Configurar TrustSec (SGTs) com ISE (marcação em linha)

Contents

Introdução

Este documento descreve como configurar e verificar o TrustSec em um Switch Catalyst e um Wireless LAN Controller com o Identity Services Engine.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico dos componentes do Cisco TrustSec (CTS)
- Conhecimento básico da configuração CLI dos switches Catalyst
- Conhecimento básico da configuração da GUI dos Cisco Wireless LAN Controllers (WLC)
- Experiência com a configuração do Identity Services Engine (ISE)

Requisitos

Você deve ter o Cisco ISE implantado em sua rede, e os usuários finais devem autenticar-se no Cisco ISE com 802.1x (ou outro método) quando se conectam com fio ou sem fio. O Cisco ISE atribui ao tráfego uma Security Group Tag (SGT) depois que eles se autenticam em sua rede sem fio.

Em nosso exemplo, os usuários finais são redirecionados para o portal do Cisco ISE Bring Your Own Device (BYOD) e recebem um certificado para que possam acessar com segurança a rede sem fio com o Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) depois que concluírem as etapas do portal BYOD.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Cisco Identity Services Engine, versão 2.4
- Switch Cisco Catalyst 3850, versão 3.7.5E
- Cisco WLC, versão 8.5.120.0
- Ponto de acesso sem fio Cisco Aironet no modo local

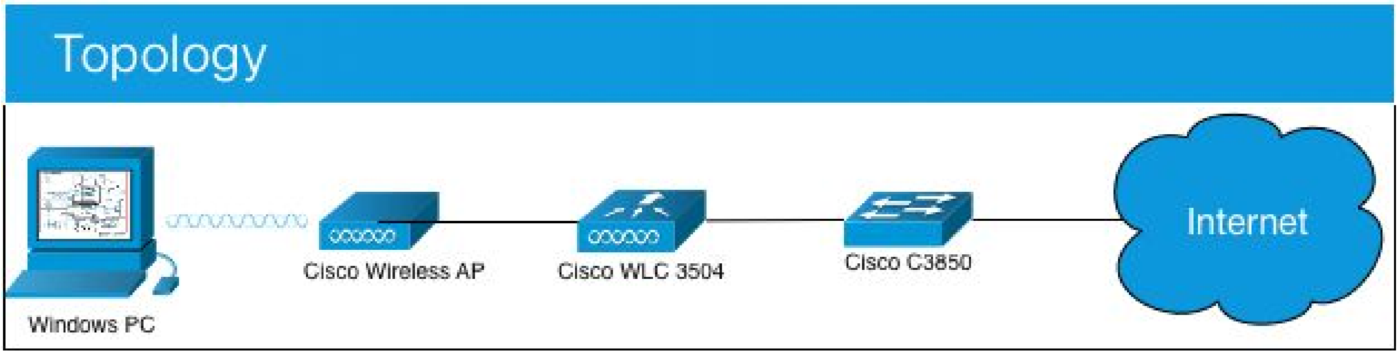
Antes da implantação do Cisco TrustSec, verifique se o switch Cisco Catalyst e/ou os modelos Cisco WLC+AP + versão de software têm suporte para:

- Tags de grupos TrustSec/Security
- Inline Tagging (caso contrário, você pode usar o SXP em vez do Inline Tagging)
- Mapeamentos estáticos de IP para SGT (se necessário)
- Mapeamentos estáticos de sub-rede para SGT (se necessário)
- Mapeamentos estáticos de VLAN para SGT (se necessário)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Neste exemplo, a WLC marca os pacotes como SGT 15, se de um consultor, e + SGT 7, se de um funcionário.

O switch negará esses pacotes se eles forem do SGT 15 ao SGT 8 (os consultores não podem acessar servidores marcados como SGT 8).

O switch permite esses pacotes se forem do SGT 7 ao SGT 8 (os funcionários podem acessar servidores marcados como SGT 8).

Meta

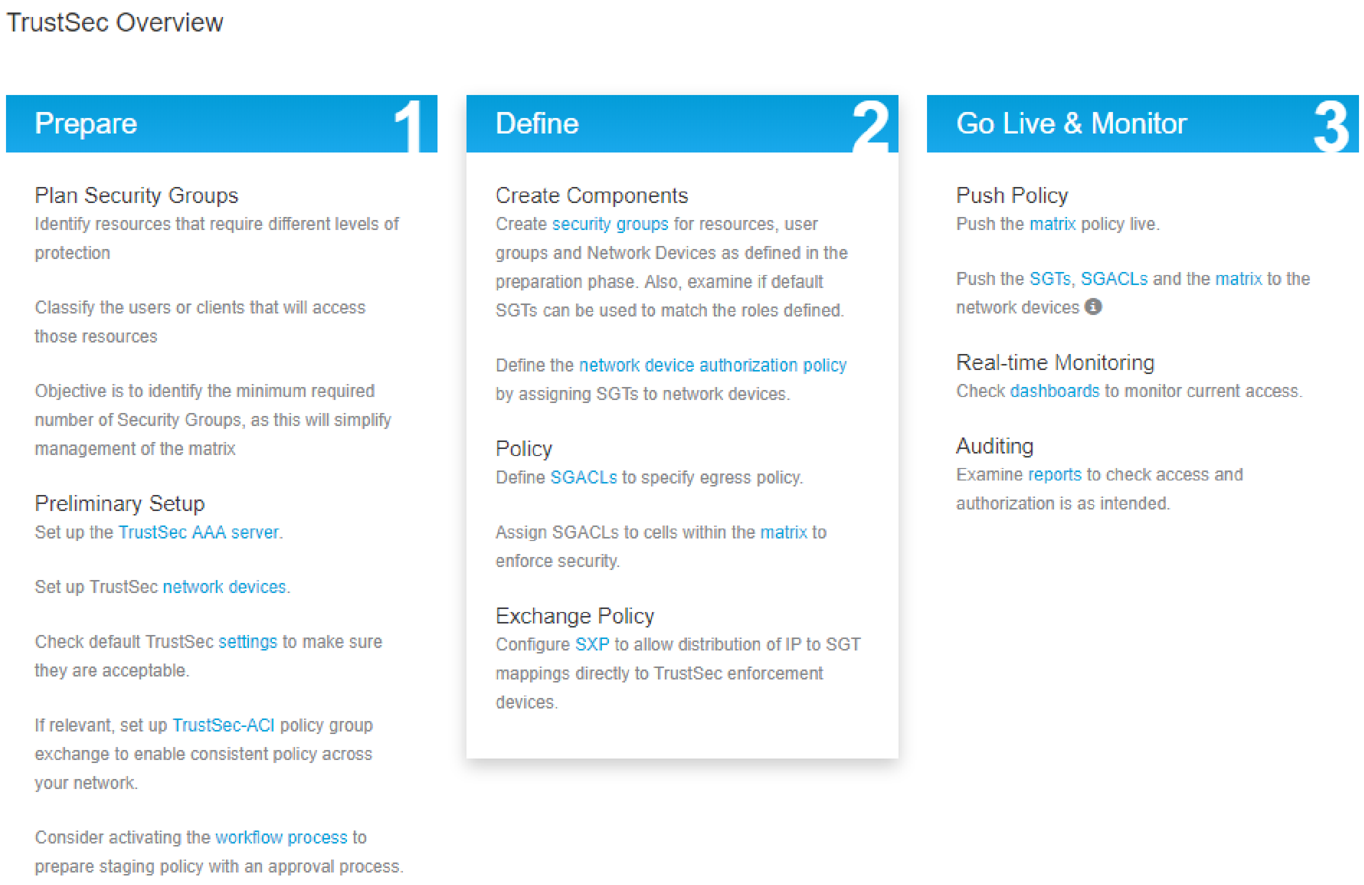
Permitir que qualquer pessoa acesse GuestSSID.
Permita que os consultores acessem o SSID do funcionário, mas com acesso restrito.
Permita que os funcionários acessem o SSID do funcionário com acesso total.

Dispositivo	Endereço IP	VLAN
ISE	10.201.214.230	463
Catalyst Switch	10.201.235.102	1115
WLC	10.201.214.229	463
Ponto de acesso	10.201.214.138	455

Nome	Nome de usuário	Grupo AD	SG	SGT
Jason Smith	jsmith	Consultores	Consultores de consumerização de TI	15
Sally Smith	smith	Funcionários	Funcionários adeptos da consumerização de TI	7
n/a	n/a	n/a	TrustSec_Devices	2

Configurações

Configurar o TrustSec no 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 ℹ

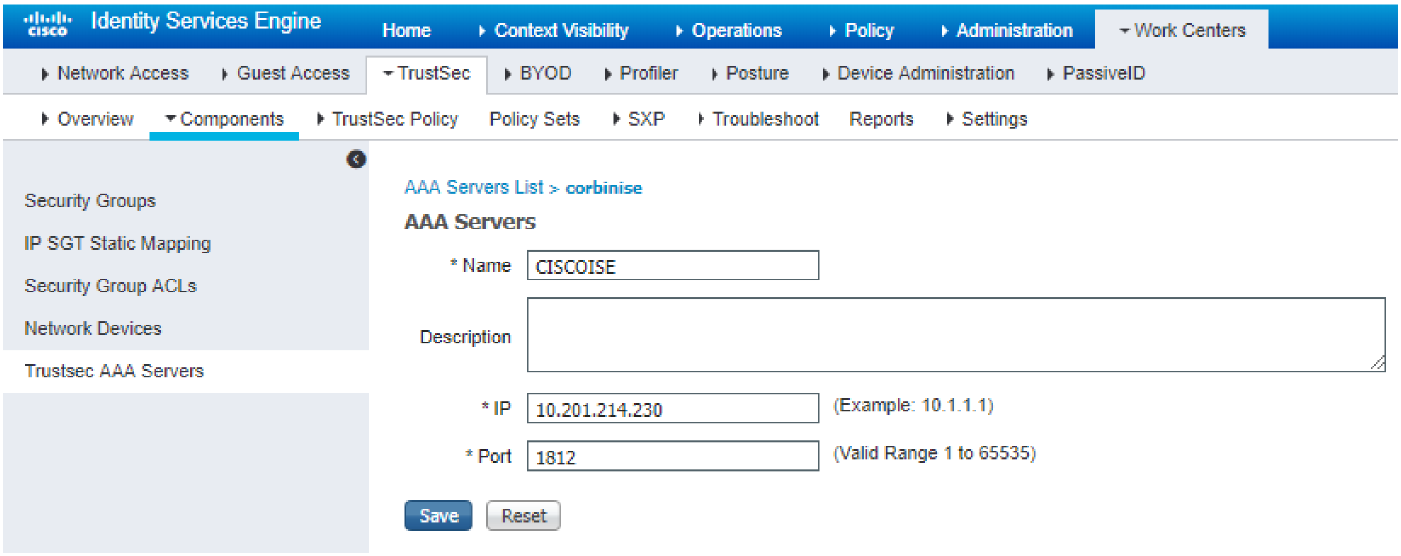
Real-time Monitoring

Check dashboards to monitor current access.

Auditing

Examine reports to check access and authorization is as intended.

Configurar o Cisco ISE como um servidor AAA TrustSec



AAA Servers List > corbinise

AAA Servers

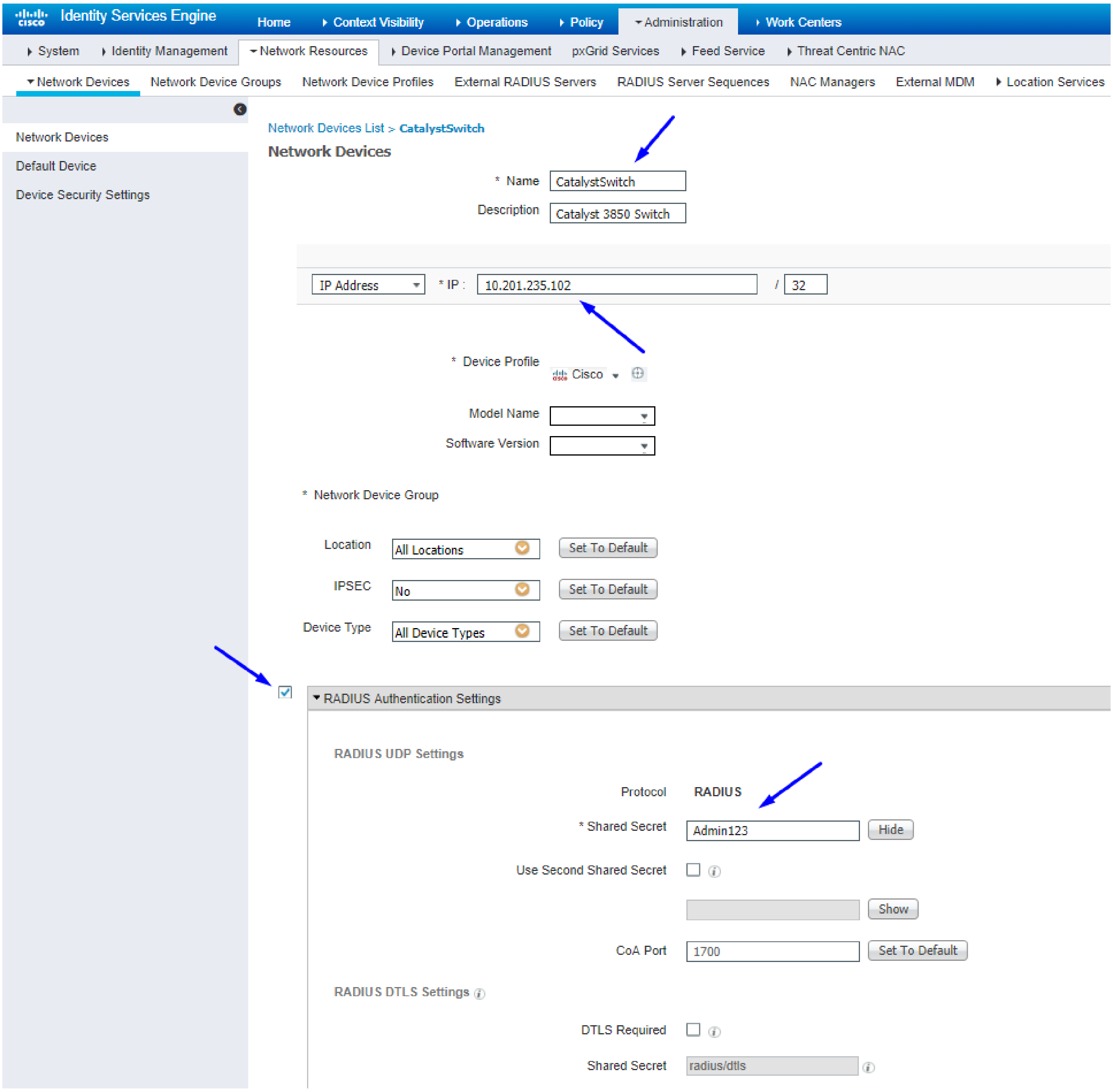
* Name: CISCOISE

Description:

* IP: 10.201.214.230 (Example: 10.1.1.1)

* Port: 1812 (Valid Range 1 to 65535)

Configurar e verificar se o switch foi adicionado como um dispositivo RADIUS no 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	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

Use Second Shared Secret: □

CoA Port: 1700

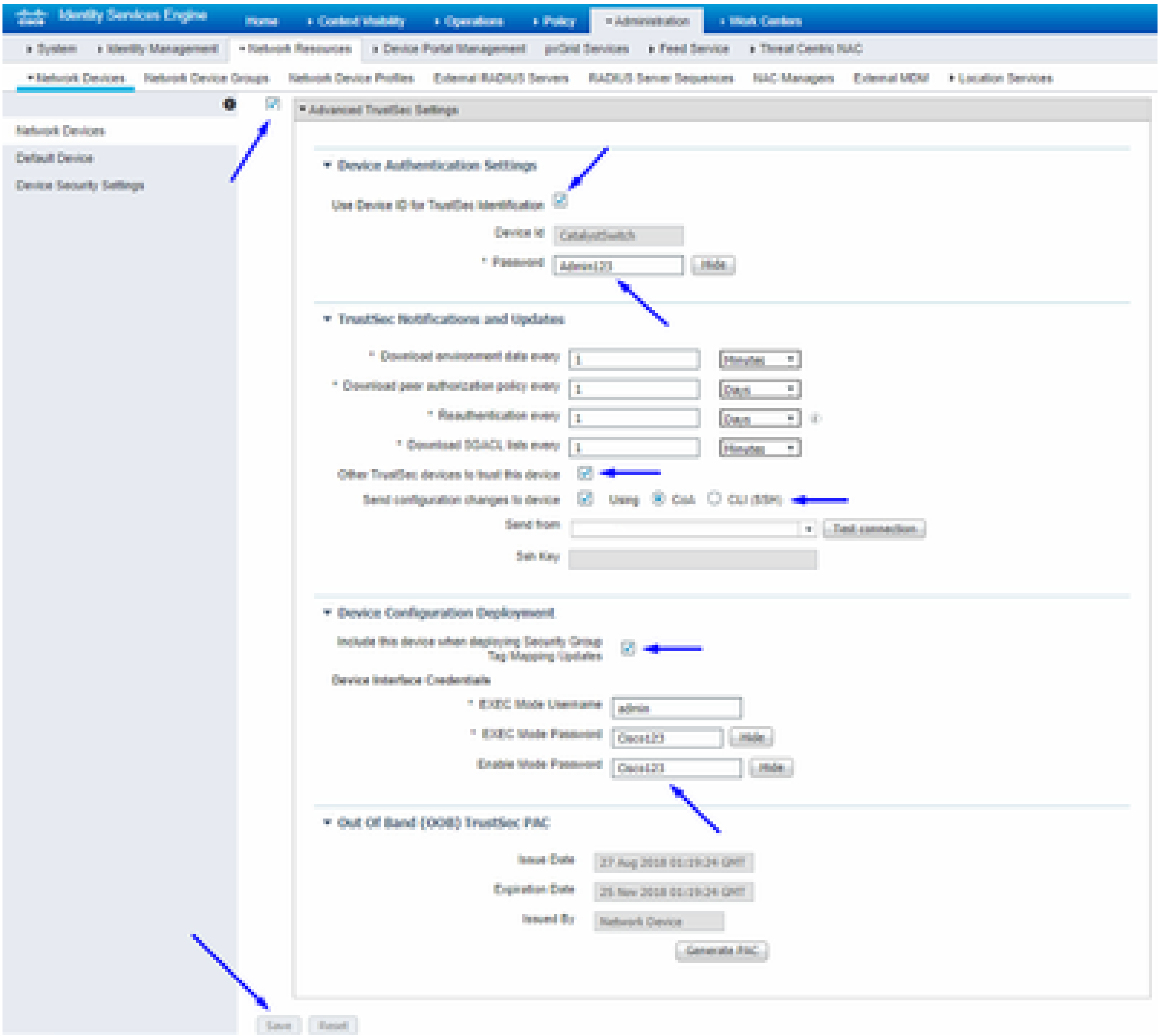
RADIUS DTLS Settings

DTLS Required: □

Shared Secret: radius/dtls

Configurar e verificar se a WLC foi adicionada como um dispositivo TrustSec no Cisco ISE

Insira suas credenciais de login para SSH. Isso permite que o Cisco ISE implante os mapeamentos estáticos de IP para SGT no switch.
Você pode criá-los na GUI da Web do Cisco ISE em Work Centers > TrustSec > Components > IP SGT Static Mappings como mostrado aqui:



☑ 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

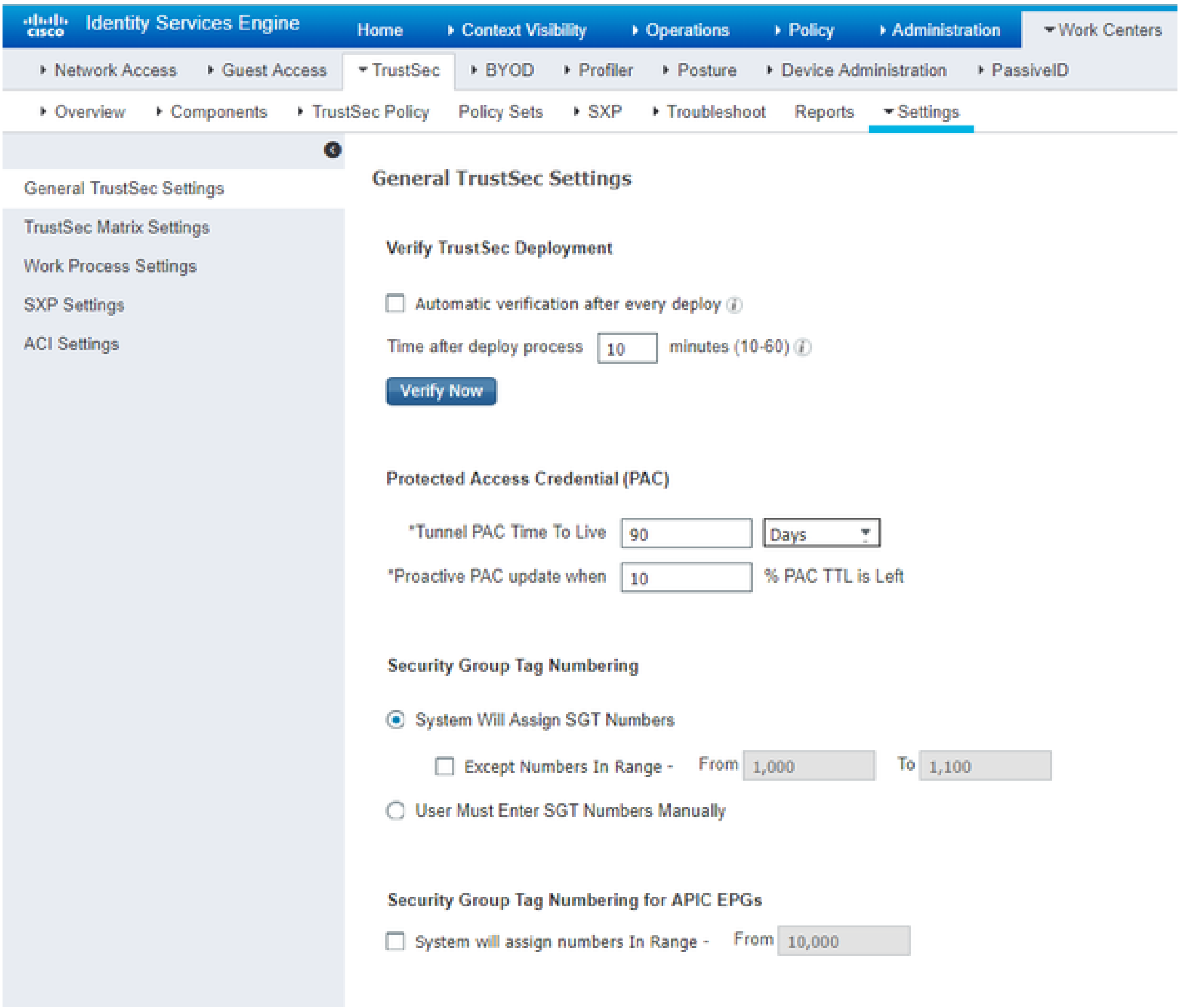
[Generate PAC]

[Save] [Reset]

Dica: se você ainda não configurou o SSH em seu Switch Catalyst, você pode usar este guia: Como configurar o Secure Shell (SSH) no Switch Catalyst.

Dica: se você não quiser permitir que o Cisco ISE acesse seu Switch Catalyst por SSH, poderá criar mapeamentos estáticos IP para SGT no Switch Catalyst com a CLI (mostrado em uma etapa aqui).

Verifique as configurações padrão do TrustSec para garantir que sejam aceitáveis (opcional)



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

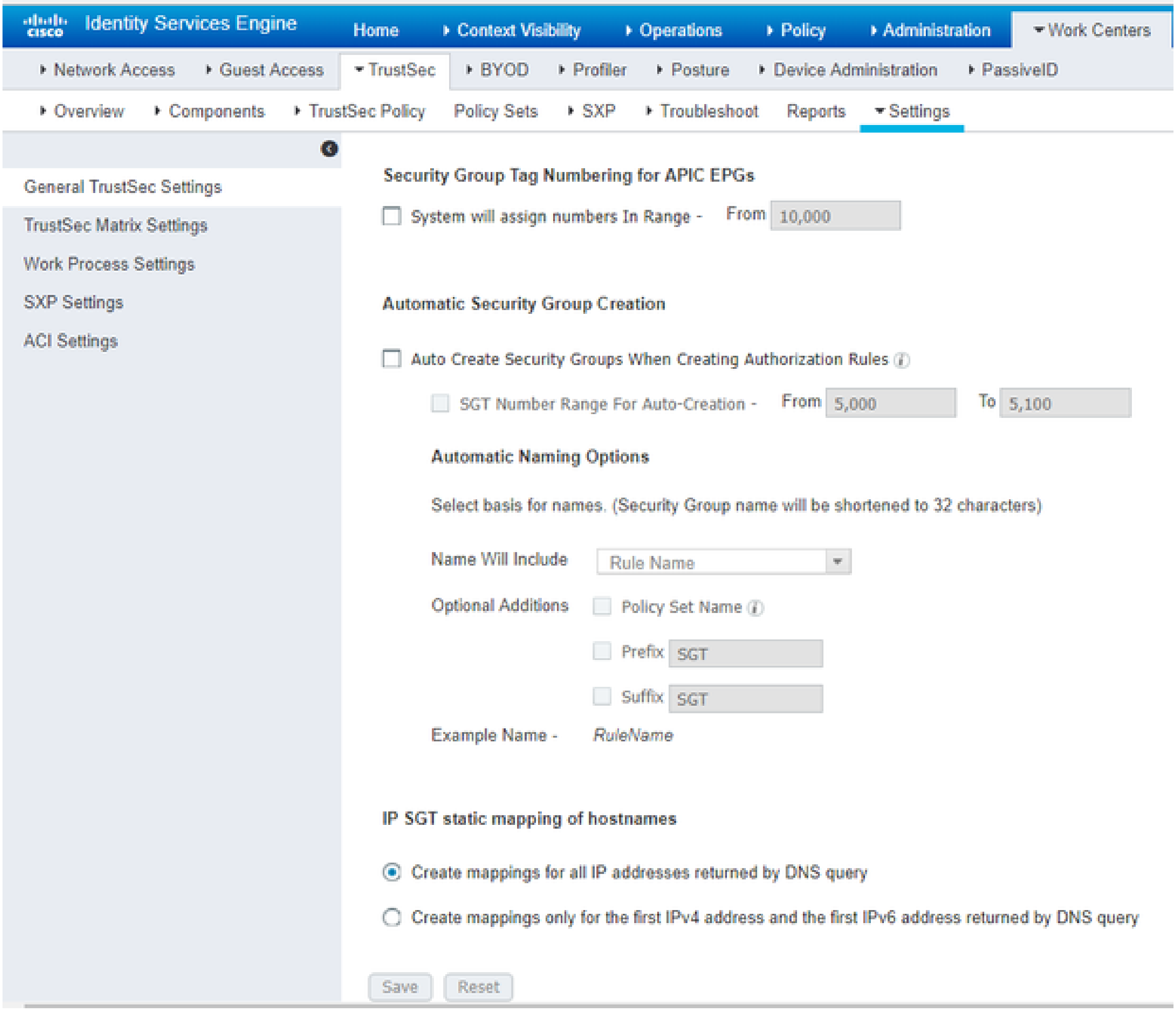
● System Will Assign SGT Numbers

□ 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

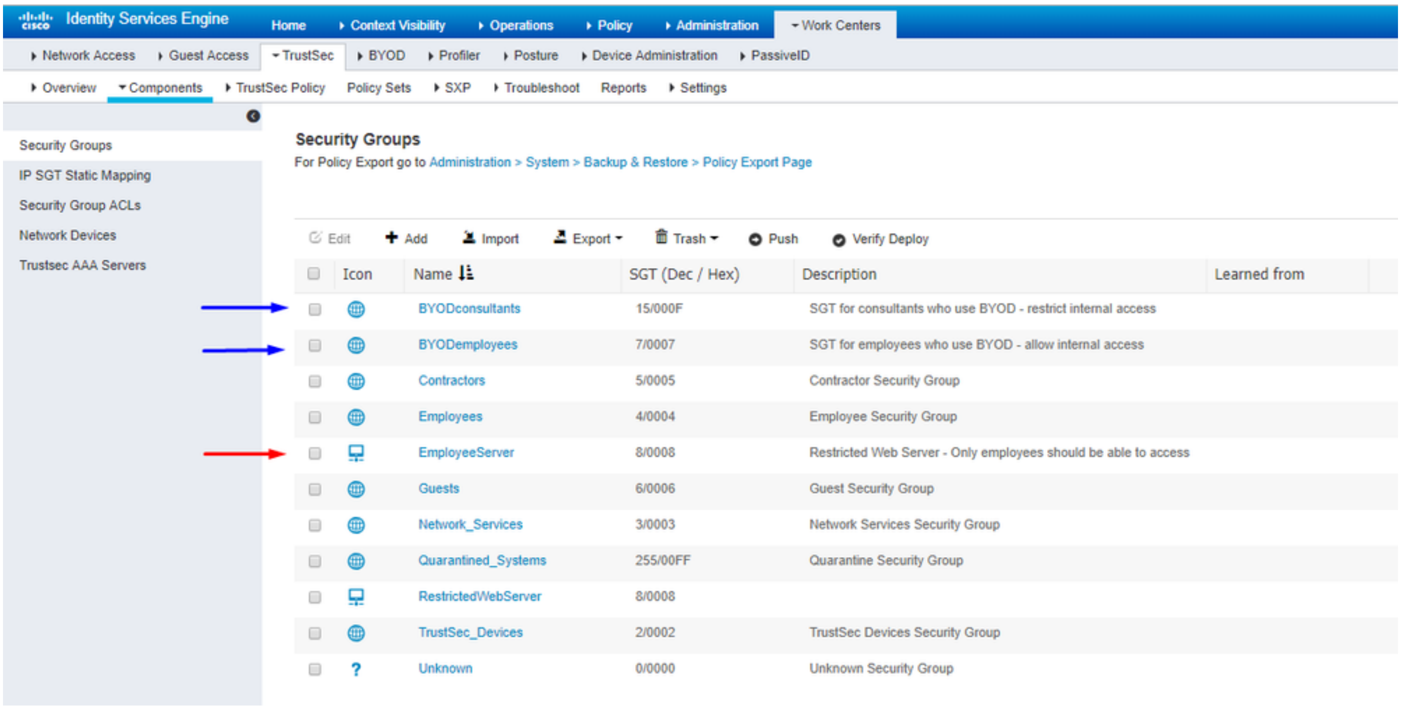
● Create mappings for all IP addresses returned by DNS query

○ Create mappings only for the first IPv4 address and the first IPv6 address returned by DNS query

Criar tags de grupo de segurança para usuários sem fio

Crie um grupo de segurança para consultores de BYOD - SGT 15

Crie um grupo de segurança para funcionários adeptos da consumerização de TI - SGT 7



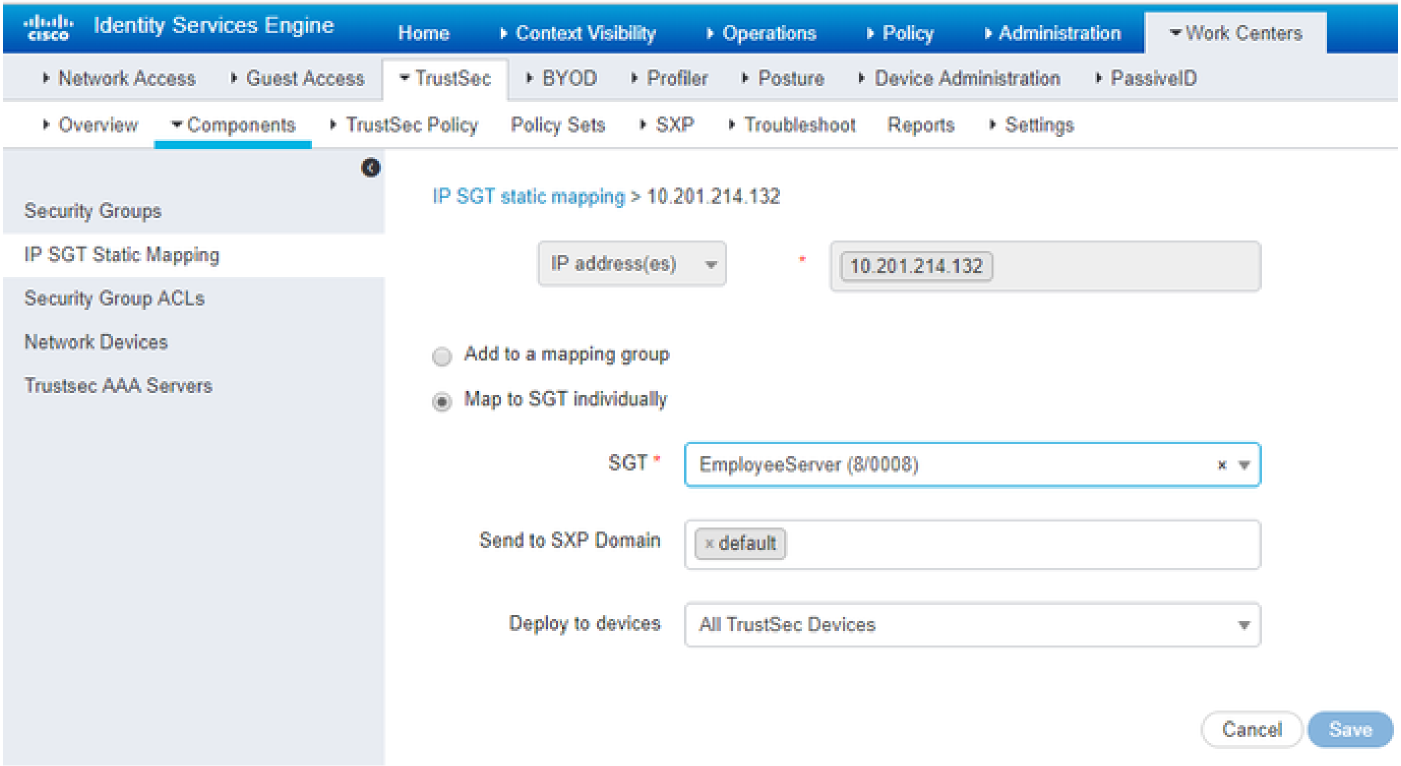
Security Groups

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	

Criar mapeamento estático de IP para SGT para o servidor Web restrito

Faça isso para qualquer outro endereço IP ou sub-rede em sua rede que não seja autenticado no Cisco ISE com MAC Authentication Bypass (MAB), 802.1x, Profiles, etc.



IP SGT static mapping > 10.201.214.132

IP address(es) * 10.201.214.132

○ Add to a mapping group

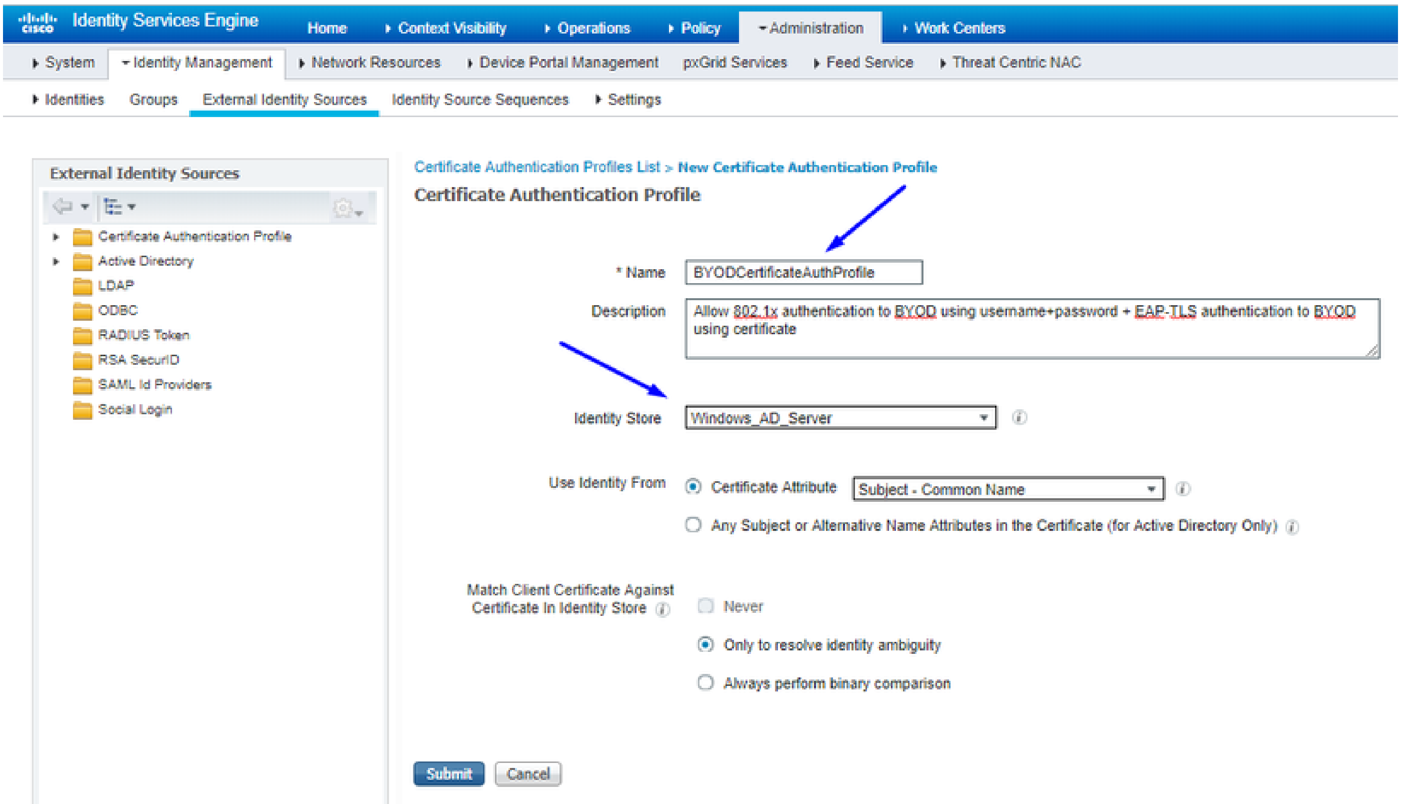
● Map to SGT individually

SGT * EmployeeServer (8/0008)

Send to SXP Domain: × default

Deploy to devices: All TrustSec Devices

Criar Perfil de Autenticação de Certificado



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)

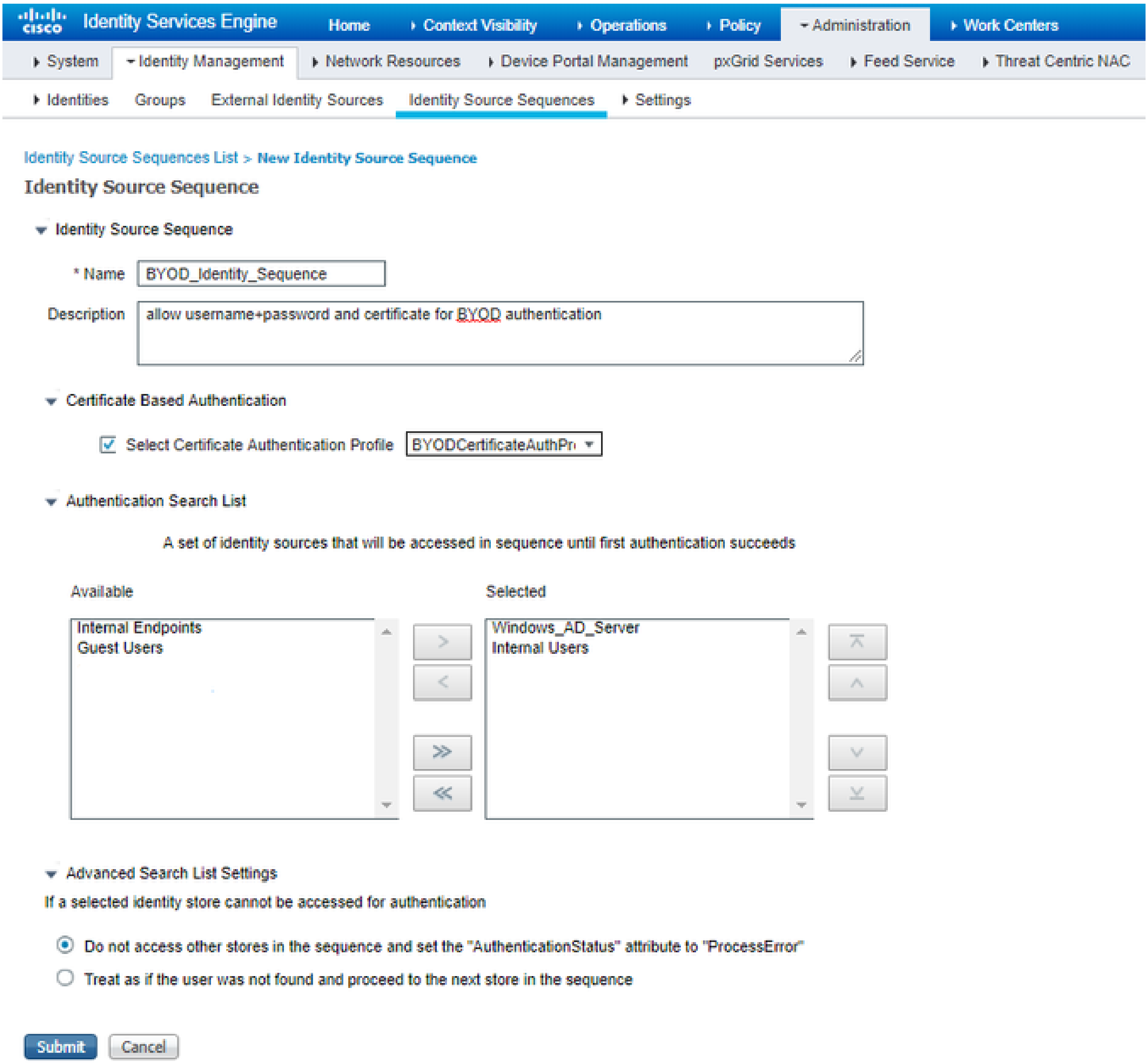
Match Client Certificate Against Certificate In Identity Store

□ Never

● Only to resolve identity ambiguity

○ Always perform binary comparison

Criar Sequência de Origem de Identidade com o Perfil de Autenticação de Certificado de Antes



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

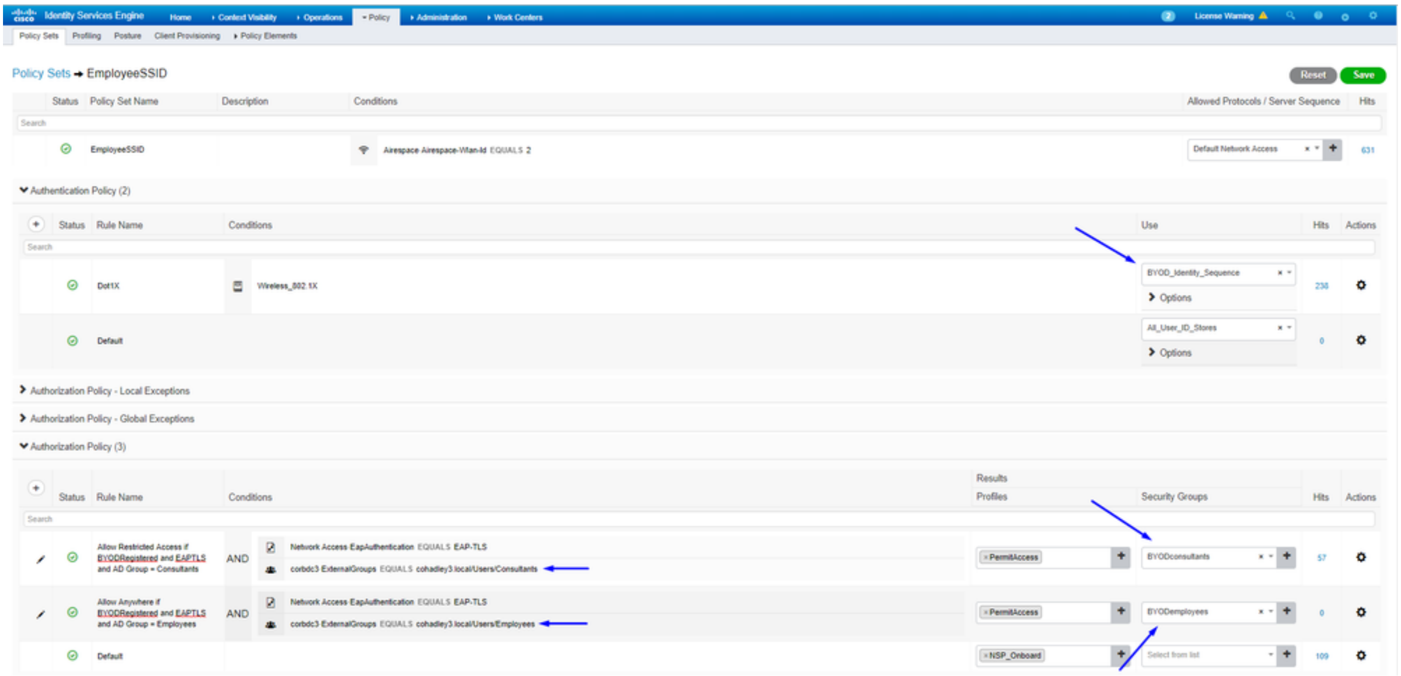
If a selected identity store cannot be accessed for authentication

● 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

Atribuir aos usuários sem fio (funcionários e consultores) um SGT apropriado

Nome	Nome de usuário	Grupo AD	SG	SGT
Jason Smith	jsmith	Consultores	Consultores de consumerização de TI	15
Sally Smith	smith	Funcionários	Funcionários adeptos da consumerização de TI	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	⚙

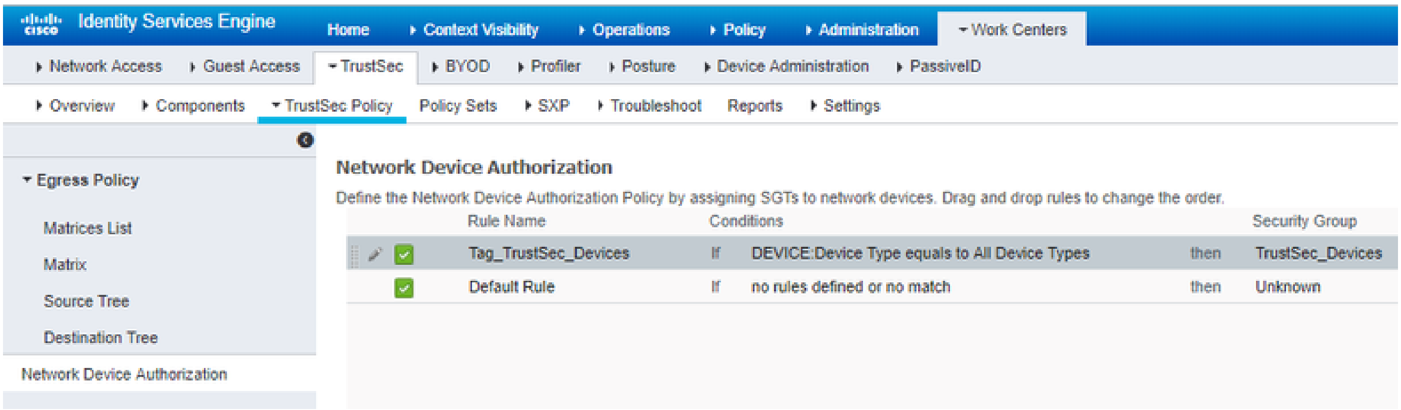
Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

	Status	Rule Name		Conditions	Results: Profiles	Results: 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	⚙

Atribuir SGTs aos dispositivos reais (switch e WLC)



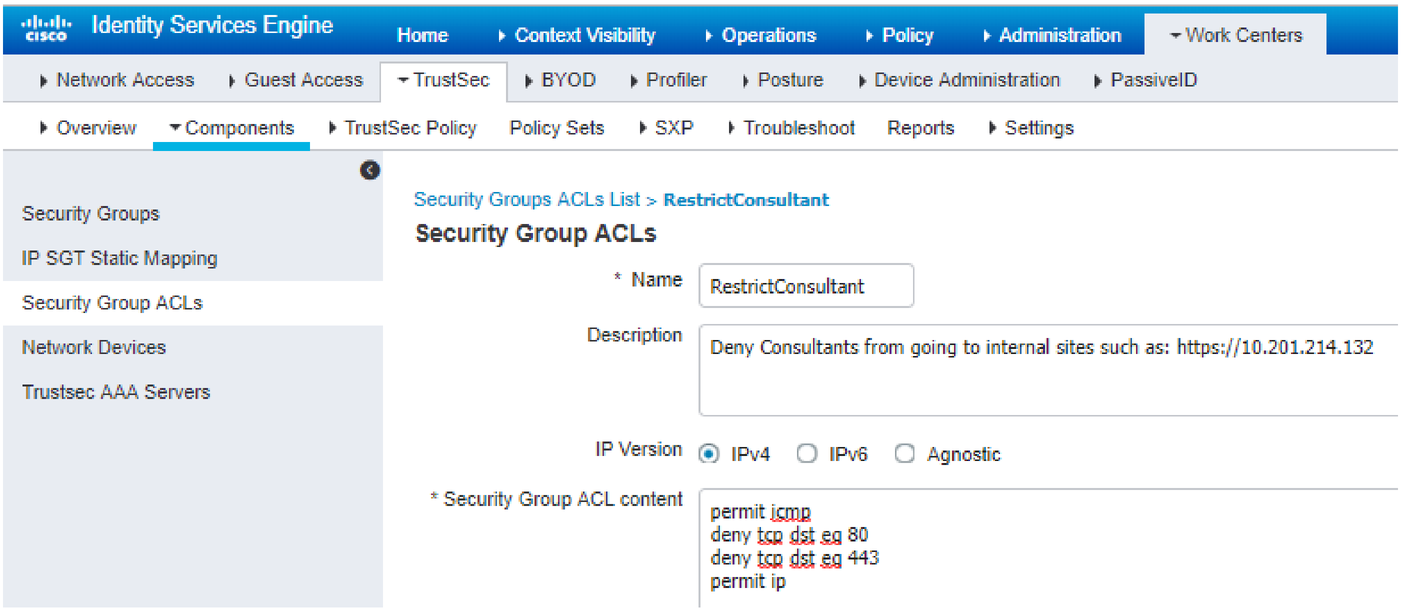
Network Device Authorization

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

Definir SGACLs para especificar a política de saída

Permitir que os consultores acessem em qualquer lugar externo, mas restringir interno:



Security Group ACLs

* Name: RestrictConsultant

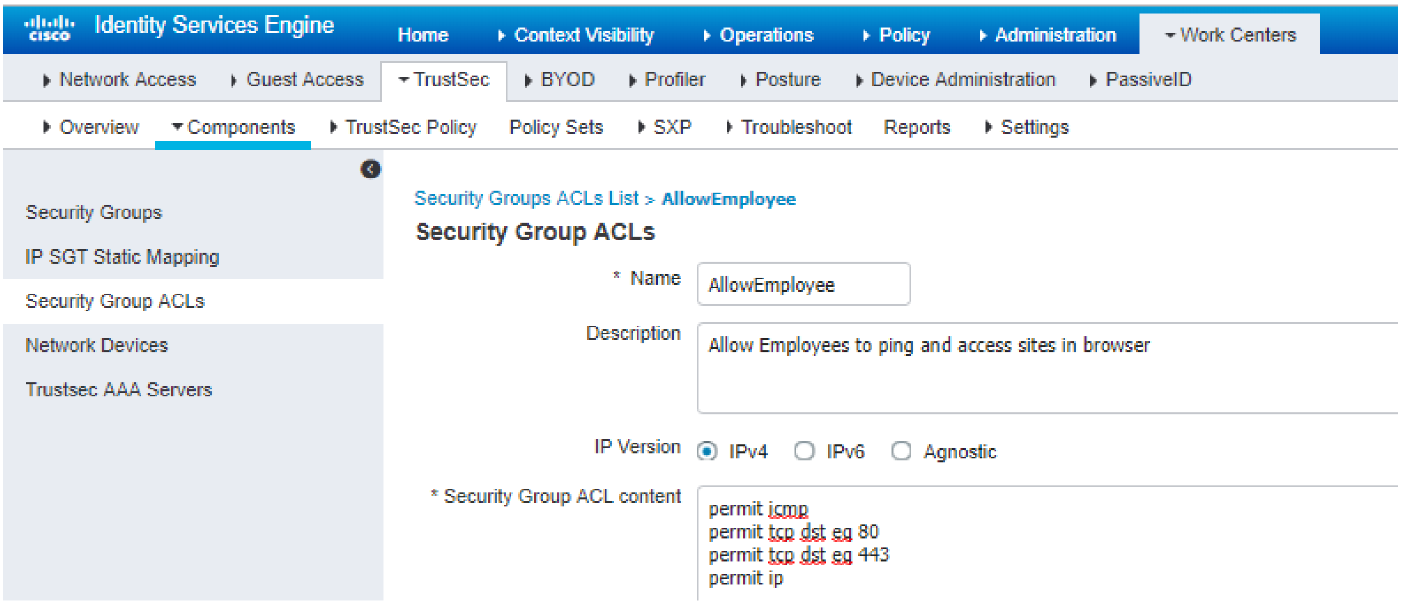
Description: Deny Consultants from going to internal sites such as: https://10.201.214.132

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

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

Permita que os funcionários acessem qualquer lugar externo e qualquer lugar interno:



Security Group ACLs

* Name: AllowEmployee

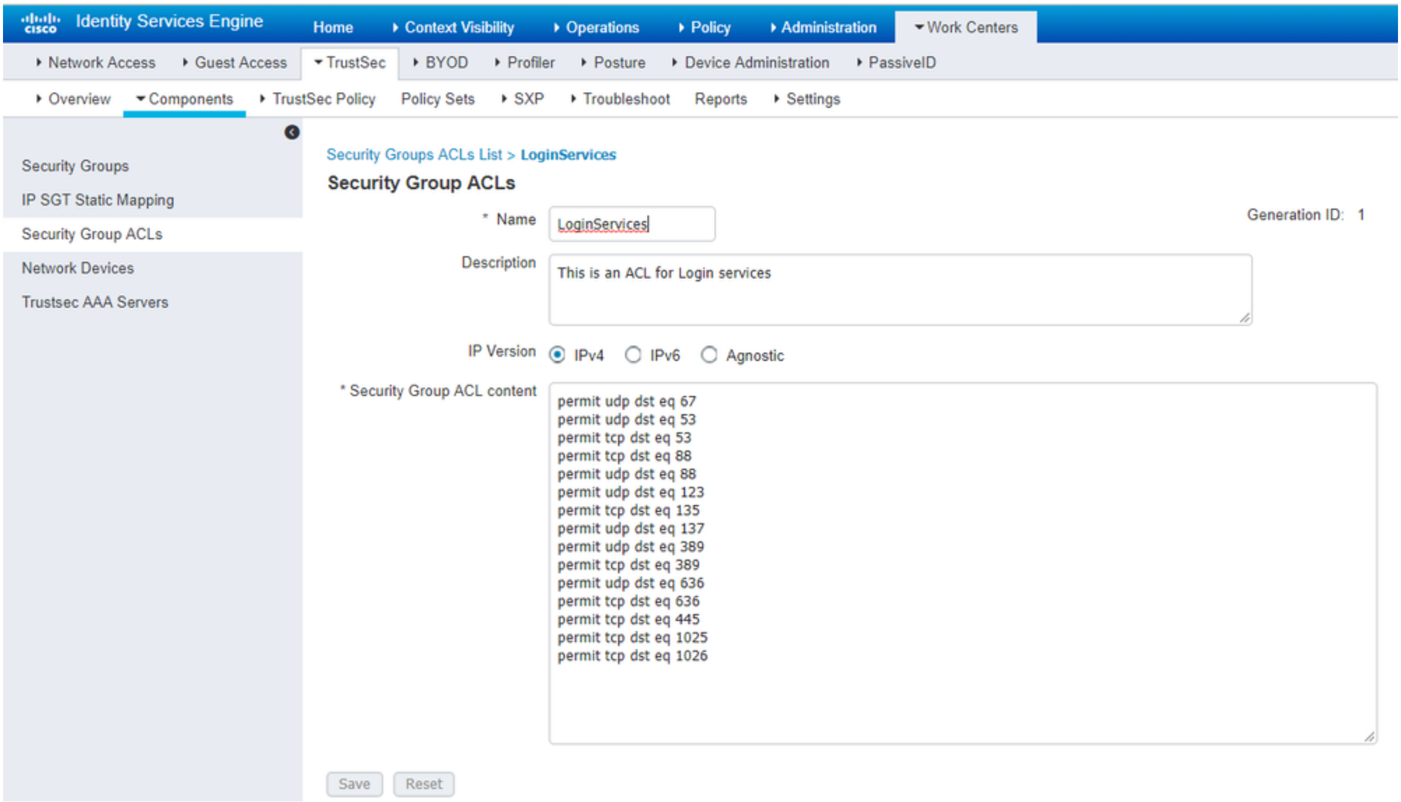
Description: Allow Employees to ping and access sites in browser

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

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

Permitir que outros dispositivos acessem serviços básicos (Opcional):



Security Groups ACLs List > LoginServices

Security Group ACLs

* Name: LoginServices

Generation ID: 1

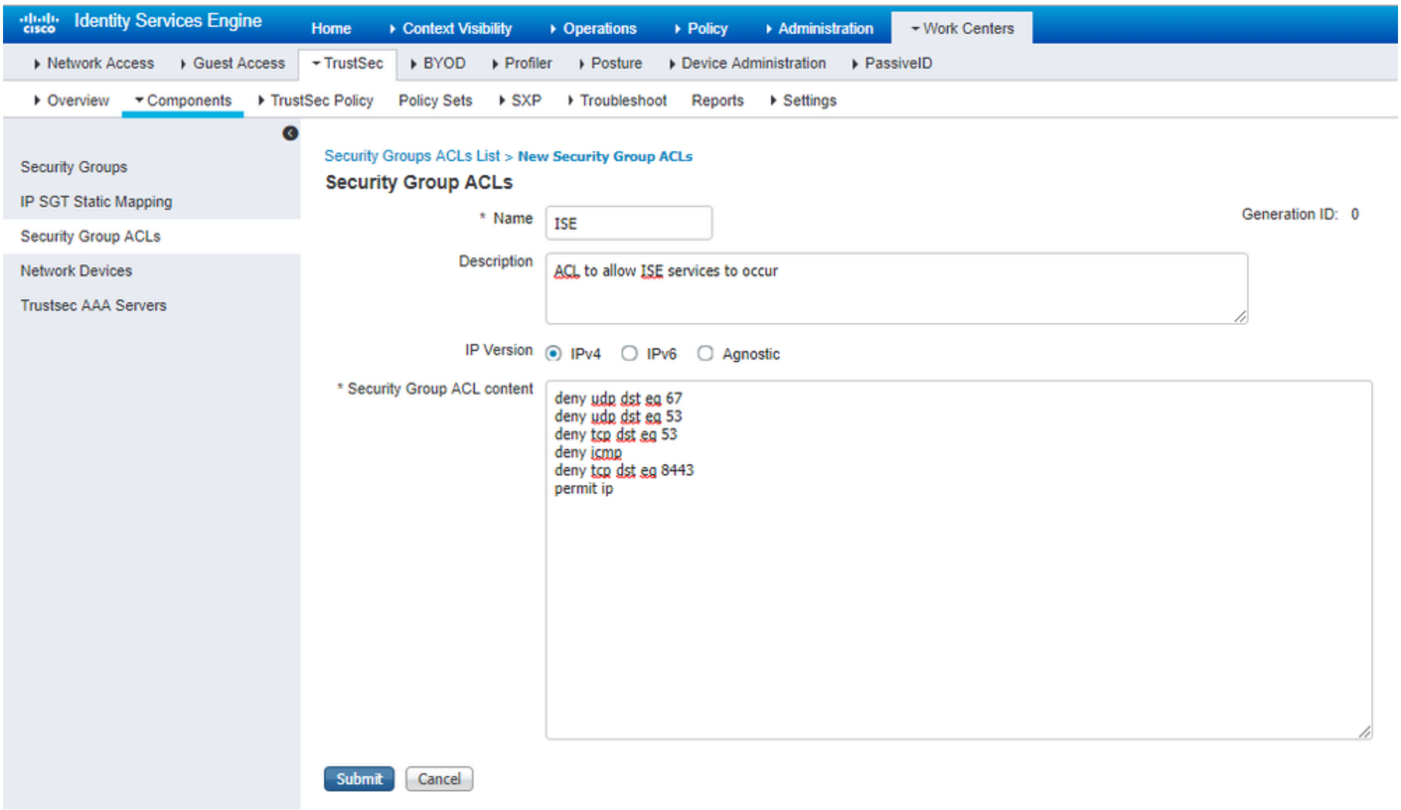
Description: This is an ACL for Login services

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
```

Redirecione todos os usuários finais para o Cisco ISE (para redirecionamento do portal BYOD). Não inclua o tráfego DNS, DHCP, ping ou WebAuth, pois eles não podem ir para o 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

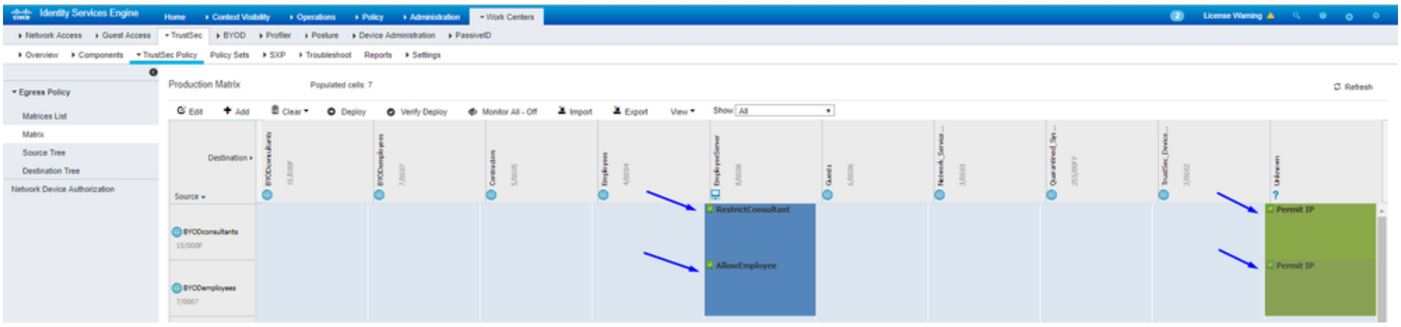
* Security Group ACL content

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

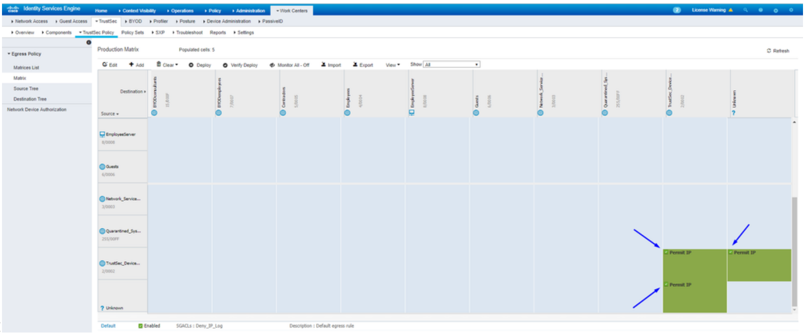
Aplique suas ACLs na matriz de políticas TrustSec no Cisco ISE

Permitir que os consultores acessem em qualquer lugar externo, mas restringir os servidores Web internos, como https://10.201.214.132

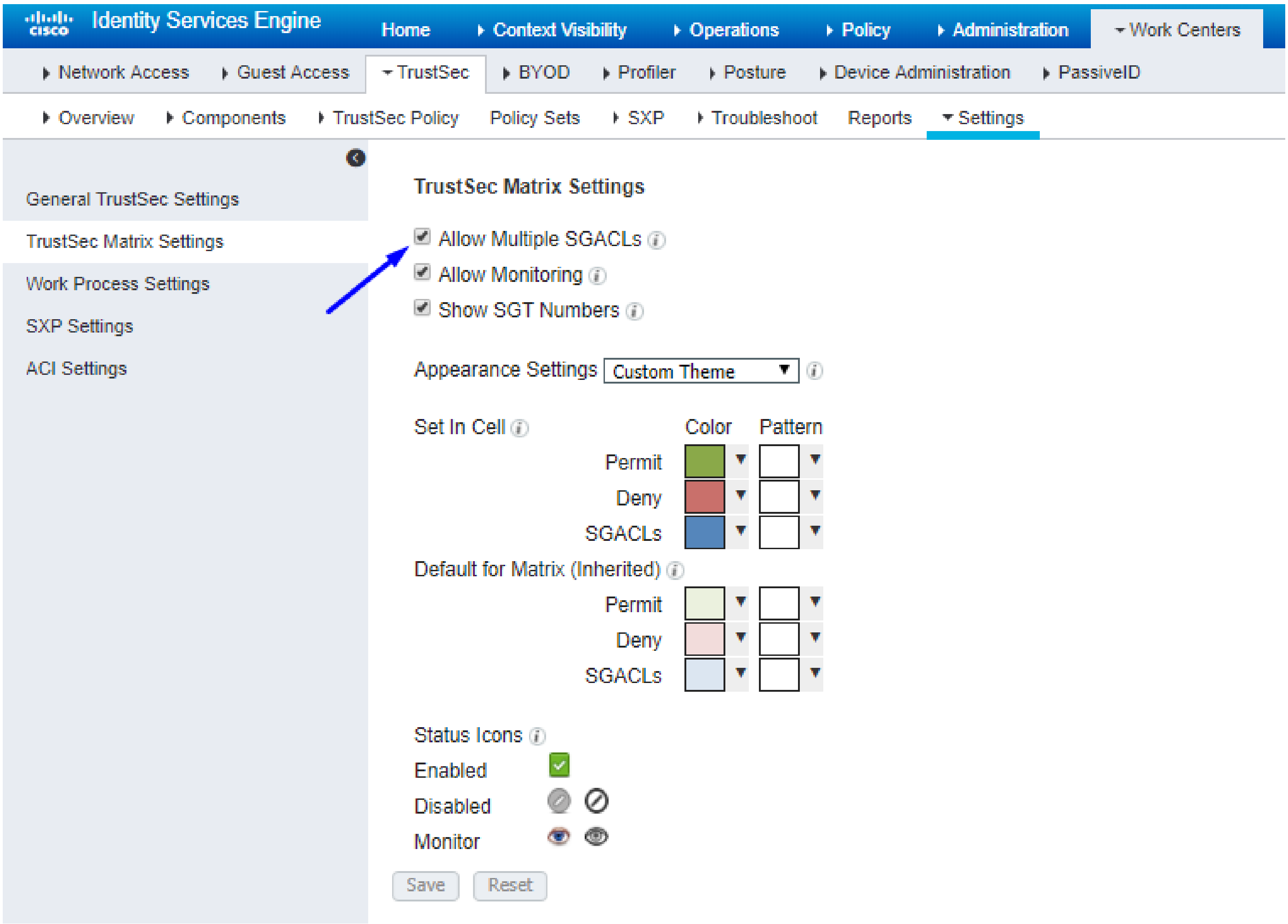
Permitir que os funcionários acessem em qualquer lugar externo e permitir servidores Web internos:



Permitir tráfego de gerenciamento (SSH, HTTPS e CAPWAP) de/para seus dispositivos na rede (switch e WLC) para que você não perca o acesso SSH ou HTTPS depois de implantar o Cisco TrustSec:



Permita que o Cisco ISE Allow Multiple SGACLs:



TrustSec Matrix Settings

☑ Allow Multiple SGACLs
☑ Allow Monitoring
☑ Show SGT Numbers

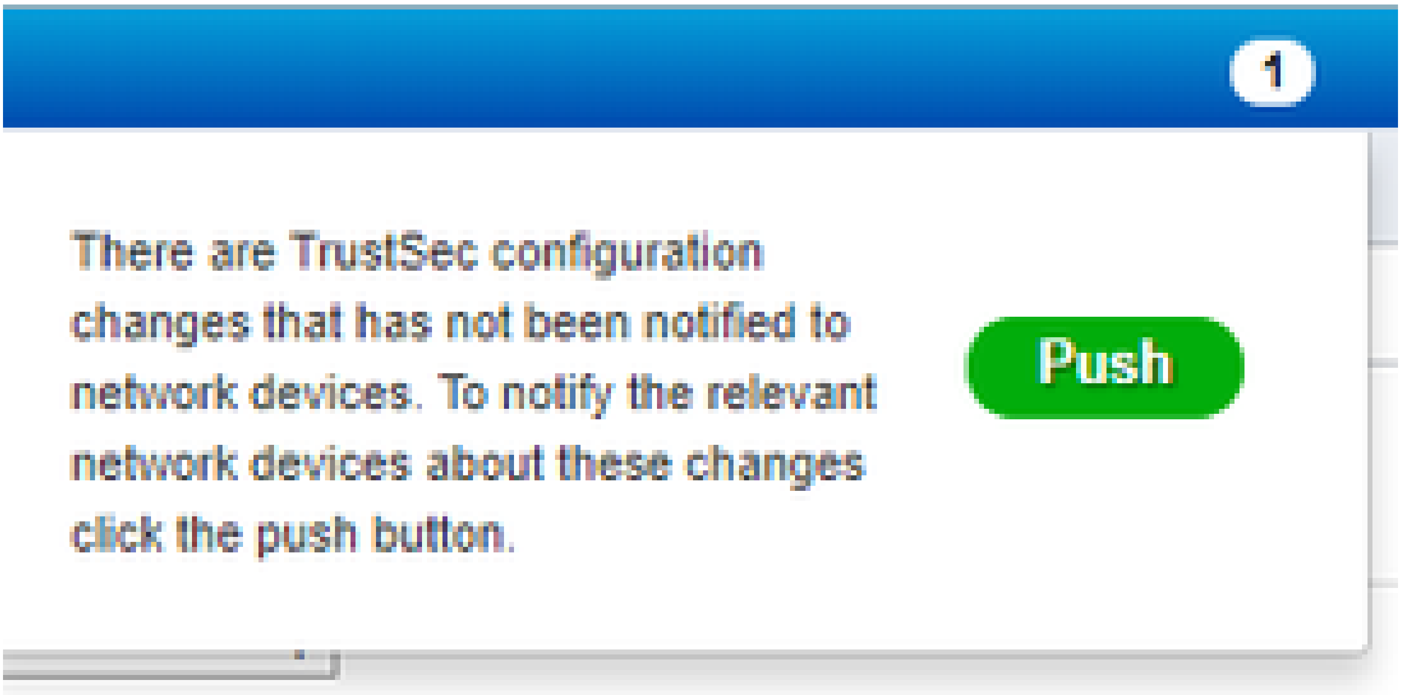
Appearance Settings: Custom Theme

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

Status Icons
Enabled ✓
Disabled ⊘
Monitor

Save Reset

CliquePush no canto superior direito do Cisco ISE para enviar sua configuração para seus dispositivos. Você também precisa fazer isso novamente mais tarde:



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.

Configurar o TrustSec no Switch Catalyst

Configurar o Switch para Usar o Cisco TrustSec para AAA no Switch Catalyst

Dica: este documento supõe que seus usuários sem fio já tenham obtido êxito com o BYOD do Cisco ISE antes da configuração mostrada aqui.

Os comandos mostrados em negrito já foram configurados antes disso (para que o BYOD Wireless funcione com o 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
```

Observação: a chave PAC deve ser a mesma que o segredo compartilhado RADIUS especificado na **Administration > Network Devices > Add Device > RADIUS Authentication Settings** seção.

<#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
```

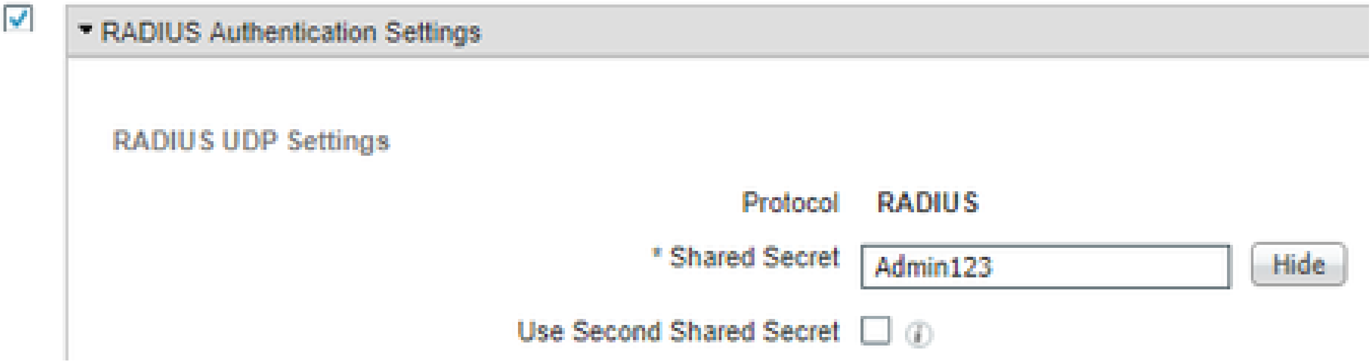
```
CatalystSwitch(config)#radius-server attribute 25 access-request include
```

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

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

Configure a chave PAC no servidor RADIUS para autenticar o switch para o 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

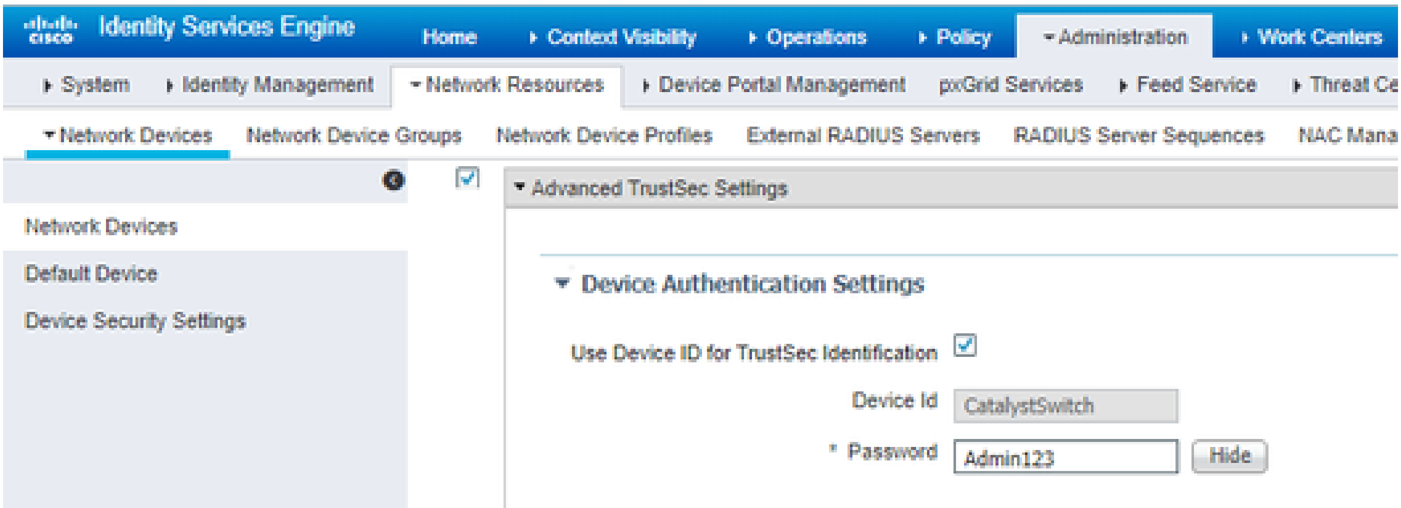
* Shared Secret Admin123

Use Second Shared Secret □

Observação: a chave PAC deve ser a mesma que o segredo compartilhado RADIUS especificado na **Administration > Network Devices > Add Device > RADIUS Authentication Settings** seção no Cisco ISE (como mostrado na captura de tela).

Configurar credenciais CTS para autenticar o switch para o 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

Observação: as credenciais CTS devem ser iguais à ID do dispositivo + senha que você especificou em As credenciais CTS devem ser iguais à ID do dispositivo + senha que você especificou na seçãoAdministration > Network Devices > Add Device > Advanced

TrustSec Settings no Cisco ISE (mostrada na captura de tela).

Em seguida, atualize sua PAC para que ela chegue novamente ao Cisco ISE:

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

Ativar CTS globalmente no switch Catalyst

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

Faça um mapeamento IP-para-SGT estático para os servidores Web restritos (opcional)

Esse servidor Web restrito nunca vem através do ISE para autenticação; portanto, você deve marcá-lo manualmente com a CLI do Switch ou a GUI da Web do ISE, que é apenas um dos muitos servidores Web da Cisco.

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

Verificar o TrustSec no Switch Catalyst

```
CatalystSwitch#show cts pac
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 PAC-Info:
 PAC-type = Cisco Trustsec
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 I-ID: CatalystSwitch
 A-ID-Info: Identity Services Engine
 Credential Lifetime: 23:43:14 UTC Nov 24 2018
 PAC-Opaque: 000200B80003000100040010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F
 Refresh timer is set for 12w5d
```

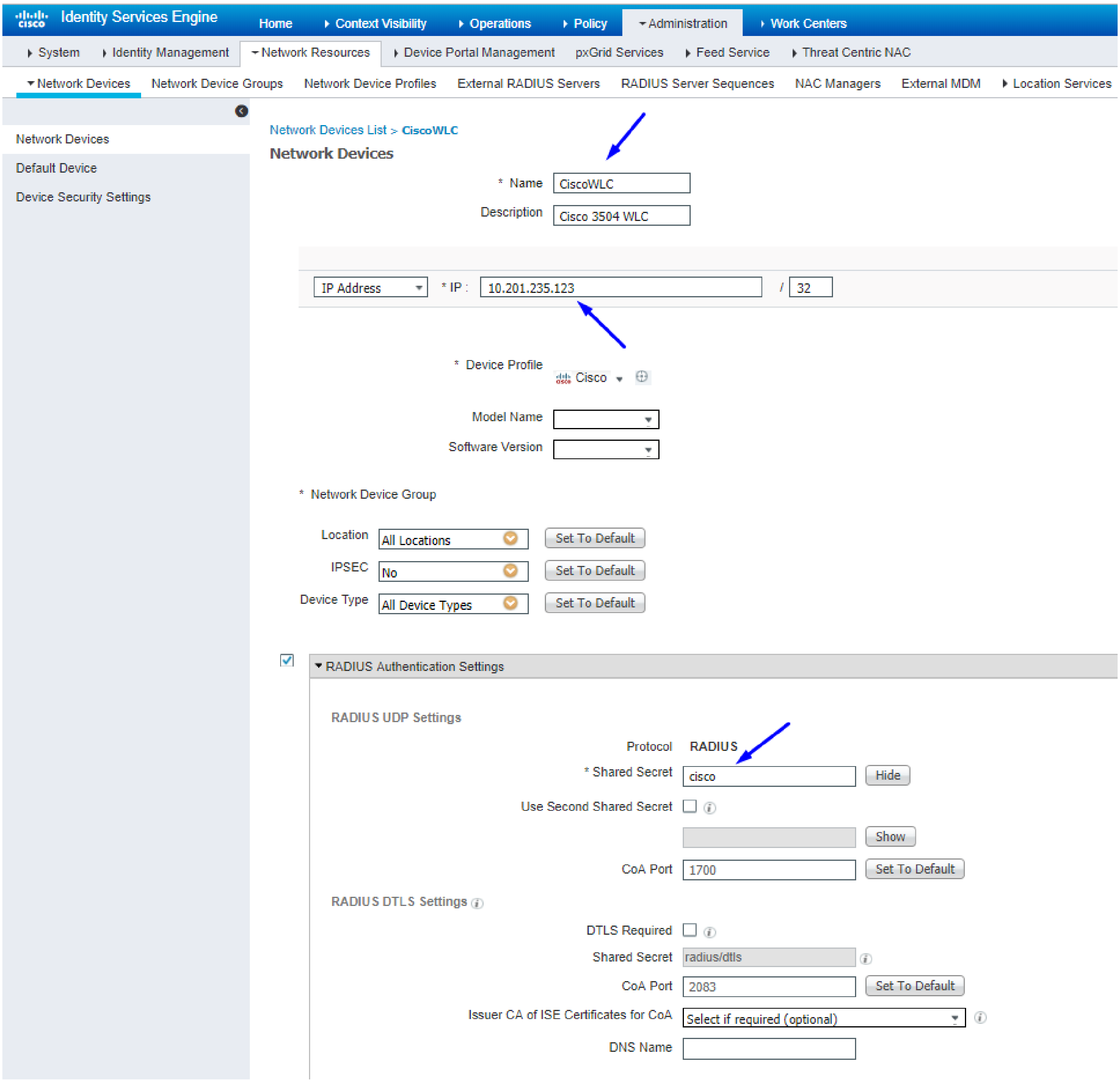
```
CatalystSwitch#cts refresh environment-data
Environment data download in progress
```

```
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
```

Configurar TrustSec no WLC

Configurar e verificar se a WLC é adicionada como um dispositivo RADIUS no Cisco ISE



* 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

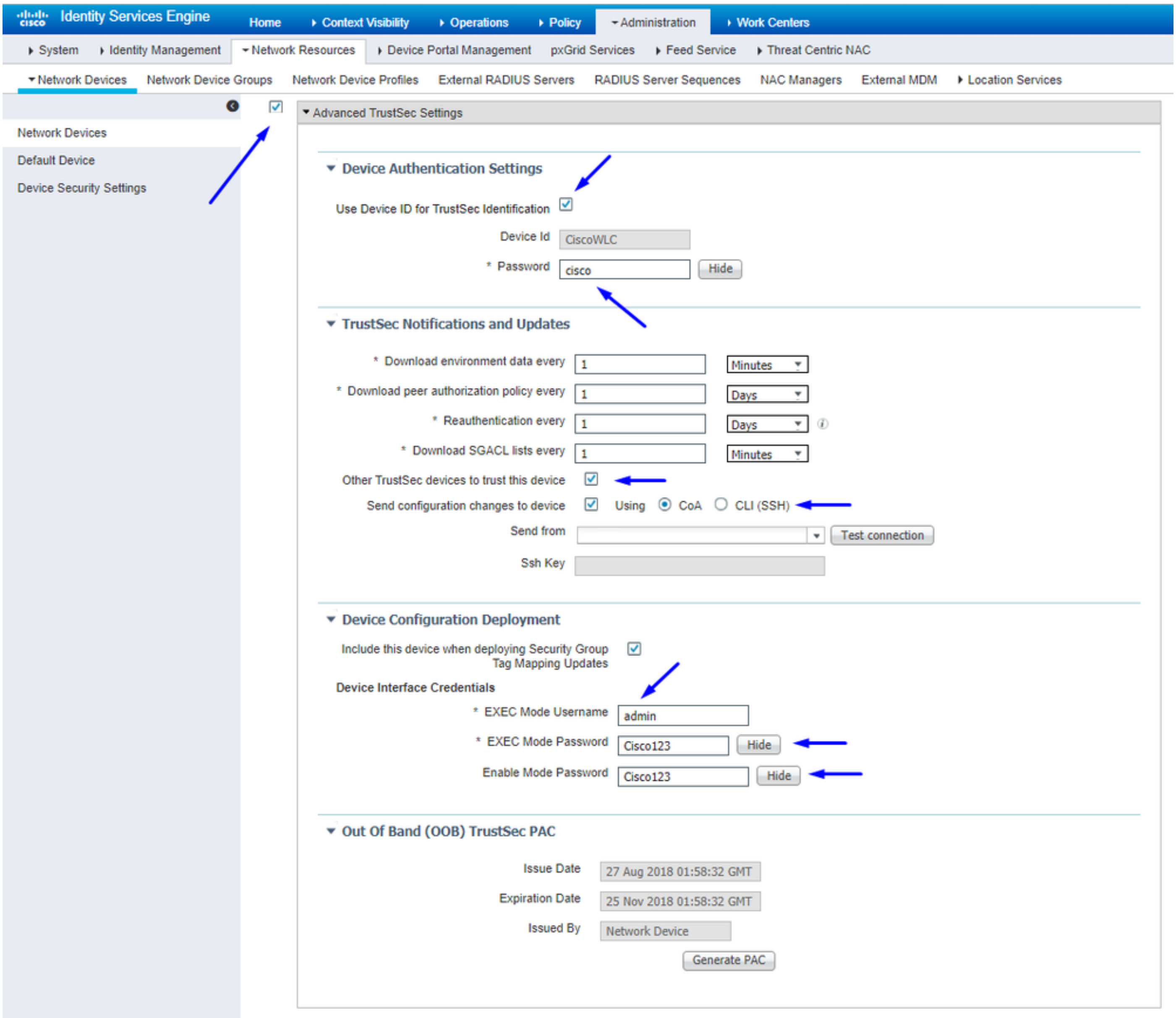
CoA Port: 2083 [Set To Default]

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

DNS Name:

Configurar e verificar se a WLC foi adicionada como um dispositivo TrustSec no Cisco ISE

Esta etapa permite que o Cisco ISE implante mapeamentos estáticos de IP para SGT na WLC. Você criou esses mapeamentos na GUI da Web do Cisco ISE em **Centros de trabalho > TrustSec > Componentes > Mapeamentos estáticos IP SGT** em uma etapa anterior.



☑ 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

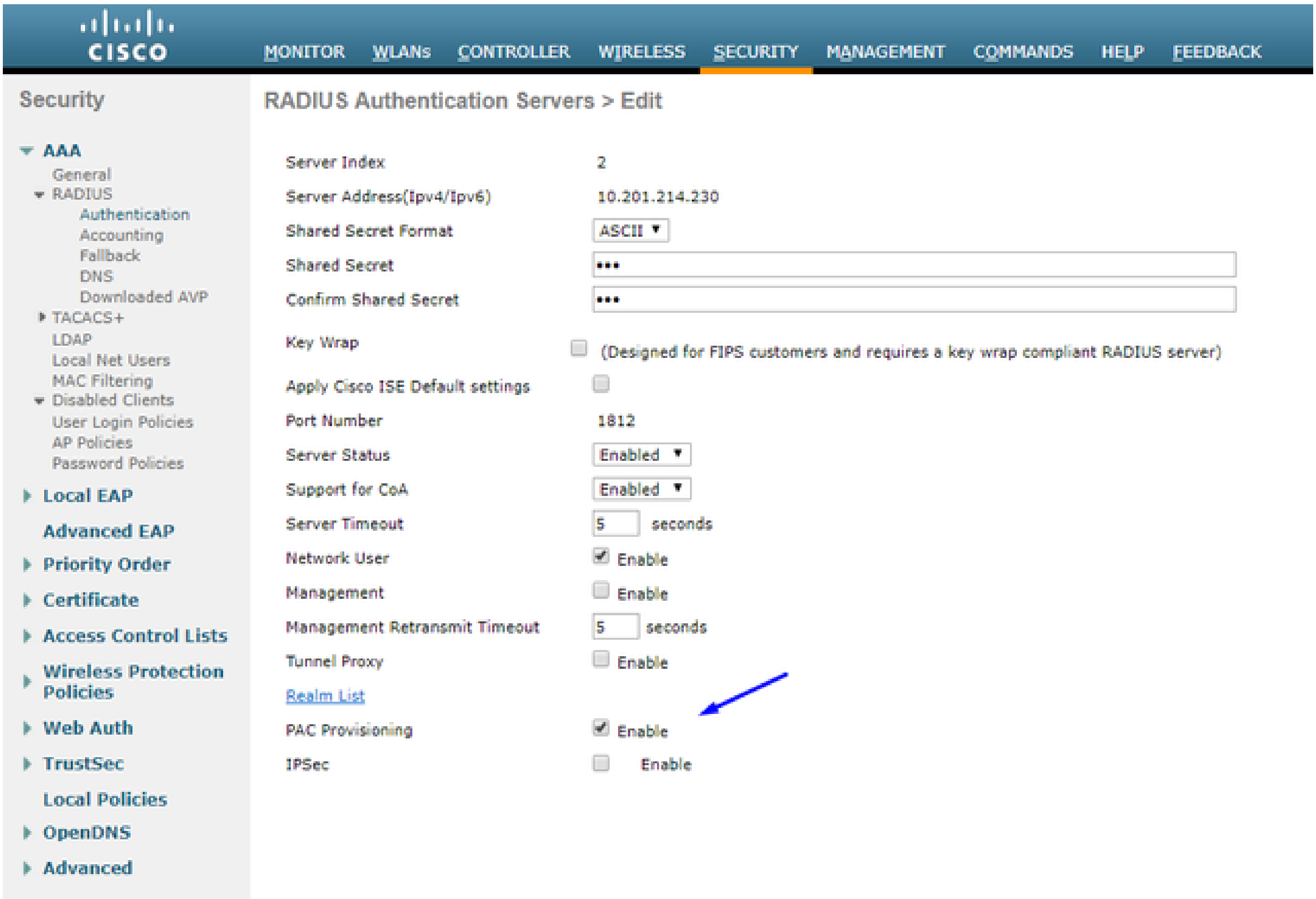
Expiration Date: 25 Nov 2018 01:58:32 GMT

Issued By: Network Device

[Generate PAC]

Observação: usamos isso Device ld e Password em uma etapa posterior, em Security > TrustSec > General na interface do usuário da Web da WLC.

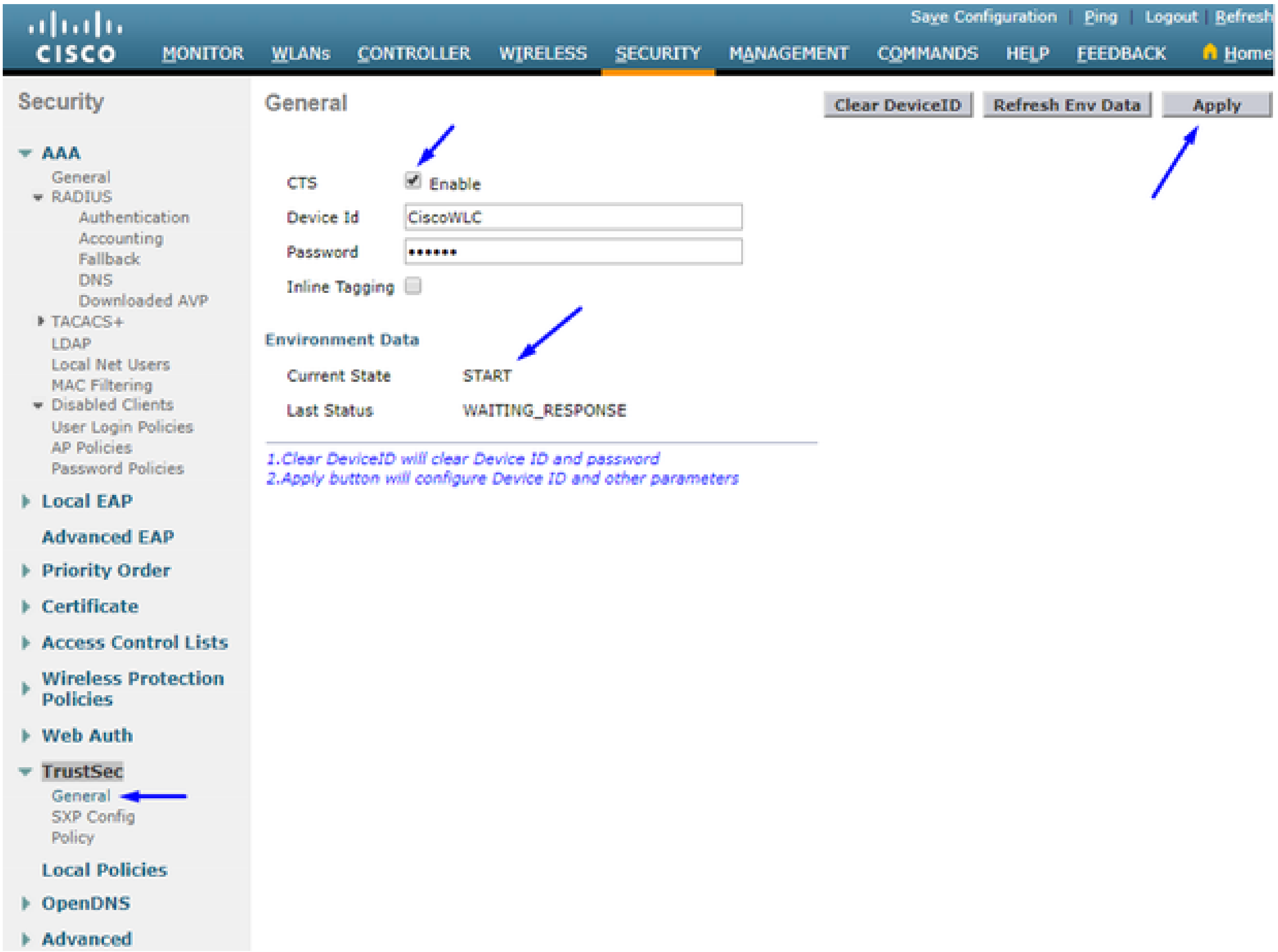
Habilitar fornecimento de PAC de WLC



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

Habilitar TrustSec no WLC



General

CTS ☑ Enable

Device Id CiscoWLC

Password ••••••

Inline Tagging □

Environment Data

Current State START

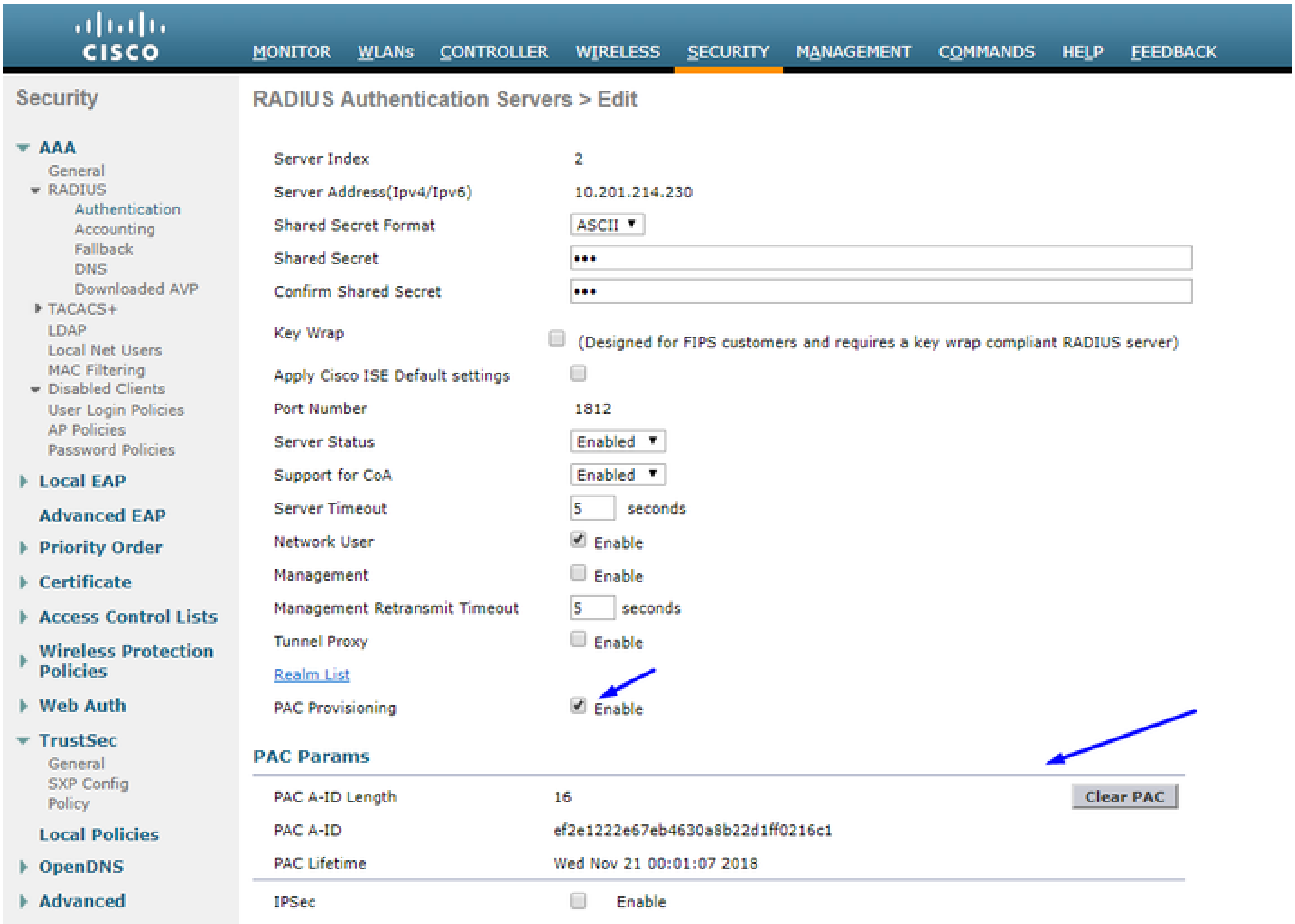
Last Status WAITING_RESPONSE

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

Observação: o CTS Device Id e o Password devem ser iguais ao Device Id e Password que você especificou na seção Administration > Network Devices > Add Device > Advanced TrustSec Settings no Cisco ISE.

Verificar se a PAC foi Provisionada na WLC

Você vê que a WLC tem a PAC fornecida com êxito depois de clicar em Refresh Env Data (você faz isso nesta etapa):



RADIUS Authentication Servers > Edit

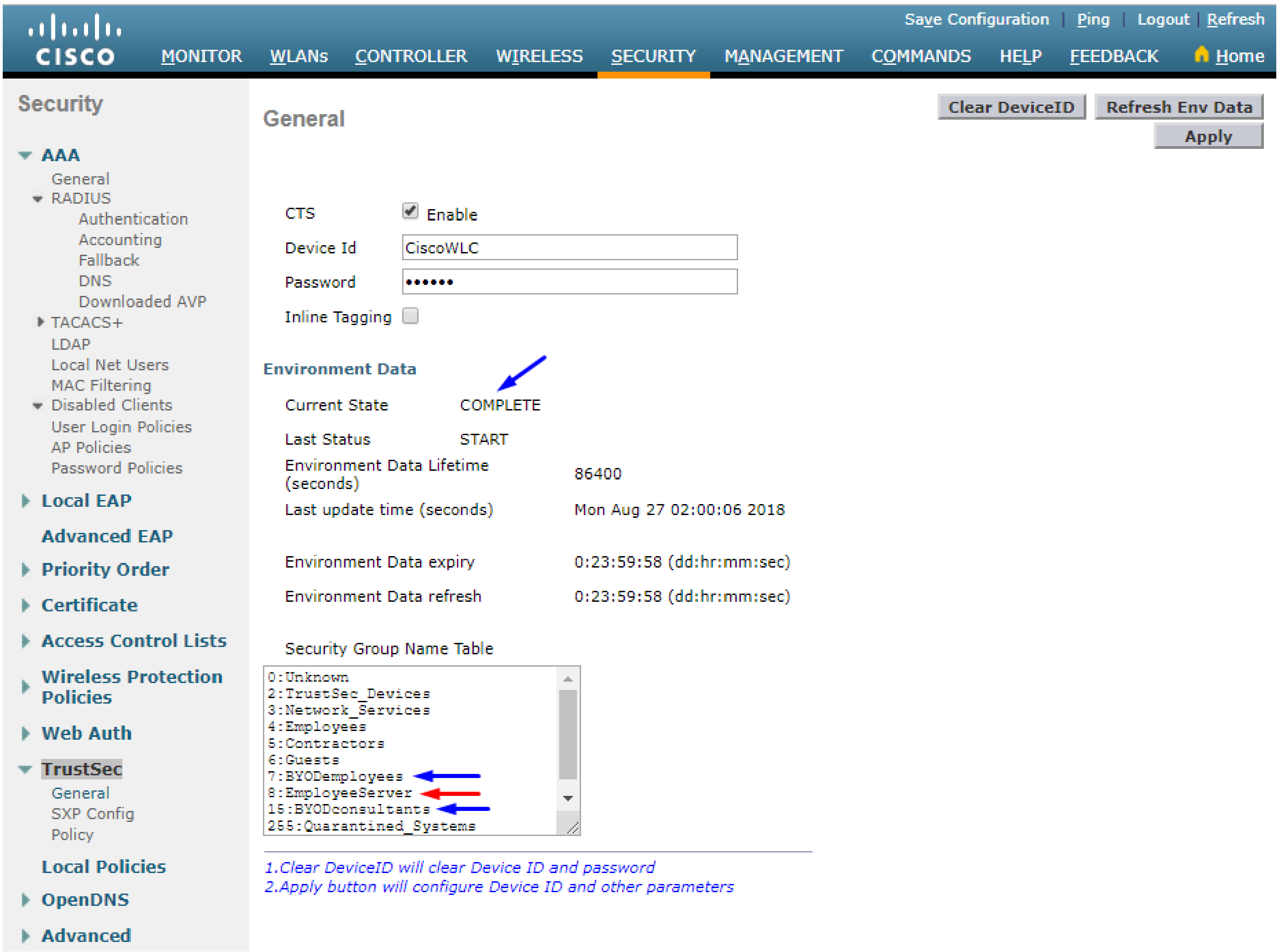
Server Index	2
Server Address(Ipv4/Ipv6)	10.201.214.230
Shared Secret Format	ASCII ▾
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	□
Port Number	1812
Server Status	Enabled ▾
Support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

Após clicar Refresh Env Data, o WLC faz o download dos 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)

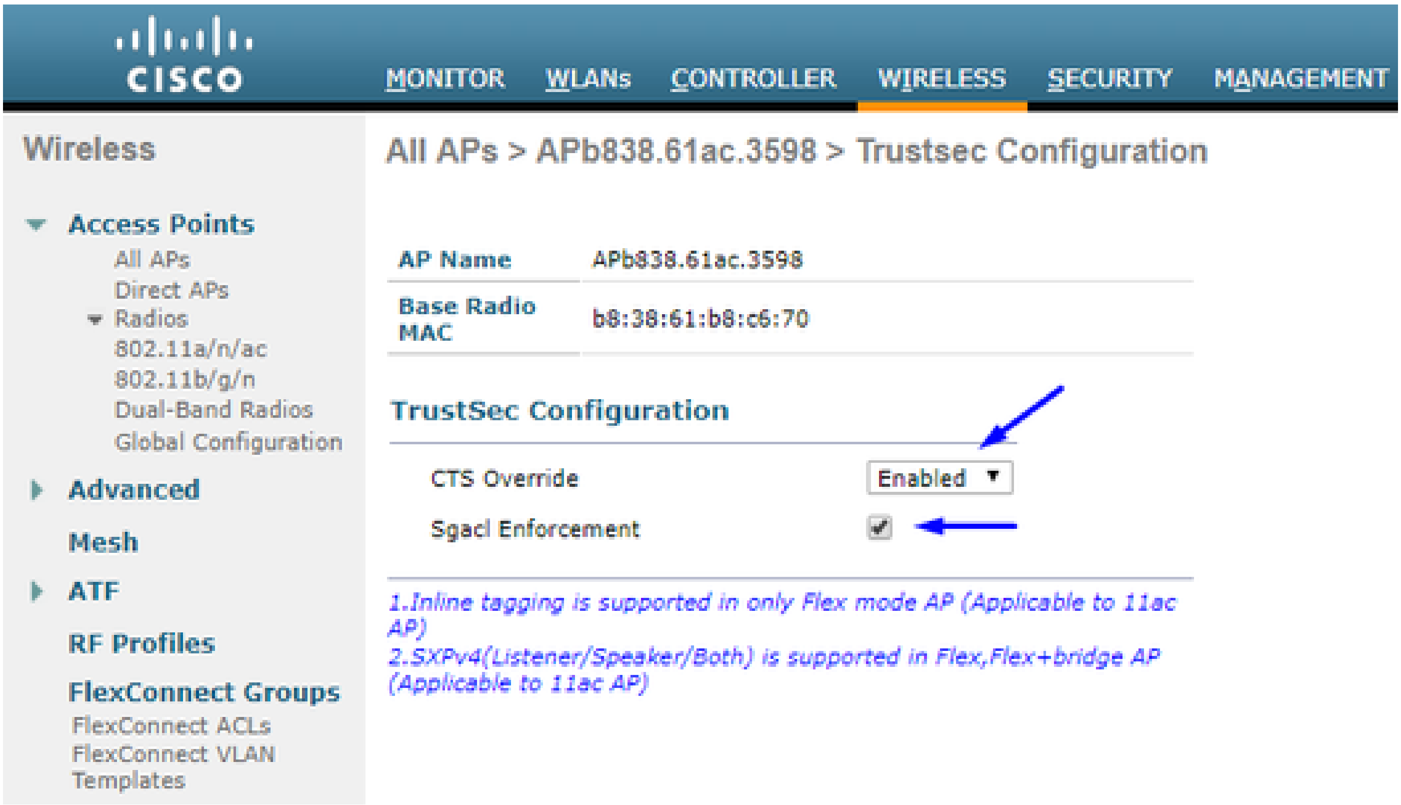
Environment Data refresh 0:23:59:58 (dd:hr:mm:sec)

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

Habilitar downloads e aplicação de SGACL no tráfego



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

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

TrustSec Configuration

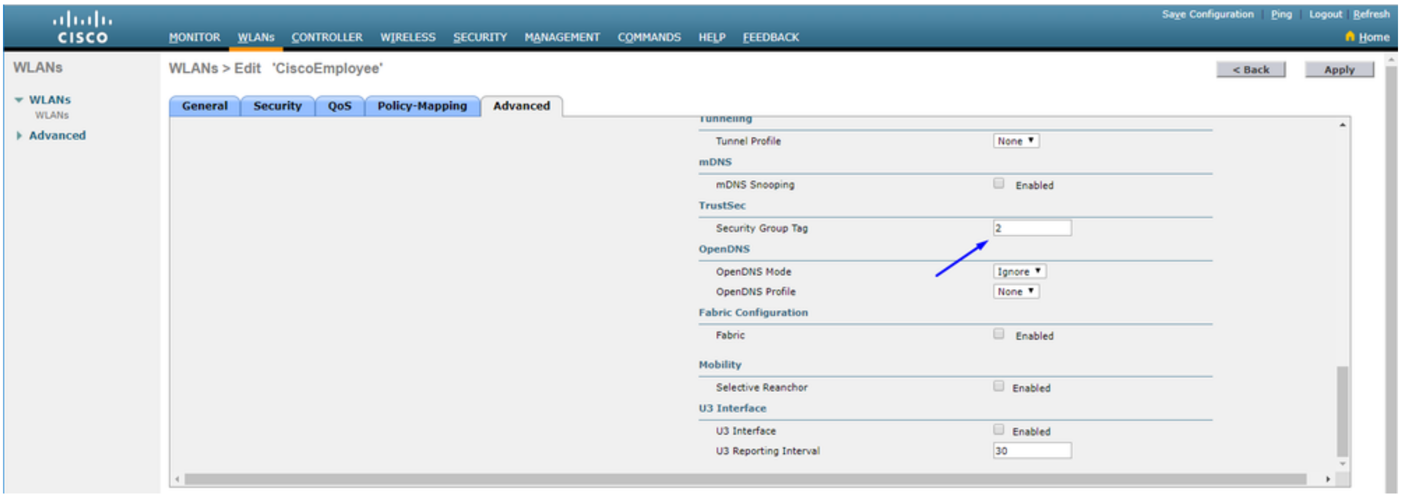
CTS Override Enabled

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)

Atribuir à WLC e ao ponto de acesso o SGT de 2 (TrustSec_Devices)

Dê à WLC+WLAN um SGT de 2 (TrustSec_Devices) para permitir o tráfego (SSH, HTTPS e CAPWAP) de/para a WLC + AP através do 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

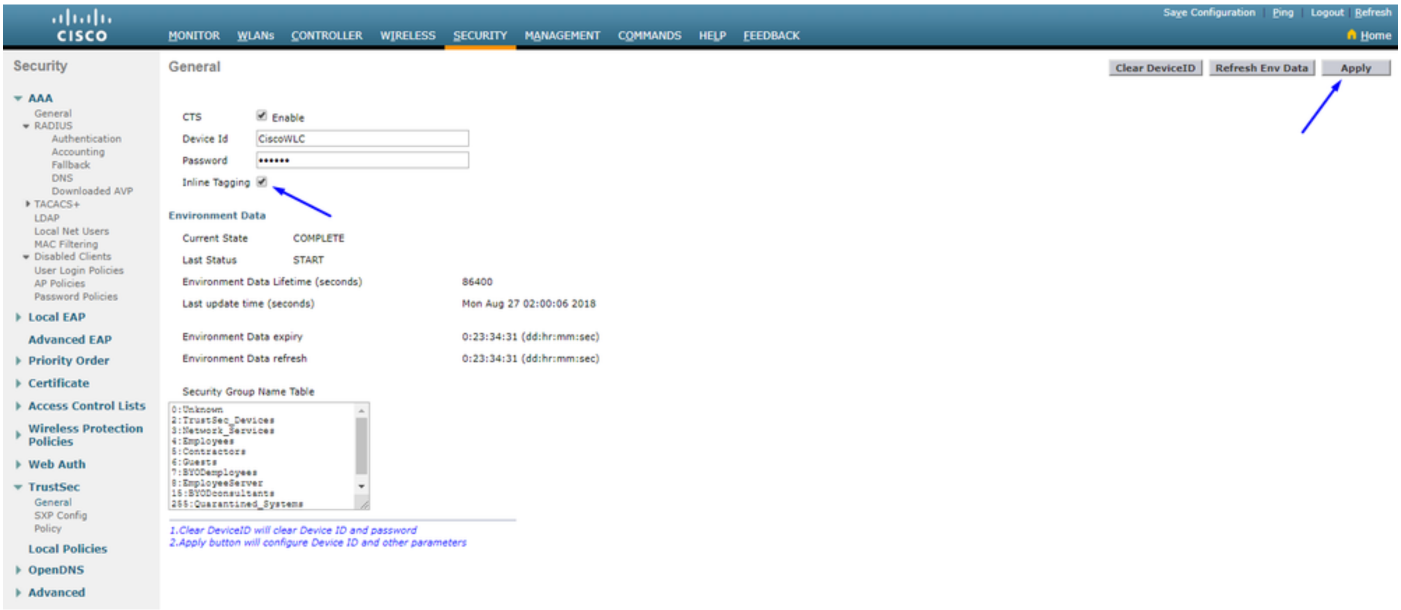
Selective Reanchor: □ Enabled

U3 Interface

U3 Interface: □ Enabled

U3 Reporting Interval: 30

Habilitar marcação embutida no 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)

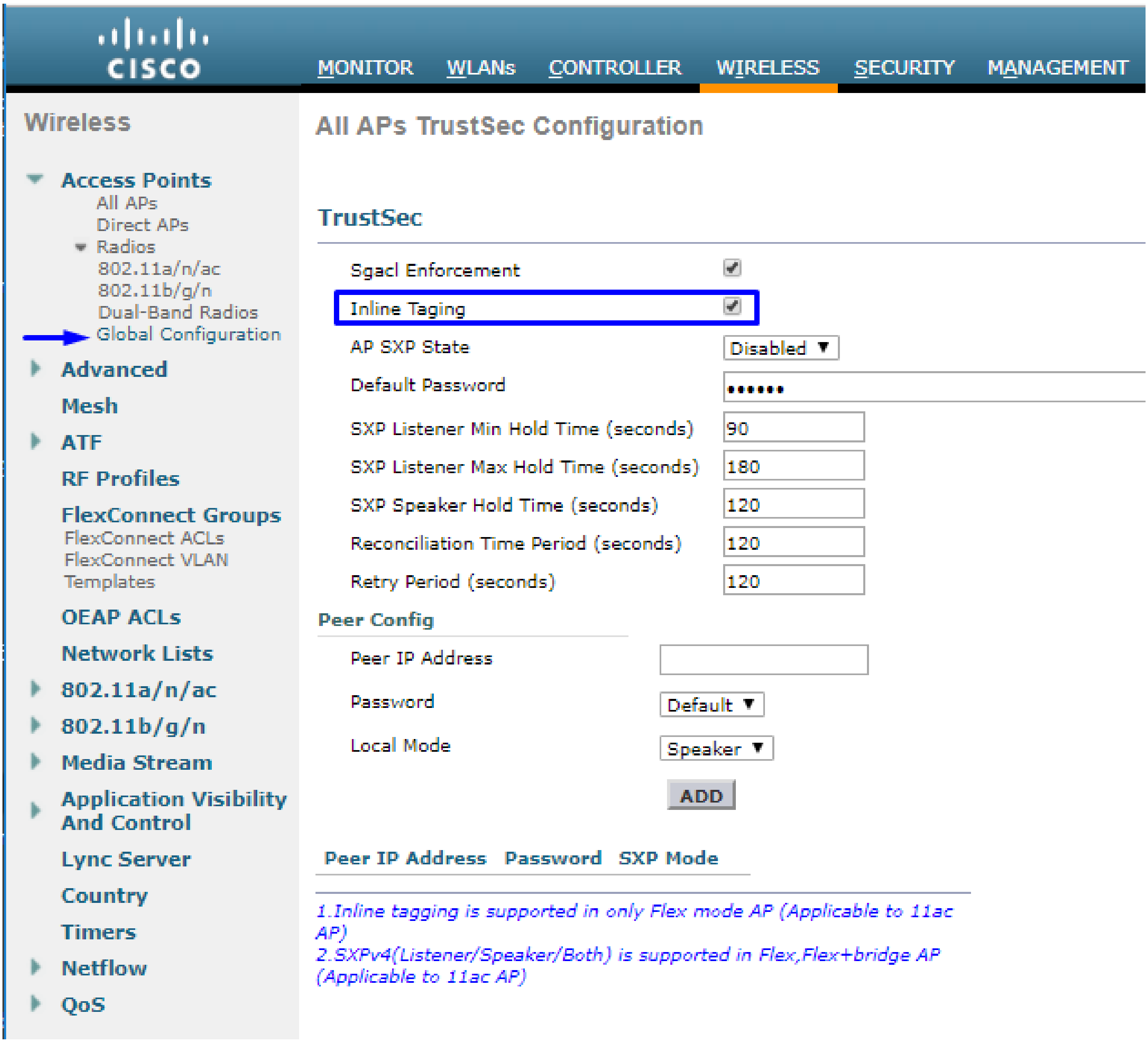
Environment Data refresh: 0:23:34:31 (dd:hr:mm:sec)

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

Em **Wireless > Access Points > Global Configuration** role para baixo e selecione **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

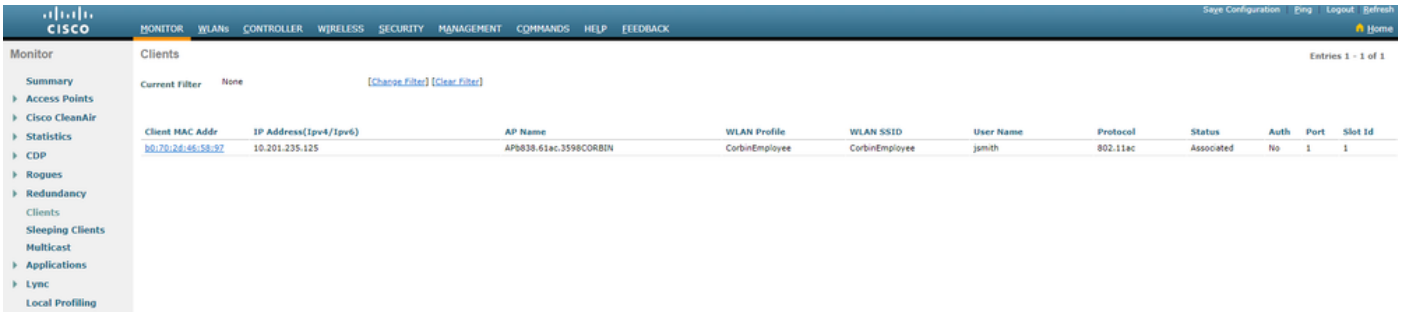
1.Inline tagging is supported in only Flex mode AP (Applicable to 11ac AP)
2.SXPv4(Listener/Speaker/Both) is supported in Flex,Flex+bridge AP (Applicable to 11ac AP)

Ativar marcação em linha no switch Catalyst

<#root>

```
CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

CatalystSwitch(config-if)#description goestoWLC


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


CatalystSwitch(config-if)#switchport trunk allowed vlan 15,455,463,1115


CatalystSwitch(config-if)#switchport mode trunk
CatalystSwitch(config-if)#cts role-based enforcement
CatalystSwitch(config-if)#cts manual
CatalystSwitch(config-if-cts-manual)#policy static sgt 2 trusted
```

Verificar



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 | SGACL inc

Queda de SGACL IPv4 de saída (454): 10 quadros

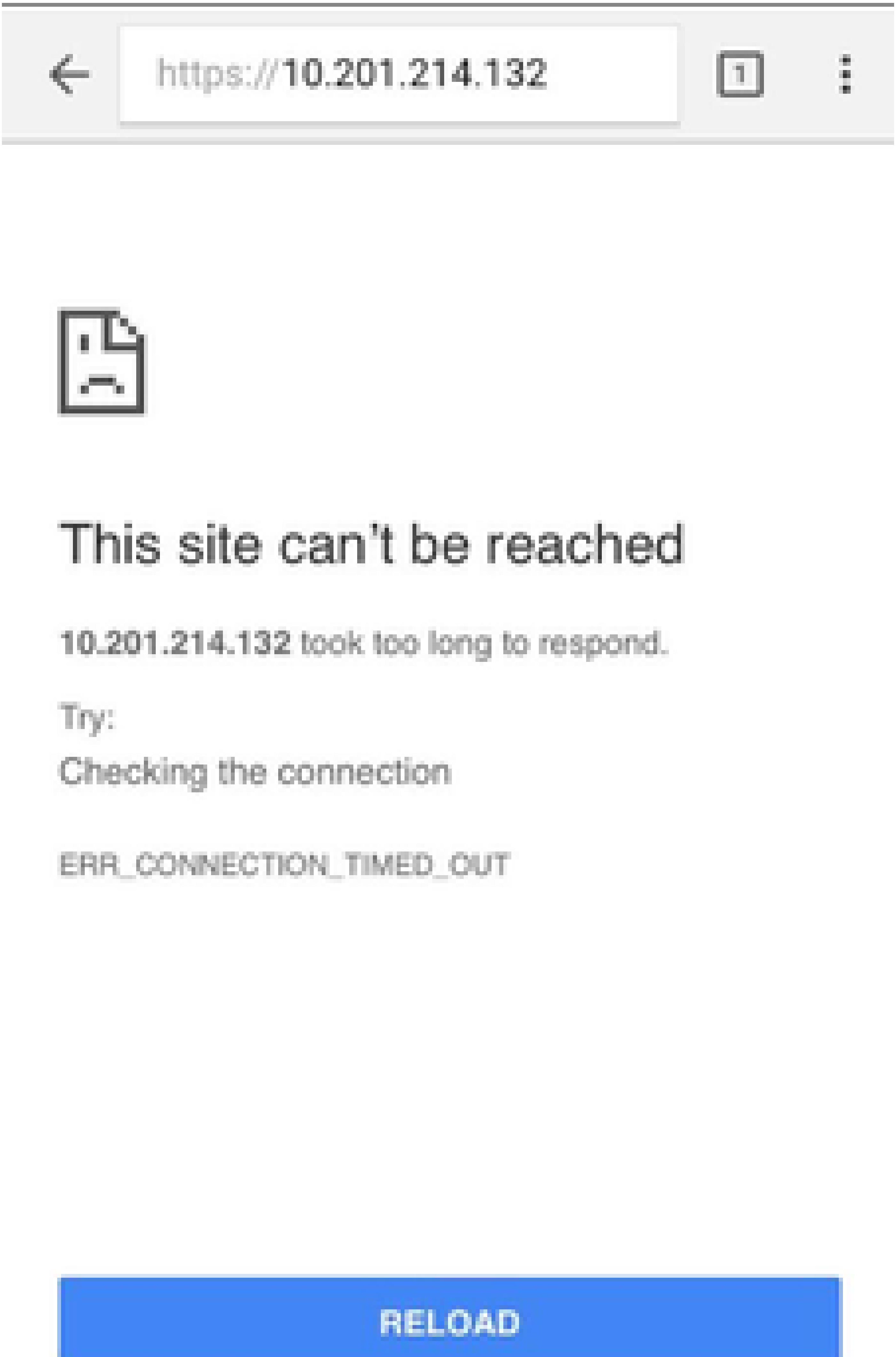
Queda de SGACL IPv6 de saída (455): 0 quadros

Queda de célula SGACL IPv4 de saída (456): 0 quadros

Queda de célula SGACL IPv6 de saída (457): 0 quadros

Dica: se você usar um Cisco ASR, Nexus ou Cisco ASA, o documento listado aqui pode ajudar a verificar se suas marcações SGT estão sendo aplicadas: Guia de solução de problemas do TrustSec.

Autentique para rede sem fio com o nome de usuário jsmith password Admin123 - você encontra a ACL deny no 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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.