

在Catalyst 9800 WLC和ISE服务器上配置和验证SGACL

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[WLC 配置](#)

[ISE 配置](#)

[FlexConnect](#)

[验证](#)

[FlexConnect本地交换](#)

[故障排除](#)

简介

本文档介绍如何在Catalyst 9800和ISE服务器上配置TrustSec以利用SGACL功能，以及本地和FlexConnect模式AP。

先决条件

要求

了解Cisco 9800 WLC、Cisco ISE、FlexConnect和TrustSec基础知识。

使用的组件

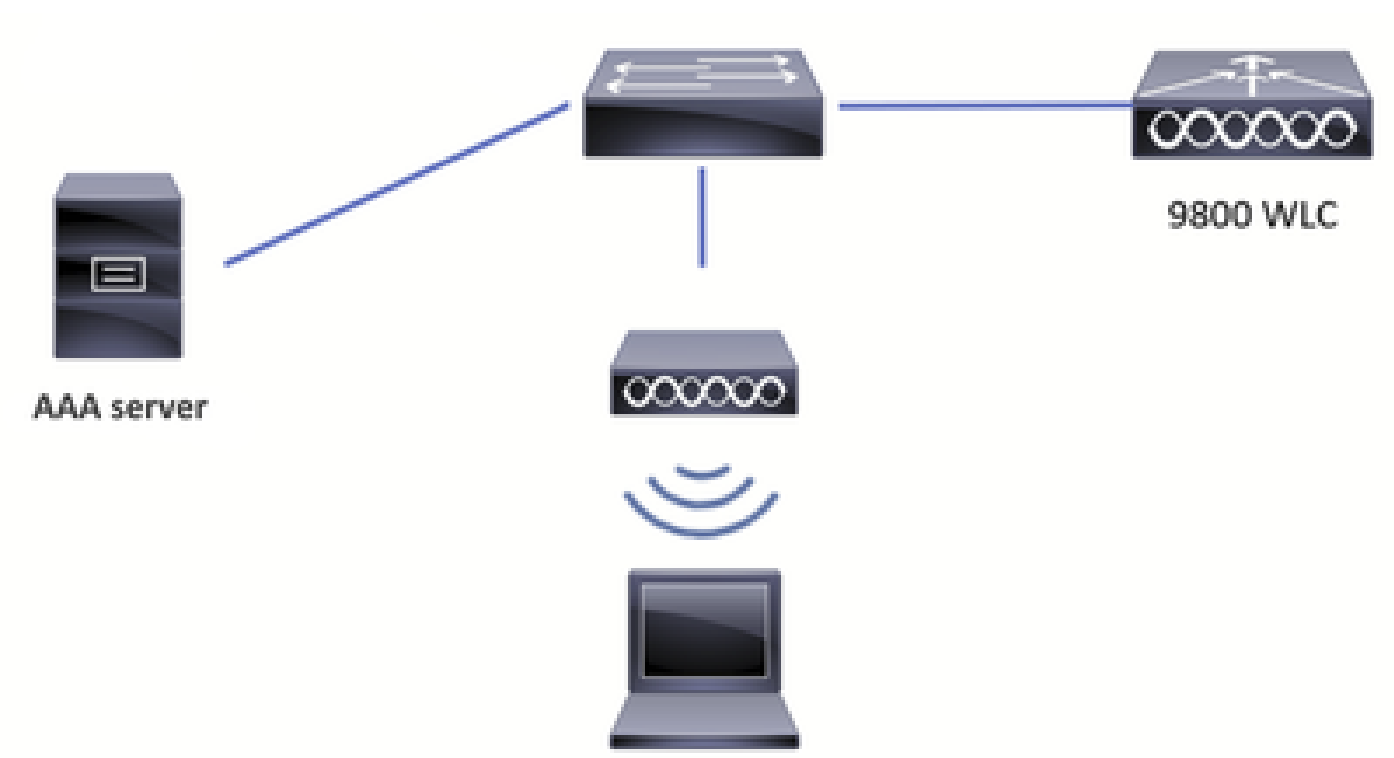
本文档中的信息基于以下软件和硬件版本：

- C9800-CL v17.12.4
- ISE 3.2.0
- 9136I无线接入点

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

配置

网络图

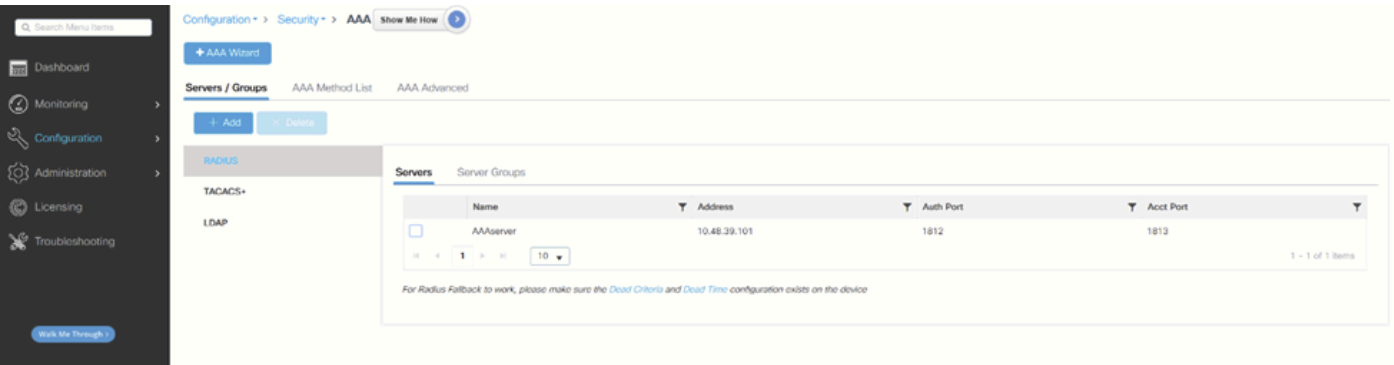


网络图

配置

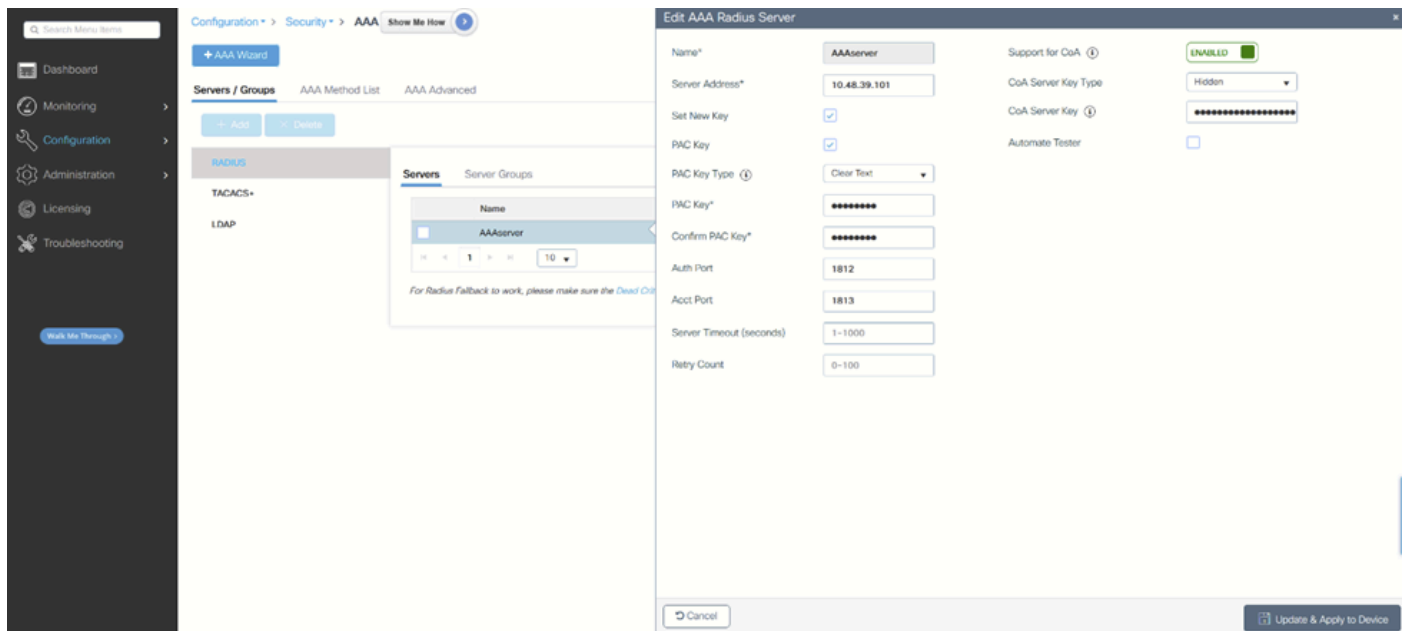
WLC 配置

1.从Configuration > Security > AAA将AAA服务器添加到WLC:



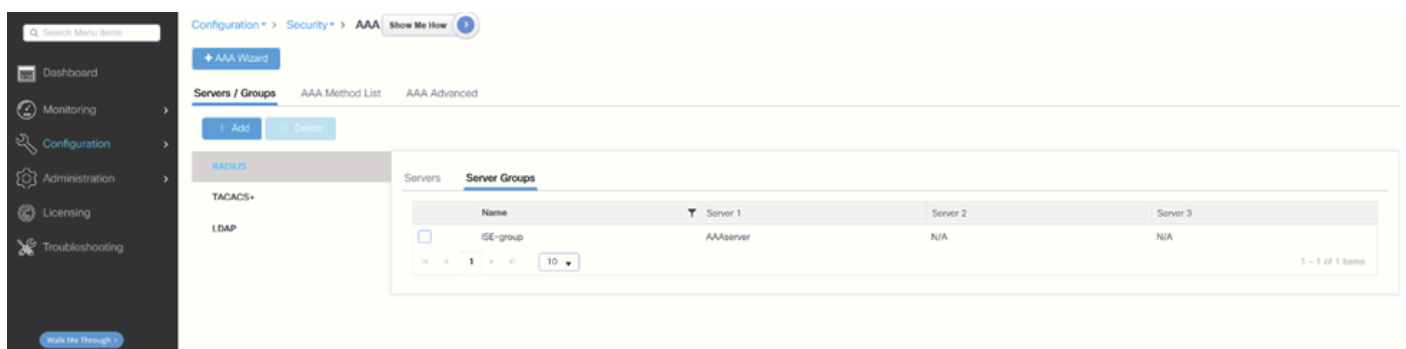
WLC AAA页

2.在ISE上添加设备时，请确保此处的密钥条目与密钥匹配。启用CoA支持并添加密钥（如果您希望使用CoA下载配置更新）：



WLC添加AAA服务器

3.创建服务器组：



WLC添加服务器组

4.添加Authorization Method List，并键入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

↻ Cancel

Apply to Device

授权方法列表

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

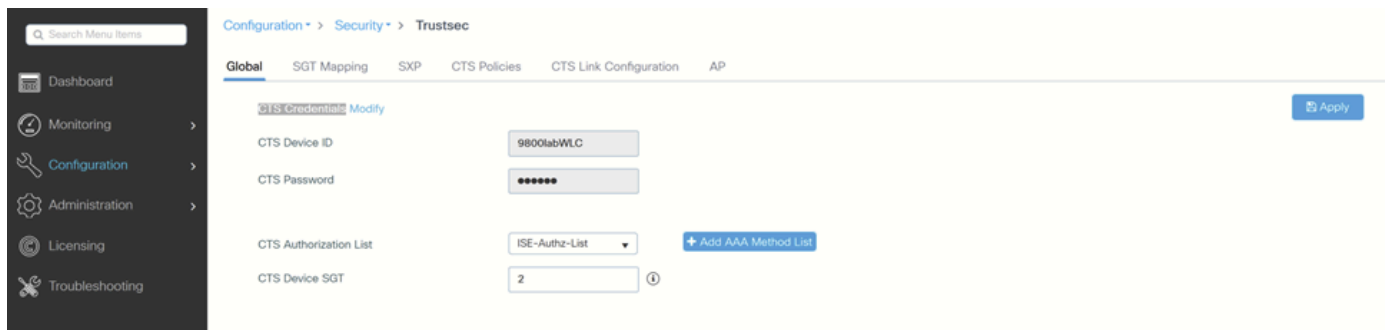
Name	Type	Group Type	Group1	Group2	Group3	Group4
☐ default	exec	local	N/A	N/A	N/A	N/A
☐ ISE-Authz-List	network	group	ISE-group	N/A	N/A	N/A

1
10
1 - 2 of 2 items

WLC AAA服务器组

5.导航到Configuration > Security > Trustsec并配置CTS Device ID和CTS Password，您将在ISE上添加设备时使用这些条目。

在此处配置您在第4步中创建的CTS授权列表：

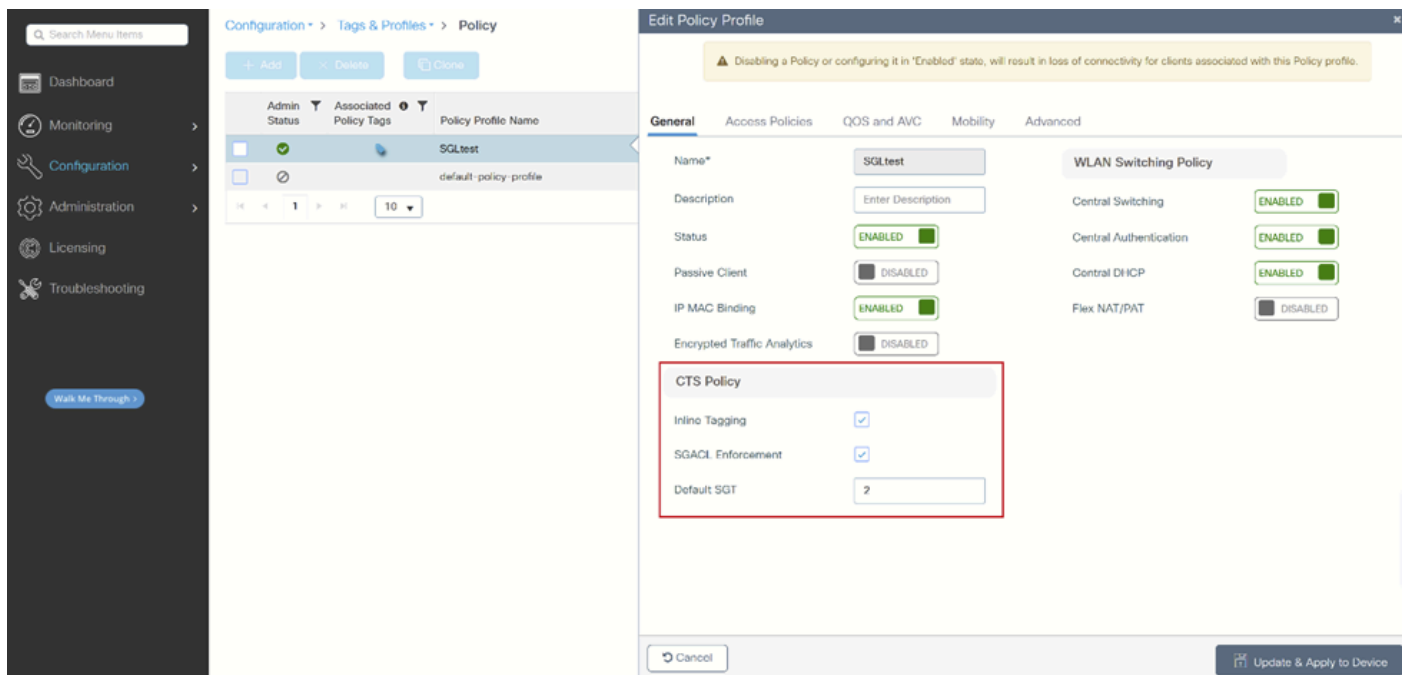


WLC TrustSec

6.在本示例中，已创建WLAN并已配置身份验证设置。

现在，导航至您要使用SGT的策略配置文件。

i.在CTS Policy下，启用Inline Tagging和SGACL Enforcement，您还可以指定Default SGT。本实验使用默认SGT 2作为示例：



WLC策略配置文件

二、在Advanced选项卡下，启用Allow AAA override和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

WLC策略配置文件高级选项卡

从 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

ISE 配置

1.导航到管理>网络资源>网络设备。

i.在此处添加WLC信息：

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 shows the 'Network Devices List' with a link to '9800labWLC'. Below this, the 'Network Devices' configuration form is displayed. The 'Name' field is set to '9800labWLC'. The 'Description' field is empty. The 'IP Address' field is set to '10.48.38.67 / 32'.

ISE网络设备页面

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 shows the 'Network Devices List' with a link to '9800labWLC'. Below this, the 'Network Devices' configuration form is displayed. The 'Name' field is set to '9800labWLC'. The 'Description' field is empty. The 'IP Address' field is set to '10.48.38.67 / 32'. The 'Device Profile' is set to 'Cisco'. The 'Model Name' field is empty. The 'Software Version' field is empty. The 'Network Device Group' is set to 'All Locations'. The 'Location' field is set to 'All Locations'. The 'IPSEC' field 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' field is set to '*****'. The 'Use Second Shared Secret' checkbox is unchecked. The 'Second Shared Secret' field is empty.

ISE添加WLC RADIUS信息

二、向下滚动并配置Advanced TrustSec Settings，启用Use Device ID for TrustSec Identification复选框并配置密码：

Cisco ISE

Administration · Network Resources

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

Network Devices

Default Device

Device Security Settings

☒

Advanced TrustSec Settings

Device Authentication Settings

☒

Use Device ID for TrustSec Identification

Device Id9800labWLC

Password●●●●●●●●Show

高级TrustSec设置

这必须与WLC配置步骤6中WLC端的配置相匹配。

三。向下滚动到TrustSec Notifications and Updates，并配置是否要使用CoA或SSH进行配置更新。选择所需的ISE节点：

Cisco ISE

Administration · Network Resources

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

NAC Managers

Network Devices

Default Device

Device Security Settings

TrustSec Notifications and Updates

Download environment data every10Seconds

Download peer authorization policy every10Seconds

Reauthentication every1Days

Download SGACL lists every10Seconds

☒ Other TrustSec devices to trust this device

☒ Send configuration changes to device

☒ CoA

☐ CLI (SSH)

Send fromvarusrin-iseTest connection

Ssh Key

TrustSec通知和更新

2.按测试连接以确保已建立连接。当它成功时，将会显示绿色的勾选标记：

☒ Send configuration changes to device

CoA

CLI (SSH)

Send from

varusrin-ise

Test connection

Ssh Key

测试连接

i.向下滚动并配置部署SGT映射更新时要包括的WLC，如果您在上一步中选择SSH选项，这一点非常重要：

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

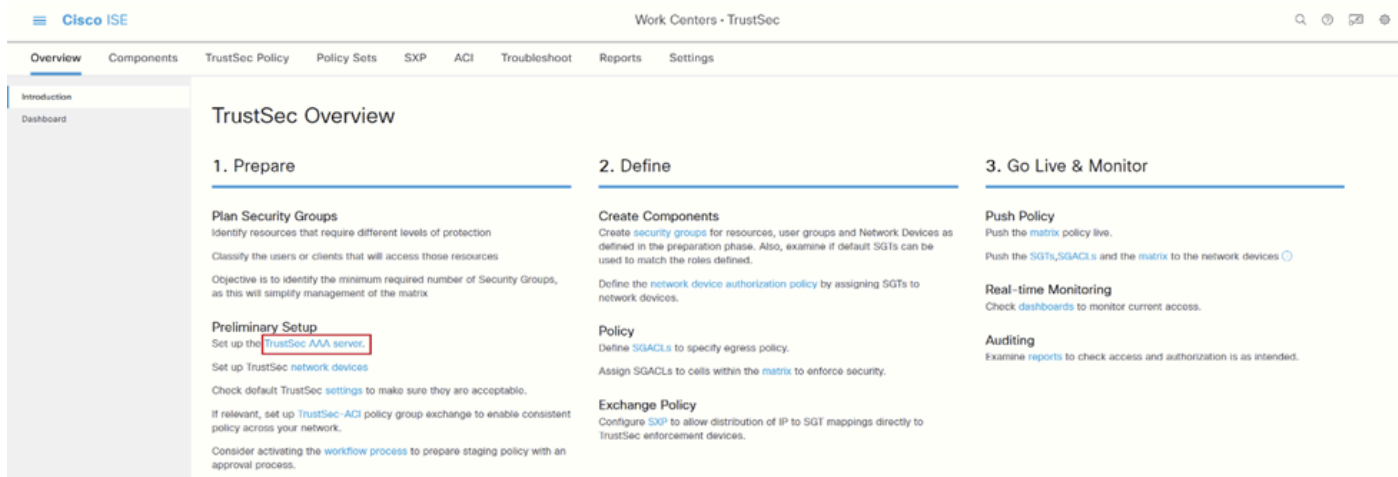
.....

Show

设备配置部署

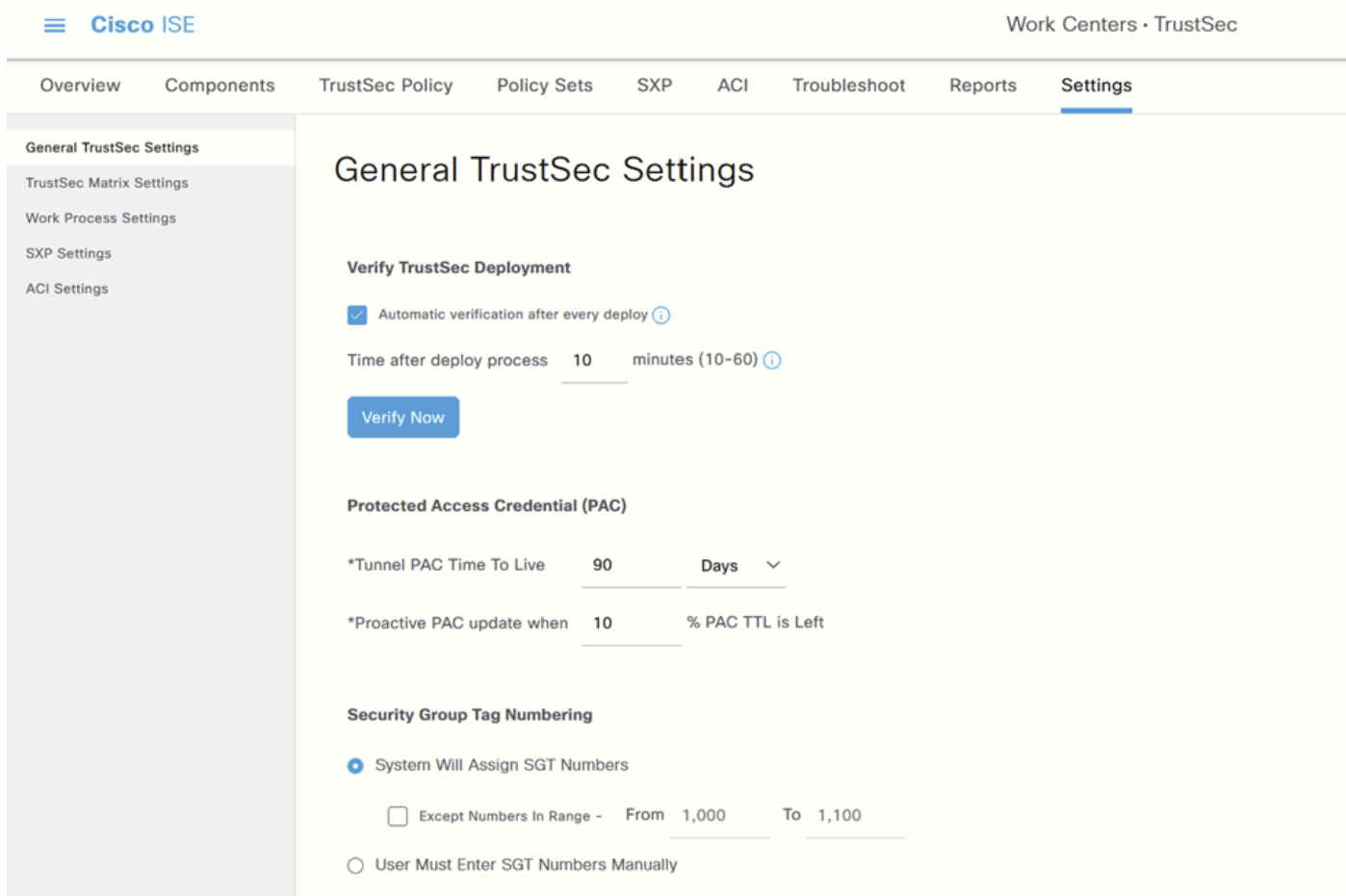
二、保存配置。

3.从“工作中心”>“TrustSec”>“概述”中，您可以选择TrustSec配置选项。选择TrustSec AAA Server以查看正在使用的ISE实例。有关使用哪个实例（如果有多个实例）的详细信息，请参阅[Cisco Catalyst无线组策略](#)。



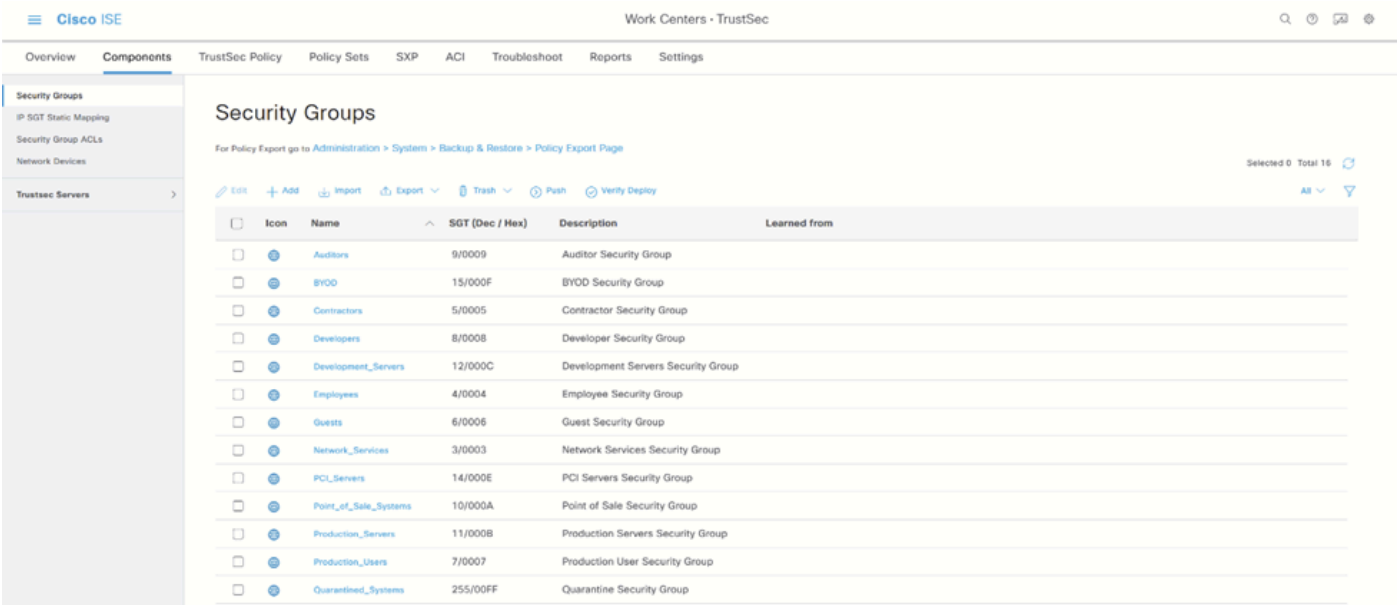
ISE TrustSec概述

4. (可选) 导航到Settings选项卡，启用Automatic verification after every deploy (如果首选)。



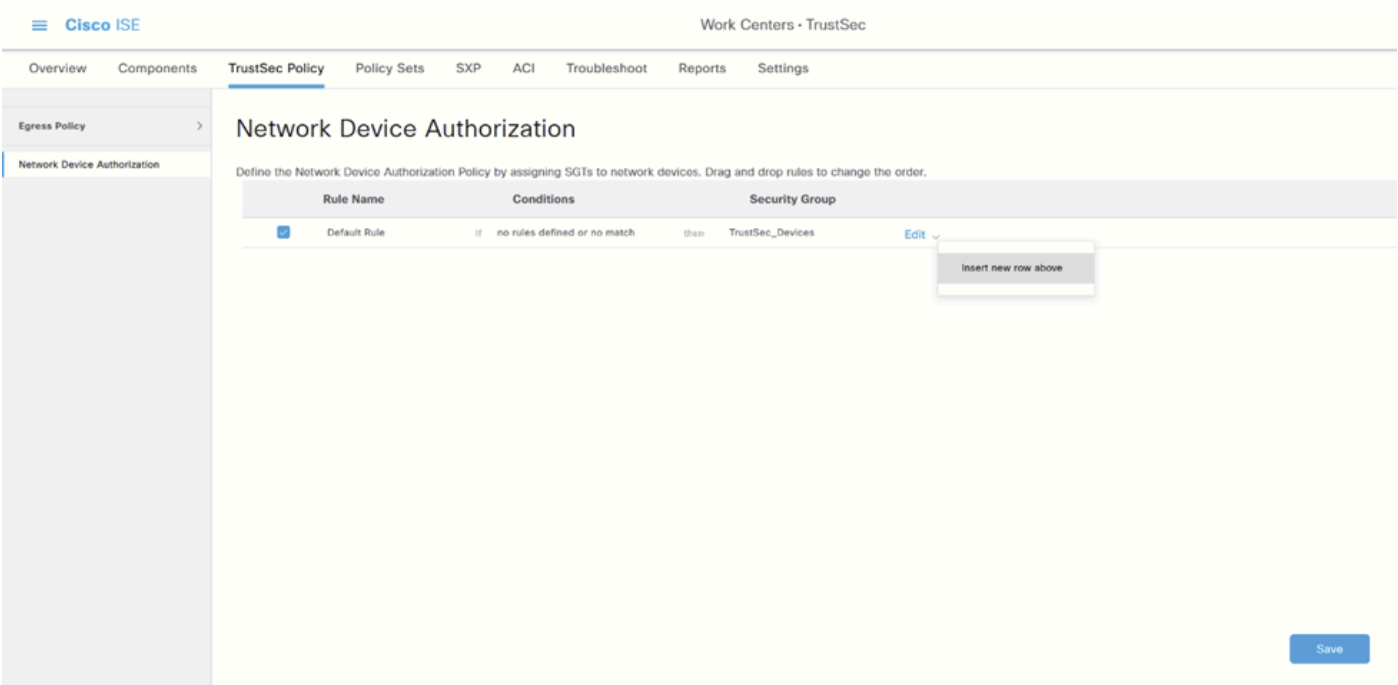
ISE TrustSec设置

5.根据您的要求，从工作中心> TrustSec >组件>安全组添加或编辑SGT值：



ISE安全组

6.如果要指定授权策略，请导航至工作中心> TrustSec > TrustSec策略>网络设备授权：



TrustSec策略

您可以保留默认值，但在本实验中，我们将使用此配置作为示例：

例如：

✕

Edit Permissions...

Source Security Group

Contractors (5/0005)

Destination Security Group

Contractors (5/0005)

Status

☒ Enabled ▾

Description

Assigned Security Group ACLs

⋮

⚙

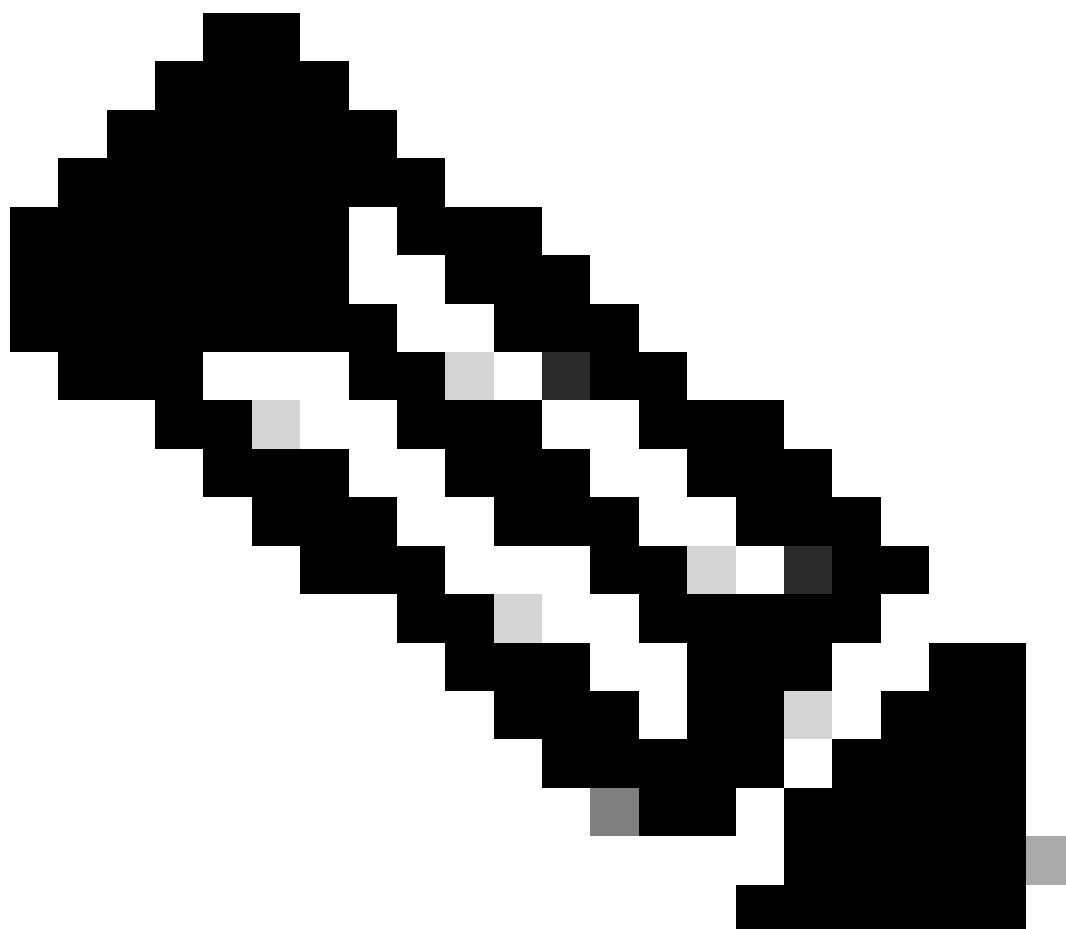
ustomDefaultSGTACL ▾

Final Catch All Rule

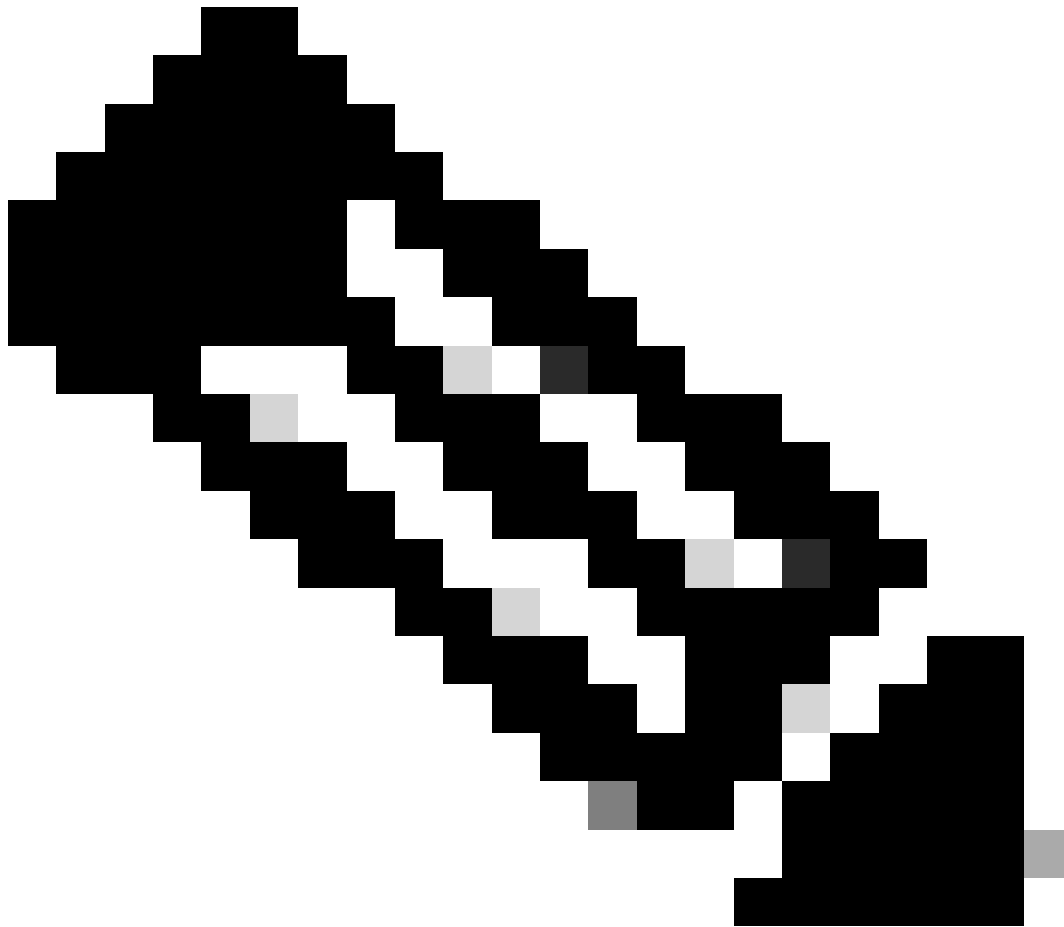
Permit IP ▾

Cancel

Save

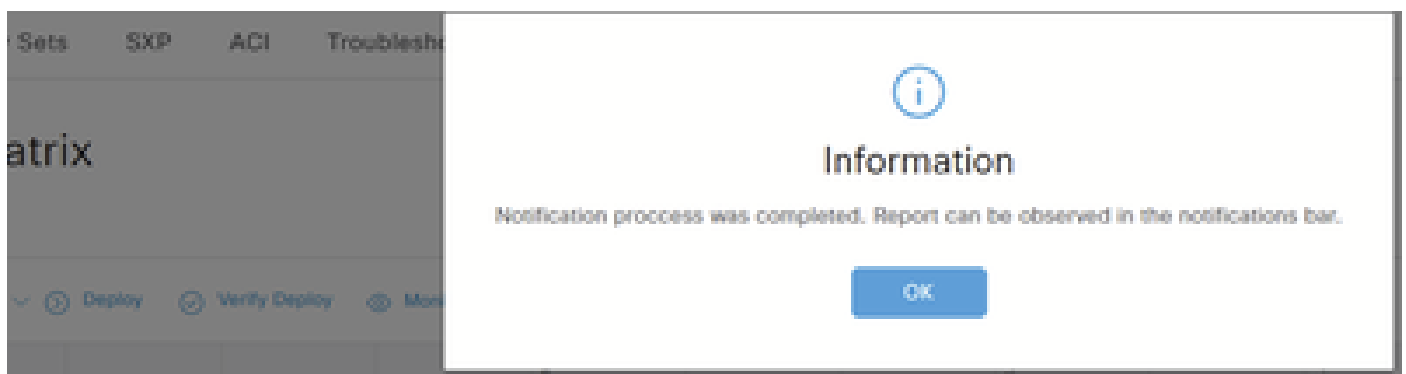


注意：如果使用Allow List模型，您需要明确允许客户端设备的DHCP协议以获取DHCP IP地址，然后请求控制器提供SGACL策略。



注意：当TrustSec策略“unknown to unknown”在TrustSec矩阵中被拒绝时，客户端接收零SGT值，DHCP客户端接收自动私有IP寻址(APIPA)地址。
当TrustSec矩阵中允许TrustSec策略“unknown to unknown”时，客户端接收正确的SGT值，DHCP客户端接收IP地址。

9.单击部署。将生成以下消息和通知：



Completed sending 2 TrustSec CoA notifications to 2 relevant network devices.

Ok

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.

Push

All

部署通知

10.导航到策略>策略集下的策略集，该策略集用于WLAN:



ISE策略集

在本实验中，我们将定义每个用户的SGT，在Security Groups字段下选择SGT:

Cisco ISE Policy - Policy Sets

Policy Sets → SGT set

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	SGT set		AND Network Access Device IP Address EQUALS 10.48.38.67 Wireless_R02 1X	Default Network Access	

> Authentication Policy (1)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions (1)
v Authorization Policy (3)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
●	Authorization Rule 2	InternalUser-Name EQUALS userb	PermitAccess		Contractors	0	
●	Authorization Rule 1	InternalUser-Name EQUALS usera	PermitAccess		Employees	0	
●	Default		DenyAccess		Select from list	0	

ISE安全组

FlexConnect

在Configuration > Tags & Policies > Flex下的Flex Profile上启用内联标记和SGACL实施:

Configuration > Tags & Profiles > Flex

Edit Flex Profile

General Local Authentication Policy ACL VLAN DNS Layer Security

Name* SGLflex

Description Enter Description

Native VLAN ID 39

HTTP Proxy Port 0

HTTP-Proxy IP Address 0.0.0.0

CTS Policy

Inline Tagging ☒

SGACL Enforcement ☒

CTS Profile Name default-sxp-profile

Fallback Radio Shut ☐

Flex Resilient ☐

ARP Caching ☒

Efficient Image Upgrade ☒

OfficeExtend AP ☐

Join Minimum Latency ☐

IP Overlap ☐

mDNS Flex Profile Search or Select

PMK Propagation ☐

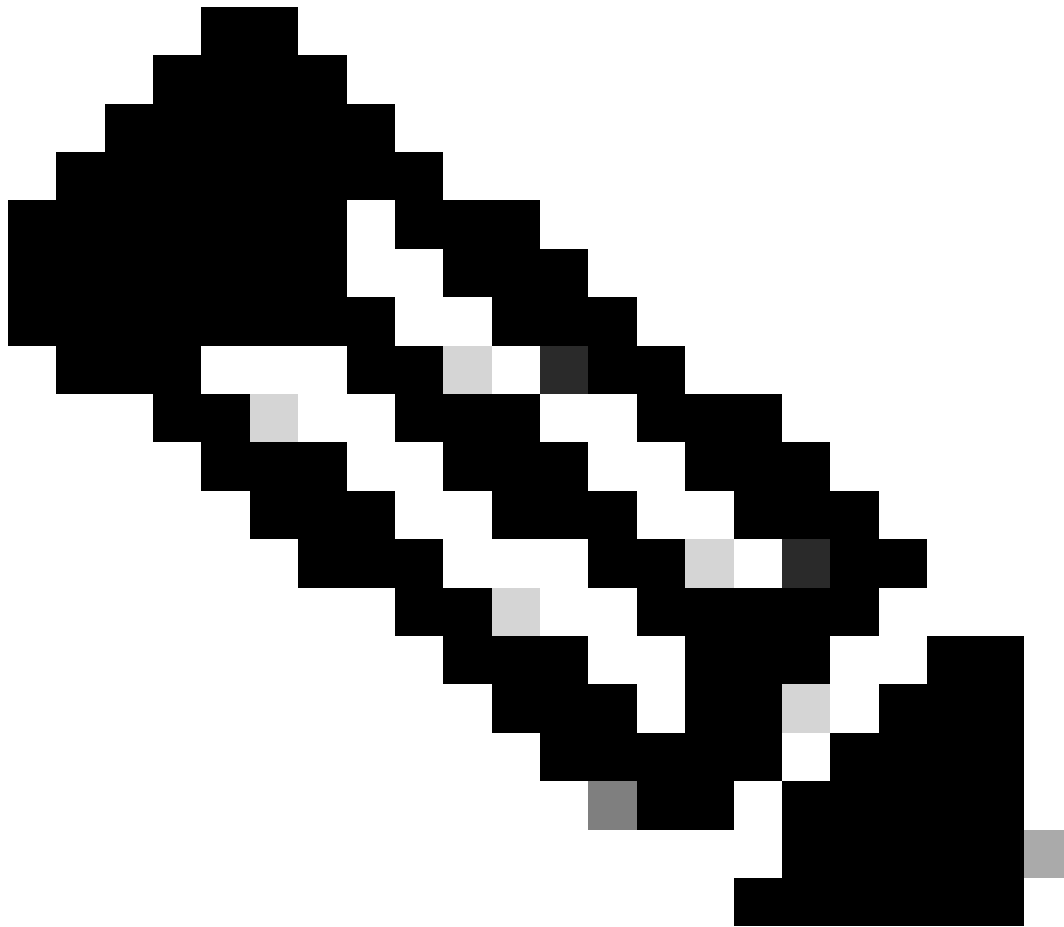
Cancel Update & Apply to Device

WLC Flex配置文件

从 CLI :

```
# configure terminal
```

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



注意：如果WLC在HA-SSO中，则不支持FlexConnect AP上的SGACL。Cisco Bug ID [CSCwn85468](#)。此错误将在17.19中添加。

验证

1. 从ISE，您必须在操作> RADIUS >实时日志下看到成功的CTS请求：

Cisco ISE

Operations · RADIUS

1

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	

ISE RADIUS实时日志

- 您可以验证是否已建立连接，以及是否已从WLC上的Monitoring > General > Trustsec下载SGT:

Search Here

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 16 Items

CTS PACs

A-ID

I-ID

A-ID-INFO

CREDENTIAL LIFETIME

DOWNLOAD STATUS

5498A6284B7C8DC7E1729C0F33A4F68D

9800labWLC

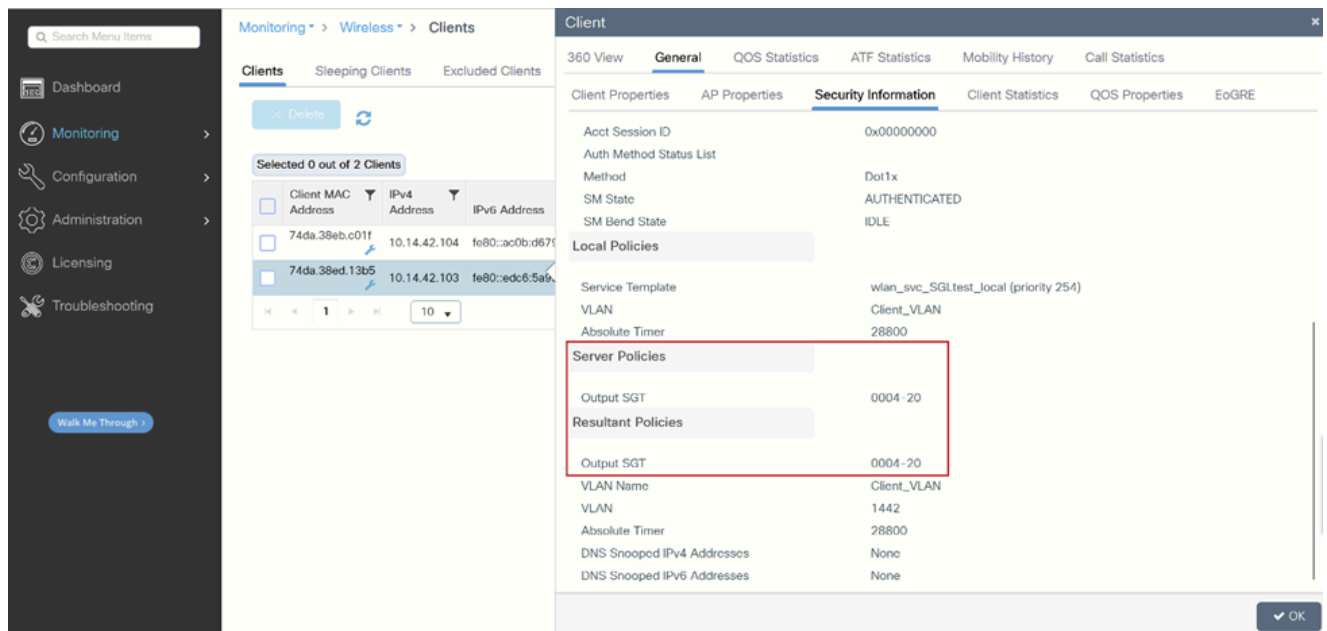
Identity Services Engine

11:13:15 Central Oct 12 2025

completed

WLC TrustSec监控

- 连接客户端时，分配的SGT将在Monitoring > Wireless > Clients下可见，选择您要检查的客户端，然后导航到General > Security information选项卡：



WLC客户端监控

从 CLI :

- 在连接客户端之前，您将从WLC输出中看到以下内容：
仅显示与未知SGT相关的权限。

<#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
```

- 连接客户端时，您可以从[RA跟踪](#)中观察这些日志，SGT从AAA应用：

<#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
```

- 在CLI中使用show wireless client mac-address <client_MAC_address> detail命令，该命令将显示分配给客户端的SGT:

<#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

```

```

...

```

- 在SGT 4中连接一个客户端后，您将注意到SGT 4的权限现在显示：
在客户端连接并分配了SGT之后添加权限。

```

<#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
=====		

- 连接两个客户端后，一个在SGT 4中，另一个在SGT 5中：

<#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
=====	=====	=====

- 现在您可以看到SGT 5的权限已添加：

<#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

- ACL在WLC上将显示为“已下载”：

<#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

```

FlexConnect本地交换

- 这是将客户端连接到AP之前的WLC输出：

<#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

- 在AP CLI中，这是将客户端连接到AP之前的权限输出：

```

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

```

- 以下是客户端连接时显示流的AP调试：

<#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

...

- 在WLC CLI中，连接SGT 4上的一个客户端时：

<#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

- 从AP CLI:
您可以看到相同的情况，仅添加了与SGT 4相关的权限。

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

- 从WLC CLI，当连接SGT 5上的第二个客户端时：

```
<#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

- AP输出：

```
<#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

```

故障排除

- 从WLC CLI:

show cts provisioning

show cts role-based permissions

show ip access-lists

show cts ap sgt-info <ap_name>

- 从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

- 无线接入点调试：
- 启用CTS数据包级别实施调试：

debug cts enforcement

学期星期一

- 要检查CAPWAP ACL事件和负载相关信息，请执行以下操作：

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 sgACL/debug_permission

学期星期一

关于此翻译

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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