Cisco APIC and Cisco ISE Integration

Revised: August 8, 2024

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Cisco APIC Release Version	Feature
6.1(1)	Support for Cisco APIC and Cisco ISE integration.

Overview of the Cisco APIC-ISE Integration

Cisco employs various controllers to manage policy, including the Application Policy Infrastructure Controller (APIC) in the Data Center and the Cisco Identity Services Engine (ISE) in campus and enterprise environments. Traditionally, these controllers operate independently, functioning as isolated systems. Both Cisco APIC and Cisco ISE facilitate the classification of devices, endpoints, and/or users into groups for policy enforcement, this classification criteria is referred to as *context*.

Integrating ISE with Cisco ACI provides a solution that allows Cisco ISE and APICs to communicate and share *context* information using Cisco pxGrid (Platform Exchange Grid). This integration enables the exchange of group information between Cisco APIC and ISE and is part of the Common Policy architecture, which supports the sharing of group context among various controllers connected to ISE as a central context exchange hub.

⚠

Attention Cisco ISE and Cisco APIC integration is an Early Field Testing (EFT/ Beta) feature. Our Beta features offer you an exclusive opportunity to explore and experiment with the latest functionalities prior to their General Availability (GA) release. We encourage you to take advantage of this early access to see what is on the horizon. However, please exercise caution when using these features, as they are still in Beta and may not represent the final version that will be included in the GA. Use Beta features in non-production environments and be aware that they are subject to change. Your understanding and acknowledgment of these conditions ensure a smoother experience as we refine our offerings.

Important terms used frequently in this document:

- Endpoint Group (EPG): is a logical entity containing a group of endpoints, belonging to the same Bridge Domain (BD), and sharing the same network and security policies. An EPG can belong to only one bridge domain.
- Endpoint Security Group (ESG): is a logical entity that contains a collection of physical or virtual network endpoints. An ESG is associated to a single VRF instance. ESGs allow you to define a security policy that spans across multiple bridge domains. With ESGs, you can group and apply policy to any number of endpoints across any number of BDs under a given VRF.
- Security Group Tag (SGT): is a unique 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.
- Trustsec: is a security architecture that uses SGTs for enforcing access control policies on the network.
- pxGrid: is an open and scalable IETF-approved standard that enables cross-platform network collaboration. Platforms can share or publish context as well as consume or subscribe to context from other platforms.
- Binding: SGTs, EPGs, and ESGs are distinct terminologies that serve the same purpose. They all classify an IP address associated with a user, device, or service into a specified group. The IP address to group association is referred to as a binding.
- Inbound SGT Domain Rules: are rules that are used to map SGT bindings with specific SGT domains.

- Outbound SGT Domain Rules: are rules that are used to assign SGT bindings to APIC as external EPGs.

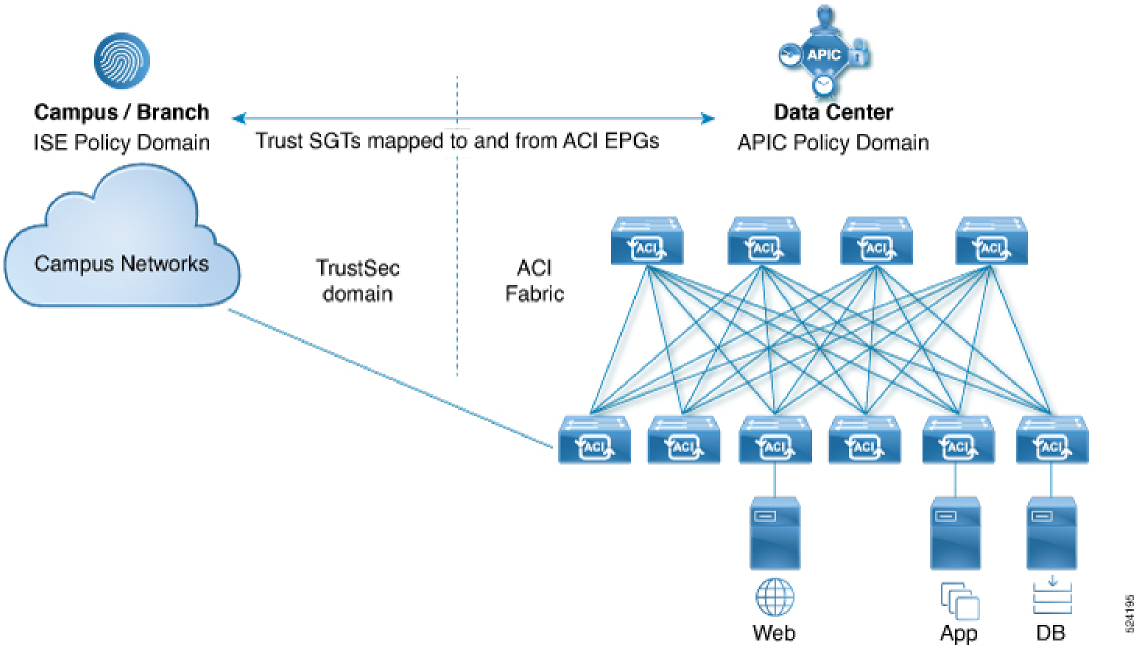
This document cannot be used alone. Refer to the Cisco ISE Administrator Guide, Release 3.4 which has relevant details, and configurations performed using Cisco ISE.

Integrating Cisco APIC with Cisco ISE

This document provides details of the Cisco APIC-ISE integration. In this integration, the ISE controller is responsible for managing the sharing of group context between domains. Configurations are performed from the ISE controller. Cisco APIC provides visibility into this integration from the Cisco APIC UI, including status of the integration connections and group and binding information for the groups being shared between the two domains.

The ISE integration supports Multi-Pod, multi-tenant, multi-VRF, and EPG/ESG context for APIC. You can set up a bi-directional connection to multiple ACI fabrics, including single pod and Multi-Pod fabrics, directly from ISE and start exchanging SGT/EPG/ESG context. The EPGs/ ESGs in ACI are normalized and stored in ISE as SGTs. This enables all the domain controllers that consume context from ISE, to configure policies for traffic from user/devices in the campus/branch to end-point groups in the data center. The SGTs in ISE are normalized and stored in ACI as external EPGs.

Figure 1: Cisco APIC and ISE Integration



ISE publishes the SGTs and bindings over the pxGrid channel to APIC. The SGTs and bindings are programmed as external EPGs (EEPGs) with subnet bindings allowing APIC to classify and apply policy on packets coming into the ACI fabric based on the group membership in ISE. Similarly, APIC publishes EPG and ESG group and endpoint information to ISE where it is translated to SGTs and bindings, allowing ISE to classify and apply policy on packets coming into the campus network from the ACI fabric.

Advantages of the Cisco APIC-ISE Integration

- Establishes context independently within each domain. The context is then normalized and stored as SGTs, allowing for sharing across different domains.

- Allows for consistent SGT-based policies for a simple, unified policy experience.
- Enforces consistent access policies between users, devices and application workloads.

Cisco APIC-ISE Terminology

Cisco APIC	Cisco ISE
End Point Group (EPG)/ End Point Security Group (ESG)	Security Group Tag (SGT)
IP-EPG Bindings	IP-SGT Bindings
Contracts	TrustSec Policy

Guidelines and Limitations for the Cisco APIC-ISE Integration

- The VRF containing SGT associated L3Out must be in egress mode. Hence the restrictions with egress mode enforcement apply, including:
  - Intersite L3Out
  - IP-based-EPGs for micro segmentation
  - Direct Server Return (DSR) (Layer 4 - Layer 7 virtual IP under an EPG)
  - Location-based PBR
- ISE to ACI connection is established on one of the controllers of the APIC cluster. If the node with the ISE-ACI connection is down, takeover time by the other nodes of the cluster is around five minutes.
- Shared service is not supported. Shared services configuration enables communication between EPGs across different VRFs within an ACI Fabric.
- One SGT is associated to one ISE-ACI connection. No support for the same SGT from multiple ISE-ACI connections.
- Configuration rollback is not supported. If you try to perform a rollback, there are chances of configuration discrepancies between ISE and ACI and you may need to remove and/or re-apply the configurations in ISE to keep ISE and ACI in sync.

For a list of open issues relevant to the Cisco APIC-ISE integration, see the Cisco APIC Release Notes, Release 6.1(1).

Supported Scale Numbers for the Cisco APIC-ISE Integration

Parameter	Scale
Number of ACI Tenants per ACI fabric	10
Number of ACI VRFs per ACI fabric	50
Number of ACI fabrics per ISE cluster	10
Number of ISE connections to the same ACI fabric	3
Number of EPGs/ESGs published from 1 ACI fabric to 1 ISE cluster	500

Parameter	Scale
Number of EPs published from 1 ACI fabric to 1 ISE cluster	20,000
Number of EPs published from 1 ACI fabric to 2 ISE clusters	10,000
Number of EPs published from 1 ACI fabric to 3 ISE clusters	7,000
Number of SGTs published from 1 ISE cluster to 1 ACI fabric	500
Number of SGTs IP bindings published from 1 ISE cluster to 1 ACI fabric	64,000
Number of SGTs IP bindings published from 3 ISE clusters to 1 ACI fabric	64,000

Note SGT bindings serve as host prefixes for external EPGs.

Using Cisco APIC for Network Visiblity

ISE creates a connection to the APIC, establishes a pxGRID channel between ISE and APIC. The SGTs created in ISE are published as external EPGs in APIC.

Prerequisites to be completed on Cisco ISE:

- Enable pxGrid and SXP services in a standalone/deployment setup.
- Configure DNS so that ACI can recognize ISE and vice versa.
- Create an ACI connection, this is indicated as an object on APIC.

Prerequisites to be completed on Cisco APIC:

- Configure standard APIC parameters such as, tenants, VRFs, L3Out ports, contracts. Ensure that the VRFs are in Egress Policy Control Enforcement Direction.
- Configure application EPGs and/or ESGs.
- Configure a DNS server for ISE pxGrid devices.
- Configure a DNS server and ensure ISE FQDN is reachable from the APIC.

There are two locations on the APIC GUI where you can get ISE-configured details.

- Details from the Integrations tab
- Details from the Tenants tab

Details from the Integrations tab

Use the following procedure to get details of the ACI connection created in ISE.

Before you begin

On the ISE GUI, configure an ACI connection (example: `S1_ACI`). You can add multiple ACI connections on Cisco ISE.

Procedure

Step 1 Log in to the Cisco APIC GUI.

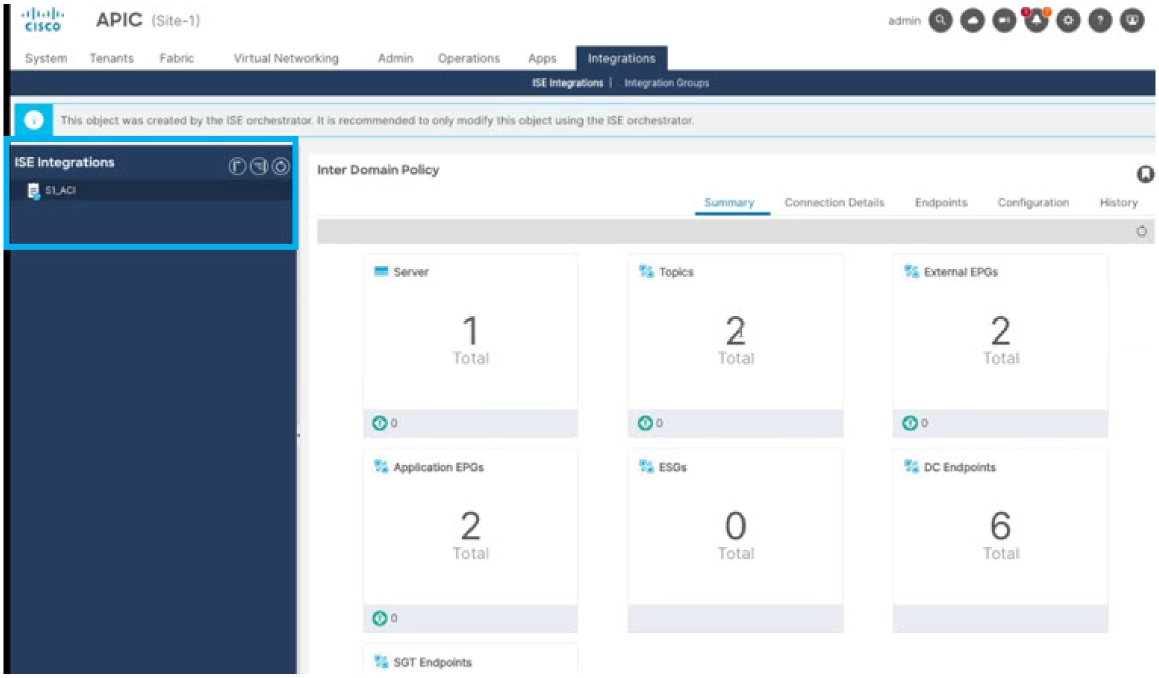
Step 2 Navigate to **Integrations** > **ISE Integrations**.

The Inter Domain Policy pane is displayed. The five tabs on the right hand side are: **Summary**, **Connection Details**, **Endpoints**, **Configuration**, **History**.

On the **ISE Integrations** pane, on the left, the connection created in ISE, `S1_ACI`, is displayed.

Step 3 Click each of these tabs to get relevant details.

Figure 2: Integrations tab



This object was created by the ISE orchestrator. It is recommended to only modify this object using the ISE orchestrator.

Details displayed in the **Summary** tab:

- Server: the number of ISE server(s).
- Topics: typically two topics – one for the published SGTs and the other for the subscribed EPGs.
- External EPGs: the number of SGTs published by ISE, which are denoted as external EPGs on APIC.
- Application EPGs: EPGs published by APIC towards ISE.
- ESGs: ESGs published by APIC towards ISE.
- DC endpoints: bindings published by APIC to ISE.
- SGT endpoints: bindings published by ISE to APIC.

Details displayed in the **Connections** tab:

- Name: connection created in ISE.
- Description: description of the connection.
- Admin state: the options are –
    - publish-and-listen: publish EPG/ESG bindings towards ISE and listen for ISE/pxgrid update for SGT binding updates.
    - listen: listen for ISE/pxgrid updates for SGT binding updates (no publishing towards ISE).
- Connection mode: is detected automatically by ISE, based on the APIC IP address configured in the ACI connection (inband or out-of-band).
- Connection Type: pxGrid connection.
- Username: user name used to create the connection.
- Servers: IP address of the ISE server, with domain name.
- Topics: the options are –
    - Publisher role: EPGs/ ESGs published by APIC to ISE.
    - Subscriber role: SGTs subscribed by APIC from ISE.

Details displayed in the **Endpoints** tab:

- SGT Endpoints sub-tab: bindings from ISE, with the SGT number. Click the row with the Binding details. A new window with the associated external EPG details is displayed.
- DC sub-tab: bindings published towards ISE, with tenant, EPG/ESG, VRF and IP address details.

Details displayed in the **Configuration** tab:

- Published EPGs/ ESGs sub-tab: the EPGs/ESGs that an ISE user selects to learn the corresponding IP bindings in ISE from ACI. For each EPG/ESG, the tenant, application profile, EPG/ESG names are displayed.

  Click the row with the tenant details to get the associated contracts.
- Subscribed SGTs sub-tab: the SGTs that an ISE user selects to publish the corresponding IP bindings from ISE to ACI. For each SGT, the tenant, L3Out and external EPG names are displayed.

Details displayed in the **History** tab:

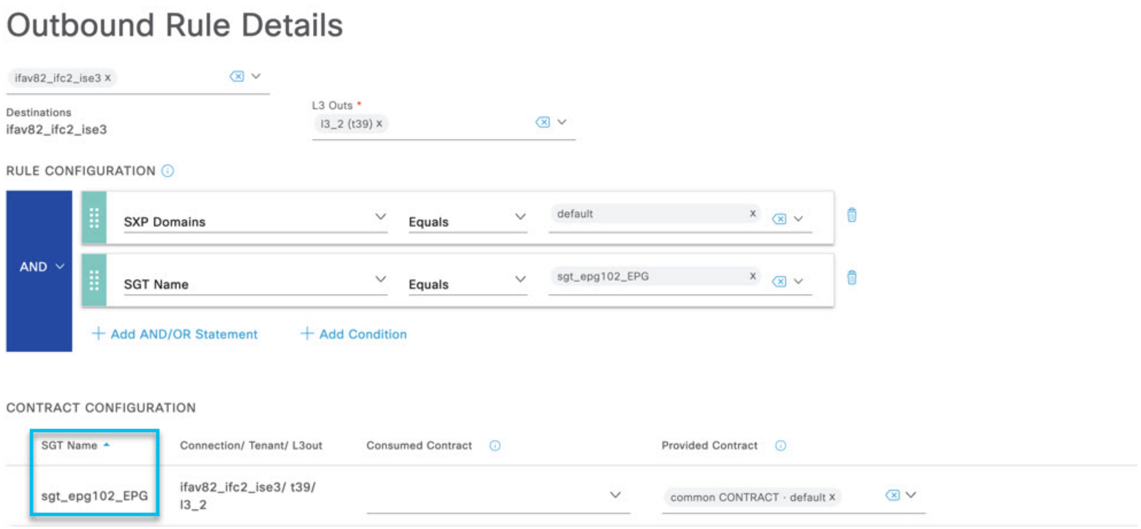
Displays standard event and audit logs.

Details from the Tenants tab

When ISE publishes the SGTs to APIC, the SGTs are configured as external EPGs under a tenant L3Out.

Use the following procedure to get details of the external EPGs (EEPG) created on APIC, based on the SGTs published by ISE. Figures 3 and 4 display the SGTs created on ISE which are available as EEPGs on APIC. The corresponding EEPG on APIC for the SGT created on ISE, `sgt_epg102_EPG`, is `ISE_SGT_1016`.

Figure 3: Outbound SGT domain rules configured on the ISE GUI



Outbound Rule Details

ifav82_ifc2_ise3

Destinations: ifav82_ifc2_ise3

L3 Outs *: l3_2 (t39)

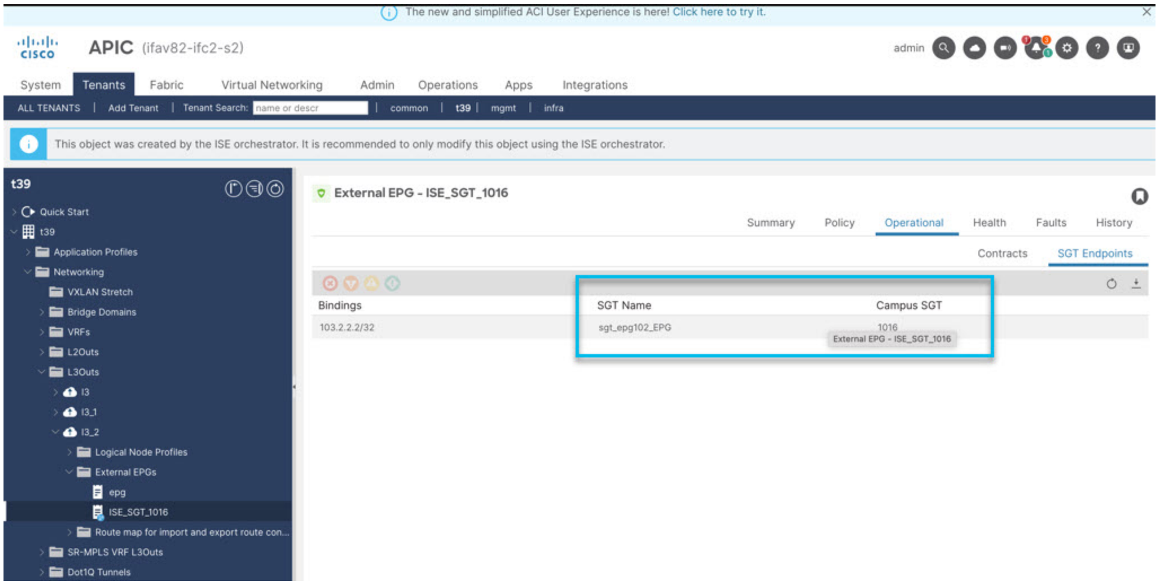
RULE CONFIGURATION

AND	SXP Domains	Equals	default
	SGT Name	Equals	sgt_epg102_EPG

CONTRACT CONFIGURATION

SGT Name	Connection/ Tenant/ L3out	Consumed Contract	Provided Contract
sgt_epg102_EPG	ifav82_ifc2_ise3/ t39/ l3_2		common CONTRACT · default

Figure 4: Mapping the SGT on ISE to EEPG on APIC



The new and simplified ACI User Experience is here! Click here to try it.

APIC (ifav82-ifc2-s2)

admin
System
Tenants
Fabric
Virtual Networking
Admin
Operations
Apps
Integrations
ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | t39 | mgmt | infra

This object was created by the ISE orchestrator. It is recommended to only modify this object using the ISE orchestrator.

External EPG - ISE_SGT_1016

Bindings	SGT Name	Campus SGT
103.2.2.2/32	sgt_epg102_EPG	1016

External EPG - ISE_SGT_1016

Procedure

Step 1 Log in to the Cisco APIC GUI.

Step 2 Navigate to **Tenants** > **Web-App** > **Networking** > **L3Outs** > **External EPGs**.

The outbound SGTs created on ISE are displayed here (APIC GUI) as external EPGs.

Step 3 Click an SGT displayed under the EEPGs to get details about it on the right side of the screen.

A banner is displayed at the top of the screen stating that the object was created using ISE and you can modify the object only using the ISE orchestrator.

Step 4 To check the bindings attached to the selected SGT, on the right side pane, click **Operational** > **SGT Endpoints**.

Note Subnet information is not available under **Policy** > **General**. To check the bindings information, check the path as mentioned above.

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

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

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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