使用ISE配置TrustSec (SGT)（内联标记）

目录

简介

本文档介绍如何使用身份服务引擎在Catalyst交换机和无线LAN控制器上配置和验证TrustSec。

先决条件

Cisco 建议您了解以下主题：

- Cisco TrustSec (CTS)组件的基础知识
- Catalyst交换机的CLI配置基础知识
- 思科无线局域网控制器(WLC)的GUI配置基础知识
- 使用身份服务引擎(ISE)配置的体验

要求

您的网络中必须部署思科ISE，最终用户在连接到无线或有线网络时必须使用802.1x（或其他方法）向思科ISE进行身份验证。思科ISE会在其流量向您的无线网络进行身份验证后为其分配安全组标记(SGT)。

在我们的示例中，最终用户被重定向到思科ISE自带设备(BYOD)门户，并调配了证书，因此他们可以在完成BYOD门户步骤后，使用可扩展身份验证协议-传输层安全(EAP-TLS)安全地访问无线网络。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- 思科身份服务引擎，版本2.4
- Cisco Catalyst 3850交换机，版本3.7.5E
- Cisco WLC版本8.5.120.0
- 本地模式下的Cisco Aironet无线接入点

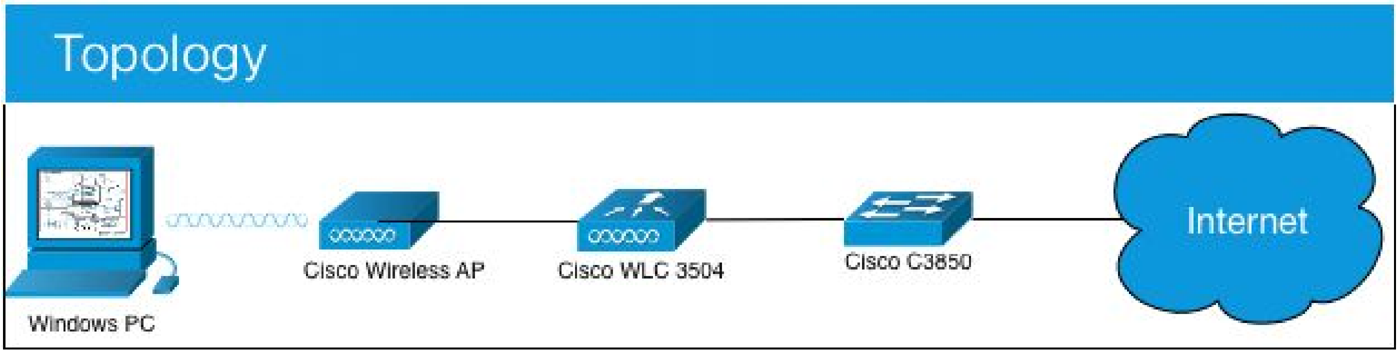
在部署Cisco TrustSec之前，验证您的Cisco Catalyst交换机和/或Cisco WLC+AP型号+软件版本是否支持以下功能：

- TrustSec/安全组标记
- 内联标记（如果不是，您可以使用SXP而不是内联标记）
- 静态IP到SGT映射（如果需要）
- 静态子网到SGT的映射（如果需要）
- 静态VLAN至SGT映射（如果需要）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



在本示例中，如果数据包来自顾问，则WLC将其标记为SGT 15；如果数据包来自员工，则标记为+ SGT 7。

如果数据包从SGT 15到SGT 8（顾问无法访问标记为SGT 8的服务器），交换机将拒绝这些数据包。

如果数据包从SGT 7到SGT 8，交换机允许这些数据包（员工可以访问标记为SGT 8的服务器）。

目标

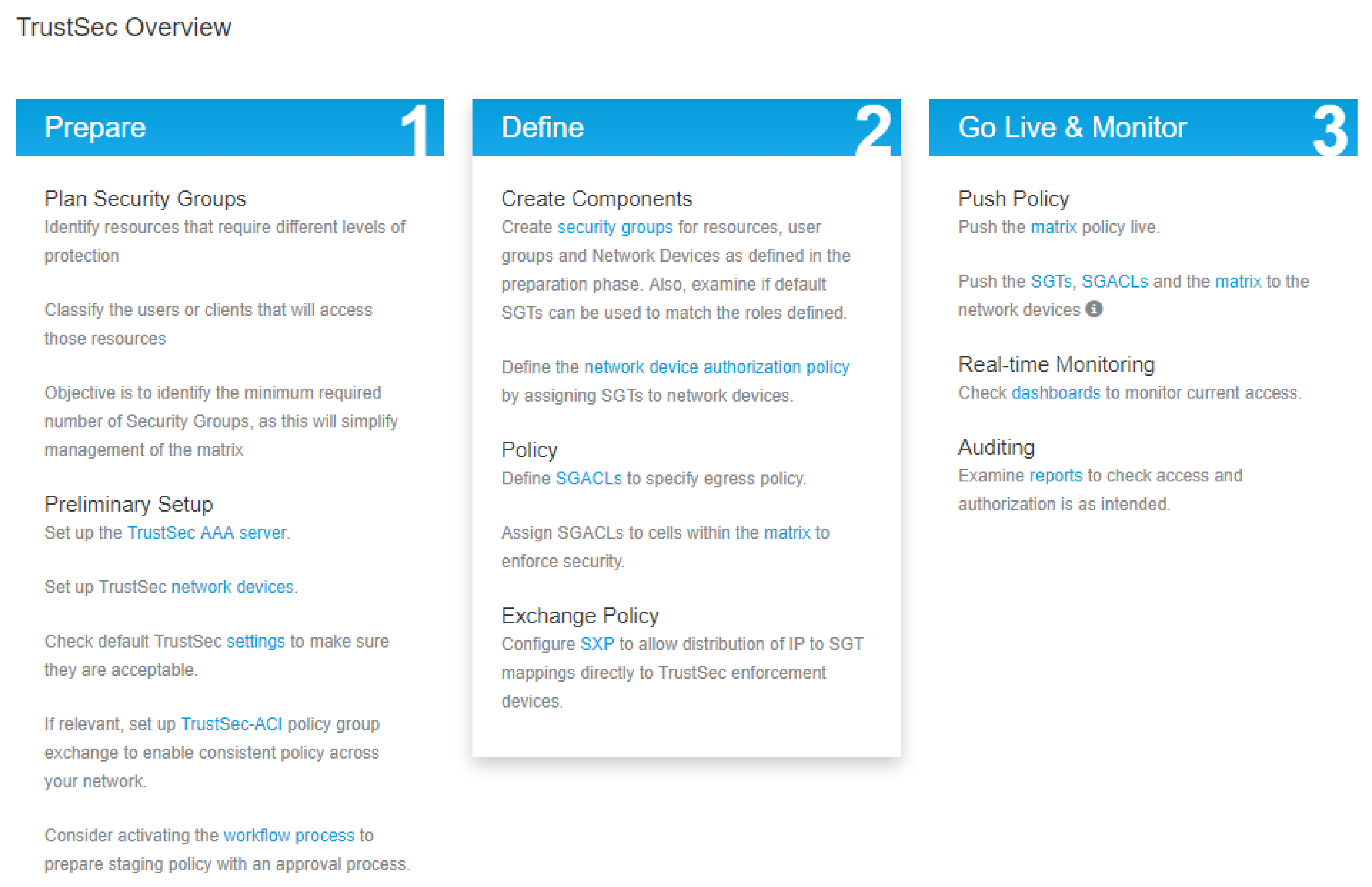
允许任何人访问GuestSSID。
允许顾问访问EmployeeSSID，但访问受限。
允许员工以完全访问权限访问EmployeeSSID。

设备	IP 地址	VLAN
ISE	10.201.214.230	463
Catalyst 交换机	10.201.235.102	1115
WLC	10.201.214.229	463
访问点	10.201.214.138	455

名称	用户名	AD组	SG	SGT
Jason Smith	jsmith	顾问	BYOD顾问	15
莎莉·史密斯	ssmith	员工	BYOD员工	7
不适用	不适用	不适用	TrustSec设备	2

配置

在ISE上配置TrustSec



TrustSec Overview

Prepare 1

Plan Security Groups

Identify resources that require different levels of protection

Classify the users or clients that will access those resources

Objective is to identify the minimum required number of Security Groups, as this will simplify management of the matrix

Preliminary Setup

Set up the TrustSec AAA server.

Set up TrustSec network devices.

Check default TrustSec settings to make sure they are acceptable.

If relevant, set up TrustSec-ACI policy group exchange to enable consistent policy across your network.

Consider activating the workflow process to prepare staging policy with an approval process.

Define 2

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.

Define the network device authorization policy by assigning SGTs to network devices.

Policy

Define SGACLs to specify egress policy.

Assign SGACLs to cells within the matrix to enforce security.

Exchange Policy

Configure SXP to allow distribution of IP to SGT mappings directly to TrustSec enforcement devices.

Go Live & Monitor 3

Push Policy

Push the matrix policy live.

Push the SGTs, SGACLs and the matrix to the network devices

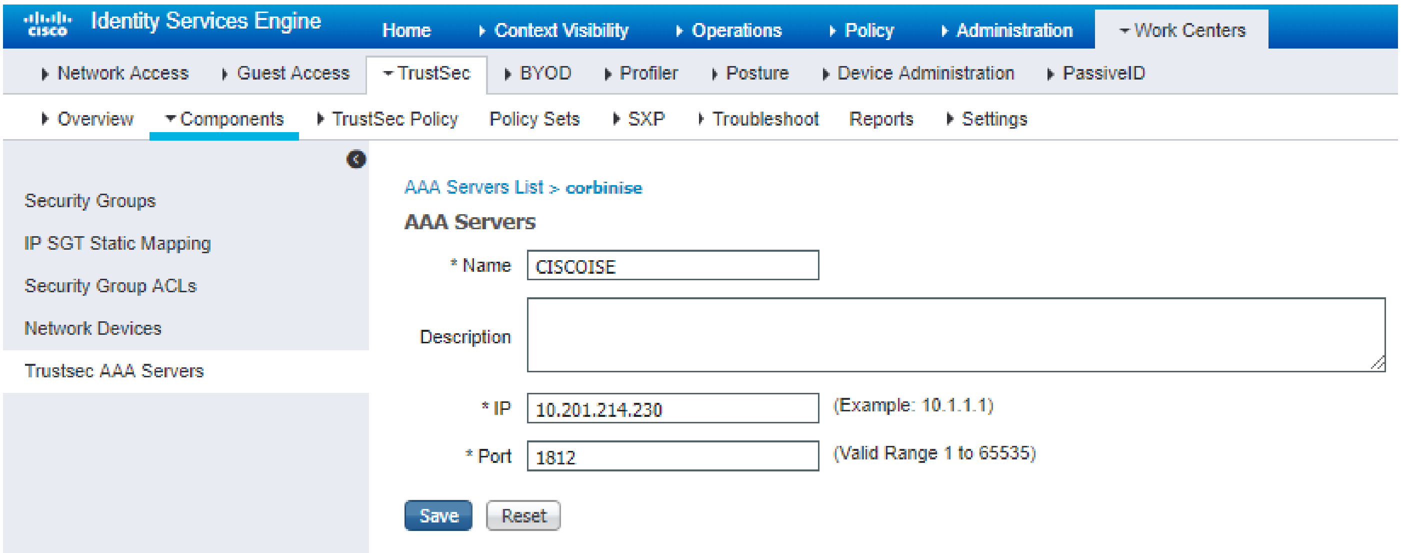
Real-time Monitoring

Check dashboards to monitor current access.

Auditing

Examine reports to check access and authorization is as intended.

将Cisco ISE配置为TrustSec AAA服务器



AAA Servers

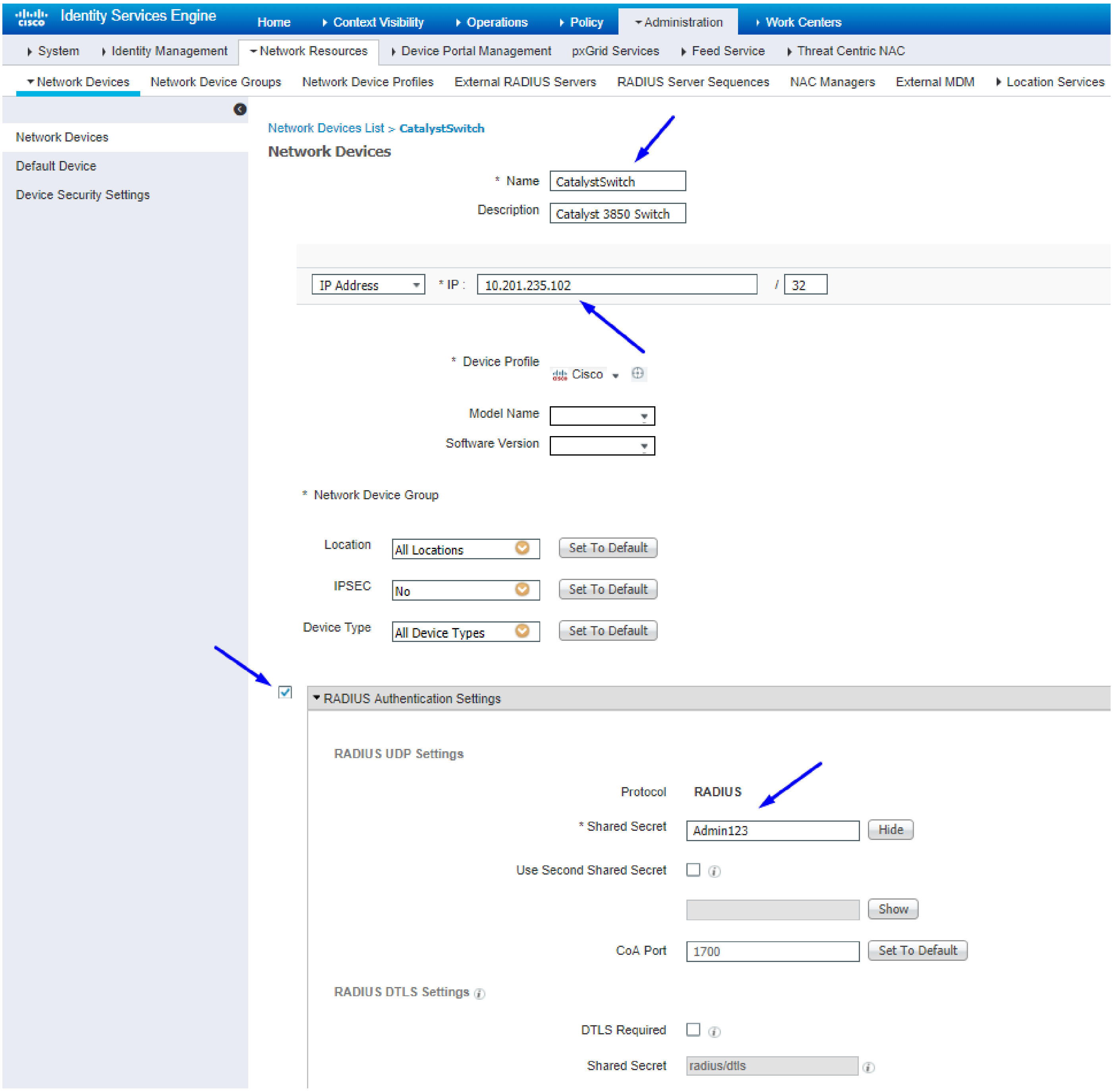
* Name: CISCOISE

Description:

* IP: 10.201.214.230 (Example: 10.1.1.1)

* Port: 1812 (Valid Range 1 to 65535)

配置并验证在Cisco ISE添加为RADIUS设备



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

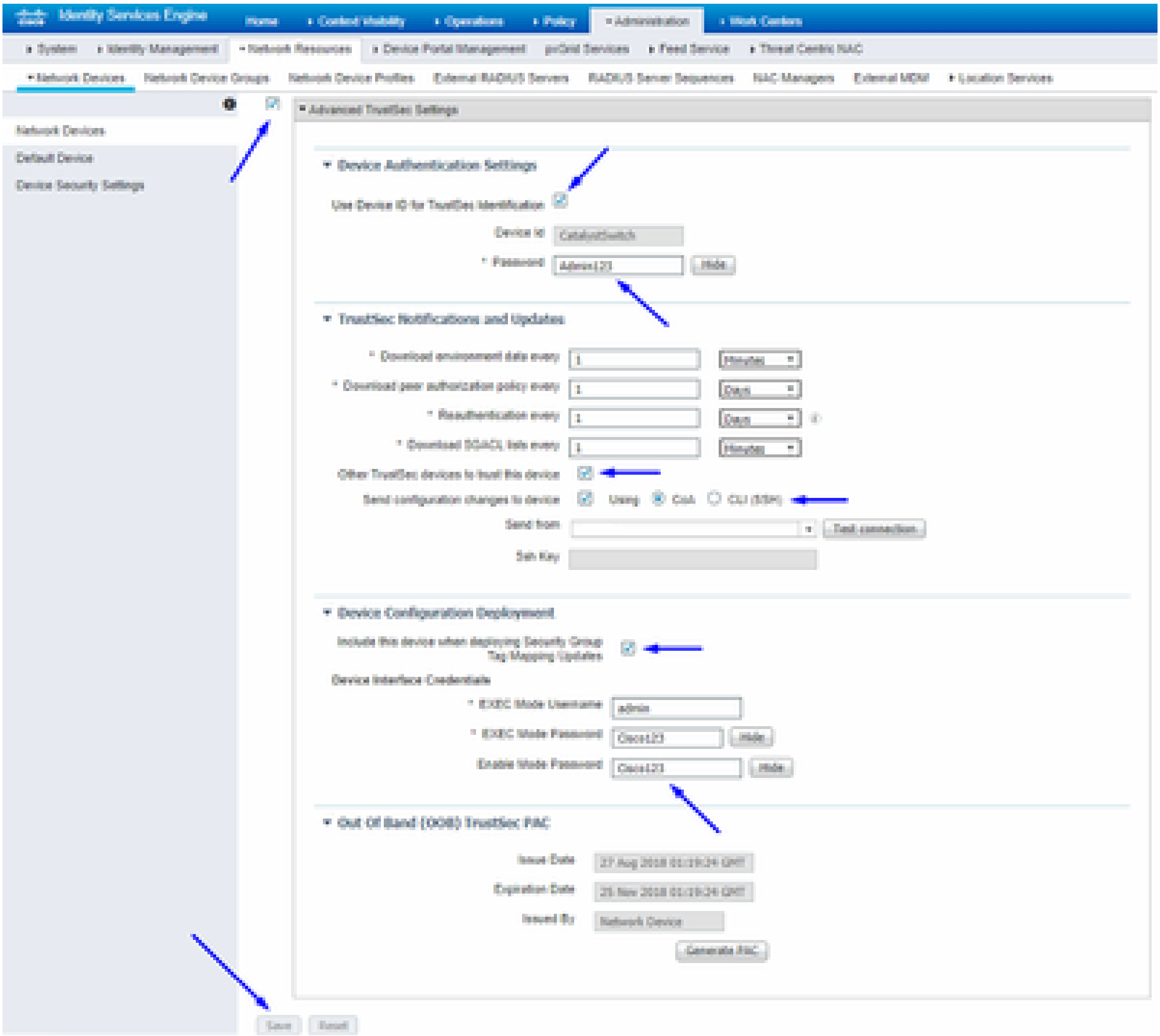
RADIUS DTLS Settings

DTLS Required ☐

Shared Secret: radius/dtls

配置和验证WLC添加为Cisco ISE中的TrustSec设备

输入您的SSH登录凭证。这使Cisco ISE部署静态IP到SGT映射至交换机。
您在Cisco ISE Web GUI中创建这些在Work Centers > TrustSec > Components > IP SGT Static Mappings下，如下所示：



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: CatalystSwitch

* Password: Admin123 [Hide]

TrustSec Notifications and Updates

* Download environment data every: 1 Minutes

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

* Download SGACL lists every: 1 Minutes

Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ● CoA ○ CLI (SSH)

Send from: [Test connection]

Ssh Key:

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username: admin

* EXEC Mode Password: Cisco123 [Hide]

Enable Mode Password: Cisco123 [Hide]

Out Of Band (OOB) TrustSec PAC

Issue Date: 27 Aug 2018 01:19:24 GMT

Expiration Date: 25 Nov 2018 01:19:24 GMT

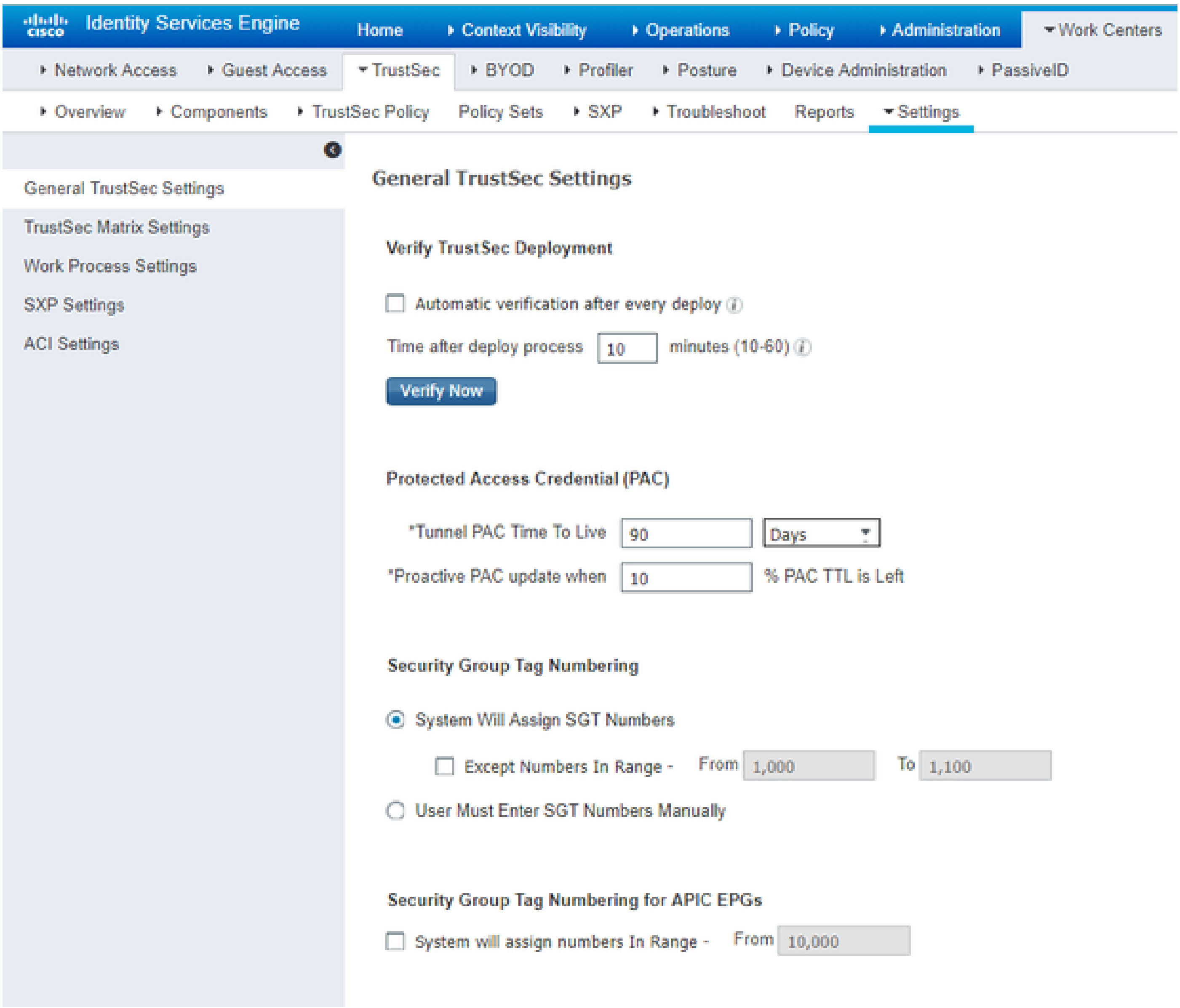
Issued By: Network Device

[Generate PAC]

提示：如果您尚未在Catalyst交换机上配置SSH，可以使用以下指南：如何在Catalyst交换机上配置安全外壳(SSH)。

提示：如果您不希望思科ISE通过SSH访问Catalyst交换机，可以使用CLI在Catalyst交换机上创建静态IP到SGT的映射（在此步骤中显示）。

验证默认TrustSec设置以确保它们可接受（可选）



General TrustSec Settings

Verify TrustSec Deployment

□ Automatic verification after every deploy

Time after deploy process 10 minutes (10-60)

Protected Access Credential (PAC)

*Tunnel PAC Time To Live 90 Days

*Proactive PAC update when 10 % PAC TTL is Left

Security Group Tag Numbering

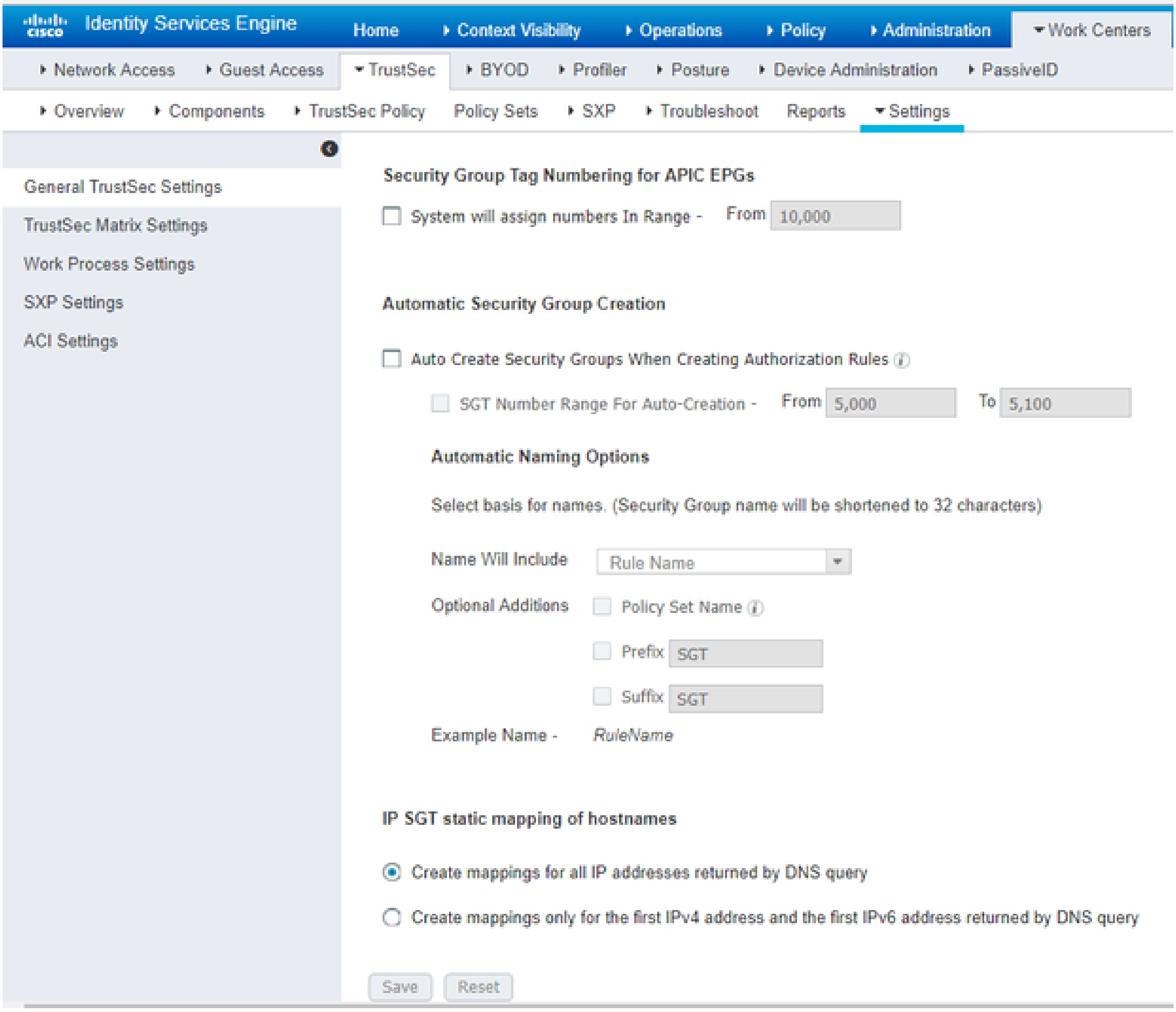
● System Will Assign SGT Numbers

□ Except Numbers In Range - From 1,000 To 1,100

○ User Must Enter SGT Numbers Manually

Security Group Tag Numbering for APIC EPGs

□ System will assign numbers In Range - From 10,000



Security Group Tag Numbering for APIC EPGs

□ System will assign numbers In Range - From 10,000

Automatic Security Group Creation

□ Auto Create Security Groups When Creating Authorization Rules

□ SGT Number Range For Auto-Creation - From 5,000 To 5,100

Automatic Naming Options

Select basis for names. (Security Group name will be shortened to 32 characters)

Name Will Include Rule Name

Optional Additions □ Policy Set Name

□ Prefix SGT

□ Suffix SGT

Example Name - *RuleName*

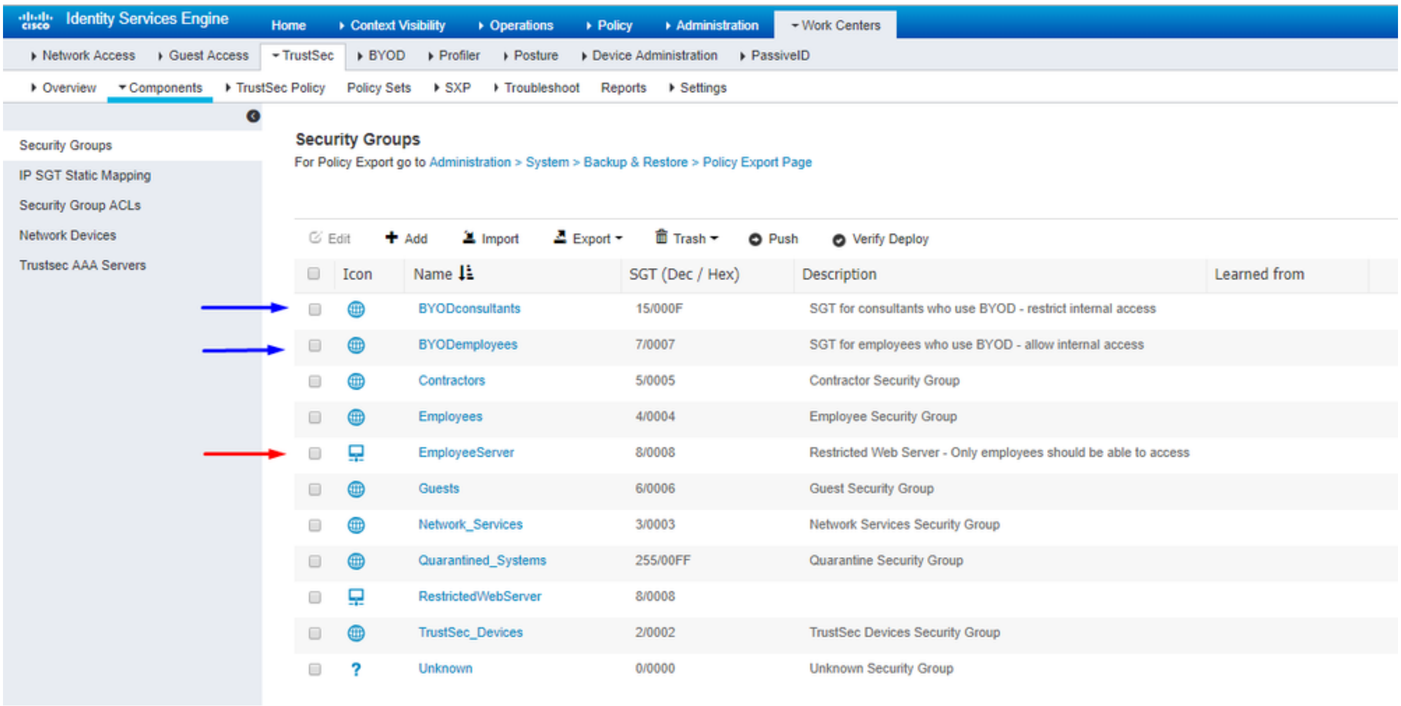
IP SGT static mapping of hostnames

● 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

为无线用户创建安全组标记

为BYOD顾问创建安全组- SGT 15
为BYOD员工创建安全组- SGT 7



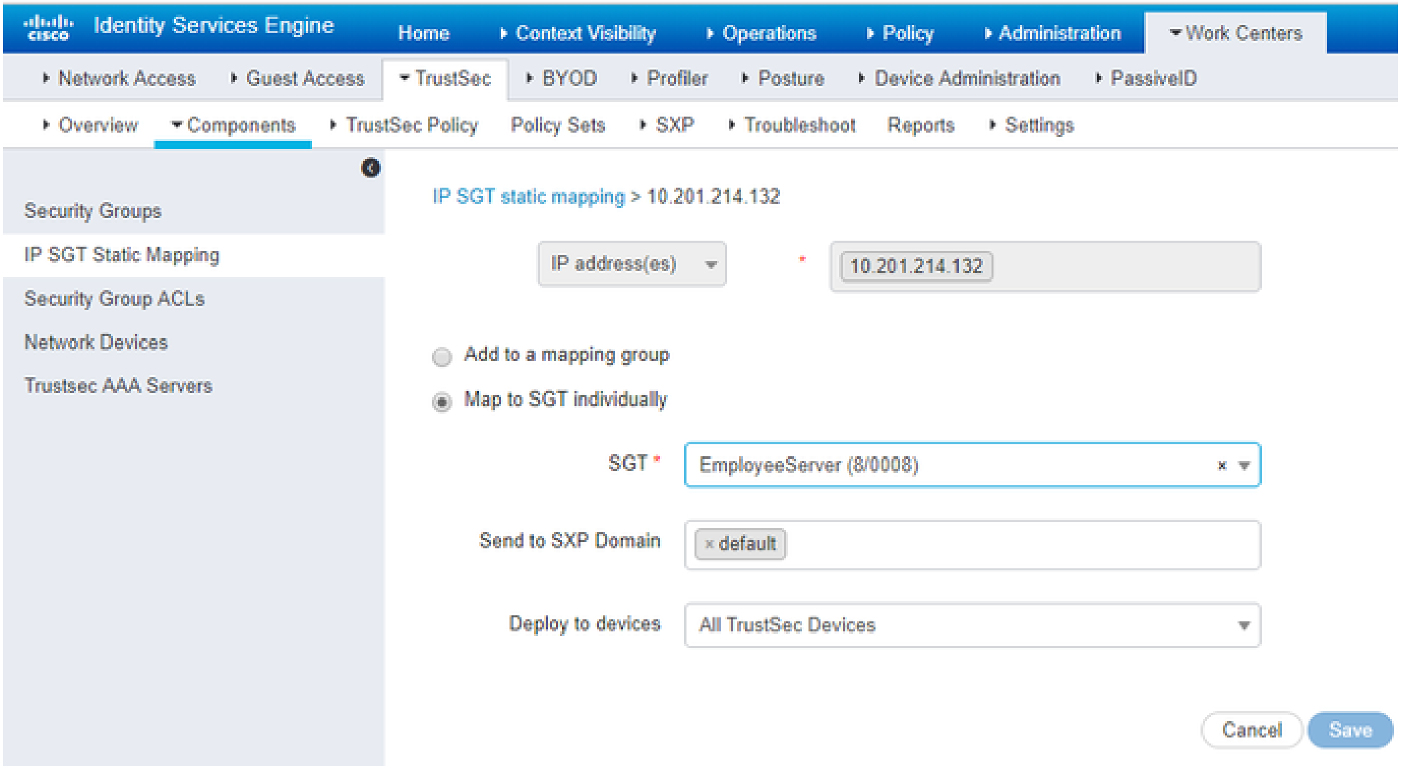
Security Groups

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	

为受限制的Web服务器创建静态IP到SGT映射

对网络中未使用MAC身份验证绕行(MAB)、802.1x、配置文件等向Cisco ISE进行身份验证的任何其他IP地址或子网执行此操作。



IP SGT static mapping > 10.201.214.132

IP address(es) * 10.201.214.132

○ Add to a mapping group

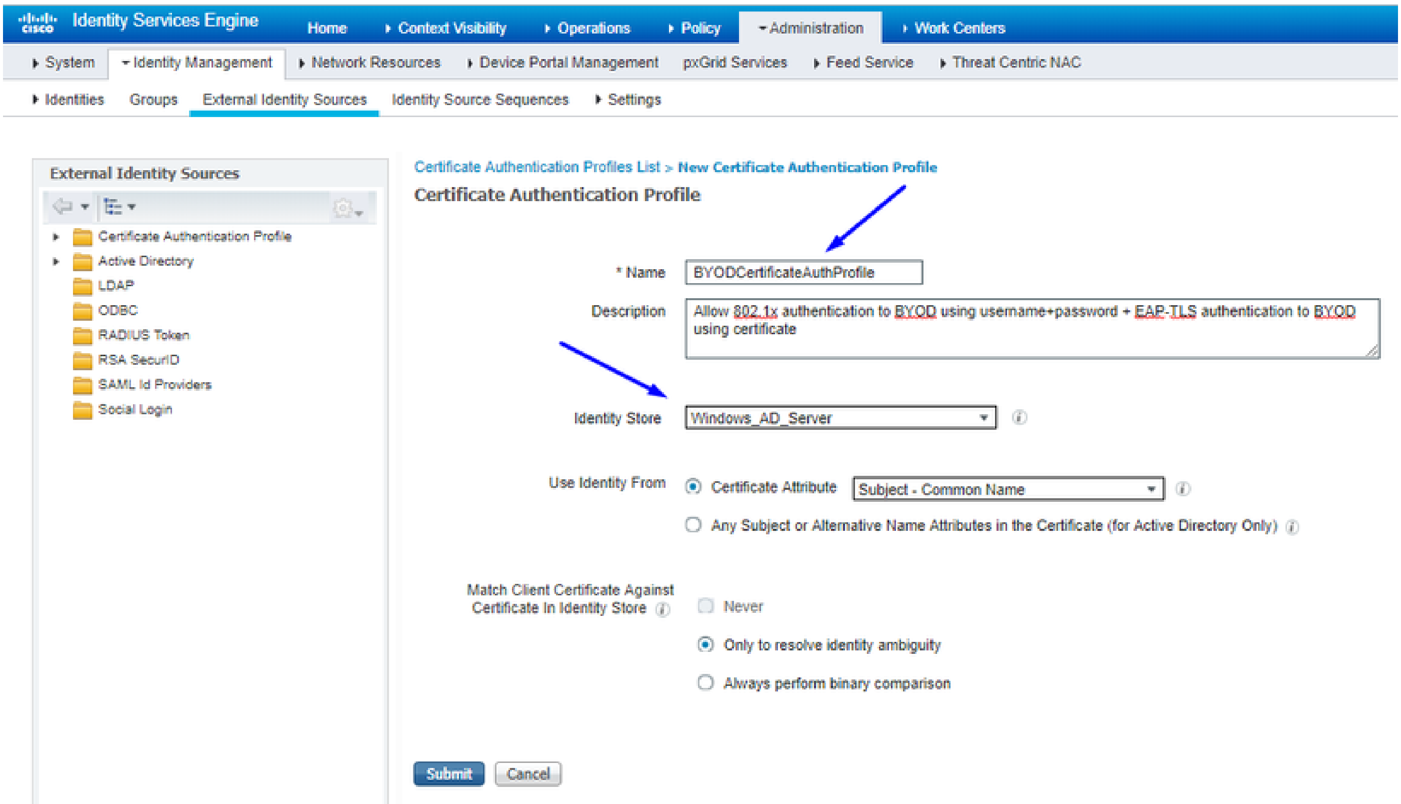
● Map to SGT individually

SGT * EmployeeServer (8/0008)

Send to SXP Domain: default

Deploy to devices: All TrustSec Devices

创建证书身份验证配置文件



Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name: BYODCertificateAuthProfile

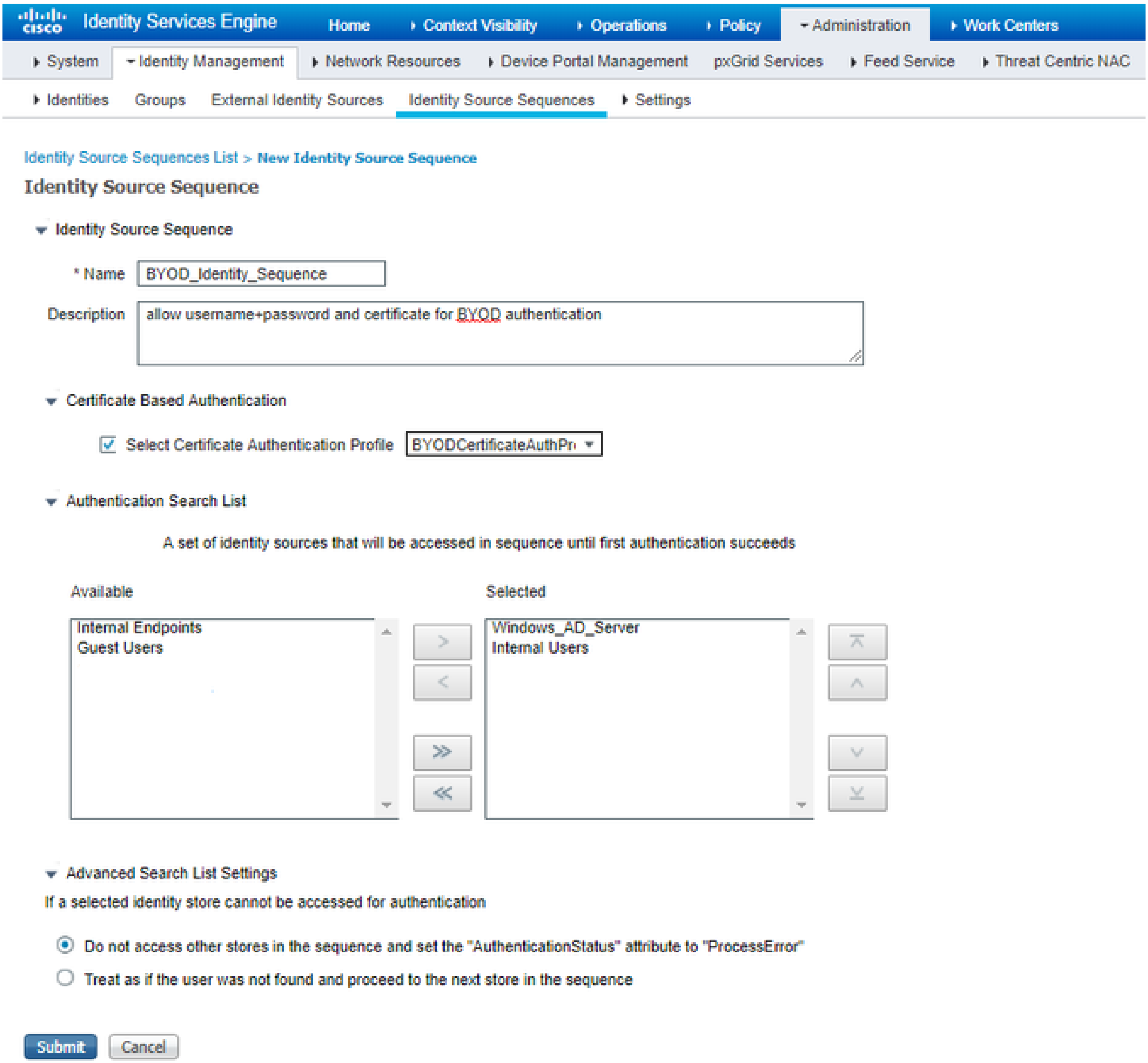
Description: Allow 802.1x authentication to BYOD using username+password + EAP-TLS authentication to BYOD using certificate

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

使用之前的证书身份验证配置文件创建身份源序列



Identity Source Sequences List > New Identity Source Sequence

Identity Source Sequence

▾ Identity Source Sequence

* Name: BYOD_Identity_Sequence

Description: allow username+password and certificate for BYOD authentication

▾ Certificate Based Authentication

☑ Select Certificate Authentication Profile: BYODCertificateAuthPr

▾ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: Internal Endpoints, Guest Users

Selected: Windows_AD_Server, Internal Users

▾ Advanced Search List Settings

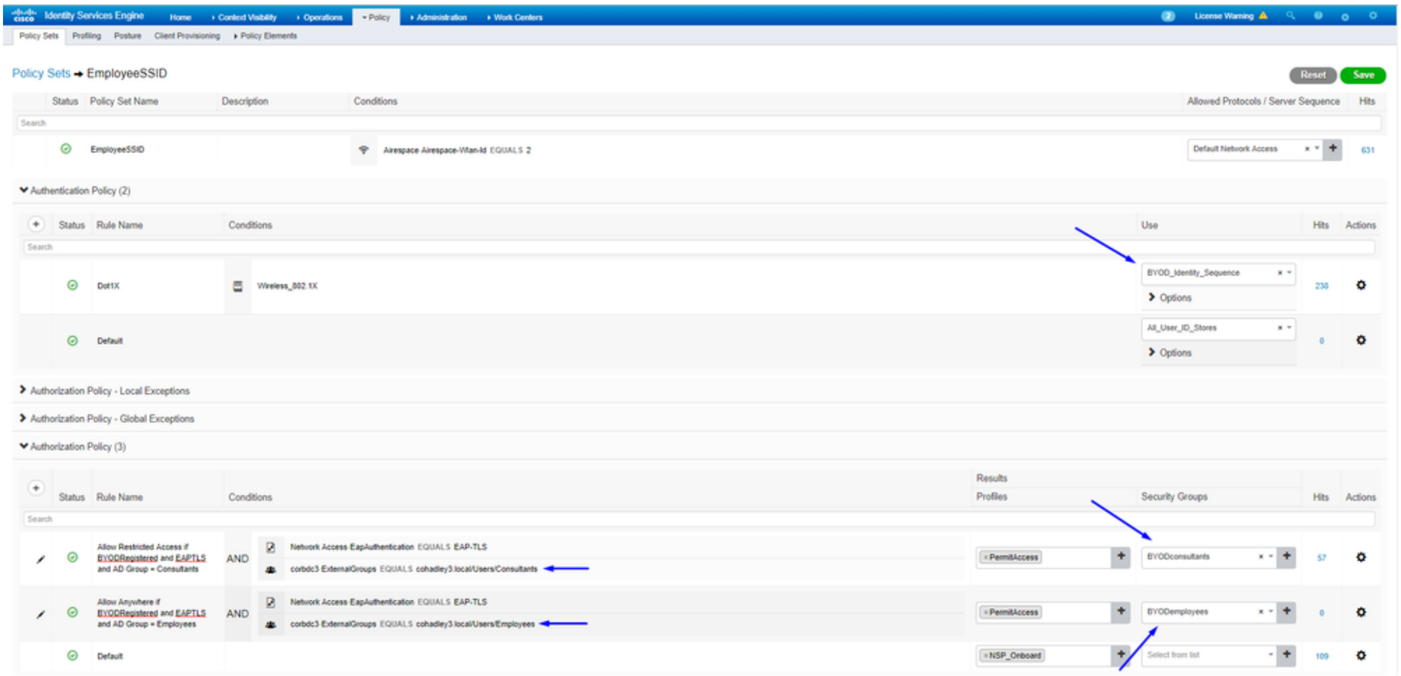
If a selected identity store cannot be accessed for authentication

● 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

为无线用户（员工和顾问）分配适当的SGT

名称	用户名	AD组	SG	SGT
Jason Smith	jsmith	顾问	BYOD顾问	15
莎莉·史密斯	ssmith	员工	BYOD员工	7
不适用	不适用	不适用	TrustSec设备	2



Policy Sets → EmployeeSSID

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	EmployeeSSID		Airespace·Airespace-Wlan-Id EQUALS 2	Default Network Access	631

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Dot1X	Wireless_802.1X	BYOD_Identity_Sequence Options	238	⚙
✓	Default		All_User_ID_Stores Options	0	⚙

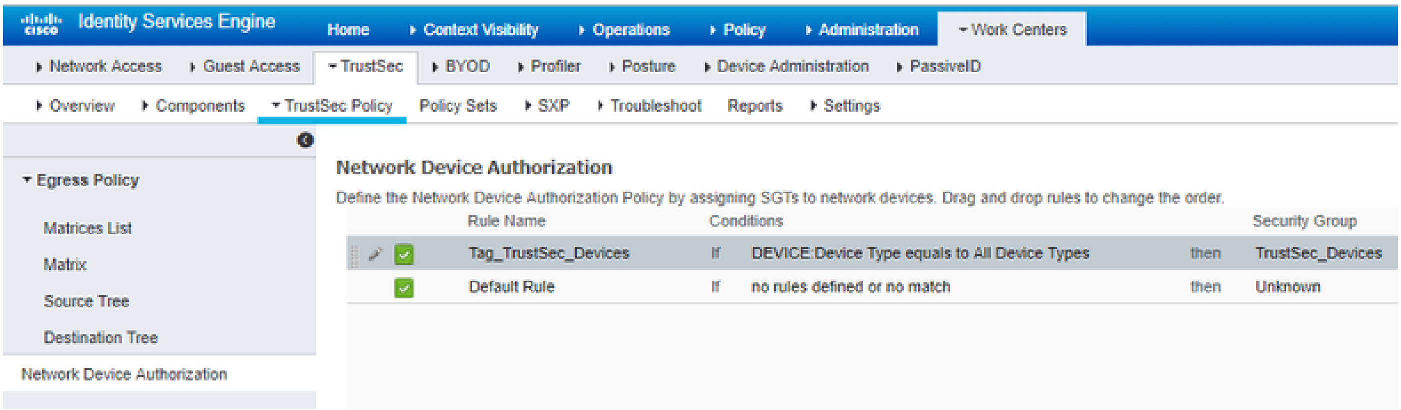
Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name		Conditions	Results Profiles	 Security Groups	Hits	Actions
✓	Allow Restricted Access if BYODRegistered and EAPTLS and AD Group = Consultants	AND	Network Access·EapAuthentication EQUALS EAP-TLS corbdc3·ExternalGroups EQUALS cohadley3.local/Users/Consultants	PermitAccess	BYODconsultants	57	⚙
✓	Allow Anywhere if BYODRegistered and EAPTLS and AD Group = Employees	AND	Network Access·EapAuthentication EQUALS EAP-TLS corbdc3·ExternalGroups EQUALS cohadley3.local/Users/Employees	PermitAccess	BYODemployees	0	⚙
✓	Default			NSP_Onboard	Select from list	109	⚙

将SGT分配到实际设备（交换机和WLC）



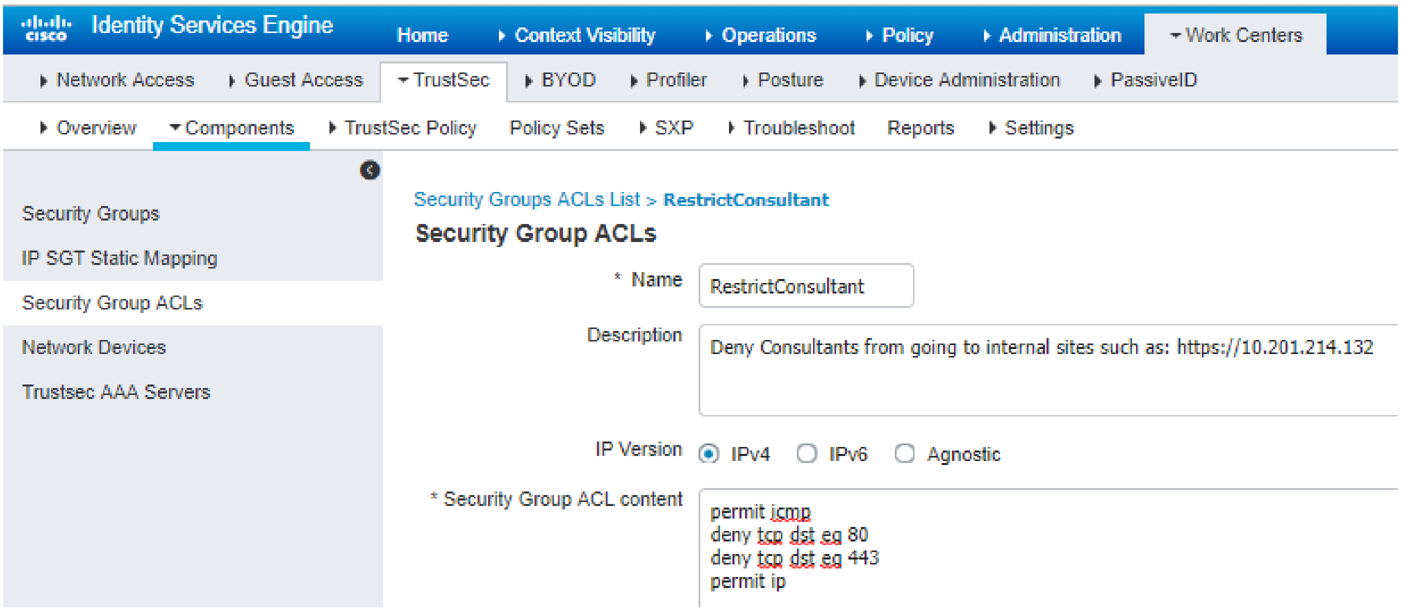
Network Device Authorization

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

定义SGACL以指定出口策略

允许顾问访问外部任何位置，但限制内部：



Security Groups ACLs List > **RestrictConsultant**

Security Group ACLs

* Name: RestrictConsultant

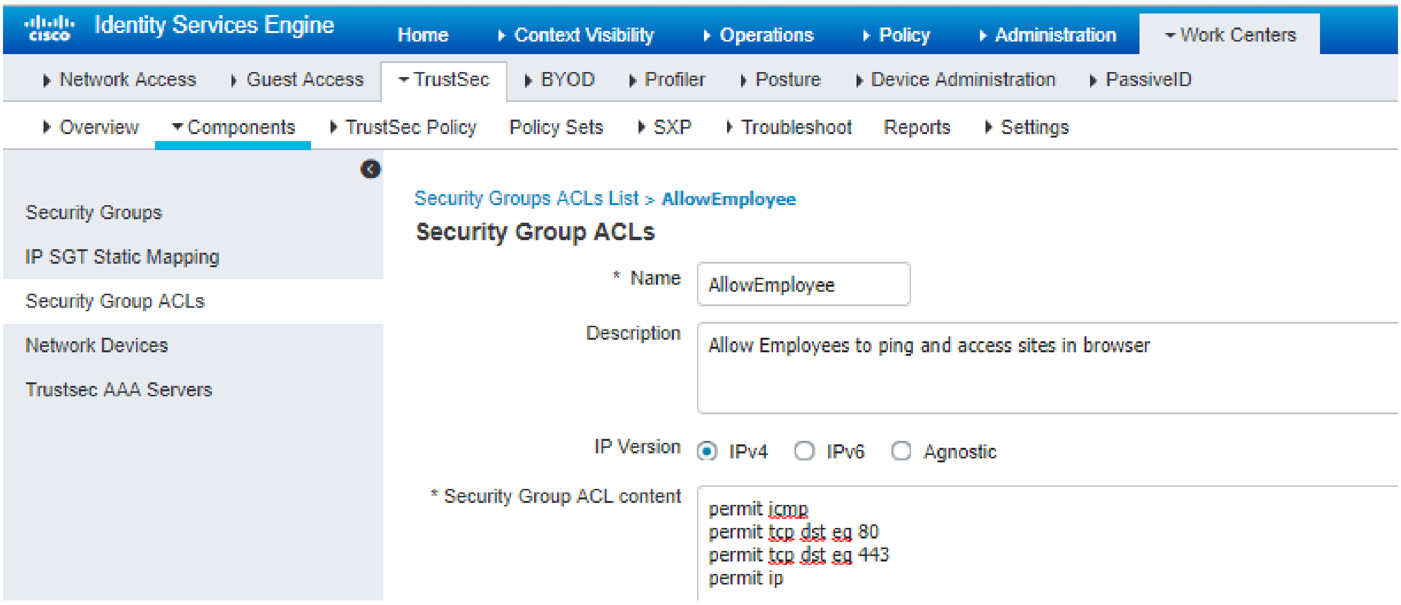
Description: Deny Consultants from going to internal sites such as: https://10.201.214.132

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

```
permit icmp
deny tcp dst eq 80
deny tcp dst eq 443
permit ip
```

允许员工访问任何外部地点和任何内部地点：



Security Groups ACLs List > **AllowEmployee**

Security Group ACLs

* Name: AllowEmployee

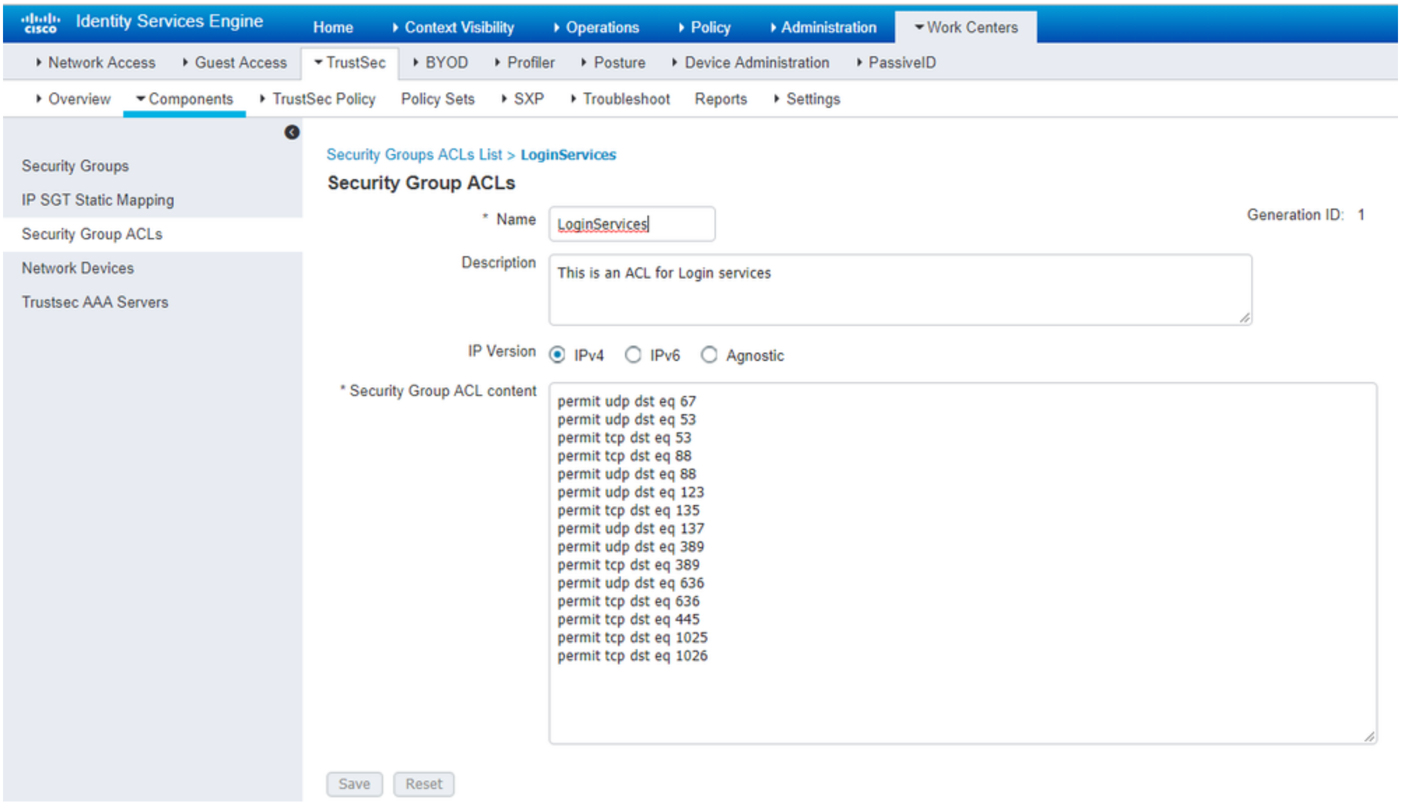
Description: Allow Employees to ping and access sites in browser

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

```
permit icmp
permit tcp dst eq 80
permit tcp dst eq 443
permit ip
```

允许其他设备访问基本服务（可选）：



Security Groups ACLs List > LoginServices

Security Group ACLs

* Name: LoginServices

Generation ID: 1

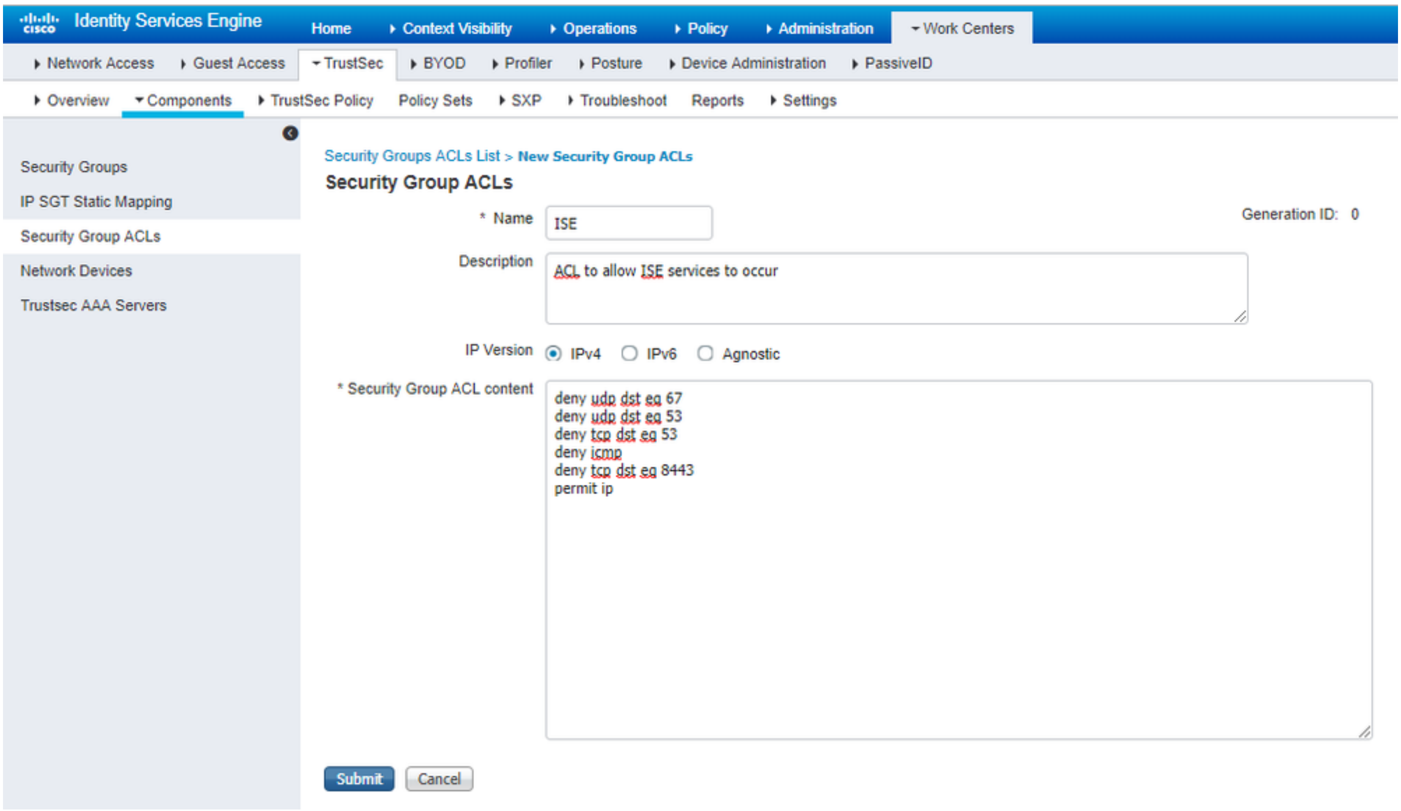
Description: This is an ACL for Login services

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
```

将所有最终用户重定向至Cisco ISE（用于BYOD门户重定向）。不包括DNS、DHCP、ping或WebAuth流量，因为这些流量无法转到Cisco ISE：



Security Groups ACLs List > New Security Group ACLs

Security Group ACLs

* Name: ISE

Generation ID: 0

Description: ACL to allow ISE services to occur

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

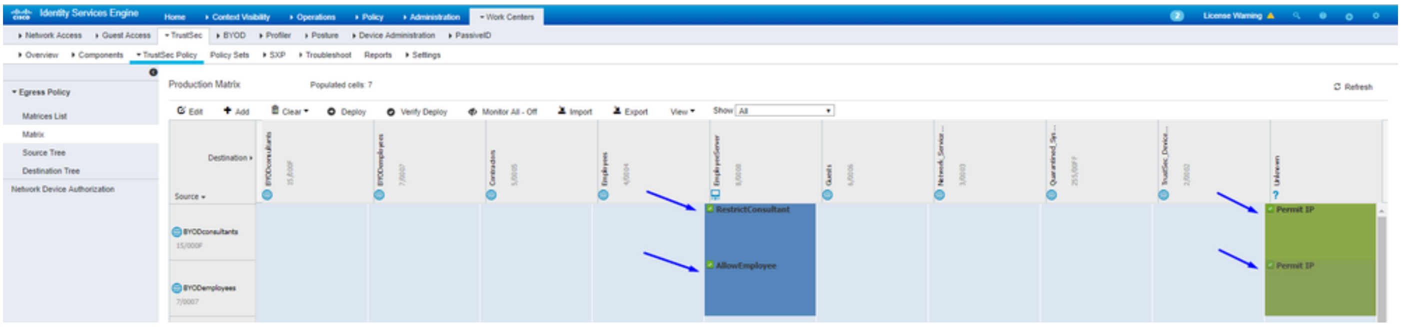
* Security Group ACL content

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

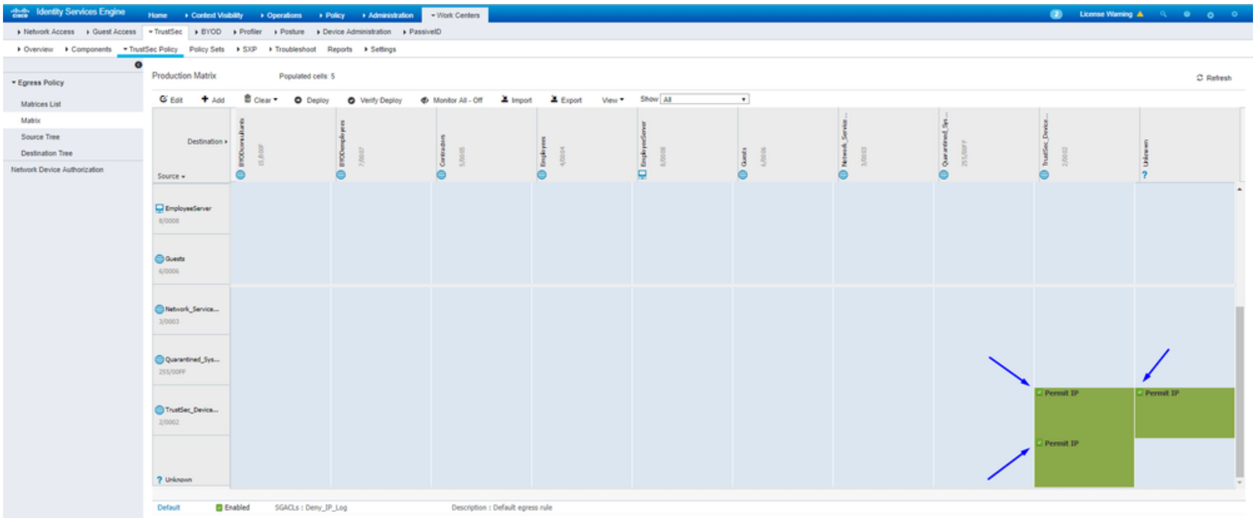
在思科ISE中的TrustSec策略矩阵上实施ACL

允许顾问访问外部任何位置，但限制内部Web服务器，例如https://10.201.214.132

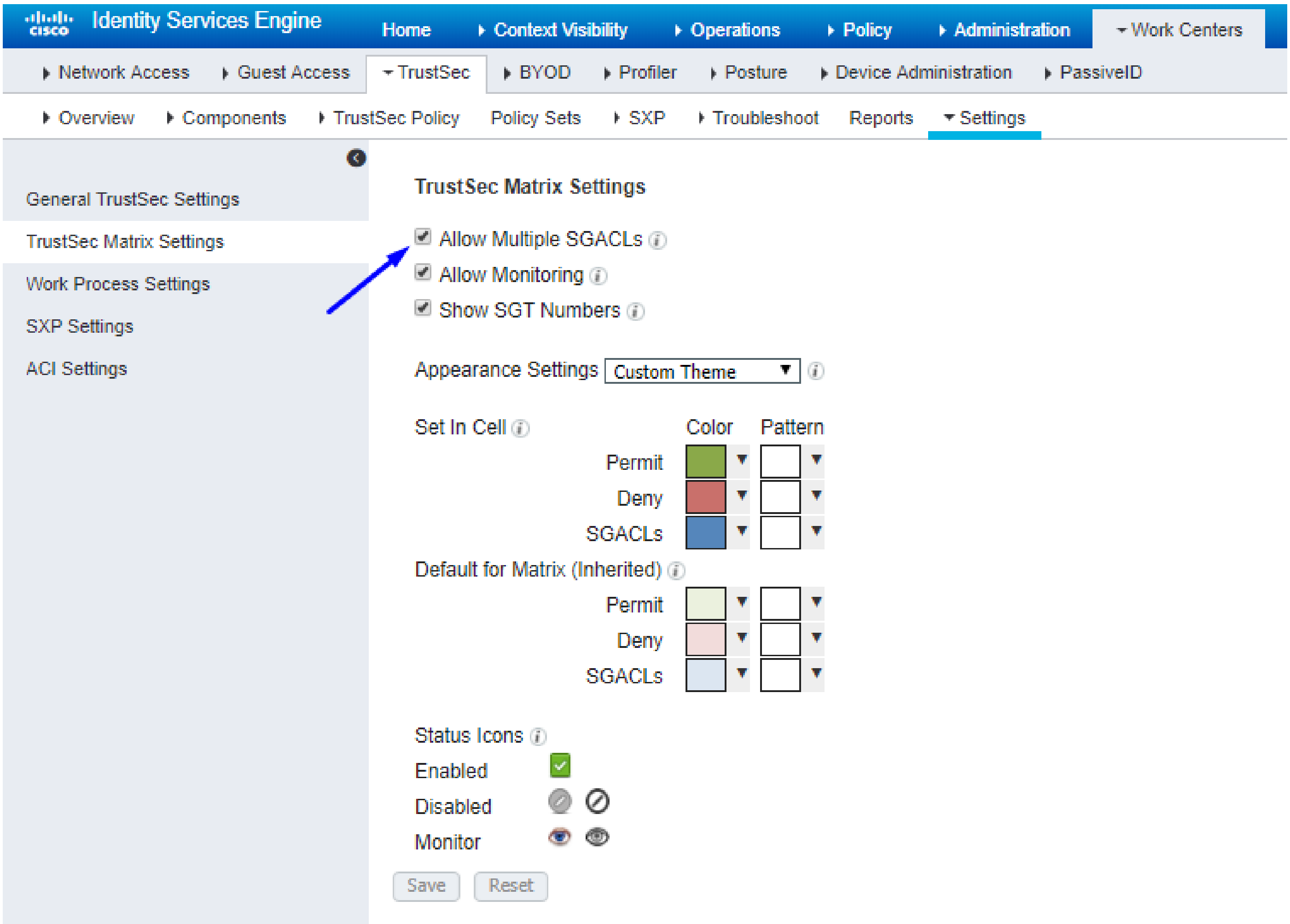
允许员工访问任何外部位置并允许内部Web服务器：



允许管理流量（SSH、HTTPS和CAPWAP）进出网络上的设备（交换机和WLC），这样在部署Cisco TrustSec后不会失去SSH或HTTPS访问：



启用思科ISE以 Allow Multiple SGACLs：



TrustSec Matrix Settings

☑ Allow Multiple SGACLs

☑ Allow Monitoring

☑ Show SGT Numbers

Appearance Settings: Custom Theme

Set In Cell	Color	Pattern
Permit	🟩	□
Deny	🟥	□
SGACLs	🟦	□
Default for Matrix (Inherited)		
Permit	□	□
Deny	□	□
SGACLs	□	□

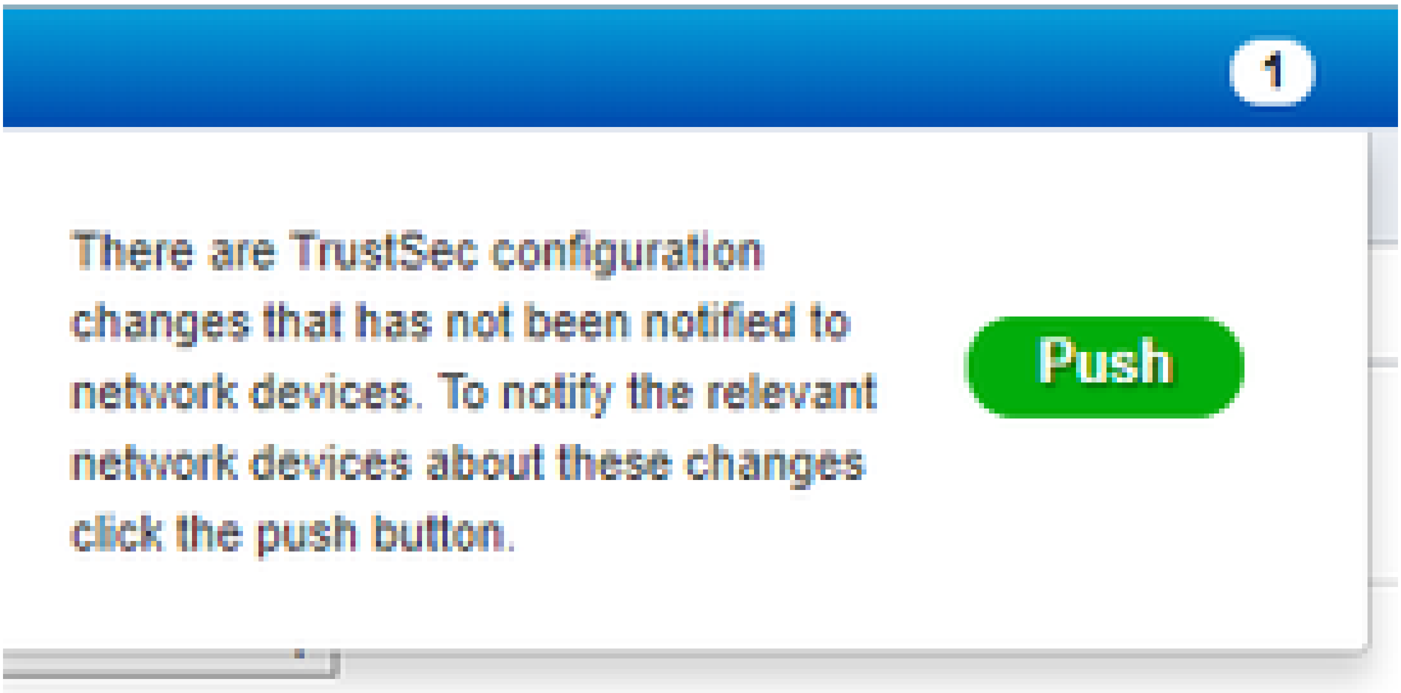
Status Icons

Enabled ✓

Disabled ⊘

Monitor

单击Cisco ISE右上角的Push，将您的配置推送到您的设备。您还需要稍后再进行此操作：



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交换机上配置TrustSec

在Catalyst交换机上配置交换机以使用Cisco TrustSec for AAA

提示：本文档假设您的无线用户成功通过Cisco ISE的BYOD，然后执行此处所示的配置。

粗体显示的命令在此之前已配置（为了使BYOD无线能够与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密钥必须与 **Administration** > **Network Devices** > **Add Device** > **RADIUS Authentication Settings** 部分中指定的RADIUS共享密钥相同。

<#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
```

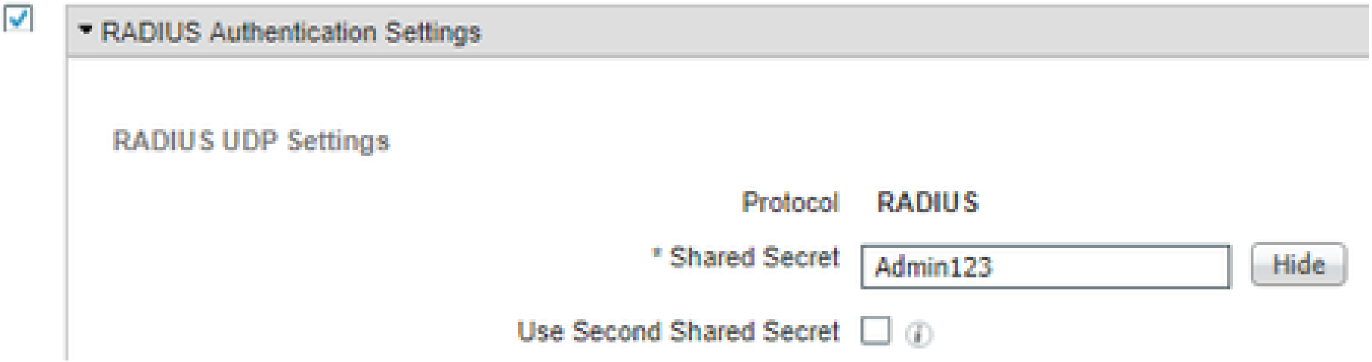
```
CatalystSwitch(config)#radius-server attribute 25 access-request include
```

```
CatalystSwitch(config)#radius-server vsa send authentication
CatalystSwitch(config)#radius-server vsa send accounting
```

```
CatalystSwitch(config)#dot1x system-auth-control
```

在RADIUS服务器下配置PAC密钥验证交换机到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

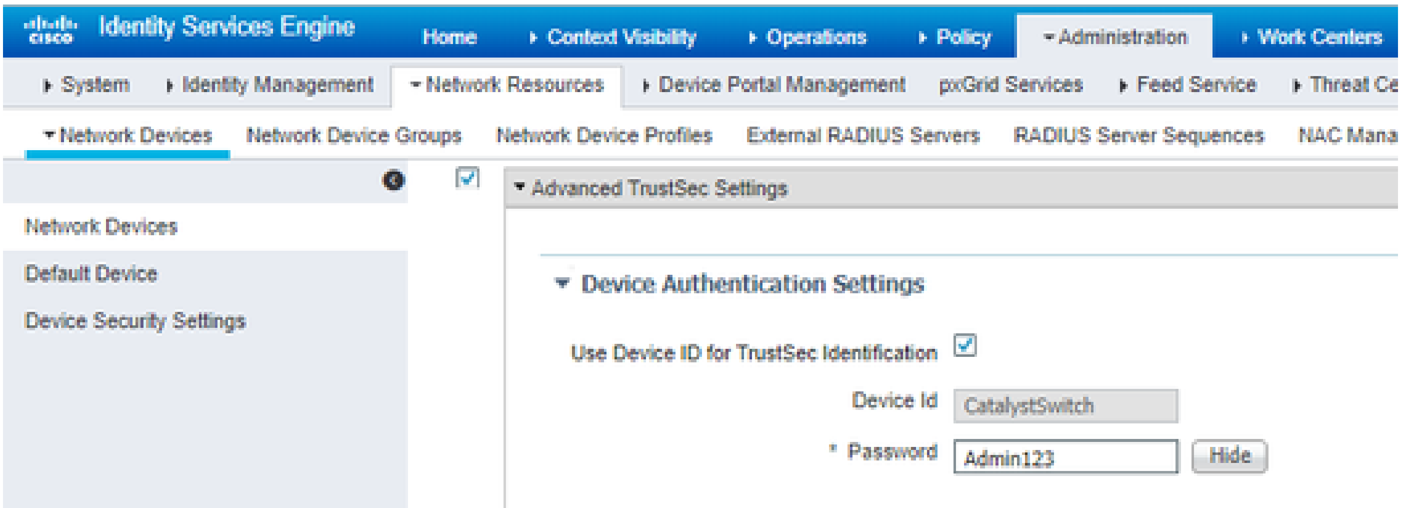
* Shared Secret Admin123

Use Second Shared Secret □

注意：PAC密钥必须与您在Cisco ISE的 **Administration > Network Devices > Add Device > RADIUS Authentication Settings** 部分下指定的RADIUS共享密钥相同（如屏幕截图所示）。

配置CTS凭证验证交换机到Cisco ISE

```
CatalystSwitch#cts credentials id CatalystSwitch password Admin123
```



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id CatalystSwitch

* Password Admin123

注：CTS凭证必须与您在CTS凭证中指定的设备ID +密码相同，必须与您在思科ISE的Administration > Network Devices > Add Device > Advanced TrustSec Settings部分（在屏幕截图中显示）中指定的设备ID +密码相同。

然后，刷新您的PAC，使其再次联系思科ISE：

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

在Catalyst交换机上全局启用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)
```

为受限制的Web服务器进行静态IP到SGT映射（可选）

受限制的Web服务器从未通过ISE进行身份验证，因此您必须使用交换机CLI或ISE Web GUI对其进行手动标记，而这仅仅是思科中的众多Web服务器之一。

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

验证Catalyst交换机上的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: 000200B80003000100040010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F6
 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
```

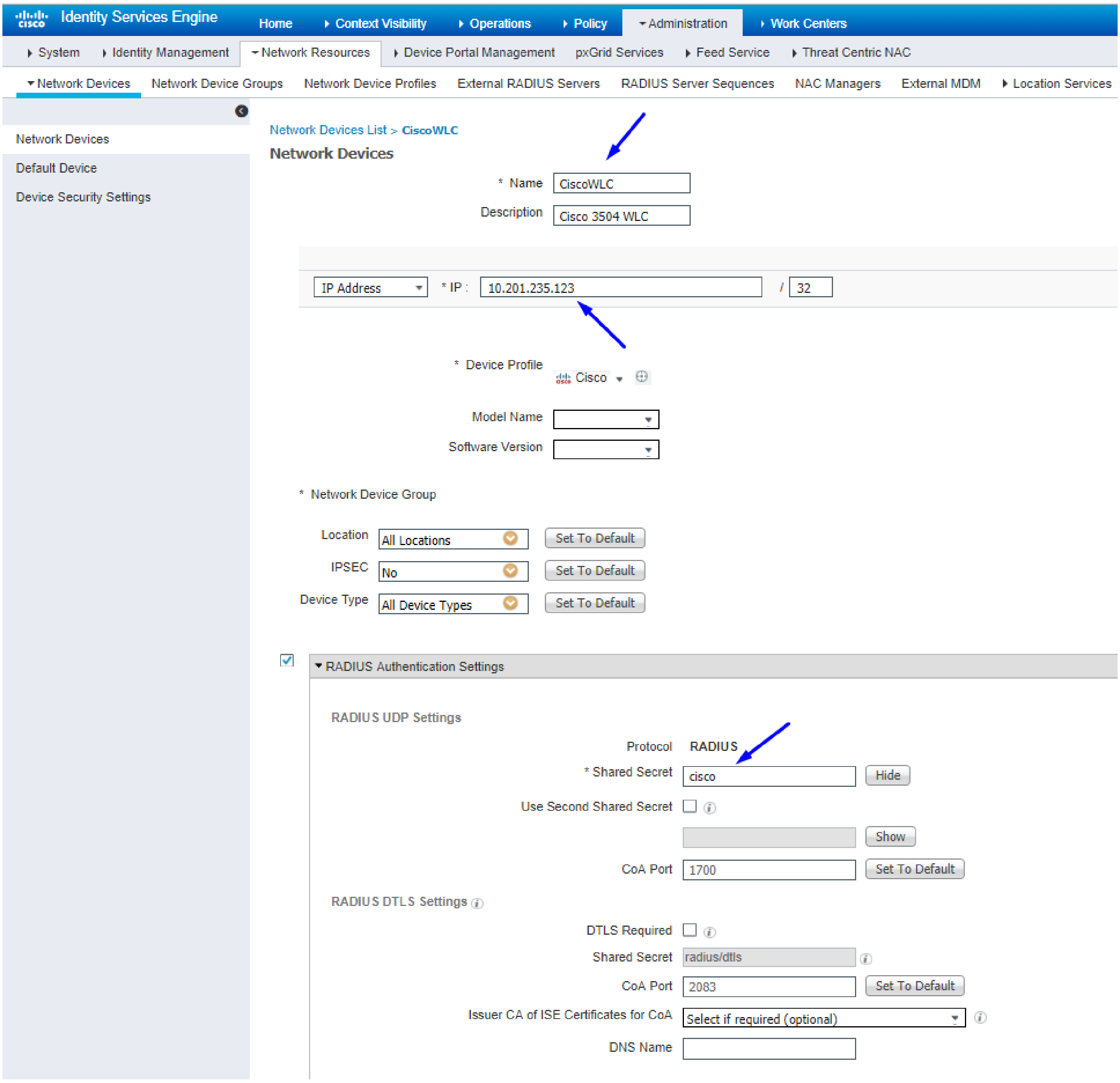
```
CatalystSwitch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

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

配置和验证WLC添加为Cisco ISE的RADIUS设备



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

IPSEC: No

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: cisco

Use Second Shared Secret: □

CoA Port: 1700

RADIUS DTLS Settings

DTLS Required: □

Shared Secret: radius/dtls

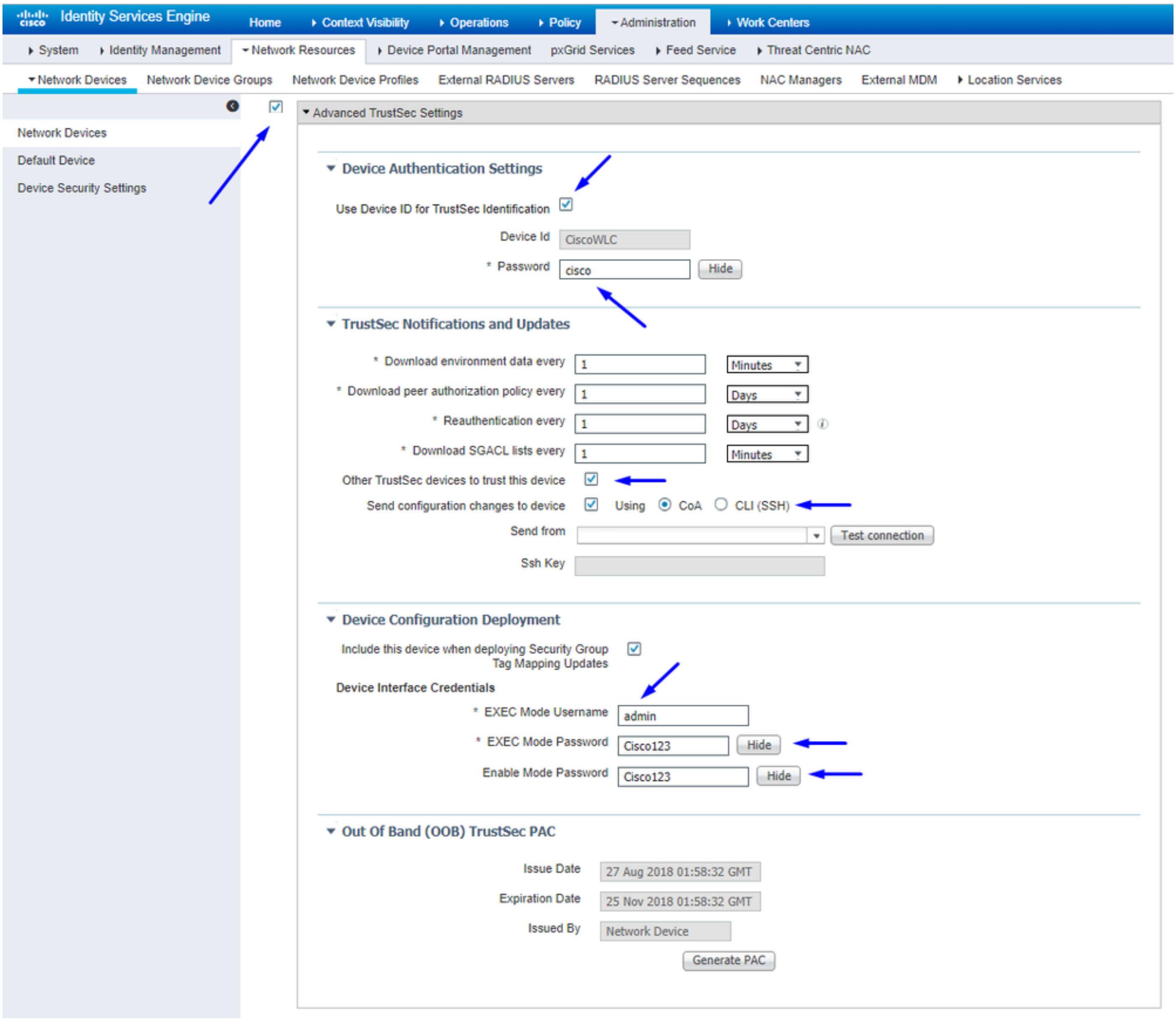
CoA Port: 2083

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

DNS Name:

配置和验证WLC添加为Cisco ISE中的TrustSec设备

此步骤使Cisco ISE部署到WLC的静态IP到SGT映射。您在上一步的**工作中心> TrustSec** >组件**> IP SGT静态映射的**Cisco ISE Web GUI中创建了这些映射。



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: CiscoWLC

* Password: cisco Hide

TrustSec Notifications and Updates

* Download environment data every: 1 Minutes

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

* Download SGACL lists every: 1 Minutes

Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ● CoA ○ CLI (SSH)

Send from: Test connection

Ssh Key:

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username: admin

* EXEC Mode Password: Cisco123 Hide

Enable Mode Password: Cisco123 Hide

Out Of Band (OOB) TrustSec PAC

Issue Date: 27 Aug 2018 01:58:32 GMT

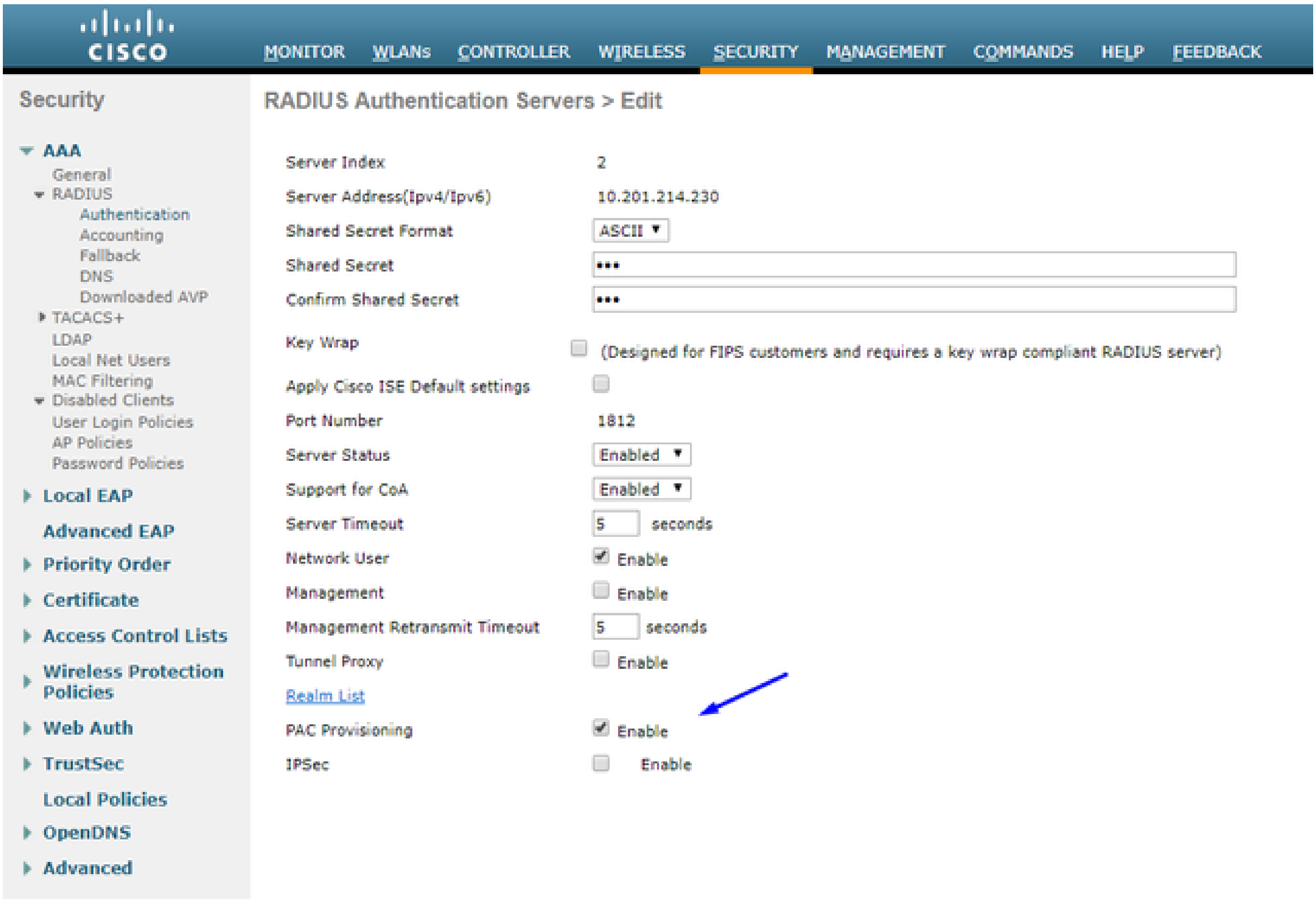
Expiration Date: 25 Nov 2018 01:58:32 GMT

Issued By: Network Device

Generate PAC

注意：我们将使用此 Device ld 命令，在后面的步骤(在WLC Web UI中介绍Security > TrustSec > General)中也会使用 Password 此命令。

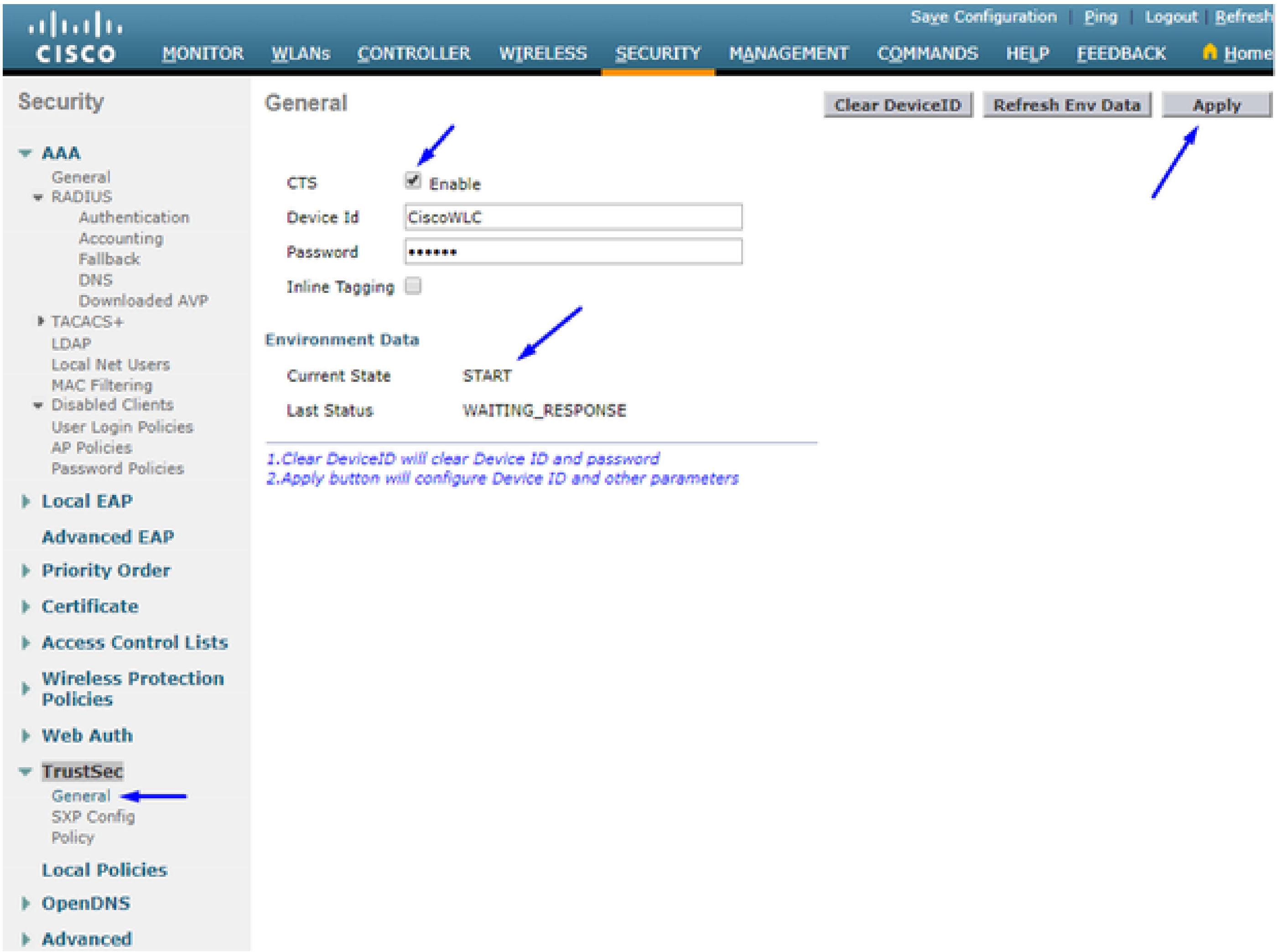
启用WLC的PAC调配



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
IPSec	□ Enable

在WLC上启用TrustSec



General

CTS ☑ Enable

Device Id CiscoWLC

Password ••••••

Inline Tagging □

Environment Data

Current State START

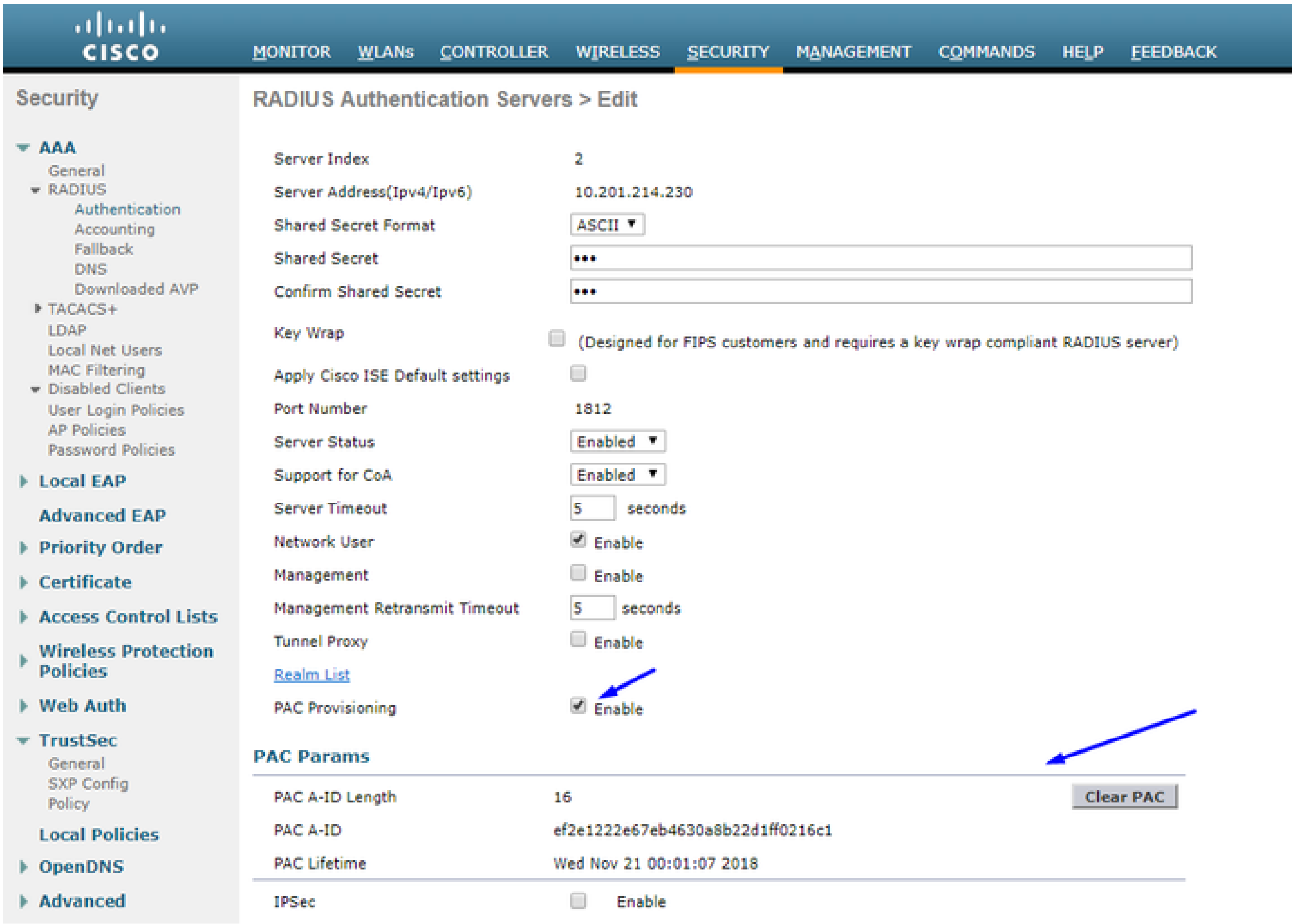
Last Status WAITING_RESPONSE

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 必须与您在思科ISE的Administration > Network Devices > Add Device > Advanced TrustSec Settings部分中指定的 Device Id 和 Password 相同。

验证PAC是否已在WLC上配置

当您单击Refresh Env Data（在此步骤中执行此操作）后，您会看到WLC已成功调配PAC：



RADIUS Authentication Servers > Edit

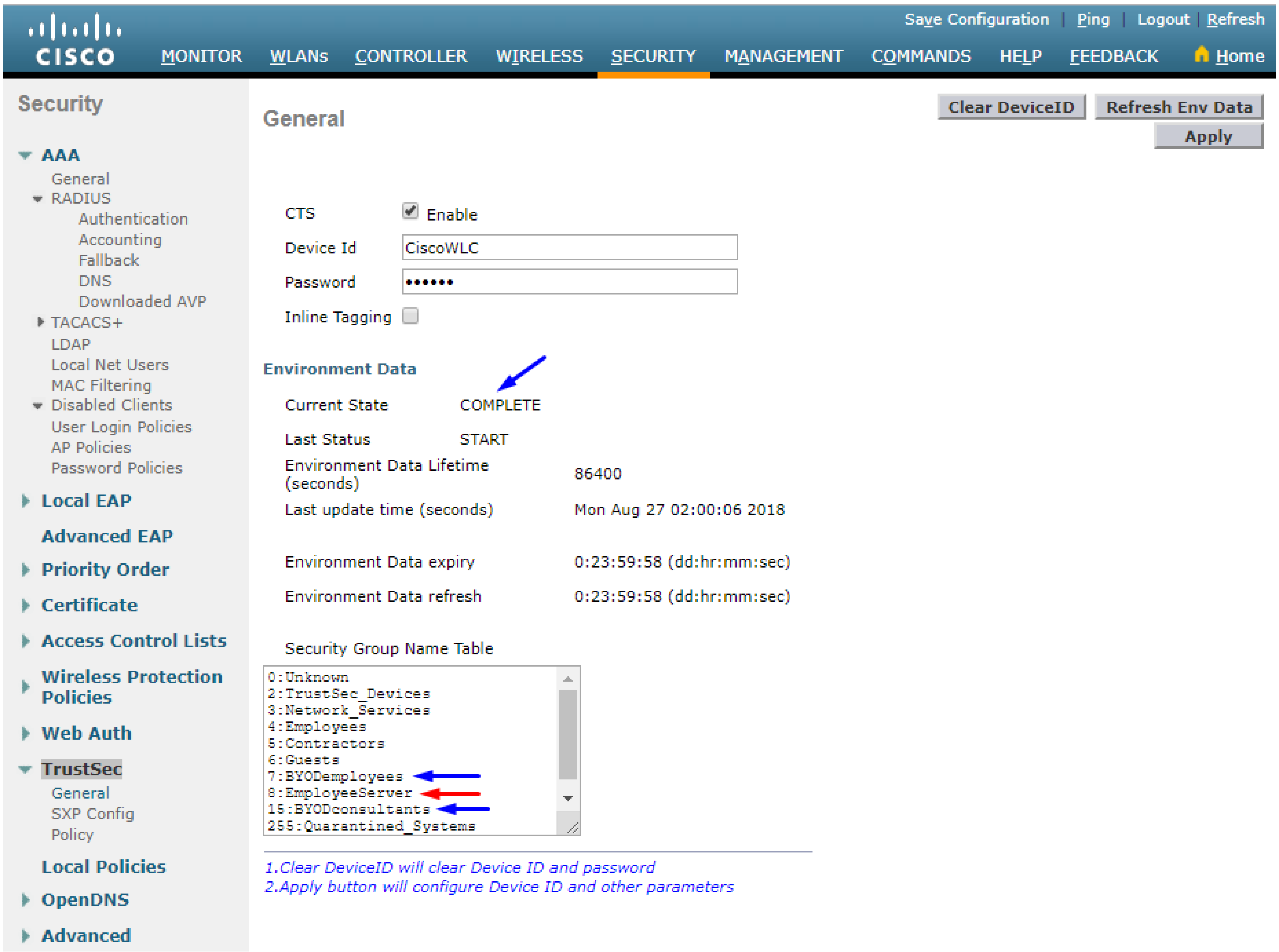
Server Index	2
Server Address(Ipv4/Ipv6)	10.201.214.230
Shared Secret Format	ASCII ▼
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	□
Port Number	1812
Server Status	Enabled ▼
Support for CoA	Enabled ▼
Server Timeout	5 seconds
Network User	☑ Enable
Management	□ Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	□ Enable
Realm List	
PAC Provisioning	☑ Enable

PAC Params

PAC A-ID Length	16
PAC A-ID	ef2e1222e67eb4630a8b22d1ff0216c1
PAC Lifetime	Wed Nov 21 00:01:07 2018
IPSec	□ Enable

将CTS环境数据从思科ISE下载到WLC

在您单击Refresh Env Data之后，您的WLC将下载您的SGT。



General

CTS ☑ Enable

Device Id: CiscoWLC

Password: ••••••

Inline Tagging ☐

Environment Data

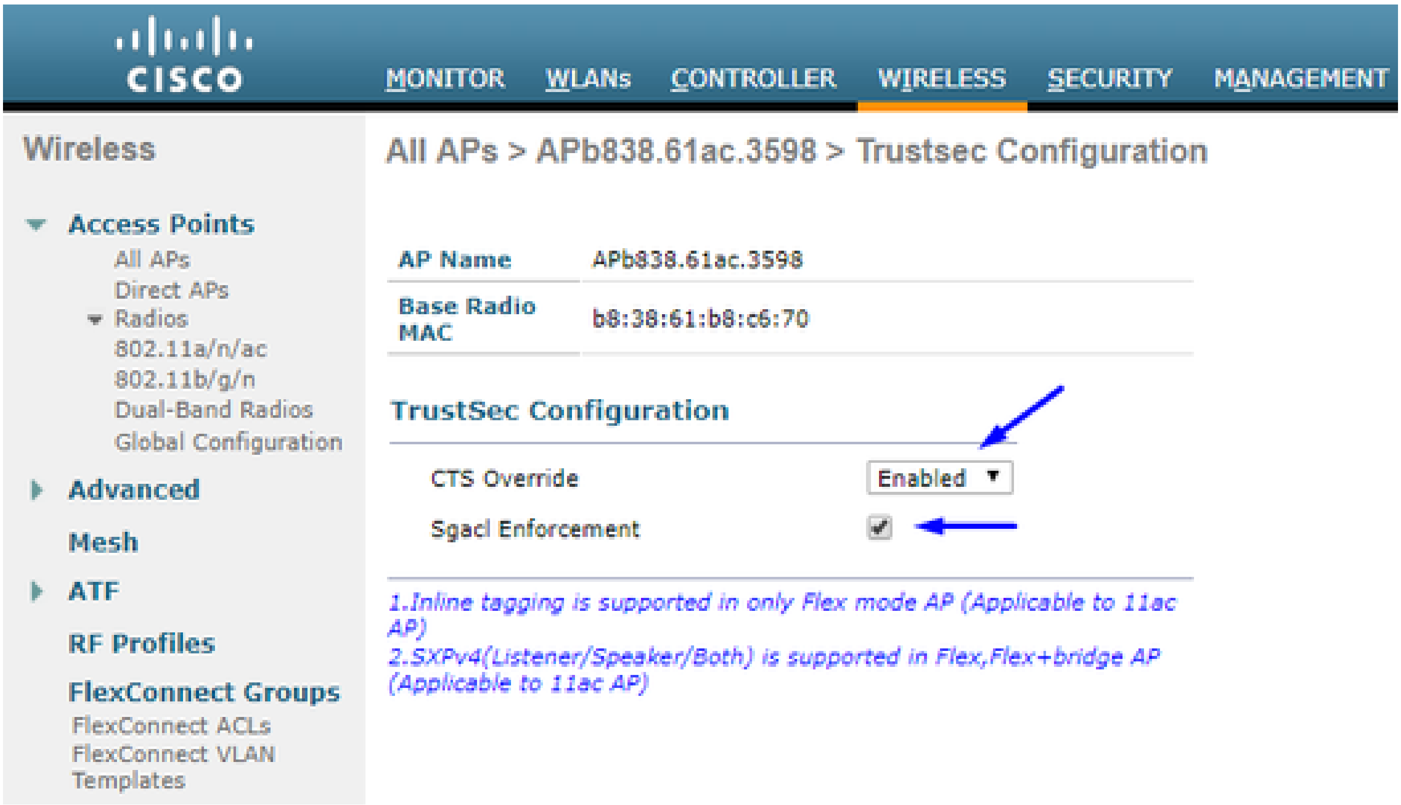
Current State	COMPLETE
Last Status	START
Environment Data Lifetime (seconds)	86400
Last update time (seconds)	Mon Aug 27 02:00:06 2018
Environment Data expiry	0:23:59:58 (dd:hr:mm:sec)
Environment Data refresh	0:23:59:58 (dd:hr:mm:sec)

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

对流量启用SGACL下载和实施



All APs > APb838.61ac.3598 > Trustsec Configuration

AP Name	APb838.61ac.3598
Base Radio MAC	b8:38:61:b8:c6:70

TrustSec Configuration

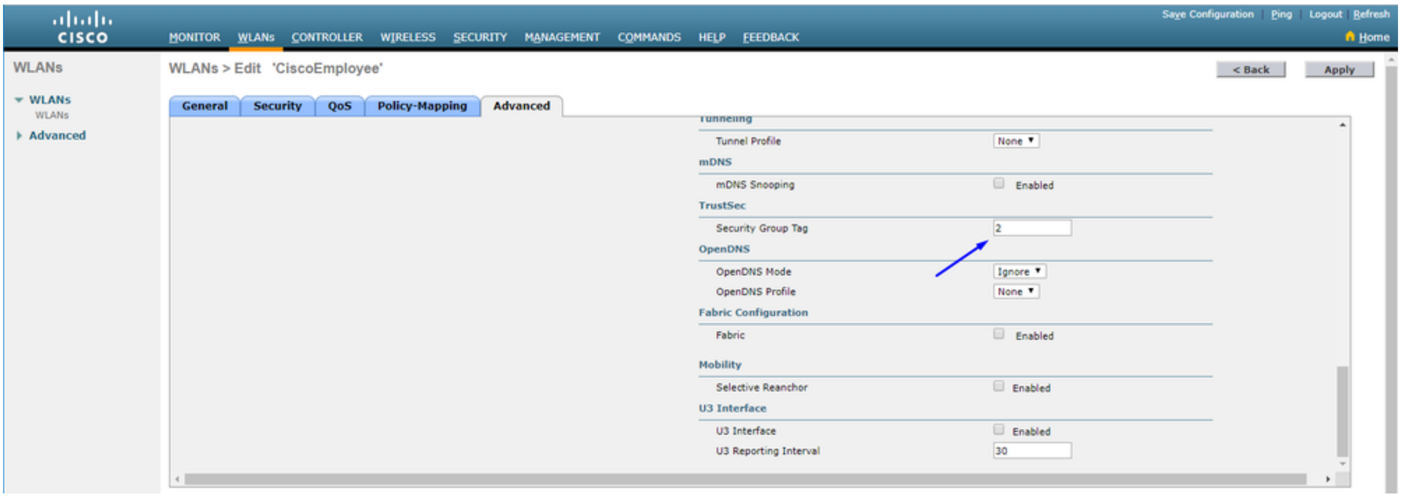
CTS Override: Enabled ▼

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)

为WLC和接入点分配SGT 2 (TrustSec_Devices)

为WLC+WLAN指定2 (TrustSec_Devices)的SGT，以允许通过交换机与WLC + AP之间的流量（SSH、HTTPS和CAPWAP）。


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Home
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced

WLANs > Edit 'CiscoEmployee'

Tunneling

Tunnel Profile: None

mDNS

mDNS Snooping ☐ Enabled

TrustSec

Security Group Tag: 2

OpenDNS

OpenDNS Mode: Ignore

OpenDNS Profile: None

Fabric Configuration

Fabric ☐ Enabled

Mobility

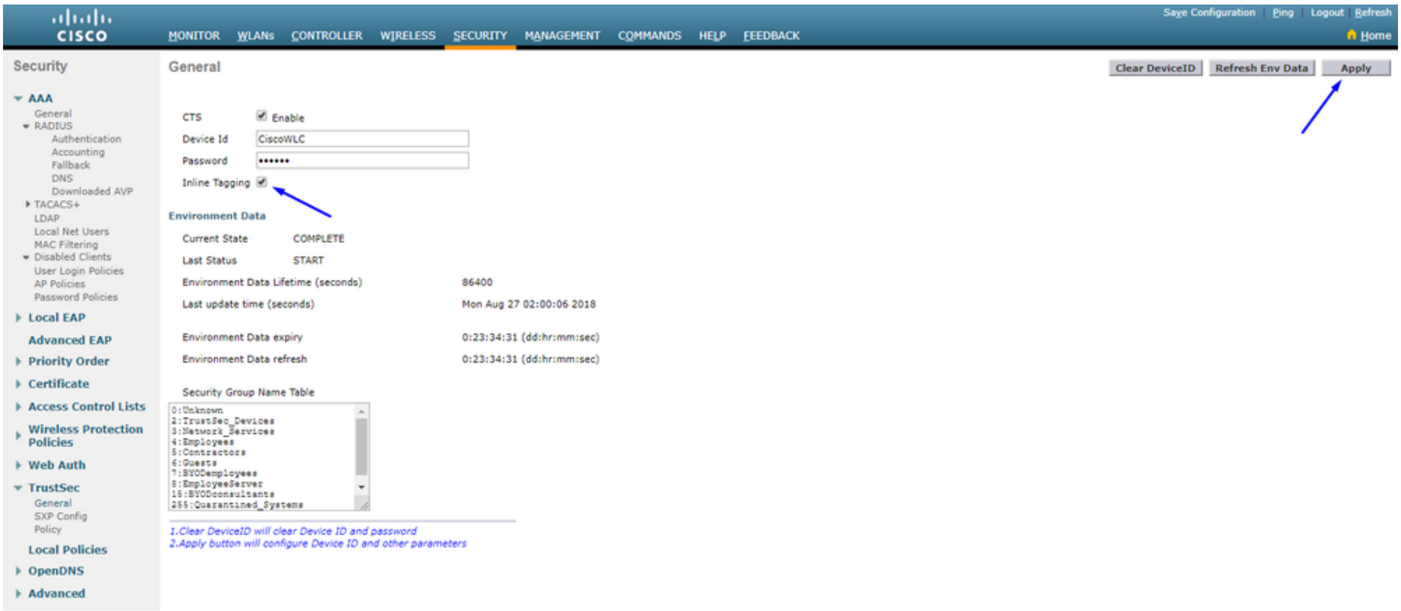
Selective Reanchor ☐ Enabled

U3 Interface

U3 Interface ☐ Enabled

U3 Reporting Interval: 30

在WLC上启用内联标记



General

CTS ☑ Enable

Device Id: CiscoWLC

Password: ••••••

Inline Tagging ☑

Environment Data

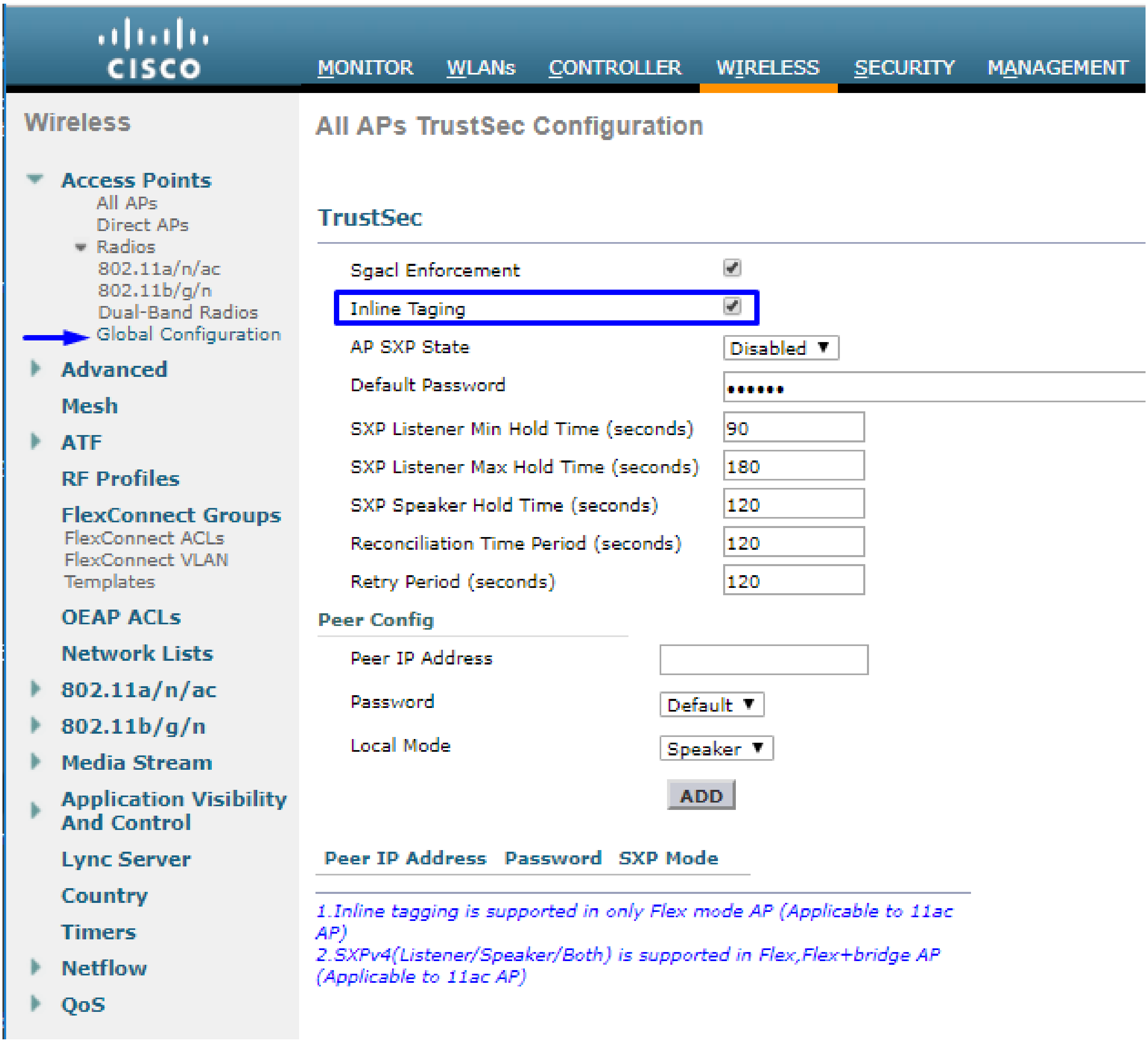
Current State	COMPLETE
Last Status	START
Environment Data Lifetime (seconds)	86400
Last update time (seconds)	Mon Aug 27 02:00:06 2018
Environment Data expiry	0:23:34:31 (dd:hr:mm:sec)
Environment Data refresh	0:23:34:31 (dd:hr:mm:sec)

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 **Wireless > Access Points > Global Configuration** 下滚动，然后选择 **TrustSec Config**。



All APs TrustSec Configuration

TrustSec

Sgacl Enforcement	☑
Inline Taging	☑
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 ▼

Peer IP Address	Password	SXP Mode

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)

在Catalyst交换机上启用Inline Tagging

<#root>

CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

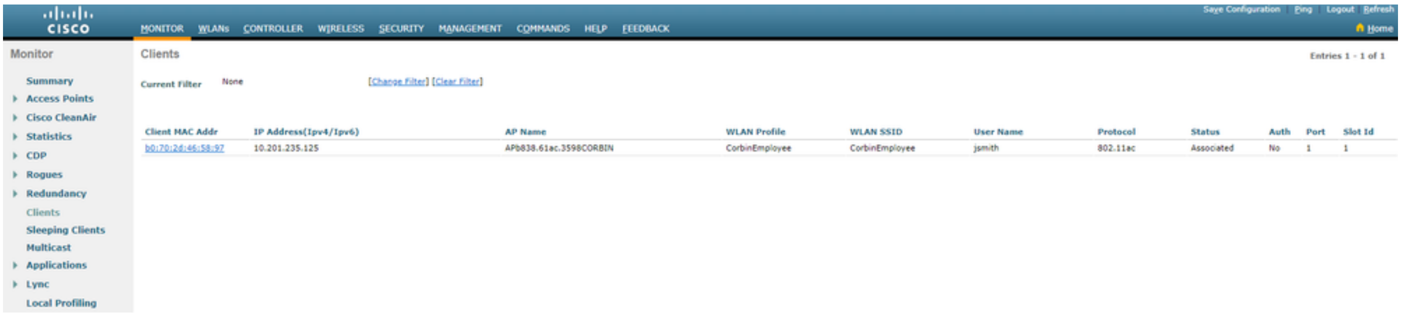
```
CatalystSwitch(config-if)#description goestoWLC


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
```

验证



Clients

Entries 1 - 1 of 1

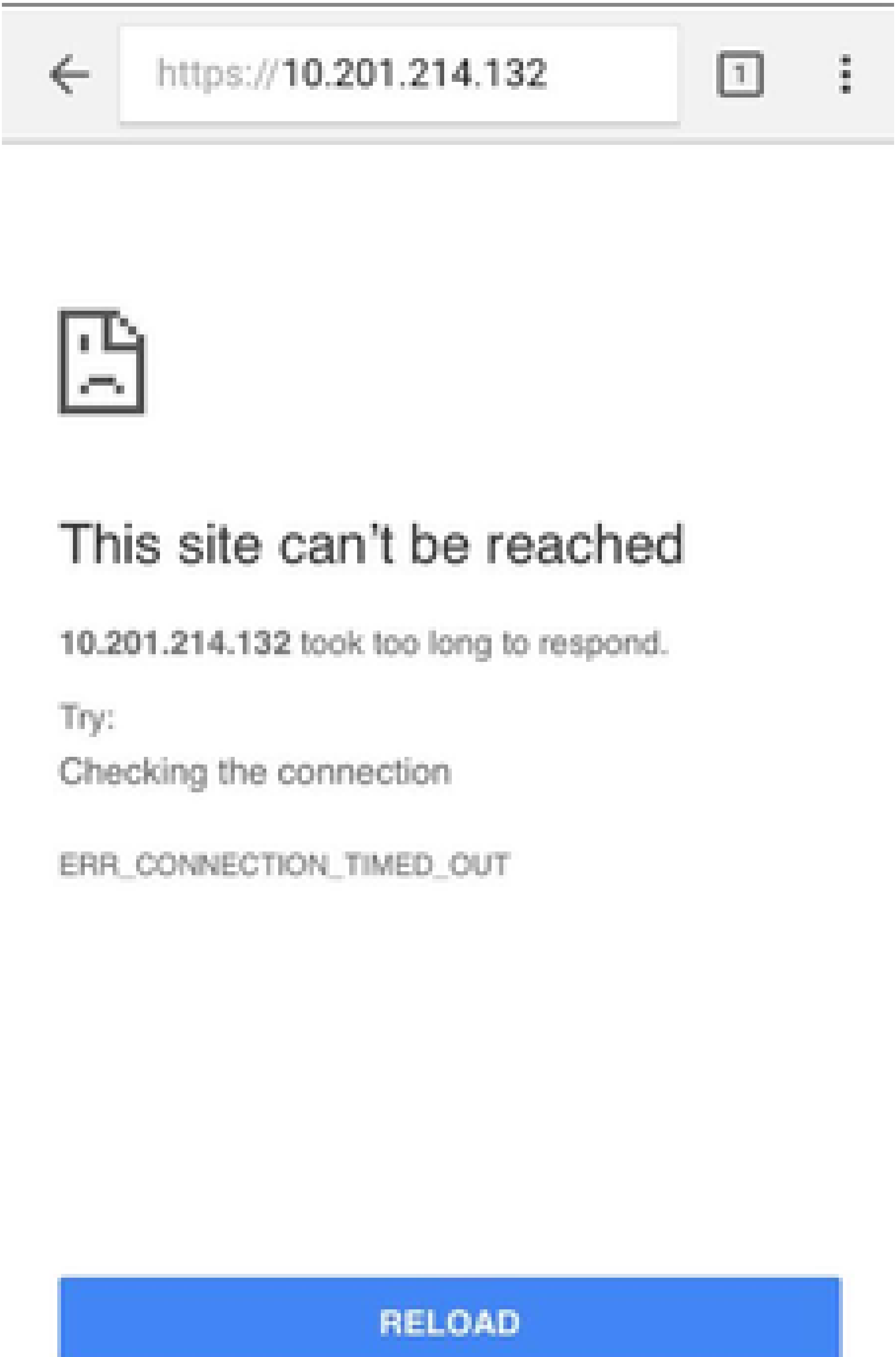
Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id
b0:70:2d:46:58:97	10.201.235.125	APb838.61ac.3598CORBIN	CorbinEmployee	CorbinEmployee	jsmith	802.11ac	Associated	No	1	1

```
CatalystSwitch#show platform acl counters hardware | inc SGACL
出口IPv4 SGACL丢弃(454)：10帧
出口IPv6 SGACL丢弃(455)：0帧
出口IPv4 SGACL信元丢弃(456)：0帧
出口IPv6 SGACL信元丢弃(457)：0帧
```

提示：如果改用Cisco ASR、Nexus或Cisco ASA，此处列出的文档可帮助您验证SGT标记是否已实施：TrustSec故障排除指南。

使用用户名jsmith密码Admin123进行无线身份验证-您在交换机中遇到拒绝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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。