将ISE配置为为PassiveID会话分配Trustsec安全组标记

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 流程图
- 配置

验证

- ISE验证
- PxGrid用户验证
- TrustSec SXP对等体验证

故障排除

- 在ISE上启用调试
- 日志片段

简介

本文档介绍如何通过ISE 3.2中的授权策略配置安全组标记(SGT)并将其分配到被动ID会话。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco ISE 3.2
- 被动ID、TrustSec和PxGrid

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ISE 3.2
- FMC 7.0.1
- 运行16.12.1的WS-C3850-24P

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

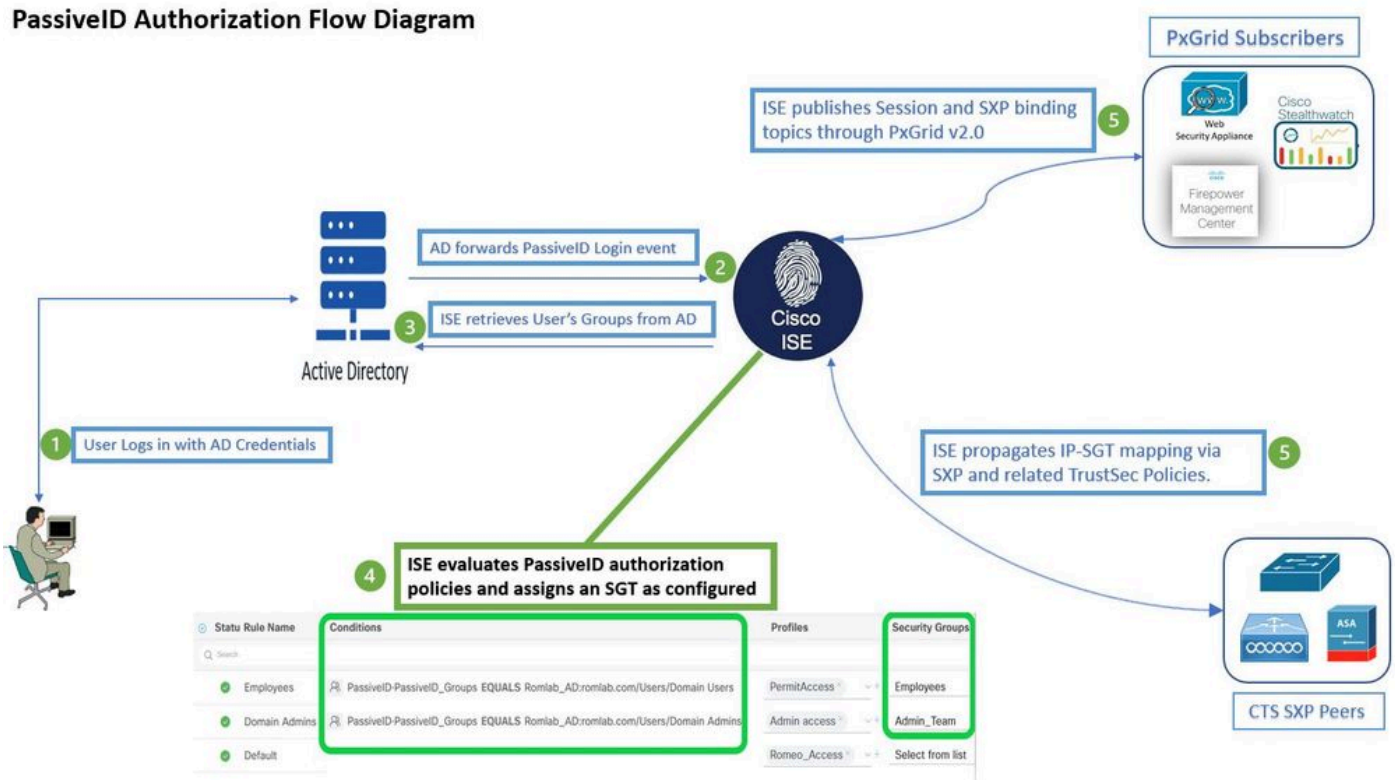
背景信息

思科身份服务引擎(ISE)3.2是支持此功能的最低版本。本文档不包括PassiveID、PxGrid和SXP配置。有关详细信息，请参阅管理员指南。

在ISE 3.1或更早版本中，安全组标记(SGT)只能分配到Radius会话或主动身份验证（例如802.1x和MAB）。使用ISE 3.2，我们可以为PassiveID会话配置授权策略，以便当身份服务引擎(ISE)从提供程序(例如Active Directory域控制器(AD DC)WMI或AD代理)接收用户登录事件时，它根据用户Active Directory(AD)组成员身份向PassiveID会话分配安全组标记(SGT)。PassiveID的IP-SGT映射和AD组详细信息可以通过SGT交换协议(SXP)发布到TrustSec域和/或发布到Cisco Firepower管理中心(FMC)和思科安全网络分析(Stealthwatch)等Platform Exchange Grid(pxGrid)用户。

配置

流程图

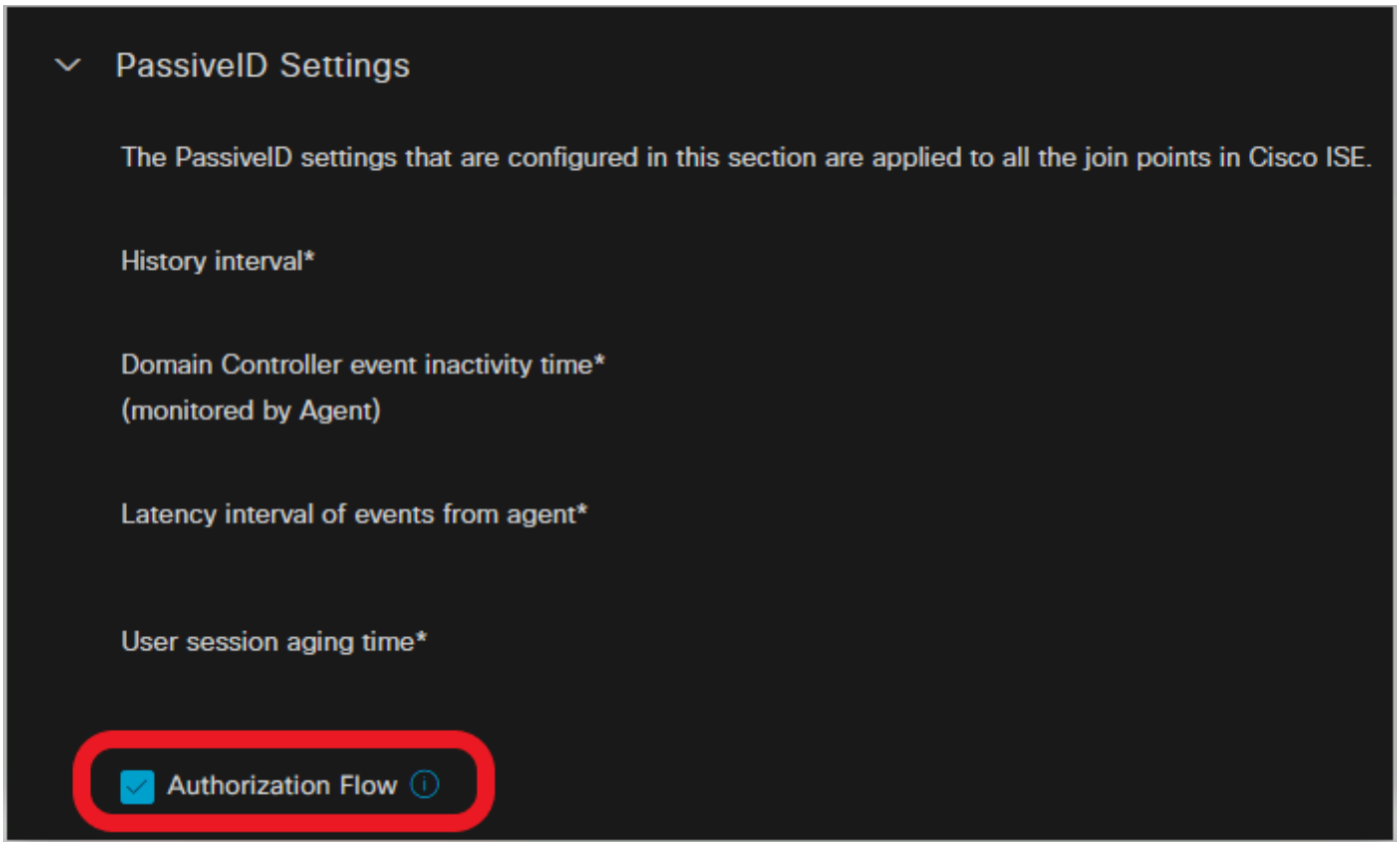


流程图

配置

启用授权流程：

导航到**Active Directory** > **Advanced Settings > PassiveID Settings**并选中复**Authorization Flow**选框，以配置PassiveID登录用户的授权策略。默认情况下该选项处于禁用状态。

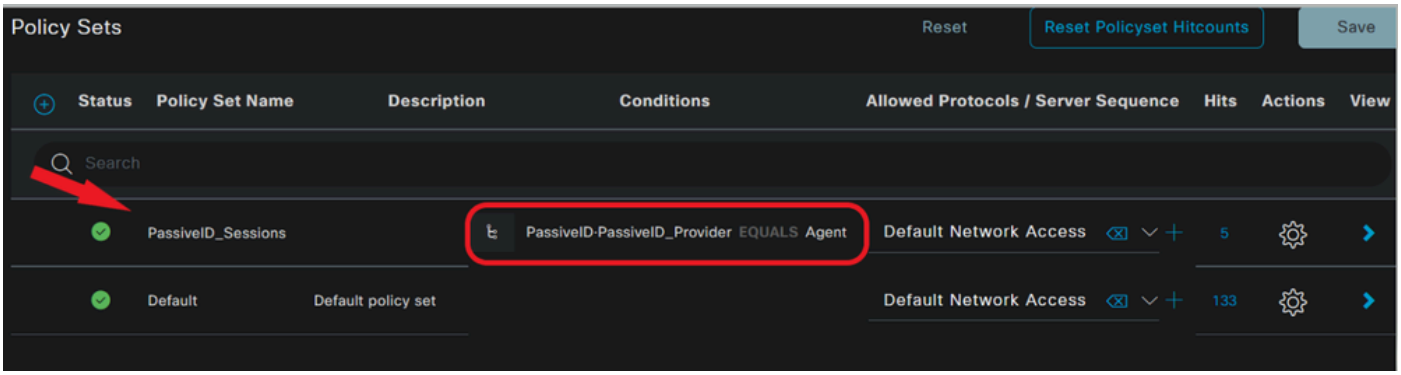


启用授权流

注意：要使用此功能，请确保在部署中运行PassiveID、PxGrid和SXP服务。您可以在以下位置进行验证 **Administration > System > Deployment**.

策略集配置：

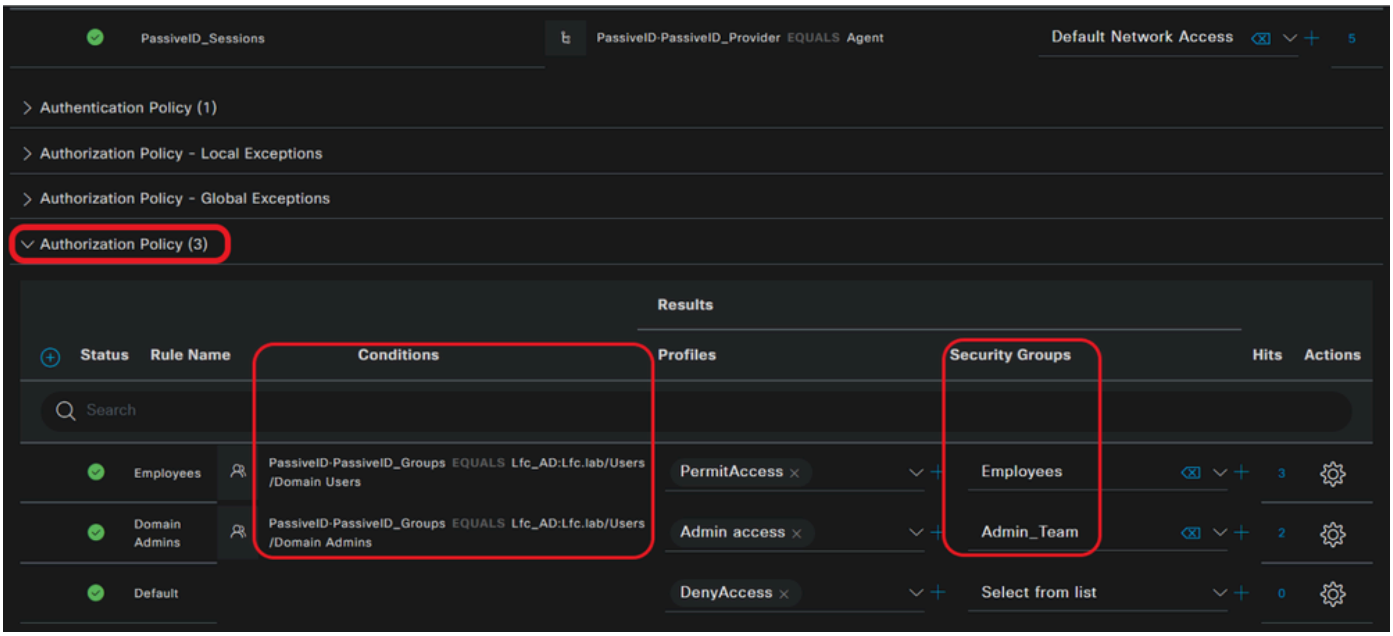
1. 为PassiveID创建单独的Policy集（推荐）。
2. 对于Conditions，请使用属性并**PassiveID·PassiveID_Provider**选择您的提供商类型。



策略集

3. 为步骤1中创建的策略集配置授权规则。

- 为每个规则创建一个条件，并根据AD组、用户名或两者使用PassiveID词典。
- 为每个规则分配Security Group Tag并保存配置。

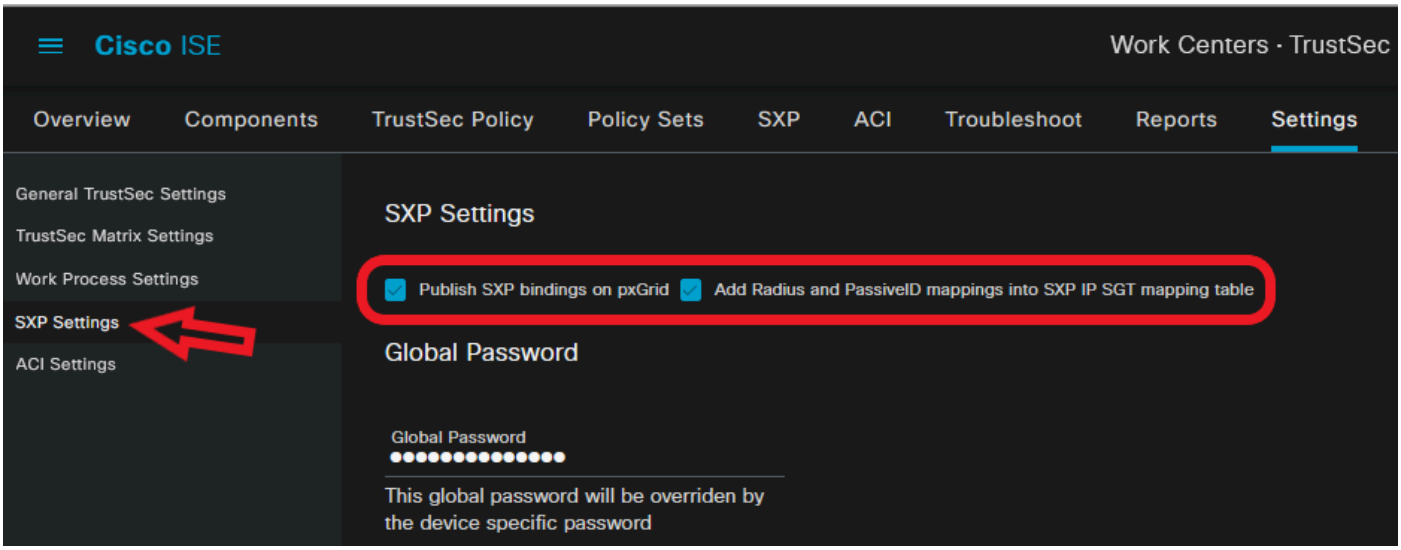


授权策略

注意：身份验证策略不相关，因为它未在此流中使用。

注意：您可以使用或PassiveID_Username, PassiveID_Groups,属PassiveID_Provider性来创建授权规则。

4.导航到**Work Centers > TrustSec > Settings > SXP Settings**以启用**Publish SXP bindings on pxGrid**和**Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table**与PxGrid用户共享PassiveID映射，并将它们包含在ISE上的SXP映射表中。



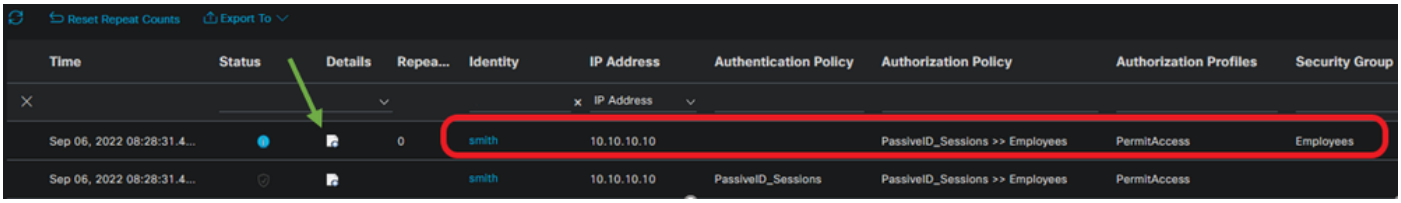
SXP设置

验证

使用本部分可确认配置能否正常运行。

ISE验证

用户登录事件从提供商(例如Active Directory域控制器(AD DC)WMI或AD代理)发送到ISE后，继续检查实时日志。依次导航至 **Operations > Radius > Live Logs**.



Radius实时日志

单击Details列中的放大镜图标，以查看用户的详细报告，在此示例中为smith（域用户），如下所示。

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

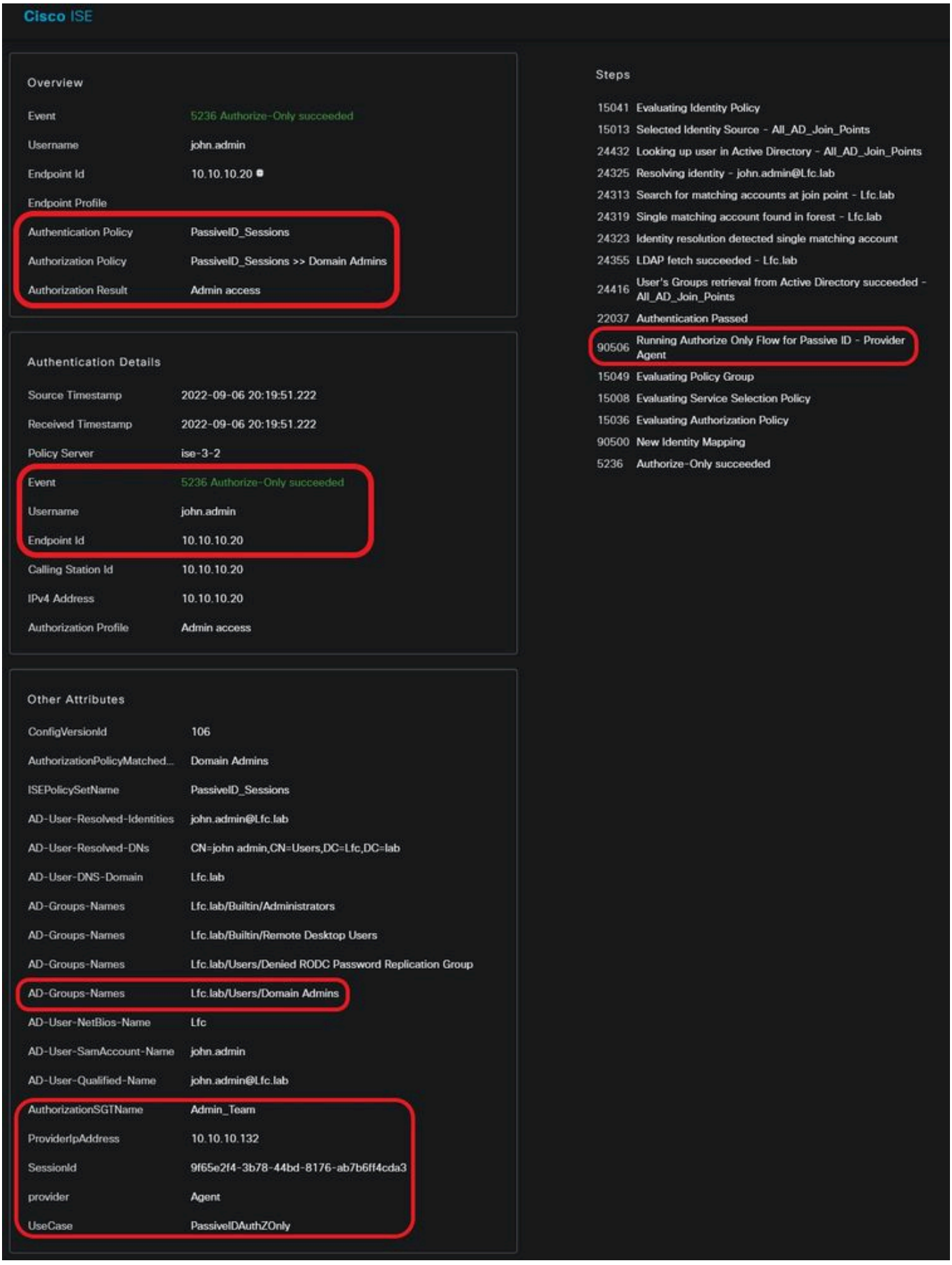
Other Attributes

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

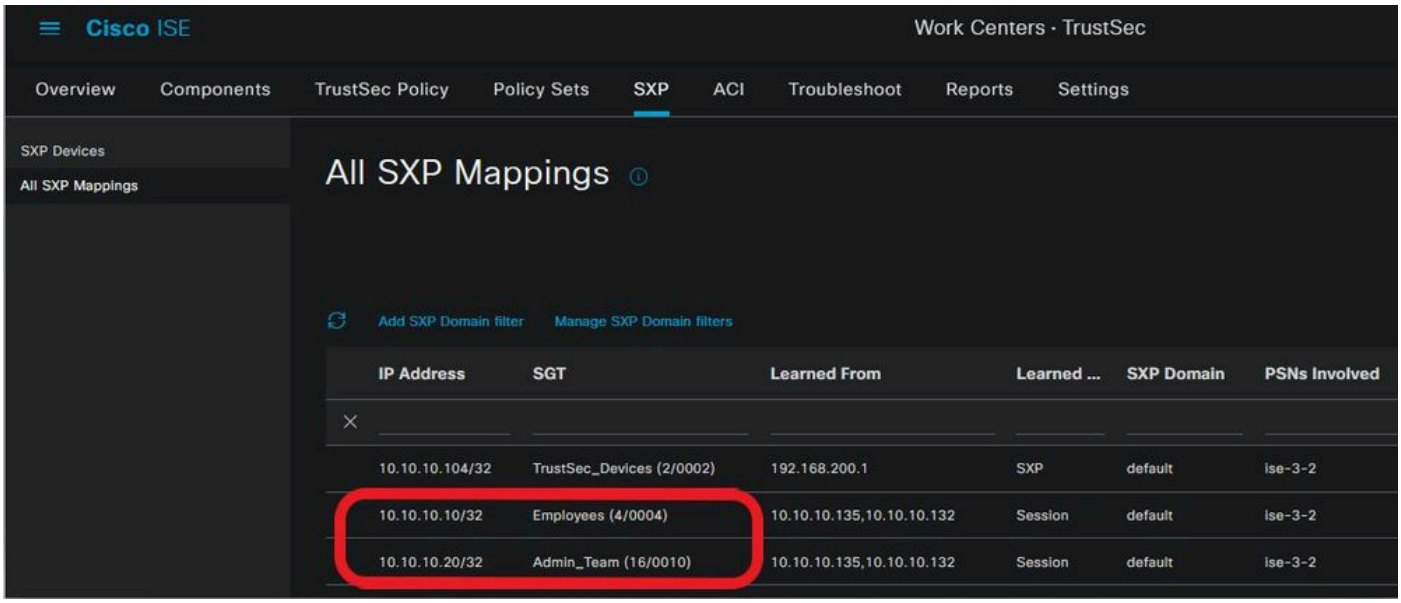
Steps

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

其他用户（域管理员）的详细报告。 如图所示，根据配置的授权策略分配不同的SGT。



验证ISE中的SGT/IP映射表。依次导航至 **Work Centers > TrustSec > All SXP Mappings**.

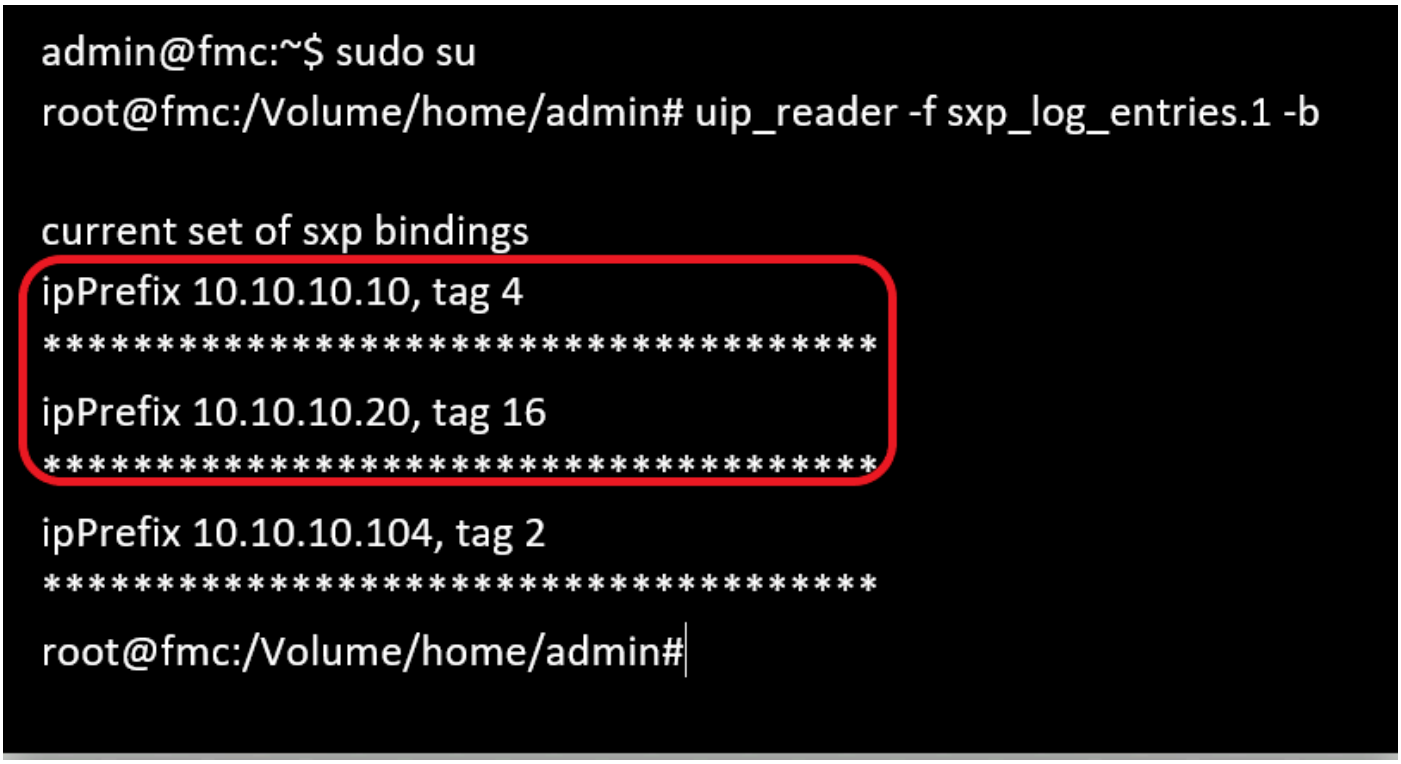


SXP映射表

注意：来自API提供程序的PassiveID事件无法发布到SXP对等体。但是，这些用户的SGT详细信息可以通过pxGrid发布。

PxGrid用户验证

此CLI代码段验证FMC是否已从ISE获取之前提到的PassiveID会话的IP-SGT映射。



FMC CLI验证

TrustSec SXP对等体验证

交换机已从ISE获知PassiveID会话的IP-SGT映射，如此CLI摘录所示。

```
sw-3850#sho cts sxp connections brief
 SXP: Enabled
Default Source IP: 10.10.10.104
------------------------------------------------------------------------------------------
   Peer_IP            Source_IP            Conn Status            Duration
------------------------------------------------------------------------------------------
10.10.10.135         10.10.10.104    On(Speaker)::On(Listener)    0:01:29:19

sw-3850#sho cts role-based sgt-map all ipv4 details

Active IPv4-SGT Bindings Information
IP Address       Security Group                Source
10.10.10.104     2:TrustSec  Devices           INTERNAL
10.10.10.10      4:Employees                   SXP
10.10.10.20      16:Admin_Team                 SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP      bindings = 2
Total number of INTERNAL bindings = 1
Total number of active   bindings = 3
```

交换机CLI验证

注意：AAA和TrustSec的交换机配置不在本文档的讨论范围之内。有关相关配置，请查看Cisco TrustSec指南。

故障排除

本节提供可用于对此流程进行故障排除的信息。

在ISE上启用调试

导航至**Administration > System > Logging > Debug Log Configuration**，将下一个组件设置为指定的级别。

节点	组件名称	日志级别	日志文件名
被动ID	passiveid	跟踪	passiveid-*.log
PxGrid	pxgrid	跟踪	pxgrid-server.log
SXP	sxp	调试	sxp.log

注意：在排除故障后，选择相关节点并单击Reset to Default以重置调试调试设置。

日志片段

1. ISE从提供商接收登录事件：

Passiveid-*.log文件：

```
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文件

2. ISE根据配置的授权策略分配SGT，并将PassiveID用户的IP-SGT映射发布到PxGrid用户和SXP对等体：

sxp.log文件：

```
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文件

pxgrid-server.log文件：

```
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文件

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。