

# Integratie van meerdere ISE-clusters met beveiligde web-applicatie voor op Tech gebaseerd beleid

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Beperkingen](#)

[Netwerkdigram](#)

[Configureren](#)

[ISE-configuratie](#)

[SXP inschakelen](#)

[SXP op de clusterknooppunten configureren](#)

[SXP op de aggregatieknop configureren](#)

[PxGrid op het aggregatieknooppunt inschakelen](#)

[Automatische goedkeuring van pxGrid](#)

[Netwerkapparaten Instellingen voor vertrouwen](#)

[Verificatie van netwerkapparaten](#)

[SGT](#)

[machtigingsbeleid](#)

[ERS inschakelen op ISE Aggregation Node \(optioneel\)](#)

[Gebruiker toevoegen aan ESR Admin-groep \(optioneel\)](#)

[Configuratie van beveiligde web-applicatie](#)

[PxGrid-certificaat](#)

[SXP en ERS inschakelen voor beveiligde webapplicatie](#)

[Identificatieprofiel](#)

[SGT-gebaseerd decryptiebeleid](#)

[Switchconfiguratie](#)

[AAA](#)

[TrustSec](#)

[Verifiëren](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft de procedure om informatie over Security Group Tag (SGT) van meerdere ISE-implementaties naar één Cisco Secure Web Appliance (Officieel Web Security Appliance WSA) via pxGrid om voordeel te halen uit SGT-gebaseerd Web Access Policy in een TrustSec-implementatie.

Vóór versie 14.5 kan Secure Web Appliance alleen integreren met één ISE-cluster voor identiteitsbeleid op basis van SGT. Dankzij de introductie van deze nieuwe versie kan Secure Web Appliance nu samenwerken met informatie uit meerdere ISE-clusters met een afzonderlijk ISE-knooppunt dat tussen deze clusters aggregeert. Dit levert grote voordelen op en stelt ons in staat gebruikersgegevens uit verschillende ISE-clusters te exporteren en de vrijheid om het punt te controleren dat een gebruiker kan gebruiken zonder de noodzaak van een 1:1-integratie.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Services Engine (ISE)
- Secure web-applicatie
- RADIUS-protocol
- TrustSec
- PxGrid

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

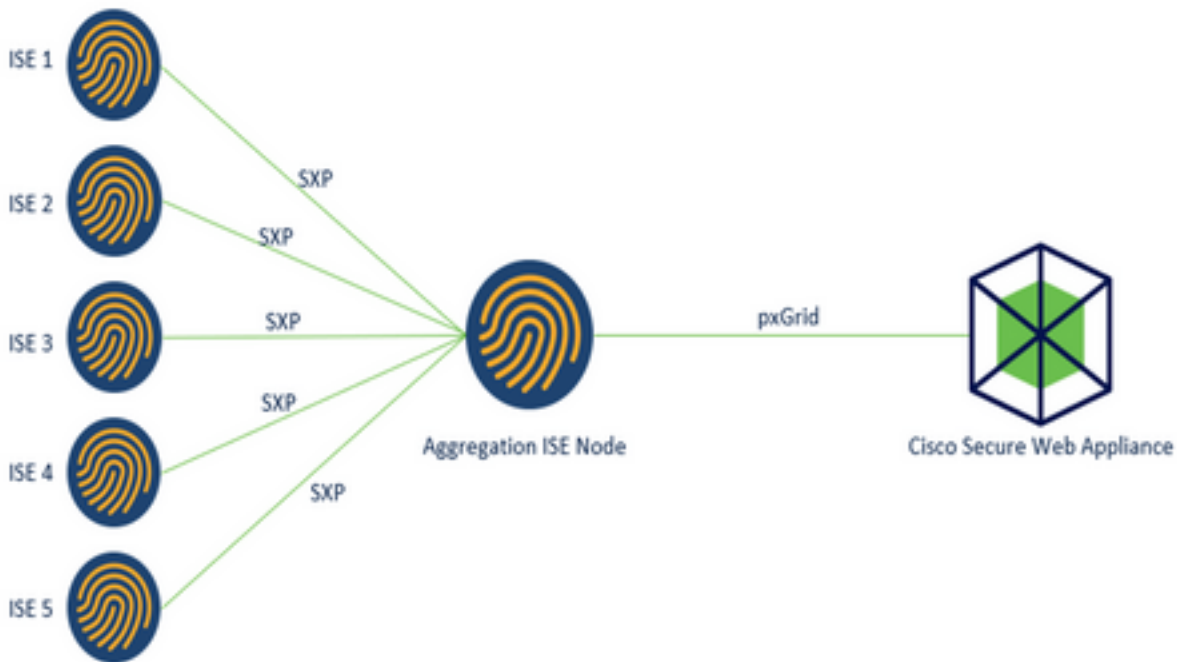
- Secure Web-applicatie 14.5
- ISE versie 3.1 P3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

### Beperkingen

1. Alle ISE-clusters moeten uniforme wachtrijen voor SGT's onderhouden.
2. ISE Aggregation Node moet de SGTs naam/nummer van de rest van de ISE-clusters hebben.
3. Secure Web Appliance kan alleen beleid (access/decryptie/routing) identificeren op basis van SGT Tag en niet groep of gebruikersnaam .
4. Rapportage en tracering zijn op SGT gebaseerde .
5. Bestaande parameters voor ISE/Secure Web Appliance blijven van toepassing voor deze functie.

## Netwerkdigram



Procesverloop:

1. Wanneer de eindgebruiker verbinding maakt met het netwerk, ontvangen zij een SGT op basis van het machtigingsbeleid in ISE.
2. De verschillende ISE-clusters sturen deze SGT-informatie vervolgens in de vorm van SGT-IP-mappings naar ISE Aggregation Node via SXP.
3. ISE Aggregation Node ontvangt deze informatie en deelt met de Secure Web Appliance via PxGrid.
4. De beveiligde webapplicatie gebruikt de SGT-informatie die zij heeft geleerd om toegang te bieden aan gebruikers op basis van een beleid voor webtoegang.

## Configureren

### ISE-configuratie

#### SXP inschakelen

**Stap 1.** Selecteer het pictogram drie regels  bevinden zich in de linker bovenhoek en selecteer deze optie op **Beheer > Systeem > Plaatsing**.

**Stap 2.** Selecteer het knooppunt dat u wilt configureren en klik op **Bewerken**.

The screenshot shows the Cisco ISE Administration interface for System. The 'Deployment' tab is active. On the left, a sidebar shows 'Deployment' and 'PAN Failover'. The main area is titled 'Deployment Nodes'. At the top right, it says 'Selected 1 Total 1'. Below this are buttons for 'Edit', 'Register', 'Syncup', and 'Deregister'. A table lists the nodes:

Hostname	Personas	Role(s)	Services	Node Status
ise01-CL1	Administration, Monitoring, Policy Service	STANDALONE	SESSION PROFILER	<span style="color: green;">✔</span>

**Stap 3.** Vink het vakje **Enable SXP Service** aan om **SXP** in te schakelen

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

**Stap 4.** Scrollt naar de onderkant en klik op **Opslaan**

**Opmerking:** Herhaal alle stappen voor de rest van de ISE-knooppunten in elke cluster, inclusief het aggregatieknooppunt.

## SXP op de clusterknooppunten configureren


**Stap 1.** Selecteer het pictogram drie lijnen  bevinden in de linker bovenhoek en selecteer in **Workforce > TrustSec > SXP**.

**Stap 2.** Klik op **+Add** om het ISE-aggregatieknooppunt te configureren als een SXP-peer.

The screenshot shows the 'SXP Devices' configuration page in Cisco ISE Work Centers - TrustSec. The '+Add' button is highlighted with a red box. The page shows a table with 2 total rows and a 'Go' button. Below the table are buttons for 'Refresh', '+Add', 'Trash', 'Edit', and 'Assign SXP Domain'.

**Stap 3.** Bepaal de **naam** en het **IP-adres** van het ISE-aggregatieknooppunt, selecteer Peerrol als

**LISTENER.** Selecteer de gewenste PSN's onder **Verbonden PSN's**, vereiste **SXP-domein**, selecteer **Ingeschakeld** onder status en selecteer **Wachtwoordtype** en gewenste **versie**.

 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

**Stap 4.** Klik op Opslaan

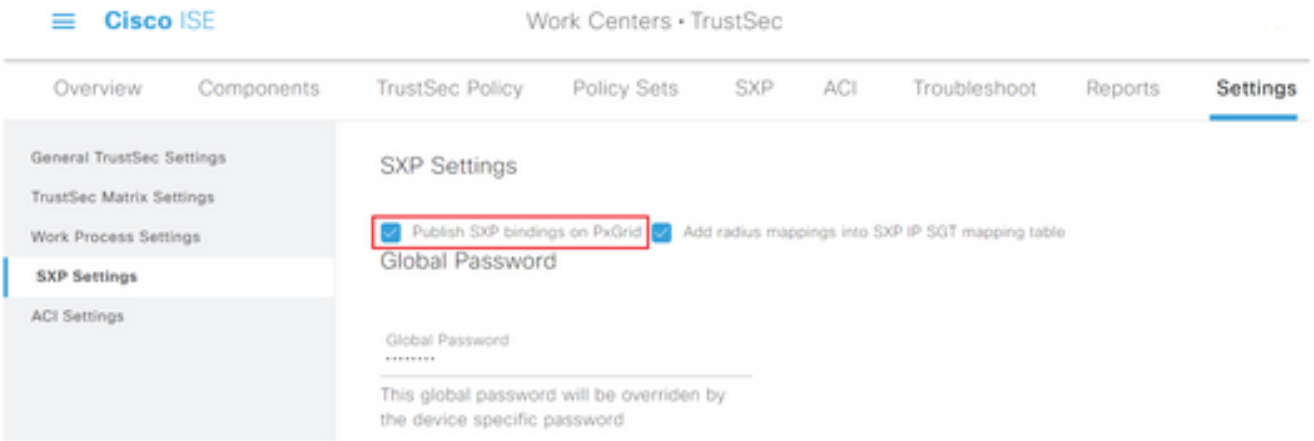
**Opmerking:** Herhaal alle stappen voor de rest van de ISE-knooppunten in elk cluster om een SXP-verbinding met het aggregatieknooppunt te maken. **Herhaal hetzelfde proces voor het aggregatieknooppunt en selecteer SPEAKER als peer rol.**

## SXP op de aggregatieknop configureren

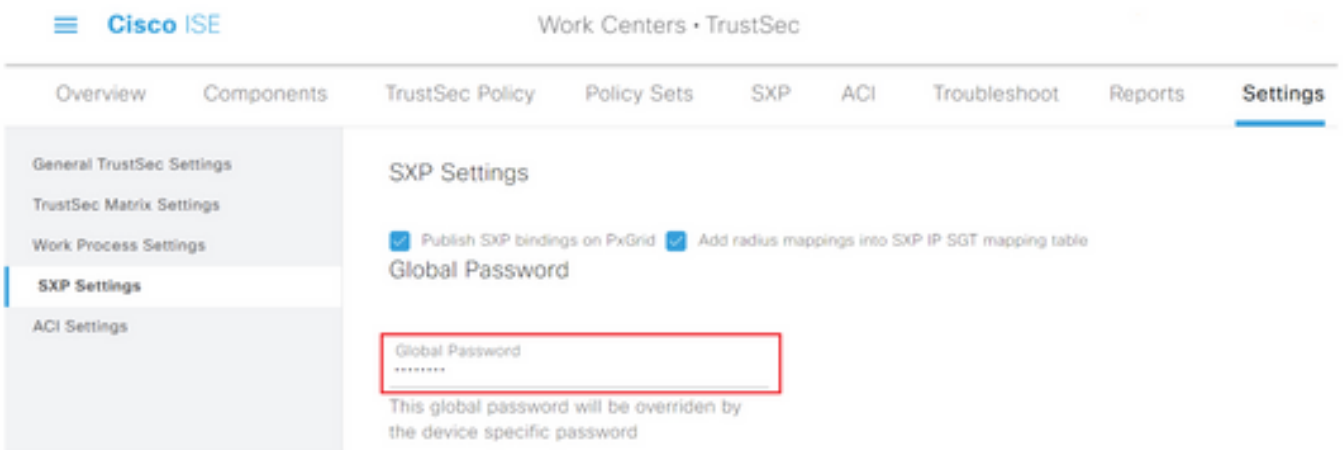
**Stap 1.** Selecteer het pictogram drie regels in de linker bovenhoek en selecteer deze optie op WorkCenter > TrustSec > Settings

**Stap 2.** Klik op het tabblad SXP-instellingen

**Stap 3.** Om de IP-SGT-mappings te propageren, vinkt u het vakje SXP-bindingen publiceren op pxGrid.



**Stap 4 (optioneel).** Definieert een standaardwachtwoord voor SXP-instellingen onder **Global Password**

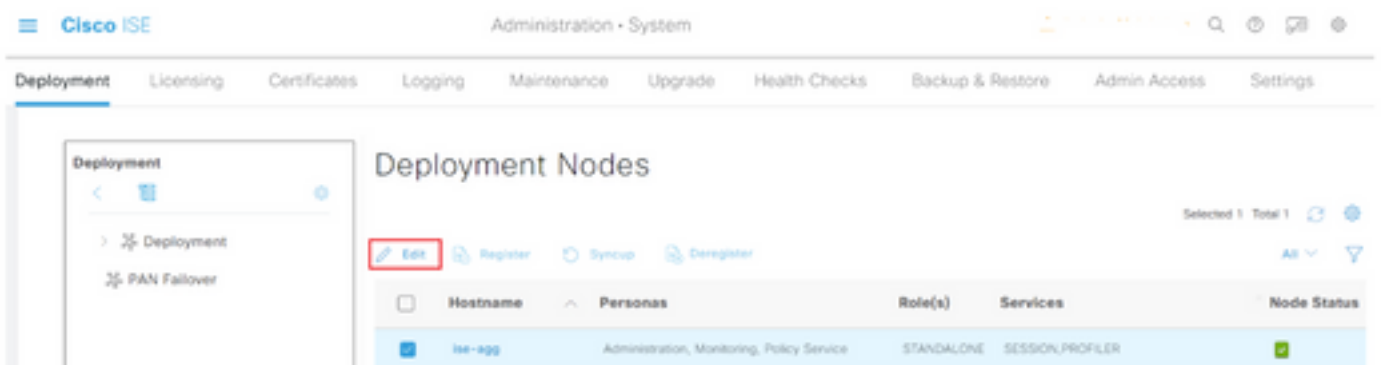


**Stap 5.** Scrollt neer en klik op **Opslaan**.

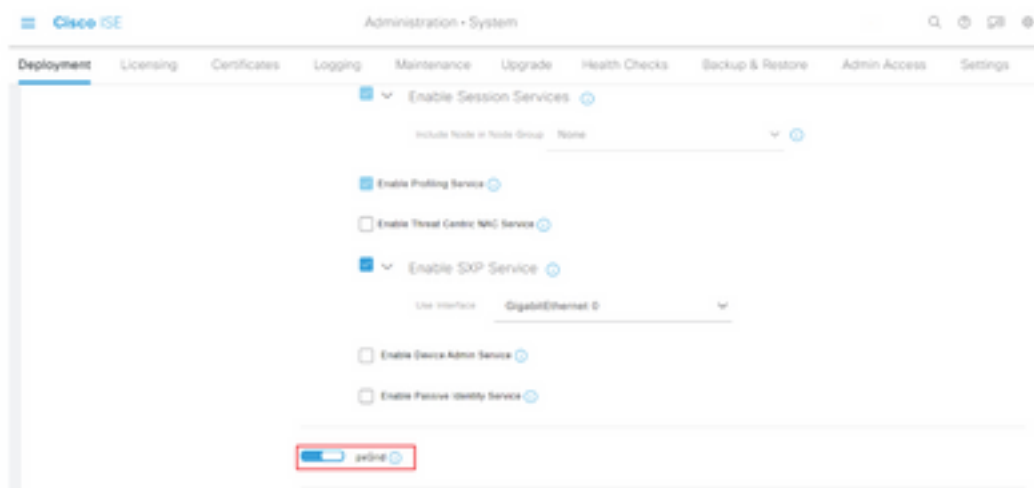
## PxGrid op het aggregatieknooppunt inschakelen

**Stap 1.** Selecteer het pictogram drie lijnen in de linker bovenhoek en selecteer dit op **Beheer > Systeem > Plaatsing**.

**Stap 2.** Selecteer het knooppunt dat u wilt configureren en klik op **Bewerken**.



**Stap 3.** Klik om pxGrid in te schakelen op de knop naast **pxGrid**.

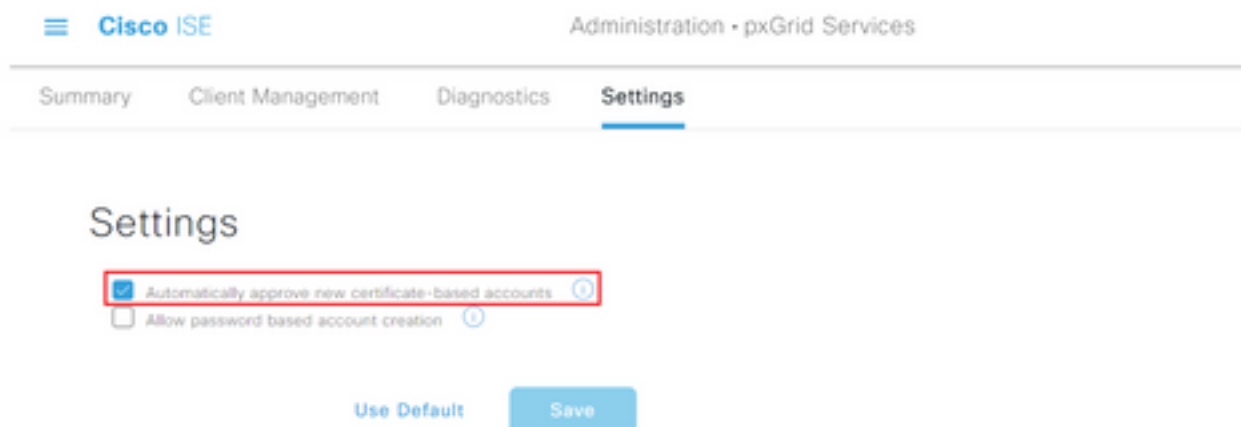


Stap 4. Scrollt naar de onderkant en klik op Opslaan.

## Automatische goedkeuring van pxGrid

Stap 1. Navigeer naar het pictogram drie lijnen in de linker bovenhoek en selecteer **Beheer > PxGrid Services > Instellingen**.

Stap 2. Standaard keurt ISE niet automatisch pxGrid de verbindingsverzoeken van nieuwe PxGrid-clients goed. Daarom moet u deze instelling inschakelen door het selectieteken te selecteren en **automatisch nieuwe op certificaat gebaseerde rekeningen goed te keuren**.



Stap 3. Klik op Opslaan

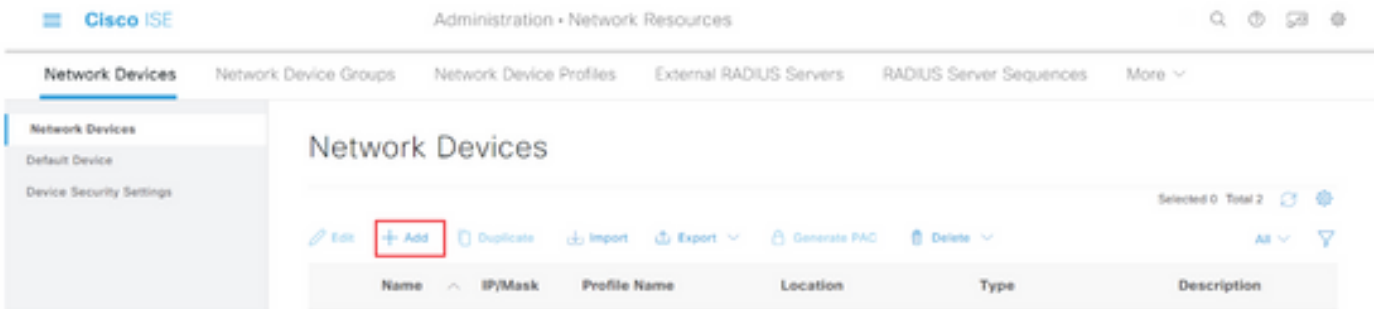
## Netwerkapparaten Instellingen voor vertrouwen

Voor Cisco ISE om verzoeken van TrustSec-enabled apparaten te verwerken, moet u deze TrustSec-enabled apparaten in Cisco ISE definiëren.

Stap 1. Navigeer naar de drie lijnen die linksboven zijn geplaatst en selecteer deze optie in **Beheer > Netwerkbronnen > Netwerkapparaten**.

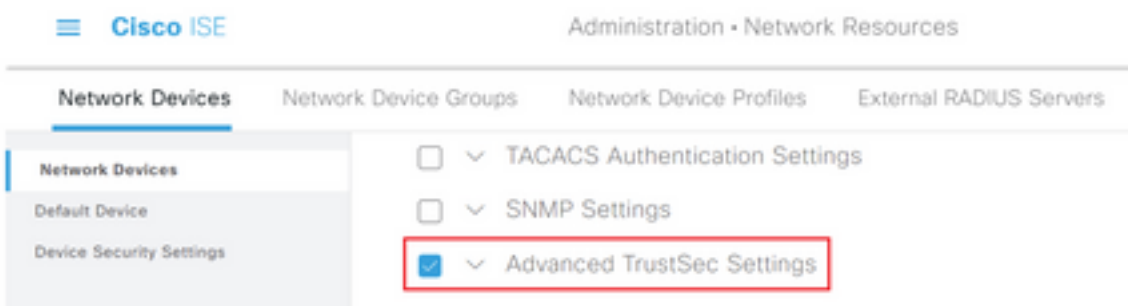
Stap 2. Klik op +Add.



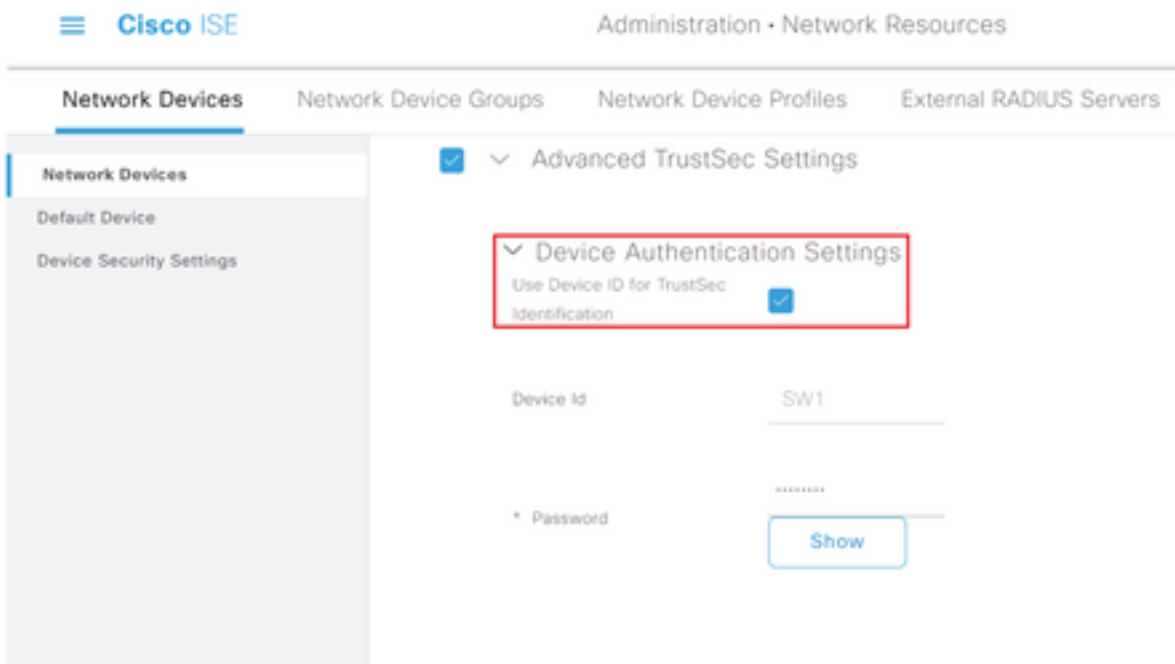


**Stap 3.** Voer de gewenste informatie in het gedeelte **Netwerkkaparameters** en in de **RADIUS-verificatie-instellingen**.

**Stap 4.** Controleer het vakje **Advanced TrustSec Settings** om een op TrustSec-enabled apparaat te configureren.

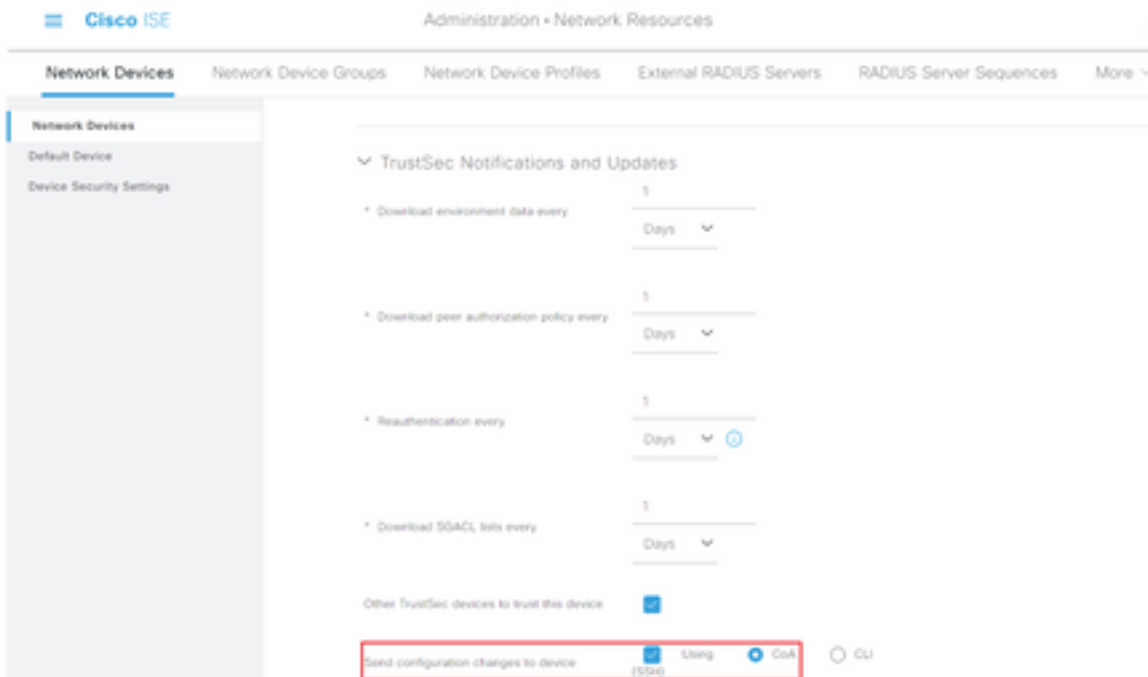


**Stap 5.** Klik op de optie **Apparaat-ID gebruiken voor de optie TechSec-identificatie** om automatisch de apparaatnaam te registreren die in het gedeelte **Netwerkkaparameters** is opgenomen. Typ een wachtwoord in het veld **Wachtwoord**.



**Opmerking:** De ID en het wachtwoord moeten overeenkomen met de opdracht "cts aanmeldingsgegevens id <ID> wachtwoord <PW>" die later op de switch wordt ingesteld.

**Stap 6.** Controleer de **configuratie-wijzigingen van het apparaat** in het aanvinkvakje **verzenden**, zodat ISE TrustSec CoA-meldingen naar het apparaat kan verzenden.



**Stap 7.** Controleer of dit apparaat ook is **gebruikt bij het aanvinken van het label** voor het koppelen van de beveiligingsgroep.

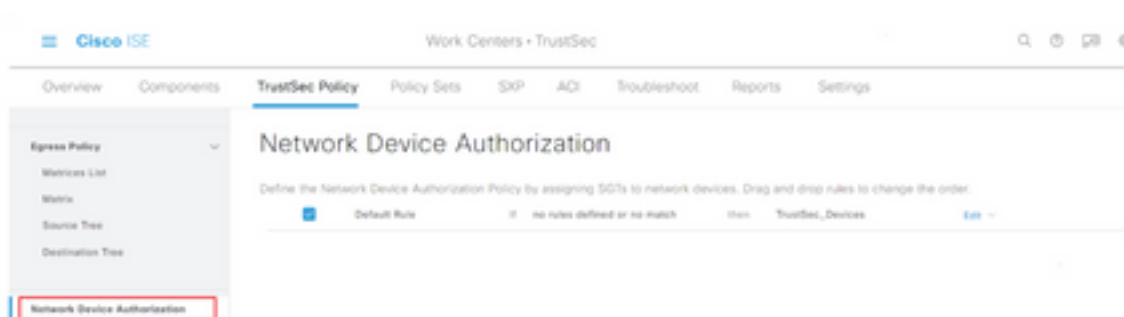
**Stap 8.** Om ISE de configuratie van het netwerkapparaat te laten bewerken, typt u de gebruikersreferenties in de velden **EXEC-mode** en **EXEC-mode wachtwoord**. Typ desgewenst het wachtwoord in het veld **Wachtwoord voor toegangsmodus**.

**Opmerking:** Herhaal de stappen voor alle andere NAD's die bedoeld zijn om deel uit te maken van het TrustSec-domein.

## Verificatie van netwerkapparaten

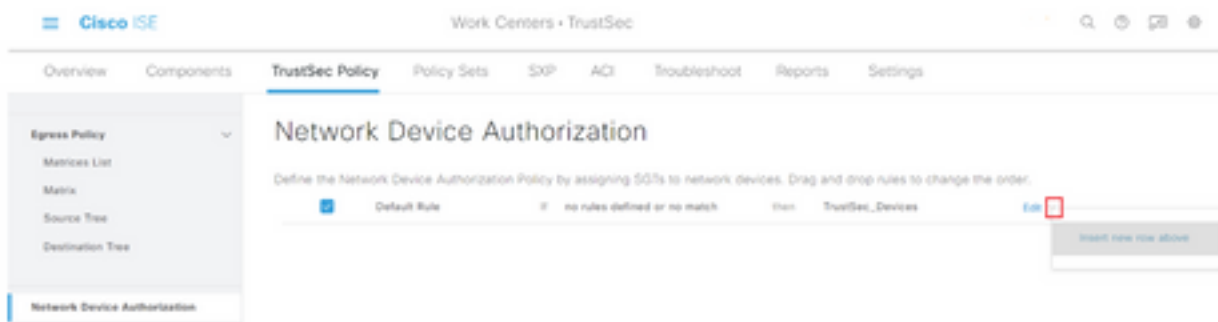
**Stap 1.** Selecteer het pictogram drie regels in de linker bovenhoek en selecteer deze optie in **Workcenters > TrustSec > TrustSec Policy**.

**Stap 2.** Klik in het linker deelvenster op **Netwerkautorisatie**.



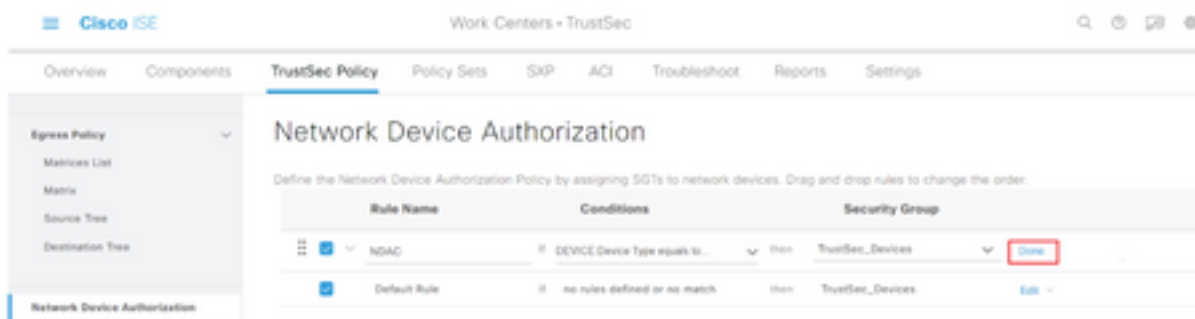
**Stap 3.** Rechts gebruikt u de vervolgkeuzelijst naast **Bewerken** en **invoegen van de nieuwe rij**

boven om een nieuwe NDA-regel te maken.



**Stap 4.** Definieer een **Naam**, **Voorwaarden** en selecteer de gewenste SGT in de vervolgkeuzelijst onder **Beveiligingsgroepen**.

**Stap 5.** Klik op Gereed naar rechts.



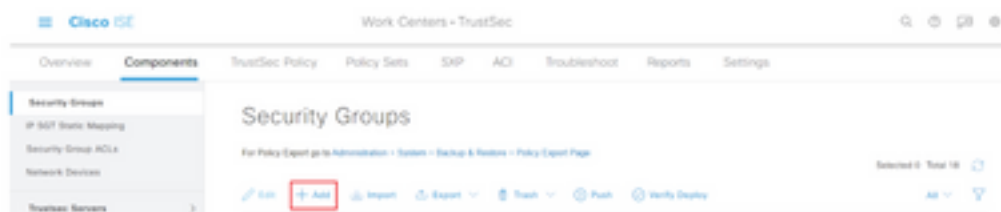
**Stap 6.** Scrollt naar beneden en klik op **Opslaan**.

## SGT

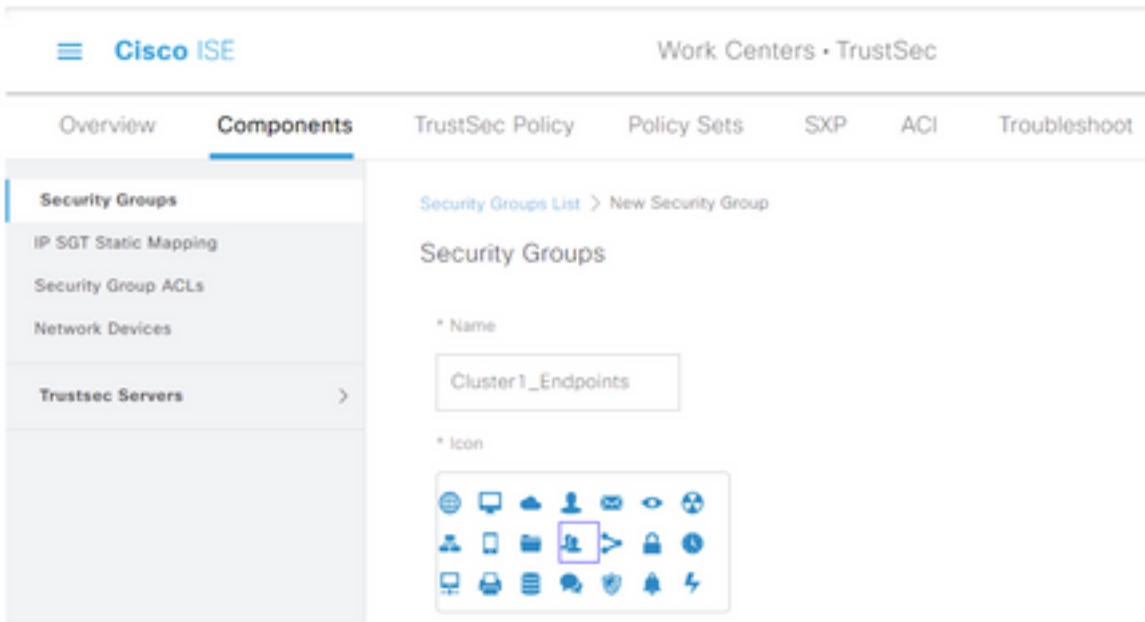
**Stap 1.** Selecteer het pictogram drie regels in de linker bovenhoek en selecteer deze optie op **Workcenters > TrustSec > Componenten**.

**Stap 2.** vouwt in het linker deelvenster **beveiligingsgroepen** uit.

**Stap 3.** Klik op **+Add** om een nieuwe SGT te maken.



**Stap 4.** Voer de naam in en kies een pictogram in de juiste velden.



**Stap 5.** Kies desgewenst een omschrijving en voer een **tagwaarde** in.

**Opmerking:** Om een tagwaarde handmatig in te kunnen voeren, navigeer naar werkcentra > TrustSec > Instellingen > General TrustSec Instellingen en selecteer de optie **Gebruiker moet SGT Number handmatig invoeren** onder **Identificatie van de Security Group**.

**Stap 6.** Scrollt neer en klik op **Indienen**

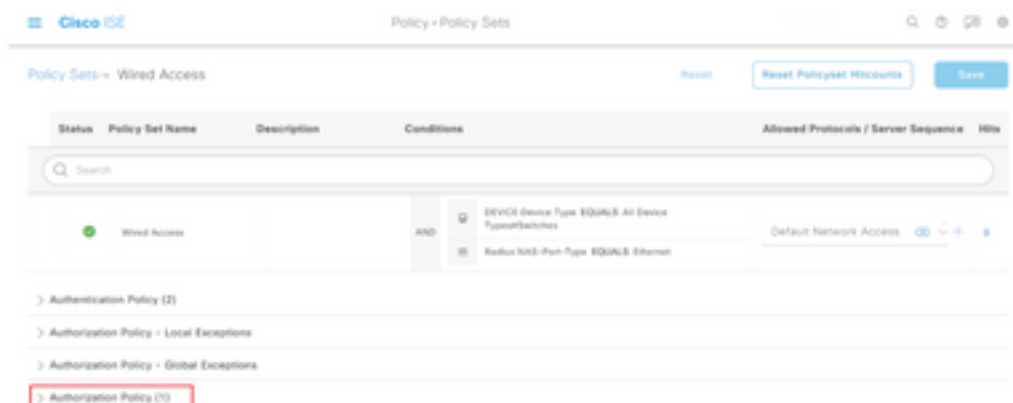
**Opmerking:** Herhaal deze stappen voor alle vereiste SGT's.


## machtigingsbeleid

**Stap 1.** Selecteer het pictogram drie regels in de linker bovenhoek en selecteer deze optie in **Beleidsformaten > Beleidsformaten**.

**Stap 2.** Selecteer de gewenste beleidsset.

**Stap 3.** Binnen het vastgestelde beleid moet het **machtigingsbeleid** worden uitgebreid.

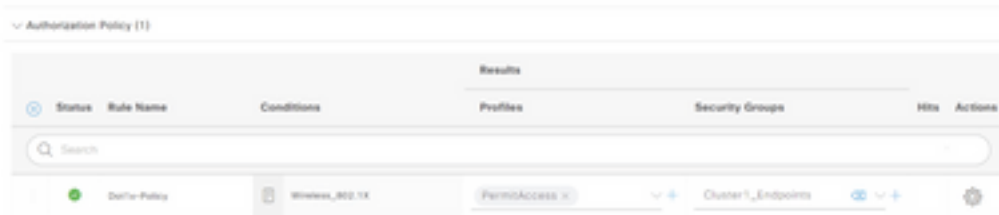


Stap 4. Klik op de  knop om een vergunningsbeleid te maken.



Authorization Policy (1)						
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
						

Stap 5. Bepaal de gewenste naam van de regel, voorwaarde/voorwaarden en profielen en selecteer de gewenste SGT in de vervolgkeuzelijst onder **Beveiligingsgroepen**.



Authorization Policy (1)						
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
						

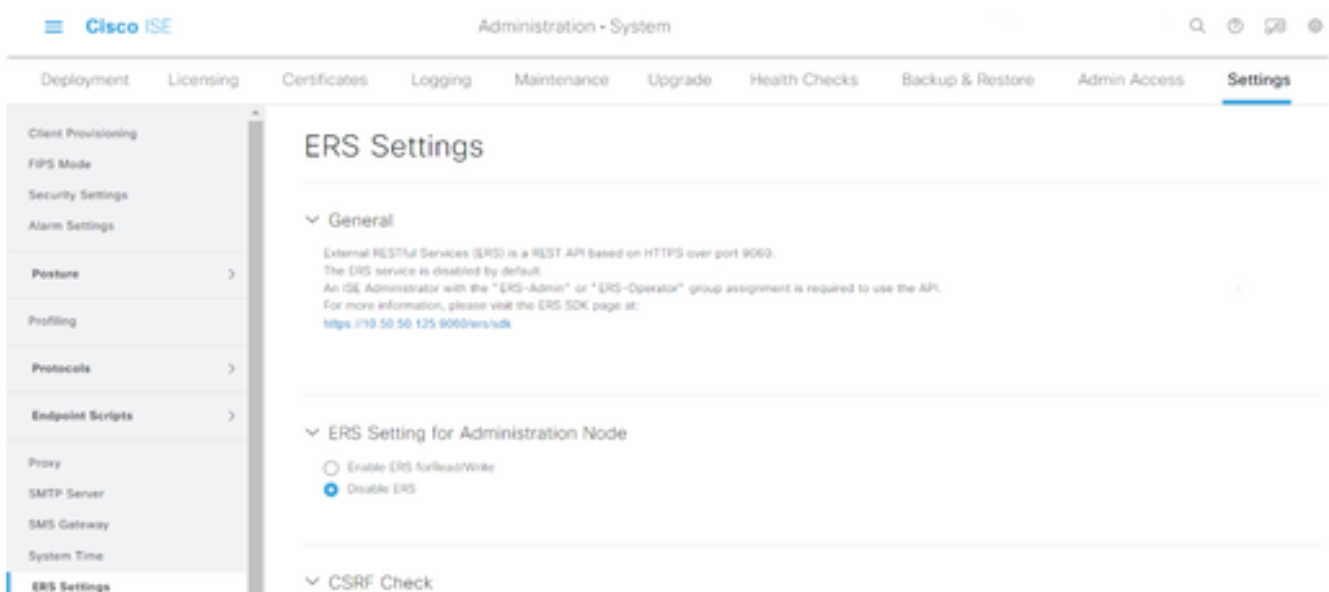
Stap 6. Klik op Opslaan.

## ERS inschakelen op ISE Aggregation Node (optioneel)

De Externe RESTful API Service (ERS) is een API die door de WSA voor groepsinformatie kan worden ingeroepen. De ERS-service is standaard uitgeschakeld op ISE. Als deze optie is ingeschakeld, kunnen klanten de API opnieuw vragen als ze zich als leden van de **ERS Admin**-groep op het ISE-knooppunt authenticiseren. U kunt de service op ISE inschakelen en een account aan de juiste groep toevoegen door de volgende stappen te volgen:

Stap 1. Selecteer het pictogram drie regels in de linker bovenhoek en selecteer deze optie op **Beheer > Systeem > Instellingen**.

Stap 2. Klik in het linker venster op **ERS-instellingen**.



Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Client Provisioning  
FIPS Mode  
Security Settings  
Alarm Settings  
**Posture** >  
Profiling  
Protocols >  
Endpoint Scripts >  
Proxy  
SMTP Server  
SMS Gateway  
System Time  
**ERS Settings**

### ERS Settings

**General**

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060. The ERS service is disabled by default. An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API. For more information, please visit the ERS SDK page at: <https://10.50.50.125:9060/ers/sdk>

**ERS Setting for Administration Node**

Enable ERS forRead/Write  
 **Disable ERS**

**CSRF Check**

Stap 3. Selecteer de optie **ERS** voor lezen/schrijven inschakelen.

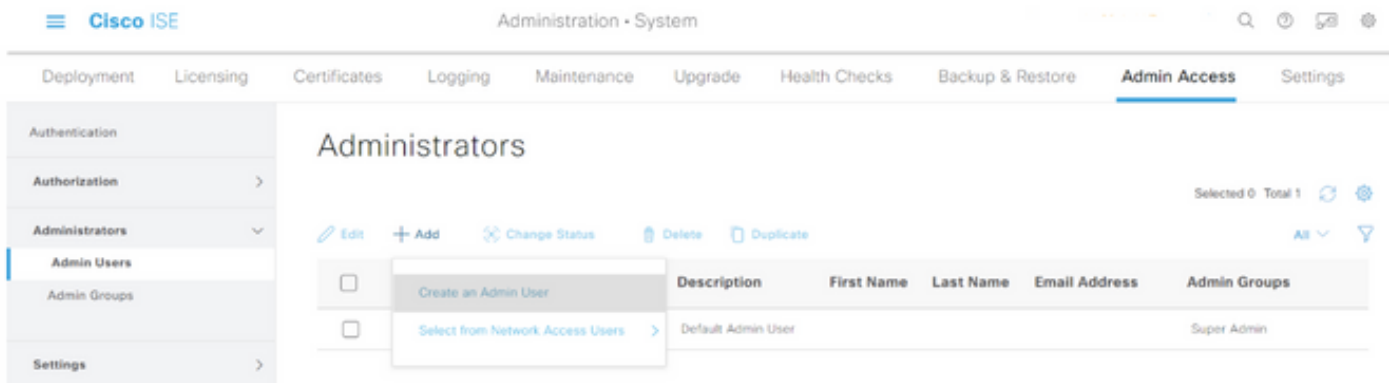
Stap 4. Klik op **Opslaan** en bevestig met **OK**.

## Gebruiker toevoegen aan ESR Admin-groep (optioneel)

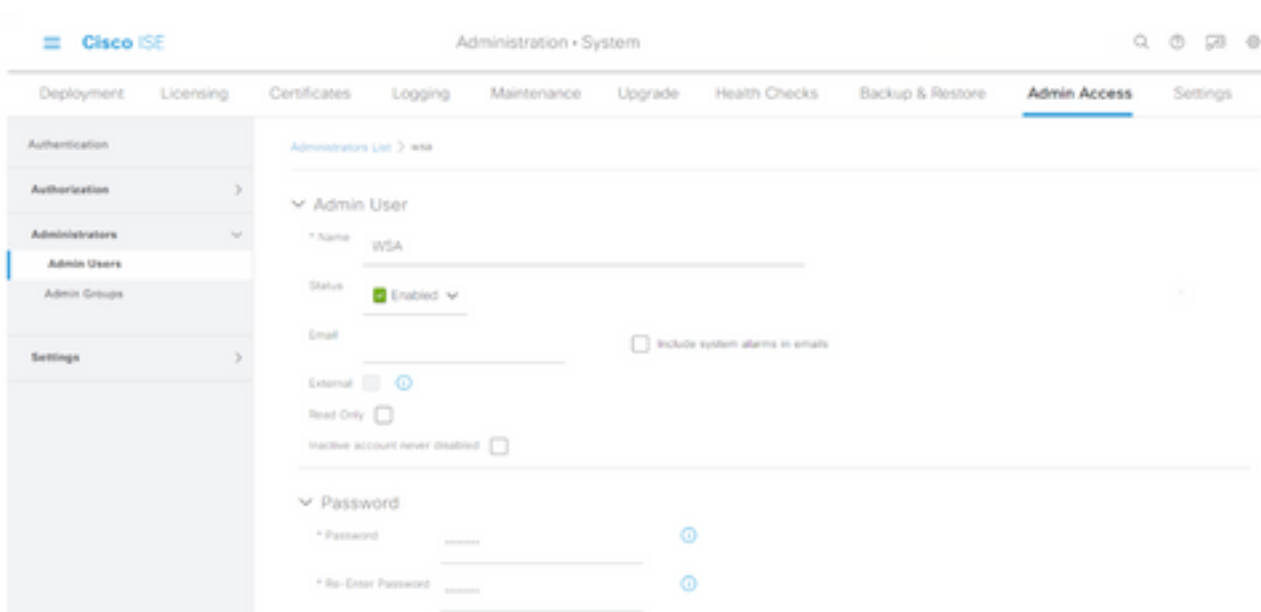
Stap 1. Selecteer het pictogram drie regels in de linker bovenhoek en selecteer **Beheer > Systeem > Admin Access**

Stap 2. Vul in het linker venster de **beheerders uit** en klik op **Admin-gebruikers**.

Stap 3. Klik op **+Add** en selecteer **Admin User** uit de vervolgkeuzelijst.



Stap 4. Voer in de juiste velden een gebruikersnaam en een wachtwoord in.



Stap 5. Gebruik in het veld **Admin Groepen** de vervolgkeuzelijst om **ERS Admin** te selecteren.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. Below this is a secondary navigation bar with tabs: 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access' (selected), and 'Settings'. On the left is a sidebar menu 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 input fields for 'First Name' and 'Last Name'. Below these is the 'Account Options' section with a 'Description' text area. The 'Admin Groups' section contains a list of groups, with 'ERS Admin' selected in a dropdown menu, which is highlighted with a red box. At the bottom right of the form are 'Save' and 'Reset' buttons.

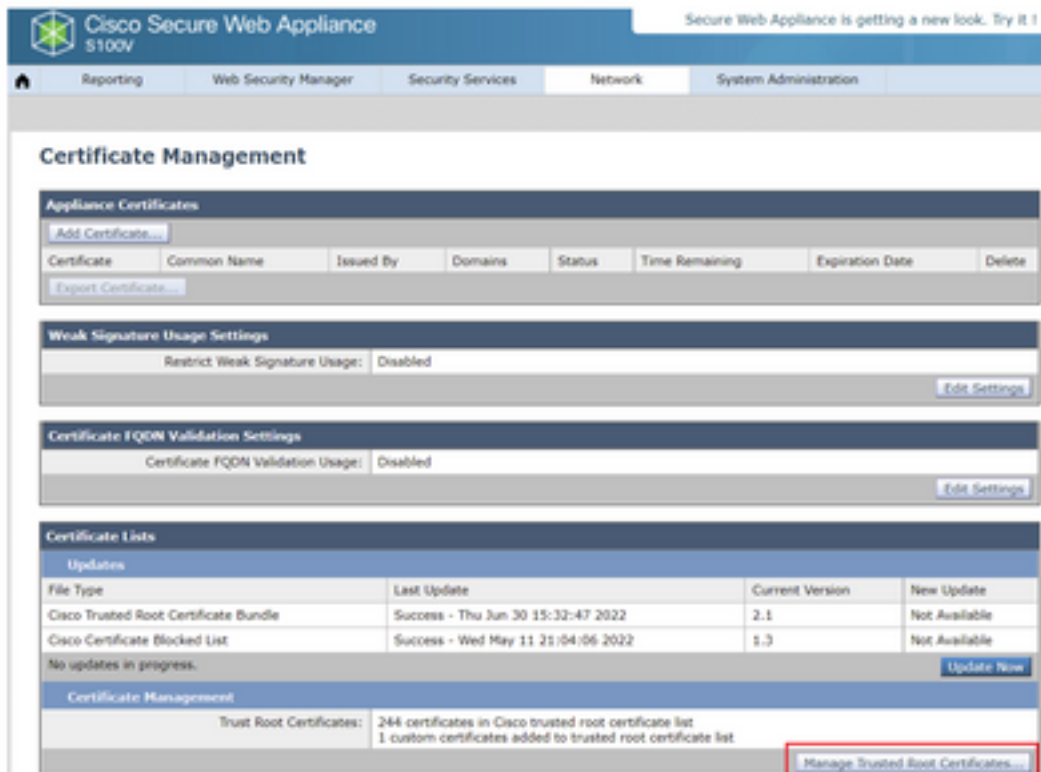
Stap 6. Klik op Opslaan.

## Configuratie van beveiligde web-applicatie

### Root-certificaat

Indien het integratieontwerp een interne certificeringsinstantie gebruikt als bron van vertrouwen voor de verbinding tussen de WSA en ISE, dan moet dit basiscertificaat op beide apparaten worden geïnstalleerd.

**Stap 1** . Navigeer naar **Netwerk > certificaatbeheer** en klik op **Trusted Root Certificates beheren** om een CA-certificaat toe te voegen.



Stap 2. Klik op Importeren.



Stap 3. Klik op Kies bestand om de gegenereerde wortelen te vinden en klik op Verzenden.

Stap 4. Klik nogmaals op Indienen.

Stap 5. Klik rechtsboven op Aanpassen.



Stap 6. Klik nogmaals op Aanmelden voor wijzigingen.

## PxGrid-certificaat

In de WSA, wordt de creatie van het zeer belangrijke paar en het certificaat voor gebruik door pxGrid voltooid als deel van de ISE dienstconfiguratie.

Stap 1. Navigeer naar Network > Identity Services Engine.

Stap 2. Klik op Instellingen inschakelen en bewerken.

Stap 3. Klik op Kies bestand om de gegenereerde wortelen te vinden en klik op Upload File.



**Opmerking:** Een veel voorkomende misconfiguratie is het uploaden van het ISE pxGrid-certificaat in deze sectie. Het basiscertificaat van CA moet worden geüpload naar het veld ISE PxGrid Node.

**Stap 4.** Selecteer in het gedeelte **Web applicatie Client certificaatcertificaat**, de optie **Gegenereerd certificaat en sleutel gebruiken**.

**Stap 5.** Klik op de knop **Nieuw certificaat genereren en sleutel** tot het invullen van de vereiste certificaatvelden.

**Stap 6.** Klik op de **aanvraag** voor het downloaden van certificaten.

**Opmerking:** Het wordt aanbevolen de knop **Indienen** te selecteren om de wijzigingen in de ISE-configuratie aan te brengen. Als de sessie wordt overgelaten aan de tijdelijke versie voordat de wijzigingen worden verzonden, kunnen de sleutels en het certificaat dat werd

gegenereerd verloren gaan, zelfs als de CSR was gedownload.

**Stap 7.** Klik nadat u de CSR met uw CA hebt ondertekend op **Kies bestand** om het certificaat te vinden.

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

**Stap 8.** Klik op **Upload File**.

**Stap 9.** Indienen en beloven.

## SXP en ERS inschakelen voor beveiligde webapplicatie

**Stap 1.** Klik op de knoppen **Enable** voor zowel SXP als ERS.

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

Enable ISE External Realmful Service (ERS)

The Web Appliance retrieves Active Directory groups, and local SXP 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.

**Stap 2.** Voer in het veld Administrator **Credentials** van **ERS** de gebruikersinformatie in die op ISE is ingesteld.

**Stap 3.** Controleer het vakje voor **Server dezelfde naam als ISE pxGrid Node** om de vorige geconfigureerde informatie te erven. Voer anders de vereiste informatie in.

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)

Stap 4. Indienen en beloven.

## Identificatieprofiel

Om de veiligheidsgroepstags of ISE-groepsinformatie in het WSA-beleid te kunnen gebruiken, moet eerst een identificatieprofiel worden gecreëerd dat ISE gebruikt als middel om op transparante wijze gebruikers te identificeren.

Stap 1. Navigeer naar **Web Security Manager > Verificatie > Identificatieprofielen**.

Stap 2. Klik op **Identificatieprofiel toevoegen**.

Stap 3. Voer een naam in en kies een omschrijving.

Stap 4. In het **gedeelte Identificatie en Verificatie**, gebruik de vervolgkeuzelijst om **gebruikers met ISE** te kiezen.

### 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:db8::1-2000:db8::10)

Define Members by Protocol:  HTTP/HTTPS

Define additional group membership criteria.

Stap 5. Indienen en beloven.

## SGT-gebaseerd decryptiebeleid

Stap 1. Navigeer naar **Web Security Manager > Web Policy > Decryptie Policy**.

**Stap 2.** Klik op **Add Policy**.

**Stap 3.** Voer een naam in en kies een omschrijving.

**Stap 4.** Gebruik in het gedeelte **Identificatieprofielen** en gebruikers de vervolgkeuzelijst om **een of meer identificatieprofielen** te selecteren.

**Stap 5.** Gebruik in het gedeelte **Identificatieprofielen** de vervolgkeuzelijst om de naam van het ISE-identificatieprofiel te kiezen.

**Stap 6.** Selecteer in het gedeelte **Geautoriseerde gebruikers en groepen** de optie **Geselecteerde groepen en gebruikers**.

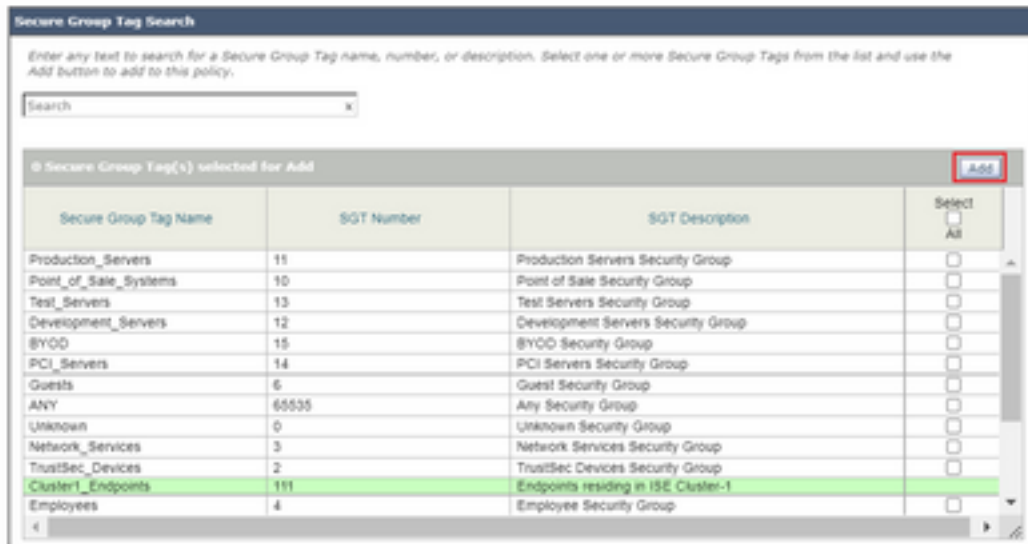
The screenshot shows the 'Policy Member Definition' configuration page. At the top, it states: 'Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.' Below this, there are two main sections: 'Identification Profiles and Users' and 'Authorized Users and Groups'. In the 'Identification Profiles and Users' section, a dropdown menu is set to 'Select One or More Identification Profiles', and 'ISE Profile' is selected. In the 'Authorized Users and Groups' section, the 'Selected Groups and Users' radio button is selected. Below this, it shows 'ISE Secure Group Tags: No tags entered', 'ISE Groups: No groups entered', and 'Users: No users entered'. There is also an 'Add Identification Profile' button on the right. At the bottom, there is a note: 'Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.' and an 'Advanced' link to 'Define additional group membership criteria.'

**Stap 7.** Klik op de hyperlink naast de **ISE Secure Group-tags**.

**Stap 8.** In het gedeelte **Secure Group Search**, kruis het vakje rechts van de gewenste SGT en klik op **Add**.

The screenshot shows the 'Authorized Secure Group Tags' configuration page. It includes a search function and a table of currently included tags. The table has four columns: 'Secure Group Tag Name', 'SGT Number', 'SGT Description', and 'Delete'. One tag is listed: 'Cluster1\_Endpoints' with SGT Number '111' and description 'Endpoints residing in ISE Cluster-1'. There is a 'Delete' button at the bottom right.

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



Stap 9. Klik op Gereedschap om terug te keren.

Stap 10. Indienen en beloven.

## Switchconfiguratie

### 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

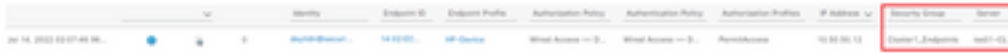
```
cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode)
cts role-based enforcement
```

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

# Verifiëren

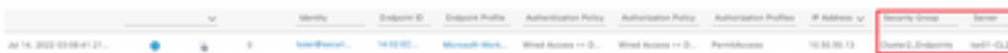
## SGT toewijzing van ISE aan eindpunt.

Hier kunt u een eindpunt van ISE Cluster 1 zien die een SGT toegewezen heeft na succesvolle authenticatie en vergunning:



Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authentication Profile	IP Address	Security Group	Domain
10.50.50.13	14-02-001	IP Device	What Access -->	What Access -->	Permissoes	10.50.50.13	Cluster1_Endpoints	ise01-01.1

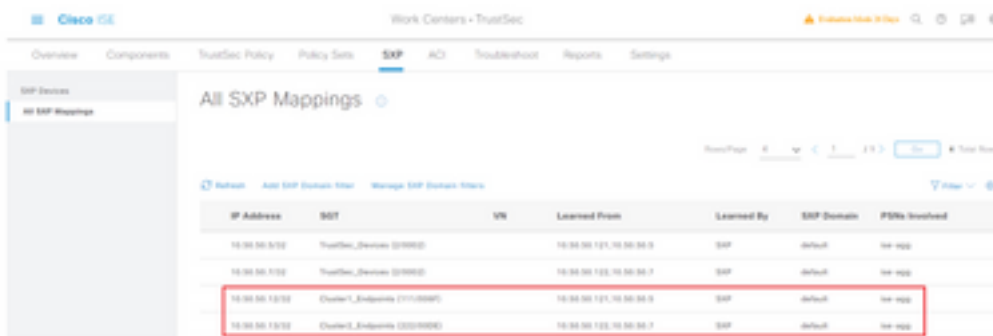
Hier kunt u een eindpunt van ISE Cluster 2 zien die een SGT toegewezen heeft na succesvolle authenticatie en vergunning:



Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authentication Profile	IP Address	Security Group	Domain
10.50.50.12	14-02-002	Microsoft-Work	What Access -->	What Access -->	Permissoes	10.50.50.12	Cluster2_Endpoints	ise01-01.1

## SXP-afbeeldingen

Aangezien SXP-communicatie tussen de clusterISE-knooppunten en de ISE-aggregatieknooppunt is ingeschakeld, worden deze SGT-IP-mappings geleerd door ISE-aggregatie via SXP:



IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PDNs Inherited
10.50.50.13	TrustSec_Device (20000)		10.50.50.121.10.50.50.0	SXP	default	no-ipp
10.50.50.13	TrustSec_Device (20000)		10.50.50.122.10.50.50.7	SXP	default	no-ipp
10.50.50.12	Cluster1_Endpoints (1110000)		10.50.50.121.10.50.50.0	SXP	default	no-ipp
10.50.50.12	Cluster2_Endpoints (2220000)		10.50.50.122.10.50.50.7	SXP	default	no-ipp

Deze SXP-mappings, van verschillende ISE-clusters, worden dan naar WSA via pxGrid door het ISE-aggregatieknooppunt verzonden:

```
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 ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[ ]> show
IP                username                               SGT#  Port Range
10.50.50.13       1sesxp_10.50.50.122_sgt222_10.50.50.13 222   -
10.50.50.12       1sesxp_10.50.50.121_sgt111_10.50.50.12 111   -
```

## Op SGT gebaseerde beleidshandhaving

Hier zie je dat de verschillende endpoints overeenkomen met hun respectievelijke beleid en dat verkeer geblokkeerd is op basis van hun SGT:

Endpoint dat behoort tot 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 (count)	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:28:17	<a href="https://bbc.com/#43/television">https://bbc.com/#43/television</a> CONTENT TYPE: - URL CATEGORY: Block URLs CL1 DESTINATION IP: - DETAILS: Decryption Policy: 'ISE_Cluster1', WBS: 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 dat behoort tot 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	<a href="https://www.facebook.com/#43/television">https://www.facebook.com/#43/television</a> CONTENT TYPE: - URL CATEGORY: Block URLs CL2 DESTINATION IP: - DETAILS: Decryption Policy: 'ISE_Cluster2', WBS: No Score, Malware Analytics File Verdict: -	Block - URL Cat	0B	isesxp_10.50.50.122_sgt222_10.50.50.13 (Identified by ISE) 10.50.50.13

## Gerelateerde informatie

- [Integratiegids voor web security applicatie en Identity Services Engine](#)

- [WSA-integratie met ISE configureren voor TrustSec Aware Services](#)
- [Administrator-gids voor Cisco Identity Services Engine, release 3.1](#)
- [Gebruikershandleiding voor AsyncOS 14.5 voor Cisco Secure Web Appliance](#)