在Catalyst 9800 WLC和ISE伺服器上配置和驗證SGACL

目錄

簡介

本文檔介紹如何在Catalyst 9800和ISE伺服器上配置TrustSec以利用SGACL功能，以及本地和FlexConnect模式AP。

必要條件

需求

瞭解Cisco 9800 WLC、Cisco ISE、FlexConnect和TrustSec基礎知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C9800-CL v17.12.4
- ISE 3.2.0
- 9136I存取點

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。

設定

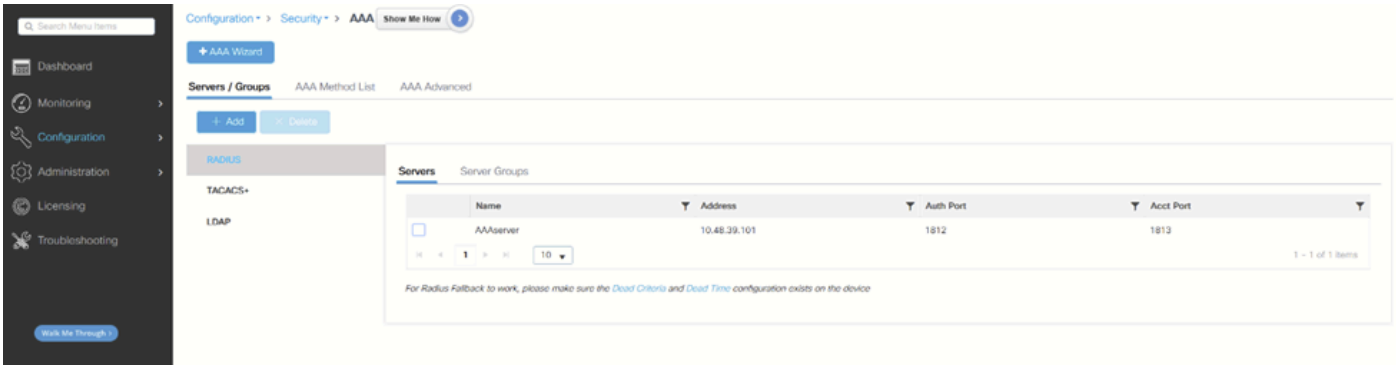
網路圖表

網路圖表

組態

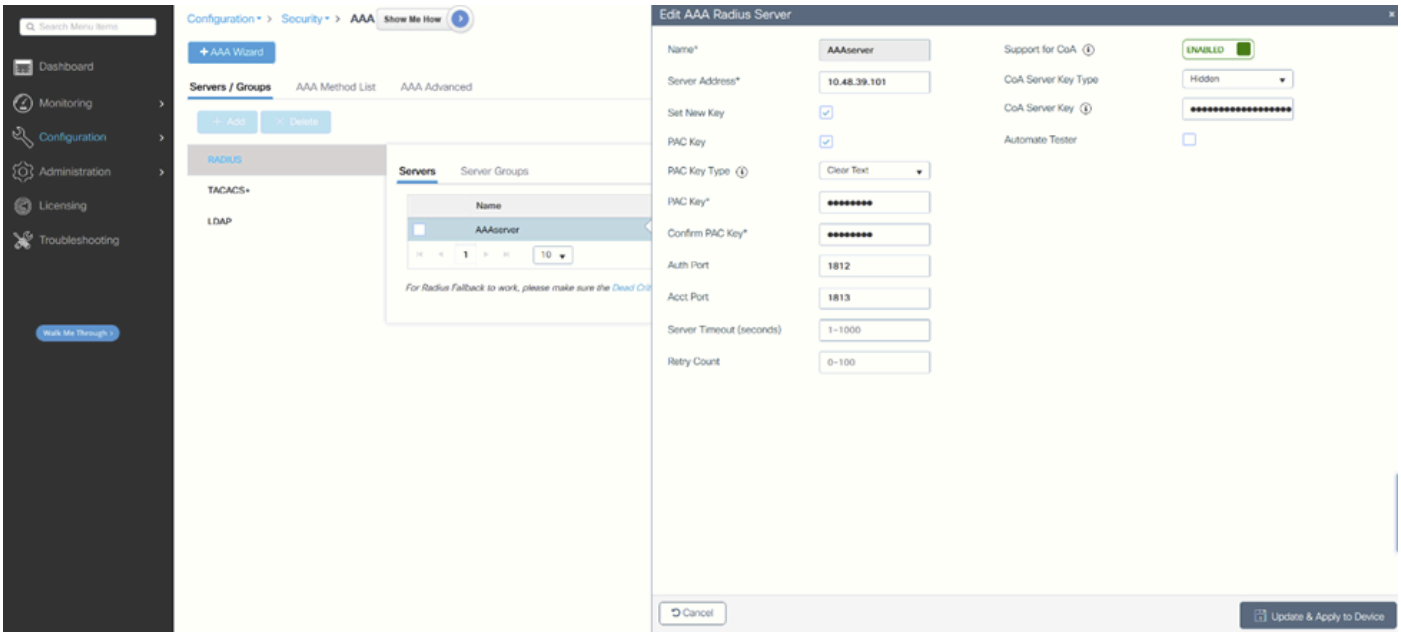
WLC組態

1.從Configuration > Security > AAA:



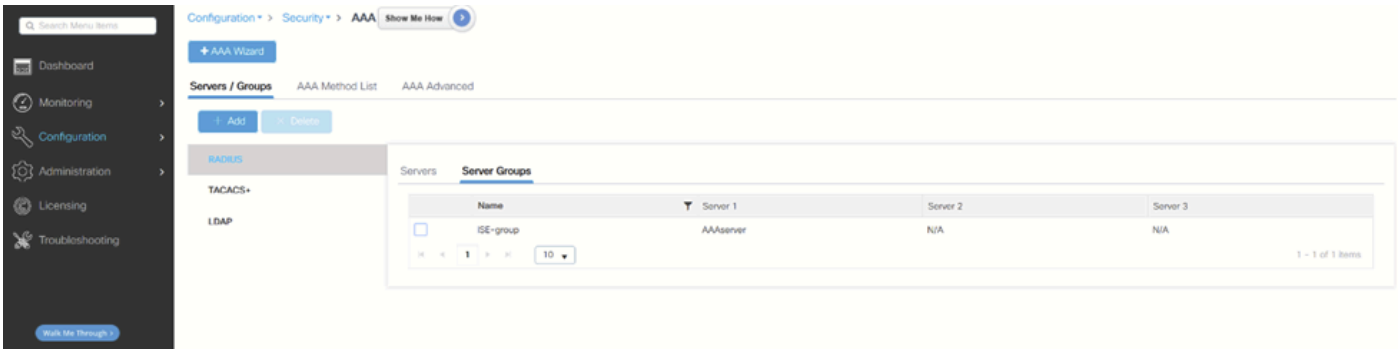
WLC AAA頁面

2.在ISE上新增裝置時，確保此處的金鑰條目與金鑰匹配。如果您希望使用CoA下載配置更新，請啟用CoA支援並新增金鑰：



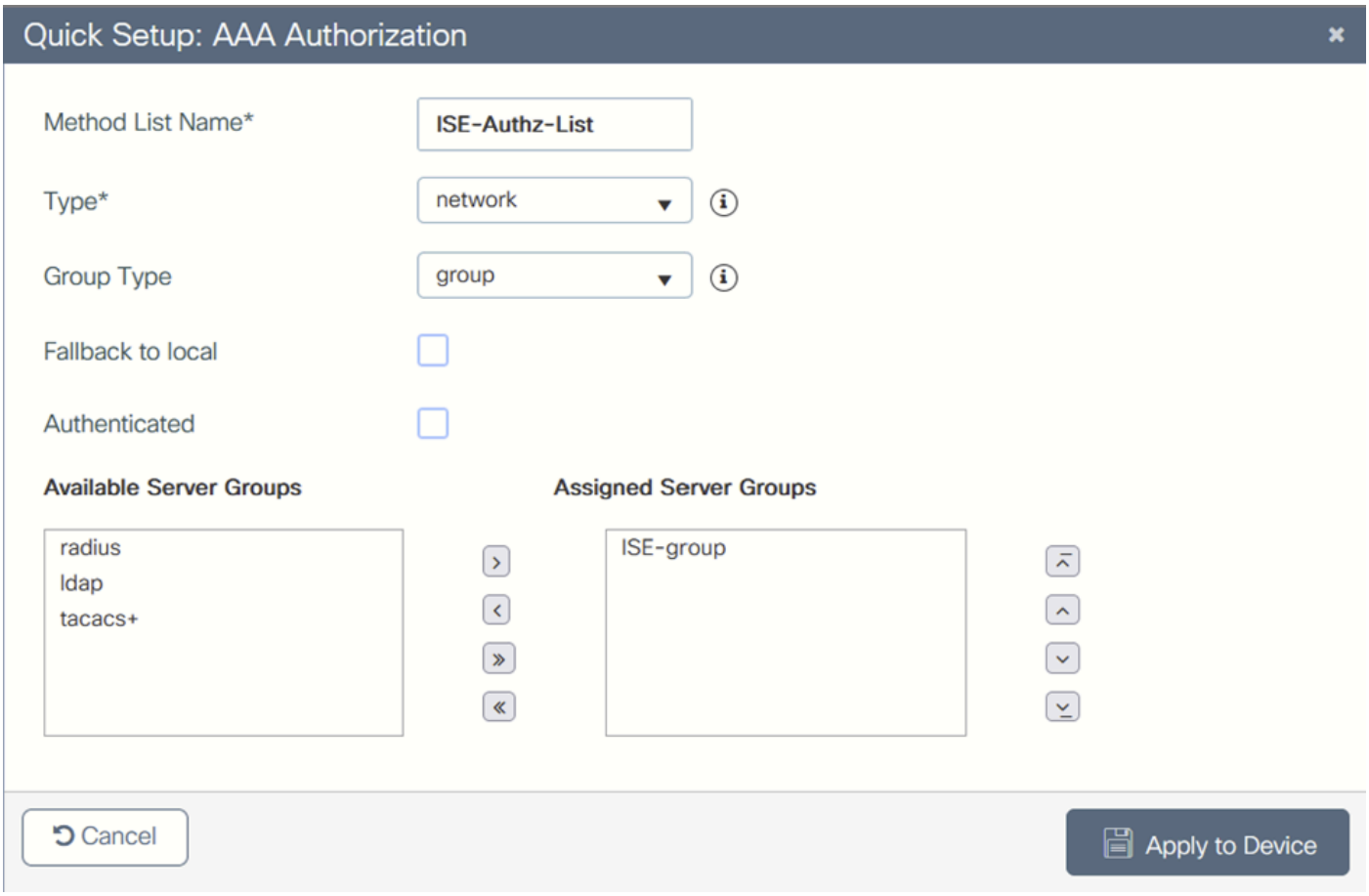
WLC增加AAA伺服器

3.建立伺服器組：

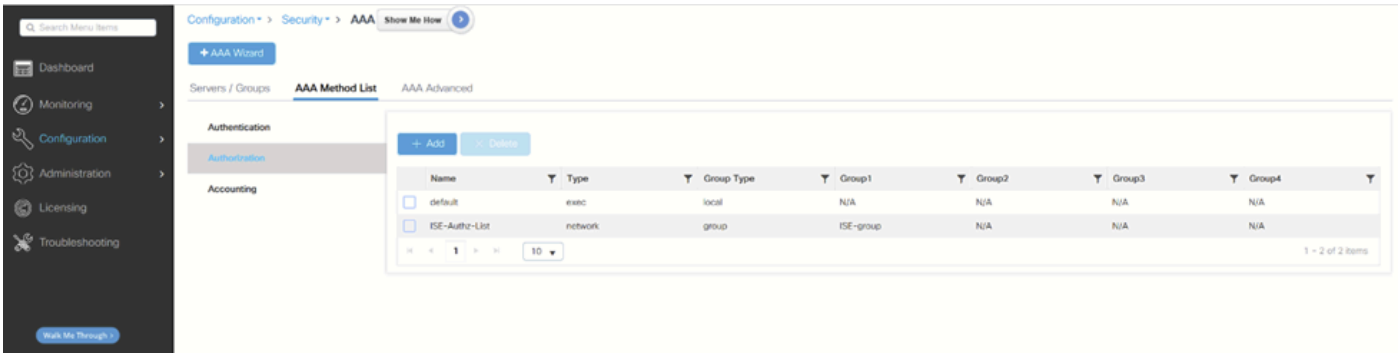


WLC新增伺服器組

4.新增network型別的Authorization Method List:



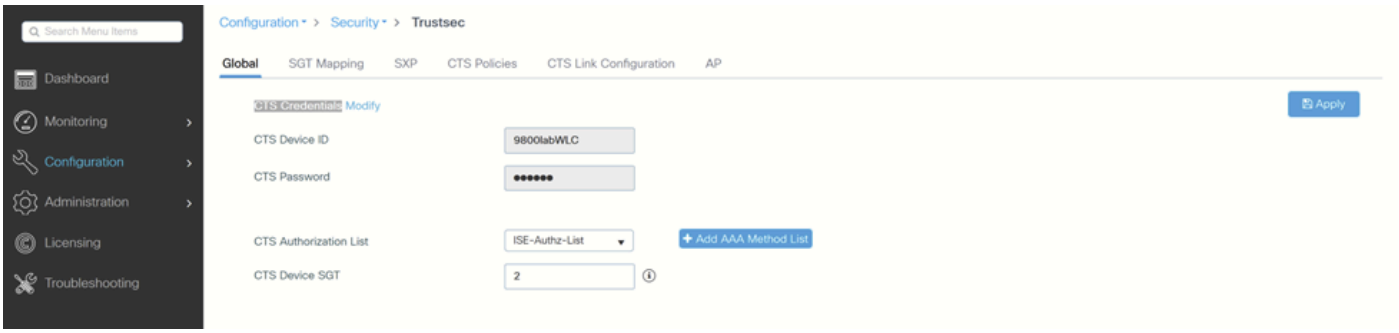
授權方法清單



WLC AAA伺服器群組

5.導航到Configuration > Security > Trustsec並配置CTS Device ID和CTS Password，您將在ISE上新增裝置時使用這些條目。

在此處配置在步驟4中建立的CTS授權清單：

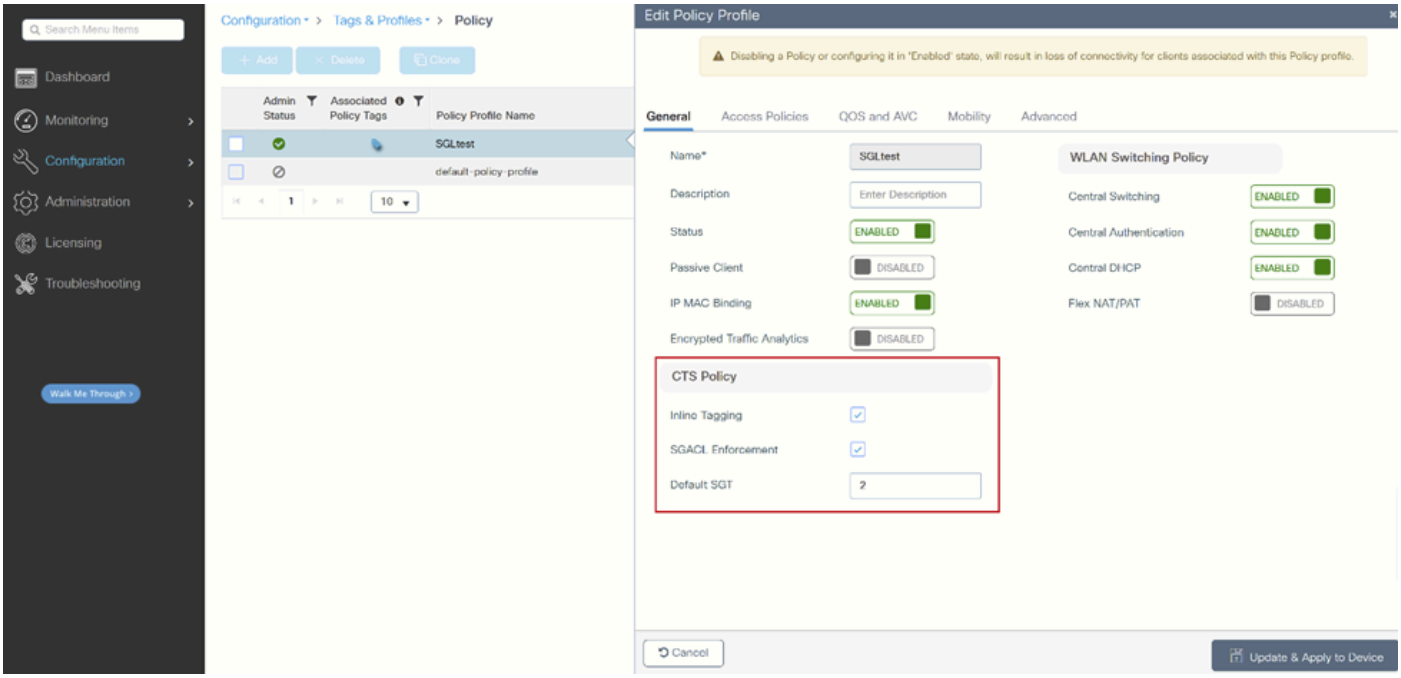


WLC TrustSec

6.在本示例中，已建立WLAN且已配置身份驗證設定。

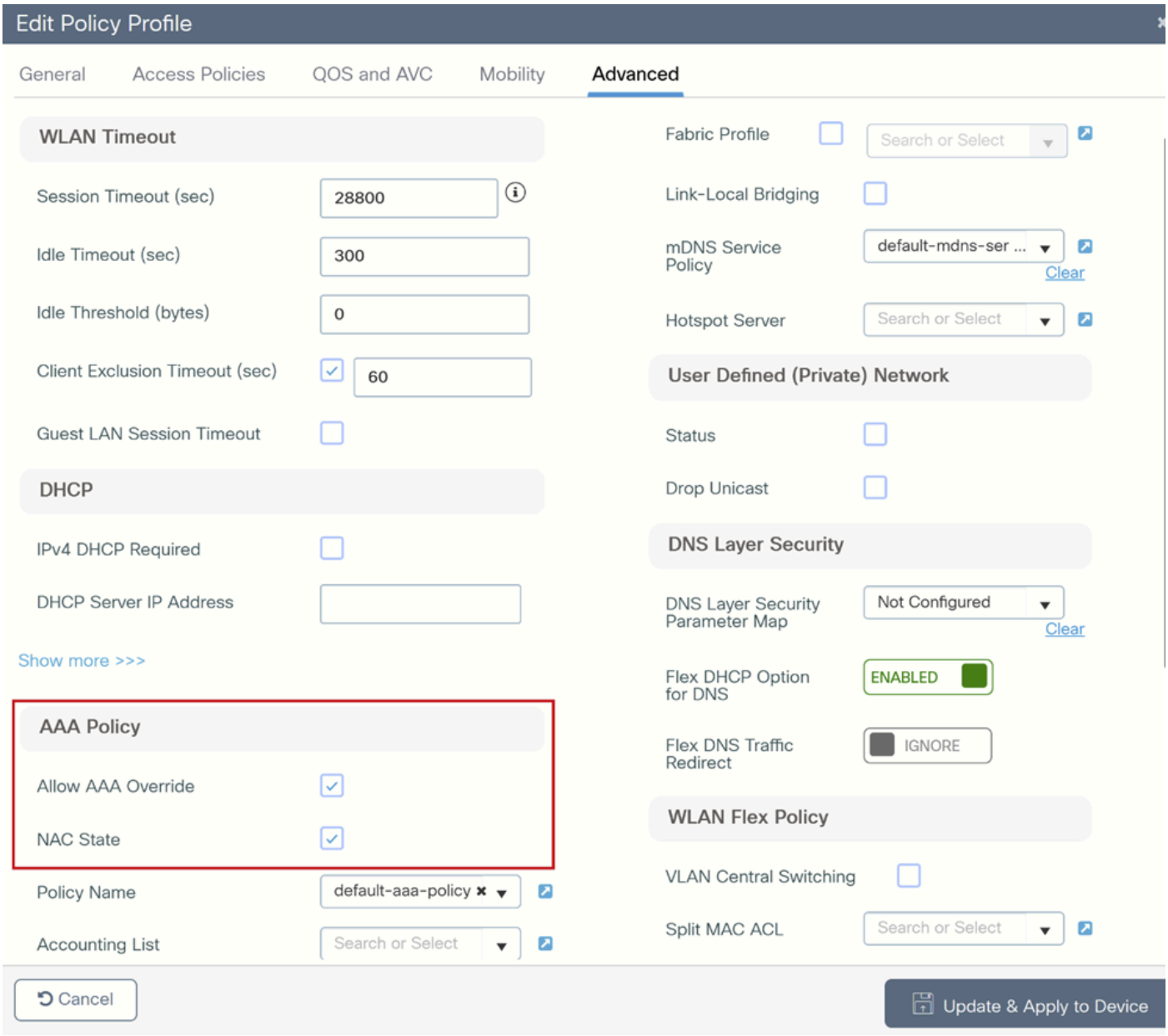
現在，導航到要在其上使用SGT的策略配置檔案。

i.在CTS Policy下，啟用Inline Tagging和SGACL Enforcement，您還可以指定Default SGT。本實驗使用預設SGT 2作為示例：



WLC原則設定檔

二。在Advanced索引標籤下，啟用Allow AAA override和NAC state:



WLC Policy Profile Advanced頁籤

在CLI上：

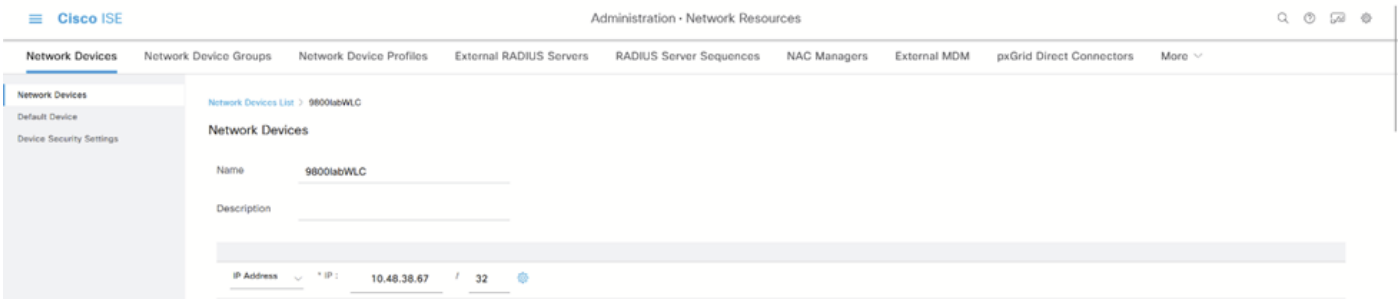
```
# configure terminal

(config)# radius server <server_name>
(config-radius-server)# address ipv4 <server_IP>
(config-radius-server)# pac key <password>

(config)# aaa server radius dynamic-author
(config-locsvr-da-radius)# client <server_IP> server-key <password>

(config)# aaa group server radius <server_group_name>
(config-sg-radius)# server name <server_name>
(config-sg-radius)# ip radius source-interface Vlan#

(config)# aaa authorization network <author_method_list> group <server_group_name>

(config)# cts authorization list <author_method_list>
```

```
(config)# wireless profile policy <policy_profile_name>
(config-wireless-policy)# shut
(config-wireless-policy)# aaa-override
(config-wireless-policy)# cts inline-tagging
(config-wireless-policy)# cts role-based enforcement
(config-wireless-policy)# cts sgt <number>
(config-wireless-policy)# no shut

# show cts credentials
CTS password is defined in keystore, device-id = 9800labWLC
```

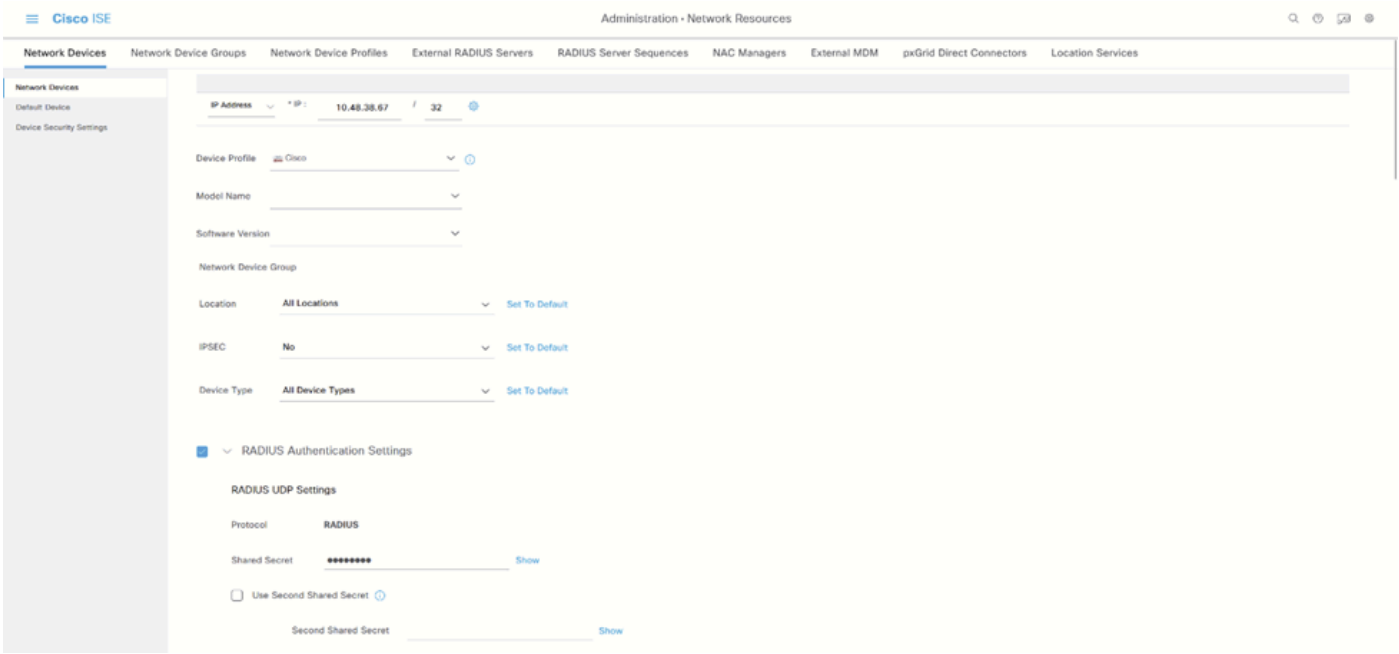
ISE 組態

1.定位至管理>網路資源>網路裝置。

i.在此處新增WLC資訊：

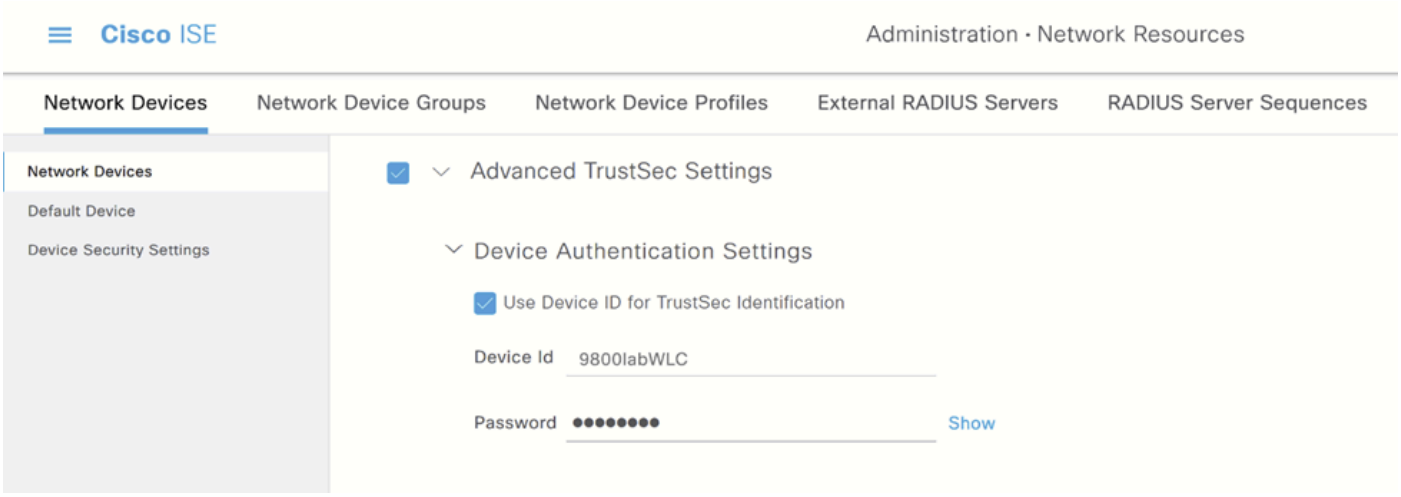


「ISE網路裝置」頁面



ISE新增WLC RADIUS資訊

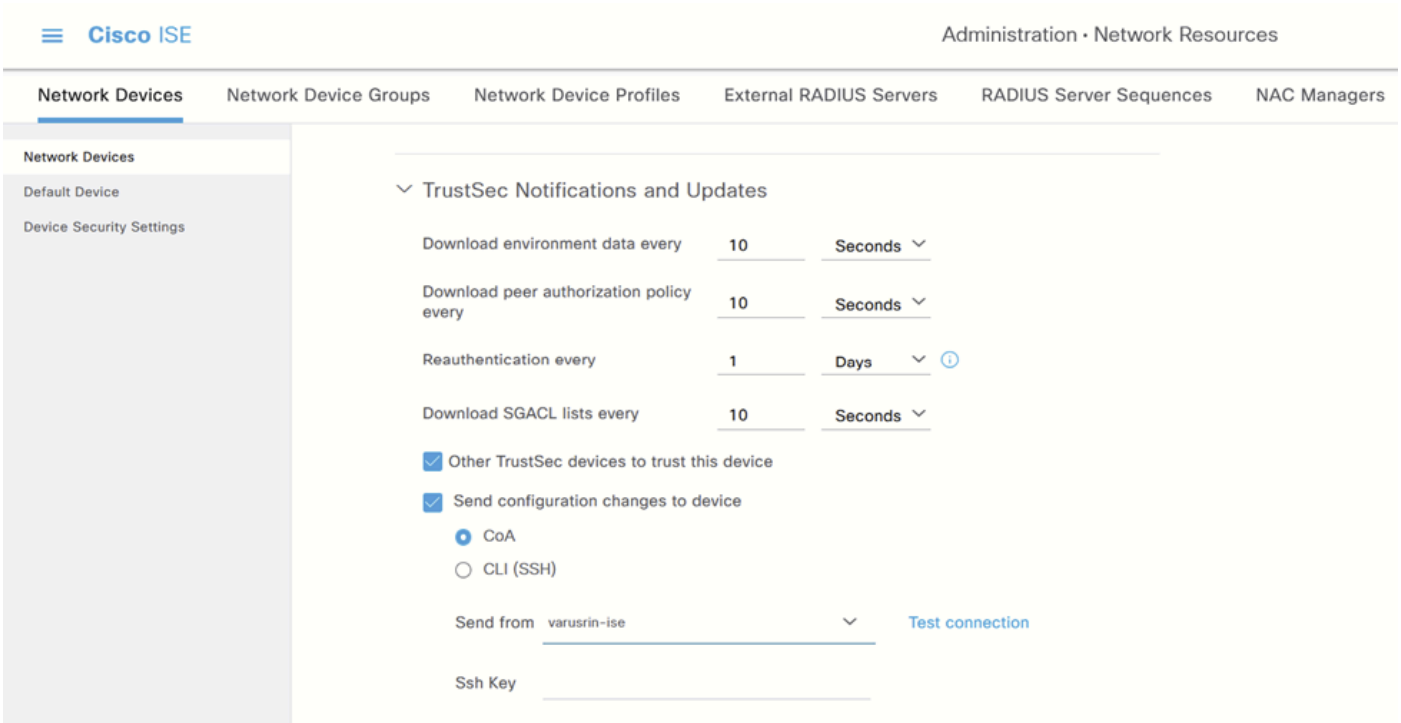
二。向下滾動並配置Advanced TrustSec Settings，啟用Use Device ID for TrustSec Identification覈取方塊並配置密碼：



高級TrustSec設定

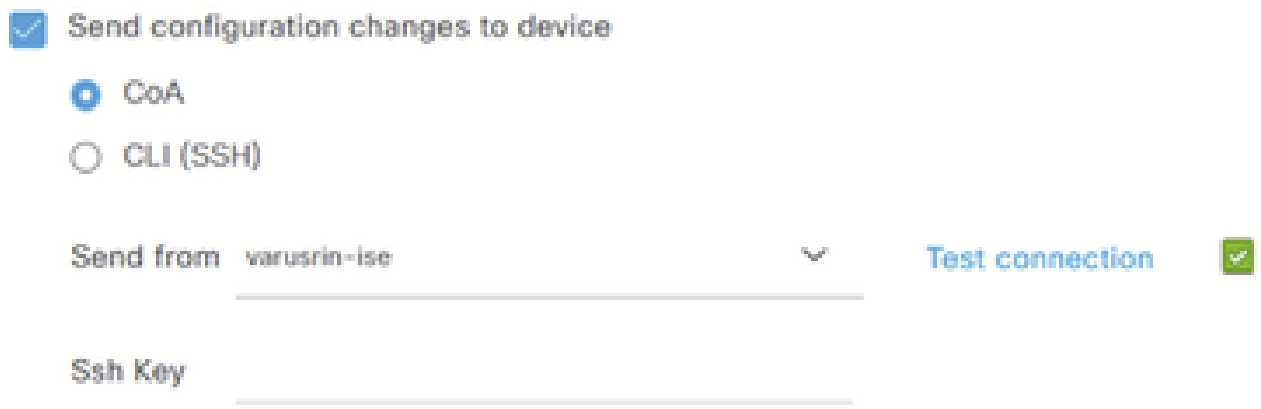
此專案必須與WLC組態步驟6中WLC一端的組態相符。

三。向下滾動到TrustSec通知和更新，並配置是否要使用CoA或SSH進行配置更新。選擇所需的ISE節點：



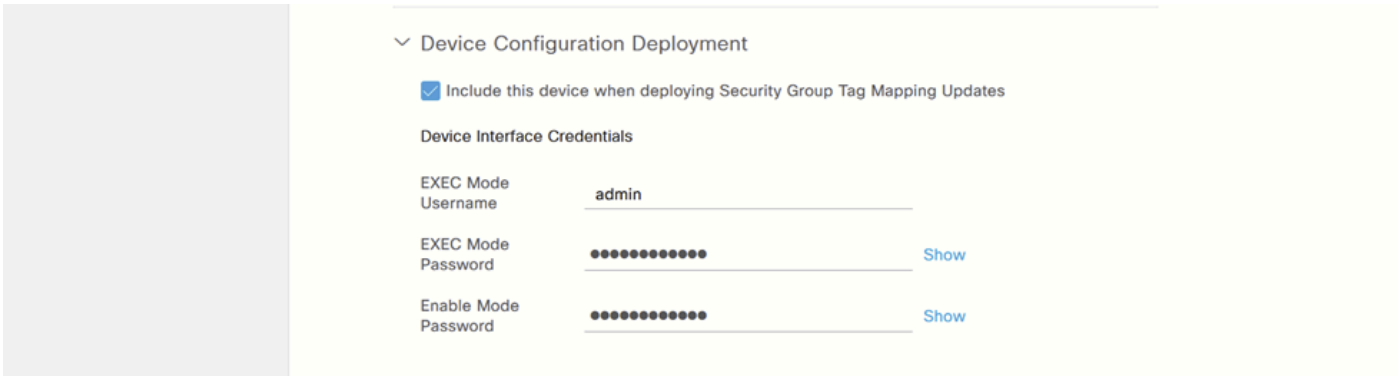
TrustSec通知和更新

2.按Test connection以確保已建立連線。當它成功時，它將顯示綠色勾選標籤：



測試連線

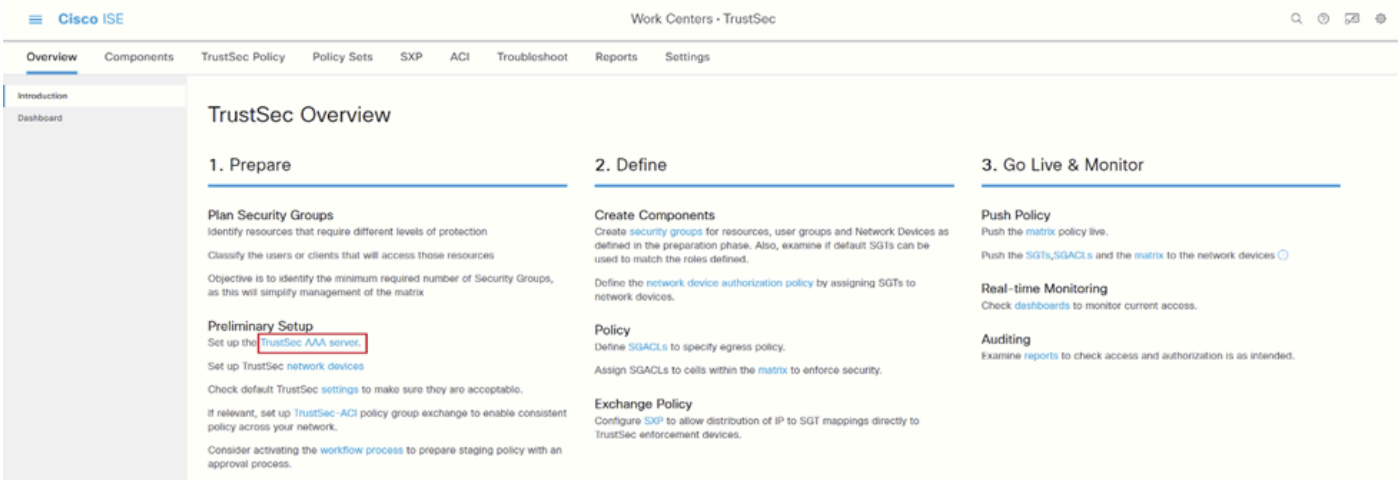
i.向下滾動並配置部署SGT對映更新時要包括的WLC，如果您在上一步中選擇了SSH選項，這一點非常重要：



裝置配置部署

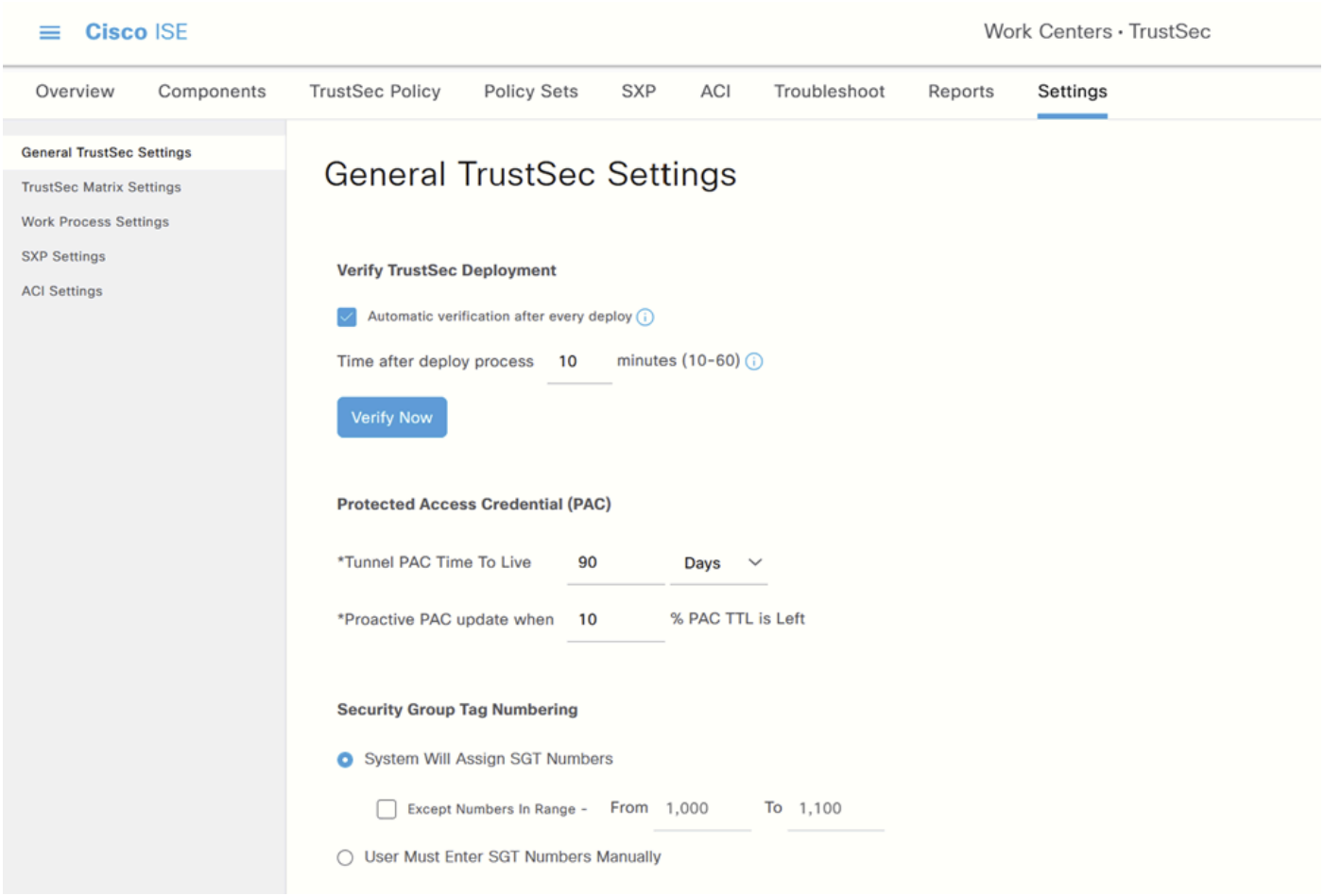
二。儲存組態。

3.在「工作中心」>「TrustSec」>「概觀」中，您有TrustSec配置選項。選擇TrustSec AAA Server以檢視正在使用的ISE例項。如果有多個例項，請參閱Cisco Catalyst無線基於組的策略，瞭解有關使用哪個例項的詳細資訊。



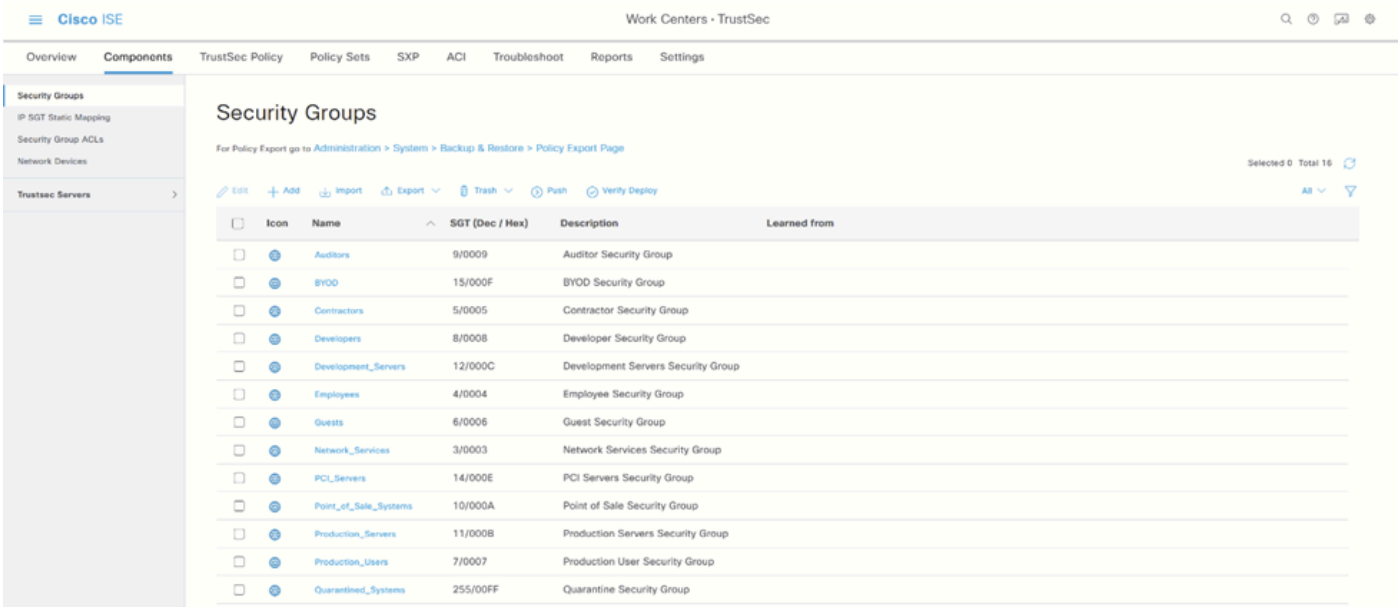
ISE TrustSec概述

4.（可選）導航到Settings頁籤，啟用Automatic verification after every deploy（如果可取）。



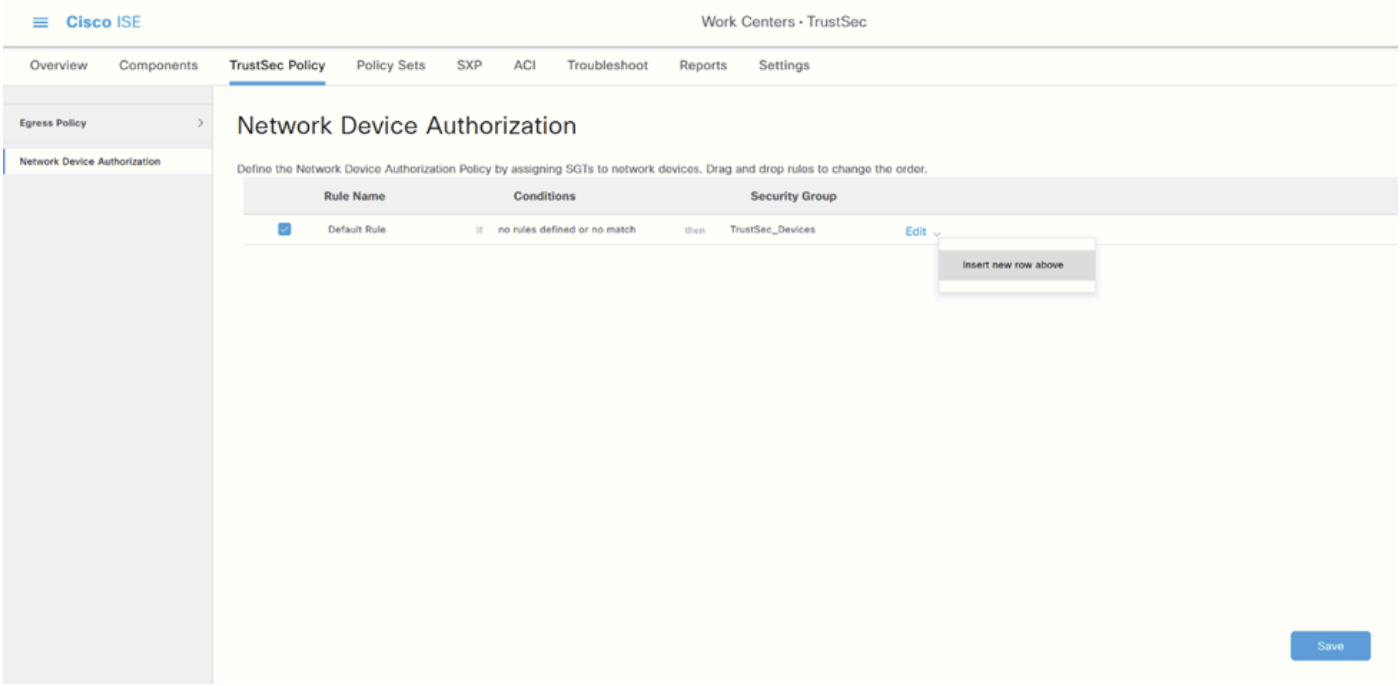
ISE TrustSec設定

5.根據您的要求，從工作中心> TrustSec > Components > Security Groups新增或編輯SGT值：



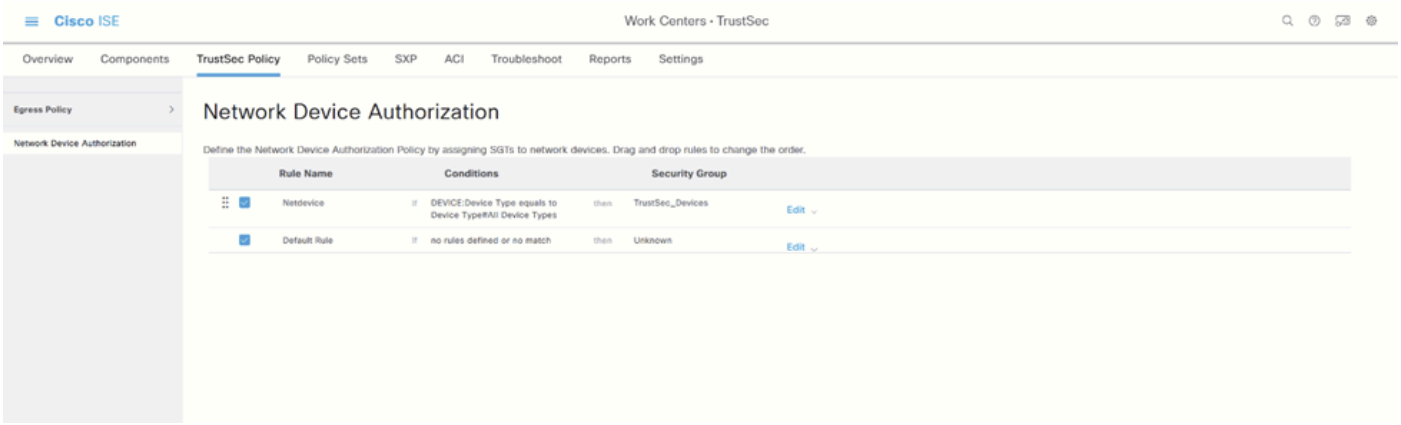
ISE安全組

6.如果要指定授權策略，請導航到工作中心> TrustSec > TrustSec Policy > Network Device Authorization:



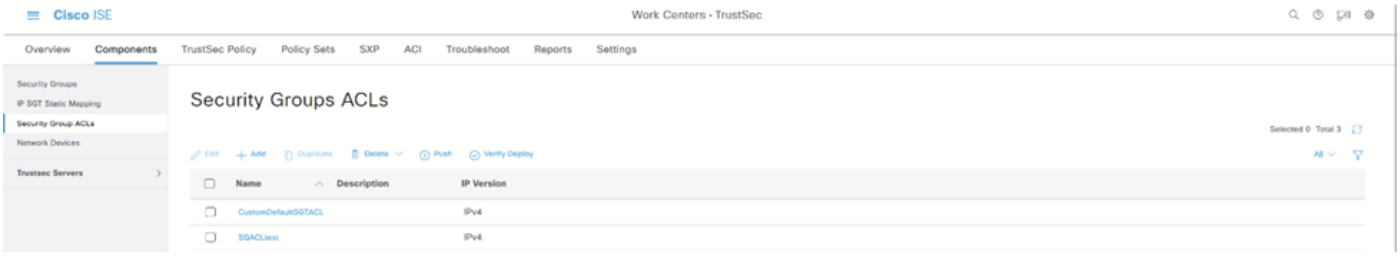
TrustSec策略

您可以保留預設值，但在本實驗中，我們使用以下配置作為示例：



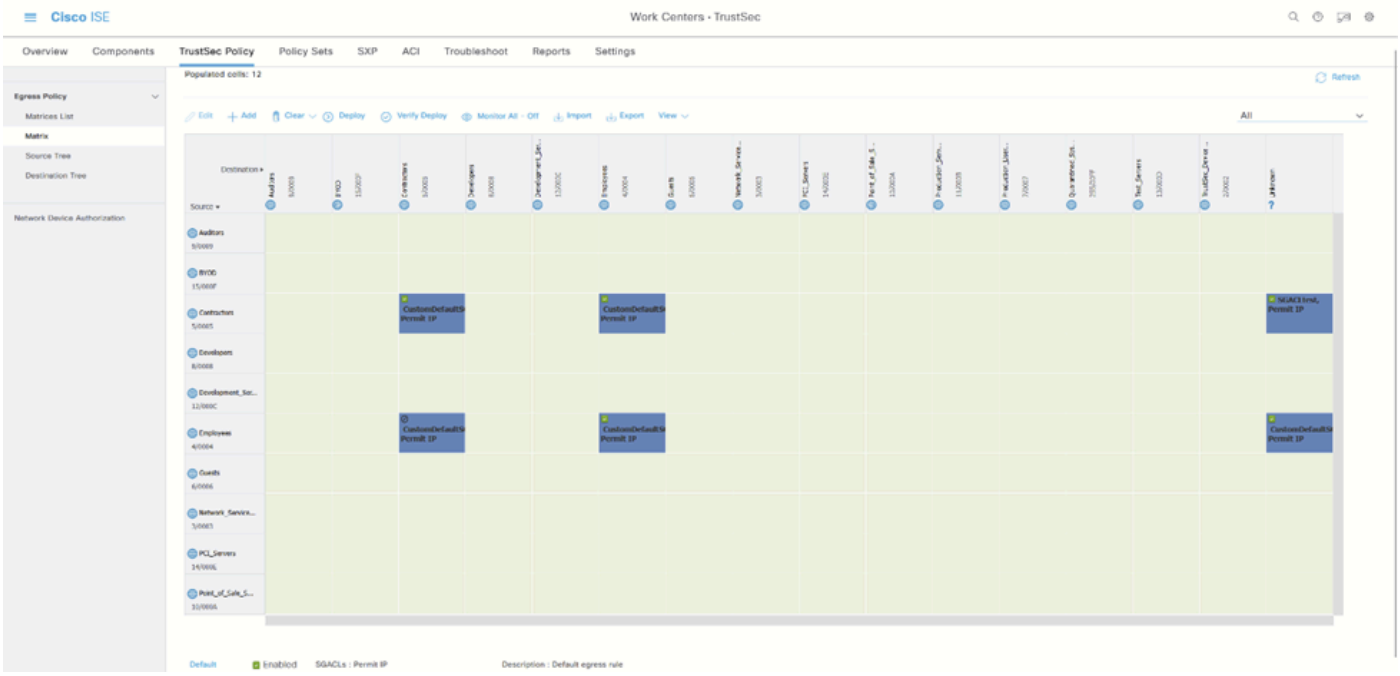
網路裝置授權

7.在Components頁籤下建立SGACL，然後建立Security Group ACL:



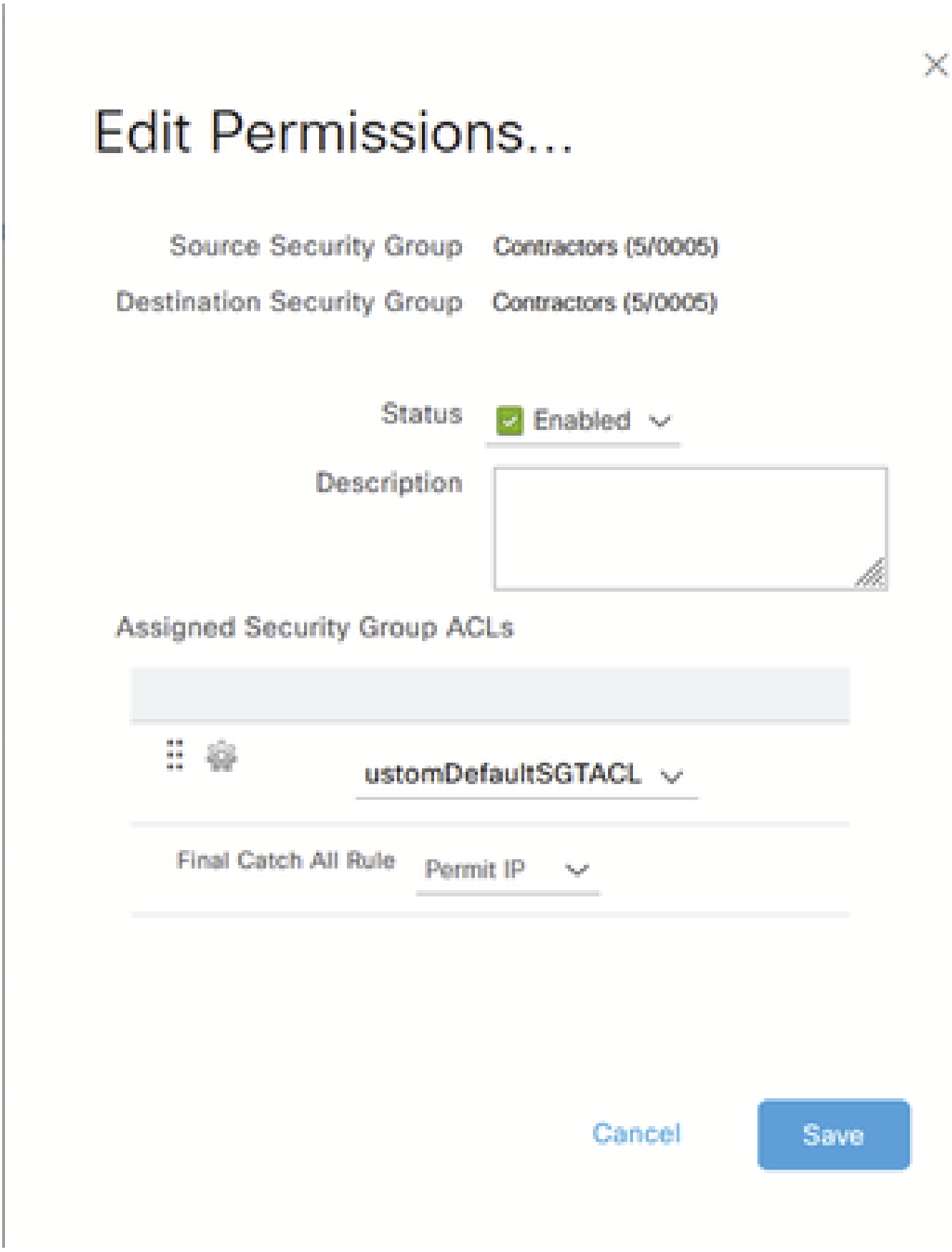
安全群組ACL

8.在TrustSec Policy頁籤下指定矩陣條目，然後在Matrix下指定。您可以通過按一下兩個SGT的交匯點來編輯許可權：

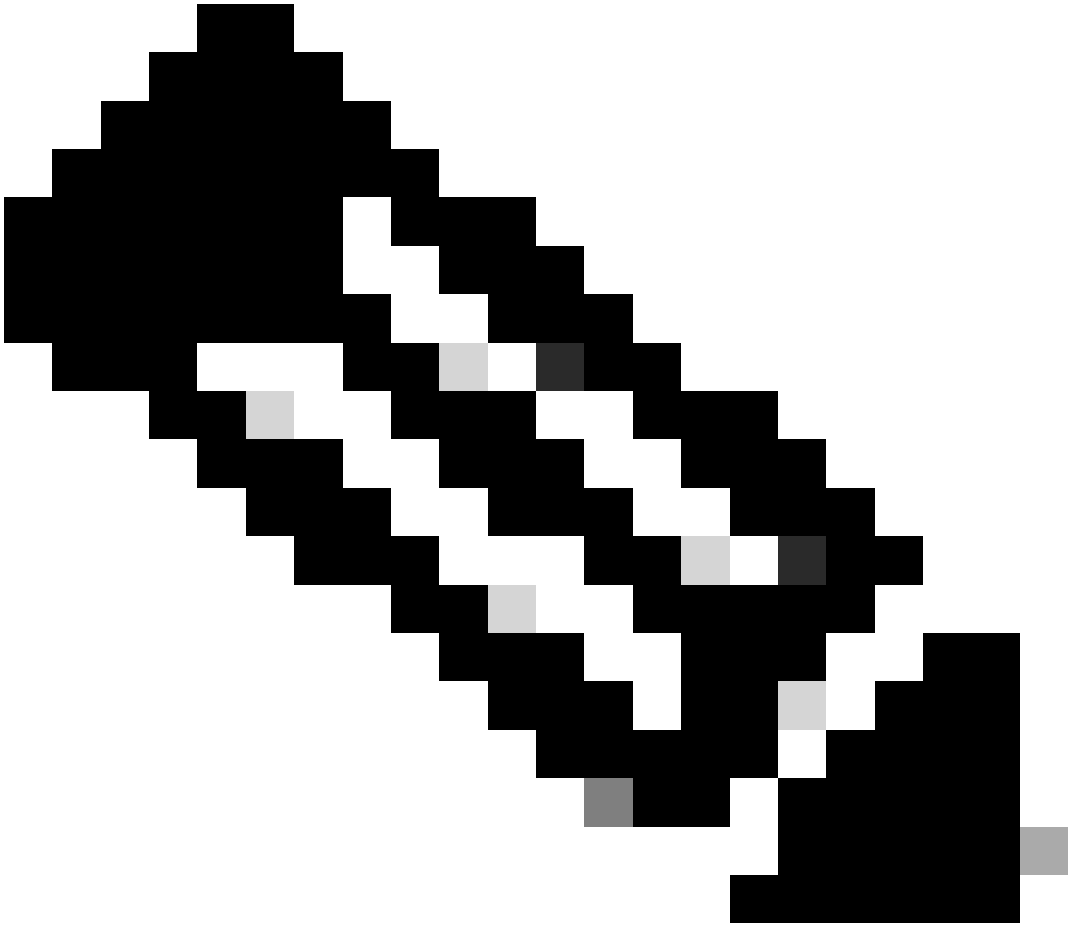


ISE TrustSec矩陣

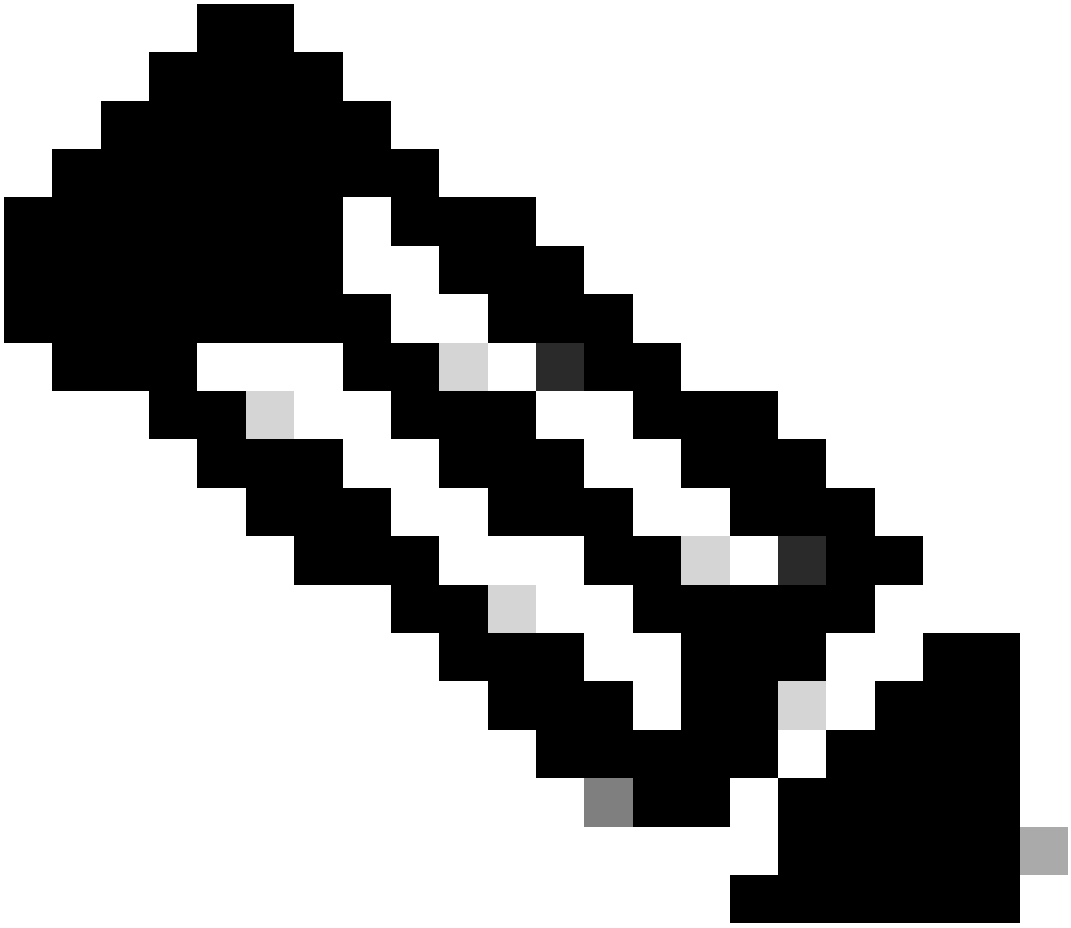
舉例來說：


Edit Permissions...
Source Security Group
Contractors (5/0005)
Destination Security Group
Contractors (5/0005)
Status
Enabled
Description
Assigned Security Group ACLs
ustomDefaultSGTACL
Final Catch All Rule
Permit IP
Cancel
Save

編輯許可權

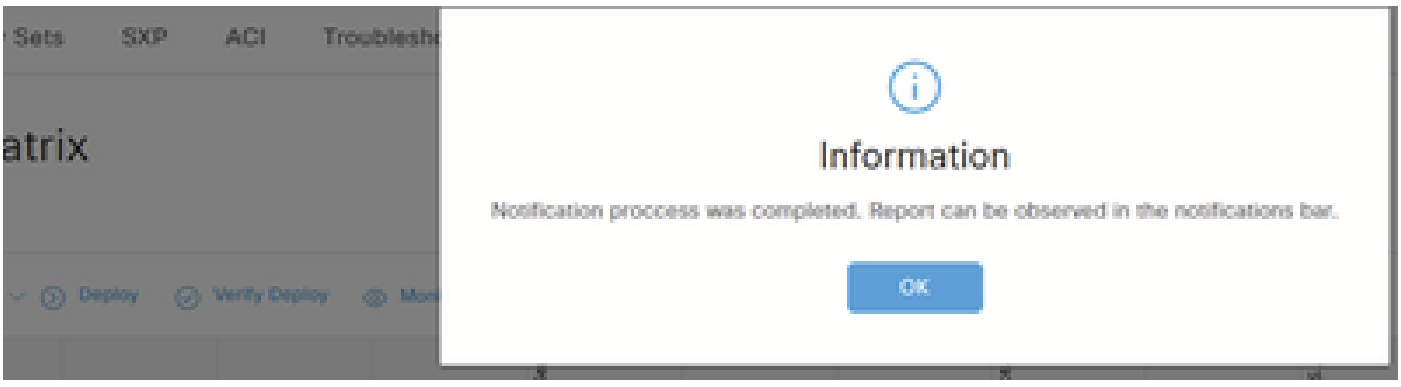


附註：在允許清單模式的情況下，您需要明確允許客戶端裝置的DHCP協定來獲取DHCP IP地址，然後請求控制器執行SGACL策略。

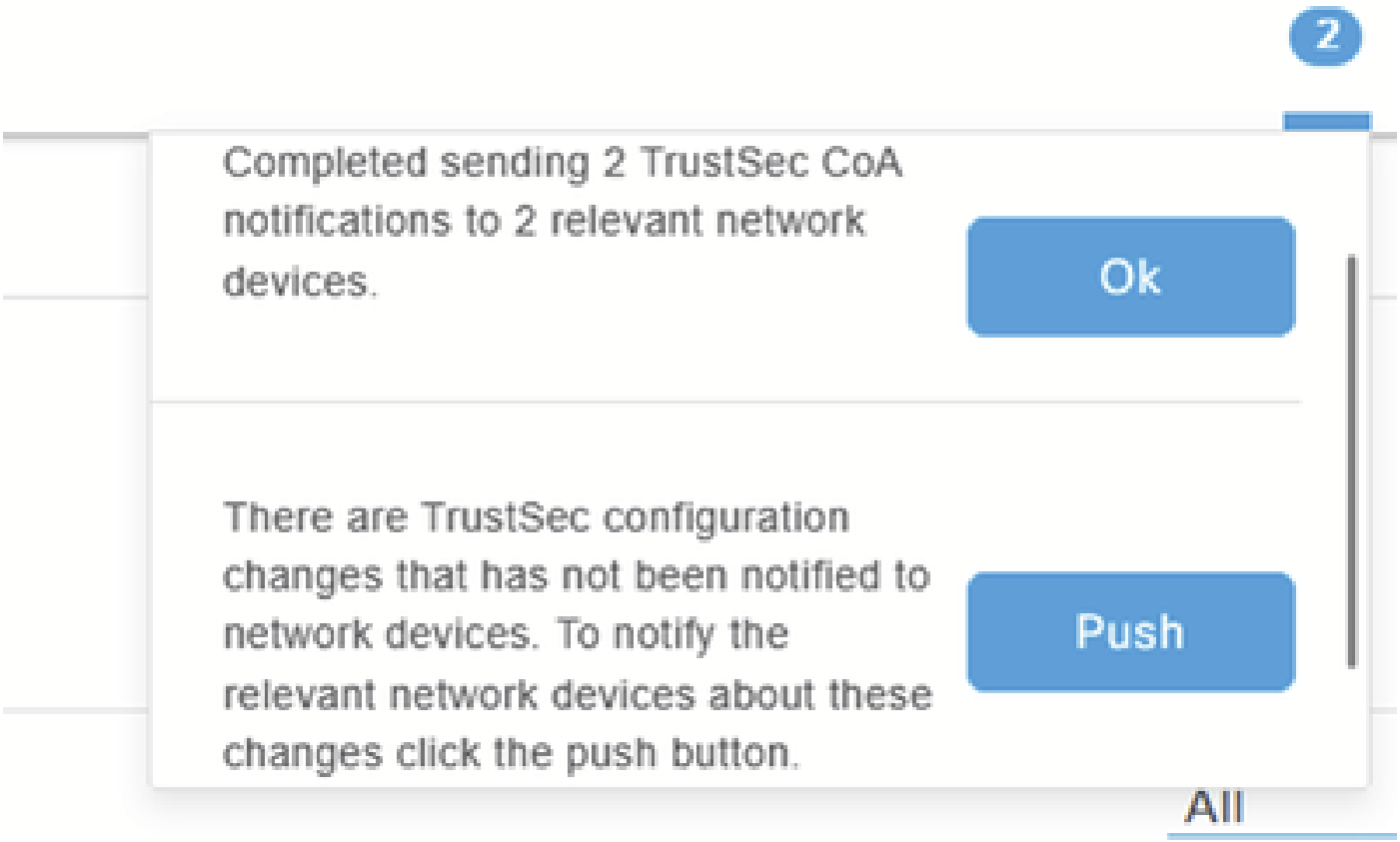


附註：當TrustSec策略「未知到未知」在TrustSec矩陣中被拒絕時，客戶端接收零SGT值，DHCP客戶端接收自動私有IP定址(APIPA)地址。
當TrustSec矩陣中允許TrustSec策略「未知到未知」時，客戶端接收正確的SGT值，DHCP客戶端接收IP地址。

9.按一下Deploy。這將產生以下消息和通知：



部署

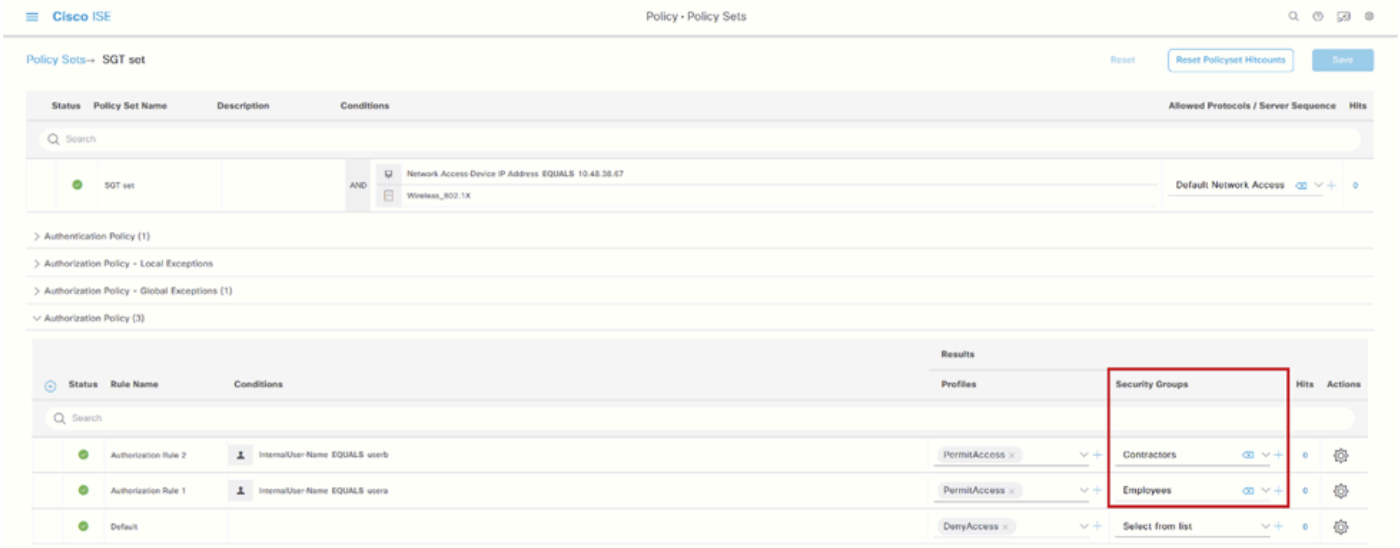


部署通知

10.導航到Policy > Policy Sets下的Policy Set for the WLAN:

ISE策略集

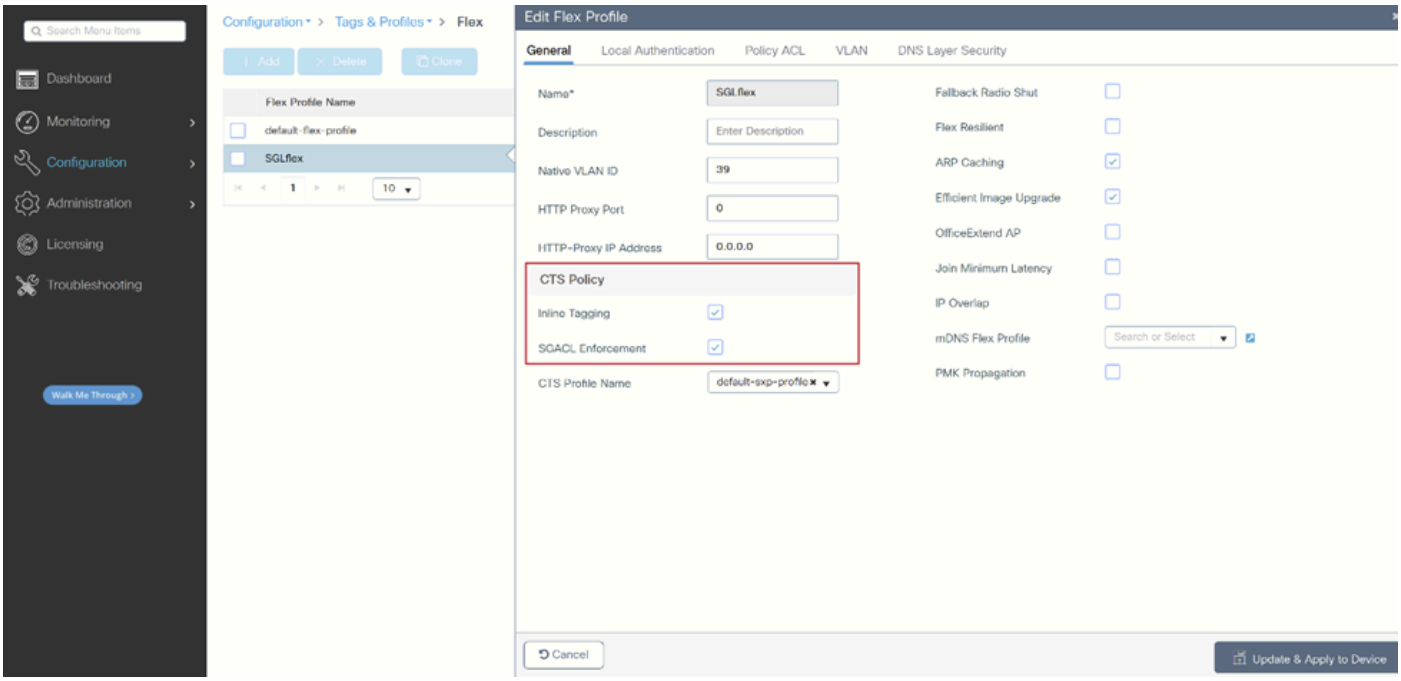
在本實驗中，我們將定義每個使用者的SGT，選擇Security Groups欄位下的SGT:



ISE安全組

Flexconnect

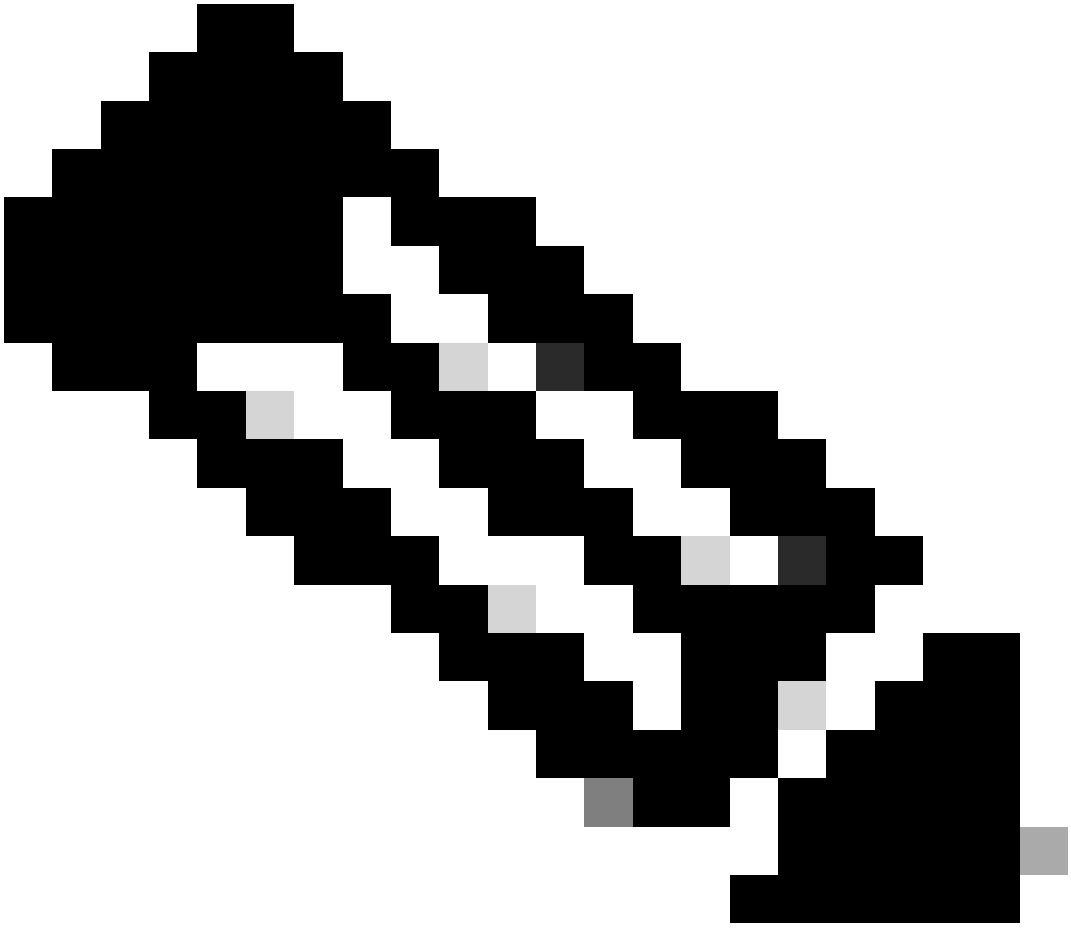
在Configuration > Tags & Policies > Flex下的Flex配置檔案上啟用內聯標籤和SGACL實施:



WLC Flex設定檔

在CLI上：

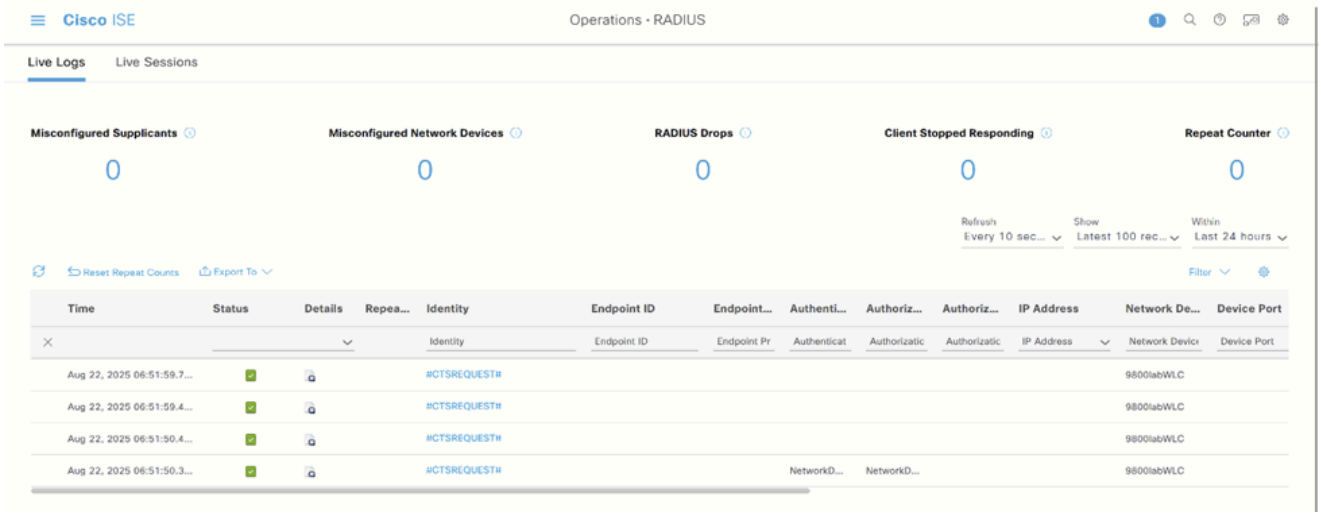
```
# configure terminal

(config)# wireless profile flex SGLflex
(config-wireless-flex-profile)# cts inline-tagging
(config-wireless-flex-profile)# cts role-based enforcement
```



附註：如果WLC在HA-SSO中，則不支援FlexConnect AP上的SGACL。思科錯誤ID CSCwn85468。此錯誤將在17.19中新增。

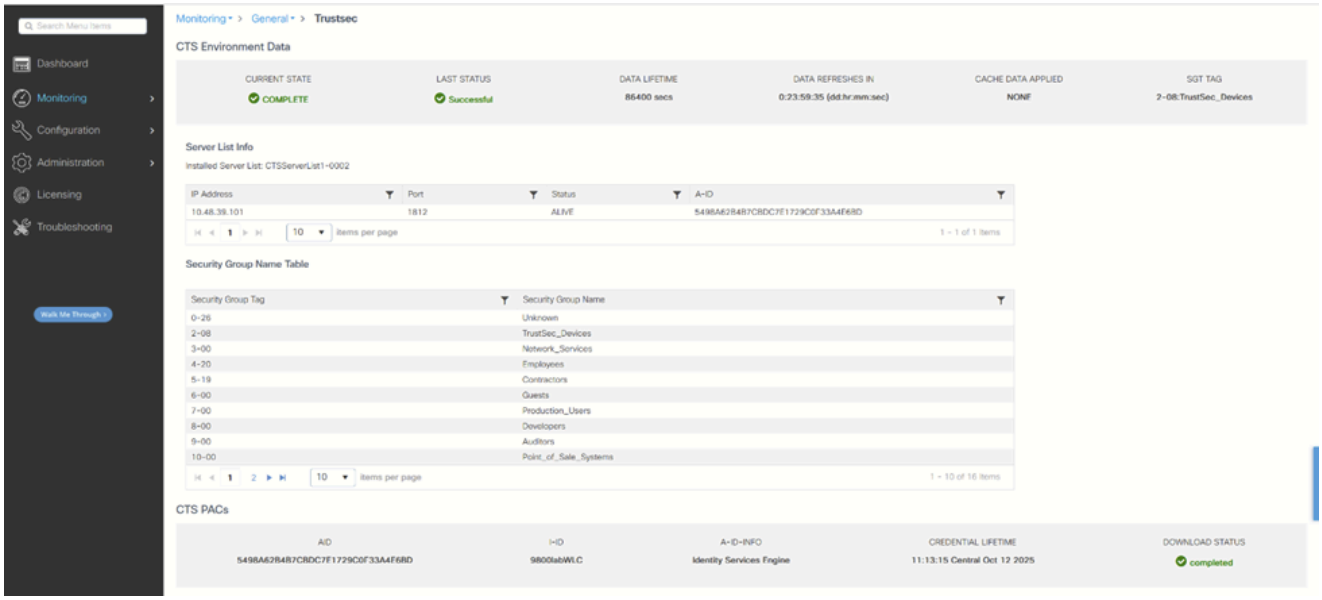
驗證

1. 在ISE中，您必須在Operations > RADIUS > Live Logs下看到成功的CTS請求：



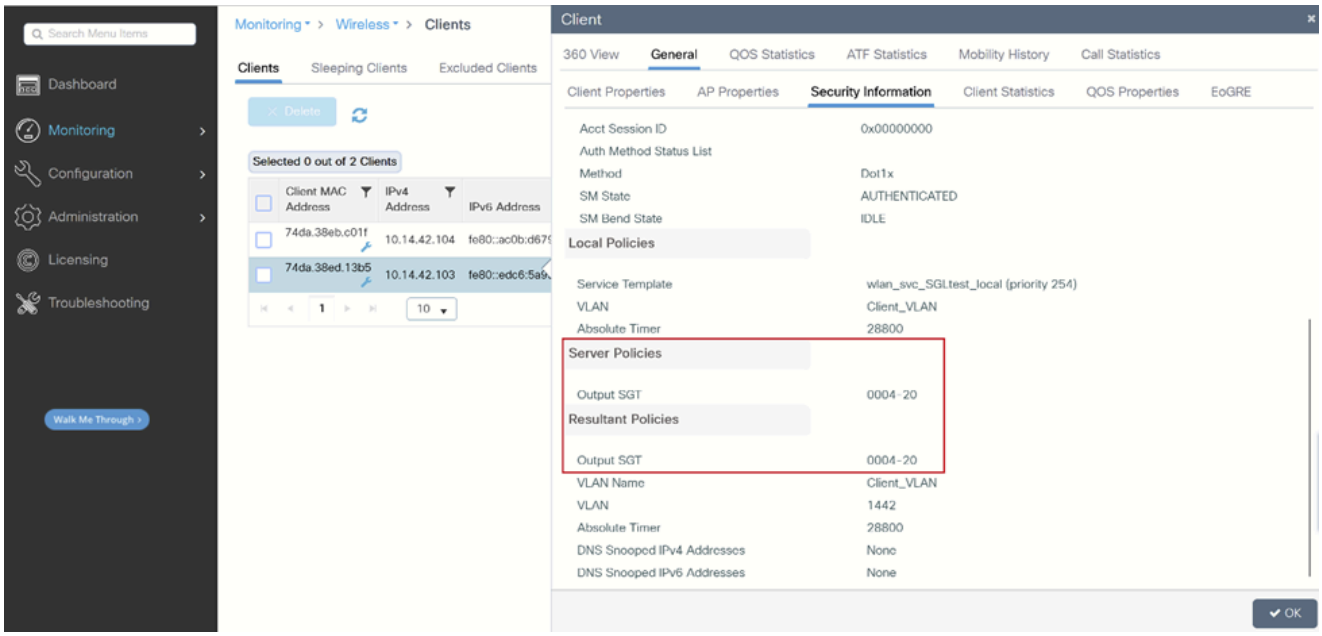
ISE RADIUS即時日誌

2. 您可以驗證是否已建立連線，以及是否已從WLC上的Monitoring > General > Trustsec下載SGT:



WLC TrustSec監控

3. 連線客戶端時，分配的SGT將顯示在Monitoring > Wireless > Clients下，選擇要檢查的客戶端，然後導航到General > Security information頁籤：



WLC使用者端監控

在CLI上：

- 在連線使用者端之前，您將在WLC輸出中看到以下內容：
  僅顯示與未知SGT相關的許可權。

```
<#root>

#

show cts role-based sgt-map all


Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.14.12.110            2       INTERNAL
10.48.39.55             2       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of INTERNAL bindings = 2
Total number of active   bindings = 2

Active IPv6-SGT Bindings Information

IP Address                                SGT     Source
============================================================


<#root>

#
```

show cts role-based permissions

```
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
        SGT32-06
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

- 連線客戶端時，您可以從RA跟蹤中觀察這些日誌，SGT從AAA應用：

<#root>

```
2025/08/14 08:44:47.072771984 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072786402 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072788080 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info):
```

[Applied attribute : security-group-tag   0 "0004-20"]

```
2025/08/14 08:44:47.072809490 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :bs
2025/08/14 08:44:47.072811627 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072824202 {wncd_x_R0-0}{1}: [auth-mgr] [15596]: (info): [0000.0000.0000:unknown]  R
2025/08/14 08:44:47.072829794 {wncd_x_R0-0}{1}: [ewlc-qos-client] [15596]: (info): MAC: 74da.38ed.13b5
2025/08/14 08:44:47.072860963 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [15596]: (debug): Managed client RUN
2025/08/14 08:44:47.072905375 {wncd_x_R0-0}{1}: [client-orch-state] [15596]: (note): MAC: 74da.38ed.13b
```

- 在CLI中使用show wireless client mac-address <client_MAC_address> detail命令，該命令將顯示分配給客戶端的SGT:

<#root>

```
#show wireless client mac-address 74da.38ed.13b5 detail

Client MAC Address : 74da.38ed.13b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.14.42.103
…
  Auth Method Status List
```

```
        Method : Dot1x
                SM State         : AUTHENTICATED
                SM Bend State    : IDLE
  Local Policies:
        Service Template : wlan_svc_SGLtest_local (priority 254)
                VLAN             : Client_VLAN
                Absolute-Timer   : 28800
  Server Policies:


       Output SGT       : 0004-20


  Resultant Policies:


Output SGT       : 0004-20


                VLAN Name        : Client_VLAN
                VLAN             : 1442
                Absolute-Timer   : 28800
…
```

- 在SGT 4中連線一個客戶端後，您會注意到SGT 4的許可權現在顯示：
  在連線客戶端並分配SGT之後新增許可權。

```
<#root>

#

show cts role-based permissions


IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
        SGT32-06

IPv4 Role-based permissions from group Unknown to group 4:Employees:


        CustomDefaultSGTACL-03


        Permit IP-00
```

IPv4 Role-based permissions from group 4:Employees to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 5:Contractors to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

```
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

<#root>

#

show cts role-based sgt-map all

```
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.14.12.110            2       INTERNAL
10.14.42.103            4       LOCAL
10.48.39.55             2       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 2
Total number of active   bindings = 3

Active IPv6-SGT Bindings Information

IP Address                                  SGT     Source
============================================================
```

- 連線兩個客戶端後，一個位於SGT 4中，另一個位於SGT 5中：

<#root>

#

show cts role-based sgt-map all

```
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
========================================
10.14.12.110            2       INTERNAL
10.14.42.103            4       LOCAL
10.14.42.104            5       LOCAL
10.48.39.55             2       INTERNAL

IP-SGT Active Bindings Summary
========================================
Total number of LOCAL    bindings = 2
Total number of INTERNAL bindings = 2
Total number of active   bindings = 4

Active IPv6-SGT Bindings Information

IP Address                                  SGT     Source
============================================================
```

- 現在您可以看到SGT 5的許可權已新增：

<#root>

#

show cts role-based permissions

```
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
        SGACLtest-03
        Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
        CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
        SGT32-06
IPv4 Role-based permissions from group Unknown to group 4:Employees:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 4:Employees:
        CustomDefaultSGTACL-03
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group 4:Employees:
        CustomDefaultSGTACL-03
        Permit IP-00
```

IPv4 Role-based permissions from group Unknown to group 5:Contractors:

```
        SGACLtest-03


        Permit IP-00


IPv4 Role-based permissions from group 4:Employees to group 5:Contractors:


        CustomDefaultSGTACL-03


        Permit IP-00


IPv4 Role-based permissions from group 5:Contractors to group 5:Contractors:


        CustomDefaultSGTACL-03


        Permit IP-00


RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

- ACL在WLC上會視為「已下載」：

```
<#root>

#

show ip access-lists


Role-based IP access list CustomDefaultSGTACL-03 (downloaded)
    10 permit udp src eq bootps (12 matches)
    20 permit udp src eq bootpc
    30 permit ip
Extended IP access list IP-Adm-V4-Int-ACL-global
    10 permit tcp any any eq www
    20 permit tcp any any eq 443
Role-based IP access list Permit IP-00 (downloaded)
    10 permit ip
Role-based IP access list SGACLtest-03 (downloaded)
    10 permit udp src eq bootps (18 matches)
    20 permit udp src eq bootpc
    30 permit udp dst eq bootps
    40 permit udp dst eq bootpc
    50 permit ip
Role-based IP access list SGT32-06 (downloaded)
    10 permit ip
Extended IP access list implicit_deny
```

```
    10 deny ip any any
Extended IP access list implicit_permit
    10 permit ip any any
Extended IP access list meraki-fqdn-dns
Extended IP access list preauth_v4
    10 permit udp any any eq domain
    20 permit tcp any any eq domain
    30 permit udp any eq bootps any
    40 permit udp any any eq bootpc
    50 permit udp any eq bootpc any
    60 deny ip any any
```

FlexConnect本地交換

- 這是將使用者端連線到AP之前的WLC輸出：

<#root>

#

show cts ap sgt-info

```
Number of SGTs referred by the AP.............: 4

SGT               PolicyPushedToAP       No.of Clients
-------------------------------------------------------------
UNKNOWN(0)        NO                     0
2                 NO                     1
DEFAULT(65535)    YES                    0
```

- 在AP CLI中，這是將客戶端連線到AP之前的許可權輸出：

```
AP#show cts role-based permissions
IPv4 role-based permissions:
SGT DGT ACL
65535 65535 Permit_IP

IPv6 role-based permissions:
SGT DGT ACL
65535 65535 Permit_IP
```

- 以下是客戶端連線以顯示流時的AP調試：

<#root>

```
[*08/14/2025 09:45:40.8504] CLSM[74:DA:38:ED:13:B5]: US Auth(b0) seq 2599 IF 72 slot 0 vap 0 len 30 sta
[*08/14/2025 09:45:40.8507] CLSM[74:DA:38:ED:13:B5]: DS Auth len 30 slot 0 vap 0
[*08/14/2025 09:45:40.8509] CLSM[74:DA:38:ED:13:B5]: Driver send mgmt frame success Radio 0 Vap 0
[*08/14/2025 09:45:40.8509] CLSM[74:DA:38:ED:13:B5]: client moved from UNASSOC to AUTH
[*08/14/2025 09:45:40.8660] CLSM[74:DA:38:ED:13:B5]: US Assoc Req(0) seq 2600 IF 72 slot 0 vap 0 len 17
...
[*08/14/2025 09:45:40.8782] CLSM[74:DA:38:ED:13:B5]: client moved from ASSOC to 8021X
[*08/14/2025 09:45:40.8783] CLSM[74:DA:38:ED:13:B5]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*08/14/2025 09:45:40.8784] CLSM[74:DA:38:ED:13:B5]:
```

SGT Data sent: 74:DA:38:ED:13:B5 0 0

!--- The client initiates the connection and it's directly put under the SGT 0.

<#root>

```
[*08/14/2025 09:45:40.8800] CLSM[74:DA:38:ED:13:B5]: ADD_CENTRAL_AUTH_INFO_MOBILE Payload
[*08/14/2025 09:45:40.8801] CLSM[74:DA:38:ED:13:B5]: msAssocTypeFlags: 2 apfMsEntryType: 2 eap_type: 0
[*08/14/2025 09:45:40.8807] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility:
[*08/14/2025 09:45:40.8812] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[*08/14/2025 09:45:41.5130] CLSM[74:DA:38:ED:13:B5]: ADD_MOBILE AID 1
[*08/14/2025 09:45:41.5135] CLSM[74:DA:38:ED:13:B5]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*08/14/2025 09:45:41.5139] chatter: 74:DA:38:ED:13:B5: web_auth status 1
[*08/14/2025 09:45:41.5140] CLSM[74:DA:38:ED:13:B5]: client moved from 8021X to
```

IPLEARN_PENDING

!--- The client must get an IP address through DHCP.

<#root>

```
[*08/14/2025 09:45:41.5144] CLSM[74:DA:38:ED:13:B5]: ADD_CENTRAL_AUTH_INFO_MOBILE Payload
[*08/14/2025 09:45:41.5144] CLSM[74:DA:38:ED:13:B5]: msAssocTypeFlags: 2 apfMsEntryType: 2 eap_type: 25
[*08/14/2025 09:45:41.5150] CLSM[74:DA:38:ED:13:B5]: TLV_FLEX_CENTRAL_AUTH_STA_PAYLOAD
[*08/14/2025 09:45:41.5155] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility:
[*08/14/2025 09:45:41.5161] CLSM[74:DA:38:ED:13:B5]:
```

SGT Data sent: 74:DA:38:ED:13:B5 4 0

!--- Afterwards, the assigned SGT for that client is going to be applied accordingly.

<#root>

```
[*08/14/2025 09:45:41.5163] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[*08/14/2025 09:45:41.6476] chatter: find_insert_client:3313
[*08/14/2025 09:45:41.6476] chatter: Update IP from 0.0.0.0 to 10.14.42.103
```

[*08/14/2025 09:45:41.6477] chatter:

Update ipsgt: IPV4 client(74:DA:38:ED:13:B5) - [10.14.42.103]

!--- Associated IP & SGT is going to be added into mapping table.

<#root>

[*08/14/2025 09:45:41.6477] chatter: Update ipsgt IPV6 client(74:DA:38:ED:13:B5) - [fe80::edc6:5a93:ada
[*08/14/2025 09:45:41.6481] CLSM[74:DA:38:ED:13:B5]: Authorize succeeded to radio intf apr0v0
[*08/14/2025 09:45:41.6490] chatter: 74:DA:38:ED:13:B5: web_auth status 1
[*08/14/2025 09:45:41.6492] CLSM[74:DA:38:ED:13:B5]: client moved from IPLEARN_PENDING to

FWD

<#root>

!--- Then for the IP-SGT mapping entry in the mapping table, SGACL policy for those SGTs is requested.
!--- This is a snippet of the AP debugs showing one of the ACLs:

CLSM[74:DA:38:ED:13:B5]: SGT Data sent: 74:DA:38:ED:13:B5 4 0
CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 165 len 148
....TLV: TLV_CTS_RBACL_DELETE(1434), level: 0, seq: 0, nested: true
....TLV: TLV_CTS_RBACL_DELETE(1437), level: 1, seq: 0, nested: false
TLV_CTS_RBACL_DELETE received
ACL Name:CustomDefaultSGTACL
....TLV: TLV_CTS_RBACL_ADD(1433), level: 0, seq: 0, nested: true
....TLV: TLV_CTS_RBACL_ADD(1437), level: 1, seq: 0, nested: false
....TLV: TLV_CTS_RBACL_ADD(1438), level: 1, seq: 1, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 2, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 3, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 4, nested: false
TLV_CTS_RBACL_ADD received

ACL Name:CustomDefaultSGTACL

ACL Type:1

ACE entry:permit udp src eq bootps

ACE entry:permit udp src eq bootpc

ACE entry:permit ip

```
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
…
```

- 在WLC CLI上，在SGT 4上連線一台客戶端時：

<#root>

#

show cts ap sgt-info

```
Number of SGTs referred by the AP.............: 4

SGT                PolicyPushedToAP       No.of Clients
-------------------------------------------------------------
UNKNOWN(0)         NO                     0
2                  NO                     1
4                  YES                    1
DEFAULT(65535)     YES                    0
```

- 在AP CLI上：
  您可以看到相同的情況，僅新增了與SGT 4相關的許可權。

```
AP#show cts role-based permissions
IPv4 role-based permissions:
SGT DGT ACL
0 4 Permit_IP, CustomDefaultSGTACL
4 4 Permit_IP, CustomDefaultSGTACL
5 4 Permit_IP, CustomDefaultSGTACL
65535 65535 Permit_IP

IPv6 role-based permissions:
SGT DGT ACL
0 4 Permit_IP
4 4 Permit_IP
5 4 Permit_IP
65535 65535 Permit_IP
```

- 在WLC CLI上，連線SGT 5上的第二個客戶端時：

<#root>

#

show cts ap sgt-info

```
Number of SGTs referred by the AP.............: 5

SGT               PolicyPushedToAP       No.of Clients
-----------------------------------------------------------
UNKNOWN(0)        NO                     0
2                 NO                     1
4                 YES                    1
5                 YES                    1
DEFAULT(65535)    YES                    0
```

- AP輸出：

<#root>

AP#

show flexconnect client

```
Flexconnect Clients:
              mac radio vap aid state       encr aaa-vlan aaa-acl aaa-ipv6-acl assoc    auth switching
```

SGT

```
74:DA:38:EB:C0:1F     0   0   1   FWD AES_CCM128     none    none         none Local Central     Local
```

5

```
74:DA:38:ED:13:B5     0   0   2   FWD AES_CCM128     none    none         none Local Central     Local
```

4

<#root>

AP#

show cts role-based sgt-map all

```
Active IPv4-SGT Bindings Information
          IP SGT SOURCE
10.14.42.103   4  LOCAL
10.14.42.104   5  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2

Active IPv6-SGT Bindings Information
                       IP SGT SOURCE
 fe80::ac0b:d679:e356:a17   5  LOCAL
fe80::edc6:5a93:adab:fff6   4  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

<#root>

AP#

show cts role-based permissions

```
IPv4 role-based permissions:
  SGT   DGT                              ACL
    0     4 Permit_IP, CustomDefaultSGTACL
    4     4 Permit_IP, CustomDefaultSGTACL
    5     4 Permit_IP, CustomDefaultSGTACL
    0     5           Permit_IP, SGACLtest
    4     5 Permit_IP, CustomDefaultSGTACL
    5     5 Permit_IP, CustomDefaultSGTACL
65535 65535 Permit_IP, CustomDefaultSGTACL

IPv6 role-based permissions:
  SGT   DGT       ACL
    0     4 Permit_IP
    4     4 Permit_IP
    5     4 Permit_IP
    0     5 Permit_IP
    4     5 Permit_IP
    5     5 Permit_IP
65535 65535 Permit_IP
```

<#root>

AP#

show cts access-lists

```
IPv4 role-based ACL:
SGACLtest
        rule 0: allow true && ip proto 17 && ( src port 67 )
        rule 1: allow true && ip proto 17 && ( src port 68 )
```

```
        rule 2: allow true && ip proto 17 && ( dst port 67 )
        rule 3: allow true && ip proto 17 && ( dst port 68 )
        rule 4: allow true
CustomDefaultSGTACL
        rule 0: allow true && ip proto 17 && ( src port 67 )
        rule 1: allow true && ip proto 17 && ( src port 68 )
        rule 2: allow true
Permit_IP
        rule 0: allow true

IPv6 role-based ACL:
Permit_IP
        rule 0: allow true
```

<#root>

AP#

show cts role-based sgt-map summary

```
        -IPv4-
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2

        -IPv6-
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

疑難排解

- 在WLC CLI上：

show cts provisioning

顯示cts基於角色的許可權

show ip access-lists

show cts ap sgt-info <ap_name>

- 在AP上：

show cts role-based sgt-map all

顯示cts基於角色的許可權

show cts access-lists <acl-name>

show cts role-based sgt-map summary

show cts access-lists

show flexconnect client

clear cts role-based counters

show cts role-based counters

- AP調試：

- 啟用CTS資料包級別實施調試：

debug cts enforcement

術語mon

- 檢查CAPWAP ACL事件和負載相關資訊：

debug dot11 client access-list <client-mac-addr>

debug capwap client acl

debug capwap client payload

debug capwap client error

debug dot11 client management information

debug dot11 client management critical

debug dot11 client management error

debug dot11 client management events

debug generic datapath client_ip_table/debug_acl

debug generic datapath client_ip_table/debug

debug generic datapath sgacl/debug

debug generic datapath sgacl/debug_sgt

debug generic datapath sgacl/debug_protocol

debug generic datapath sgacl/debug_permission

術語mon

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）。