# 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 <u>使用するコンポーネント</u> 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 <u>ネットワークデバイス認可</u> 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。
- 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. レポーティングとトラッキングは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 左上隅にある[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。

E Cisco ISE		Administration - System				Administration - System			Q		73 (
Deployment Licensing	Certificates	Logging	Maintenance	Upgrade Her	alth Checks Bac	kup & Restore	Admin Access	Setting	gs.		
Deployment < > 25 Deployment	• De	eploymer	nt Nodes	Deregister			Selected 1 Total 1	1 2 4 W Y	8		
35 PAN Failover	C	Hostname	A Personas		Role(s)	Services	No	ode Statu	us		
		ise01-CL1	Administra	tion, Monitoring, Policy Se	nikoe STANDALONE	SESSION, PROFILER					

**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

E Cisco ISE	Cisco ISE Administration - System					. Q	0 23 0
Deployment Lic	ensing Certificates	Logging Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
		📴 🛩 Enable Sessi	on Services G	)			
		Include Node in N	ode Group None		× 0		
		🛃 Enable Profiling Service 🤅					
		Enable Threat Centric NAC	: Service 🕕				
		🖉 🛩 Enable SXP S	iervice 🕢				
		Use interface	GigabitEthernet	0	~		

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。

クラスタノードでのSXPの設定

0

**ステップ1:3行**のアイコンを選択します <sup>=</sup> 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

■ Cisco ISE	Work Centers - TrustSec	
Overview Compone	ts TrustSec Policy Policy Sets SXP ACI Trout	bleshoot Reports Settings
SXP Devices All SXP Mappings	SXP Devices o	
	Rows	Page 2 v K ( 1 /1>>) Go 2 Total Rows
	Ø Refresh 🕂 Add 🛛 Trash ✓ 🖉 Edit — Assign SXP Domain	⊽rmer ∽ ⊕

**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。

Overview	Components	TrustSec Policy	Policy Sets	SXP	AC
SXP Devices		SXP Devices > SXP C	onnection		
All SXP Mappings		<ul> <li>Upload from a CS<sup>1</sup></li> </ul>	V file		
		- Add Single Device			
		Input fields marked v	with an asterisk (*)	are required	Ι.
		Name ISE Aggregation n	ode		
		IP Address * 10.50.50.125			
		Peer Role * LISTENER		~	
		Connected DSNs *			
		ise01-CL1 ×			



Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI
SXP Devices All SXP Mappings		SXP Domains * default ×		~	
		Status *			
		Enabled		$\sim$	
		Password Type * CUSTOM		~	
		Password			
		Version * V4		~	
		Advanced Settings	1		
			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

E Cisco ISE		Work Centers · TrustSec							
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings	
General TrustSec 1 TrustSec Matrix Se	Settings ettings	SXP Settings							
Work Process Sett	ings	Publish SXP bindir Global Dascuus	ngs on PxGrid 🛃 Ad	d radius map	opings into S	O/P IP SGT mapping table	0		
SXP Settings		Giobai Passwoi	0						
ACI Settings		Global Password This global passwor the device specific	rd will be overriden password	by					

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。

Cisco ISE	Administration - System	1 · · · · · · · · · · ·	0 50 0
Deployment Licensing Certifica	tes Logging Maintenance Upgrade Health Checks	Backup & Restore Admin Access	Settings
Deployment C C C C	Deployment Nodes	Selected	н том г. 2) Ф Аг ∨ — 7
.g. PAN Fallover	Hostname	Role(s) Services	Node Status
	ativities age Administration, Monitoring, Policy Service	STANDALONE SESSION/PROFILER	۰

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。

Cisco ISE	Administration - System	Q,	0 50 0
Deployment Uconsing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access	Settings
	Enable Session Services ()		
	Include Node in Tende Group Nome 🗸 🕥		
	Evalue Probing Service 🕤		
	🗌 Emailse Thread Cantor: NHG Service 💿		
	Enable SXP Service ()		
	Lite smothers digabit@thernet.0 V		
	🗌 Enables (Iwaras Admin Sararas 💿		
	Costine Pessore coentry Service 📀		
	teque O		

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。

E Cisco ISE			Administration - pxGrid Services		
Summary	Client Management	Diagnostics	Settings		
Set	tings				
	utomatically approve new certification and the second based account cre	ate-based accounts	0		
	Use D	efault Sa	ive		

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。

Cisco ISE	Administration - Network Resources
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers
Network Devices	TACACS Authentication Settings
Default Device	SNMP Settings
Device Security Settings	Advanced TrustSec Settings

**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。

Cisco ISE	Administration • Network Resources					
Network Devices	Network Device Groups	Network Device	e Profiles	External RADIUS Servers		
Network Devices	🔄 🗸 Adv	anced TrustSec	Settings			
Default Device Device Security Settings	✓ De Use De Identifié Device * Pass	vice Authentical vice ID for TrustSec ation Id	SW1	\$		

**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。

Cisco ISE		Administration - Network Resources						
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More ~			
Network Devices								
Default Device	V Tru	stSec Notifications and U	pdates					
Device Security Settings		the day in the second second	1					
	- (com	road envelopment data every	Days 🗸					
	* Dow	<ul> <li>Download peer authorization policy every</li> </ul>	Days 🖌					
			,					
	* Pers	thertication every	Days 🛩 🕢					
			1					
	* Dow	rioad SGACL lists every	Days ¥					
	Other 1	institled devices to trust this device						
	Send o	orfiguration changes to device	Using O CoA (	0 eu				

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。

Overview 0	Components	TrustSec Policy	Policy Sets	SIP /	CI Troubleshoot	Reports	Settings		
Igneen Policy Matrices List	~	Network D	)evice Au	uthoriza	tion				
Matrix		Define the Network D	Neves Autoreano	n Policy by and	gning SG15 to network de	vices. brag and	drop rules to change the r	order.	

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。

E Cisco ISE	Work Centers - TrustSec	
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports Settings	
Egross Policy ~ ~	Network Device Authorization	e order.
Matrix Source Tree Destination Tree	Default Bule If no rules defined or no match than TruetSec_Devices	Ede Disset new row above
Network Device Authorization		

**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。

E Cisco ISE	Work	0.020		
Overview Components	TrustSec Policy Policy Sets	SXP ACI Troubleshoo	x Reports Settings	
Egress Policy ~ ~ Matrices List	Network Device A	Authorization	devices. Drag and drop rules to change the order.	
Source Tree	Rule Name	Conditions	Security Group	
Destination Tree	🗄 🗃 🗠 NDAD	# DEVICE Device Type equals to	v ter Turbec,Devices v 🖸	
Network Device Authorization	<ul> <li>Default Rule</li> </ul>	if no rules defined or no match	then TrustBee_Devices 6d	· ·

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。

III Cisco ISE	Work Centers - TrustSec	0.0000
Overview Components	TrustSec Policy Policy Sets SNP ACI TrustRenhost Reports Settings	
Security-Drouge	October October	
IP 967 Static Mapping	Security Groups	
Security Group ACLA	For Policy Expert prior Advancementation + Sectory & Renton + Policy Expert Prope	
Natwork Devices		Selected II Total 18
Instant Servers >	J <sup>2</sup> Elli → And () Separt () Separt () Senation () Neutro Deploy	AI ~

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。

Cisco ISE	Work Centers · TrustSec					
Overview Components	TrustSec Policy Policy Sets SXP ACI Troubleshoo					
Security Groups	Security Groups List > New Security Group					
P SGT Static Mapping	Security Groups					
Security Group ACLs						
Network Devices	* Name					
Trustsec Servers >	Cluster1_Endpoints					
	* Icon					

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。

Cisco ISE	Policy = Pr	olicy	Sets			9. 0	ça o
Policy Sets-+ Wired Access				Reset	Reset Policyset Hitcourt		
Status Policy Set Name D	escription Conditio	***			Allowed Protocols / Serv	er Sequence	Hits
Q Seed							
Wind Access	100		DEVICE Onvice Paper EQUINER AT Device - Papers/Switches		Default Network Access		
-		B Ratio MS Part Type B2063 Ethernet					
> Authentication Policy (2)							
> Authorization Policy - Local Exceptions							
> Authorization Policy - Global Exceptions							
> Authorization Policy (1)							



- Management and Di-					
		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

**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。

		Results	Results			
Status Rule Name	Conditions	Profiles	Security Groups			
Q Search						
O Dathe-Pathop	() Winters, 852.1X	PermitAccess ×	v + Ouster1_Endpoints d8 v	+ 0		

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。

E Cisco	ISE		A	dministration - S	stration - System			Q	0 90
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Client Provisioning FIPS Mode Security Settings	ĺ	ERS S	ettings						
Alarm Settings		✓ Genera	4						
Posture		External RE The ERS se An ISE Adm	STM Services (D rvice is disabled t inistrator with the	IS) is a REST API based ly default. " ERS-Admin" or " ERS	-Operator® group	ort 9060. assignment is required to r	use the API.		
Profiling		For more in https://10.5	formation, please 0.50.125.9060/ers	visit the ERS SDK page /sdk	M:				
Protocols									
Endpoint Scripts	>	✓ ERS Se	tting for Adr	ninistration Node	,				
Proxy		O Erable	Did forhead/Write						
SMTP Server		O Deable	ERS						
SMS Gateway									
lystem Time									
ERS Settings		CSRF C	Check						

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。

≡ Cisco I	SE		Administration - System						C © 50 ¢				
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & R	lestore	Admin Acces	s Setting	js		
Authentication		Admir	nistrators	5									
Authorization	>								Selec	ted 0 Total 1 📿			
Administrators	~	0 ton -	- Add 🛞 C	hange Status	Delete DD	uplicate				AI V	Y		
Admin Users													
Admin Groups			Create an Admin	User	Description	First Name	Last Name	Email Add	ress Admi	n Groups			
			Select from Netv	work Access Users	> Default Admin	User			Super	Admin			
Settings	>												

### 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。

I Cisco ISE			Administration • S	lystem	Q	0 20 0	
Deployment L	Licensing	Certificates Log	ping Maintenance	Upgrade Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Administrations Unit 2 =	58				
Authorization	-	✓ Admin User					
Administrators	~	"Name WSA					
Admin Usors							
Admin Groups		Status 🖬 Enab	ied 🛩				
		Email		D Include system alarms in emails			
Settings	>			0			
		and C					
		hastles account new	r disabled				
			0				
		✓ Password					
		* Password		0			
		* Re-Enter Parsec					

**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。

E Cisco I	SE		A	Administration - System				Q,	© 58 ⊕
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		First Name							
Authorization	>	Last Name							
Administrators	~								
Admin Usors		× Accourt	t Octions						
Admin Groups		Description					*		
Settings	>								
		<ul> <li>Admin</li> <li>∎</li> </ul>	Groups ERS Admin		× +				
								Save	Reset

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。

🛃 Cisco S	Secure Web Appliance			Secure Web Appliance is get	ting a new look. Try it
Reporting	Web Security Manager	Security Services	Network	System Administration	
Certificate	Management				
Appliance Certil	licates				
Add Certificate.					
Certificate	Common Name Issued	By Domains	Status Time I	Remaining Expiration	Date Delete
Export Certificat	Here .				
Weak Signature	Usage Settings				
	Restrict Weak Signature Usage:	Disabled			
					Edit Settings
Certificate FQD	N Validation Settings				
0	ertificate FQON Validation Usage:	Disabled			
					Edit Settings
Certificate Lists					
Updates					
File Type		Last Update		Current Version	New Update
Cisco Trusted Rox	ot Certificate Bundle	Success - Thu Jun 30 1	5:32:47 2022	2.1	Not Available
Cisco Certificate	Blocked List	Success - Wed May 11	21:04:06 2022	1.3	Not Available
No updates in pro	igress.				Update Now
Certificate H	anagement				
	Trust Root Certificates:	244 certificates in Cisco tr 1 custom certificates adde	rusted root certificate is ed to trusted root certif	et Icate Int	
				Manage True	and Boot Certificates

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。

**Identity Services Engine** 

Edit Scientity Services Engine Settings	
C Enable 150 Dervice	
Primary 15E peloid Node:	The Blob Appliance will communicate with the 202 partial rook to support Blob Appliance data subscription (separag sphere). A primary 202 partial node (server) must be configured.
	(Sectore or Det addres)
	Itst pedret hole Certificate: If the ISE pedret hole certificate is signed by a Certificate Authority, conferm that the Certificate Authority is lated in the Trusted Root Certificates list (see Network in Certificate Management) and uplace the CA-regiment not certificate basins. If the certificate is set signed, region the certificate from the Egi priority revise it and basis. If the certificate later is includes any intermediate certificate region the certification from the Egi priority revise it and basis. Notice update the confidence in the Includes any intermediate certificates
	Certificate Ocean File I for the Ocean

**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 to the ISE period node()	in between the Web Appliance i () configured above.	and the ISE paGrid servers, provide a clier	it certificate. This may need to be u
	O Use Uploaded Cert	ficate and Key		
	Certificate:	Choose File No file chosen.	Upload files	
	Key:	Choose File No file chosen		
		Key is Encrypted		
		No certificate has been upload	led.	
	Use Generated O	ertificate and Key	Generate New 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 an	d Key	$\boxtimes$
Common Name:		
Organization:		
Organizational Unit:		
Country:		
Duration before expiration:	months	
Basic Constraints:	<ul> <li>Set X509v3 Basic Constraints Extension to Critical</li> </ul>	
Generate Cancel		

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.					
	O Use Uploaded Certificate and Key					
	Certificate: Choose File No file chosen Upload Files					
	Key: Choose File No file chosen					
	Key is Encrypted					
	No certificate has been uploaded.					
	Use Generated Certificate and Key     Generate New Certificate and Key					
	Common name: wsa.security/abunet					
	Organizational Unit: Security					
	Country: SI					
	Expiration Date: May 50 19:19:26 2024 GMT					
	Basic Constraints: Not Oritical					
	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: Choose File No file chosen Upload File					

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。



**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:	WSA	
	Password:		
	ERS Servers		
	Server name same as ISE pxGrid Node		
	Primary:	ise-agg.securitylab.net	(Hostname or IPv4 address)
	Secondary (Optional):		(Hostname or IPv4 address)
	Port:	9060 (Enter the port ru	mber specified for ERS in 1SE)

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

Enable Identification Profile	
Name: 🕐	ISE Profile (e.g. my IT Profile)
Description:	Identification profile for ESE Integration. (Havimum allowed characters 256)
Insert Above:	2 (Slobel Profile) V
Identification Hethod	
Identification and Authentication: 🕐	Transparently identify users with ISE V
Fallback to Authentication Realm or Guest Privileges: 2	If user information is not available from the Identity Services Engine:
	Support Guest Privileges
	Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manaper > Decryption Policies, Routing Policies and Access Policies).
herabio Definition	
benship is defined by any combination of the R	slowing options. All criteria must be met for the policy to take effect.
Define Members by Subnet:	
	(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:115, 2000:888:1-2000:888:10)
Define Members by Protocol:	HTTP/HTTPS

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。

Identification Profiles and Users:	Select One or More Identification Profiles 💙				
	Identification Profile	Authorized Users and Groups	Add Identification Pro		
	ISE Profile	All Authenticated Users			
		Selected Groups and Users (2) ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered	8		
		Guests (users falling authentication)			
	Authentication information may not proxy traffic, user agent information	be available at HTTPS connection tin is unavailable for decryption policie	ne. For transparent 5.		
h Advanced	Particle and Direct over an end works				

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。

there a success well all concerned mental	ded in this policy.		
Secure Group Tag Name	SGT Number	SGT Description	Delete
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	0

ecure Group Tag Search			
Enter any text to search for a Sec Add botton to add to this policy. Search	ure Group Tag name, number, or o	lescription. Select one or more Secure Group Tags from th	e list and use the
0 Secure Group Tag(s) select	ed for Add		_A04
Secure Group Tag Name	SGT Number	SGT Description	Setect At
Production_Servers	15	Production Servers Security Group	0 .
Point of Sale Systems	10	Point of Sale Security Group	
Test_Servers	13	Test Servers Security Group	0
Development_Servers	12	Development Servers Security Group	0
syop	15	8YOO Security Group	Ö
PCI_Servers	14	PCI Servers Security Group	0
Guests	6	Guest Security Group	
ANY	65535	Any Security Group	0
Unknown	0	Unknown Security Group	0
Network_Services	3	Network Services Security Group	0
TrustSec_Devices	2	TrustSec Devices Security Group	0
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	
When the second	4	Employee Receipt Course	

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  $\tt Cisco123$  (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。

 w
 Industrie
 Industrie
 Automation Public
 Automation Public
 Automation Public
 Automation Public
 Material

 26 10, 100 110741 Mb.
 Image: Automation Public
 Imag

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。

 v
 Methy
 Segure D
 Depart Pulse
 Autorization Pulse
 Autorization Pulse
 Filables
 Ensure Group
 Ensure

 Al 16,2023-02-041
 B
 Methods
 Million
 Million

#### 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。

III Oisco 155		Work Center	s • TrustSec			-	
Overview Components	Trustlec Policy P	No SP AD	houbleahoot	Reports Settings			
DIP-Devices NO 507 Westings	All SXP Ma	opings o	-		handhaga <u>k</u>	<u>v</u> < <u>1</u> _1	1) the back
	IF Address	967	-	Learned From	Learned By	SNP Domain	PSNs involved
	10.00.00.0.00	Turbs, Jacob (1991)		103030-12120-0030-0	5.0	anut	14 422
	10.00.00.100	Testler, Jacob (1993)		10.00.001123.10.00.007	547	defect.	144-400
	10.00.00.10.02	Ounter1, Endpoints (111,0007)		10.30.30.121.10.30.30.3	5.0	defect.	144-400
	10.00.00.10.07	Daniel Johnson (201900)		10100310222-00302	347	darlault.	144-100

### 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。



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





Usemame: 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

Results					
					Items Displayed 50 🛩
Displaying 1 - 50 of 13	7 items.				+ Previous   1   2   3   Next +
Time (GRT +02:00) +	Website (munt)	Display All Details	Disposition	Bandwidth	User / Client IP
54 34 2022 54 28 57	https://bbc.com/s45/Tavicon.ice coversari 1999 - um. Cartonic Biok URLs CL1 destroation IP- derinitis Decrystein Policy: "ISE_Ou Malware Analytics File Verdict: -	uber1", WBRS: No Score,	Block - URL CH	¢8	isessg_10.50.50.121_sg7111_10.50.50.12 (3den0fed by 158) 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 Displaye	d		
Based ( https	on your organization's access polic //www.facebook.com/ ) has been b	cies, access to thi locked.	s web site	
If you codes	have questions, please contact you shown below.	r organization's n	etwork admini	strator and provide the
Date: 1 Usemi Source URL: 0 Catege Reaso Notific	Thu, 14 Jul 2022 14:23:58 CEST Ime: isesxp_10.50.50.122_sgt222_ IP: 10.50.50.13 SET https://www.facebook.com/ iy; Block URLs CL2 n: UNKNOWN ation: BLOCK_DEST	10.50.50.13		
papaying 1 - 2 of 2 ite	ng. Malaita (asuat) Disalas Al	Datala Dissection	Rendelath	United A Classif Mit
14 34 2022 14:23:58	https://www.facebook.com/std2/favicon.ico	Block - URL Cat	08	inesup_30.50.50.122_sqt222_10.50.50.
	CONTRACT FYRE - URL OFFECONT Block URLs CL2 DESTINATION DY - CONTRACT, CARDING BUILD, 2018 (Contract), which is			(20+054d by 2 30.50.50



- <u>"Web Security Appliance and Identity Service Engine Integration Guide\_</u>
- <u>TrustSec 認識サービス用の ISE と WSA との統合設定</u>
- Cisco Identity Services Engine 管理者ガイド リリース 3.1
- <u>AsyncOS 14.5 for Cisco Secure Web Applianceユーザガイド</u>