

Configurar e verificar o SGACL no Catalyst 9800 WLC e no ISE Server

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração de WLC](#)

[Configuração do ISE](#)

[Flexconnect](#)

[Verificar](#)

[Switching local FlexConnect](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar o TrustSec no Catalyst 9800 e no servidor ISE para utilizar o recurso SGACL, com APs locais e no modo FlexConnect.

Pré-requisitos

Requisitos

Conhecimento dos fundamentos do Cisco 9800 WLC, Cisco ISE, FlexConnect e TrustSec.

Componentes Utilizados

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

- C9800-CL v17.12.4
- ISE 3.2.0
- Access Point 9136I

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

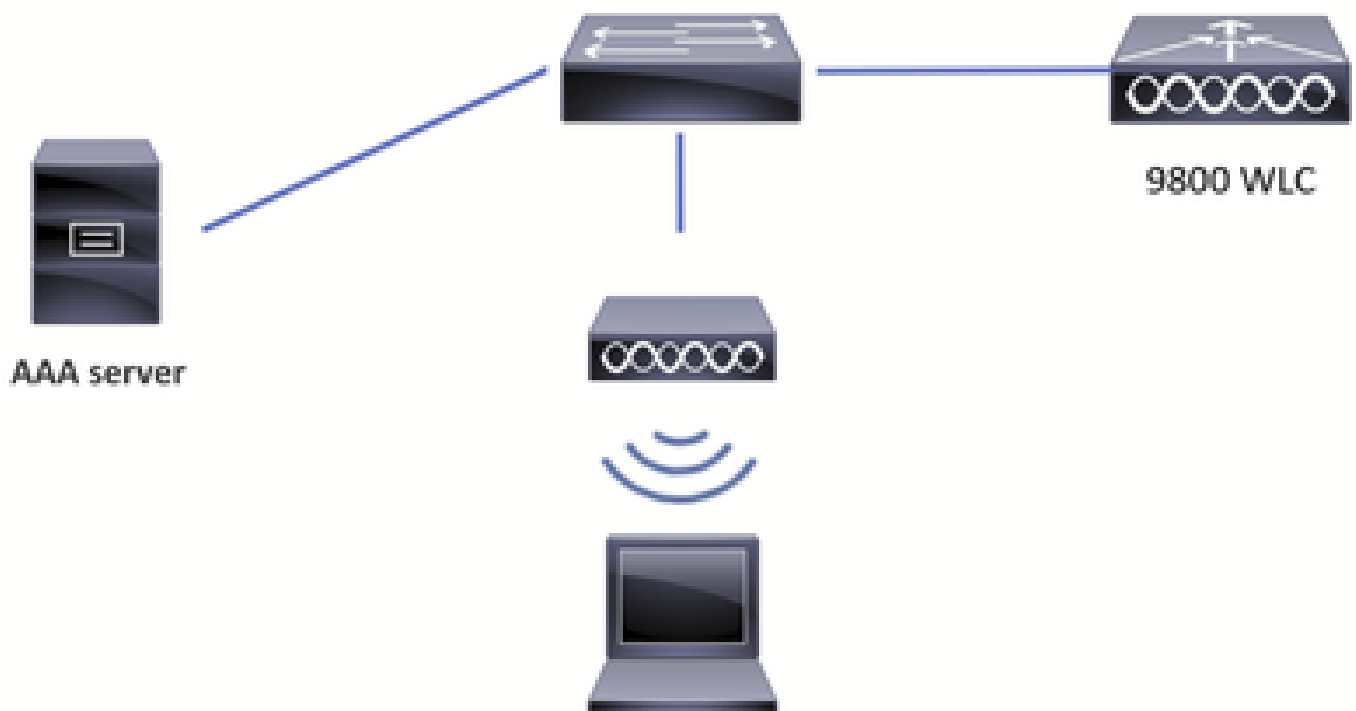
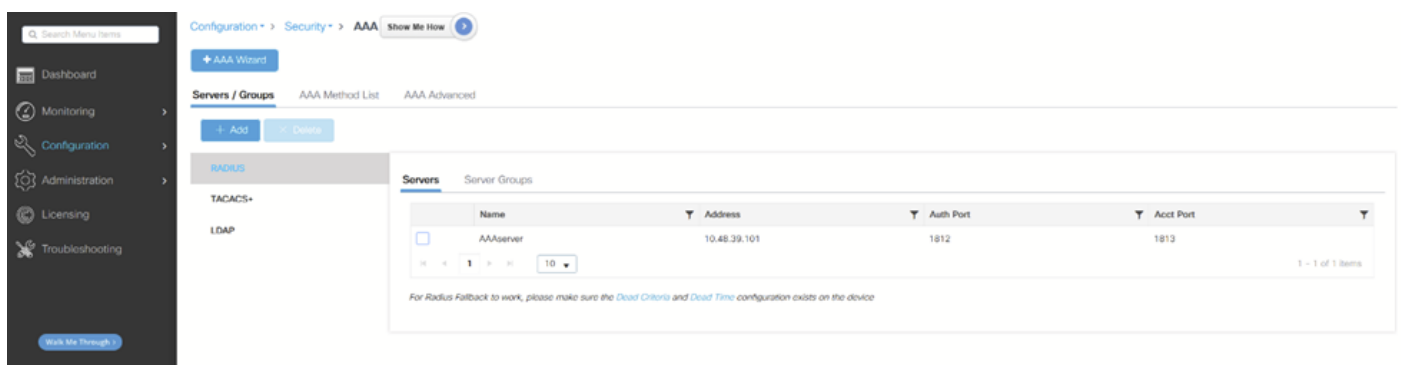


Diagrama de Rede

Configurações

Configuração de WLC

1. Adicione o servidor AAA ao WLC em Configuration > Security > AAA:



página AAA da WLC

2. Certifique-se de que as entradas de chave aqui correspondam à chave quando você adicionar

o dispositivo no ISE. Habilite Suporte para CoA e adicione a chave se quiser usar CoA para fazer download das atualizações de configuração:

The screenshot shows the Cisco ISE configuration interface. On the left is a dark sidebar with navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Configuration > Security > AAA' with a 'Show Me How' link. Below this are tabs for 'Servers / Groups', 'AAA Method List', and 'AAA Advanced'. The 'Servers / Groups' tab is active, showing a list of servers with 'AAAserver' selected. A modal window titled 'Edit AAA Radius Server' is open, displaying configuration fields for the selected server. The fields include: Name (AAAserver), Server Address (10.48.39.101), Set New Key (checked), PAC Key (checked), PAC Key Type (Clear Text), PAC Key (masked), Confirm PAC Key (masked), Auth Port (1812), Acct Port (1813), Server Timeout (seconds) (1-1000), and Retry Count (0-100). On the right side of the modal, there are checkboxes for 'Support for CoA' (ENABLED), 'CoA Server Key Type' (Hidden), 'CoA Server Key' (masked), and 'Automate Tester' (unchecked). At the bottom of the modal are 'Cancel' and 'Update & Apply to Device' buttons.

Servidor AAA de adição de WLC

3. Crie o Grupo de Servidores:

The screenshot shows the Cisco ISE configuration interface with the 'Server Groups' tab active. A table lists the server groups. The table has columns for Name, Server 1, Server 2, and Server 3. The first row shows a group named 'ISE-group' with 'AAAserver' in the Server 1 column and 'N/A' in the Server 2 and Server 3 columns. The table is paginated, showing 1 of 1 items.

Name	Server 1	Server 2	Server 3
ISE-group	AAAserver	N/A	N/A

WLC adicionar grupo de servidores

4. Adicione a Lista de Métodos de Autorização com o tipo network:

Quick Setup: AAA Authorization

Method List Name*

ISE-Authz-List

Type*

network

Group Type

group

Fallback to local

Authenticated

Available Server Groups

radius

ldap

tacacs+

>

<

>>

<<

Assigned Server Groups

ISE-group

^

^

v

v

Cancel

Apply to Device

Lista de métodos de autorização

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Walk Me Through

Configuration > Security > AAA

Show Me How

AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

- Delete

Name	Type	Group Type	Group1	Group2	Group3	Group4
☐ default	exec	local	N/A	N/A	N/A	N/A
☐ ISE-Authz-List	network	group	ISE-group	N/A	N/A	N/A

1

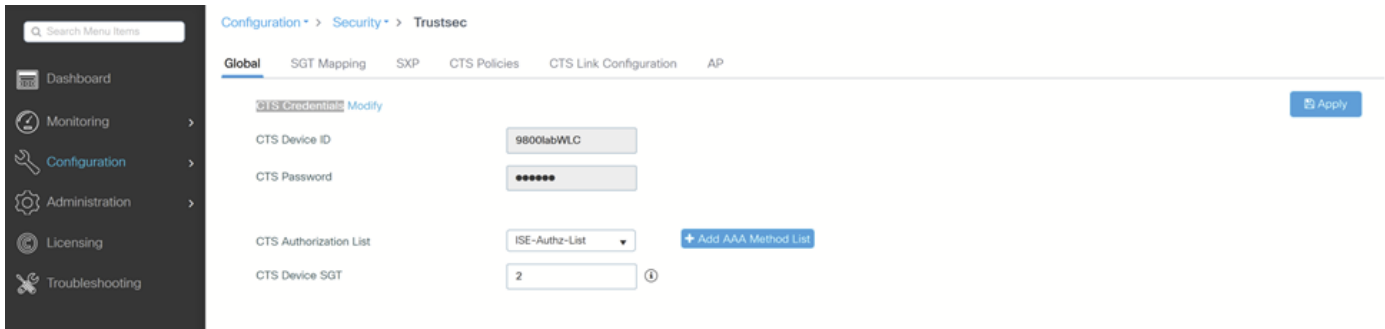
10

1 - 2 of 2 items

Grupo de servidores AAA da WLC

5. Navegue para Configuration > Security > Trustsec e configure a CTS Device ID e a CTS Password, você usará essas entradas ao adicionar o dispositivo no ISE.

Configure a lista de autorização CTS que você criou nas etapas 4 aqui também:

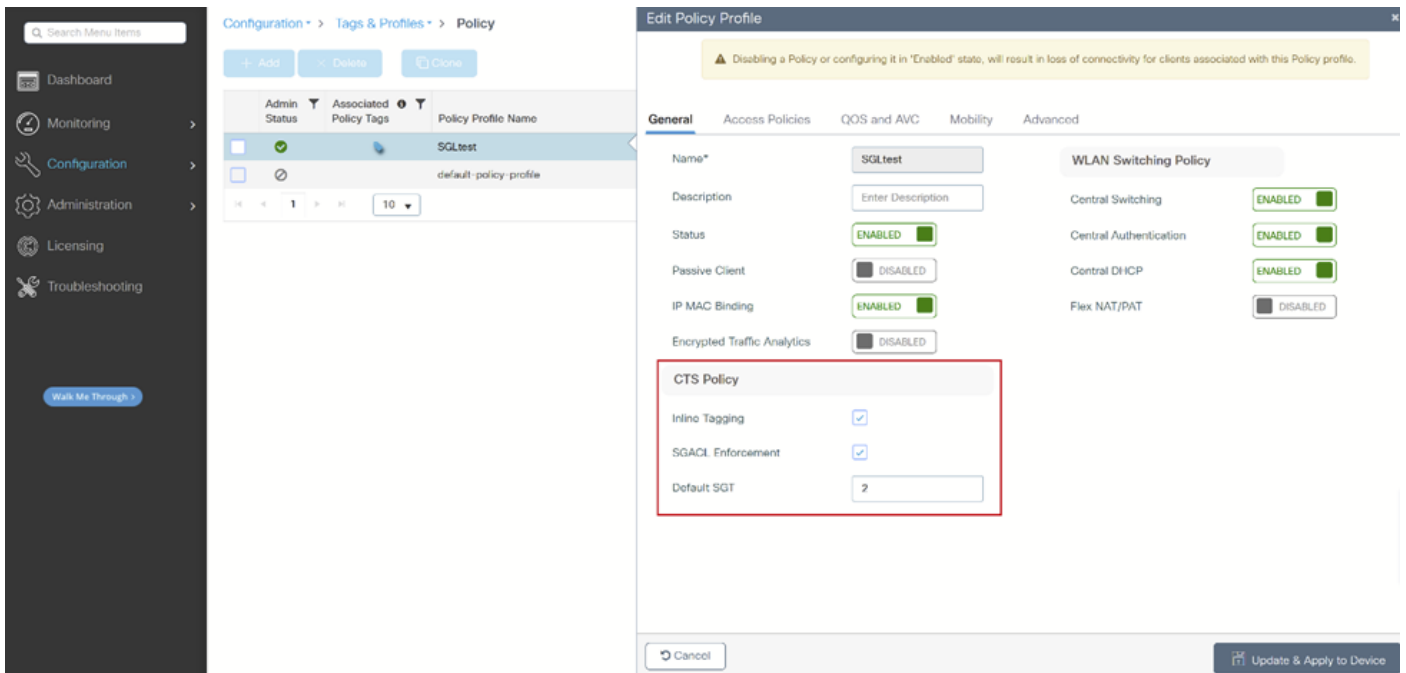


TrustSec da WLC

6. Neste exemplo, a WLAN já foi criada e as configurações de autenticação já estão definidas.

Agora, navegue até o Perfil de política no qual você gostaria de usar SGTs.

i. Em CTS Policy, habilite Inline Tagging e SGACL Enforcement, você pode especificar o Default SGT também. O SGT 2 padrão é usado para este laboratório como exemplo:



Perfil de política da WLC

ii) Na guia Advanced, habilite Allow AAA override e NAC state:

Edit Policy Profile

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)
28800

Idle Timeout (sec)
300

Idle Threshold (bytes)
0

Client Exclusion Timeout (sec)
☒
60

Guest LAN Session Timeout
☐

DHCP

IPv4 DHCP Required
☐

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override
☒

NAC State
☒

Policy Name
default-aaa-policy

Accounting List
Search or Select

Fabric Profile
☐
Search or Select

Link-Local Bridging
☐

mDNS Service Policy
default-mdns-ser ...
Clear

Hotspot Server
Search or Select

User Defined (Private) Network

Status
☐

Drop Unicast
☐

DNS Layer Security

DNS Layer Security Parameter Map
Not Configured
Clear

Flex DHCP Option for DNS
ENABLED

Flex DNS Traffic Redirect
IGNORE

WLAN Flex Policy

VLAN Central Switching
☐

Split MAC ACL
Search or Select

Cancel
Update & Apply to Device

Guia Avançado do Perfil de Política da WLC

Na CLI:

configure terminal

```
(config)# radius server <server_name>
(config-radius-server)# address ipv4 <server_IP>
(config-radius-server)# pac key <password>
```

```
(config)# aaa server radius dynamic-author
(config-locsvr-da-radius)# client <server_IP> server-key <password>
```

```
(config)# aaa group server radius <server_group_name>
(config-sg-radius)# server name <server_name>
(config-sg-radius)# ip radius source-interface Vlan#
```

```
(config)# aaa authorization network <author_method_list> group <server_group_name>
```

```
(config)# cts authorization list <author_method_list>
```

```
(config)# wireless profile policy <policy_profile_name>
(config-wireless-policy)# shut
(config-wireless-policy)# aaa-override
(config-wireless-policy)# cts inline-tagging
(config-wireless-policy)# cts role-based enforcement
(config-wireless-policy)# cts sgt <number>
(config-wireless-policy)# no shut
```

show cts credentials

CTS password is defined in keystore, device-id = 9800labWLC

Configuração do ISE

1. Navegue até Administration > Network Resources > Network Devices.

i. Adicione as informações da WLC aqui:

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - Network Resources'. The left sidebar has 'Network Devices' selected. The main content area is titled 'Network Devices List > 9800labWLC'. Below this, the 'Network Devices' configuration form is visible. The 'Name' field is set to '9800labWLC'. The 'Description' field is empty. The 'IP Address' field is set to '10.48.38.67 / 32'.

Página Dispositivos de rede do ISE

This screenshot shows the same Cisco ISE Administration console, but with the 'RADIUS Authentication Settings' section expanded. The 'Device Profile' is set to 'Cisco'. The 'Model Name' and 'Software Version' fields are empty. The 'Network Device Group' is set to 'All Locations'. The 'Location' is set to 'All Locations'. The 'IPSEC' is set to 'No'. The 'Device Type' is set to 'All Device Types'. The 'RADIUS Authentication Settings' section is expanded, showing 'RADIUS UDP Settings'. The 'Protocol' is set to 'RADIUS'. The 'Shared Secret' is masked with '*****'. The 'Use Second Shared Secret' checkbox is unchecked. The 'Second Shared Secret' field is also masked with '*****'.

ISE adiciona informações de RADIUS de WLC

ii) Role para baixo e configure Advanced TrustSec Settings, ative a caixa de seleção Use Device ID for TrustSec Identification e configure a senha:

The screenshot shows the Cisco ISE Administration interface under 'Network Resources'. The 'Network Devices' tab is selected. In the left sidebar, 'Network Devices' is expanded, showing 'Default Device' and 'Device Security Settings'. The main content area shows 'Advanced TrustSec Settings' with a checked checkbox. Below it, 'Device Authentication Settings' is expanded, showing 'Use Device ID for TrustSec Identification' with a checked checkbox. The 'Device Id' field contains '9800labWLC' and the 'Password' field is masked with dots, with a 'Show' link next to it.

Configurações avançadas do TrustSec

Isso deve corresponder à configuração no lado da WLC na etapa 6 da configuração da WLC.

iii) Role para baixo até Notificações e atualizações TrustSec e configure se você deseja usar CoA ou SSH para atualizações de configuração. Selecione o nó do ISE necessário:

The screenshot shows the Cisco ISE Administration interface under 'Network Resources'. The 'Network Devices' tab is selected. In the left sidebar, 'Network Devices' is expanded, showing 'Default Device' and 'Device Security Settings'. The main content area shows 'TrustSec Notifications and Updates' with several settings: 'Download environment data every' set to 10 seconds, 'Download peer authorization policy every' set to 10 seconds, 'Reauthentication every' set to 1 day, and 'Download SGACL lists every' set to 10 seconds. There are two checked checkboxes: 'Other TrustSec devices to trust this device' and 'Send configuration changes to device'. Under the second checkbox, 'CoA' is selected with a radio button, and 'CLI (SSH)' is unselected. The 'Send from' dropdown is set to 'varusrin-ise', and there is a 'Test connection' link. The 'Ssh Key' field is empty.

Notificações e atualizações do TrustSec

2. Pressione Conexão de teste para certificar-se de que a conexão esteja estabelecida. Quando for bem-sucedido, exibirá um sinal verde:

☒ Send configuration changes to device

☒ CoA

☐ CLI (SSH)

Send from varusrin-ise ▼ Test connection 

Ssh Key _____

Testar conexão

i. Role para baixo e configure a WLC a ser incluída ao implantar atualizações de mapeamento SGT. Isso é importante se você selecionar a opção SSH na etapa anterior:

Device Configuration Deployment

☒ Include this device when deploying Security Group Tag Mapping Updates

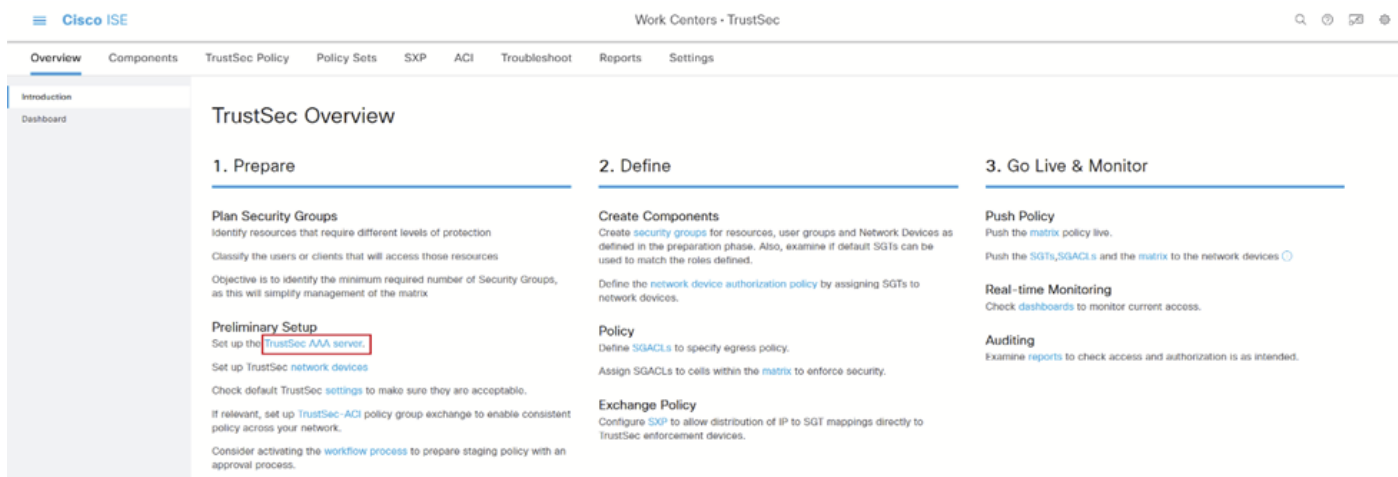
Device Interface Credentials

EXEC Mode Username	admin
EXEC Mode Password	•••••••••• Show
Enable Mode Password	•••••••••• Show

Implantação de configuração de dispositivo

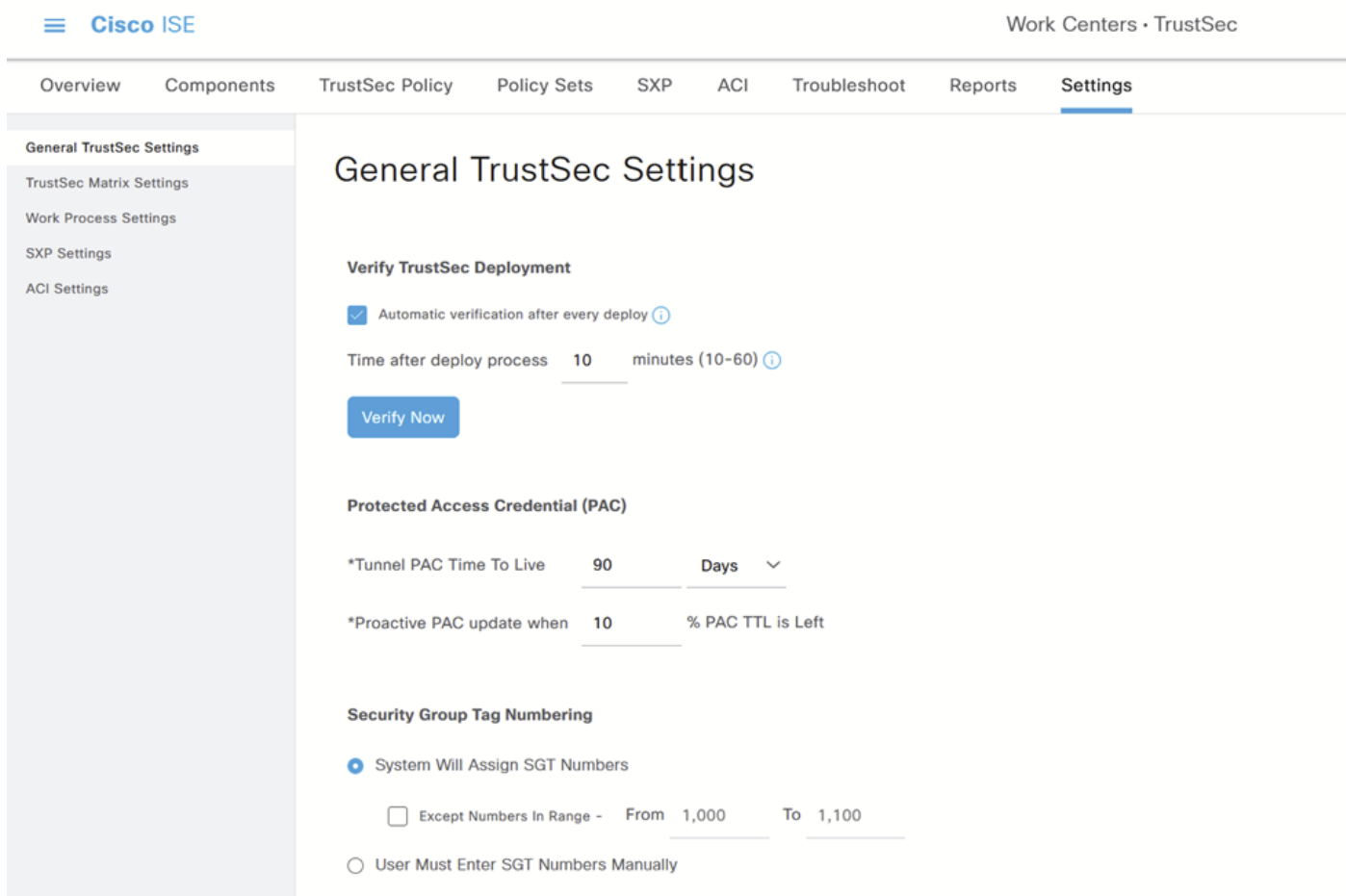
ii) Salve a configuração.

3. Em Centros de Trabalho > TrustSec > Visão Geral, você tem as opções de configuração TrustSec. Escolha TrustSec AAA Server para exibir a instância do ISE em uso. Consulte [Cisco Catalyst Wireless Group Based Policy](#) para obter mais informações sobre qual instância é usada se você tiver múltiplos.



Visão geral do ISE TrustSec

4. (Opcional) Navegue até a guia Configurações, habilite Verificação automática após cada implantação, se preferível.



Configurações do ISE TrustSec

5. Adicione ou edite os valores de SGT em Centros de trabalho > TrustSec > Componentes > Grupos de segurança, dependendo de seus requisitos:

Cisco ISE

Work Centers - TrustSec

OverviewComponentsTrustSec PolicyPolicy SetsSXPACITroubleshootReportsSettings

Security Groups

IP SGT Static Mapping

Security Group ACLs

Network Devices

TrustSec Servers

Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Selected 0 Total 16

✎ Edit✚ Add📁 Import📄 Export🗑 Trash🔄 Push🔍 Verify Deploy

All▼

☐	Icon	Name	SGT (Dec / Hex)	Description	Learned from
☐	🔵	Auditors	9/0009	Auditor Security Group	
☐	🔵	BYOD	15/000F	BYOD Security Group	
☐	🔵	Contractors	5/0005	Contractor Security Group	
☐	🔵	Developers	8/0008	Developer Security Group	
☐	🔵	Development_Servers	12/000C	Development Servers Security Group	
☐	🔵	Employees	4/0004	Employee Security Group	
☐	🔵	Guests	6/0006	Guest Security Group	
☐	🔵	Network_Services	3/0003	Network Services Security Group	
☐	🔵	PCI_Servers	14/000E	PCI Servers Security Group	
☐	🔵	Point_of_Sale_Systems	10/000A	Point of Sale Security Group	
☐	🔵	Production_Servers	11/000B	Production Servers Security Group	
☐	🔵	Production_Users	7/0007	Production User Security Group	
☐	🔵	Quarantined_Systems	255/00FF	Quarantine Security Group	

Grupos de segurança do ISE

6. Se quiser especificar a política de autorização, navegue para Centros de Trabalho > TrustSec > Política TrustSec > Autorização de Dispositivo de Rede:

Cisco ISE

Work Centers - TrustSec

OverviewComponentsTrustSec PolicyPolicy SetsSXPACITroubleshootReportsSettings

Egress Policy

Network Device Authorization

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	
☒ Default Rule	if no rules defined or no match	then TrustSec_Devices	Edit

Insert new row above

Save

Política TrustSec

Você pode manter o padrão, mas para este laboratório estamos usando esta configuração como um exemplo:

The screenshot shows the Cisco ISE Work Centers - TrustSec interface. The left sidebar has a menu with 'Egress Policy' and 'Network Device Authorization'. The main area is titled 'Network Device Authorization' and contains a table with two rules. The first rule is 'Netdevice' with the condition 'DEVICE Device Type equals to Device TypeAll Device Types' and the security group 'TrustSec_Devices'. The second rule is 'Default Rule' with the condition 'no rules defined or no match' and the security group 'Unknown'. Both rules have an 'Edit' link.

Rule Name	Conditions	Security Group
Netdevice	if DEVICE Device Type equals to Device TypeAll Device Types then	TrustSec_Devices
Default Rule	if no rules defined or no match then	Unknown

Autorização de dispositivo de rede

7. Crie o SGACL na guia Components e depois nas ACLs Security Group:

The screenshot shows the Cisco ISE Work Centers - TrustSec interface. The left sidebar has a menu with 'Security Groups', 'IP SGT Static Mapping', 'Security Group ACLs', 'Network Devices', and 'TrustSec Servers'. The main area is titled 'Security Groups ACLs' and contains a table with two ACLs. The first ACL is 'CustomDefaultSGTACL' with the IP version 'IPv4'. The second ACL is 'SGACLtest' with the IP version 'IPv4'. Both ACLs have a checkbox in the first column.

Name	Description	IP Version
CustomDefaultSGTACL		IPv4
SGACLtest		IPv4

ACLs do grupo de segurança

8. Especifique as entradas da matriz na guia TrustSec Policy e, em seguida, na Matrix. Você pode editar as Permissões clicando no ponto que dois SGTs atendem:

Matriz ISE TrustSec

Por exemplo:



Edit Permissions...

Source Security Group Contractors (5/0005)

Destination Security Group Contractors (5/0005)

Status ☒ Enabled 

Description

Assigned Security Group ACLs

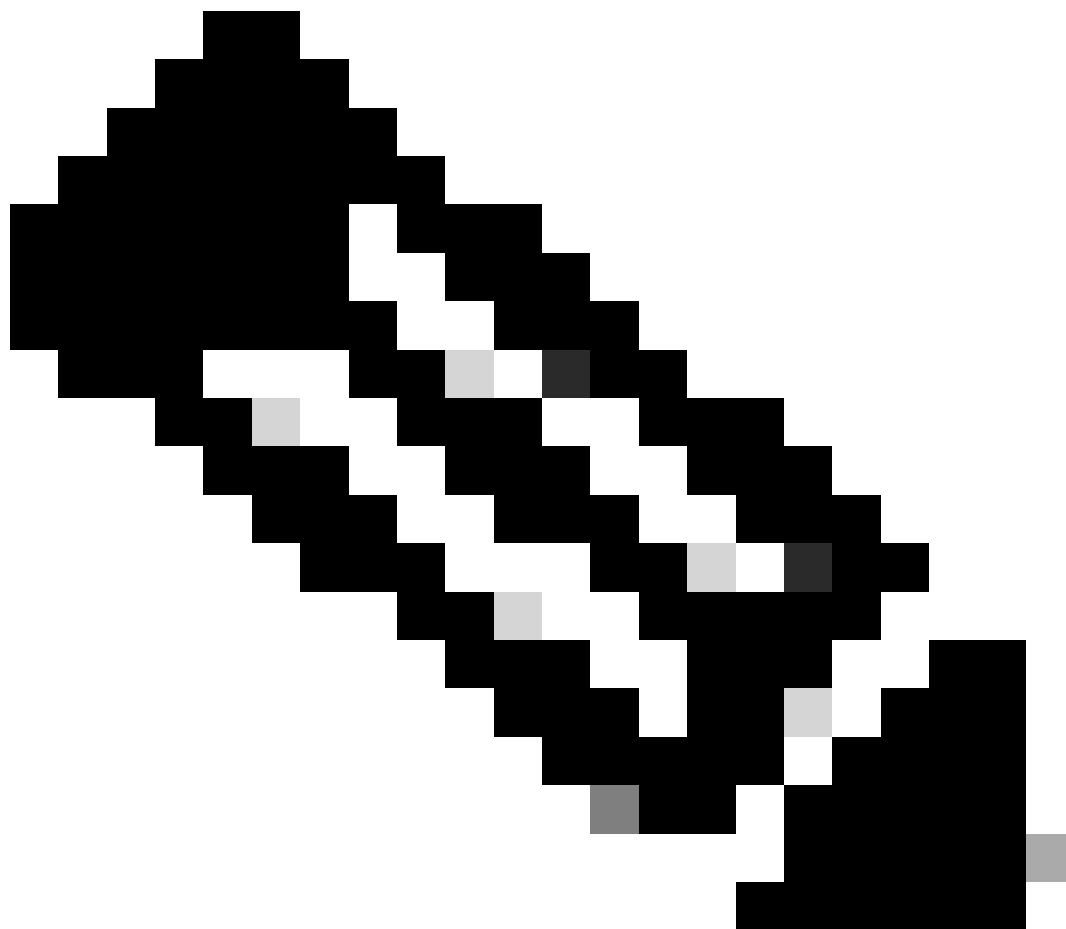


ustomDefaultSGTACL 

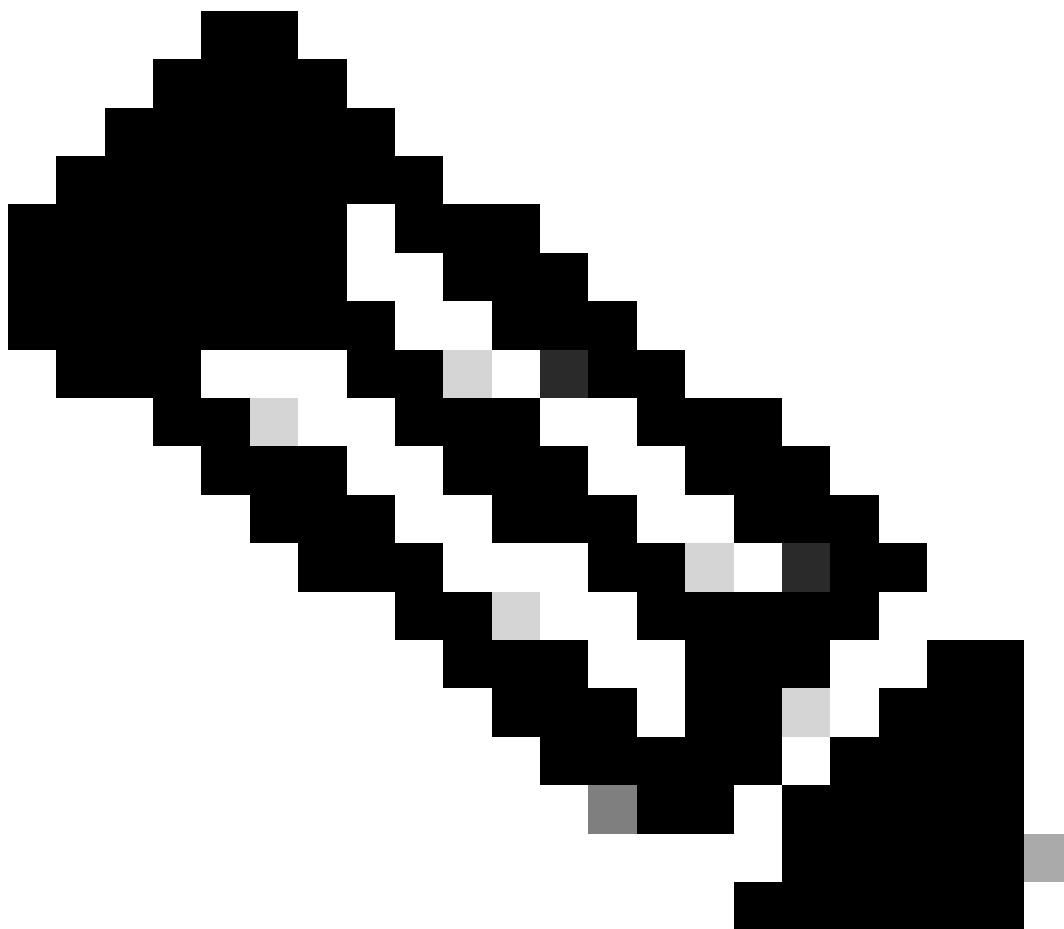
Final Catch All Rule Permit IP 

Cancel

Save



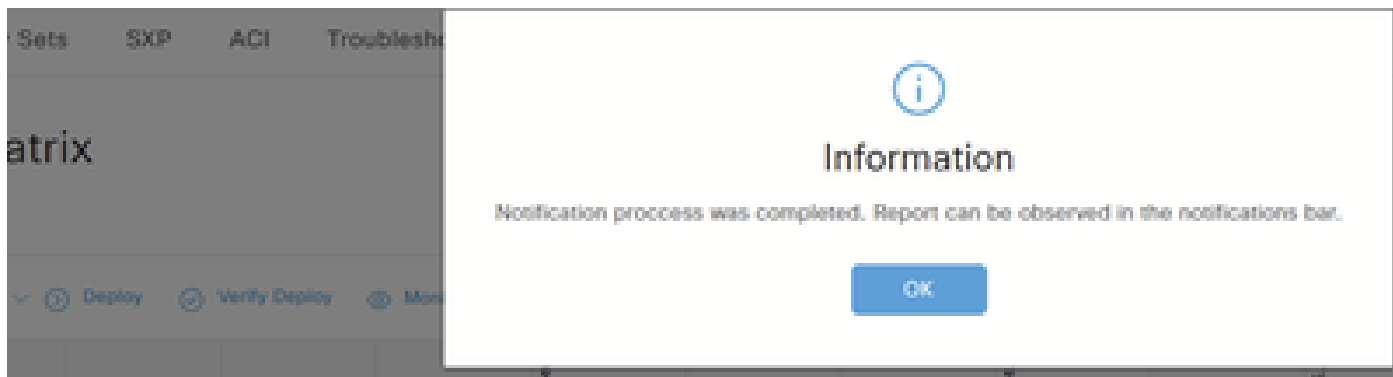
Note: No caso do modelo de lista de permissões, você precisa permitir explicitamente o protocolo DHCP para que os dispositivos cliente obtenham o endereço IP DHCP e depois solicitar o controlador para políticas SGACL.



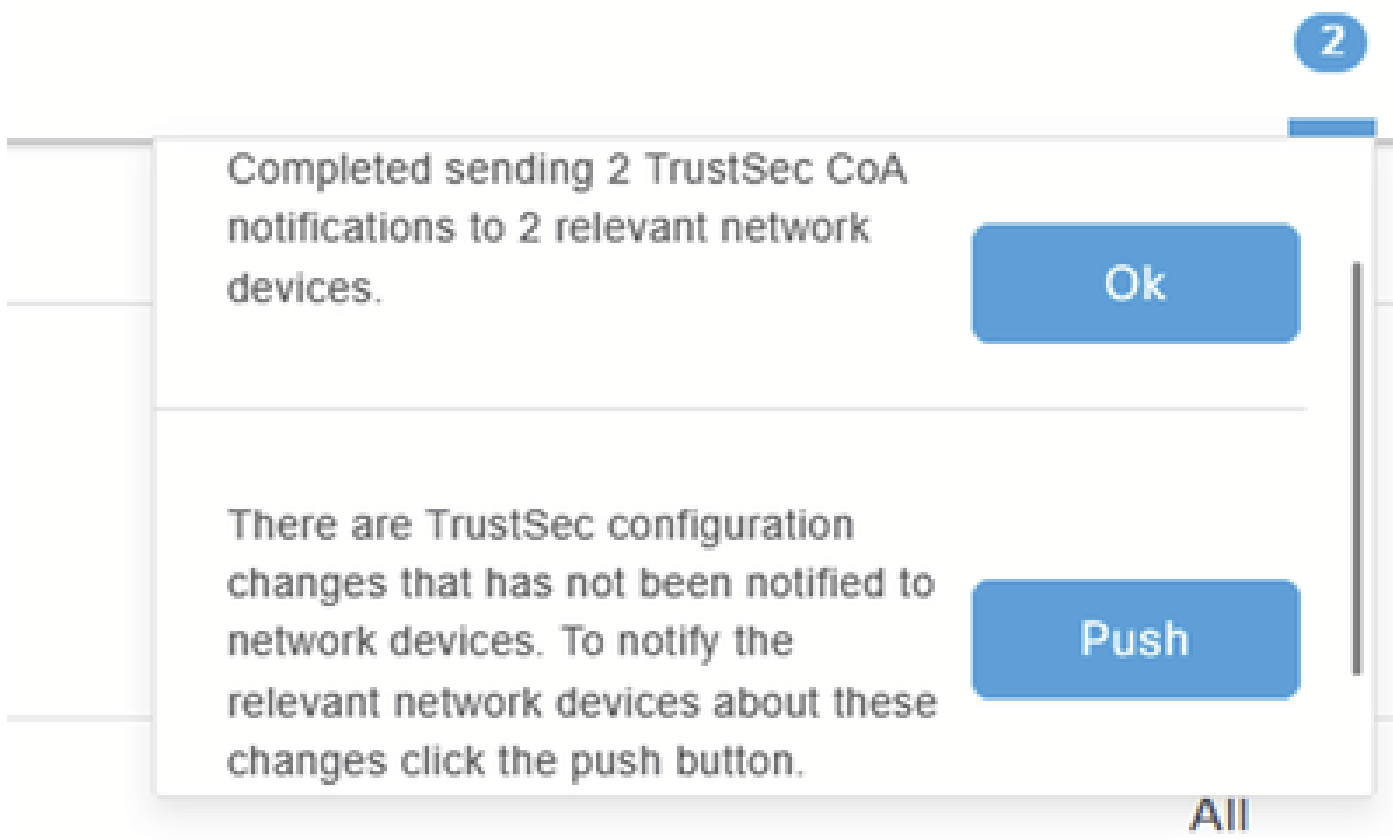
Note: Os clientes recebem um valor SGT zero e os clientes DHCP recebem um endereço APIPA (Automatic Private IP Addressing) quando a política TrustSec "desconhecida para desconhecida" é negada na matriz TrustSec.

Os clientes recebem valores SGT corretos e os clientes DHCP recebem um endereço IP quando a política TrustSec "desconhecido para desconhecido" é permitida na matriz TrustSec.

9. Clique em Implantar. O que resultará nestas mensagens e notificações:



Implantar



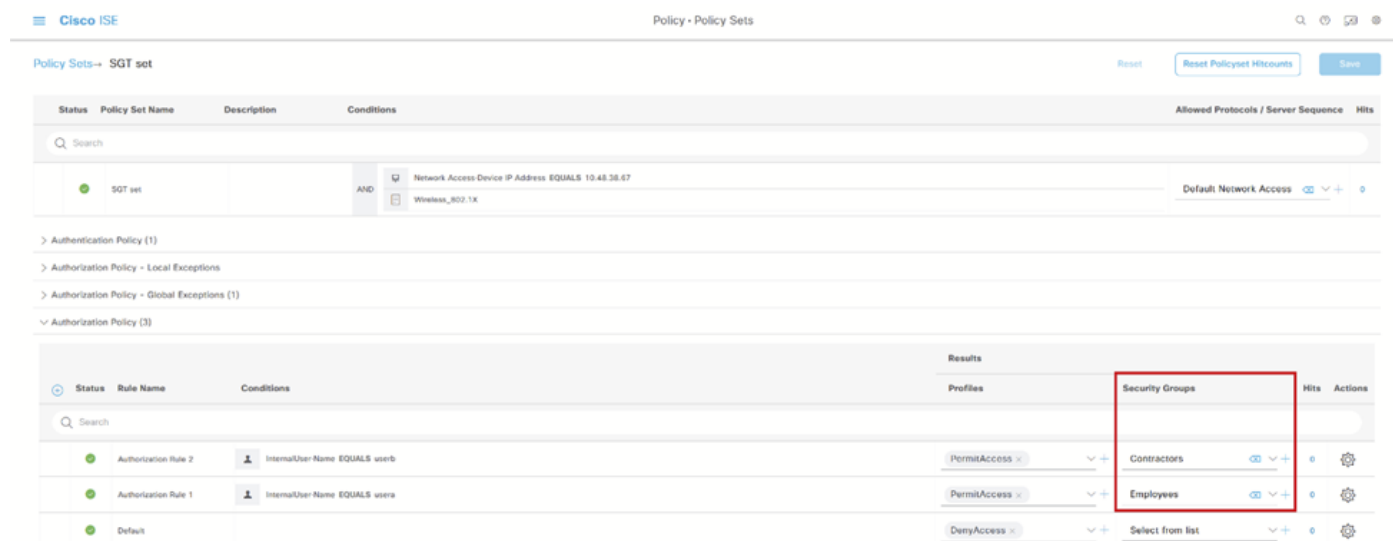
Implantar notificações

10. Navegue até o Policy Set usado para a WLAN em Policy > Policy Sets:



Conjuntos de políticas do ISE

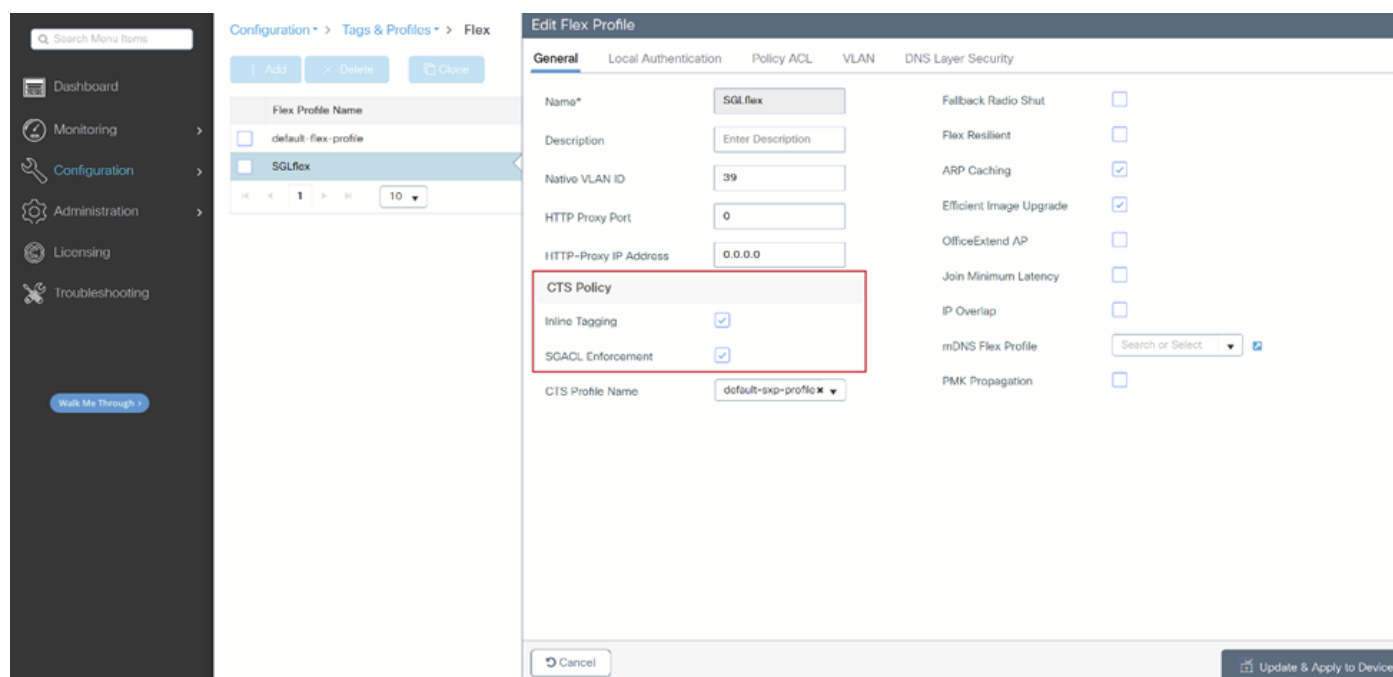
Neste laboratório, estamos definindo o SGT por usuário, selecione o SGT no campo Grupos de segurança:



Grupos de segurança do ISE

Flexconnect

Habilite Inline Tagging e Aplicação de SGACL no Perfil Flex em Configuration > Tags & Policies > Flex:

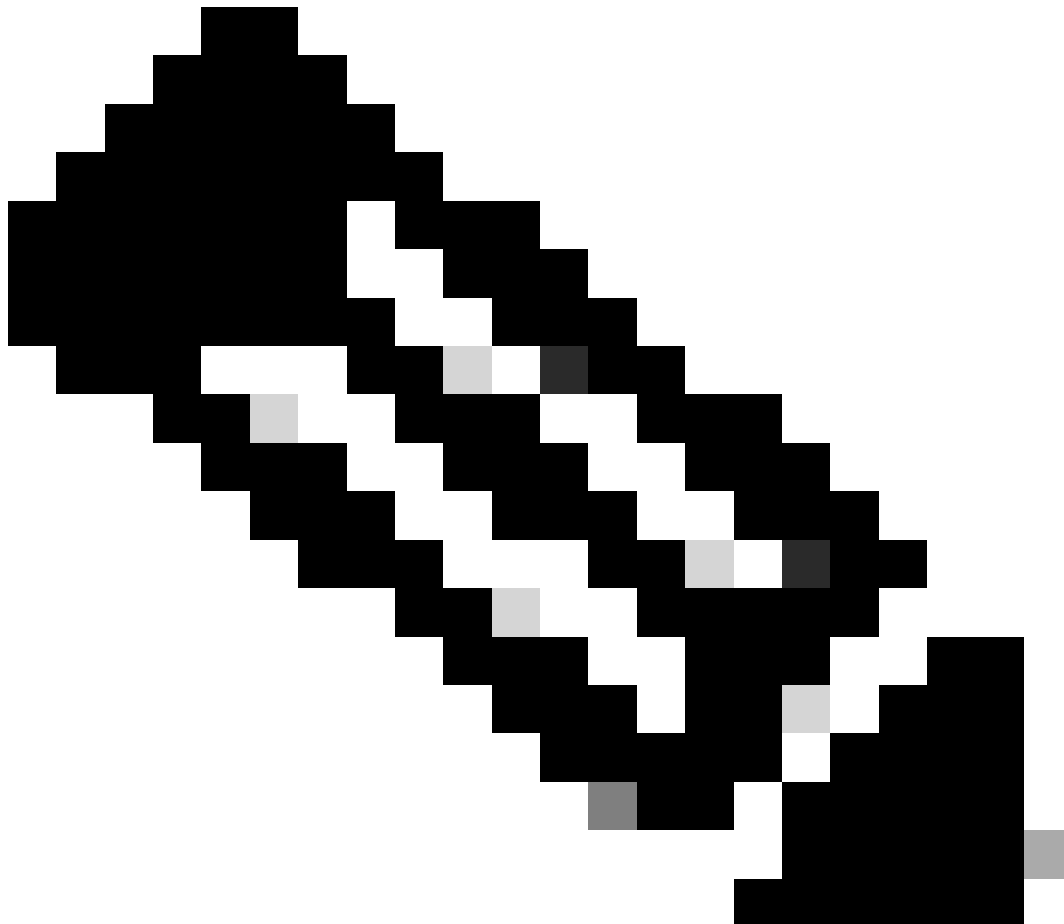


Perfil Flex da WLC

Na CLI:

```
# configure terminal
```

```
(config)# wireless profile flex SGLflex
(config-wireless-flex-profile)# cts inline-tagging
(config-wireless-flex-profile)# cts role-based enforcement
```



Note: Se a WLC estiver em HA-SSO, o SGACL nos APs FlexConnect não será suportado. ID de bug da Cisco [CSCwn85468](https://tools.cisco.com/bugtools/bugsearch/show/CSCwn85468). Isso será adicionado em 17.19.

Verificar

1. No ISE, você deve ver a solicitação CTS bem-sucedida em Operations > RADIUS > Live Logs:

Cisco ISE

Operations - RADIUS

Live Logs

Live Sessions

Misconfigured Supplicants

0

Misconfigured Network Devices

0

RADIUS Drops

0

Client Stopped Responding

0

Repeat Counter

0

Refresh Every 10 sec

Show Latest 100 rec

Within Last 24 hours

Reset Repeat Counts

Export To

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port
X				Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network Device	Device Port
Aug 22, 2025 06:51:59.7...				#CTSREQUEST#							9800labWLC	
Aug 22, 2025 06:51:59.4...				#CTSREQUEST#							9800labWLC	
Aug 22, 2025 06:51:50.4...				#CTSREQUEST#							9800labWLC	
Aug 22, 2025 06:51:50.3...				#CTSREQUEST#			NetworkD...	NetworkD...			9800labWLC	

Logs ao vivo do ISE RADIUS

2. Você pode verificar se a conexão foi estabelecida e se os SGTs foram baixados de Monitoring > General > Trustsec no WLC:

Search Items...

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Work Via Through

Monitoring

General

Trustsec

CTS Environment Data

CURRENT STATE

LAST STATUS

DATA LIFETIME

DATA REFRESHES IN

CACHE DATA APPLIED

SGT TAG

COMPLETE

Successful

86400 secs

0:23:59:35 (dd:hr:mm:sec)

NONE

2-08:TrustSec_Devices

Server List Info

Installed Server List: CTS:ServerList1-0002

IP Address

Port

Status

A-ID

10.48.39.101

1812

ALIVE

5498A6284B7C8DC7E1729C0F33A4F68D

10

items per page

1 - 1 of 1 Items

Security Group Name Table

Security Group Tag

Security Group Name

0-26

Unknown

2-08

TrustSec_Devices

3-00

Network_Services

4-20

Employees

5-19

Contractors

6-00

Guests

7-00

Production_Users

8-00

Developers

9-00

Auditors

10-00

Point_of_Sale_Systems

10

items per page

1 - 10 of 10 Items

CTS PACs

A-ID

I-ID

A-ID-INFO

CREDENTIAL LIFETIME

DOWNLOAD STATUS

5498A6284B7C8DC7E1729C0F33A4F68D

9800labWLC

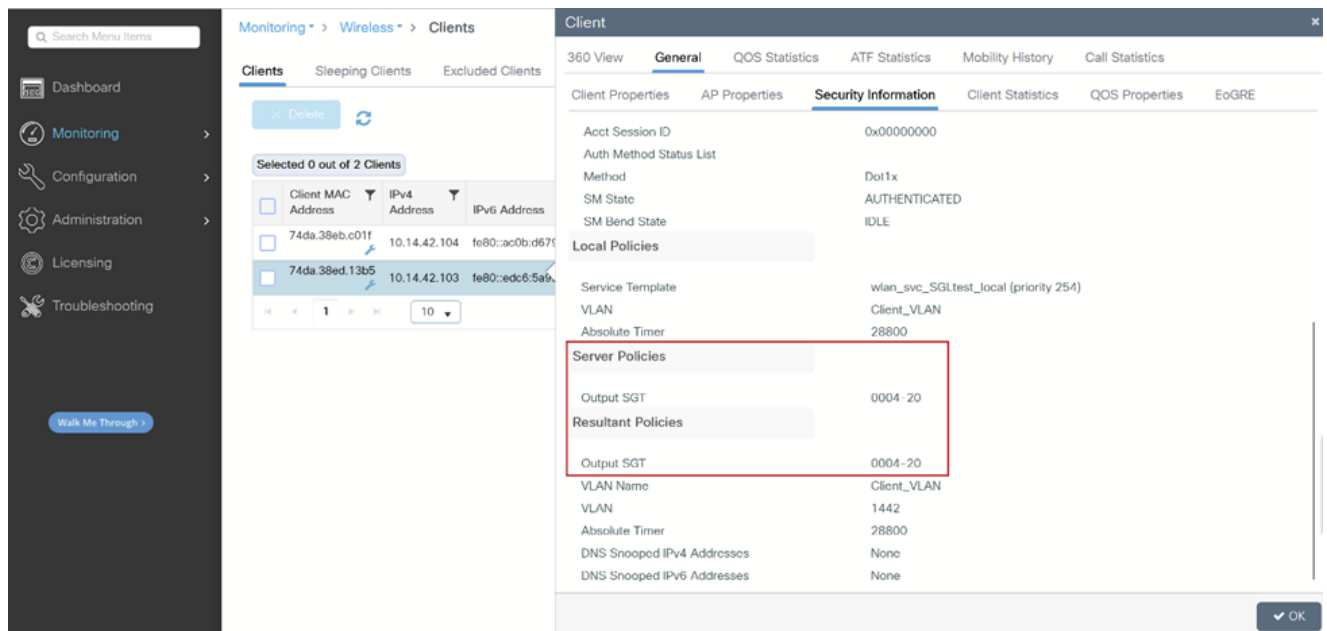
Identity Services Engine

11:13:15 Central Oct 12 2025

completed

Monitoramento do WLC TrustSec

3. Ao conectar um cliente, o SGT atribuído ficará visível em Monitoring > Wireless > Clients, escolha o cliente que deseja verificar e navegue até a guia General > Security information:



Monitoramento de cliente WLC

Na CLI:

- Antes de conectar o cliente, isso é o que você verá na saída da WLC:
Somente as permissões relacionadas a SGTs desconhecidos serão exibidas.

<#root>

#

show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address	SGT	Source
10.14.12.110	2	INTERNAL
10.48.39.55	2	INTERNAL

IP-SGT Active Bindings Summary

```

=====
Total number of INTERNAL bindings = 2
Total number of active bindings = 2

```

Active IPv6-SGT Bindings Information

IP Address	SGT	Source
------------	-----	--------

<#root>

#

show cts role-based permissions

```
IPv4 Role-based permissions default:
  Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
  SGACLtest-03
  Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
  CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
  CustomDefaultSGTACL-03
  Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
  SGACLtest-03
  Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
  CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
  SGT32-06
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

- Ao conectar o cliente, você pode observar esses logs a partir dos [rastreamentos RA](#), o SGT é aplicado a partir do AAA:

<#root>

```
2025/08/14 08:44:47.072771984 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072786402 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072788080 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info):
```

```
[ Applied attribute : security-group-tag 0 "0004-20" ]
```

```
2025/08/14 08:44:47.072809490 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :bs
2025/08/14 08:44:47.072811627 {wncd_x_R0-0}{1}: [aaa-attr-inf] [15596]: (info): [ Applied attribute :
2025/08/14 08:44:47.072824202 {wncd_x_R0-0}{1}: [auth-mgr] [15596]: (info): [0000.0000.0000:unknown] R
2025/08/14 08:44:47.072829794 {wncd_x_R0-0}{1}: [ewlc-qos-client] [15596]: (info): MAC: 74da.38ed.13b5
2025/08/14 08:44:47.072860963 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [15596]: (debug): Managed client RUN
2025/08/14 08:44:47.072905375 {wncd_x_R0-0}{1}: [client-orch-state] [15596]: (note): MAC: 74da.38ed.13b
```

- Use o comando show wireless client mac-address <client_MAC_address> detail da CLI, que mostrará o SGT atribuído ao cliente:

<#root>

```
#show wireless client mac-address 74da.38ed.13b5 detail
```

```
Client MAC Address : 74da.38ed.13b5
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.14.42.103
```

```

...
Auth Method Status List
  Method : Dot1x
        SM State      : AUTHENTICATED
        SM Bend State  : IDLE
Local Policies:
  Service Template : wlan_svc_SGLtest_local (priority 254)
  VLAN             : Client_VLAN
  Absolute-Timer   : 28800
Server Policies:

```

Output SGT : 0004-20

Resultant Policies:

Output SGT : 0004-20

```

VLAN Name      : Client_VLAN
VLAN           : 1442
Absolute-Timer : 28800

```

...

- Depois de conectar um cliente no SGT 4, você perceberá que as permissões para o SGT 4 agora aparecem:
As permissões são adicionadas depois que o cliente é conectado e recebe um SGT.

<#root>

#

show cts role-based permissions

```

IPv4 Role-based permissions default:
  Permit IP-00
IPv4 Role-based permissions from group Unknown to group Unknown:
  SGACLtest-03
  Permit IP-00
IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:
  CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 4:Employees to group Unknown:
  CustomDefaultSGTACL-03
  Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group Unknown:
  SGACLtest-03
  Permit IP-00
IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:
  CustomDefaultSGTACL-03
IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:
  SGT32-06

```

IPv4 Role-based permissions from group Unknown to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 4:Employees to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 5:Contractors to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

<#root>

#

show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address	SGT	Source
=====		
10.14.12.110	2	INTERNAL
10.14.42.103	4	LOCAL
10.48.39.55	2	INTERNAL

IP-SGT Active Bindings Summary

=====	
Total number of LOCAL	bindings = 1
Total number of INTERNAL	bindings = 2
Total number of active	bindings = 3

Active IPv6-SGT Bindings Information

IP Address	SGT	Source
=====		

- Depois de conectar dois clientes, um no SGT 4 e o outro no SGT 5:

<#root>

#

show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address	SGT	Source
=====		
10.14.12.110	2	INTERNAL
10.14.42.103	4	LOCAL
10.14.42.104	5	LOCAL
10.48.39.55	2	INTERNAL

IP-SGT Active Bindings Summary

```
=====
Total number of LOCAL bindings = 2
Total number of INTERNAL bindings = 2
Total number of active bindings = 4
```

Active IPv6-SGT Bindings Information

IP Address	SGT	Source
=====		

- Agora você pode ver que as permissões de SGT 5 são adicionadas:

<#root>

#

show cts role-based permissions

IPv4 Role-based permissions default:

Permit IP-00

IPv4 Role-based permissions from group Unknown to group Unknown:

SGACLtest-03

Permit IP-00

IPv4 Role-based permissions from group 2:TrustSec_Devices to group Unknown:

CustomDefaultSGTACL-03

IPv4 Role-based permissions from group 4:Employees to group Unknown:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 5:Contractors to group Unknown:

SGACLtest-03

Permit IP-00

IPv4 Role-based permissions from group Unknown to group 2:TrustSec_Devices:

CustomDefaultSGTACL-03

IPv4 Role-based permissions from group 2:TrustSec_Devices to group 2:TrustSec_Devices:

SGT32-06

IPv4 Role-based permissions from group Unknown to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 4:Employees to group 4:Employees:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 5:Contractors to group 4:Employees:

CustomDefaultSGTACL-03
Permit IP-00

IPv4 Role-based permissions from group Unknown to group 5:Contractors:

SGACLtest-03

Permit IP-00

IPv4 Role-based permissions from group 4:Employees to group 5:Contractors:

CustomDefaultSGTACL-03

Permit IP-00

IPv4 Role-based permissions from group 5:Contractors to group 5:Contractors:

CustomDefaultSGTACL-03

Permit IP-00

RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

- As ACLs parecerão como "baixadas" na WLC:

<#root>

#

show ip access-lists

```
Role-based IP access list CustomDefaultSGTACL-03 (downloaded)
  10 permit udp src eq bootps (12 matches)
  20 permit udp src eq bootpc
  30 permit ip
Extended IP access list IP-Adm-V4-Int-ACL-global
  10 permit tcp any any eq www
  20 permit tcp any any eq 443
Role-based IP access list Permit IP-00 (downloaded)
  10 permit ip
Role-based IP access list SGACLtest-03 (downloaded)
  10 permit udp src eq bootps (18 matches)
  20 permit udp src eq bootpc
  30 permit udp dst eq bootps
```

```

40 permit udp dst eq bootpc
50 permit ip
Role-based IP access list SGT32-06 (downloaded)
10 permit ip
Extended IP access list implicit_deny
10 deny ip any any
Extended IP access list implicit_permit
10 permit ip any any
Extended IP access list meraki-fqdn-dns
Extended IP access list preauth_v4
10 permit udp any any eq domain
20 permit tcp any any eq domain
30 permit udp any eq bootps any
40 permit udp any any eq bootpc
50 permit udp any eq bootpc any
60 deny ip any any

```

Switching local FlexConnect

- Esta é a saída da WLC antes de conectar clientes ao AP:

```
<#root>
```

```
#
```

```
show cts ap sgt-info
```

```
Number of SGTs referred by the AP.....: 4
```

SGT	PolicyPushedToAP	No.of Clients
UNKNOWN(0)	NO	0
2	NO	1
DEFAULT(65535)	YES	0

- Na CLI do AP, esta é a saída de permissões antes de conectar clientes ao AP:

```

AP#show cts role-based permissions
IPv4 role-based permissions:
SGT DGT ACL
65535 65535 Permit_IP

```

```

IPv6 role-based permissions:
SGT DGT ACL
65535 65535 Permit_IP

```

- Estas são as depurações de AP enquanto o cliente está se conectando para mostrar o fluxo:

<#root>

```
[*08/14/2025 09:45:40.8504] CLSM[74:DA:38:ED:13:B5]: US Auth(b0) seq 2599 IF 72 slot 0 vap 0 len 30 sta
[*08/14/2025 09:45:40.8507] CLSM[74:DA:38:ED:13:B5]: DS Auth len 30 slot 0 vap 0
[*08/14/2025 09:45:40.8509] CLSM[74:DA:38:ED:13:B5]: Driver send mgmt frame success Radio 0 Vap 0
[*08/14/2025 09:45:40.8509] CLSM[74:DA:38:ED:13:B5]: client moved from UNASSOC to AUTH
[*08/14/2025 09:45:40.8660] CLSM[74:DA:38:ED:13:B5]: US Assoc Req(0) seq 2600 IF 72 slot 0 vap 0 len 17
...
[*08/14/2025 09:45:40.8782] CLSM[74:DA:38:ED:13:B5]: client moved from ASSOC to 8021X
[*08/14/2025 09:45:40.8783] CLSM[74:DA:38:ED:13:B5]: Added to WCP client table AID 1 Radio 0 Vap 0 Enc
[*08/14/2025 09:45:40.8784] CLSM[74:DA:38:ED:13:B5]:
```

SGT Data sent: 74:DA:38:ED:13:B5 0 0

!--- The client initiates the connection and it's directly put under the SGT 0.

<#root>

```
[*08/14/2025 09:45:40.8800] CLSM[74:DA:38:ED:13:B5]: ADD_CENTRAL_AUTH_INFO_MOBILE Payload
[*08/14/2025 09:45:40.8801] CLSM[74:DA:38:ED:13:B5]: msAssocTypeFlags: 2 apfMsEntryType: 2 eap_type: 0
[*08/14/2025 09:45:40.8807] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility: 0
[*08/14/2025 09:45:40.8812] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[*08/14/2025 09:45:41.5130] CLSM[74:DA:38:ED:13:B5]: ADD_MOBILE AID 1
[*08/14/2025 09:45:41.5135] CLSM[74:DA:38:ED:13:B5]: Client ADD Encrypt Key success AID 1 Radio 0 Enc 4
[*08/14/2025 09:45:41.5139] chatter: 74:DA:38:ED:13:B5: web_auth status 1
[*08/14/2025 09:45:41.5140] CLSM[74:DA:38:ED:13:B5]: client moved from 8021X to
```

IPLEARN_PENDING

!--- The client must get an IP address through DHCP.

<#root>

```
[*08/14/2025 09:45:41.5144] CLSM[74:DA:38:ED:13:B5]: ADD_CENTRAL_AUTH_INFO_MOBILE Payload
[*08/14/2025 09:45:41.5144] CLSM[74:DA:38:ED:13:B5]: msAssocTypeFlags: 2 apfMsEntryType: 2 eap_type: 25
[*08/14/2025 09:45:41.5150] CLSM[74:DA:38:ED:13:B5]: TLV_FLEX_CENTRAL_AUTH_STA_PAYLOAD
[*08/14/2025 09:45:41.5155] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENTCAPABILITYPAYLOAD: capbaility: 0
[*08/14/2025 09:45:41.5161] CLSM[74:DA:38:ED:13:B5]:
```

SGT Data sent: 74:DA:38:ED:13:B5 4 0

!--- Afterwards, the assigned SGT for that client is going to be applied accordingly.

<#root>

```
[*08/14/2025 09:45:41.5163] CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[*08/14/2025 09:45:41.6476] chatter: find_insert_client:3313
[*08/14/2025 09:45:41.6476] chatter: Update IP from 0.0.0.0 to 10.14.42.103
[*08/14/2025 09:45:41.6477] chatter:
```

Update ipsgt: IPV4 client(74:DA:38:ED:13:B5) - [10.14.42.103]

!--- Associated IP & SGT is going to be added into mapping table.

<#root>

```
[*08/14/2025 09:45:41.6477] chatter: Update ipsgt IPV6 client(74:DA:38:ED:13:B5) - [fe80::edc6:5a93:ada
[*08/14/2025 09:45:41.6481] CLSM[74:DA:38:ED:13:B5]: Authorize succeeded to radio intf apr0v0
[*08/14/2025 09:45:41.6490] chatter: 74:DA:38:ED:13:B5: web_auth status 1
[*08/14/2025 09:45:41.6492] CLSM[74:DA:38:ED:13:B5]: client moved from IPLEARN_PENDING to
```

FWD

<#root>

**!--- Then for the IP-SGT mapping entry in the mapping table, SGACL policy for those SGTs is requested.
!--- This is a snippet of the AP debugs showing one of the ACLs:**

```
CLSM[74:DA:38:ED:13:B5]: SGT Data sent: 74:DA:38:ED:13:B5 4 0
CLSM[74:DA:38:ED:13:B5]: Decoding TLV_CLIENT_TYPE_PAYLOAD: Client Type : 0
[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)
.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8
[DEC] CAPWAP_CONFIGURATION_UPDATE_REQUEST(7) seq 165 len 148
....TLV: TLV_CTS_RBACL_DELETE(1434), level: 0, seq: 0, nested: true
....TLV: TLV_CTS_RBACL_DELETE(1437), level: 1, seq: 0, nested: false
TLV_CTS_RBACL_DELETE received
ACL Name:CustomDefaultSGTACL
....TLV: TLV_CTS_RBACL_ADD(1433), level: 0, seq: 0, nested: true
....TLV: TLV_CTS_RBACL_ADD(1437), level: 1, seq: 0, nested: false
....TLV: TLV_CTS_RBACL_ADD(1438), level: 1, seq: 1, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 2, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 3, nested: false
....TLV: TLV_CTS_RBACL_ADD(1439), level: 1, seq: 4, nested: false
TLV_CTS_RBACL_ADD received
```

ACL Name:CustomDefaultSGTACL

ACL Type:1

ACE entry:permit udp src eq bootps

ACE entry:permit udp src eq bootpc

ACE entry:permit ip

[ENC] CAPWAP_CONFIGURATION_UPDATE_RESPONSE(8)

.Msg Elem Type: CAPWAP_MSGELE_RESULT_CODE(33) Len 8 Total 8

...

- Na CLI da WLC, ao conectar um cliente no SGT 4:

<#root>

#

show cts ap sgt-info

Number of SGTs referred by the AP.....: 4

SGT	PolicyPushedToAP	No.of Clients

UNKNOWN(0)	NO	0
2	NO	1
4	YES	1
DEFAULT(65535)	YES	0

- Do AP CLI:

Você pode ver a mesma coisa, apenas as permissões relacionadas ao SGT 4 são adicionadas.

AP#show cts role-based permissions

IPv4 role-based permissions:

SGT DGT ACL

0 4 Permit_IP, CustomDefaultSGTACL

4 4 Permit_IP, CustomDefaultSGTACL

5 4 Permit_IP, CustomDefaultSGTACL

65535 65535 Permit_IP

IPv6 role-based permissions:

SGT DGT ACL

```

0 4 Permit_IP
4 4 Permit_IP
5 4 Permit_IP
65535 65535 Permit_IP

```

- Na CLI da WLC, ao conectar o segundo cliente no SGT 5:

```
<#root>
```

```
#
```

```
show cts ap sgt-info
```

```
Number of SGTs referred by the AP.....: 5
```

SGT	PolicyPushedToAP	No.of Clients

UNKNOWN(0)	NO	0
2	NO	1
4	YES	1
5	YES	1
DEFAULT(65535)	YES	0

- Saídas AP:

```
<#root>
```

```
AP#
```

```
show flexconnect client
```

```
Flexconnect Clients:
```

```
mac radio vap aid state encr aaa-vlan aaa-acl aaa-ipv6-acl assoc auth switching
```

```
SGT
```

```
74:DA:38:EB:C0:1F 0 0 1 FWD AES_CCM128 none none none Local Central Local
```

```
5
```

```
74:DA:38:ED:13:B5 0 0 2 FWD AES_CCM128 none none none Local Central Local
```

```
4
```

<#root>

AP#

show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

	IP	SGT	SOURCE
10.14.42.103	4	LOCAL	
10.14.42.104	5	LOCAL	

IP-SGT Active Bindings Summary

=====

Total number of LOCAL	bindings = 2
Total number of active	bindings = 2

Active IPv6-SGT Bindings Information

	IP	SGT	SOURCE
fe80::ac0b:d679:e356:a17	5	LOCAL	
fe80::edc6:5a93:adab:fff6	4	LOCAL	

IP-SGT Active Bindings Summary

=====

Total number of LOCAL	bindings = 2
Total number of active	bindings = 2

<#root>

AP#

show cts role-based permissions

IPv4 role-based permissions:

SGT	DGT	ACL
0	4	Permit_IP, CustomDefaultSGTACL
4	4	Permit_IP, CustomDefaultSGTACL
5	4	Permit_IP, CustomDefaultSGTACL
0	5	Permit_IP, SGACLtest
4	5	Permit_IP, CustomDefaultSGTACL
5	5	Permit_IP, CustomDefaultSGTACL
65535	65535	Permit_IP, CustomDefaultSGTACL

IPv6 role-based permissions:

SGT	DGT	ACL
0	4	Permit_IP
4	4	Permit_IP
5	4	Permit_IP
0	5	Permit_IP
4	5	Permit_IP
5	5	Permit_IP
65535	65535	Permit_IP

<#root>

AP#

show cts access-lists

IPv4 role-based ACL:

SGACLtest

```
rule 0: allow true && ip proto 17 && ( src port 67 )
rule 1: allow true && ip proto 17 && ( src port 68 )
rule 2: allow true && ip proto 17 && ( dst port 67 )
rule 3: allow true && ip proto 17 && ( dst port 68 )
rule 4: allow true
```

CustomDefaultSGTACL

```
rule 0: allow true && ip proto 17 && ( src port 67 )
rule 1: allow true && ip proto 17 && ( src port 68 )
rule 2: allow true
```

Permit_IP

```
rule 0: allow true
```

IPv6 role-based ACL:

Permit_IP

```
rule 0: allow true
```

<#root>

AP#

show cts role-based sgt-map summary

-IPv4-

IP-SGT Active Bindings Summary

=====

Total number of LOCAL bindings = 2

Total number of active bindings = 2

-IPv6-

IP-SGT Active Bindings Summary

=====

Total number of LOCAL bindings = 2

Total number of active bindings = 2

Troubleshooting

- Da CLI da WLC:

show cts provisioning

show cts role-based permissions

show ip access-lists

show cts ap sgt-info <ap_name>

- Do AP:

show cts role-based sgt-map all

show cts role-based permissions

show cts access-lists <acl-name>

show cts role-based sgt-map summary

show cts access-lists

show flexconnect client

clear cts role-based counters

show cts role-based counters

- Depurações de AP:
- Habilita a depuração de imposição de nível de pacote CTS:

debug cts enforcement

term mon

- Para verificar eventos da ACL CAPWAP e informações relacionadas à carga útil:

debug dot11 client access-list <client-mac-addr>

debug capwap client acl

debug capwap client payload

debug capwap client error

debug dot11 client management information

debug dot11 client management critical

debug dot11 client management error

debug dot11 client management events

debug generic datapath client_ip_table/debug_acl

debug generic datapath client_ip_table/debug

debug generic datapath sgACL/debug

debug generic datapath sgACL/debug_sgt

debug generic datapath sgACL/debug_protocol

debug generic datapath sgac/debug_permission

term mon

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.