

# 使用ISE配置TrustSec (SGT) ( 內聯標籤 )

## 目錄

---

### [簡介](#)

### [必要條件](#)

[需求](#)

[採用元件](#)

### [設定](#)

[網路圖表](#)

[目標](#)

[組態](#)

[在ISE上配置TrustSec](#)

[將Cisco ISE配置為TrustSec AAA伺服器](#)

[配置並驗證交換機是否增加為Cisco ISE中的RADIUS裝置](#)

[配置並驗證WLC在思科ISE中增加為TrustSec裝置](#)

[驗證預設TrustSec設定以確保這些設定可接受 \( 可選 \)](#)

[為無線使用者建立安全組標籤](#)

[為受限制的Web伺服器建立靜態IP到SGT對映](#)

[建立憑證驗證設定檔](#)

[從之前使用證書身份驗證配置檔案建立身份源序列](#)

[為無線使用者 \( 員工和顧問 \) 分配適當的SGT](#)

[將SGT分配給實際裝置 \( 交換機和WLC \)](#)

[定義SGACL以指定出口策略](#)

[在思科ISE的TrustSec策略矩陣上實施您的ACL](#)

[在Catalyst交換機上配置TrustSec](#)

[將交換機配置為在Catalyst交換機上使用Cisco TrustSec for AAA](#)

[在RADIUS伺服器下配置PAC金鑰以向思科ISE驗證交換機](#)

[配置CTS憑證以向思科ISE驗證交換機](#)

[在Catalyst交換機上全局啟用CTS](#)

[為受限制的Web伺服器進行靜態IP到SGT對映 \( 可選 \)](#)

[驗證Catalyst交換機上的TrustSec](#)

[在WLC上配置TrustSec](#)

[配置和驗證WLC在思科ISE中增加為RADIUS裝置](#)

[配置並驗證WLC在思科ISE中增加為TrustSec裝置](#)

[啟用WLC的PAC配置](#)

[在WLC上啟用TrustSec](#)

[驗證是否已在WLC上提供PAC](#)

[將CTS環境資料從思科ISE下載到WLC](#)

[在流量上啟用SGACL下載和實施](#)

[為WLC和存取點分配SGT 2 \(TrustSec Devices\)](#)

[在WLC上啟用內聯標籤](#)

[在Catalyst交換機上啟用內聯標籤](#)

### [驗證](#)

---

## 簡介

本文檔介紹如何在帶有身份服務引擎的Catalyst交換機和無線LAN控制器上配置和驗證TrustSec。

## 必要條件

思科建議您瞭解以下主題：

- Cisco TrustSec (CTS)元件的基礎知識
- Catalyst交換機的CLI配置基礎知識
- 思科無線LAN控制器(WLC)的GUI組態基本知識
- 體驗身份服務引擎(ISE)配置

## 需求

您必須在網路中部署思科ISE，終端使用者在連線到無線或有線網路時必須使用802.1x ( 或其他方法 ) 向思科ISE進行身份驗證。Cisco ISE在他們的流量認證到您的無線網路後，為其分配一個安全組標籤(SGT)。

在我們的示例中，終端使用者被重定向到Cisco ISE自帶裝置(BYOD)門戶，並調配了證書，以便他們在完成BYOD門戶步驟後，可以使用可擴展身份驗證協定-傳輸層安全(EAP-TLS)安全地訪問無線網路。

## 採用元件

本文件中的資訊是以下列硬體與軟體版本為依據：

- 思科身分辨識服務引擎，版本2.4
- Cisco Catalyst 3850交換器3.7.5E版
- Cisco WLC 8.5.120.0版
- 本地模式下的Cisco Aironet無線存取點

在部署Cisco TrustSec之前，驗證您的Cisco Catalyst交換機和/或Cisco WLC+AP型號+軟體版本支援：

- TrustSec/安全組標籤
- 內嵌標籤 ( 如果沒有，您可以使用SXP而非內嵌標籤 )
- 靜態IP到SGT對映 ( 如果需要 )
- 靜態子網到SGT的對映 ( 如果需要 )
- 靜態VLAN到SGT對映 ( 如果需要 )

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

### 網路圖表

## Topology



在本示例中，如果資料包來自顧問，則WLC將其標籤為SGT 15；如果資料包來自員工，則標籤為+SGT 7。

如果資料包是從SGT 15到SGT 8（顧問無法訪問標籤為SGT 8的伺服器），交換機將拒絕這些資料包。

如果資料包是從SGT 7到SGT 8，交換機允許這些資料包（員工可以訪問標籤為SGT 8的伺服器）。

### 目標

允許任何人訪問GuestSSID。

允許顧問訪問EmployeeSSID，但訪問受限。

允許員工以完全訪問許可權訪問EmployeeSSID。

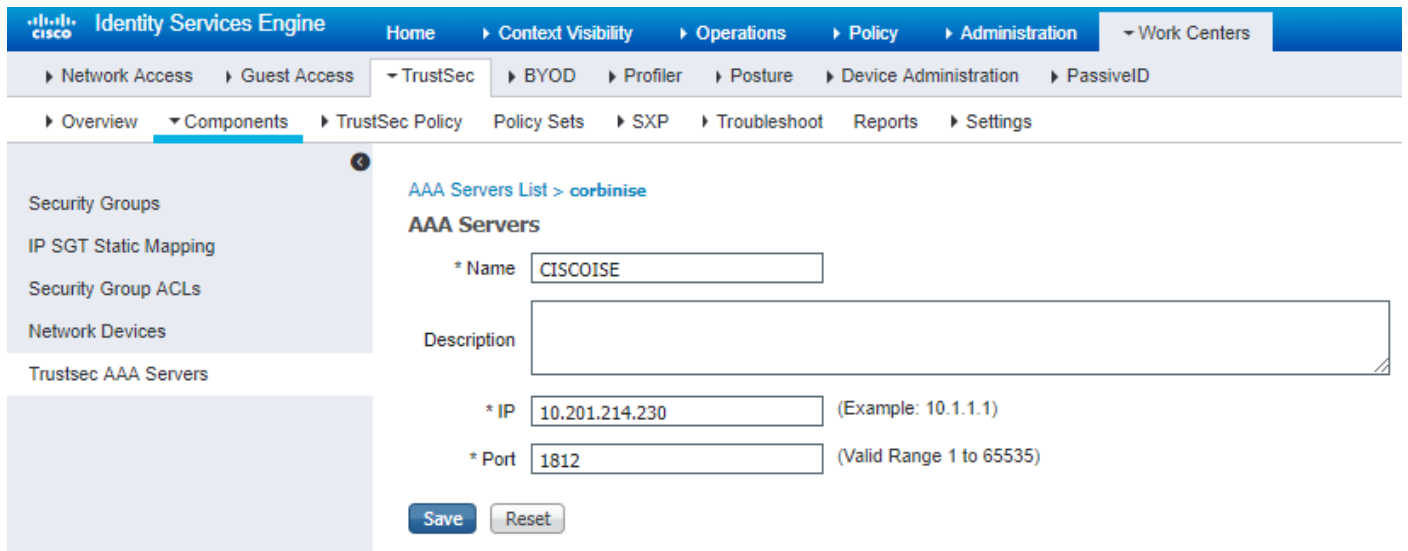
裝置	IP 位址	VLAN		
ISE	10.201.214.230	463		
Catalyst交換器	10.201.235.102	1115		
WLC	10.201.214.229	463		
存取點	10.201.214.138	455		
名稱	使用者名稱	AD組	SG	SGT
傑森·史密夫	jsmith	顧問	BYOD顧問	15
莎莉·史密夫	ssmith	員工	自帶裝置員工	7
不適用	不適用	不適用	TrustSec裝置	2

### 組態

在ISE上配置TrustSec

<h3>1 Prepare</h3> <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>	<h3>2 Define</h3> <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>	<h3>3 Go Live &amp; Monitor</h3> <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>
---	--	--

## 將Cisco ISE配置為TrustSec AAA伺服器



## 配置並驗證交換機是否增加為Cisco ISE中的RADIUS裝置

Identity Services Engine 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 List > CatalystSwitch

Network Devices

Default Device

Device Security Settings

\* 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

## 配置並驗證WLC在思科ISE中增加為TrustSec裝置

輸入您的SSH登入憑證。這使思科ISE能夠將靜態IP到SGT對映部署到交換機。  
您將在Work Centers > TrustSec > Components > IP SGT Static Mappings下的思科ISE Web GUI中建立如下：

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:

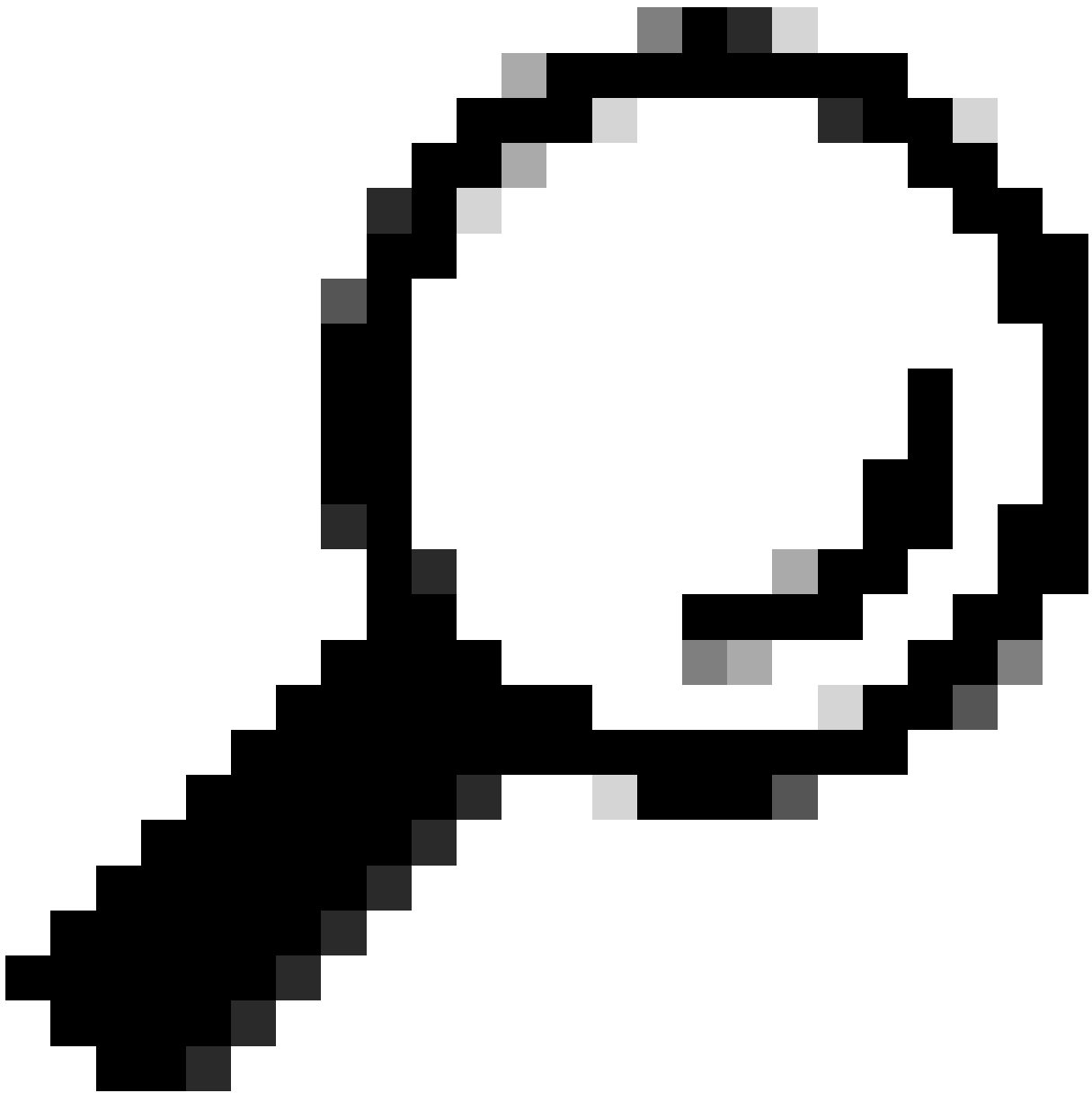
---

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

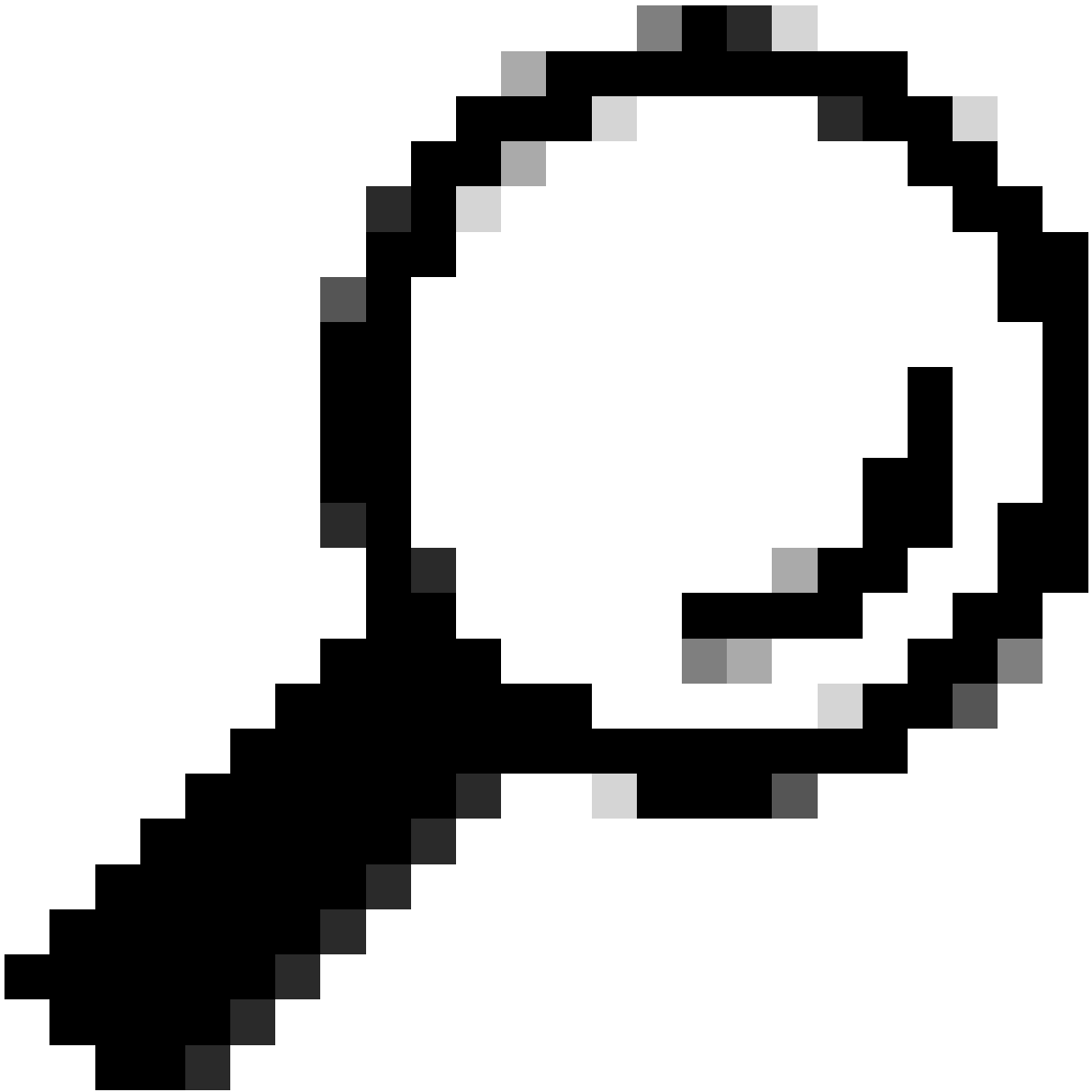
Issue Date:

Expiration Date:

Issued By:



提示：如果您尚未在Catalyst交換機上配置SSH，可以使用本指南：[如何在Catalyst交換機上配置安全外殼\(SSH\)](#)。



提示：如果您不想啟用思科ISE透過SSH訪問Catalyst交換機，則可以用CLI在Catalyst交換機上建立靜態IP到SGT對映（在此步驟中顯示）。

---

驗證預設TrustSec設定以確保這些設定可接受（可選）





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

為無線使用者建立安全組標籤

為BYODconsultants建立安全組- SGT 15

為BYOD員工建立安全組- 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	

為受限制的Web伺服器建立靜態IP到SGT對映

對網路中未使用MAC身份驗證繞行(MAB)、802.1x、配置檔案等向Cisco ISE進行身份驗證的任何其他IP地址或子網執行此操作。

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

建立憑證驗證設定檔

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

從之前使用證書身份驗證配置檔案建立身份源序列

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

為無線使用者 ( 員工和顧問 ) 分配適當的SGT

名稱	使用者名稱	AD組	SG	SGT
傑森·史密夫	jsmith	顧問	BYOD顧問	15
莎莉·史密夫	ssmith	員工	自帶裝置員工	7
不適用	不適用	不適用	TrustSec裝置	2

The screenshot shows the Cisco ISE Policy Sets configuration for 'EmployeeSSID'. It includes a table of Policy Sets and two sections for Authentication and Authorization Policies. Blue arrows point to specific configuration elements: 'BYOD\_Identity\_Sequence' in the Authentication Policy 'DetIX', and 'BYODconsultants' and 'BYODEmployees' in the Authorization Policy rules.

將SGT分配給實際裝置 ( 交換機和WLC )

The screenshot shows the Cisco ISE Network Device Authorization configuration page. It displays a table of Network Device Authorization rules. A rule named 'Tag\_TrustSec\_Devices' is defined with the condition 'If DEVICE:Device Type equals to All Device Types' and the security group 'TrustSec\_Devices'.

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

定義SGACL以指定出口策略

允許顧問訪問任何外部位置，但限制內部：

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

```

允許員工在外部和內部的任何位置訪問：

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

```

允許其他裝置訪問基本服務（可選）：

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

將所有終端使用者重定向至Cisco ISE (用於BYOD門戶重定向)。請勿包含DNS、DHCP、ping或WebAuth流量，因為這些流量無法進入思科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

```

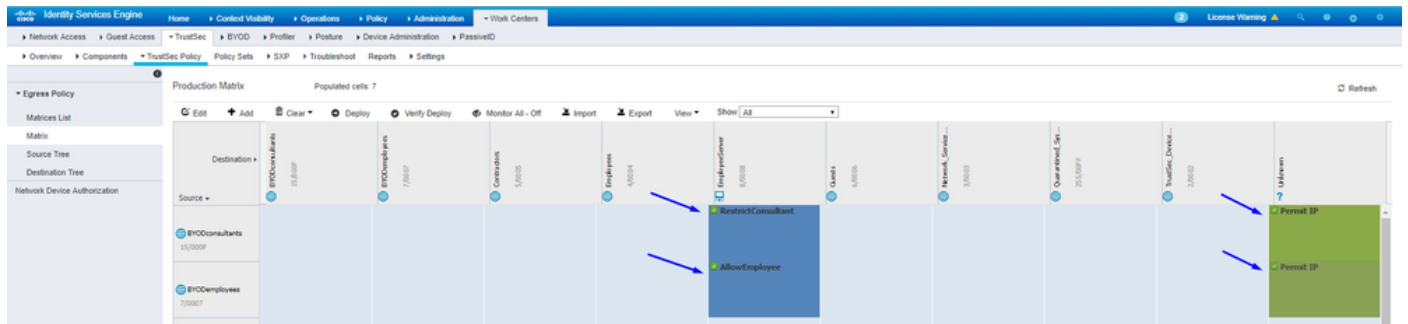
Submit Cancel

在思科ISE的TrustSec策略矩陣上實施您的ACL

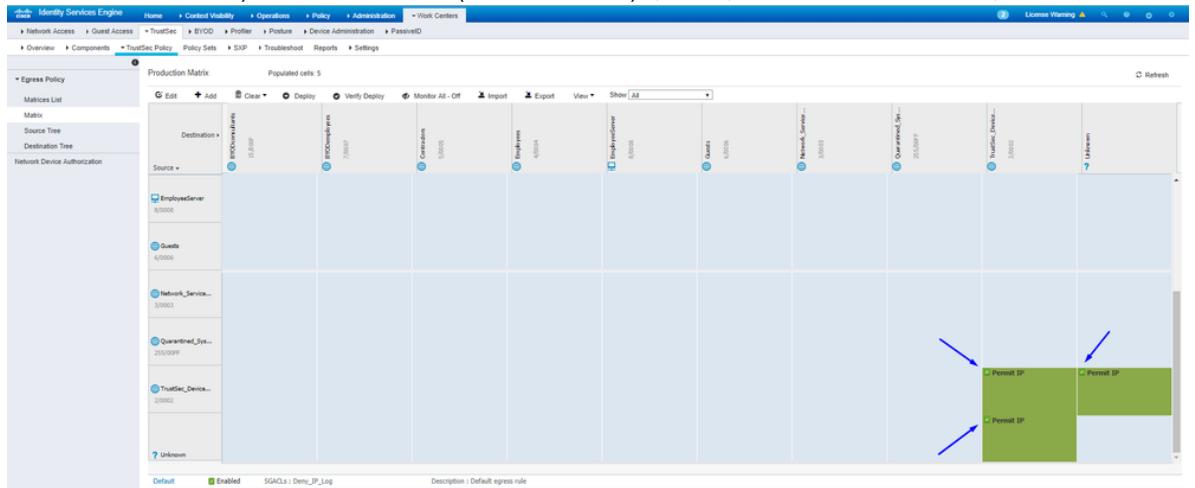
允許顧問在任意位置訪問外部，但限制內部Web伺服器，例如<https://10.201.214.132>



允許員工在任何地方訪問外部，並允許內部Web伺服器：



允許管理流量 (SSH、HTTPS和CAPWAP) 進出網路上的裝置 (交換機和WLC)，這樣，在部署Cisco TrustSec後，您不會丟失



SSH或HTTPS訪問：

啟用思科ISE以 Allow Multiple SGACLs：

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

### TrustSec Matrix Settings

- Allow Multiple SGACLs ⓘ
- Allow Monitoring ⓘ
- Show SGT Numbers ⓘ

Appearance Settings Custom Theme ⓘ

Set In Cell ⓘ	Color	Pattern
Permit	<span style="background-color: #6aa84f; border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>	<span style="border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>
Deny	<span style="background-color: #c0392b; border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>	<span style="border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>
SGACLs	<span style="background-color: #3498db; border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>	<span style="border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>

Default for Matrix (Inherited) ⓘ	Color	Pattern
Permit	<span style="background-color: #d4edda; border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>	<span style="border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>
Deny	<span style="background-color: #f8d7da; border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>	<span style="border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>
SGACLs	<span style="background-color: #d1ecf1; border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>	<span style="border: 1px solid #ccc; display: inline-block; width: 15px; height: 15px;"></span>

Status Icons ⓘ

- Enabled
- Disabled
- Monitor

Save Reset

點選Cisco ISE右上角的Push，將您的配置下推到您的裝置。您稍後也需要再次執行此動作：

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.**

在Catalyst交換機上配置TrustSec

將交換機配置為在Catalyst交換機上使用Cisco TrustSec for AAA



提示：本文檔假定在配置此處所示之前，您的無線使用者已透過Cisco ISE成功完成自帶裝置(BYOD)。

---

在此之前，已經配置了以粗體顯示的命令（以便自帶裝置無線與ISE配合使用）。

**<#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
```



注意：PAC金鑰必須與您在 **Administration > Network Devices > Add Device > RADIUS Authentication Settings** 部分中指定的RADIUS共用金鑰相同。

---

```
<#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
```

在RADIUS伺服器下配置PAC金鑰以向思科ISE驗證交換機

```
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  ⓘ

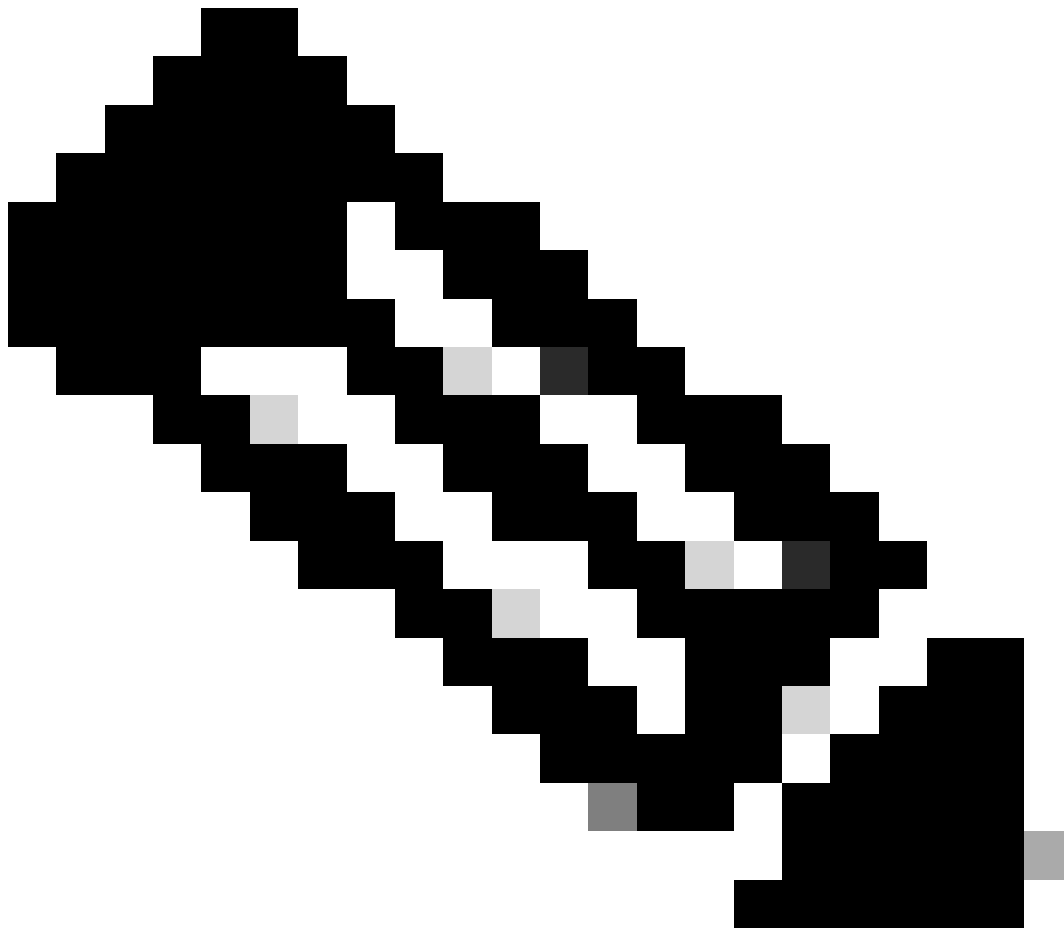
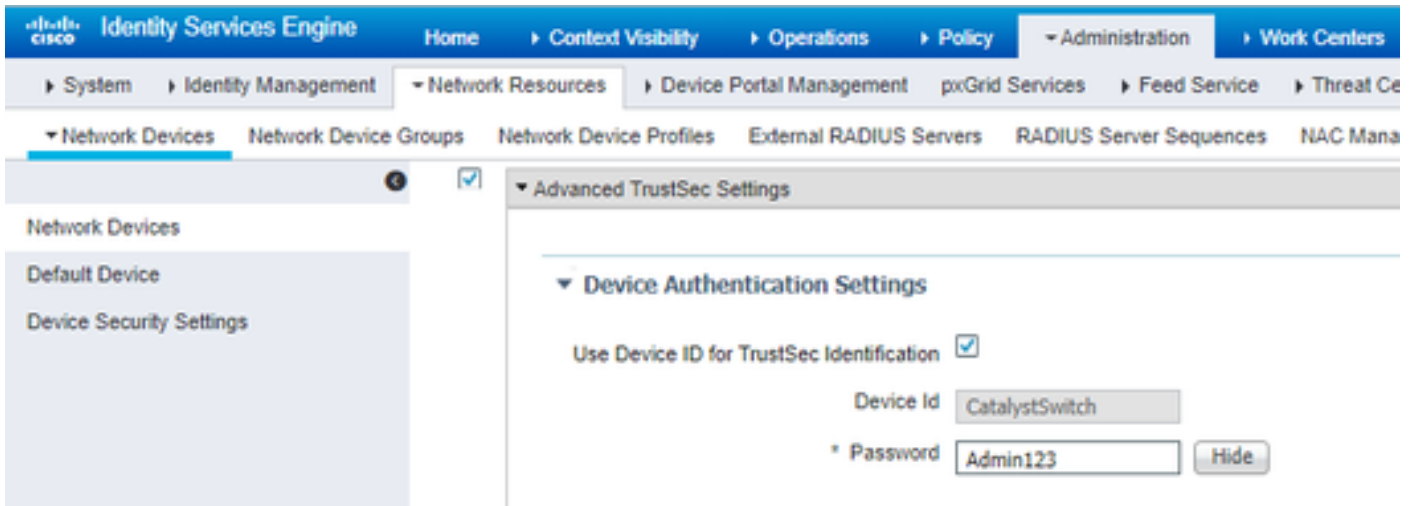


**注意：** PAC金鑰必須與您在Cisco ISE的 **Administration > Network Devices > Add Device > RADIUS Authentication Settings** 部分下指定的RADIUS共用金鑰相同（如螢幕截圖所示）。

---

配置CTS憑證以向思科ISE驗證交換機

CatalystSwitch#cts credentials id CatalystSwitch password Admin123



注意：CTS憑證必須與您在CTS憑證中指定的裝置ID + 密碼相同，必須與您在思科ISE的Administration > Network Devices > Add Device > Advanced TrustSec Settings部分（在螢幕截圖中顯示的）中指定的裝置ID + 密碼相同。



---

然後，重新整理您的PAC，使其再次連線思科ISE：

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

在Catalyst交換機上全局啟用CTS

```
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)
```

為受限制的Web伺服器進行靜態IP到SGT對映（可選）

該受限制的Web伺服器從未通過ISE進行身份驗證，因此您必須使用交換機CLI或ISE Web GUI對其進行手動標籤，這只是Cisco中眾多Web伺服器之一。

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

驗證Catalyst交換機上的TrustSec

```
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

在WLC上配置TrustSec

配置和驗證WLC在思科ISE中增加為RADIUS裝置

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 > 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  Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls

CoA Port 2083 Set To Default

Issuer CA of ISE Certificates for CoA Select if required (optional)

DNS Name

配置並驗證 WLC 在思科 ISE 中增加為 TrustSec 裝置

此步驟使思科 ISE 能夠部署到 WLC 的靜態 IP 到 SGT 對映。您在上一步的工作中心 > TrustSec > 元件 > IP SGT 靜態對映的 Cisco ISE Web GUI 中建立這些對映。

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



注意：我們會使用此 Device Id 命令，然後 Password 在後面的步驟(在 WLC Web UI 中的 Security > TrustSec > General)中使用此命令。

---

啟用WLC的PAC配置

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 Management	<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



在WLC上啟用TrustSec

### 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





**注意：**CTS Device Id 和 Password 必須與您在思科ISE的Administration > Network Devices > Add Device > Advanced TrustSec Settings Device Id Password 和部分中指定的相同。

---

驗證是否已在WLC上提供PAC

當您按一下Refresh Env Data ( 在此步驟中執行此操作 ) 後，您會看到WLC成功調配了PAC：



**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	<a href="#">Clear PAC</a>
PAC A-ID	ef2e1222e67eb4630a8b22d1ff0216c1	
PAC Lifetime	Wed Nov 21 00:01:07 2018	

IPSec:  Enable

將CTS環境資料從思科ISE下載到WLC

按一下Refresh Env Data後，WLC將下載您的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

在流量上啟用SGACL下載和實施

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

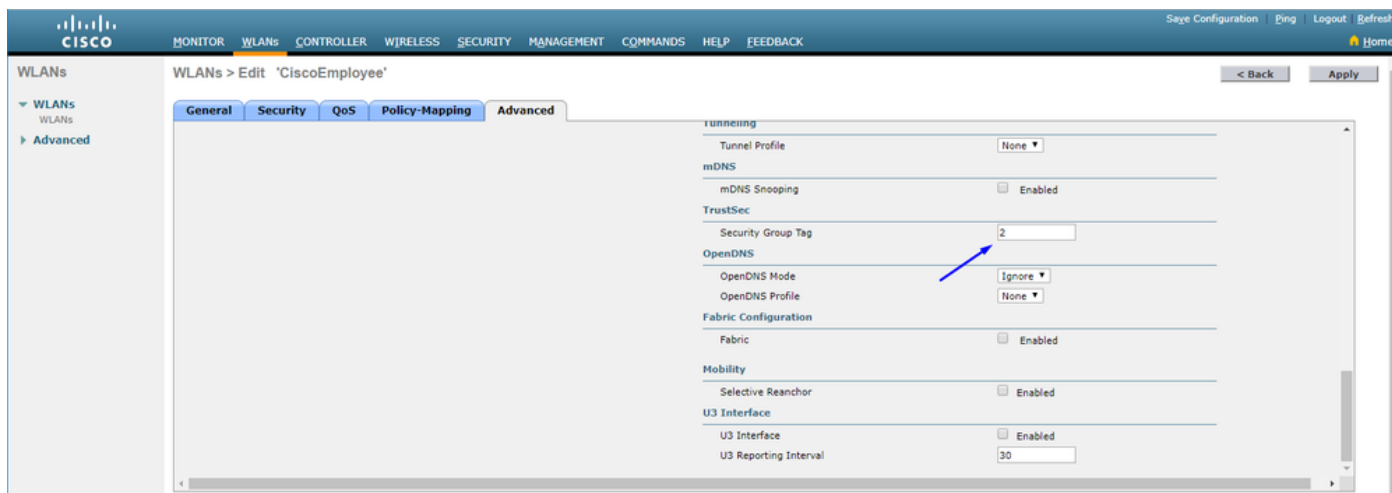
CTS Override

Sgacl Enforcement

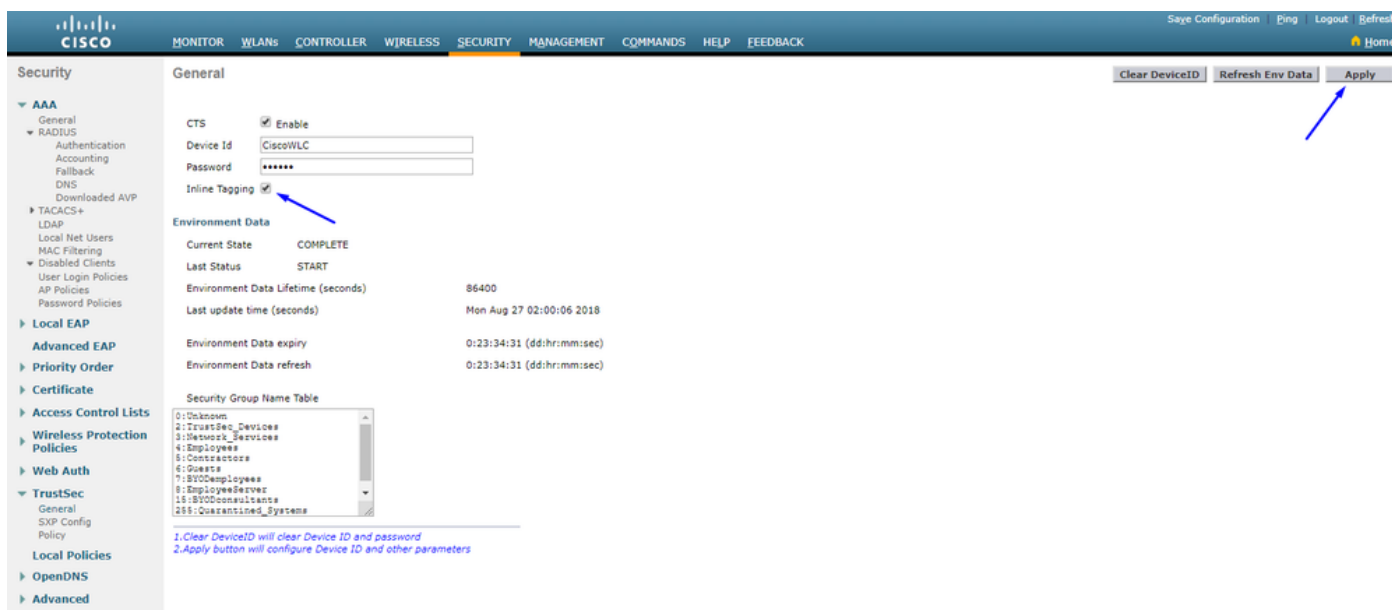
1. Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)  
 2. SXPv4(Listener/Speaker/Both) is supported in Flex, Flex+bridge AP (Applicable to 11ac AP)

為WLC和存取點分配SGT 2 (TrustSec\_Devices)

為WLC+WLAN指定值為2的SGT (TrustSec\_Devices) , 以允許透過交換機與WLC + AP之間的流量 ( SSH、HTTPS和CAPWAP ) 。



在WLC上啟用內聯標籤



在「 Wireless > Access Points > Global Configuration 向下滾動」下，選擇「 TrustSec Config」。

The screenshot displays the Cisco Catalyst configuration interface for 'All APs TrustSec Configuration'. The left sidebar shows the navigation menu with 'Global Configuration' selected. The main area shows the following configuration options:

- TrustSec**
  - 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
- Peer Config**
  - Peer IP Address:
  - Password: Default ▼
  - Local Mode: Speaker ▼
  - ADD**

Below the Peer Config section, there is a table header:

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

在Catalyst交換機上啟用內聯標籤

<#root>

CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

CatalystSwitch(config-if)#description goestoWLC

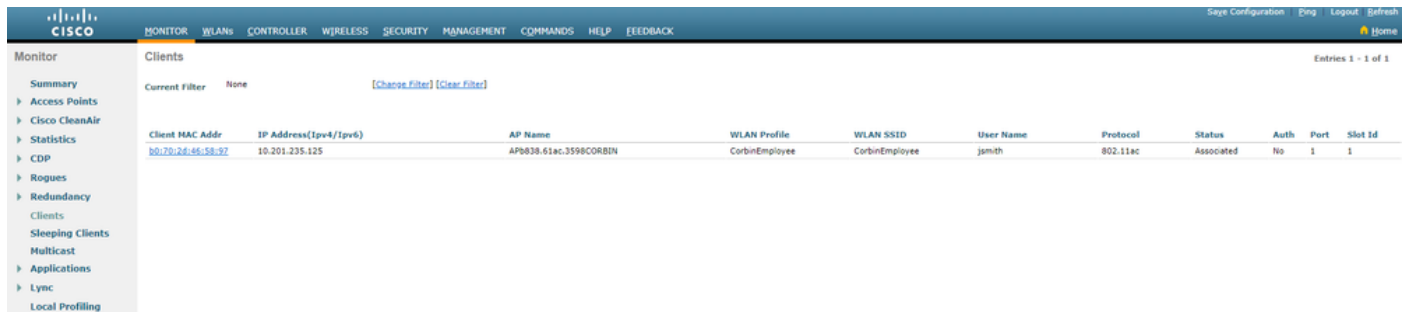
CatalystSwitch(config-if)#switchport trunk native vlan 15

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
```

## 驗證



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

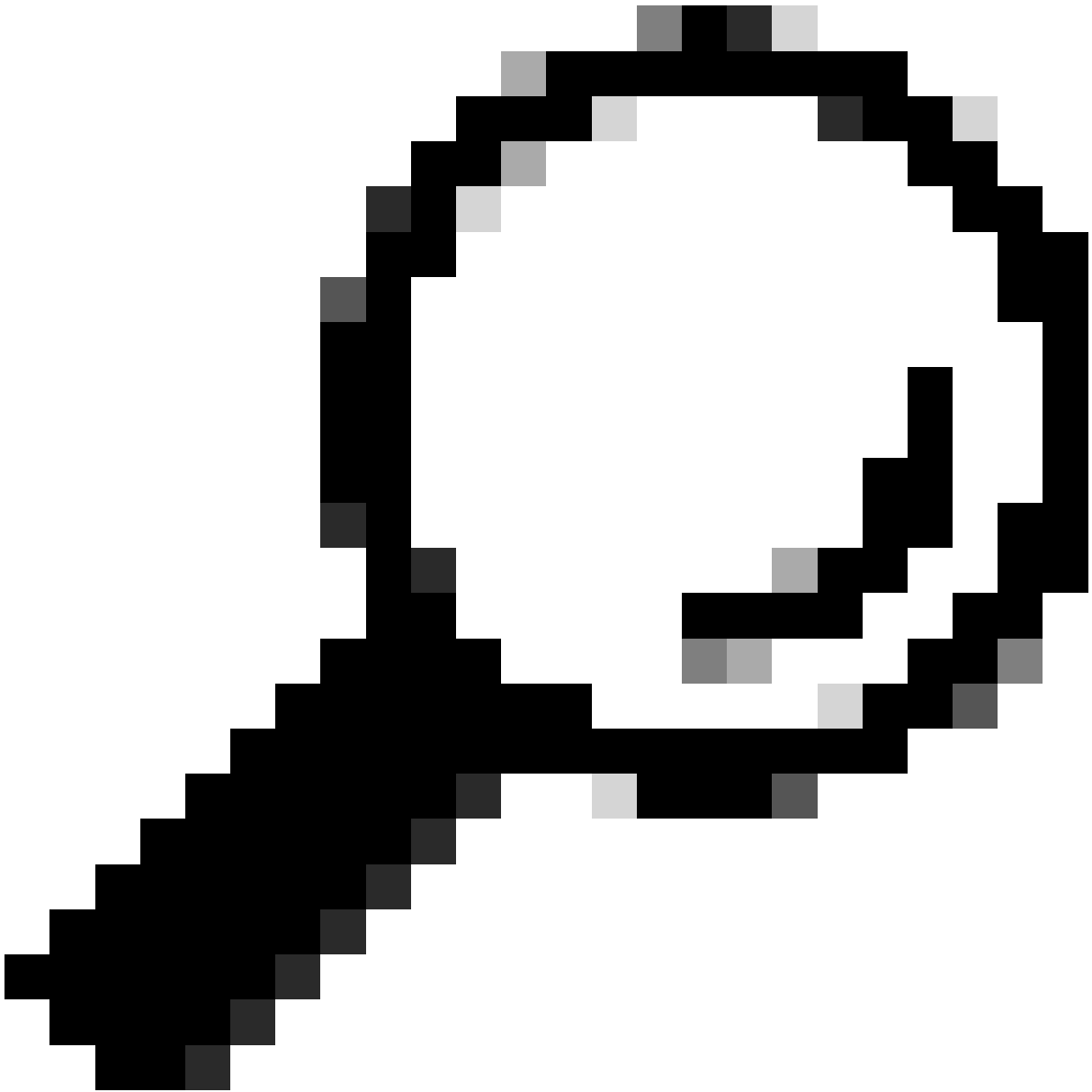
CatalystSwitch#show platform acl counters hardware | 包括SGACL

輸出IPv4 SGACL丟棄(454) : 10個幀

出口IPv6 SGACL丟棄(455) : 0個幀

輸出IPv4 SGACL信元丟棄(456) : 0個幀

出口IPv6 SGACL信元丟棄(457) : 0幀



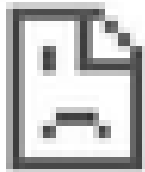
提示：如果改用Cisco ASR、Nexus或Cisco ASA，此處列出的文檔可幫助驗證您的SGT標籤是否已實施：[TrustSec故障排除指南](#)。

---

使用使用者名稱jsmith密碼Admin123向無線進行身份驗證-您在交換機中遇到deny ACL：



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





## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。