

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:

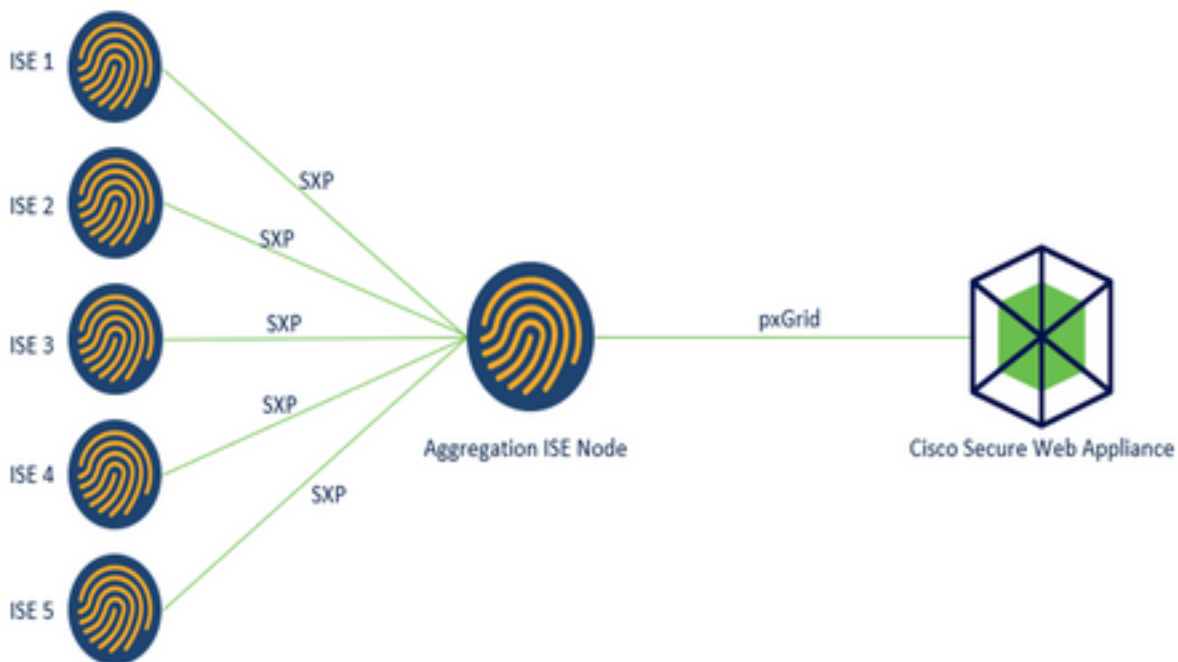
- Secure Web Appliance 14.5
- ISE versione 3.1 P3

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/decriptografia/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  nell'angolo superiore sinistro e selezionare **Amministrazione > Sistema > Distribuzione**.

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

The screenshot shows the Cisco ISE Administration - System interface. The 'Deployment' tab is active. On the left, a sidebar shows 'Deployment' and 'PAN Failover'. The main area is titled 'Deployment Nodes'. At the top right, it says 'Selected 1 Total 1'. Below this are buttons for 'Edit', 'Register', 'Syncup', and 'Deregister'. A table lists the nodes:

Hostname	Personas	Role(s)	Services	Node Status
ise01-cl1	Administration, Monitoring, Policy Service	STANDALONE	SESSION_PROFILER	✔

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

The screenshot shows the 'Enable Session Services' configuration page in Cisco ISE Administration - System. The 'Enable SXP Service' checkbox is checked and highlighted with a red box. Other options include 'Enable Profiling Service' (checked), 'Enable Threat Centric NAC Service' (unchecked), and 'Use Interface' set to 'GigabitEthernet 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.

The screenshot shows the 'SXP Devices' configuration page in Cisco ISE Administration - System. The '+Add' button is highlighted with a red box. The page shows a table for SXP Devices with a pagination bar at the bottom indicating '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**.

 Work Centers • TrustSec

Overview Components TrustSec Policy Policy Sets **SXP** ACI

SXP Devices

All SXP Mappings

[SXP Devices](#) > [SXP Connection](#)

► **Upload from a CSV file**

▼ **Add Single Device**

Input fields marked with an asterisk (*) are required.

Name
ISE Aggregation node

IP Address *
10.50.50.125

Peer Role *
LISTENER

Connected PSNs *
ise01-CL1

Overview Components TrustSec Policy Policy Sets **SXP** ACI

SXP Devices

All SXP Mappings

SXP Domains *
default x

Status *
Enabled

Password Type *
CUSTOM

Password

Version *
V4

► Advanced Settings

Cancel Save

Passaggio 4. Fare clic su **Salva**

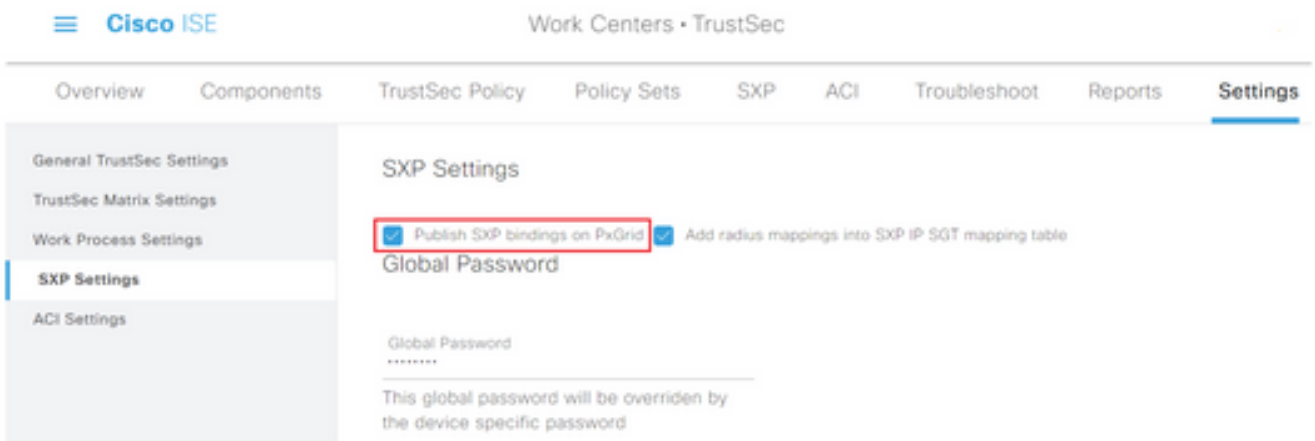
Nota: Ripetere tutti i passaggi per gli altri nodi ISE in ogni cluster per creare una connessione SXP al nodo di aggregazione. **Ripetere lo stesso processo sul nodo di aggregazione e selezionare SPEAKER come ruolo peer.**

Configurare SXP sul nodo di aggregazione

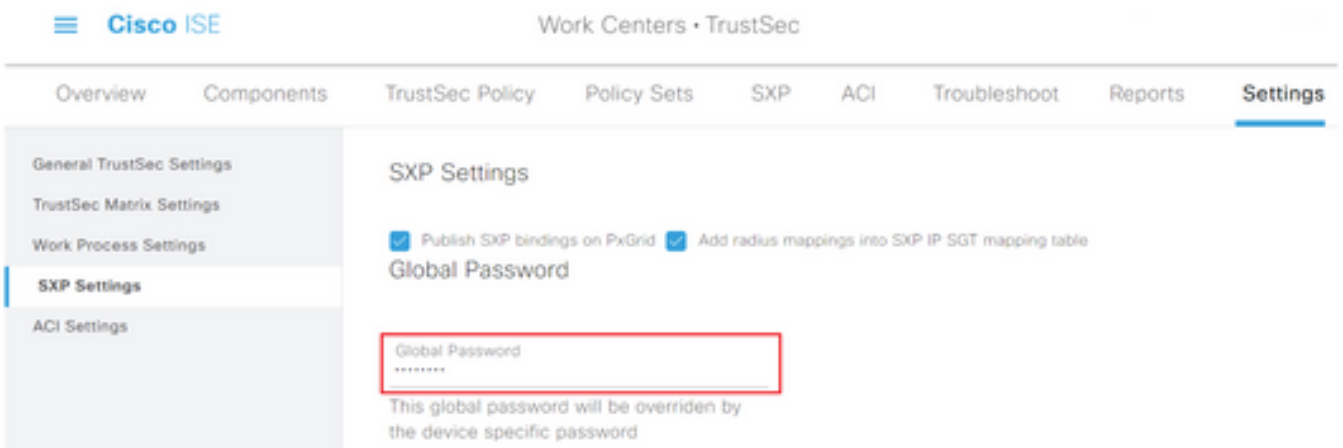
Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere **Centro di lavoro > TrustSec > Impostazioni**

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**

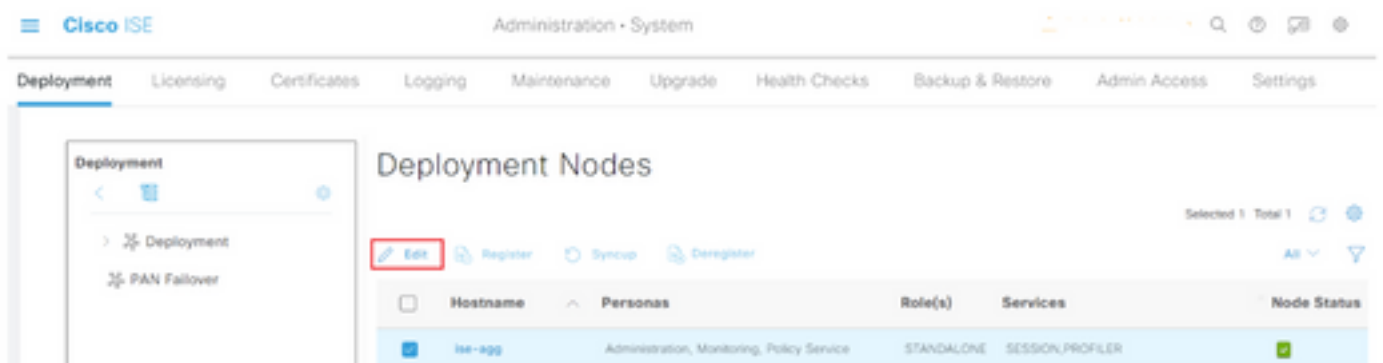


Passaggio 5. Scorrere verso il basso e fare clic su **Salva**.

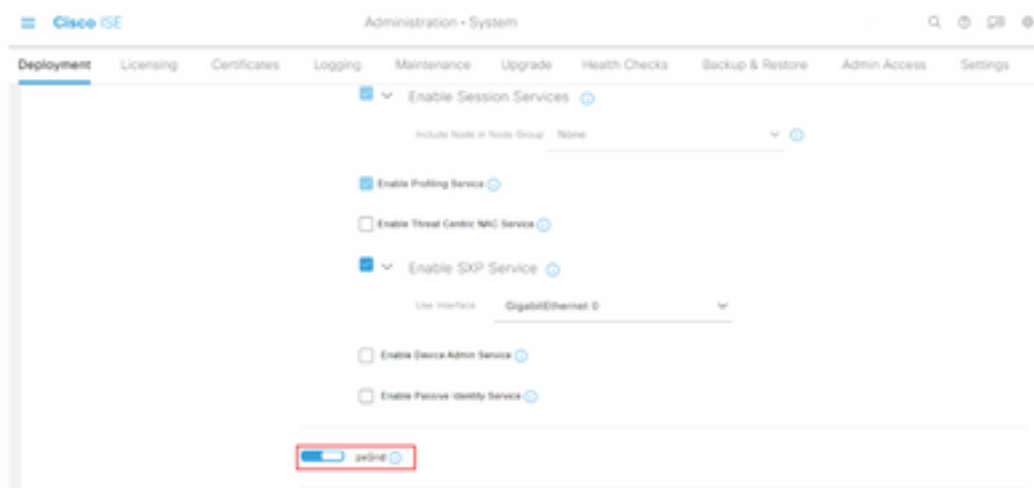
Abilita pxGrid sul nodo di aggregazione

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**.



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

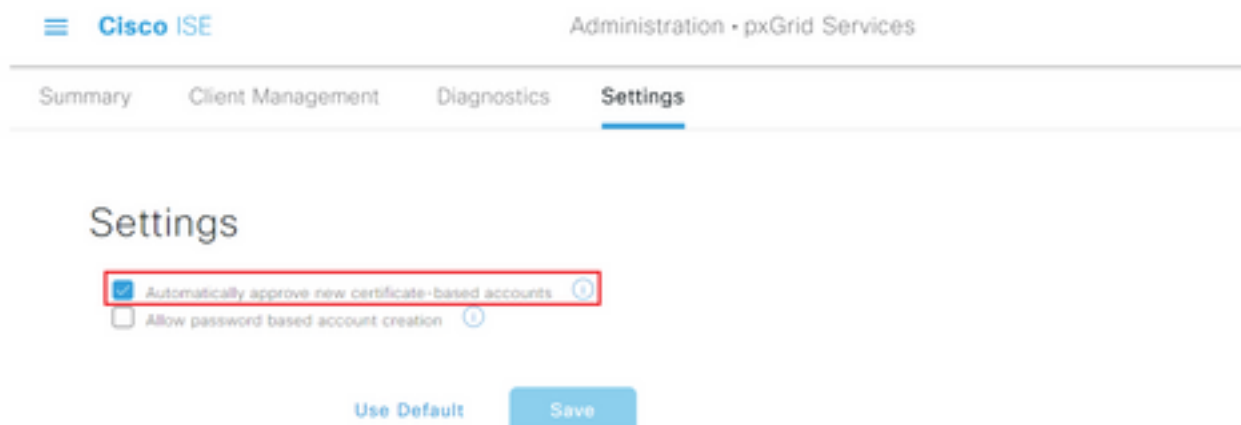


Passaggio 4. Scorrere verso il basso e fare clic su **Salva**.

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**.



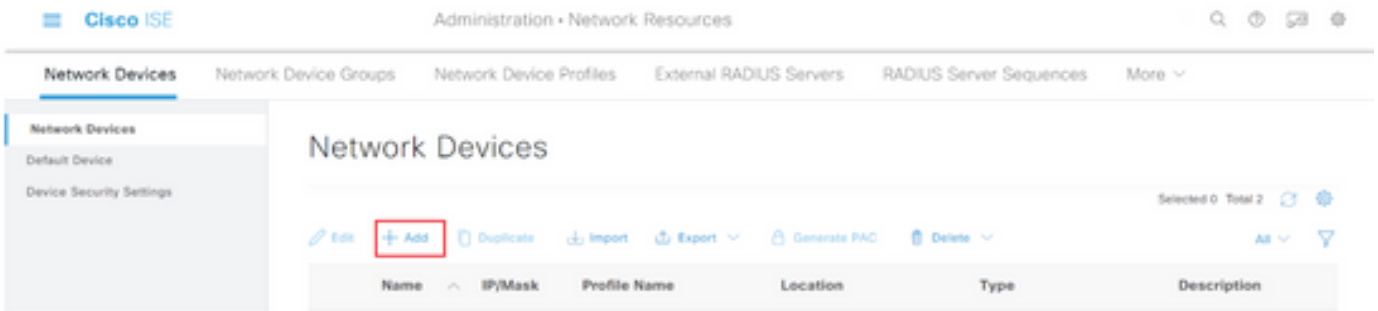
Passaggio 3. Fare clic su **Salva**

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.

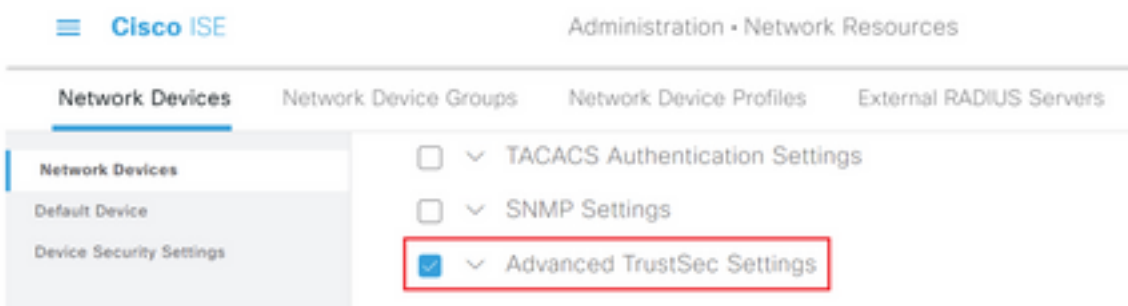
Passaggio 1. Passare alle tre linee dell'icona nell'angolo superiore sinistro e selezionare **Amministrazione > Risorse di rete > Dispositivi di rete**.

Passaggio 2. Fare clic su **+Aggiungi**.

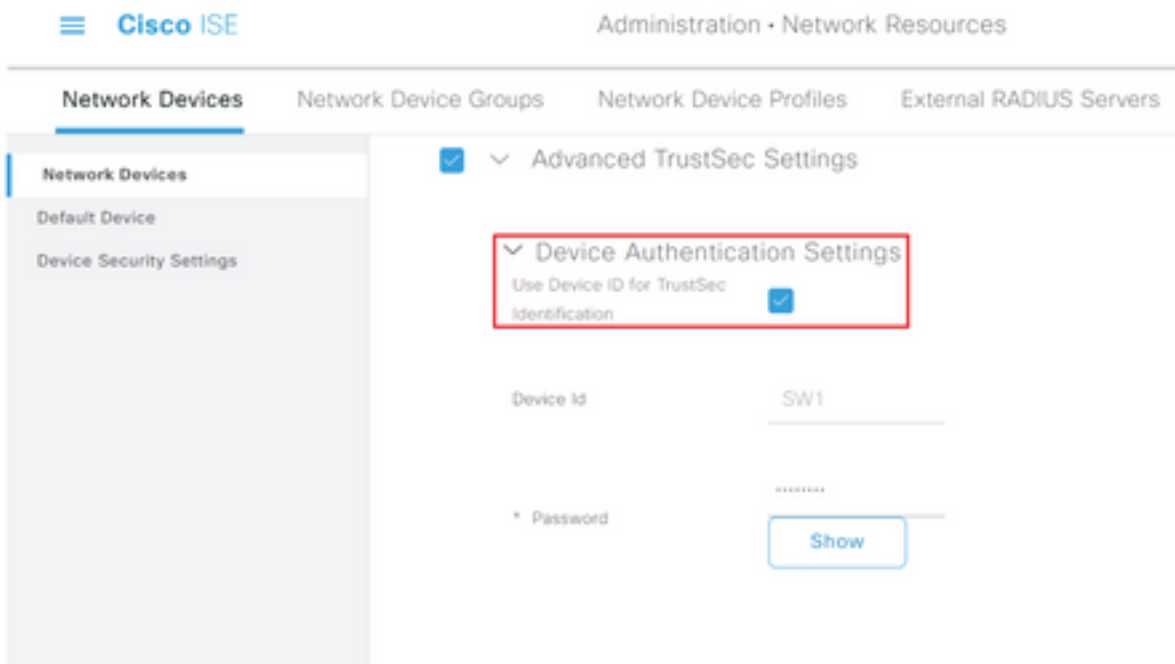


Passaggio 3. Immettere le informazioni richieste nella sezione **Dispositivi di rete** e in **Impostazioni autenticazione RADIUS**.

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

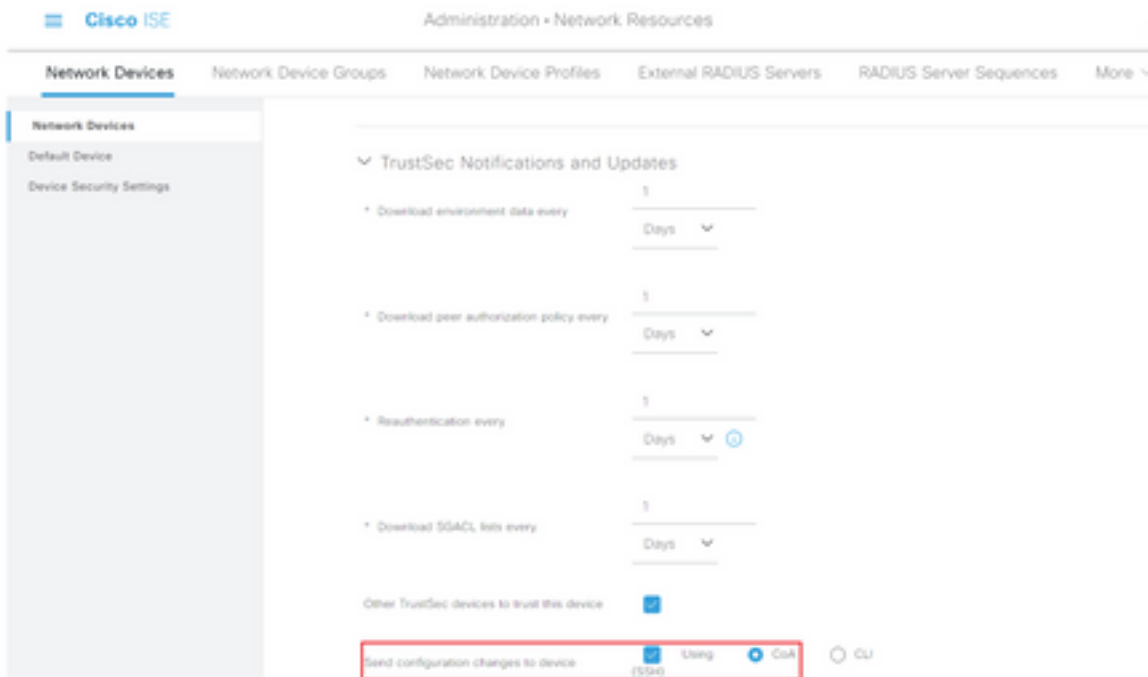


Passaggio 5. Fare clic sulla casella di controllo **Utilizza ID dispositivo per identificazione trustSec** per popolare automaticamente il Nome dispositivo elencato nella sezione **Dispositivi di rete**. Immettere una password nel campo **Password**.



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.



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

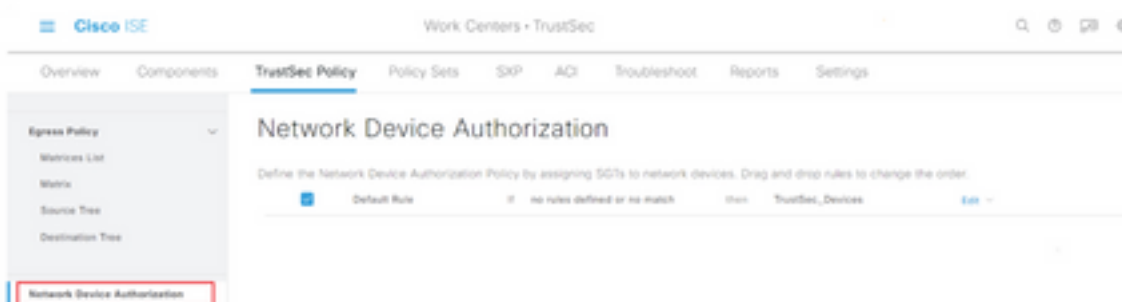
Passaggio 8. Per consentire a ISE di modificare la configurazione del dispositivo di rete, immettere le credenziali utente nei campi **Nome utente modalità di esecuzione** e **Password modalità di esecuzione**. Se necessario, specificare la password di abilitazione nel campo **Password modalità di abilitazione**.

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

Autorizzazione dispositivo di rete

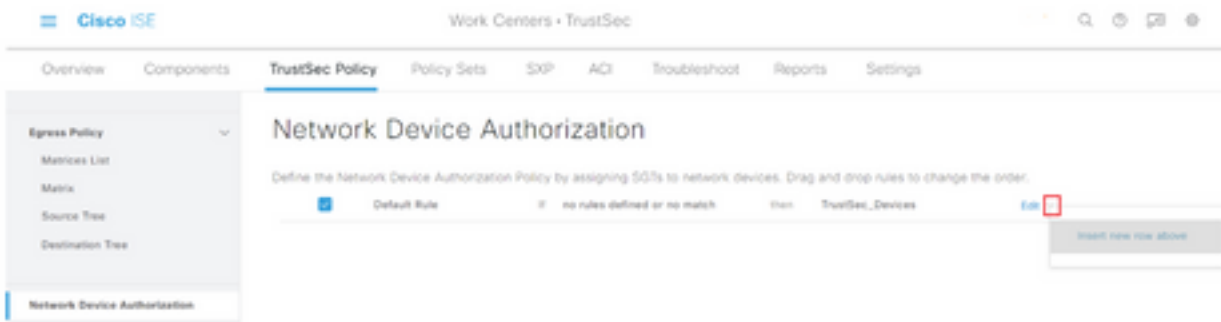
Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere **Centro di lavoro > TrustSec > Criteri TrustSec**.

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



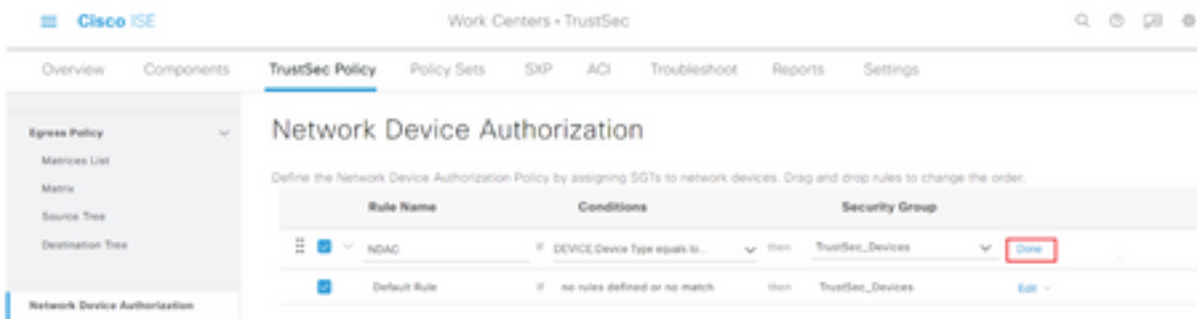
Passaggio 3. A destra, utilizzare l'elenco a discesa accanto a **Modifica** e **Inserisci nuova riga** sopra

per creare una nuova regola NDA.



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.



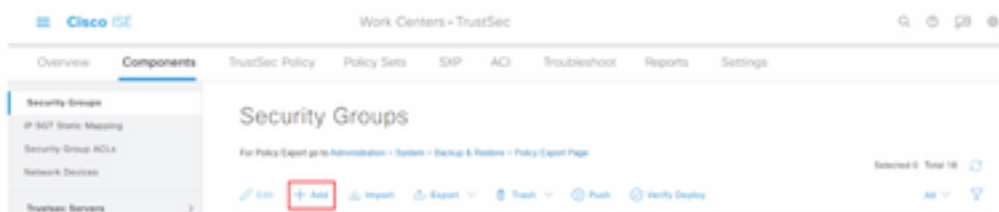
Passaggio 6. Scorrere verso il basso e fare clic su **Salva**.

SGT

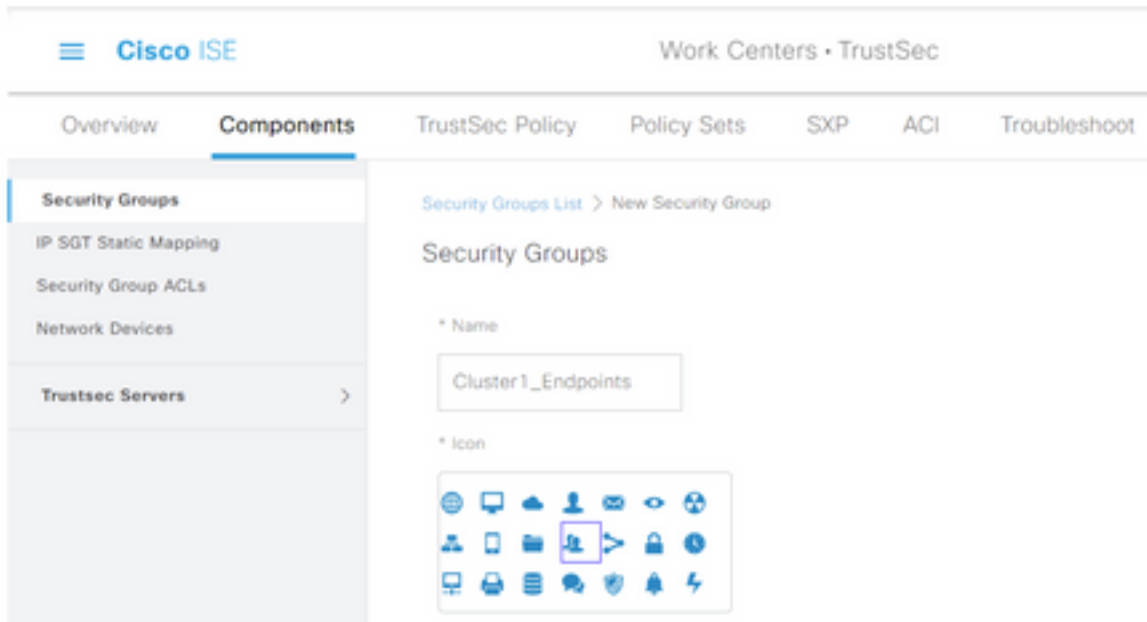
Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e scegliere **Centri di lavoro > TrustSec > Componenti**.

Passaggio 2. Nel riquadro sinistro espandere **Gruppi di sicurezza**.

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



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



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)**

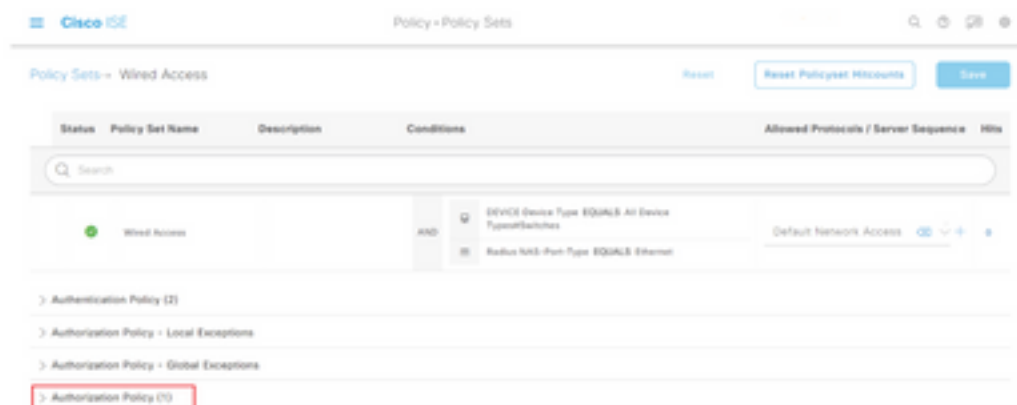
Nota: Ripetere questi passaggi per tutte le SGT necessarie.

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.

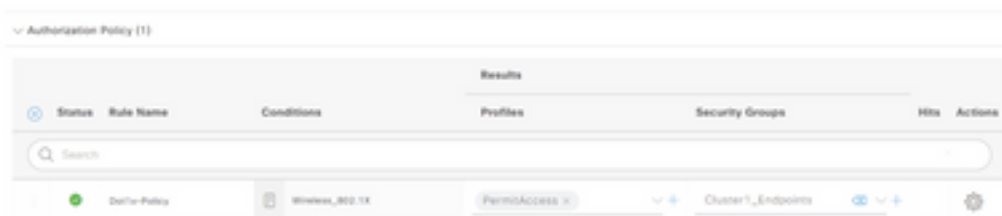
Passaggio 3. Nel set di criteri espandere i **criteri di autorizzazione**.



Passaggio 4. Fare clic sul pulsante  per creare un **criterio di autorizzazione**.



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**.



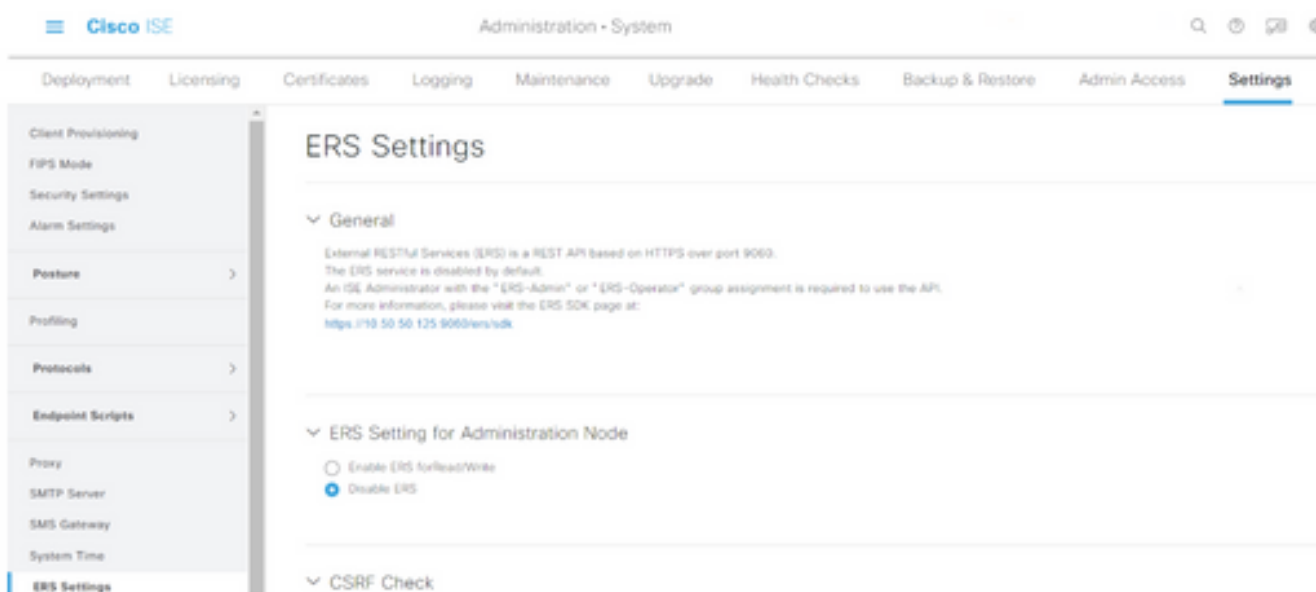
Passaggio 6. Fare clic su **Salva**.

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**.



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

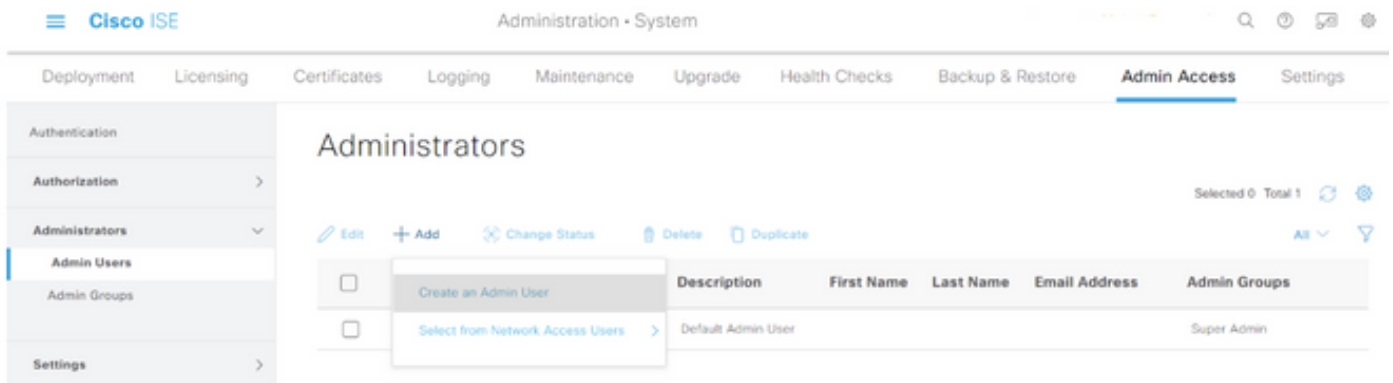
Passaggio 4. Fare clic su **Salva** e confermare con **OK**.

Aggiungi utente al gruppo Amministratore ESR (facoltativo)

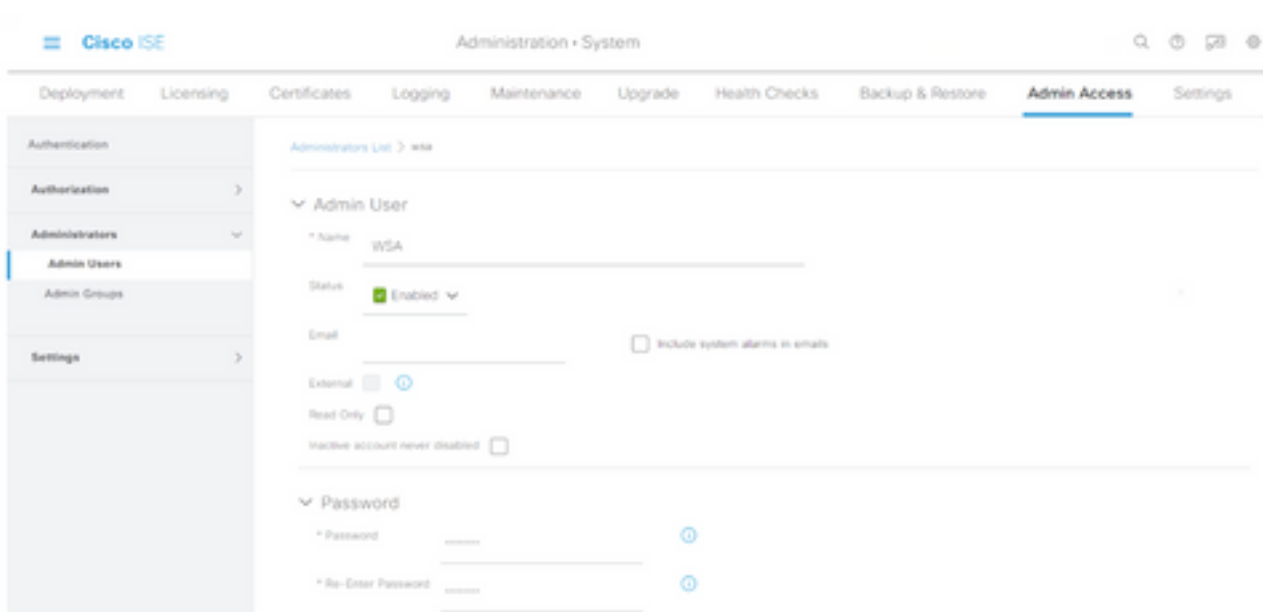
Passaggio 1. Selezionare l'icona a tre righe nell'angolo superiore sinistro e selezionare **Amministrazione > Sistema > Accesso amministratore**

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.



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



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

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. The main navigation menu has tabs for 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Admin Access' tab is active. On the left, a sidebar menu shows 'Authentication', 'Authorization', 'Administrators', 'Admin Users', 'Admin Groups', and 'Settings'. The main content area is for configuring an admin user. It has fields for 'First Name' and 'Last Name'. Below these is the 'Account Options' section with a 'Description' text area. The 'Admin Groups' section shows a list of groups, with 'ERS Admin' selected and highlighted by a red box. At the bottom right, there are 'Save' and 'Reset' buttons.

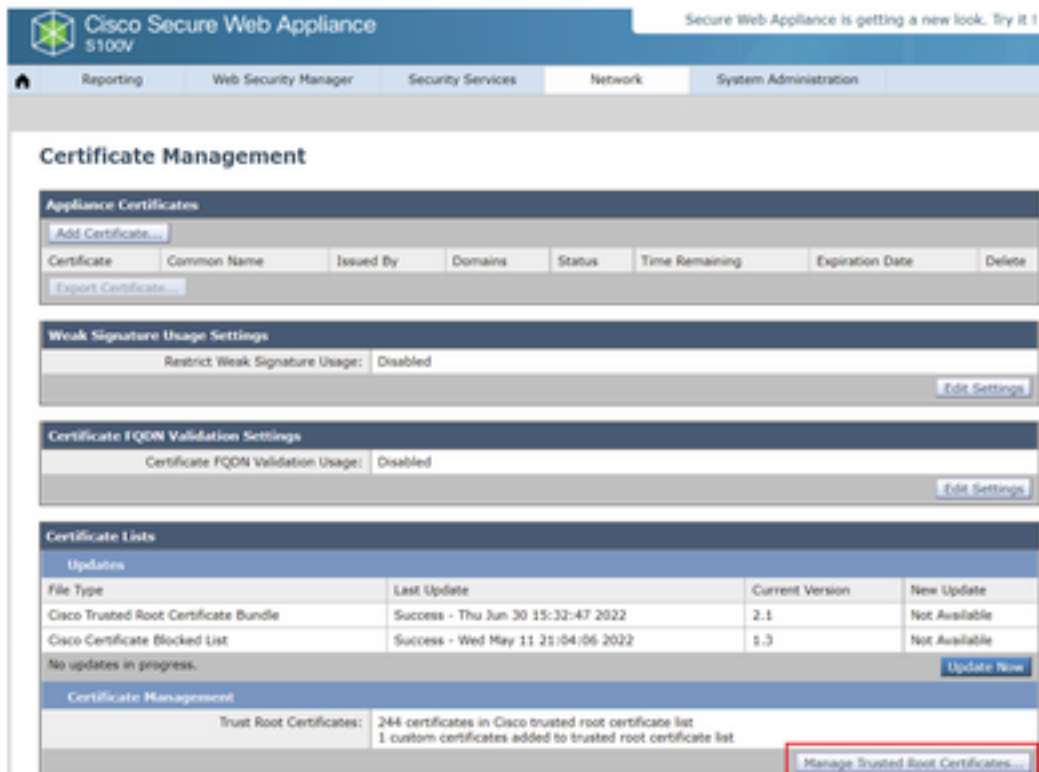
Passaggio 6. Fare clic su **Salva**.

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.



Passaggio 2. Fare clic su **Import**.



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**.

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**.

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

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: No file chosen

Key: No file chosen

Key is Encrypted

No certificate has been uploaded.

Use Generated Certificate and Key

Common name: wsa.securitylab.net

Organization: Cisco

Organizational Unit: Security

Country: SE

Expiration Date: May 10 19:19:26 2024 GMT

Basic Constraints: Not Critical

[Download Certificate...](#) | [Download Certificate Signing Request...](#)

Signed Certificate:

To use a signed certificate, first download a certificate signing request using the link above. Submit the request to a certificate authority, and when you receive the signed certificate, upload it using the field below.

Certificate: No file chosen

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.

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

Enable ISE External RADIUS Service (ERS)

The Web Appliance retrieves Active Directory groups, and local SXP groups from ISE using the ERS. If you are configuring the Web Appliance's policies using Active Directory groups, or in combination with Secure Group Tags (SGTs), you should enable 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:

Password:

ERS Servers

Server name same as ISE pxGrid node

Primary: (Hostname or IPv4 address)

Secondary (Optional): (Hostname or IPv4 address)

Port: (Enter the port number specified for ERS in ISE)

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**.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

Enable Identification Profile

Name:
(e.g. my IT Profile)

Description:
(Maximum allowed characters: 256)

Insert Above:

User Identification Method

Identification and Authentication:

Fallback to Authentication Realm or Guest Privileges:
Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet:
(examples: 20.1.1.0; 20.1.1.0/24; 20.1.1.1-20; 2001:420:80::1:5; 2000:db8::1-2000:db8::10)

Define Members by Protocol: HTTP/HTTPS

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

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**.

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: ISE Profile

Authorized Users and Groups

All Authenticated Users

Selected Groups and Users (2)

ISE Secure Group Tags: No tags entered

ISE Groups: No groups entered

Users: No users entered

Guests (users failing authentication)

Add Identification Profile

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Advanced Define additional group membership criteria.

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**.

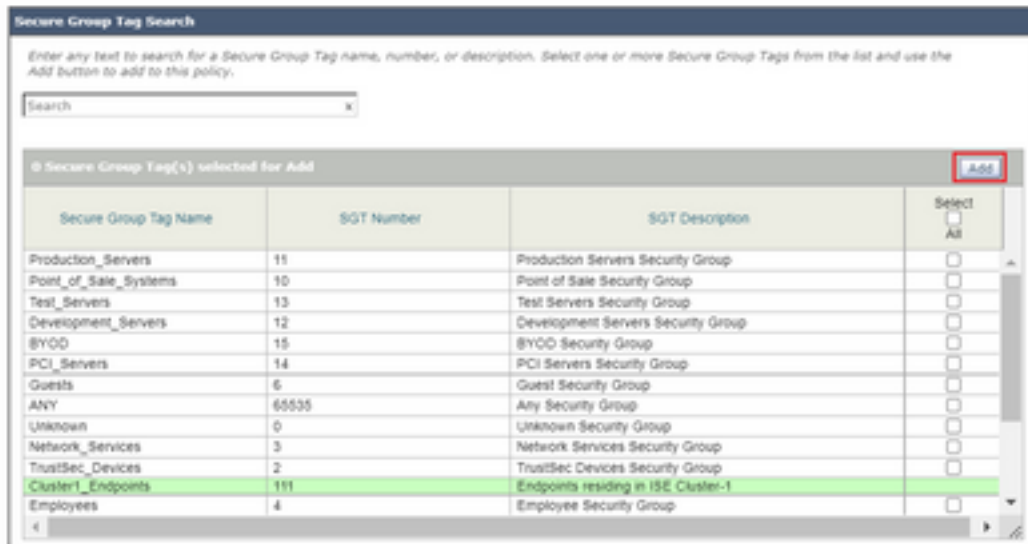
Authorized Secure Group Tags

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

1 Secure Group Tag(s) currently included in this policy.

Secure Group Tag Name	SGT Number	SGT Description	Delete
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	<input type="checkbox"/>

Delete



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

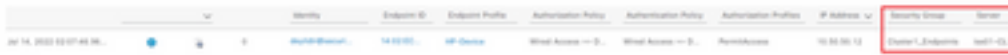
```
cts credentials id SW1 password Cisco123 (This is configured in Privileged EXEC Mode)
cts role-based enforcement
```

```
aaa authorization network cts-list group ISE
cts authorization list cts-list
```

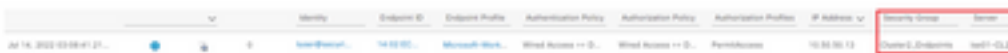
Verifica

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:

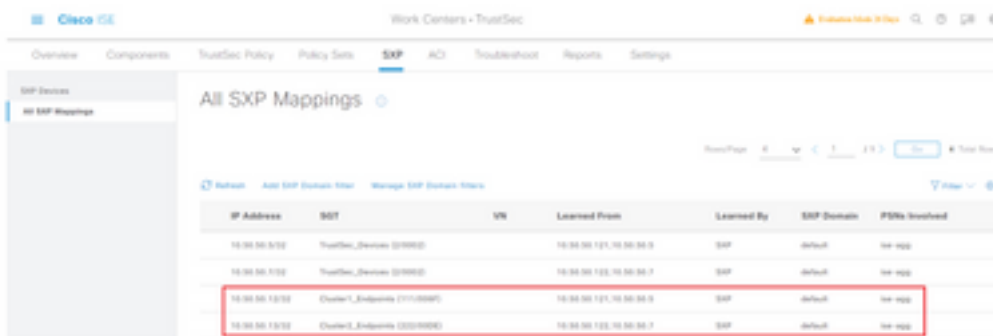


Qui è possibile vedere un endpoint da ISE Cluster 2 a cui è stato assegnato un SGT dopo la corretta autenticazione e autorizzazione:



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:



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

```
wsa2.securitylab.net> isedata
Choose the operation you want to perform:
- STATISTICS - Show the ISE server status and ISE statistics.
- CACHE - Show the ISE cache or check an IP address.
- SGTS - Show the ISE Secure Group Tag (SGT) table.
- GROUPS - Show the ISE Groups table.
[ ]> cache

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
[ ]> show
IP                username                               SGT#  Port Range
10.50.50.13       1sesxp_10.50.50.122_sgt222_10.50.50.13 222   -
10.50.50.12       1sesxp_10.50.50.121_sgt111_10.50.50.12 111   -
```

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
Username: isesxp_10.50.50.121_sgt111_10.50.50.12
Source IP: 10.50.50.12
URL: GET https://bbc.com/
Category: Block URLs CL1
Reason: UNKNOWN
Notification: BLOCK_DEST

Results

Displaying 1 - 50 of 137 items. Items Displayed: 50

Time (GMT +02:00)	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:28:17	https://bbc.com/#43/television CONTENT TYPE: - URL CATEGORY: Block URLs CL1 DESTINATION IP: - DETAILS: Decryption Policy: 'ISE_Cluster1', WBSA: No Score, Malware Analytics File Verdict: -		Block - URL Cat	0B	isesxp_10.50.50.121_sgt111_10.50.50.12 (Identified by ISE) 10.50.50.12

Endpoint che appartiene a ISE Cluster 2

This Page Cannot Be Displayed
Based on your organization's access policies, access to this web site (<https://www.facebook.com/>) has been blocked.
If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Thu, 14 Jul 2022 14:23:58 CEST
Username: isesxp_10.50.50.122_sgt222_10.50.50.13
Source IP: 10.50.50.13
URL: GET https://www.facebook.com/
Category: Block URLs CL2
Reason: UNKNOWN
Notification: BLOCK_DEST

Results

Displaying 1 - 2 of 2 items.

Time (GMT +02:00)	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:23:58	https://www.facebook.com/#43/television CONTENT TYPE: - URL CATEGORY: Block URLs CL2 DESTINATION IP: - DETAILS: Decryption Policy: 'ISE_Cluster2', WBSA: No Score, Malware Analytics File Verdict: -		Block - URL Cat	0B	isesxp_10.50.50.122_sgt222_10.50.50.13 (Identified by ISE) 10.50.50.13

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](#)