

# 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:

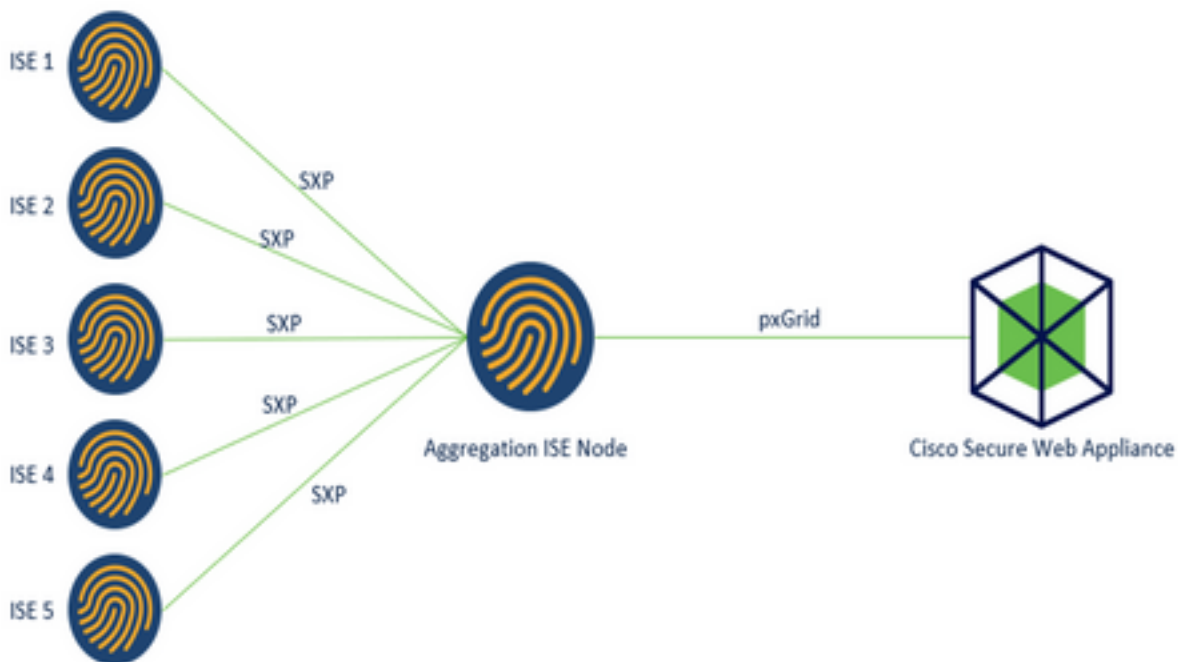
- Sichere Web-Appliance 14.5
- ISE Version 3.1 P3

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.

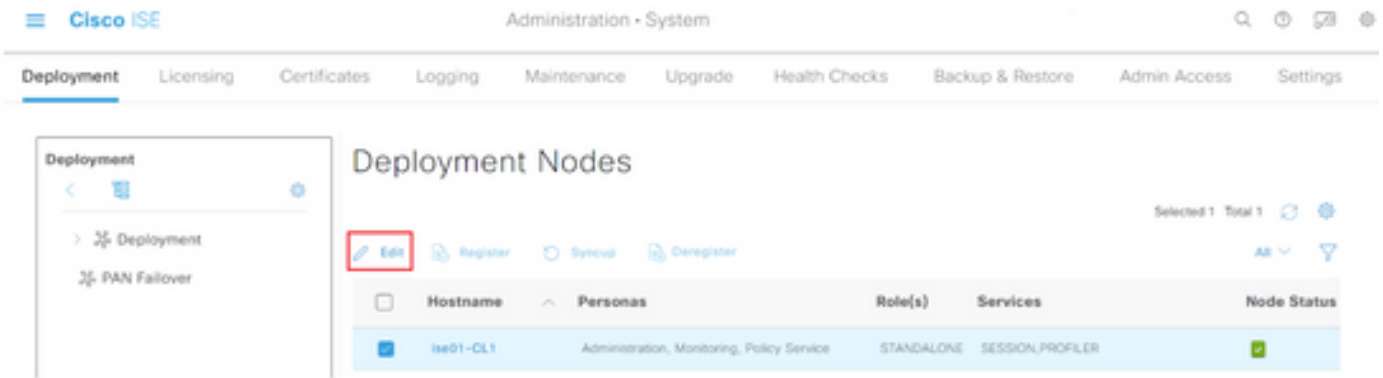
## Konfigurieren

### ISE-Konfiguration

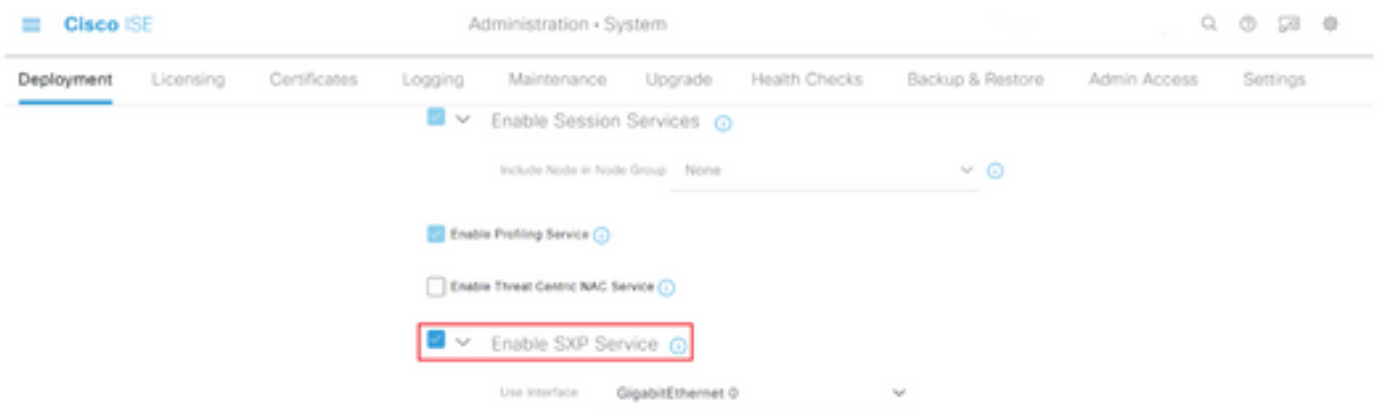
#### SXP aktivieren

**Schritt 1:** Wählen Sie das Symbol für drei Leitungen  in der linken oberen Ecke unter **Administration > System > Deployment**.

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




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



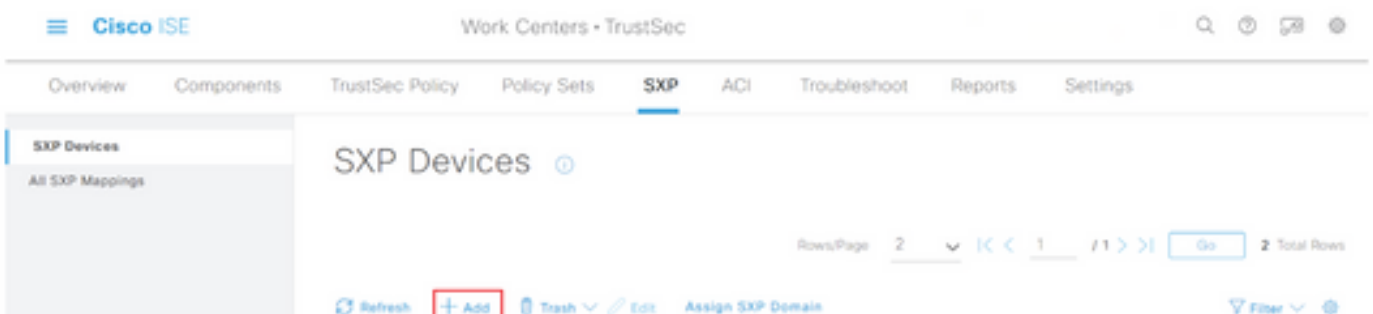
**Schritt 4:** Blättern Sie nach unten, und klicken Sie auf **Speichern**.

**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 sich in der linken oberen Ecke und wählen Sie eine **Work Center > TrustSec > SXP**.

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



**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.

The screenshot shows the Cisco ISE management interface. At the top left is the Cisco ISE logo. At the top right, it says 'Work Centers • TrustSec'. Below this is a navigation bar with tabs: 'Overview', 'Components', 'TrustSec Policy', 'Policy Sets', 'SXP' (which is selected and highlighted with a blue underline), and 'ACI'. On the left side, there is a sidebar with 'SXP Devices' and 'All SXP Mappings'. The main content area shows the breadcrumb 'SXP Devices > SXP Connection'. Below this are two main options: 'Upload from a CSV file' and 'Add Single Device'. The 'Add Single Device' option is expanded, showing a form with the following fields: 'Name' (with the value 'ISE Aggregation node'), 'IP Address \*' (with the value '10.50.50.125'), 'Peer Role \*' (with the value 'LISTENER' and a dropdown arrow), and 'Connected PSNs \*' (with the value 'ise01-CL1' and a dropdown arrow). A note above the form states: 'Input fields marked with an asterisk (\*) are required.'

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

**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**.

Overview Components TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports **Settings**

General TrustSec Settings  
TrustSec Matrix Settings  
Work Process Settings  
**SXP Settings**  
ACI Settings

**SXP Settings**

Publish SXP bindings on PxGrid  Add radius mappings into SXP IP SGT mapping table

**Global Password**

Global Password  
\*\*\*\*\*

This global password will be overridden by the device specific password

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

Overview Components TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports **Settings**

General TrustSec Settings  
TrustSec Matrix Settings  
Work Process Settings  
**SXP Settings**  
ACI Settings

**SXP Settings**

Publish SXP bindings on PxGrid  Add radius mappings into SXP IP SGT mapping table

**Global Password**

Global Password  
\*\*\*\*\*

This global password will be overridden by the device specific password

**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**.

Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

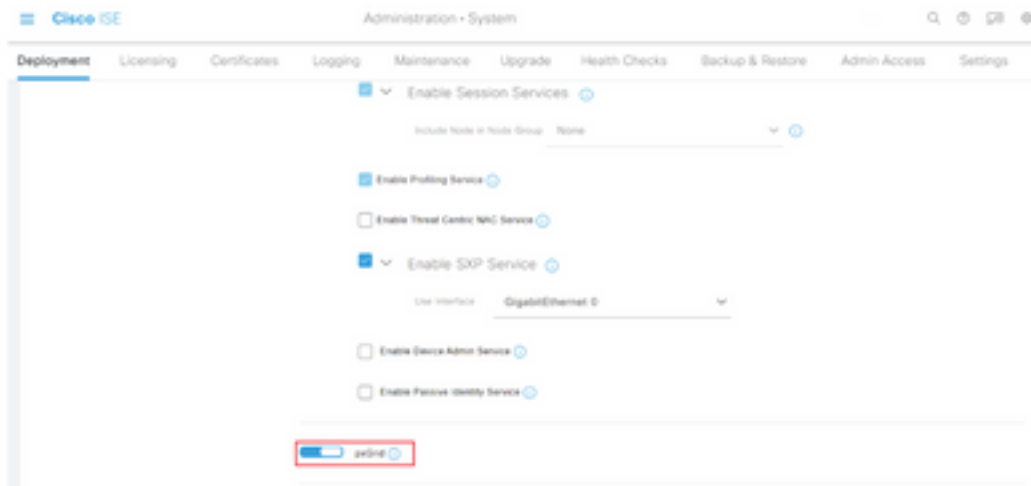
**Deployment Nodes**

Selected 1 Total 1

**Edit** Register Syncup Deregister

Hostname	Personas	Role(s)	Services	Node Status
ise-agg	Administration, Monitoring, Policy Service	STANDALONE	SESSIONPROFILER	<span style="color: green;">■</span>

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

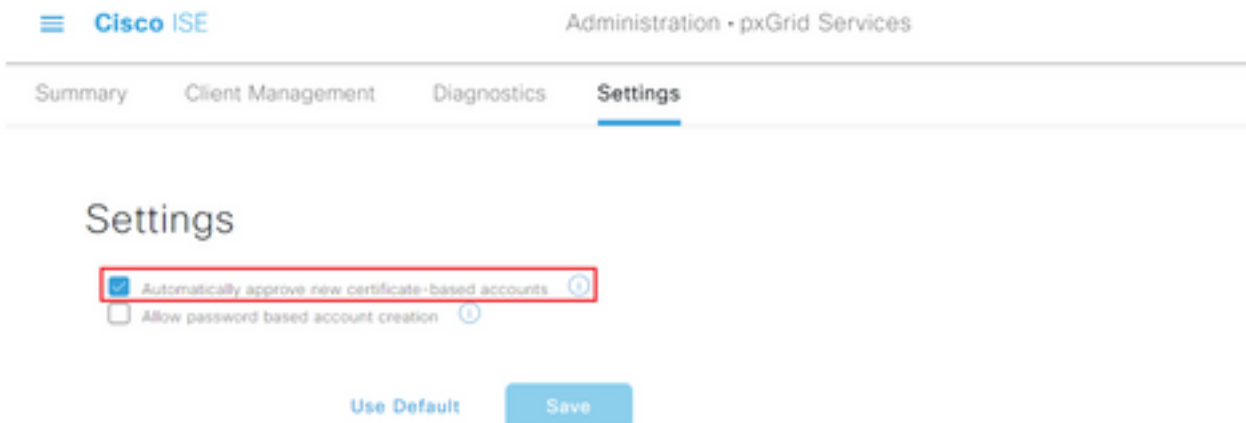


**Schritt 4:** Blättern Sie nach unten, und klicken Sie auf **Speichern**.

## 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**

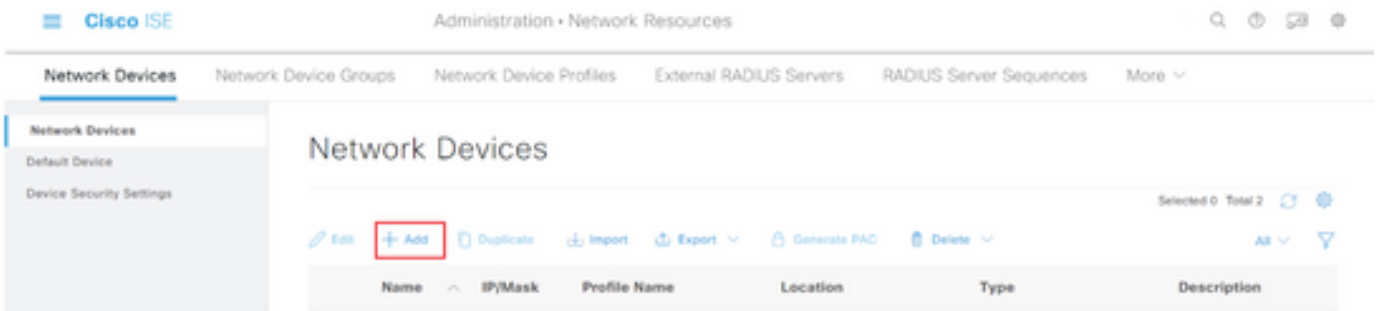
## TrustSec-Einstellungen für Netzwerkgeräte

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.

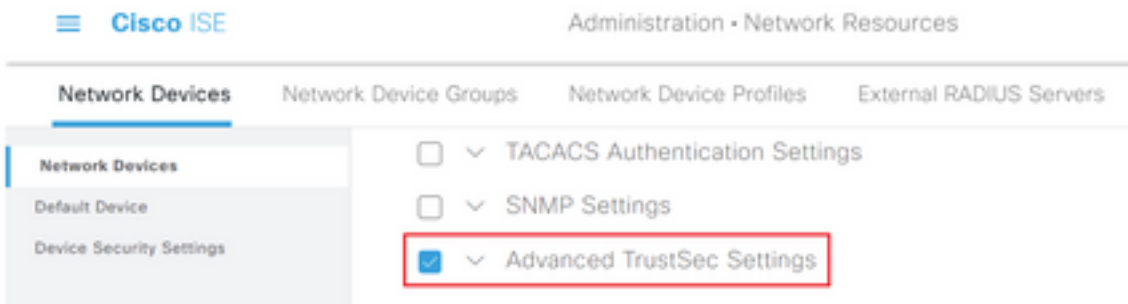


**Schritt 2:** Klicken Sie auf **+Hinzufügen**.

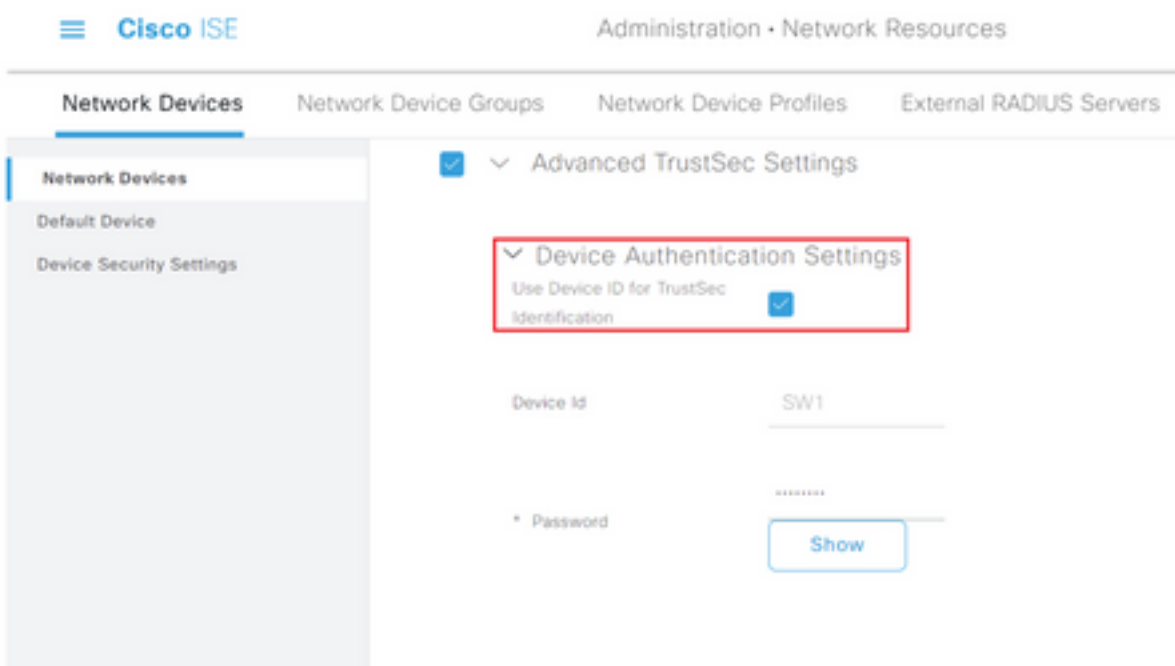


**Schritt 3:** Geben Sie die erforderlichen Informationen im Abschnitt **Netzwerkgeräte** und in den **RADIUS-Authentifizierungseinstellungen** ein.

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

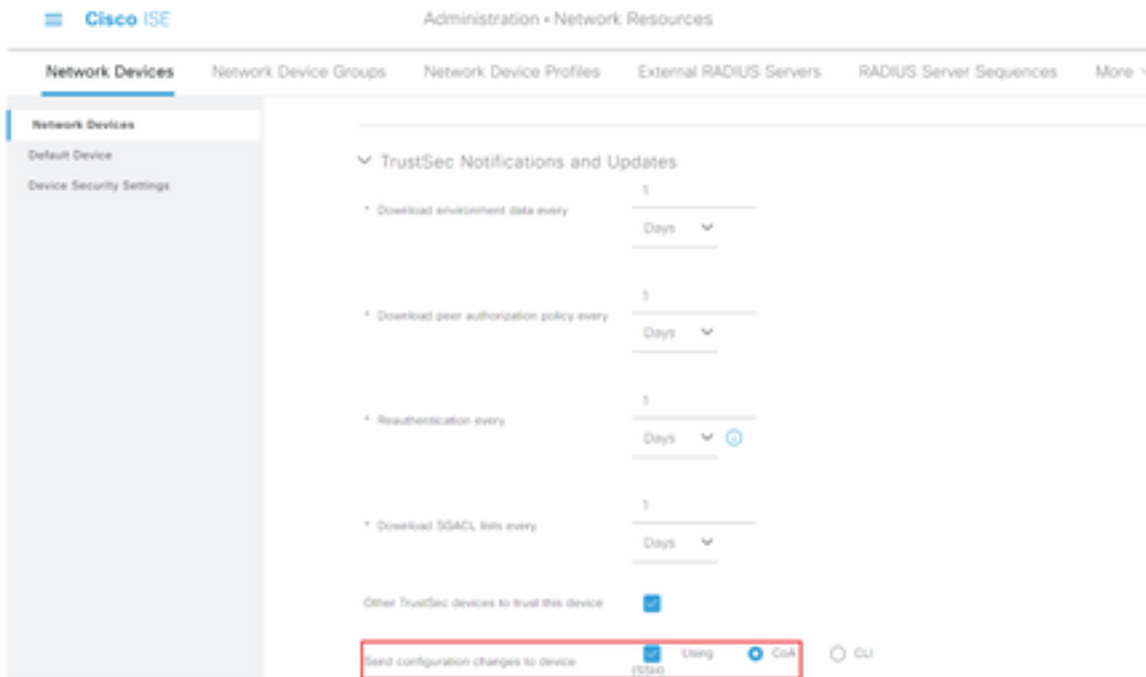


**Schritt 5:** Klicken Sie auf das Kontrollkästchen **Geräte-ID für die TrustSec-Identifizierung verwenden**, um den im Abschnitt **Netzwerkgeräte** aufgeführten Gerätenamen automatisch auszufüllen. Geben Sie ein Kennwort in das Feld **Kennwort** ein.



**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.



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

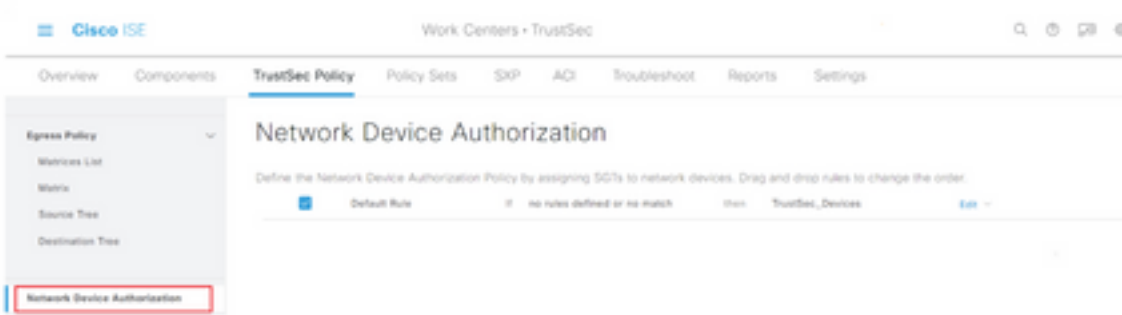
**Schritt 8:** Um ISE die Konfiguration des Netzwerkgeräts bearbeiten zu lassen, geben Sie die Benutzeranmeldeinformationen in die Felder **EXEC Mode Username (Benutzername für den EXEC-Modus)** und **EXEC Mode Password (Kennwort für den EXEC-Modus)** ein. Geben Sie optional das enable-Kennwort im Feld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

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

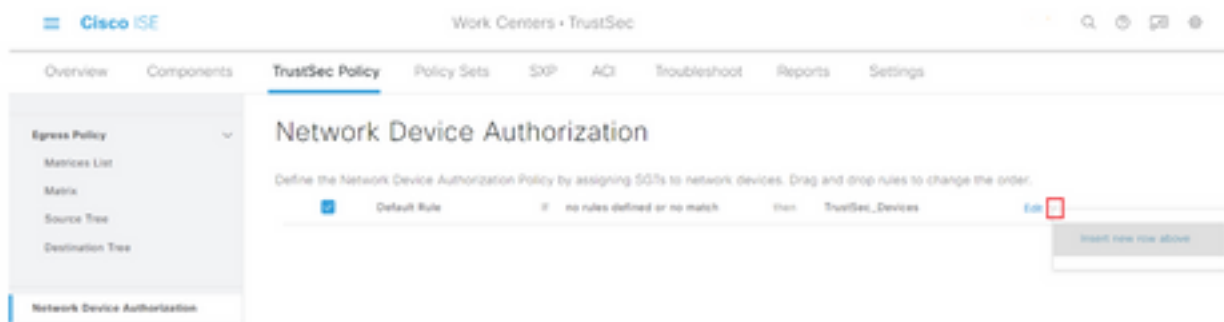
## Autorisierung von Netzwerkgeräten

**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**.

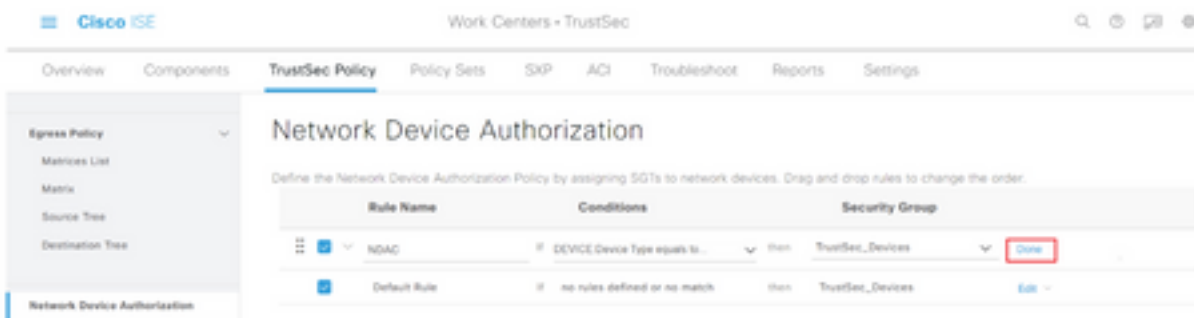


**Schritt 3:** Verwenden Sie rechts das Dropdown-Menü neben **Bearbeiten** und **Neue Zeile einfügen oben**, um eine neue NDA-Regel zu erstellen.



**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**.



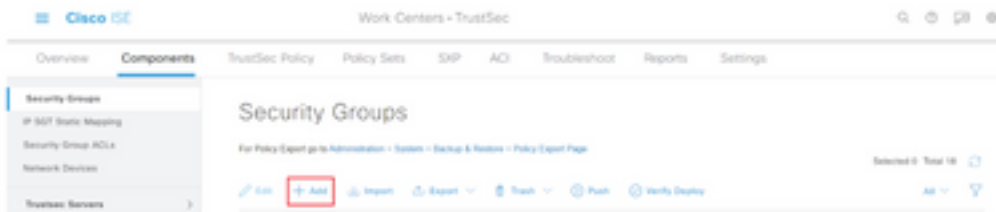
**Schritt 6:** Blättern Sie nach unten, und klicken Sie auf **Speichern**.

## SGT

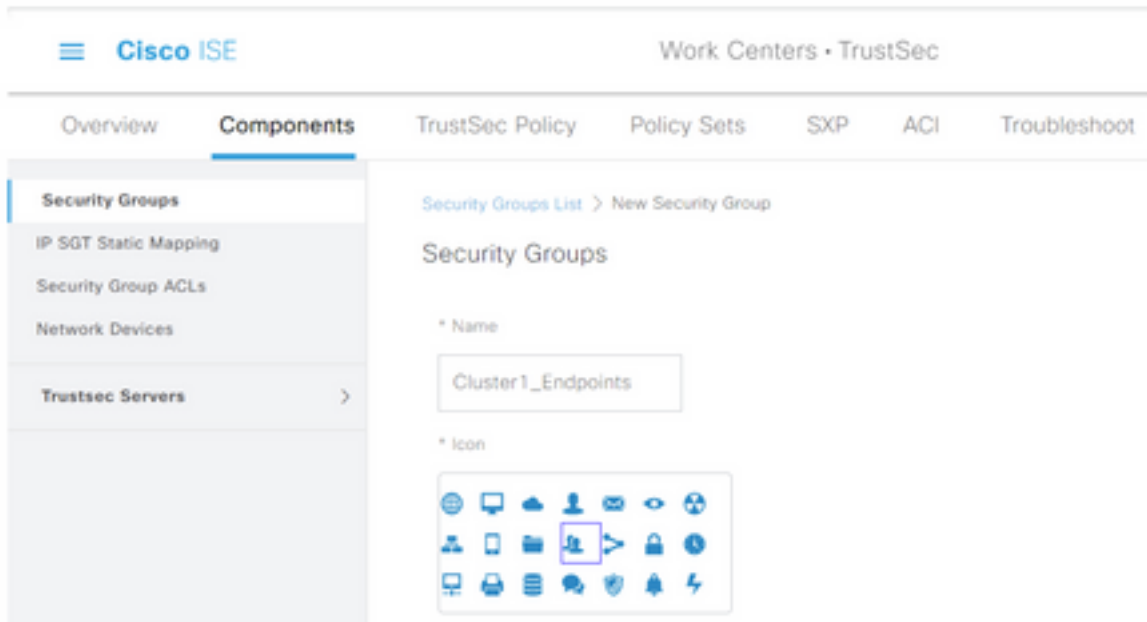
**Schritt 1:** Wählen Sie das Symbol für drei Zeilen in der oberen linken Ecke aus, und wählen Sie unter **Work Centers > TrustSec > Components**.

**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.



**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**.

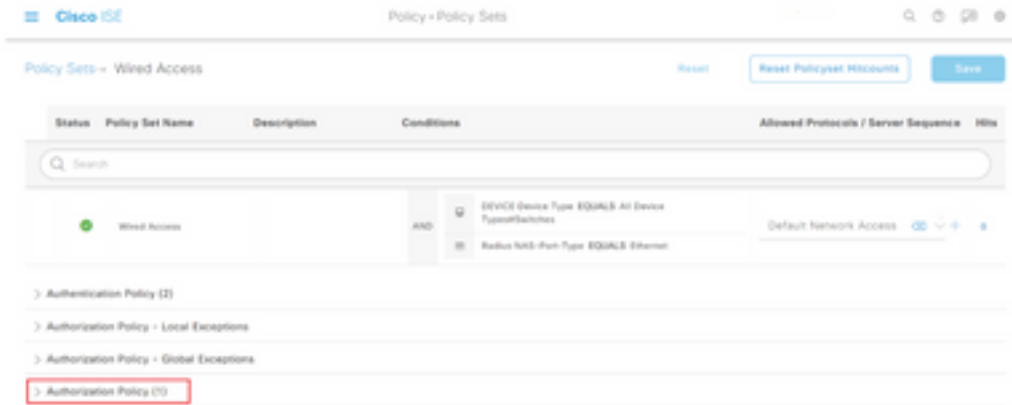
**Anmerkung:** Wiederholen Sie diese Schritte für alle erforderlichen SGTs.

## Autorisierungsrichtlinie

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

**Schritt 2:** Wählen Sie den entsprechenden Richtlinienatz aus.

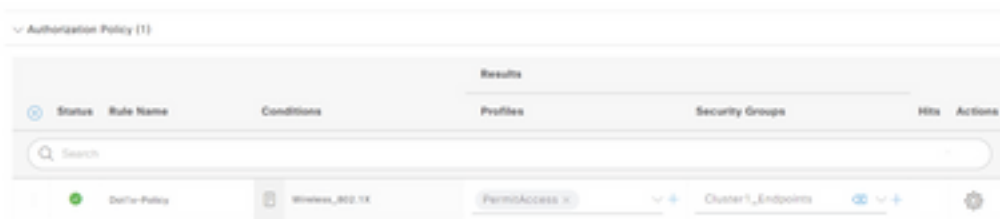
**Schritt 3:** Erweitern Sie im Richtlinienatz die **Autorisierungsrichtlinie**.



**Schritt 4:** Klicken Sie auf  um eine **Autorisierungsrichtlinie** zu erstellen.



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



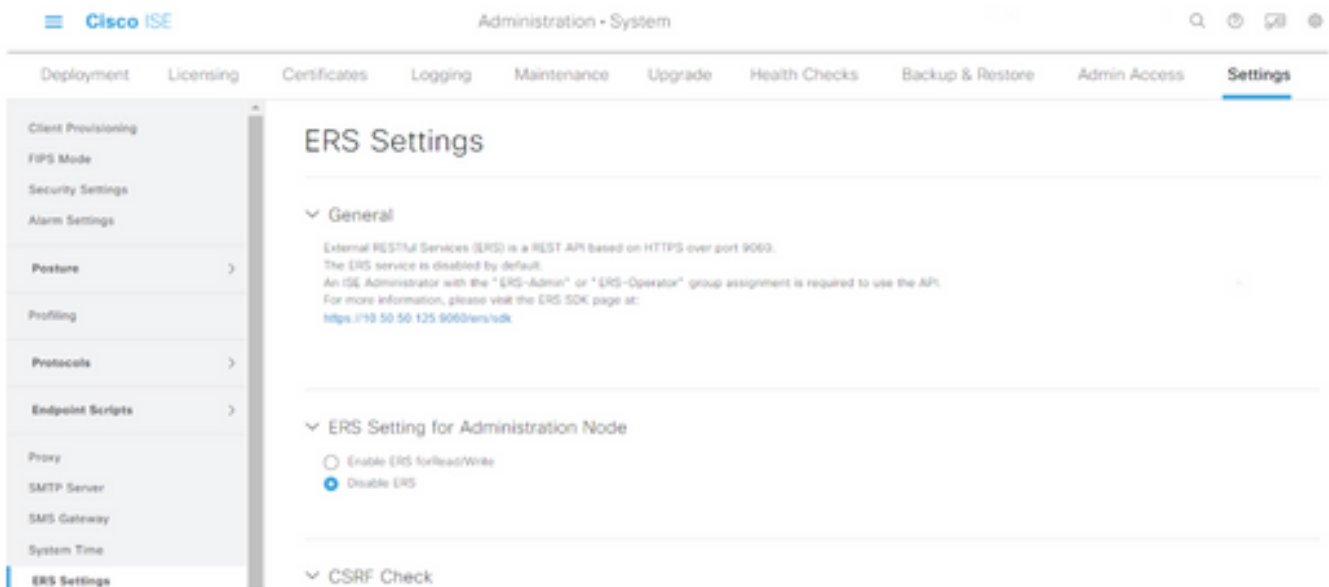
**Schritt 6:** Klicken Sie auf **Speichern**.

## 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**.



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

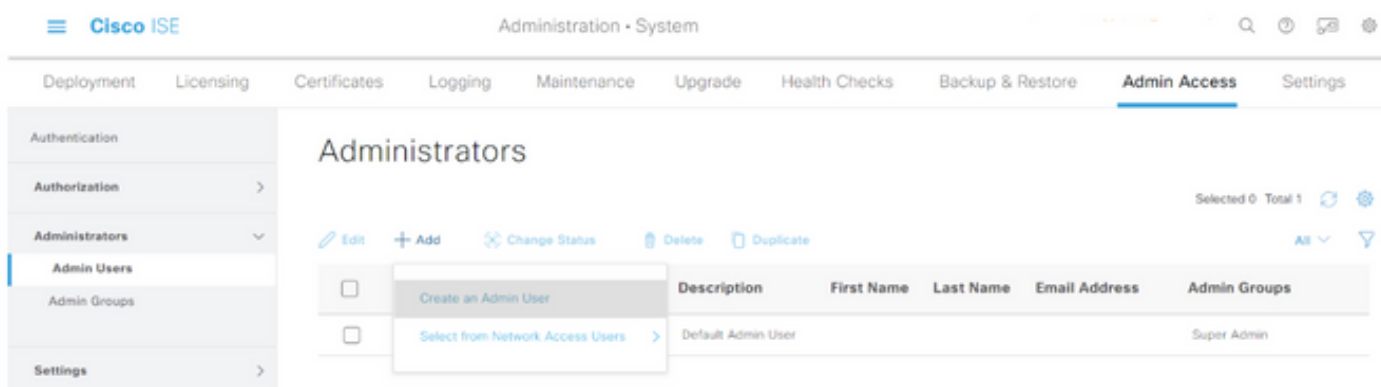
**Schritt 4:** Klicken Sie auf **Speichern** und bestätigen Sie mit **OK**.

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

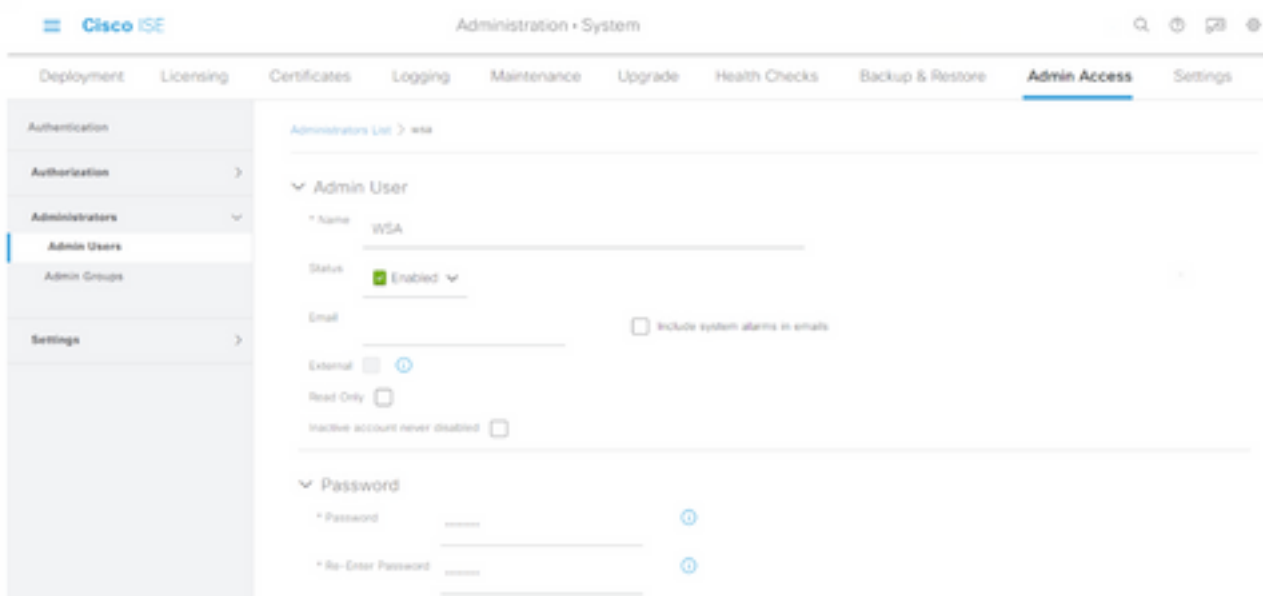
**Schritt 1:** Wählen Sie das Symbol für drei Zeilen in der linken oberen Ecke aus, und wählen Sie **Administration > System > Admin Access (Verwaltung > System > Administratorzugriff)** aus.

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

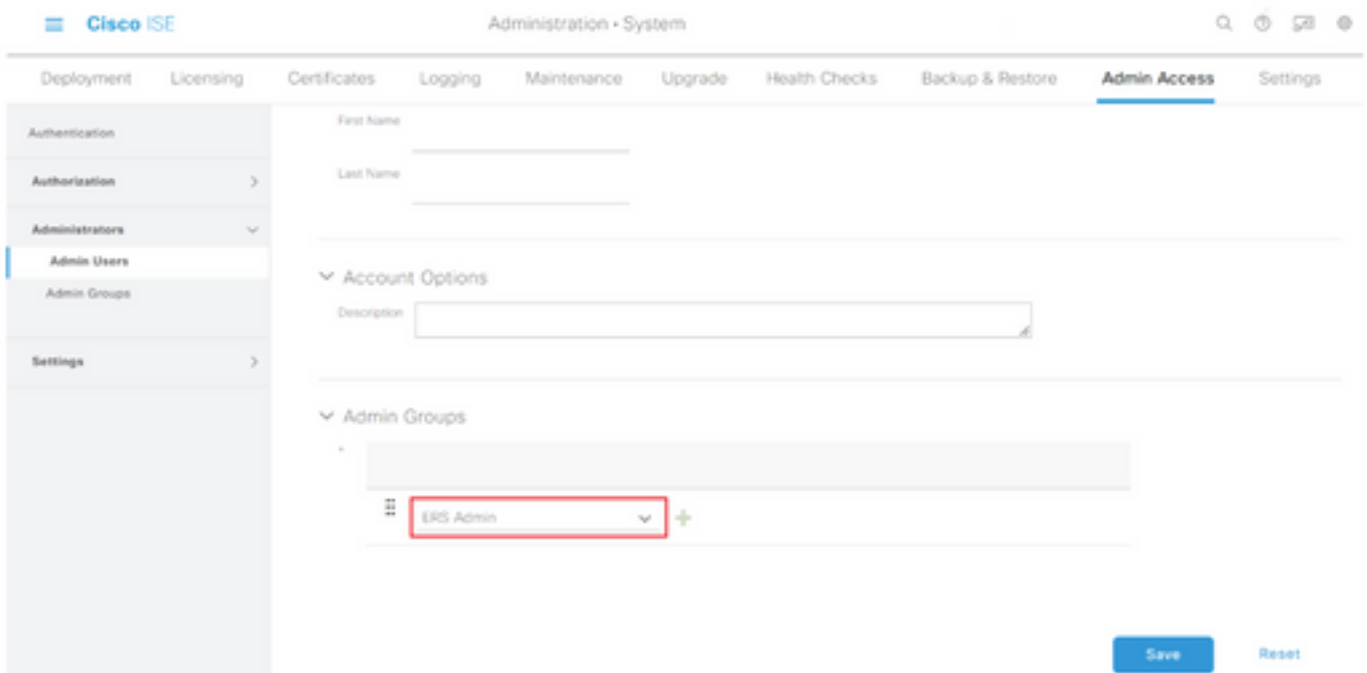
**Schritt 3:** Klicken Sie auf **+Hinzufügen** und wählen Sie **Admin User** aus dem Dropdown-Menü aus.



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



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



**Schritt 6:** Klicken Sie auf **Speichern**.

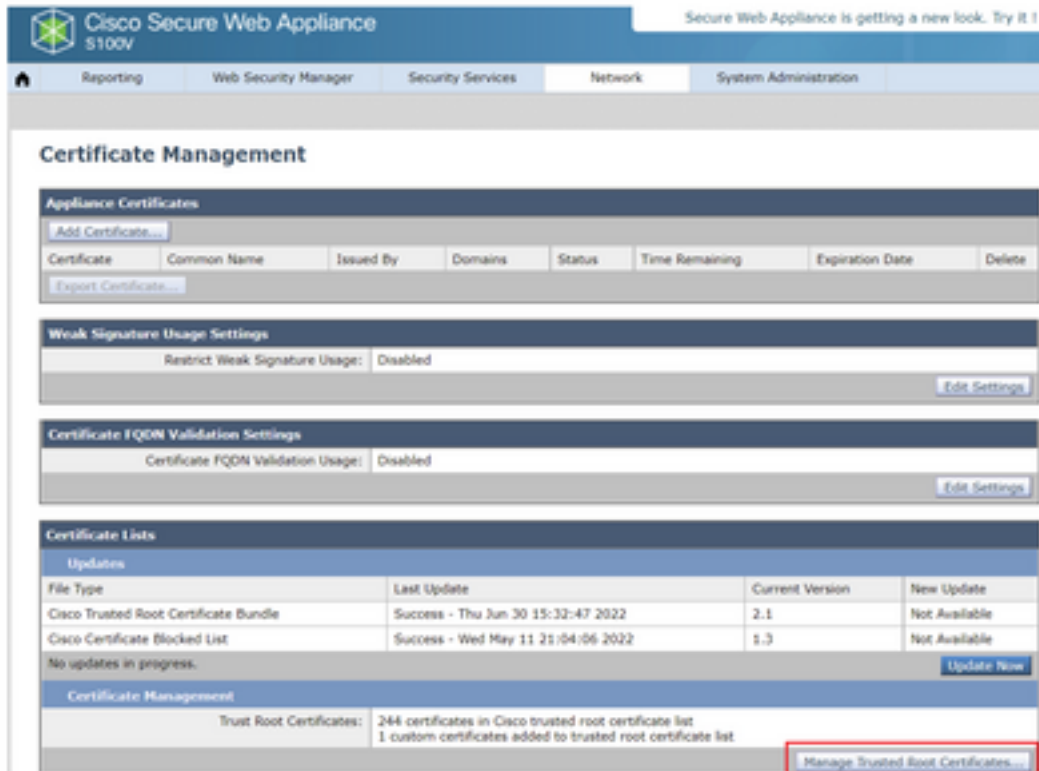
## Sichere Web-Appliance-Konfiguration

### 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.



**Schritt 2:** Klicken Sie auf **Importieren**.



**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 Identity Services Engine Settings

Enable ISE Service

Primary ISE pxGrid Node: The Web Appliance will communicate with the ISE pxGrid node to support Web Appliance data subscription (ongoing updates). A primary ISE pxGrid node (server) must be configured.

hostname or IP address

ISE pxGrid Node Certificate: If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trustall Root Certificates list (see Network > Certificate Management) and upload the CA-signed root certificate below. If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below. You can upload the certificate chain that includes any intermediate certificates.

Certificate: Choose File No file chosen Upload File

**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: 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 Upload File

Key: Choose File No 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 and Key

Common Name: [input field]

Organization: [input field]

Organizational Unit: [input field]

Country: [input field]

Duration before expiration: [input field] months

Basic Constraints:  Set X509v3 Basic Constraints Extension to Critical

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.

**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.

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)

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.

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

---

Membership Definition

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

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

Define Members by Protocol:  HTTP/HTTPS

Define additional group membership criteria.

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**.

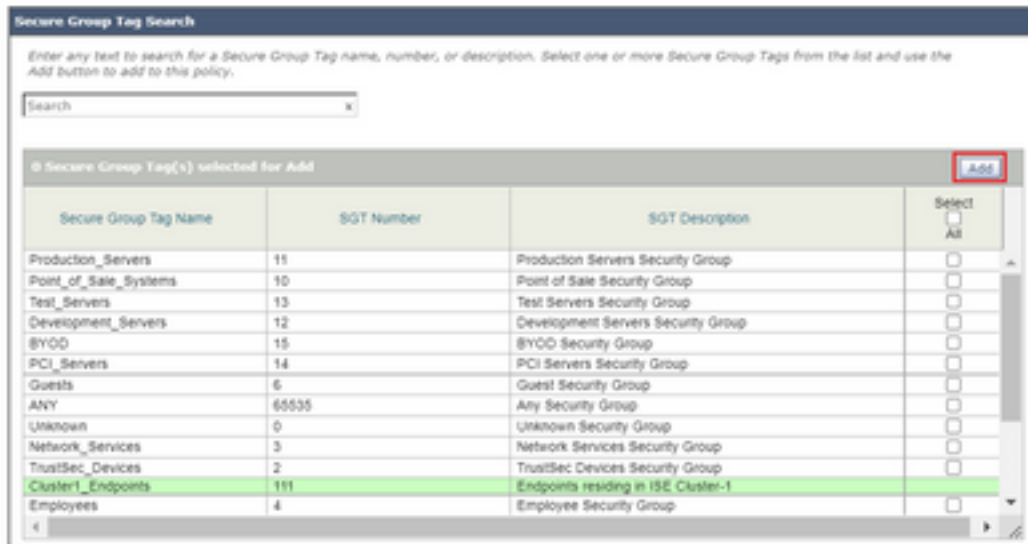
The screenshot shows the 'Policy Member Definition' configuration page. It includes a dropdown menu for 'Identification Profiles and Users' set to 'Select One or More Identification Profiles'. Below this, there are two main sections: 'Identification Profile' and 'Authorized Users and Groups'. The 'Identification Profile' section has a dropdown menu with 'ISE Profile' selected. The 'Authorized Users and Groups' section has three radio button options: 'All Authenticated Users', 'Selected Groups and Users' (which is selected), and 'Guests (users failing authentication)'. The 'Selected Groups and Users' option is expanded to show details: 'ISE Secure Group Tags: No tags entered', 'ISE Groups: No groups entered', and 'Users: No users entered'. There is an 'Add Identification Profile' button on the right. At the bottom, there is a note about authentication information availability and an 'Advanced' link to define additional group membership criteria.

**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**.

The screenshot shows the 'Authorized Secure Group Tags' configuration page. It includes a search function and a table of authorized SGTs. The table has four columns: 'Secure Group Tag Name', 'SGT Number', 'SGT Description', and 'Delete'. The first row shows 'Cluster1\_Endpoints' with SGT Number '111' and description 'Endpoints residing in ISE Cluster-1'. There is a checkbox in the 'Delete' column for this row. Below the table, there is a 'Delete' button.

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



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 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:

Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authentication Profile	IP Address	Security Group	Domain
10.50.50.12	14 03 00...	IP Device	What Access -->	What Access -->	Permissive	10.50.50.12	Cluster1_Endpoints	isp01-01.1

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

Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authentication Profile	IP Address	Security Group	Domain
10.50.50.12	14 03 00...	Microsoft Work	What Access -->	What Access -->	Permissive	10.50.50.12	Cluster2_Endpoints	isp01-01.1

## 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:

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PDNs Involved
10.50.50.12	TrustSec_Device (20000)		10.50.50.121,10.50.50.0	SXP	default	10-100
10.50.50.12	Cluster1_Endpoints (1111111)		10.50.50.121,10.50.50.0	SXP	default	10-100
10.50.50.12	Cluster2_Endpoints (2222222)		10.50.50.122,10.50.50.7	SXP	default	10-100

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

```
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   -
```

## 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  
 Username: isesxp\_10.50.50.121\_sgt111\_10.50.50.12  
 Source IP: 10.50.50.12  
 URL: GET https://bbc.com/  
 Category: Block URLs CL1  
 Reason: UNKNOWN  
 Notification: BLOCK\_DEST

Time (GMT +02:00)	Website (count)	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:28:17	<a href="https://bbc.com/#43/television">https://bbc.com/#43/television</a> 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

Endpunkt, der zum ISE-Cluster 2 gehört

**This Page Cannot Be Displayed**

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

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

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

Time (GMT +02:00)	Website (count)	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:23:58	<a href="https://www.facebook.com/#43/television">https://www.facebook.com/#43/television</a> 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

## 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](#)