

# ISE ( インラインタギング ) を使用した TrustSec(SGT)の設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [設定](#)

#### [ネットワーク図](#)

#### [目標](#)

#### [コンフィギュレーション](#)

##### [ISEでのTrustSecの設定](#)

##### [TrustSec AAAサーバとしてのCisco ISEの設定](#)

##### [スイッチがCisco ISEのRADIUSデバイスとして追加されるように設定および確認する](#)

##### [Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認](#)

##### [TrustSecのデフォルト設定が許容可能であることを確認する \( オプション \)](#)

##### [ワイヤレスユーザ用のセキュリティグループタグの作成](#)

##### [制限付きWebサーバのスタティックIP-to-SGTマッピングの作成](#)

##### [証明書認証プロファイルの作成](#)

##### [以前の証明書認証プロファイルを使用したIDソースシーケンスの作成](#)

##### [ワイヤレスユーザ \( 従業員およびコンサルタント \) に適切なSGTを割り当てる](#)

##### [実際のデバイス \( スwitchおよびWLC \) へのSGTの割り当て](#)

##### [出力ポリシーを指定するSGACLの定義](#)

##### [Cisco ISEのTrustSecポリシーマトリックスでのACLの適用](#)

#### [CatalystスイッチでのTrustSecの設定](#)

##### [CatalystスイッチでAAAにCisco TrustSecを使用するためのスイッチの設定](#)

##### [Cisco ISEに対してスイッチを認証するためのRADIUSサーバでのPACキーの設定](#)

##### [スイッチをCisco ISEに認証するためのCTSクレデンシャルの設定](#)

##### [CatalystスイッチでのCTSのグローバルな有効化](#)

##### [制限付きWebサーバのスタティックIP-to-SGTマッピングの作成 \( オプション \)](#)

##### [CatalystスイッチでのTrustSecの確認](#)

#### [WLCでのTrustSecの設定](#)

##### [Cisco ISEでRADIUSデバイスとして追加されるWLCの設定と確認](#)

##### [Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認](#)

##### [WLCのPACプロビジョニングの有効化](#)

##### [WLCでのTrustSecの有効化](#)

##### [PACがWLCでプロビジョニングされていることの確認](#)

##### [Cisco ISEからWLCへのCTS環境データのダウンロード](#)

##### [トラフィックに対するSGACLのダウンロードと適用の有効化](#)

##### [WLCとアクセスポイントに2のSGTを割り当てる \( TrustSec Devices \)](#)

##### [WLCでのインラインタギングの有効化](#)

##### [Catalystスイッチでのインラインタギングの有効化](#)

### [確認](#)

---

# はじめに

このドキュメントでは、Identity Services Engine(ISE)を使用して、CatalystスイッチおよびワイヤレスLANコントローラ(WLC)上でTrustSecを設定および確認する方法について説明します。

## 前提条件

次の項目に関する知識があることが推奨されます。

- Cisco TrustSec(CTS)コンポーネントの基礎知識
- Catalyst スwitchの CLI 設定に関する基本的な知識
- CiscoワイヤレスLANコントローラ(WLC)のGUI設定に関する基本的な知識
- Identity Services Engine ( ISE ) 設定の経験

## 要件

Cisco ISEをネットワークに導入し、エンドユーザがワイヤレスまたは有線に接続する際は、802.1x ( またはその他の方法 ) でCisco ISEに認証する必要があります。Cisco ISEは、ワイヤレスネットワークへの認証後に、トラフィックにセキュリティグループタグ(SGT)を割り当てます。

この例では、エンドユーザはCisco ISEの個人所有デバイスの持ち込み(BYOD)ポータルにリダイレクトされ、証明書がプロビジョニングされます。これにより、エンドユーザはBYODポータルの手順を完了した後、Extensible Authentication Protocol-Transport Layer Security(EAP-TLS)を使用してワイヤレスネットワークに安全にアクセスできます。

## 使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco Identity Services Engineバージョン2.4
- Cisco Catalyst 3850スイッチバージョン3.7.5E
- Cisco WLCバージョン8.5.120.0
- ローカルモードのCisco Aironetワイヤレスアクセスポイント

Cisco TrustSecを導入する前に、ご使用のCisco CatalystスイッチまたはCisco WLC+APモデル+ソフトウェアバージョンで次の機能がサポートされていることを確認します。

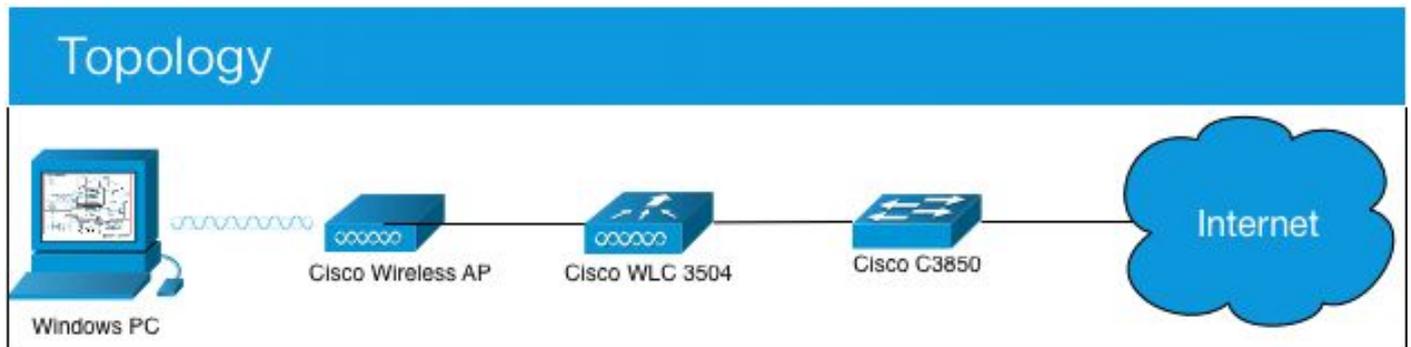
- TrustSec/セキュリティグループタグ
- インラインタギング ( 使用しない場合は、インラインタギングの代わりにSXPを使用できません )
- IPからSGTへの静的マッピング ( 必要に応じて )
- サブネットからSGTへのスタティックマッピング ( 必要な場合 )
- VLANからSGTへのスタティックマッピング ( 必要な場合 )

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな ( デフォルト ) 設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ネットワーク図



この例では、WLCは、コンサルタントからの場合はSGT 15、従業員からの場合は+ SGT 7としてパケットをタグ付けします。

これらのパケットがSGT 15からSGT 8の場合、スイッチはこれらのパケットを拒否します（コンサルタントはSGT 8としてタグ付けされたサーバにアクセスできません）。

スイッチは、SGT 7からSGT 8のパケットを許可します（従業員はSGT 8としてタグ付けされたサーバにアクセスできます）。

### 目標

誰でもGuestSSIDにアクセスできる。

コンサルタントはEmployeeSSIDにアクセスできるが、アクセスは制限される

従業員はフルアクセスでEmployeeSSIDにアクセスできます。

デバイス	IP アドレス	VLAN
ISE	10.201.214.230	463
Catalyst スイッチ	10.201.235.102	1115
WLC	10.201.214.229	463
アクセス ポイント	10.201.214.138	455

[名前(Name)]	ユーザ名	ADグループ	SG	SGT
ジェイソン・ スミス	ジャスミス	コンサルタント	BYODコンサルタント	15
サリー・ スミス	スミス	従業員	BYOD従業員	7
該当なし	該当なし	該当なし	TrustSec_Devices	2

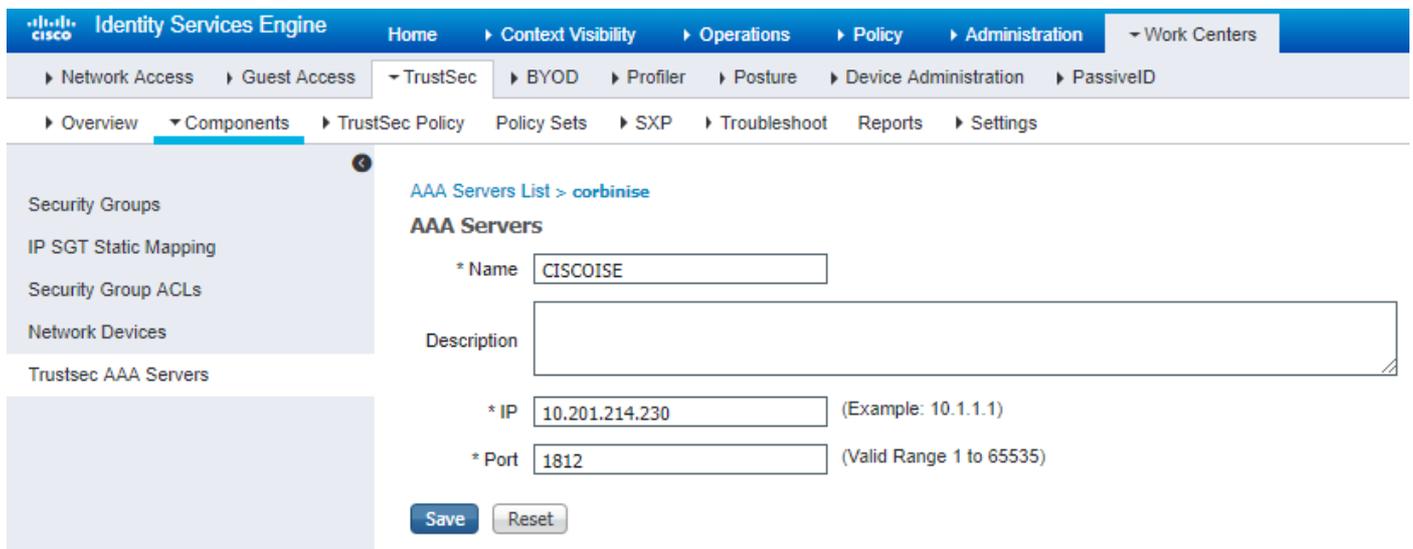
### コンフィギュレーション

# ISEでのTrustSecの設定

## 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="#">?</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>

## TrustSec AAAサーバとしてのCisco ISEの設定



スイッチがCisco ISEのRADIUSデバイスとして追加されるように設定および確認する

The screenshot displays the Cisco ISE Web GUI for configuring a Network Device. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC > Network Devices. The left sidebar shows 'Network Devices' with sub-items 'Default Device' and 'Device Security Settings'. The main content area is titled 'Network Devices List > CatalystSwitch' and 'Network Devices'. The configuration form includes: \* Name: CatalystSwitch; Description: Catalyst 3850 Switch; IP Address: 10.201.235.102 / 32; \* Device Profile: Cisco; Model Name: (empty); Software Version: (empty); \* Network Device Group: Location (All Locations), IPSEC (No), Device Type (All Device Types); and RADIUS Authentication Settings (checked) with RADIUS UDP Settings: Protocol (RADIUS), \* Shared Secret (Admin123), Use Second Shared Secret (unchecked), CoA Port (1700), and RADIUS DTLS Settings: DTLS Required (unchecked), Shared Secret (radius/dtls).

## Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認

SSHのログインクレデンシャルを入力します。これにより、Cisco ISEはスタティックIP-to-SGTマッピングをスイッチに導入できます。

これらはCisco ISE Web GUIのWork Centers > TrustSec > Components > IP SGT Static Mappingsで次のように作成します。

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:

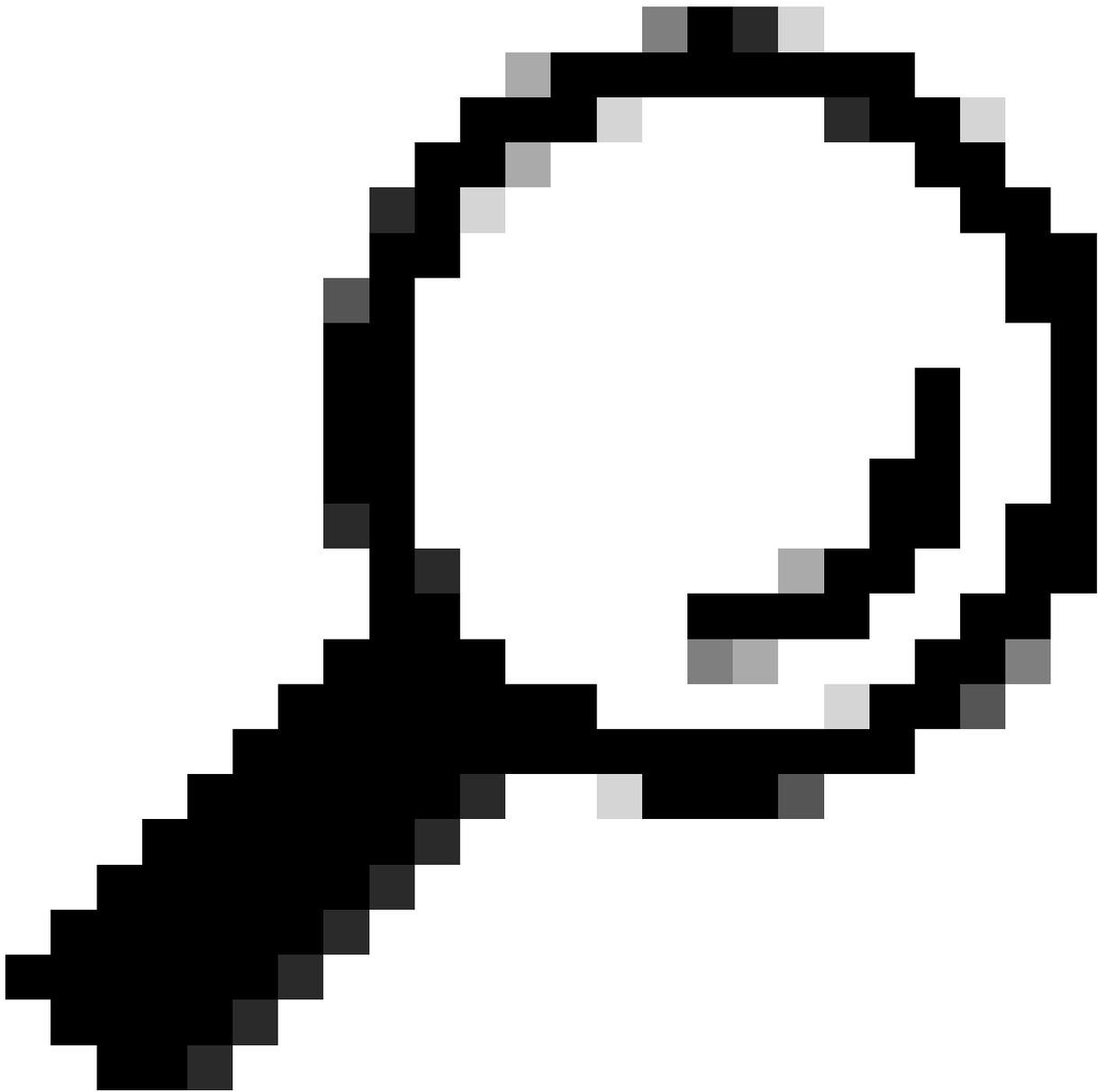
---

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

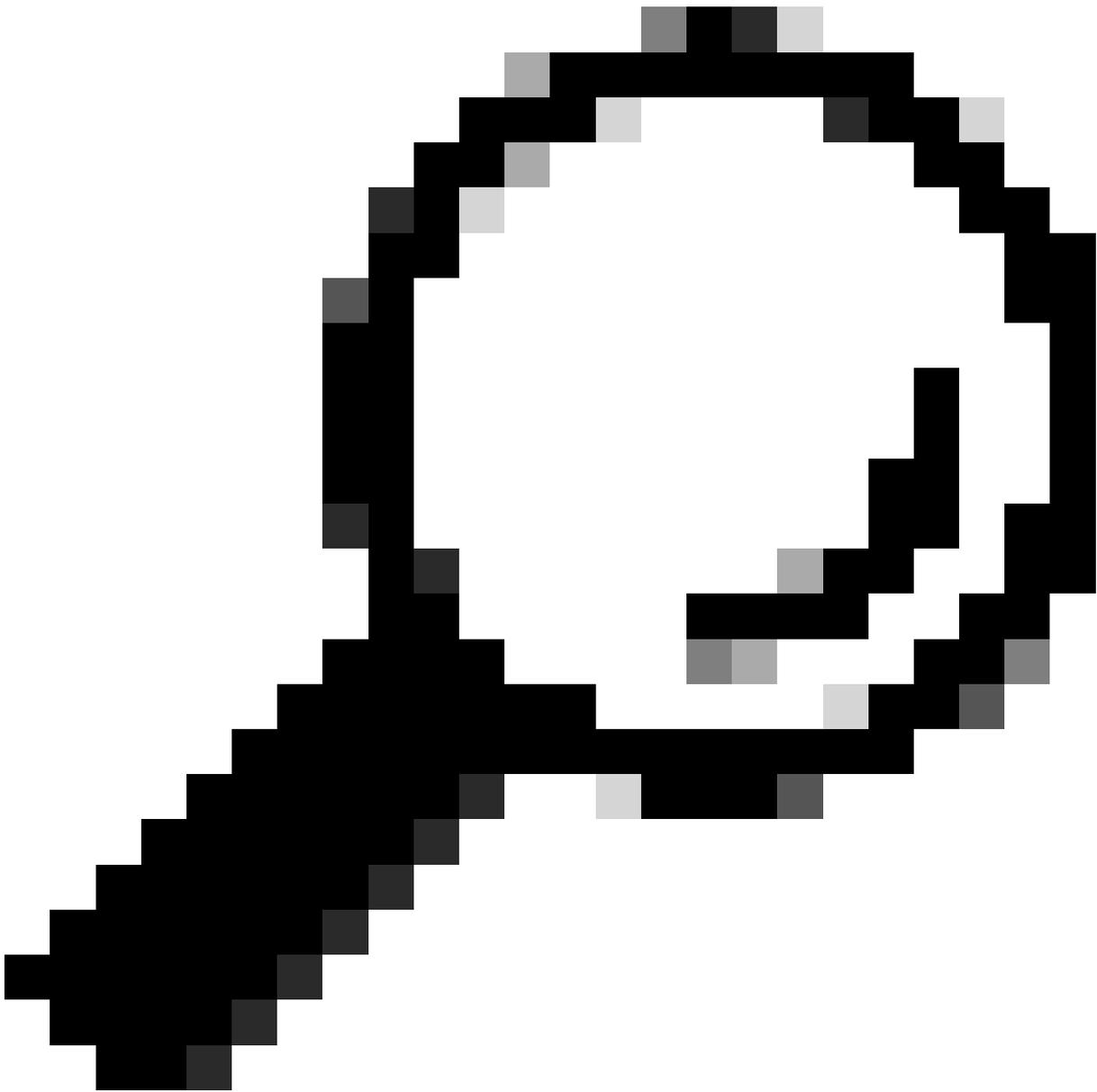
Issue Date:

Expiration Date:

Issued By:



ヒント：まだCatalystスイッチでSSHを設定していない場合は、このガイド「[Catalystスイッチでのセキュアシェル \(SSH\)の設定方法](#)」を使用できます。



ヒント: Cisco ISEがSSH経由でCatalystスイッチにアクセスできるようにしたくない場合は、代わりにCLIを使用して、Catalystスイッチ上でIPとSGTの静的マッピングを作成できます(このステップを参照)。

---

TrustSecのデフォルト設定が許容可能であることを確認する(オプション)



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 ⓘ

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 ⓘ

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

ワイヤレスユーザ用のセキュリティグループタグの作成

BYODコンサルタント用セキュリティグループの作成 – SGT 15

BYOD従業員用セキュリティグループの作成 – 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	

### 制限付きWebサーバのスタティックIP-to-SGTマッピングの作成

MAC認証バイパス(MAB)、802.1x、プロファイルなどでCisco ISEに対して認証されないネットワーク内の他のIPアドレスまたはサブネットに対して、これを実行します。

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

### 証明書認証プロファイルの作成

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

以前の証明書認証プロファイルを使用したIDソースシーケンスの作成

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="&gt;"/> <input type="button" value="&lt;"/> <input type="button" value="&gt;&gt;"/> <input type="button" value="&lt;&lt;"/>	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

ワイヤレスユーザ（従業員およびコンサルタント）に適切なSGTを割り当てる

[名前(Name)]	ユーザ名	ADグループ	SG	SGT
ジェイソン・スミス	ジャスミス	コンサルタント	BYODコンサルタント	15
サリー・スミス	スミス	従業員	BYOD従業員	7
該当なし	該当なし	該当なし	TrustSec_Devices	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_User_ID_Stores	0	Options

Authorization Policy (3)

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

実際のデバイス (スイッチおよびWLC) へのSGTの割り当て

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

Egress Policy

- Matrices List
- Matrix
- Source Tree
- Destination Tree
- Network Device Authorization

### 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

出力ポリシーを指定するSGACLの定義

コンサルタントは外部の任意の場所からアクセスできるが、内部のアクセスは制限：

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

```

従業員が外部および内部の任意の場所からアクセスできるようにする：

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

```

他のデバイスから基本サービスへのアクセスを許可する（オプション）：

Identity Services Engine > Administration > Work Centers > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > 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

```

すべてのエンドユーザをCisco ISEにリダイレクトします ( BYODポータルリダイレクション用 )。DNS、DHCP、ping、またはWebAuthトラフィックはCisco ISEに送信できないため、これらを含めないでください。

Identity Services Engine > Administration > Work Centers > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > 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

```

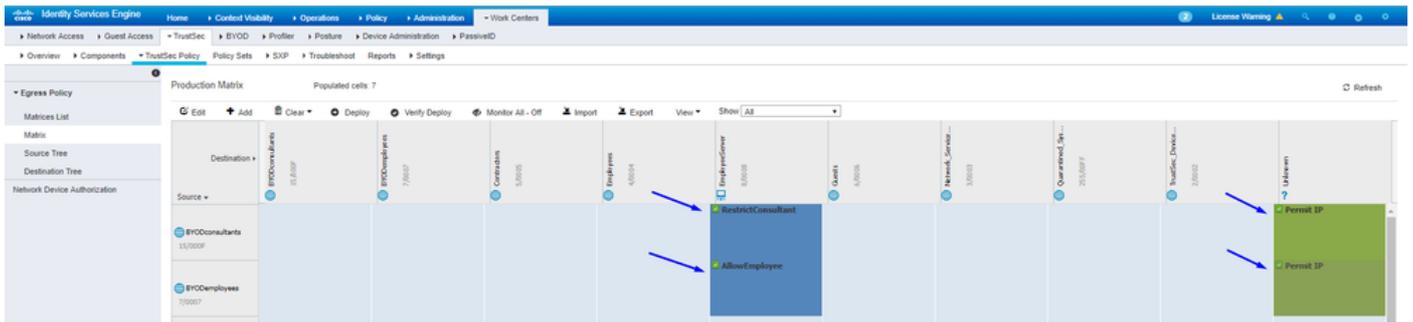
deny udp dst eq 67
deny udp dst eq 53
deny tcp dst eq 53
deny icmp
deny tcp dst eq 8443
permit ip

```

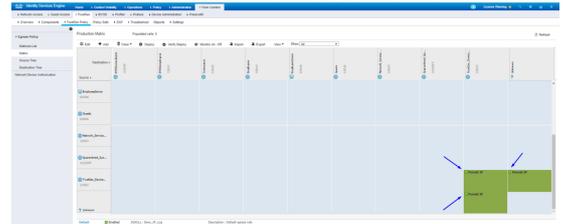
#### Cisco ISEのTrustSecポリシーマトリックスでのACLの適用

コンサルタントは外部のあらゆる場所からアクセスできるが、<https://10.201.214.132>などの内部Webサーバは制限される

従業員が外部の任意の場所にアクセスできるようにし、内部Webサーバを許可する：

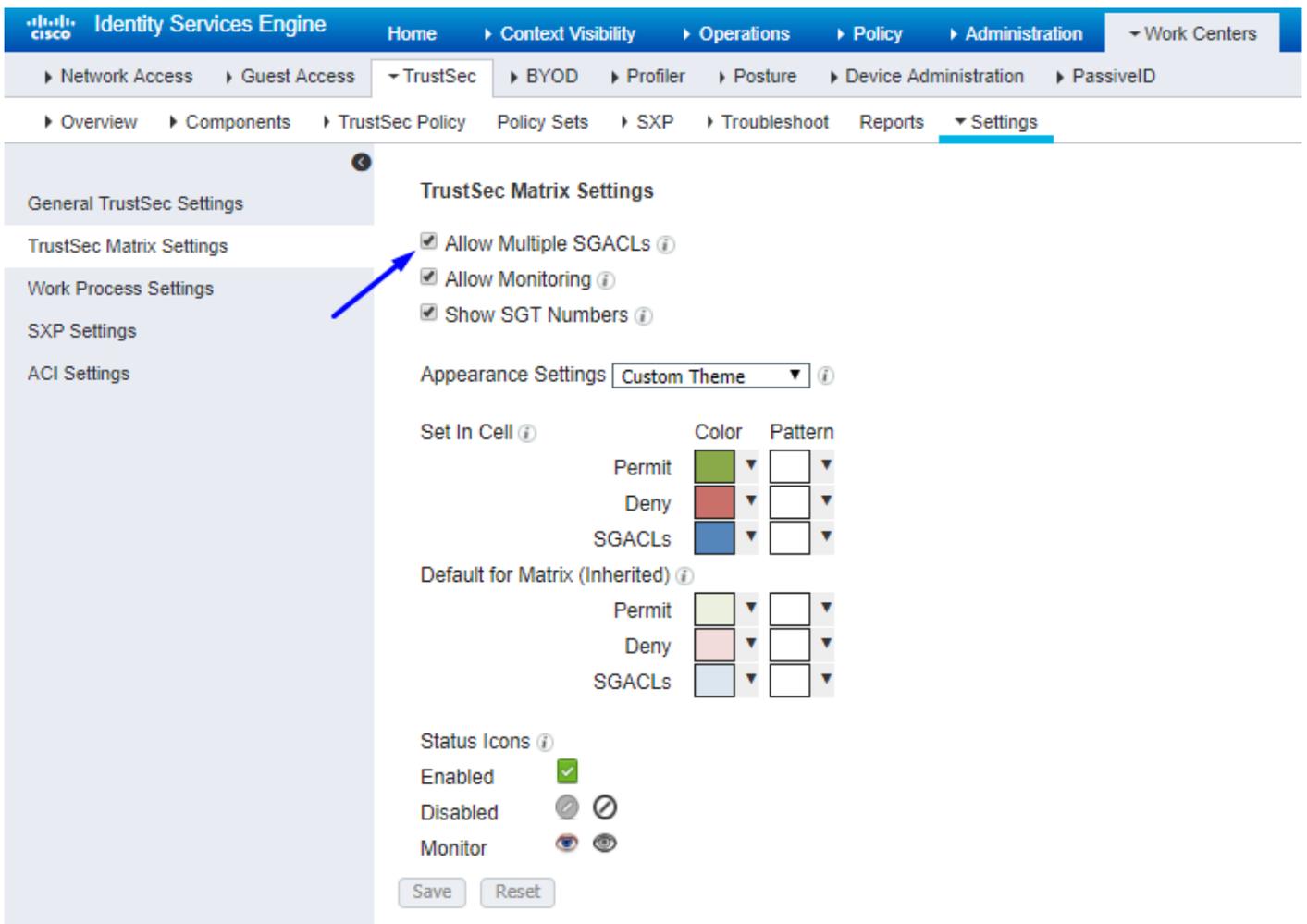


ネットワーク上のデバイス (スイッチとWLC) との間の管理トラフィック (SSH、HTTPS、およびCAPWAP) を許可し、Cisco



TrustSecを導入した後にSSHまたはHTTPSアクセスが失われないようにします。

Cisco ISEで Allow Multiple SGACLsを有効にします。



Cisco ISEの右上隅にあるPushをクリックして、設定をデバイスに適用します。この作業は後で行う必要があります。

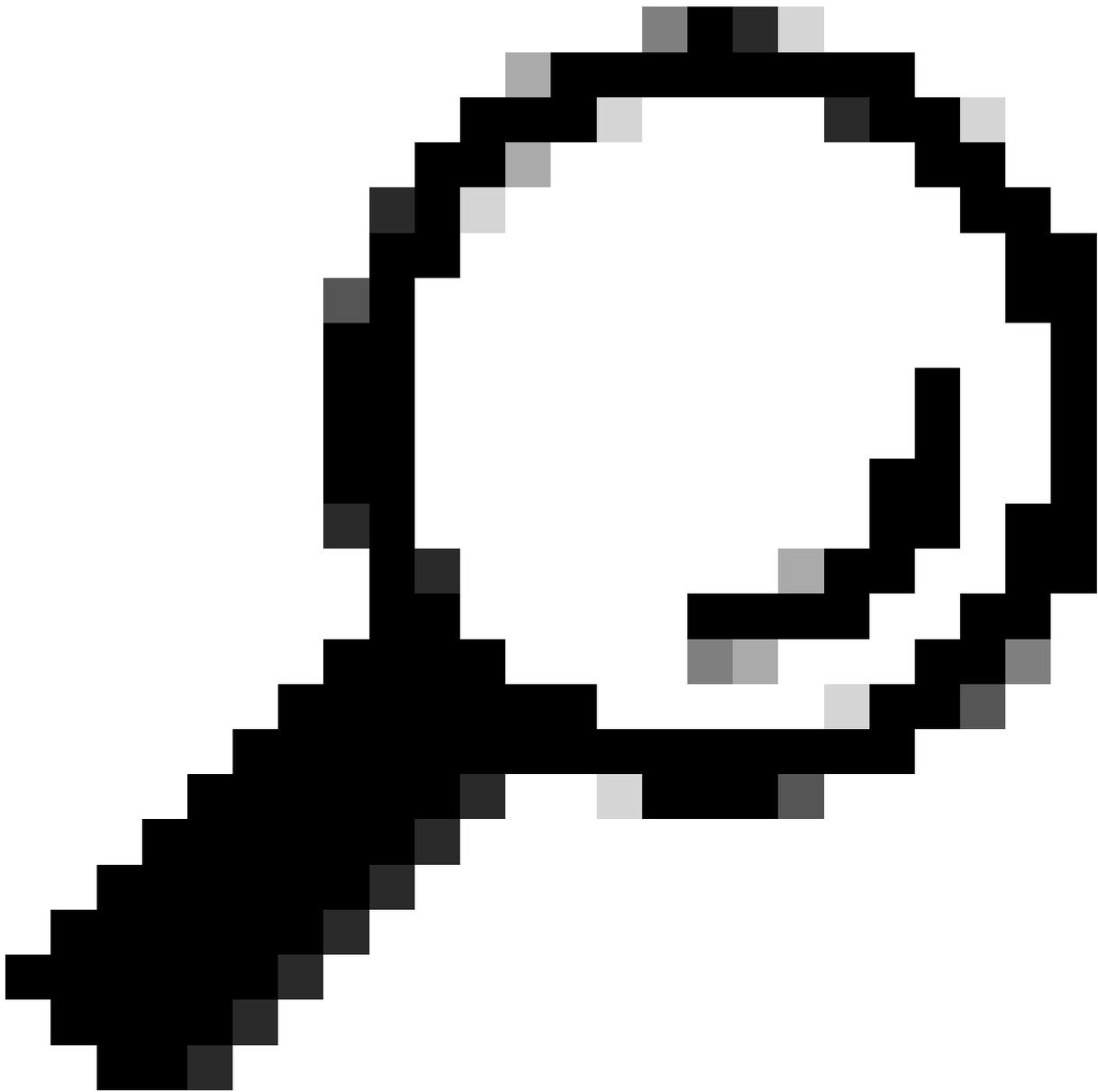
There are TrustSec configuration changes that has not been notified to network devices. To notify the relevant network devices about these changes click the push button.



Push

CatalystスイッチでのTrustSecの設定

CatalystスイッチでAAAにCisco TrustSecを使用するためのスイッチの設定



ヒント：このドキュメントでは、ワイヤレスユーザがCisco ISEによるBYODをすでに完了していることを前提としています。

---

太字で示されているコマンドは、BYODワイヤレスがISEと連動するようにこの前にすでに設定されています。

<#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
```



注:PACキーは、 **Administration > Network Devices > Add Device > RADIUS Authentication Settings** セクションで指定したRADIUS共有秘密と同じである必要があります。

---

<#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
```

Cisco ISEに対してスイッチを認証するためのRADIUSサーバでのPACキーの設定

```
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  ⓘ



注:PACキーは、Cisco ISEの **Administration > Network Devices > Add Device > RADIUS Authentication Settings** セクションで指定したRADIUS共有秘密と同じである必要があります (画面キャプチャを参照)。

---

スイッチをCisco ISEに認証するためのCTSクレデンシャルの設定

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

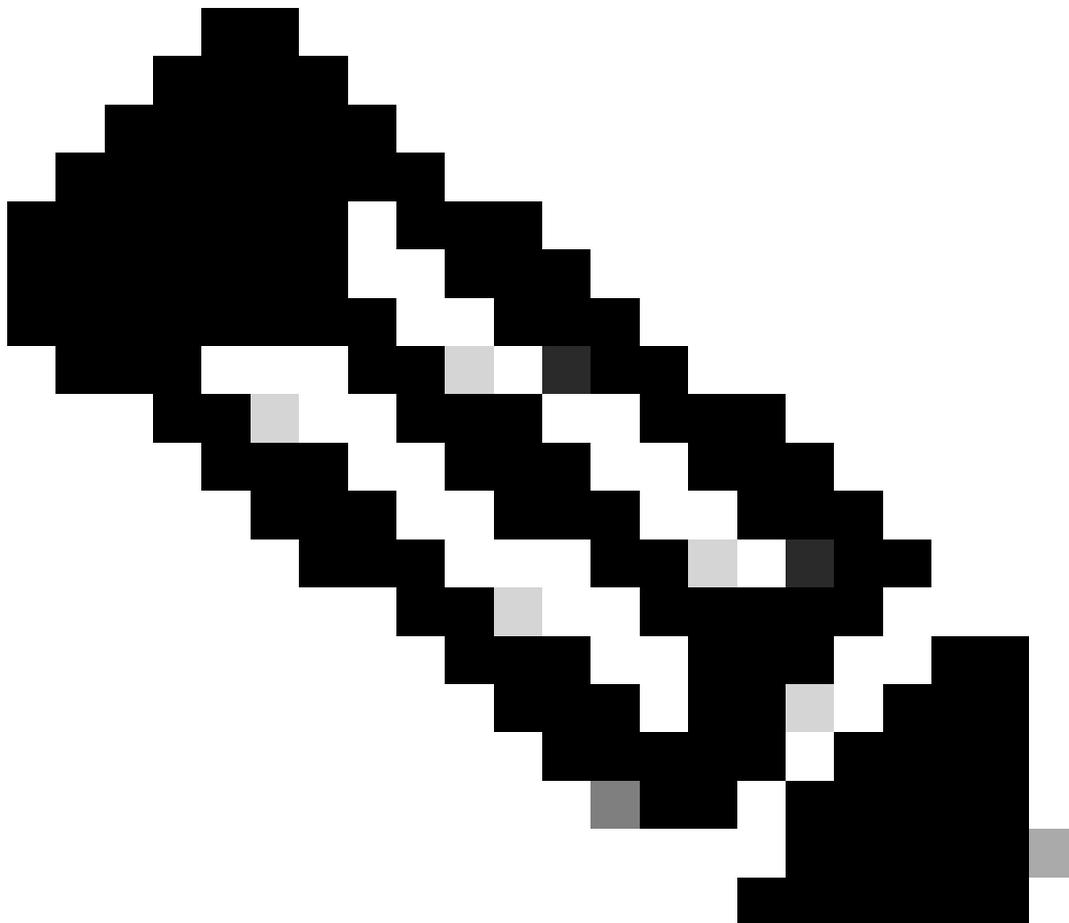
Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id CatalystSwitch

\* Password Admin123 Hide



注：CTSクレデンシャルは、デバイスID +パスワードと同じでなければなりません。CTSクレデンシャルは、Cisco ISEのAdministration > Network Devices > Add Device > Advanced TrustSec Settingsセクションで指定したデバイスID +パス

---

ワードと同じである必要があります ( 画面キャプチャを参照 ) 。

---

次に、PACを更新してCisco ISEに再びアクセスできるようにします。

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

CatalystスイッチでのCTSのグローバルな有効化

```
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)
```

制限付きWebサーバのスタティックIP-to-SGTマッピングの作成 ( オプション )

この制限付きWebサーバは、これまで認証のためにISEを経由することはないため、スイッチCLIまたはISE Web GUIを使用して手動でタグ付けする必要があります。これは、シスコに数多く存在するWebサーバの1つです。

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

CatalystスイッチでのTrustSecの確認

```
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
```

## WLCでのTrustSecの設定

### Cisco ISEでRADIUSデバイスとして追加されるWLCの設定と確認

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

**Network Devices List > CiscoWLC**

**Network Devices**

- \* Name: CiscoWLC
- Description: Cisco 3504 WLC

**IP Address** \* IP: 10.201.235.123 / 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: 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: [ ]

### Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認

このステップにより、Cisco ISEはIPからSGTへのスタティックなマッピングをWLCに導入できます。これらのマッピングは、前の手順でCisco ISE Web GUIのWork Centers > TrustSec > Components > IP SGT Static Mappingsで作成しました。

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

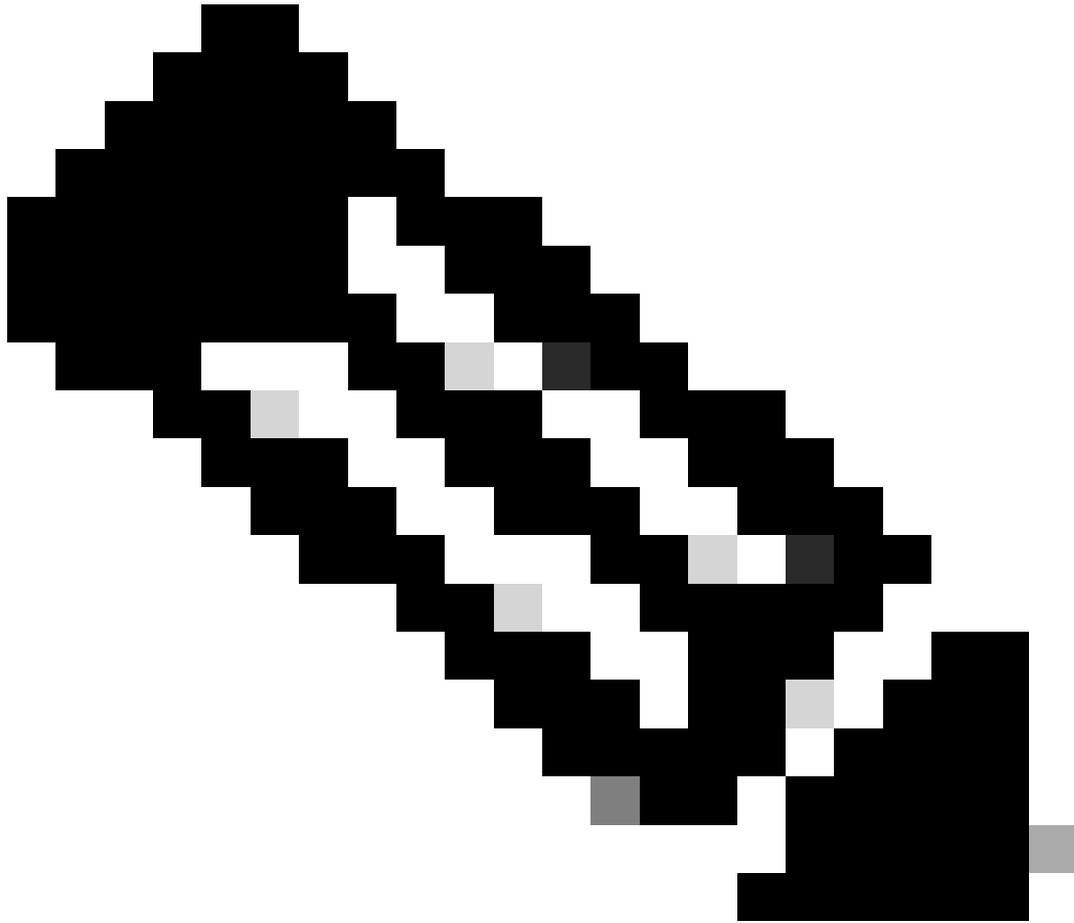
Enable Mode Password

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

Issue Date

Expiration Date

Issued By



注：この Device Id と Password は後の手順でWLC Web UIのSecurity > TrustSec > Generalで使用します。

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



WLCでのTrustSecの有効化

### 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

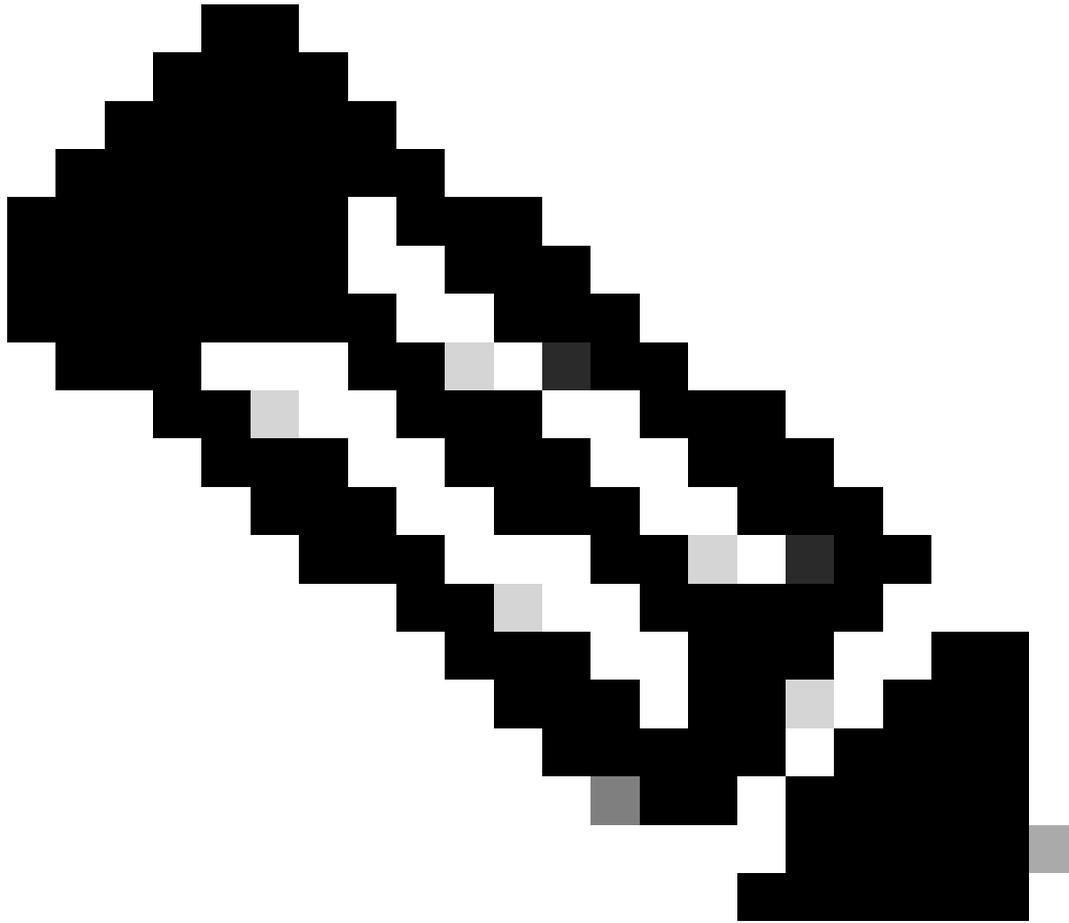
### Environment Data

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





**注:**CTSおよび Device Id び Password は、Cisco ISEのAdministration > Network Devices > Add Device > Advanced TrustSec Settingsセクションで指定した Device Id および Password と同じにする必要があります。

---

PACがWLCでプロビジョニングされていることの確認

Refresh Env Dataをクリックすると、WLCにPACが正常にプロビジョニングされたことが表示されます (このステップで実行します)。

**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	<input type="button" value="Clear PAC"/>
PAC A-ID	ef2e1222e67eb4630a8b22d1ff0216c1	
PAC Lifetime	Wed Nov 21 00:01:07 2018	

IPSec:  Enable

Cisco ISEからWLCへのCTS環境データのダウンロード

Refresh Env Dataをクリックすると、WLCがSGTをダウンロードします。

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

トラフィックに対するSGACLのダウンロードと適用の有効化

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

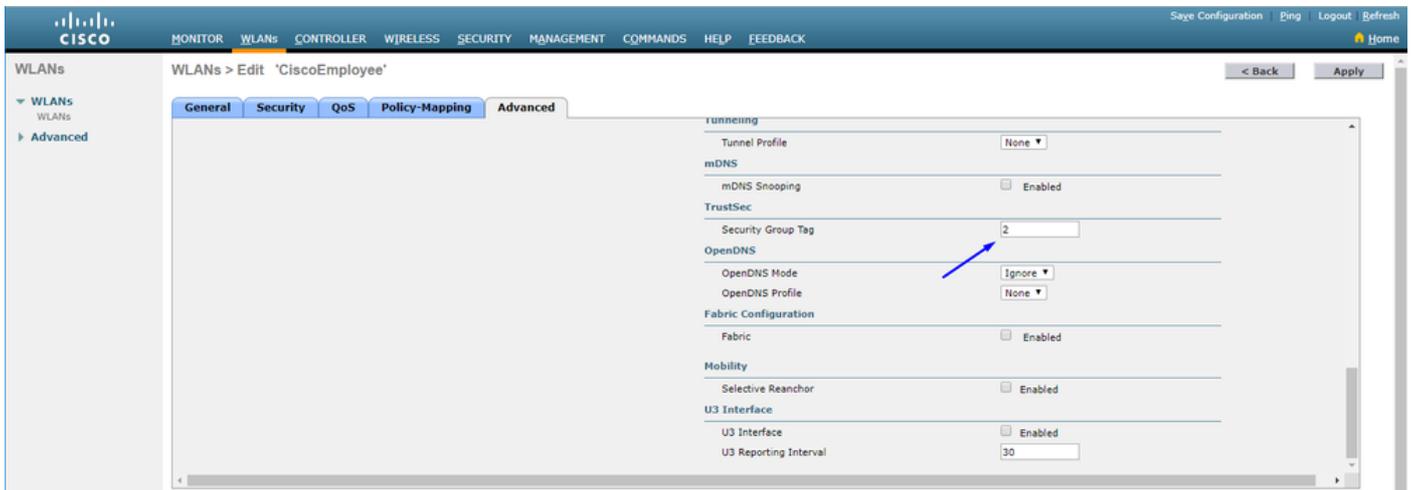
CTS Override Enabled

Sgacl Enforcement

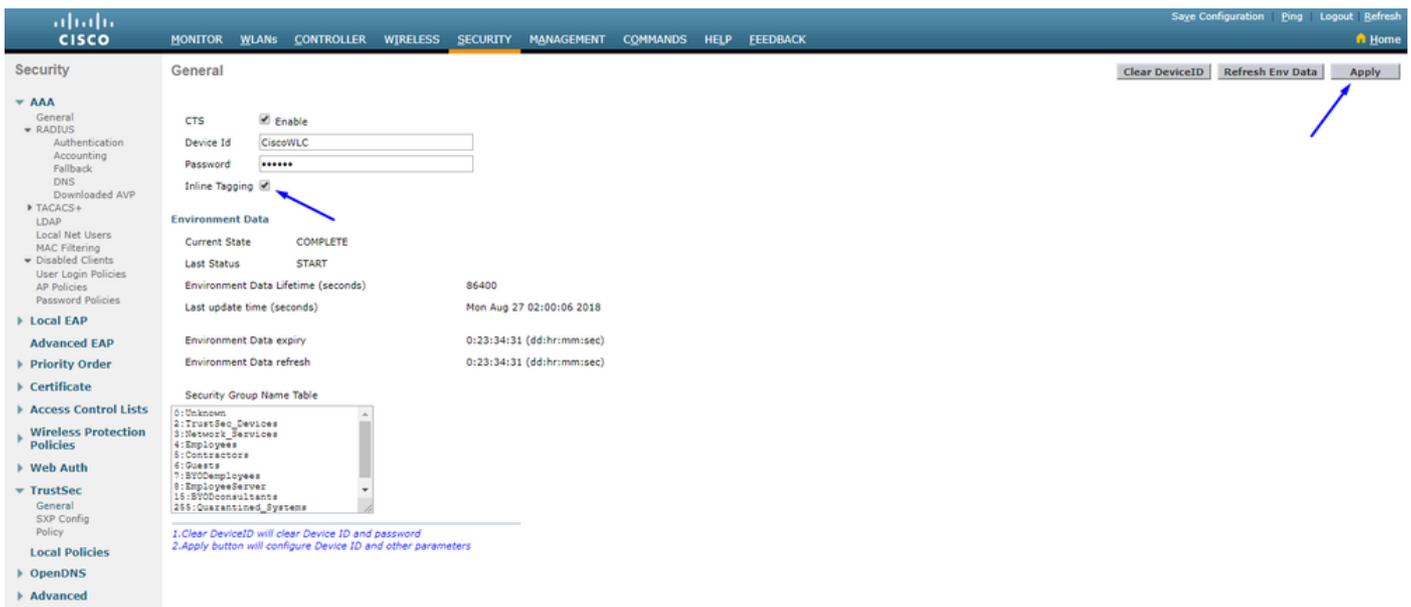
1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)  
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

WLCとアクセスポイントに2のSGTを割り当てる(TrustSec\_Devices)

WLC+WLANに2(TrustSec\_Devices)のSGTを割り当て、スイッチを介したWLC+APとの間のトラフィック ( SSH、HTTPS、およびCAPWAP ) を許可します。



WLCでのインラインタギングの有効化



下にスク Wireless > Access Points > Global Configuration ロールダウンして、 TrustSec Configを選択します。

The screenshot shows the Cisco Catalyst switch configuration interface for 'All APs TrustSec Configuration'. The left sidebar contains a navigation menu with categories like 'Wireless', 'Access Points', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', 'Network Lists', '802.11a/n/ac', '802.11b/g/n', 'Media Stream', 'Application Visibility And Control', 'Lync Server', 'Country', 'Timers', 'Netflow', and 'QoS'. The main content area is titled 'All APs TrustSec Configuration' and includes a 'TrustSec' section with the following settings:

- Sgac 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 the TrustSec section is the 'Peer Config' section, which includes fields for Peer IP Address, Password (Default ▼), and Local Mode (Speaker ▼), along with an 'ADD' button. At the bottom, there is a table header for 'Peer IP Address Password SXP Mode' and two lines of explanatory 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)

Catalystスイッチでのインラインタギングの有効化

<#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
```

## 確認

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

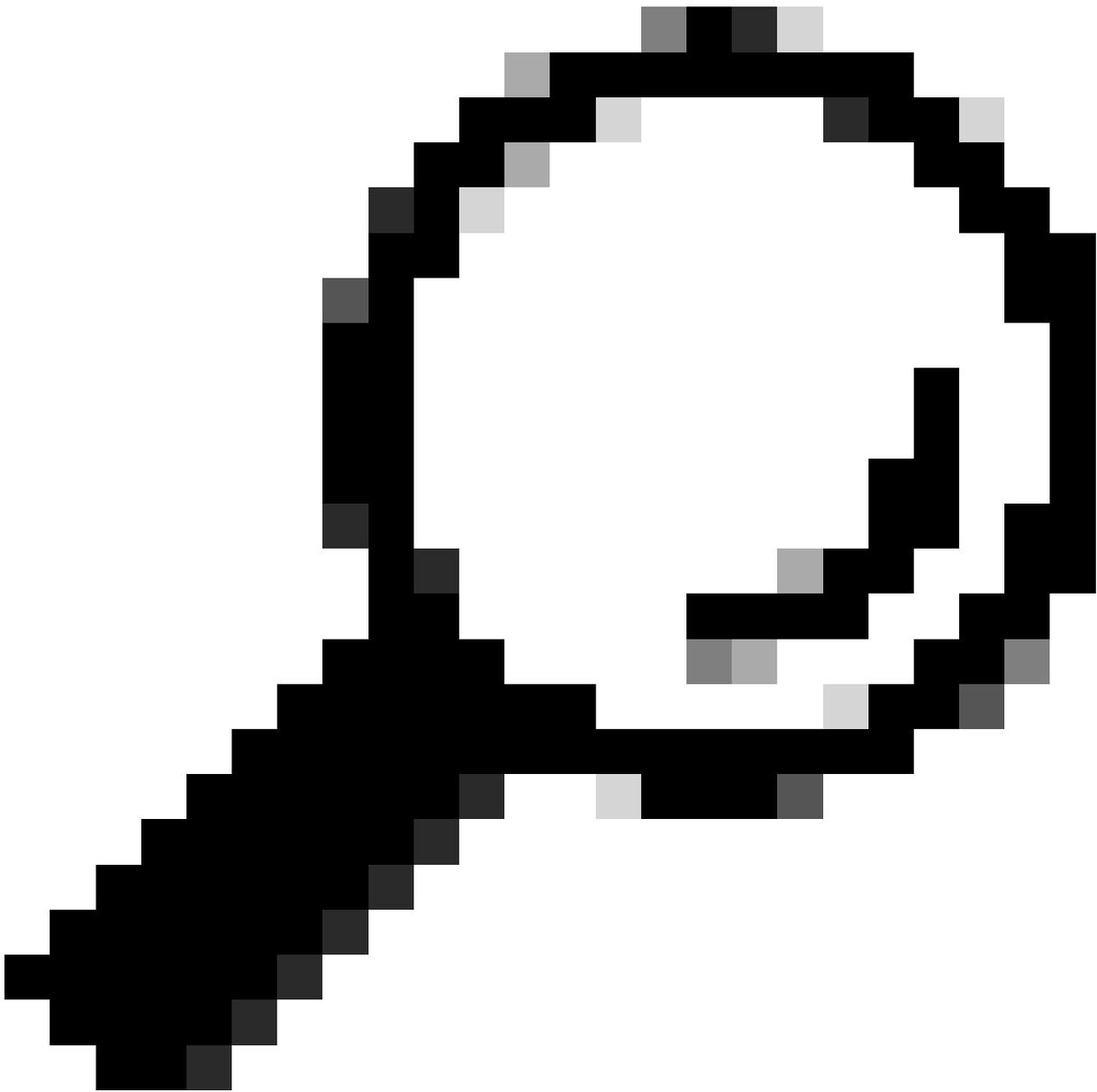
```
CatalystSwitch#show platform acl counters hardware | SGACLを含む
```

出力IPv4 SGACLドロップ(454):10フレーム

出力IPv6 SGACLドロップ(455):0フレーム

出力IPv4 SGACLセルドロップ(456):0フレーム

出力IPv6 SGACLセルドロップ(457):0フレーム



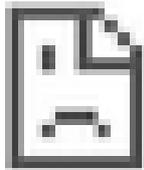
ヒント：代わりにCisco ASR、Nexus、またはCisco ASAを使用する場合は、次に示すドキュメントが、SGTタグが適用されていることを確認するのに役立ちます：『[TrustSec Troubleshooting Guide](#)』。

---

ユーザ名jsmith、パスワードAdmin123を使用して無線に対して認証を行うと、スイッチでdeny ACLが検出されます。



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



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。