

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

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Doel](#)

[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](#)

[Controleer de standaardinstellingen van TrustSec om te controleren of deze acceptabel zijn \(optioneel\)](#)

[Security Group-tags voor draadloze gebruikers maken](#)

[Statische IP-naar-SGT-toewijzing maken voor de beperkte webserver](#)

[Certificaatverificatieprofiel maken](#)

[Creëer een Identity Source Sequence met het Certificaatverificatieprofiel van Vóór](#)

[Wijs draadloze gebruikers \(werknemers en consultants\) een geschikt SGT toe](#)

[SGT's toewijzen aan de feitelijke apparaten \(Switch en WLC\)](#)

[SGACL's definiëren om het uitgaande beleid te specificeren](#)

[Handhaaf uw ACL's op de TrustSec Policy Matrix in Cisco ISE-software](#)

[Configureer TrustSec op Catalyst Switch](#)

[Switch configureren voor gebruik van Cisco TrustSec voor AAA op Catalyst Switch](#)

[De PAC-toets configureren onder de RADIUS-server om de Switch te verifiëren naar Cisco ISE](#)

[CTS-referenties configureren om de Switch te verifiëren naar Cisco ISE](#)

[CTS wereldwijd inschakelen op Catalyst Switch](#)

[Maak een statische IP-naar-SGT toewijzing voor de beperkte webserver \(optioneel\)](#)

[Controleer TrustSec op Catalyst Switch](#)

[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](#)

[PAC-levering van WLC inschakelen](#)

[TrustSec op WLC inschakelen](#)

[Controleer of PAC is geleverd op WLC](#)

[CTS Environment Data downloaden van Cisco ISE naar WLC](#)

[SGACL-downloads en -handhaving inschakelen op verkeer](#)

[WLC en access point toewijzen aan SGT van 2 \(TrustSec Devices\)](#)

[Inline tagging op WLC inschakelen](#)

[Inline tagging op Catalyst Switch inschakelen](#)

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:

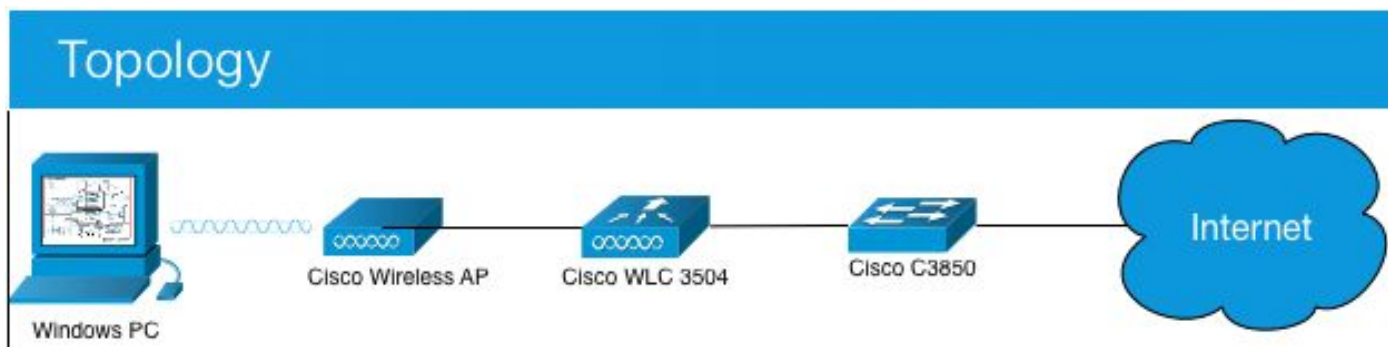
- TrustSec/Security Group-tags
- Inline tagging (indien niet, kunt u SXP gebruiken in plaats van Inline tagging)
- Statische IP-naar-SGT-toewijzingen (indien nodig)
- Statische Subnet-to-SGT-toewijzingen (indien nodig)
- Statische VLAN-naar-SGT-toewijzingen (indien nodig)

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

Netwerkdigram



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

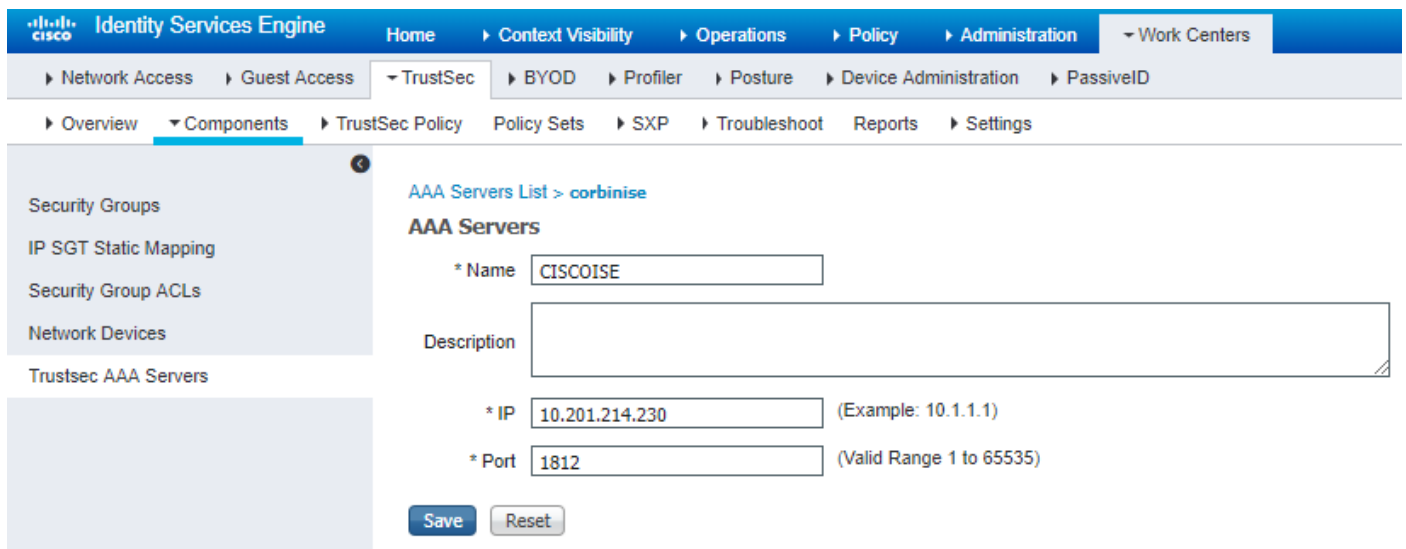
Configuraties

TrustSec op ISE configureren

TrustSec Overview

1 Prepare	2 Define	3 Go Live & Monitor
<p>Plan Security Groups Identify resources that require different levels of protection</p> <p>Classify the users or clients that will access those resources</p> <p>Objective is to identify the minimum required number of Security Groups, as this will simplify management of the matrix</p> <p>Preliminary Setup Set up the TrustSec AAA server.</p> <p>Set up TrustSec network devices.</p> <p>Check default TrustSec settings to make sure they are acceptable.</p> <p>If relevant, set up TrustSec-ACI policy group exchange to enable consistent policy across your network.</p> <p>Consider activating the workflow process to prepare staging policy with an approval process.</p>	<p>Create Components Create security groups for resources, user groups and Network Devices as defined in the preparation phase. Also, examine if default SGTs can be used to match the roles defined.</p> <p>Define the network device authorization policy by assigning SGTs to network devices.</p> <p>Policy Define SGACLs to specify egress policy.</p> <p>Assign SGACLs to cells within the matrix to enforce security.</p> <p>Exchange Policy Configure SXP to allow distribution of IP to SGT mappings directly to TrustSec enforcement devices.</p>	<p>Push Policy Push the matrix policy live.</p> <p>Push the SGTs, SGACLs and the matrix to the network devices ?</p> <p>Real-time Monitoring Check dashboards to monitor current access.</p> <p>Auditing Examine reports to check access and authorization is as intended.</p>

Cisco ISE configureren als een TrustSec AAA-server



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

The screenshot displays the Cisco ISE web interface for configuring a Network Device. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices. The left sidebar shows 'Network Devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'Network Devices List > CatalystSwitch' and 'Network Devices'. The configuration form includes:

- * Name: CatalystSwitch
- Description: Catalyst 3850 Switch
- IP Address: 10.201.235.102 / 32
- * Device Profile: Cisco
- Model Name: (empty dropdown)
- Software Version: (empty dropdown)
- * Network Device Group:
 - Location: All Locations (Set To Default)
 - IPSEC: No (Set To Default)
 - Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings:
 - RADIUS UDP Settings:
 - Protocol: RADIUS
 - * Shared Secret: Admin123 (Hide)
 - Use Second Shared Secret: (i)
 - CoA Port: 1700 (Set To Default)
 - RADIUS DTLS Settings (i):
 - DTLS Required: (i)
 - Shared Secret: radius/dtls (i)

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:

Network Devices

Default Device

Device Security Settings

Save Cancel

Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device ID:

* Password:

TrustSec Notifications and Updates

* Download environment data every:

* Download peer authorization policy every:

* Reauthentication every:

* Download SGNCL file every:

Other TrustSec devices to trust this device:

Send configuration changes to device: Using Out CLI (SSH)

Send from:

Set Key:

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates:

Device Interface Credentials

* EXEC Mode Username:

* EXEC Mode Password:

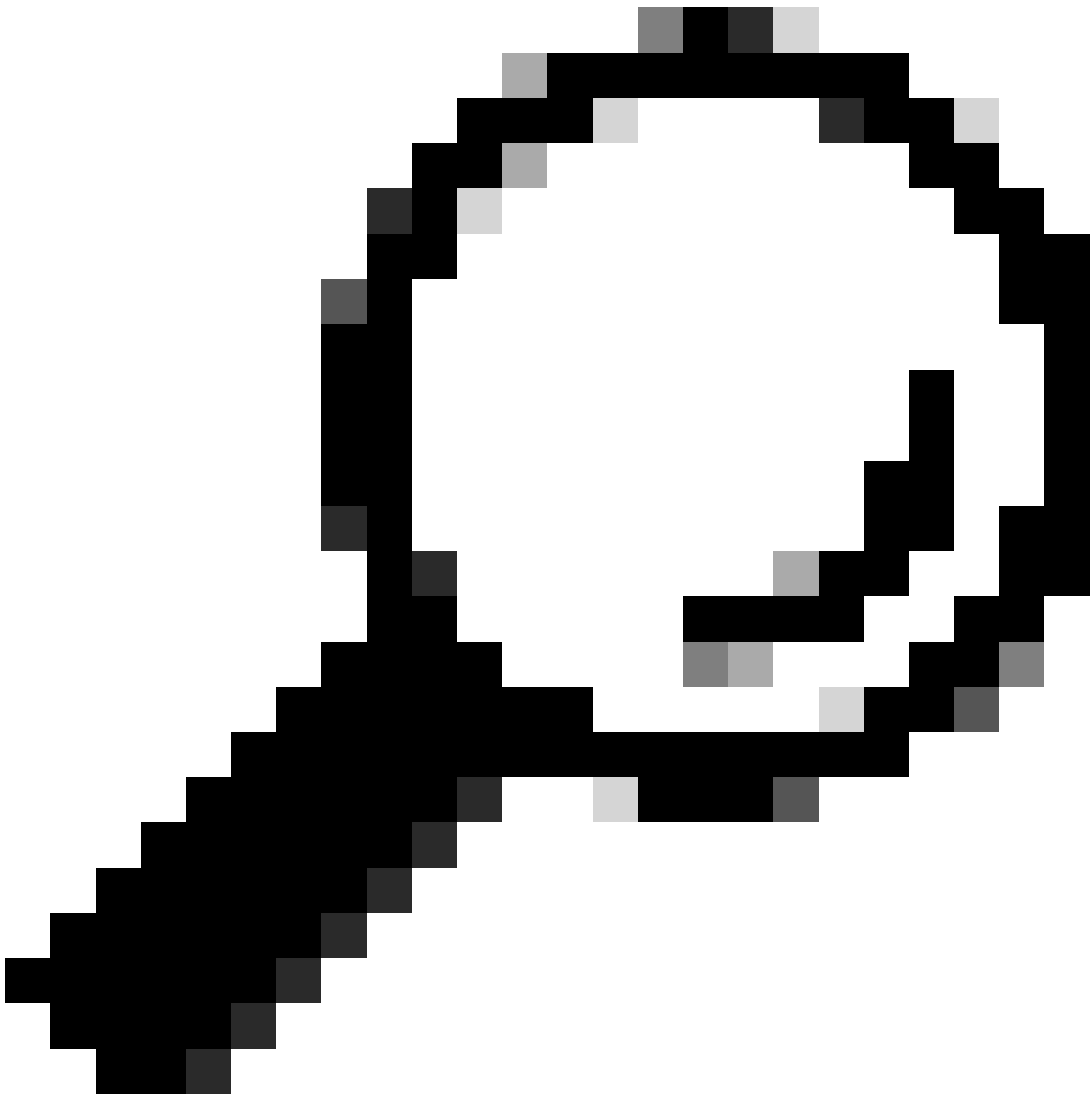
Enable Mode Password:

Out Of Band (OOB) TrustSec PAC

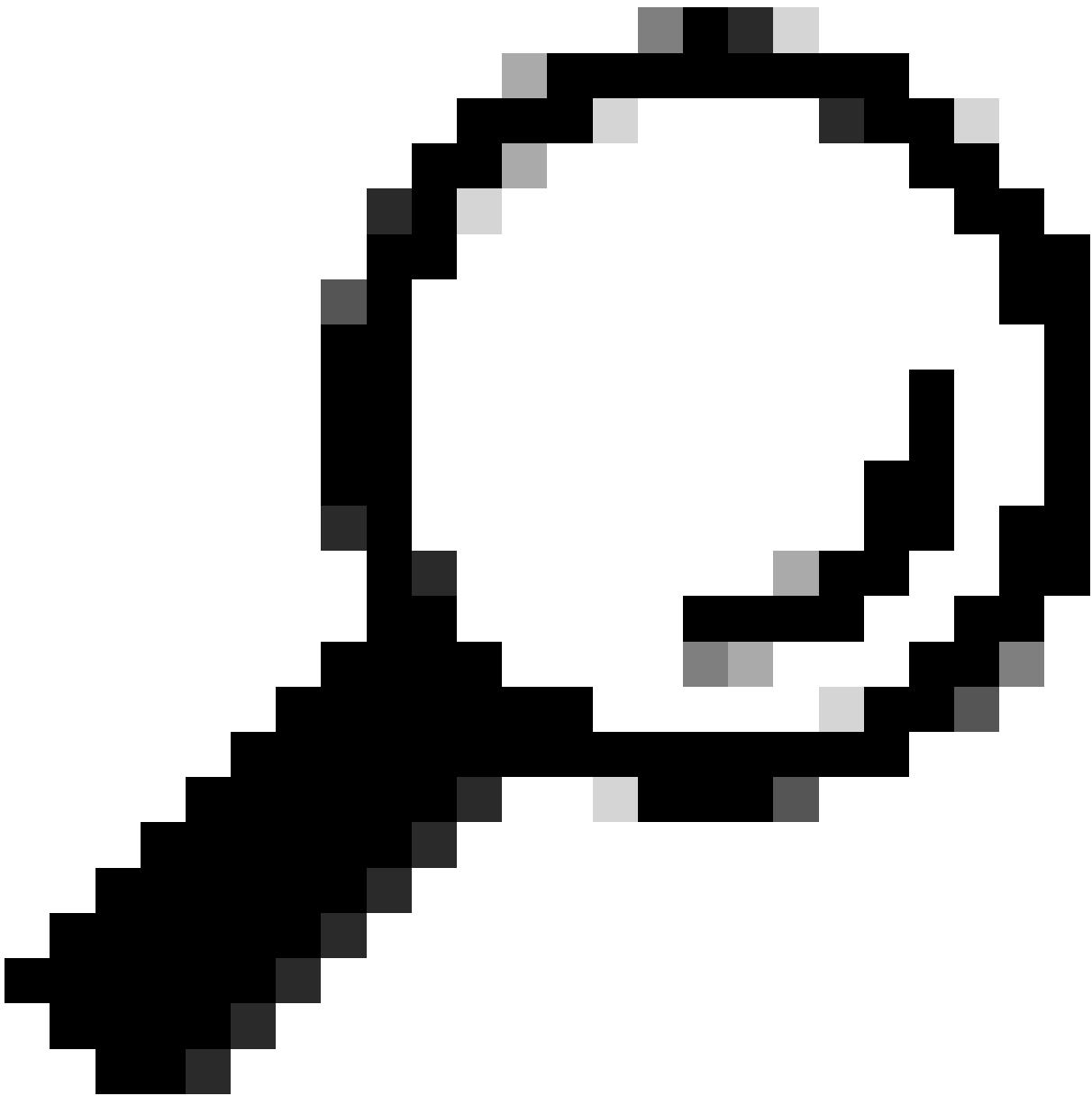
Issue Date:

Expiration Date:

Issued By:



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)



General TrustSec Settings

TrustSec Matrix Settings

Work Process Settings

SXP Settings

ACI Settings

General TrustSec Settings

Verify TrustSec Deployment

Automatic verification after every deploy (i)

Time after deploy process minutes (10-60) (i)

Verify Now

Protected Access Credential (PAC)

*Tunnel PAC Time To Live

*Proactive PAC update when % PAC TTL is Left

Security Group Tag Numbering

System Will Assign SGT Numbers

Except Numbers In Range - From To

User Must Enter SGT Numbers Manually

Security Group Tag Numbering for APIC EPGs

System will assign numbers In Range - From

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

Security Group Tag Numbering for APIC EPGs

System will assign numbers In Range - From

Automatic Security Group Creation

Auto Create Security Groups When Creating Authorization Rules *(i)*

SGT Number Range For Auto-Creation - From To

Automatic Naming Options

Select basis for names. (Security Group name will be shortened to 32 characters)

Name Will Include

Optional Additions

Policy Set Name *(i)*

Prefix

Suffix

Example Name - *RuleName*

IP SGT static mapping of hostnames

Create mappings for all IP addresses returned by DNS query

Create mappings only for the first IPv4 address and the first IPv6 address returned by DNS query

Security Group-tags voor draadloze gebruikers maken

Security Group voor BYODconsultants maken - SGT 15

Security Group voor BYOD-medewerkers maken - SGT 7

Security Groups
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Icon	Name	SGT (Dec / Hex)	Description	Learned from
	BYODconsultants	15/000F	SGT for consultants who use BYOD - restrict internal access	
	BYODEmployees	7/0007	SGT for employees who use BYOD - allow internal access	
	Contractors	5/0005	Contractor Security Group	
	Employees	4/0004	Employee Security Group	
	EmployeeServer	8/0008	Restricted Web Server - Only employees should be able to access	
	Guests	6/0006	Guest Security Group	
	Network_Services	3/0003	Network Services Security Group	
	Quarantined_Systems	255/00FF	Quarantine Security Group	
	RestrictedWebServer	8/0008		
	TrustSec_Devices	2/0002	TrustSec Devices Security Group	
	Unknown	0/0000	Unknown Security Group	

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.

IP SGT static mapping > 10.201.214.132

IP address(es) *

Add to a mapping group
 Map to SGT individually

SGT *

Send to SXP Domain

Deploy to devices

Certificaatverificatieprofiel maken

External Identity Sources

- Certificate Authentication Profile
- Active Directory
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - SAML Id Providers
 - Social Login

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name: BYODCertificateAuthProfile

Description: Allow 802.1x authentication to BYOD using username+password + EAP-TLS authentication to BYOD using certificate

Identity Store: Windows_AD_Server

Use Identity From: Certificate Attribute: Subject - Common Name
 Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store: Never
 Only to resolve identity ambiguity
 Always perform binary comparison

Submit Cancel

Creëer een Identity Source Sequence met het Certificaatverificatieprofiel van Vóór

Identity Source Sequences List > New Identity Source Sequence

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

<p>Available</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> Internal Endpoints Guest Users </div>	<input type="button" value=">"/> <input type="button" value="<"/> <input type="button" value=">>"/> <input type="button" value="<<"/>	<p>Selected</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> Windows_AD_Server Internal Users </div>	<input type="button" value="↕"/> <input type="button" value="↕"/> <input type="button" value="↕"/> <input type="button" value="↕"/>
---	--	--	--

▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

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

Policy Sets - EmployeeSSID

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
On	EmployeeSSID		Airspace Airspace-VlanId EQUALS 2	Default Network Access	631

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
On	Dot1X	Wireless_802.1X	BYOD_Identity_Sequence	230	Options
On	Default		All_Users_ID_Stores	0	Options

Authorization Policy (3)

Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
On	Allow Restricted Access if BYODRegistered and EAP-TLS and AD Group = Consultants	Network Access EapAuthentication EQUALS EAP-TLS corbdc3 ExternalGroups EQUALS cohadley3 local/Users/Consultants	PermAccess	BYODconsultants	57	Options
On	Allow Anywhere if BYODRegistered and EAP-TLS and AD Group = Employees	Network Access EapAuthentication EQUALS EAP-TLS corbdc3 ExternalGroups EQUALS cohadley3 local/Users/Employees	PermAccess	BYODEmployees	0	Options
On	Default		NISP_Onboard	Selected from list	109	Options

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

Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

Rule Name	Conditions	Security Group
Tag_TrustSec_Devices	If DEVICE:Device Type equals to All Device Types then	TrustSec_Devices
Default Rule	If no rules defined or no match then	Unknown

SGACL's definiëren om het uitgaande beleid te specificeren

Laat consultants overall externe toegang toe, maar beperk interne:

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

Security Groups
IP SGT Static Mapping
Security Group ACLs

Network Devices
Trustsec AAA Servers

Security Groups ACLs List > RestrictConsultant

Security Group ACLs

* Name: RestrictConsultant

Description: Deny Consultants from going to internal sites such as: https://10.201.214.132

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:

```

permit icmp
deny tcp dst eq 80
deny tcp dst eq 443
permit ip

```

Werknemers toegang geven tot externe en interne werkplekken:

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

Security Groups
IP SGT Static Mapping
Security Group ACLs

Network Devices
Trustsec AAA Servers

Security Groups ACLs List > AllowEmployee

Security Group ACLs

* Name: AllowEmployee

Description: Allow Employees to ping and access sites in browser

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content:

```

permit icmp
permit tcp dst eq 80
permit tcp dst eq 443
permit ip

```

Geef andere apparaten toegang tot basisdiensten (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

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers

Security Groups ACLs List > LoginServices

Security Group ACLs

* Name: Generation ID: 1

Description:

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content

```

permit udp dst eq 67
permit udp dst eq 53
permit tcp dst eq 53
permit tcp dst eq 88
permit udp dst eq 88
permit udp dst eq 123
permit tcp dst eq 135
permit udp dst eq 137
permit udp dst eq 389
permit tcp dst eq 389
permit udp dst eq 636
permit tcp dst eq 636
permit tcp dst eq 445
permit tcp dst eq 1025
permit tcp dst eq 1026

```

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:

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

Security Groups
IP SGT Static Mapping
Security Group ACLs
Network Devices
Trustsec AAA Servers

Security Groups ACLs List > New Security Group ACLs

Security Group ACLs

* Name: Generation ID: 0

Description:

IP Version: IPv4 IPv6 Agnostic

* Security Group ACL content

```

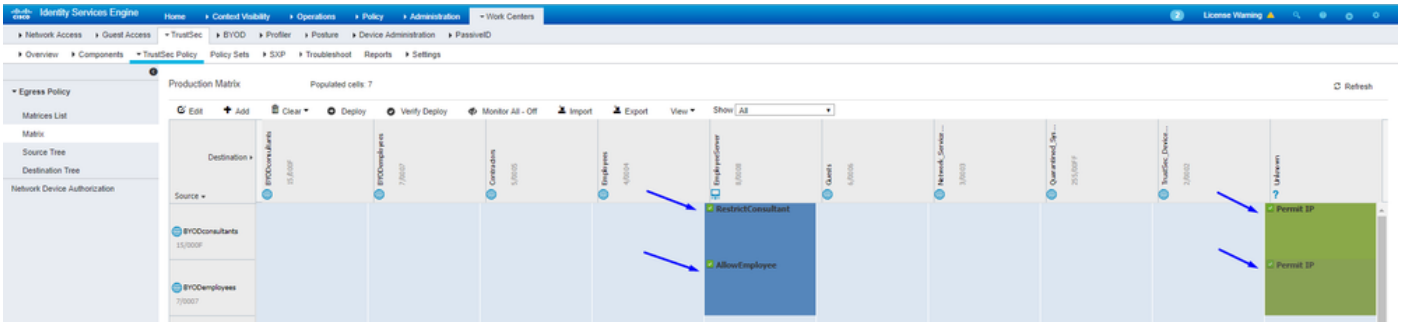
deny udp dst eq 67
deny udp dst eq 53
deny tcp dst eq 53
deny icmp
deny tcp dst eq 8443
permit ip

```

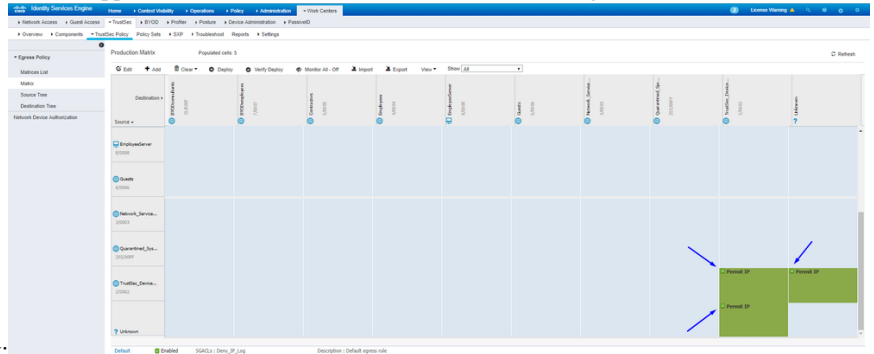
Handhaaf uw ACL's op de TrustSec Policy Matrix in Cisco ISE-software

Laat Consultants overall externe toegang toe, maar beperk interne webserver, zoals <https://10.201.214.132>

Werknemers toegang geven tot externe sites en interne webservers toestaan:

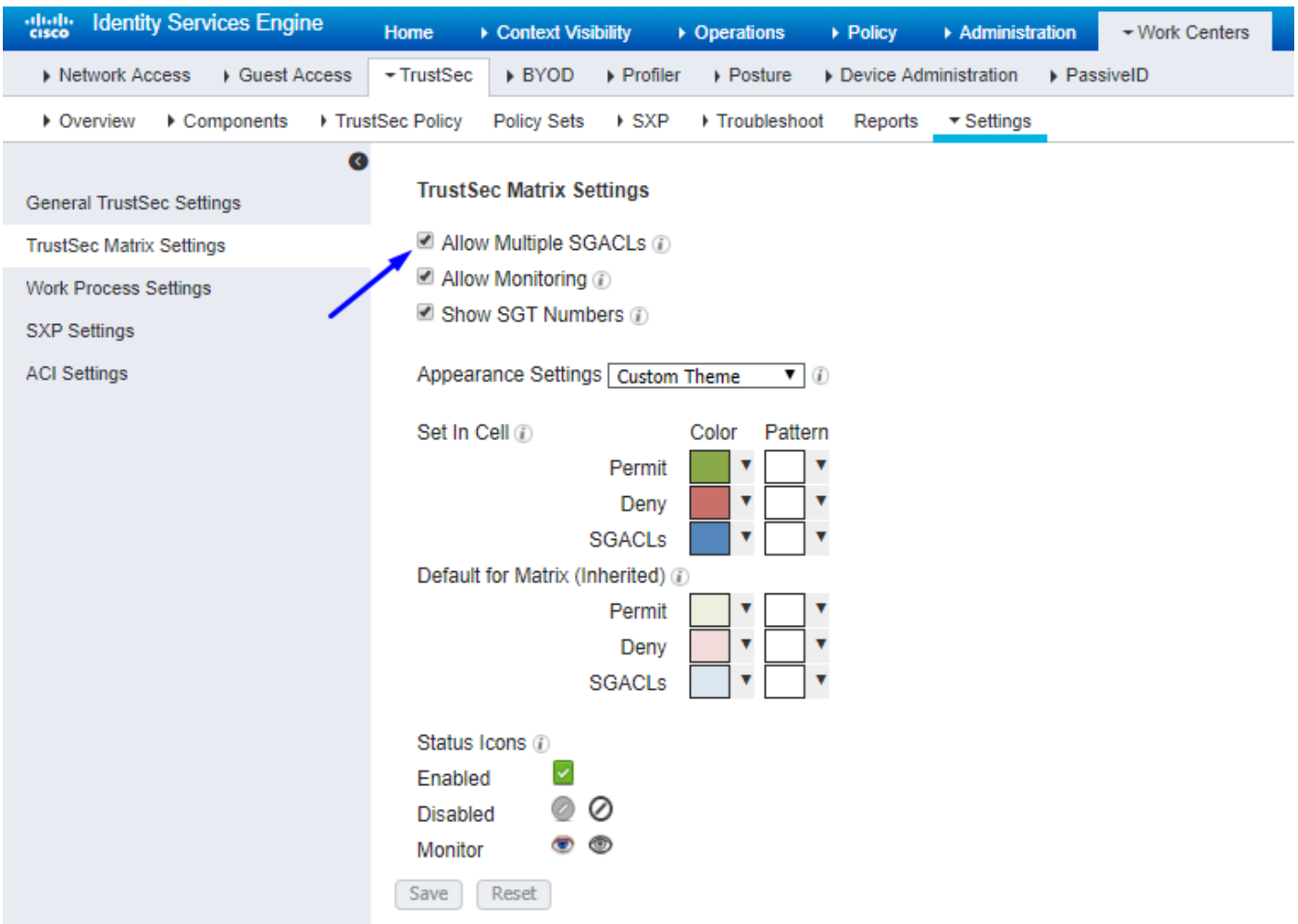


Sta beheerverkeer (SSH, HTTPS en CAPWAP) toe aan/van uw apparaten in het netwerk (switch en WLC), zodat u geen SSH of HTTPS-

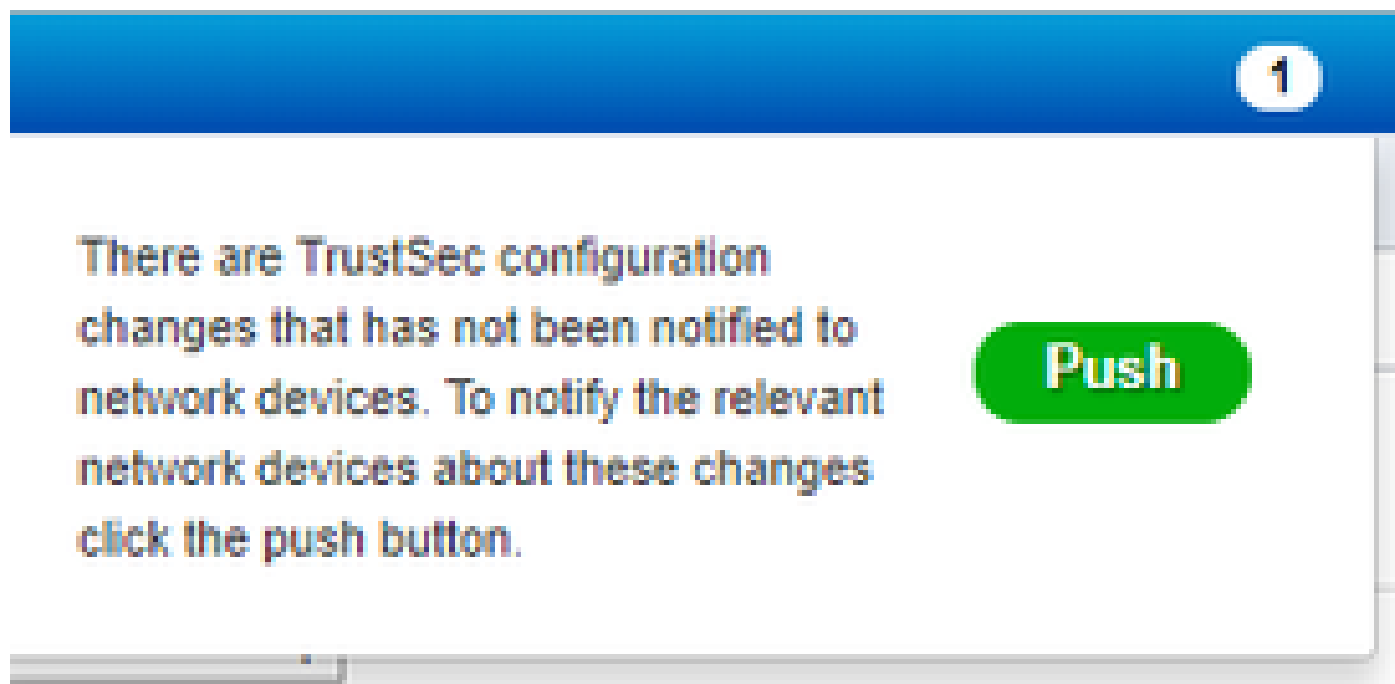


toegang verliest zodra u Cisco TrustSec implementeert:

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
```

The screenshot shows a configuration page titled "RADIUS Authentication Settings". Under the "RADIUS UDP Settings" section, the "Protocol" is set to "RADIUS". The "Shared Secret" field contains the text "Admin123" and has a "Hide" button next to it. The "Use Second Shared Secret" checkbox is unchecked, and there is an information icon (i) next to it.



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

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Ce

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Mana

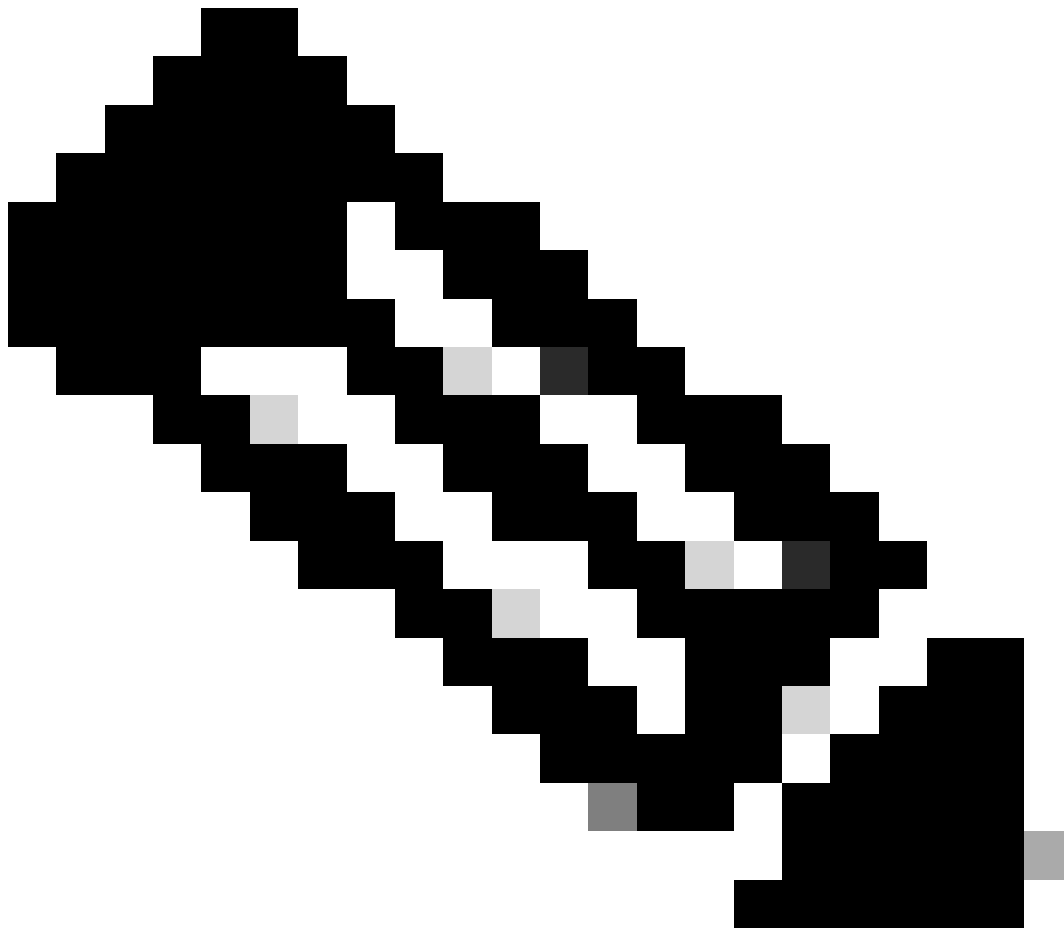
Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id CatalystSwitch

* Password Admin123 Hide



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: 000200B80003000100040010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F0
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

The screenshot displays the Cisco ISE Administration console interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows 'Network Devices' and 'Device Security Settings'. The main content area is titled 'Network Devices List > CiscoWLC' and 'Network Devices'. The configuration form includes the following fields:

- * Name: CiscoWLC
- Description: Cisco 3504 WLC
- IP Address: 10.201.235.123 / 32
- * Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- * Network Device Group:
 - Location: All Locations (Set To Default)
 - IPSEC: No (Set To Default)
 - Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings
 - RADIUS UDP Settings:
 - Protocol: RADIUS
 - * Shared Secret: cisco (Hide)
 - Use Second Shared Secret: (i)
 - CoA Port: 1700 (Set To Default)
 - RADIUS DTLS Settings (i):
 - DTLS Required: (i)
 - Shared Secret: radius/dtls (i)
 - CoA Port: 2083 (Set To Default)
 - Issuer CA of ISE Certificates for CoA: Select if required (optional) (i)
 - DNS Name: (empty)

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.

Network Devices

- Default Device
- Device Security Settings

Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id

* Password

TrustSec Notifications and Updates

* Download environment data every

* Download peer authorization policy every

* Reauthentication every ⓘ

* Download SGACL lists every

Other TrustSec devices to trust this device

Send configuration changes to device Using CoA CLI (SSH)

Send from

Ssh Key

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates

Device Interface Credentials

* EXEC Mode Username

* EXEC Mode Password

Enable Mode Password

Out Of Band (OOB) TrustSec PAC

Issue Date

Expiration Date

Issued By



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

PAC-levering van WLC inschakelen

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
 - Local Policies
- OpenDNS
- Advanced

RADIUS Authentication Servers > Edit

Server Index	2
Server Address(Ipv4/Ipv6)	10.201.214.230
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	<input type="checkbox"/>
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
Realm List	
PAC Provisioning	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable



TrustSec op WLC inschakelen

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

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):

CISCO | MONITOR | WLANs | CONTROLLER | WIRELESS | **SECURITY** | MANAGEMENT | COMMANDS | HELP | FEEDBACK

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

RADIUS Authentication Servers > Edit

Server Index: 2

Server Address(Ipv4/Ipv6): 10.201.214.230

Shared Secret Format: ASCII

Shared Secret: ***

Confirm Shared Secret: ***

Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Apply Cisco ISE Default settings:

Port Number: 1812

Server Status: Enabled

Support for CoA: Enabled

Server Timeout: 5 seconds

Network User: Enable

Management: Enable

Management Retransmit Timeout: 5 seconds

Tunnel Proxy: Enable

[Realm List](#)

PAC Provisioning: Enable

PAC Params

PAC A-ID Length	16	Clear PAC
PAC A-ID	ef2e1222e67eb4630a8b22d1ff0216c1	
PAC Lifetime	Wed Nov 21 00:01:07 2018	

IPSec: Enable

CTS Environment Data downloaden van Cisco ISE naar WLC

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

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

Password

Inline Tagging

Environment Data

Current State COMPLETE

Last Status START

Environment Data Lifetime (seconds) 86400

Last update time (seconds) Mon Aug 27 02:00:06 2018

Environment Data expiry 0:23:59:58 (dd:hr:mm:sec)

Environment Data refresh 0:23:59:58 (dd:hr:mm:sec)

Security Group Name Table

0:Unknown
2:TrustSec_Devices
3:Network_Services
4:Employees
5:Contractors
6:Guests
7:BYODEmployees
8:EmployeeServer
15:BYODconsultants
255:Quarantined_Systems

1. Clear DeviceID will clear Device ID and password
 2. Apply button will configure Device ID and other parameters

SGACL-downloads en -handhaving inschakelen op verkeer

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT

Wireless

- Access Points
 - All APs
 - Direct APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
- Mesh
- ATF
- RF Profiles
- FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN
 - Templates

All APs > APb838.61ac.3598 > Trustsec Configuration

AP Name APb838.61ac.3598

Base Radio MAC b8:38:61:b8:c6:70

TrustSec Configuration

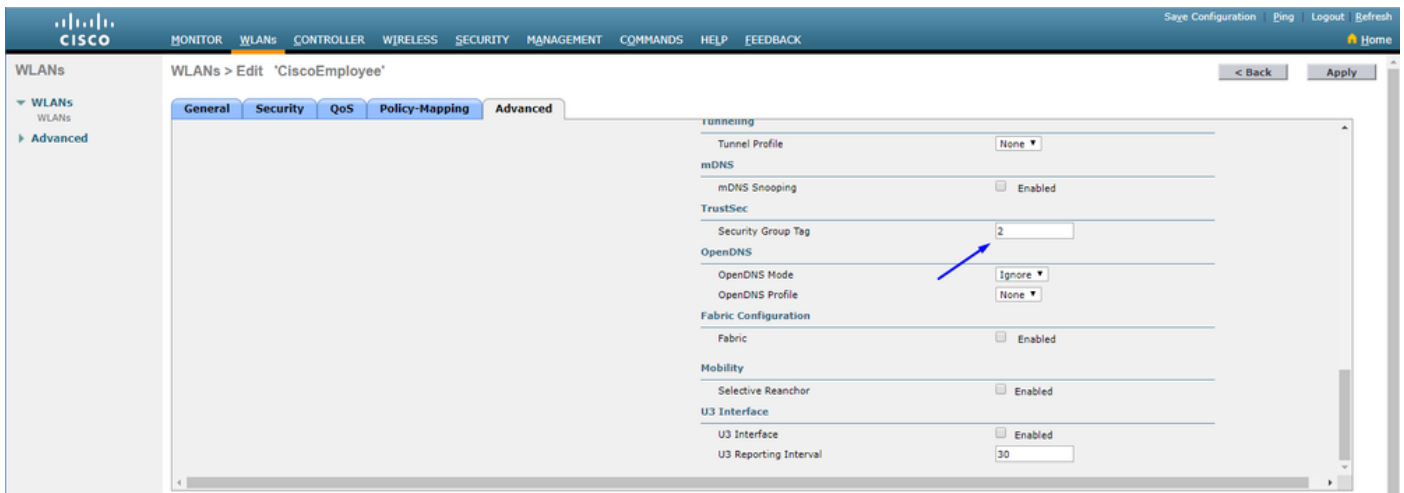
CTS Override Enabled

Sgacl Enforcement

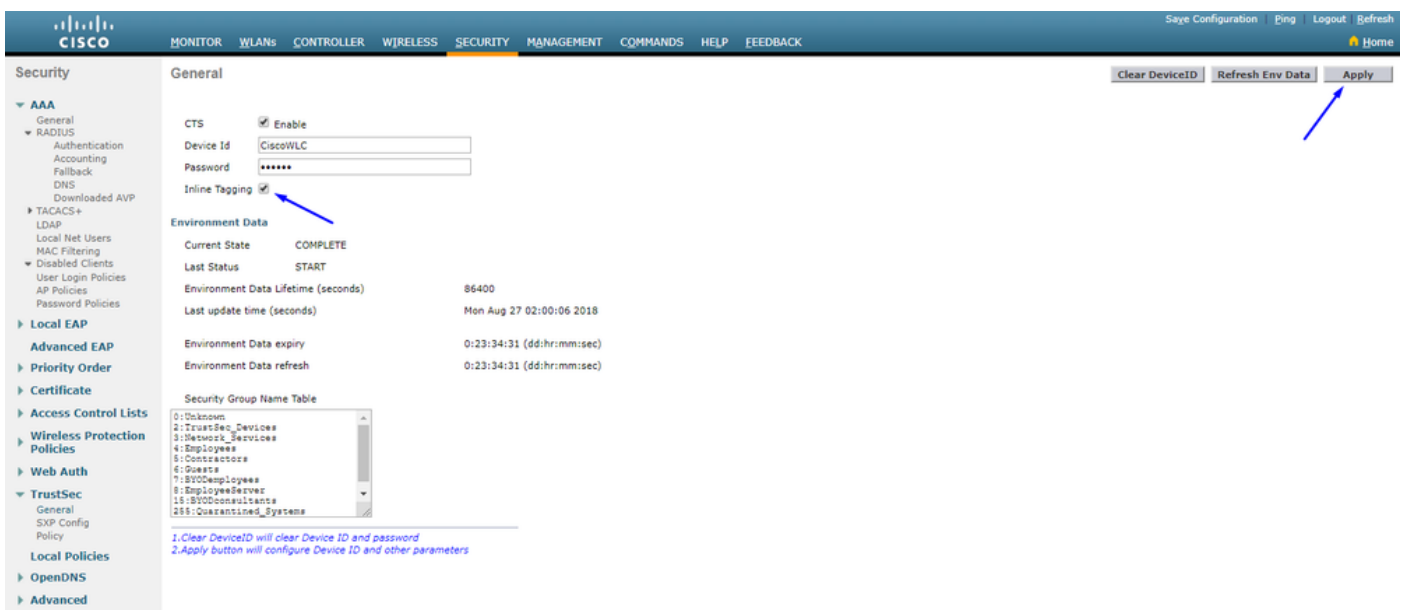
1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

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**.

Wireless

- Access Points
 - All APs
 - Direct APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
- Mesh
- ATF
- RF Profiles
- FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
- OEAP ACLs
- Network Lists
- 802.11a/n/ac
- 802.11b/g/n
- Media Stream
- Application Visibility And Control
- Lync Server
- Country
- Timers
- Netflow
- QoS

All APs TrustSec Configuration

TrustSec

Sgacl Enforcement

Inline Tagging

AP SXP State Disabled ▾

Default Password ••••••

SXP Listener Min Hold Time (seconds)

SXP Listener Max Hold Time (seconds)

SXP Speaker Hold Time (seconds)

Reconciliation Time Period (seconds)

Retry Period (seconds)

Peer Config

Peer IP Address

Password Default ▾

Local Mode Speaker ▾

ADD

Peer IP Address	Password	SXP Mode
<p>1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)</p> <p>2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)</p>		

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



Monitor Clients Entries 1 - 1 of 1

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id
b0:70:26:46:58:97	10.201.235.125	AP0838.61ac.3598CORBIN	CorbinEmployee	CorbinEmployee	jsmith	802.11ac	Associated	No	1	1

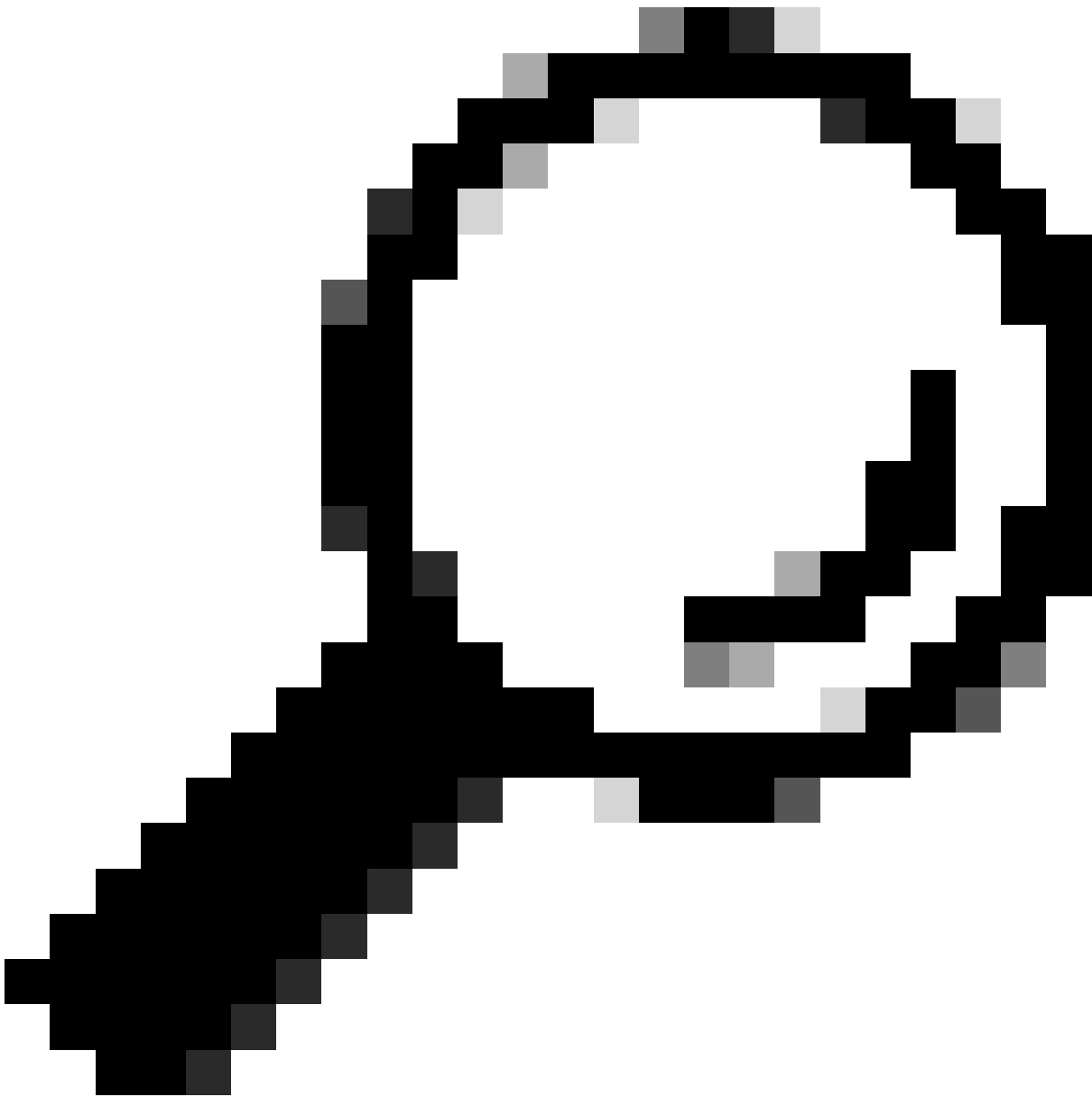
```
Catalyst 2960Switch#show-platform beltellers, hardware | Inc. SGACL
```

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

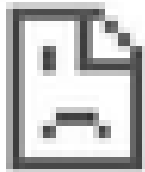


Tip: als u in plaats daarvan een Cisco ASR, Nexus of Cisco ASA gebruikt, kan het document dat hier wordt vermeld helpen verifiëren of uw SGT-tags worden gehandhaafd: [TrustSec Probleemoplossing Guide](#).

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



https://10.201.214.132



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.