Configuration et vérification de SGACL sur le WLC Catalyst 9800 et le serveur ISE

Table des matières

Introduction

Ce document décrit comment configurer TrustSec sur Catalyst 9800 et le serveur ISE pour utiliser la fonctionnalité SGACL, avec des AP en mode local et FlexConnect.

Conditions préalables

Exigences

Connaissance des principes fondamentaux du WLC Cisco 9800, de Cisco ISE, de FlexConnect et de TrustSec.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C980-CL v17.12.4
- ISE 3.2.0
- Point d'accès 9136I

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

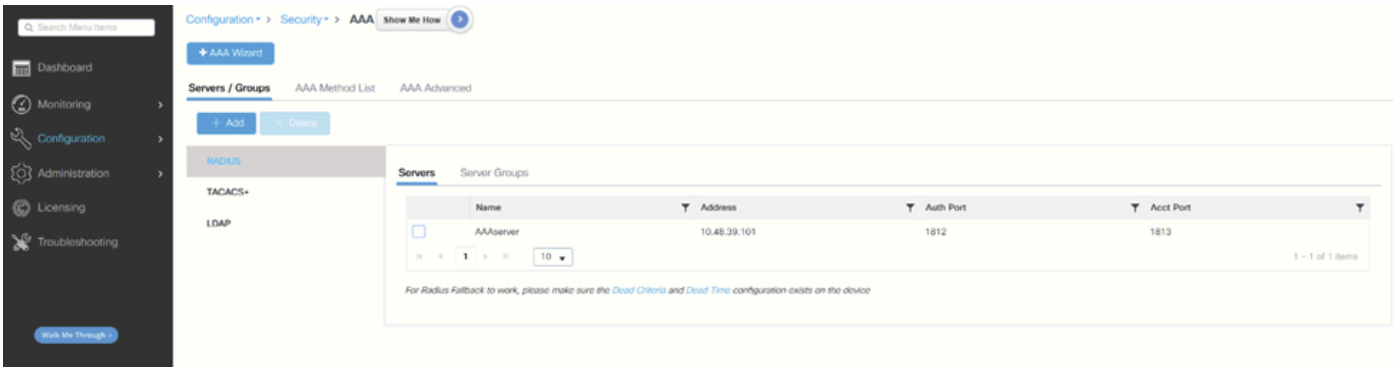
Diagramme du réseau

Diagramme du réseau

Configurations

Configuration WLC

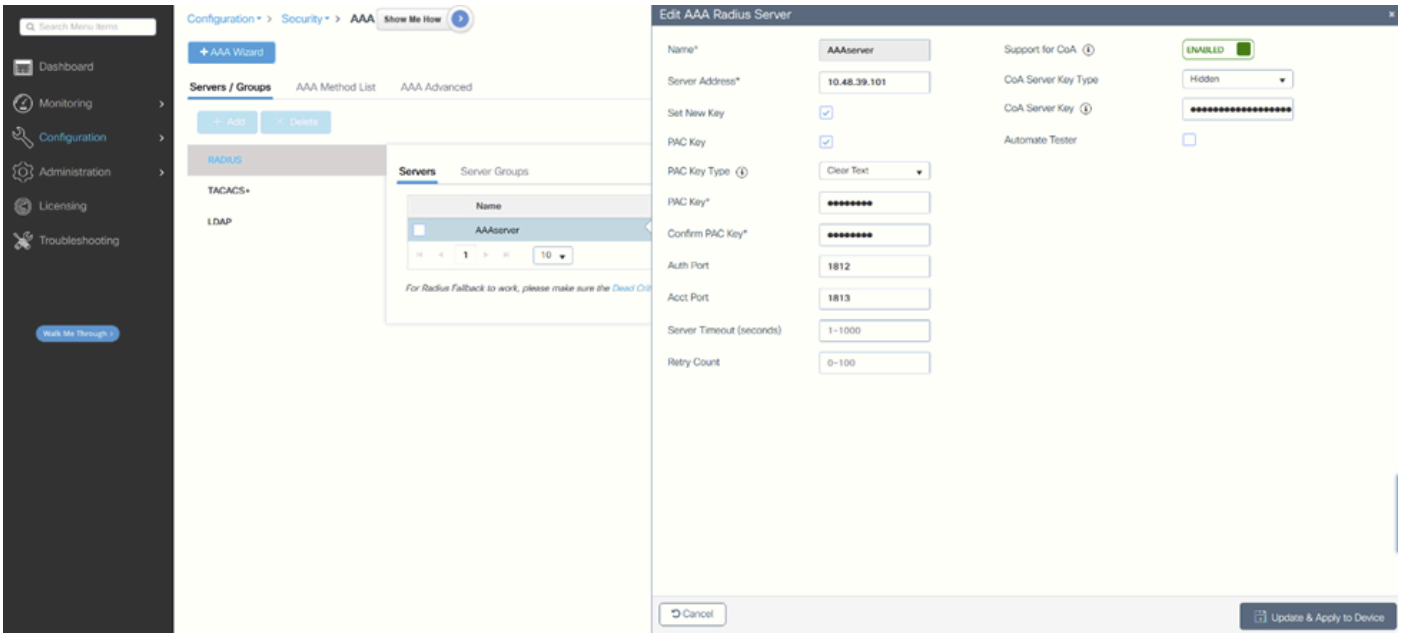
1. Ajoutez le serveur AAA au WLC à partir de Configuration > Security > AAA :



Page WLC AAA

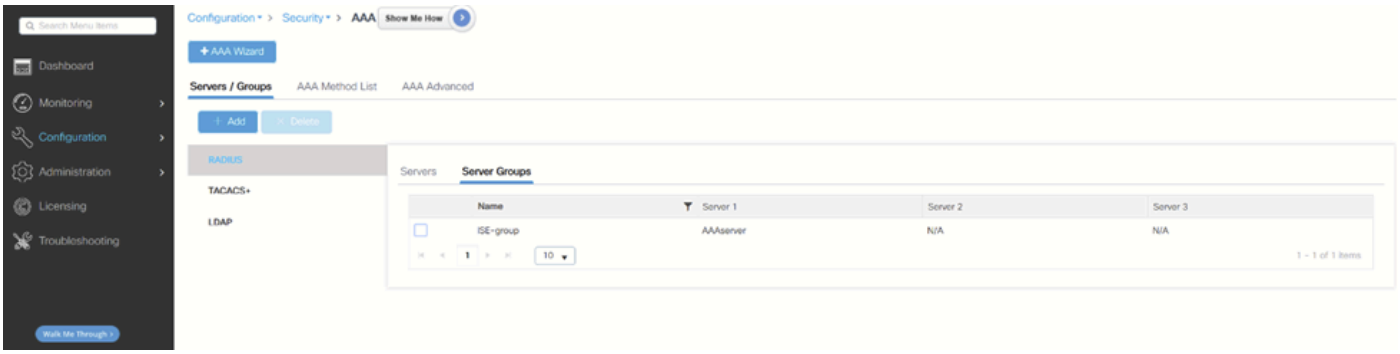
2. Assurez-vous que les entrées de clé ici correspondent à la clé lorsque vous ajoutez le

périphérique sur ISE. Activez Support for CoA et ajoutez la clé si vous souhaitez utiliser CoA pour télécharger les mises à jour de configuration :



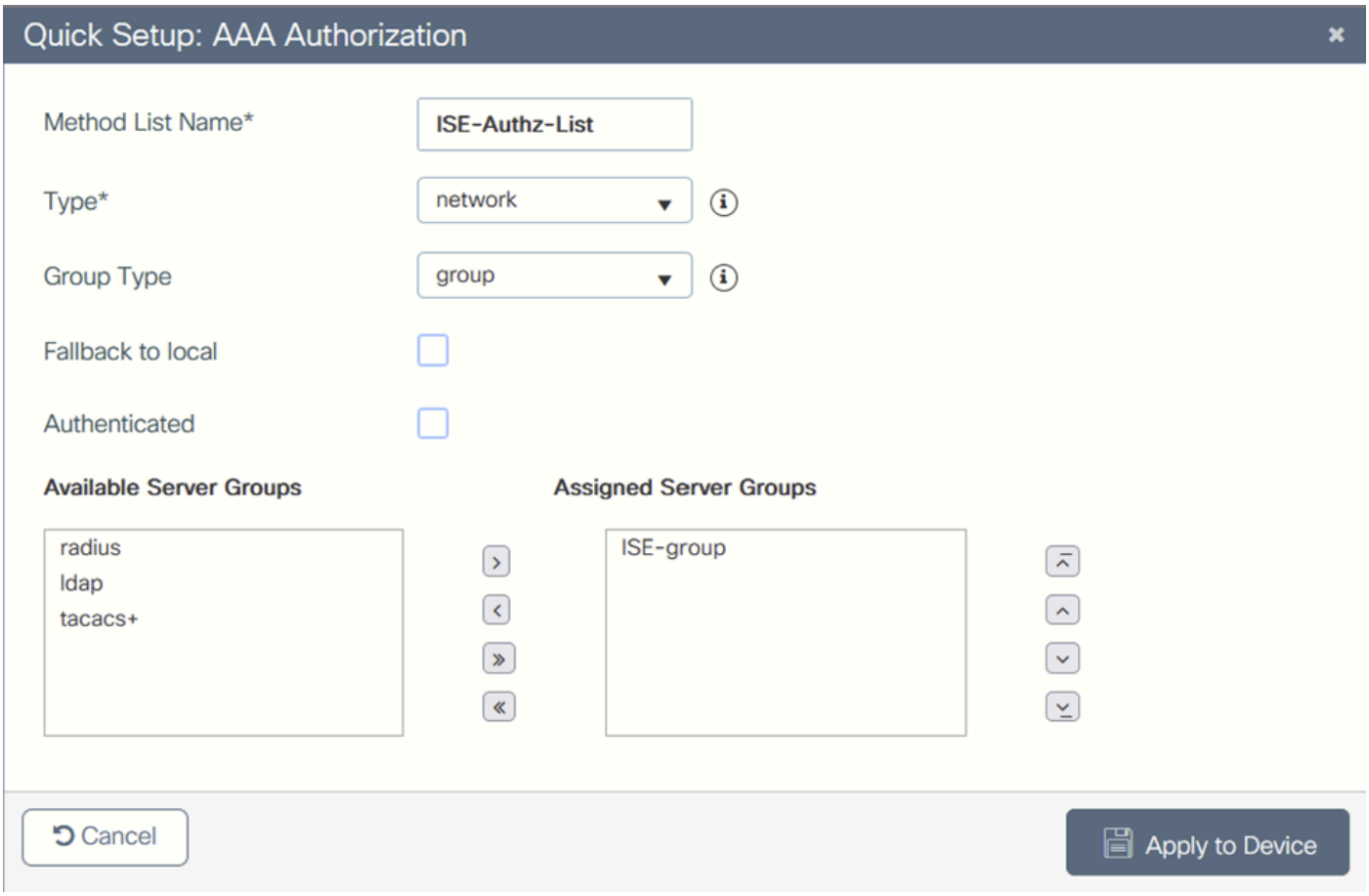
WLC add AAA server

3. Créez le groupe de serveurs :

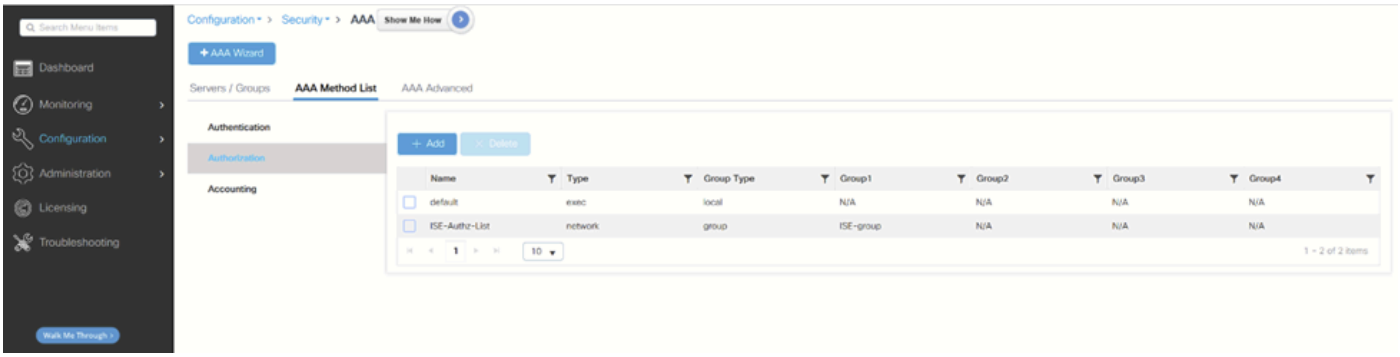


WLC add Server Group

4. Ajoutez la liste des méthodes d'autorisation avec le type network :



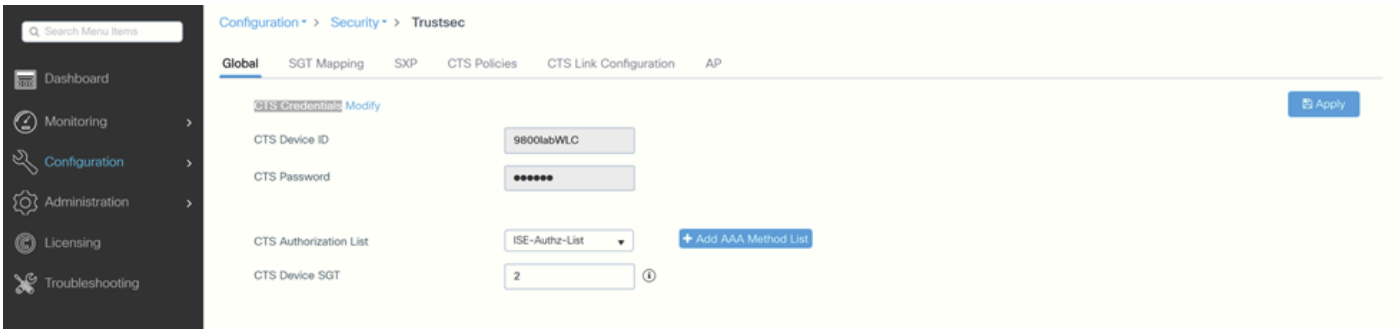
Liste des méthodes d'autorisation



Groupe de serveurs AAA WLC

5. Accédez à Configuration > Security > Trustsec et configurez l'ID de périphérique CTS et le mot de passe CTS, vous allez utiliser ces entrées lors de l'ajout du périphérique sur ISE.

Configurez également ici la liste d'autorisations CTS que vous avez créée à l'étape 4 :

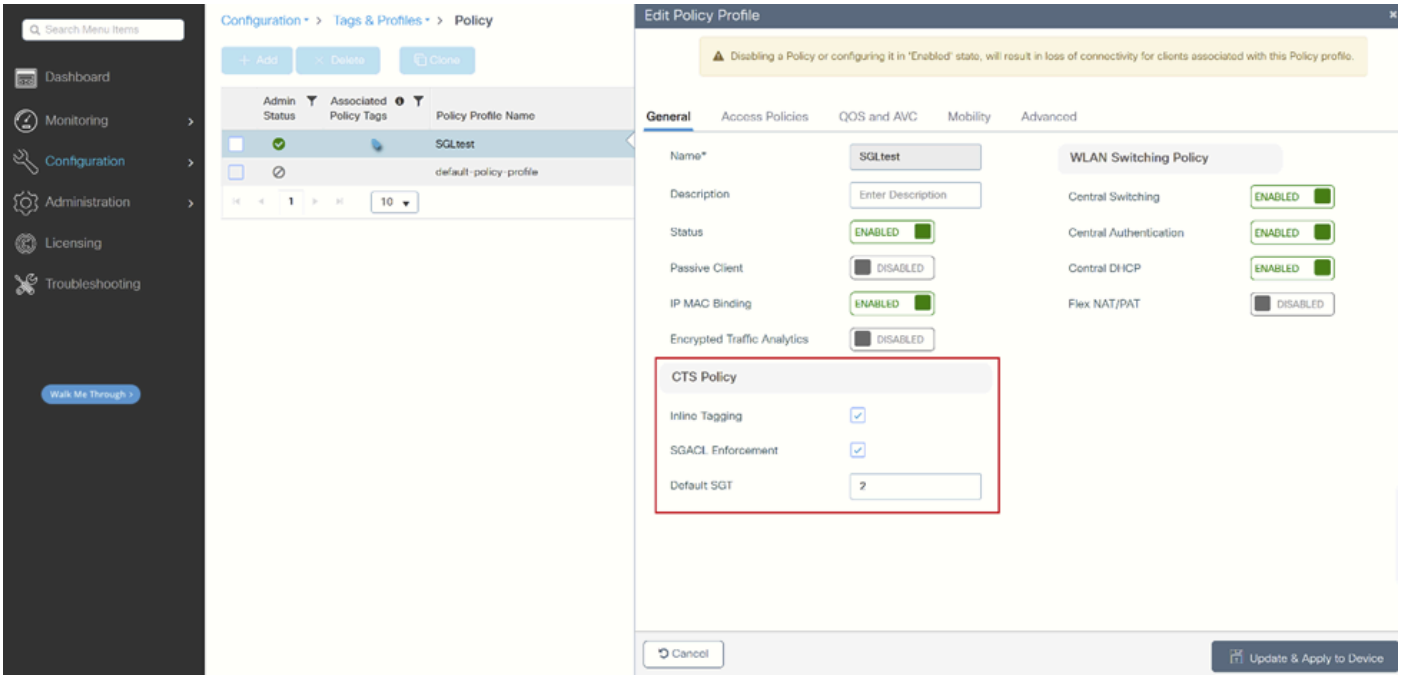


TrustSec WLC

6. Dans cet exemple, le WLAN est déjà créé et les paramètres d'authentification sont déjà configurés.

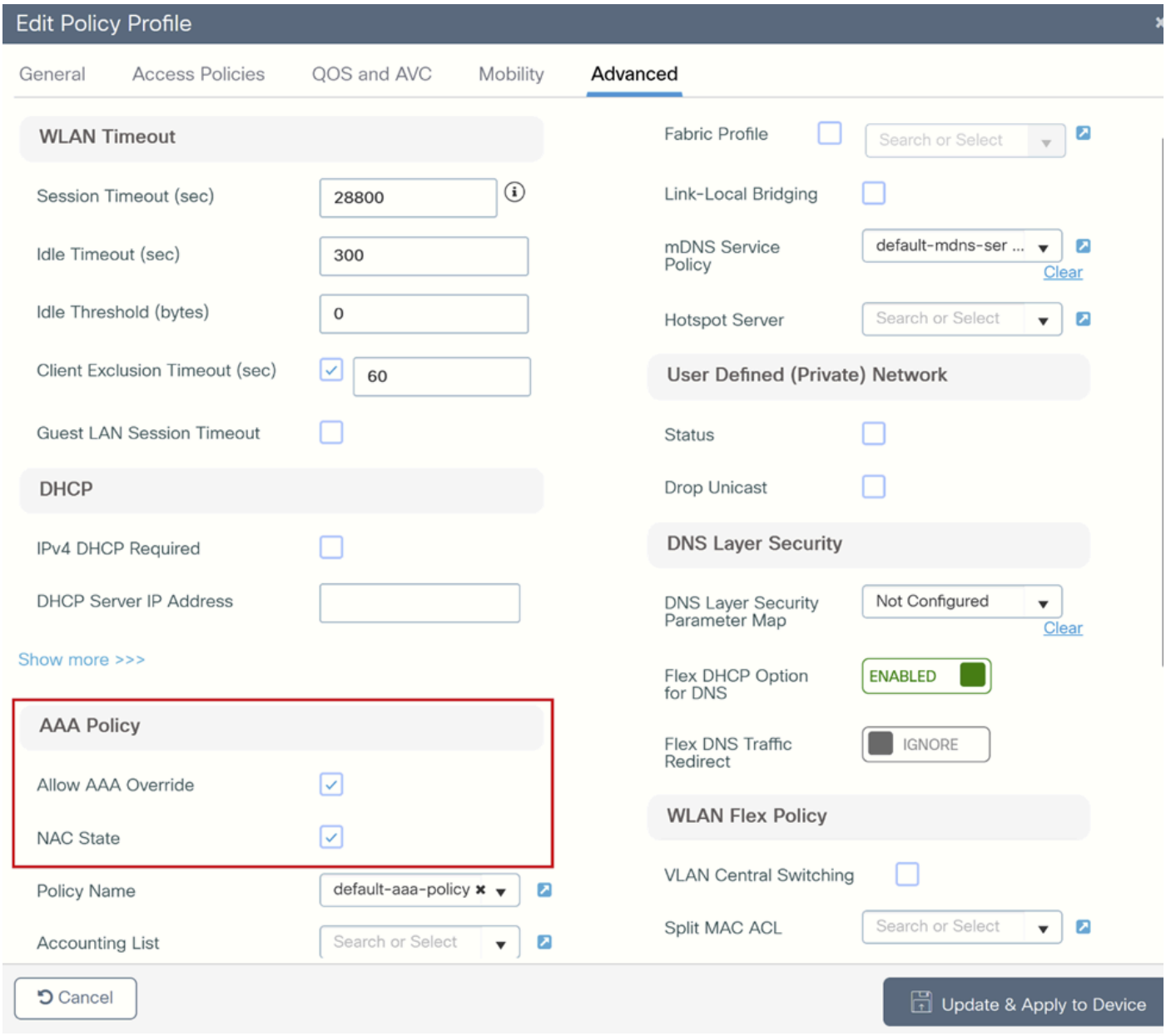
À présent, accédez au profil de stratégie sur lequel vous souhaitez utiliser les balises de groupe de sécurité.

i. Sous CTS Policy, activez Inline Tagging et SGACL Enforcement, vous pouvez également spécifier le SGT par défaut. La SGT 2 par défaut est utilisée pour ces travaux pratiques à titre d'exemple :



Profil de stratégie WLC

ii. Sous l'onglet Advanced, activez Allow AAA override et l'état NAC :



Onglet Profil de stratégie WLC avancé

À partir de la CLI :

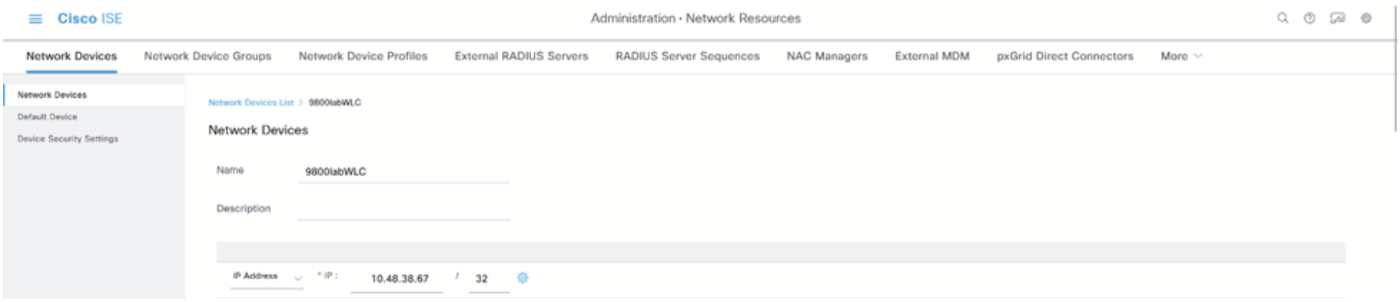
```
# configure terminal

(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
```

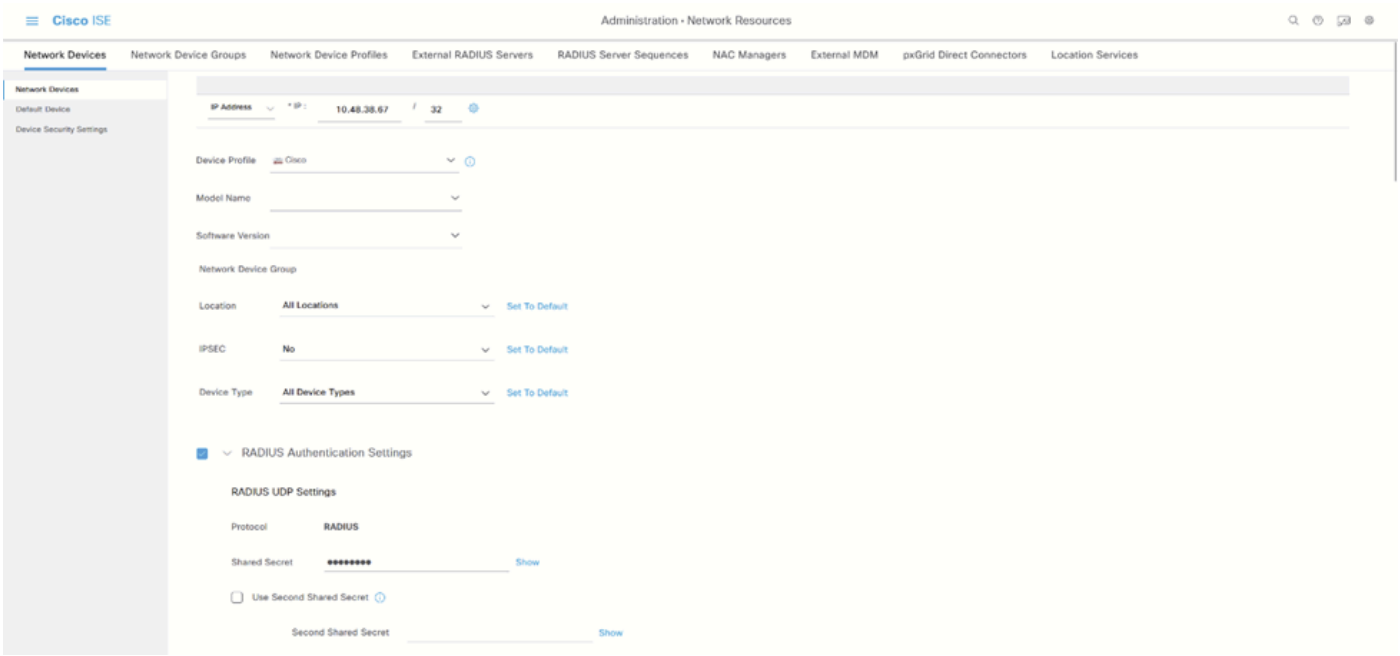
Configuration ISE

1. Accédez à Administration > Network Resources > Network Devices.

i. Ajoutez les informations WLC ici :

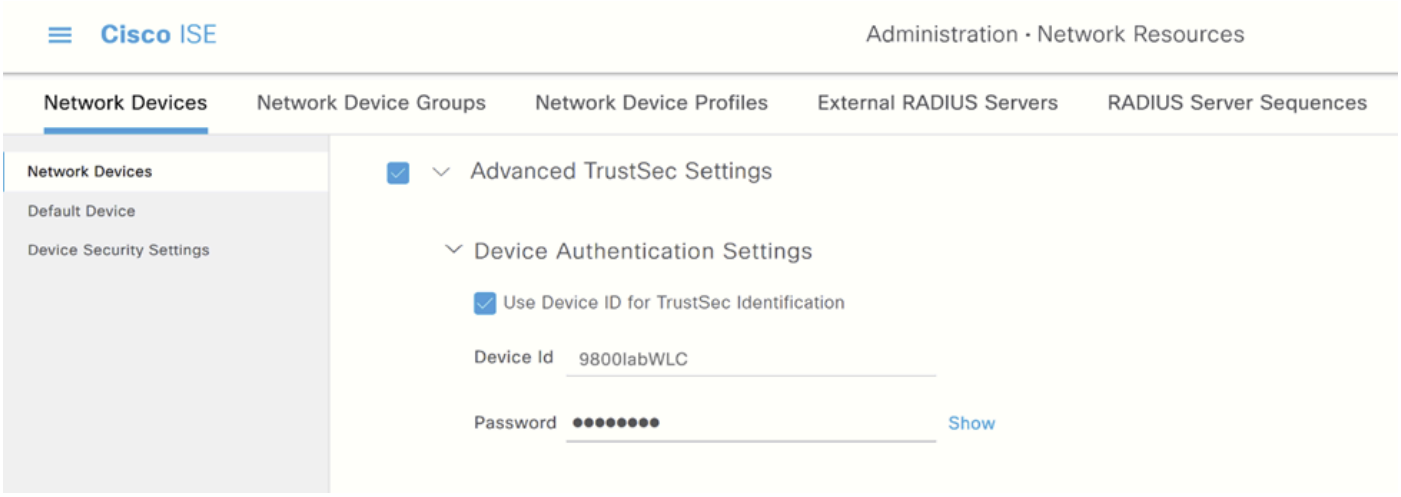


Page Périphériques réseau ISE



ISE ajouter des informations WLC RADIUS

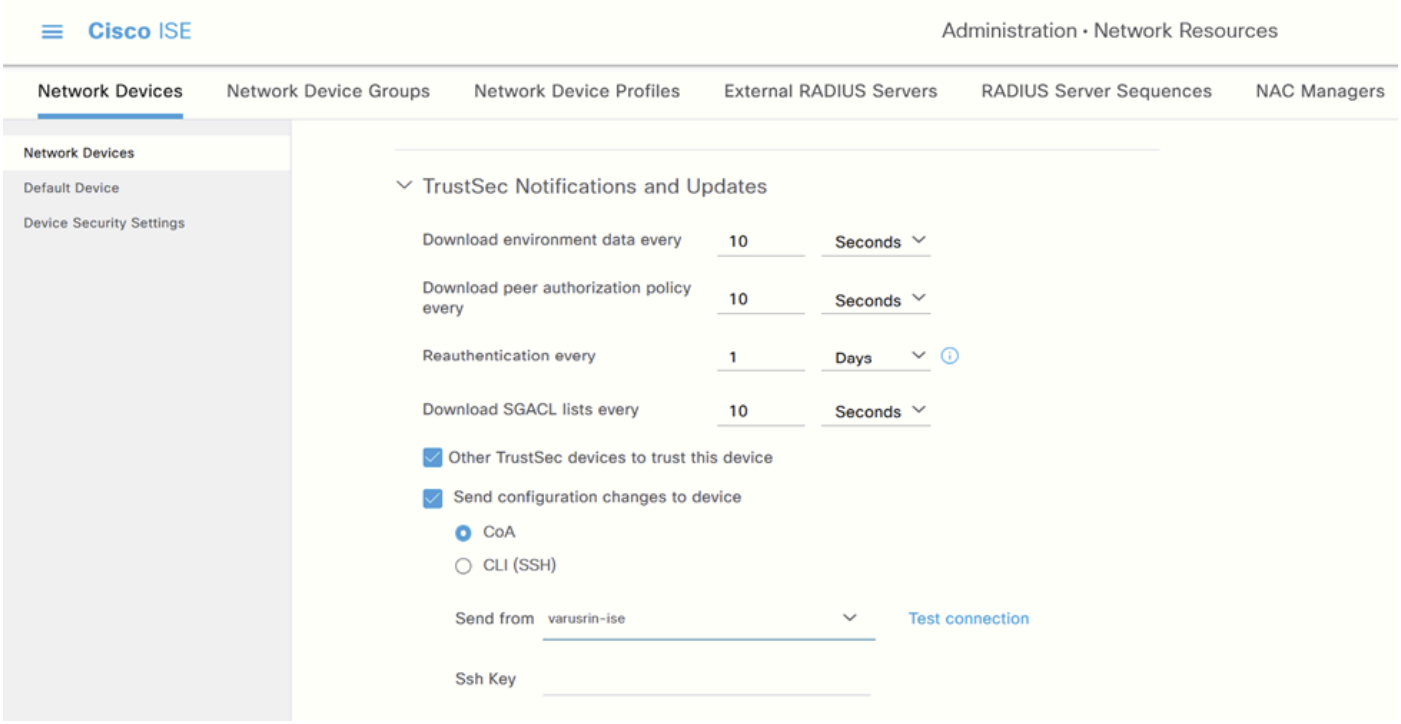
ii. Faites défiler vers le bas et configurez Advanced TrustSec Settings, activez la case à cocher Use Device ID for TrustSec Identification et configurez le mot de passe :



Paramètres TrustSec avancés

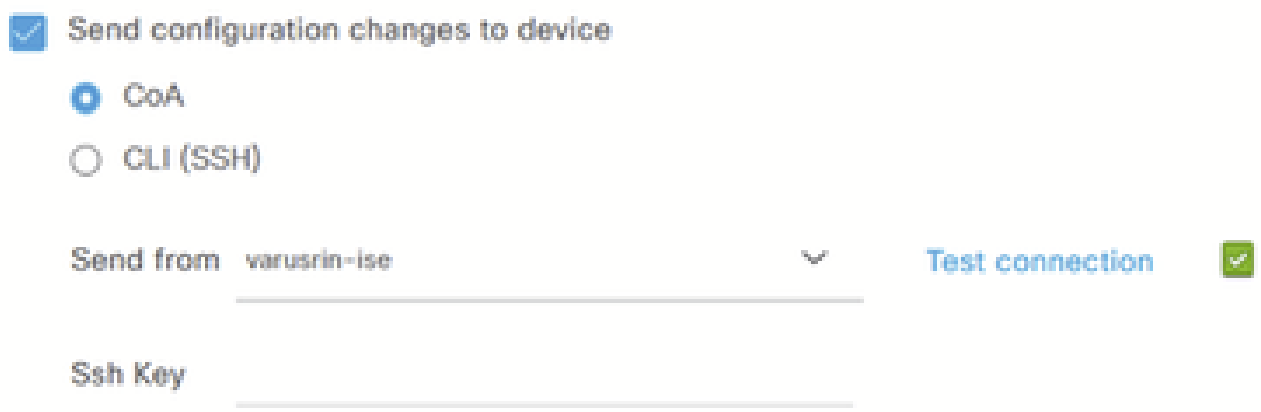
Cela doit correspondre à la configuration côté WLC à l'étape 6 de la configuration WLC.

iii. Faites défiler jusqu'à Notifications et mises à jour TrustSec et configurez si vous souhaitez utiliser CoA ou SSH pour les mises à jour de configuration. Sélectionnez le noeud ISE requis :



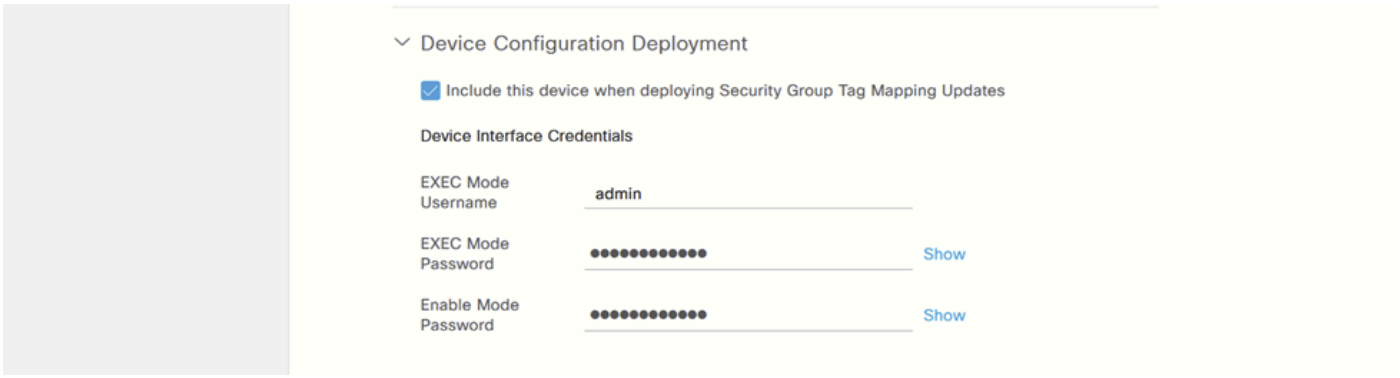
Notifications et mises à jour TrustSec

2. Appuyez sur Test connection pour vous assurer que la connexion est établie. Quand il réussit, il va afficher une coche verte :



Tester la connexion

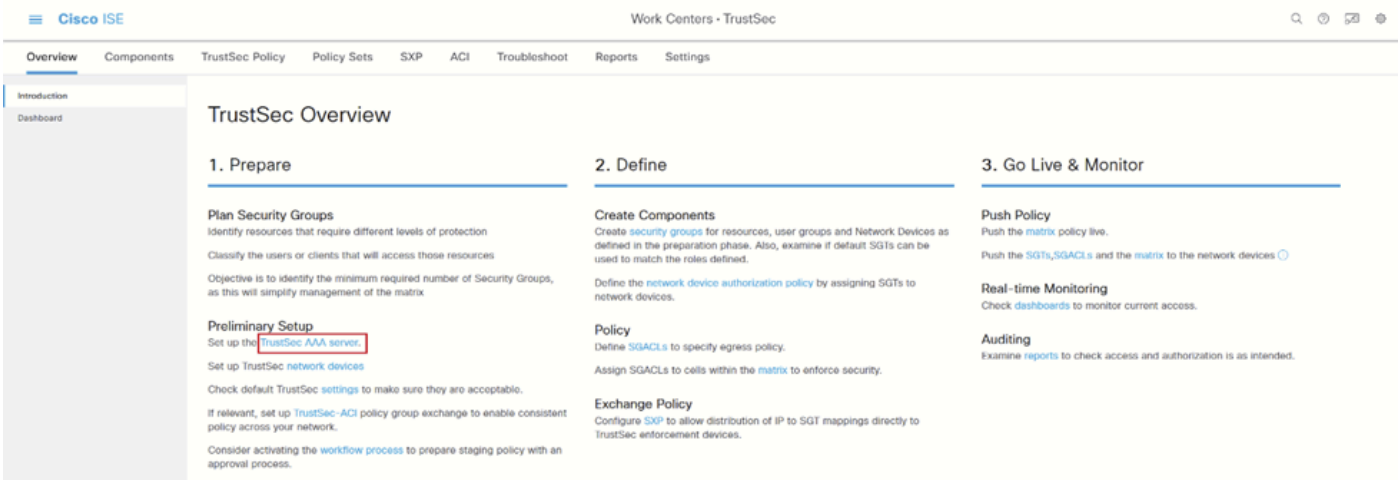
i. Faites défiler vers le bas et configurez le WLC à inclure lors du déploiement des mises à jour de mappage SGT. Ceci est important si vous sélectionnez l'option SSH à l'étape précédente :



Déploiement de la configuration des périphériques

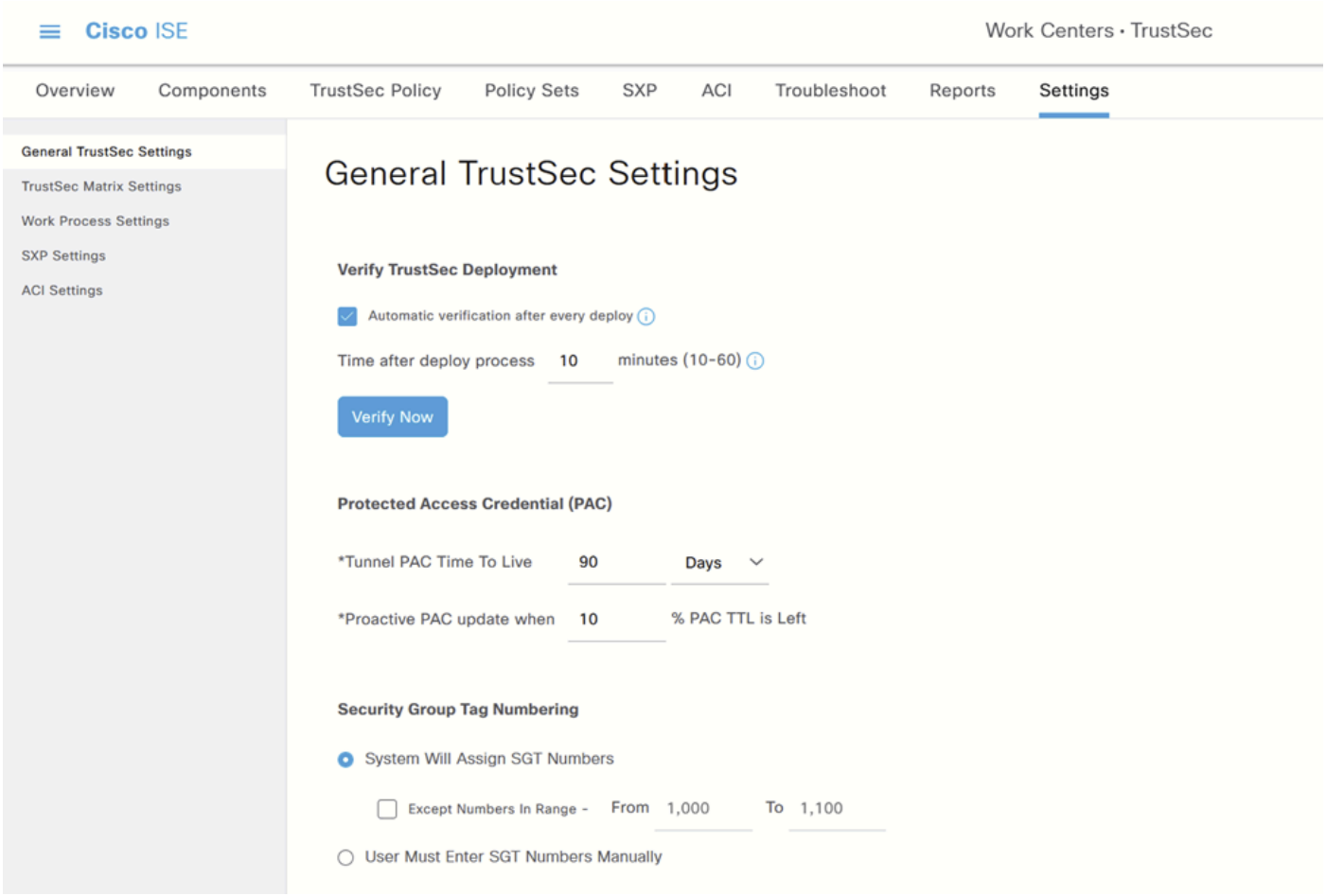
ii. Enregistrez la configuration.

3. Dans Work Centers > TrustSec > Overview, vous disposez des options de configuration TrustSec. Choisissez TrustSec AAA Server pour afficher l'instance ISE en cours d'utilisation. Référez-vous à Stratégie de groupe sans fil Cisco Catalyst pour plus d'informations sur l'instance qui est utilisée si vous avez des multiples.



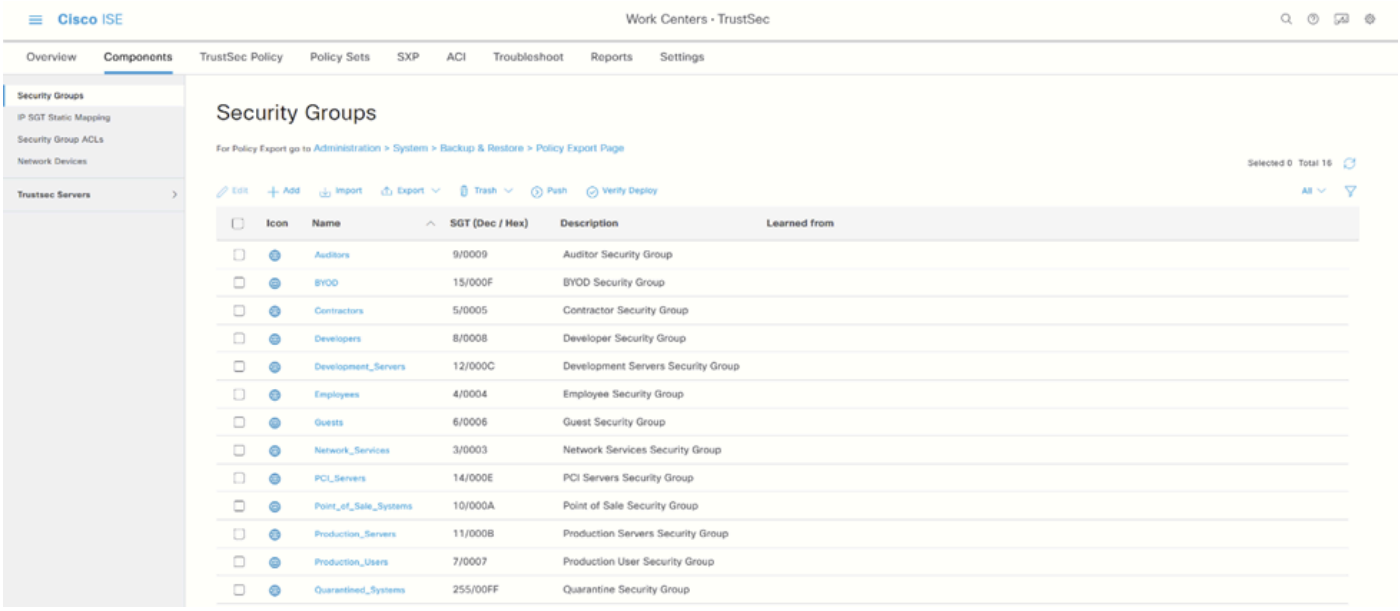
Présentation d'ISE TrustSec

4. (Facultatif) Accédez à l'onglet Paramètres, activez la vérification automatique après chaque déploiement si vous le souhaitez.



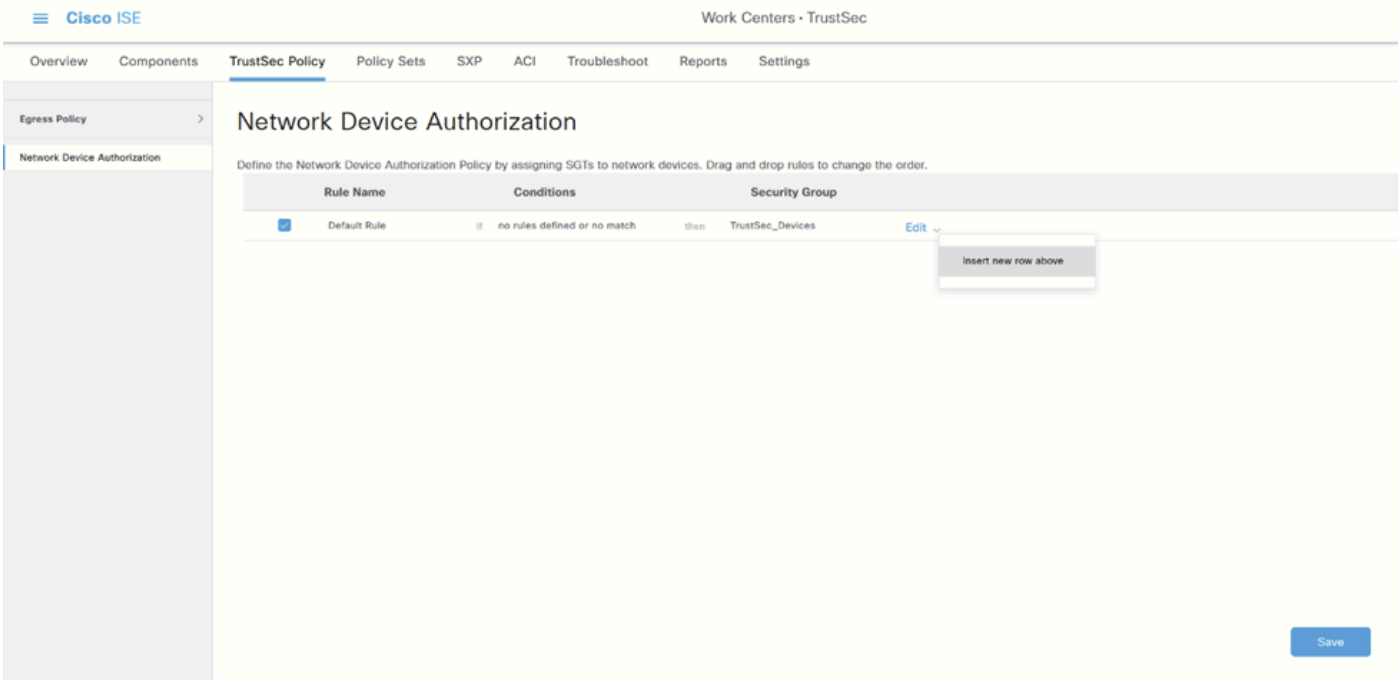
Paramètres TrustSec ISE

5. Ajoutez ou modifiez les valeurs SGT à partir de Work Centers > TrustSec > Components > Security Groups selon vos besoins :



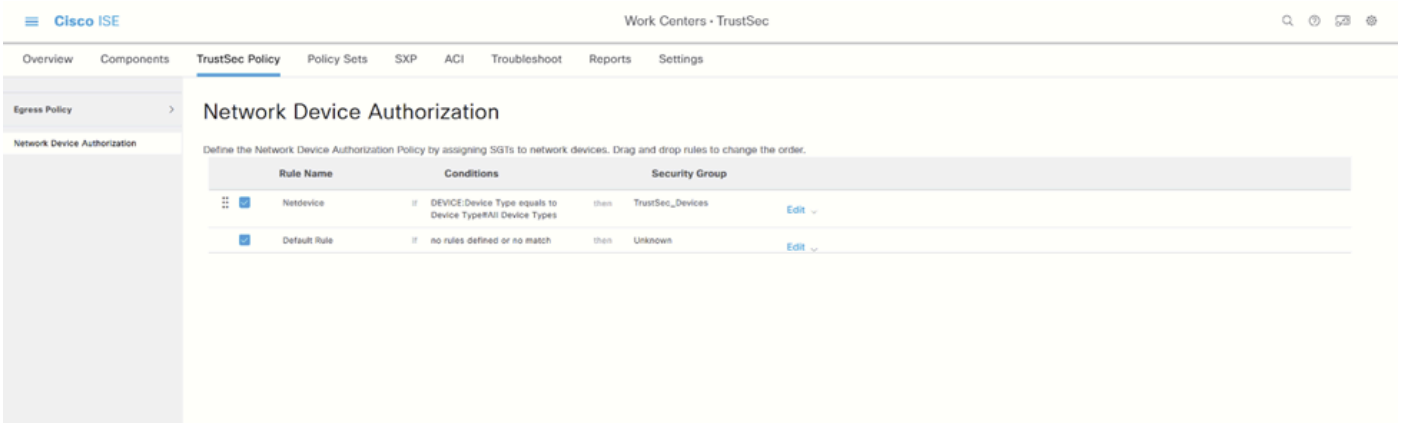
Groupes de sécurité ISE

6. Si vous souhaitez spécifier la stratégie d'autorisation, accédez à Work Centers > TrustSec > TrustSec Policy > Network Device Authorization :



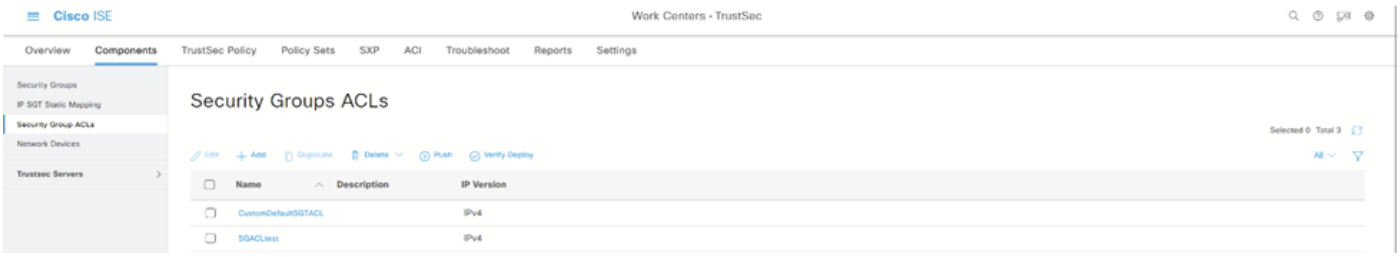
Stratégie TrustSec

Vous pouvez conserver la valeur par défaut, mais pour ces travaux pratiques, nous utilisons cette configuration comme exemple :



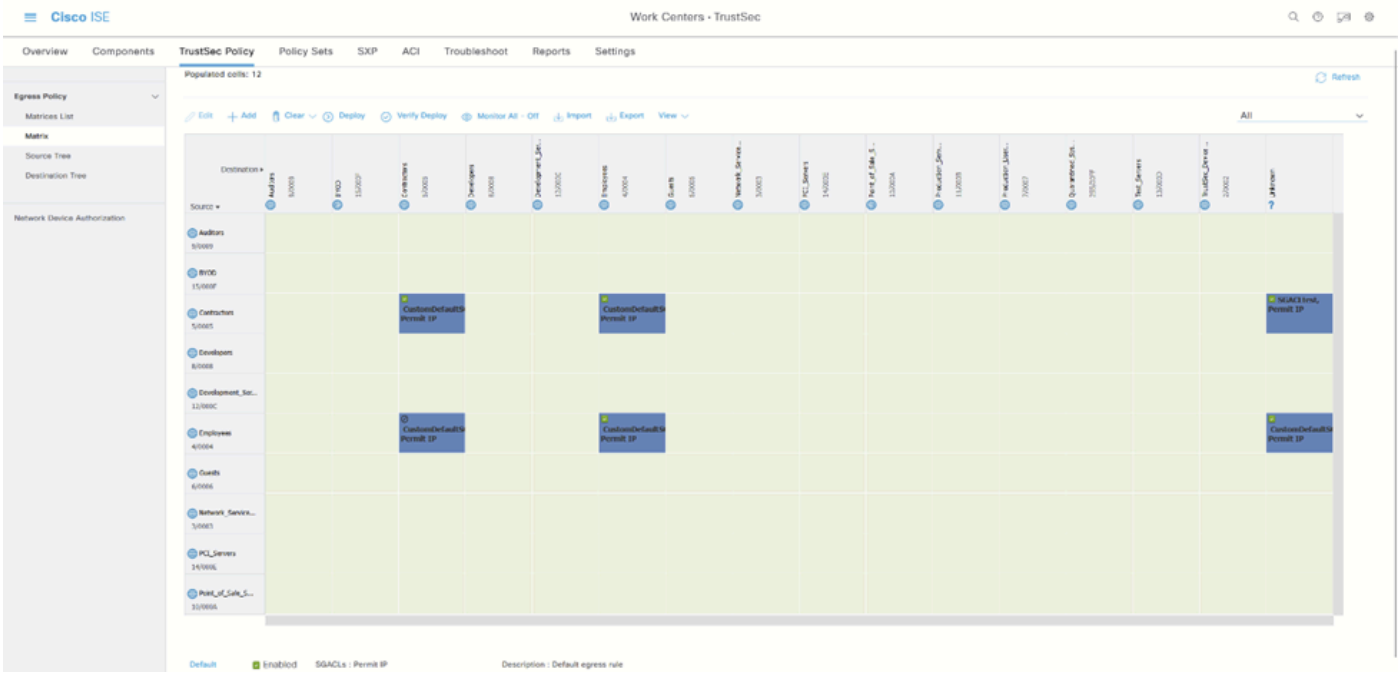
Autorisation de périphérique réseau

7. Créez la SGACL sous l'onglet Composants, puis les ACL du groupe de sécurité :



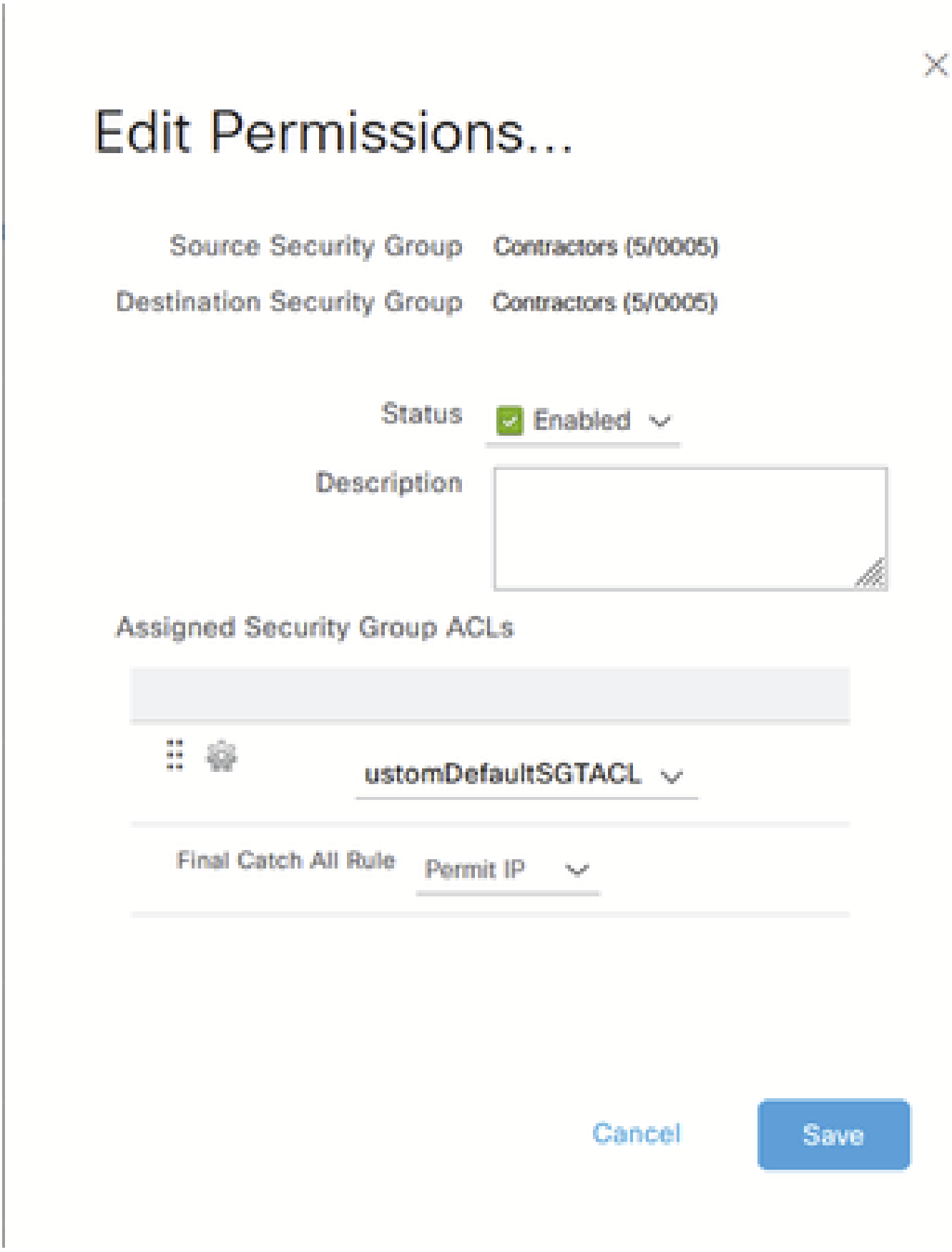
ACL de groupe de sécurité

8. Spécifiez les entrées de la matrice sous l'onglet Stratégie TrustSec, puis Matrice. Vous pouvez modifier les autorisations en cliquant sur le point auquel deux SGT se rencontrent :

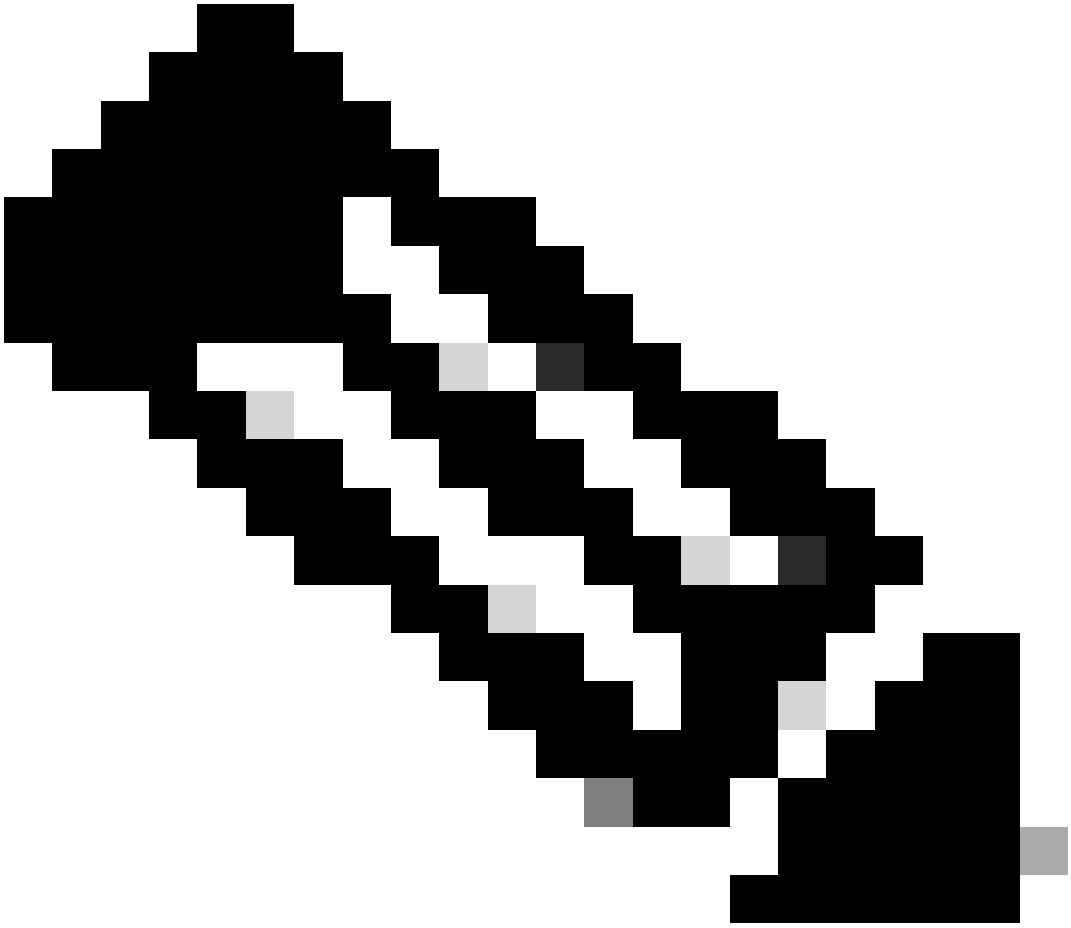


Matrice ISE TrustSec

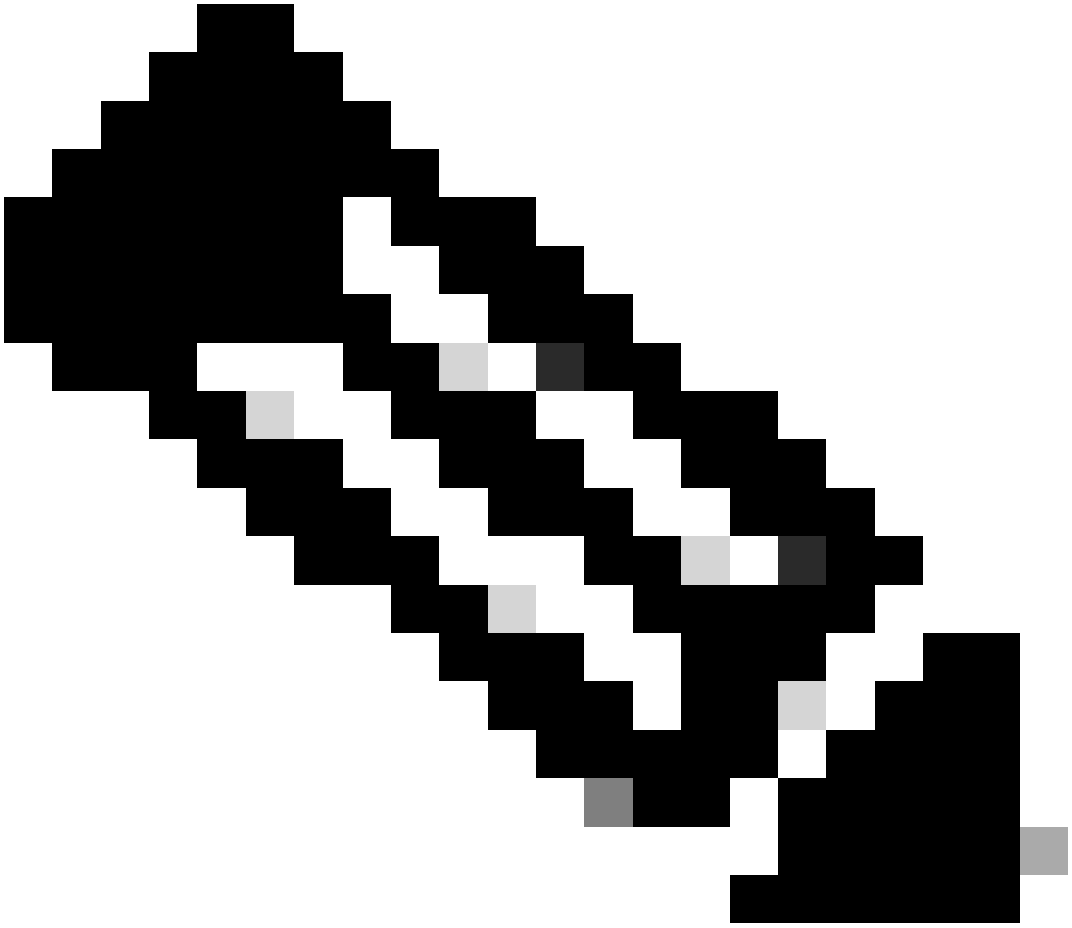
Exemple :



Modifier les autorisations

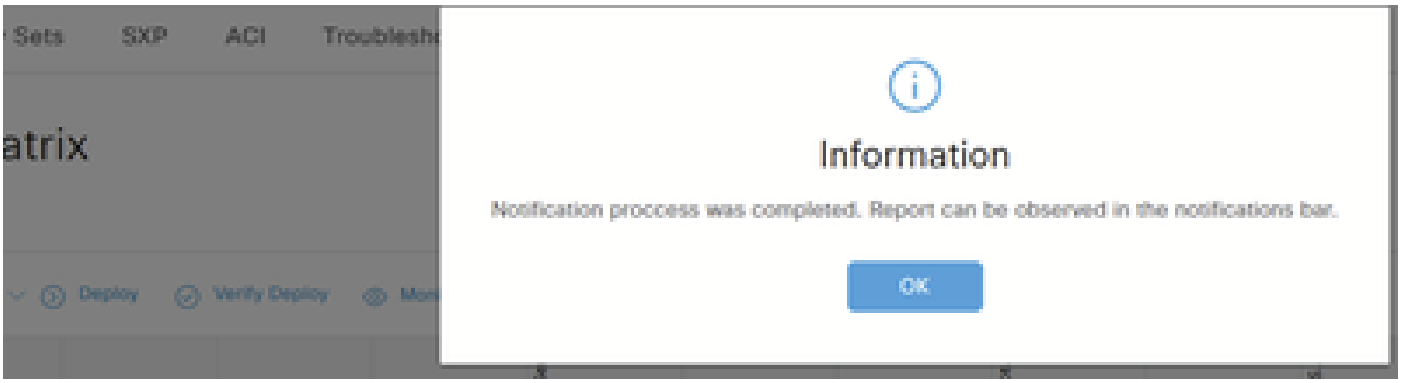


Remarque : Dans le cas d'un modèle de liste verte, vous devez explicitement autoriser le protocole DHCP pour que les périphériques clients obtiennent l'adresse IP DHCP, puis demander au contrôleur des stratégies SGACL.

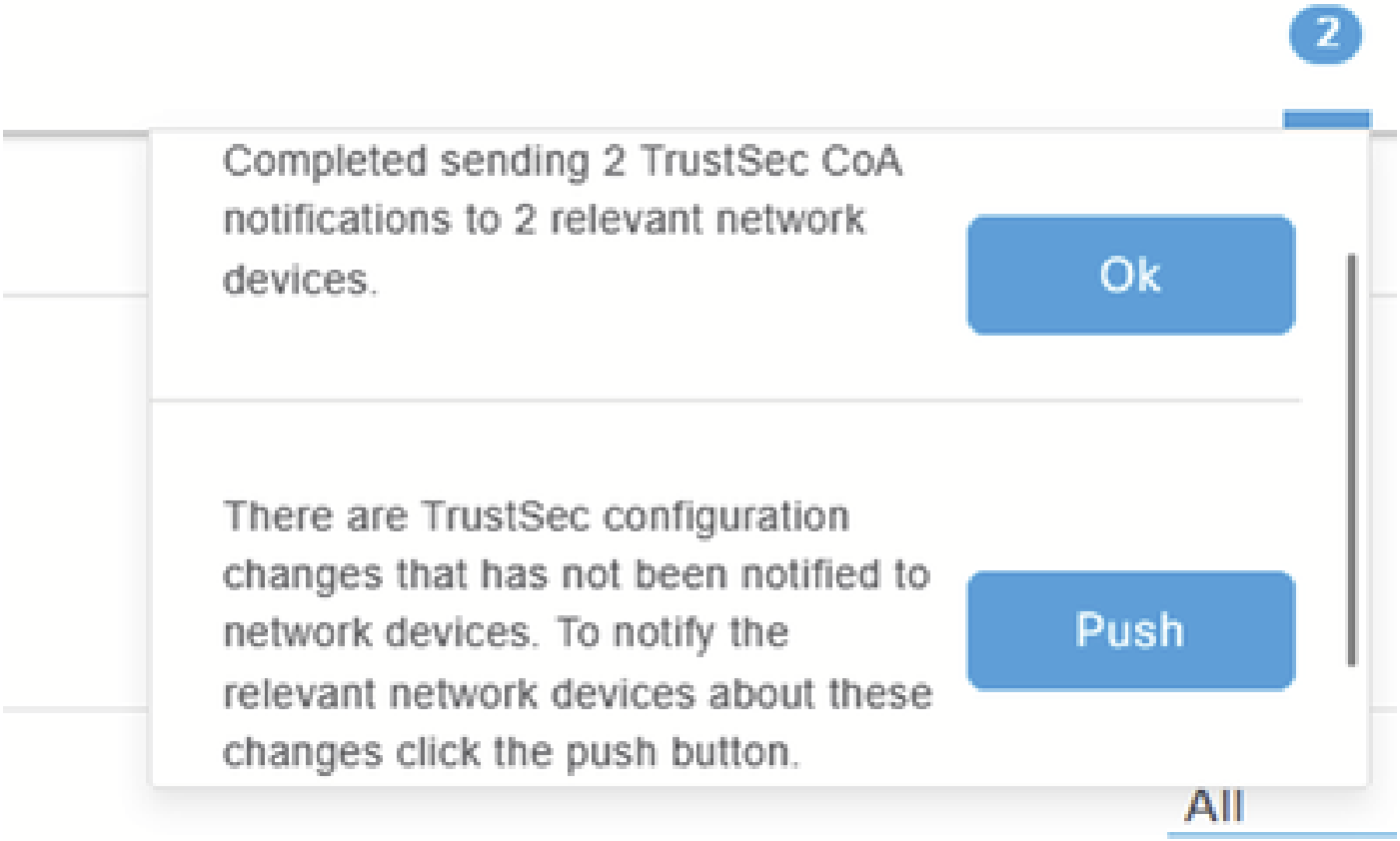


Remarque : Les clients reçoivent une valeur SGT nulle et les clients DHCP reçoivent une adresse APIPA (Automatic Private IP Addressing) lorsque la stratégie TrustSec « unknown to unknown » est refusée dans la matrice TrustSec.
Les clients reçoivent les valeurs SGT correctes et les clients DHCP reçoivent une adresse IP lorsque la stratégie TrustSec « unknown to unknown » est autorisée dans la matrice TrustSec.

9. Cliquez sur Déployer. Ce qui va donner lieu à ces messages et notifications :



Déploiement

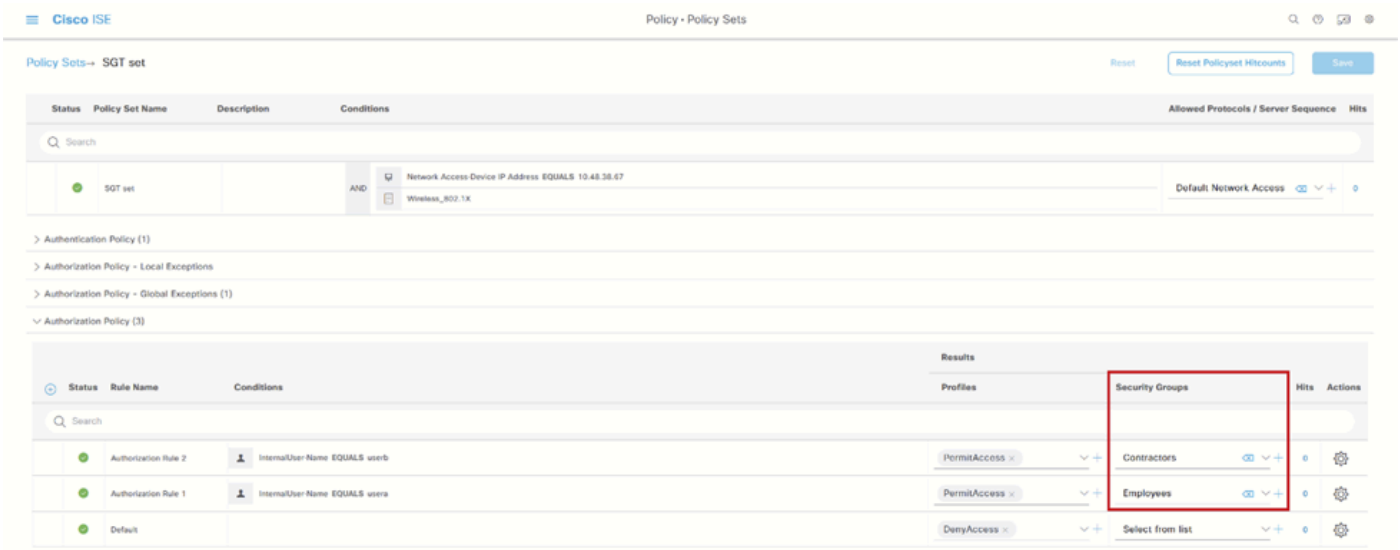


Déployer des notifications

10. Accédez à l'ensemble de stratégies utilisé pour le WLAN sous Stratégie > Ensembles de stratégies :

Ensembles de stratégies ISE

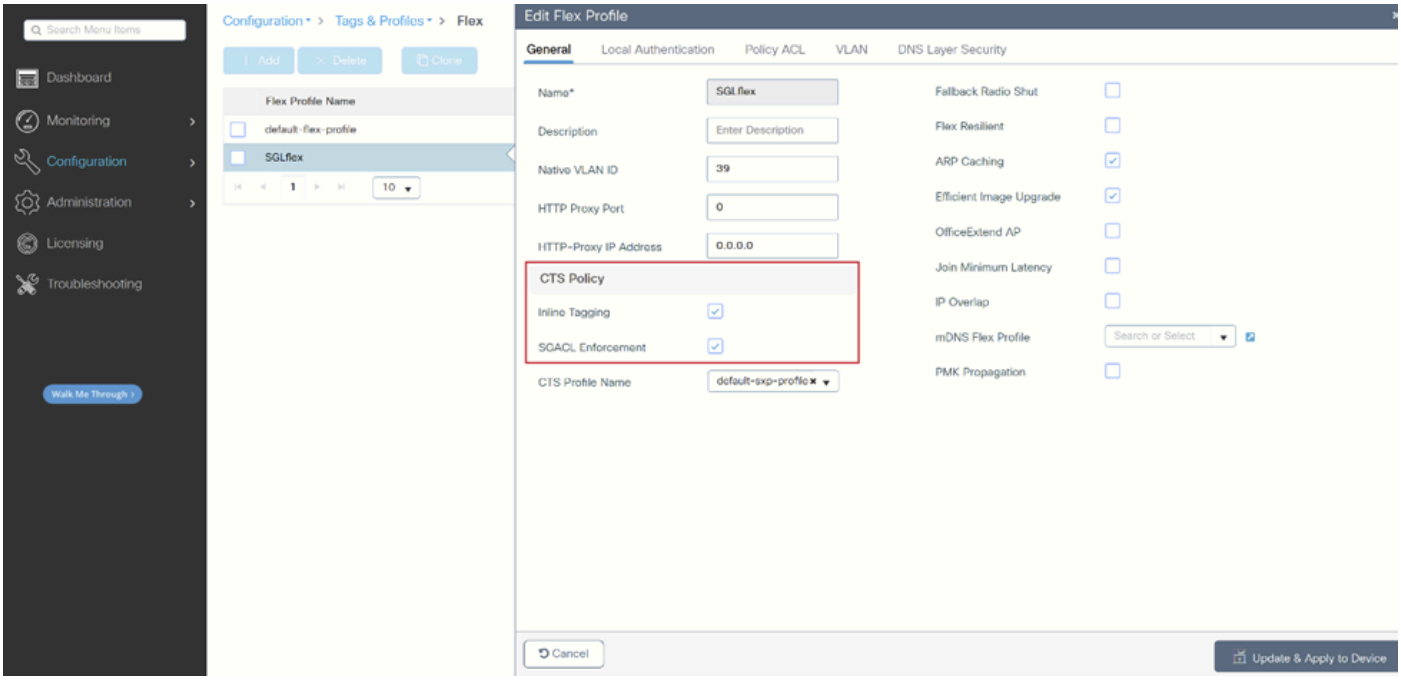
Au cours de ces travaux pratiques, nous allons définir le SGT par utilisateur. Sélectionnez le SGT dans le champ Groupes de sécurité :



Groupes de sécurité ISE

Flexconnect

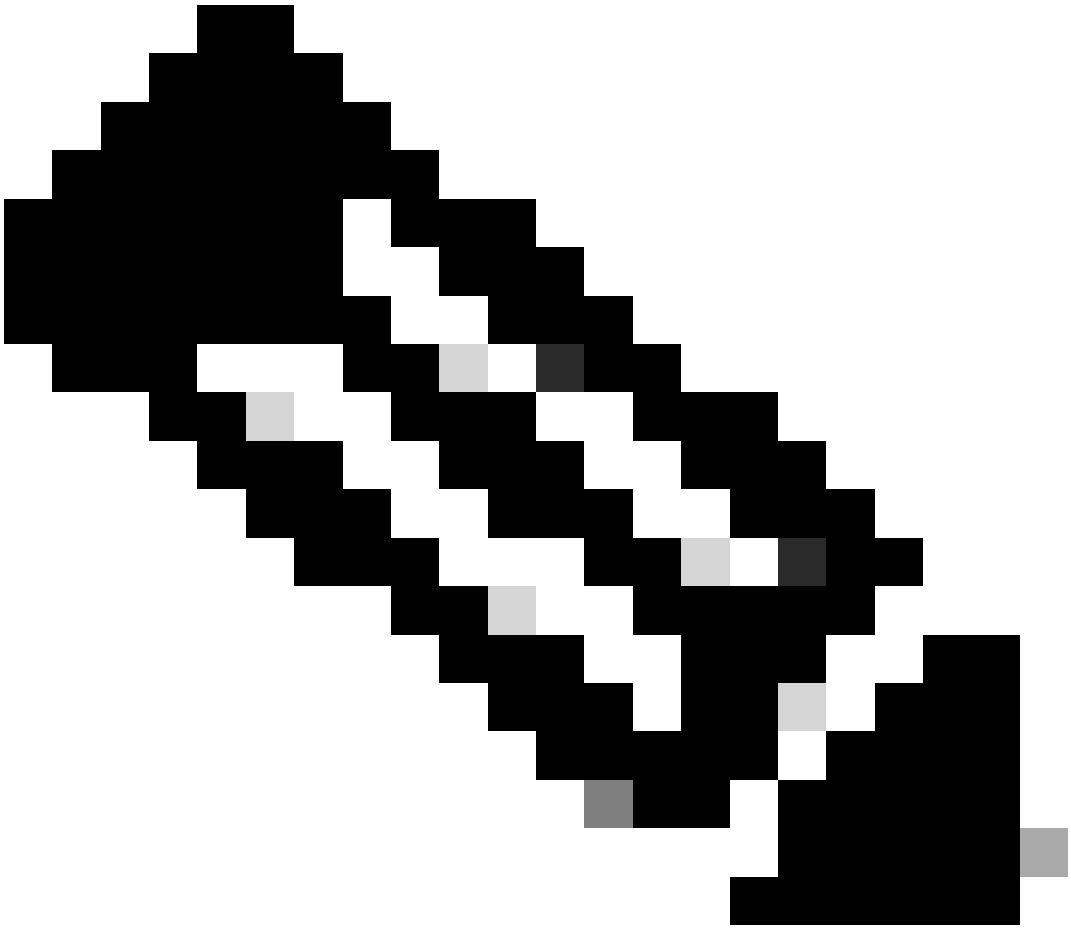
Activez le balisage en ligne et l'application de SGACL sur le profil Flex sous Configuration > Tags & Policies > Flex :



Profil WLC Flex

À partir de la CLI :

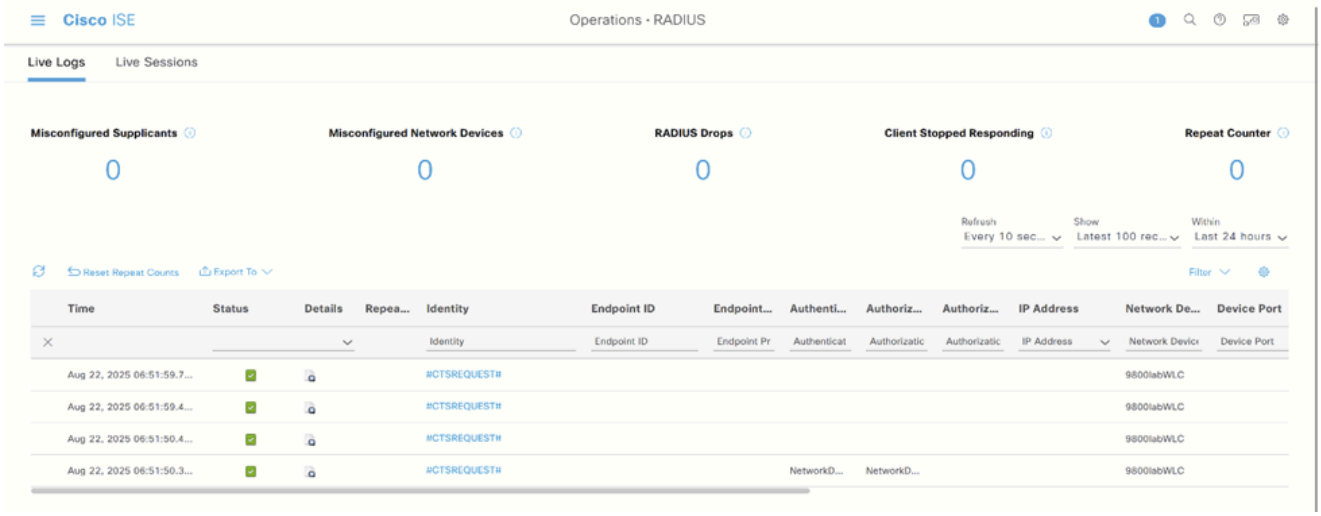
```
# configure terminal

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



Remarque : Si le WLC est dans HA-SSO, SGACL sur les AP FlexConnect n'est pas pris en charge. ID de bogue Cisco CSCwn85468. Il va être ajouté dans la version 17.19.

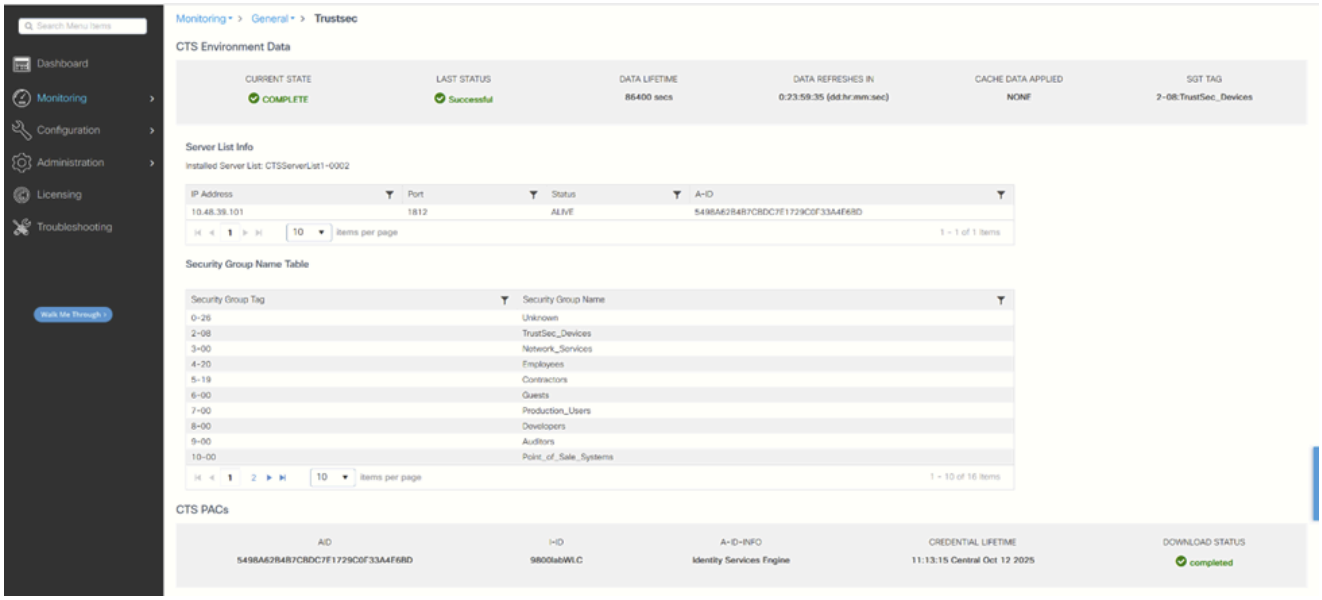
Vérifier

1. Dans ISE, vous devez voir la requête CTS réussie sous Operations > RADIUS > Live Logs :



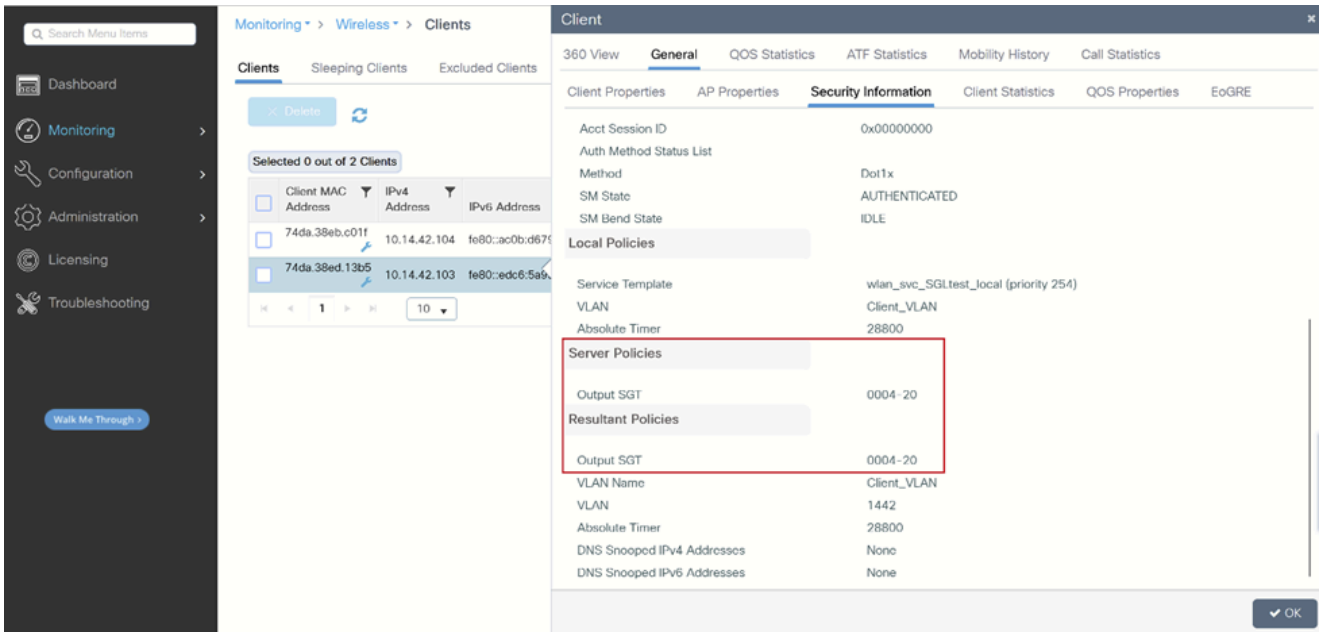
Journaux en direct ISE RADIUS

2. Vous pouvez vérifier que la connexion a été établie et que les SGT ont été téléchargés à partir de Monitoring > General > Trustsec sur le WLC :



Surveillance TrustSec WLC

3. Lors de la connexion d'un client, le SGT attribué va être visible sous Surveillance > Sans fil > Clients, choisissez le client que vous souhaitez vérifier et accédez à Général > Informations de sécurité onglet :



Surveillance du client WLC

À partir de la CLI :

- Avant de connecter le client, voici ce que vous allez voir dans la sortie du WLC : Seules les autorisations liées aux balises de groupe de sécurité inconnues vont apparaître.

```
<#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
```

- Lors de la connexion du client, vous pouvez observer ces journaux à partir des traces RA, le SGT est appliqué à partir de 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
```

- Utilisez la commande show wireless client mac-address <client_MAC_address> detail de l'interface de ligne de commande, qui va afficher le SGT attribué au 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
…
```

- Après avoir connecté un client dans SGT 4, vous remarquerez que les autorisations pour SGT 4 apparaissent maintenant :
  Les autorisations sont ajoutées après la connexion du client et l'attribution d'un 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
============================================================
```

- Après avoir connecté deux clients, l'un dans SGT 4 et l'autre dans 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
============================================================
```

- Maintenant, vous pouvez voir que les autorisations de SGT 5 sont ajoutées :

<#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
```

- Les listes de contrôle d'accès auront l'apparence « téléchargées » sur le 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
```

Commutation locale FlexConnect

- Voici la sortie du WLC avant de connecter les clients au point d'accès :

<#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
```

- À partir de l'interface de ligne de commande AP, voici le résultat des autorisations avant de connecter les clients à l'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
```

- Voici les débogages AP pendant que le client se connecte pour afficher le flux :

<#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
…
```

- À partir de l'ILC WLC, lors de la connexion d'un client sur SGT 4 :

<#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
```

- À partir de AP CLI :
  Vous pouvez voir la même chose, seules les autorisations liées à SGT 4 sont ajoutées.

```
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
```

- À partir de l'ILC WLC, lors de la connexion du deuxième client sur SGT 5 :

```
<#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
```

- Sorties AP :

```
<#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
```

Dépannage

- À partir de CLI WLC :

show cts provisioning

show cts role-based permissions

show ip access-lists

show cts ap sgt-info <ap_name>

- À partir du point d'accès :

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

- Débogages AP :

- Active le débogage d'application au niveau paquet CTS :

debug cts enforcement

terme mon

- Pour vérifier les événements ACL CAPWAP et les informations relatives aux données utiles :

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

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

terme mon

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.