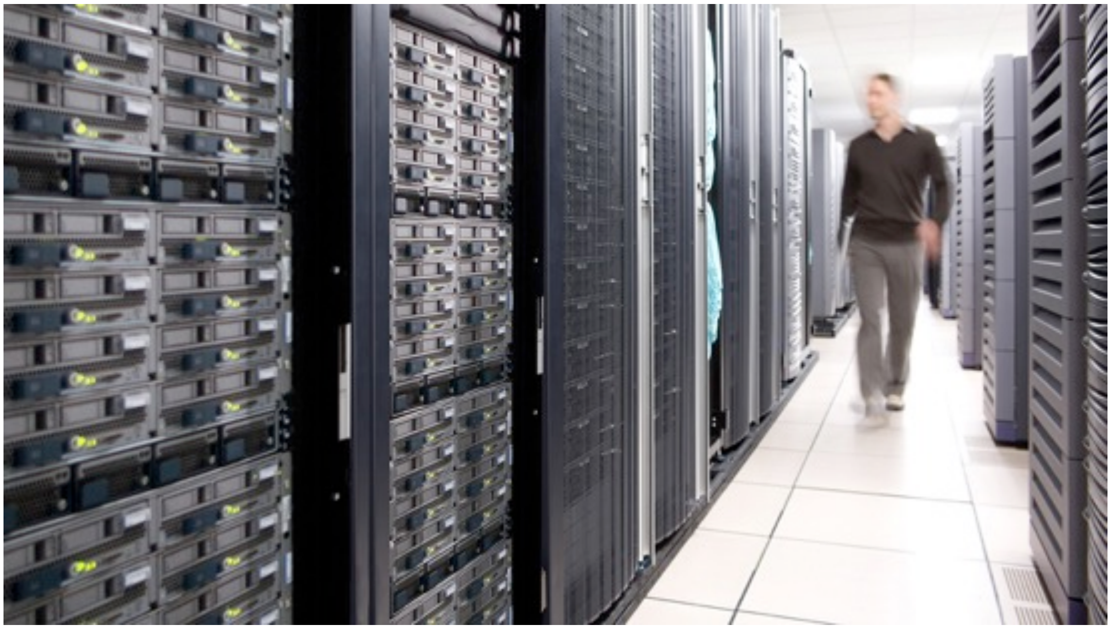


TrustSec Configuration Guides

TrustSec – ACI Policy Plane Integration

Enabling Group-based Policies Across Enterprise Networks with Software-Defined Segmentation

TrustSec
Software-Defined
Segmentation

Table of Contents

TrustSec – ACI Policy Plane Integration

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.

Cisco Application Centric Infrastructure (ACI) is a comprehensive SDN architecture. ACI provides a network that is deployed, monitored, and managed in a way that benefits different teams in the IT organization including SDN Network, Cloud and DevOps, and Security. It supports rapid application change by reducing complexity with a common policy framework that can automate provisioning and resource management. These benefits are achieved through the integration of physical and virtual environments under one policy model for networks, servers, storage, services, and security.

The TrustSec-ACI Policy Plane Integration

a) Helps in addressing the breaches, segmentation & compliance challenges by sharing policy groups between TrustSec-enabled networks and ACI data centers.

b) Enables consistent security policy management across the enterprises by leveraging user roles and device type together with application context anywhere in the network. The complementary group-based policy approach used by TrustSec and ACI vastly simplifies security design, operations and compliance.

The functionality is provided as part of ISE release 2.1 release.

Application Centric Infrastructure (ACI) Overview

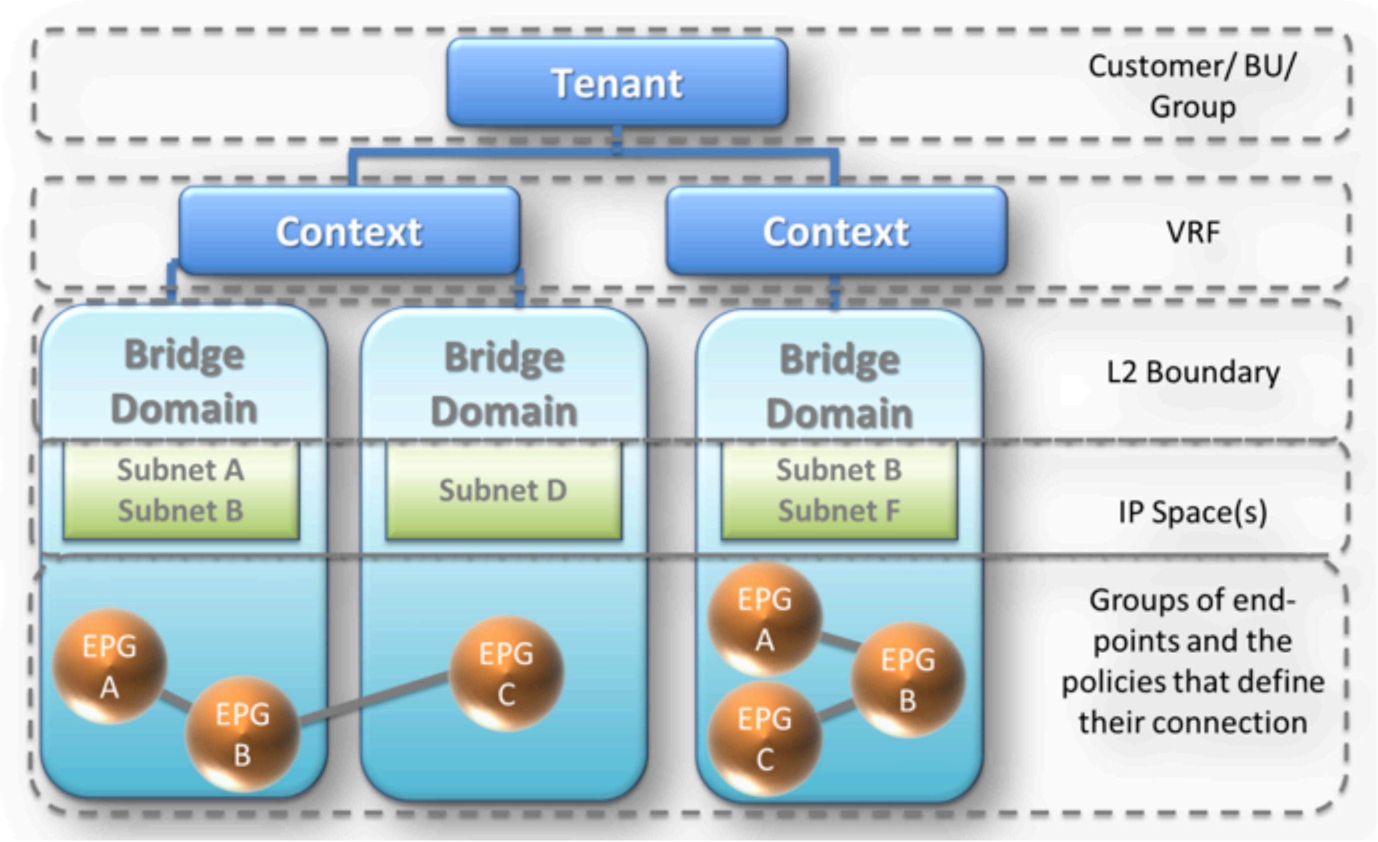
The Cisco Nexus 9000 platform has two modes of operation. In the first mode Nexus 9000 utilizes an enhanced version of the NXOS operating system to provide a traditional switching model with advanced automation and programmability capabilities, which is known as “Standalone”.
In the second mode, ACI Mode the Nexus 9000 provides an Application Centric representation of the Data Center network (DC) as a whole utilizing advanced features and profile based deployment to abstract the complexity of the underlying network while improving application visibility and greater business agility through DevOps methodologies.

ACI is a Data Center network architecture from Cisco, which uses a policy based approach to abstract traditional network constructs (e.g. VLANs, VRFs, IP subnets, etc.). Cisco Nexus 9000 (running in ACI mode) + APIC-DC Controller (APIC) comprise the ACI elements which use the policy based approach by focusing on the application. The Nexus 9000 platform forms the physical switching infrastructure, while the APIC-DC is a clustered policy management system responsible for all aspects of fabric configuration.

The applications in ACI are grouped as Endpoints (EP) and Endpoint Groups (EPGs). The communication between the Endpoint Groups (EPGs) is determined based on the policies using Contract Filters (contract) by allowing specific ports and protocols between EPGs. The collection of Internal Endpoint Groups (IEPGs) and External Endpoint Groups (EEPGs) and the policies that define how they communicate form an Application Profile (AP). A Tenant is a container for all Network, Security, Troubleshooting and L4-L7 Service Policies. Tenant resources are isolated from each other, allowing management by different administrators. VRFs (also called contexts) are defined within a tenant to allow isolated and potentially overlapping IP address space. Within a private network (VRF), one or more Bridge Domains (BD) must be defined. A Bridge Domain is a L2 forwarding construct within the fabric, used to constrain broadcast and multicast traffic. This is the basic introduction to ACI and its major components.

Note: ISE 2.1 only supports single tenant to add and read the IP/EPG information from APIC-DC and share that to the network devices as an SGT

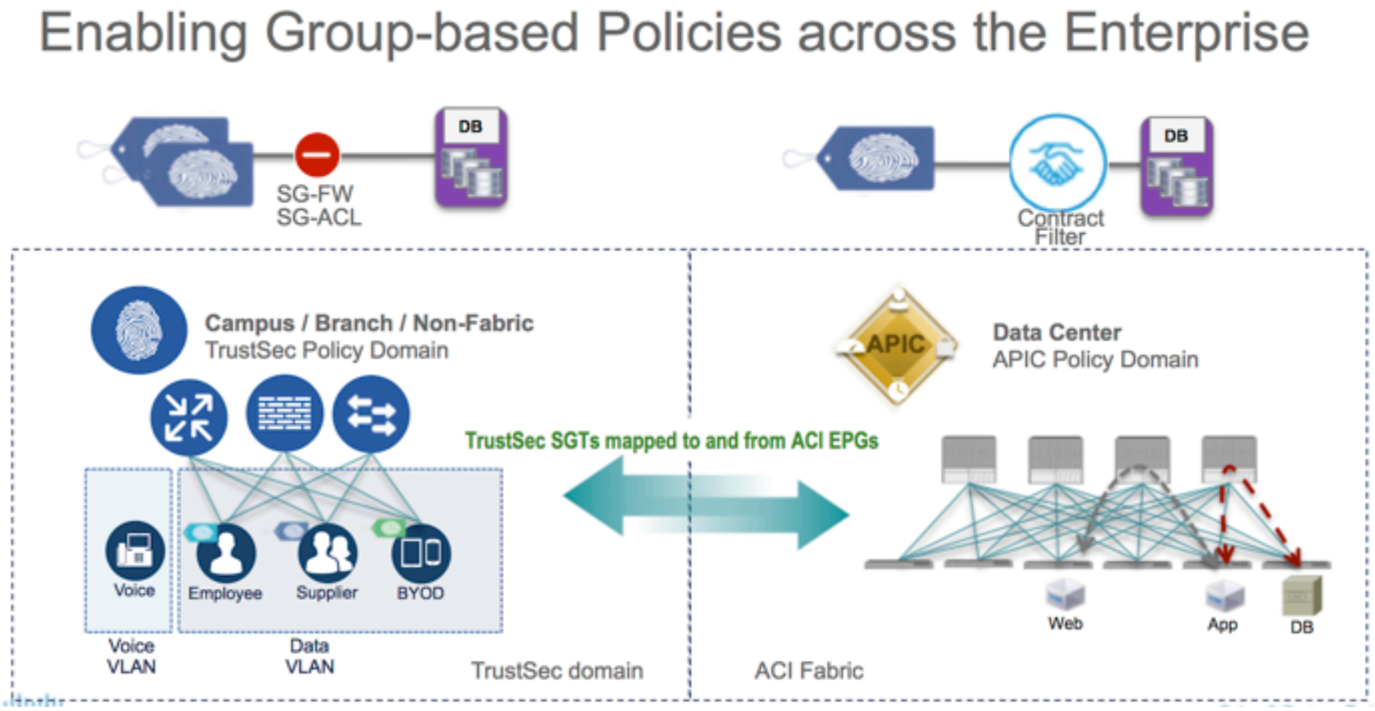
Figure 1: Tenant Tree View and its components:



TrustSec - ACI Policy Plane Integration Overview

Through this integration the Security Group Tags (SGTs) in a TrustSec-enabled network can be converted to Endpoint Groups (EPGs) in the ACI Data Center network, and the EPGs from ACI can be converted to SGTs in the Enterprise Network. Thus, Cisco Identity Service Engine (ISE) enables the sharing of consistent security policy groups between TrustSec and ACI domains. To enable groups from the ACI domain to be used in the TrustSec domain, ISE will synchronize Internal EPGs from the APIC-DC controller and create corresponding Security Groups in the TrustSec environment. ISE will also synchronize Security Groups and associated IP-Security Group mappings with the APIC-DC External End Points (EEPGs) and subnets configuration.

Figure 2: Topology showing the group-based policies shared between TrustSec and ACI domains



Overview of TrustSec-ACI Configuration

TrustSec - ACI Policy Plane Integration utilizes functions on both ISE Policy Administration Nodes (PAN) and ISE Policy Services Nodes (PSN) and the APIC-DC controller must be reachable from both nodes.
ISE Policy Administration Nodes (PAN) communicates with the APIC-DC Controller to synchronize Security Groups and EndPoint Groups.
Group membership functions, i.e. the IP–Group mappings, are managed by an ISE PSN running an SGT eXchange Protocol (SXP) service, which will also need to communicate with the APIC-DC Controller.
Currently one Policy Services Node (PSN) must be dedicated to running the SGT eXchange Protocol (SXP) service.

For TrustSec-ACI policy element exchange to function both the SXP and TrustSec-ACI functions in ISE need to be enabled
The APIC-DC configuration parameters and credentials entered in ISE will be used by both the PAN and PSN and the TrustSec-ACI policy element exchange functions started or stopped according to the ACI Settings configuration in ISE.

Once enabled, ISE will makes a call to the ACI API to create a subscription in order to receive configuration change notifications for APIC-DC management objects. The API subscription feature uses the WebSocket protocol (RFC 6455) to implement a two-way connection with the API client (ISE) through which the API can send unsolicited notification messages to ISE. As part of the WebSocket connection establishment, ISE validates the server (APIC-DC) certificate against its ISE Certificate store. In the case of validation failure, ISE fails the connection and notifies the ISE admin through an alarm and audit log. With ISE 2.1 release, ISE will connect up to three APIC controllers as part of the same ACI fabric supporting a single tenant.

Configuration

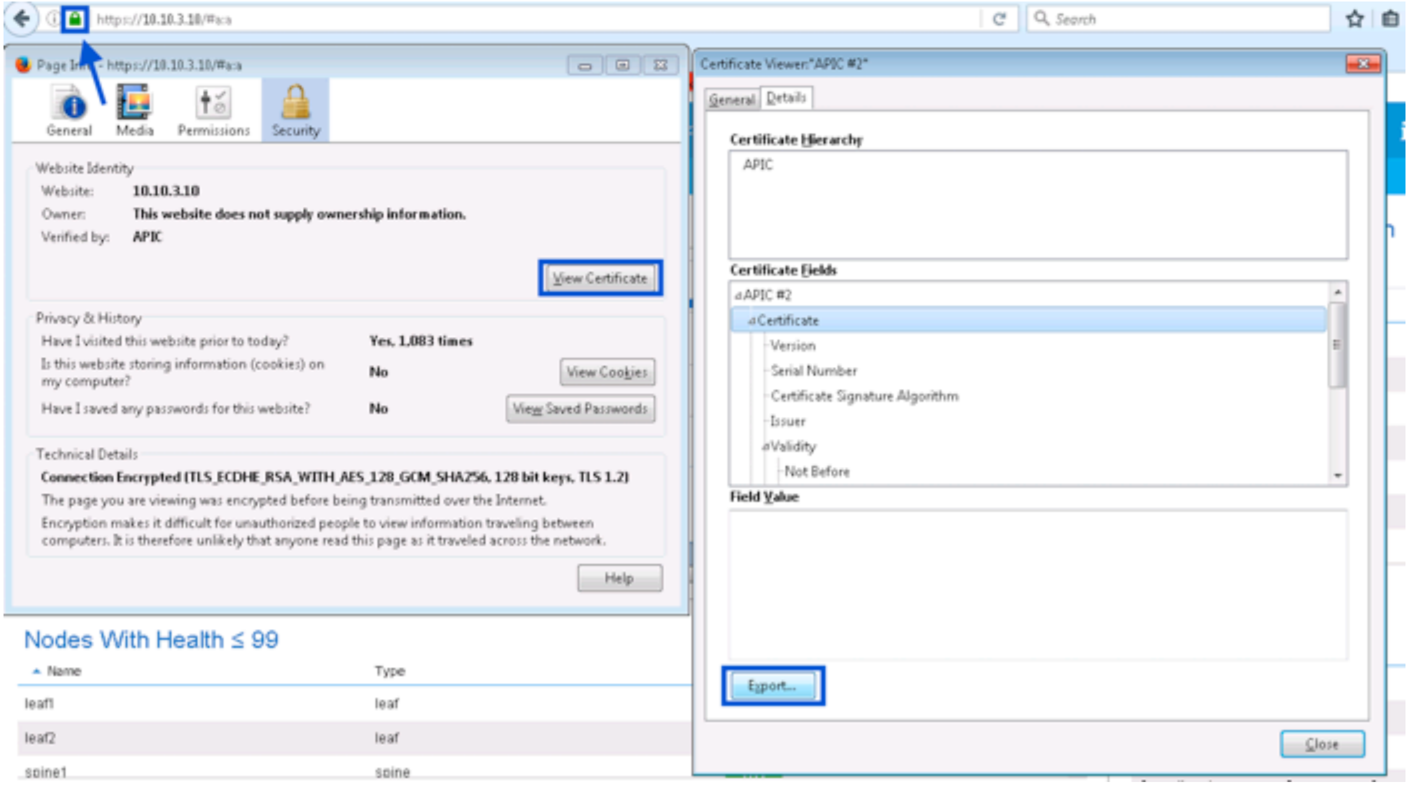
Import APIC-DC Certificate into ISE

In order to establish communications between the ACI domain and TrustSec domain, the APIC-DC Controller Certificate needs to be imported into the ISE certificate store.

Step 1 From the Browser window of the APIC-DC controller click the **Padlock** icon to view the **Website Identity**

Step 2 Click **View Certificate** to see the details of the certificate

Step 3 Click **Export** to save the certificate to your local computer



Website Identity

Website: 10.10.3.10

Owner: This website does not supply ownership information.

Verified by: APIC

Privacy & History

Have I visited this website prior to today? Yes, 1,083 times

Is this website storing information (cookies) on my computer? No

Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

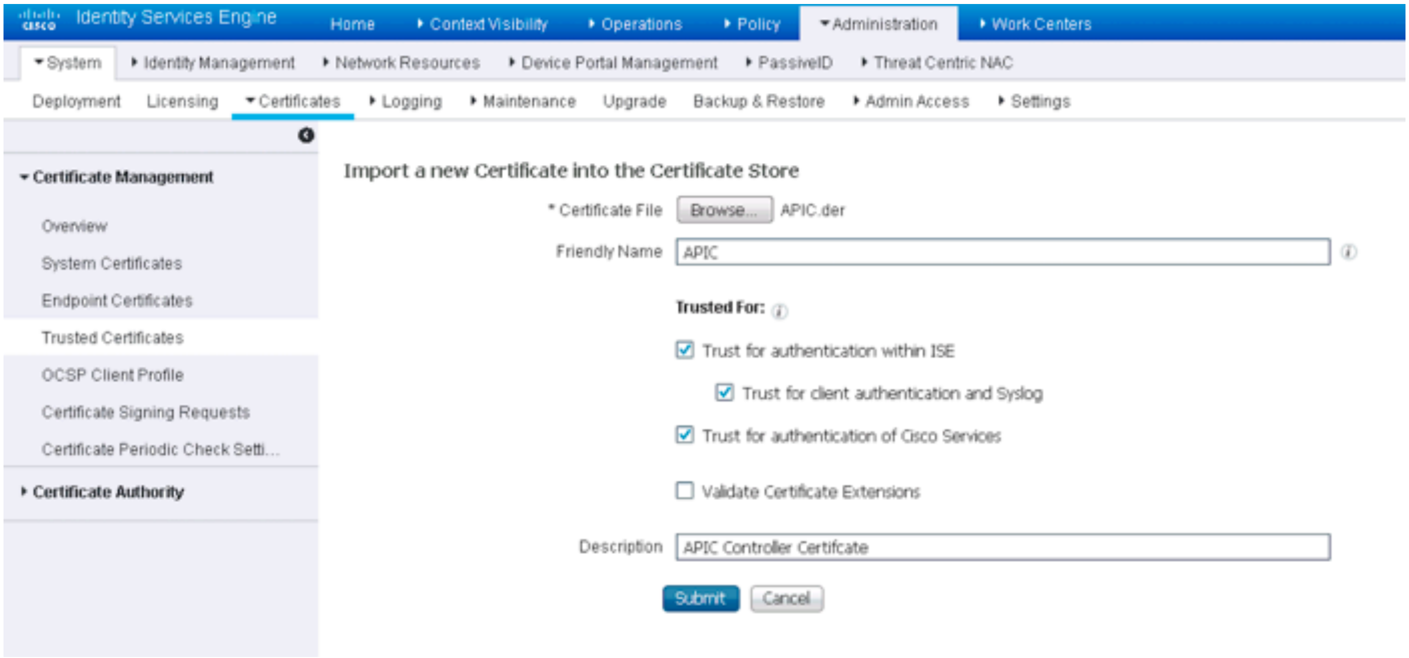
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Nodes With Health ≤ 99

Name	Type
leaf1	leaf
leaf2	leaf
spine1	spine

Step 4 Navigate to Trusted Certificates section in the ISE UI: **Administration > System > Certificates > Trusted Certificates**

Step 5 Click **Import** to import the APIC-DC certificate to the ISE Certificate Store.



Import a new Certificate into the Certificate Store

* Certificate File Browse... APIC.der

Friendly Name APIC

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☑ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

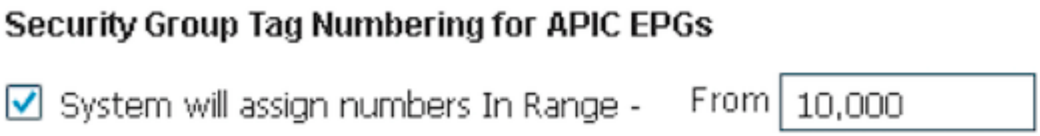
Description APIC Controller Certifcate

Security Group Tag Numbering for APIC-DC EPGs

The EPGs that are received by ISE are assigned SGT values. By default the EPGs received by ISE will be assigned a SGT start value of 10,000, and the box is unchecked. To modify the starting value to something other than the default value of 10,000:

Step 1 Navigate to General TrustSec Settings: **Work Centers > TrustSec > Settings > General TrustSec Settings**

Step 2 Go to **Security Group Tag Numbering for APIC EPGs** and Check the box and modify the SGT value to the desired starting SGT value



Security Group Tag Numbering for APIC EPGs

☑ System will assign numbers In Range - From 10,000

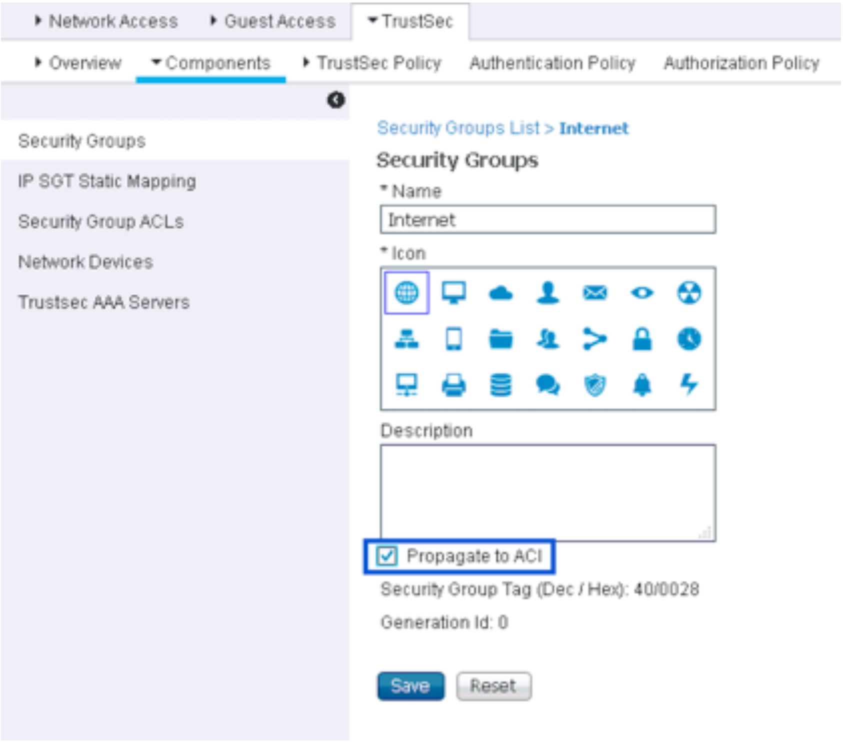
Propagate Security Groups to ACI

By default, Security Groups that are part of ISE 2.1 bootstrap configuration will automatically propagate to APIC. In order to propagate newly created SGTs to the ACI fabric:

Step 1 Navigate to the TrustSec Security Groups: **Work Centers > TrustSec > Components > Security Groups**

Step 2 Edit the newly created Security Group and check the **Propagate to ACI** box, and save the setting

Note: Default Security Groups part of ISE 2.1 bootstrap configuration will have the check mark in the box. Only the newly created SGTs need to be checked to propagate to ACI



Security Groups List > **Internet**

Security Groups

* Name: Internet

☑ Propagate to ACI

Security Group Tag (Dec / Hex): 40/0028

Generation Id: 0

ACI Settings in ISE

To enable the TrustSec - ACI Policy Plane integration, the APIC controller must be configured in ISE:

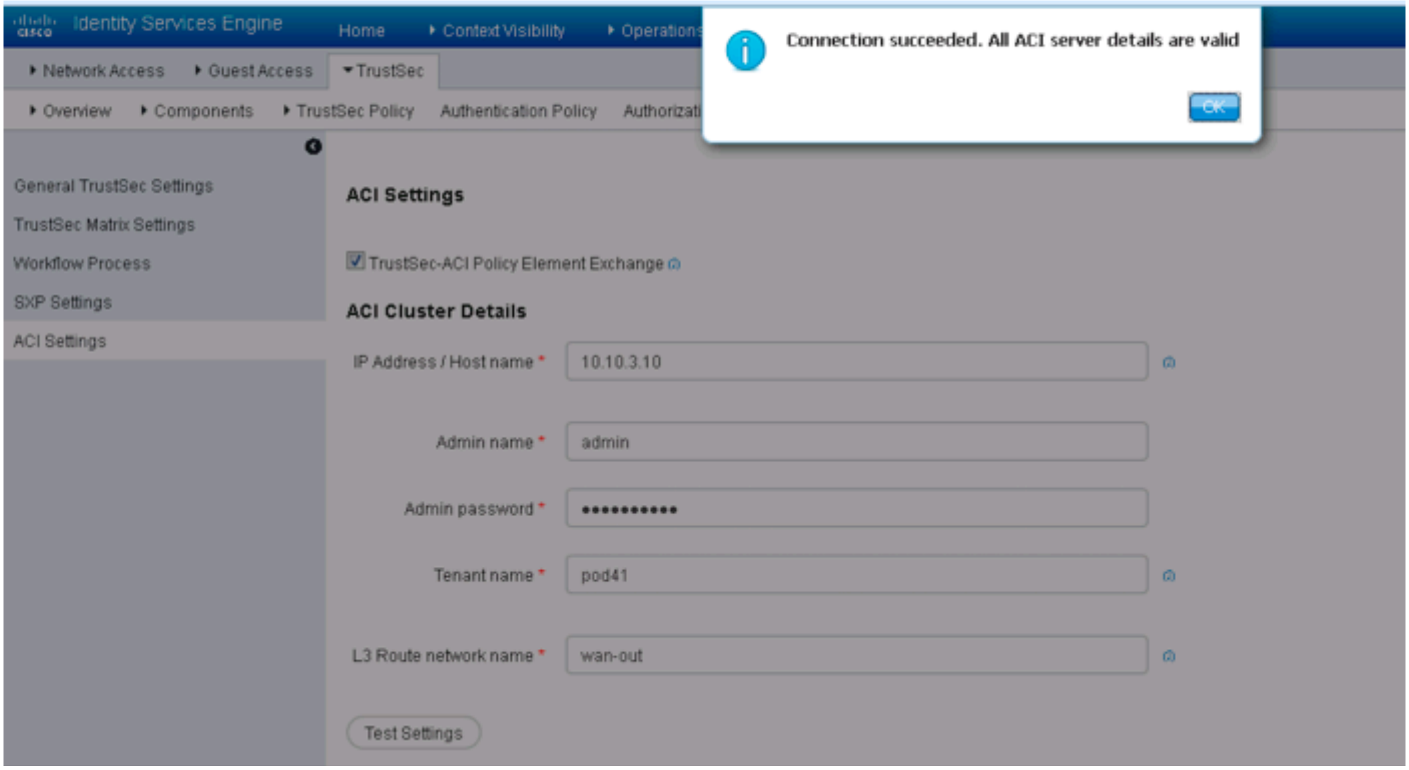
Step 1 Navigate to ACI Settings Screen: **Work Centers > TrustSec > Settings > ACI Settings**

Step 2 Enable the exchange by checking **TrustSec-ACI Policy Element Exchange**

Step 3 Configure the following objects under the ACI cluster Details: **APIC-DC IP/Hostname**, **Admin** Credentials and **Tenant** name and **L3 Out** network name.

Step 4 Validate the connection by clicking **Test Settings**

Note: ACI can connects to an outside networks using layer 3 technology. Layer 3 outside connections (L3 Out), or external routed networks, provide IP connectivity between a private network of a tenant and an external IP network. Each layer 3 outside connection is associated with one private network. L3 Out explores the forwarding behaviour between internal and external endpoints, and how the policy is enforced for the traffic flow between them.



Connection succeeded. All ACI server details are valid

ACI Settings

☑ TrustSec-ACI Policy Element Exchange

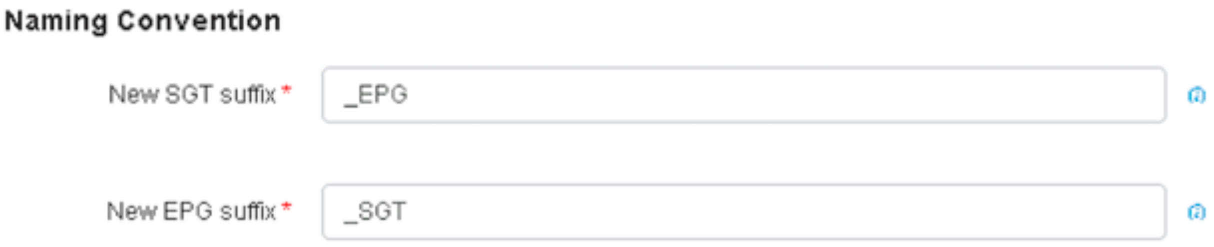
ACI Cluster Details

IP Address / Host name * 10.10.3.10
Admin name * admin
Admin password * ●●●●●●●●●●●
Tenant name * pod41
L3 Route network name * wan-out

Note: ISE 2.1 allows a single cluster of 3 APIC-DC controllers. But it only supports single Tenant and a L3 Out network.

Step 5 Configure the Naming Convention for the exchanged group tags by navigating to **Naming Convention**

Step 6 Define the suffixes for both new SGTs and EPGs: **New SGT suffix, New EPG suffix**. The configured suffix will be appended to the converted SGTs and EPGs in the APIC-DC controller and ISE.



Naming Convention

New SGT suffix * _EPG
New EPG suffix * _SGT

SXP Propagation

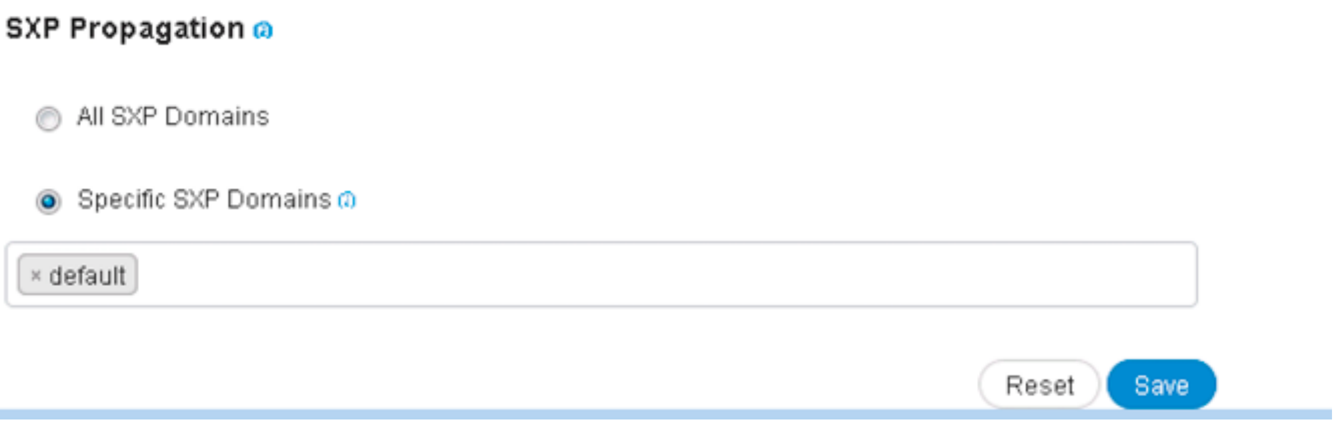
Before configuring the SXP Propagation settings there is a concept of SXP Domains that needs to be understood. An SXP Domain provides a means to logically group network devices to which SXP mappings should be exchanged. These “Domains” are arbitrarily defined and purely optional; if none are defined the system default VPN named “default” is used. This allows for granular control of where specific SXP mappings will be advertised.

For TrustSec - ACI Policy Plane Integration, all the domains or specific ones can be exchanged

Step 1 Navigate to ACI Settings Screen: **Work Centers > TrustSec > Settings > ACI Settings**

Step 2 Look for **SXP Propagation** under the ACI Settings and define

Step 3 Specify the SXP domains that can share the mappings with the ACI fabric by clicking **All SXP Domains** or **Specific SXP Domains** and their values



SXP Propagation

○ All SXP Domains

● Specific SXP Domains

× default

Step 4 **Save** the configured ACI settings in ISE

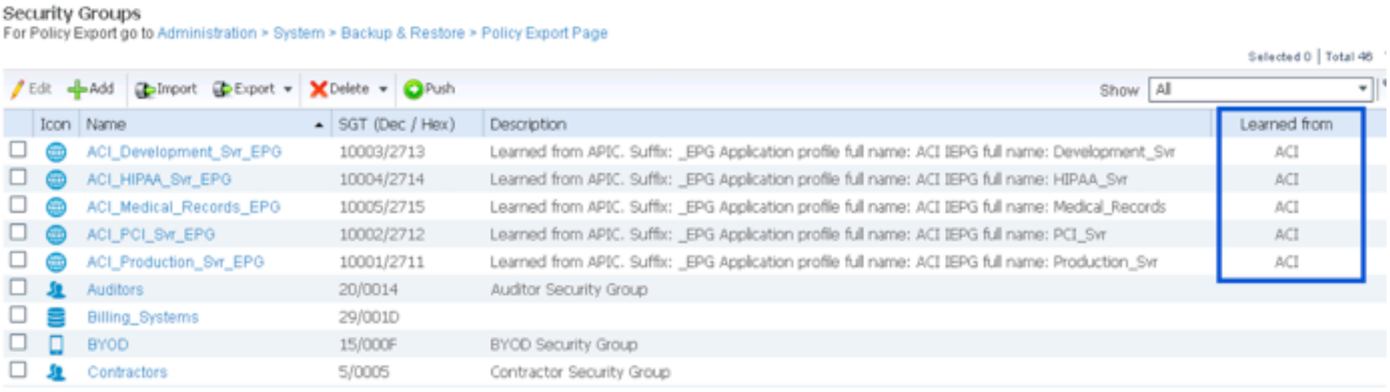
Once saved ISE and the APIC-DC controller will start sharing the policy group information (SGTs & EPGs) with each other.

Verify IEPGs propagated to ISE

Now that the Certificate is imported and the ACI settings are configured in ISE, ISE will retrieve IEPGs (Internal Endpoint Groups) from the APIC-DC controller. To validate that the APIC-DC EPGs are received in ISE

Step 1 Navigate to **Security Groups** to see all the Security Groups in ISE under **Work Centers > TrustSec > Components > Security Groups**

Step 2 Verify that there are newly created Security Groups with a suffix '_EPG' are imported into ISE



Security Groups

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

	Icon	Name	SGT (Dec / Hex)	Description	Learned from
☐	🌐	ACI_Development_Svr_EPG	10003/2713	Learned from APIC. Suffix: _EPG Application profile full name: ACI IEPG full name: Development_Svr	ACI
☐	🌐	ACI_HIPAA_Svr_EPG	10004/2714	Learned from APIC. Suffix: _EPG Application profile full name: ACI IEPG full name: HIPAA_Svr	ACI
☐	🌐	ACI_Medical_Records_EPG	10005/2715	Learned from APIC. Suffix: _EPG Application profile full name: ACI IEPG full name: Medical_Records	ACI
☐	🌐	ACI_PCI_Svr_EPG	10002/2712	Learned from APIC. Suffix: _EPG Application profile full name: ACI IEPG full name: PCI_Svr	ACI
☐	🌐	ACI_Production_Svr_EPG	10001/2711	Learned from APIC. Suffix: _EPG Application profile full name: ACI IEPG full name: Production_Svr	ACI
☐	👥	Auditors	20/0014	Auditor Security Group	
☐	🛢	Billing_Systems	29/001D		
☐	📱	BYOD	15/000F	BYOD Security Group	
☐	👥	Contractors	5/0005	Contractor Security Group	

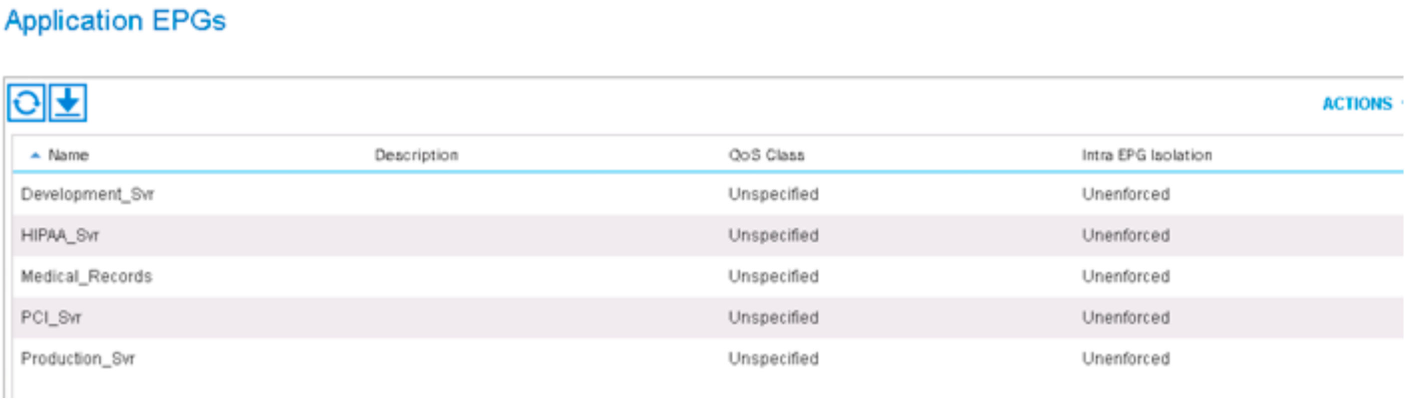
Those security groups are assigned a value from 10,000 and higher (as we configured above). They are described as ‘Learned from ACI’. The description field contains the complete details of the EPG with the Application profile name and the IEPG full name.

Note: ISE 2.1 supports only 32 characters SGT name whereas ACI supports a 64 character EPG. In those cases the name will be truncated and the full EPG name details can be viewed in the description. Also ISE supports only underscore ‘_’ and alphanumeric characters for the SGTs so the IEPGS need to be on the similar format to propagate to ISE.

Verify IEPGs in APIC-DC

Step 1 From the APIC-DC controller navigate to Tenants > Application Profiles > Application EPGs

Step 2 All the application EPGs propagated into ISE can be verified from the APIC-DC controller UI



Application EPGs

Name	Description	QoS Class	Intra EPG Isolation
Development_Svr		Unspecified	Unenforced
HIPAA_Svr		Unspecified	Unenforced
Medical_Records		Unspecified	Unenforced
PCI_Svr		Unspecified	Unenforced
Production_Svr		Unspecified	Unenforced

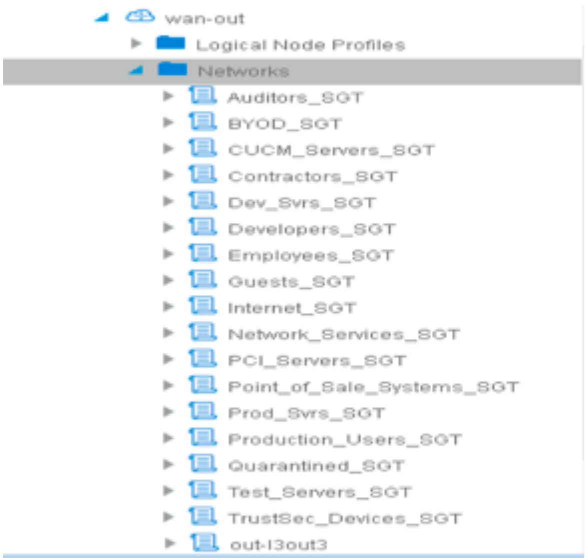
Verify EEPGs propagated to ACI

The SGTs from the ISE are propagated as External Endpoint Groups (EEPGs) in ACI. Validate that the specified groups are being shared with ACI by going to the APIC-DC controller UI.

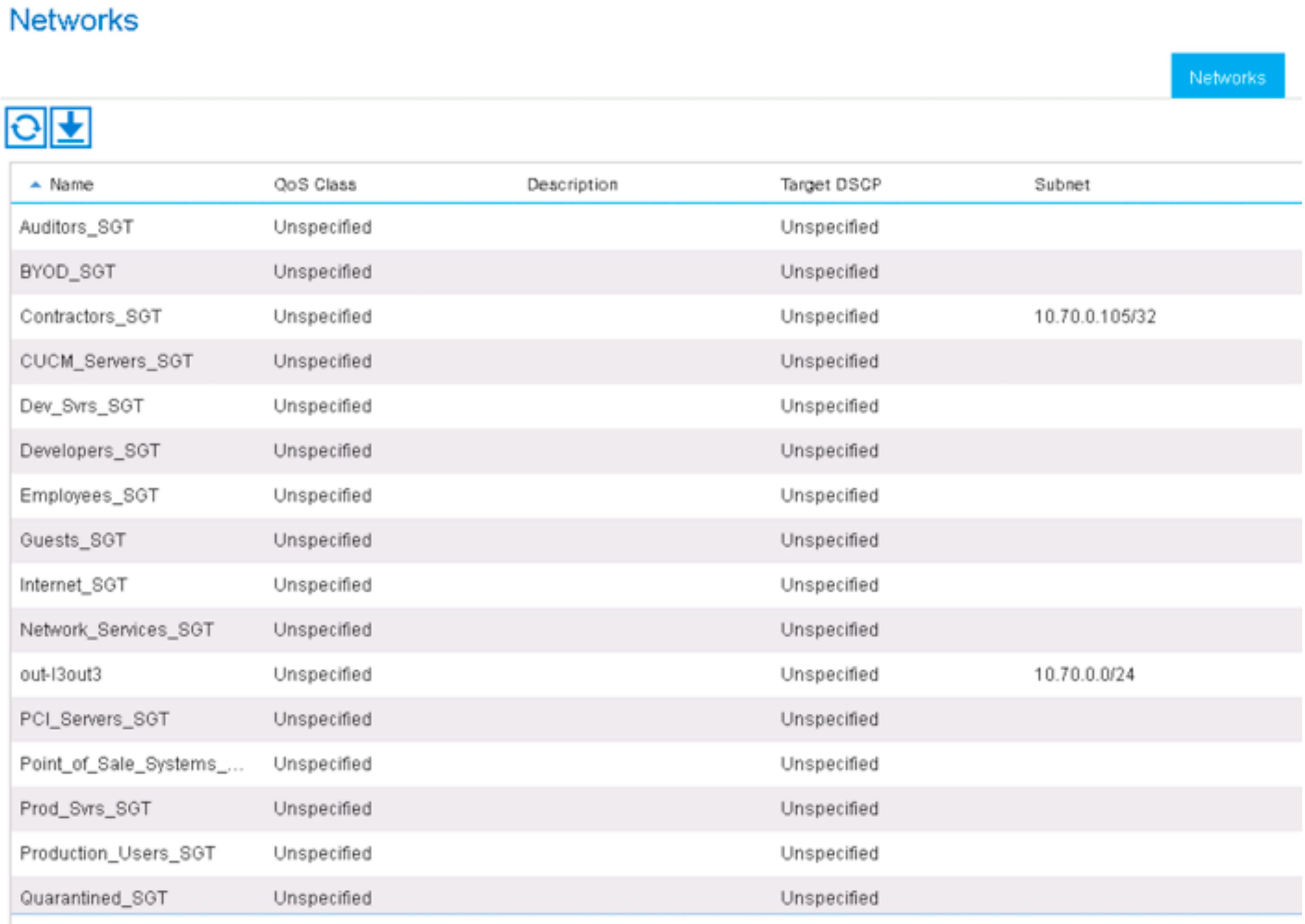
Step 1 In the APIC-DC Controller navigate to **Tenants > Networking > External Routed Networks > L3 Outside** (click on the one which was added under ISE ACI Settings)

Step 2 Click **‘Networks’** to see the propagated Security Groups from ISE as the new EEPGs with a suffix ‘_SGT’ (configured earlier)

Only the Security Groups that were configured earlier to send to ACI are propagated as EEPGs as shown below



- wan-out
  - Logical Node Profiles
  - Networks
    - Auditors_SGT
    - BYOD_SGT
    - CUCM_Servers_SGT
    - Contractors_SGT
    - Dev_Svrs_SGT
    - Developers_SGT
    - Employees_SGT
    - Guests_SGT
    - Internet_SGT
    - Network_Services_SGT
    - PCI_Servers_SGT
    - Point_of_Sale_Systems_SGT
    - Prod_Svrs_SGT
    - Production_Users_SGT
    - Quarantined_SGT
    - Test_Servers_SGT
    - TrustSec_Devices_SGT
    - out-l3out3



Networks

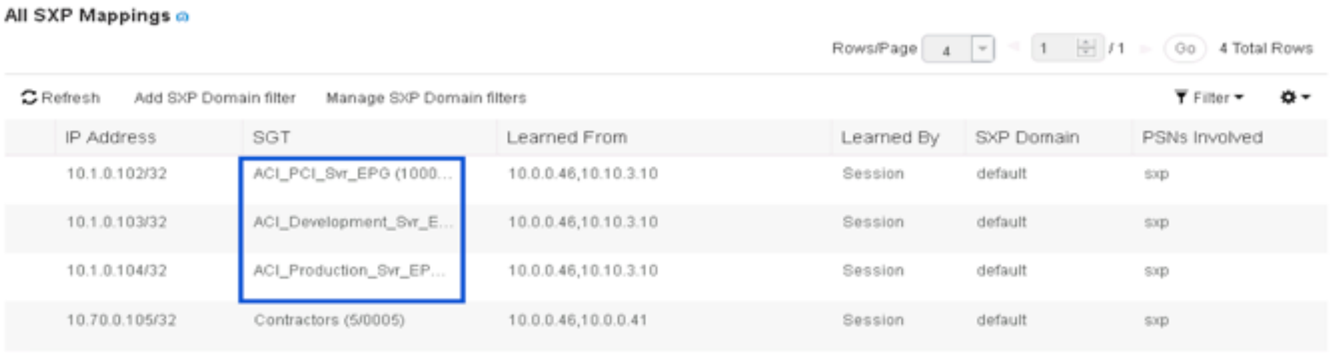
Name	QoS Class	Description	Target DSCP	Subnet
Auditors_SGT	Unspecified		Unspecified	
BYOD_SGT	Unspecified		Unspecified	
Contractors_SGT	Unspecified		Unspecified	10.70.0.105/32
CUCM_Servers_SGT	Unspecified		Unspecified	
Dev_Svrs_SGT	Unspecified		Unspecified	
Developers_SGT	Unspecified		Unspecified	
Employees_SGT	Unspecified		Unspecified	
Guests_SGT	Unspecified		Unspecified	
Internet_SGT	Unspecified		Unspecified	
Network_Services_SGT	Unspecified		Unspecified	
out-l3out3	Unspecified		Unspecified	10.70.0.0/24
PCI_Servers_SGT	Unspecified		Unspecified	
Point_of_Sale_Systems_...	Unspecified		Unspecified	
Prod_Svrs_SGT	Unspecified		Unspecified	
Production_Users_SGT	Unspecified		Unspecified	
Quarantined_SGT	Unspecified		Unspecified	

Verify the ACI Endpoints (EPs) converted in ISE as IP-SGT Mappings

Once the EPGs are converted to the relevant SGTs in ISE, the Endpoints (EPs) of the EPGs are converted to IP-Mappings under the All SXP Mappings in ISE. This can be verified in ISE:

Step 1 In ISE navigate to **SXP Mappings** under **Work Centers > TrustSec > SXP > All SXP Mappings**

Step 2 Look for the newly created IP-SGT Mappings of the Security Groups (from EPGs) with the relevant SXP Domain

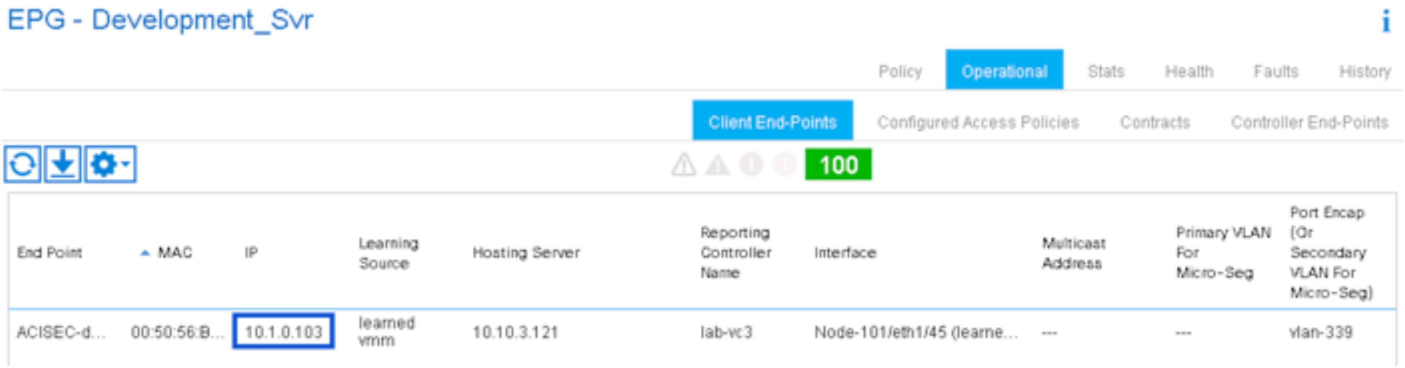

All SXP Mappings

IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs Involved
10.1.0.102/32	ACI_PCI_Svr_EPG (1000...	10.0.0.46,10.10.3.10	Session	default	sxp
10.1.0.103/32	ACI_Development_Svr_E...	10.0.0.46,10.10.3.10	Session	default	sxp
10.1.0.104/32	ACI_Production_Svr_EP...	10.0.0.46,10.10.3.10	Session	default	sxp
10.70.0.105/32	Contractors (5/0005)	10.0.0.46,10.0.0.41	Session	default	sxp

Step 3 On the APIC-DC Controller, verify the Endpoint (EP) details by navigating to **Tenants > Application Profiles > Application EPGs**

Step 4 Click the name of the EPG which needs to be validated.

Step 5 Click on the **Operational** tab and **Client End-Points** tab for the Endpoint (EP) details such as the IP address and name.


EPG - Development_Svr

End Point	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Primary VLAN For Micro-Seg	Port Encap (Or Secondary VLAN For Micro-Seg)
ACISEC-d...	00:50:56:B...	10.1.0.103	learned vmm	10.10.3.121	lab-vc3	Node-101/eth1/45 (learne...	---	---	vlan-339

Step 6 The above IP address of the Endpoint is already propagated to ISE under IP-SGT Mappings (above)

Step 7 Repeat the same on the rest of the EPGs for verification

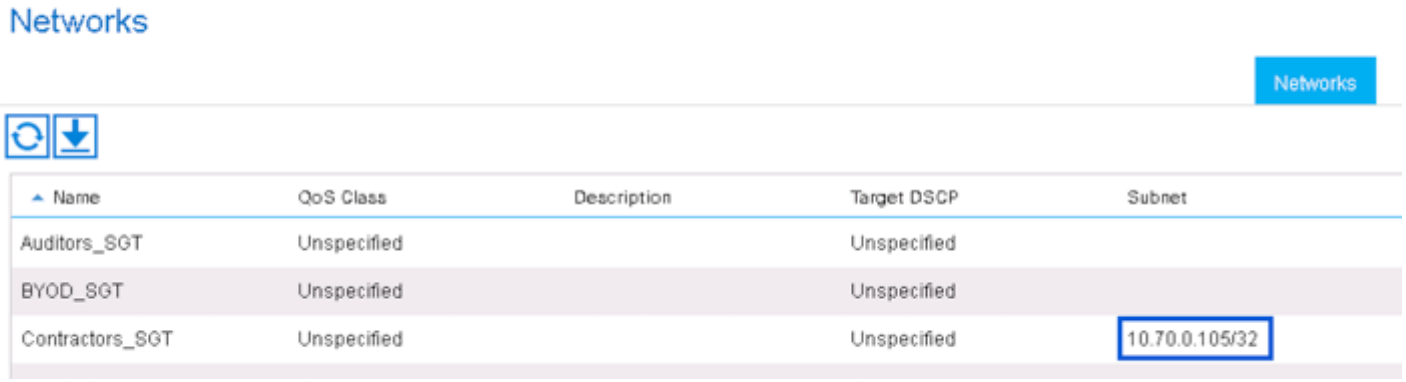
Verify the IP-SGT Mappings from ISE are converted to EEPG Members

As soon as the SGTs from ISE are propagated as External Endpoint Groups (EEPGs) in ACI, the IP-SGT Mappings from ISE are also visible in ACI as Subnets under the EEPGs.

Step 1 Verify this on the APIC-DC controller UI by navigating to **Tenants > Networking > External Routed Networks > L3 Outside** (click on the one which was added under ISE ACI Settings)

Step 2 Click **Networks** to see the propagated Security Groups from ISE as the new EEPGs with a suffix '_SGT' (configured earlier)

Step 3 Look for the Subnets containing the IP address. Verify the Subnet information with the IP-SGT mapping information in ISE



Name	QoS Class	Description	Target DSCP	Subnet
Auditors_SGT	Unspecified		Unspecified	
BYOD_SGT	Unspecified		Unspecified	
Contractors_SGT	Unspecified		Unspecified	10.70.0.105/32

Note: **TrustSec-ACI Integration Scalability Limits**

These are the scaling numbers supported in this initial release of TrustSec-ACI Policy Plane Integration.

ACI Fabrics **currently** supports up to **250 Security Groups** from the TrustSec policy domain. On the number of **IP-Group** mappings in the ACI fabric, the older generation Leaf switches can support up to **4000** (/32) mappings. The newer generation (gen2) Leaf switches (EX) can scale up to **10,000** (/32) IP-SGT mappings. There as no hard limits on the number of EPGs or group members being **retrieved by** ISE (2.1), which supports **500,000** IP-SGT mappings and **4000** Security Groups.

Use Cases for Policy Enforcement

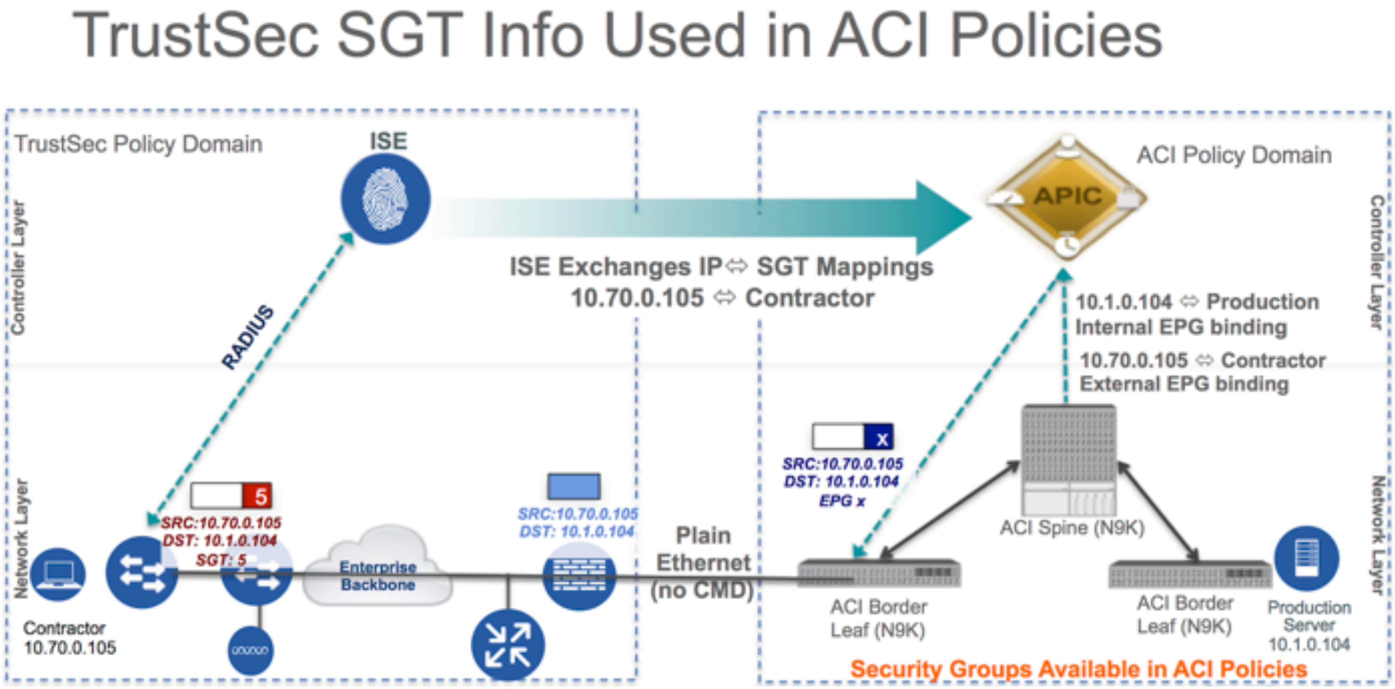
Depending on the policy goals of a given organization, different use-cases may call for policy enforcement to be enabled within the ACI environment, within the TrustSec domain or even both.
Two typical scenarios are included for reference, based upon experience with early adopters.

Sample Use Case with Policy Enforcement enabled in ACI

ISE can dynamically provision the TrustSec Security Groups into the ACI fabric with this policy plane integration so that these SGT classifications may be used to enforce policy in the ACI environment. We have seen how the relevant SGTs from ISE are converted to EEPGs in the previous section. For example, if we take a PCI compliance use case, where the critical assets like PCI servers located in the ACI data center need to be accessed by the specific campus users and groups like Auditors or Point of Sale (PoS) systems. Through ISE we can dynamically provision the Auditor and PoS systems Security Group information in the ACI fabric as EEPGs. With the use of Contracts and Filters in the ACI, we can enable access to the PCI servers located in the ACI data center from the campus security groups like Auditors and PoS systems.

In the example shown below we have a role called Contractor in the TrustSec Policy Domain trying to access the Production Server group in the ACI data center. ISE will dynamically provision the contractor Security Group in the ACI fabric as an EEPG. We can then create a Contract between these two EPGs to allow communication.

Figure 3: TrustSec Security Groups Provisioned in ACI:



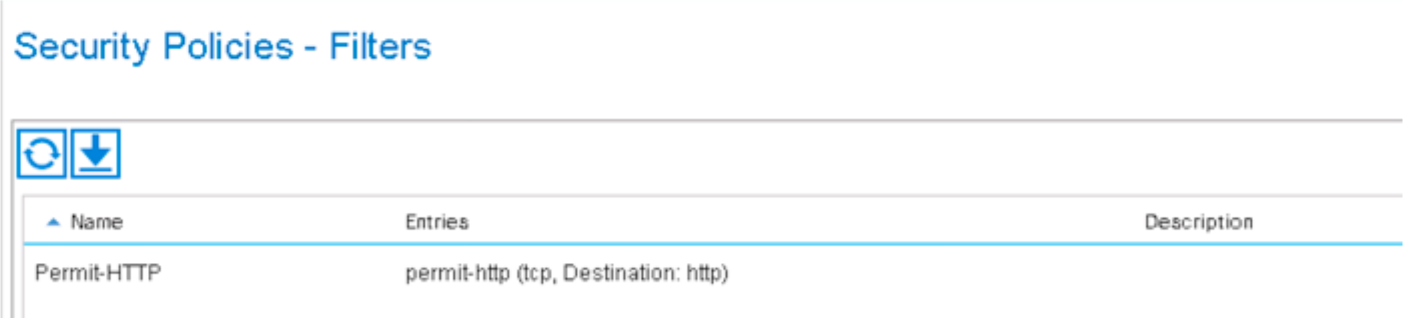
Contracts and Filters are required in the APIC-DC controller of the ACI fabric to allow the communication between the different EPGs (Inc. IEPGs and EEPGs). These are typically the protocols and the ports needed for communication.

ACI uses a whitelist model so you need to explicitly allow the ports and the protocols using filters and contracts for communication otherwise the EPGs and the EPs (part of EPGs) will not communicate with each other. Below are the steps required to configure the Contracts and Filters to allow communication between the IEPG Production Server and the EEPG Contractor.

Configuration of Filters

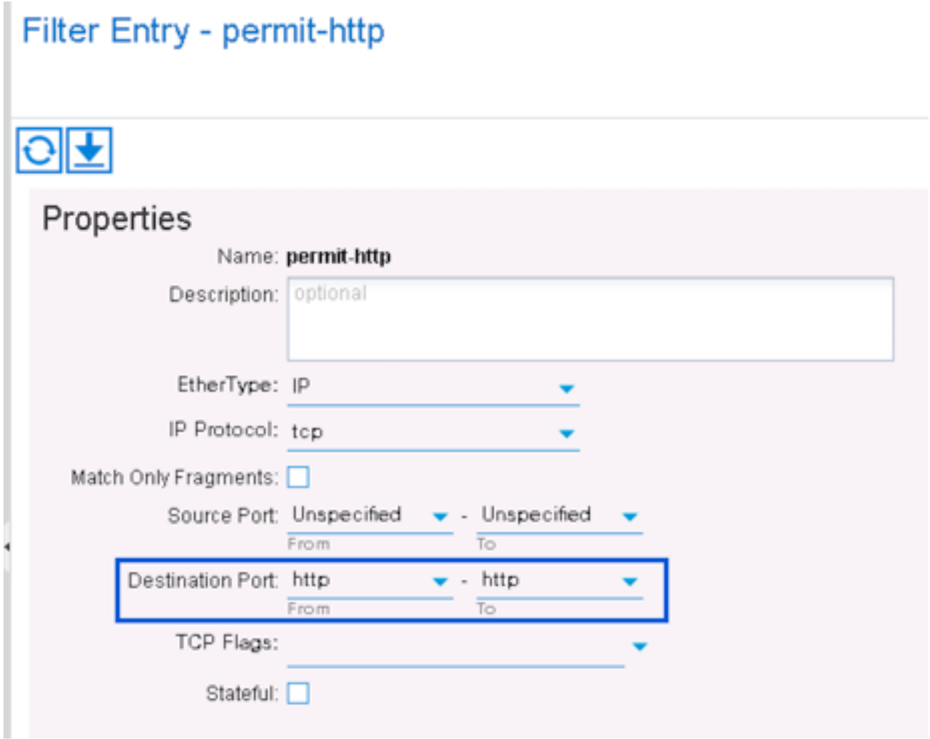
Step 1 From the APIC-DC Controller UI navigate to **Tenants > Security Policies > Filters** to create the Filter and the Filter entry

Below is the sample Filter Permit-HTTP with a Filter Entry 'permit-http'



Security Policies - Filters

Name	Entries	Description
Permit-HTTP	permit-http (tcp, Destination: http)	



Filter Entry - permit-http

Properties

Name: **permit-http**

Description: optional

EtherType: IP

IP Protocol: tcp

Match Only Fragments: ☐

Source Port: Unspecified (From) - Unspecified (To)

Destination Port: http (From) - http (To)

TCP Flags:

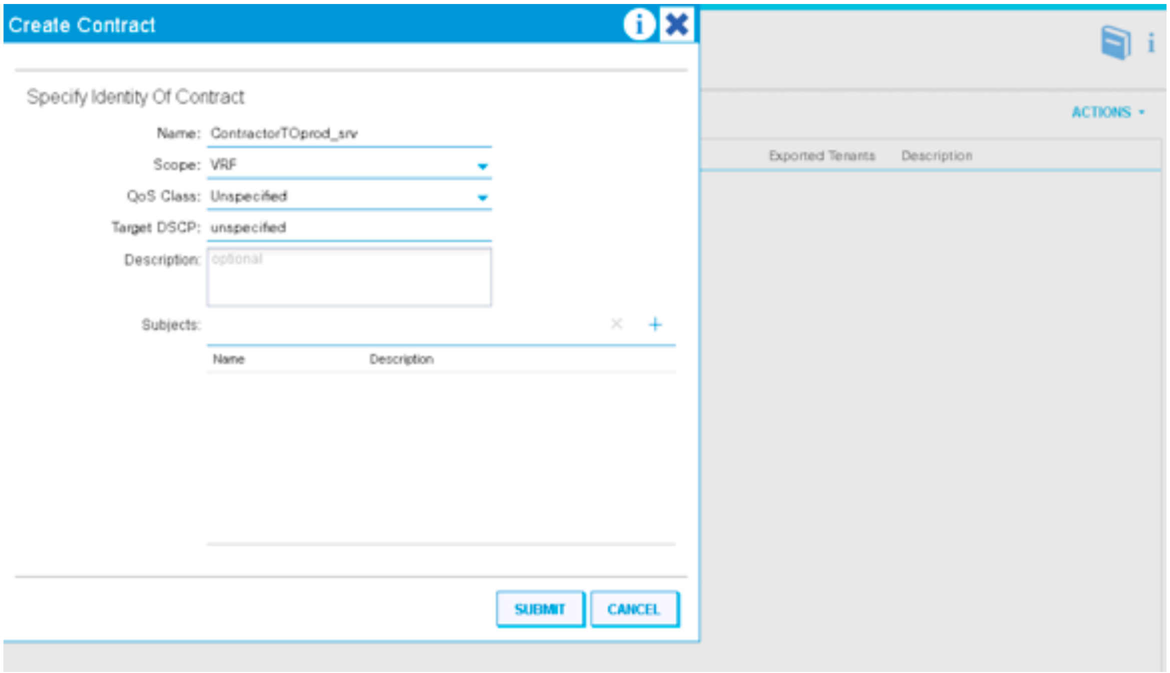
Stateful: ☐

The configured Filter would be used in a Contract to allow the communication between the EPGs

Configuration of Contracts

Step 1 From the APIC-DC Controller UI navigate to **Tenants > Security Policies > Contracts** to create a contract

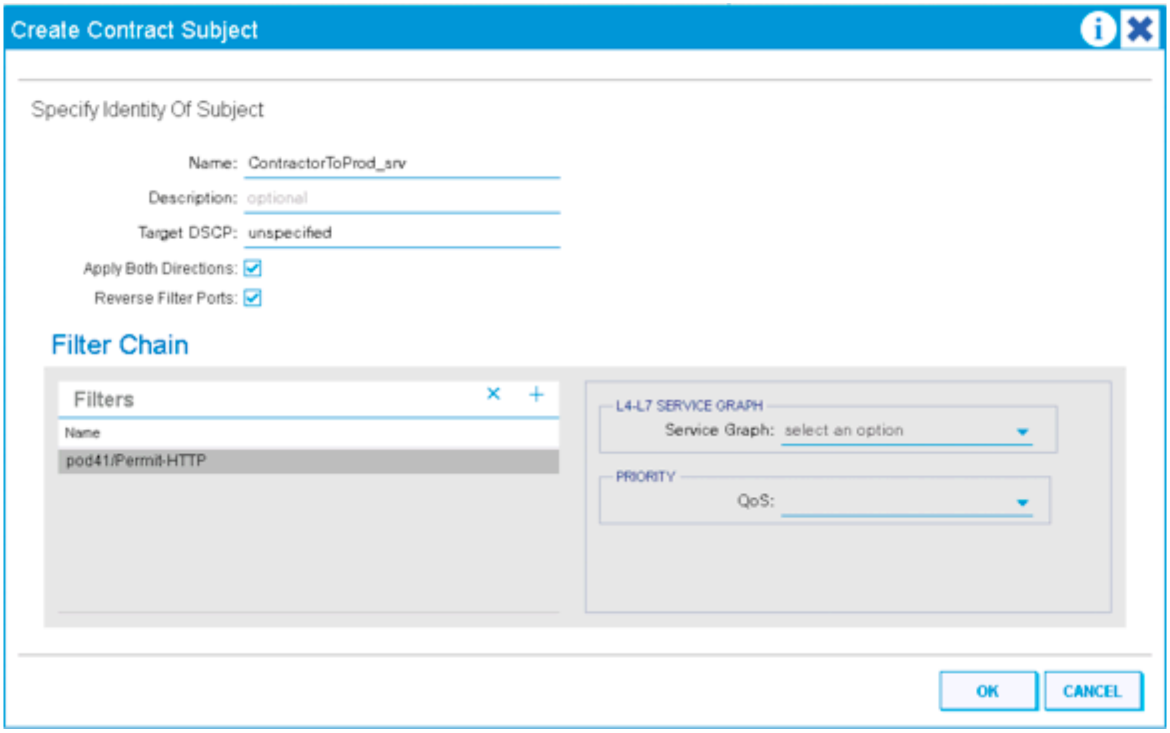
Step 2 Click on the **Actions** tab on the Right side and select the drop down to create a new Contract



Specify Identity Of Contract

Name: ContractorTOprod_srv
Scope: VRF
QoS Class: Unspecified
Target DSCP: unspecified
Description: optional

Step 3 Add a new Subject with the name and the Filter. Use the above created filter Permit-HTTP



Specify Identity Of Subject

Name: ContractorToProd_srv
Description: optional
Target DSCP: unspecified
Apply Both Directions: ☑
Reverse Filter Ports: ☑

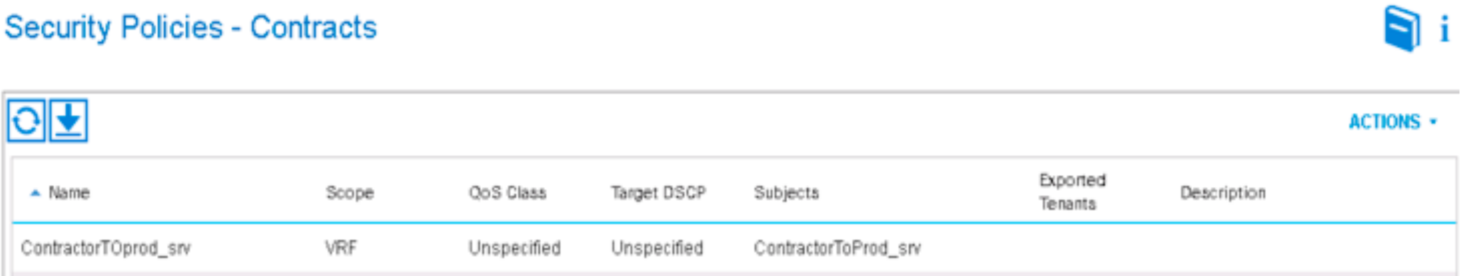
Filter Chain

Filters
Name
pod41/Permit-HTTP

L4-L7 SERVICE GRAPH
Service Graph: select an option

PRIORITY
QoS:

Step 4 Click **OK** and Submit the Contract. It creates a new contract as shown below

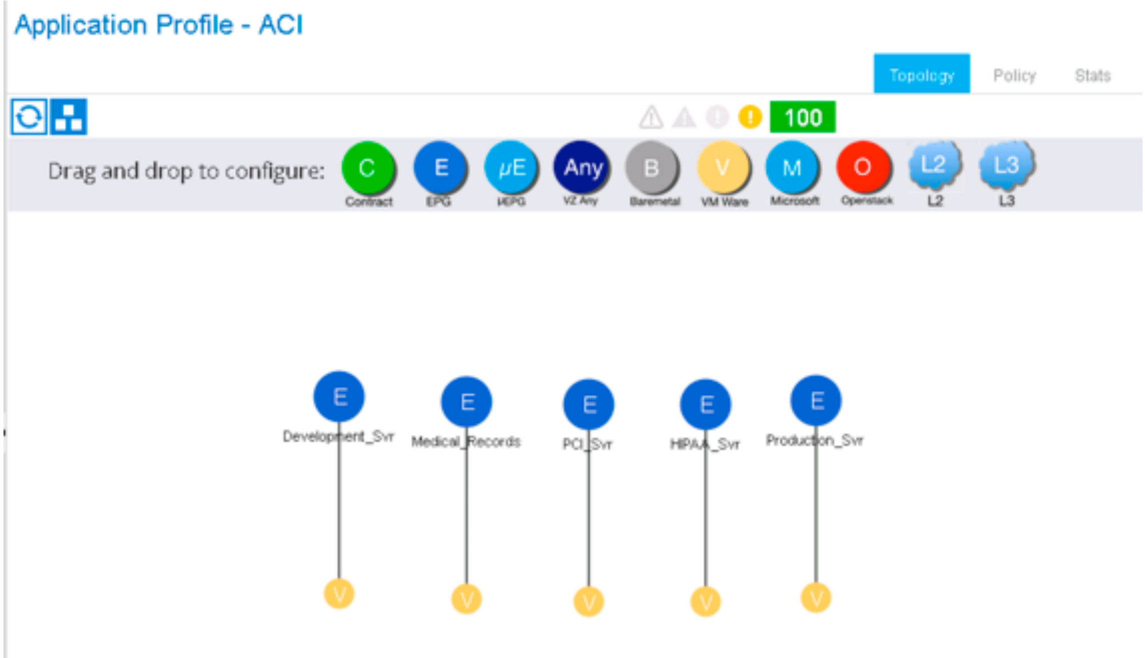


Security Policies - Contracts

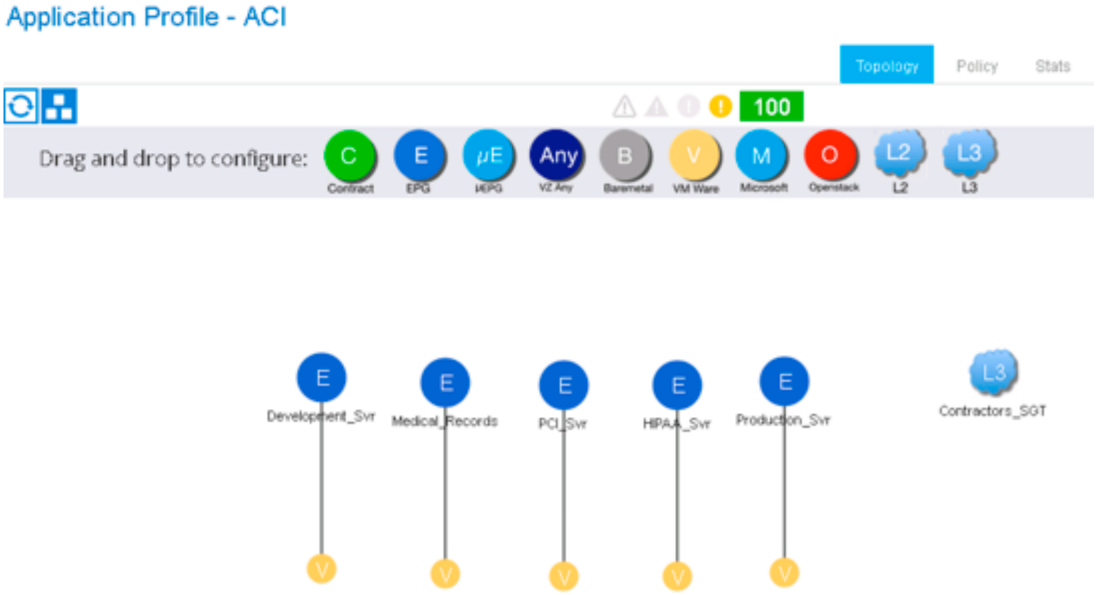
Name	Scope	QoS Class	Target DSCP	Subjects	Exported Tenants	Description
ContractorTOprod_srv	VRF	Unspecified	Unspecified	ContractorToProd_srv		

Step 5 Now to create a Contract between the EPGs navigate to **Tenants > Application Profiles > Application Profile** name (which is already configured)

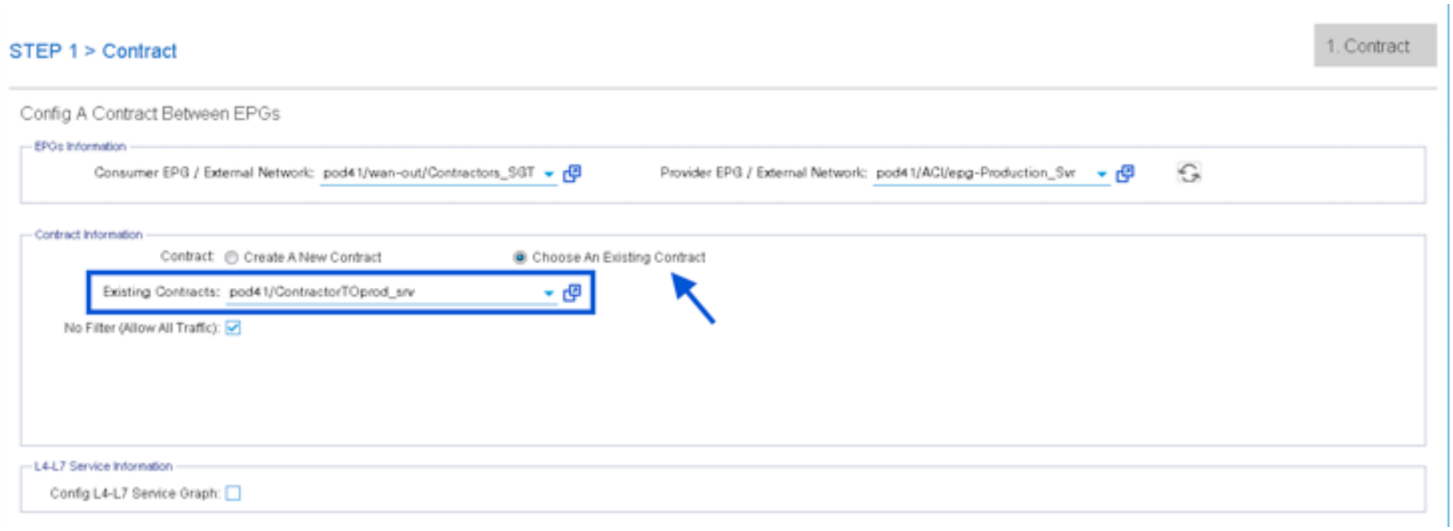
Step 6 Drag and drop to configure the Contract between the EPGs.



Step 7 Drag the L3 Outside network icon and select the Contractor External Endpoint Group



Step 8 Drag the Contract icon between the Contractor and Production Server EPGs to configure a contract and use the existing contract configured above (ContractorToProd_srv)



STEP 1 > Contract

1. Contract

Config A Contract Between EPGs

EPGs Information

Consumer EPG / External Network: pod41/wan-out/Contractors_SGT

Provider EPG / External Network: pod41/ACI/epg-Production_Svr

Contract Information

Contract: ○ Create A New Contract ● Choose An Existing Contract

Existing Contracts: pod41/ContractorTOprod_srv

No Filter (Allow All Traffic): ☑

L4-L7 Service Information

Config L4-L7 Service Graph: ☐

Step 9 Click **OK** to save the contract between the EPGs to allow the communication.

Through the above configuration the contractor would only get access to the Production Web server (http only). Ping from the user to the server fails, as it needs to be explicitly allowed.

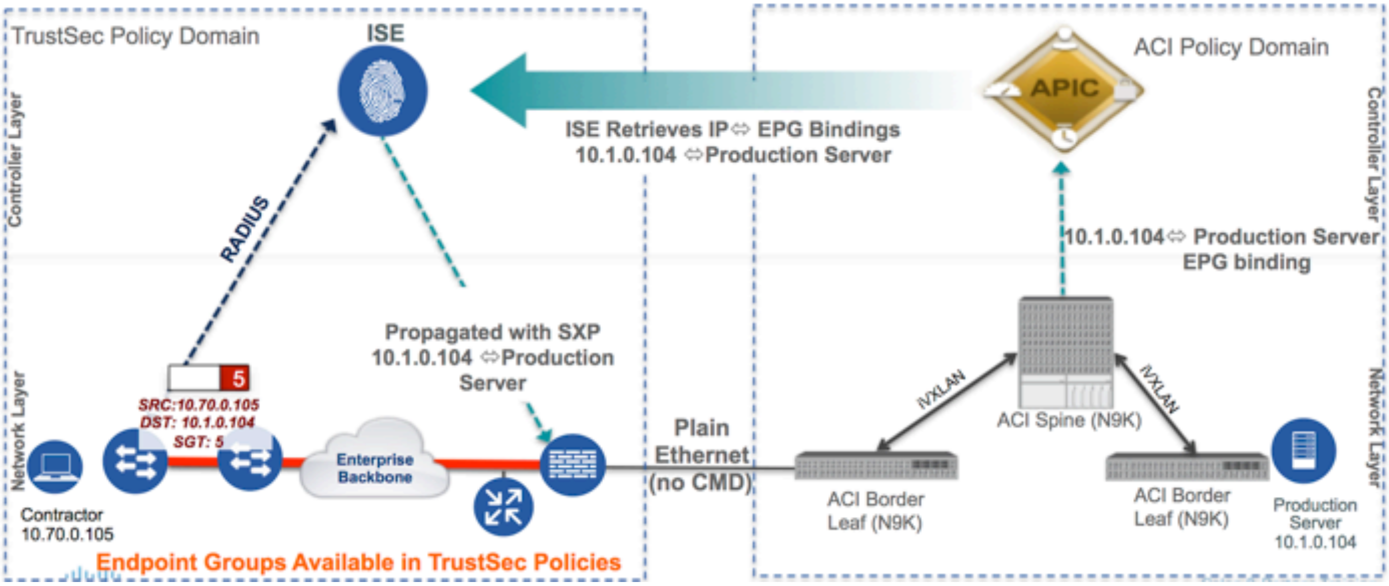
Sample Use Case with Policy Enforcement Enabled in the TrustSec Domain

ISE can dynamically learn the Endpoint Groups (EPGs) and the Endpoints (EPs) from the ACI fabric with this policy plane integration. As such, the relevant EPGs from the ACI fabric (detailed in the previous section) are converted to SGTs. Essentially classifications for the new workloads and the application servers from the ACI enabled datacenter are available in the TrustSec policy domain so that policy enforcement can be enabled in campus, branch, VPN or TrustSec-enabled data centers. For example if we take a healthcare use case where the critical assets like Medical Records servers located in the ACI data center need to be accessed by the campus users such as Doctors. Through ISE we can dynamically learn the Medical Record Server EPG information from the ACI fabric. The corresponding SGTs would be created in ISE and used for policy enforcement.

Similarly in the example below we have a Contractor role in the TrustSec Policy Domain in a campus location trying to access a Production Server in the ACI data center. ISE dynamically learns the Production Server IEPG from the ACI fabric and creates a corresponding SGT. That SGT classification can be used to enforce policy in the TrustSec domain using an SGACL on a switch, router, WLC or a Security Group Firewall (SGFW) rule as illustrated below.

Figure 4: ACI EPGs used to enforce policy in the TrustSec Policy Domain

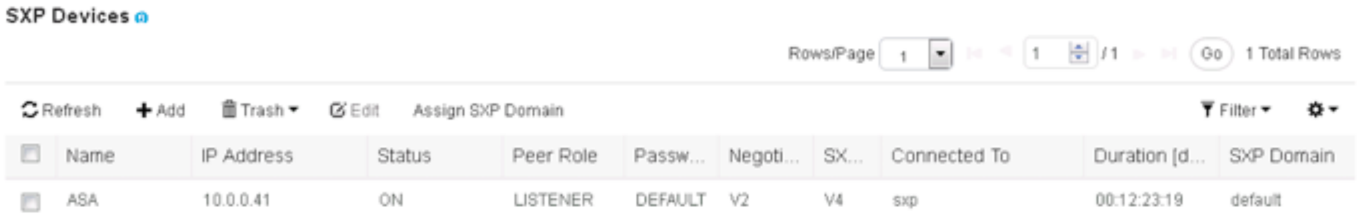
ACI EPG Info Used in TrustSec Policies



Here an ASAv is configured as a SXP listener in ISE. The ACI EPGs and the Endpoints (EPs) are converted in ISE as Security Groups and the IP-SGT Mappings. These mappings are propagated to ASAv via SXP. The ASAv is configured with SGFW rules for policy enforcement to allow the communication between the Contractor SGT and the Production Server SGT.

Step 1 Navigate to **Work Centers > TrustSec > SXP > SXP Devices**

Step 2 Configure the ASAv as the SXP listener in ISE

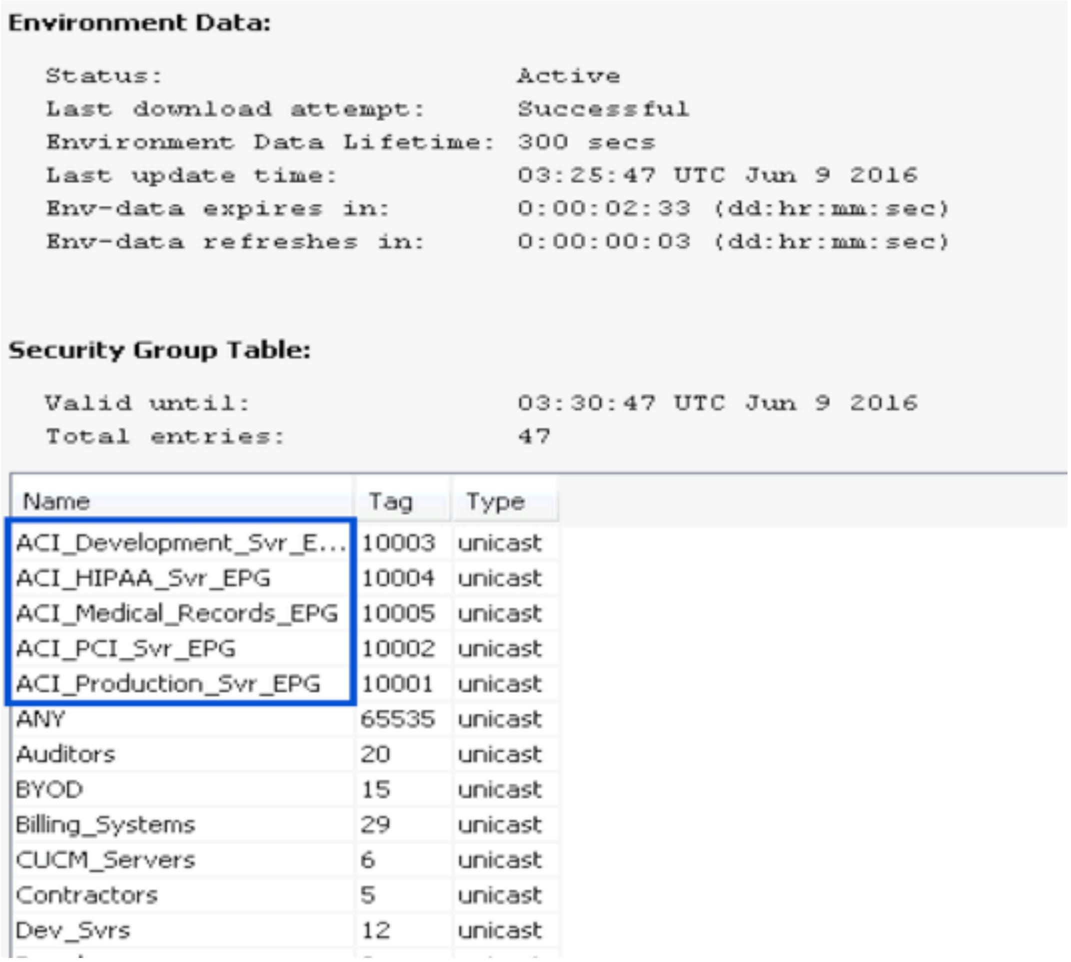


☐	Name	IP Address	Status	Peer Role	Passw...	Negoti...	SX...	Connected To	Duration [d...	SXP Domain
☐	ASA	10.0.0.41	ON	LISTENER	DEFAULT	V2	V4	sxp	00:12:23:19	default

Policy Enforcement Configuration on the ASAv

Step 1 From the ASDM of the ASAv navigate to **Monitoring > Properties > Identity by TrustSec > Environment Data**

Step 2 Look for the Security Groups propagated from ACI into ISE.



Environment Data:

```
Status:                       Active
Last download attempt:        Successful
Environment Data Lifetime:    300 secs
Last update time:             03:25:47 UTC Jun 9 2016
Env-data expires in:          0:00:02:33 (dd:hr:mm:sec)
Env-data refreshes in:        0:00:00:03 (dd:hr:mm:sec)
```

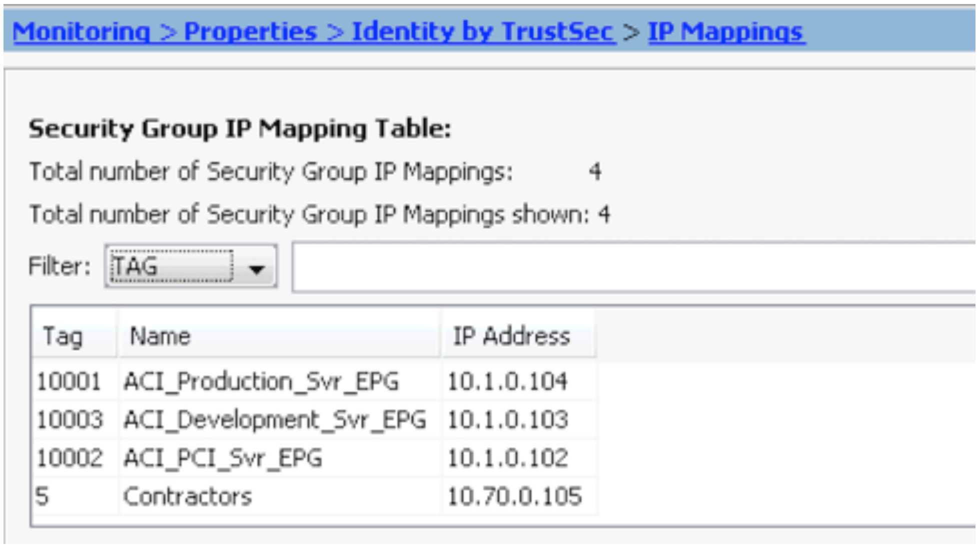
Security Group Table:

```
Valid until:                  03:30:47 UTC Jun 9 2016
Total entries:                47
```

Name	Tag	Type
ACI_Development_Svr_E...	10003	unicast
ACI_HIPAA_Svr_EPG	10004	unicast
ACI_Medical_Records_EPG	10005	unicast
ACI_PCI_Svr_EPG	10002	unicast
ACI_Production_Svr_EPG	10001	unicast
ANY	65535	unicast
Auditors	20	unicast
BYOD	15	unicast
Billing_Systems	29	unicast
CUCM_Servers	6	unicast
Contractors	5	unicast
Dev_Svrs	12	unicast

Similarly look for the IP Mappings information in ASAv. Those should contain the mappings of the Endpoints (EPs) from ACI.

Step 3 Navigate to **Monitoring > Properties > Identity by TrustSec > IP Mappings**. These contain the mappings of the Endpoints (EPs) from ACI



Monitoring > Properties > Identity by TrustSec > IP Mappings

Security Group IP Mapping Table:

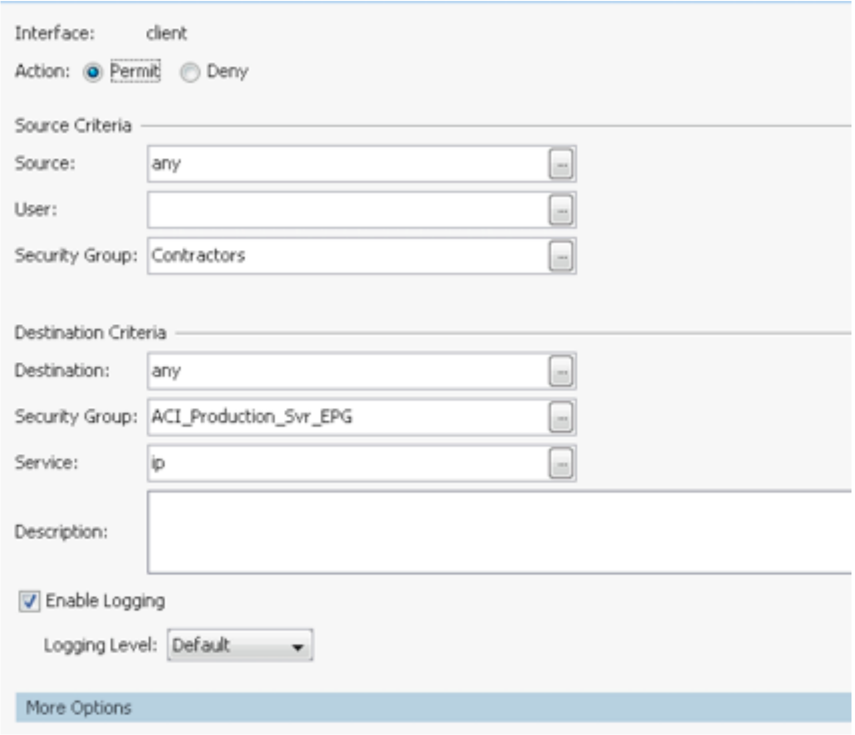
Total number of Security Group IP Mappings: 4

Total number of Security Group IP Mappings shown: 4

Filter: TAG

Tag	Name	IP Address
10001	ACI_Production_Svr_EPG	10.1.0.104
10003	ACI_Development_Svr_EPG	10.1.0.103
10002	ACI_PCI_Svr_EPG	10.1.0.102
5	Contractors	10.70.0.105

Step 4 Now create a new Access Rule on the ASAv to allow the communication between Contractor and the Production Server by permitting the traffic.



Interface: client

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

Security Group: Contractors

Destination Criteria

Destination: any

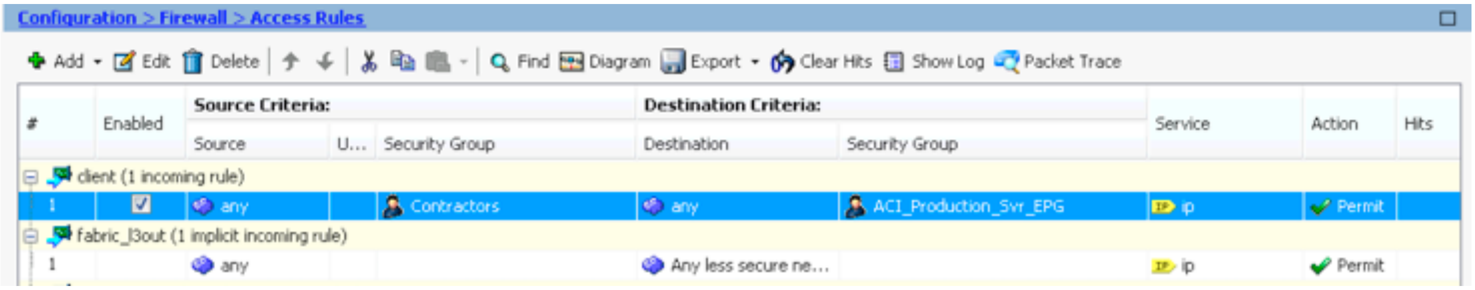
Security Group: ACI_Production_Svr_EPG

Service: ip

Description:

☑ Enable Logging

Logging Level: Default



#	Enabled	Source Criteria: Source	U...	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits
client (1 incoming rule)									
1	☑	any		Contractors	any	ACI_Production_Svr_EPG	ip	✓ Permit	
fabric_l3out (1 implicit incoming rule)									
1		any			Any less secure ne...		ip	✓ Permit	

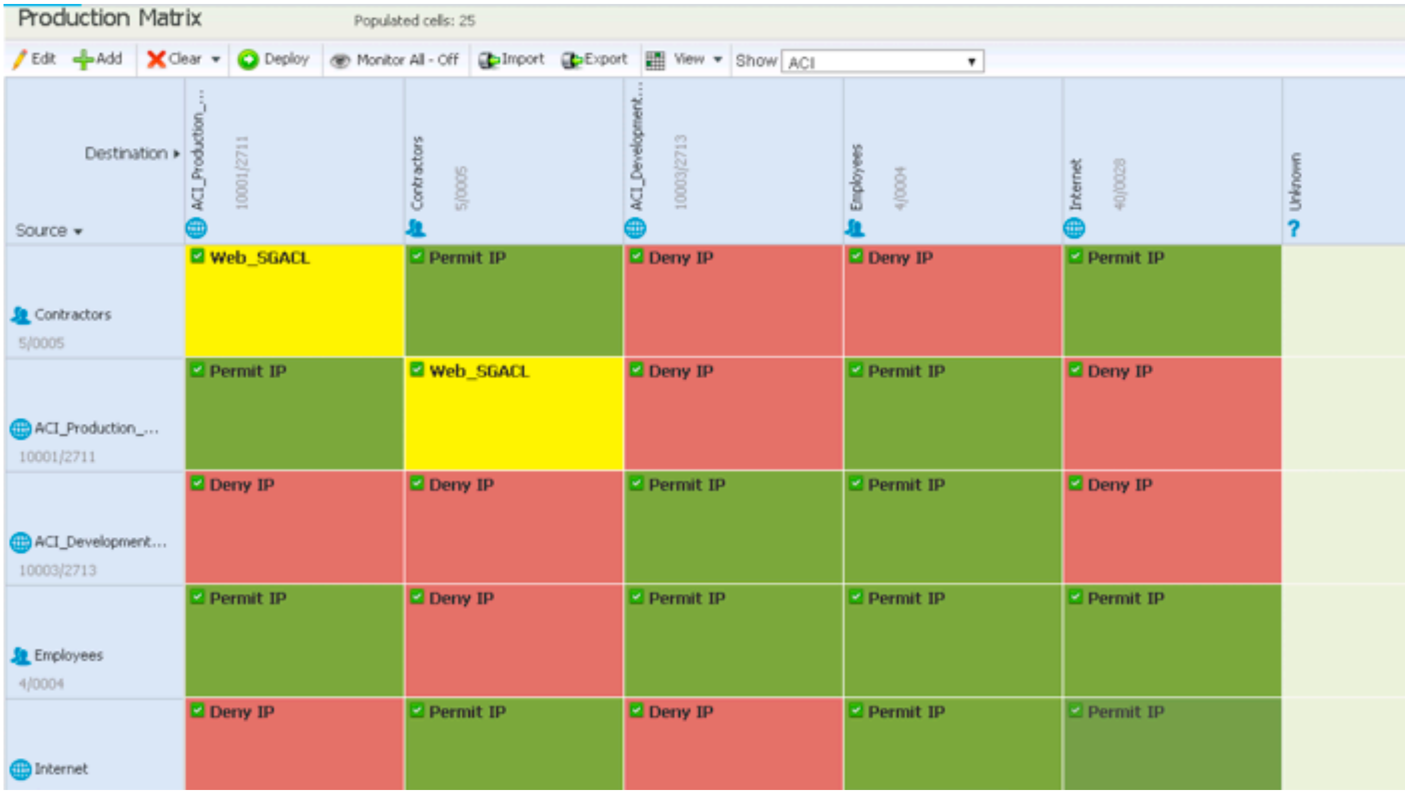
IEPG security groups from the ACI enabled data center are used in configuring the SGFW access rules in the ASAv. The TrustSec Domain is completely aware of the ACI workloads and the application servers of the ACI fabric.

TrustSec Policy Matrix in ISE

In the previous section the Security Group Firewall (SGFW) is used in the TrustSec domain for enforcing the traffic with the security groups from the ACI fabric. Instead of using a SGFW we can also 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.

Here is the sample TrustSec Policy Matrix from ISE with the policies configured similar to our example of Contractor and the Production Server.

Step 1 Navigate to **Work Centers > TrustSec > TrustSec Policy > Egress Policy** and click **Matrix** to view the TrustSec Policy Matrix



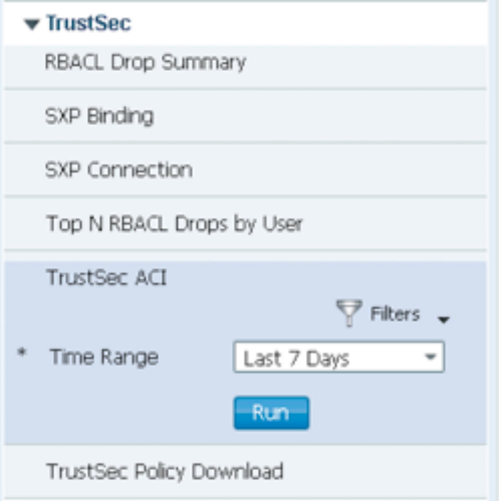
Source ▾ / Destination ▸	ACI_Production_... 10001/2711	Contractors 5/0005	ACI_Development... 10003/2713	Employees 4/0004	Internet 40/0028	Unknown
Contractors 5/0005	Web_SGACL	Permit IP	Deny IP	Deny IP	Permit IP	
ACI_Production_... 10001/2711	Permit IP	Web_SGACL	Deny IP	Permit IP	Deny IP	
ACI_Development... 10003/2713	Deny IP	Deny IP	Permit IP	Permit IP	Deny IP	
Employees 4/0004	Permit IP	Deny IP	Permit IP	Permit IP	Permit IP	
Internet	Deny IP	Permit IP	Deny IP	Permit IP	Permit IP	

Through the use of the policy matrix configuration and subsequent deployment, all the network devices comprising the TrustSec domain are aware of the EPGs from the ACI fabric.

TrustSec-ACI Reports

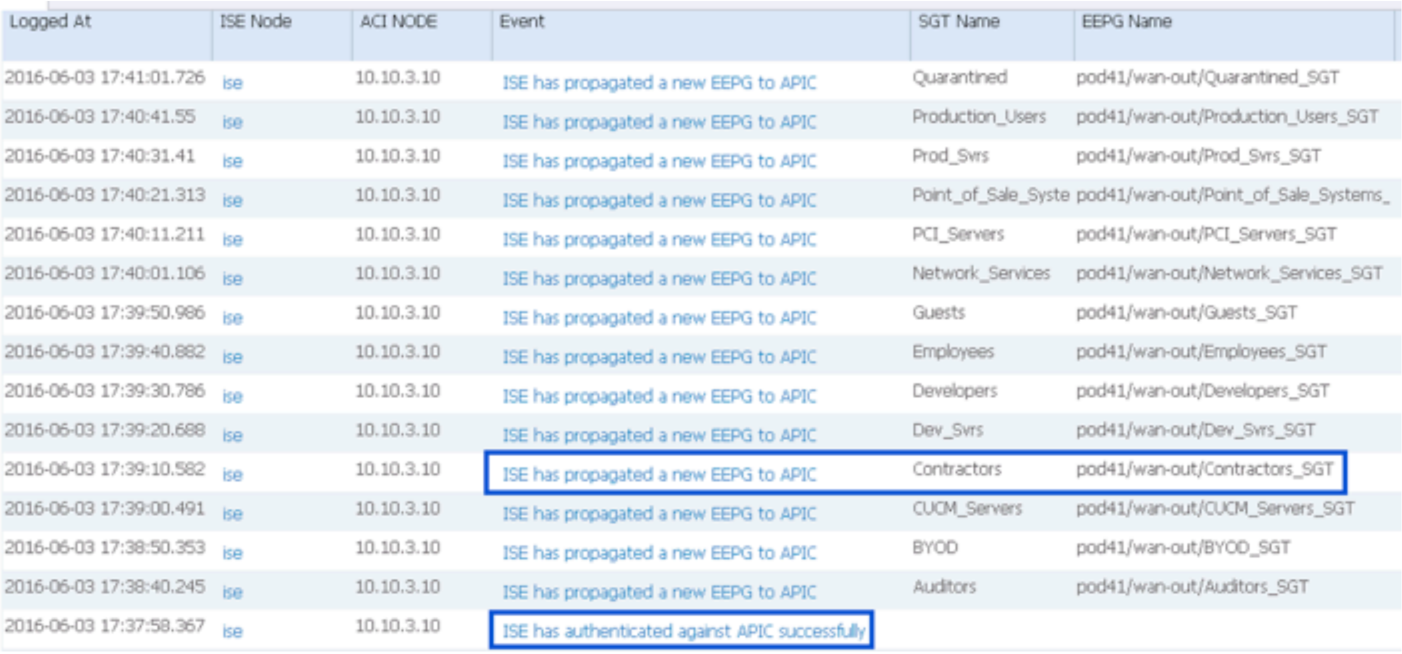
Step 1 TrustSec-ACI reports can be displayed by navigating to **Operations > Reports > TrustSec > TrustSec ACI**

Step 2 Set the time range and/or Filters and run the report:



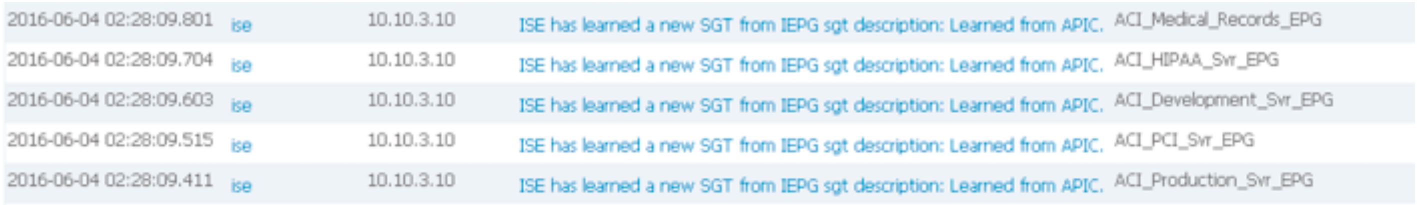
* Time Range: Last 7 Days

These reports help the administrator in Monitoring and Troubleshooting the flow. The report below shows the successful authentication of ISE against the APIC-DC controller. Once ISE is authenticated, the Security Groups from ISE are propagated as EEPGs in APIC-DC (shown below).



Logged At	ISE Node	ACI NODE	Event	SGT Name	EEPG Name
2016-06-03 17:41:01.726	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Quarantined	pod41/wan-out/Quarantined_SGT
2016-06-03 17:40:41.55	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Production_Users	pod41/wan-out/Production_Users_SGT
2016-06-03 17:40:31.41	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Prod_Svrs	pod41/wan-out/Prod_Svrs_SGT
2016-06-03 17:40:21.313	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Point_of_Sale_Syste	pod41/wan-out/Point_of_Sale_Systems_
2016-06-03 17:40:11.211	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	PCI_Servers	pod41/wan-out/PCI_Servers_SGT
2016-06-03 17:40:01.106	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Network_Services	pod41/wan-out/Network_Services_SGT
2016-06-03 17:39:50.986	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Guests	pod41/wan-out/Guests_SGT
2016-06-03 17:39:40.882	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Employees	pod41/wan-out/Employees_SGT
2016-06-03 17:39:30.786	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Developers	pod41/wan-out/Developers_SGT
2016-06-03 17:39:20.688	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Dev_Svrs	pod41/wan-out/Dev_Svrs_SGT
2016-06-03 17:39:10.582	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Contractors	pod41/wan-out/Contractors_SGT
2016-06-03 17:39:00.491	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	CUCM_Servers	pod41/wan-out/CUCM_Servers_SGT
2016-06-03 17:38:50.353	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	BYOD	pod41/wan-out/BYOD_SGT
2016-06-03 17:38:40.245	ise	10.10.3.10	ISE has propagated a new EEPG to APIC	Auditors	pod41/wan-out/Auditors_SGT
2016-06-03 17:37:58.367	ise	10.10.3.10	ISE has authenticated against APIC successfully		

Similarly the report below shows the new SGTs learned from IEPGs of the APIC-DC controller and ACI fabric



2016-06-04 02:28:09.801	ise	10.10.3.10	ISE has learned a new SGT from IEPG sgt description: Learned from APIC.	ACI_Medical_Records_EPG
2016-06-04 02:28:09.704	ise	10.10.3.10	ISE has learned a new SGT from IEPG sgt description: Learned from APIC.	ACI_HIPAA_Svr_EPG
2016-06-04 02:28:09.603	ise	10.10.3.10	ISE has learned a new SGT from IEPG sgt description: Learned from APIC.	ACI_Development_Svr_EPG
2016-06-04 02:28:09.515	ise	10.10.3.10	ISE has learned a new SGT from IEPG sgt description: Learned from APIC.	ACI_PCI_Svr_EPG
2016-06-04 02:28:09.411	ise	10.10.3.10	ISE has learned a new SGT from IEPG sgt description: Learned from APIC.	ACI_Production_Svr_EPG

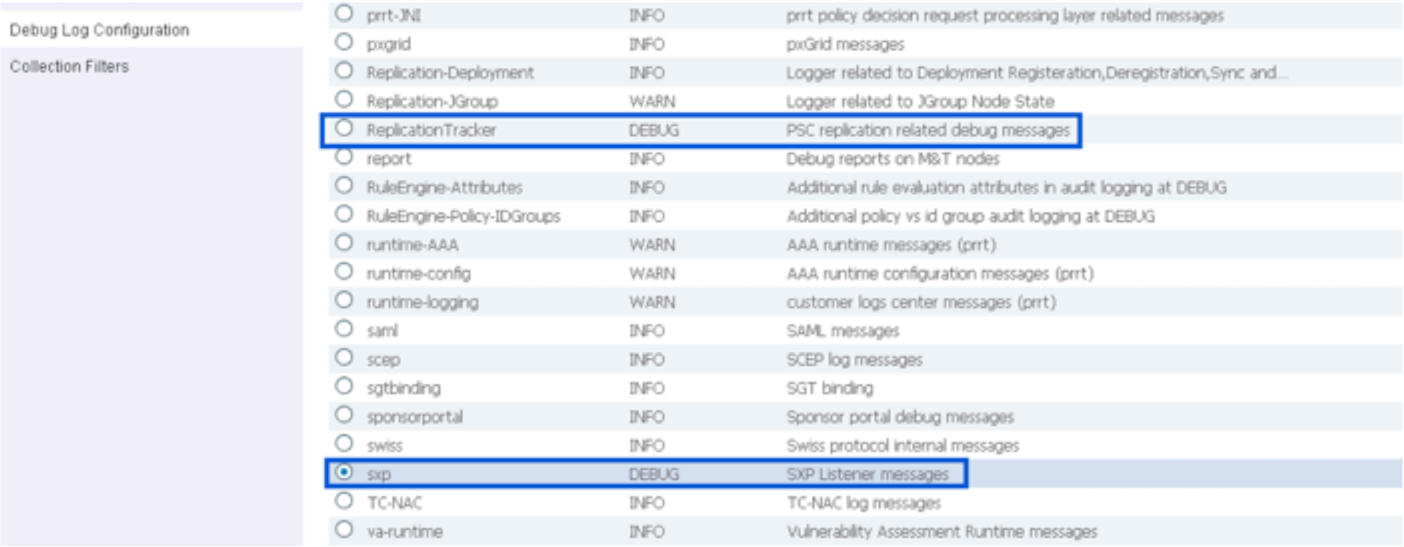
Debug TrustSec-ACI and SXP

TrustSec-ACI integration requires a dedicated SXP node (PSN with SXP persona). To debug any propagation related issues of EPGs and EPs into 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



○	prrt-JNI	INFO	prrt policy decision request processing layer related messages
○	pxgrid	INFO	pxGrid messages
○	Replication-Deployment	INFO	Logger related to Deployment Registeration,Deregistration,Sync and...
○	Replication-JGroup	WARN	Logger related to JGroup Node State
○	ReplicationTracker	DEBUG	PSC replication related debug messages
○	report	INFO	Debug reports on M&T nodes
○	RuleEngine-Attributes	INFO	Additional rule evaluation attributes in audit logging at DEBUG
○	RuleEngine-Policy-IDGroups	INFO	Additional policy vs id group audit logging at DEBUG
○	runtime-AAA	WARN	AAA runtime messages (prrt)
○	runtime-config	WARN	AAA runtime configuration messages (prrt)
○	runtime-logging	WARN	customer logs center messages (prrt)
○	saml	INFO	SAML messages
○	scep	INFO	SCEP log messages
○	sgtbinding	INFO	SGT binding
○	sponsorportal	INFO	Sponsor portal debug messages
○	swiss	INFO	Swiss protocol internal messages
●	sxp	DEBUG	SXP Listener messages
○	TC-NAC	INFO	TC-NAC log messages
○	va-runtime	INFO	Vulnerability Assessment Runtime messages

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

To debug the issue of communication between the ISE and APIC-DC controller, look in the ise-psc.logs on the PAN.