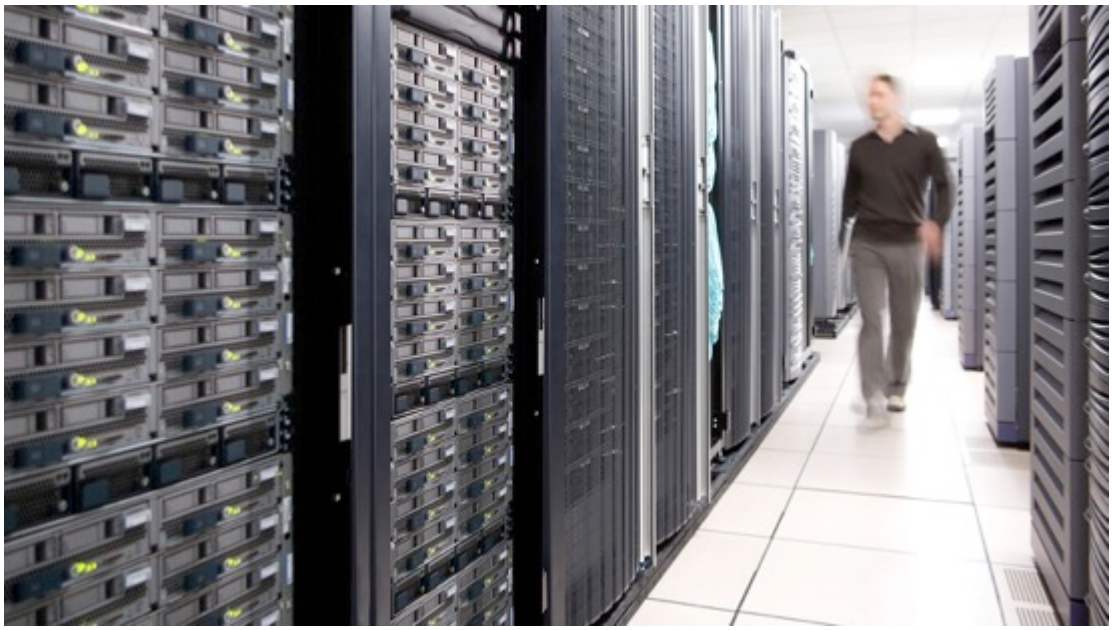


TrustSec Configuration Guides

TrustSec Capabilities on Wireless 8.4

Software-Defined Segmentation through SGACL Enforcement on Wireless Access Points

TrustSec
Software-Defined
Segmentation

Table of Contents

TrustSec Capabilities on Wireless 8.4

Introduction

Cisco TrustSec (TrustSec) provides software-defined segmentation to reduce the risk of malware propagation, simplify security operations, and assist in meeting compliance goals. With TrustSec, controls are defined simply using endpoint roles, not IP addresses. By classifying systems using human-friendly logical groups, security rules can be defined using these groups, which are more flexible and much easier to manage than using IP address-based controls. IP addresses do not indicate the role of a system, the type of application a server hosts, the purpose of an IoT device or the threat-state of a system, but a TrustSec Security Group can denote any of these roles. These security groups can be used to simplify firewall rules, web security appliance policies and the access control lists used in switches, WLAN controllers and routers. This can simplify provisioning and management of network access, make security operations more efficient, and help to enforce segmentation policy consistently, anywhere in the network.

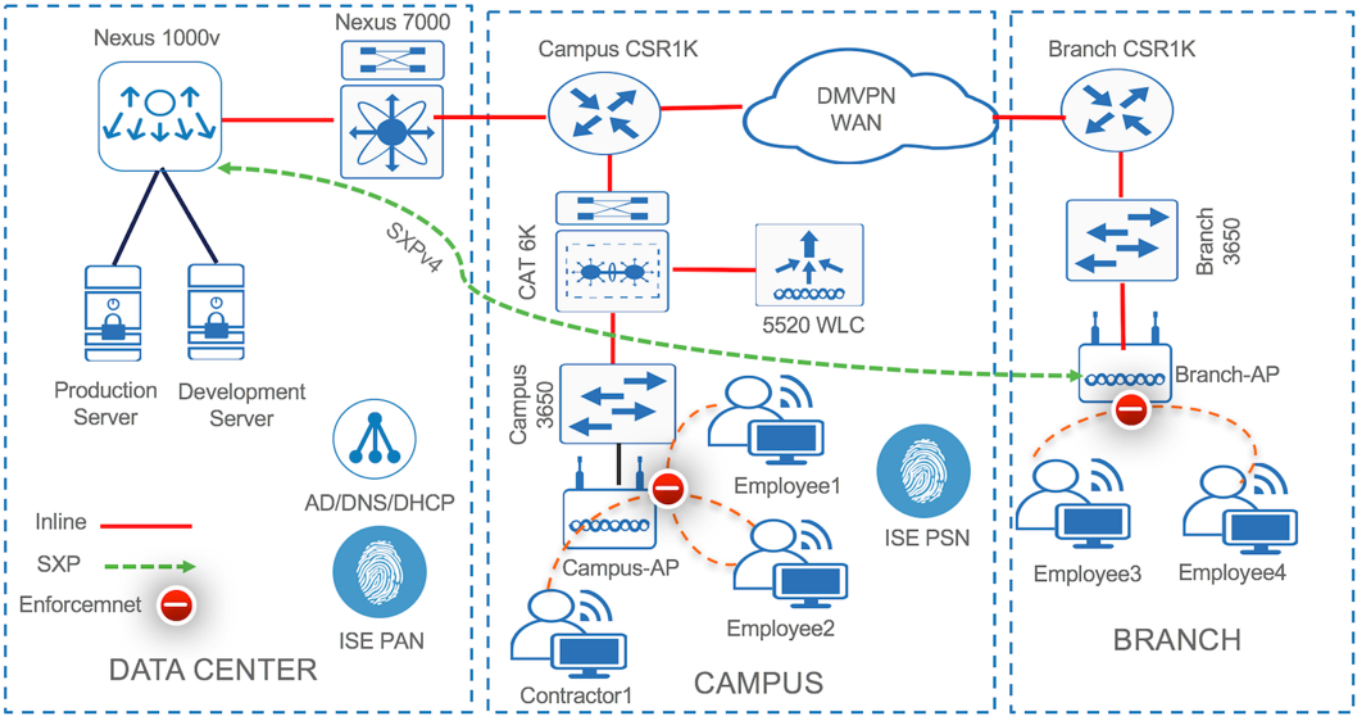
Wireless deployments in Campus and Branch in general deployed using both Centralized and FlexConnect modes. Control and Provisioning of Wireless Access Points (CAPWAP) supports these two layer 3 modes of operation. FlexConnect is most widely used wireless solution for branch office and remote office deployments. It enables an option to the wireless network administrator to configure and control access points in a branch or remote office from the corporate office through a wide area network (WAN) link without the deployment of a controller in each office. The FlexConnect access points (APs) can switch client data traffic locally and perform client authentication locally. When these APs connect to the controller, they can even send traffic back to the controller.

TrustSec capabilities on Wireless LAN Controllers (WLAN) were first released in 7.6 (release). That is where the wireless clients authenticating to the network would be assigned Security Group Tags (SGTs) dynamically based on attributes such as the role of the user and/or device through Cisco Identity Services Engine (Cisco ISE). Apart from dynamic SGT assignment WLCs also support SGT eXchange Protocol (SXP), which is SXPv2. Wireless LAN Controller could act as a SXP speaker sharing the IP-SGT binding information to its peer SXP listeners for enforcement. It was only supported for Central Switched SSIDs (WLANs). Wireless 8.3 is the first official release to support SGT assignment for the Access Points running FlexConnect mode.

Cisco Wireless Release 8.4 extends the capability to simplify access control management through SGACL enforcement on Access Points (APs). This is supported on both Central Switched SSIDs and FlexConnect SSIDs (WLANs). Instead of using an upstream switch/router for enforcement, the wireless traffic can now be enforced directly on the Access Points. This would help in reducing the Malware propagation on wireless clients by blocking the Lateral movement. It is not the Wireless LAN Controller, which does the enforcement. The WLC downloads the TrustSec Policy (SGACLs) from ISE and shares through CAPWAP tunnel to the Access Points for enforcement. The Access Points that supports SGACL enforcement includes both Wave1 (1700, 2700, 3700) and Wave2 (1800, 2800, 3800) APs. 5520 and 8540 are the only two WLC platforms supporting the SGACL enforcement on the Access Points.

Cisco Wireless Release 8.4 also adds the inline-tagging capability on both 5520 and 8540 WLCs. These two platforms now could propagate the Security Group Tags natively. Apart from inline-tagging propagation through WLCs, the Cisco Wireless Access Points (both Wave1 and Wave2) running in FlexConnect mode supports both inline-tagging and SXPv4 propagation. Both SXPv4 and inline-tagging features are supported on FlexConnect APs only. SXPv4 not only supports SXP speaker role but also SXP listener and Both (SXP Speaker and Listener) modes of operation. It helps in Loop detection and prevention with a built-in Keep Alive mechanism. Cisco Access Points from branch offices can now learn and share Security Group membership information over an SGT eXchange Protocol (SXP) connection from switches, routers, and firewalls to simplify access control list management and firewall rule management elsewhere in the network and even do enforcement locally from the learned mappings for wireless access control management providing software-defined segmentation.

Figure 1: Sample topology showing a typical Wireless Local/FlexConnect deployment with Campus and Branch



ISE Configuration

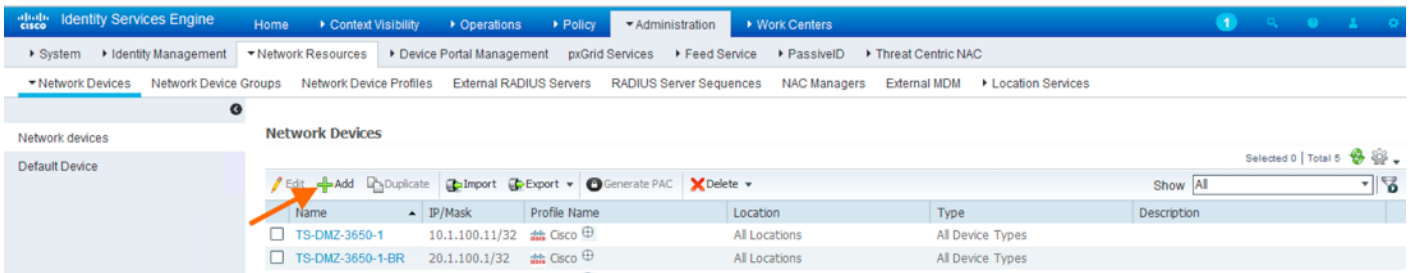
Cisco Identity Services Engine needs to be configured to assign a Security Group Tag dynamically as part of an authorization rule. ISE can authorize devices coming through MAB or 802.1X based on attributes such as the role of the user and/or device and assign a Security Group Tag dynamically.

Add Wireless LAN Controller in ISE

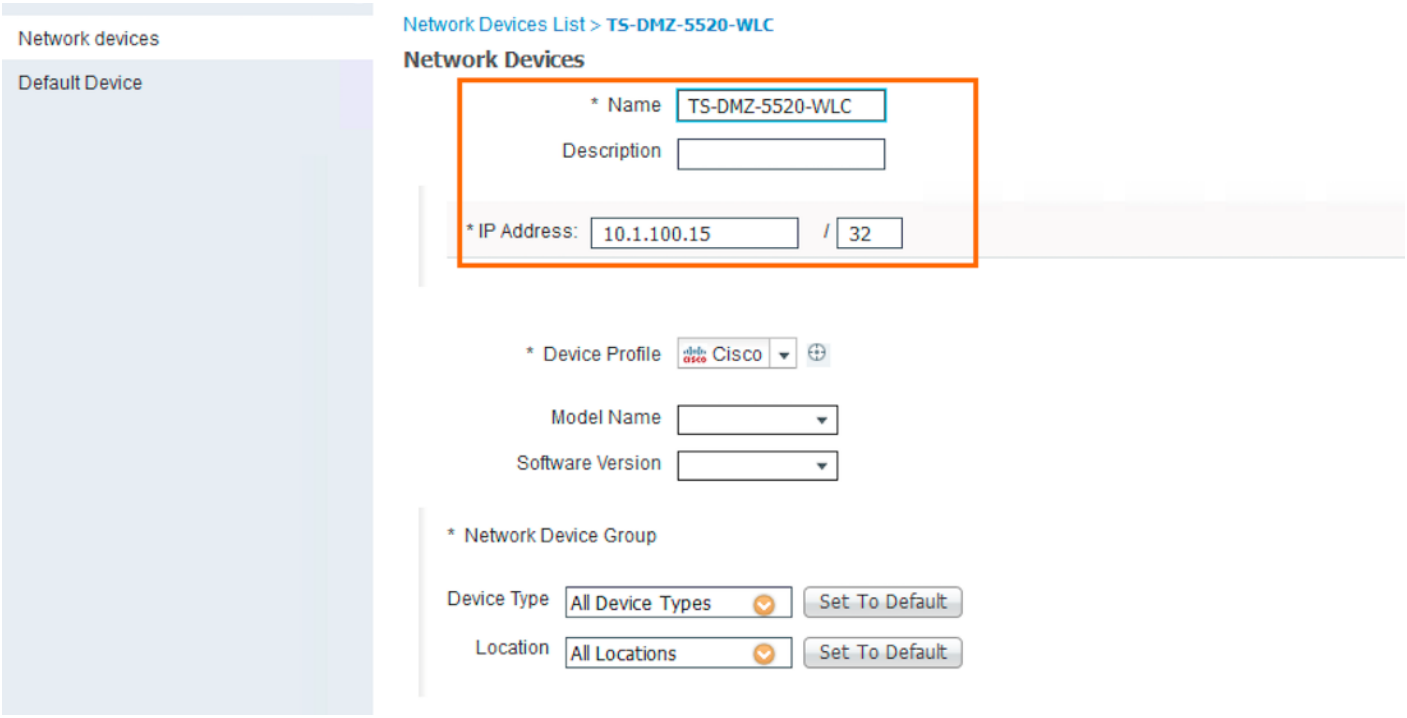
Step 1 Login to Cisco Identity Service Engine (ISE)

Step 2 Go to Network Devices in ISE by navigating to **Administration > Network Resources > Network Devices**

Step 3 Click **Add** to add the new **WLC** in ISE

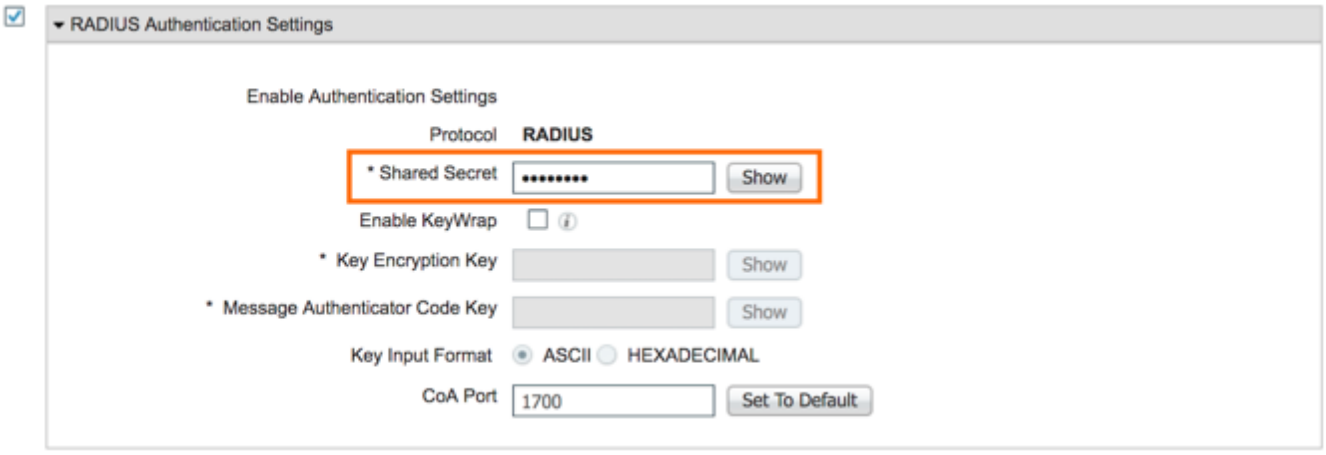


Step 4 Type the **Name** of the WLC, **IP Address** and any Network Device Group information (optional) like **Device Type** and **Location**



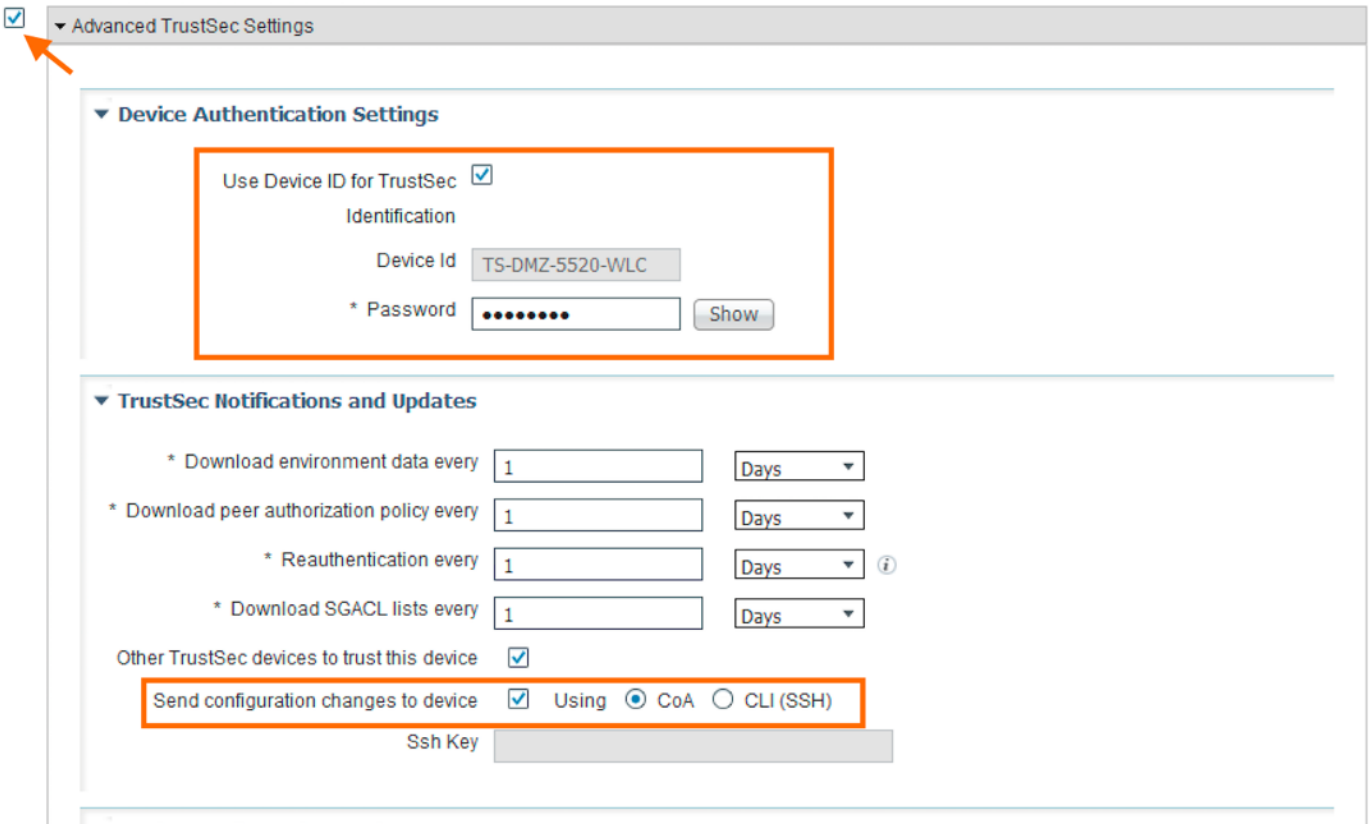
Step 5 Configure the **Radius Authentication Settings** by typing a new **Shared Secret**

Note: The same Shared Secret needs to be configured while adding the Radius servers on the WLC



Step 6 Configure any SNMP configuration (Optional)

Step 7 Now enable the **Advanced TrustSec Settings**



☑ Advanced TrustSec Settings		Description
Device Authentication Settings		
Use Device ID for TrustSec	☑	
Device Id	TS-DMZ-5520-WLC	This is automatically populated from the Device Name if Use Device ID for SGA identification is checked. This ID must match the "cts device-id" command that is later configured on the WLC.
Password	<####>	TrustSec authentication password. This must match the password that is associated with the "cts device-id" command
TrustSec Notifications and Updates		
Download environment data every	1 Days	Specifies the expiry time for environment data. ISE returns this information when the WLC queries for environment data. The default is 1 day
Download peer authorization policy every	1 Days	Specifies the expiry time for the peer authorization policy. ISE returns this information to the device in response to a peer policy request. The default is 1 day

Reauthentication every	1 Days	Specifies the dot1x re-authentication period. ISE configures this for the supplicant and returns this information to the authenticator. The default is 1 day
Download SGACL lists every	1 Days	Specifies the expiry time for SGACL lists. ISE returns this information to the device in the response to a request for SGACL lists. The default is 1 day.
Other TrustSec devices to trust the device	☑	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Send configuration changes to device	☑ Using ⊙ CoA	This configuration allows network device to receive Per Policy Change of Authorization push from ISE. When there is a policy change (add/delete/update SGACL in Egress policy), administrator can use Push button to initiate CoA to network device. After receiving CoA notification from ISE, network device queries if there is any new egress policy configured in ISE. If there is new policy, it downloads this new policy immediately.

Step 8 Configure **Device Configuration Deployment** (Optional)

Device Configuration Deployment		
Include this device when deploying Security Group Tag Mapping Updates	☑	When selected, any IP/SGT Mappings defined at ISE will be pushed to that device. This box should be unchecked for all those network devices where the static ISE mappings are undesirable.
Device Interface Credentials		
EXEC Mode Username EXEC Mode Password Enable Mode Password	admin <####> <####>	These are the credentials for ISE to login to the WLC and configure static IP-SGT mappings.

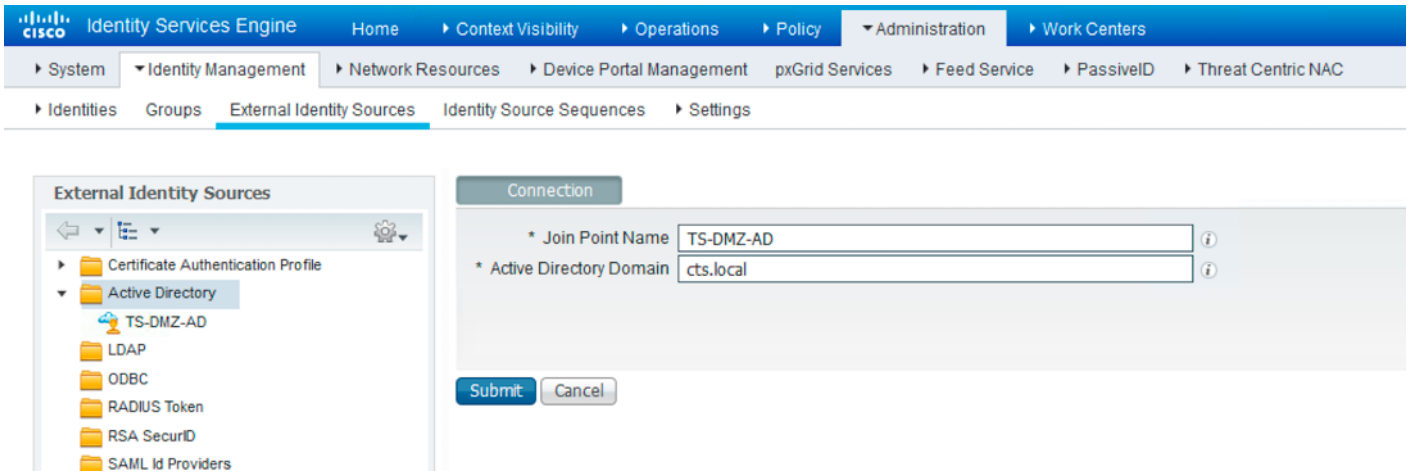
Step 9 Click **Save**

Active Directory Configuration in ISE

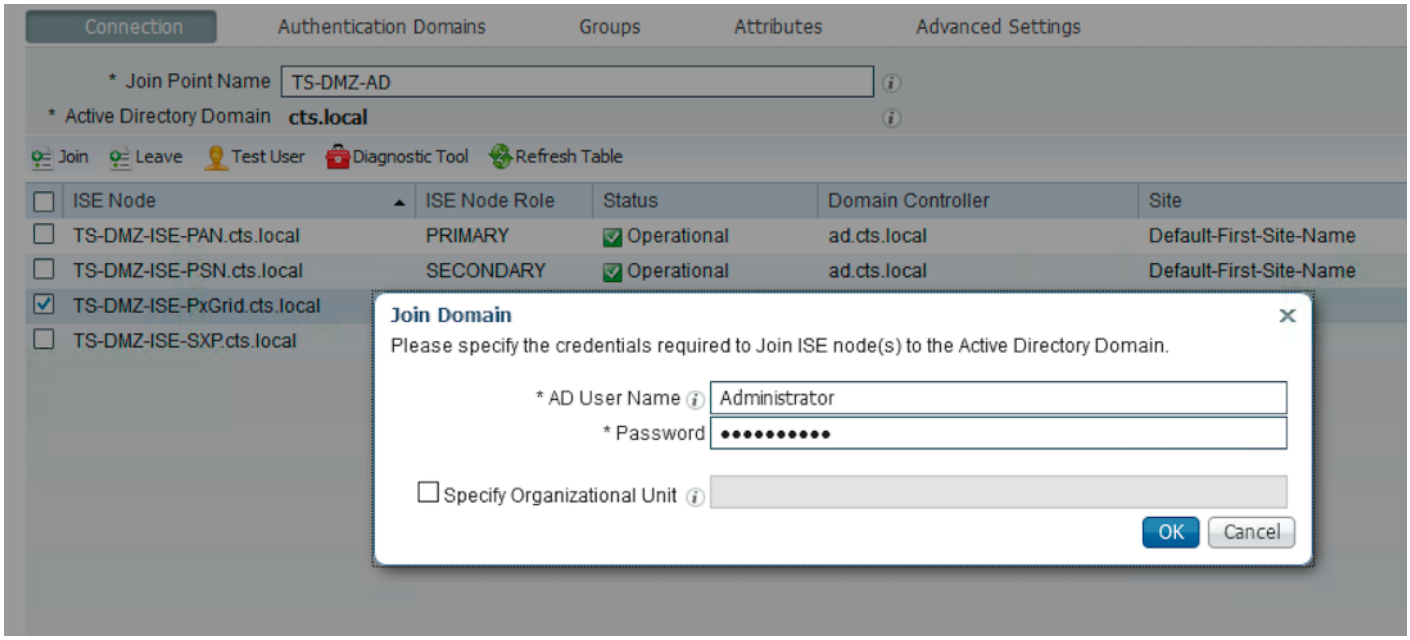
By retrieving the AD groups from the configured Active Directory in ISE the administrator would have an option to assign a Security Group value based on the user role

Step 1 To add a new AD server in ISE navigate to **Administration > Identity Management > External Identity Sources > Active Directory**

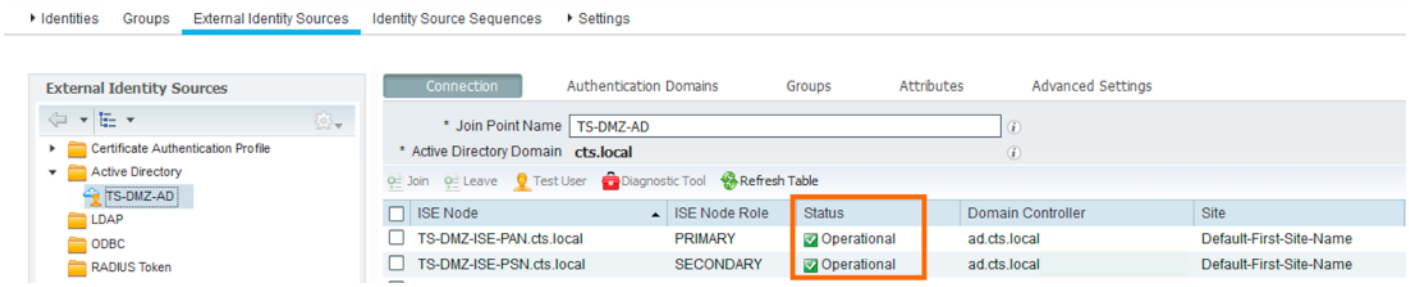
Step 2 Click **Add** for a new connection with a **Join Point Name** and **Active Directory Domain** name and **Submit**



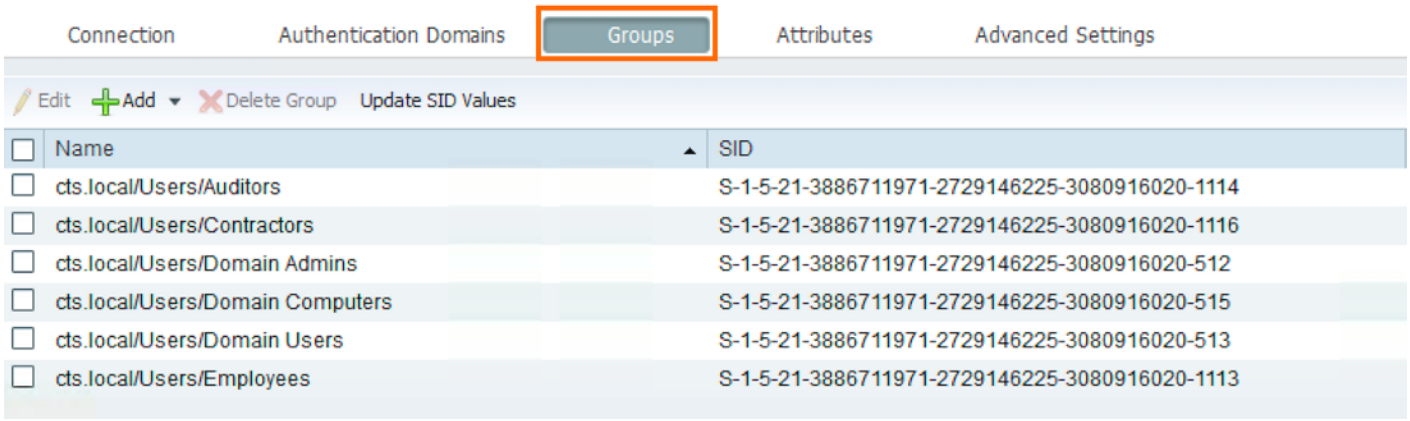
Step 1 Select all the ISE nodes and click **Join** to connect the nodes to the AD server. Provide the **AD User Name** and **Password**



Step 2 Click **OK** to see the status **Operational** and Save the connection



Step 3 Now switch to the Groups tab and retrieve the AD groups from the AD server



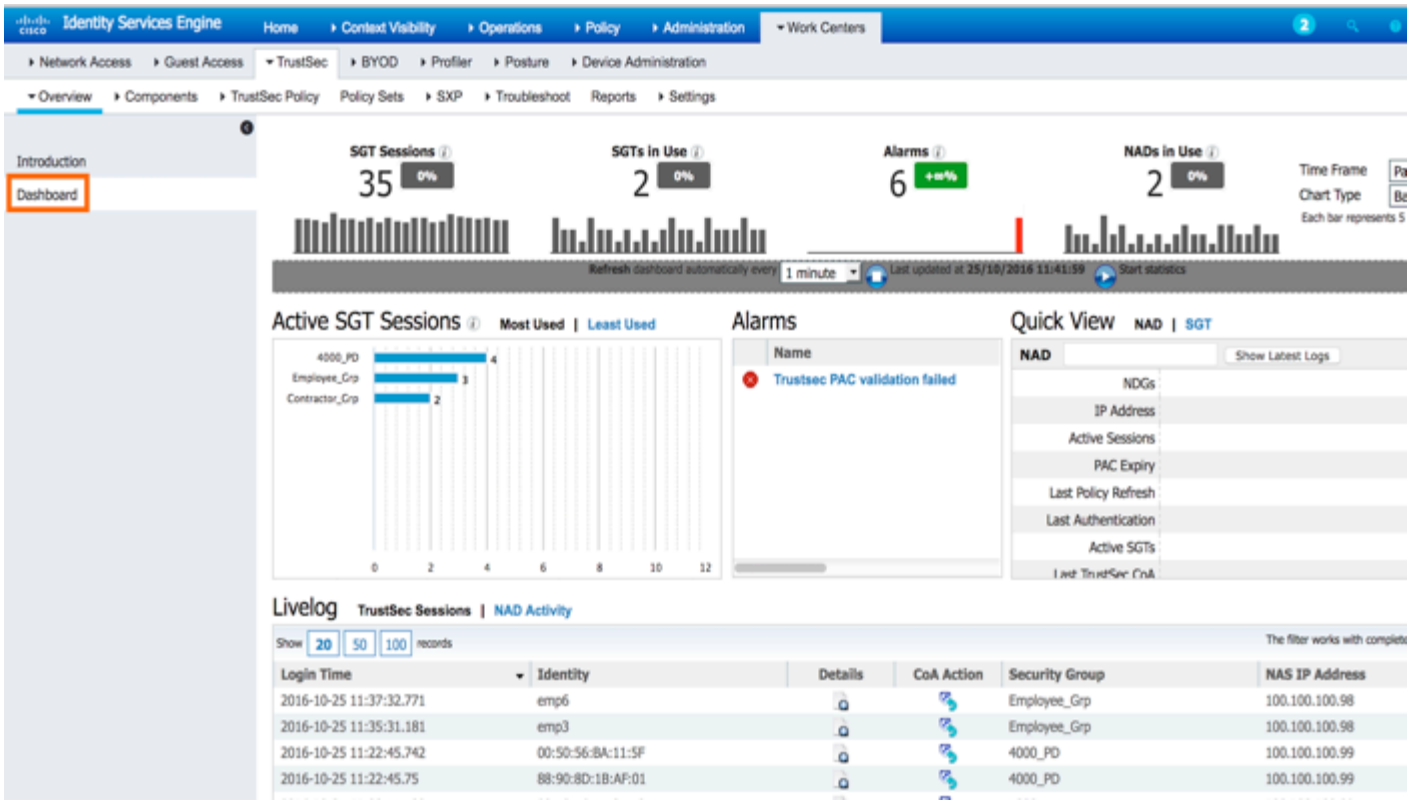
Note: These AD Groups would be useful for the administrators in creating the Authorization policies based on user roles.

TrustSec Work Centers

Since ISE 2.0 in admin UI there is new Work Centers with TrustSec where we can configure all the TrustSec settings in ISE. That is a one-stop shop for all the TrustSec related activity. There is a new TrustSec Dashboard to view all the Alarms, Active SGT sessions, Security Groups and NADs

Step 1 From ISE to navigate to TrustSec Work Centers go to **Work Centers > TrustSec**

Step 2 To view the TrustSec Dashboard navigate from ISE to **Work Centers > TrustSec > TrustSec Dashboard**



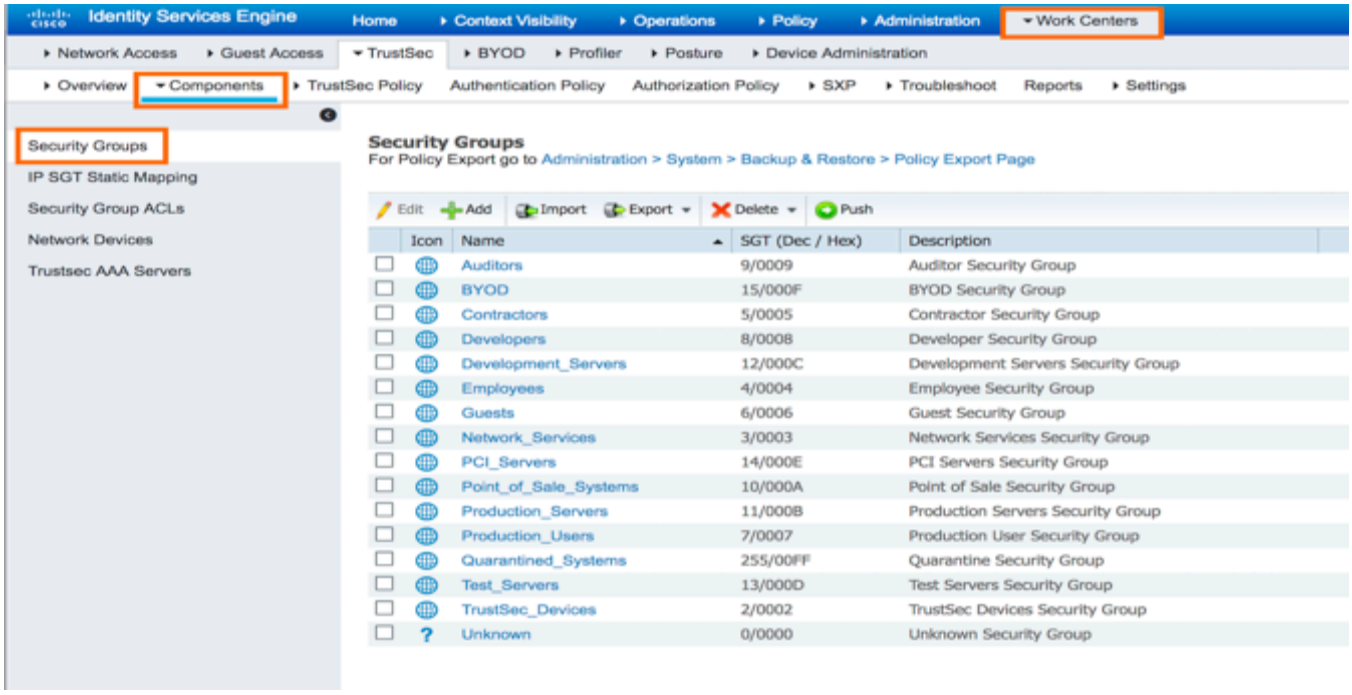
Configure Security Groups in ISE

Security Group Tag is a unique 16-bit tag that is assigned to a unique role. It represents the privilege of the source user, device, or entity and is tagged at the ingress of the Cisco TrustSec domain. SGTs can be assigned through any of the following Endpoint Admission Control (EAC) access methods:

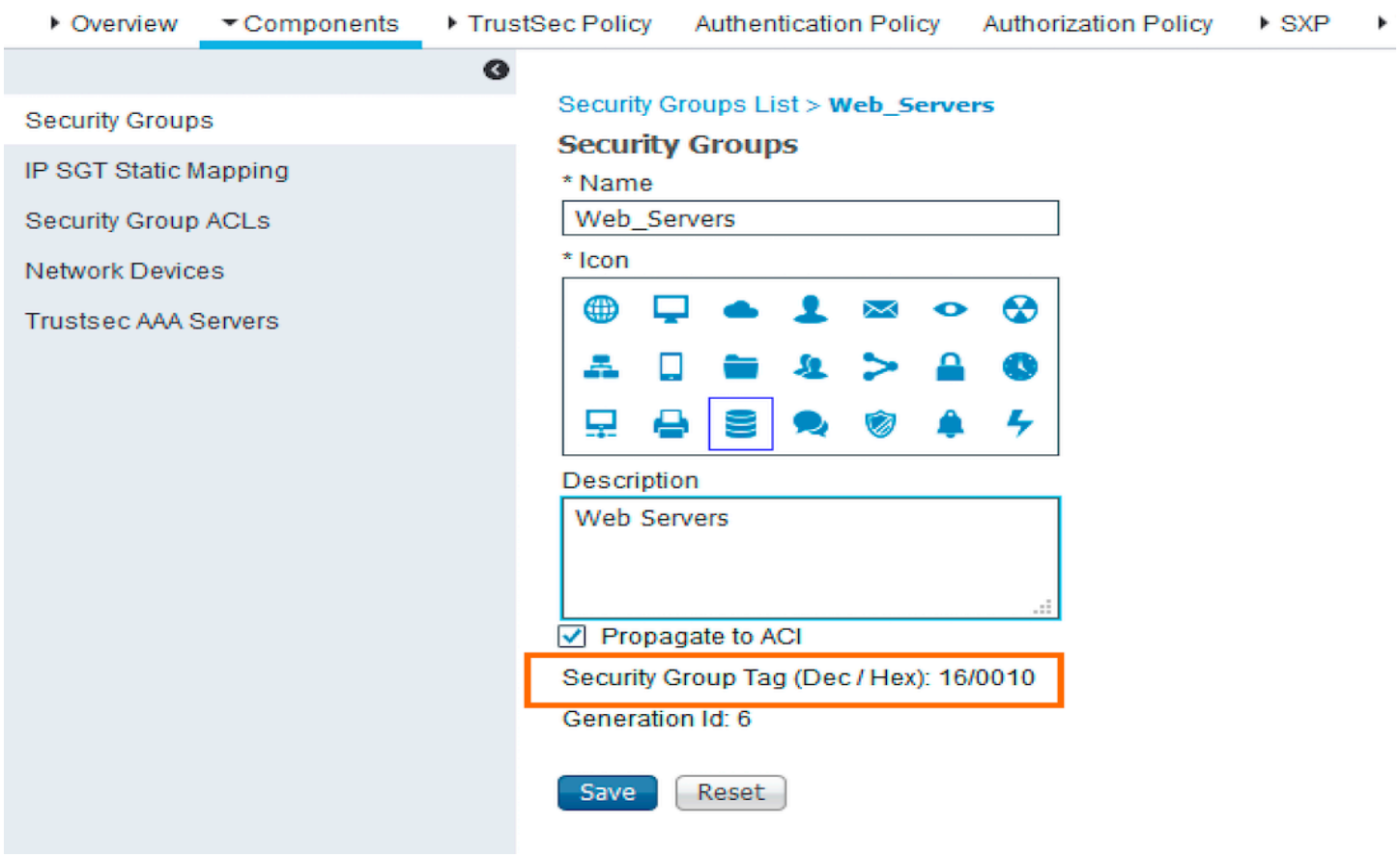
- 802.1X port-based authentication
- MAC Authentication Bypass (MAB)
- Web Authentication

Step 1 To view and add any new Security Groups in ISE navigate to **Work Centers > TrustSec > Components > Security Groups**

Step 2 ISE 2.0 and above have pre-defined **Security Groups** configured in ISE like Employees, Contractors etc. and assigned a **SGT** value

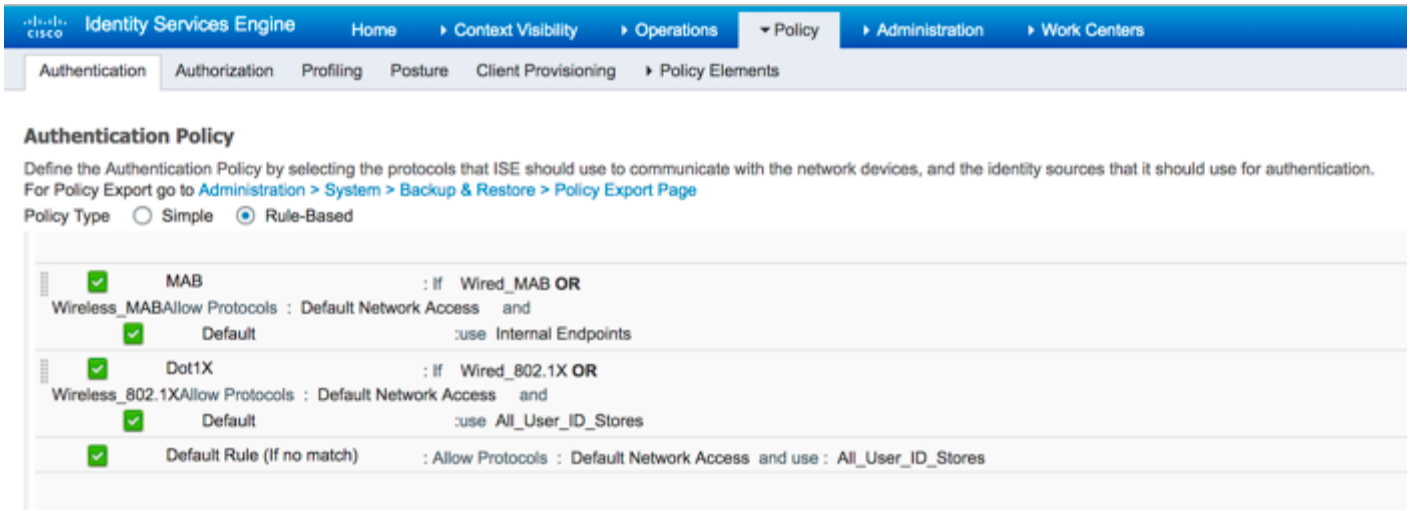


Step 3 Click **Add** to add a new Security Group in ISE and **Submit**. ISE would automatically assign a Tag value

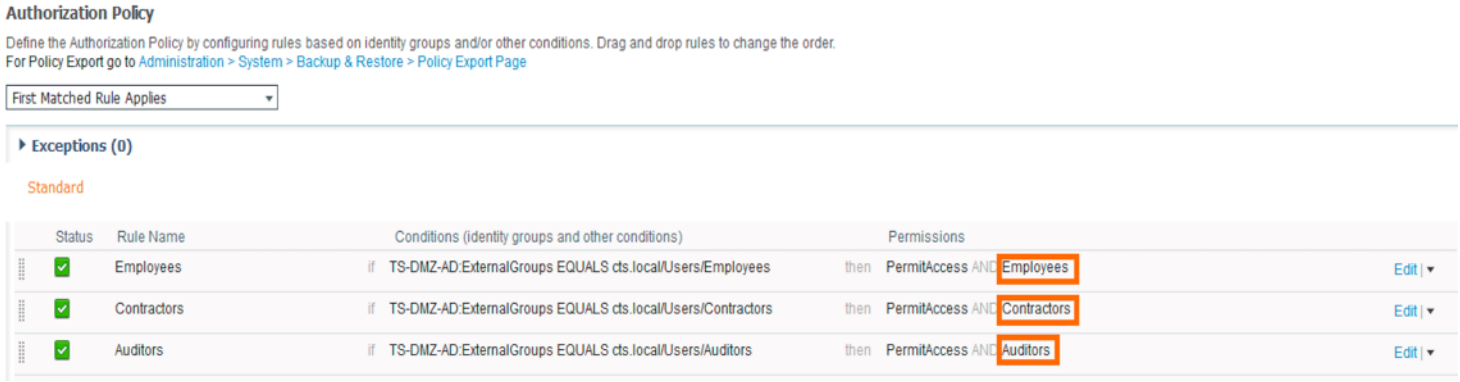


Authentication and Authorization Policies in ISE

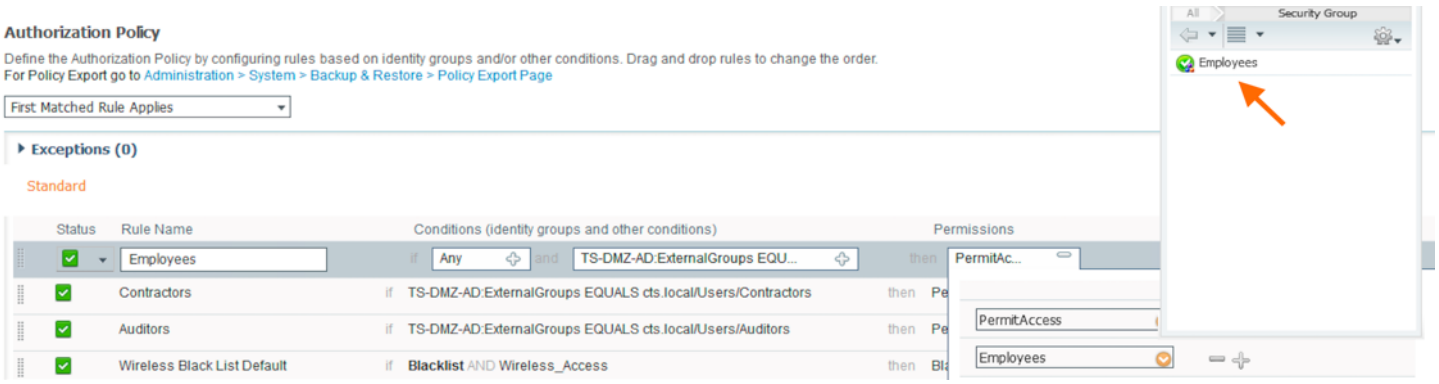
Step 1 Navigate to **Policy > Authentication** for the **Authentication Policy**. Here is a sample Authentication policy for both **MAB** and **Dot1X**



Step 2 Navigate to **Policy > Authorization** for the **Authorization Policy**. Here is a sample Authorization policy for employees, Contactors and Guest users.



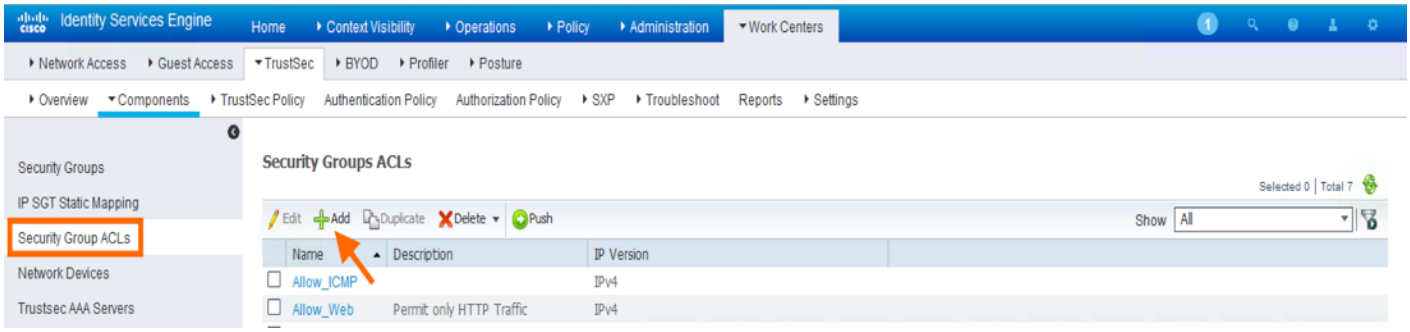
Step 3 Assign a security group to each of the Authorization rule based on the user role/device type like **Employees** etc.



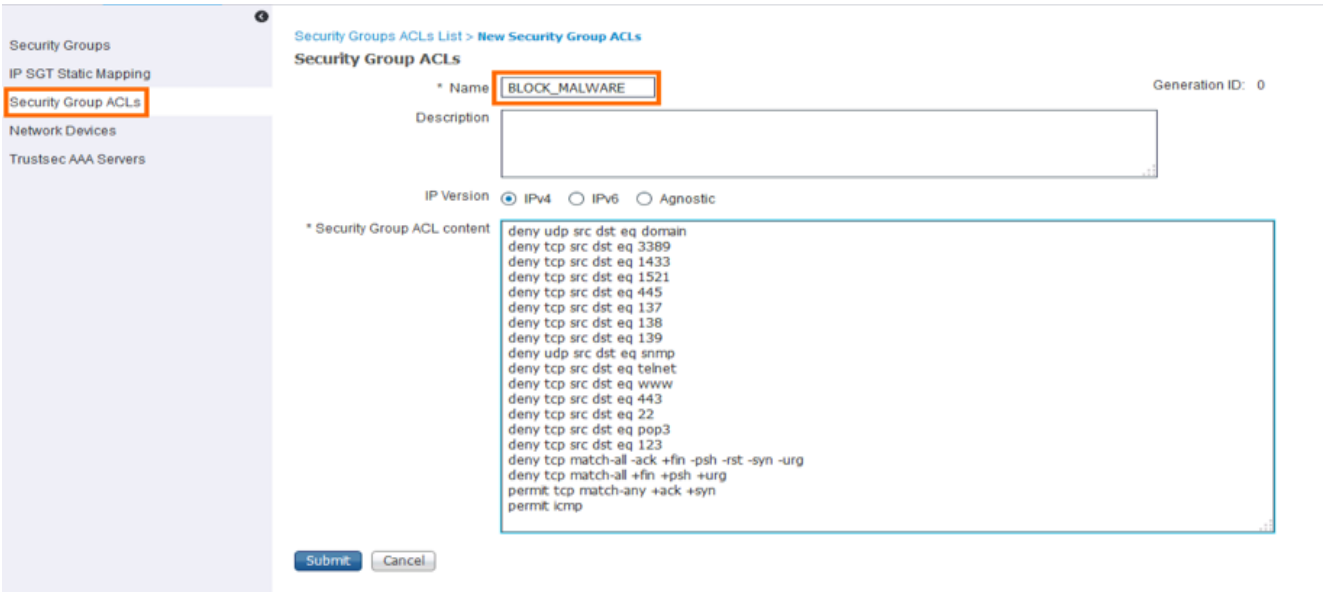
SGACL Configuration in ISE

Security Group Access Control Lists (SGACLs) are the permissions that can control or restrict the operations that users can perform based on the role of the user using the security group assignments instead of an IP address. We can configure the SGACLs manually on the devices or on ISE administrative node by pushing to the respective network devices through the TrustSec Policy Matrix. To configure the SGACLs on ISE:

Step 1 Navigate to **Work Centers > TrustSec > Components > Security Group ACLs** and click **Add**



Step 2 Give it a **Name** and the **IP Version** if it is **IPv4**, **IPv6** or **Agnostic** (both). Add the **Security Group ACL Content** with Permit and Deny using Protocols and Port Numbers. Here is a sample SGACL for your reference.



Step 3 After adding the SGACL content click **Save**

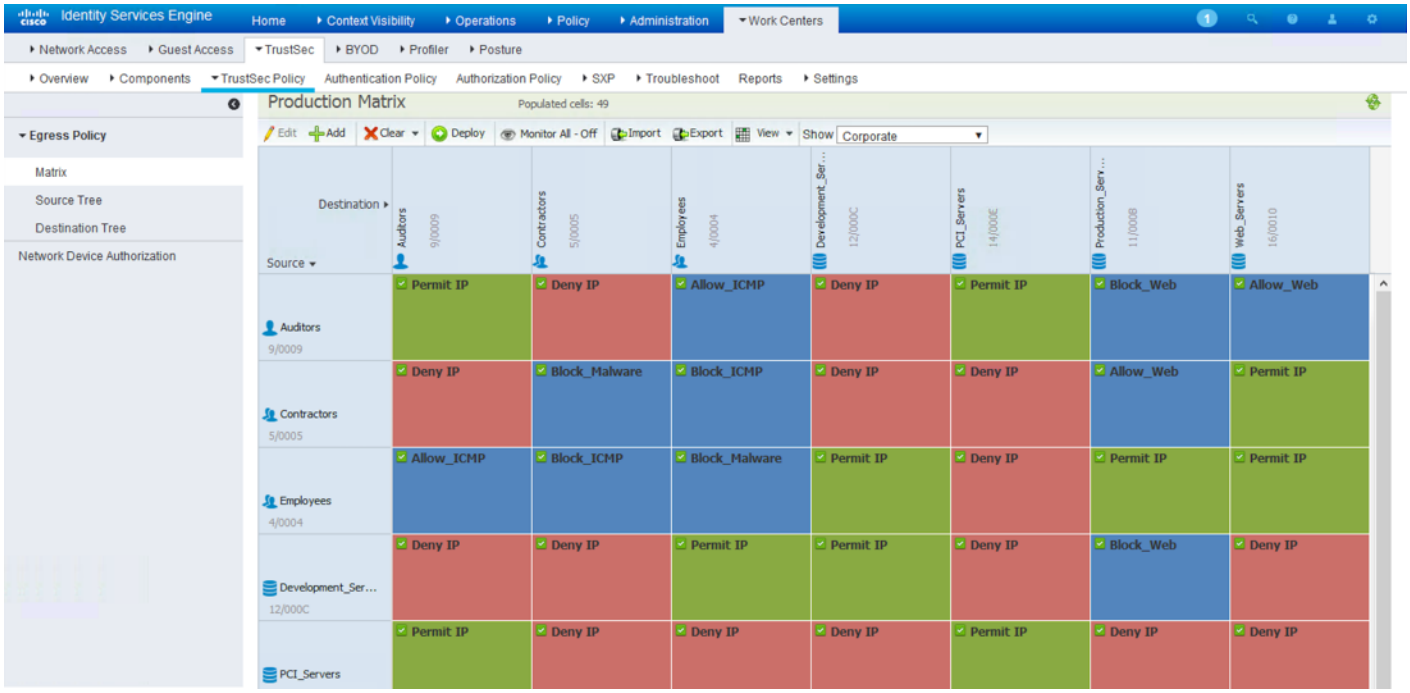
TrustSec Policy Matrix in ISE

TrustSec Policy Matrix in ISE needs to be configured to enforce the policy on the APs, access and datacenter switches (Cat6k, N1kv, N7k etc.) and routers using SGACLs. We can configure the SGACLs manually on the devices or on ISE by pushing to the respective network devices. Through ISE you can centrally push the SGACLs to all the network devices instead of typing manually on each and every switch. ISE also has a Policy Matrix view (customizable) with the Source group tags and the Destination group tags where you can configure and push the SGACLs.

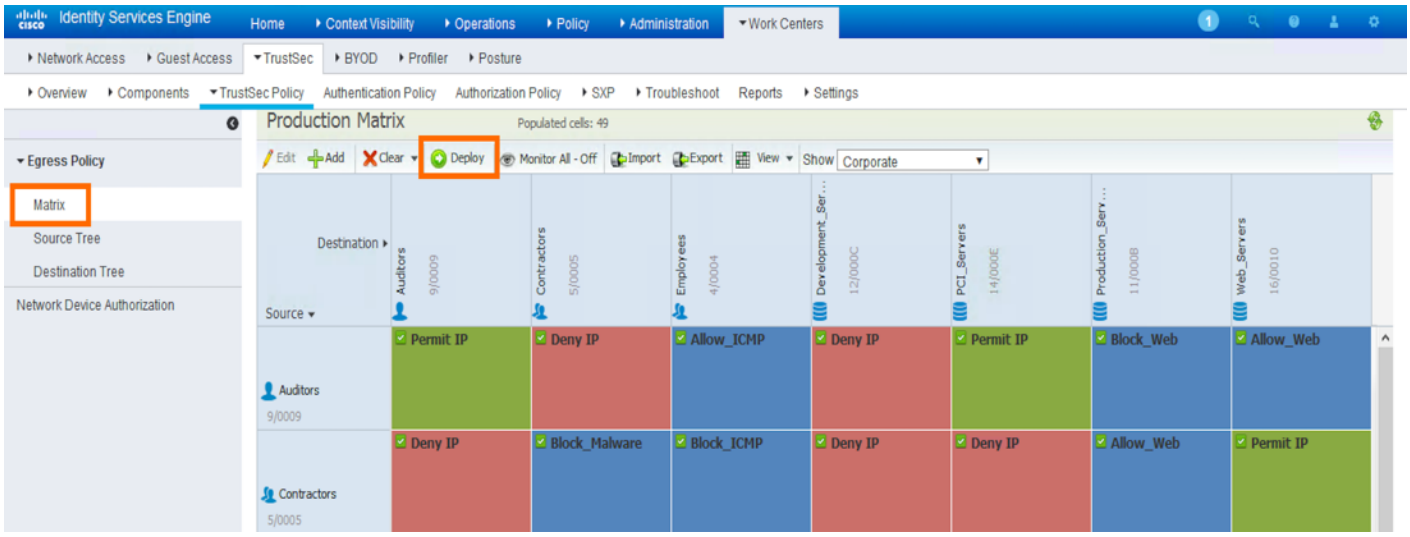
Step 4 Navigate to **Work Centers > TrustSec > TrustSec Policy > Egress Policy** and click **Matrix** to configure the TrustSec policy Matrix in ISE

Here is a sample TrustSec Policy Matrix with Source, Destination groups and the SGACLs

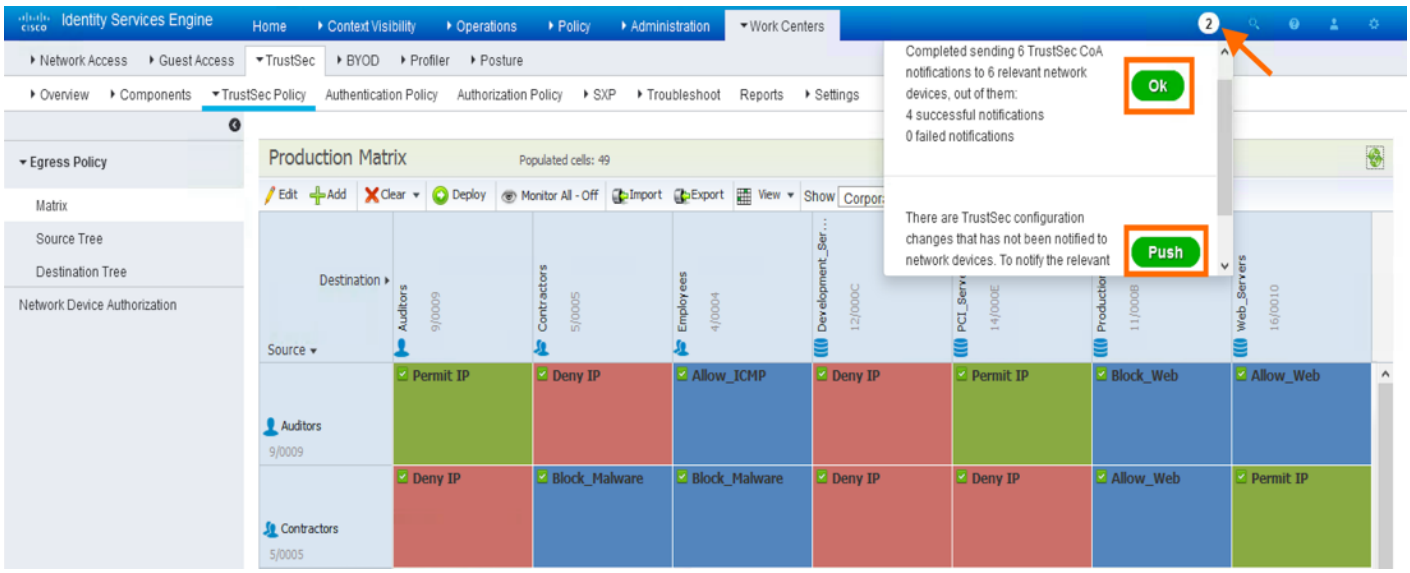
Note: The below configured TrustSec Policy Matrix is just for your reference.



Step 5 Once the TrustSec Policy Matrix is configured click **Deploy** to push the **SGACLs** and their permissions to the network devices.

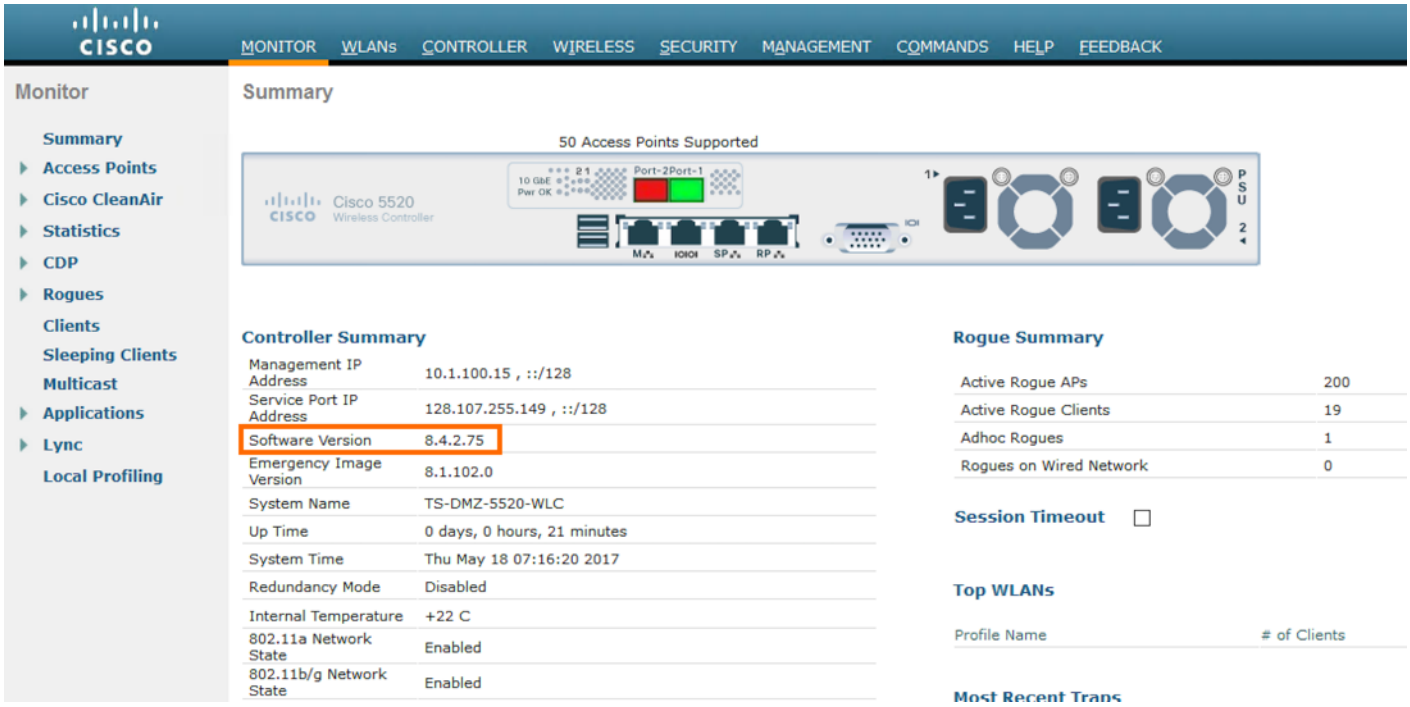


Step 6 After the Matrix is deployed look for the notifications messages (CoA) on the upper right corner. **Push** to send any configuration changes to the network devices or click **OK** to acknowledge the notification messages



WLC Configuration

In order to have TrustSec SGACL support on the APs, ensure that the WLC is running 8.4.100 or later code.



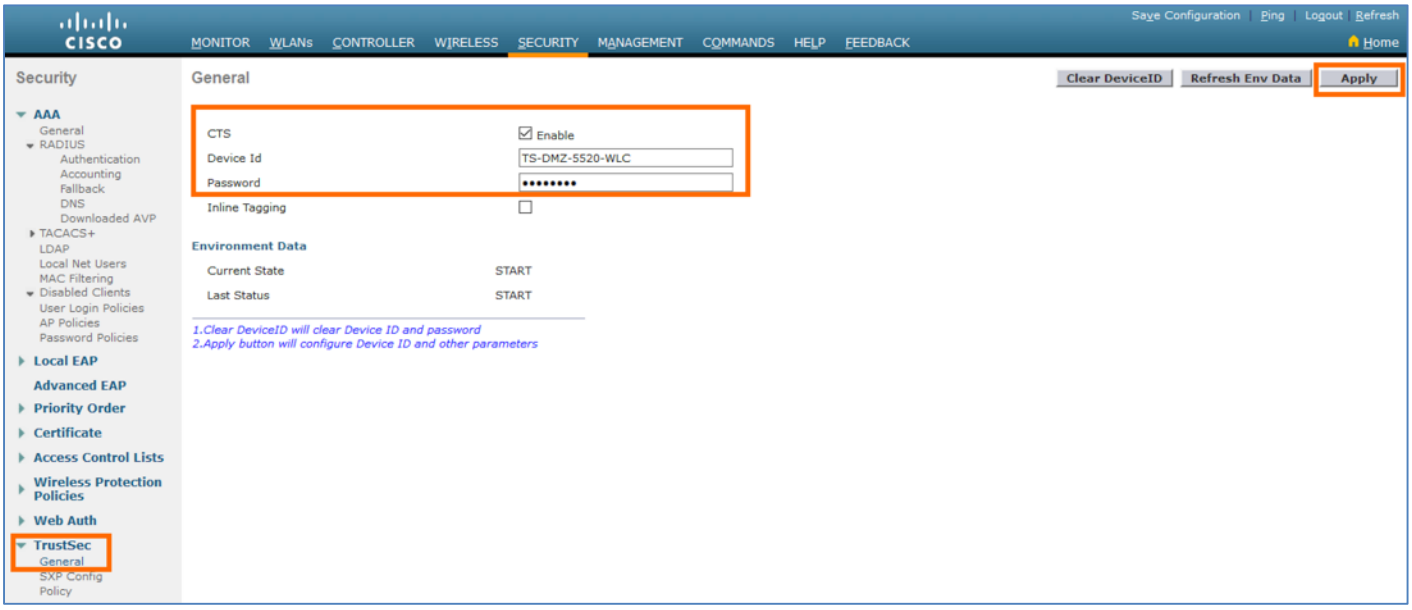
TrustSec NDAC for Security Groups and SGACL Download

Any device that participates in the TrustSec (CTS) network requires to be authenticated and trusted. In order to facilitate the authentication process new devices connected to TrustSec network under goes an enrollment process called Network Device Admission Control (NDAC), where in the device obtains the credentials that is specifically needed for device authentication and CTS environment data. The Wireless LAN Controller 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

Step 1 From WLC navigate to **Security > TrustSec > General**

Step 2 Click the checkbox to enable **CTS** and provide the **Device ID** and **Password** which matches the **Device ID** and **Password** of WLC in ISE under **Device Authentication Settings** configured under the **Advanced TrustSec Settings** and click **Apply**

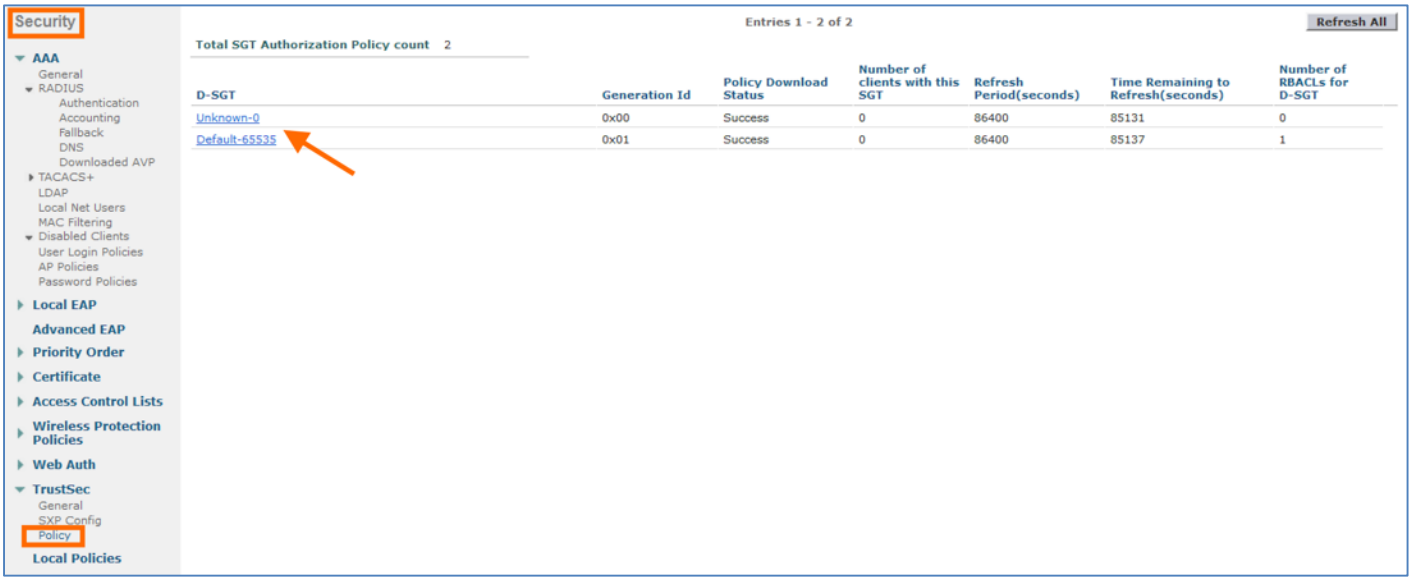
Note: The **Device ID** and **Password** should match with the configured credentials in ISE



Step 3 Click **Refresh ENV Data** to download the **Security Group Name Table** by the WLC from ISE. All the Security Groups defined in ISE would be downloaded by the WLC.

After successful PAC (Protected Access Credential) provisioning over a EAP-FAST TLS tunnel, WLC would now start downloading SGACL policies from ISE. The WLC will download the specific 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).

Step 4 Navigate to **Security > TrustSec > Policy** to see the downloaded SGACL policies on the WLC.



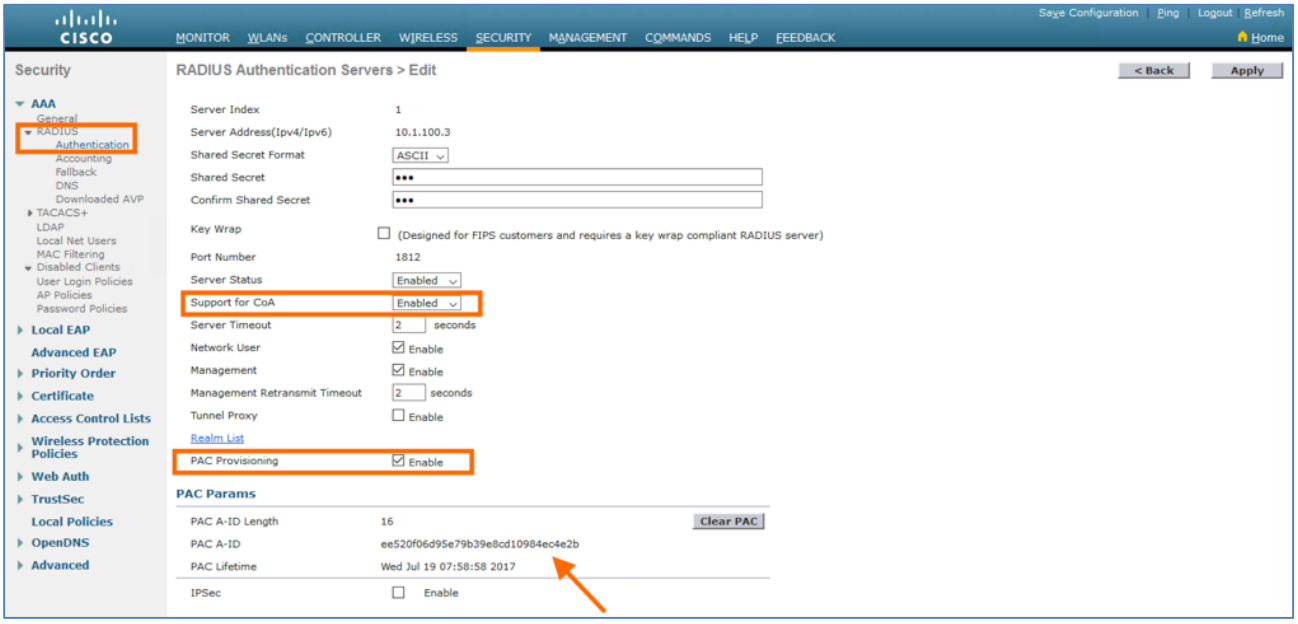
Note: Above screenshot shows the SGACL policies of default and unknown only being downloaded as there are no authenticated clients with SGTs to download the respective SGACL policies.

Radius Configuration on WLC

The ISE PSNs need to be added as the Radius Servers in the WLC to authenticate the user sessions against ISE

Step 1 From WLC navigate to **Security > Radius > Authentication** and Click **New**

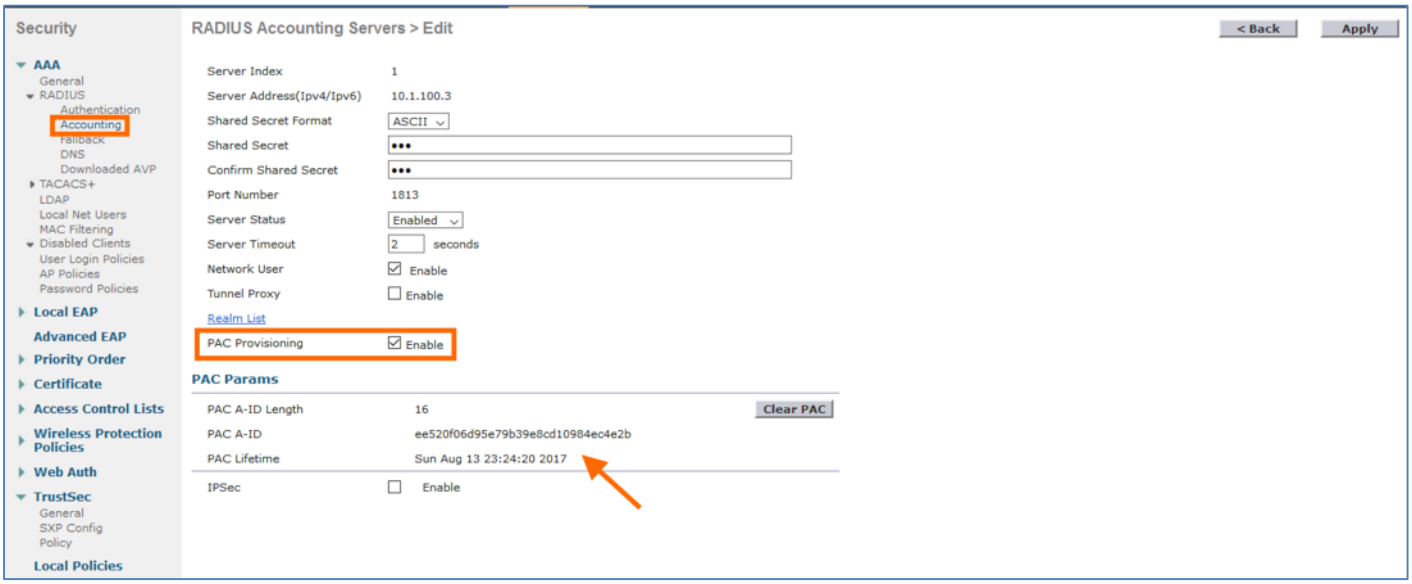
Step 2 Add the **Server IP address** of the ISE PSN and use the same **Shared Secret** configured in ISE, Enable the **Support for CoA** and enable **PAC Provisioning** Click **Apply**



Note: The **PAC Params** would be downloaded to the Wireless LAN Controller since we enabled the PAC Provisioning

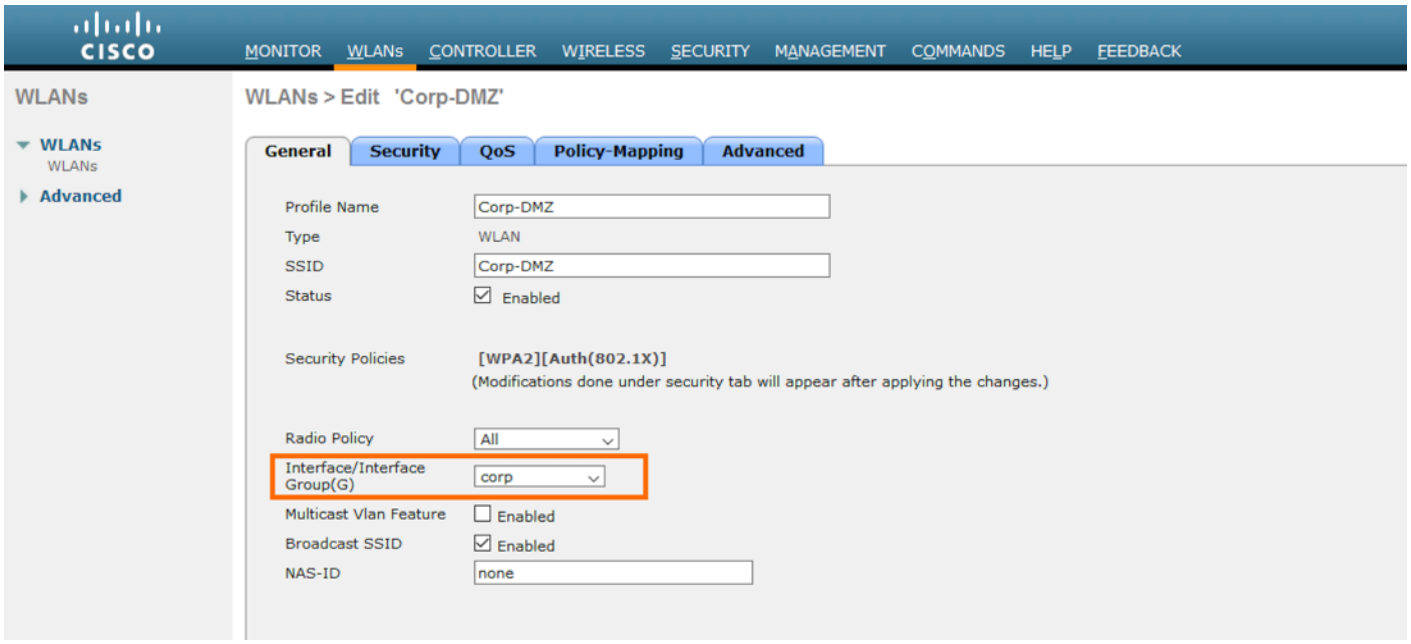
Step 3 From WLC navigate to **Security > Radius > Accounting** and Click **New**

Step 4 Add the **Server IP address** of the ISE PSN and use the same **Shared Secret** configured in ISE and enable **PAC Provisioning** and click **Apply**

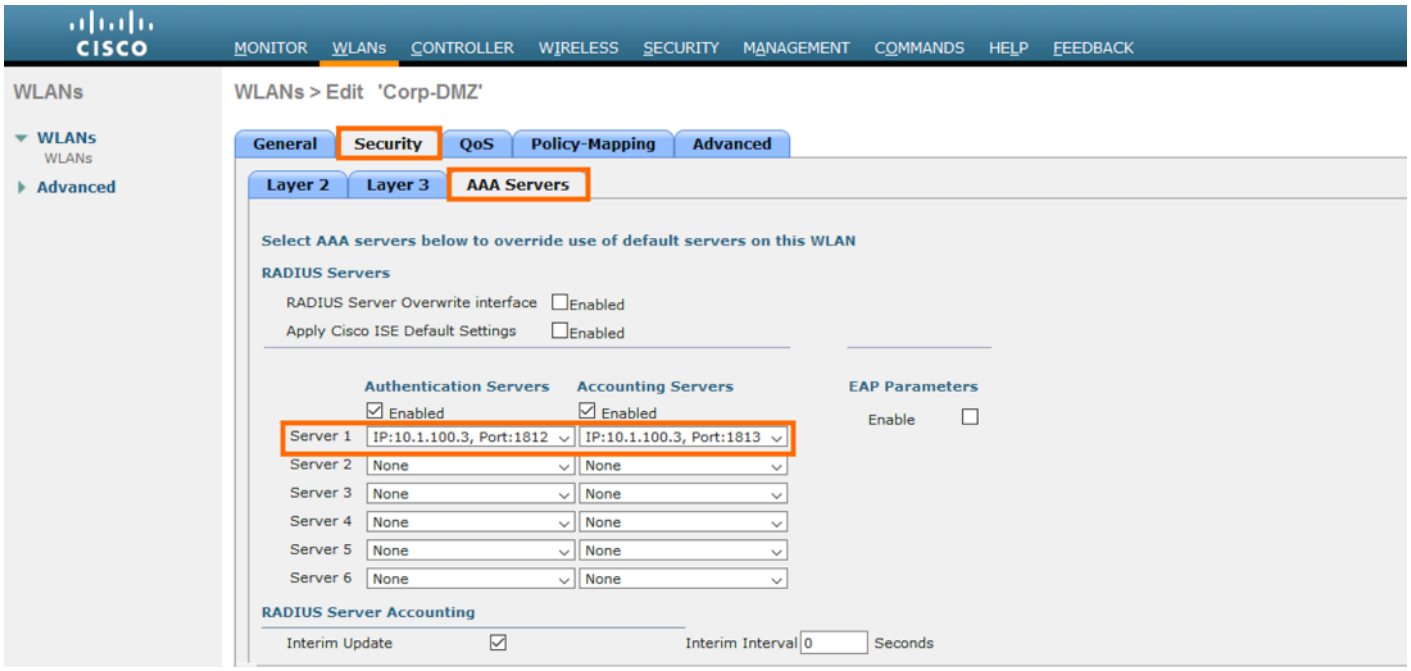


WLAN Configuration on WLC

Step 1 From WLC navigate to **WLANs** and **Edit** the **Corporate** SSID

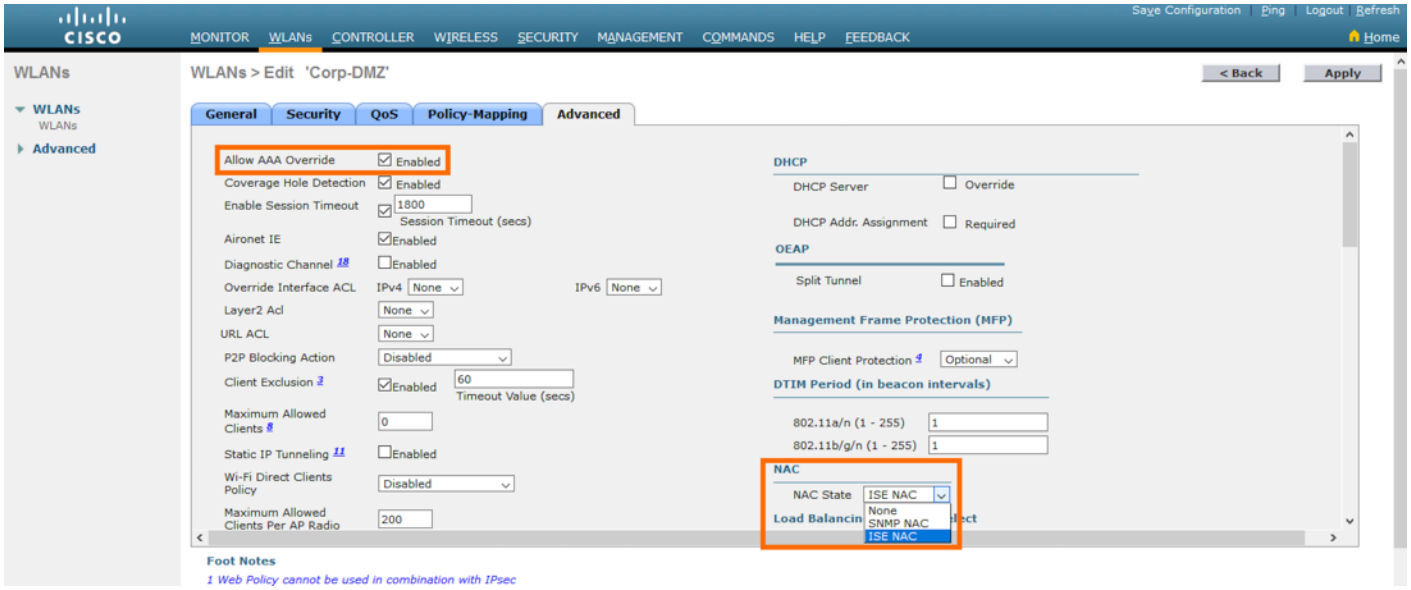


Step 2 Click on **Security > AAA Servers** and select the ISE PSN as the Authentication and Accounting Server from the drop down



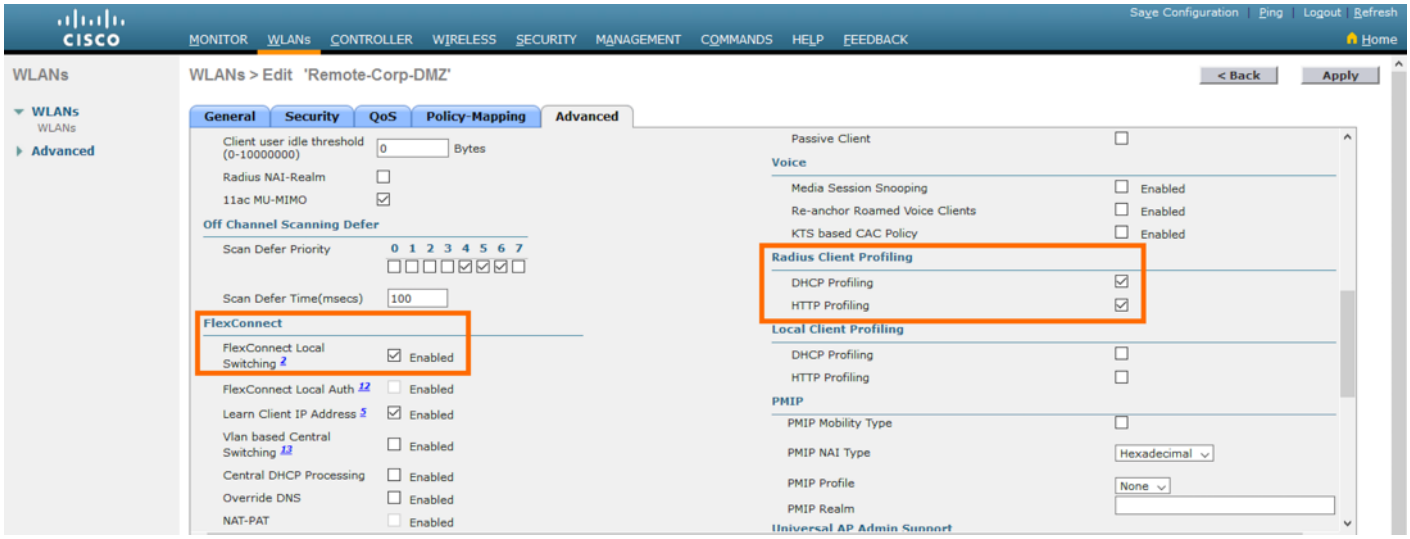
Step 3 Click **Advanced** tab and Enable **Allow AAA Override** and select **NAC State** from the dropdown as **ISE NAC**

Note: Cisco TrustSec Security Group Tag is applied only when AAA Override is enabled on the WLAN



Step 4 If it is **FlexConnect SSID** then scroll down in the **Advanced** Tab and Enable **FlexConnect Local Switching** to run WLAN in FlexConnect Local Switching mode

Step 5 Use ISE PSNs to profile the endpoints and users connecting to this SSID by enabling **DHCP Profiling** and **HTTP Profiling** under the **Radius Client Profiling**

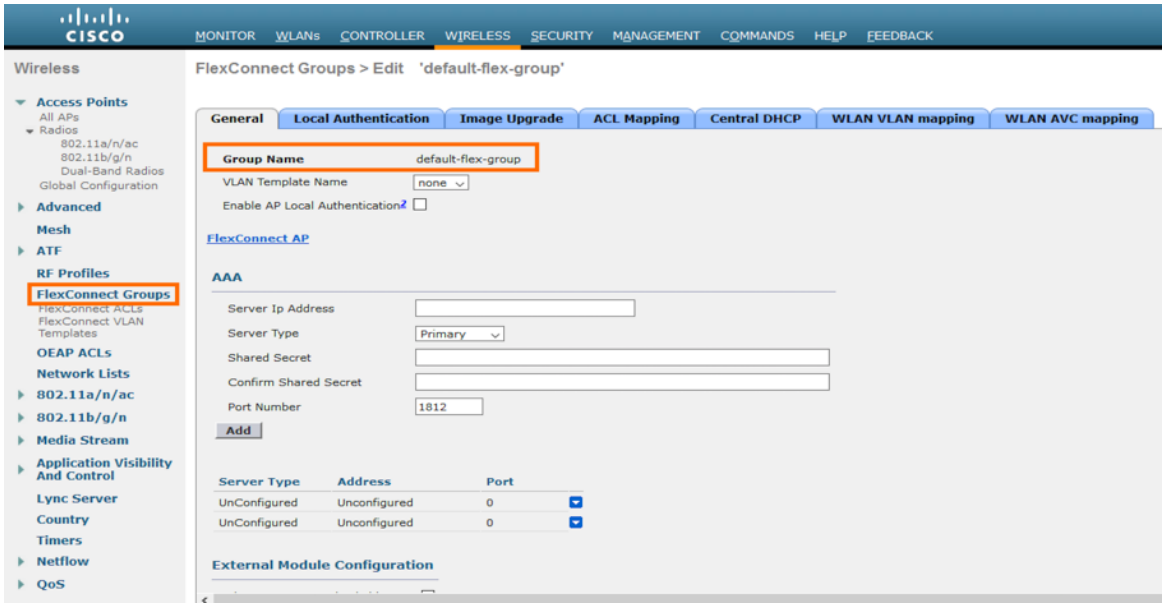


Step 6 Click **Apply** to save the changes to the SSID

Step 7 Repeat the **steps 2** to **6** for the rest of the SSIDs in the network

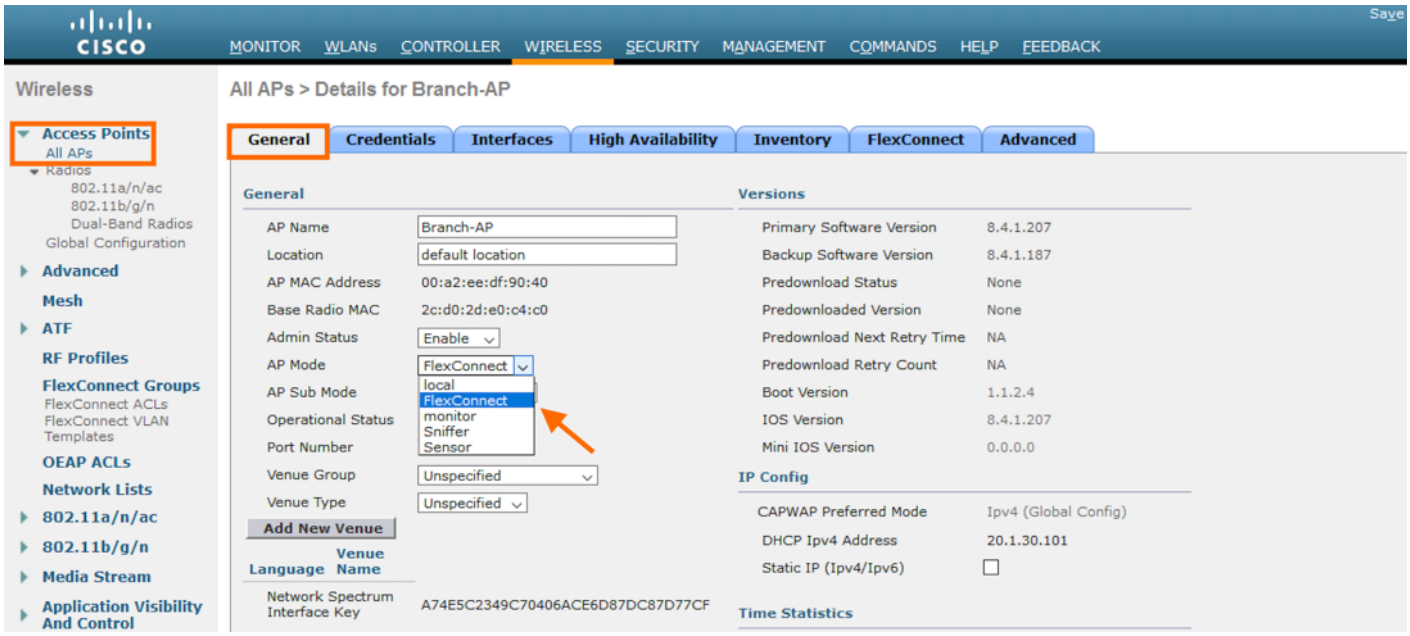
FlexConnect Configuration on WLC and AP

Step 1 From WLC navigate to **Wireless > FlexConnect Groups** and Click **New** and add a name to the FlexConnect group or use the **default-flex-group**

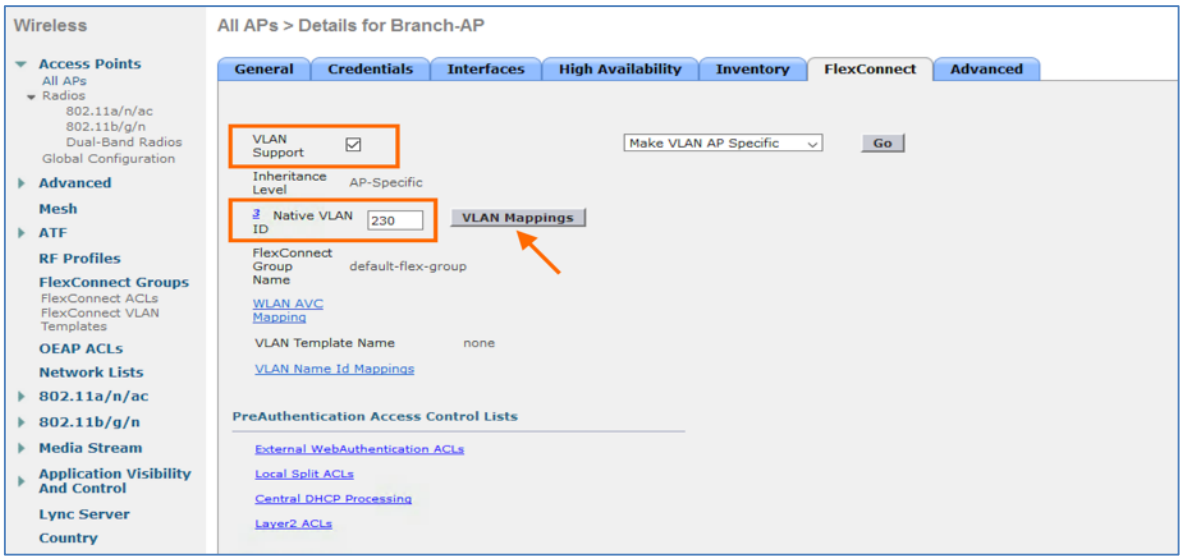


Step 2 Add the existing AP in the branch to the newly created FlexConnect Group by Navigating to **Wireless > All APs**

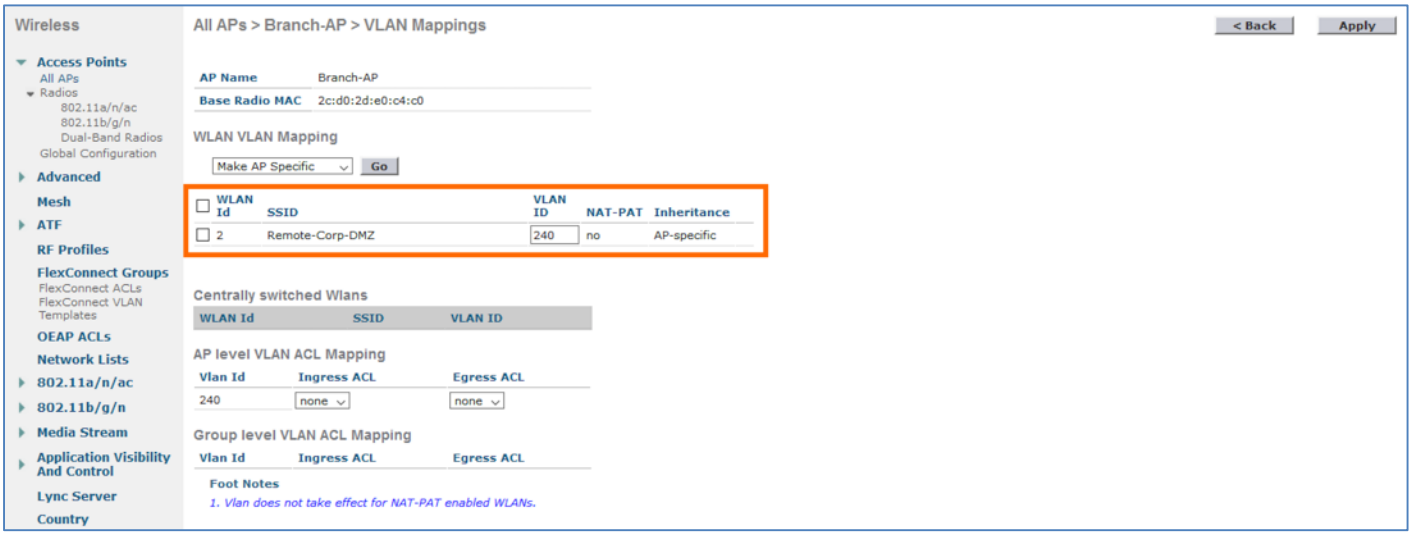
Step 3 Click the **AP name** for Details and from **General** Tab select the **AP mode** as **FlexConnect**



Step 4 Now switch to the **FlexConnect** tab and enable **VLAN support** and add the **Native VLAN ID** of that network



Step 5 Click **VLAN Mappings** to map the specific **WLAN VLAN mappings** used by the FlexConnect AP. Select the specific WLAN ID used by the AP and click **Apply**

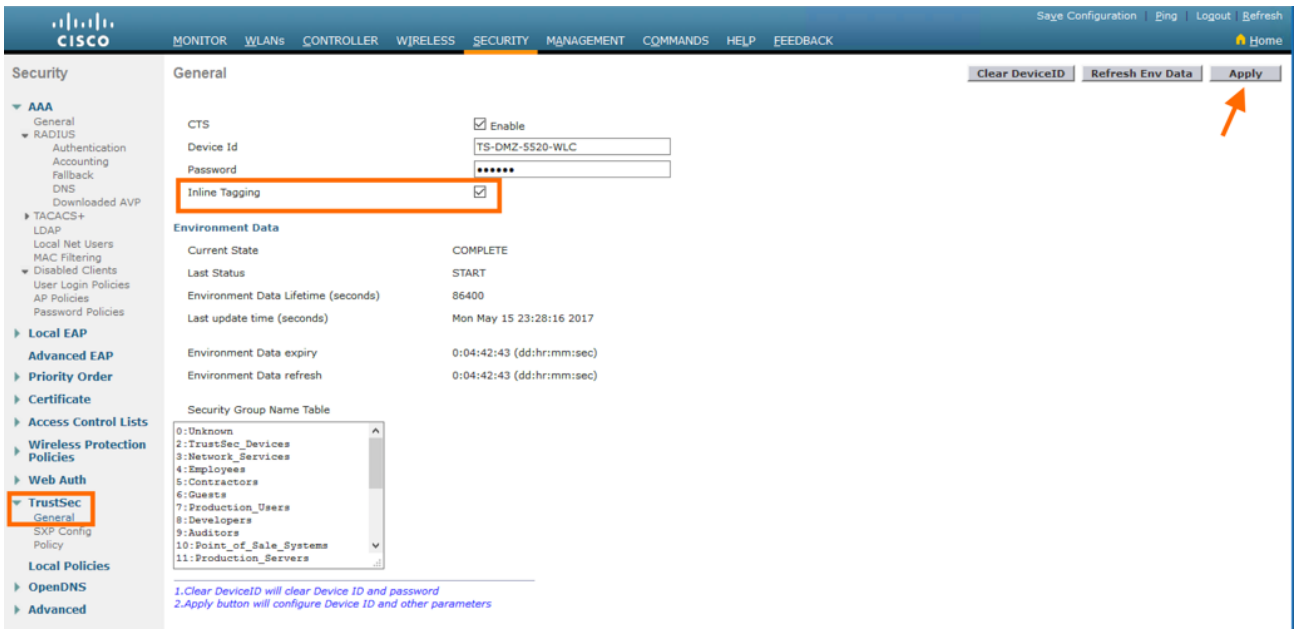


Inline Tagging configuration on WLC

Inline tagging functionality is a SGT propagation mechanism by which a wireless controller understands the source SGT (S-SGT). For Central Switching WLANs or for Centrally Switched packets, Wireless LAN Controller performs inline tagging for all packets sourced from wireless clients that reside on the WLC by tagging it with Cisco Meta Data (CMD) tag. Inline tagging also involves WLC stripping off the CMD header from the packet to learn the S-SGT tag. WLC then forwards the packet including the S- SGT for SGACL enforcement.

Note: For the FlexConnect SSIDs/WLANs Inline Tagging is enabled directly on the Access Point running in FlexConnect mode

Step 1 To enable Inline Tagging on the WLC navigate to **Security > TrustSec > General** and click the checkbox **Inline Tagging** and click **Apply**



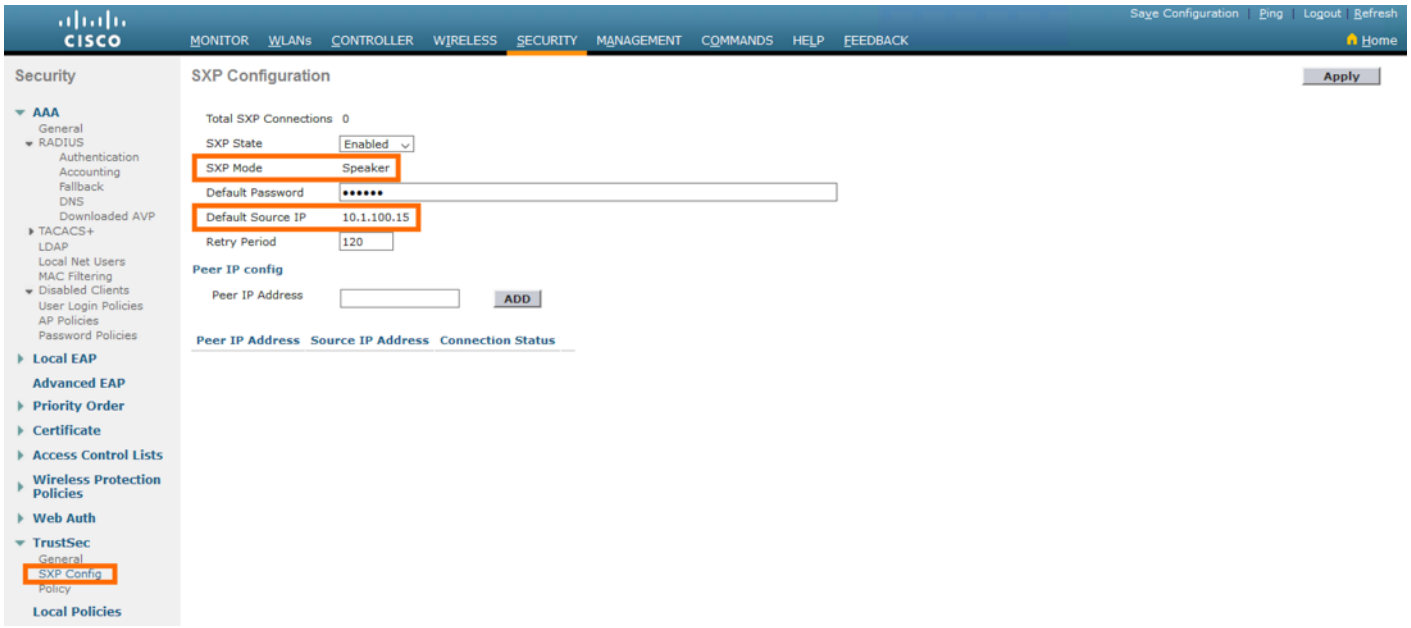
TrustSec SXP configuration on WLC

SXP is a control plane protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets natively on the Ethernet frame. SXP uses TCP as the transport protocol, and the TCP port 64999 for connection initiation. SXP uses Message Digest 5 (MD5) for authentication and integrity check. It has two defined roles—speaker (initiator) and listener (receiver).

Note: Wireless LAN Controller always operates in SXP Speaker mode. It supports SXPv2

Cisco TrustSec filters packets at the egress interface. During endpoint authentication, a host accessing the Cisco TrustSec domain (the endpoint IP address) is associated with an SGT at the access device through Dynamic Host Control Protocol (DHCP) snooping and IP device tracking. The access device transmits that association or binding through SXP to Cisco TrustSec hardware-capable egress devices. These devices maintain a table of source IP-to-SGT bindings. Packets are filtered on the egress interface by Cisco TrustSec hardware-capable devices by applying security group access control lists (SGACLs). SXP passes IP-to-SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.

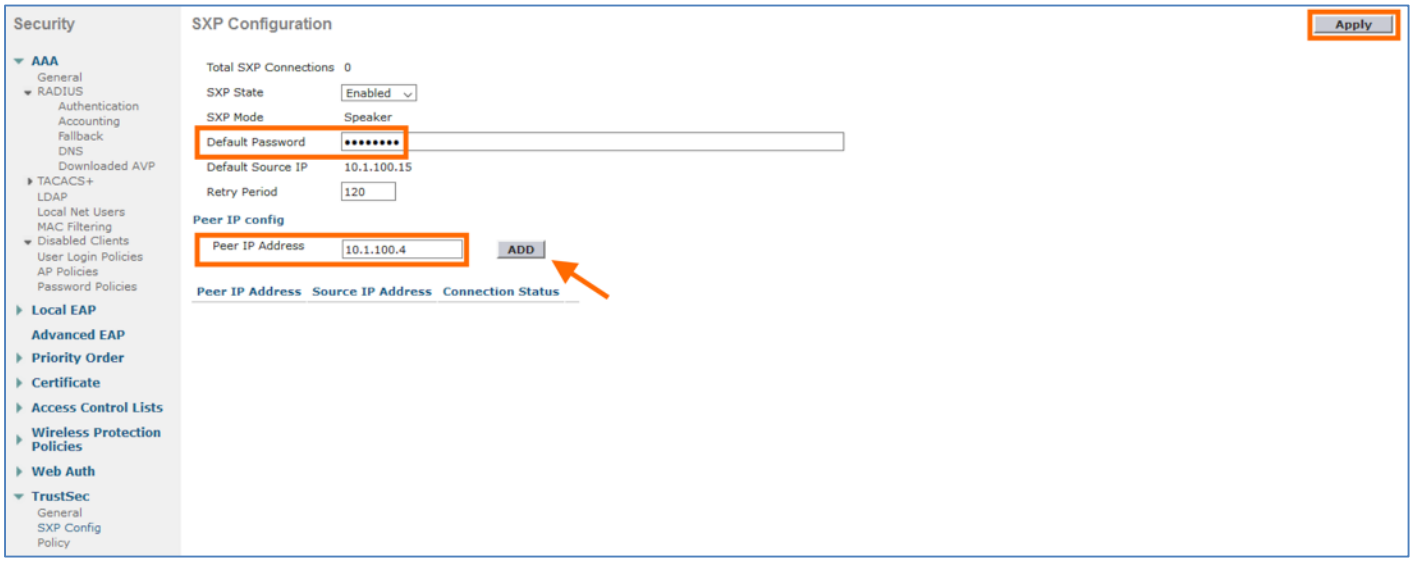
Step 1 To configure SXP on the controller navigate to **Security > TrustSec > SXP Config**. The page lists the SXP configuration details



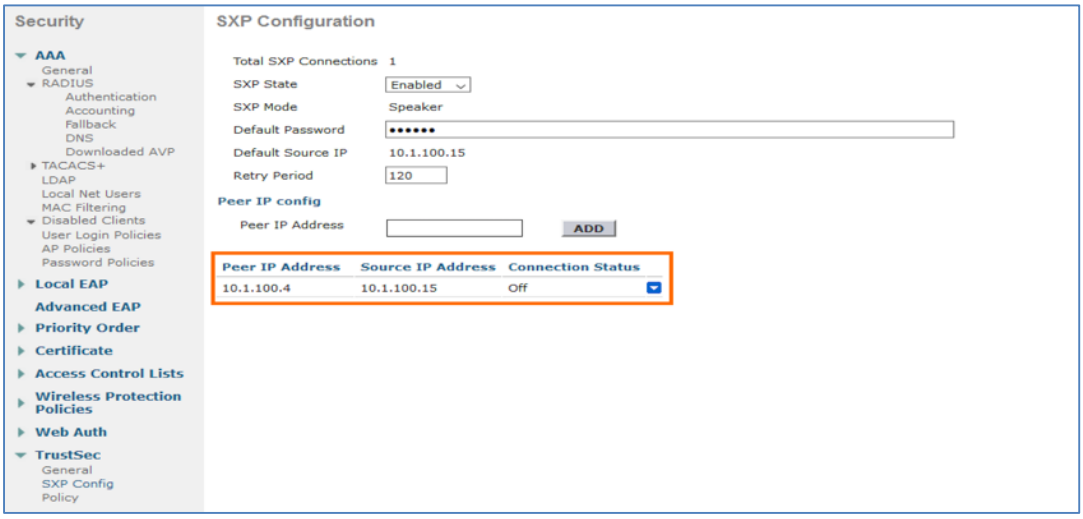
- **Total SXP Connections**—Number of SXP connections that are configured.
- **SXP State**—Status of SXP connections as either disabled or enabled.
- **SXP Mode**—SXP mode of the controller. The controller is always set to Speaker mode for SXP connections.
- **Default Password**—Password for MD5 authentication of SXP messages. We recommend that the password contain a minimum of 6 characters.

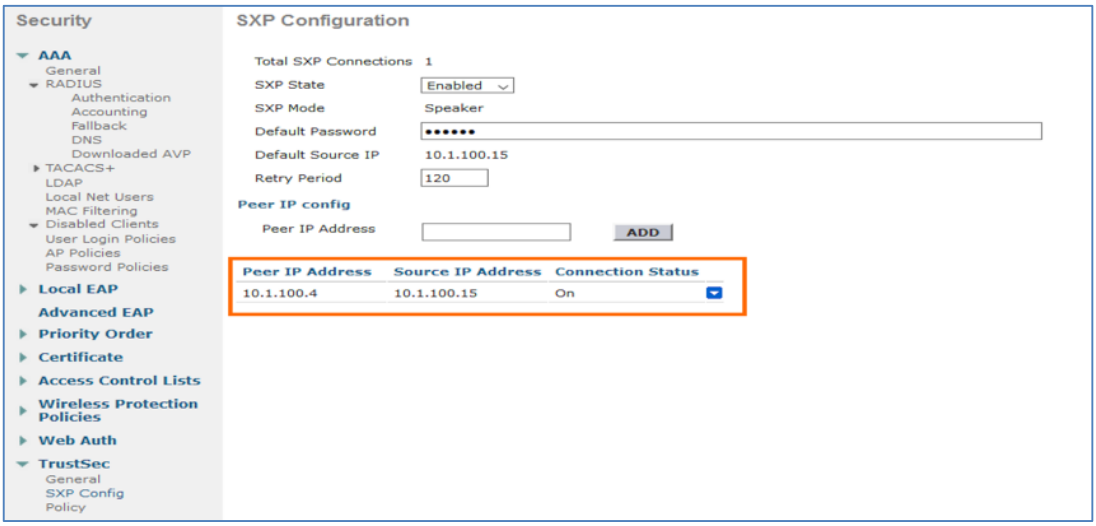
- **Default Source IP**—IP address of the management interface. SXP uses the default source IP address for all new TCP connections.
- **Retry Period**—SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000 seconds. The SXP retry period determines how often the controller retries for an SXP connection. When an SXP connection is not successfully set up, the controller makes a new attempt to set up the connection after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.
- **Peer IP Address**—The IP address of the peer, that is the IP address of the next hop switch to which the controller is connected. There is no effect on the existing TCP connections when you configure a new peer connection.
- **Source IP Address**—The IP address of the source, that is the management IP address of the controller.
- **Connection Status**—Status of the SXP connection.

Step 2 Add the **Default Password** and the **Peer IP address** to which the WLC can send the IP-SGT mappings and click **Apply**



Step 3 The **Connection Status** moves from **OFF** to **On** to form a successful SXP peering with the network device



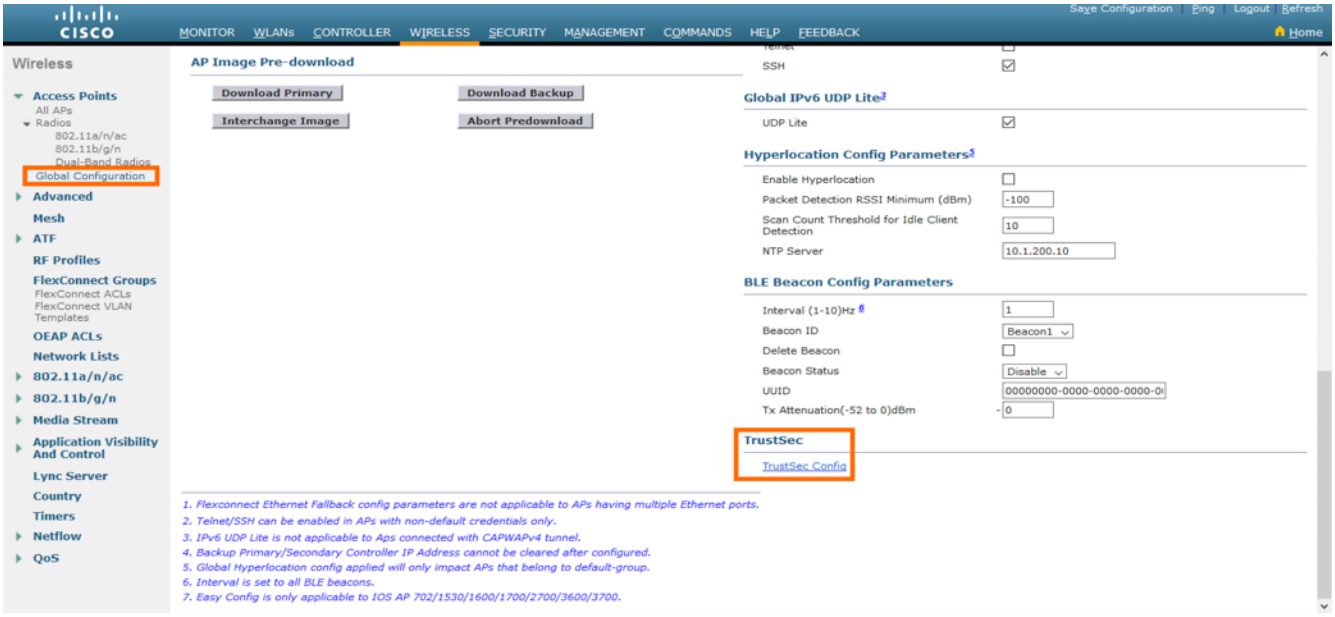


TrustSec Global configuration for Access Points on WLC

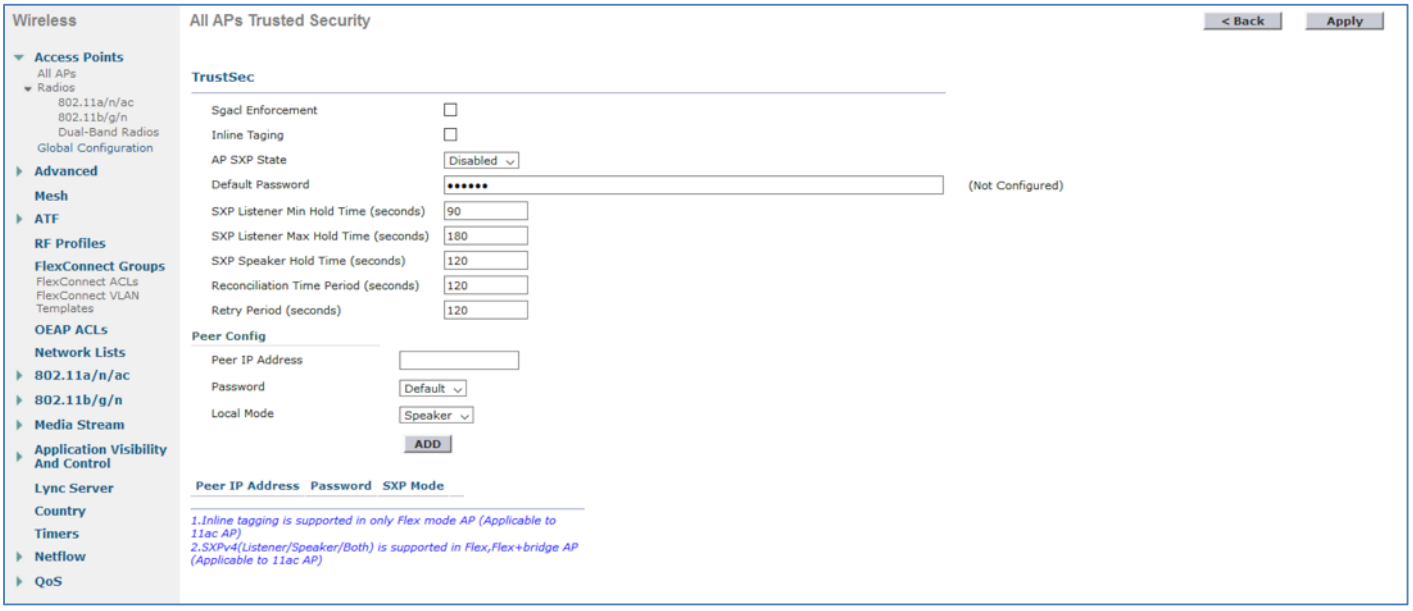
Wireless 8.4 allows an option to add TrustSec configuration globally for all the wireless access points. That includes SGACL enforcement, SXP configuration (SXPv4) and Inline Tagging.

Note: Inline Tagging and SXP configuration for an Access Point is allowed only on APs running FlexConnect mode

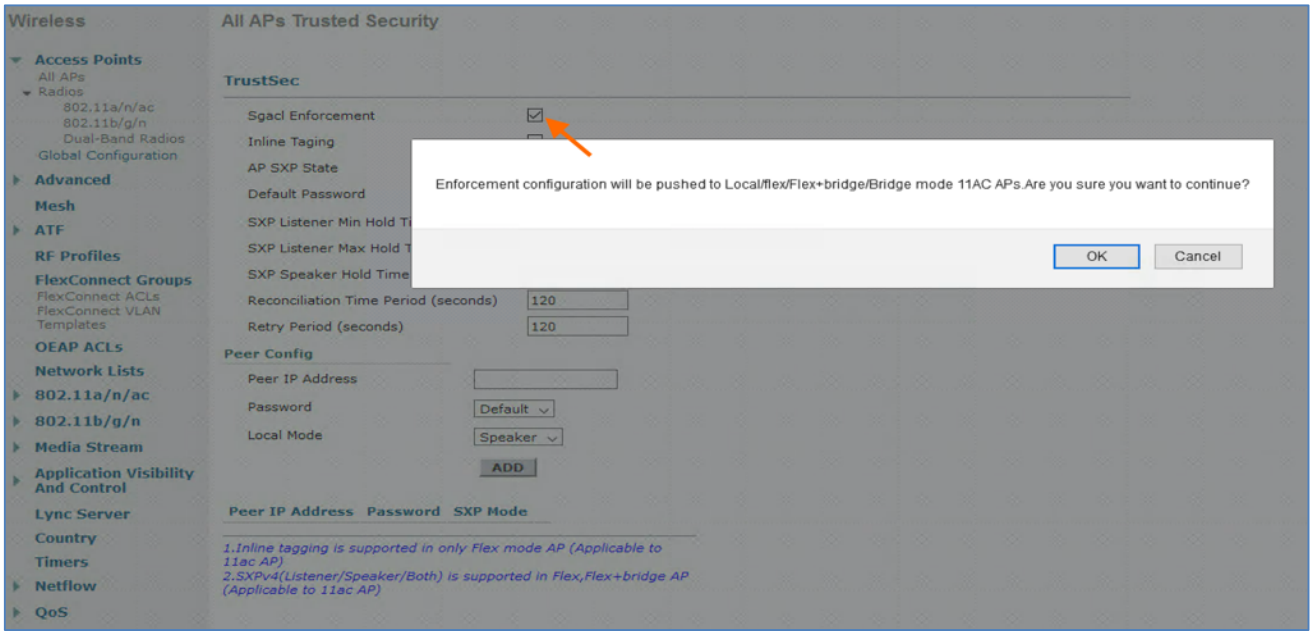
Step 1 From WLC navigate to **Wireless > Access Points > Global Configuration** and look for **TrustSec** and click **TrustSec Config** on the bottom right to add or modify any configuration



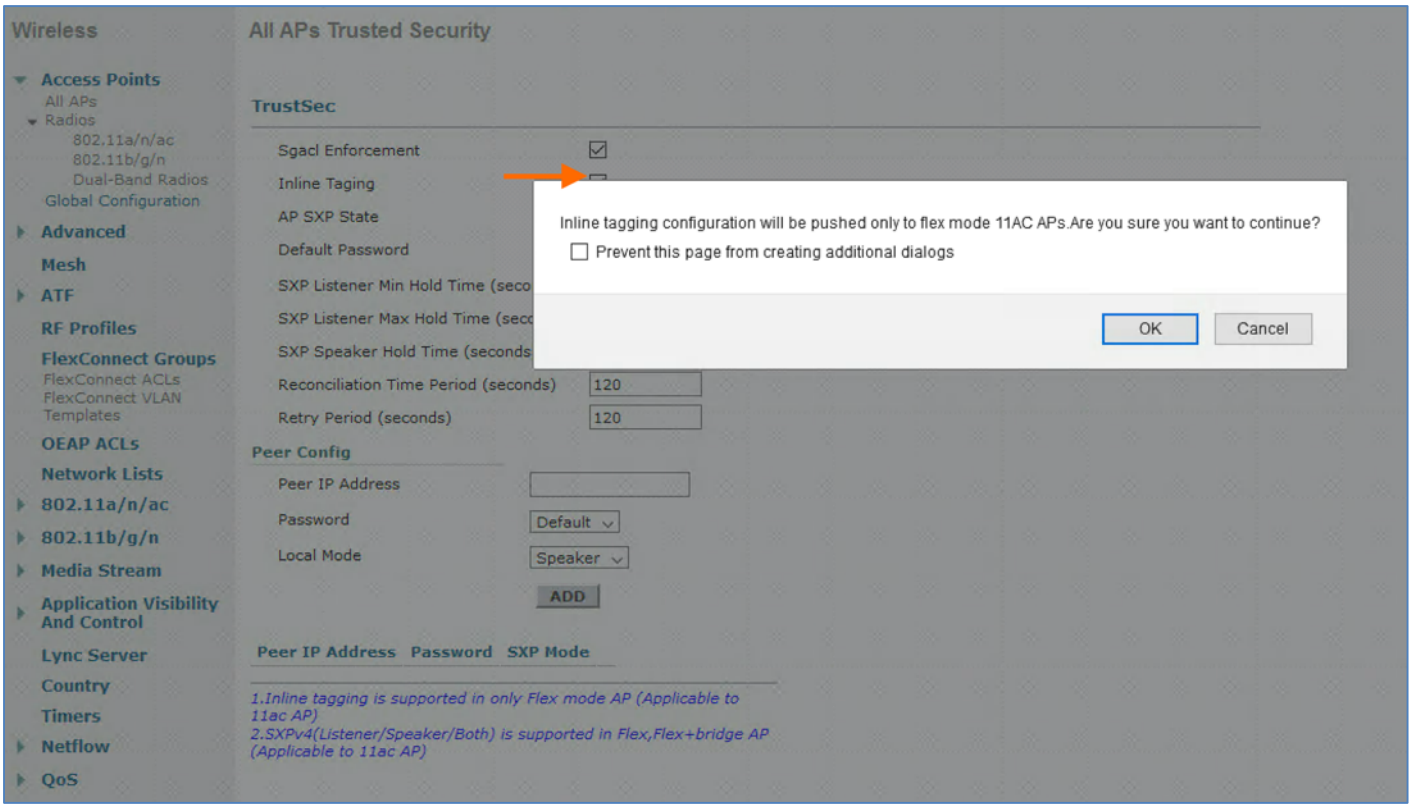
Step 2 TrustSec Configuration page would be displayed which provides the option to configure **SGACL Enforcement**, **Inline Tagging**, **SXP Peer Config**



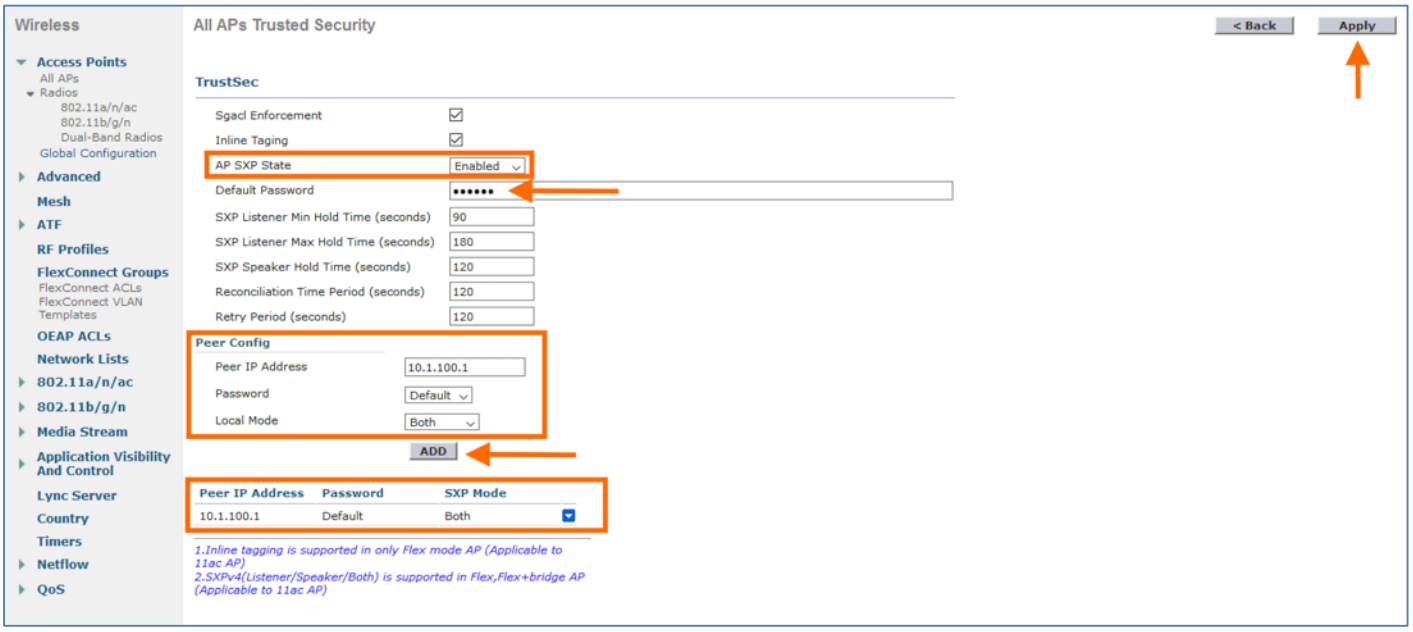
Step 3 Enable checkbox for **SGACL Enforcement** to push SGACL enforcement configuration to all the Access Points running both local as well as FlexConnect mode



Step 4 Enable checkbox for **Inline Tagging** to push Inline Tagging configuration to all the Access Points running FlexConnect mode



Step 5 Configure SXP settings of Access Points by enabling **AP SXP State**, Configure **Default Password**, **Peer IP Address** information and **Local Mode** of the APs and click **ADD** and **Apply** to save



The above SXP configuration would only be pushed to the Access Points running in FlexConnect mode.

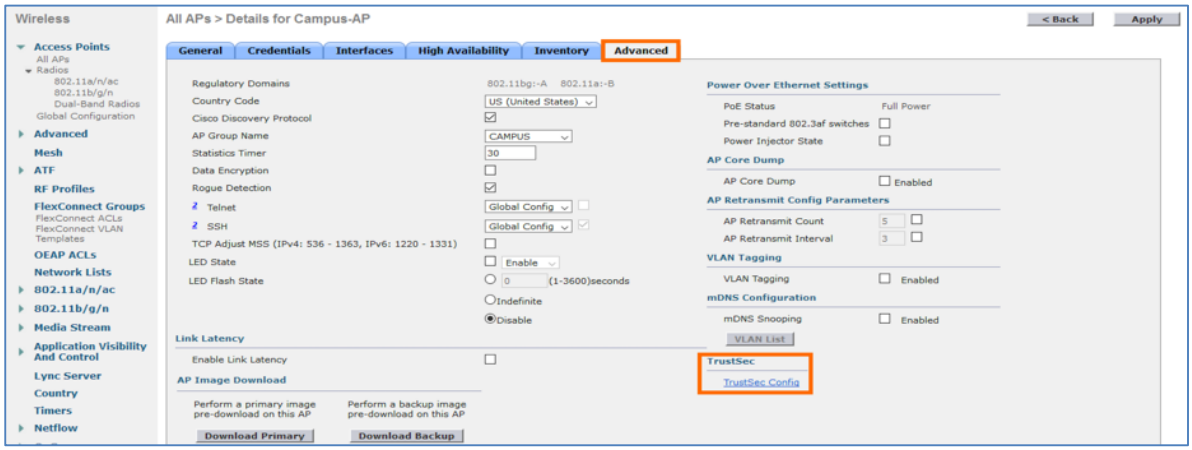
Access Point Specific TrustSec configuration on WLC

Instead of configuring TrustSec globally for all the wireless access points you also have an option to configure Access Point specific TrustSec configuration. That would overwrite the global configuration added before on the Wireless LAN Controller. Local mode AP only allows SGACL enforcement whereas FlexConnect AP allows Inline Tagging and SXPv4 along with enforcement.

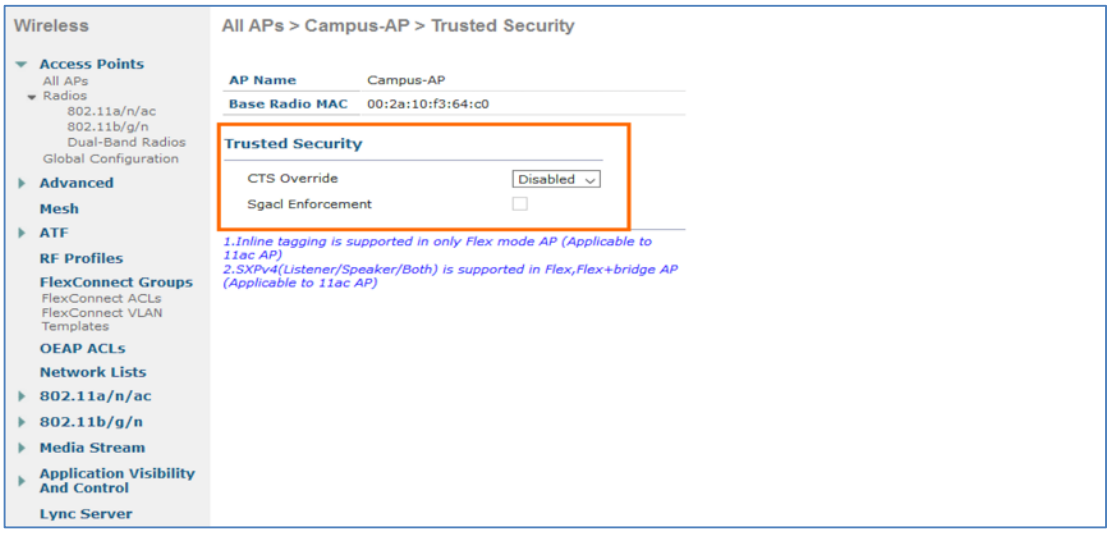
Step 1 From WLC navigate to **Wireless > Access Points** for all the APs connected to the WLC

Step 2 Click on the **AP Name** for the Access Point **Details**

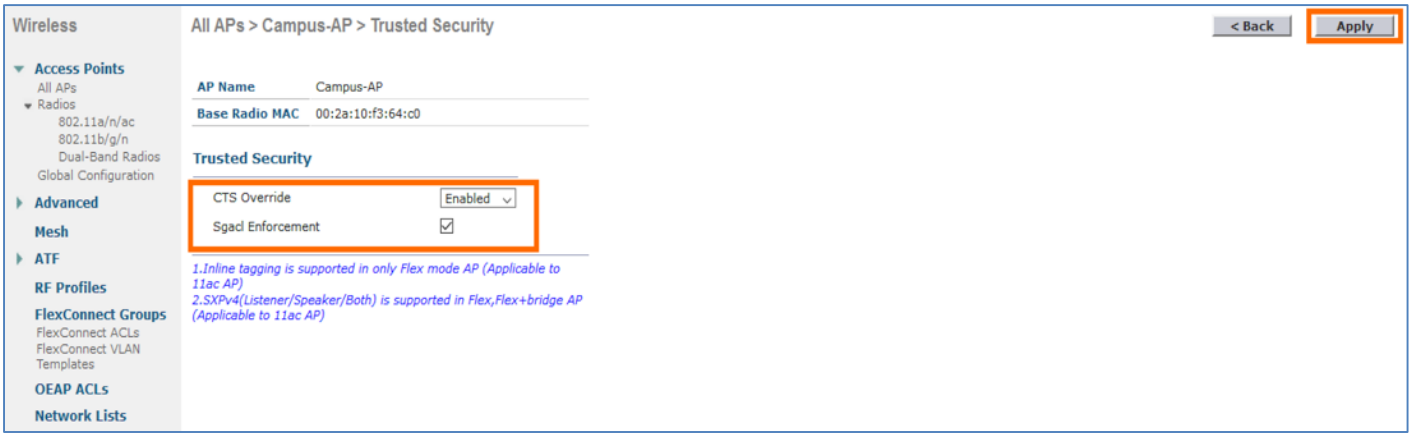
Step 3 In the AP Details click **Advanced** to go to **TrustSec** and **TrustSec Config** seen on the bottom right



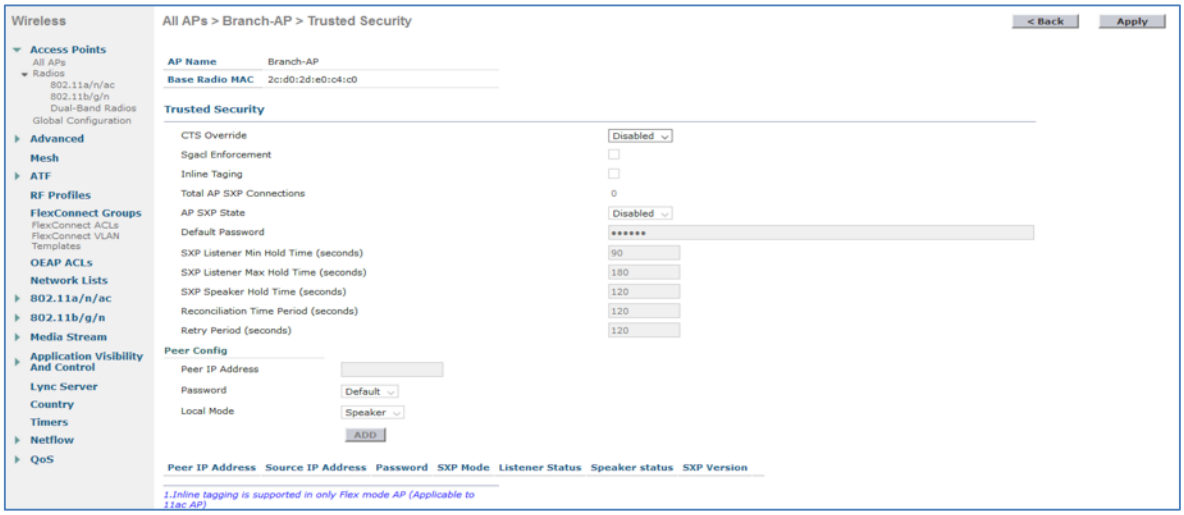
Step 4 For an Access Point running in Local mode have option for **CTS Override** and **SGACL Enforcement**



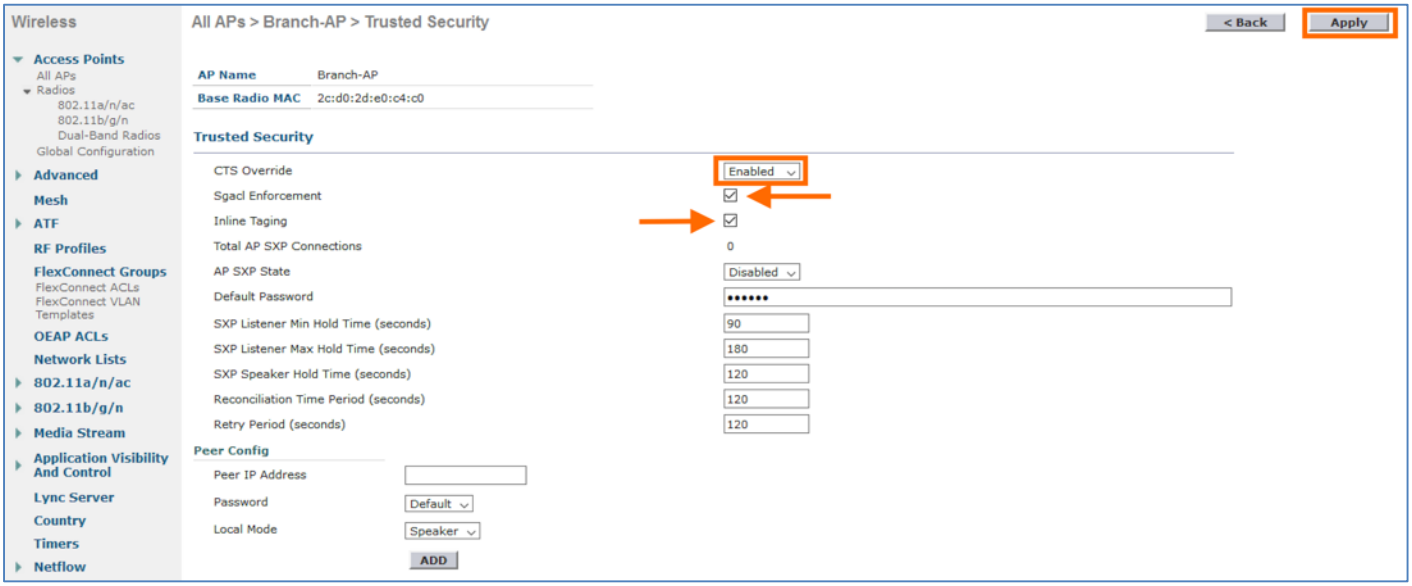
Step 5 To modify click the drop down to enable **CTS Override** and click on the checkbox to enable **SGACL Enforcement** and **Apply**



Step 6 For an Access Point running in FlexConnect mode have additional options to enable **Inline Tagging** and **SXP** configuration along with **CTS Override** and **SGACL Enforcement**

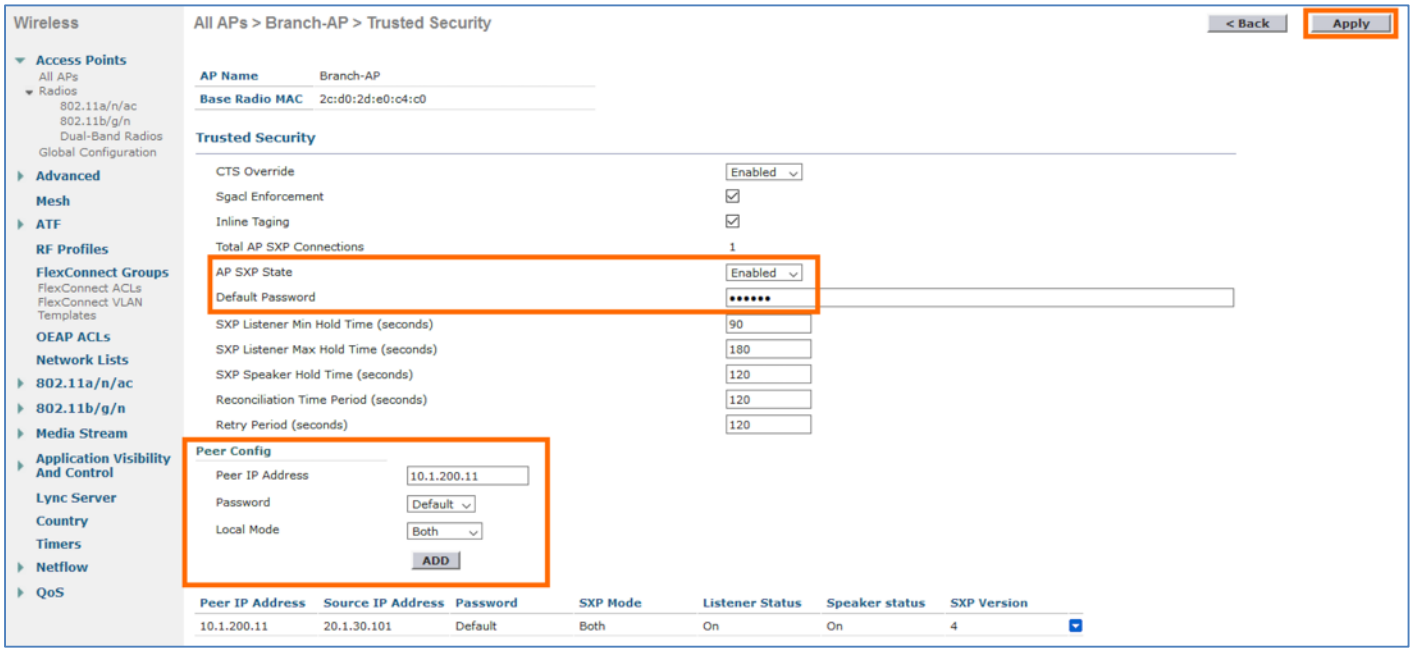


Step 7 To modify click the drop down to enable **CTS Override** and click on the checkbox to enable **SGACL Enforcement** and also **Inline Tagging** and click **Apply**

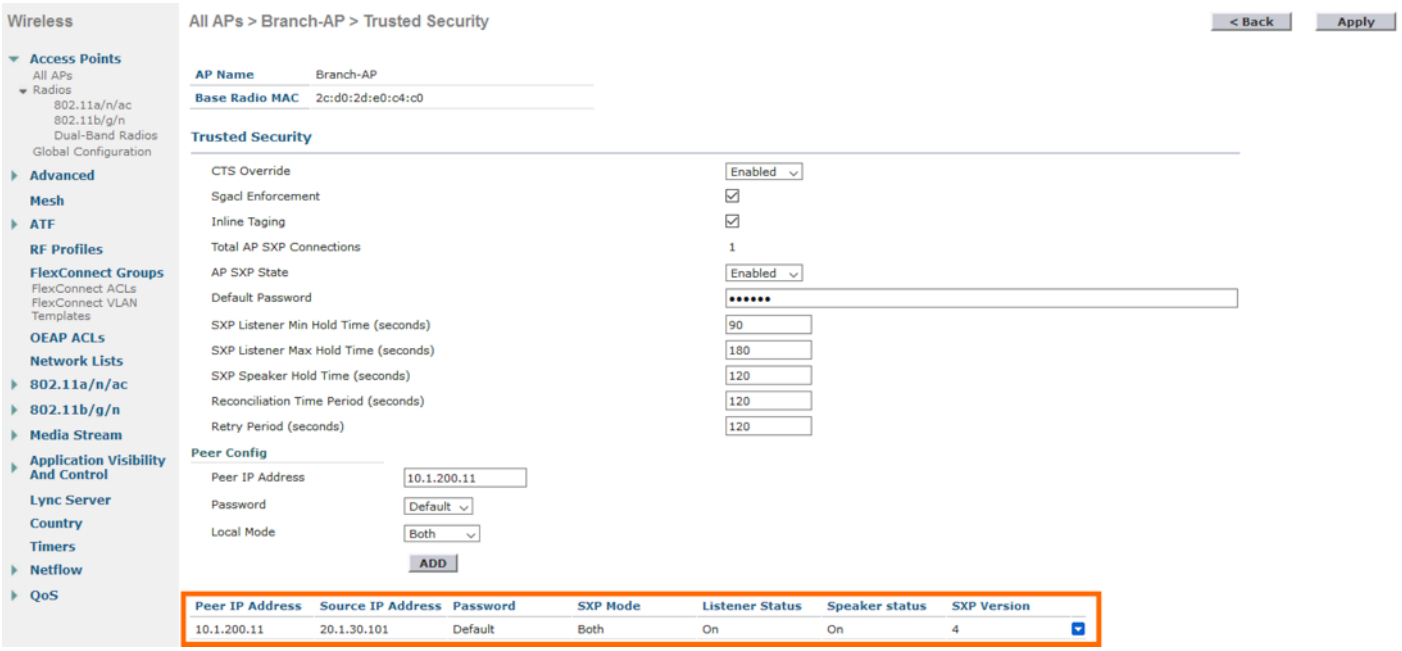


Step 8 Configure SXP settings on the Access Point by clicking the drop down to enable **AP SXP State** and add the **Default Password**.

Step 9 Under **Peer Config** add the **Peer IP Address** information, Password either **Default/None** and **Local Mode** of the AP with either **Speaker/Listener/Both** and click **ADD** and **Apply** to save it



Depending on the **SXP Mode** the respective status of SXP peer for **Speaker/Listener** or **Both** would move from **Off** to **On**.



Switch Interface Configuration for TrustSec

The Wireless LAN Controller and Access Points would be connected to the Switch Ports in general for network connectivity. The following section will show the basic Switch Port configuration of the physical interfaces where controller and AP is connected to. Apart from that, this section also shows Inline Tagging configuration needed on the physical interfaces where WLC and FlexConnect AP is connected along with SXPv4 peer configuration between the FlexConnect AP and Network Access Device (NAD).

Switch Port Configuration Connected to WLC

Below is the interface configuration of the switch port where the WLC is connected.

```
description "Connected to 5520-WLC"
switchport trunk native vlan 100
switchport mode trunk
```

Management interface IP address of the WLC would be from **VLAN 100** network

Switch Port Configuration of Local Mode AP and FlexConnect AP

Below is the interface configuration of the switch port where the Access Point running in Local mode is connected.

```
description "Connected to Local Mode Campus-AP"
switchport trunk native vlan 30
switchport mode trunk
spanning-tree portfast trunk
```

IP address of the Local Mode Access Point would be from **VLAN 30** network

Below is the interface configuration of the switch port where the Access Point running in FlexConnect mode

```
description "Connected to FlexConnect Branch-AP"
switchport trunk native vlan 230
switchport mode trunk
spanning-tree portfast trunk
```

IP address of the FlexConnect Access Point would be from **VLAN 230** network

Switch Port Configuration of WLC interface for Inline Tagging

Below is the interface configuration of the switch port where the WLC is connected and Inline Tagging being enabled on the trunk interface

```
description "Connected to 5520-WLC"
switchport trunk native vlan 100
switchport mode trunk
cts manual
  policy static sgt 2 trusted
```

CTS Manual enables TrustSec Inline Tagging on the trunk interface with manual mode of operation. **Policy static SGT 2 trusted** command allows static SGT ingress policy on the interface and defines the trustworthiness of an SGT received on the interface. With the **trusted** keyword the SGT value received in the Ethernet packet on this interface is trusted and will be used by the device for any SG-aware policy enforcement or for purpose of egress-tagging and it wouldn't override with the configured SGT value (2).

Since adding SGT value in the Ethernet frame would have an additional overhead it is recommended to increase the interface MTU value on the Inline Tagging enabled interfaces. Some of the network infrastructure would support this Baby Giant frames (jumbo) but it is highly recommended to adjust the MTU value at least on the interfaces where the WLC and APs are connected.

```
system mtu 1600
system mtu jumbo 1600
```

The default MTU value is 1500. The above commands once added would change the MTU value to 1600 on the interfaces but it is recommended to reload the switch for those commands to take effect.

Note: Some of the platforms would require "system mtu jumbo 1600" to change the MTU value on the Gig and TenGig interfaces

Switch Port Configuration of AP interface for Inline Tagging

Below is the interface configuration of the switch port where the FlexConnect Access Point is connected and Inline Tagging being enabled on the trunk interface.

```
description "Connected to FlexConnect Branch-AP"
switchport trunk native vlan 230
switchport mode trunk
spanning-tree portfast trunk
cts manual
  policy static sgt 2 trusted
```

It is required to adjust the MTU value as recommended earlier in this section on the interface AP is connected. Below is a sample configuration of a Gig interface with the adjusted MTU.

```
GigabitEthernet1/0/24 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 78da.6e3a.f418 (bia 78da.6e3a.f418)
  Description: "Connected to FlexConnect Branch-AP"
  MTU 1600 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
```

SXP Peer Configuration Connected to AP

Cisco Wireless Access Points (both Wave1 and Wave2) running in FlexConnect mode supports SXPv4 propagation. SXPv4 allows SXP speaker role, SXP listener role and Both (SXP Speaker and Listener) modes of operation. It helps in Loop detection and prevention with a built-in Keep Alive mechanism. Cisco Access Points from branch offices can now learn and share Security Group membership information over an SGT eXchange Protocol (SXP) connection from switches, routers, and firewalls to simplify access control list management and firewall rule management elsewhere in the network and even do enforcement locally from the learned mappings for wireless access control management providing software-defined segmentation. Below is a sample peer SXPv4 configuration of both IOS switch and NX-OS switch.

```
cts sxp enable
cts sxp default password <####>
cts sxp default source-ip 10.1.100.1
cts sxp connection peer 20.1.30.101 password default mode local both
```

20.1.30.101 is the FlexConnect AP IP Address and 10.1.100.1 is the IP Address of the peer, which is an IOS device.

```
cts sxp enable
cts sxp node-id interface mgmt0
cts sxp default password <####>
cts sxp default source-ip 10.1.200.11
cts sxp connection peer 20.1.30.101 password default mode both vrf management
```

20.1.30.101 is the FlexConnect AP IP Address and 10.1.200.11 is the IP Address of the peer, which is an NX-OS device.

Use Cases on SGACL Enforcement on Access Points

Wireless Access Points running in both Local/FlexConnect mode now supports SGACL enforcement. This would help in reducing the Malware propagation on wireless clients by blocking the Lateral movement. That is East-West wireless segmentation using TrustSec. Earlier wireless releases would implement East-West segmentation (P2P) by forwarding the wireless traffic to an upstream switch for enforcement. SGACL enforcement on the APs would simplify TrustSec segmentation for wireless as it removes the need of an upstream device (switch).

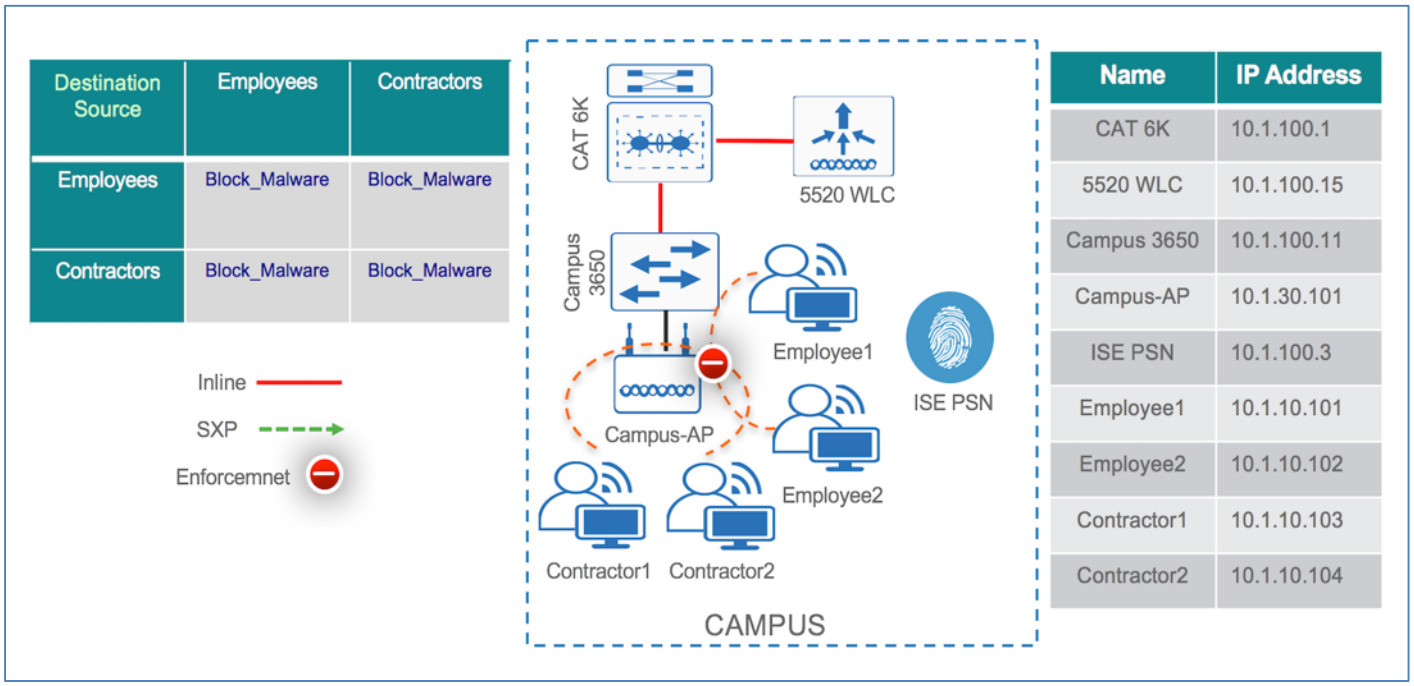
Note: These use cases below are just for your reference.

East-West Segmentation using SGACL enforcement on Local Mode AP

This use case will walk you through the basic configuration to do East-West segmentation or micro-segmentation in the campus using SGACL enforcement on the Access Point running Local Mode. When a wireless client is authenticated to the network, Cisco Identity Service Engine (ISE) would push a Dynamic Security Group Tag based on the Authorization Profile configured on ISE. Client classification happens at ingress by ISE that assigns a unique S-SGT to the wireless client based on client identity. Wireless LAN Controller now receives the SGT associated with the wireless client. WLC will treat client SGT as D- SGT and initiate download of SGACL policy names for the destination from ISE. The SGACL policies downloaded will be all possible / known S-SGTs paired with the specific client D-SGT. Once the Wireless LAN Controller downloads SGACLs from ISE, it caches and pushes the SGACL policies associated with the D-SGT to the Access Point. Enforcement enabled Access Point only receives the policies of the client Security Groups which are associated to the AP. Successful enforcement can be validated directly on the Access Point with the SGACL counters.

Note: The below usecase covers SGACL enforcement only for the clients associated to a single AP. Inline Tagging needed to be enabled on the WLC to enforce the policy between the wireless clients connected to multiple Local Mode Access Points.

Figure 2: Topology showing a wireless deployment in campus with SGACL enforcement on AP running Local mode



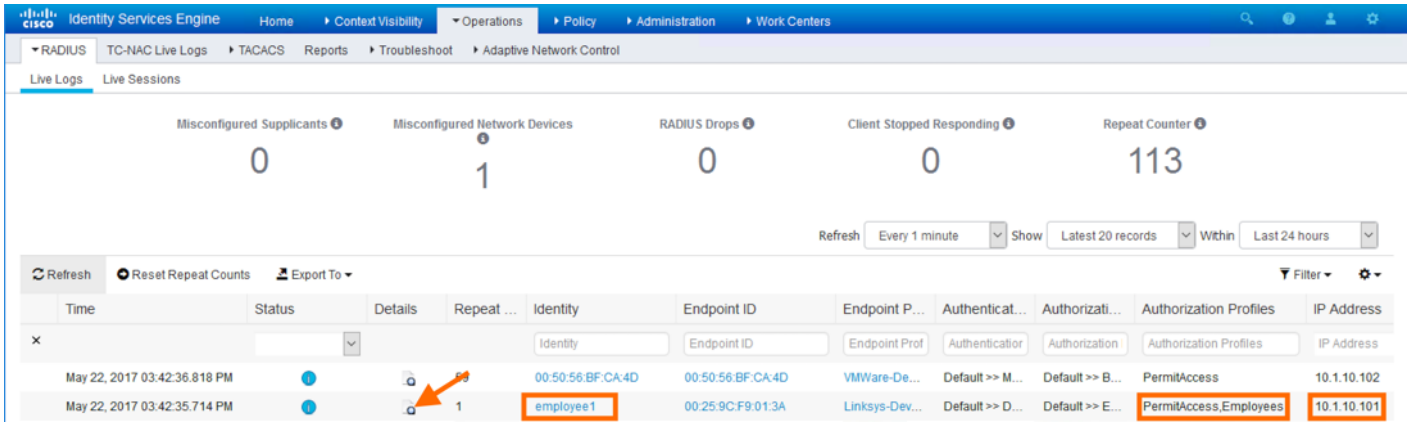
The above topology shows four users Employee1, Employee2, Contractor1 and Contractor2 from Campus connected on a wireless network to a Local Mode Access Point. The AP (Campus-AP) physically connected to a wired switch (Campus 3650) is associated to the WLC (5520 WLC) over CAPWAP. As soon as the endpoints connect to the network they would be authenticated and authorized by cisco ISE and would be assigned an SGT dynamically based on their role. The Access Point would have the IP-SGT binding information locally for those associated clients. WLC downloads the SGACL policies (Block_Malware) from ISE and would push those SGACLs (shown in the topology) to the AP (Campus-AP). By looking at the Source and Destination Group Tag and the downloaded SGACL policy (Block_Malware), AP (Campus-AP) would enforce the policy and would block the malware propagation between the Employees and Contractors.

Note: The basic ISE configuration and WLC configuration is not covered here as it was already shown in the above sections.

Step 1 Connect the **Employee1** PC to the wireless SSID in Campus

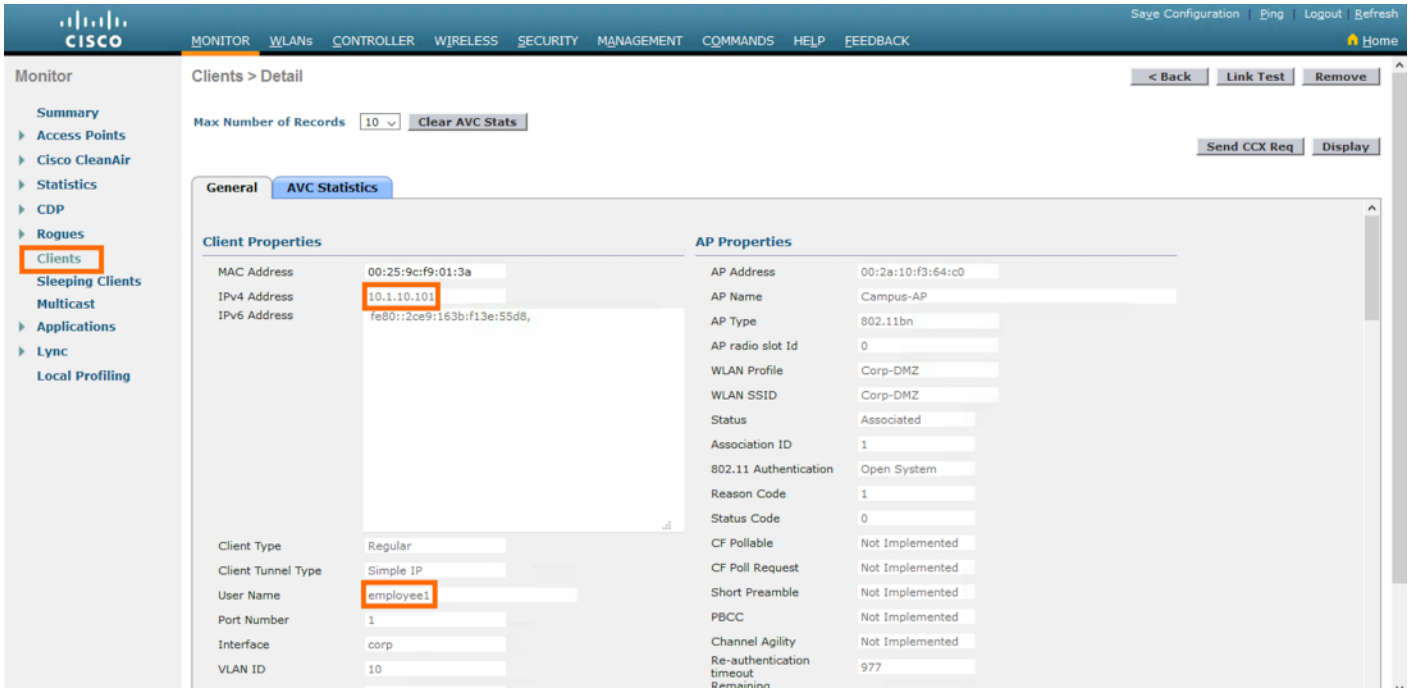
Step 2 The user **Employee1** would be assigned an **Employees SGT** (**4**) dynamically as per the Authorization policy configuration earlier during the ISE configuration

Step 3 Once connected hop on to ISE and navigate to **Operations > RADIUS > Live Logs** to see the endpoint details. Click on the **Details** icon below for all the session related information.

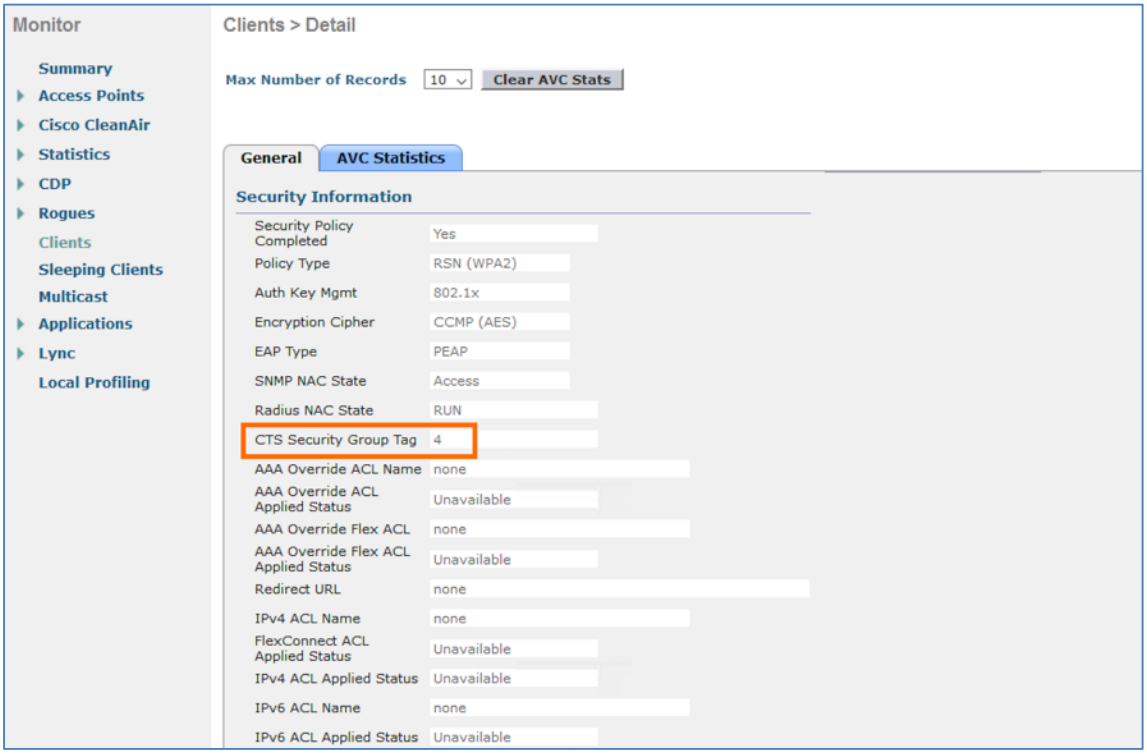


Step 4 The **Live Logs Details** shows the all the endpoint details including the associated Security Group for that endpoint

Step 5 To validate the Security Group assignment of the client **Employee1** on the WLC navigate to **Monitor > Clients** and click on **Client MAC Addr** for the details



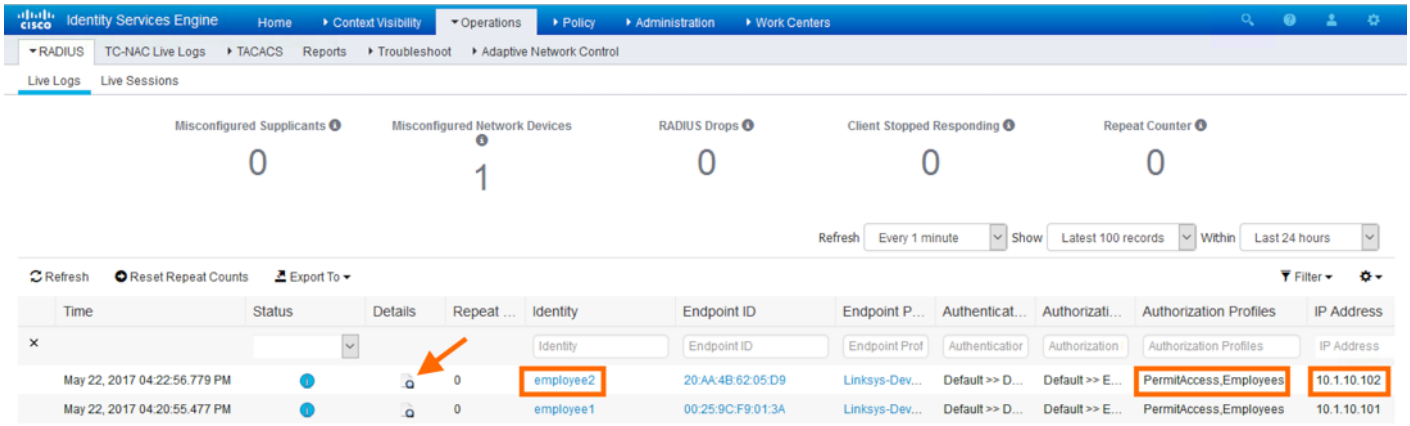
Step 6 Scroll down and look at the **Security Information** for the **CTS Security Group Tag** assigned to the client Employee1, which is **4** (**Employees**)



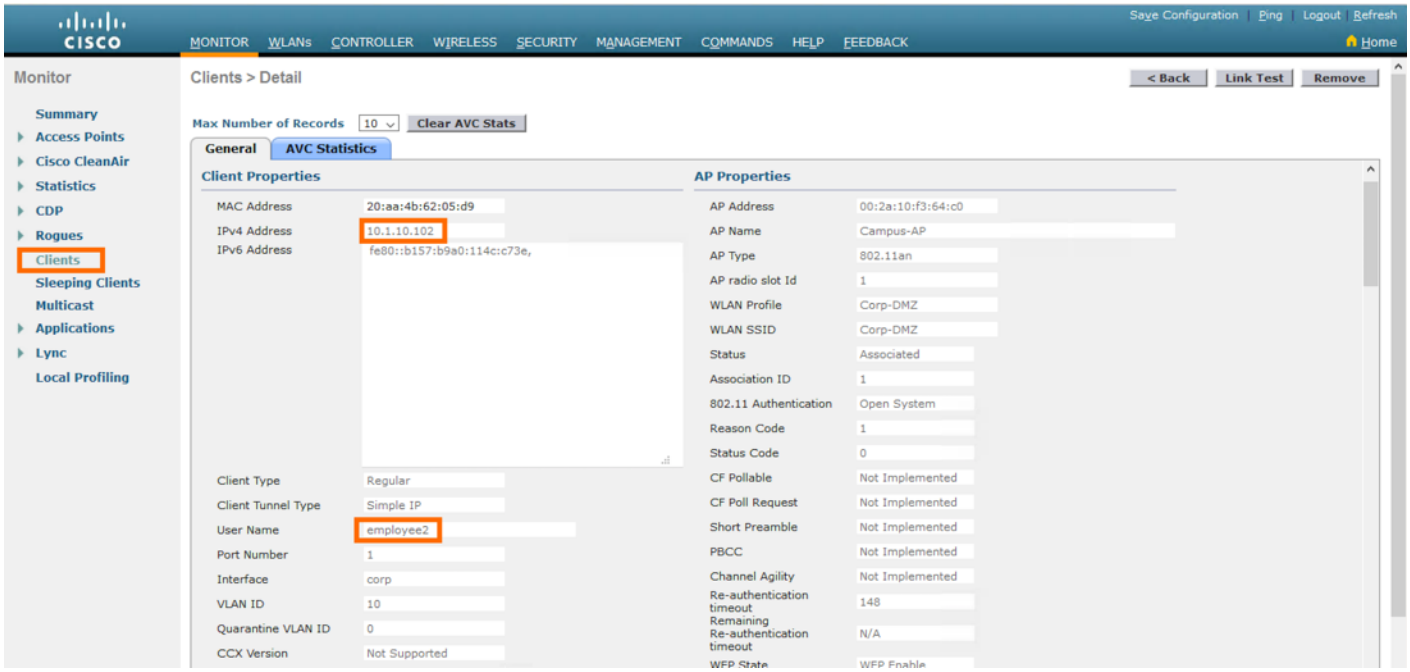
Step 7 Now connect the **Employee2** PC to the wireless SSID in Campus

Step 8 The user **Employee2** would be assigned an **Employees SGT** (**4**)

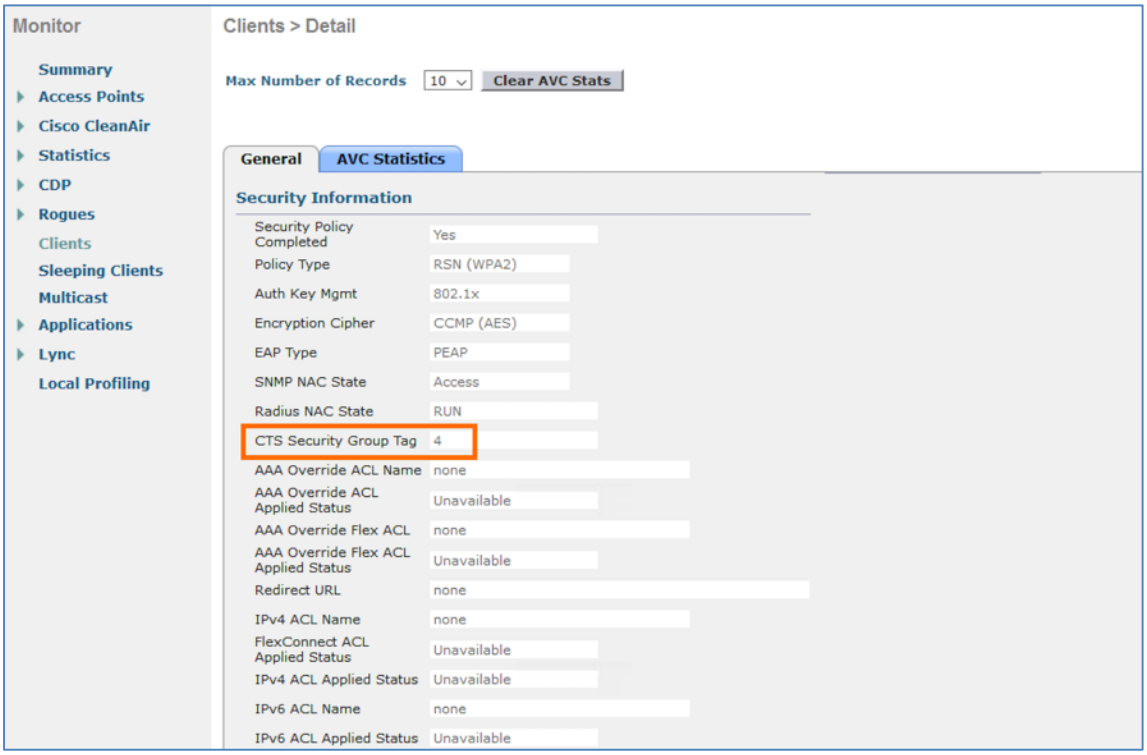
Step 9 On ISE and navigate to **Operations > RADIUS > Live Logs** to see the endpoint details. Click on the **Details** icon below for all the session related information.



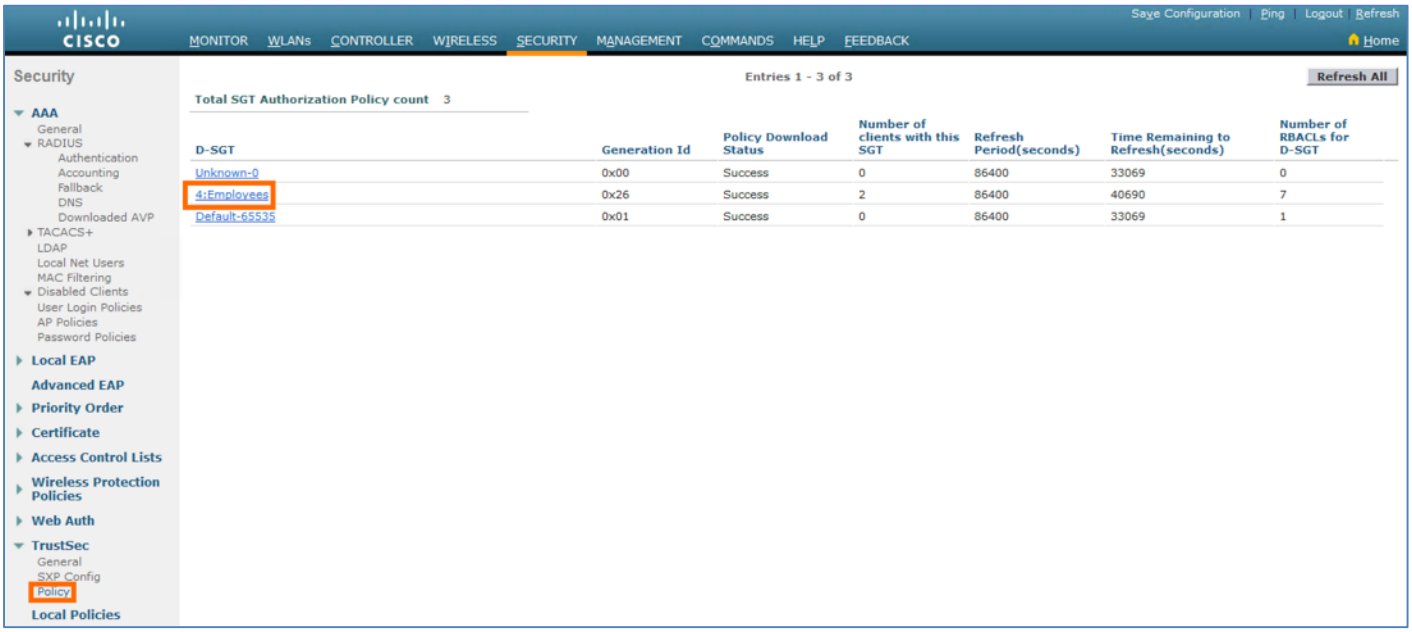
Step 10 To validate the Security Group assignment of the client **Employee2** on the WLC navigate to **Monitor > Clients** and click on **Client MAC Addr** for the details



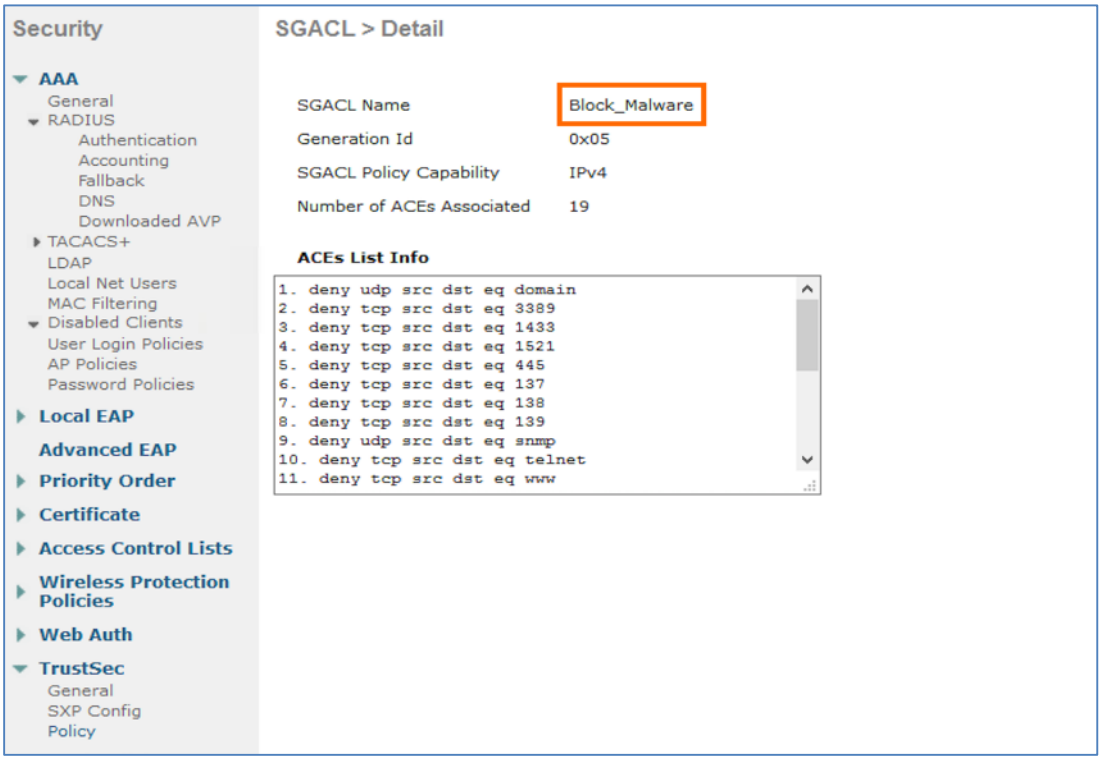
Step 11 Scroll down and look at the **Security Information** for the **CTS Security Group Tag** assigned to the client **Employee2**, which is **4** (**Employees**)



Step 12 Now from the WLC navigate to **Security > TrustSec > Policy** to see the newly downloaded SGACL policies on the WLC for the **Employees** Security Group



Step 13 Click on the **D-SGT** name **Employees** for the **BLOCK_MALWARE** SGACL pushed from ISE between **Employee** Security Groups (S-SGT and D-SGT)



Step 14 Now look for the IP-SGT binding information on Access Point using the below command. The endpoints, which are connected to the **Campus-AP** that got a SGT would be seen below

```
Campus-AP#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
         IP SGT SOURCE
10.1.10.101   4  LOCAL
10.1.10.102   4  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::2ce9:163b:f13e:55d8   4  LOCAL
fe80::b157:b9a0:114c:c73e   4  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
Campus-AP#
```

Step 15 To verify the SGACL permissions between the S-SGT and the D-SGT use the below command on the Access Point

```
Campus-AP#show cts role-based permissions
IPv4 role-based permissions:
  SGT   DGT           ACL
    4     4 Block_Malware
    5     4 Block_Malware
    9     4    Allow_ICMP
   11     4     Permit_IP
   12     4     Permit_IP
   14     4       Deny_IP
   16     4     Permit_IP
65535 65535     Permit_IP

IPv6 role-based permissions:
  SGT   DGT       ACL
   11     4 Permit_IP
   12     4 Permit_IP
   14     4   Deny_IP
   16     4 Permit_IP
65535 65535 Permit_IP

Campus-AP#
```

Block_Malware SGACL is downloaded to the AP and that would be invoked between the **Employees** (**4**) Security Group

Step 16 Use the following CLI command on the Access Point to verify the **SGACL** content and the **Access Control Entries** (ACEs)

```
Campus-AP#show cts access-lists
IPv4 role-based ACL:
Allow_ICMP
        rule 0: allow true && ip proto 1
Block_Malware
        rule 0: deny true && ip proto 17 && ( dst port 53 )
        rule 1: deny true && ip proto 6 && ( dst port 3389 )
        rule 2: deny true && ip proto 6 && ( dst port 1433 )
        rule 3: deny true && ip proto 6 && ( dst port 1521 )
        rule 4: deny true && ip proto 6 && ( dst port 445 )
        rule 5: deny true && ip proto 6 && ( dst port 137 )
        rule 6: deny true && ip proto 6 && ( dst port 138 )
        rule 7: deny true && ip proto 6 && ( dst port 139 )
        rule 8: deny true && ip proto 17 && ( dst port 161 )
        rule 9: deny true && ip proto 6 && ( dst port 23 )
        rule 10: deny true && ip proto 6 && ( dst port 80 )
        rule 11: deny true && ip proto 6 && ( dst port 443 )
        rule 12: deny true && ip proto 6 && ( dst port 22 )
        rule 13: deny true && ip proto 6 && ( dst port 110 )
        rule 14: deny true && ip proto 6 && ( dst port 123 )
        rule 15: deny true && ip proto 6 &&  tcp opt !ack &&  tcp opt fin &&
tcp opt !psh &&  tcp opt !rst &&  tcp opt !syn &&  tcp opt !urg
        rule 16: deny true && ip proto 6 &&  tcp opt fin &&  tcp opt psh &&
tcp opt urg
```

```
        rule 17: allow true && ip proto 1
        rule 18: allow true && ip proto 6 &&  tcp opt ack ||  tcp opt syn
Permit_IP
        rule 0: allow true
Deny_IP
        rule 0: deny true

IPv6 role-based ACL:
Permit_IP
        rule 0: allow true
Deny_IP
        rule 0: deny true

Campus-AP#
```

Step 17 Ping the **Employee2** IP address from **Employee1** PC

```
C:\Users\employee1>ping 10.1.10.102

Pinging 10.1.10.102 with 32 bytes of data:
Reply from 10.1.10.102: bytes=32 time=4ms TTL=125
Reply from 10.1.10.102: bytes=32 time=3ms TTL=125
Reply from 10.1.10.102: bytes=32 time=7ms TTL=125
Reply from 10.1.10.102: bytes=32 time=5ms TTL=125

Ping statistics for 10.1.10.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 4ms

C:\Users\employee1>
```

Ping should succeed as the **Permit ICMP** is enabled in the SGACL. Similarly, if you would try to access the Employee2 PC through any other port (ex: 137 etc..) then the access would be denied.

Step 18 Validate the **SGACL enforcement** on the Access Point through the **SGACL Counters** command. To check the counters between the **Employees** Security Group (**4**) use the following command on AP.

```
Campus-AP#show cts role-based counters from 4 to 4
IPv4 ACL: Block_Malware
Packets Allowed : 4
Packets Denied  : 5

Campus-AP#
```

Deny counters (Packets Denied) are incremented above due to the Port Scan on Employee2 PC on port 137 and port 138.

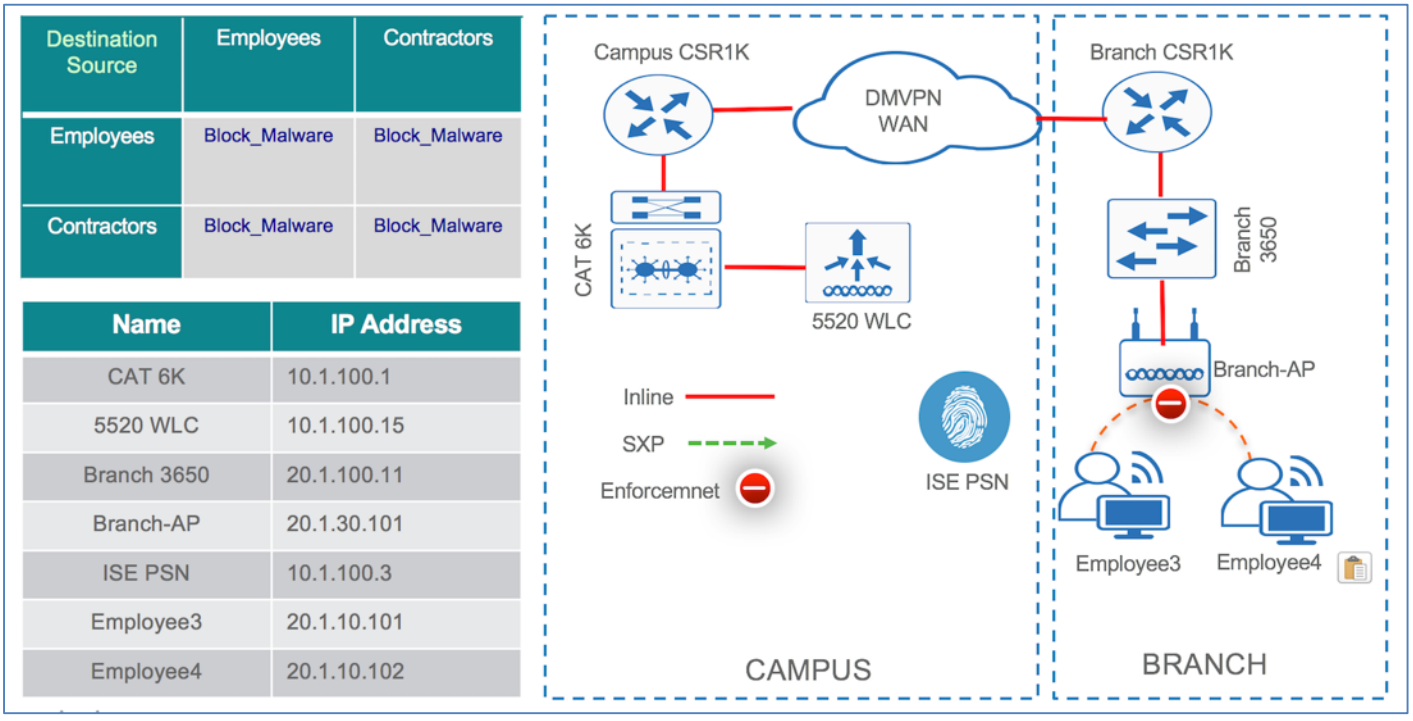
Note: Similarly, repeat all the steps above to enforce the policy between the Contractors and Employees or between the Contractors. The above steps only covered the enforcement between the employees.

East-West Segmentation using SGACL enforcement on FlexConnect AP

This use case will walk you through the basic configuration to do East-West segmentation or micro-segmentation in the branch network running FlexConnect deployment using SGACL enforcement on the Access Point running in FlexConnect Mode. The FlexConnect access points (APs) can switch client data traffic locally and perform client authentication locally. When a wireless client is authenticated to the network, Cisco Identity Service Engine (ISE) would push a Dynamic Security Group Tag based on the Authorization Profile configured on ISE. Client classification happens at ingress by ISE that assigns a unique S- SGT to the wireless client based on client identity. Wireless LAN Controller now receives the SGT associated with the wireless client. WLC will treat client SGT as D- SGT and initiate download of SGACL policy names for the destination from ISE. The SGACL policies downloaded will be all possible / known S-SGTs paired with the specific client D-SGT. Once the Wireless LAN Controller downloads SGACLs from ISE, it caches and pushes the SGACL policies associated with the D-SGT to the Access Point. Enforcement enabled Access Point only receives the policies of the client Security Groups which are associated to the AP. Successful enforcement can be validated directly on the Access Point with the SGACL counters.

Note: This usecase covers SGACL enforcement only for the clients associated to a single AP. Inline Tagging or SXP needed to be enabled on the FlexConnect AP to enforce the policy between the wireless clients connected to multiple FlexConnect Access Points.

Figure 3: Topology showing a wireless FlexConnect deployment with the enforcement on AP



The above topology shows two users Employee3 and Employee4 from Branch connected on a wireless network to a FlexConnect Access Point. The AP (Branch-AP) physically connected to a wired switch (Branch 3650) is associated to the WLC (5520 WLC) over CAPWAP. As soon as the endpoints connect to the network they would be authenticated and authorized by cisco ISE and would be assigned an SGT dynamically based on their role. The Access Point would have the IP-SGT binding information locally for those associated clients. WLC downloads the SGACL policies (Block_Malware) from ISE and would push those SGACLs (shown in the topology) to the AP (Branch-AP). By

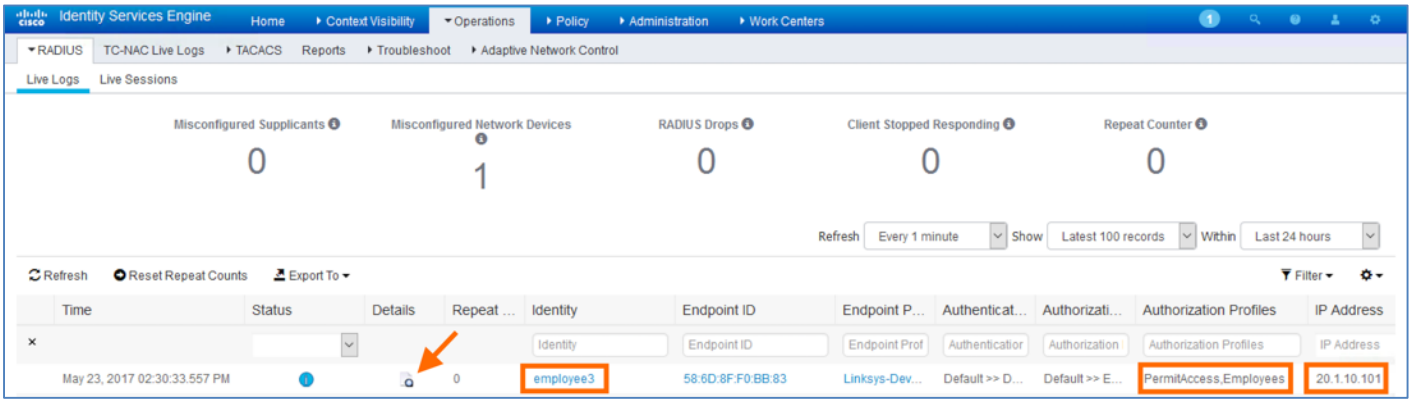
looking at the Source and Destination Group Tag and the downloaded SGACL policy (Block_Malware), AP (Branch-AP) would enforce the policy and would block the malware propagation between the Employees and Contractors.

Note: The basic ISE configuration, WLC and AP specific configuration is not covered here as it was already shown in the above sections.

Step 1 Connect the **Employee3** PC to the wireless SSID in Branch

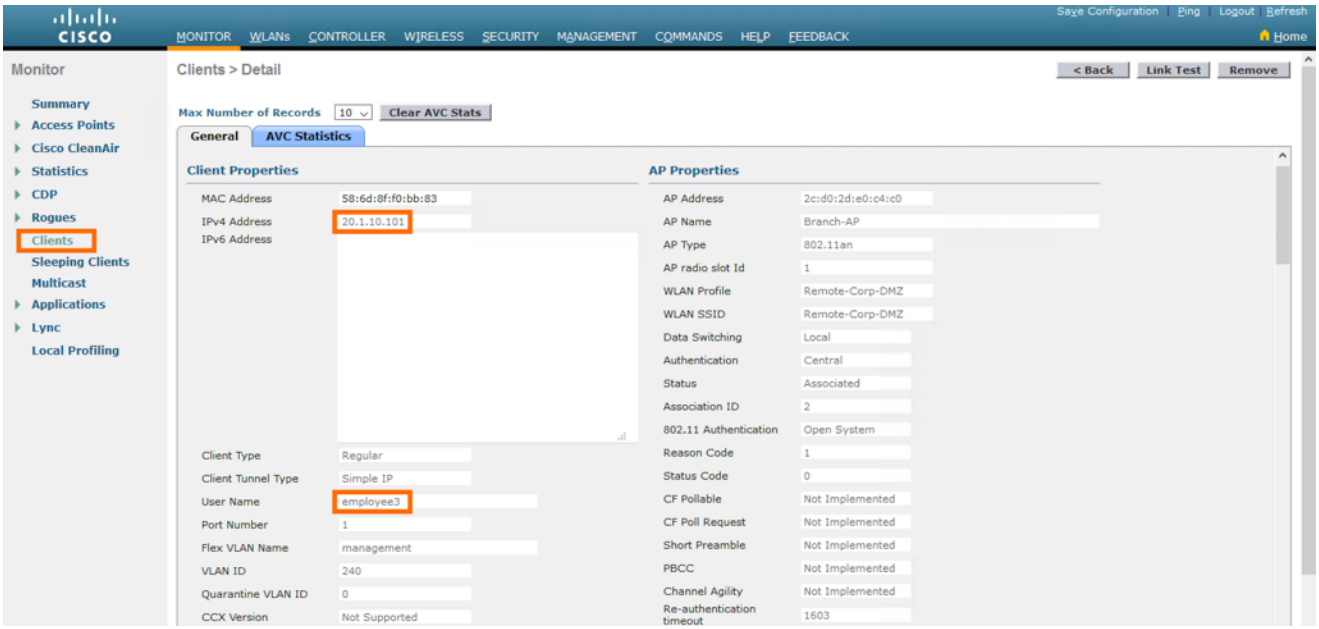
Step 2 The user **Employee3** would be assigned an **Employees SGT** (**4**) dynamically as per the Authorization policy configuration earlier during the ISE configuration

Step 3 Once connected hop on to ISE and navigate to **Operations > RADIUS > Live Logs** to see the endpoint details. Click on the **Details** icon below for all the session related information.

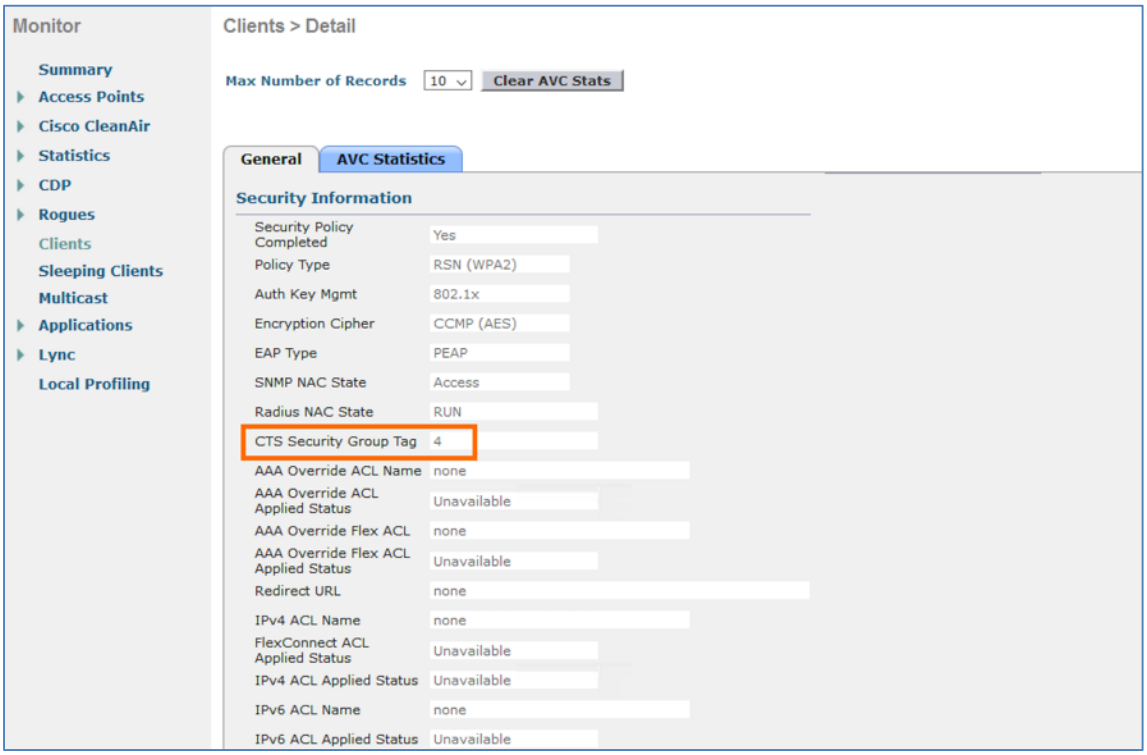


Step 4 The **Live Logs Details** shows the all the endpoint details including the associated Security Group for that endpoint

Step 5 To validate the Security Group assignment of the client **Employee3** on the WLC navigate to **Monitor > Clients** and click on **Client MAC Addr** for the details



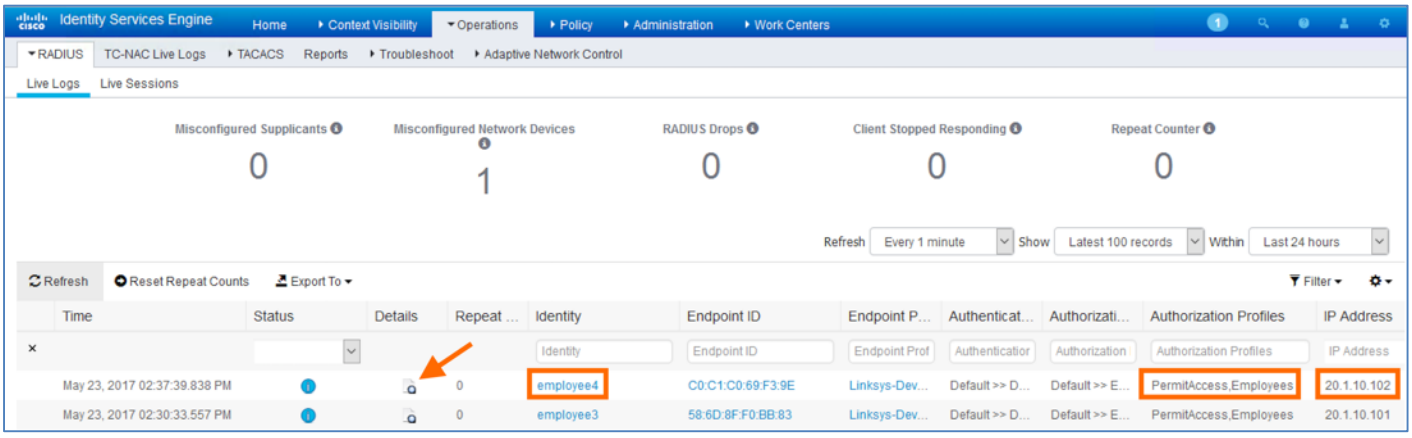
Step 6 Scroll down and look at the **Security Information** for the **CTS Security Group Tag** assigned to the client Employee1, which is **4** (**Employees**)



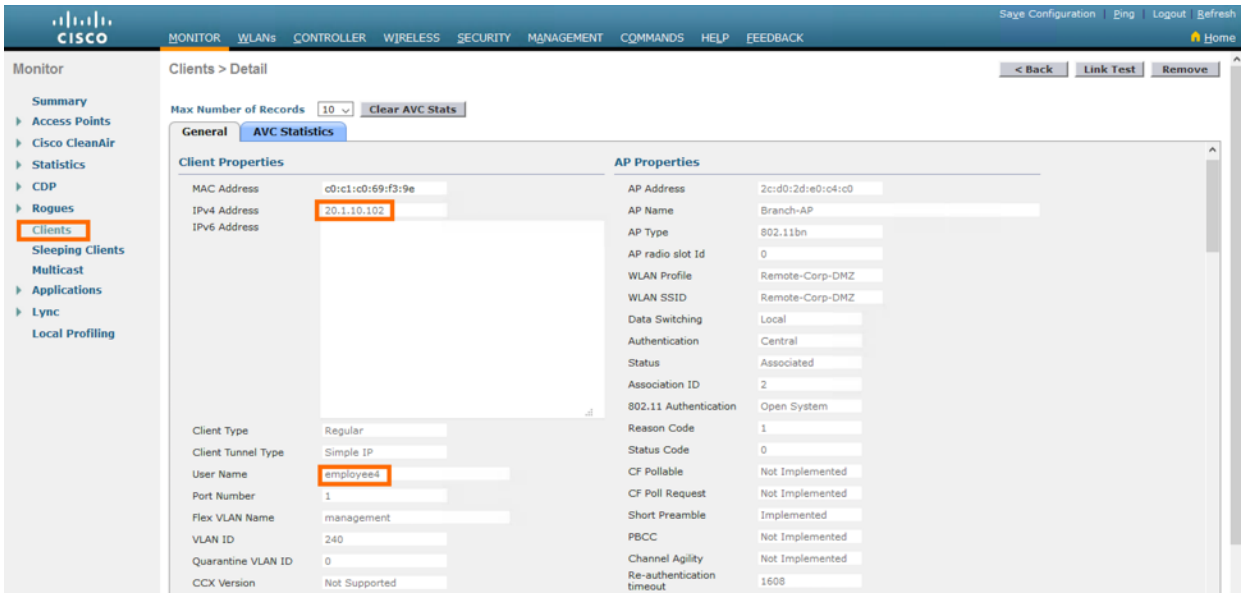
Step 7 Now connect the **Employee4** PC to the wireless SSID in Campus

Step 8 The user **Employee4** would be assigned an **Employees SGT** (**4**)

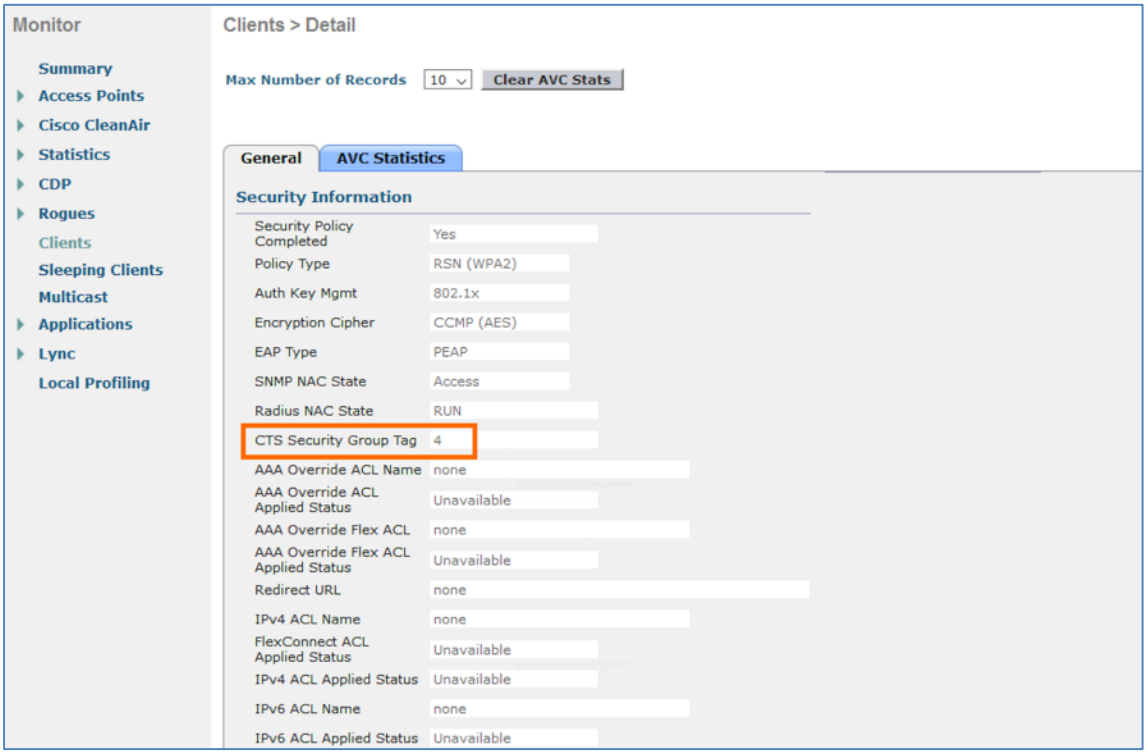
Step 9 On ISE and navigate to **Operations > RADIUS > Live Logs** to see the endpoint details. Click on the **Details** icon below for all the session related information.



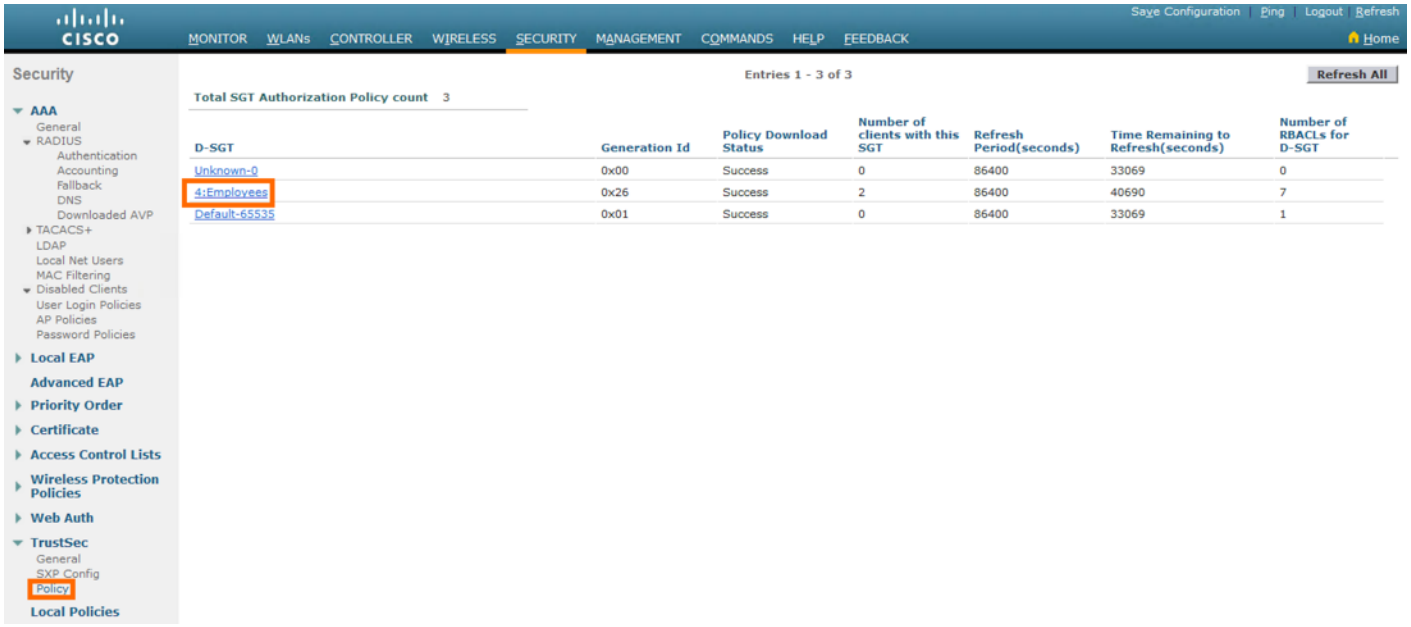
Step 10 To validate the Security Group assignment of the client **Employee4** on the WLC navigate to **Monitor > Clients** and click on **Client MAC Addr** for the details



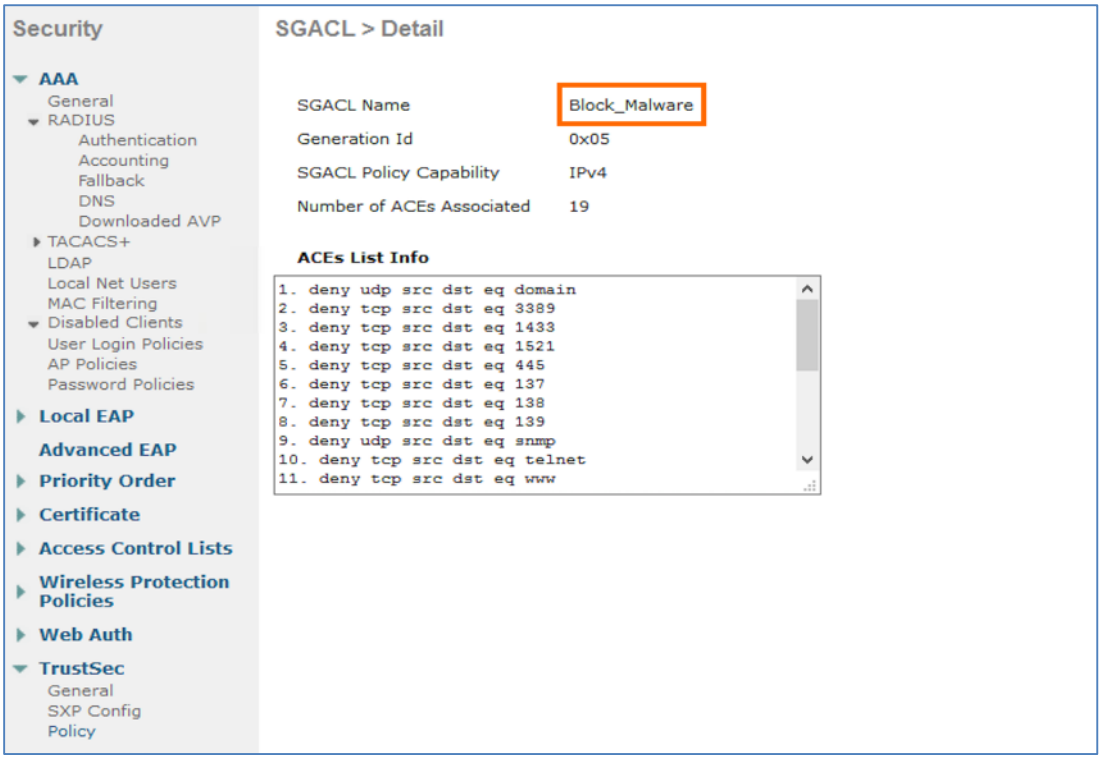
Step 11 Scroll down and look at the **Security Information** for the **CTS Security Group Tag** assigned to the client Employee4, which is **4** (**Employees**)



Step 12 Now from the WLC navigate to **Security > TrustSec > Policy** to see the newly downloaded SGACL policies on the WLC for the **Employees** Security Group



Step 13 Click on the **D-SGT** name **Employees** for the **BLOCK_MALWARE** SGACL pushed from ISE between **Employee** Security Groups (S-SGT and D-SGT)



Step 14 Now look for the IP-SGT binding information on Access Point using the below command. The endpoints, which are connected to the **Branch-AP** that got a SGT would be seen below

```
Branch-AP#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
         IP SGT SOURCE
20.1.10.101   4  LOCAL
20.1.10.102   4  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::4937:6a00:95a7:f00e   4  LOCAL
fe80::b129:ae1f:c787:173b   4  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
Branch-AP#
```

Step 15 To verify the SGACL permissions between the S-SGT and the D-SGT use the below command on the Access Point

```
Branch-AP#show cts role-based permissions
IPv4 role-based permissions:
  SGT   DGT           ACL
    4     4 Block_Malware
    5     4 Block_Malware
    9     4    Allow_ICMP
   11     4     Permit_IP
   12     4     Permit_IP
   14     4       Deny_IP
   16     4     Permit_IP
65535 65535     Permit_IP

IPv6 role-based permissions:
  SGT   DGT       ACL
   11     4 Permit_IP
   12     4 Permit_IP
   14     4   Deny_IP
   16     4 Permit_IP
65535 65535 Permit_IP

Branch-AP#
```

Block_Malware SGACL is downloaded to the AP and that would be invoked between the **Employees** (**4**) Security Group

Step 16 Use the following CLI command on the Access Point to verify the **SGACL** content and the **Access Control Entries** (ACEs)

```
Branch-AP#show cts access-lists
IPv4 role-based ACL:
Allow_ICMP
        rule 0: allow true && ip proto 1
Block_Malware
        rule 0: deny true && ip proto 17 && ( dst port 53 )
        rule 1: deny true && ip proto 6 && ( dst port 3389 )
        rule 2: deny true && ip proto 6 && ( dst port 1433 )
        rule 3: deny true && ip proto 6 && ( dst port 1521 )
        rule 4: deny true && ip proto 6 && ( dst port 445 )
        rule 5: deny true && ip proto 6 && ( dst port 137 )
        rule 6: deny true && ip proto 6 && ( dst port 138 )
        rule 7: deny true && ip proto 6 && ( dst port 139 )
        rule 8: deny true && ip proto 17 && ( dst port 161 )
        rule 9: deny true && ip proto 6 && ( dst port 23 )
        rule 10: deny true && ip proto 6 && ( dst port 80 )
        rule 11: deny true && ip proto 6 && ( dst port 443 )
        rule 12: deny true && ip proto 6 && ( dst port 22 )
        rule 13: deny true && ip proto 6 && ( dst port 110 )
        rule 14: deny true && ip proto 6 && ( dst port 123 )
        rule 15: deny true && ip proto 6 &&  tcp opt !ack &&  tcp opt fin &&
tcp opt !psh &&  tcp opt !rst &&  tcp opt !syn &&  tcp opt !urg
        rule 16: deny true && ip proto 6 &&  tcp opt fin &&  tcp opt psh &&
tcp opt urg
        rule 17: allow true && ip proto 1
        rule 18: allow true && ip proto 6 &&  tcp opt ack ||  tcp opt syn
Permit_IP
        rule 0: allow true
Deny_IP
        rule 0: deny true

IPv6 role-based ACL:
Permit_IP
        rule 0: allow true
Deny_IP
        rule 0: deny true

Branch-AP#
```

Step 17 Ping the **Employee4** IP address from **Employee3** PC

```
C:\Users\employee3>ping 20.1.10.102

Pinging 20.1.10.102 with 32 bytes of data:
Reply from 20.1.10.102: bytes=32 time=4ms TTL=125
Reply from 20.1.10.102: bytes=32 time=3ms TTL=125
Reply from 20.1.10.102: bytes=32 time=7ms TTL=125
Reply from 20.1.10.102: bytes=32 time=5ms TTL=125

Ping statistics for 20.1.10.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 4ms
```

```
C:\Users\employee3>
```

Ping should succeed as the **Permit ICMP** is enabled in the SGACL. Similarly, if you would try to access the Employee4 PC through any other port (ex: 137 etc..) then the access would be denied.

Step 18 Validate the **SGACL enforcement** on the Access Point through the **SGACL Counters** command. To check the counters between the **Employees** Security Group (**4**) use the following command on AP.

```
Branch-AP#show cts role-based counters from 4 to 4
IPv4 ACL: Block_Malware
Packets Allowed : 4
Packets Denied  : 5

Branch-AP#
```

Deny counters (Packets Denied) are incremented above due to the Port Scan on **Employee4** PC on port 138 and port 139.

User to Datacenter Access Control with Wireless APs using SXPv4 and Inline Tagging

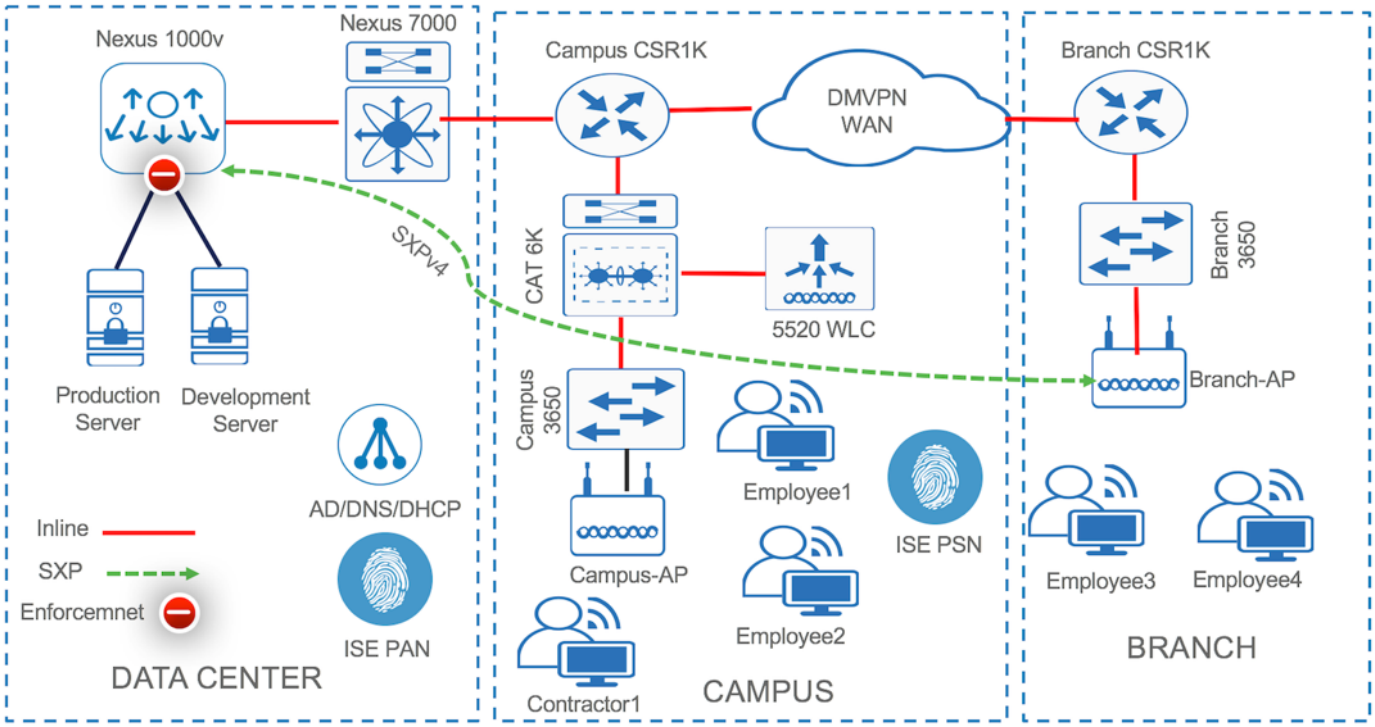
The User to Datacenter (North – South) segmentation is the most widely deployed TrustSec usecase. The critical assets part of the datacenter are protected through TrustSec Software-Defined Segmentation. The Use Cases could be as simple as providing differentiated access to the shared servers/services like Production and Development to enabling compliance for PCI, HIPAA and other regulations through segmentation. This particular usecase will go through SXPv4 and Inline Tagging configuration on the FlexConnect Access Point. By enabling either Inline Tagging or SXP, AP can share the S-SGT of the wireless clients to the enforcement points (Switch, ASA) in the datacenter. Once the enforcement device receives the IP-SGT bindings from the AP, it would download the SGACL policies for the S-SGT and D-SGT and would do the enforcement. FlexConnect AP could even enforce the policy locally (ingress filtering) through Inline Tagging and SXPv4 supporting bi-directional SXP with both SXP Speaker as well as Listener mode.

Note: It is best practice to have AP run Speaker mode while SXP peering with the Datacenter devices due to the scaling limitations. In the large enterprise networks, it is ideal to run SXP on WLC instead of AP to share the IP-SGT bindings for North – South Segmentation.

Below are some of the TrustSec scaling limitations on the Access Points for this release.

Max Active SGTs AP can support are 50 IP-SGT entries. Max SXPv4 sessions APs can peer are 5. MAX number of SGACL policies an AP can support are 50. Max ACEs within a SGACL are 16. WLC can support 50 Source and 50 Destination SGTs for SGACL policy download.

Figure 4: Topology showing User to Datacenter segmentation with SXPv4 between AP and DC Switch



Destination Source	Employees	Contractors	Development Servers	Production Servers
Employees	Block_Malware	Block_Malware	Allow_ICMP	Permit_IP
Contractors	Block_Malware	Block_Malware	Deny_IP	Allow_Web
Development Servers	Allow_ICMP	Deny_IP	Permit_IP	Block_Web
Production Servers	Permit_IP	Allow_Web	Block_Web	Permit_IP

Name	IP Address
5520 WLC	10.1.100.15
Branch 3650	20.1.100.11
Branch-AP	20.1.30.101
Nexus 1000v	10.1.200.11
Development Server	10.1.210.10
Production Server	10.1.210.20
Employee3	20.1.10.101
Employee4	20.1.10.102

The above topology shows two users Employee3 and Employee4 from Branch connected on a wireless network to a FlexConnect Access Point. The AP (Branch-AP) physically connected to a wired switch (Branch 3650) is associated to the WLC (5520 WLC) over CAPWAP. The Access Point (Branch-AP) would have the IP-SGT binding information locally for those associated clients. AP would share those local bindings to the DC switch (Nexus 1000v) using either Inline Tagging or SXPv4. Classification of servers (Production and Development servers) in the datacenter connected to Nexus 1000v is done through Port Profiles. Inside the Port profile configuration, the Security Group Tag is defined. As a VM (server) is powered on and the vEthernet port on the Nexus 1000V comes up, IP device tracking is used to learn the IP-SGT mapping of the servers.

The IP-SGT bindings from Nexus 1000v would then be advertised to other SXP peers (Branch-AP). It also receives the mappings from its SXP peers (Branch-AP) which could be further used for policy enforcement purposes. ISE pushes the SGACLs to Nexus 1000v. Nexus 1000v downloads only specific SGACLs relevant for its Security Groups.

Once enforcement is enabled the RBACL configured for the SGT, DGT pair is applied on the egress. From the above policy matrix Employees would be allowed to access the Production Server but would only have ICMP access to the Development Server.

Note: The basic ISE configuration, TrustSec configuration on Nexus 1000v and AP specific configuration is not covered here.

Step 1 Here is the command on the **Branch-AP** to see the IP-SGT binding information of the endpoints, which are connected and got a SGT

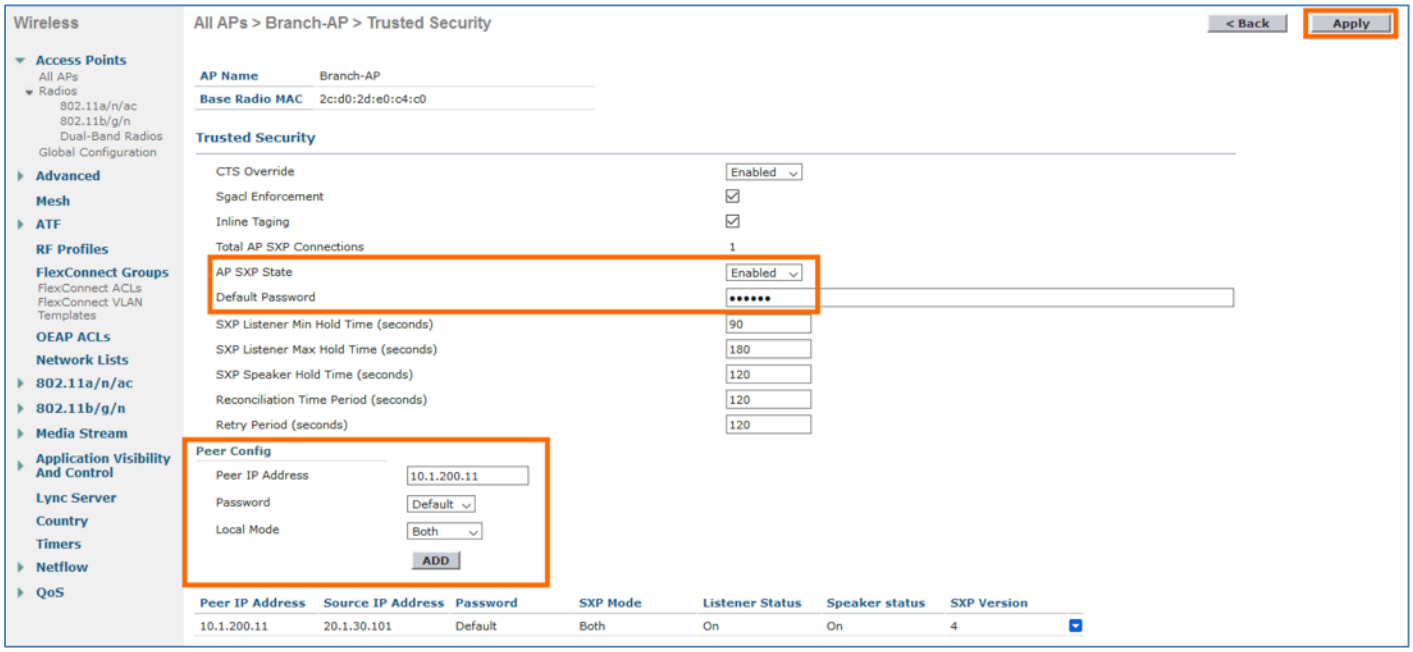
```
Branch-AP#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
         IP SGT SOURCE
20.1.10.101   4  LOCAL
20.1.10.102   4  LOCAL

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::4937:6a00:95a7:f00e   4  LOCAL
fe80::b129:ae1f:c787:173b   4  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
Branch-AP#
```

Step 2 Here is the command on the **Nexus 1000v** to see the IP-SGT binding information of the Production and Development Servers.

10.1.210.20 with an SGT 11 and 10.1.210.10 with an SGT 12 are learned through Device Tracking when the VM is powered-on

```
Nexus1000v# show cts role-based sgt-map
IP ADDRESS          SGT             VRF/VLAN        SGT CONFIGURATION
10.1.210.10         12              vlan:210        Device Tracking
10.1.210.20         11              vlan:210        Device Tracking
Nexus1000v#
```

Step 3 FlexConnect AP in Branch as configured in the earlier sections (WLC & AP configuration) should have either Inline Tagging or SXPv4 peering with the DC switch (Nexus 1000v) to send the IP-SGT bindings.



10.1.200.11 is the IP address of the Nexus 1000v and **20.1.30.101** is the IP address of the Branch-AP

Step 4 Below is the inline tagging configuration on the switch port where the Branch-AP is connected to send the Tags in ASIC or through data plane

```
description "Connected to FlexConnect Branch-AP"
switchport trunk native vlan 230
switchport mode trunk
spanning-tree portfast trunk
cts manual
  policy static sgt 2 trusted
```

Note: Tags could be propagated to the enforcement switches using Inline Tagging or SXP or both. With Inline Tagging the CTS manual configuration needs to be enabled between switch-switch links all the way to the DC switch.

Step 5 Here is the SXP configuration on the Nexus 1000v to form peering with the Branch-AP

```
cts sxp enable
cts sxp node-id interface mgmt0
cts sxp default password <####>
cts sxp default source-ip 10.1.200.11
cts sxp connection peer 20.1.30.101 password default mode both vrf management
```

Step 6 Here is the Inline Tagging configuration on the Nexus 1000v connected to an upstream DC switch.

```
port-profile type ethernet UPLINK-TRUNK
  switchport mode trunk
  switchport trunk allowed vlan 1-3967,4048-4093
  cts manual
    policy static sgt 2 trusted
    role-based enforcement
  no shutdown
  system vlan 200
  state enabled
  vmware port-group
```

Step 7 Now that SXPv4 with both SXP Speaker and Listener is configured on **Branch-AP**, all the bindings from the **Nexus 1000v** are learned by the AP.

```
Branch-AP#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
         IP SGT SOURCE
10.1.210.10  12    SXP
10.1.210.20  11    SXP
20.1.10.101   4  LOCAL
20.1.10.102   4  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of SXP      bindings = 2
Total number of active   bindings = 4

Active IPv6-SGT Bindings Information
                       IP SGT SOURCE
fe80::4937:6a00:95a7:f00e   4  LOCAL
fe80::b129:ae1f:c787:173b   4  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
Branch-AP#
```

Production and Development server IP addresses and the respective SGTs are learned by the Branch-AP through SXP

Step 8 Similarly, **Nexus 1000v** switch learns the IP-SGT bindings of the Endpoints from **Branch-AP**

```
Nexus1000v# show cts role-based sgt-map
IP ADDRESS          SGT             VRF/VLAN        SGT CONFIGURATION
10.1.210.10         12              vlan:210        Device Tracking
10.1.210.20         11              vlan:210        Device Tracking
20.1.10.101         4               management      SXP peer:20.1.30.101
20.1.10.102         4               management      SXP peer:20.1.30.101
Nexus1000v#
```

Step 9 To check the **SGACLs** and its **Permissions** downloaded by **Nexus 1000v** from ISE, use the below CLI command

```
Nexus1000v# show cts role-based policy

sgt:4
dgt:11  rbacl:Permit IP
        permit ip

sgt:4
dgt:12  rbacl:Allow_ICMP
        permit icmp log

sgt:5
dgt:11  rbacl:Allow_Web
        permit tcp src eq 80
        permit tcp dst eq 80
        deny icmp log

sgt:5
dgt:12  rbacl:Deny IP
        deny ip

sgt:11
dgt:11  rbacl:Permit IP
        permit ip

sgt:11
dgt:12  rbacl:Block_Web
        deny tcp dst eq 80
        deny tcp src eq 80
        permit icmp log

sgt:12
dgt:11  rbacl:Block_Web
        deny tcp dst eq 80
        deny tcp src eq 80
        permit icmp log

sgt:12
dgt:12  rbacl:Permit IP
        permit ip

sgt:any
dgt:any rbacl:Permit IP
        permit ip
Nexus1000v#
```

Employees have full access to the production server but only ICMP (ping) access to the Development server

Step 10 Use the below CLI command to check the **RBACLs** (ACEs) on **Nexus 1000v**

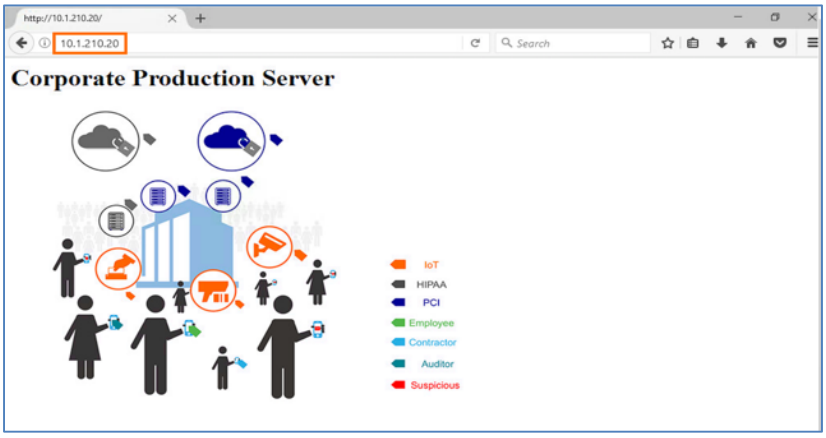
```
Nexus1000v# show cts role-based access-list
rbacl:Allow_ICMP
        permit icmp log
rbacl:Allow_Web
        permit tcp src eq 80
        permit tcp dst eq 80
        deny icmp log
rbacl:Block_Web
        deny tcp dst eq 80
        deny tcp src eq 80
        permit icmp log
rbacl:Deny IP
        deny ip
rbacl:Permit IP
        permit ip
Nexus1000v#
```

Step 11 Ping the **Production Server** IP address from **Employee3** PC

```
C:\Users\employee3>ping 10.1.210.20

Pinging 10.1.210.20 with 32 bytes of data:
Reply from 10.1.210.20: bytes=32 time=4ms TTL=125
Reply from 10.1.210.20: bytes=32 time=3ms TTL=125
Reply from 10.1.210.20: bytes=32 time=7ms TTL=125
Reply from 10.1.210.20: bytes=32 time=5ms TTL=125

Ping statistics for 10.1.210.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 4ms

C:\Users\employee3>
```

Ping should succeed as the default **Permit IP** is enabled in the policy.

Step 12 Similarly, if you would try to access the **Production Server** through **Web** (http/https), the access would be allowed.



Step 13 Validate the **SGACL enforcement** on the **Nexus 1000v** through the **SGACL Counters** command. To check the counters between the **Employees** Security Group (**4**) and the **Production Servers** Security Group (**12**) use the following command.

```
Nexus1000v# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: ▒▒▒M
Counters last updated on 6▒M:
rbacl:Allow_ICMP
        permit icmp log                                 [0]
rbacl:Allow_Web
        permit tcp src eq 80                            [0]
        permit tcp dst eq 80                            [0]
        deny icmp log                                   [0]
rbacl:Block_Web
        deny tcp dst eq 80                              [0]
        deny tcp src eq 80                              [0]
        permit icmp log                                 [0]
rbacl:Deny IP
        deny ip                                         [0]
rbacl:Permit IP
        permit ip                                       [32]
Nexus1000v#
```

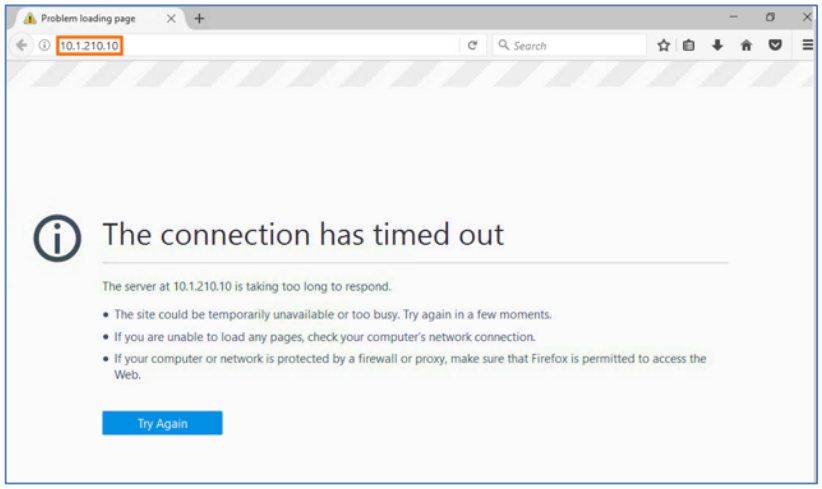
The counters for **Permit IP** would be incremented when **Employee3** try to access the **ICMP** or **Web**

Step 14 Now from **Employee3** PC **ping** the **Development Server** IP address

```
C:\Users\employee3>ping 10.1.210.10

Pinging 10.1.210.20 with 32 bytes of data:
Reply from 10.1.210.10: bytes=32 time=4ms TTL=125
Reply from 10.1.210.10: bytes=32 time=3ms TTL=125
Reply from 10.1.210.10: bytes=32 time=7ms TTL=125
Reply from 10.1.210.10: bytes=32 time=5ms TTL=125

Ping statistics for 10.1.210.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 4ms

C:\Users\employee3>
```

Ping should succeed as the default **Permit ICMP** is enabled in the policy.

Step 15 Similarly, if you would try to access the **Development Server** through **Web** (http/https), the access would be Denied as the policy only allows ICMP.



Step 16 Validate the **SGACL enforcement** on the **Nexus 1000v** through the **SGACL Counters** command. To check the counters between the **Employees** Security Group (**4**) and the **Development Servers** Security Group (**12**) use the following command.

```
Nexus1000v# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: ▒▒M
Counters last updated on 6▒M:
rbacl:Allow_ICMP
        permit icmp log                                 [4]
rbacl:Allow_Web
        permit tcp src eq 80                            [0]
        permit tcp dst eq 80                            [0]
        deny icmp log                                   [0]
rbacl:Block_Web
        deny tcp dst eq 80                              [0]
        deny tcp src eq 80                              [0]
        permit icmp log                                 [0]
rbacl:Deny IP
        deny ip                                         [0]
rbacl:Permit IP
        permit ip                                       [0]
Nexus1000v#
```

The counters for **Allow_ICMP** would be incremented when **Employee3** try to access the **ICMP**

Debugs on ISE, WLC and Switch

Debug SXP on ISE

To Debug SXP connections and bindings in ISE, the debug needs to be turned on the dedicated SXP node.

Step 1 In ISE, navigate to **Administration > System > Logging > Debug Log Configuration**

Step 2 Select the ISE SXP node

Step 3 **Edit** to enable the **'Log Level'** to debug for the following Components: SXP and Replication Tracker

Step 4 To download the logs in ISE, navigate to **Operations > Troubleshoot > Download Logs**

Step 5 Select the ISE node (SXP)

Step 6 Select the **Debug Logs** tab and scroll down to the Debug Log

Step 7 Look for **sxp** debug log files

Debug CTS on WLC

To Debug **CTS** on **WLC**, enable the following debug commands.

```
(Cisco Controller) >debug cts ?

aaa             Configure the CTS AAA debug options.
authz           Configure the CTS SG-ACL download 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.
```

```
sgt             Configures SGT debugging for upto 10 sgt
sxp             Configures the CTS SXP debug options
```

Debug CTS on Access Point

To Debug **CTS** issues on the **Switches**, enable the following debug commands.

```
Campus-AP#debug cts ?
  enforcement  Enable CTS packet level enforcement debugging
  parser       Enable CTS ACL parser debugging
  sxp          Enable CTS SXP debugging
```

Additionally, the following commands is handy in troubleshooting all the client related issues on AP

```
Campus-AP#debug client trace all
```