将多个ISE集群与基于TrustSec的策略的安全网络设备集成

目录

简介

本文档介绍通过pxGrid将来自多个ISE部署的安全组标记(SGT)信息发送到单个思科安全网络设备（正式版网络安全设备WSA）以在TrustSec部署中利用基于SGT的Web访问策略的过程。

在版本14.5之前，安全网络设备只能与单个ISE集群集成基于SGT的身份策略。通过引入此新版本，安全网络设备现在可与来自多个ISE集群的信息进行互操作，并在它们之间汇聚一个单独的ISE节点。这带来了巨大的好处，使我们能够导出来自不同ISE集群的用户数据，并自由控制用户可以使用的退出点，无需1:1集成。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎 (ISE)
- 安全Web设备
- RADIUS协议
- TrustSec
- pxGrid

使用的组件

本文档中的信息基于以下软件和硬件版本：

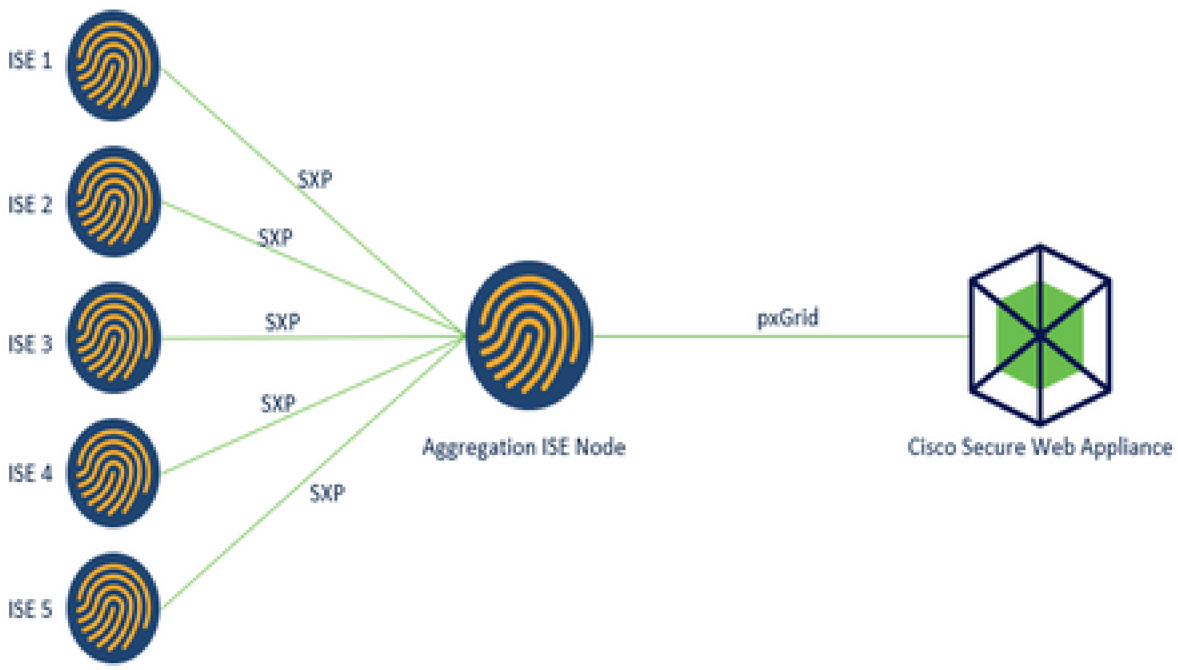
- 安全Web设备14.5
- ISE版本3.1 P3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

限制

1. 所有ISE集群需要为SGT维护统一的映射。
2. ISE汇聚节点必须拥有其他ISE集群的SGT名称/编号。
3. 安全Web设备只能根据SGT标记识别策略（访问/解密/路由），而不能识别组和用户。
4. 报告和跟踪基于SGT。
5. 现有的ISE/安全Web设备规模调整参数继续适用于此功能。

网络图



Process:

1.当最终用户连接到网络时，他们根据ISE中的授权策略接收SGT。

2.然后，不同的ISE集群通过SXP将此SGT信息以SGT-IP映射的形式发送到ISE汇聚节点。

3. ISE汇聚节点接收此信息并通过pxGrid与单个安全网络设备共享。

4.安全Web设备使用它学到的SGT信息，根据Web访问策略向用户提供访问权限。

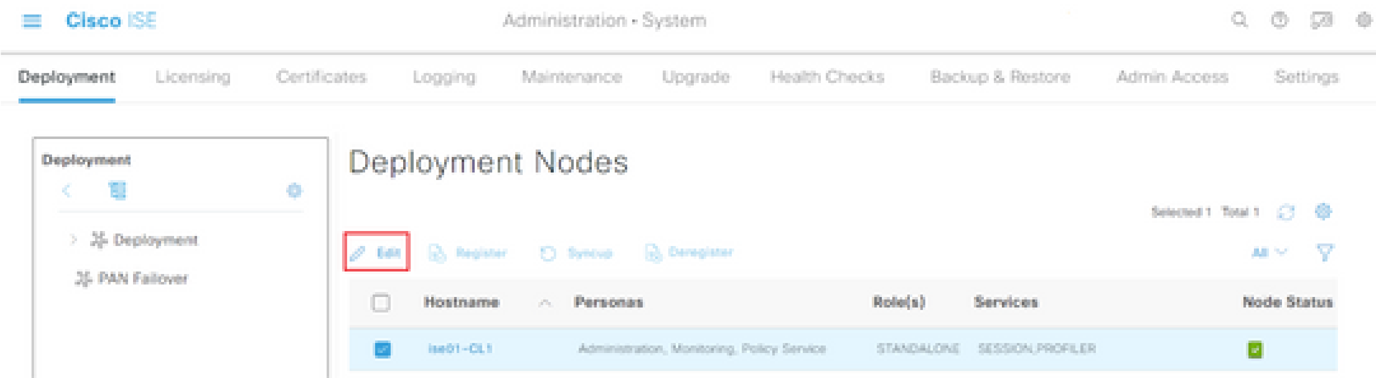
配置

ISE 配置

启用SXP

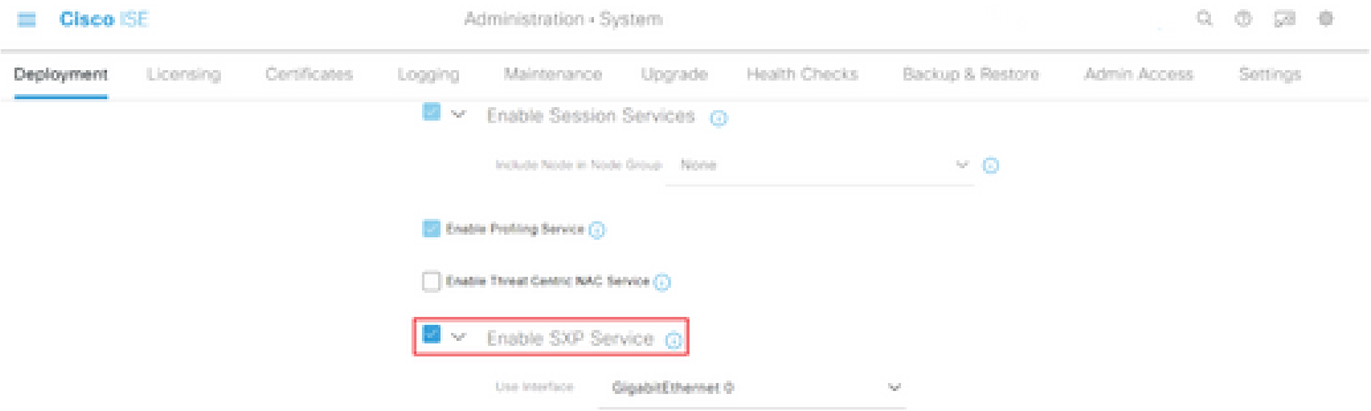
步骤1.选择三行图标 ☰ 位于左上角，在**Administration > System > Deployment**中选择。

步骤2.选择要配置的节点，然后点击**编辑。**



☐	Hostname	Personas	Role(s)	Services	Node Status
☑	ise01-CL1	Administration, Monitoring, Policy Service	STANDALONE	SESSION,PROFILER	✓

步骤3.要启用SXP，请勾选框**Enable SXP Service**



☑ Enable Session Services

Include Node in Node Group: None

☑ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface: GigabitEthernet 0

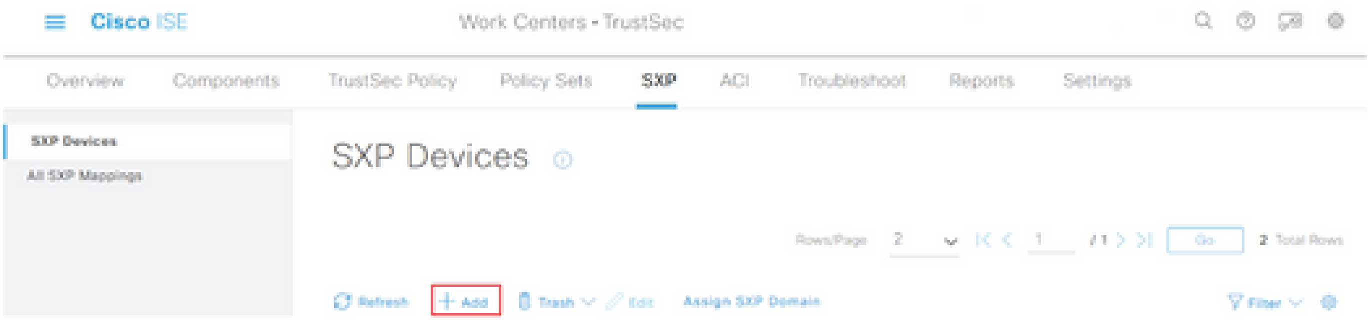
步骤4.向下滚动到底部，然后点击**保存**

注意：对每个集群中的其他ISE节点（包括汇聚节点）重复所有步骤。

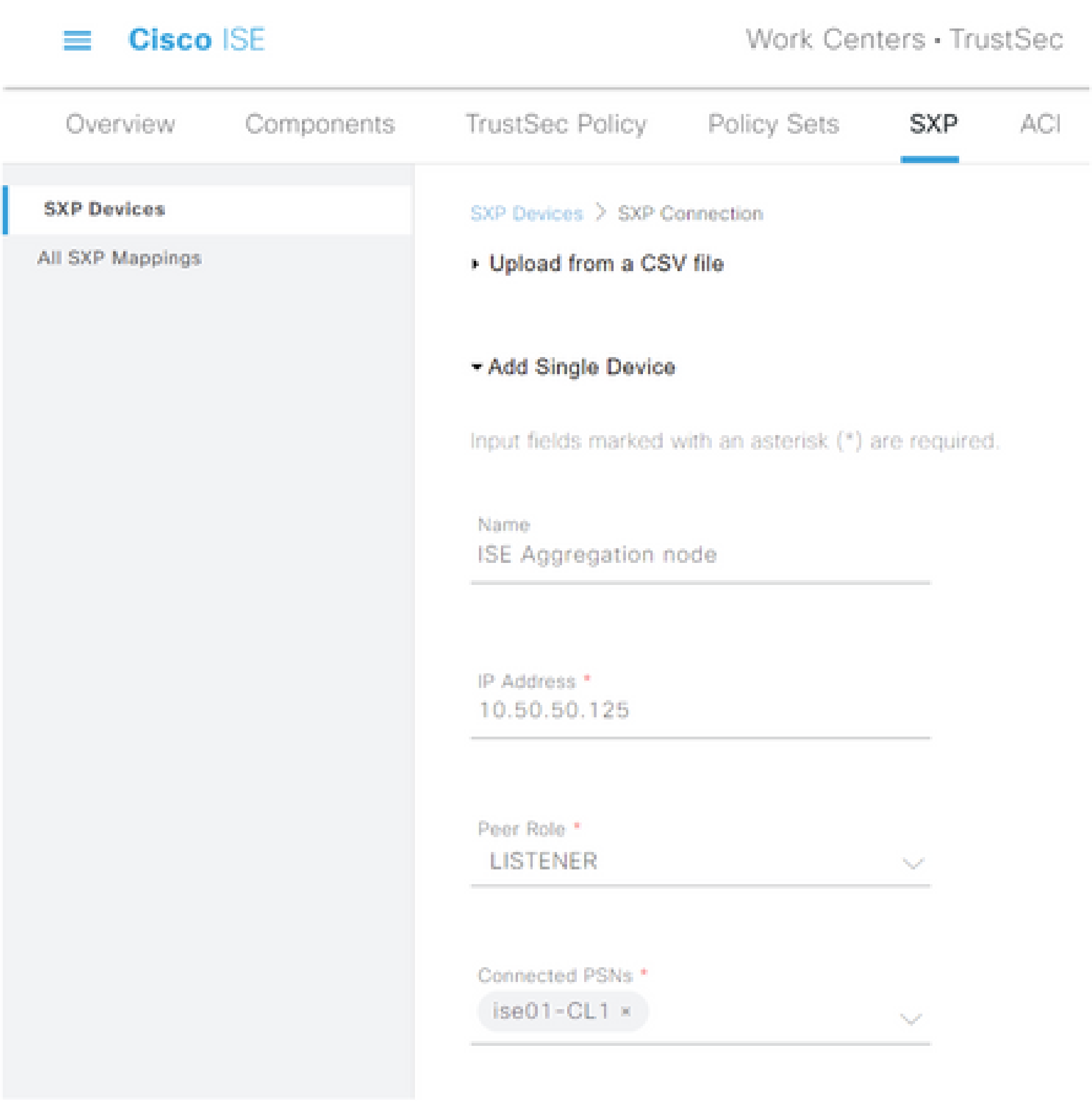
在群集节点上配置SXP

步骤1.选择三行图标 ☰ 位于左上角，然后选择 **工作中心> TrustSec > SXP。**

步骤2.点击**+Add**将ISE汇聚节点配置为SXP对等体。



步骤3.定义ISE聚**合节**点**的名**称和IP地址，选择对等角色作为**LISTENER**。在**连接的PSN**、所需的**SXP域**下选择所需的PSN，在“状态”下选择**启用**，然后选择**密码类型**和所需的**版本**。



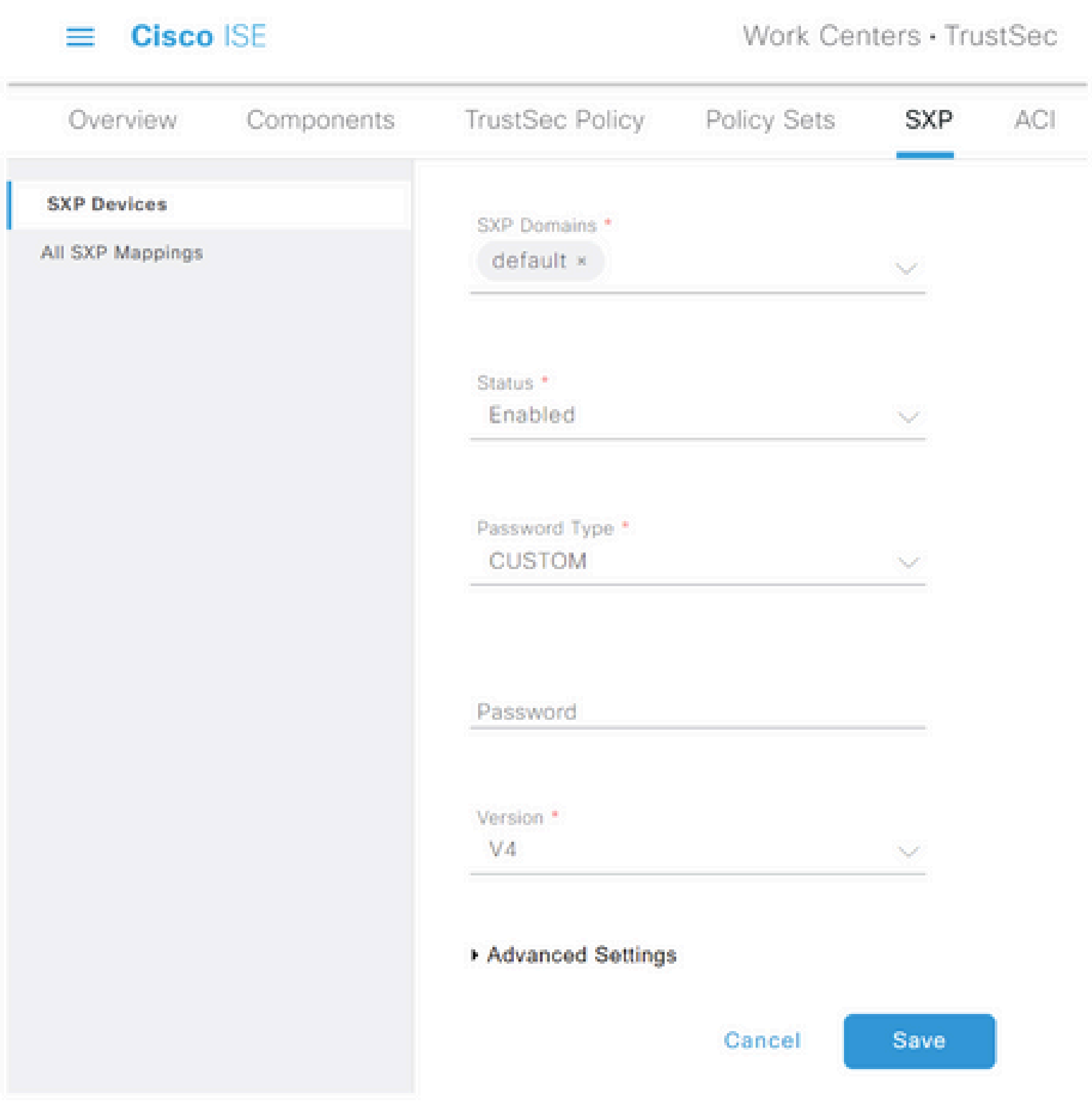
Input fields marked with an asterisk (*) are required.

Name
ISE Aggregation node

IP Address *
10.50.50.125

Peer Role *
LISTENER

Connected PSNs *
ise01-CL1 ×



SXP Domains * default ×

Status * Enabled

Password Type * CUSTOM

Password

Version * V4

步骤4.单击**保存**

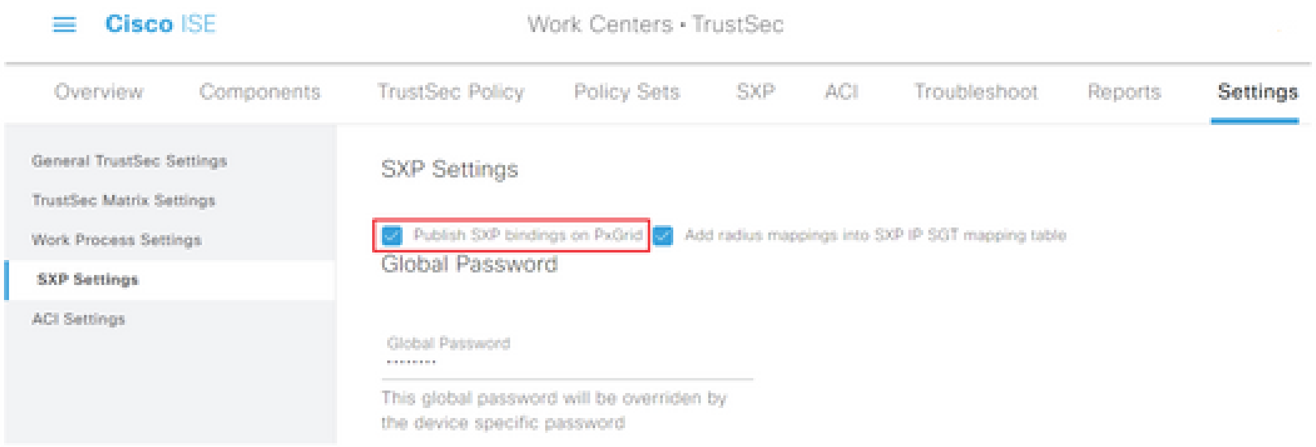
> **注意**：对每个集群中的其他ISE节点重复所有步骤，以构建与汇聚节点的SXP连接。**在汇聚节点上重复相同的过程，并选择SPEAKER作为对等角色。**

在汇聚节点上配置SXP

步骤1.选择位于左上角的三行图标，然后在“工作中心”>“**TrustSec”>“设置”中进行选择**

第二步： 单击**SXP Settings**选项卡

步骤3.要传播IP-SGT映射，请勾选**在pxGrid上发布SXP**绑定复选框。



SXP Settings

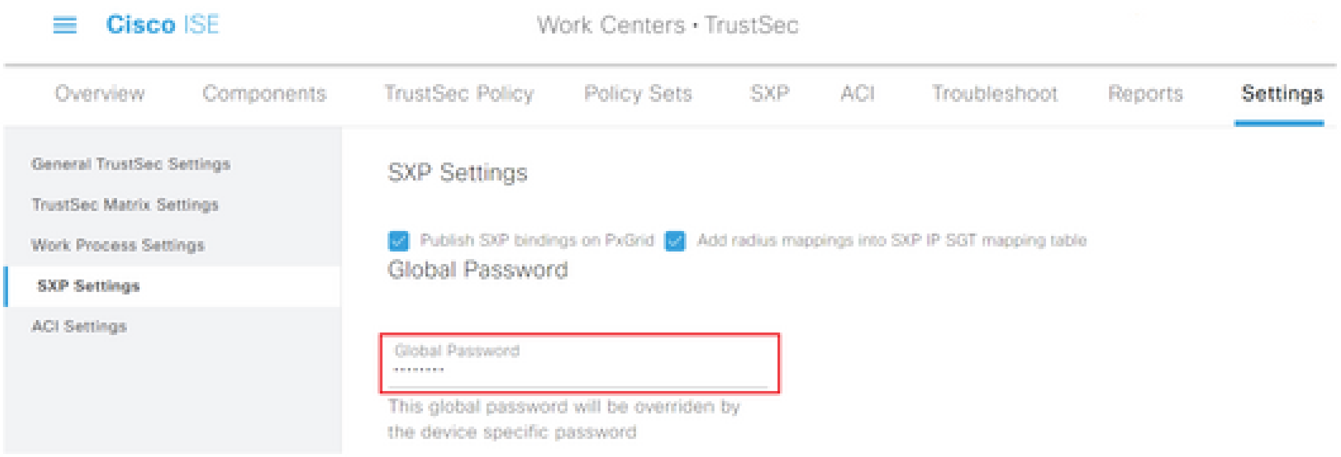
☑ Publish SXP bindings on PxGrid ☑ Add radius mappings into SXP IP SGT mapping table

Global Password

Global Password
········

This global password will be overriden by the device specific password

第 4 步（可选）： 在Global Password下定义SXP设置的默**认密码**



SXP Settings

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

Global Password

Global Password
········

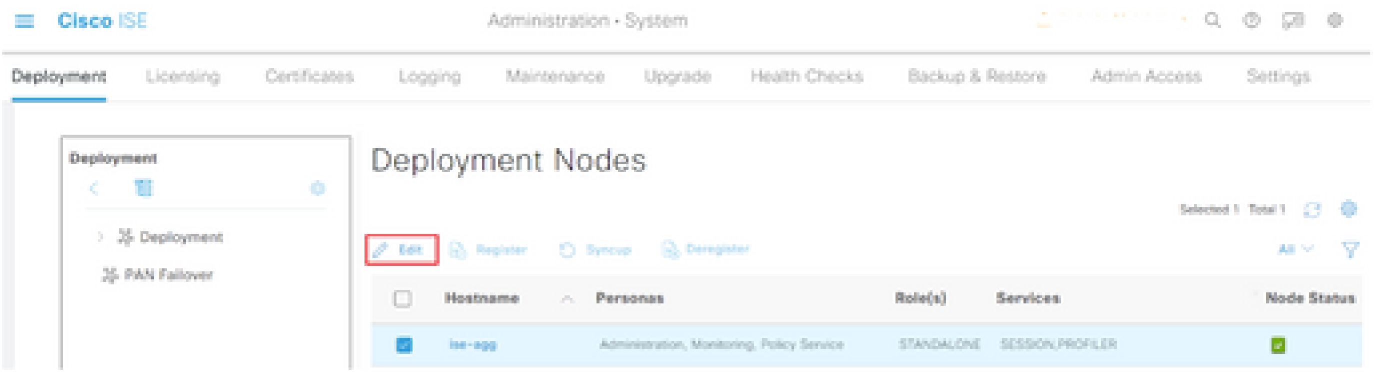
This global password will be overriden by the device specific password

步骤5.向下滚动并点击**保存。**

在聚合节点上启用pxGrid

第1步：选择位于左上角的三行图标，然后在**Administration > System > Deployment上选择。**

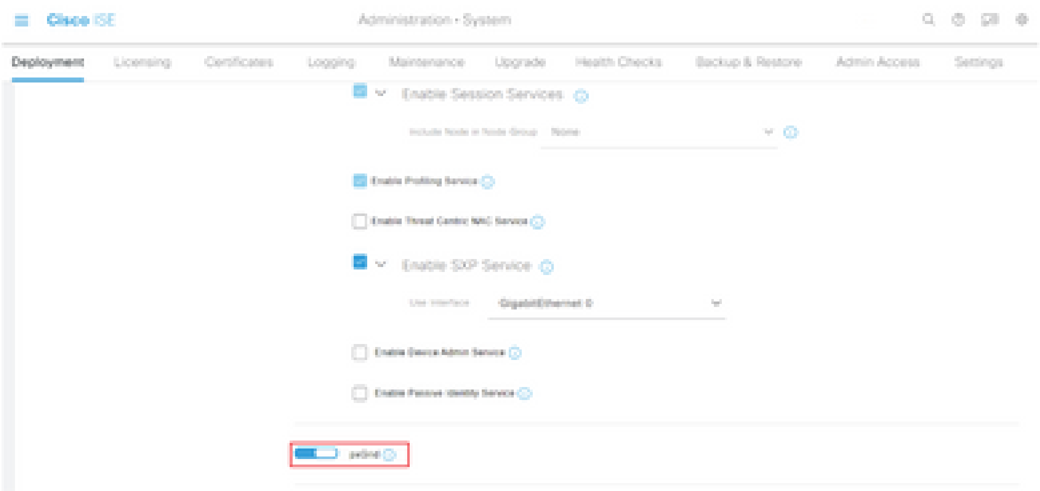
步骤2.选择要配置的节点，然后点击**编辑。**



Deployment Nodes

	Hostname	Personas	Role(s)	Services	Node Status
☑	ise-agg	Administration, Monitoring, Policy Service	STANDALONE	SESSION,PROFILER	🟩

步骤3.要启用pxGrid，请点击pxGrid旁边的按**钮。**



☑ Enable Session Services

Include Node in Node Group: None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface: GigabitEthernet 0

□ Enable Device Admin Service

□ Enable Passive Identity Service

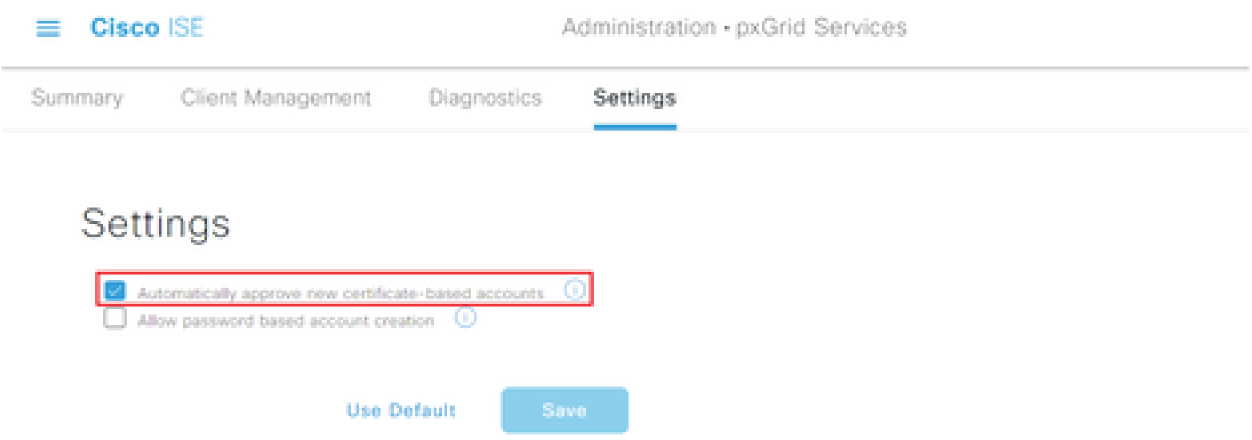
pxGrid (enabled)

步骤4.向下滚动到底部，然后点击**保存。**

pxGrid自动审批

第1步：导航到左上角的三行图标并选择**管理> pxGrid服务>设置。**

第二步： 默认情况下，ISE不会自动批准pxGrid来自新pxGrid客户端的连接请求，因此必须通过选中**Automatically approve new certificate-based accounts复选框启用该设置。**



Settings

☑ Automatically approve new certificate-based accounts

□ Allow password based account creation

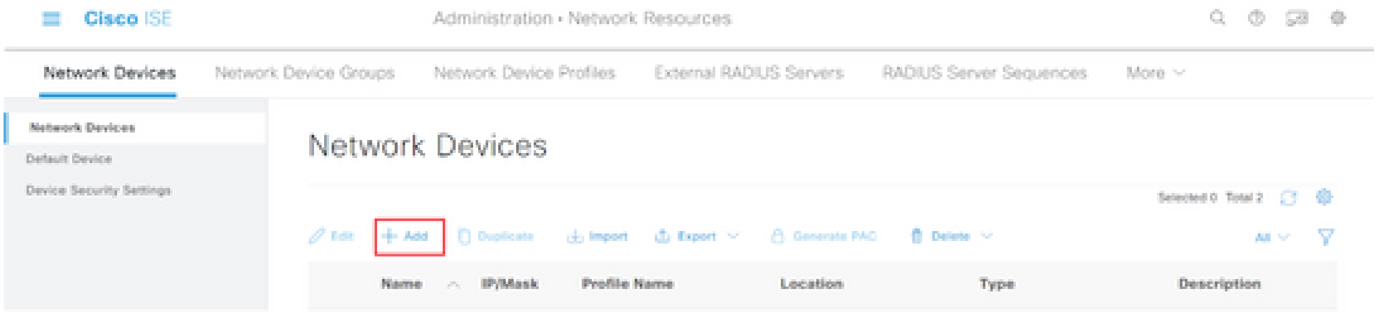
步骤3.点击**保存**

网络设备TrustSec设置

对于思科ISE处理来自支持TrustSec的设备请求，您必须在思科ISE中定义这些支持TrustSec的设备。

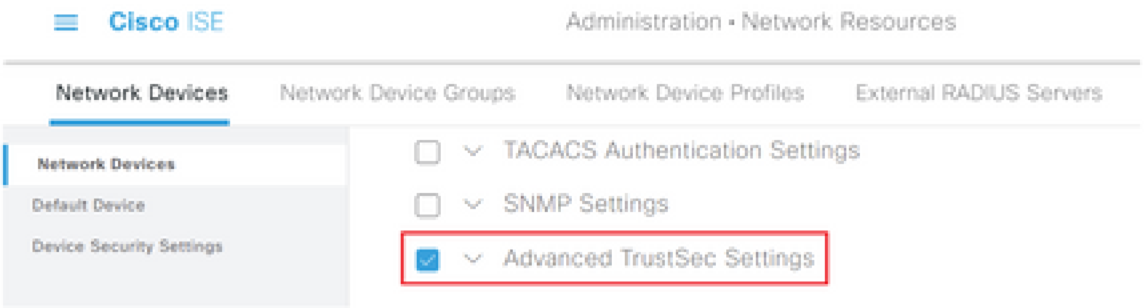
步骤1.导航至位于左上角的三个行图标，然后在**Administration > Network Resources > Network Devices中选择。**

第二步： 单击**+Add。**



步骤3.在Network Devices部分和**RADIUS Authentication Settings**中输入所**需的信息。**

步骤4.选中**Advanced TrustSec Settings**复选框以配置启用TrustSec的设备。

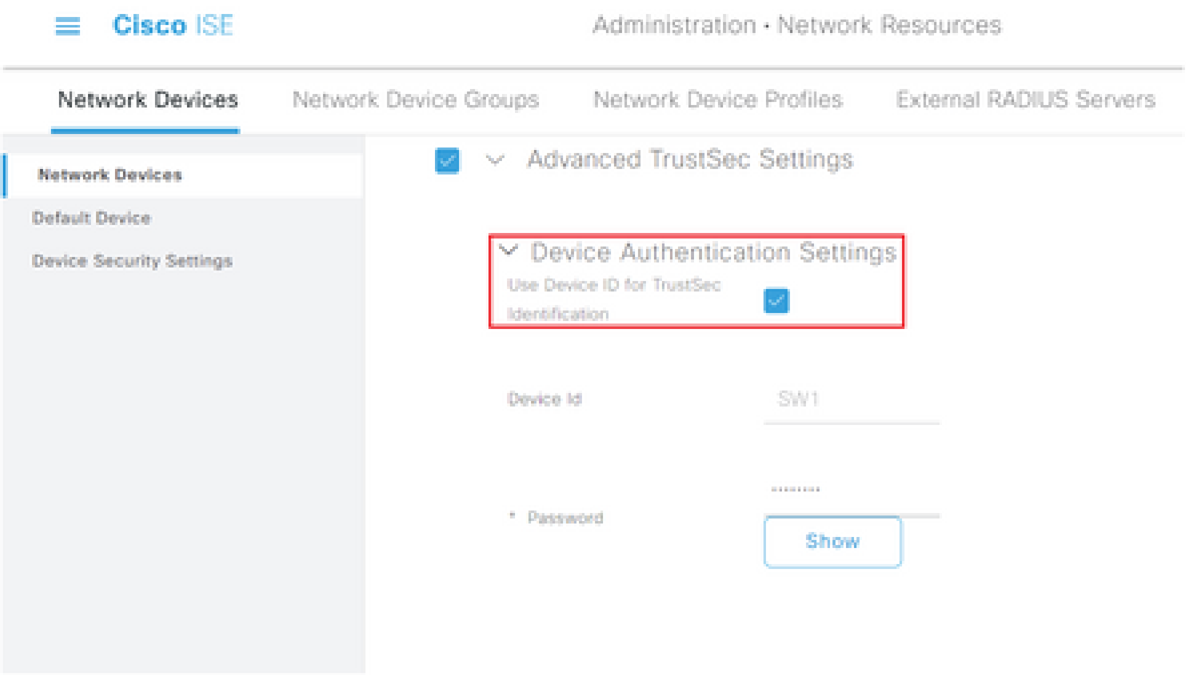


□ TACACS Authentication Settings

□ SNMP Settings

☑ Advanced TrustSec Settings

第5步：点击**Use Device ID for TrustSec Identification复选框**，以自动填充**Network Devices**（网络设备）部分中列出**的设备**名称。在**密码**字段中输入密码。



☑ Advanced TrustSec Settings

Device Authentication Settings

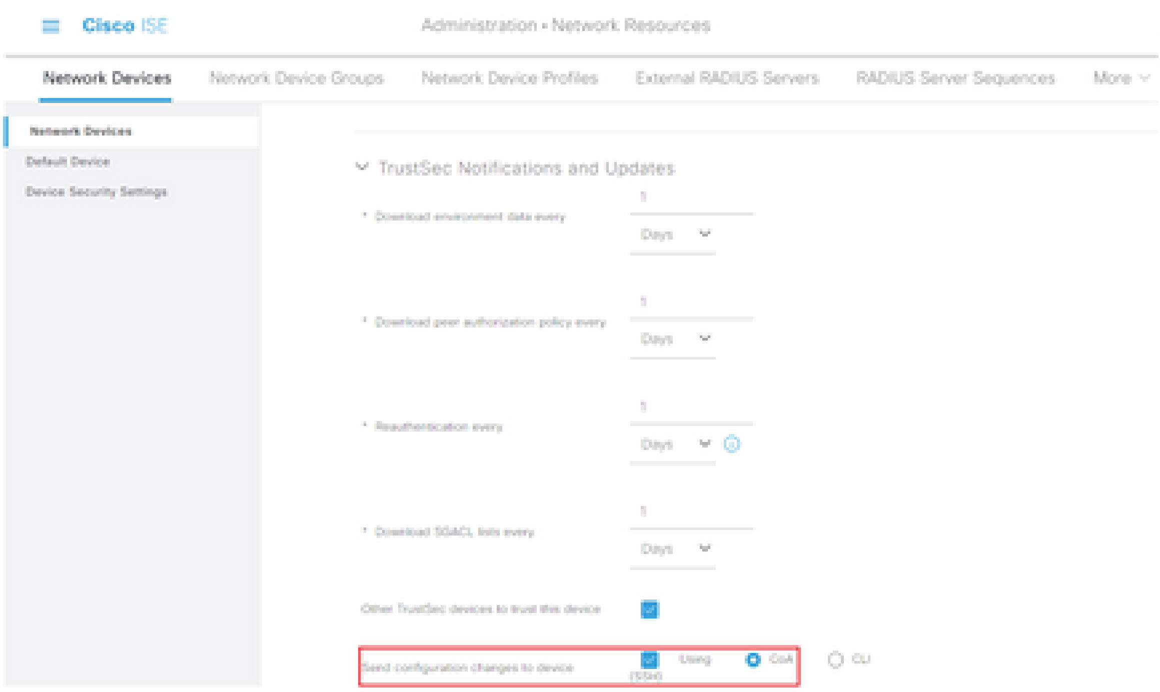
Use Device ID for TrustSec Identification ☑

Device Id SW1

* Password ········

注意：ID和密码必须与随后在交换机上配置的“cts credentials id <ID> password <PW>”命令匹配。

步骤6.选中**Send configuration changes to device复**选框，以便ISE可以向设备发送TrustSec CoA通知。



TrustSec Notifications and Updates

* Download environment data every 1 Days
* Download peer authorization policy every 1 Days
* Reauthentication every 1 Days
* Download SGACL lists every 1 Days

Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ● CoA ○ CLI (SSH)

步骤7.选中**Include this device when deploying Security Group Tag Mapping Updates复**选框。

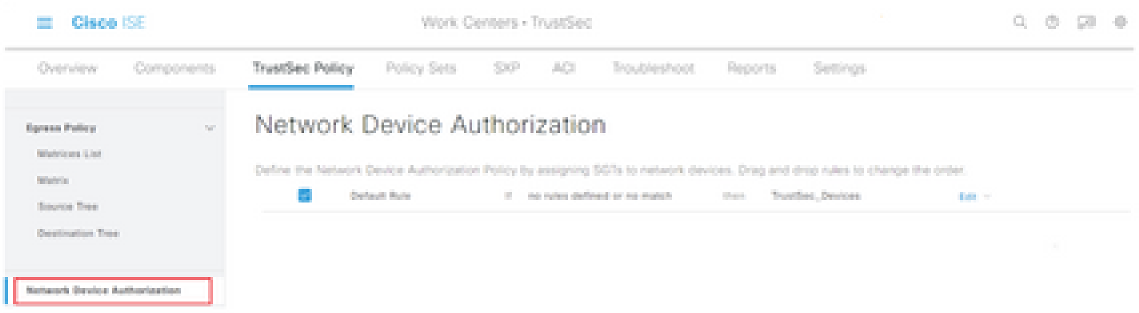
步骤8.要让ISE编辑网络设备的配置，请在**EXEC Mode Username**和**EXEC Mode Password字段中输入**用**户凭**证。或者，在**启用模式密码**字段中提供启用密码。

注意：对要成为TrustSec域一部分的所有其他NAD重复上述步骤。

网络设备授权

第1步：选择位于左上角的三行图标，然后依次选择工作中心(**Work Centers)> TrustSec > TrustSec策略(TrustSec Policy)。**

第二步： 在左侧窗格中，单击**网络设备授权。**

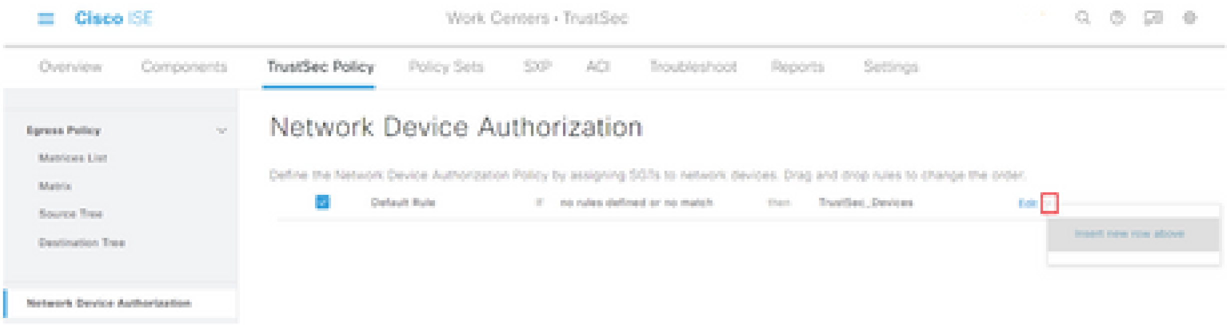


Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

☑ Default Rule If no rules defined or no match then TrustSec_Devices Edit

步骤3.在右侧，使用上文**Edit 和Insert new row 旁边的下拉列表创建新的NDA规则。**



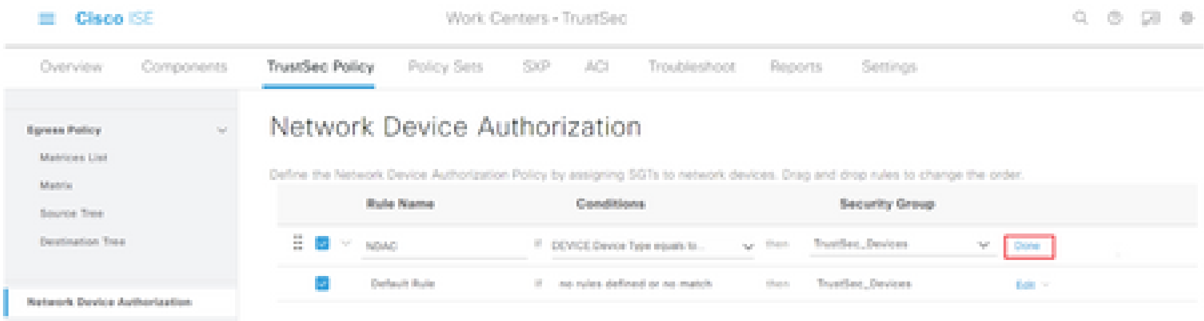
Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

☑ Default Rule if no rules defined or no match then TrustSec_Devices

第4步：定义规**则名称、条**件，并从**Security Groups下的下拉列表选择适当的SGT。**

步骤5.点击最右边的**完成。**



Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

Rule Name		Conditions		Security Group
☑ NDAC	if	DEVICE:Device Type equals to...	then	TrustSec_Devices
☑ Default Rule	if	no rules defined or no match	then	TrustSec_Devices

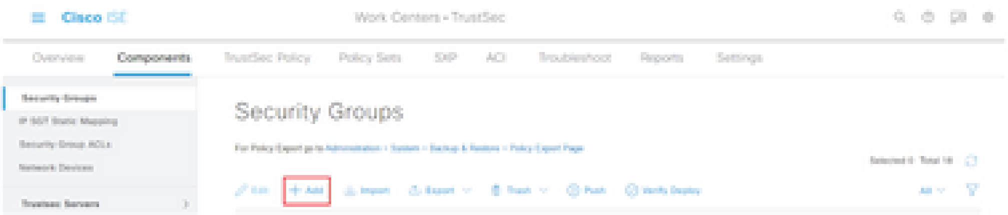
步骤6.向下滚动并点击**保存。**

SGT

第1步：选择位于左上角的三行图标，然后在“工作中心”(**Work Centers)>“TrustSec”(TrustSec)>“组件”(Components)中选择。**

第二步： 在左侧窗格中，展开**Security Groups**。

步骤3.点击**+Add**以创建新的SGT。

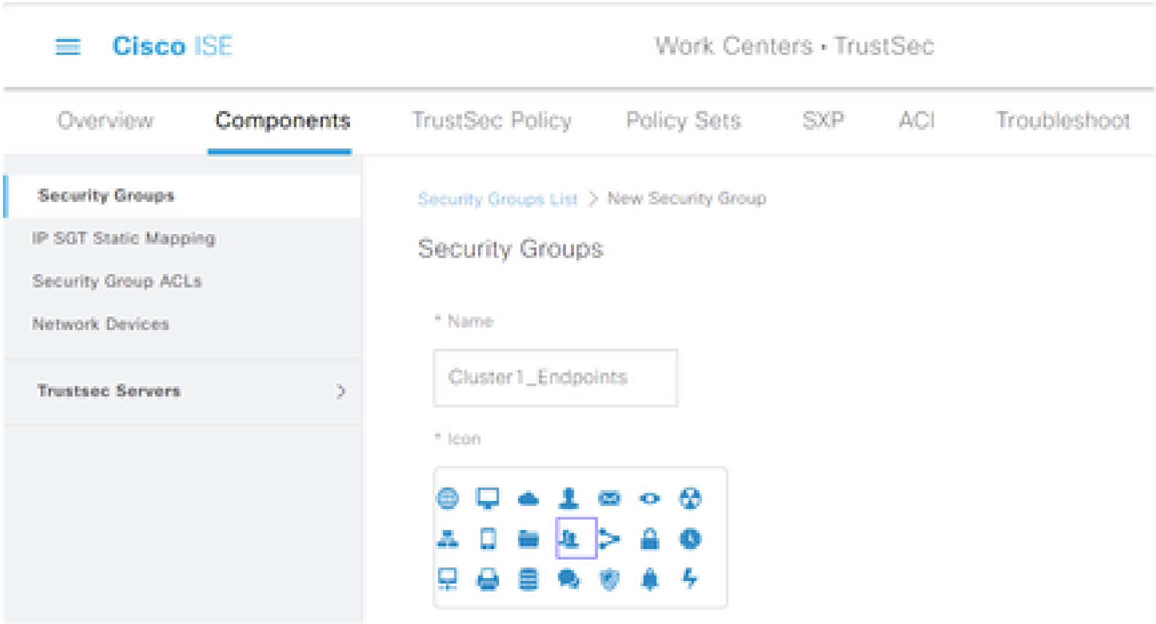


Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 18

步骤4.输入名称，然后在相应字段中选择一个图标。



* Name

Cluster1_Endpoints

步骤5.(可选)为其提供说明并输入**标记值。**

> **注意：**为了能够手动输入标记值，导航到工作中心(Work Centers)> TrustSec >设置(Settings)> General TrustSec设置(General TrustSec Settings)，并选择安全组标记编号(**Security Group Tag Numbering)下的选项User Must Enter SGT Number**。

步骤6.向下滚动并点击**Submit**

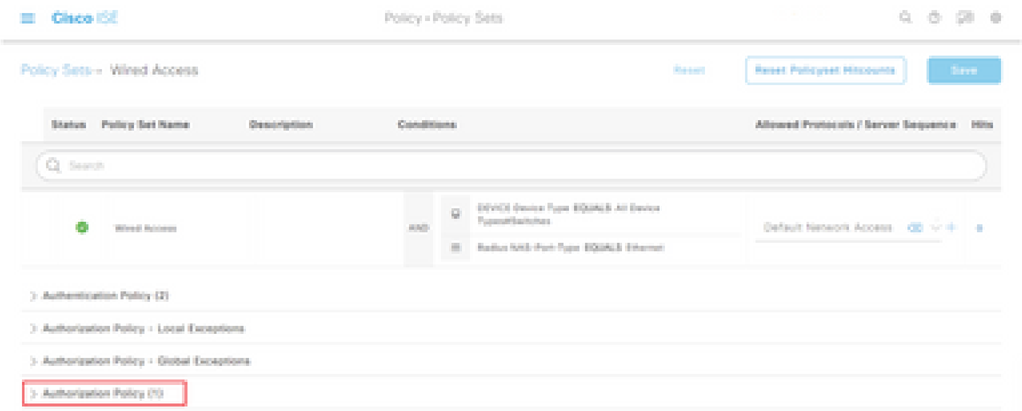
> **注意：**对所有必需的SGT重复这些步骤。

授权策略

第1步：选择位于左上角的三行图标，然后在**Policy > Policy Sets中选择。**

第二步： 选择适当的策略集。

步骤3.在策略集中，展开授**权策略。**



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Wired Access		AND DEVICE·Device Type EQUALS All Device Types#Switches Radius·NAS-Port-Type EQUALS Ethernet	Default Network Access	

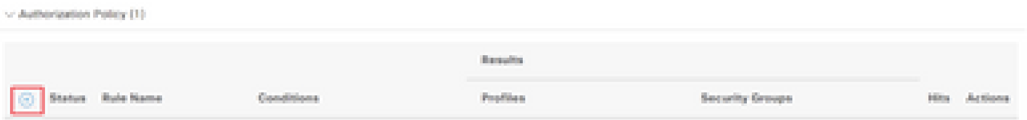
> Authentication Policy (2)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

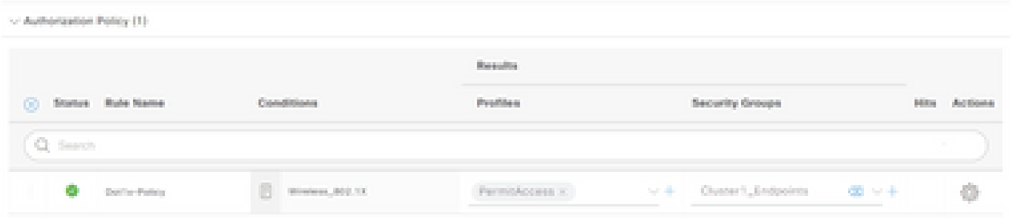
> Authorization Policy (1)

步骤4.单击 ⊕ 按钮以创建授**权策略。**



⊕	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions

第5步：定义所需的**规则名称、条件**和配置**文**件，然后从**Security Groups下的下拉列表中选择适当的SGT。**



⊕	Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
	●	Dot1x-Policy	Wireless_802.1X	PermitAccess ×	Cluster1_Endpoints		⚙

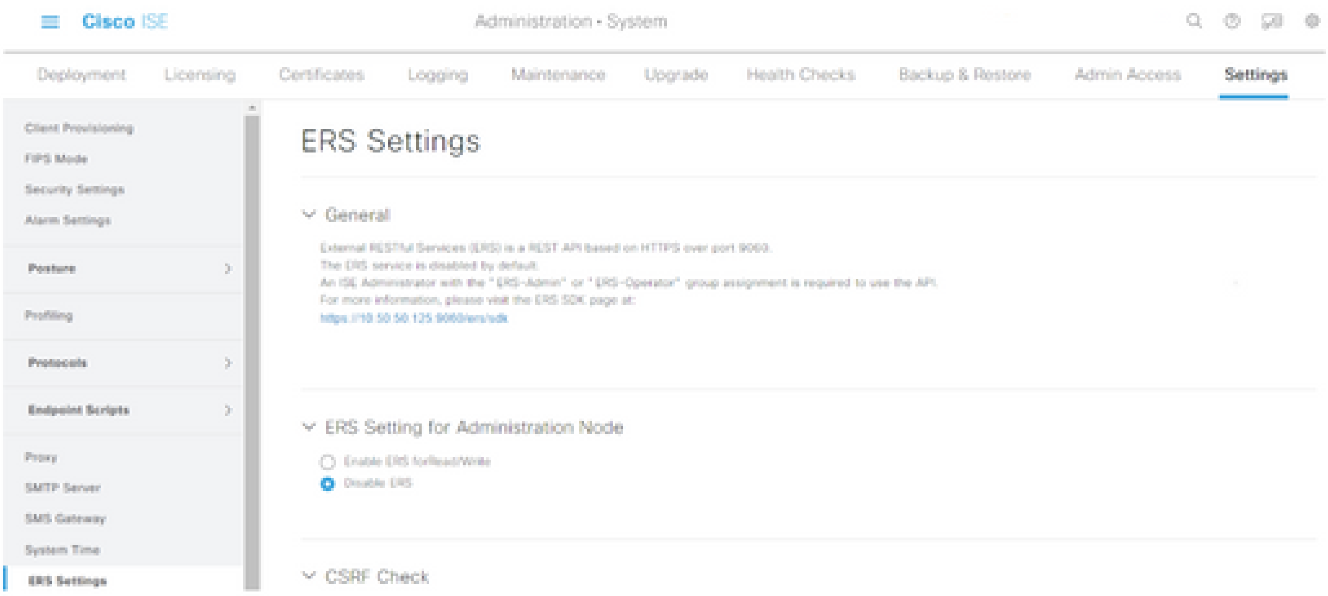
步骤6.点击**保存。**

在ISE汇聚节点上启用ERS（可选）

外部RESTful API服务(ERS)是WSA可以查询组信息的API。默认情况下，ISE上禁用ERS服务。启用后，如果客户端作为ISE节点上的**ERS Admin组成员进行身份验证，则可**以查询API。要在ISE上启用服务并将帐户添加到正确的组，请执行以下步骤：

步骤1.选择位于左上角的三行图标，然后在**Administration > System > Settings上选择。**

第二步： 在左侧窗格中，单击**ERS Settings**。



ERS Settings

General

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060.
The ERS service is disabled by default.
An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API.
For more information, please visit the ERS SDK page at:
https://10.50.50.125:9060/ers/sdk

ERS Setting for Administration Node

○ Enable ERS for Read/Write
● Disable ERS

CSRF Check

步骤3.选择选项**Enable ERS for Read/Write。**

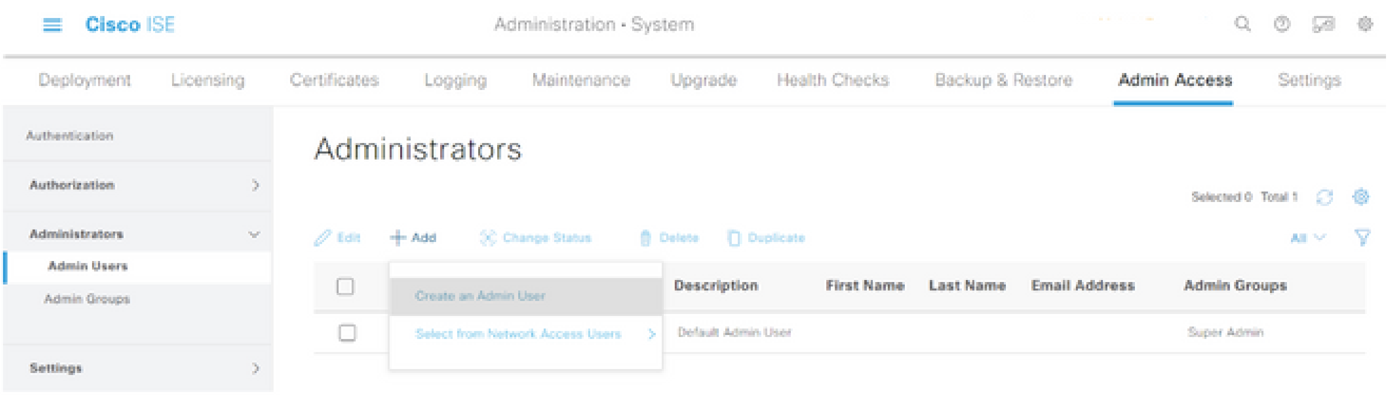
步骤4.单击**保存**并使用OK**确认。**

将用户添加到ESR管理员组（可选）

第1步：选择位于左上角的三行图标，然后选择**Administration > System > Admin Access**

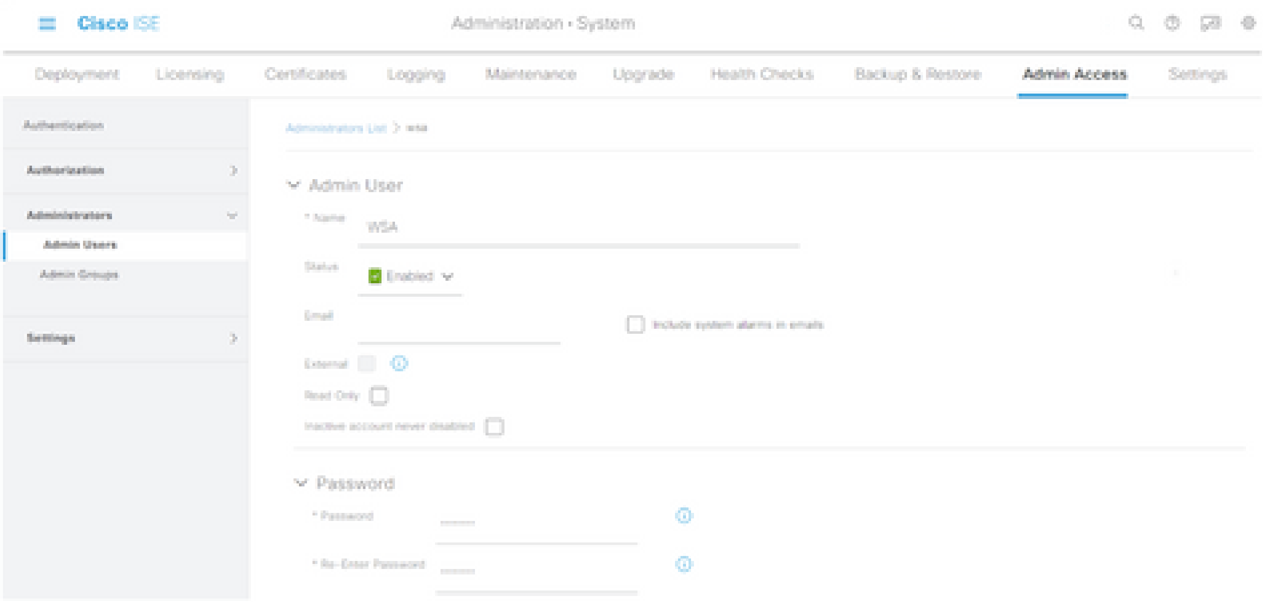
第二步： 在左侧窗格中，展开**Administrators**，然后单击**Admin Users。**

第3步：点击**+Add**并从下拉列表中选择**Admin User。**



	Description	First Name	Last Name	Email Address	Admin Groups
□	Default Admin User				Super Admin

步骤4.在相应的字段中输入用户名和密码。



Admin User

* Name WSA

Status ☑ Enabled

Email

□ Include system alarms in emails

External □

Read Only □

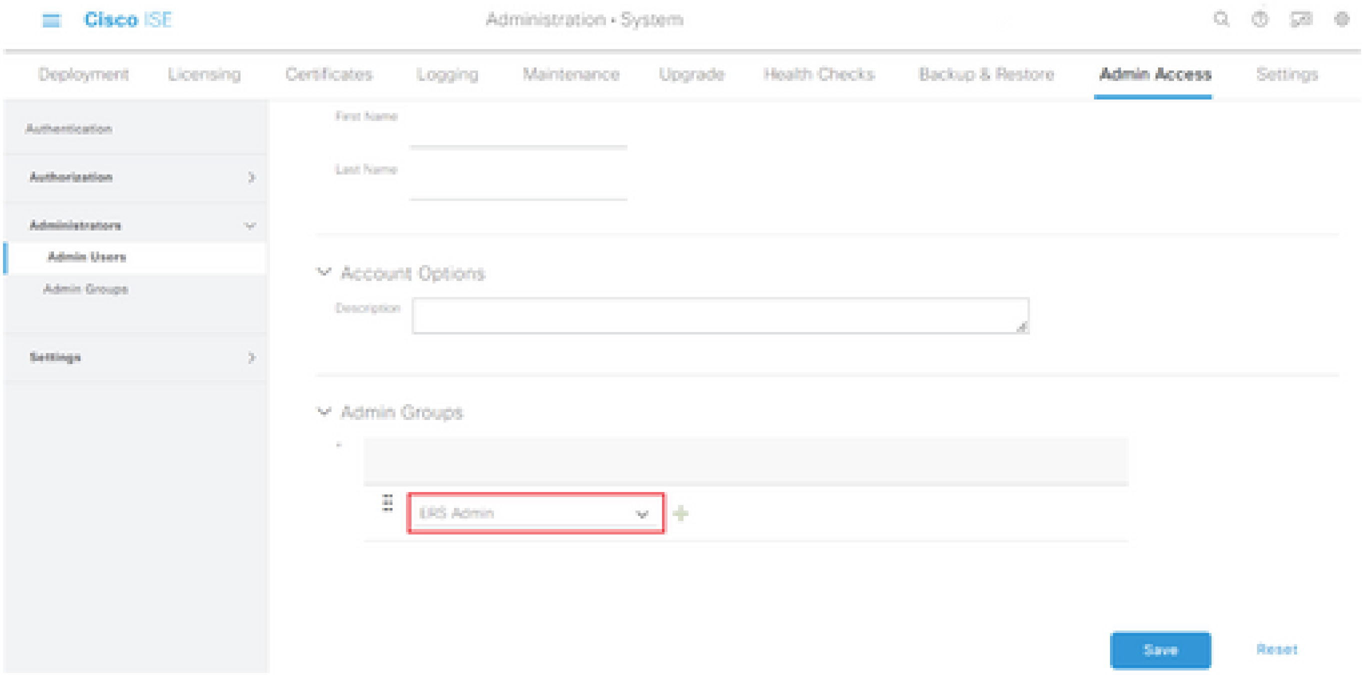
Inactive account never disabled □

Password

* Password ·······

* Re-Enter Password ·······

第5步：在**Admin Groups**字段中，使用下拉菜单选择**ERS Admin。**



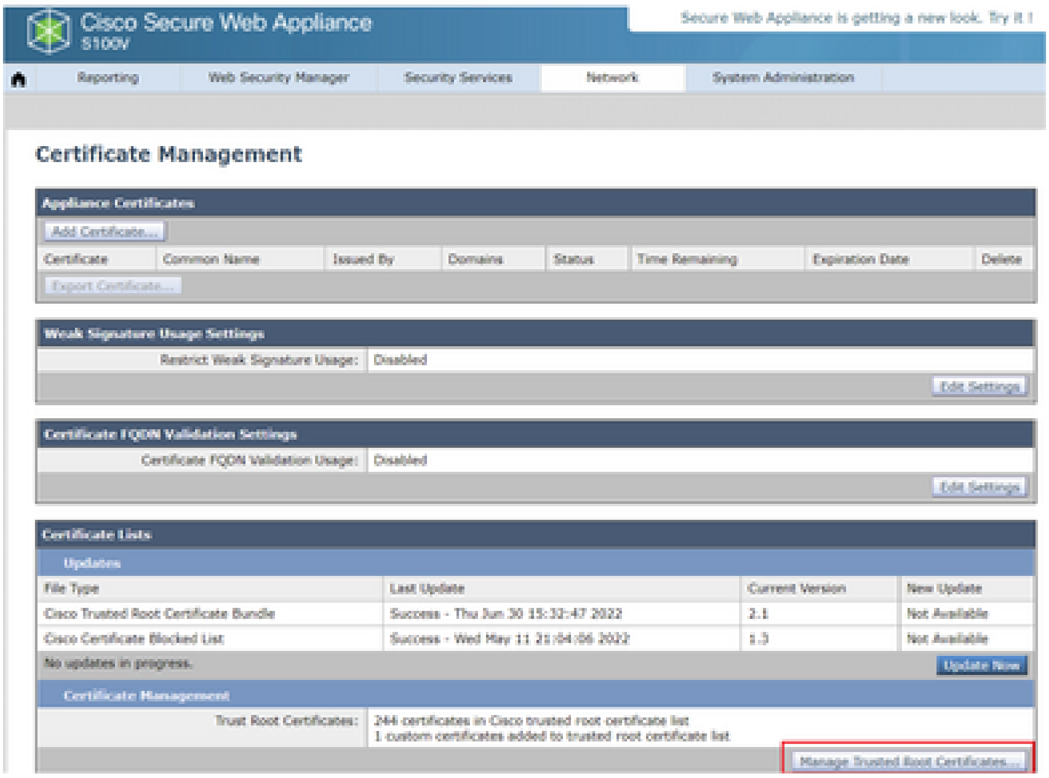
步骤6.点击**保存。**

安全Web设备配置

根证书

如果集成设计使用内部证书颁发机构作为WSA和ISE之间的连接的信任根，则必须在两台设备上安装此根证书。

第1步：导航到**Network > Certificate Management，然后单击Manage Trusted Root Certificates以添加CA证书。**



Appliance Certificates

Certificate	Common Name	Issued By	Domains	Status	Time Remaining	Expiration Date	Delete

Weak Signature Usage Settings

Restrict Weak Signature Usage: Disabled

Certificate FQDN Validation Settings

Certificate FQDN Validation Usage: Disabled

Certificate Lists

Updates

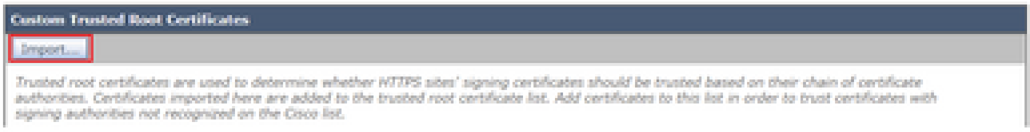
File Type	Last Update	Current Version	New Update
Cisco Trusted Root Certificate Bundle	Success - Thu Jun 30 15:32:47 2022	2.1	Not Available
Cisco Certificate Blocked List	Success - Wed May 11 21:04:06 2022	1.3	Not Available

No updates in progress.

Certificate Management

Trust Root Certificates: 244 certificates in Cisco trusted root certificate list
1 custom certificates added to trusted root certificate list

步骤2.点击**导入。**



Custom Trusted Root Certificates

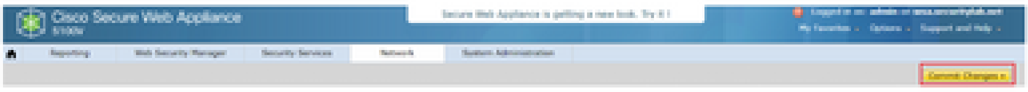
Import...

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.

步骤3.单击**Choose File**以查找生成的根CA，然后点击**Submit。**

步骤4.重新点**击Submit**。

步骤5.在右上角，点击**Commit Changes。**



步骤6.重新点**击Commit Changes**。

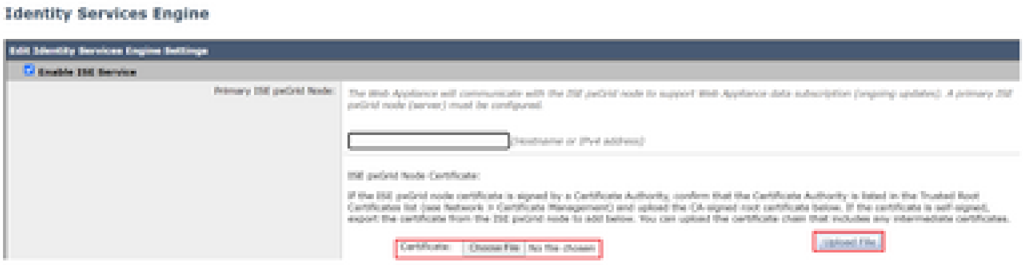
pxGrid证书

在WSA中，创建密钥对和证书供pxGrid使用作为ISE服务配置的一部分完成。

步骤1.导航到**网络>身份服务引擎。**

步骤2.单击**启用和编辑设置。**

步骤3.单击**Choose File**以查找生成的根CA，然后点击**Upload File。**



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 IPv4 address)

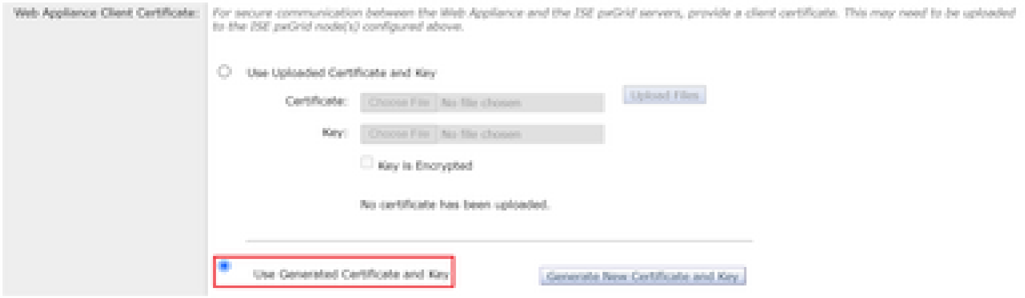
ISE pxGrid Node Certificate:

If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted 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

> **注意：**常见的错误配置是上载此部分中的ISE pxGrid证书。必须将根CA证书上传到ISE pxGrid节点证书字段。

第4步：在 Web设备**客户端证书**部分，选择**使用生成的证书和密钥。**



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 Files

Key: Choose File No file chosen

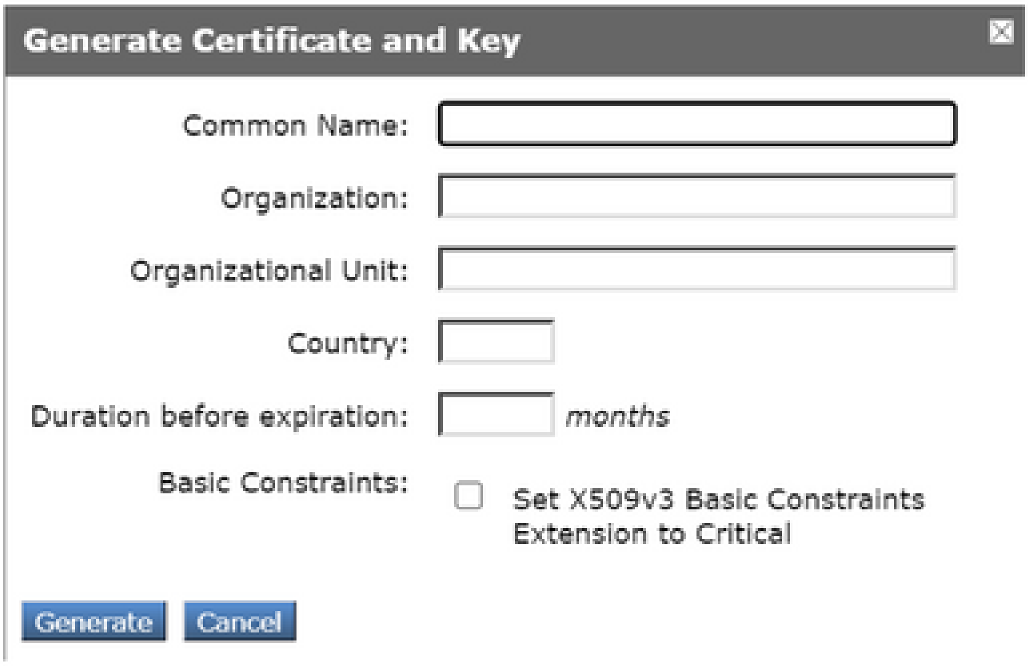
□ Key is Encrypted

No certificate has been uploaded.

● Use Generated Certificate and Key

Generate New Certificate and Key

第5步：单击**Generate New Certificate and Key按**钮并填写所需的证书字段。



Generate Certificate and Key

Common Name:

Organization:

Organizational Unit:

Country:

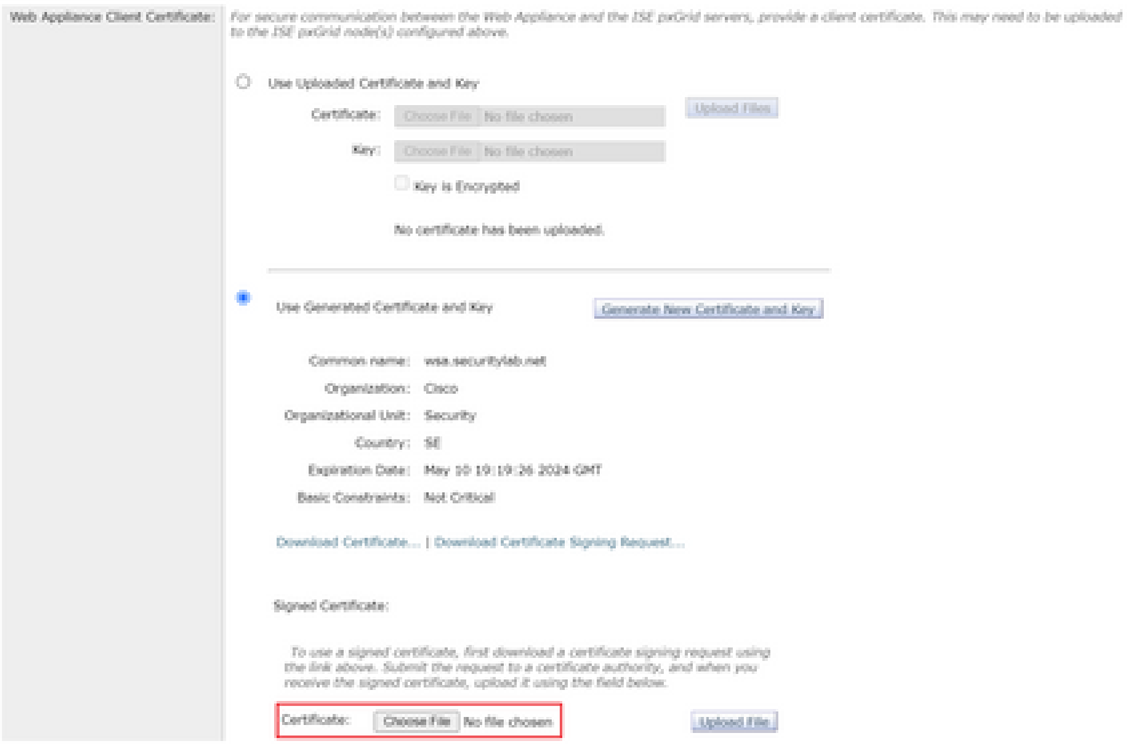
Duration before expiration: months

Basic Constraints: □ Set X509v3 Basic Constraints Extension to Critical

步骤6.点击**Download Certificate Signing Request。**

> **注意：**建议选择**Submit**按钮提交对ISE配置的更改。如果在提交更改之前会话超时，则即使已下载CSR，生成的密钥和证书也会丢失。

第7步：在与CA签署CSR后，点击**选择文件**以查找证书。



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

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

Signed Certificate:

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

Certificate: Choose File No file chosen

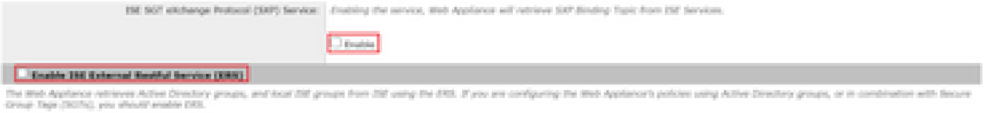
Upload Files
Generate New Certificate and Key
Download Certificate... | Download Certificate Signing Request...
Upload File

步骤8.点击**上传文件。**

步骤9.提交并**提交。**

在安全Web设备上启用SXP和ERS

步骤1.单击**SXP和**ERS的Enable按钮。



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

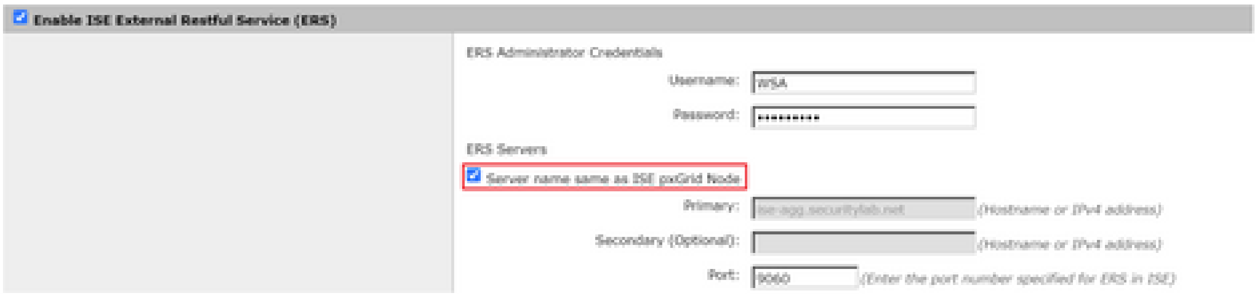
□ Enable

□ Enable ISE External Restful Service (ERS)

The Web Appliance retrieves Active Directory groups, and local ISE 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.

第2步：在**ERS Administrator Credentials字**段中，输入在ISE上配置的用户信息。

步骤3.选中与**ISE** pxGrid节点相同**的服务器名称的复选框**，以继承早期配置的信息。否则，请在此处输入所需信息。



☑ 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 number specified for ERS in ISE)

步骤4.提交并**提交。**

标识配置文件

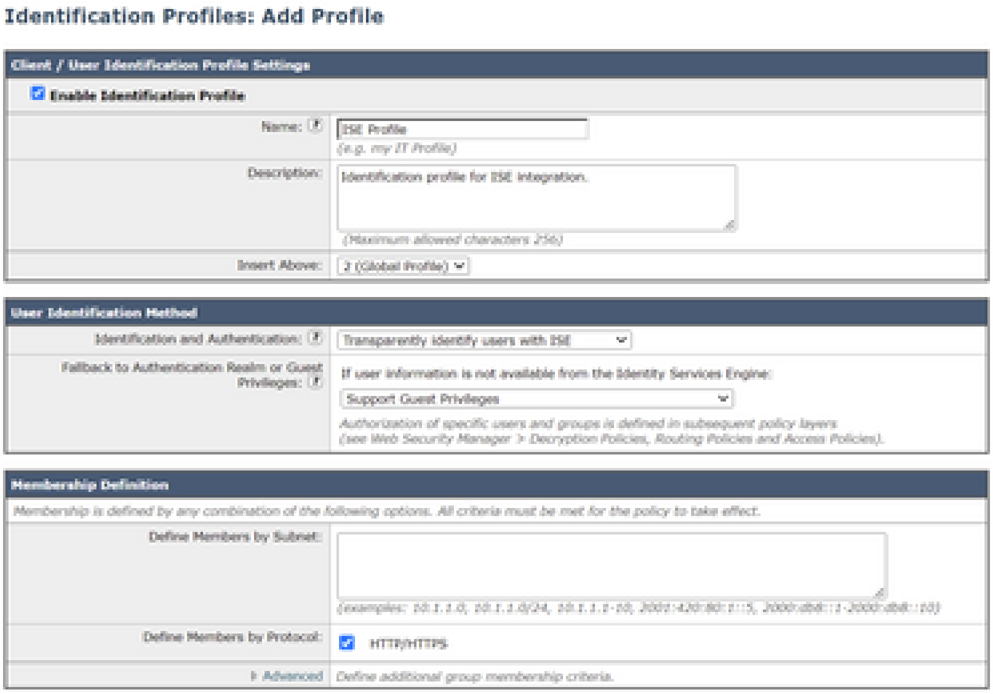
为了在WSA策略中使用安全组标记或ISE组信息，必须首先创建标识配置文件，该配置文件利用ISE作为透明标识用户的方法。

步骤1.导航到**Web Security Manager > Authentication > Identication Profiles。**

步骤2.单击**Add Identification Profile。**

步骤3.输入名称和说明（可选）。

第4步：在 Identification and **Authentication部分**，使用下拉菜单选择**Transparently identify users with ISE。**



Identification Profiles: Add Profile

Client / User Identification Profile Settings

☑ Enable Identification Profile

Name: ISE Profile (e.g. my IT Profile)

Description: Identification profile for ISE integration. (Maximum allowed characters 256)

Insert Above: 2 (Global Profile)

User Identification Method

Identification and Authentication: Transparently identify users with ISE

Fallback to Authentication Realm or Guest Privileges: If user information is not available from the Identity Services Engine: Support Guest Privileges

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

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: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol: ☑ HTTP/HTTPS

Advanced: Define additional group membership criteria.

步骤5.提交并提交。

基于SGT的解密策略

步骤1.导航到Web Security Manager > Web Policies > Decryption Policies。

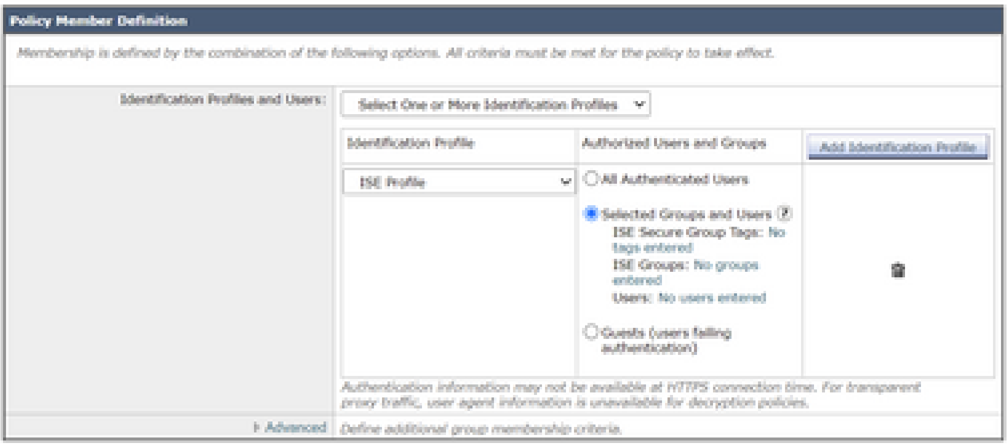
步骤2.点击**Add Policy。**

步骤3.输入名称和说明（可选）。

第4步：在标识配**置文件和用户**部分，使用下拉菜单选择选择一个**或多个标识配置文件。**

第5步：在**Identification Profiles**部分，使用下拉列表选择ISE标识配置文件的名称。

第6步：在 Authorized **Users and Groups部分**，选择**Selected Groups and Users。**



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

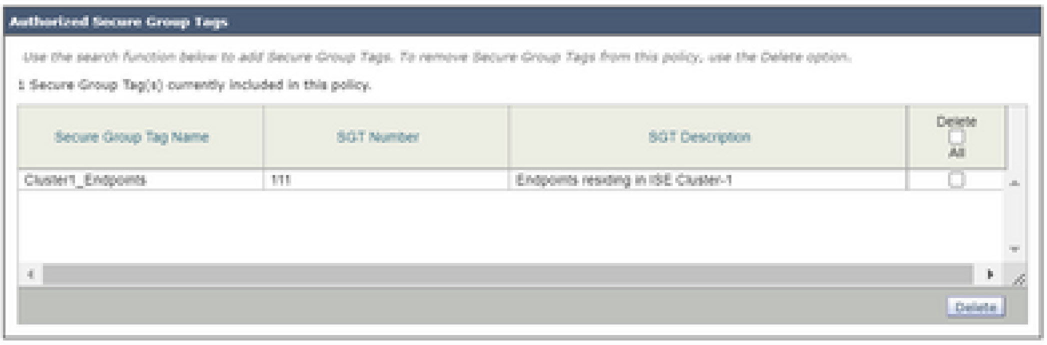
Identification Profile	Authorized Users and Groups	Add Identification Profile
ISE Profile	○ All Authenticated Users ● Selected Groups and Users ISE Secure Group Tags: No tags entered ISE Groups: No groups entered Users: No users entered ○ Guests (users failing authentication)	🗑

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.

步骤7.点击**ISE Secure Group Tags**旁边的**超链接。**

第8步：在**Secure Group Tag Search**部分，选中所需SGT右侧的框，然后点击**Add。**

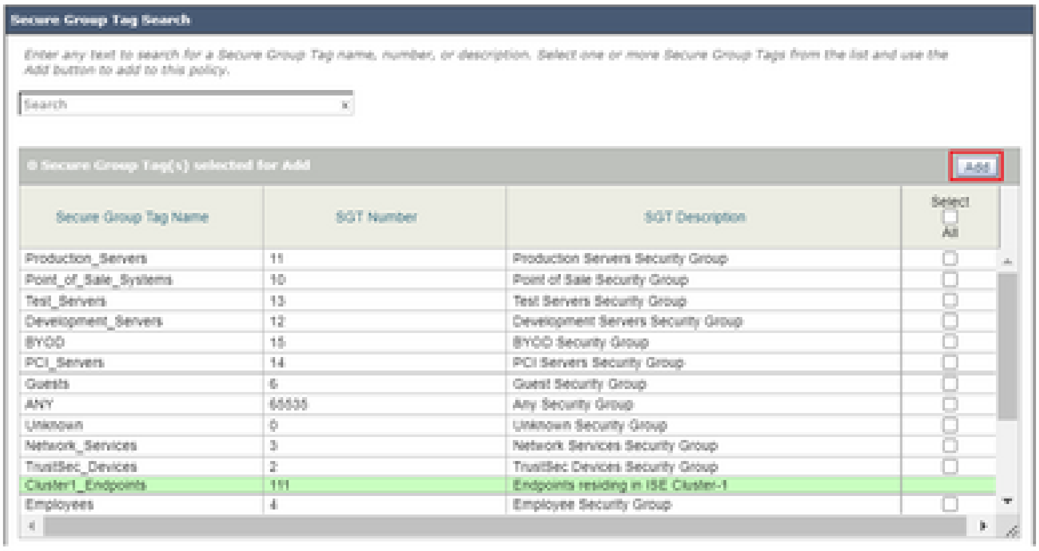


Authorized Secure Group Tags

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 □ All
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	□



Secure Group Tag Search

Enter any text to search for a Secure Group Tag name, number, or description. Select one or more Secure Group Tags from the list and use the Add button to add to this policy.

Secure Group Tag Name	SGT Number	SGT Description	Select □ All
Production_Servers	11	Production Servers Security Group	□
Point_of_Sale_Systems	10	Point of Sale Security Group	□
Test_Servers	13	Test Servers Security Group	□
Development_Servers	12	Development Servers Security Group	□
BYOD	15	BYOD Security Group	□
PCI_Servers	14	PCI Servers Security Group	□
Guests	6	Guest Security Group	□
ANY	65535	Any Security Group	□
Unknown	0	Unknown Security Group	□
Network_Services	3	Network Services Security Group	□
TrustSec_Devices	2	TrustSec Devices Security Group	□
Cluster1_Endpoints	111	Endpoints residing in ISE Cluster-1	
Employees	4	Employee Security Group	□

步骤9.单击“**完成**”返回。

步骤10.提交并**提交。**

交换机配置

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
```

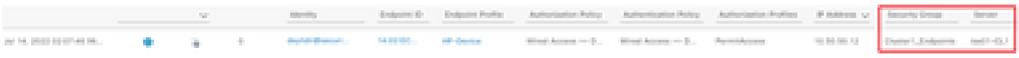
TrustSec

```
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
```

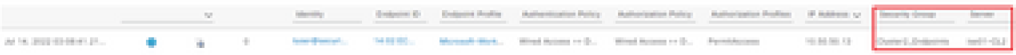
验证

从ISE到终端的SGT分配。

在这里，您可以看到来自ISE集群1的终端在成功身份验证和授权后分配了SGT:

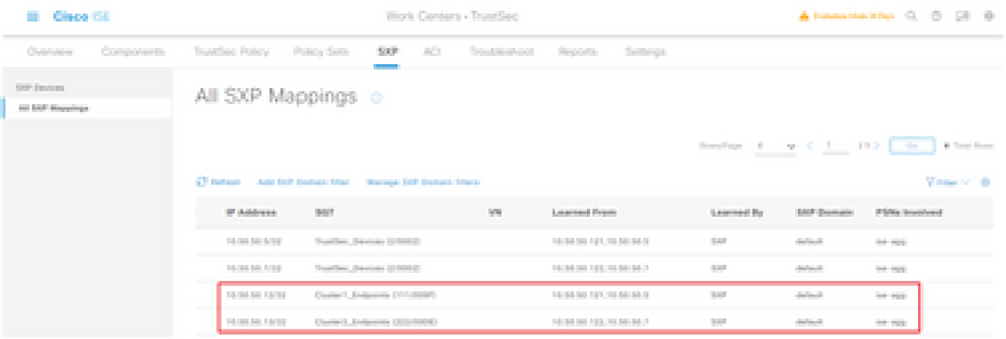


在这里，您可以看到来自ISE集群2的终端在成功身份验证和授权后分配了SGT:

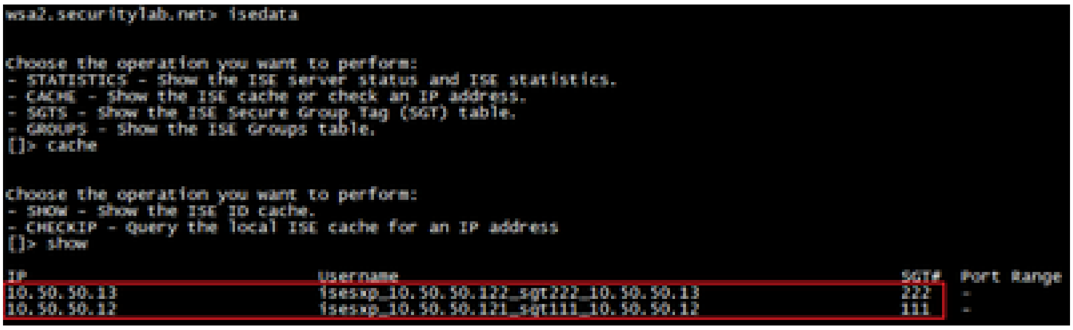


SXP映射

由于群集ISE节点和ISE汇聚节点之间启用了SXP通信，这些SGT-IP映射通过SXP通过ISE汇聚获取：



这些SXP映射来自不同的ISE集群，然后通过pxGrid通过ISE汇聚节点发送到WSA:

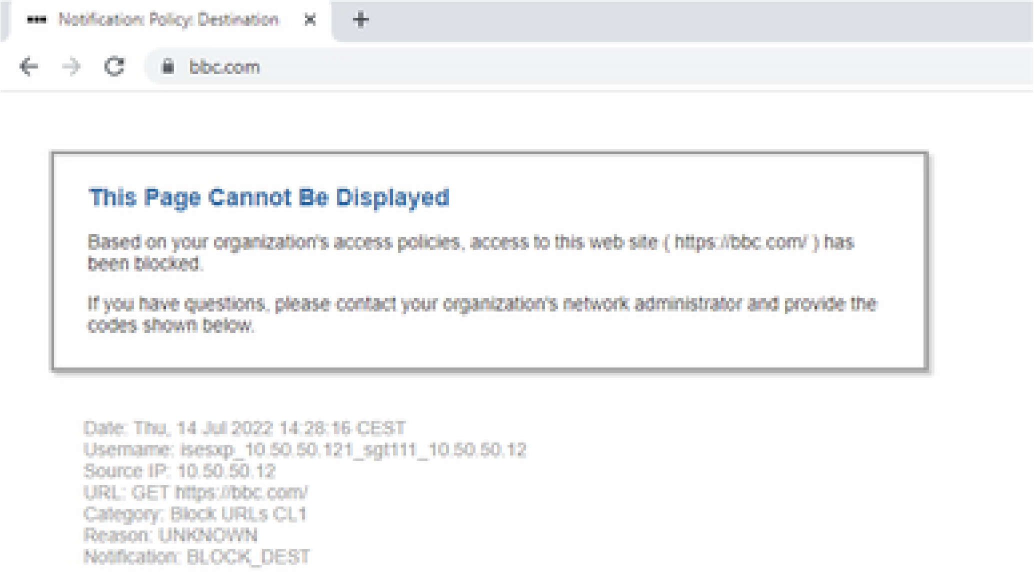


```
wsa2.securitylab.net> isedata

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                isesxp_10.50.50.122_sgt222_10.50.50.13        222   -
10.50.50.12                isesxp_10.50.50.121_sgt111_10.50.50.12        111   -
```

基于SGT的策略实施

在这里，您可以看到不同的终端与其各自的策略匹配，并且根据其SGT阻止流量：

属于ISE集群1的终端

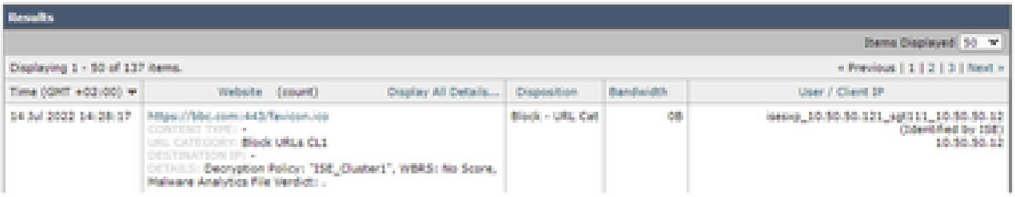


This Page Cannot Be Displayed

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

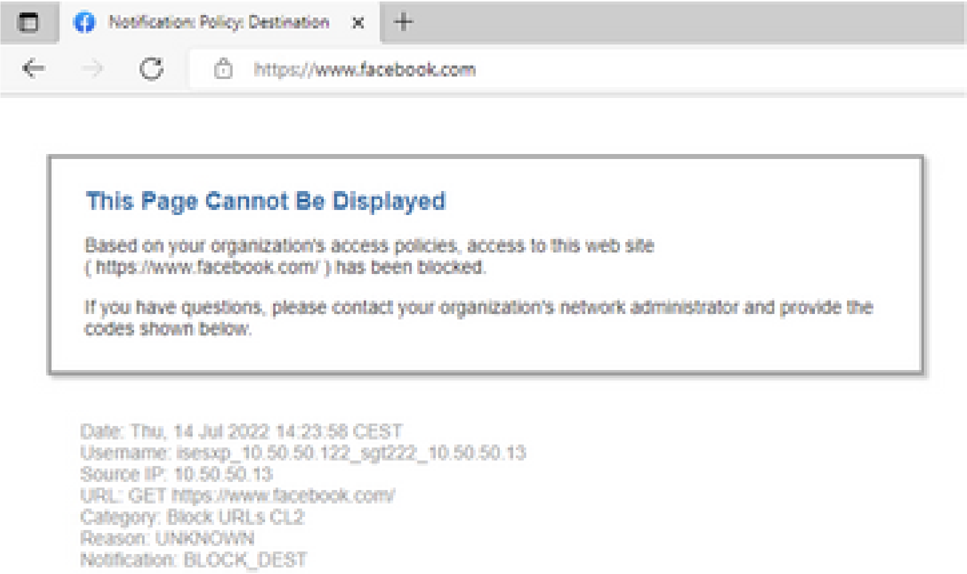
Items Displayed 50

Displaying 1 - 50 of 137 items.

« Previous | 1 | 2 | 3 | Next »

Time (GMT +02:00) ▾	Website (count) Display All Details...	Disposition	Bandwidth	User / Client IP
14 Jul 2022 14:28:17	https://bbc.com:443/favicon.ico CONTENT TYPE: - URL CATEGORY: Block URLs CL1 DESTINATION IP: - DETAILS: Decryption Policy: "ISE_Cluster1", WBRS: 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

属于ISE集群2的终端

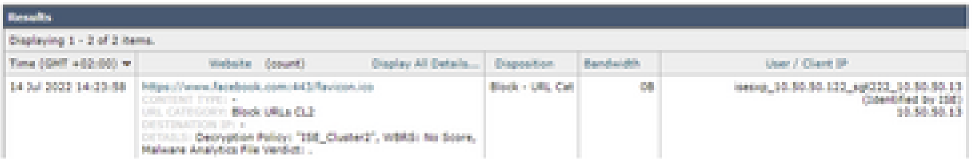


This Page Cannot Be Displayed

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:443/favicon.ico CONTENT TYPE: - URL CATEGORY: Block URLs CL2 DESTINATION IP: - DETAILS: Decryption Policy: "ISE_Cluster2", WBRS: 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

相关信息

- 网络安全设备和身份服务引擎集成指南
- 为 TrustSec 感知服务配置 WSA 与 ISE 的集成
- 思科身份服务引擎管理员指南，版本3.1
- 思科安全网络设备AsyncOS 14.5用户指南