

Integre vários clusters ISE com o Secure Web Appliance para políticas baseadas em TrustSec

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Limitações](#)

[Diagrama de Rede](#)

[Configurar](#)

[Configuração do ISE](#)

[Habilitar SXP](#)

[Configurar o SXP nos nós do cluster](#)

[Configurar o SXP no nó de agregação](#)

[Ativar o pxGrid no nó de agregação](#)

[Aprovação automática do pxGrid](#)

[Configurações do TrustSec dos dispositivos de rede](#)

[Autorização de dispositivo de rede](#)

[SGT](#)

[Política de Autorização](#)

[Ativação do ERS no nó de agregação do ISE \(opcional\)](#)

[Adicionar usuário ao grupo ESR Admin \(Opcional\)](#)

[Configuração segura de dispositivo da Web](#)

[Certificado pxGrid](#)

[Ativar SXP e ERS no Secure Web Appliance](#)

[Perfil de identificação](#)

[Política de descryptografia baseada em SGT](#)

[Configuração do Switch](#)

[AAA](#)

[TrustSec](#)

[Verificar](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve o procedimento para enviar informações de Security Group Tag (SGT) de várias implantações do ISE para um único Cisco Secure Web Appliance (Formalmente Web Security Appliance WSA) através do pxGrid para aproveitar as políticas de acesso à Web baseadas em SGT em uma implantação do TrustSec.

Antes da versão 14.5, o Secure Web Appliance só pode ser integrado a um único cluster do ISE para políticas de identidade baseadas em SGT. Com a introdução dessa nova versão, o Secure

Web Appliance agora pode interoperar com informações de vários clusters do ISE com um nó separado do ISE que se agrega entre eles. Isso traz grandes benefícios e nos permite exportar dados de usuários de diferentes clusters do ISE e a liberdade de controlar o ponto de saída que um usuário pode usar sem a necessidade de uma integração de 1:1.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity services engine (ISE)
- Dispositivo da Web seguro
- protocolo RADIUS
- TrustSec
- pxGrid

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

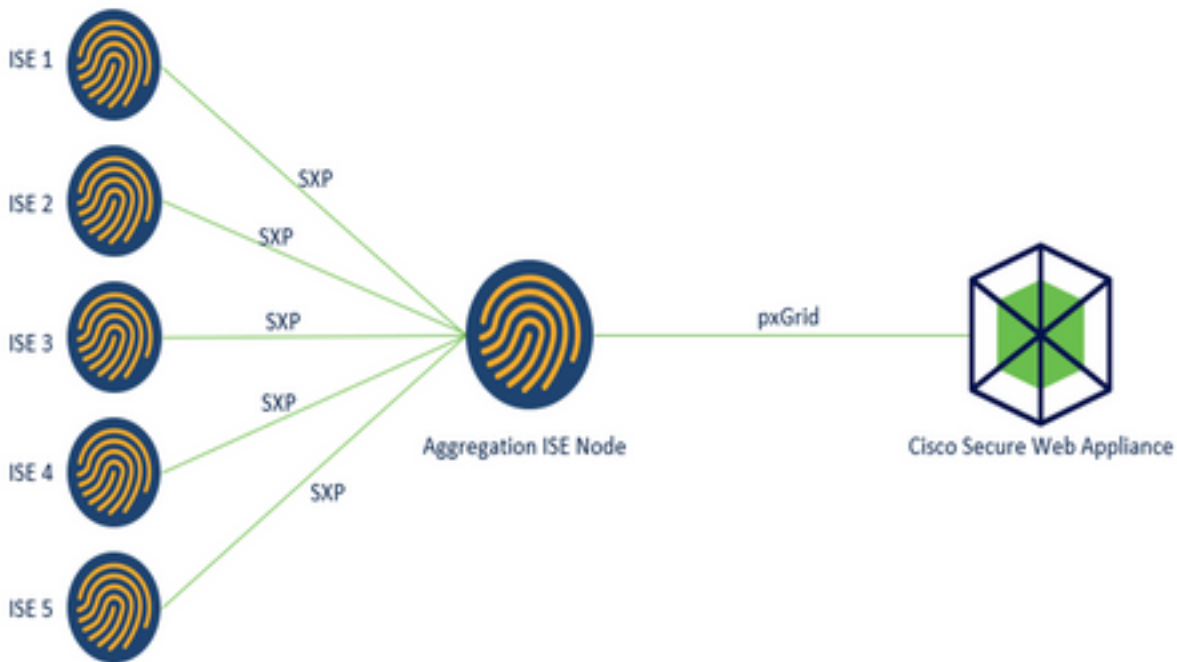
- Secure Web Appliance 14.5
- ISE versão 3.1 P3

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Limitações

1. Todos os clusters do ISE precisam manter mapeamentos uniformes para SGTs.
2. O nó de agregação do ISE deve ter o nome/número de SGTs do restante dos clusters do ISE.
3. O Secure Web Appliance só pode identificar a política (Acesso/Descritografia/Roteamento) com base na tag SGT e não no grupo nem no nome de usuário.
4. Relatórios e rastreamento são baseados em SGT.
5. Os parâmetros de dimensionamento do ISE/Secure Web Appliance existentes continuam a ser aplicados a este recurso.

Diagrama de Rede



Processo:

1. Quando o usuário final se conecta à rede, ele recebe um SGT baseado em políticas de autorização no ISE.
2. Em seguida, os diferentes clusters do ISE enviam essas informações de SGT na forma de mapeamentos de SGT-IP para o nó de agregação do ISE por meio do SXP.
3. Nó de agregação do ISE recebe essas informações e compartilha-as com o único Secure Web Appliance por meio do pxGrid.
4. O Secure Web Appliance usa as informações de SGT que aprendeu para fornecer acesso aos usuários com base nas Políticas de Acesso à Web.

Configurar

Configuração do ISE

Habilitar SXP

Etapa 1. Selecione o ícone de três linhas  localizado no canto superior esquerdo e selecione **Administration > System > Deployment**.

Etapa 2. Selecione o nó que deseja configurar e clique em **Editar**.

The screenshot shows the Cisco ISE Administration - System interface. The 'Deployment' tab is active. On the left, there is a navigation pane with 'Deployment' and 'PAN Failover' options. The main area displays 'Deployment Nodes' with a table containing one node: 'ise01-CL1'. Above the table, there are buttons for 'Edit', 'Register', 'Syncup', and 'Deregister'. The 'Edit' button is highlighted with a red box.

Hostname	Personas	Role(s)	Services	Node Status
ise01-CL1	Administration, Monitoring, Policy Service	STANDALONE	SESSION PROFILER	✔

Etapa 3. Para ativar o SXP, marque a caixa **Ativar serviço SXP**

The screenshot shows the 'Enable Session Services' configuration page in Cisco ISE Administration - System. The 'Enable SXP Service' checkbox is checked and highlighted with a red box. Other options include 'Enable Profiling Service' (checked) and 'Enable Threat Centric NAC Service' (unchecked). The 'Use Interface' is set to 'GigabitEthernet 0'.

Etapa 4. Role para baixo e clique em **Save**

Note: Repita todas as etapas para o restante dos nós do ISE em cada cluster, incluindo o nó de agregação.

Configurar o SXP nos nós do cluster


Etapa 1. Selecione o ícone de três linhas  localizado no canto superior esquerdo e selecione em **Centro de trabalho > TrustSec > SXP**.

Etapa 2. Clique em **+Add** para configurar o nó de agregação do ISE como um par do SXP.

The screenshot shows the Cisco ISE Work Centers - TrustSec interface. The 'SXP' tab is active. The main area displays 'SXP Devices' with a table. Below the table, there are buttons for 'Refresh', '+Add', 'Trash', 'Edit', and 'Assign SXP Domain'. The '+Add' button is highlighted with a red box.

Etapa 3. Defina o **Nome** e o **endereço IP** do nó de agregação do ISE, selecione peer role como

LISTENER. Selecione PSNs necessários em **Connected PSNs**, obrigatório **SXP Domains**, selecione **Enabled** em status e, em seguida, selecione **Password Type** e required **Version**.

 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

Etapa 4. Clique em **Salvar**

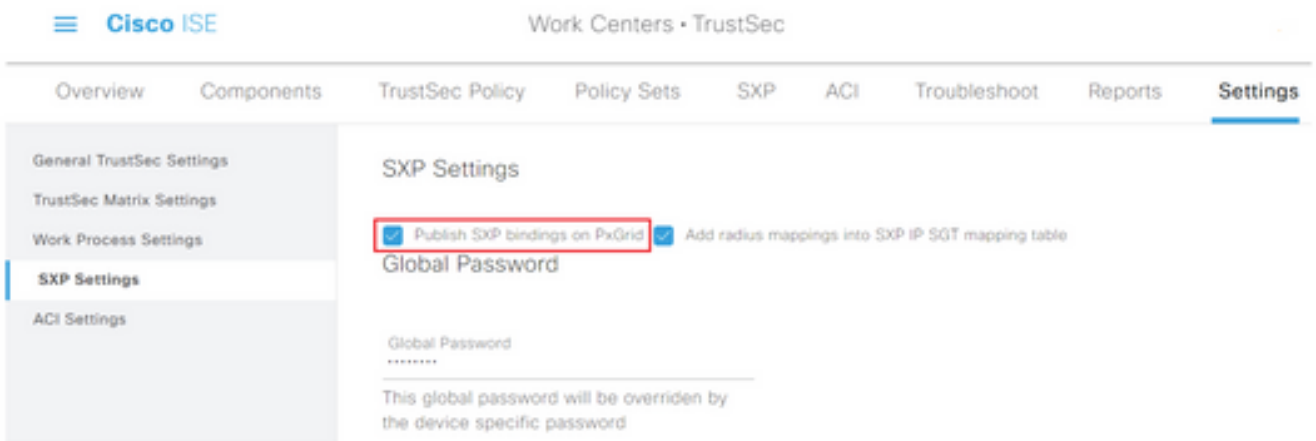
Note: Repita todas as etapas para o restante dos nós do ISE em cada cluster para criar uma conexão SXP com o nó de agregação. **Repita o mesmo processo no nó de agregação e selecione ALTO-FALANTE como função de peer.**

Configurar o SXP no nó de agregação

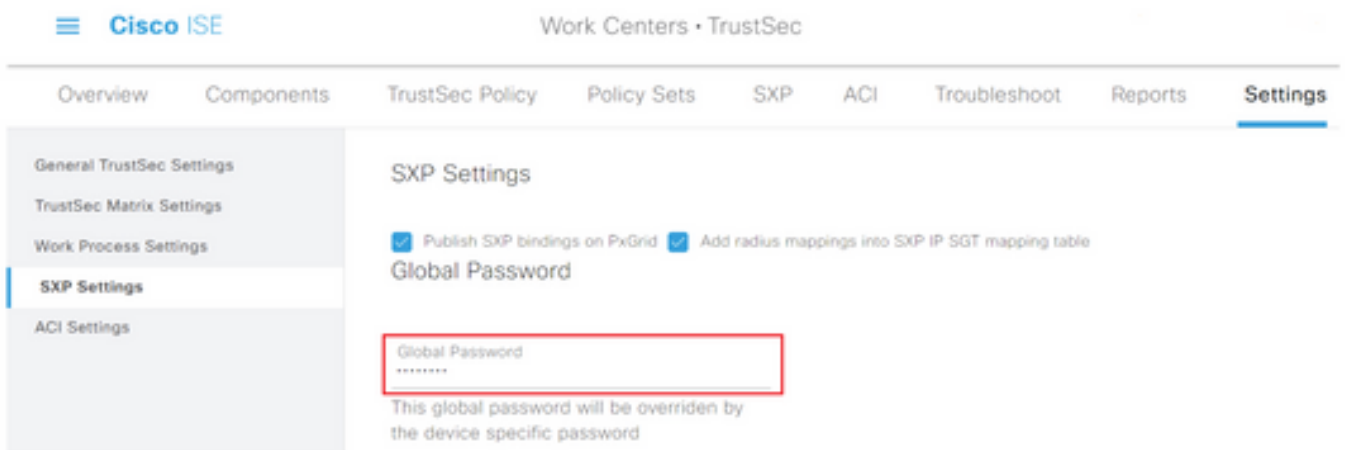
Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Work Center > TrustSec > Settings**

Etapa 2. Clique na guia **Configurações do SXP**

Etapa 3. Para propagar os mapeamentos IP-SGT, marque a caixa de seleção **Publicar vinculações SXP no pxGrid.**



Etapa 4 (opcional). Defina uma senha padrão para as configurações do SXP em **Senha global**

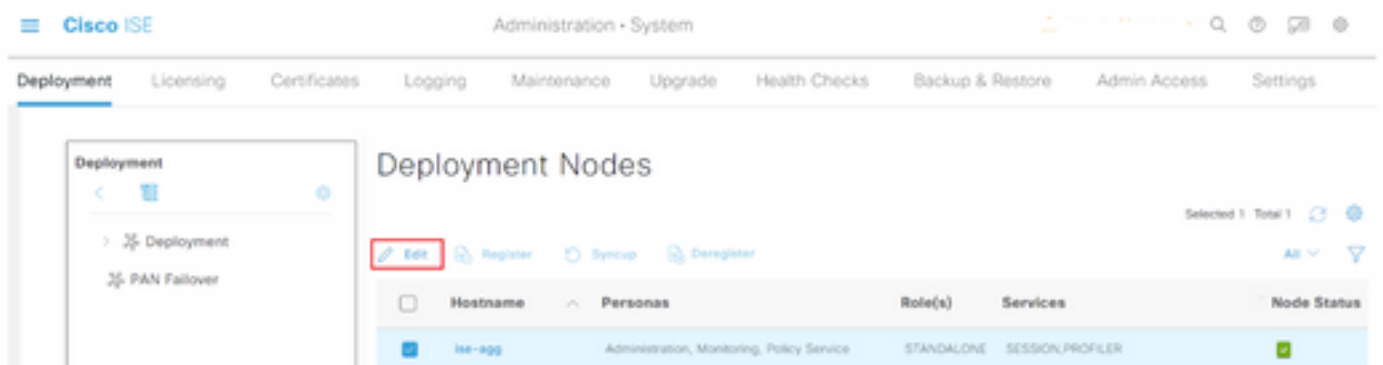


Etapa 5. Role para baixo e clique em **Salvar**.

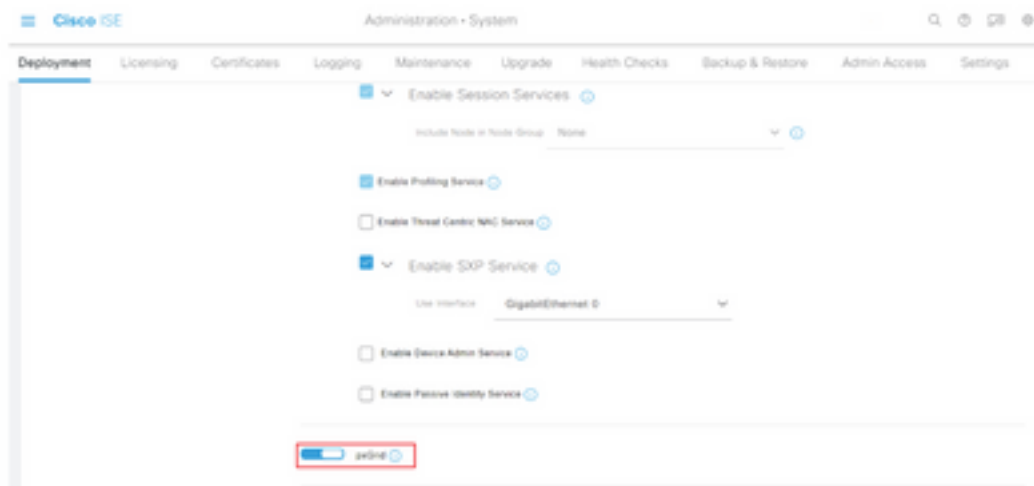
Ativar o pxGrid no nó de agregação

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Administração > Sistema > Implantação**.

Etapa 2. Selecione o nó que deseja configurar e clique em **Editar**.



Etapa 3. Para ativar o pxGrid, clique no botão ao lado de **pxGrid**.

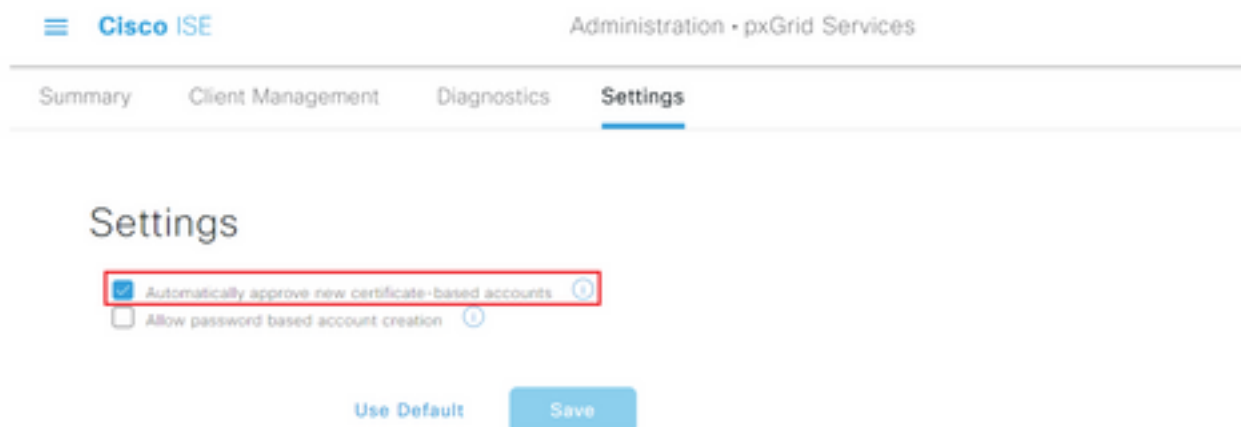


Etapa 4. Role para baixo e clique em **Save**.

Aprovação automática do pxGrid

Etapa 1. Navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione **Administration > pxGrid Services > Settings**.

Etapa 2. Por padrão, o ISE não aprova automaticamente o pxGrid para as solicitações de conexão de novos clientes pxGrid; portanto, você deve habilitar essa configuração marcando a caixa de seleção **Aprovar automaticamente novas contas baseadas em certificado**.



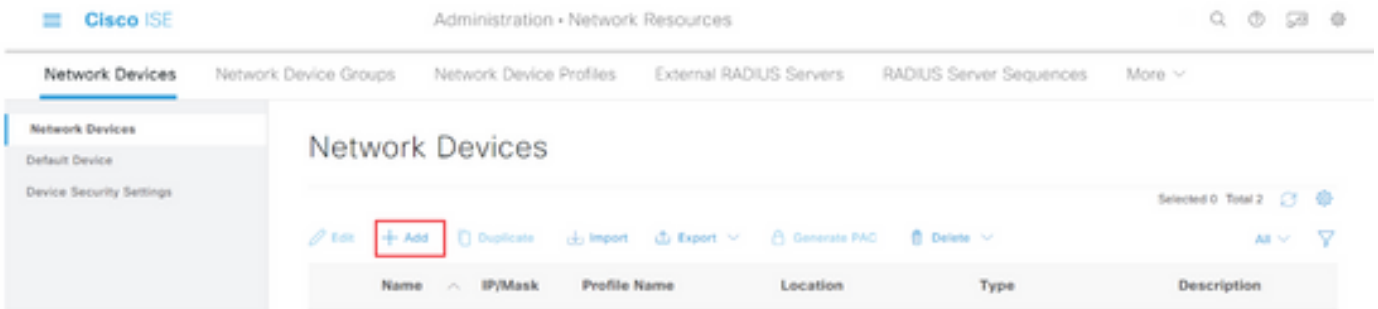
Etapa 3. Clique em **Salvar**

Configurações do TrustSec dos dispositivos de rede

Para que o Cisco ISE processe solicitações de dispositivos habilitados para TrustSec, você deve definir esses dispositivos habilitados para TrustSec no Cisco ISE.

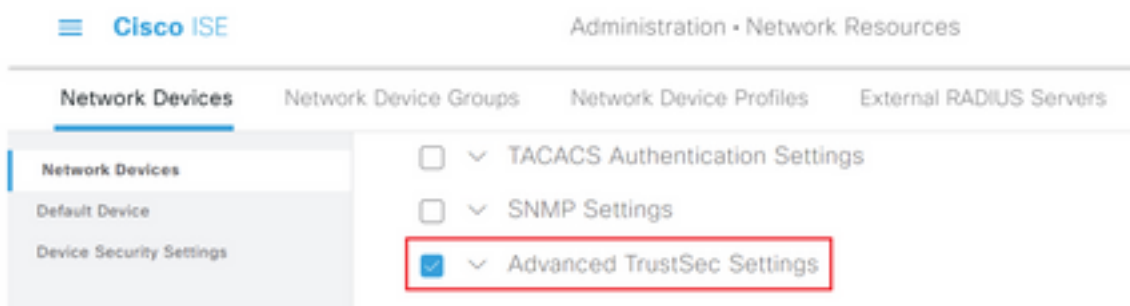
Etapa 1. Navegue até o ícone de três linhas localizado no canto superior esquerdo e selecione em **Administration > Network Resources > Network Devices**.

Etapa 2. Clique em **+Adicionar**.

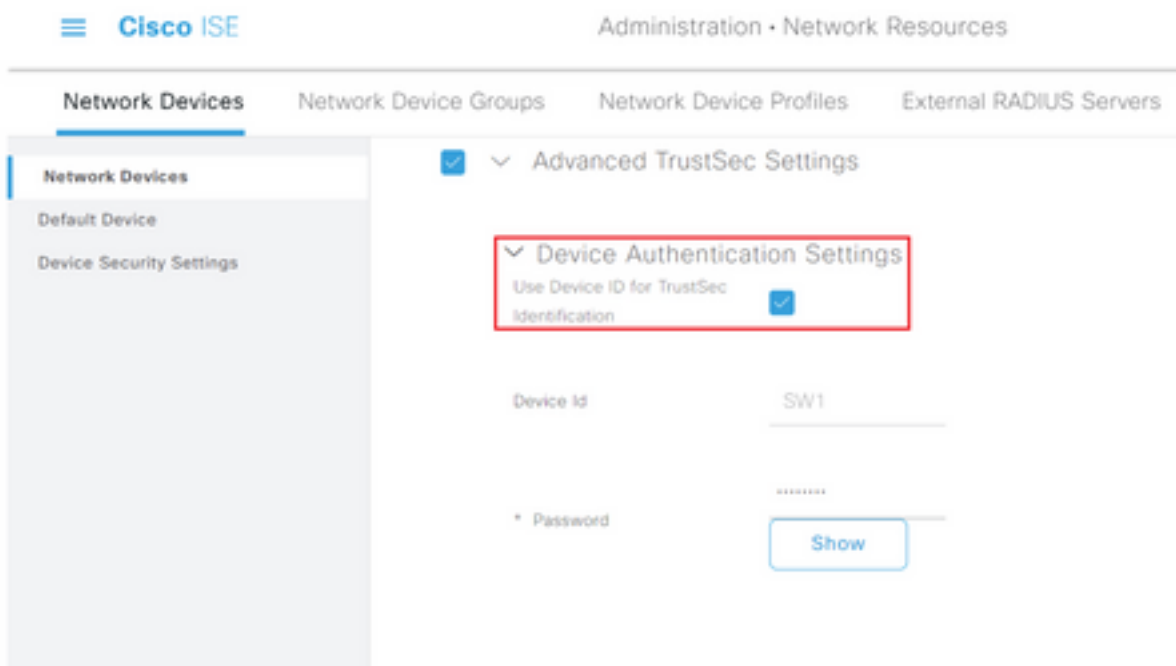


Etapa 3. Insira as informações necessárias na seção **Network Devices** e nas configurações de autenticação **RADIUS**.

Etapa 4. Marque a caixa de seleção **Configurações avançadas do TrustSec** para configurar um dispositivo habilitado para TrustSec.

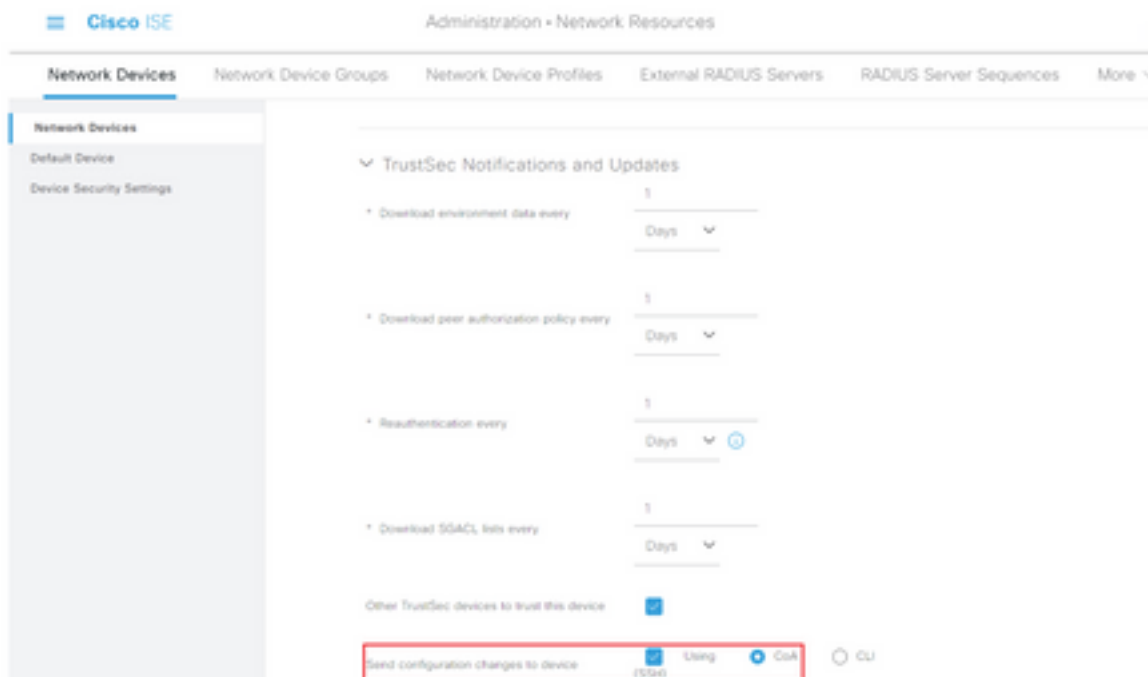


Etapa 5. Clique na caixa de seleção **Use Device ID for TrustSec Identification** para preencher automaticamente o nome do dispositivo listado na seção **Network Devices** . Digite uma senha no campo **Senha**.



Note: A ID e a senha devem corresponder ao comando "cts credentials id <ID> password <PW>" que é configurado posteriormente no switch.

Etapa 6. Marque a caixa de seleção **Send configuration changes to device** para que o ISE possa enviar notificações de TrustSec CoA para o dispositivo.



Etapa 7. Marque a caixa de seleção **Incluir este dispositivo ao implantar atualizações de mapeamento de tag de grupo de segurança**.

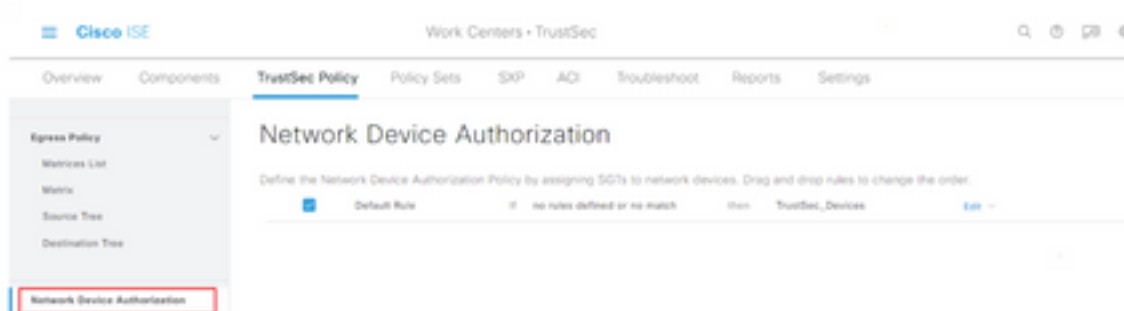
Etapa 8. Para permitir que o ISE edite a configuração do dispositivo de rede, insira as credenciais do usuário nos campos **EXEC Mode Username** e **EXEC Mode Password**. Opcionalmente, forneça a senha de ativação no campo **Senha do modo de ativação**.

Note: Repita as etapas para todos os outros NADs que devem fazer parte do domínio TrustSec.

Autorização de dispositivo de rede

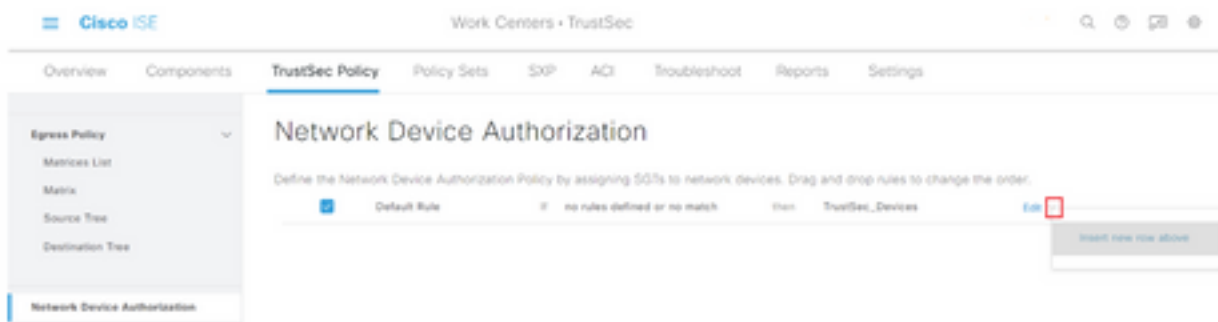
Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Centros de trabalho > TrustSec > Política TrustSec**.

Etapa 2. No painel esquerdo, clique em **Network Device Authorization**.



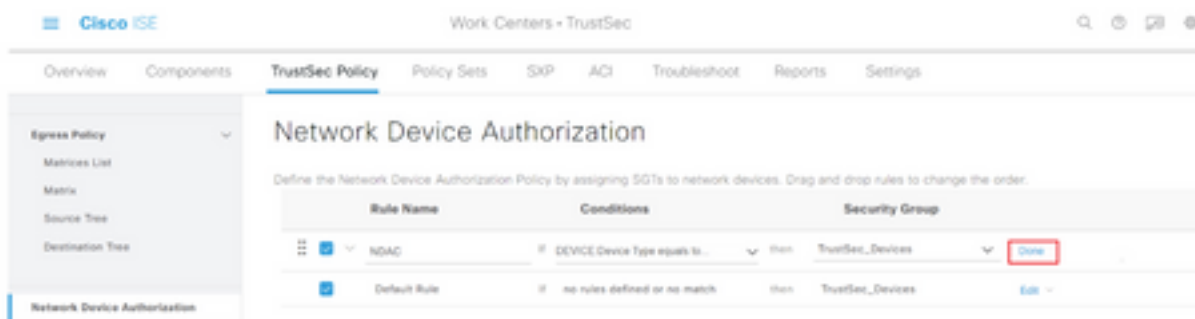
Etapa 3. À direita, use a lista suspensa ao lado de **Edit** e **Insert new row above** para criar uma

nova regra NDA.



Etapa 4. Defina um **Nome da regra**, **Condições** e selecione o SGT apropriado na lista suspensa em **Grupos de segurança**.

Etapa 5. Clique em **Concluído** à direita.



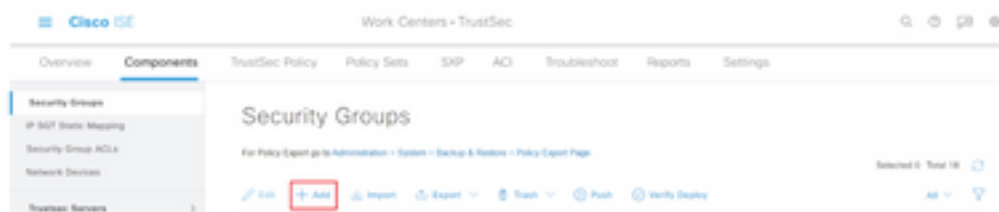
Etapa 6. Role para baixo e clique em **Salvar**.

SGT

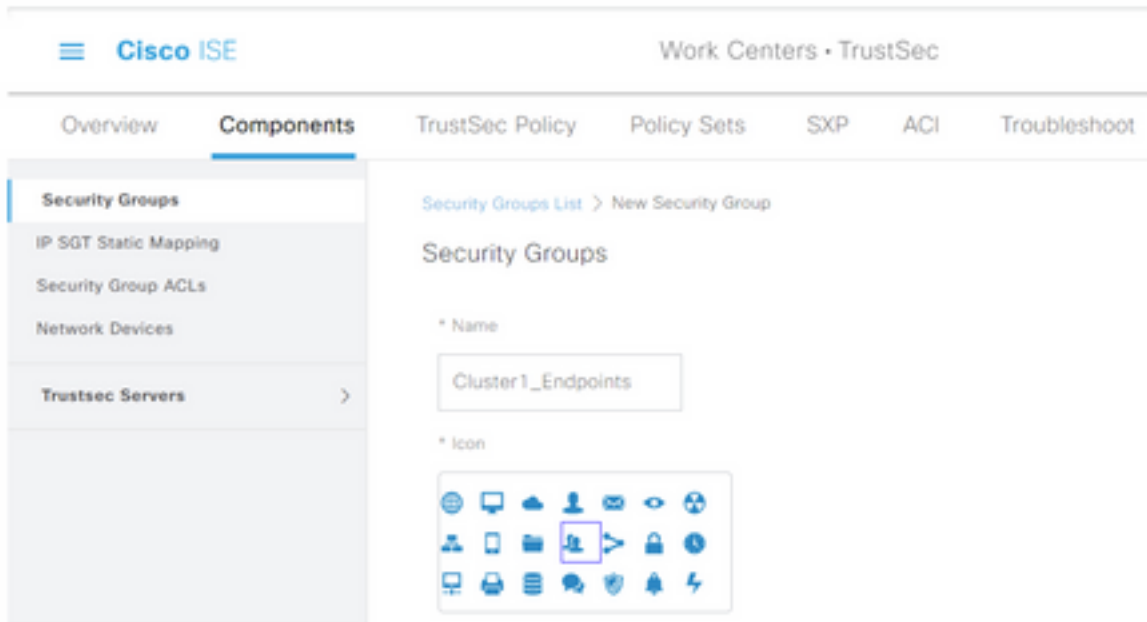
Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Centros de trabalho > TrustSec > Componentes**.

Etapa 2. No painel esquerdo, expanda **Grupos de segurança**.

Etapa 3. Clique em **+Add** para criar um novo SGT.



Etapa 4. Digite o nome e escolha um ícone nos campos apropriados.



Etapa 5. Se desejar, dê a ele uma descrição e informe um **Valor de Marca**.

Note: Para poder inserir manualmente um valor de tag, navegue até Centros de trabalho > TrustSec > Configurações > Configurações gerais do TrustSec e selecione a opção **O usuário deve inserir o número SGT manualmente em Numeração de tag do grupo de segurança**.

Etapa 6. Role para baixo e clique em **Enviar**

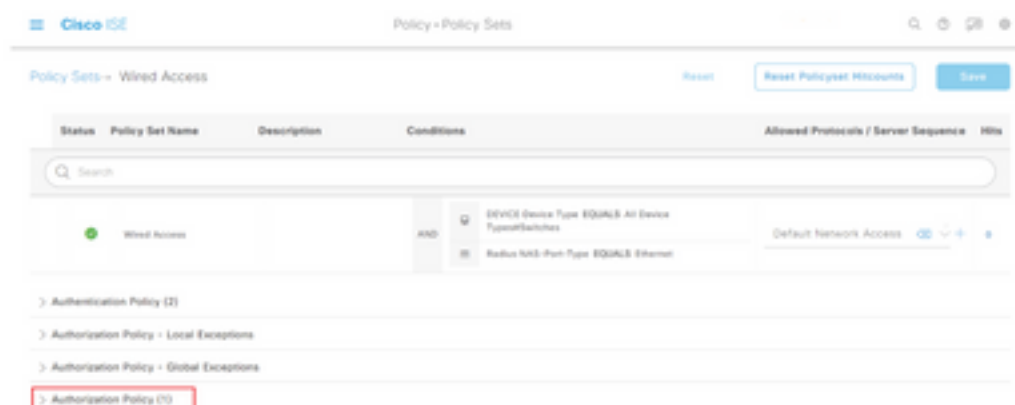
Note: Repita essas etapas para todos os SGTs necessários.

Política de Autorização

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Policy > Policy Sets**.

Etapa 2. Selecione o conjunto de políticas apropriado.

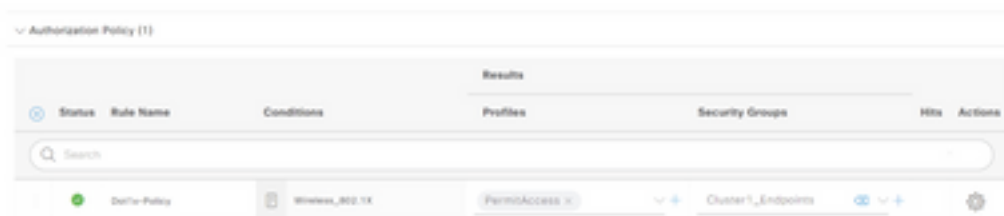
Etapa 3. No conjunto de políticas, expanda a **Política de autorização**.



Etapa 4. Clique no botão  para criar uma **Diretiva de Autorização**.



Etapa 5. Defina o **Nome da regra**, a(s) **condição(ões)** e os **Perfis obrigatórios** e **selecione o SGT apropriado na lista suspensa em Grupos de segurança**.



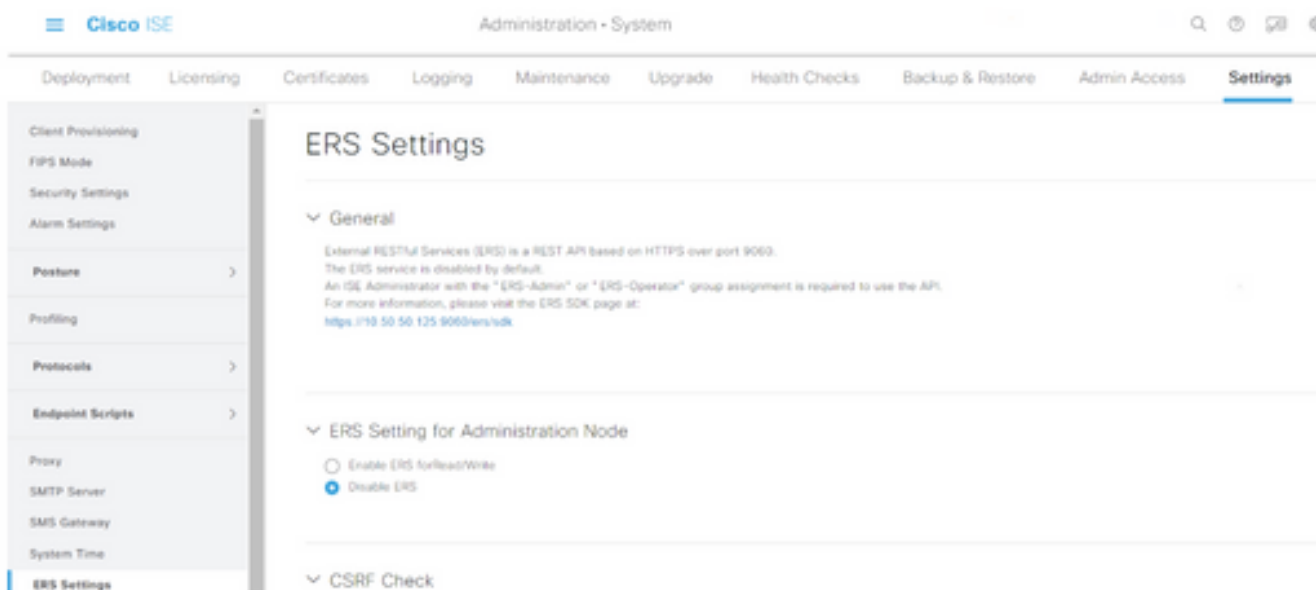
Etapa 6. Clique em **Salvar**.

Ativação do ERS no nó de agregação do ISE (opcional)

O Serviço de API RESTful externo (ERS) é uma API que pode ser consultada pelo WSA para obter informações de grupo. O serviço ERS é desativado por padrão no ISE. Depois de habilitada, os clientes podem consultar a API se autenticarem como membros do grupo **ERS Admin** no nó ISE. Para ativar o serviço no ISE e adicionar uma conta ao grupo correto, siga estas etapas:

Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione em **Administração > Sistema > Configurações**.

Etapa 2. No painel esquerdo, clique em **ERS Settings (Configurações ERS)**.



Etapa 3. Selecione a opção **Enable ERS for Read/Write**.

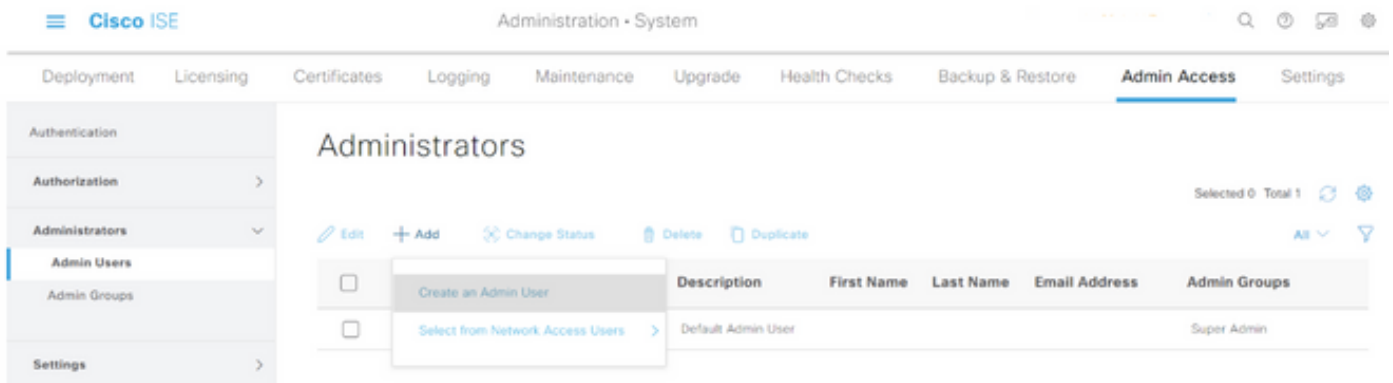
Etapa 4. Clique em **Salvar e confirme com OK**.

Adicionar usuário ao grupo ESR Admin (Opcional)

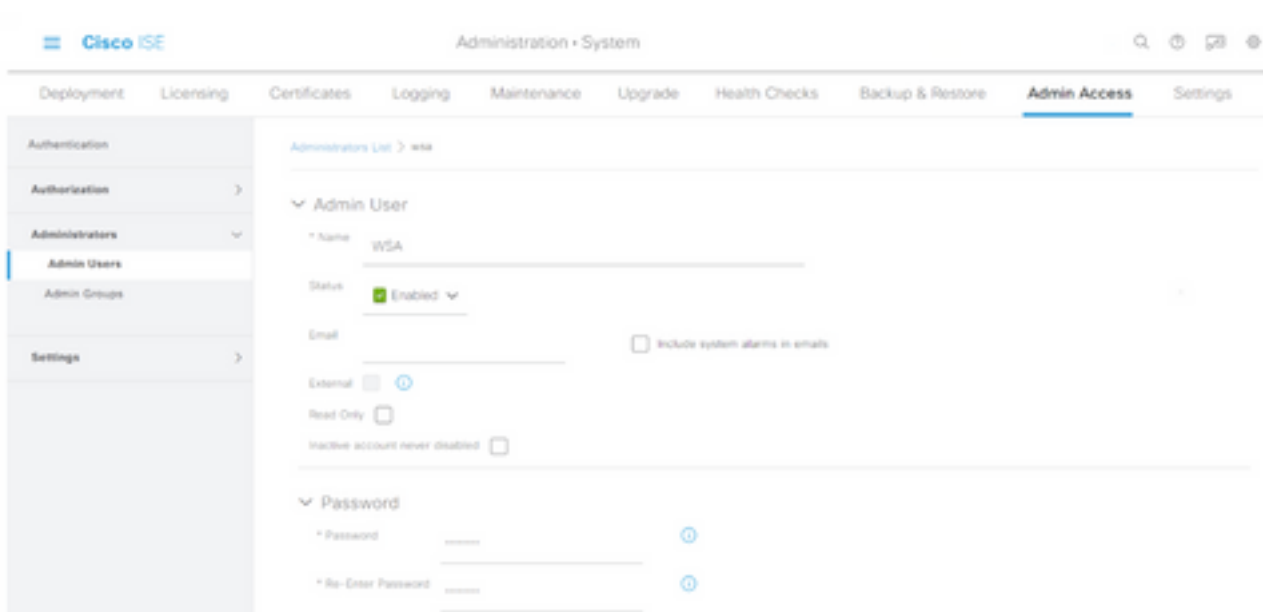
Etapa 1. Selecione o ícone de três linhas localizado no canto superior esquerdo e selecione **Administration > System > Admin Access**

Etapa 2. No painel esquerdo, expanda **Administrators** e clique em **Admin Users**.

Etapa 3. Clique em **+Add** e selecione **Admin User** no menu suspenso.



Etapa 4. Digite um nome de usuário e uma senha nos campos apropriados.



Etapa 5. No campo **Admin Groups** , use a lista suspensa para selecionar o **ERS Admin**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. Below this is a menu with options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, **Admin Access**, and Settings. The left sidebar has a tree view with 'Authentication', 'Authorization', 'Administrators' (expanded to show 'Admin Users' and 'Admin Groups'), and 'Settings'. The main content area is for 'Admin Access' configuration. It has fields for 'First Name' and 'Last Name'. Below these is a section for 'Account Options' with a 'Description' text area. The 'Admin Groups' section shows a list of groups, with 'ERS Admin' selected in a dropdown menu, which is highlighted with a red box. At the bottom right, there are 'Save' and 'Reset' buttons.

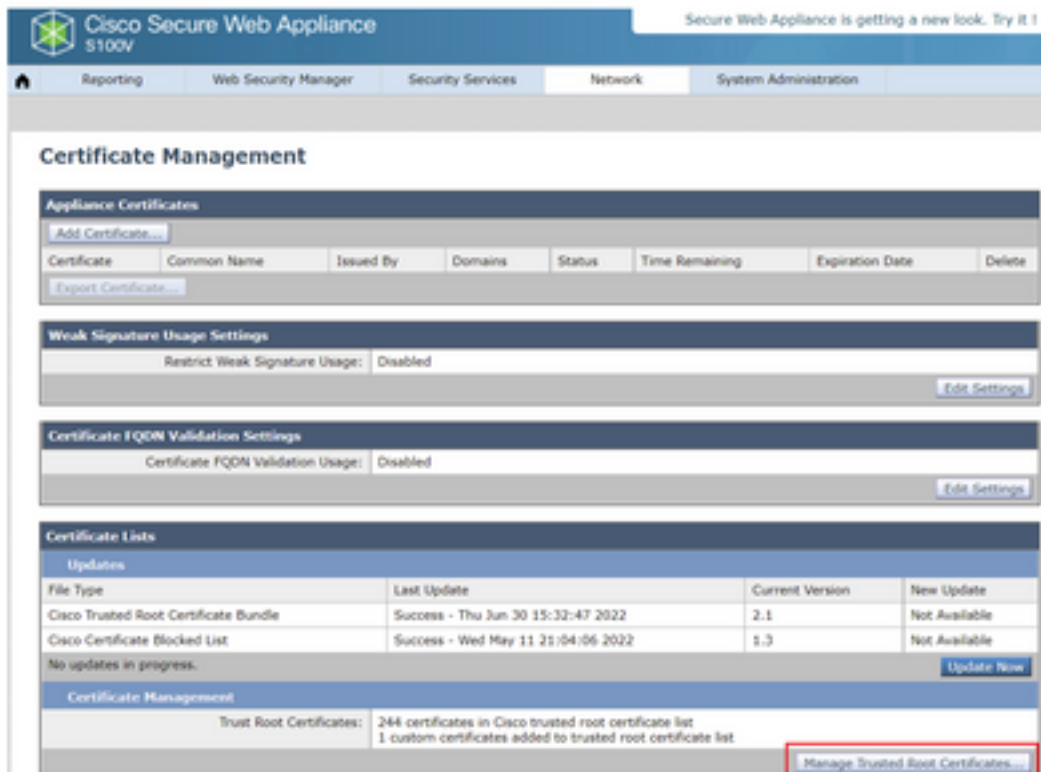
Etapa 6. Clique em **Salvar**.

Configuração segura de dispositivo da Web

Certificado raiz

Se o projeto de integração usar uma autoridade de certificação interna como raiz de confiança para a conexão entre o WSA e o ISE, esse certificado raiz deverá ser instalado nos dois dispositivos.

Etapa 1. Navegue até **Network > Certificate Management** e clique em **Manage Trusted Root Certificates** para adicionar um certificado CA.



Etapa 2. Clique em **Import**.



Etapa 3. Clique em **Escolher arquivo** para localizar a CA raiz gerada e clique em **Enviar**.

Etapa 4. Clique em **Enviar** novamente.

Etapa 5. No canto superior direito, clique em **Confirmar Alterações**.



Etapa 6. Clique em **Confirmar alterações** novamente.

Certificado pxGrid

No WSA, a criação do par de chaves e do certificado para uso pelo pxGrid é concluída como parte da configuração dos serviços do ISE.

Etapa 1. Navegue até **Rede > Identity Service Engine**.

Etapa 2. Clique em **Enable and Edit Settings**.

Etapa 3. Clique em **Escolher arquivo** para localizar a CA raiz gerada e clique em **Carregar arquivo**.

Note: Um erro de configuração comum é carregar o certificado pxGrid do ISE nesta seção. O certificado CA raiz deve ser carregado no campo Certificado do nó pxGrid do ISE.

Etapa 4. Na seção **Certificado de cliente do equipamento para Web**, selecione **Usar certificado e chave gerados**.

Etapa 5. Clique no botão **Gerar novo certificado e chave** e preencha os campos de certificado necessários.

Etapa 6. Clique em **Download Certificate Signing Request**.

Note: É recomendável selecionar o botão **Submit** para confirmar as alterações na configuração do ISE. Se a sessão for deixada para expirar antes de as alterações serem enviadas, as chaves e o certificado gerados poderão ser perdidos, mesmo se o CSR tiver sido baixado.

Etapa 7. Depois de assinar o CSR com sua CA, clique em **Choose File** (Escolher arquivo) para localizar o 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: No file chosen

Key: No file chosen

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: No file chosen

Etapa 8. Clique em **Upload File**.

Etapa 9. Enviar e Confirmar.

Ativar SXP e ERS no Secure Web Appliance

Etapa 1. Clique nos botões **Enable** para SXP e ERS.

ISE SXP Exchange Protocol (SXP) Service: Enabling the service, Web Appliance will retrieve SXP Binding Table 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 Trust (SGT), you should enable ERS.

Etapa 2. No campo **ERS Administrator Credentials**, insira as informações do usuário que foram configuradas no ISE.

Etapa 3. Marque a caixa para **Server name same as ISE pxGrid Node** para herdar as informações configuradas anteriormente. Caso contrário, insira as informações necessárias.

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)

Etapa 4. Enviar e Confirmar.

Perfil de identificação

Para usar tags de grupos de segurança ou informações de grupos do ISE nas políticas do WSA, primeiro é necessário criar um perfil de identificação que utilize o ISE como meio de identificar usuários de forma transparente.

Etapa 1. Navegue até **Web Security Manager > Authentication > Identification Profiles**.

Etapa 2. Clique em **Add Identification Profile**.

Etapa 3. Informe um nome e, opcionalmente, uma descrição.

Etapa 4. Na seção **Identificação e autenticação**, use a lista suspensa para escolher **Identificar usuários com ISE de forma transparente**.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

Enable Identification Profile

Name:
(e.g. my IT 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, 2001:420:80:1::5, 2000:ab8::2-2000:ab8::10)

Define Members by Protocol: HTTP/HTTPS

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

Etapa 5. Enviar e Confirmar.

Política decriptografia baseada em SGT

Etapa 1. Navegue até **Web Security Manager > Web Policies > Decryption Policies**.

Etapa 2. Clique em **Add Policy**.

Etapa 3. Informe um nome e, opcionalmente, uma descrição.

Etapa 4. Na seção **Perfis de identificação e usuários**, use a lista suspensa para escolher **Selecionar um ou mais perfis de identificação**.

Etapa 5. Na seção **Perfis de identificação**, use a lista suspensa para escolher o nome do perfil de identificação do ISE.

Etapa 6. Na seção **Usuários e grupos autorizados**, selecione **Grupos e usuários selecionados**.

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)

Add Identification Profile

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.

Etapa 7. Clique no hiperlink ao lado de **Tags de grupo seguras ISE**.

Etapa 8. Na seção **Secure Group Tag Search**, marque a caixa à direita do SGT desejado e clique em **Add**.

Authorized Secure Group Tags

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

Secure Group Tag Search

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

Etapa 9. Clique em **Concluído** para retornar.

Etapa 10. Enviar e Confirmar.

Configuração do 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

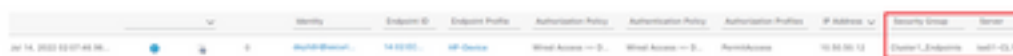
```
cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode)
cts role-based enforcement
```

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

Verificar

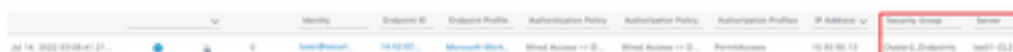
Atribuição de SGT do ISE para o endpoint.

Aqui você pode ver um endpoint do cluster 1 do ISE atribuído a um SGT após a autenticação e autorização bem-sucedidas:



Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authentication Policy	Authorization Profile	IP Address	Security Group	Server
10.50.50.120	14 02 00...	IP Device	Word Access --> D...	Word Access --> D...	PermitAccess	10.50.50.12	Cluster1_Endpoint	ise01-cl1

Aqui você pode ver um endpoint do cluster 2 do ISE atribuído a um SGT após a autenticação e autorização bem-sucedidas:



Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authentication Policy	Authorization Profile	IP Address	Security Group	Server
10.50.50.121	14 02 00...	Microsoft-Work	Word Access --> D...	Word Access --> D...	PermitAccess	10.50.50.12	Cluster2_Endpoint	ise02-cl2

Mapeamentos SXP

Como a comunicação SXP é habilitada entre os nós do ISE do cluster e o nó de agregação do ISE, esses mapeamentos de SGT-IP são aprendidos pela agregação do ISE por meio do SXP:

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PDNs Involved
10.50.50.121	TrustSec_Device (20000)		10.50.50.121, 10.50.50.0	SXP	default	10.50.50.0
10.50.50.122	TrustSec_Device (20000)		10.50.50.122, 10.50.50.7	SXP	default	10.50.50.0
10.50.50.121	Cluster_Endpoints (1110000)		10.50.50.121, 10.50.50.0	SXP	default	10.50.50.0
10.50.50.122	Cluster_Endpoints (2220000)		10.50.50.122, 10.50.50.7	SXP	default	10.50.50.0

Esses mapeamentos do SXP, de clusters diferentes do ISE, são enviados ao WSA sobre pxGrid por meio do nó de agregação do ISE:

```

wsa2.securitylab.net> isedata
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   -
  
```

Aplicação de política baseada em SGT

Aqui você pode ver que os diferentes endpoints correspondem às suas respectivas políticas e o tráfego é bloqueado com base em seu SGT:

Endpoint que pertence ao cluster do ISE 1

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', WBRAS: 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

Endpoint que pertence ao Cluster 2 do ISE



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/ice CONTENT TYPE: ... URL CATEGORY: Block URLs CL2 DESTINATION IP: ... DETAILS: Decryption 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

Informações Relacionadas

- [Web Security Appliance e Guia de integração do Identity Service Engine](#)
- [Configurar a integração do WSA com o ISE para serviços cientes do TrustSec](#)
- [Guia do Administrador do Cisco Identity Services Engine, Versão 3.1](#)
- [Manual do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance](#)