

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Limitaciones](#)

[Diagrama de la red](#)

[Configurar](#)

[Configuración de ISE](#)

[Activar SXP](#)

[Configure SXP en los nodos del clúster](#)

[Configure SXP en el nodo de agregación](#)

[Habilitar pxGrid en el nodo de agregación](#)

[aprobación automática de pxGrid](#)

[Configuración TrustSec de dispositivos de red](#)

[Autorización de dispositivo de red](#)

[SGT](#)

[Política de autorización](#)

[Habilitación de ERS en el nodo de agregación de ISE \(opcional\)](#)

[Agregar usuario al grupo de administración ESR \(opcional\)](#)

[Configuración del dispositivo web seguro](#)

[Certificado pxGrid](#)

[Habilitar SXP y ERS en un dispositivo web seguro](#)

[Perfil de identificación](#)

[Política de descifrado basada en SGT](#)

[Configuración del switch](#)

[AAA](#)

[TrustSec](#)

[Verificación](#)

[Información Relacionada](#)

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.

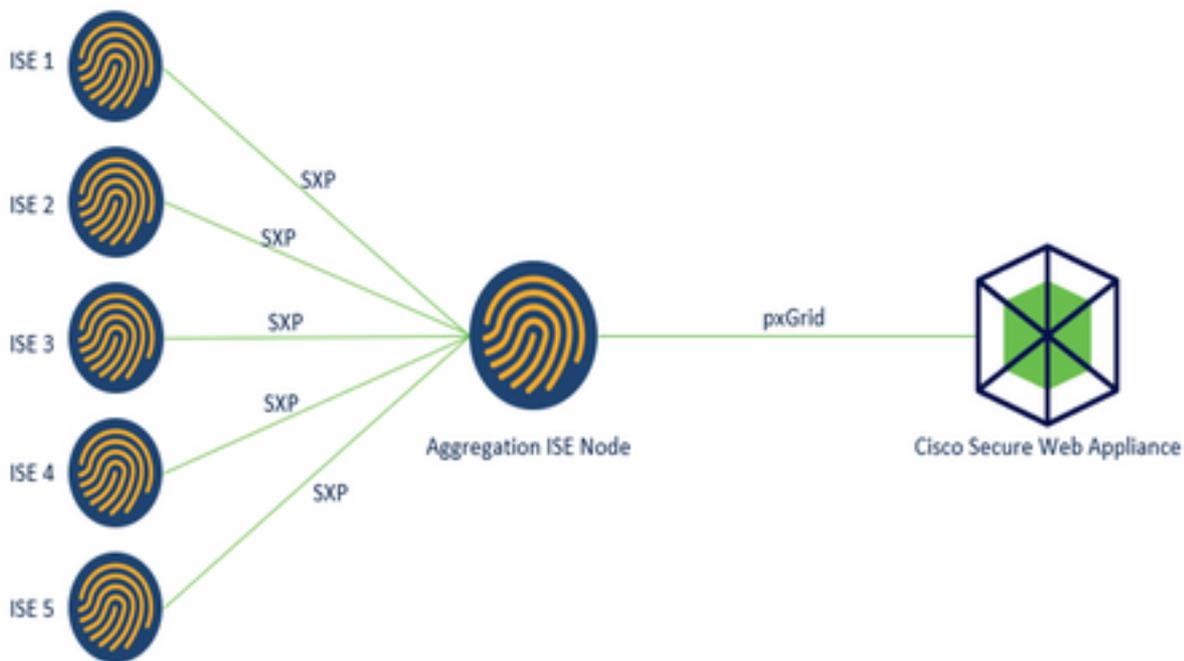
- Dispositivo web seguro 14.5
- ISE versión 3.1 P3

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.

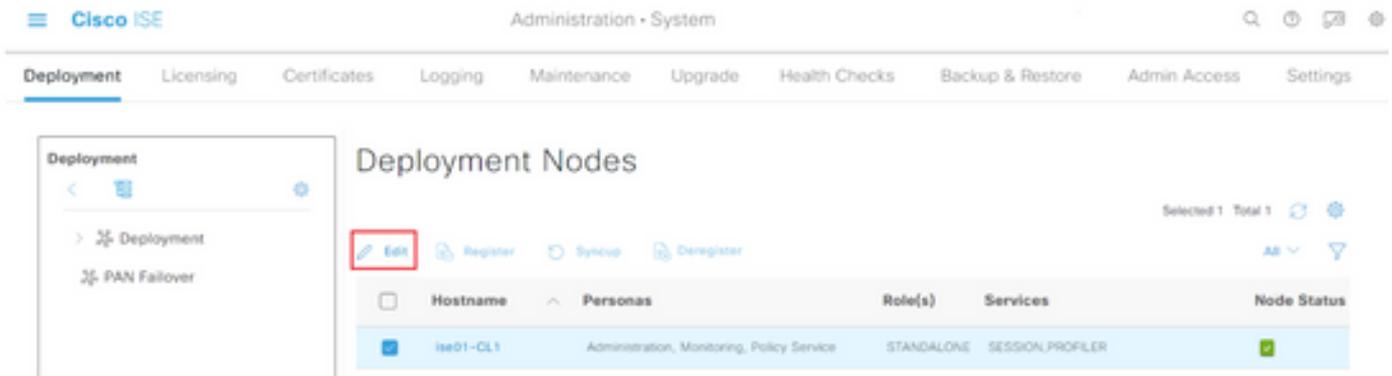
Configurar

Configuración de ISE

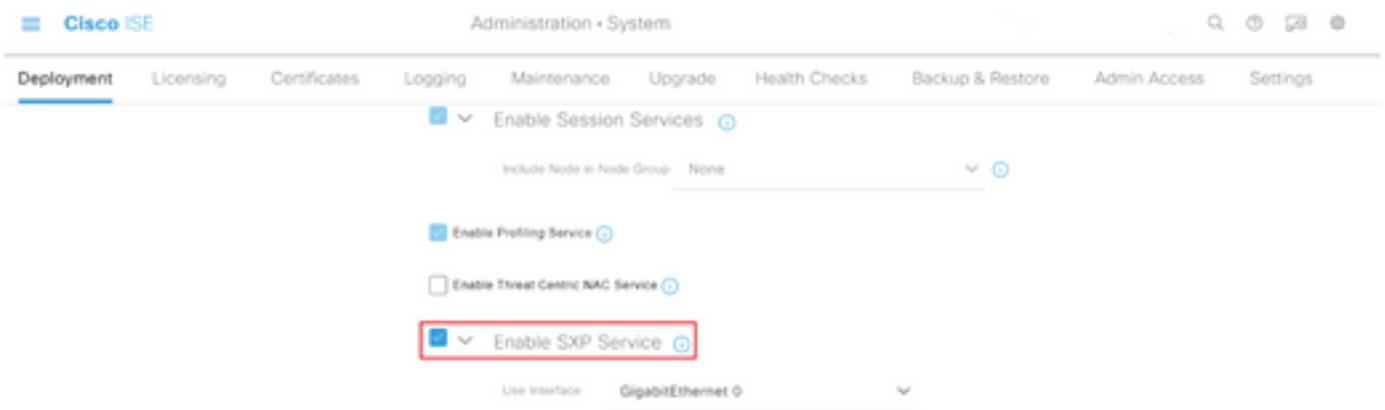
Activar SXP

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)**



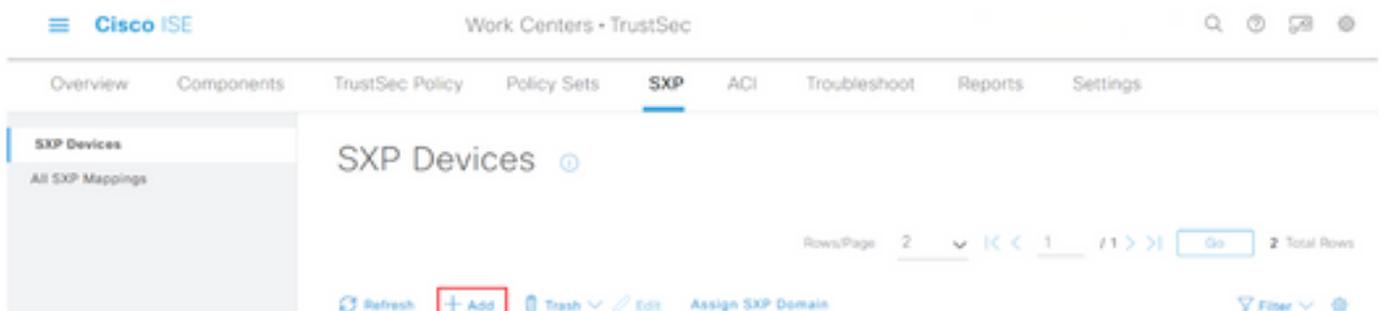
Paso 4. Desplácese hacia abajo y haga clic en **Guardar**

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**.

Cisco ISE Work Centers • TrustSec

Overview Components TrustSec Policy Policy Sets **SXP** ACI

SXP Devices

All SXP Mappings

[SXP Devices](#) > [SXP Connection](#)

- ▶ **Upload from a CSV file**
- ▼ **Add Single Device**

Input fields marked with an asterisk (*) are required.

Name
ISE Aggregation node

IP Address *
10.50.50.125

Peer Role *
LISTENER

Connected PSNs *
ise01-CL1

Overview Components TrustSec Policy Policy Sets **SXP** ACI

SXP Devices

All SXP Mappings

SXP Domains *
default x

Status *
Enabled

Password Type *
CUSTOM

Password

Version *
V4

► Advanced Settings

Cancel Save

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

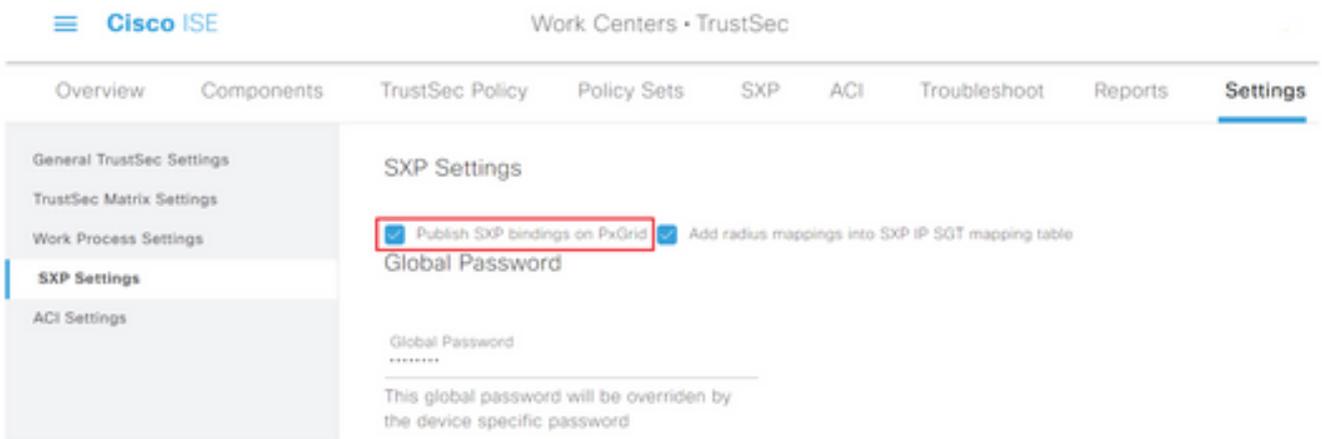
Nota: Repita todos los pasos para el resto de los nodos ISE en cada clúster para generar una conexión SXP al nodo de agregación. **Repita el mismo proceso en el nodo de agregación y seleccione SPEAKER como rol de peer.**

Configure SXP en el nodo de agregación

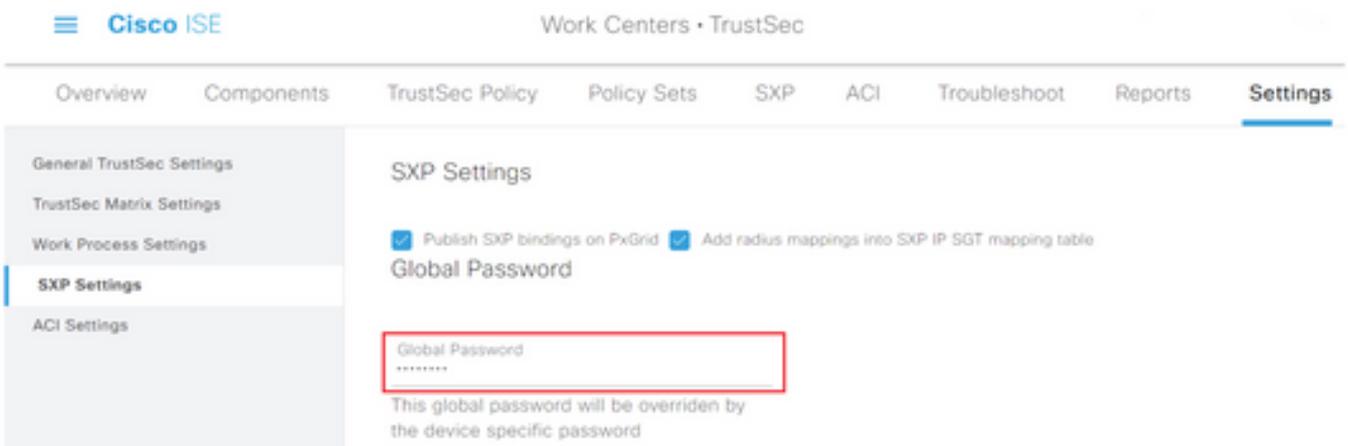
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centro de trabajo > TrustSec > Configuración**

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

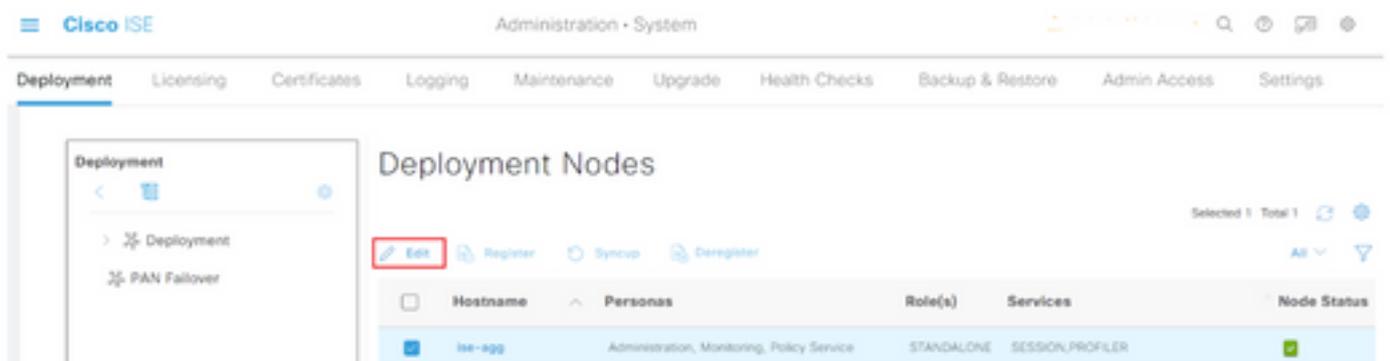


Paso 5. Desplácese hacia abajo y haga clic en **Guardar**.

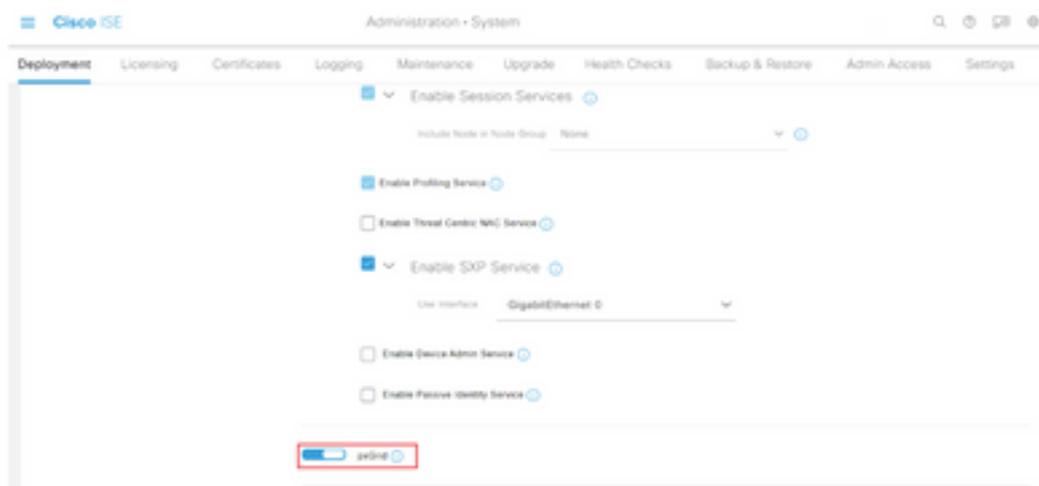
Habilitar pxGrid en el nodo de agregación

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**.

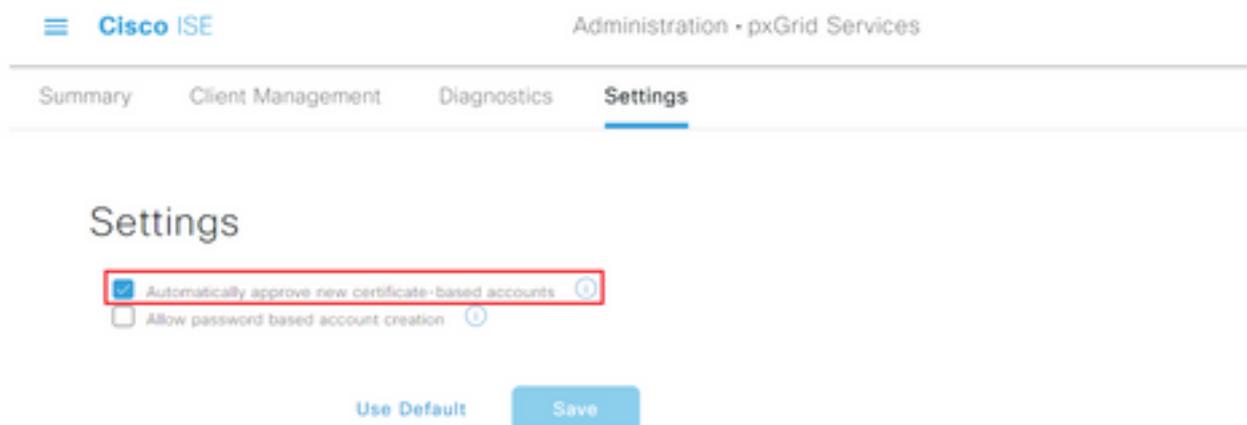


Paso 4. Desplácese hacia abajo y haga clic en **Guardar**.

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**.



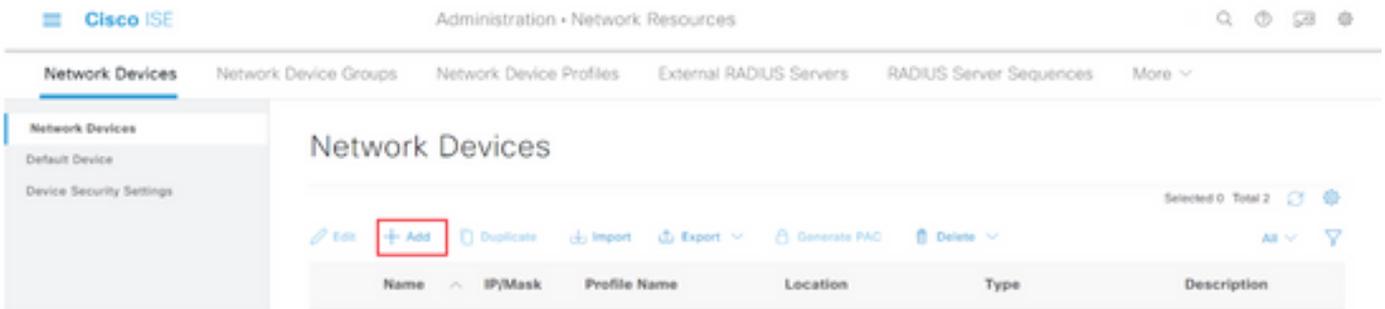
Paso 3. Haga clic en **Save (Guardar)**.

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.

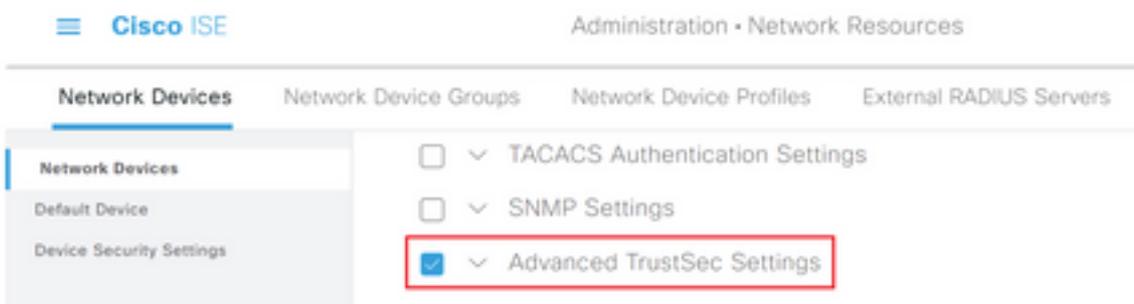
Paso 1. Navegue hasta las tres líneas ubicadas en la esquina superior izquierda y seleccione en **Administración > Recursos de red > Dispositivos de red**.

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

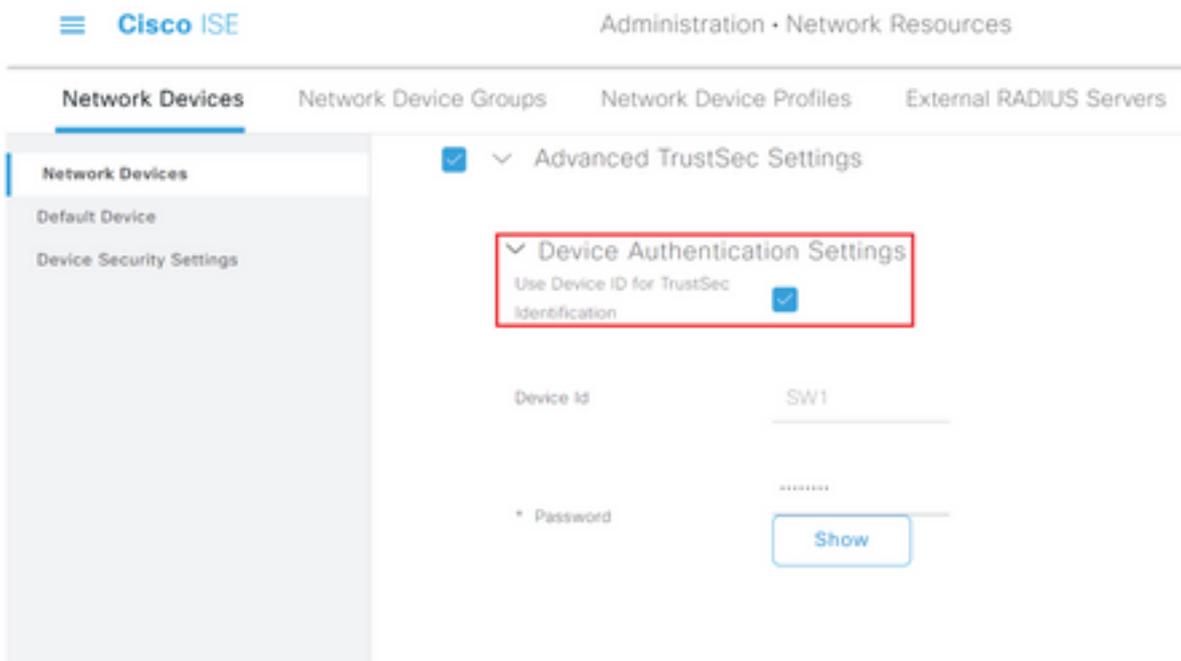


Paso 3. Ingrese la información requerida en la sección **Dispositivos de Red** y en **Configuración de Autenticación RADIUS**.

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

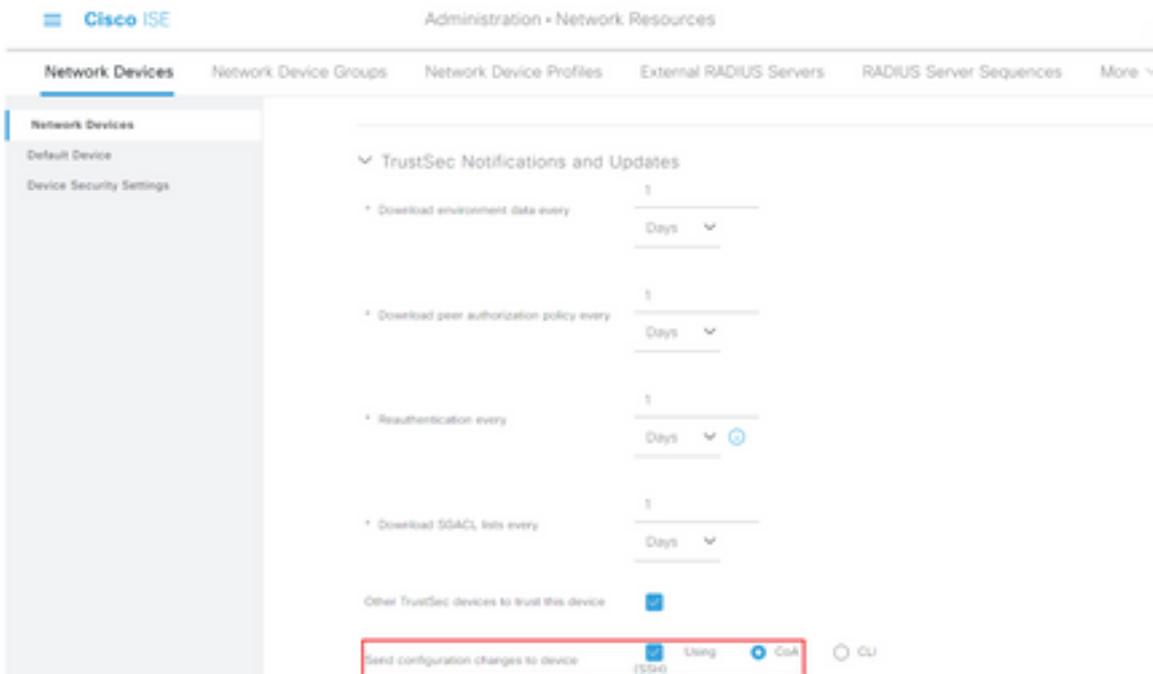


Paso 5. Haga clic en la casilla de verificación **Usar ID de dispositivo para la identificación TrustSec** para rellenar automáticamente el nombre de dispositivo que aparece en la sección **Dispositivos de red**. Introduzca una contraseña en el campo **Password**.



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**.

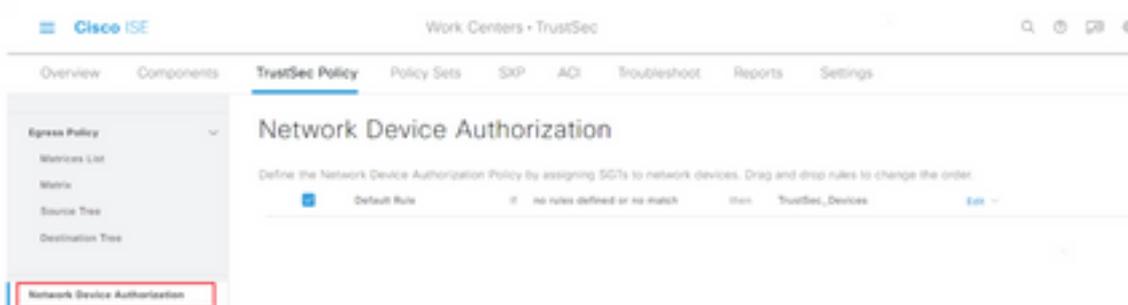
Paso 8. Para permitir que ISE edite la configuración del dispositivo de red, ingrese las credenciales de usuario en los campos **Nombre de usuario del modo EXEC** y **Contraseña del modo EXEC**. Opcionalmente, proporcione enable password en el campo **Enable Mode Password**.

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

Autorización de dispositivo de red

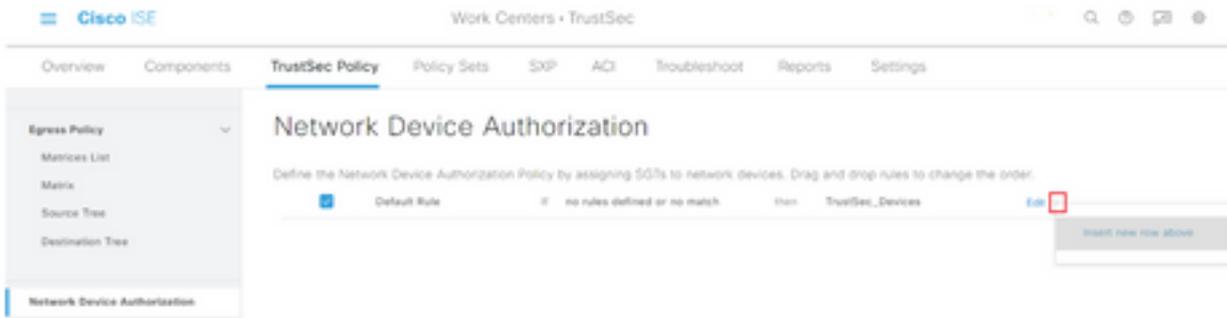
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centros de trabajo > TrustSec > Política TrustSec**.

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



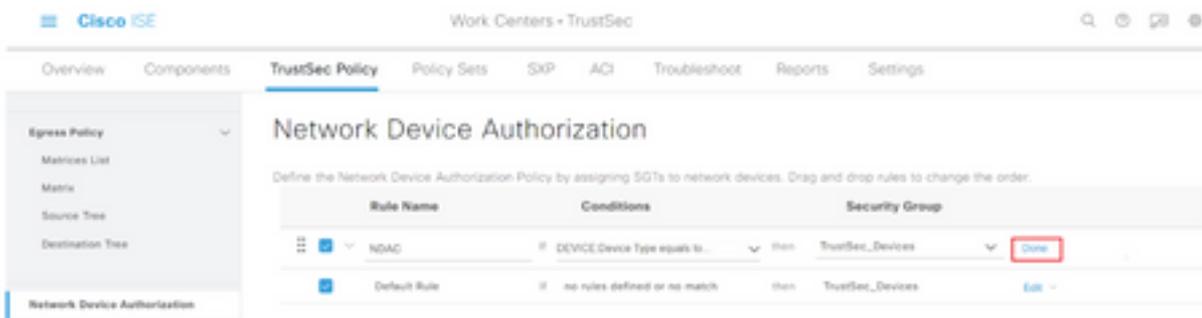
Paso 3. A la derecha, utilice el menú desplegable situado junto a **Editar** e **Insertar nueva fila arriba**

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.



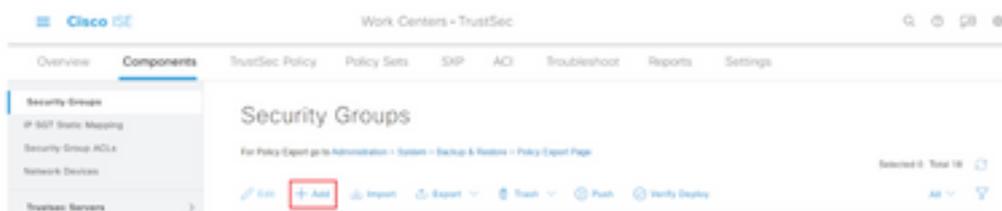
Paso 6. Desplácese hacia abajo y haga clic en **Guardar**.

SGT

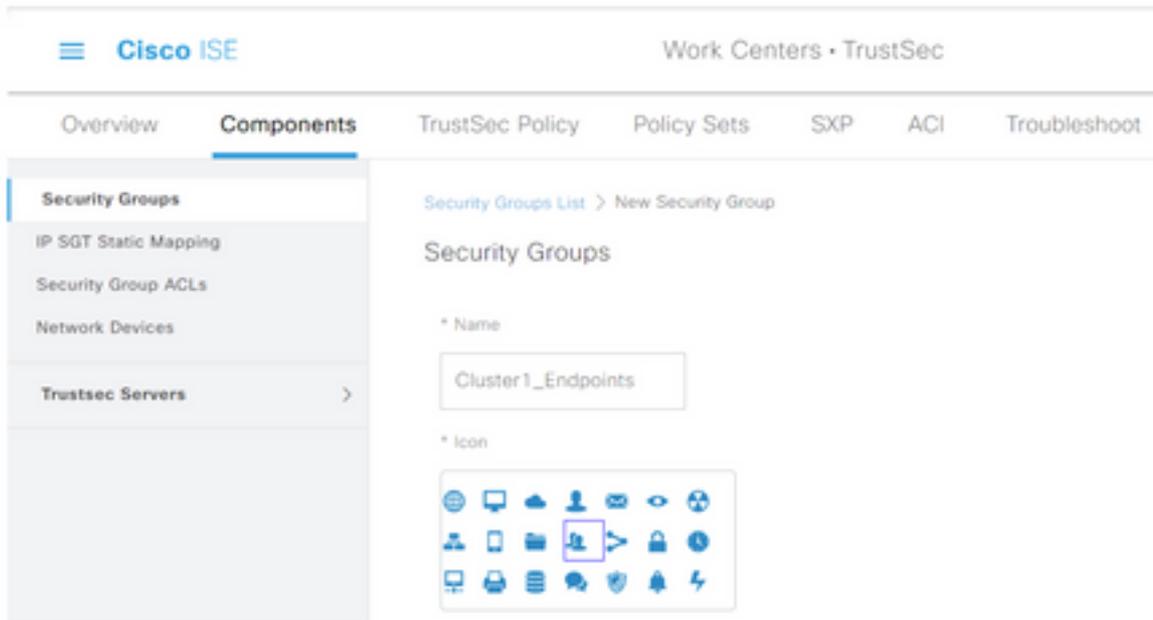
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione en **Centros de trabajo > TrustSec > Componentes**.

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**

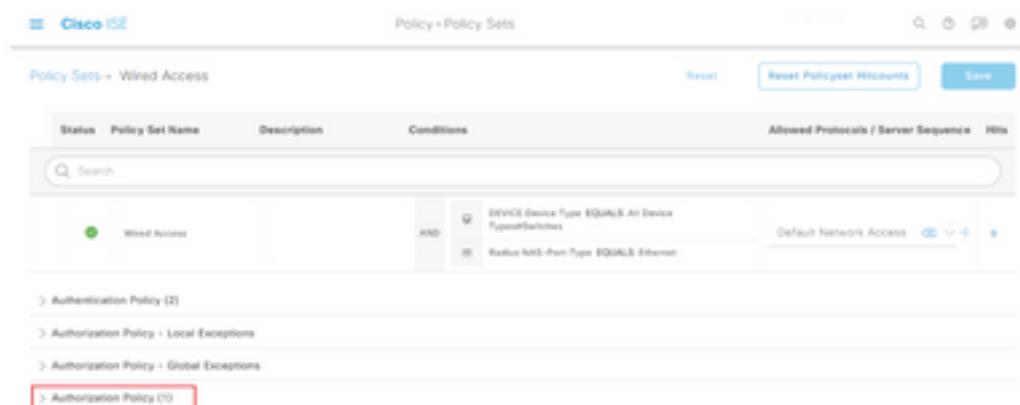
Nota: Repita estos pasos para todas las SGT necesarias.

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.

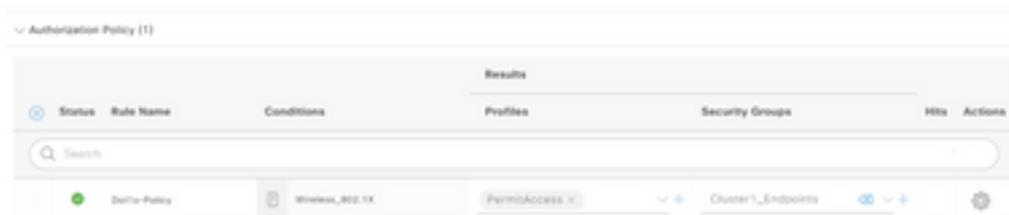
Paso 3. Dentro del conjunto de políticas, expanda la **Política de autorización**.



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**.



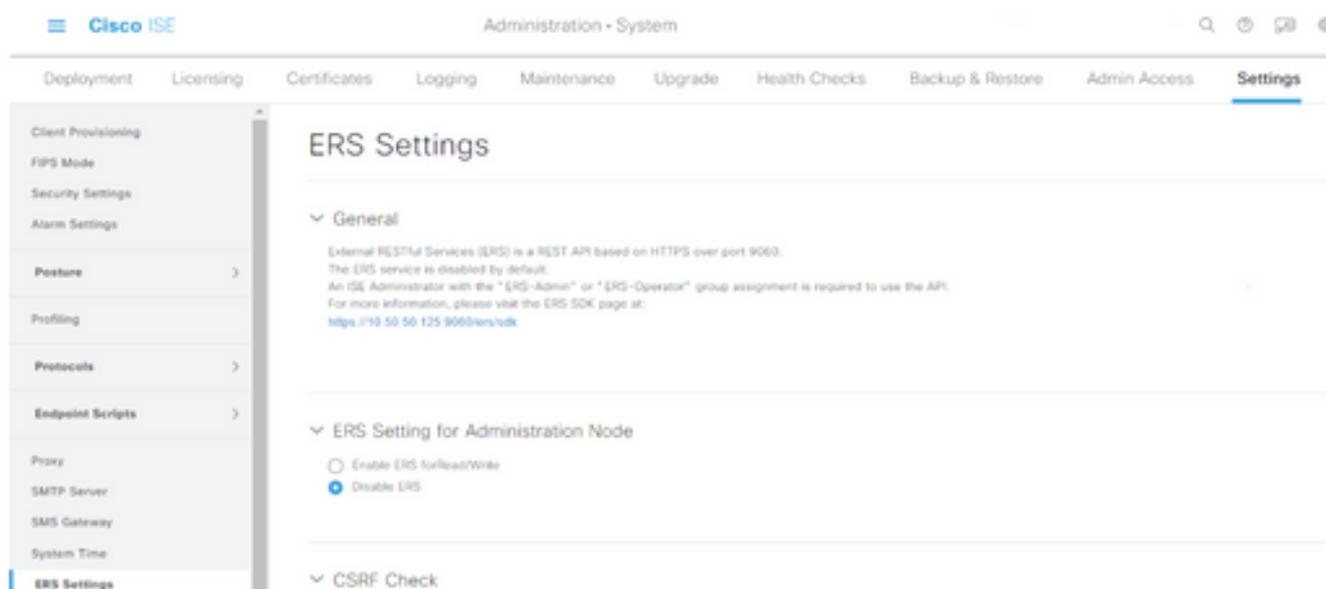
Paso 6. Click **Save**.

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)**.

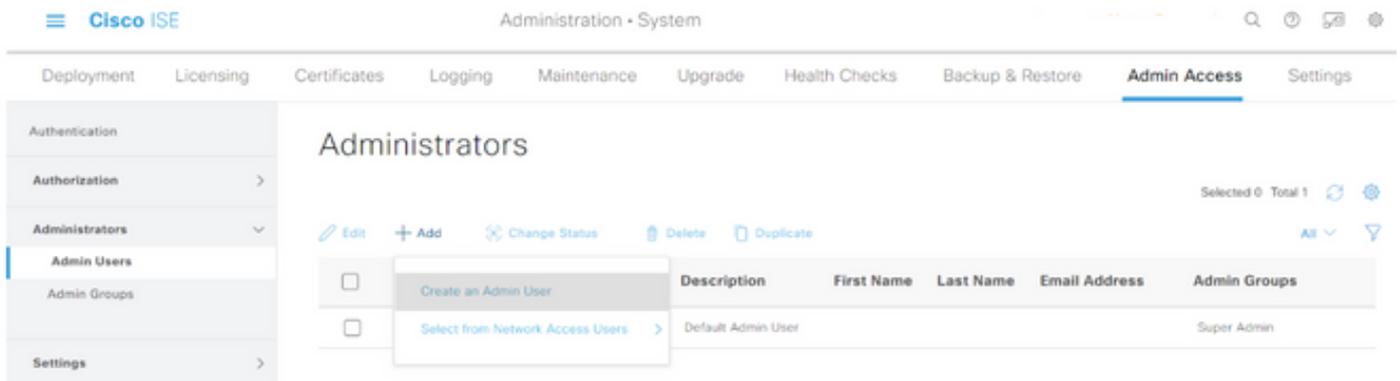
Paso 4. Haga clic en **Guardar** y confirme con **Aceptar**.

Agregar usuario al grupo de administración ESR (opcional)

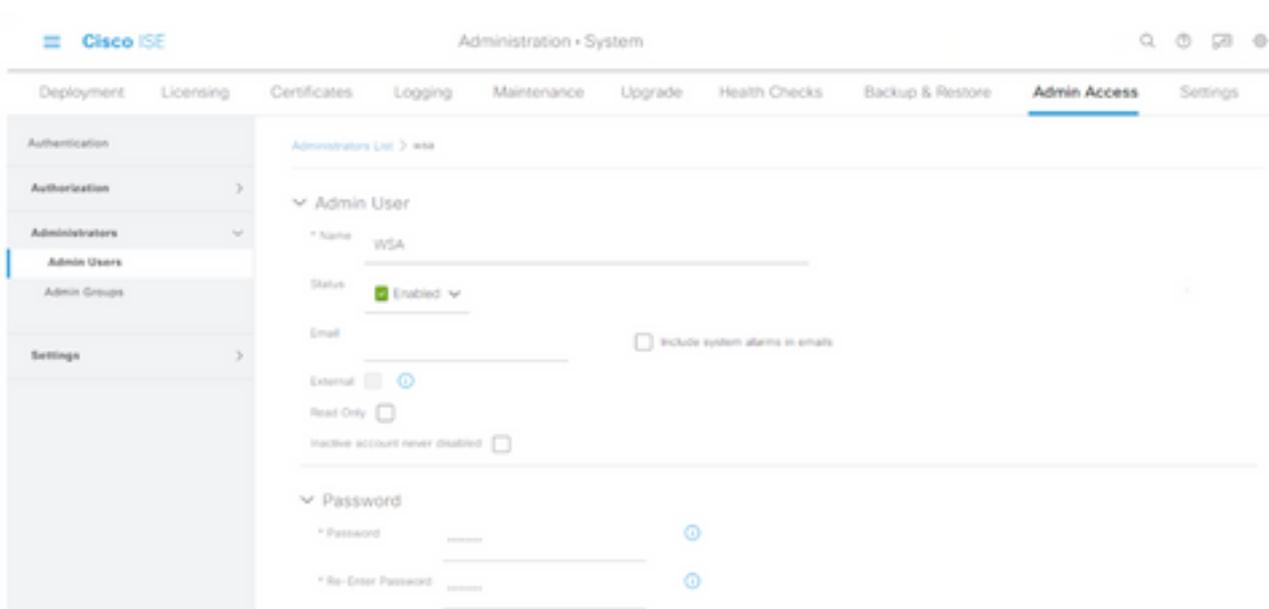
Paso 1. Seleccione el icono de tres líneas situado en la esquina superior izquierda y seleccione **Administration > System > Admin Access**

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

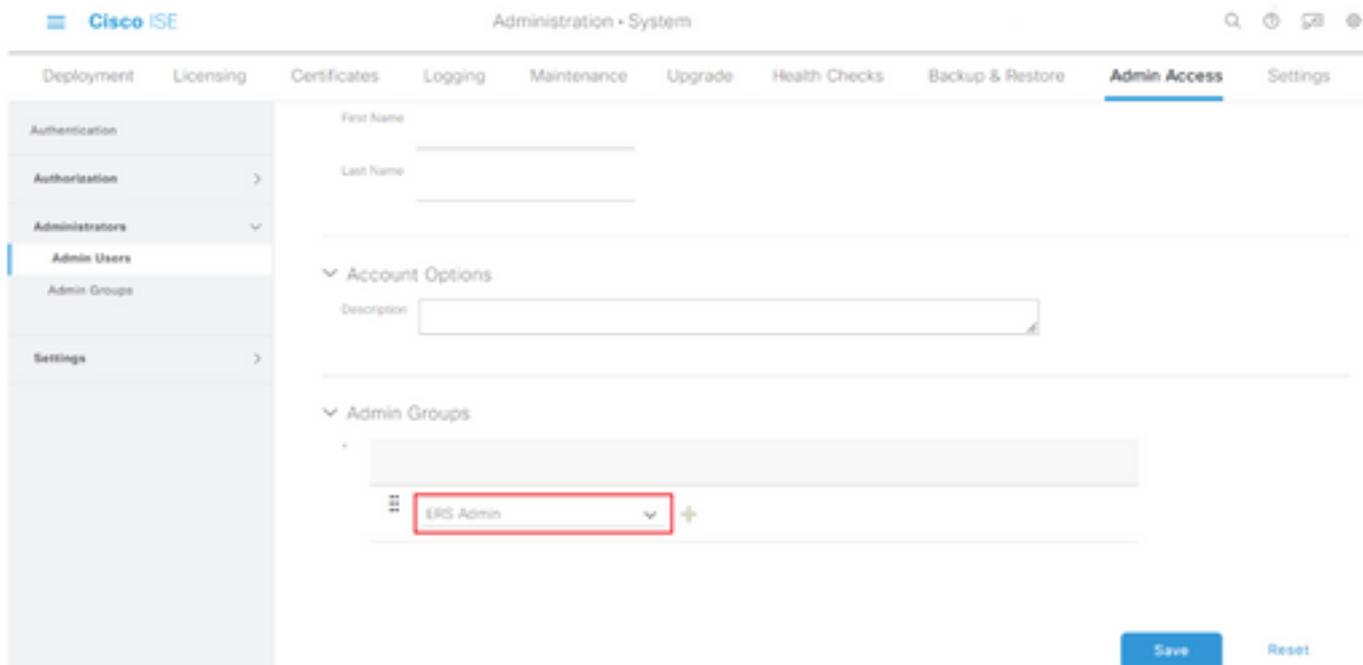
Paso 3. Haga clic en **+Add** y seleccione **Admin User** en la lista desplegable.



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**.



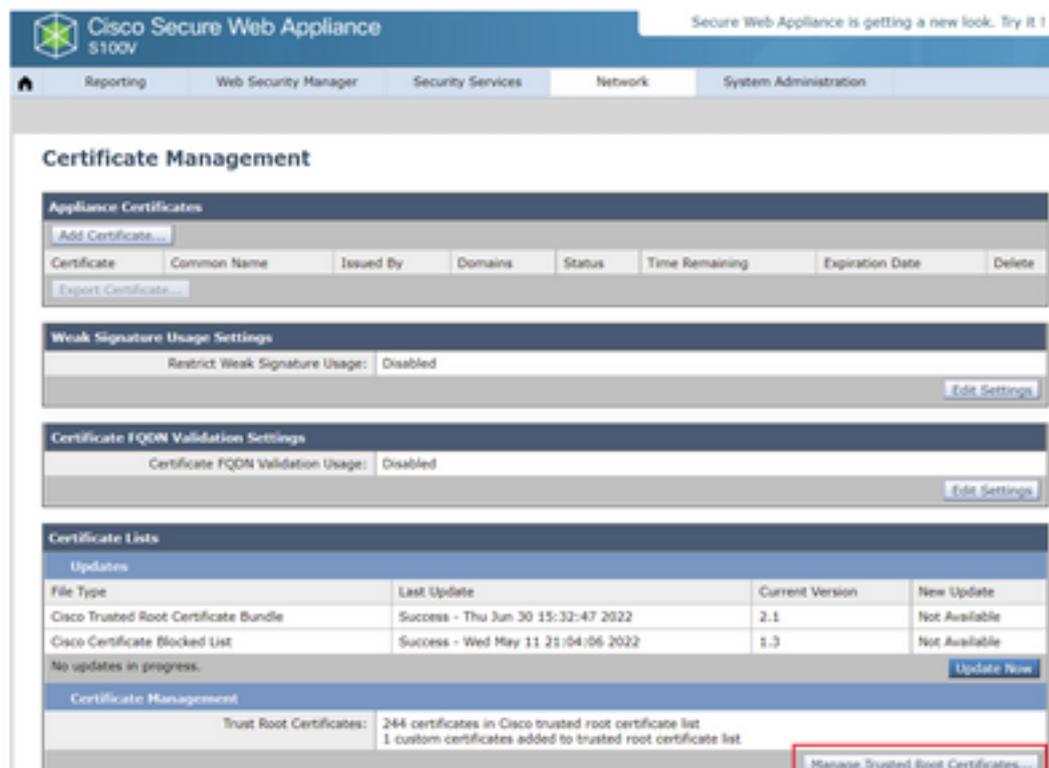
Paso 6. Click Save.

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.

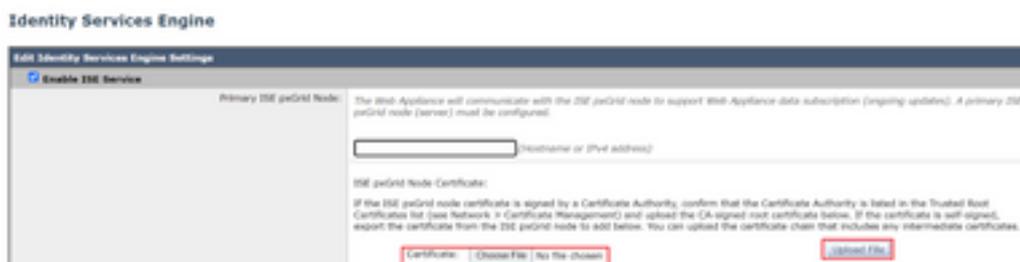
Certificado pxGrid

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**.

Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

Use Uploaded Certificate and Key

Certificate: No file chosen

Key: No file chosen

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key

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

Generate Certificate and Key

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: Set X509v3 Basic Constraints Extension to Critical

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.

Web Appliance Client Certificate: For secure communication between the Web Appliance and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.

Use Uploaded Certificate and Key

Certificate:

Key:

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key

Common name: wsa.securitylab.net
 Organization: Cisco
 Organizational Unit: Security
 Country: SE
 Expiration Date: May 10 19:19:26 2024 GMT
 Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate:

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.

ISE SOAP Exchange Protocol (SXP) Service: Enabling the service, Web Appliance will retrieve SXP Binding Topic from ISE Services.

Enable ISE External Restful Service (ERS)

The Web Appliance retrieves Active Directory groups, and local ISE groups from ISE using the ERS. If you are configuring the Web Appliance's policies using Active Directory groups, or in combination with Secure Group Page (SGP), you should enable 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.

Enable ISE External Restful Service (ERS)

ERS Administrator Credentials

Username:

Password:

ERS Servers

Server name same as ISE pxGrid Node

Primary: (Hostname or IPv4 address)

Secondary (Optional): (Hostname or IPv4 address)

Port: (Enter the port number specified for ERS in ISE)

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**.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

Enable Identification Profile

Name:
(e.g. my ISE Profile)

Description:
(Maximum allowed characters 256)

Insert Above:

User Identification Method

Identification and Authentication:

Fallback to Authentication Realm or Guest Privileges:

Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:
(examples: 20.1.1.0, 20.1.1.0/24, 20.1.1.1-10, 2001:420:80:2::5, 2000:db8::1-2000:db8::68)

Define Members by Protocol: HTTP/HTTPS

[Advanced](#) Define additional group membership criteria.

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.

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: ISE Profile

Authorized Users and Groups: Selected Groups and Users (2)
ISE Secure Group Tags: No tags entered
ISE Groups: No groups entered
Users: No users entered

All Authenticated Users

Guests (users failing authentication)

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Advanced Define additional group membership criteria.

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.**

Use the search function below to add Secure Group Tags. To remove Secure Group Tags from this policy, use the Delete option.

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	<input type="checkbox"/>

Delete

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Search

0 Secure Group Tag(s) selected for Add

Secure Group Tag Name	SGT Number	SGT Description	Select
Production_Servers	11	Production Servers Security Group	<input type="checkbox"/>
Point_of_Sale_Systems	10	Point of Sale Security Group	<input type="checkbox"/>
Test_Servers	13	Test Servers Security Group	<input type="checkbox"/>
Development_Servers	12	Development Servers Security Group	<input type="checkbox"/>
BYOD	15	BYOD Security Group	<input type="checkbox"/>
PCI_Servers	14	PCI Servers Security Group	<input type="checkbox"/>
Guests	6	Guest Security Group	<input type="checkbox"/>
ANY	65535	Any Security Group	<input type="checkbox"/>
Unknown	0	Unknown Security Group	<input type="checkbox"/>
Network_Services	3	Network Services Security Group	<input type="checkbox"/>
TrustSec_Devices	2	TrustSec Devices Security Group	<input type="checkbox"/>
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	<input checked="" type="checkbox"/>
Employees	4	Employee Security Group	<input type="checkbox"/>

Add

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:



Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
10.14.2022.02:07:46.56.	14.02.02.	IP-Device	Word Access --> 0.	Word Access --> 0.	PermitAccess	10.50.50.12	Cluster1_EdgePorts	ise01-cl1

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



Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
10.14.2022.02:08:47.21.	14.02.02.	Microsoft-Work	Word Access --> 0.	Word Access --> 0.	PermitAccess	10.50.50.12	Cluster2_EdgePorts	ise01-cl1

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:

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PDNs Involved
10.50.50.112	TrustSec_Device (20000)		10.50.50.121_10.50.50.0	SXP	default	10.50.50.0
10.50.50.112	TrustSec_Device (20000)		10.50.50.122_10.50.50.7	SXP	default	10.50.50.0
10.50.50.121	Cluster1_Endpoints (1110000)		10.50.50.121_10.50.50.0	SXP	default	10.50.50.0
10.50.50.122	Cluster1_Endpoints (2220000)		10.50.50.122_10.50.50.7	SXP	default	10.50.50.0

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

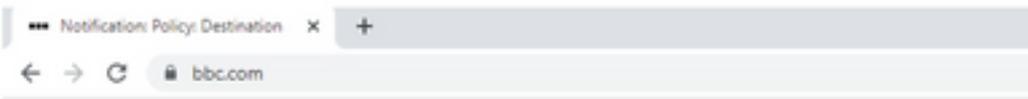
```
wsa2.securitylab.net> lisedata
Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTs - Show the ISE Secure Group Tag (SGT) table.
- GROUPS - Show the ISE Groups table.
[>] cache

Choose the operation you want to perform:
- SHOW - Show the ISE IP cache.
- CHECKIP - Query the local ISE cache for an IP address
[>] show
IP                username                                     SGT#  Port Range
10.50.50.13       isesxp_10.50.50.122_sgt222_10.50.50.13    222   -
10.50.50.12       isesxp_10.50.50.121_sgt111_10.50.50.12    111   -
```

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



This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site (<https://bbc.com/>) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

```
Date: Thu, 14 Jul 2022 14:28:16 CEST
Username: isesxp_10.50.50.121_sgt111_10.50.50.12
Source IP: 10.50.50.12
URL: GET https://bbc.com/
Category: Block URLs CL1
Reason: UNKNOWN
Notification: BLOCK_DEST
```

Time (GMT +02:00)	Website (source)	Disposition	Bandwidth	User / Client IP
04 Jul 2022 14:28:17	https://bbc.com/443/television CONTENT TYPE: - URL CATEGORY: Block URLs CL1 DESTINATION IP: DETAILS: Decryption Policy: 'ISE_Cluster1', WBARs: No Score, Malware Analytics File Verdict: -	Block - URL Cat	0B	isesxp_10.50.50.121_sgt111_10.50.50.12 (Identified by ISE) 10.50.50.12

Extremo que pertenece al ISE Cluster 2



This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site (https://www.facebook.com/) has been blocked.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Thu, 14 Jul 2022 14:23:58 CEST
Username: isesxp_10.50.50.122_sgt222_10.50.50.13
Source IP: 10.50.50.13
URL: GET https://www.facebook.com/
Category: Block URLs CL2
Reason: UNKNOWN
Notification: BLOCK_DEST

Time (GMT +02:00)	Website (count)	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:23:58	https://www.facebook.com/43/revision.js CONTENT TYPE: ... URL CATEGORY: Block URLs CL2 DESTINATION IP: ... REASON: DenyList Policy: 'ISE_Cluster2', WBS: No Score, Malware Analysis File Verdict: ...	Block - URL Cat	0B	isesxp_10.50.50.122_sgt222_10.50.50.13 (Identified by ISE) 10.50.50.13

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](#)