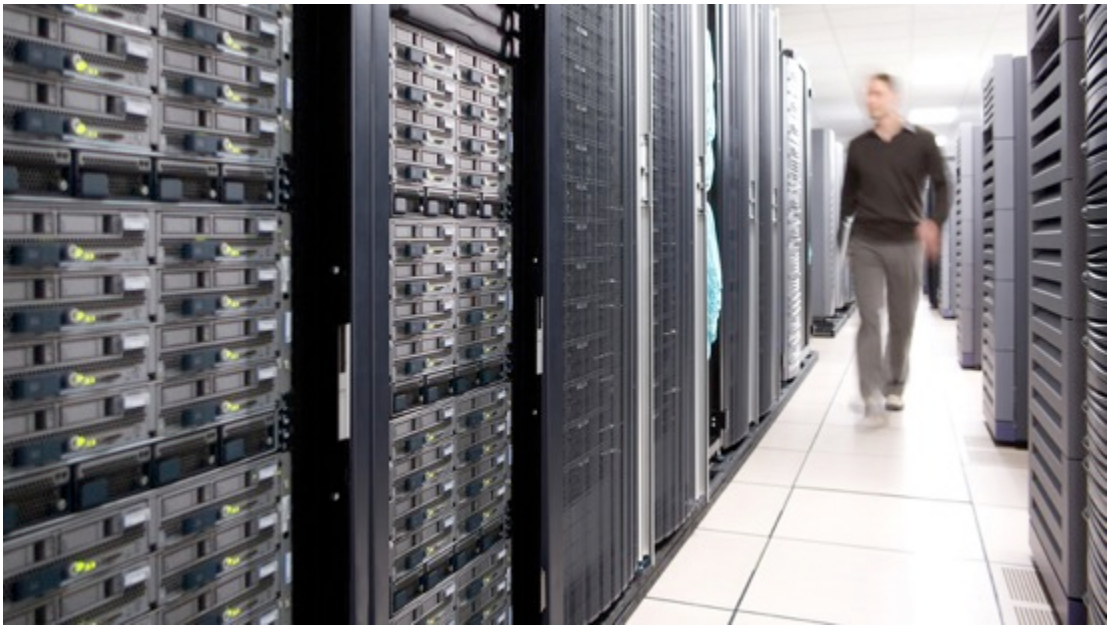


TrustSec Configuration Guides

Wireless FlexConnect Access Control using TrustSec

Enabling SXP Support for Access Points running FlexConnect Local Mode

TrustSec
Software-Defined
Segmentation

Table of Contents

Wireless FlexConnect Access Control using TrustSec

Introduction

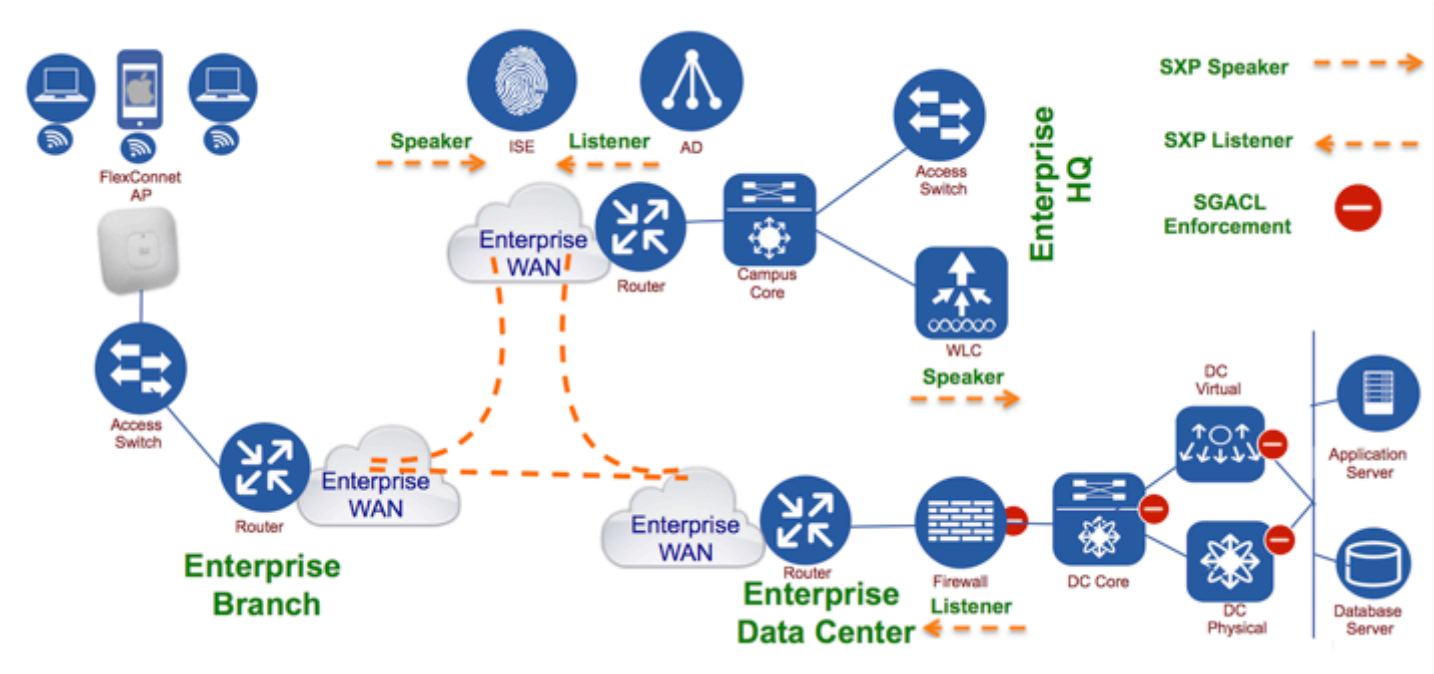
Cisco TrustSec (TrustSec) provides software-defined segmentation to reduce the risk of malware propagation, simplify security operations, and assist in meeting compliance goals. With TrustSec, controls are defined simply using endpoint roles, not IP addresses. By classifying systems using human-friendly 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.

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.

FlexConnect APs are capable of supporting the following switching modes concurrently, on a per-WLAN basis. One is Central Switched and other is Locally Switched. Central switched WLANs tunnel both the wireless user traffic and all control traffic via CAPWAP to the centralized WLC where the user traffic is mapped to a dynamic interface/VLAN on the WLC. This is the normal CAPWAP mode of operation. The traffic of a branch user, who is associated to a central switched WLAN, is tunneled directly to the centralized WLC. If that user needs to communicate with computing resources within the branch (where that client is associated), their data is forwarded as standard IP packets back across the WAN link to the branch location. Locally Switched WLANs map wireless user traffic to discrete VLANs via 802.1Q trunking, either to an adjacent router or switch. If so desired, one or more WLANs can be mapped to the same local 802.1Q VLAN. A branch user, who is associated to a local switched WLAN, has their traffic forwarded by the on-site router. Traffic destined off-site (to the central site) is forwarded as standard IP packets by the branch router. All AP control/management-related traffic is sent to the centralized Wireless LAN Controller (WLC) separately via Control and Provisioning of Wireless Access Points protocol (CAPWAP).

Cisco Wireless Release 8.3 extends the capability to simplify access control management using Cisco TrustSec Security Groups to users connected to FlexConnect APs. Users connected to FlexConnect APs can now be classified with a Security Group Tag (SGT) to simplify policy management. Cisco WLCs can now share Security Group membership information over an SGT eXchange Protocol (SXP) connection with switches, routers, and firewalls to simplify access control list management and firewall rule management elsewhere in the network. To use this capability, Cisco Identity Services Engine would be required to authorize devices based on attributes such as the role of the user and/or device and assign a Security Group Tag dynamically as part of an authorization rule. Other devices receiving SGT information over SXP can then apply Security Group Access Control Lists and group-based firewall rules, which are more flexible and much easier to manage than using IP address-based controls. This feature complements existing support for Security Group-based policies for centrally switched user traffic in the earlier Cisco Wireless releases.

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



ISE Configuration

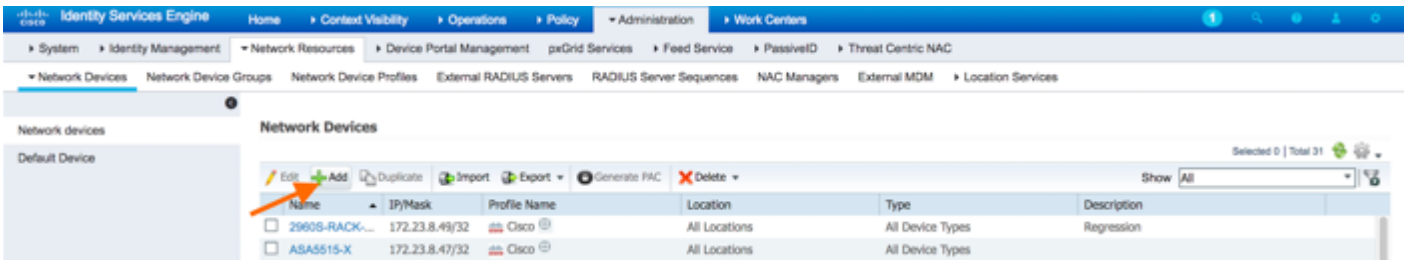
Cisco Identity Services Engine needs to be configured to assign a Security Group Tag dynamically as part of an authorization rule. ISE can authorize devices coming through MAB or 802.1X based on attributes such as the role of the user and/or device and assign a Security Group Tag dynamically.

Add Wireless LAN Controller in ISE

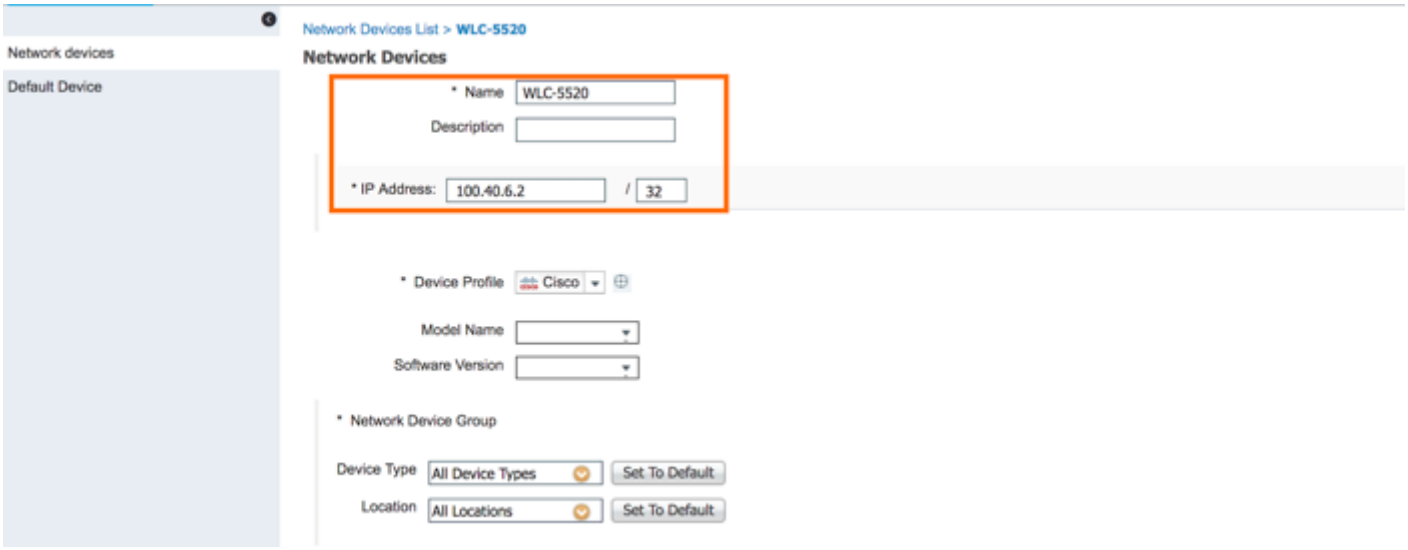
Step 1 Login to Cisco Identity Service Engine (ISE)

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

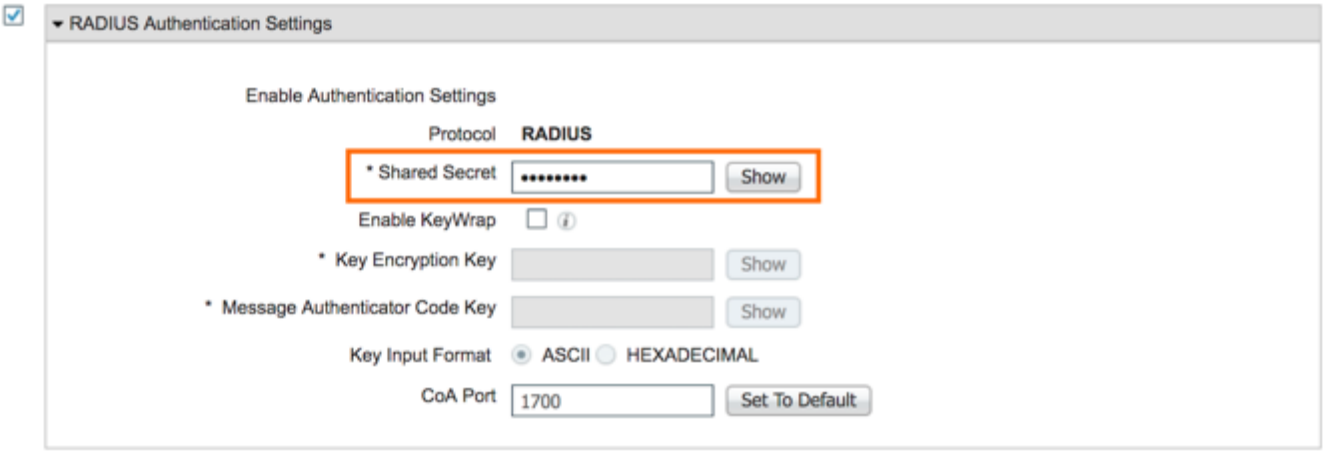


Step 4 Type the **Name** of the WLC, **IP Address** and any Network Device Group information (optional) like **Device Type** and **Location**



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



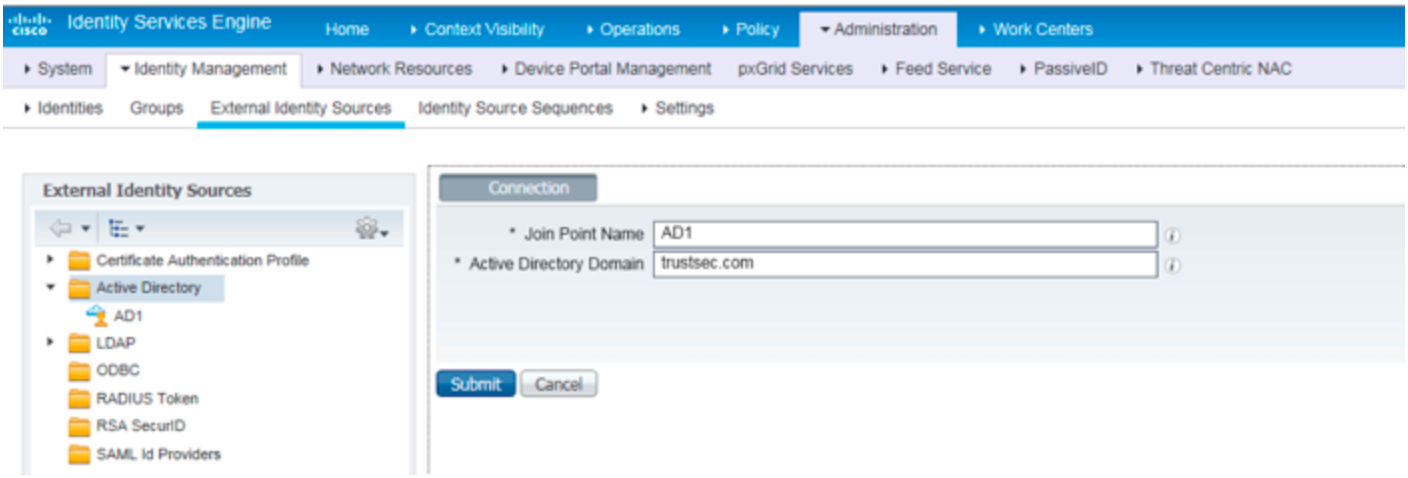
Step 6 Configure any SNMP configuration (Optional) and click **Save**

Active Directory Configuration in ISE

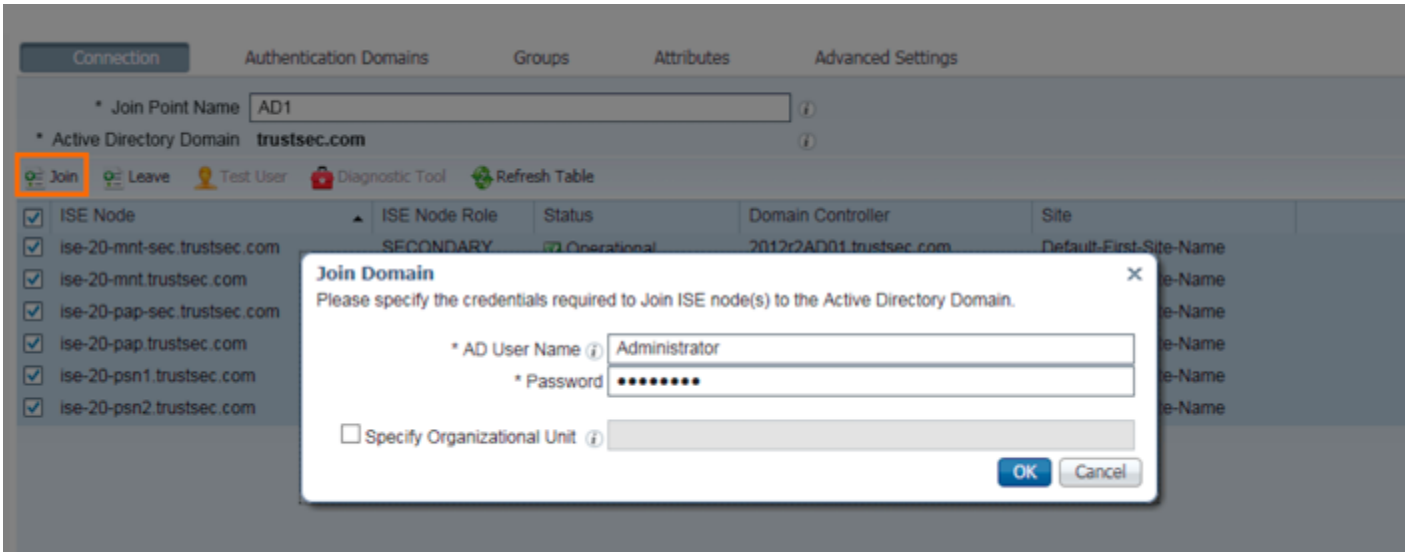
By retrieving the AD groups from the configured Active Directory in ISE the administrator would have an option to assign a Security Group value based on the user role

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

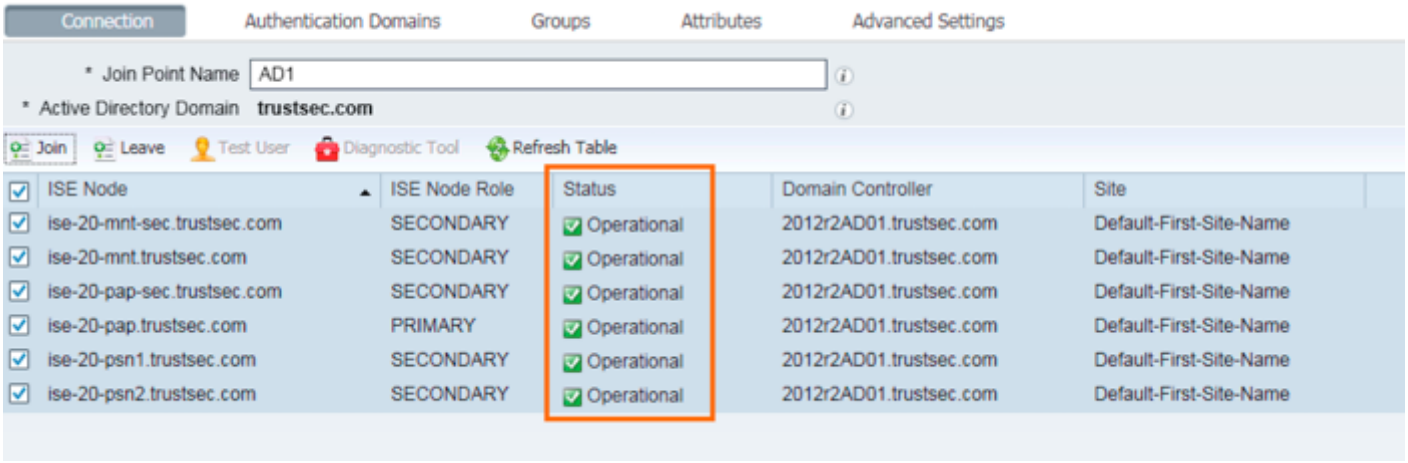
Step 2 Click **Add** for a new connection with a **Join Point Name** and **Active Directory Domain** name and **Submit**



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

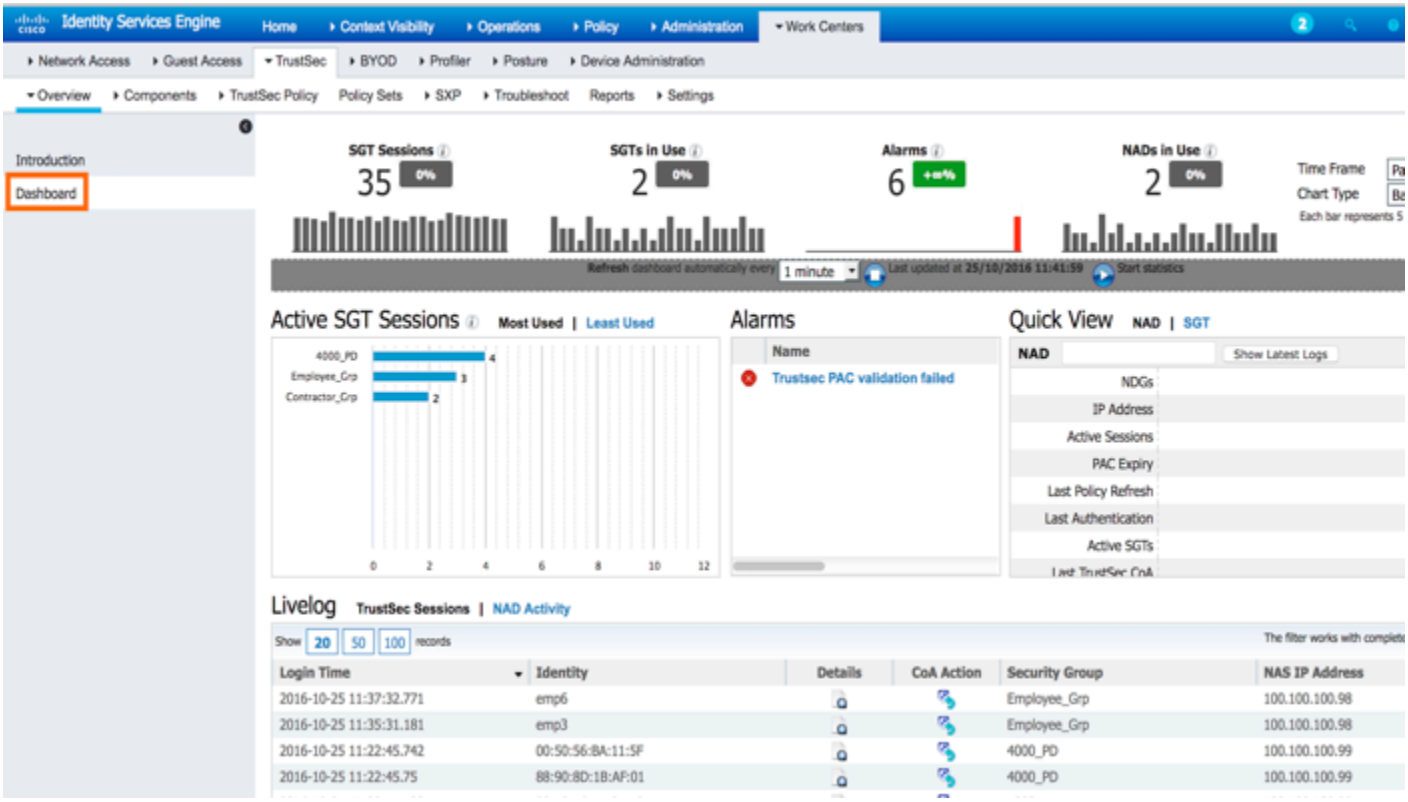
Note: These AD Groups would be useful for the administrators in creating the Authorization policies based on user roles.

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**

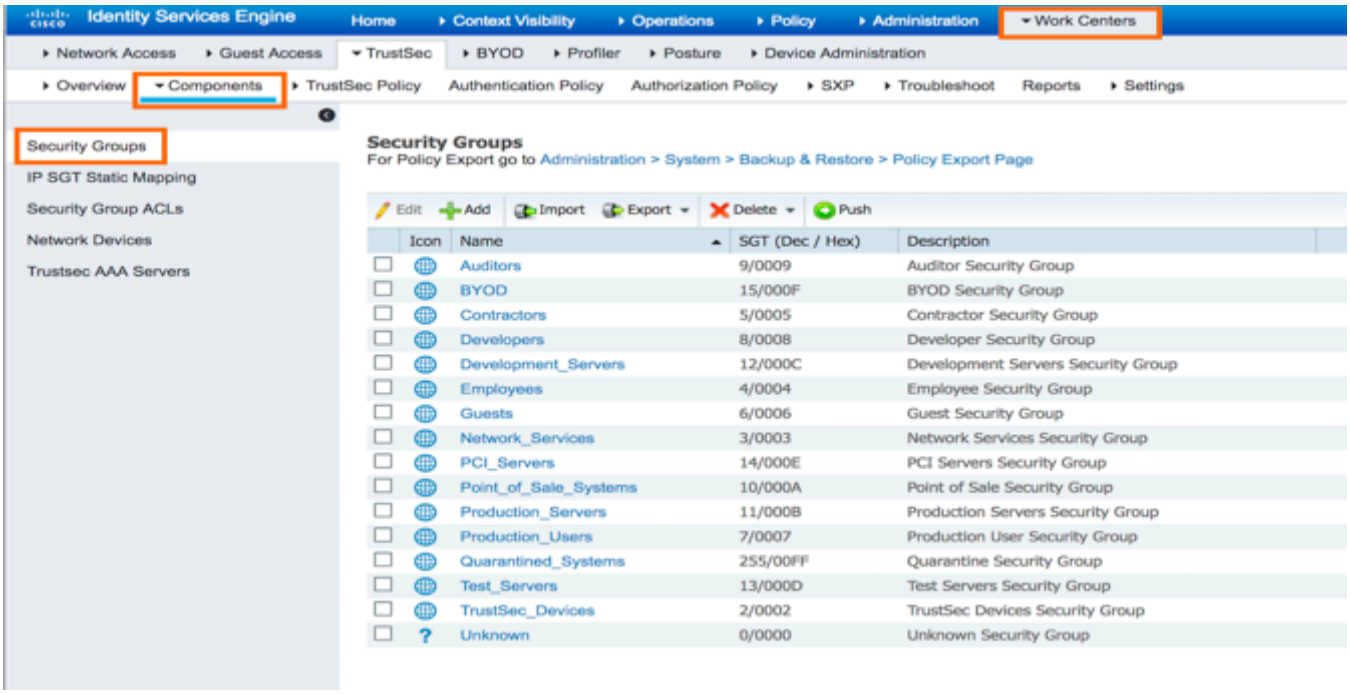
Step 2 To view the TrustSec Dashboard navigate from ISE to **Work Centers > TrustSec > TrustSec Dashboard**



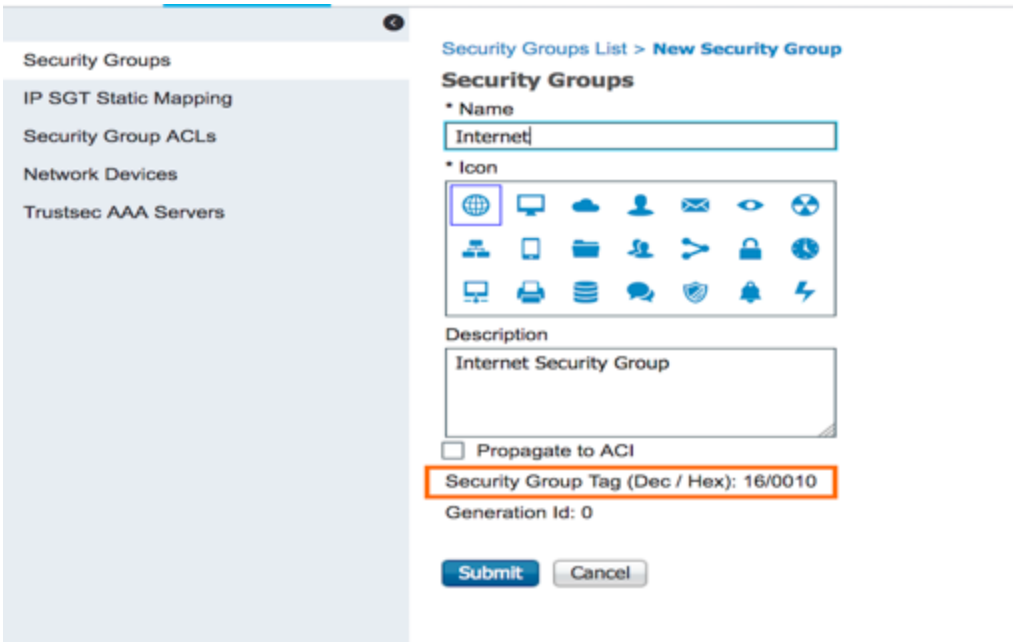
Configure Security Groups in ISE

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

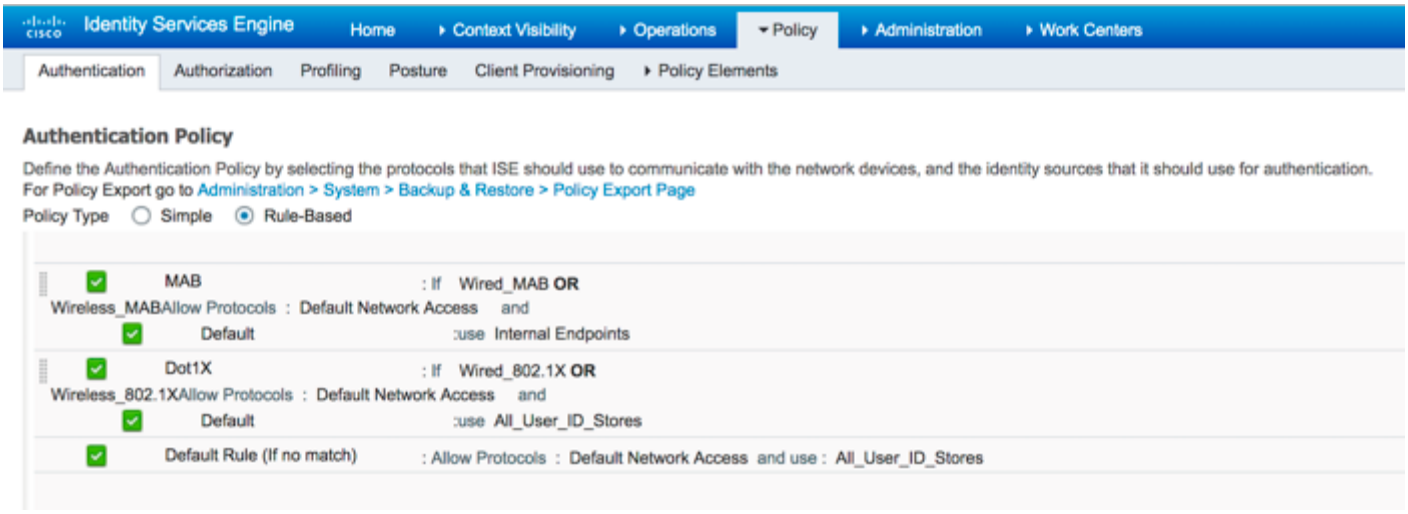


Step 3 Click **Add** to add a new Security Group in ISE and **Submit**. ISE would automatically assign a Tag value

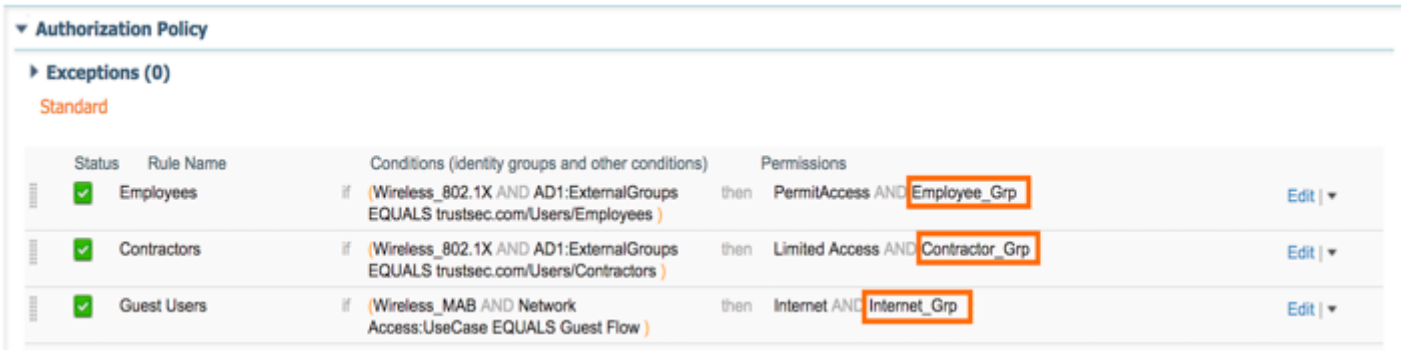


Authentication and Authorization Policies in ISE

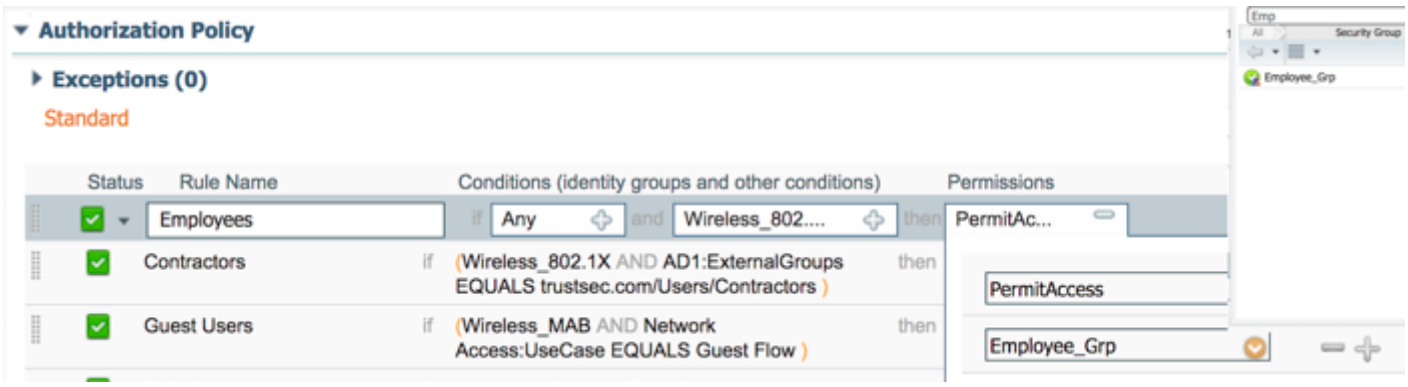
Step 1 Navigate to **Policy > Authentication** for the **Authentication Policy**. Here is a sample Authentication policy for both **MAB** and **Dot1X**



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



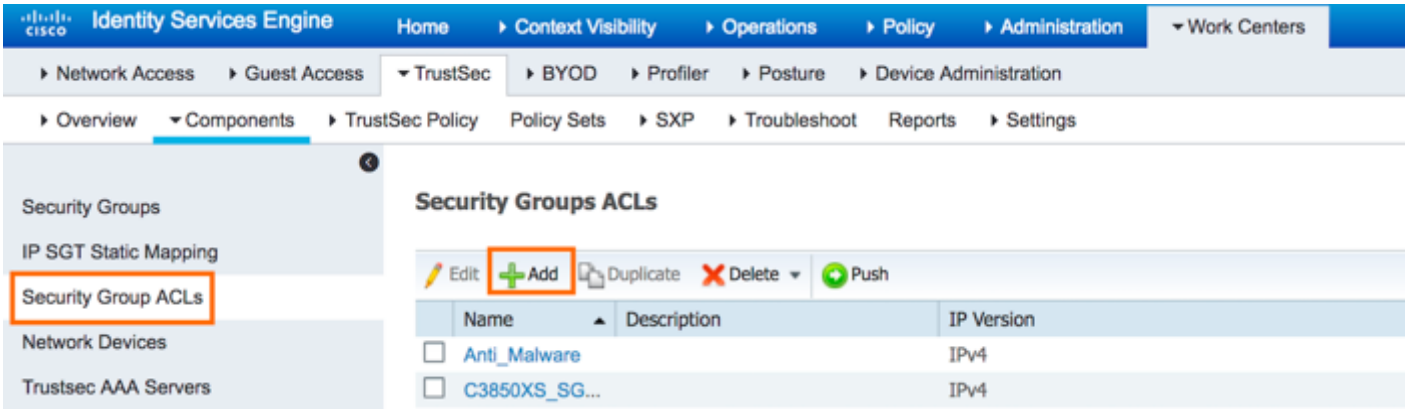
Step 3 Assign a security group to each of the Authorization rule based on the user role/device type like **Employee_Grp** etc.



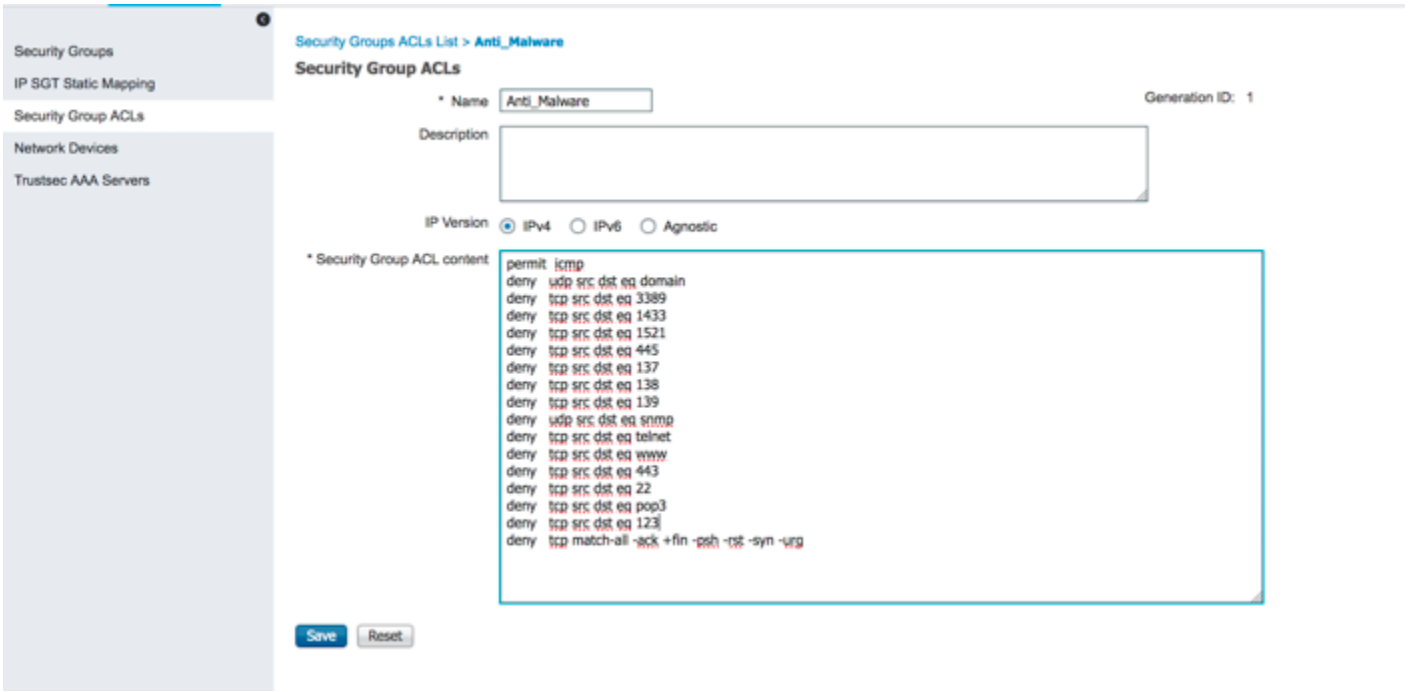
SGACL Configuration in ISE

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**

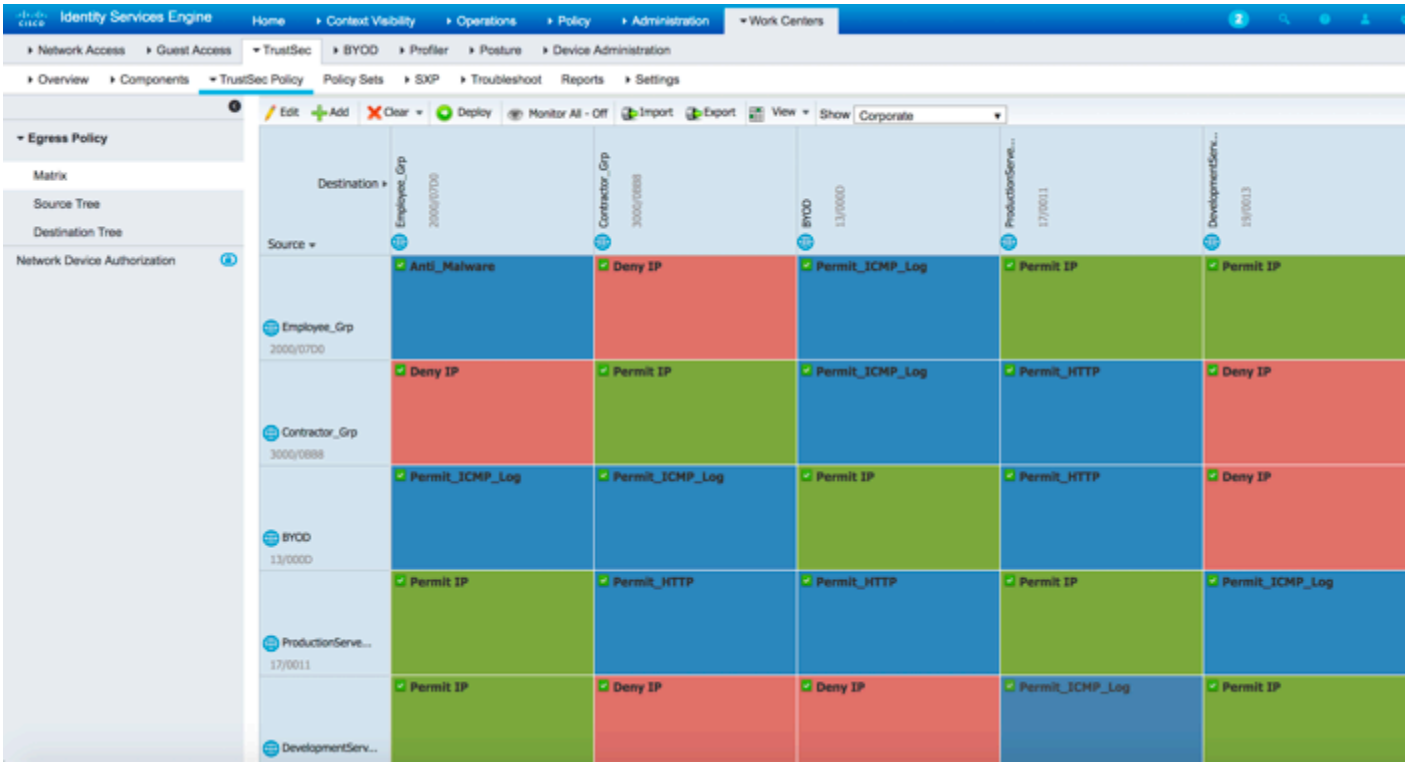
TrustSec Policy Matrix in ISE

TrustSec Policy Matrix in ISE needs to be configured to enforce the policy on the access and datacenter switches (Cat6k, N1kv, N7k etc.) 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.

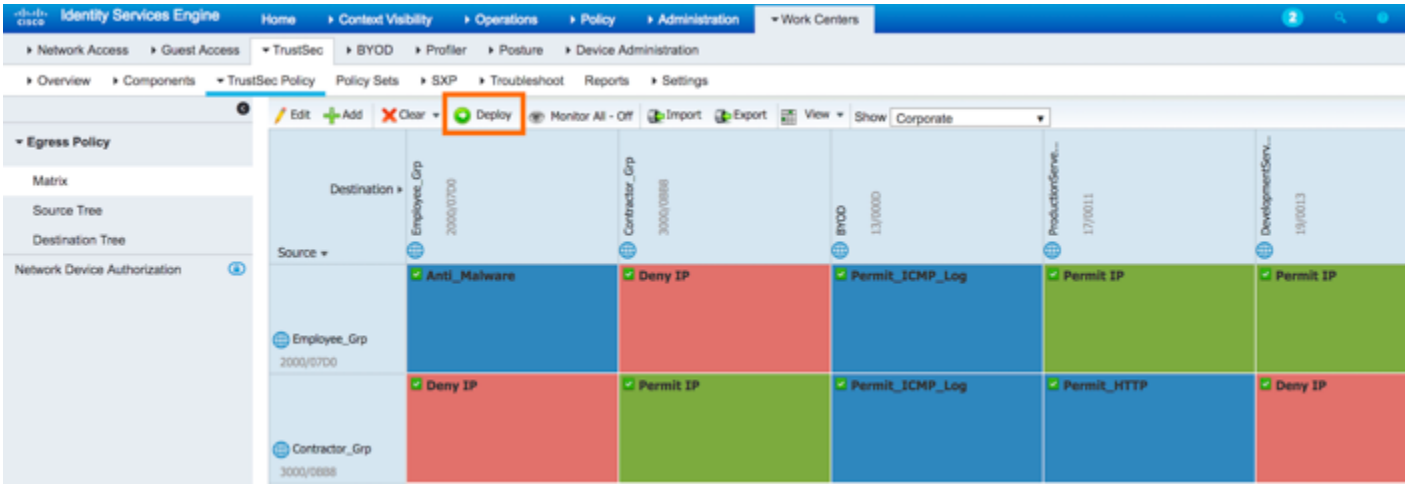
Step 4 Navigate to **Work Centers > TrustSec > TrustSec Policy > Egress Policy** and click **Matrix** to configure the TrustSec policy Matrix in ISE

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

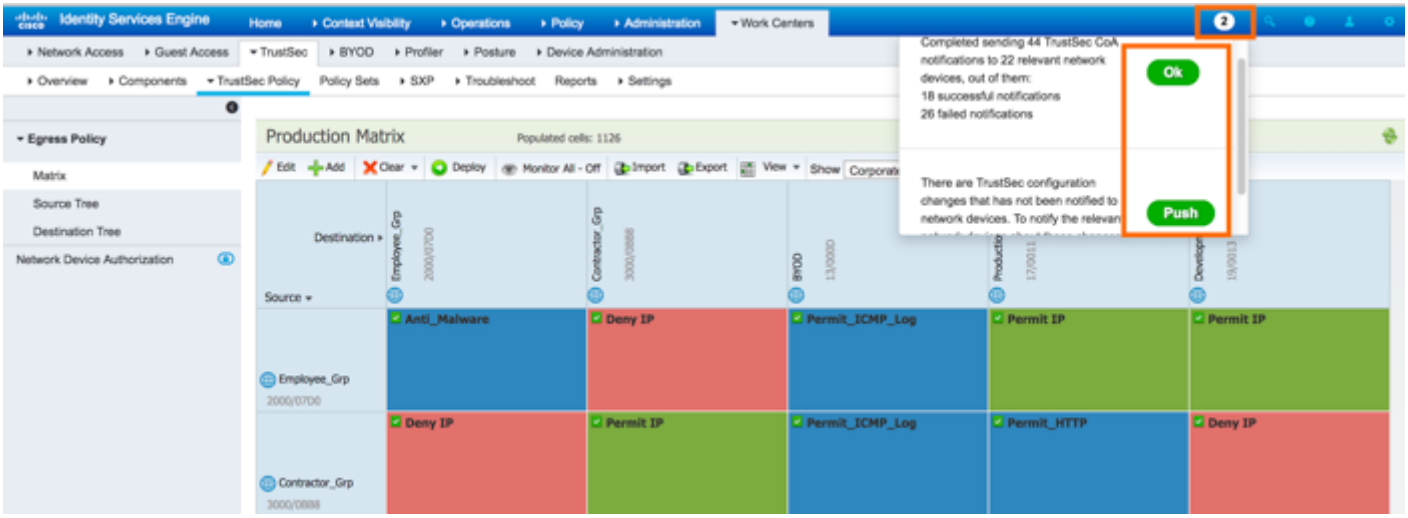
Note: The below configured TrustSec Policy Matrix is just for your reference.



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

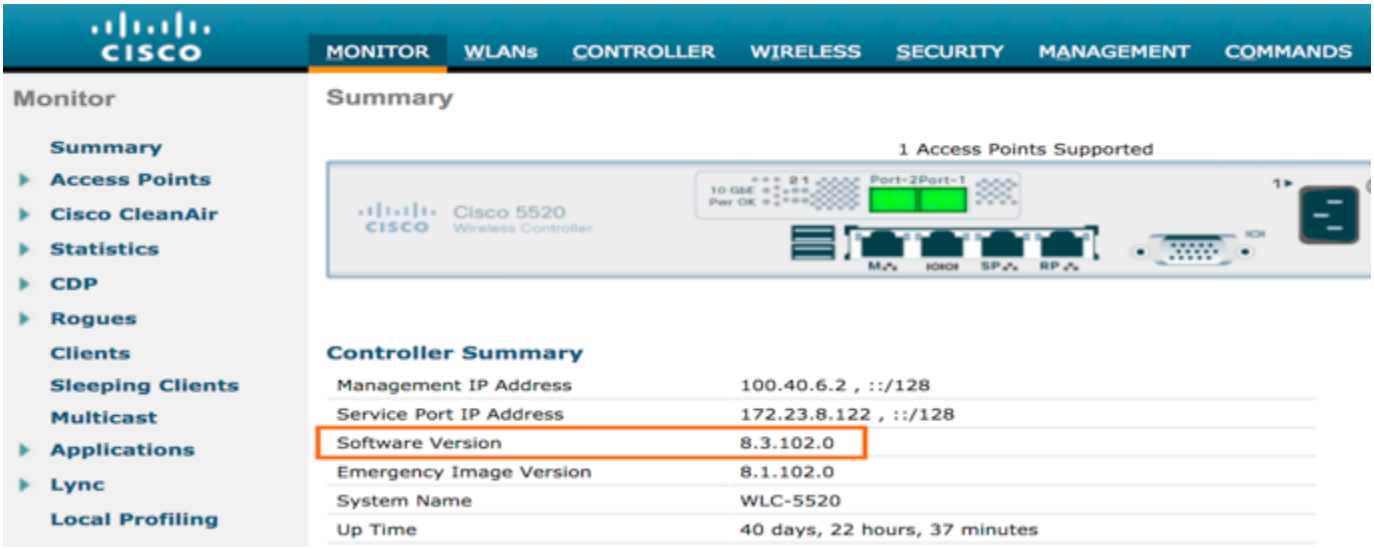


Step 6 After the Matrix is deployed look for the notifications messages (CoA) on the upper right corner. **Push** to send any configuration changes to the network devices or click **OK** to acknowledge the notification messages



WLC Configuration

In order to have TrustSec SXP support on FlexConnect APs, ensure that the WLC is running 8.3.102 or later code.

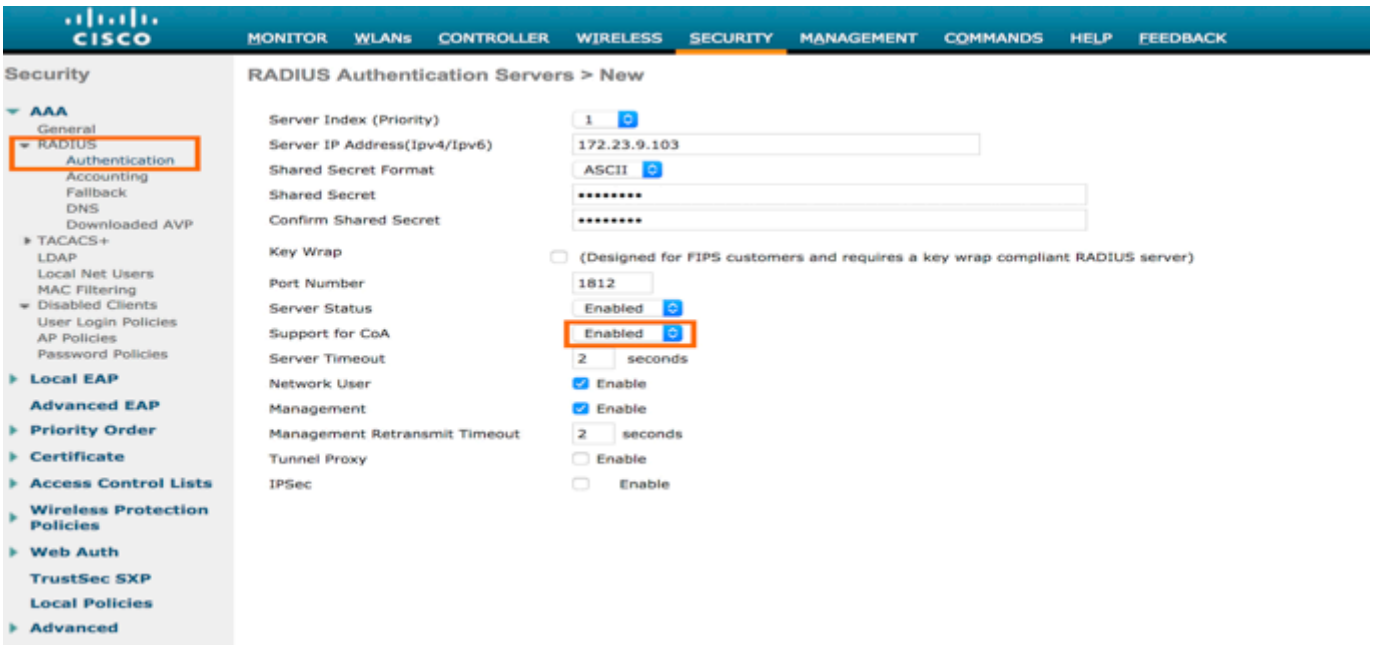


Radius Configuration on WLC

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

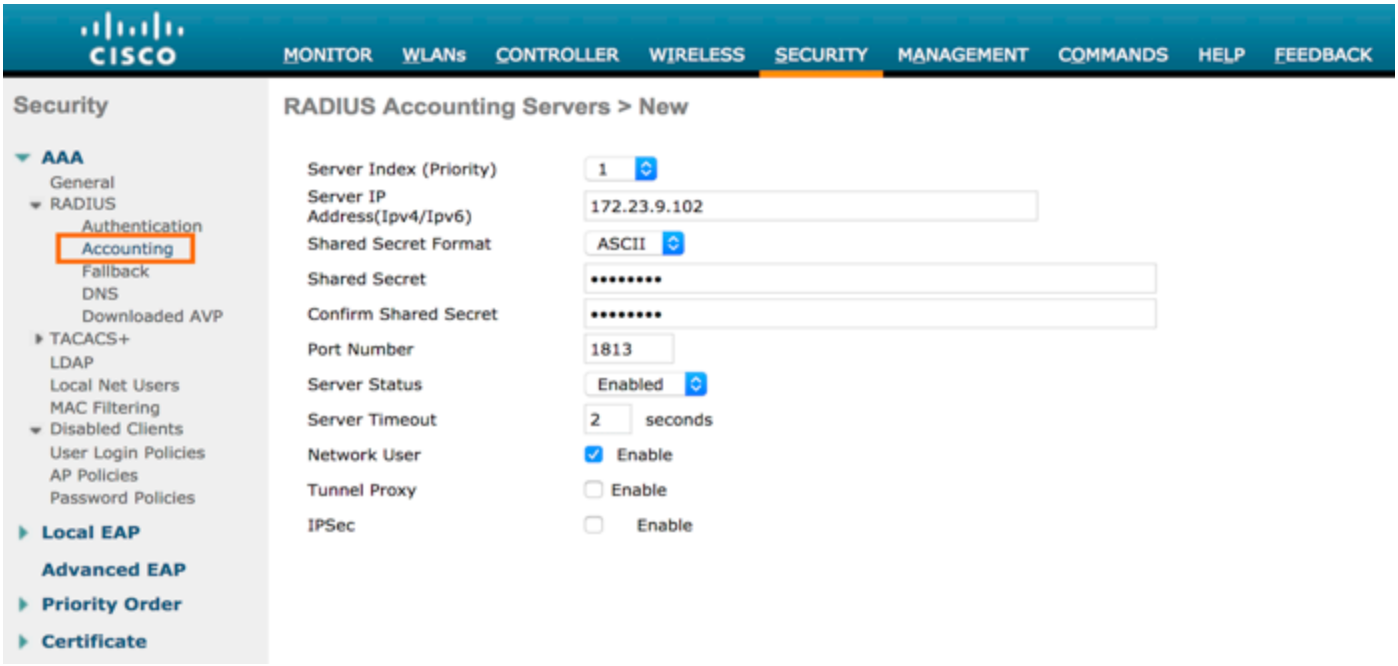
Step 7 From WLC navigate to **Security > Radius > Authentication** and Click **New**

Step 8 Add the **Server IP address** of the ISE PSN and use the same **Shared Secret** configured in ISE and Enable the **Support for CoA** and click **Apply**



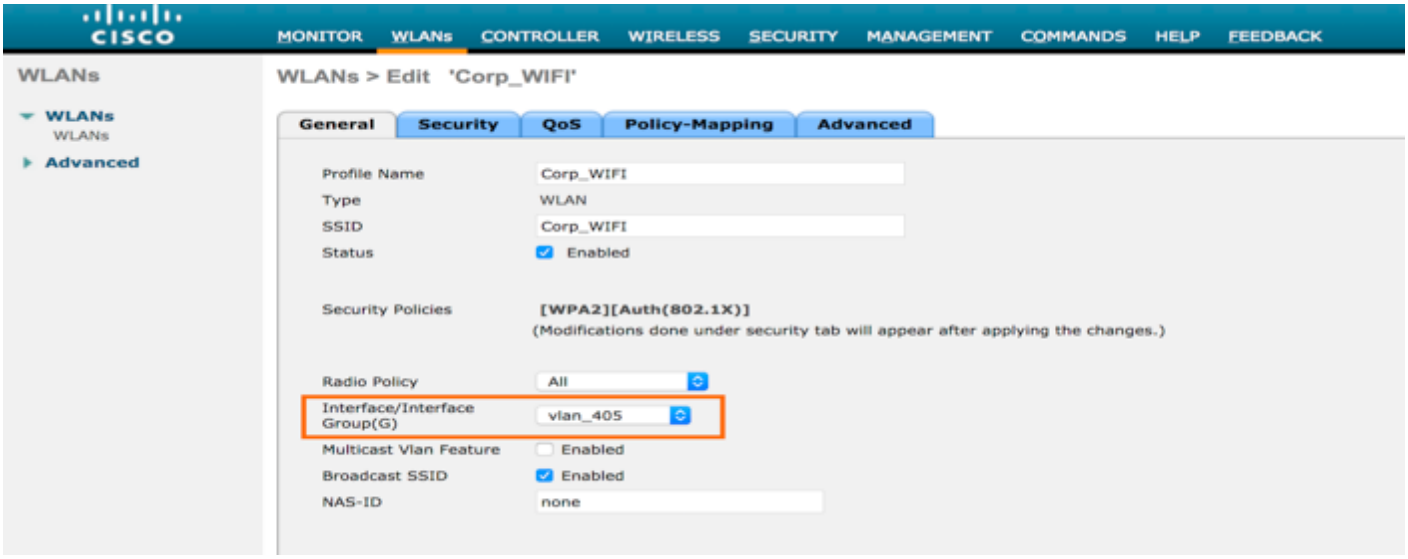
Step 9 From WLC navigate to **Security > Radius > Accounting** and Click **New**

Step 10 Add the **Server IP address** of the ISE PSN and use the same **Shared Secret** configured in ISE and click **Apply**

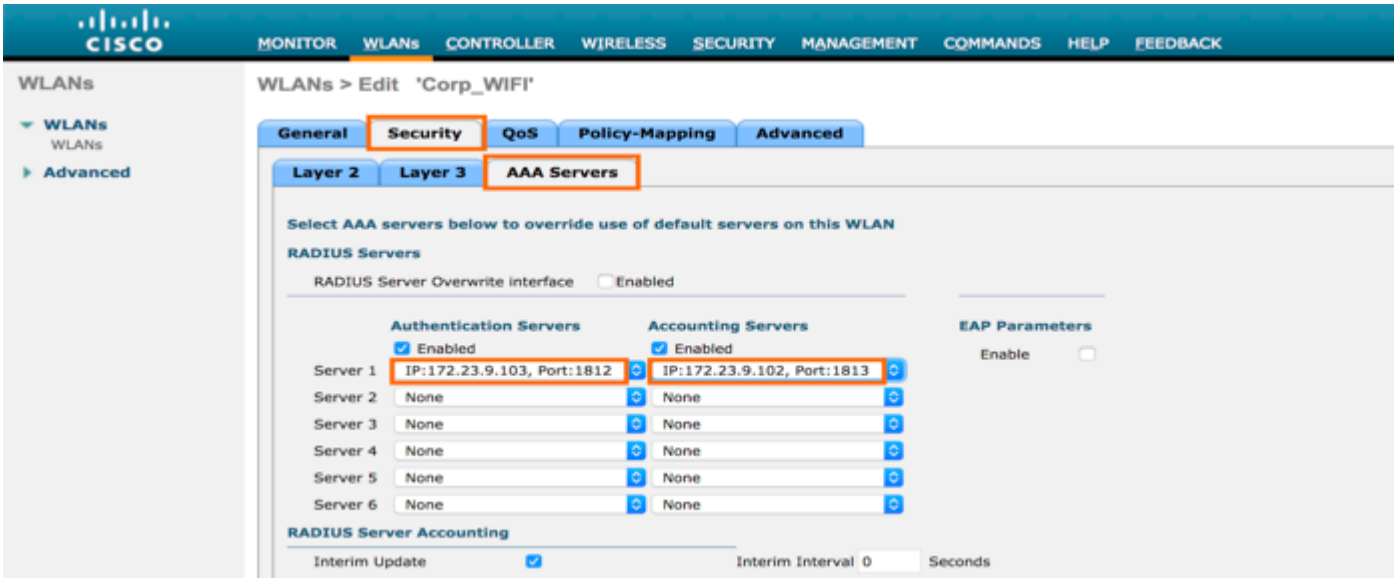


WLAN Configuration on WLC

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

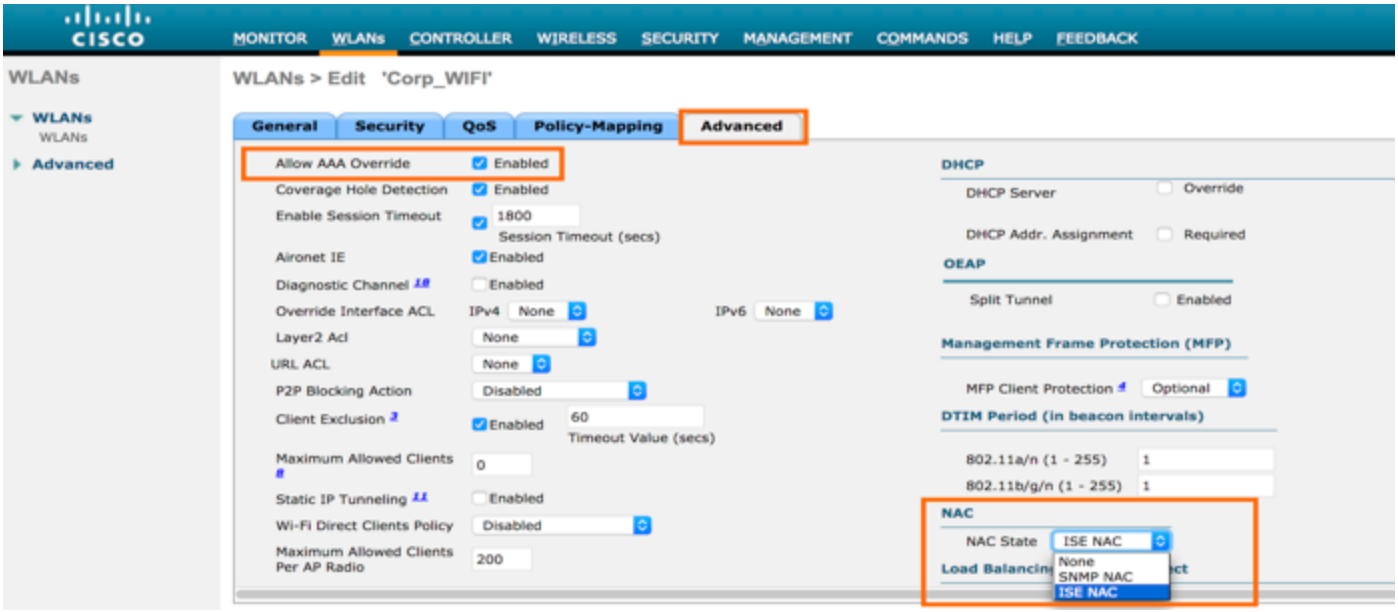


Step 2 Click on **Security > AAA Servers** and select the ISE PSN as the Authentication and Accounting Server from the drop down



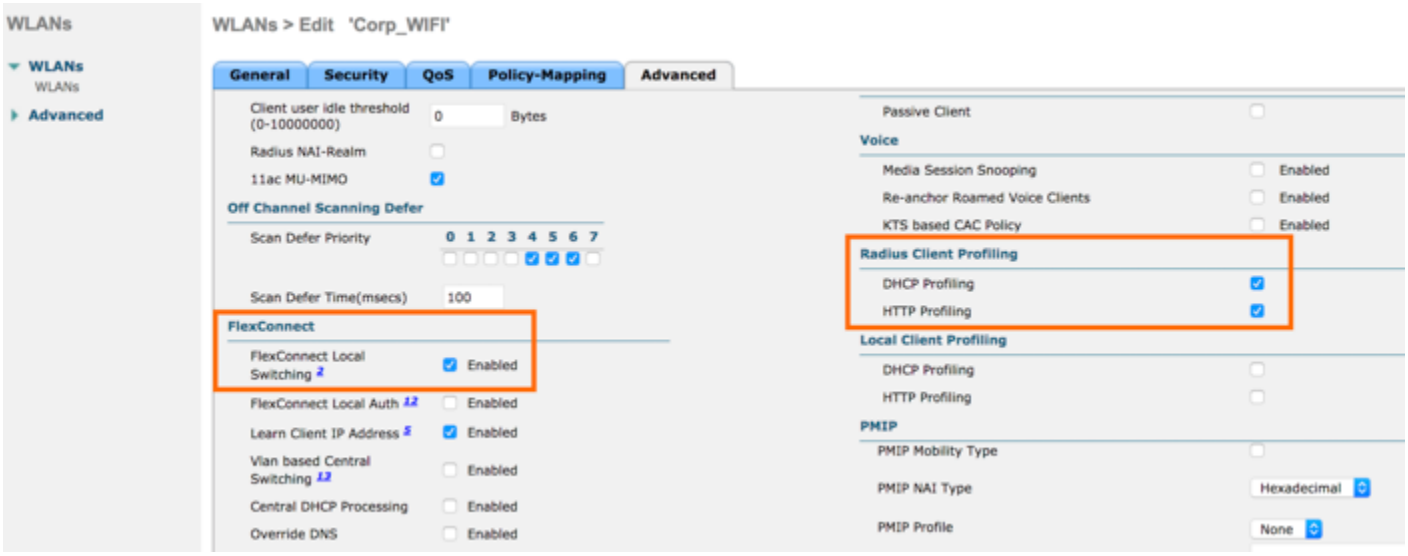
Step 3 Click **Advanced** tab and Enable **Allow AAA Override** and select **NAC State** from the dropdown as **ISE NAC**

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



Step 4 Scroll down in the **Advanced** Tab and Enable **FlexConnect Local Switching** to run WLAN in FexConnect Local Switching mode

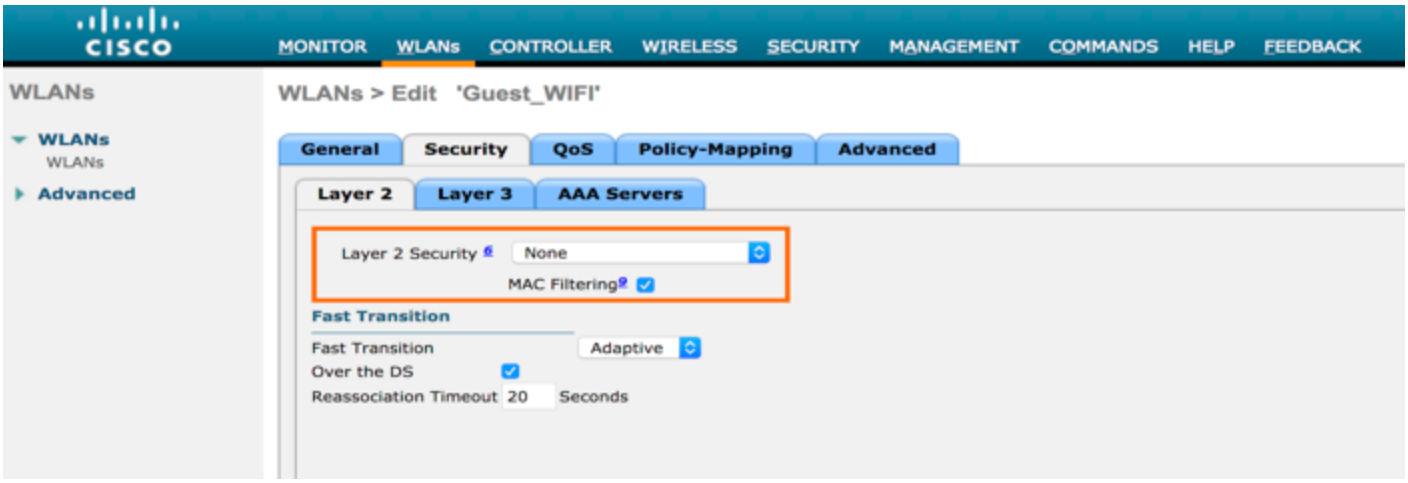
Step 5 Use ISE PSNs to profile the endpoints and users connecting to this SSID by enabling DHCP Profiling and HTTP Profiling



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

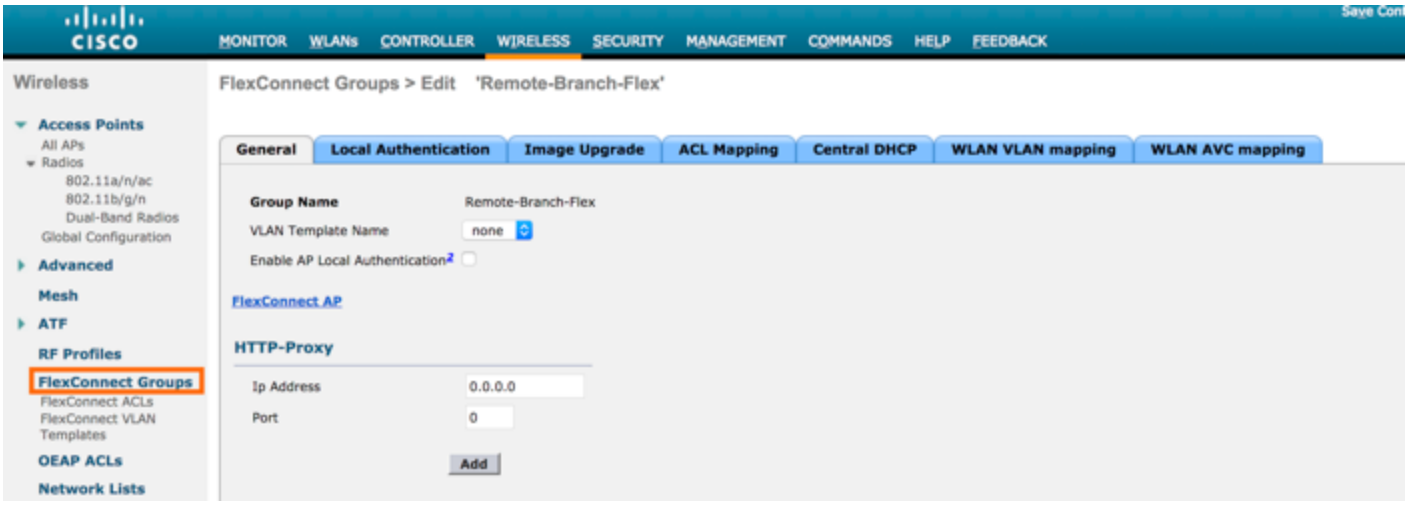
Step 7 Repeat the **steps 2** to **6** for the rest of the SSIDs in the network

Step 8 Here is an example of **Guest** SSID in the network with **MAC Filtering** enabled for the Guest user authentication



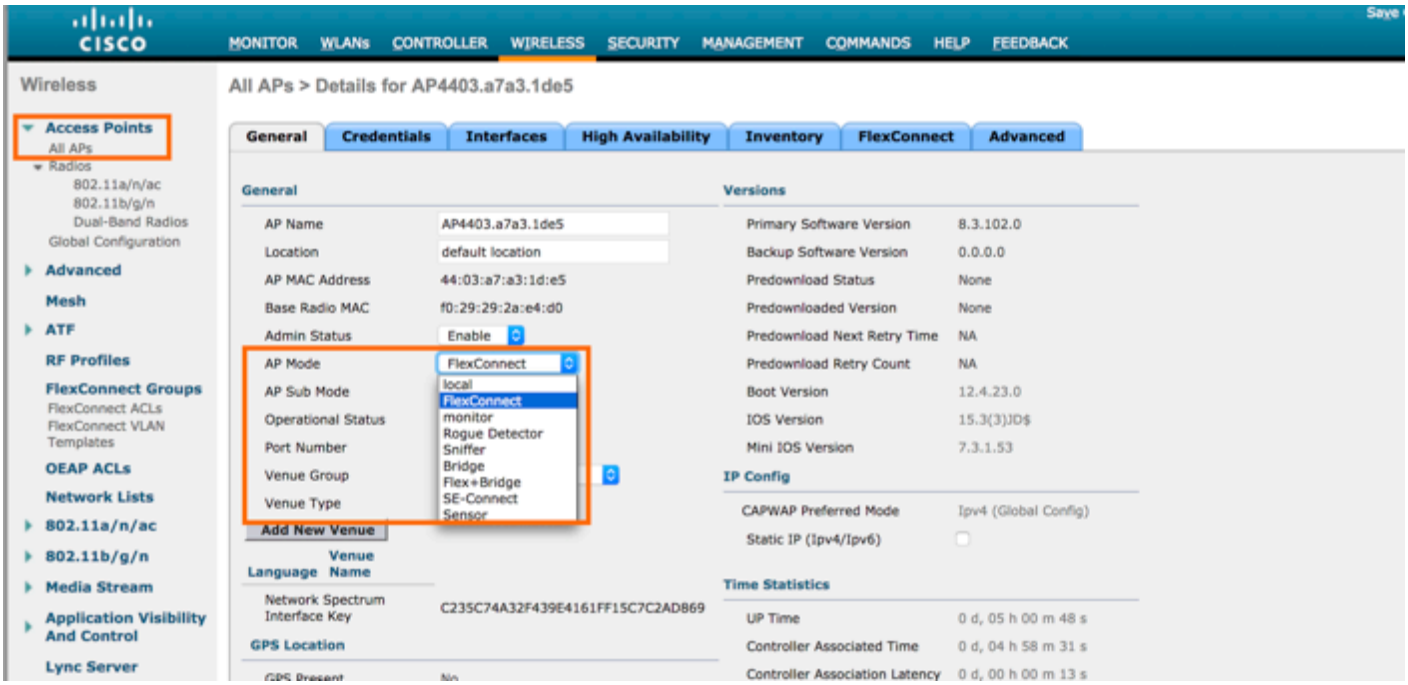
FlexConnect Configuration on WLC and AP

Step 1 From WLC navigate to **Wireless > FlexConnect Groups** and Click **New** and add a name to the FlexConnect group

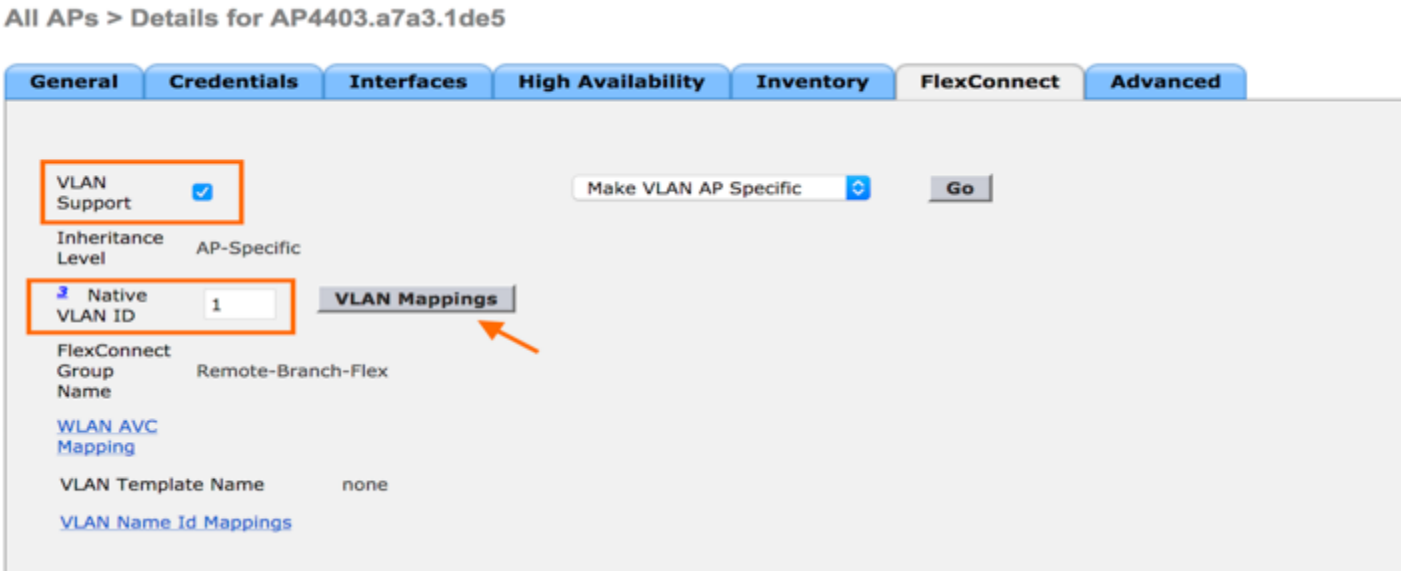


Step 2 Add the existing AP in the branch to the newly created FlexConnect Group by Navigating to **Wireless > All APs**

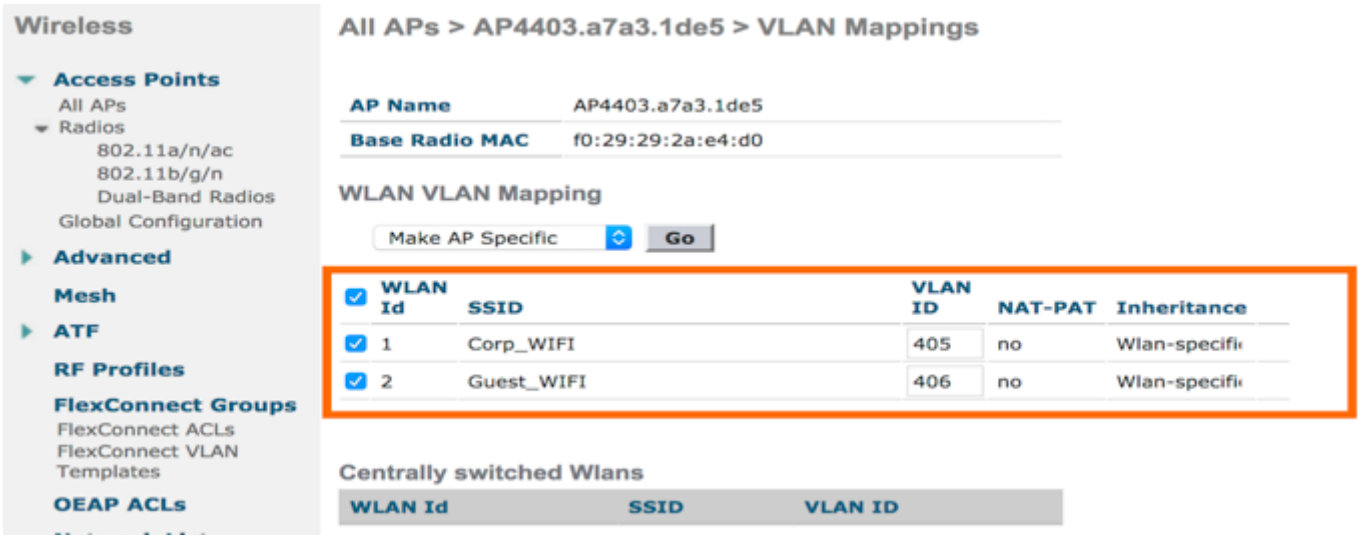
Step 3 Click the **AP name** for Details and from **General** Tab select the **AP mode** as **FlexConnect**



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**



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

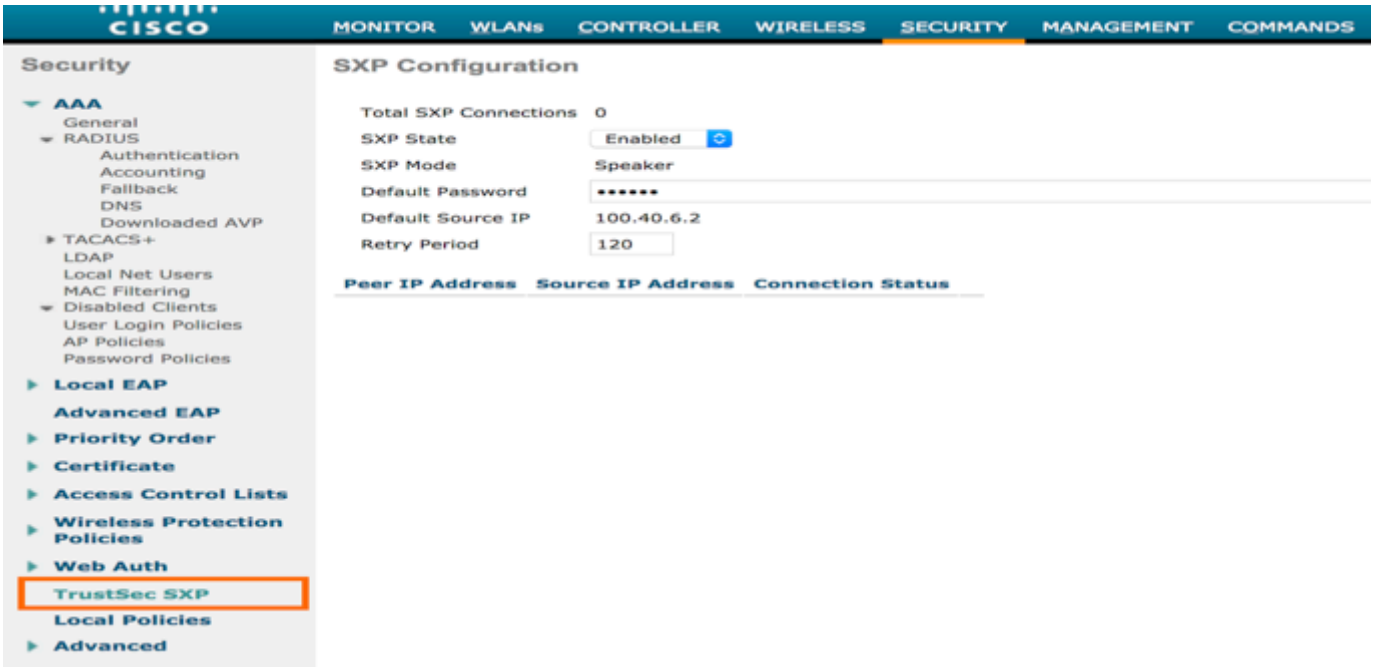
Cisco TrustSec filters packets at the egress interface. During endpoint authentication, a host accessing the Cisco TrustSec domain (the endpoint IP address) is associated with an SGT at the access device through Dynamic Host Control Protocol (DHCP) snooping and IP device tracking. The access device transmits 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.

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

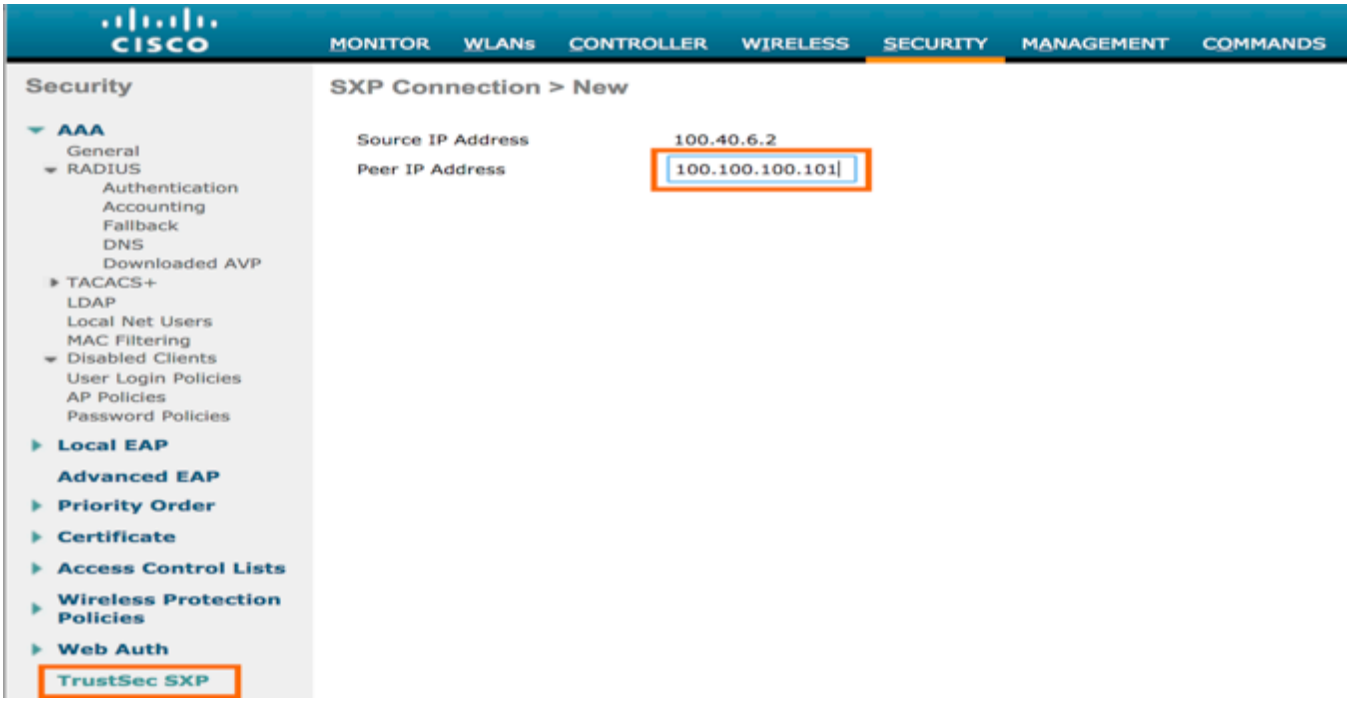


- **Total SXP Connections**—Number of SXP connections that are configured.
- **SXP State**—Status of SXP connections as either disabled or enabled.
- **SXP Mode**—SXP mode of the controller. The controller is always set to Speaker mode for SXP connections.
- **Default Password**—Password for MD5 authentication 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.

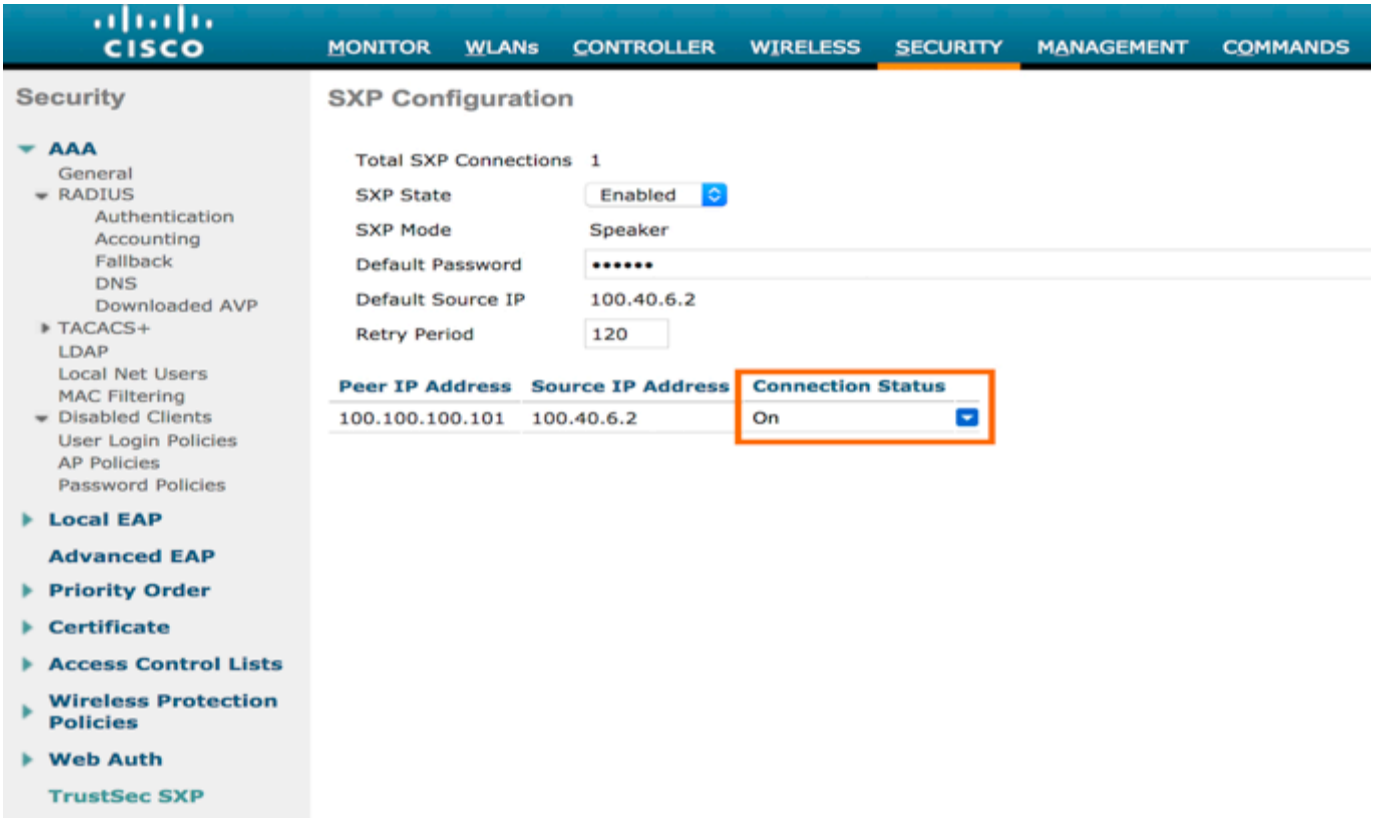
- **Retry Period**—SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000 seconds. The SXP retry period determines how often the controller retries for an SXP connection. When an SXP connection is not successfully set up, the controller makes a new attempt to set 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 Click **New** on the right to add a new SXP connection

Step 3 Add the **Peer IP address** to which the WLC can send the IP-SGT mappings and click **Apply**



Step 4 The **Connection Status** moves from **OFF** to **On** to form a successful SXP peering with the network device



Use Cases on SXP Peering and Policy Enforcement

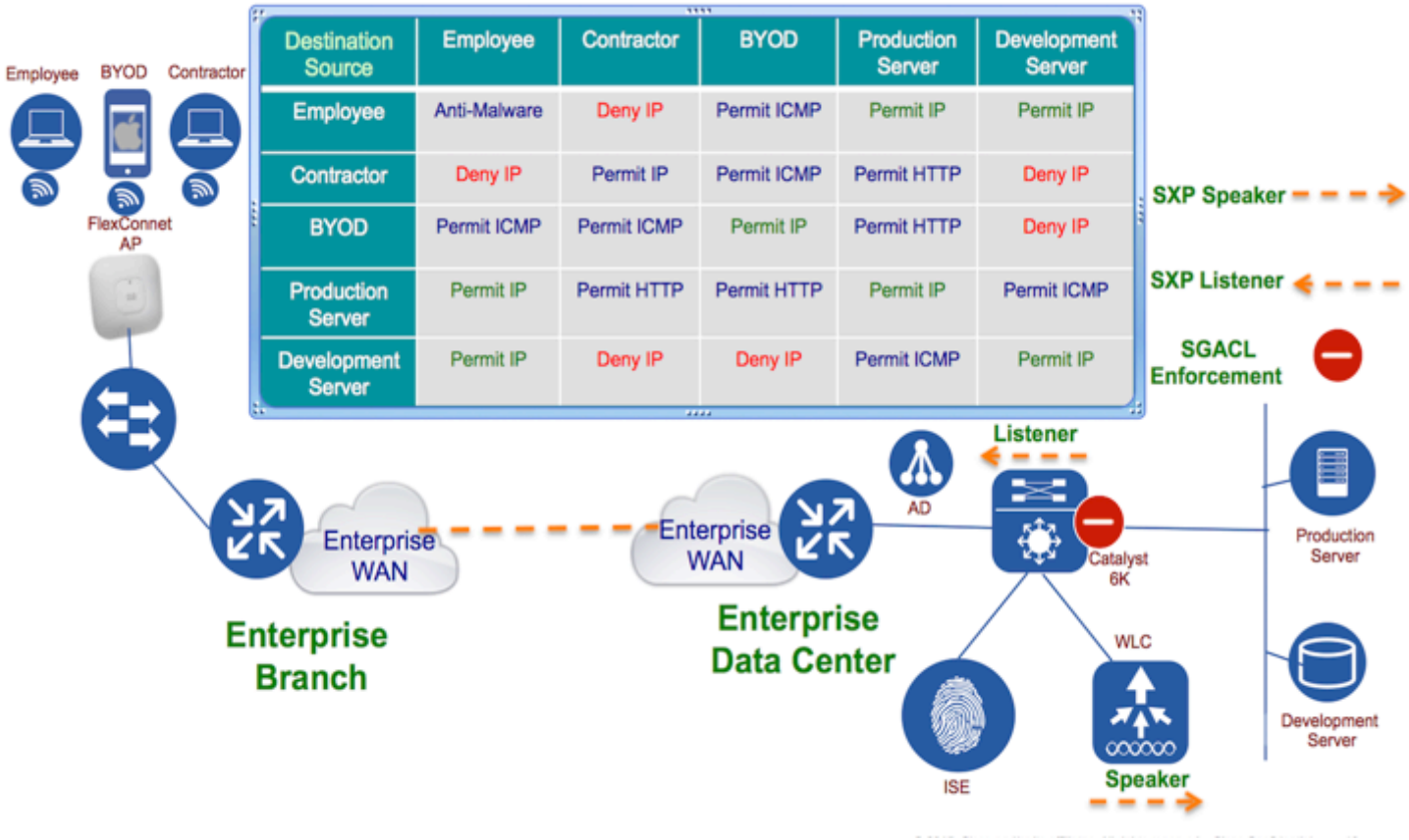
Depending on the policy goals of a given organization, different use-cases may call for SXP peering (with the WLC) and policy enforcement. In this configuration guide couple of scenarios are included for reference based upon customer experience and feedback.

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

Sample Use Case of FlexConnect with SXP Peering and SGACL enforcement on Cat6K

Cat6K is most widely deployed Campus Core / Data Center core network device. This use case will walk you through the basic configuration showing SXP peering between the Cat6K and WLC. WLC would act as SXP (SXPv2) speaker and Cat6K would act as SXP listener to form the SXP peering. All the IP-SGT binding information from the WLC would be learned by switch. Since Cat6K supports SGACL enforcement, through TrustSec Policy Matrix, ISE would centrally push the SGACLs to Cat6K switch. It can either enforce the policy locally or share the IP-SGT bindings to other enforcement devices using SXP or Inline Tagging (SGT over Ethernet).

Figure 2: Topology showing a wireless FlexConnect deployment with SXP and enforcement on Cat6K



The above topology shows three users Employee, Employee with Mobile device or BYOD device and a Contractor connecting to an Access Point running in the FlexConnect mode in an enterprise Branch network. The enterprise branch network is connected to the enterprise Data Center over the WAN. The Cat6K switch acting as the core device in the data center is connected to the WLC. WLC would act as a SXP Speaker and Cat6K would act as an SXP Listener to form the SXP peering. 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 IP-SGT information from the WLC now would be shared with the Cat6K switch. Through the TrustSec Policy Matrix, ISE would push the SGACLs (shown in the topology) to the Cat6K switch. By looking at the Source and Destination Group Tag and the downloaded SGACL policy Cat6k would enforce the policy and would allow or deny the network access to the endpoints and servers in the data center.

Step 1 Configure SXP on the Cat 6K. Here are the commands which needed to enable SXP and forming a connection peering with the WLC

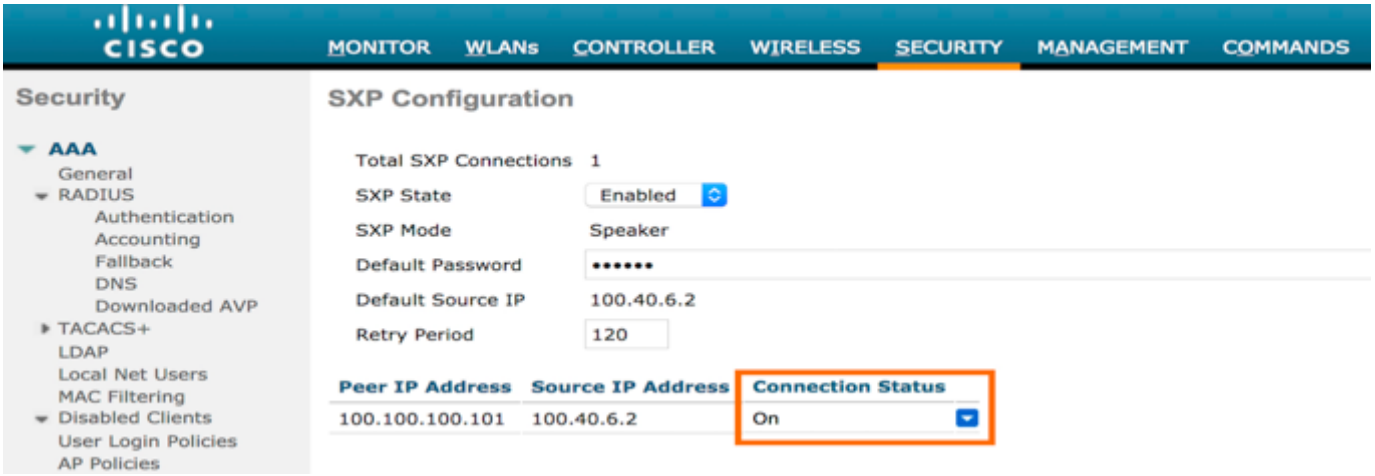
```
6506E-VSS#show run | i sxp
cts sxp enable
cts sxp default password <#####>
cts sxp retry period 10
cts sxp connection peer 100.40.6.2 source 100.100.100.101 password default mode
local listener hold-time 0 0
```

Note: The default password should be same on both Cat6K and the WLC

Step 2 To configure SXP on the controller navigate to **Security > TrustSec SXP**

Step 3 Add the Cat6K IP address in the **Peer IP address** and click **Apply**

Step 4 One successful the **Connection Status** should be **ON**



Step 5 Validate the connection status on the Cat6K with the below command. The connection version is **2** since WLC supports **SXPv2**

Note: Though 6K supports SXP version 4 it will negotiate to SXPv2 since WLC only supports SXPv2

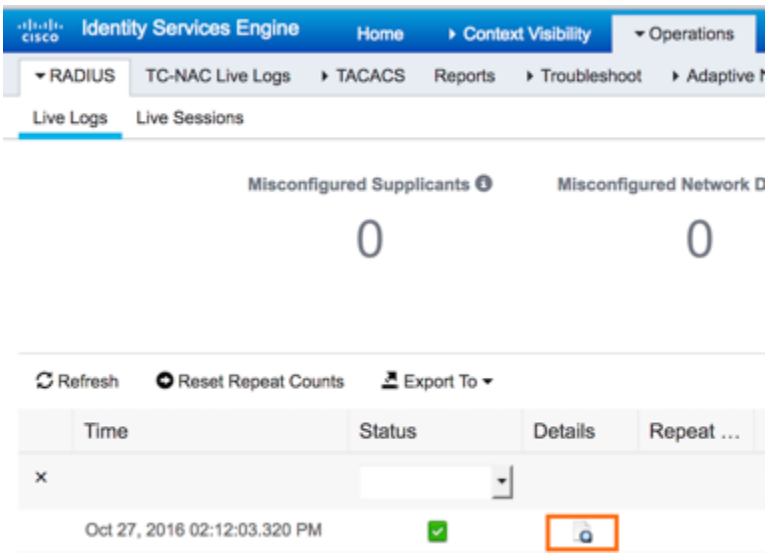
```
6506E-VSS#show cts sxp connections
 SXP                : Enabled
 Highest Version Supported: 4
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is running
----------------------------------------------
Peer IP           : 100.40.6.2
Source IP         : 100.100.100.101
Conn status       : On
Conn version      : 2
Local mode        : SXP Listener
Connection inst#  : 42
TCP conn fd       : 10
TCP conn password: default SXP password
```

```
Duration since last state change: 0:00:30:28 (dd:hr:mm:sec)--------------------
-------------------------
```

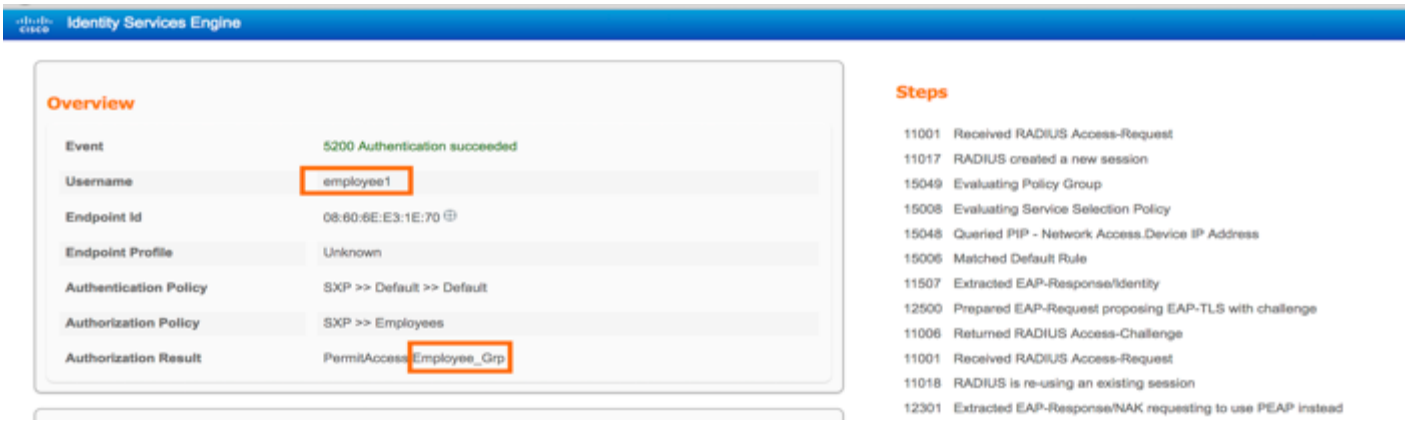
Step 6 Now connect the Employee PC to the wireless SSID

Step 7 The employee should be assigned an **Employee SGT** (**Employee_Grp**) dynamically as per the Authorization policy configuration earlier during the ISE configuration

Step 8 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 9 The **Live Logs Details** shows the all the endpoint details including the Security Group it got assigned



Authentication Details

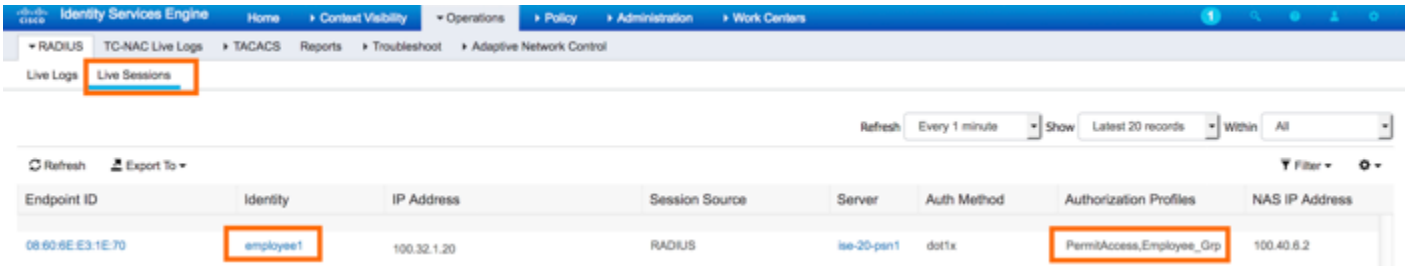
Source Timestamp	2016-10-25 06:59:24.387
Received Timestamp	2016-10-25 06:59:24.387
Policy Server	ise-20-psn1
Event	5200 Authentication succeeded
Username	employee1
Endpoint Id	08:60:6E:E3:1E:70
Calling Station Id	08-60-6e-e3-1e-70
Endpoint Profile	Unknown
Authentication Identity Store	AD1
Identity Group	Unknown
Audit Session Id	0206286400000027b640f58
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	WLC-5520
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	100.40.6.2
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	PermitAccess,Employee_Grp
Security Group	Employee_Grp

11018	RADIUS is re-using an existing session
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated
12318	Successfully negotiated PEAP version 0
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12810	Prepared TLS ServerDone message
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request (Step latency=2383 ms)
11018	RADIUS is re-using an existing session
11042	Received duplicate RADIUS request; retransmitting previous response
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
12318	Successfully negotiated PEAP version 0
12812	Extracted TLS ClientKeyExchange message
12813	Extracted TLS CertificateVerify message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
12802	Prepared TLS Finished message

Result

State	ReauthSession:0206286400000027b640f58
Class	CACS:0206286400000027b640f58:ise-20-psn1/263187244/1565636
cisco-av-pair	cts:security-group-tag=07d0-60
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Base license consumed

Step 10 Similarly look in the Live Sessions in ISE by navigating to **Operations > RADIUS > Live Sessions**



Step 11 Now look for the IP-SGT binding information on switch using the below command. The endpoints, which are connected to the FlexConnect AP that got a Tag, would be seen in 6K since the WLC sends all the IP-SGT mappings through SXP to Cat6K

```
6506E-VSS#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
2.2.2.2                 2       INTERNAL
90.90.90.10             19      CLI
90.90.90.20             17      CLI
90.90.90.50             16      CLI
90.98.90.78             140     CLI
100.18.1.100            181     CLI
100.30.100.2            2       INTERNAL
100.32.1.1              2       INTERNAL
100.32.1.20             2000    SXP
100.32.1.21             2000    SXP
100.32.1.22             3000    SXP
100.32.1.23             3000    SXP
100.50.1.1              2       INTERNAL
100.50.1.12             501     CLI
100.50.1.20             501     CLI
100.50.2.1              2       INTERNAL
100.50.2.11             502     CLI
100.50.2.12             502     CLI
100.50.4.11             504     CLI
100.50.5.1              2       INTERNAL
100.50.5.11             505     CLI
100.50.6.1              2       INTERNAL
100.50.6.12             506     CLI
100.51.1.1              2       INTERNAL
100.60.1.1              2       INTERNAL
100.60.1.6              2       INTERNAL
100.70.1.11             70      CLI
100.78.7.2              2       INTERNAL
100.100.100.101         2       INTERNAL
100.102.1.11            70      CLI
100.202.1.254           2       INTERNAL
187.1.1.1               9       CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 15
Total number of SXP      bindings = 4
Total number of INTERNAL bindings = 13
Total number of active   bindings = 32
```

The above command shows all the IP-SGT mappings. Look for the bindings from SXP. The Security Groups in this use case of **Employee** and **Contractor** are **2000** and **3000**. These IP-SGT mappings are sent by the WLC. The Security Groups with a Tag **19** and **17** are **Development Servers** and **Production Servers**, which are configured statically through the CLI on the switch

Step 12 The below specific command on Cat6K shows all the SXP mappings it received.

```
6506E-VSS#show cts sxp sgt-map brief
SXP Node ID(generated):0x64646465(100.100.100.101)
IP-SGT Mappings as follows:
IPv4,SGT: <100.32.1.21 , 2000:Employee_Grp>
IPv4,SGT: <100.32.1.22 , 2000:Employee_Grp>
IPv4,SGT: <100.32.1.23 , 3000:Contractor_Grp>
IPv4,SGT: <100.32.1.24 , 3000:Contractor_Grp>
Total number of IP-SGT Mappings: 4
```

Step 13 On Cat6K Use the below command to view the role-based permissions between the security groups downloaded from ISE through the TrustSec Policy Matrix

```
6506E-VSS#show cts role-based permissions
IPv4 Role-based permissions default:
    Permit_IP_Log-10
IPv4 Role-based permissions from group 13:BYOD to group 3000:Contractor_Grp:
    Permit_ICMP_Log-30
IPv4 Role-based permissions from group 17:ProductionServers_Grp to group
3000:Contractor_Grp:
    Permit_HTTP-10
IPv4 Role-based permissions from group 19:DevelopmentServers_Grp to group
3000:Contractor_Grp:
    Deny IP-00
IPv4 Role-based permissions from group 2000:Employee_Grp to group
2000:Employee_Grp:
    Anti_Malware-00
IPv4 Role-based permissions from group 2000:Employee_Grp to group
3000:Contractor_Grp:
    Deny IP-00
IPv4 Role-based permissions from group 3000:Contractor_Grp to group
3000:Contractor_Grp:
    Permit IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Step 14 Type the below command to view the SGACL entries downloaded from ISE

```
6506E-VSS#show cts rbacl
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name    = Anti_Malware-00
  IP protocol version = IPV4
  refcnt = 2
  flag    = 0x41000000
  stale   = FALSE
  RBACL ACEs:
    permit  icmp
    deny udp src dst eq domain
    deny tcp src dst eq 3389
```

```
    deny tcp src dst eq 1433
    deny tcp src dst eq 1521
    deny tcp src dst eq 445
    deny tcp src dst eq 137
    deny tcp src dst eq 138
    deny tcp src dst eq 139
    deny udp src dst eq snmp
    deny tcp src dst eq telnet
    deny tcp src dst eq www
    deny tcp src dst eq 443
    deny tcp src dst eq 22
    deny tcp src dst eq pop3
    deny tcp src dst eq 123
    deny tcp match-all -ack +fin -psh -rst -syn -urg

  name   = Deny IP-00
  IP protocol version = IPV4, IPV6
  refcnt = 4
  flag   = 0xC1000000
  stale  = FALSE
  RBACL ACEs:
    deny ip

  name   = Permit_HTTP-10
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit tcp src eq 80
    permit tcp src eq 443

  name   = Permit_ICMP_Log-30
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit icmp log

6506E-VSS#
```

Step 15 To validate the policy enforcement on the switch, **Role-Based Enforcement** needs to be enabled. Enable enforcement on the switch with the below command

```
6506E-VSS(config)#cts role-based enforcement
```

Step 16 Validate the policy enforcement on the switch with the **counters** command. To check the counters on the switch use the following command.

```
6506E-VSS#show cts role-based counters
```

Step 17 For example if a **Contractor** (**SGT 3000**) tries to access the **Development Server** (**SGT 19**) he should be denied access as per the configured policy and the deny counters on the switch need to be incremented. Similarly if an Employee (SGT 2000) tries to access the Development Server (SGT 19) he should be permitted access and the permit counters need to be incremented

```
6506E-VSS#show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-
Monitor
*       *       0          0          533526     0          0          0
2       0       0          0          0          18377      0          0
0       2       0          0          622542     0          0          0
2       2       0          0          62376      0          0          0
2000    17      0          0          0          0          0          0
2000    19      0          0          0          34762      0          0
3000    17      0          0          0          0          0          0
3000    19      0          2485       0          0          0          0
4000    501     0          0          0          34758      0          0
13      3000    0          0          0          0          0          0
14      3000    0          0          0          0          0          0
17      3000    0          0          0          0          0          0
19      3000    0          0          0          0          0          0
2000    3000    0          0          0          0          0          0
3000    3000    0          0          0          0          0          0
6506E-VSS#
```

Step 18 Cat6K switch even provides an option to view the counters between the specific security groups. To view the counters between the specific security groups use the following command. The below example shows the counters between the **Contractor** (**SGT 3000**) and the **Development Server** (**SGT 19**)

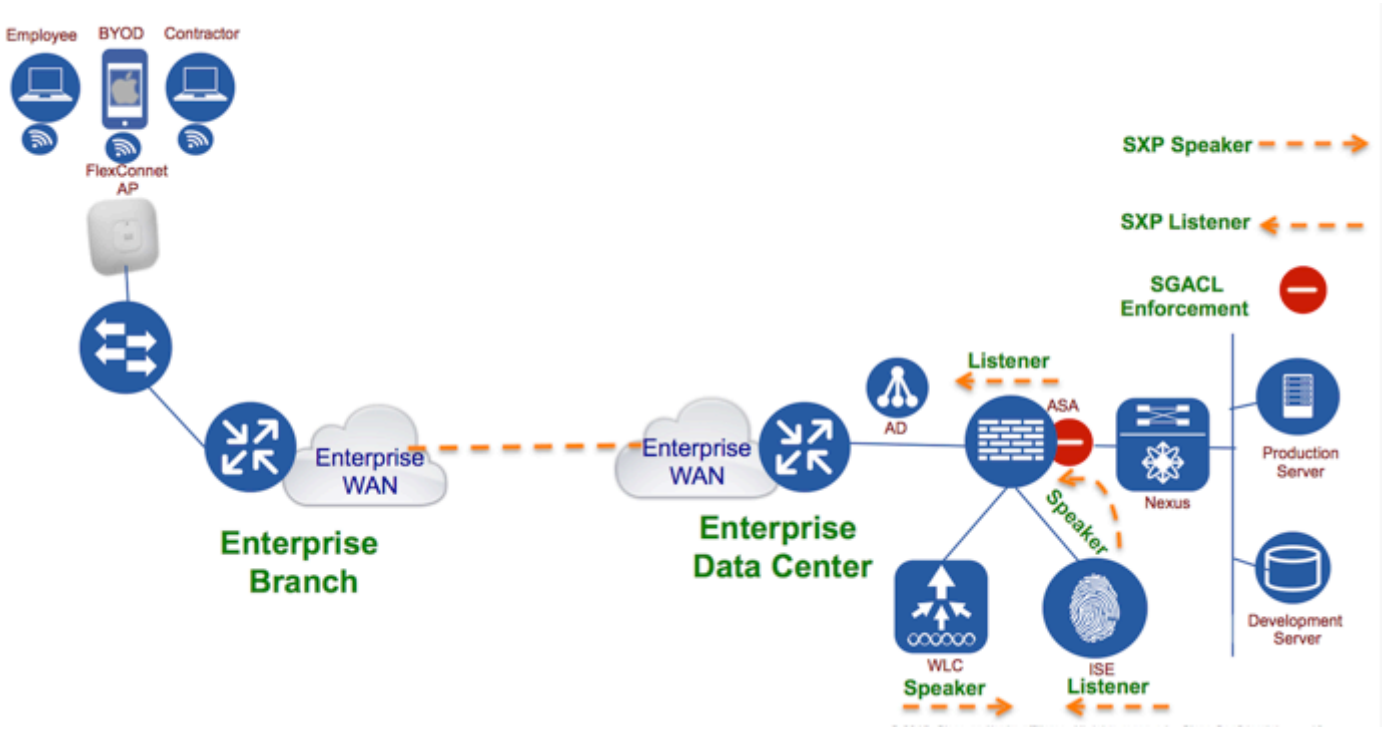
```
6506E-VSS#show cts role-based counters from 3000 to 19
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-
Monitor
3000    19      0          2485       0          0          0          0
```

An employee or a contractor connecting from a remote branch office wireless Access Point running in FlexConnect Local mode now can be assigned a security group tag and are allowed or denied network access based on their roles thus providing access control and wireless segmentation using TrustSec.

Sample Use Case Showing SXP Peering between ISE and WLC

Instead of running SXP peering between the network devices and WLC even ISE can be used to form the peering with the WLC. For that the SXP service needs to be enabled on ISE. Since ISE 2.0, ISE can act as both SXP Speaker and SXP Listener. The peers can also be configured in bi-directional mode where each of them can act as both SXP Speaker and SXP Listener.

Figure 3: Topology showing a wireless FlexConnect deployment with SXP enabled on ISE

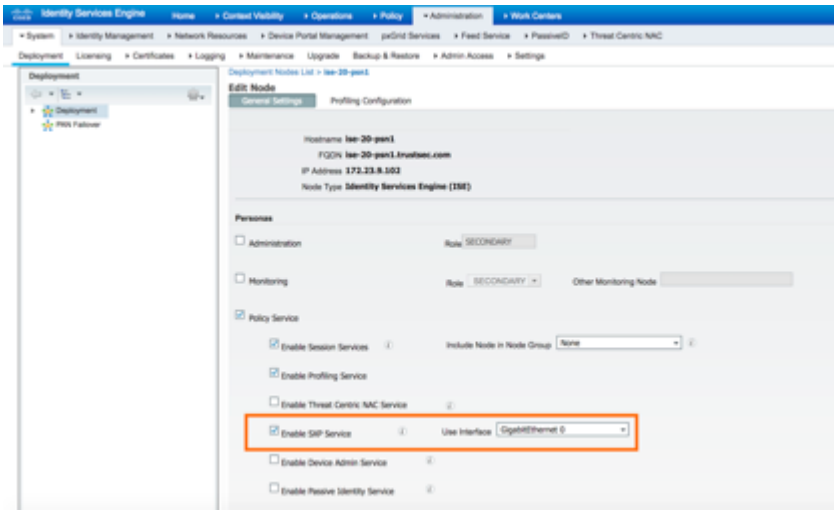


The above topology shows the SXP peering between ISE and WLC. Since ISE is acting as both SXP speaker and Listener it can not only receive the IP-SGT binding information from the WLC (SXP Speaker) but also can share the IP-SGT bindings to other devices in the network. The above topology shows ISE as a SXP Speaker sharing the IP-SGT binding information to an ASA. Here is the configuration to enable the peering between ISE and WLC.

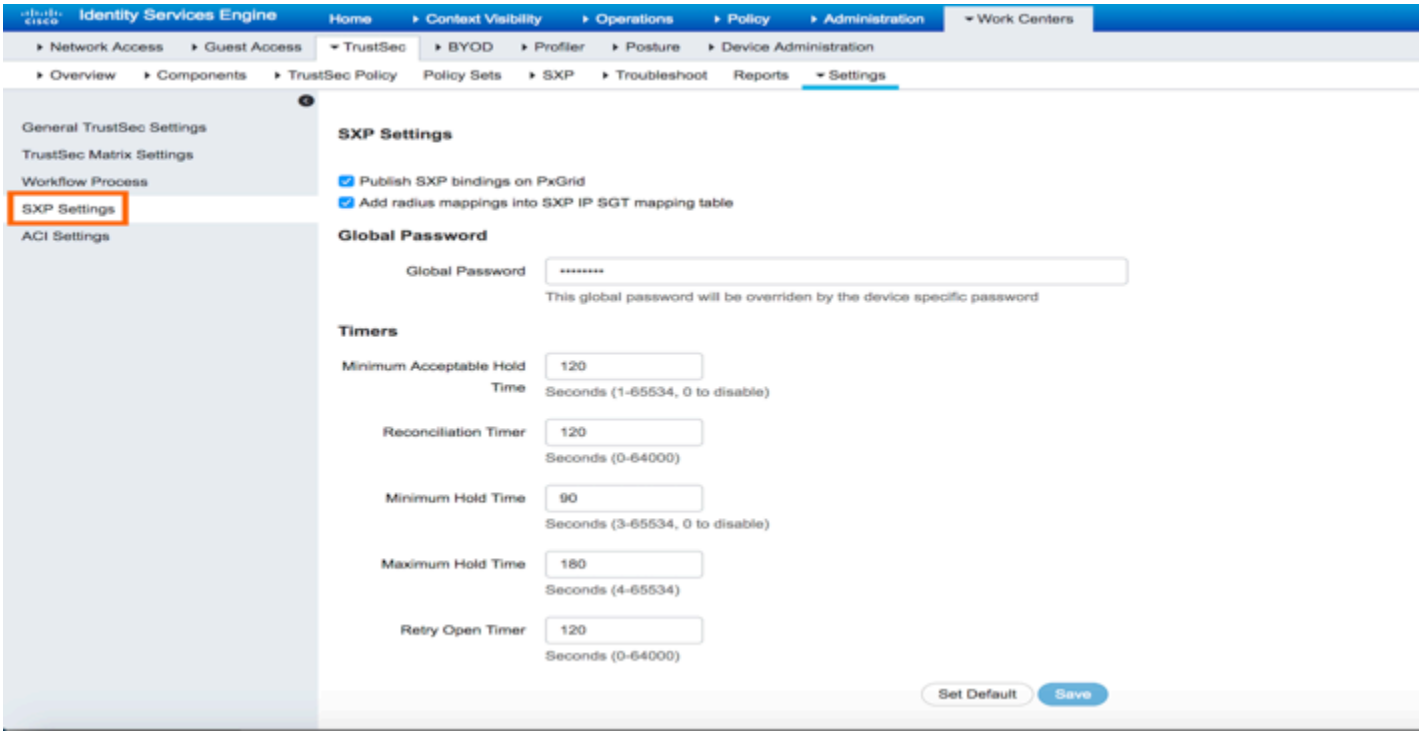
Step 1 To enable the SXP service on ISE node navigate to **Administration > System > Deployment**

Step 2 Edit the Node and **Enable SXP Service** check box in **General Node Settings** page and specify the ISE **interface** used for SXP service.

Note: It is recommended to run SXP service as a separate persona. ISE 2.1 can support up to four SXP nodes

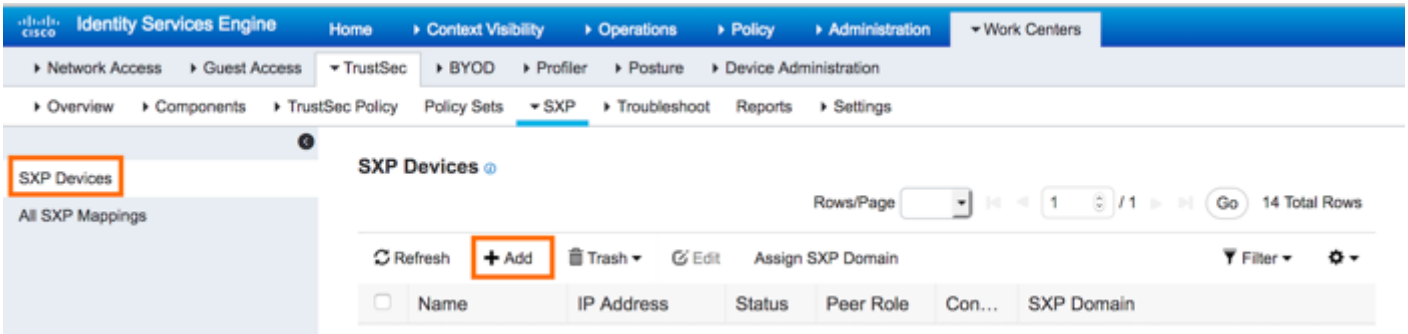


Step 3 Configure the **SXP Settings** in ISE by navigating to **Work Centers > TrustSec > Settings > SXP Settings**

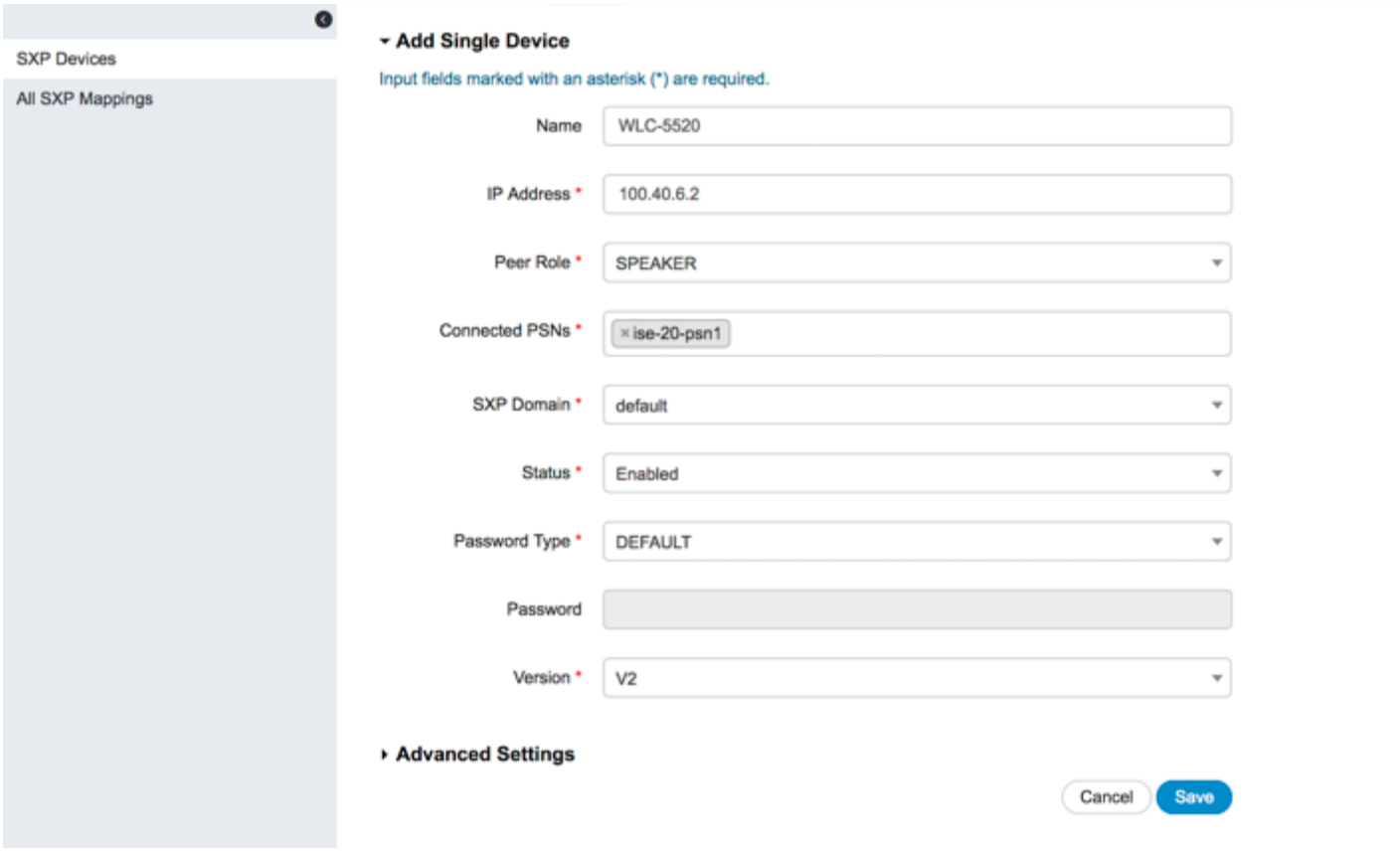


Step 4 Enable the Check Mark if intended to **Publish SXP bindings on PxGrid** nodes. Also Enable the Check Mark to **Add radius mappings into SXP IP SGT mapping table** where the IP-SGT bindings derived from radius session can be added under SXP mappings in ISE. Configure the **Global Password** to form the peering instead of a typing a custom password while adding a new SXP peer every time. Configure the **Timers** or can be left to default values.

Step 5 To add the WLC as the SXP Peer in ISE navigate to **Work Centers > TrustSec > SXP > SXP Devices** and Click **Add**



Step 6 Provide the **Name**, **IP Address**, **Peer Role** Speaker as WLC is a **SXP Speaker**, **Connected PSNs** on which the SXP Service is running, **SXP Domain** which could be default domain or a custom created one, **Status** as Enabled, **Password Type** can be **DEFAULT Global Password** or a **CUSTOM** created and the SXP **Version** it needs to be running which is **V2** for the WLC.



SXP Domain provides a means to logically group network devices to which SXP mappings should be exchanged. These "Domains" are arbitrarily defined and purely optional; if none are defined the system default VPN named "default" is used. This allows for granular control of where specific SXP mappings will be advertised

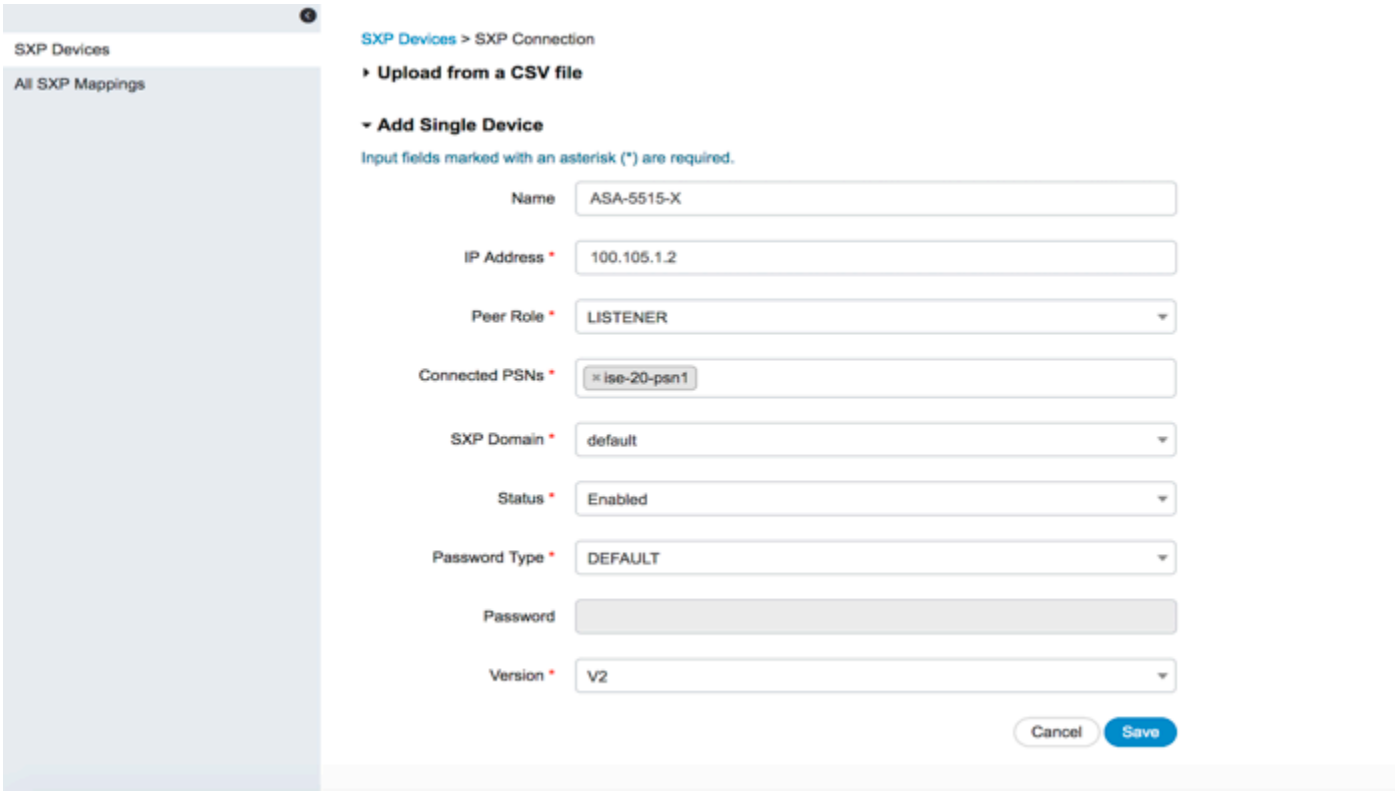
Note: ISE 2.1 can support up to 100 SXP peers with a HA pair and 200 Peers without the HA pair

Step 7 Click **Save**

Step 8 Now hop on the WLC and add ISE as the new SXP peer under **Security > TrustSec SXP** and click **Apply**

Step 9 The SXP **Connection Status** for ISE on the WLC moves to **On**

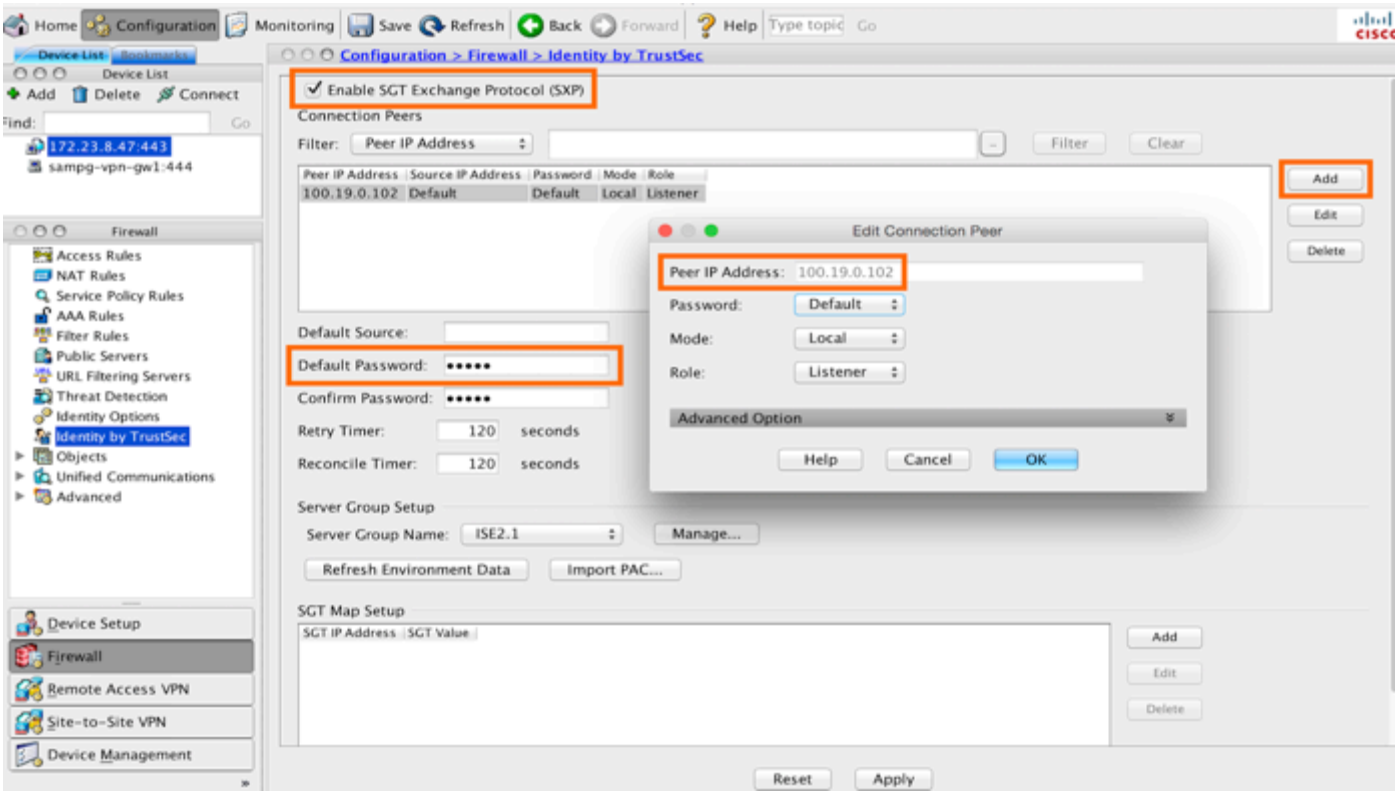
Step 10 Now enable the SXP peering between ISE and ASA with ISE as SXP Speaker and ASA as a SXP Listener to share all the IP-SGT mappings that ISE received from WLC to ASA.



Step 11 Login to the **ASDM** of the ASA and navigate to **Configuration > Firewall > Identity by TrustSec** to configure TrustSec

Note: ASA supports SXPv3 with version 9.6.1 and above. This ASA version is running 9.5.1 so it only support SXPv2

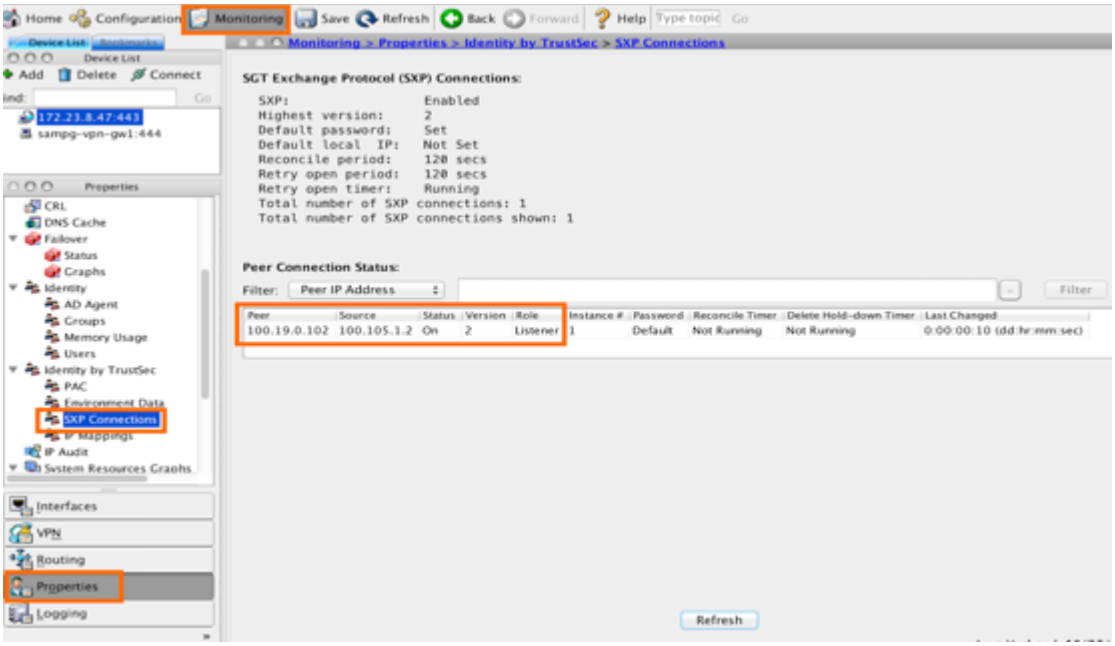
Step 12 Enable the **SXP Service** with the check mark **Enable SGT Exchange Protocol (SXP)**



Step 13 Click **Add** to add a new SXP peer. Add the **Peer IP Address**, **Password** – configured **Default Password**, **Mode** Local and **Role** Listener (Since ASA is the Listener)

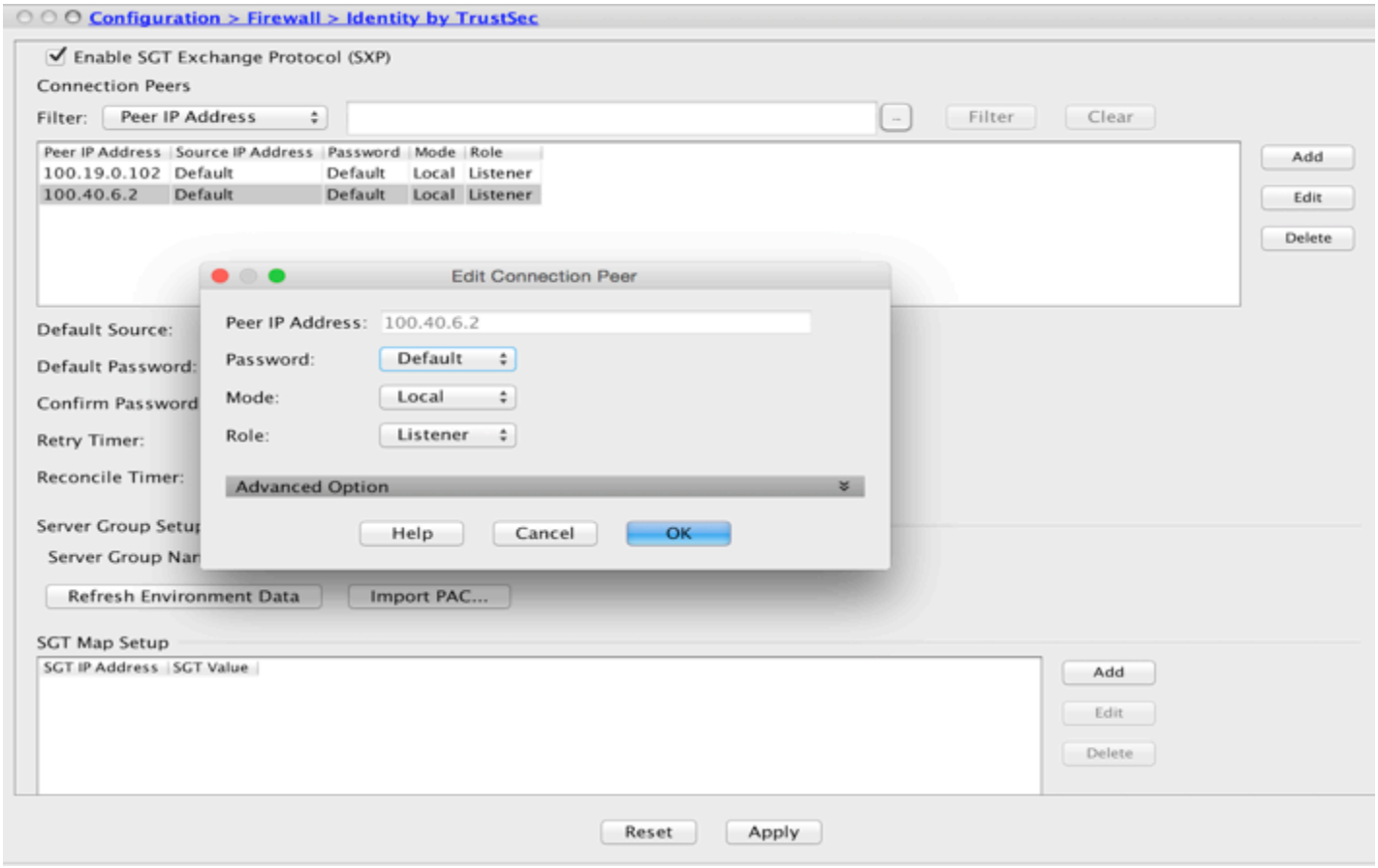
Step 14 Click **Ok** and **Apply**

Step 15 To validate the SXP Connection status on the ASA navigate to **Monitoring > Properties > Identity by TrustSec > SXP Connections**



Step 16 Instead of ISE sending the IP-SGT mappings to ASA we can even have peering enabled between ASA and WLC.

Note: Since ISE receives the IP-SGT mapping from all the network devices it is best practice to have SXP enabled between ISE and ASA



Step 17 Now hop on the WLC and add ASA as the new SXP peer under **Security > TrustSec SXP** and click **Apply**

Step 18 The SXP **Connection Status** for ASA on the WLC moves to **On**

Step 19 To validate the SXP Connection status of WLC on the ASA navigate to **Monitoring > Properties > Identity by TrustSec > SXP Connections**

SGT Exchange Protocol (SXP) Connections:

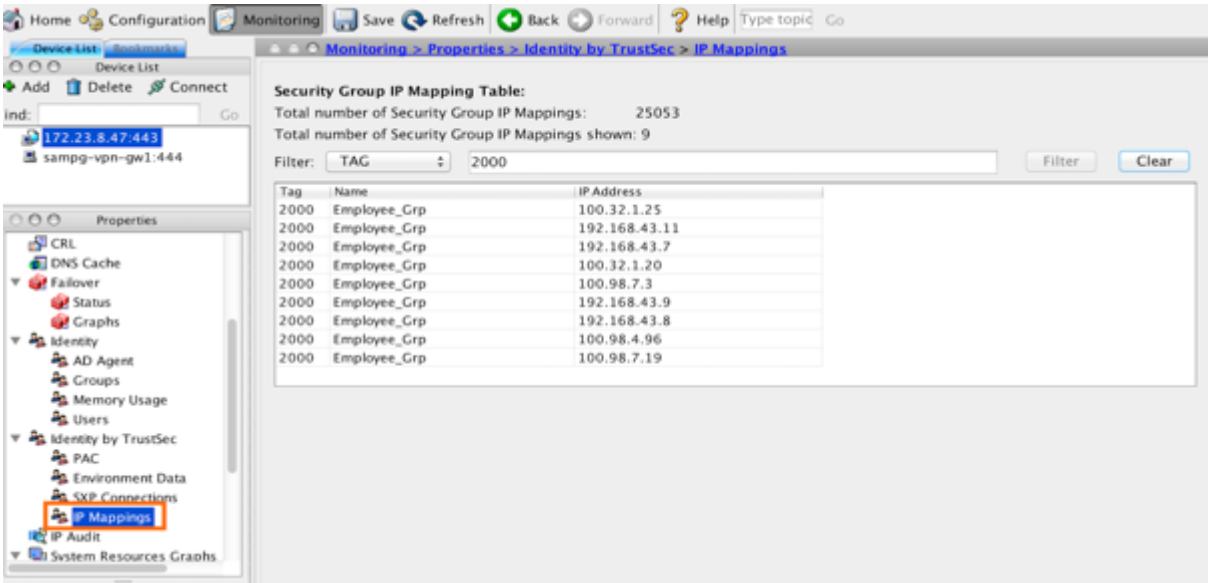
```
SXP:                    Enabled
Highest version:        2
Default password:       Set
Default local  IP:      Not Set
Reconcile period:       120 secs
Retry open period:      120 secs
Retry open timer:       Running
Total number of SXP connections: 2
Total number of SXP connections shown: 2
```

Peer Connection Status:

Filter: Peer IP Address — Filter

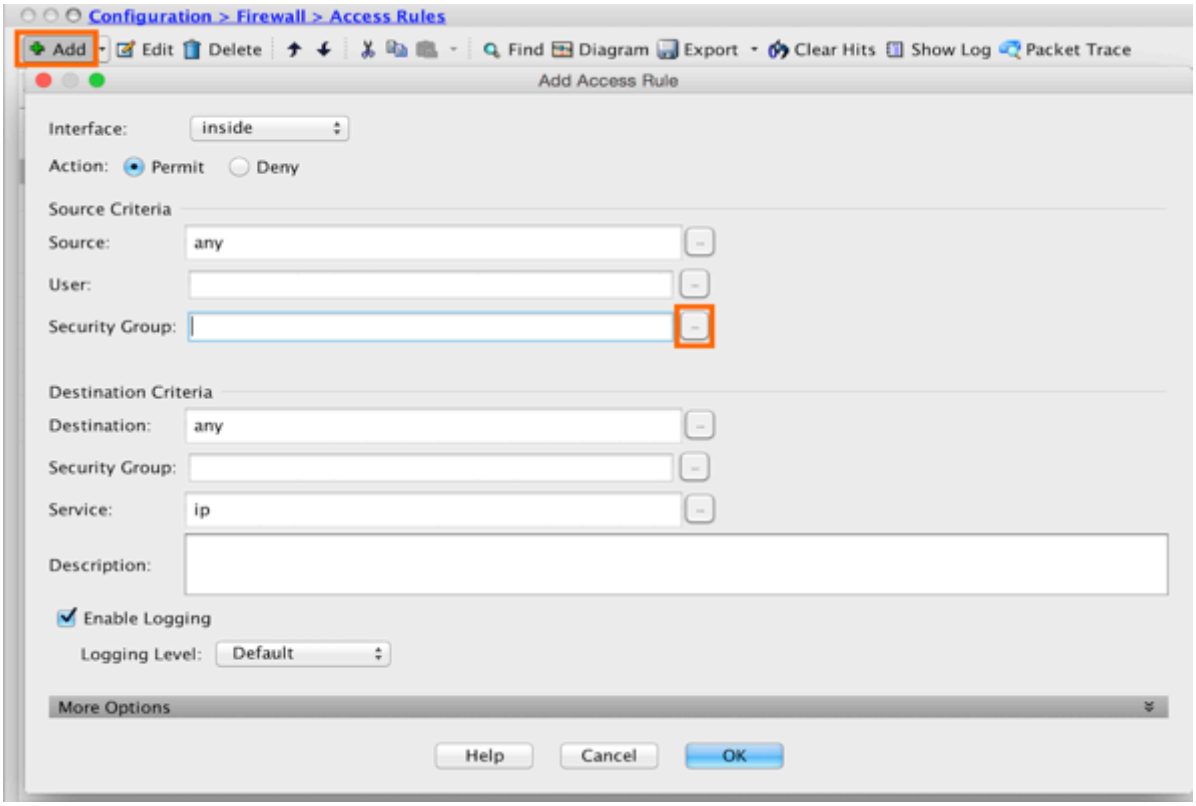
Peer	Source	Status	Version	Role	Instance #	Password	Reconcile Timer	Delete Hold-down Timer	Last Changed
100.19.0.102	100.105.1.2	On	2	Listener	1	Default	Not Running	Not Running	0:00:17:48 (dd:hr:mm:sec)
100.40.6.2	100.105.1.2	On	2	Listener	1	Default	Not Running	Not Running	0:00:00:22 (dd:hr:mm:sec)

Step 20 To validate the SXP Mappings received on the ASA navigate to **Monitoring > Properties > Identity by TrustSec > IP Mappings**



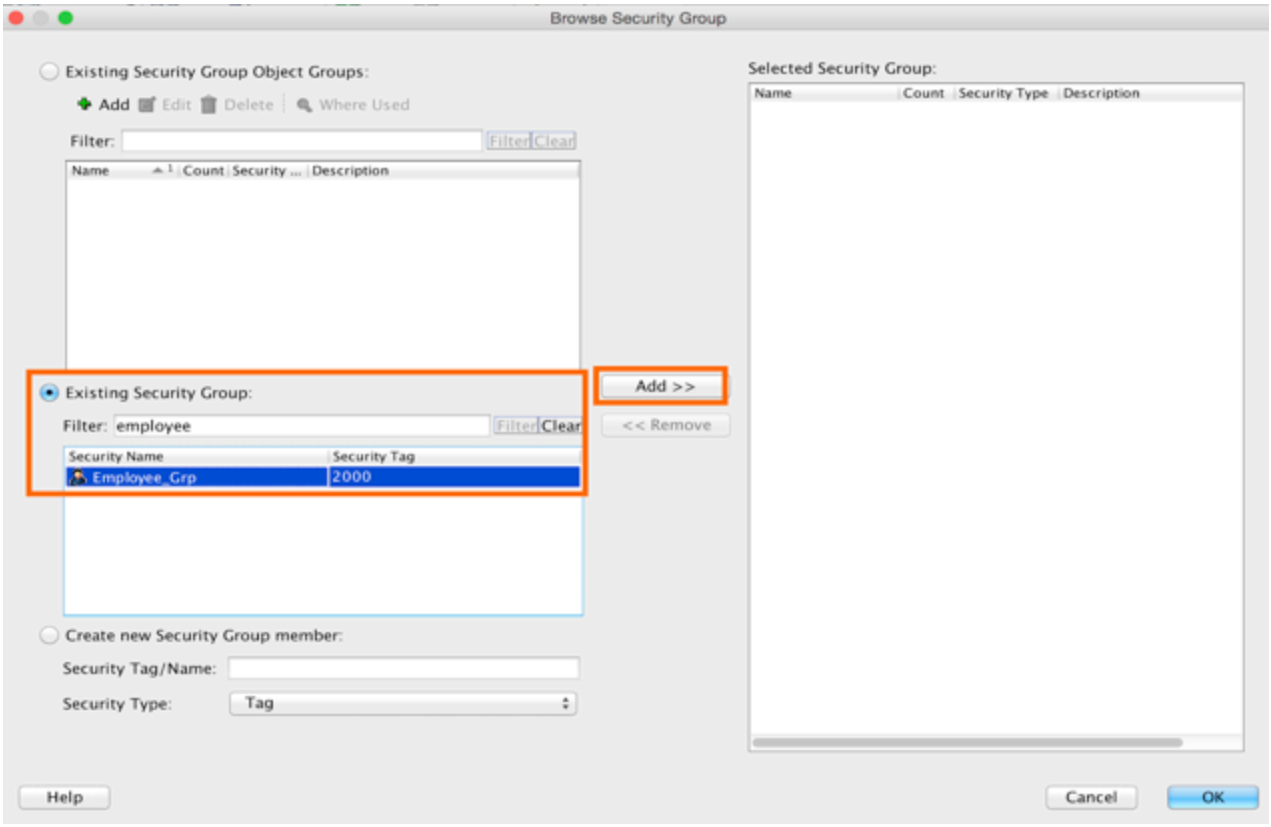
ASA can act as a **Security Group Firewall** (**SGFW**) with the policy enforcement based on security Groups. Instead of ISE pushing the SGACLs for enforcement to the network devices, ASA has the capability to do the enforcement with the firewall rules utilizing Security Groups

Step 21 To add the new **Access Rules** using TrustSec **Security Groups** navigate to **Configuration > Firewall > Access Rules** and click **Add** to add a new rule



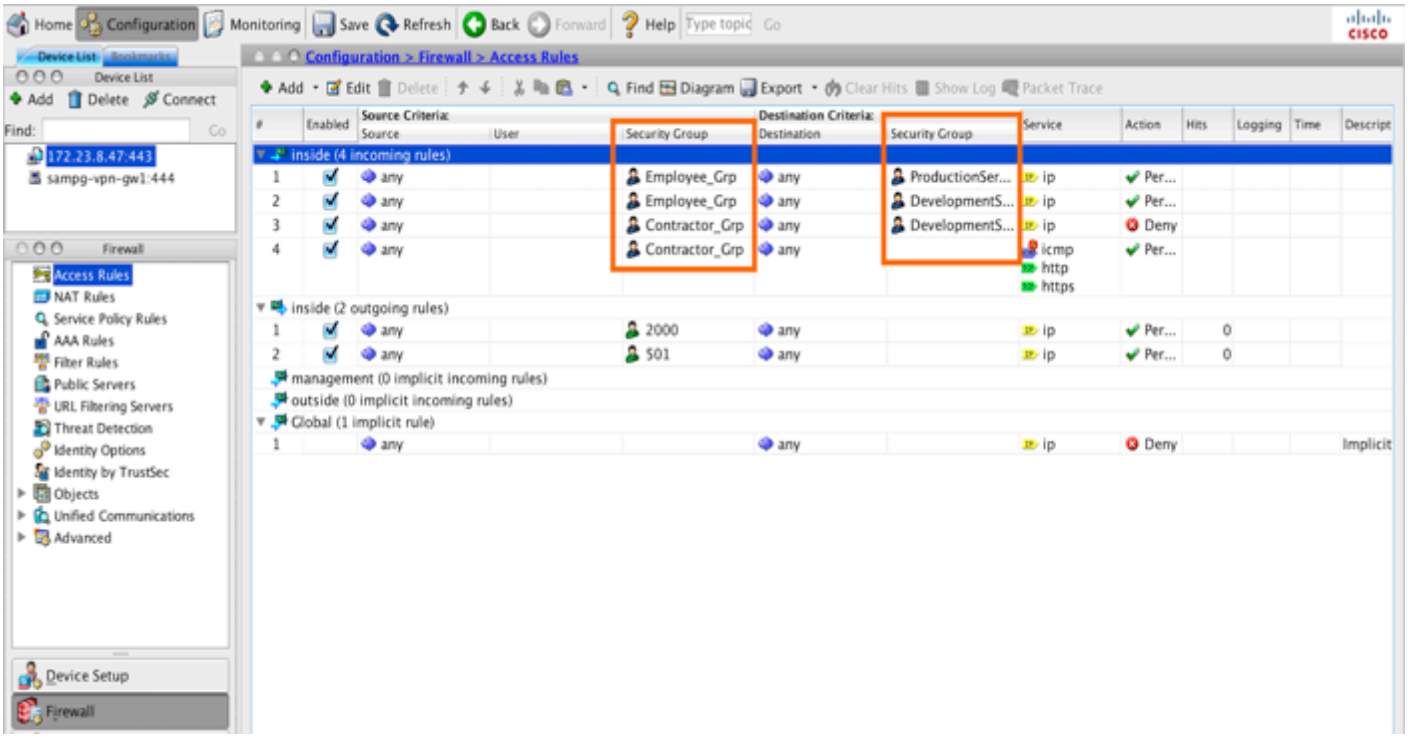
Step 22 Under the **Source Criteria** look for **Security Group** and click on the Icon on the right most side of the Security Group to **Browse Security Groups**

Step 23 Select the **Existing Security Group** or can even **Filter** and once selected click **Add** to populate the Security Group on the right and once finished adding all the groups for the source criteria click **OK**



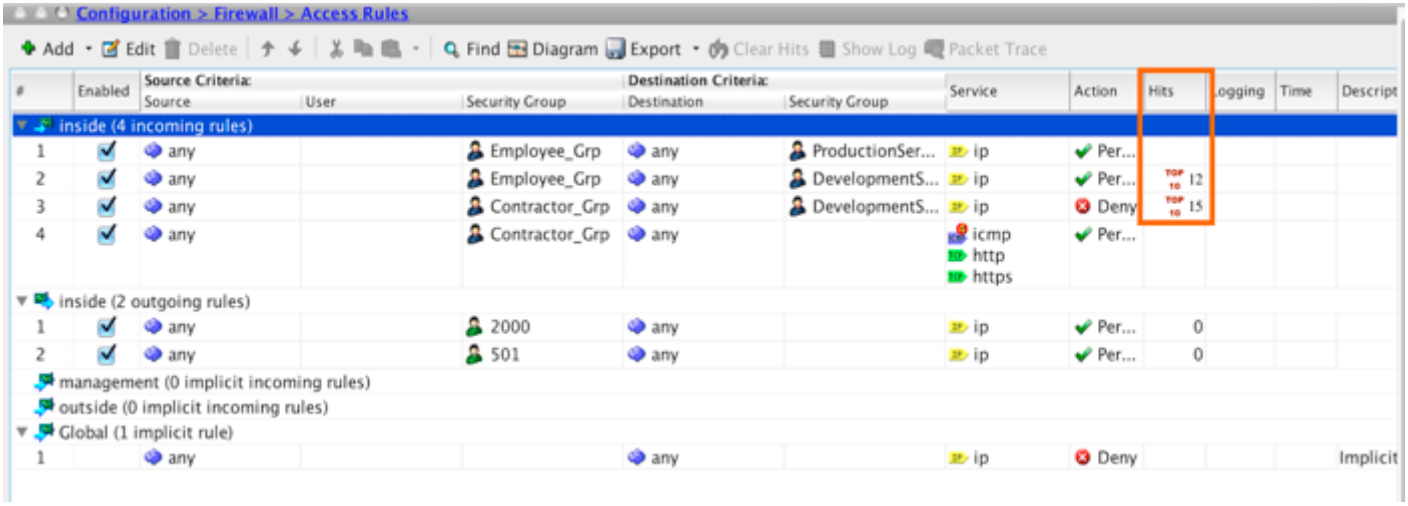
Step 24 Repeat the same steps for the **Destination Criteria Security Group**

Step 25 Once added the **SGFW Access Rules** should look something similar to the one in below



The above access rules shown in the screenshot have the policies based on Security Groups like **Employee**, **Contractor** on the source with the **Production Server** and **Development Server** on the destination. **Permit** and **Deny** actions now can be taken using SGFW rules.

Step 26 To validate the enforcement on the **Security Group Firewall** (**SGFW**) look to see if the number of **Hits** being incremented on the **Access Rules** page



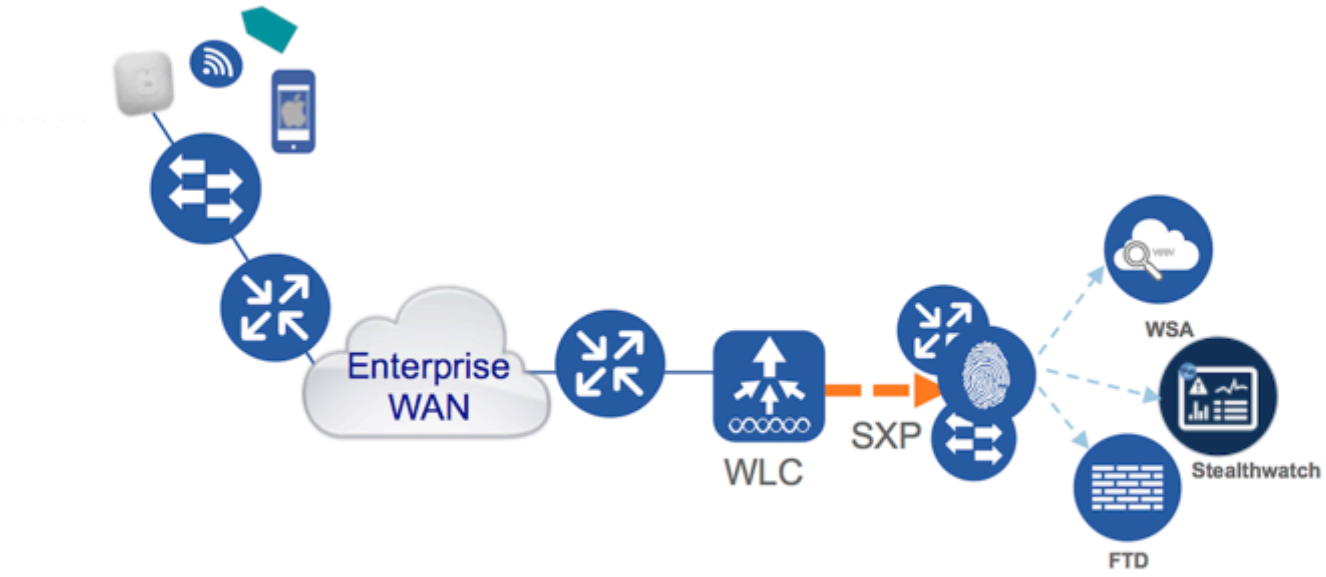
As soon as an **Employee** tries to access the **Development Server**, as per the **Permit** action configured on the access rule of the SGFW policy he would be granted network access and the number of **Hits** would be incremented. Similarly when a **Contractor** tries to access the **Development Server**, as per the **Deny** action configured on the access rule he would be denied network access and the number of **Hits** would be incremented.

Sharing Security Groups of FlexConnect Users to other Security Products

The Security Groups of the wireless users coming from both Central and FlexConnect deployments can be shared to other security products like FirePower Threat Defense (FTD), StealthWatch and WSA through Cisco Platform Exchange Grid (PxGrid). Cisco PxGrid feature enables sharing of context and security groups information from ISE. This configuration guide will not go into the details of the PxGrid capabilities but shows how the Security Group information from ISE could be used by different security products like WSA to apply the access policies based on Security Groups, simplifying security rules using security group tags with FTD, StealthWatch to monitor the traffic flows and quarantine the endpoints based on SGTs.

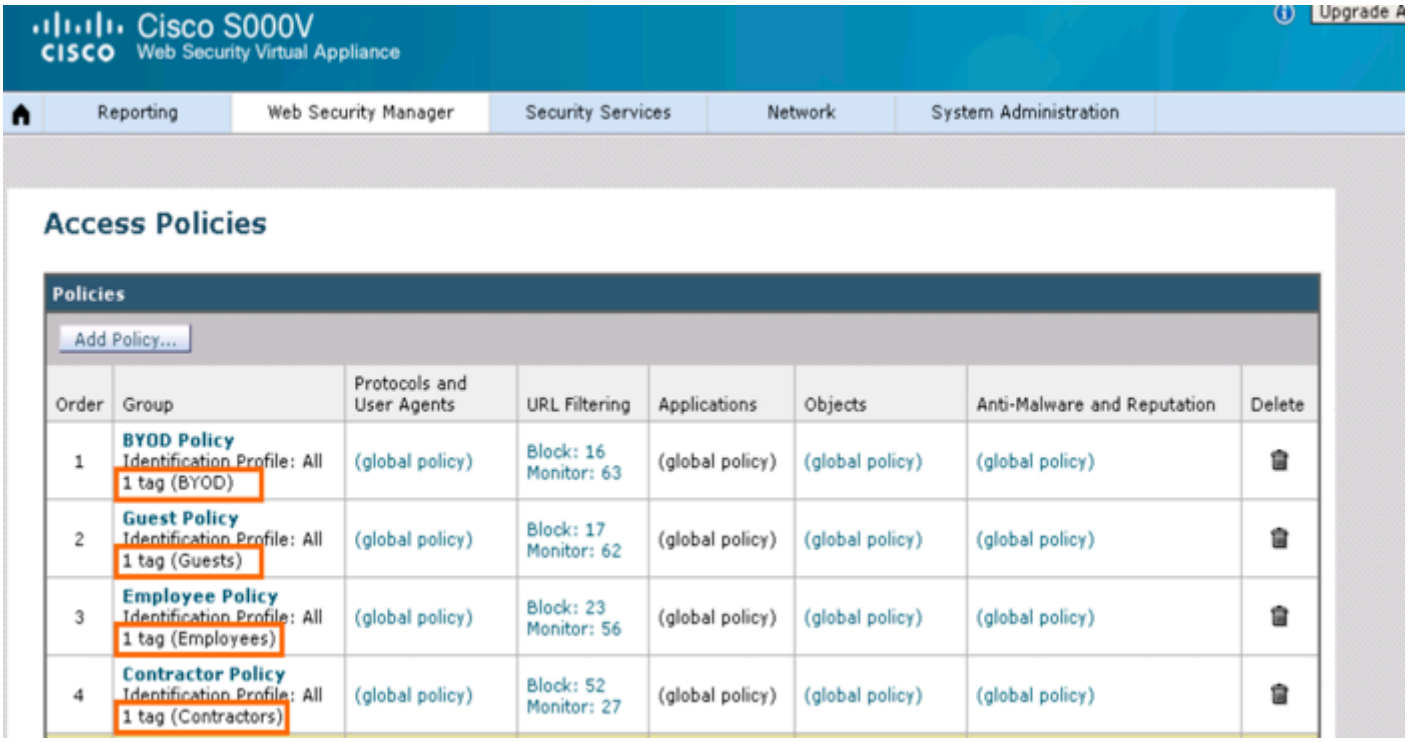
Note: PxGrid node needs to be deployed as a separate persona in ISE

Figure 3: Topology showing FlexConnect users Security Groups being shared with different security products



WSA Access Policies based on Security Groups

WSA could block the access of the wireless users (both Central/FlexConnect) to certain sites through URL Filtering based on Security Groups. Here is a sample screenshot showing the WSA access policies being created based on the TrustSec Security Groups. We could simplify the access polices on the WSA with the security groups. The security groups below are received by WSA through ISE PxGrid.



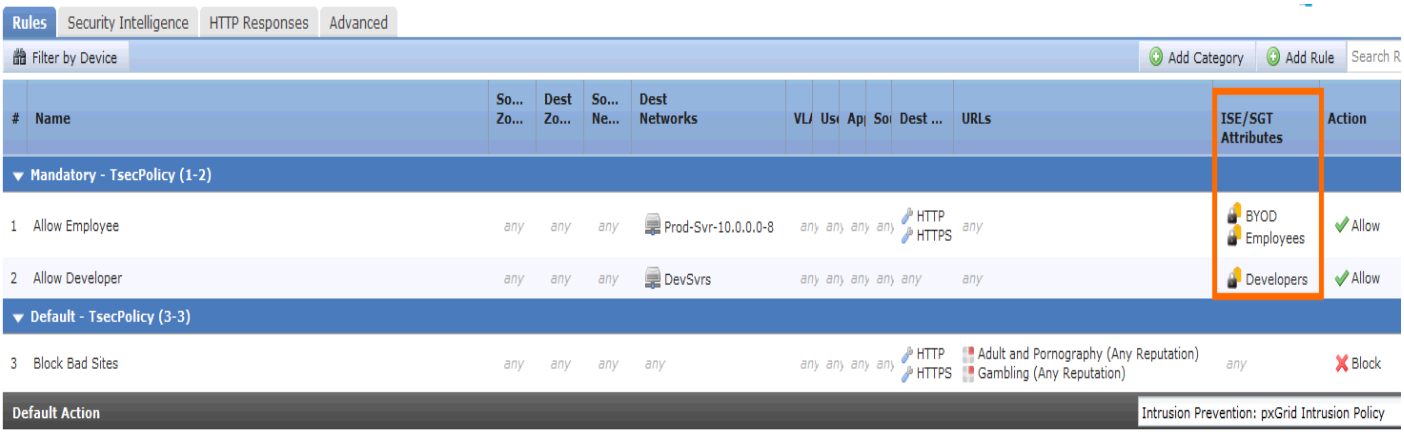
For more information on the integration between ISE and WSA click the below link.

https://communities.cisco.com/servlet/JiveServlet/previewBody/68290-102-1-125507/How-To_104_Integrate_Cisco_WSA_using_ISE_and_TrustSec_through_pxGrid.pdf

Simplifying Security Rules on FTD with Security Groups

Here is a sample screenshot showing the security policies on FirePower Threat Defense (FTD) with Security Groups. We could simplify the security rules using trustsec security group tags on the FTD instead of IP based rules.

Note: Security Groups on FTD currently supports Source Criteria only



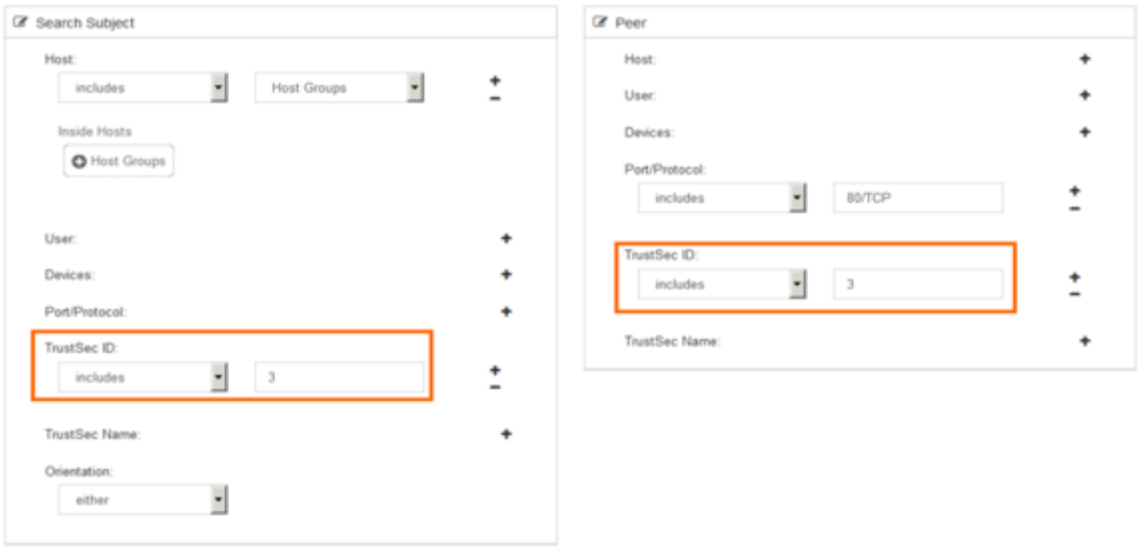
Additionally FTD provides **Rapid Threat Containment** (**RTC**) capability by detecting the threat and sharing that information over Cisco PxGrid to ISE and ISE could quarantine that endpoint using the TrustSec Security Group Tags.

For more information on the integration between ISE and FirePower click the below link.

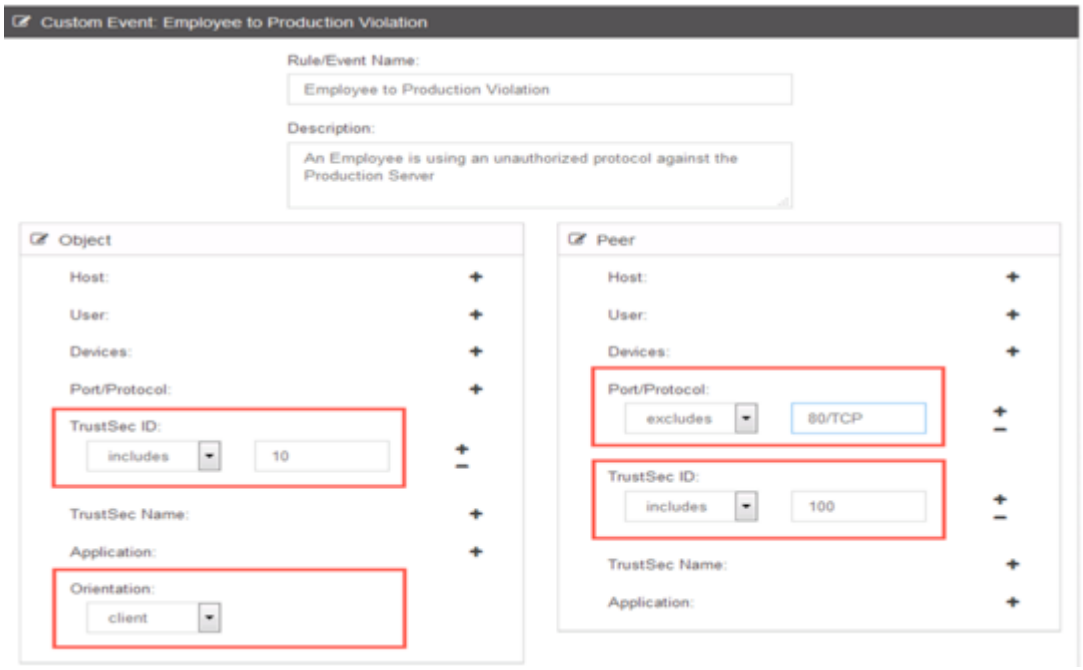
https://communities.cisco.com/servlet/JiveServlet/previewBody/68292-102-1-125510/How-To_Firepower_ISE_pxGrid.pdf

Monitoring TrustSec Security Groups with StealthWatch

StealthWatch solution leveraging NetFlow from the network infrastructure like switches and firewalls provides deeper visibility into the network through the collection, aggregation and analysis of NetFlow data. Since NetFlow records now aware of TrustSec Security Groups, StealthWatch could actively monitor the TrustSec policy segmented traffic. Here is a sample screenshot showing TrustSec ID (Security Group Tag) information in StealthWatch.



Additionally even StealthWatch can provide **Rapid Threat Containment** (**RTC**) and Network as a Sensor and Enforcer (NaaS/E) capability by detecting the threats through policy violation and sharing that information over Cisco PxGrid to ISE and ISE could quarantine that endpoint using the TrustSec Security Group Tags.



For more information on the integration between ISE and StealthWatch click the below link.

https://communities.cisco.com/servlet/JiveServlet/previewBody/68288-102-1-125505/How-To_101_Deploying_Lancope_StealthWatch_with_pxGrid.pdf

Debug SXP 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 SXP on WLC

To Debug SXP connection errors in **WLC**, enable the following debug commands.

```
(Cisco Controller) >debug cts sxp ?

all             Configures debug of all CTS SXP messages.
errors          Configures debug of CTS SXP errors.
events          Configures debug of CTS SXP events.
framework       Configures debug of CTS SXP framework.
message         Configures debug of CTS SXP message.
```

Debug SXP on Switch

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

```
6506E-VSS#debug cts sxp ?
  conn      CTS SXP connection
  error     CTS SXP errors
  internal  CTS SXP internal information
  mdb       CTS SXP mapping db
  message   CTS SXP message
```

Additionally the following two commands are handy in troubleshooting SXP on the switches

```
6506E-VSS#debug ip tcp transactions

6506E-VSS#debug ip tcp packet
```