

Intégrer plusieurs clusters ISE avec une appliance Web sécurisée pour les stratégies basées sur TrustSec

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Limites](#)

[Diagramme du réseau](#)

[Configuration](#)

[Configuration ISE](#)

[Activer SXP](#)

[Configurer SXP sur les noeuds de cluster](#)

[Configurer SXP sur le noeud d'agrégation](#)

[Activer pxGrid sur le noeud d'agrégation](#)

[Approbation automatique pxGrid](#)

[Paramètres TrustSec des périphériques réseau](#)

[Autorisation des périphériques réseau](#)

[SGT](#)

[Stratégie d'autorisation](#)

[Activation de l'ERS sur le noeud d'agrégation ISE \(facultatif\)](#)

[Ajouter un utilisateur au groupe d'administration ESR \(facultatif\)](#)

[Configuration sécurisée des appareils Web](#)

[certificat pxGrid](#)

[Activer SXP et ERS sur l'appliance Web sécurisée](#)

[Profil d'identification](#)

[Stratégie de déchiffrement basée sur SGT](#)

[Configuration du commutateur](#)

[AAA](#)

[TrustSec](#)

[Vérification](#)

[Informations connexes](#)

Introduction

Ce document décrit la procédure à suivre pour envoyer des informations SGT (Security Group Tag) de plusieurs déploiements ISE à un seul appareil Web sécurisé Cisco (officiellement Web Security Appliance WSA) via pxGrid afin de tirer parti des stratégies d'accès Web basées sur SGT dans un déploiement TrustSec.

Avant la version 14.5, Secure Web Appliance ne peut s'intégrer qu'à un seul cluster ISE pour les stratégies d'identité basées sur SGT. Avec l'introduction de cette nouvelle version, Secure Web Appliance peut désormais interagir avec des informations provenant de plusieurs clusters ISE avec un noeud ISE distinct qui s'agrège entre eux. Cela apporte un grand avantage et nous permet d'exporter des données utilisateur de différents clusters ISE et de contrôler le point de sortie qu'un utilisateur peut utiliser sans avoir besoin d'une intégration 1:1.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Identity Services Engine (ISE)
- Appareil Web sécurisé
- protocole RADIUS
- TrustSec
- pxGrid

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

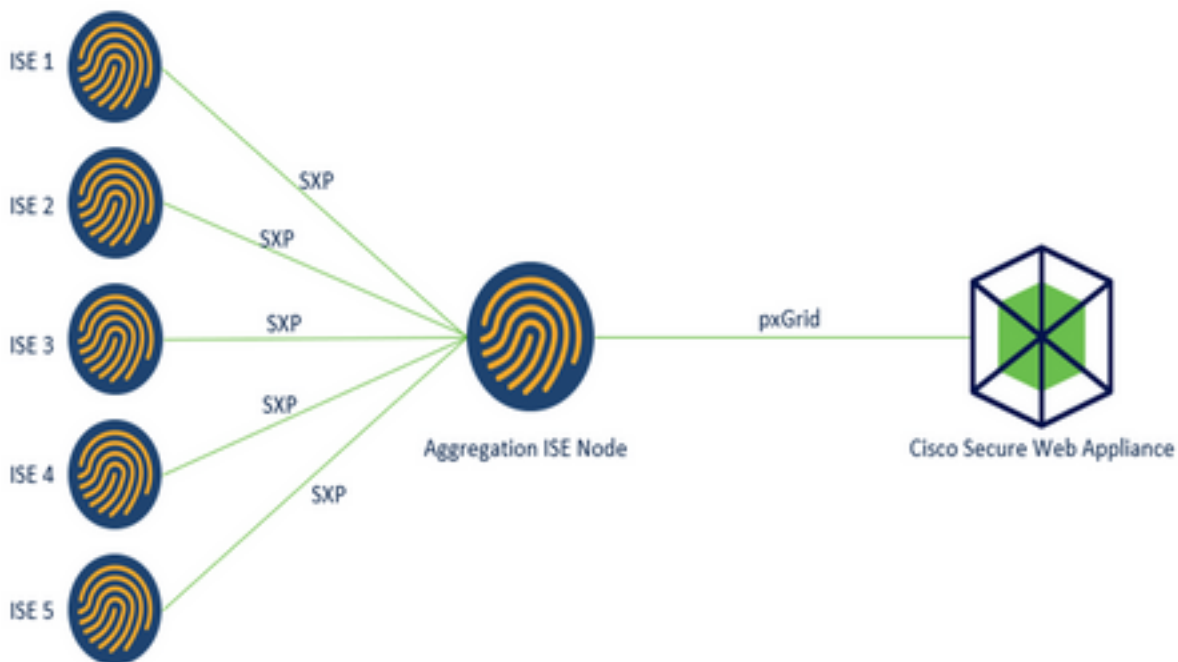
- Appareil Web sécurisé 14.5
- ISE version 3.1 P3

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Limites

1. Tous les clusters ISE doivent maintenir des mappages uniformes pour les balises de groupe de sécurité.
2. Le noeud d'agrégation ISE doit avoir le nom/numéro des SGT des autres clusters ISE.
3. L'appliance Web sécurisée peut uniquement identifier la stratégie (accès/déchiffrement/routage) en fonction de la balise SGT et non de de groupe ou de nom d'utilisateur.
4. Le reporting et le suivi sont des basées sur SGT.
5. Les paramètres de dimensionnement ISE/Secure Web Appliance existants continuent de s'appliquer à cette fonctionnalité.

Diagramme du réseau



Process:

1. Lorsque l'utilisateur final se connecte au réseau, il reçoit une SGT basée sur les stratégies d'autorisation dans ISE.
2. Les différents clusters ISE envoient ensuite ces informations SGT sous forme de mappages SGT-IP au noeud d'agrégation ISE via SXP.
3. Le noeud d'agrégation ISE reçoit ces informations et les partage avec l'appliance Web sécurisée unique via pxGrid.
4. Secure Web Appliance utilise les informations SGT qu'il a apprises pour fournir un accès aux utilisateurs en fonction des stratégies d'accès Web.

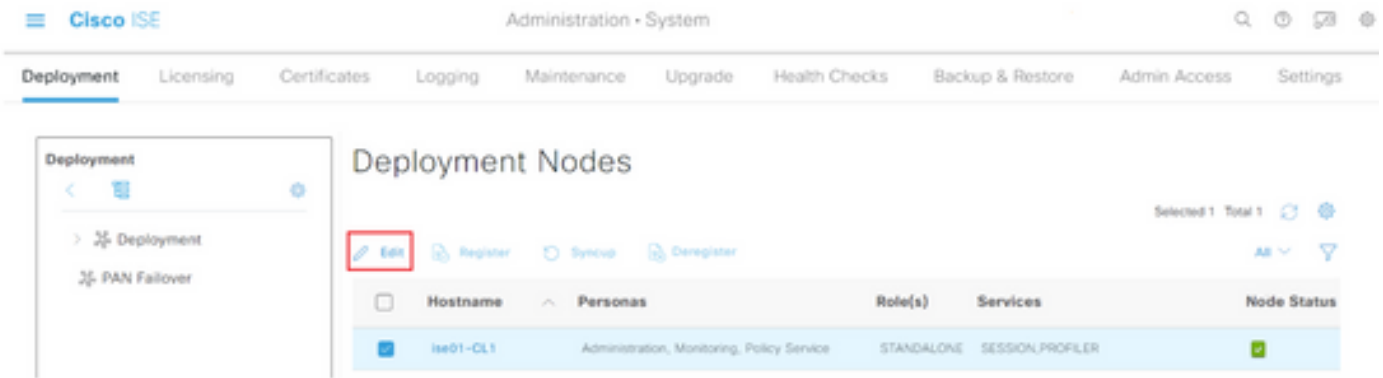
Configuration

Configuration ISE

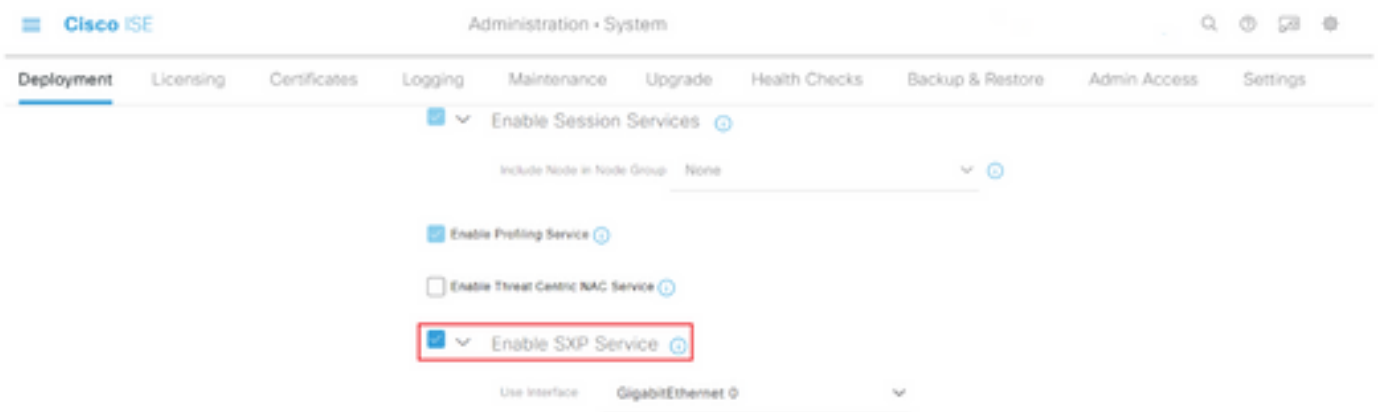
Activer SXP

Étape 1. Sélectionner l'icône des trois lignes  situé dans le coin supérieur gauche et sélectionnez **Administration > System > Deployment**.

Étape 2. Sélectionnez le noeud à configurer et cliquez sur **Modifier**.



Étape 3. Pour activer SXP, cochez la case **Activer le service SXP**



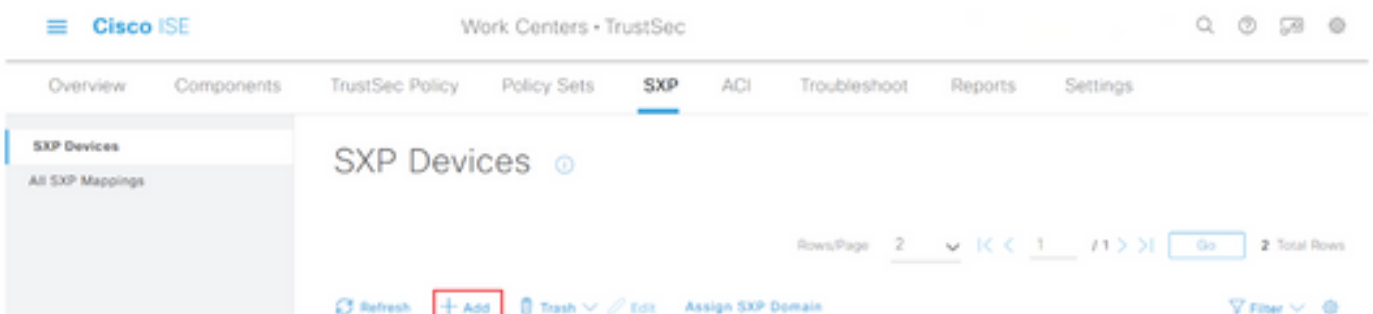
Étape 4. Faites défiler la page vers le bas et cliquez sur **Enregistrer**

Note: Répétez toutes les étapes pour les autres noeuds ISE de chaque cluster, le noeud d'agrégation inclus.

Configurer SXP sur les noeuds de cluster

Étape 1. Sélectionner l'icône des trois lignes  situé dans le coin supérieur gauche et sélectionnez **Centre de travail > TrustSec > SXP**.

Étape 2. Cliquez sur **+Ajouter** pour configurer le noeud d'agrégation ISE en tant qu'homologue SXP.



Étape 3. Définissez le **nom** et l'**adresse IP** du noeud d'agrégation ISE, sélectionnez le rôle homologue en tant que **LISTENER**. Sélectionnez les PSN requis sous **PSN connectés**, les **domaines SXP** requis, sélectionnez **Activé** sous l'état, puis **Type de mot de passe** et **Version requise**.

The screenshot shows the Cisco ISE Work Centers - TrustSec interface. The navigation bar includes 'Overview', 'Components', 'TrustSec Policy', 'Policy Sets', 'SXP', and 'ACI'. The 'SXP' tab is active. The left sidebar shows 'SXP Devices' and 'All SXP Mappings'. The main content area displays the 'SXP Connection' configuration page. It includes a breadcrumb 'SXP Devices > SXP Connection', an 'Upload from a CSV file' button, and an 'Add Single Device' dropdown menu. Below this, a note states 'Input fields marked with an asterisk (*) are required.' The form fields are: 'Name' (ISE Aggregation node), 'IP Address *' (10.50.50.125), 'Peer Role *' (LISTENER), and 'Connected PSNs *' (ise01-CL1).

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

Étape 4. Cliquez sur **Save** (enregistrer)

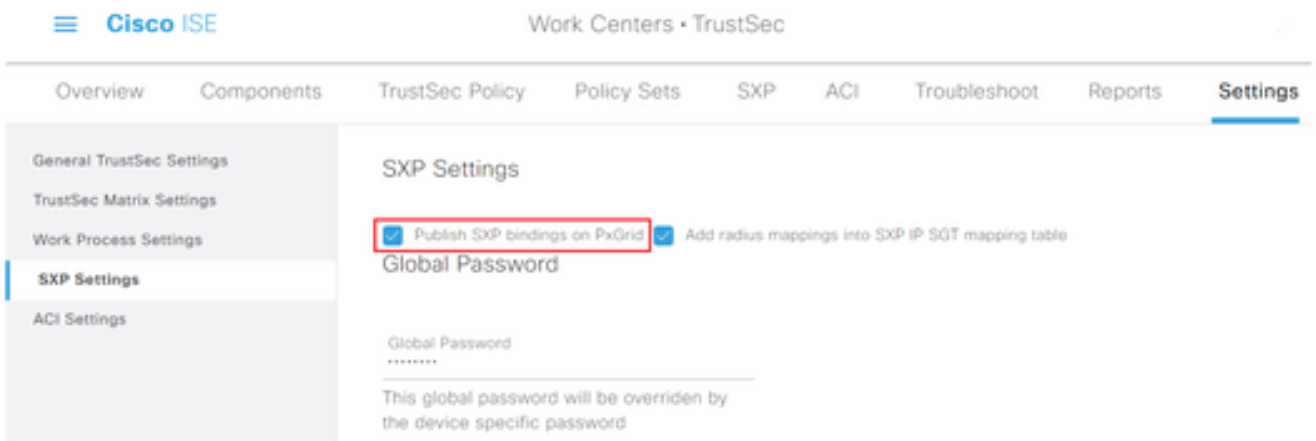
Note: Répétez toutes les étapes pour les autres nœuds ISE de chaque cluster pour créer une connexion SXP au nœud d'agrégation. **Répétez le même processus sur le nœud d'agrégation et sélectionnez SPEAKER comme rôle homologue.**

Configurer SXP sur le nœud d'agrégation

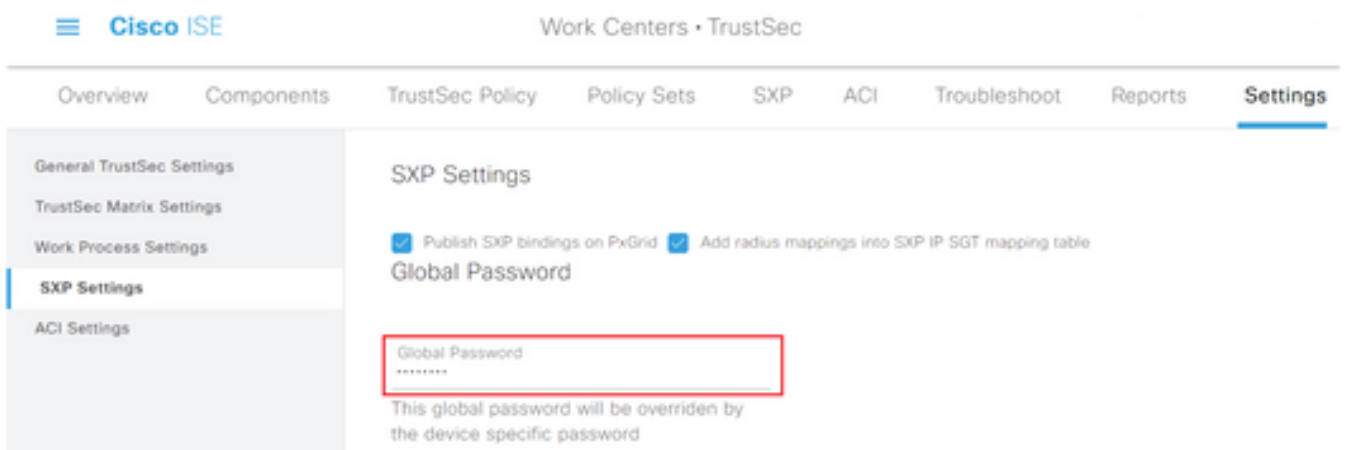
Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez dans **Centre de travail > TrustSec > Paramètres.**

Étape 2. Cliquez sur l'onglet **Paramètres SXP**

Étape 3. Pour propager les mappages IP-SGT, cochez la case **Publier les liaisons SXP sur pxGrid.**



Étape 4 (facultatif). Définir un mot de passe par défaut pour les paramètres SXP sous **Mot de passe global**

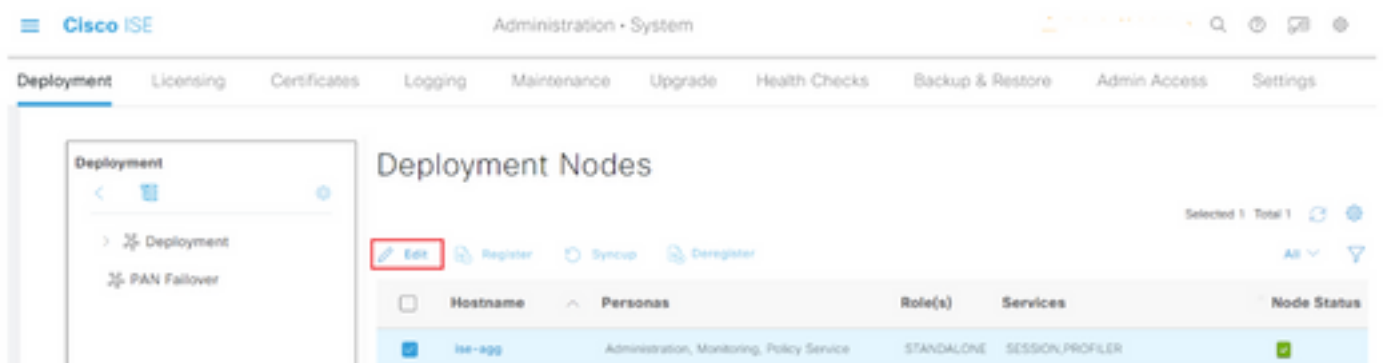


Étape 5. Faites défiler la liste vers le bas et cliquez sur **Enregistrer**.

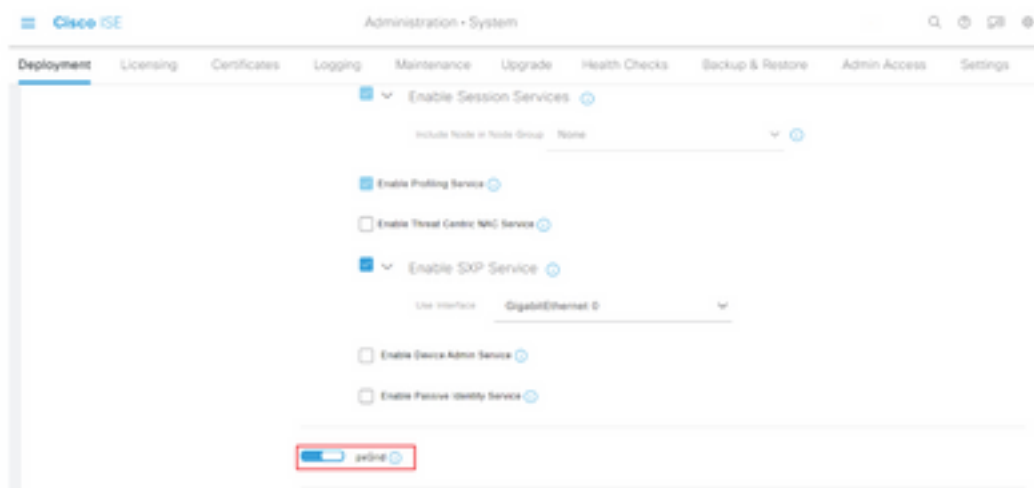
Activer pxGrid sur le noeud d'agrégation

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez **Administration > System > Deployment**.

Étape 2. Sélectionnez le noeud à configurer et cliquez sur **Modifier**.



Étape 3. Pour activer pxGrid, cliquez sur le bouton en regard de **pxGrid**.

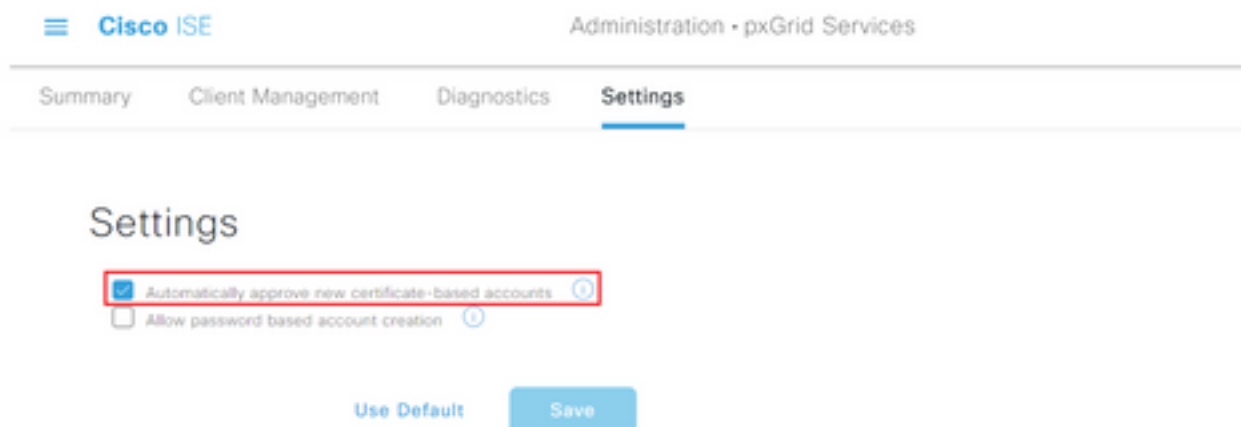


Étape 4. Faites défiler la page vers le bas et cliquez sur **Enregistrer**.

Approbation automatique pxGrid

Étape 1. Accédez à l'icône de trois lignes située dans le coin supérieur gauche et sélectionnez **Administration > pxGrid Services > Settings**.

Étape 2. Par défaut, ISE n'approuve pas automatiquement pxGrid les demandes de connexion des nouveaux clients pxGrid. Par conséquent, vous devez activer ce paramètre en cochant la case **Approuver automatiquement les nouveaux comptes basés sur des certificats**.



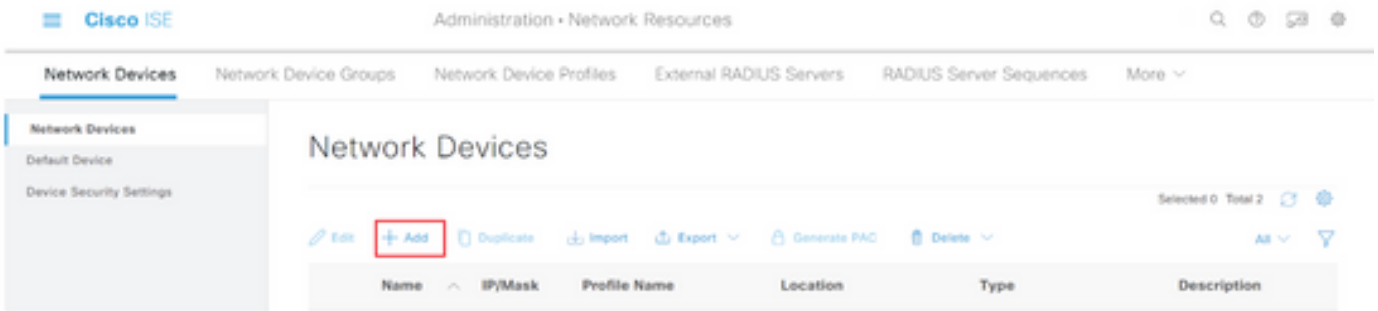
Étape 3. Cliquez sur **Save (enregistrer)**

Paramètres TrustSec des périphériques réseau

Pour que Cisco ISE traite les demandes des périphériques compatibles TrustSec, vous devez définir ces périphériques compatibles TrustSec dans Cisco ISE.

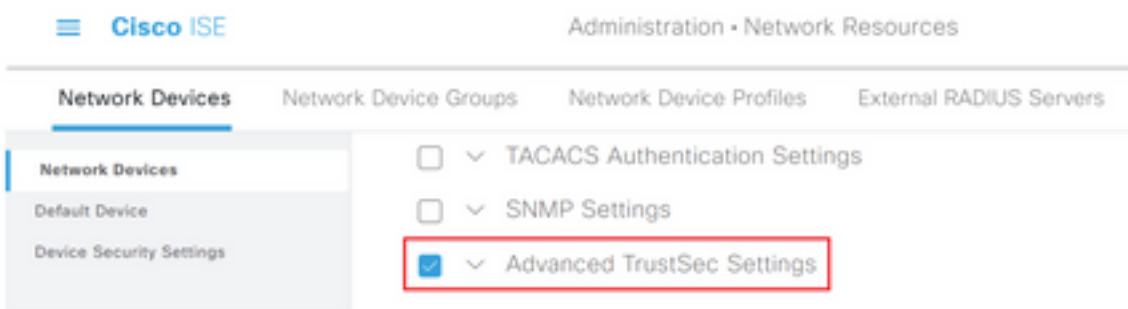
Étape 1. Accédez à l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez **Administration > Network Resources > Network Devices**.

Étape 2. Cliquez sur **+Ajouter**.

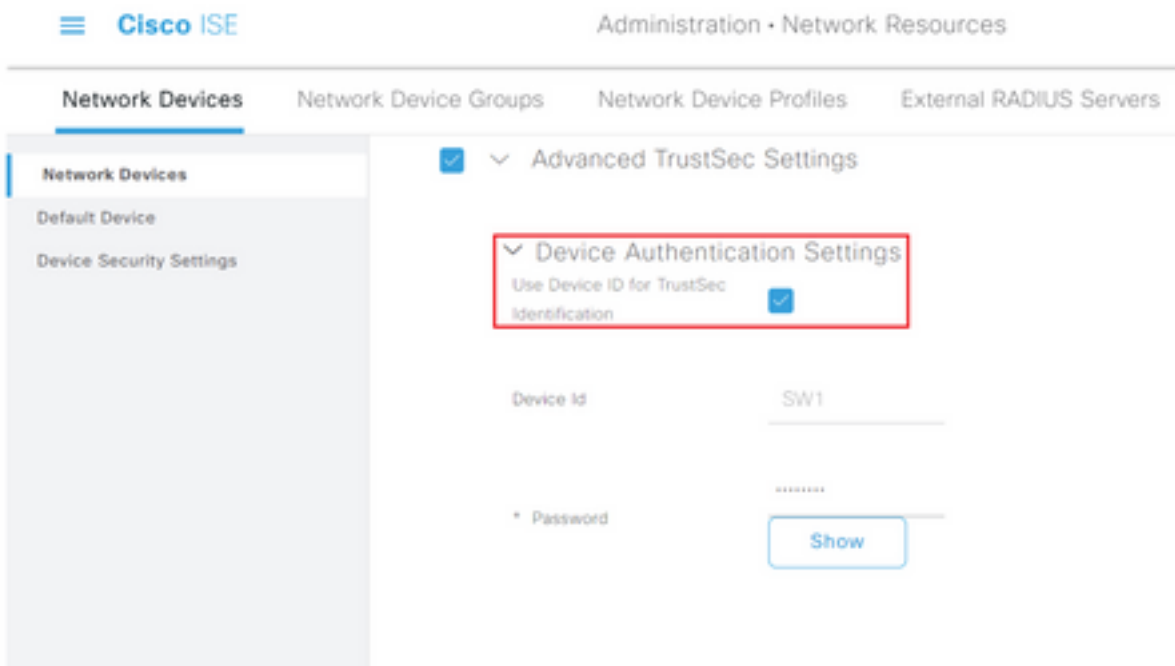


Étape 3. Entrez les informations requises dans la section **Périphériques réseau** et dans **Paramètres d'authentification RADIUS**.

Étape 4. Cochez la case **Advanced TrustSec Settings** pour configurer un périphérique compatible TrustSec.

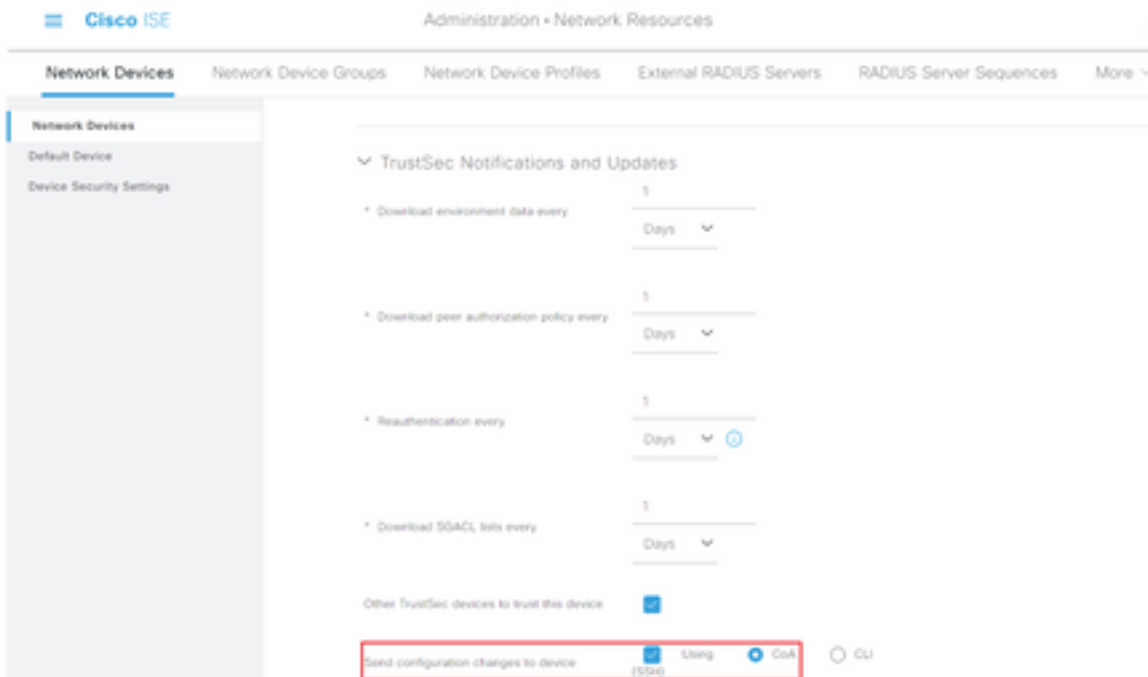


Étape 5. Cochez la case **Utiliser l'ID de périphérique pour l'identification TrustSec** pour renseigner automatiquement le nom de périphérique répertorié dans la section **Périphériques réseau**. Entrez un mot de passe dans le champ **Mot de passe**.



Note: L'ID et le mot de passe doivent correspondre à la commande “ cts identifiants id <ID> password <PW> ” qui est configurée ultérieurement sur le commutateur.

Étape 6. Cochez la case **Envoyer les modifications de configuration au périphérique** afin que ISE puisse envoyer des notifications TrustSec CoA au périphérique.



Étape 7. Cochez la case **Inclure ce périphérique lors du déploiement des mises à jour de mappage de balises de groupe de sécurité**.

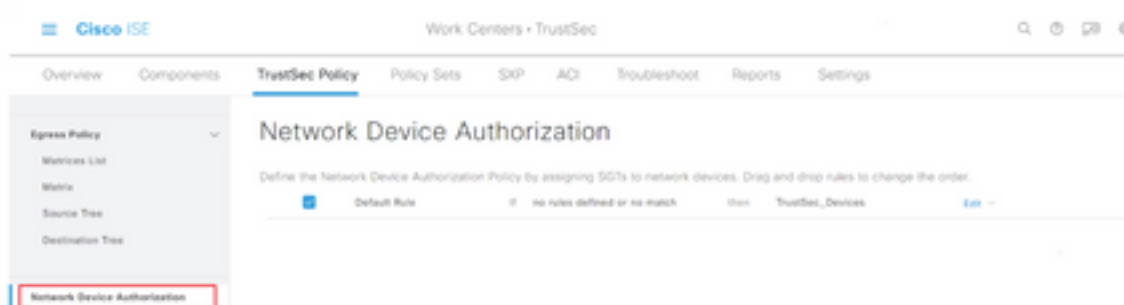
Étape 8. Afin de permettre à ISE de modifier la configuration du périphérique réseau, entrez les informations d'identification de l'utilisateur dans les champs **Nom d'utilisateur du mode EXEC** et **Mot de passe du mode EXEC**. Le cas échéant, indiquez le mot de passe enable dans le champ **Mot de passe du mode enable**.

Note: Répétez les étapes pour tous les autres NAD qui sont destinés à faire partie du domaine TrustSec.

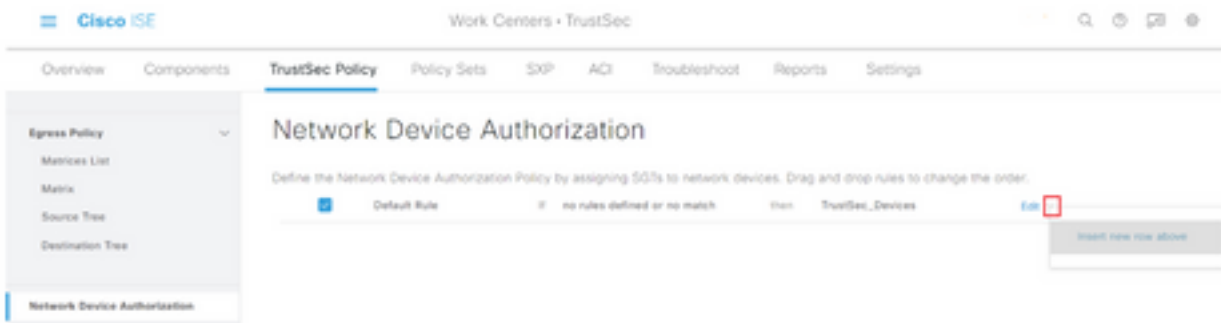
Autorisation des périphériques réseau

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez dans **Centres de travail > TrustSec > Stratégie TrustSec**.

Étape 2. Dans le volet gauche, cliquez sur **Network Device Authorization**.

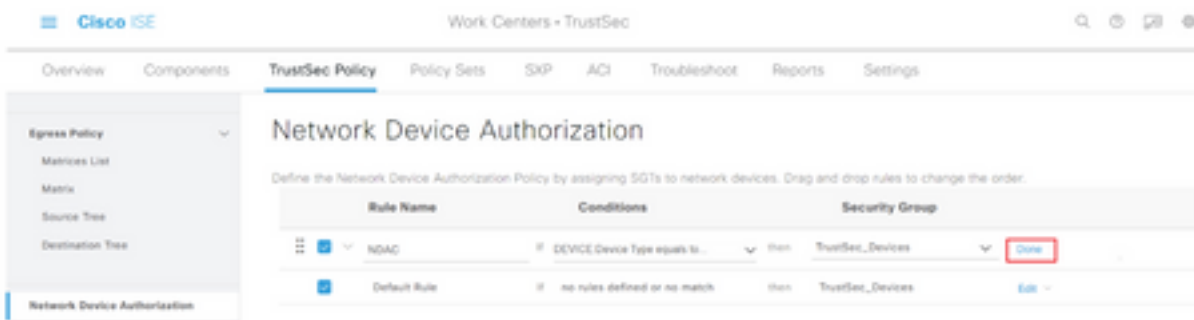


Étape 3. À droite, utilisez la liste déroulante en regard de **Modifier** et **Insérer une nouvelle ligne ci-dessus** pour créer une nouvelle règle NDA.



Étape 4. Définissez un **nom de règle**, des **conditions** et sélectionnez la SGT appropriée dans la liste déroulante sous **Groupes de sécurité**.

Étape 5. Cliquez sur **Terminé** à l'extrême droite.



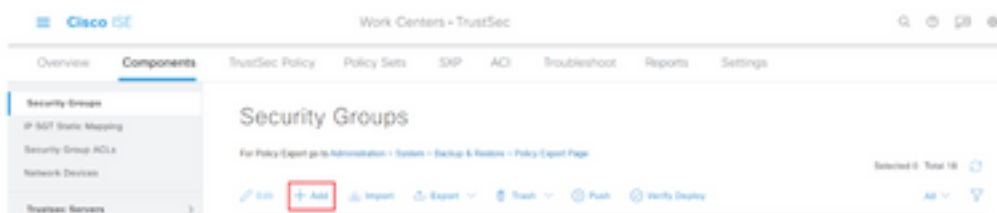
Étape 6. Faites défiler la liste vers le bas et cliquez sur **Enregistrer**.

SGT

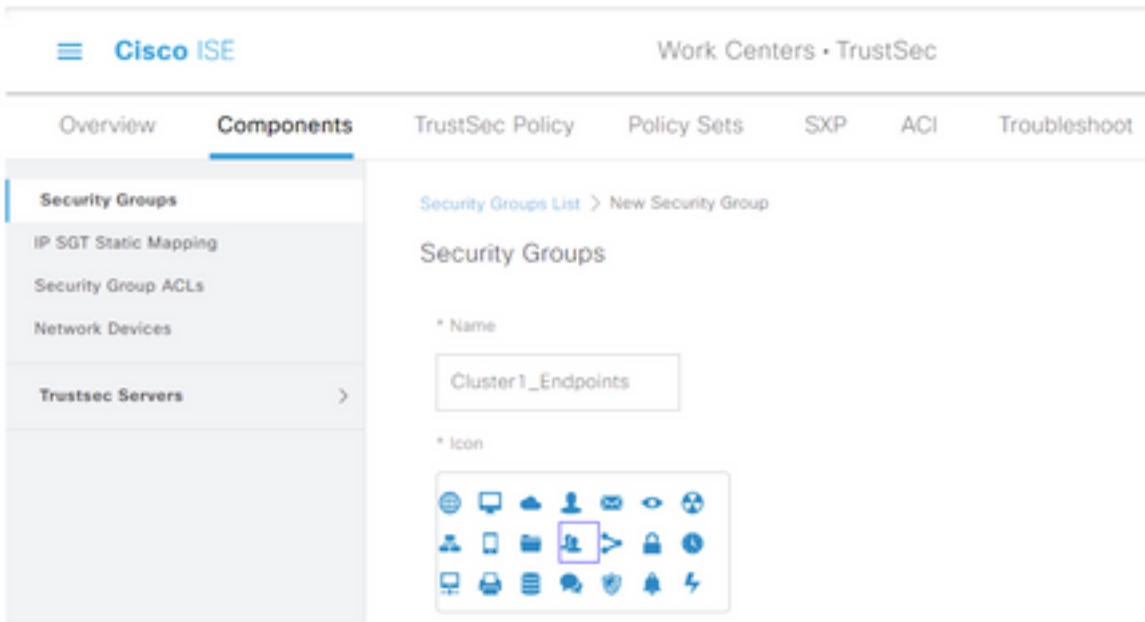
Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez dans **Centres de travail > TrustSec > Composants**.

Étape 2. Dans le volet gauche, développez **Groupes de sécurité**.

Étape 3. Cliquez sur **+Ajouter** pour créer une nouvelle SGT.



Étape 4. Entrez le nom et choisissez une icône dans les champs appropriés.



Étape 5. Vous pouvez éventuellement lui donner une description et saisir une **valeur de balise**.

Note: Afin de pouvoir saisir manuellement une valeur de balise, accédez à Centres de travail > TrustSec > Paramètres > Paramètres généraux TrustSec et sélectionnez l'option **L'utilisateur doit saisir manuellement le numéro de balise de groupe de sécurité** sous **Numérotation de balise de groupe de sécurité**.

Étape 6. Faites défiler la liste vers le bas et cliquez sur **Soumettre**.

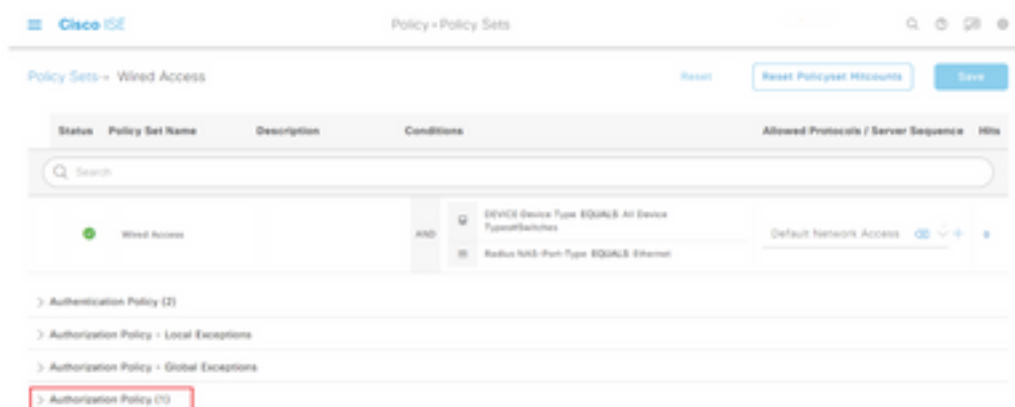
Note: Répétez ces étapes pour toutes les balises de groupe de sécurité requises.


Stratégie d'autorisation

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez **Stratégie > Jeux de stratégies**.

Étape 2. Sélectionnez le jeu de stratégies approprié.

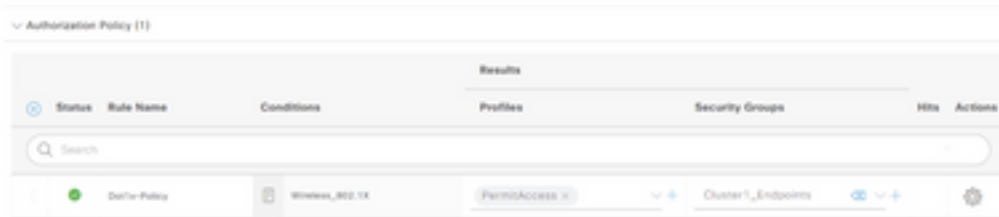
Étape 3. Dans le jeu de stratégies, développez la **stratégie d'autorisation**.



Étape 4. Cliquez sur le bouton  pour créer une **stratégie d'autorisation**.



Étape 5. Définissez le **nom** de la **règle** requise, les **conditions** et les **profils** et sélectionnez la SGT appropriée dans la liste déroulante sous **Groupes de sécurité**.



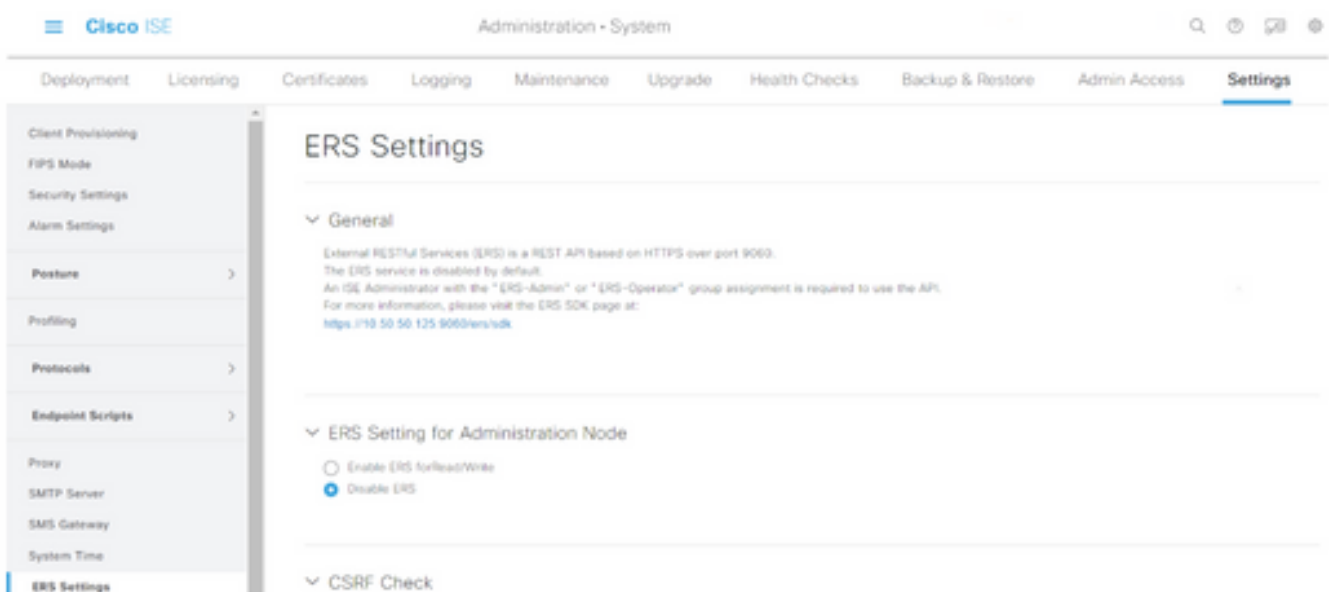
Étape 6. Cliquez **Save**.

Activation de l'ERS sur le noeud d'agrégation ISE (facultatif)

Le service ERS (External RESTful API Service) est une API qui peut être interrogée par le WSA pour obtenir des informations sur le groupe. Le service ERS est désactivé par défaut sur ISE. Une fois qu'il est activé, les clients peuvent interroger l'API s'ils s'authentifient en tant que membres du groupe **ERS Admin** sur le noeud ISE. Pour activer le service sur ISE et ajouter un compte au groupe approprié, procédez comme suit :

Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez **Administration > System > Settings**.

Étape 2. Dans le volet gauche, cliquez sur **Paramètres ERS**.



Étape 3. Sélectionnez l'option **Activer ERS** pour lecture/écriture.

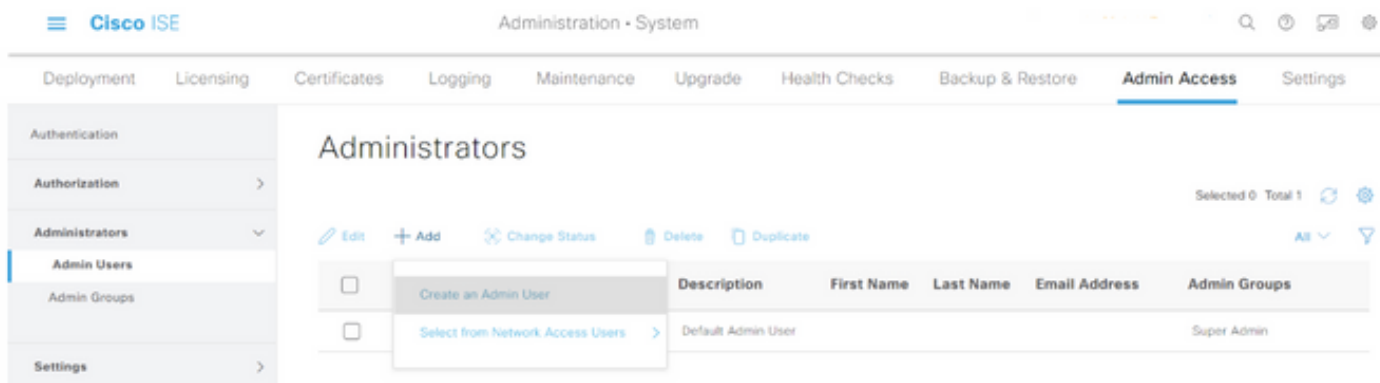
Étape 4. Cliquez sur **Enregistrer** et confirmer avec **OK**.

Ajouter un utilisateur au groupe d'administration ESR (facultatif)

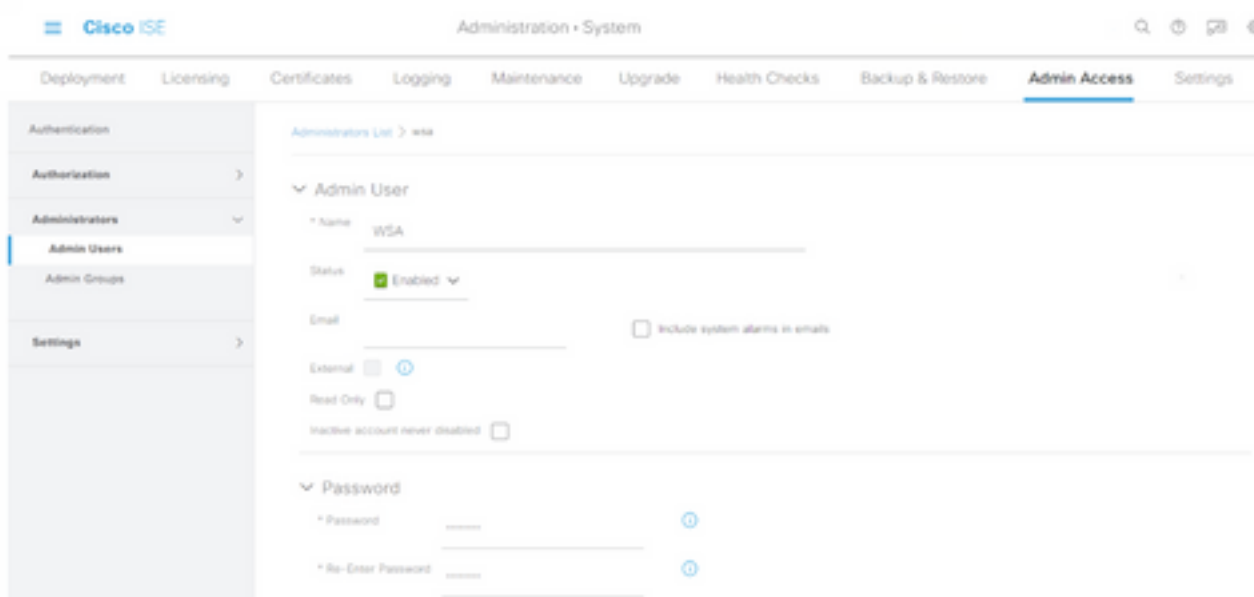
Étape 1. Sélectionnez l'icône des trois lignes située dans le coin supérieur gauche et sélectionnez **Administration > System > Admin Access**.

Étape 2. Dans le volet gauche, développez **Administrateurs** et cliquez sur **Utilisateurs Admin**.

Étape 3. Cliquez sur **+Ajouter** et sélectionnez **Utilisateur Admin** dans la liste déroulante.



Étape 4. Entrez un nom d'utilisateur et un mot de passe dans les champs appropriés.



Étape 5. Dans le champ **Groupes d'administrateurs**, utilisez la liste déroulante pour sélectionner **Administrateur ERS**.

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. The main navigation menu has tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Admin Access' tab is selected. On the left, a sidebar menu shows 'Authentication', 'Authorization', 'Administrators', 'Admin Users', 'Admin Groups', and 'Settings'. The main content area is titled 'Admin Access' and contains the following fields and sections:

- 'First Name' and 'Last Name' text input fields.
- 'Account Options' section with a 'Description' text area.
- 'Admin Groups' section with a dropdown menu currently set to 'ERS Admin', which is highlighted with a red box.
- 'Save' and 'Reset' buttons at the bottom right.

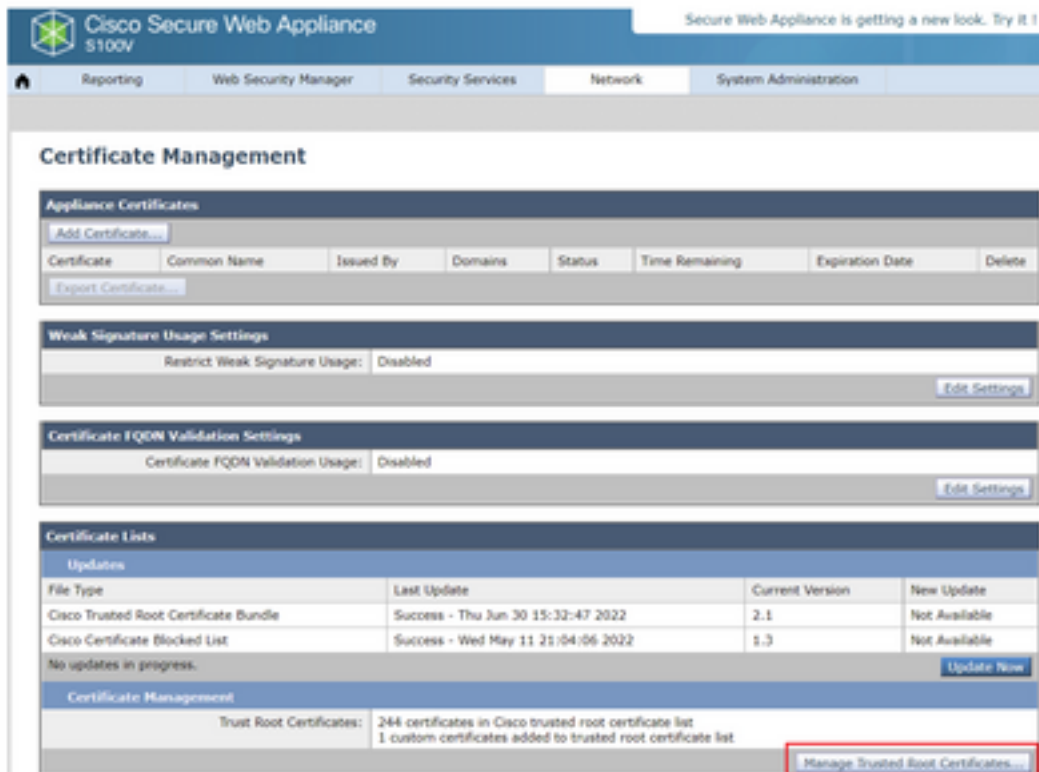
Étape 6. Cliquez sur **Save**.

Configuration sécurisée des appareils Web

Certificat racine

Si la conception d'intégration utilise une autorité de certification interne comme racine de confiance pour la connexion entre le WSA et ISE, ce certificat racine doit être installé sur les deux appliances.

Étape 1. Accédez à **Network > Certificate Management** et cliquez sur **Manage Trusted Root Certificates** pour ajouter un certificat CA.



Étape 2. Cliquez sur **Importer**.



Étape 3. Cliquez sur **Choose File** pour localiser l'autorité de certification racine générée et cliquez sur **Submit**.

Étape 4. Cliquez de nouveau sur **Soumettre**.

Étape 5. Dans le coin supérieur droit, cliquez sur **Valider les modifications**.



Étape 6. Cliquez à nouveau sur **Valider les modifications**.

certificat pxGrid

Dans le WSA, la création de la paire de clés et du certificat à utiliser par pxGrid est terminée dans le cadre de la configuration des services ISE.

Étape 1. Accédez à **Network > Identity Service Engine**.

Étape 2. Cliquez sur **Activer et modifier les paramètres**.

Étape 3. Cliquez sur **Choose File** pour localiser l'autorité de certification racine générée et cliquez sur **Upload File**.

Identity Services Engine

Edit Identity Services Engine Settings

Enable ISE Service

Primary ISE pxGrid Node: The Web Appliance will communicate with the ISE pxGrid node to support Web Appliance data subscription (ongoing updates). A primary ISE pxGrid node (server) must be configured.

hostname or IP address

ISE pxGrid Node Certificate: If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management) and upload the CA-signed root certificate below. If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below. You can upload the certificate chain that includes any intermediate certificates.

Certificate:

Note: Une erreur de configuration courante consiste à télécharger le certificat ISE pxGrid dans cette section. Le certificat d'autorité de certification racine doit être téléchargé dans le champ ISE pxGrid Node Certificate.

Étape 4. Dans la section **Certificat client de l'appliance Web**, sélectionnez **Utiliser le certificat et la clé générés**.

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

Étape 5. Cliquez sur le bouton **Générer un nouveau certificat et une nouvelle clé** et renseignez les champs de certificat requis.

Generate Certificate and Key

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration: months

Basic Constraints: Set X509v3 Basic Constraints Extension to Critical

Étape 6. Cliquez sur **Télécharger la demande de signature de certificat**.

Note: Il est recommandé de sélectionner le bouton **Soumettre** pour valider les modifications apportées à la configuration ISE. Si le délai d'attente de la session est dépassé avant l'envoi des modifications, les clés et le certificat générés peuvent être perdus, même si le CSR a

été téléchargé.

Étape 7. Après avoir signé le CSR avec votre CA, cliquez sur **Choose File** pour localiser le certificat.

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

Étape 8. Cliquez sur **Télécharger le fichier**.

Étape 9. Envoyer et valider.

Activer SXP et ERS sur l'appliance Web sécurisée

Étape 1. Cliquez sur les boutons **Activer** pour SXP et ERS.

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

Enable ISE External Realm 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 Type (SGT), you should enable ERS.

Étape 2. Dans le champ **Informations d'identification de l'administrateur ERS**, saisissez les informations utilisateur configurées sur ISE.

Étape 3. Cochez la case **Nom de serveur identique au noeud ISE pxGrid** pour hériter des informations configurées précédemment. Sinon, saisissez les informations requises.

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)

Étape 4. Envoyer et valider.

Profil d'identification

Afin d'utiliser des balises de groupe de sécurité ou des informations de groupe ISE dans les stratégies WSA, il faut d'abord créer un profil d'identification qui utilise ISE comme moyen d'identifier les utilisateurs de manière transparente.

Étape 1. Accédez à **Web Security Manager > Authentication > Identification Profiles**.

Étape 2. Cliquez sur **Ajouter un profil d'identification**.

Étape 3. Saisissez un nom et éventuellement une description.

Étape 4. Dans la **section Identification et authentification**, utilisez la liste déroulante pour sélectionner **Identifier de manière transparente les utilisateurs avec ISE**.

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

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

Étape 5. Envoyer et valider.

Stratégie de déchiffrement basée sur SGT

Étape 1. Accédez à **Gestionnaire de sécurité Web > Stratégies Web > Stratégies de**

déchiffrement.

Étape 2. Cliquez sur **Ajouter une stratégie**.

Étape 3. Saisissez un nom et éventuellement une description.

Étape 4. Dans la section **Profils et utilisateurs d'identification**, utilisez la liste déroulante pour sélectionner **Sélectionner un ou plusieurs profils d'identification**.

Étape 5. Dans la section **Profils d'identification**, utilisez la liste déroulante pour choisir le nom du profil d'identification ISE.

Étape 6. Dans la section **Utilisateurs et groupes autorisés**, sélectionnez **Groupes et utilisateurs sélectionnés**.

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: Select One or More Identification Profiles

Identification Profile: ISE Profile

Authorized Users and Groups

All Authenticated Users

Selected Groups and Users (2)

ISE Secure Group Tags: No tags entered

ISE Groups: No groups entered

Users: No users entered

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.

Étape 7. Cliquez sur le lien hypertexte en regard de **Balises de groupe sécurisé ISE**.

Étape 8. Dans la section **Recherche de balises de groupe sécurisé**, cochez la case à droite de la SGT souhaitée et cliquez sur **Ajouter**.

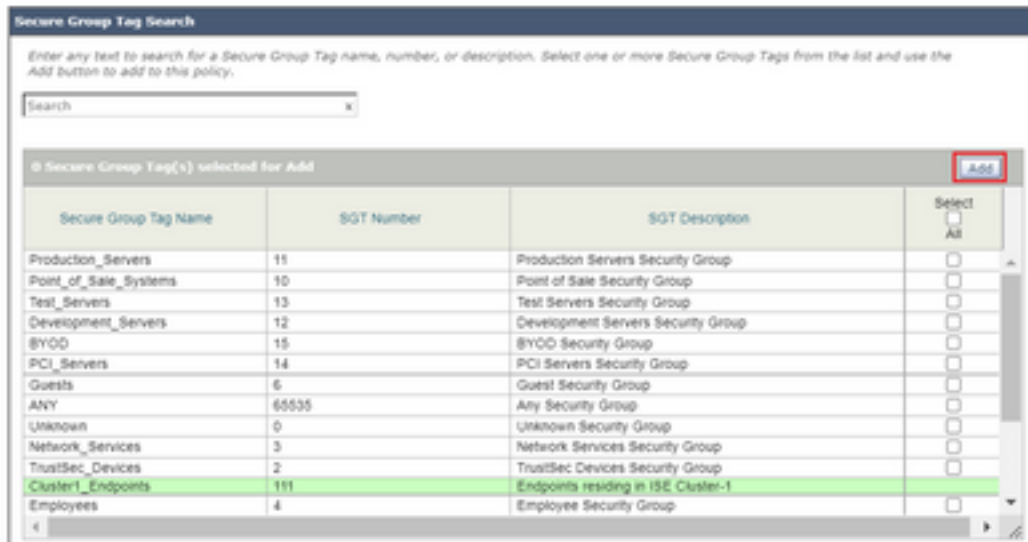
Authorized Secure Group Tags

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

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



Étape 9. Cliquez sur Terminé pour revenir.

Étape 10. Envoyer et valider.

Configuration du commutateur

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

```

Vérification

Affectation de balises de groupe de sécurité entre ISE et terminal.

Vous pouvez voir ici un point de terminaison du cluster ISE 1 affecté à une SGT après une authentification et une autorisation réussies :

Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Domain
user@domain	14.00.00...	Microsoft-Work	Work Access -- S...	Work Access -- S...	Permissive	10.50.50.13	Cluster1_Endpoints	sgt01-01.1

Vous pouvez voir ici un point de terminaison du cluster ISE 2 affecté à une SGT après une authentification et une autorisation réussies :

Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profile	IP Address	Security Group	Domain
user@domain	14.00.00...	Microsoft-Work	Work Access -- S...	Work Access -- S...	Permissive	10.50.50.12	Cluster2_Endpoints	sgt02-02.1

Mappages SXP

Puisque la communication SXP est activée entre les noeuds ISE du cluster et le noeud d'agrégation ISE, ces mappages SGT-IP sont appris par l'agrégation ISE via SXP :

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PDNs Inherited
10.50.50.9/32	TrustSec_Devices (20000)		10.50.50.121.10.50.50.0	SXP	default	no-ipp
10.50.50.7/32	TrustSec_Devices (20000)		10.50.50.122.10.50.50.7	SXP	default	no-ipp
10.50.50.12/32	Cluster1_Endpoints (1110000)		10.50.50.121.10.50.50.0	SXP	default	no-ipp
10.50.50.13/32	Cluster1_Endpoints (2000000)		10.50.50.122.10.50.50.7	SXP	default	no-ipp

Ces mappages SXP, provenant de différents clusters ISE, sont ensuite envoyés à WSA via pxGrid via le noeud d'agrégation 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 ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[ ]> show
IP                username                               SGT#  Port Range
-----
10.50.50.13       tsesxp_10.50.50.122_sgt222_10.50.50.13 222   -
10.50.50.12       tsesxp_10.50.50.121_sgt111_10.50.50.12 111   -
```

Application des politiques basée sur SGT

Vous pouvez voir ici que les différents points d'extrémité correspondent à ses stratégies respectives et que le trafic est bloqué en fonction de leur SGT :

Point de terminaison appartenant au cluster ISE 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	https://bbc.com/#43/television 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

Point de terminaison appartenant au cluster ISE 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/television 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

Informations connexes

- [Guide d'intégration de l'appliance de sécurité Web et de Identity Service Engine](#)

- [Configurez l'intégration du WSA au moyen des services ISE TrustSec](#)
- [Guide de l'administrateur de Cisco Identity Services Engine, version 3.1](#)
- [Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance](#)