Configure and Verify SGACL on Catalyst 9800 WLC and ISE Server

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Network Diagram
- Configurations
  - WLC Configuration
  - ISE Configuration
  - Flexconnect

Verify

- FlexConnect Local Switching

Troubleshoot

Introduction

This document describes how to configure TrustSec on Catalyst 9800 and ISE server to utilize SGACL feature, with local and FlexConnect mode APs.

Prerequisites

Requirements

Knowledge of Cisco 9800 WLC, Cisco ISE, FlexConnect and TrustSec fundamentals.

Components Used

The information in this document is based on these software and hardware versions:

- C9800-CL v17.12.4
- ISE 3.2.0
- 9136I Access Point

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram

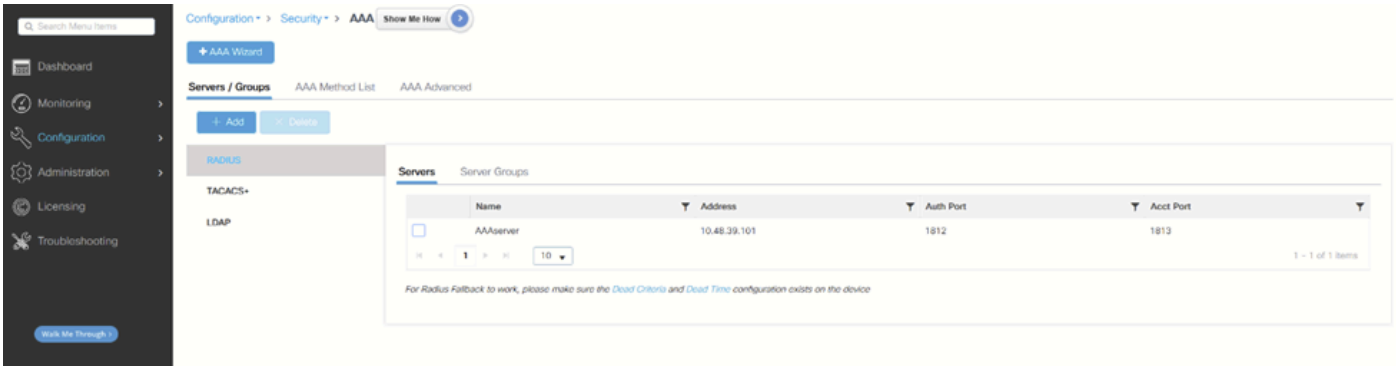


Network Diagram

Configurations

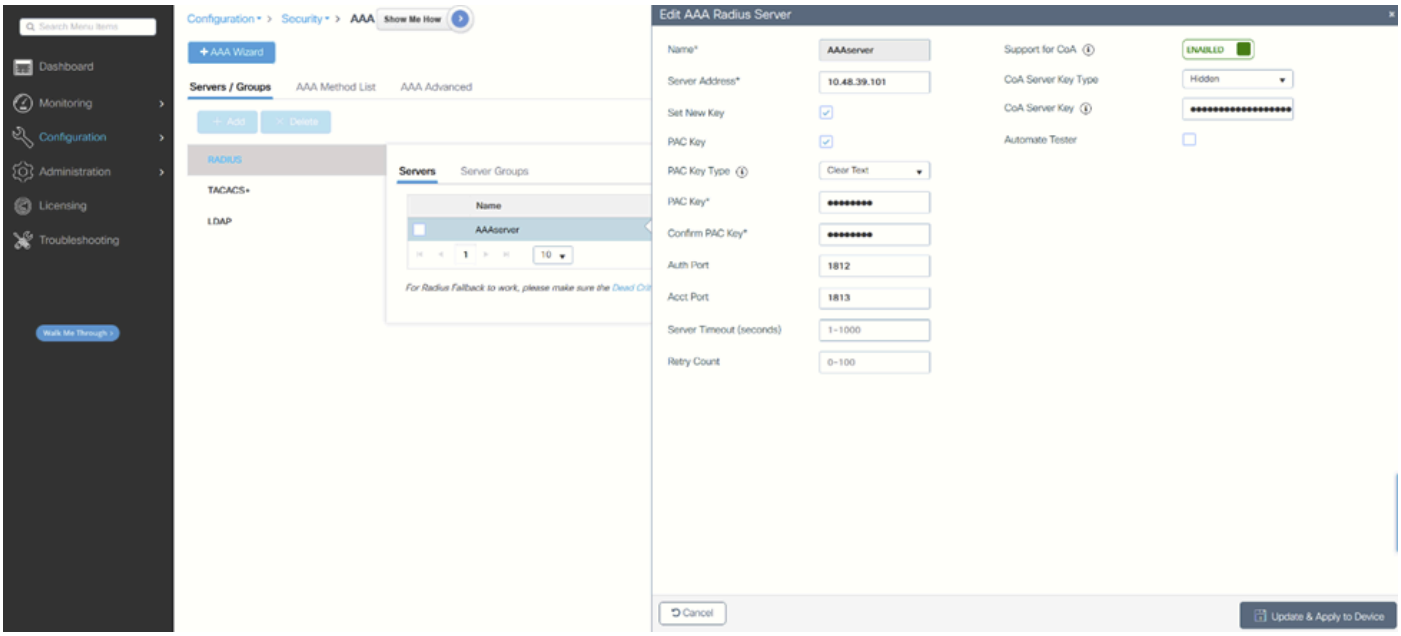
WLC Configuration

1. Add the AAA server to the WLC from **Configuration > Security > AAA**:



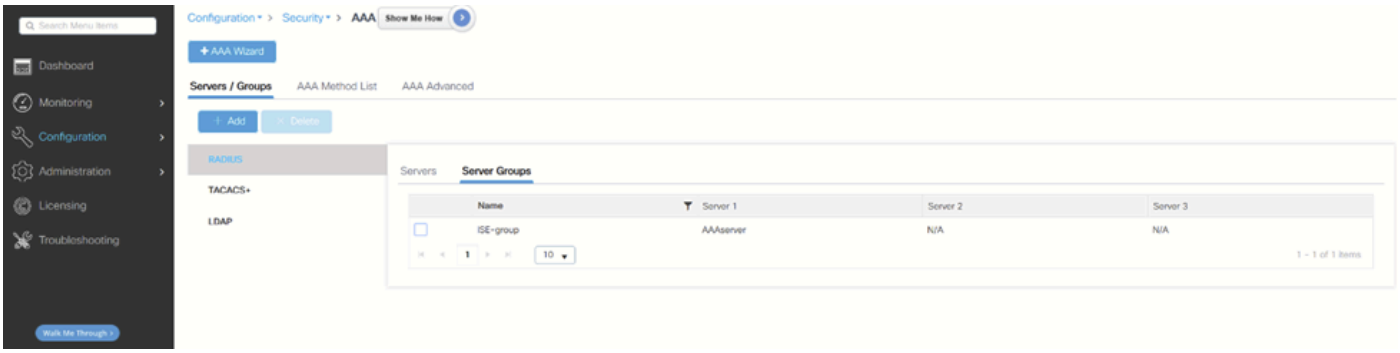
WLC AAA page

2. Make sure the key entries here are matching the key when you add the device on ISE. Enable **Support for CoA** and add the key if you would like to use CoA for downloading the configuration updates:



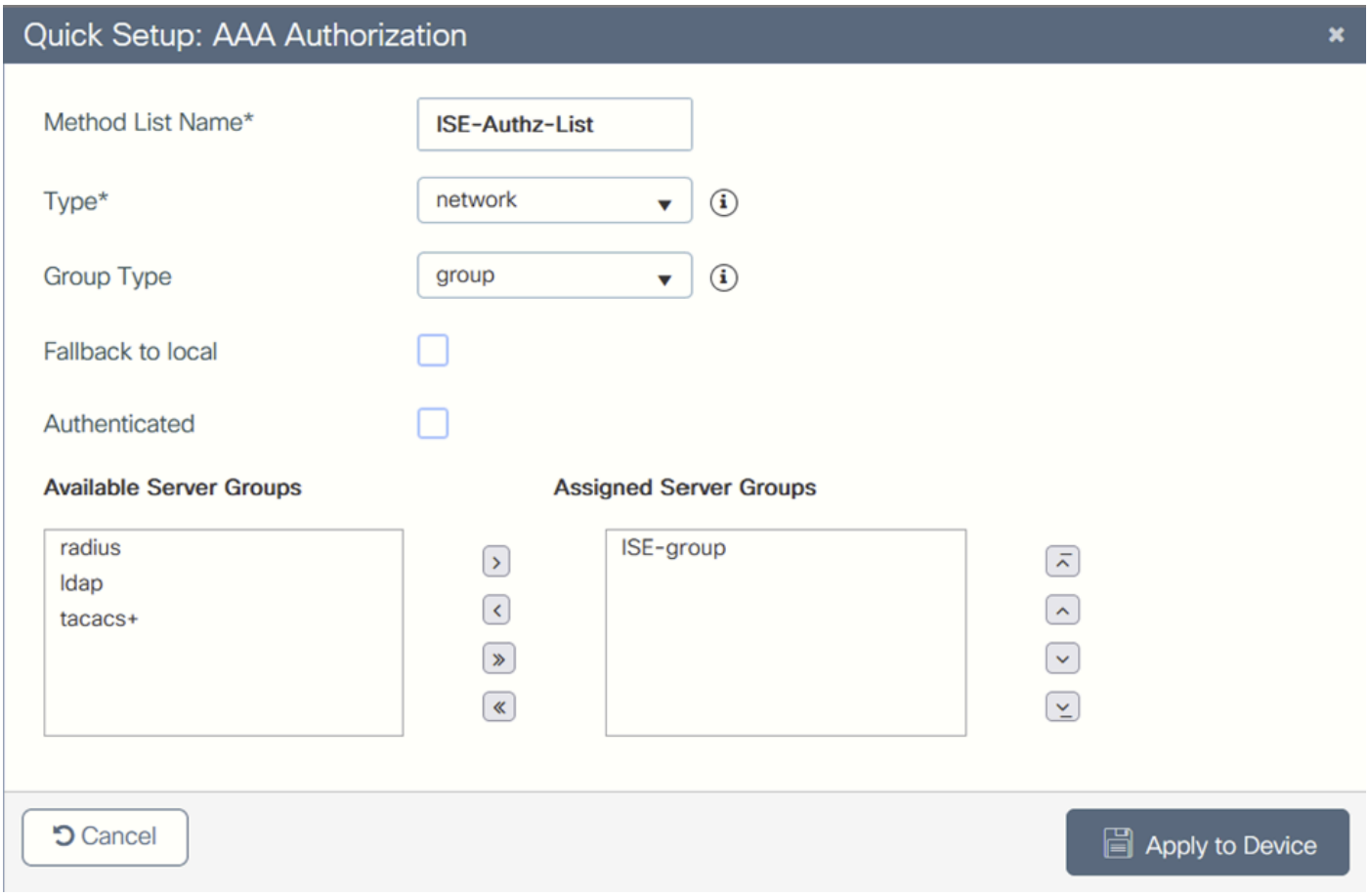
WLC add AAA server

3. Create the Server Group:

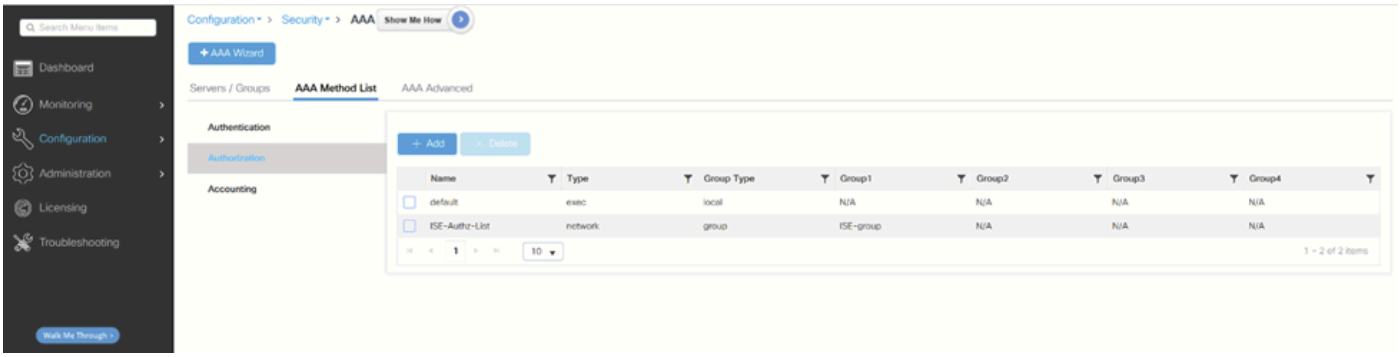


WLC add Server Group

4. Add the **Authorization Method List** with type **network**:



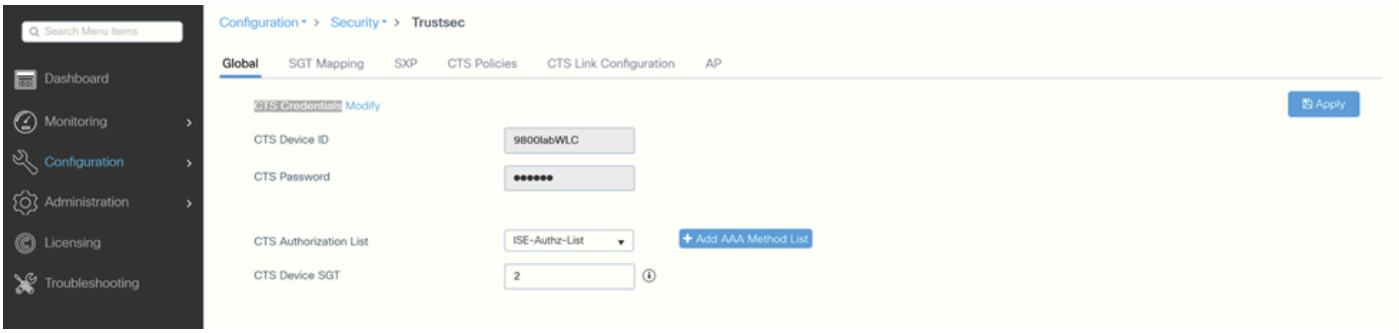
Authorization Method List



WLC AAA server group

5. Navigate to **Configuration > Security > Trustsec** and configure the **CTS Device ID** and **CTS Password**, you are going to use these entries when adding the device on ISE.

Configure the CTS Authorization List you created in steps 4 here as well:

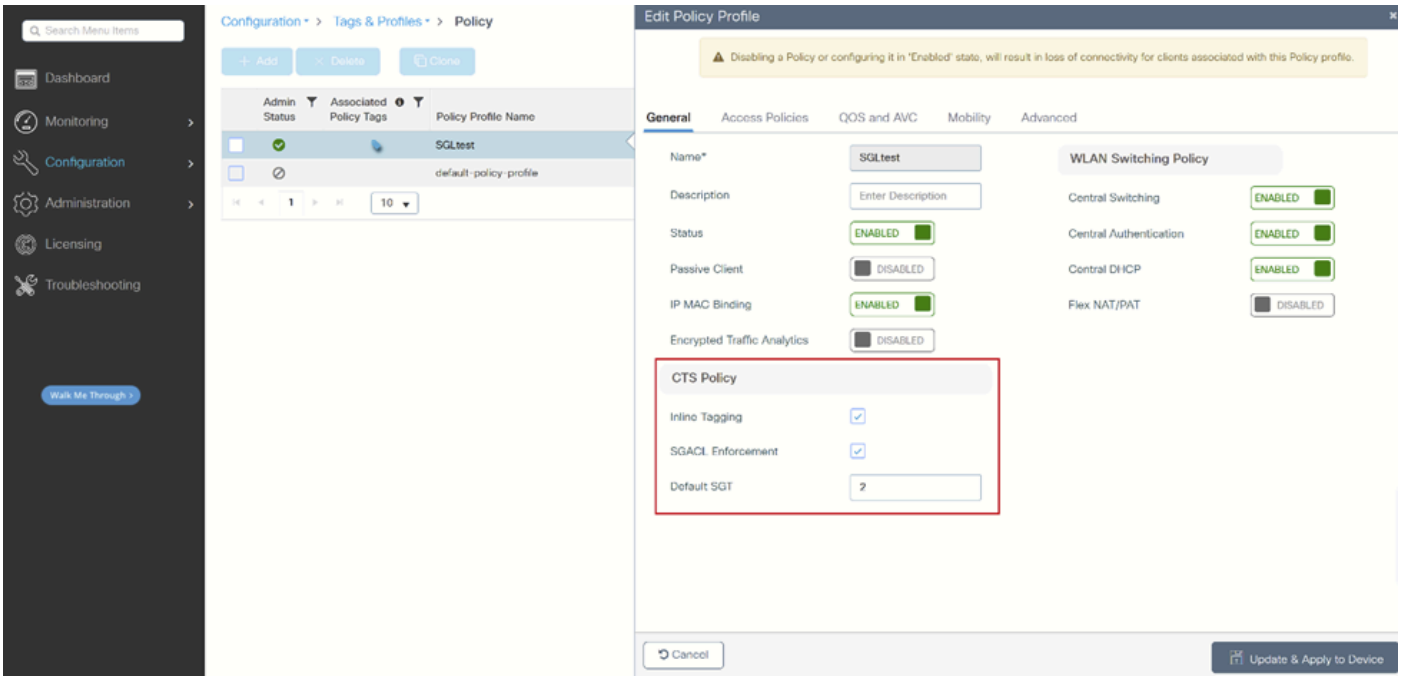


WLC TrustSec

6. In this example, the WLAN is already created and the authentication settings are already configured.

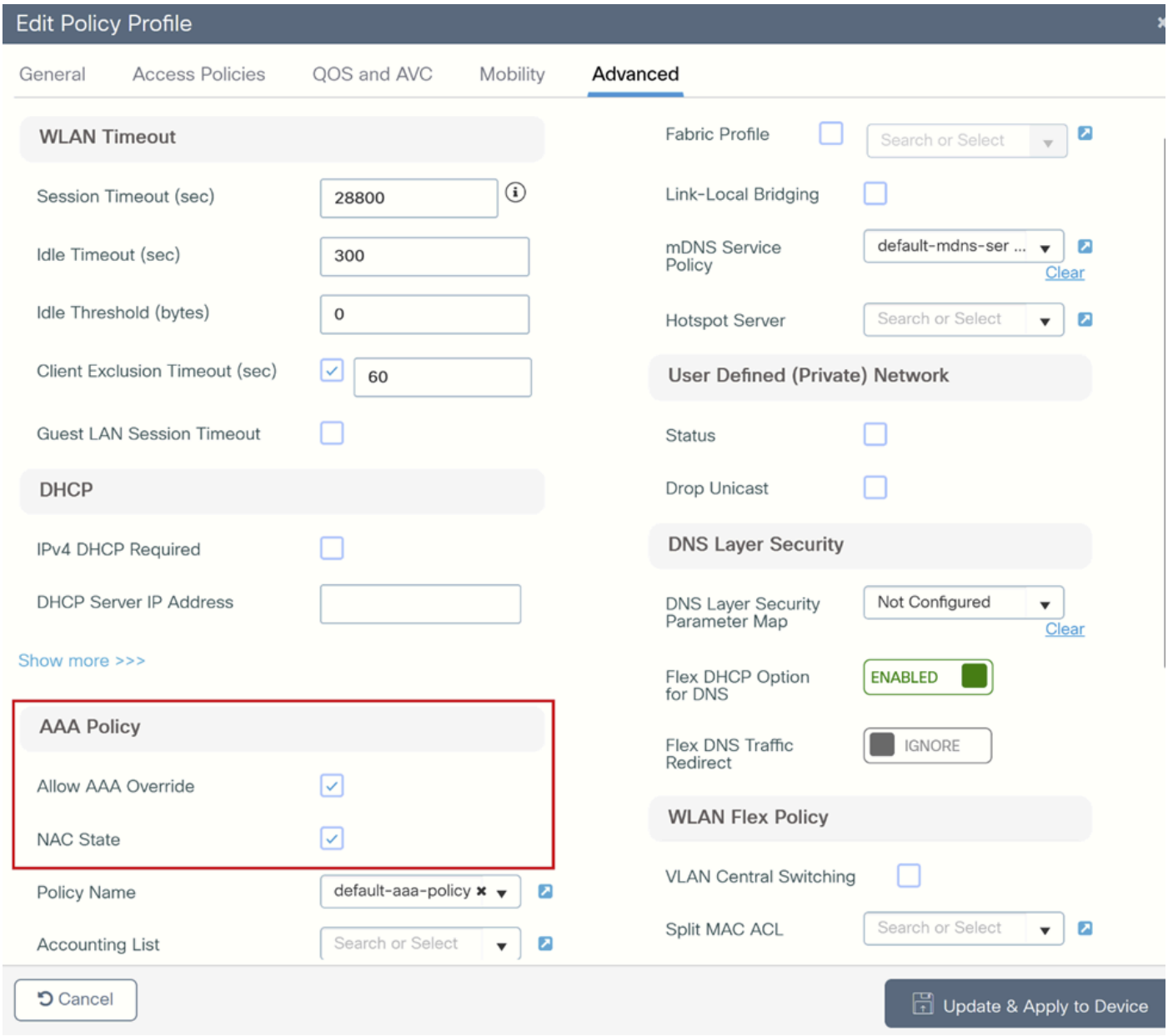
Now, navigate to the Policy Profile you would like to use SGTs on.

i. Under **CTS Policy**, enable **Inline Tagging** and **SGACL Enforcement**, you can specify the **Default SGT** as well. Default SGT 2 is used for this lab as an example:



WLC Policy Profile

ii. Under the **Advanced** tab, enable **Allow AAA override** and **NAC state**:



WLC Policy Profile Advanced tab

From the CLI:

```
# 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>

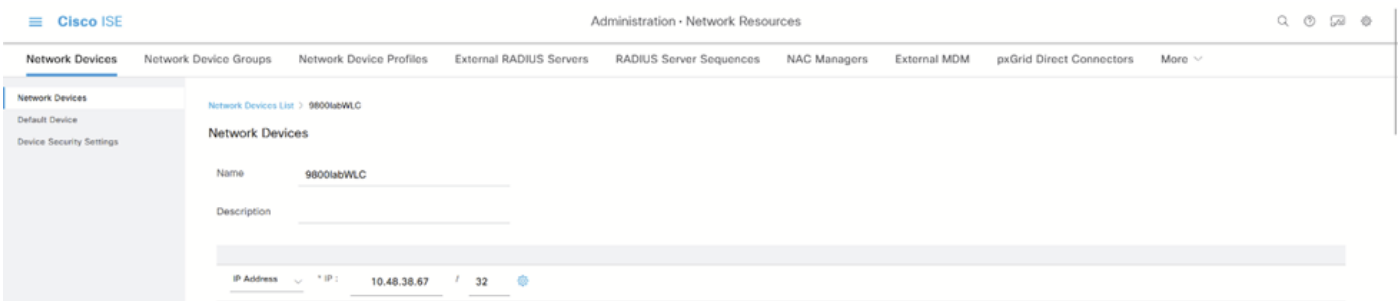
(config)# wireless profile policy <policy_profile_name>
(config-wireless-policy)# shut
(config-wireless-policy)# aaa-override
(config-wireless-policy)# cts inline-tagging
(config-wireless-policy)# cts role-based enforcement
(config-wireless-policy)# cts sgt <number>
(config-wireless-policy)# no shut

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

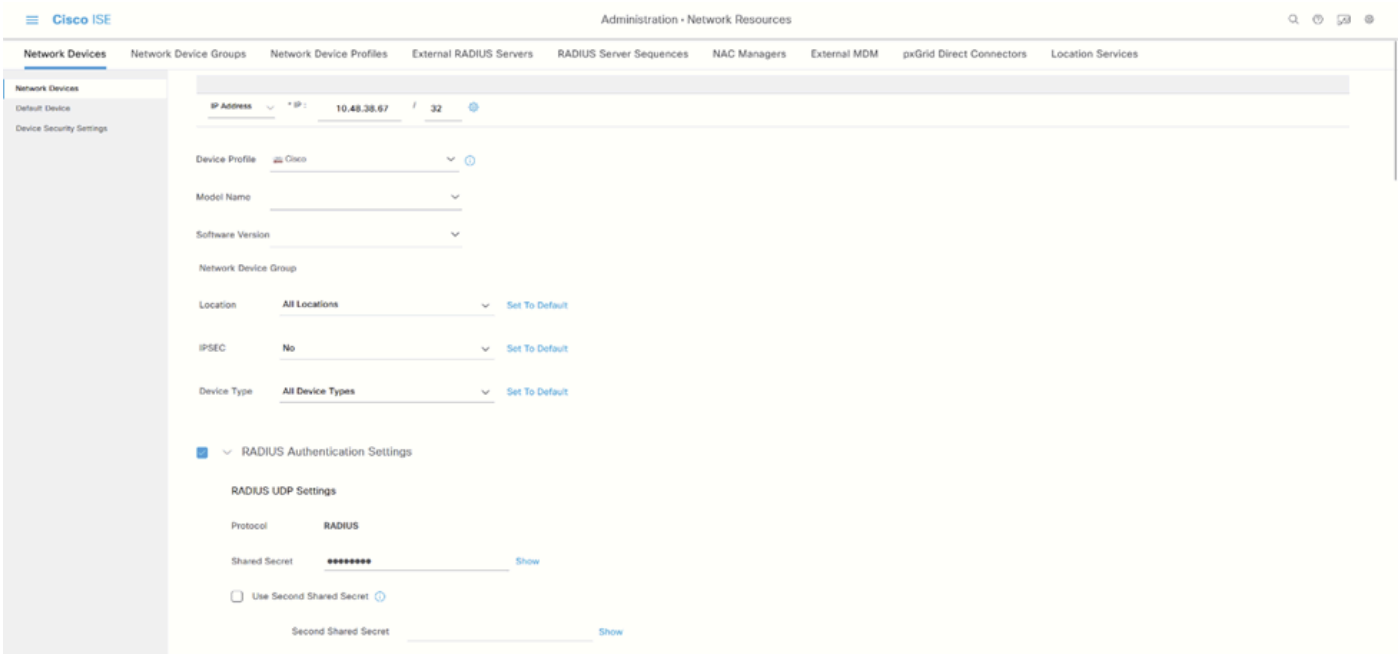
ISE Configuration

1. Navigate to **Administration > Network Resources > Network Devices**.

i. Add the WLC information here:

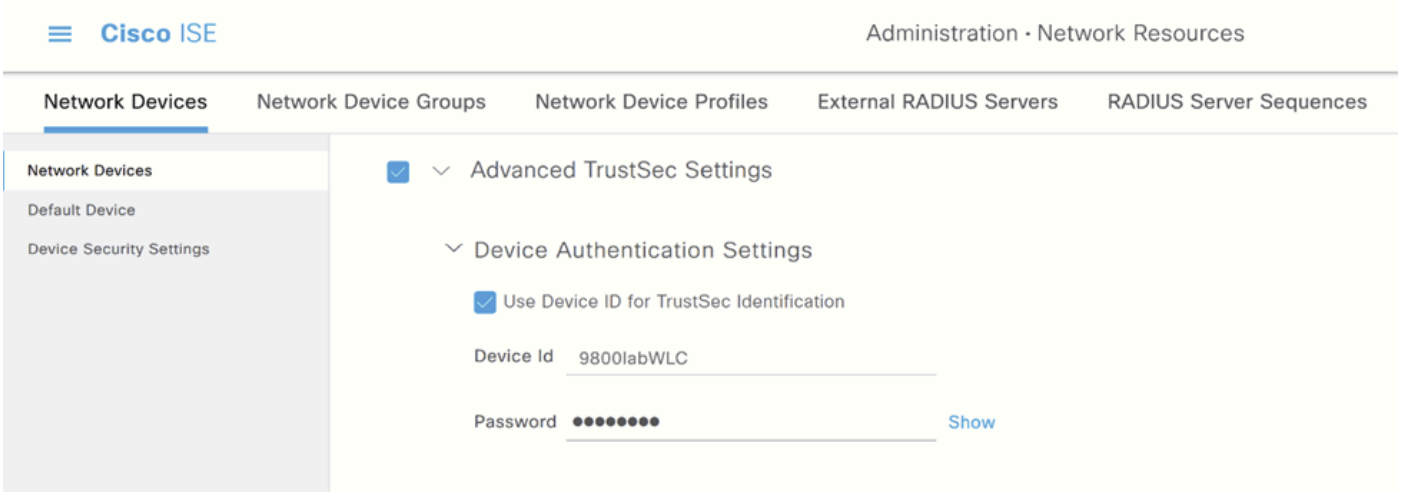


ISE Network Devices page



ISE add WLC RADIUS info

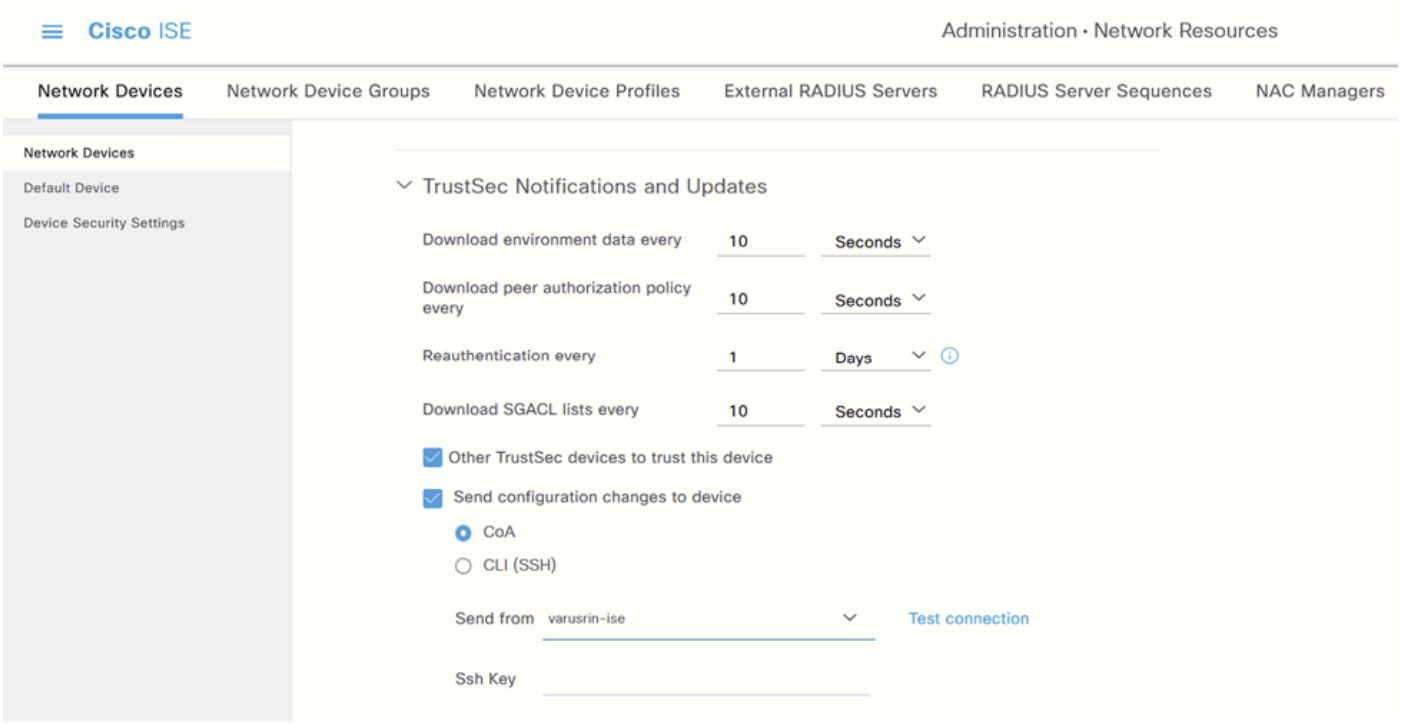
ii. Scroll down and configure **Advanced TrustSec Settings**, enable the checkbox **Use Device ID for TrustSec Identification** and configure the password:



Advanced TrustSec Settings

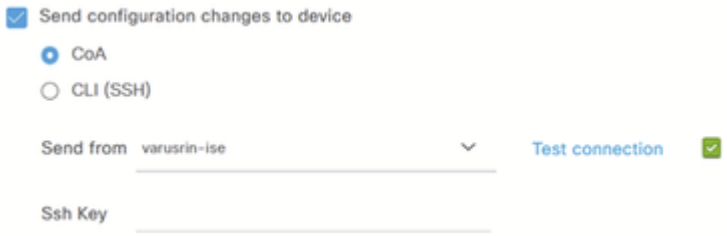
This must match the configuration on the WLC side in step 6 of WLC configuration.

iii. Scroll down to **TrustSec Notifications and Updates** and configure whether you would like to use CoA or SSH for configuration updates. Select the ISE node needed:



TrustSec Notifications and Updates

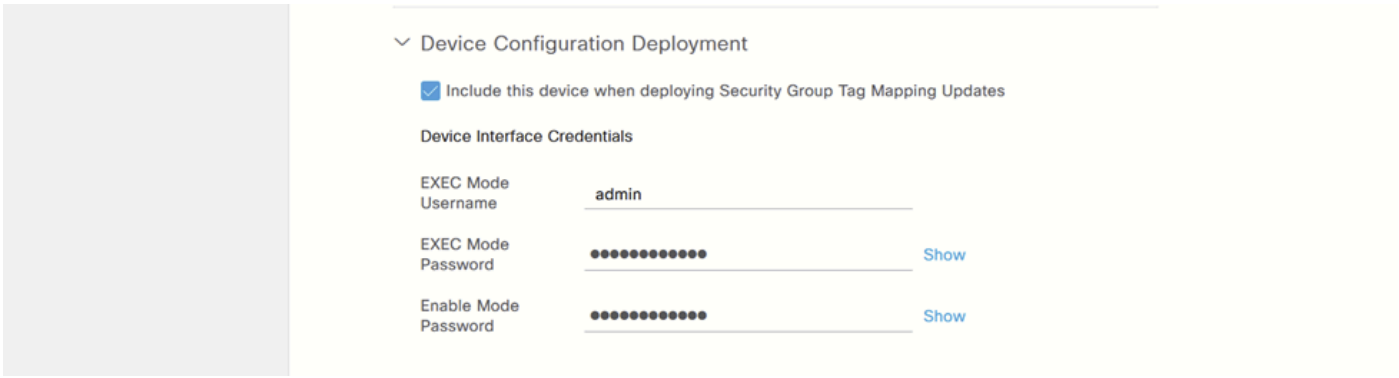
2. Press on **Test connection** to make sure the connection is established. When it is successful, it is going to show a green tick:



Test connection

i. Scroll down and configure the WLC to be included when deploying SGT mapping updates, this is

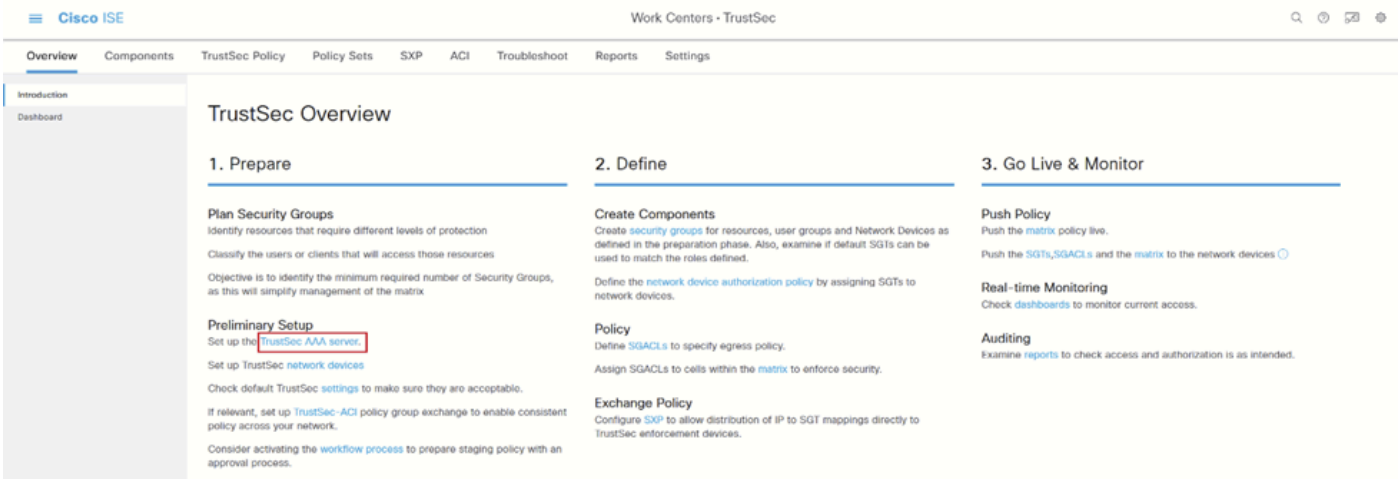
important if you select the SSH option in the previous step:



Device Configuration Deployment

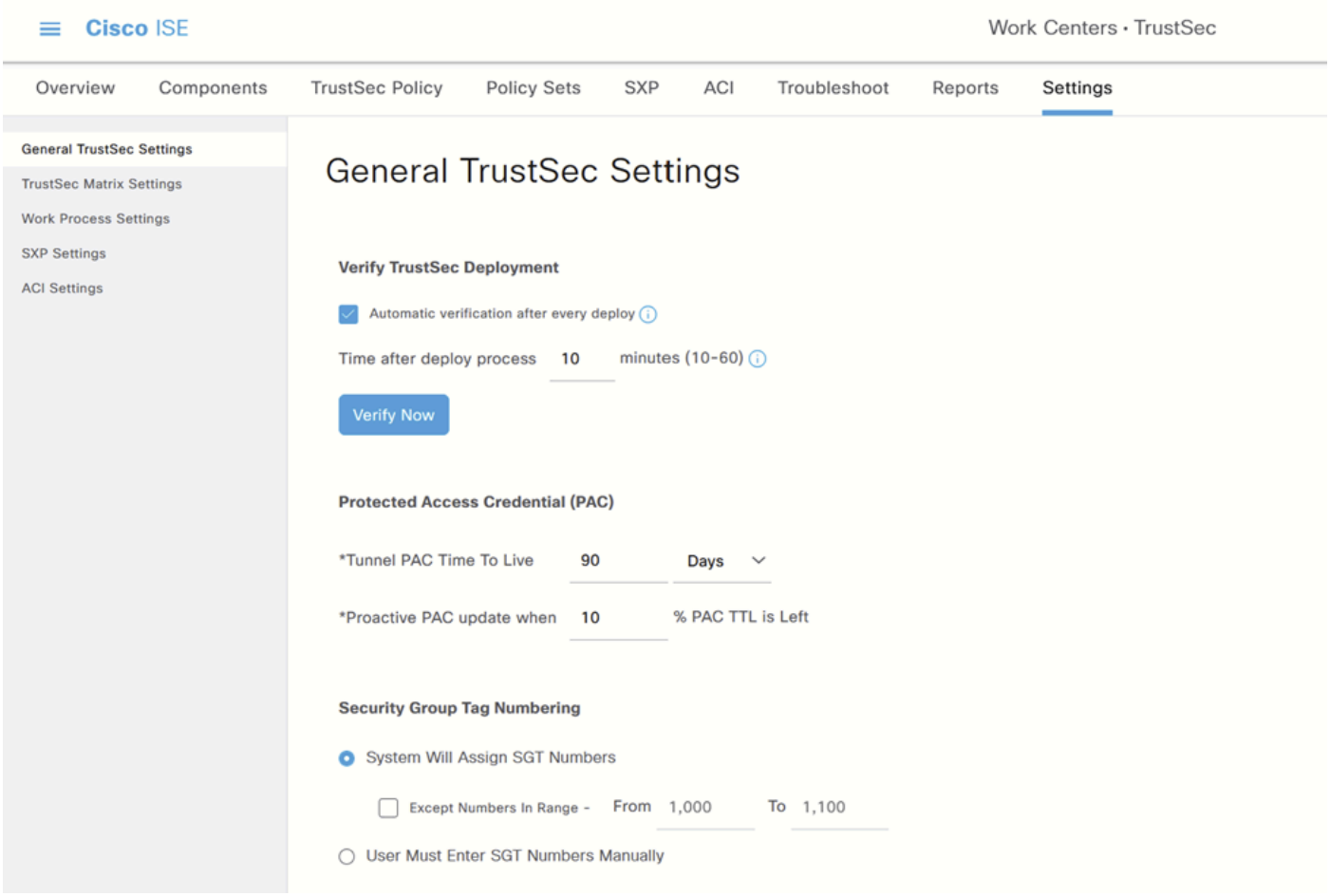
ii. Save the configuration.

3. From Work **Centers > TrustSec > Overview**, you have the TrustSec configuration options. Choose **TrustSec AAA Server** to view the ISE instance in use. Refer to the [Cisco Catalyst Wireless Group Based Policy] for more information on which instance is used if you have multiples.



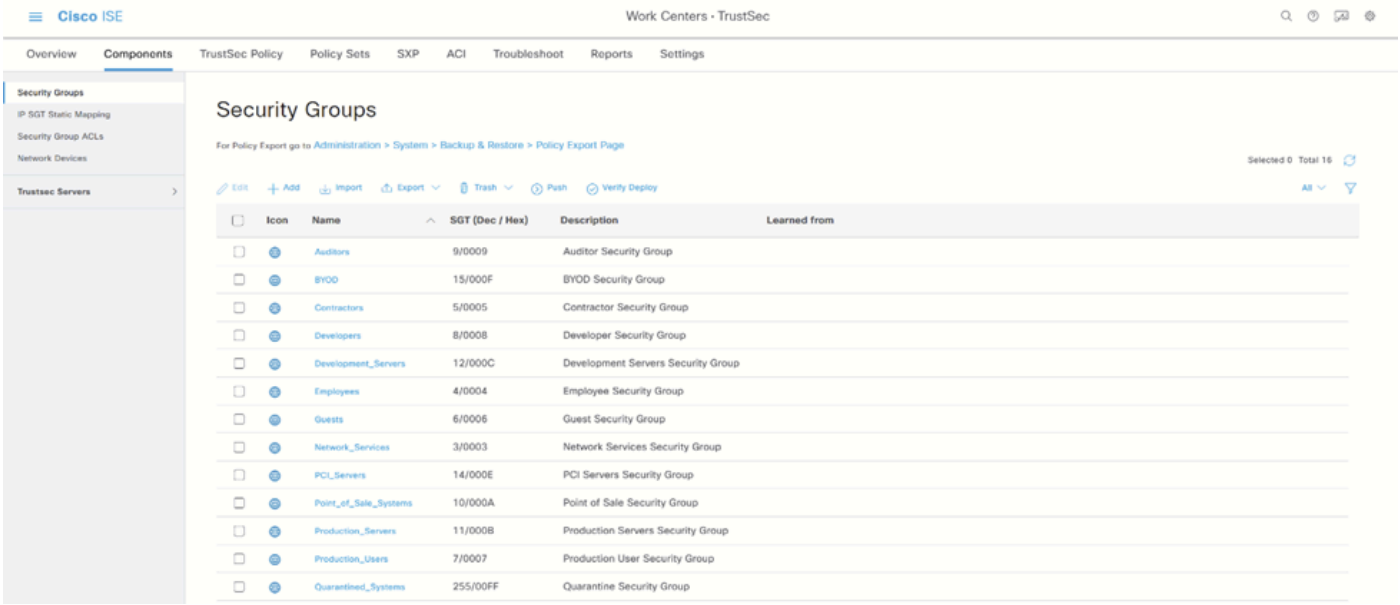
ISE TrustSec Overview

4. (Optional) Navigate to **Settings** tab, enable **Automatic verification after every deploy** if preferable.

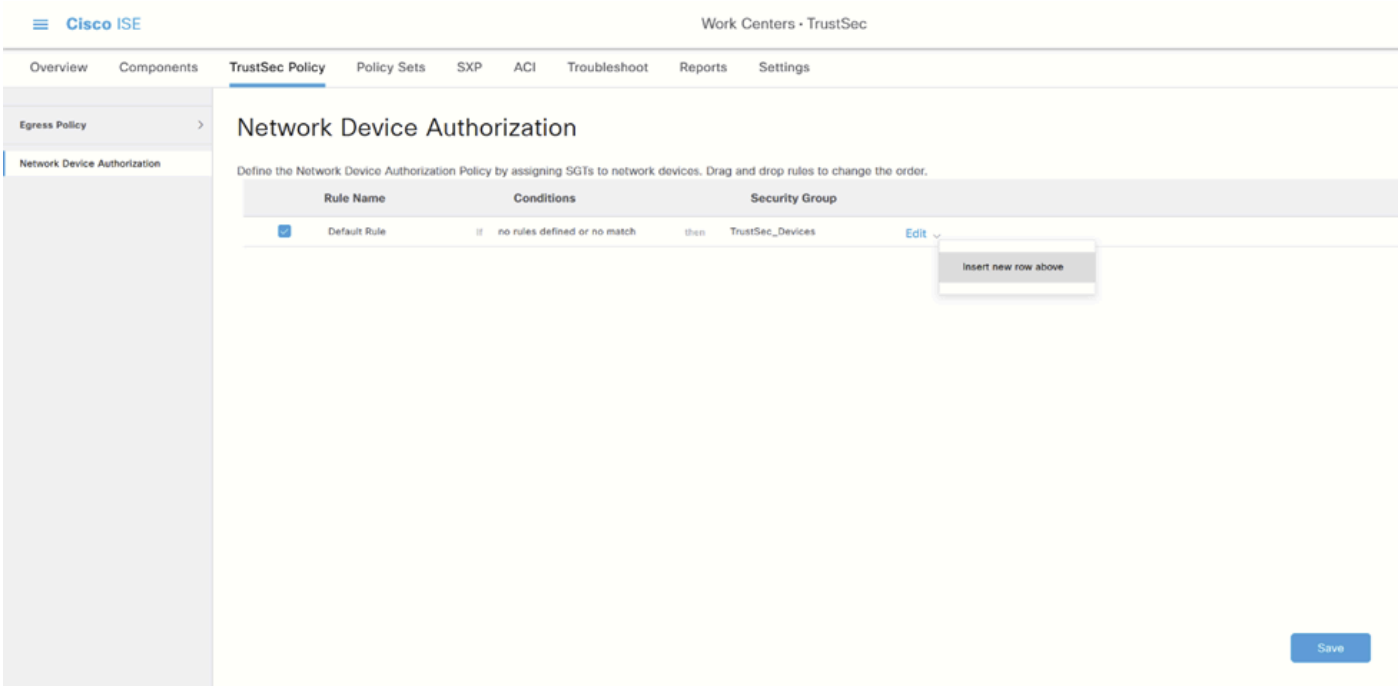


ISE TrustSec Settings

5. Add or edit the SGT values from **Work Centers > TrustSec > Components > Security Groups** depending on your requirements:

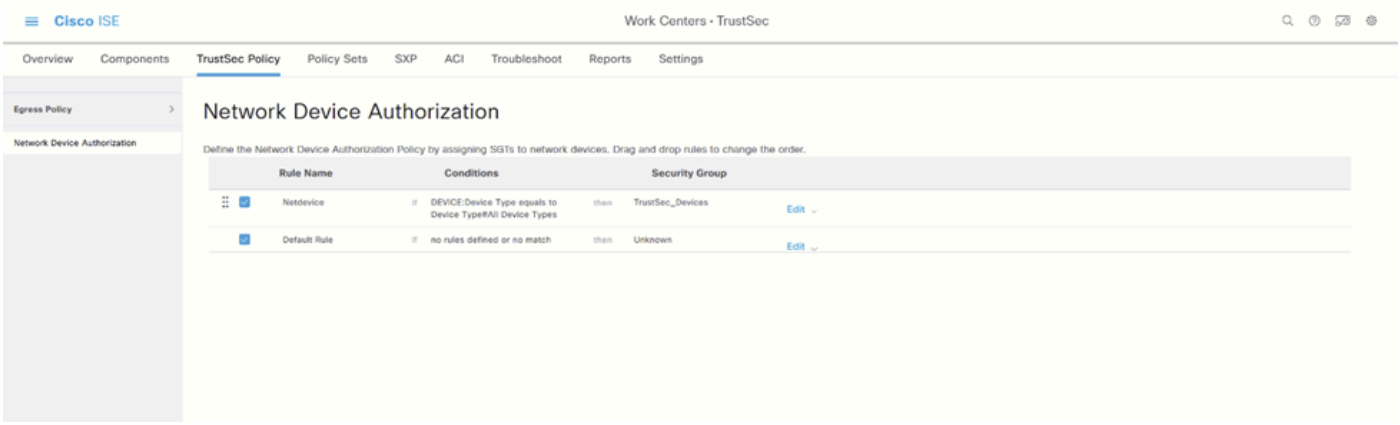


6. If you would like to specify the authorization policy, navigate to **Work Centers > TrustSec > TrustSec Policy > Network Device Authorization**:



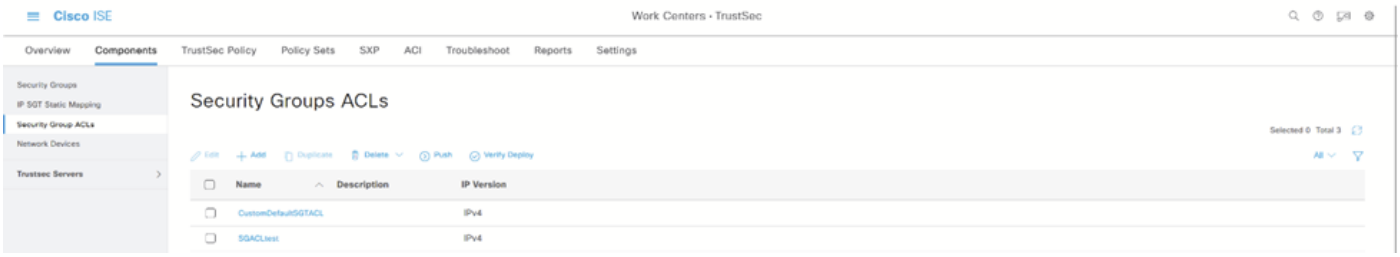
TrustSec Policy

You can keep the default, but for this lab we are using this configuration as an example:



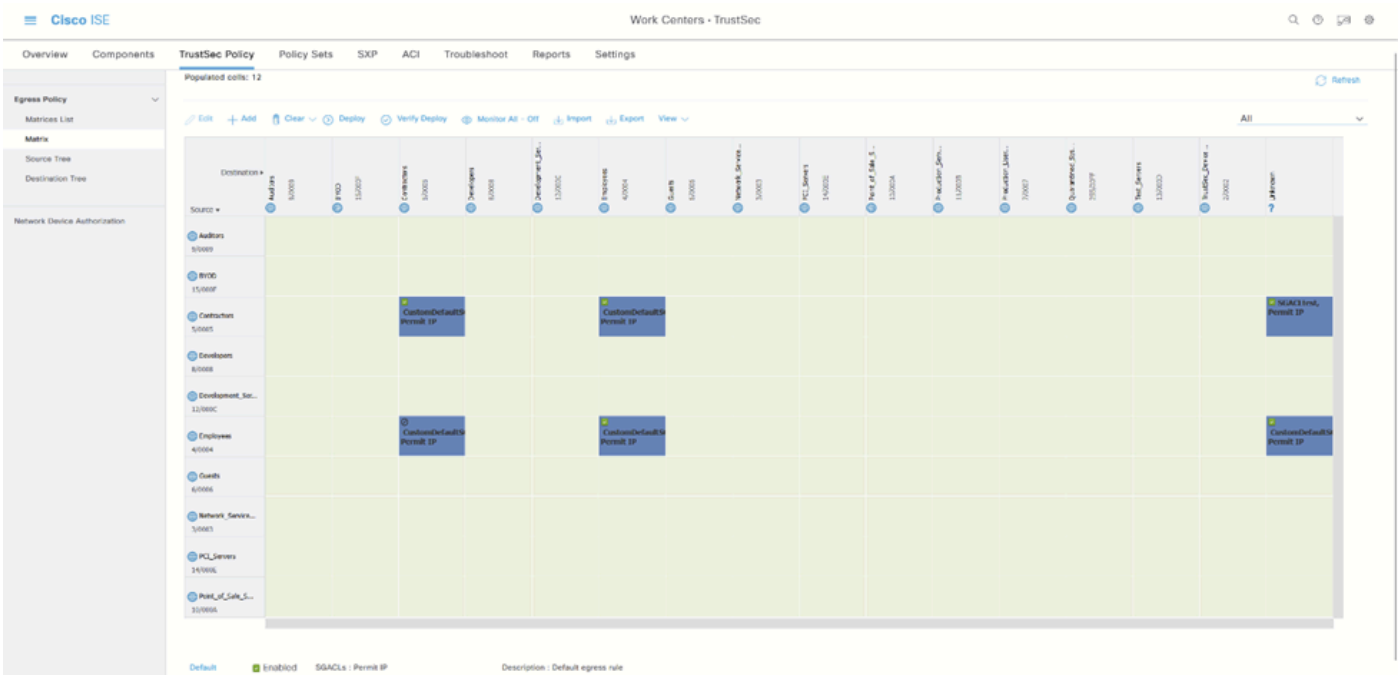
Network Device Authorization

7. Create the SGACL under **Components** tab then **Security Group ACLs**:



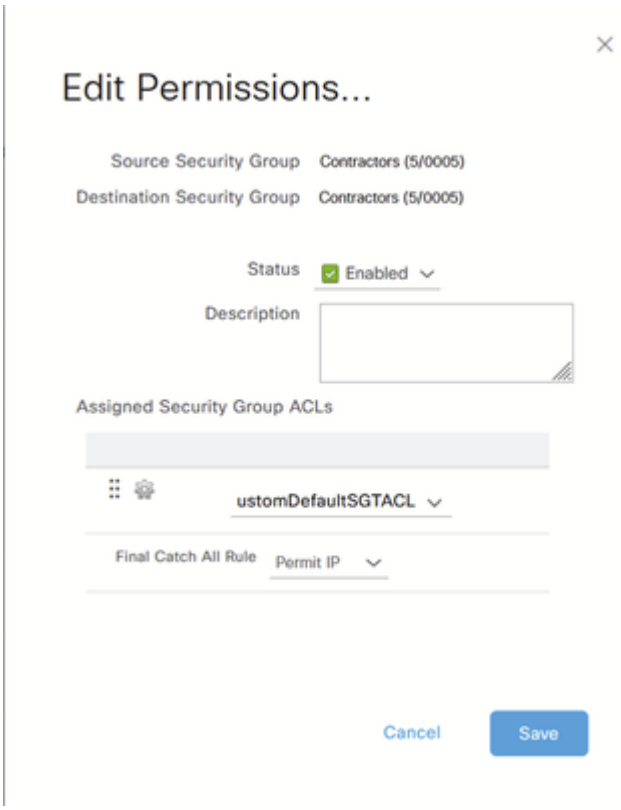
Security Group ACLs

8. Specify the matrix entries under **TrustSec Policy** tab then **Matrix**. You can edit the Permissions by clicking on the point which two SGTs meet:



ISE TrustSec Matrix

For example:



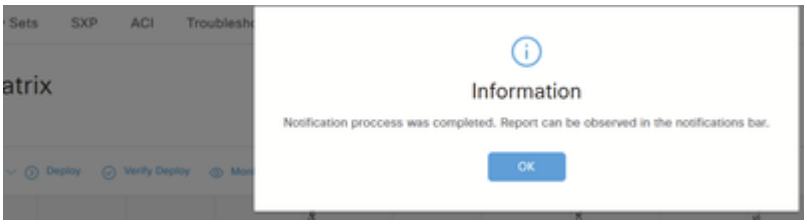
Edit Permissions

Note: In case of Allow List model, you need to explicitly allow DHCP protocol for the client devices to get the DHCP IP address and then request the controller for SGACL policies.

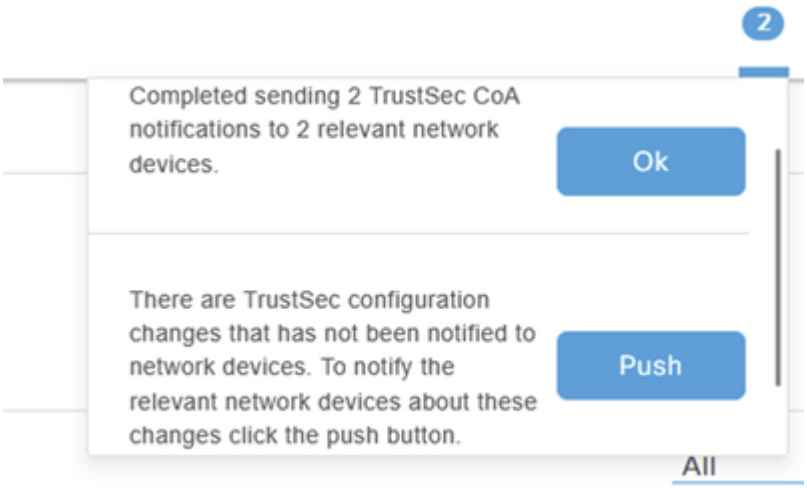
Note: Clients receive zero SGT value and DHCP clients receive an Automatic Private IP Addressing (APIPA) address when TrustSec policy “unknown to unknown” is denied in TrustSec matrix.
Clients receive correct SGT values and DHCP clients receive an IP address when TrustSec policy “unknown to unknown” is permitted in TrustSec matrix.

---

9. Click on **Deploy**. Which is going to result in these message and notifications:



Deploy



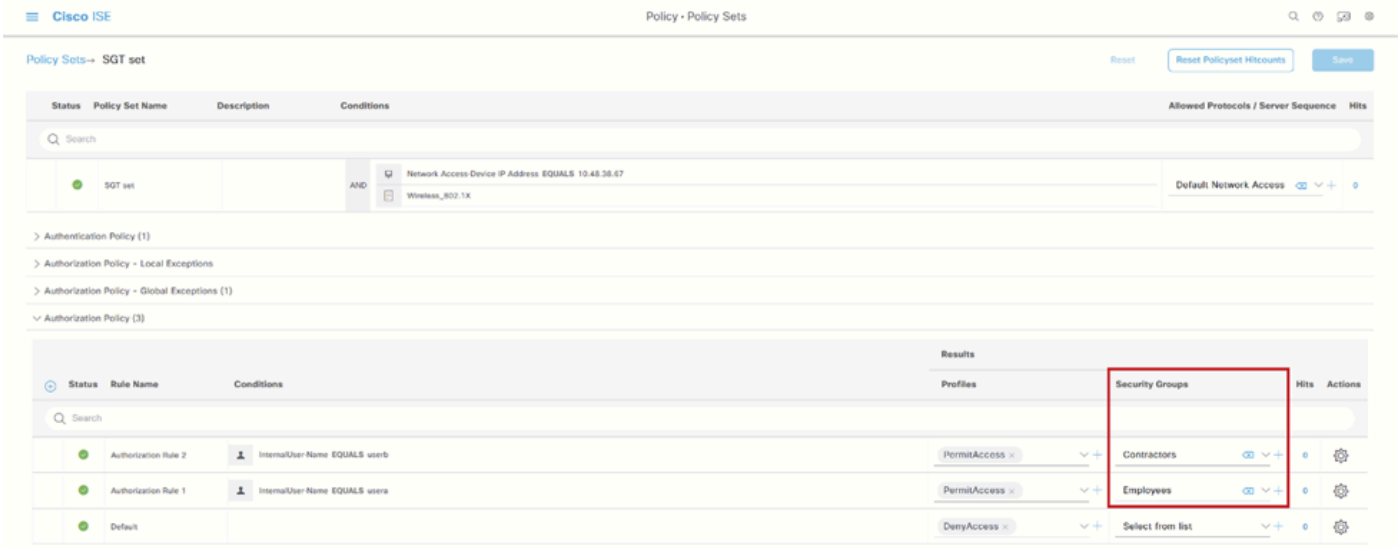
Deploy notifications

10. Navigate to the **Policy Set** used for the WLAN under **Policy > Policy Sets**:



ISE Policy Sets

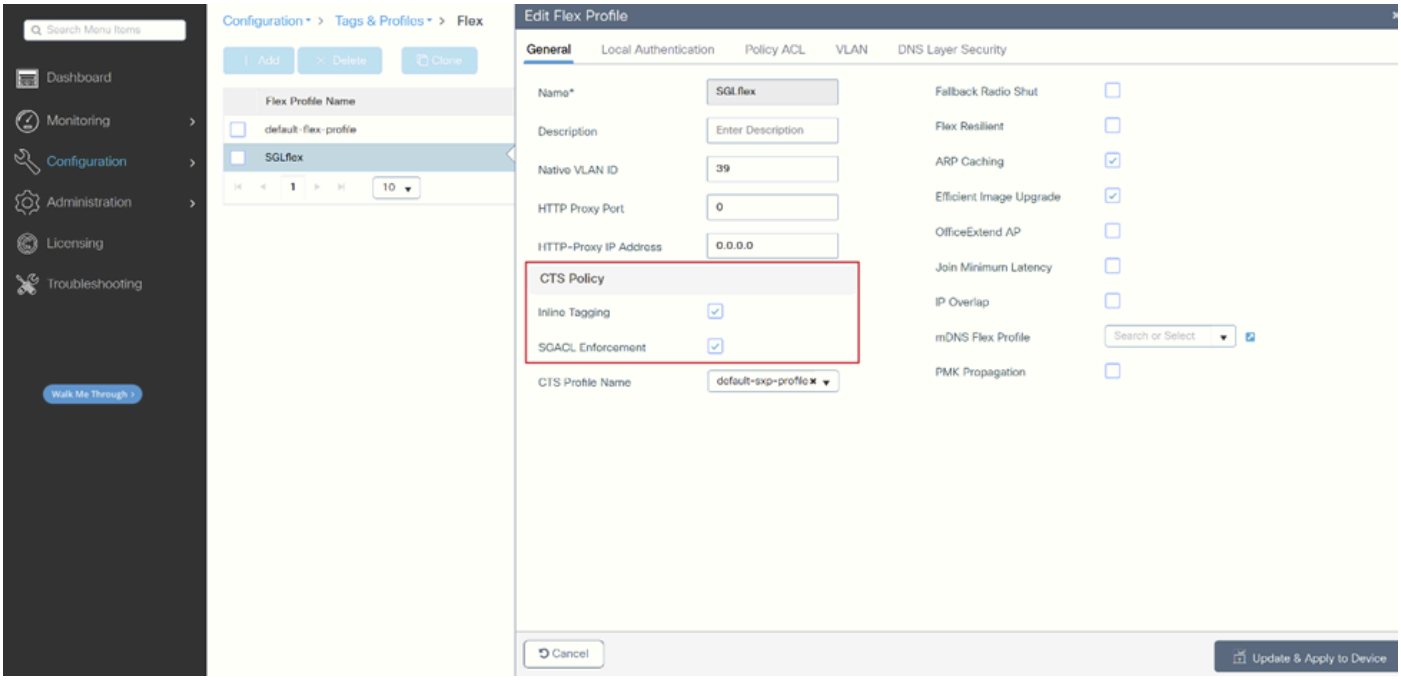
In this lab, we are defining the SGT per user, select the SGT under **Security Groups** field:



ISE Security Groups

Flexconnect

Enable **Inline Tagging** and **SGACL Enforcement** on the **Flex Profile** under **Configuration > Tags & Policies > Flex**:



WLC Flex Profile

From the CLI:

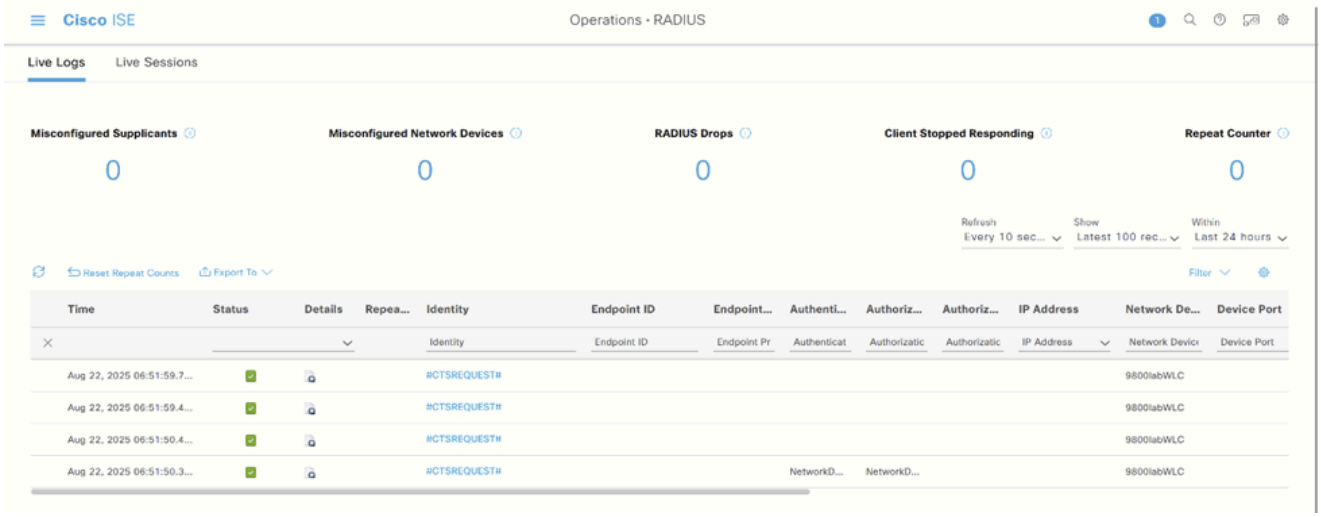
```
# configure terminal

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

Note: Trustsec policy HA support for FlexConnect mode APs starts on 17.18.2.

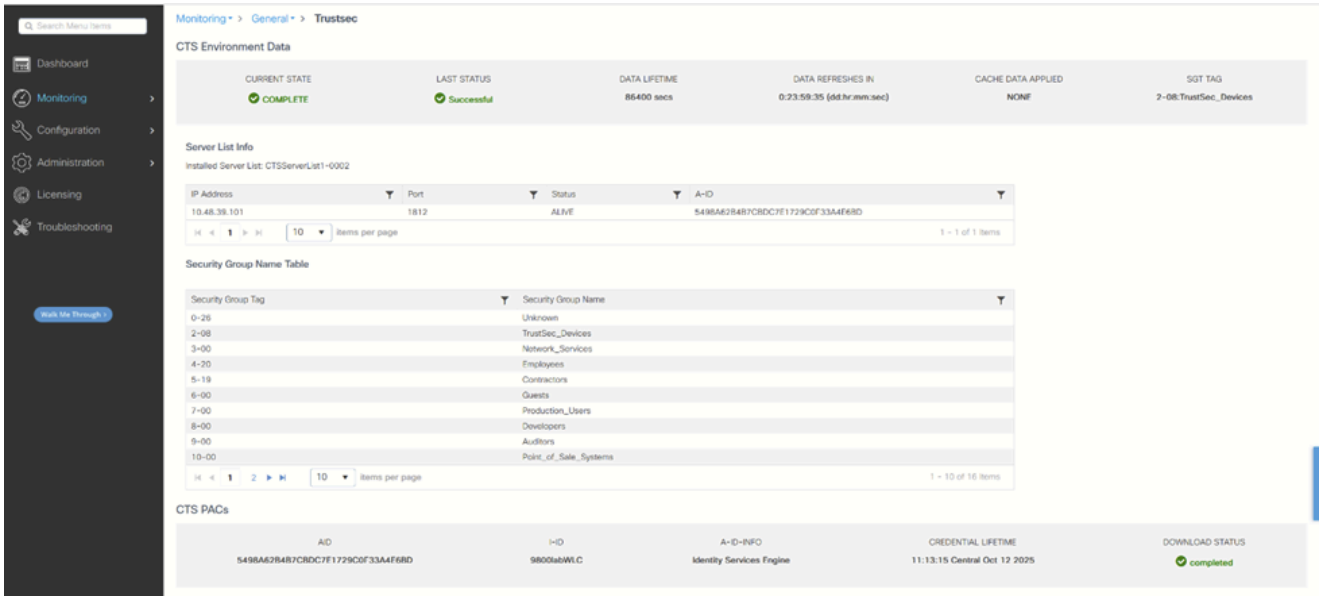
Verify

1. From ISE, you must see successful CTS request under **Operations > RADIUS > Live Logs**:



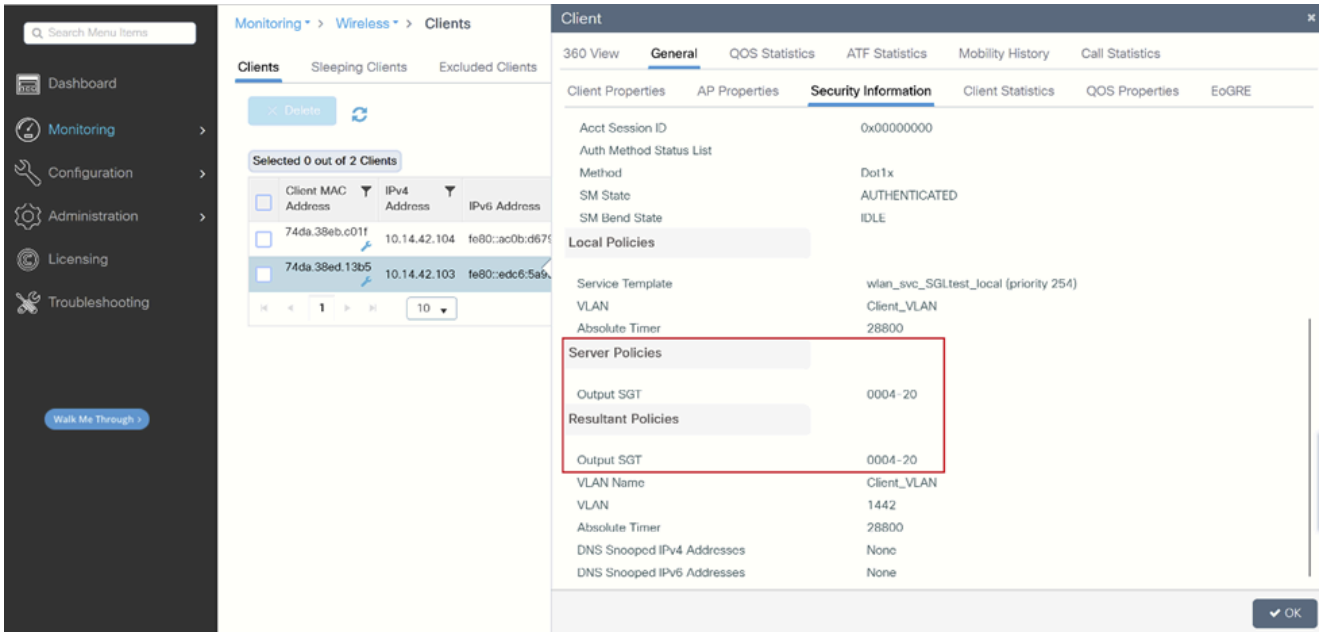
ISE RADIUS Live Logs

2. You can verify that the connection has been established and that the SGTs have been downloaded from **Monitoring > General > Trustsec** on the WLC:



WLC TrustSec Monitoring

3. When connecting a client, the SGT assigned is going to be visible under **Monitoring > Wireless > Clients**, choose the client you would like to check and navigate to **General > Security information** tab:



WLC client monitoring

From the CLI:

- Before connecting the client, this is what you are going to see from the WLC output:

Only the permissions related to unknown SGTs is going to appear.

```
<#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
```

- When connecting the client, you can observe these logs from the RA traces, the SGT gets applied from AAA:

<#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
```

- Use **show wireless client mac-address <client_MAC_address> detail** command from CLI, which is going to show the SGT assigned to the client:

<#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
…
```

- After connecting one client in SGT 4, you are going to notice that the permissions for SGT 4 now appear:
  The permissions are added after the client is connected and is assigned an SGT.

<#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
============================================================
```

- After connecting two clients, one in SGT 4 and the other in SGT 5:

<#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
============================================================
```

- Now you can see that the permissions of SGT 5 are added:

<#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
```

- The ACLs are going to look as "downloaded" on the WLC:

<#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 Local Switching

- This is the WLC output before connecting clients to the AP:

<#root>

#

show cts ap sgt-info <AP_name>

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

SGT               PolicyPushedToAP       No.of Clients
-----------------------------------------------------------
UNKNOWN(0)        NO                     0
```

```
2                NO                    1
DEFAULT(65535)   YES                   0
```

- From AP CLI, this is the permissions output before connecting clients to the AP:

```
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
```

- These are the AP debugs while the client is connecting to show the flow:

<#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
…
```

- From WLC CLI, when connecting one client on SGT 4:

<#root>

#

show cts ap sgt-info

<AP_name>

```
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
```

- From AP CLI:
  You can see the same thing, only permissions related to SGT 4 are added.

```
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
```

- From WLC CLI, when connecting the second client on SGT 5:

<#root>

#

show cts ap sgt-info

<AP_name>

```
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 outputs:

<#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
```

Troubleshoot

- From WLC CLI:

show cts provisioning

show cts role-based permissions

show ip access-lists

show cts ap sgt-info <ap_name>

- From AP:

show cts role-based sgt-map all

show cts role-based permissions

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 debugs:

- Enables CTS packet level enforcement debugging:

debug cts enforcement

term mon

- To check CAPWAP ACL events and payload related information:

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

term mon