

Configuration de TrustSec (SGT) avec ISE (étiquetage en ligne)

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Objectif](#)

[Configurations](#)

[Configurer TrustSec sur ISE](#)

[Configurer Cisco ISE en tant que serveur AAA TrustSec](#)

[Configuration et vérification de l'ajout du commutateur en tant que périphérique RADIUS dans Cisco ISE](#)

[Configurer et vérifier que le WLC est ajouté en tant que périphérique TrustSec dans Cisco ISE](#)

[Vérifiez les paramètres TrustSec par défaut pour vous assurer qu'ils sont acceptables \(facultatif\)](#)

[Créer des balises de groupe de sécurité pour les utilisateurs sans fil](#)

[Créer un mappage statique IP-vers-SGT pour le serveur Web restreint](#)

[Créer un profil d'authentification de certificat](#)

[Créer une séquence source d'identité avec le profil d'authentification de certificat d'avant](#)

[Affecter un SGT approprié aux utilisateurs sans fil \(employés et consultants\)](#)

[Attribuer des balises SGT aux périphériques réels \(commutateur et WLC\)](#)

[Définition des SGACL pour spécifier la stratégie de sortie](#)

[Appliquer vos listes de contrôle d'accès sur la matrice de stratégie TrustSec dans Cisco ISE](#)

[Configurer TrustSec sur un commutateur Catalyst](#)

[Configurer le commutateur pour utiliser Cisco TrustSec pour AAA sur le commutateur Catalyst](#)

[Configurez la clé PAC sous le serveur RADIUS pour authentifier le commutateur auprès de Cisco ISE](#)

[Configuration des informations d'identification CTS pour authentifier le commutateur auprès de Cisco ISE](#)

[Activer CTS globalement sur le commutateur Catalyst](#)

[Effectuer un mappage statique IP vers SGT pour les serveurs Web restreints \(facultatif\)](#)

[Vérification de TrustSec sur le commutateur Catalyst](#)

[Configurer TrustSec sur WLC](#)

[Configuration et vérification de l'ajout du WLC en tant que périphérique RADIUS dans Cisco ISE](#)

[Configurer et vérifier que le WLC est ajouté en tant que périphérique TrustSec dans Cisco ISE](#)

[Activer le provisionnement PAC du WLC](#)

[Activer TrustSec sur WLC](#)

[Vérifiez que le PAC a été configuré sur le WLC](#)

[Télécharger les données d'environnement CTS de Cisco ISE vers WLC](#)

[Activer les téléchargements et l'application SGACL sur le trafic](#)

[Attribuer le SGT de 2 au WLC et au point d'accès \(TrustSec_Devices\)](#)

Introduction

Ce document décrit comment configurer et vérifier TrustSec sur un commutateur Catalyst et un contrôleur de réseau local sans fil avec Identity Services Engine.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base des composants Cisco TrustSec (CTS)
- Connaissances de base de la configuration CLI des commutateurs Catalyst
- Connaissances de base de la configuration GUI des contrôleurs LAN sans fil (WLC) Cisco
- Expérience de la configuration ISE (Identity Services Engine)

Exigences

Cisco ISE doit être déployé sur votre réseau et les utilisateurs finaux doivent s'authentifier auprès de Cisco ISE avec 802.1x (ou une autre méthode) lorsqu'ils se connectent à un réseau sans fil ou filaire. Cisco ISE attribue une balise de groupe de sécurité (SGT) à leur trafic une fois qu'ils se sont authentifiés sur votre réseau sans fil.

Dans notre exemple, les utilisateurs finaux sont redirigés vers le portail Cisco ISE Bring Your Own Device (BYOD) et reçoivent un certificat leur permettant d'accéder en toute sécurité au réseau sans fil avec le protocole EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) une fois qu'ils ont terminé les étapes du portail BYOD.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine, version 2.4
- Commutateur Cisco Catalyst 3850, version 3.7.5E
- Cisco WLC, version 8.5.120.0
- Point d'accès sans fil Cisco Aironet en mode local

Avant le déploiement de Cisco TrustSec, vérifiez que votre commutateur Cisco Catalyst et/ou les modèles Cisco WLC+AP + version logicielle prennent en charge les éléments suivants :

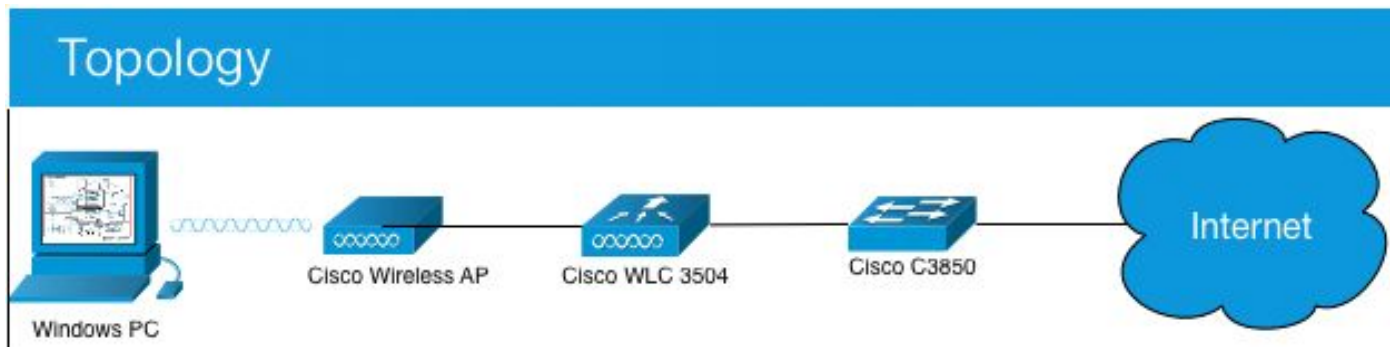
- Balises TrustSec/Groupe de sécurité
- Balisage en ligne (sinon, vous pouvez utiliser SXP au lieu du Balisage en ligne)
- Mappages IP-vers-SGT statiques (si nécessaire)
- Mappages statiques de sous-réseau vers SGT (si nécessaire)

- Mappings VLAN-SGT statiques (si nécessaire)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Dans cet exemple, le WLC marque les paquets comme SGT 15 s'ils proviennent d'un consultant et + SGT 7 s'ils proviennent d'un employé.

Le commutateur refuse ces paquets s'ils sont de SGT 15 à SGT 8 (les consultants ne peuvent pas accéder aux serveurs étiquetés SGT 8).

Le commutateur autorise ces paquets s'ils sont de SGT 7 à SGT 8 (les employés peuvent accéder aux serveurs étiquetés SGT 8).

Objectif

Permettre à quiconque d'accéder à GuestSSID.

Autoriser les consultants à accéder au SSID Employé, mais avec un accès restreint.

Autoriser les employés à accéder à EmployeeSSID avec un accès complet.

Périphérique	Adresse IP	VLAN
ISE	10.201.214.230	463
Catalyst Switch	10.201.235.102	1115
WLC	10.201.214.229	463
Point d'accès	10.201.214.138	455

Nom	Nom d'utilisateur	Groupe AD	SG	SGT
Jason Smith	maréchal-ferrant	Consultants	consultants pour le BYOD	15
Sally Smith	maréchal-ferrant	Employés	Employés BYOD	7
S/O	S/O	S/O	Périphériques_TrustSec	2

Configurations

Configurer TrustSec sur 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>

Configurer Cisco ISE en tant que serveur AAA 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 > Policy Sets > SXP > Troubleshoot > Reports > Settings. The left sidebar shows a tree view with 'Trustsec AAA Servers' selected. The main content area is titled 'AAA Servers List > corbinise' and 'AAA Servers'. It contains a form with the following fields: '* Name' (text input: CISCOISE), 'Description' (text area), '* IP' (text input: 10.201.214.230, with an example '(Example: 10.1.1.1)'), and '* Port' (text input: 1812, with a valid range '(Valid Range 1 to 65535)'). At the bottom of the form are 'Save' and 'Reset' buttons.

Configuration et vérification de l'ajout du commutateur en tant que périphérique RADIUS dans Cisco ISE

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

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

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > CatalystSwitch

Network Devices

* Name CatalystSwitch

Description Catalyst 3850 Switch

IP Address * IP: 10.201.235.102 / 32

* Device Profile Cisco

Model Name

Software Version

* 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 Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls

Configurer et vérifier que le WLC est ajouté en tant que périphérique TrustSec dans Cisco ISE

Entrez vos informations de connexion pour SSH. Cela permet à Cisco ISE de déployer les mappages statiques IP vers SGT sur le commutateur.

Vous pouvez les créer dans l'interface utilisateur graphique Web de Cisco ISE sous Work Centers > TrustSec > Composants > IP SGT Static Mappings, comme indiqué ci-dessous :

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:

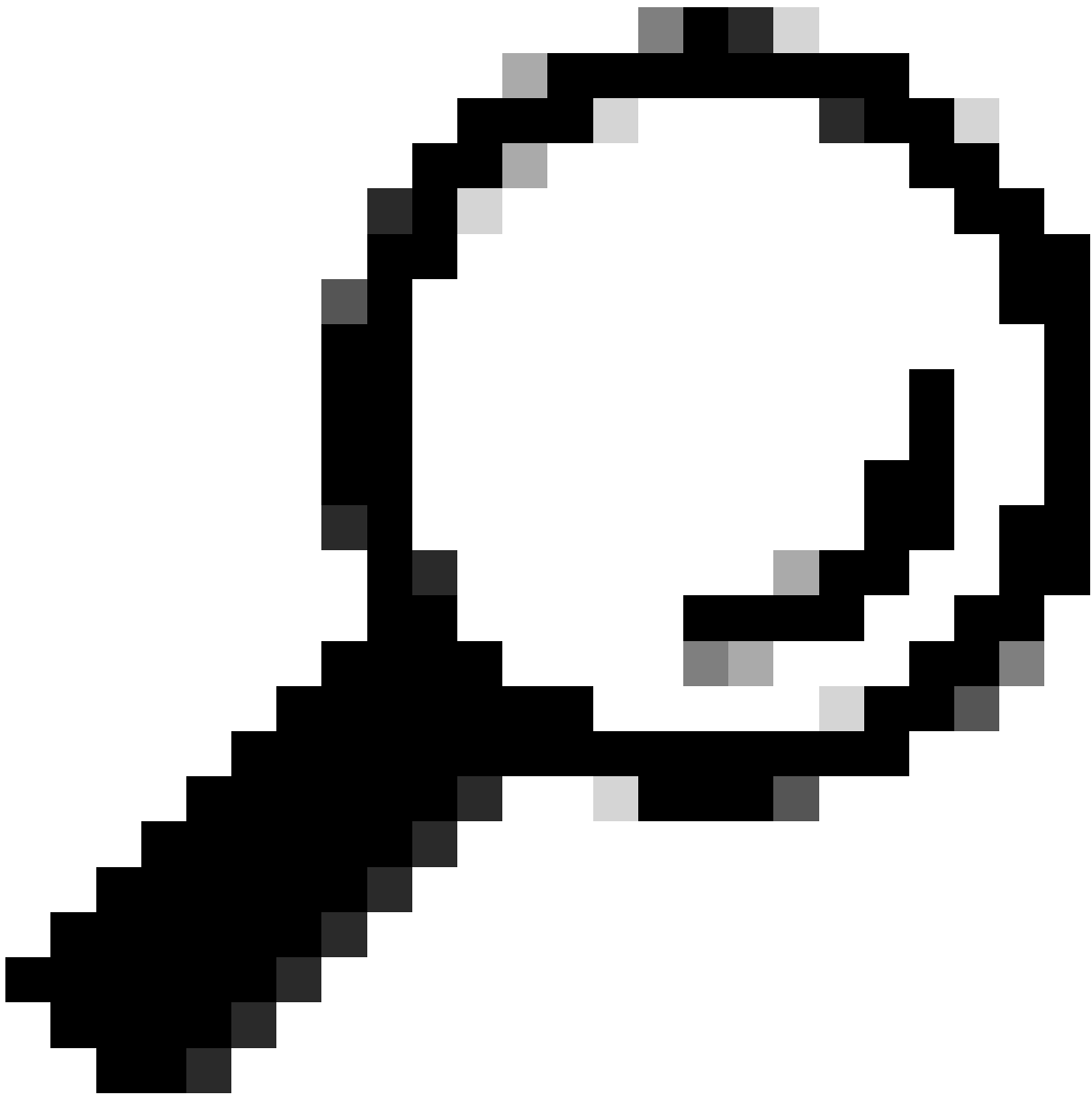
Enable Mode Password:

Out Of Band (OOB) TrustSec PAC

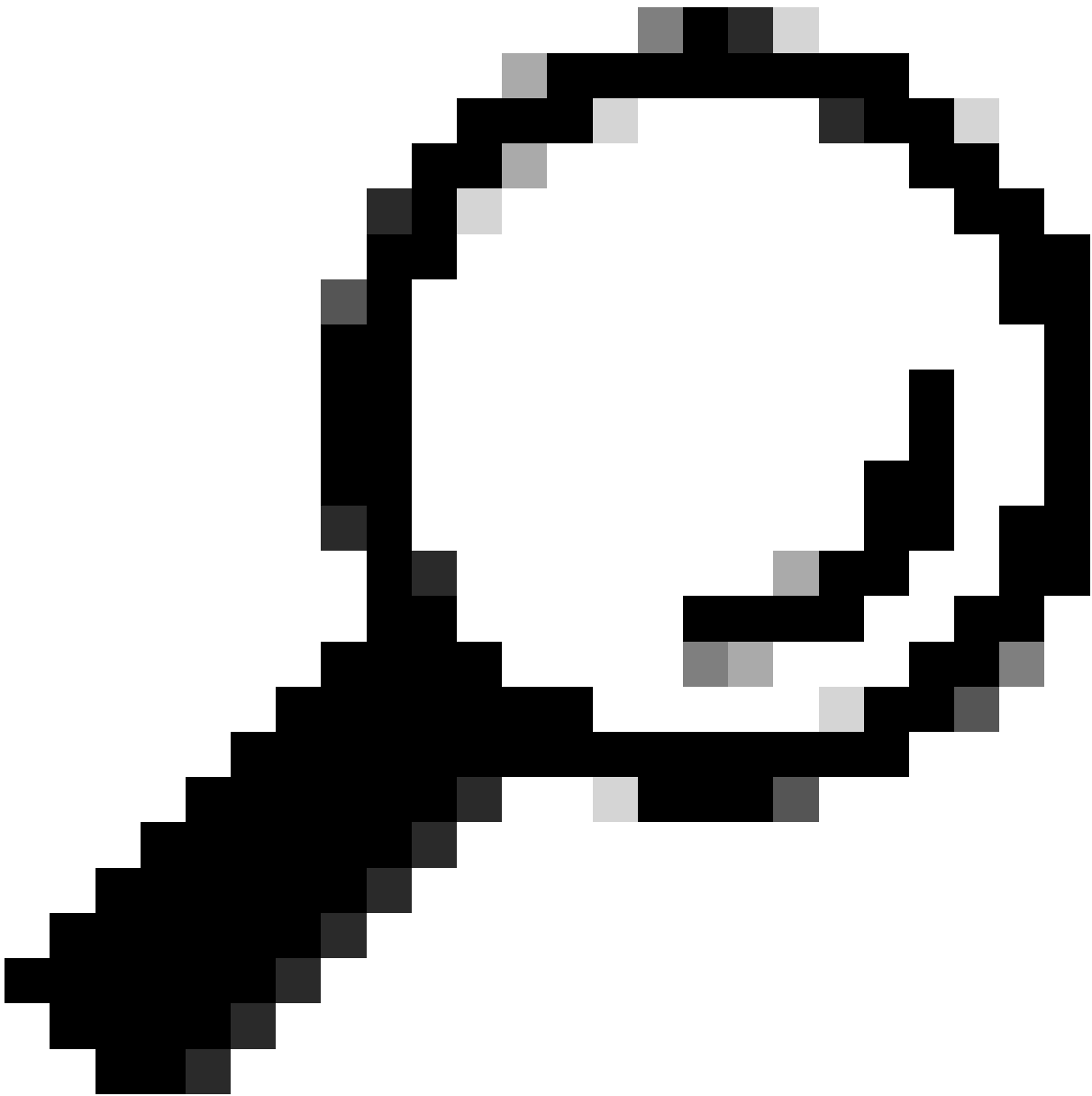
Issue Date:

Expiration Date:

Issued By:



Conseil : Si vous n'avez pas encore configuré SSH sur votre commutateur Catalyst, vous pouvez utiliser ce guide : [Comment configurer Secure Shell \(SSH\) sur le commutateur Catalyst.](#)



Conseil : si vous ne souhaitez pas autoriser Cisco ISE à accéder à votre commutateur Catalyst via SSH, vous pouvez créer des mappages IP-vers-SGT statiques sur le commutateur Catalyst à l'aide de l'interface de ligne de commande (CLI) (voir l'étape ci-dessous).

Vérifiez les paramètres TrustSec par défaut pour vous assurer qu'ils sont acceptables (facultatif)



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

Créer des balises de groupe de sécurité pour les utilisateurs sans fil

Créer un groupe de sécurité pour les consultants BYOD - SGT 15

Créer un groupe de sécurité pour les employés 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	

Créer un mappage statique IP-vers-SGT pour le serveur Web restreint

Effectuez cette opération pour toutes les autres adresses IP ou sous-réseaux de votre réseau qui ne s'authentifient pas auprès de Cisco ISE avec MAC Authentication Bypass (MAB), 802.1x, Profiles, 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

Créer un profil d'authentification de certificat

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

Créer une séquence source d'identité avec le profil d'authentification de certificat d'avant

[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

Available		Selected
Internal Endpoints	<input type="button" value=">"/> <input type="button" value="<"/> <input type="button" value=">>"/> <input type="button" value="<<"/>	Windows_AD_Server
Guest Users		Internal Users
		<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

Affecter un SGT approprié aux utilisateurs sans fil (employés et consultants)

Nom	Nom d'utilisateur	Groupe AD	SG	SGT
Jason Smith	maréchal-ferrant	Consultants	consultants pour le BYOD	15
Sally Smith	maréchal-ferrant	Employés	Employés BYOD	7
S/O	S/O	S/O	Périphériques_TrustSec	2

The screenshot shows the Cisco ISE Policy Sets configuration for EmployeeSSID. It includes sections for Authentication Policy (2) and Authorization Policy (3). In the Authentication Policy section, the 'DetIX' rule is configured with 'BYOD_Identity_Sequence' as the 'Use' value. In the Authorization Policy section, the rule 'Allow Restricted Access if BYODRegistered and EAP-TLS and AD Group = Consultants' is configured with 'BYODconsultants' as the Security Group. Another rule 'Allow Anywhere if BYODRegistered and EAP-TLS and AD Group = Employees' is configured with 'BYODEmployees' as the Security Group.

Attribuer des balises SGT aux périphériques réels (commutateur et WLC)

The screenshot shows the Cisco ISE Network Device Authorization configuration page. It displays a table of Network Device Authorization rules. The 'Tag_TrustSec_Devices' rule is configured with the condition 'If DEVICE:Device Type equals to All Device Types' and the Security Group 'TrustSec_Devices'. The 'Default Rule' is configured with the condition 'If no rules defined or no match' and the Security Group 'Unknown'.

Définition des SGACL pour spécifier la stratégie de sortie

Autoriser les consultants à accéder à tout emplacement externe, mais restreindre les accès internes :

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

```

Permettre aux employés d'accéder à n'importe quel emplacement externe et 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 > 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

```

Autoriser d'autres périphériques à accéder aux services de base (facultatif) :

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 Generation ID: 1

* Name: LoginServices

Description: This is an ACL for Login services

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

```

Save Reset

Rediriger tous les utilisateurs finaux vers Cisco ISE (pour la redirection du portail BYOD). N'incluez pas le trafic DNS, DHCP, ping ou WebAuth, car ils ne peuvent pas accéder à 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 Generation ID: 0

* Name: ISE

Description: ACL to allow ISE services to occur

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

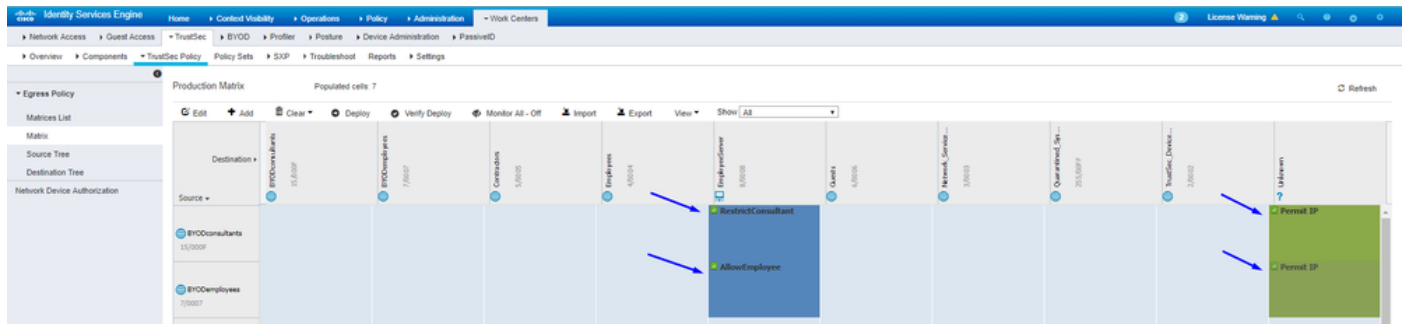
```

Submit Cancel

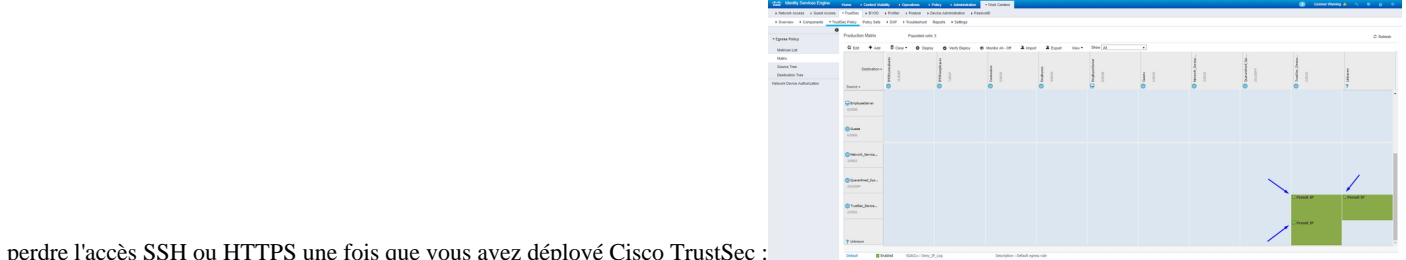
Appliquer vos listes de contrôle d'accès sur la matrice de stratégie TrustSec dans Cisco ISE

Autoriser les consultants à accéder à n'importe quel emplacement externe, mais restreindre les serveurs Web internes, tels que <https://10.201.214.132>

Autoriser les employés à accéder à tout emplacement externe et autoriser les serveurs Web internes :

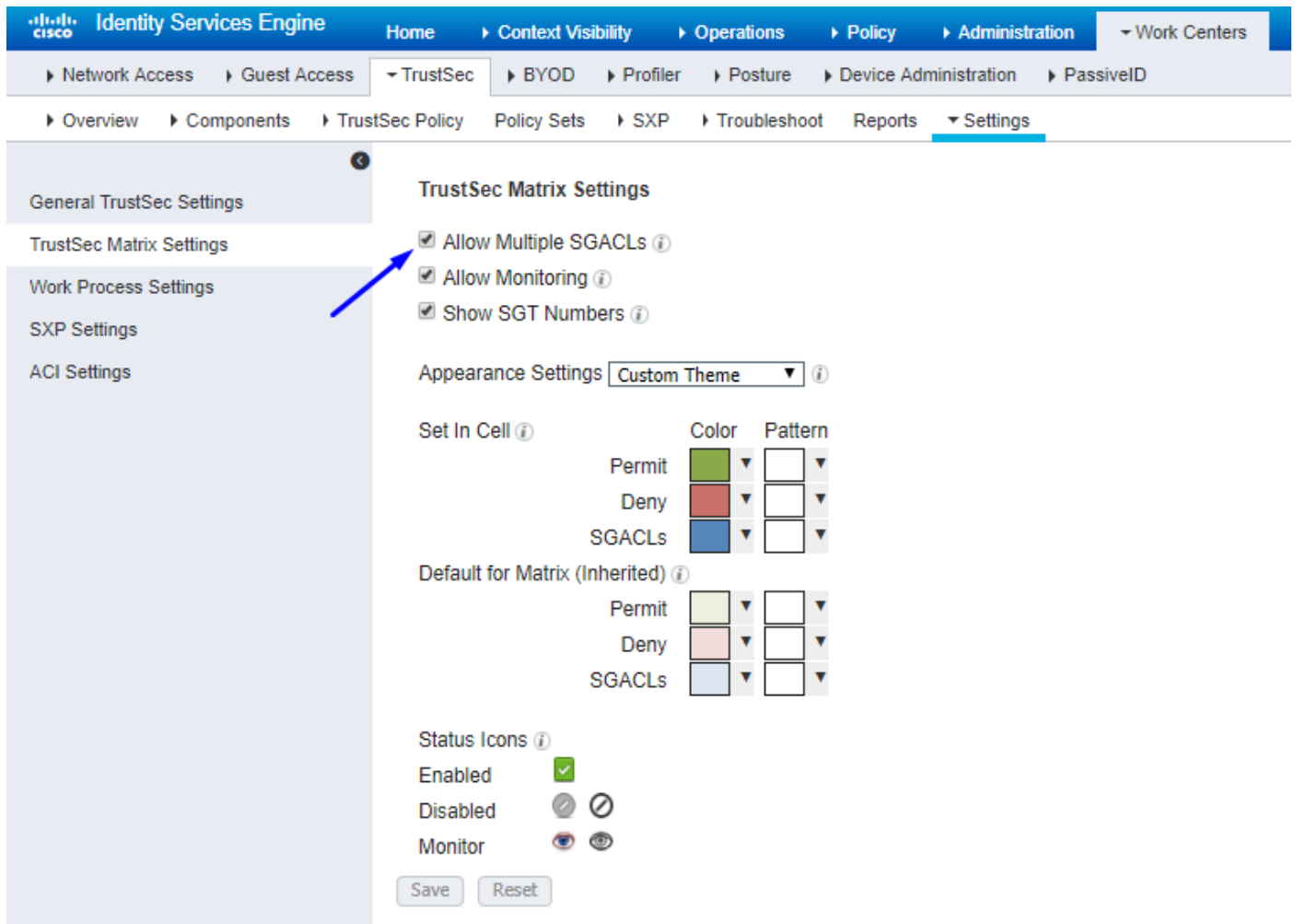


Autorisez le trafic de gestion (SSH, HTTPS et CAPWAP) vers/depuis vos périphériques sur le réseau (commutateur et WLC) afin de ne pas



perdre l'accès SSH ou HTTPS une fois que vous avez déployé Cisco TrustSec :

Permettre à Cisco ISE de Allow Multiple SGACLs:



Cliquez sur Push dans l'angle supérieur droit de Cisco ISE, pour afficher votre configuration sur vos périphériques. Vous devez le faire à nouveau plus tard également :

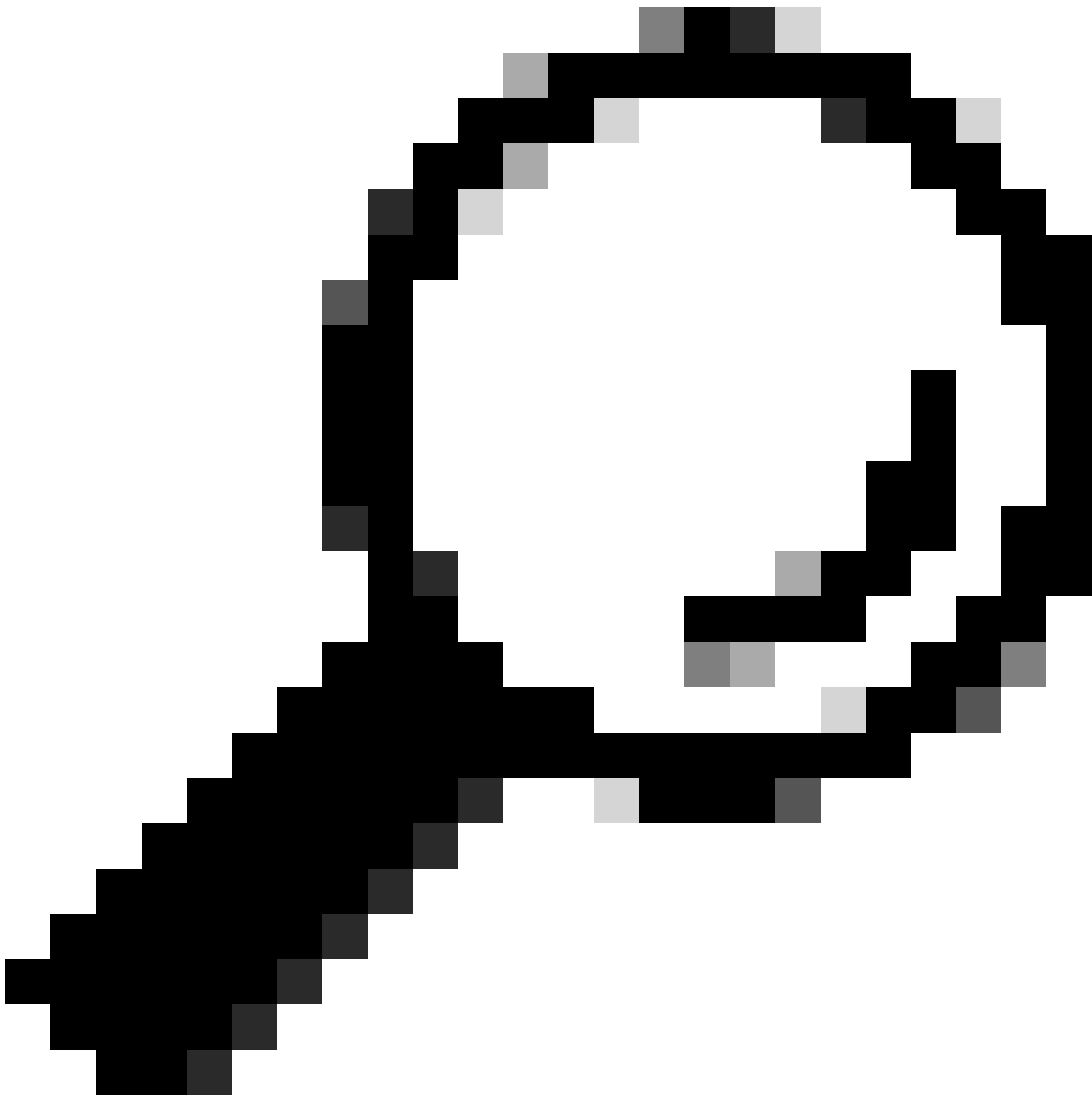
There are TrustSec configuration changes that has not been notified to network devices. To notify the relevant network devices about these changes click the push button.



Push

Configurer TrustSec sur un commutateur Catalyst

Configurer le commutateur pour utiliser Cisco TrustSec pour AAA sur le commutateur Catalyst



Conseil : ce document suppose que vos utilisateurs sans fil ont déjà réussi avec le BYOD par Cisco ISE avant la configuration présentée ici.

Les commandes indiquées en gras ont déjà été configurées avant cela (afin que BYOD Wireless fonctionne avec 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
```



Remarque : la clé PAC doit être identique à la clé secrète partagée RADIUS que vous avez spécifiée dans la **Administration > Network Devices > Add Device > RADIUS Authentication Settings** section.

<#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
```

Configurez la clé PAC sous le serveur RADIUS pour authentifier le commutateur auprès de 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 ⓘ



Remarque : la clé PAC doit être identique à la clé secrète partagée RADIUS que vous avez spécifiée dans la **Administration > Network Devices > Add Device > RADIUS Authentication Settings** section de Cisco ISE (comme indiqué dans la capture d'écran).

Configuration des informations d'identification CTS pour authentifier le commutateur auprès de Cisco ISE

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

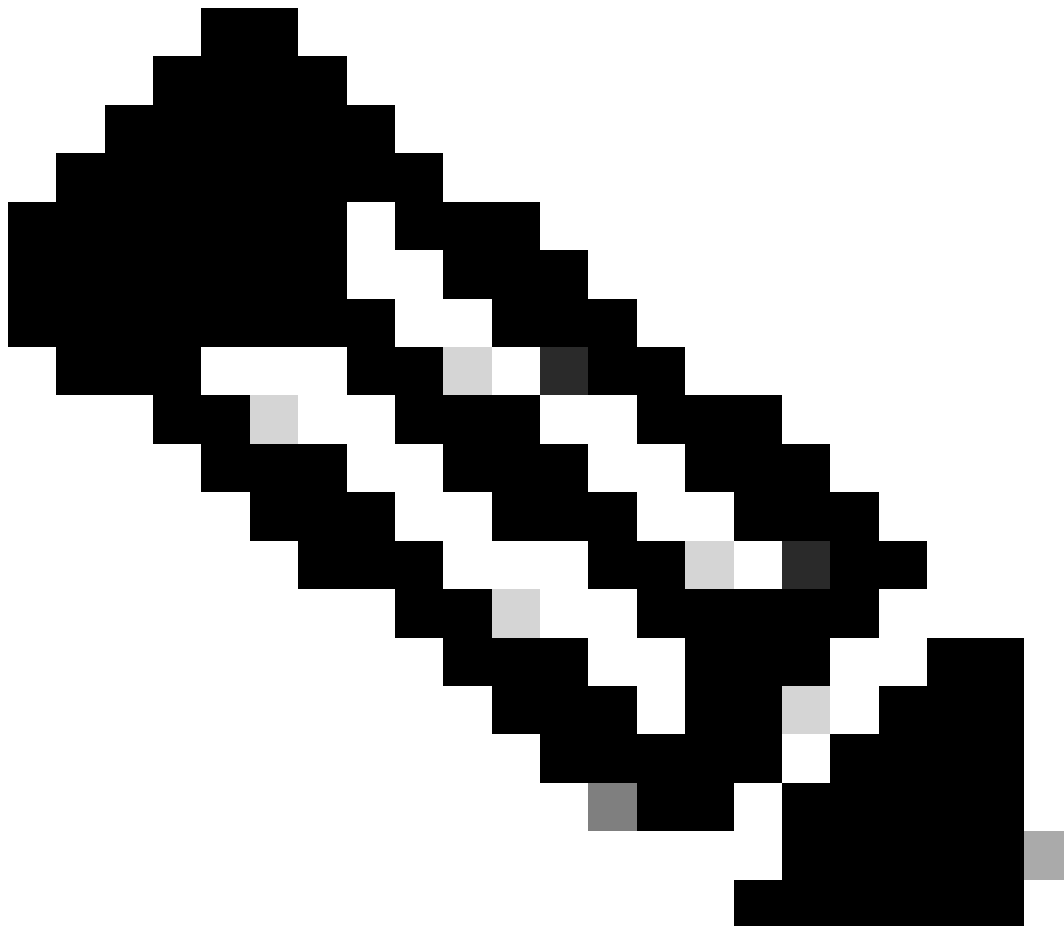
Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id CatalystSwitch

* Password Admin123



Remarque : les informations d'identification CTS doivent être identiques à l'ID de périphérique + mot de passe que vous avez spécifié dans Les informations d'identification CTS doivent être identiques à l'ID de périphérique + mot de passe que vous avez

spécifié dans la section Administration > Network Devices > Add Device > Advanced TrustSec Settings de Cisco ISE (affichée dans la capture d'écran).

Ensuite, actualisez votre PAC afin qu'il atteigne à nouveau Cisco ISE :

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

Activer CTS globalement sur le commutateur 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)
```

Effectuer un mappage statique IP vers SGT pour les serveurs Web restreints (facultatif)

Ce serveur Web restreint ne passe jamais par ISE pour l'authentification. Vous devez donc l'étiqueter manuellement avec l'interface de ligne de commande du commutateur ou l'interface utilisateur graphique Web ISE, qui n'est qu'un des nombreux serveurs Web de Cisco.

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

Vérification de TrustSec sur le commutateur 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
```

Configurer TrustSec sur WLC

Configuration et vérification de l'ajout du WLC en tant que périphérique RADIUS dans Cisco ISE

The screenshot displays the Cisco ISE Administration console 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.

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

- 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
- RADIUS Authentication Settings:**
 - RADIUS UDP Settings:**
 - Protocol:** RADIUS
 - Shared Secret:** cisco
 - Use Second Shared Secret:** (unchecked)
 - CoA Port:** 1700
 - RADIUS DTLS Settings:**
 - DTLS Required:** (unchecked)
 - Shared Secret:** radius/dtls
 - CoA Port:** 2083
 - Issuer CA of ISE Certificates for CoA:** Select if required (optional)
 - DNS Name:** (empty)

Configurer et vérifier que le WLC est ajouté en tant que périphérique TrustSec dans Cisco ISE

Cette étape permet à Cisco ISE de déployer des mappages IP-vers-SGT statiques sur le WLC. Vous avez créé ces mappages dans l'interface utilisateur graphique Web de Cisco ISE dans **Work Centers > TrustSec > Components > IP SGT Static Mappings** à l'étape précédente.

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

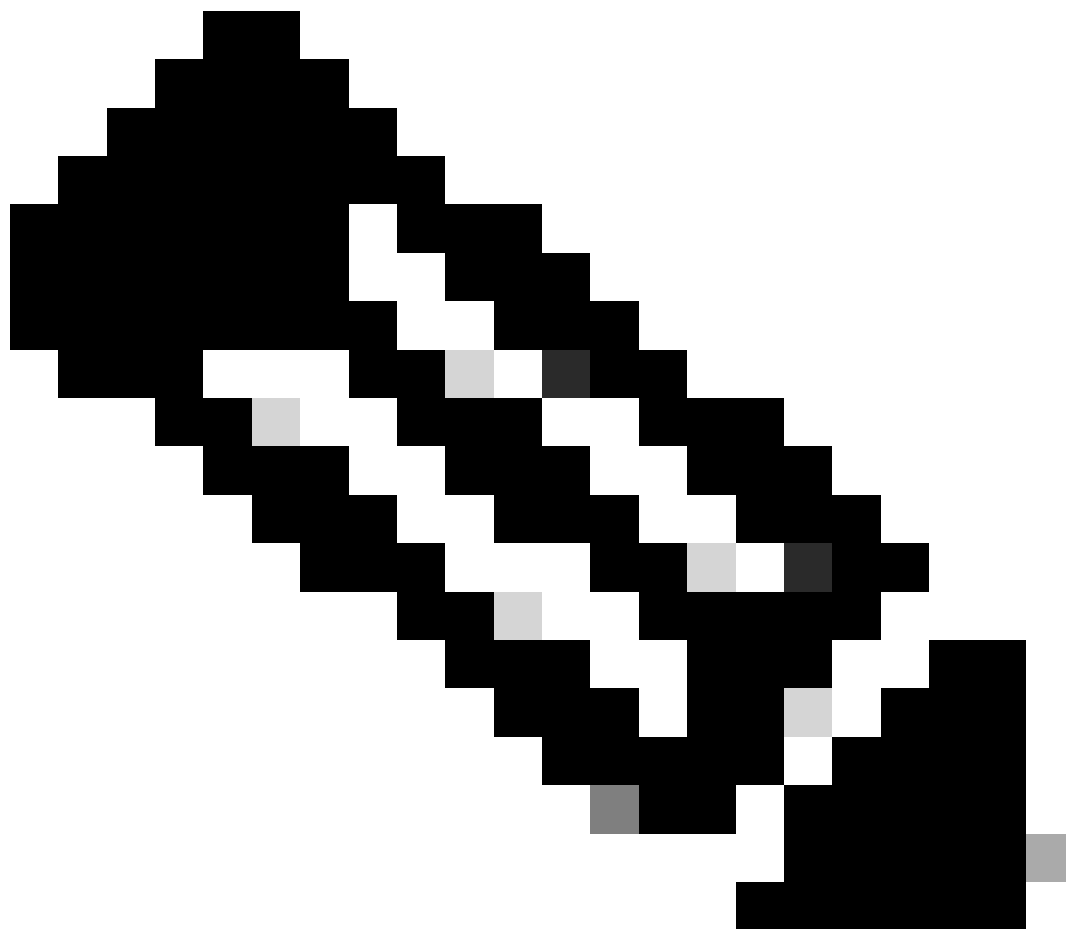
Enable Mode Password

Out Of Band (OOB) TrustSec PAC

Issue Date

Expiration Date

Issued By



Remarque : nous utilisons ceci Device Id et Password dans une étape ultérieure, dans Security > TrustSec > General dans l'interface utilisateur Web du WLC.

Activer le provisionnement PAC du 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
Realm List	
PAC Provisioning	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable



Activer TrustSec sur 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





Remarque : le CTS Device Id et le Password doivent être identiques au Device Id et Password que vous avez spécifiés dans la section Administration > Network Devices > Add Device > Advanced TrustSec Settings de Cisco ISE.

Vérifiez que le PAC a été configuré sur le WLC

Vous voyez le WLC a le PAC provisionné avec succès après avoir cliqué sur Refresh Env Data (vous faites ceci dans cette étape) :

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

Télécharger les données d'environnement CTS de Cisco ISE vers WLC

Après avoir cliqué sur Refresh Env Data, votre WLC télécharge vos 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

Activer les téléchargements et l'application SGACL sur le trafic

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

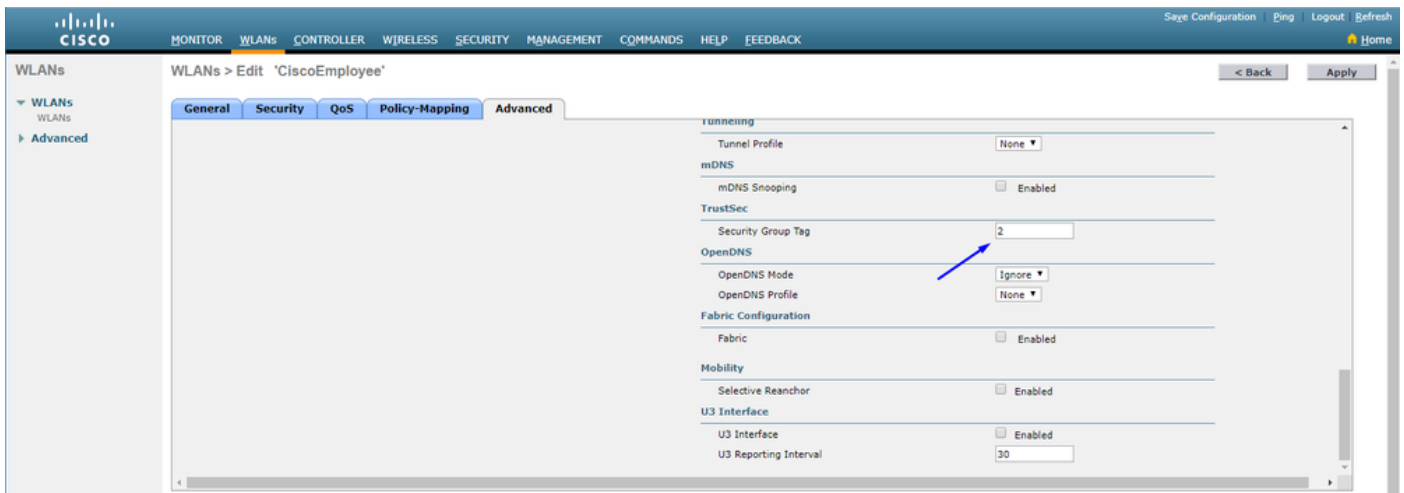
CTS Override Enabled

Sgacl Enforcement

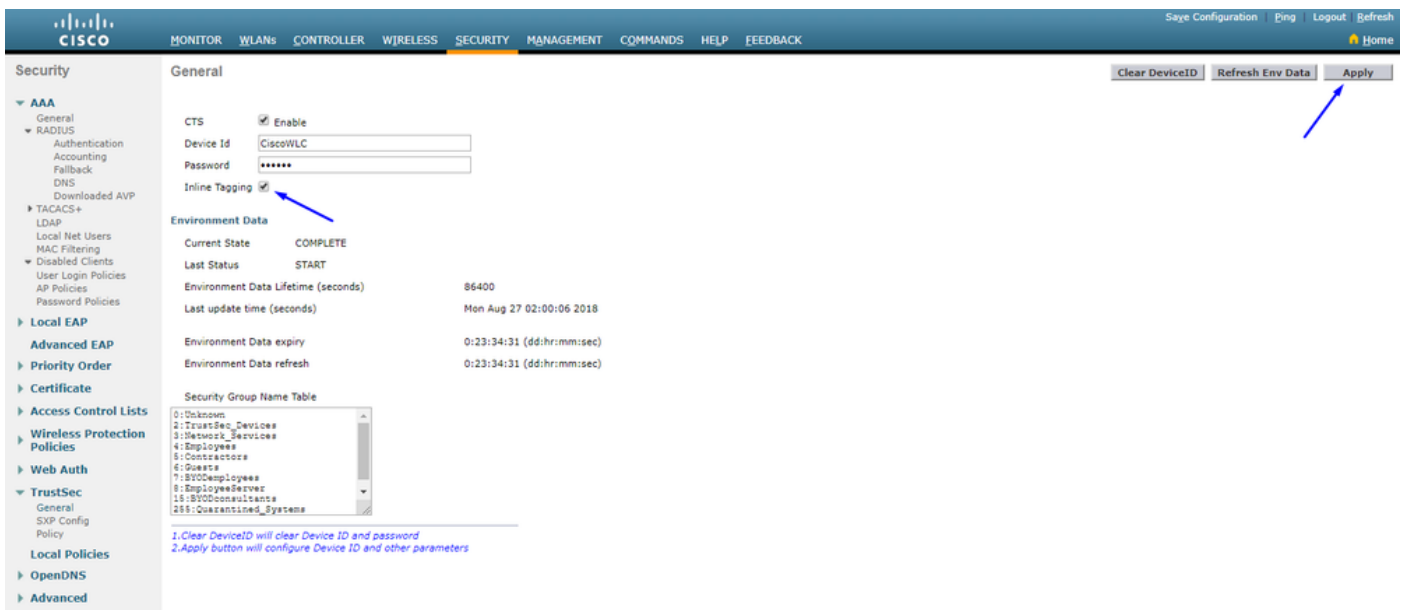
1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

Attribuer le SGT de 2 au WLC et au point d'accès (TrustSec_Devices)

Attribuez au WLC+WLAN un SGT de 2 (TrustSec_Devices) pour autoriser le trafic (SSH, HTTPS et CAPWAP) vers/depuis le WLC+AP via le commutateur.



Activer l'étiquetage en ligne sur WLC



Sous **Wireless > Access Points > Global Configuration** défiler vers le bas et sélectionnez **TrustSec Config**.

The screenshot shows the Cisco Wireless configuration page for 'All APs TrustSec Configuration'. The left sidebar contains a navigation menu with 'Global Configuration' selected. The main content area is titled 'TrustSec' and includes several configuration options:

- Sgacl Enforcement**:
- Inline Taging**: (highlighted with a blue box)
- AP SXP State**: Disabled ▼
- Default Password**: ••••••
- SXP Listener Min Hold Time (seconds)**: 90
- SXP Listener Max Hold Time (seconds)**: 180
- SXP Speaker Hold Time (seconds)**: 120
- Reconciliation Time Period (seconds)**: 120
- Retry Period (seconds)**: 120

Below these settings is the 'Peer Config' section with the following fields:

- Peer IP Address**: [Empty text box]
- Password**: Default ▼
- Local Mode**: Speaker ▼

An 'ADD' button is located below the Peer Config fields. At the bottom, there is a table header with columns: Peer IP Address, Password, SXP Mode. Below the header, there are two lines of blue text:

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)

Activer l'étiquetage en ligne sur le commutateur 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
```

Vérifier



Monitor Clients

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

Entries 1 - 1 of 1

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

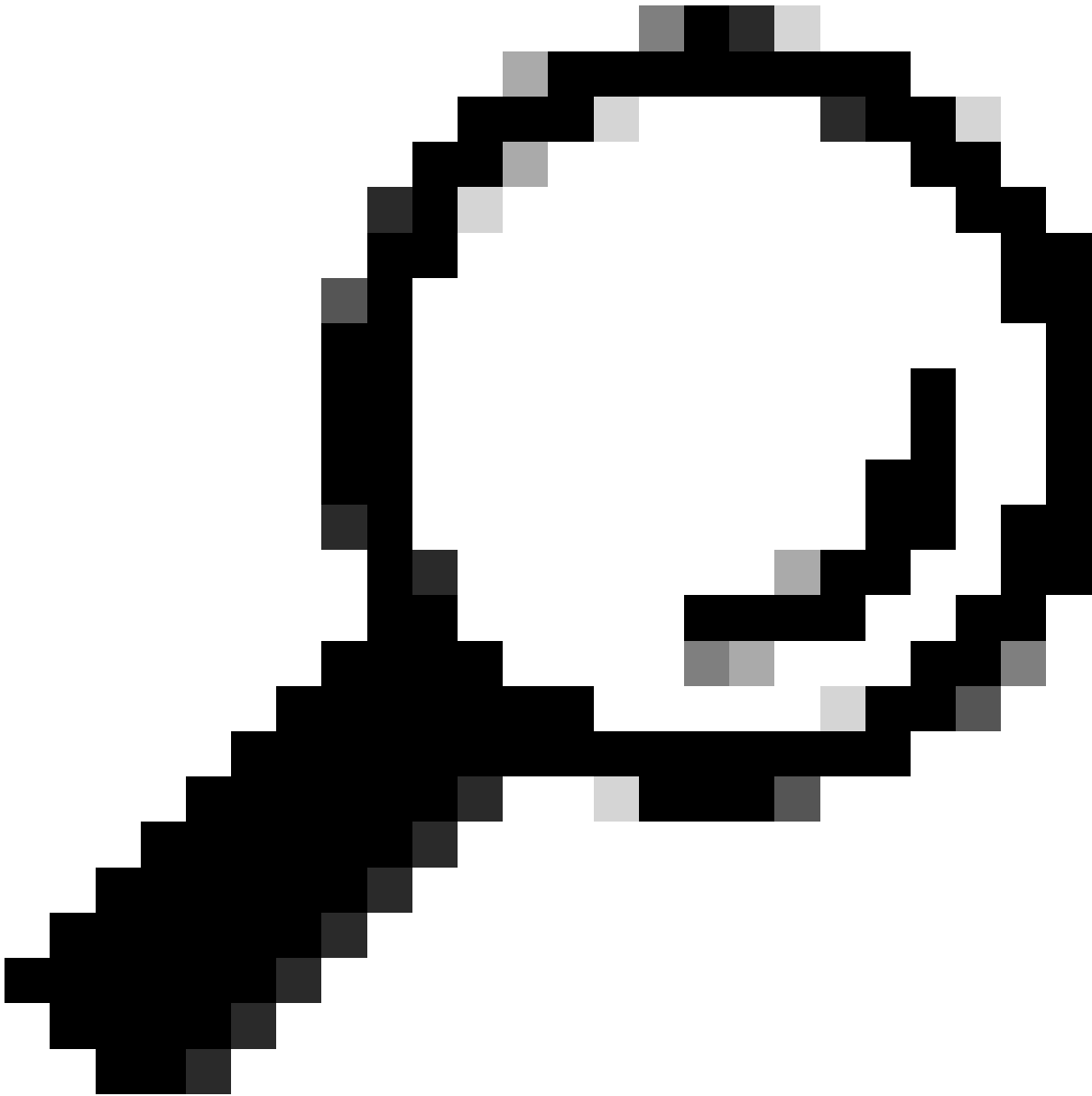
```
CatalystSwitch#show platform compteurs d'acl matériel | SGACL inc
```

Sortie IPv4 SGACL Drop (454) : 10 trames

Sortie SGACL IPv6 Drop (455) : 0 trame

Perte de cellule SGACL IPv4 en sortie (456) : 0 trame

Perte de cellule SGACL IPv6 en sortie (457) : 0 trame

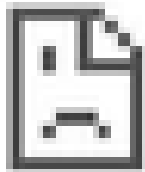


Conseil : si vous utilisez plutôt Cisco ASR, Nexus ou Cisco ASA, le document répertorié ici peut vous aider à vérifier que vos balises SGT sont appliquées : [Guide de dépannage TrustSec](#).

Authentifiez-vous sur le réseau sans fil avec le nom d'utilisateur jsmith password Admin123 - vous rencontrez la liste de contrôle d'accès deny dans le commutateur :



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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.