Configuración del flujo de autorización para sesiones de ID pasivas en ISE 3.2

Contenido

Introducción

Este documento describe cómo configurar reglas de autorización para eventos de ID pasivo para asignar SGT a las sesiones.

Antecedentes

Los servicios de identidad pasiva (ID pasiva) no autentican a los usuarios directamente, sino que recopilan identidades de usuario y direcciones IP de servidores de autenticación externos como Active Directory (AD), conocidos como proveedores, y, a continuación, comparten esa información con los suscriptores.

ISE 3.2 introduce una nueva función que permite configurar una directiva de autorización para asignar una etiqueta de grupo de seguridad (SGT) a un usuario en función de la pertenencia al grupo de Active Directory.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ISE 3.X
- Integración de ID pasiva con cualquier proveedor
- Administración de Active Directory (AD)
- Segmentación (Trustsec)
- PxGrid (Platform Exchange Grid)

Componentes Utilizados

- Versión 3.2 del software Identity Service Engine (ISE)

- Directorio activo de Microsoft
- Registros del sistema

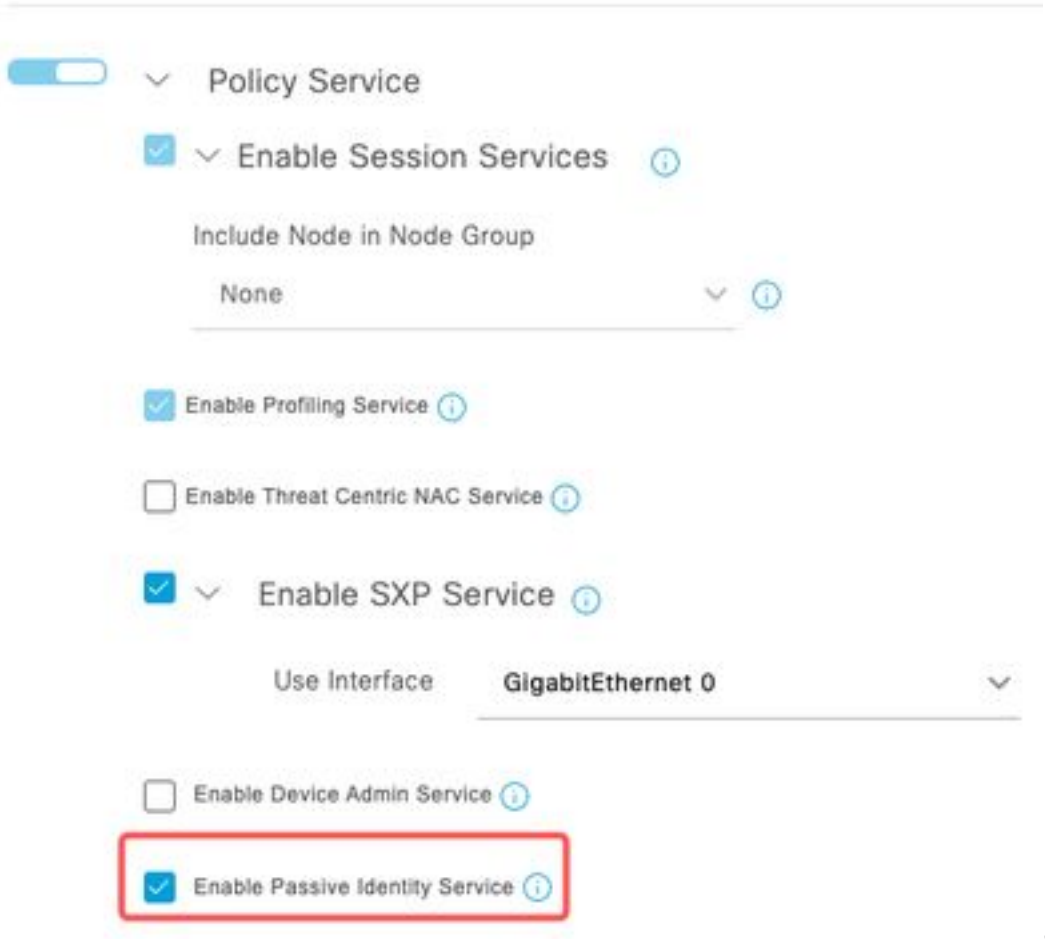
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Configuración

Paso 1. Habilitar servicios ISE.

1. En ISE, navegue hasta Administración > **Implementación**, elija el nodo de ISE y haga clic en **Editar**, habilite **Servicio de políticas** y elija **Habilitar Servicio de identidad pasivo**. Opcionalmente, puede habilitar SXP y PxGrid si las sesiones de identificación pasiva necesitan publicarse a través de cada una. Click Save.

   Advertencia: los detalles de SGT de los usuarios de inicio de sesión con ID pasiva autenticados por el proveedor de API no se pueden publicar en SXP. Sin embargo, los detalles de SGT de estos usuarios se pueden publicar a través de pxGrid y pxGrid Cloud.

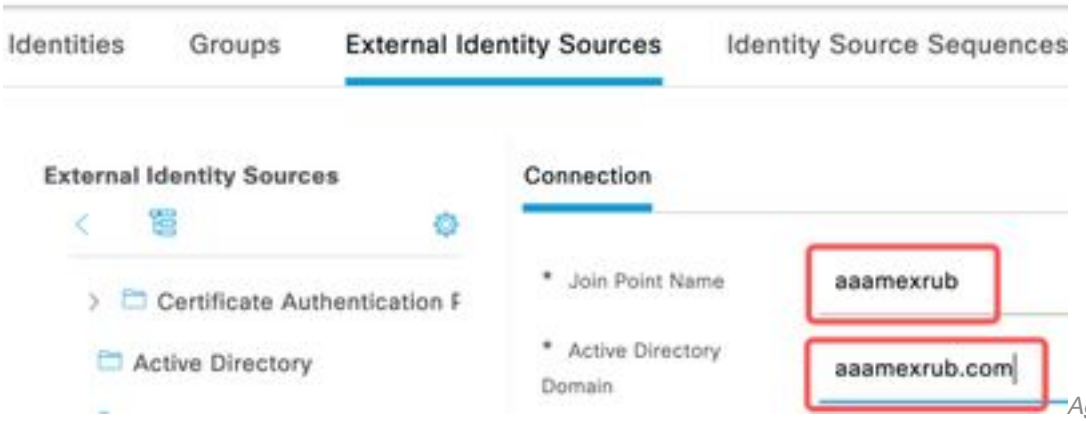


Servicios habilitados

Paso 2. Configure Active Directory.

1. Navegue hasta Administración > **Administración de identidades** > **Orígenes de identidades externas** y elija **Active directory** y luego haga clic en el botón Agregar.
2. Ingrese el **Nombre del Punto de Unión** y el **Dominio de Active Directory**. Haga clic en Submit

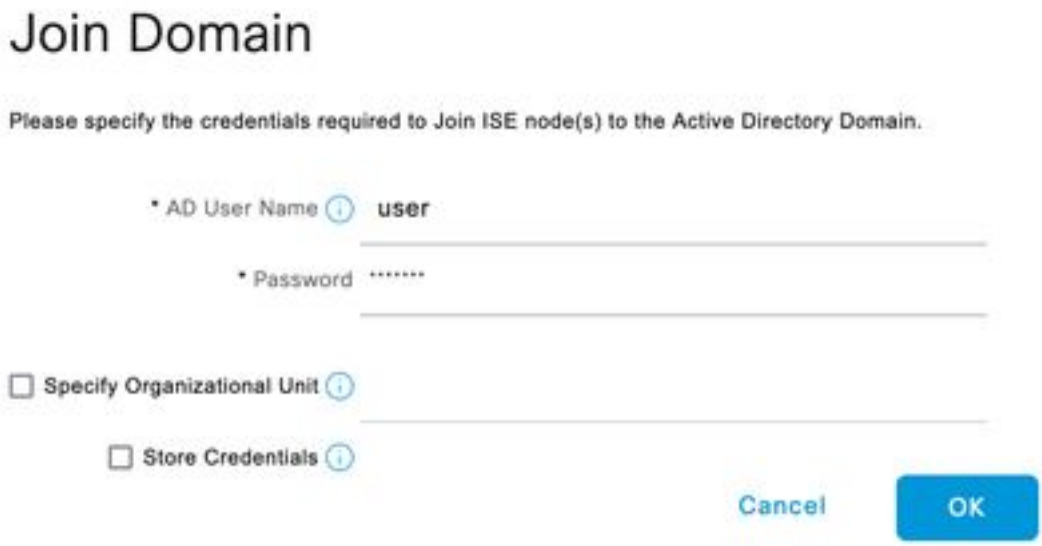
(Enviar).



Agregar Active Directory

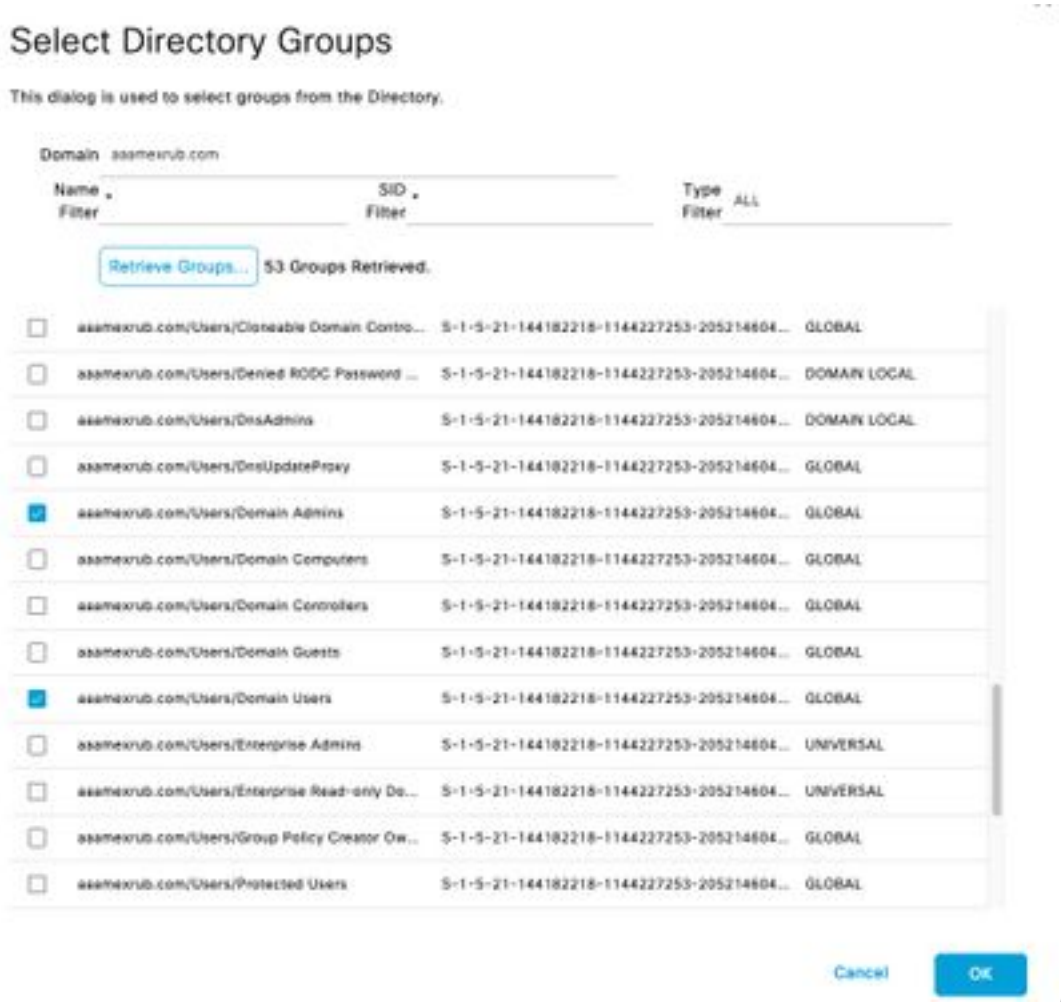
3. Aparece una ventana emergente para unir ISE al AD. Haga clic en Sí Ingrese el nombre de usuario y la contraseña. Click OK.

Continuar para unirse a

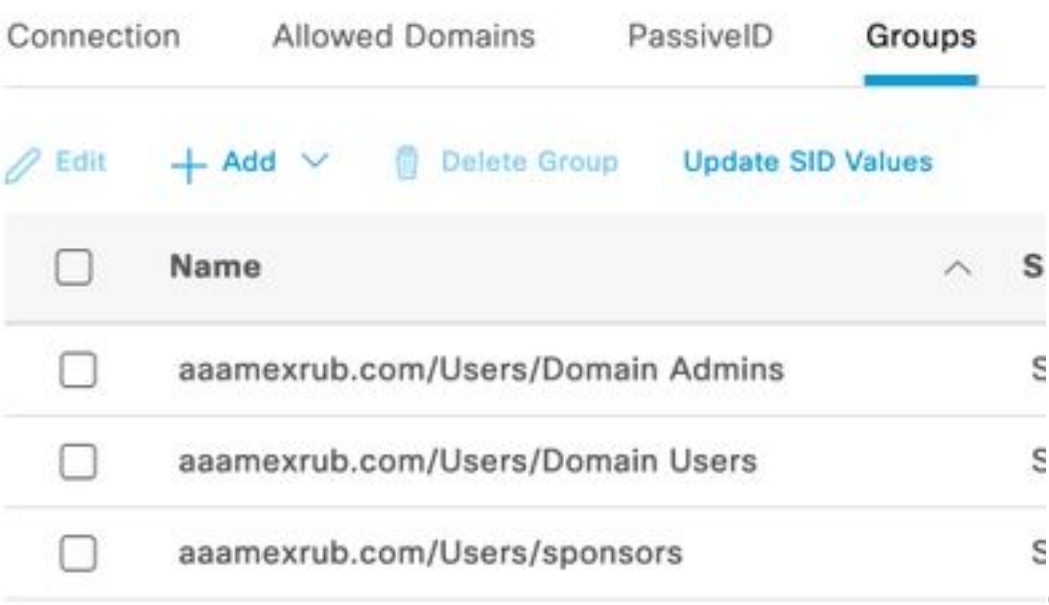


ISE *Unirse a Active Directory*

4. Recuperar grupos AD. Navegue hasta **Grupos**, haga clic en **Agregar**, luego haga clic en **Recuperar Grupos** y elija todos los grupos interesados y haga clic en **Aceptar**.

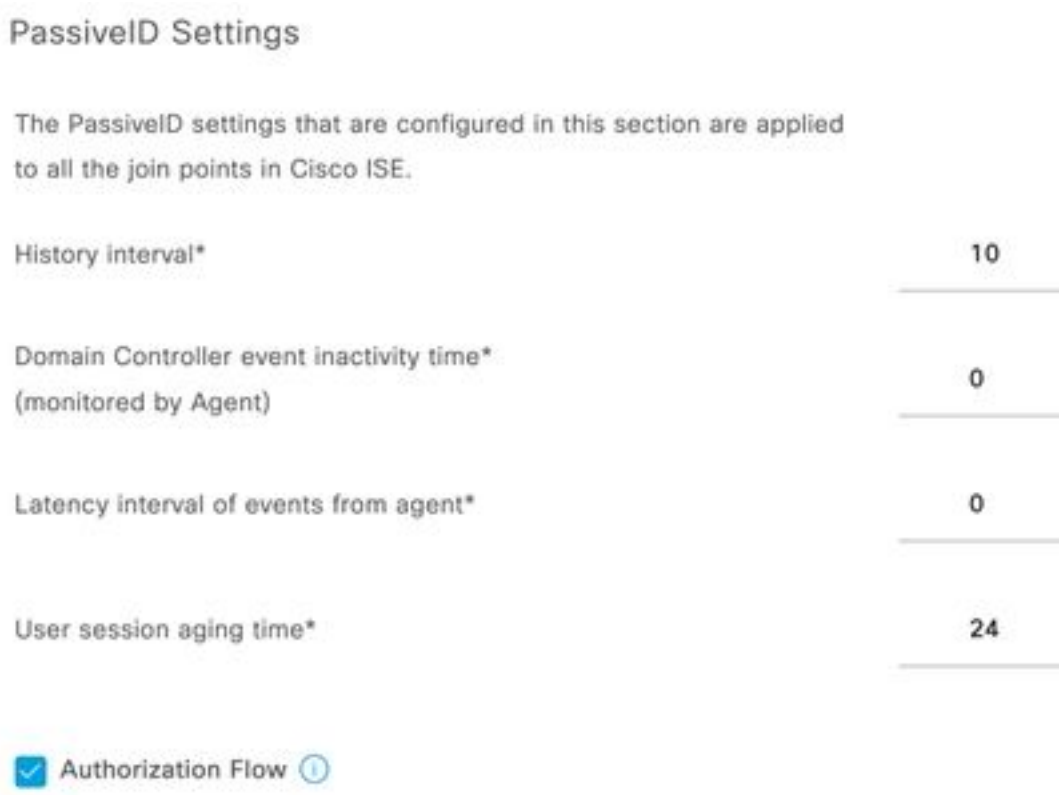


Recuperar grupos AD



Grupos recuperados

5. Active el flujo de autorización. Navegue hasta **Advanced Settings** y en la sección **PassiveID Settings** marque la casilla de verificación **Authorization Flow**. Click Save.

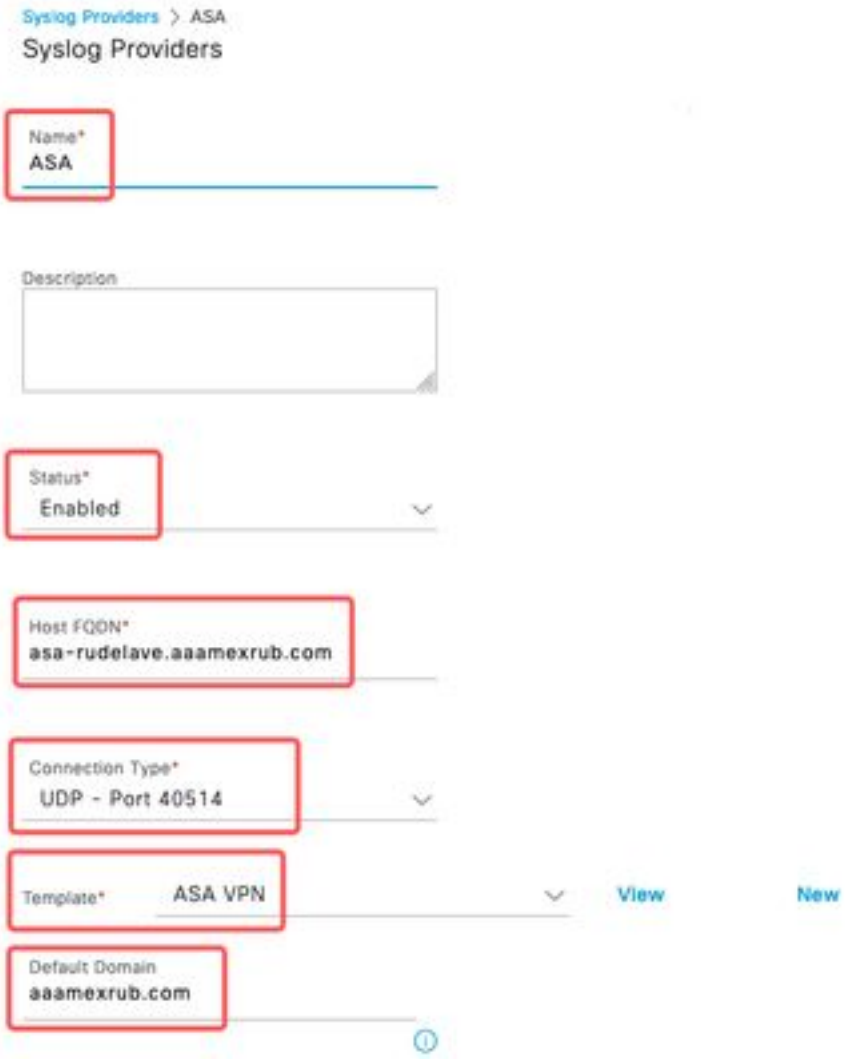


Habilitar flujo de autorización

Paso 3. Configure el proveedor de Syslog.

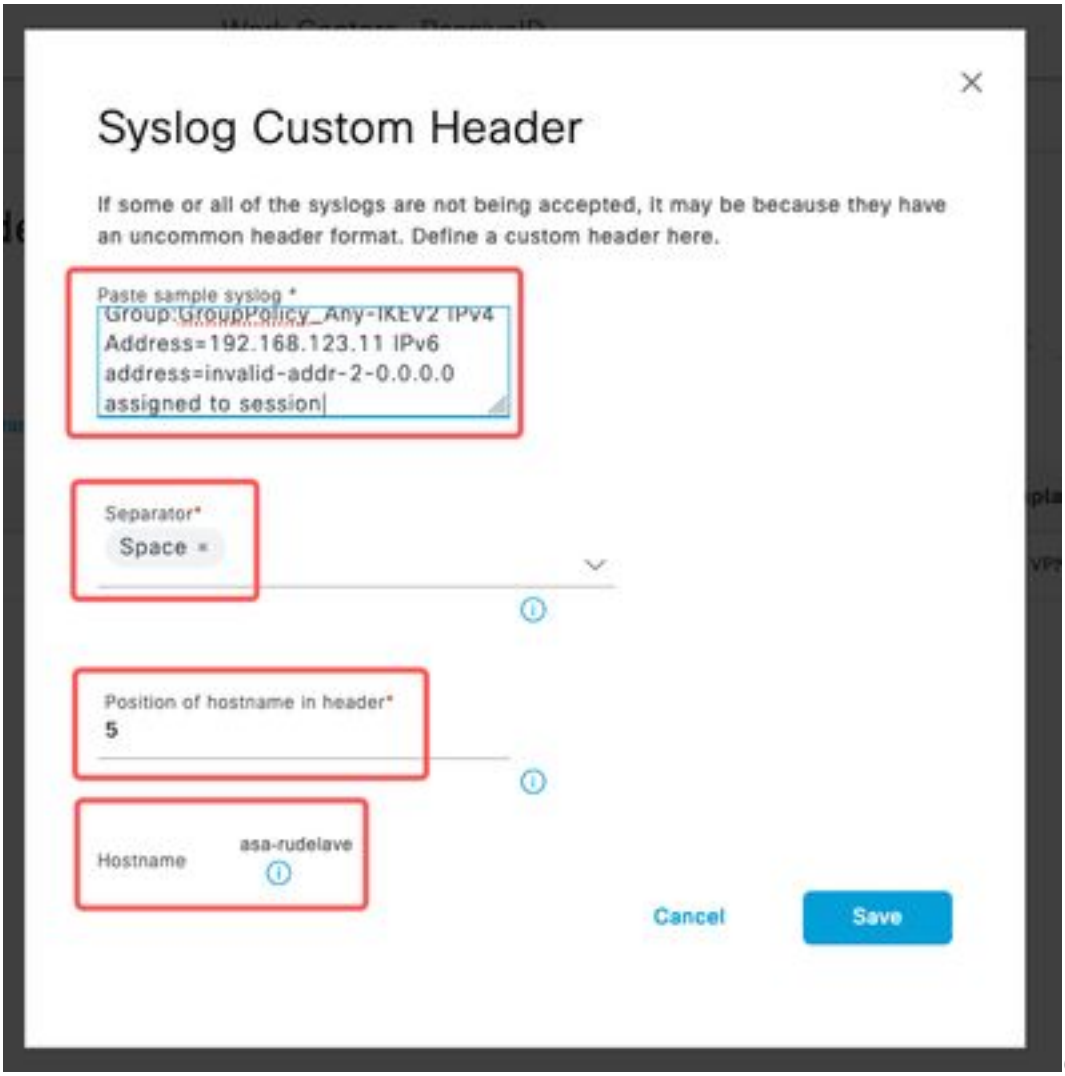
1. Navegue hasta Centros de trabajo > **PassiveID** > **Proveedores**, elija **Proveedores de Syslog**, haga clic en Agregar y complete la información. Haga clic en Save (Guardar).

   Precaución: en este caso, ISE recibe el mensaje syslog de una conexión VPN exitosa en un ASA, pero este documento no describe esa configuración.



Configurar el proveedor de Syslog

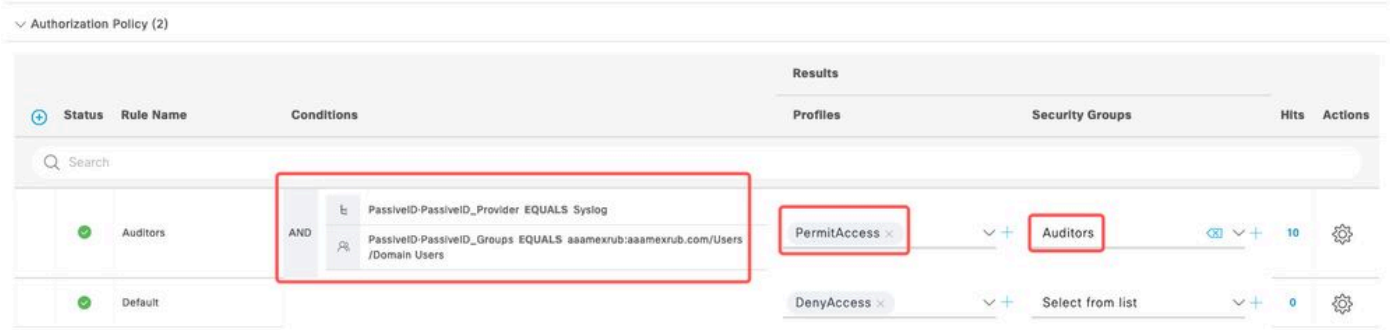
2. Haga clic en **Encabezado personalizado**. Pegue el syslog de ejemplo y utilice un Separador o Tab para encontrar el nombre de host del dispositivo. Si es correcto, aparece el nombre de host. Haga clic en Save (Guardar).



Configurar encabezado personalizado

Paso 4. Configuración de las reglas de autorización

1. Vaya a Política > Conjuntos de políticas. Para este caso, utiliza la política predeterminada. Haga clic en la directiva **Default**. En la **directiva de autorización**, agregue una nueva regla. En las políticas de ID pasiva, ISE cuenta con todos los proveedores. Puede combinar este grupo con un grupo PassiveID. Elija **Permit Access** as Profile, y en **Security Groups** elija la necesidad de SGT.



Configuración de las reglas de autorización

Verificación

Una vez que ISE recibe el registro del sistema, puede comprobar los registros en directo de Radius para ver el flujo de autorización. Navegue hasta **Operaciones > Radius > Registros en**

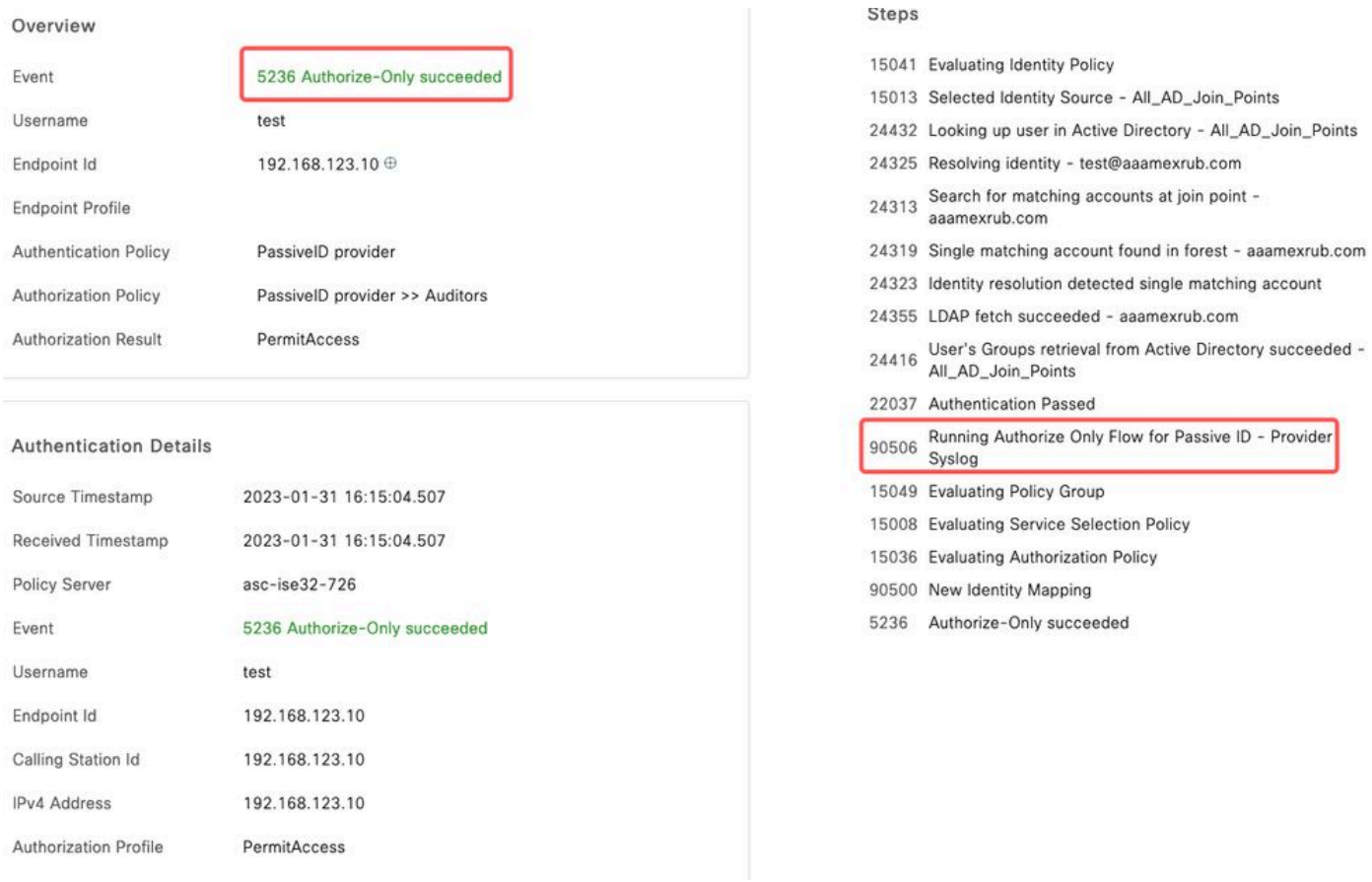
vivo.

En los registros puede ver el evento Authorization. Este contiene el nombre de usuario, la política de autorización y la etiqueta de grupo de seguridad asociados con él.

Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
				Identity	Endpoint ID	Authentication Pol	Authorization Policy	Authorization Profi	Security Gr	IP Address
Jan 31, ...			0	test	192.168.123.10		PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...				test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

Registro en directo de Radius

Para comprobar más detalles, haga clic en el **informe detallado**. Aquí puede ver el flujo de solo autorización que evalúa las políticas para asignar la SGT.



Overview

Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Endpoint Profile	
Authentication Policy	PassiveID provider
Authorization Policy	PassiveID provider >> Auditors
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2023-01-31 16:15:04.507
Received Timestamp	2023-01-31 16:15:04.507
Policy Server	asc-ise32-726
Event	5236 Authorize-Only succeeded
Username	test
Endpoint Id	192.168.123.10
Calling Station Id	192.168.123.10
IPv4 Address	192.168.123.10
Authorization Profile	PermitAccess

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 - test@aaamexrub.com
24313	Search for matching accounts at join point - aaamexrub.com
24319	Single matching account found in forest - aaamexrub.com
24323	Identity resolution detected single matching account
24355	LDAP fetch succeeded - aaamexrub.com
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 Syslog
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15036	Evaluating Authorization Policy
90500	New Identity Mapping
5236	Authorize-Only succeeded

Informe de registro de Radius Live

Troubleshoot

Para este caso, utiliza dos flujos: las sesiones passiveID y el flujo de autorización. Para habilitar los debugs, navegue hasta **Operaciones > Troubleshooting > Debug Wizard > Debug Log Configuration** y elija el nodo ISE.

Para PassiveID, habilite los siguientes componentes al nivel **DEBUG**:

- PassiveID

Para comprobar los registros, basándose en el proveedor de ID pasiva, el archivo que se debe comprobar para este escenario, debe revisar el **archivo** passiveid-syslog.log, para los otros

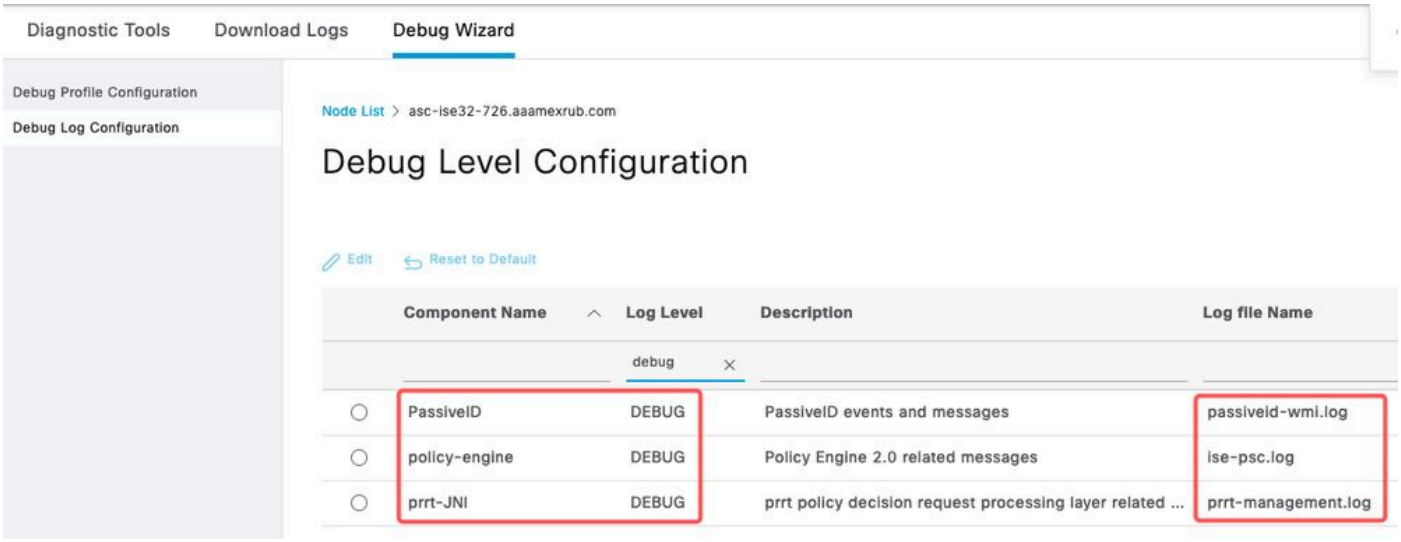
proveedores:

- passiveid-agent.log
- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- passiveid-wmilog

Para el flujo de autorización, habilite los siguientes componentes en el nivel **DEBUG**:

- motor de políticas
- prt-JNI

Ejemplo:



Depuraciones habilitadas

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).