Configure TrustSec (SGTs) with ISE (Inline Tagging)

Contents

Introduction

This document describes how to configure and verify TrustSec on a Catalyst Switch and Wireless LAN Controller with the Identity Services Engine.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Cisco TrustSec (CTS) components
- Basic knowledge of CLI configuration of Catalyst switches
- Basic knowledge of GUI configuration of Cisco Wireless LAN Controllers (WLC)
- Experience with Identity Services Engine (ISE) configuration

Requirements

You must have Cisco ISE deployed in your network, and end users must authenticate to Cisco ISE with 802.1x (or other method) when they connect to wireless or wired. Cisco ISE assigns their traffic a Security Group Tag (SGT) once they authenticate to your wireless network.

In our example, end users are redirected to the Cisco ISE Bring Your Own Device (BYOD) portal and are provisioned a certificate so they can securely access the wireless network with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) once they complete the BYOD portal steps.

Components Used

The information in this document is based on these hardware and software versions:

- Cisco Identity Services Engine, version 2.4
- Cisco Catalyst 3850 Switch, version 3.7.5E
- Cisco WLC, version 8.5.120.0
- Cisco Aironet Wireless Access Point in Local mode

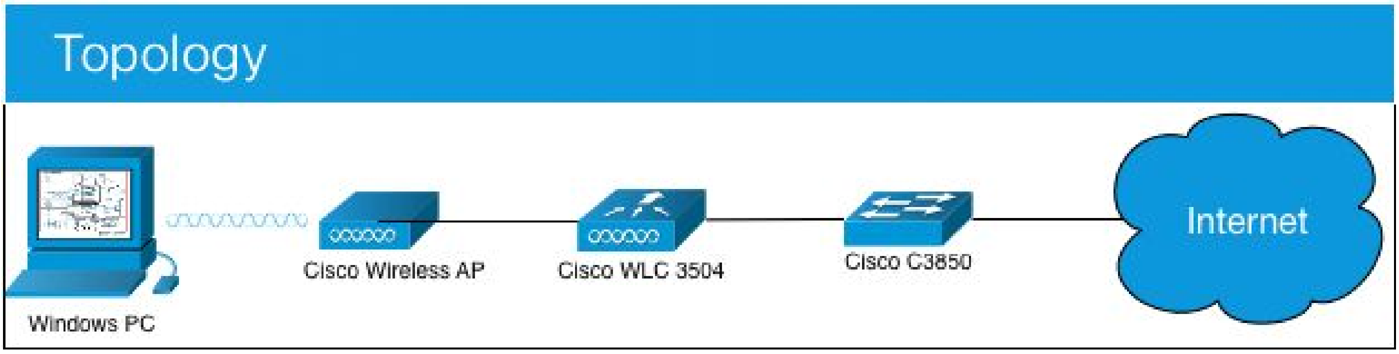
Before deployment of Cisco TrustSec, verify your Cisco Catalyst Switch and/or Cisco WLC+AP models + software version has support for:

- TrustSec/Security Group Tags
- Inline Tagging (if not, you can use SXP instead of Inline Tagging)
- Static IP-to-SGT mappings (if needed)
- Static Subnet-to-SGT mappings (if needed)
- Static VLAN-to-SGT mappings (if needed)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



In this example, the WLC tags the packets as SGT 15 if from a Consultant, and + SGT 7 if from an Employee.

The switch denies those packets if they are from SGT 15 to SGT 8 (consultants cannot access servers tagged as SGT 8).

The switch allows those packets if they are from SGT 7 to SGT 8 (employees can access servers tagged as SGT 8).

Goal

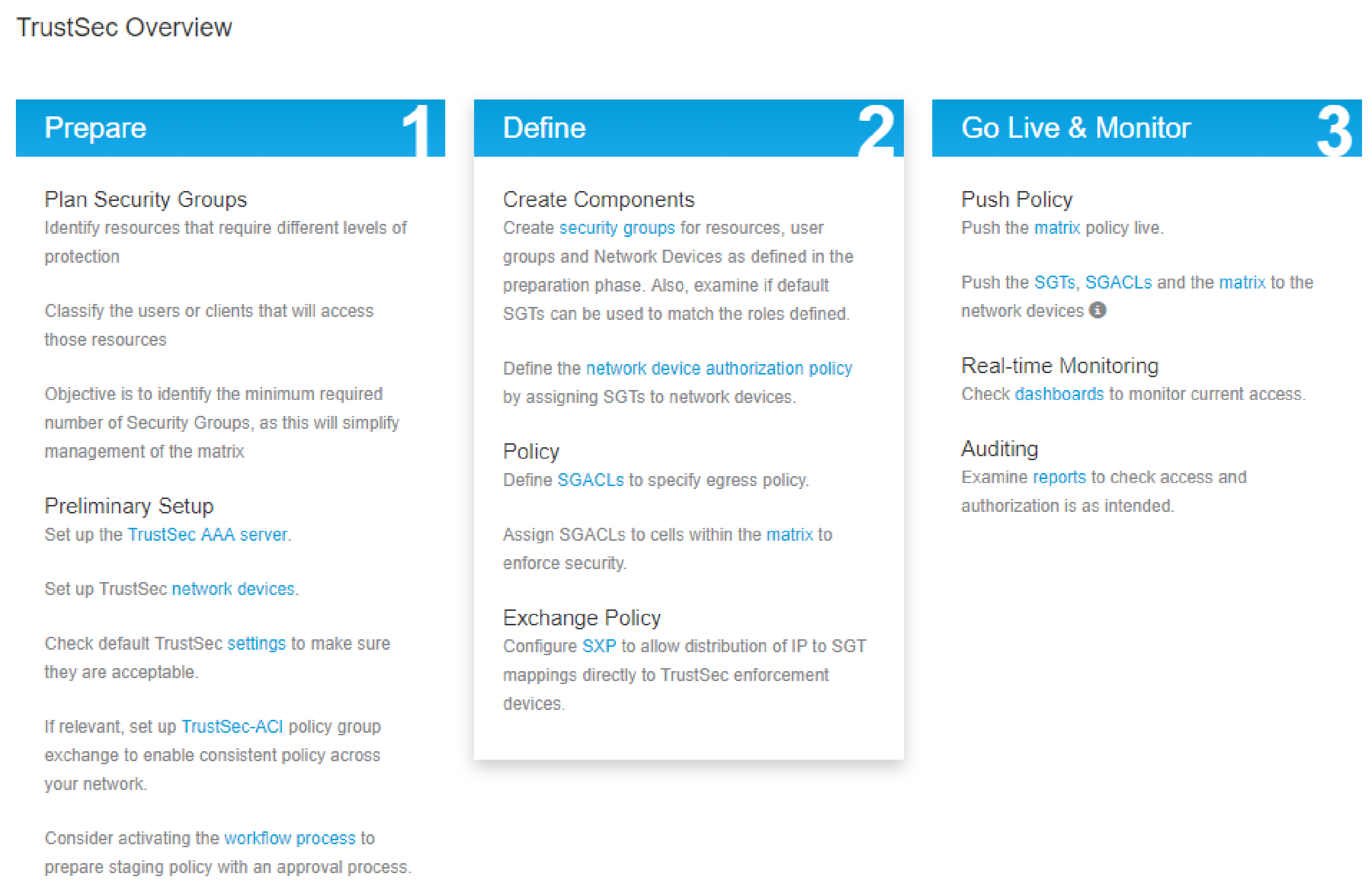
Let anyone access GuestSSID.
Let Consultants access EmployeeSSID, but with restricted access.
Let Employees access EmployeeSSID with full access.

Device	IP address	VLAN
ISE	10.201.214.230	463
Catalyst Switch	10.201.235.102	1115
WLC	10.201.214.229	463
Access Point	10.201.214.138	455

Name	Username	AD Group	SG	SGT
Jason Smith	jsmith	Consultants	BYODconsultants	15
Sally Smith	ssmith	Employees	BYODemployees	7
n/a	n/a	n/a	TrustSec_Devices	2

Configurations

Configure TrustSec on ISE



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

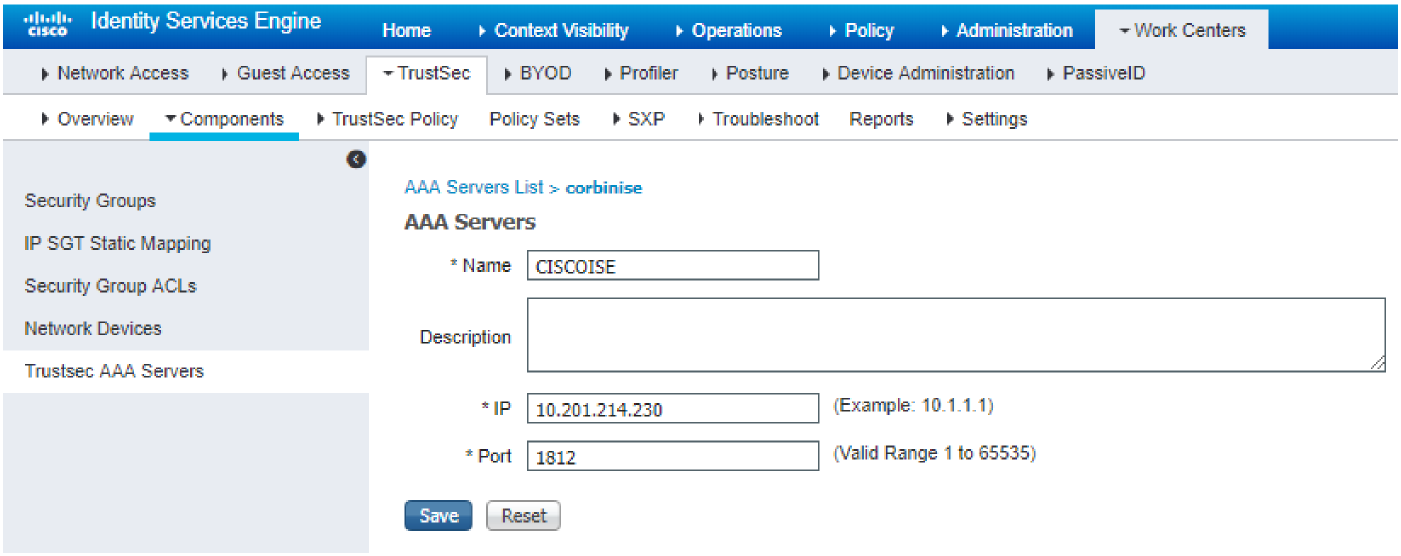
Real-time Monitoring

Check dashboards to monitor current access.

Auditing

Examine reports to check access and authorization is as intended.

Configure Cisco ISE as a TrustSec AAA Server



AAA Servers List > corbinise

AAA Servers

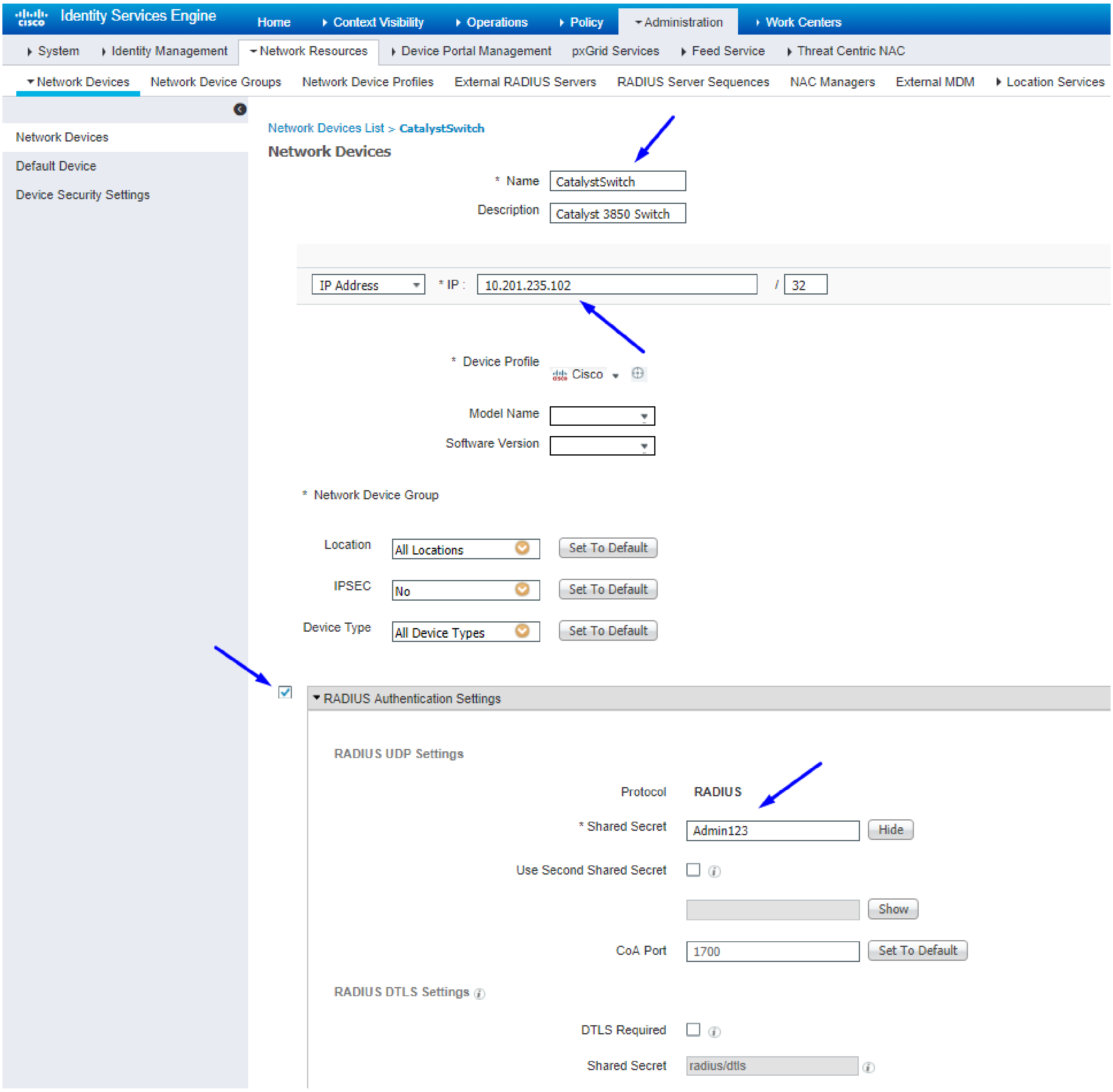
* Name CISCOISE

Description

* IP 10.201.214.230 (Example: 10.1.1.1)

* Port 1812 (Valid Range 1 to 65535)

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



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

IPSEC: No

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: Admin123

Use Second Shared Secret: □

CoA Port: 1700

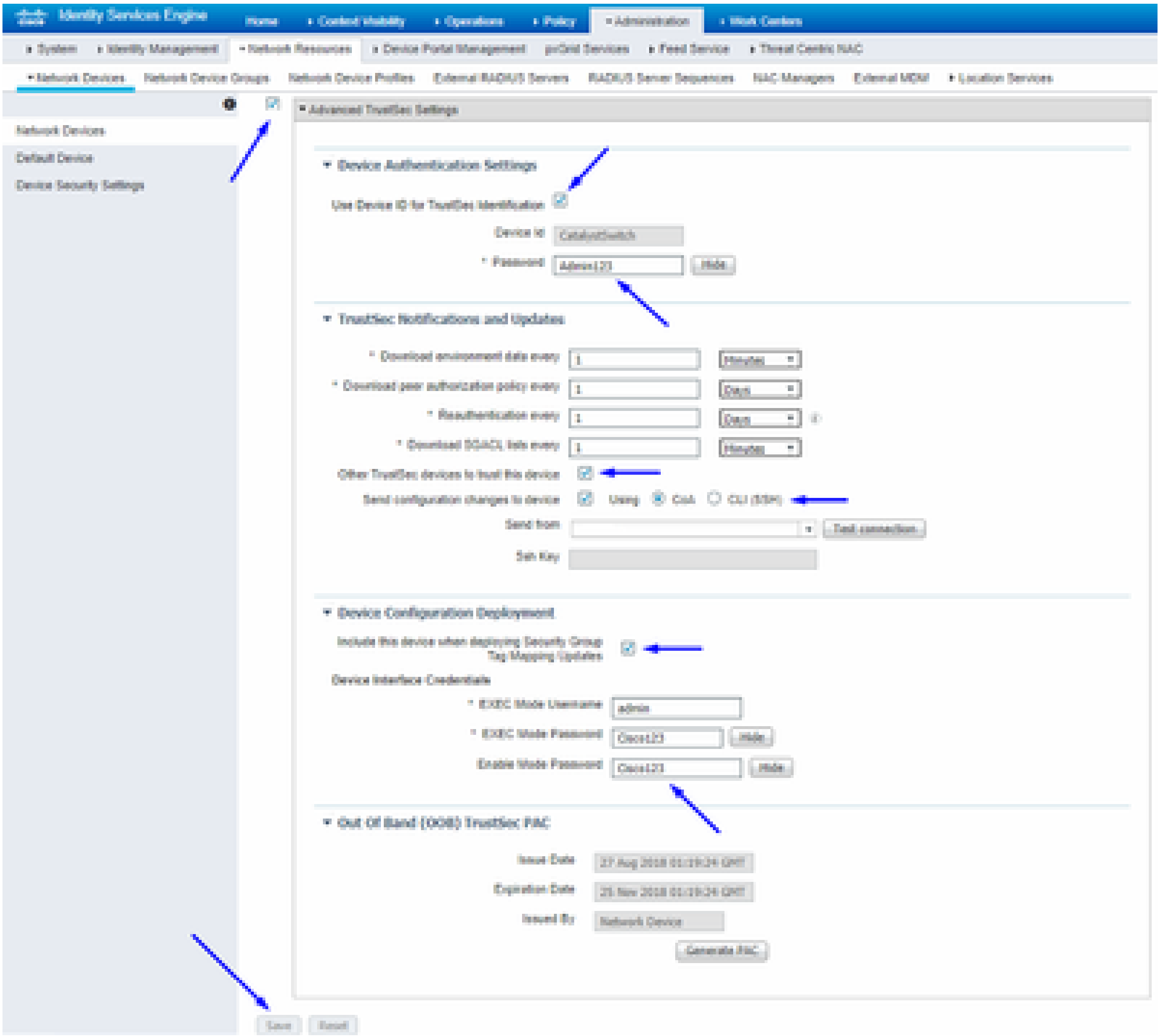
RADIUS DTLS Settings

DTLS Required: □

Shared Secret: radius/dtls

Configure and Verify WLC is Added as a TrustSec Device in Cisco ISE

Enter your log in credentials for SSH. This enables Cisco ISE to deploy the static IP-to-SGT Mappings to the switch.
You create these in the Cisco ISE Web GUI under Work Centers > TrustSec > Components > IP SGT Static Mappings as shown here:



☑ ▾ 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

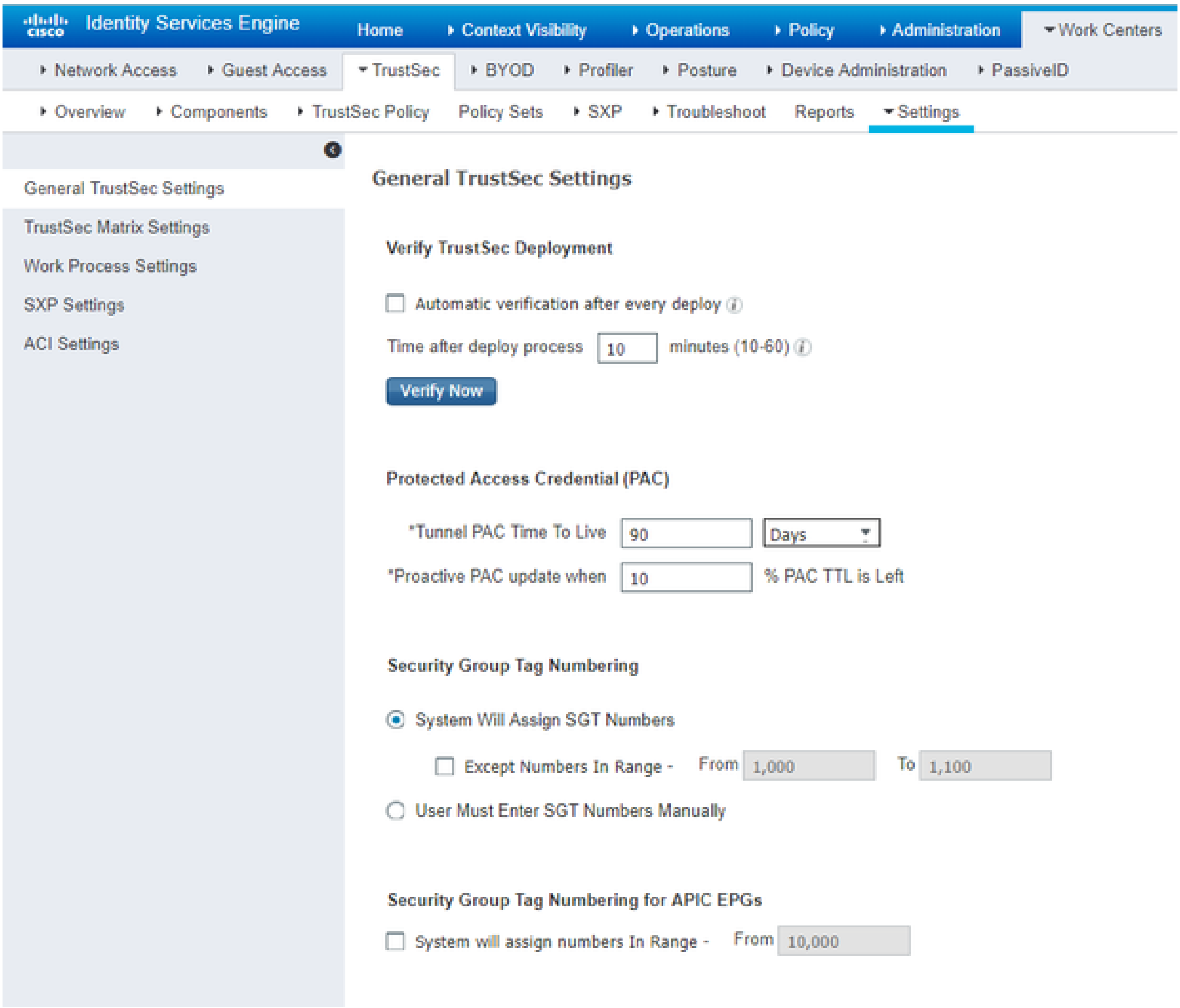
Issued By: Network Device

[Generate PAC]

Tip: If you have not yet configured SSH on your Catalyst Switch, you can use this guide: How to Configure Secure Shell (SSH) on Catalyst Switch.

Tip: If you do not want to enable Cisco ISE to access your Catalyst Switch over SSH, you can create Static IP-to-SGT mappings on the Catalyst Switch with the CLI instead (shown in a step here).

Verify Default TrustSec Settings to Make Sure They are Acceptable (Optional)



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

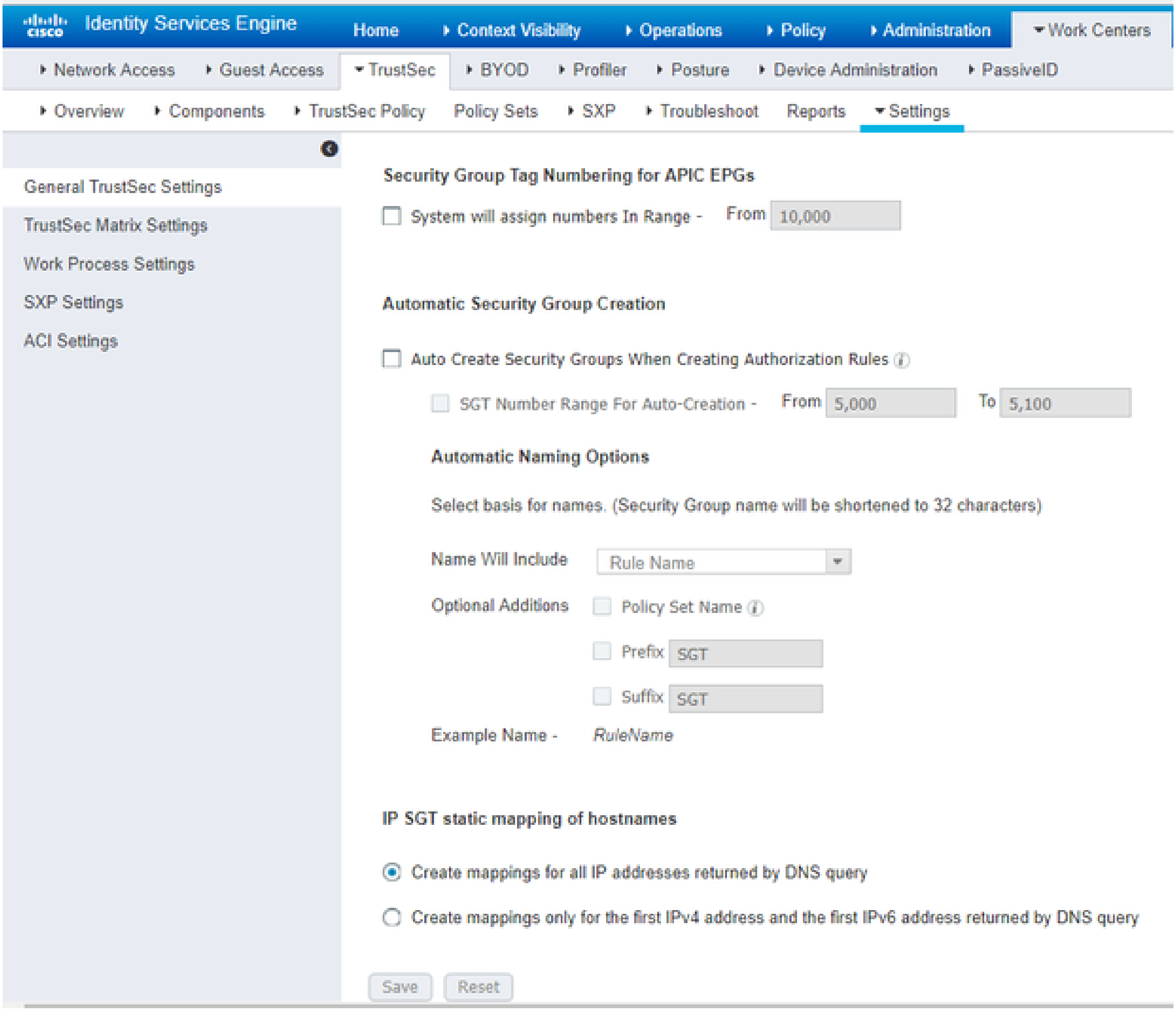
● System Will Assign SGT Numbers

□ 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*

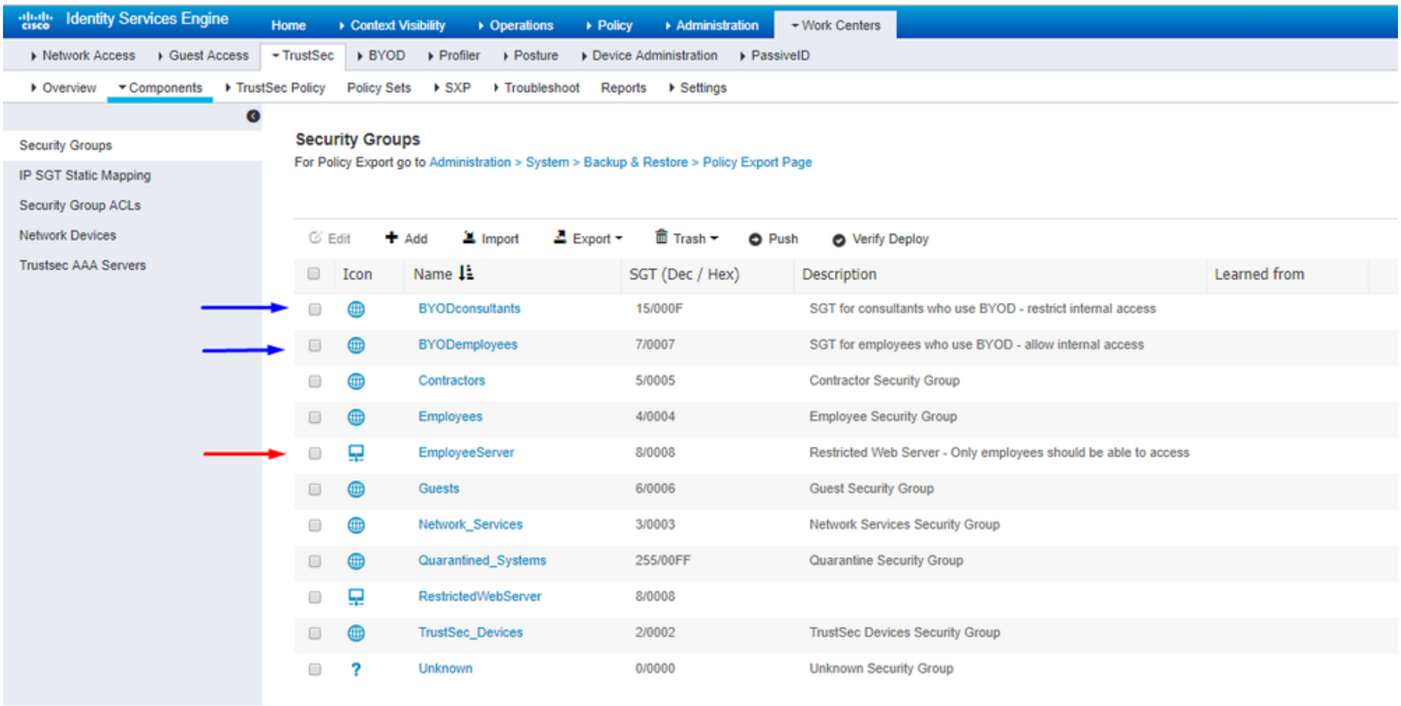
IP SGT static mapping of hostnames

● 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

Create Security Group Tags for Wireless Users

Create Security Group for BYODconsultants - SGT 15
Create Security Group for BYODemployees - SGT 7



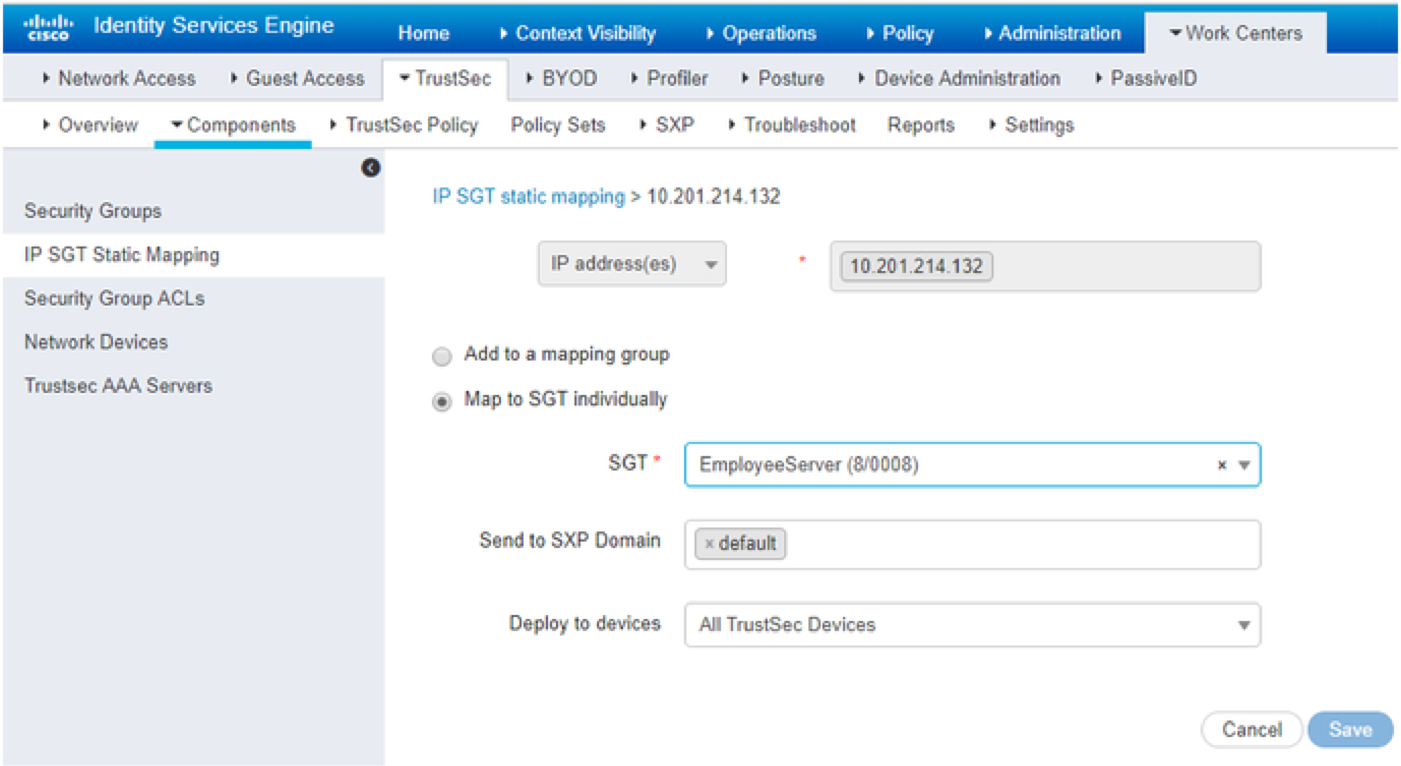
Security Groups

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	

Create Static IP-to-SGT Mapping for the Restricted Web Server

Do this for any other IP addresses or subnets in your network that do not authenticate to Cisco ISE with MAC Authentication Bypass (MAB), 802.1x, Profiles, and so on.



IP SGT static mapping > 10.201.214.132

IP address(es) * 10.201.214.132

○ Add to a mapping group

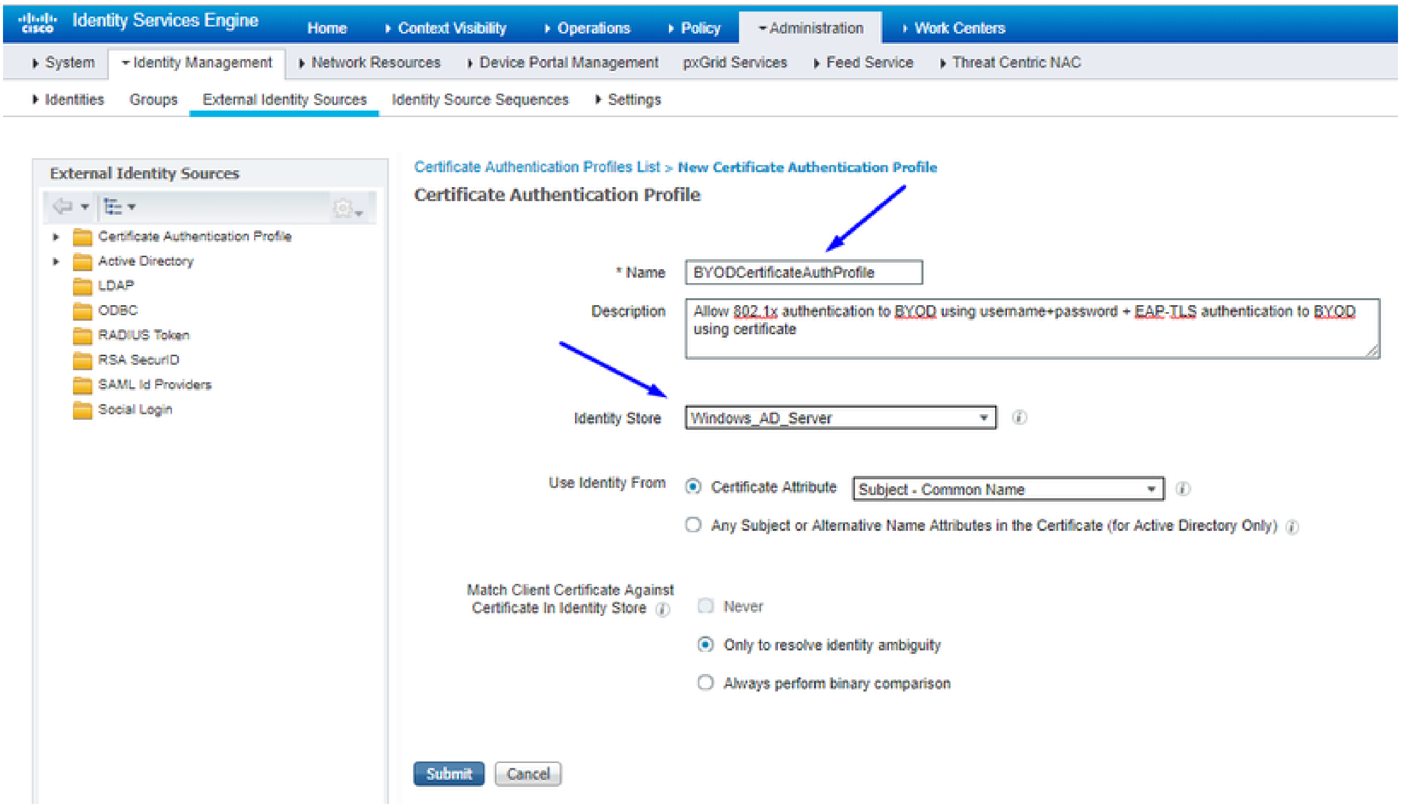
● Map to SGT individually

SGT * EmployeeServer (8/0008)

Send to SXP Domain: default

Deploy to devices: All TrustSec Devices

Create 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)

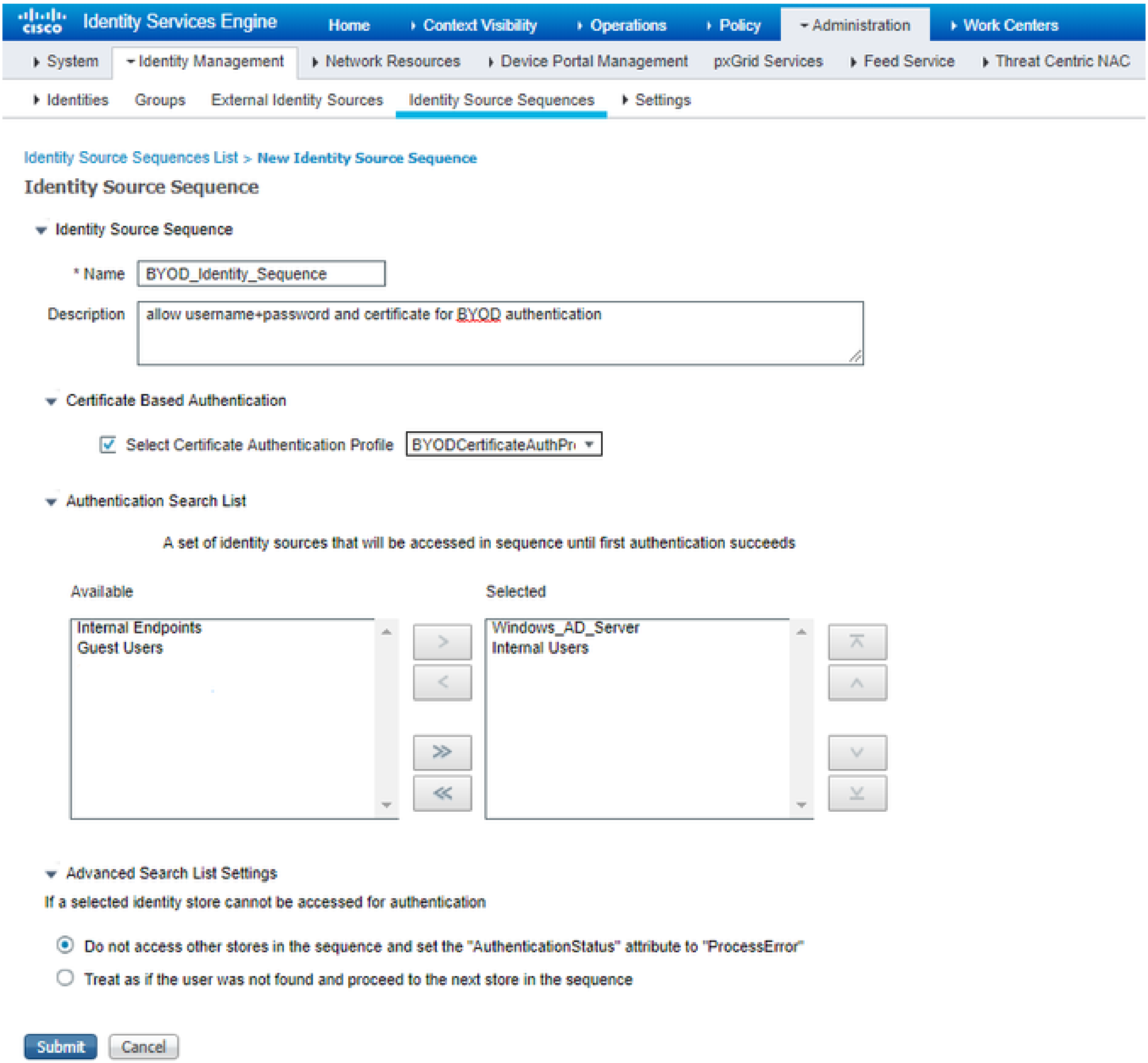
Match Client Certificate Against Certificate In Identity Store

□ Never

● Only to resolve identity ambiguity

○ Always perform binary comparison

Create Identity Source Sequence with the Certificate Authentication Profile from Before



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	Selected
Internal Endpoints Guest Users	Windows_AD_Server Internal Users

Advanced Search List Settings

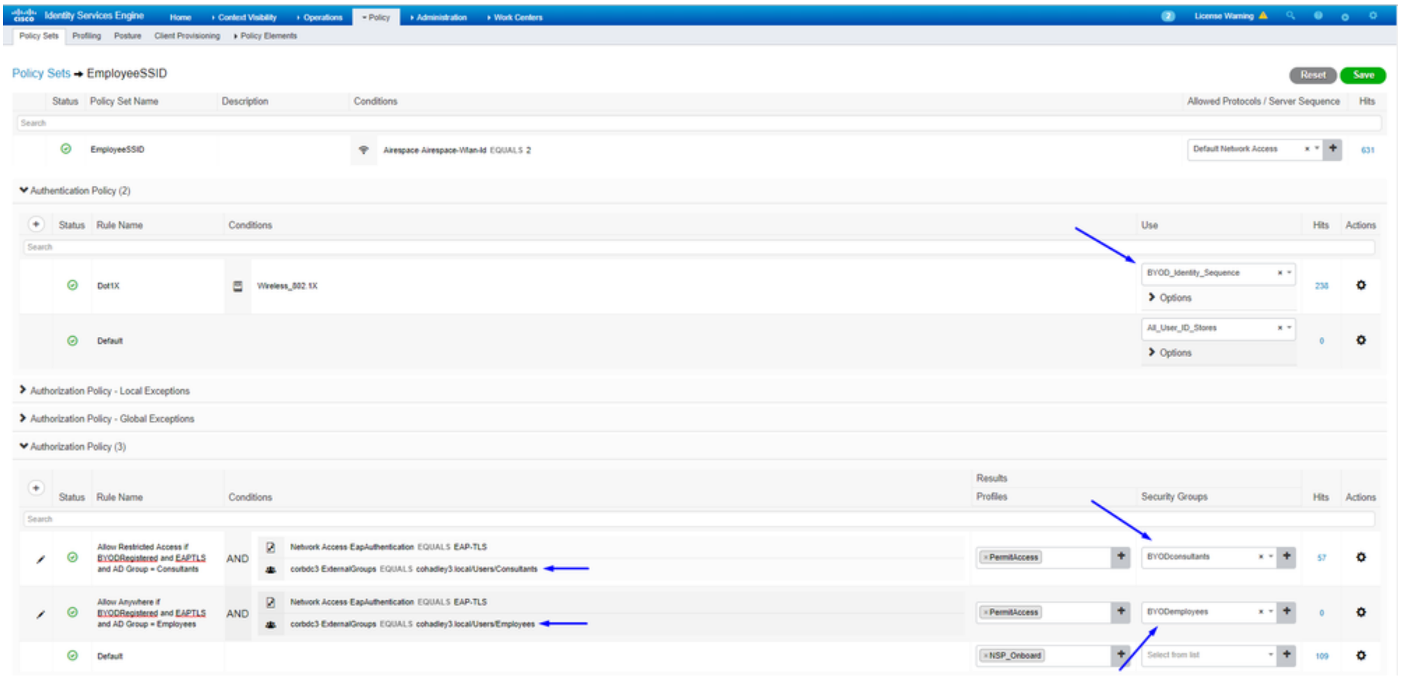
If a selected identity store cannot be accessed for authentication

● 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

Assign Wireless Users (Employees and Consultants) an Appropriate SGT

Name	Username	AD Group	SG	SGT
Jason Smith	jsmith	Consultants	BYODconsultants	15
Sally Smith	ssmith	Employees	BYODemployees	7
n/a	n/a	n/a	TrustSec_Devices	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	⚙

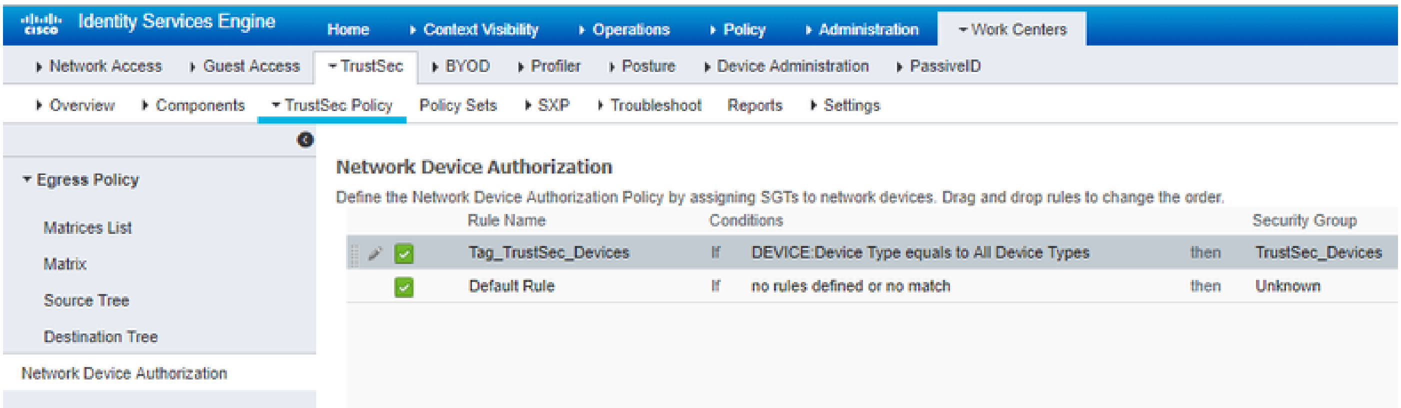
Authorization Policy - Local Exceptions

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	⚙

Assign SGTs to the Actual Devices (Switch and WLC)



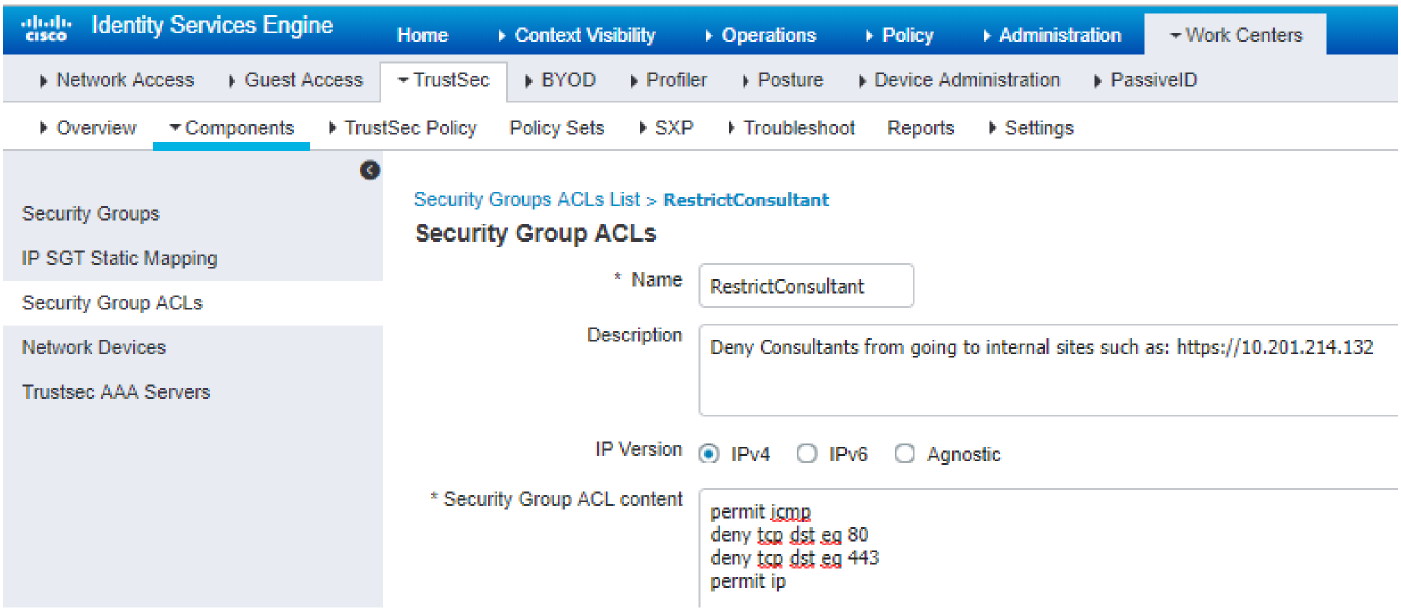
Network Device Authorization

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

Define SGACLs to Specify the Egress Policy

Allow Consultants to access anywhere external, but restrict internal:



Security Groups ACLs List > **RestrictConsultant**

Security Group ACLs

* Name: RestrictConsultant

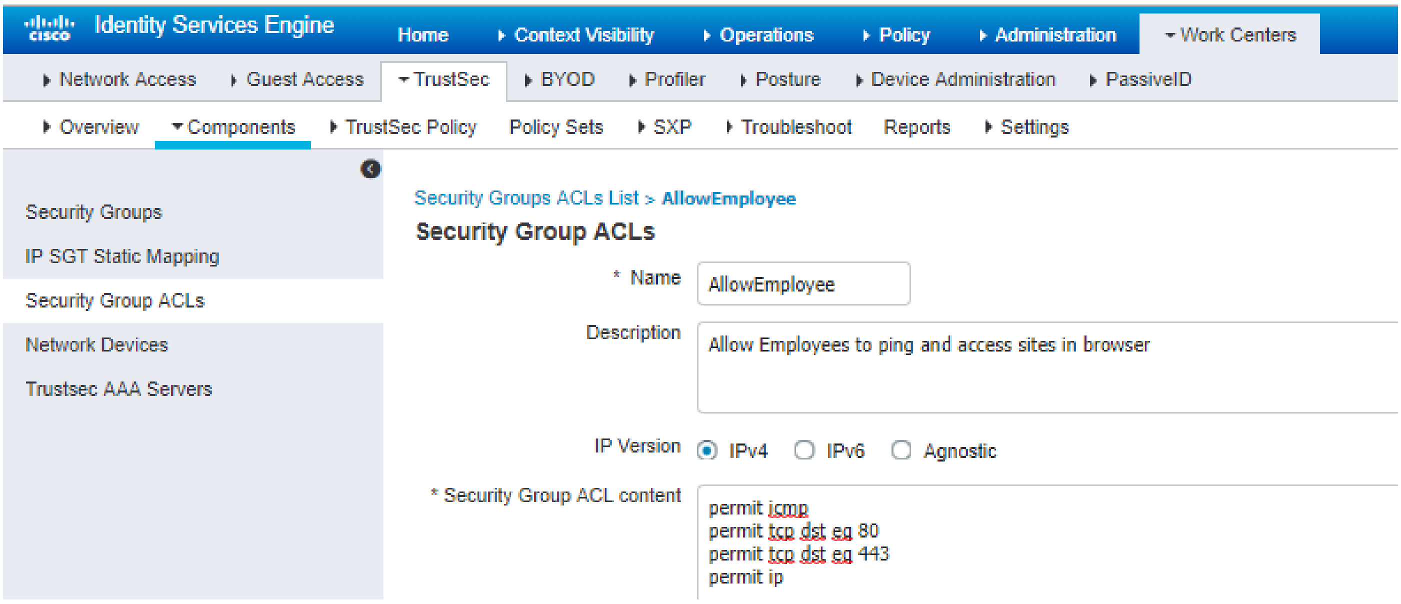
Description: Deny Consultants from going to internal sites such as: https://10.201.214.132

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

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

Allow Employees to access anywhere external and anywhere internal:



Security Groups ACLs List > **AllowEmployee**

Security Group ACLs

* Name: AllowEmployee

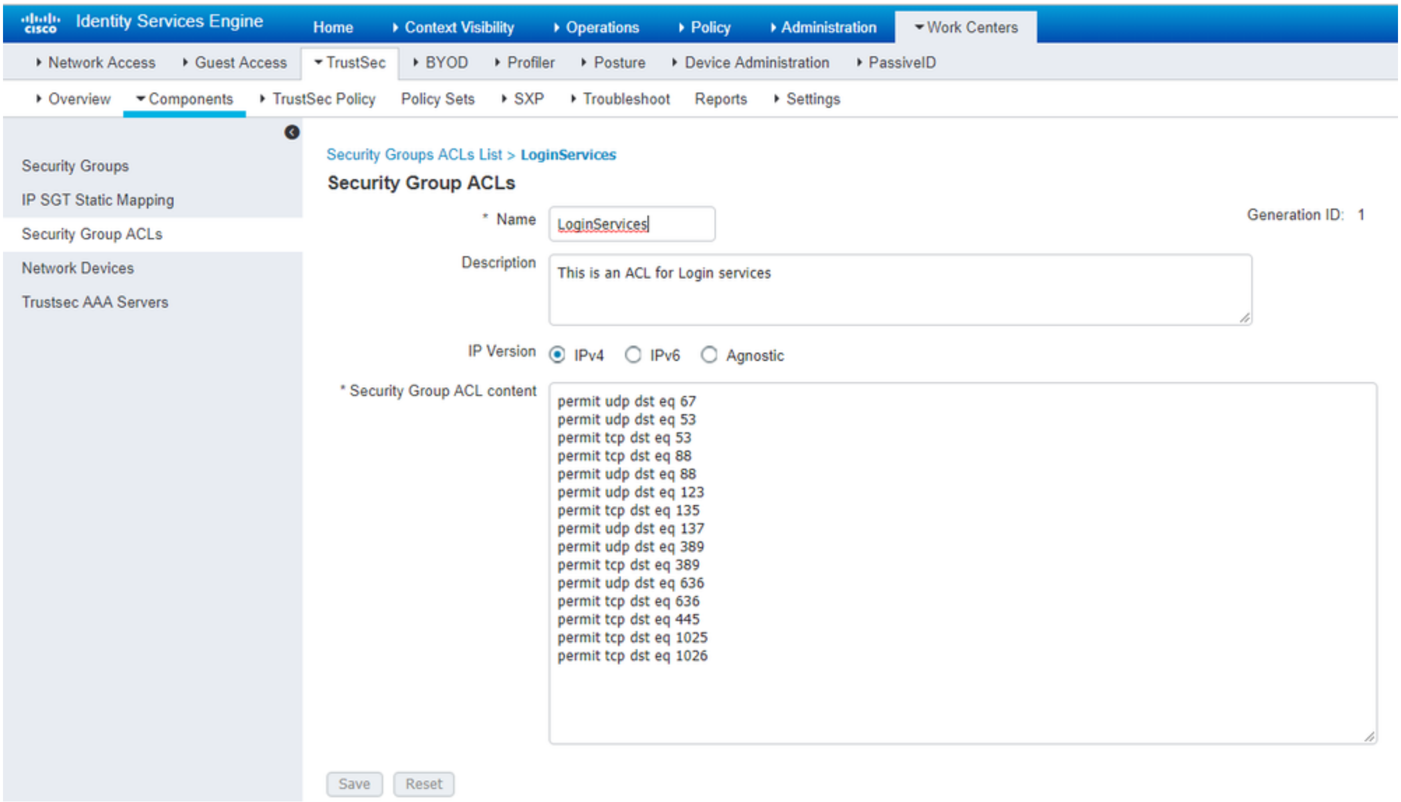
Description: Allow Employees to ping and access sites in browser

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

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

Allow other devices access to basic services (Optional):



Security Groups ACLs List > LoginServices

Security Group ACLs

* Name: LoginServices

Generation ID: 1

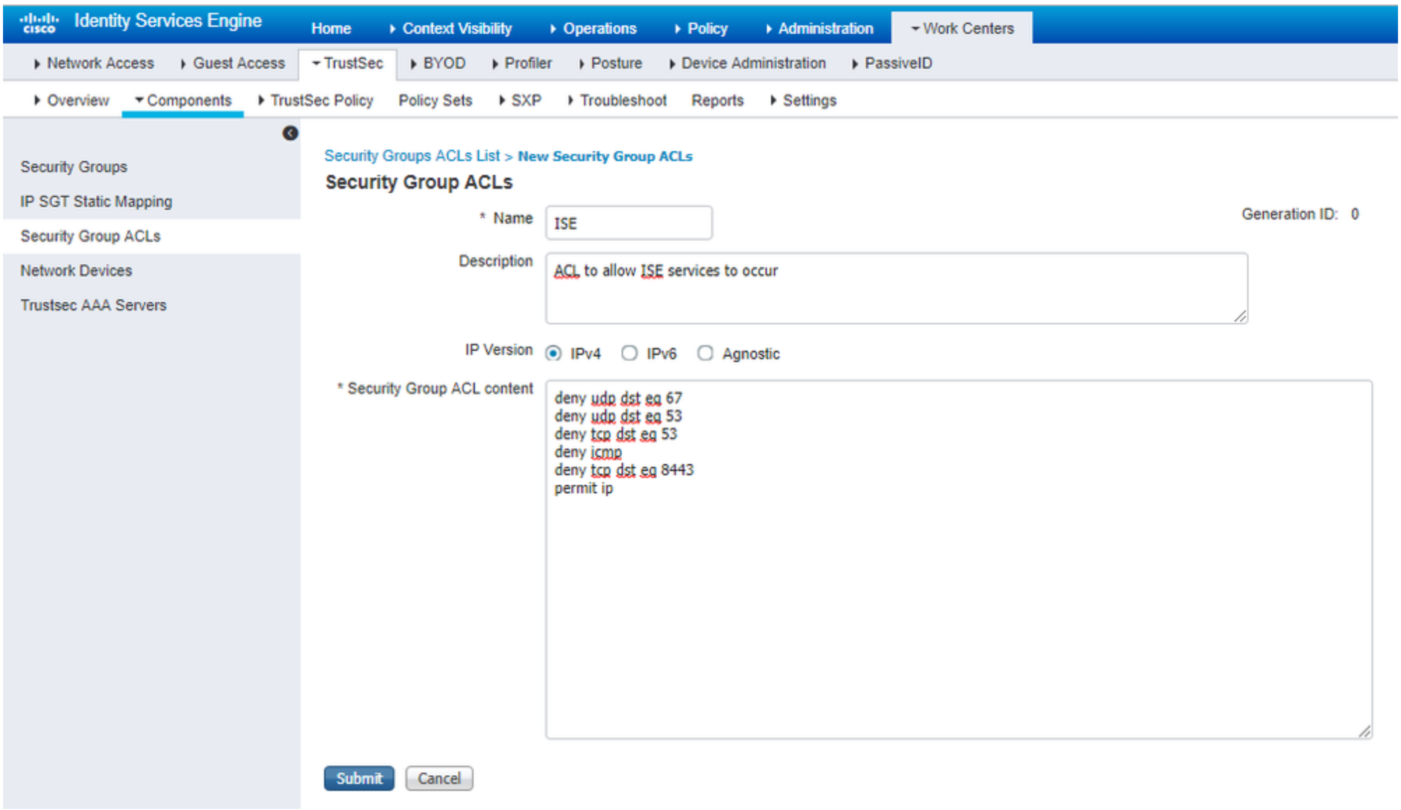
Description: This is an ACL for Login services

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
```

Redirect all end users to Cisco ISE (for BYOD portal redirection). Do not include DNS, DHCP, ping, or WebAuth traffic as those cannot go to 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

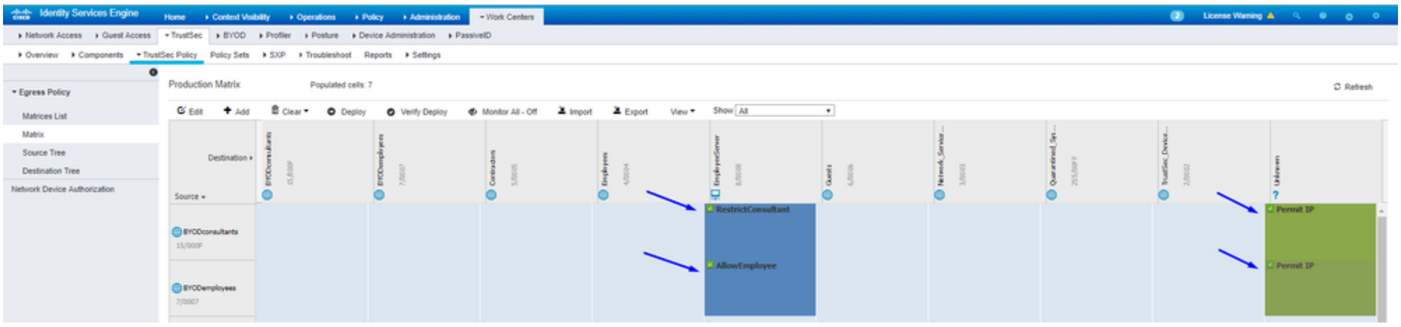
* Security Group ACL content

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

Enforce Your ACLs on the TrustSec Policy Matrix in Cisco ISE

Allow Consultants to access anywhere external, but restrict internal web servers, such as https://10.201.214.132

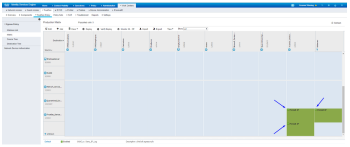
Allow Employees to access anywhere external and allow internal web servers:



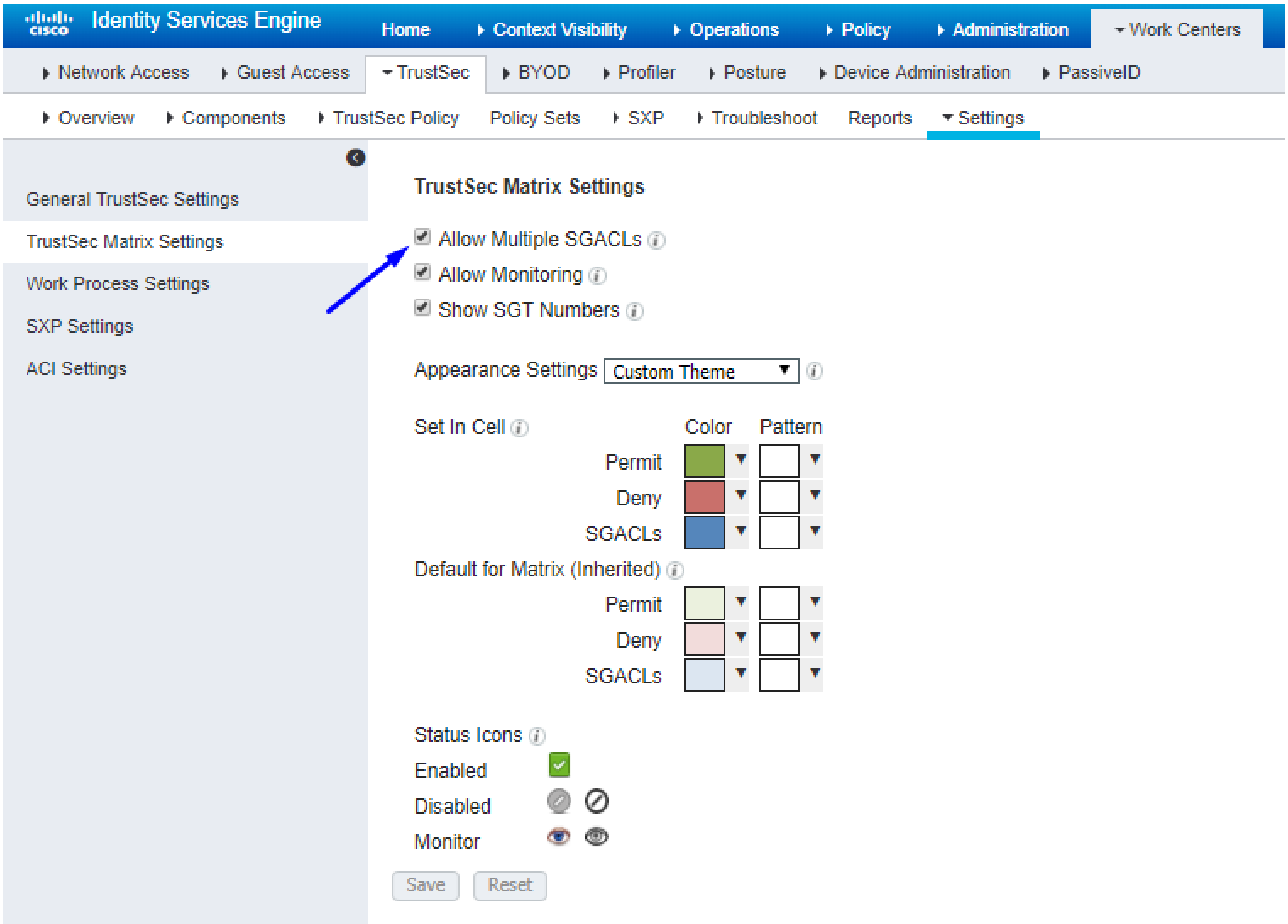
Production Matrix Populated cells: 7

Show All

Source ▾ / Destination ▸	BYODconsultants 15/000F	BYODemployees 7/0007	Contractors 5/0005	Employees 4/0004	EmployeeServer 8/0008	Guests 6/0006	Network_Service... 3/0003	Quarantined_Sys... 255/00FF	TrustSec_Device... 2/0002	Unknown
BYODconsultants 15/000F					RestrictConsultant					Permit IP
BYODemployees 7/0007					AllowEmployee					Permit IP

Allow management traffic (SSH, HTTPS, and CAPWAP) to/from your devices on the network (switch and WLC) so you do not lose SSH or HTTPS access once you deploy Cisco TrustSec: 

Enable Cisco ISE to 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	🟦	□

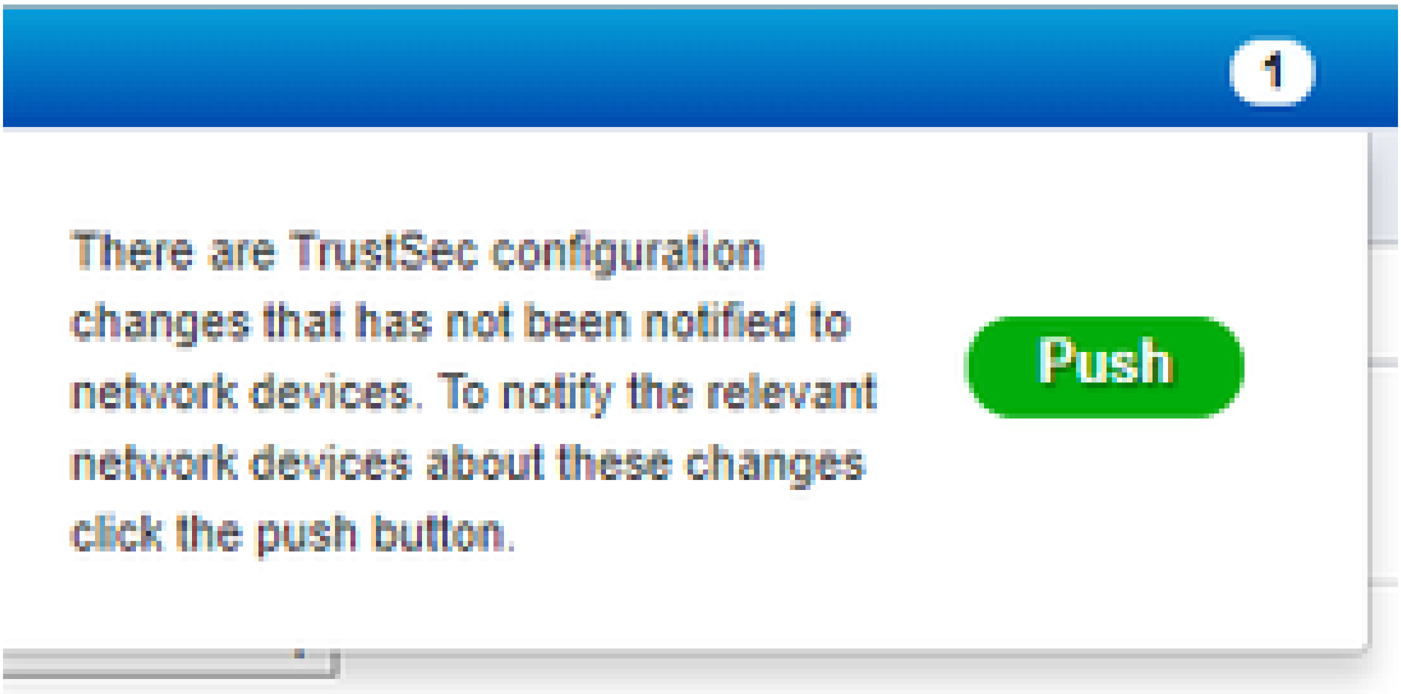
Status Icons

Enabled ✓

Disabled ⊘

Monitor 👁

Click Push in the top-right corner of Cisco ISE, to push your configuration down to your devices. You need to do this again later as well:



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.

Configure TrustSec on Catalyst Switch

Configure Switch to Use Cisco TrustSec for AAA on Catalyst Switch

Tip: This document assumes your wireless users are already successful with BYOD by Cisco ISE before the configuration shown here.

The commands shown in bold were already configured prior to this (in order for BYOD Wireless to work with ISE).

<#root>

```
CatalystSwitch(config)#aaa new-model


CatalystSwitch(config)#aaa server radius policy-device


CatalystSwitch(config)#ip device tracking
CatalystSwitch(config)#radius server CISCOISE
```

```
CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813
```

```
CatalystSwitch(config)#aaa group server radius AAASERVER
CatalystSwitch(config-sg-radius)#server name CISCOISE
```

```
CatalystSwitch(config)#aaa authentication dot1x default group radius
CatalystSwitch(config)#cts authorization list SGLIST
CatalystSwitch(config)#aaa authorization network SGLIST group radius
```

```
CatalystSwitch(config)#aaa authorization network default group AAASERVER
```

```
CatalystSwitch(config)#aaa authorization auth-proxy default group AAASERVER
```

```
CatalystSwitch(config)#aaa accounting dot1x default start-stop group AAASERVER
```

```
CatalystSwitch(config)#aaa server radius policy-device
```

```
CatalystSwitch(config)#aaa server radius dynamic-author
CatalystSwitch(config-locsvr-da-radius)#client 10.201.214.230 server-key Admin123
```

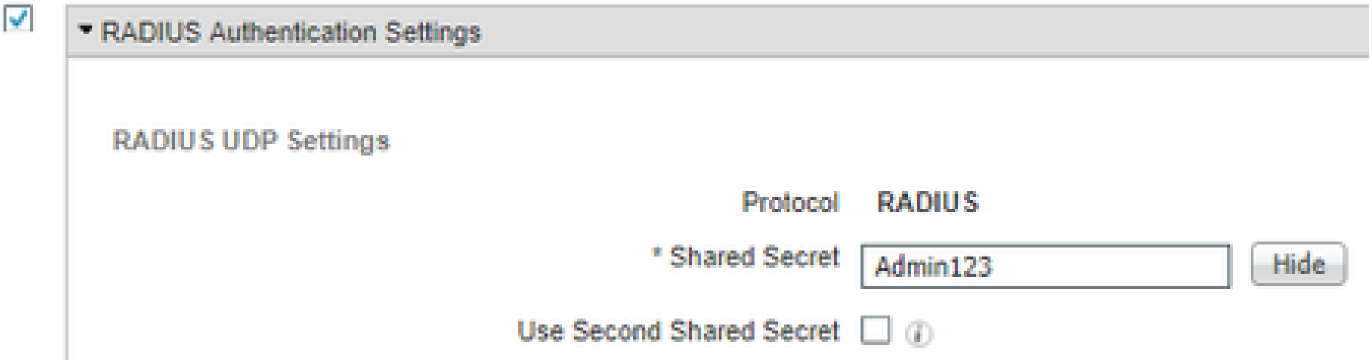
Note: The PAC key must be the same as the RADIUS Shared Secret that you specified in the **Administration > Network Devices > Add Device > RADIUS Authentication Settings** section.

<#root>

```
CatalystSwitch(config)#radius-server attribute 6 on-for-login-auth



CatalystSwitch(config)#radius-server attribute 6 support-multiple



CatalystSwitch(config)#radius-server attribute 8 include-in-access-req



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


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

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

Configure PAC Key Under the RADIUS Server to Authenticate the Switch to 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

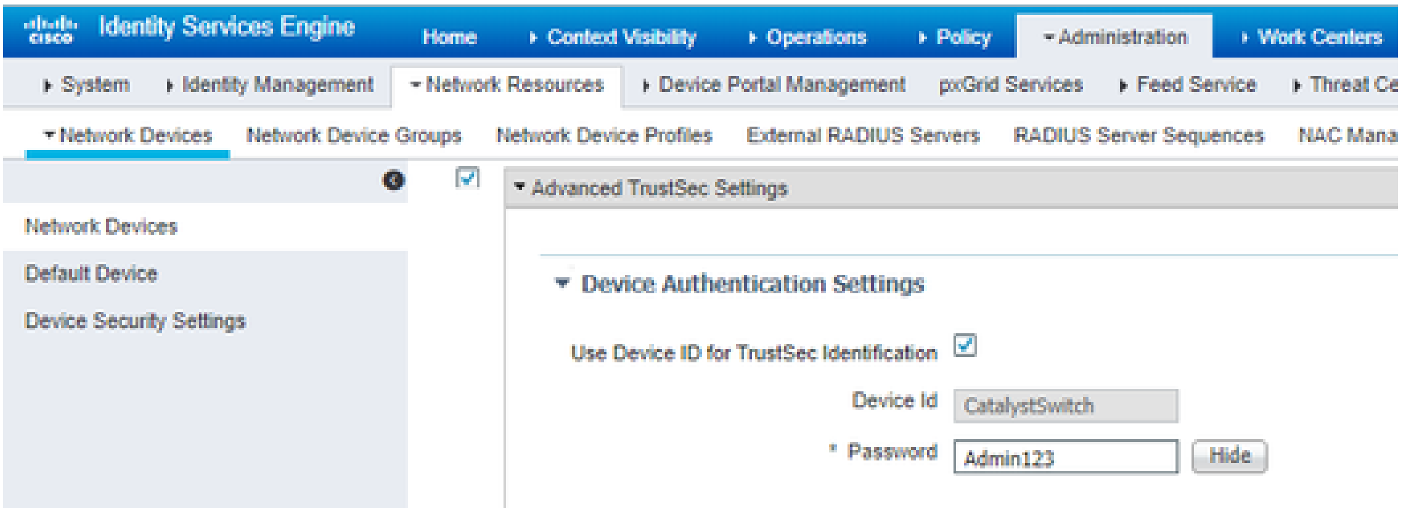
* Shared Secret Admin123

Use Second Shared Secret □

Note: The PAC key must be the same as the RADIUS Shared Secret that you specified under the **Administration > Network Devices > Add Device > RADIUS Authentication Settings** section in Cisco ISE (as shown in the screen capture).

Configure CTS Credentials to Authenticate the Switch to 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 Hide

Note: The CTS credentials must be the same as the Device ID + password that you specified in The CTS credentials must be the same as the Device ID + password that you specified in the Administration > Network Devices > Add Device > Advanced TrustSec Settings section in Cisco ISE (shown in the screen capture).

Then, refresh your PAC so it reaches out to Cisco ISE again:

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

Enable CTS Globally on Catalyst Switch

```
CatalystSwitch(config)#cts role-based enforcement
CatalystSwitch(config)#cts role-based enforcement vlan-list 1115 (choose the vlan that your end user de
```

Make a Static IP-to-SGT Mapping for the Restricted Web Servers (Optional)

That Restricted Web Server does not come through ISE for authentication ever, so you must tag it manually with the Switch CLI or ISE Web GUI, that is just one of many web servers in Cisco.

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

Verify TrustSec on Catalyst Switch

```
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: 000200B80003000100040010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352
 Refresh timer is set for 12w5d
```

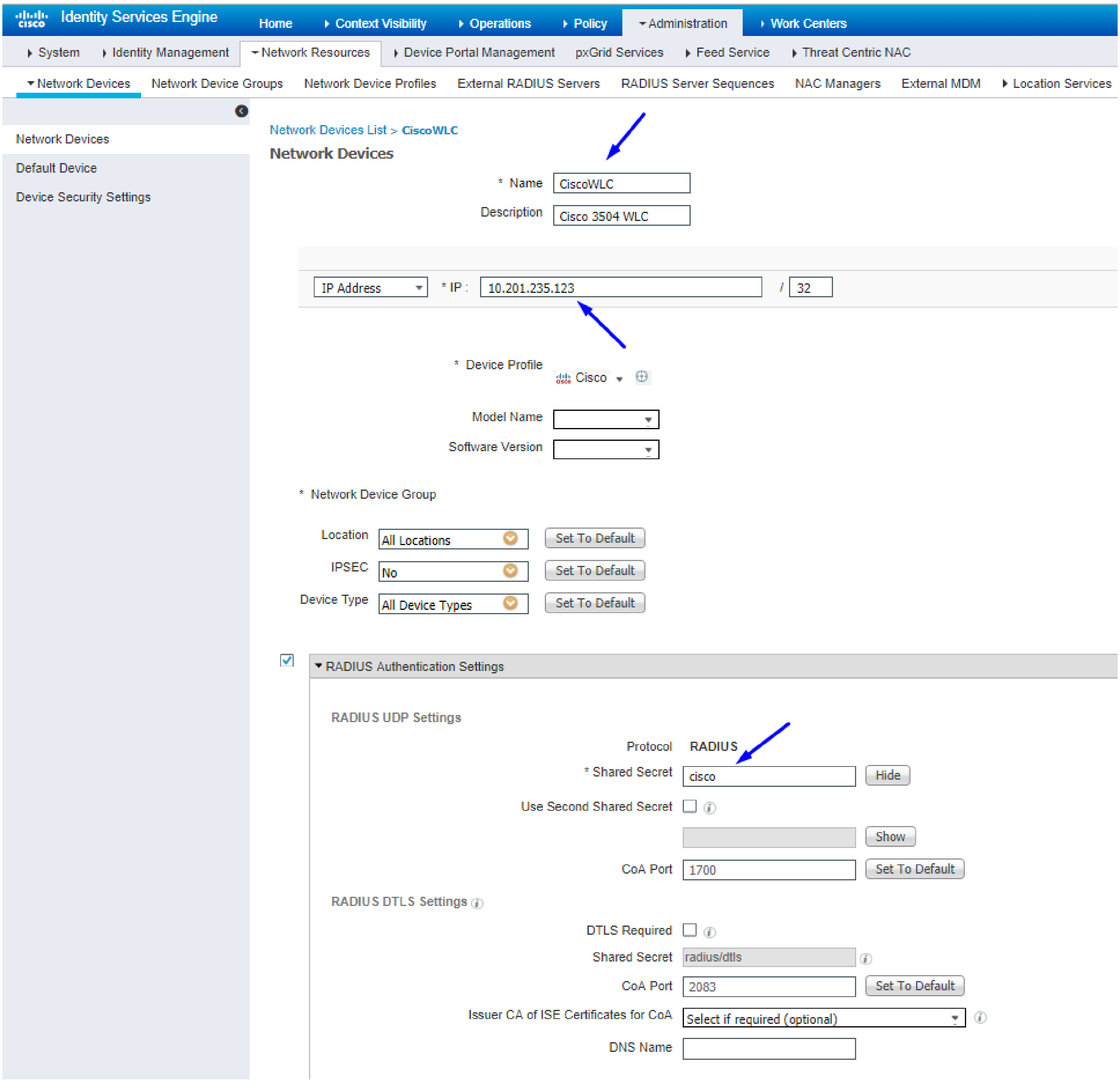
```
CatalystSwitch#cts refresh environment-data
Environment data download in progress
```

```
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
```

Configure TrustSec on WLC

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



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

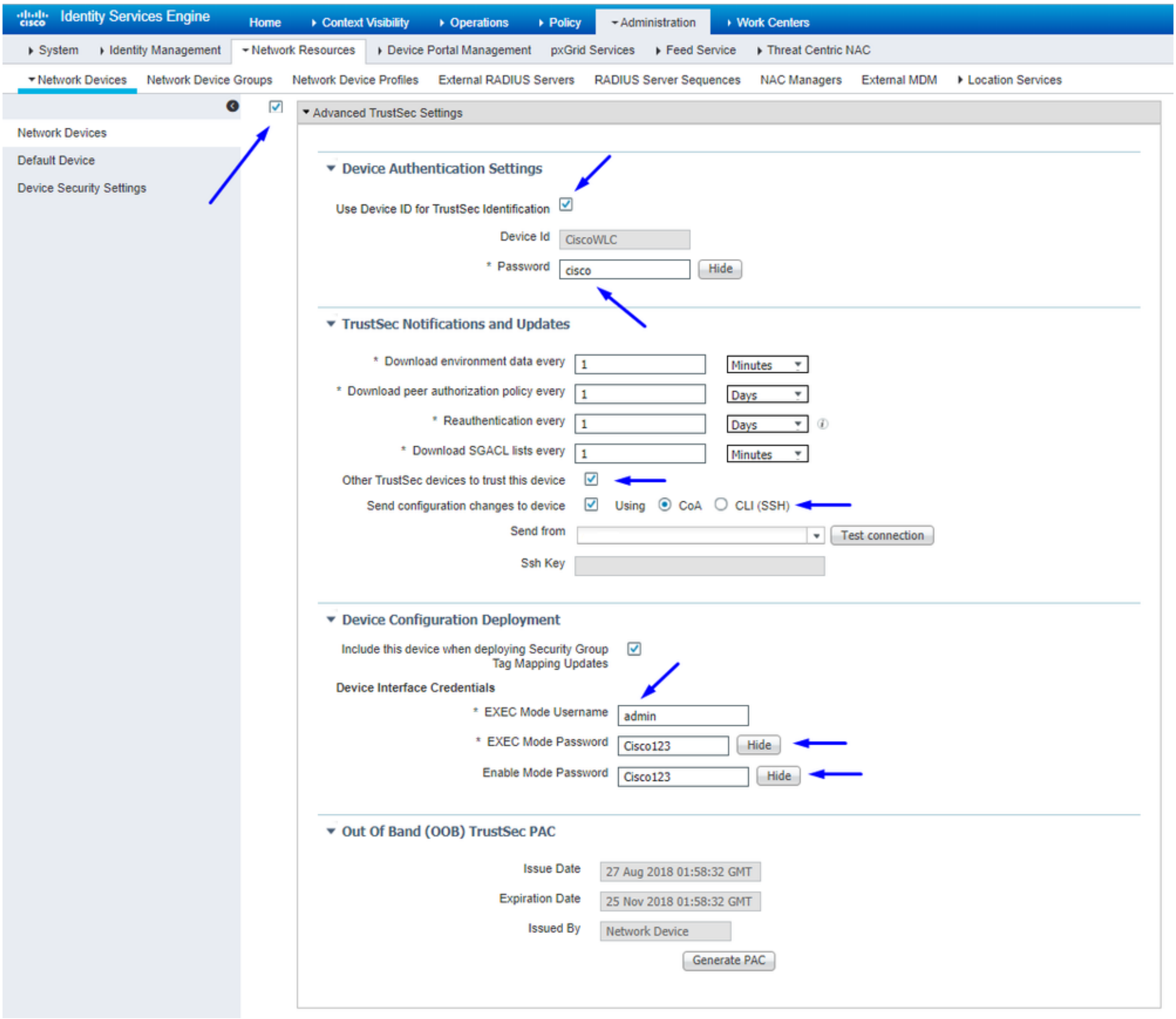
CoA Port: 2083 [Set To Default]

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

DNS Name:

Configure and Verify WLC is Added as a TrustSec Device in Cisco ISE

This step enables Cisco ISE to deploy static IP-to-SGT Mappings to the WLC. You created these mappings in the Cisco ISE Web GUI in **Work Centers > TrustSec > Components > IP SGT Static Mappings** in a previous step.



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: CiscoWLC

* Password: cisco

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:

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

Enable Mode Password: Cisco123

Out Of Band (OOB) TrustSec PAC

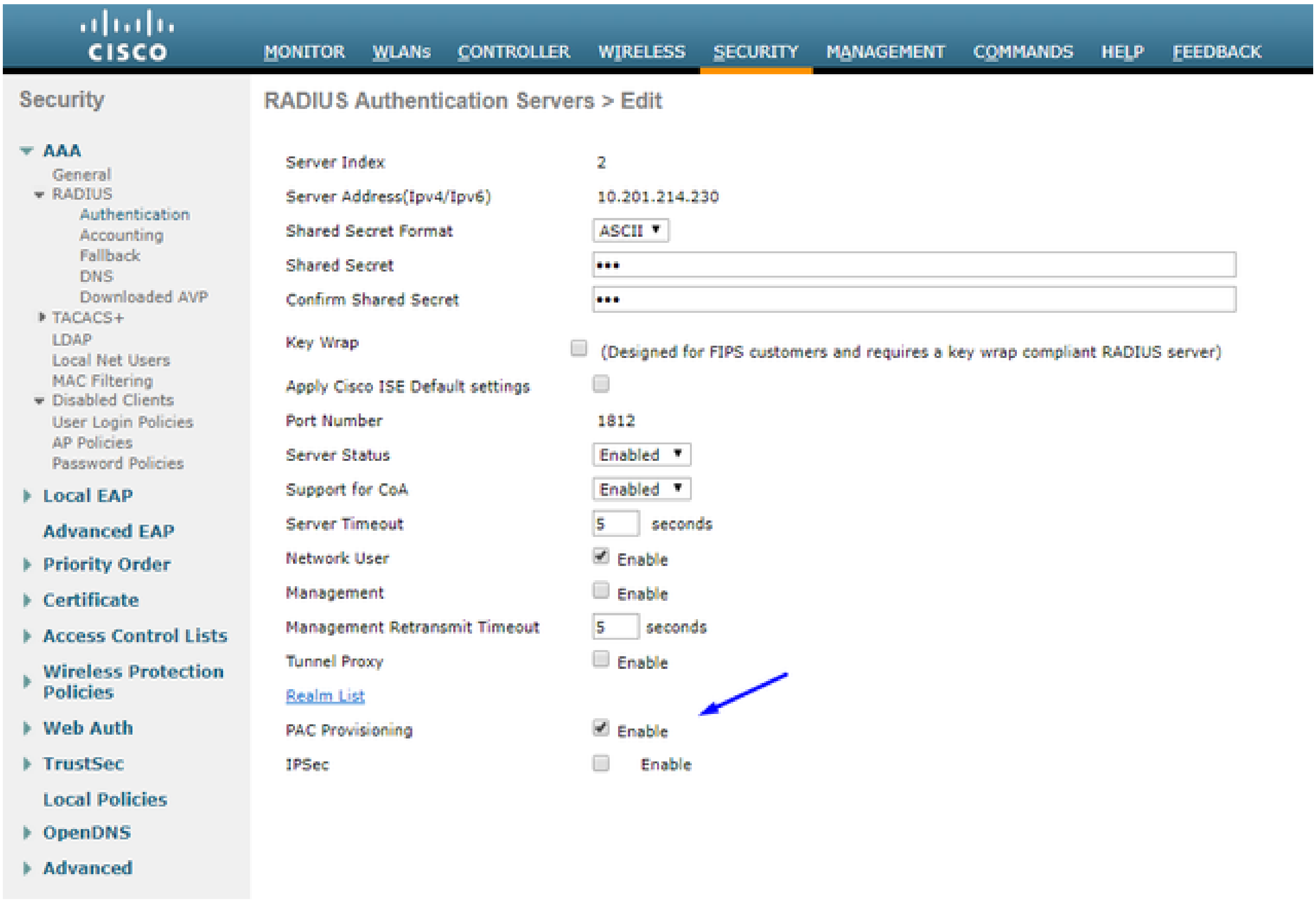
Issue Date: 27 Aug 2018 01:58:32 GMT

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

Issued By: Network Device

Note: We use this Device Id and Password in a later step, in Security > TrustSec > General in the WLC Web UI.

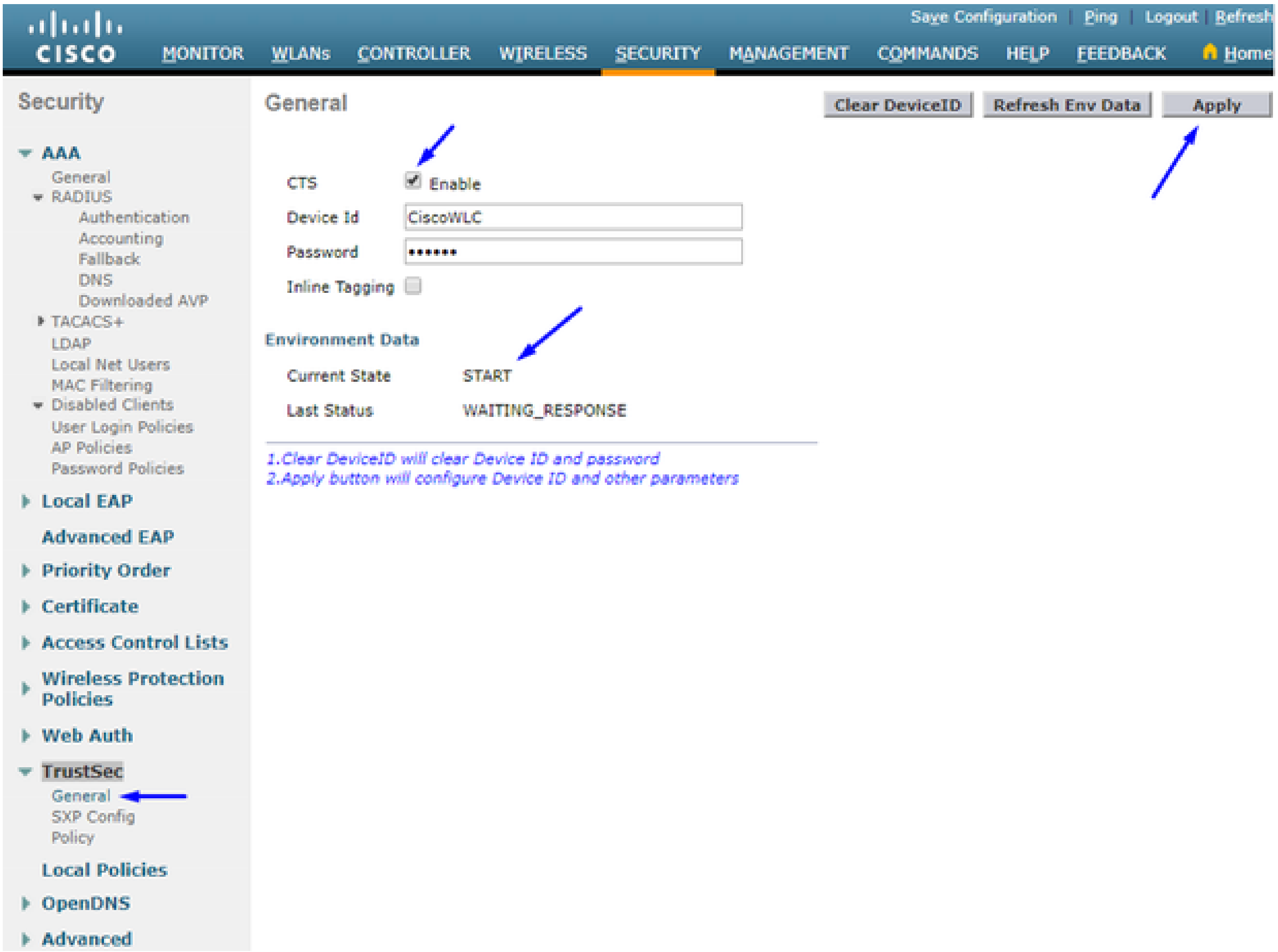
Enable PAC Provision of WLC



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

Enable TrustSec on WLC



General

CTS ☑ Enable

Device Id CiscoWLC

Password ••••••

Inline Tagging □

Environment Data

Current State START

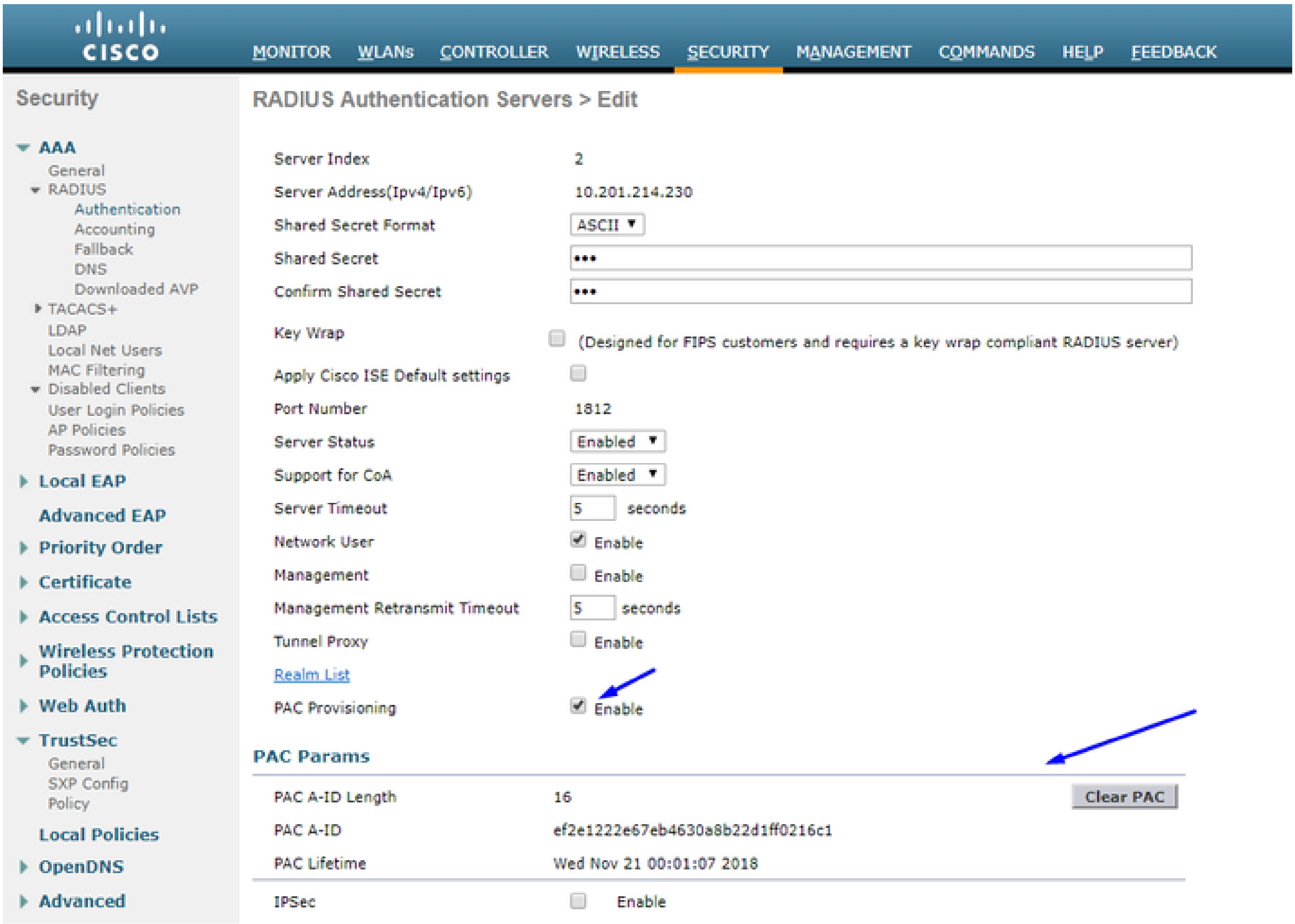
Last Status WAITING_RESPONSE

1.Clear DeviceID will clear Device ID and password
2.Apply button will configure Device ID and other parameters

Note: The CTS Device Id and Password must be the same as the Device Id and Password that you specified in Administration > Network Devices > Add Device > Advanced TrustSec Settings section in Cisco ISE.

Verify PAC has been Provisioned on WLC

You see the WLC has the PAC provisioned successfully after you click Refresh Env Data (you do this in this step):



RADIUS Authentication Servers > Edit

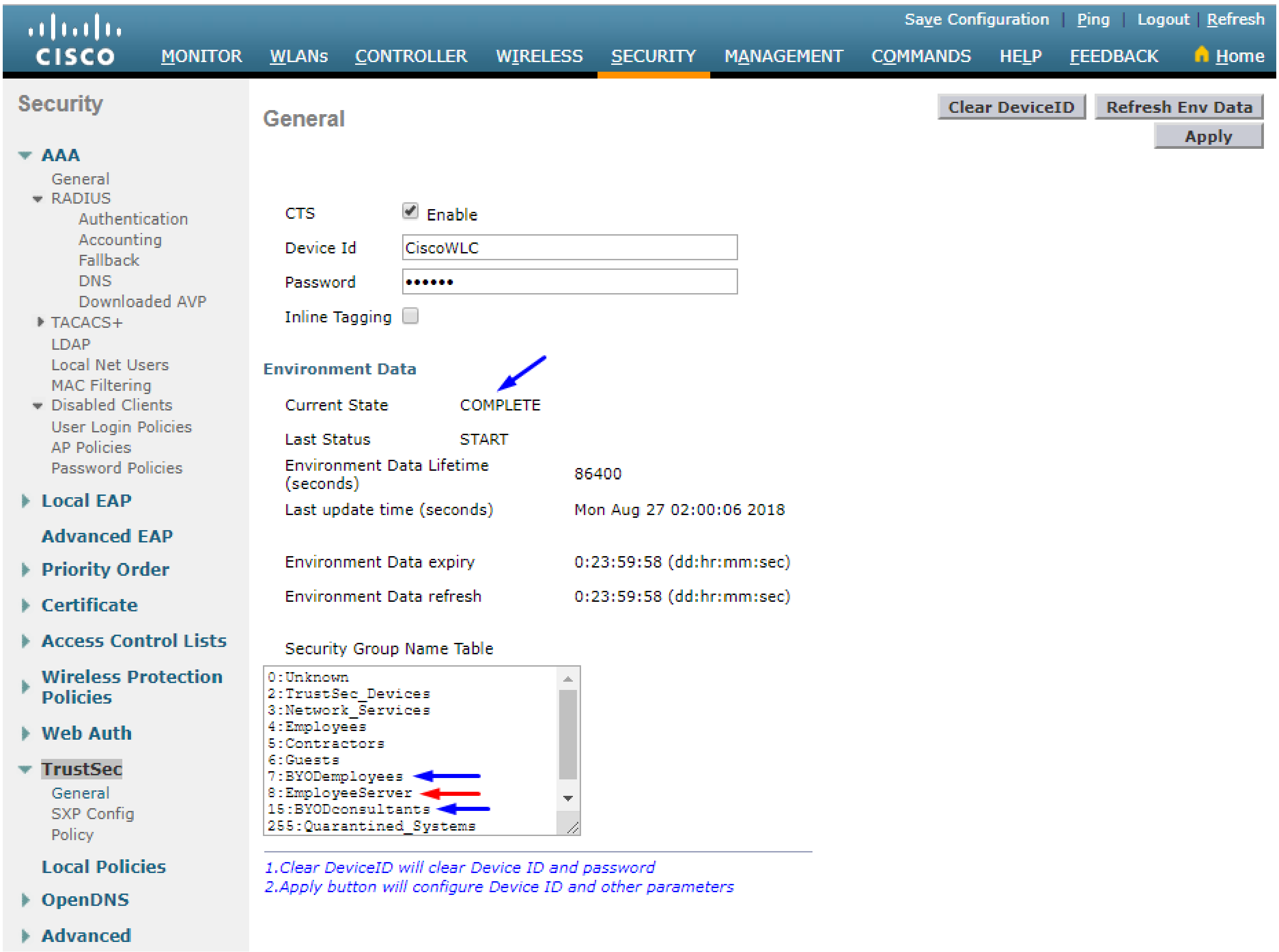
Server Index	2
Server Address(Ipv4/Ipv6)	10.201.214.230
Shared Secret Format	ASCII ▼
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	□
Port Number	1812
Server Status	Enabled ▼
Support 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

Download CTS Environment Data from Cisco ISE to WLC

After you click Refresh Env Data, your WLC downloads your SGTs.



General

CTS	☑ Enable
Device Id	CiscoWLC
Password	••••••
Inline Tagging	□

Environment Data

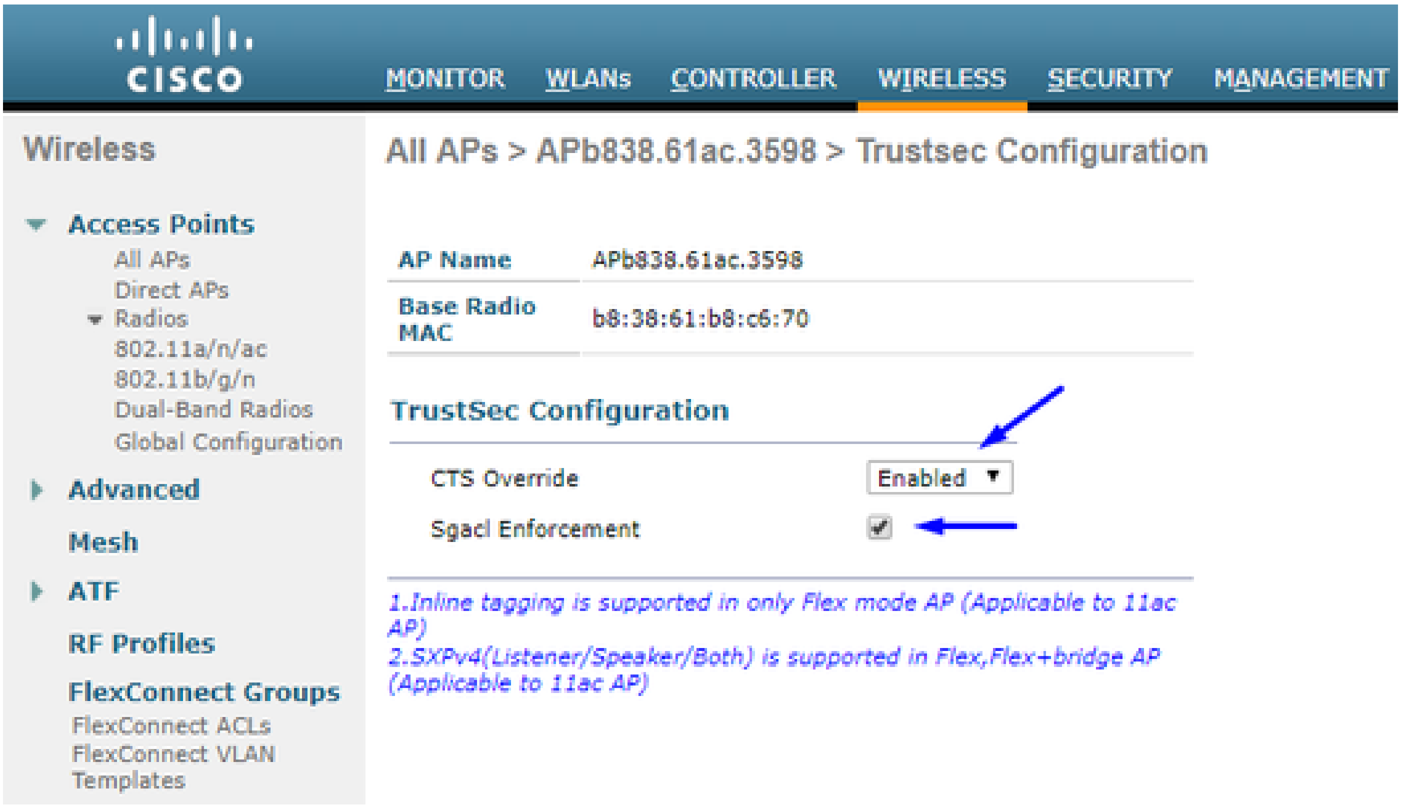
Current State	COMPLETE
Last Status	START
Environment Data Lifetime (seconds)	86400
Last update time (seconds)	Mon Aug 27 02:00:06 2018
Environment Data expiry	0:23:59:58 (dd:hr:mm:sec)
Environment Data refresh	0:23:59:58 (dd:hr:mm:sec)

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

Enable SGACL Downloads and Enforcement on Traffic



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

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

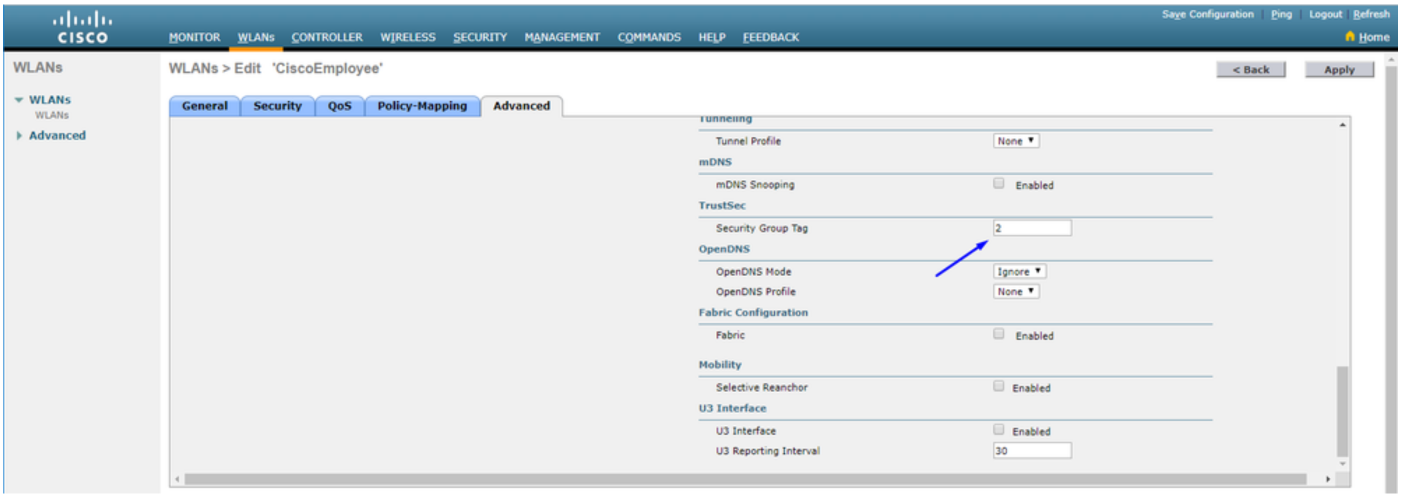
TrustSec Configuration

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)

Assign WLC and Access Point the SGT of 2 (TrustSec_Devices)

Give the WLC+WLAN an SGT of 2 (TrustSec_Devices) to allow traffic (SSH, HTTPS, and CAPWAP) to/from the WLC + AP through the switch.



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

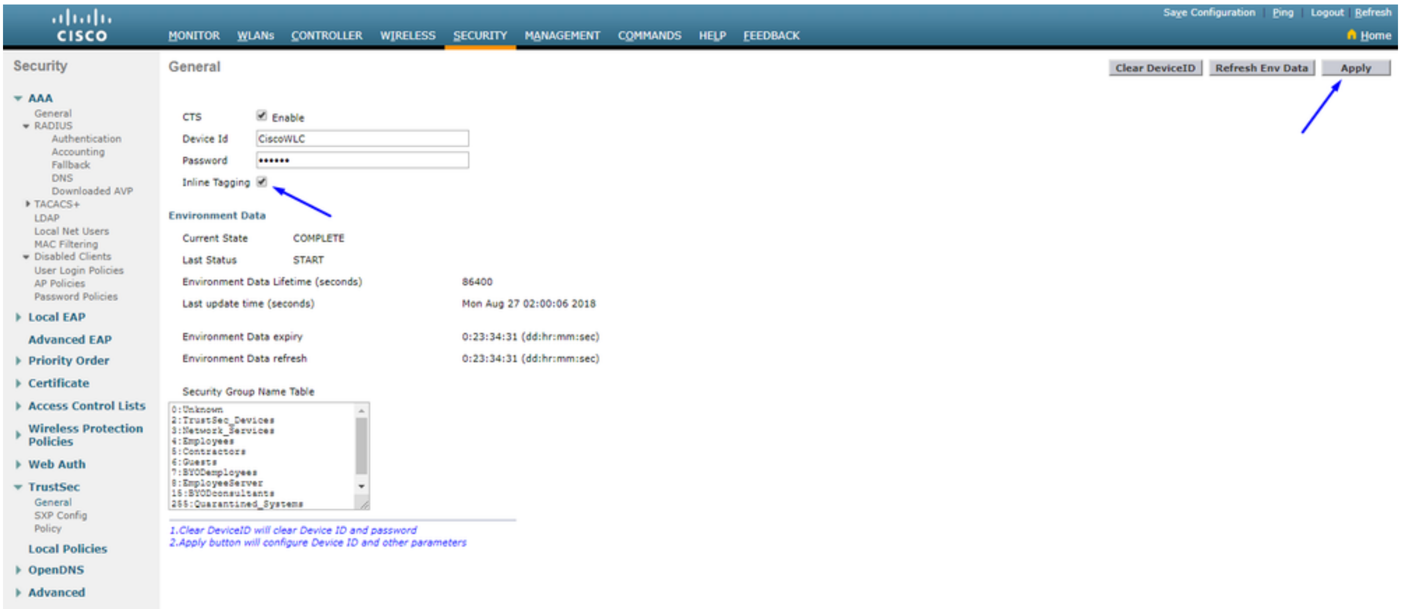
Selective Reanchor: □ Enabled

U3 Interface

U3 Interface: □ Enabled

U3 Reporting Interval: 30

Enable Inline Tagging on WLC



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)

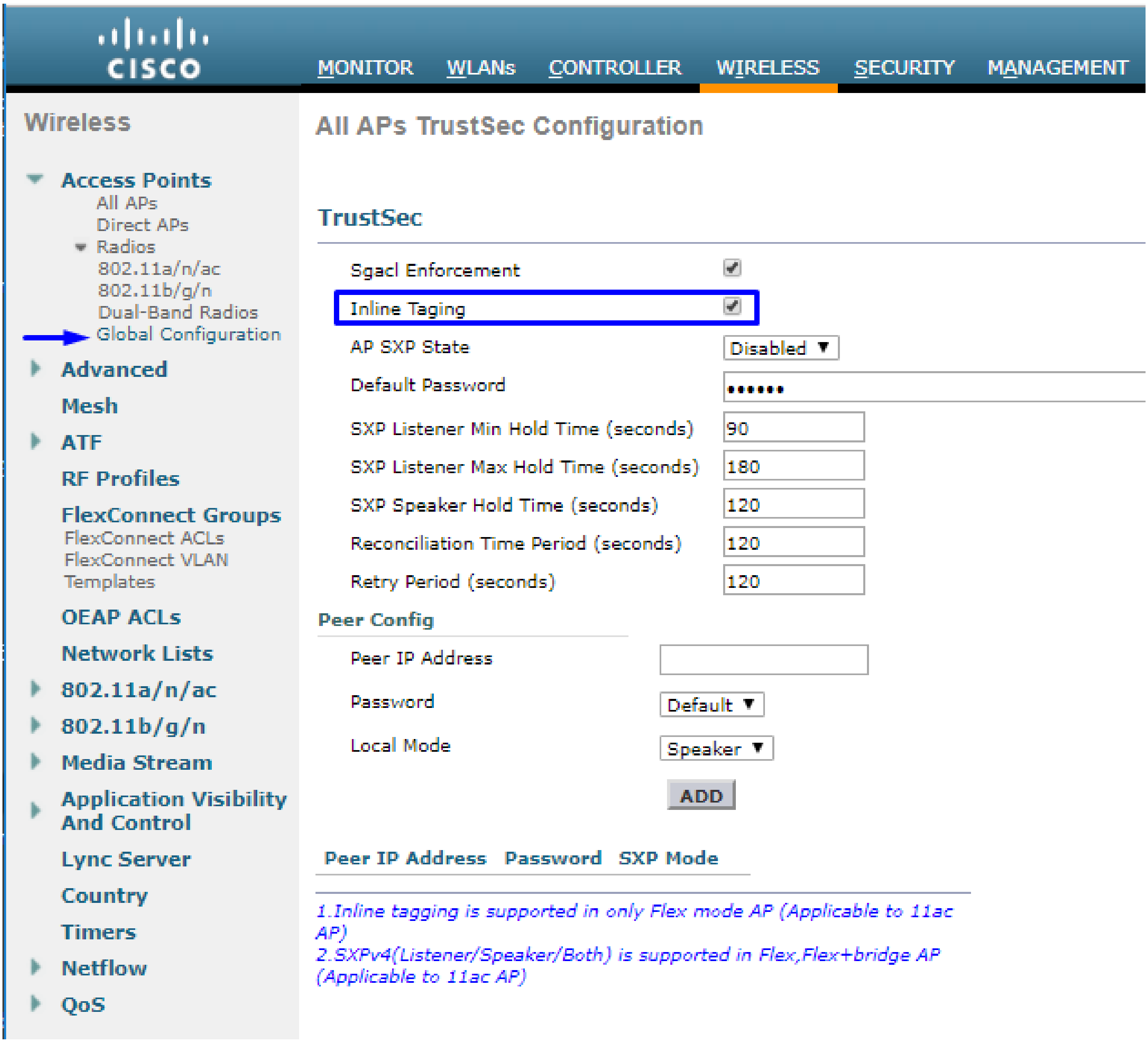
Environment Data refresh: 0:23:34:31 (dd:hr:mm:sec)

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

Under **Wireless > Access Points > Global Configuration** scroll down and select **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

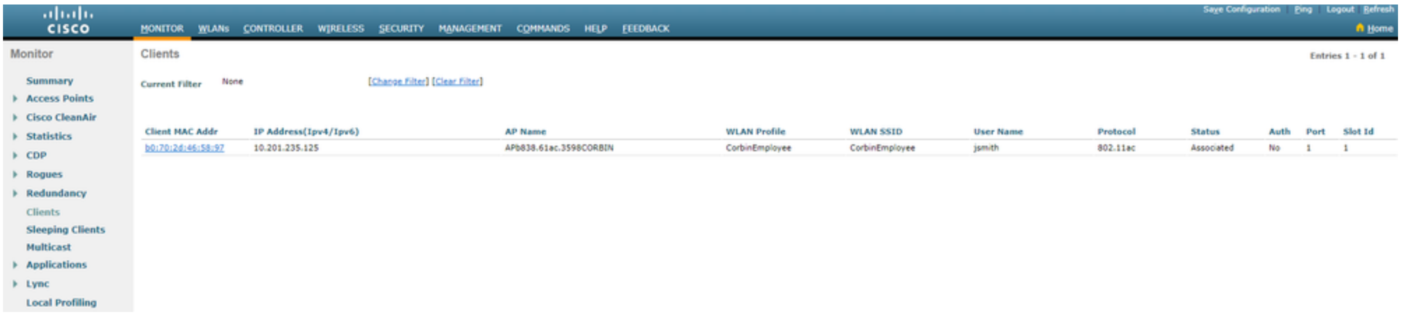
1.Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
2.SXPv4(Listener/Speaker/Both) is supported in Flex,Flex+bridge AP (Applicable to 11ac AP)

Enable Inline Tagging on Catalyst Switch

<#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
```

Verify



Clients

Entries 1 - 1 of 1

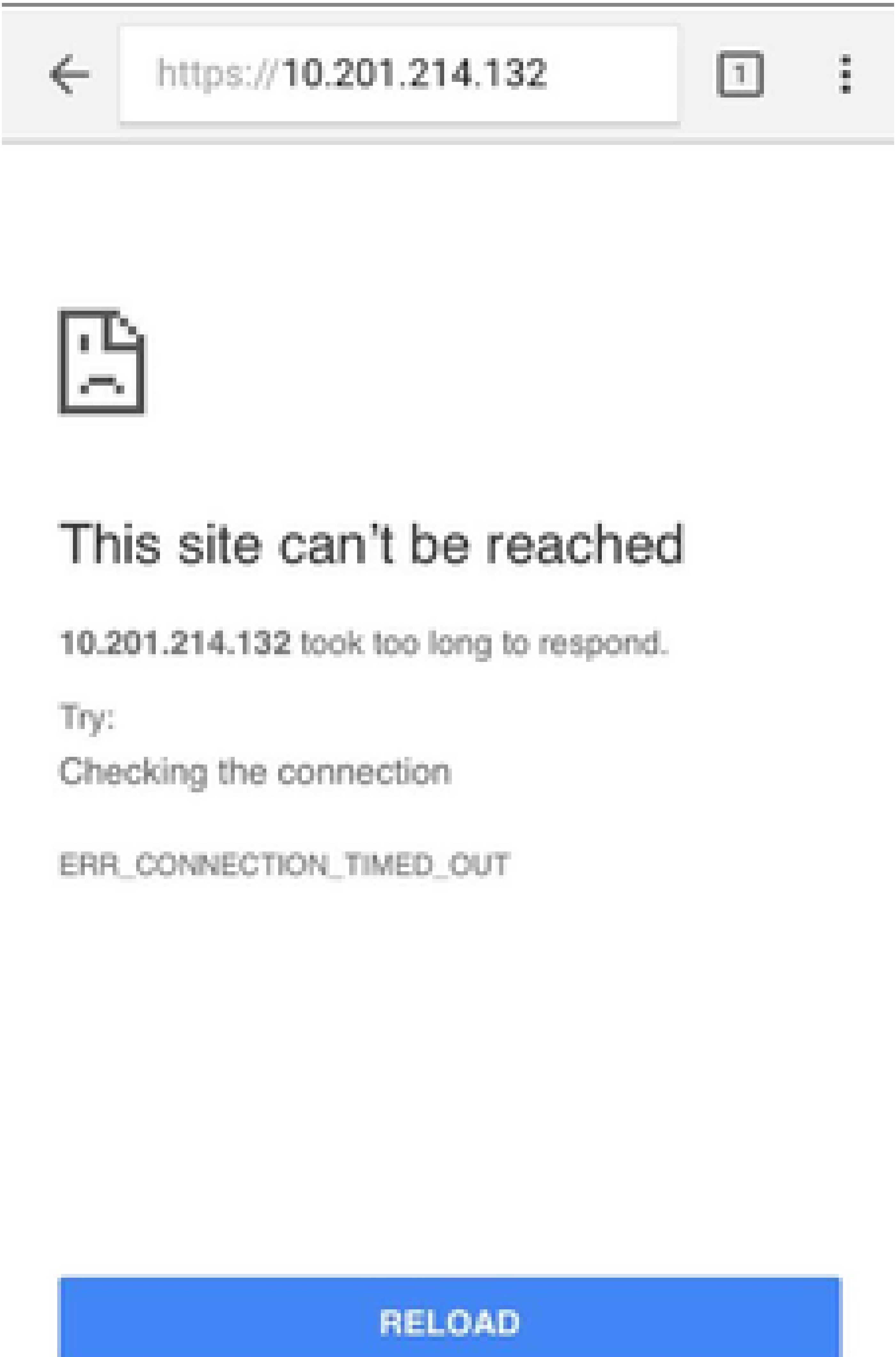
Current Filter None

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
Egress IPv4 SGACL Drop (454): 10 frames
Egress IPv6 SGACL Drop (455): 0 frames
Egress IPv4 SGACL Cell Drop (456): 0 frames
Egress IPv6 SGACL Cell Drop (457): 0 frames
```

Tip: If you use a Cisco ASR, Nexus, or Cisco ASA instead, the document listed here can help verify your SGT taggings are enforced: TrustSec Troubleshooting Guide.

Authenticate to wireless with username jsmith password Admin123 - you encounter the deny ACL in the switch:



https://10.201.214.132

This site can't be reached

10.201.214.132 took too long to respond.

Try:

Checking the connection

ERR_CONNECTION_TIMED_OUT