# Integration mehrerer ISE-Cluster mit einer sicheren Web-Appliance für TrustSec-basierte Richtlinien

# Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Einschränkungen Netzwerkdiagramm Konfigurieren **ISE-Konfiguration** SXP aktivieren Konfigurieren von SXP auf den Cluster-Knoten Konfigurieren von SXP auf dem Aggregationsknoten Aktivieren Sie pxGrid auf dem Aggregationsknoten. pxGrid-automatische Genehmigung TrustSec-Einstellungen für Netzwerkgeräte Autorisierung von Netzwerkgeräten SGT Autorisierungsrichtlinie Aktivieren von ERS auf ISE Aggregation Node (optional) Benutzer zur ESR-Admin-Gruppe hinzufügen (optional) Sichere Web-Appliance-Konfiguration pxGrid-Zertifikat Aktivieren Sie SXP und ERS auf einer sicheren Web-Appliance Identifizierungsprofil SGT-basierte Entschlüsselungsrichtlinie Switch-Konfiguration AAA **TrustSec** Überprüfung Zugehörige Informationen

# Einleitung

In diesem Dokument wird das Verfahren beschrieben, mit dem die Security Group Tag (SGT)-Informationen von mehreren ISE-Bereitstellungen über pxGrid an eine einzige Cisco Secure Web Appliance (Formally Web Security Appliance WSA) gesendet werden, um die SGT-basierten Webzugriffsrichtlinien in einer TrustSec-Bereitstellung zu nutzen. Vor Version 14.5 kann eine sichere Web-Appliance für Identitätsrichtlinien, die auf einem SGT basieren, nur in einen einzelnen ISE-Cluster integriert werden. Mit der Einführung dieser neuen Version kann die sichere Web-Appliance jetzt mit Informationen von mehreren ISE-Clustern zusammenarbeiten, wobei ein separater ISE-Knoten zwischen ihnen aggregiert wird. Dies bringt große Vorteile und ermöglicht uns, Benutzerdaten aus verschiedenen ISE-Clustern zu exportieren und die Möglichkeit zu haben, den Exit Point zu kontrollieren, den ein Benutzer verwenden kann, ohne dass eine 1:1-Integration erforderlich ist.

# Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Identity Services Engine (ISE)
- Sichere Web-Appliance
- RADIUS-Protokoll
- TrustSec
- pxGrid

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sichere Web-Appliance 14.5
- ISE Version 3.1 P3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

### Einschränkungen

- 1. Alle ISE-Cluster müssen einheitliche Zuordnungen für SGTs aufrechterhalten.
- 2. Der ISE Aggregation Node muss den Namen/die Nummer der SGTs für die übrigen ISE-Cluster aufweisen.
- 3. Sichere Web-Appliance kann Richtlinien (Zugriff/Entschlüsselung/Routing) nur anhand des SGT-Tags identifizieren, nicht jedoch anhand von Gruppen- oder Benutzernamen-.
- 4. Reporting und Tracking basieren auf SGT-basierten .
- 5. Für diese Funktion gelten weiterhin die bestehenden Größen-Parameter für ISE/Secure Web Appliance.

# Netzwerkdiagramm



Prozess:

1. Wenn der Endbenutzer eine Verbindung zum Netzwerk herstellt, erhält er ein SGT, das auf den Autorisierungsrichtlinien der ISE basiert.

2. Die verschiedenen ISE-Cluster senden diese SGT-Informationen dann in Form von SGT-IP-Zuordnungen an den ISE-Aggregationsknoten über SXP.

3. ISE Aggregation Node erhält diese Informationen und gibt sie über pxGrid an die einzelne sichere Webappliance weiter.

4. Die sichere Web-Appliance verwendet die erhaltenen SGT-Informationen, um Benutzern den Zugriff auf der Grundlage von Web-Zugriffsrichtlinien zu ermöglichen.

# Konfigurieren

# **ISE-Konfiguration**

SXP aktivieren

Schritt 1: Wählen Sie das Symbol für drei Leitungen Administration > System > Deployment.

in der linken oberen Ecke unter

Schritt 2: Wählen Sie den Knoten aus, den Sie konfigurieren möchten, und klicken Sie auf Bearbeiten.

E Cisco ISE			Administration -	System			Q	0 🕫	0
Deployment Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	5
Deployment	• De	eploymer	nt Nodes				Selected 1 Total 1	0.0	
> 35 Deployment	0	late 🕞 Angleon	D Byrova	Deregister				•~ 7	
AP PARTIE DATE	C	Hostname	Personat		Role(s)	Services	No	ide Status	
		ise01-CL1	Administra	tion, Monitoring, Polic	y Service STANDA	LONE SESSION, PROFIL	IR 🛃	1	

Schritt 3: Um SXP zu aktivieren, aktivieren Sie das Kontrollkästchen SXP-Dienst aktivieren.

E Cisco	SE		A	dministration • S	ystern			Q.	0 53 0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
			<b>2</b> ~	Enable Session	Services g	)			
				Include Node in Nod	e Group None		~ o		
			🛃 Enab	ie Profiling Service 🕣					
			Cneb	ie Threat Centric NAC S	ervice 🕕				
			<b>-</b>	Enable SXP Se	rvice 🕢				
				Use Interface	GipabitEthernet	0	~		

Schritt 4: Blättern Sie nach unten, und klicken Sie auf Speichern.

**Anmerkung:** Wiederholen Sie alle Schritte für die übrigen ISE-Knoten in jedem Cluster, dem Aggregationsknoten, der enthalten ist.

### Konfigurieren von SXP auf den Cluster-Knoten

Schritt 1: Wählen Sie das Symbol für drei Leitungen befindet und wählen Sie eine Work Center > TrustSec > SXP.

befindet sich in der linken oberen Ecke

Schritt 2: Klicken Sie auf +Hinzufügen, um den ISE-Aggregationsknoten als SXP-Peer zu konfigurieren.

≡ Cisco I	SE	W	ork Centers - Ti	rustSec					Q,	0	59	0
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings				
SXP Devices At SXP Mappings		SXP Devi	ces 💿							_		
		© Refresh + Ad	s 🛛 Trash 🗸 🖉	Edit Ad	ssign SXP	Rows/Page 2			Go	∑ Fite	rotal R	OWS

Schritt 3: Definieren Sie den Namen und die IP-Adresse des ISE-Aggregationsknotens, und wählen Sie Peer-Rolle als LISTENER aus. Wählen Sie die erforderlichen PSNs unter Verbundene PSNs, erforderliche SXP-Domänen, wählen Sie Aktiviert unter dem Status aus, und wählen Sie dann Kennworttyp und erforderliche Version aus.

Overview Components	TrustSec Policy Policy Sets SX	P AC
SXP Devices	SXP Devices > SXP Connection	
II SXP Mappings	<ul> <li>Upload from a CSV file</li> </ul>	
	- Add Single Device	
	Input fields marked with an asterisk (*) are req	uired.
	Name ISE Aggregation node	
	IP Address * 10.50.50.125	
	Peer Role *	
	ise01-CL1 ×	



Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI
SXP Devices		SYP Domains *			
All SXP Mappings		default ×		$\sim$	
		Status * Enabled		~	
		Password Type * CUSTOM		~	
		Password			
		Version *			
		V4		~	
		<ul> <li>Advanced Settings</li> </ul>			
			Cancel	Save	

Schritt 4: Klicken Sie auf Speichern

Anmerkung: Wiederholen Sie alle Schritte für die übrigen ISE-Knoten in jedem Cluster, um eine SXP-Verbindung zum Aggregationsknoten zu erstellen. Wiederholen Sie den gleichen Vorgang auf dem Aggregationsknoten, und wählen Sie SPEAKER als Peer-Rolle aus.

### Konfigurieren von SXP auf dem Aggregationsknoten

Schritt 1: Wählen Sie das Symbol für drei Zeilen in der oberen linken Ecke aus, und wählen Sie unter Work Center > TrustSec > Settings aus.

Schritt 2: Klicken Sie auf die Registerkarte SXP-Einstellungen

Schritt 3: Um die IP-SGT-Zuordnungen weiterzugeben, aktivieren Sie das Kontrollkästchen SXP-Bindungen für pxGrid veröffentlichen.



Schritt 4 (optional). Legen Sie unter Globales Kennwort ein Standardkennwort für SXP-Einstellungen fest.

≡ Cisco IS	SE	W	/ork Centers • T	rustSec				
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings
General TrustSec Sett TrustSec Matrix Settin	lings 1gs	SXP Settings						
Work Process Setting	5	Publish SXP bindir	ngs on PxGrid 🛃 Ad	d radius map	pings into S	XP IP SGT mapping table	0	
SXP Settings		Global Passwor	ď					
ACI Settings		Global Password 	rd will be overriden password	by				

Schritt 5: Blättern Sie nach unten, und klicken Sie auf Speichern.

### Aktivieren Sie pxGrid auf dem Aggregationsknoten.

Schritt 1: Wählen Sie das Symbol für die drei Zeilen in der linken oberen Ecke aus, und wählen Sie unter Administration > System > Deployment.

Schritt 2: Wählen Sie den Knoten aus, den Sie konfigurieren möchten, und klicken Sie auf Bearbeiten.

E Cisco ISE		Administration •	System					0 🖓	0
Deployment Licensing Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup &	Restore	Admin Access	Settings	
Deployment C T O O O O O O O O O O O O O O O O O O O	Deployn	nent Node	2 S Deregator		Bole(a)	Revices	Selected	Node S	e ● ▽
	<ul> <li>Interaction</li> </ul>	N Adv	inistration, Monitoring	, Policy Service	STANDALONE	SESSION,PRO	FLER		

Schritt 3: Um pxGrid zu aktivieren, klicken Sie auf die Schaltfläche neben pxGrid.

Cisco ISE	Administration + System	୍ ୦ ହା ୧
eployment Uconsing O	ersficates Logging Maintenance Upgrade Health Checks Backup & Restore	Admin Access Settings
	Enable Session Services (0)	
	rectues have a have droug. None v 🕥	
	Enable Probing Service 🕟	
	Catation Thread Genetics WHG Services ⊘	
	Enable SXP Service ()	
	Une Institute Cogabil@hernet.0 V	
	📋 Enaltie George Admin Service 🕝	
	Costine Pressive coentry Service 🔿	
	extent O	

Schritt 4: Blättern Sie nach unten, und klicken Sie auf Speichern.

### pxGrid-automatische Genehmigung

Schritt 1: Navigieren Sie zu drei Linien-Symbol in der oberen linken Ecke, und wählen Sie Administration > pxGrid Services > Settings aus.

**Schritt 2:** Standardmäßig genehmigt die ISE die Verbindungsanforderungen neuer pxGrid-Clients nicht automatisch pxGrid. Daher müssen Sie diese Einstellung aktivieren, indem Sie das Kontrollkästchen **Neue zertifikatbasierte Konten automatisch genehmigen**.



Schritt 3: Klicken Sie auf Speichern

#### TrustSec-Einstellungen für Netzwerkgeräte

Damit die Cisco ISE Anforderungen von TrustSec-fähigen Geräten verarbeiten kann, müssen diese TrustSec-fähigen Geräte in der Cisco ISE definiert werden.

Schritt 1: Navigieren Sie zu den drei Zeilen in der linken oberen Ecke, und wählen Sie unter Administration > Network Resources > Network Devices (Verwaltung > Netzwerkressourcen > Netzwerkgeräte) aus. Schritt 2: Klicken Sie auf +Hinzufügen.



Schritt 3: Geben Sie die erforderlichen Informationen im Abschnitt Netzwerkgeräte und in den RADIUS-Authentifizierungseinstellungen ein.

Schritt 4: Aktivieren Sie das Kontrollkästchen Erweiterte TrustSec-Einstellungen, um ein TrustSecfähiges Gerät zu konfigurieren.



Schritt 5: Klicken Sie auf das Kontrollkästchen Geräte-ID für die TrustSec-Identifizierung verwenden, um den im Abschnitt Netzwerkgeräte aufgeführten Gerätenamen automatisch auszufüllen. Geben Sie ein Kennwort in das Feld Kennwort ein.

Cisco ISE		Administration •	Network Re	esources
Network Devices	Network Device Groups	Network Device P	Profiles 8	External RADIUS Servers
Network Devices	🗹 🗸 Adv	anced TrustSec S	ettings	
Default Device				
Device Security Settings	V De Use De Identifi	vice Authenticatio vice ID for TrustSec cation	n Settings	
	Device	ld	SW1	
	1.000			
	- P855	word	Show	

**Anmerkung:** Die ID und das Kennwort müssen mit dem Befehl "cts login id <ID> password <PW>" übereinstimmen, der später auf dem Switch konfiguriert wird.

Schritt 6: Aktivieren Sie das Kontrollkästchen Konfigurationsänderungen an Gerät senden, damit ISE TrustSec CoA-Benachrichtigungen an das Gerät senden kann.

Cisco ISE		Administration - Network	Resources		
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Ser	vers RADIUS Server Sequences	More >
Network Devices					
Default Device	V Tru	stSec Notifications and U	pdates		
rvice Security Settings			1		
	* Down	ricad environment data every	Days 👻		
			1		
	* Down	rioad peer authorization policy every	Days 🐱		
			1		
	* Real	thertication every	Days 🛩 🕢		
			,		
	* Dow	ricad SGACL lists every	Days V		
	Other 1	hustSec devices to trust this device			
	Send o	onfiguration changes to device	Using O Co	- 0 cu	

Schritt 7. Aktivieren Sie das Kontrollkästchen Dieses Gerät bei der Bereitstellung von Security Group Tag Mapping Updates einschließen.

Schritt 8: Um ISE die Konfiguration des Netzwerkgeräts bearbeiten zu lassen, geben Sie die Benutzeranmeldeinformationen in die Felder EXEC Mode Username (Benutzername für den EXEC-Modus) und EXEC Mode Password (Kennwort für den EXEC-Modus) ein. Geben Sie optional das enable-Kennwort im Feld Enable Mode Password (Aktivierungsmodus-Kennwort aktivieren) ein.

Anmerkung: Wiederholen Sie die Schritte für alle anderen NADs, die Teil der TrustSec-Domäne sein sollen.

#### Autorisierung von Netzwerkgeräten

Schritt 1: Wählen Sie das Symbol für drei Zeilen in der oberen linken Ecke aus, und wählen Sie unter Work Center > TrustSec > TrustSec Policy aus.

Schritt 2: Klicken Sie im linken Teilfenster auf Netzwerkgeräteautorisierung.

	mana warmana - maanaraa			-	
Overview Components	TrustSec Policy Policy Sets SNP ACI Troubleshoot Reports	Settings			
	Network Device Authorization				
Watrices List	Define the Network Devine Authorization Photo In Jestimen 52% to return devines. Dran and de	no cars to channe the	a contar		
Marriers List Matrix Source Tree	Define the Network Device Authorization Policy by assigning 50% to network devices. Drag and dh	top rules to change the lac_Devices	e order. East ~		

Schritt 3: Verwenden Sie rechts das Dropdown-Menü neben Bearbeiten und Neue Zeile einfügen oben, um eine neue NDA-Regel zu erstellen.



Schritt 4: Definieren Sie einen Regelnamen, Bedingungen, und wählen Sie in der Dropdown-Liste unter Sicherheitsgruppen das entsprechende SGT aus.

Schritt 5: Klicken Sie ganz rechts auf Fertig.

Cisco ISE			Work Center	s • TrustSec		Q,	۲	98	0
Overview Com	ponents	TrustSec Policy	Policy Sets SX	P ACI Troublesho	ot Reports Settings				
Egress Policy Matrices List	v	Network D	evice Authorization Polic	Drization	devices. Drag and drop rules to chang	e the order.			
Source Tree		Rule	Name	Conditions	Security Group				
Destination Tree		🗄 🖬 🗠 NDAG		DEVICE Device Type equals to	v ter further, beien	V Done			
Network Device Authorias	6140	Deh	ut Rule III	no rules defined or no match	then TrustSec_Devices	60 ×			

Schritt 6: Blättern Sie nach unten, und klicken Sie auf Speichern.

#### SGT

Schritt 1: Wählen Sie das Symbol für drei Zeilen in der oberen linken Ecke aus, und wählen Sie unter Work Centers > TrustSec > Components.

Schritt 2: Erweitern Sie im linken Teilfenster die Option Sicherheitsgruppen.

Schritt 3: Klicken Sie auf +Hinzufügen, um ein neues SGT zu erstellen.



Schritt 4: Geben Sie den Namen ein, und wählen Sie ein Symbol in den entsprechenden Feldern.

≡ Cisco	ISE		Work Cen	ters • Tru	stSec	
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoo
Security Groups		Security Groups List	New Security Group			
IP SGT Static Mapp Security Group ACL	sing La	Security Groups	ŝ			
Network Devices		* Name				
Trustsec Servers	>	Cluster1_Endpo	ints			
		* lcon				
		⊜ ♀ ▲ 1	<b>a</b> • 0			
		A 🗆 🖴 🗷	> # 0			
		9 0 8 <b>n</b>	0 4 5			

Schritt 5: Geben Sie optional eine Beschreibung ein, und geben Sie einen Tag-Wert ein.

Anmerkung: Um einen Tag-Wert manuell eingeben zu können, navigieren Sie zu Work Centers > TrustSec > Settings > General TrustSec Settings, und wählen Sie die Option User Muss SGT Number Manually unter Security Group Tag Numbering (Sicherheitsgruppen-Tag-Nummerierung) eingeben.

Schritt 6: Blättern Sie nach unten, und klicken Sie auf Senden.

Anmerkung: Wiederholen Sie diese Schritte für alle erforderlichen SGTs.

#### Autorisierungsrichtlinie

Schritt 1: Wählen Sie das Symbol für drei Zeilen in der oberen linken Ecke aus, und wählen Sie unter Richtlinien > Richtliniensätze aus.

Schritt 2: Wählen Sie den entsprechenden Richtliniensatz aus.

Schritt 3: Erweitern Sie im Richtliniensatz die Autorisierungsrichtlinie.

E Cisco ISE		Policy - Policy S	465		9.0 20 4
Policy Sets-+ Wired Access				Reset Policyte	te Hitcourite
Status Policy Set Name	Description	Conditions		Allowed Proto	cuis / Server Sequence - Hits
Q Seat					
Wheel Access		***	EVICE Owners Pyper EQUALS At Davies specifications autor AAS-Port Pyper EQUALS Education	Default Netw	ork Access 😅 🔆 + 🔹
> Authentication Policy (2)					
> Authorization Policy - Local Except	tions				
> Authorization Policy - Global Excep	ptiona				
> Authorization Policy - Global Excel > Authorization Policy (1)	ptions				
> Autorization Policy - Great Even > Autorization Policy (0)	Sie auf	Đ <sub>um e</sub>	ine <b>Autorisie</b> r	ungsrichtlin	<b>ie</b> zu erstell
Autorization Policy (1)	Sie auf	Đ <sub>um e</sub>	ine <b>Autorisie</b> r	ungsrichtlin	<b>ie</b> zu erstell
Authorization Policy - Global Exer Authorization Policy (1)	Sie auf	Đ um e	ine <b>Autorisier</b>	ungsrichtlin	<b>ie</b> zu erstell

Schritt 5: Definieren Sie den erforderlichen Regelnamen, die Bedingungen und Profile, und wählen Sie in der Dropdown-Liste unter Sicherheitsgruppen das entsprechende SGT aus.

~ Authorization Policy (1)				
		Results		
Status Rule Name	Conditions	Profiles	Security Groups	Hits Actions
Q Seech				
Delte-Pallay	() Windows, 802.1X	PermitAccess ×	v + Ouster1,Endpoirm 🗠 v	+ 0

Schritt 6: Klicken Sie auf Speichern.

### Aktivieren von ERS auf ISE Aggregation Node (optional)

Der External RESTful API Service (ERS) ist eine API, die von der WSA nach Gruppeninformationen abgefragt werden kann. Der ERS-Service ist auf der ISE standardmäßig deaktiviert. Nach der Aktivierung können Clients die API abfragen, wenn sie sich als Mitglieder der **ERS Admin-**Gruppe auf dem ISE-Knoten authentifizieren. Um den Service auf der ISE zu aktivieren und der richtigen Gruppe ein Konto hinzuzufügen, gehen Sie wie folgt vor:

Schritt 1: Wählen Sie das Symbol für drei Zeilen in der oberen linken Ecke aus, und wählen Sie unter Administration > System > Settings aus.

Schritt 2: Klicken Sie im linken Teilfenster auf ERS Settings.

E Cisco ISE			A	dministration • S	ystem			Q	0 50 0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Client Provisioning FIPS Mode Security Settings	Í	ERS S	Settings						
Alarm Settings		✓ Genera	4						
Posture		External RE The ERS se An ISE Adm	STM Services (D rvice is disabled t iiristrator with the	l5) is a REST API based y default. "ERS-Admin" or "ERS	on HTTPS over pr -Operator® group	rt 9060. assignment is required to r	use the API.		
Profiling		For more in https://10.5	donmation, please 0 50 125 9060/ers	visit the ERS SDK page lydk	at:				
Protocols									
Endpoint Scripts	$\rightarrow$	✓ ERS Se	stting for Adr	ninistration Node	,				
Proxy		O Enable	DIS forhead Write						
SMTP Server		O DeadAr	045						
SMS Gateway									
System Time									
ERS Settings		✓ CSRF C	Check						

Schritt 3: Wählen Sie die Option ERS für Lese-/Schreibzugriff aktivieren aus.

Schritt 4: Klicken Sie auf Speichern und bestätigen Sie mit OK.

#### Benutzer zur ESR-Admin-Gruppe hinzufügen (optional)

Schritt 1: Wählen Sie das Symbol für drei Zeilen in der linken oberen Ecke aus, und wählen Sie Administration > System > Admin Access (Verwaltung > System > Administratorzugriff) aus.

Schritt 2: Erweitern Sie im linken Teilfenster die Option Administratoren und klicken Sie auf Admin Users.

Schritt 3: Klicken Sie auf +Hinzufügen und wählen Sie Admin User aus dem Dropdown-Menü aus.

≡ Cisco I	SE		Administration - System						Q	0 73	0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & I	Restore	Admin Access	Settings	
Authentication		Admir	histrators	s							
Authorization	>								Selected 0	) Total 1 🦪	0
Administrators	~	0 ton -	- Add 🛞 o	hange Status	0	uplicate				AL Y	V
Admin Users		-									
Admin Groups			Create an Admir	n User	Description	First Name	Last Name	Email Add	Iress Admin Gr	oups	
			Select from Net	work Access Users	> Default Admin	User			Super Adv	nin	
Settings	>										

Schritt 4: Geben Sie in die entsprechenden Felder einen Benutzernamen und ein Kennwort ein.

I Cisco IS	ε	Administration - System						Q.	0 20 0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Administrators List	> ====						
Authorization	>	✓ Admin Us	er						
Administrators	~	"Name wS	A						
Admin Users									
Admin Groups		Status 🖬	Enabled 🛩						
		Ernal			D Include	system alarms in emails			
Settings	>	Annual III			_				
		Bust Only	~						
		Inactive account	t never disable	•					
		~ Password	đ						
		* Password			G	)			
		* Re-Enter Par	meord		0	)			

Schritt 5: Wählen Sie im Feld Admin Groups (Admin-Gruppen) aus dem Dropdown-Menü die Option ERS Admin (ERS-Administrator) aus.

E Cisco I	SE Administration - System			Q,	6 58 e				
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		First Name							
Authorization	>	Last Name							
Administrators	~								
Admin Usors		V Account	Ontions						
Admin Groups		Description					*		
Settings	>								
		<ul> <li>Admin</li> <li>∃</li> </ul>	Groups ERS Admin		× +				
								Save	Reset

Schritt 6: Klicken Sie auf Speichern.

# Sichere Web-Appliance-Konfiguration

#### Stammzertifikat

Wenn im Integrationsdesign eine interne Zertifizierungsstelle als Vertrauensquelle für die Verbindung zwischen der WSA und der ISE verwendet wird, muss dieses Stammzertifikat auf beiden Appliances installiert werden.

Schritt 1: Navigieren Sie zu Network > Certificate Management und klicken Sie auf Manage Trusted Root Certificates (Vertrauenswürdige Stammzertifikate verwalten), um ein Zertifizierungsstellenzertifikat hinzuzufügen.

accordy accredes	THEORY A.	ary svern married actors	
sued By Domains	Status Time	Remaining Expiration	Date Del
e: Disabled			
			Edit Settie
e: Disabled			
			Edit Settie
Last Update		Current Version	New Update
Success - Thu Jun 30 1	5:32:47 2022	2.1	Not Available
Success - Wed May 11	21/04/06 2022	1.3	Not Available
			Update N
	sued By Domains e: Disabled e: Disabled Last Update Success - Thu Jun 30 1 Success - Wed May 11	sued By Domains Status Time i et: Disabled et: Disabled Last Update Success - Thu Jun 30 15:32:47 2022 Success - Wed May 11 21:04:06 2022	sued By Domains Status Time Remaining Expiration           Bitsbled         Expiration           et:         Disabled           Expiration         Expiration           Expiration         Expiration           et:         Disabled           Expiration         Expiration           Expiration         Expiration

Schritt 2: Klicken Sie auf Importieren.

I	Custom Trusted Root Certificates
I	Importue
	Trusted root certificates are used to determine whether WTIPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Schritt 3: Klicken Sie auf Choose File (Datei auswählen), um die generierte Root CA zu suchen, und klicken Sie auf Submit (Senden).

Schritt 4: Klicken Sie erneut auf Senden.

Schritt 5: Klicken Sie in der rechten oberen Ecke auf Änderungen bestätigen.



Schritt 6: Klicken Sie erneut auf Änderungen bestätigen.

#### pxGrid-Zertifikat

In der WSA wird die Erstellung des Schlüsselpaars und des Zertifikats zur Verwendung durch pxGrid im Rahmen der ISE-Service-Konfiguration abgeschlossen.

Schritt 1: Navigieren Sie zu Netzwerk > Identity Service Engine.

Schritt 2: Klicken Sie auf Einstellungen aktivieren und bearbeiten.

Schritt 3: Klicken Sie auf Choose File (Datei auswählen), um die generierte Root-CA zu suchen, und klicken Sie auf Upload File (Datei hochladen).

Identity Services Engine	
Edit Mentily Services Engine Settings	
C Exable INE Bervice	
Primary 158 peCrist Node:	The Black Appliance will communicate will the 201 period node to support Black Appliance data subscription (inspiring updates). A primary 201 period node (server) must be configured.
	(Headmanne or (Phyl address)
	Itil peloid Node Cartificate:
	If the BB packet note excitation is signed by a Certificate Authority, confere Net the Certificate Authority is taked in the Touted Net Certificates list (see Network in Certificate Messagement) and uplace the CA-signed root antificate basins. If the certificate is self-apped, asplot: the certificate from the Sign packet Network and basins the cuplet of the Certificate basins in Automation Certificates.
	Carlifornia: Onesee File Ino the Ocean

**Anmerkung:** Eine häufige Fehlkonfiguration besteht darin, das ISE pxGrid-Zertifikat in diesem Abschnitt hochzuladen. Das Stammzertifikat der Zertifizierungsstelle muss in das Feld ISE pxGrid Node Certificate hochgeladen werden.

Schritt 4: Wählen Sie im Abschnitt Web Appliance Client Certificate die Option Generated Certificate and Key (Generiertes Zertifikat und Schlüssel verwenden) aus.

Web Appliance Client Certificate:	In secure communication between the Web Appliance and the ISE perGrid servers, provide a client certificate. This may need to be uploads to be ISE perGrid node(s) configured above. O Use Uploaded Certificate and Key	ď
	Certificate: Chaose File No. Ille chosen Abland Files	
	Keyi Chonse File Also file chosen	
	Key is Encrypted	
	No certificate has been uploaded.	
	Use Generated Certificate and Key Generate New Certificate and Key	

Schritt 5: Klicken Sie auf die Schaltfläche Neues Zertifikat und neuen Schlüssel generieren, und füllen Sie die erforderlichen Zertifikatfelder aus.

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		

Schritt 6: Klicken Sie auf Zertifikatssignaturanforderung herunterladen.

Anmerkung: Es wird empfohlen, die Schaltfläche Senden auszuwählen, um die Änderungen an der ISE-Konfiguration zu bestätigen. Wenn die Sitzung vor dem Einsenden der Änderungen an einem Timeout verbleibt, können die generierten Schlüssel und Zertifikate verloren gehen, selbst wenn die CSR heruntergeladen wurde.

Schritt 7. Nachdem Sie die CSR-Anfrage mit Ihrer CA unterzeichnet haben, klicken Sie auf Choose File (Datei auswählen), um das Zertifikat zu suchen.

Web Appliance Client Certificate:	For secure communication between the Web Applier to the ISE pxGrid node(s) configured above.	ice and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded				
	O Use Uploaded Certificate and Key					
	Certificate: Choose File No file choose	en Upload Files				
	Key: Choose File No file choo	en .				
	Key is Encrypted					
	No certificate has been up	koeded.				
	Use Generated Certificate and Key	Generate New Certificate and Key				
	Common name: wsa.security/ab.net					
	Organization: Osco					
	Coganizational Unit: Security					
	Emiration Date: May 10 19:19:26 203	N GHT				
	Basic Constraints: Not Critical					
	Download Certificate   Download Certificate Signing Request					
	Signed Certificate:					
	To use a signed certificate, first download the link above. Submit the request to a cert receive the signed certificate, upload it usin	a certificate signing request using blicate authority, and when you g the field below.				
	Certificate: Choose File No file chosen	Upland File				

Schritt 8: Klicken Sie auf Datei hochladen.

Schritt 9. Senden und Übernehmen.

### Aktivieren Sie SXP und ERS auf einer sicheren Web-Appliance

Schritt 1: Klicken Sie auf die Schaltflächen Aktivieren für SXP und ERS.



Schritt 2: Geben Sie im Feld ERS Administrator Credentials (Benutzerdaten für ERS-Administrator) die Benutzerinformationen ein, die für die ISE konfiguriert wurden.

Schritt 3: Aktivieren Sie das Kontrollkästchen Servername identisch mit ISE pxGrid Node, um die zuvor konfigurierten Informationen zu erben. Geben Sie andernfalls die erforderlichen Informationen dort ein.

C 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 re	umber specified for ERS in 1SE)

Schritt 4: Senden und Übernehmen.

### Identifizierungsprofil

Um Sicherheitsgruppentags oder ISE-Gruppeninformationen in den WSA-Richtlinien zu verwenden, muss zunächst ein Identifizierungsprofil erstellt werden, das ISE als Mittel zur transparenten Identifizierung von Benutzern verwendet.

Schritt 1: Navigieren Sie zu Web Security Manager > Authentication > Identification Profiles.

Schritt 2: Klicken Sie auf Identifikationsprofil hinzufügen.

Schritt 3: Geben Sie einen Namen und optional eine Beschreibung ein.

Schritt 4: Wählen Sie im Abschnitt Identifikation und Authentifizierung im Dropdown-Menü die Option Benutzer mit ISE transparent identifizieren aus.

Provent and the second second	
Enable Identification Profile	
Name: 🕐	ISE Profile (e.g. my IT Profile)
Description:	Identification profile for ISE Integration.
Insert Above:	2 (Global Profile) V
dentification Hethod	
Identification and Authentication: 🕐	Transparently identify users with ISE
Fallback to Authentication Realm or Guest Privileges: 1	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 Manager > Decryption Policies, Routing Policies and Access Policies).
erabio Definition	
within is defined by any combination of the A	ollowing options. All criteria must be met for the policy to take effect.
Define Members by Subnet:	
	Cexamples: 20.2.2.0, 20.2.2.0/24, 20.2.2.2.20, 2002;420:80:21:5, 2000;408:12-2000;408:10
Define Members by Protocol:	HTTP/HTTPS

Identification Profiles: Add Profile

Schritt 5: Senden und Übernehmen.

SGT-basierte Entschlüsselungsrichtlinie

Schritt 1: Navigieren Sie zu Websicherheits-Manager > Webrichtlinien >

#### Entschlüsselungsrichtlinien.

Schritt 2: Klicken Sie auf Policy hinzufügen.

Schritt 3: Geben Sie einen Namen und optional eine Beschreibung ein.

Schritt 4: Wählen Sie im Bereich Identifikationsprofile und Benutzer im Dropdown-Menü die Option Ein oder mehrere Identifikationsprofile auswählen.

Schritt 5: Wählen Sie im Abschnitt Identifikationsprofile im Dropdown-Menü den Namen des ISE-Identifizierungsprofils aus.

Schritt 6: Wählen Sie im Abschnitt "Autorisierte Benutzer und Gruppen" die Option Ausgewählte Gruppen und Benutzer.

Policy Hember Definition			
Membership is defined by the combination of the	following options. All criteria must be r	net for the policy to take effect.	
Identification Profiles and Users:	Select One or More Identification	ivofiles 👻	
	Identification Profile	Authorized Users and Groups	Add Identification Profile
	ISE Profile V	O All Authenticated Users	
		Selected Groups and Users ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered Guests (users falling authentication)	2
	Authentication information may not a proxy traffic, user agent information	be available at HTTPS connection tin is unavailable for decryption policie	ne. For transparent 5.
Advanced	Define additional group membership	oriteria.	

Schritt 7. Klicken Sie auf den Hyperlink neben ISE Secure Group Tags.

Schritt 8: Aktivieren Sie im Abschnitt Secure Group Tag Search (Tag-Suche für sichere Gruppen) das Kontrollkästchen rechts neben dem gewünschten SGT, und klicken Sie auf Hinzufügen.

Secure Group Tag(s) currently in	cluded in this policy.	neres a rab vala vara rue bourt are ne neres abou		
Secure Group Tag Name	SGT Number	SGT Description	Delete All	T
Ouster1_Endpoints	111	Endpoints residing in ISE Cluster-1	0	

ecure Group Tag Search			
Enter any text to search for a Se Add botton to add to this policy. Search	oure 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		Add
Secure Group Tag Name	\$37 Number	SGT Description	Select All
Production_Servers	11	Production Servers Security Group	0 .
Point_of_Sale_Systems	10	Point of Sale Security Group	0
Test Servers	13	Test Servers Security Group	0
Development_Servers	12	Development Servers Security Group	0
SYOD	15	8YOO Security Group	0
PCI_Servers	14	PCI Servers Security Group	0
Guests	6	Guest Security Group	0
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	
Employees	4	Employee Security Group	

Schritt 9. Klicken Sie auf Fertig, um zurückzukehren.

Schritt 10. Senden und Übernehmen.

### Switch-Konfiguration

#### 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
```

# Überprüfung

SGT-Zuweisung von der ISE zum Endpunkt.

Hier sehen Sie einen Endpunkt aus ISE-Cluster 1, dem nach erfolgreicher Authentifizierung und Autorisierung ein SGT zugewiesen wurde:



Hier sehen Sie einen Endpunkt aus ISE-Cluster 2, dem nach erfolgreicher Authentifizierung und Autorisierung ein SGT zugewiesen wurde:

	v	Marriely.	Desperies D	Delpare Polite	Automation Paricy	Autorization Pulloy	Autorization Profiles	PARTS V	Security Group	lar-ser
AFK 20210344121		lose the contract.	141010	Mount Res.	We define the $0$ -	We all the set $t \in \mathbb{D}_+$	Periodicioni	10.00.00.12	Owned, Desires	1011-012

#### SXP-Zuordnungen

Da die SXP-Kommunikation zwischen den ISE-Knoten des Clusters und dem ISE-Aggregationsknoten aktiviert ist, werden diese SGT-IP-Zuordnungen von der ISE-Aggregation über SXP erfasst:

III Olece 155	Work Centers - TrustSec					A Trabana Mar	9 0 0 P
Overview Components	Trustlec Policy P	hicyden <b>99</b> AD	Toubleshoot	Reports Settings			
17 Invian III 187 Magainge	All SXP Map	ppings o					
					Sector 4		
	() Referen - Aust (1971	Jonais Itter - Marsage DIP Donais	trans.				V Aller V
	() faiture Aust (1071) 19 Address	Sonan ther - Marage SVP Botant	trace	named From	Learned By	SNP Junais	V rate -
	C Indexes And Cold ( 19 Address 19-19-19-19-19	Balan Star Ball Tradim, Jacob (1991)	we b	named From	Learned By	MP bonan	Viter - PSNs involved Int-120
	C Rabus Aus Lab (	Martin Marcal (27 Datas) MAT Pattier, Swater (2002) Pattier, Jewan (2002)	trees tree to	aarned From 1 56 50 1 (1 , 10 , 56 , 56 ) 1 56 50 1 (2 , 10 , 56 , 56 )	Learned By Ser	BP Jonain Mind Mind	Viter - PSNs booked to - up
	Contract Acre (2011)     Contract Acre (2011)     Contract Acre (2011)     Contract Acres (	Series for Series 107 (sear Ser Series Jeven 10000 Series Jeven 10000 Dame (Jedgein (2000)	Ne L	100 00 10 00 00 00 00 00 00 00 00 00 00	Learned By Sci Sci Sci	SAP Domain colorad colorad colorad	V Aue + PDIs Involved 10 + 100 10 + 100 10 + 100

Diese SXP-Zuordnungen verschiedener ISE-Cluster werden dann über pxGrid über den ISE-Aggregationsknoten an die WSA gesendet:



#### SGT-basierte Richtliniendurchsetzung

Hier sehen Sie die verschiedenen Endpunkte, die mit den jeweiligen Richtlinien übereinstimmen, und der Datenverkehr wird basierend auf ihrem SGT blockiert:

Endpunkt, der zum ISE-Cluster 1 gehört



#### 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 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 (GNT +02:00) +	Website (mont)	Display All Details	Disposition	Bandwidth	User / Client IP
54 Jul 2022 54 28 57	Maau/fibic.com/s42/favicer.ice content mitte das.com/com/ Black URLs CL1 DESTRUCTION IP DETUNES: Decoysteen Relice: "ISE_Out Malware Analytics File Verdict: -	er1", WBRS: No Score,	Block - URL CH	ce	ixexup_10.50.30.121_xgf111_10.50.30.12 (2dem0fed by 158) 10.50.50.12

#### Endpunkt, der zum ISE-Cluster 2 gehört

Based ( http:	f on your organization's ac //www.facebook.com/ ) h	cess policies, ar as been blocked	ccess to this	s web site	
If you codes	have questions, please co shown below.	untact your organ	nization's ne	etwork adminit	strator and provide the
Date: Usem Souro URL: ( Categ Reaso Notific	Thu, 14 Jul 2022 14:23:58 ame: isesxp_10.50.50.122 e IP: 10.50.50.13 GET https://www.facebook ory: Block URLs CL2 in: UNKNOWN ation: BLOCK_DEST	CEST _sgt222_10.50. .com/	50.13		
Results					
Displaying 1 - 2 of 2 its	ma.	Disalar Al Datala	Constant of	Rest 182	iters ( Classif R)
14 Jul 2022 14:23:58	Here Version Academic com 443/favior Contrast Proto Unit Correctorie Block Villa CL2 Destructure Destyption Policy 1285_Clust Malware Analytics Pile Verdict: .	nice net2", w8K3: No Score,	Block - URL Cat	CB	isessp_10.50.30.132_sp(222_10.50.50.1 (24e65640 br 155 10.50.50.1)

### Zugehörige Informationen

Integrationsanleitung für Web Security Appliance und Identity Service Engine

- Konfigurieren der WSA-Integration mit der ISE für TrustSec-basierte Services
- Administratoranleitung für Cisco Identity Services Engine, Version 3.1
- Benutzerhandbuch für AsyncOS 14.5 für Cisco Secure Web Appliance