SGACL configureren en verifiëren op Catalyst 9800 WLC en ISE Server

Inhoud

Inleiding

In dit document wordt beschreven hoe u TrustSec op Catalyst 9800 en ISE-server kunt configureren om de SGACL-functie te gebruiken, met lokale en FlexConnect-toegangspunten.

Voorwaarden

Vereisten

Kennis van Cisco 9800 WLC, Cisco ISE, FlexConnect en TrustSec fundamentals.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C9800-CL v17.12.4
- ISE 3.2.0
- 9136I-toegangspunt

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

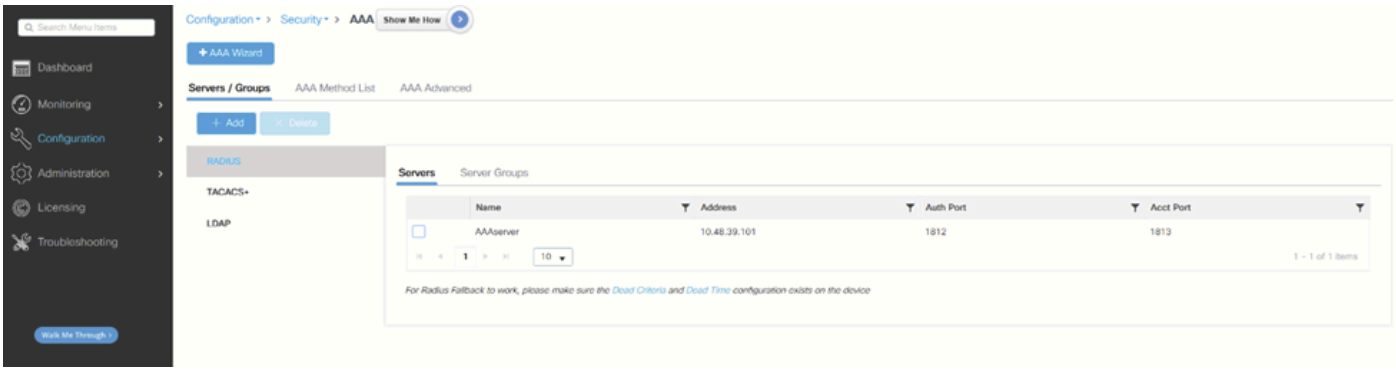
Netwerkdiagram

Netwerkdiagram

Configuraties

WLC-configuratie

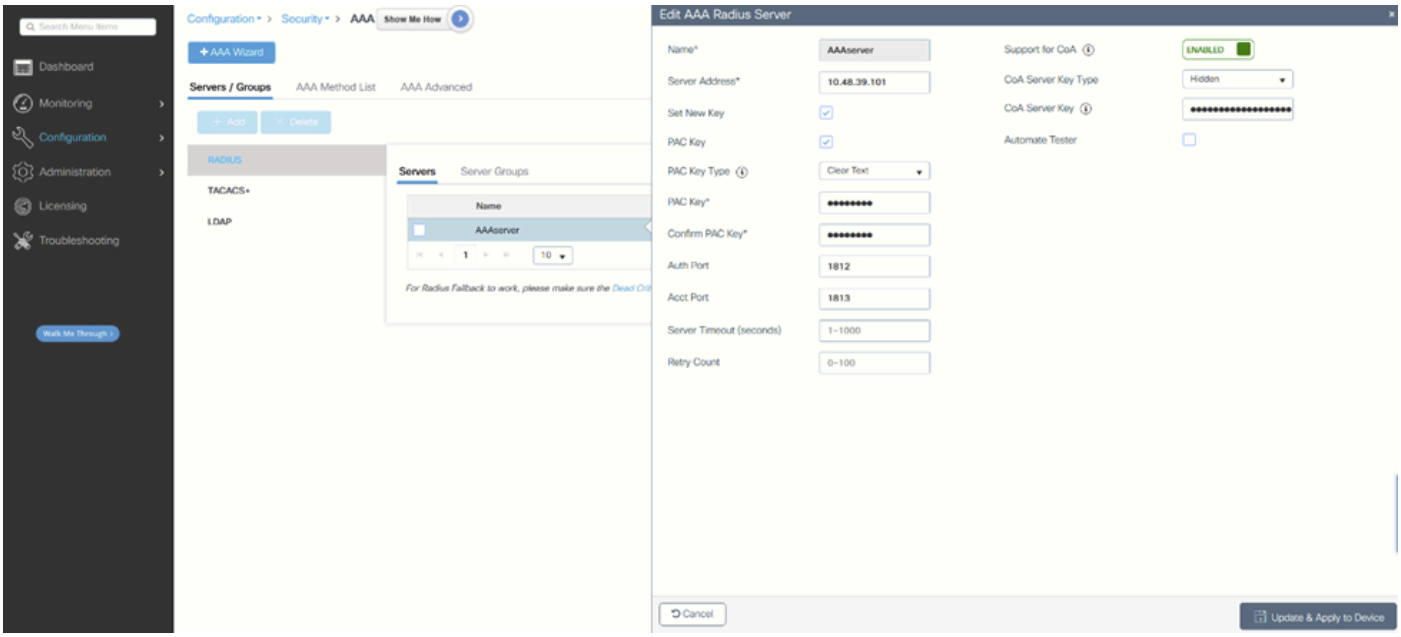
1. Voeg de AAA-server toe aan de WLC vanuit Configuratie > Beveiliging > AAA:



WLC AAA-pagina

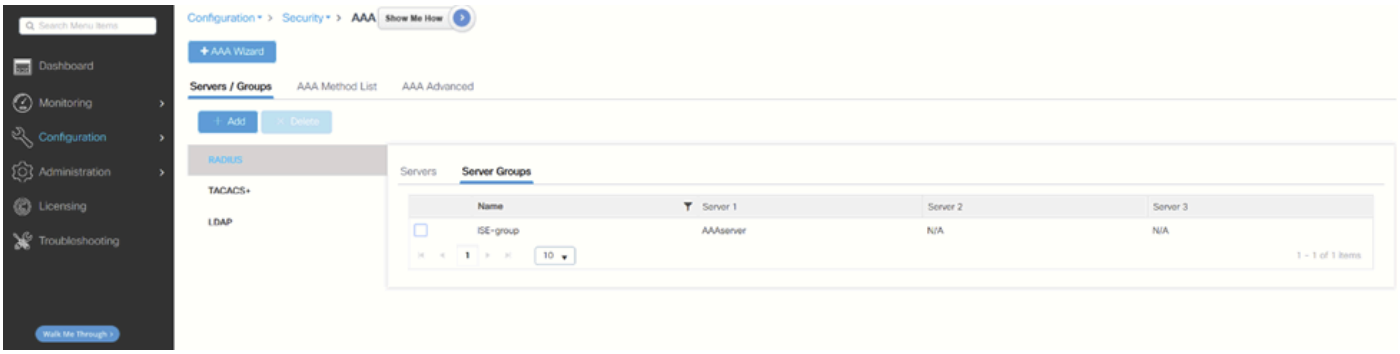
2. Zorg ervoor dat de belangrijkste items hier overeenkomen met de sleutel wanneer u het

apparaat toevoegt op ISE. Schakel Ondersteuning voor CoA in en voeg de sleutel toe als u CoA wilt gebruiken voor het downloaden van de configuratie-updates:



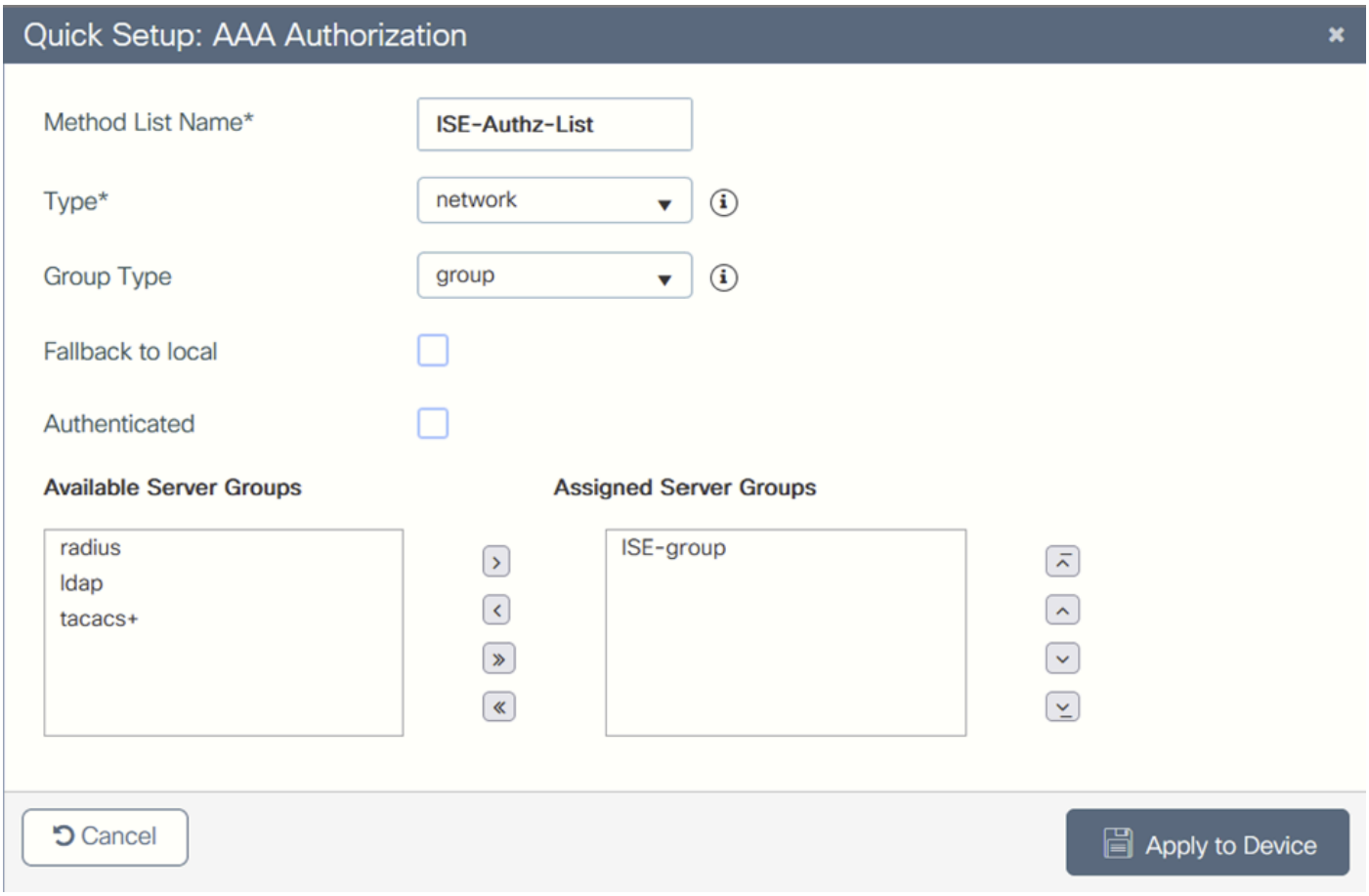
WLC AAA-server toevoegen

3. Maak de servergroep aan:

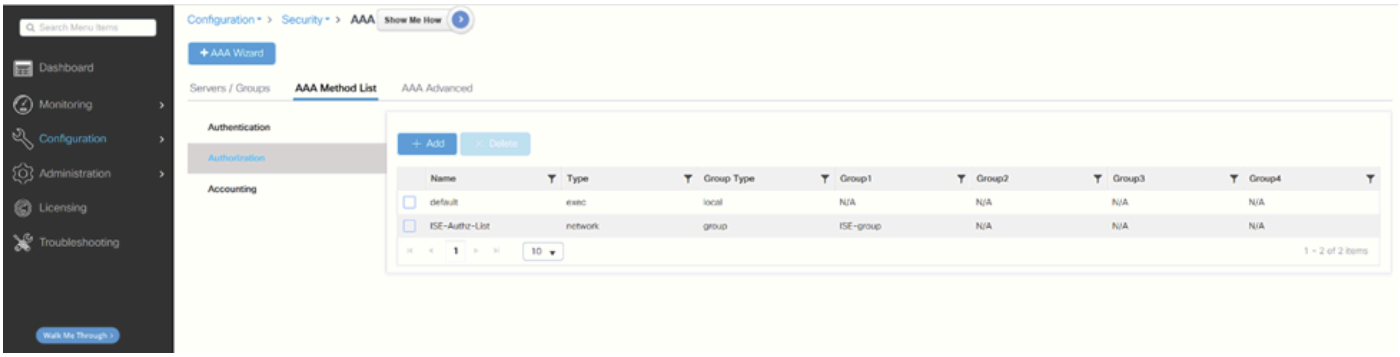


WLC-servergroep toevoegen

4. Voeg de lijst van autorisatiemethoden toe met het type netwerk:



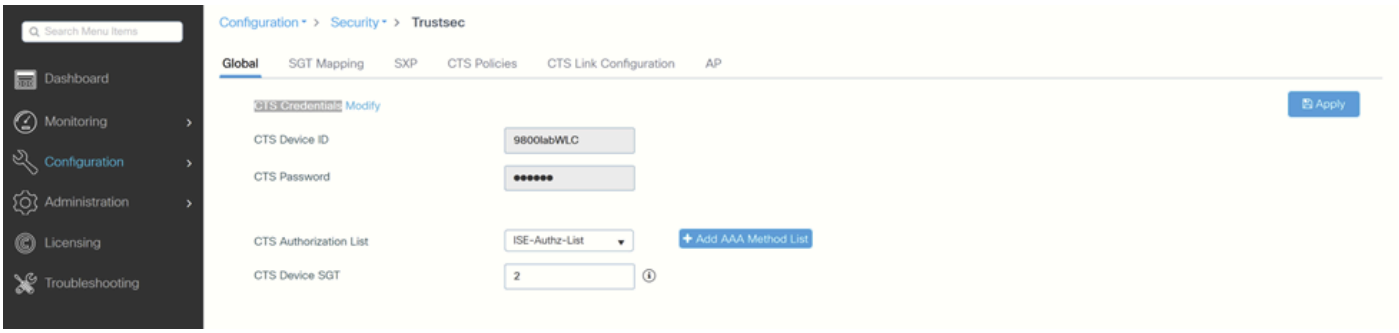
autorisatiemethode



WLC AAA-servergroep

5. Navigeer naar Configuratie > Beveiliging > Trustsec en configureer de CTS Device ID en CTS Password, u gaat deze vermeldingen gebruiken bij het toevoegen van het apparaat aan ISE.

Configureer ook de CTS-autorisatielijst die u in stap 4 hebt gemaakt:

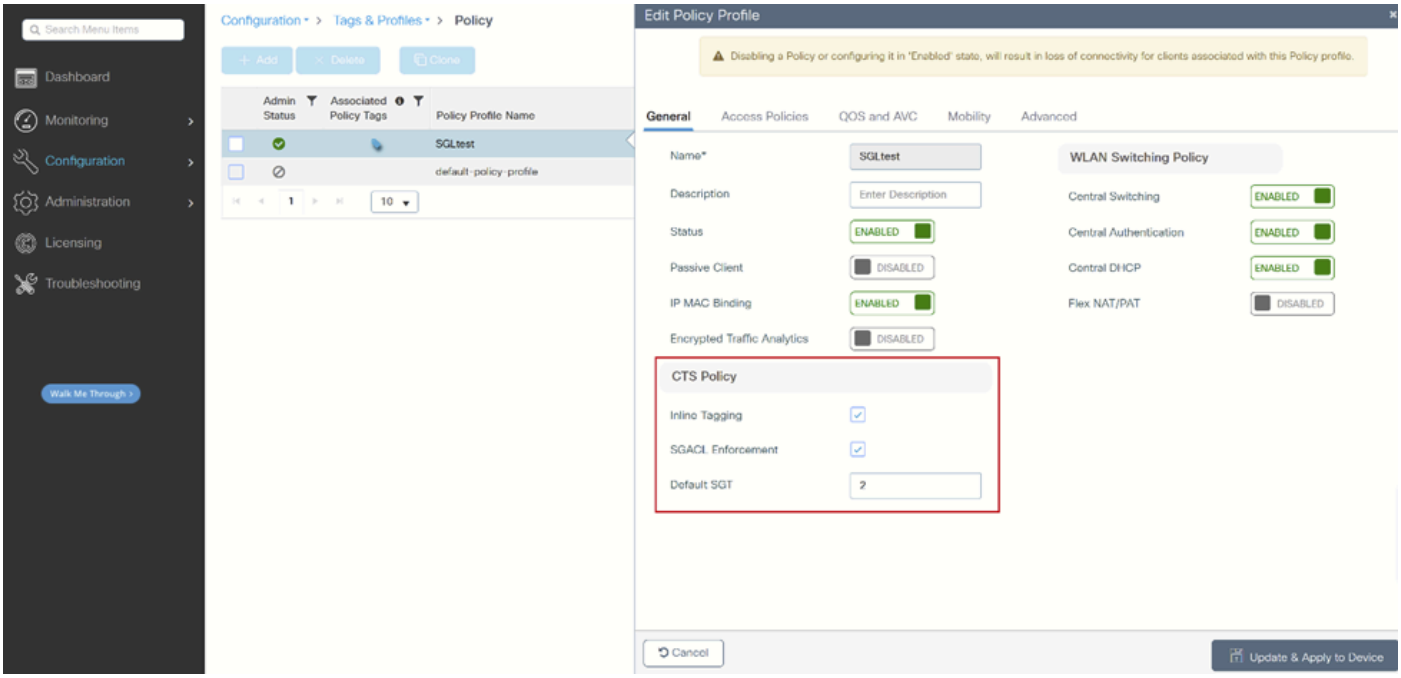


WLC TrustSec

6. In dit voorbeeld is het WLAN al gemaakt en zijn de verificatie-instellingen al geconfigureerd.

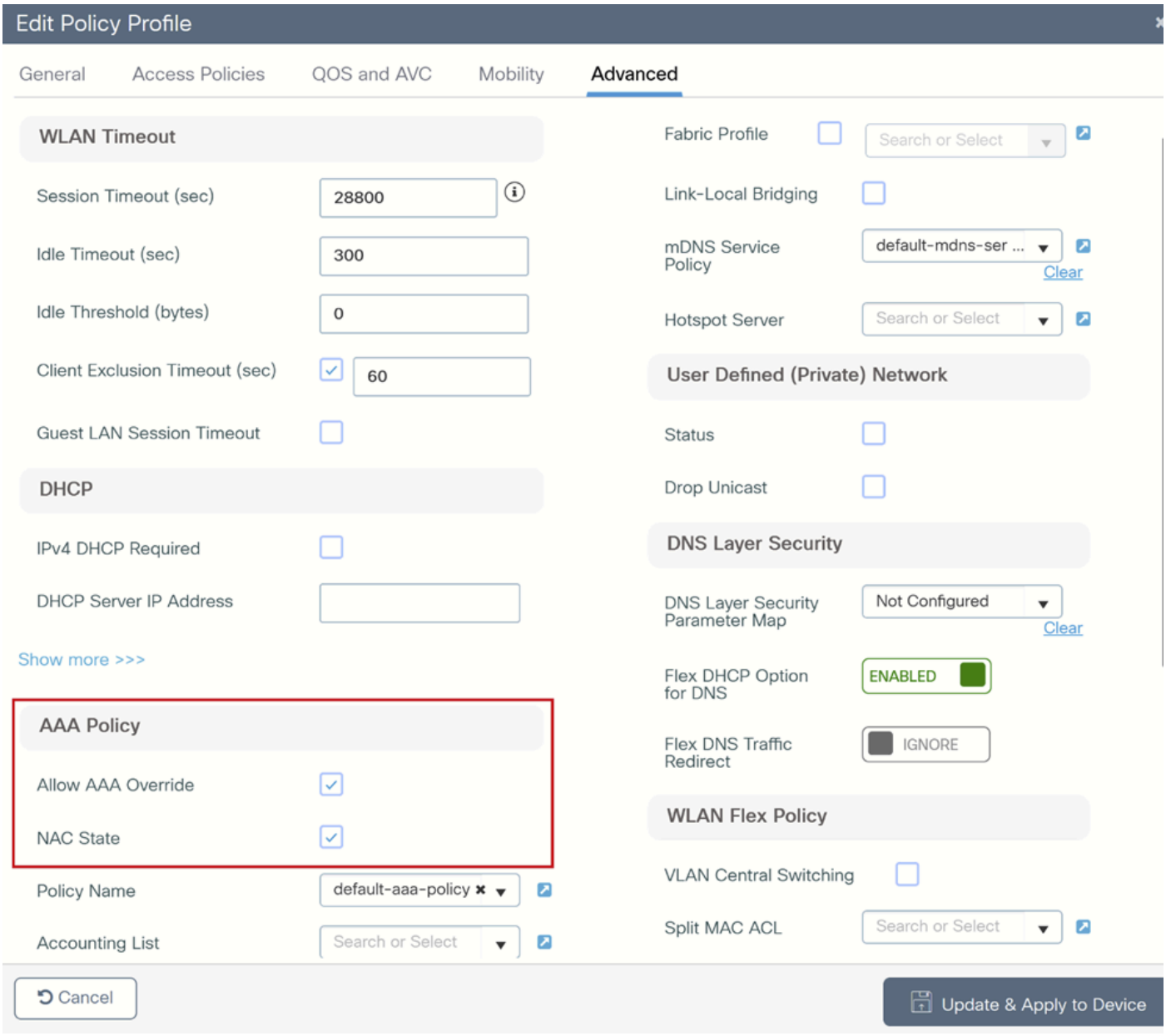
Navigeer nu naar het beleidsprofiel waarop u SGT's wilt gebruiken.

i. Onder CTS-beleid, Inline tagging en SGACL-handhaving inschakelen, kunt u ook de standaard SGT opgeven. Standaard SGT 2 wordt gebruikt voor dit lab als voorbeeld:



WLC-beleidsprofiel

ii. Schakel onder het tabblad Geavanceerd de optie AAA-overschrijving toestaan en de NAC-status in:



tabblad Geavanceerd van WLC-beleidsprofiel

Vanuit de 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>
```

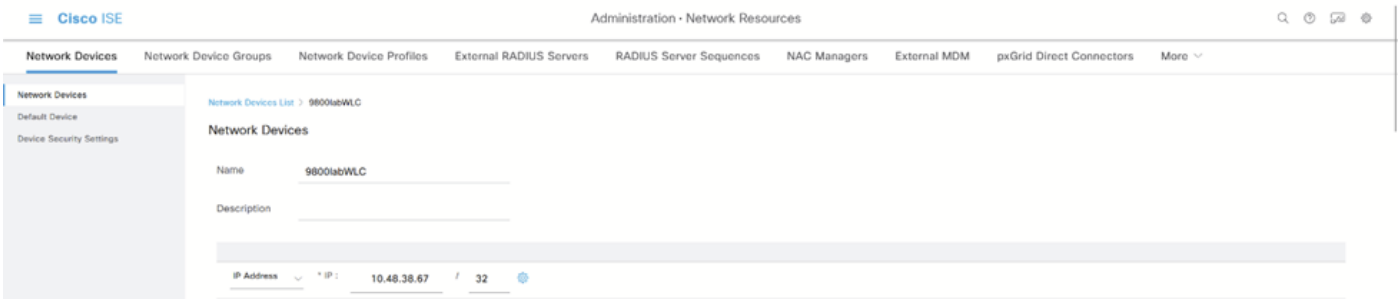
```
(config)# wireless profile policy <policy_profile_name>
(config-wireless-policy)# shut
(config-wireless-policy)# aaa-override
(config-wireless-policy)# cts inline-tagging
(config-wireless-policy)# cts role-based enforcement
(config-wireless-policy)# cts sgt <number>
(config-wireless-policy)# no shut

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

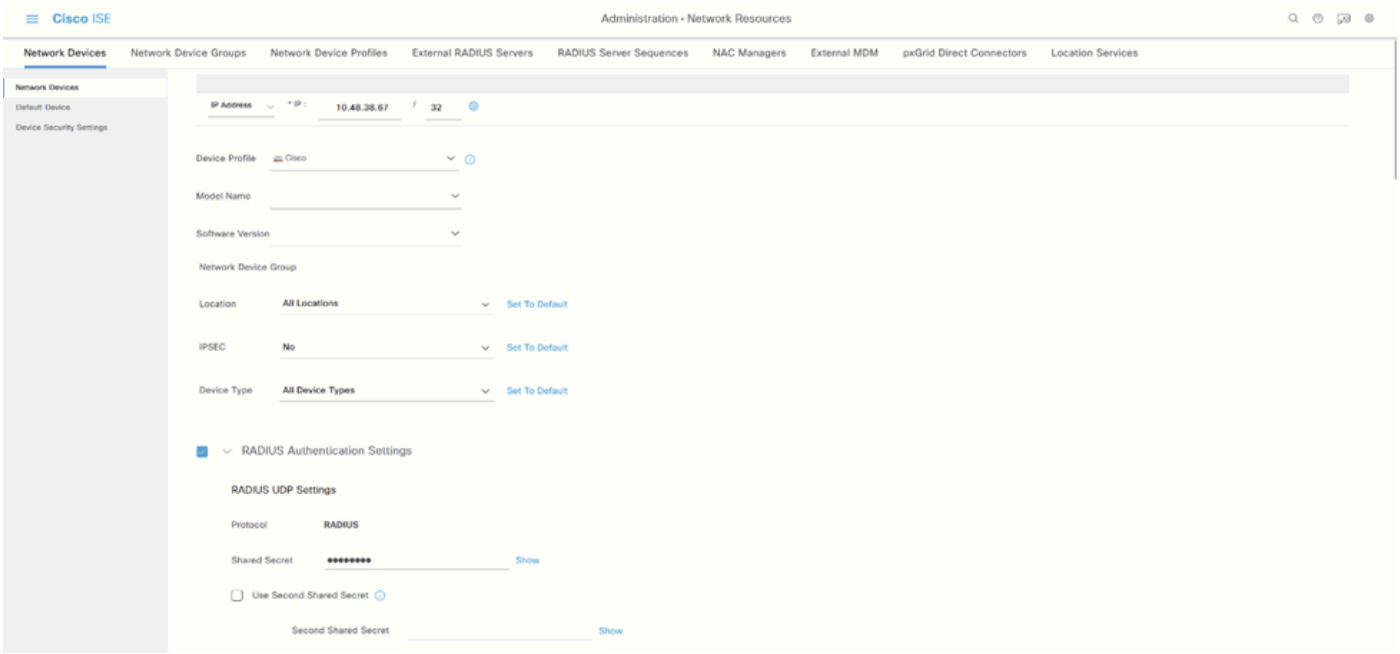
ISE-configuratie

1. Ga naar Beheer > Netwerkbronnen > Netwerkapparaten.

i. Voeg hier de WLC-informatie toe:

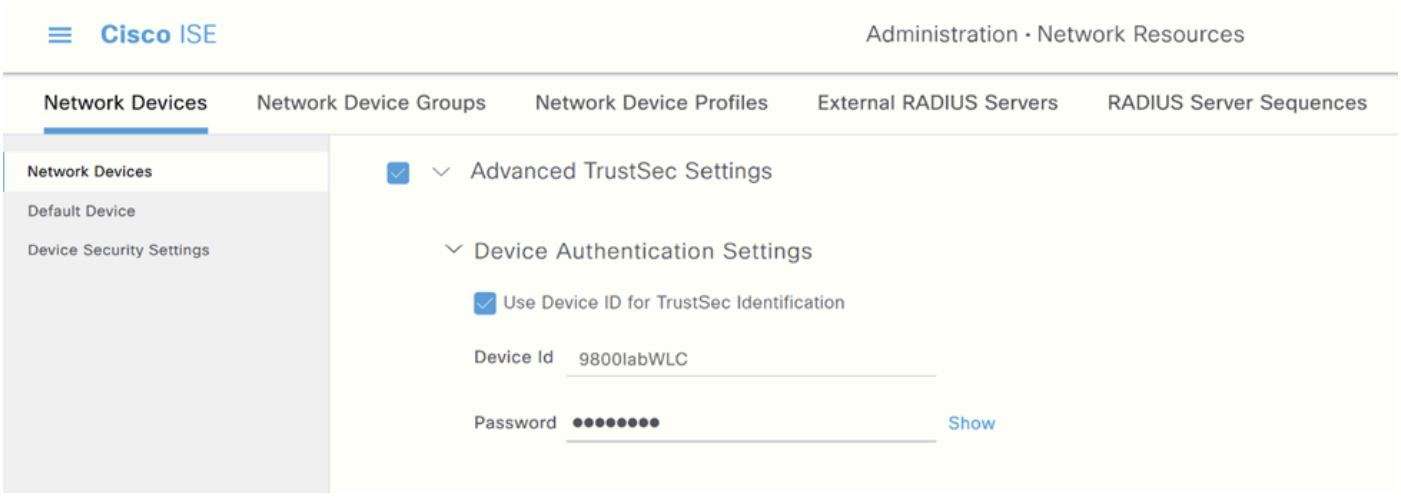


ISE-pagina Netwerkapparaten



ISE WLC RADIUS-info toevoegen

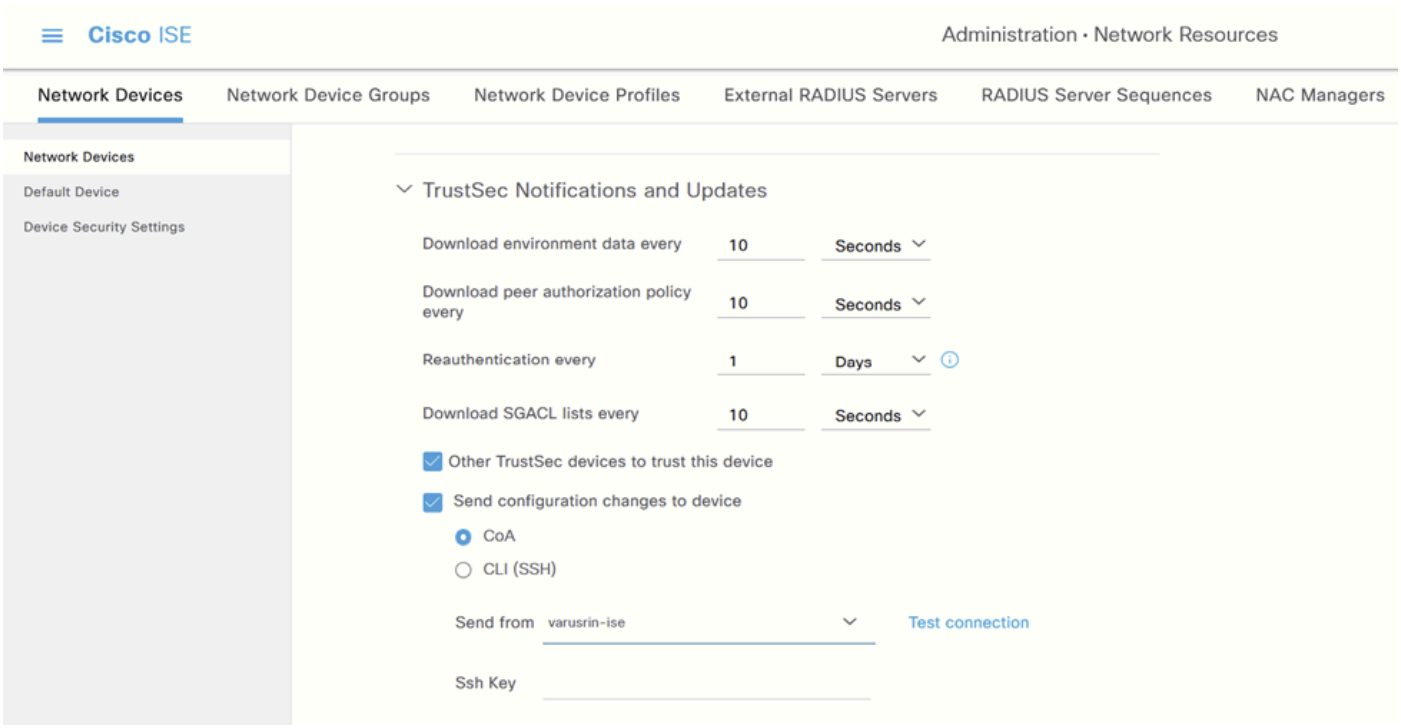
ii. Blader omlaag en configureer Geavanceerde TrustSec-instellingen, schakel het selectievakje Apparaat-ID gebruiken voor TrustSec-identificatie in en configureer het wachtwoord:



Geavanceerde TrustSec-instellingen

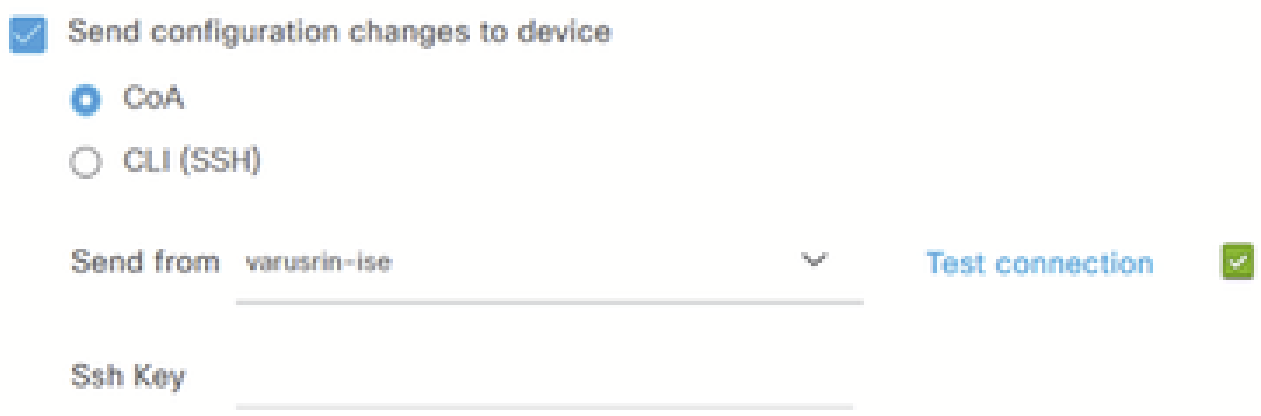
Dit moet overeenkomen met de configuratie aan de WLC-zijde in stap 6 van de WLC-configuratie.

iii. Blader omlaag naar TrustSec-meldingen en -updates en configureer of u CoA of SSH wilt gebruiken voor configuratie-updates. Selecteer het gewenste ISE-knooppunt:



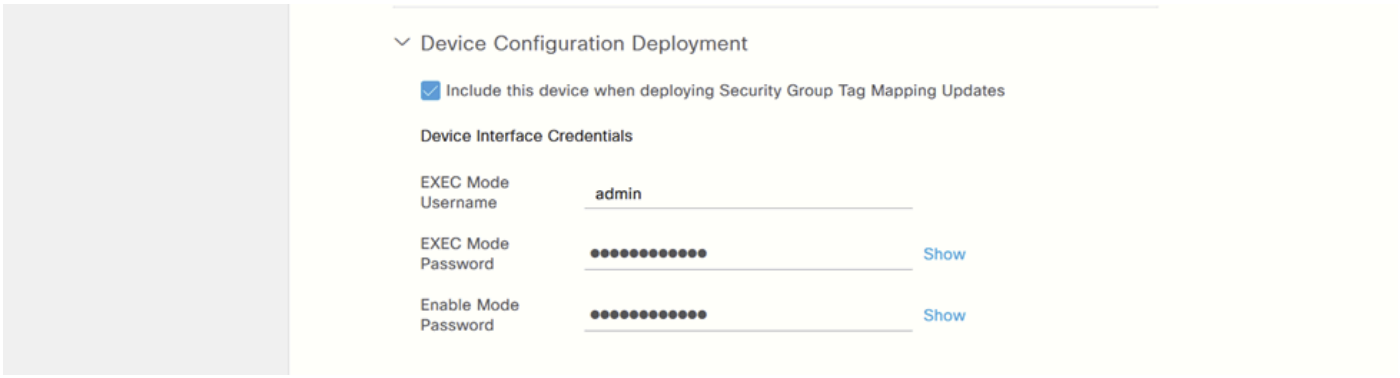
Meldingen en updates van TrustSec

2. Druk op Testverbinding om er zeker van te zijn dat de verbinding tot stand is gebracht. Wanneer het succesvol is, zal het een groene teek laten zien:



Verbinding testen

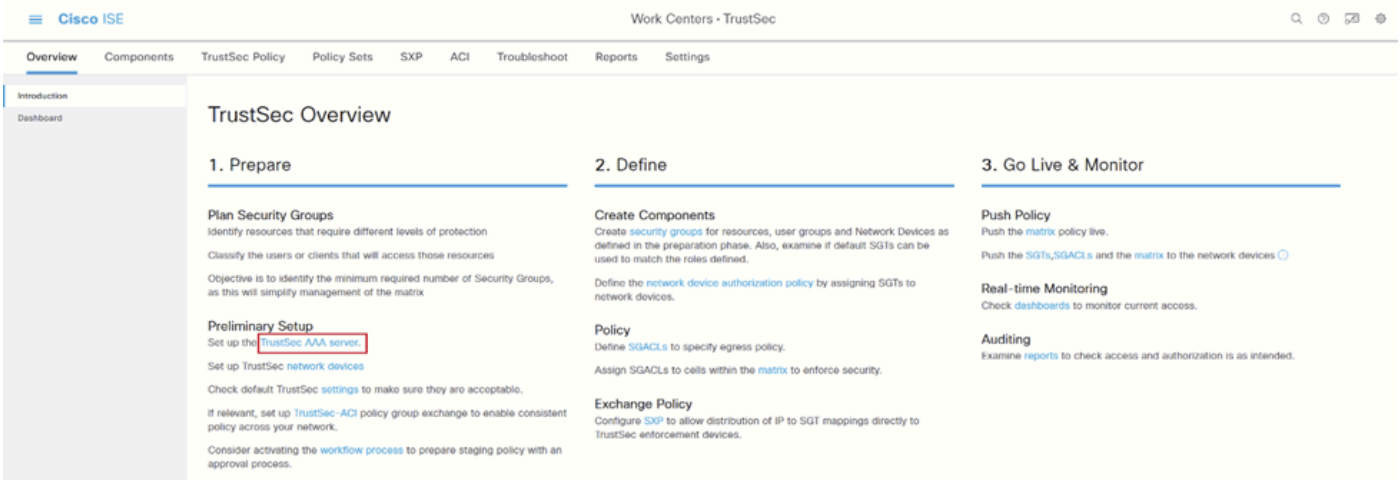
i. Scroll naar beneden en configureer de WLC die moet worden opgenomen bij het implementeren van SGT-toewijzingsupdates, dit is belangrijk als u de SSH-optie selecteert in de vorige stap:



Implementatie van apparaatconfiguratie

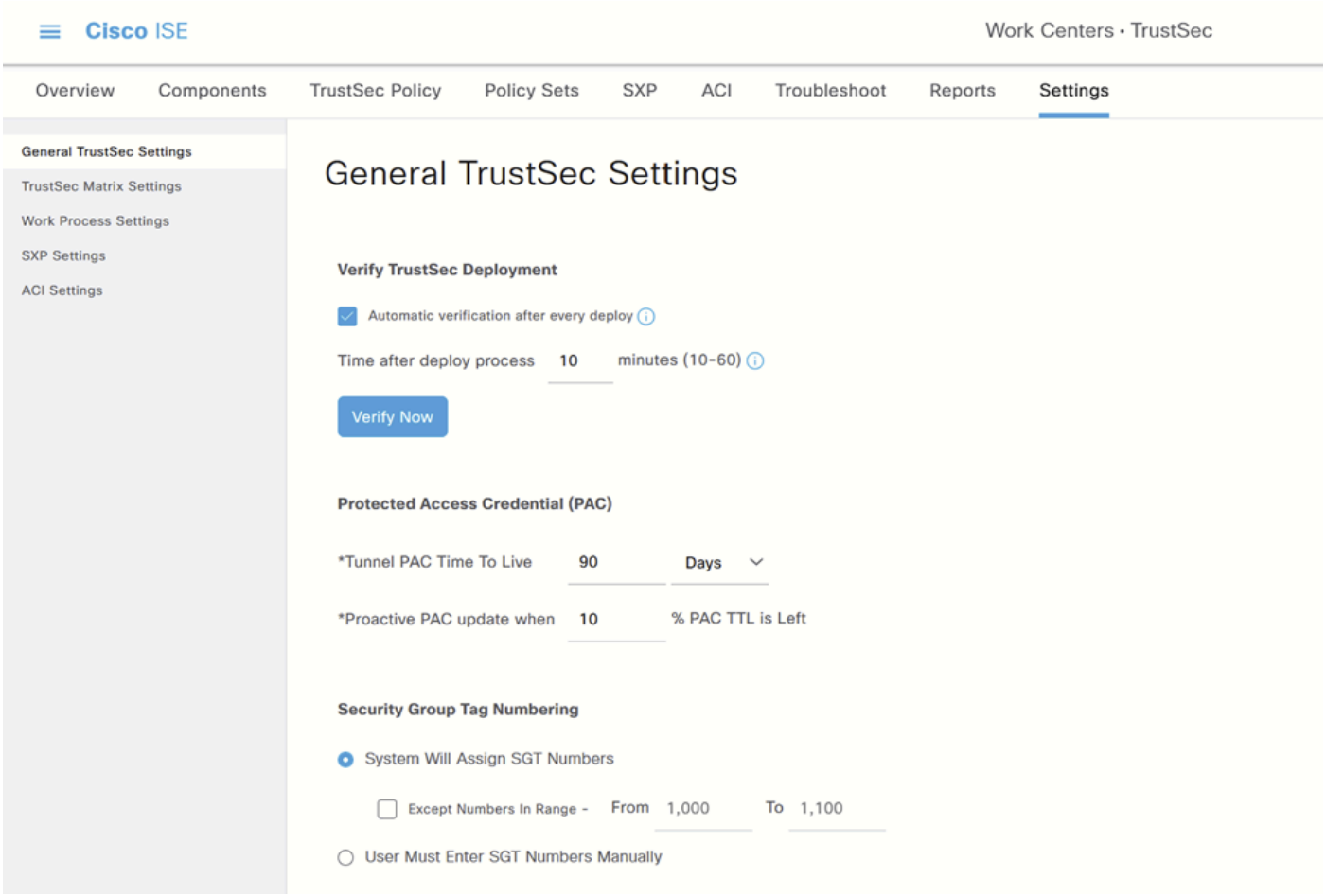
ii. De configuratie opslaan.

3. Vanuit Work Centers > TrustSec > Overzicht hebt u de configuratieopties van TrustSec. Kies TrustSec AAA Server om de gebruikte ISE-instantie te bekijken. Raadpleeg het Cisco Catalyst Wireless Group Based Policy voor meer informatie over welk exemplaar wordt gebruikt als u meerdere exemplaren hebt.



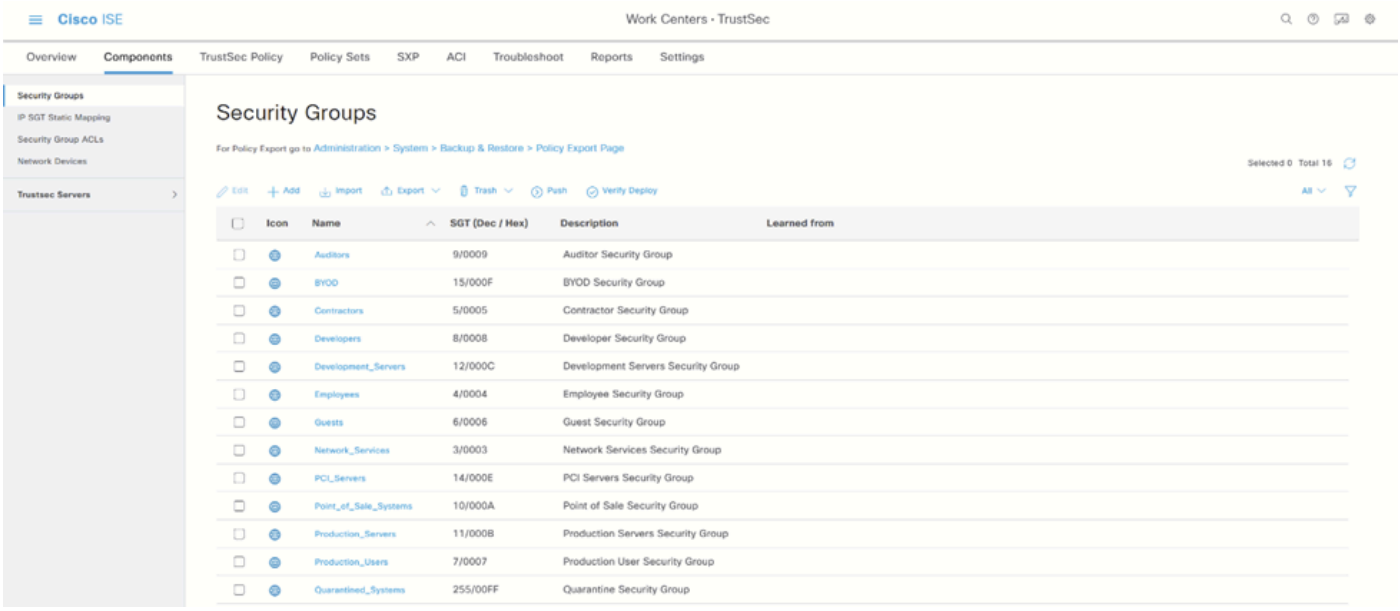
Overzicht van ISE TrustSec

4. (Optioneel) Navigeer naar het tabblad Instellingen, schakel Automatische verificatie in na elke implementatie indien gewenst.



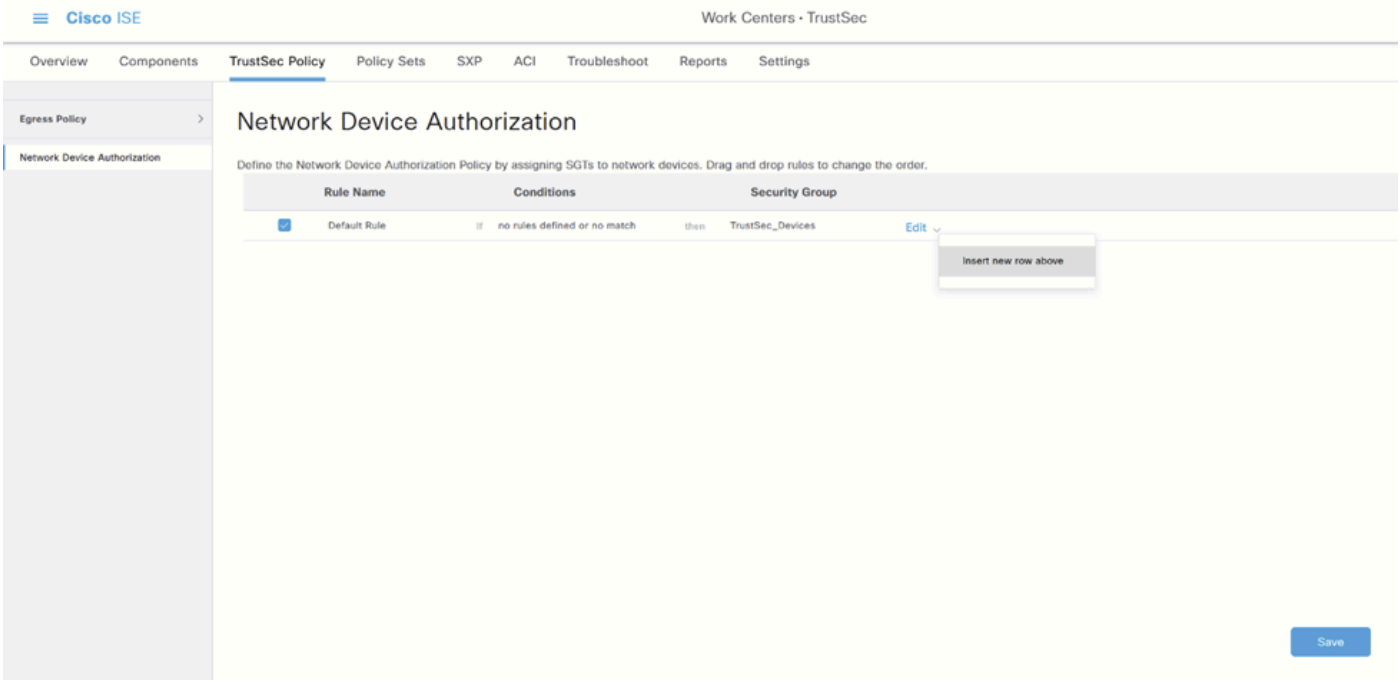
ISE TrustSec-instellingen

5. Voeg de SGT-waarden toe of bewerk deze vanuit Work Centers > TrustSec > Componenten > Beveiligingsgroepen, afhankelijk van uw behoeften:



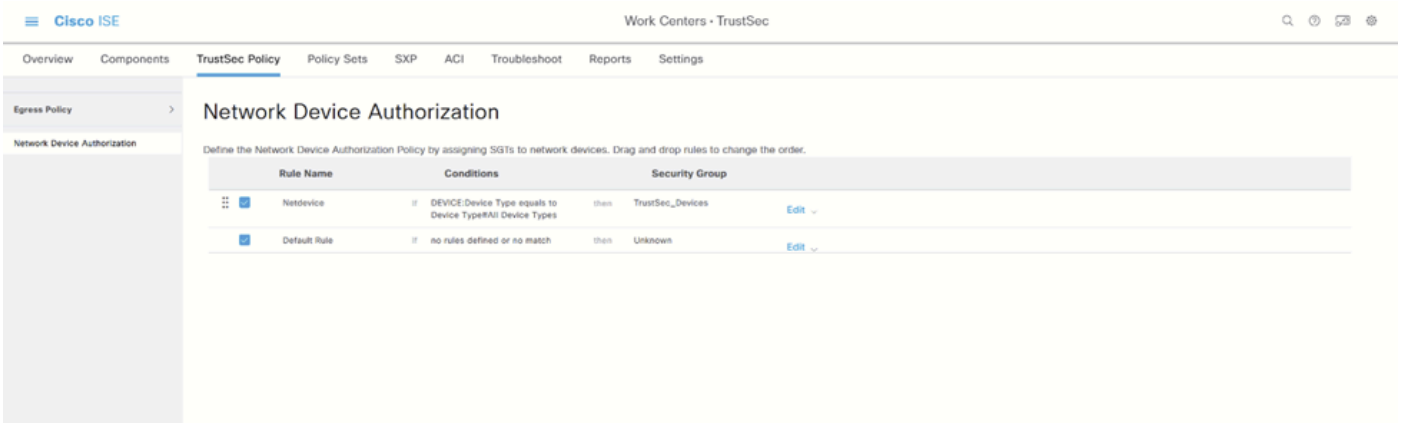
ISE-beveiligingsgroepen

6. Als u het machtigingsbeleid wilt opgeven, gaat u naar Werkcentra > TrustSec > TrustSec-beleid > Machtiging netwerkapparaat:



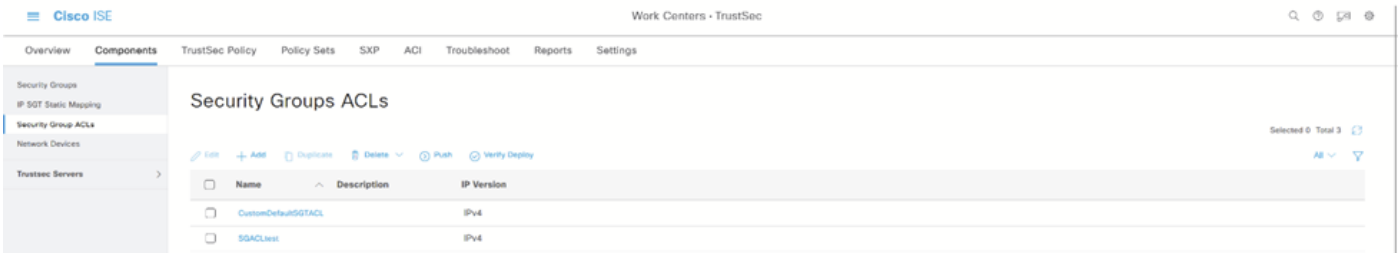
TrustSec-beleid

U kunt de standaard behouden, maar voor dit lab gebruiken we deze configuratie als voorbeeld:



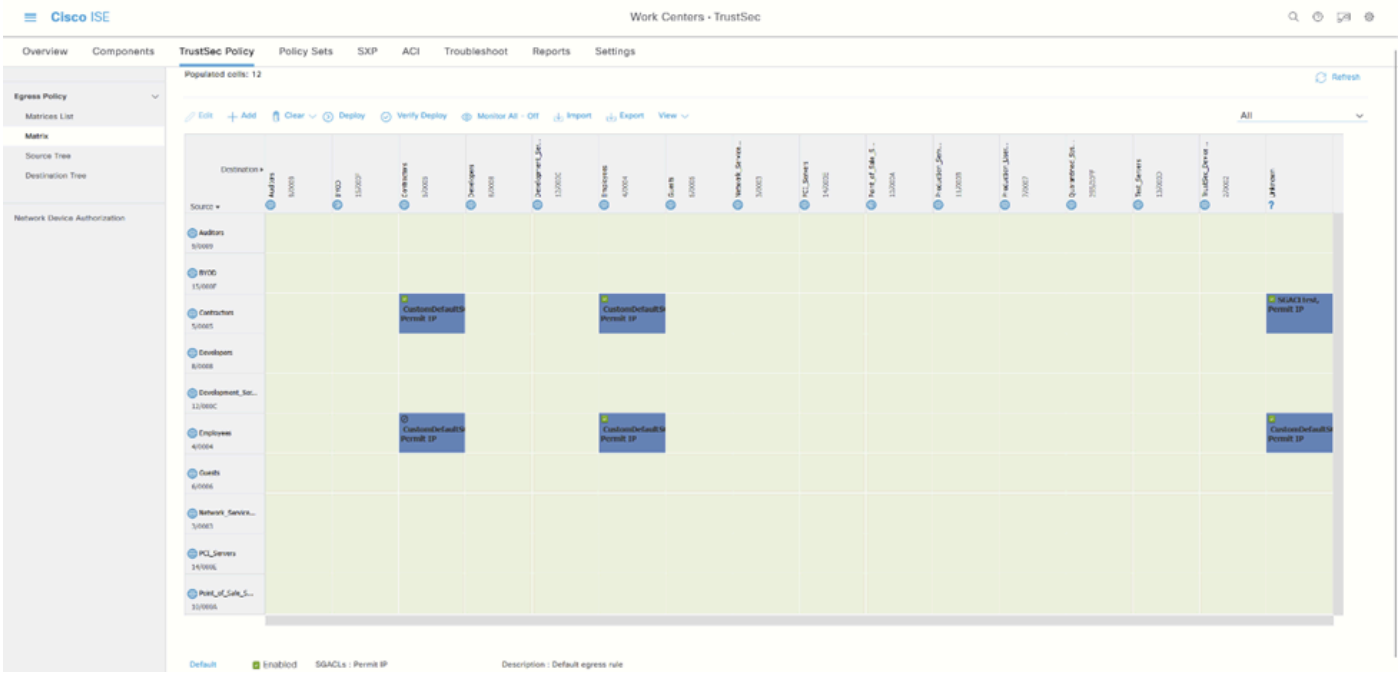
Network Device Authorization

7. Maak de SGACL aan onder het tabblad Componenten en vervolgens onder ACL's van de beveiligingsgroep:



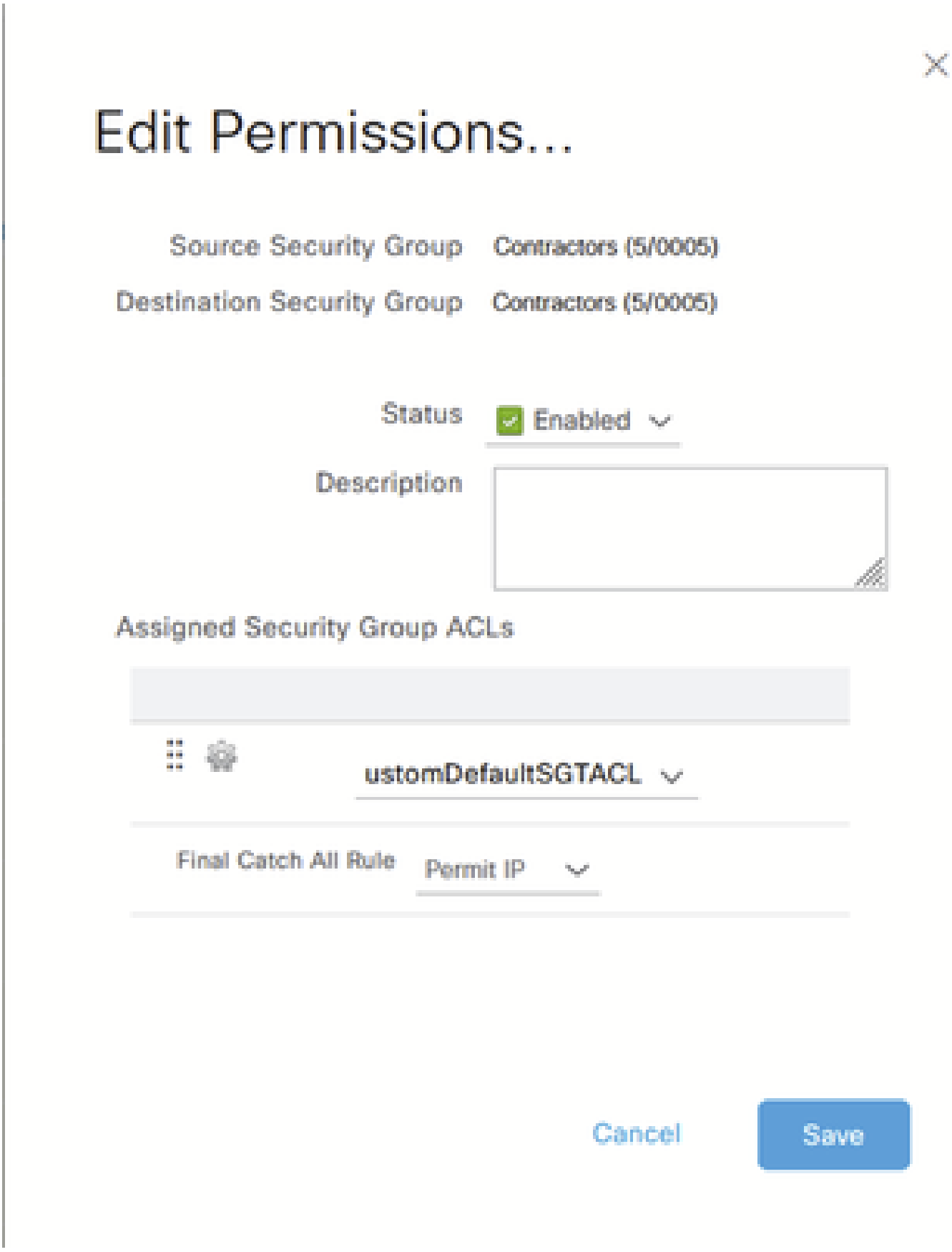
ACL's van de beveiligingsgroep

8. Geef de matrixitems op onder het tabblad Beleid voor TrustSec en vervolgens onder Matrix. U kunt de machtigingen bewerken door te klikken op het punt waar twee SGT's samenkomen:

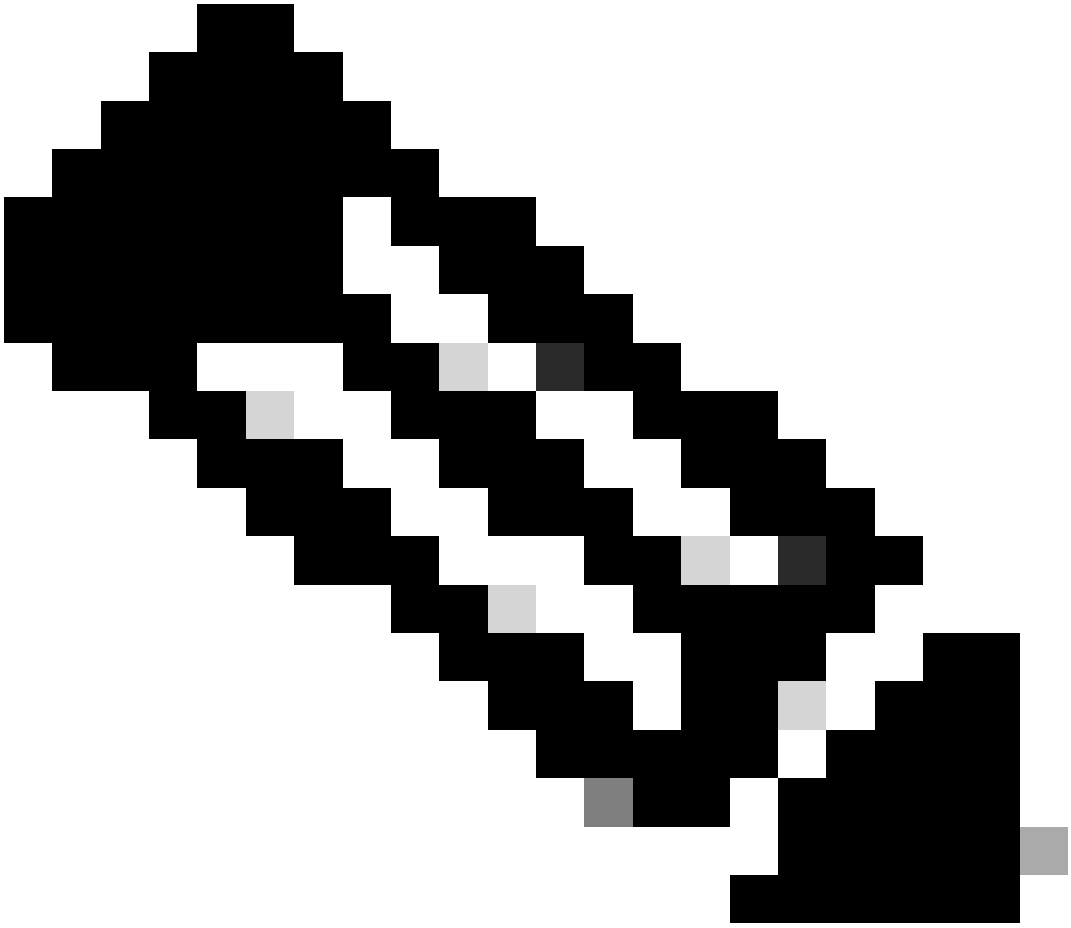


ISE TrustSec-matrix

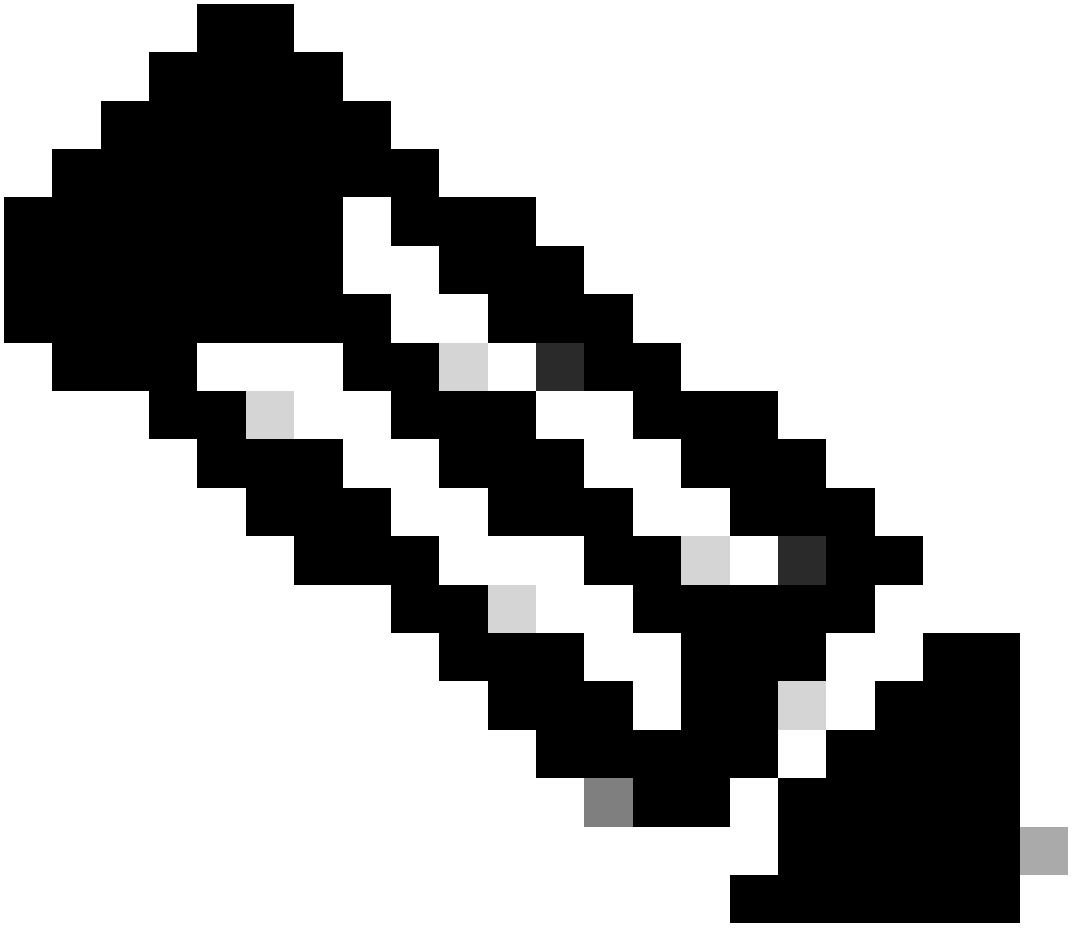
Voorbeeld:



Rechten bewerken



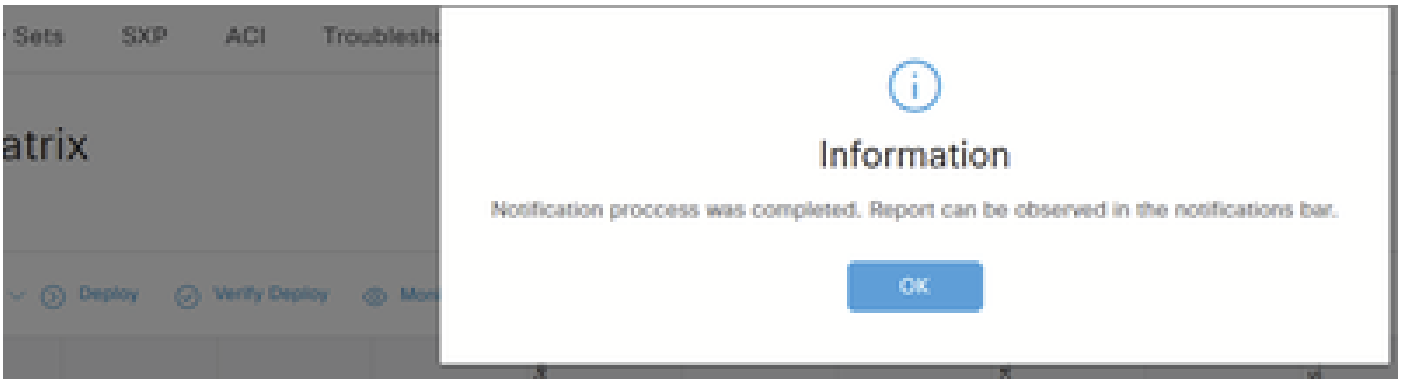
Opmerking: in het geval van het model Allow List moet u expliciet toestaan dat het DHCP-protocol voor de clientapparaten het DHCP-IP-adres ophaalt en vervolgens de controller om SGACL-beleid vragen.



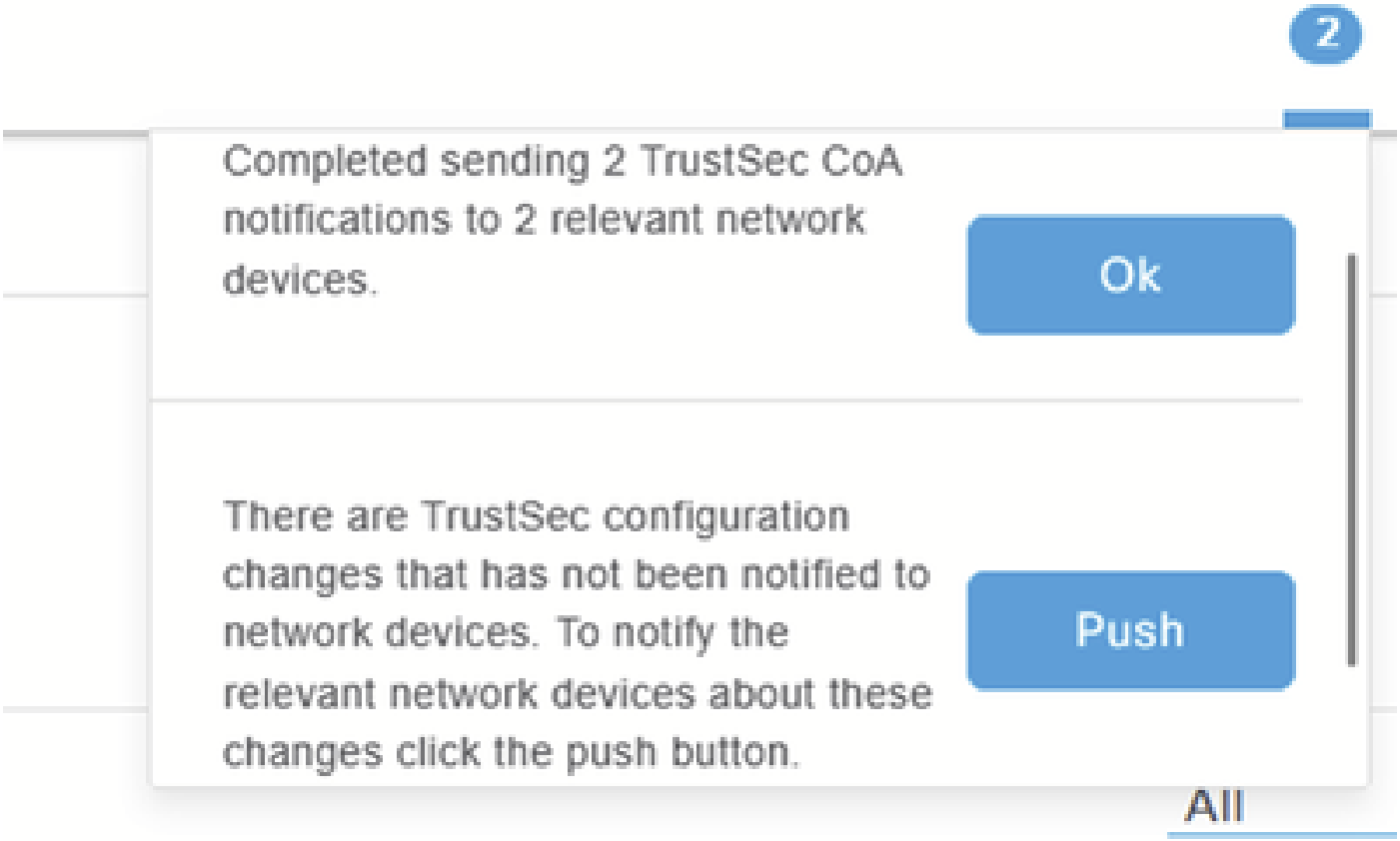
Opmerking: clients ontvangen geen SGT-waarde en DHCP-clients ontvangen een APIPA-adres (Automatic Private IP Addressing) wanneer het beleid van TrustSec "onbekend tot onbekend" wordt geweigerd in de TrustSec-matrix.
Klanten ontvangen de juiste SGT-waarden en DHCP-clients ontvangen een IP-adres wanneer het beleid van TrustSec "onbekend tot onbekend" is toegestaan in de TrustSec-matrix.

---

9. Klik op Implementeren. Wat zal resulteren in deze berichten en meldingen:



Implementeren

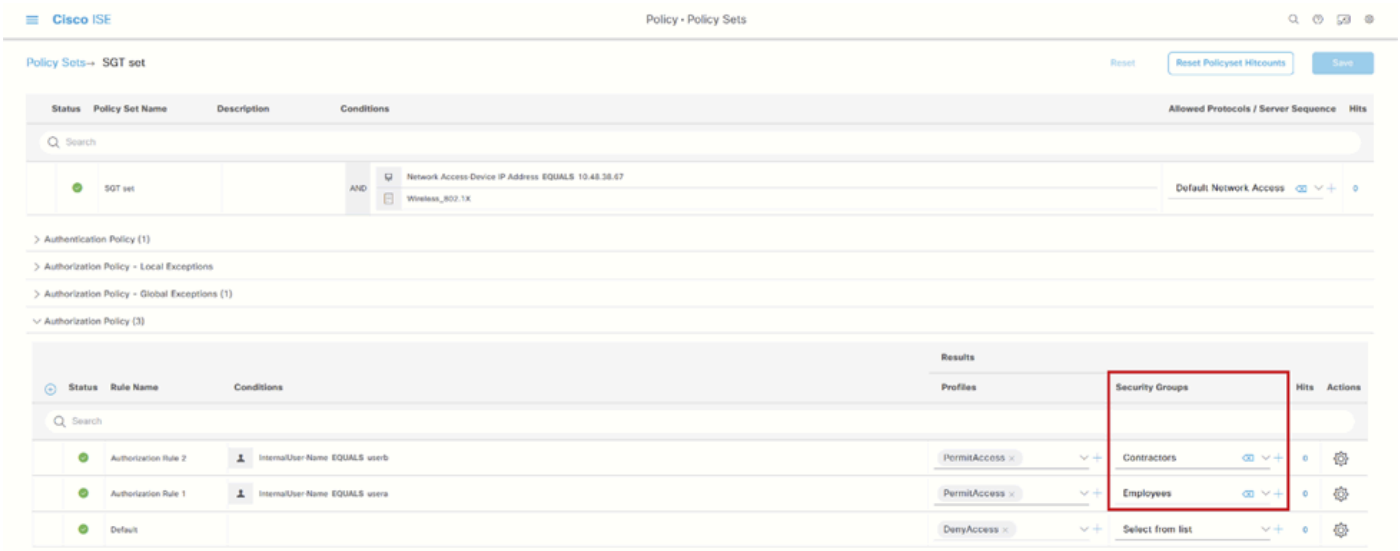


Meldingen implementeren

10. Navigeer naar de beleidsset die voor het WLAN wordt gebruikt onder Beleid > Beleidssets:

ISE-beleidssets

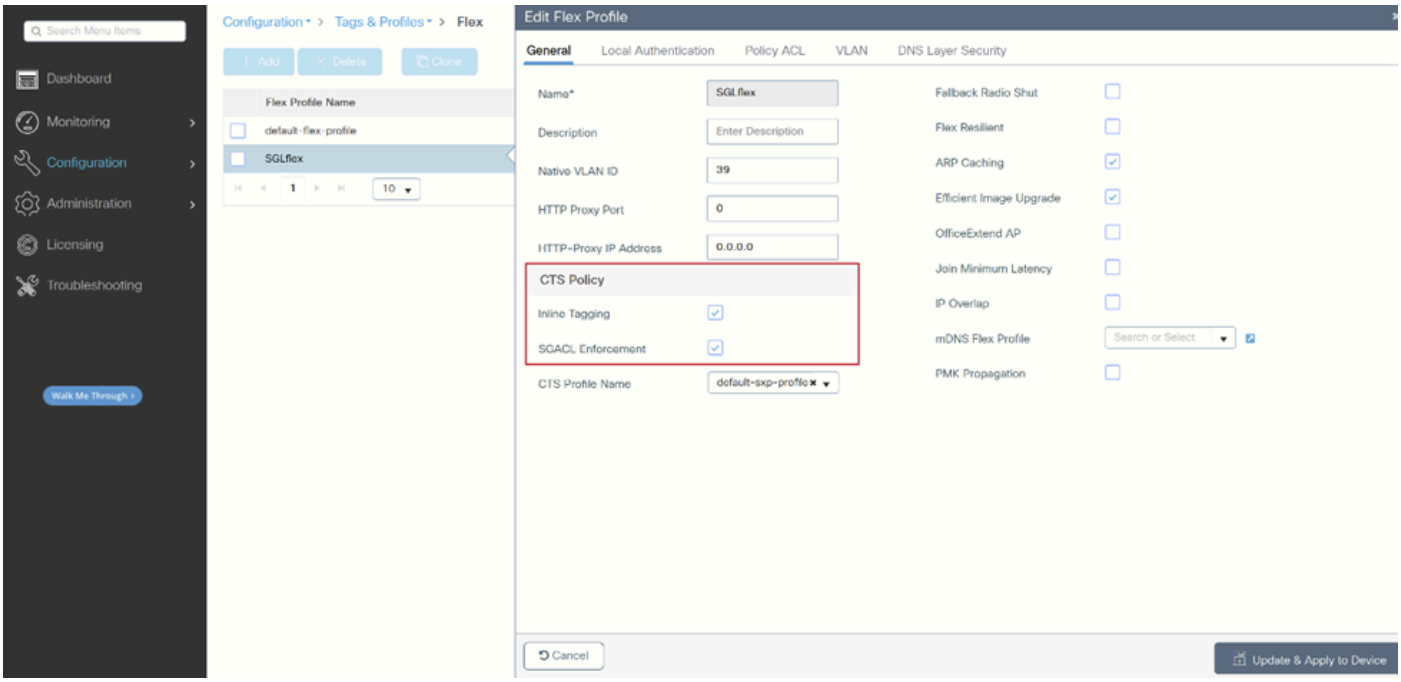
In dit lab definiëren we de SGT per gebruiker, selecteer het veld SGT onder Beveiligingsgroepen:



ISE-beveiligingsgroepen

FlexConnect

Inline tagging en SGACL-handhaving inschakelen op het Flex-profiel onder Configuratie > Tags en beleidsregels > Flex:



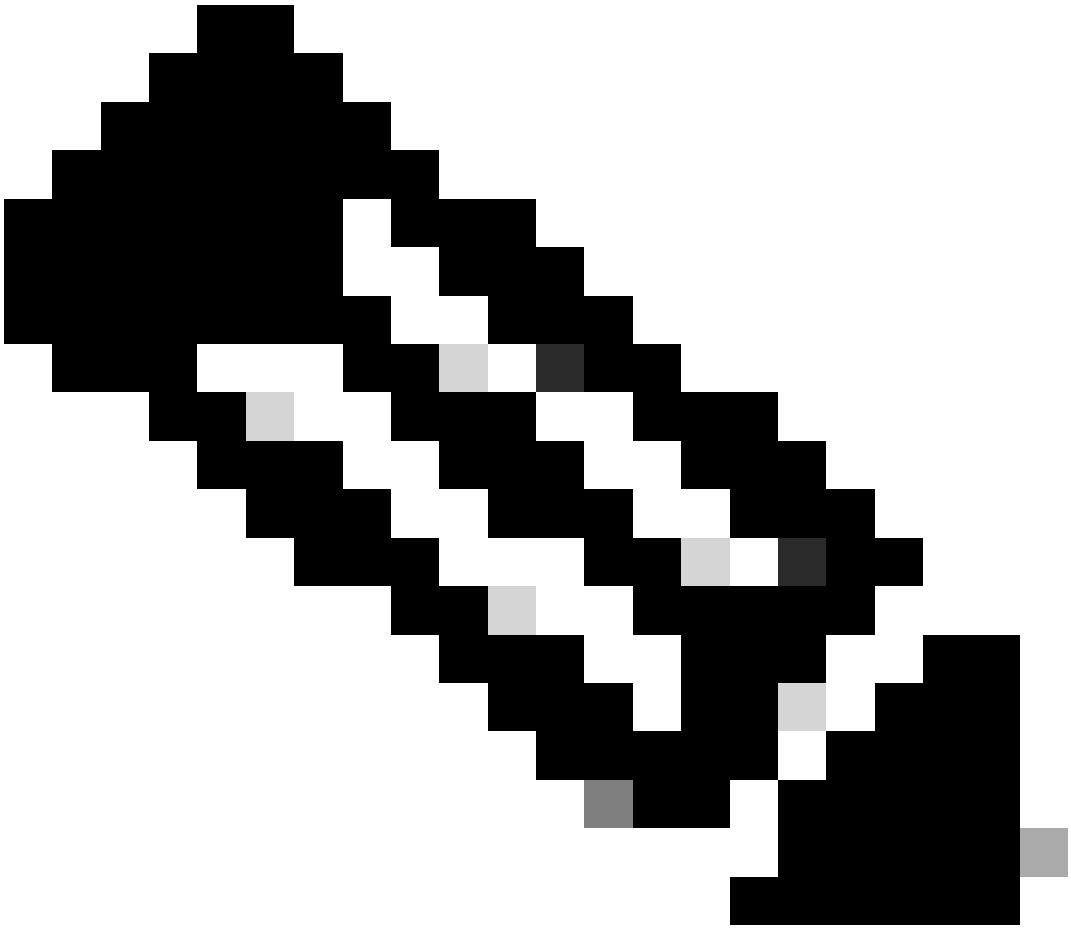
WLC Flex-profiel

Vanuit de CLI:

```
# configure terminal

(config)# wireless profile flex SGLflex
```

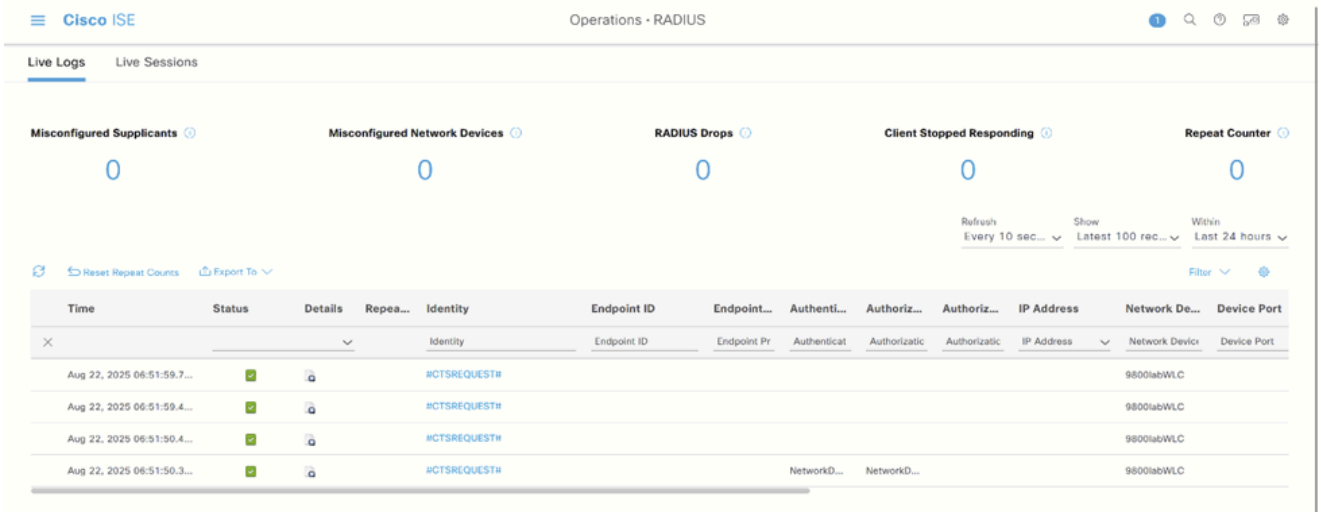
```
(config-wireless-flex-profile)# cts inline-tagging
(config-wireless-flex-profile)# cts role-based enforcement
```



Opmerking: als de WLC zich in HA-SSO bevindt, wordt SGACL op FlexConnect-toegangspunten niet ondersteund. Cisco bug ID CSCwn85468. Dit wordt toegevoegd in 17.19.

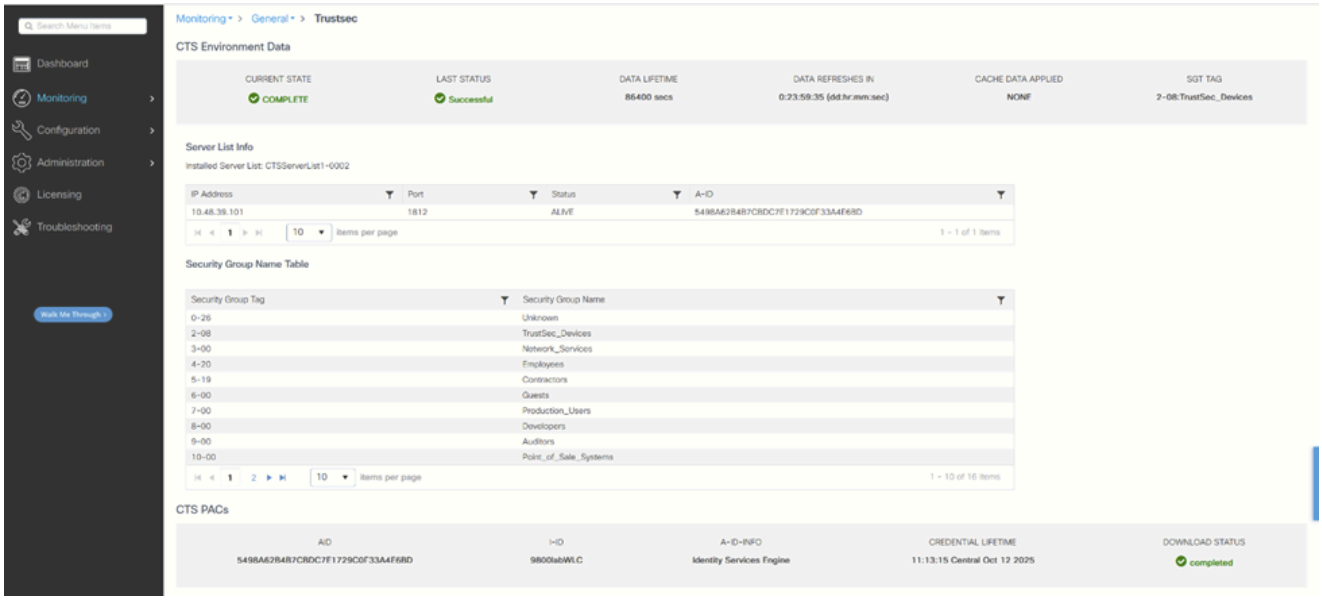
Verifiëren

1. Vanuit ISE moet u een succesvol CTS-verzoek zien onder Bewerkingen > RADIUS > Live Logs:



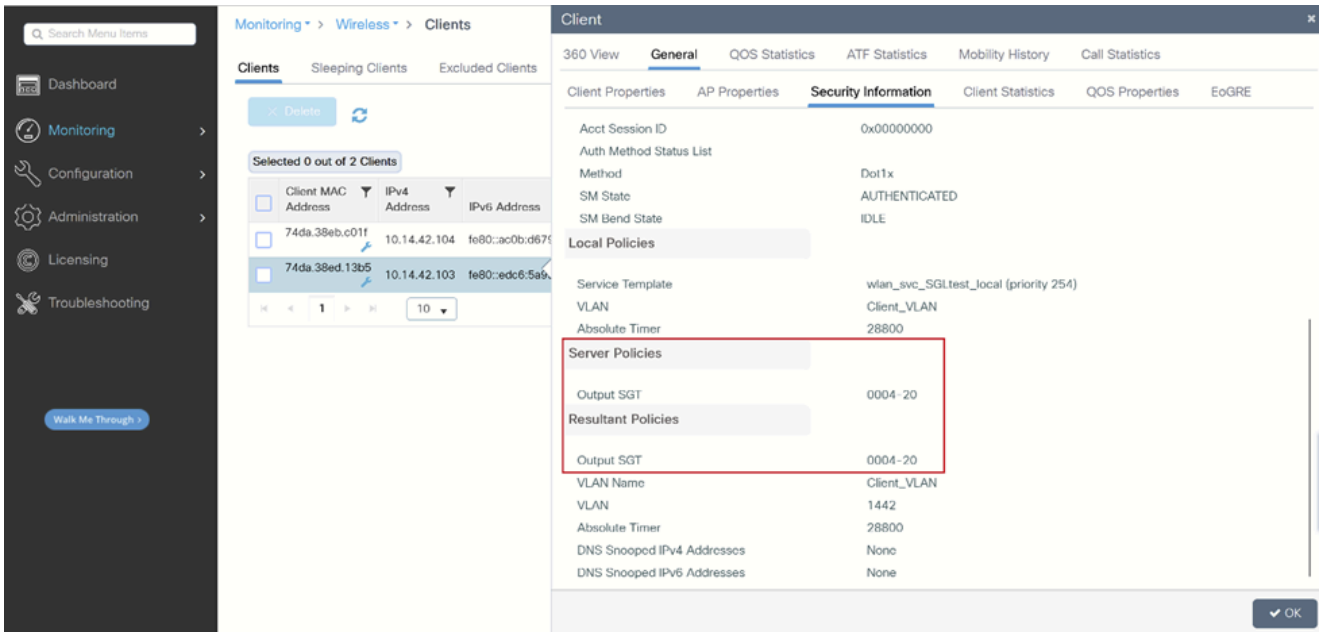
Live-logs van ISE RADIUS

2. U kunt controleren of de verbinding tot stand is gebracht en of de SGT's zijn gedownload van Monitoring > Algemeen > Trustsec op de WLC:



WLC TrustSec-bewaking

3. Wanneer u verbinding maakt met een client, wordt de toegewezen SGT zichtbaar onder Bewaken > Draadloos > Cliënten, kiest u de client die u wilt controleren en navigeert u naar Algemeen > Beveiligingsinformatie tabblad:



WLC-clientbewaking

Vanuit de CLI:

- Voordat u de client aansluit, is dit wat u gaat zien van de WLC-uitvoer:
  Alleen de machtigingen met betrekking tot onbekende SGT's worden weergegeven.

```
<#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
```

- Bij het verbinden van de client kunt u deze logs observeren vanuit de RA-sporen, de SGT wordt toegepast vanuit 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
```

- Gebruik de opdracht draadloos client-mac-adres <client_MAC_address> detail van CLI, die de SGT toont die aan de client is toegewezen:

<#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
…
```

- Nadat u één client in SGT 4 hebt verbonden, zult u merken dat de machtigingen voor SGT 4 nu worden weergegeven:
  De machtigingen worden toegevoegd nadat de client is verbonden en een SGT is toegewezen.

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

- Na het verbinden van twee clients, één in SGT 4 en de andere 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
============================================================
```

- Nu kunt u zien dat de machtigingen van SGT 5 worden toegevoegd:

<#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
```

- De ACL's zullen er als "gedownload" uitzien op de 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
```

Lokale FlexConnect-switching

- Dit is de WLC-uitvoer voordat clients op het toegangspunt worden aangesloten:

<#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
```

- Vanuit de AP CLI is dit de uitvoer voor toegangsrechten voordat clients met het AP worden verbonden:

```
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
```

- Dit zijn de AP-foutmeldingen terwijl de client verbinding maakt om de stroom weer te geven:

<#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
…
```

- Van WLC CLI, bij het aansluiten van één client op 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
```

- Van AP CLI:
  U kunt hetzelfde zien, alleen machtigingen met betrekking tot SGT 4 worden toegevoegd.

```
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
```

- Vanaf WLC CLI, bij het aansluiten van de tweede client op 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
```

- Uitgangen toegangspunt:

```
<#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
```

Problemen oplossen

- Van WLC CLI:

CTS-provisioning weergeven

Op rollen gebaseerde CTS-machtigingen weergeven

IP-toegangslijsten weergeven

CTS AP SGT-Info <AP_NAME> weergeven

- Van AP:

CTS-rolgebaseerde SGT-map weergeven Alles

Op rollen gebaseerde CTS-machtigingen weergeven

CTS-toegangslijsten <ACL-name> weergeven

Op rollen gebaseerde CTS SGT-Map-samenvatting weergeven

CTS-toegangslijsten weergeven

FlexConnect-client weergeven

Op rollen gebaseerde CTS-tellers wissen

Op rollen gebaseerde CTS-tellers weergeven

- AP-debugs:

- Maakt foutopsporing op CTS-pakketniveau mogelijk:

debugplicht

term mon

- Om CAPWAP ACL-gebeurtenissen en informatie met betrekking tot de lading te controleren:

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

Foutopsporingsclient-ACL

Debug Capwap Client-payload

Fout bij foutopsporing van Capwap-client

foutopsporingsgegevens DOT11-clientbeheer

Foutopsporingsdot11-clientbeheer kritiek

Fout in foutopsporing DOT11-clientbeheer

Foutopsporingsgebeurtenissen voor DOT11-clientbeheer

Foutopsporing Generieke datapath client_ip_table/debug_acl

Foutopsporing Generieke DataPath Client_IP_Table/Foutopsporing

Debug Generieke Datapath SGACL/Debug

Debug Generieke Datapath sgacl/debug_sgt

Debug Generieke DataPath SGACL/Debug_Protocol

Debug Generieke DataPath sgacl/debug_permission

term mon

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.