

Konfigurieren von TrustSec (SGTs) mit ISE (Inline-Tagging)

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Ziel](#)

[Konfigurationen](#)

[Konfigurieren von TrustSec auf der ISE](#)

[Konfigurieren der Cisco ISE als TrustSec-AAA-Server](#)

[Konfiguration und Überprüfung, ob der Switch als RADIUS-Gerät in der Cisco ISE hinzugefügt wurde](#)

[Konfigurieren und Überprüfen, ob der WLC als TrustSec-Gerät in der Cisco ISE hinzugefügt wurde](#)

[Überprüfen der TrustSec-Standardinstellungen, um sicherzustellen, dass sie akzeptabel sind \(optional\)](#)

[Sicherheitsgruppen-Tags für Wireless-Benutzer erstellen](#)

[Erstellen einer statischen IP-SGT-Zuordnung für den eingeschränkten Webserver](#)

[Zertifikatauthentifizierungsprofil erstellen](#)

[Identitätssequenz mit dem Zertifikatauthentifizierungsprofil von vor erstellen](#)

[Zuweisen eines geeigneten SGT zu Wireless-Benutzern \(Mitarbeiter und Berater\)](#)

[Zuweisen von SGTs zu den tatsächlichen Geräten \(Switch und WLC\)](#)

[Definieren von SGACLs zum Angeben der Ausgangs-Policy](#)

[Durchsetzen Ihrer ACLs in der TrustSec-Richtlinienmatrix der Cisco ISE](#)

[TrustSec auf Catalyst Switch konfigurieren](#)

[Switch für Verwendung von Cisco TrustSec für AAA auf Catalyst Switch konfigurieren](#)

[Konfigurieren des PAC-Schlüssels unter dem RADIUS-Server für die Authentifizierung des Switches für die Cisco ISE](#)

[CTS-Anmeldeinformationen für die Authentifizierung des Switches für die Cisco ISE konfigurieren](#)

[Globale CTS-Aktivierung auf Catalyst Switch](#)

[Erstellen einer statischen IP-zu-SGT-Zuordnung für die eingeschränkten Webserver \(optional\)](#)

[TrustSec auf Catalyst Switch überprüfen](#)

[TrustSec auf WLC konfigurieren](#)

[Konfigurieren und Überprüfen, ob der WLC als RADIUS-Gerät in der Cisco ISE hinzugefügt wurde](#)

[Konfigurieren und Überprüfen, ob der WLC als TrustSec-Gerät in der Cisco ISE hinzugefügt wurde](#)

[PAC-Bereitstellung von WLC aktivieren](#)

[TrustSec auf WLC aktivieren](#)

[Überprüfen, ob PAC auf WLC bereitgestellt wurde](#)

[CTS-Umgebungsdaten von der Cisco ISE auf WLC herunterladen](#)

[SGACL-Downloads und -Durchsetzung im Datenverkehr aktivieren](#)

[WLC und Access Point das SGT von 2 \(TrustSec Devices\) zuweisen](#)

Einleitung

In diesem Dokument wird beschrieben, wie TrustSec auf einem Catalyst Switch und einem Wireless LAN Controller mit der Identity Services Engine konfiguriert und verifiziert wird.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Cisco TrustSec-Komponenten (CTS)
- Grundkenntnisse der CLI-Konfiguration von Catalyst Switches
- Grundkenntnisse der GUI-Konfiguration der Cisco Wireless LAN Controller (WLC)
- Erfahrung mit der Identity Services Engine (ISE)-Konfiguration

Anforderungen

Sie müssen die Cisco ISE in Ihrem Netzwerk implementieren, und die Endbenutzer müssen sich bei der Cisco ISE mit 802.1x (oder einer anderen Methode) authentifizieren, wenn sie eine Wireless- oder kabelgebundene Verbindung herstellen. Die Cisco ISE weist dem Datenverkehr ein Security Group Tag (SGT) zu, sobald er sich bei Ihrem Wireless-Netzwerk authentifiziert.

In unserem Beispiel werden Endbenutzer zum Cisco ISE Bring Your Own Device (BYOD)-Portal umgeleitet und erhalten ein Zertifikat, sodass sie nach Abschluss der Schritte des BYOD-Portals mit Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) sicher auf das Wireless-Netzwerk zugreifen können.

Verwendete Komponenten

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

- Cisco Identity Services Engine, Version 2.4
- Cisco Catalyst Switch der Serie 3850, Version 3.7.5E
- Cisco WLC, Version 8.5.120.0
- Cisco Aironet Wireless Access Point im lokalen Modus

Überprüfen Sie vor der Bereitstellung von Cisco TrustSec, ob der Cisco Catalyst Switch und/oder die Cisco WLC+AP-Modelle und -Softwareversion Unterstützung für Folgendes bieten:

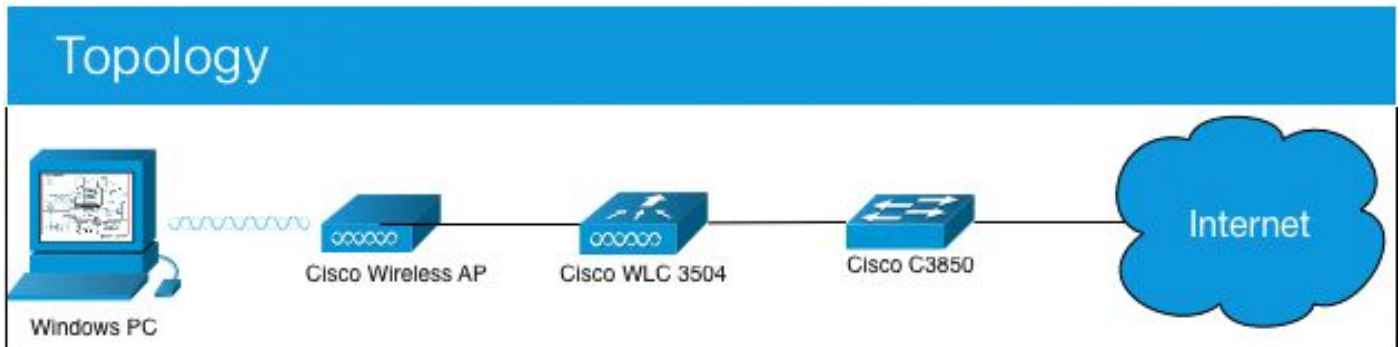
- TrustSec/Security Group Tags
- Inline-Tagging (andernfalls können Sie SXP anstelle von Inline-Tagging verwenden)
- Statische Zuordnungen von IP zu SGT (falls erforderlich)
- Statische Zuordnungen von Subnetz zu SGT (falls erforderlich)

- Statische VLAN-zu-SGT-Zuordnungen (falls erforderlich)

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



In diesem Beispiel kennzeichnet der WLC die Pakete als SGT 15, wenn von einem Berater, und + SGT 7, wenn von einem Mitarbeiter.

Der Switch verweigert diese Pakete, wenn sie sich zwischen SGT 15 und SGT 8 befinden (Berater können nicht auf Server zugreifen, die als SGT 8 getaggt sind).

Der Switch lässt diese Pakete zu, wenn sie sich zwischen SGT 7 und SGT 8 befinden (Mitarbeiter können auf Server zugreifen, die als SGT 8 getaggt sind).

Ziel

Jeder kann auf die GuestSSID zugreifen.

Zugriff für Berater auf die EmployeeSSID, jedoch mit eingeschränktem Zugriff

Ermöglichen Sie Mitarbeitern den Zugriff auf EmployeeSSID mit vollständigem Zugriff.

"Slot0:"	IP-Adresse	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		
Name	Benutzername	AD-Gruppe	SG	SGT
Jason Smith	Schmied	Berater	BYOD-Berater	15
Sally Smith	Schmied	Mitarbeiter	BYOD-Mitarbeiter	7
-	-	-	TrustSec-Geräte	2

Konfigurationen

Konfigurieren von TrustSec auf der ISE

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>

Konfigurieren der Cisco ISE als TrustSec-AAA-Server

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'TrustSec' menu is expanded, showing options like 'BYOD', 'Profiler', 'Posture', 'Device Administration', and 'PassiveID'. The 'TrustSec Policy' sub-menu is selected, showing 'Overview', 'Components', 'TrustSec Policy', 'Policy Sets', 'SXP', 'Troubleshoot', 'Reports', and 'Settings'. The 'TrustSec AAA Servers' configuration page is displayed, showing the following fields:

- AAA Servers List > corbinise**
- AAA Servers**
- * Name:** CISCOISE
- Description:** (Empty text area)
- * IP:** 10.201.214.230 (Example: 10.1.1.1)
- * Port:** 1812 (Valid Range 1 to 65535)
- Buttons:** Save, Reset

Konfiguration und Überprüfung, ob der Switch als RADIUS-Gerät in der Cisco ISE hinzugefügt wurde

The screenshot displays the Cisco ISE web interface for configuring a Network Device. The breadcrumb navigation shows: Home > Context Visibility > Operations > Policy > Administration > Work Centers > 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.

The main configuration area is titled "Network Devices" and shows the configuration for a device named "CatalystSwitch". The configuration includes:

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

Konfigurieren und Überprüfen, ob der WLC als TrustSec-Gerät in der Cisco ISE hinzugefügt wurde

Geben Sie Ihre Anmeldeinformationen für SSH ein. Auf diese Weise kann die Cisco ISE die statischen IP-zu-SGT-Zuordnungen für den Switch bereitstellen.

Sie erstellen diese in der Cisco ISE Web-GUI unter Work Centers > TrustSec > Components > IP SGT Static Mappings, wie hier gezeigt:

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:

SSH Key:

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates:

Device Interface Credentials

* EXEC Mode Username:

* EXEC Mode Password:

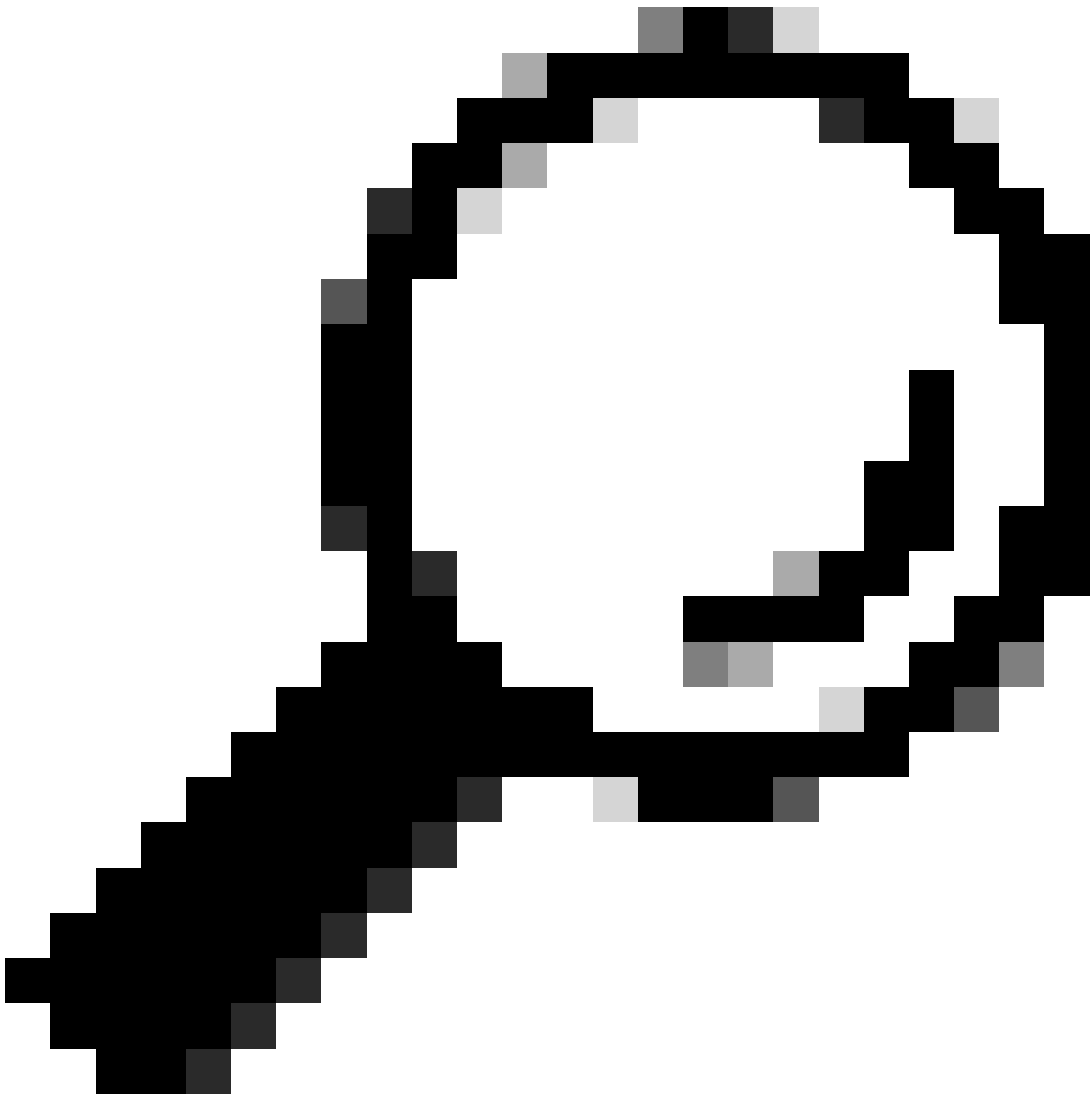
Enable Mode Password:

Out Of Band (OOB) TrustSec PAC

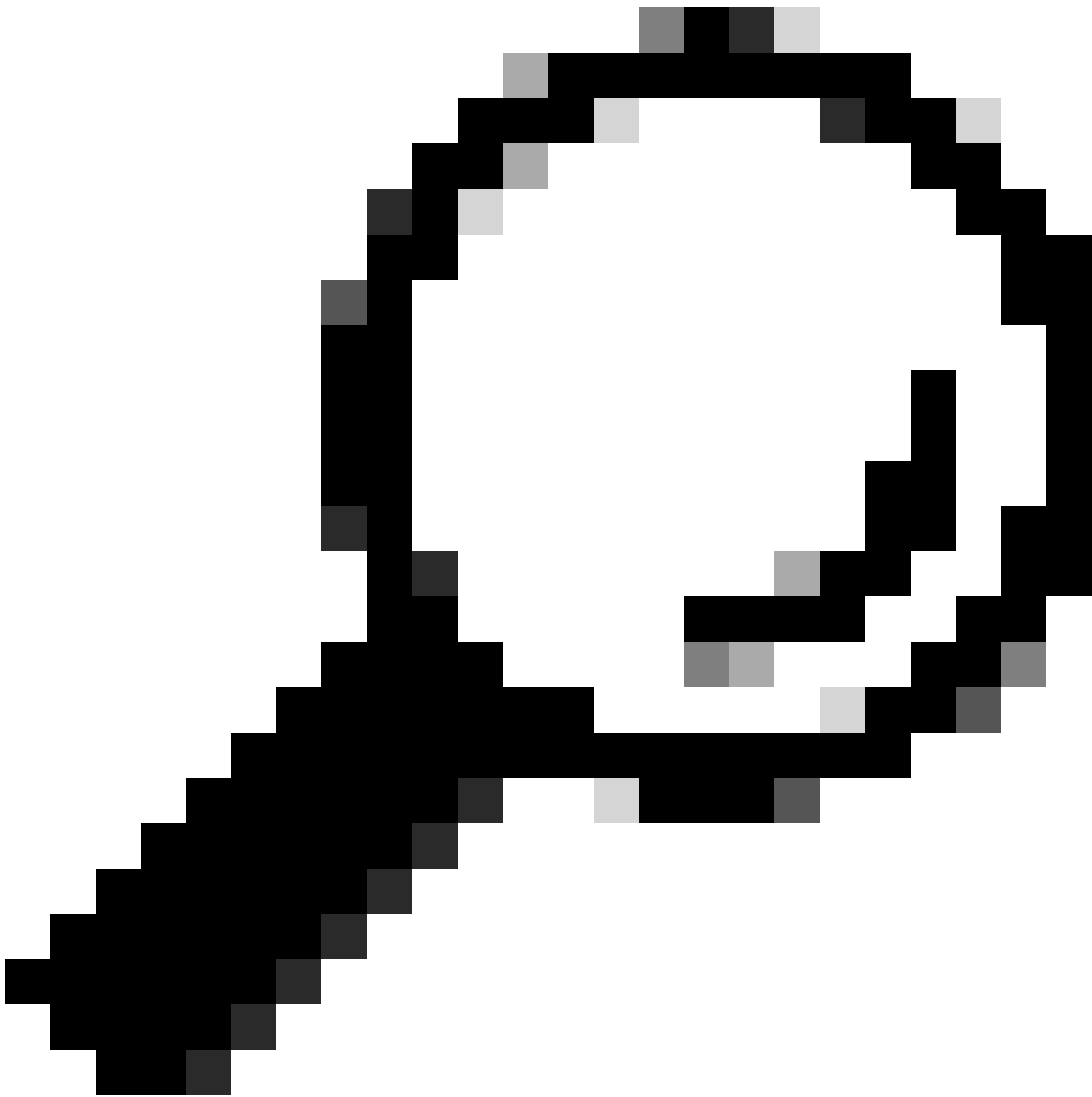
Issue Date:

Expiration Date:

Issued By:



Tipp: Wenn Sie SSH auf Ihrem Catalyst Switch noch nicht konfiguriert haben, können Sie dieses Handbuch verwenden: [How to Configure Secure Shell \(SSH\) on Catalyst Switch](#).



Tipp: Wenn Sie nicht möchten, dass die Cisco ISE über SSH auf Ihren Catalyst Switch zugreift, können Sie stattdessen statische IP-zu-SGT-Zuordnungen auf dem Catalyst Switch mit der CLI erstellen (hier in einem Schritt dargestellt).

Überprüfen der TrustSec-Standardeinstellungen, um sicherzustellen, dass sie akzeptabel sind (optional)



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

Sicherheitsgruppen-Tags für Wireless-Benutzer erstellen

Einrichtung einer Sicherheitsgruppe für BYOD-Berater - SGT 15

Einrichtung einer Sicherheitsgruppe für BYOD-Mitarbeiter - 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	

Erstellen einer statischen IP-SGT-Zuordnung für den eingeschränkten Webserver

Führen Sie dies für alle anderen IP-Adressen oder Subnetze in Ihrem Netzwerk aus, die sich nicht bei der Cisco ISE mit MAB (MAC Authentication Bypass), 802.1x, Profilen usw. authentifizieren.

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

Zertifikatauthentifizierungsprofil erstellen

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

Identitätsquellensequenz mit dem Zertifikatauthentifizierungsprofil von vor erstellen

[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;"> <p>Internal Endpoints</p> <p>Guest Users</p> </div>	<p>></p> <p><</p> <p>>></p> <p><<</p>	<p>Selected</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <p>Windows_AD_Server</p> <p>Internal Users</p> </div>	<p>⏪</p> <p>⏩</p> <p>⏴</p> <p>⏵</p>
---	---	--	-------------------------------------

▼ 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

Zuweisen eines geeigneten SGT zu Wireless-Benutzern (Mitarbeiter und Berater)

Name	Benutzername	AD-Gruppe	SG	SGT
Jason Smith	Schmied	Berater	BYOD-Berater	15
Sally Smith	Schmied	Mitarbeiter	BYOD-Mitarbeiter	7
–	–	–	TrustSec-Geräte	2

Policy Sets - EmployeeSSID

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
On	EmployeeSSID		Airspace Airspace-10anId EQUALS 2	Default Network Access	631

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
On	DetX	Wireless_802.1X	BYODIdentitySequence	230	Options
On	Default		AllUsersIDStores	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	NetworkAccess EapAuthentication EQUALS EAP-TLS corbd3 ExternalGroups EQUALS cohadley3 localUsers/Consultants	PermAccess	BYODconsultants	57	Options
On	Allow Anywhere if BYODRegistered and EAP-TLS and AD Group = Employees	NetworkAccess EapAuthentication EQUALS EAP-TLS corbd3 ExternalGroups EQUALS cohadley3 localUsers/Employees	PermAccess	BYODEmployees	0	Options
On	Default		NISP_Onboard	Selected from list	109	Options

Zuweisen von SGTs zu den tatsächlichen Geräten (Switch und WLC)

Identity Services Engine - Work Centers - TrustSec - BYOD - Profiler

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

Definieren von SGACLs zum Angeben der Ausgangs-Policy

Ermöglichen Sie Beratern den Zugriff von einem beliebigen externen Standort aus, schränken Sie jedoch den internen Zugriff ein:

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

```

Ermöglichen Sie Mitarbeitern den Zugriff von einem externen und einem internen Standort aus:

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

```

Zulassen des Zugriffs auf Basisdienste für andere Geräte (optional):

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

```

Umleitung aller Endbenutzer auf die Cisco ISE (für die BYOD-Portalumleitung) Keine DNS-, DHCP-, Ping- oder WebAuth-Zugriffe, da diese nicht an die Cisco ISE gesendet werden können:

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

```

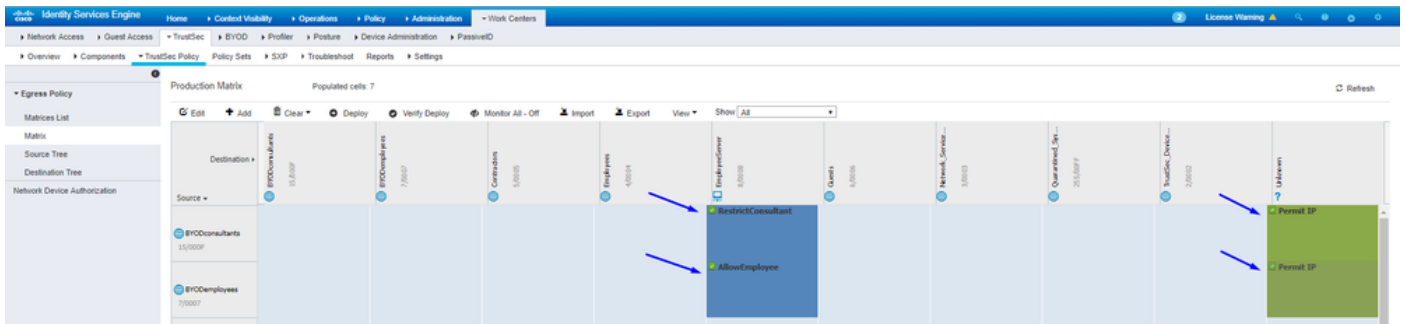
deny udp dst eq 67
deny udp dst eq 53
deny tcp dst eq 53
deny icmp
deny tcp dst eq 8443
permit ip

```

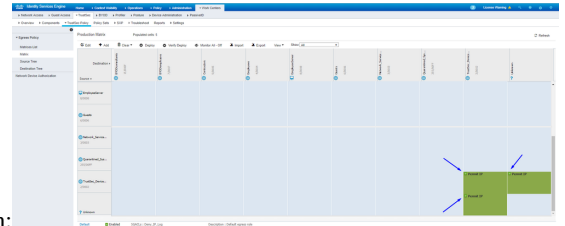
Durchsetzen Ihrer ACLs in der TrustSec-Richtlinienmatrix der Cisco ISE

Zugriff für Berater von beliebigen externen Standorten aus, jedoch mit Einschränkungen für interne Webserver wie <https://10.201.214.132>

Mitarbeitern den Zugriff von beliebigen externen Standorten und internen Webservern ermöglichen:

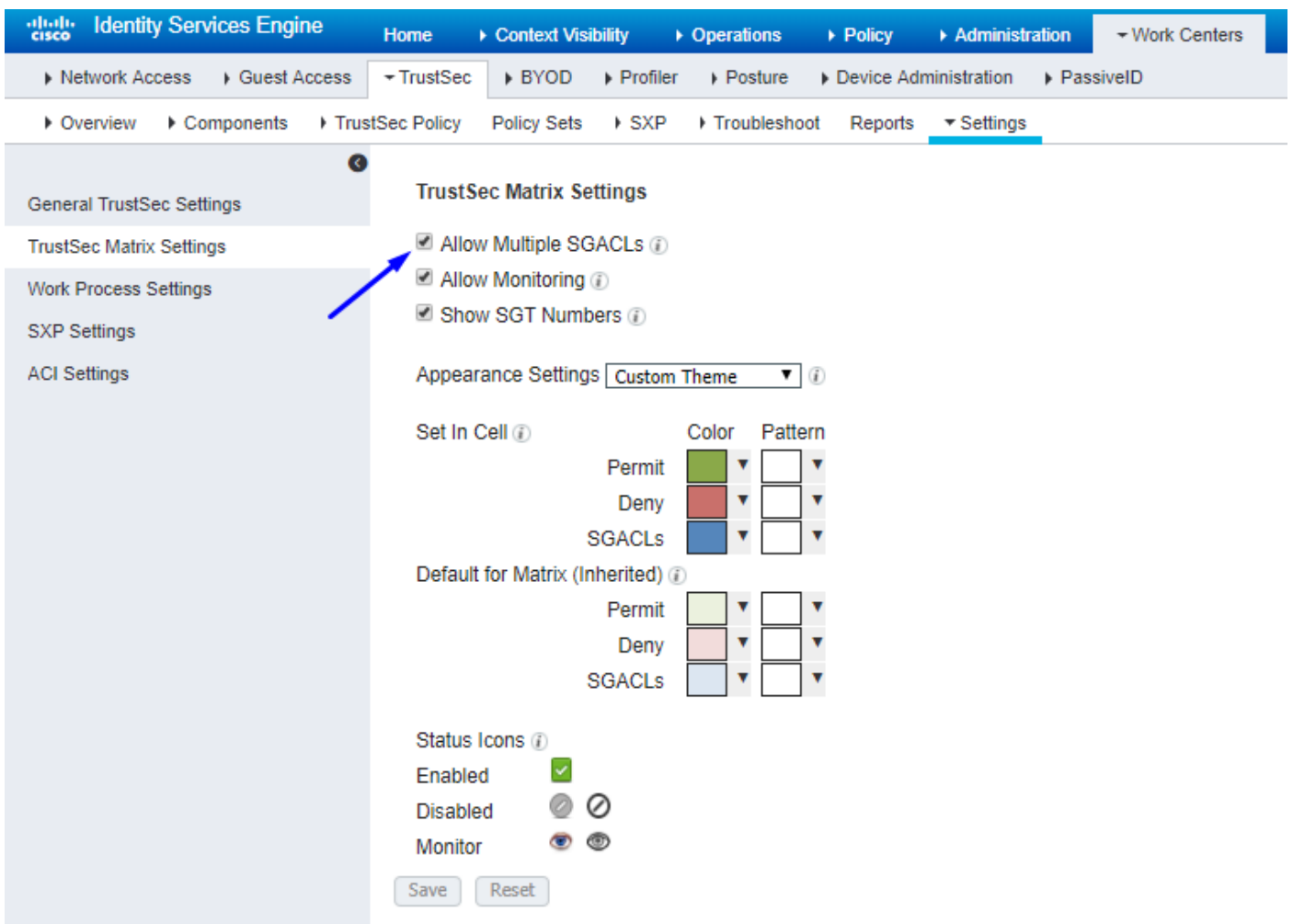


Lassen Sie den Verwaltungsdatenverkehr (SSH, HTTPS und CAPWAP) zu/von Ihren Geräten im Netzwerk (Switch und WLC) zu, damit Sie



nach der Bereitstellung von Cisco TrustSec keinen SSH- oder HTTPS-Zugriff verlieren:

Vorteile der Cisco ISE Allow Multiple SGACLs:



Push Klicken Sie oben rechts auf der Cisco ISE auf, um die Konfiguration auf die gewünschten Geräte zu verschieben. Dies müssen Sie später erneut tun:

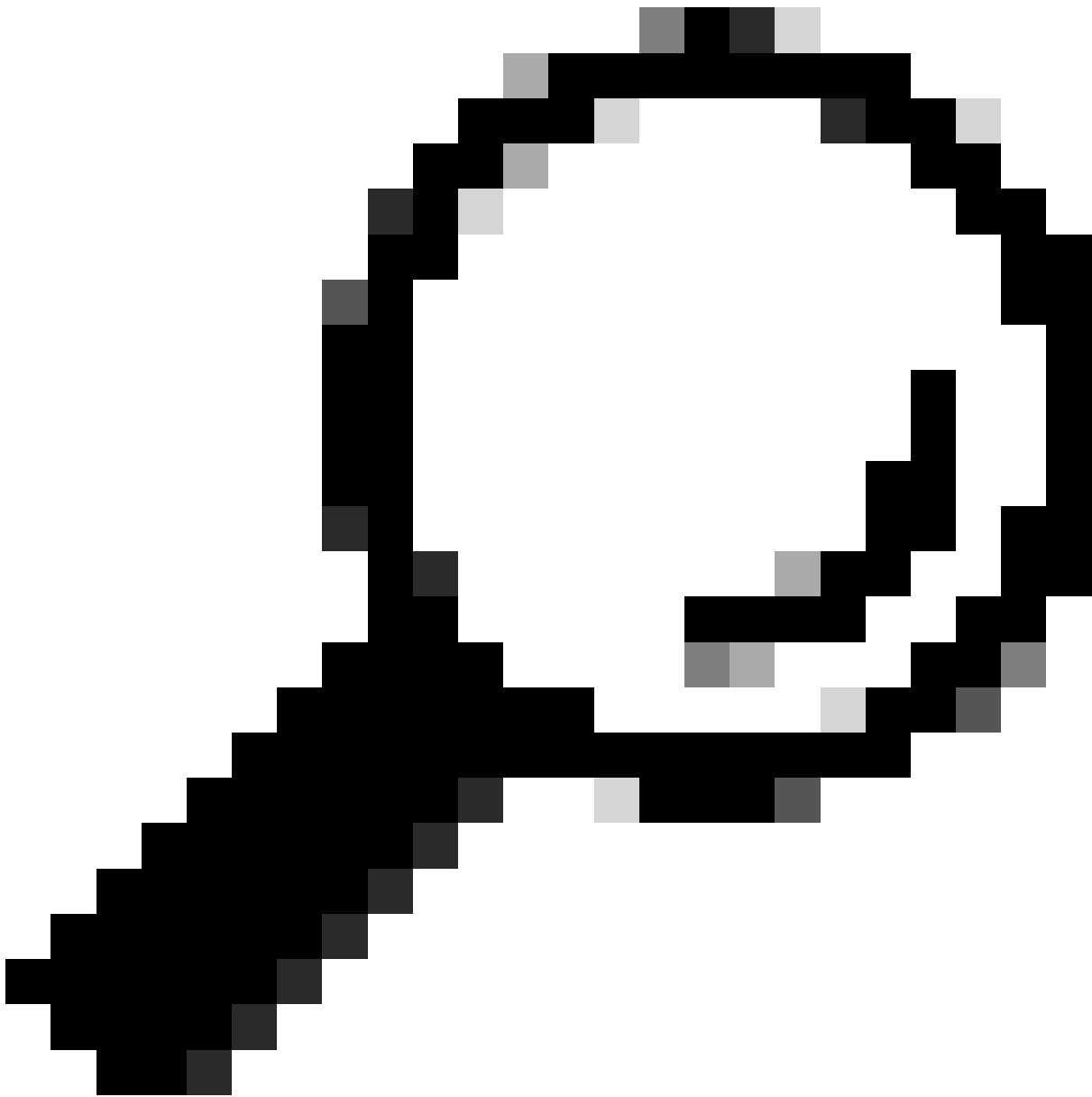
There are TrustSec configuration changes that has not been notified to network devices. To notify the relevant network devices about these changes click the push button.



Push

TrustSec auf Catalyst Switch konfigurieren

Switch für Verwendung von Cisco TrustSec für AAA auf Catalyst Switch konfigurieren



Tipp: In diesem Dokument wird davon ausgegangen, dass Ihre Wireless-Benutzer bereits vor der hier gezeigten Konfiguration erfolgreich BYOD über die Cisco ISE nutzen.

Die fett formatierten Befehle wurden bereits zuvor konfiguriert (damit BYOD Wireless mit der ISE funktioniert).

<#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
```



Hinweis: Der PAC-Schlüssel muss mit dem RADIUS Shared Secret identisch sein, das Sie im **Administration > Network Devices > Add Device > RADIUS Authentication Settings** Abschnitt angegeben haben.

<#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
```

Konfigurieren des PAC-Schlüssels unter dem RADIUS-Server für die Authentifizierung des Switches für die 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
```

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret

Use Second Shared Secret ⓘ



Hinweis: Der PAC-Schlüssel muss mit dem RADIUS Shared Secret identisch sein, das Sie im **Administration > Network Devices > Add Device > RADIUS Authentication Settings** Abschnitt in der Cisco ISE angegeben haben (wie im Screenshot gezeigt).

CTS-Anmeldeinformationen für die Authentifizierung des Switches für die Cisco ISE konfigurieren

CatalystSwitch#cts credentials id CatalystSwitch password Admin123

Identity Services Engine

Home > Context Visibility > Operations > Policy > 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

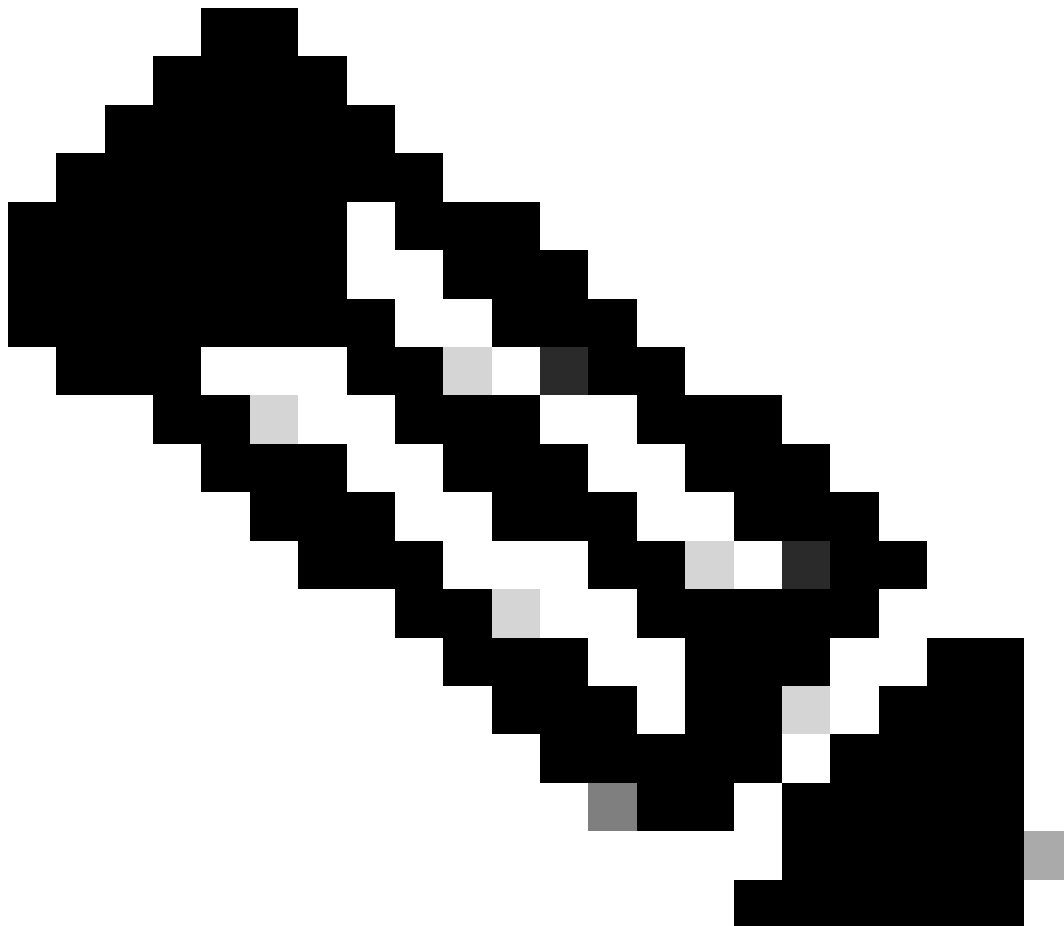
Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id CatalystSwitch

* Password Admin123



Hinweis: Die CTS-Anmeldedaten müssen mit der Geräte-ID + dem Kennwort übereinstimmen, die Sie unter Die CTS-Anmeldedaten müssen mit der Geräte-ID + dem Kennwort übereinstimmen, die Sie im Abschnitt derAdministration > Network

Devices > Add Device > Advanced TrustSec Settings Cisco ISE (im Screenshot dargestellt) angegeben haben.

Aktualisieren Sie anschließend Ihre PAC, damit sie sich erneut an die Cisco ISE wendet:

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

Globale CTS-Aktivierung auf 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)
```

Erstellen einer statischen IP-zu-SGT-Zuordnung für die eingeschränkten Webserver (optional)

Dieser eingeschränkte Webserver wird niemals zur Authentifizierung über die ISE übermittelt. Sie müssen ihn daher manuell mit der Switch-CLI oder der ISE Web-GUI taggen, die nur einer von vielen Webservern in Cisco ist.

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

TrustSec auf Catalyst Switch überprüfen

```
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
```

TrustSec auf WLC konfigurieren

Konfigurieren und Überprüfen, ob der WLC als RADIUS-Gerät in der Cisco ISE hinzugefügt wurde

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: * IP: 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]

Konfigurieren und Überprüfen, ob der WLC als TrustSec-Gerät in der Cisco ISE hinzugefügt wurde

Mit diesem Schritt kann die Cisco ISE statische IP-SGT-Zuordnungen zum WLC bereitstellen. Sie haben diese Zuordnungen in einem vorherigen Schritt in der Cisco ISE-Web-GUI unter **Work Centers > TrustSec > Components > IP SGT Static Mappings** erstellt.

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



Hinweis: Wir verwenden diese Device Id und Password in einem späteren Schritt in der WLC-Webbenutzeroberfläche Security > TrustSec > General.

PAC-Bereitstellung von WLC aktivieren

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
 - 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 auf WLC aktivieren

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





Hinweis: CTS Device Id und Password müssen mit dem Device Id übereinstimmen, Password das Sie in Cisco ISE imAdministration > Network Devices > Add Device > Advanced TrustSec Settings Abschnitt angegeben haben.

Überprüfen, ob PAC auf WLC bereitgestellt wurde

Wenn Sie auf klicken, wird die PAC erfolgreich vom WLC bereitgestellt (in diesem Schritt durchführen)Refresh Env Data:

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-Umgebungsdaten von der Cisco ISE auf WLC herunterladen

Wenn Sie auf klickenRefresh Env Data, lädt der WLC Ihre SGTs herunter.

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 und -Durchsetzung im Datenverkehr aktivieren

CISCO 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

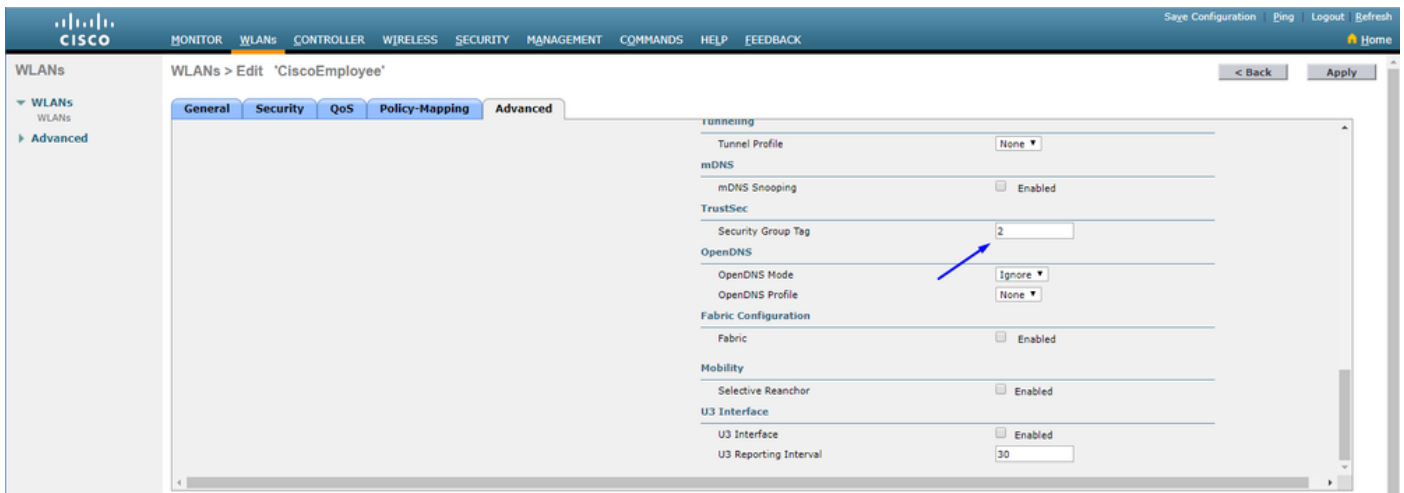
CTS Override Enabled

Sgacl Enforcement

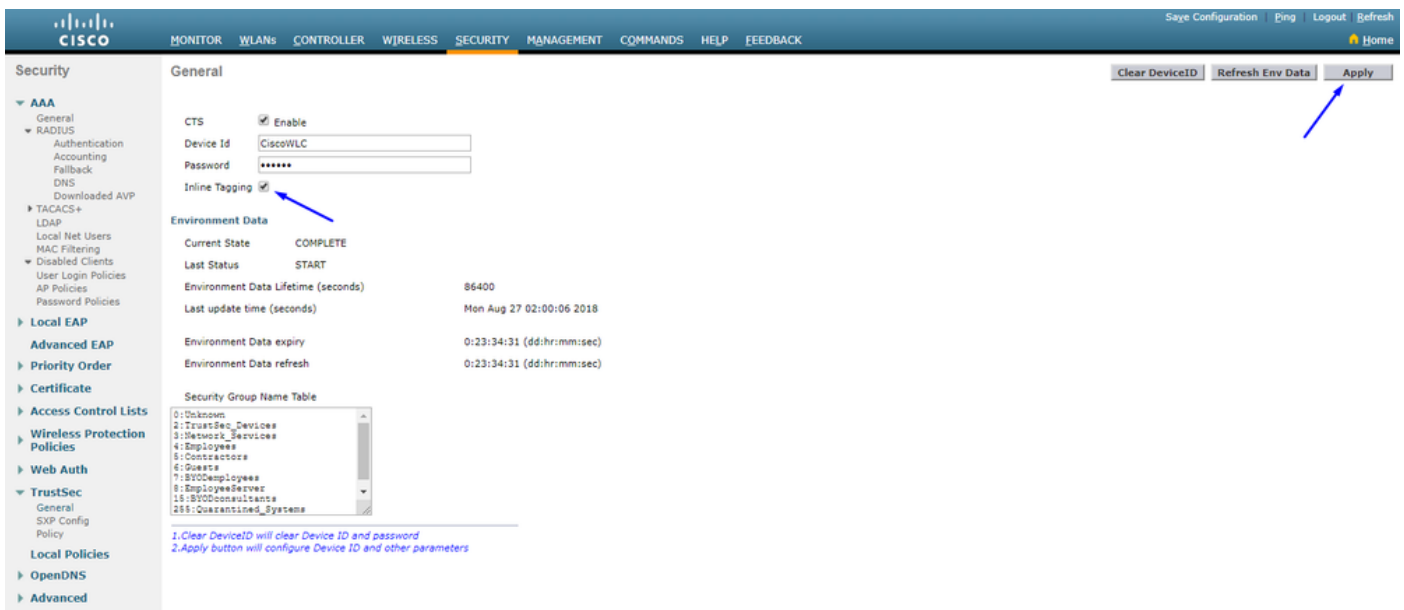
1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

WLC und Access Point das SGT von 2 (TrustSec_Devices) zuweisen

Weisen Sie dem WLC+WLAN ein SGT von 2 (TrustSec_Devices) zu, um Datenverkehr (SSH, HTTPS und CAPWAP) vom/zum WLC+AP über den Switch zuzulassen.



Inline-Tagging auf WLC aktivieren



Scrollen Sie **Wireless > Access Points > Global Configuration** nach unten und wählen Sie **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 auf Catalyst Switch aktivieren

```
<#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
```

Überprüfung



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
b0:70:2d:46:58:97	10.201.235.125	AP0838.61ac.3598CORBIN	CorbinEmployee	CorbinEmployee	jsmith	802.11ac	Associated	No	1	1

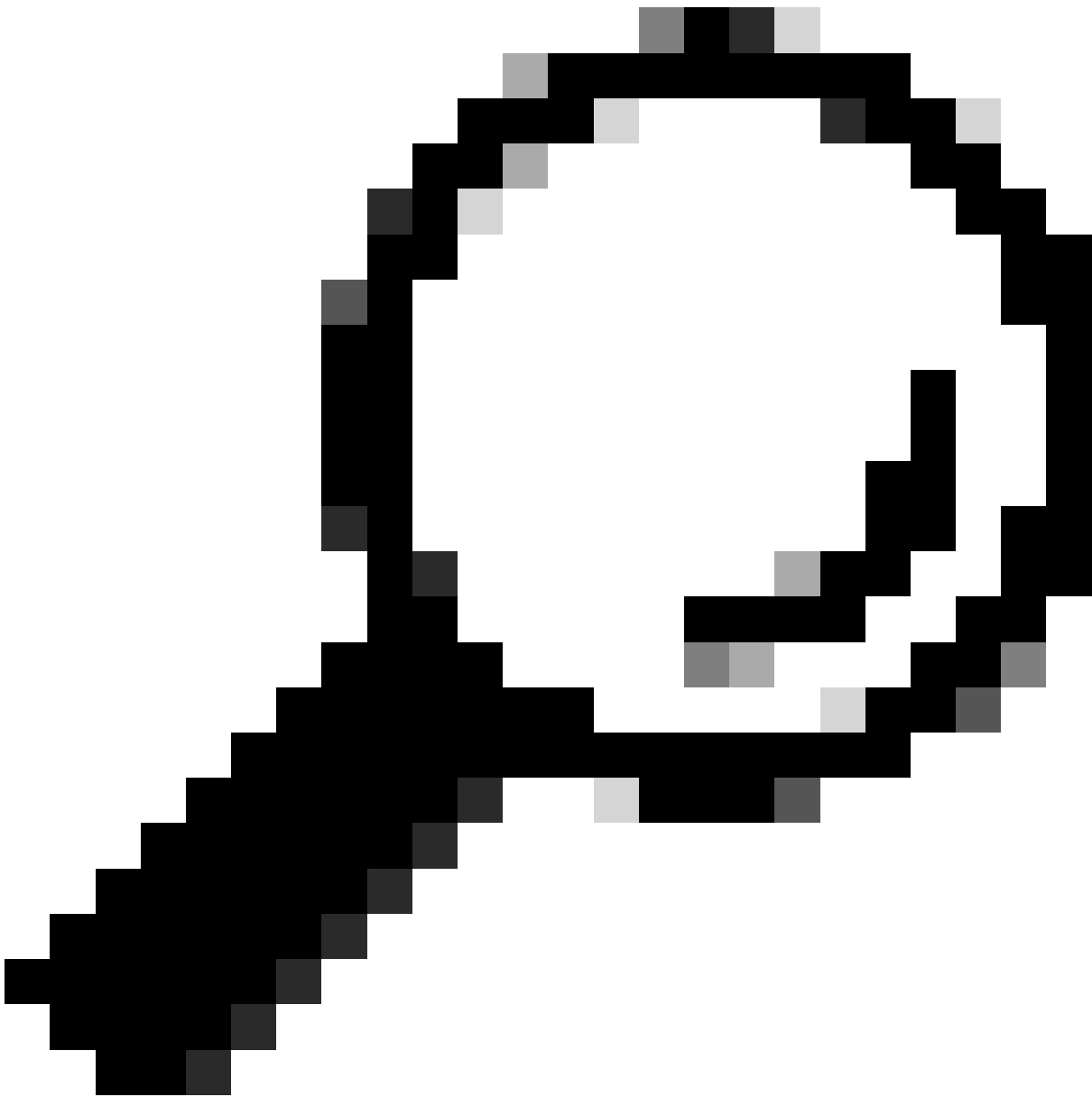
```
CatalystSwitch#show platform acl counters hardware | inkl. SGACL
```

Ausgangs-IPv4-SGACL-Drop (454): 10 Frames

Ausgangs-IPv6-SGACL-Drop (455): 0 Frames

Ausgangs-IPv4-SGACL-Zellverlust (456): 0 Frames

Ausgangs-IPv6-SGACL-Zellverlust (457): 0 Frames

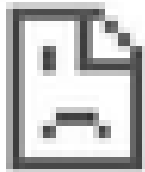


Tipp: Wenn Sie stattdessen einen Cisco ASR, Nexus oder Cisco ASA verwenden, kann das hier aufgeführte Dokument dabei helfen, sicherzustellen, dass Ihre SGT-Tags durchgesetzt werden: [TrustSec Troubleshooting Guide](#).

Mit dem Benutzernamen jsmith password Admin123 für Wireless-Zugriff authentifizieren - auf dem Switch wird die ACL "deny" (ACL ablehnen) angezeigt:



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

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.