Konfiguration und Überprüfung von SGACL auf Catalyst 9800 WLC- und ISE-Server

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie TrustSec auf dem Catalyst 9800 und ISE-Server für die Verwendung der SGACL-Funktion mit lokalen und FlexConnect-Modus-APs konfiguriert wird.

Voraussetzungen

Anforderungen

Kenntnis der Grundlagen von Cisco 9800 WLC, Cisco ISE, FlexConnect und TrustSec

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

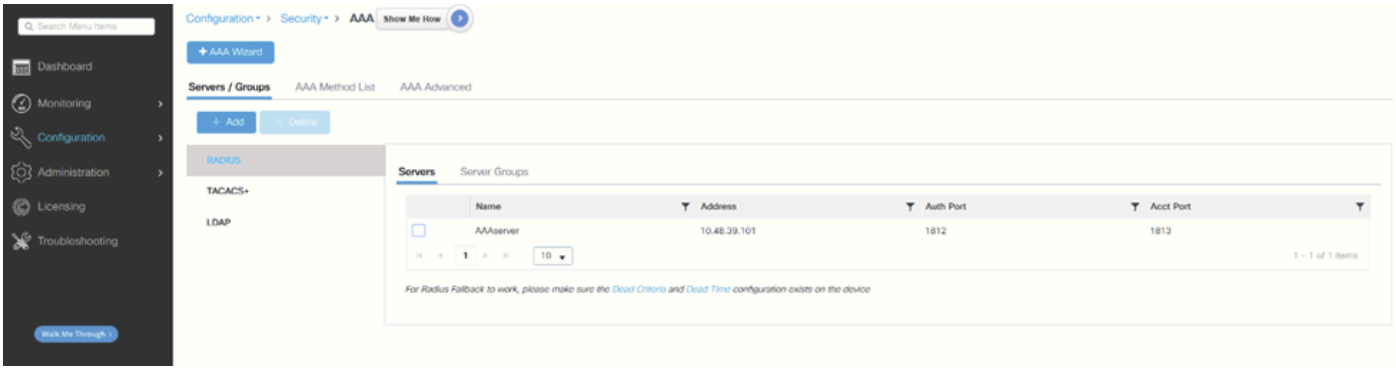
Netzwerkdiagramm

Netzwerkdiagramm

Konfigurationen

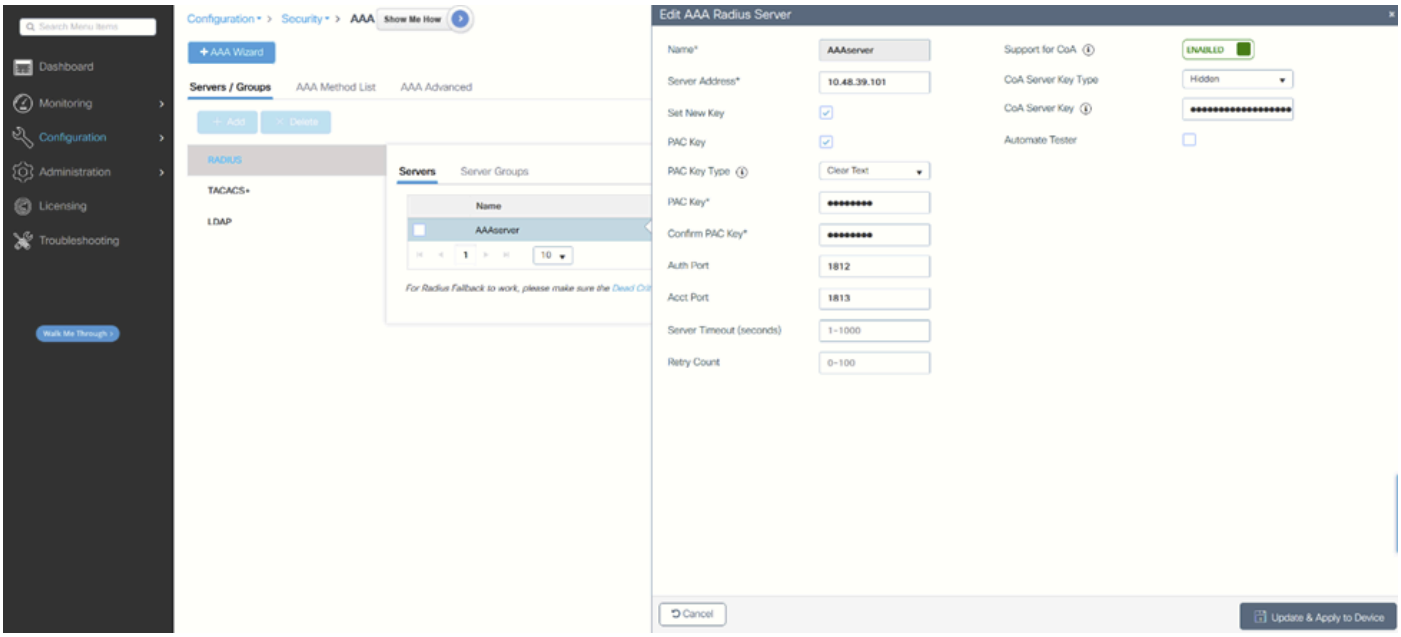
WLC-Konfiguration

1. Fügen Sie den AAA-Server dem WLC hinzu. Gehen Sie dazu wie folgt vor: Configuration > Security > AAA:



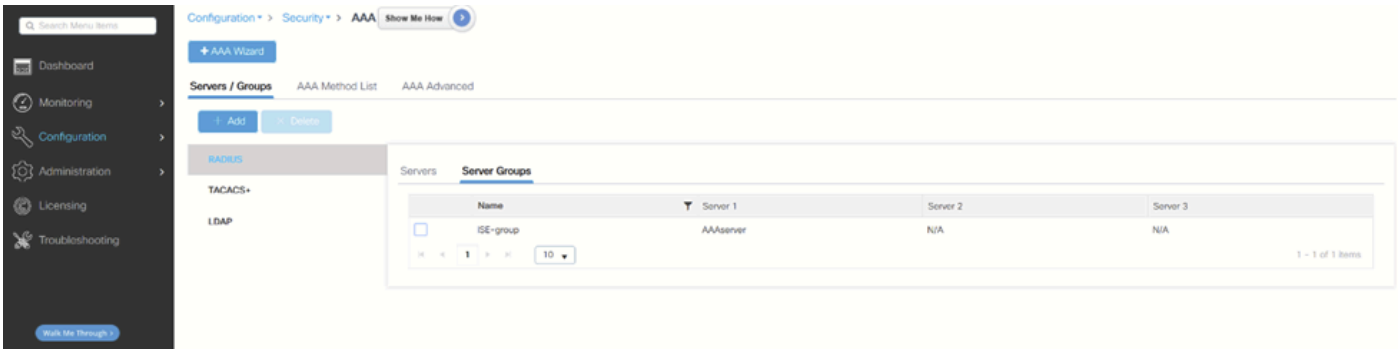
WLC AAA-Seite

2. Stellen Sie sicher, dass die Schlüsseleinträge mit dem Schlüssel übereinstimmen, wenn Sie das Gerät zur ISE hinzufügen. Aktivieren Sie Support für CoA, und fügen Sie den Schlüssel hinzu, wenn Sie CoA zum Herunterladen der Konfigurationsaktualisierungen verwenden möchten:



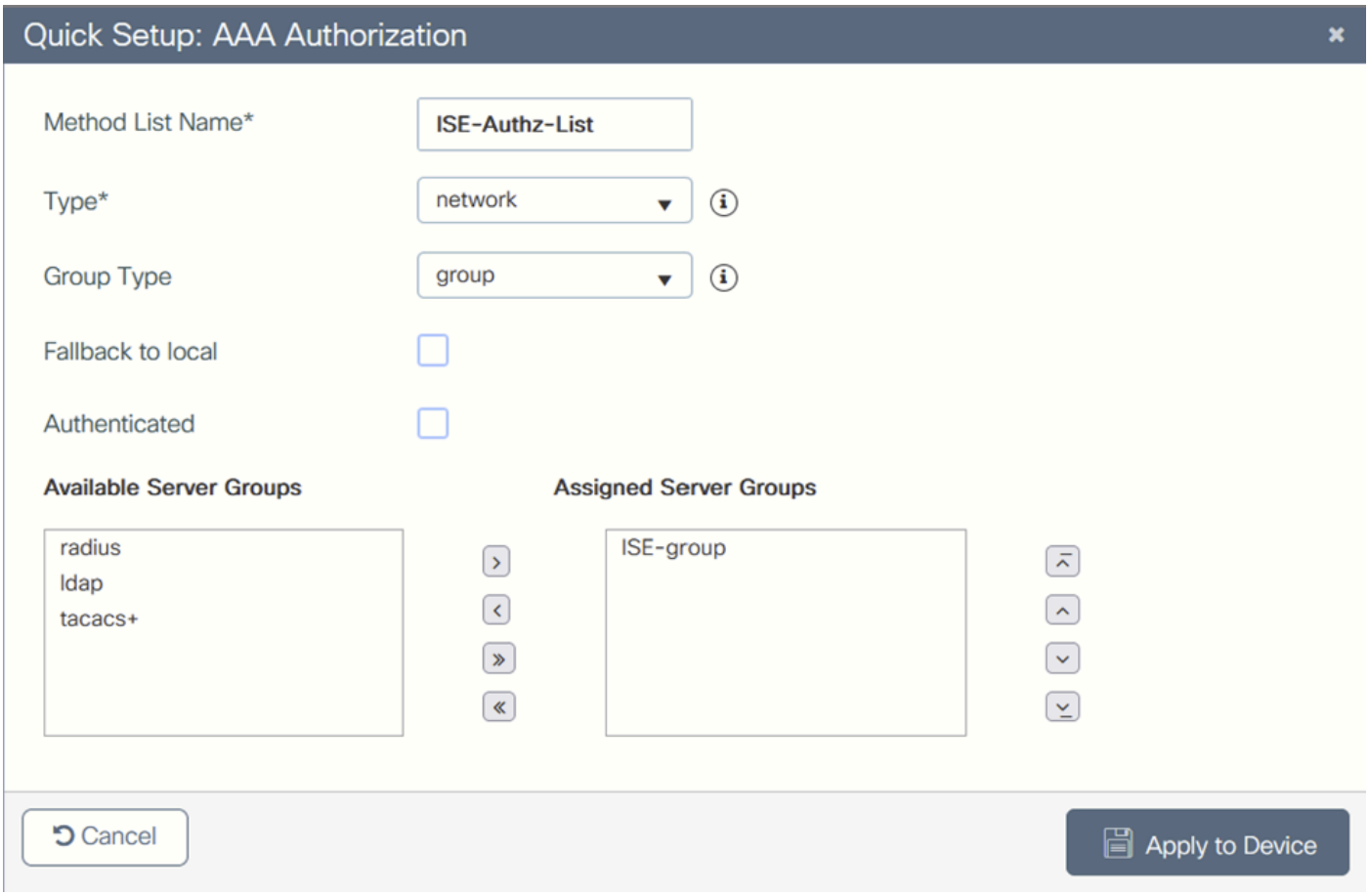
WLC AAA-Server hinzufügen

3. Servergruppe erstellen:

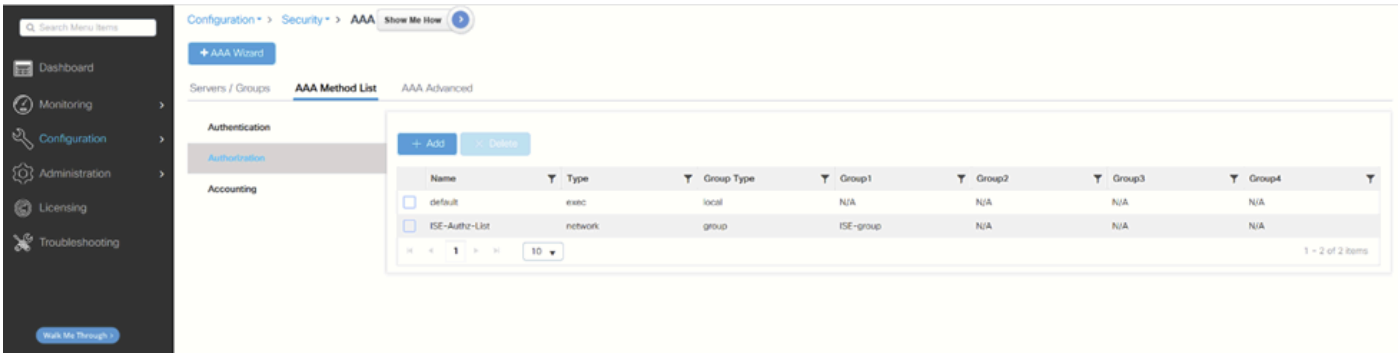


WLC Servergruppe hinzufügen

4. Fügen Sie die Liste der Autorisierungsmethoden mit dem Netzwerktyp hinzu:



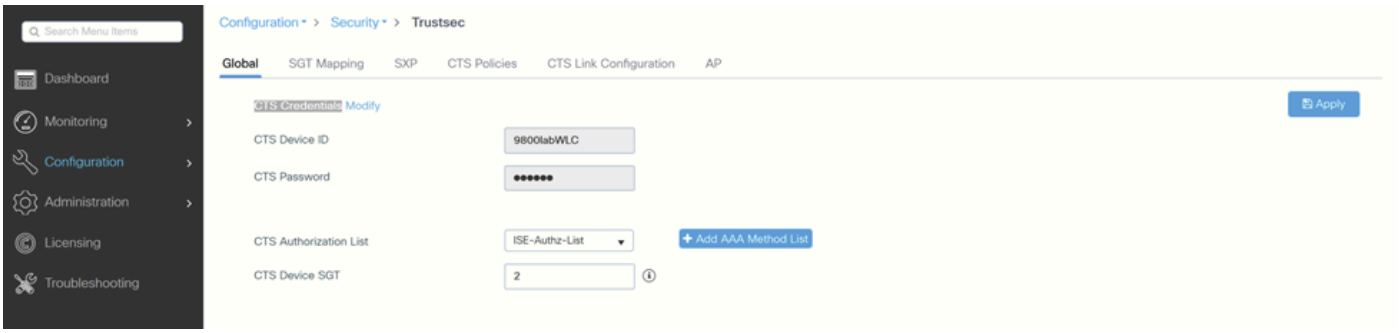
Liste der Autorisierungsmethoden



WLC AAA-Servergruppe

5. Navigieren Sie zu Configuration > Security > TrustSec, und konfigurieren Sie die CTS Geräte-ID und das CTS-Kennwort. Sie verwenden diese Einträge, wenn Sie das Gerät zur ISE hinzufügen.

Konfigurieren Sie auch hier die CTS-Autorisierungsliste, die Sie in Schritt 4 erstellt haben:

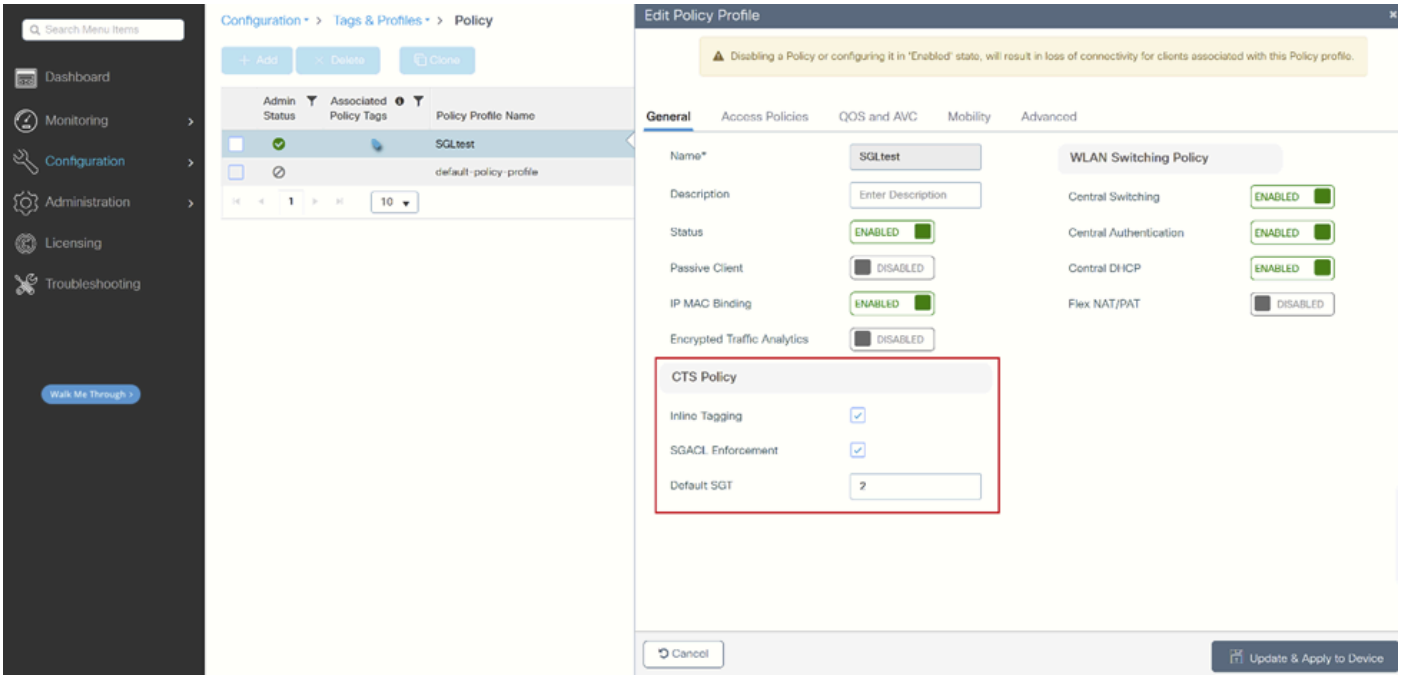


WLC TrustSec

6. In diesem Beispiel ist das WLAN bereits erstellt und die Authentifizierungseinstellungen sind bereits konfiguriert.

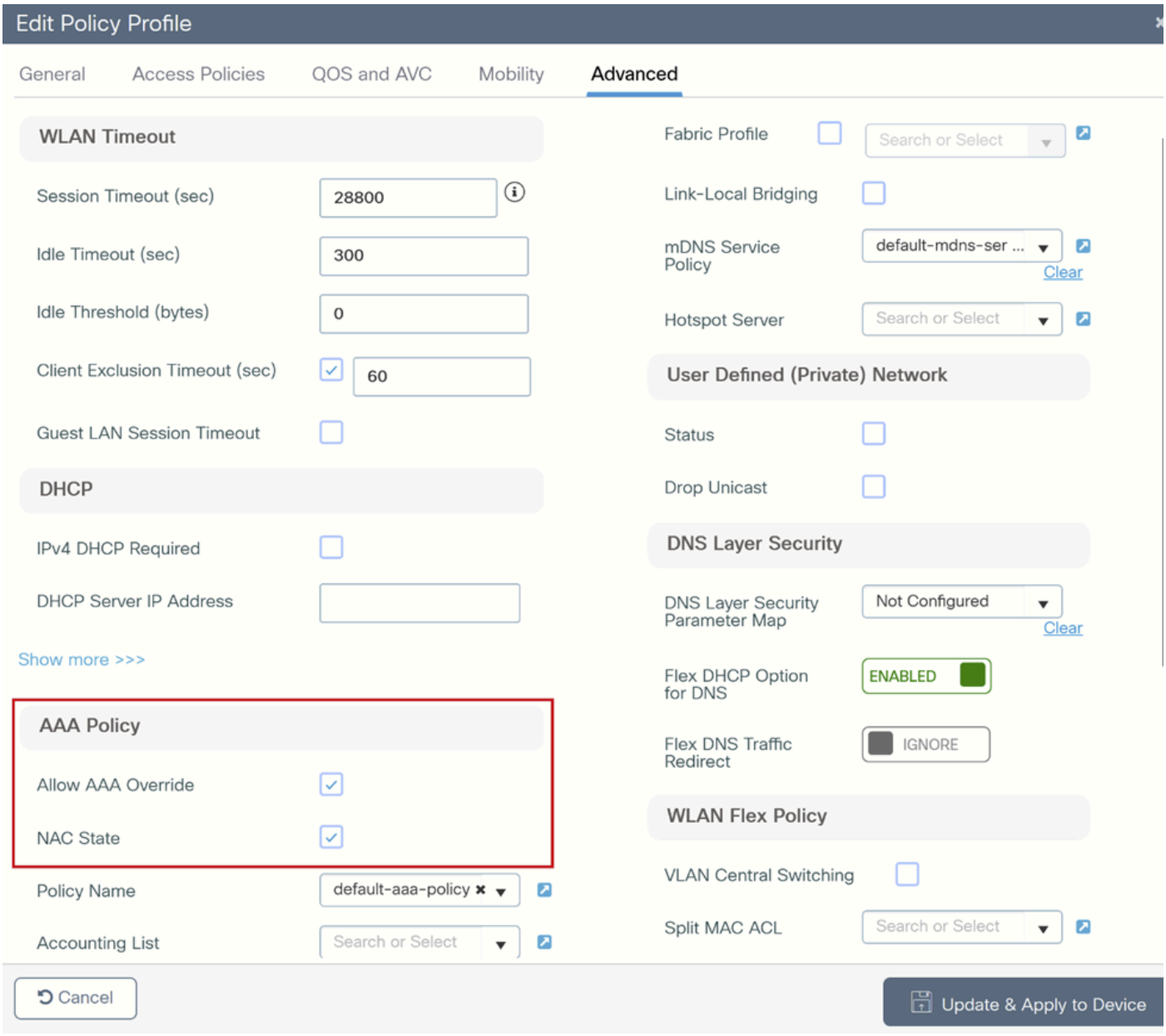
Navigieren Sie nun zu dem Richtlinienprofil, in dem Sie SGTs verwenden möchten.

i. Aktivieren Sie unter CTS Policy (CTS-Richtlinie) Inline Tagging und SGACL Enforcement (SGACL-Durchsetzung), und geben Sie auch das Standard-SGT an. Das Standard-SGT 2 wird für diese Übung als Beispiel verwendet:



WLC-Richtlinienprofil

ii) Aktivieren Sie auf der Registerkarte Advanced die Option Allow AAA override and NAC state:



Registerkarte "WLC Policy Profile Advanced"

Über die CLI:

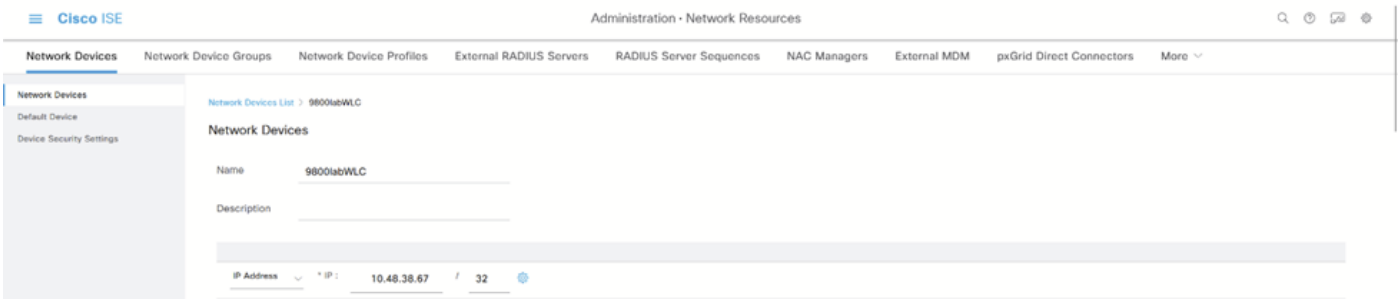
```
# configure terminal

(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
```

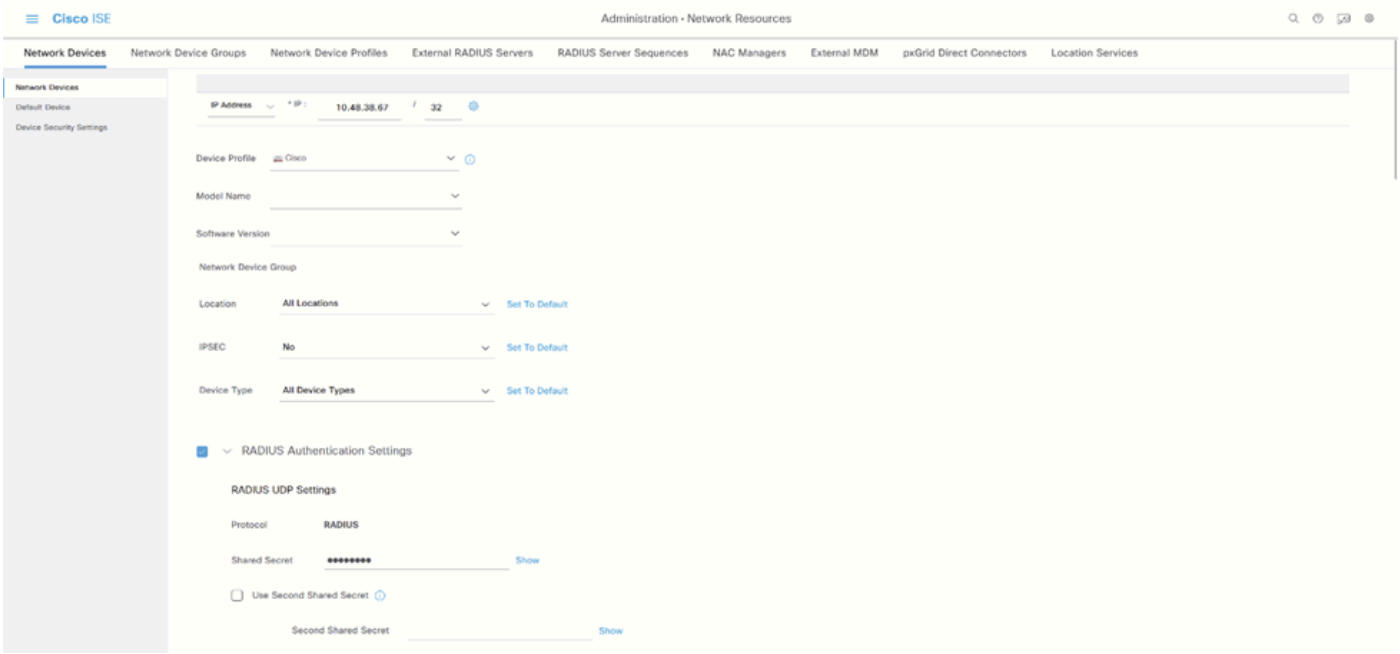
ISE-Konfiguration

1. Navigieren Sie zu Administration > Network Resources > Network Devices (Verwaltung > Netzwerkressourcen > Netzwerkgeräte).

i. Fügen Sie hier die WLC-Informationen hinzu:

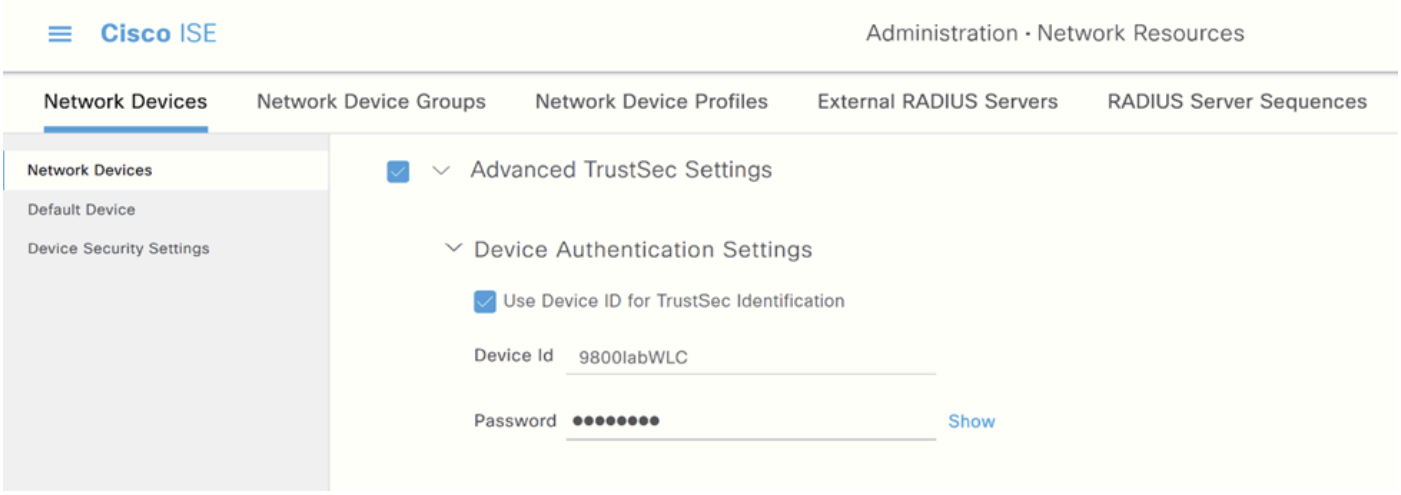


ISE-Netzwerkgeräteseite



ISE WLC RADIUS-Informationen hinzufügen

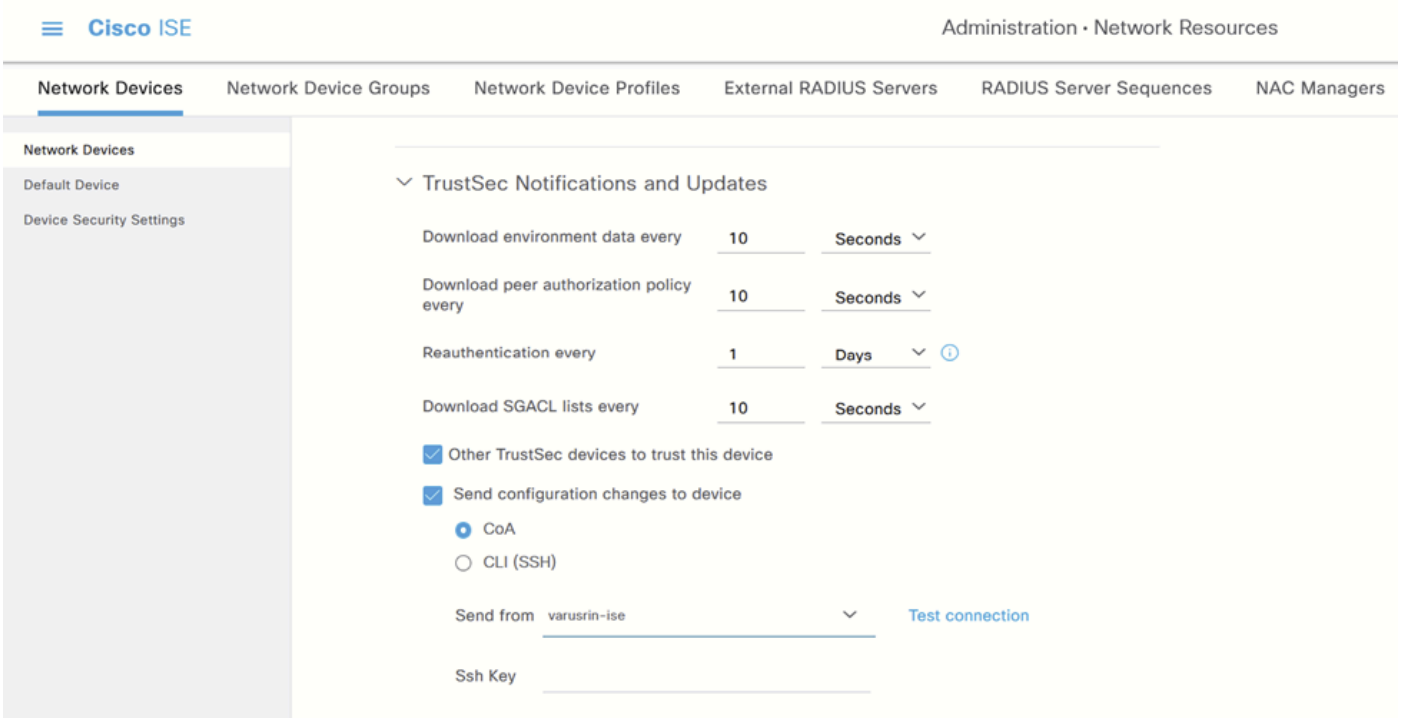
ii) Scrollen Sie nach unten, und konfigurieren Sie die erweiterten TrustSec-Einstellungen. Aktivieren Sie das Kontrollkästchen Use Device ID for TrustSec Identification (Geräte-ID für TrustSec-Identifizierung verwenden), und konfigurieren Sie das Kennwort:



Erweiterte TrustSec-Einstellungen

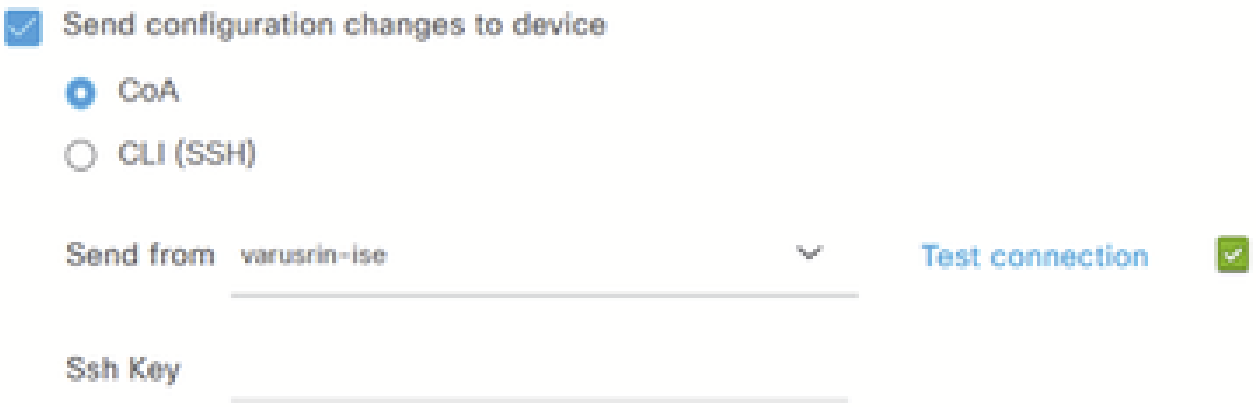
Dies muss mit der Konfiguration auf WLC-Seite in Schritt 6 der WLC-Konfiguration übereinstimmen.

iii. Blättern Sie nach unten zu TrustSec-Benachrichtigungen und -Updates, und konfigurieren Sie, ob Sie CoA oder SSH für Konfigurationsaktualisierungen verwenden möchten. Wählen Sie den benötigten ISE-Knoten aus:



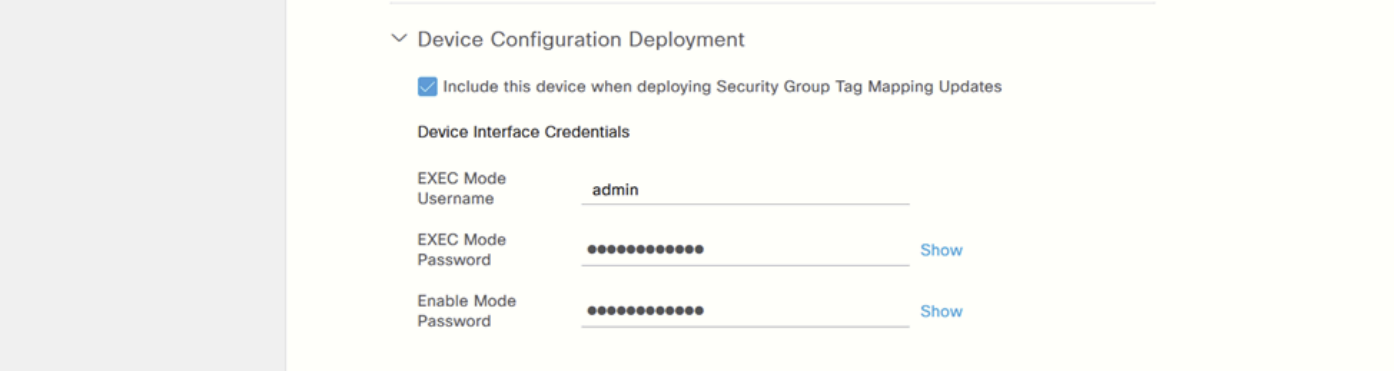
TrustSec-Benachrichtigungen und -Updates

2. Drücken Sie auf Verbindung testen, um sicherzustellen, dass die Verbindung hergestellt ist. Wenn es erfolgreich ist, wird es ein grünes Häkchen zeigen:



Testverbindung

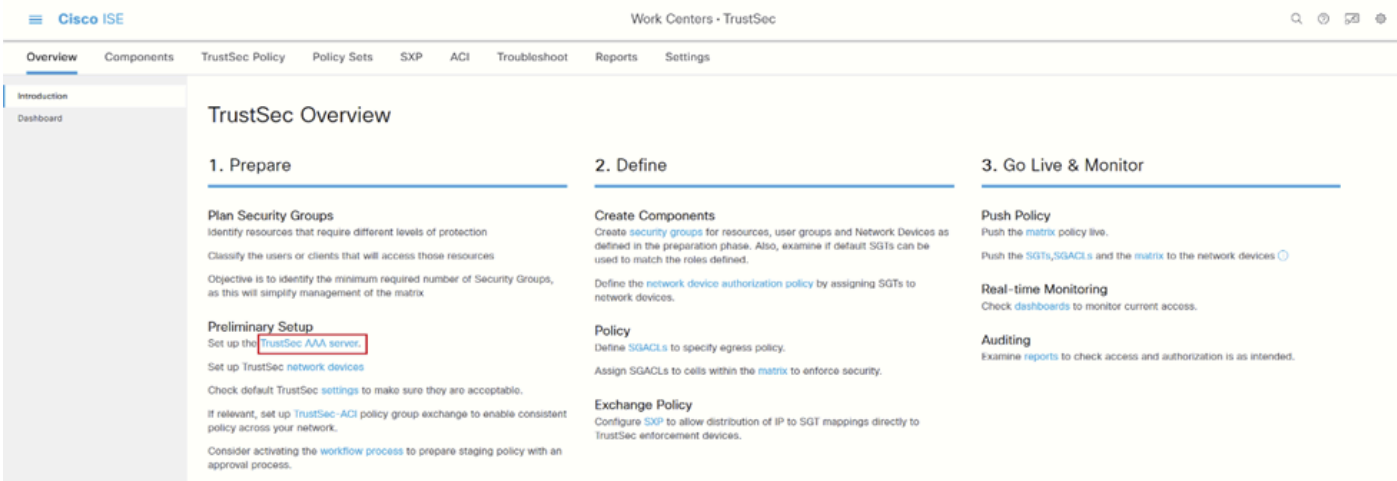
i. Scrollen Sie nach unten, und konfigurieren Sie den WLC so, dass er bei der Bereitstellung von Updates für die SGT-Zuordnung eingeschlossen ist. Dies ist wichtig, wenn Sie im vorherigen Schritt die SSH-Option auswählen:



Bereitstellung der Gerätekonfiguration

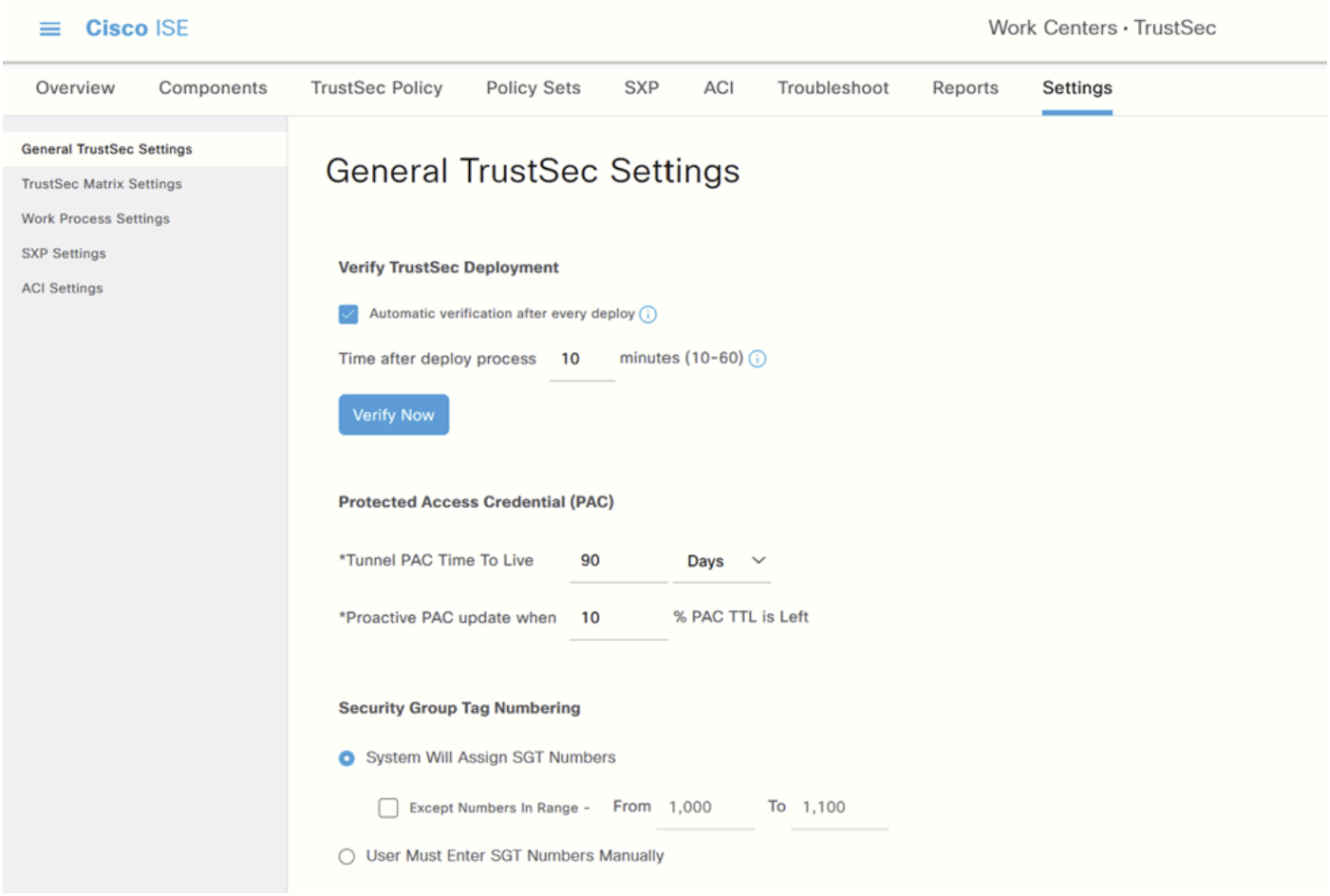
ii) Speichern Sie die Konfiguration.

3. Aus Work Centers > TrustSec > Overview (Übersicht) werden die TrustSec-Konfigurationsoptionen angezeigt. Wählen Sie TrustSec AAA Server aus, um die verwendete ISE-Instanz anzuzeigen. Weitere Informationen zur verwendeten Instanz bei mehreren Catalyst Wireless-Geräten finden Sie in der Cisco Catalyst Wireless Group Based Policy (Gruppenbasierte Richtlinie für Cisco Catalyst Wireless).



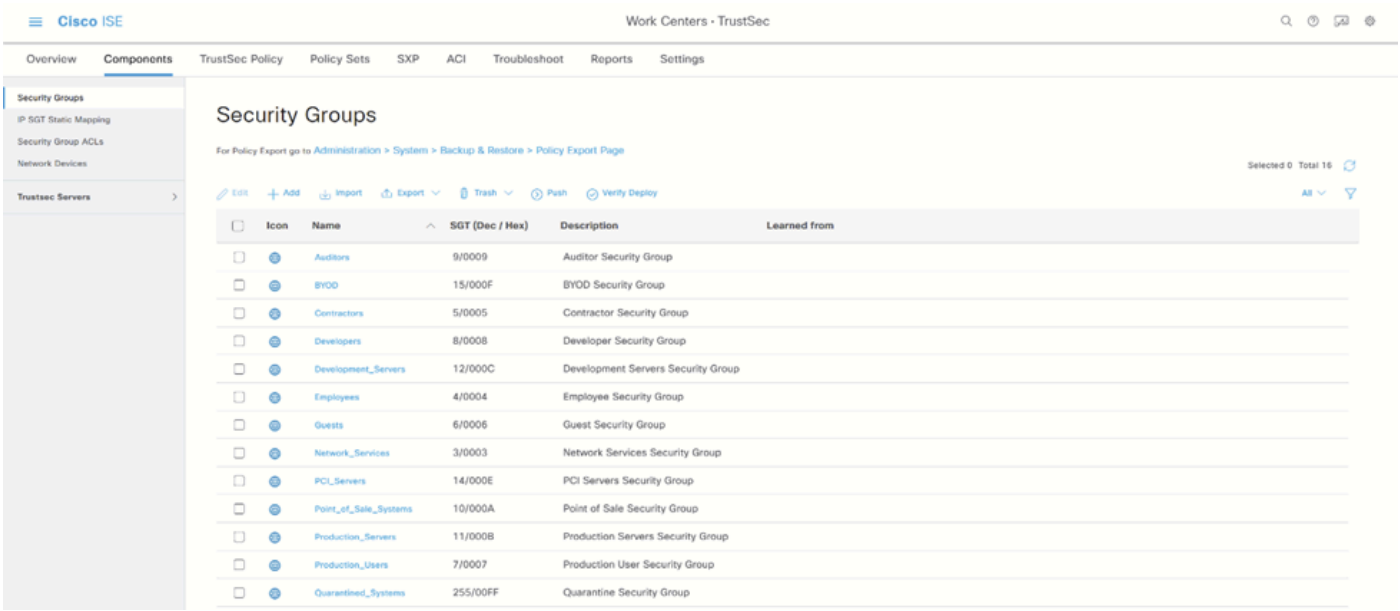
ISE TrustSec - Überblick

4. (Optional) Navigieren Sie zur Registerkarte Einstellungen, und aktivieren Sie ggf. nach jeder Bereitstellung die automatische Überprüfung.

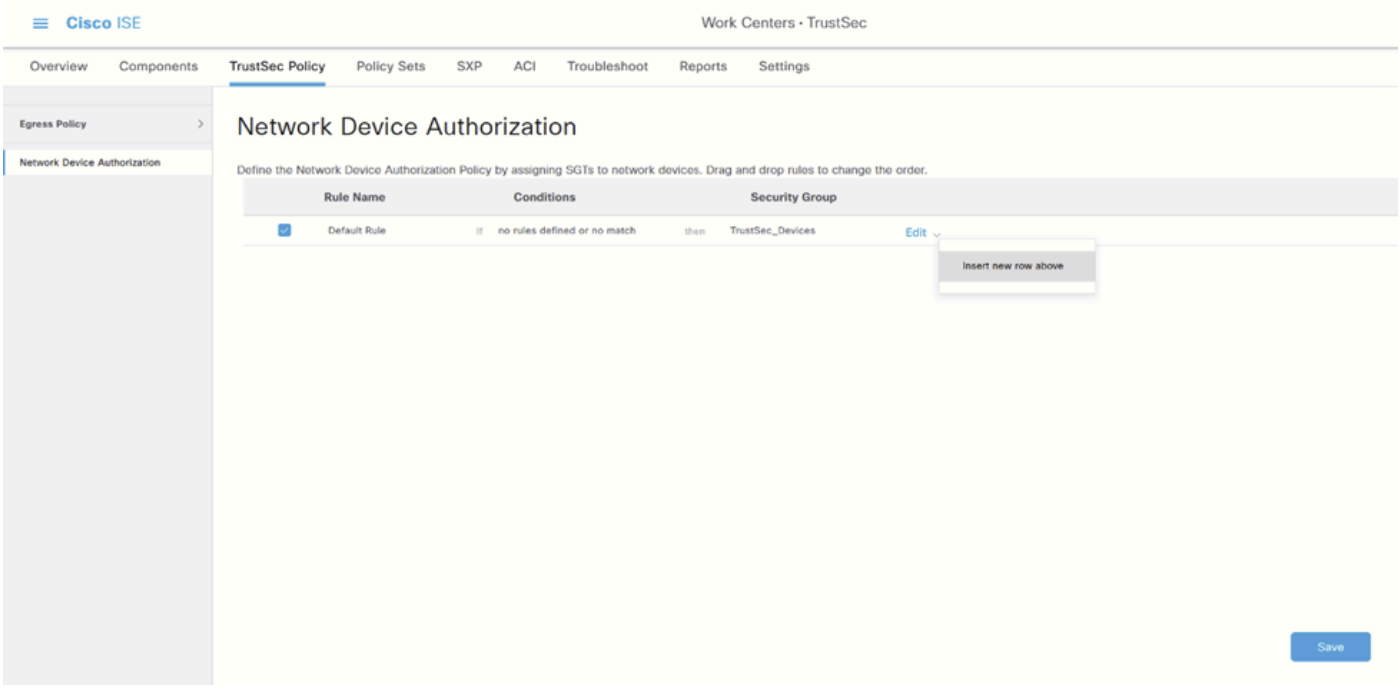


ISE TrustSec-Einstellungen

5. Fügen Sie die SGT-Werte je nach Anforderungen von Work Centers > TrustSec > Components > Security Groups hinzu, oder bearbeiten Sie diese:

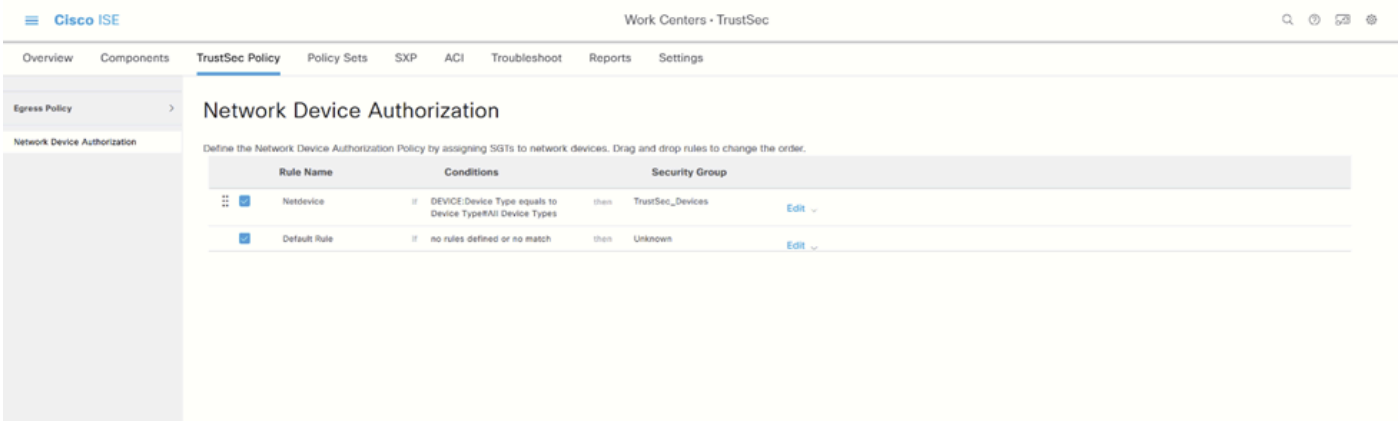


6. Wenn Sie die Autorisierungsrichtlinie angeben möchten, navigieren Sie zu Work Centers > TrustSec > TrustSec Policy > Network Device Authorization:



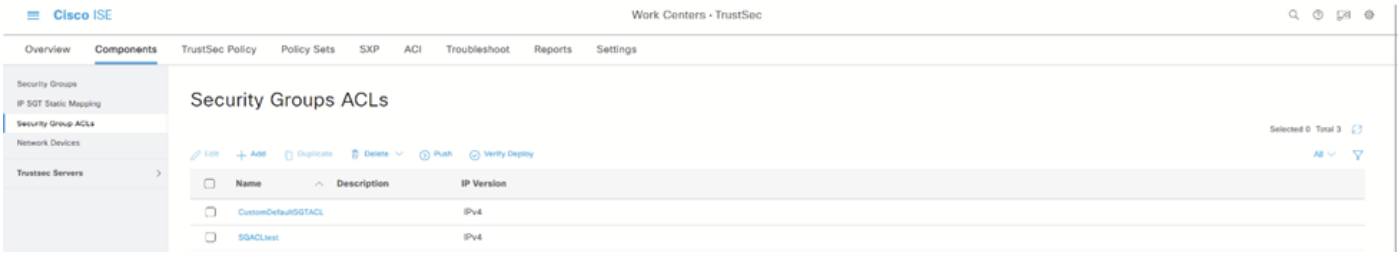
TrustSec-Richtlinie

Sie können die Standardeinstellung beibehalten, für diese Übung verwenden wir jedoch diese Konfiguration als Beispiel:



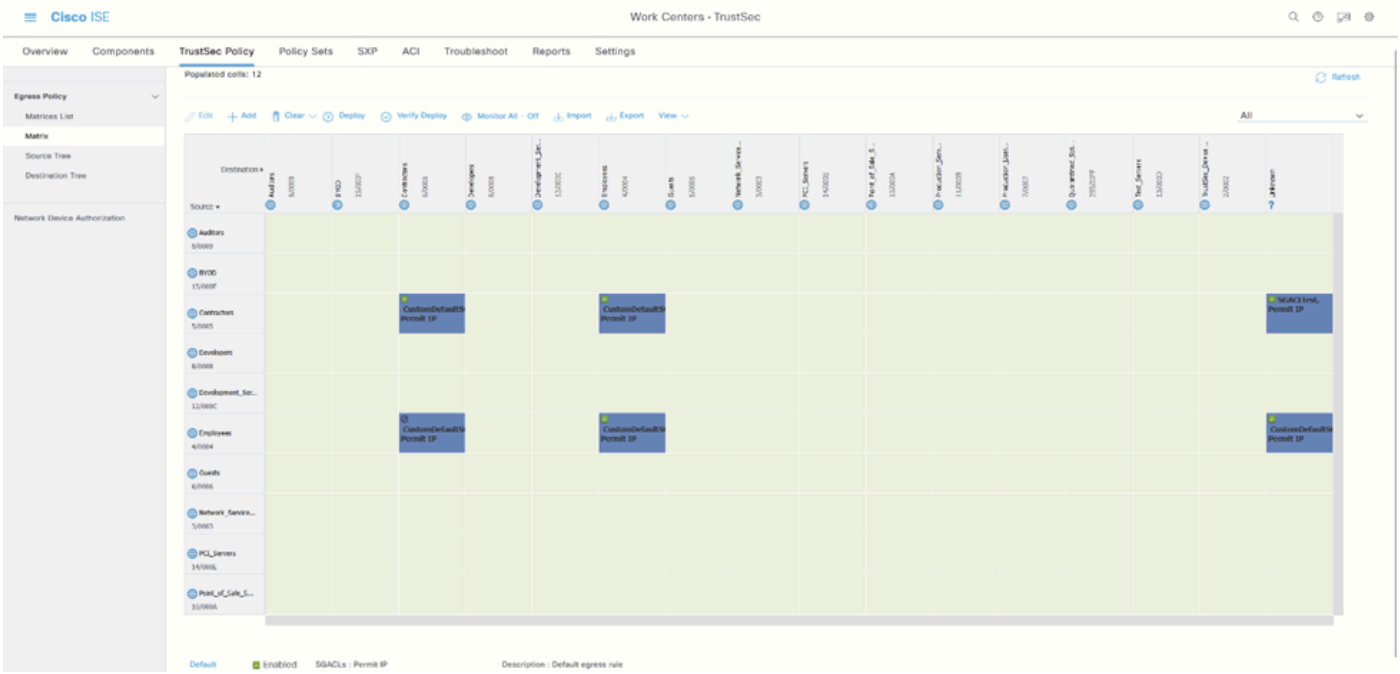
Autorisierung von Netzwerkgeräten

7. Erstellen Sie die SGACL auf der Registerkarte Components (Komponenten) und anschließend die Security Group ACLs:



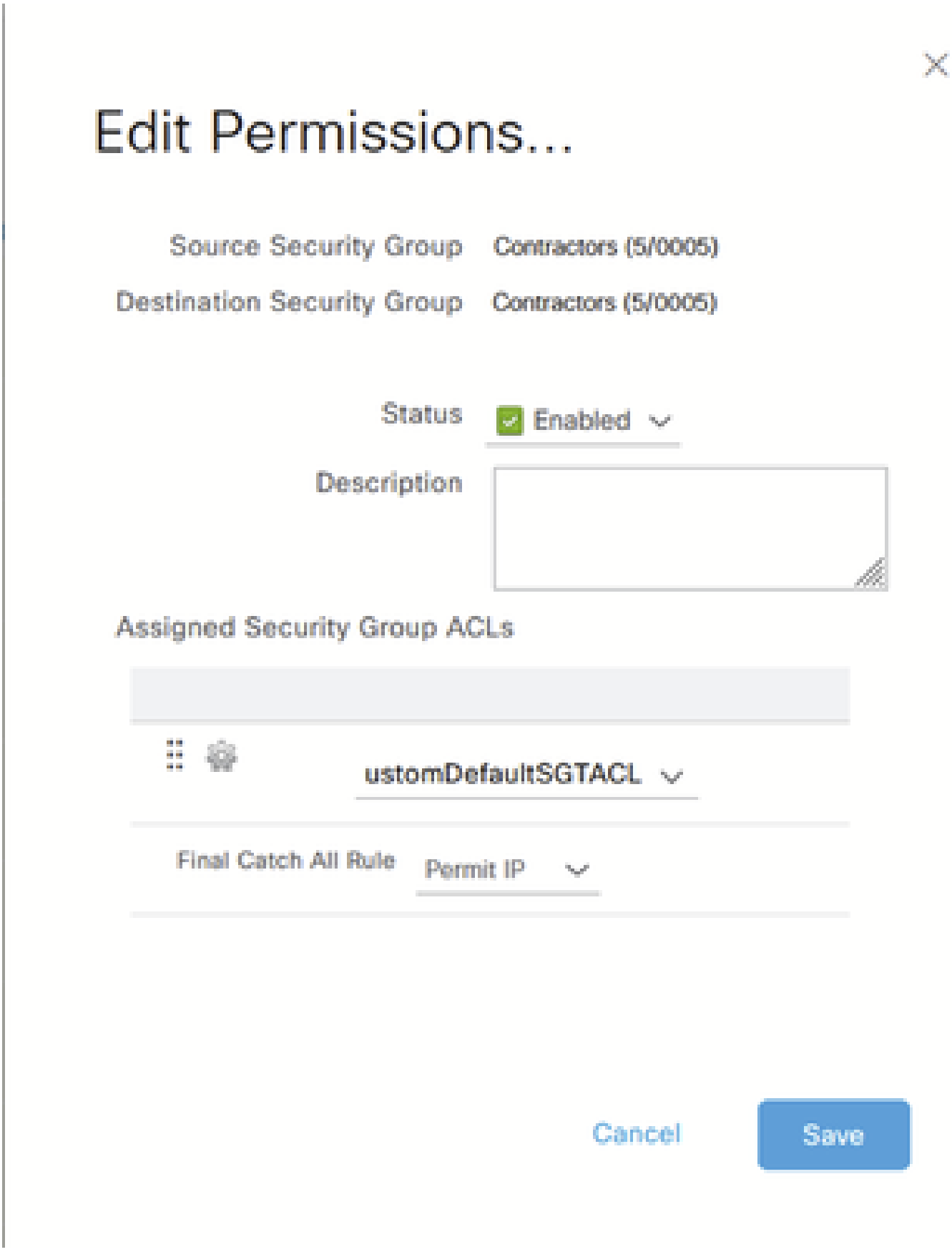
Sicherheitsgruppen-ACLs

8. Geben Sie die Matrixeinträge auf der Registerkarte TrustSec Policy (TrustSec-Richtlinie) und dann Matrix an. Sie können die Berechtigungen bearbeiten, indem Sie auf den Punkt klicken, den zwei SGTs erfüllen:

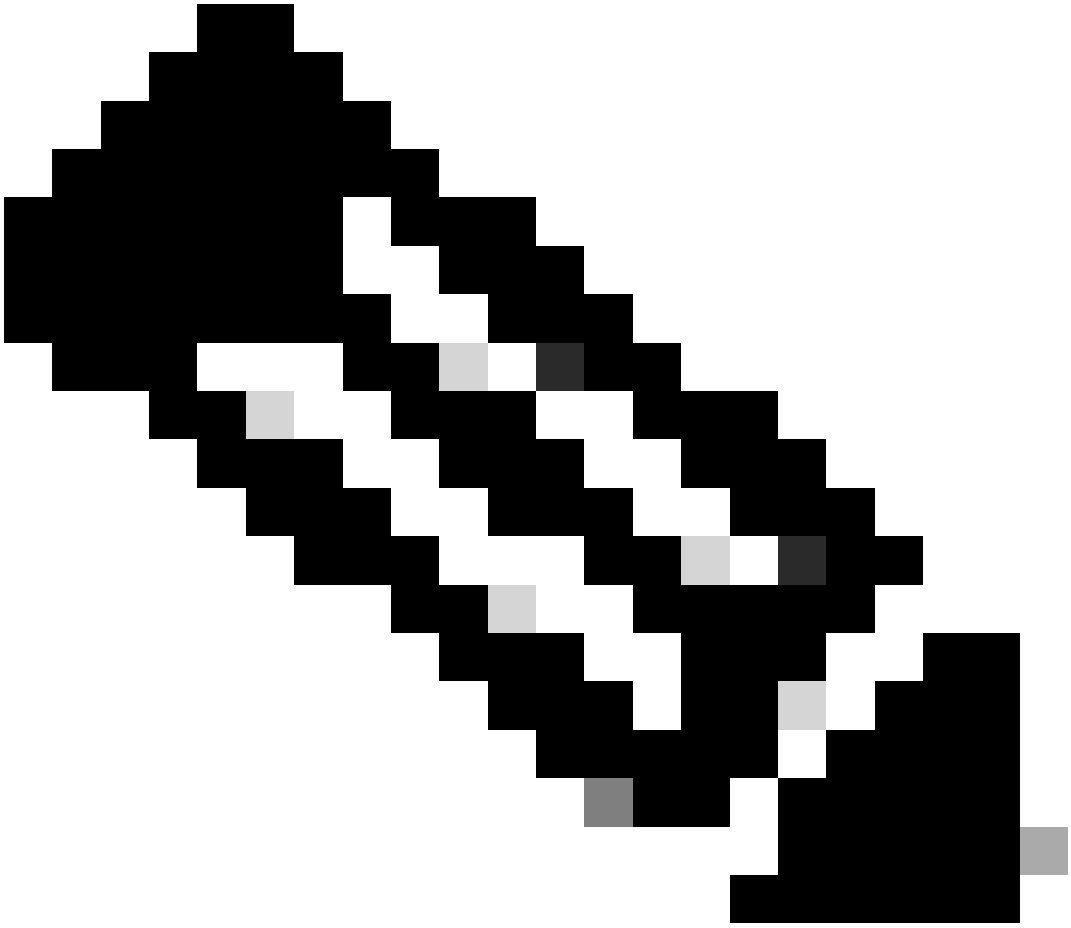


ISE TrustSec-Matrix

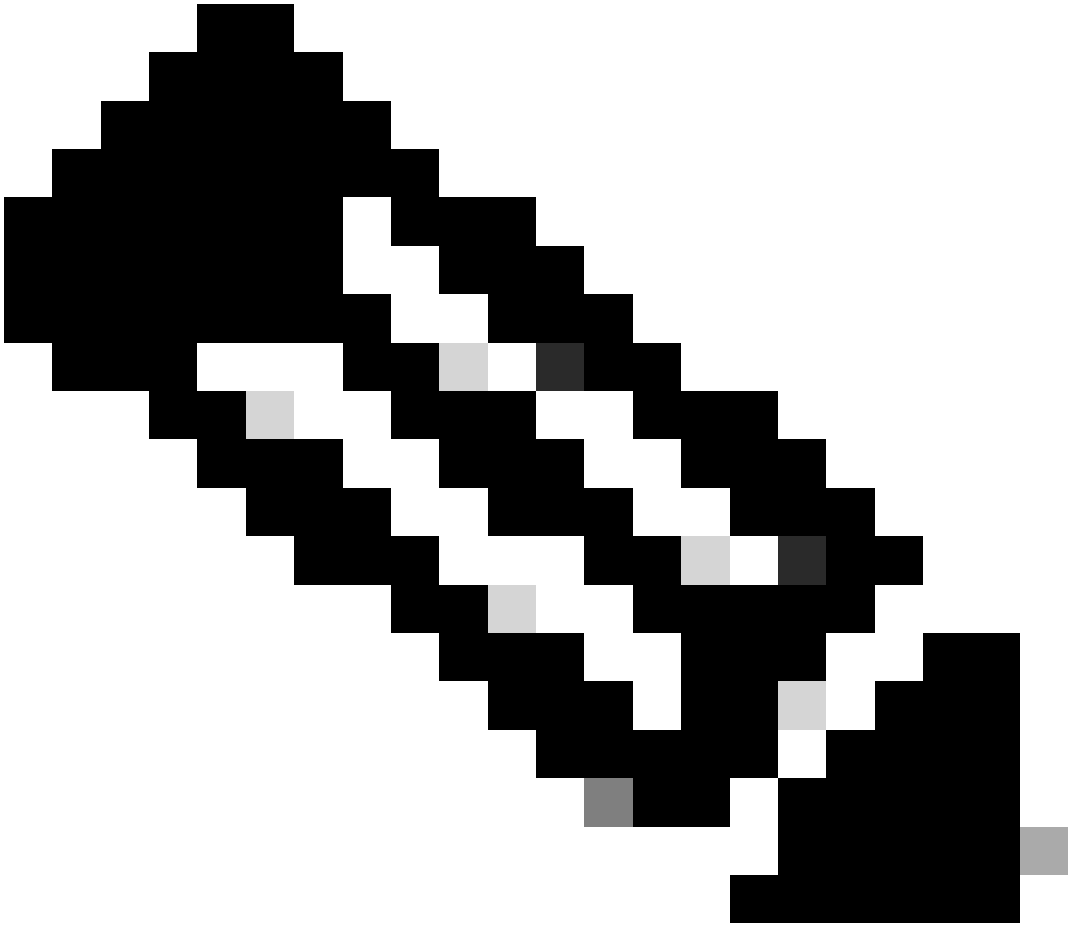
Beispiele:



Berechtigungen bearbeiten

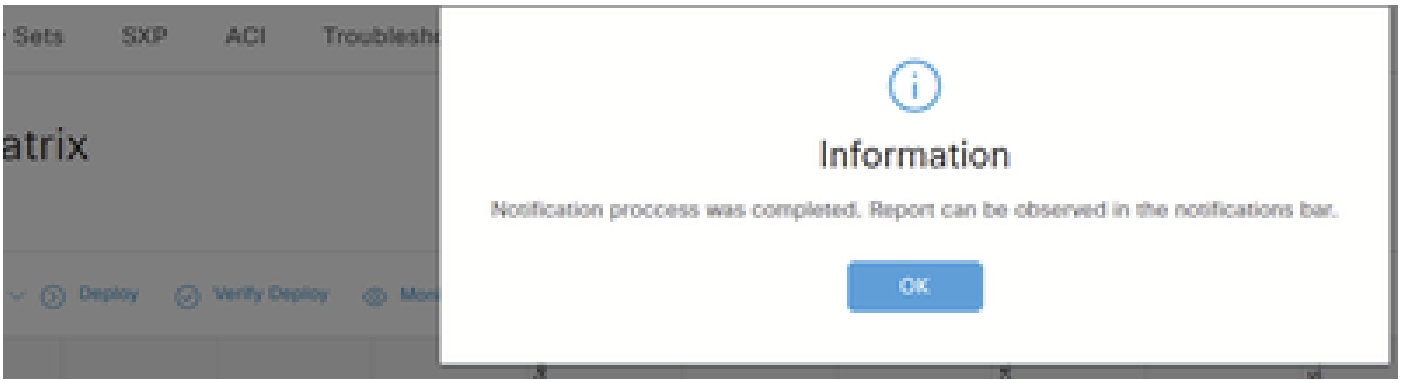


Anmerkung: Im Fall des Allow List-Modells müssen Sie den Client-Geräten explizit erlauben, dass das DHCP-Protokoll die DHCP-IP-Adresse abruft, und dann den Controller für SGACL-Richtlinien anfordern.

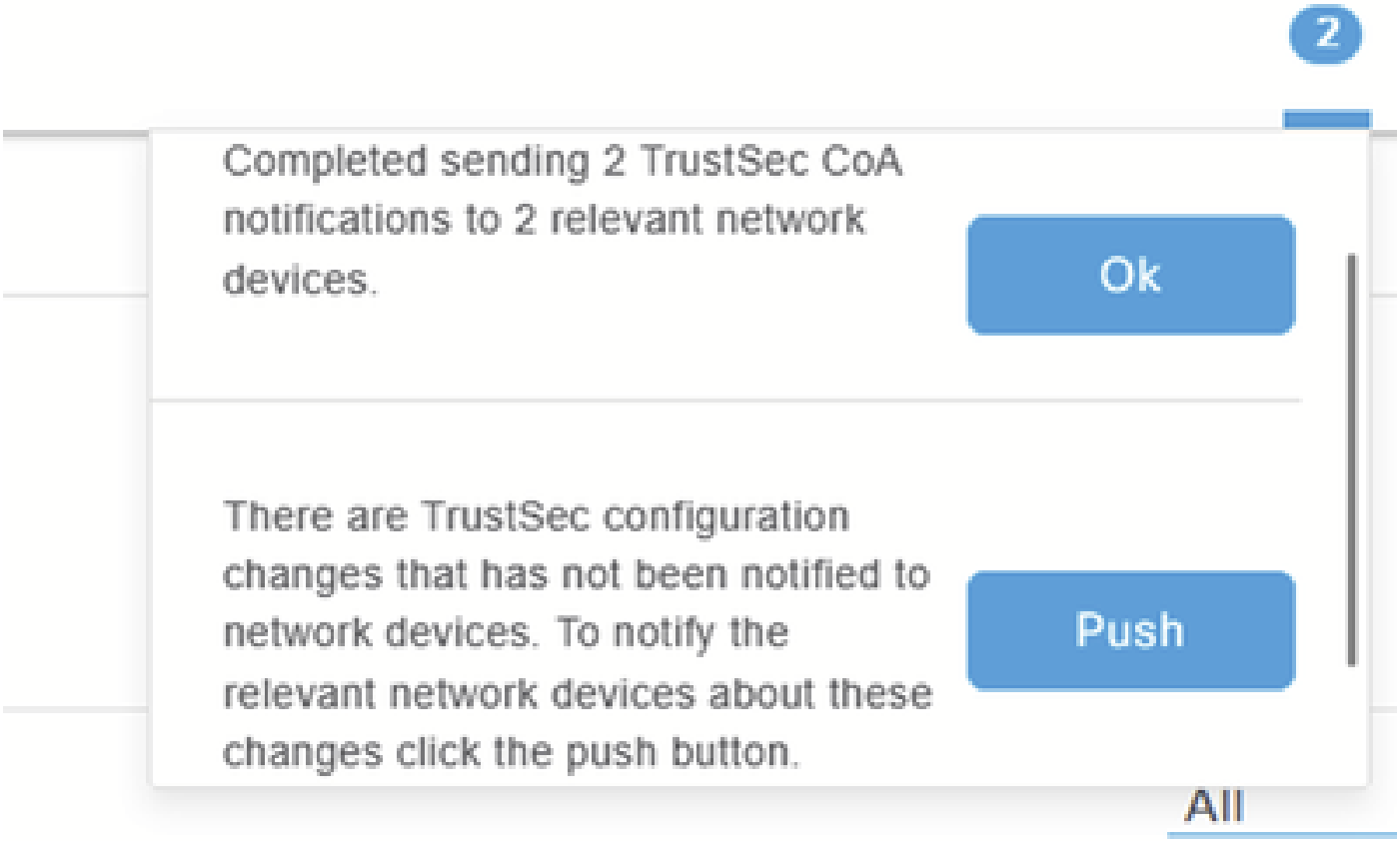


Anmerkung: Clients erhalten keinen SGT-Wert, und DHCP-Clients erhalten eine automatische private IP-Adressierungsadresse (APIPA), wenn die TrustSec-Richtlinie in der TrustSec-Matrix abgelehnt wird.
Clients erhalten die richtigen SGT-Werte, und DHCP-Clients erhalten eine IP-Adresse, wenn die TrustSec-Richtlinie in der TrustSec-Matrix als "unbekannt" zugelassen ist.

9. Klicken Sie auf Bereitstellen. Die folgenden Nachrichten und Benachrichtigungen werden angezeigt:



Bereitstellung

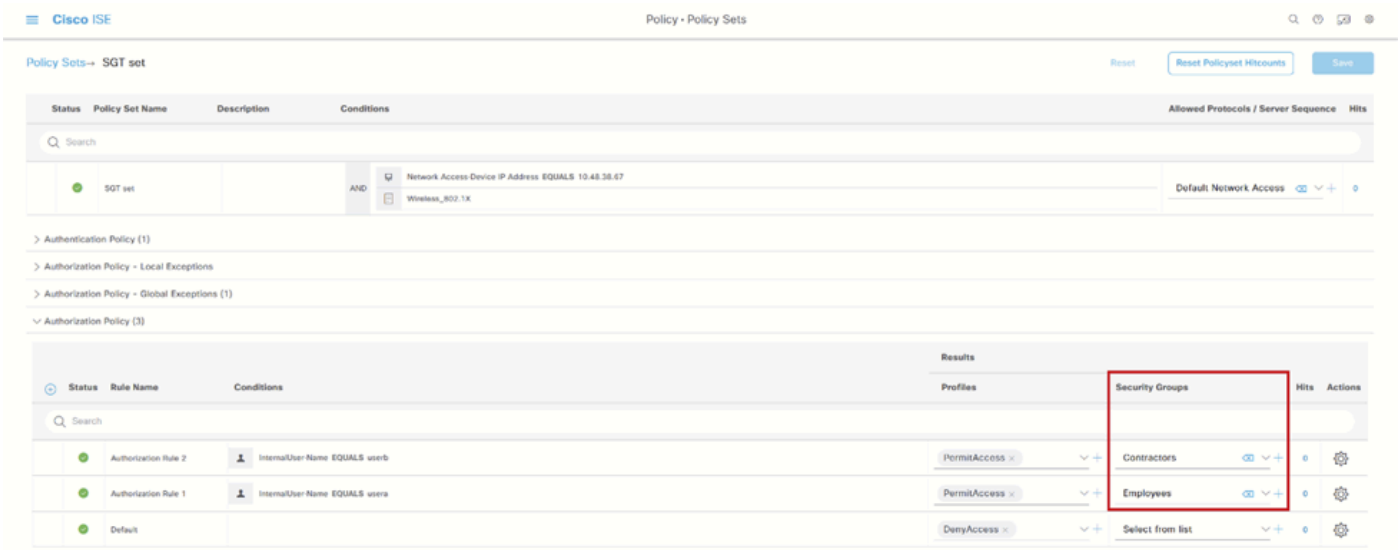


Benachrichtigungen bereitstellen

10. Navigieren Sie zu dem für das WLAN verwendeten Richtliniensatz unter Richtlinie > Richtliniensätze:

ISE-Richtliniensätze

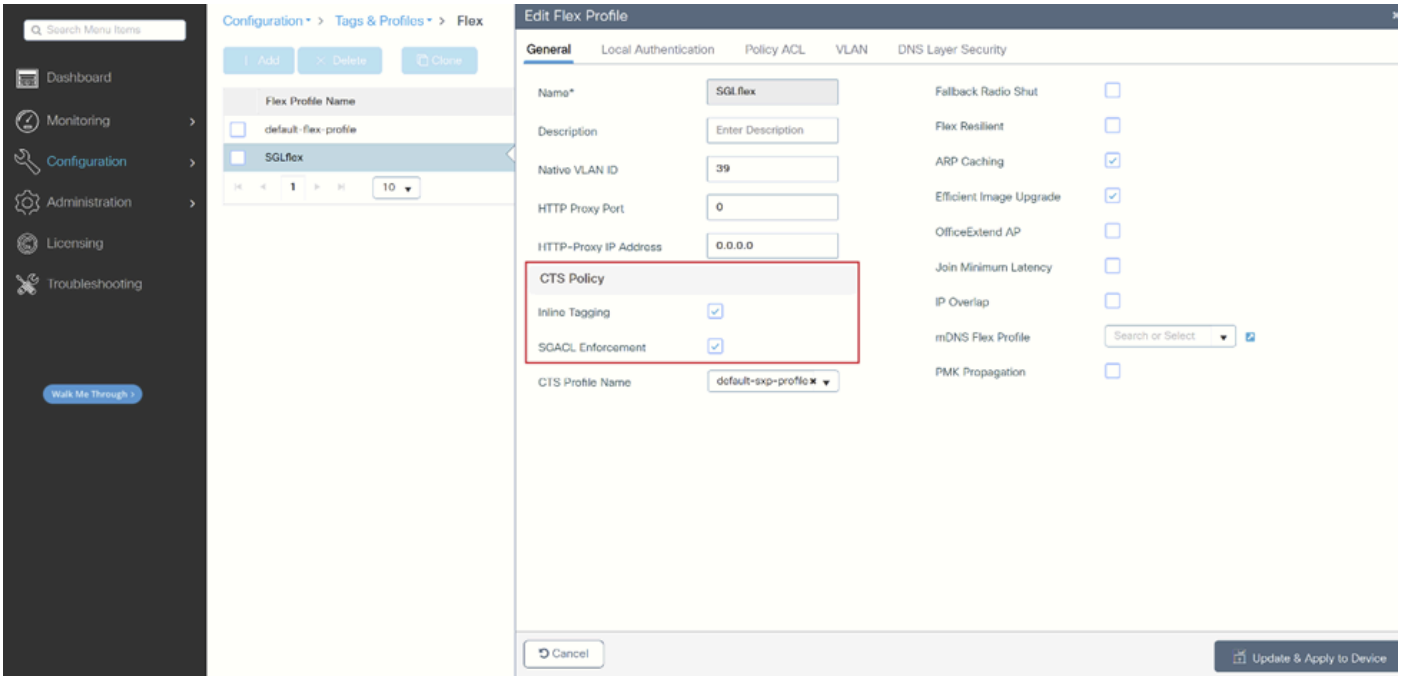
In dieser Übung definieren wir das SGT pro Benutzer. Wählen Sie das SGT im Feld Security Groups (Sicherheitsgruppen) aus:



ISE-Sicherheitsgruppen

Flexconnect

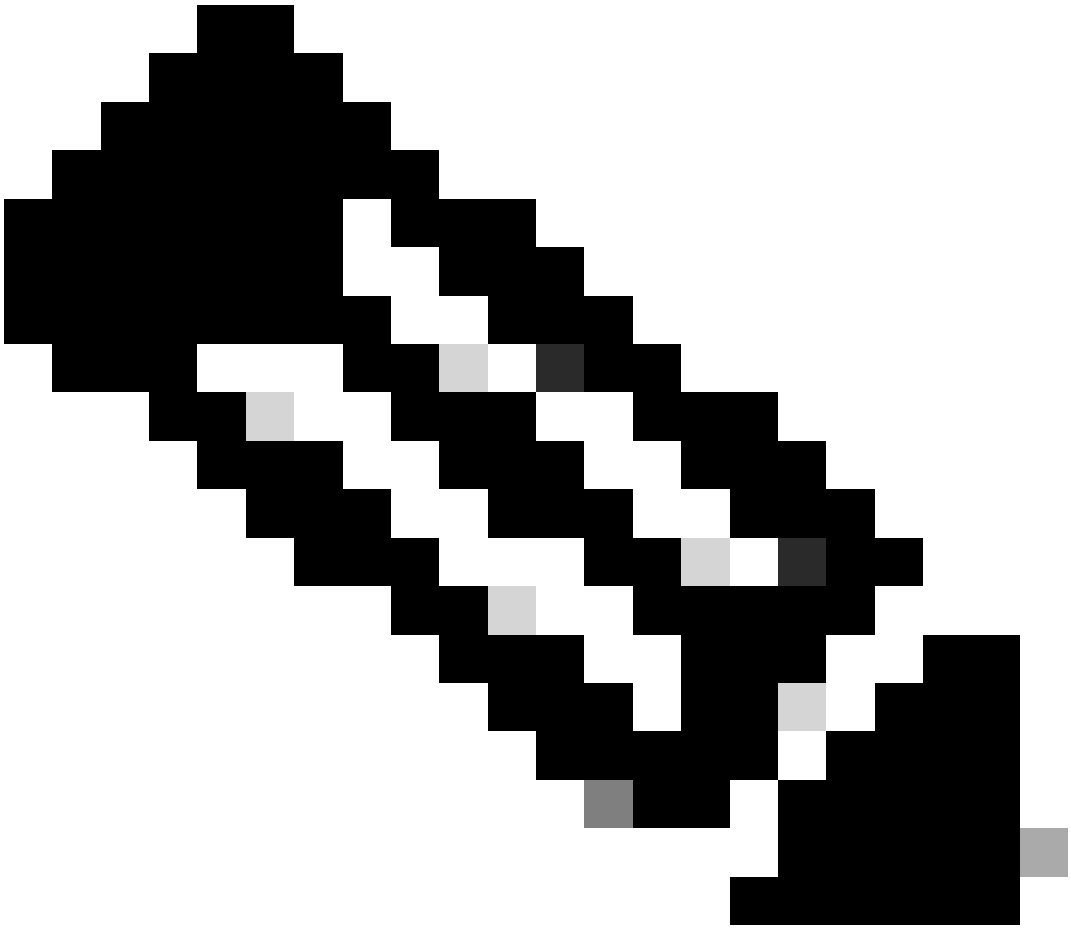
Aktivieren Sie Inline-Tagging und die SGACL-Durchsetzung auf dem Flex Profile unter Konfiguration > Tags und Richtlinien > Flex:



WLC Flex-Profil

Über die CLI:

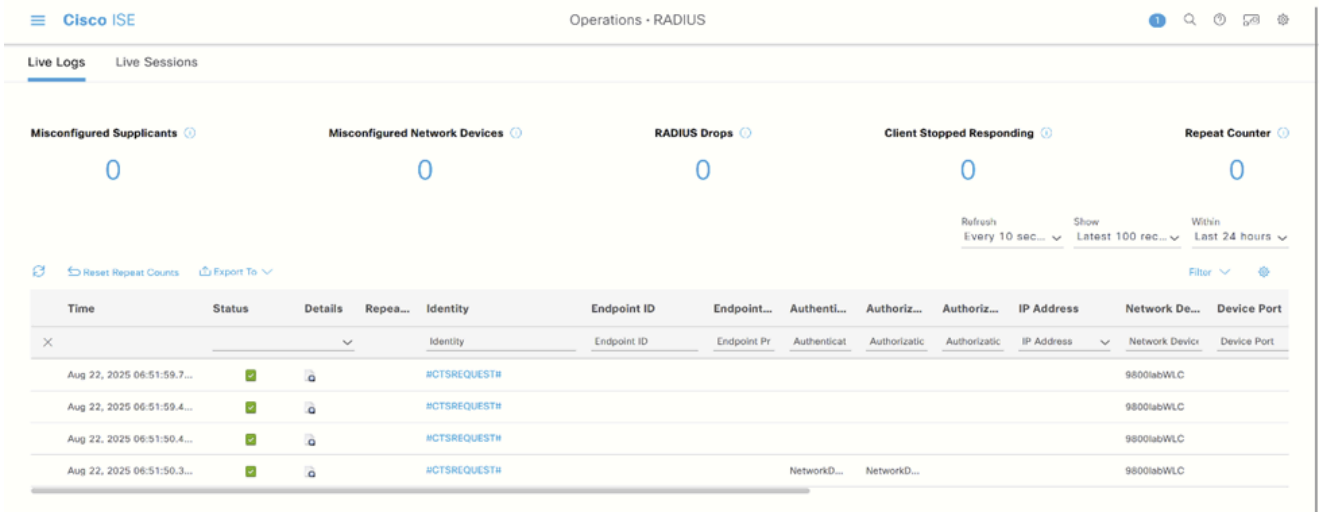
```
# configure terminal

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



Anmerkung: Wenn sich der WLC in HA-SSO befindet, wird SGACL auf FlexConnect-APs nicht unterstützt. Cisco Bug-ID CSCwn85468. Diese wird in 17.19 hinzugefügt.

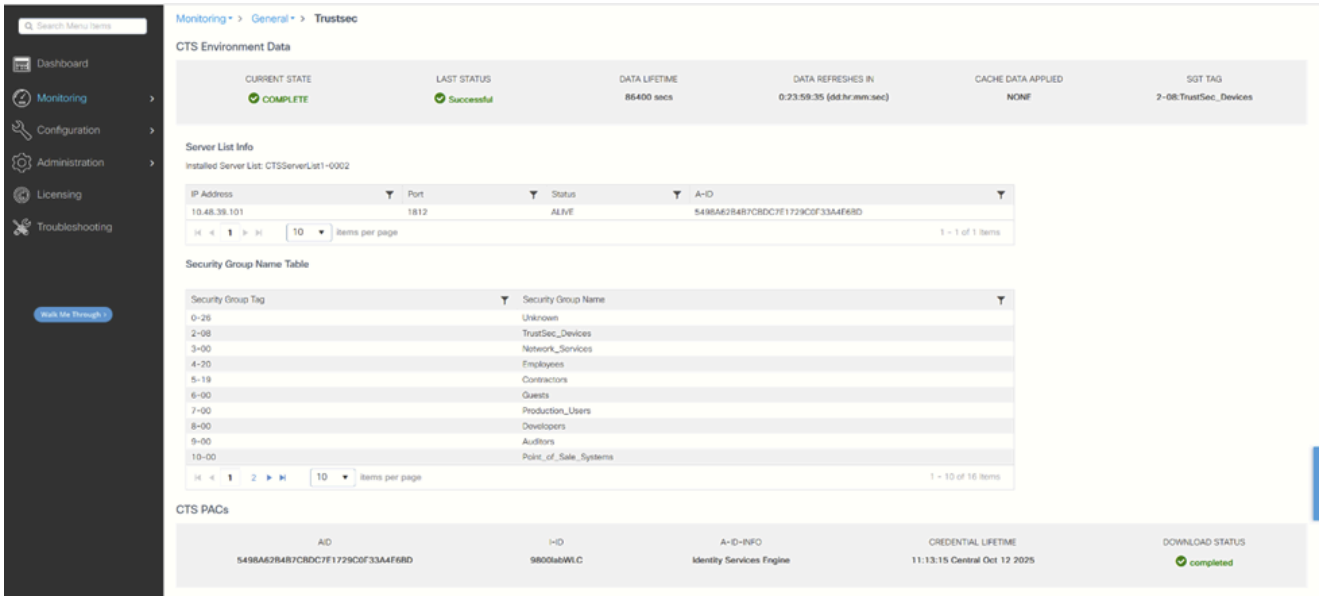
Überprüfung

1. Auf der ISE muss eine erfolgreiche CTS-Anforderung unter Operations > RADIUS > Live Logs (Betrieb > RADIUS > Live-Protokolle) angezeigt werden:



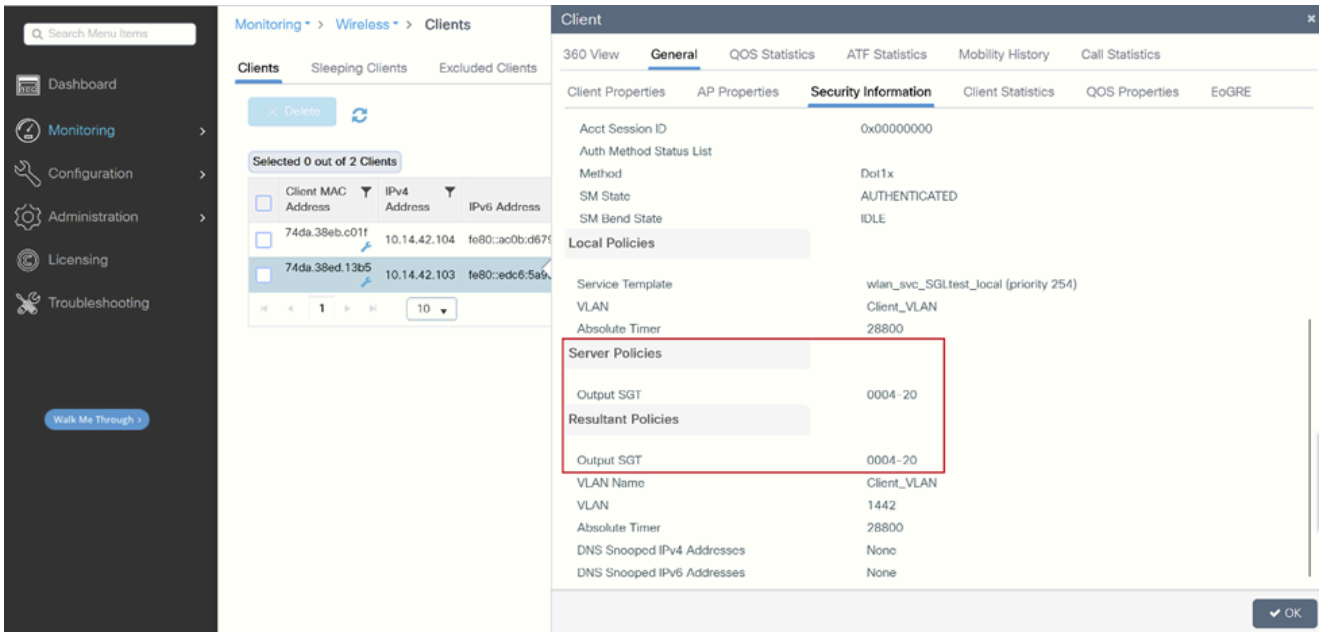
ISE RADIUS-Live-Protokolle

2. Sie können überprüfen, ob die Verbindung hergestellt wurde und ob die SGTs von Monitoring > General > TrustSec auf den WLC heruntergeladen wurden:



WLC TrustSec-Überwachung

3. Wenn Sie einen Client verbinden, wird das zugewiesene SGT unter Überwachung > Wireless > Clients angezeigt. Wählen Sie den Client aus, den Sie überprüfen möchten, und navigieren Sie zur Registerkarte Allgemein > Sicherheitsinformationen:



WLC-Client-Überwachung

Über die CLI:

- Bevor Sie den Client anschließen, sehen Sie Folgendes in der WLC-Ausgabe: Nur die Berechtigungen für unbekannte SGTs werden angezeigt.

```
<#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
```

- Beim Herstellen der Verbindung mit dem Client können Sie diese Protokolle über die RA-Ablaufverfolgungen beobachten. Das SGT wird von AAA angewendet:

<#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
```

- Verwenden Sie den CLI-Befehl show wireless client mac-address <client_MAC_address> detail, um das dem Client zugewiesene SGT anzuzeigen:

<#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
…
```

- Nachdem Sie einen Client in SGT 4 verbunden haben, werden Sie feststellen, dass die Berechtigungen für SGT 4 jetzt angezeigt werden:
  Die Berechtigungen werden hinzugefügt, nachdem der Client verbunden wurde und ihm ein SGT zugewiesen wurde.

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

- Nach dem Verbinden von zwei Clients, einer im SGT 4 und der andere im 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
============================================================
```

- Nun können Sie sehen, dass die Berechtigungen für SGT 5 hinzugefügt wurden:

<#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
```

- Die ACLs werden auf dem WLC als "heruntergeladen" angezeigt:

<#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 - Lokales Switching

- Dies ist der WLC-Ausgang vor dem Verbinden der Clients mit dem AP:

<#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
```

- Von der AP-CLI werden die Berechtigungen ausgegeben, bevor Clients mit dem AP verbunden werden:

```
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
```

- Dies sind die AP-Debugging-Vorgänge, die der Client beim Herstellen einer Verbindung durchführt, um den Datenfluss anzuzeigen:

<#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
…
```

- Über die WLC-CLI bei Verbindung eines Clients mit 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
```

- Von AP-CLI:
  Sie können das Gleiche sehen, nur Berechtigungen, die sich auf SGT 4 beziehen, werden hinzugefügt.

```
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
```

- Über die WLC-CLI beim Verbinden des zweiten Clients mit 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
```

- AP-Ausgänge:

<#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
```

Fehlerbehebung

- Über die WLC-CLI:

show cts bereitstellung

show cts rollenbasierte Berechtigungen

IP-Zugriffslisten anzeigen

show cts ap sgt-info <ap_name>

- Vom AP:

show cts rollenbasierte sgt-map all

show cts rollenbasierte Berechtigungen

show cts-Zugriffslisten <acl-name>

show cts rollenbasierte sgt-map zusammenfassung

show cts-Zugriffslisten

Flexconnect-Client anzeigen

Clear CTS, rollenbasierte Zähler

Anzeige von CTS-rollenbasierten Zählern

- AP-Debugging:

- Aktiviert das Debuggen der CTS-Paketdurchsetzung:

debug cts-Durchsetzung

Laufzeit

- So überprüfen Sie CAPWAP-ACL-Ereignisse und Payload-bezogene Informationen:

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

debug capwap client acl

debug capwap client payload

debug capwap client error

debug dot11 Client-Verwaltungsinformationen

debug dot11 client management kritisch

debug dot11 client management error

debug dot11-Clientverwaltungsereignisse

debug generischer datapath client_ip_table/debug_acl

debug generischer datapath client_ip_table/debug

debug generisch datapath sgacl/debug

debug generischer Datenpfad sgacl/debug_sgt

debug generischer Datenpfad sgacl/debug_protocol

debug generischer Datenpfad sgacl/debug_permit

Laufzeit

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.