Configure ISE to Assign Trustsec 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.

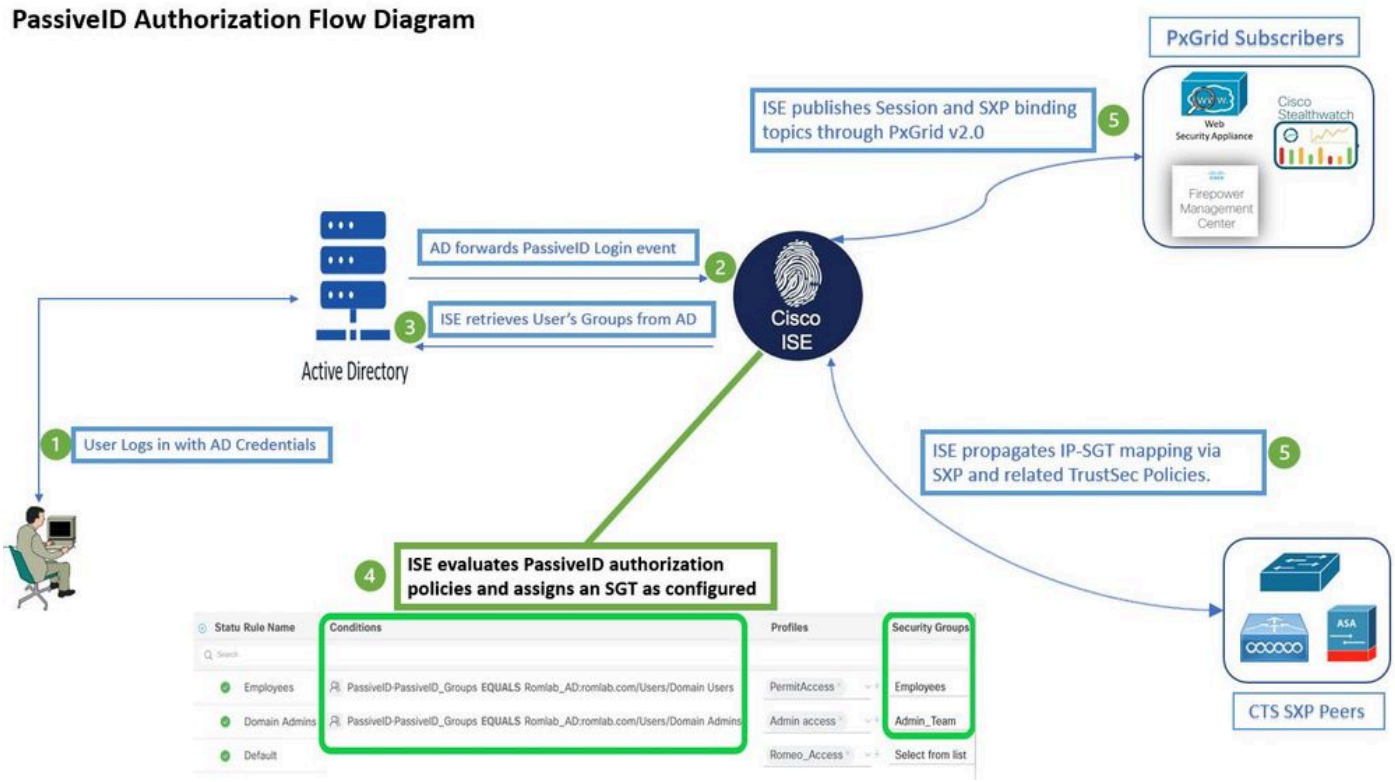
Background Information

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

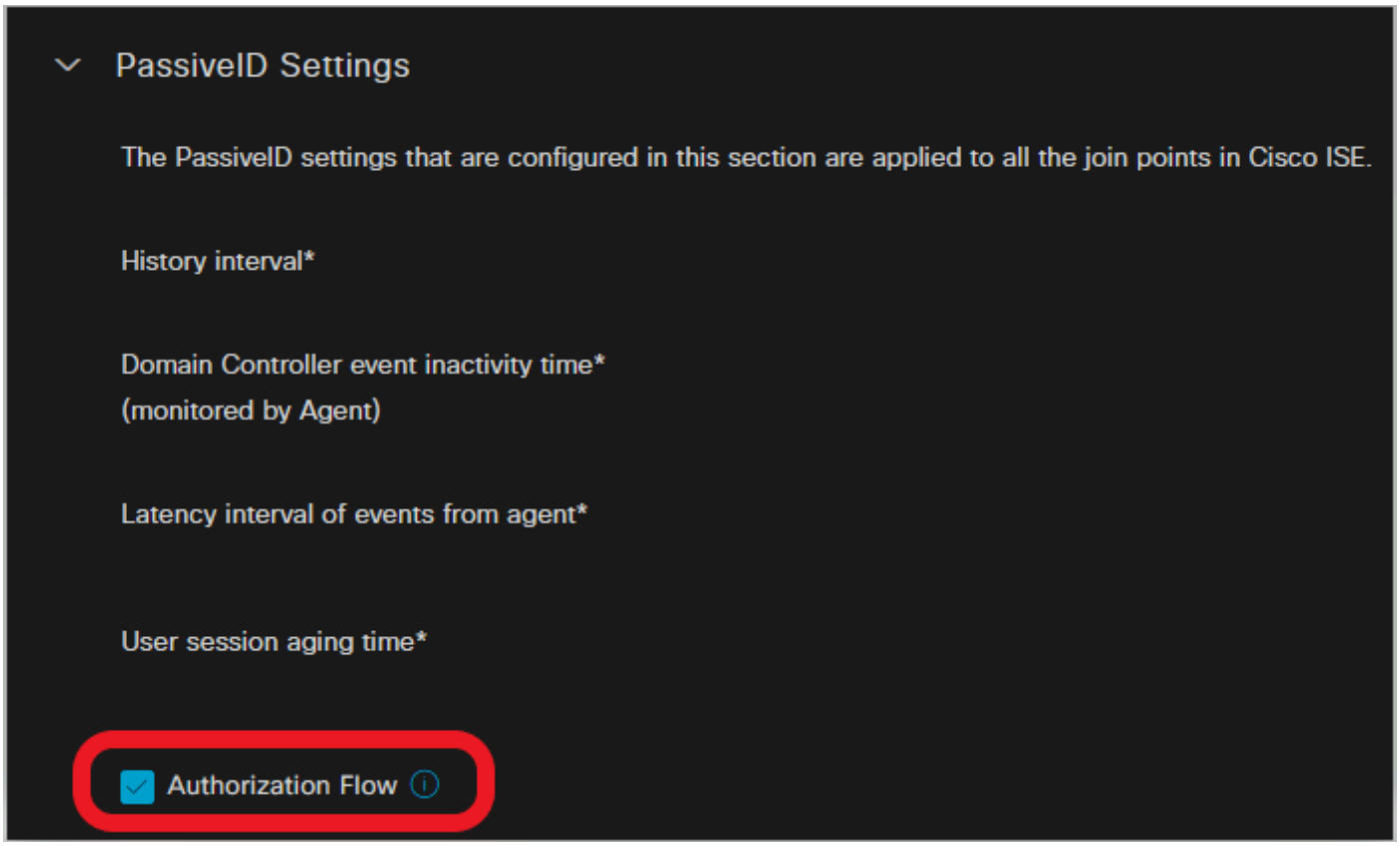


Flow Diagram

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.

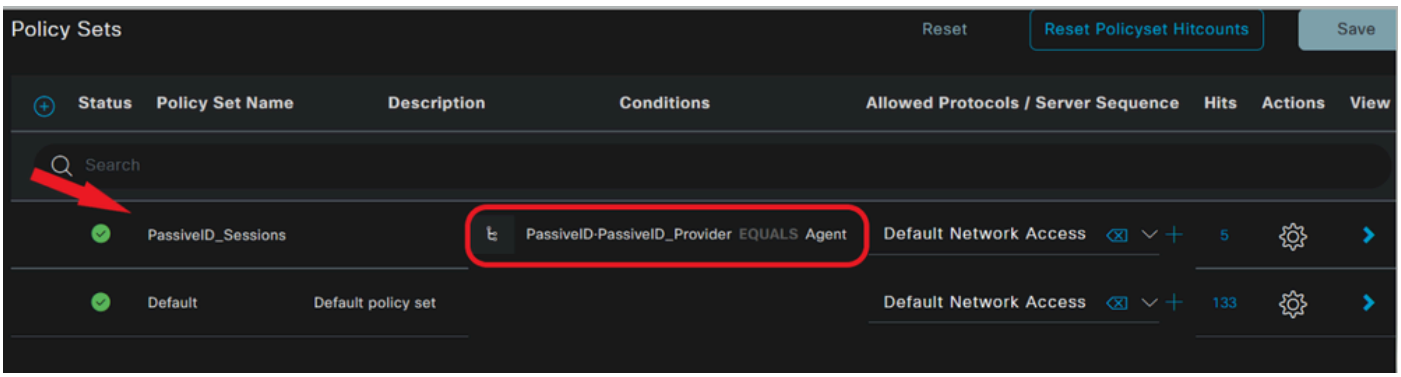


Enable the authorization flow

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

Policy Set Configuration:

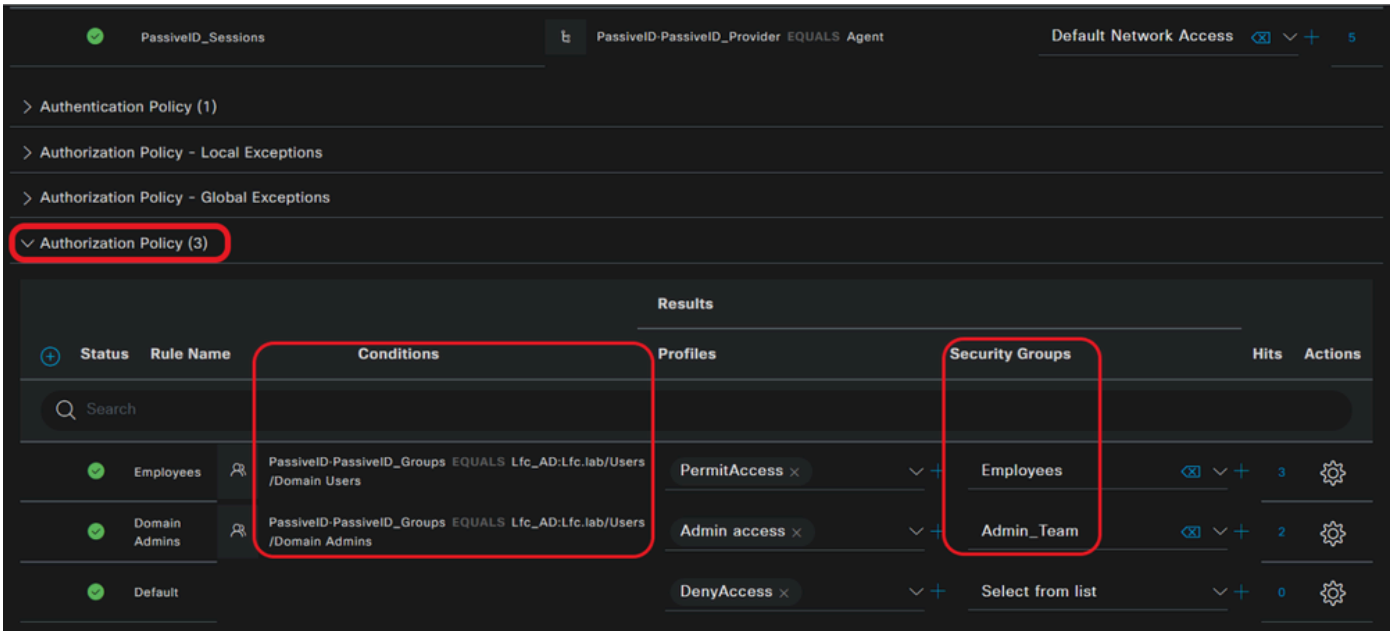
1. Create a separate **Policy Set** for PassiveID (recommended).
2. For Conditions, use the attribute **PassiveID·PassiveID_Provider** and select your **provider** type.



Policy Sets

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

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

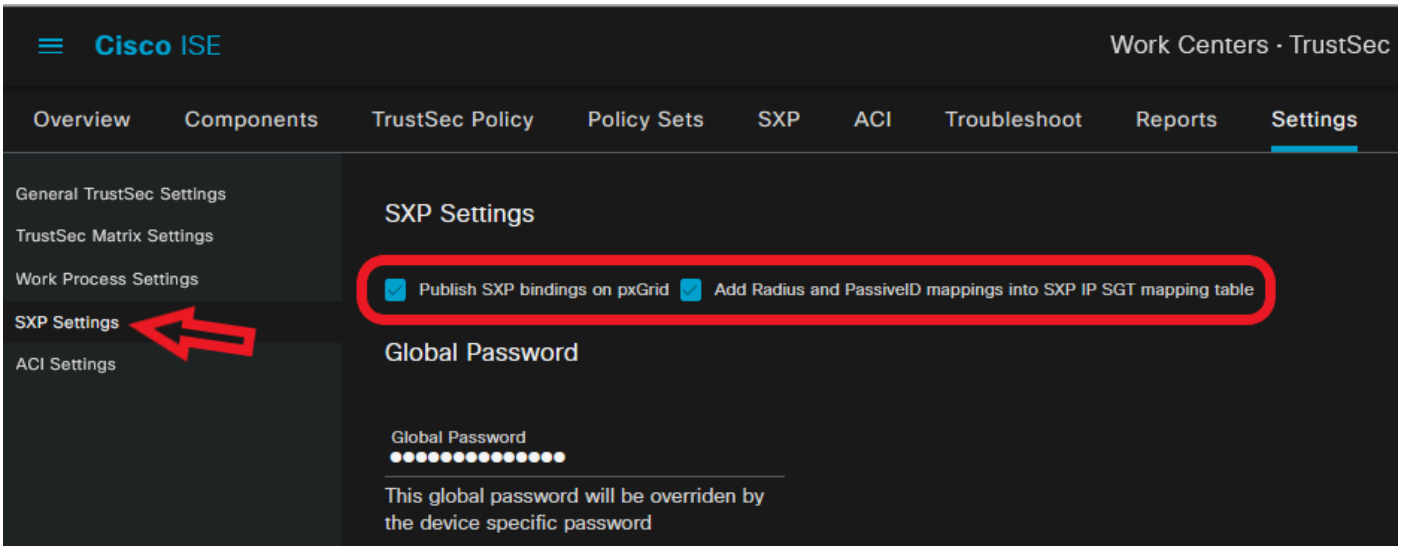


Authorization Policy

Note: The authentication policy is irrelevant as it is 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.



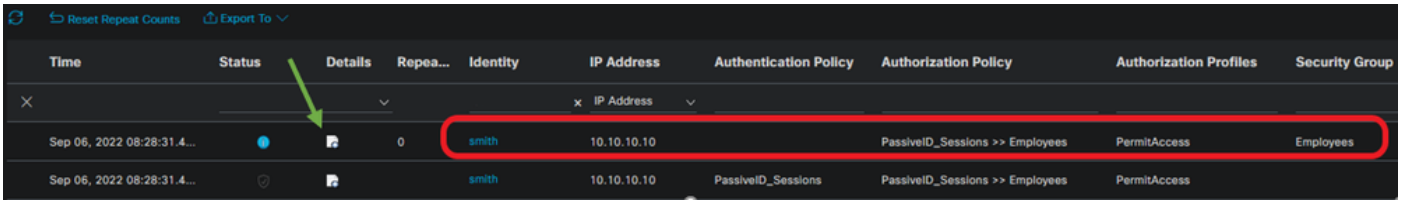
SXP Settings

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**.



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.

Cisco ISE

Overview

Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Endpoint Profile	
Authentication Policy	PassiveID_Sessions
Authorization Policy	PassiveID_Sessions >> Employees
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2022-09-06 20:28:31.393
Received Timestamp	2022-09-06 20:28:31.393
Policy Server	ise-3-2
Event	5236 Authorize-Only succeeded
Username	smith
Endpoint Id	10.10.10.10
Calling Station Id	10.10.10.10
IPv4 Address	10.10.10.10
Authorization Profile	PermitAccess

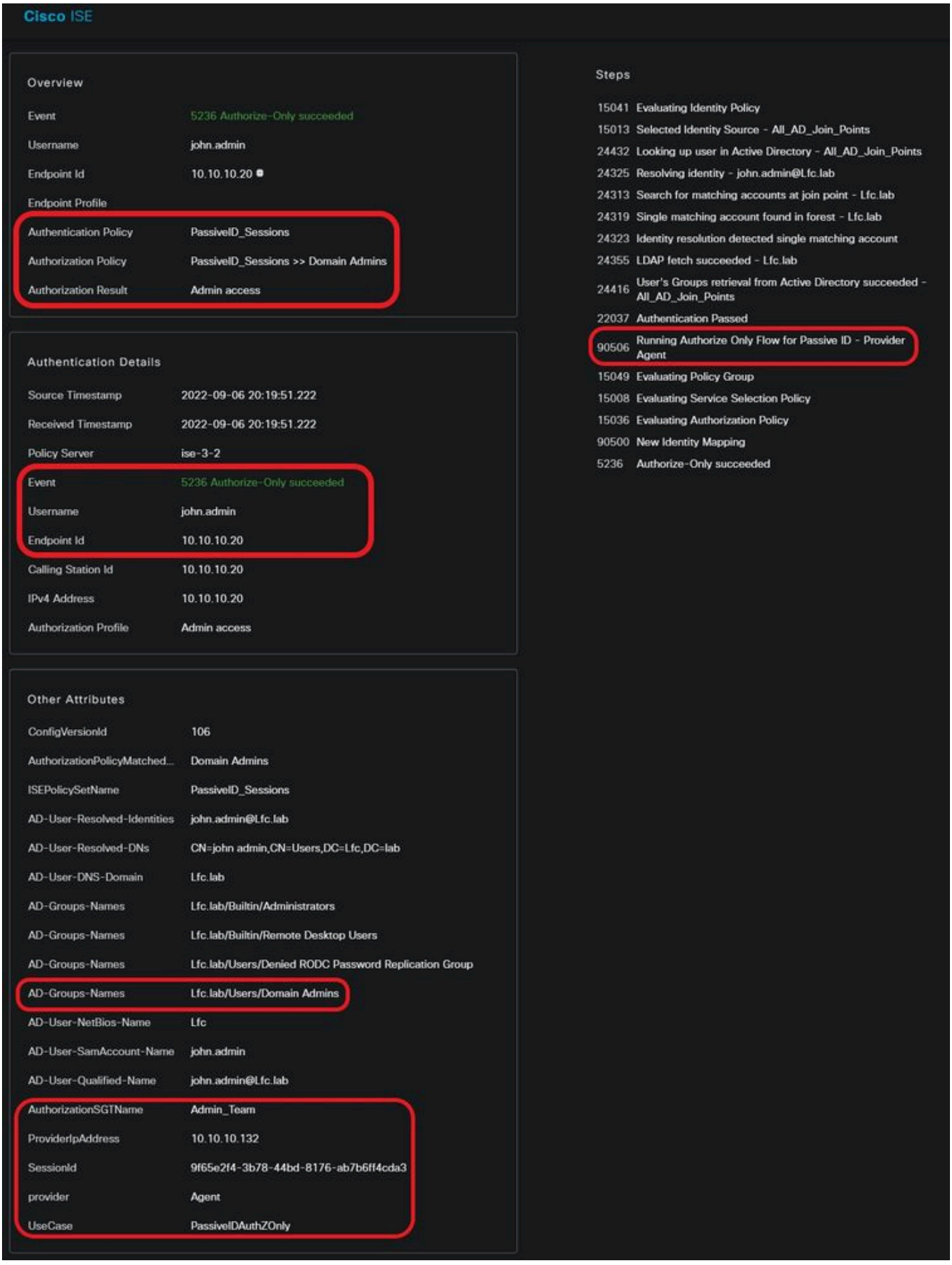
Other Attributes

ConfigVersionId	108
AuthorizationPolicyMatched...	Employees
ISEPolicySetName	PassiveID_Sessions
AD-User-Resolved-Identities	smith@Lfc.lab
AD-User-Resolved-DNs	CN=smith,CN=Users,DC=Lfc,DC=lab
AD-User-DNS-Domain	Lfc.lab
AD-Groups-Names	Lfc.lab/Builtin/Administrators
AD-Groups-Names	Lfc.lab/Builtin/Remote Desktop Users
AD-Groups-Names	Lfc.lab/Builtin/Remote Management Users
AD-Groups-Names	Lfc.lab/Builtin/Users
AD-Groups-Names	Lfc.lab/Users/Denied RODC Password Replication Group
AD-Groups-Names	Lfc.lab/Users/Domain Test
AD-Groups-Names	Lfc.lab/Users/NAD Admins
AD-Groups-Names	Lfc.lab/Users/Domain Users
AD-User-NetBios-Name	Lfc
AD-User-SamAccount-Name	smith
AD-User-Qualified-Name	smith@Lfc.lab
AuthorizationSGTName	Employees
ProviderIpAddress	10.10.10.132
SessionId	cf0d2acd-0d3d-413b-b2fb-6860df3f0d84
provider	Agent
UseCase	PassiveIDAuthZOnly

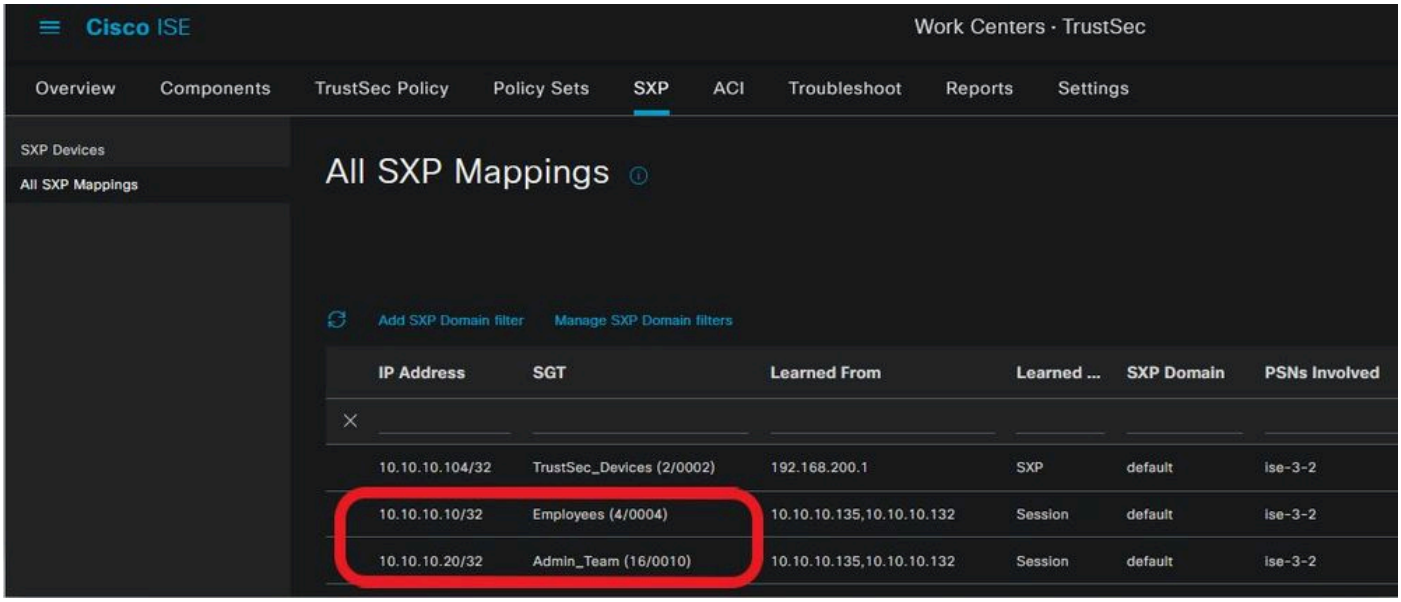
Steps

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 - Lfc\smith
24313	Search for matching accounts at join point - Lfc.lab
24315	Single matching account found in domain - Lfc.lab
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - Lfc.lab
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 Agent
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

A detailed report for another user (Domain Admins). As shown here, a different SGT is assigned per the configured authorization policy.



Verify SGT/IP Mapping Table in ISE. Navigate to **Work Centers > TrustSec > All SXP Mappings**.

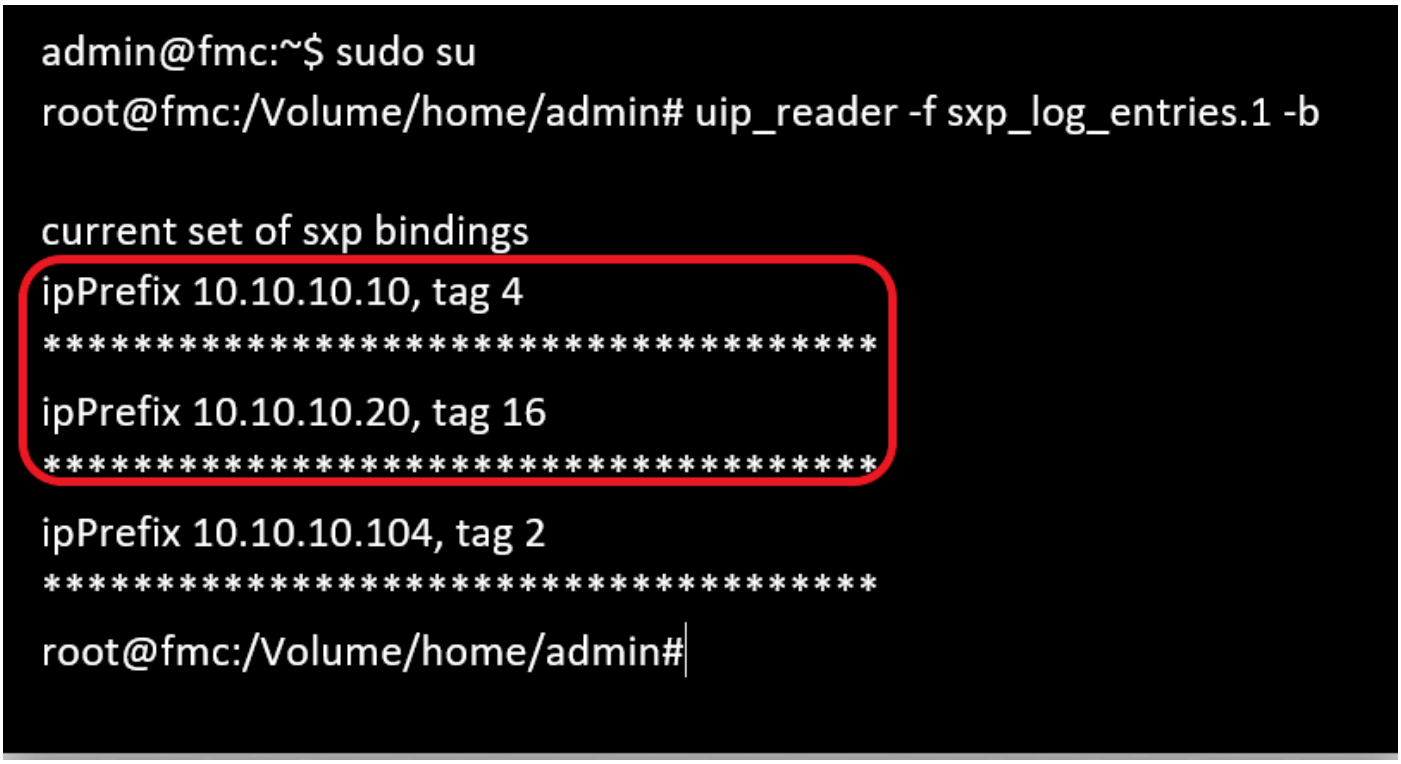


SXP Mappings Table

Note: PassiveID events from an API provider cannot be published to SXP peers. However, the SGT details of these users can be published through pxGrid.

PxGrid Subscriber Verification

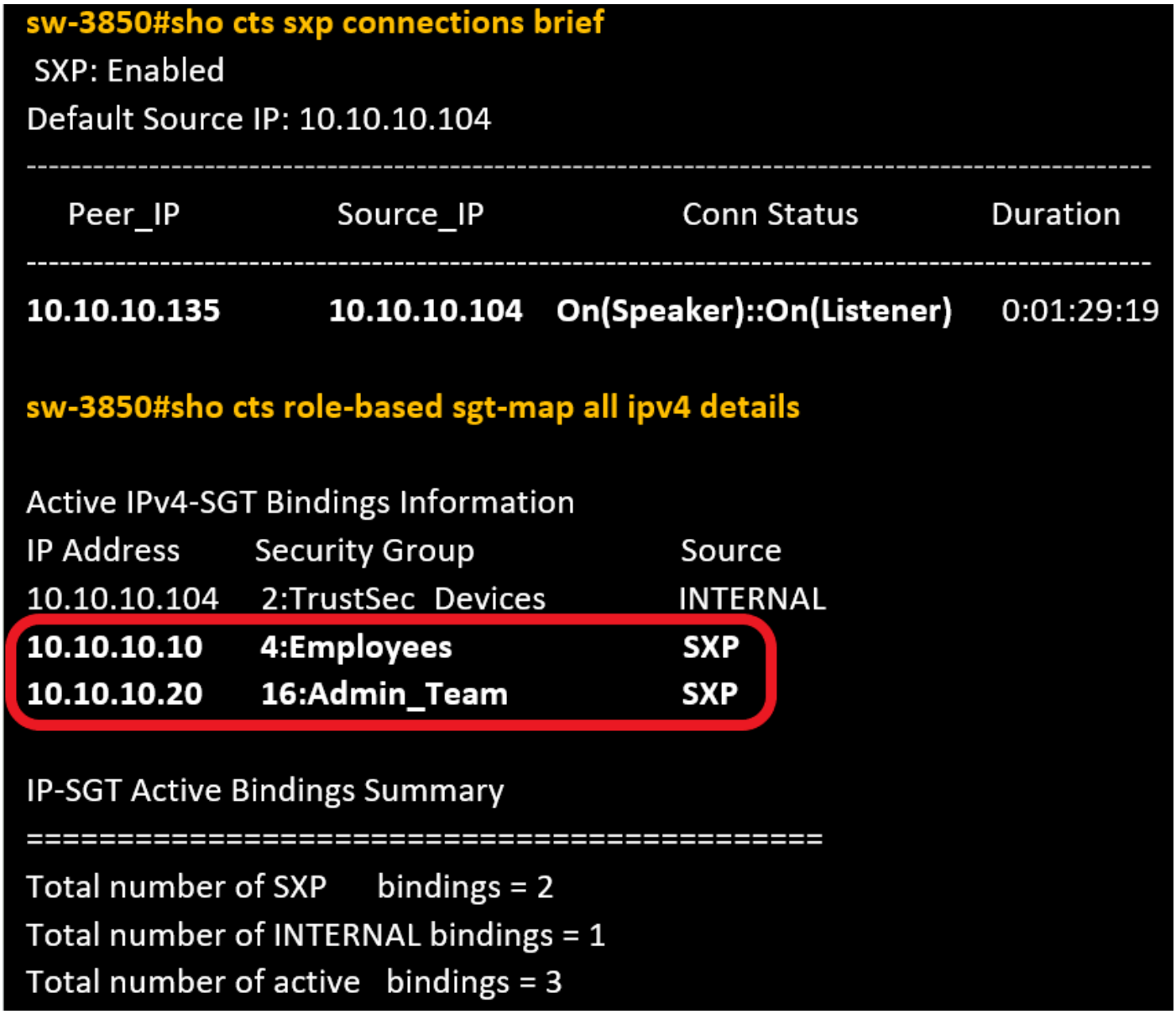
This CLI snippet verifies that the FMC has learned the IP-SGT mappings for the previously mentioned PassiveID sessions from ISE.



FMC CLI Verification

TrustSec SXP Peer Verification

The switch has learned the IP-SGT mappings for PassiveID sessions from ISE, as seen in this CLI excerpt.



Switch CLI verification

Note: The switch configuration for AAA and TrustSec is outside the scope of this document. Please check the Cisco TrustSec Guide for related configs.

Troubleshoot

This section provides information you can use in order to troubleshoot this flow.

Enable Debugs on ISE

Navigate to **Administration** > **System** > **Logging** > **Debug Log Configuration** to set the next components to the specified level.

Node	Component Name	Log Level	Log Filename
PassiveID	passiveid	Trace	passiveid-*.log
PxGrid	pxgrid	Trace	pxgrid-server.log
SXP	sxp	Debug	sxp.log

Note: After troubleshooting, reset the debug settings by selecting the **relevant node** and clicking **Reset to Default**.

Logs Snippets

1. ISE receives login events from the provider:

Passiveid-*.log file:

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- **Received login event.** Identity Mapping.probe = Agent , dc-host = /10.10.10.132 , Identity Mapping.server = ise-3-2 , event-operation-type = ADD ,

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- **Validating incoming loging event...**

2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Building login event to be published to session directory.
2022-09-06 20:28:31,309 DEBUG [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- **retrieving user's additional information from Active Directory.**

2022-09-06 20:28:31,326 DEBUG [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- **Forwarded login event to session directory.** Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainname = Lfc.lab , Identity Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-port-end = -1 , **Identity Mapping.event-user-name = smith** , Identity Mapping.dc-host = /10.10.10.132 , Identity Mapping.agentId = , Identity Mapping.server = ise-3-2 , **Identity Mapping.event-ip-address = 10.10.10.10 ,**

Passiveid-.log file*

2. ISE assigns SGT per the configured authorization policy and publishes IP-SGT mapping for PassiveID users to PxGrid Subscribers and SXP Peers:

sxp.log file:

```
2022-09-06 20:28:31,587 DEBUG [sxpservice-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:27 - Adding session binding tag=4, ip=10.10.10.10, vns=[], vpns=[null] nasIp=10.10.10.132
2022-09-06 20:28:31,587 DEBUG [sxpservice-http-96443] cisco.ise.sxp.rest.SxpGlueRestAPI:23 - session binding created for ip address : 10.10.10.10/32

2022-09-06 20:28:31,613 DEBUG [SxpNotification] cisco.cpm.sxp.engine.SxpEngine:23 - Adding 1 session bindings

2022-09-06 20:28:31,613 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.engine.SxpEngine:42 - Adding session binding RestSxpLocalBinding(tag=4, groupName=null, ipAddress=10.10.10.10/32, nasIp=10.10.10.132, sessionId=cf0d2acd-0d3d-413b-b2fb-6860df3f0d84, peerSequence=null, sxpBindingOpType=ADD, sessionExpiryTimeInMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs [default]
```

sxp.log file

pxgrid-server.log file:

```
2022-09-06 20:28:31,693 TRACE  [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -::::- Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=1859, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via=~ise-fanout-ise-3-2],content-len=1859] content=MESSAGE
content-length:1730
destination:/topic/com.cisco.ise.session
message-id:616
subscription:2
via:~ise-fanout-ise-3-2
{"sessions":[{"timestamp":"2022:09:06T20:28:31.41105:00","state":"AUTHENTICATED","userName":"smith","callingStationId":"10.10.10.10","auditSessionId":"ddda40ec-e557-4457-81db-a36af7b7d4ec",
"ipAddresses":["10.10.10.10"],"nasIpAddress":"10.10.10.132" "ctsSecurityGroup":"Employees" "adNormalizedUser":"smith",
"adUserDomainName":"Lfc.lab","adUserNetBiosName":"Lfc","adUserResolvedIdentities":"smith@Lfc.lab","selectedAuthzProfiles":["PermitAccess"]}],"sequence":13}

2022-09-06 20:28:31,673 TRACE  [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -::::- Send. session=[id=b0df936b-bfab-435f-80e6-aa836aa3b24c,client=~ise-fanout-ise-3-2,server=wss://ise-3-2.Lfc.lab:8910/pxgrid/ise/pubsub] frame=[command=SEND,headers=[content-length=308, destination=/topic/distributed, from=~ise-fanout-ise-3-2, via=~ise-fanout-ise-3-2],content-len=308] content=MESSAGE
content-length:176
destination:/topic/com.cisco.ise.sxp.binding
message-id:612
subscription:2
via:~ise-fanout-ise-3-2
{"operation":"CREATE","binding":{"ipPrefix":"10.10.10.10/32","tag":4, source":"10.10.10.132",
"peerSequence":"10.10.10.135,10.10.10.132","vpn":"default"},"sequence":17}
```

pxgrid-server.log file