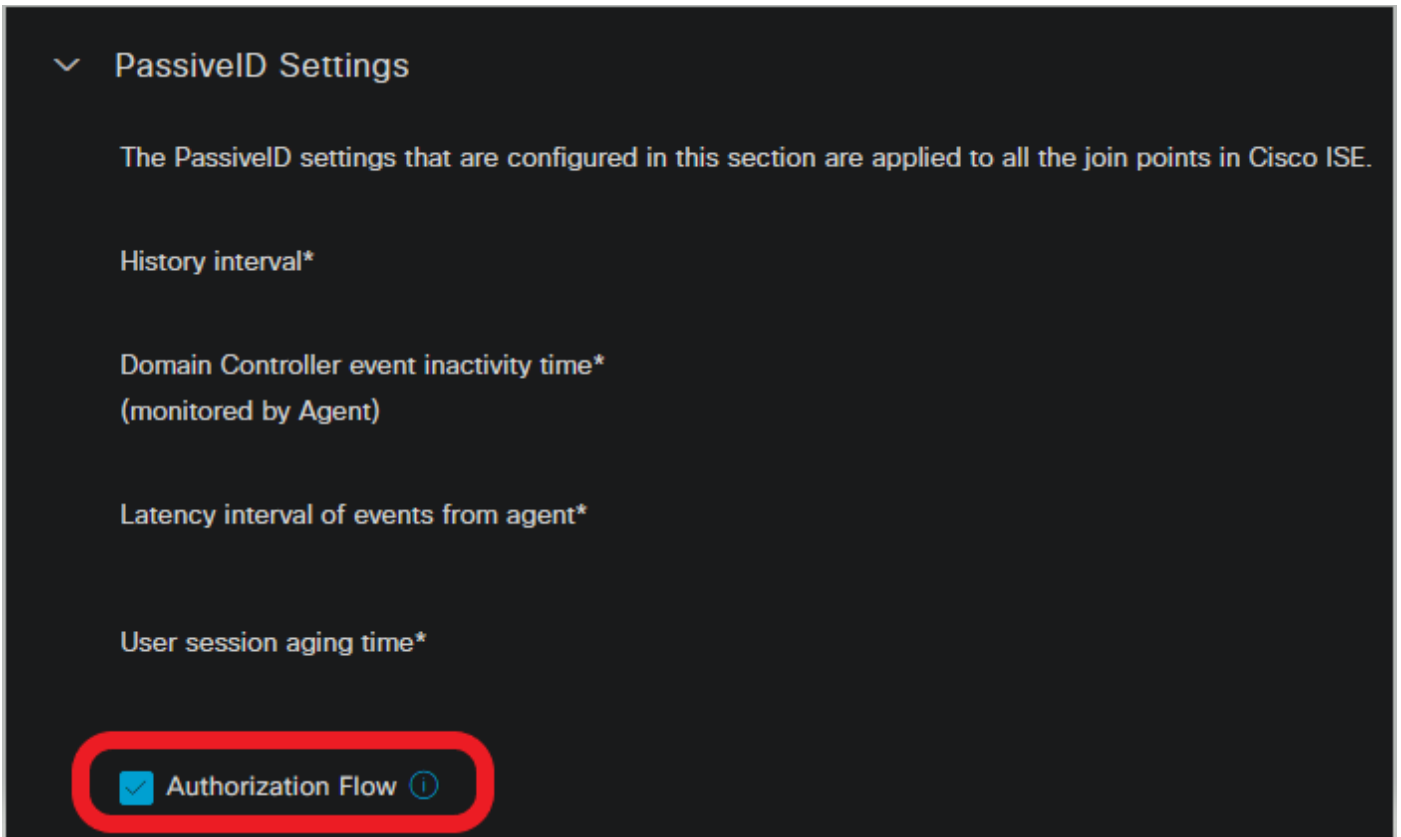


Flow Diagram

## Configurations

Enable the authorization flow:

Navigate to **Active Directory > Advanced Settings > PassiveID Settings** and check the **Authorization Flow** checkbox in order to configure authorization policies for PassiveID login users. This option is disabled by default.

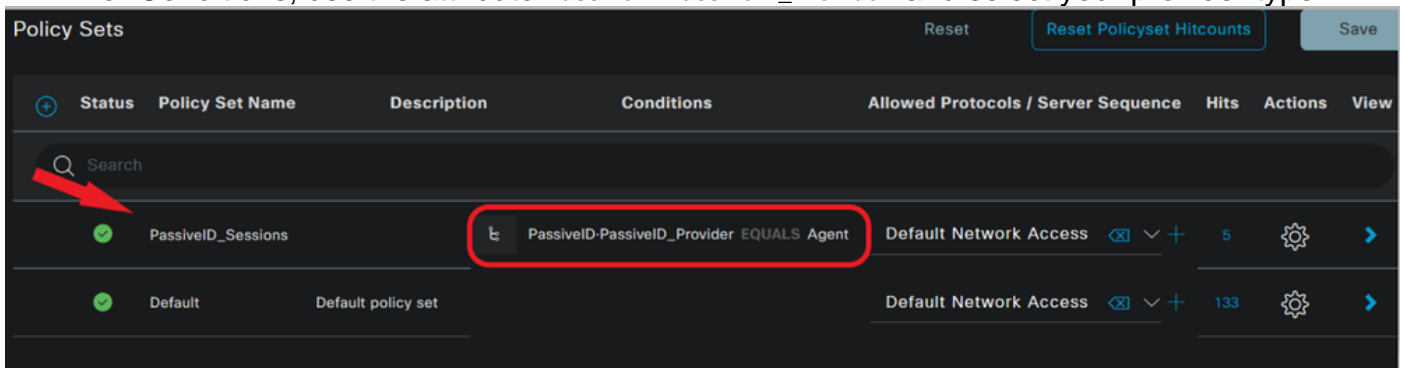


Enable the authorization flow

**Note:** For this feature to work, ensure that you run PassivID, PxGrid, and SXP services in your deployment. You can verify this under **Administration > System > Deployment**.

### Policy Set Configuration:

1. Create a separate Policy Set for PassivID (recommended).
2. For Conditions, use the attribute **PassivID-PassivID\_Provider** and select your provider type.



Policy Sets

3. Configure Authorization rules for the Policy Set created in Step 1.

- Create a condition for each rule and use the PassivID dictionary based on AD groups, Usernames, or Both.
- Assign a Security Group Tag for each rule and save the configurations.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Employees	PassiveID-PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Users	PermitAccess x	Employees	3	ⓘ v + ⚙
●	Domain Admins	PassiveID-PassiveID_Groups EQUALS Lfc_AD:Lfc.lab/Users /Domain Admins	Admin access x	Admin_Team	2	ⓘ v + ⚙
●	Default		DenyAccess x	Select from list	0	v + ⚙

Authorization Policy

**Note:** The authentication policy is irrelevant as it's not used in this flow.

**Note:** You can use `PassiveID_Username`, `PassiveID_Groups`, or `PassiveID_Provider` attributes to create the authorization rules.

4. Navigate to **Work Centers > TrustSec > Settings > SXP Settings** to enable **Publish SXP bindings on pxGrid** and **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** to share PassiveID mappings with PxGrid subscribers and include them in the SXP mappings table on ISE.

**SXP Settings**

- Publish SXP bindings on pxGrid
- Add Radius and PassiveID mappings into SXP IP SGT mapping table

**Global Password**

Global Password  
●●●●●●●●●●

This global password will be overridden by the device specific password

SXP Settings

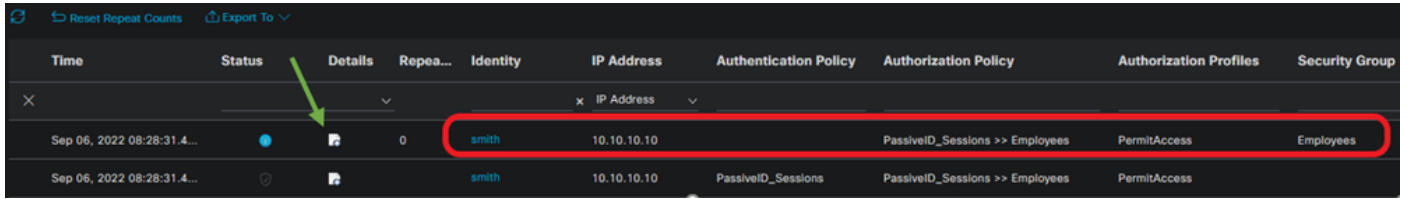
## Verify

Use this section in order to confirm that your configuration works properly.



## ISE Verification

Once the user login events have been sent to ISE from a provider such as Active Directory

Domain Controllers (AD DC) WMI or AD Agent, proceed to check the Live Logs. Navigate to **Operations > Radius > Live Logs**.



The screenshot shows a table with the following columns: Time, Status, Details, Repea..., Identity, IP Address, Authentication Policy, Authorization Policy, Authorization Profiles, and Security Group. The first row is highlighted with a red border. A green arrow points to a magnifier icon in the Details column of the first row.

Time	Status	Details	Repea...	Identity	IP Address	Authentication Policy	Authorization Policy	Authorization Profiles	Security Group
Sep 06, 2022 08:28:31.4...	●		0	smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Employees	PermitAccess	Employees
Sep 06, 2022 08:28:31.4...	●			smith	10.10.10.10	PassiveID_Sessions	PassiveID_Sessions >> Employees	PermitAccess	

*Radius LiveLogs*

Click the magnifier icon in the Details column to view a detailed report for a user, in this example smith (Domain Users) as shown here.

