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

Contenido

Introducción

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

Prerequisites

- 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.

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

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

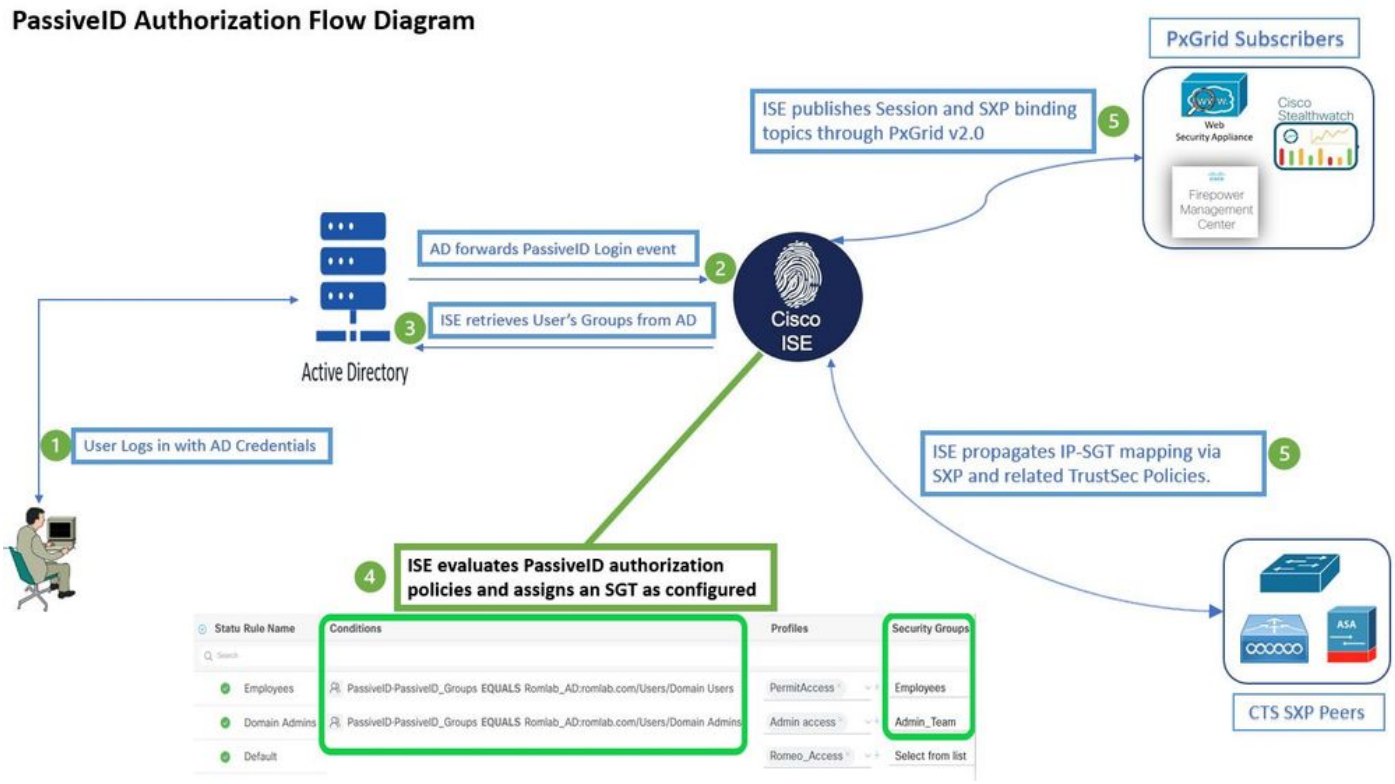
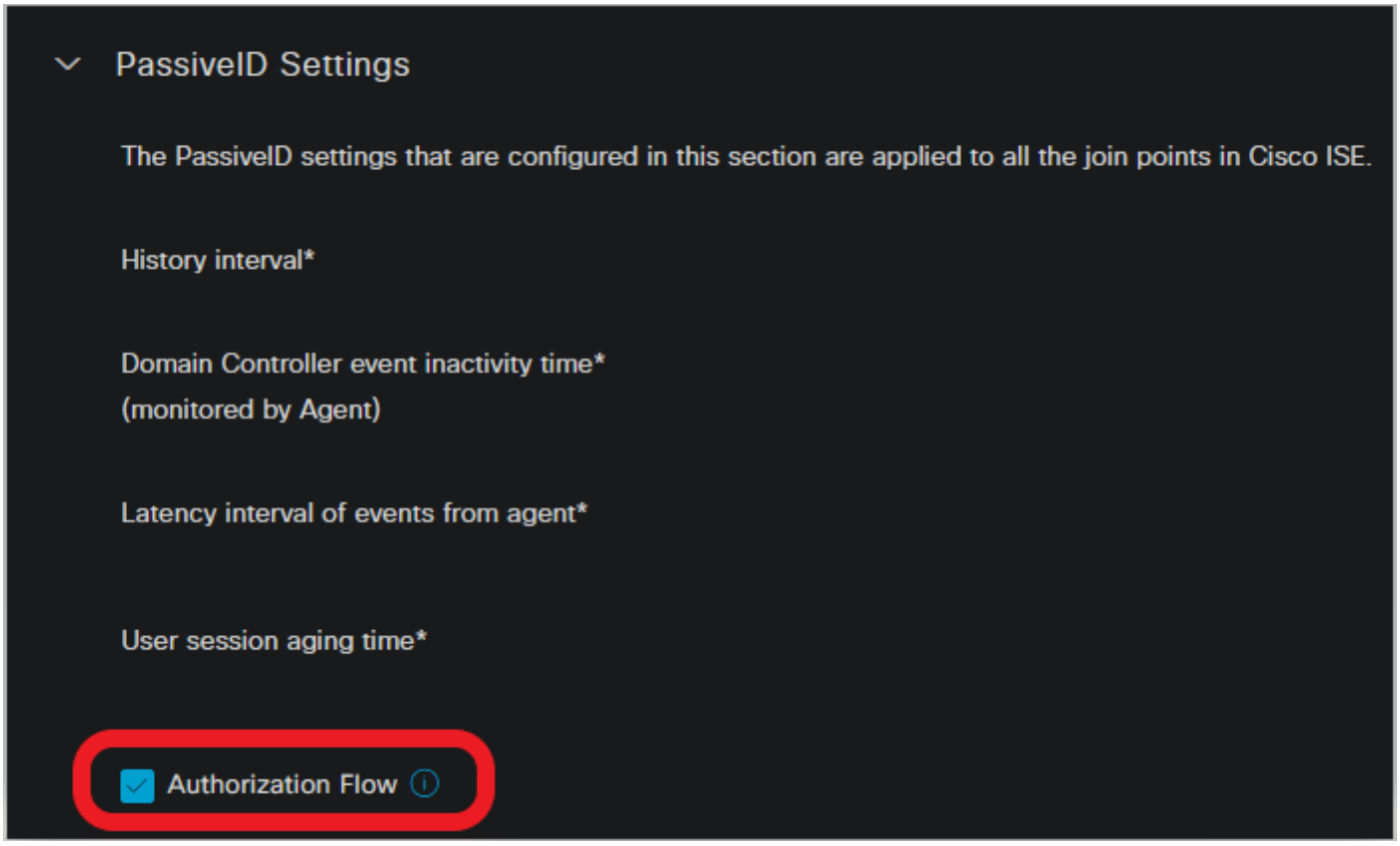


Diagrama de flujo

Configuraciones

Habilitar el flujo de autorización:

Desplácese hasta **Active Directory >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.

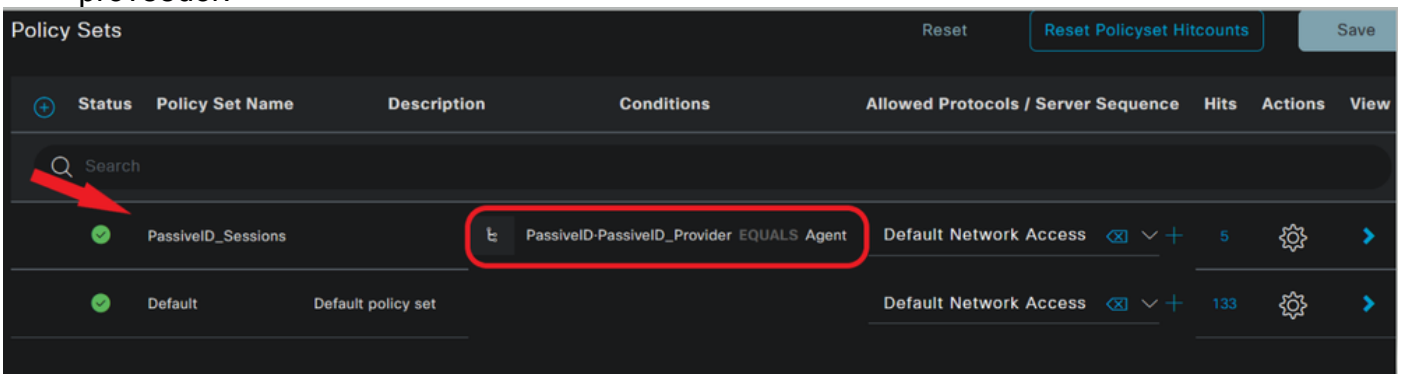


Habilitar el flujo de autorización

> **Nota**: 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.



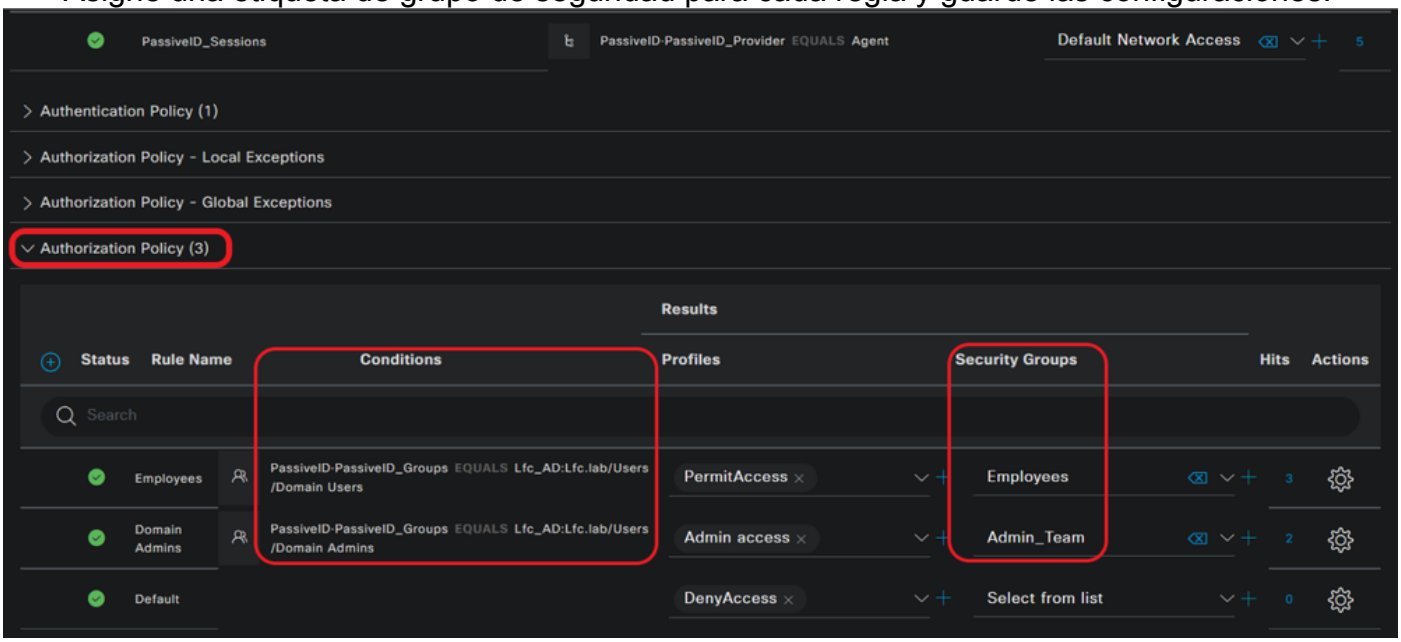
Conjuntos de políticas

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.

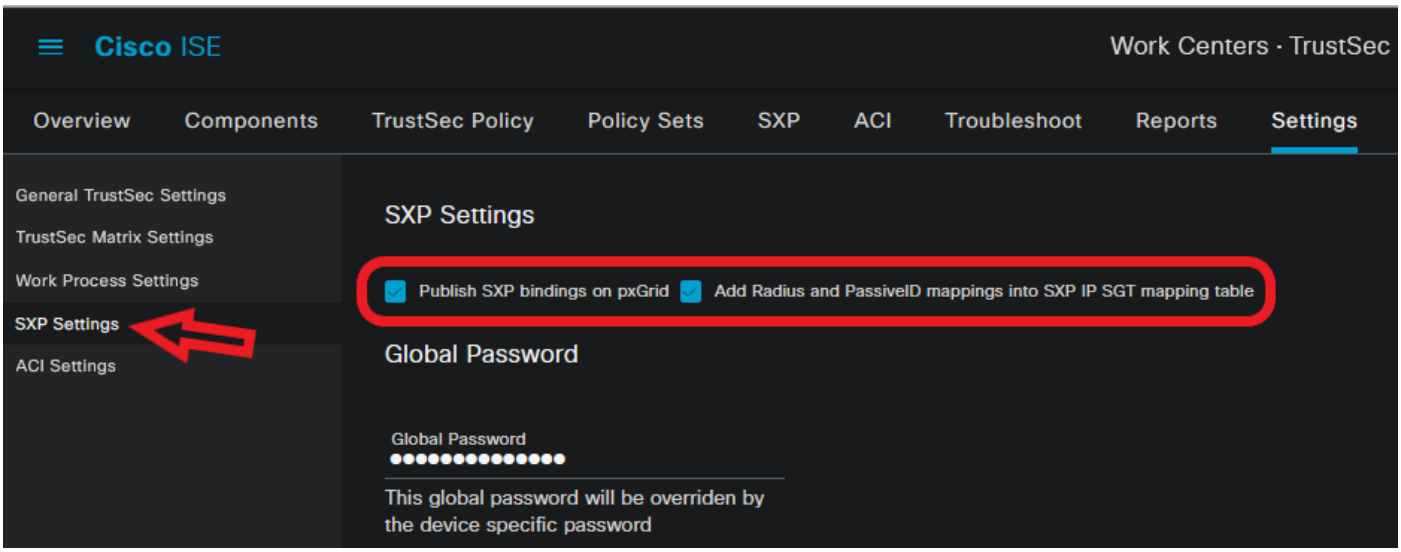


Política de autorización

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 **Add RADIUS and PassiveID Mappings into SXP IP SGT Mapping Table** para compartir asignaciones de PassiveID con suscriptores de PxGrid e incluirlos en la tabla de asignaciones de SXP en ISE.



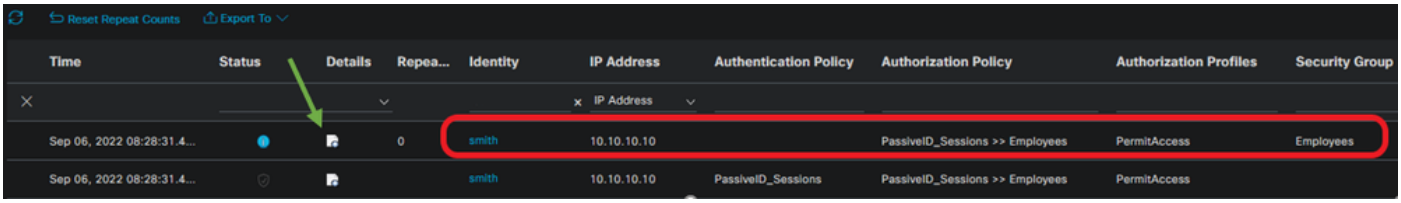
Configuración de SXP

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verificación de ISE

Una vez que los eventos de inicio de sesión de los usuarios se han enviado a ISE desde un proveedor como el agente WMI o el agente AD 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.

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).