Integre varios clústeres de ISE con un dispositivo web seguro para las políticas basadas en TrustSec

Contenido

Introducción

Este documento describe el procedimiento para enviar información de Security Group Tag (SGT) desde varias implementaciones de ISE a un único Cisco Secure Web Appliance (oficialmente Web Security Appliance WSA) a través de pxGrid para aprovechar las políticas de acceso web basadas en SGT en una implementación de TrustSec.

Antes de la versión 14.5, Secure Web Appliance solo puede integrarse con un solo clúster de ISE para las políticas de identidad basadas en SGT. Con la introducción de esta nueva versión, Secure Web Appliance ahora puede interoperar con información de varios clústeres ISE con un nodo ISE independiente que se agrega entre ellos. Esto aporta grandes ventajas y nos permite exportar datos de usuarios de diferentes clústeres de ISE, así como la libertad de controlar el punto de salida que un usuario puede utilizar sin la necesidad de una integración 1:1.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Identity Services Engine (ISE)
- Dispositivo web seguro
- protocolo RADIUS
- TrustSec
- pxGrid

Componentes Utilizados

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

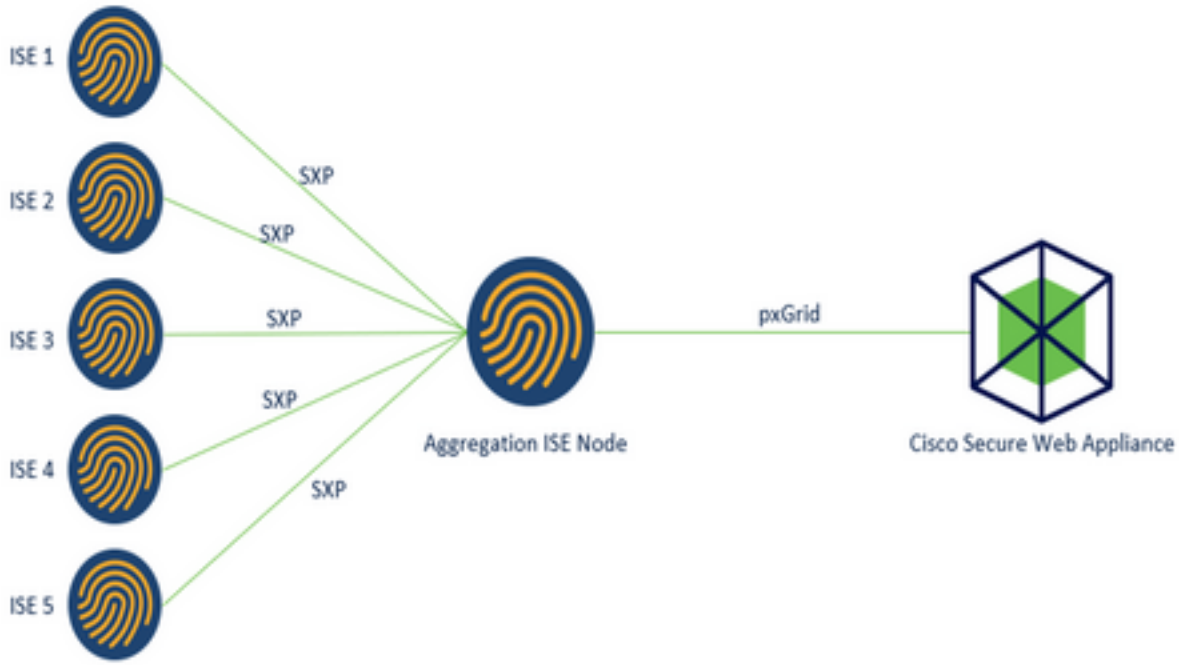
- Dispositivo web seguro 14.5
- ISE versión 3.1 P3

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Limitaciones

1. Todos los clústeres de ISE deben mantener asignaciones uniformes para SGT.
2. El nodo de agregación de ISE debe tener el nombre/número de SGT del resto de los clústeres de ISE.
3. Secure Web Appliance sólo puede identificar la política (acceso/descifrado/enrutamiento) basada en la etiqueta SGT y no en el grupo ni el nombre de usuario .
4. La generación de informes y el seguimiento se basan en SGT.
5. Los parámetros de tamaño existentes de ISE/Secure Web Appliance siguen aplicándose a esta función.

Diagrama de la red



Proceso:

1. Cuando el usuario final se conecta a la red, recibe una SGT basada en las políticas de autorización de ISE.

2. A continuación, los diferentes clústeres de ISE envían esta información SGT en forma de asignaciones SGT-IP al nodo de agregación de ISE a través de SXP.

3. ISE Aggregation Node recibe esta información y la comparte con el único Secure Web Appliance a través de pxGrid.

4. Secure Web Appliance utiliza la información SGT que ha aprendido para proporcionar acceso a los usuarios en función de las políticas de acceso Web.

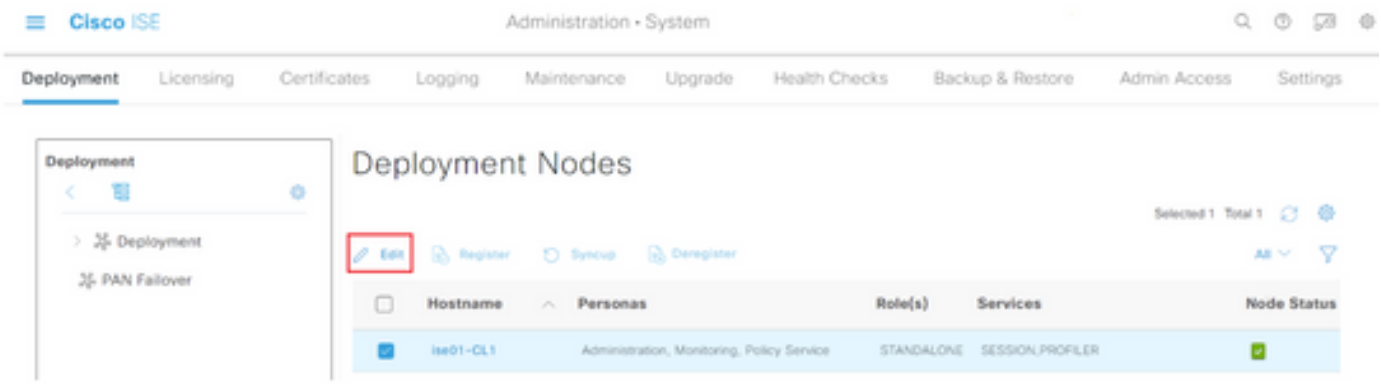
Configurar

Configuración de ISE

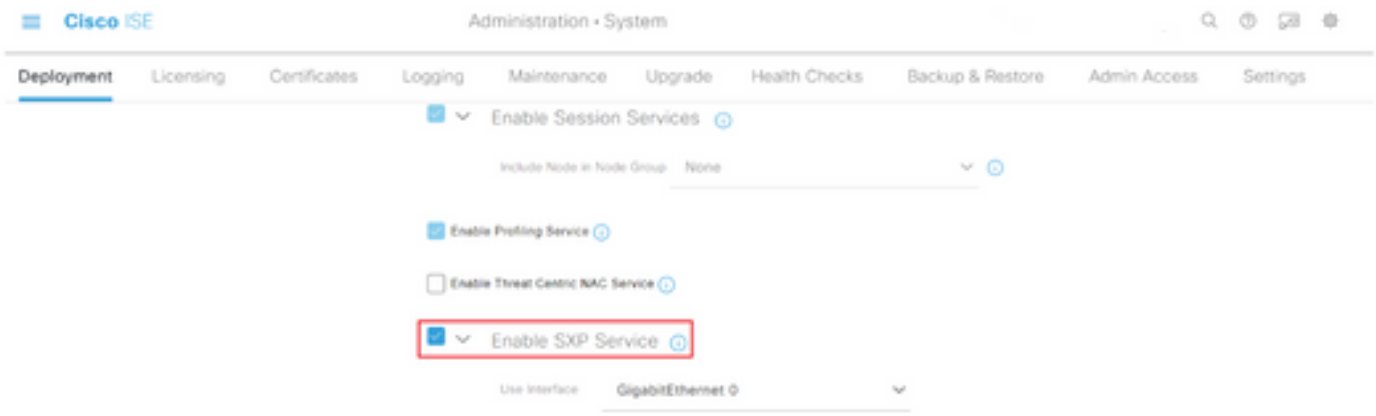
Activar SXP

Paso 1. Seleccione el icono de tres líneas se encuentra en la esquina superior izquierda y seleccione en **Administration > System > Deployment.**

Paso 2. Seleccione el nodo que desea configurar y haga clic en **Editar.**



Paso 3. Para activar SXP, marque la casilla **Enable SXP Service (Activar servicio SXP)**



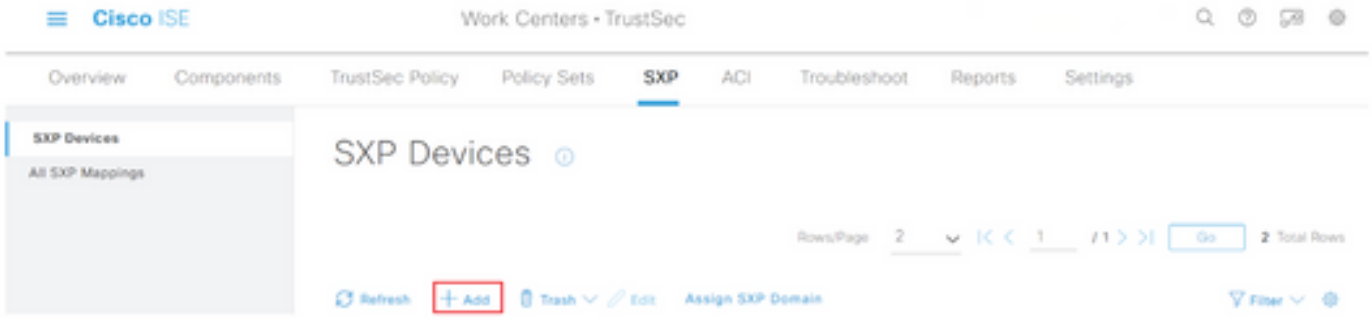
Paso 4. Desplácese hacia abajo y haga clic en **Guardar**

> **Nota:** Repita todos los pasos para el resto de los nodos ISE en cada clúster, el nodo de agregación incluido.

Configure SXP en los nodos del clúster

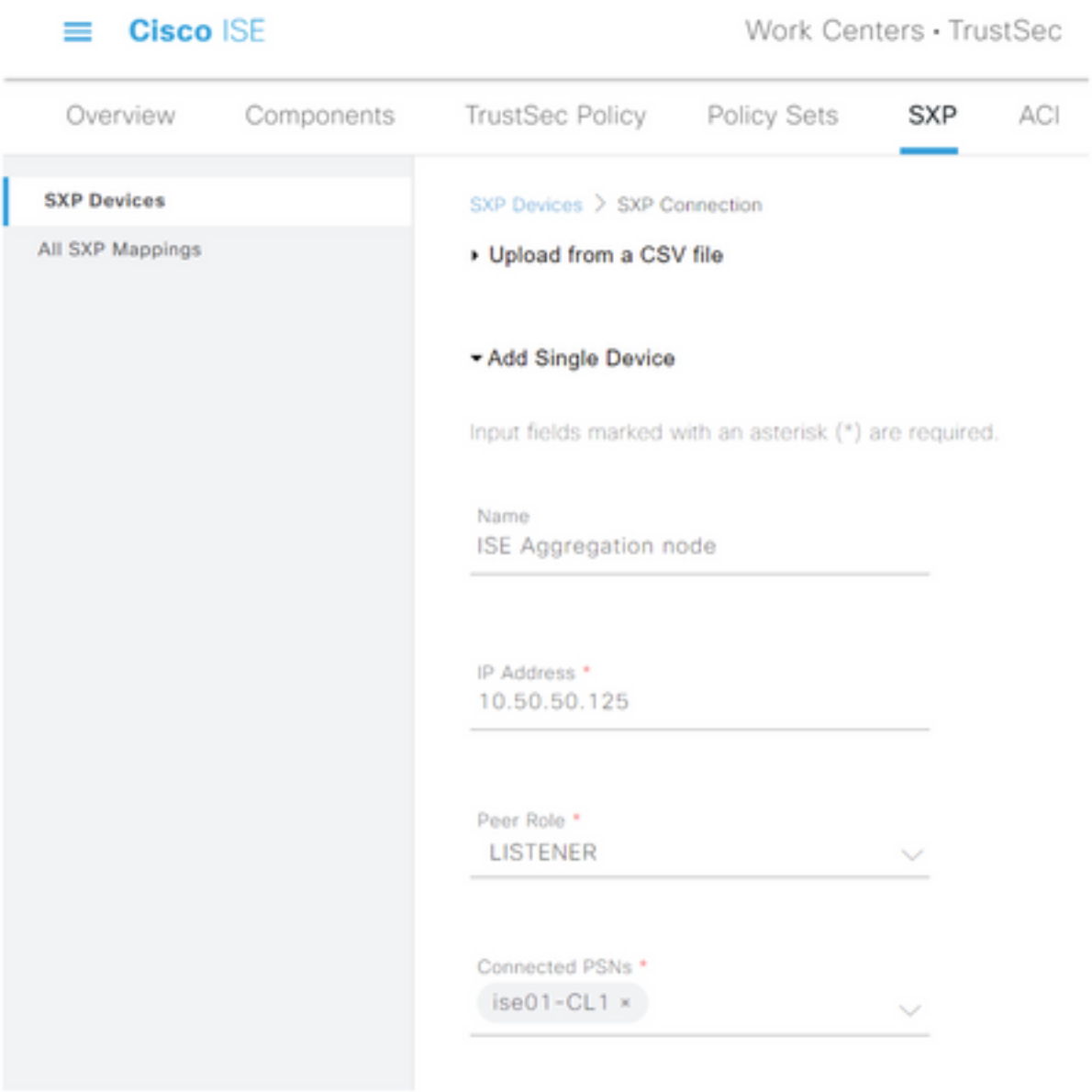
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centro de trabajo > TrustSec > SXP.**

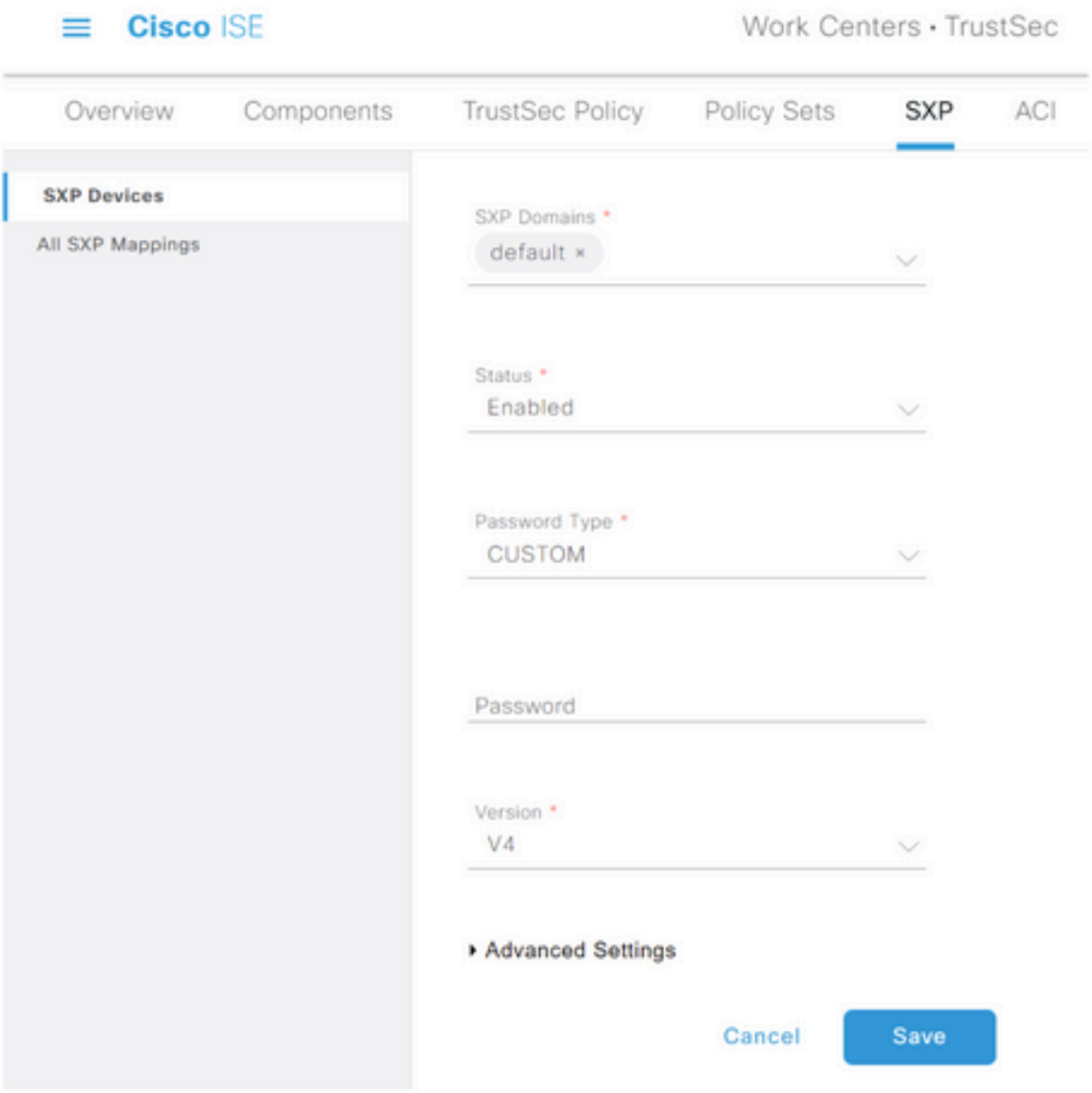
Paso 2. Haga clic en **+Add** para configurar el nodo de agregación ISE como un peer SXP.



Paso 3. Defina el nombre y la **dirección IP** del nodo de agregación ISE, seleccione la función de

peer como **LISTENER**. Seleccione los PSN requeridos en **PSNs conectados**, **dominios SXP** obligatorios, seleccione **habilitado** en estado, luego seleccione **tipo de contraseña** y **versión requerida**.





Paso 4. Haga clic en **Save (Guardar).**

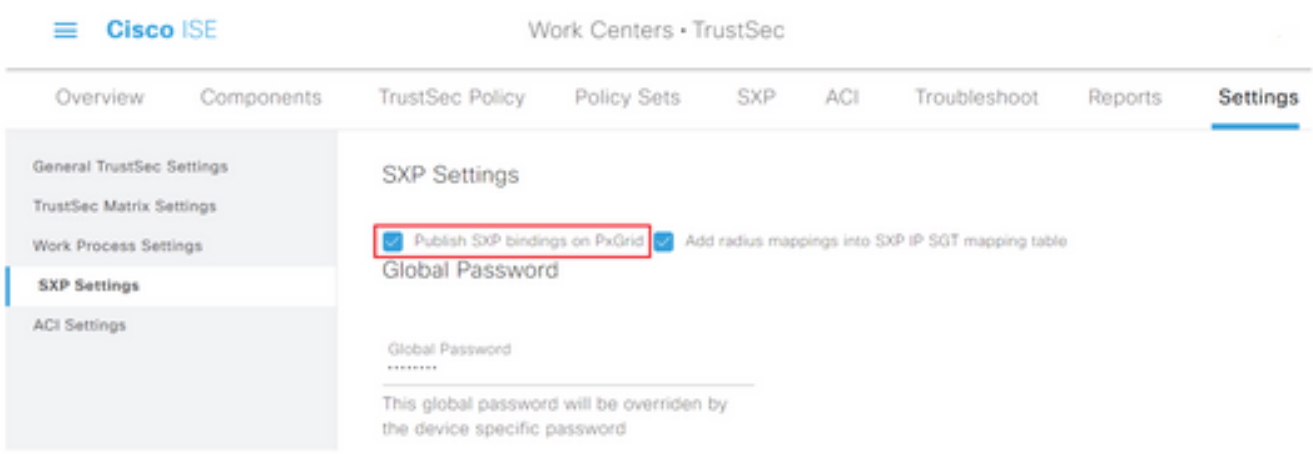
> **Nota:** Repita todos los pasos para el resto de los nodos ISE en cada clúster para generar una conexión SXP al nodo de agregación. **Repita el mismo proceso en el nodo de agregación y seleccione SPEAKER como rol de peer.**

Configure SXP en el nodo de agregación

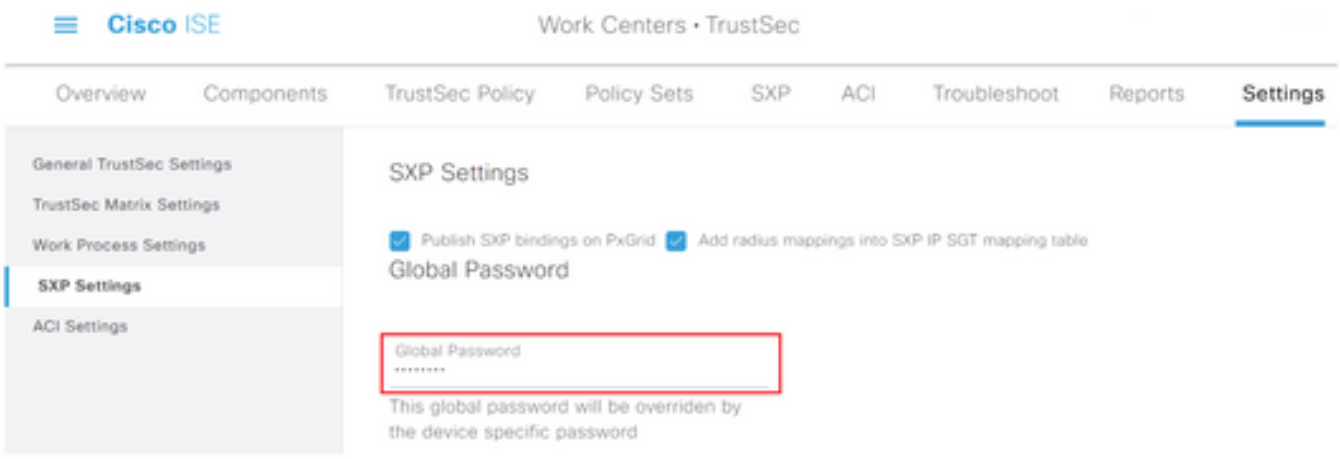
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centro de trabajo > TrustSec > Configuración**

Paso 2. Haga clic en la pestaña **Configuración de SXP**

Paso 3. Para propagar las asignaciones IP-SGT, marque la casilla de verificación **Publicar enlaces SXP en pxGrid**.



Paso 4 (opcional). Defina una contraseña predeterminada para la configuración de SXP en **Contraseña global**

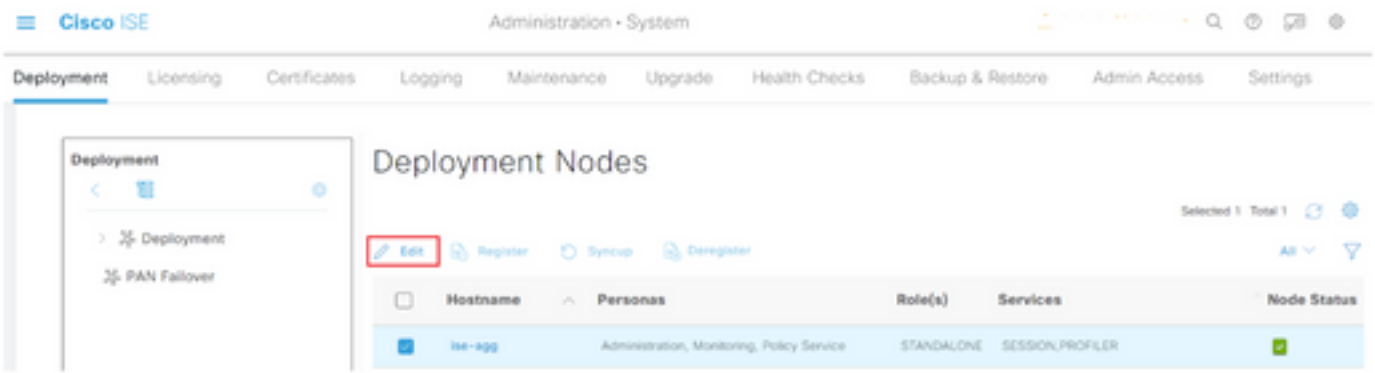


Paso 5. Desplácese hacia abajo y haga clic en **Guardar.**

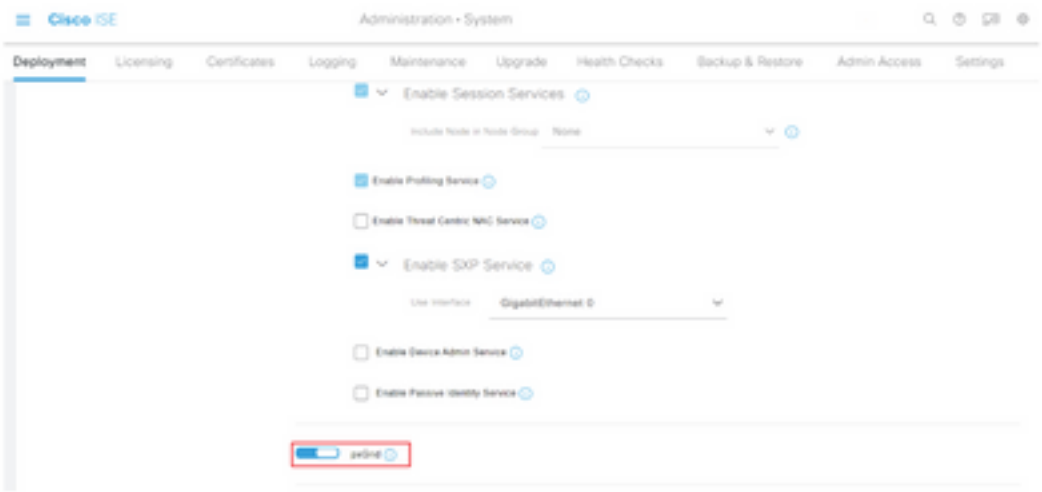
Habilitar pxGrid en el nodo de agregación

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Administración > Sistema > Implementación.**

Paso 2. Seleccione el nodo que desea configurar y haga clic en **Editar.**



Paso 3. Para habilitar pxGrid, haga clic en el botón situado junto a **pxGrid.**

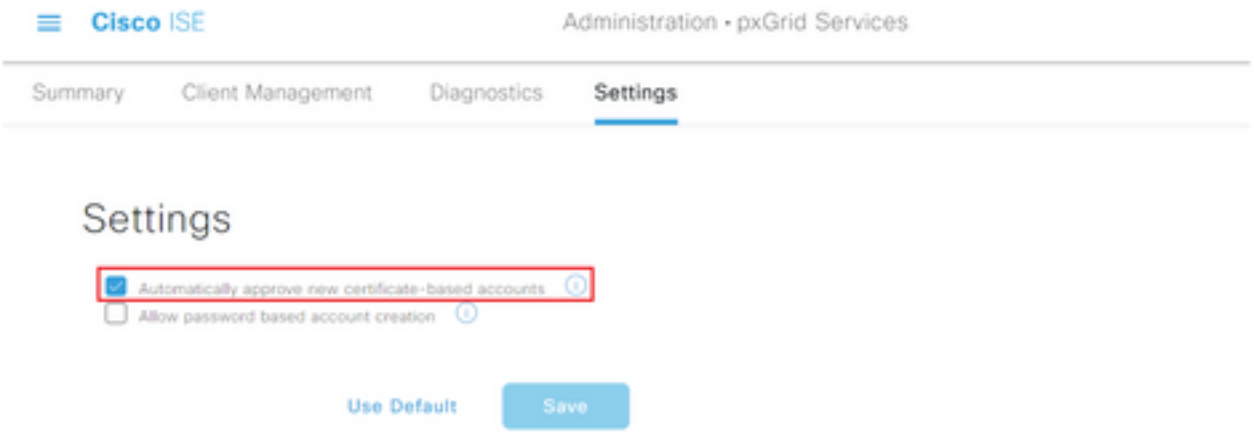


Paso 4. Desplácese hacia abajo y haga clic en **Guardar.**

aprobación automática de pxGrid

Paso 1. Navegue hasta el icono de tres líneas situado en la esquina superior izquierda y seleccione **Administration > pxGrid Services > Settings.**

Paso 2. De forma predeterminada, ISE no aprueba automáticamente pxGrid las solicitudes de conexión de los nuevos clientes pxGrid, por lo que debe activar esa configuración seleccionando la casilla de verificación **Aprobar automáticamente nuevas cuentas basadas en certificados.**



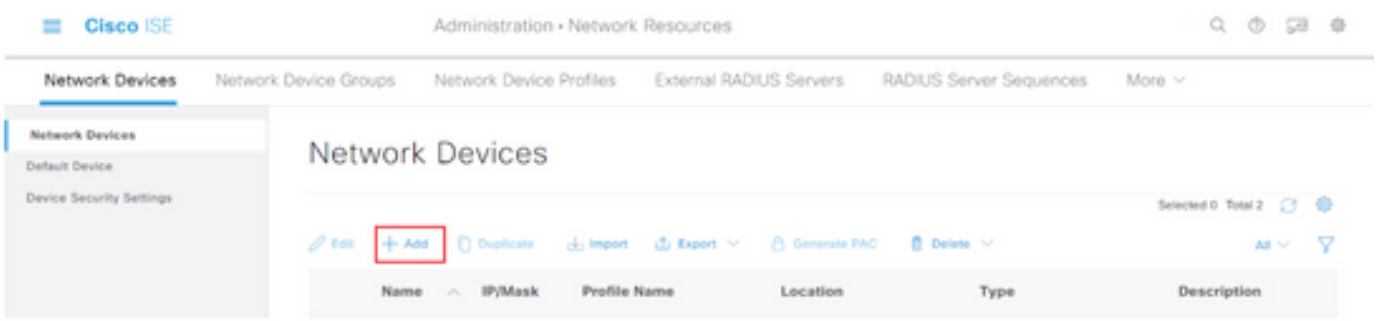
Paso 3. Haga clic en **Save (Guardar).**

Configuración TrustSec de dispositivos de red

Para que Cisco ISE procese las solicitudes de los dispositivos habilitados para TrustSec, debe definir estos dispositivos habilitados para TrustSec en Cisco ISE.

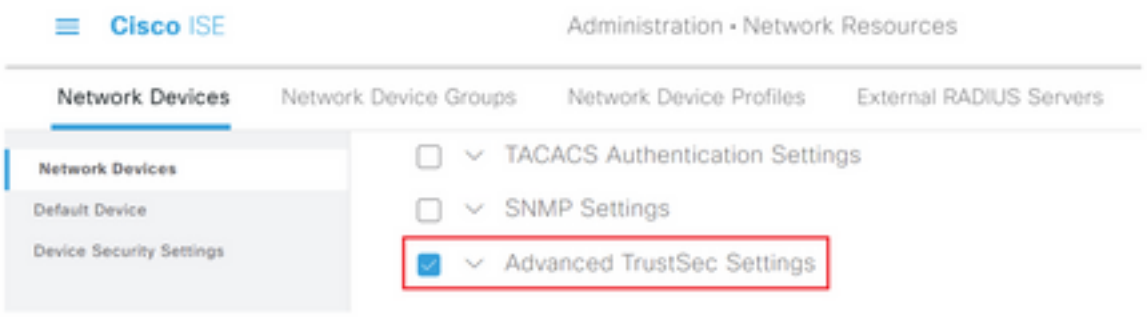
Paso 1. Navegue hasta las tres líneas ubicadas en la esquina superior izquierda y seleccione en **Administración > Recursos de red > Dispositivos de red.**

Paso 2. Haga clic en **+Agregar.**

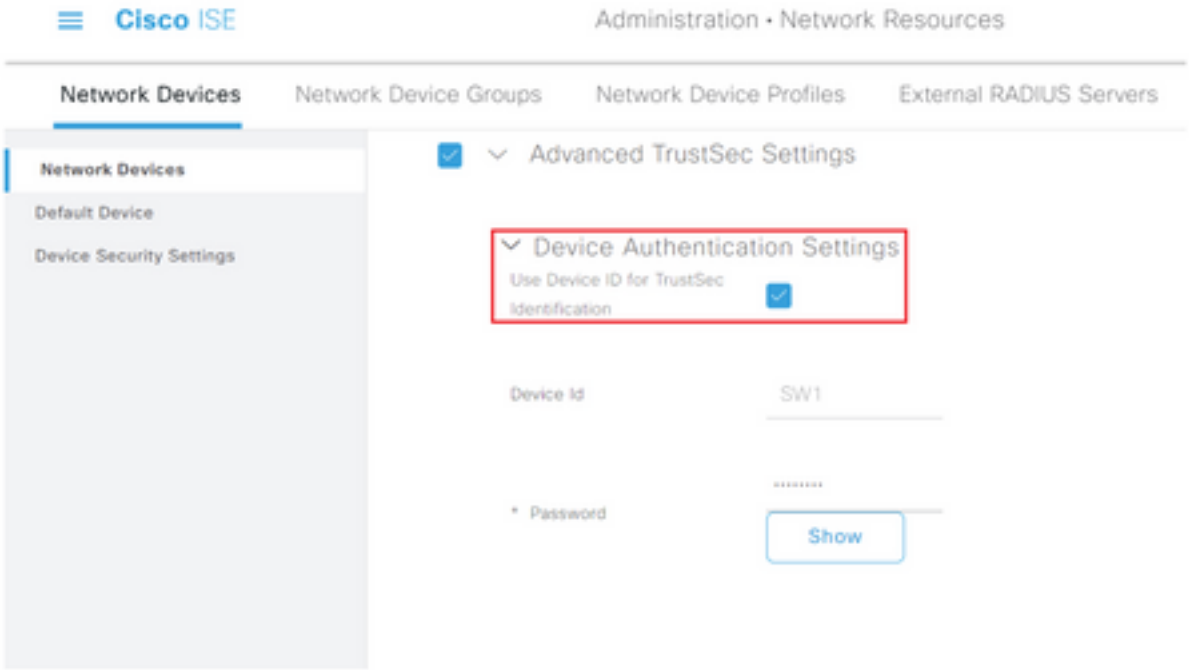


Paso 3. Ingrese la información requerida en la sección **Dispositivos de Red** y en **Configuración de Autenticación RADIUS.**

Paso 4. Marque la casilla de verificación **Advanced TrustSec Settings** para configurar un dispositivo habilitado para TrustSec.

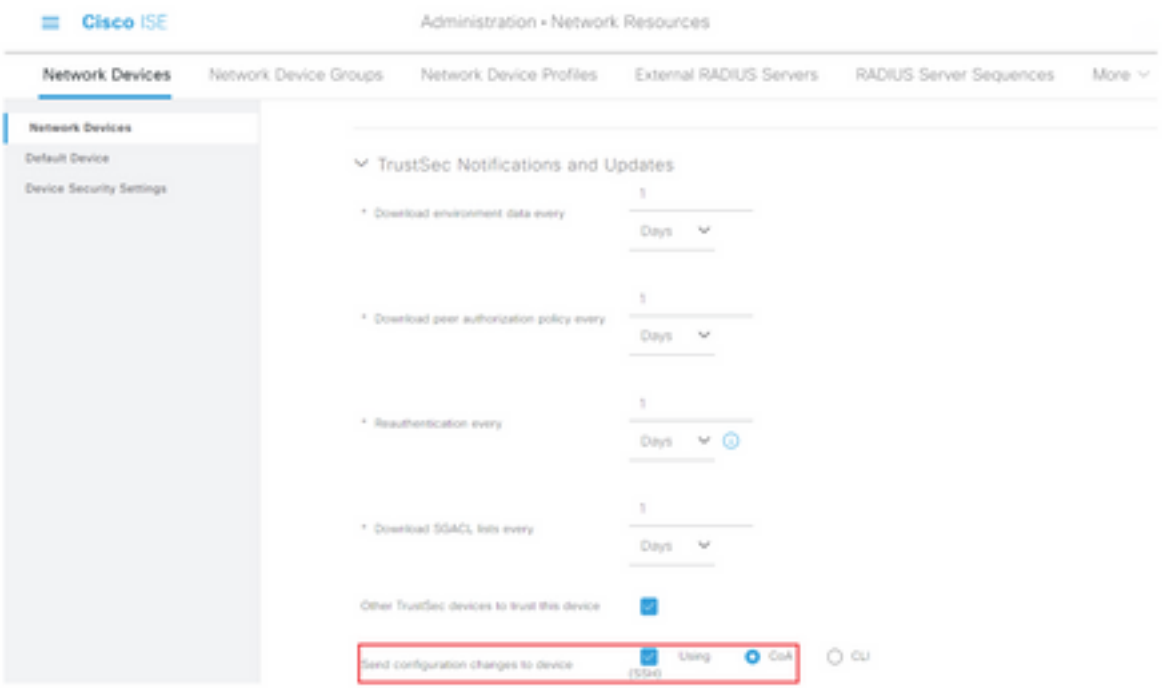


Paso 5. Haga clic en la casilla de verificación **Usar ID de dispositivo para la identificación TrustSec** para rellenar automáticamente el nombre de dispositivo que aparece en la sección **Dispositivos de red**. Introduzca una contraseña en el campo **Password**.



Nota: El ID y la contraseña deben coincidir con el comando "cts credentials id <ID> password <PW>" que se configura posteriormente en el switch.

Paso 6. Marque la casilla de verificación **Enviar cambios de configuración al dispositivo** para que ISE pueda enviar notificaciones de CoA de TrustSec al dispositivo.



Paso 7. Marque la casilla de verificación **Incluir este dispositivo al implementar actualizaciones de asignación de etiquetas de grupo de seguridad**.

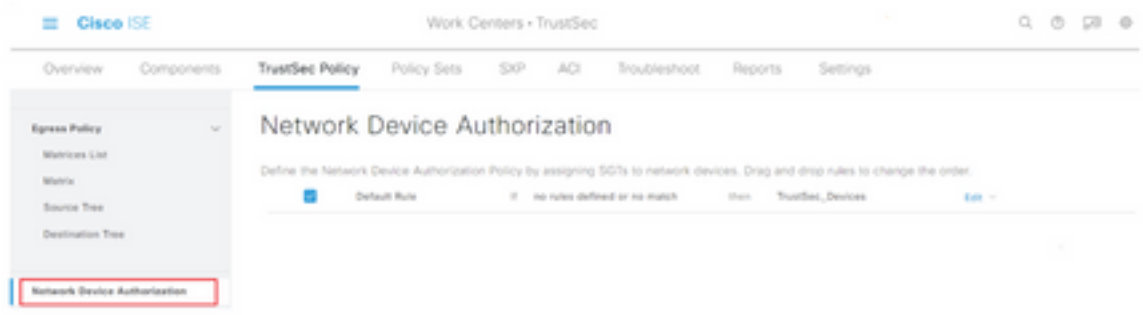
Paso 8. Para permitir que ISE edite la configuración del dispositivo de red, ingrese las credenciales de usuario en los campos Nombre de usuario del modo EXEC y **Contraseña del modo EXEC**. Opcionalmente, proporcione enable password en el campo **Enable Mode Password**.

> **Nota:** Repita los pasos para todos los demás NAD que estén destinados a formar parte del dominio TrustSec.

Autorización de dispositivo de red

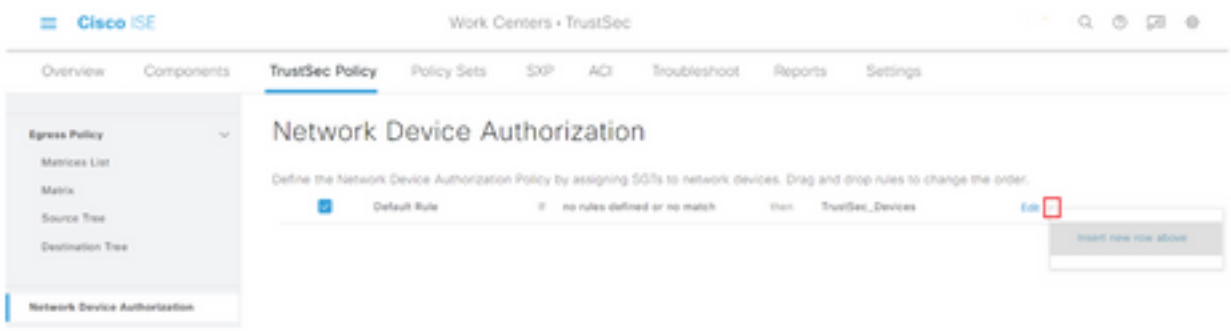
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centros de trabajo > TrustSec > Política TrustSec.**

Paso 2. En el panel izquierdo, haga clic en **Autorización de dispositivo de red.**



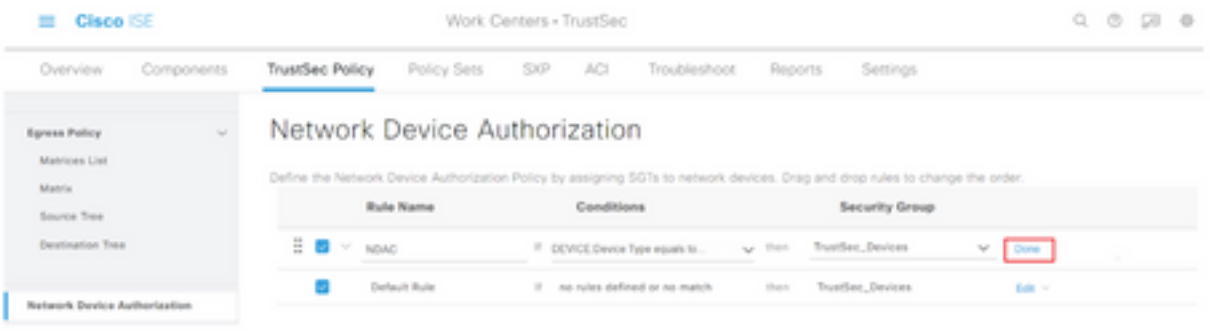
Paso 3. A la derecha, utilice el menú desplegable situado junto a **Editar** e **Insertar nueva fila arriba**

para crear una nueva regla NDA.



Paso 4. Defina un **Nombre de regla, Condiciones** y seleccione la SGT adecuada en la lista desplegable en **Grupos de seguridad.**

Paso 5. Haga clic en **Finalizado** en el extremo derecho.



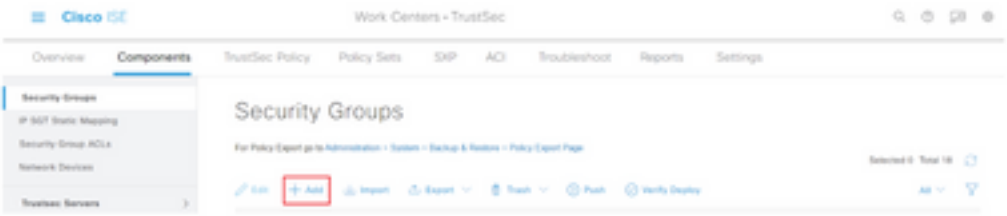
Paso 6. Desplácese hacia abajo y haga clic en **Guardar.**

SGT

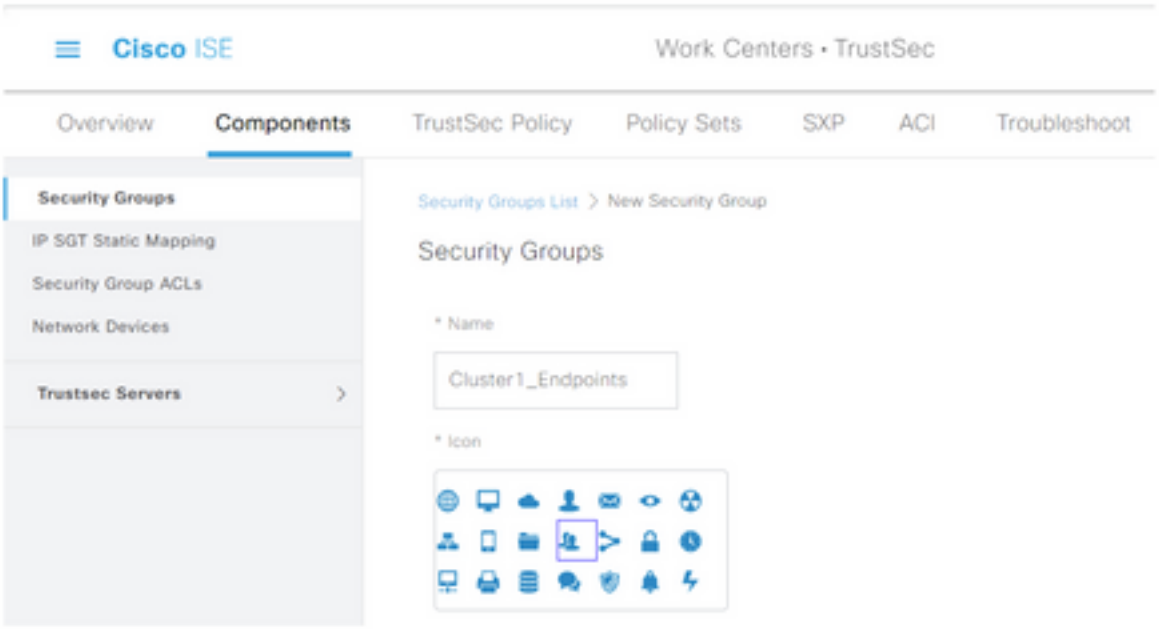
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centros de trabajo > TrustSec > Componentes.**

Paso 2. En el panel izquierdo, expanda **Grupos de seguridad.**

Paso 3. Haga clic en **+Agregar** para crear una nueva SGT.



Paso 4. Introduzca el nombre y seleccione un icono en los campos correspondientes.



Paso 5. Opcionalmente, proporcione una descripción e introduzca un **valor de etiqueta.**

> **Nota:** Para poder introducir manualmente un valor de etiqueta, navegue hasta Centros de trabajo > TrustSec > Configuración > Configuración general de TrustSec y seleccione la opción **El usuario debe introducir manualmente el número SGT** en **Numeración de etiquetas de grupo de seguridad.**

Paso 6. Desplácese hacia abajo y haga clic en **Enviar**

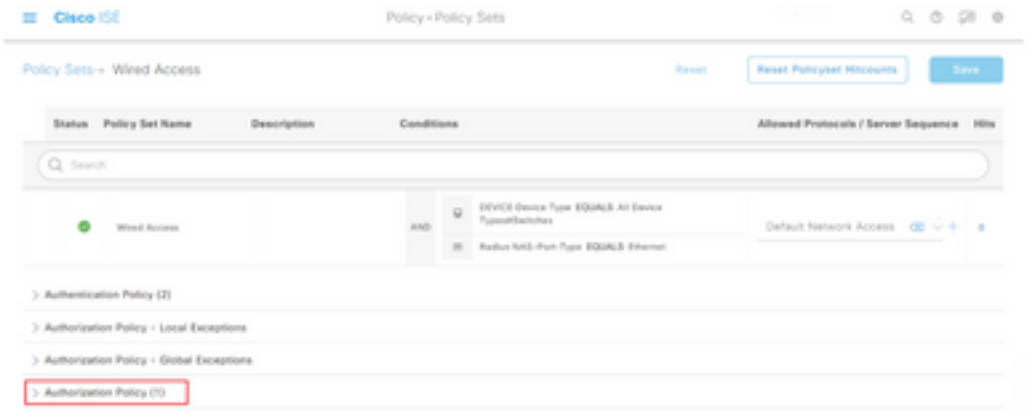
> **Nota:** Repita estos pasos para todas las SGT necesarias.

Política de autorización

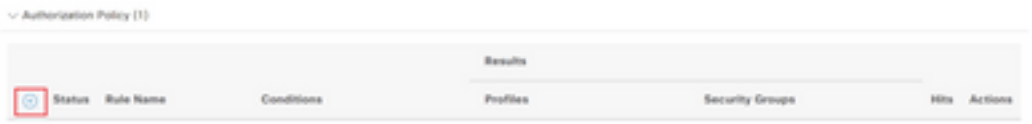
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Política > Conjuntos de políticas.**

Paso 2. Seleccione el conjunto de políticas adecuado.

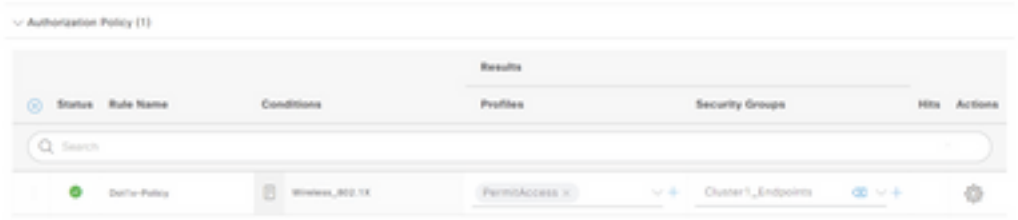
Paso 3. Dentro del conjunto de políticas, expanda la **Política de autorización.**



Paso 4. Haga clic en el  para crear una **directiva de autorización.**



Paso 5. Defina el **Nombre de la Regla, las Condiciones** y los **Perfiles** requeridos **y seleccione la SGT adecuada en la lista desplegable en Grupos de Seguridad.**



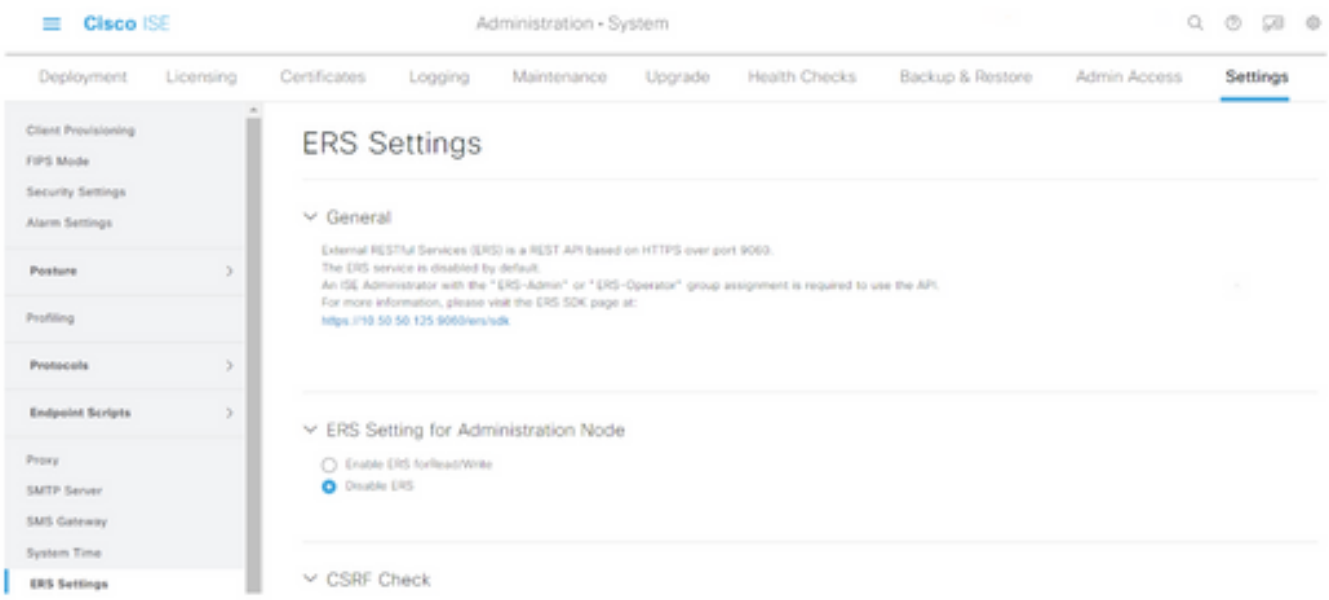
Paso 6. Click **Save.**

Habilitación de ERS en el nodo de agregación de ISE (opcional)

El servicio de API RESTful externo (ERS) es una API que WSA puede consultar para obtener información del grupo. El servicio ERS está inhabilitado de forma predeterminada en ISE. Una vez habilitada, los clientes pueden consultar la API si se autentican como miembros del grupo **ADR** en el nodo ISE. Para habilitar el servicio en ISE y agregar una cuenta al grupo correcto, siga estos pasos:

Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Administración > Sistema > Configuración.**

Paso 2. En el panel izquierdo, haga clic en **Configuración de ERS.**



Paso 3. Seleccione la opción **Enable ERS for Read/Write (Habilitar ERS para lectura/escritura).**

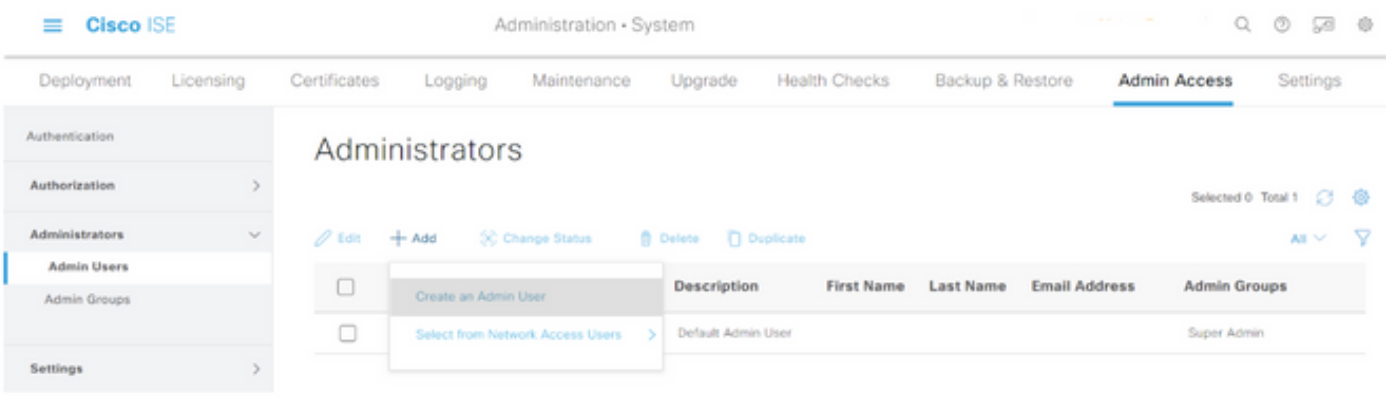
Paso 4. Haga clic en **Guardar** y confirme con **Aceptar.**

Agregar usuario al grupo de administración ESR (opcional)

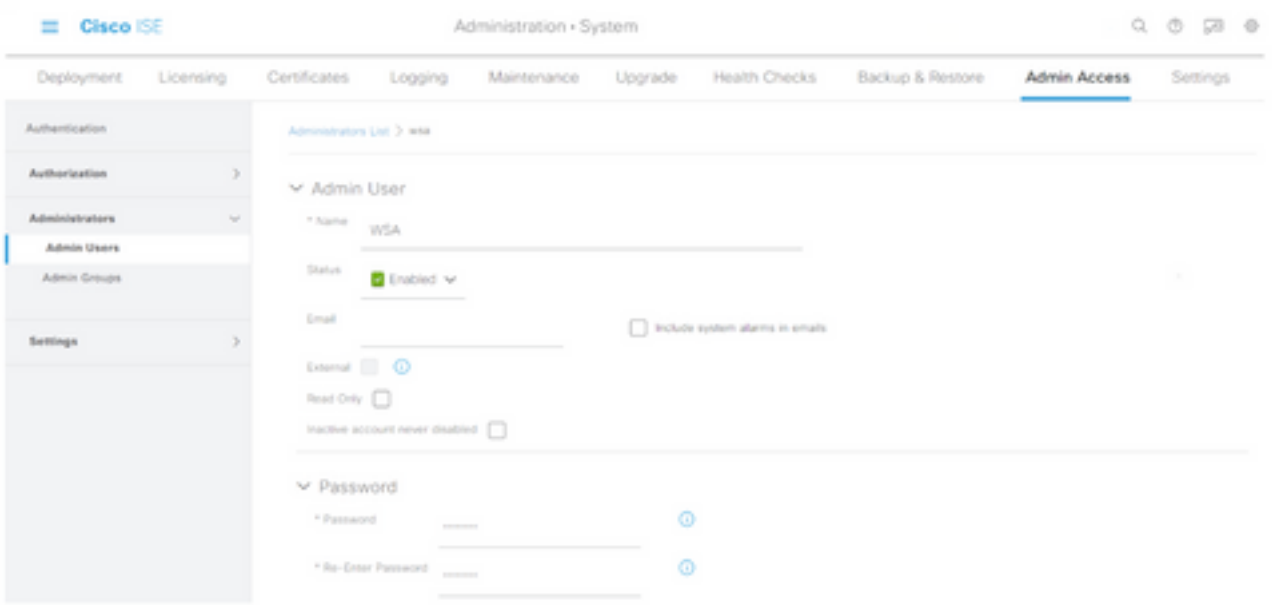
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione **Administration > System > Admin Access**

Paso 2. En el panel izquierdo, expanda **Administradores** y haga clic en **Usuarios administrativos.**

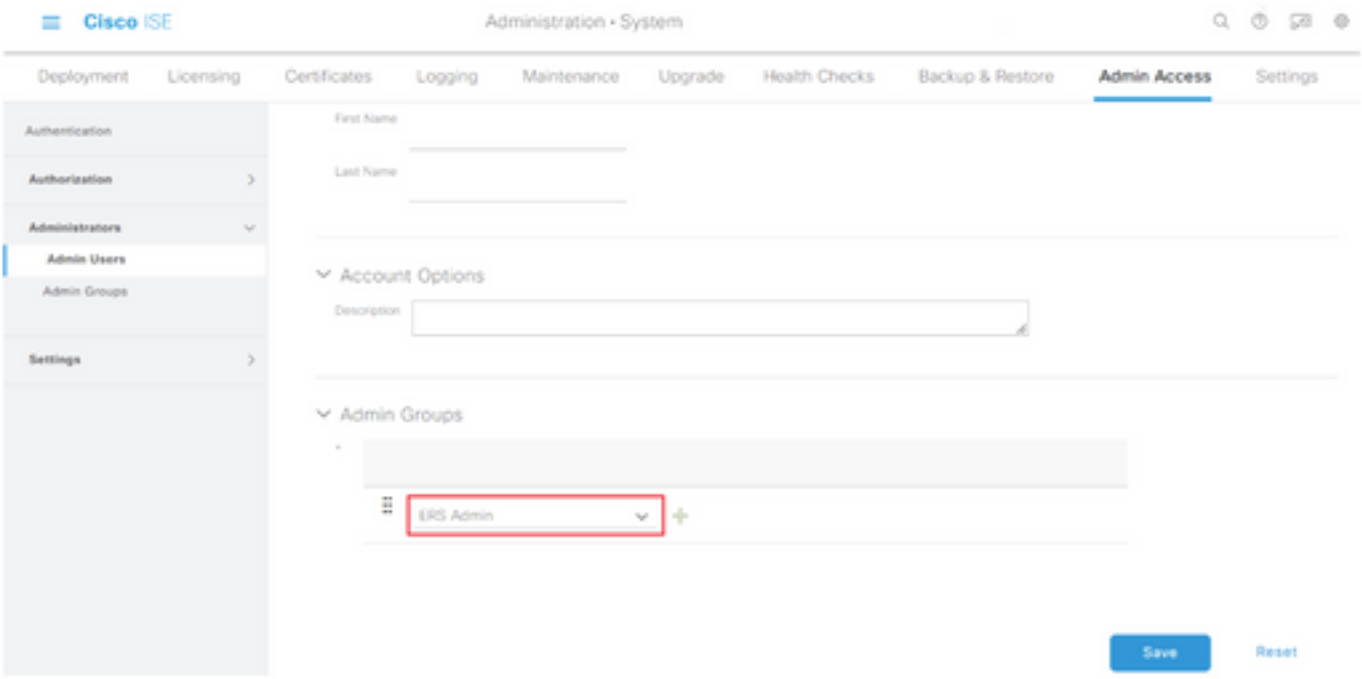
Paso 3. Haga clic en **+Add** y seleccione **Admin User** en la lista desplegable.



Paso 4. Introduzca un nombre de usuario y una contraseña en los campos correspondientes.



Paso 5. En el campo **Admin Groups**, utilice el menú desplegable para seleccionar **ERS Admin.**



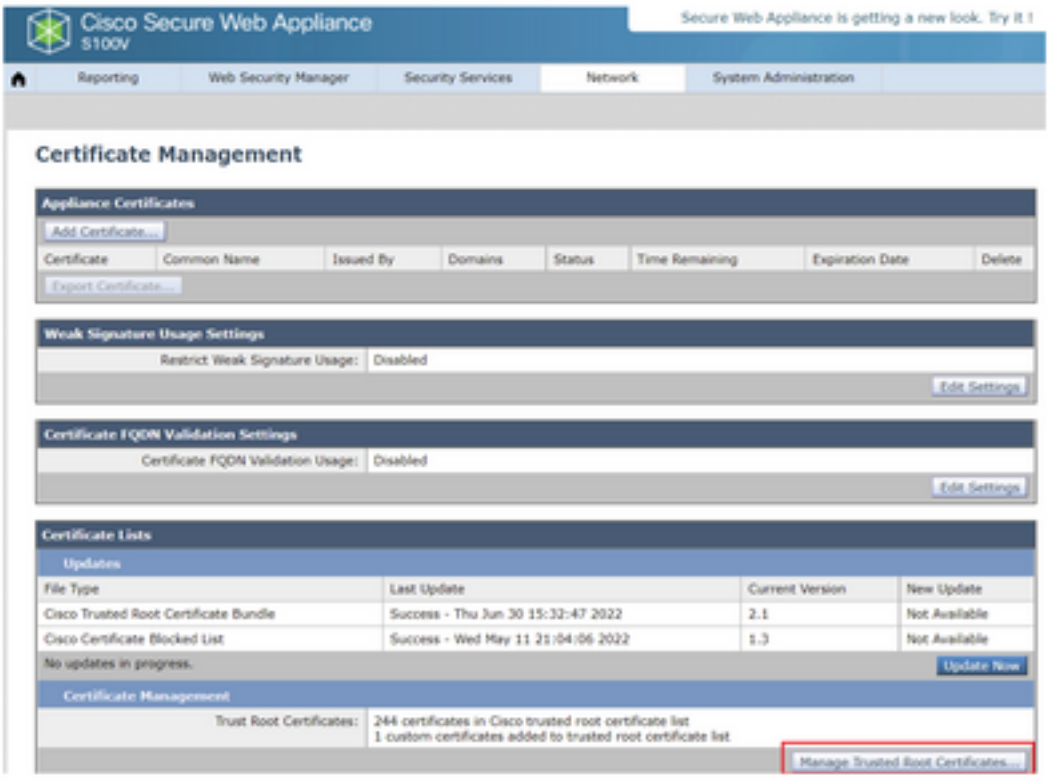
Paso 6. Click **Save.**

Configuración del dispositivo web seguro

Certificado raíz

Si el diseño de integración utiliza una autoridad de certificados interna como raíz de la confianza para la conexión entre WSA e ISE, este certificado raíz se debe instalar en ambos dispositivos.

Paso 1. Navegue hasta **Red > Administración de certificados** y haga clic en **Administrar certificados raíz de confianza** para agregar un certificado de CA.



Paso 2. Haga clic en **Importar.**

Paso 3. Haga clic en **Elegir archivo** para localizar la CA raíz generada y haga clic en **Enviar.**

Paso 4. Haga clic en **Enviar** de nuevo.

Paso 5. En la esquina superior derecha, haga clic en **Registrar cambios.**

Paso 6. Haga clic en **Registrar cambios** de nuevo.

Certificado pxGrid

En WSA, la creación del par de claves y el certificado para su uso por pxGrid se completa como parte de la configuración de servicios ISE.

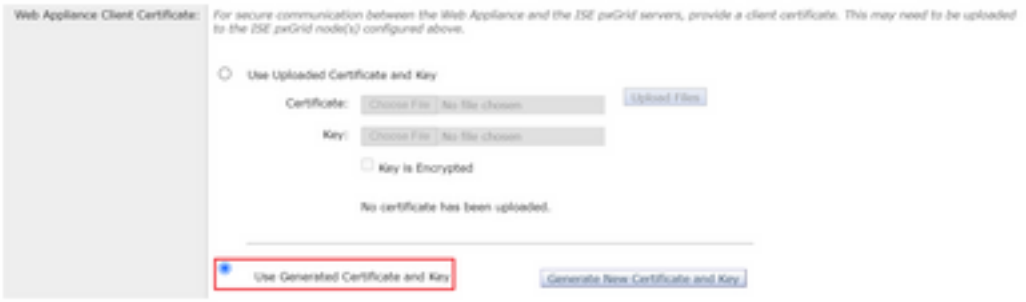
Paso 1. Vaya a **Red > Identity Service Engine.**

Paso 2. Haga clic en **Activar y editar configuración.**

Paso 3. Haga clic en **Elegir archivo** para localizar la CA raíz generada y haga clic en **Cargar archivo.**

> **Nota:** Una configuración incorrecta común es cargar el certificado pxGrid de ISE en esta sección. El certificado de CA raíz se debe cargar en el campo Certificado de nodo de pxGrid de ISE.

Paso 4. En la sección **Certificado de cliente de dispositivo web**, seleccione **Usar certificado y clave generados.**

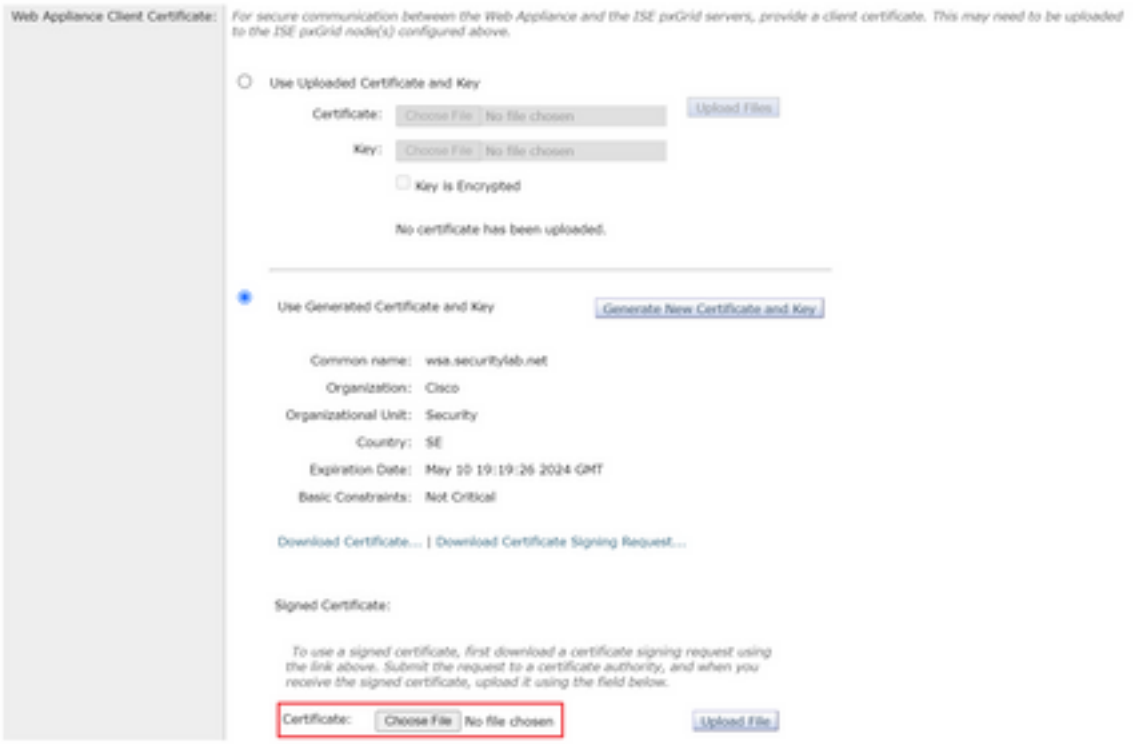


Paso 5. Haga clic en el botón **Generar nuevo certificado y clave** y complete los campos de certificado requeridos.

Paso 6. Haga clic en **Descargar solicitud de firma de certificado.**

> **Nota:** Se recomienda seleccionar el botón **Enviar** para registrar los cambios en la configuración de ISE. Si la sesión se deja en tiempo de espera antes de que se envíen los cambios, las claves y el certificado que se generaron pueden perderse, incluso si se descargó el CSR.

Paso 7. Una vez que haya firmado la CSR con su CA, haga clic en **Elegir archivo** para localizar el certificado.



Paso 8. Haga clic en **Cargar archivo.**

Paso 9. Enviar y **confirmar.**

Habilitar SXP y ERS en un dispositivo web seguro

Paso 1. Haga clic en los botones **Enable** para SXP y ERS.

Paso 2. En el campo **Credenciales de administrador ERS**, introduzca la información de usuario configurada en ISE.

Paso 3. Marque la casilla para **que el nombre del servidor sea igual que el nodo pxGrid de ISE** para heredar la información configurada anteriormente. De lo contrario, introduzca la información necesaria allí.

Paso 4. Enviar y **confirmar.**

Perfil de identificación

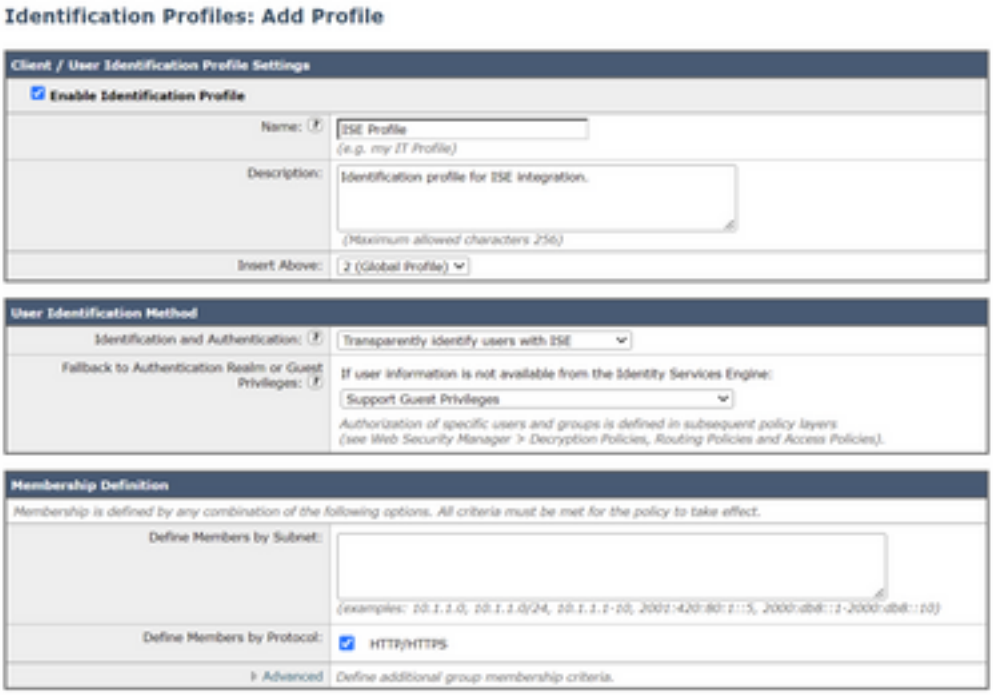
Para utilizar las etiquetas de grupos de seguridad o la información de grupo ISE en las políticas WSA, primero se debe crear un perfil de identificación que utilice ISE como medio para identificar a los usuarios de forma transparente.

Paso 1. Vaya a **Web Security Manager > Authentication > Identification Profiles.**

Paso 2. Haga clic en **Agregar perfil de identificación.**

Paso 3. Introduzca un nombre y, opcionalmente, una descripción.

Paso 4. En la **sección Identificación y Autenticación**, utilice el menú desplegable para elegir **Identificar de forma transparente a los usuarios con ISE.**



Paso 5. Enviar y **confirmar.**

Política de descifrado basada en SGT

Paso 1. Vaya a **Web Security Manager > Web Policies > Decryption Policies.**

Paso 2. Haga clic en **Agregar política.**

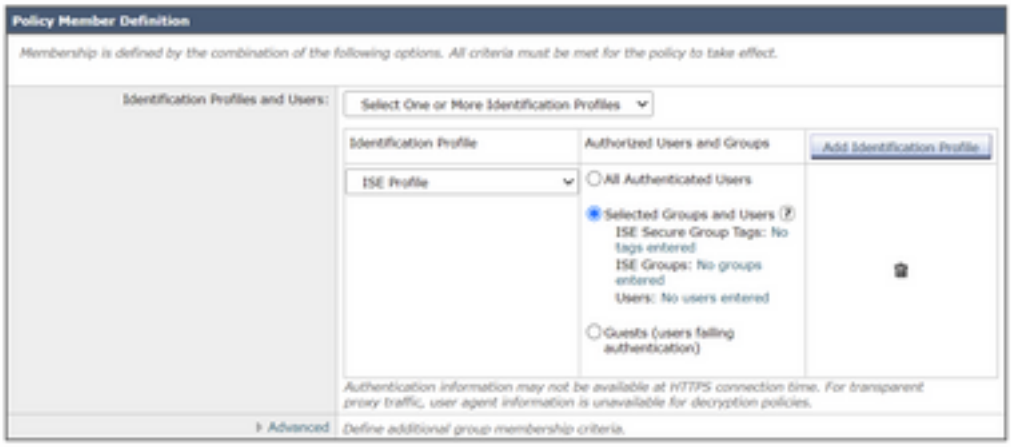
Paso 3. Introduzca un nombre y, opcionalmente, una descripción.

Paso 4. En la sección **Perfiles de identificación y usuarios**, utilice el menú desplegable para elegir **Seleccionar uno o más perfiles de identificación.**

Paso 5. En la sección **Perfiles de identificación**, utilice el menú desplegable para elegir el nombre del perfil de identificación de ISE.

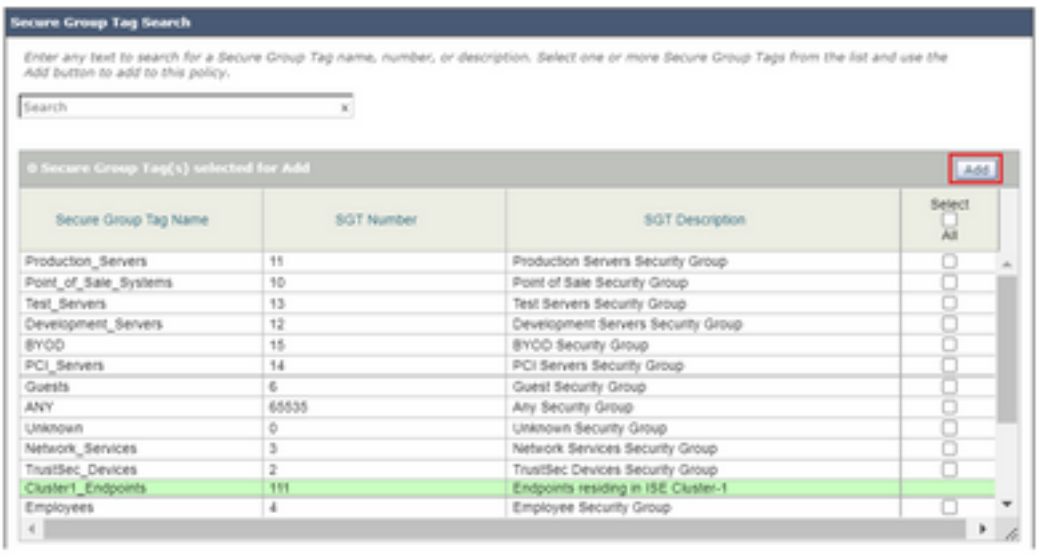
Paso 6. En la sección **Usuarios y grupos autorizados**, seleccione **Grupos y usuarios**

seleccionados.



Paso 7. Haga clic en el hipervínculo situado junto a **Etiquetas de grupo seguras de ISE.**

Paso 8. En la sección **Búsqueda segura de etiquetas de grupo**, marque la casilla a la derecha de la SGT deseada y haga clic en **Agregar.**



Paso 9. Haga clic en **Finalizado** para volver.

Paso 10. Enviar y **confirmar.**

Configuración del switch

AAA

```
aaa new-model

aaa group server radius ISE
 server name ise01-cl1
 server name ise02-cl1
 ip radius source-interface Vlan50

aaa authentication dot1x default group ISE
aaa authorization network ISE group ISE
aaa accounting update newinfo periodic 2440
aaa accounting dot1x default start-stop group ISE

aaa server radius dynamic-author
 client 10.50.50.120 server-key Cisco123
 client 10.50.50.121 server-key Cisco123
 auth-type any

radius server ise01-cl1
 address ipv4 10.50.50.121 auth-port 1812 acct-port 1813
 pac key Cisco123
radius server ise02-cl1
 address ipv4 10.50.50.120 auth-port 1812 acct-port 1813
pac key Cisco123
```

TrustSec

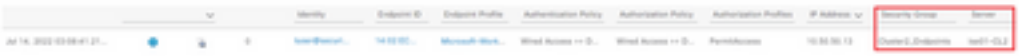
```
cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode)
cts role-based enforcement

aaa authorization network cts-list group ISE
cts authorization list cts-list
```

Verificación

Asignación SGT de ISE a terminal.

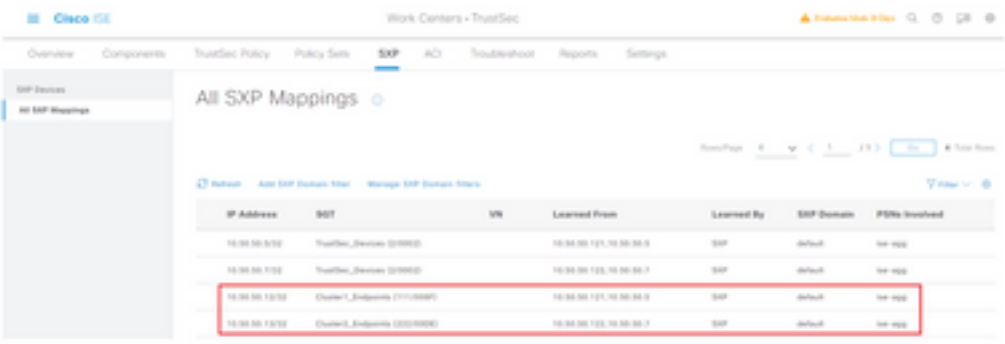
Aquí puede ver un terminal del ISE Cluster 1 asignado a una SGT después de una autenticación y autorización exitosas:

Aquí puede ver un terminal del ISE Cluster 2 asignado a una SGT después de una autenticación y autorización exitosas:

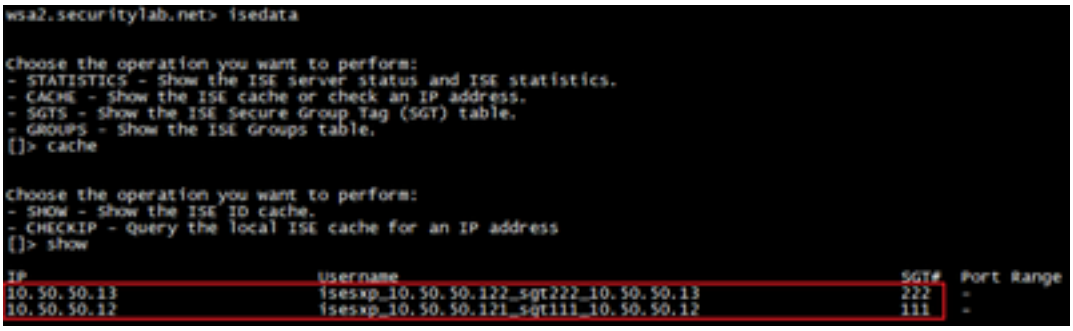


Asignaciones SXP

Dado que la comunicación SXP está habilitada entre los nodos ISE del clúster y el nodo de agregación ISE, estos mapeos SGT-IP son aprendidos por la agregación ISE a través de SXP:



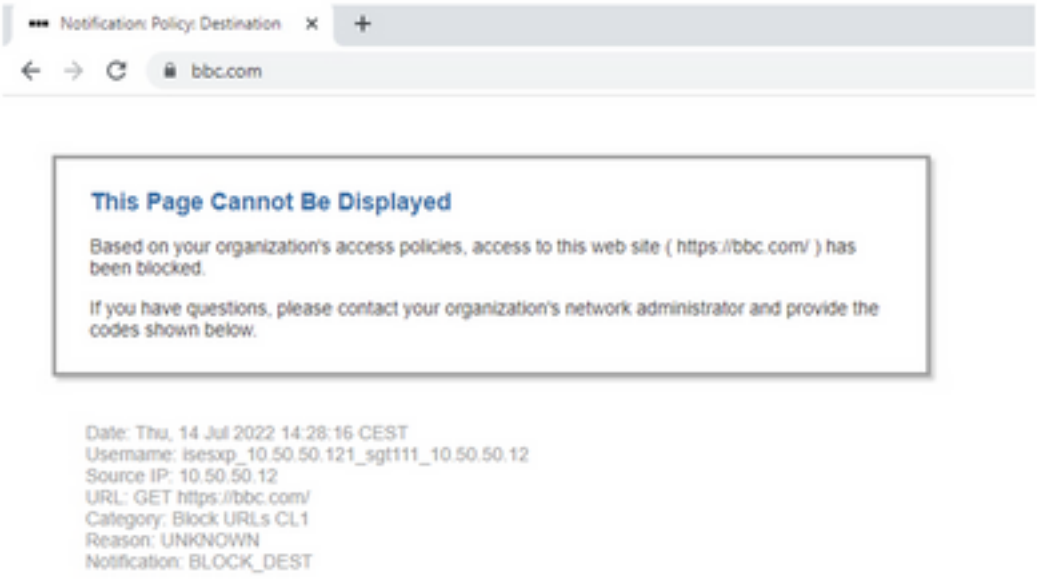
Estas asignaciones SXP, de diferentes clústeres de ISE, se envían a WSA a través de pxGrid a través del nodo de agregación ISE:

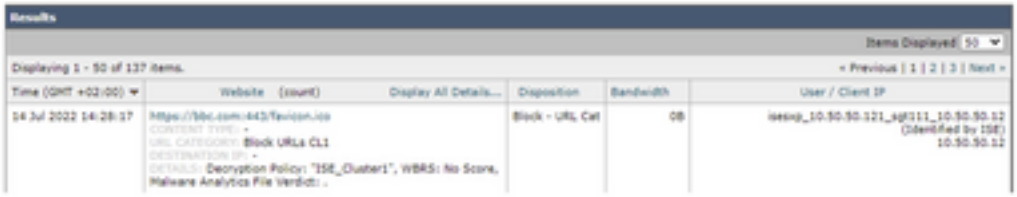


Aplicación de políticas basada en SGT

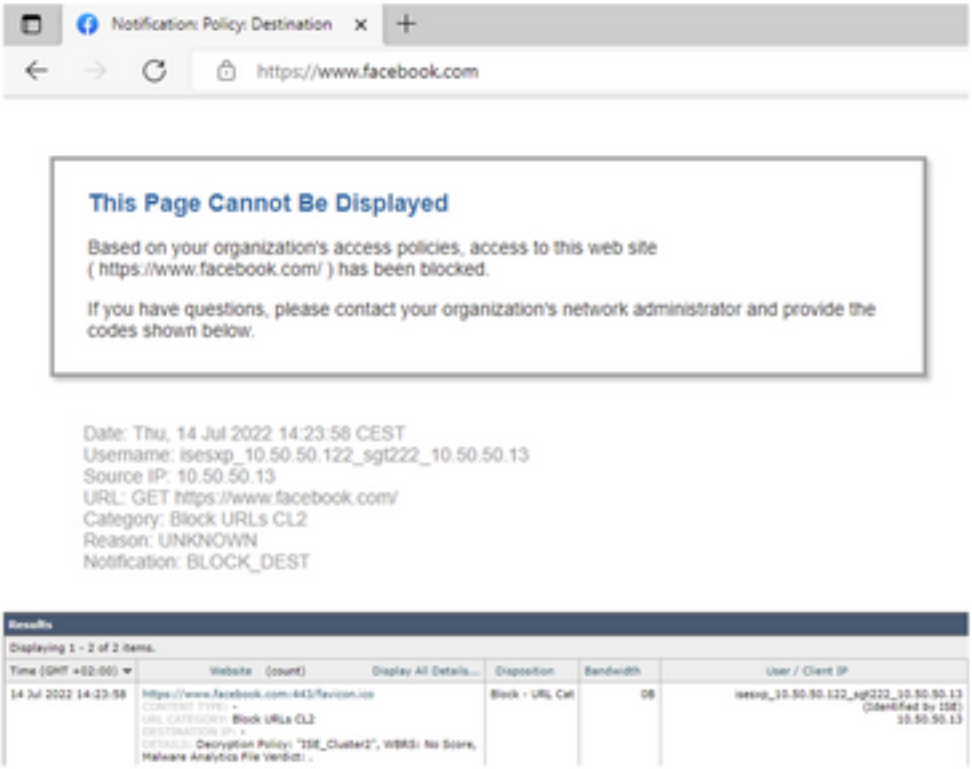
Aquí puede ver que los diferentes terminales coinciden con sus respectivas políticas y el tráfico se bloquea en función de su SGT:

Extremo que pertenece al clúster 1 de ISE





Extremo que pertenece al ISE Cluster 2



Información Relacionada

- Guía de integración de Web Security Appliance e Identity Service Engine
- Configuran la integración de WSA con ISE para TrustSec Aware Services
- Guía del administrador de Cisco Identity Services Engine, versión 3.1
- Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance