

# 複数のISEクラスタとTrustSecベースのポリシー用のセキュアなWebアプライアンスの統合

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[制限](#)

[ネットワーク図](#)

[設定](#)

[ISE の設定](#)

[SXPの有効化](#)

[クラスタノードでのSXPの設定](#)

[集約ノードでのSXPの設定](#)

[集約ノードでpxGridを有効にします](#)

[pxGrid自動承認](#)

[ネットワークデバイスのTrustSec設定](#)

[ネットワークデバイス認可](#)

[SGT](#)

[認可ポリシー](#)

[ISEアグリゲーションノードでのERSの有効化 \( オプション \)](#)

[ESR管理グループへのユーザの追加 \( オプション \)](#)

[セキュアWebアプライアンスの設定](#)

[pxGrid証明書](#)

[セキュアWebアプライアンスでのSXPおよびERSの有効化](#)

[識別プロファイル](#)

[SGTベースの復号化ポリシー](#)

[スイッチの設定](#)

[\[AAA\]](#)

[TrustSec](#)

[確認](#)

[関連情報](#)

## 概要

このドキュメントでは、TrustSec環境でSGTベースのWebアクセスポリシーを利用するために、複数のISE環境からpxGridを介して単一のCisco Secure Web Appliance ( 旧称Web Security Appliance WSA ) にセキュリティグループタグ(SGT)情報を送信する手順について説明します。

バージョン14.5より前のSecure Web Applianceは、SGTに基づくアイデンティティポリシー用に単一のISEクラスタとのみ統合できます。この新しいバージョンの導入により、Secure Web Applianceは、複数のISEクラスタ間で集約された個別のISEノードを使用して、複数のISEクラス

タの情報と相互運用できるようになりました。これにより、さまざまなISEクラスタからユーザデータをエクスポートでき、1:1統合を必要とせずにユーザが使用できる出力点を制御できます。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine ( ISE )
- セキュアWebアプライアンス
- RADIUS プロトコル
- TrustSec
- pxGrid

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

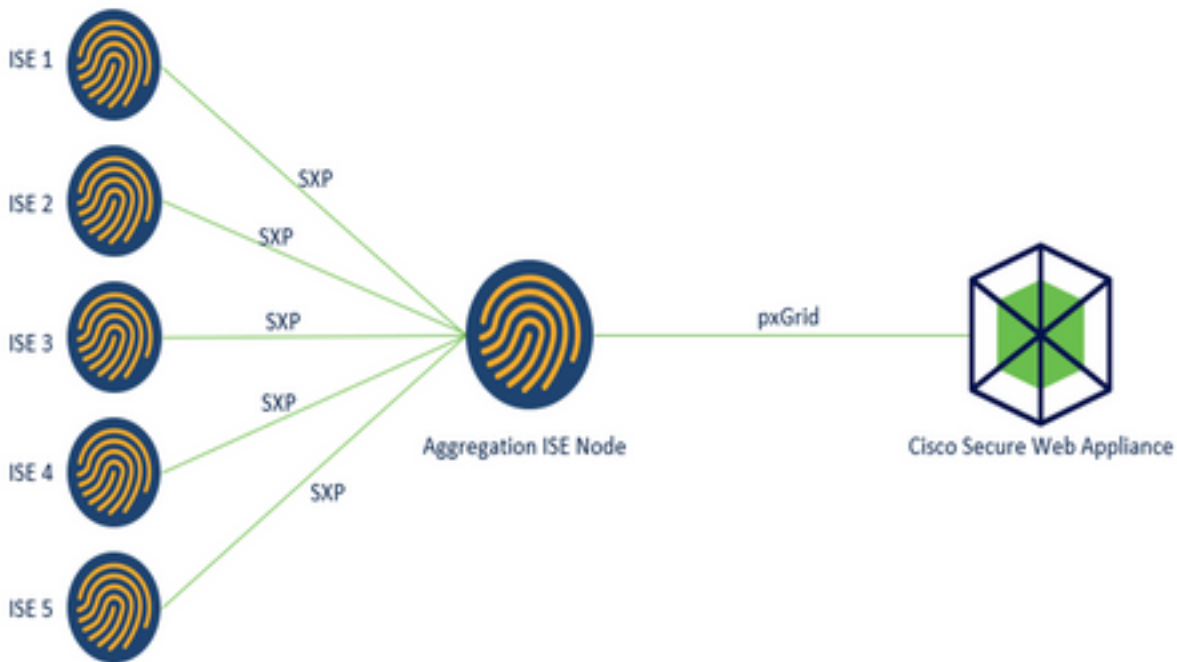
- Secure Web Appliance 14.5
- ISEバージョン3.1 P3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

### 制限

1. すべてのISEクラスタは、SGTの均一なマッピングを維持する必要があります。
2. ISEアグリゲーションノードには、残りのISEクラスタのSGT名/番号が必要です。
3. セキュアなWebアプライアンスでは、SGTタグに基づいてポリシー（アクセス/復号化/ルーティング）を識別することしかできず、グループやユーザ名は識別できません
4. レポートとトラッキングはSGTベースです。
5. 既存のISE/セキュアWebアプライアンスのサイジングパラメータは、引き続きこの機能に適用されます。

## ネットワーク図



プロセス :

- 1.エンドユーザがネットワークに接続すると、ISEの許可ポリシーに基づいてSGTを受信します。
- 2.異なるISEクラスタは、このSGT情報をSGT-IPマッピングの形式でSXPを介してISEアグリゲーションノードに送信します。
3. ISEアグリゲーションノードはこの情報を受信し、pxGridを介して単一のセキュアWebアプライアンスと共有します。
- 4.セキュアWebアプライアンスは、Webアクセスポリシーに基づいてユーザにアクセスを提供するために学習したSGT情報を使用します。

## 設定

### ISE の設定

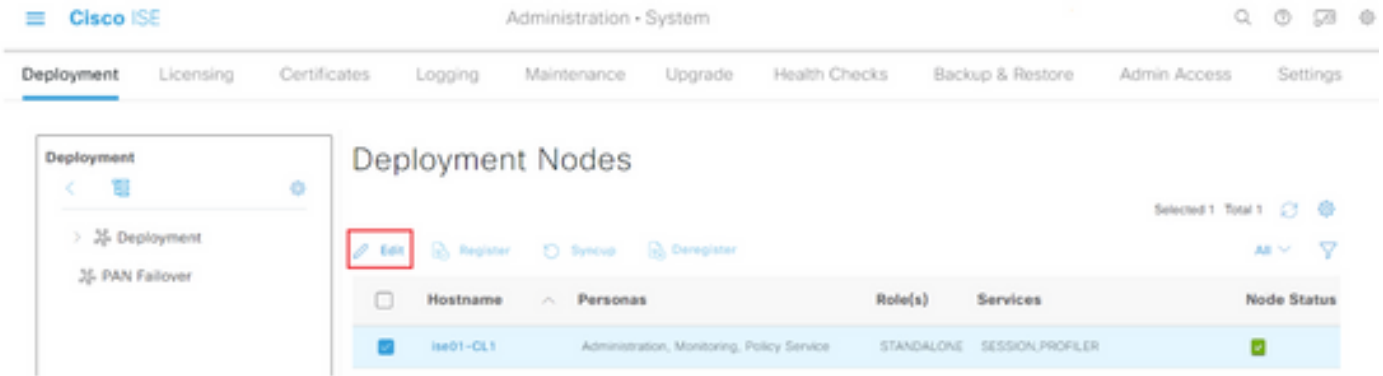
#### SXPの有効化

ステップ1:[Three Lines]アイコンを選択します  
[Deployment] を選択します。

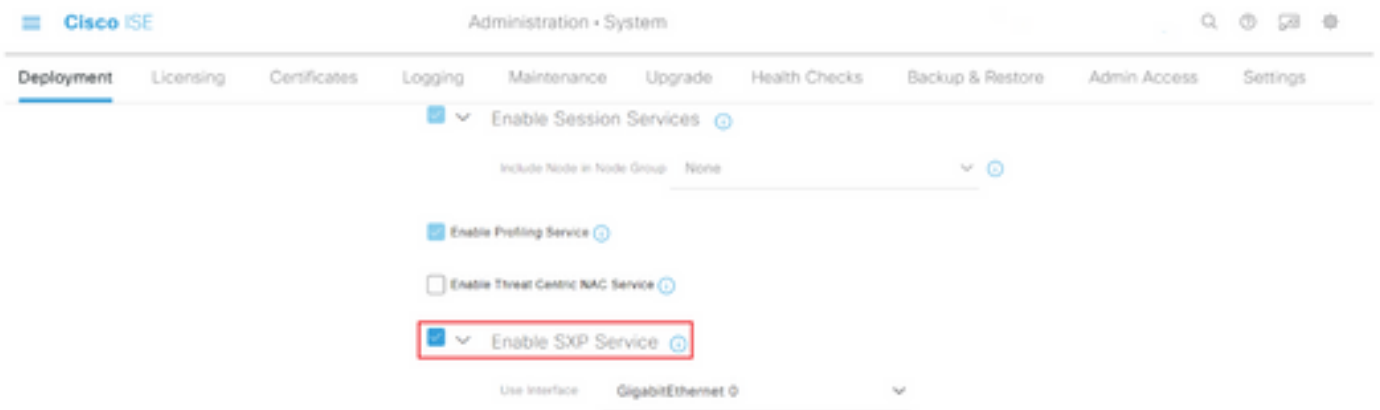


左上隅にある[Administration] > [System] >

ステップ2 : 設定するノードを選択し、[Edit]をクリックします。



ステップ3:SXPを有効にするには、[Enable SXP Service] チェックボックスをオンにします



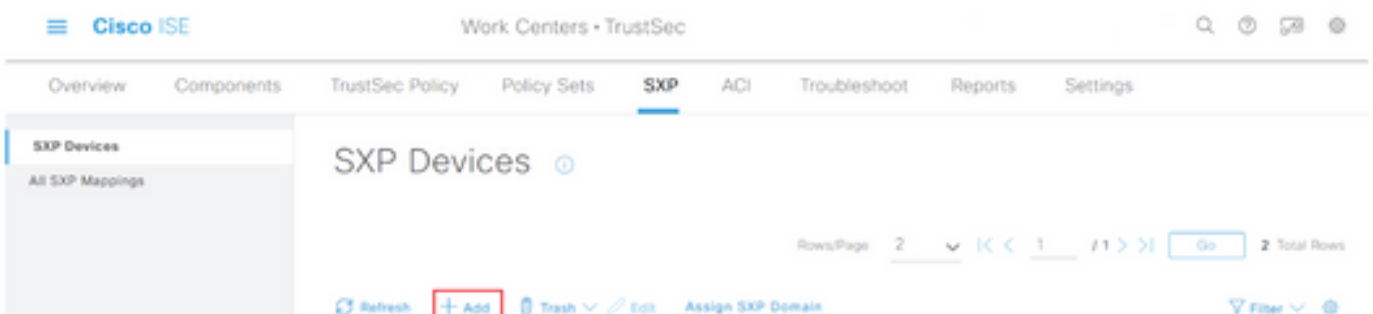
ステップ4：下部までスクロールし、[Save]をクリックします

注：アグリゲーションノードを含む各クラスターの残りのISEノードに対して、すべての手順を繰り返します。


## クラスターノードでのSXPの設定

ステップ1:3行のアイコンを選択します  を選択します。[Work Center] > [TrustSec] > [SXP]。

ステップ2:ISEアグリゲーションノードをSXPピアとして設定するには、[Add] をクリックします。



ステップ3: ISE集約ノードの名前とIPアドレスを定義し、ピアロールをLISTENERとして選択します。 [Connected PSNs] で必要なPSNを選択し、 [Required SXP Domains] で [Enabled] を選択してから、 [Password Type] と必要な [Version] を選択します。

 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

ステップ 4 : [Save] をクリックします。

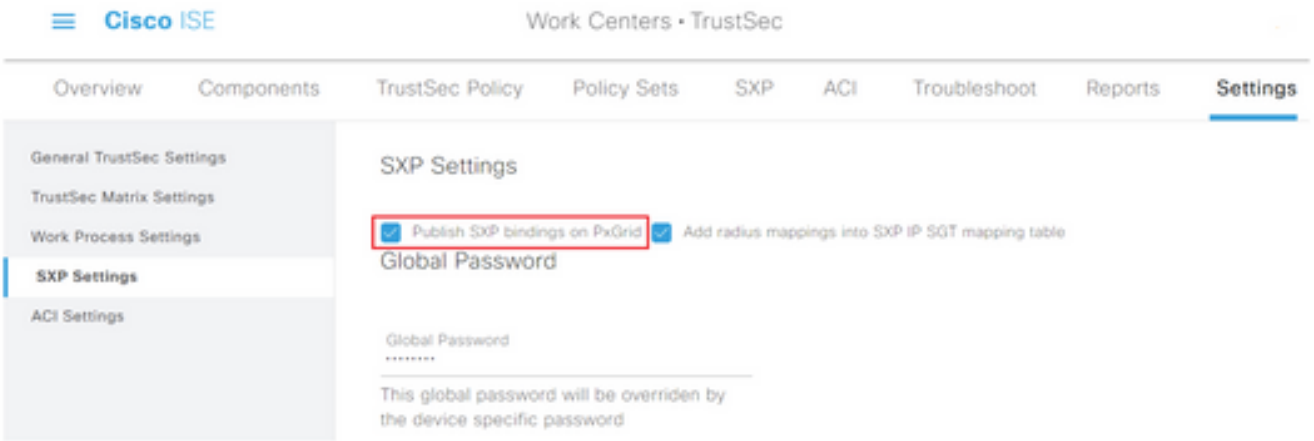
注 : 各クラスタ内の残りのISEノードに対してすべての手順を繰り返し、集約ノードへのSXP接続を構築します。集約ノードで同じプロセスを繰り返し、ピアロールとして[SPEAKER]を選択します。

## 集約ノードでのSXPの設定

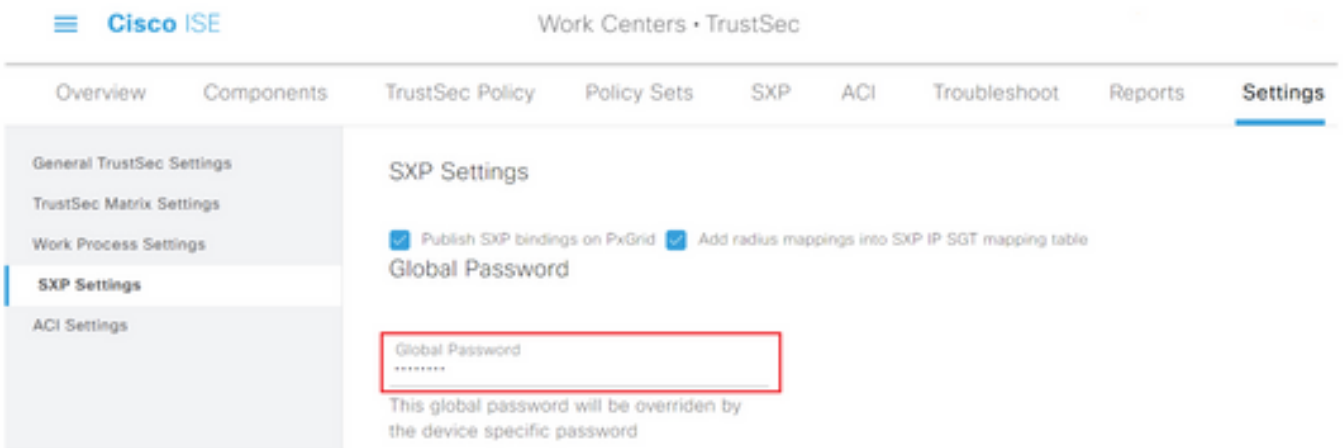
ステップ1:左上隅にある3行のアイコンを選択し、[Work Center] > [TrustSec] > [Settings] を選択します

ステップ 2 : [SXP Settings] タブをクリックします

ステップ3:IP-SGTマッピングを伝搬するには、[Publish SXP bindings on pxGrid] チェックボックスをオンにします。



ステップ 4 (任意) : [Global Password] でSXP設定のデフォルトパスワードを定義します

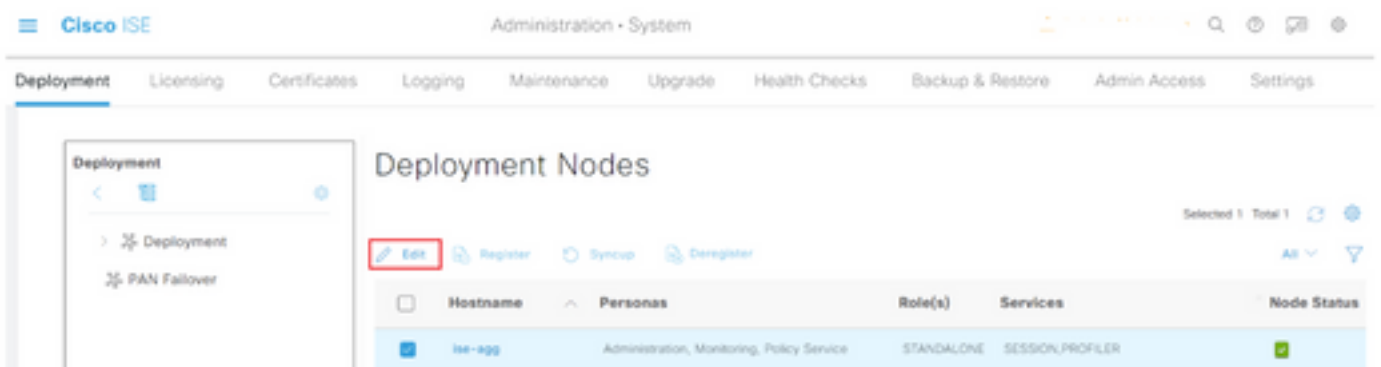


ステップ5 : 下にスクロールして、[Save]をクリックします。

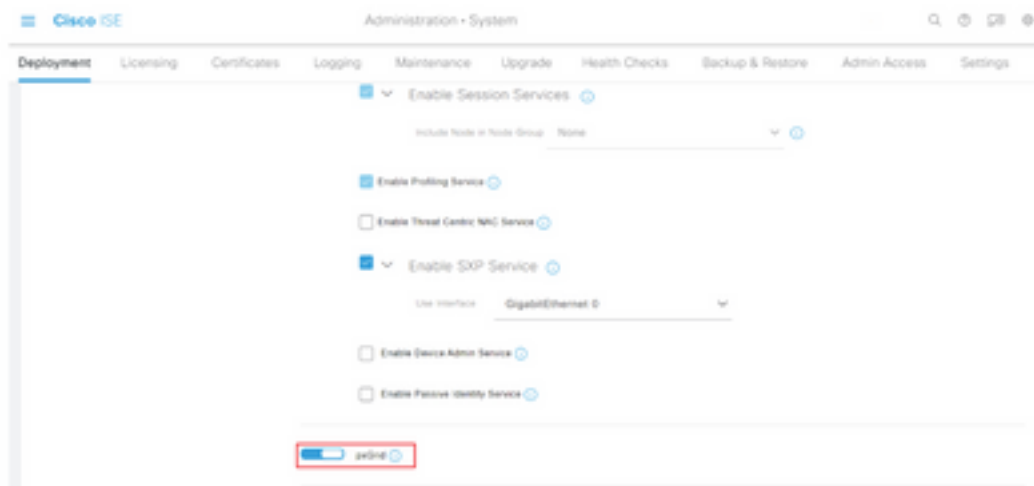
## 集約ノードでpxGridを有効にします

ステップ1:左上隅にある3行のアイコンを選択し、[Administration] > [System] > [Deployment]を選択します。

ステップ2 : 設定するノードを選択し、[Edit]をクリックします。



ステップ3:pxGridを有効にするには、pxGridの横にあるボタンをクリックします。

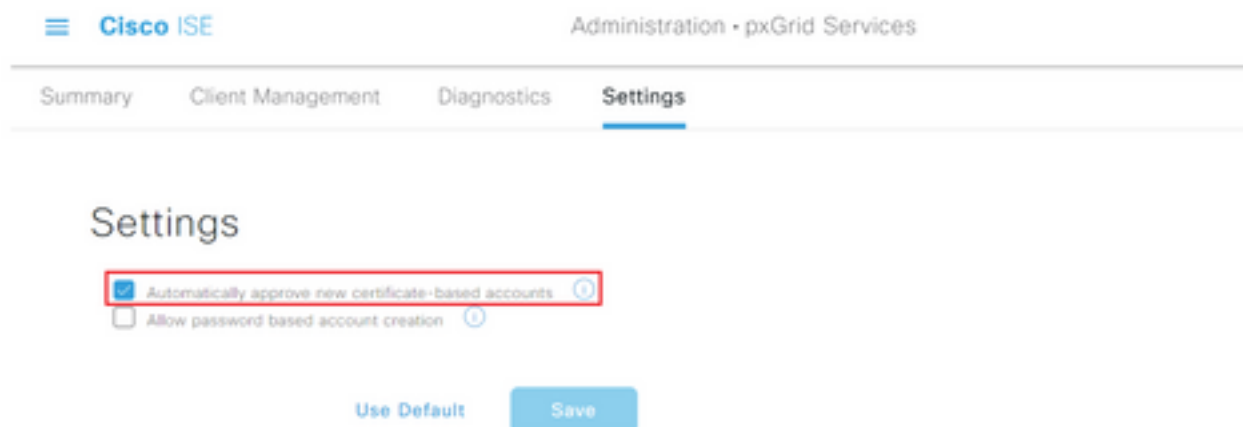


ステップ4：下部までスクロールし、[Save]をクリックします。

## pxGrid自動承認

ステップ1:左上隅にある3行のアイコンに移動し、[Administration] > [pxGrid Services] > [Settings]を選択します。

ステップ2：デフォルトでは、ISEは新しいpxGridクライアントからの接続要求に対してpxGridを自動的に承認しません。したがって、[Automatically approve new certificate-based accounts]チェックボックスをオンにして、この設定を有効にする必要があります。



ステップ3：[Save] をクリックします。

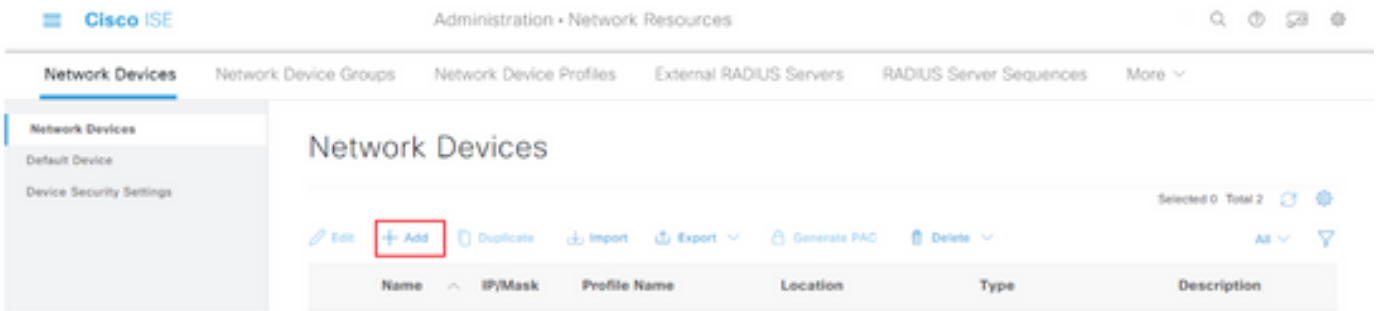
## ネットワークデバイスのTrustSec設定

Cisco ISEがTrustSec対応デバイスからの要求を処理するには、Cisco ISEでこれらのTrustSec対応デバイスを定義する必要があります。

ステップ1:左上隅にある3行のアイコンに移動し、[Administration] > [Network Resources] > [Network Devices]を選択します。

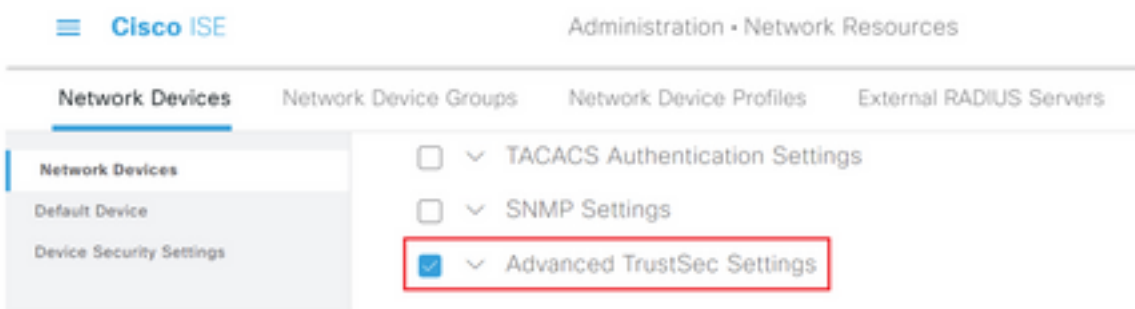
ステップ2：+Addをクリックします。



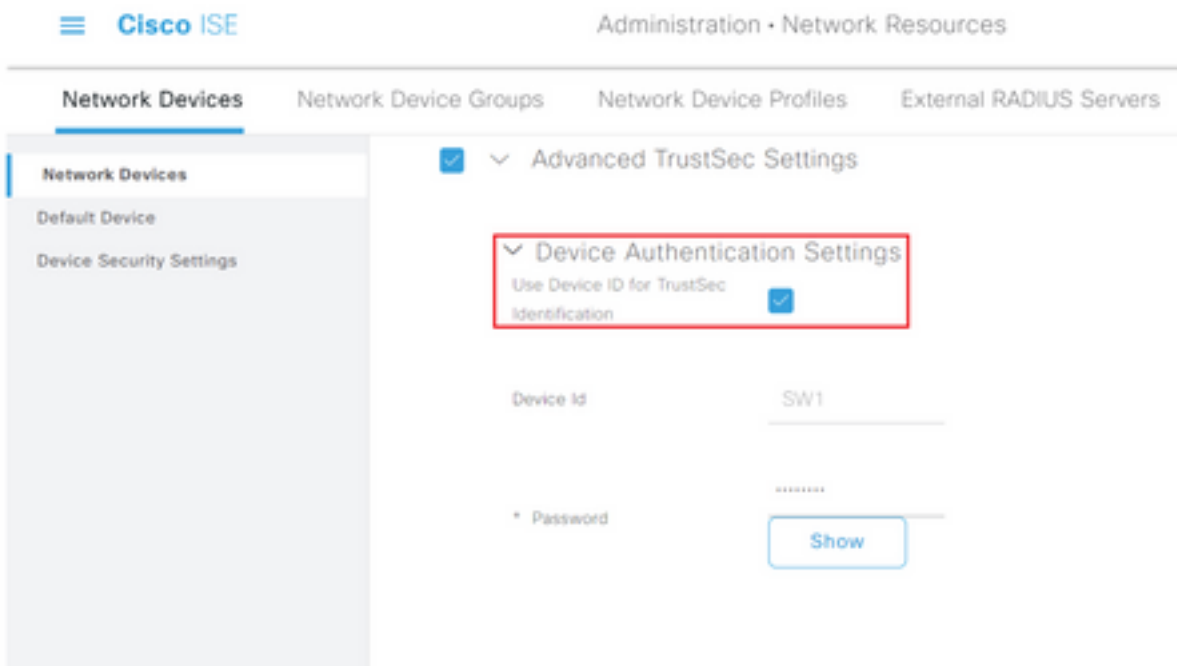


ステップ3:[Network Devices] セクションと[RADIUS Authentication Settings] に必要な情報を入力します。

ステップ4:TrustSec対応デバイスを設定するには、[Advanced TrustSec Settings] チェックボックスをオンにします。

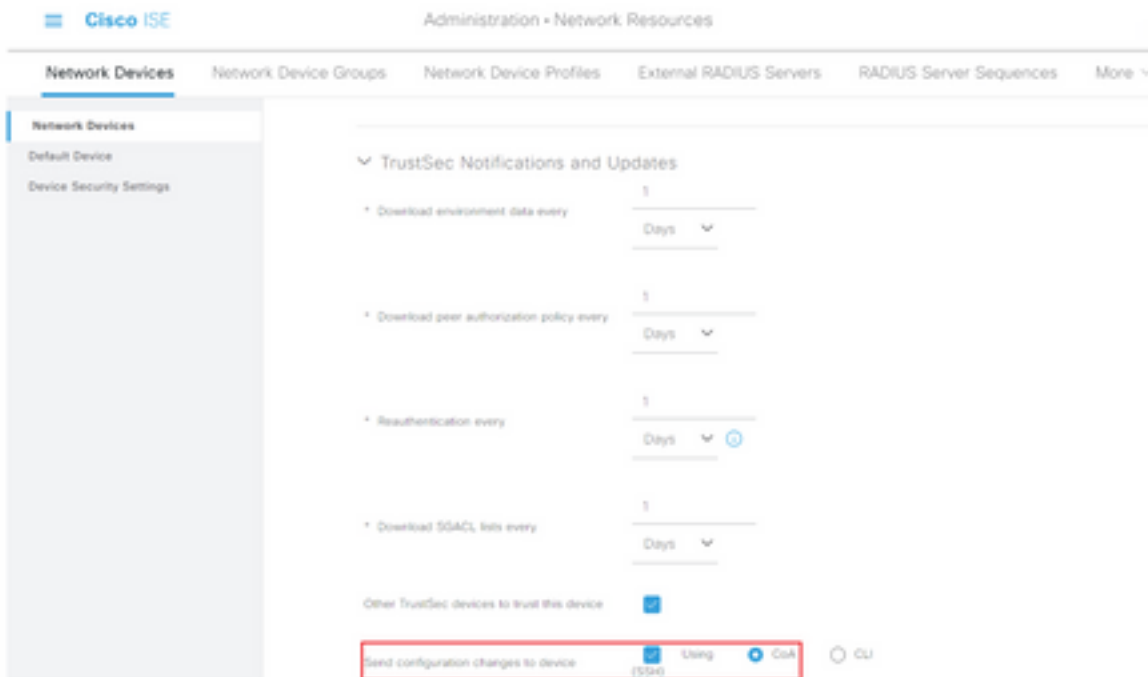


ステップ5:[Use Device ID for TrustSec Identification] チェックボックスをオンにして、[Network Devices] セクションに表示されるデバイス名を自動的に入力します。[Password] フィールドにパスワードを入力します。



注：IDとパスワードは、スイッチで後から設定する「cts credentials id <ID> password <PW>」コマンドと一致する必要があります。

ステップ6: ISEがTrustSec CoA通知をデバイスに送信できるように、[Send configuration changes to device] チェックボックスをオンにします。



ステップ7: [Include this device when deploying Security Group Tag Mapping Updates] チェックボックスをオンにします。

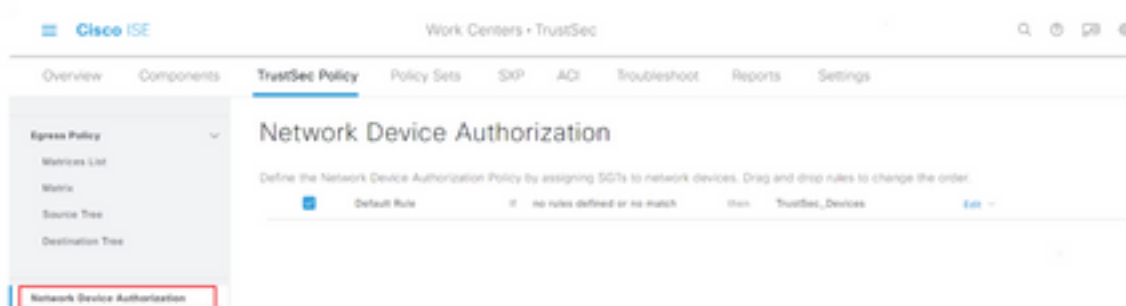
ステップ8: ISEでネットワークデバイスの設定を編集できるようにするには、[EXEC Mode Username] フィールドと[EXEC Mode Password] フィールドにユーザクレデンシャルを入力します。オプションで、[Enable Mode Password] フィールドにイネーブルパスワードを入力します。

注：TrustSecドメインの一部として使用する他のすべてのNADについて、この手順を繰り返します。

## ネットワークデバイス認可

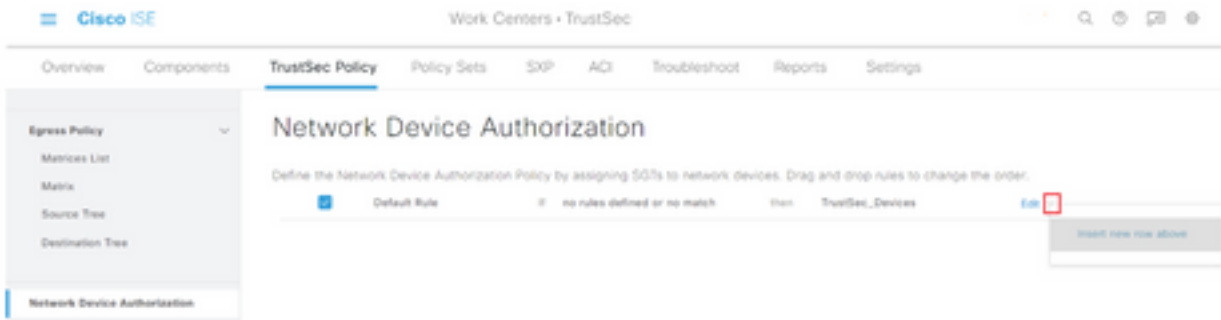
ステップ1: 左上隅にある3行のアイコンを選択し、[Work Centers] > [TrustSec] > [TrustSec Policy] を選択します。

ステップ2: 左側のペインで、[Network Device Authorization]をクリックします。



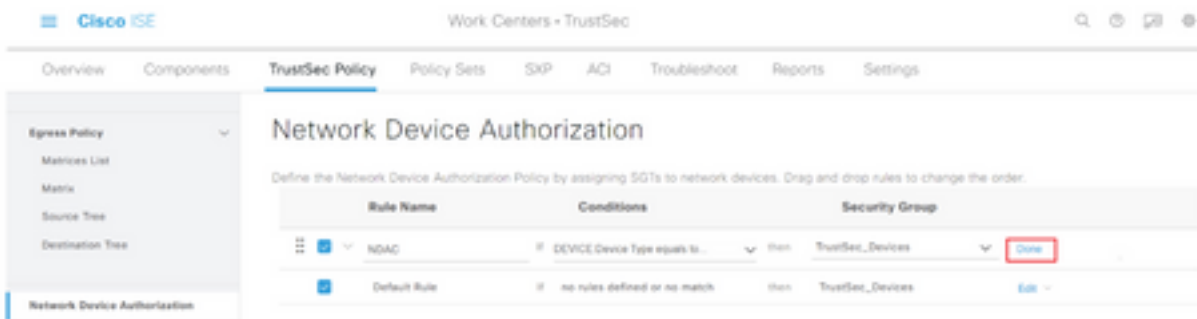
ステップ3: 右側で、[Edit] の横にあるドロップダウンを使用し、[Insert new row above] で新しい

NDAルールを作成します。



ステップ4:ルール名と条件を定義し、[Security Groups] のドロップダウンリストから適切なSGTを選択します。

ステップ5 : 右端の[Done] をクリックします。



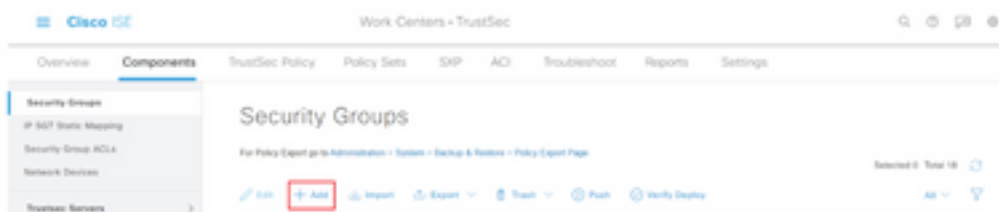
ステップ6 : 下にスクロールして、[Save]をクリックします。

## SGT

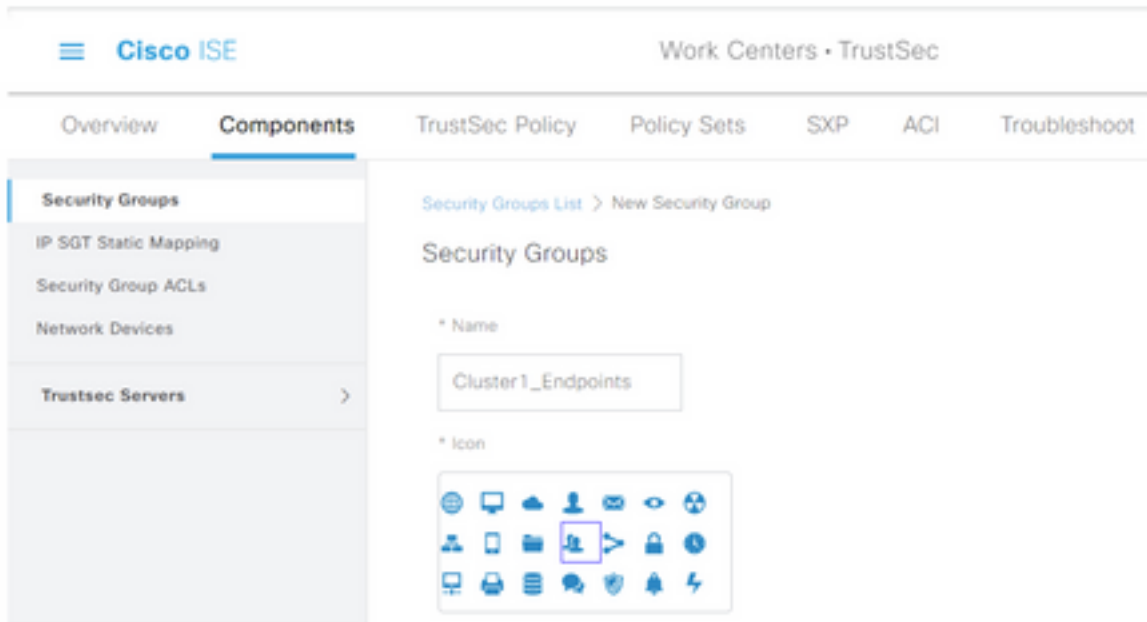
ステップ1:左上隅にある3行のアイコンを選択し、[Work Centers] > [TrustSec] > [Components]を選択します。

ステップ 2 : 左側のペインで、[Security Groups] を展開します。

ステップ3:+Addをクリックして新しいSGTを作成します。



ステップ4 : 名前を入力し、該当するフィールドでアイコンを選択します。



ステップ5 : オプションで、説明を入力し、[Tag Value]を入力します。

注 : タグ値を手動で入力できるようにするには、[Work Centers] > [TrustSec] > [Settings] > [General TrustSec Settings]に移動し、[Security Group Tag Numbering] で[User Must Enter SGT Number Manually] オプションを選択します。

ステップ6 : 下にスクロールして、[Submit]をクリックします

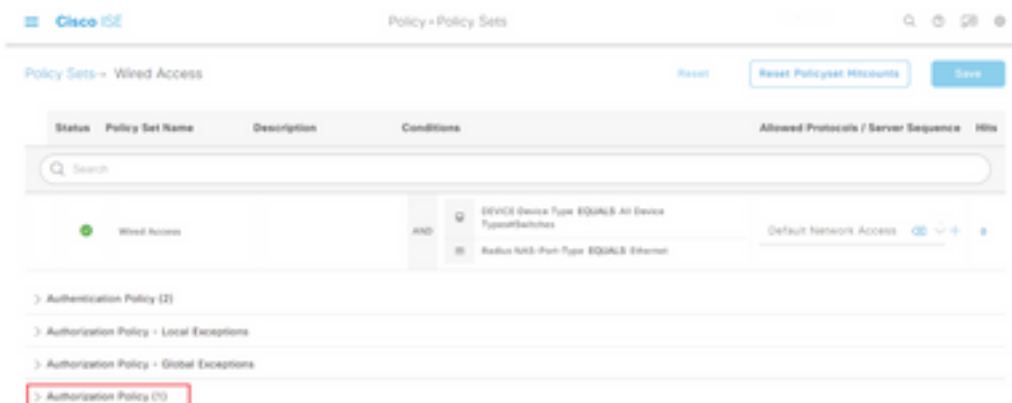
注 : 必要なすべてのSGTについて、これらの手順を繰り返します。


## 認可ポリシー

ステップ1:左上にある3行のアイコンを選択し、[Policy] > [Policy Sets]を選択します。

ステップ 2 : 適切なポリシーセットを選択します。

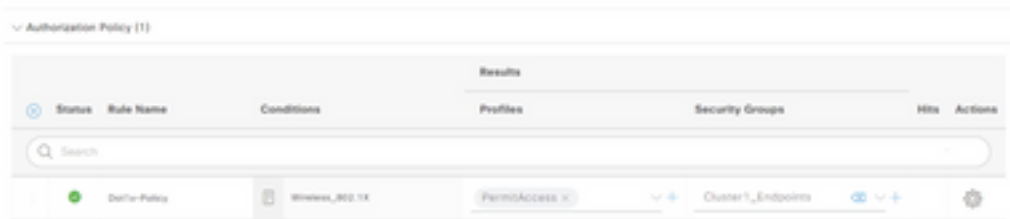
ステップ3 : ポリシーセット内で、[Authorization Policy] を展開します。



ステップ4:[Configuration]  ボタンをクリックして認可ポリシーを作成します。



ステップ5:必要な[Rule Name]、[Condition/s]、および[Profiles] を定義し、[Security Groups] のドロップダウンリストから適切なSGTを選択します。



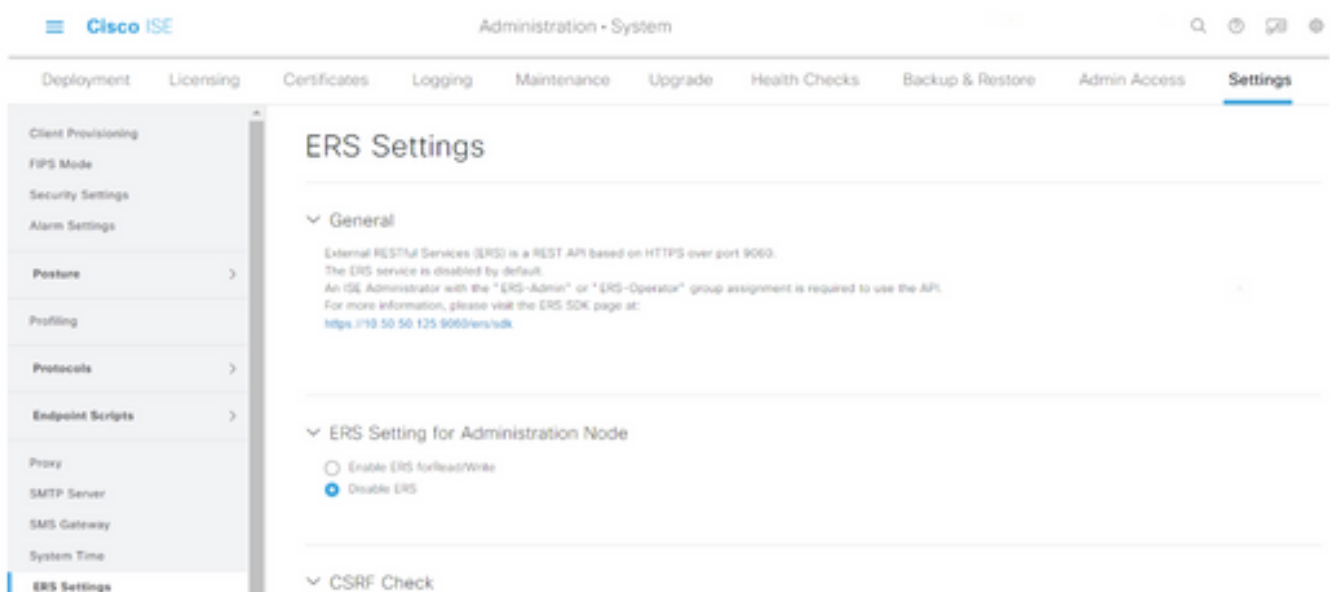
ステップ6:[Save] をクリックします。

## ISEアグリゲーションノードでのERSの有効化 ( オプション )

外部RESTful APIサービス(ERS)は、WSAがグループ情報を照会できるAPIです。ISEでは、ERSサービスはデフォルトで無効になっています。この機能を有効にすると、クライアントはISEノード上のERS Adminグループのメンバーとして認証される場合にAPIを照会できます。ISEでサービスを有効にし、アカウントを正しいグループに追加するには、次の手順を実行します。

ステップ1:左上隅にある3行のアイコンを選択し、[Administration] > [System] > [Settings]を選択します。

ステップ 2 : 左ペインで、[ERS Settings]をクリックします。



ステップ3:[Enable ERS for Read/Write] オプションを選択します。

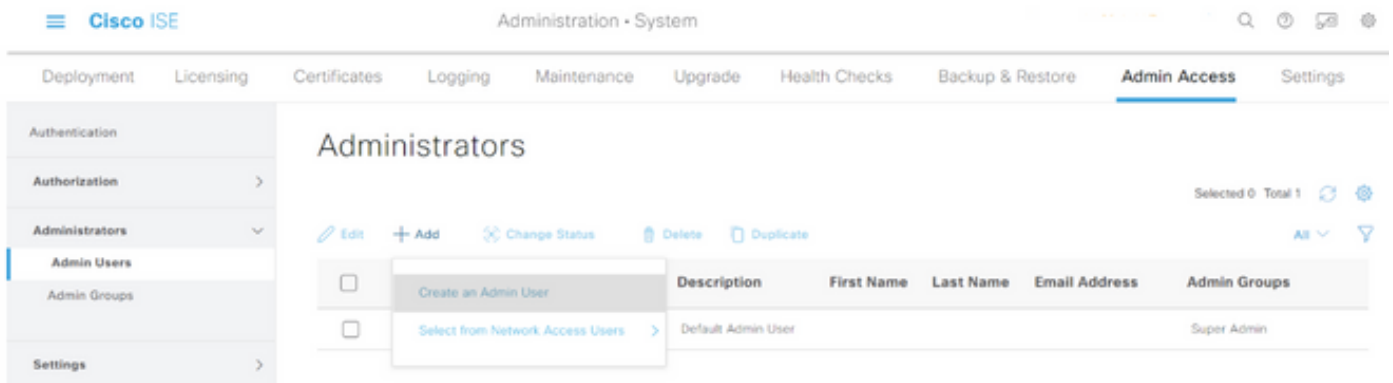
ステップ4:[Save] をクリックし、[OK] をクリックして確定します。

## ESR管理グループへのユーザの追加 ( オプション )

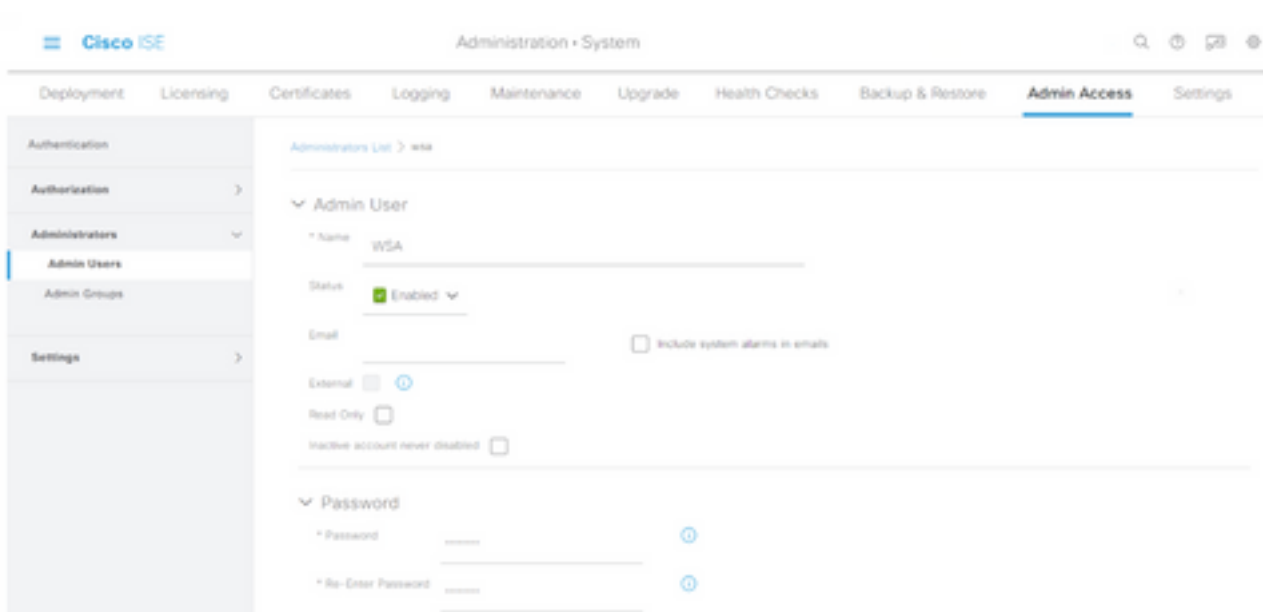
ステップ1:左上隅にある3行のアイコンを選択し、[Administration] > [System] > [Admin Access] を選択します

ステップ 2 : 左側のペインで[Administrators] を展開し、[Admin Users] をクリックします。

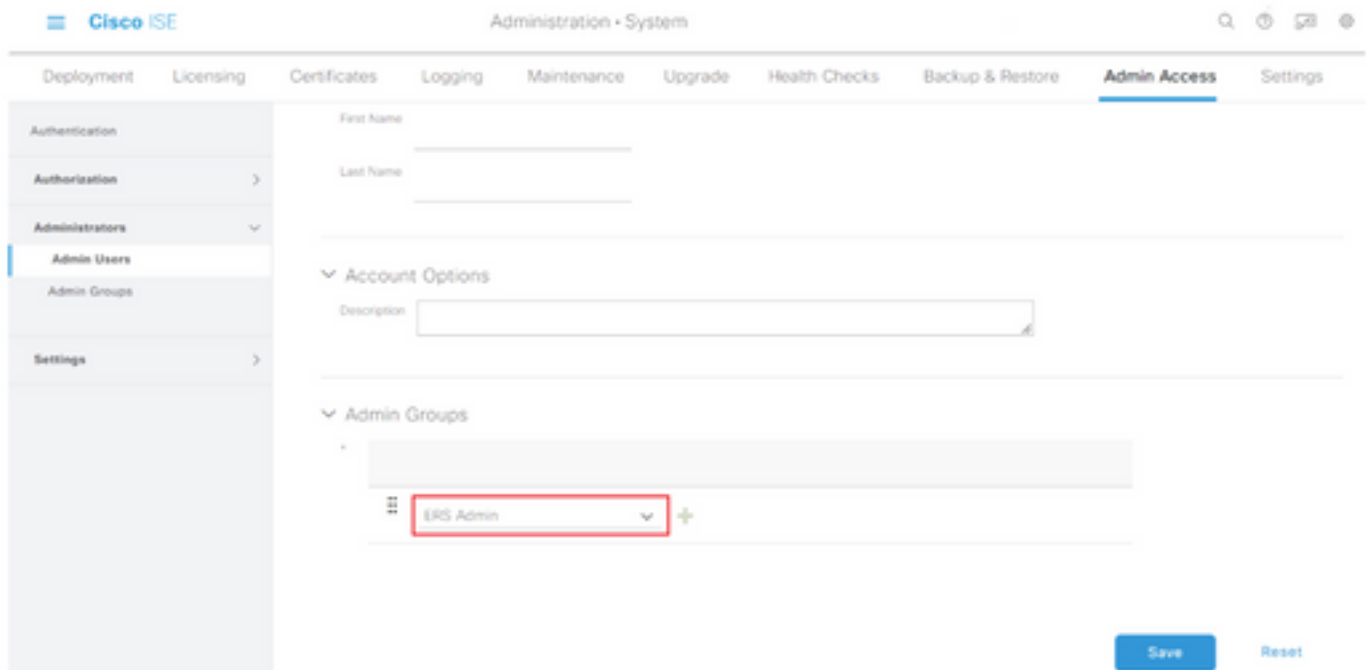
ステップ3:[Add] をクリックし、ドロップダウンから[Admin User] を選択します。



ステップ4 : 該当するフィールドにユーザ名とパスワードを入力します。



ステップ5:[Admin Groups] フィールドで、ドロップダウンを使用して[ERS Admin] を選択します。



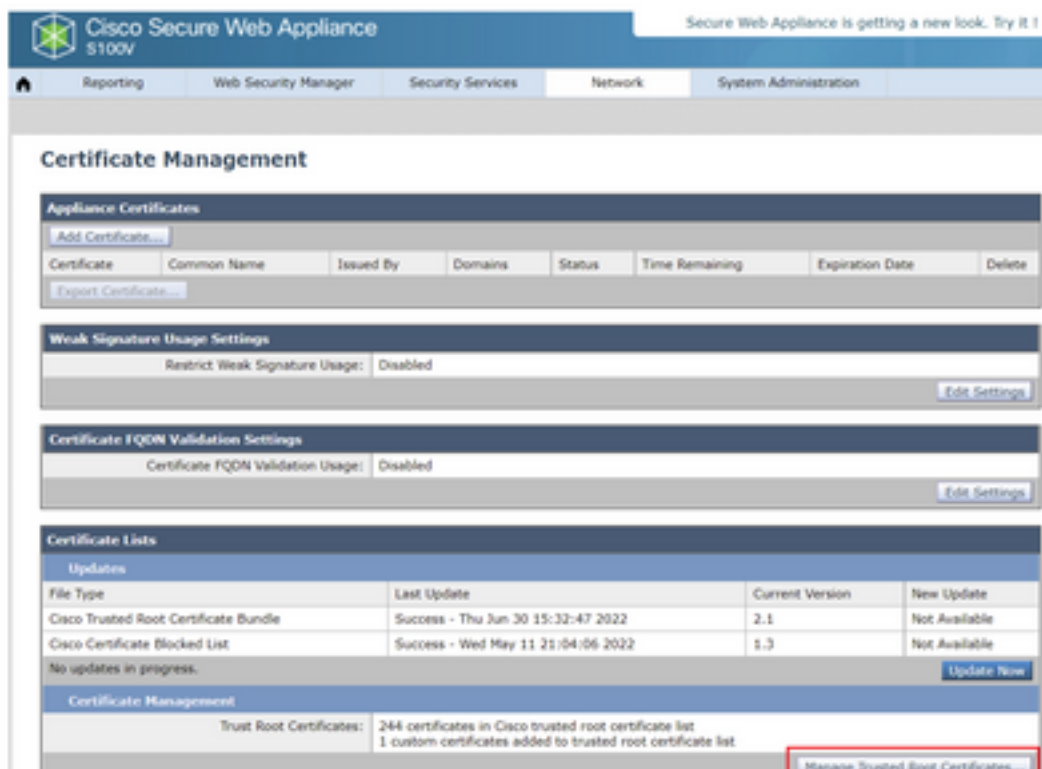
ステップ6:[Save] をクリックします。

## セキュアWebアプライアンスの設定

### ルート証明書

統合設計で、WSAとISE間の接続の信頼ルートとして内部認証局(CA)を使用する場合、このルート証明書を両方のアプライアンスにインストールする必要があります。

ステップ1:[Network] > [Certificate Management] に移動し、[Manage Trusted Root Certificates] をクリックしてCA証明書を追加します。



ステップ2:[Import]をクリックします。



ステップ3:[Choose File] をクリックして、生成されたルートCAを探し、[Submit] をクリックします。

ステップ4:[Submit] をもう一度クリックします。

ステップ5:右上隅の[Commit Changes] をクリックします。



ステップ6:[Commit Changes] をもう一度クリックします。

## pxGrid証明書

WSAでは、pxGridで使用するキーペアと証明書の作成が、ISEサービス設定の一部として完了します。

ステップ1:[Network] > [Identity Service Engine]に移動します。

ステップ2:[Enable and Edit Settings] をクリックします。

ステップ3:[Choose File] をクリックして生成されたルートCAを探し、[Upload File] をクリックします。



注：一般的な誤設定は、このセクションでISE pxGrid証明書をアップロードすることです。ルートCA証明書を[ISE pxGrid Node Certificate]フィールドにアップロードする必要があります。

ステップ4:[Web Appliance Client Certificate] セクションで、[Use Generated Certificate and Key] を選択します。



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

ステップ5:[Generate New Certificate and Key] ボタンをクリックし、必要な証明書フィールドに入力します。

### Generate Certificate and Key

Common Name:

Organization:

Organizational Unit:

Country:

Duration before expiration:  months

Basic Constraints:  Set X509v3 Basic Constraints Extension to Critical

ステップ6:[Download Certificate Signing Request] をクリックします。

注：[Submit] ボタンを選択して、変更をISE設定にコミットすることをお勧めします。変更が送信される前にセッションがタイムアウトのままになっている場合、CSRがダウンロードされていても、生成されたキーと証明書が失われる可能性があります。

ステップ7:CAでCSRに署名した後、[Choose File] をクリックして証明書を見つけます。

**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: ws-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:

ステップ8:[Upload File] をクリックします。

ステップ9:送信して確定します。

## セキュアWebアプライアンスでのSXPおよびERSの有効化

ステップ1:SXPとERSの両方の[Enable]ボタンをクリックします。

ISE SXP 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 Type (SGT), you should enable ERS.

ステップ2:[ERS Administrator Credentials] フィールドに、ISEで設定されたユーザ情報を入力します。

ステップ3:[Server name same as ISE pxGrid Node] チェックボックスをオンにして、以前に設定した情報を継承します。それ以外の場合は、必要な情報を入力します。

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)

ステップ4:SubmitとCommitを実行します。

## 識別プロファイル

WSAポリシーでセキュリティグループタグまたはISEグループ情報を使用するには、ユーザを透過的に識別する手段としてISEを利用する識別プロファイルを最初に作成する必要があります。

ステップ1:[Web Security Manager] > [Authentication] > [Identification Profiles] に移動します。

ステップ2:[Add Identification Profile] をクリックします。

ステップ3 : 名前と説明 ( オプション ) を入力します。

ステップ4:[Identification and Authentication] セクションで、ドロップダウンを使用して [Transparently identify users with ISE] を選択します。

#### Identification Profiles: Add Profile

**Client / User Identification Profile Settings**

Enable Identification Profile

Name: ISE Profile  
(e.g. my IZ 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:

(examples: 20.1.1.0, 20.1.1.0/24, 20.1.1.1-10, 2001:420:80:2::5, 2000:db8::2-2000:db8::10)

Define Members by Protocol:  HTTP/HTTPS

Advanced Define additional group membership criteria.

ステップ5:SubmitおよびCommitです。

## SGTベースの復号化ポリシー

ステップ1:[Web Security Manager] > [Web Policies] > [Decryption Policies] に移動します。

ステップ2:[Add Policy] をクリックします。

ステップ3 : 名前と説明 ( オプション ) を入力します。

ステップ4:[Identification Profiles and Users] セクションで、ドロップダウンを使用して [Select One or More Identification Profiles] を選択します。

ステップ5:[Identification Profiles] セクションで、ドロップダウンを使用してISE識別プロファイルの名前を選択します。

ステップ6:[Authorized Users and Groups] セクションで、 [Selected Groups and Users] を選択します。

**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	<input type="button" value="Add Identification Profile"/>
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 falling authentication)	<input type="button" value="Add"/>

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.

ステップ7:[ISE Secure Group Tags]の横にあるハイパーリンクをクリックします。

ステップ8:[Secure Group Tag Search] セクションで、目的のSGTの右側のボックスをオンにし、[Add] をクリックします。

**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"/>

**Secure Group Tag Search**

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

Search

0 Secure Group Tag(s) selected for Add

Secure Group Tag Name	SGT Number	SGT Description	Select <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"/>

ステップ9:[Done] をクリックして戻ります。

ステップ10:送信して確定します。

## スイッチの設定

[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

```

## 確認

ISEからエンドポイントへのSGT割り当て。

次に、認証と認可が成功した後にSGTが割り当てられたISEクラスタ1のエンドポイントを示します。

Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authentication Policy	Authentication Profile	IP Address	Security Group	Server
10.50.50.120	14.02.001	IP Device	Word Access -->	Word Access -->	Permissive	10.50.50.12	Cluster1_Endpoint	ise01-cl1

次に、認証と認可が成功した後にSGTが割り当てられたISEクラスタ2からのエンドポイントを示します。

Identity	Endpoint ID	Endpoint Profile	Authorization Policy	Authentication Policy	Authentication Profile	IP Address	Security Group	Server
10.50.50.121	14.02.002	Microsoft Work	Word Access -->	Word Access -->	Permissive	10.50.50.12	Cluster2_Endpoint	ise02-cl1

## SXPマッピング

クラスタISEノードとISEアグリゲーションノードの間でSXP通信が有効になっているため、これらのSGT-IPマッピングはSXPを介してISEアグリゲーションによって学習されます。

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	10-422
10.50.50.112	TrustSec_Device (20000)		10.50.50.122_10.50.50.7	SXP	default	10-422
10.50.50.121	Cluster_Endpoints (1110000)		10.50.50.121_10.50.50.5	SXP	default	10-422
10.50.50.122	Cluster_Endpoints (2220000)		10.50.50.122_10.50.50.7	SXP	default	10-422

異なるISEクラスタからのこれらのSXPマッピングは、ISEアグリゲーションノードを介してpxGrid経由でWSAに送信されます。

```

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ベースのポリシー適用

ここでは、さまざまなエンドポイントがそれぞれのポリシーに一致し、トラフィックがSGTに基づいてブロックされることを確認できます。

## ISEクラスタ1に属するエンドポイント



**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', WBSA: 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

## ISEクラスタ2に属するエンドポイント



### This Page Cannot Be Displayed

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

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

Date: Thu, 14 Jul 2022 14:23:58 CEST  
Username: isesxp\_10.50.50.122\_sgt222\_10.50.50.13  
Source IP: 10.50.50.13  
URL: GET https://www.facebook.com/  
Category: Block URLs CL2  
Reason: UNKNOWN  
Notification: BLOCK\_DEST

Time (GMT +02:00)	Website (count)	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:23:58	https://www.facebook.com/43/revision/ice CONTENT TYPE: ... URL CATEGORY: Block URLs CL2 DESTINATION IP: ... DETAILS: Decryption Policy: 'ISE_Cluster2', WBSA: 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

## 関連情報

- [『Web Security Appliance and Identity Service Engine Integration Guide』](#)
- [TrustSec 認識サービス用の ISE と WSA との統合設定](#)
- [Cisco Identity Services Engine 管理者ガイド リリース 3.1](#)
- [AsyncOS 14.5 for Cisco Secure Web Appliance ユーザガイド](#)