將多個ISE群集與基於TrustSec的策略的安全網路裝置整合

目錄

簡介

本文檔介紹通過pxGrid將安全組標籤(SGT)資訊從多個ISE部署傳送到單個思科安全網路裝置（形式上為網路安全裝置WSA）的過程，以便在TrustSec部署中利用基於SGT的Web訪問策略。

在版本14.5之前，安全網路裝置只能與單個ISE集群整合以基於SGT的身份策略。通過引入此新版

本，Secure Web Appliance現在可以與來自多個ISE集群的資訊進行互操作，並在它們之間聚合一個單獨的ISE節點。這帶來了巨大的好處，使我們能夠從不同的ISE集群匯出使用者資料，並可以在不需要1:1整合的情況下自由控制使用者可以使用的退出點。

必要條件

需求

思科建議您瞭解以下主題：

- 身分識別服務引擎 (ISE)
- 安全Web裝置
- RADIUS通訊協定
- TrustSec
- pxGrid

採用元件

本文中的資訊係根據以下軟體和硬體版本：

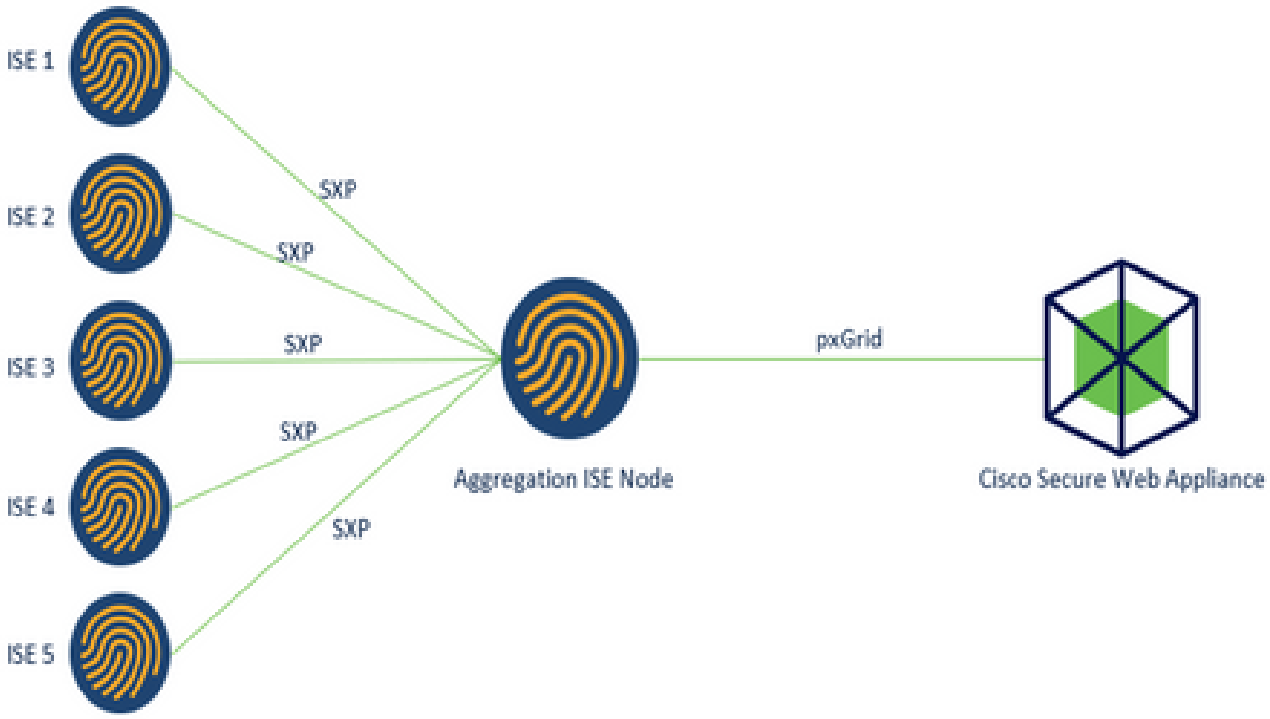
- 安全網路裝置14.5
- ISE版本3.1 P3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

限制

1. 所有ISE集群需要為SGT維護統一的對映。
2. ISE聚合節點必須具有其餘ISE群集的SGT名稱/編號。
3. 安全Web裝置只能根據SGT標籤識別策略（訪問/解密/路由），而不能識別組和用戶名。
4. 報告和跟蹤基於SGT。
5. 現有的ISE/安全Web裝置大小調整引數繼續適用於此功能。

網路圖表



流程：

1.當終端使用者連線到網路時，他們根據ISE中的授權策略接收SGT。

2.然後，不同的ISE群集將此SGT資訊以SGT-IP對映的形式通過SXP傳送到ISE聚合節點。

3. ISE聚合節點接收此資訊並通過pxGrid與單個安全網路裝置共用。

4. Secure Web Appliance使用它學到的SGT資訊，根據Web訪問策略為使用者提供訪問許可權。

設定

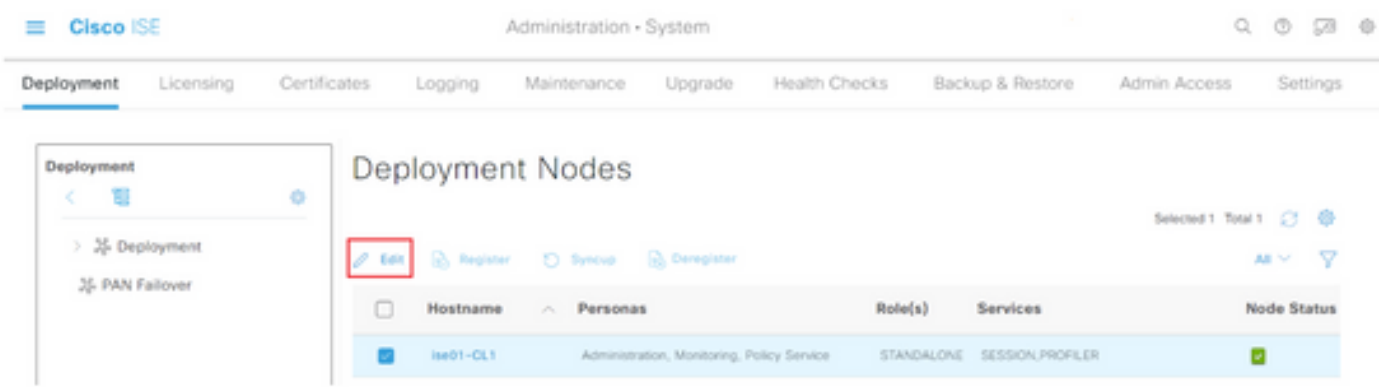
ISE 組態

啟用SXP

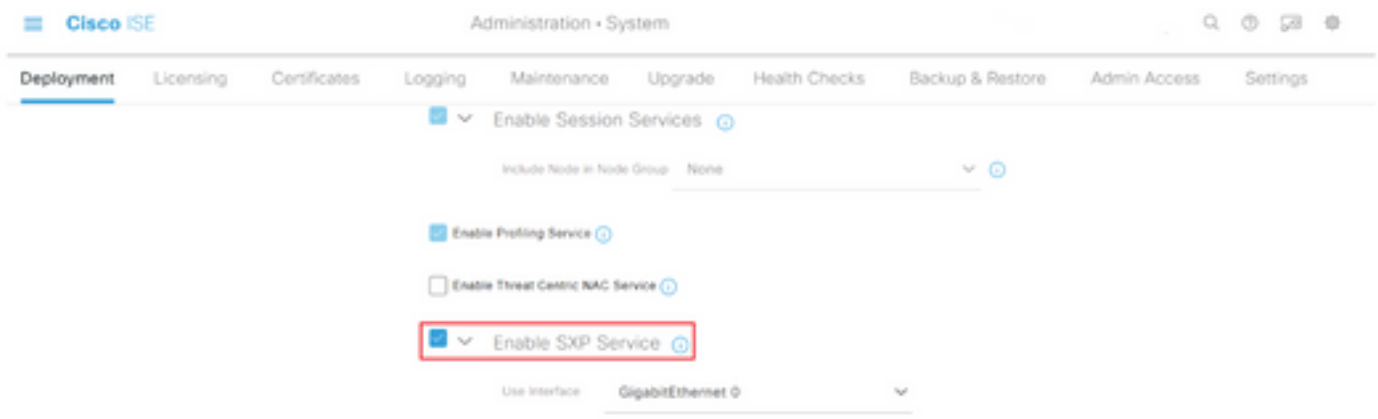
步驟1.選擇三行圖示

位於左上角，然後選擇管理>系統>部署。

步驟2.選擇要配置的節點，然後按一下Edit。



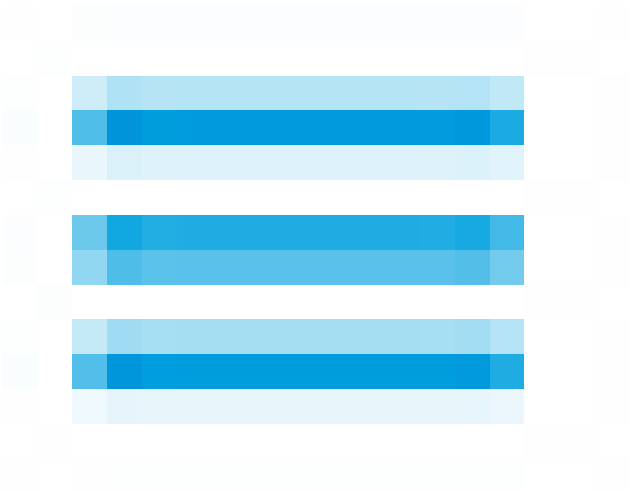
步驟3.要啟用SXP，請勾選啟用SXP服務



步驟4.向下滾動到底部，然後按一下「Save」

附註：對每個集群中其餘的ISE節點（包括匯聚節點）重複所有步驟。

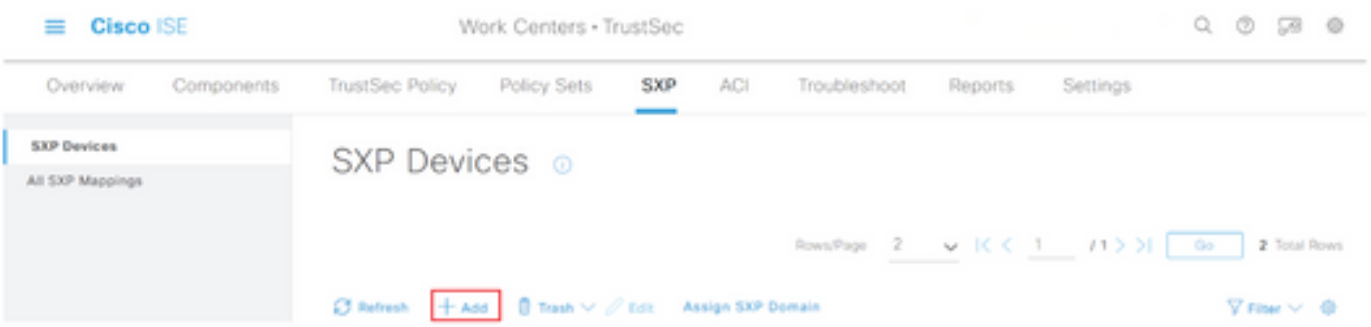
在群集節點上配置SXP



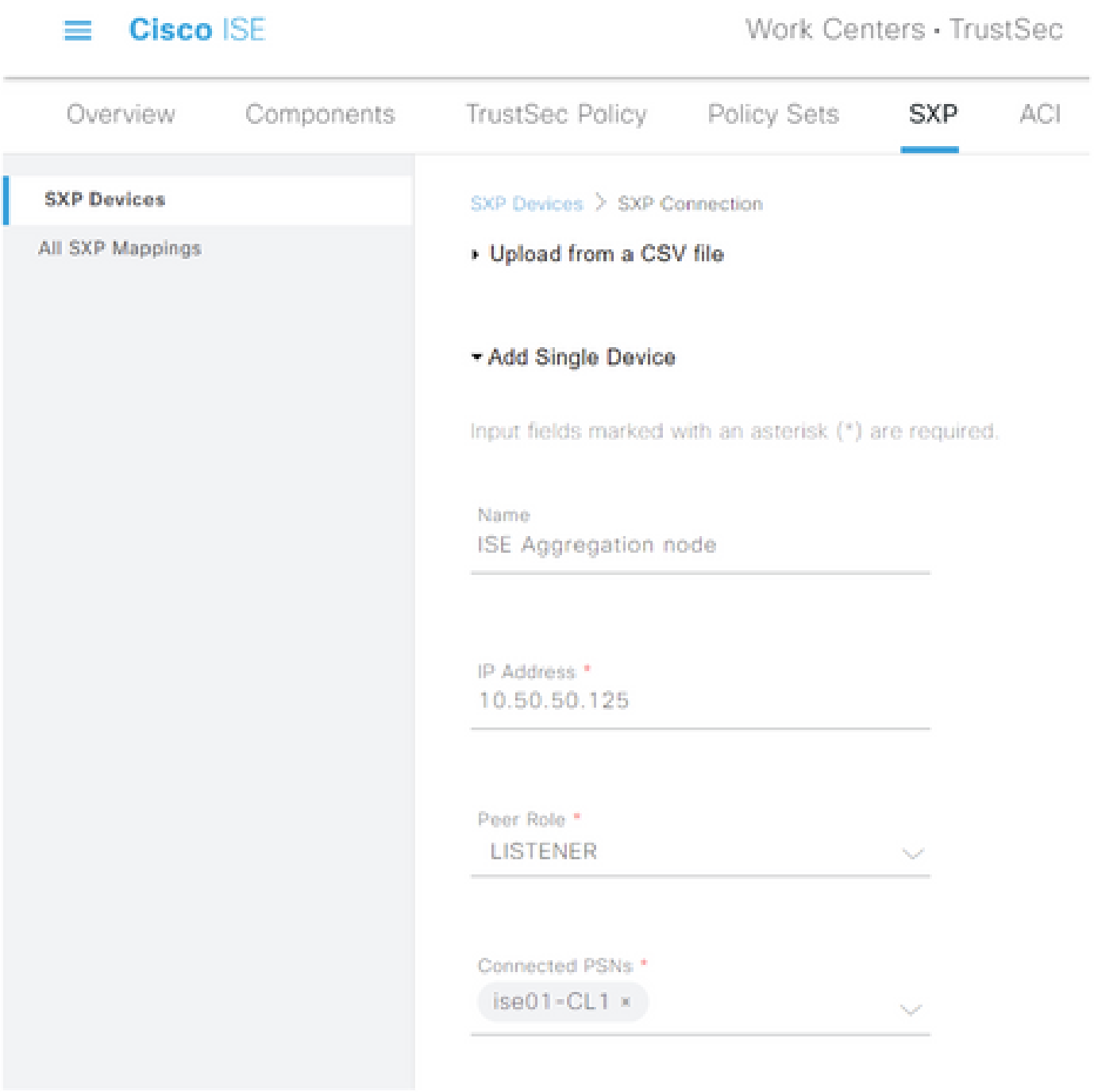
步驟1.選擇三行圖示

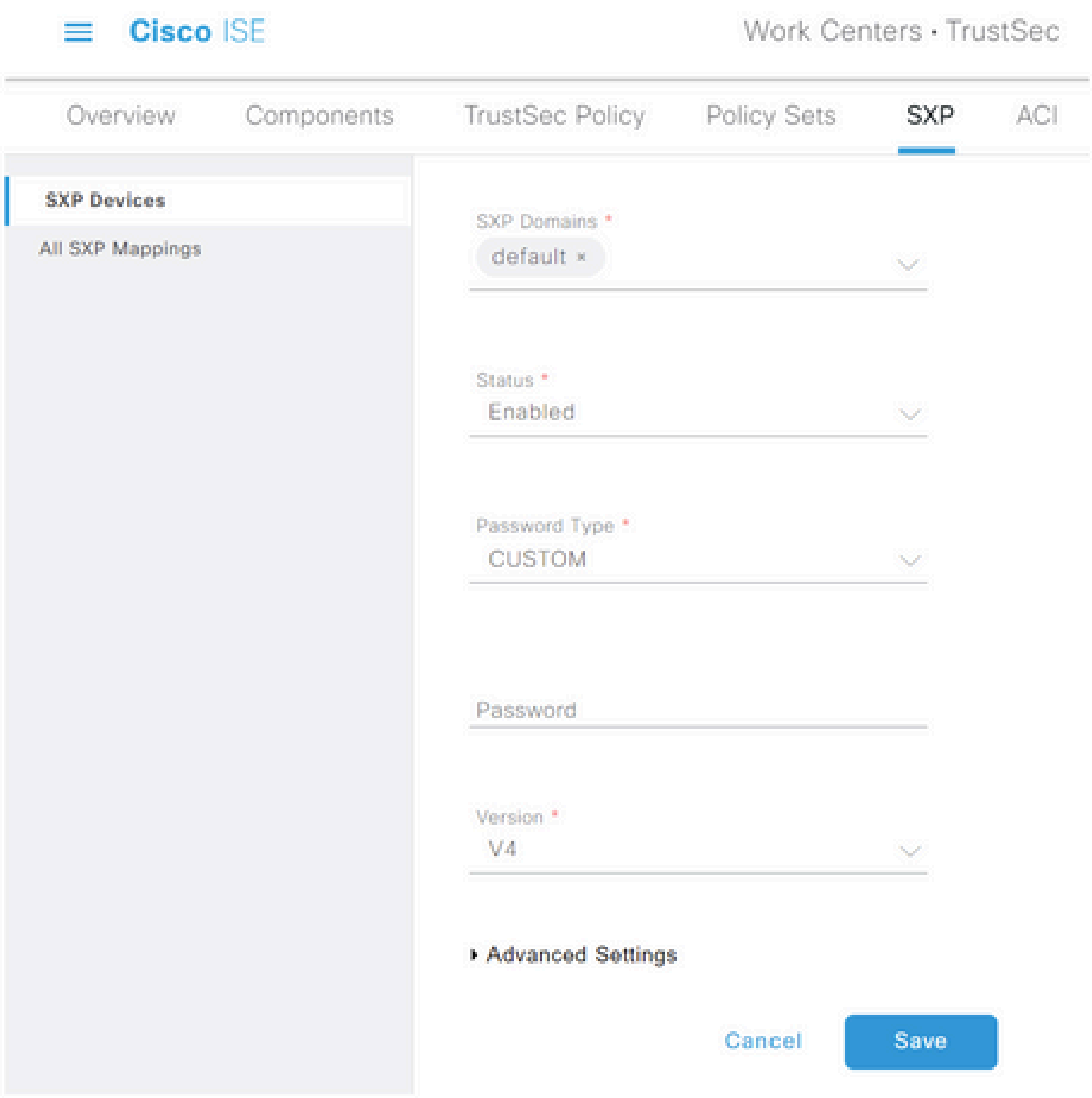
位於左上角，然後選擇 工作中心> TrustSec > SXP。

步驟2. 按一下+Add將ISE聚合節點配置為SXP對等體。



步驟3.定義ISE聚合節點的名稱和IP地址，選擇對等角色作為LISTENER。在已連線的PSN、所需的SXP域下選擇所需的PSN，在status下選擇Enabled，然後選擇Password Type和requiredVersion。


Cisco ISE
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



步驟4.按一下Save

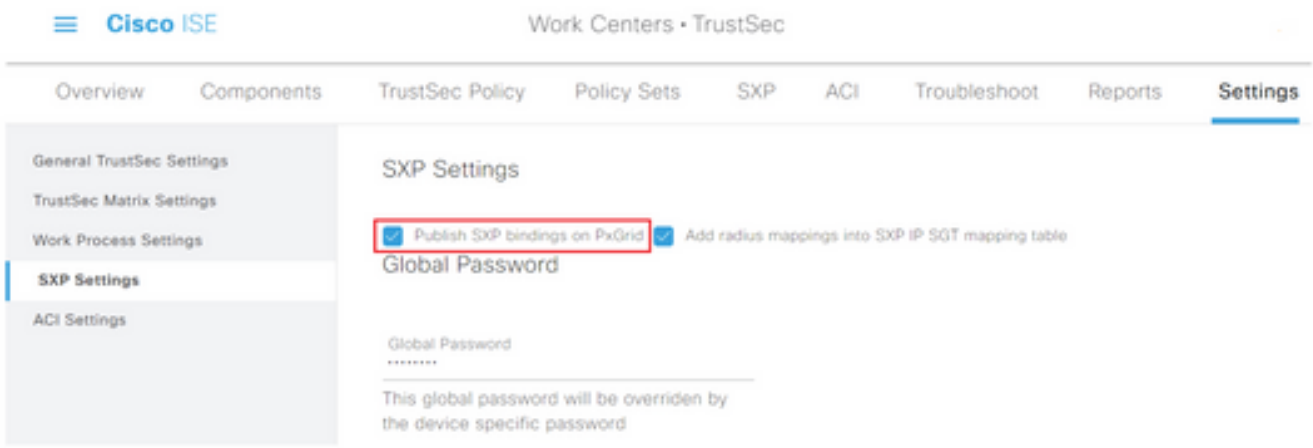
附註：對每個集群中的其餘的ISE節點重複所有步驟，以構建與匯聚節點的SXP連線。在聚合節點上重複相同的過程，然後選擇SPEAKER作為對等角色。

在聚合節點上配置SXP

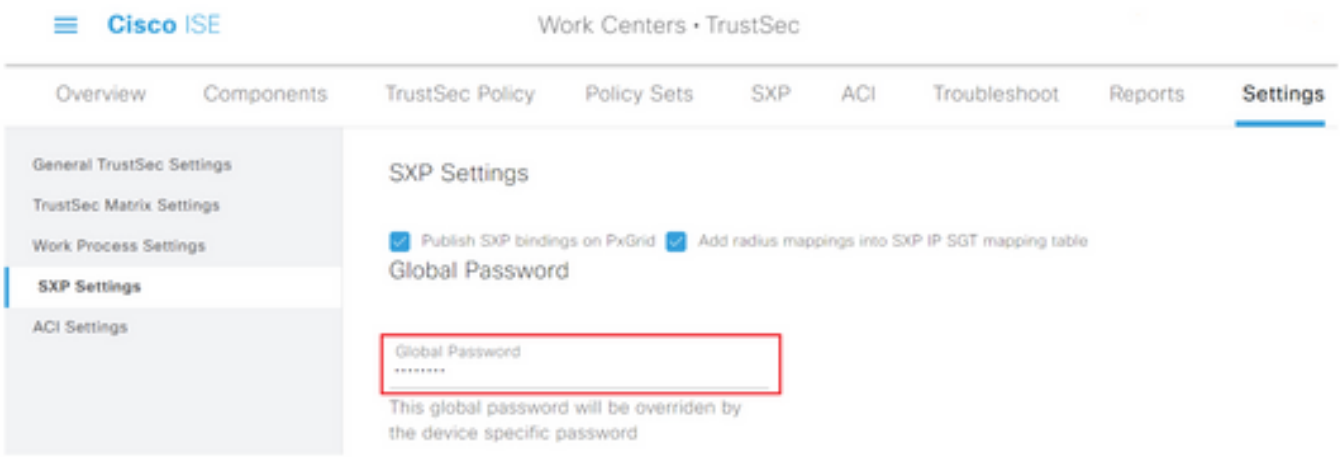
步驟1.選擇位於左上角的三行圖示，然後在「工作中心」>「TrustSec」>「設定」上選擇

步驟2. 按一下SXP Settings頁籤

步驟3.要傳播IP-SGT對映，請勾選在pxGrid上發佈SXP繫結覈取方塊。



第4步（可選）。 在Global Password（全域性密碼）下定義SXP設定的默認密碼

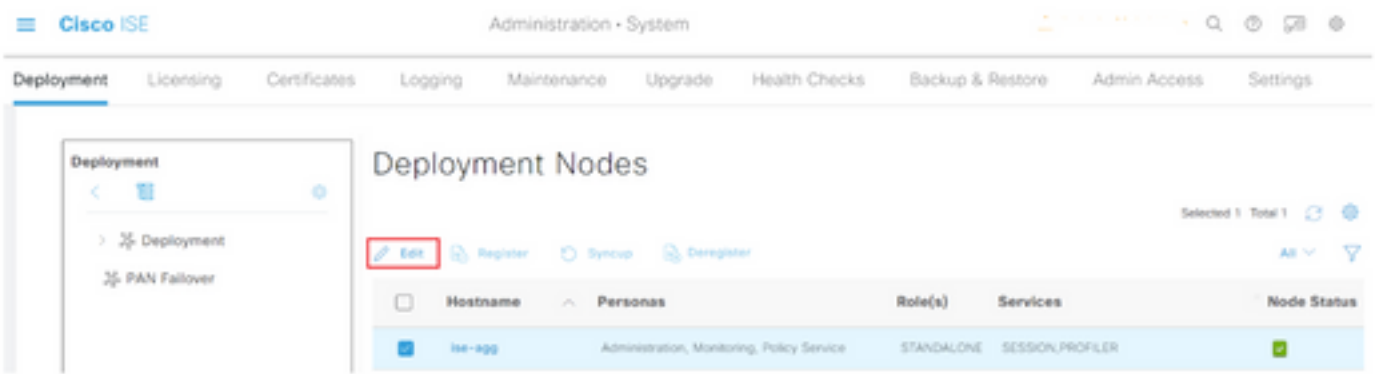


步驟5.向下滾動並點選儲存。

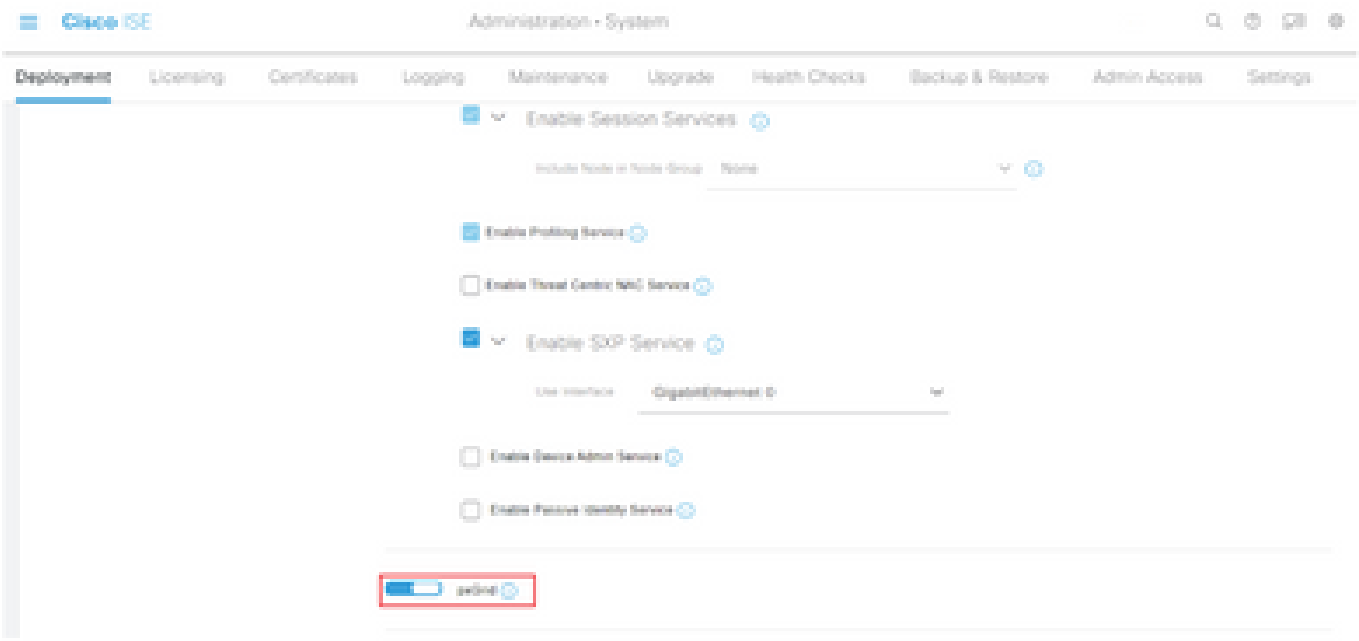
在聚合節點上啟用pxGrid

步驟1.選擇位於左上角的三行圖示，然後在Administration > System > Deployment中選擇。

步驟2.選擇要配置的節點，然後按一下Edit。



步驟3.要啟用pxGrid，請按一下pxGrid旁邊的按鈕。

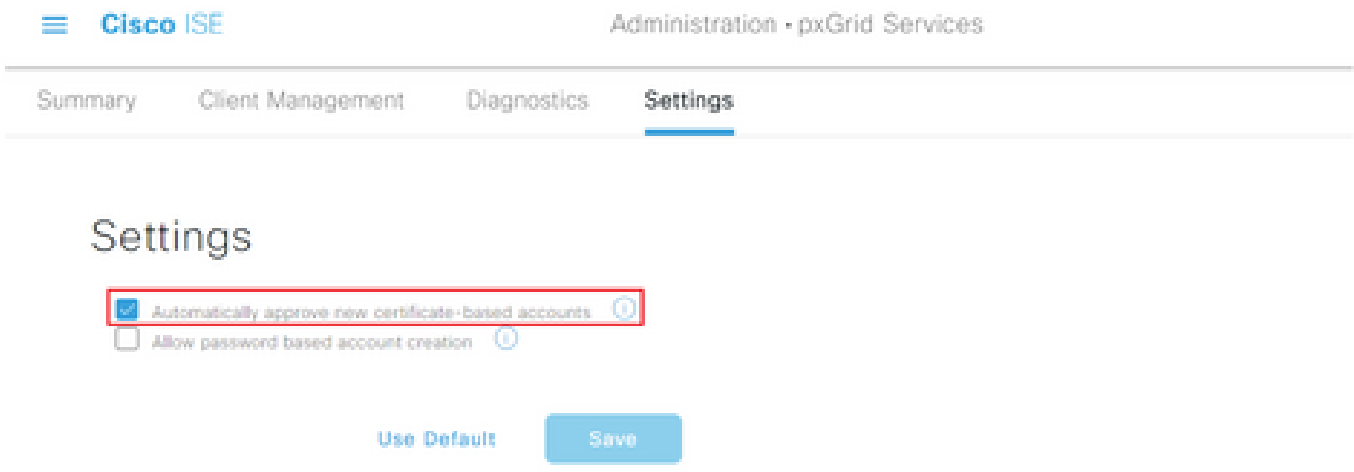


步驟4.向下滾動到底部，然後按一下「Save」。

pxGrid自動批准

步驟1.導航至位於左上角的三行圖示，然後選擇管理> pxGrid服務>設定。

步驟2. 預設情況下，ISE不會自動批准pxGrid來自新pxGrid客戶端的連線請求，因此必須通過選中Automatically approve new certificate-based accounts覈取方塊啟用該設定。



步驟3.按一下Save

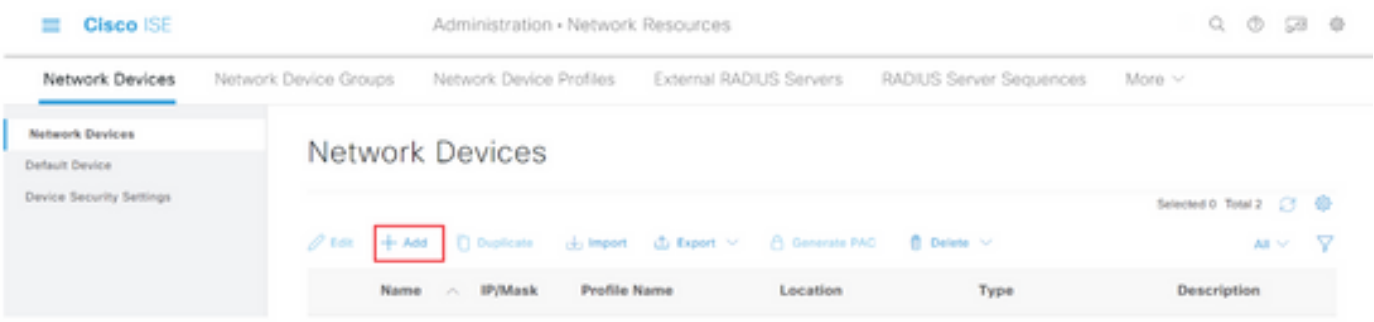
網路裝置TrustSec設定

對於思科ISE處理來自啟用TrustSec的裝置請求，您必須在思科ISE中定義這些啟用TrustSec的裝置

。

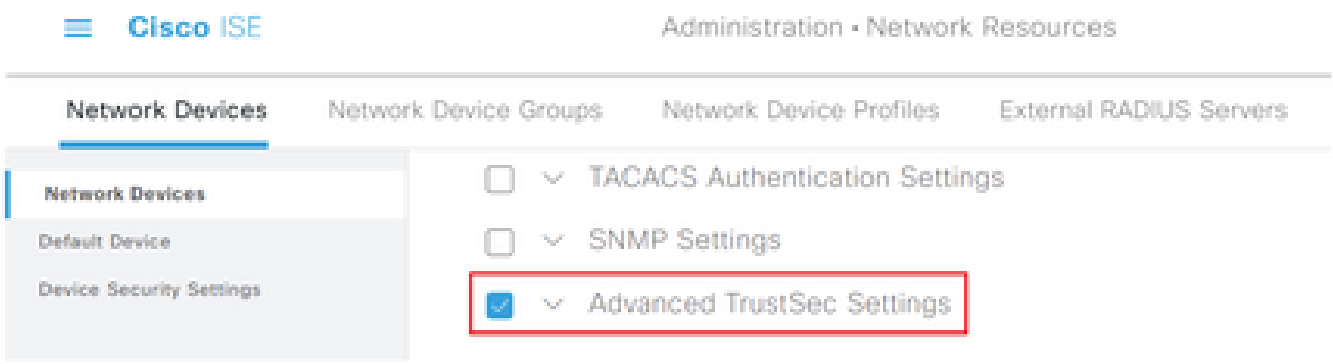
步驟1.導航至位於左上角的三行圖示，然後選擇Administration > Network Resources > Network Devices。

步驟2. 按一下+Add。

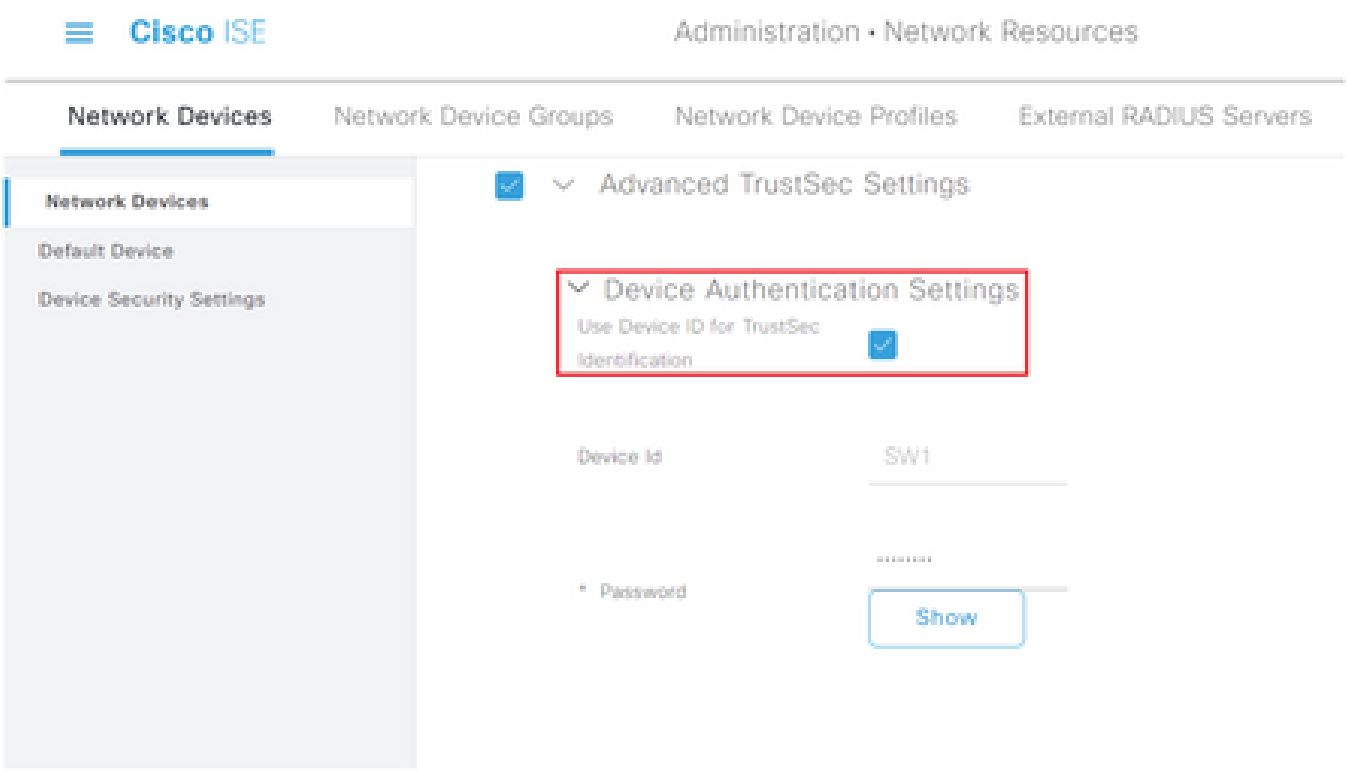


步驟3.在「Network Devices」部分和「RADIUS Authentication Settings」中輸入所需的資訊。

步驟4.選中Advanced TrustSec Settings覈取方塊以配置啟用TrustSec的裝置。

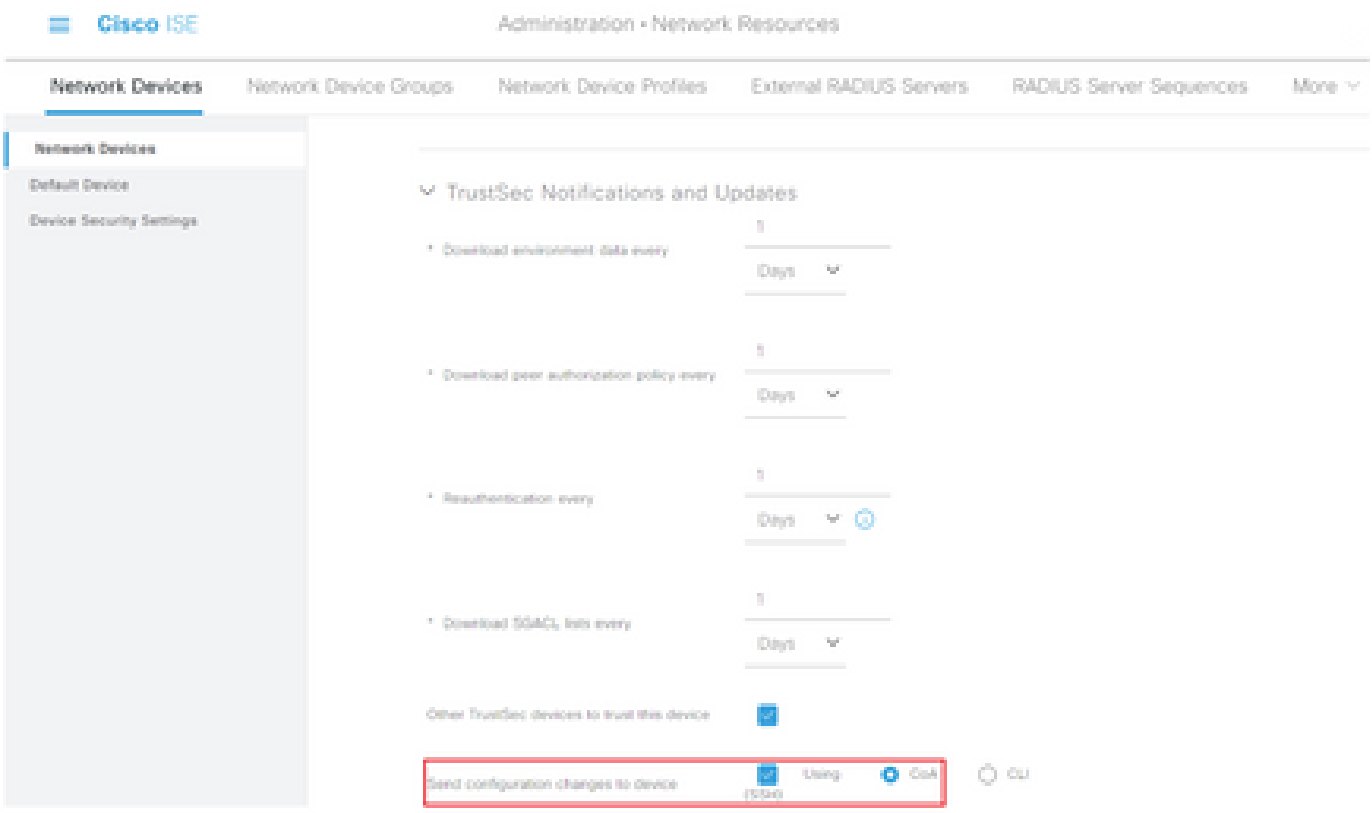


步驟5.點選Use Device ID for TrustSec Identification覈取方塊以自動填充Network Devices部分中列出的Device Name。在「Password」欄位中輸入密碼。



附註：ID和密碼必須與交換機上稍後配置的「cts credentials id <ID> password <PW>」命令匹配。

步驟6.選中Send configuration changes to device覈取方塊，以便ISE可以向裝置傳送TrustSec CoA通知。



步驟7.選中部署安全組標籤對映更新時包含此裝置覈取方塊。

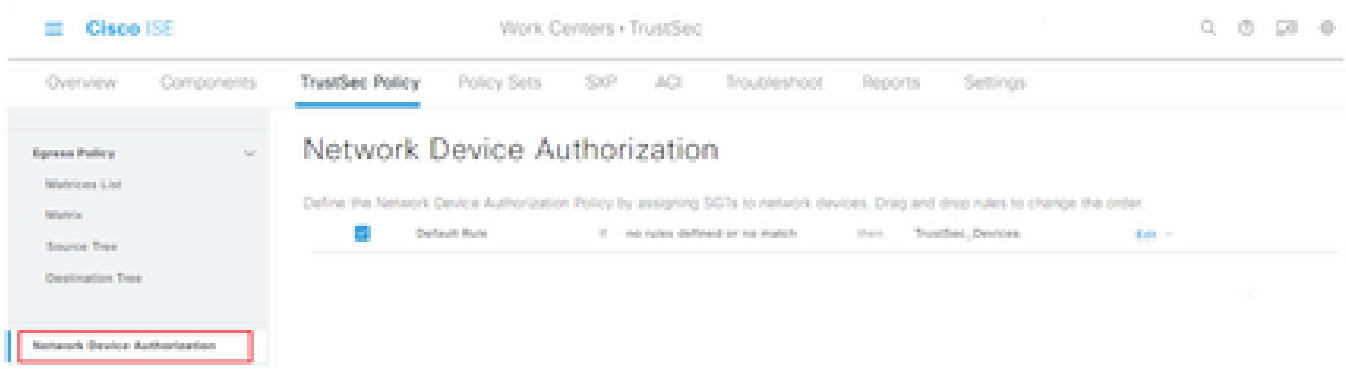
步驟8.要讓ISE編輯網路裝置的配置，請在EXEC模式使用者名稱和EXEC模式密碼欄位中輸入使用者憑證。或者，在Enable Mode Password 欄位中提供啟用密碼。

附註：對要成為TrustSec域一部分的所有其他NAD重複這些步驟。

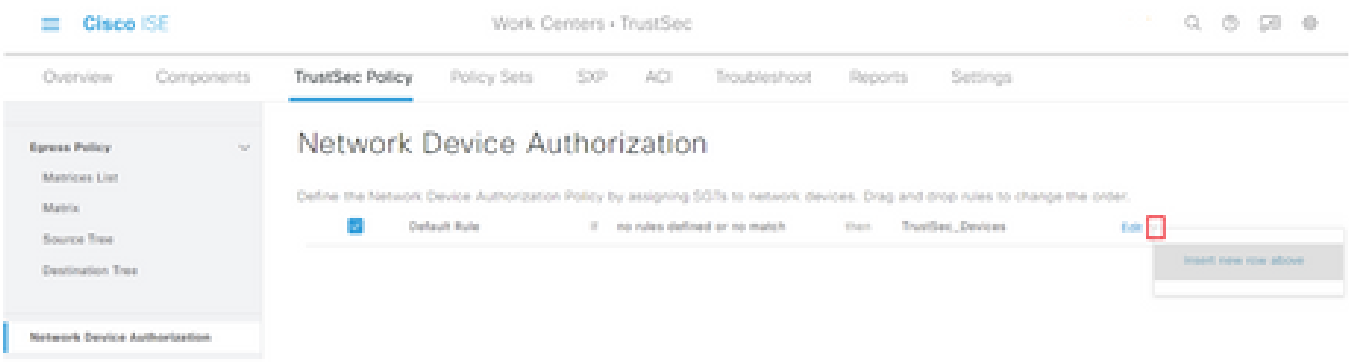
網路裝置授權

步驟1.選擇位於左上角的三行圖示，然後在Work Centers > TrustSec > TrustSec Policy上選擇。

步驟2. 在左窗格中，按一下網路裝置授權。

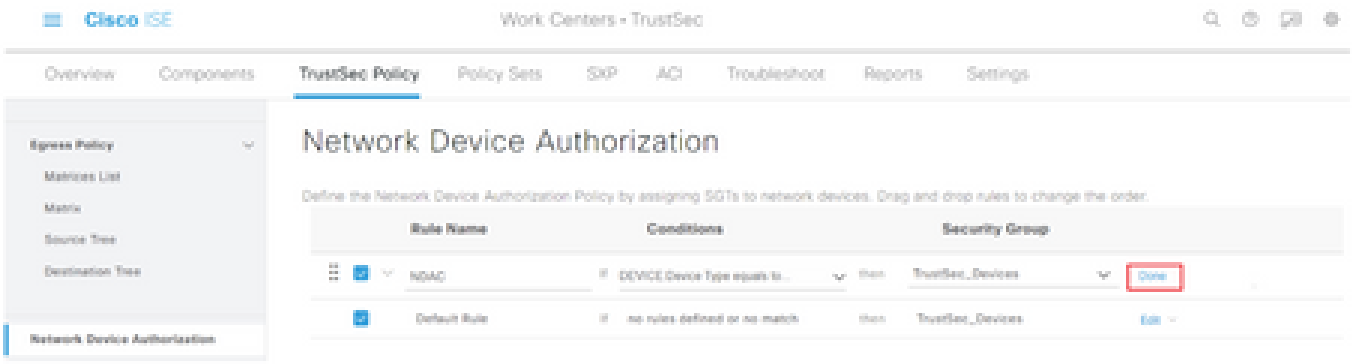


步驟3.在右側，使用上面Edit 和Insert new row 旁邊的下拉選單建立新的NDA規則。



步驟4.定義規則名稱、條件，並從Security Groups下的下拉選單中選擇適當的SGT。

步驟5. 按一下最右邊的完成。



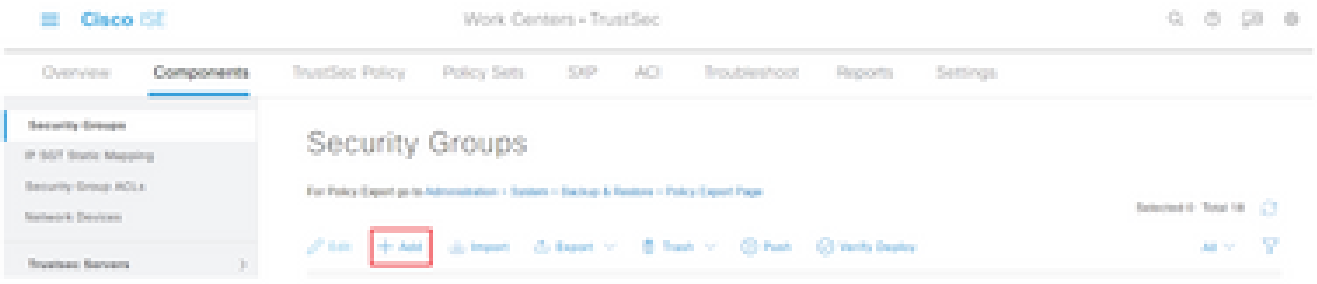
步驟6.向下滾動並點選儲存。

SGT

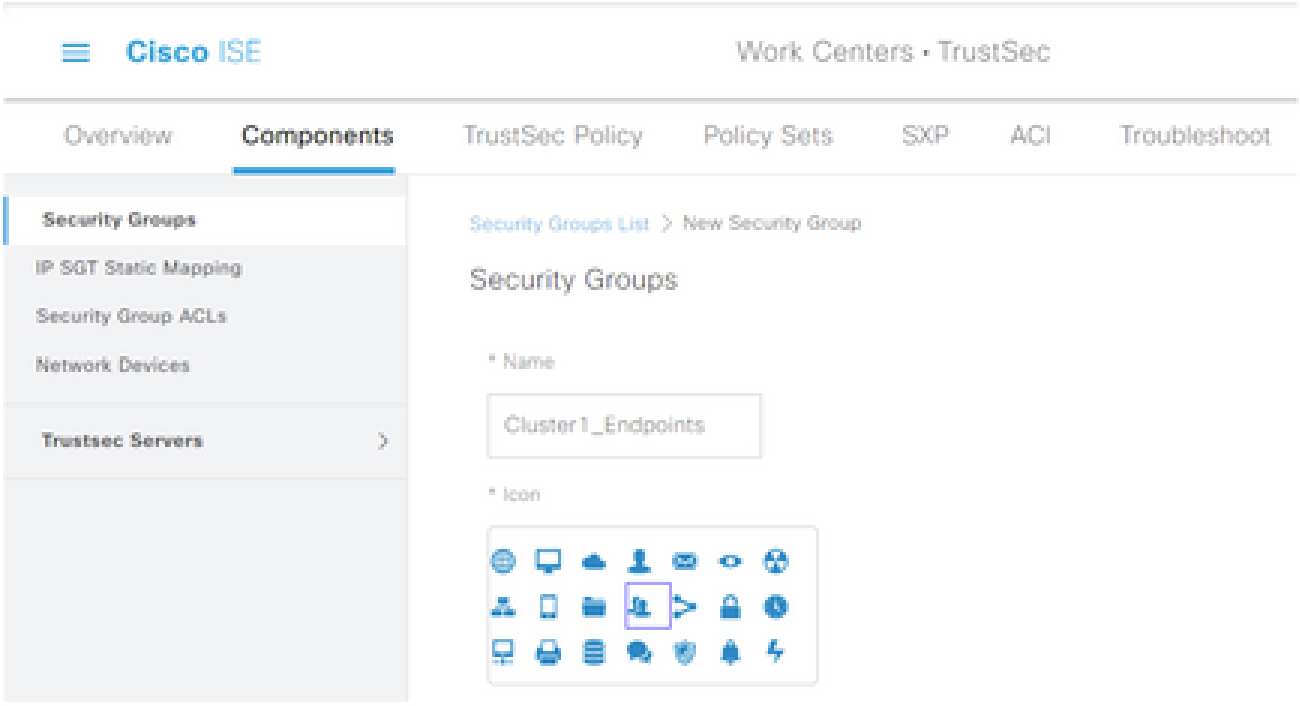
步驟1.選擇位於左上角的三行圖示，然後在「工作中心」(Work Centers)>「信任安全」(TrustSec)>「元件」(Components)上選擇。

步驟2. 在左窗格中，展開Security Groups。

步驟3.按一下+Add建立新的SGT。



步驟4.輸入名稱並在相應欄位中選擇一個圖示。



步驟5.（可選）為其提供說明並輸入標籤值。

附註：為了能夠手動輸入標籤值，請導航到工作中心(Work Centers)> TrustSec >設定(Settings)> General TrustSec設定(General TrustSec Settings)，然後選擇安全組標籤編號(Security Group Tag Numbering)下的使用者必須手動輸入SGT編號(User Must Manually Enter SGT Number)選項。

步驟6.向下滾動並點選Submit

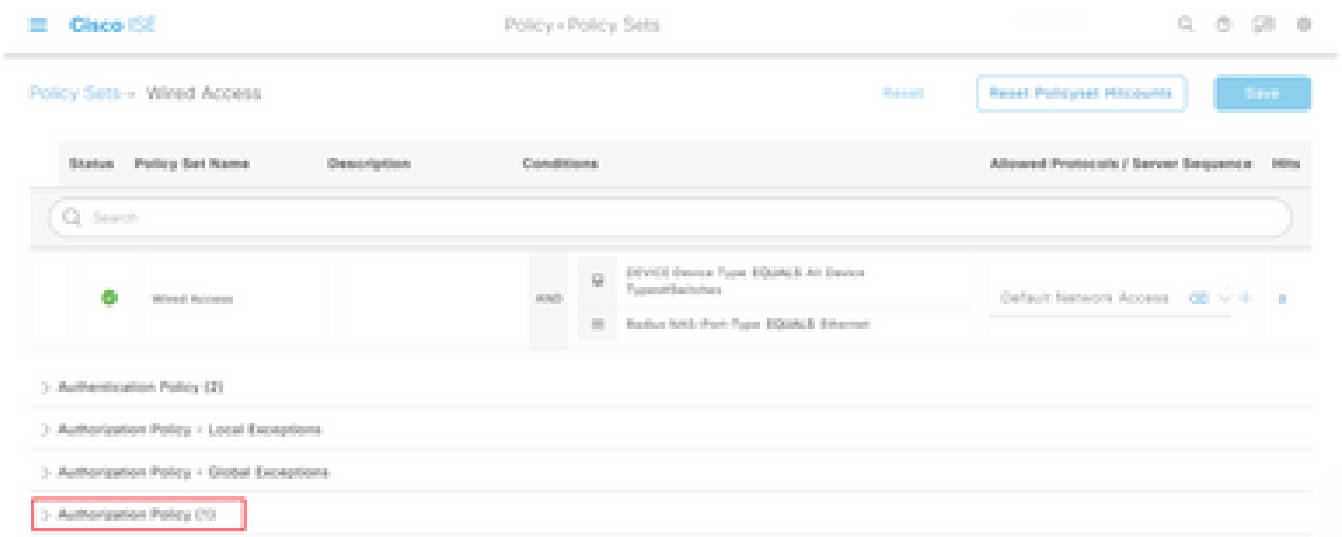
附註：對所有所需的SGT重複這些步驟。

授權策略

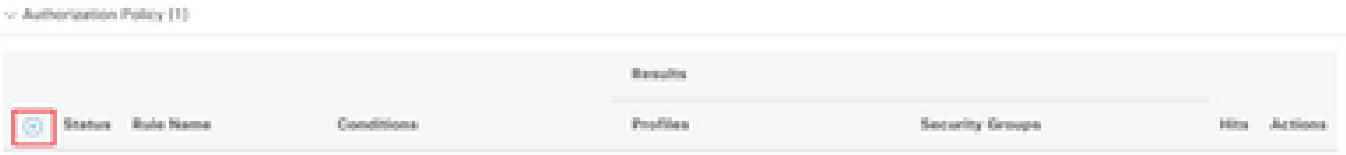
步驟1.選擇位於左上角的三行圖示，然後在Policy > Policy Sets中選擇。

步驟2. 選擇適當的策略集。

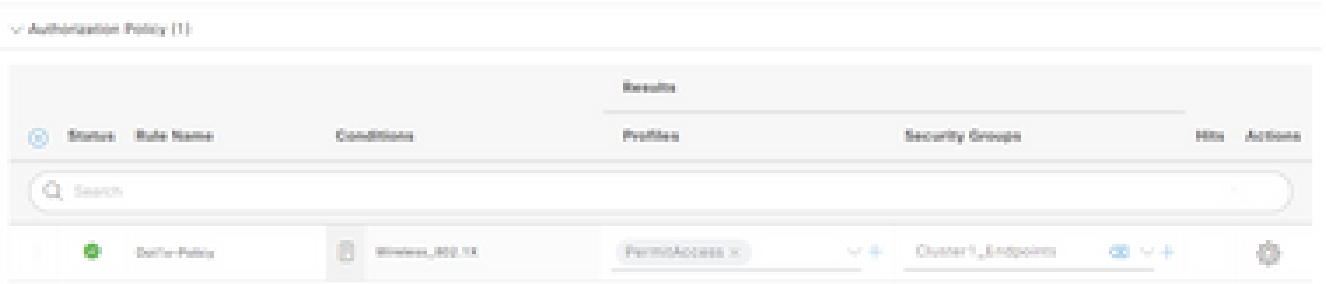
步驟3.在策略集中，展開Authorization Policy。



步驟4.按一下
按鈕建立授權策略。



步驟5. 定義所需的規則名稱、條件和配置檔案，並從Security Groups下的下拉選單中選擇適當的SGT。



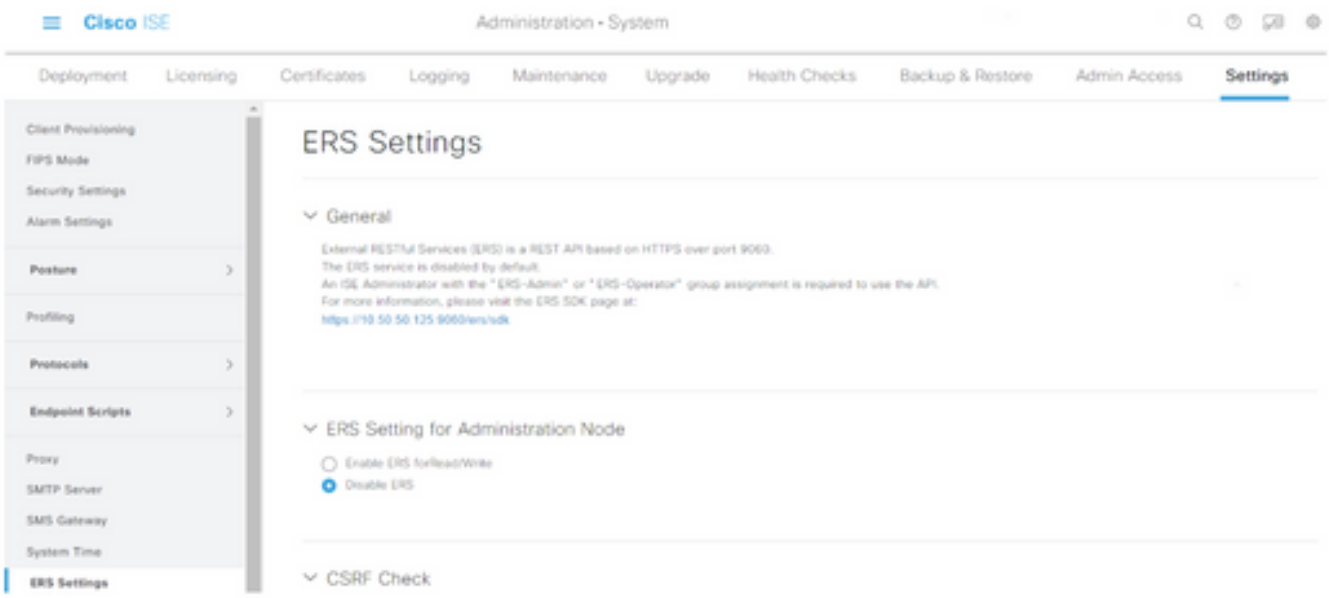
步驟6.按一下Save。

在ISE聚合節點上啟用ERS（可選）

外部RESTful API服務(ERS)是WSA可以查詢組資訊的API。ISE上預設禁用ERS服務。啟用後，如果客戶端作為ISE節點上的ERS Admin組成員進行身份驗證，則可以查詢API。要在ISE上啟用服務並將帳戶新增到正確的組，請執行以下步驟：

步驟1.選擇位於左上角的三行圖示，然後在Administration > System > Settings中選擇。

步驟2. 在左窗格中，按一下ERS Settings。



步驟3.選擇Enable ERS for Read/Write選項。

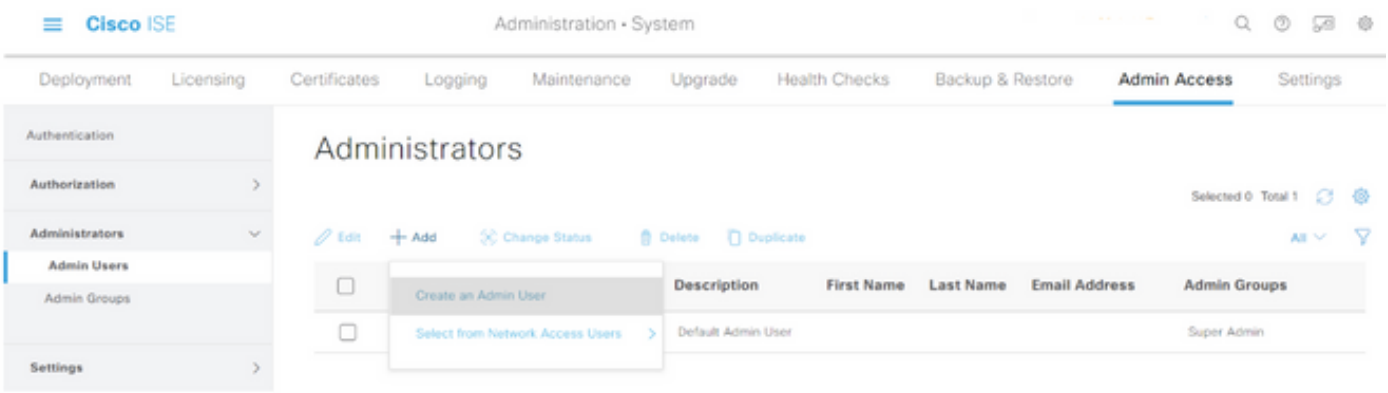
步驟4.按一下Save，然後使用OK確認。

將使用者新增到ESR管理員組（可選）

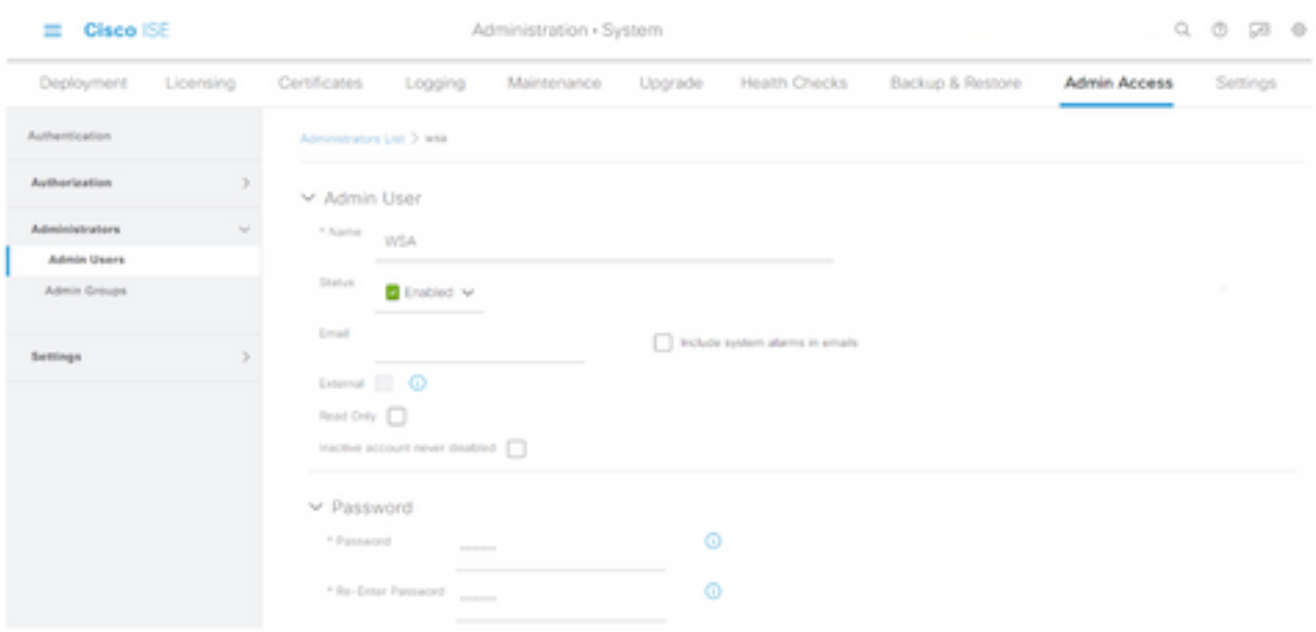
步驟1.選擇位於左上角的三行圖示，然後選擇Administration > System > Admin Access

步驟2. 在左窗格中，展開Administrators，然後按一下Admin Users。

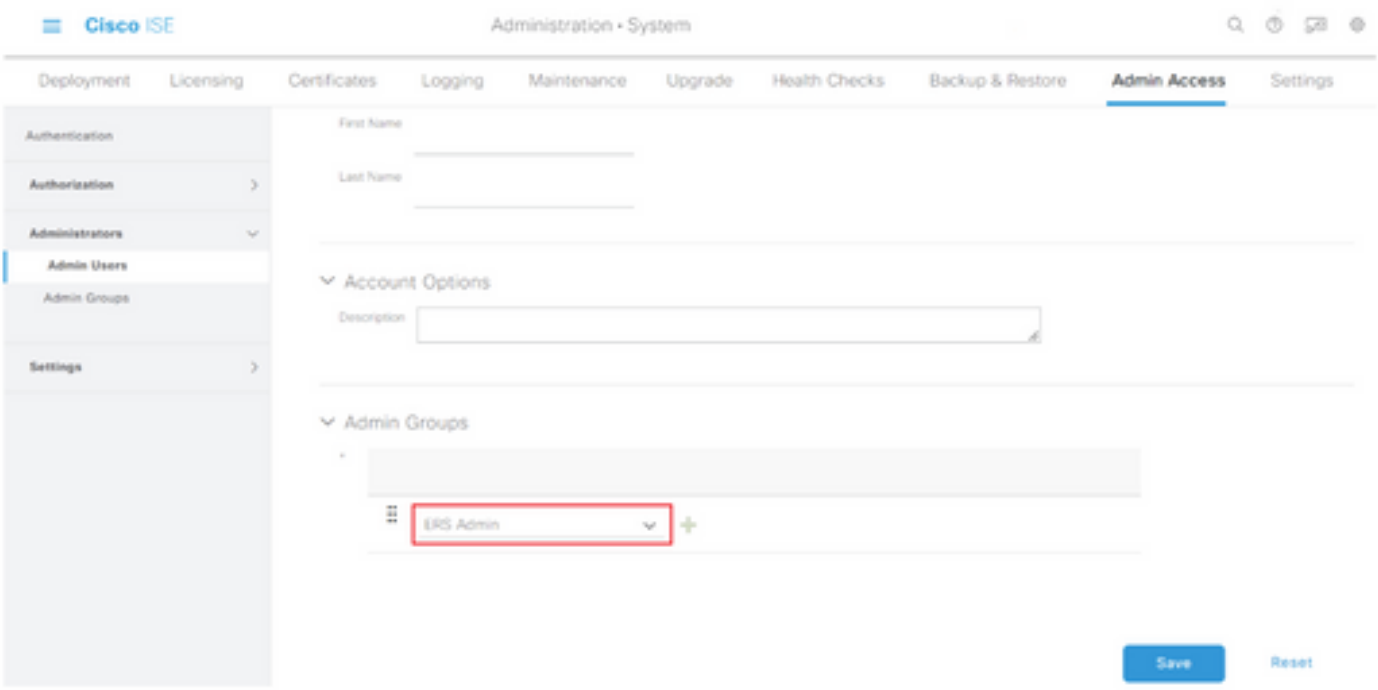
步驟3. 按一下+Add ，然後從下拉式選單中選擇Admin User。



步驟4.在相應欄位中輸入使用者名稱和密碼。



步驟5.在Admin Groups欄位中，使用下拉選單選擇ERS Admin。



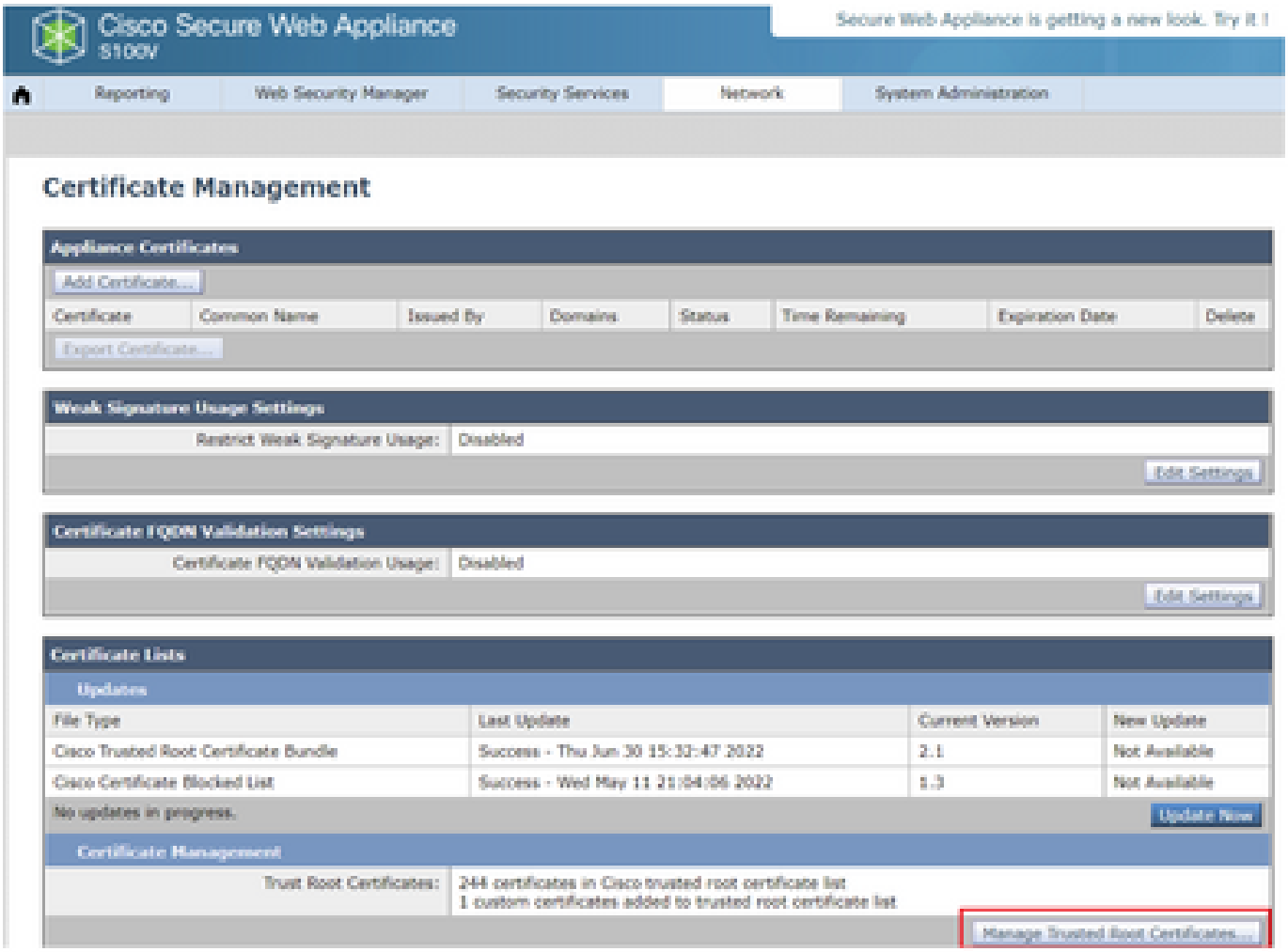
步驟6.按一下Save。

安全Web裝置配置

根證書

如果整合設計使用內部證書頒發機構作為WSA和ISE之間連線的信任根，則必須在兩個裝置上安裝此根證書。

步驟1.導覽至Network > Certificate Management，然後按一下Manage Trusted Root Certificates以新增CA憑證。

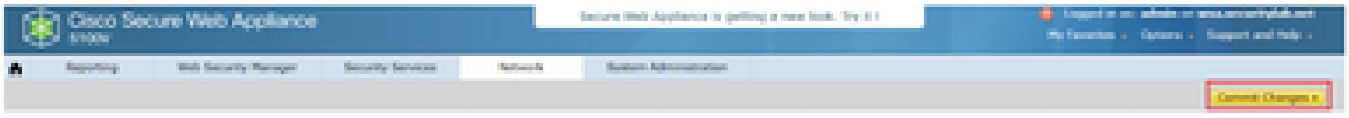


步驟2.按一下Import。

步驟3.按一下Choose File 以找到產生的根CA，然後按一下Submit。

步驟4.再次按一下Submit。

步驟5.在右上角，按一下Commit Changes。



步驟6.再次按一下Commit Changes。

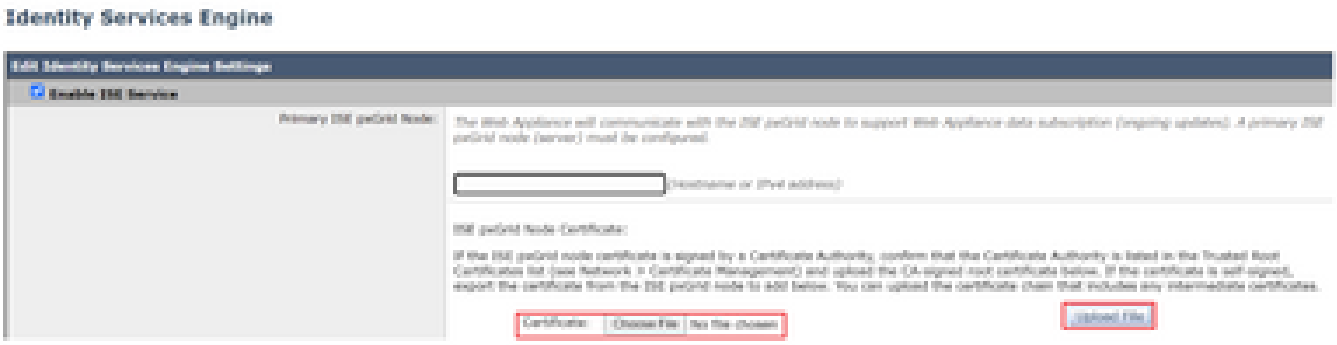
pxGrid證書

在WSA中，建立供pxGrid使用的金鑰對和證書作為ISE服務配置的一部分完成。

步驟1。導覽至Network > Identity Service Engine。

步驟2. 按一下Enable and Edit Settings。

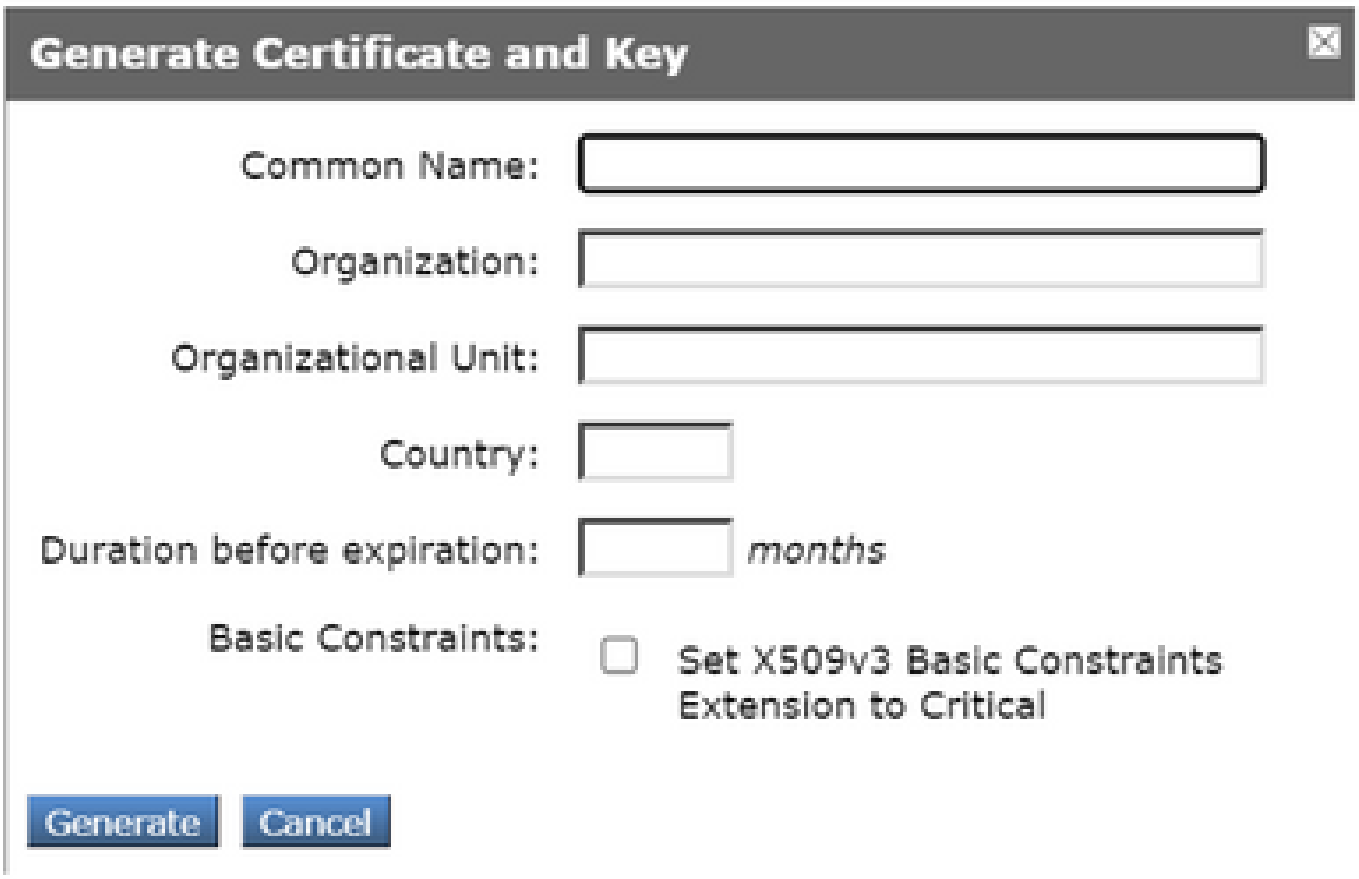
步驟3.按一下Choose File 以找到產生的根CA，然後按一下Upload File。



附註：常見的配置錯誤是上載此部分中的ISE pxGrid證書。必須將根CA證書上傳到ISE pxGrid節點證書欄位。

步驟4.在Web Appliance Client Certificate部分，選擇Use Generated Certificate and Key。

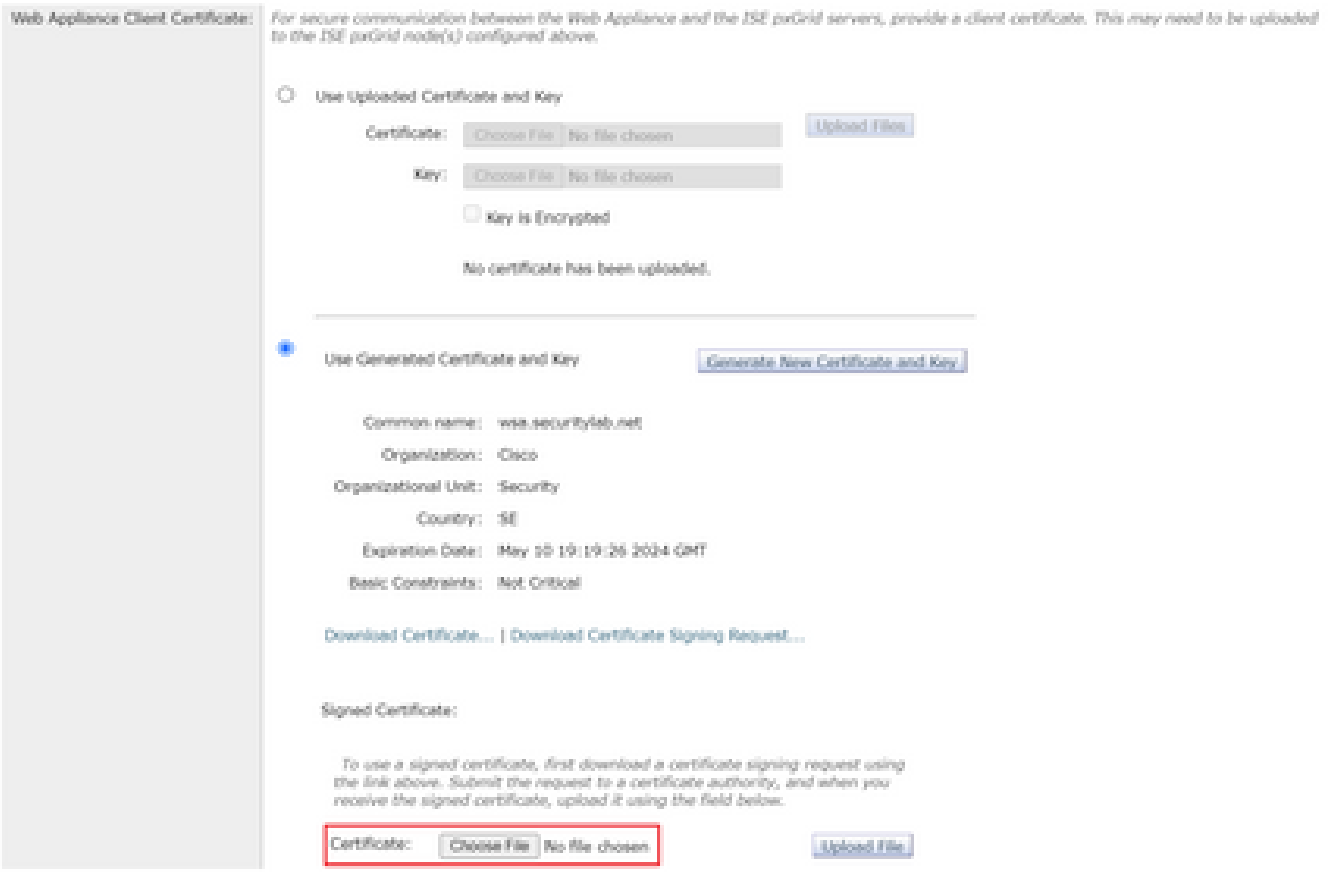
步驟5.按一下Generate New Certificate and Key 按鈕，然後填寫所需的憑證欄位。



步驟6.按一下Download Certificate Signing Request。

附註：建議選擇Submit按鈕提交對ISE配置的更改。如果在提交更改之前會話進入超時狀態，則即使已下載CSR，生成的金鑰和證書也會丟失。

步驟7.與CA簽署CSR後，按一下Choose File 以找到憑證。



步驟8.按一下Upload File。

步驟9.提交並提交。

在安全網路裝置上啟用SXP和ERS

步驟1.按一下SXP和ERS的Enable按鈕。

步驟2.在ERS Administrator Credentials欄位中，輸入在ISE上配置的使用者資訊。

步驟3.選中與ISE pxGrid節點相同的伺服器名稱框，以繼承早期配置的資訊。否則，請在此處輸入所需資訊。

步驟4.提交並提交。

標識配置檔案

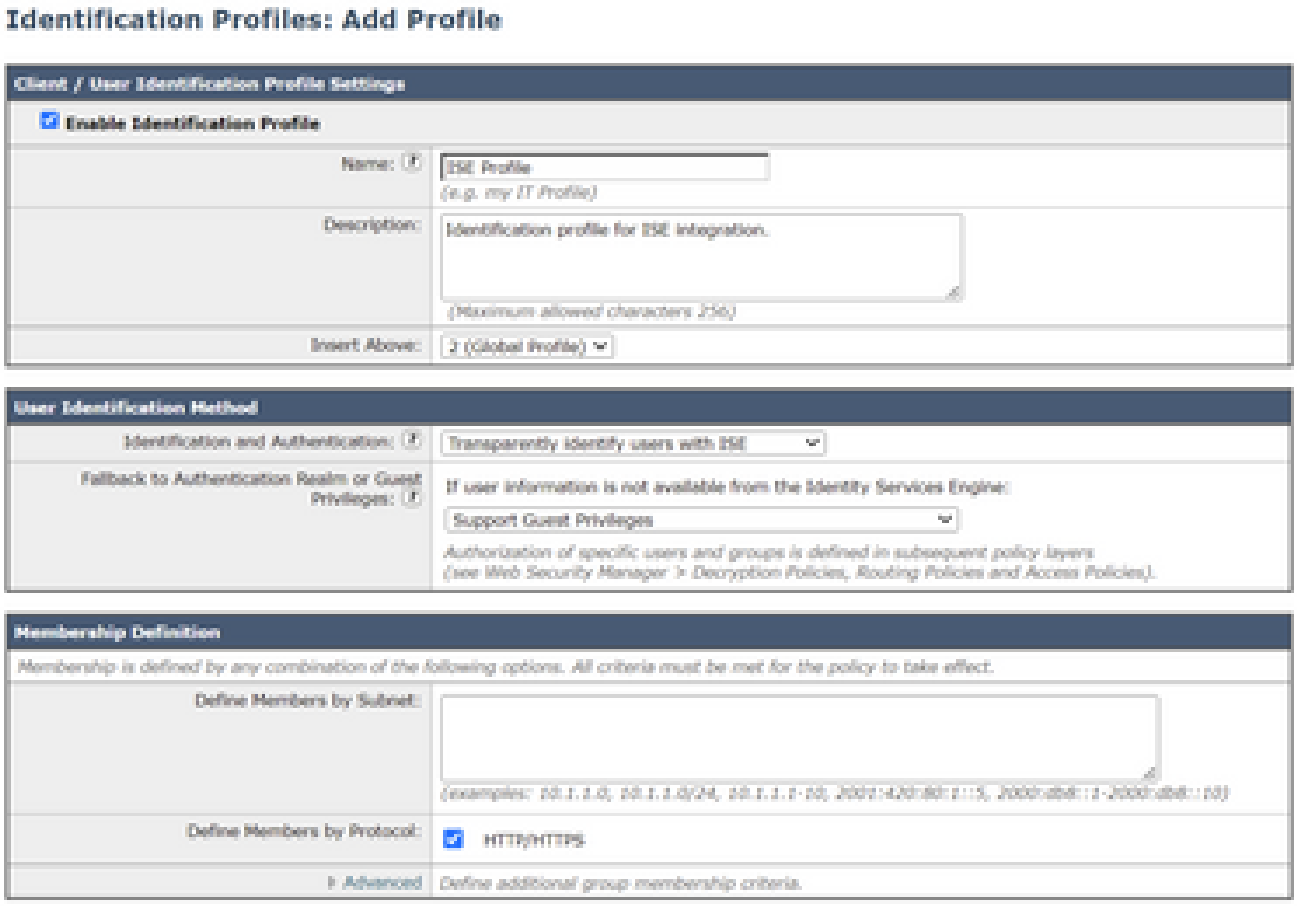
為了在WSA策略中使用安全組標籤或ISE組資訊，必須首先建立標識配置檔案，該配置檔案利用ISE作為透明標識使用者的方法。

步驟1.導覽至Web Security Manager > Authentication > Identication Profiles。

步驟2. 按一下Add Identification Profile。

步驟3.輸入名稱和（可選）說明。

步驟4.在Identification and Authentication部分，使用下拉選單選擇Transparentically identify users with ISE。



步驟5.提交並提交。

基於SGT的解密策略

步驟1。導覽至Web Security Manager > Web Policies > Decryption Policies。

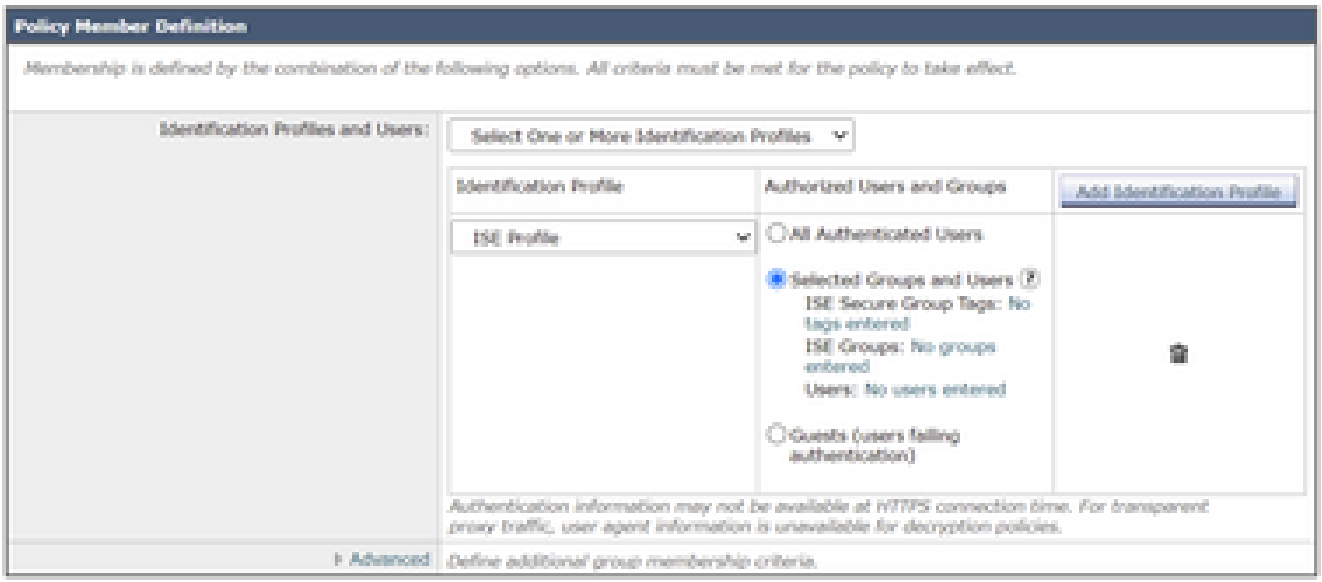
步驟2. 按一下Add Policy。

步驟3.輸入名稱和（可選）說明。

步驟4.在Identification Profiles and Users部分，使用下拉選單選擇Select One or More Identification Profiles。

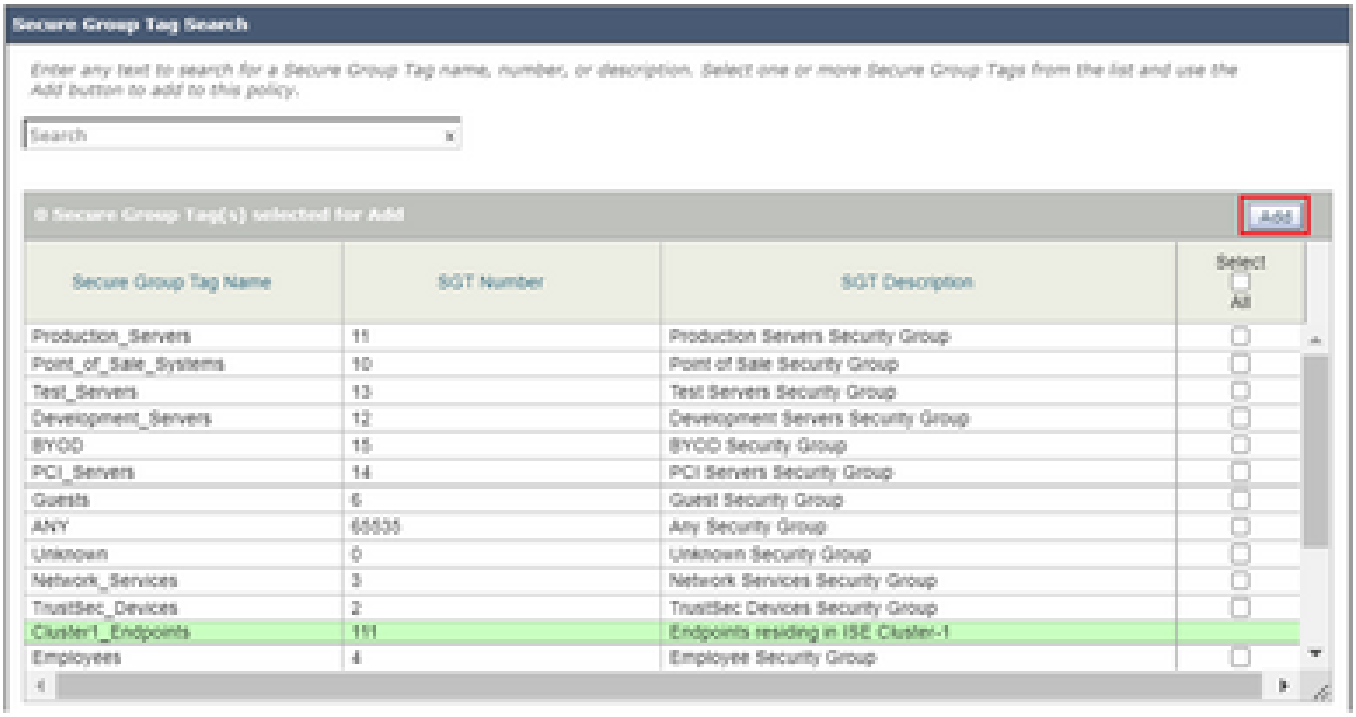
步驟5. 在Identification Profiles部分，使用下拉選單選擇ISE標識配置檔案的名稱。

步驟6.在Authorized Users and Groups部分，選擇Selected Groups and Users。



步驟7.單擊ISE Secure Group Tags旁的超連結。

步驟8.在Secure Group Tag Search部分，選中所需SGT右側的覈取方塊，然後點選Add。



步驟9.按一下Done以返回。

步驟10.提交並提交。

交換器組態

AAA

<#root>

```
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
```

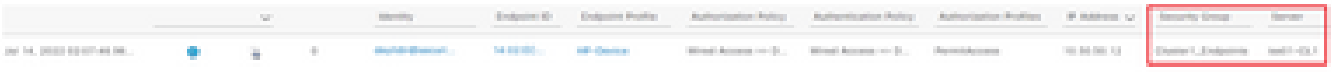
TrustSec

```
<#root>
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
```

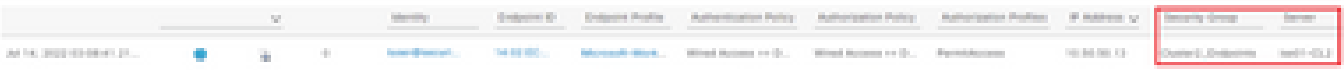
驗證

從ISE到終端的SGT分配。

在這裡，您可以看到來自ISE集群1的終端在成功身份驗證和授權後分配了SGT:

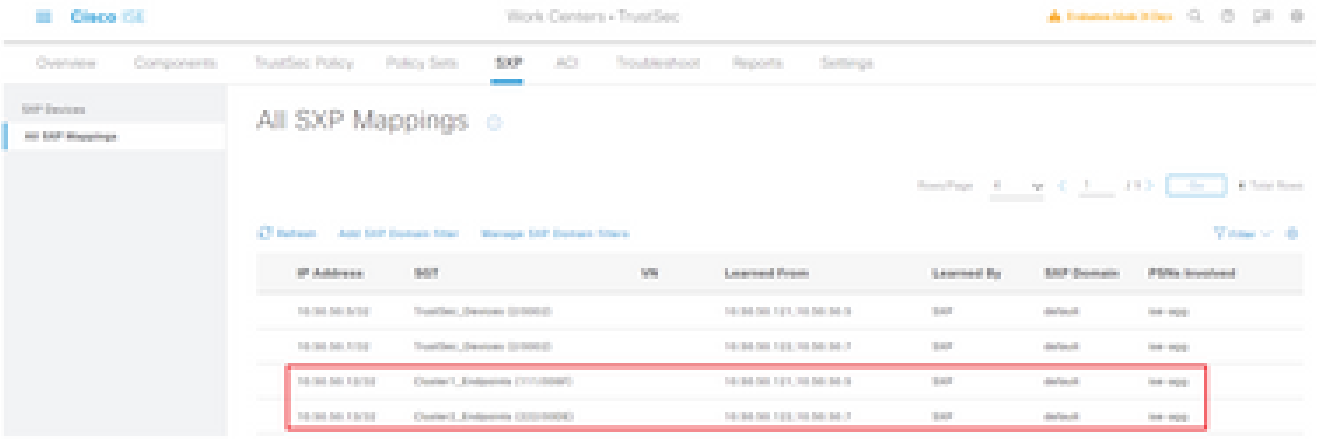


在這裡，您可以看到來自ISE集群2的終端在成功身份驗證和授權後分配了SGT:



SXP對映

由於群集ISE節點和ISE聚合節點之間啟用了SXP通訊，這些SGT-IP對映通過ISE聚合通過SXP獲知：



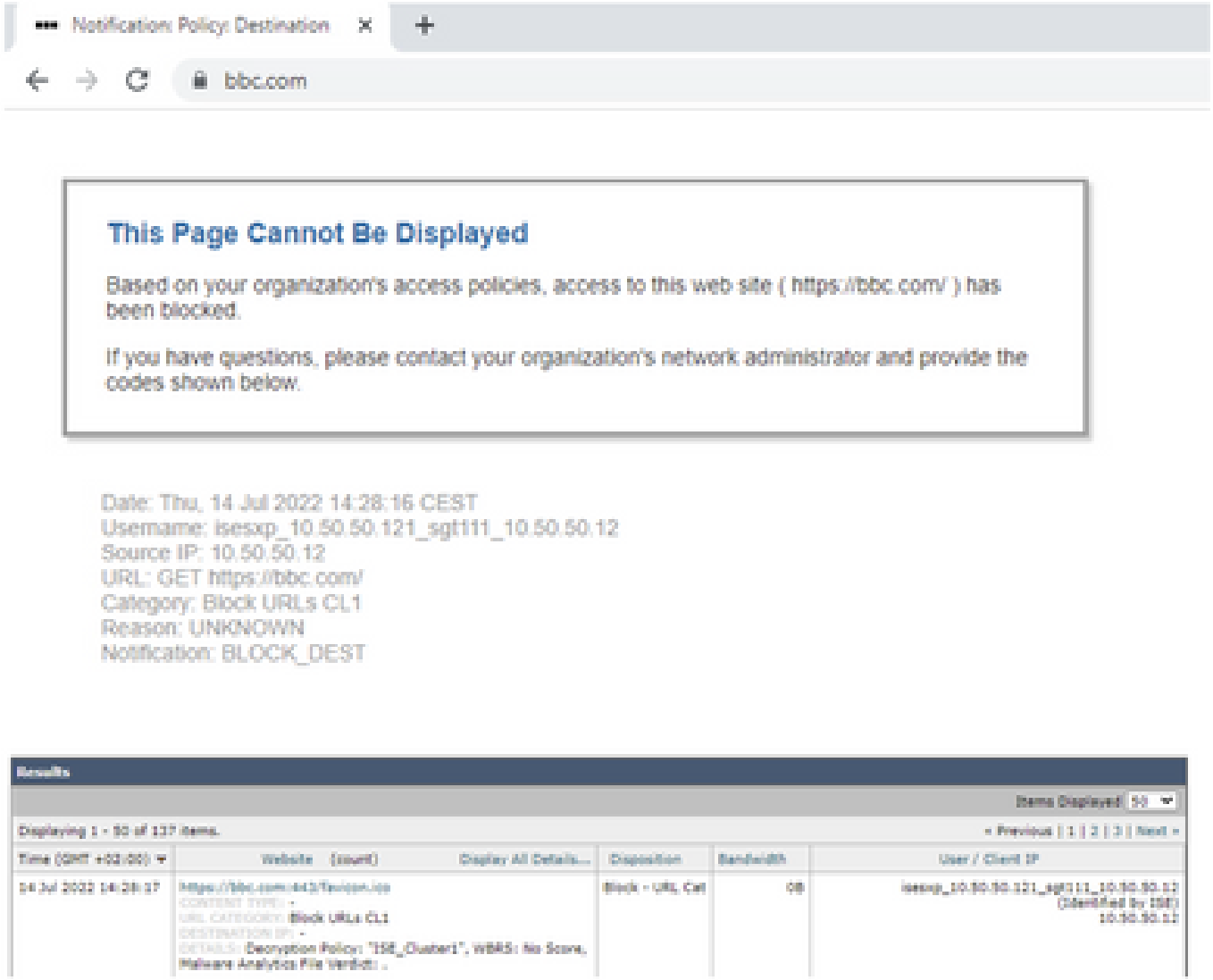
這些SXP對映來自不同的ISE群集，然後通過pxGrid通過ISE聚合節點傳送到WSA:

```
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   -
```

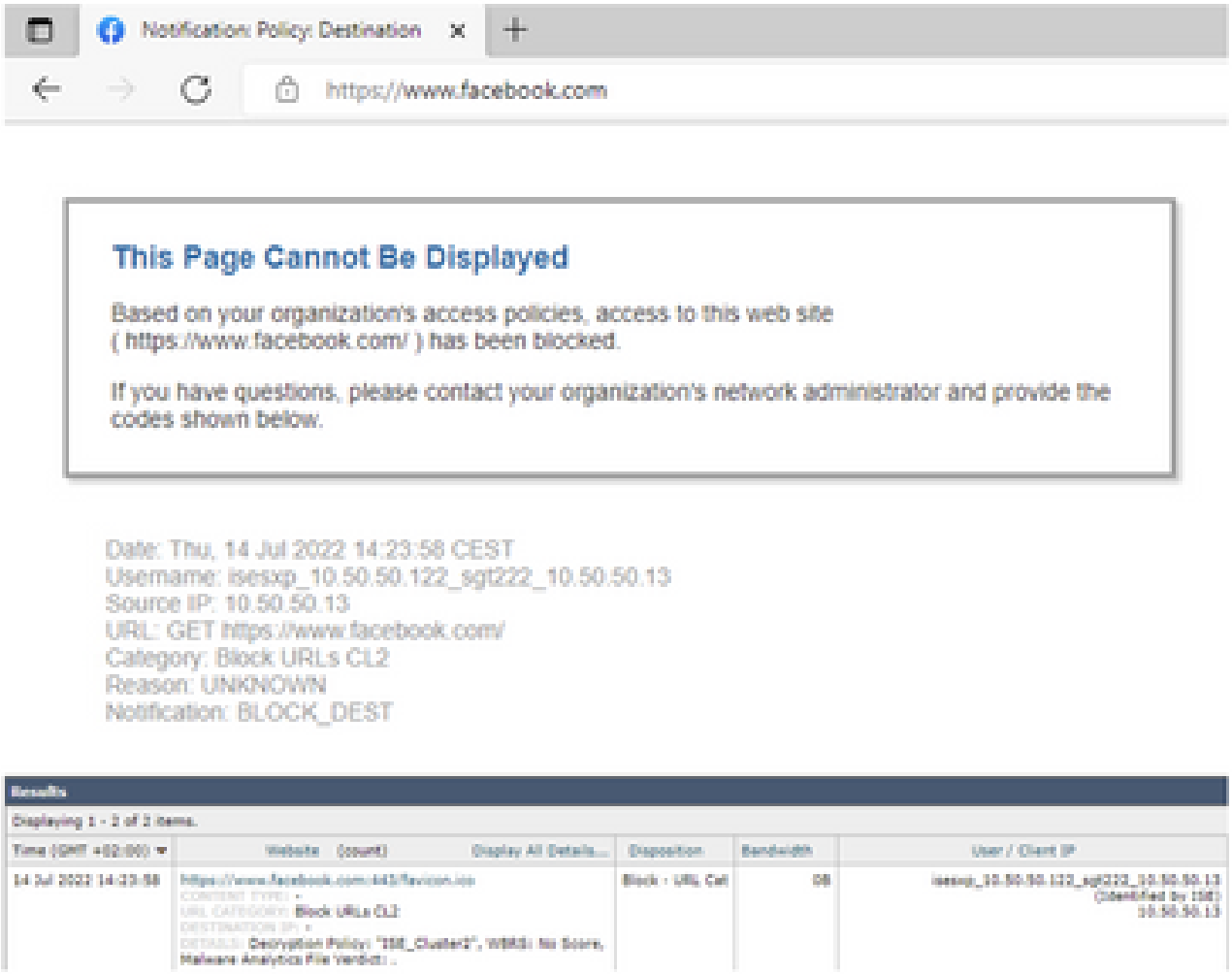
基於SGT的策略實施

在這裡，您可以看到不同的終端與其各自的策略匹配，並根據其SGT阻止流量：

屬於ISE集群1的端點



屬於ISE集群2的終結點



相關資訊

- 網路安全裝置和身份服務引擎整合指南
- 為TrustSec感知服務配置WSA與ISE整合
- 思科身份服務引擎管理員指南3.1版
- Cisco Secure Web Appliance AsyncOS 14.5使用手冊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。