Configuración de ISE 3.2 para asignar etiquetas de grupos de seguridad a sesiones de PassiveID

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Diagrama de flujo](#)
[Configuraciones](#)
[Verificación](#)
[Verificación de ISE](#)
[Verificación del suscriptor de PxGrid](#)
[Verificación de par SXP TrustSec](#)
[Troubleshoot](#)
[Habilitar depuraciones en ISE](#)
[Fragmentos de registro](#)

Introducción

Este documento describe cómo configurar y asignar etiquetas de grupos de seguridad (SGT) a sesiones de ID pasivas mediante políticas de autorización en ISE 3.2.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ISE 3.2
- Passive ID, TrustSec y PxGrid

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE 3.2
- FMC 7.0.1
- WS-C3850-24P que ejecuta 16.12.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Identity Services Engine (ISE) 3.2 es la versión mínima que admite esta capacidad. Este documento no cubre la configuración de PassiveID, PxGrid y SXP. Para obtener información relacionada, consulte la Guía de administración.

En ISE 3.1 o versiones anteriores, una etiqueta de grupo de seguridad (SGT) solo se puede asignar a una sesión Radius o a una autenticación activa, como 802.1x y MAB. Con ISE 3.2, podemos configurar directivas de autorización para sesiones de PassiveID de modo que cuando Identity Services Engine (ISE) recibe eventos de inicio de sesión de usuario de un proveedor como el agente WMI o el agente AD de los controladores de dominio de Active Directory (AD DC), asigna una etiqueta de grupo de seguridad (SGT) a la sesión de PassiveID en función de la pertenencia al grupo de Active Directory (AD) del usuario. La asignación IP-SGT y los detalles del grupo AD para el ID pasivo se pueden publicar en el dominio TrustSec a través del protocolo de intercambio SGT (SXP) o de suscriptores de Platform Exchange Grid (pxGrid), como Cisco Firepower Management Center (FMC) y Cisco Secure Network Analytics (Stealthwatch).

Configurar

Diagrama de flujo

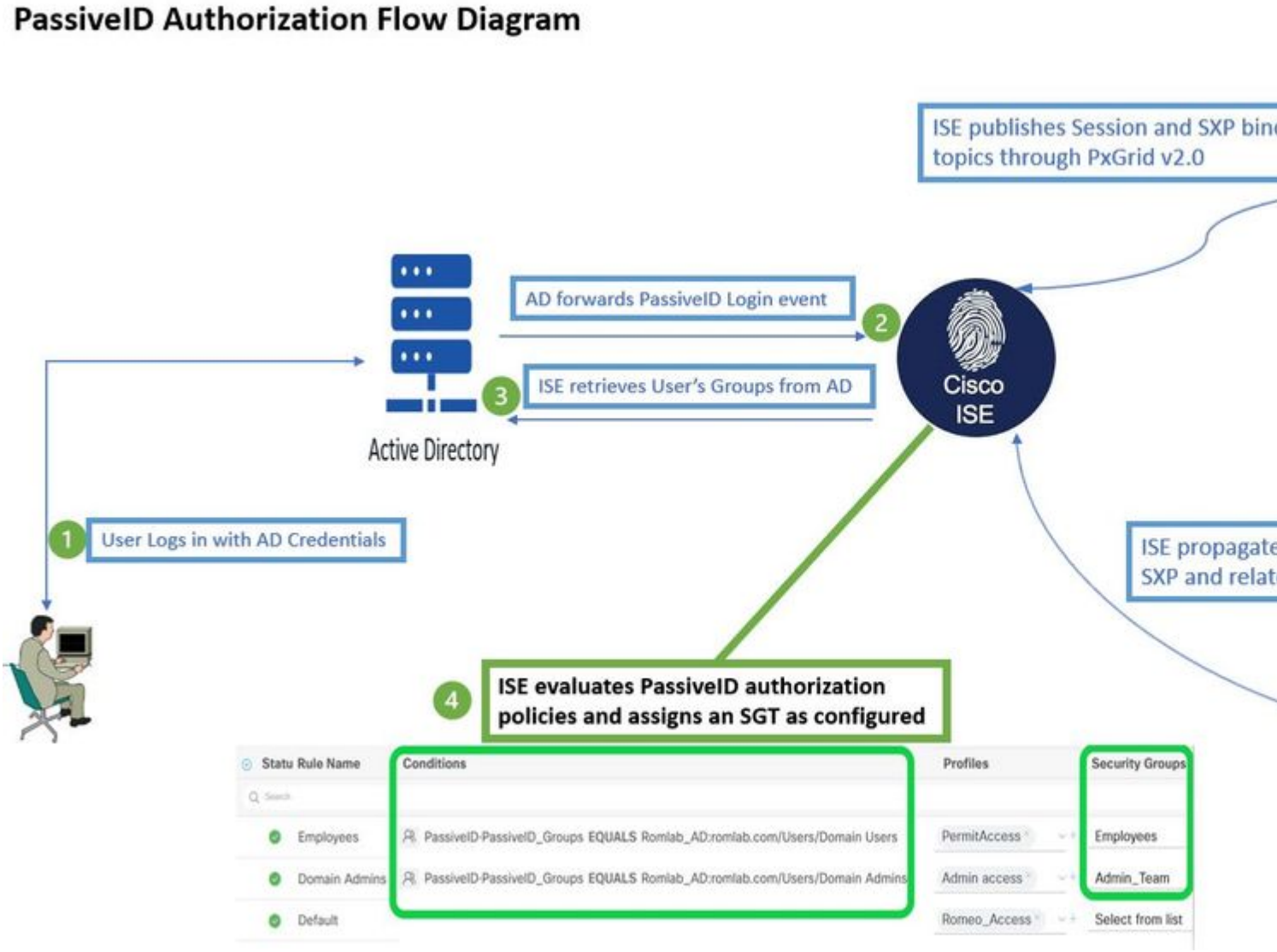
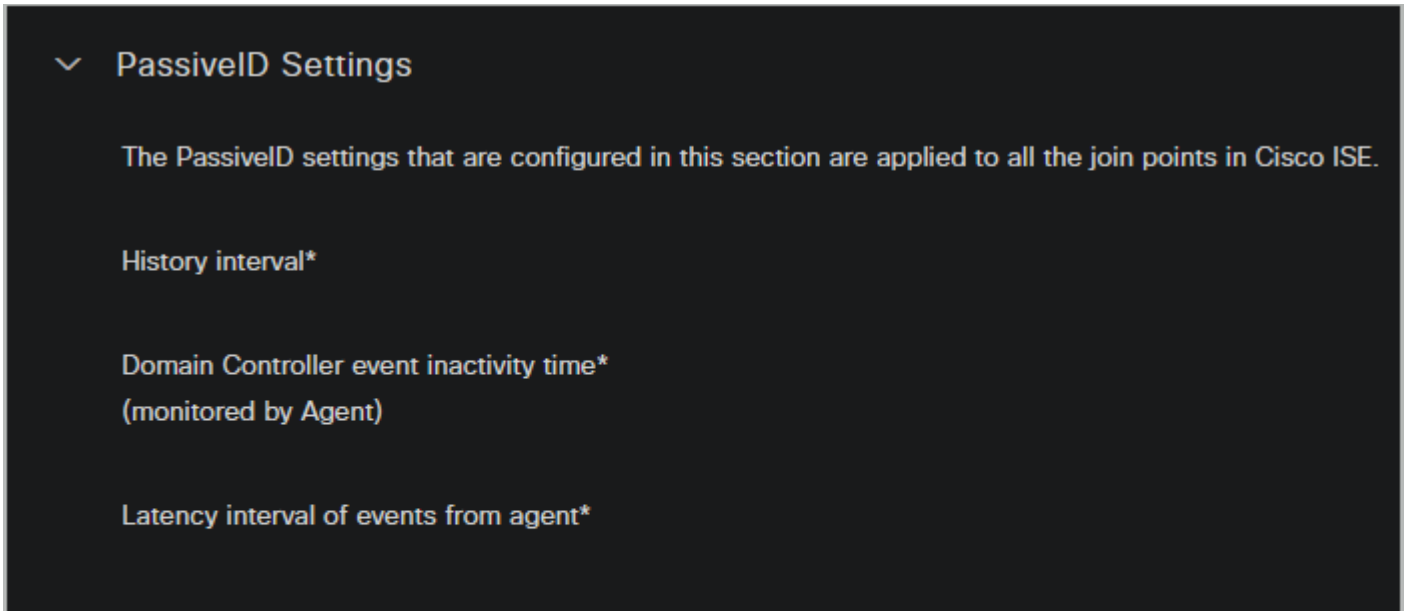


Diagrama de flujo

Configuraciones

Habilitar el flujo de autorización:

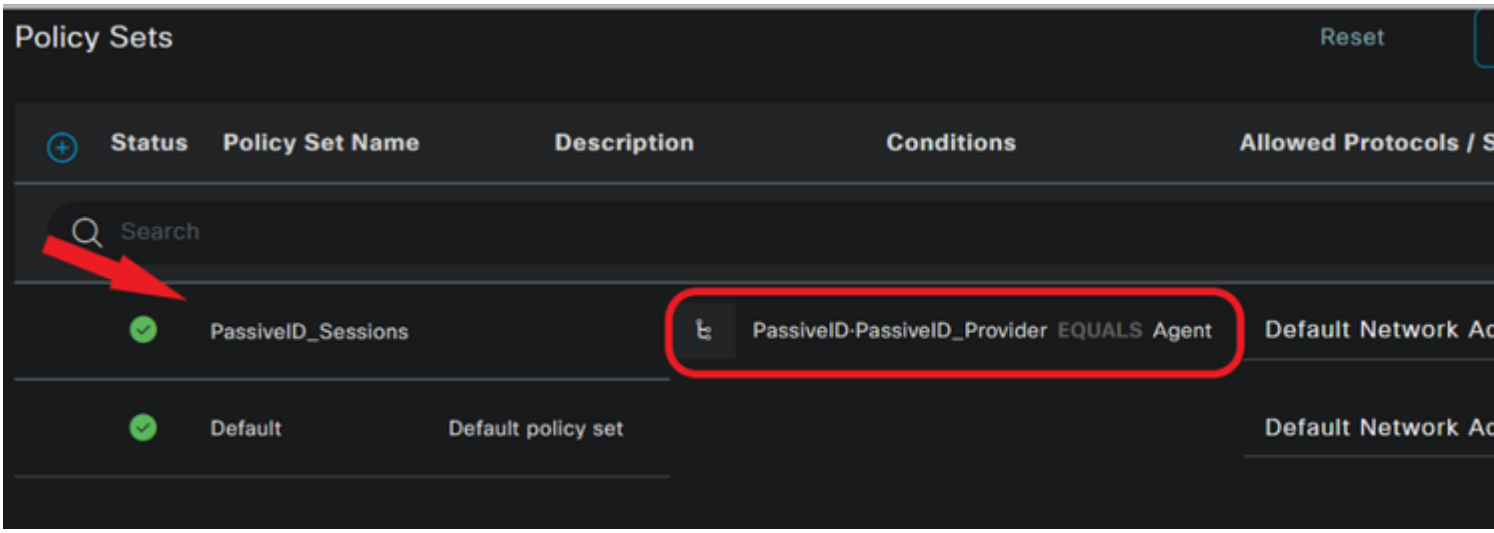
Desplácese hasta **Active Directory >â€¯Advanced Settings > PassiveID Settings** y compruebe la **Authorization Flow** para configurar las políticas de autorización para los usuarios de inicio de sesión de PassiveID. Esta opción está desactivada de forma predeterminada.



: Para que esta función funcione, asegúrese de ejecutar los servicios PassiveID, PxGrid y SXP en la implementación. Puede verificar esto en **Administration > System > Deployment** .

Configuración del conjunto de políticas:

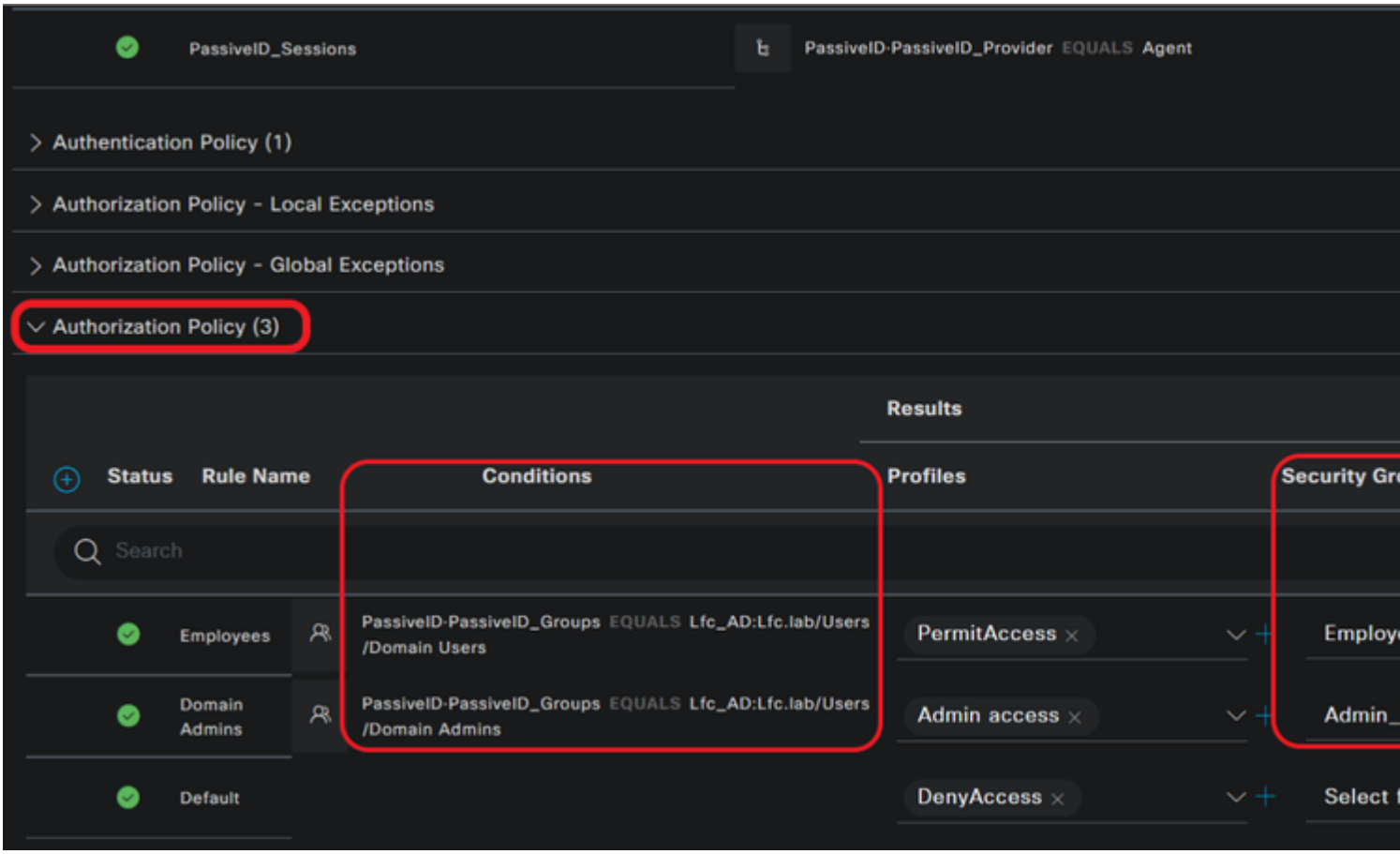
1. Cree un conjunto de políticas independiente para PassiveID (recomendado).
2. Para Condiciones, utilice el atributo **PassiveID·PassiveID_Provider** y seleccione el tipo de proveedor.



Conjuntos de políticas

3. Configure las reglas de autorización para el conjunto de políticas creado en el paso 1.

- Cree una condición para cada regla y utilice el diccionario PassiveID basado en grupos AD, nombres de usuario o Both (Ambos).
- Asigne una etiqueta de grupo de seguridad para cada regla y guarde las configuraciones.



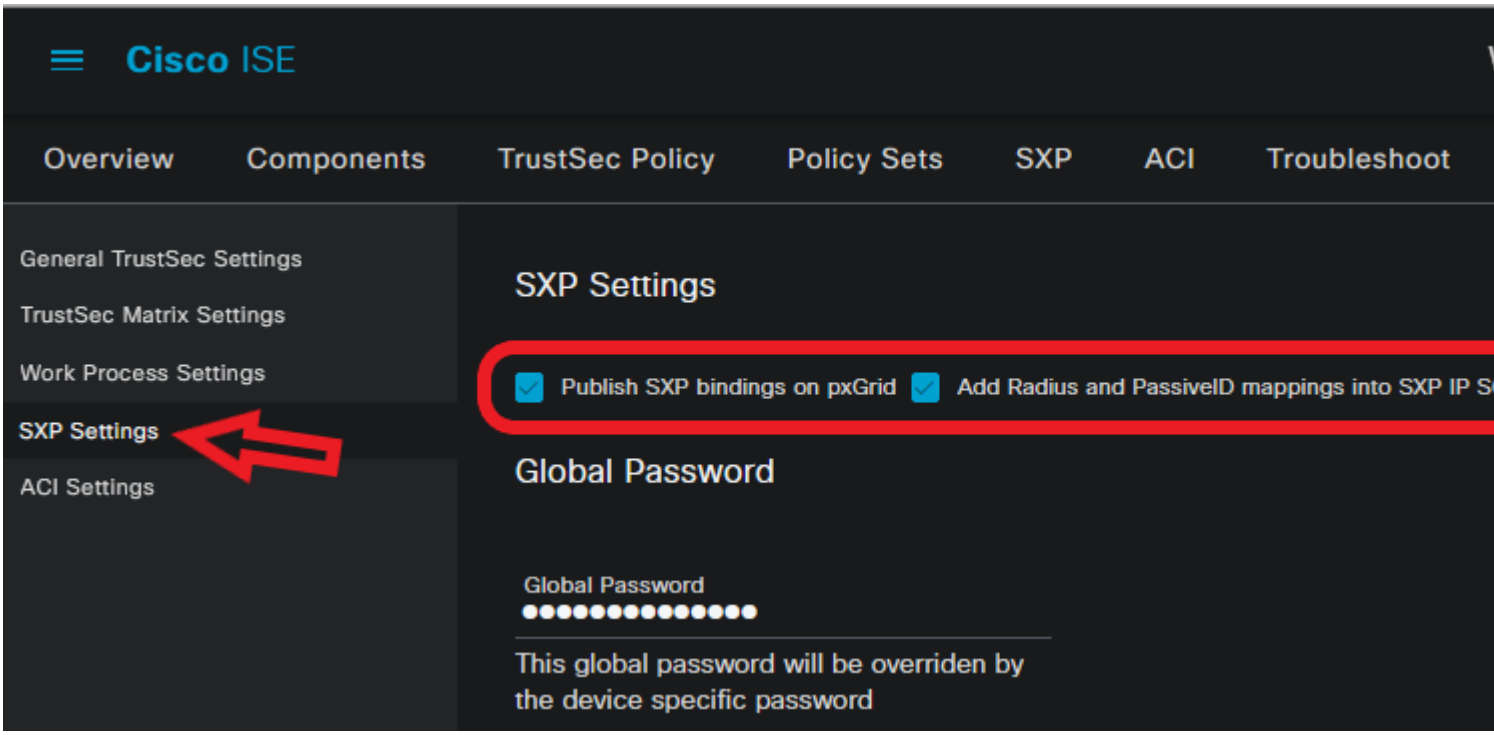
Política de autorización

Nota: la política de autenticación es irrelevante, ya que no se utiliza en este flujo.

Nota: puede utilizar **PassiveID_Username, PassiveID_Groups**,or **PassiveID_Provider** atributos para crear las reglas de autorización.

4. Acceda a **Work Centers > TrustSec > Settings > SXP Settings** para habilitar **Publish SXP bindings on pxGrid** y

para compartir asignaciones de PassiveID con suscriptores de PxGrid e incluirlos en la tabla de asignaciones de SXP en ISE.



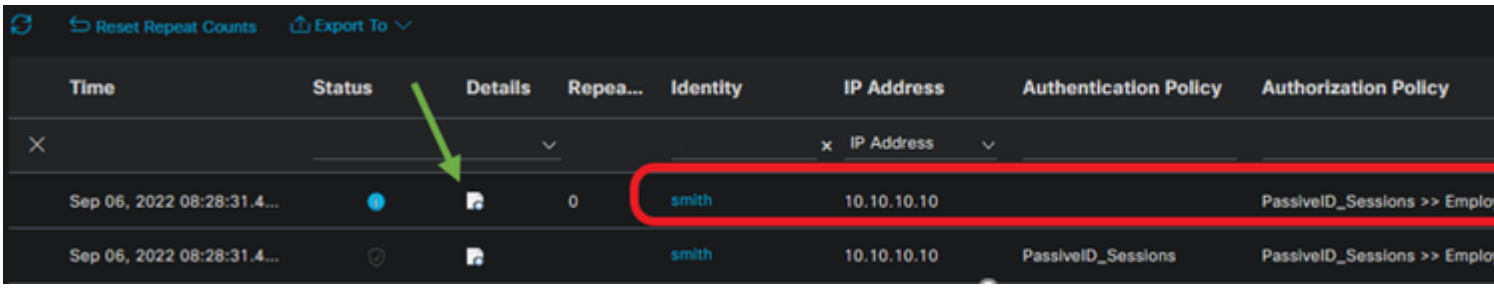
Configuración de SXP

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

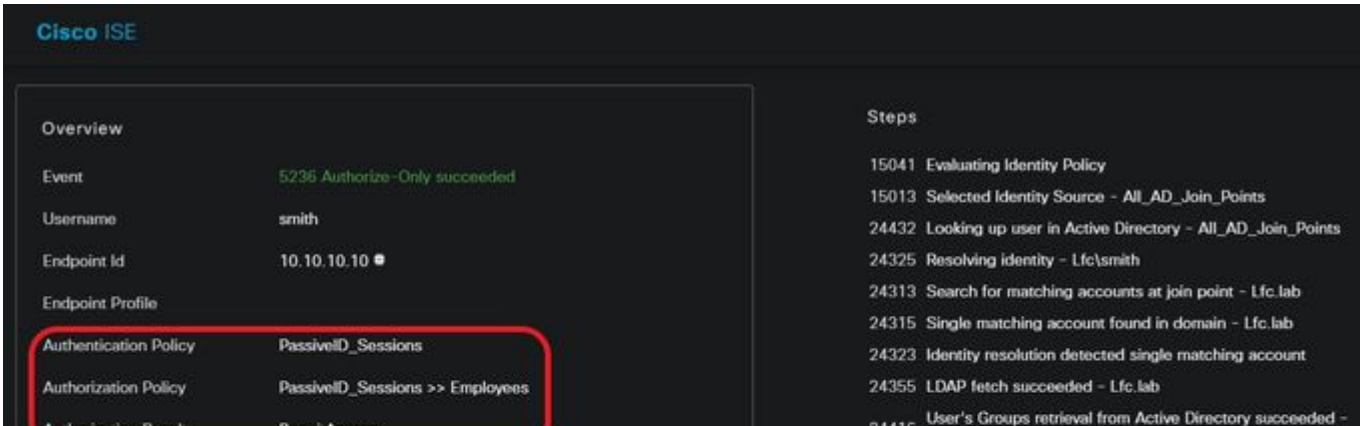
Verificación de ISE

Una vez que los eventos de inicio de sesión del usuario se han enviado a ISE desde un proveedor como el agente de AD o WMI de los controladores de dominio de Active Directory (AD DC), compruebe los registros en directo. Desplácese hasta **Operations > Radius > Live Logs**.



LiveLogs de Radius

Haga clic en el icono de lupa de la columna Detalles para ver un informe detallado de un usuario, en este ejemplo smith (Usuarios de dominio), como se muestra aquí.



: Los eventos PassiveID de un proveedor API no se pueden publicar en los peers SXP. Sin embargo, los detalles de SGT de estos usuarios se pueden publicar a través de pxGrid.

Verificación del suscriptor de PxGrid

Este fragmento de CLI verifica que FMC ha aprendido las asignaciones de IP-SGT para las sesiones PassiveID mencionadas anteriormente de ISE.

```
admin@fmc:~$ sudo su
root@fmc:/Volume/home/admin# uip_reader -f sxp_log_entries.1

current set of sxp bindings
ipPrefix 10.10.10.10, tag 4
**********************************
ipPrefix 10.10.10.20, tag 16
**********************************
ipPrefix 10.10.10.104, tag 2
**********************************
root@fmc:/Volume/home/admin#
```

Verificación CLI de FMC

Verificación de par SXP TrustSec

El switch ha aprendido las asignaciones de IP-SGT para las sesiones PassiveID de ISE, como se muestra en este extracto de CLI.

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

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
```

: La configuración del switch para AAA y TrustSec está fuera del alcance de este documento. Consulte la Guía de Cisco TrustSec para ver las configuraciones relacionadas.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Habilitar depuraciones en ISE

Desplácese hasta **Administration > System > Logging > Debug Log Configuration** para establecer los componentes siguientes en el nivel especificado.

Nodo	Nombre del componente	Nivel de registro	Nombre de archivo de registro
PassiveID	pasivo	Seguimiento	passiveid-*.log
PxGrid	pxgrid	Seguimiento	pxgrid-server.log
SXP	sxp	Depurar	sxp.log

Nota: Cuando haya terminado con la resolución de problemas, recuerde restablecer los debugs y seleccione el nodo relacionado y haga clic en **Reset to Default.**

Fragmentos de registro

1. ISE recibe eventos de inicio de sesión del proveedor:

Archivo Passiveid-*.log:

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

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

2022-09-06 20:28:31,309 DEBUG  [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- Build
published to session directory.
2022-09-06 20:28:31,309 DEBUG  [Grizzly-worker(27)][[]] com.cisco.idc.agent-probe- retrie
information from Active Directory.

2022-09-06 20:28:31,326 DEBUG  [Grizzly-worker(26)][[]] com.cisco.idc.agent-probe- Forw
session directory. Identity Mapping.id-src-first-port = -1 , Identity Mapping.dc-domainnam
Mapping.id-src-port-start = -1 , Identity Mapping.probe = Agent , Identity Mapping.id-src-p
Mapping.event-user-name = smith , Identity Mapping.dc-host = /10.10.10.132 , Identity M
Identity Mapping.server = ise-3-2 , Identity Mapping.event-ip-address = 10.10.10.10 ,
```

Archivo Passiveid-.log*

2. ISE asigna SGT según la política de autorización configurada y publica la asignación IP-SGT para usuarios de PassiveID a suscriptores de PxGrid y peers de SXP:

archivo sxp.log:

```
2022-09-06 20:28:31,587 DEBUG [sxpservice-http-96443] cisco.ise.sxp.rest.SxpGlueRe
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.SxpGlueRe
created for ip address : 10.10.10.10/32

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

2022-09-06 20:28:31,613 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.eng
session binding RestSxpLocalBinding(tag=4, groupName=null, ipAddress=10.10.10.1
sessionId=cf0d2acd-0d3d-413b-b2fb-6860df3f0d84, peerSequence=null, sxpBindingOp
sessionExpiryTimeInMillis=-1, apic=false, routable=true, vns=[DEFAULT_VN]) to VPNs
```

archivo sxp.log

archivo pxgrid-server.log:

```
2022-09-06 20:28:31,693 TRACE  [Grizzly(1)][[]] cpm.pxgrid.ws.client.WsEndpoint -::::- Send, se
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).