Revised: May 6, 2025

Connect Cisco Application Centric Infrastructure with Cisco ISE

Connect Cisco Application Centric Infrastructure with Cisco ISE

Cisco ISE enables you to create and enforce consistent access policies across multiple domains. Cisco ISE can share the SGTs and IP-SGT bindings with Cisco ACI and receive the Endpoint Group (EPG), Endpoint Security Group (ESG), and endpoint configuration information from Cisco ACI.

You can add multiple Cisco ACI connections to Cisco ISE. Each connection can be used to connect to different ACI fabrics. Cisco ISE can be integrated with individual and Multi-Pod Cisco ACI fabrics. Cisco ISE supports Cisco ACI Multi-Tenant and Multi-Virtual Routing and Forwarding (VRF) deployments.

You can configure rules to manage the learned context in Cisco ISE and to optimize the context flows between Cisco ISE and Cisco ACI.

Terminologies used in Cisco ISE and Cisco ACI integration

These terms are commonly used to describe Cisco ISE and Cisco ACI integration:

- EPG: Used in Cisco ACI. An EPG is a logical entity that contains a collection of endpoints. EPGs are associated to a single bridge domain and used to define security zones within a bridge domain.
- ESG: Used in Cisco ACI. An ESG is a logical entity that contains a collection of physical or virtual network endpoints. An ESG is associated to a single VRF instance instead of a bridge domain.
- Inbound SGT domain rules: Used in Cisco ISE to map incoming SGT bindings with specific SGT domains.
- Outbound SGT domain rules: Used in Cisco ISE to designate target destinations for specific SGT bindings.
- Workload classification rules: Used in Cisco ISE to assign primary and secondary SGTs to workloads.
- Secondary SGTs: SGTs that can be tagged along with primary SGT.

Note that the following terminology changes are made in Cisco ISE Release 3.4:

Cisco ISE Release 3.3 and earlier	Cisco ISE Release 3.4 and later
SXP mapping	SGT binding
SXP domain	SGT domain

Data synchronization between Cisco ISE and Cisco ACI

Cisco ISE supports packets coming from the Cisco ACI domain to the TrustSec domain by synchronizing EPGs and ESGs, and creating correlating SGTs in Cisco ISE. These SGTs map the endpoints configured in Cisco ACI and create correlating SGT bindings in Cisco ISE.

Cisco ACI supports the packets that are sent from the TrustSec domain to the Cisco ACI domain by synchronizing the SGTs and creating correlating EEPGs. Cisco ACI creates subnets under EEPG based on the SGT bindings from Cisco ISE. These subnets are deleted from Cisco ACI, when the corresponding SGT bindings are deleted in Cisco ISE.

When an EPG or ESG is deleted in Cisco ACI, the synced EPG list is updated in Cisco ISE. If the EPG or ESG is not used in any of the inbound or outbound SGT domain rules, then it is deleted in Cisco ISE. When an EPG or ESG is deleted, the IP-SGT bindings learned from that EPG or ESG are also deleted from Cisco ISE and the corresponding IP-SGT delete events are sent through the pxGrid SXP topics.

If the EPG or ESG is used in an inbound or outbound SGT domain rule, then it is not deleted. You must delete that EPG or ESG manually. Alarms are raised in both cases.

When an SGT is added to an outbound SGT domain rule in Cisco ISE, an EEPG is created in Cisco ACI. When the SGT is deleted from the outbound SGT domain rule, the corresponding EEPG is deleted in Cisco ACI.

Note

If two endpoints have the same IP address, the latest endpoint binding event overwrites the existing IP-SGT bindings learned from that ACI connection.

If the connection with the Cisco ACI server is lost, the connection status is marked as **Disconnected** in the **Workload Connections** page, and an alarm is raised. After the connection is reestablished, the connection status is marked as **Connected**. Cisco ISE resynchronizes the data when the connection is reestablished. Configuration drift checks are performed for all resources and an alarm is raised if any mismatch is found. Similar checks are performed whenever Cisco ISE is restarted or the Cisco ACI connection status changes from **Suspend** to **Connected**.

Compatibility matrix for Cisco ACI integration

The following versions are required for the new ACI connection workflow:

Product	Version
Cisco ISE	3.4.1 or later
Cisco ACI	6.1.1 or later
SD-WAN	20.12.2 (validated version)
Cisco Catalyst Center	2.3.7.7 or later
Cisco Firepower Management Center	7.2.5 (validated version)