Configurazione di TrustSec (SGT) con ISE (Inline Tagging)

Sommario

Introduzione

In questo documento viene descritto come configurare e verificare TrustSec su uno switch Catalyst e un controller LAN wireless con Identity Services Engine.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei componenti Cisco TrustSec (CTS)
- Conoscenze base della configurazione CLI degli switch Catalyst
- Conoscenze base di configurazione GUI dei Cisco Wireless LAN Controller (WLC)
- Esperienza nella configurazione di Identity Services Engine (ISE)

Requisiti

È necessario che Cisco ISE sia installato nella rete e che gli utenti finali eseguano l'autenticazione a Cisco ISE con 802.1x (o un altro metodo) quando si connettono a una rete wireless o cablata. Cisco ISE assegna al traffico un codice SGT (Security Group Tag) dopo l'autenticazione alla rete wireless.

Nell'esempio, gli utenti finali vengono reindirizzati al portale Cisco ISE Bring Your Own Device (BYOD) e ricevono un certificato che consente di accedere in modo sicuro alla rete wireless con EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) una volta completate le fasi del portale BYOD.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software:

- Cisco Identity Services Engine, versione 2.4
- Cisco Catalyst 3850 Switch, versione 3.7.5E
- Cisco WLC, versione 8.5.120.0
- Cisco Aironet Wireless Access Point in modalità locale

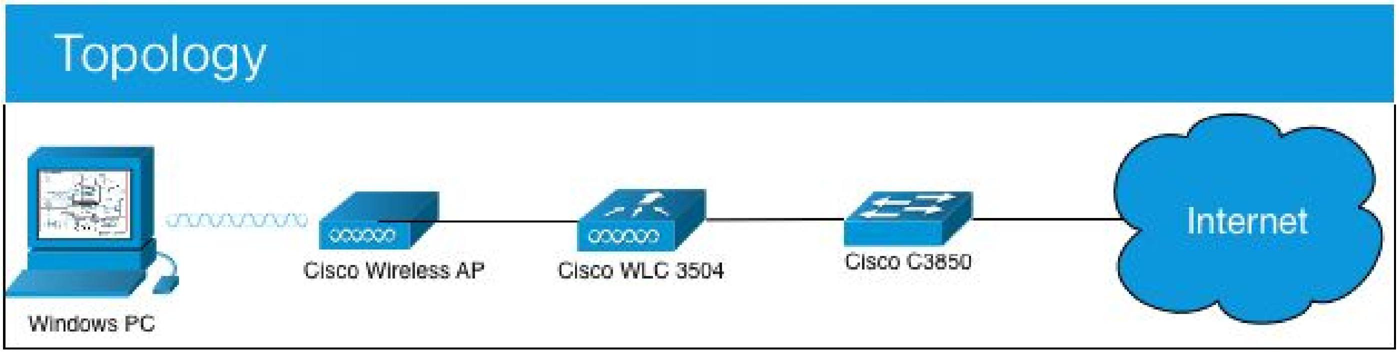
Prima di implementare Cisco TrustSec, verificare che la versione software e lo switch Cisco Catalyst e/o i modelli Cisco WLC+AP supportino:

- Tag TrustSec/Security Group
- Applicazione di tag in linea (in caso contrario, è possibile utilizzare SXP anziché Inline Tagging)
- Mapping IP-SGT statico (se necessario)
- Mapping statici da subnet a SGT (se necessario)
- Mapping VLAN-SGT statici (se necessario)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Nell'esempio, il WLC contrassegna i pacchetti come SGT 15 se provenienti da un consulente e + SGT 7 se provenienti da un dipendente.

Lo switch rifiuta questi pacchetti se sono da SGT 15 a SGT 8 (i consulenti non possono accedere ai server contrassegnati come SGT 8).

Lo switch consente questi pacchetti se sono da SGT 7 a SGT 8 (i dipendenti possono accedere ai server contrassegnati come SGT 8).

Obiettivo

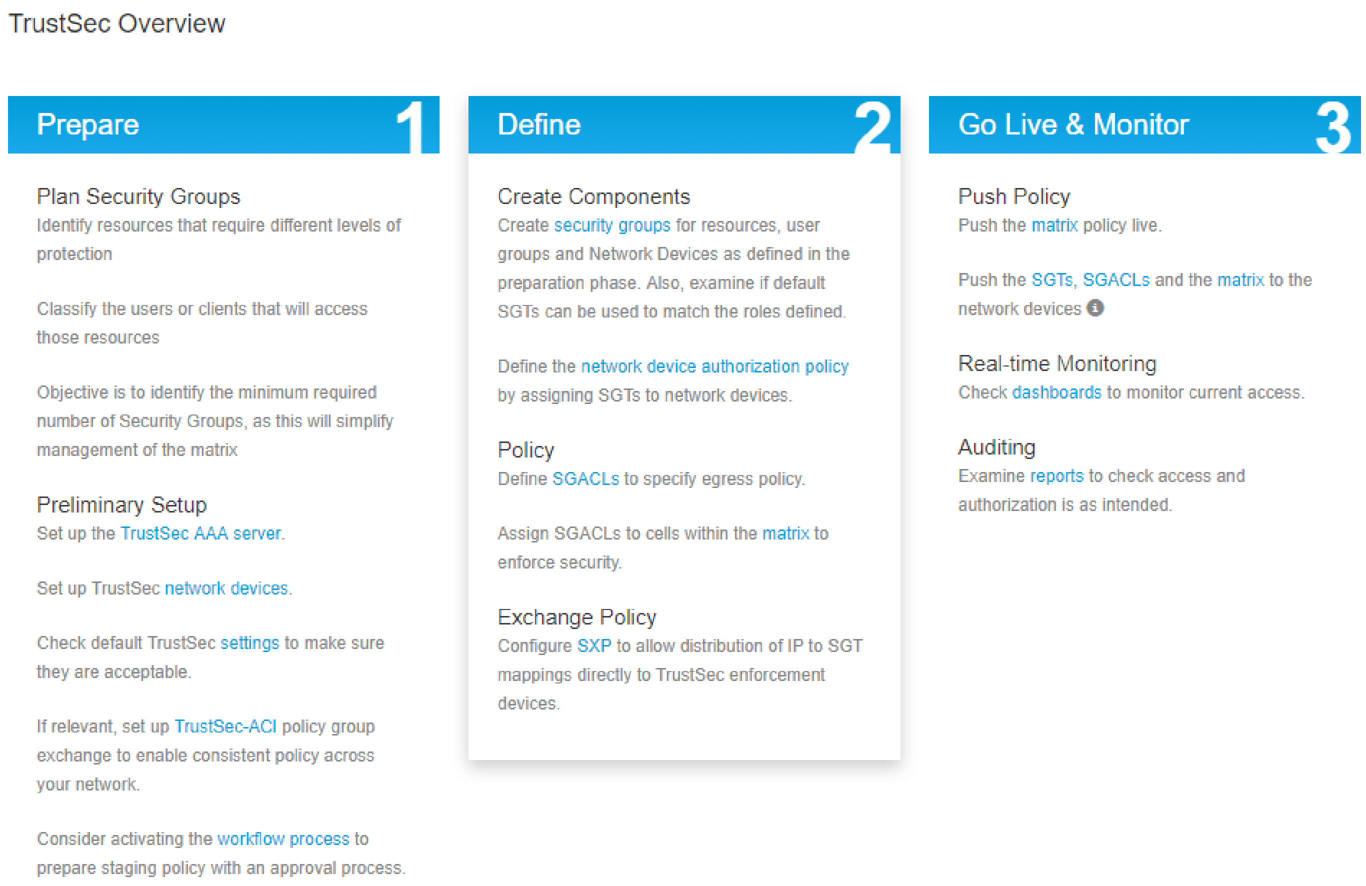
Consentire l'accesso a GuestSSID a tutti gli utenti.
Consentire ai consulenti di accedere a EmployeeSSID, ma con accesso limitato.
Consenti ai dipendenti di accedere a EmployeeSSID con accesso completo.

Sul dispositivo bootflash o slot0:	Indirizzo IP	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

Nome	Username	Gruppo AD	SG	SGT
Jason Smith	fabbro	Consulenti	Consulenti BYOD	15
Sally Smith	omino	Dipendenti	Dipendenti BYOD	7
n/d	n/d	n/d	TrustSec_Devices	2

Configurazioni

Configurazione di TrustSec su 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

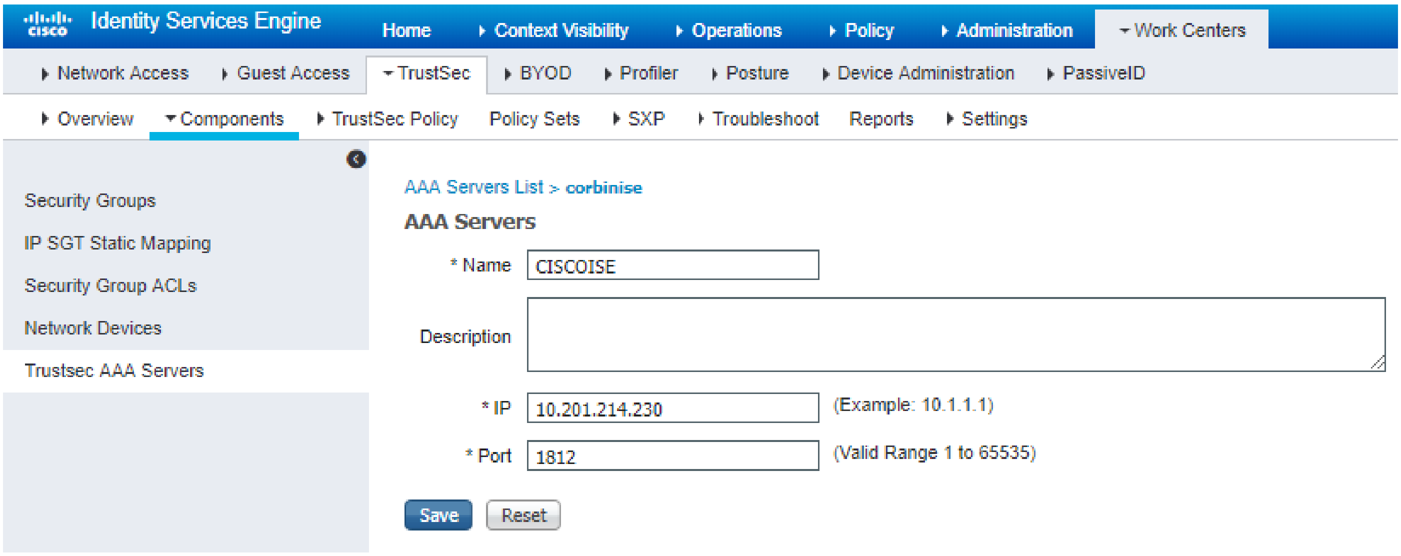
Real-time Monitoring

Check dashboards to monitor current access.

Auditing

Examine reports to check access and authorization is as intended.

Configurazione di Cisco ISE come server TrustSec AAA



AAA Servers List > corbinise

AAA Servers

* Name: CISCOISE

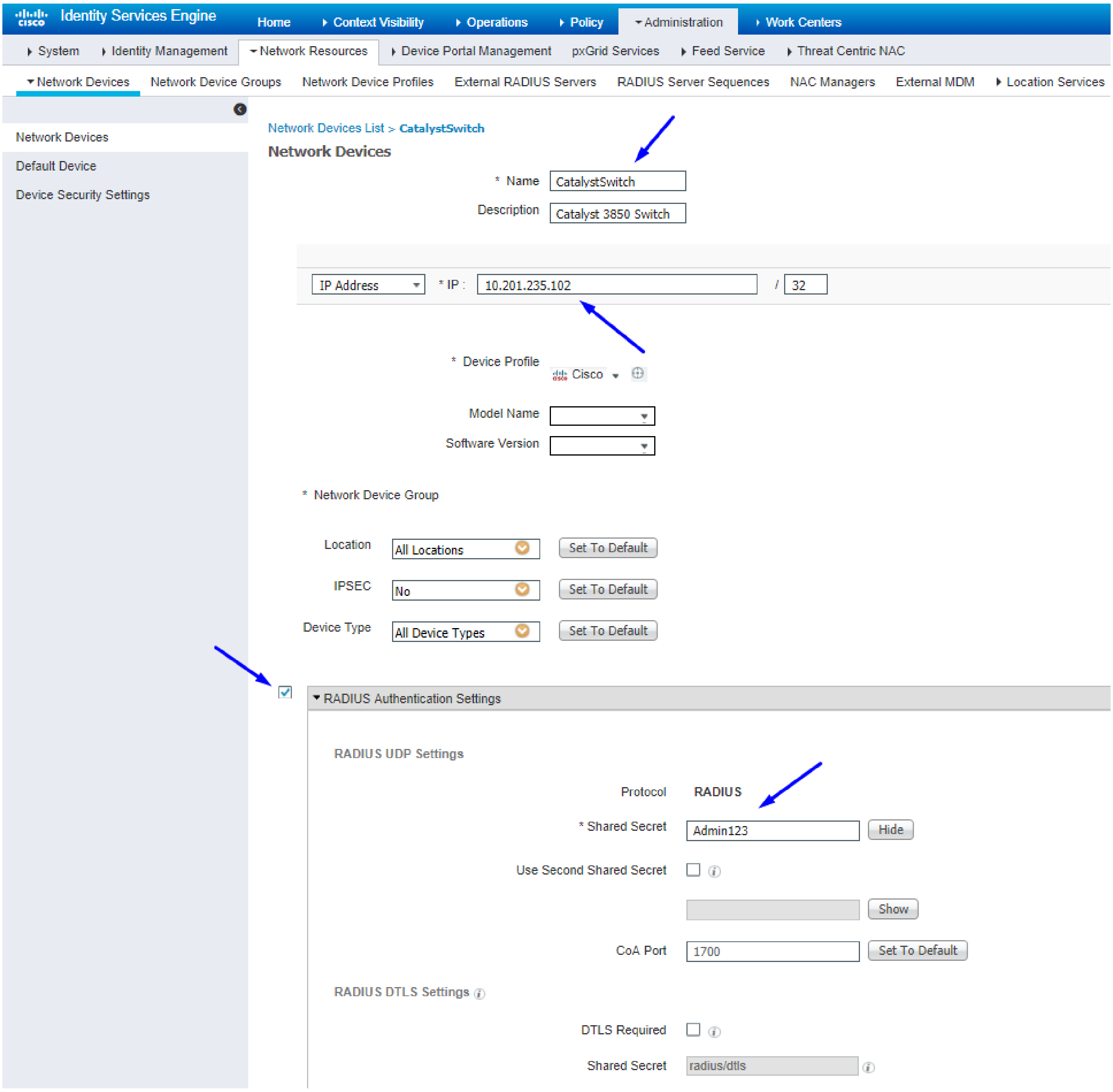
Description:

* IP: 10.201.214.230 (Example: 10.1.1.1)

* Port: 1812 (Valid Range 1 to 65535)

Save   Reset

Configurazione e verifica dell'aggiunta dello switch come dispositivo RADIUS 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 — 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

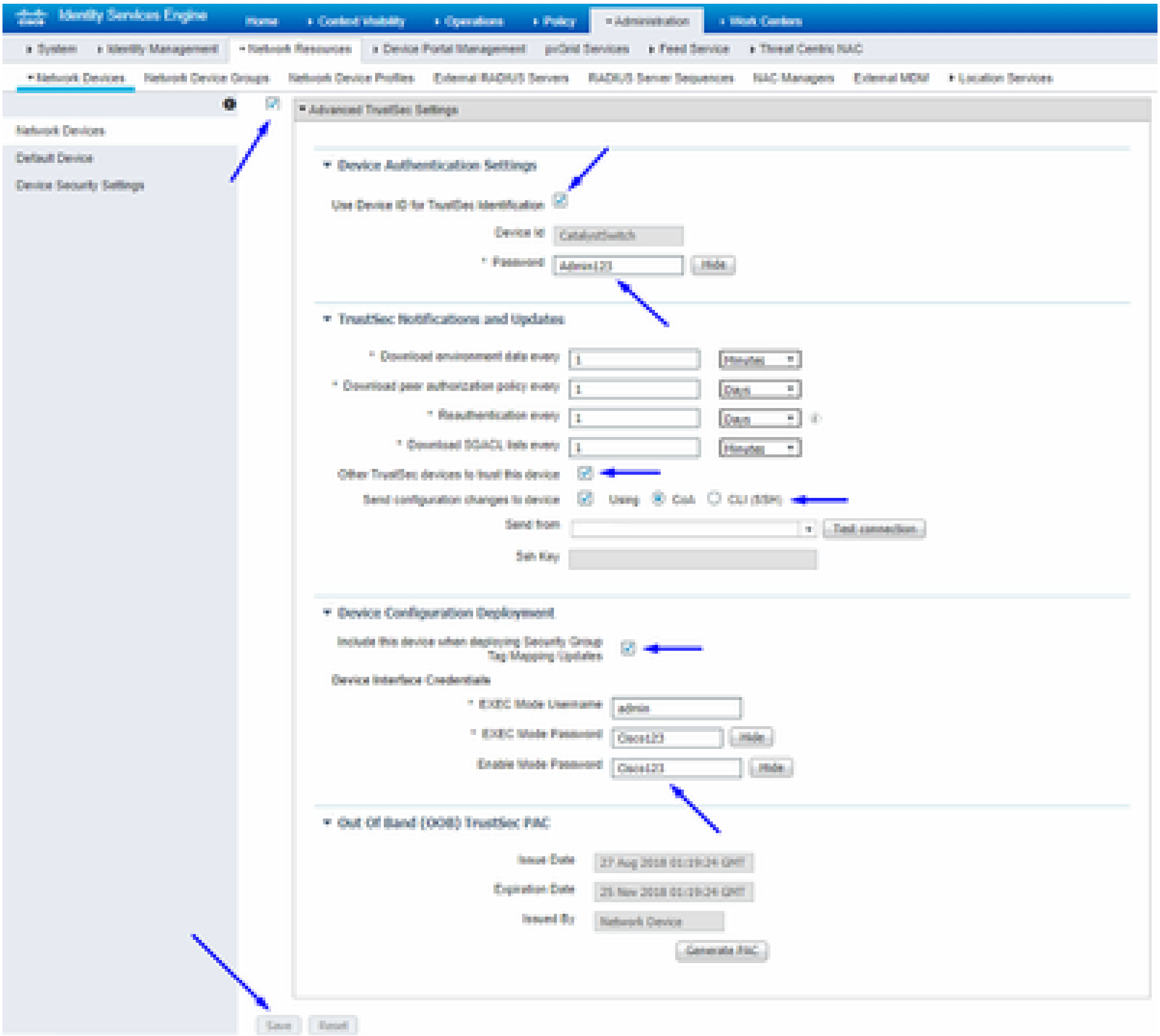
DTLS Required: □

Shared Secret: radius/dtls

Configurazione e verifica dell'aggiunta del WLC come dispositivo TrustSec in Cisco ISE

Immettere le credenziali di accesso per SSH. Ciò consente a Cisco ISE di implementare i mapping IP-SGT statici sullo switch.

Queste impostazioni vengono create nell'interfaccia utente grafica Web di Cisco ISEWork Centers > TrustSec > Components > IP SGT Static Mappings in base a quanto mostrato di seguito:



☑ 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

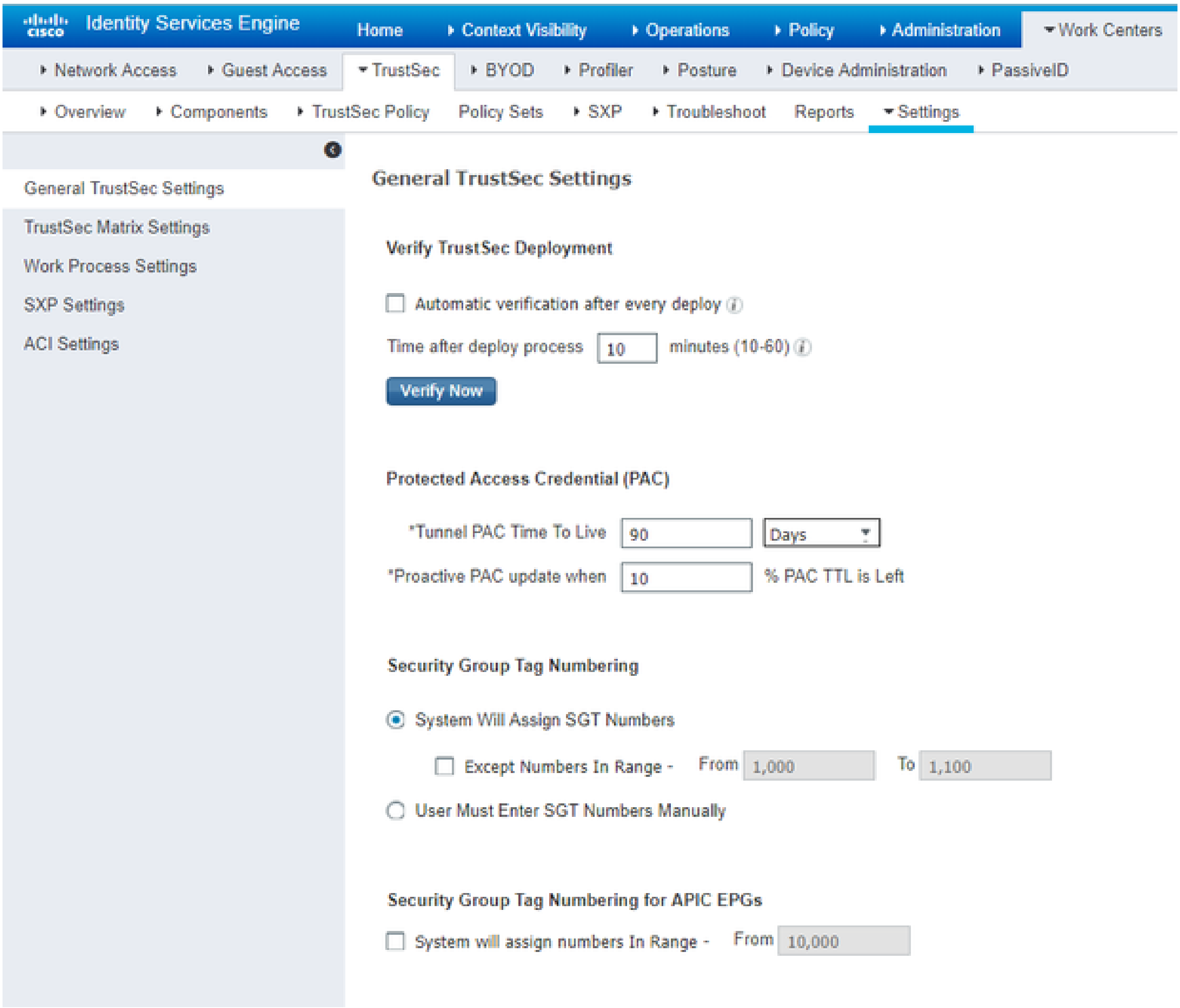
[Generate PAC]

[Save] [Reset]

Suggerimento: se non è stato ancora configurato il protocollo SSH sullo switch Catalyst, è possibile usare questa guida: How to Configure Secure Shell (SSH) on Catalyst Switch.

Suggerimento: se non si desidera abilitare Cisco ISE per accedere allo switch Catalyst su SSH, è possibile creare mapping IP-SGT statici sullo switch Catalyst tramite CLI (mostrato in un passaggio qui).

Verificare le impostazioni predefinite di TrustSec per accertarsi che siano accettabili (facoltativo)



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

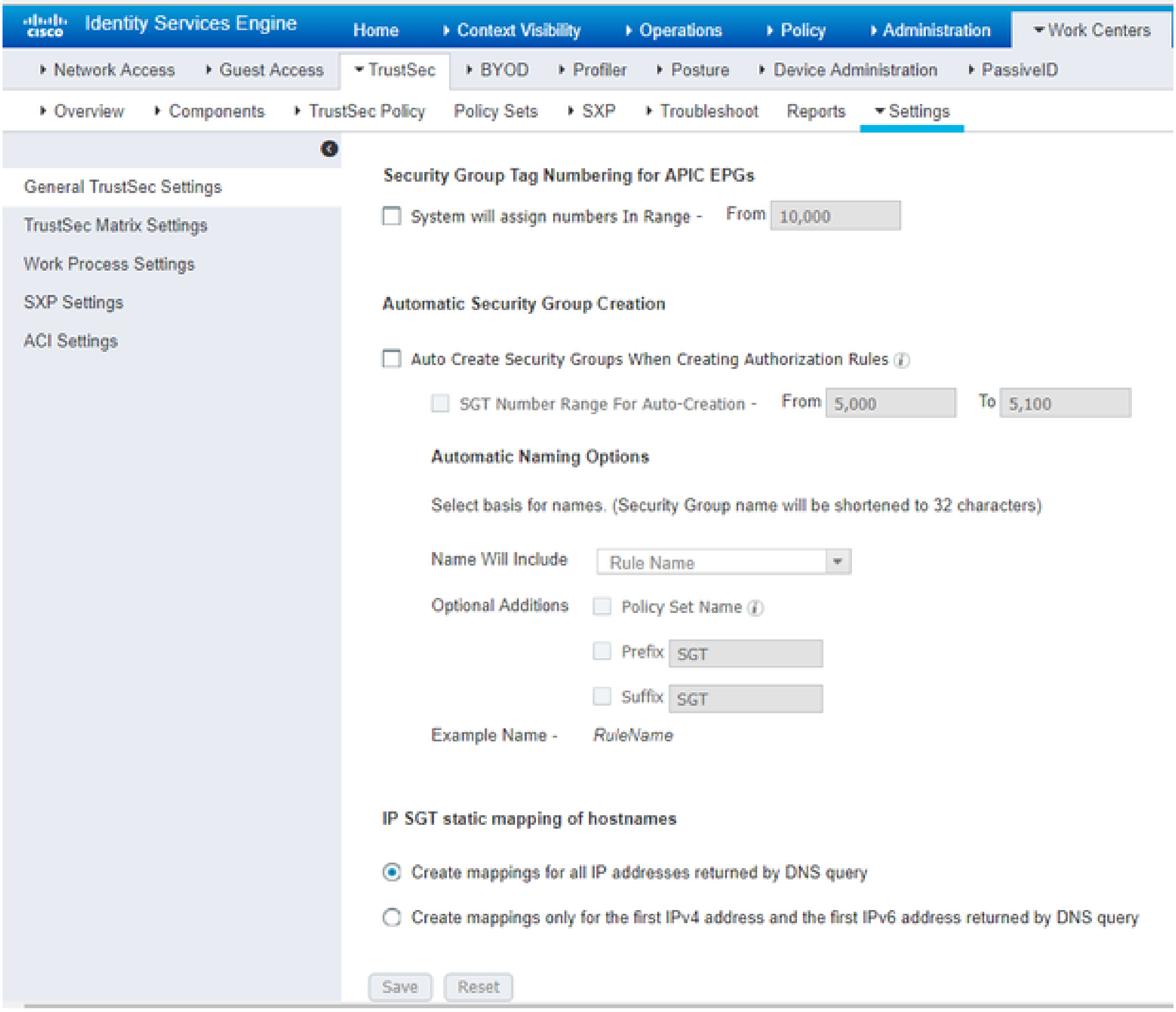
● System Will Assign SGT Numbers

□ 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

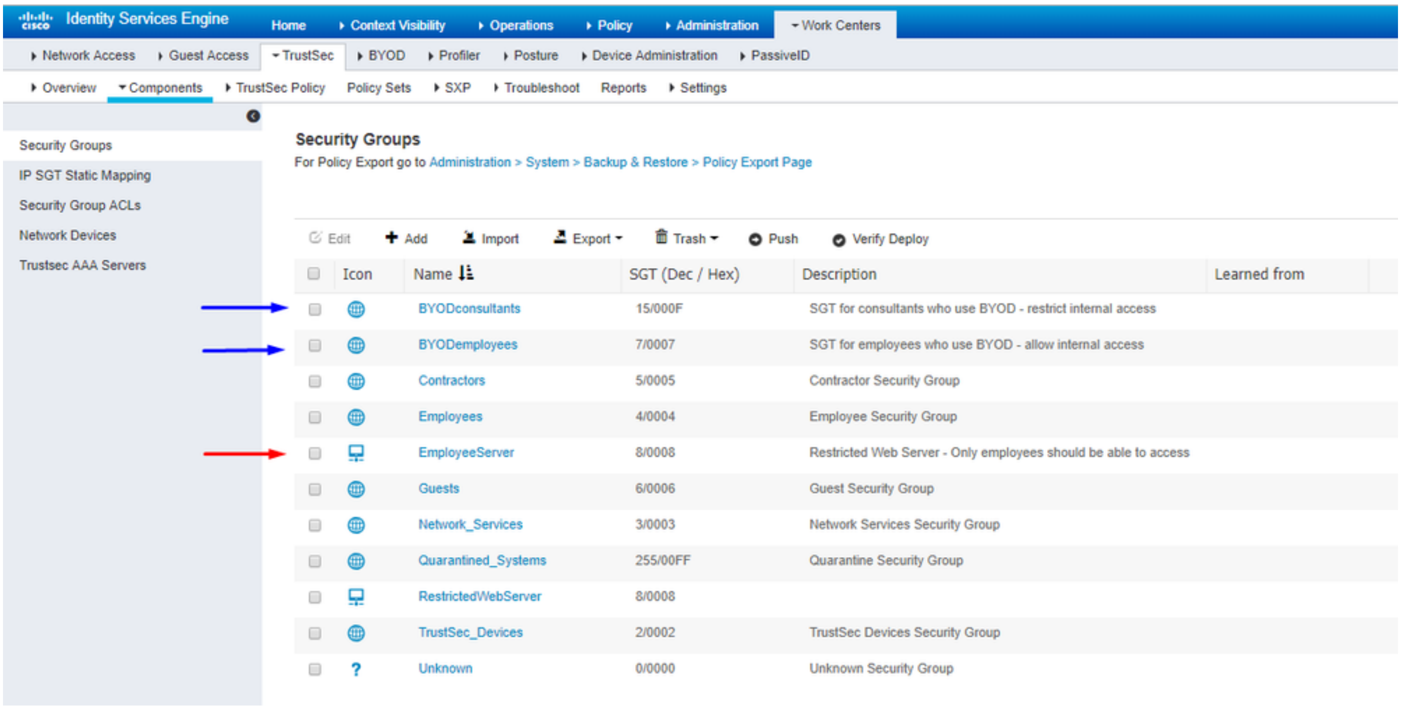
● Create mappings for all IP addresses returned by DNS query

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

Creazione di tag dei gruppi di sicurezza per gli utenti wireless

Crea gruppo di sicurezza per consulenti BYOD - SGT 15

Crea gruppo di sicurezza per dipendenti BYOD - SGT 7



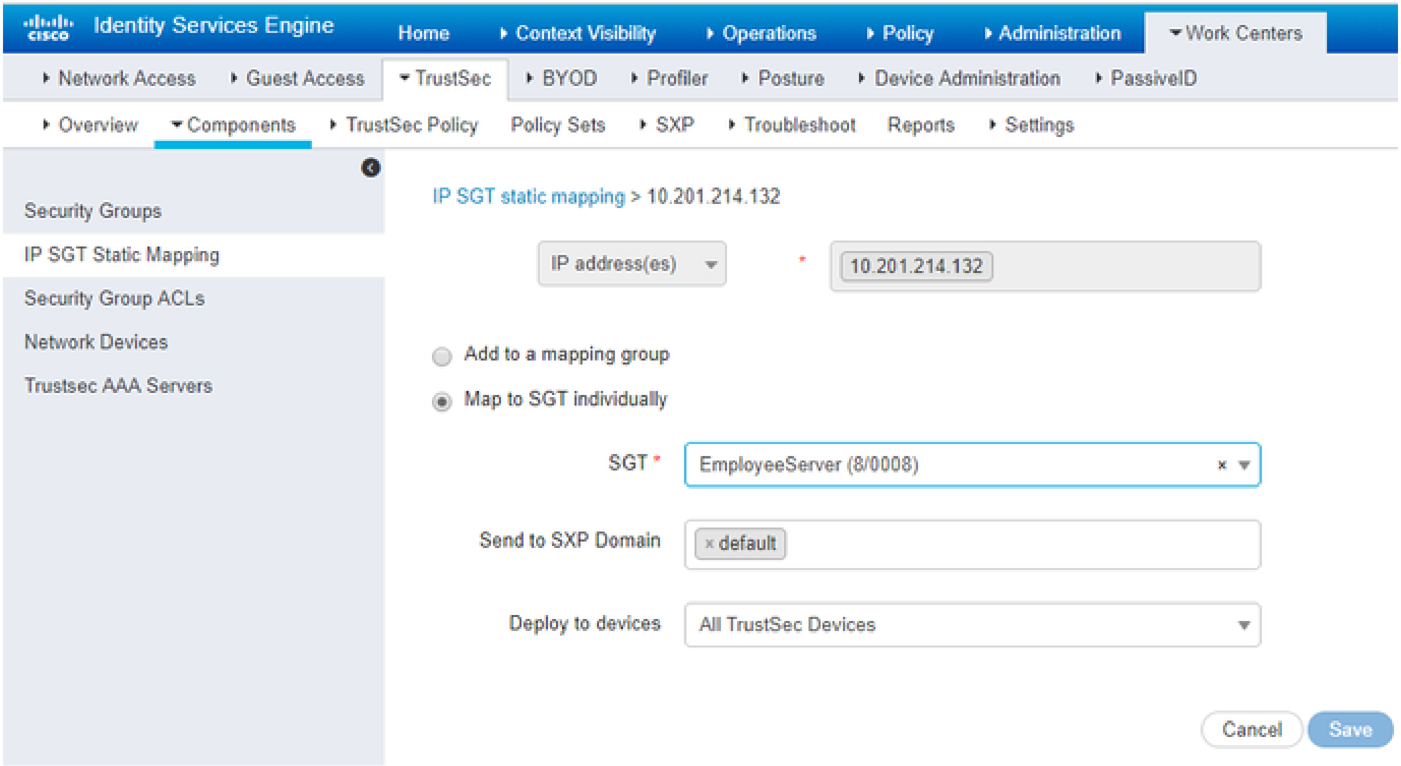
Security Groups

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	

Crea mapping IP-SGT statico per il server Web con restrizioni

Ripetere l'operazione per tutti gli altri indirizzi IP o subnet della rete che non eseguono l'autenticazione a Cisco ISE con MAC Authentication Bypass (MAB), 802.1x, Profiles e così via.



IP SGT static mapping > 10.201.214.132

IP address(es) * 10.201.214.132

○ Add to a mapping group

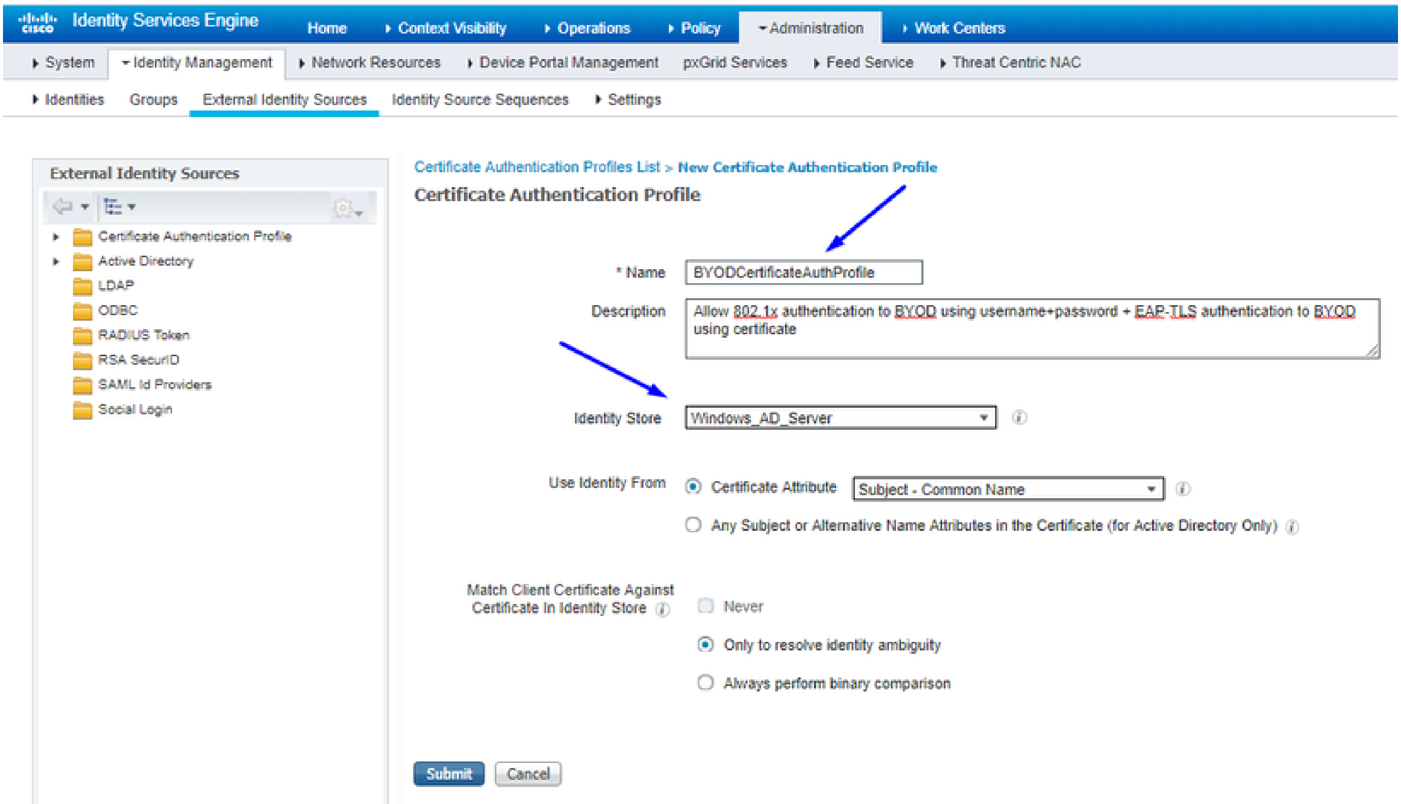
● Map to SGT individually

SGT * EmployeeServer (8/0008)

Send to SXP Domain: default

Deploy to devices: All TrustSec Devices

Crea profilo di autenticazione certificato



* Name: BYODCertificateAuthProfile

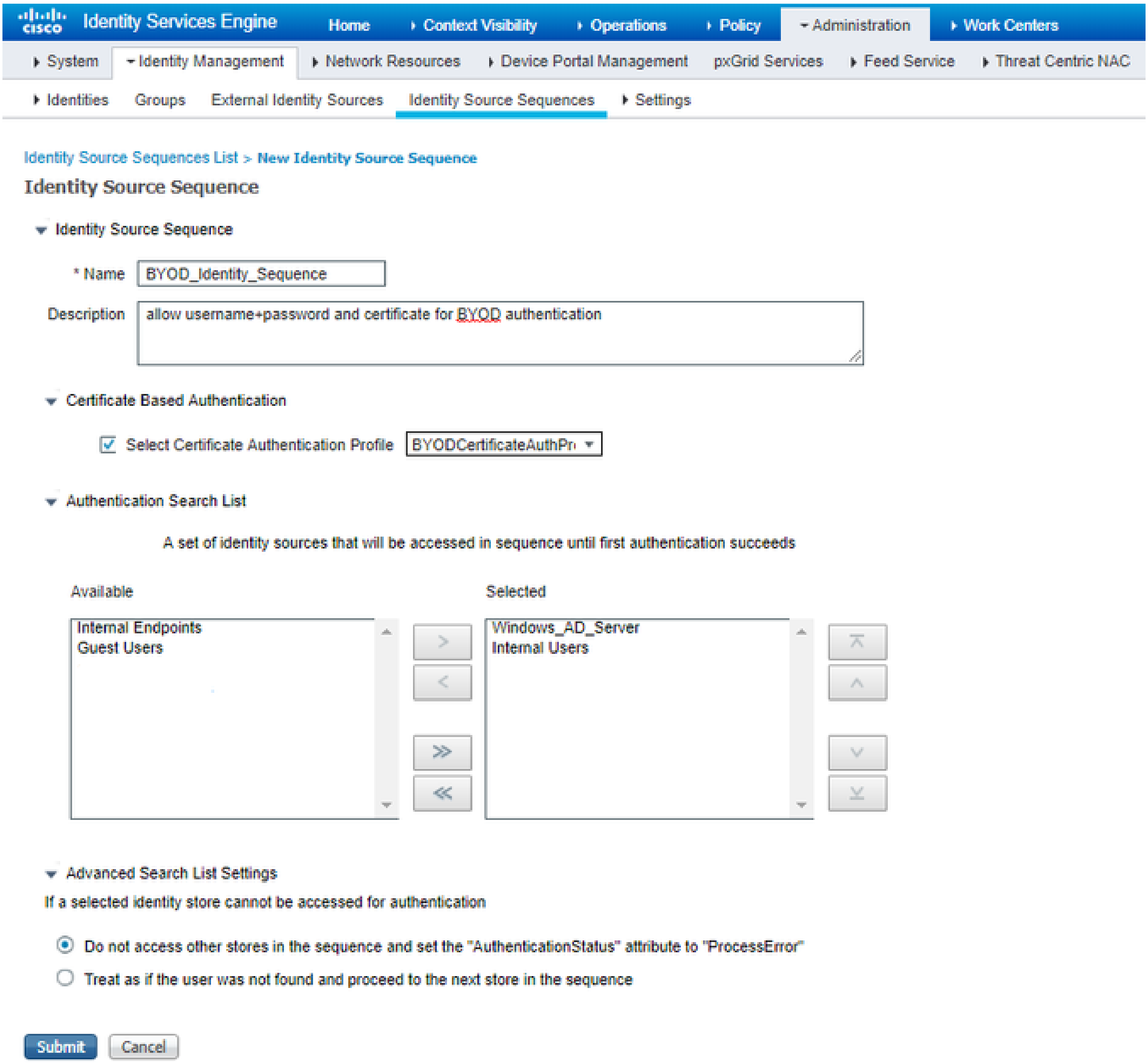
Description: Allow 802.1x authentication to BYOD using username+password + EAP-TLS authentication to BYOD using certificate

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

Crea sequenza di origine identità con il profilo di autenticazione certificato da prima



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

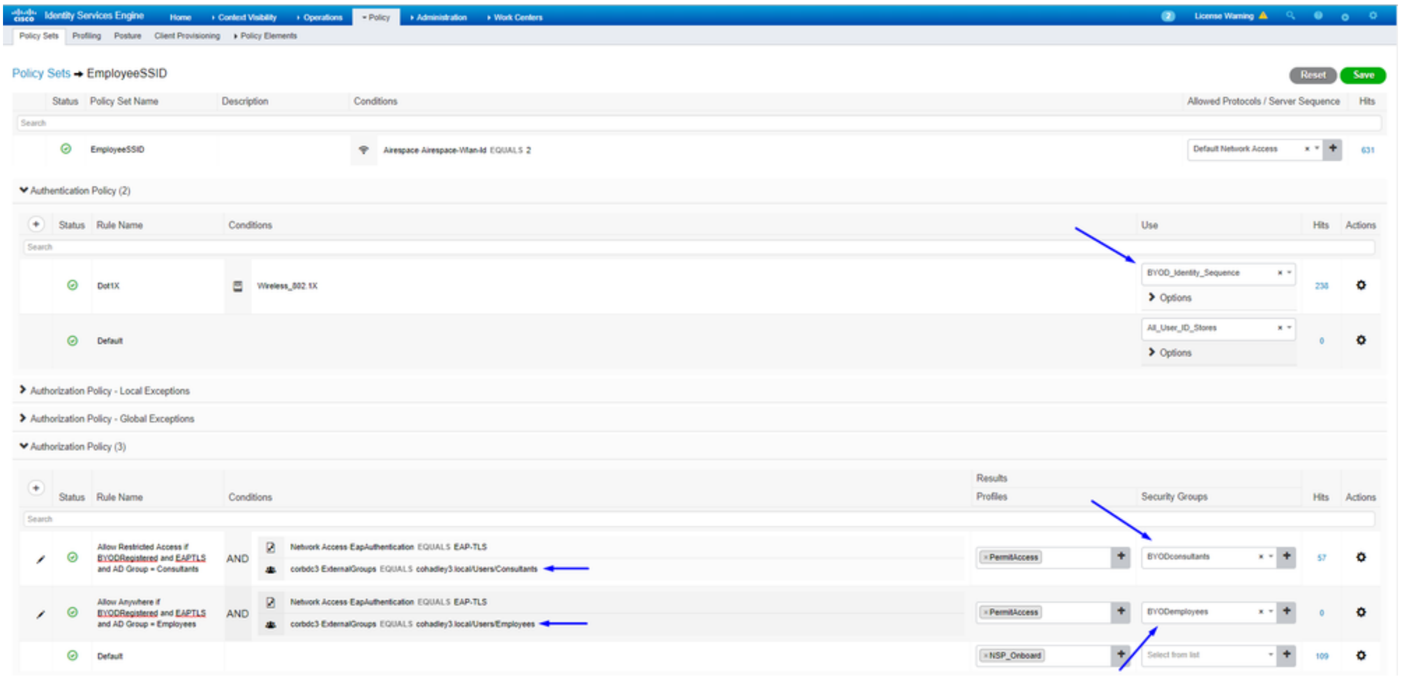
If a selected identity store cannot be accessed for authentication

● 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

Assegnare agli utenti wireless (dipendenti e consulenti) un SGT appropriato

Nome	Username	Gruppo AD	SG	SGT
Jason Smith	fabbro	Consulenti	Consulenti BYOD	15
Sally Smith	omino	Dipendenti	Dipendenti BYOD	7
n/d	n/d	n/d	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	⚙

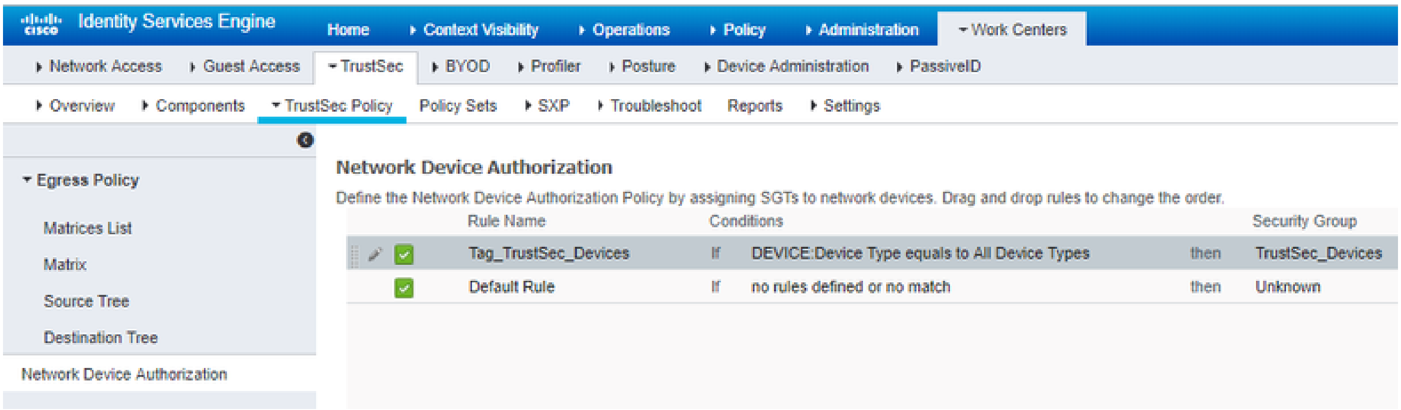
Authorization Policy - Local Exceptions

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	⚙

Assegnazione di SGT ai dispositivi effettivi (switch e WLC)



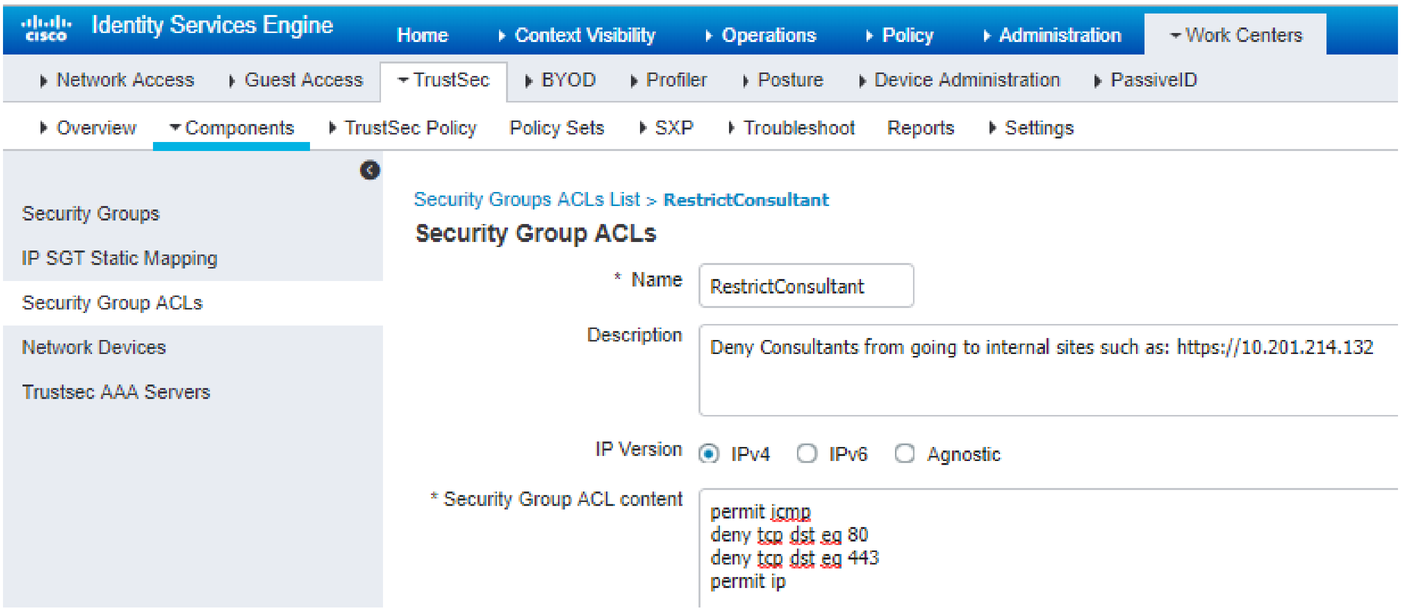
Network Device Authorization

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

Definizione degli SGACL per specificare il criterio di uscita

Consenti ai consulenti di accedere ovunque all'esterno, ma limitando l'accesso interno:



Security Groups ACLs List > **RestrictConsultant**

Security Group ACLs

* Name: RestrictConsultant

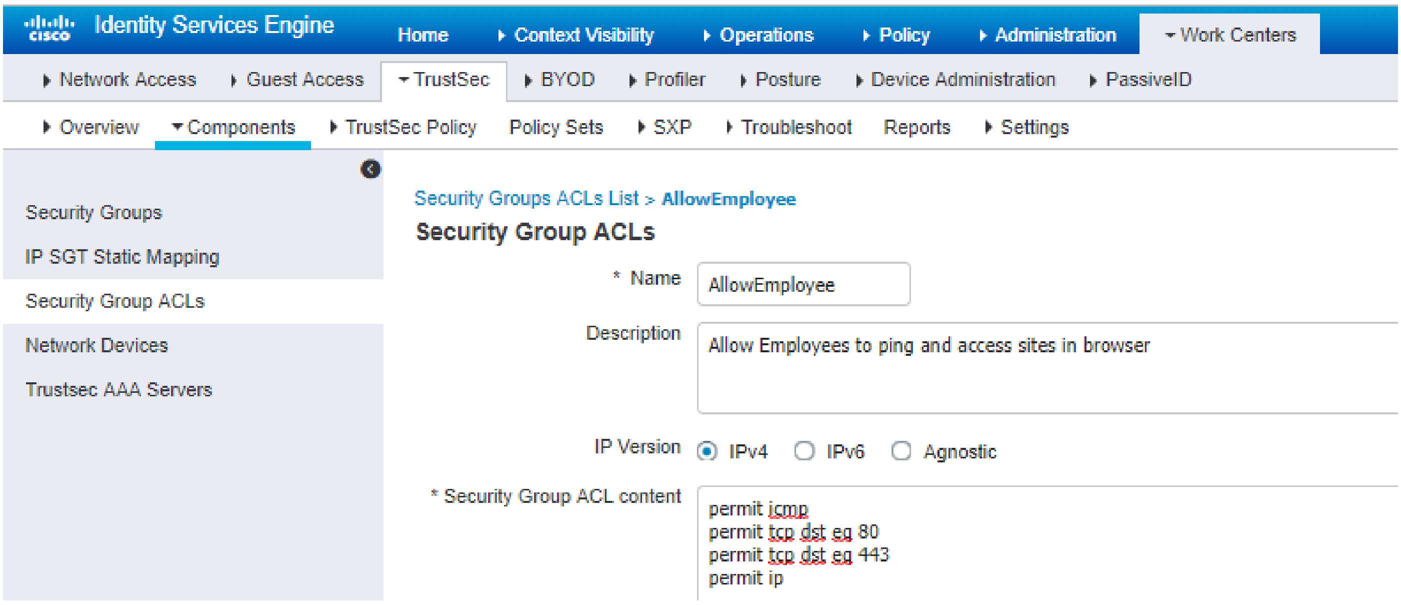
Description: Deny Consultants from going to internal sites such as: https://10.201.214.132

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content

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

Consenti ai dipendenti di accedere ovunque all'esterno e ovunque all'interno:



Security Groups ACLs List > **AllowEmployee**

Security Group ACLs

* Name: AllowEmployee

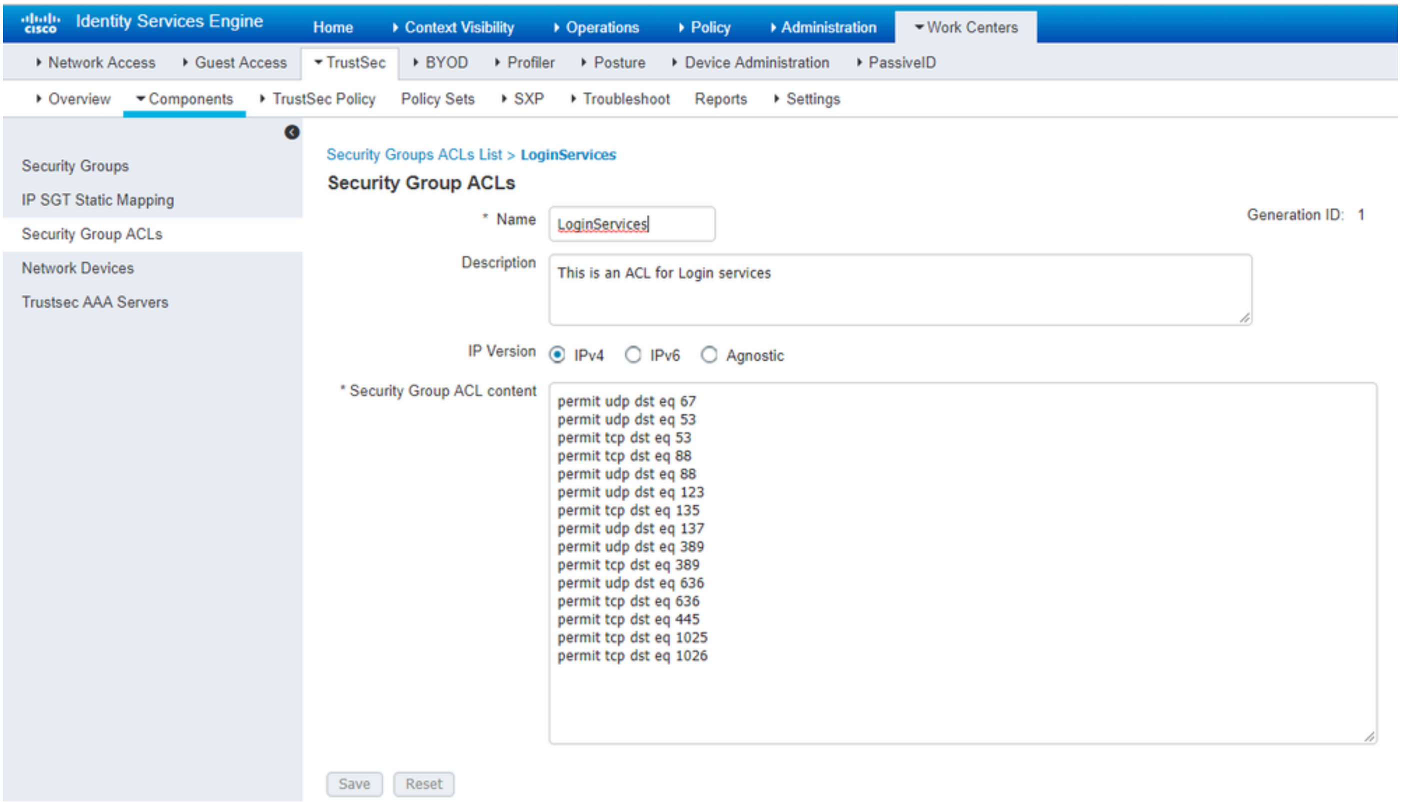
Description: Allow Employees to ping and access sites in browser

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content

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

Consenti ad altre periferiche l'accesso ai servizi di base (facoltativo):



Security Groups ACLs List > **LoginServices**

Security Group ACLs

* Name: LoginServices

Generation ID: 1

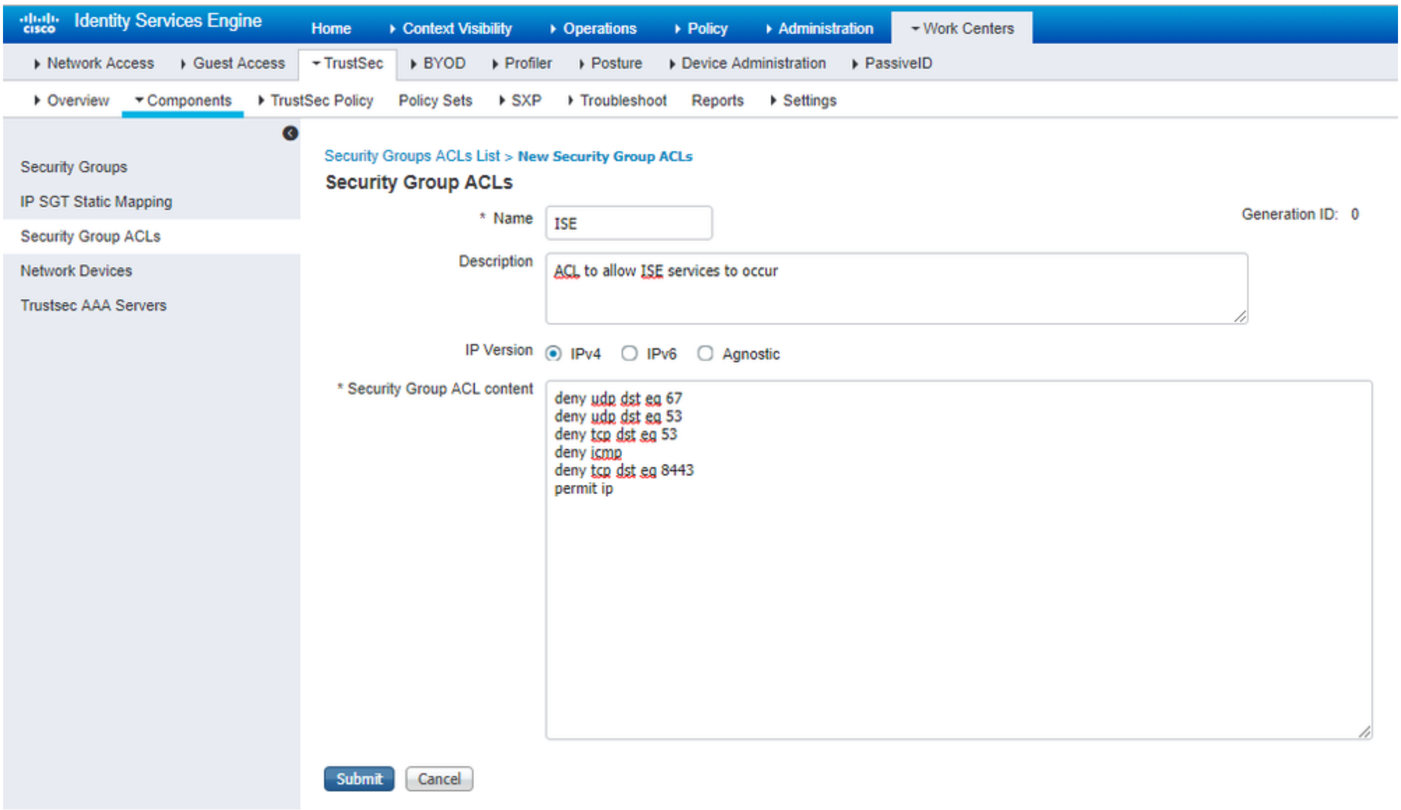
Description: This is an ACL for Login services

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
```

Reindirizzare tutti gli utenti finali a Cisco ISE (per il reindirizzamento del portale BYOD). Non includere il traffico DNS, DHCP, ping o WebAuth poiché non può essere indirizzato a 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

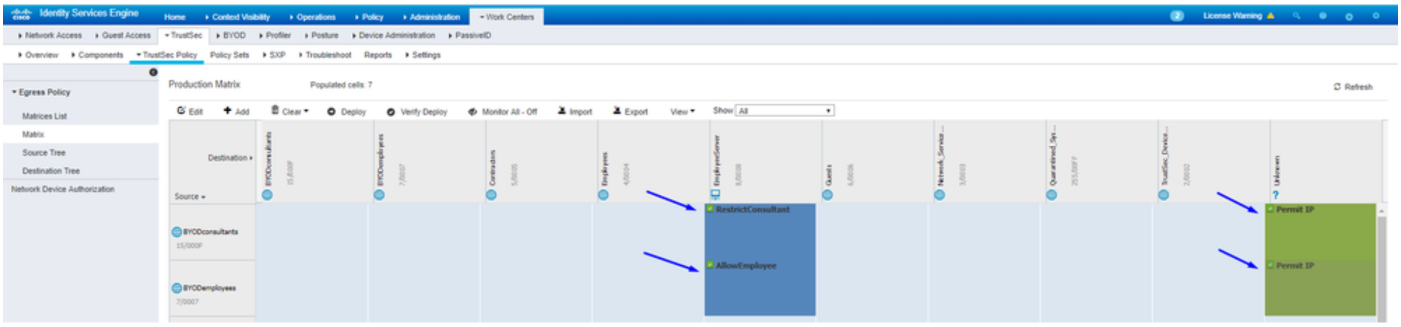
* Security Group ACL content

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

Applicazione degli ACL alla matrice dei criteri di TrustSec in Cisco ISE

Consentire ai consulenti di accedere ovunque all'esterno, limitando al contempo i server Web interni, ad esempio https://10.201.214.132

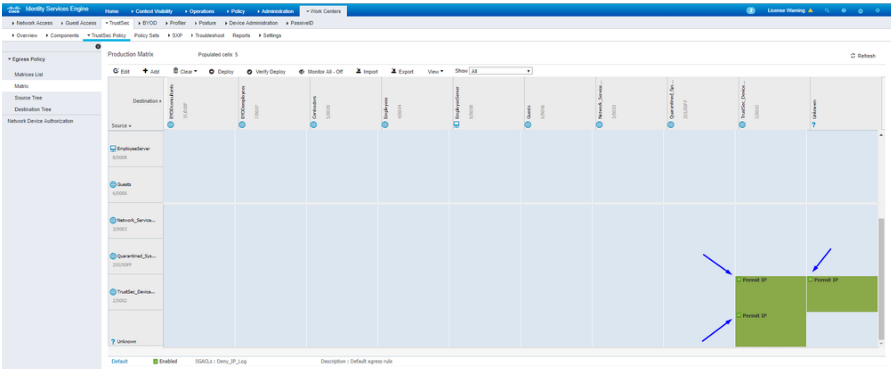
Consenti ai dipendenti di accedere ovunque all'esterno e ai server Web interni:



Production Matrix Populated cells: 7

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

Consentire il traffico di gestione (SSH, HTTPS e CAPWAP) da/verso i dispositivi della rete (switch e WLC) in modo da non perdere l'accesso SSH o HTTPS dopo aver distribuito Cisco TrustSec:

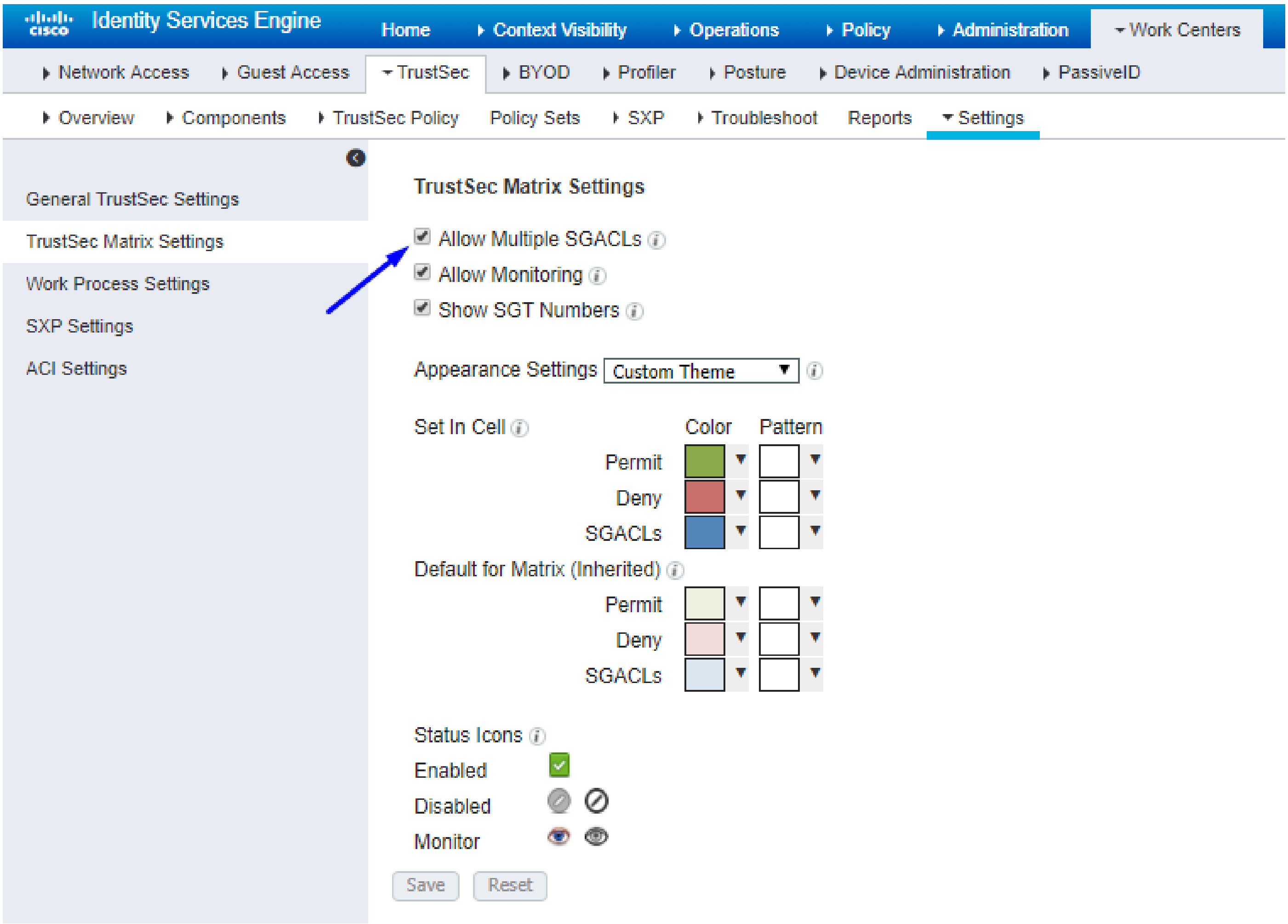


Production Matrix Populated cells: 5

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
EmployeeServer 8/0008										
Guests 6/0006										
Network_Service... 3/0003										
Quarantined_Sys... 255/00FF										
TrustSec_Device... 2/0002									✓ Permit IP	✓ Permit IP
Unknown									✓ Permit IP	

Default ✓ Enabled SGACLs : Deny_IP_Log Description : Default egress rule

Abilitare Cisco ISE a Allow Multiple SGACLs:



TrustSec Matrix Settings

☑ Allow Multiple SGACLs
☑ Allow Monitoring
☑ Show SGT Numbers

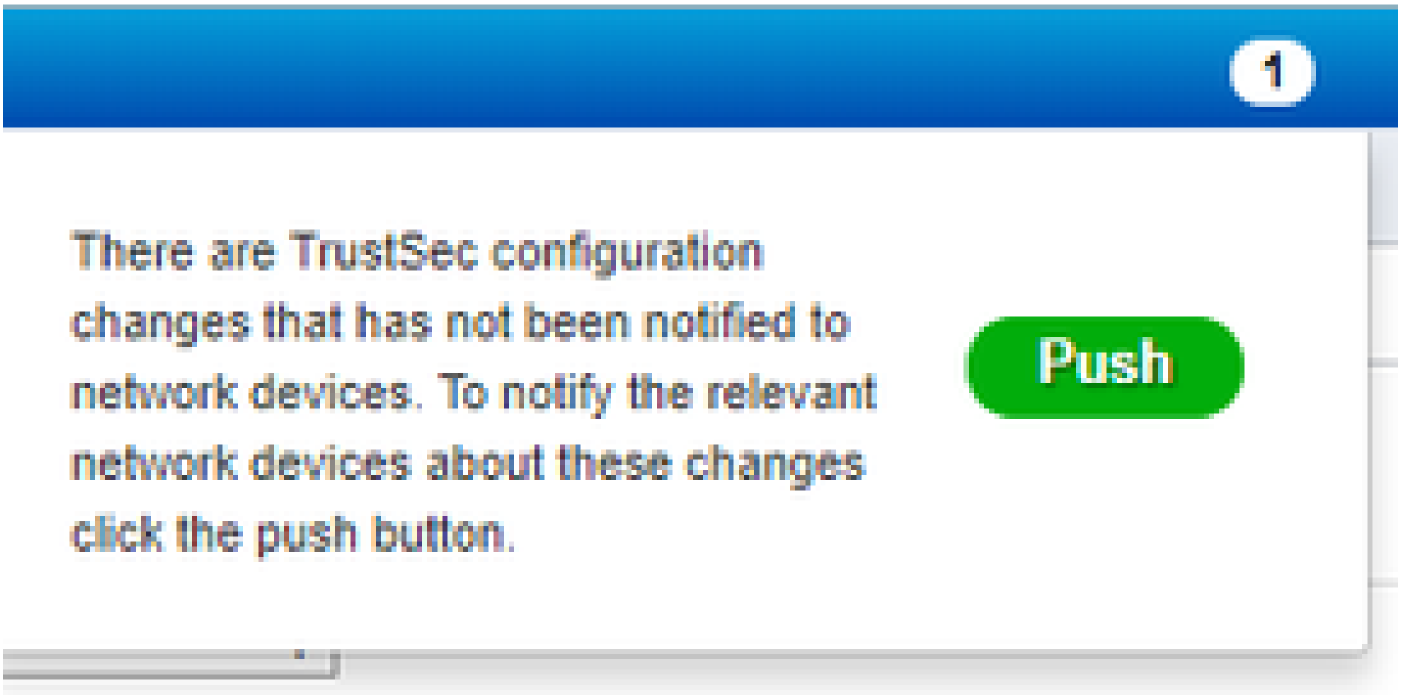
Appearance Settings: Custom Theme

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

Status Icons

Enabled	✓
Disabled	● ⊘
Monitor	👁 👁

Fai clic Push su nell'angolo in alto a destra di Cisco ISE, per ridurre la configurazione ai dispositivi. Questa operazione deve essere ripetuta anche in seguito:



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.

Configurazione di TrustSec sugli switch Catalyst

Configurazione dello switch per l'utilizzo di Cisco TrustSec per AAA su switch Catalyst

Suggerimento: in questo documento si presume che gli utenti wireless abbiano già avuto successo con BYOD da Cisco ISE prima della configurazione mostrata qui.

I comandi mostrati in grassetto erano già stati configurati prima di questo (per far funzionare BYOD Wireless con 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
```

Nota: la chiave PAC deve corrispondere al segreto condiviso RADIUS specificato nella **Administration > Network Devices > Add Device > RADIUS Authentication Settings** sezione.

<#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
```

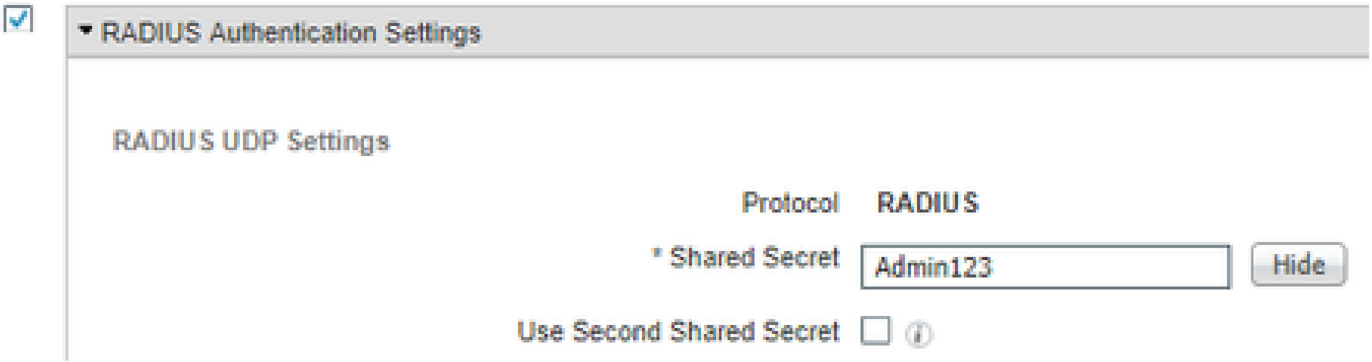
```
CatalystSwitch(config)#radius-server attribute 25 access-request include
```

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

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

Configurazione della chiave PAC sul server RADIUS per autenticare lo switch su 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

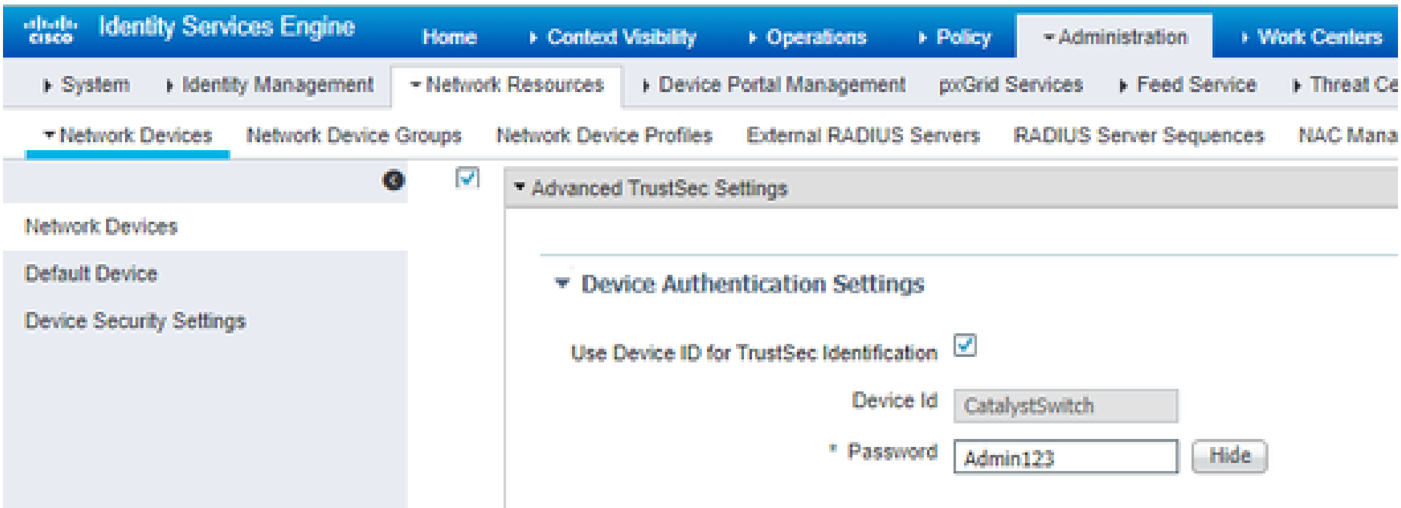
* Shared Secret: Admin123

Use Second Shared Secret: □

Nota: la chiave PAC deve corrispondere al segreto condiviso RADIUS specificato nella **Administration > Network Devices > Add Device > RADIUS Authentication Settings** sezione in Cisco ISE (come mostrato nell'acquisizione schermo).

Configurazione delle credenziali CTS per l'autenticazione dello switch per 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

Nota: le credenziali CTS devono essere uguali all'ID e alla password del dispositivo specificati in Le credenziali CTS devono essere uguali all'ID e alla password del dispositivo specificati nellaAdministration > Network Devices > Add Device > Advanced TrustSec

Settings sezione in Cisco ISE (mostrata nell'acquisizione schermo).

Quindi, aggiornare la PAC in modo che raggiunga di nuovo Cisco ISE:

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

Abilitazione di CTS a livello globale sullo 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)
```

Creare un mapping IP-SGT statico per i server Web con restrizioni (facoltativo)

Poiché il server Web con restrizioni non viene mai autenticato tramite ISE, è necessario contrassegnarlo manualmente con la CLI dello switch o con l'interfaccia grafica Web di ISE, uno dei tanti server Web di Cisco.

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

Verifica di TrustSec sugli 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
```

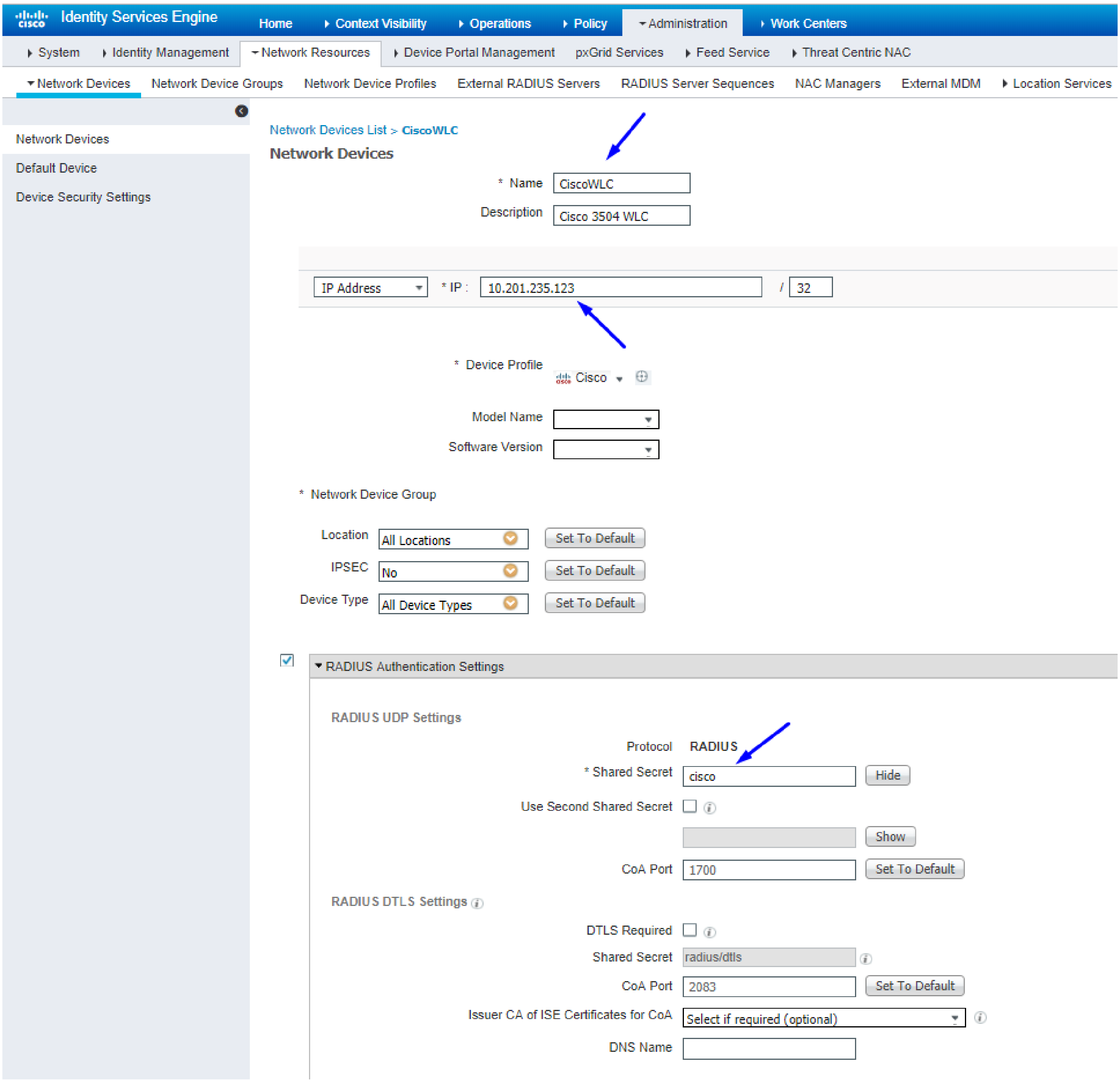
```
CatalystSwitch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

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
```

Configura TrustSec su WLC

Configurazione e verifica dell'aggiunta del WLC come dispositivo RADIUS in Cisco ISE



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

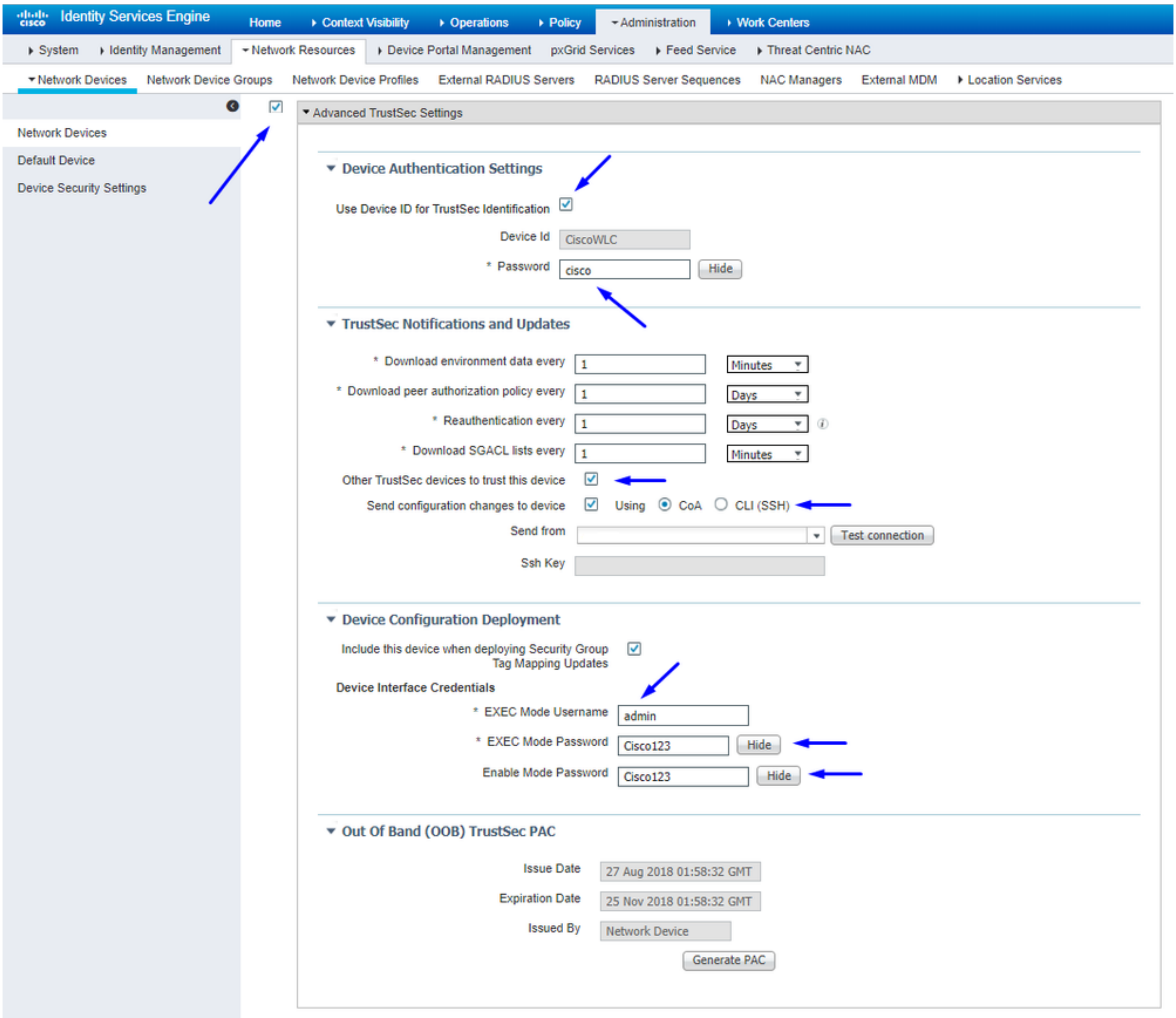
CoA Port: 2083

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

DNS Name:

Configurazione e verifica dell'aggiunta del WLC come dispositivo TrustSec in Cisco ISE

Questo passaggio consente a Cisco ISE di distribuire i mapping IP-SGT statici sul WLC. Questi mapping sono stati creati nella GUI Web di Cisco ISE in **Work Centers > TrustSec > Components > IP SGT Static Mappings** in un passaggio precedente.



☑ 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

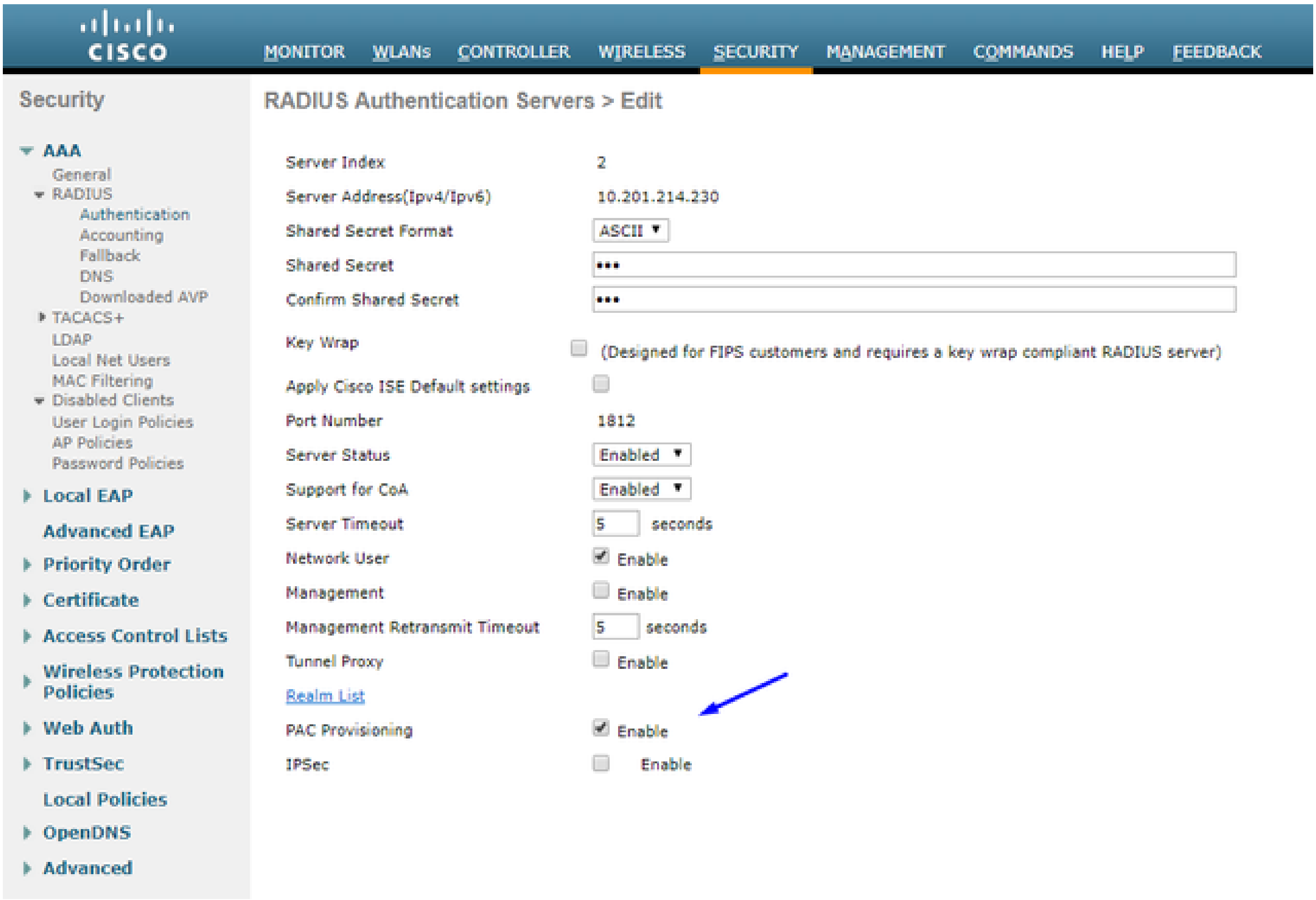
Issue Date: 27 Aug 2018 01:58:32 GMT

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

Issued By: Network Device

Nota: questa opzione viene utilizzata Device ld e Password in un passaggio successivo Security > TrustSec > Generalnell'interfaccia utente Web WLC.

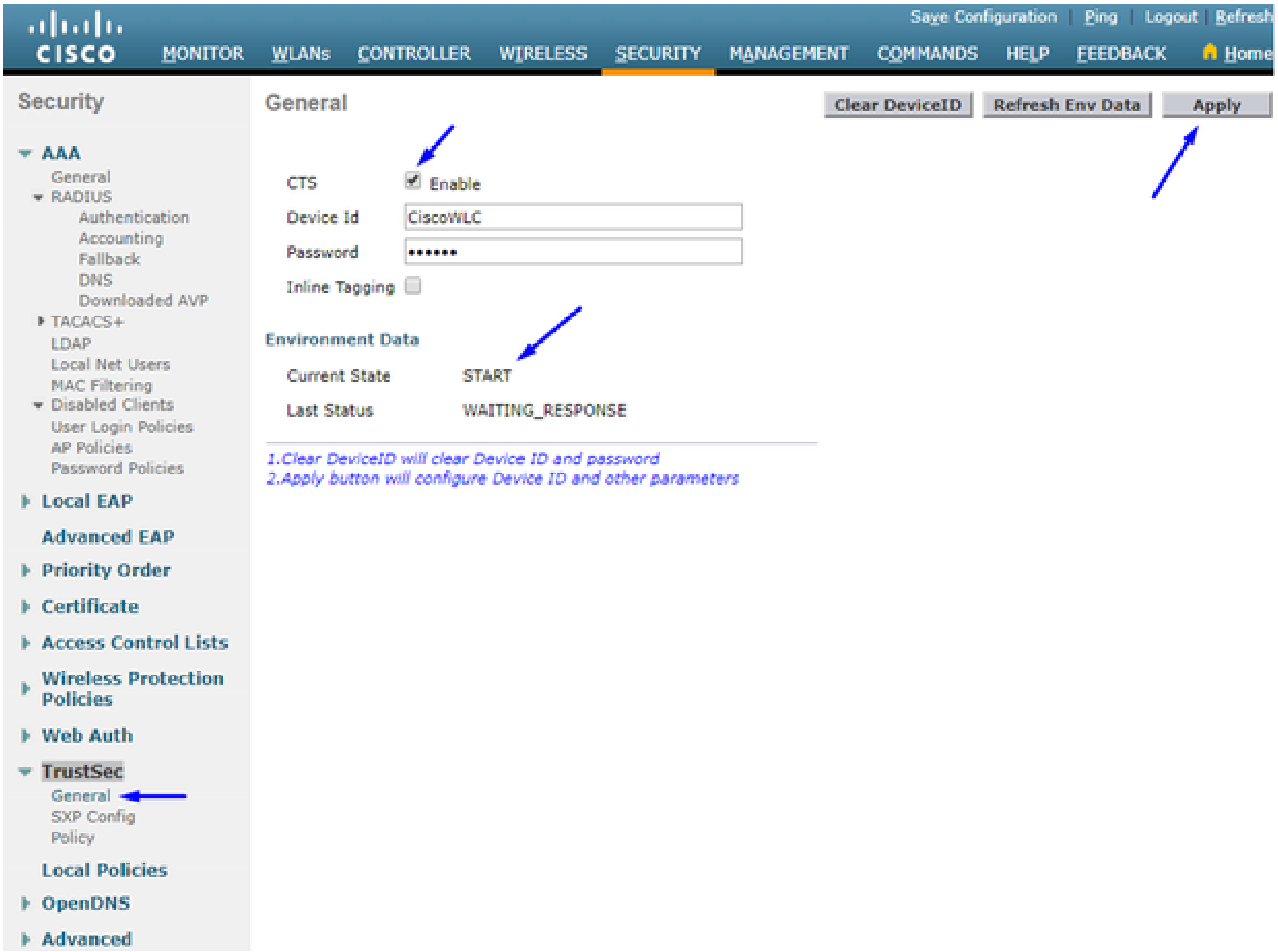
Abilita provisioning PAC di WLC



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

Abilita TrustSec su WLC



General

CTS ☑ Enable

Device Id CiscoWLC

Password ••••••

Inline Tagging ☐

Environment Data

Current State START

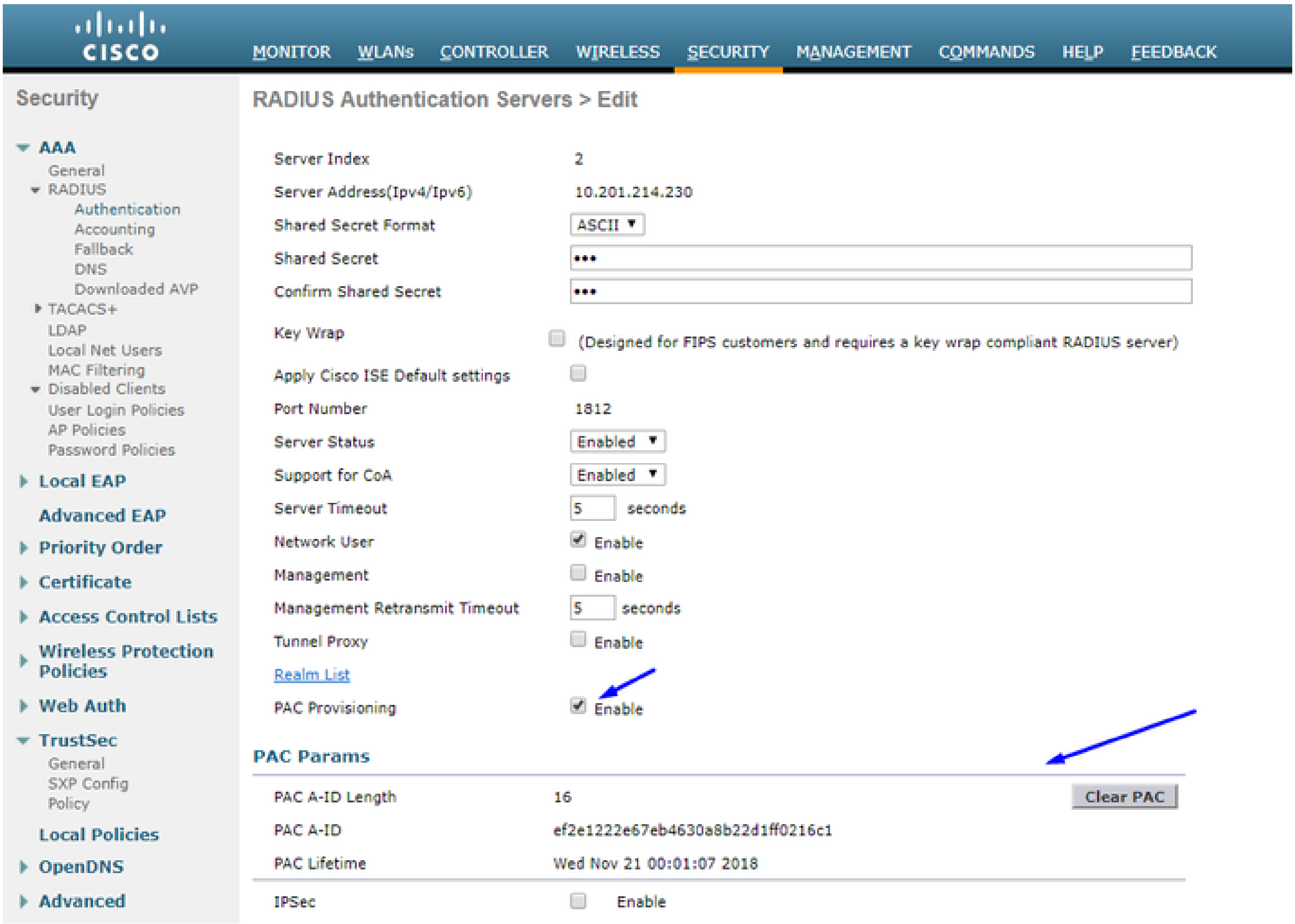
Last Status WAITING_RESPONSE

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

Nota: il valore CTS Device Id e Password deve essere uguale a Device Id e Password a quello specificato nella Administration > Network Devices > Add Device > Advanced TrustSec Settings sezione in Cisco ISE.

Verificare che sia stato eseguito il provisioning della PAC sul WLC

Dopo aver fatto clic su Refresh Env Data, sul WLC la PAC è stata fornita correttamente (eseguire questa operazione in questo passaggio):



RADIUS Authentication Servers > Edit

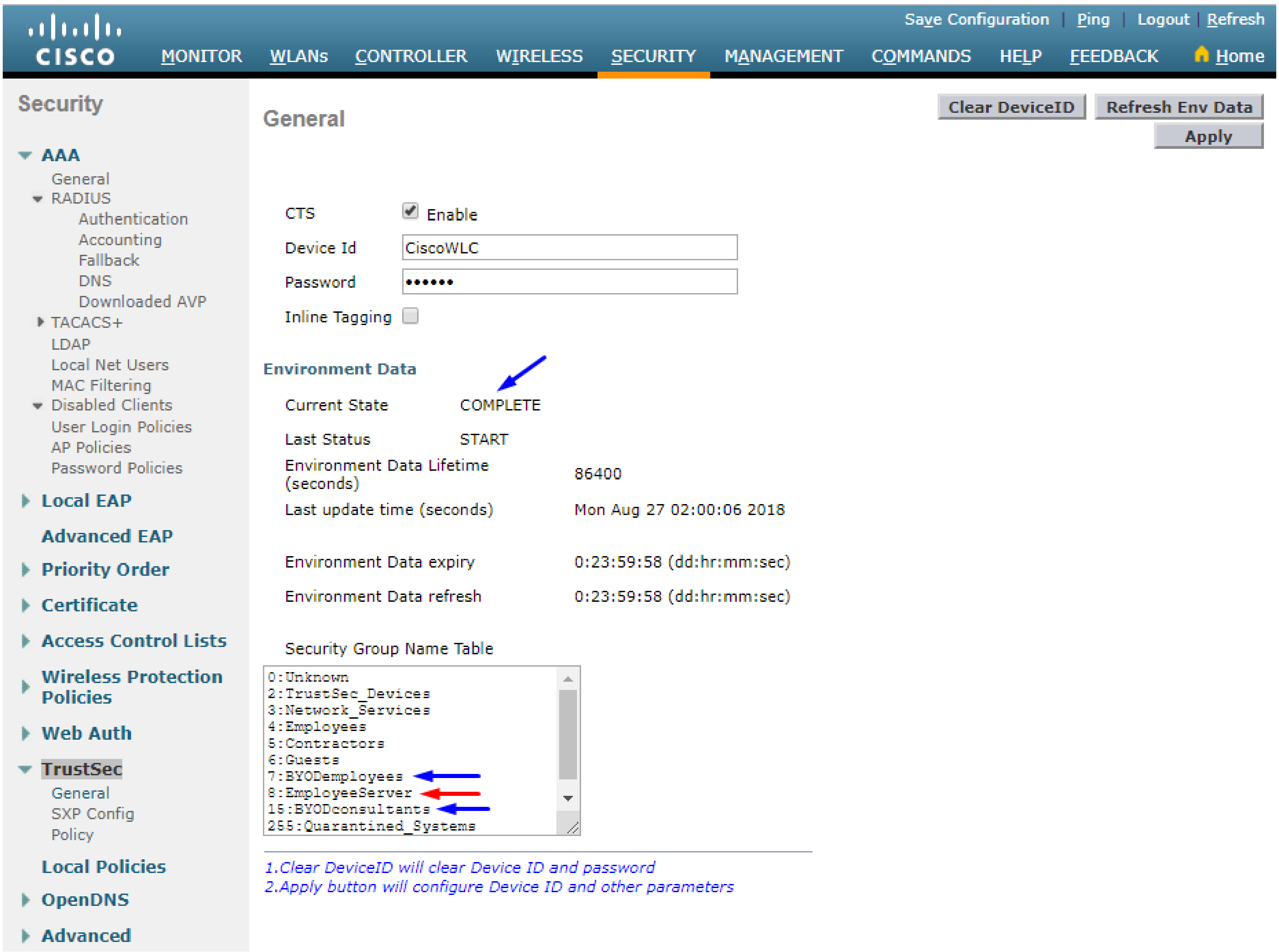
Server Index	2
Server Address(Ipv4/Ipv6)	10.201.214.230
Shared Secret Format	ASCII ▼
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Apply Cisco ISE Default settings	□
Port Number	1812
Server Status	Enabled ▼
Support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

Scarica i dati dell'ambiente CTS da Cisco ISE a WLC

Dopo aver fatto clic suRefresh Env Data, il WLC scarica le SGT.



General

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

Environment Data

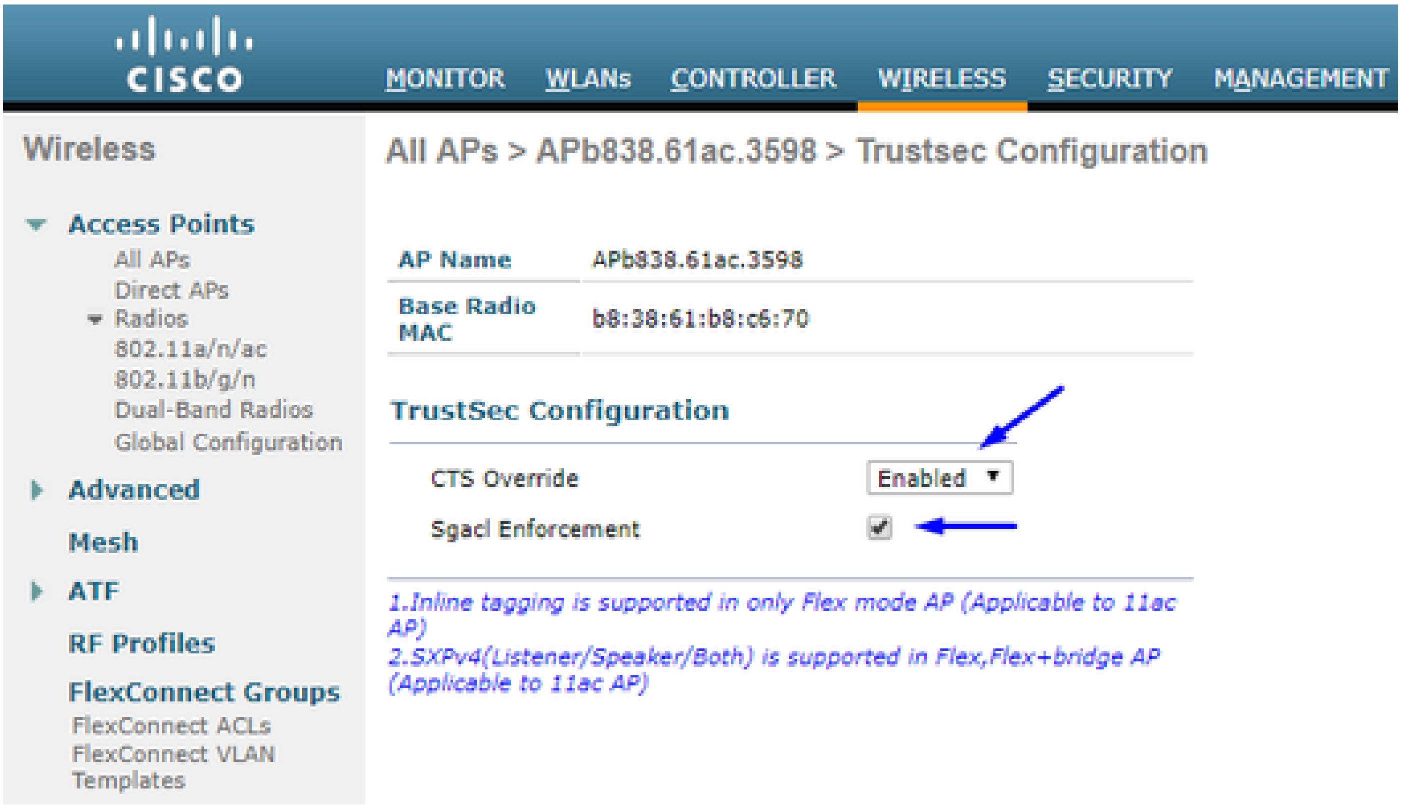
Current State	COMPLETE
Last Status	START
Environment Data Lifetime (seconds)	86400
Last update time (seconds)	Mon Aug 27 02:00:06 2018
Environment Data expiry	0:23:59:58 (dd:hr:mm:sec)
Environment Data refresh	0:23:59:58 (dd:hr:mm:sec)

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

Abilita download SGACL e applicazione sul traffico



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

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

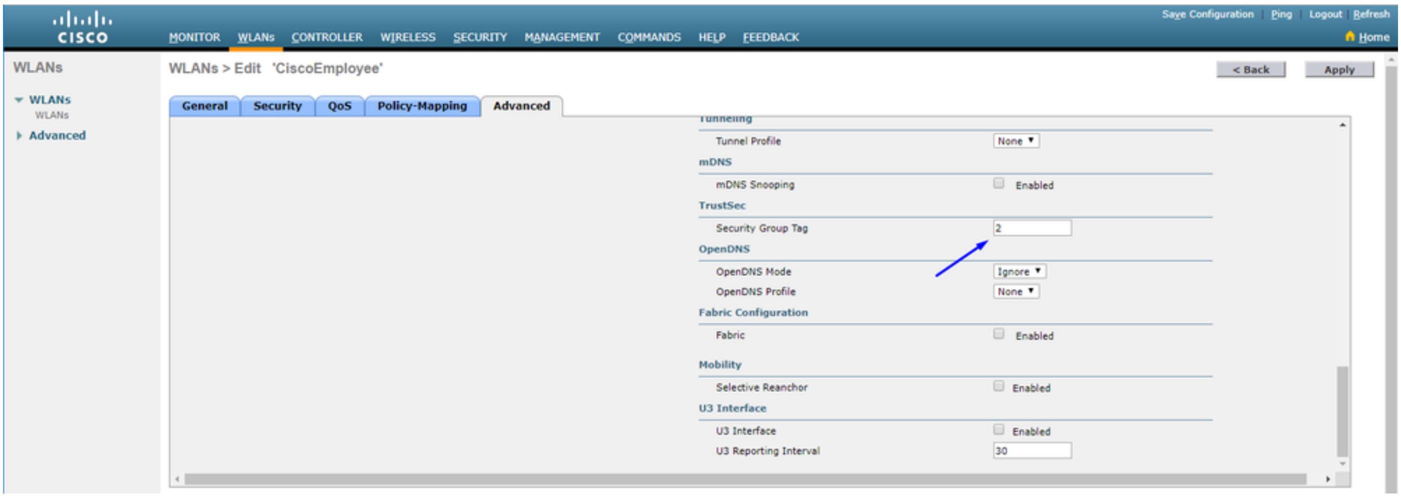
TrustSec Configuration

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)

Assegna WLC e Access Point al SGT di 2 (TrustSec_Devices)

Fornire alla WLC+WLAN un SGT di 2 (TrustSec_Devices) per consentire il traffico (SSH, HTTPS e CAPWAP) da/verso il WLC + AP tramite lo 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

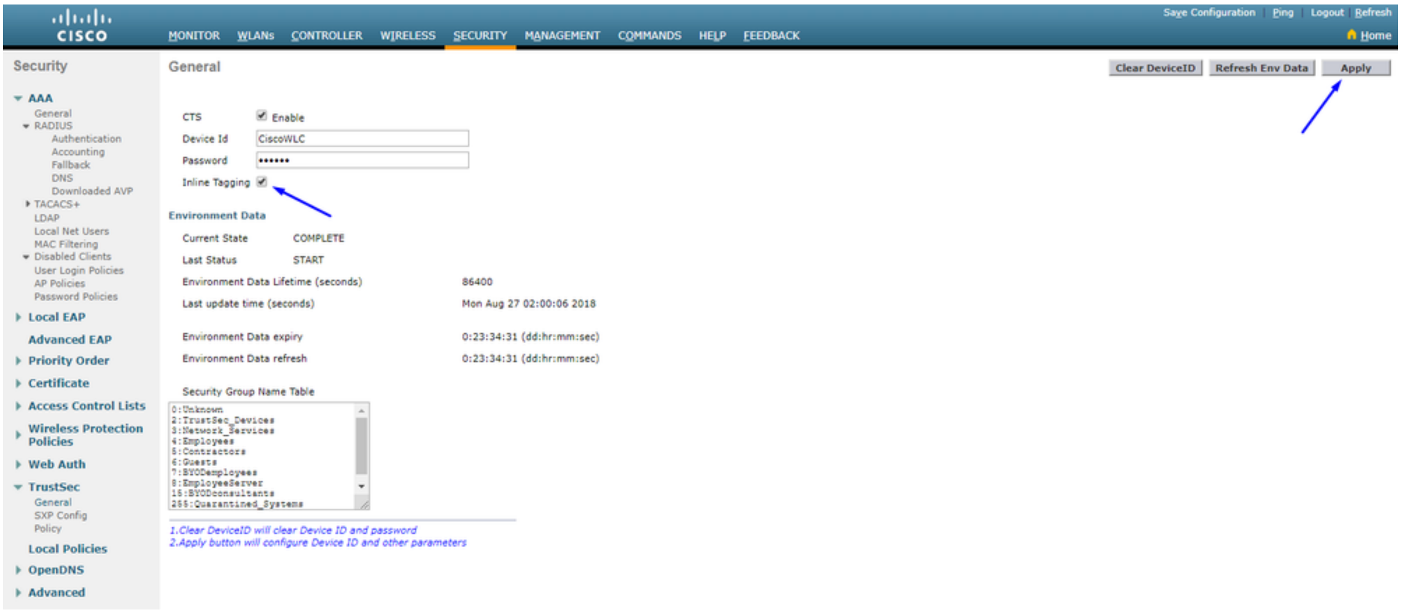
Selective Reanchor: □ Enabled

U3 Interface

U3 Interface: □ Enabled

U3 Reporting Interval: 30

Abilita tag in linea sul 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)

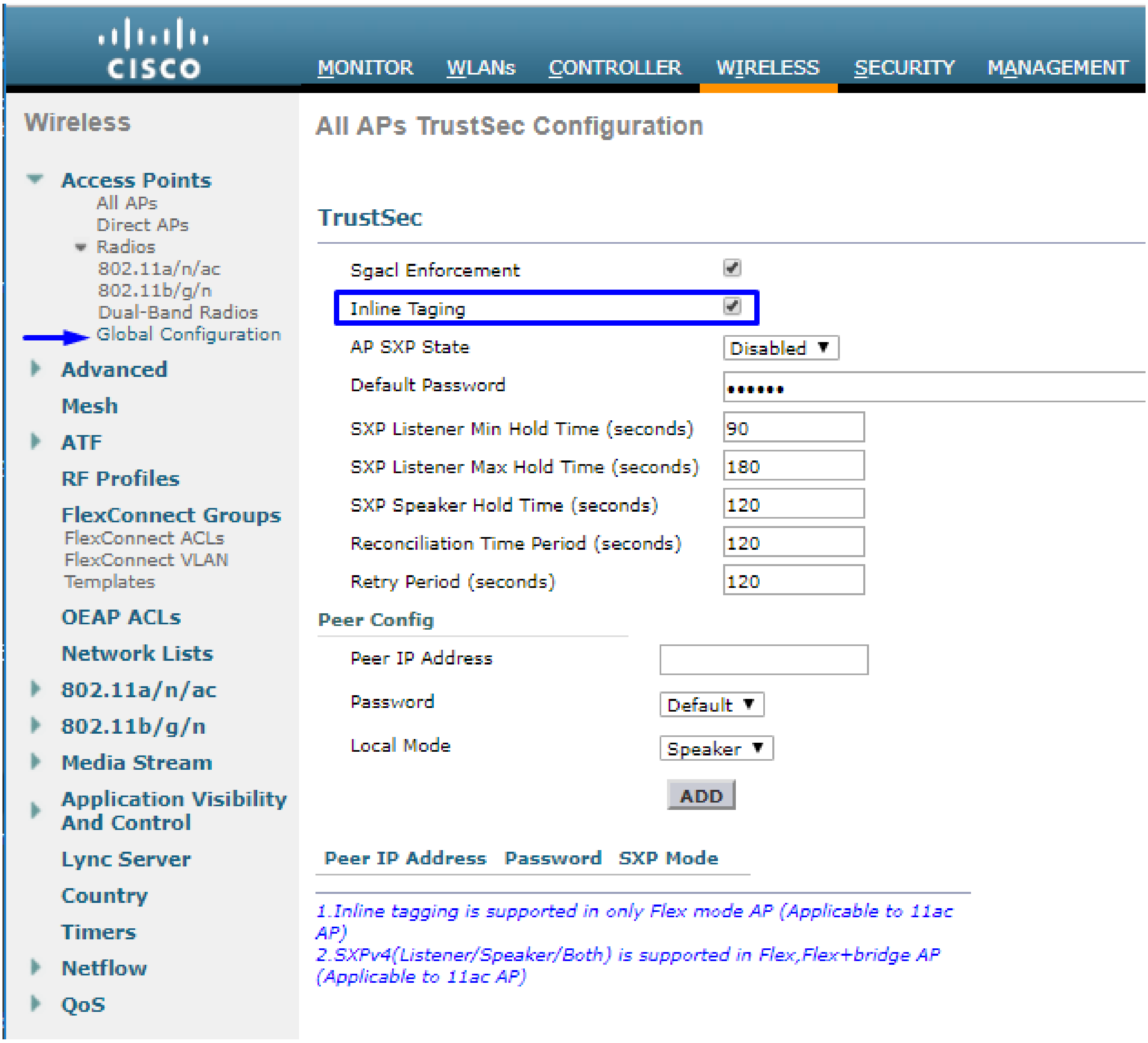
Environment Data refresh: 0:23:34:31 (dd:hr:mm:sec)

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

In **Wireless > Access Points > Global Configuration** scorrere verso il basso e selezionare **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)

Abilitazione del tagging inline sullo switch Catalyst

<#root>

CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

CatalystSwitch(config-if)#description goestoWLC

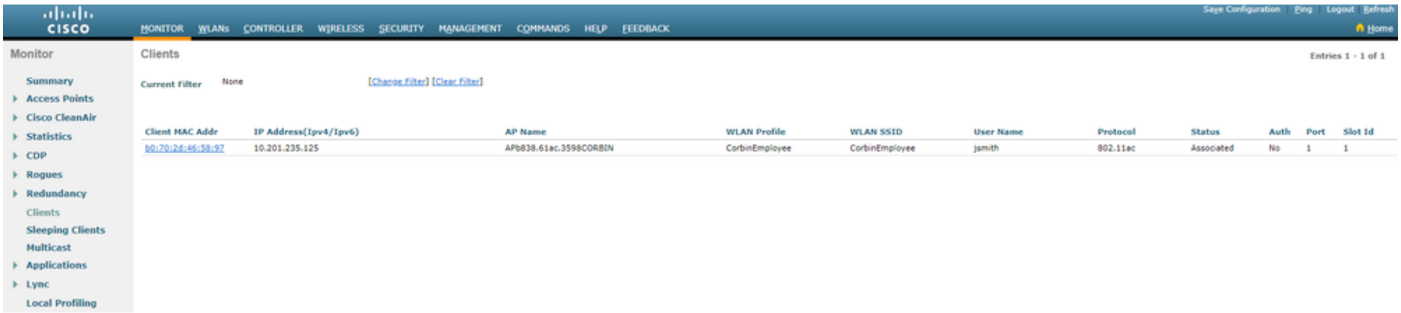
CatalystSwitch(config-if)#switchport trunk native vlan 15

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
```

Verifica



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

Hardware dei contatori ACL della piattaforma Catalyst#show switch | inc SGACL

Perdita SGACL IPv4 in uscita (454): 10 frame

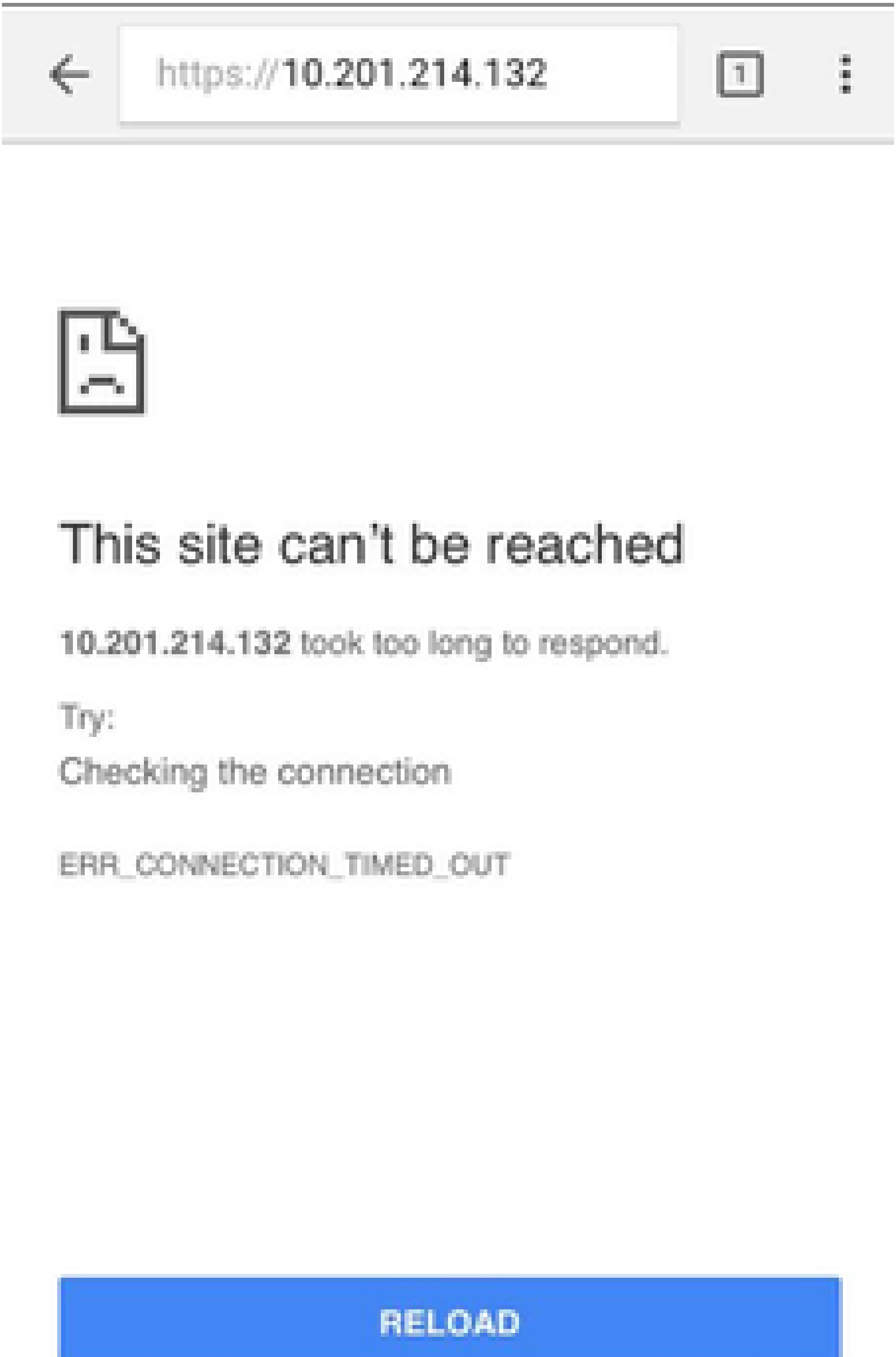
Perdita SGACL IPv6 in uscita (455): 0 frame

Caduta cella SGACL IPv4 in uscita (456): 0 frame

Caduta cella SGACL IPv6 in uscita (457): 0 frame

Suggerimento: se si usa invece un Cisco ASR, Nexus o Cisco ASA, il documento elencato qui può aiutare a verificare che i tag SGT siano applicati: TrustSec Troubleshooting Guide (Guida alla risoluzione dei problemi di TrustSec).

Autenticare la connessione wireless con il nome utente jsmith e la password Admin123. Sullo switch è presente l'ACL di negazione:



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

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l&rsquo;accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).