

# Integrate Multiple ISE Clusters with Secure Web Appliance for TrustSec Based Policies

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Limitations](#)

[Network Diagram](#)

[Configure](#)

[ISE Configuration](#)

[Enable SXP](#)

[Configure SXP on the cluster nodes](#)

[Configure SXP on the aggregation node](#)

[Enable pxGrid on the aggregation node](#)

[pxGrid Auto Approval](#)

[Network devices TrustSec settings](#)

[Network Device Authorization](#)

[SGT](#)

[Authorization Policy](#)

[Enabling ERS on ISE Aggregation Node \(Optional\)](#)

[Add user to ESR Admin group \(Optional\)](#)

[Secure Web Appliance Configuration](#)

[pxGrid Certificate](#)

[Enable SXP and ERS on Secure Web Appliance](#)

[Identification Profile](#)

[SGT Based Decryption Policy](#)

[Switch Configuration](#)

[AAA](#)

[TrustSec](#)

[Verify](#)

[Related Information](#)

## Introduction

This document describes the procedure to send Security Group Tag (SGT) information from multiple ISE Deployments to a single Cisco Secure Web Appliance (Formally Web Security Appliance WSA) through pxGrid in order to take advantage of SGT-Based Web Access Policies in a TrustSec deployment.

Prior to version 14.5, Secure Web Appliance can only integrate with a single ISE cluster for identity policies based on SGT. With the introduction of this new version, Secure Web Appliance

can now interoperate with information from multiple ISE clusters with a separate ISE node that aggregates between them. This brings great benefit and enables us to export user data from different ISE clusters and the liberty to control the exit point a user can use without the need for a 1:1 integration.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Identity Services Engine (ISE)
- Secure Web Appliance
- RADIUS protocol
- TrustSec
- pxGrid

### Components Used

The information in this document is based on these software and hardware versions:

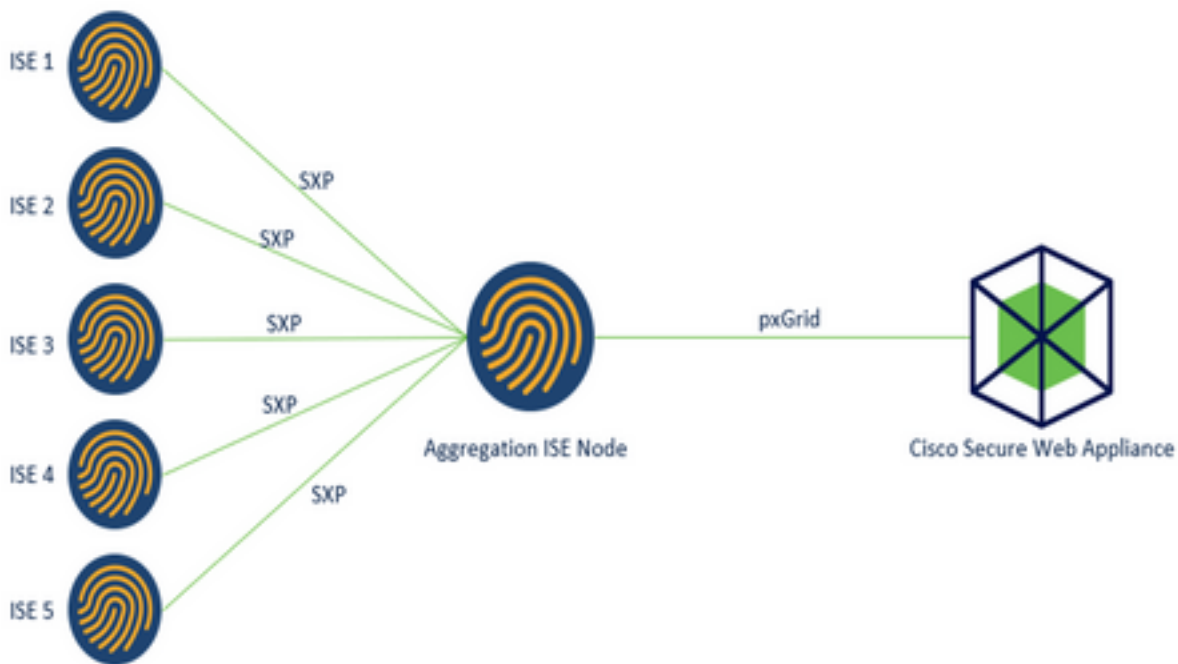
- Secure Web Appliance 14.5
- ISE version 3.1 P3

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. If your network is live, ensure that you understand the potential impact of any command.

### Limitations

1. All ISE Cluster need to maintain uniform mappings for SGTs.
2. ISE Aggregation Node must have the SGTs name/number of the rest of the ISE clusters.
3. Secure Web Appliance can only identify policy (Access/Decryption/Routing) based on SGT Tag and not group nor username.
4. Reporting and Tracking is SGT based.
5. Existing ISE/Secure Web Appliance sizing parameters continue to apply for this feature.

## Network Diagram




Process:

1. When the end user connects to the network, they receive an SGT based on Authorization policies in ISE.
2. The different ISE clusters then send this SGT information in form of SGT-IP mappings to ISE Aggregation Node through SXP.
3. ISE Aggregation Node receive this information and share with the single Secure Web Appliance through pxGrid.
4. Secure Web Appliance uses the SGT information it has learnt to provide access to users based on Web Access Policies.

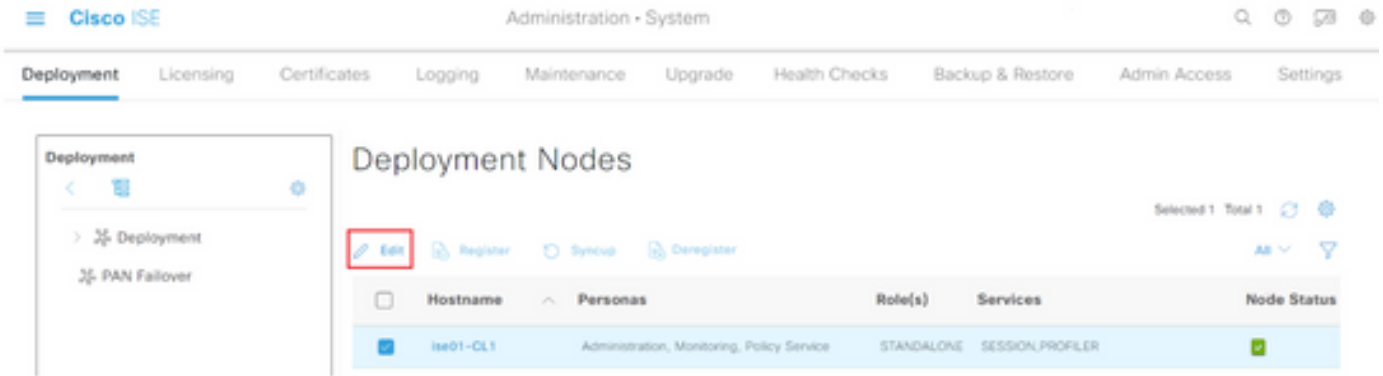
## Configure

### ISE Configuration

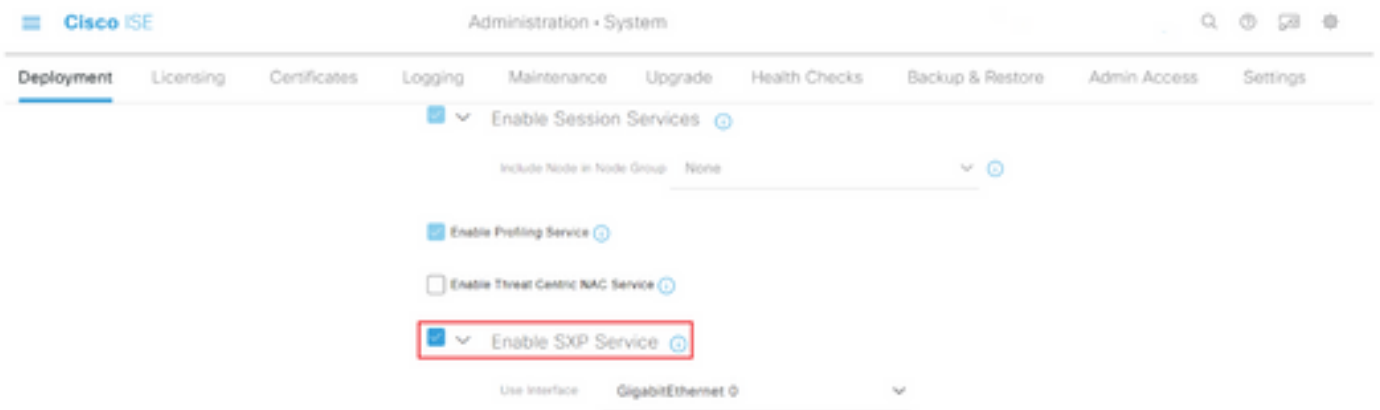
#### Enable SXP

**Step 1.** Select the three lines icon  located in the upper left corner and select on **Administration > System > Deployment.**

**Step 2.** Select the node you want to configure and click **Edit.**




**Step 3.** To enable SXP, tick the box **Enable SXP Service**



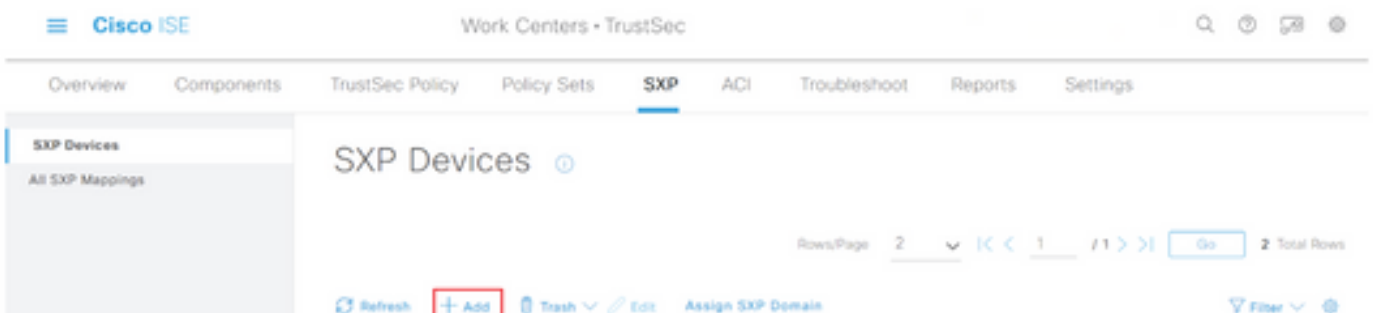
**Step 4.** Scroll down to the bottom and click **Save**

**Note:** Repeat all the steps for the rest of the ISE nodes in each cluster, the aggregation node included.

## Configure SXP on the cluster nodes


**Step 1.** Select the three lines icon  located in the upper left corner and select on **Work Center > TrustSec > SXP**.

**Step 2.** Click **+Add** to configure the ISE aggregation node as an SXP peer.



**Step 3.** Define the **Name** and **IP address** of the ISE aggregation node, select peer role as

**LISTENER.** Select required PSNs under **Connected PSNs**, required **SXP Domains**, select **Enabled** under status, then select **Password Type** and 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

**Step 4.** Click **Save**

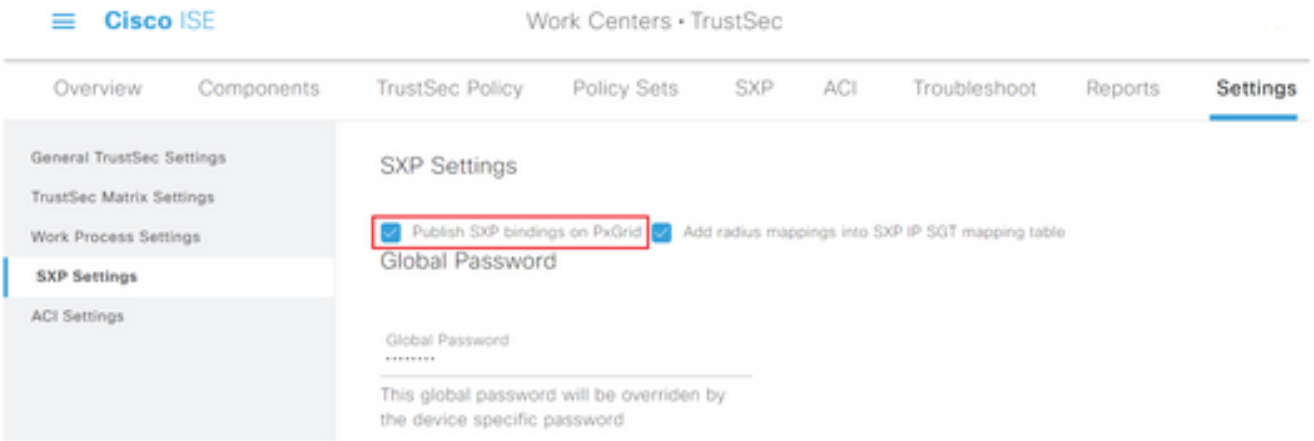
**Note:** Repeat all the steps for the rest of the ISE nodes in each cluster to build an SXP connection to the aggregation node. **Repeat the same process on the aggregation node and select SPEAKER as peer role.**

## Configure SXP on the aggregation node

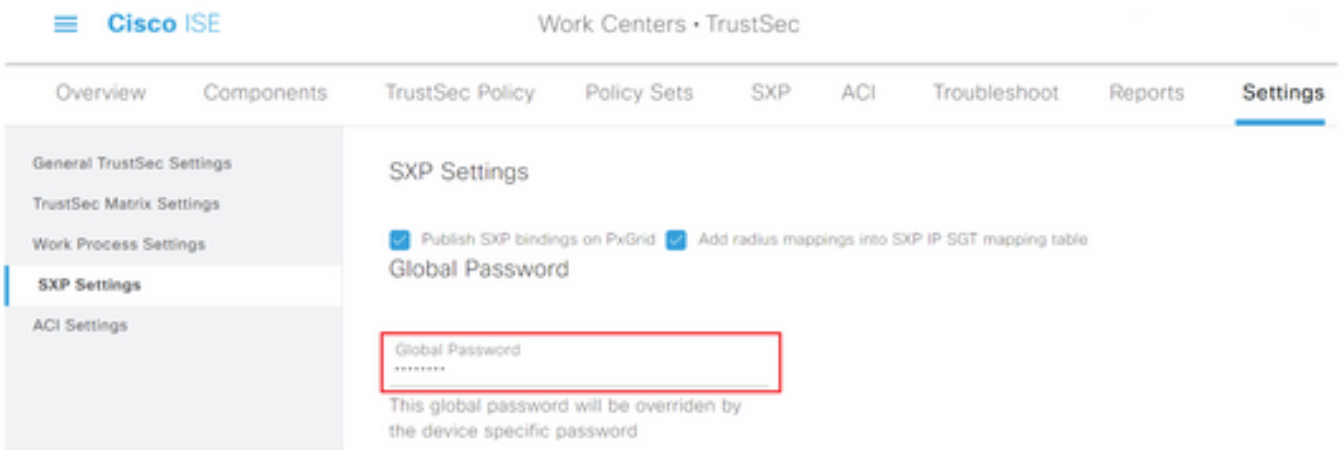
**Step 1.** Select the three lines icon located in the upper left corner and select on **Work Center > TrustSec > Settings**

**Step 2.** Click the tab **SXP Settings**

**Step 3.** To propagate the IP-SGT mappings, tick the **Publish SXP bindings on pxGrid** check box.



**Step 4 (Optional).** Define a default password for SXP settings under **Global Password**

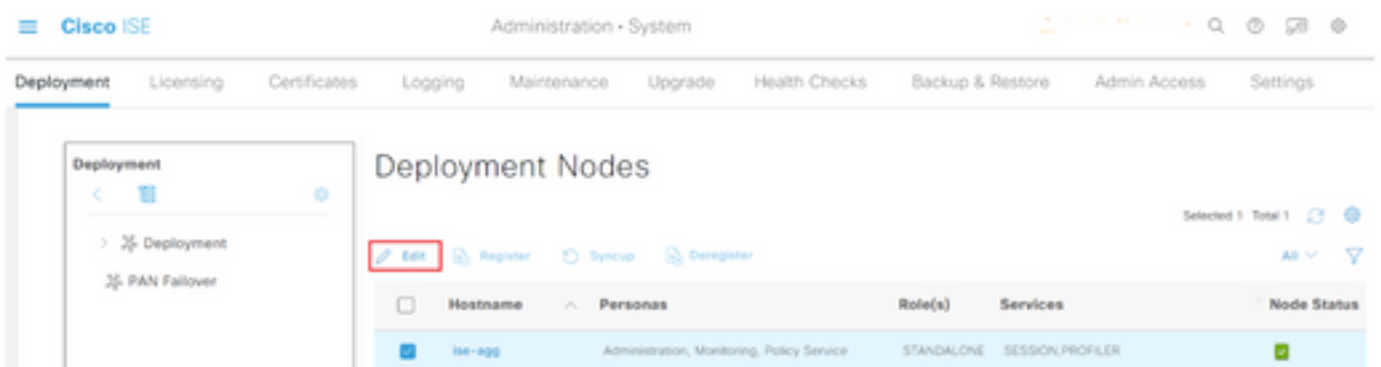


**Step 5.** Scroll down and click **Save**.

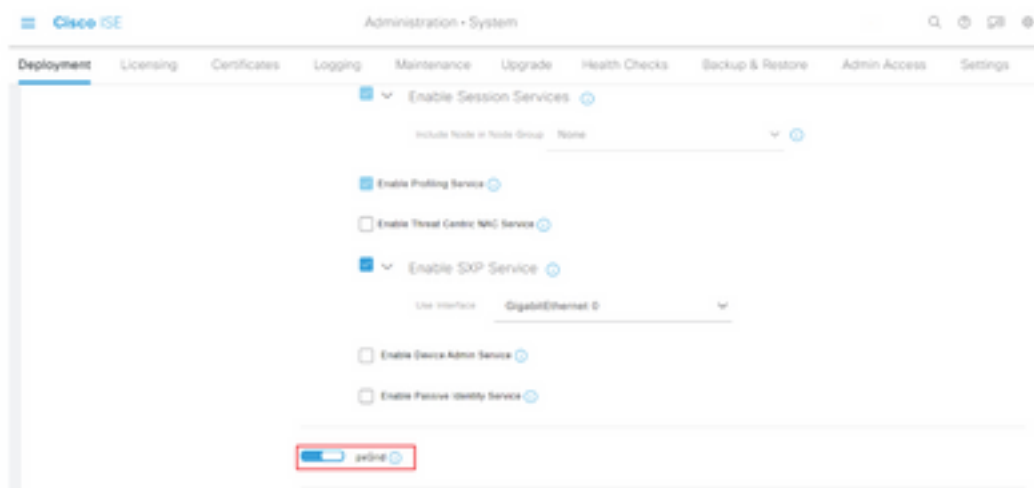
## Enable pxGrid on the aggregation node

**Step 1.** Select the three lines icon located in the upper left corner and select on **Administration > System > Deployment**.

**Step 2.** Select the node you want to configure and click **Edit**.



**Step 3.** To enable pxGrid, click the button next to **pxGrid**.

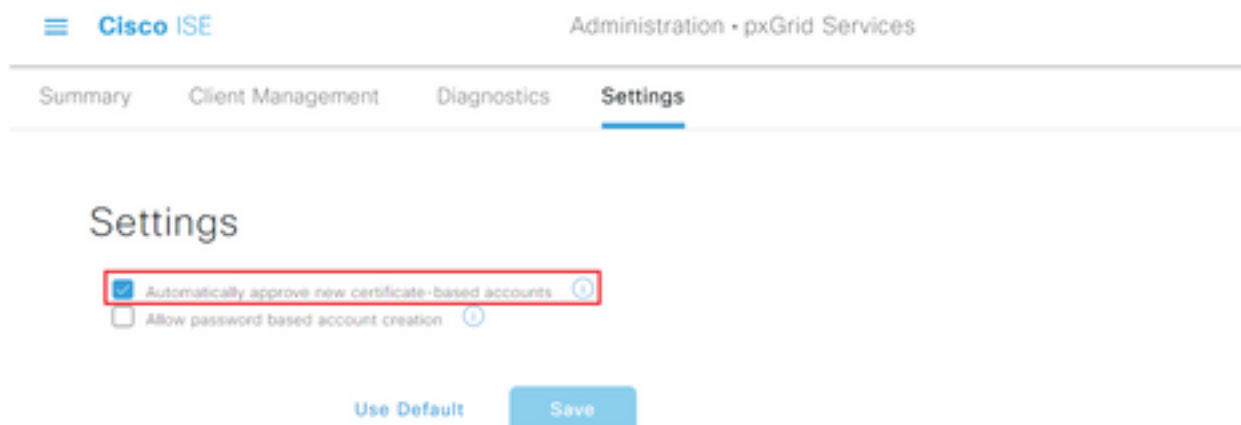


**Step 4.** Scroll down to the bottom and click **Save**.

## pxGrid Auto Approval

**Step 1.** Navigate to three lines icon located in the upper left corner and select **Administration > pxGrid Services > Settings**.

**Step 2.** By default, ISE does not automatically approve pxGrid the connection requests from new pxGrid clients, therefore you must enable that setting by select the checkbox **Automatically approve new certificate-based accounts**.



**Step 3.** Click **Save**

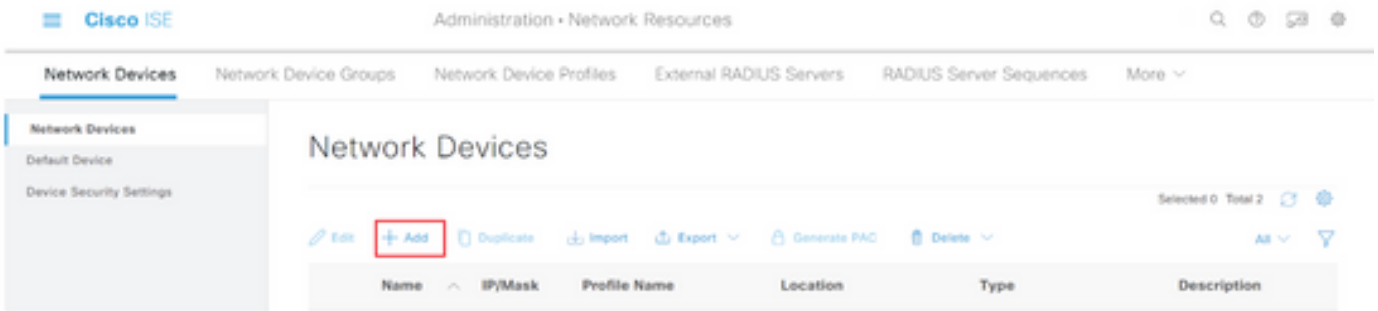
## Network devices TrustSec settings

For Cisco ISE to process requests from TrustSec-enabled devices, you must define these TrustSec-enabled devices in Cisco ISE.

**Step 1.** Navigate to the three lines icon located in the upper left corner and select on **Administration > Network Resources > Network Devices**.

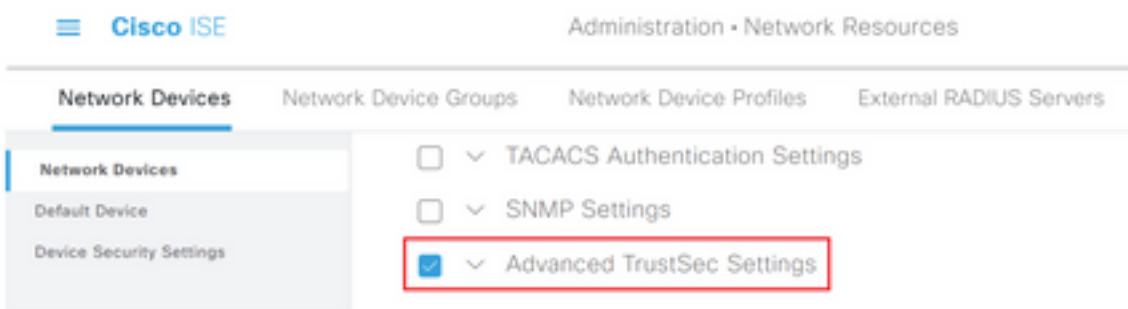
**Step 2.** Click **+Add**.



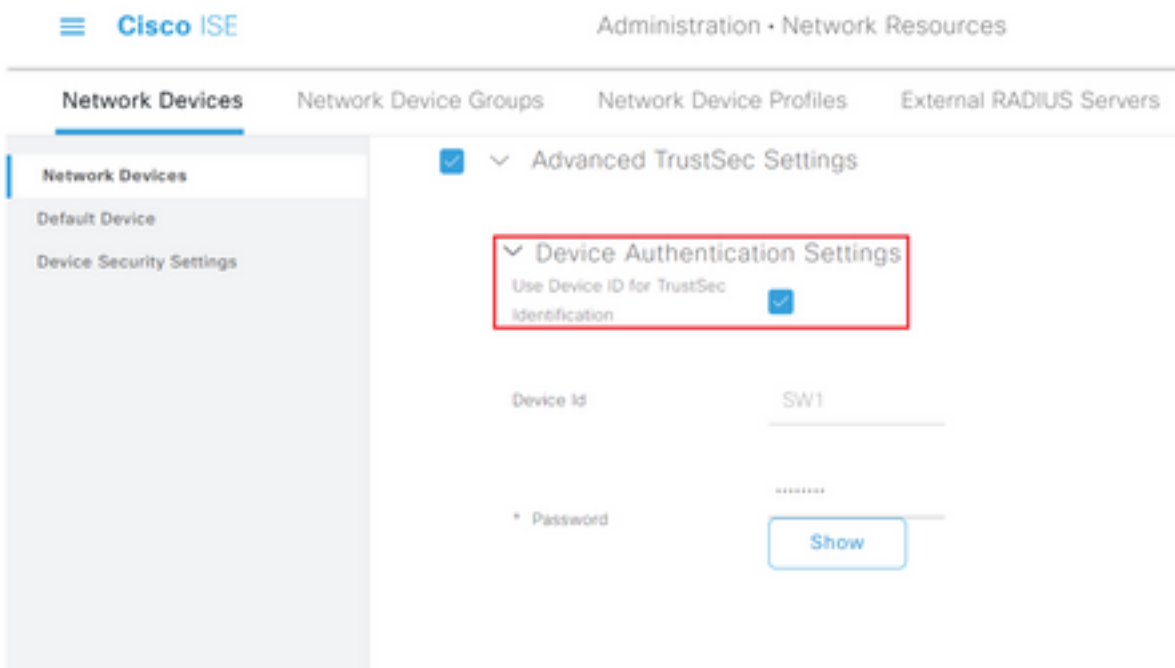


**Step 3.** Enter the required information in the **Network Devices** section and in **RADIUS Authentication Settings**.

**Step 4.** Check the **Advanced TrustSec Settings** check box to configure a TrustSec-enabled device.



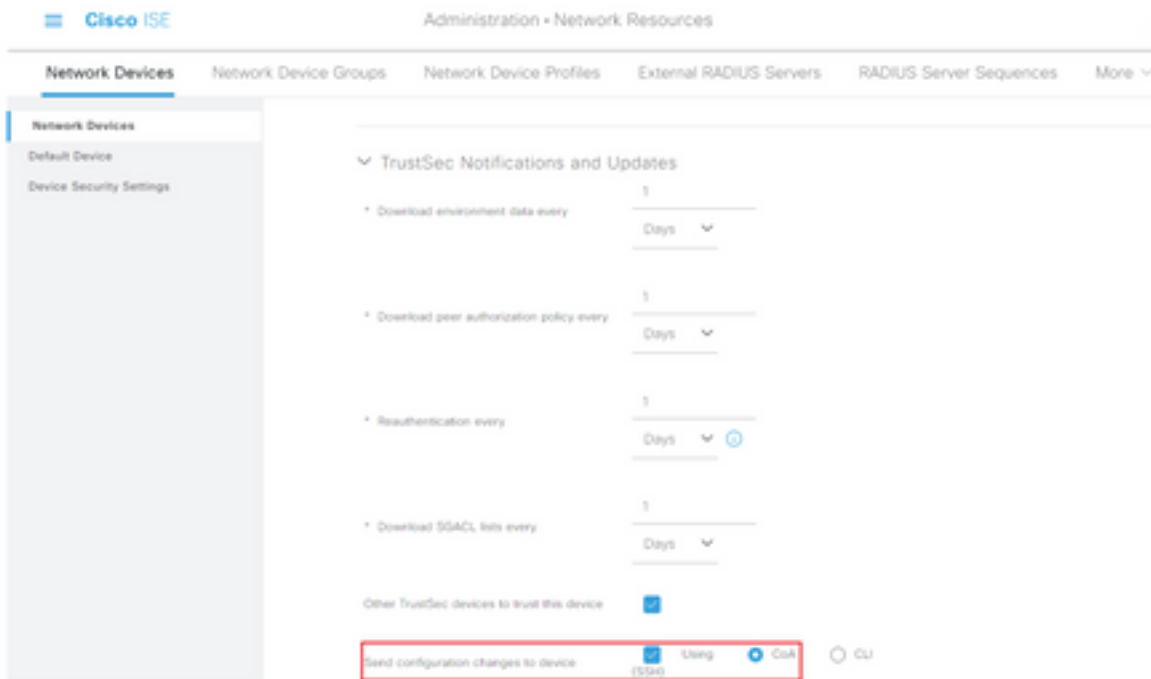
**Step 5.** Click the **Use Device ID for TrustSec Identification** check box to automatically populate the Device Name listed in the **Network Devices** section. Enter a password in the **Password** field.



**Note:** The ID and password must match the “cts credentials id <ID> password <PW>” command that is later configured on the switch.

**Step 6.** Check the **Send configuration changes to device** check box so that ISE can send

TrustSec CoA notifications to the device.



**Step 7.** Check the **Include this device when deploying Security Group Tag Mapping Updates** check box.

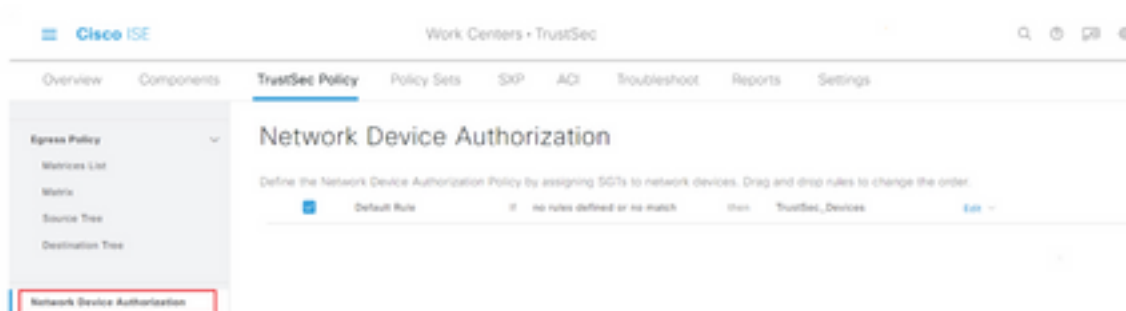
**Step 8.** In order to let ISE edit the configuration of the network device, enter the user credentials in the **EXEC Mode Username** and **EXEC Mode Password** fields. Optionally, provide enable password in the **Enable Mode Password** field.

**Note:** Repeat the steps for all other NADs that are intended to be a part of the TrustSec domain.

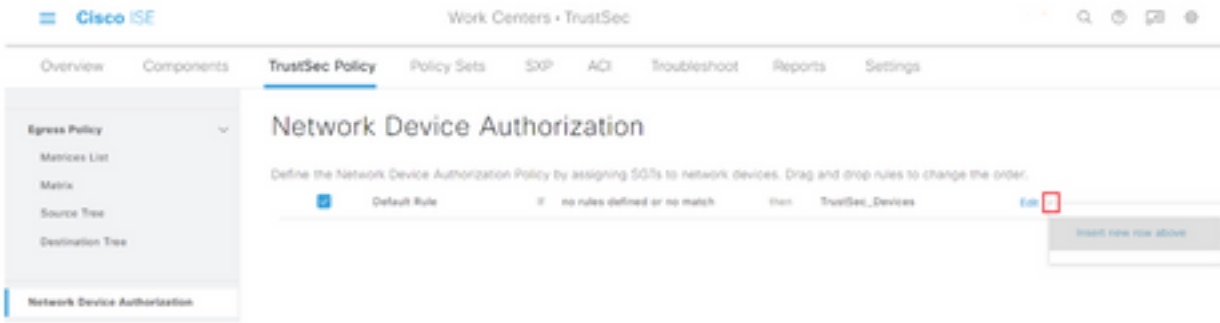
## Network Device Authorization

**Step 1.** Select the three lines icon located in the upper left corner and select on **Work Centers > TrustSec > TrustSec Policy**.

**Step 2.** In the left pane, click **Network Device Authorization**.

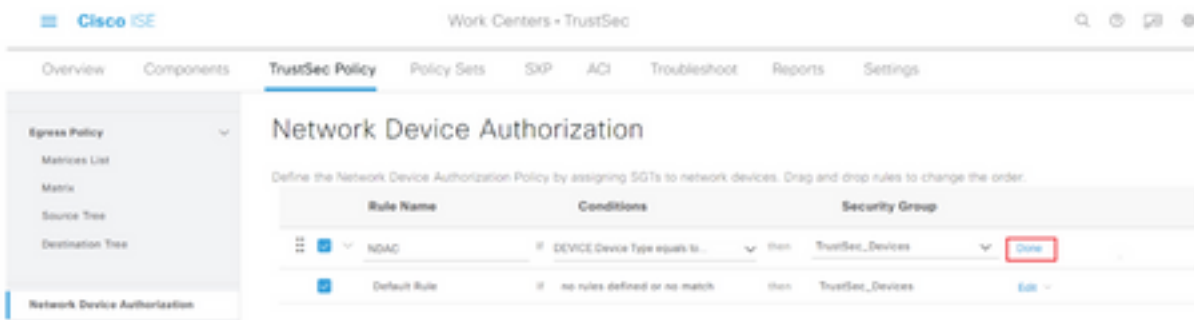


**Step 3.** On the right, use the drop-down next to **Edit** and **Insert new row above** to create a new NDA rule.



**Step 4.** Define a **Rule Name**, **Conditions** and select the appropriate SGT from the drop-down list under **Security Groups**.

**Step 5.** Click **Done** to the far right.



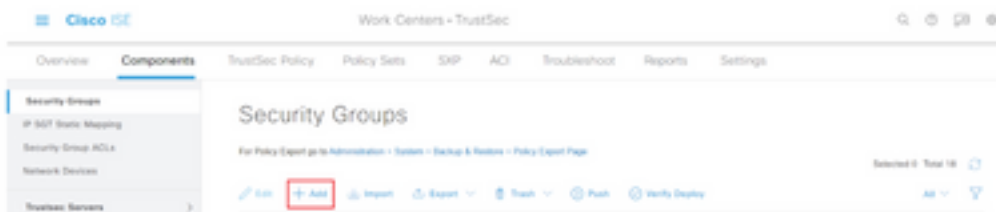
**Step 6.** Scroll down and click **Save**.

## SGT

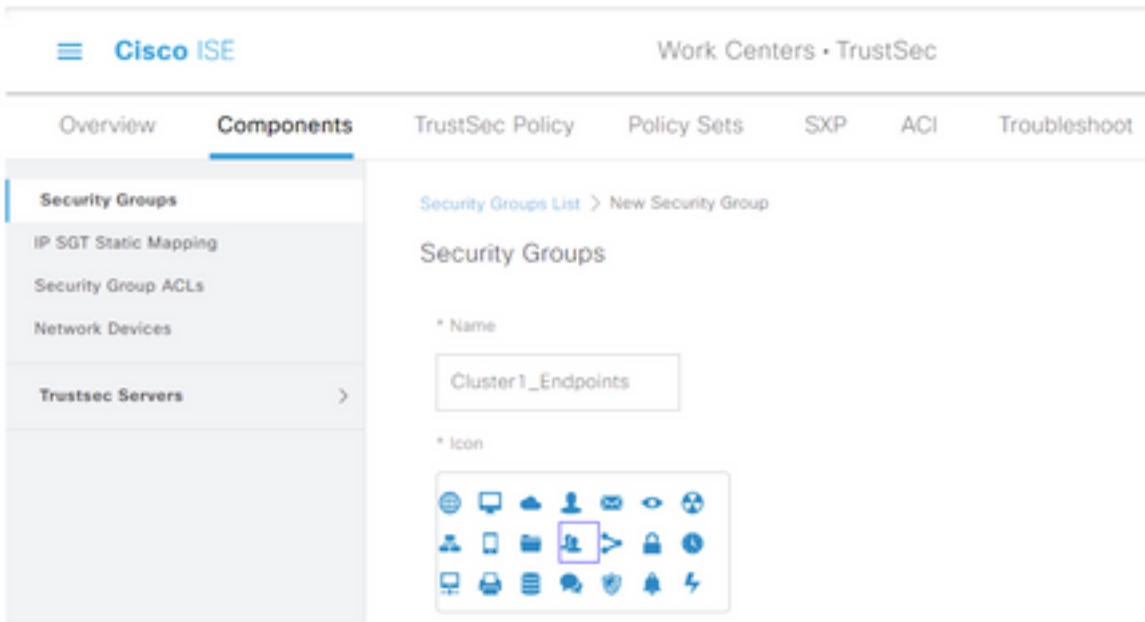
**Step 1.** Select the three lines icon located in the upper left corner and select on **Work Centers > TrustSec > Components**.

**Step 2.** In the left pane, expand **Security Groups**.

**Step 3.** Click **+Add** to create a new SGT.



**Step 4.** Enter the name and choose an icon in the appropriate fields.



**Step 5.** Optionally, give it a description and enter a **Tag Value**.

**Note:** In order to be able to manually enter a Tag Value, navigate to Work Centers > TrustSec > Settings > General TrustSec Settings and select the option **User Must Enter SGT Number Manually** under **Security Group Tag Numbering**.

**Step 6.** Scroll down and click **Submit**

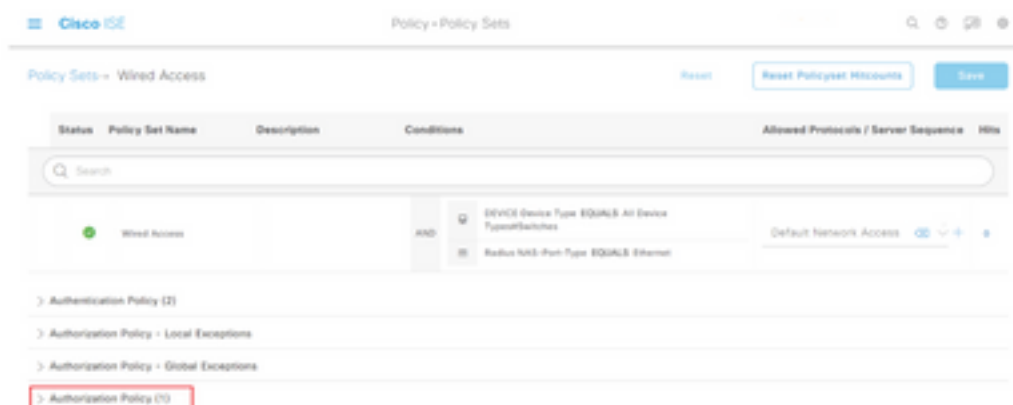
**Note:** Repeat these steps for all required SGTs.


## Authorization Policy

**Step 1.** Select the three lines icon located in the upper left corner and select on **Policy > Policy Sets**.

**Step 2.** Select the appropriate policy set.

**Step 3.** Within the policy set, expand the **Authorization Policy**.



**Step 4.** Click the  button to create an **Authorization Policy**.



**Step 5.** Define the required **Rule Name**, **Condition/s**, and **Profiles** and select the appropriate SGT from the drop-down list under **Security Groups**.



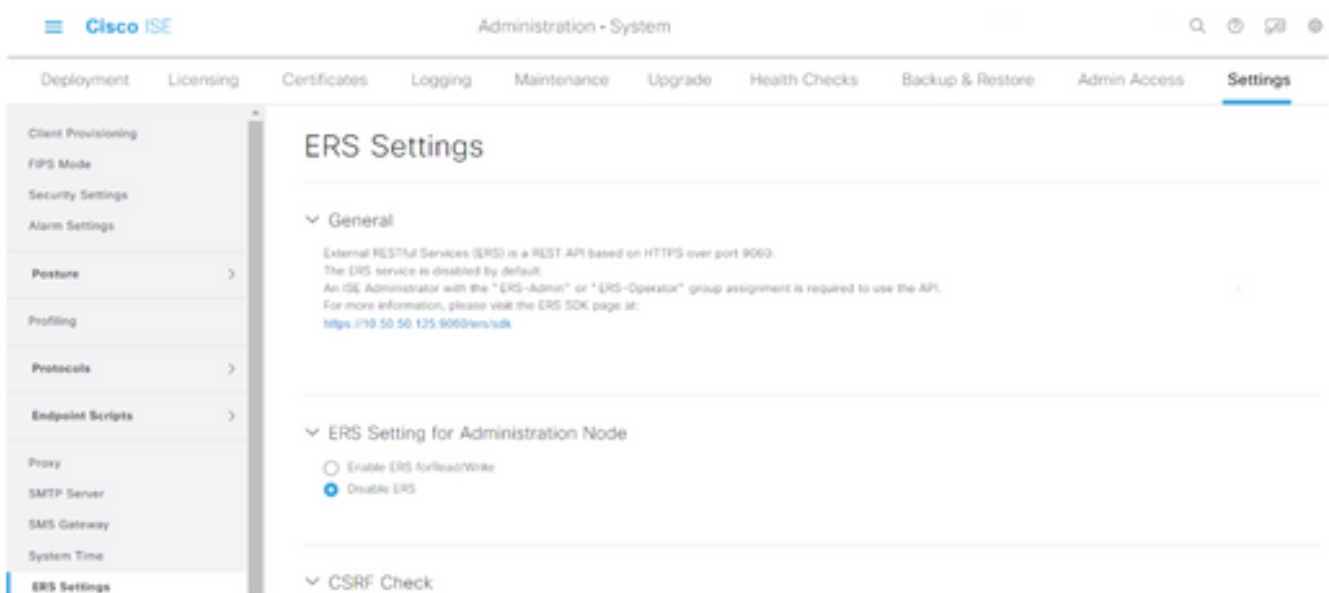
**Step 6.** Click **Save**.

## Enabling ERS on ISE Aggregation Node (Optional)

The External RESTful API Service (ERS) is an API that can be queried by the WSA for group information. The ERS service is disabled by default on ISE. Once it is enabled, clients can query the API if they authenticate as members of the **ERS Admin** group on the ISE node. To enable the service on ISE and add an account to the correct group, follow these steps:

**Step 1.** Select the three lines icon located in the upper left corner and select on **Administration > System > Settings**.

**Step 2.** In the left pane, click **ERS Settings**.



**Step 3.** Select the option **Enable ERS for Read/Write**.

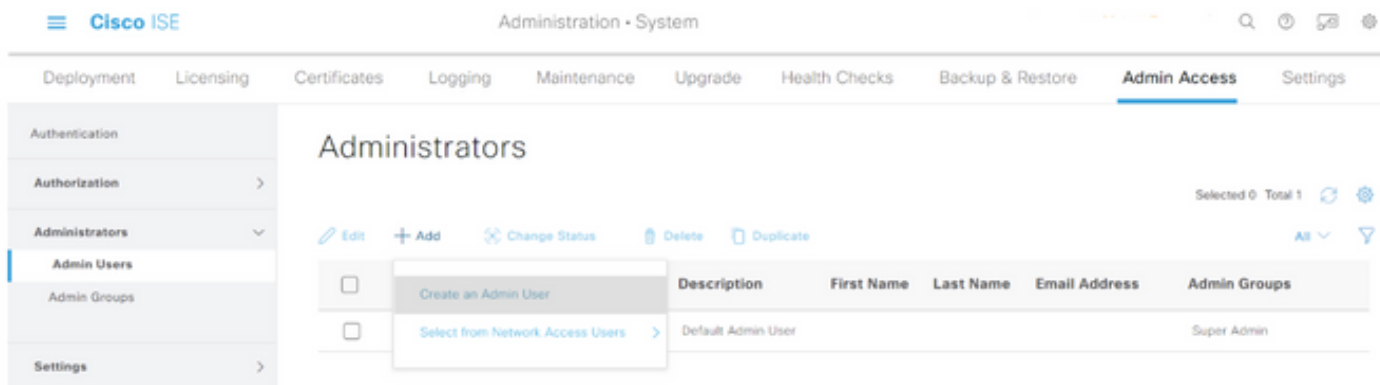
**Step 4.** Click **Save** and confirm with **OK**.

## Add user to ESR Admin group (Optional)

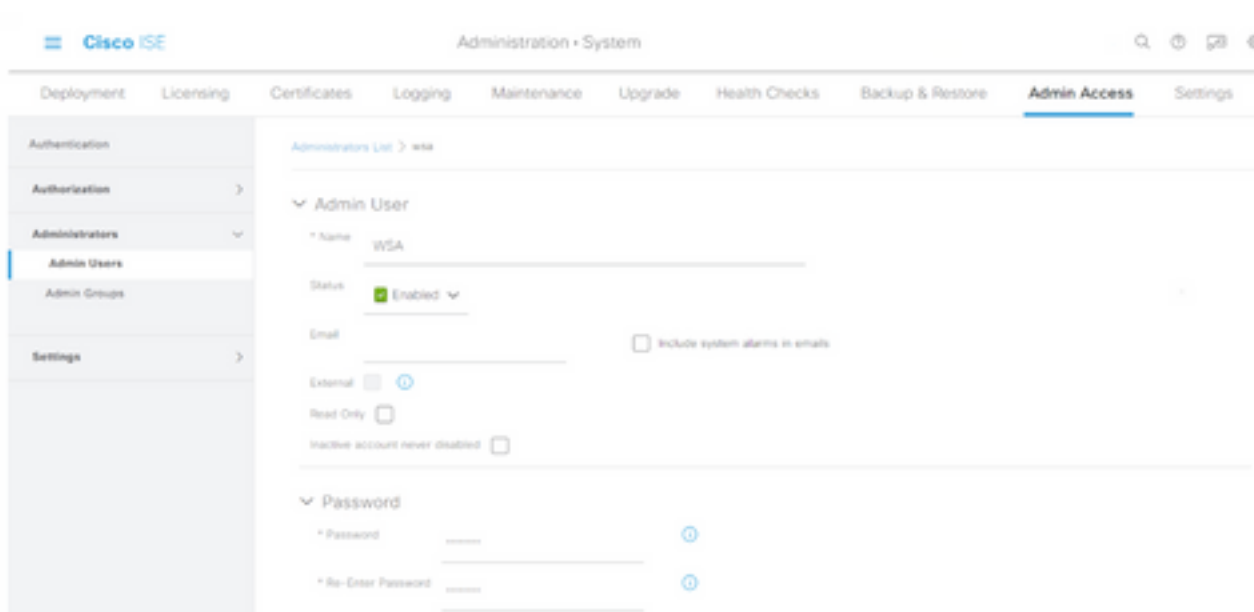
**Step 1.** Select the three lines icon located in the upper left corner and select **Administration > System > Admin Access**

**Step 2.** In the left pane, expand **Administrators** and click **Admin Users**.

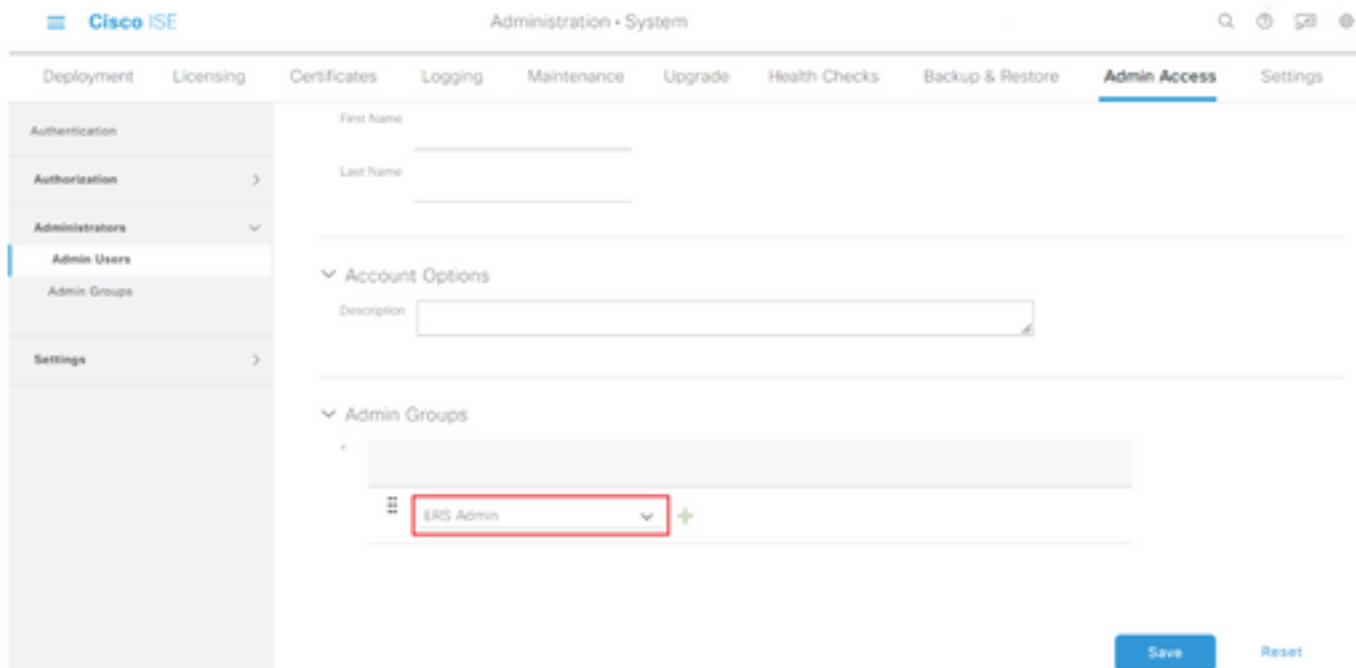
**Step 3.** Click **+Add** and select **Admin User** from the drop-down.



**Step 4.** Enter a username and password in the appropriate fields.



**Step 5.** In the **Admin Groups** field, use the drop-down to select **ERS Admin**.



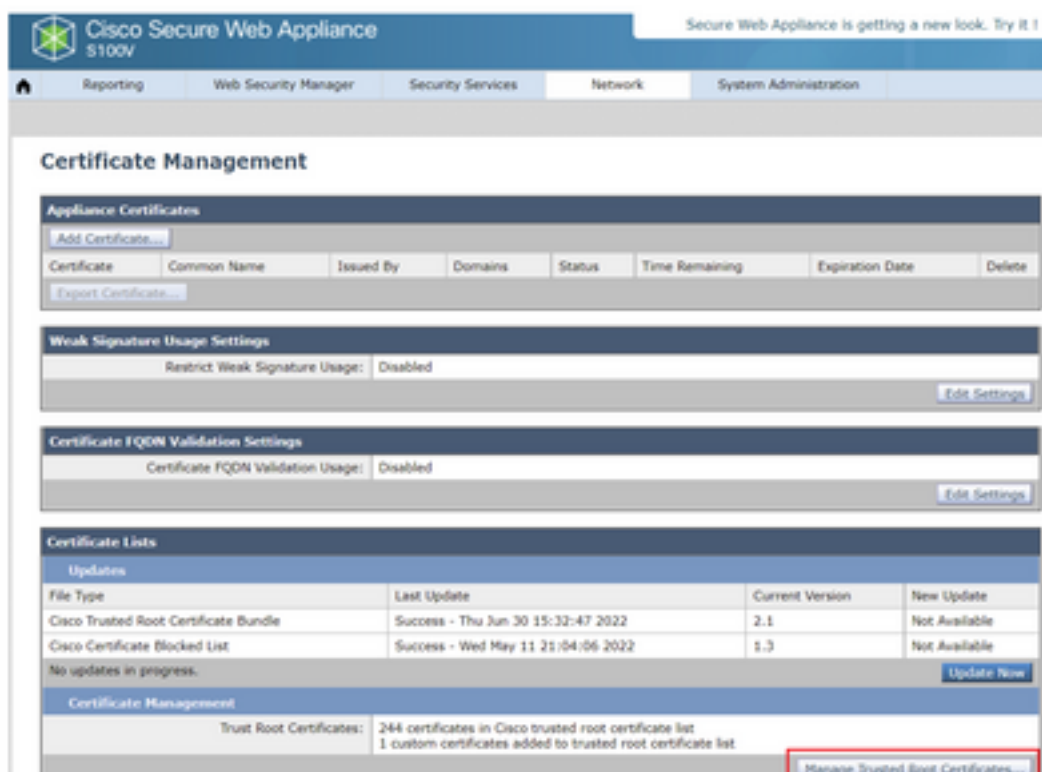
Step 6. Click **Save**.

## Secure Web Appliance Configuration

### Root certificate

If the integration design uses an internal certificate authority as the root of trust for the connection between the WSA and ISE, then this root certificate must be installed on both appliances.

**Step 1.** Navigate to **Network > Certificate Management** and click on **Manage Trusted Root Certificates** to add a CA certificate.



**Step 2.** Click on **Import**.



**Step 3.** Click on **Choose File** to locate the generated Root CA and click **Submit**.

**Step 4.** Click **Submit** again.

**Step 5.** At the upper right corner, click **Commit Changes**.



**Step 6.** Click **Commit Changes** again.

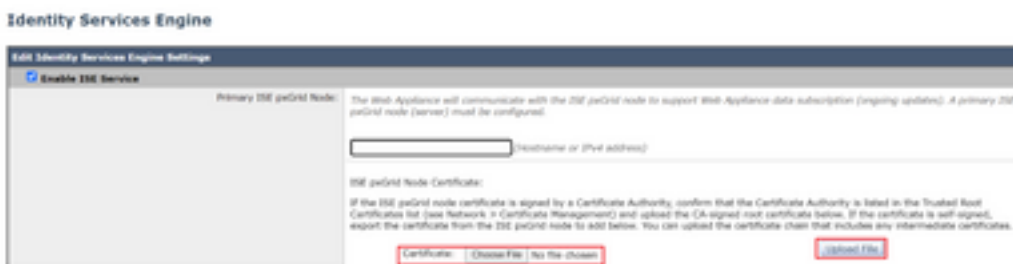
## pxGrid Certificate

In the WSA, the creation of the key pair and certificate for use by pxGrid is completed as part of the ISE services configuration.

**Step 1.** Navigate to **Network > Identity Service Engine**.

**Step 2.** Click on **Enable and Edit Settings**.

**Step 3.** Click on **Choose File** to locate the generated Root CA and click **Upload File**.



**Note:** A common misconfiguration is to upload the ISE pxGrid certificate in this section. The root CA certificate must be uploaded to the ISE pxGrid Node Certificate field.

**Step 4.** In the **Web Appliance Client Certificate** section, select **Use Generated Certificate and Key**.



**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

**Step 5.** Click the **Generate New Certificate and Key** button and complete the required certificate fields.

**Generate Certificate and Key** ✕

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration:  months

Basic Constraints:  Set X509v3 Basic Constraints Extension to Critical

**Step 6.** Click on **Download Certificate Signing Request.**

**Note:** It is recommend to select the **Submit** button to commit the changes to the ISE configuration. If the session is left to timeout before the changes are submitted, the keys and certificate that were generated can be lost, even if the CSR was downloaded.

**Step 7.** After you have signed the CSR with your CA, click on **Choose File** to locate the certificate.

**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:

**Step 8. Click Upload File.**

**Step 9. Submit and Commit.**

## Enable SXP and ERS on Secure Web Appliance

**Step 1. Click the Enable buttons for both SXP and 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 Tags (SGTs), you should enable ERS.

**Step 2. In the ERS Administrator Credentials field, enter the user information that was configured on ISE.**

**Step 3. Check the box for Server name same as ISE pxGrid Node to inherit the earlier configured information. Otherwise, enter the required information there.**

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)

**Step 4. Submit and Commit.**

## Identification Profile

In order to use security group tags or ISE group information in the WSA policies, an identification profile must first be created that utilizes ISE as a means to transparently identify users.

**Step 1.** Navigate to **Web Security Manager > Authentication > Identification Profiles.**

**Step 2.** Click on **Add Identification Profile.**

**Step 3.** Enter a name and optionally a description.

**Step 4.** In the **Identification and Authentication** section, use the drop-down to choose **Transparently identify users with ISE.**

#### Identification Profiles: Add Profile

**Client / User Identification Profile Settings**

Enable Identification Profile

Name: ISE Profile  
(e.g. my IT Profile)

Description: Identification profile for ISE integration.  
(Maximum allowed characters 256)

Insert Above: 2 (Global Profile)

**User Identification Method**

Identification and Authentication: Transparently identify users with ISE

Fallback to Authentication Realm or Guest Privileges: Support 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:

Define Members by Protocol:  HTTP/HTTPS

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

**Step 5.** Submit and Commit.

## SGT Based Decryption Policy

**Step 1.** Navigate to **Web Security Manager > Web Policies > Decryption Policies.**

**Step 2.** Click **Add Policy.**

**Step 3.** Enter a name and optionally a description.

**Step 4.** In the **Identification Profiles and Users** section, use the drop-down to choose **Select One or More Identification Profiles.**

**Step 5.** In the **Identification Profiles** section, use the drop-down to choose the name of the ISE identification profile.

**Step 6.** In the **Authorized Users and Groups** section, select **Selected Groups and Users.**

**Policy Member Definition**

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:

Identification Profile	Authorized Users and Groups	<a href="#">Add Identification Profile</a>
ISE Profile	<input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users (2) ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered <input type="radio"/> 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.

**Step 7.** Click the hyperlink next to **ISE Secure Group Tags**.

**Step 8.** In the **Secure Group Tag Search** section, check the box to the right of the desired SGT and click **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 <input type="checkbox"/> All
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.

0 Secure Group Tag(s) selected for Add [Add](#)

Secure Group Tag Name	SGT Number	SGT Description	Select <input type="checkbox"/> All
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"/>

**Step 9.** Click **Done** to return.

**Step 10.** Submit and **Commit**.

## Switch Configuration

### 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

```

## Verify

### SGT assignment from ISE to endpoint.

Here you can see an endpoint from ISE Cluster 1 assigned an SGT after successful authentication and authorization:

Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
Auth@Boson	14 02 02	IP Device	Wind Access -- S...	Wind Access -- S...	PermitAccess	10.50.50.12	Cluster1_Endpoint_ise01-cl1	ise01-cl1

Here you can see an endpoint from ISE Cluster 2 assigned an SGT after successful authentication and authorization:

Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Server
Auth@Boson	14 02 02	Microsoft-Wor...	Wind Access -- S...	Wind Access -- S...	PermitAccess	10.50.50.12	Cluster2_Endpoint_ise01-cl1	ise01-cl1

## SXP Mappings

Since SXP communication is enabled between the cluster ISE nodes and ISE aggregation node, these SGT-IP mappings are learned by ISE aggregation through SXP:

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PDNs Involved
10.50.50.112	TrustSec_Device (20000)		10.50.50.121_10.50.50.5	SXP	Default	10.50.50.5
10.50.50.112	TrustSec_Device (20000)		10.50.50.122_10.50.50.7	SXP	Default	10.50.50.7
10.50.50.121	Cluster_Endpoints (1110000)		10.50.50.121_10.50.50.5	SXP	Default	10.50.50.5
10.50.50.122	Cluster_Endpoints (2220000)		10.50.50.122_10.50.50.7	SXP	Default	10.50.50.7

These SXP mappings, from different ISE clusters, are then sent to WSA over pxGrid through the ISE aggregation node:

```

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
10.50.50.11      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   -
  
```

### SGT based policy enforcement

Here you can see the different endpoints match its respective policies and traffic are blocked based on their SGT:

Endpoint that belongs to ISE Cluster 1

**This Page Cannot Be Displayed**

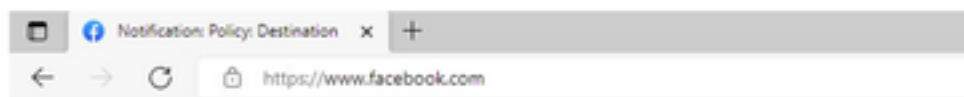
Based on your organization's access policies, access to this web site ( <https://bbc.com/> ) has been blocked.

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
14 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 that belongs to 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

## Related Information

- [Web Security Appliance and Identity Service Engine Integration Guide](#)
- [Configure WSA Integration with ISE for TrustSec Aware Services](#)
- [Cisco Identity Services Engine Administrator Guide, Release 3.1](#)
- [User Guide for AsyncOS 14.5 for Cisco Secure Web Appliance](#)