

# Configuración de TrustSec (SGT) con ISE (etiquetado en línea)

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

### [Configurar](#)

[Diagrama de la red](#)

[Objetivo](#)

[Configuraciones](#)

[Configuración de TrustSec en ISE](#)

[Configuración de Cisco ISE como servidor AAA de TrustSec](#)

[Configure and Verify Switch is Added as a RADIUS Device in Cisco ISE](#)

[Configure y verifique que el WLC se agrega como un dispositivo TrustSec en Cisco ISE](#)

[Verifique la configuración predeterminada de TrustSec para asegurarse de que es aceptable \(opcional\)](#)

[Creación de etiquetas de grupos de seguridad para usuarios inalámbricos](#)

[Crear asignación de IP a SGT estática para el servidor web restringido](#)

[Crear perfil de autenticación de certificado](#)

[Crear secuencia de origen de identidad con el perfil de autenticación de certificado anterior](#)

[Asignar a los usuarios inalámbricos \(empleados y consultores\) una SGT adecuada](#)

[Asignar SGT a los dispositivos reales \(switch y WLC\)](#)

[Definición de SGACL para Especificar la Política de Salida](#)

[Aplique sus ACL en la matriz de políticas de TrustSec en Cisco ISE](#)

[Configuración de TrustSec en el switch Catalyst](#)

[Configuración del switch para utilizar Cisco TrustSec para AAA en el switch Catalyst](#)

[Configuración de la clave PAC en el servidor RADIUS para autenticar el switch en Cisco ISE](#)

[Configuración de credenciales CTS para autenticar el switch en Cisco ISE](#)

[Habilitación global de CTS en switch Catalyst](#)

[Creación de una asignación estática de IP a SGT para los servidores web restringidos \(opcional\)](#)

[Verifique TrustSec en el switch Catalyst](#)

[Configuración de TrustSec en WLC](#)

[Configure y verifique que el WLC se agrega como un dispositivo RADIUS en Cisco ISE](#)

[Configure y verifique que el WLC se agrega como un dispositivo TrustSec en Cisco ISE](#)

[Habilitación de la Provisión PAC del WLC](#)

[Activar TrustSec en WLC](#)

[Verifique que PAC se haya aprovisionado en el WLC](#)

[Descargue los datos del entorno CTS de Cisco ISE al WLC](#)

[Habilitar las descargas SGACL y su aplicación en el tráfico](#)

[Asignar WLC y punto de acceso al SGT de 2 \(TrustSec Devices\)](#)

[Activar etiquetado en línea en WLC](#)

[Activar etiquetado en línea en switch Catalyst](#)

### [Verificación](#)

---

# Introducción

Este documento describe cómo configurar y verificar TrustSec en un switch Catalyst y un controlador de LAN inalámbrica con Identity Services Engine.

## Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de los componentes de Cisco TrustSec (CTS)
- Conocimientos básicos sobre la configuración CLI de los switches Catalyst
- Conocimientos básicos de la configuración GUI de Cisco Wireless LAN Controllers (WLC)
- Experiencia con la configuración de Identity Services Engine (ISE)

## Requirements

Debe tener Cisco ISE implementado en la red y los usuarios finales deben autenticarse en Cisco ISE con 802.1x (u otro método) cuando se conectan a redes inalámbricas o por cable. Cisco ISE asigna a su tráfico una etiqueta de grupo de seguridad (SGT) una vez que se autentica en la red inalámbrica.

En nuestro ejemplo, se redirige a los usuarios finales al portal "Traiga su propio dispositivo" (BYOD) de Cisco ISE y se les proporciona un certificado para que puedan acceder de forma segura a la red inalámbrica con protocolo de autenticación ampliable-seguridad de la capa de transporte (EAP-TLS) una vez que completen los pasos del portal BYOD.

## Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cisco Identity Services Engine, versión 2.4
- Switch Cisco Catalyst 3850, versión 3.7.5E
- Cisco WLC, versión 8.5.120.0
- Punto de acceso inalámbrico Cisco Aironet en modo local

Antes de implementar Cisco TrustSec, compruebe que el switch Catalyst de Cisco o los modelos WLC+AP de Cisco + versión de software son compatibles con:

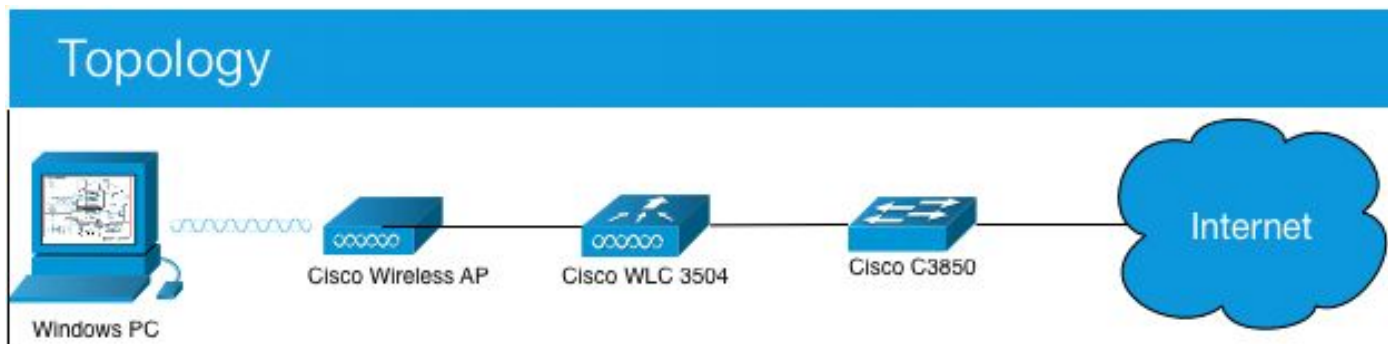
- TrustSec/Security Group Tags
- Etiquetado en línea (si no es así, puede utilizar SXP en lugar de Etiquetado en línea)
- Asignaciones de IP a SGT estáticas (si es necesario)
- Asignaciones de subred a SGT estáticas (si es necesario)
- Asignaciones de VLAN a SGT estáticas (si es necesario)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

## Configurar

### Diagrama de la red



En este ejemplo, el WLC etiqueta los paquetes como SGT 15 si provienen de un Consultor, y + SGT 7 si provienen de un Empleado.

El switch deniega esos paquetes si van de SGT 15 a SGT 8 (los consultores no pueden acceder a los servidores etiquetados como SGT 8).

El switch permite estos paquetes si van de SGT 7 a SGT 8 (los empleados pueden acceder a los servidores etiquetados como SGT 8).

### Objetivo

Permita que cualquier persona acceda a GuestSSID.

Permita que los consultores accedan a EmployeeSSID, pero con acceso restringido.

Permita que los empleados accedan a EmployeeSSID con acceso completo.

Dispositivo	Dirección IP	VLAN		
ISE	10.201.214.230	463		
Catalyst Switch	10.201.235.102	1115		
WLC	10.201.214.229	463		
Punto de Acceso	10.201.214.138	455		
Nombre	Nombre de usuario	Grupo AD	SG	SGT
Jason Smith	jsmith	Consultores	Consultores BYOD	15
Sally Smith	hormiguero	Empleados	Empleados BYOD	7
n/a	n/a	n/a	Dispositivos_TrustSec	2

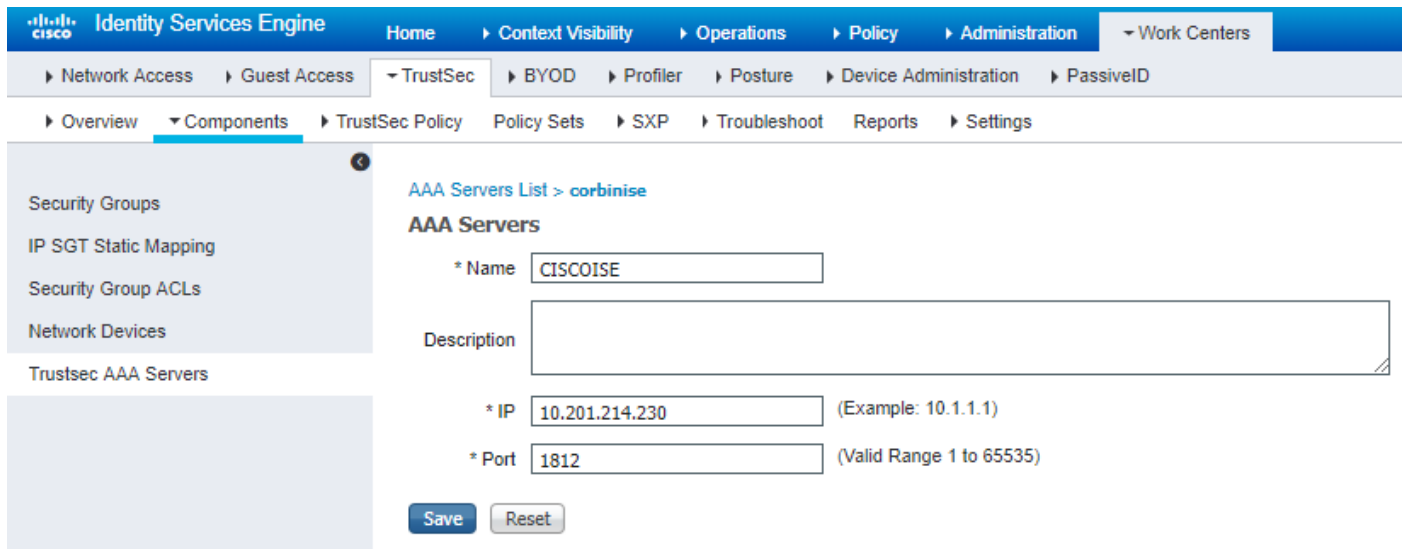
### Configuraciones

#### Configuración de TrustSec en ISE

## TrustSec Overview

1 Prepare	2 Define	3 Go Live & Monitor
<p><b>Plan Security Groups</b> 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><b>Preliminary Setup</b> Set up the <a href="#">TrustSec AAA server</a>.</p> <p>Set up TrustSec <a href="#">network devices</a>.</p> <p>Check default TrustSec <a href="#">settings</a> to make sure they are acceptable.</p> <p>If relevant, set up <a href="#">TrustSec-ACI</a> policy group exchange to enable consistent policy across your network.</p> <p>Consider activating the <a href="#">workflow process</a> to prepare staging policy with an approval process.</p>	<p><b>Create Components</b> Create <a href="#">security groups</a> 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 <a href="#">network device authorization policy</a> by assigning SGTs to network devices.</p> <p><b>Policy</b> Define <a href="#">SGACLs</a> to specify egress policy.</p> <p>Assign SGACLs to cells within the <a href="#">matrix</a> to enforce security.</p> <p><b>Exchange Policy</b> Configure <a href="#">SXP</a> to allow distribution of IP to SGT mappings directly to TrustSec enforcement devices.</p>	<p><b>Push Policy</b> Push the <a href="#">matrix</a> policy live.</p> <p>Push the <a href="#">SGTs</a>, <a href="#">SGACLs</a> and the <a href="#">matrix</a> to the network devices <a href="#">i</a></p> <p><b>Real-time Monitoring</b> Check <a href="#">dashboards</a> to monitor current access.</p> <p><b>Auditing</b> Examine <a href="#">reports</a> to check access and authorization is as intended.</p>

## Configuración de Cisco ISE como servidor AAA de TrustSec



The screenshot shows the Cisco ISE web interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > Overview > Components > TrustSec Policy > AAA Servers List > corbinise. The main content area is titled "AAA Servers" and contains a form for configuring a new server. The form fields are: \* Name (CISCOISE), Description (empty), \* IP (10.201.214.230, Example: 10.1.1.1), and \* Port (1812, Valid Range 1 to 65535). There are "Save" and "Reset" buttons at the bottom of the form.

## Configure and Verify Switch is Added as a RADIUS Device in Cisco ISE

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path 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' selected, with sub-items for '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 and Software Version: (empty dropdowns); \* Network Device Group: Location (All Locations), IPSEC (No), Device Type (All Device Types), each with a 'Set To Default' button. A checked checkbox is visible on the left side of the 'RADIUS Authentication Settings' section. This section is expanded to show 'RADIUS UDP Settings' with: Protocol: RADIUS; \* Shared Secret: Admin123; Use Second Shared Secret: (unchecked); CoA Port: 1700; and 'RADIUS DTLS Settings' with: DTLS Required: (unchecked); Shared Secret: radius/dtls. Blue arrows point to the Name, IP Address, Device Profile, and Protocol fields.

Configure y verifique que el WLC se agrega como un dispositivo TrustSec en Cisco ISE

Introduzca sus credenciales de inicio de sesión para SSH. Esto permite a Cisco ISE implementar las asignaciones de IP a SGT estáticas en el switch.

Puede crearlos en la GUI web de Cisco ISE en Work Centers > TrustSec > Components > IP SGT Static Mappings como se muestra a continuación:

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:

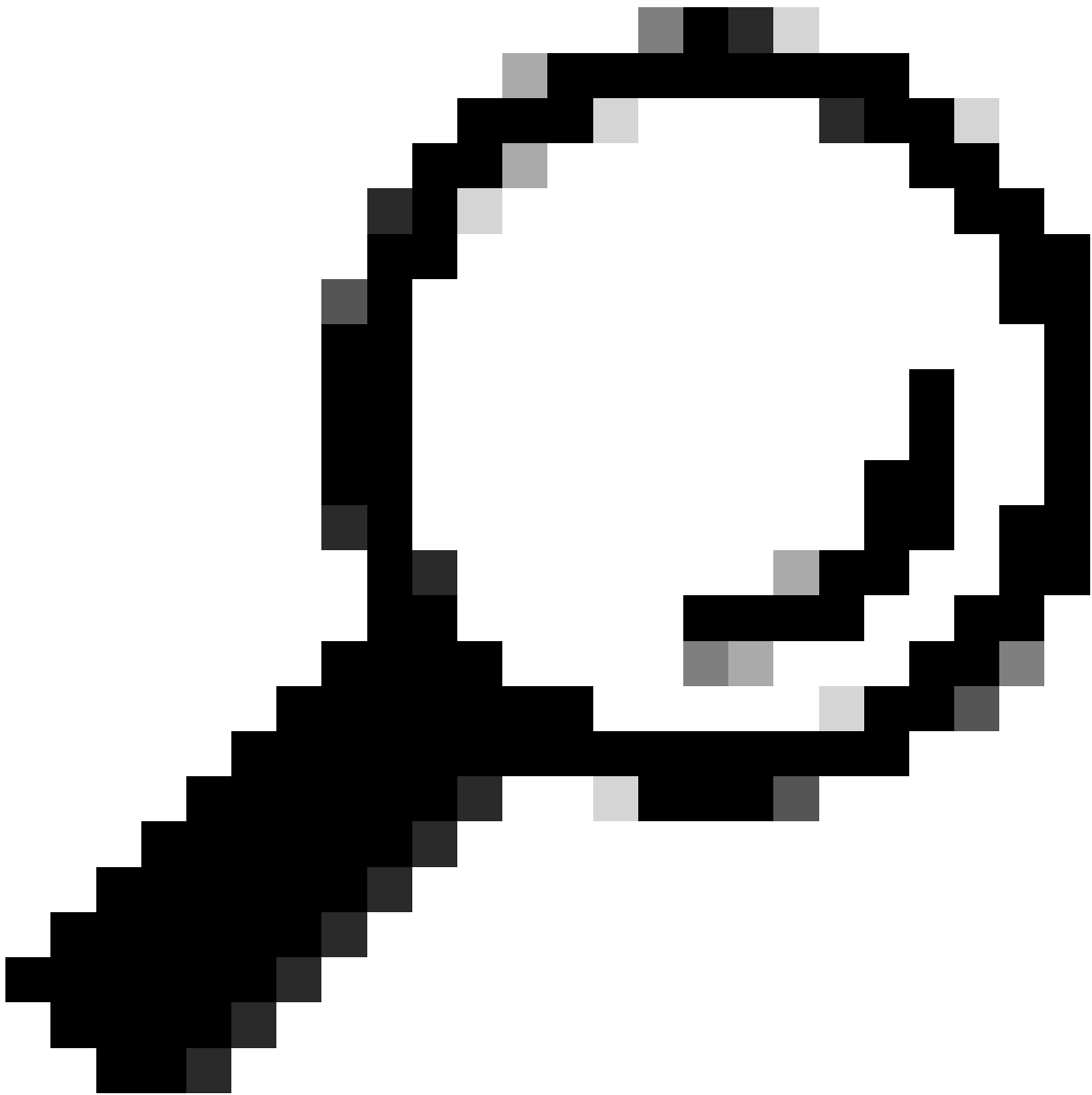
---

**Out Of Band (OOB) TrustSec PAC**

Issue Date:

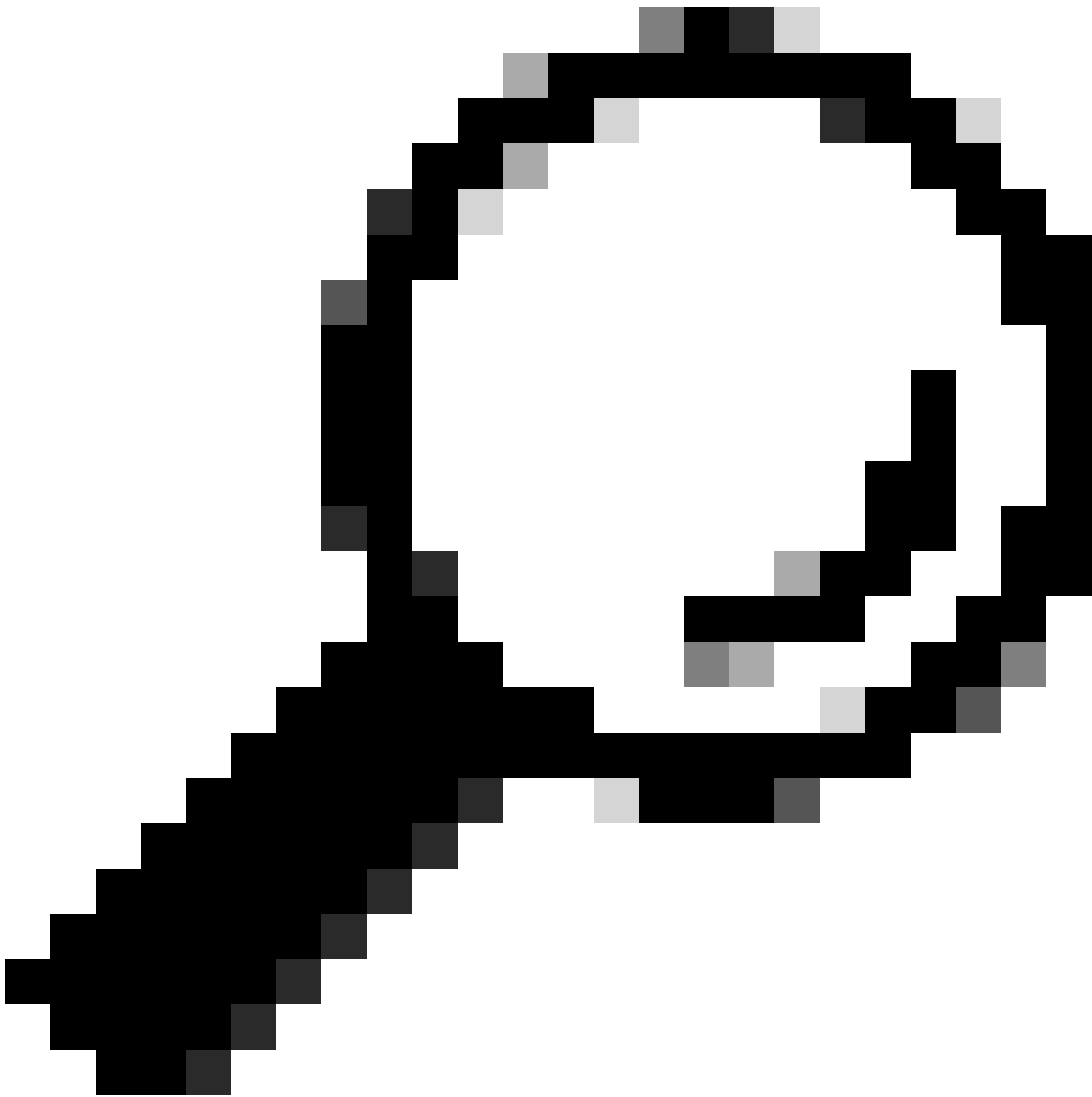
Expiration Date:

Issued By:



**Sugerencia:** Si aún no ha configurado SSH en su switch Catalyst, puede utilizar esta guía: [Cómo Configurar Secure Shell \(SSH\) en el switch Catalyst](#).

---



**Consejo:** Si no desea habilitar Cisco ISE para acceder a su switch Catalyst a través de SSH, puede crear asignaciones de IP a SGT estáticas en el switch Catalyst con la CLI en su lugar (se muestra en un paso aquí).

---

Verifique la configuración predeterminada de TrustSec para asegurarse de que es aceptable (opcional)





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  minutes (10-60) ⓘ

**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

Creación de etiquetas de grupos de seguridad para usuarios inalámbricos

Crear un grupo de seguridad para consultores BYOD: SGT 15

Crear un grupo de seguridad para empleados BYOD: 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	

Crear asignación de IP a SGT estática para el servidor web restringido

Realice esta acción para cualquier otra dirección IP o subred de la red que no se autentique en Cisco ISE con omisión de autenticación MAC (MAB), 802.1x, perfiles, etc.

**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

Crear perfil de autenticación de certificado

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

Crear secuencia de origen de identidad con el perfil de autenticación de certificado anterior

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>&gt;</p> <p>&lt;</p> <p>&gt;&gt;</p> <p>&lt;&lt;</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>
---	---	--

▼ 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

Asignar a los usuarios inalámbricos (empleados y consultores) una SGT adecuada

Nombre	Nombre de usuario	Grupo AD	SG	SGT
Jason Smith	jsmith	Consultores	Consultores BYOD	15
Sally Smith	hormiguero	Empleados	Empleados BYOD	7
n/a	n/a	n/a	Dispositivos_TrustSec	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	DetIX	Wireless_802.1X	BYOD_Identity_Sequence	230	Options
On	Default		All_Users_ID_Stores	0	Options

► Authorization Policy - Local Exceptions  
► Authorization Policy - Global Exceptions

▼ 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	Select from list	109	Options

Asignar SGT a los dispositivos reales (switch y WLC)

Identity Services Engine

Home → Context Visibility → Operations → Policy → Administration → Work Centers

Network Access → Guest Access → TrustSec → BYOD → Profiler → Posture → Device Administration → PassivID

Overview → Components → TrustSec Policy → Policy Sets → SXP → Troubleshoot → Reports → Settings

### 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

Definición de SGACL para Especificar la Política de Salida

Permitir que los consultores accedan desde cualquier lugar externo, pero restringir interno:

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

```

Permitir a los empleados acceder desde cualquier lugar externo y desde cualquier lugar interno:

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

```

Permitir el acceso de otros dispositivos a servicios básicos (opcional):

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

```

Redirigir a todos los usuarios finales a Cisco ISE (para la redirección del portal BYOD). No incluya el tráfico DNS, DHCP, ping o WebAuth, ya que no pueden dirigirse a Cisco ISE:

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

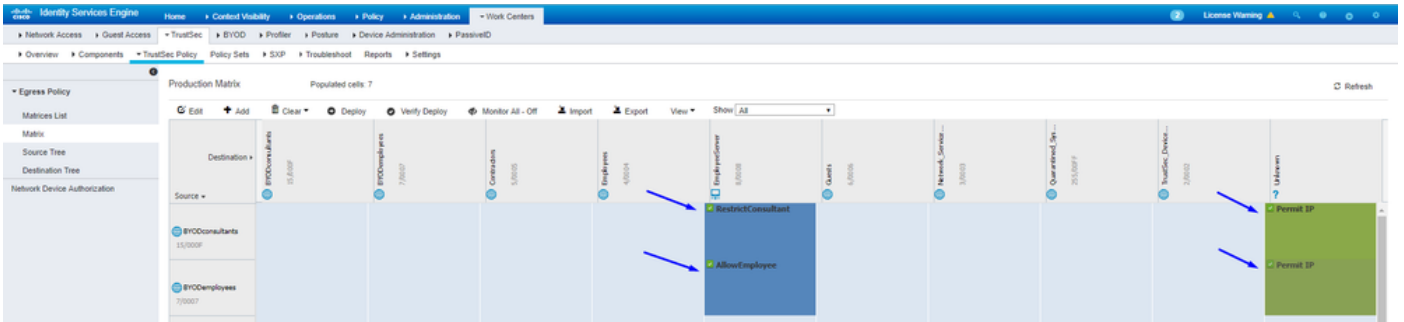
```

Aplique sus ACL en la matriz de políticas de TrustSec en Cisco ISE

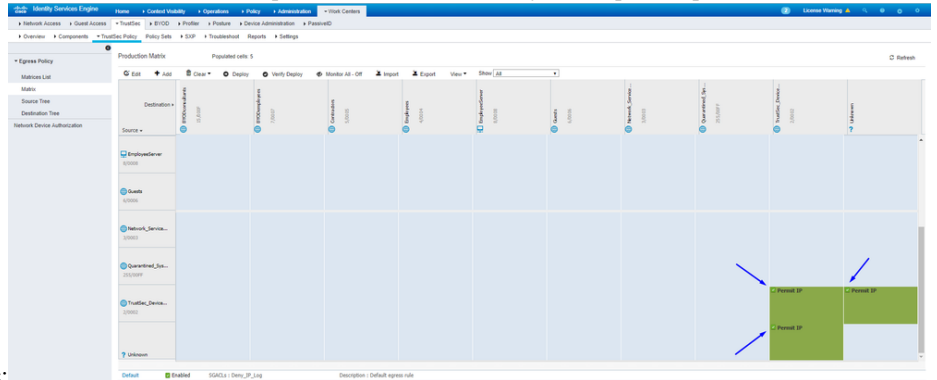
Permitir que los consultores accedan desde cualquier lugar externo, pero restringir los servidores web internos, como <https://10.201.214.132>



Permitir que los empleados accedan desde cualquier lugar externo y permitir servidores web internos:

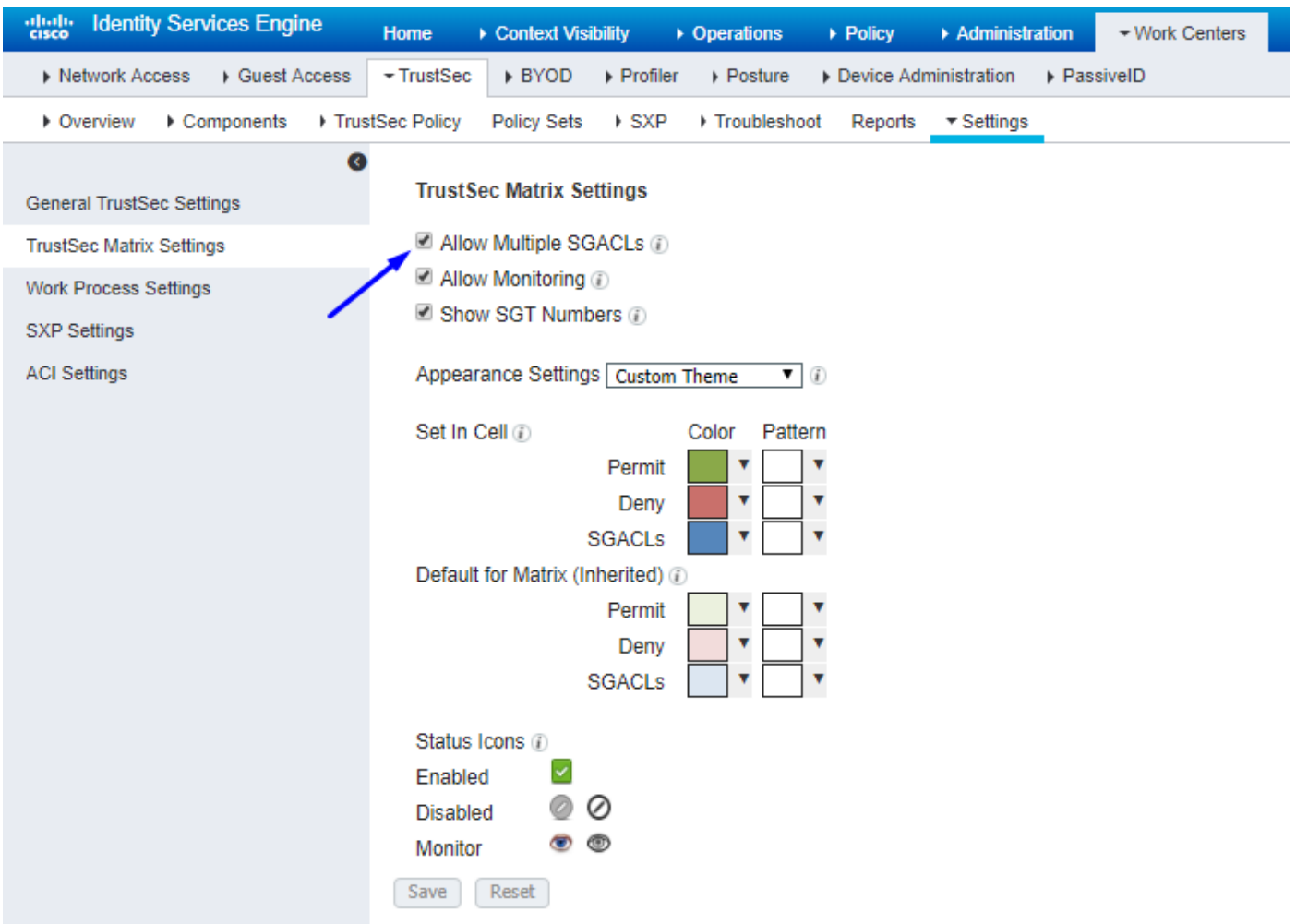


Permitir el tráfico de gestión (SSH, HTTPS y CAPWAP) hacia/desde los dispositivos de la red (switch y WLC) para no perder el acceso SSH o



HTTPS una vez que implemente Cisco TrustSec:

Habilite Cisco ISE para Allow Multiple SGACLs:



Haga clic Push en la esquina superior derecha de Cisco ISE para trasladar la configuración a los dispositivos. También debe volver a hacer esto más tarde:

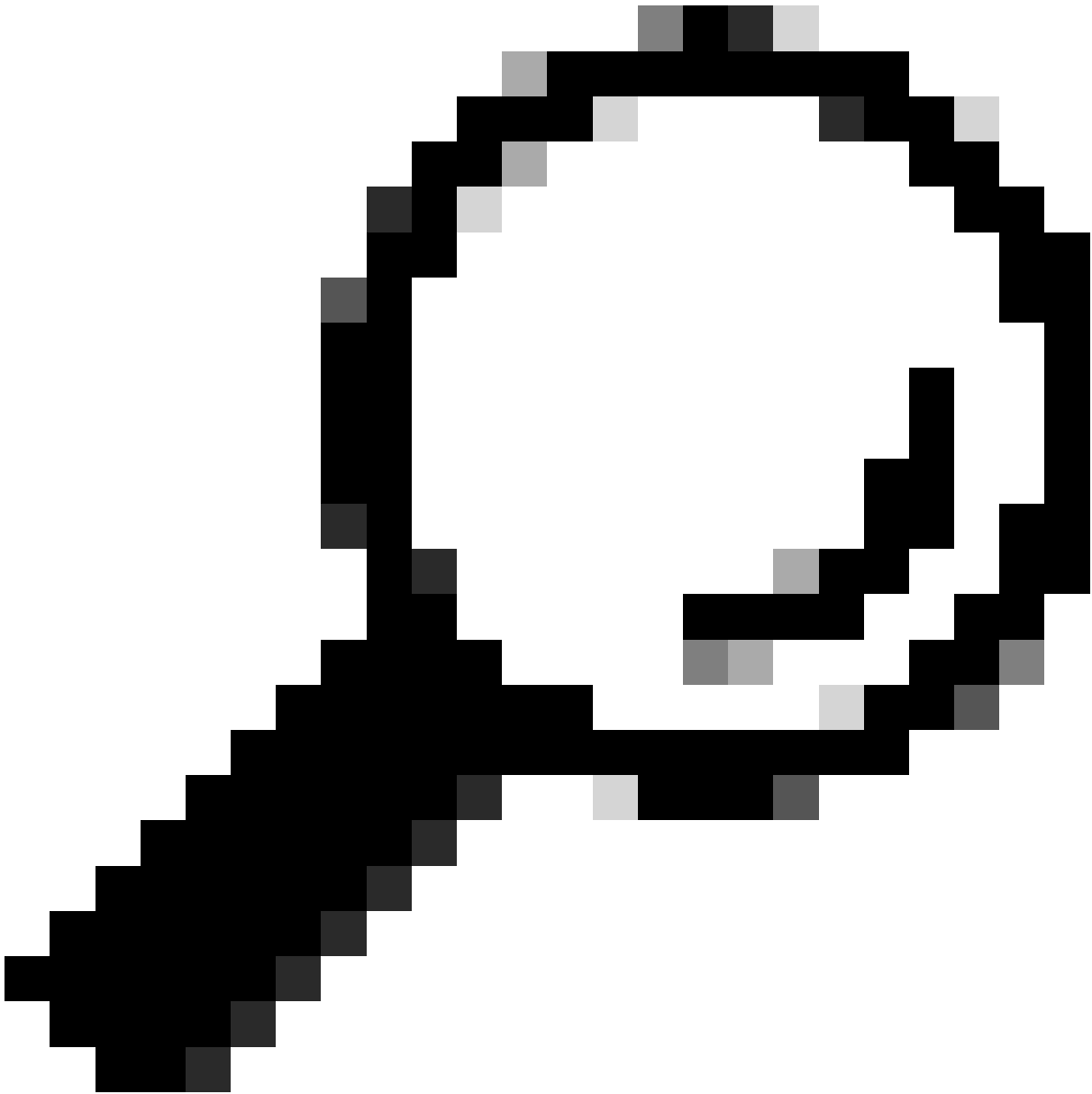
1

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

Configuración de TrustSec en el switch Catalyst

Configuración del switch para utilizar Cisco TrustSec para AAA en el switch Catalyst



**Sugerencia:** en este documento se da por hecho que los usuarios inalámbricos ya han adoptado BYOD con Cisco ISE antes de la configuración que se muestra aquí.

---

Los comandos que se muestran en negrita ya estaban configurados antes de esto (para que BYOD Wireless funcione con ISE).

**<#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
```



**Nota:** La clave PAC debe ser la misma que la clave secreta compartida RADIUS especificada en la **Administration > Network Devices > Add Device > RADIUS Authentication Settings** sección.

---

<#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
```

Configuración de la clave PAC en el servidor RADIUS para autenticar el switch en 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  ⓘ



**Nota:** La clave PAC debe ser la misma que la clave secreta compartida RADIUS especificada en la **Administration > Network Devices > Add Device > RADIUS Authentication Settings** sección de Cisco ISE (como se muestra en la captura de pantalla).

---

Configuración de credenciales CTS para autenticar el switch en 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

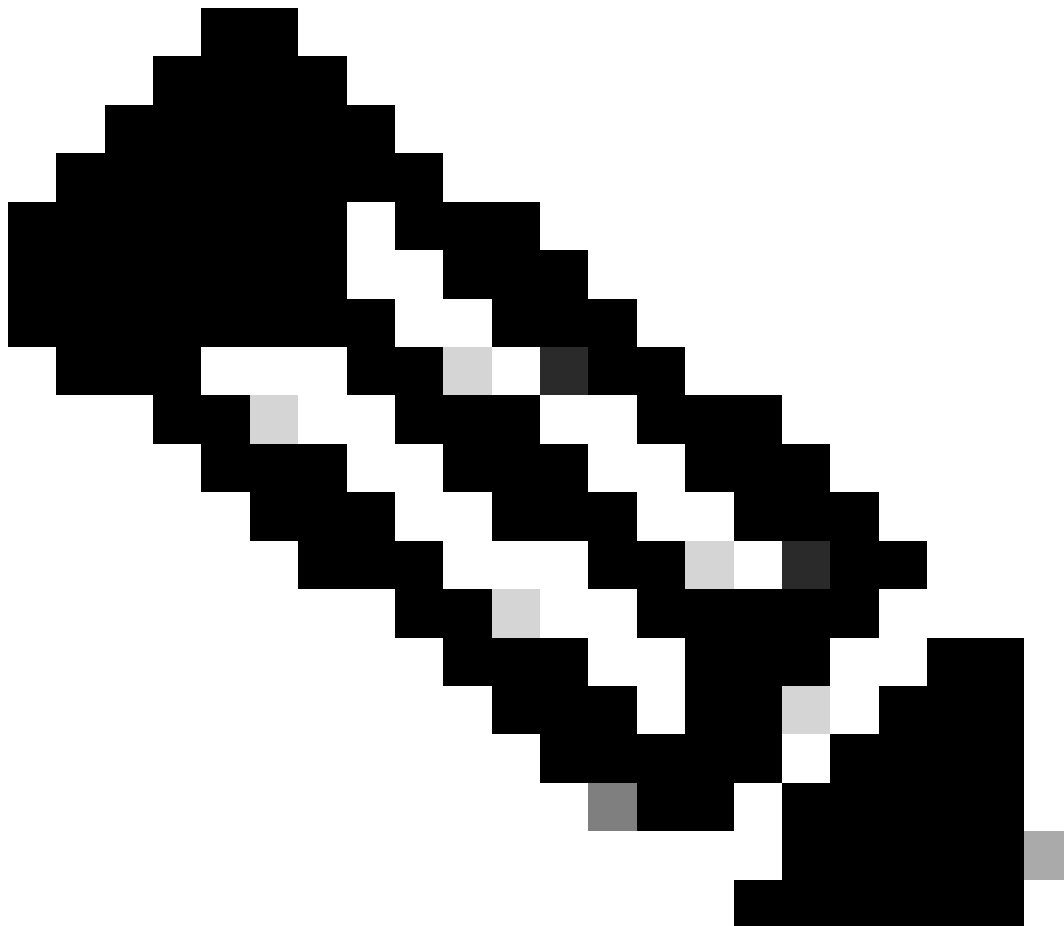
Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id CatalystSwitch

\* Password Admin123 Hide



**Nota:** las credenciales de CTS deben ser las mismas que las de Device ID + password especificadas en Las credenciales de CTS deben ser las mismas que las de Device ID + password especificadas en la Administration > Network Devices > Add Device >



---

Advanced TrustSec Settings sección de Cisco ISE (mostrada en la captura de pantalla).

---

A continuación, actualice su PAC para que vuelva a ponerse en contacto con Cisco ISE:

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

Habilitación global de CTS en switch Catalyst

```
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)
```

Creación de una asignación estática de IP a SGT para los servidores web restringidos (opcional)

Ese servidor web restringido no se suministra a través de ISE para la autenticación en cualquier momento, por lo que debe etiquetarlo manualmente con la CLI del switch o la GUI web de ISE, que es solo uno de los muchos servidores web de Cisco.

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

Verifique TrustSec en el switch Catalyst

```
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
```

## Configuración de TrustSec en WLC

Configure y verifique que el WLC se agrega como un dispositivo RADIUS en Cisco ISE

The screenshot displays the Cisco ISE Administration GUI for configuring a Network Device. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices.

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

- 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
  - IPSEC:** No
  - Device Type:** All Device Types

The "RADIUS Authentication Settings" section is expanded, showing the following configurations:

- RADIUS UDP Settings:**
  - Protocol:** RADIUS
  - Shared Secret:** cisco
  - Use Second Shared Secret:** No
  - CoA Port:** 1700
- RADIUS DTLS Settings:**
  - DTLS Required:** No
  - Shared Secret:** radius/dtls
  - CoA Port:** 2083
  - Issuer CA of ISE Certificates for CoA:** Select if required (optional)
  - DNS Name:** (empty)

Configure y verifique que el WLC se agrega como un dispositivo TrustSec en Cisco ISE

Este paso permite que Cisco ISE implemente las asignaciones estáticas de IP a SGT en el WLC. Estas asignaciones se crearon en la GUI web de Cisco ISE en **Centros de trabajo > TrustSec > Componentes > Asignaciones estáticas de SGT de IP** en un paso anterior.

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



**Nota:** Utilizamos esto Device Id y Password en un paso posterior, en Security > TrustSec > Generalen la interfaz de usuario web del WLC.

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
<a href="#">Realm List</a>	
PAC Provisioning	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable



Activar TrustSec en WLC

### 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





**Nota:** CTS Device Id y Password debe ser el mismo que el Device Id y Password que especificó en la Administration > Network Devices > Add Device > Advanced TrustSec Settings sección en Cisco ISE.

---

Verifique que PAC se haya aprovisionado en el WLC

Verá que el WLC tiene la PAC aprovisionada correctamente después de hacer clic en Refresh Env Data (haga esto en este paso):



**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

PAC A-ID: ef2e1222e67eb4630a8b22d1ff0216c1

PAC Lifetime: Wed Nov 21 00:01:07 2018

IPSec:  Enable

Descargue los datos del entorno CTS de Cisco ISE al WLC

Después de hacer clic Refresh Env Data, su WLC descarga sus SGT.

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

Habilitar las descargas SGACL y su aplicación en el tráfico

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

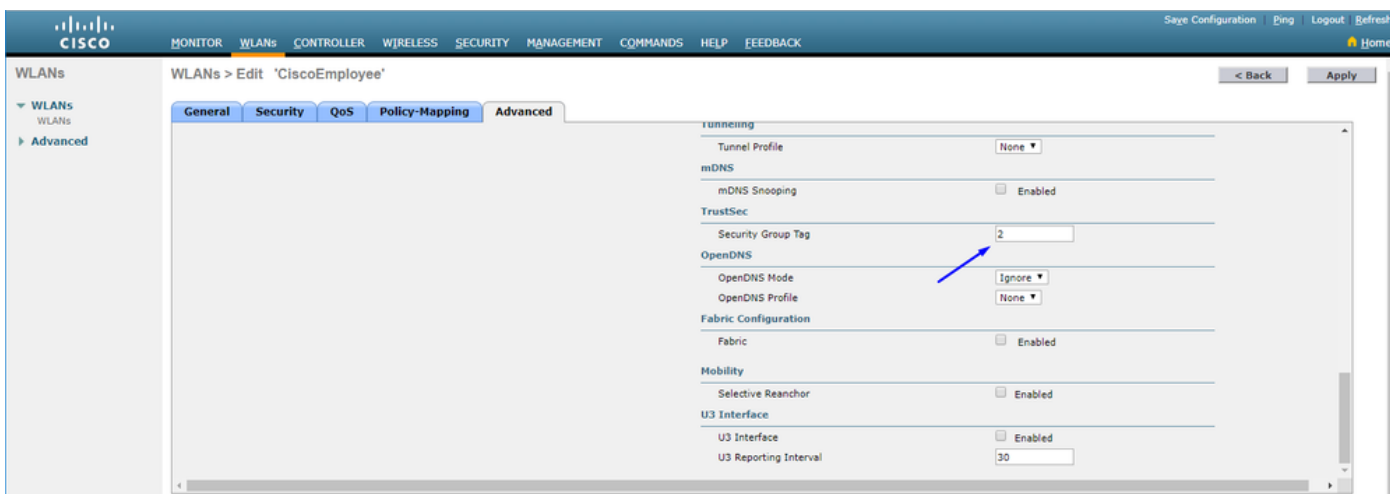
CTS Override Enabled

Sgacl Enforcement

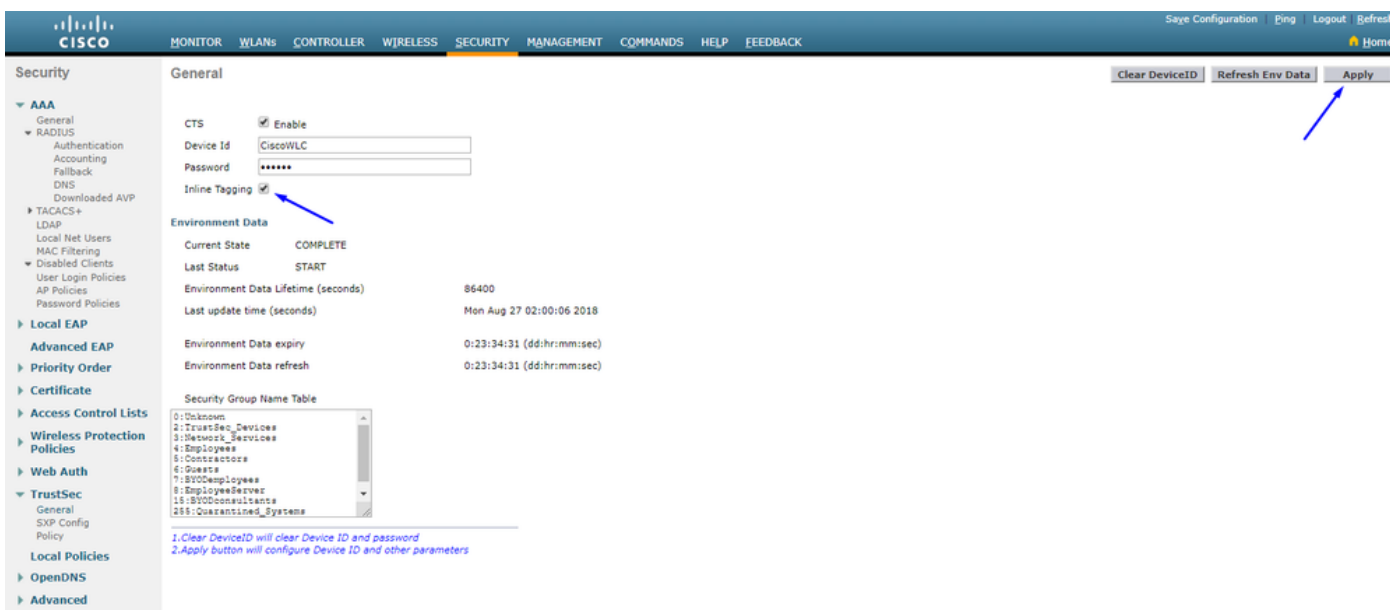
1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)  
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

Asignar WLC y punto de acceso al SGT de 2 (TrustSec\_Devices)

Dé al WLC+WLAN un SGT de 2 (TrustSec\_Devices) para permitir el tráfico (SSH, HTTPS, y CAPWAP) hacia/desde el WLC + AP a través del switch.



Activar etiquetado en línea en WLC



En **Wireless > Access Points > Global Configuration** desplácese hacia abajo y seleccione **TrustSec Config**.

The screenshot shows the Cisco Wireless Management interface. The left sidebar contains a navigation menu with categories like 'Access Points', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', 'Network Lists', and various radio standards. The main content area is titled 'All APs TrustSec Configuration'. Under the 'TrustSec' section, several settings are visible: 'Sgac Enforcement' (checked), 'Inline Taging' (checked and highlighted with a blue box), 'AP SXP State' (set to 'Disabled'), 'Default Password' (masked with dots), and several SXP-related time settings (Listener Min/Max Hold Time, Speaker Hold Time, Reconciliation Time Period, and Retry Period). Below this is the 'Peer Config' section with fields for 'Peer IP Address', 'Password' (set to 'Default'), and 'Local Mode' (set to 'Speaker'), along with an 'ADD' button. At the bottom, there are two informational notes about inline tagging and SXPv4 support.

Activar etiquetado en línea en switch Catalyst

```
<#root>
```

```
CatalystSwitch(config)#interface TenGigabitEthernet1/0/48
```

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

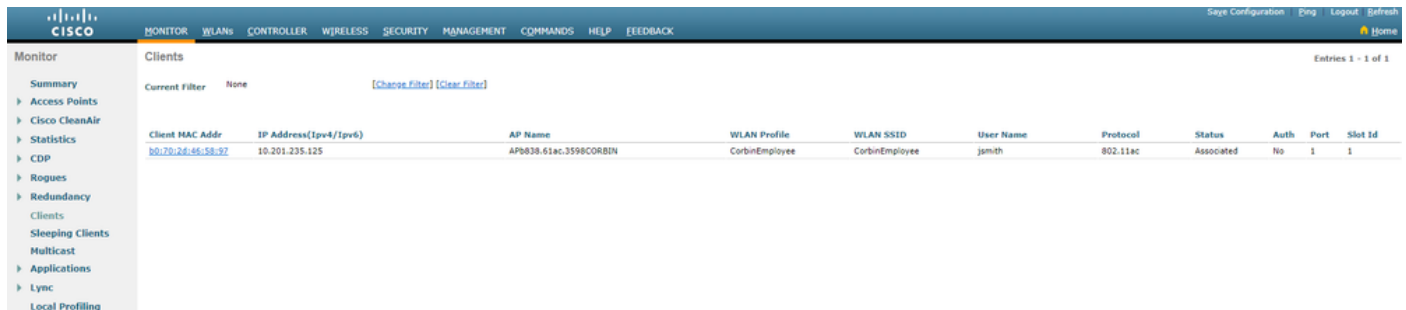
```
CatalystSwitch(config-if)#switchport trunk native vlan 15
```

```
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
```

## Verificación



The screenshot shows the Cisco Catalyst Switch Monitor interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The main content area is titled 'Clients' and shows a table with one entry. The table columns are Client MAC Addr, IP Address(Ipv4/Ipv6), AP Name, WLAN Profile, WLAN SSID, User Name, Protocol, Status, Auth, Port, and Slot Id. The entry shows a client with MAC address b0:70:26:46:58:97, IP address 10.201.235.125, AP name AP0838.61ac.3598CORBIN, WLAN Profile CorbinEmployee, WLAN SSID CorbinEmployee, User Name jsmith, Protocol 802.11ac, Status Associated, Auth No, Port 1, and Slot Id 1.

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

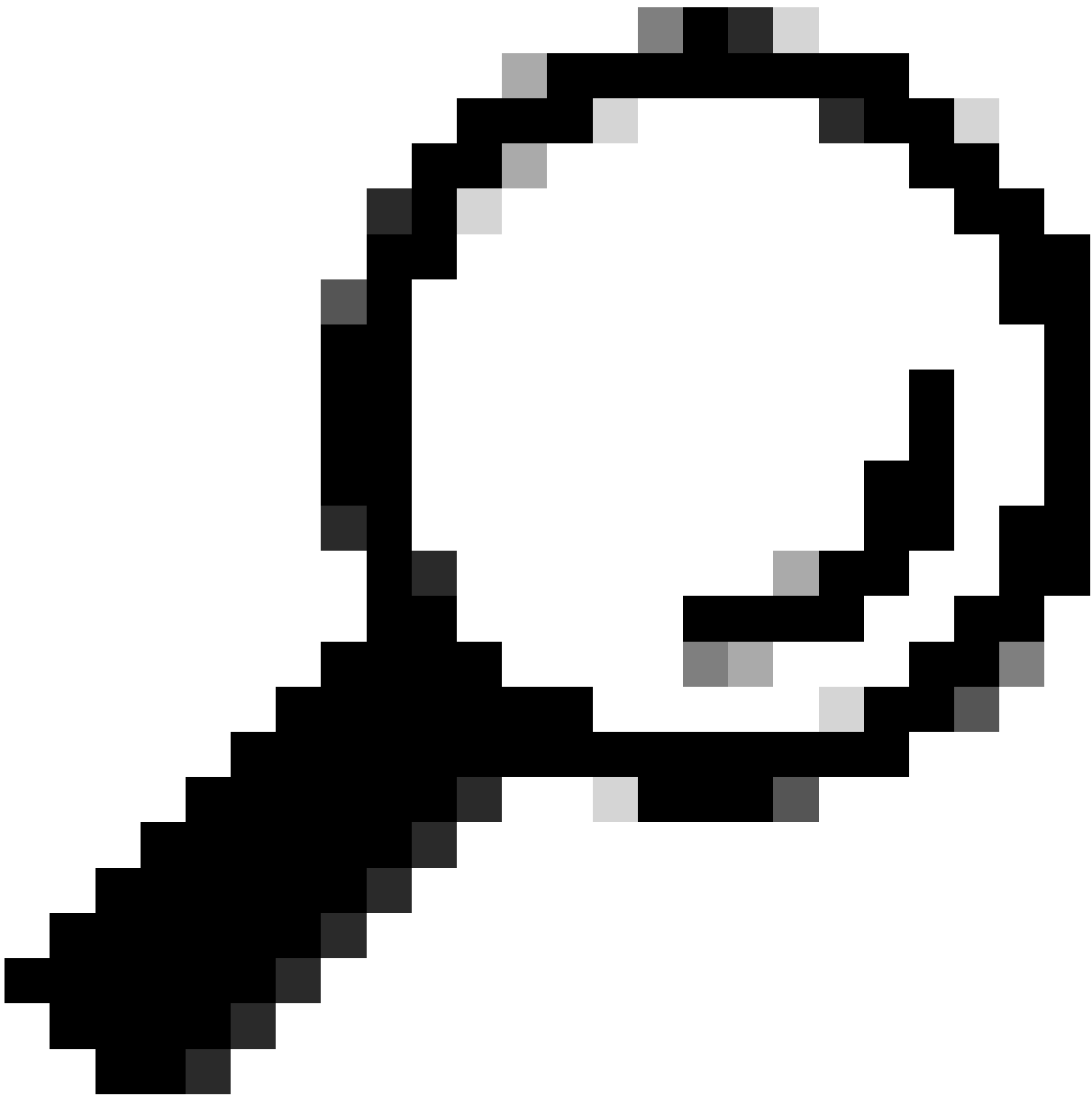
```
CatalystSwitch#show platform acl counters hardware | inc SGACL
```

Descarte de SGACL IPv4 de salida (454): 10 tramas

Eliminación de SGACL IPv6 de salida (455): 0 tramas

Abandono de celda SGACL IPv4 de salida (456): 0 tramas

Abandono de celda SGACL IPv6 de salida (457): 0 tramas



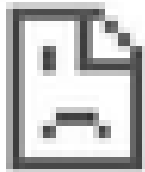
**Sugerencia:** si utiliza un Cisco ASR, Nexus o Cisco ASA en su lugar, el documento que aparece aquí puede ayudarle a verificar que se aplican las etiquetas SGT: [Guía de resolución de problemas de TrustSec](#).

---

Authenticate to wireless with username jsmith password Admin123 - se encuentra con la ACL deny en el 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





## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).