Wireless TrustSec Deployment Guide

Revised: October 3, 2024

Introduction

This document introduces Wireless TrustSec feature and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of Wireless TrustSec feature
- Highlight supported Key Features
- Provide details on deploying and managing Wireless TrustSec on WLC

The focus of this guide is only on Wireless TrustSec features.

For deep dive on wired TrustSec, please refer to the following:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/design-guide-listing.html

Pre-requisite

Customers must have AireOS 8.0 or higher release on a Wireless LAN Controller in order to upgrade to the 8.4 code.

Requirements

There is no specific requirement for this document.

Components Used

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

Conventions

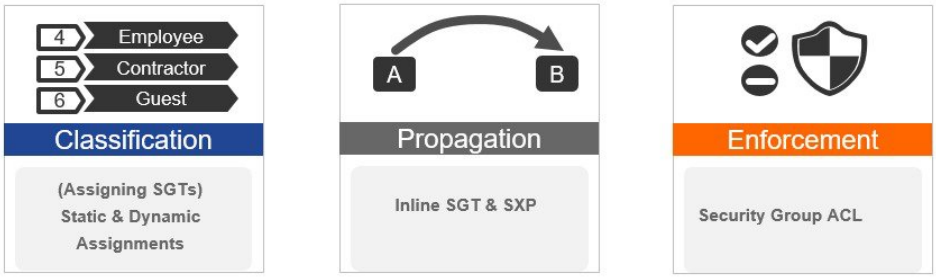
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Feature Overview

The Cisco TrustSec (CTS) architecture provides an end-to-end secure network where each entity is authenticated and trusted by its neighbors and communication links secured that help ensure data confidentiality, authenticity and integrity protection. In addition, CTS facilitates to create a consistent and unified set of policies across network. The following sections describe specific aspects related to CTS infrastructure support on AireOS WLC platforms.

Implementation

Figure 1: Wireless TrustSec Solution



Every end point that touches the TrustSec domain gets classified by ISE based on end user identity like role, device-type (other client attributes) and is associated with a unique tag called SGT(Security Group Tag) that is then shared with the device that requested the client authentication upon successful authentication. This allows grouping of clients based on client identity attributes thereby reducing the number of Access Control Entities (ACE) considerably. A major benefit to SGACL use is the consolidation of access ACEs and the operational savings involved with maintenance of those traditional access lists.

Trustsec solution is realized across the following three distinct phases within TrustSec domain:

- **Client classification** at ingress by a centralized policy database (ISE) and assigning unique SGT to client based on client identity attributes like role and so on.
- **Propagation** of IP to SGT binding to neighboring devices using SXPv4 and / or inline tagging methods.
- **SGACL policy enforcement**: AP will be enforcement point for central / local switching (central authentication).

SXPv4 on AP

WLC still supports SXPv2 Speaker mode to propagate IP to SGT bindings to neighboring devices, we don't support SXPv4. AP will support SXPv4 listener and speaker mode.

CTS PAC Provisioning and Device Enrollment

Any device that participates in the CTS network requires it to be authenticated and trusted. In order to facilitate the authentication process new devices connected to CTS network under goes an enrollment process where in the device obtains the credentials that is specifically needed for CTS device authentication and obtain general CTS environment information.

The WLC device enrollment is initiated by the WLC as part of PAC provisioning with ISE server. The WLC will initiate EAP-FAST and obtains a PAC. This is accomplished by using the infrastructure of LOCAL-EAP EAP-FAST PAC-provisioning. The PAC obtained uniquely maps to the Device ID. If the Device ID changes, PAC data associated with the previous Device ID is removed from the PAC store. PAC provisioning is triggered when a radius server instance is enabled to provision the PAC.

In case of High Availability (HA) setup, PACs will be synced to the standby box.

Environment Data

CTS Environment data is a set of information or attributes that helps the device to perform CTS related functions.

The device (AirOS WLC) acquires the environment data from the authentication server when the device first joins a Cisco Trust Sec domain by sending a secure radius access-request. The authentication server returns RADIUS Access-Accept with attributes including

environment expiry timeout attributes. This is the time interval that controls how often the Cisco Trust Sec device must refresh its environment data.

Inline Tagging

Inline tagging functionality is a transport mechanism by which a wireless controller or an access point understand the source SGT (S-SGT). It covers the following two types:

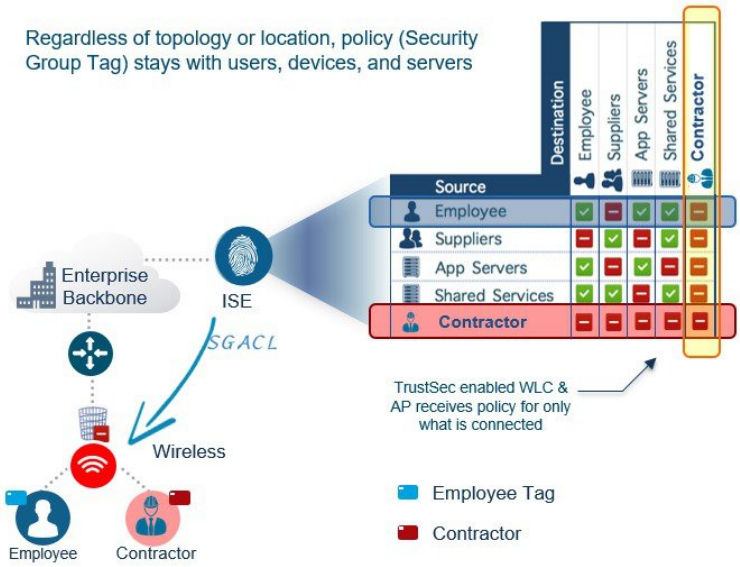
- **Central switching**: For centrally switched packets, WLC performs inline tagging for all packets sourced from wireless clients that reside on the WLC by tagging it with Cisco Meta Data (CMD) tag. For packets inbound from the DS, inline tagging also involves WLC will strip the packet of the header and send it to the AP over CAPWAP for the AP to learn the S-SGT tag. SGACL enforcement will happen at the AP.
- **Local switching**: For transmitting ,locally switched traffic AP performs inline tagging for packets sourced from clients that reside on the AP. When receiving traffic, AP will handle both locally switched and centrally switched packets and use S-SGT tag for packets and apply the SGACL policy.

With wireless TrustSec enabled on WLC the choice of also enabling and configuring SXP to exchange tags with the switches is optional and both modes i.e. SXP speaker mode and inline tagging are supported; however there is no use case to have both SXP and wireless TrustSec on AP to be enabled simultaneously

Workflow

Before a WLC can start downloading SGACL policies from ISE, it must initiate PAC (Protected Access Credential) provisioning over an EAP-FAST TLS tunnel. This will be used to download SGACL as required, based on authenticated client SGT tag. Currently, ISE supports SGACL policy download for given destination SGT (D-SGT) from all known source SGT (S-SGT). When a wireless client is authenticated by ISE, WLC receives a SGT associated with the client. WLC will treat client SGT as D-SGT and initiate download of SGACL policy names for the destination from ISE. The policy names returned will be all possible / known S-SGTs paired with the specific client D-SGT. These policies associated with the D-SGT are cached on WLC and pushed to the AP associated with the client.

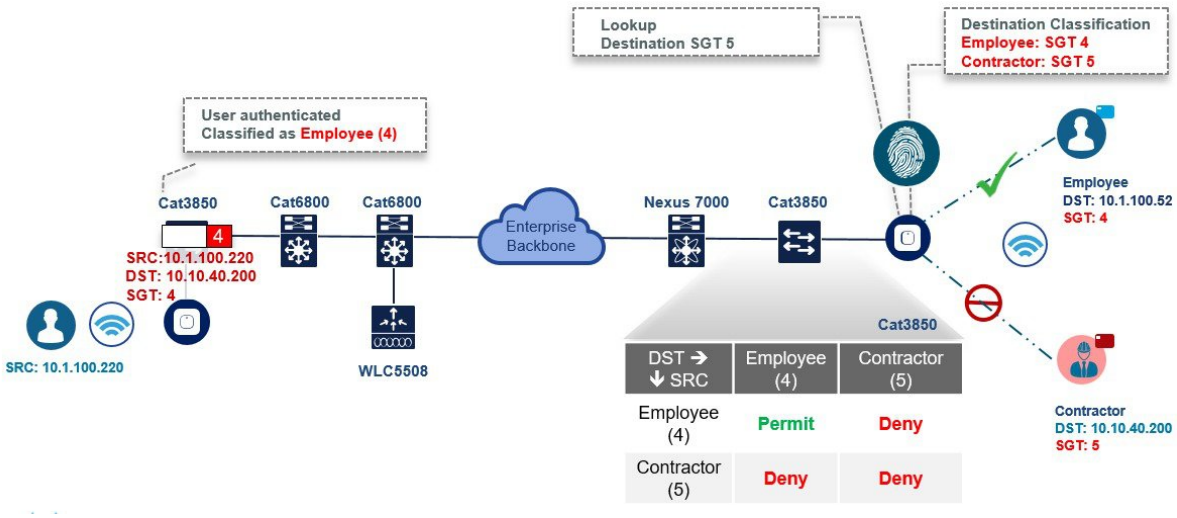
Figure 2: Simplified ACL management for Inter/Intra VLAN traffic



Client classification happens at ingress by centralized policy database (ISE) that assigns a unique S- SGT to client based on client identity as per policy rules. SGACL download and policy is enforced (associated with the D-SGT) on the egress side.

- SGACL enforcement for local and central switched traffic happens on AP and not on WLC.
- In a flex mode AP doing local authentication, enforcement point will be the AP.

Figure 3: Ingress Classification, Egress enforcement



Wireless TrustSec Support on WLC 8.4

Feature	Platform
Inline SGT tagging and SG-ACL enforcement	17xx, 27xx,37xx, 18xx, 28xx, 38xx, 5520 and 8540
SXPv2	5520, 8540, 8510, 7510, vWLC, 5508, WISM2, 2504
SXPv4	17xx, 27xx,37xx, 18xx, 28xx and 38xx

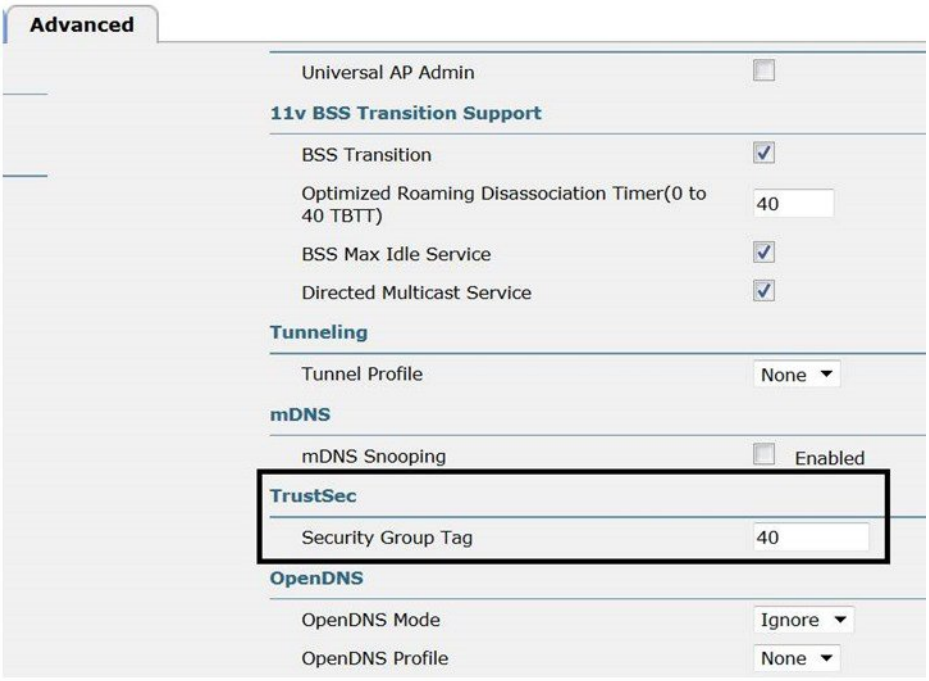
Use case for Wireless TrustSec Deployment

The configuration example below demonstrates a simple use case when clients with different roles (employee and contractor) connect to the same WLAN (single SSID) and obtain IP address from a same VLAN but inherit different SGT tags from ISE. Furthermore, we will create a policy on ISE which blocks communication between these two user groups (employee and contractor) over wireless. In this process, you will understand how to configure ISE and the WLC for Cisco Wireless TrustSec.

ISE is the central point for all TrustSec configurations that include the following:

- Defining NDAC (Network Device Admission Control) for trusted domain of network devices.
- Centrally defining SGT (Security Group Tag).
- SGACL / Name table: TrustSec policy matrix to be pushed down to the enforcers through secure channel.
- ISE authenticates Wired/Wireless/VPN clients and assigns SGTs.

Clients that are not authenticating through ISE (open/webauth/PSK) can be configured for a SGT tag on the WLCs as shown below by navigating through the **WLAN** > **Advanced** setting.



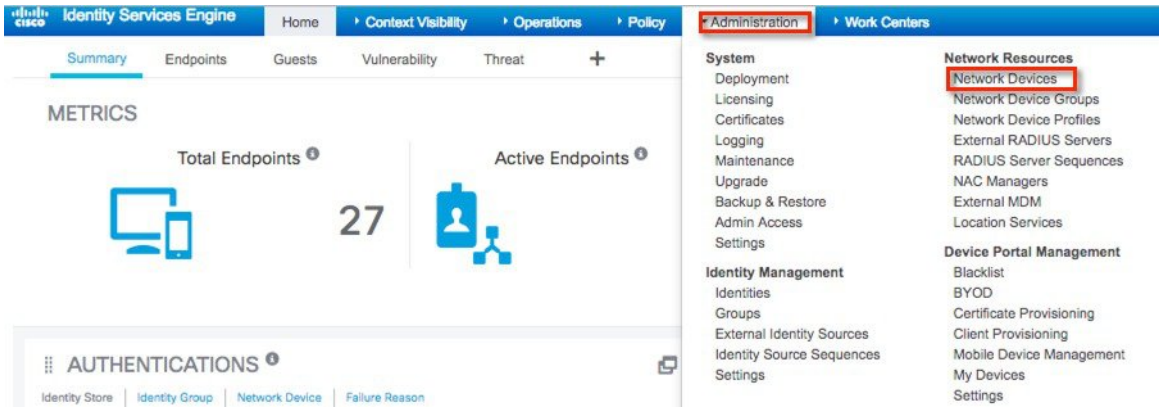
Wireless TrustSec Configuration Checklist (Reference)

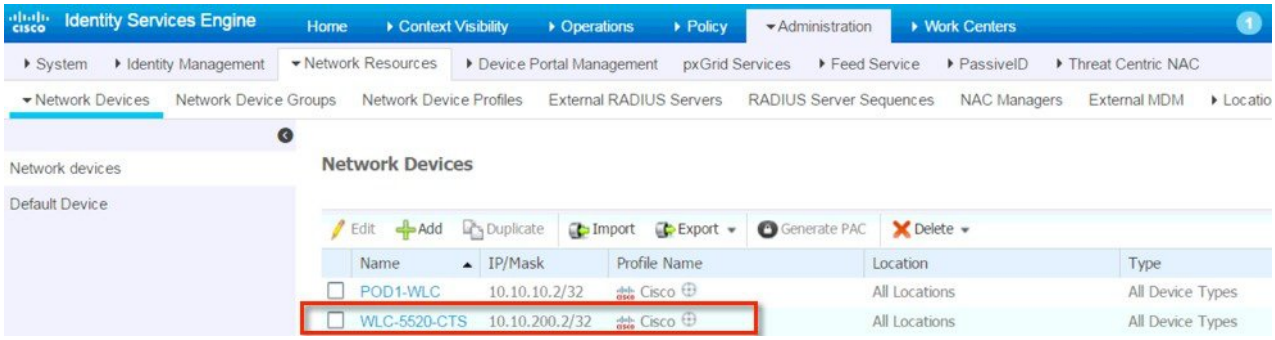
- *Basic Infrastructure setup*: Certificates, Active Directory integration and so on.
- Create Security Group Tags to be used in the network.
- Setup Network Device Admission Control (NDAC).
- Define Authentication and Authorization policies for users and devices.
- Configure SGACL and Egress Policies.

Configuration Steps

The following procedure shows ISE configuration for adding device:

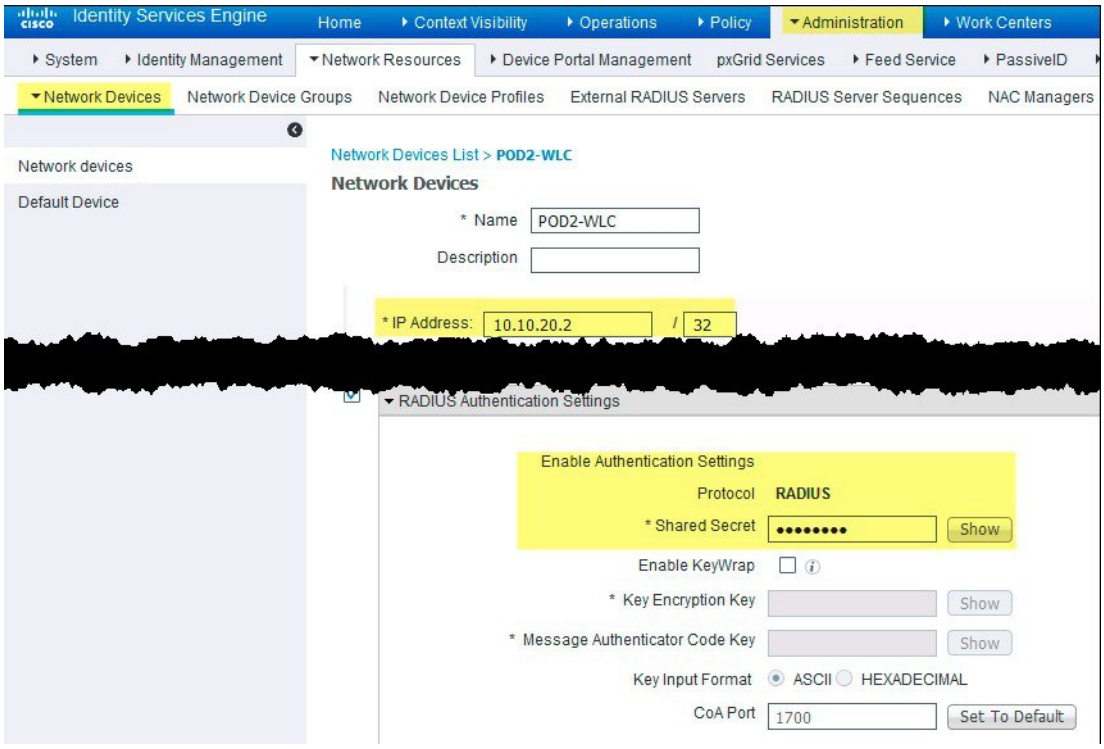
1. Verify WLC is added to ISE for Radius and TrustSec. Go to **Administration** > **Network Resources** > **Network Devices** from ISE main menu.



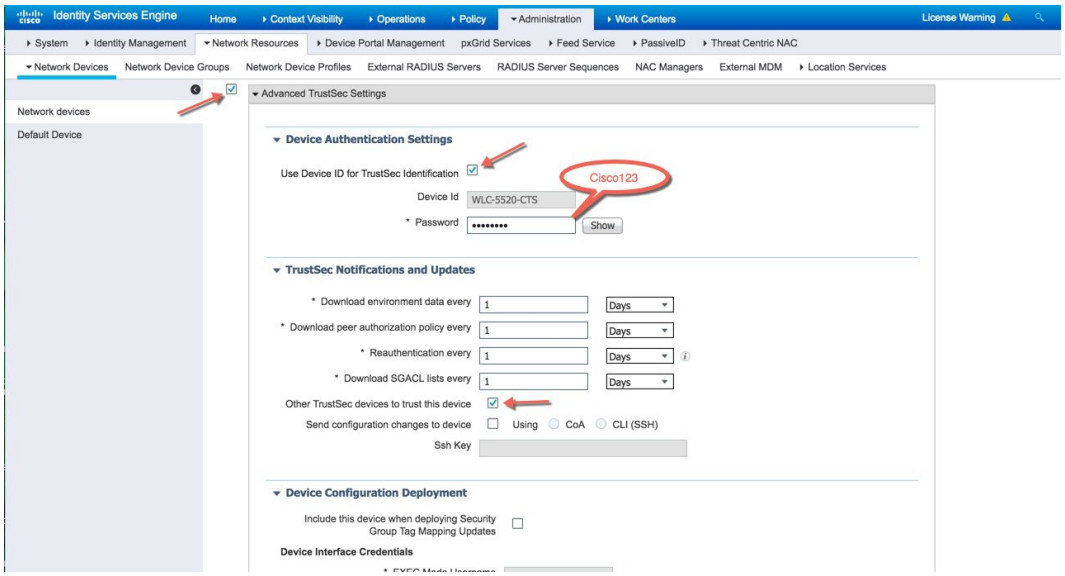


We have pre-configured the Network Device page with the following inputs:

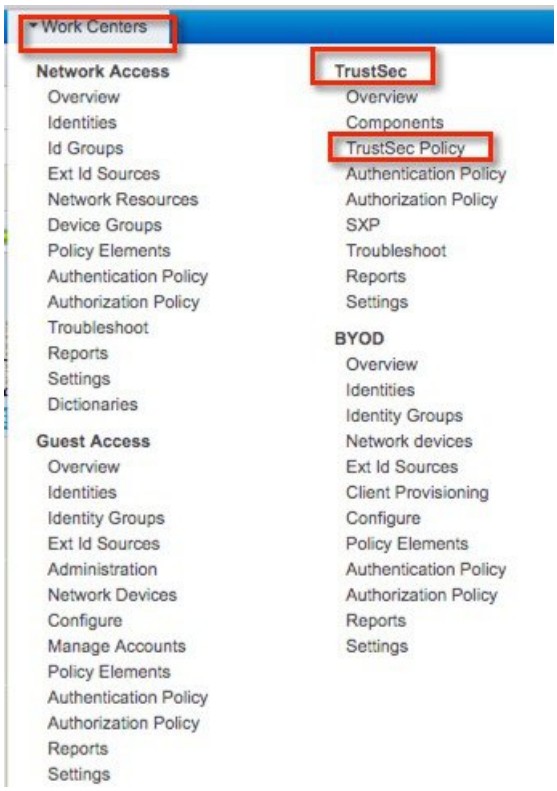
- WLC Name
- IP Address of WLC
- Enabled Radius Authentication Settings by checking the box
- Shared secret
- Enabled Advance TrustSec Settings > Identification by checking the box for use Device ID
- Under Device Authentication Settings, configured password



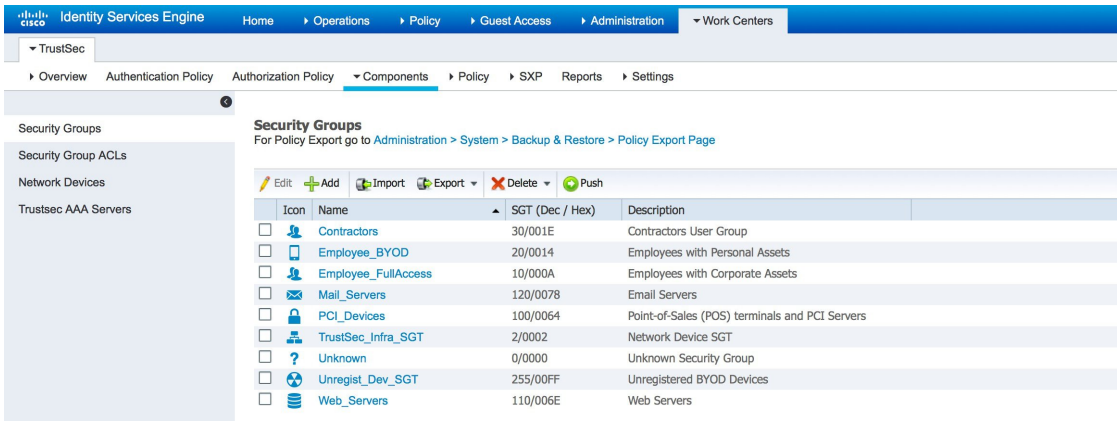
Any device that participates in the CTS network requires it to be authenticated and trusted. In order to facilitate the authentication process new devices connected to CTS network under goes an enrollment process where in the device obtains the credentials that is specifically needed for CTS device authentication and obtain general CTS environment information



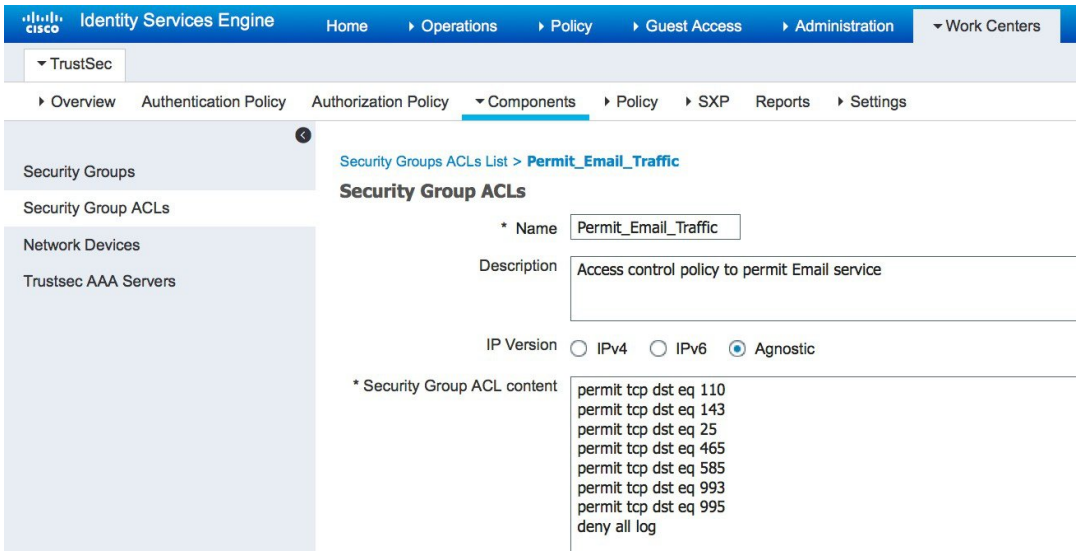
2. For ISE TrustSec Policy Configuration, go to **Work Centers > TrustSec** from ISE main menu.



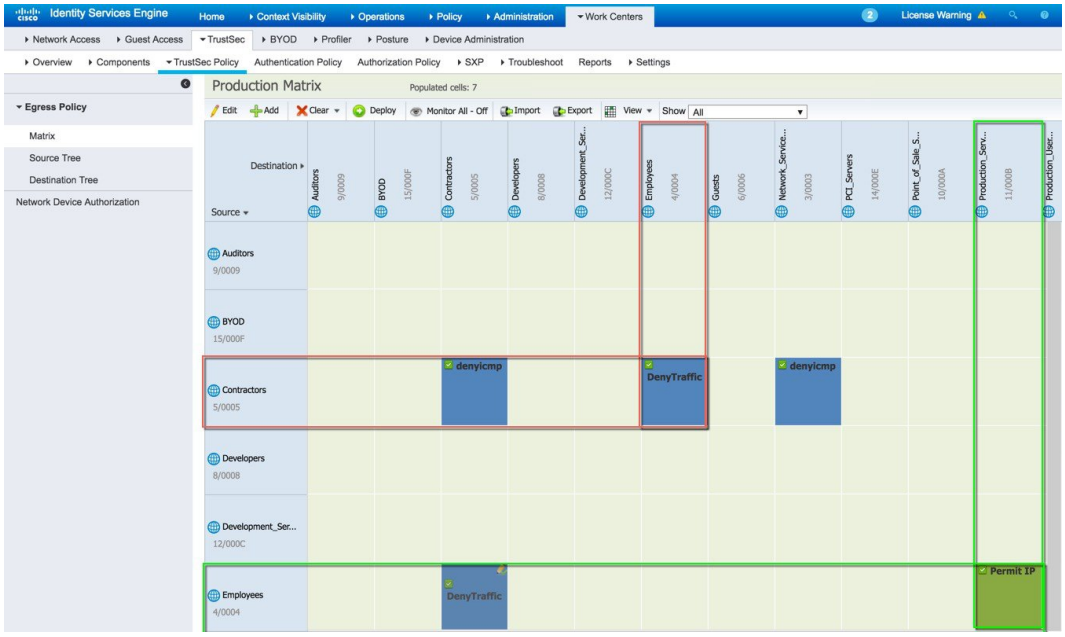
3. Under **Work Centers>TrustSec> Components**, Security Groups and the associated SGT are listed.



4. To create a SGACL, go to **TrustSec > Components > Security Group ACLs.** Example on how to configure a SGACL is shown below:



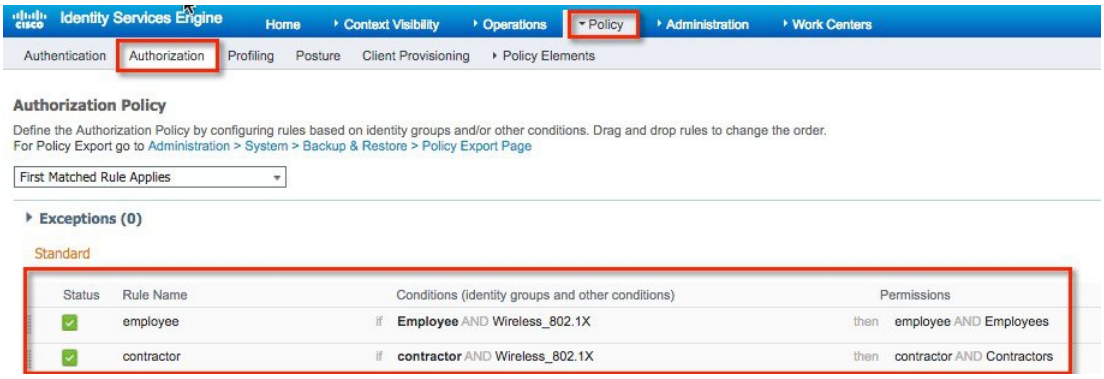
5. Go to **Work Centers>TrustSec>TrustSec Policy** and view the created policies. We have configured a policy to deny employee and contractor from communicating with each other. Notice that the employee tag is 4 and contractor tag is 5. These tags will be inherited by clients once they associate to the WLAN.



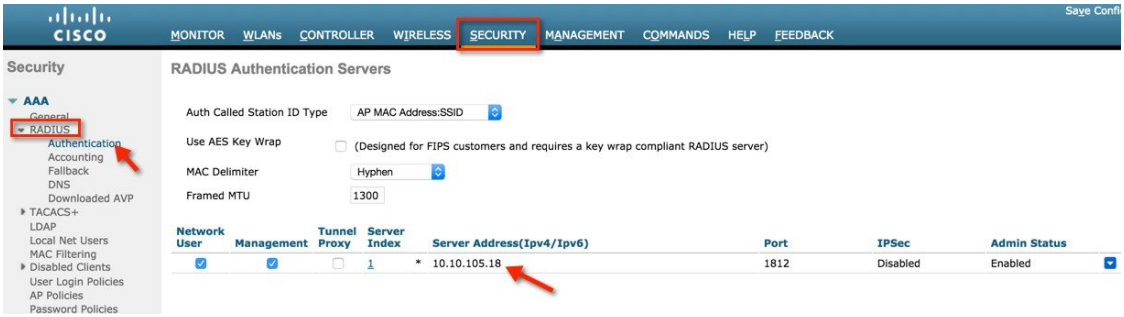
Default Rule can be Permit or Deny

Following is the SGACL configuration to deny rule:

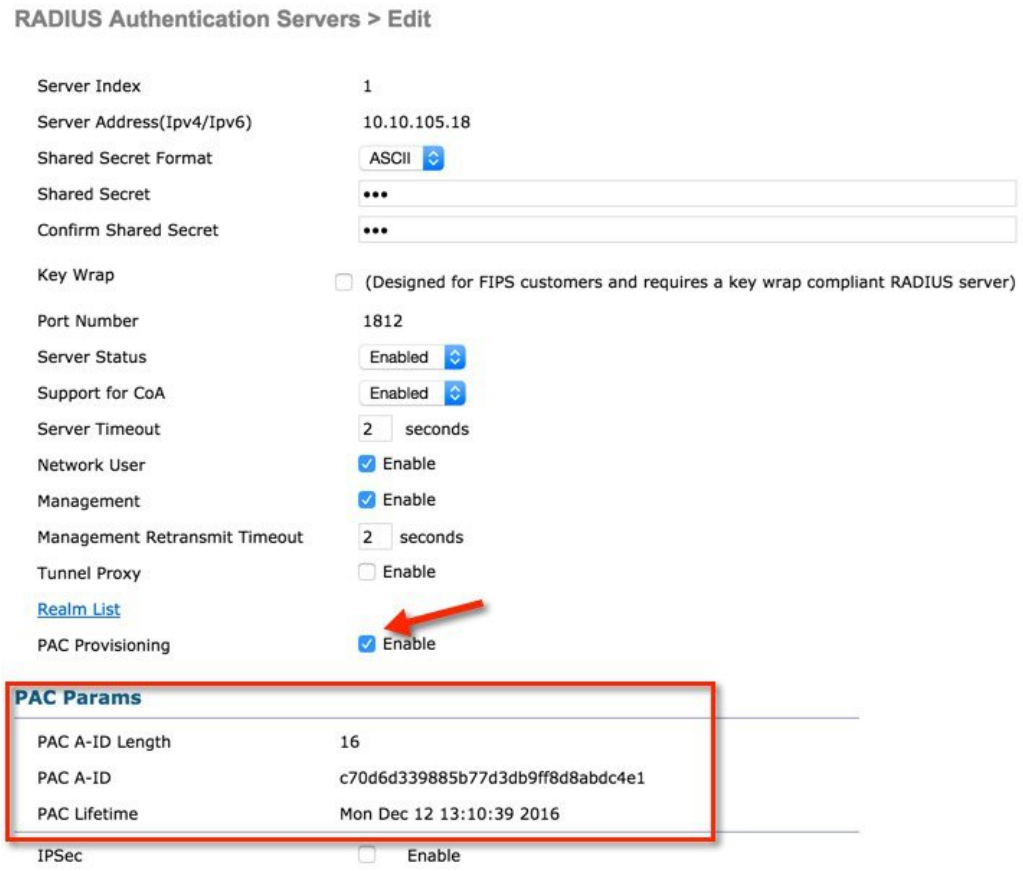
6. Also, under **Policy > Authorization** we have configured Authorization rules for employee and contractor to pass the tags once the clients get authenticated.



7. For integrating Wireless LAN Controller with ISE, go to **Security >RADIUS>Authentication** from WLC GUI main menu and verify that ISE server is added.

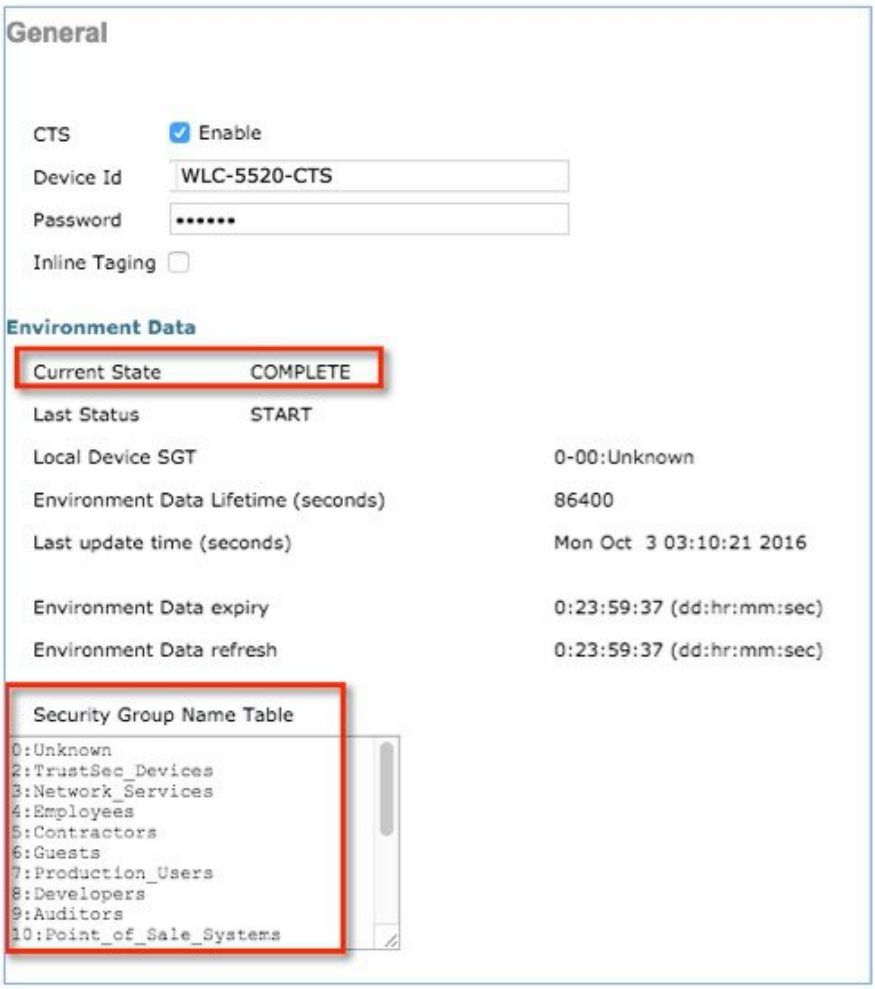


8. Click on server index for ISE and verify that PAC Provisioning is 'Enabled' and the PAC parameters are downloaded from ISE.



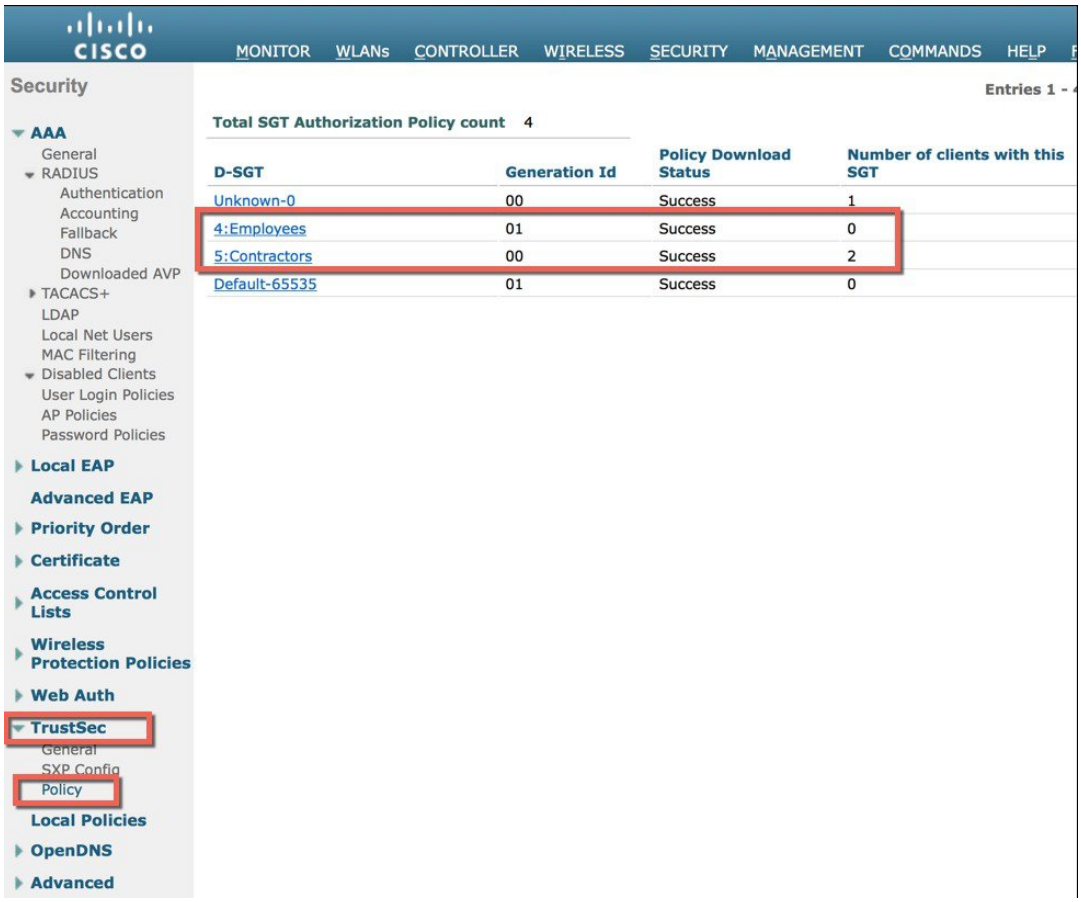
9. Verify the following from **Security > TrustSec > General:**

- CTS is Enabled
- Configure Device ID
- Password is configured the same as on ISE
- Current Status shows Complete
- Security Group Table should be populated

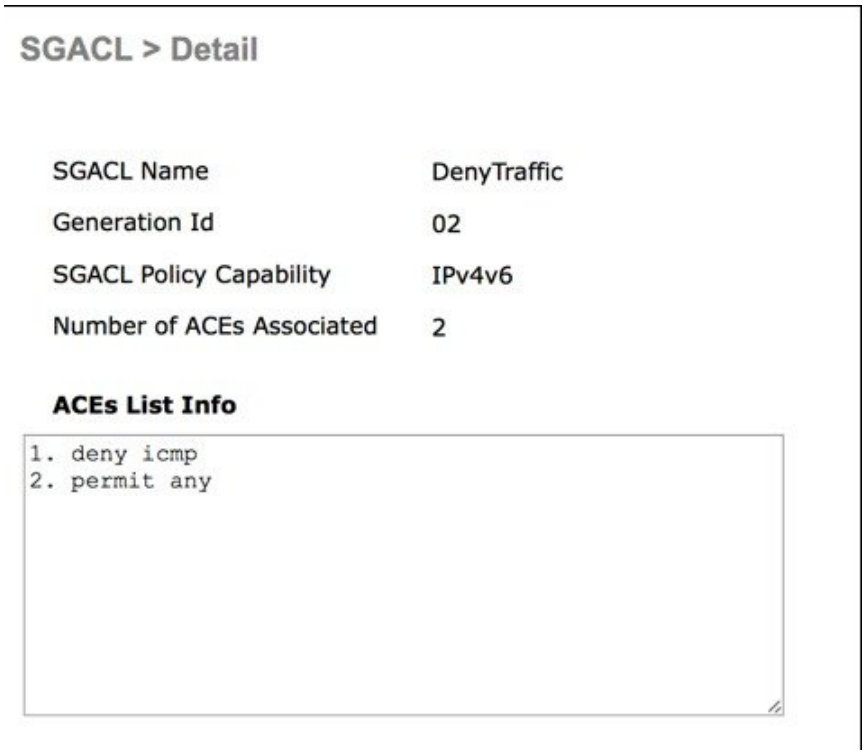


10. Navigate to **SECURITY** > **TrustSec** > **Policy** and verify the SGT-TAG list to see that the policy is downloaded on the WLC.

Note In order for the SGT-TAG list to populate on the Wireless LAN Controller (WLC), a client must first connect with the targ
SGT. Once the client is connected, the WLC will pull the SGT-TAG list and install it, similar to the process on the wired sid
Ensure that a client connection is established to trigger this synchronisation.



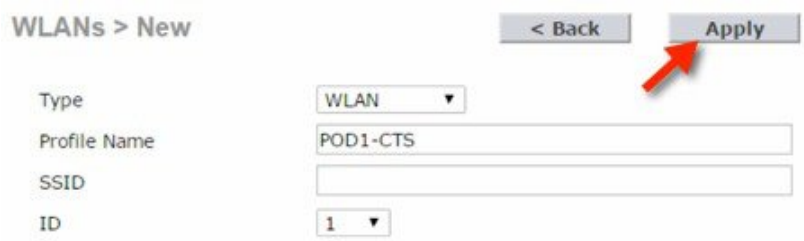
Drill down the Policy and you can see the SGACL:



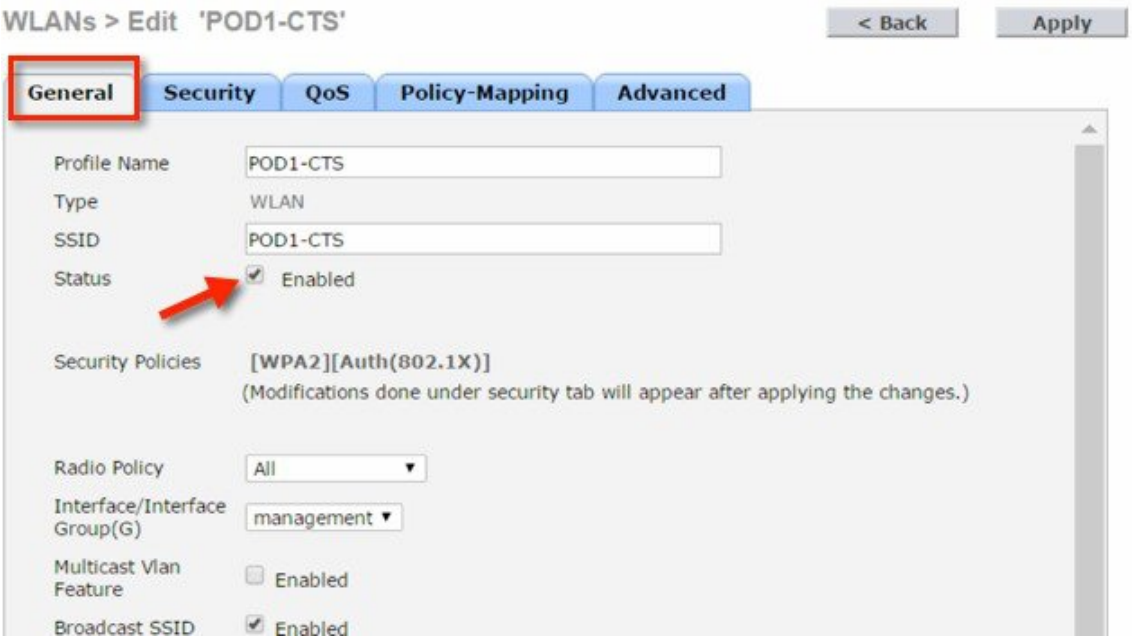
You can drill down further to see the ACEs per SGACL:

11. To configure WLANs on WLC, Select Create New from WLANs and click **Go**.

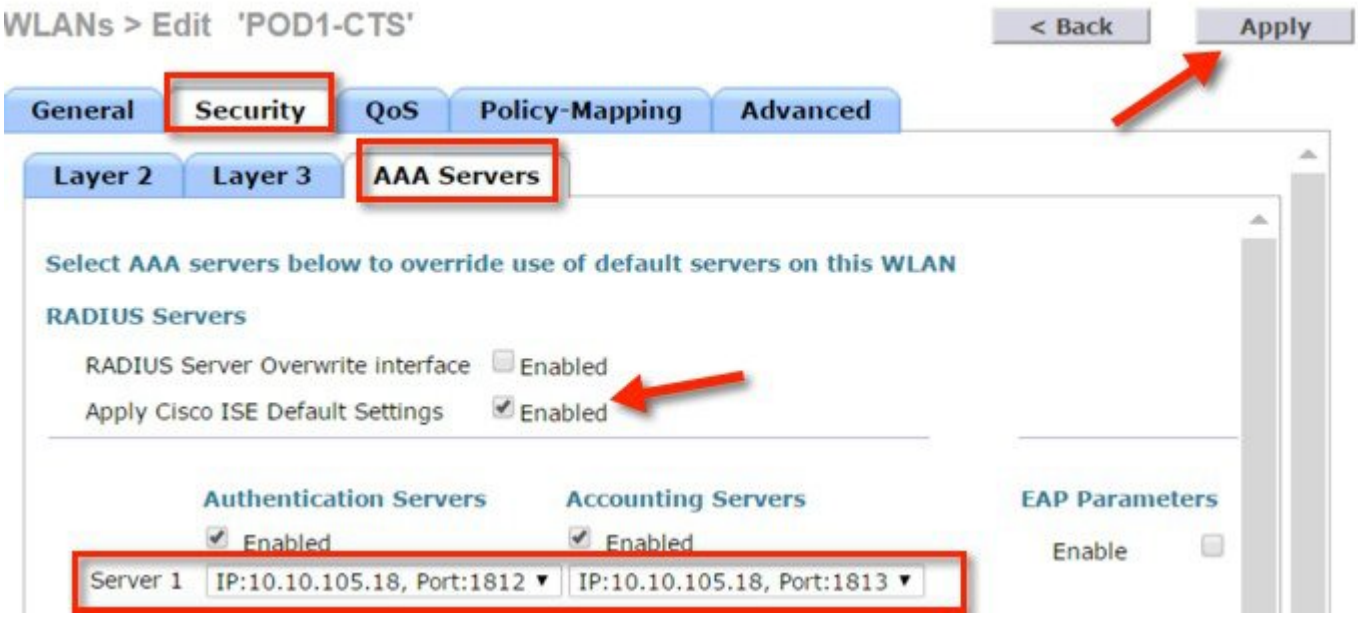
Set the profile name as POD1-CTS and click **Apply**.



From General Tab, **Enable** the WLAN.

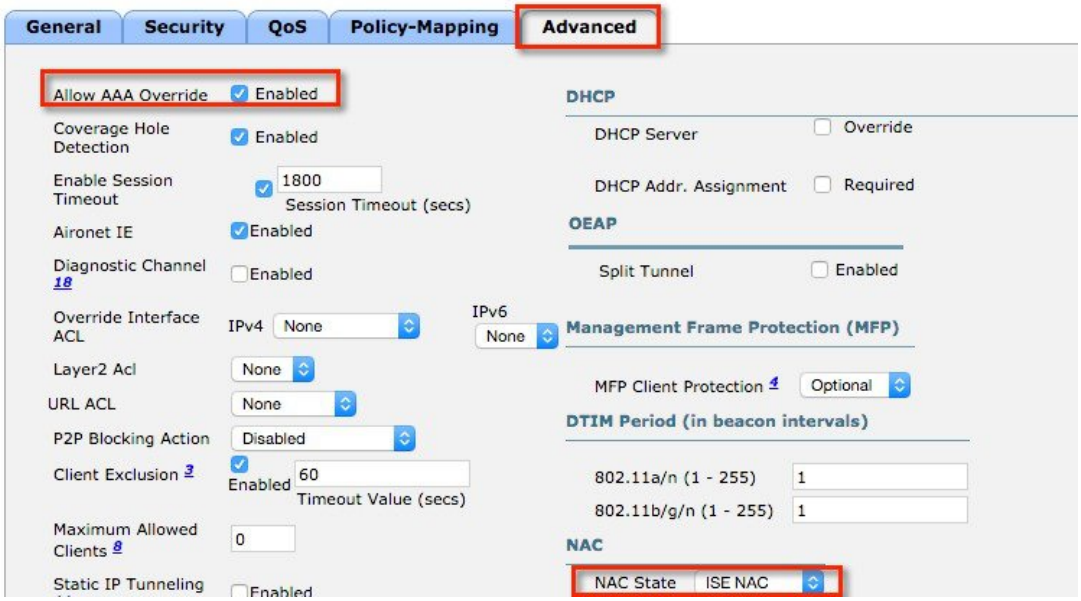


12. From **Security** > **AAA Servers**, select the AAA server which is configured above and click**Apply**.



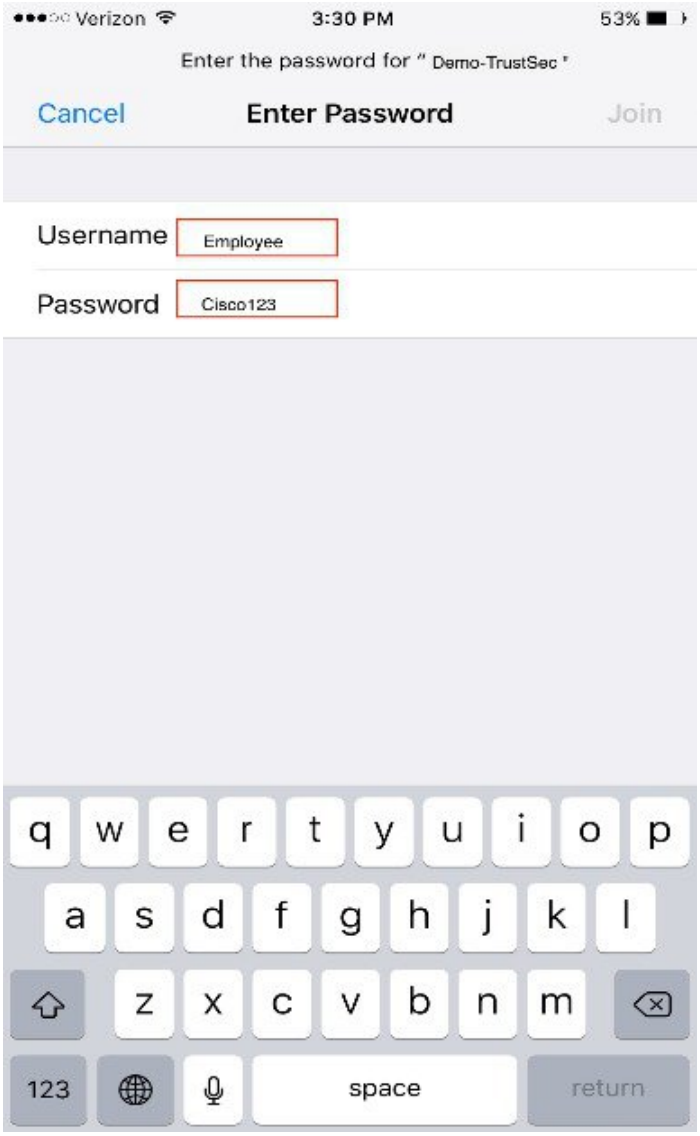
13. Once you enable ISE default settings, the WLC automatically configures the following settings on the WLAN advance tab:

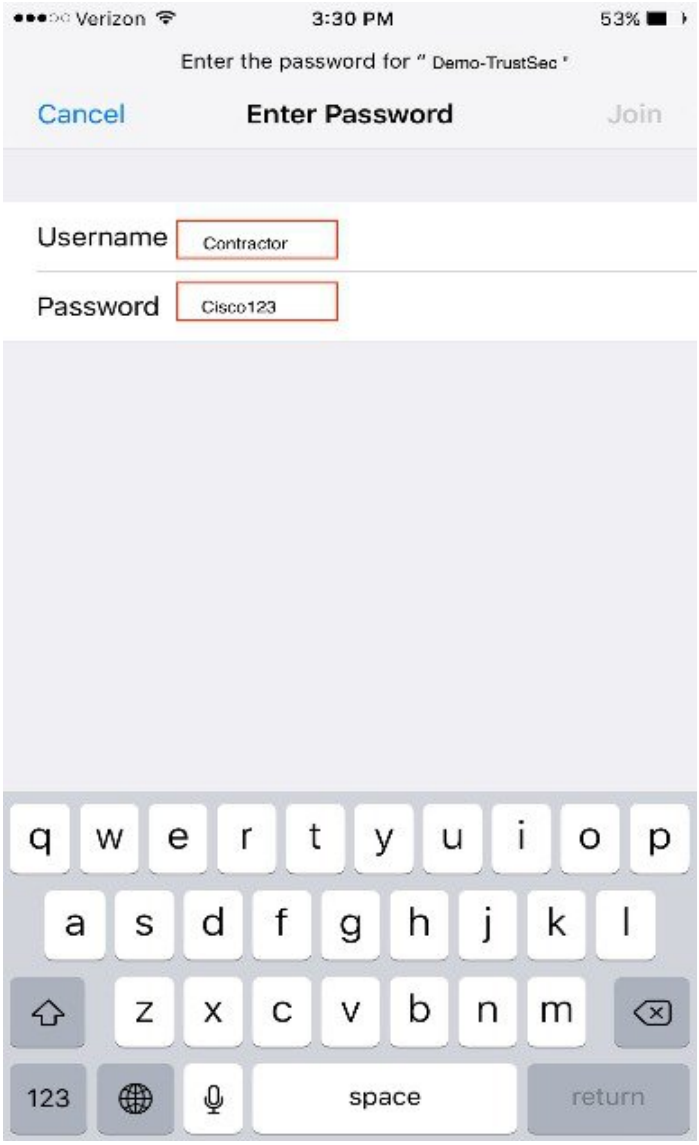
- Allow AAA override=Enabled



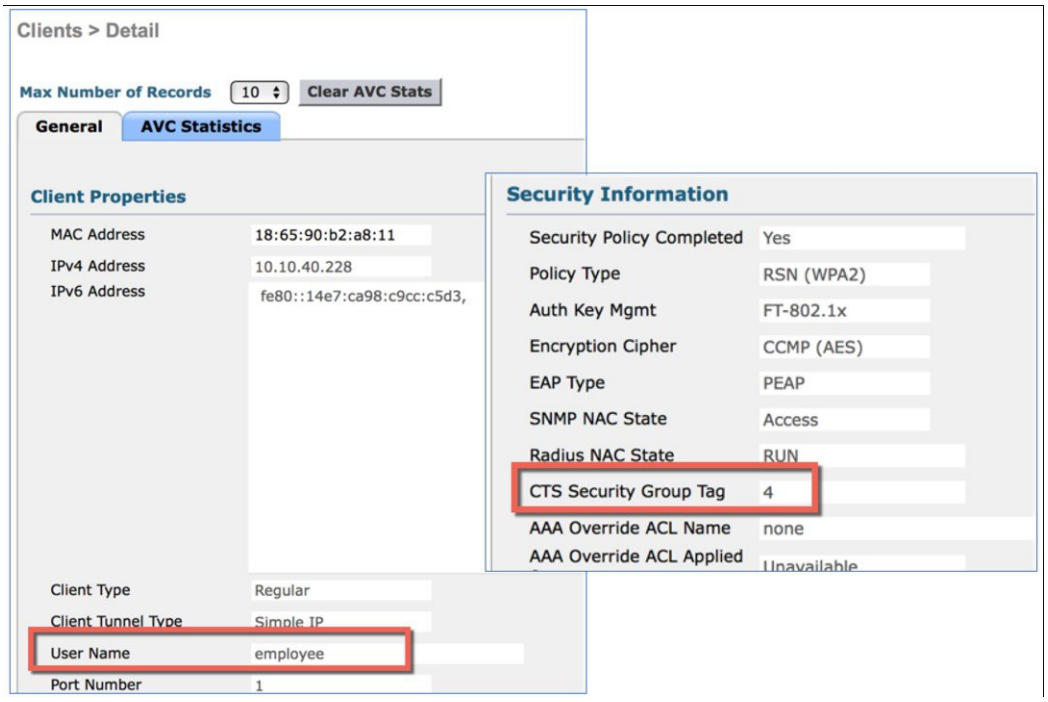
14. To test with client traffic without enforcing SGACL on the AP, follow the below steps:

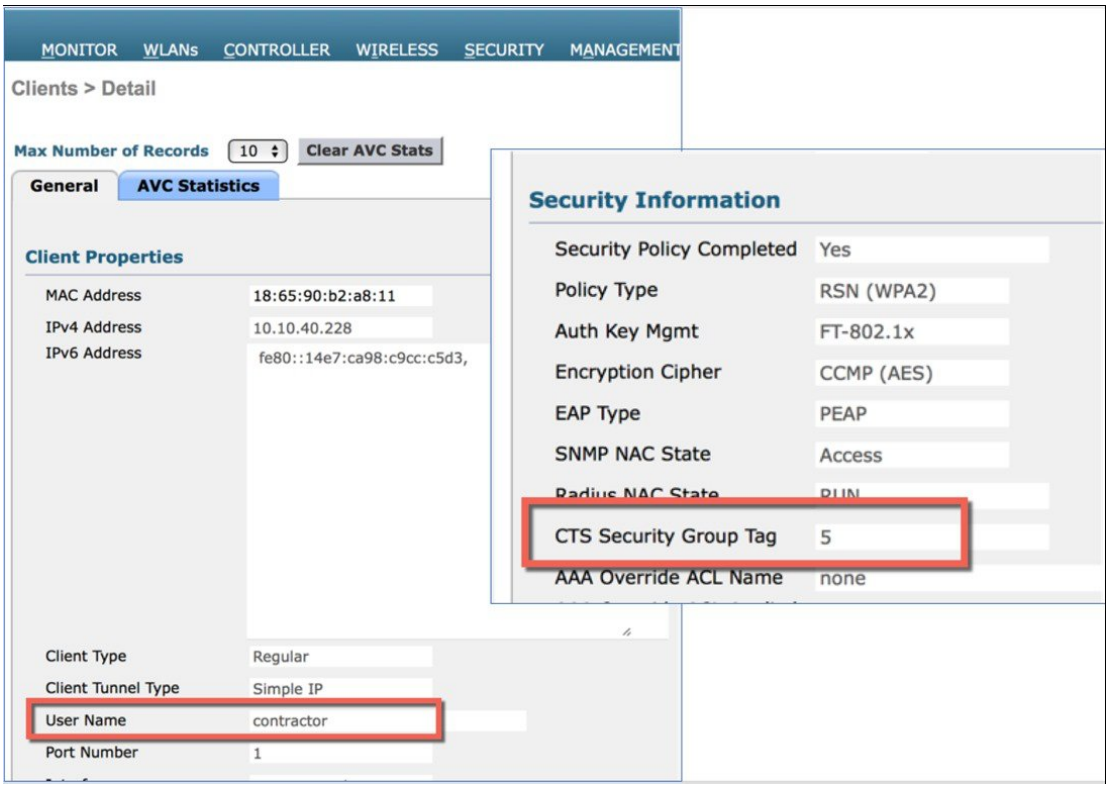
a. Using your client devices, log in as an employee from one client and as a contractor from a different client.


Verizon
3:30 PM
53%
Enter the password for " Demo-TrustSec "
Cancel
Enter Password
Join
Username
Employee
Password
Cisco123
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
return



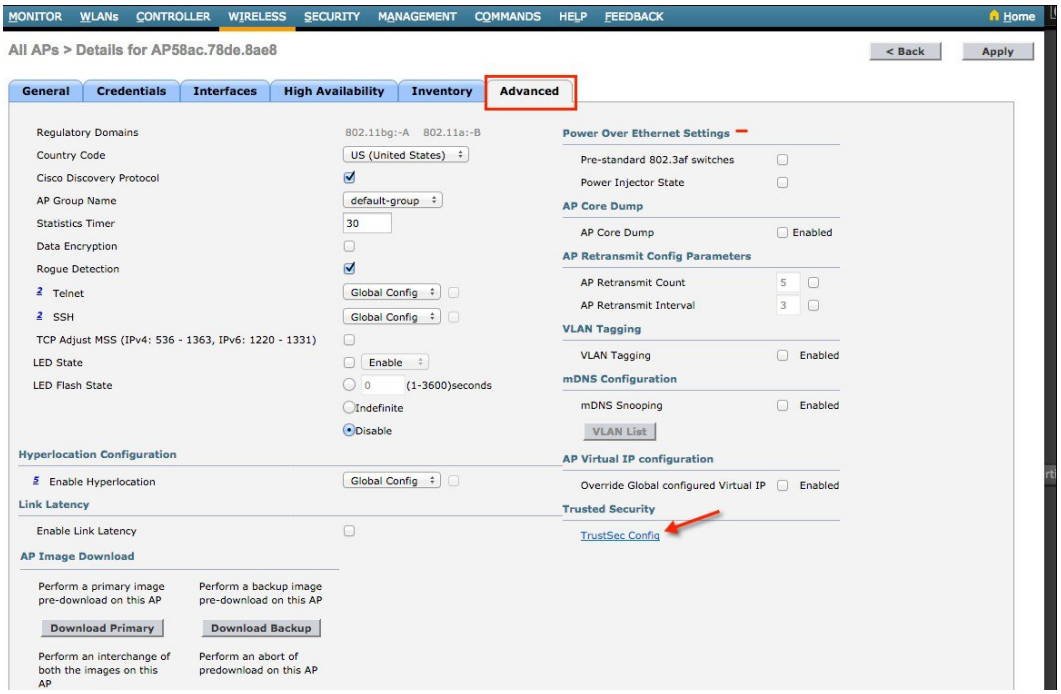
b. From the WLC page, check client details under **Monitor** > **Clients** for both users and SGT security tag pushed on both.

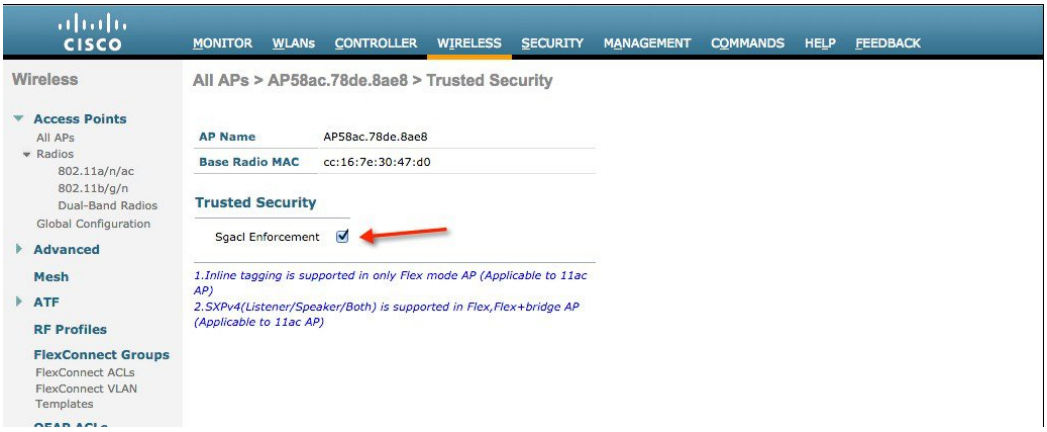




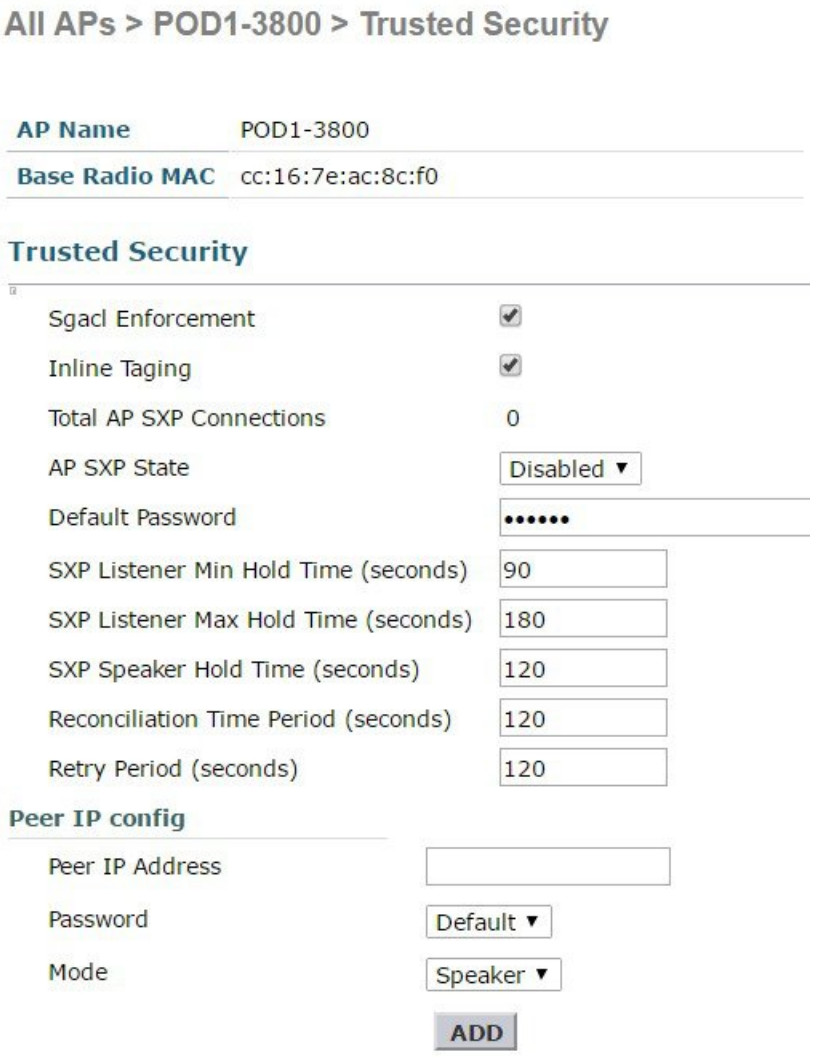
c. To test applications per SGACL, use one device to connect as an employee and other device as a contractor, and make sure that both clients can ping each other. Below is an example of ICMP communication from Contractor device to an employee device (IP: 10.10.40.200).

15. **a.** To enable TrustSec enforcement on a local mode AP, navigate to **Wireless tab** > **Select an Access point** > **Advanced** tab and enforce SGACL as shown below.





b. To add SXP or inline config on a Flexconnect AP, go to **Wireless** > **AP** > **Advanced** > **Trusted Security** > **TrustSec Config**.



16. After enforcing "TrustSec" on AP, you should not be able to ping between the two clients (employee and contractor) as shown below.

CLI Commands for Wireless TrustSec Configuration

1. PAC download on WLC

```
# config radius auth pac <server-index> enable
# config radius acct pac <server-index> enable
```

It enables the CTS PAC download on the server.

```
# config cts device-id <device-id> password <pwd>
```

Configures the CTS device ID and Password to be used during initial PAC download.

```
# show cts pacs
```

To check PAC download status on WLC.

```
# clear cts pac <A-ID>
```

To clear the PAC.

2. **Inline tagging**

CLI commands on WLC:

```
# config cts inline tagging {enable | disable}
# show cts summary
```

CLI command on AP:

```
#config cts inline-tag (enable|disable)
# show cts ap summary
# show ap config general
#config cts ap inline-tagging {enable | disable} <apname/all>
```

3. **SXPv4**

```
# config cts sxpv ap {ap name} enable/disable
# show cts ap summary
# show ap config general
#config sxp ap enable/disable <ap_name/all>
#config cts sxp ap connection default password <passwd> <ap/all>
#config cts sxp ap connection peer <ipaddr> password [default | none] mode [speaker | listener | both]
<ap/all>
#config cts sxp ap listener holdtime <min> <max> <ap-name/all>
#config cts sxp ap speaker holdtime <secs> <ap-name/all>
#config cts sxp ap reconciliation period <secs> <ap-name/all>
#config cts sxp ap retry period <val> <ap_name/all>
```

4. Debug

Available debug options:

```
#debug cts ?
aaa             Configure the CTS AAA debug options.
authz           Configures the CTS SXP debug options.
capwap          Debugs for CTS policy download over capwap messages
env-data        Configure the CTS environment data debugs.
ha              Configure the CTS HA debug options.
key-store       Configure the CTS Key-store debug options.
provisioning    Configure the CTS PAC Provisioning debug options.
sxp             Configures the CTS SXP debug options.
```

5. Show commands on AP

Note There are difference in commands for different AP platforms.

11AC wave1 and earlier APs (17xx, 27xx, 37xx):

SXPv4:

```
#sh ct sxp connections brief
```

to check connections

```
# sh ct sxp sgt-map brief
```

to check SXP bindings

```
# sh ct role-based sgt-map all
```

to check IP-SGT binding for local switching ONLY.

```
# sh controllers dot11Radio 1 | beg SG
```

to check SGT for central switching clients

Check SGALC:

```
#sh ct role permissions ?
    default  Default Permission list
    from     Source Group
    ipv4     Protocol Version - IPv4
    ipv6     Protocol Version - IPv6
    to       Destination Group
    |        Output modifiers
    <cr>
sh access-lists <name>
```

Debug:

```
#debug rbm dp packets.
  #sh cts role-based counters ?
  default  Default policy counters
  from     Source Group
  ipv4     Protocol Version - IPv4
  ipv6     Protocol Version - IPv6
  to       Destination Group
  |        Output modifiers
  <cr>
```

Wave2 APs (18xx,28xx, 38xx):

SXP:

```
#sh ct sxp connections
```

to check connections

```
#sh ct sxp sgt-map
```

to check SXP bindings

```
# sh ct role-based sgt-map all
```

to check IP-SGT binding (for both central and local switching only)

Check SGALCs:

```
#sh cts role-based permissions
#sh cts access-lists <name>
```

Debug:

```
#debug ct enforcement
#sh cts role-based counters
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.