# Configureer TrustSec (SGT's) met ISE (inline tagging)

## Inhoud

Verifiëren

# Inleiding

Dit document beschrijft hoe u TrustSec op een Catalyst Switch en draadloze LAN-controller kunt configureren en verifiëren met de Identity Services Engine.

# Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco TrustSec (CTS)-componenten
- Basiskennis van de CLI-configuratie van Catalyst switches
- Basiskennis van GUI-configuratie van Cisco draadloze LAN-controllers (WLC)
- Ervaring met configuratie van Identity Services Engine (ISE)

## Vereisten

U moet Cisco ISE hebben geïmplementeerd in uw netwerk en eindgebruikers moeten zich verifiëren bij Cisco ISE met 802.1x (of een andere methode) wanneer ze verbinding maken met een draadloze of bekabelde switch. Cisco ISE kent aan hun verkeer een Security Group Tag (SGT) toe zodra deze aan uw draadloze netwerk zijn geverifieerd.

In ons voorbeeld worden eindgebruikers omgeleid naar het Cisco ISE Bring Your Own Device (BYOD)-portal en hebben ze een certificaat meegeleverd, zodat ze veilig toegang kunnen krijgen tot het draadloze netwerk met Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) nadat ze de stappen van het BYOD-portal hebben voltooid.

## Gebruikte componenten

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

- Cisco Identity Services Engine, versie 2.4
- Cisco Catalyst 3850 Switch, versie 3.7.5E
- Cisco WLC, versie 8.5.120.0
- Cisco Aironet draadloos access point in lokale modus

Voordat Cisco TrustSec wordt geïmplementeerd, moet u controleren of uw Cisco Catalyst Switch en/of Cisco WLC+AP-modellen + softwareversie ondersteuning heeft voor:

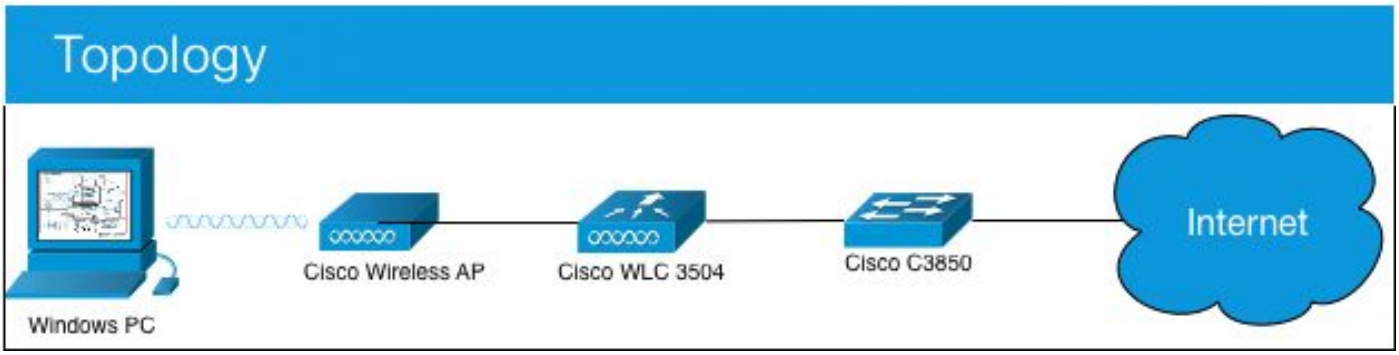
- TrustSec/Security Group-tags
- Inline tagging (indien niet, kunt u SXP gebruiken in plaats van Inline tagging)
- Statische IP-naar-SGT-toewijzingen (indien nodig)
- Statische Subnet-to-SGT-toewijzingen (indien nodig)
- Statische VLAN-naar-SGT-toewijzingen (indien nodig)

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




In dit voorbeeld, de WLC markeert de pakketten als SGT 15 indien van een Consultant, en + SGT 7 indien van een Medewerker.

De switch ontkent deze pakketten als ze van SGT 15 tot SGT 8 zijn (consultants kunnen geen toegang krijgen tot servers die als SGT 8 zijn getagd).

De switch staat die pakketten toe als zij van SGT 7 tot SGT 8 zijn (medewerkers kunnen tot servers toegang hebben die als SGT 8 worden geëtiketteerd).

## Doel

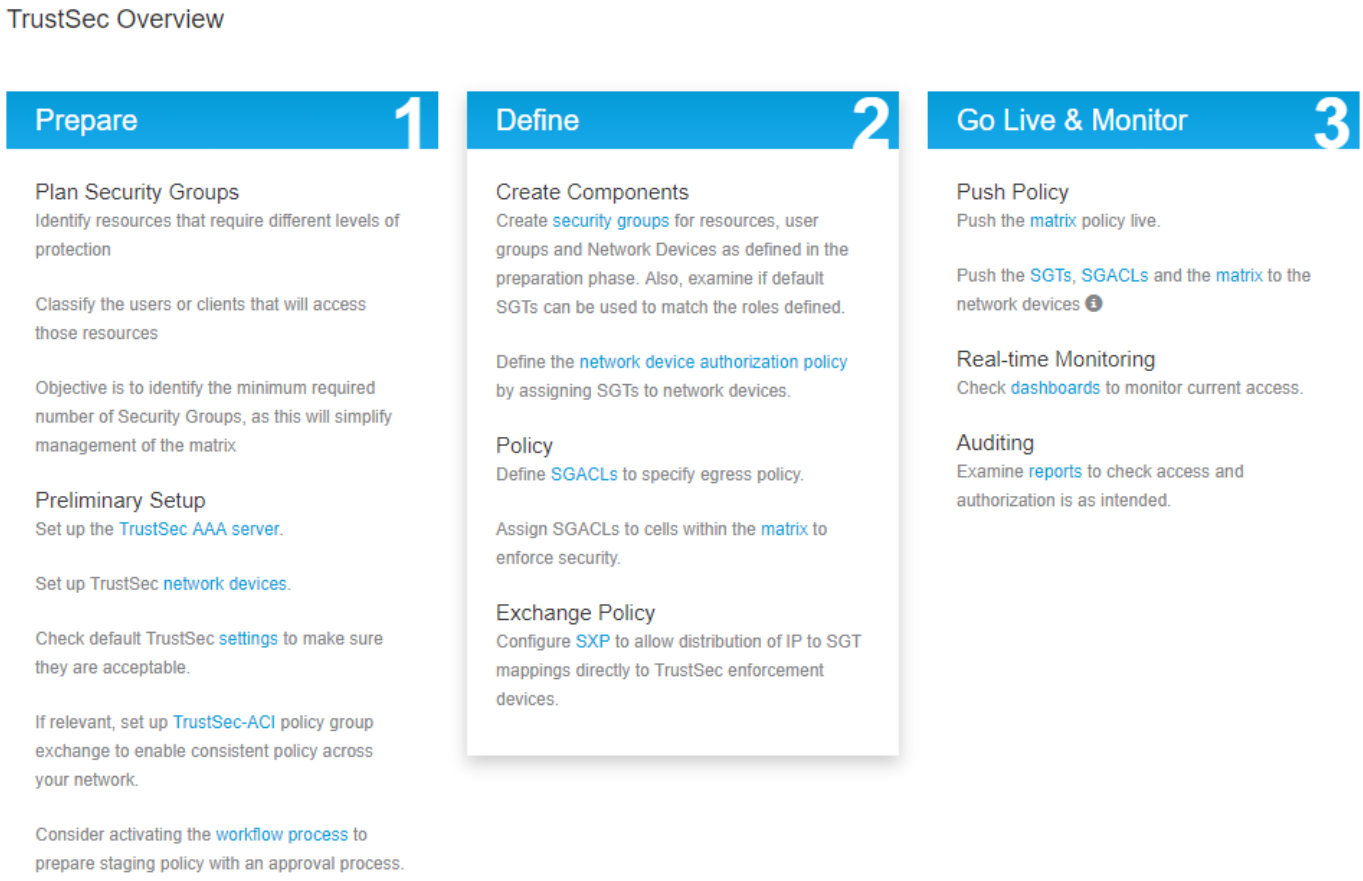
Laat iedereen toegang tot GuestSSID.
Laat Consultants werknemerSSID, maar met beperkte toegang.
Laat Werknemers toegang MedewerkerSSID met volledige toegang.

| Apparaat | IP-adres | VLAN |
|---|---|---|
| ISE | 10.201.214.230 | 463 |
| Catalyst Switch | 10.201.235.102 | 1115 |
| WLC | 10.201.214.229 | 463 |
| Access point | 10.201.214.138 | 455 |

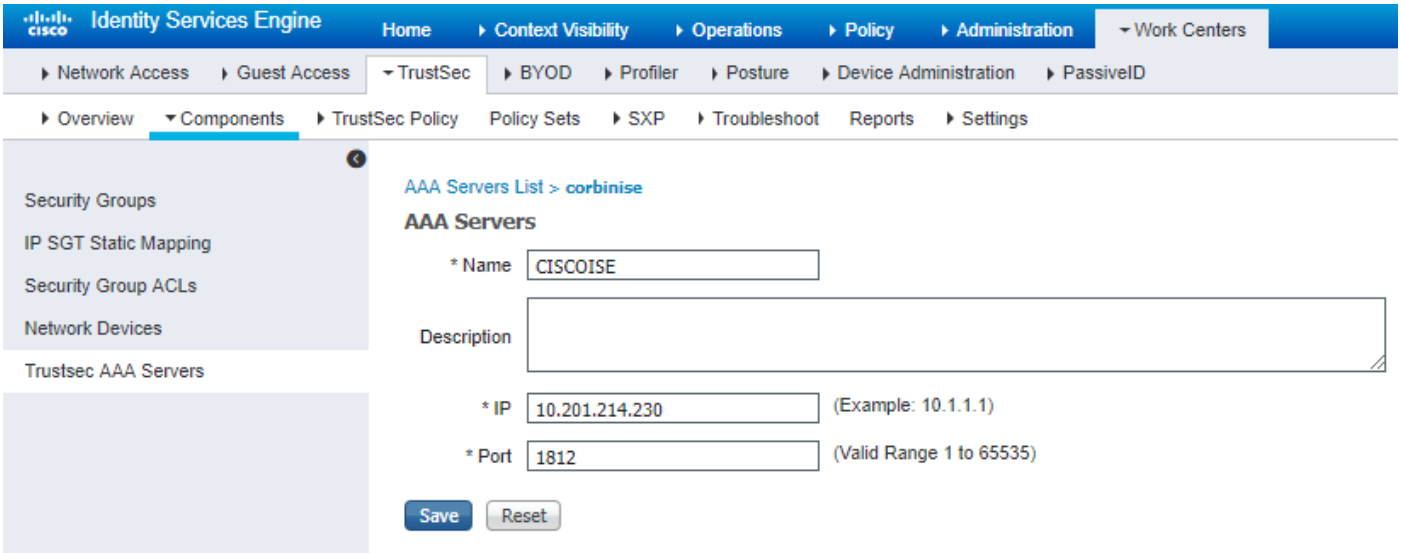
| Naam | Username | AD-groep | SG | SGT |
|---|---|---|---|---|
| Jason Smith | jsmid | Adviseurs | BYOD-consultants | 15 |
| Sally Smith | smid | Werknemers | BYOD-medewerkers | 7 |
| N.v.t. | N.v.t. | N.v.t. | TrustSEC_apparaten | 2 |

## Configuraties

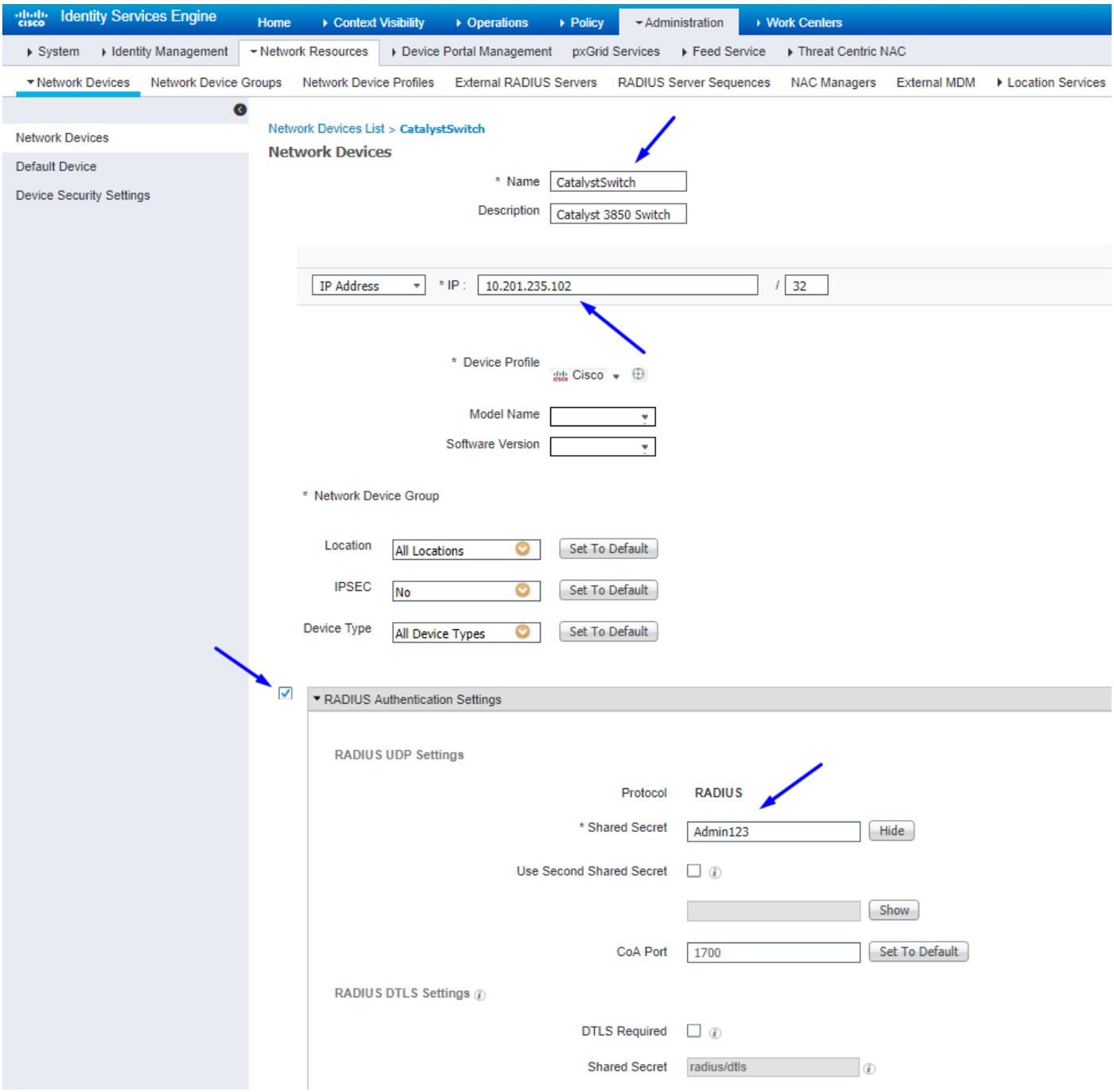
## TrustSec op ISE configureren




## Cisco ISE configureren als een TrustSec AAA-server

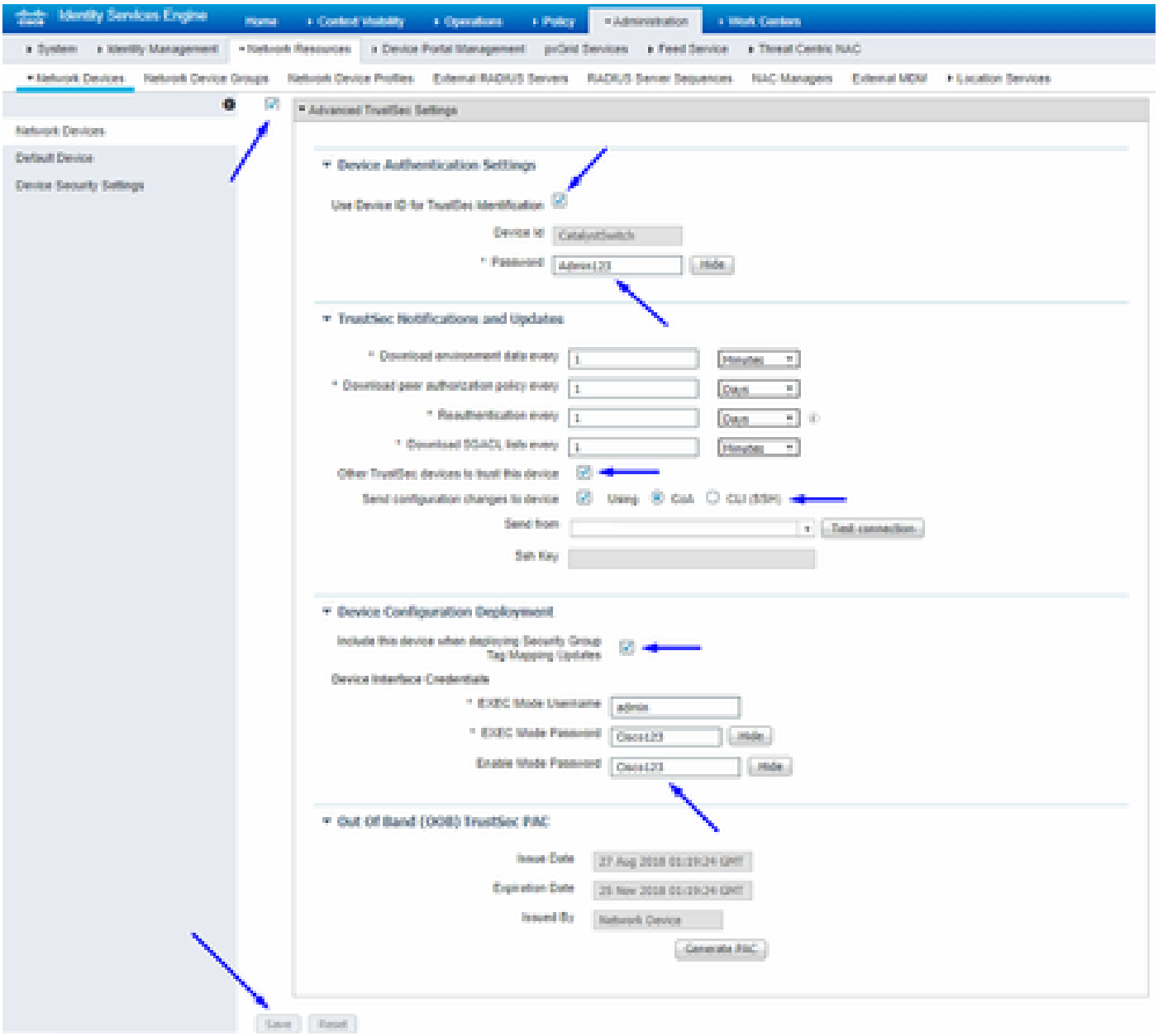


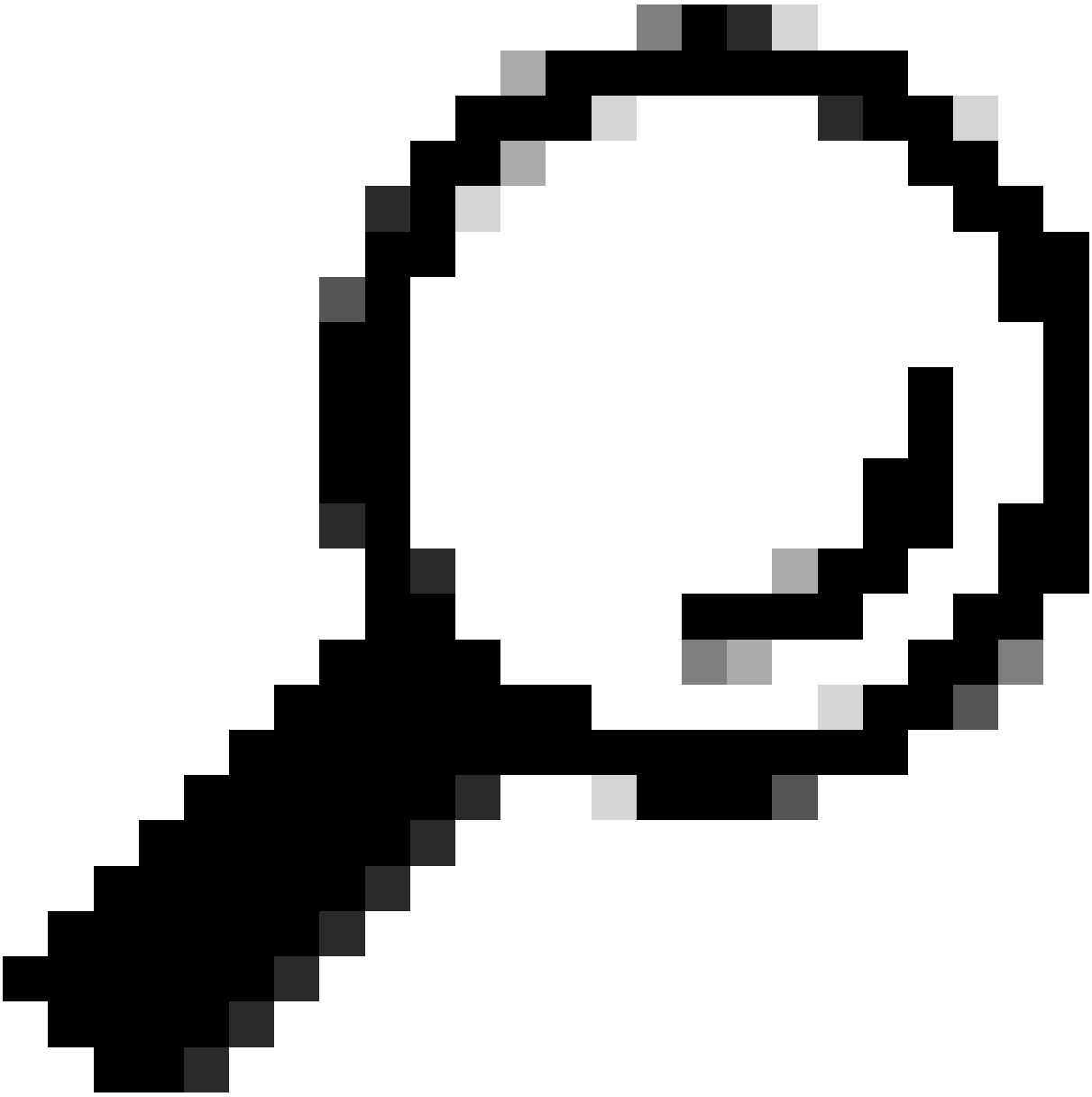

## De Switch configureren en controleren als RADIUS-apparaat wordt toegevoegd in Cisco ISE-software



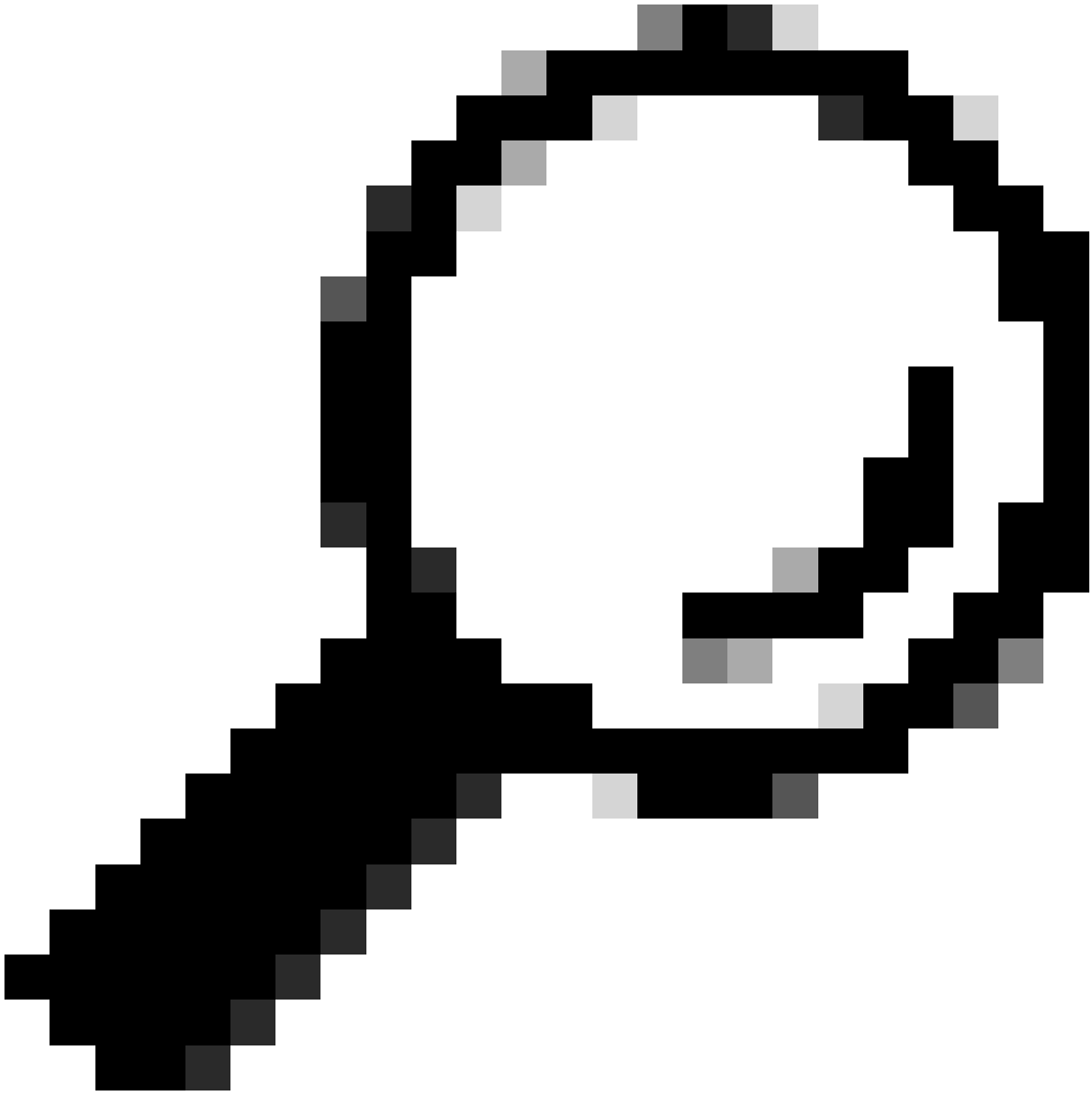

Configureer en controleer of WLC wordt toegevoegd als een TrustSec-apparaat in Cisco ISE

Voer uw inlogreferenties in voor SSH. Hiermee kan Cisco ISE de statische IP-naar-SGT toewijzingen aan de switch implementeren.
U maakt deze in de Cisco ISE-webGUI onder Work Centers > TrustSec > Components > IP SGT Static Mappings, zoals hier wordt getoond:


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
Network Devices
Default Device
Device Security Settings
Advanced TrustSec Settings
Device Authentication Settings
Use Device ID for TrustSec Identification
Device Id
CatalystSwitch
* Password
Admin123
Hide
TrustSec Notifications and Updates
* Download environment data every
1
Minutes
* Download peer authorization policy every
1
Days
* Reauthentication every
1
Days
* Download SGACL lists every
1
Minutes
Other TrustSec devices to trust this device
Send configuration changes to device
Using
CoA
CLI (SSH)
Send from
Test Connection
Ssh Key
Device Configuration Deployment
Include this device when deploying Security Group Tag Mapping Updates
Device Interface Credentials
* EXEC Mode Username
admin
* EXEC Mode Password
Cisco123
Hide
Enable Mode Password
Cisco123
Hide
Out Of Band (OOB) TrustSec PAC
Issue Date
27 Aug 2018 01:19:24 GMT
Expiration Date
25 Nov 2018 01:19:24 GMT
Issued By
Network Device
Generate PAC
Save
Reset

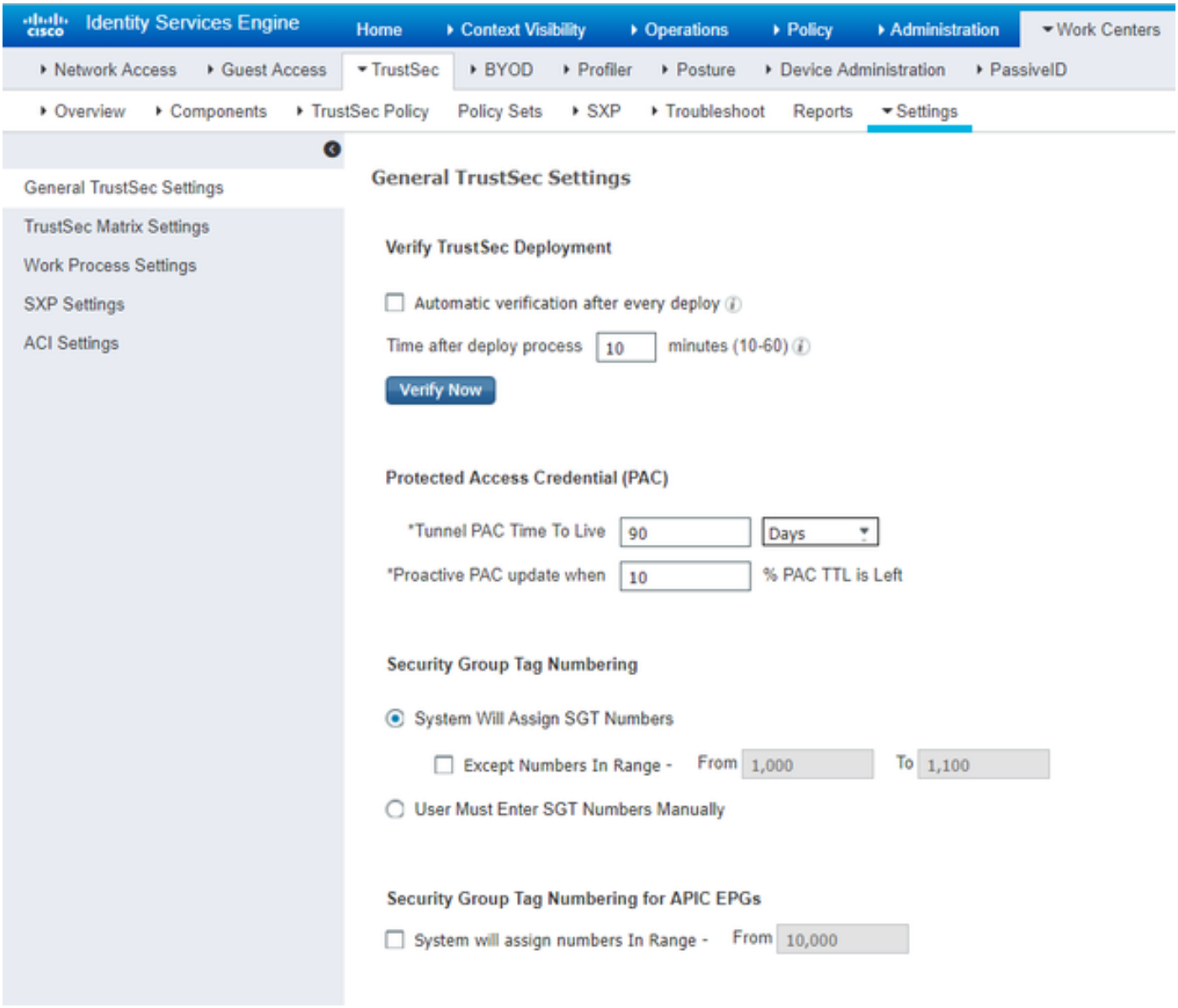


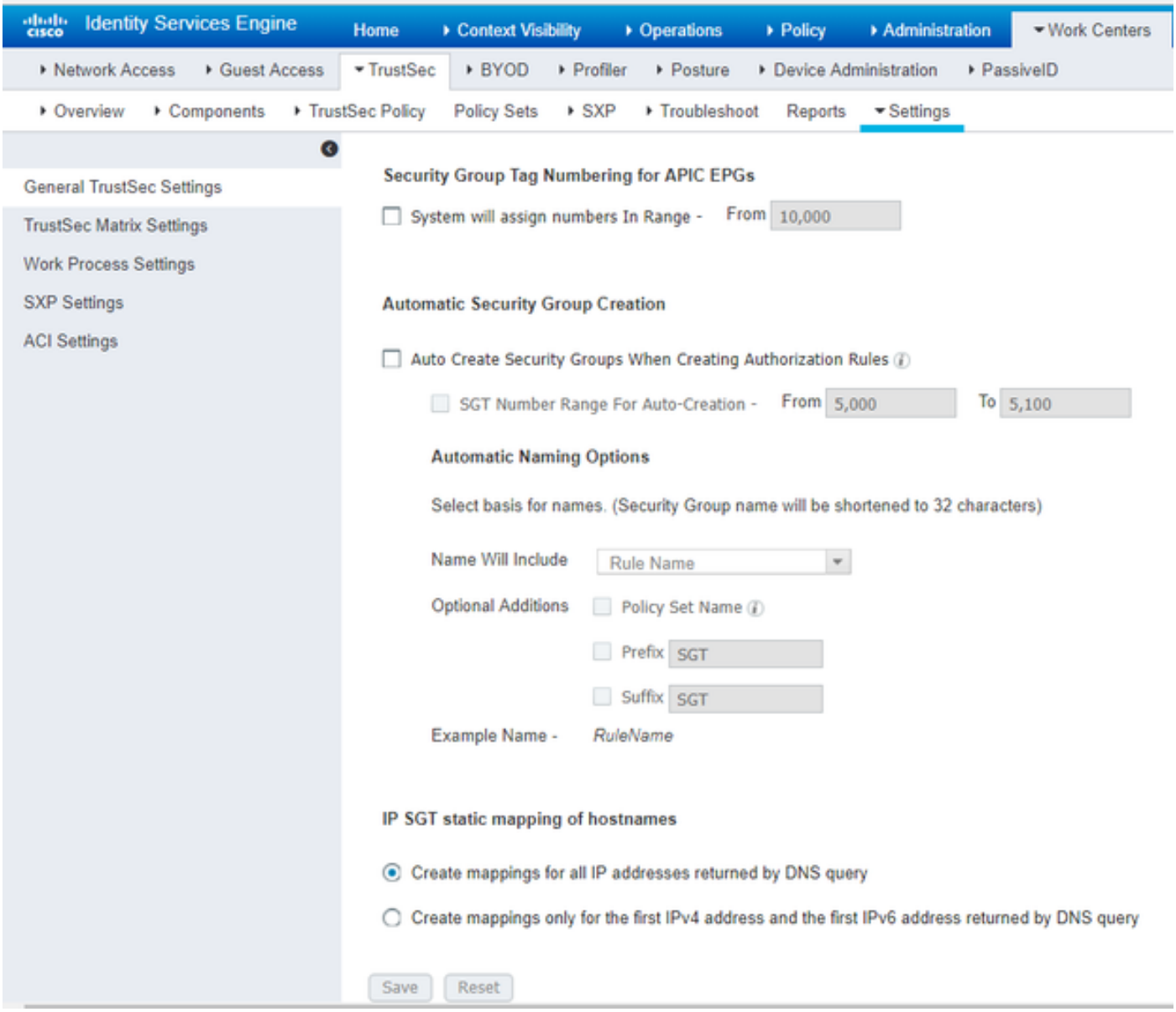
**Tip**: Als u nog geen SSH hebt geconfigureerd op uw Catalyst Switch, kunt u deze handleiding gebruiken: Hoe configureer je Secure Shell (SSH) op Catalyst Switch .



**Tip**: als u Cisco ISE niet wilt inschakelen om uw Catalyst Switch via SSH te openen, kunt u statische IP-naar-SGT-toewijzingen maken op de Catalyst Switch met de CLI (zie hier een stap).

Controleer de standaardinstellingen van TrustSec om te controleren of deze acceptabel zijn (optioneel)

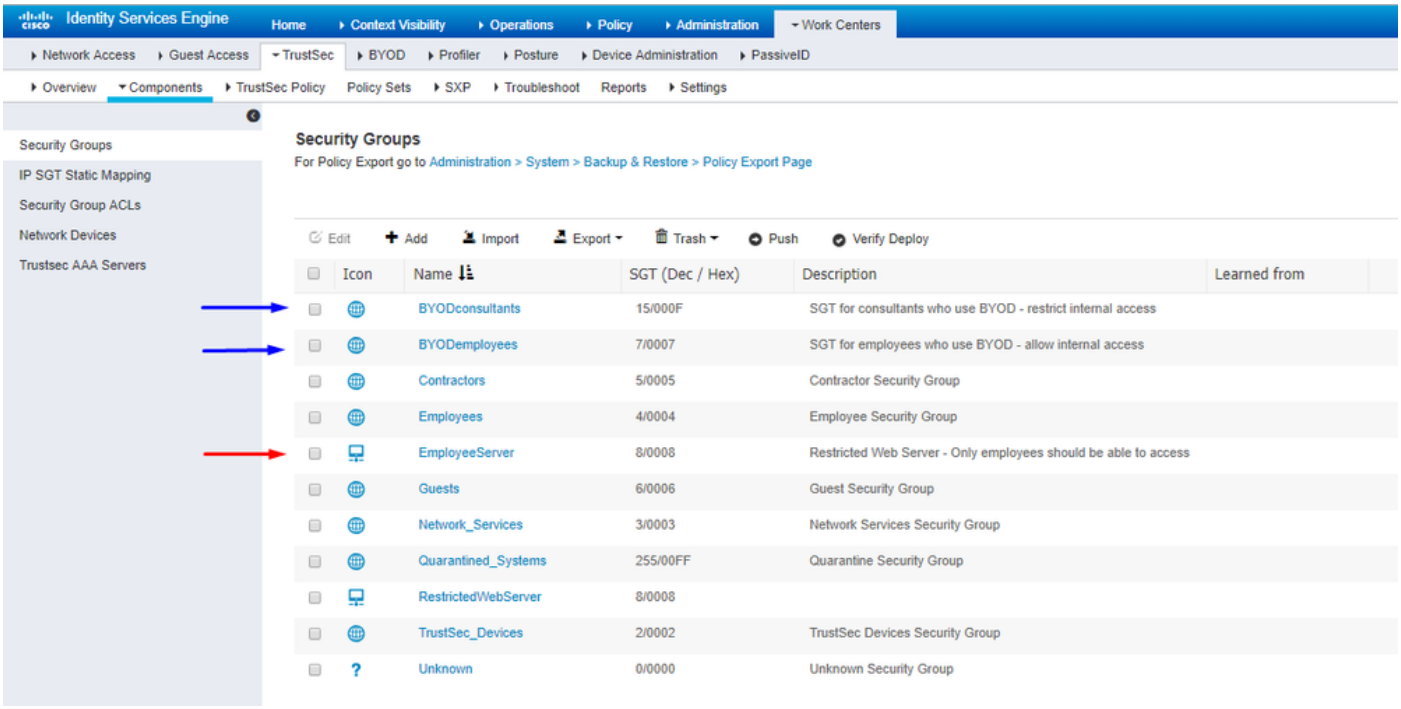

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Components
TrustSec Policy
Policy Sets
SXP
Troubleshoot
Reports
Settings
General TrustSec Settings
TrustSec Matrix Settings
Work Process Settings
SXP Settings
ACI Settings
General TrustSec Settings
Verify TrustSec Deployment
Automatic verification after every deploy
Time after deploy process 10 minutes (10-60)
Verify Now
Protected Access Credential (PAC)
*Tunnel PAC Time To Live 90 Days
*Proactive PAC update when 10 % PAC TTL is Left
Security Group Tag Numbering
System Will Assign SGT Numbers
Except Numbers In Range - From 1,000 To 1,100
User Must Enter SGT Numbers Manually
Security Group Tag Numbering for APIC EPGs
System will assign numbers In Range - From 10,000




Security Group-tags voor draadloze gebruikers maken

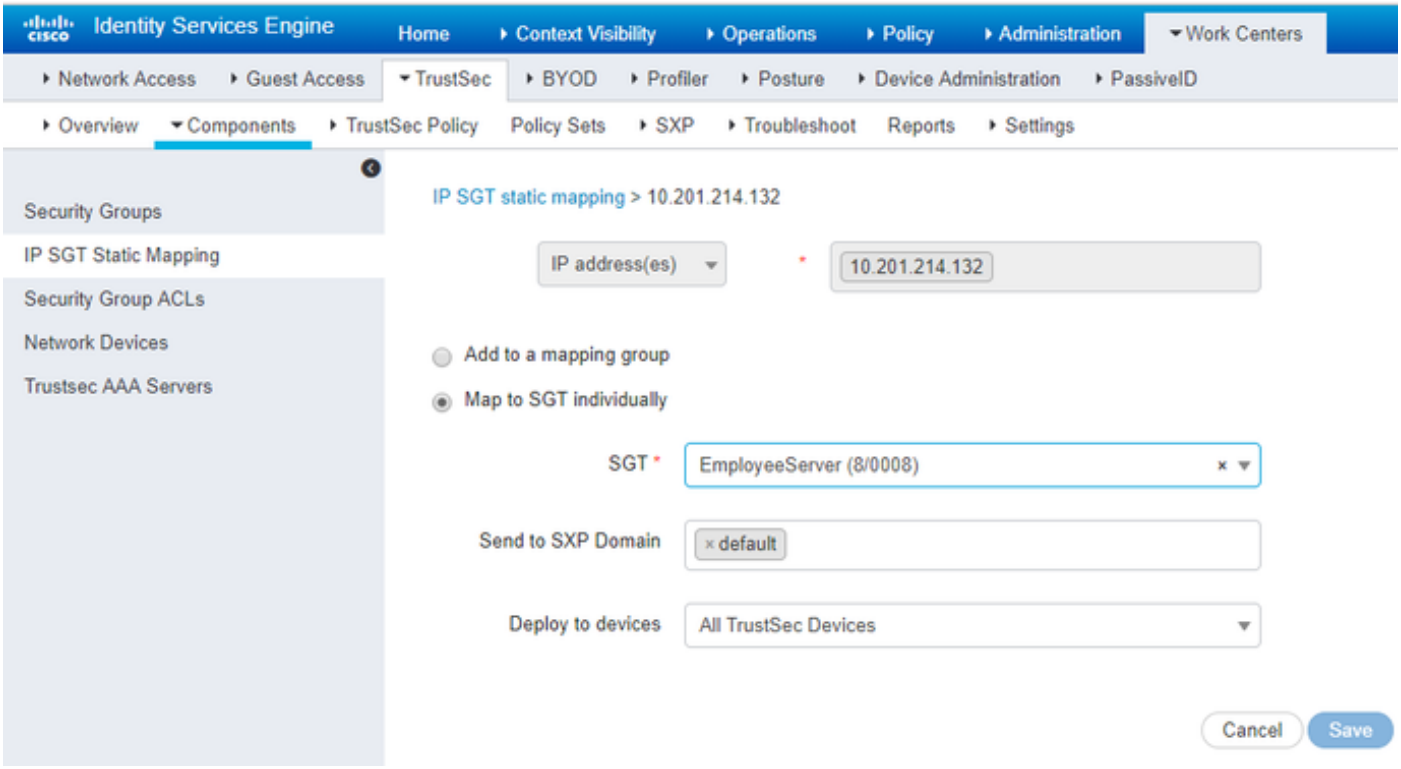
Security Group voor BYODconsultants maken - SGT 15

Security Group voor BYOD-medewerkers maken - SGT 7

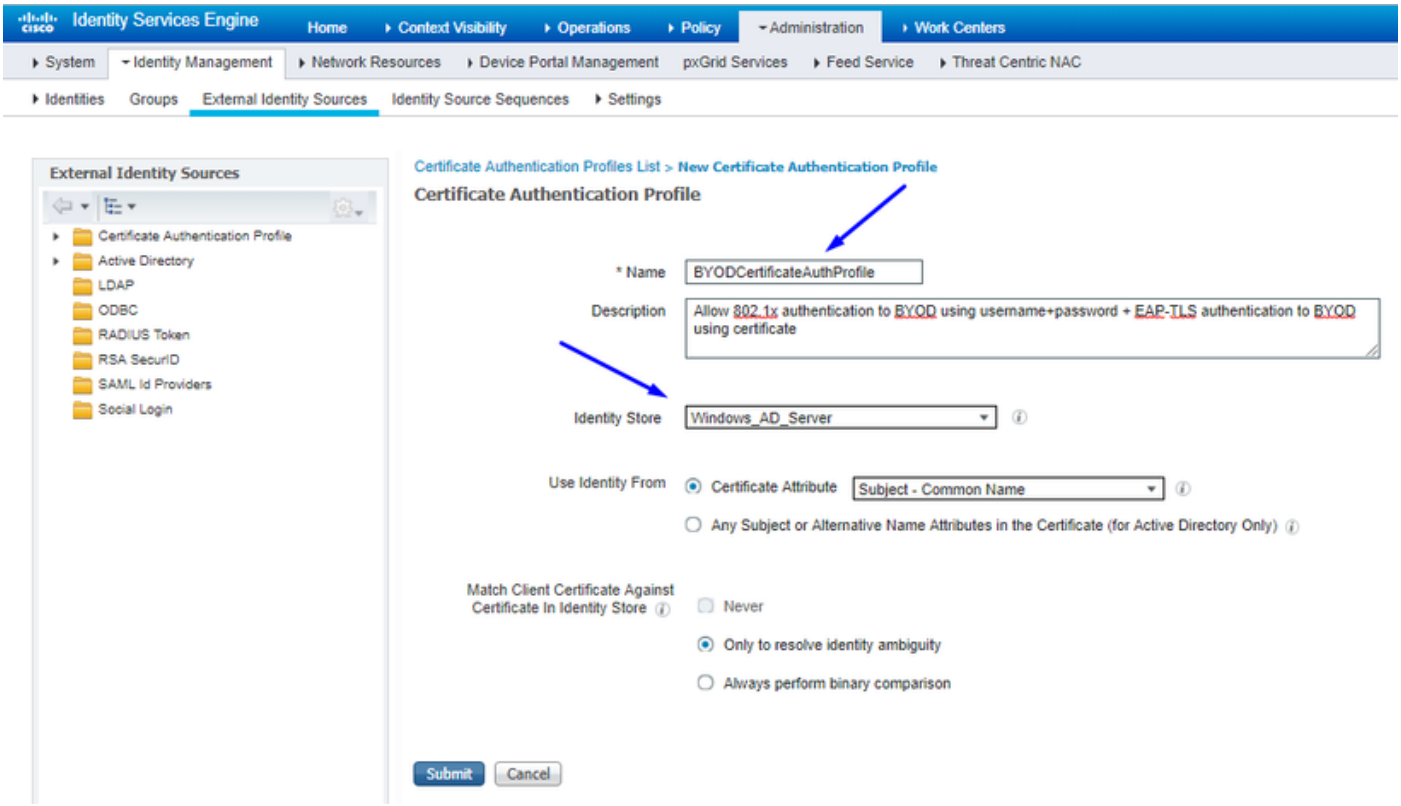



Statische IP-naar-SGT-toewijzing maken voor de beperkte webserver

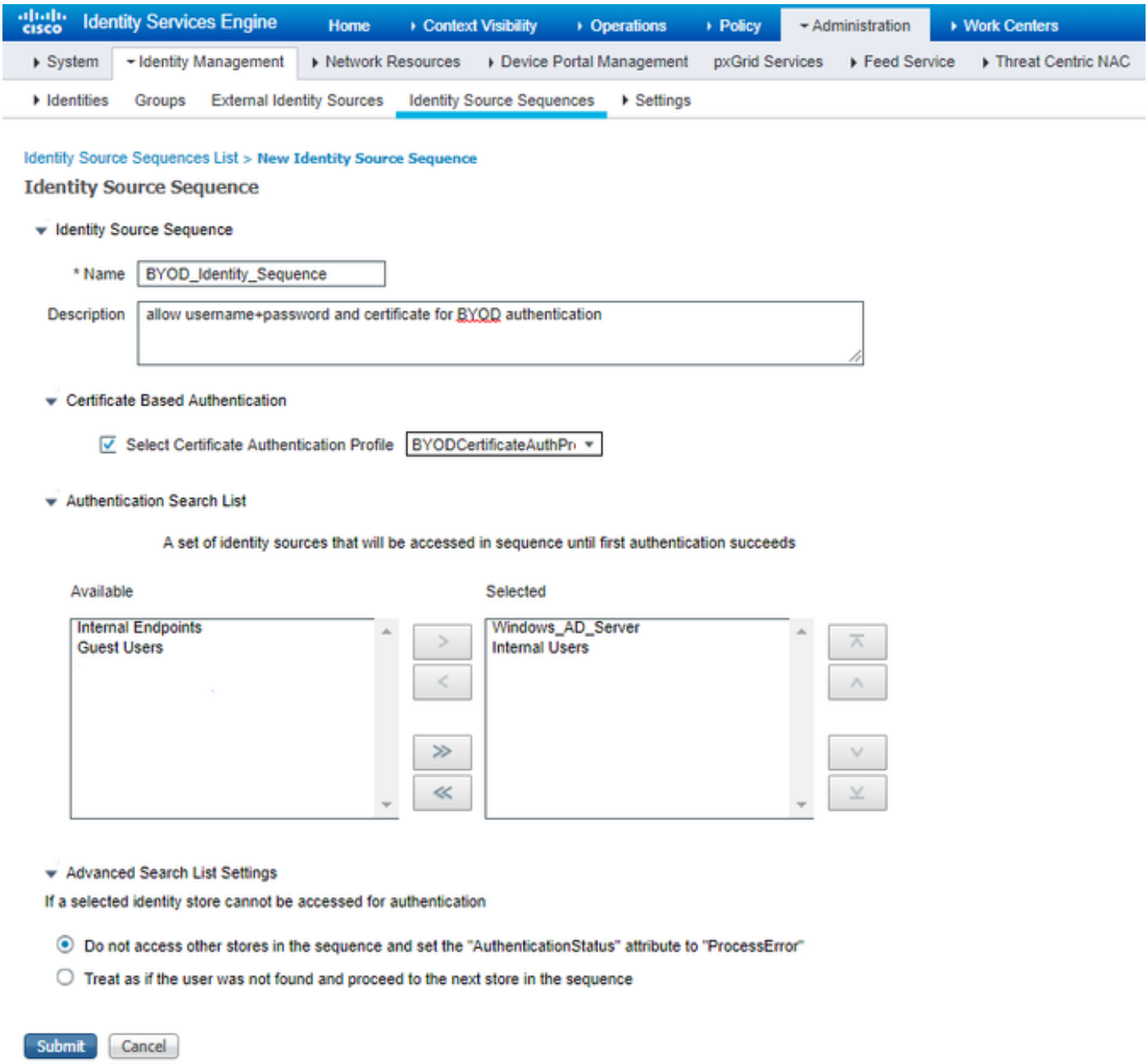
Doe dit voor andere IP-adressen of subnetten in uw netwerk die niet worden geverifieerd naar Cisco ISE met MAC-verificatie-omzeiling (MAB), 802.1x, profielen enzovoort.




Certificaatverificatieprofiel maken

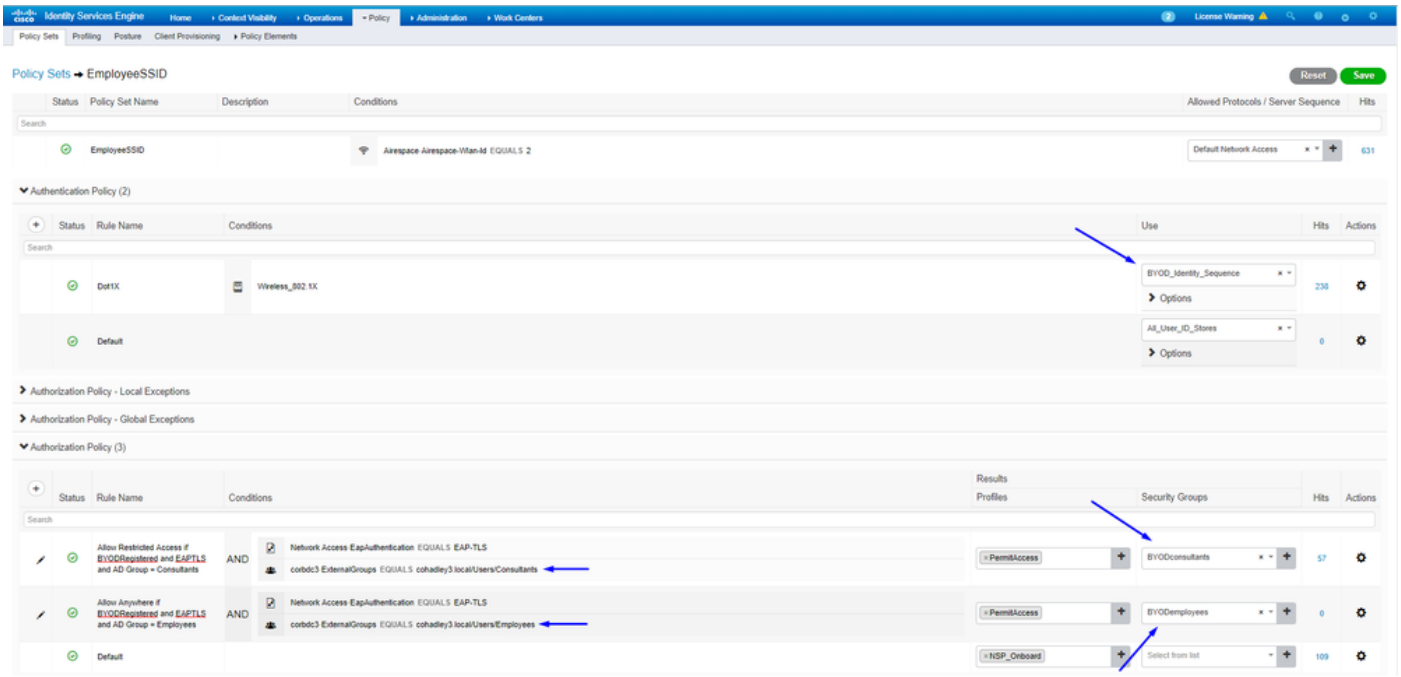



Creëer een Identity Source Sequence met het Certificaatverificatieprofiel van Vóór

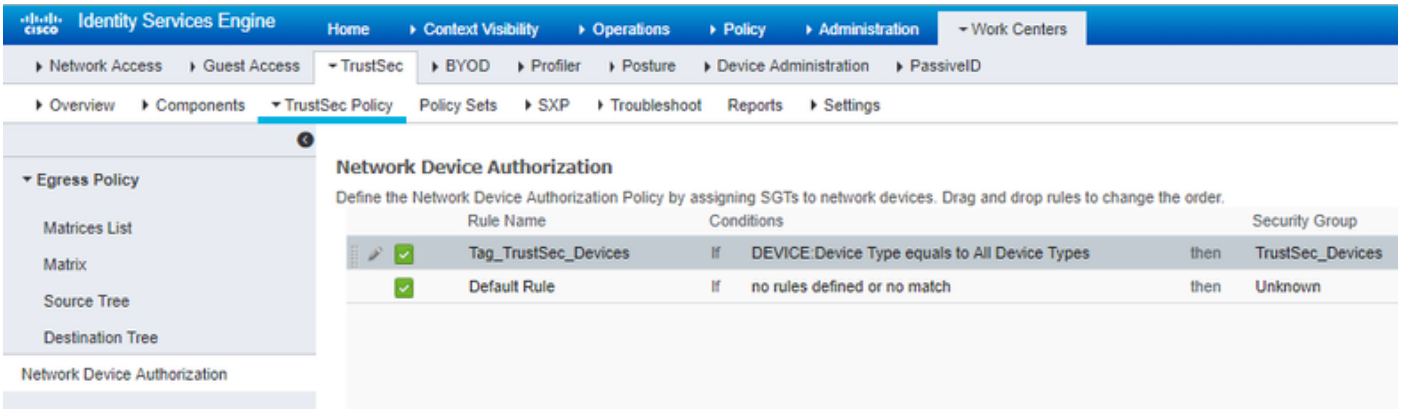



Wijs draadloze gebruikers (werknemers en consultants) een geschikt SGT toe

| Naam | Username | AD-groep | SG | SGT |
|---|---|---|---|---|
| Jason Smith | jsmid | Adviseurs | BYOD-consultants | 15 |
| Sally Smith | smid | Werknemers | BYOD-medewerkers | 7 |
| N.v.t. | N.v.t. | N.v.t. | TrustSEC_apparaten | 2 |

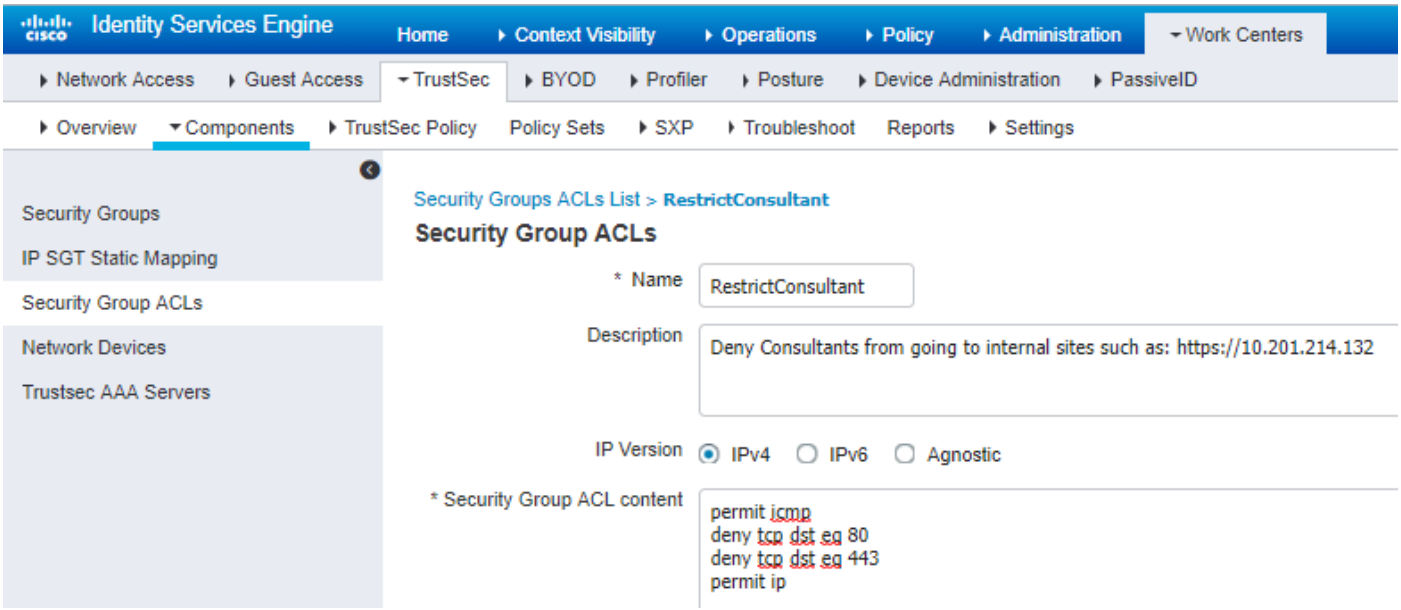



SGT's toewijzen aan de feitelijke apparaten (Switch en WLC)

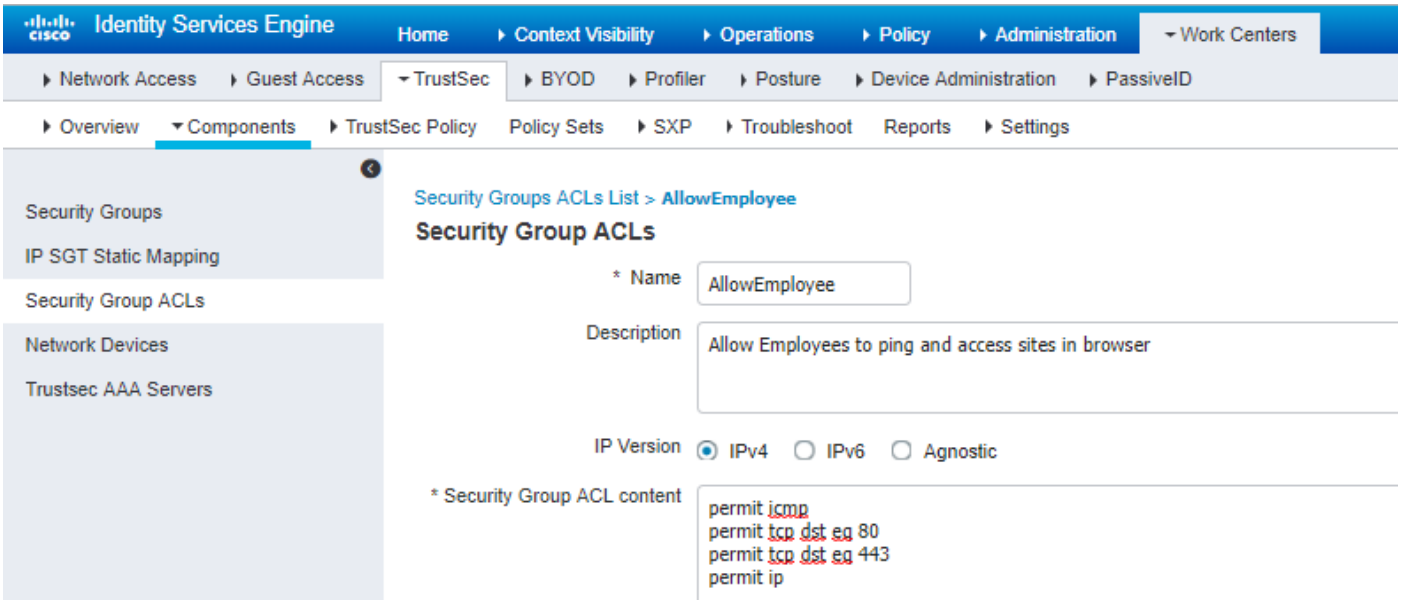



SGACL’s definiëren om het uitgaande beleid te specificeren

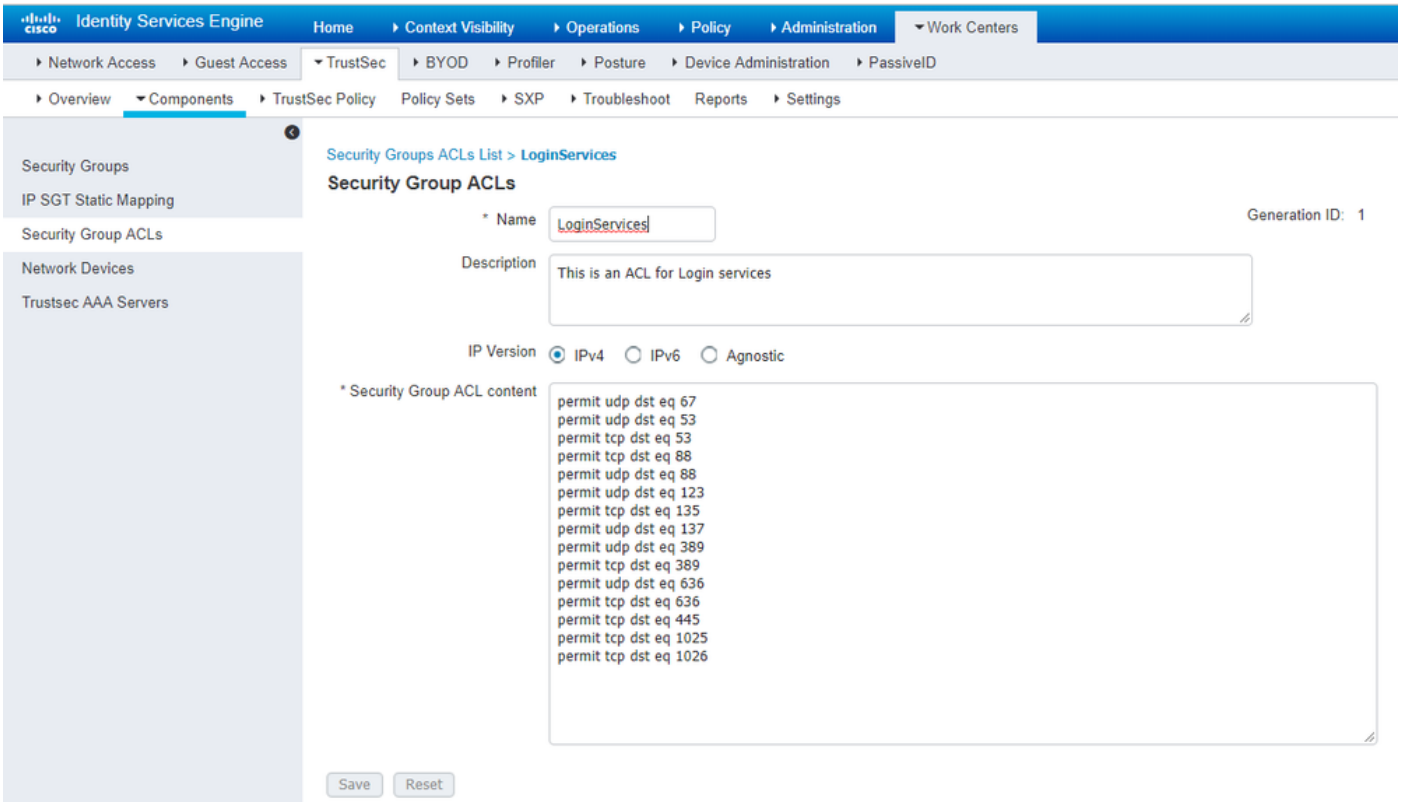
Laat consultants overal externe toegang toe, maar beperk interne:



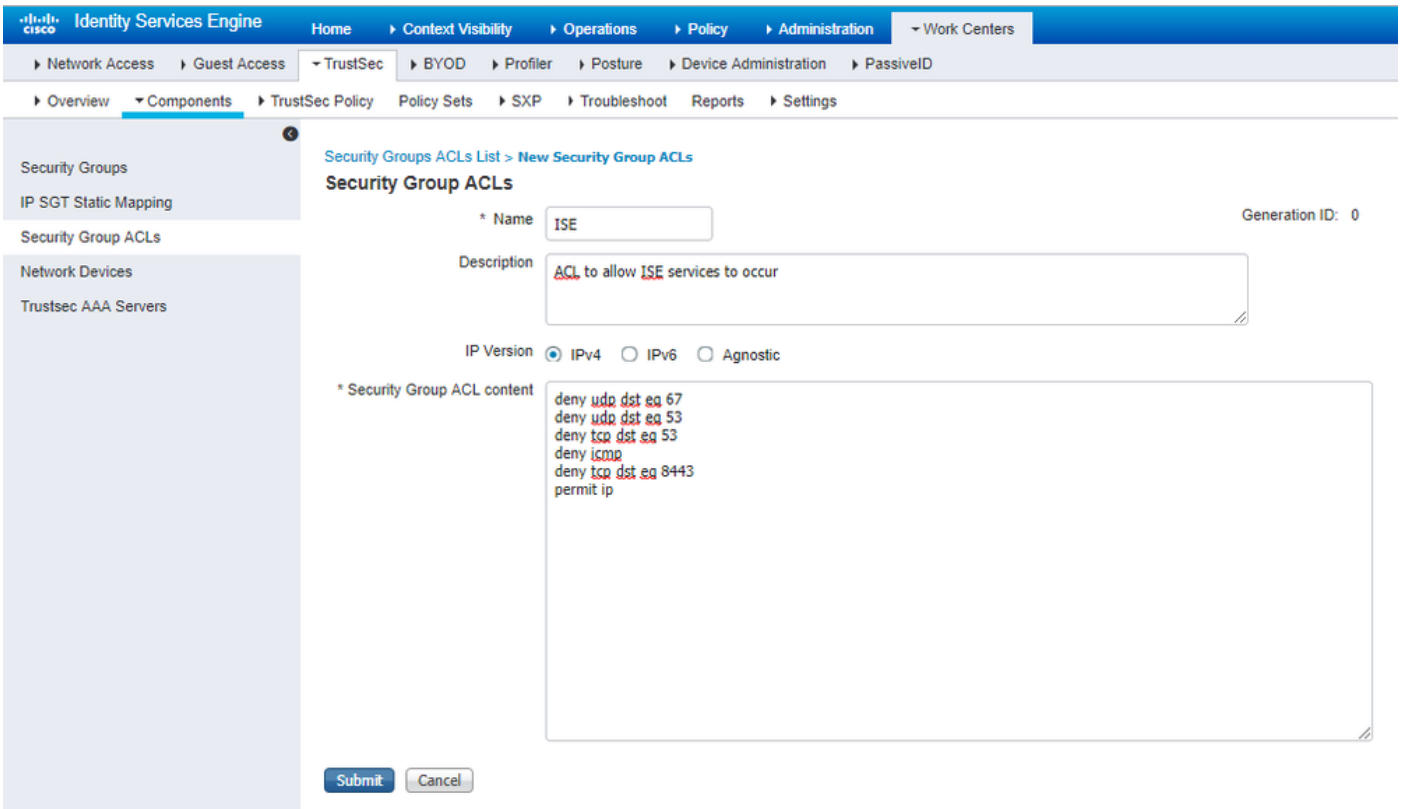

Werknemers toegang geven tot externe en interne werkplekken:




Geef andere apparaten toegang tot basisdiensten (optioneel):



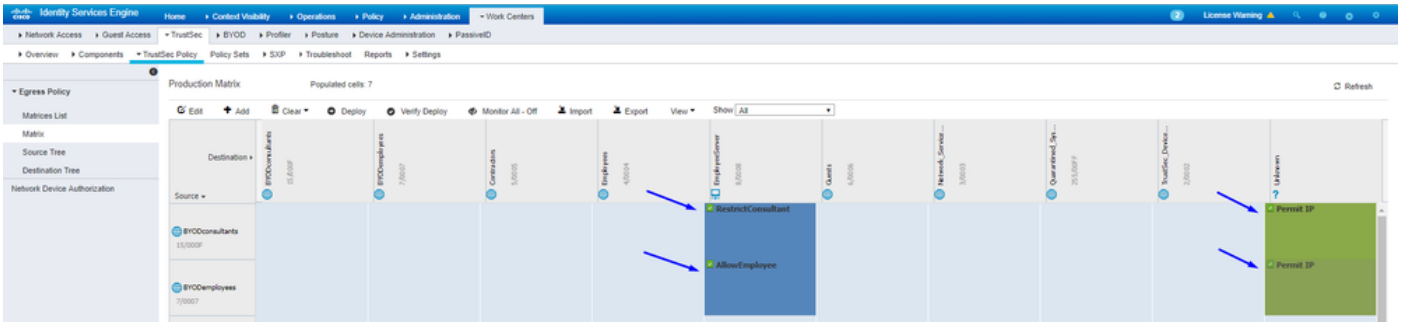

Richt alle eindgebruikers door naar Cisco ISE (voor BYOD portal omleiding). Omvat geen DNS-, DHCP-, ping- of Webex-verkeer, aangezien die niet naar Cisco ISE kunnen gaan:



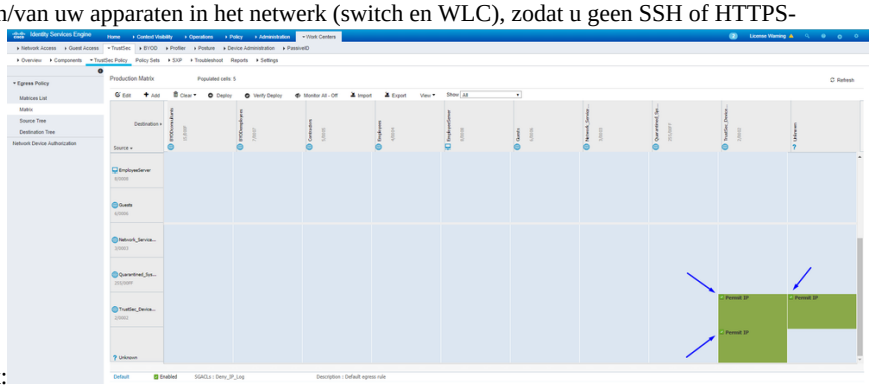

Handhaaf uw ACL's op de TrustSec Policy Matrix in Cisco ISE-software

Laat Consultants overal externe toegang toe, maar beperk interne webservers, zoals https://10.201.214.132

Werknemers toegang geven tot externe sites en interne webservers toestaan:

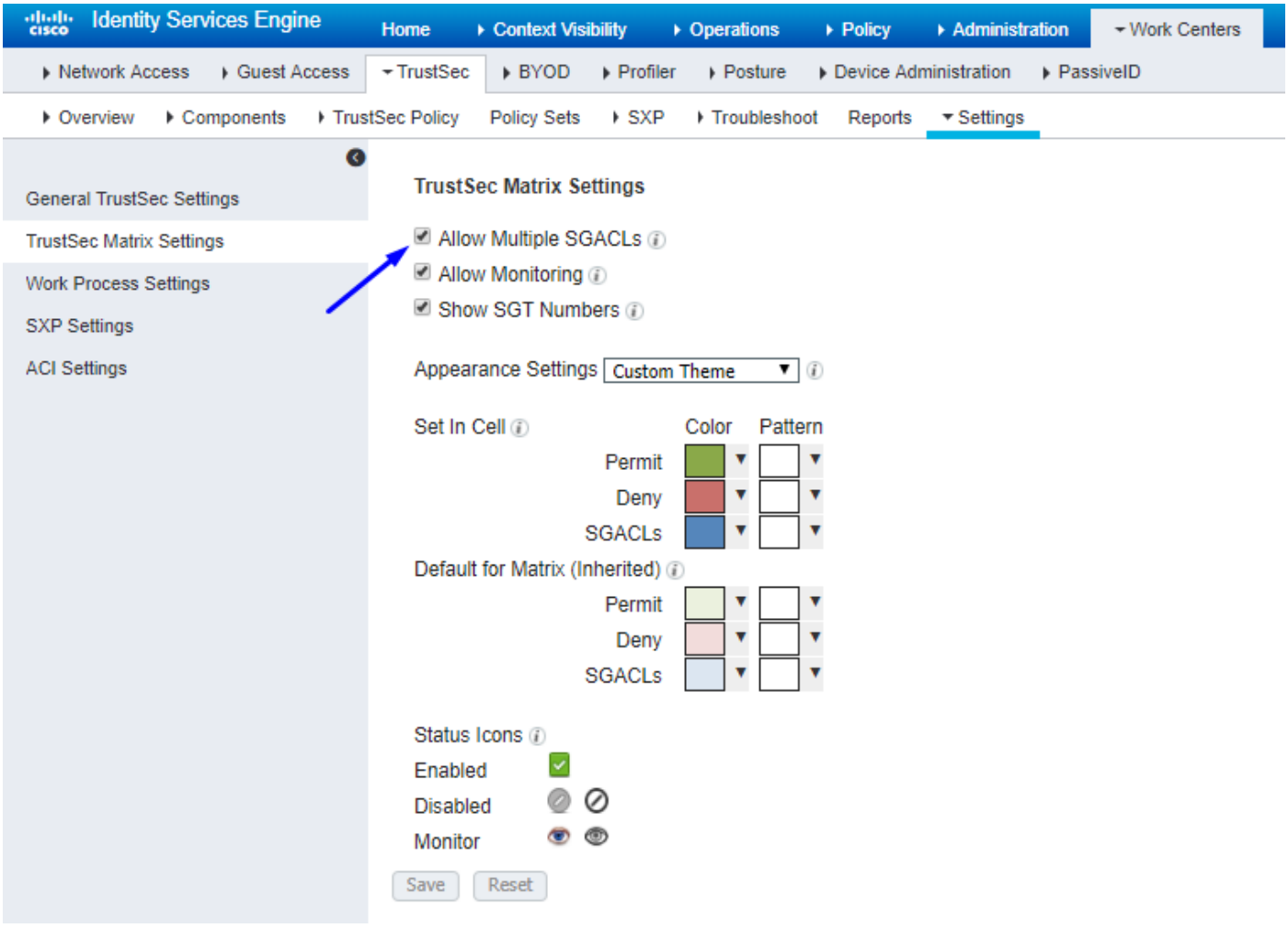


Sta beheerverkeer (SSH, HTTPS en CAPWAP) toe aan/van uw apparaten in het netwerk (switch en WLC), zodat u geen SSH of HTTPS-

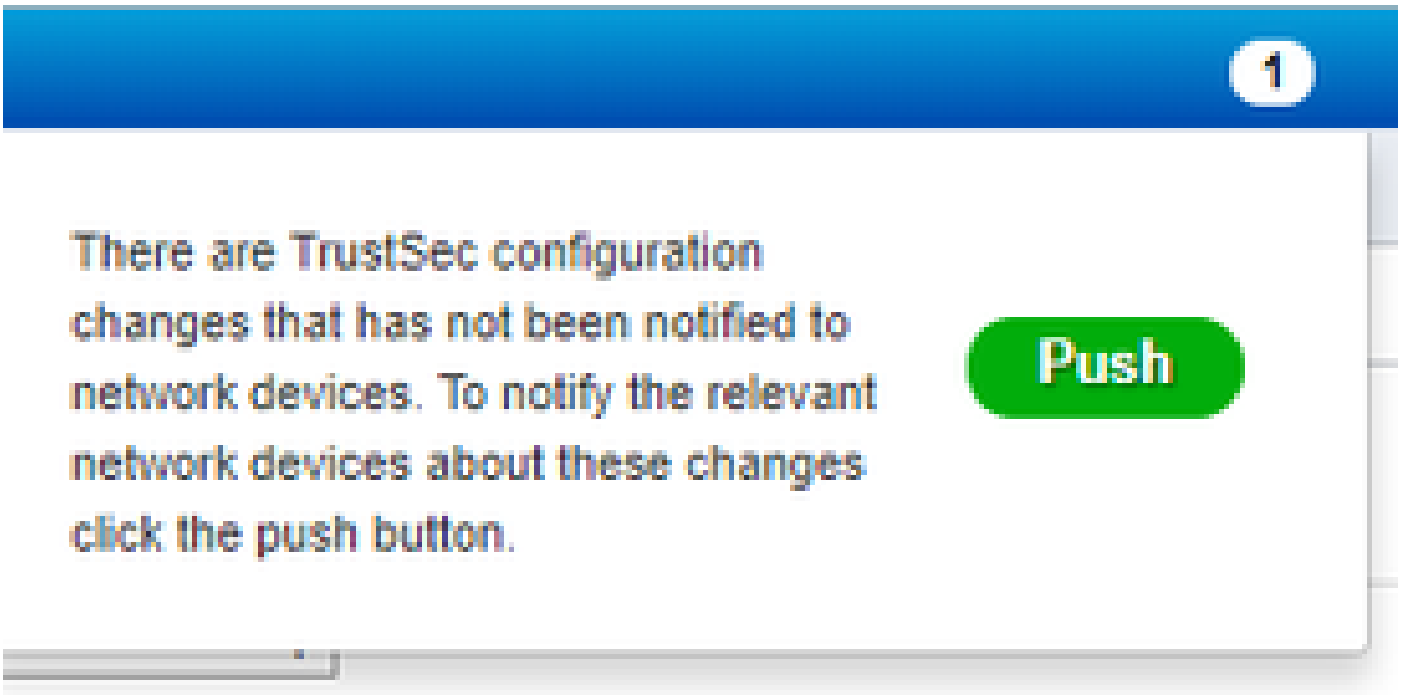


toegang verliest zodra u Cisco TrustSec implementeert:

Cisco ISE inschakelen Allow Multiple SGACLs:

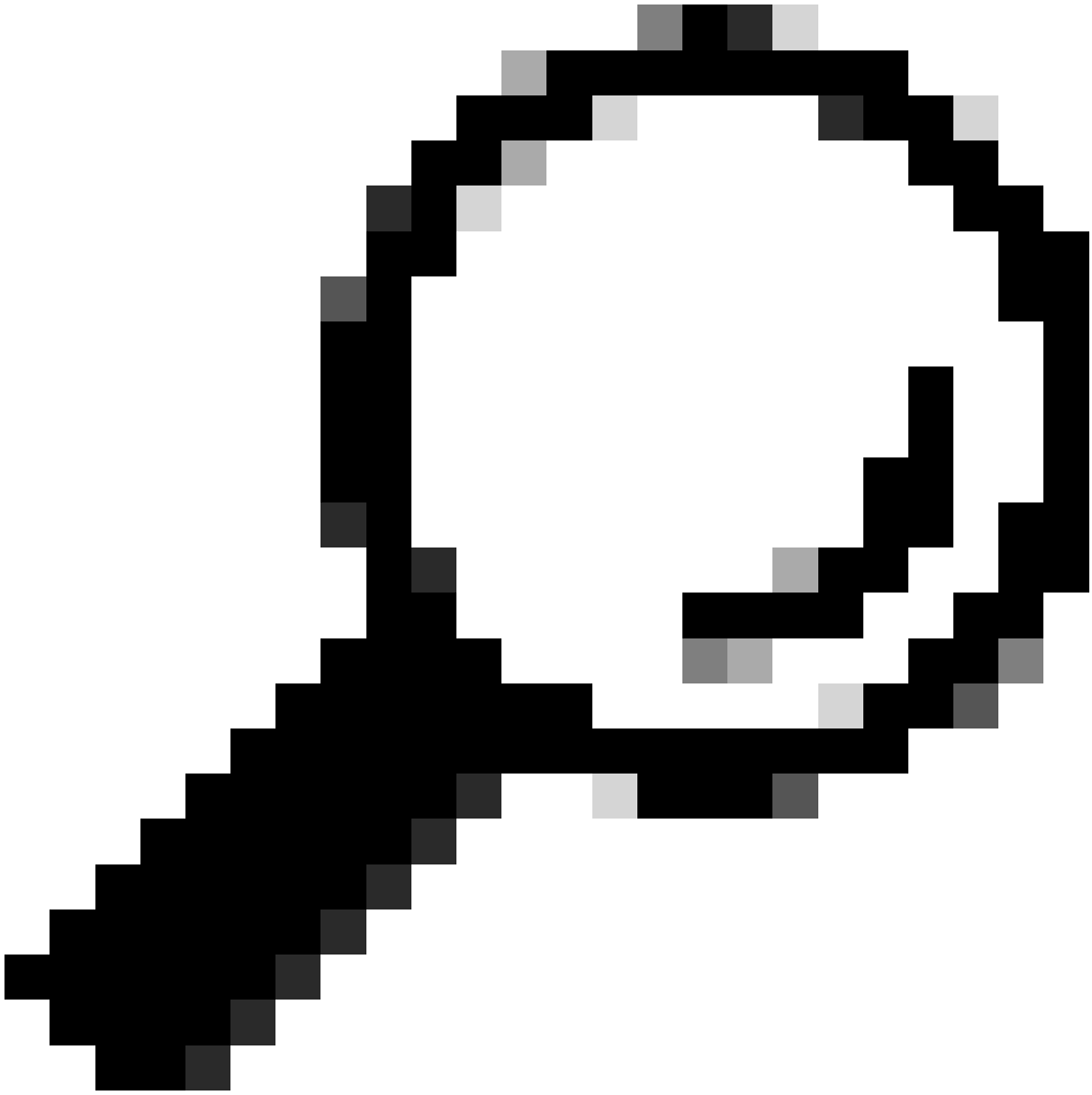


Klik Push in de rechterbovenhoek van Cisco ISE om uw configuratie naar beneden te drukken naar uw apparaten. U moet dit later ook opnieuw doen:




Configureer TrustSec op Catalyst Switch

Switch configureren voor gebruik van Cisco TrustSec voor AAA op Catalyst Switch



**Tip**: dit document gaat ervan uit dat uw draadloze gebruikers al met BYOD zijn geslaagd door Cisco ISE voordat de configuratie hier wordt weergegeven.

De opdrachten die in vet zijn weergegeven, zijn al eerder geconfigureerd (zodat BYOD Wireless met ISE kan werken).

<#root>

**CatalystSwitch(config)#aaa new-model**

**CatalystSwitch(config)#aaa server radius policy-device**

**CatalystSwitch(config)#ip device tracking**

**CatalystSwitch(config)#radius server CISCOISE**

**CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813**

CatalystSwitch(config)#aaa group server radius AAASERVER
CatalystSwitch(config-sg-radius)#server name CISCOISE

CatalystSwitch(config)#aaa authentication dot1x default group radius
CatalystSwitch(config)#cts authorization list SGLIST
CatalystSwitch(config)#aaa authorization network SGLIST group radius

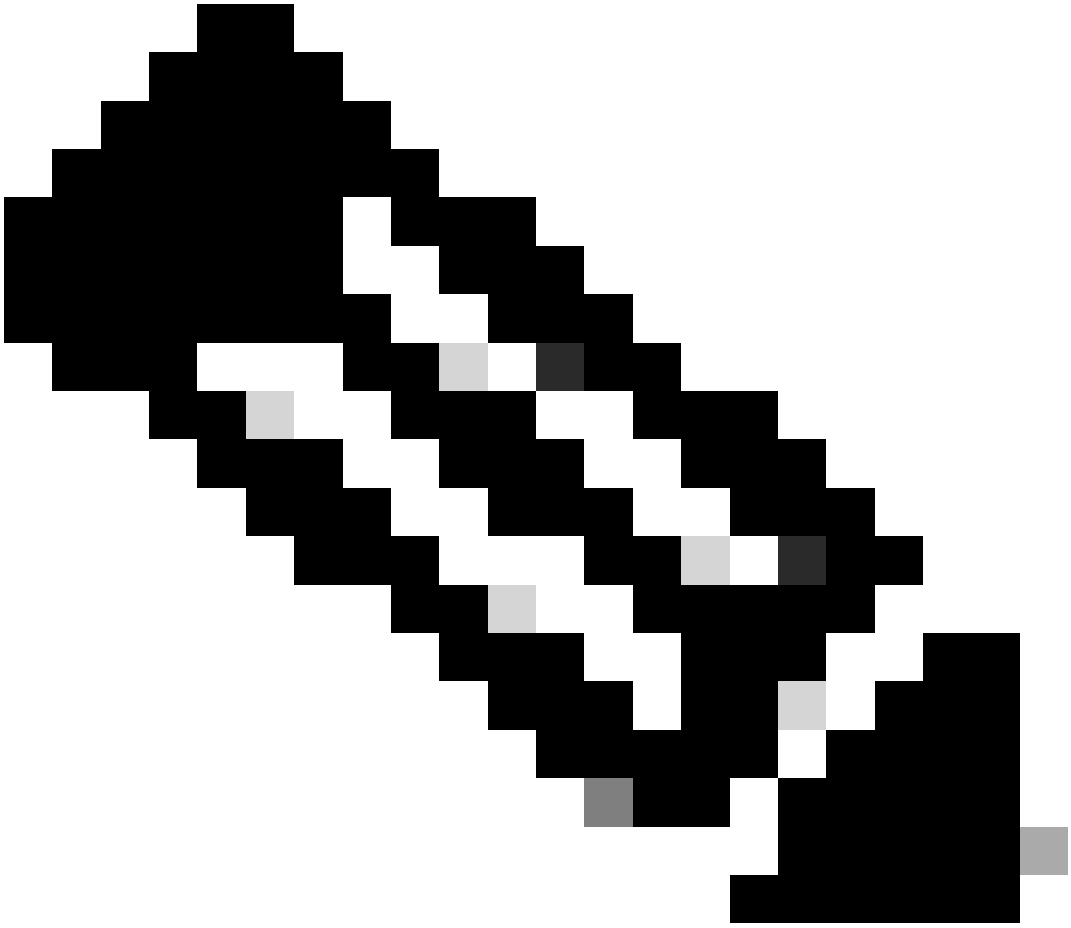
**CatalystSwitch(config)#aaa authorization network default group AAASERVER**

**CatalystSwitch(config)#aaa authorization auth-proxy default group AAASERVER**

**CatalystSwitch(config)#aaa accounting dot1x default start-stop group AAASERVER**

**CatalystSwitch(config)#aaa server radius policy-device**

CatalystSwitch(config)#aaa server radius dynamic-author
CatalystSwitch(config-locsvr-da-radius)#client 10.201.214.230 server-key Admin123



**Opmerking**: de PAC-toets moet dezelfde zijn als het RADIUS-gedeelde geheim dat u in de **Administration > Network Devices > Add Device > RADIUS Authentication Settings** sectie hebt opgegeven.

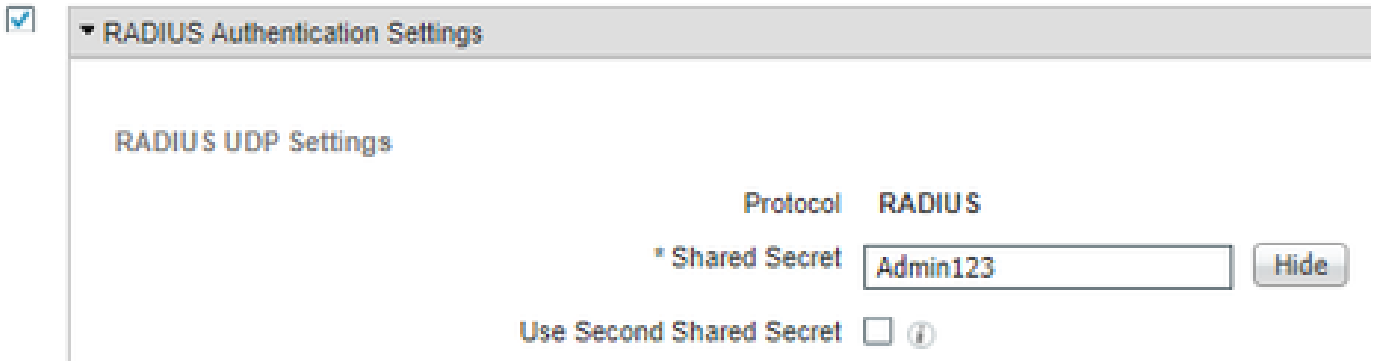
<#root>

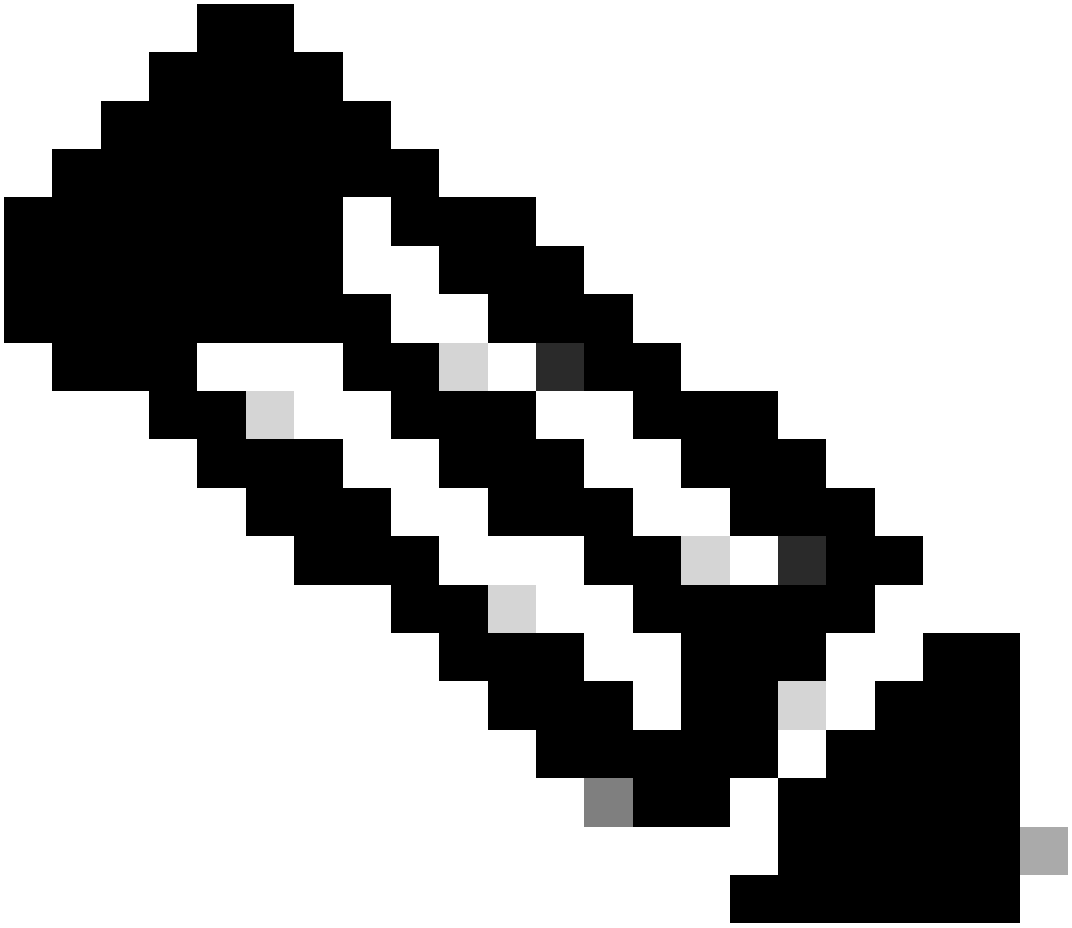
```
CatalystSwitch(config)#radius-server attribute 6 on-for-login-auth

CatalystSwitch(config)#radius-server attribute 6 support-multiple
```

```
CatalystSwitch(config)#radius-server attribute 8 include-in-access-req


CatalystSwitch(config)#radius-server attribute 25 access-request include


CatalystSwitch(config)#radius-server vsa send authentication
CatalystSwitch(config)#radius-server vsa send accounting

CatalystSwitch(config)#dot1x system-auth-control
```

De PAC-toets configureren onder de RADIUS-server om de Switch te verifiëren naar Cisco ISE

CatalystSwitch(config)#radius server CISCOISE
CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813
CatalystSwitch(config-radius-server)#pac key Admin123



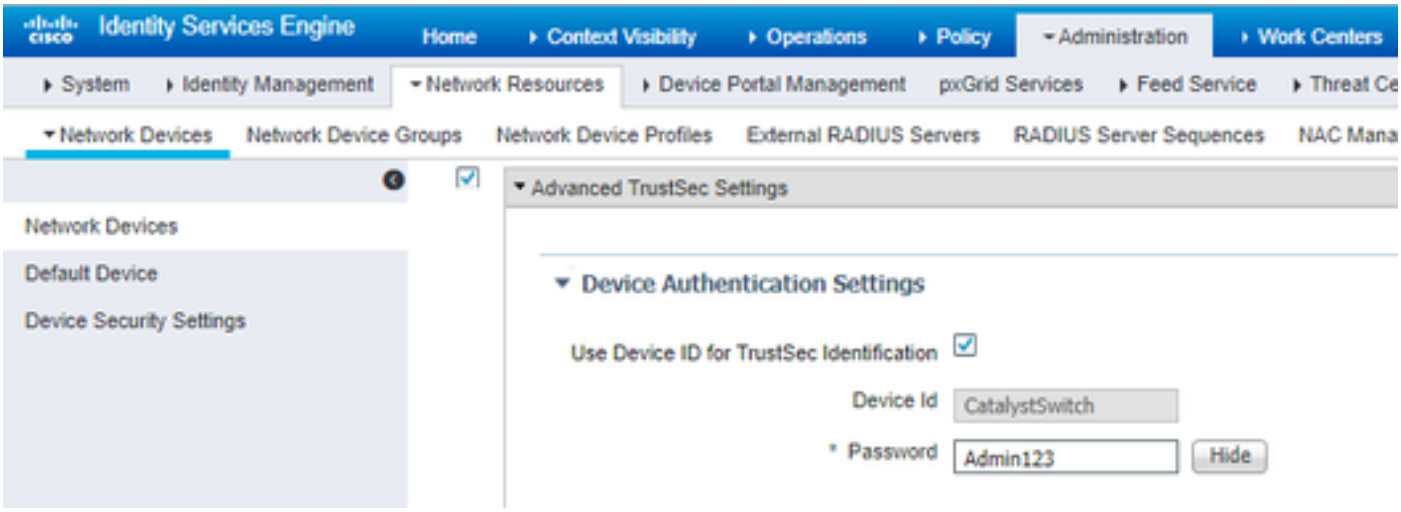


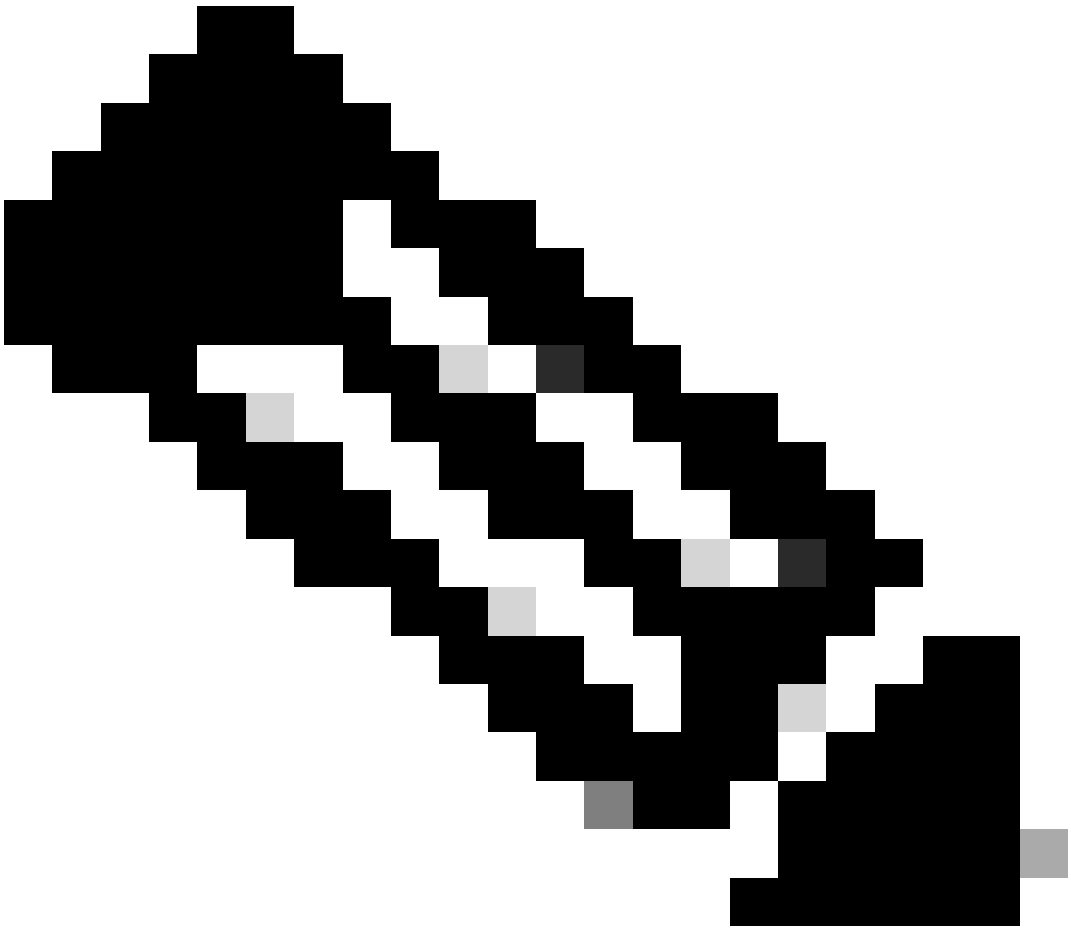
**Opmerking**: de PAC-toets moet gelijk zijn aan het RADIUS gedeelde geheim dat u in de **Administration > Network Devices > Add Device > RADIUS Authentication Settings** sectie in Cisco ISE hebt opgegeven (zoals in de schermopname).

---

CTS-referenties configureren om de Switch te verifiëren naar Cisco ISE

CatalystSwitch#cts credentials id CatalystSwitch password Admin123



Administration > Network Devices > Add Device > Advanced TrustSec Settings **Opmerking**: de CTS-referenties moeten hetzelfde zijn als het wachtwoord voor het apparaat-ID + dat u in de CTS-referenties hebt opgegeven, moeten hetzelfde zijn als het

wachtwoord voor het apparaat-ID + dat u in de sectie in Cisco ISE hebt gespecificeerd (zie de schermopname).

---

Verfris vervolgens uw PAC zodat deze weer contact maakt met Cisco ISE:

```
CatalystSwitch(config)#radius server CISCOISE
CatalystSwitch(config-radius-server)#exit
 Request successfully sent to PAC Provisioning driver.
```

CTS wereldwijd inschakelen op Catalyst Switch

```
CatalystSwitch(config)#cts role-based enforcement
CatalystSwitch(config)#cts role-based enforcement vlan-list 1115 (choose the vlan that your end user devices are on only)
```

Maak een statische IP-naar-SGT toewijzing voor de beperkte webservers (optioneel)

Die Restricted Web Server komt niet door ISE voor verificatie ooit, dus u moet het handmatig labelen met de Switch CLI of ISE Web GUI, dat is slechts een van de vele webservers in Cisco.

```
CatalystSwitch(config)#cts role-based sgt-map 10.201.214.132 sgt 8
```

Controleer TrustSec op Catalyst Switch

```
CatalystSwitch#show cts pac
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 PAC-Info:
 PAC-type = Cisco Trustsec
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 I-ID: CatalystSwitch
 A-ID-Info: Identity Services Engine
 Credential Lifetime: 23:43:14 UTC Nov 24 2018
 PAC-Opaque: 000200B80003000100040010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F6
 Refresh timer is set for 12w5d
```

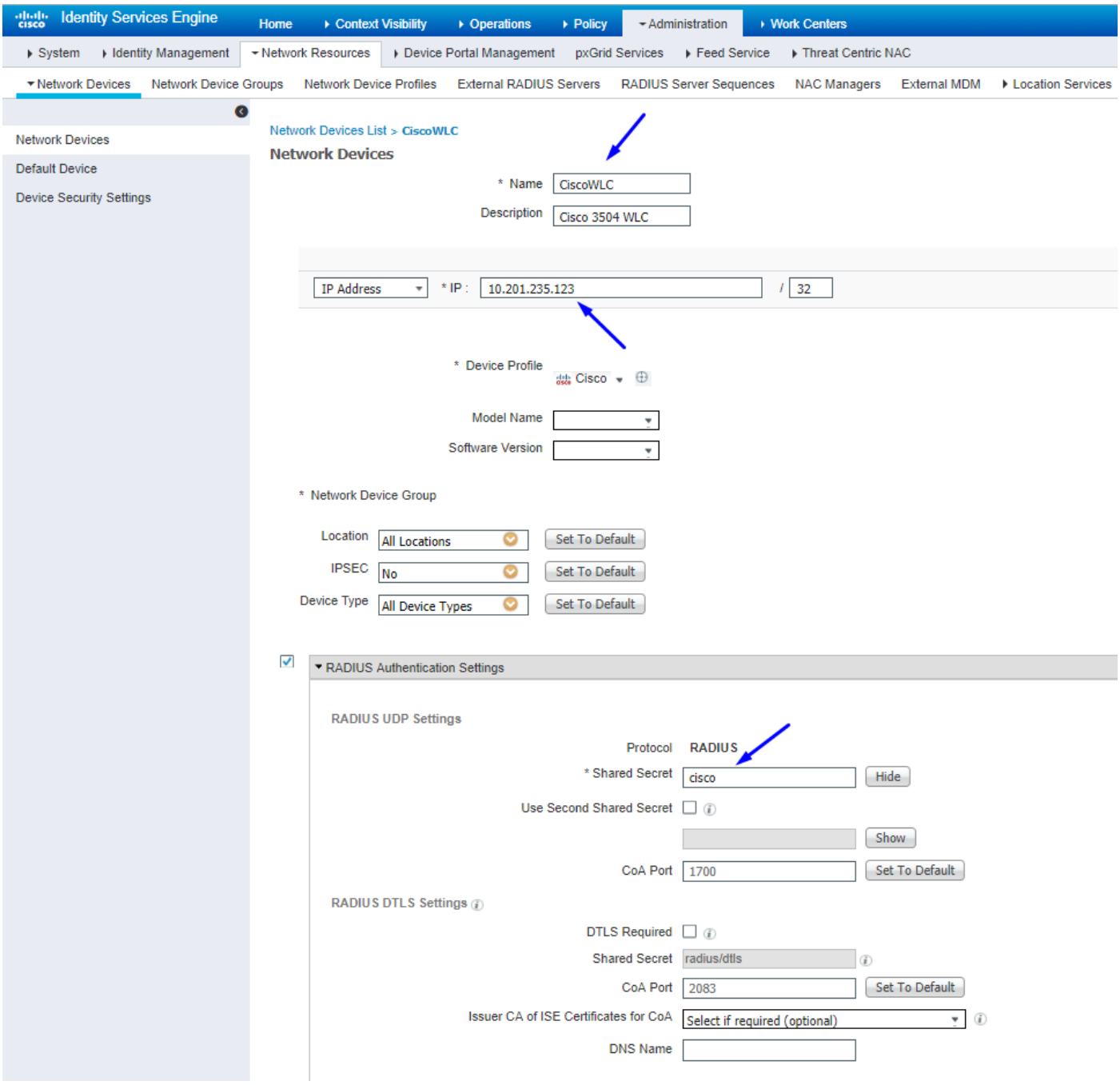
```
CatalystSwitch#cts refresh environment-data
Environment data download in progress
```

```
CatalystSwitch#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 2-02:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.201.214.230, port 1812, A-ID EF2E1222E67EB4630A8B22D1FF0216C1
 Status = ALIVE flag(0x11)
 auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
 0001-31 :
 0-00:Unknown
 2-00:TrustSec_Devices
 3-00:Network_Services
 4-00:Employees
 5-00:Contractors
 6-00:Guests
 7-00:BYODemployees
 8-00:EmployeeServer
 15-00:BYODconsultants
 255-00:Quarantined_Systems
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 16:04:29 UTC Sat Aug 25 2018
Env-data expires in 0:23:57:01 (dd:hr:mm:sec)
Env-data refreshes in 0:23:57:01 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

```
CatalystSwitch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address SGT Source
============================================
10.201.214.132 8 CLI
10.201.235.102 2 INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI bindings = 1
Total number of INTERNAL bindings = 1
Total number of active bindings = 2
```

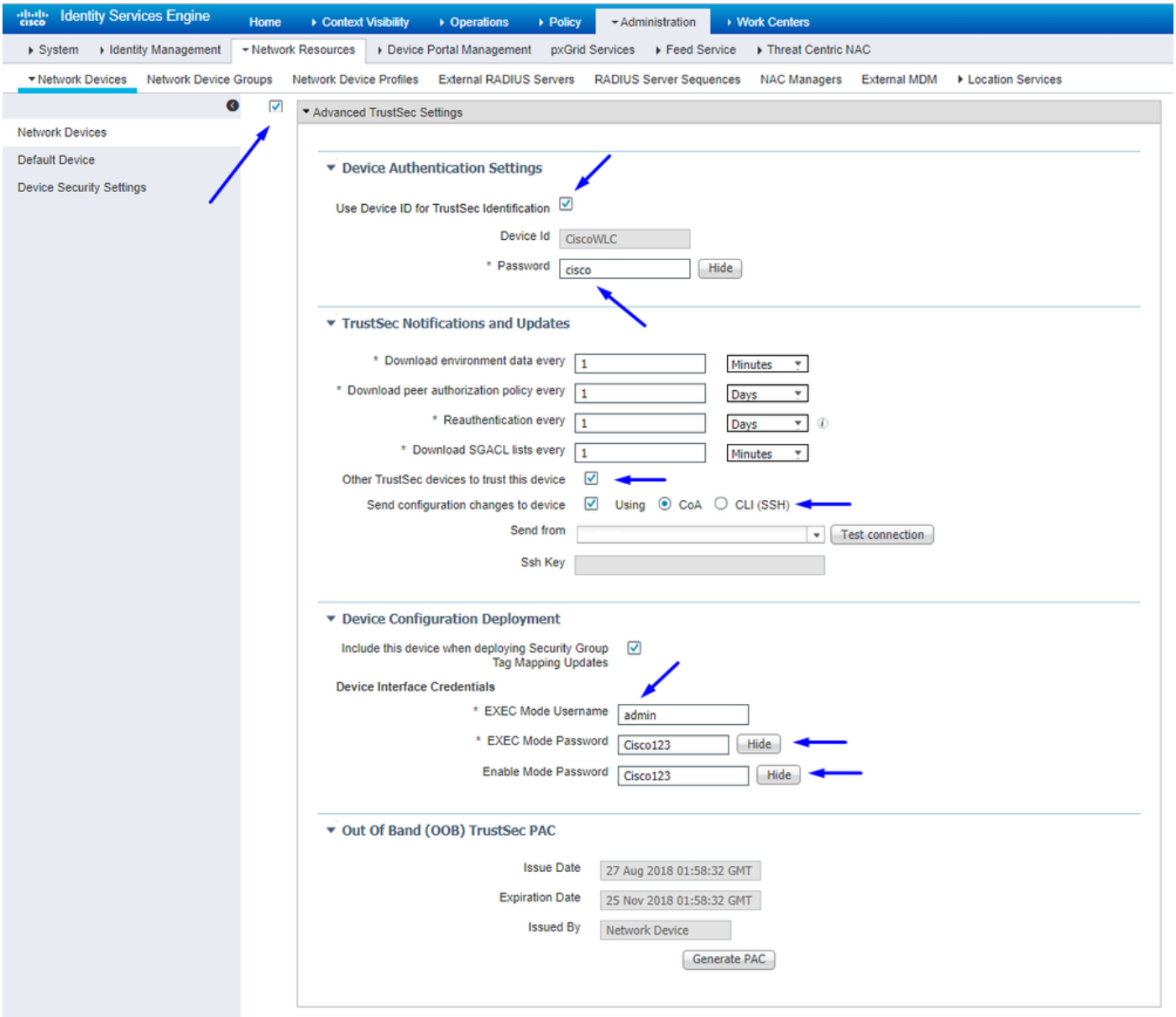
Configure TrustSec op WLC

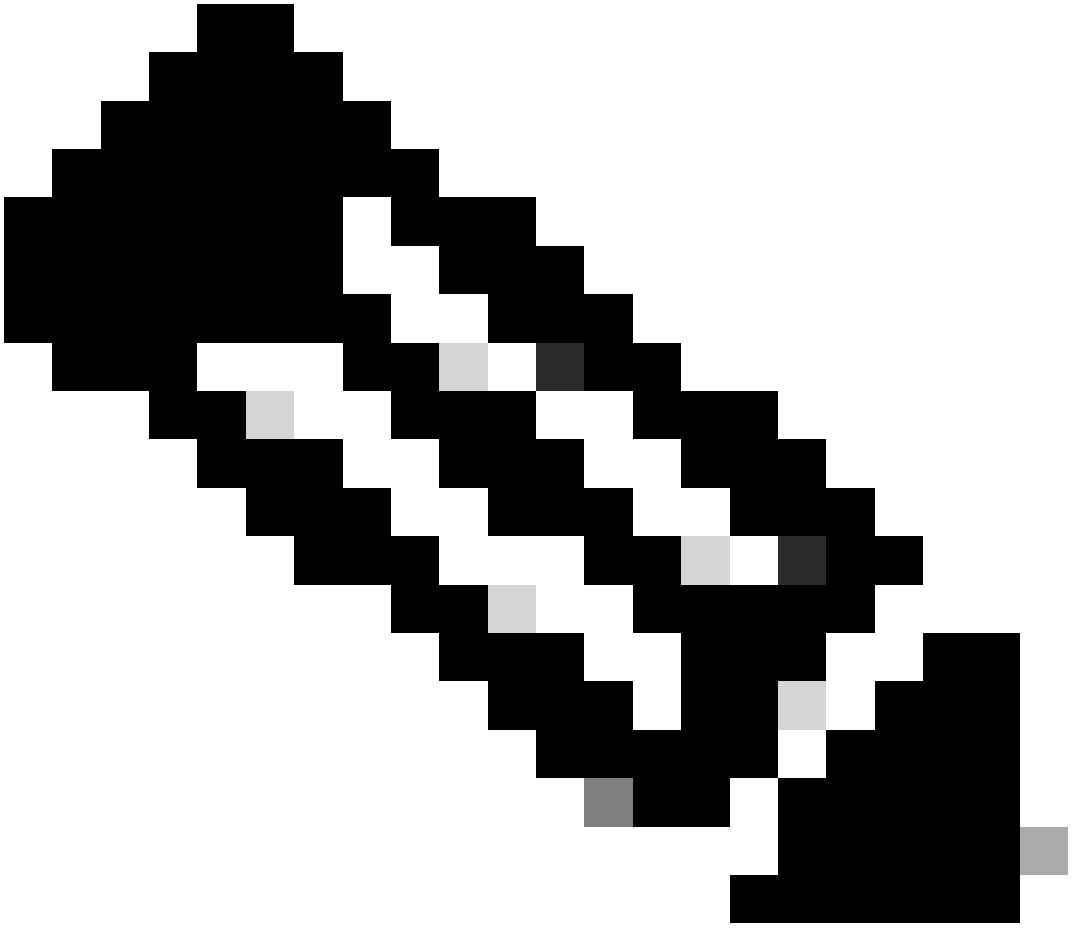
Configureer en controleer of WLC als RADIUS-apparaat wordt toegevoegd in Cisco ISE-software




Configureer en controleer of WLC wordt toegevoegd als een TrustSec-apparaat in Cisco ISE

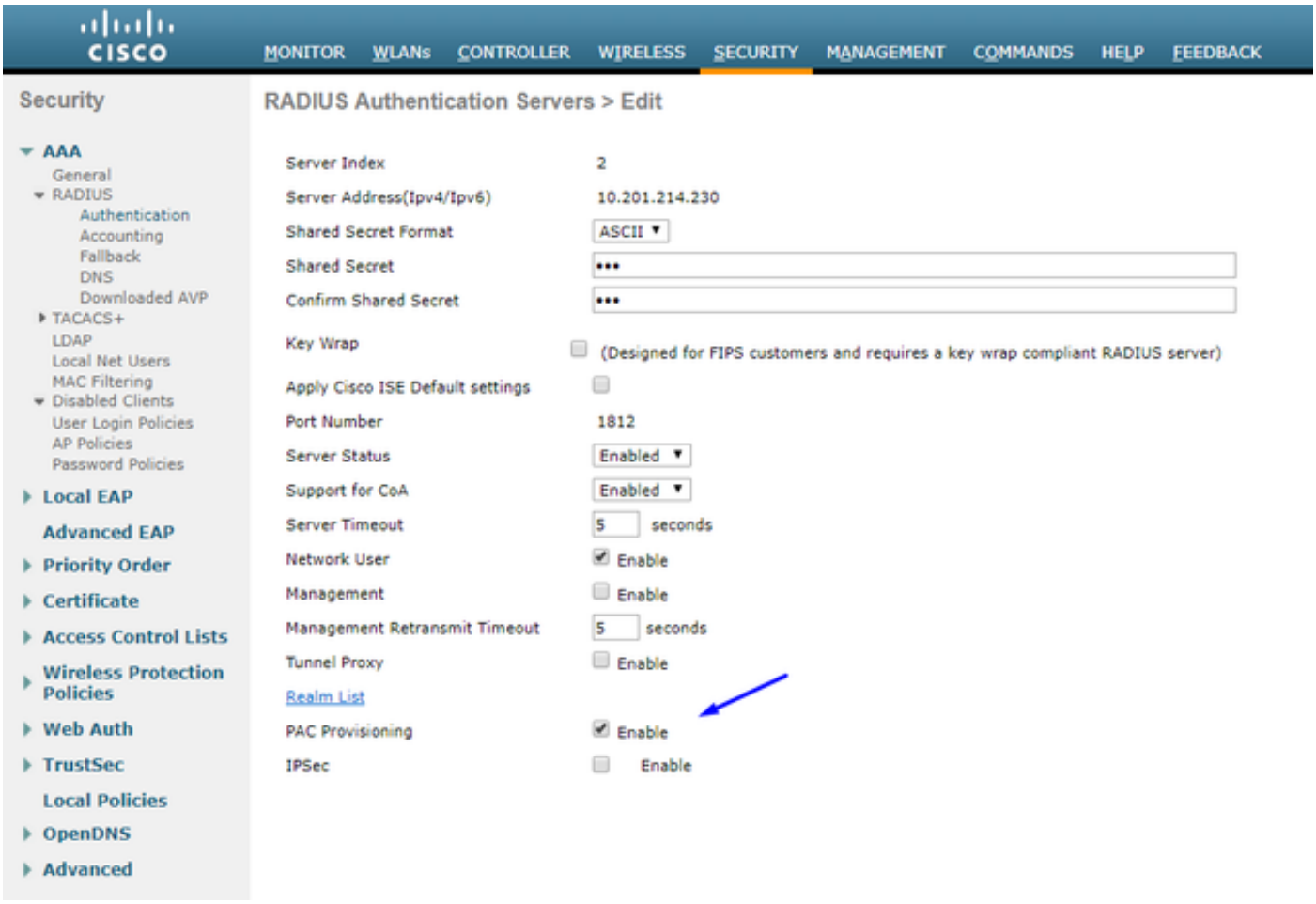
Met deze stap kan Cisco ISE statische IP-naar-SGT toewijzingen naar de WLC implementeren. U hebt deze toewijzingen in de Cisco ISE-webGUI in **werkcentra > TrustSec > Componenten > Statische toewijzingen van IP SGT** in een vorige stap gemaakt.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
Network Devices
Default Device
Device Security Settings
Advanced TrustSec Settings
Device Authentication Settings
Use Device ID for TrustSec Identification
Device Id
CiscoWLC
* Password
cisco
Hide
TrustSec Notifications and Updates
* Download environment data every
1
Minutes
* Download peer authorization policy every
1
Days
* Reauthentication every
1
Days
* Download SGACL lists every
1
Minutes
Other TrustSec devices to trust this device
Send configuration changes to device
Using
CoA
CLI (SSH)
Send from
Test connection
Ssh Key
Device Configuration Deployment
Include this device when deploying Security Group Tag Mapping Updates
Device Interface Credentials
* EXEC Mode Username
admin
* EXEC Mode Password
Cisco123
Hide
Enable Mode Password
Cisco123
Hide
Out Of Band (OOB) TrustSec PAC
Issue Date
27 Aug 2018 01:58:32 GMT
Expiration Date
25 Nov 2018 01:58:32 GMT
Issued By
Network Device
Generate PAC

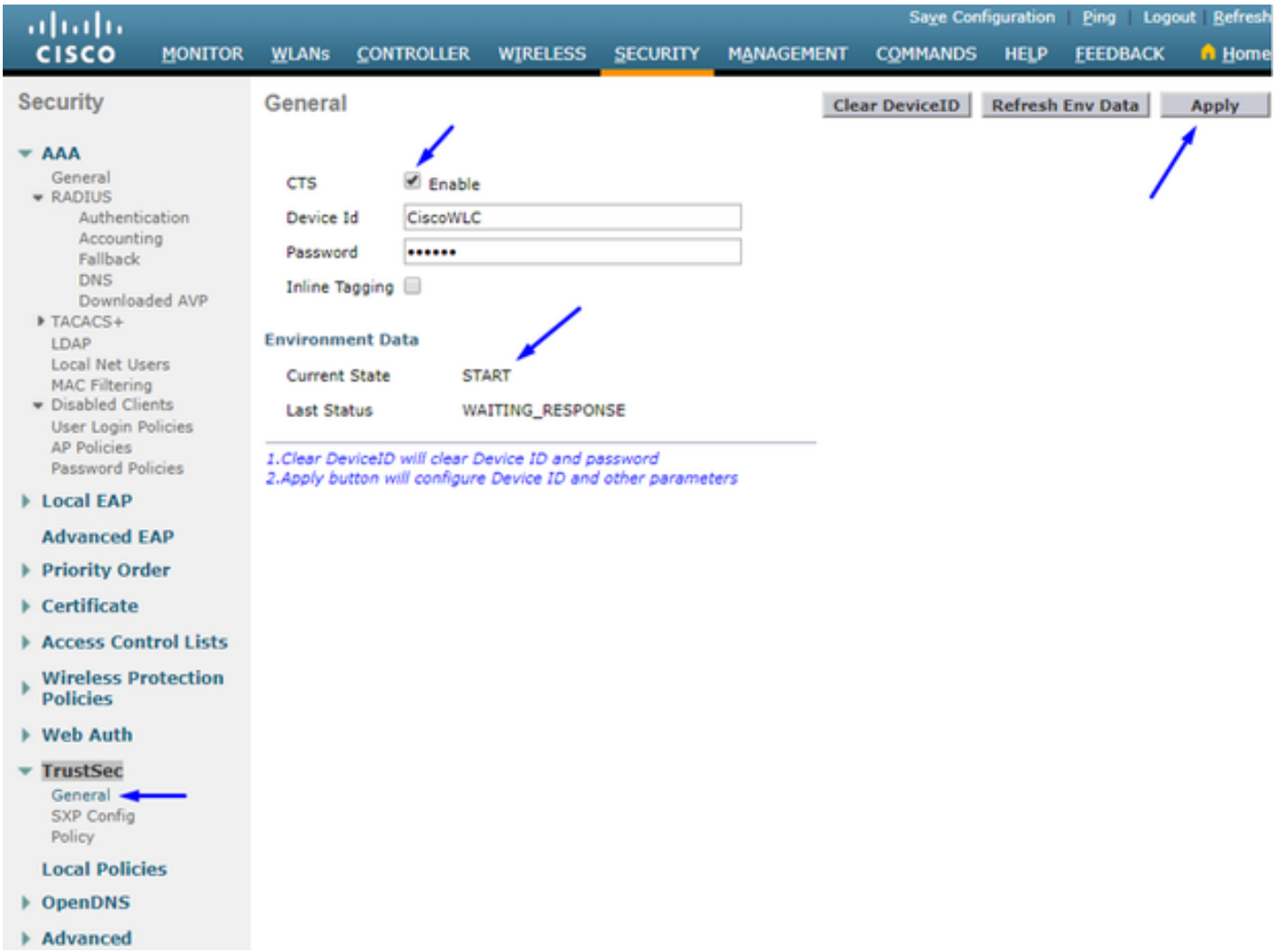


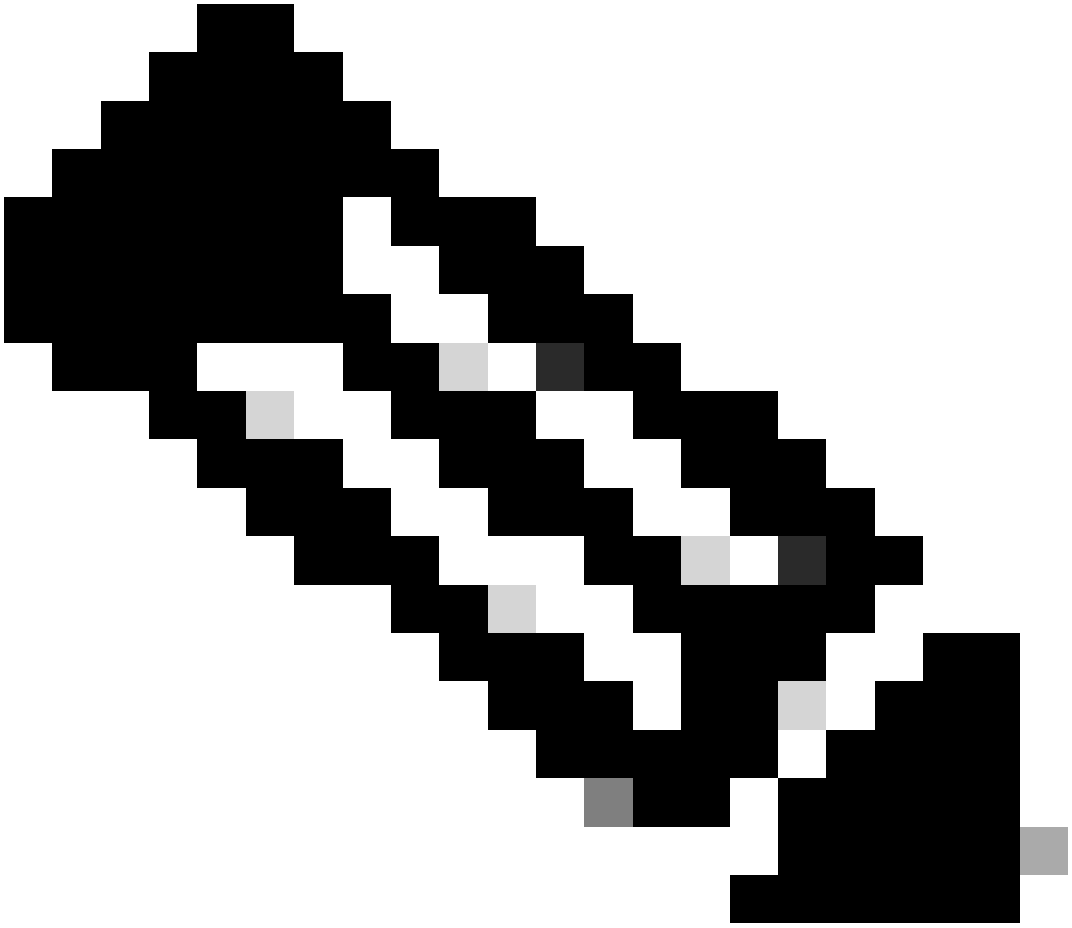
**Opmerking**: We gebruiken dit Device ld en Password in een latere stap, in Security > TrustSec > General de WLC Web UI.

PAC-levering van WLC inschakelen




TrustSec op WLC inschakelen

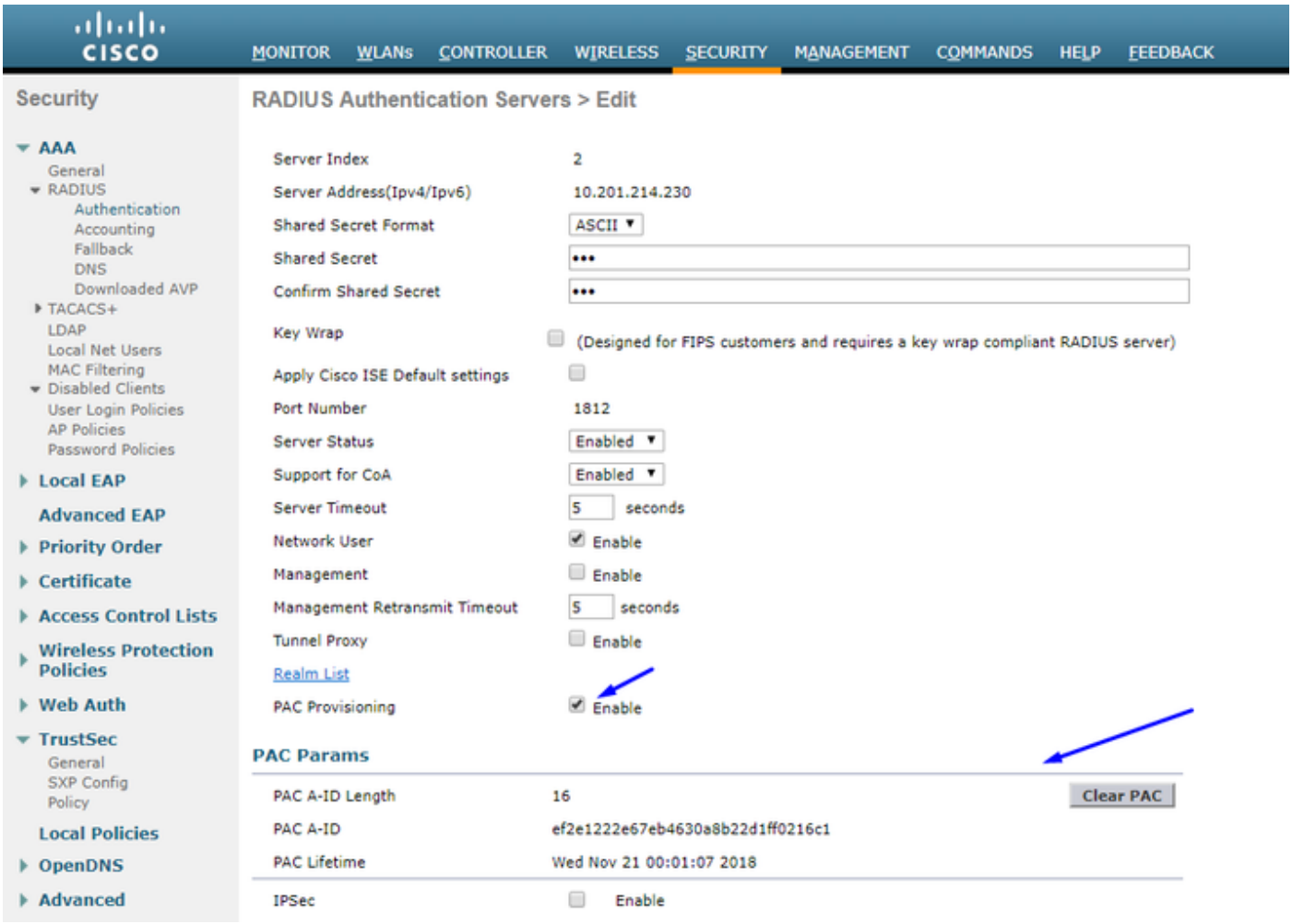

Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec
General
SXP Config
Policy
Local Policies
OpenDNS
Advanced
General
Clear DeviceID
Refresh Env Data
Apply
CTS
Enable
Device Id
CiscoWLC
Password
Inline Tagging
Environment Data
Current State
START
Last Status
WAITING_RESPONSE
1.Clear DeviceID will clear Device ID and password
2.Apply button will configure Device ID and other parameters



**Opmerking**: de CTS Device Id en Password moeten hetzelfde zijn als de Device Id en Password die u in Administration > Network Devices > Add Device > Advanced TrustSec Settingssectie in Cisco ISE hebt opgegeven.

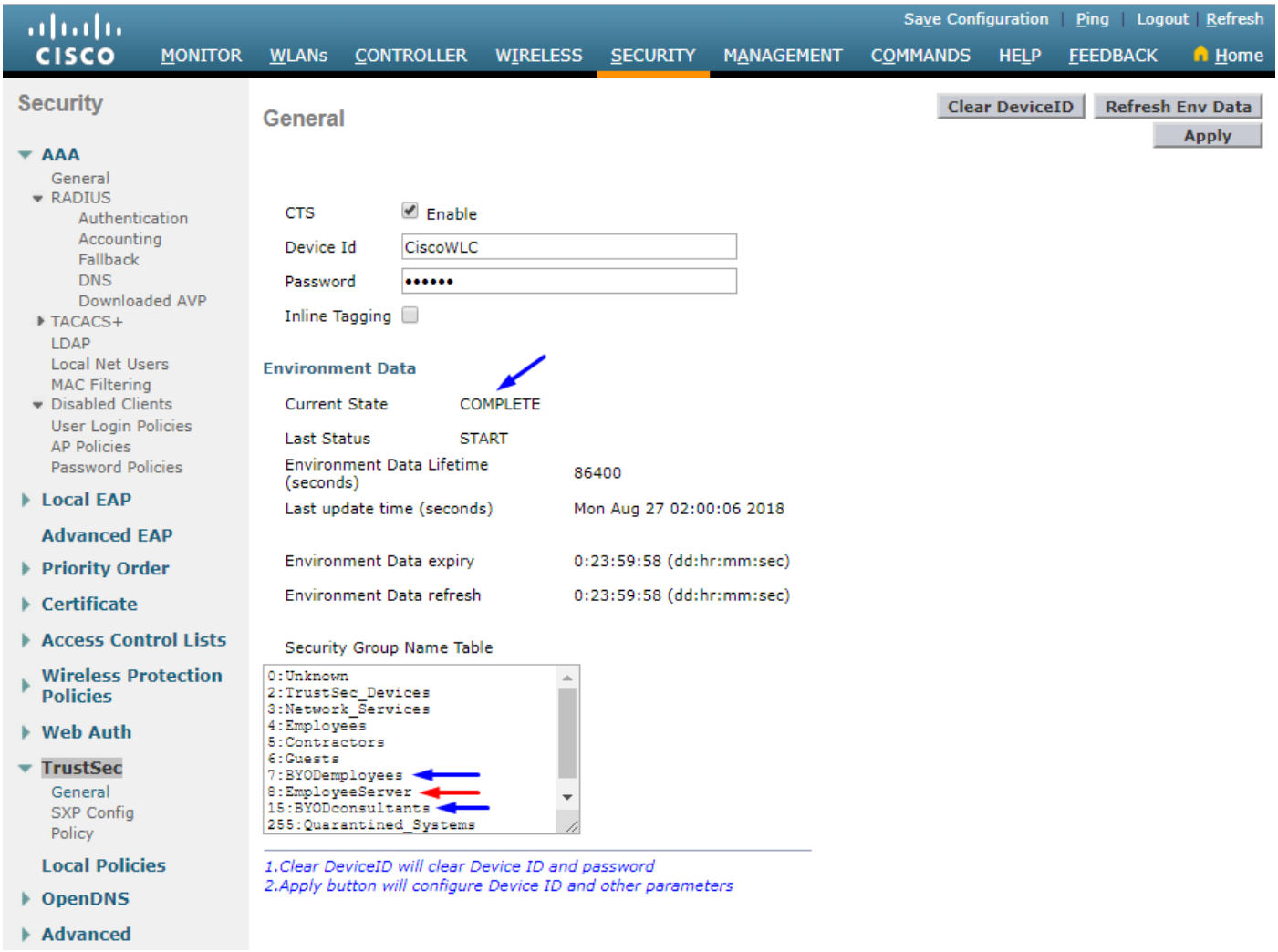
Controleer of PAC is geleverd op WLC

U ziet dat de WLC de PAC met succes heeft geleverd nadat u hebt geklikt Refresh Env Data (u doet dit in deze stap):




CTS Environment Data downloaden van Cisco ISE naar WLC

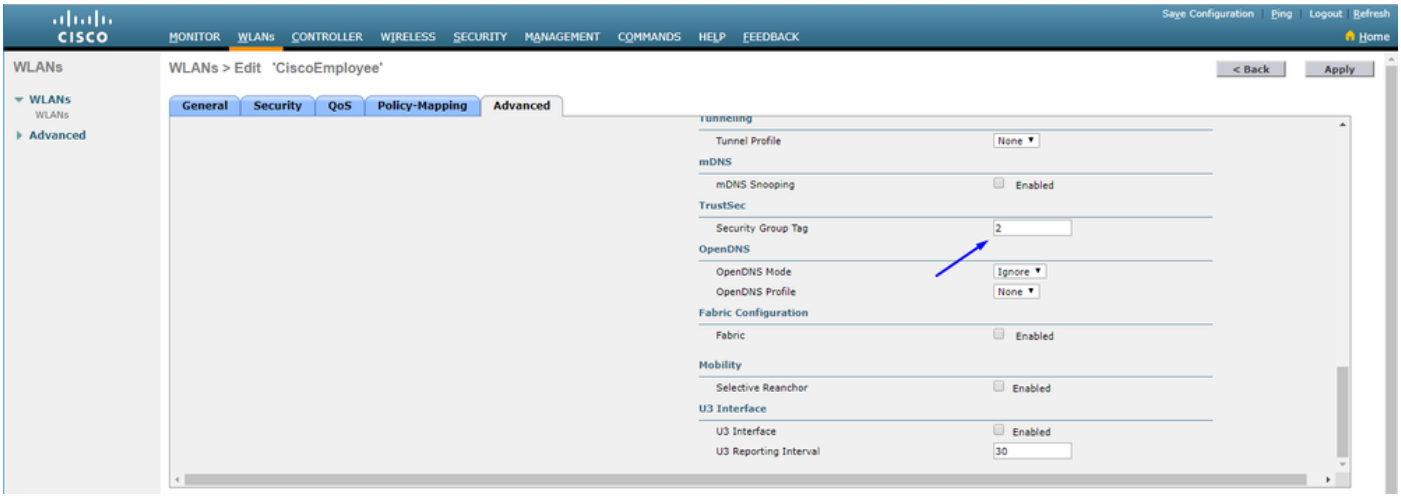
Nadat u klikt Refresh Env Data, uw WLC downloadt uw SGT's.



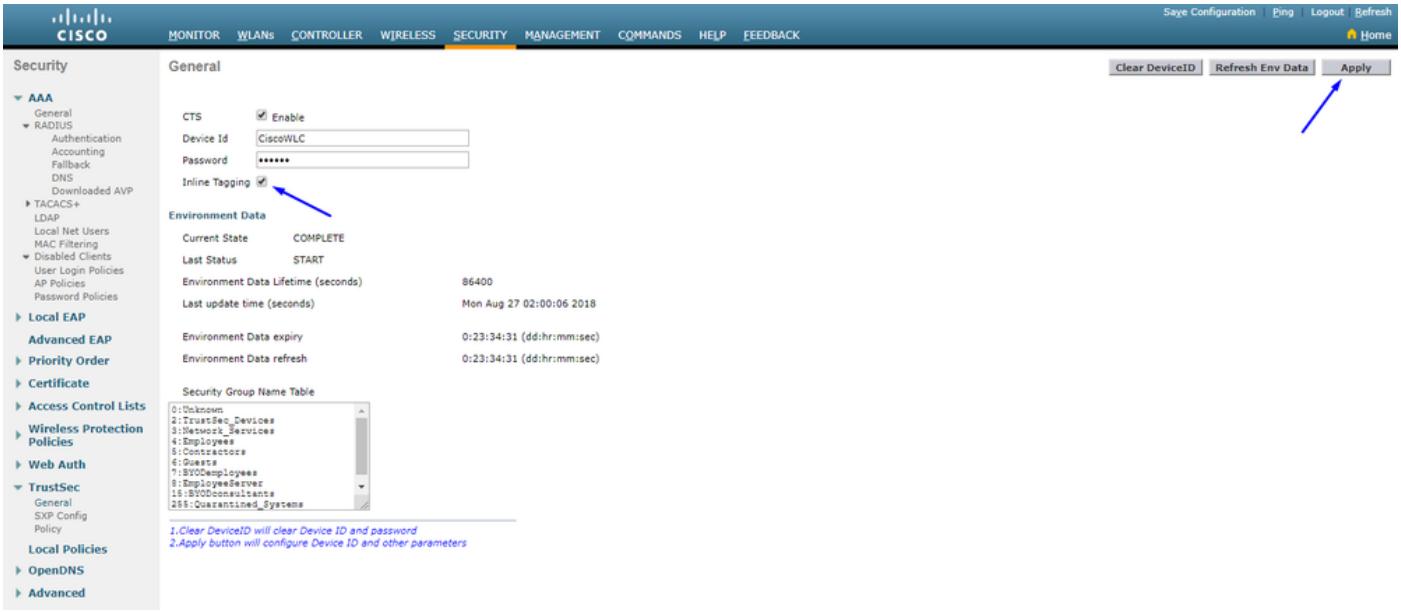

SGACL-downloads en -handhaving inschakelen op verkeer

WLC en access point toewijzen aan SGT van 2 (TrustSec_Devices)

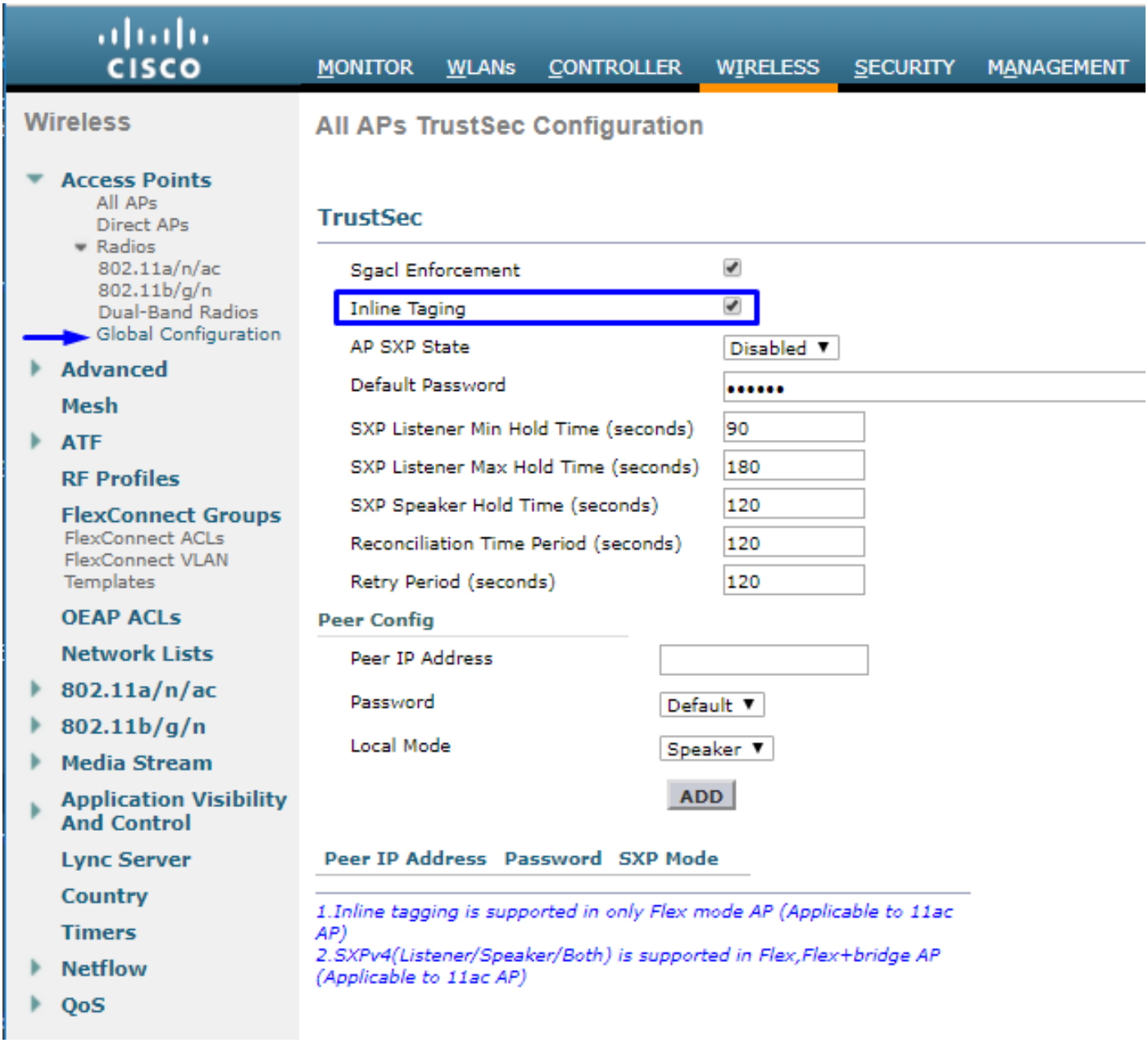
Geef WLC+WLAN een SGT van 2 (TrustSec_Devices) om verkeer (SSH, HTTPS en CAPWAP) naar/van WLC + AP via de switch toe te staan.




Inline tagging op WLC inschakelen




Selecteer onder **Wireless > Access Points > Global Configuration** het kopje Omlaag en kies **TrustSec Config**.




Inline tagging op Catalyst Switch inschakelen

<#root>

CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

**CatalystSwitch(config-if)#description goestoWLC**

**CatalystSwitch(config-if)#switchport trunk native vlan 15**

**CatalystSwitch(config-if)#switchport trunk allowed vlan 15,455,463,1115**

**CatalystSwitch(config-if)#switchport mode trunk**

```
CatalystSwitch(config-if)#cts role-based enforcement
CatalystSwitch(config-if)#cts manual
CatalystSwitch(config-if-cts-manual)#policy static sgt 2 trusted
```

Verifiëren

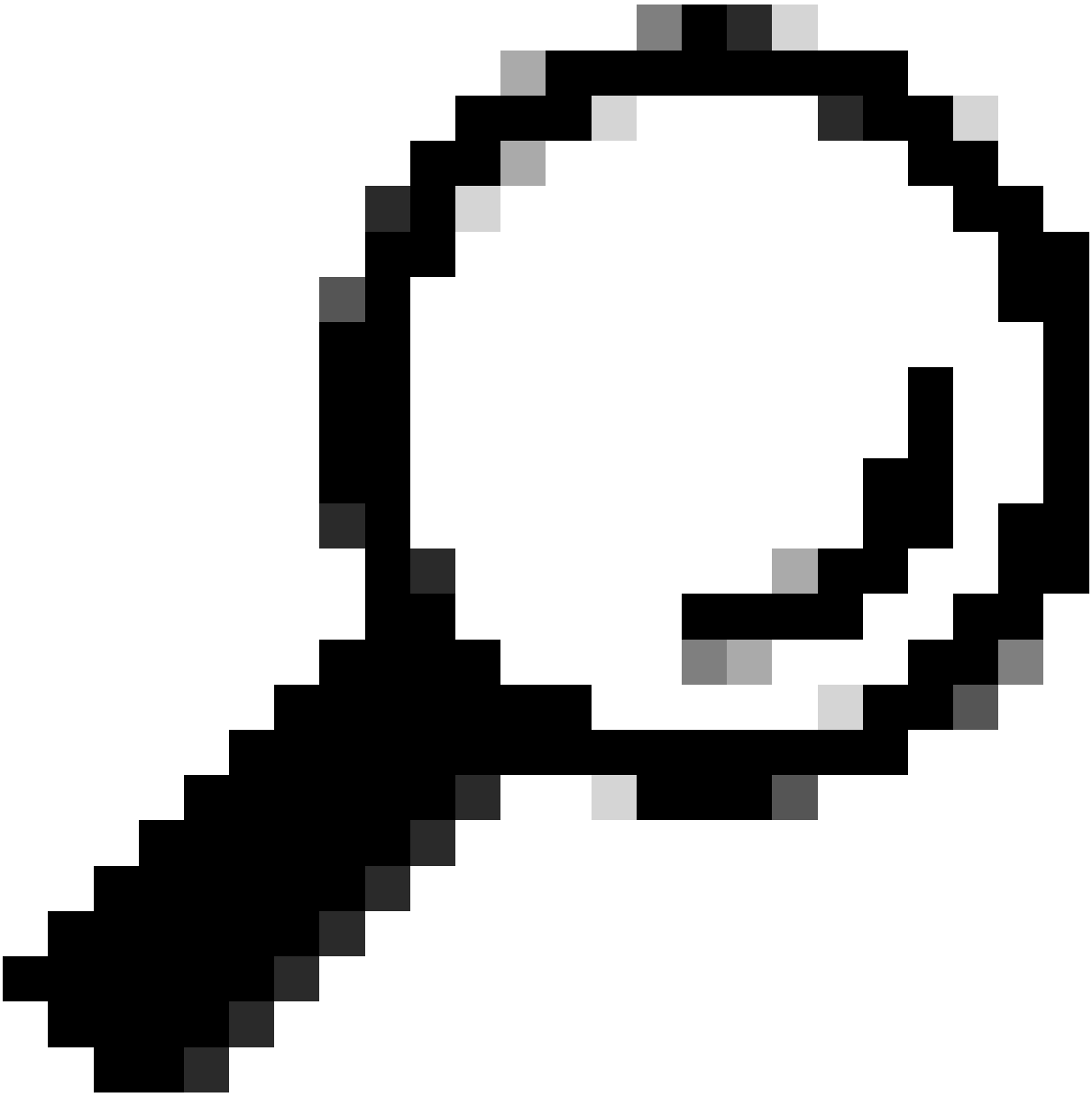

Catalyst 2960Switch#show-platform beltellers, hardware | Inc. SGACL

Uitgaande IPv4 SGACL Drop (454): 10 frames

Uitgaande IPv6 SGACL Drop (455): 0 frames

Uitgaande IPv4 SGACL-celdrop (456): 0 frames

Uitgaande IPv6 SGACL-celdrop (457): 0 frames



**Tip**: als u in plaats daarvan een Cisco ASR, Nexus of Cisco ASA gebruikt, kan het document dat hier wordt vermeld helpen verifiëren of uw SGT-tags worden gehandhaafd: TrustSec Probleemoplossing Guide.

---

Verifiëren naar draadloze verbinding met gebruikersnaam en wachtwoord Admin123 - u stuit op de ontkennen ACL in de switch:


# This site can't be reached

**10.201.214.132** took too long to respond.

Try:

Checking the connection

ERR_CONNECTION_TIMED_OUT

RELOAD

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.