# Integrazione di più cluster ISE con policy basate su Secure Web Appliance for TrustSec

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Limitazioni Esempio di rete Configurazione Configurazione di ISE Attiva SXP Configurare SXP nei nodi del cluster Configurare SXP sul nodo di aggregazione Abilita pxGrid sul nodo di aggregazione Approvazione automatica pxGrid Impostazioni TrustSec dispositivi di rete Autorizzazione dispositivo di rete SGT Criteri di autorizzazione Abilitazione di ERS su ISE Aggregation Node (opzionale) Aggiungi utente al gruppo Amministratore ESR (facoltativo) Configurazione sicura di Web Appliance Certificato pxGrid Abilitare SXP e ERS su Secure Web Appliance Profilo di identificazione Criterio di decrittografia basato su SGT Configurazione degli switch AAA **TrustSec** Verifica Informazioni correlate

# Introduzione

In questo documento viene descritta la procedura per inviare le informazioni SGT (Security Group Tag) da più distribuzioni ISE a una singola appliance Cisco Secure Web Appliance (Formally Web Security Appliance WSA) tramite pxGrid per trarre vantaggio dai criteri di accesso Web basati su SGT in una distribuzione TrustSec.

Nelle versioni precedenti alla 14.5, Secure Web Appliance può essere integrata solo con un singolo cluster ISE per policy di identità basate su SGT. Con l'introduzione di questa nuova

versione, Secure Web Appliance può ora interagire con le informazioni di più cluster ISE con un nodo ISE separato che le aggrega. Questo ci offre grandi vantaggi e ci permette di esportare i dati degli utenti da diversi cluster ISE, oltre alla libertà di controllare il punto di uscita che un utente può utilizzare senza la necessità di un'integrazione 1:1.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- Secure Web Appliance
- protocollo RADIUS
- TrustSec
- pxGrid

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Web Appliance 14.5
- ISE versione 3.1 P3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Limitazioni

- 1. Tutti i cluster ISE devono mantenere mappature uniformi per le SGT.
- 2. ISE Aggregation Node deve avere il nome/numero SGTs degli altri cluster ISE.
- 3. Secure Web Appliance è in grado di identificare i criteri (accesso/decrittografia/routing) solo in base al tag SGT e non al nome utente o di gruppo
- 4. Reporting and Tracking è basato su SGT.
- 5. I parametri di dimensionamento di ISE/Secure Web Appliance esistenti continuano ad essere applicati per questa funzione.

# Esempio di rete



Processo:

1. Quando l'utente finale si connette alla rete, riceve un SGT basato sulle policy di autorizzazione in ISE.

2. I diversi cluster ISE inviano quindi queste informazioni SGT sotto forma di mapping SGT-IP a ISE Aggregation Node tramite SXP.

3. ISE Aggregation Node riceve queste informazioni e le condivide con un'unica appliance Web sicura tramite pxGrid.

4. Secure Web Appliance utilizza le informazioni SGT apprese per fornire l'accesso agli utenti in base ai criteri di accesso Web.

# Configurazione

# Configurazione di ISE

Attiva SXP

Passaggio 1. Selezionare l'icona delle tre linee Amministrazione > Sistema > Distribuzione. nell'angolo superiore sinistro e selezionare

Passaggio 2. Selezionare il nodo da configurare e fare clic su Modifica.

E Cisco ISE		Administration - System				0.0			0	
Deployment Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Set	tings	
Deployment < 10 → 24 Deployment	• De	ploymer	nt Nodes				Selected 1 Total	10	0	
35- PAN Failover		Hostname	Personas     Administra	ton, Monitoring, Policy	Role(s)	Services	R	lode St	atus	

#### Passaggio 3. Per abilitare SXP, selezionare la casella Enable SXP Service

E Cisco ISE	Administration - System		. Q	0530
Deployment Licensi	ng Certificates Logging Maintenance Upgrade Health Checks	Backup & Restore	Admin Access	Settings
	Enable Session Services ()			
	Include Node in Node Group None	~ o		
	Enable Profiling Service ()			
	Enable Threat Centric NAC Service ()			
	Enable SXP Service ()			
	Use Interface GigabitEthemet 0	~		

Passaggio 4. Scorrere verso il basso e fare clic su Salva

**Nota:** Ripetere tutti i passaggi per gli altri nodi ISE in ciascun cluster, incluso il nodo di aggregazione.

## Configurare SXP nei nodi del cluster

**Passaggio 1.** Selezionare l'icona a tre righe situato nell'angolo superiore sinistro e selezionare **Area di produzione > TrustSec > SXP.** 

Passaggio 2. Fare clic su +Add per configurare il nodo di aggregazione ISE come peer SXP.

Cisco ISE	Work Centers - TrustSec		
Overview Components	TrustSec Policy Policy Sets SXP ACI Troublesh	oot Reports	Settings
SXP Devices All SXP Mappings	SXP Devices o		
	RowsPage	2 V K C 1	/1 >>  2 Total Rows

Passaggio 3. Definire il nome e l'indirizzo IP del nodo di aggregazione ISE, selezionare il ruolo

peer come LISTENER. Selezionare i nomi dei nomi dei nomi dei nomi dei nomi dei domini di rete richiesti in PSN connessi, Domini SXP obbligatori, selezionare Abilitato in stato, quindi selezionare Tipo di password e Versione richiesta.

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



Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI
SXP Devices		SYD Domaine *			
All SXP Mappings		default ×		$\sim$	
		Status *			
		Enabled		~	
		Password Type *			
		CUSTOM			
		Password			
		Version *			
		<ul> <li>Advanced Settings</li> </ul>	1		
			Cancel	Save	

Passaggio 4. Fare clic su Salva

Nota: Ripetere tutti i passaggi per gli altri nodi ISE in ogni cluster per creare una connessione SXP al nodo di aggregazione. Ripetere lo stesso processo sul nodo di aggregazione e selezionare SPEAKER come ruolo peer.

## Configurare SXP sul nodo di aggregazione

Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere Centro di lavoro > TrustSec > Impostazioni

Passaggio 2. Fare clic sulla scheda Impostazioni SXP

**Passaggio 3.** Per propagare i mapping IP-SGT, selezionare la casella di controllo **Pubblica associazioni SXP su pxGrid**.



Passaggio 4 (facoltativo). Definire una password predefinita per le impostazioni SXP in Password globale

≡ Cisco	ISE	Work Centers · TrustSec						
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings
General TrustSec	Settings	SXP Settings						
Work Process Set	tings	Publish SXP bindir	ngs on PxGrid 🛃 Ad	id radius map	pings into S	OVP IP SGT mapping table	e	
SXP Settings		Global Passwor	a					
ACI Settings								
		Global Password						
		This global passwor	d will be overriden	by				
		the device specific	password					

Passaggio 5. Scorrere verso il basso e fare clic su Salva.

## Abilita pxGrid sul nodo di aggregazione

**Passaggio 1.** Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere **Amministrazione > Sistema > Distribuzione.** 

Passaggio 2. Selezionare il nodo da configurare e fare clic su Modifica.

E Cisco ISE		Administration - System				_ · · · · · · · · · Q @			
Deployment Licensing Co	rtificates	Loggin	g Maintenanc	e Upgrade	Health Checks	Backup &	Restore	Admin Access	Settings
Deployment < 10	0	Deplo	yment No	des				Selected	1 Totel 1 🕃 🔮
> 35 Deployment		1 100	🗟 Register 🖸 S	lyncup 🔒 Deregie	last.				AI Y V
Ab Lord Landada		О н	lostname 🗠	Personas		Role(s)	Services		Node Status
			ise-agg	Administration, Monito	ing, Policy Service	STANDALONE	SESSION,PRO	FLER	

Passaggio 3. Per abilitare pxGrid, fare clic sul pulsante accanto a pxGrid.

E Cisco ISE	Administration - System	0.0500
Deployment Uccersing Coroll	icates Logging Maintenance Upgrade Health Checks Backup & Res	tore Admin Access Settings
	Enable Session Services 💿	
	Include Node in Tools Group None V	
	Evalue Profiling Service 🕟	
	🗌 Enable Thread Gardinic MHG Service 🌀	
	Enable SXP Service 💿	
	Uni ministro digabilithemat 0 V	
	🗌 Enaite George Admin Samore ⊘	
	📄 Enative Parasses identity Service 💮	
	select 🕓	

Passaggio 4. Scorrere verso il basso e fare clic su Salva.

## Approvazione automatica pxGrid

**Passaggio 1.** Passare all'icona con tre righe nell'angolo superiore sinistro e selezionare **Amministrazione > pxGrid Services > Impostazioni**.

**Passaggio 2.** Per impostazione predefinita, ISE non approva automaticamente pxGrid le richieste di connessione dei nuovi client pxGrid, pertanto è necessario abilitare questa impostazione selezionando la casella di controllo **Approva automaticamente i nuovi account basati su certificato**.



Passaggio 3. Fare clic su Salva

## Impostazioni TrustSec dispositivi di rete

Per consentire a Cisco ISE di elaborare le richieste provenienti da dispositivi abilitati per TrustSec, è necessario definire tali dispositivi in Cisco ISE.

Passaggio 1. Passare alle tre linee dell'icona nell'angolo superiore sinistro e selezionare Amministrazione > Risorse di rete > Dispositivi di rete.

Passaggio 2. Fare clic su +Aggiungi.



Passaggio 3. Immettere le informazioni richieste nella sezione Dispositivi di rete e in Impostazioni autenticazione RADIUS.

**Passaggio 4.** Selezionare la casella di controllo **Impostazioni avanzate TrustSec** per configurare un dispositivo abilitato per TrustSec.

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

**Passaggio 5.** Fare clic sulla casella di controllo **Utilizza ID dispositivo per identificazione trustSec** per popolare automaticamente il Nome dispositivo elencato nella sezione **Dispositivi di rete**. Immettere una password nel campo **Password**.



**Nota:** L'ID e la password devono corrispondere al comando "cts credentials id <ID> password <PW>" configurato successivamente sullo switch.

**Passaggio 6.** Selezionare la casella di controllo **Invia modifiche alla configurazione al dispositivo** in modo che ISE possa inviare notifiche TrustSec CoA al dispositivo.

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			1		
	* Dow	ricad environment data every	Days V		
	* Down	rioad peer authorization policy every	Days 👻		
			,		
	* Sea	thertication every	Days 🛩 🕢		
	* Dow	rioad SGACL lists every	-		
			Days •		
	Other 1	rustlec devices to trust this device			
	Send o	orfiguration changes to device	Using O CoA	) cu	

Passaggio 7. Selezionare la casella di controllo Includi il dispositivo durante la distribuzione degli aggiornamenti del mapping dei tag del gruppo di sicurezza.

Passaggio 8. Per consentire a ISE di modificare la configurazione del dispositivo di rete, immettere le credenziali utente nei campi Nome utente modalità di esecuzione e Password modalità di esecuzione. Se necessario, specificare la password di abilitazione nel campo Password modalità di abilitazione.

Nota: Ripetere i passaggi per tutti gli altri NAD che devono far parte del dominio TrustSec.

#### Autorizzazione dispositivo di rete

Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere Centro di lavoro > TrustSec > Criteri TrustSec.

Passaggio 2. Nel riquadro sinistro fare clic su Autorizzazione dispositivo di rete.

E Cisco ISE	Work Centers - TrustSec		0.0580
Overview Components	TrustSec Policy Policy Sets SVP ACI Troubleshoot Reports	Settings	
Egrass Policy ~ ~	Network Device Authorization	drop rules to change the o	unitar.
Matrix Source Tree	Default Rule If no rules defined or no munch then. Thus	thes_Devices	tet ×
Destination Tree			
Natarok Device Authorization			

Passaggio 3. A destra, utilizzare l'elenco a discesa accanto a Modifica e Inserisci nuova riga sopra

per creare una nuova regola NDA.

Cisco ISE	Work Centers - TrustSec	
Overview Components	TrustSec Policy Policy Sets SXP ACI Trust/eshoot Reports Settings	
Egress Policy ~ Metrices List	Network Device Authorization Define the Network Device Authorization Policy by assigning 50.55 to network devices. Drag and drop rules to change i	the order.
Source Tree	Default Rule IF no rules defined or no match than TrustBee, Devices	
Destination Tree		
Network Device Authorization		

Passaggio 4. Definire un Nome regola, Condizioni e selezionare il SGT appropriato dall'elenco a discesa in Gruppi di sicurezza.

Passaggio 5. Fare clic su Fine all'estrema destra.

E Cisco ISE	Work	Centers - TrustSec		0.024
Overview Components	TrustSec Policy Policy Sets	SXP ACI Troubleshoo	t 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	🗄 🖪 🗠 NDAC	F DEVICE Device Type equals to	v tes Twifer,Devices v Done	
Natarork Device Authorization	Default Rule	If in rules defined or no match	thes Trustlet_Devices Edit -	

Passaggio 6. Scorrere verso il basso e fare clic su Salva.

#### SGT

Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere Centri di lavoro > TrustSec > Componenti.

Passaggio 2. Nel riquadro sinistro espandere Gruppi di sicurezza.

Passaggio 3. Fare clic su +Aggiungi per creare un nuovo SGT.

E Cisco ISE	Work Centers - TrustSec	0.0 58 0
Overview Components	TrustSec Policy Policy Sets SVP ACI Trushenhost Reports Settings	
Security Groups	Security Orauge	
IP 967 Static Mapping	Security Groups	
Security Droup ACLs	For Palcy Equal prior Administration + Stations - Backup & Restore - Palcy Equal Page	
Nation's Devices		Selected to Total 18
Trainer Berners	Z En + Ant ≥ Input ≥ Expert × 8 Track × © Funk ⊘ Yorky Deploy	м ~

Passaggio 4. Inserire il nome e scegliere un'icona nei campi appropriati.

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

Passaggio 5. Se necessario, fornire una descrizione e inserire un valore di tag.

Nota: Per poter immettere manualmente un valore di tag, passare a Centri di lavoro > TrustSec > Impostazioni > Impostazioni generali TrustSec e selezionare l'opzione User Must Enter SGT Number Manually in Security Group Tag Numbering.

Passaggio 6. Scorrere verso il basso e fare clic su Submit (Invia)

Nota: Ripetere questi passaggi per tutte le SGT necessarie.

## Criteri di autorizzazione

Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere Criterio > Set di criteri.

Passaggio 2. Selezionare il set di criteri appropriato.

Passaggio 3. Nel set di criteri espandere i criteri di autorizzazione.

II Cisco ISE	Policy = I	olicy	Sets		9.0	(3 O
Policy Sets Wired Access				Reset	Reset Policyset Hiscourts	Sava
Status Policy Set Name Description	Condition				Allowed Protocols / Server Sequent	a 18%
Q Seed						
Wind Access	**0	9	DEVICE Onvice Pype EQUALS AT Device PyperHilarholies		Default Network Access	
			Radio MS-Pot Type EQALS Ethernet			
> Authentication Policy (2)						
> Authorization Policy - Local Exceptions						
> Authorization Policy - Global Exceptions						
> Authorization Policy (1)						



per creare un criterio di autorizzazione.

<ul> <li>Authorization Policy (1)</li> </ul>					
		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

**Passaggio 5.** Definire il **Nome regola, la Condizione o le Condizioni** e i **Profili** richiesti, quindi selezionare il valore SGT appropriato dall'elenco a discesa in **Gruppi di sicurezza**.

C Roma Rela Nama Conditions Profiles Security Security		
Contract in the second contract	Hits	Actions
Q fearth		

Passaggio 6. Fare clic su Salva.

Passaggio 4. Fare clic sul pulsante

## Abilitazione di ERS su ISE Aggregation Node (opzionale)

ERS (External RESTful API Service) è un'API che può essere richiesta da WSA per ottenere informazioni sui gruppi. Il servizio ERS è disabilitato per impostazione predefinita su ISE. Una volta abilitata, i client possono eseguire query sull'API se eseguono l'autenticazione come membri del gruppo **ERS Admin** sul nodo ISE. Per abilitare il servizio su ISE e aggiungere un account al gruppo corretto, attenersi alla seguente procedura:

Passaggio 1. Selezionare l'icona a tre linee situata nell'angolo superiore sinistro e scegliere Amministrazione > Sistema > Impostazioni.

Passaggio 2. Nel riquadro sinistro fare clic su Impostazioni ERS.

≡ Cisco I	SE		A	dministration - S	ystem			Q	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	Ы						
Posture		External PE The EVS so An ISE Adr	STM Services (D rivice is disabled t rivistrator with the	IS) is a REST API based ly default. * ERS-Admin* or * ERS	-Operator <sup>a</sup> group	ort 9060. assignment is required to o	use the API.		
Profiling		For more in https://10.5	dormation, please i0 50 125 9060/ers	visit the ERS SDK page /sdk	at:				
Protocols									
Endpoint Scripts	>	✓ ERS Se	etting for Adr	ninistration Node	,				
Proxy		O Enable	Did forleas/Write						
MTP Server		O Daubh	045						
IMS Gateway									
lystem Time									
ERS Settings		CSRF (     CSR	Check						

Passaggio 3. Selezionare l'opzione Abilita ERS per lettura/scrittura.

Passaggio 4. Fare clic su Salva e confermare con OK.

## Aggiungi utente al gruppo Amministratore ESR (facoltativo)

Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e selezionare Amministrazione > Sistema > Accesso amministratore

Passaggio 2. Nel riquadro sinistro espandere Administrators e fare clic su Admin Users.

Passaggio 3. Fare clic su +Add e selezionare Admin User dall'elenco a discesa.

≡ Cisco IS	SE		Ad	dministration - S	ystem				Q	0 53	0
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Re	store Admir	n Access	Settings	5
Authentication		Admir	histrator	S							
Authorization	>								Selected 0	Total 1 🧭	۲
Administrators	~	0 ton -	- Add 🛞 C	hange Status	Delete 0 0	uplicate					Y
Admin Users											
Admin Groups			Create an Admir	User	Description	First Name	Last Name	Email Address	Admin Gro	ups	
			Select from Net	work Access Users	> Default Admir	User			Super Admi	n	
Settings	>										

Passaggio 4. Inserire un nome utente e una password nei campi appropriati.

😄 Cisco 🗄	35		Q.	0 28 0				
Deployment	Licensing	Certificates Logo	ing Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
Authentication		Administrators List 3 with						
Authorization	)	✓ Admin User						
Administrators	~	"Name wSA						
Admin Users								
Admin Groups		Email Email	ed ¥	C Include and	ten atens is enais			
Settings	>	External Dela Dela Dela Dela Dela Dela Dela De	r disabled	0				
		✓ Password *Password		0				
		* Ro-Enter Passwort		0				

Passaggio 5. Nel campo Gruppi amministrativi, utilizzare l'elenco a discesa per selezionare Amministratore ERS.

E Cisco	SE		Administration - System						Administration - System				Q	0 52 O
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings					
Authentication		First Name												
Authorization	>	Last Name												
Administrators	~													
Admin Usors		× Account	ontines											
Admin Groups		Description					*							
Settings	>													
		✓ Admin 	Groups ERS Admin		v +									
								Save	Reset					

Passaggio 6. Fare clic su Salva.

# Configurazione sicura di Web Appliance

#### Certificato radice

Se il progetto di integrazione utilizza un'autorità di certificazione interna come radice di attendibilità per la connessione tra WSA e ISE, questo certificato radice deve essere installato su entrambi gli accessori.

Passaggio 1. Passare a Rete > Gestione certificati e fare clic su Gestisci certificati radice attendibili per aggiungere un certificato CA.

> \$100V Reporting	Web Security Manager	Constant Constant				
Reporting	Web Security Manager	Examples Examples				
		security services	Network	System Adr	inistration	
ertificate M	anagement					
	anagement					
opliance Certificat	8					
Add Certificate						
ertificate Co	mmon Name Issue	d By Domains	Status Tir	ne Remaining	Expiration Date	Delet
biport Certificate						
leak Signature Usa	age Settings					
Res	strict Weak Signature Usage:	Disabled				
						Edit Settings
ertificate FQDN Va	didation Settings					
Certifi	cate FQDN Validation Usage:	Disabled				
						Edit Settings
artificate Lists						
Updates						
le Type		Last Update		Curren	e Version	New Update
aco Trusted Root Ce	rtificate Bundle	Success - Thu Jun 30 5	15:32:47 2022	2.1		Not Available
aco Certificate Block	ed List	Success - Wed May 11	21:04:06 2022	1.3		Not Available
a updates in progres	ik.					Update Now
Contribution Manager	gement					
contendance mama						

#### Passaggio 2. Fare clic su Import.

Custom Trusted Rost Certificates
Import
Trusted root certificates are used to determine whether HTTPS 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.

Passaggio 3. Fare clic su Scegli file per individuare la CA radice generata e fare clic su Sottometti.

Passaggio 4. Fare nuovamente clic su Invia.

Passaggio 5. Nell'angolo superiore destro fare clic su Commit modifiche.



Passaggio 6. Fare nuovamente clic su Conferma modifiche.

## Certificato pxGrid

Nel WSA, la creazione della coppia di chiavi e del certificato per l'uso da parte di pxGrid è completata come parte della configurazione dei servizi ISE.

Passaggio 1. Passare a Rete > Identity Service Engine.

Passaggio 2. Fare clic su Abilita e modifica impostazioni.

Passaggio 3. Fare clic su Scegli file per individuare la CA radice generata e fare clic su Carica file.

Identity Services Engine	
Edit Identity Services Engine Settings	
C Enable ISE Dervice	
Primary ISE gedinid Node:	The Bild Applance will communicate with the 202 packed non-to support Bild Applance data subscription (impaing updates). A primary 202 packed node (server) must be configured.
	198 pedint Node Certificate:
	If the IBI public involvement is signed by a Certificate Authority, confirm that the Certificate Authority is based in the Trouted Root Certificate list (see Network in Certificate Menagement) and upload the CA-agreed nucl certificate bases, If the certificate is self-signed regard the certificate from the ISE public head in add bases. To concertificate certificate in routides any intermediate certificates
	Certificate Channel In the Content

**Nota:** Una configurazione errata comune consiste nel caricare il certificato ISE pxGrid in questa sezione. Il certificato CA radice deve essere caricato nel campo Certificato del nodo PxGrid ISE.

Passaggio 4. Nella sezione Certificato client Web Appliance selezionare Usa certificato e chiave generati.

Web Appliance Client Certificate:	For secure communication to the ISE petirid node(s)	in between the Web Appliance and the ISE puGrid servers, provide a client certificate. This may need to be uploaded ) configured above.
	O Use Uploaded Certif	floate and Key
	Certificate:	Chucos Fite Nus file chosen. Upload Files.
	Key:	Choose Fire Na Ne the chosen
		Key is Encrypted
		No certificate has been uploaded.
	Use Generated Cer	Generate New Certificate and Key

Passaggio 5. Fare clic sul pulsante Genera nuovo certificato e chiave e completare i campi obbligatori del certificato.

Generate Certificate an	d Key	$\times$
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		

Passaggio 6. Fare clic su Download della richiesta di firma del certificato.

**Nota:** Si consiglia di selezionare il pulsante **Submit** per eseguire il commit delle modifiche alla configurazione ISE. Se la sessione viene lasciata in timeout prima dell'invio delle modifiche, le chiavi e il certificato generati possono andare persi, anche se il CSR è stato

scaricato.

**Passaggio 7.** Dopo aver firmato il CSR con la CA, fare clic su **Choose File** per individuare il certificato.

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: Choose File No file chosen						
	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/ab.ret						
	Organization: Cisco						
	Organizational Unit: Security						
	Country: SE						
	Expiration Date: May 10 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: Choese File No file chosen Upload File						

Passaggio 8. Fare clic su Upload File.

Passaggio 9. Sottomettere e confermare.

## Abilitare SXP e ERS su Secure Web Appliance

Passaggio 1. Fare clic sui pulsanti Abilita sia per SXP che per ERS.



Passaggio 2. Nel campo Credenziali amministratore ERS, immettere le informazioni utente configurate su ISE.

**Passaggio 3.** Selezionare la casella **Nome server uguale a ISE pxGrid Node** per ereditare le informazioni configurate in precedenza. In caso contrario, immettere le informazioni richieste.

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 n	umber specified for ERS in 1SE)

#### Passaggio 4. Sottomettere e confermare.

## Profilo di identificazione

Per utilizzare le etichette dei gruppi di sicurezza o le informazioni dei gruppi ISE nelle policy WSA, è necessario prima creare un profilo di identificazione che utilizzi ISE come mezzo per identificare in modo trasparente gli utenti.

Passaggio 1. Passare a Web Security Manager > Autenticazione > Profili di identificazione.

Passaggio 2. Fare clic su Aggiungi profilo di identificazione.

Passaggio 3. Inserire un nome ed eventualmente una descrizione.

Passaggio 4. Nella sezione Identificazione e autenticazione, usare l'elenco a discesa per scegliere Identificazione trasparente degli utenti con ISE.

/ User Identification Profile Settings	
Enable Edentification Profile	
Name: 🕐	ISE Profile (e.g. my IT Profile)
Description:	Identification profile for ISE Integration.
	(Maximum allowed characters 256)
Insert Above:	2 (Globel Profile) Y
destification Mathed	
Meeting and Automation Te	The second state of the se
stenoncation and Authentication: (1)	Transparently identify users with tot
Fallback to Authentication Realm or Guest Privileges: 7	If user information is not available from the Identity Services Engine:
	Support Guest Privileges V
	Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).
ership Definition	
ership 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:	
	(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:11:5, 2000:408::1-2000:408::10
Define Members by Protocol:	HTTP/HTTPS

**Identification Profiles: Add Profile** 

Passaggio 5. Sottomettere e confermare.

Criterio di decrittografia basato su SGT

Passaggio 1. Passare a Web Security Manager > Criteri Web > Criteri di decrittografia.

Passaggio 2. Fare clic su Aggiungi criterio.

Passaggio 3. Inserire un nome ed eventualmente una descrizione.

Passaggio 4. Nella sezione Profili e utenti di identificazione, utilizzare l'elenco a discesa per scegliere Seleziona uno o più profili di identificazione.

**Passaggio 5.** Nella sezione **Profili di identificazione**, usare l'elenco a discesa per scegliere il nome del profilo di identificazione ISE.

Passaggio 6. Nella sezione Utenti e gruppi autorizzati, selezionare Gruppi e utenti selezionati.

ership is defined by the combination of the	following options. All criteria mut	it be met for the policy to take effect.
Identification Profiles and Users:	Select One or More Identifica	ition Profiles 👻
	Identification Profile	Authorized Users and Groups Add Identification I
	ISE Profile	OAl Authenticated Users     Selected Groups and Users      ISE Secure Group Tags: No     tags entered     ISE Groups: No groups     entered     Bertered
		Users: No users entered Couests (users falling authentication)
	Authentication information may proxy traffic, user agent inform	not be available at HTTPS connection time. For transparent ation is unavailable for decreption policies.
	Authentication information may proxy traffic, user agent inform	r not be available at HTTPS connection time. For transparent ation is unavailable for decryption policies.

Passaggio 7. Fare clic sul collegamento ipertestuale accanto a ISE Secure Group Tags.

Passaggio 8. Nella sezione Ricerca per tag Secure Group, selezionare la casella a destra dell'SGT desiderato e fare clic su Aggiungi.

Nathorized Secure Group Tags				
Use the search function below to a 1 Secure Group Tag(s) currently in	edd Secure Group Tags. To remove cluded in this policy.	Becure Group Tags from this policy, use the Delete optio	n.	
Secure Group Tag Name	SGT Number	SGT Description	Delete	
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	0	
and Coders		any end tenerg these enders		
4				Ŧ
			Delete	]

Secure Group Tag Search			
Enter any text to search for a Se Add button to add to this policy. Search	oure Group Tag name, number, or o	lescription. Belect one or more Secure Group Tags from th	e list and use the
0 Secure Group Tag(s) select			
Secure Group Tag Name	SGT Number	SGT Description	Select All
Production_Servers	11	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
BYOD	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	191	Endpoints residing in ISE Cluster-1	
Employees	4	Employee Security Group	
4			> //

Passaggio 9. Fare clic su Chiudi per tornare.

Passaggio 10. Sottomettere e confermare.

## Configurazione degli switch

## 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
```

# Verifica

Assegnazione SGT da ISE a endpoint.

Qui è possibile vedere un endpoint da ISE Cluster 1 a cui è stato assegnato un SGT dopo la corretta autenticazione e autorizzazione:



Qui è possibile vedere un endpoint da ISE Cluster 2 a cui è stato assegnato un SGT dopo la corretta autenticazione e autorizzazione:

	v		identify.	Ordpatric D	Delpare Polite	Advertisation Particip	Autorization Pulloy	Autorization Profiles	PARTIE V	Security Group	heres
ALC: UND DO NOT 11.		+	lose Press	141010	Manual Base	We define the $\mathbb{D}_{+}$	West Access to D.,	Participation	10.00.00.12	Over1,0-serve	1001-012

#### Mapping SXP

Poiché la comunicazione SXP è abilitata tra i nodi ISE del cluster e il nodo di aggregazione ISE, queste mappature SGT-IP vengono apprese dall'aggregazione ISE tramite SXP:

III Cieco 155	Work Centers - TrustSec					A Transaction	
Overview Components	Trustlec Policy P	No 900 million	houtieshoot	Reports Settings			
DIP Devices All DAP Requires	All SXP Ma	opings o					
	() Balance - Ann 1977	Install The Manage Diff Donald			2000/Pape 4	<u>v</u> ( <u>)</u> )	1) the first first first the second sec
	IP Address	947	ww.	Learned From	Lowrood By	507 Domain	PSNs involved
	10.00.00.010	Turbs, Jacob (2001)		101010-022-03030-0	547	anut	144-400
	10.00.00.1102	Number, Jacobs (2000)		10.00.00.122.70.00.007	547	annut	144 100
	10.00.00.10.02	Dunet_Extening (11,0005)		10.00.00.121.20.00.00.0	5.0	default.	144-920
	10.00.00.10/02	Darter1_Endpoints (20211000)		10.00.00.102.00.00.00.0	147	defect.	144-1000

Queste mappature SXP, da diversi cluster ISE, vengono quindi inviate a WSA tramite pxGrid attraverso il nodo di aggregazione ISE:



Applicazione delle policy basata su SGT

Qui è possibile vedere i diversi endpoint corrispondenti ai rispettivi criteri e il traffico viene bloccato in base al relativo SGT:

Endpoint che appartiene a ISE Cluster 1



#### This Page Cannot Be Displayed

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

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

Date: Thu, 14 Jul 2022 14:28:16 CEST 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 (GHT +02:00) +	Website (court)	Display All Details	Disposition	Bandwidth	User / Client IP
54 Jul 2022 54:28:57	Mass/Moc.asmid43/Taripaniles Content Trial and Cardionim Block URLs CL1 Destruction In - Octavity Decrystee Palicer 1158_Our Malware Analytics File Verdict -	uber1", WBAS: No Score,	Block - URL CH	ce	ieese_10.50.50.121_sgr11_10.50.50. (Demtified by 15 10.50.50.

#### Endpoint che appartiene a ISE Cluster 2

	() Notification: Policy: Destination X					+
~	$\rightarrow$	C	Ô	https://ww	w.fa	cebook.com

This	Page Cannot Be D	lisplayed									
Based ( https	Based on your organization's access policies, access to this web site ( https://www.facebook.com/ ) has been blocked.										
If you codes	have questions, please c shown below.	ontact your organ	nization's ne	etwork admini	strator and provide the						
Date: 1 Usemi Sourci URL: 0 Categi Reaso Notific	Thu, 14 Jul 2022 14:23:58 ame: isesxp_10.50.50.12 e IP: 10.50.50.13 GET https://www.facebool ory: Block URLs CL2 n: UNKNOWN ation: BLOCK_DEST	8 CEST 2_sgt222_10.50: k.com/	50.13								
selts											
ne (GMT +02:00) =	Website (count)	Display All Details	Disposition	Bandwidth	User / Clant IP						
4 34 2022 14:23:58	Https://www.facebook.com/403/favior constant Frints - URL CATEGORY: Block URLs CL2 CESTIONATION IP: -	PA.109	Block - URL Cat	08	isesup_10.50.50.122_sp(022_10.50.50.1 (2dentified by 158 00.50.50.1						

# Informazioni correlate

• Guida all'integrazione di Web Security Appliance e Identity Service Engine

- Configurazione dell'integrazione WSA con ISE per i servizi compatibili con TrustSec
- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.1
- Guida per l'utente di AsyncOS 14.5 per Cisco Secure Web Appliance