



Cisco APIC and Cisco ISE Integration

New and Changed Information 2

Overview of the Cisco APIC-ISE integration 2

Integrating Cisco APIC with Cisco ISE 3

Using Cisco APIC for network visibility 5

Configure route leaking for shared services 10

Revised: July 14, 2025

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(3)	Modified GUI for enhanced user experience and ease of use.
6.1(2)	Support for shared services using route-leak across EPGs and support for microsegment (useg) EPGs.
6.1(1)	Support for Cisco APIC and Cisco ISE integration. Note Limited availability (Beta) feature for this release.

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.

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.

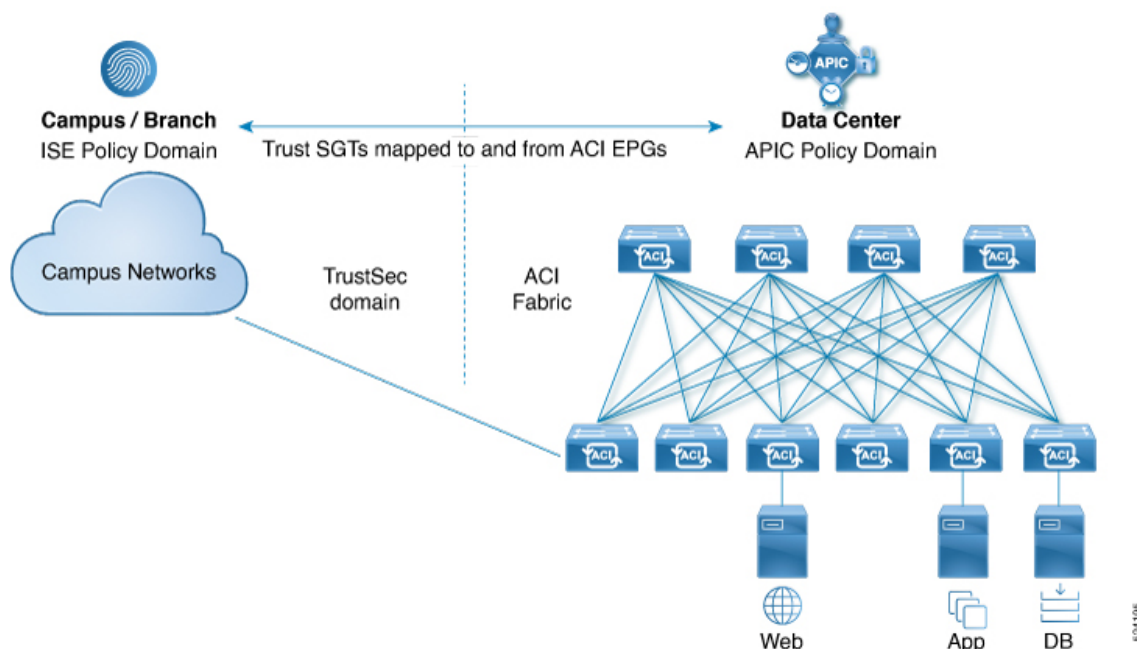
This document cannot be used alone. Refer to the [Cisco ISE Administrator Guide, Release 3.4](#) which has relevant details, and configurations performed using Cisco ISE.

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 (or 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 (or 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) or 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

Guidelines

- The supported ISE version is ISE 3.4P1.
- 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 services are supported between campus SGT to EPG or campus SGT to SGT.

Limitations

- The VRF containing SGT associated L3Out can be in ingress mode or egress mode.

VRFs containing L3Outs with SGT external EPGs (referred to as campus SGT L3Out in this document) can be configured in ingress or egress policy control enforcement direction.

Restrictions with ingress policy control enforcement direction:

- Intersite L3Out.
- Dynamic EPG classification (DEC) cannot co-exist with configurations in the same L3Out.
- EPGs need to be providers for shared service contracts.
- For pure non-border leaf to campus-border leaf traffic, policy is applied at the campus-border leaf node.
- One SGT is associated to one ISE-ACI connection. One SGT to multiple ISE-ACI connections is not supported. As multiple ISE connections are programming SGTs in ACI, each ISE connection must configure a unique SGT name when programmed under the same L3Out.
- A few seconds of traffic loss may be seen for prefixes learned on a campus SGT L3Out when the first SGT (external EPG) is configured by ISE.
- 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.

Supported scale numbers for the Cisco APIC-ISE integration

Parameter	Scale
ACI Sites or ACI Clusters	75

Parameter	Scale
Minimum number of ISE connections per ACI fabric	3
Tenants per ACI fabric	10
VRFs per ACI fabric	50
Maximum L3Outs per ACI fabric	500
Maximum SGTs Per L3Out	250
Maximum EPG/ESG Published from 1 ACI fabric to ISE	500
Maximum SGTs Subscribed from all ISEs by 1 ACI Fabric	500
Maximum SGTs – ISE	50000
Maximum Trustsec Matrix	10000
Maximum IPv4 and IPv6 Bindings Per ACI Fabric Per ISE Connection	32000
Maximum IPv4 and IPv6 Bindings for Solution	2 million
Maximum IPv4 Bindings Received by 1 ACI Fabric from all ISE Connections	64000
Maximum IPv6 Bindings Received by 1 ACI Fabric from all ISE Connections	64000
Maximum IPv4 and IPv6 Bindings Received by 1 ACI Fabric from all ISE Connections	64000



Note SGT bindings serve as host prefixes for external EPGs.

Using Cisco APIC for network visibility

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.

Complete these prerequisites 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.

Complete these prerequisites on Cisco APIC:

- Configure standard APIC configurations such as, tenants, VRFs, L3Out, contracts.
- 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.

- [Integrations tab](#)
- [Tenants tab](#)

Details from the Integrations tab

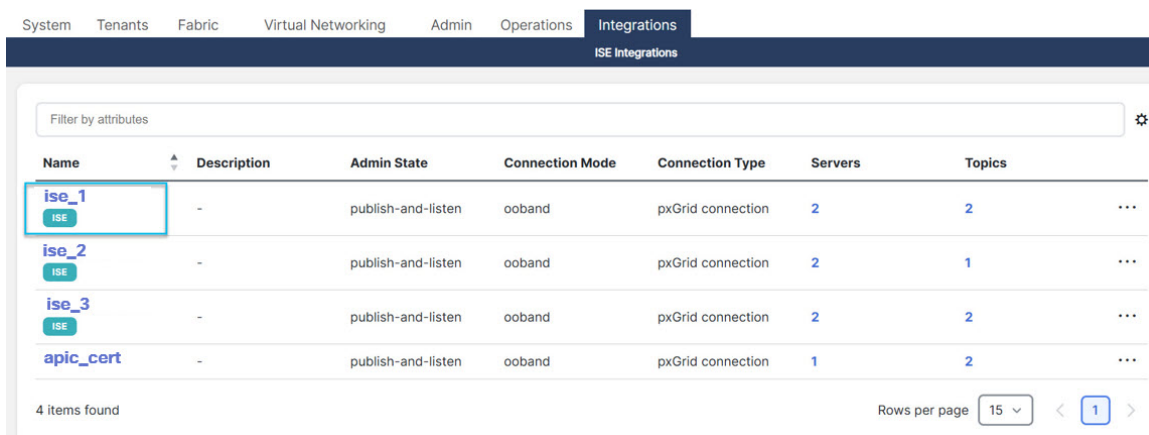
Use the following procedure to get details of the ACI connection created in ISE.

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 ACI-ISE connections are displayed.

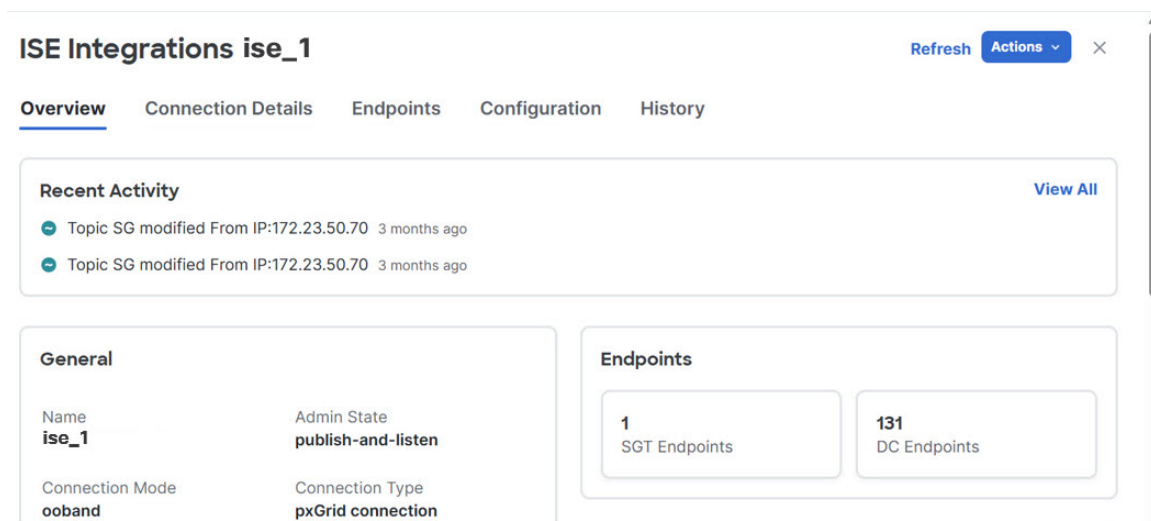


System Tenants Fabric Virtual Networking Admin Operations Integrations							
ISE Integrations							
Filter by attributes							
Name	Description	Admin State	Connection Mode	Connection Type	Servers	Topics	
ise_1 ISE	-	publish-and-listen	ooband	pxGrid connection	2	2	...
ise_2 ISE	-	publish-and-listen	ooband	pxGrid connection	2	1	...
ise_3 ISE	-	publish-and-listen	ooband	pxGrid connection	2	2	...
apic_cert	-	publish-and-listen	ooband	pxGrid connection	1	2	...

4 items found

Rows per page 15 < 1 >

- Step 3** Click a connection name to get more information about each connection.
- The details displayed for each connection are: Overview, Connection Details, Endpoints, Configuration, History.
- The details for each of these tabs are available as *clickable* tiles, such as General, Endpoints, etc. Click a tile to get a new pop-up screen that displays the details.



Details displayed in the **Overview** tab:

- Server: the number of ISE server(s).
- Topics: typically two topics – one for the published EPGs or ESGs, and the other for the subscribed SGTs.
- 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:

- DCs sub-tab: bindings published towards ISE, with tenant, EPG/ESG, VRF and IP address details.
- 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.

Details displayed in the **Configuration** tab:

The screenshot shows the 'ISE Integrations ise_1' interface with the 'Configuration' tab selected. Under the 'Published EPG/ESGs' sub-tab, a table lists various EPGs and ESGs. Each row includes the EPG/ESG name, tenant, application profile, contracts, and DC bindings, with 'View All' links for the last two columns. A filter bar and pagination controls are also visible.

EPG/ESG	Tenant	Application Profile	Contracts	DC Bindings
EP-1 EPG	tenant_1	AP-1	View All	View All
EP-2 EPG	tenant_2	AP-1	View All	View All
EPG_1 ESG	tenant_3	AEP	View All	View All
EP-1 EPG	tenant_4	AP-1	View All	View All
EP-2 EPG	tenant_5	AP-1	View All	View All
EP-3 EPG	tenant_6	AP-1	View All	View All

- 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. The EPGs and ESGs are clearly indicated with the words EPG in a green capsule and ESG in a blue capsule.
- 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, contract and external EPG names and SGT bindings are displayed. The details displayed under the Contracts and SGT Bindings columns are displayed as *clickable* links.

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 2: Outbound SGT domain rules configured on the ISE GUI

Outbound Rule Details

ifav82_ifc2_ise3 X

Destinations
ifav82_ifc2_ise3

L3 Outs
I3_2 (t39) X

RULE CONFIGURATION

AND

SXP Domains

Equals

default X

SGT Name

Equals

sgt_epg102_EPG X

+ Add AND/OR Statement

+ Add Condition

CONTRACT CONFIGURATION

SGT Name

Connection/ Tenant/ L3out

Consumed Contract

Provided Contract

sgt_epg102_EPG

ifav82_ifc2_ise3/ t39/
I3_2

common CONTRACT - default X

Figure 3: Mapping the SGT on ISE to EEPG on APIC

APIC (ifav82-ifc2-s2)

admin

System Tenants Fabric Virtual Networking Admin Operations Apps Integrations

ALL TENANTS Add Tenant Tenant Search: name or desc common t39 mgmt infra

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

t39

Quick Start

t39

Application Profiles

Networking

VXLAN Stretch

Bridge Domains

VRFs

L2Outs

L3Outs

I3

I3_1

I3_2

Logical Node Profiles

External EPGs

epg

ISE_SGT_1016

Route map for import and export route con...

SR-MPLS VRF L3Outs

Dot1Q Tunnels

External EPG - ISE_SGT_1016

Summary Policy Operational Health Faults History

Contracts SGT Endpoints

Bindings

103.2.2/32

SGT Name

Campus SGT

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.
-

Configure route leaking for shared services

The IP prefix is learned through the campus SGT L3Out; use this procedure to share it across VRFs.

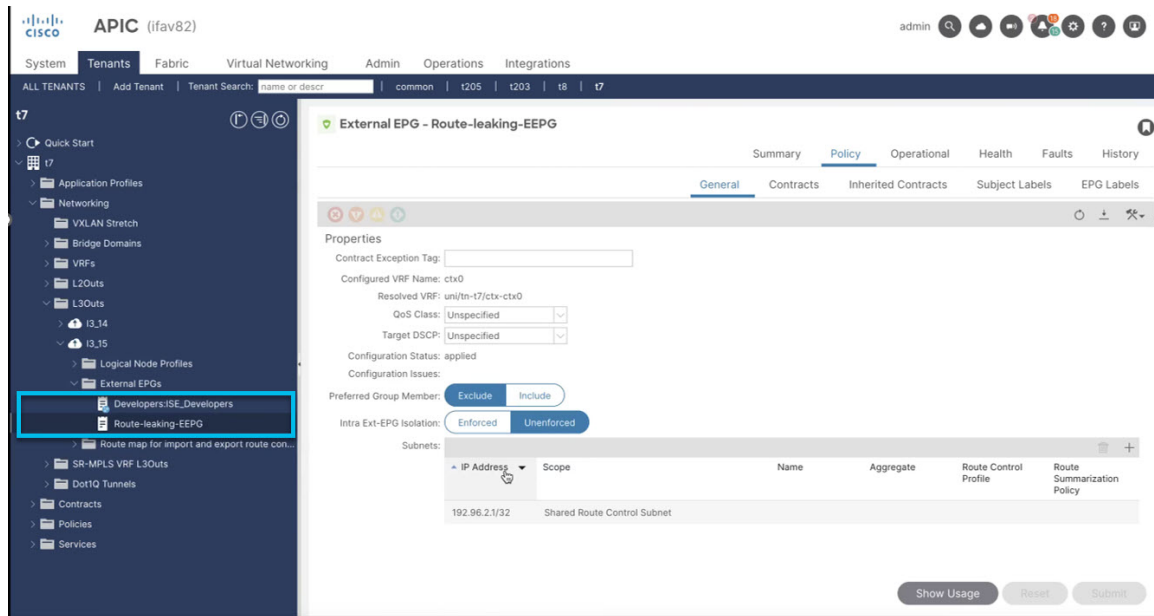
Before you begin

To support shared services between an SGT and an external EPG (or an AEPg) or shared services between an SGT to SGT, you need to configure route leaking across VRFs on APIC by configuring a route-leaking subnet. The policy-plane configuration is driven by ISE.

For route leaking, you need two external EPGs with the same shared contract:

- Configure an external EPG on APIC: set up an external EPG (e.g. Route-leaking-EEPG) on the APIC with the shared-route control flag enabled. Attach a shared contract to this external EPG to facilitate prefix leakage across the VRF.
- Integrate ISE with SGT: configure an SGT (e.g. ISE_Developers) on ISE. Deploy this SGT from ISE (SGTs from ISE appear as external EPGs on APIC) with the same shared contract attached, enabling the policy plane to allow or deny traffic based on the defined policies.

Figure 4: External EPGs on APIC

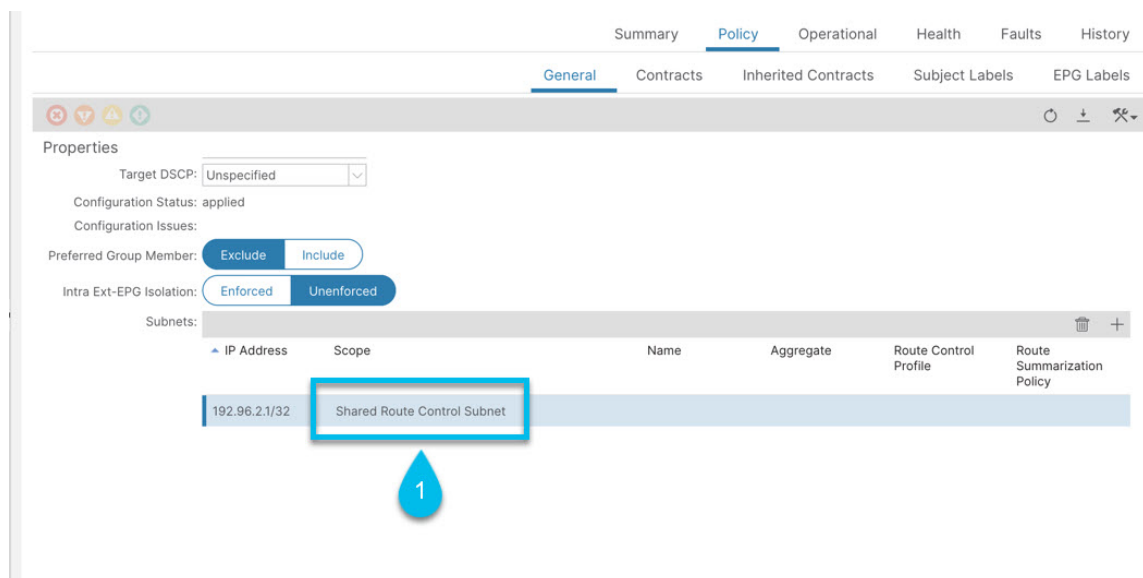


Note You can configure route-leaking external EPGs even with aggregate-shared control flag having aggregate-subnet or the default-subnet (0.0.0.0/0).

Procedure

- Step 1** On the Cisco APIC GUI, click the **Tenants** tab.
- Step 2** Navigate to **Networking** > **L3Outs** > **L3_out_name** > **External EPGs**. Right-click and select **Create External EPG**.
- Step 3** On the **Create External EPG** window that is displayed, enter the required details.
- Step 4** In the **Subnets** pane, click (+).
- Step 5** On the **Create Subnet** window that is displayed, enter the **IP address** and select the **Shared Route Control Subnet** check-box.
The subnet here is the IP prefix learned through the campus SGT L3Out.
- Step 6** Click **OK**, and then **Submit** (External EPG window).

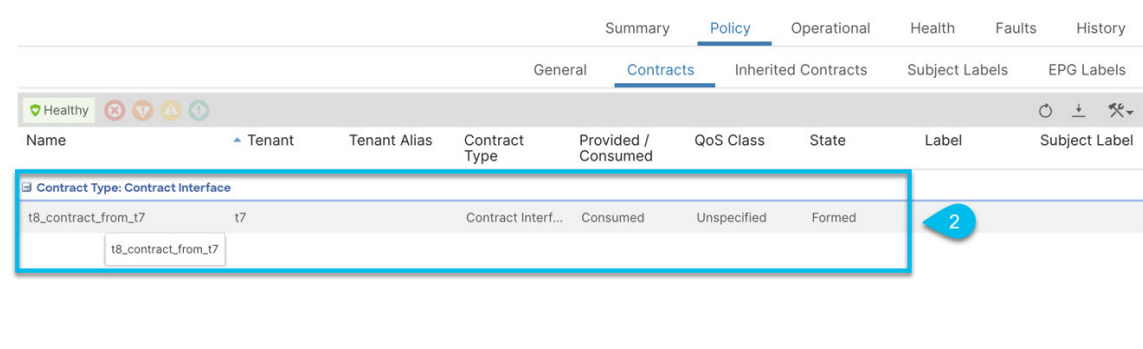
Figure 5: Subnet with the selected scope



Step 7 Click the created external EPG and select the **Policy > Contracts** tab.

Step 8 Click the **Actions** icon, and select a contract from the drop-down list.

Figure 6: Contract type



Step 9 (On the ISE GUI) Deploy the ISE SGT with the IP prefix and contract from ISE. Ensure to select the same shared contract as was defined for the external EPG on APIC.



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

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

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam, The Netherlands

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.