Cisco Common Policy Integration Guide

January 14, 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

Document purpose and use

The purpose of this document is to outline the typical Common Policy deployment profile that Cisco Systems recommends. It provides guidelines for a typical deployment that includes the Catalyst Center for managing SD-Access networks, SD-WAN Manager for managing the SD-WAN fabric, Cisco Application Policy Infrastructure Controller (APIC) for managing Application Centric Infrastructure (ACI) data centers, and Cisco Secure Firewall Management Center (formerly Firepower Management Center) for managing Cisco Firepower platforms. This document's theoretical sections should be used in conjunction with its practical sections to help a deployment engineer understand the service requirements. The document will also help the deployment engineer make the best decisions for their network during deployment and configuration.

© 2026 Cisco and/or its affiliates. All rights reserved.

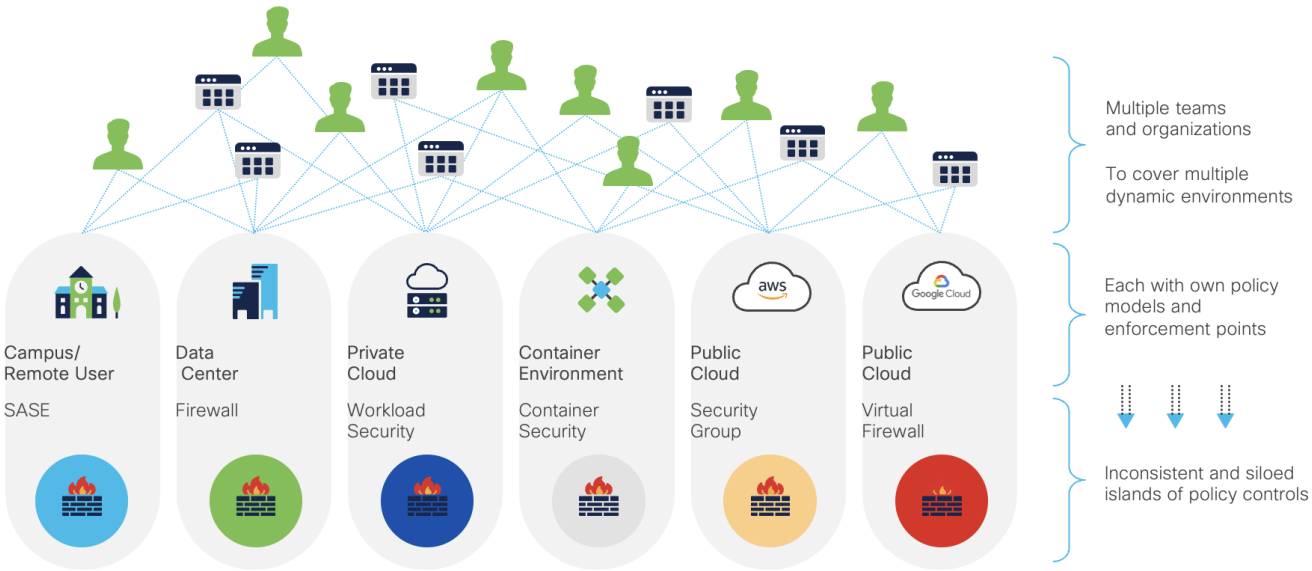
Target audience

The target audience for this Common Policy profile is the technical staff that is responsible for engineering and operating the network, as well as the implementation teams.

© 2026 Cisco and/or its affiliates. All rights reserved.

Introduction

The significant rise in hybrid workspace since the pandemic has led to the increase in remote and in-office workers accessing applications that are hosted in both the private data centers and in the public cloud. Moreover, many IoT devices are being connected to enterprise networks, further aggravating the complexity of securing user and device traffic. Applying consistent security policies across hybrid environments is complex and often inconsistent because each domain has its own policy models and enforcement points. For example, campus and remote users, data center, and workloads in private and public clouds can each have different policy enforcement points. The result is siloed islands of access policies.



The Common Policy Architecture addresses this concern by enabling contextual information about users, endpoints, and applications to be shared across domains. This gives IT Security administrators the ability to create and enforce consistent access policies at different enforcement points.

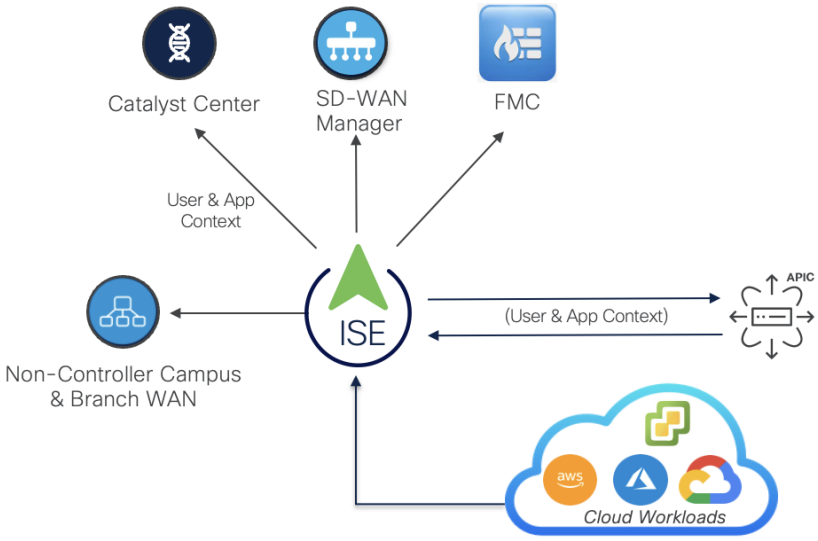
This guide describes the validated Common Policy solution, where Cisco Identity Services Engine (ISE) acts as the hub to normalize context information that can be shared and understood by each domain. In this solution testing, ISE is already integrated with various controllers such as Catalyst Center, SD-WAN Manager, and Cisco Secure Firewall Management Center (FMC). ISE is then connected with Application Centric Infrastructure (ACI) and cloud providers. Context information received from Cisco ACI is normalized as Security Group Tags (SGTs) on ISE and shared with ISE ecosystems. Campus SGTs shared with ACI are converted to External Endpoint Groups (EEPGs). Consumer and provider contracts can be applied to the EEPGs for policy enforcement in ACI. In addition, ISE can connect to AWS, Azure, GCP, and vCenter deployments, to download workload information and assign SGTs to the workloads. This solution testing validates the context exchange between domains and consistent policy enforcement applied to different enforcement points.

Common policy overview

Common Policy Framework enables consistent policy in a hybrid environment. In Common Policy, Cisco ISE acts as the hub to learn context information, normalize it, and share context with different domains. ISE forms a secure connection to ACI and AWS, Azure, GCP, and vCenter deployments through the workload connector.

© 2026 Cisco and/or its affiliates. All rights reserved.

Policy can then be applied to different enforcement points of the network, whether that be in the data center, campus, SD-WAN Edge, or Cisco Firepower.

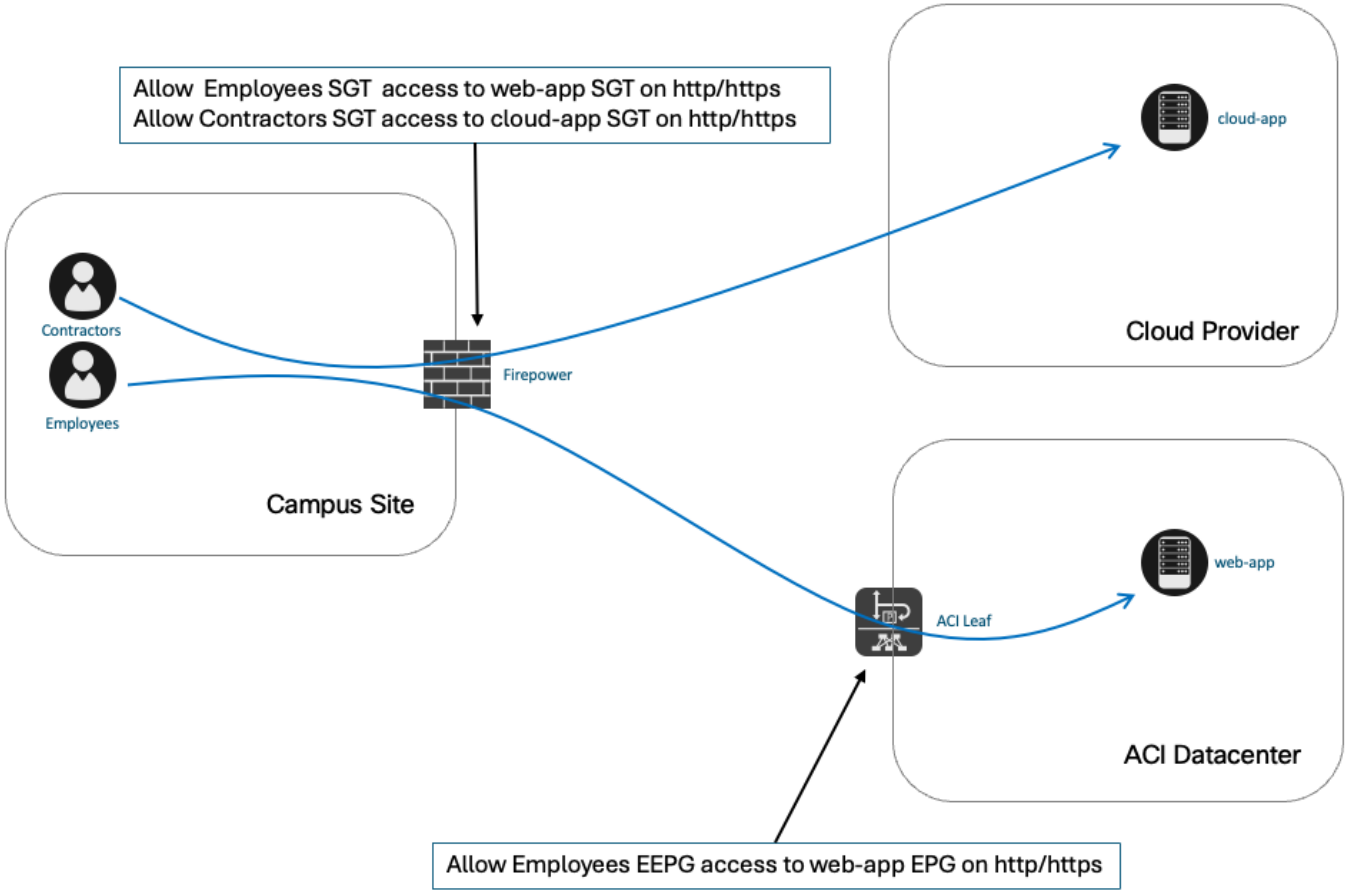


ISE 3.4 Patch 1 capabilities that enable the Common Policy Architecture include:

- ISE ACI Connector creates connections to Cisco APIC to discover endpoint groups (EPGs) and endpoint security groups (ESGs), then maps these to SGTs.
- ISE Cloud Connector creates connections to vCenter, AWS, Azure, and GCP deployments to learn the application workloads, virtual machines, and maps these to SGTs.
- ISE then communicates the context (IP to SGT bindings) to pxGrid destinations (Catalyst Center, SD-WAN Manager, Cisco FMC, APIC) or SXP devices so that a consistent policy can be enforced at different domain enforcement points.

© 2026 Cisco and/or its affiliates. All rights reserved.

Consider this use case demonstrating the flexibility of applying a policy at different enforcement points in the network.



The firewall at the campus site permits users classified as Employees connecting to the network to access the web application (classified as web-app SGT) in the data center. Also, the firewall only permits users classified as Contractors to access the cloud application (classified as 'cloud-app' SGT by a workload classification rule).

Additionally, APIC can have a policy applied to the ACI leaf switch to permit only Employees users (classified as Employees EEPG) to access the web-app EPG.

© 2026 Cisco and/or its affiliates. All rights reserved.

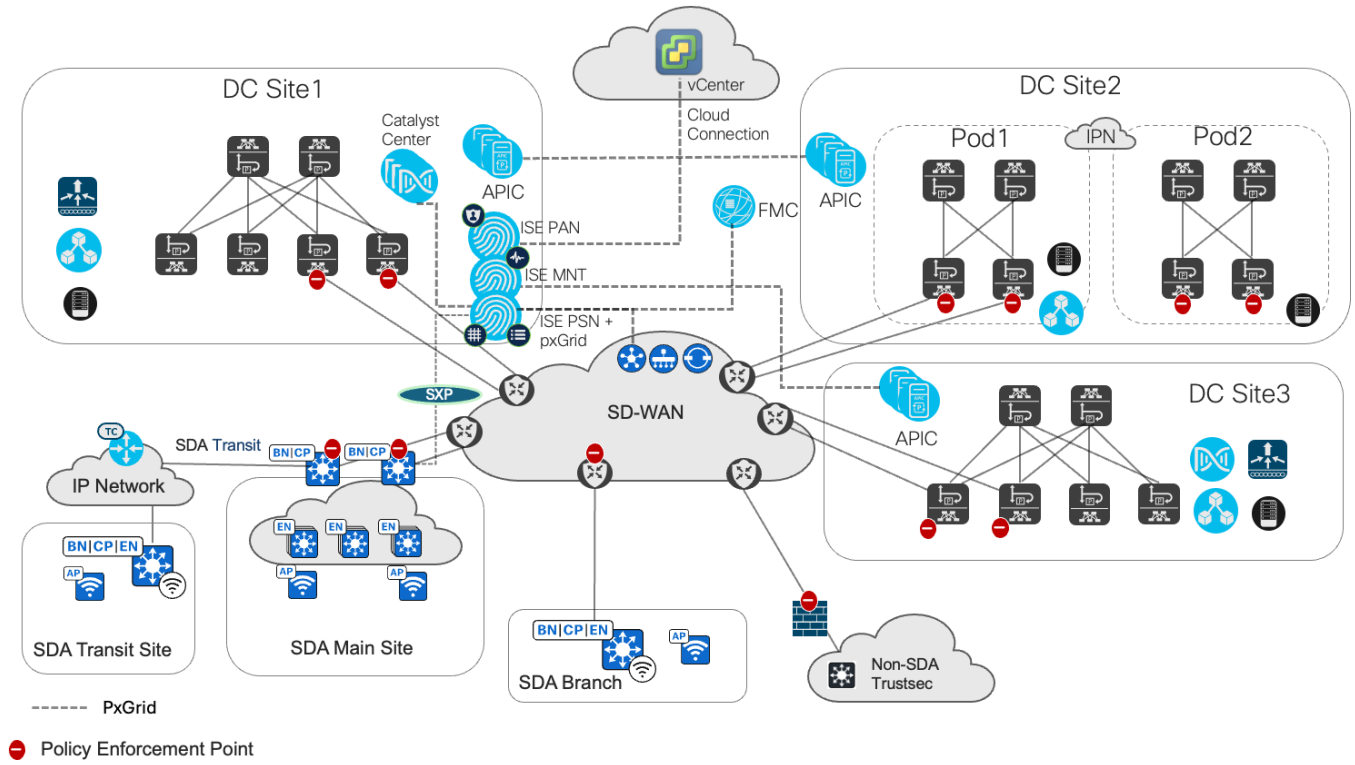
Hardware and software specifications

The solution is validated with the hardware and software listed in this table.

Role	Model name	Hardware platform	Software version	Software version
Catalyst Center Controller	DN2-HW-APL	Catalyst Center Appliance 3-Node Cluster	Cisco Catalyst Center 2.3.7.7	Catalyst Center 2.3.7.9
Identity Management, RADIUS Server	ISE-VM-K9 Cisco SNS-3600 Cisco SNS-3700	Cisco Identity Services Engine on Virtual Appliance and on Cisco SNS Appliance	Cisco Identity Services Engine 3.4 Patch 1	Cisco Identity Services Engine 3.4 Patch 1
Cisco SD-WAN	SD-WAN Manager	Cisco SD-WAN Manager	20.15.1	20.15.1
	C8300 C8500	Cisco Edge Services Router	17.9.5f, 17.12.4b, 17.15.1a	17.9.5f, 17.12.4b, 17.15.1a
Cisco Core and Distribution Node	C9500H C9600	Cisco Catalyst 9500 Series Switches Cisco Catalyst 9600 Series Switches	17.9.6a, 17.12.4, 17.15.1	17.9.6a, 17.12.5, 17.15.3
Cisco Access Node	C9300-48P C9300-24P	Cisco Catalyst 9300 Series Switches	17.9.6a, 17.12.4, 17.15.1	17.9.6a, 17.12.5, 17.15.3
Cisco Wireless Controller	C9800-40-K9	Cisco Catalyst 9800 Series Wireless Controller	17.9.6, 17.12.4, 17.15.1	17.9.6, 17.12.5,17.15.3
Cisco Access Points	9120-AXI 9130-AXI	Cisco Catalyst Access Points	17.9.6, 17.12.4, 17.15.1	17.9.6, 17.12.5,17.15.3
Cisco Firepower Threat Defense Security Appliances	FPR2110	Firepower 2100	7.2.5	7.2.5
Cisco Secure Firewall Management Center	FMCv	Cisco Firewall Management Center Virtual	7.2.5	7.2.5
Cisco APIC Controller	APIC-SERVER-M3	Cisco APIC Appliance	6.1.2	6.1.2
Cisco ACI Switches	N9K-C93240YC-FX2 N9K-C9332C	Cisco Nexus 9000 ACI-Mode Switches	16.1.2	6.1.2

© 2026 Cisco and/or its affiliates. All rights reserved.

Solution topology



The solution test bed used to validate the Common Policy solution consists of three ACI data centers, SD-Access sites, and TrustSec sites without SD-Access. The enforcement points are ACI Border Leafs, SD-Access Fabric Borders, SD-WAN Edge, and Cisco Firepower device.

The three ACI data centers have separate ACI fabrics and use the multi-fabric design through Layer 3-only connectivity across sites. Each ACI fabric is autonomous with unique IP subnets and establishes Layer 3 connectivity to other ACI fabrics through a Layer 3 Out (L3Out) data path.

Note: The L3Out can be deployed with border leafs in both pods in the multi-pod fabric.

The main campus site and branch campus sites are connected across the SD-WAN fabric. Data plane, control plane, and policy plane integration is achieved using eBGP, VRF-lite and inline SGT between SD-Access Border Node and SD-WAN Edge devices. The deployment procedure is based on Cisco SD-Access | SD-WAN Independent Domain Pairwise Integration Prescriptive Deployment Guide.

SXP is configured between ISE and the SD-Access Main site Border Nodes for each Virtual Network (VN). SGTs learned from the SXP subscription are propagated inline towards the SD-Access Fabric and the SD-WAN Edges to maintain consistent policy plane across SD-Access and SD-WAN fabrics.

© 2026 Cisco and/or its affiliates. All rights reserved.

Solution use cases

Category	Use case
ISE integrations	ISE and ACI integration
	ACI Multi-Tenant and Multi-VRF
	Context exchange between ACI fabrics
	ISE and Catalyst Center integration
	ISE and SD-WAN Manager integration
	ISE and Secure Firewall Management Center integration
Policy enforcement	Policy enforcement on ACI leaf switches
	Policy enforcement on SD-Access Border nodes
	Policy enforcement on SD-WAN Edge nodes
	Policy enforcement on Firepower appliances
Network robustness	Link failures
	Node failures
Day-*n* operations	Add, remove, and modify configurations
IPv6 scenarios	Context exchange for IPv6 bindings

© 2026 Cisco and/or its affiliates. All rights reserved.

Scale

This solution test verified the scale numbers listed in this table.

Table 1. Scale per ACI fabric

Parameter	Scale
ACI tenants	10
ACI VRFs	50
EPGs and ESGs	1000
Max number of IPv4 + IPv6 combined	64,000
Number of endpoints	32,000
Number of SGTs from ISE to L3Out as EEPG	500
Number of Mappings per EEPG	8000

ACI has limit of receiving maximum of 64,000 IP-SGT bindings from ISE. See Performance and Scaling Guide for Cisco Identity Services Engine for ISE scale information on:

- Cisco ISE and Cisco application centric infrastructure scaling
- Cisco ISE and workload connector scaling

© 2026 Cisco and/or its affiliates. All rights reserved.

ISE integrations

This section covers the ISE integrations to ACI and cloud providers with workload connectors and ISE integration with other domain controllers, Catalyst Center, SD-WAN Manager, and FMC.

Cisco ISE and ACI integration

Cisco ISE and ACI Integration is a part of the Common Policy architecture. To enable this integration, a secure connection is built between Cisco ISE and Cisco APIC. ISE imports the workload context, normalizes the context into SGTs, and shares the context with other domains to build consistent policies.

Cisco ISE and ACI Integration in Cisco ISE 3.4 Patch 1 and ACI release 6.1(2) supported features include:

- Multiple Cisco ACI fabrics, which can be individual or Multi-Pod
- Cisco ACI multi-tenant, multi-VRF, and multiple L3Outs
- Inter-VRF and shared L3Out
- Context sharing between different ACI fabrics
- ISE learns ACI contracts and allows the admin to choose existing contracts along with the shared SGTs (EEPGs)

ISE supports packets coming from the Cisco ACI domain to the TrustSec domain by synchronizing EPGs and ESGs to SGTs in Cisco ISE. The ACI endpoints associated with the EPGs and ESGs are mapped to corresponding IP-SGT bindings in Cisco ISE.

Cisco ACI supports packets coming from the TrustSec domain to Cisco ACI domain by synchronizing SGTs to EEPGs and creating endpoint bindings based on the received IP-SGT bindings.

ISE prerequisites:

- pxGrid and SXP services are enabled.
- DNS is configured to resolve APIC node hostnames.
- Delete the legacy ACI Integration if one exists.

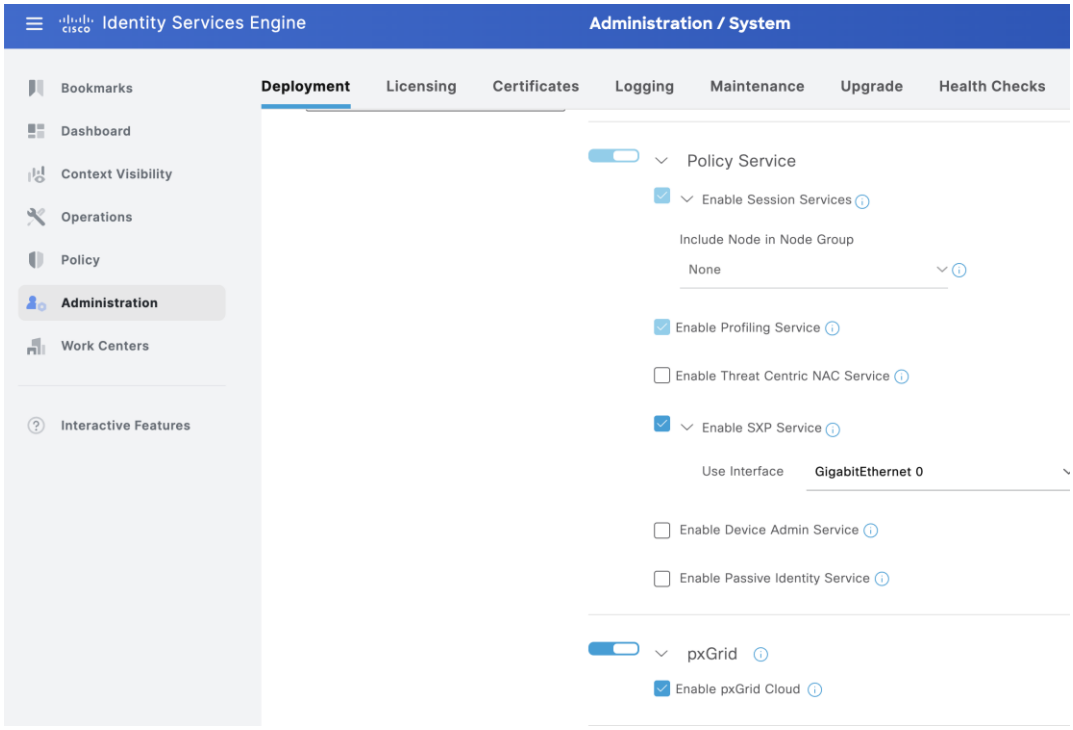
ACI prerequisites:

- Tenants, VRFs, application EPGs or ESGs, L3Outs, and contracts are already configured in APIC.
- DNS is configured to resolve ISE pxGrid hostnames.

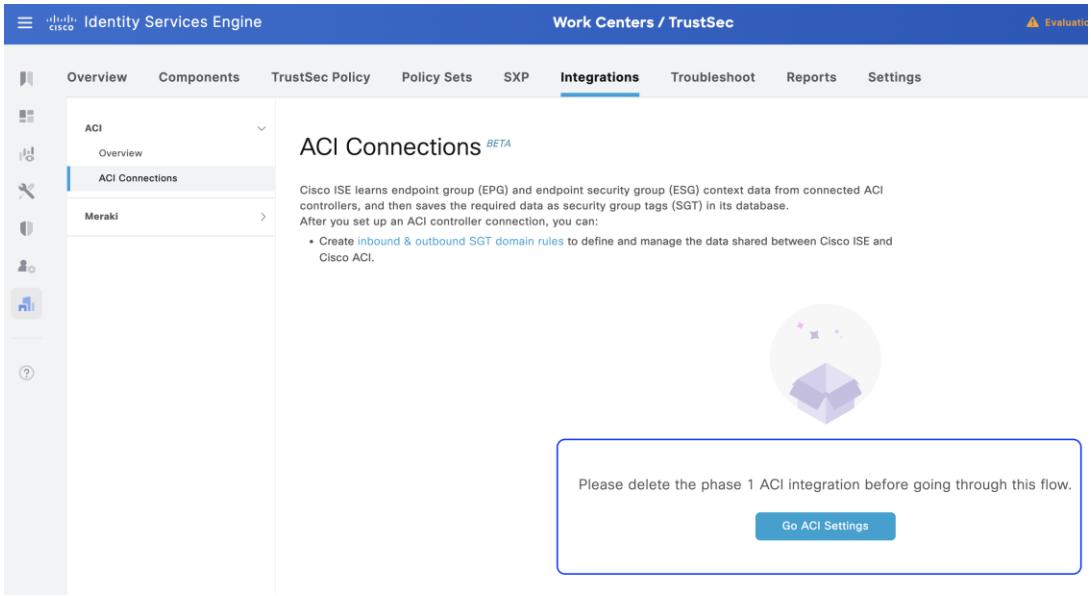
Procedure 1. To integrate Cisco ISE and ACI:

Step 1. Under **Administration > Deployment > Deployment Node**, choose **Enable SXP Service** and **Enable pxGrid Cloud**.

© 2026 Cisco and/or its affiliates. All rights reserved.

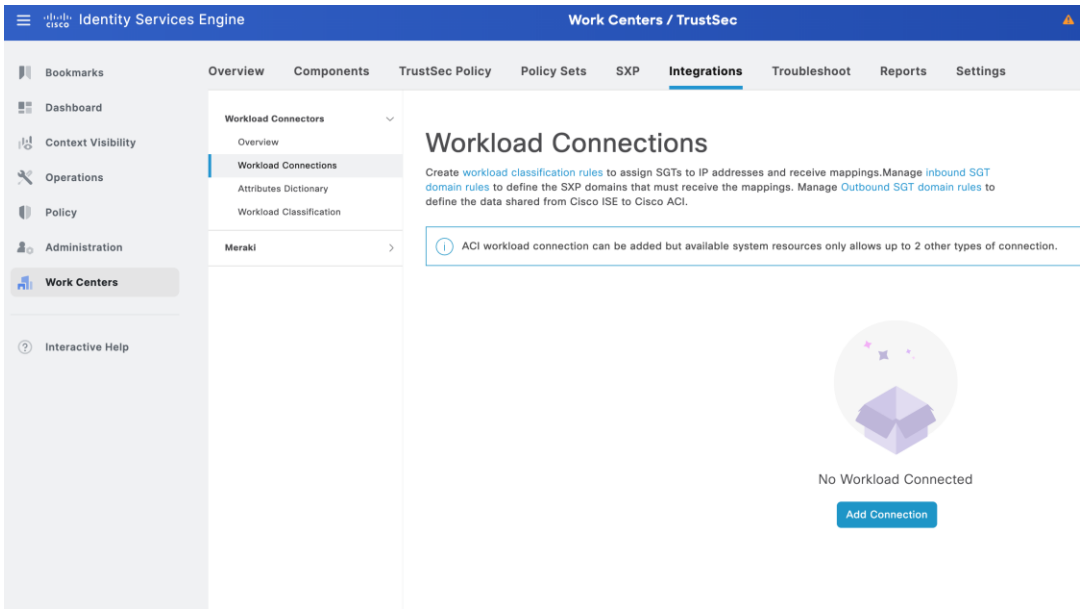


Step 2. Delete the legacy ACI Integration if one exists.

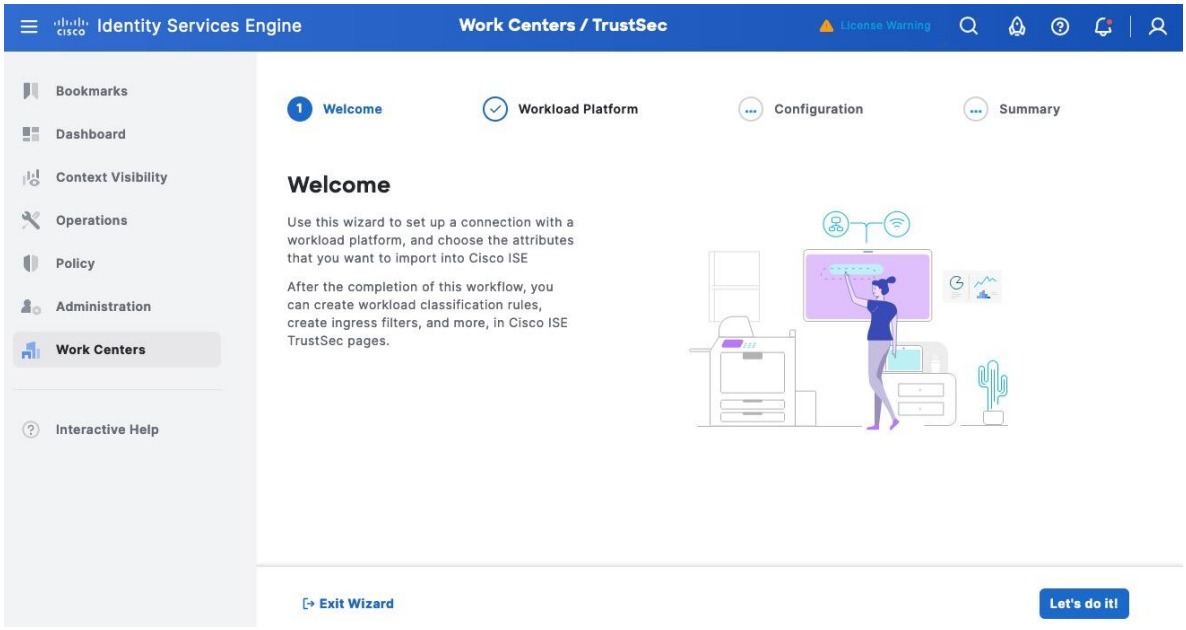


Step 3. Under **Work Centers > Workload Connections**, click **Add Connection**.

© 2026 Cisco and/or its affiliates. All rights reserved.

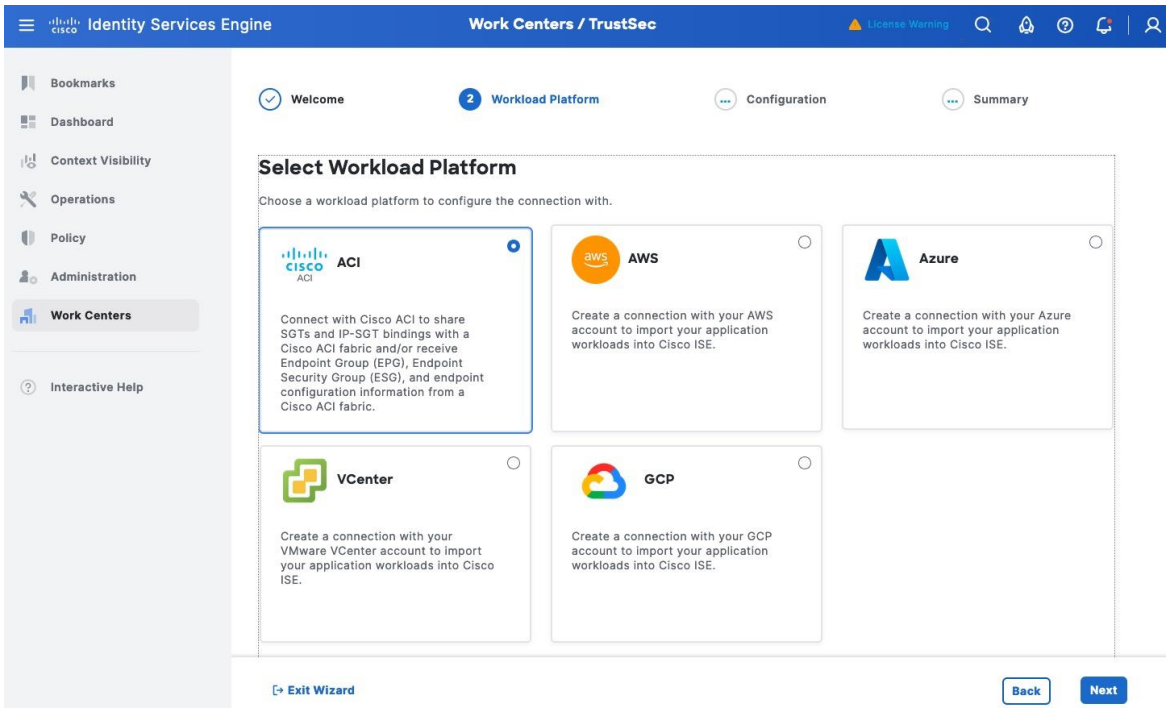


Step 4. In the **Welcome** window, under **Add Connection**, click **Let's Do it**.

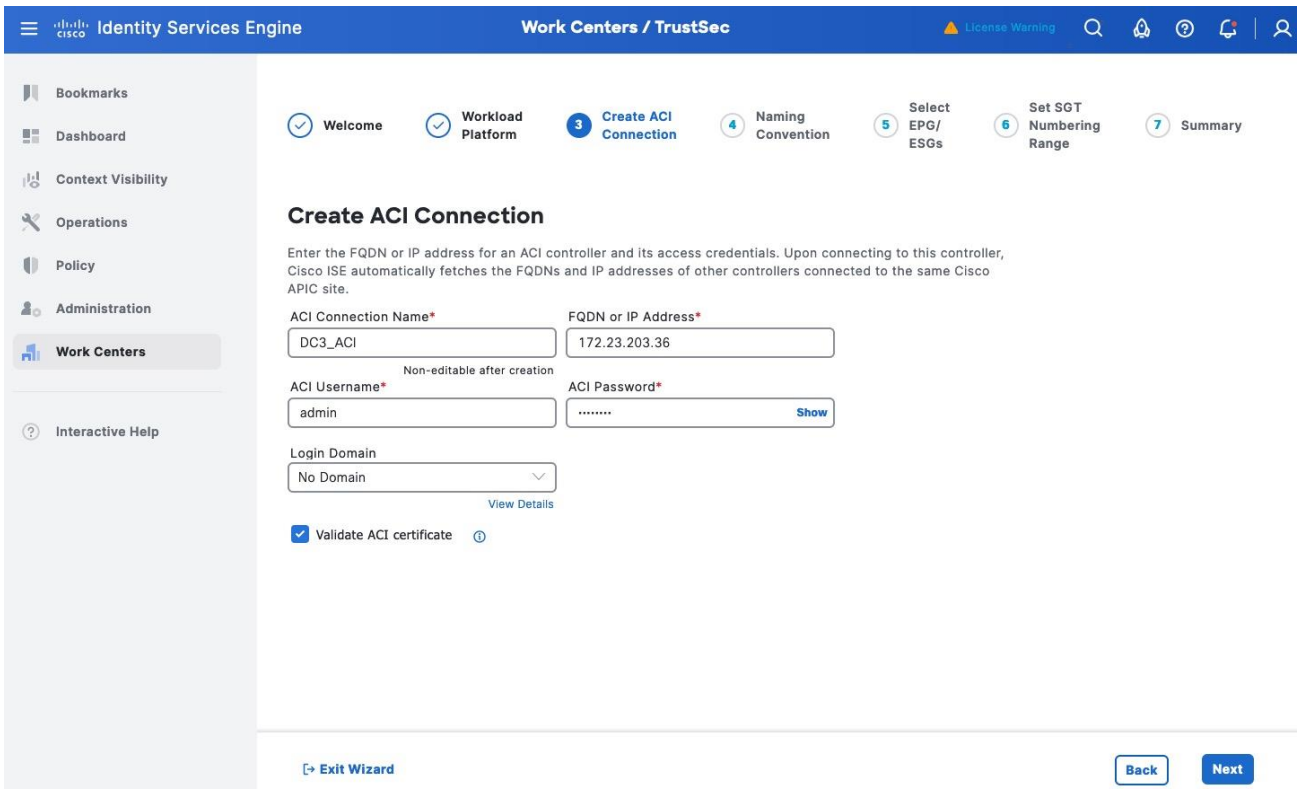


Step 5. Choose **Cisco ACI** as the Workload Platform.

© 2026 Cisco and/or its affiliates. All rights reserved.

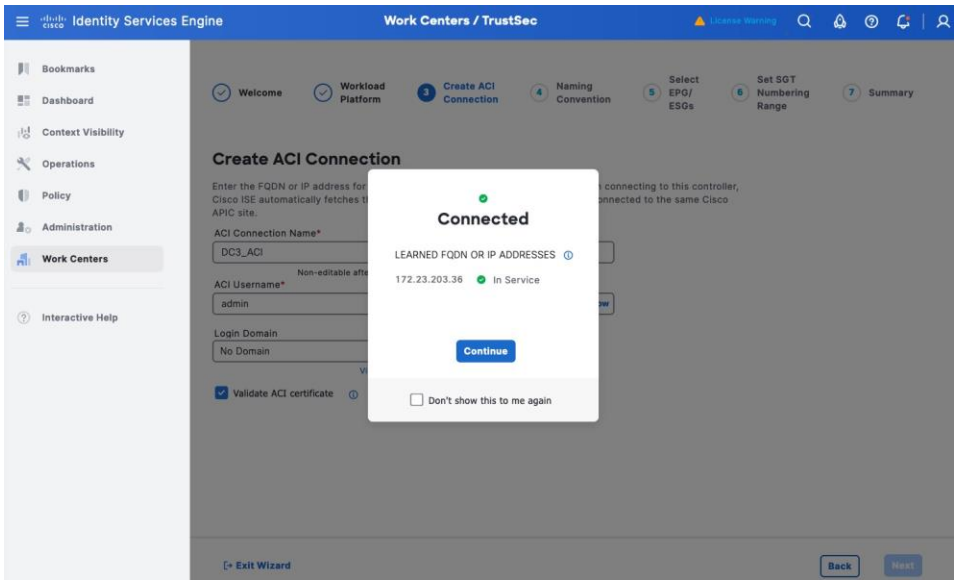


Step 6. Configure the ACI Connection.

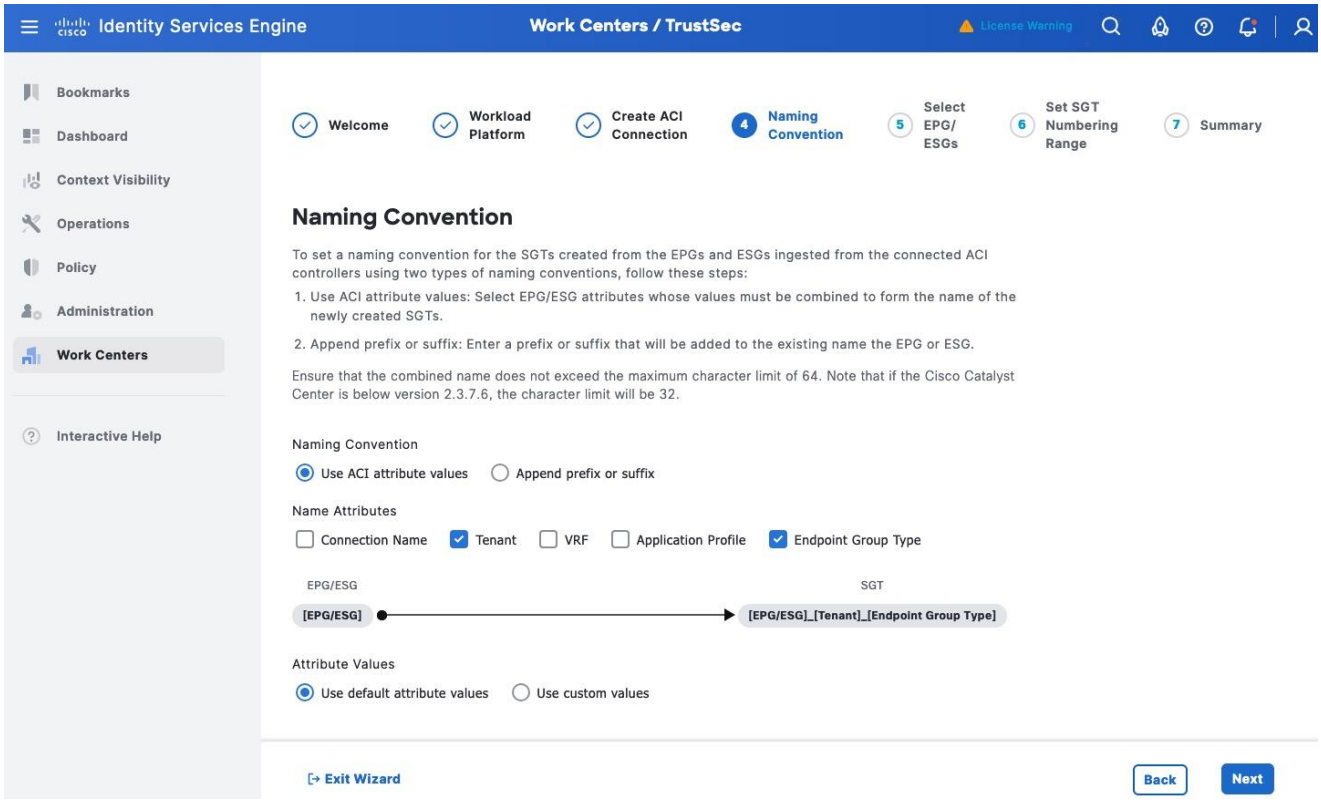


- If ACI certificate validation is required, check the **Validate ACI certificate** check box. The ACI Certificates need to be added to the certificate Trust Store in ISE.
- If the connection succeeds, a **Connected** status displays. Click **Continue**.

© 2026 Cisco and/or its affiliates. All rights reserved.

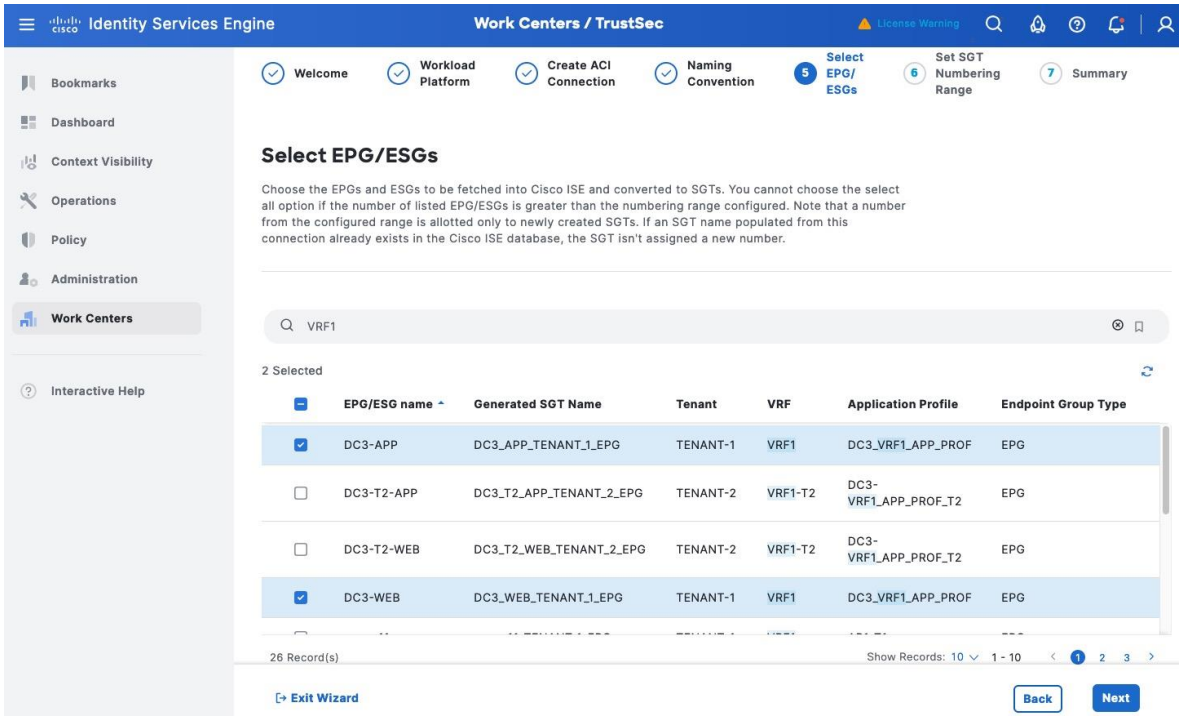


Step 7. Choose the naming convention for SGTs. The attributes can be based on the **Connection Name**, **Tenant**, **VRF**, **Application Profile**, and **Endpoint Group Type**.



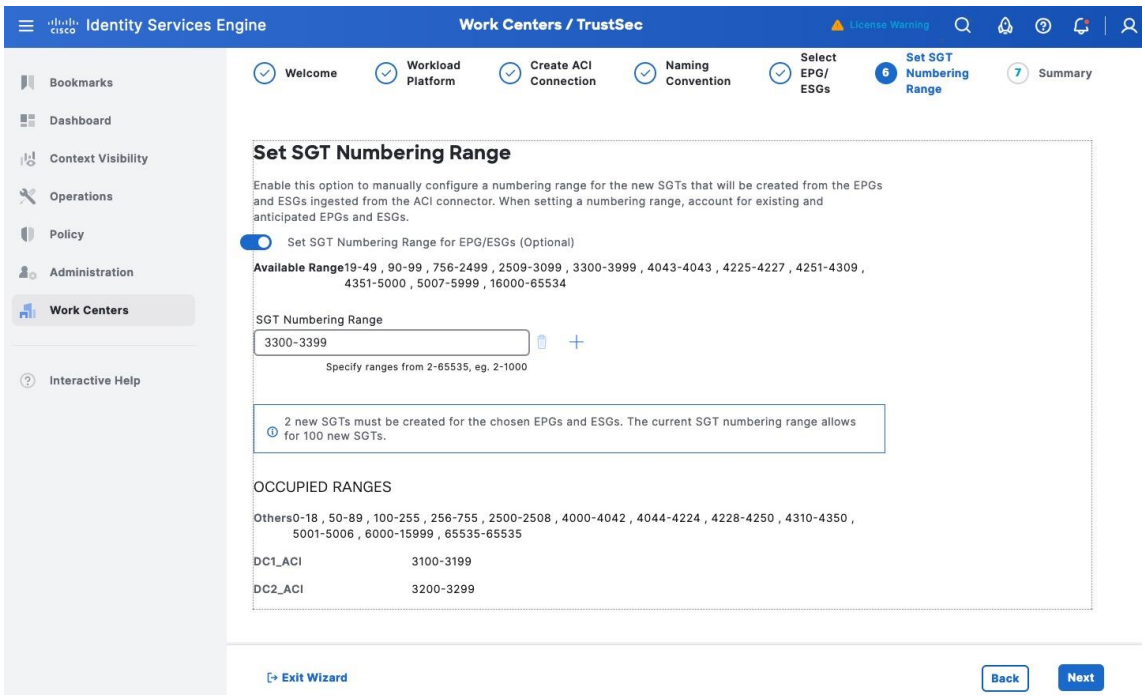
Step 8. Choose the EPGs and ESGs.

© 2026 Cisco and/or its affiliates. All rights reserved.



Note: The administrator can choose EPGs/ESGs and corresponding IP bindings from the ACI connection. If no EGPs/ESGs are chosen, the connection remains in the **suspended** state upon creation.

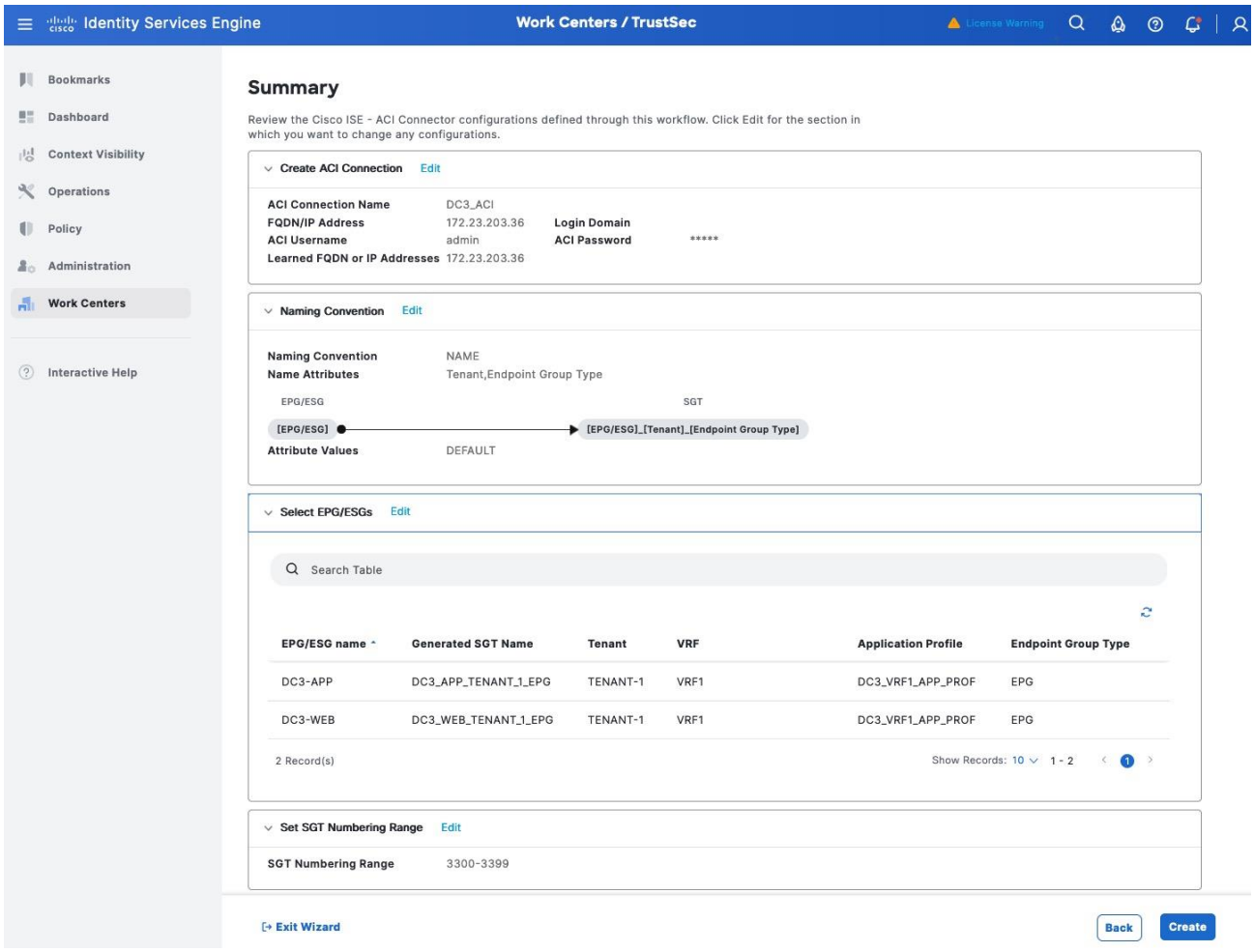
Step 9. (Optional) Reserve **SGT Numbering Ranges**.



Note: By default, all selected SGTs are automatically assigned with available SGT tags. This option is useful to assign specific SGTs to EPGs/ESGs learned from an ACI data center to identify them by a numbering range. For example, 3100s SGTs are coming from DC1, 3200s SGTs are sourced from DC2, and so on.

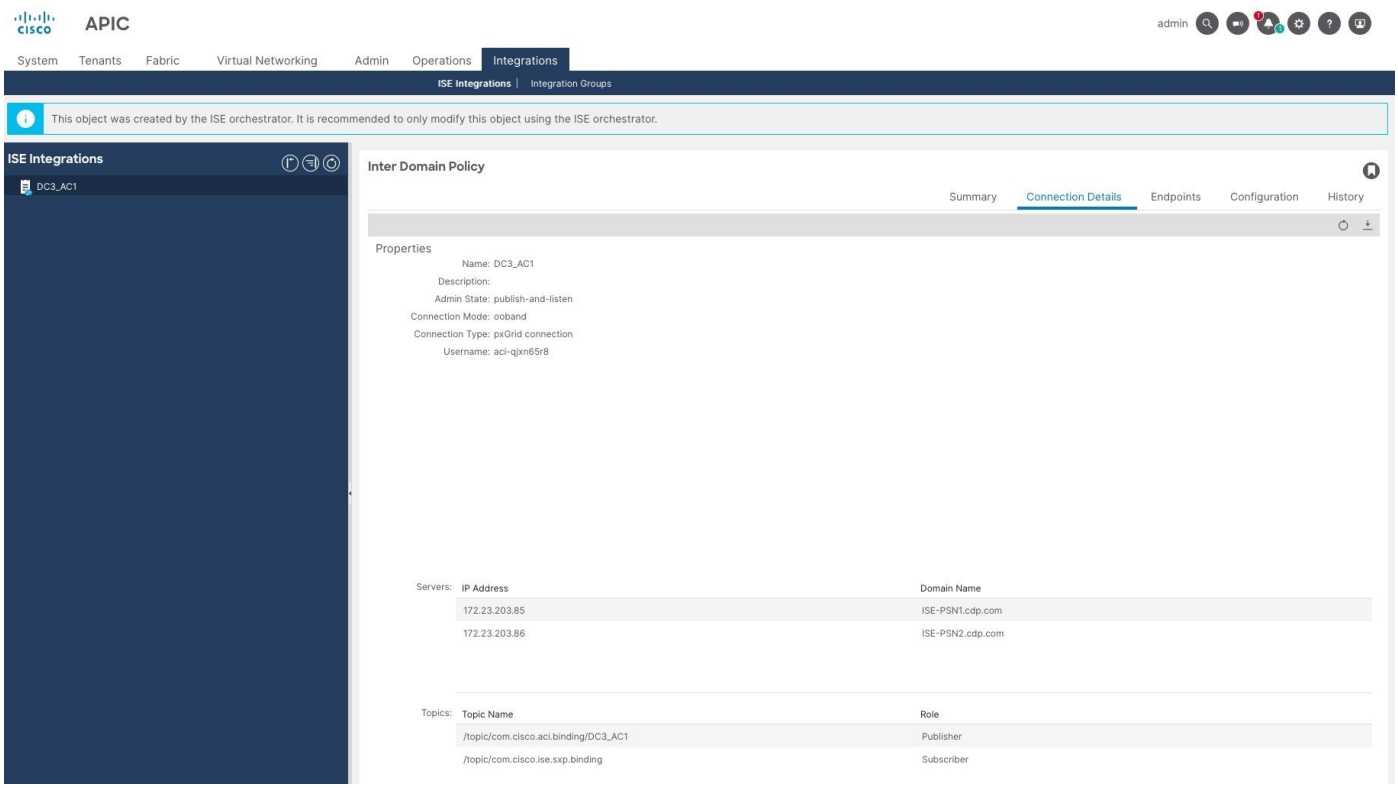
© 2026 Cisco and/or its affiliates. All rights reserved.

Step 10. Review the **Summary** window then click **Create** to make the connection.



Step 11. Verify the ISE integration in ACI. Verify that the ACI connection has been made in APIC under **Integrations > ISE Integrations**.

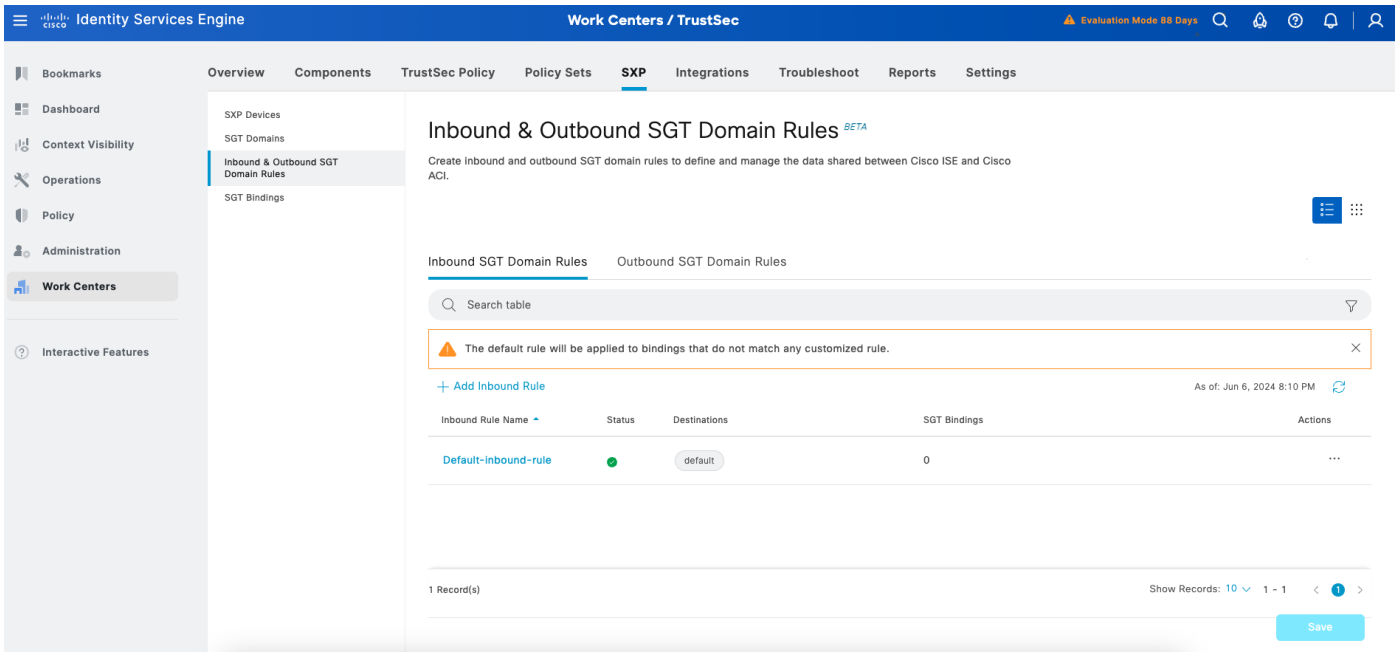
© 2026 Cisco and/or its affiliates. All rights reserved.



Define Inbound SGT domain rules and Outbound SGT domain rules

Inbound SGT domain rules

Inbound SGT domain rules allow the administrator to map incoming SGT bindings to specific SGT domains. If no Inbound SGT domain rule is defined, the bindings are sent to the Default SGT domain. The Default SGT domain is enabled automatically and cannot be disabled.



Outbound SGT domain rules

© 2026 Cisco and/or its affiliates. All rights reserved.

Outbound SGT domain rules define what data is shared from Cisco ISE to Cisco ACI.

Procedure 2. To define an Outbound SGT domain rule:

Step 1. Go to **Work Centers > Inbound & Outbound SGT Domain Rules > Outbound SGT Domain Rules** then click **+ Add Outbound Rule**.

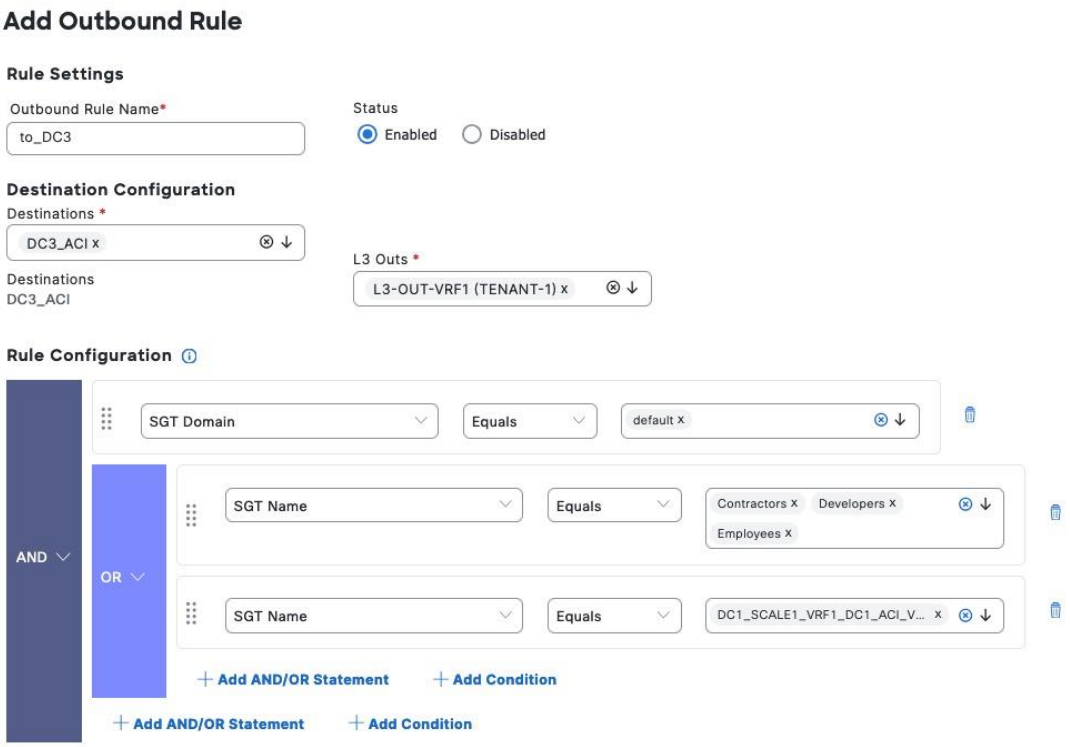
The administrator creates the Outbound SGT domain rule to define conditions for sharing IP bindings to ACI connections.

By default, ACI does not learn any context from ISE. Configure an outbound rule on ISE to determine which SGTs to share with the ACI connection. This is required for ACI to learn context from ISE.

Step 2. Enter an **Outbound Rule Name**.

Step 3. In the **Destinations** field, choose the ACI connection.

Step 4. Choose the **L3 Outs** that this rule will be applied to.



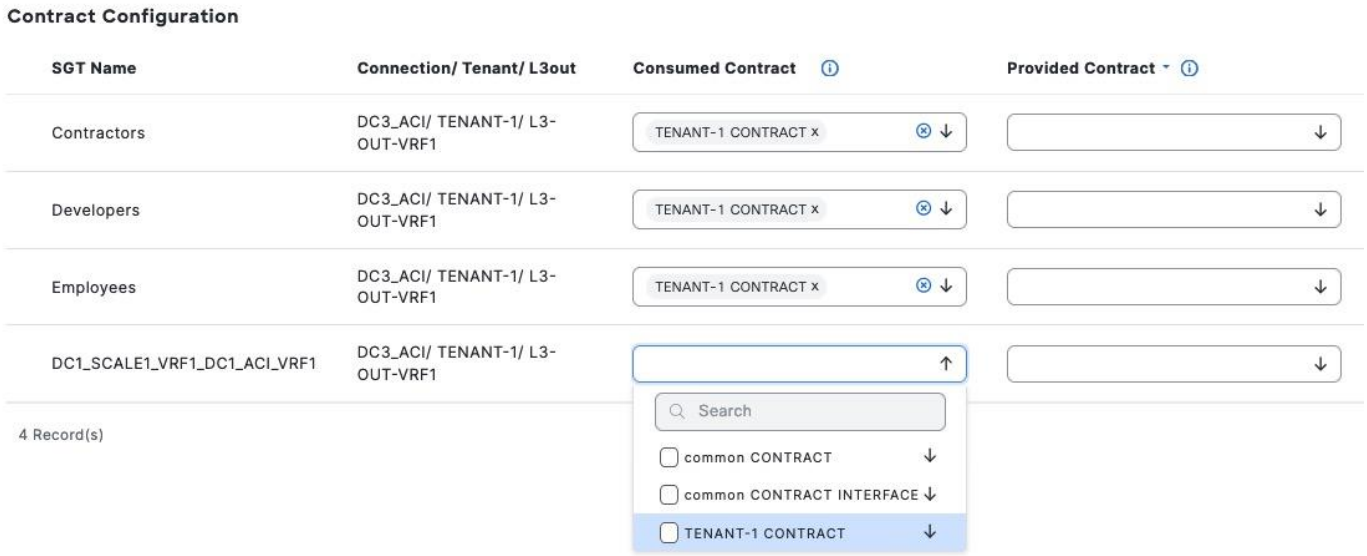
The **Rule Settings** define two conditions:

- SGTs from the default SGT domain.
- SGT names matching Contractors, Developers, Employees or DC1_SCALE_VRF1_DC1 (learned through DC1 ACI) will be propagated to this DC3 ACI connection.

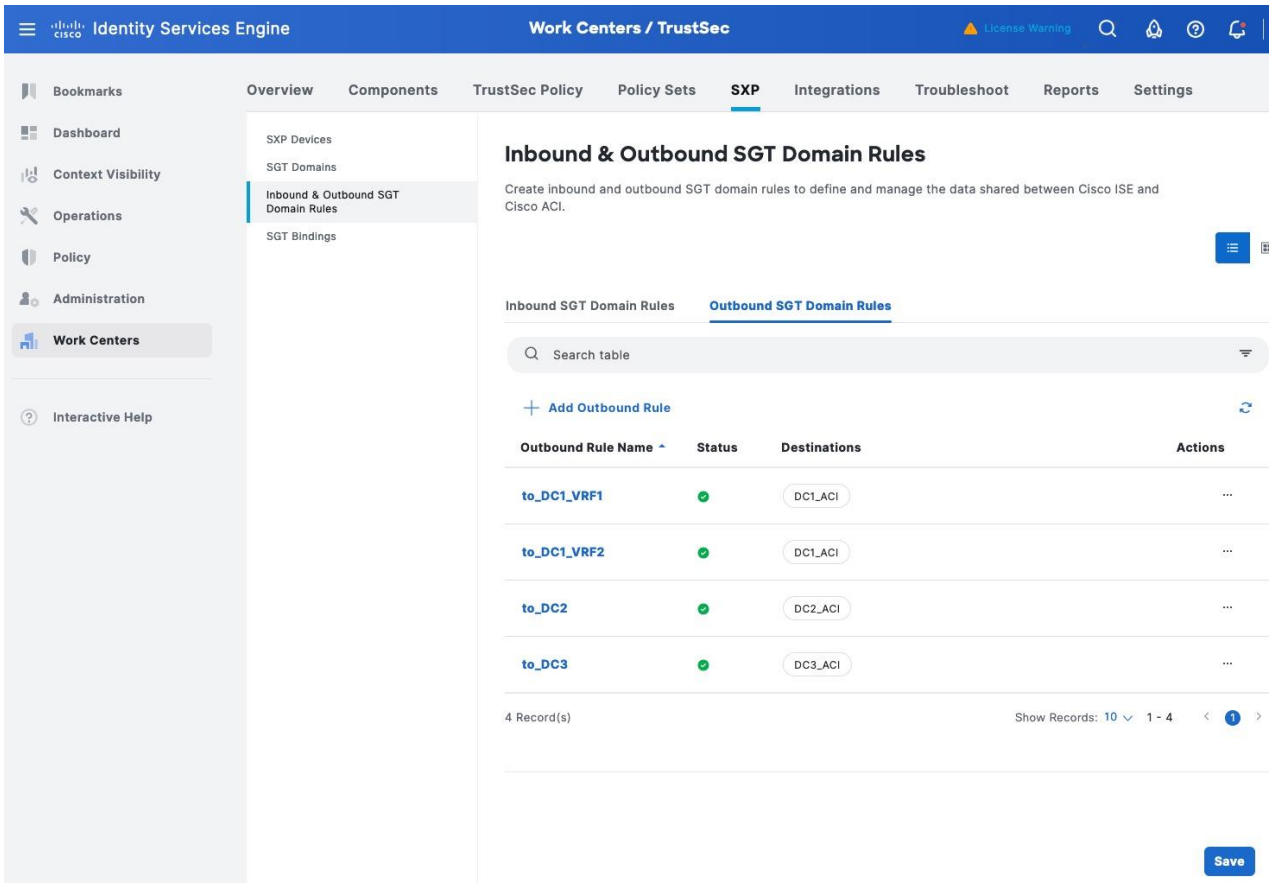
For each selected SGT, ISE pushes configurations to ACI to create an EEPG in the selected L3Out. After the conditions have been defined, an option to choose the contract configuration becomes available. ISE attaches provider and consumer contracts defined in the rule for the EEPG in ACI.

© 2026 Cisco and/or its affiliates. All rights reserved.

Below the **Rule Configuration** section, the administrator has the option to choose the **Consumed Contract** and **Provided Contract** to apply to the chosen SGTs. The chosen SGTs appear as EEPGs in ACI under the chosen L3Out. The contracts are applied to EEPGs.



Step 5. Click **Save** to submit the new outbound rule.



© 2026 Cisco and/or its affiliates. All rights reserved.

ISE to vCenter integration

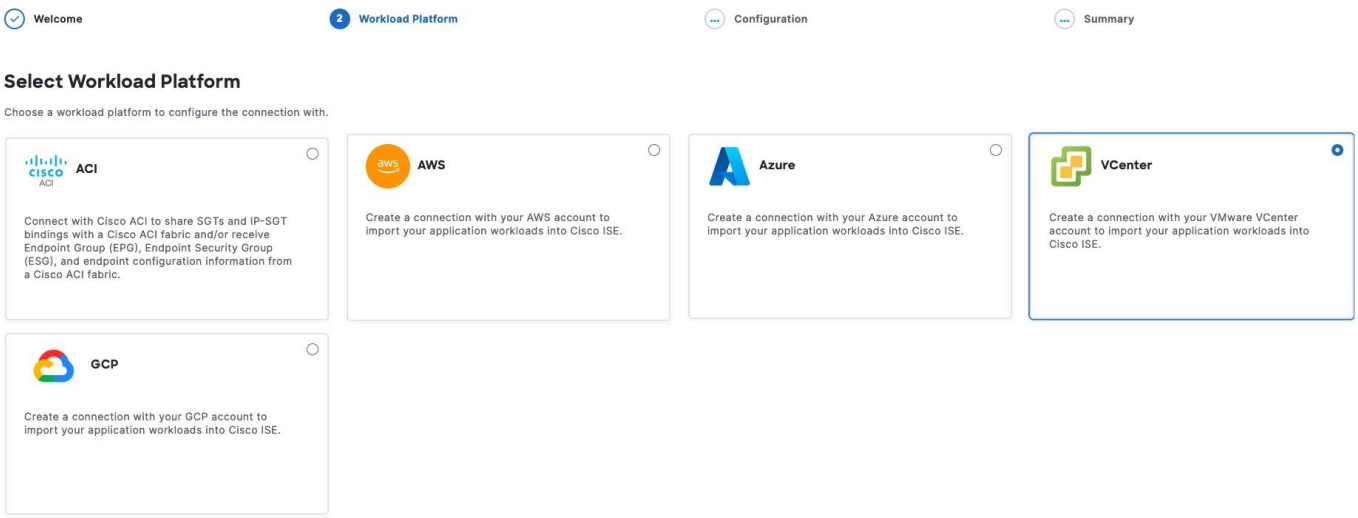
Besides creating the connection to ACI, the workload connector can also create connections to AWS, Azure, GCP, and vCenter deployments. Workload Connector configurations for AWS, Azure, and GCP deployments are similar.

Procedure 1. To use the workload connector to connect to the vCenter to learn-workloads:

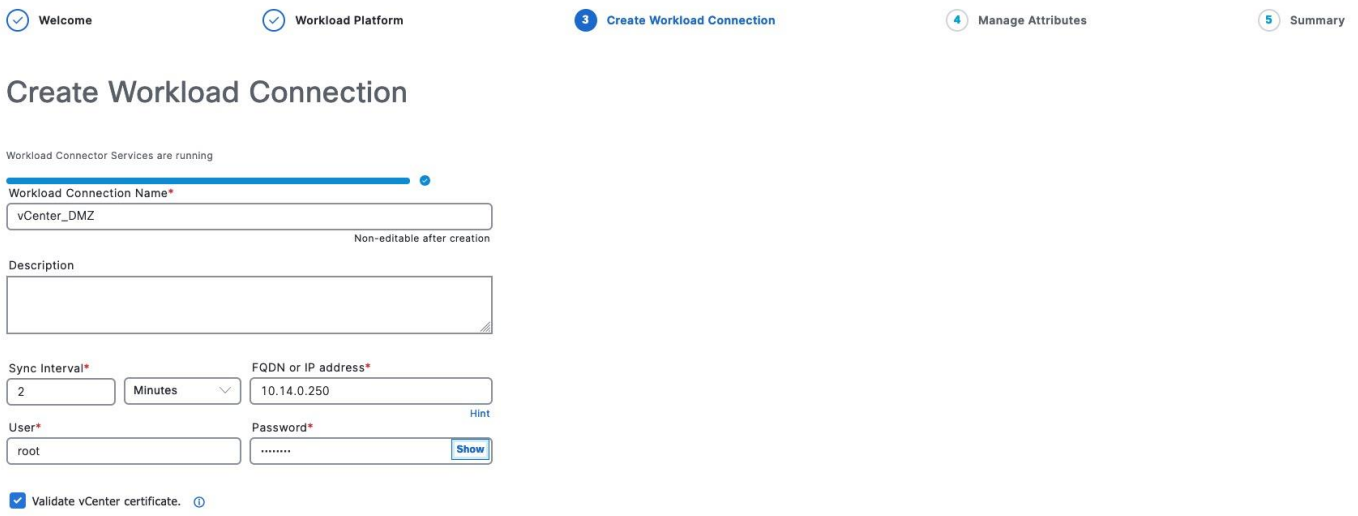
Step 1. Choose **Work Centers > Integrations > Workload Connections > + Add Connection**.

Step 2. In the **Welcome** window, click **Let's Do it**.

Step 3. Choose **VCenter** under **Workload Platform**.



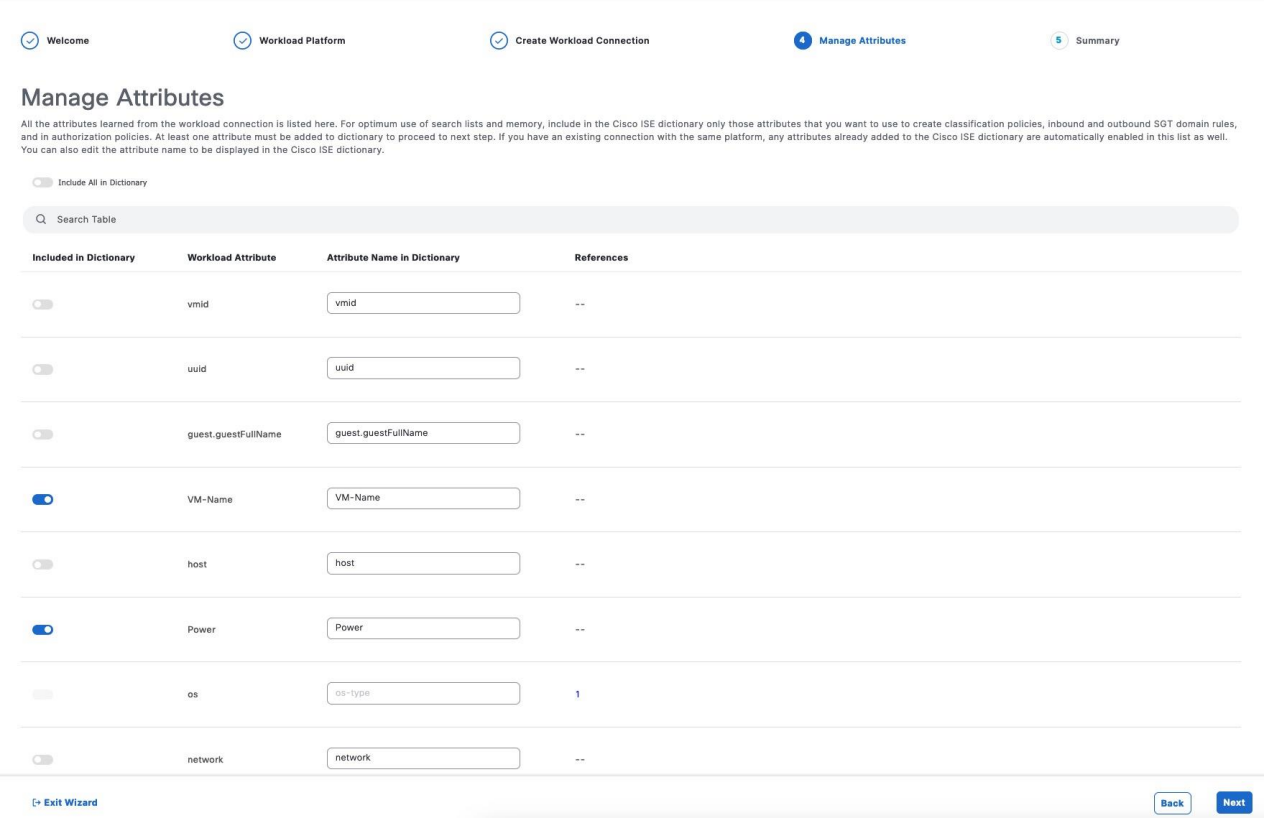
Step 4. Enter **Workload Connection** parameters.



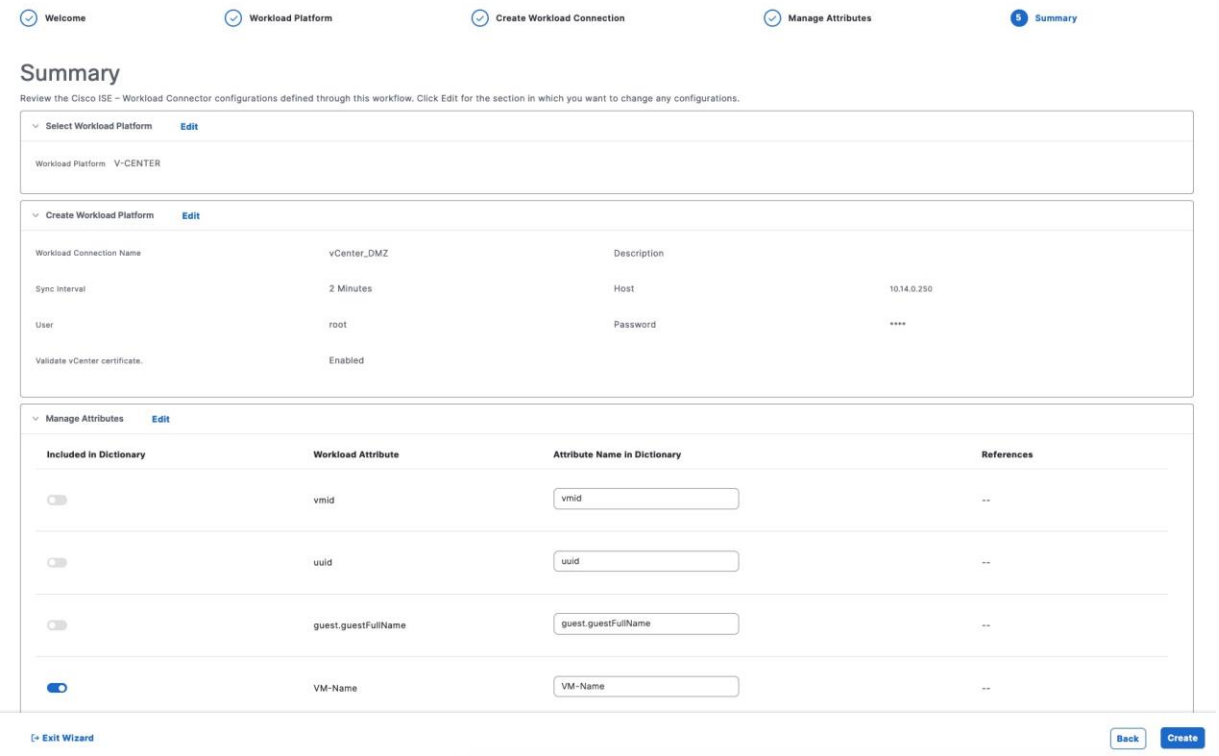
Step 5. When **Validate vCenter certificate** is chosen, ensure vCenter certificates have been uploaded to the ISE Trusted Certificate Store.

Step 6. Choose the **Attributes** to classify the workloads in the SGTs.

© 2026 Cisco and/or its affiliates. All rights reserved.



Step 7. Review **Summary** window information then click **Create**.



Workload classification rules

© 2026 Cisco and/or its affiliates. All rights reserved.

After the vCenter connection is established, from **Work Centers > Workload Connectors > Workload Classification > + Add Classification Rule**, create Workload Classification rules to define how the workloads will be classified.

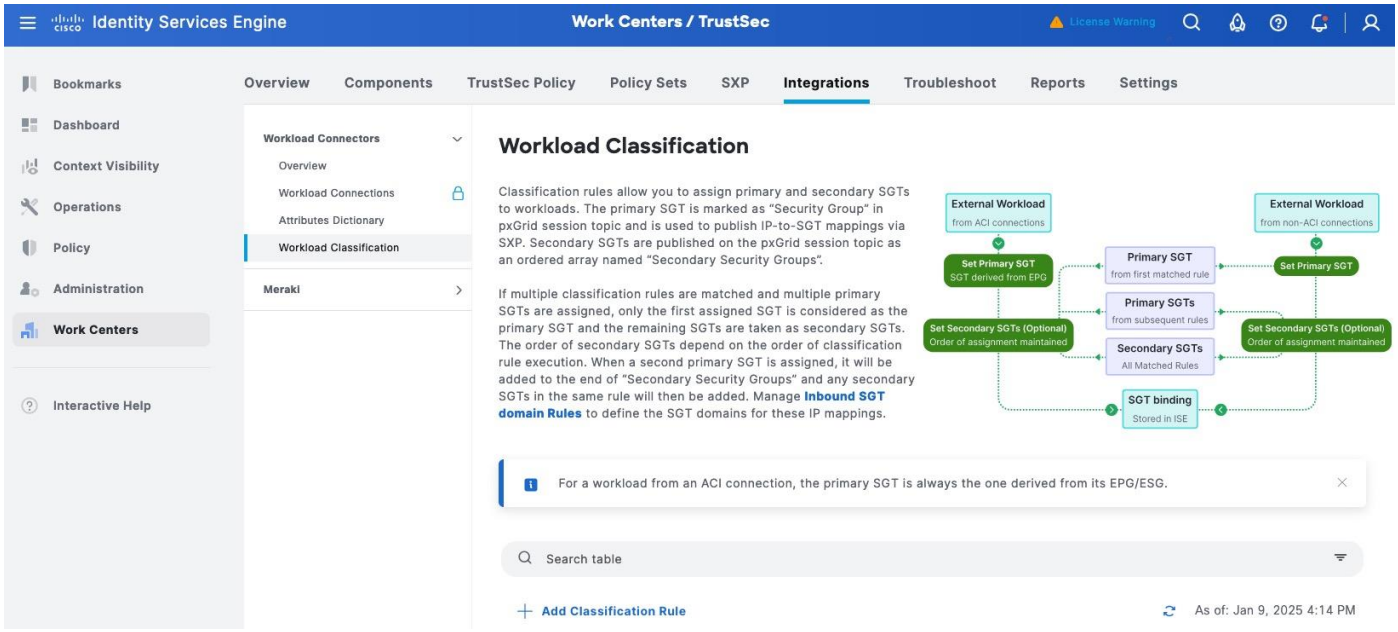
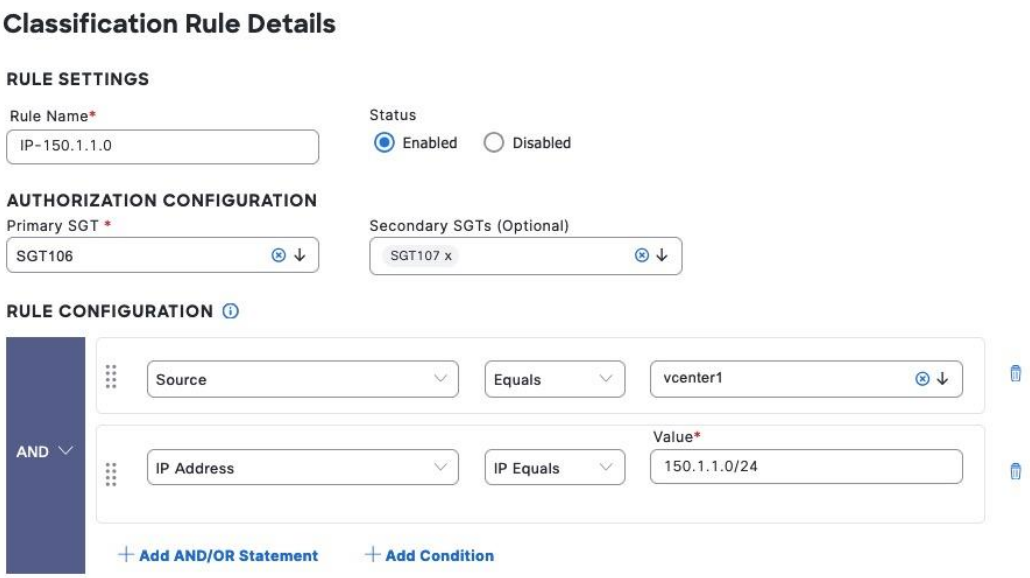
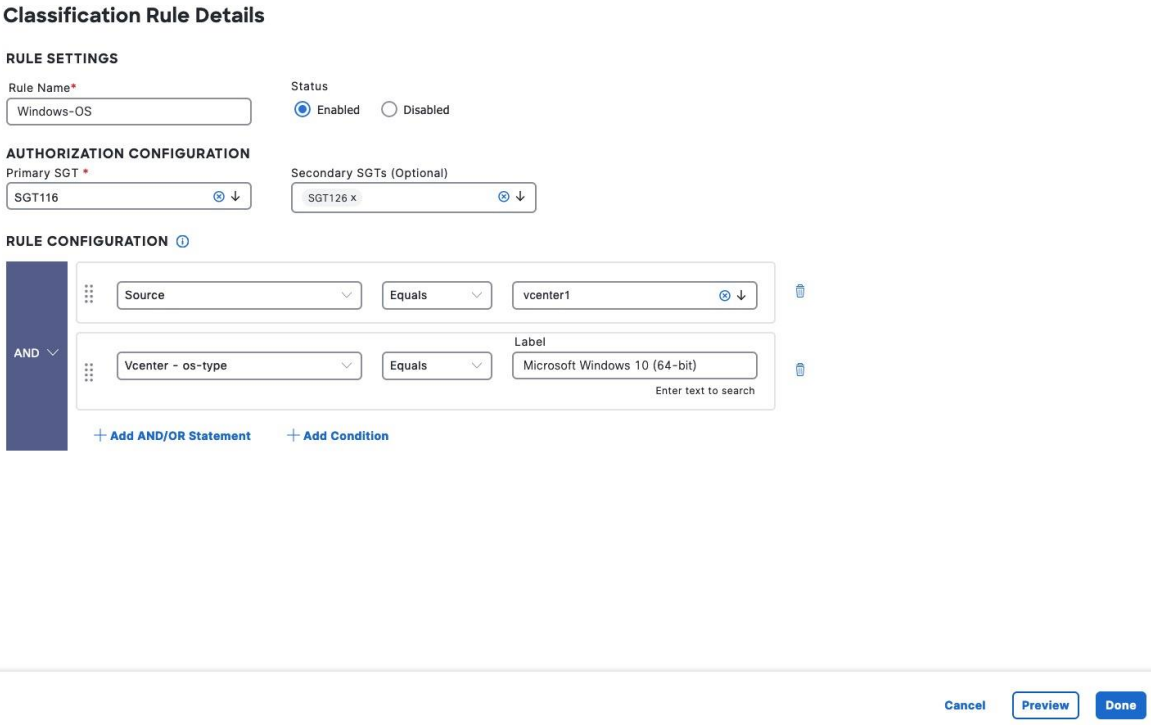


Figure 1. Example of a Classification Rule based on an IP address



© 2026 Cisco and/or its affiliates. All rights reserved.

Figure 2. Example of a Classification Rule based on operating system type (os-type)

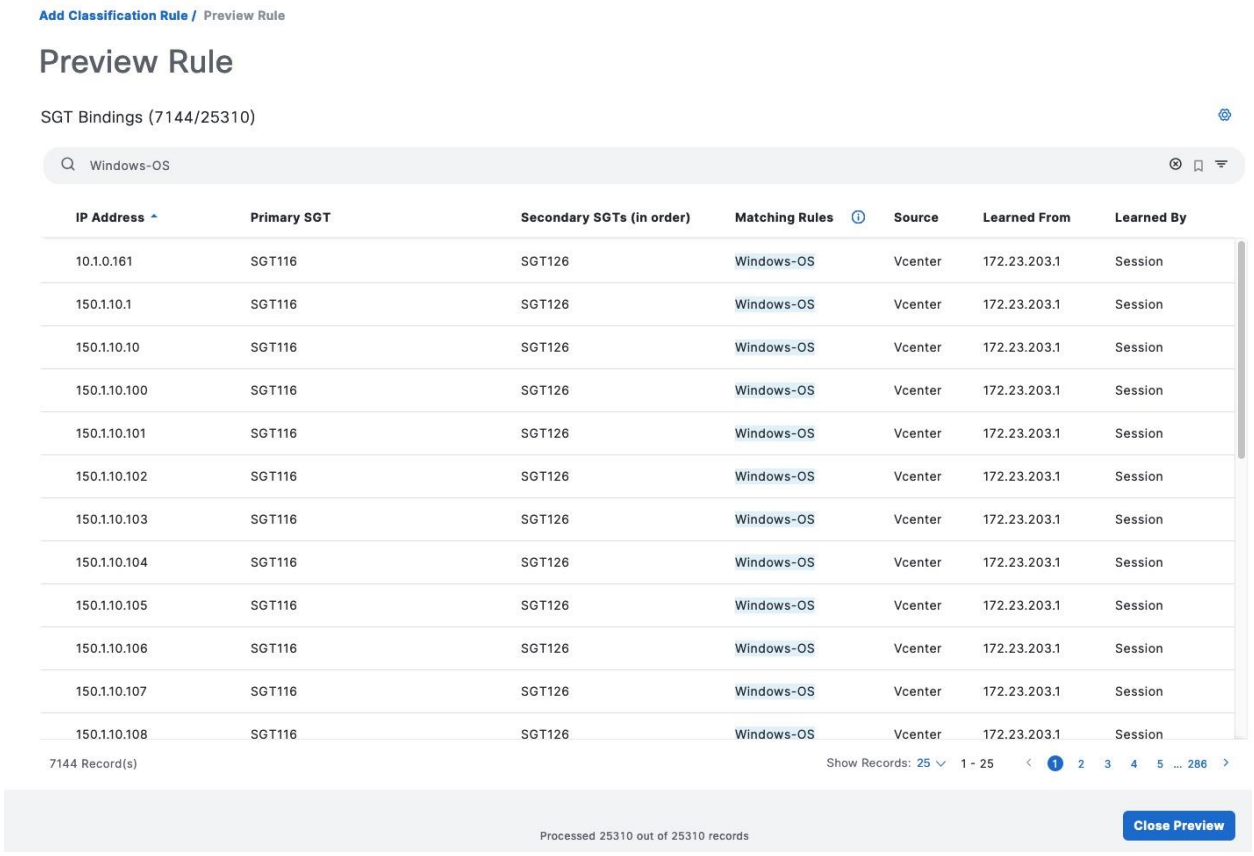


The primary SGT is marked as **Security Group** in the pxGrid session topic and is used to publish IP-to-SGT mappings through SXP. The secondary SGT is sent out through the pxGrid session topic as an ordered array named **Secondary Security Groups**.

Procedure 1. To display the result of the Classification Rule:

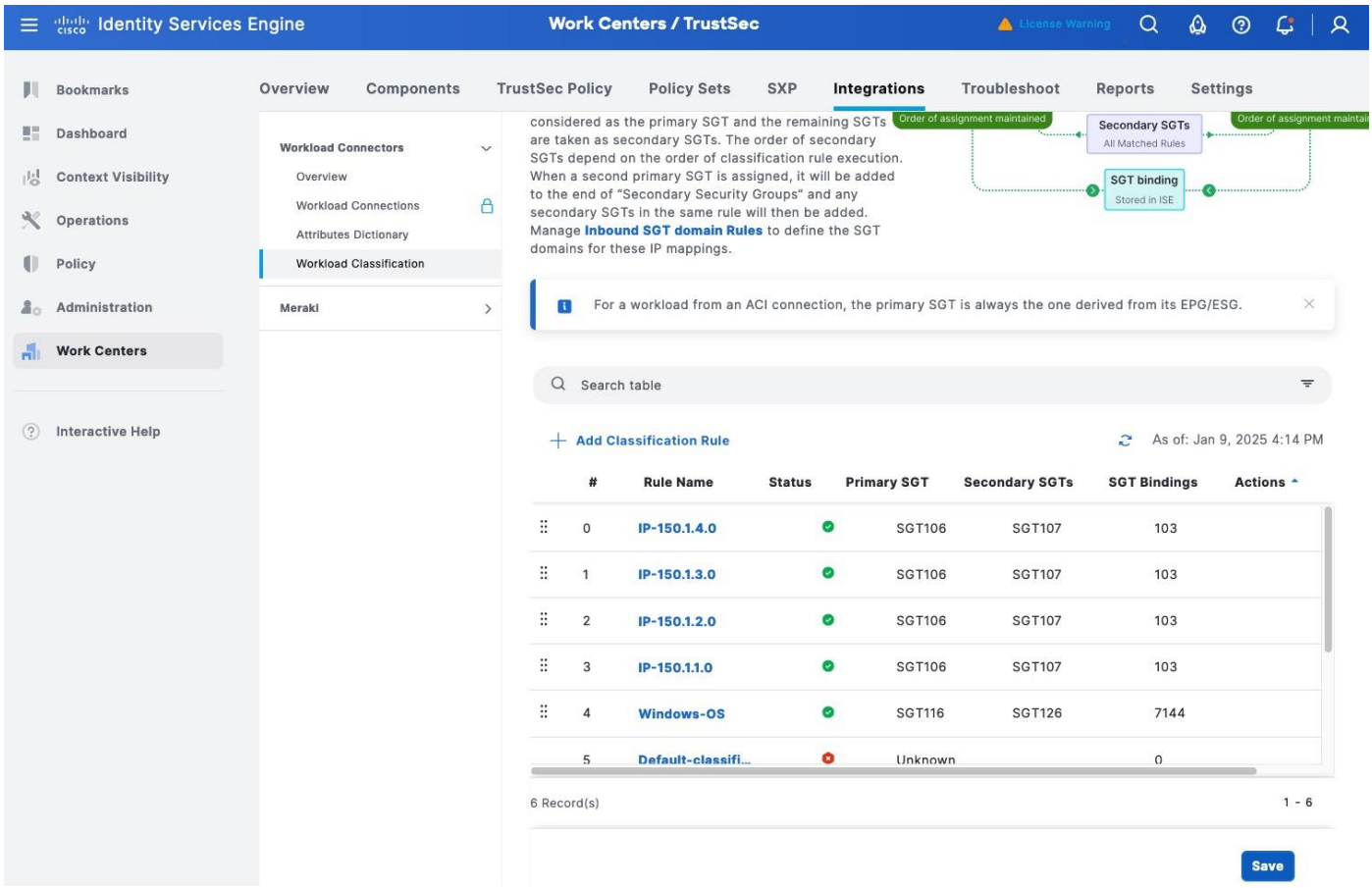
Step 1. Use the **Preview Rule** window with a search criterion.

© 2026 Cisco and/or its affiliates. All rights reserved.



Step 2. Click **Save** to submit the Classification Rule.

© 2026 Cisco and/or its affiliates. All rights reserved.

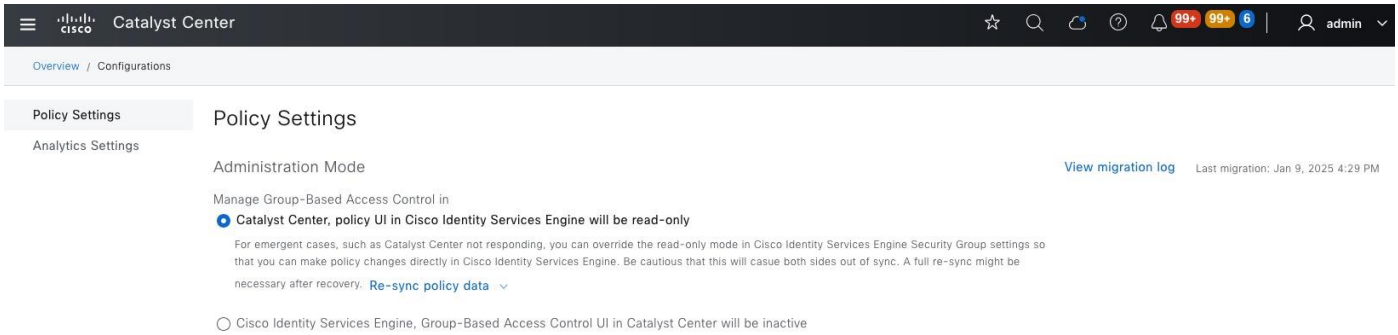


After the vCenter workloads are mapped to SGTs, a policy can be applied to these workloads at different enforcement points, such as ACI Leafs, SD-Access Border nodes, SD-WAN Edge nodes, and Cisco Firepower devices.

ISE integration with Cisco Catalyst Center

In this solution test, ISE is integrated with Cisco Catalyst Center as described in Catalyst Center and Cisco ISE Integration.

Catalyst Center is configured to be the policy administration point. TrustSec policy configuration is done from Catalyst Center. Security groups, access contracts, and policies in ISE are read-only.

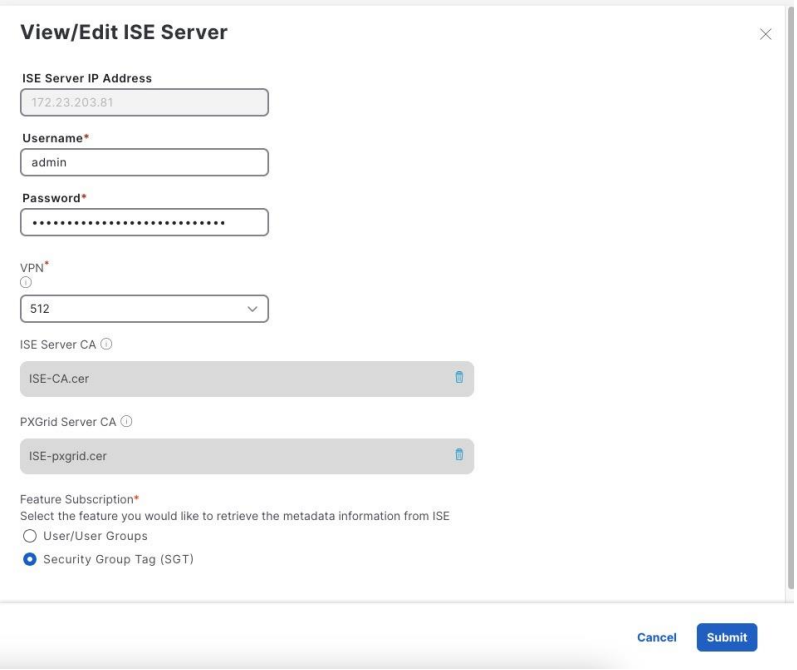


© 2026 Cisco and/or its affiliates. All rights reserved.

ISE integration with Cisco SD-WAN Manager

Cisco Catalyst SD-WAN Identity-Based Firewall Policy Enhancement for SGT integration with Cisco ISE is supported since Cisco SD-WAN Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a.

ISE Integration with Cisco SD-WAN Manager is initiated from the Cisco SD-WAN Manager UI under **Administration > Integration Management > Identity Services Engine**. The procedure is found in Configure PxGrid in Cisco ISE for Connectivity to Cisco SD-WAN Controller.



Verify ISE pxGrid integration on the SD-WAN Controller:

```
sdwan-controller# show idmgr pxgrid-status
idmgr pxgrid-status default
----------------------------------------
Identity Manager Tenant - default
----------------------------------------
State                          Connection and subscriptions successful
Current event                  EVT-None
Previous event                 SXP websocket create eveent
Session base URL
Session pubsub base URL
Session topic
UserGroups topic
Session Websocket status       ws-disconnected
SXP base URL                   https://ISE-MNT1.cdp.com:8910/pxgrid/ise/sxp
SXP pubsub base URL            wss://ISE-PSN1.cdp.com:8910/pxgrid/ise/pubsub
SXP topic                      /topic/com.cisco.ise.sxp.binding
SXP Websocket status           ws-connected
Last notification sent         Connection successful
Timestamp of recent session
```

After integration is enabled, the SD-WAN administrator can configure a Cisco Catalyst SD-WAN Identity-Based Firewall Policy. SGTs are sent to SD-WAN Manager (formerly vManage) for policy configuration. IP-SGT mappings are sent to SD-WAN Controller (formerly vSmart). Based on the configured SGT domain

© 2026 Cisco and/or its affiliates. All rights reserved.

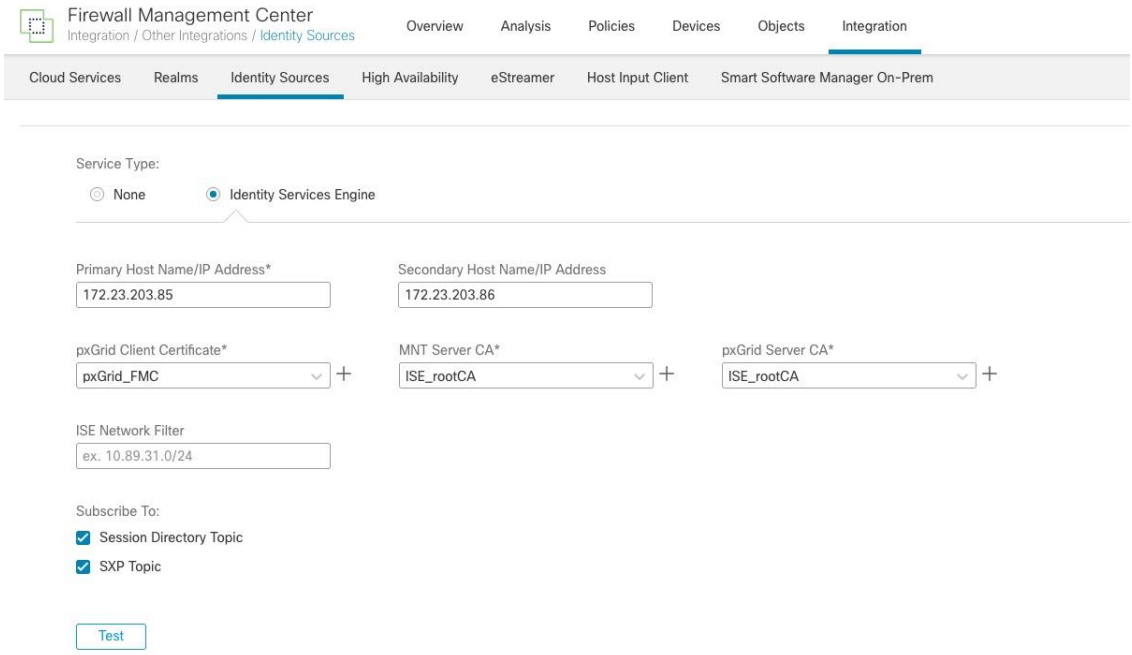
inbound rule, ISE sends IP-SGT bindings, learned from ACI, to a specific SD-WAN VPN that matches the SGT domain name.

ISE integration with FMC

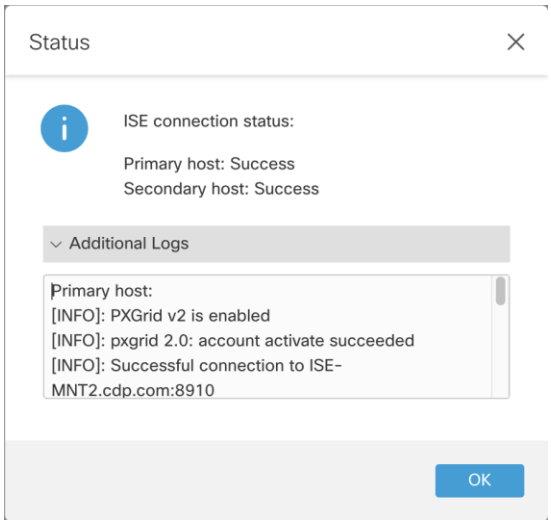
FMC integration with ISE using pxGrid 2.0 has been supported since release 6.7. The integration is initiated from the FMC UI.

Procedure 1. To configure ISE integration with FMC:

Step 1. Configure ISE integration with FMC under **Integration > Identity Sources > Identity Services Engine**.



Step 2. Click **Test** to verify that the pxGrid connection to ISE succeeds.



The detailed procedure to integrate ISE with FMC is found in Configure and Troubleshoot ISE 3.2 with FMC 7.2.4 Integration.

© 2026 Cisco and/or its affiliates. All rights reserved.

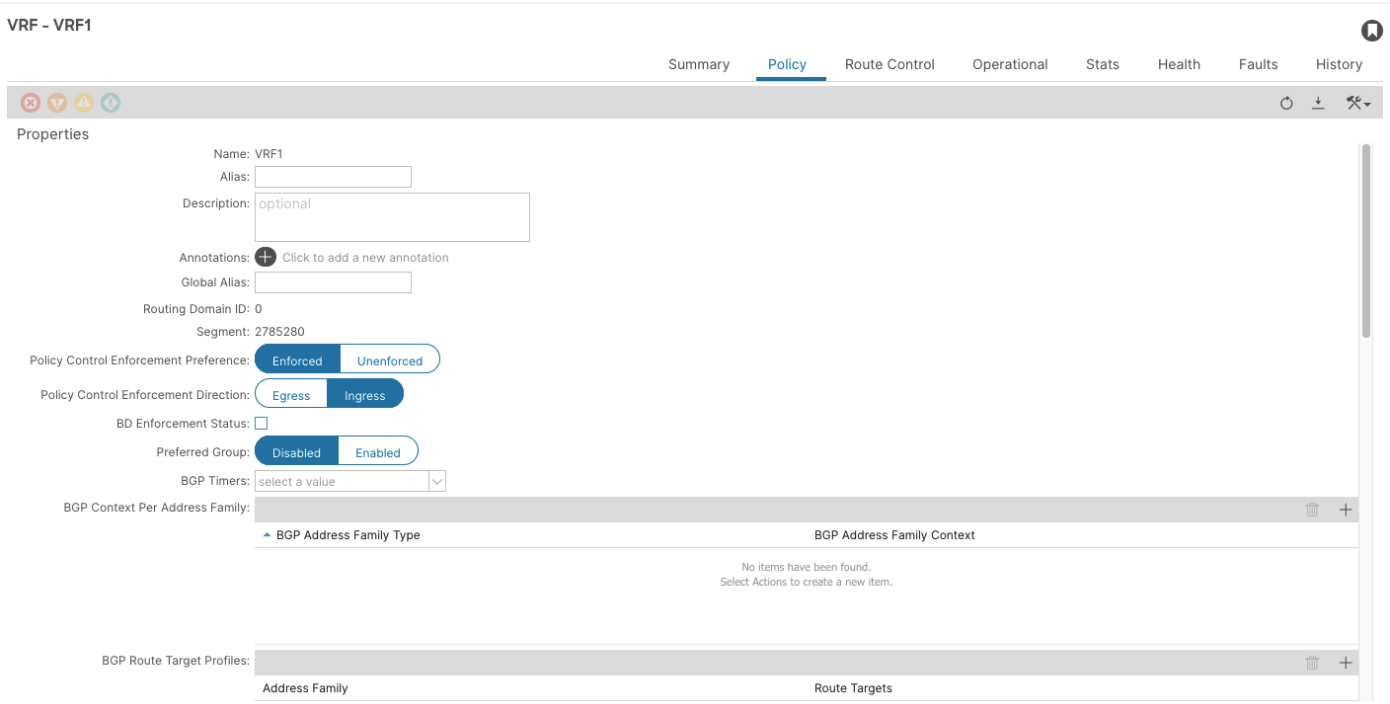
ISE subscribes to selected EPGs and ESGs in the ACI fabric, which are sent to FMC for traffic enforcement.

Policy enforcement points

ACI leaf policy enforcement

ISE learns the IP-SGT binding of the user or device that connects to the campus network, either through dot1x, or MAC Authentication Bypass (MAB). This context is propagated to ACI data centers through the outbound SGT domain rule to enable policy enforcement on the ACI Leafs.

The policy control enforcement direction can be set to either **Ingress** (default) or **Egress** under the ACI VRF Policy configuration.



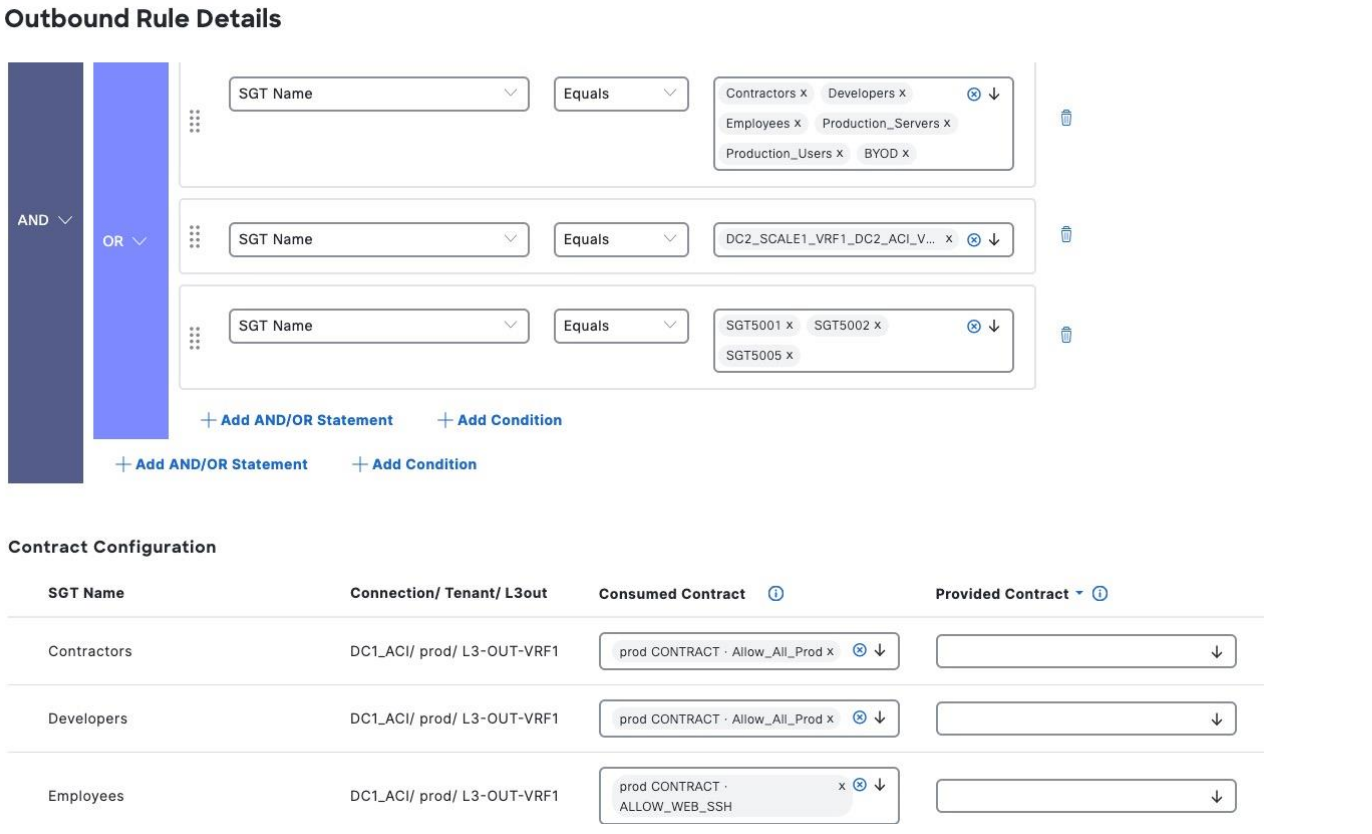
In this example procedure, we apply the contract to allow Employees SGT users to reach the web server behind the ACI data center on TCP ports 22, 80, 443. The web server belongs to the WEB EPG.

Procedure 1. To apply a contract:

Step 1. In the **Contract Configuration** section under **Outbound Rule Details**, for the **Employees** SGT, in the **Consumed Contract** drop-down list, choose the **ALLOW_WEB_SSH** contract.

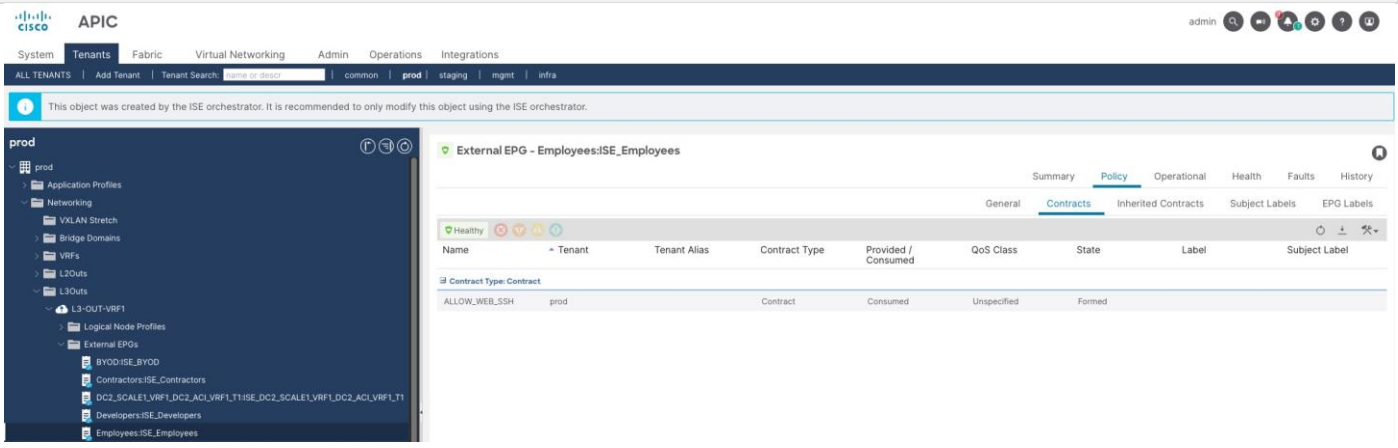
In this case, the **Consumed Contract** of **ALLOW_WEB_SSH** applies to the **Employees** SGT.

© 2026 Cisco and/or its affiliates. All rights reserved.



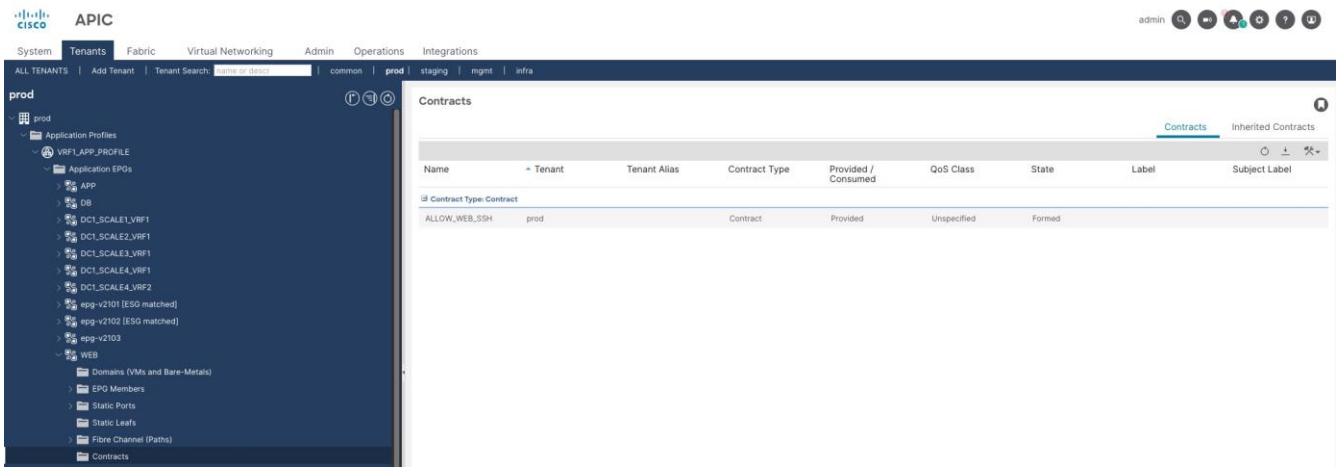
Step 2. Verify in ACI that the consumed contract applies to the corresponding EEPG.

Note: In this example, only the **Consumed Contract** configuration is applied to the SGT because data center devices do not need to access campus devices. However, if data center devices require access to campus devices, a provided contract must be configured.



Step 3. Ensure that there is a corresponding provided contract applied to the WEB EPG, which the web server belongs to.

© 2026 Cisco and/or its affiliates. All rights reserved.



Policy enforcement in SD-Access Border Nodes

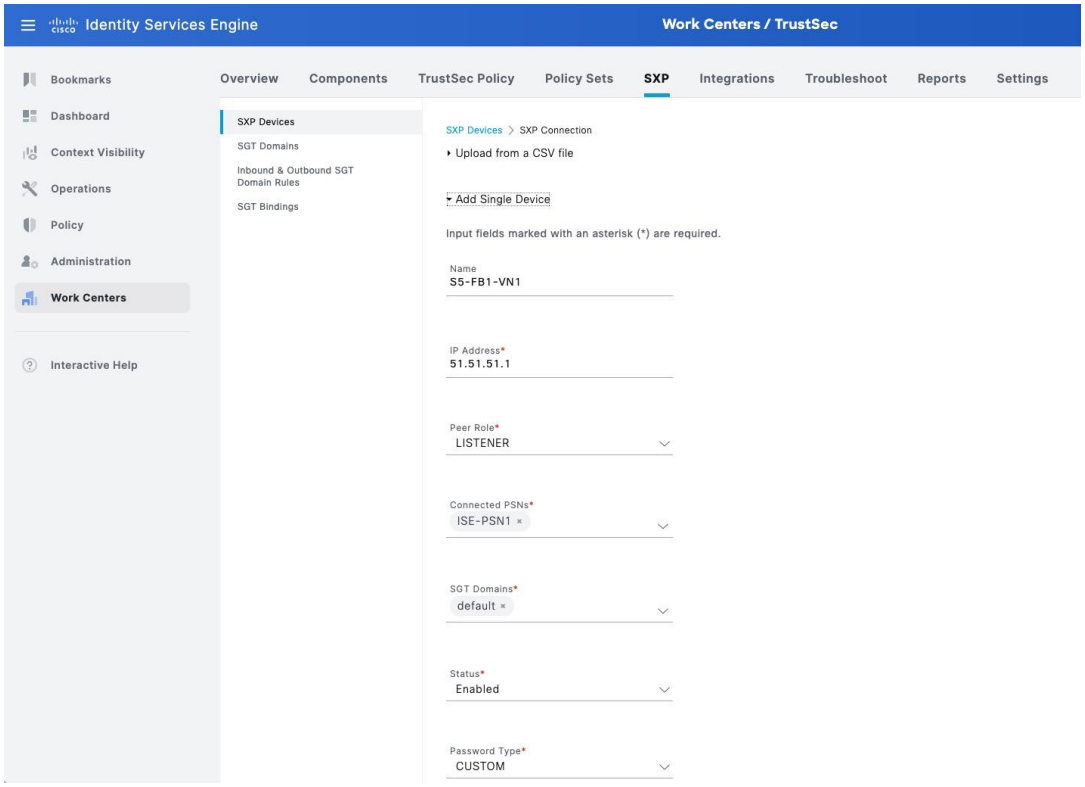
Outbound filtering from the SD-Access campus to ACI data center on the SD-Access Border Nodes requires SXP connection between ISE Policy Service Nodes (PSNs), enabled with SXP service, and the SD-Access Border Nodes. IP-SGT bindings sourced from ACI are learned by ISE and propagated to the SD-Access Border Nodes. With this context, the SD-Access Borders Nodes can filter traffic from campus towards the ACI data centers.

Note: The SD-Access Border Nodes are configured to be a listener for SXP because ISE does not need to learn IP-SGT bindings from the SD-Access Border Nodes through SXP. Instead, ISE learns campus IP-SGT bindings through Dot1x and MAB authentications from the SD-Access Edge Nodes through RADIUS.

Procedure 1. To create an SXP connection between ISE PSNs and the SD-Access Border Nodes:

Step 1. In ISE, configure the SD-Access Border Node as an SXP device under **ISE SXP > SXP Devices > Add**.

© 2026 Cisco and/or its affiliates. All rights reserved.



Step 2. Apply SXP configurations to the SD-Access Border Node.

Figure 3. Example of the SXP configuration applied to the SD-Access Border Node

```
!Create a new loopback interface in VRF to be used as the source of the SXP connection
to ISE-PSN1 and ISE-PSN2, which are enabled with SXP service

interface Loopback 51
 vrf forwarding VN1
 ip address 51.51.51.1 255.255.255.255

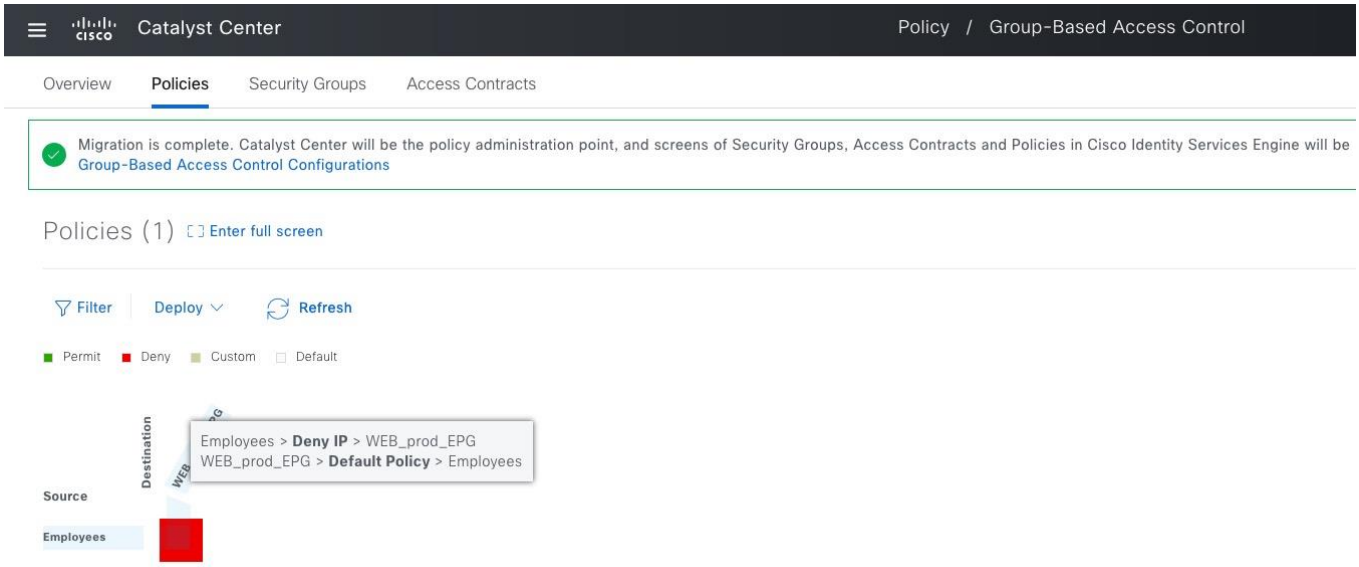
!Define SXP connection to ISE-PSN1 per VRF
cts sxp enable
cts sxp default password 7 060506324F41
cts sxp connection peer 111.30.0.85 source 51.51.51.1 password default mode local
listener hold-time 0 0 vrf VN1

!Define SXP connection to ISE-PSN2 per VRF
cts sxp connection peer 111.30.0.86 source 51.51.51.1 password default mode local
listener hold-time 0 0 vrf VN1

!Enable cts enforcement on SVIs towards fusion router
cts role-based enforcement
cts role-based enforcement vlan-list 2003,2005
```

Step 3. Configure the Catalyst Center policy to deny traffic from Employees to WEB_prod_EPG, which is the SGT learned from ACI.

© 2026 Cisco and/or its affiliates. All rights reserved.



Step 4. Verify traffic enforcement on the SD-Access Border Node.

Figure 4. Example of traffic enforcement verification on an SD-Access Border Node

```
S5-FB1#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 4:Employees to group 3103:WEB_prod_EPG:
        Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

S5-FB1#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          987        353681     0          0
4       3103    0          5          0          0          0          0
S5-FB1#

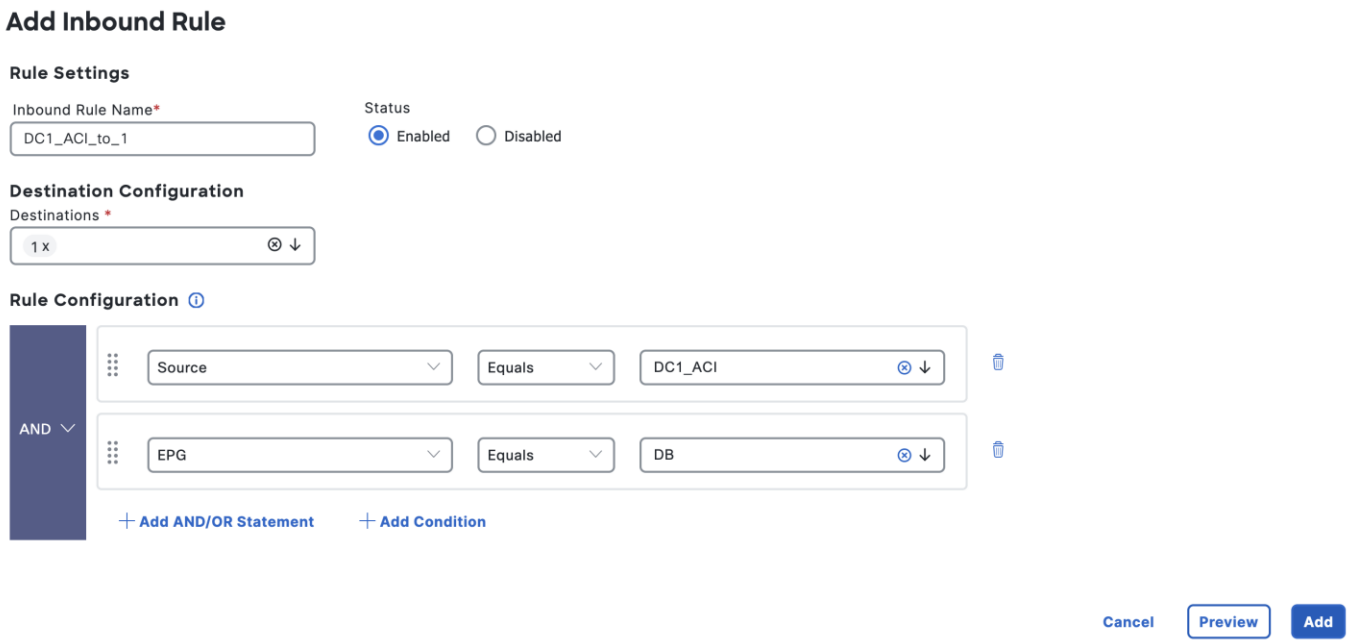
S5-FB1#show cts role-based sgt-map vrf VN1 all | i 111.1.1.101
111.1.1.101             3103    SXP
```

Policy enforcement on the SD-WAN Edge

To enable traffic enforcement on the SD-WAN Edge, an Inbound SGT domain rule is configured to send context to specific SD-WAN VPN #. The SGT domain name matches the SD-WAN VPN number. For example, Inbound rule with destination SGT domain '1' will send SGT context to SD-WAN VPN '1'.

Procedure 1. To configure an Inbound SGT domain rule:

© 2026 Cisco and/or its affiliates. All rights reserved.



Step 1. Verify bindings are received in VPN 1 on the SD-WAN Edge.

```
S3-CE1#show cts role-based sgt-map vrf 1 summary

            -IPv4-

IP-SGT Active Bindings Summary
============================================
Total number of OMP      bindings = 500
Total number of active   bindings = 500


            -IPv6-

IP-SGT Active Bindings Summary
============================================
Total number of OMP      bindings = 500
Total number of active   bindings = 500

S3-CE1#show cts role-based sgt-map vrf 1 all | inc 111.11.0.31
111.11.0.31             3101    OMP
```

Step 2. Verify bindings received on the SD-WAN Controller.

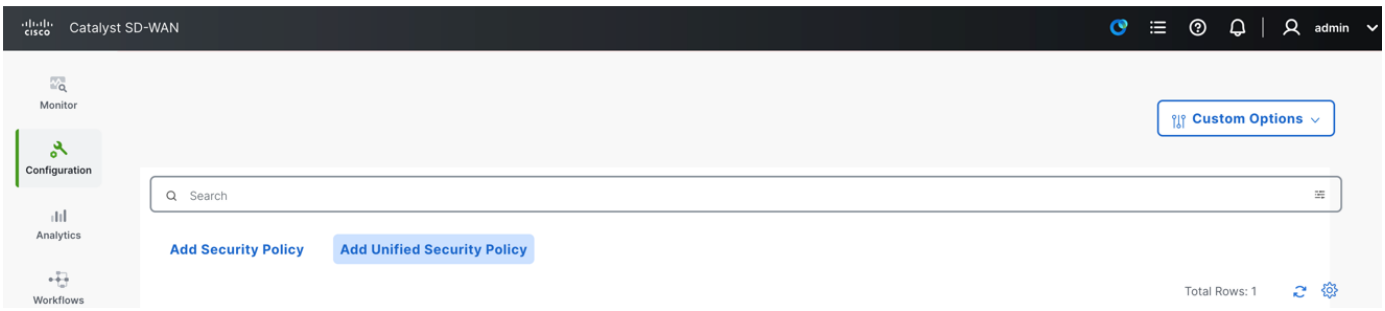
```
sdwan-controller# show idmgr omp ip-sgt-bindings | inc 111.11.0.31
111.11.0.31/32   1    3101   omp-updated
```

Policy enforcement in SD-WAN Edge

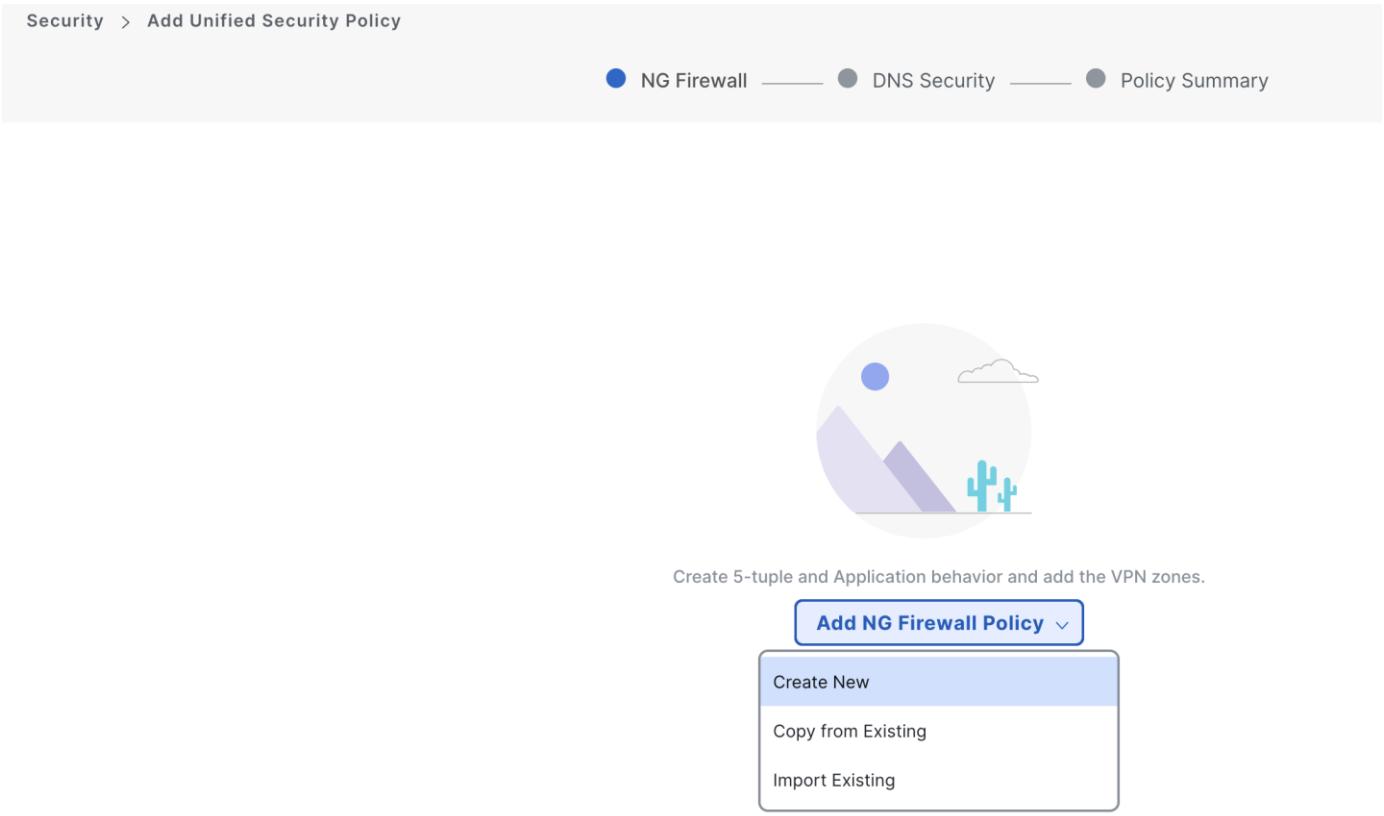
Procedure 1. To create the SD-WAN Security Policy:

Step 1. Choose **Configuration > Security > Add Unified Security Policy**.

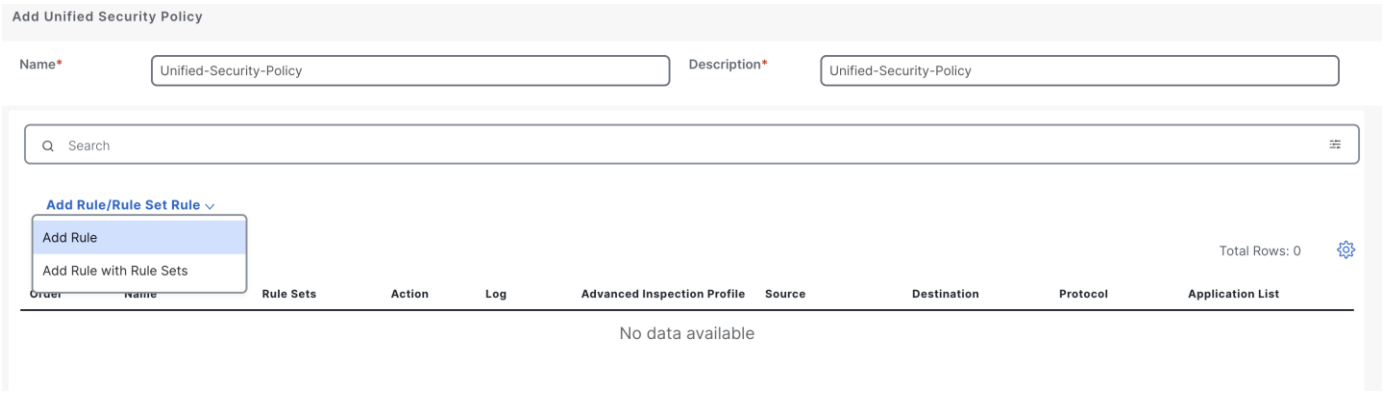
© 2026 Cisco and/or its affiliates. All rights reserved.



Step 2. Click **Add NG Firewall Policy** then choose **Create New**.

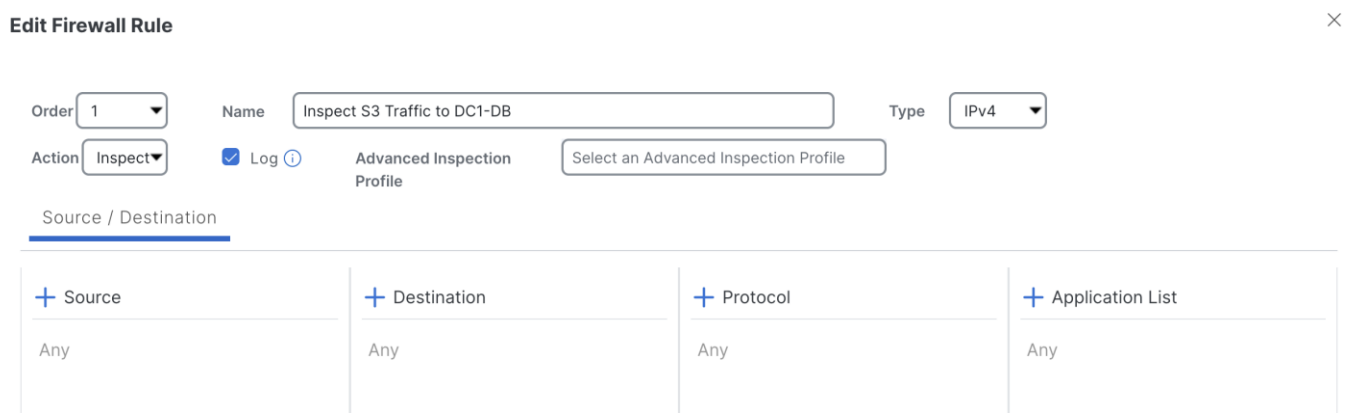


Step 3. Enter a **Name** and **Description** for the **Unified Security Policy**, then click **Add Rule**.

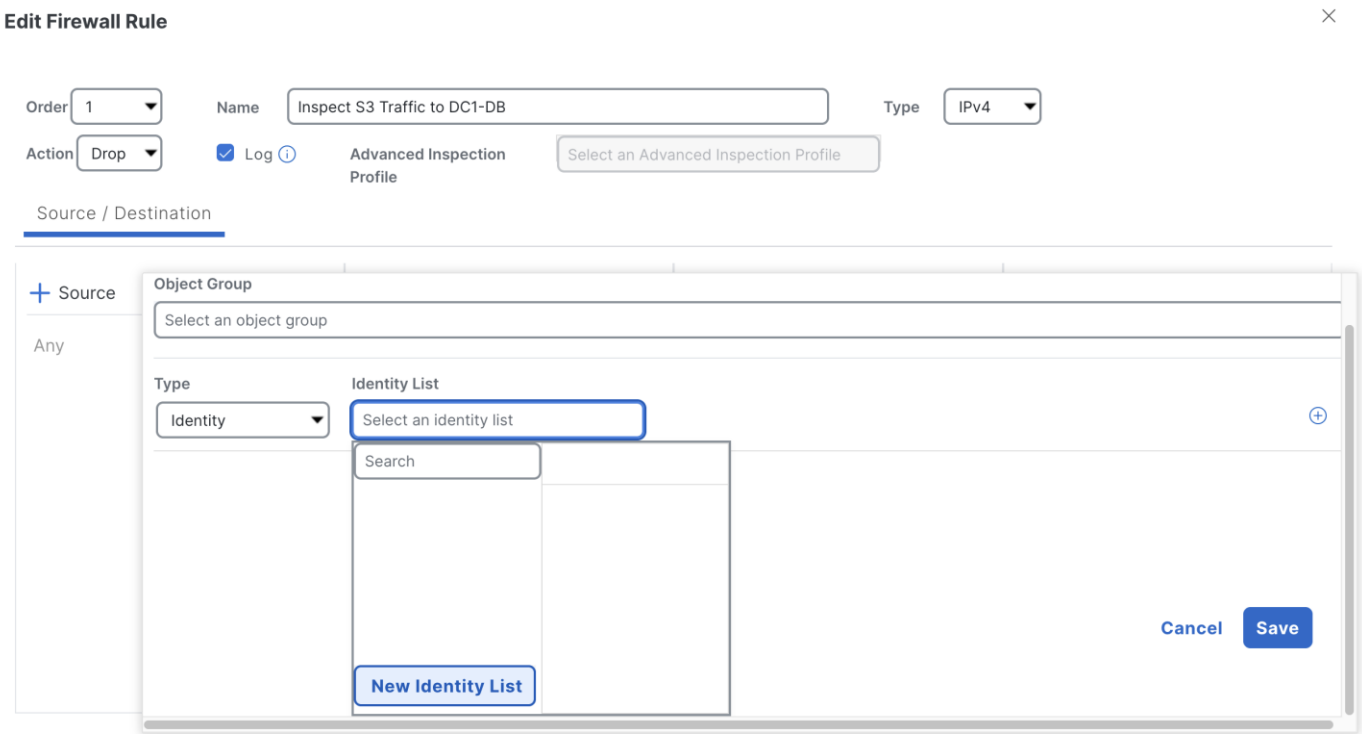


Step 4. Enter a **Name** for the firewall rule. For **Action** choose **Inspect**, then click **+ Destination**.

© 2026 Cisco and/or its affiliates. All rights reserved.

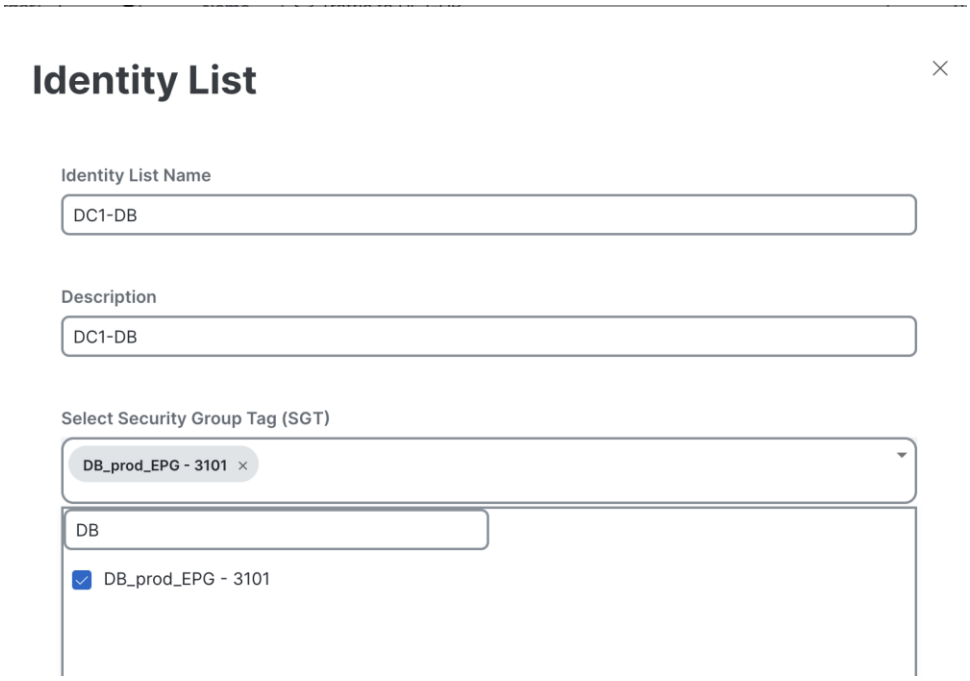


Step 5. For **Type**, choose **Identity**. For the **Identity List**, click **New Identity List**.

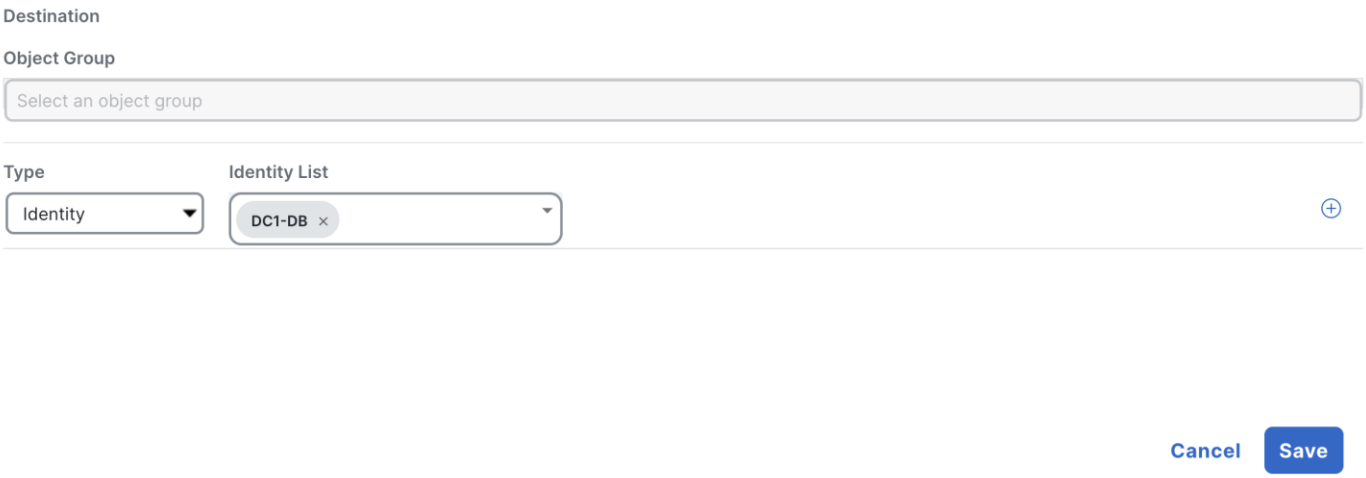


Step 6. Enter an **Identity List Name** and **Description**, choose the **Security Group Tag**, then click **Save**.

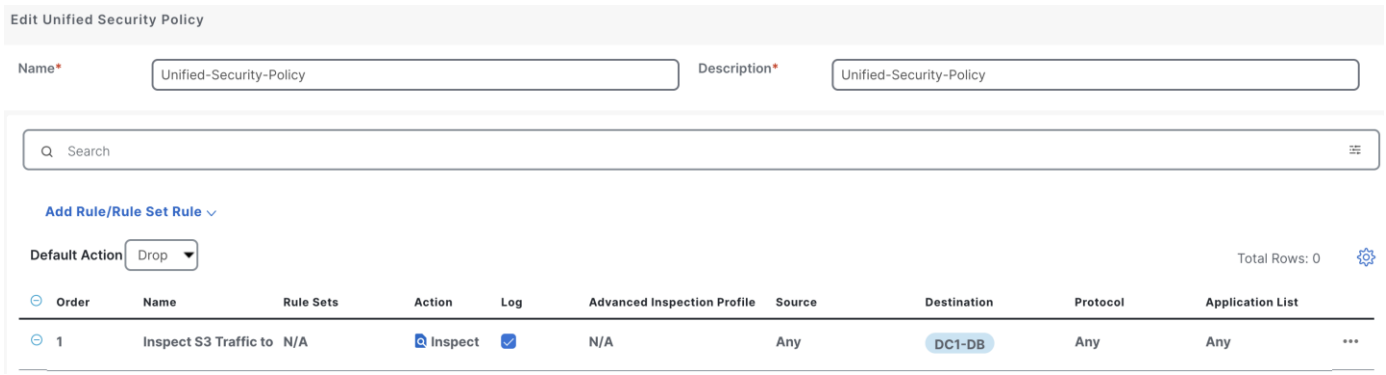
© 2026 Cisco and/or its affiliates. All rights reserved.



Step 7. After creating a new identity list, it becomes available for choosing in the **Destination** section **Identity List**. Choose the identity list you created in Step 6, then click **Save**.

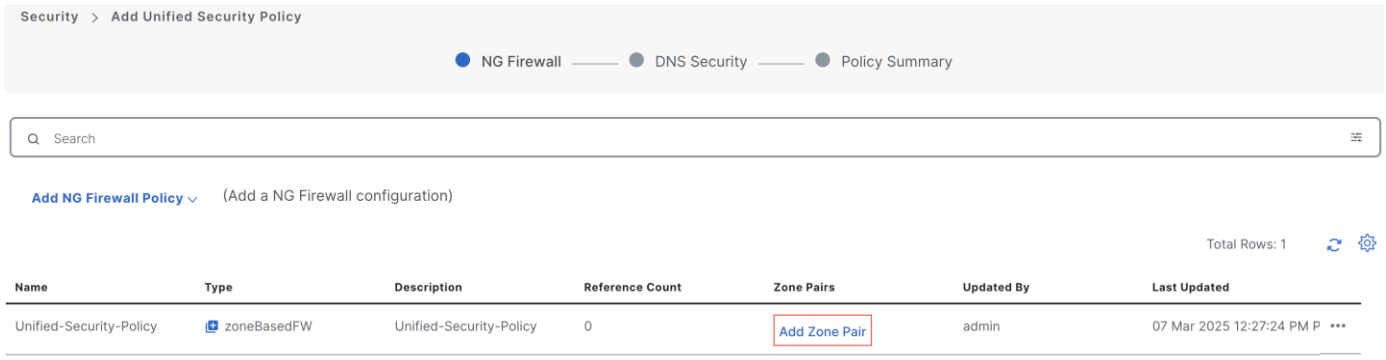


Step 8. Click **Save Unified Security Policy** at the bottom of the window.

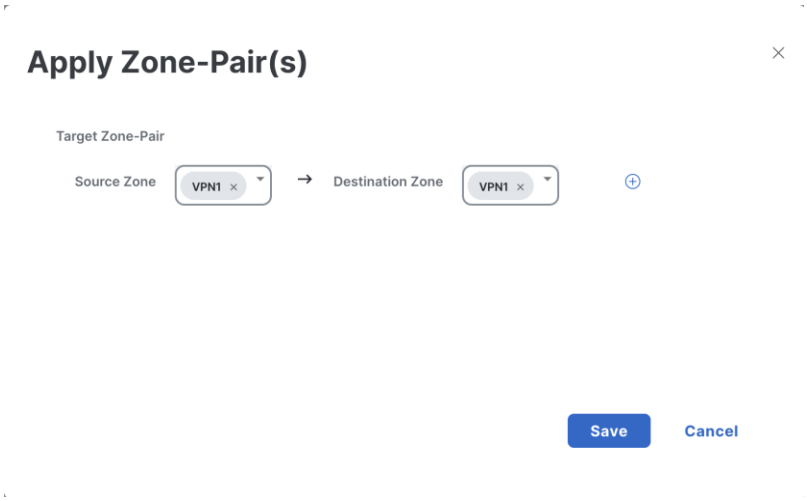


Step 9. After the unified security policy has been created, click **Add Zone Pair**.

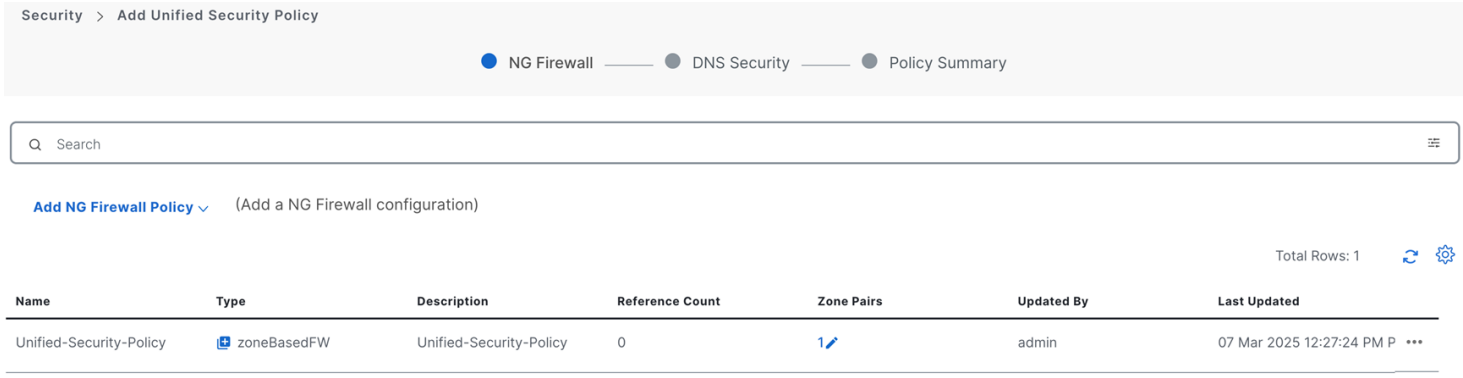
© 2026 Cisco and/or its affiliates. All rights reserved.



Step 10. Under **Apply Zone-Pairs**, choose the relevant service VPN for the **Source Zone** and **Destination Zone**. In this example, **VPN1** is chosen. Click **Save**.

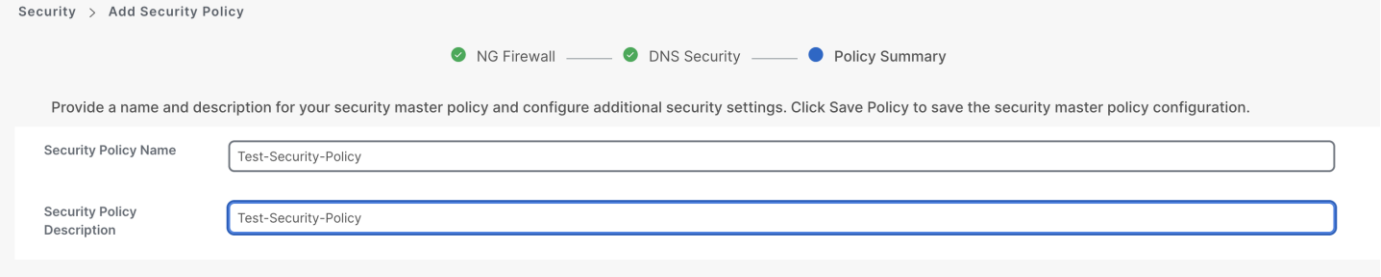


Step 11. Click **Next** at the bottom of the window to proceed. Under the **DNS Security** section (not shown), click **Next** again at the bottom of the window to proceed.

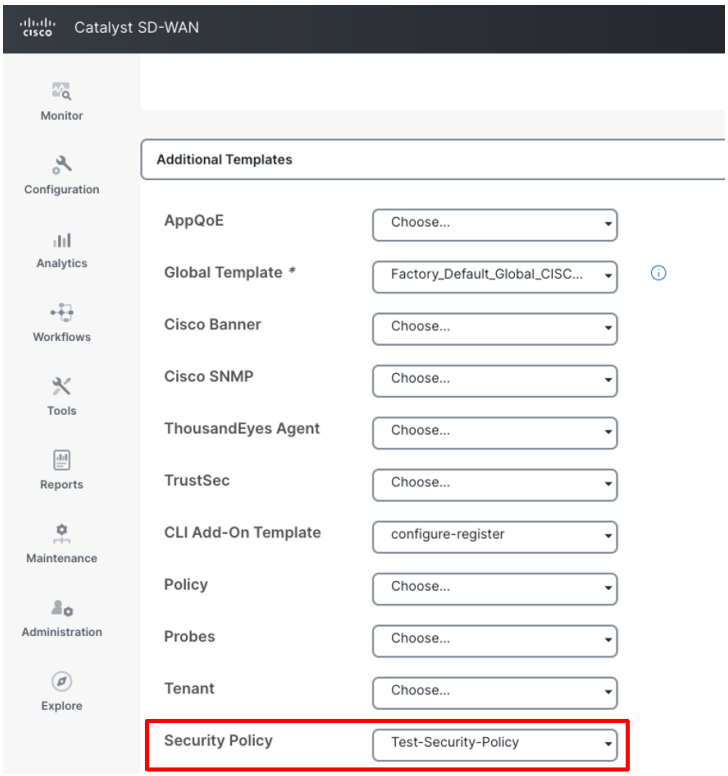


Step 12. Under **Policy Summary**, enter the **Security Policy Name** and **Security Policy Description**, then click **Save Policy**.

© 2026 Cisco and/or its affiliates. All rights reserved.



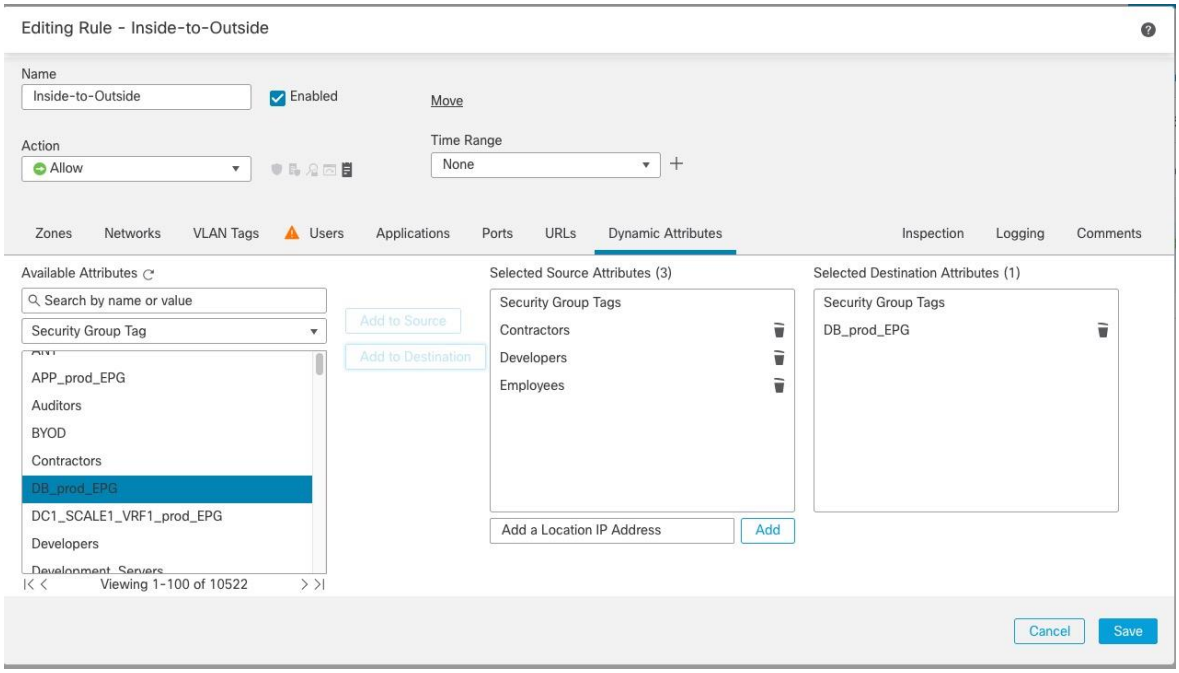
Step 13. From **Configuration> Templates**, choose an existing device template that is attached to a device. From the **Additional Templates** section, click **Security Policy** and choose the **Security Policy** called **Test-Security-Policy** that was created previously.



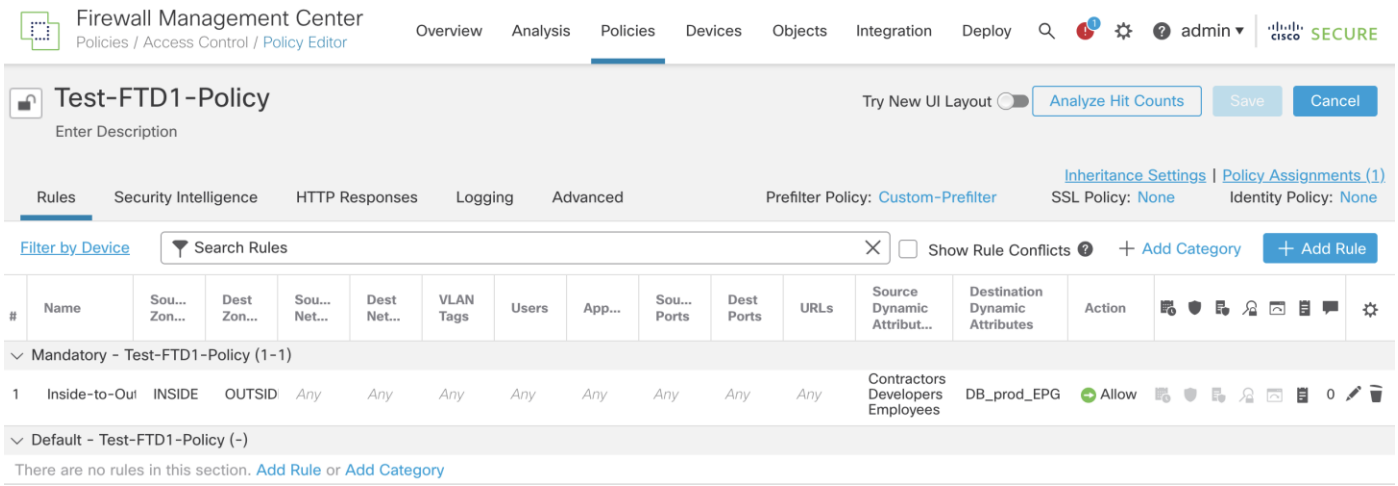
Firewall Threat Defense (FTD) policy enforcement

After the FMC has been integrated with ISE, it is able to get SGTs and associated IP-SGT bindings. The Access Policy rule shows the available SGTs that can be chosen as the source and destination attributes under the **Dynamic Attributes** tab.

© 2026 Cisco and/or its affiliates. All rights reserved.



The firewall policy permits traffic from campus SGTs (Contractors, Developers, and Employees) to DB_prod_EPG, which is the SGT learned from ACI.



Access rule policy enforcement based on SGTs can be verified by using the packet-tracer command or through the **Analysis > Connection Events > Table View of Connection Events** window.

Figure 5. Example verification with the packet-tracer command

```
> packet-tracer input FB1-VN1-INSIDE1 tcp 25.1.10.5 1024 111.11.0.31 443

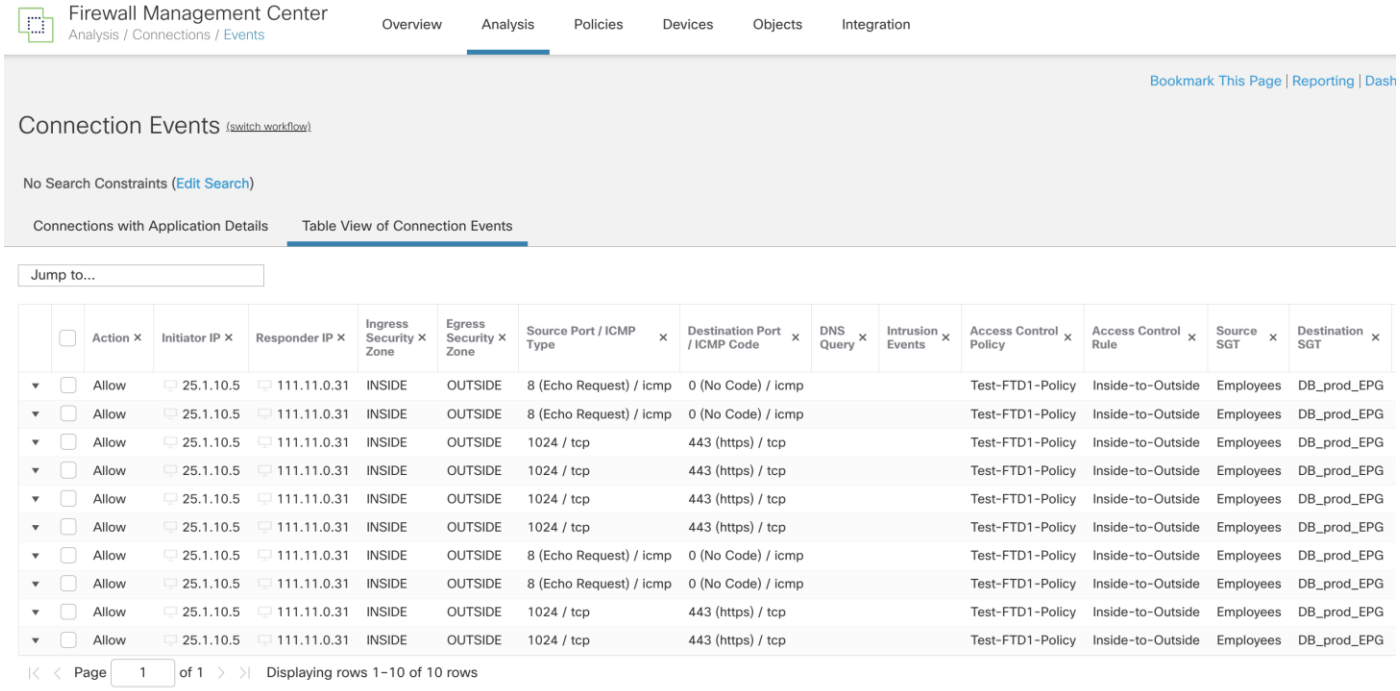
---Truncated---

Phase: 13
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 202428 ns
Config:
```

© 2026 Cisco and/or its affiliates. All rights reserved.

```
Network 0, Inspection 0, Detection 0, Rule ID 268435456
Additional Information:
Starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, src sgt: 4, src sgt type:
sxp, dst sgt: 3101, dst sgt type: sxp, user 9999997, no url or host, no xff
Matched rule ids 268435456 - Allow
```

Figure 6. Example verification with the Connection Events table

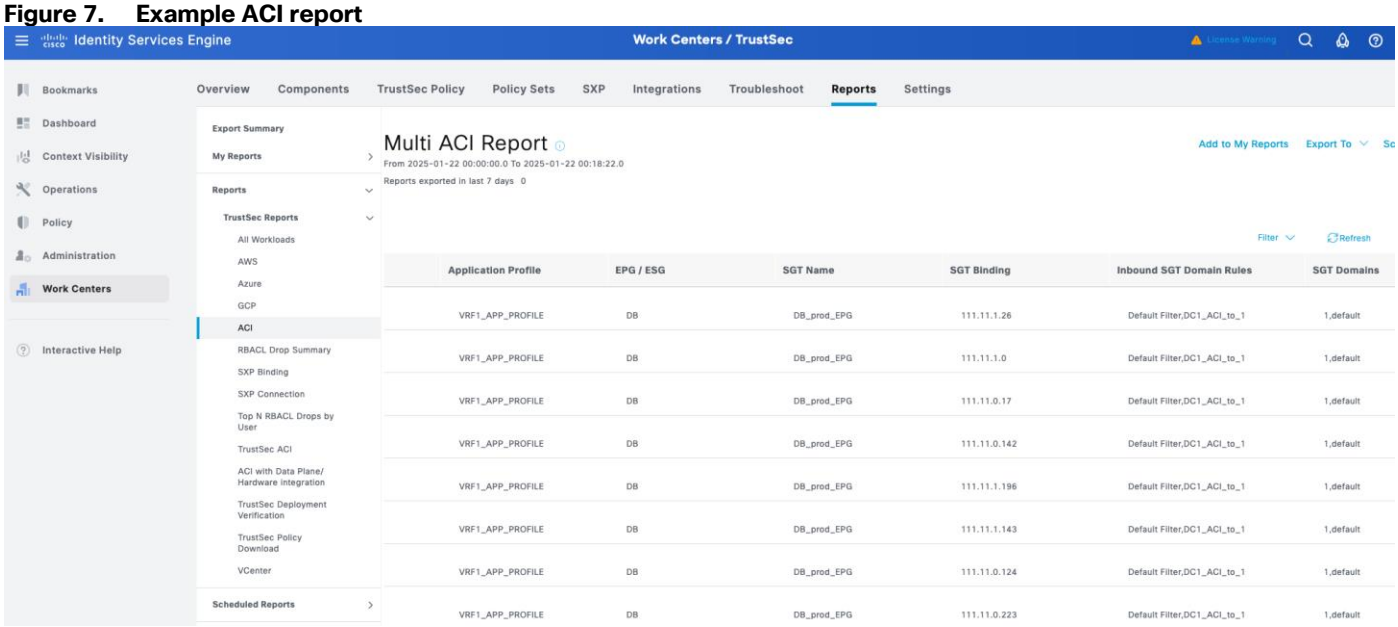


© 2026 Cisco and/or its affiliates. All rights reserved.

Workload reports

Workload reports provide information about workloads received from Cisco ACI controllers and on-premises vCenter controllers to show how an IP-SGT binding is classified. Reporting is useful for checking which IPs are present in the domain and how they are classified. They can also be exported for recording purposes.

Figure 7. Example ACI report



Troubleshooting

This section explains the basic steps for troubleshooting.

Procedure 1. To troubleshoot campus to data center communication:

Step 1. Verify that the campus user and device are assigned the correct SGT.

```
S5-FE1#show authentication sessions interface gigabitEthernet 1/0/1 details

            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x1B62F583
          MAC Address:  0050.56a4.d8c0
         IPv6 Address:  fe80::4f:5b8c:c44:58ed
                        2001:db8:51:1::403
                        2001:db8:51:1::402
         IPv4 Address:  35.1.1.252
            User-Name:  employee-user
          Device-type:  VMWare-Device
          Device-name:  VMWARE, INC.
                  VRF:  VN1
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  multi-auth
    Oper control dir:  both
     Session timeout:  N/A
  Acct update timeout:  172800s (local), Remaining: 85286s
    Common Session ID:  0100011900026AA971A16340
      Acct Session ID:  0x0001967b
```

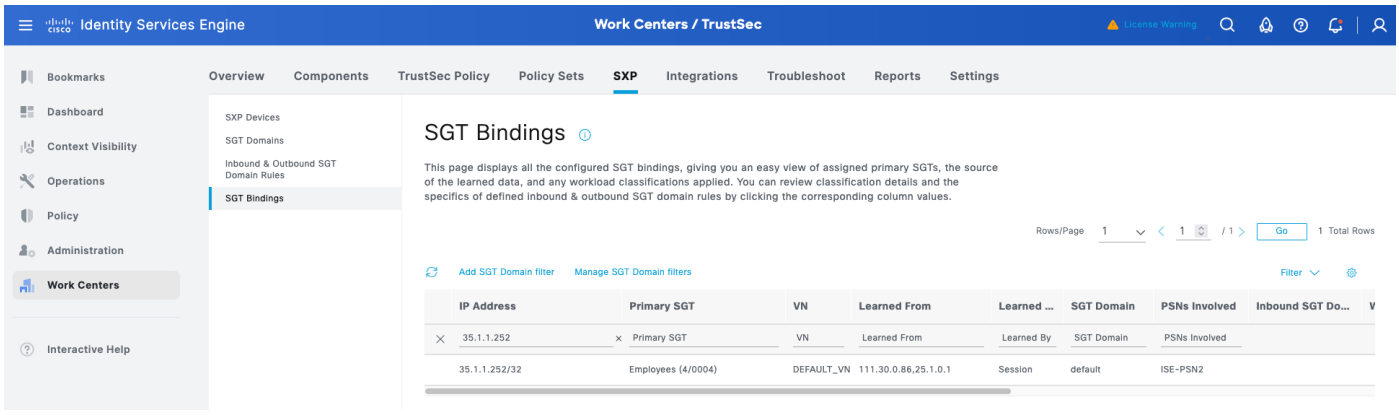
© 2026 Cisco and/or its affiliates. All rights reserved.

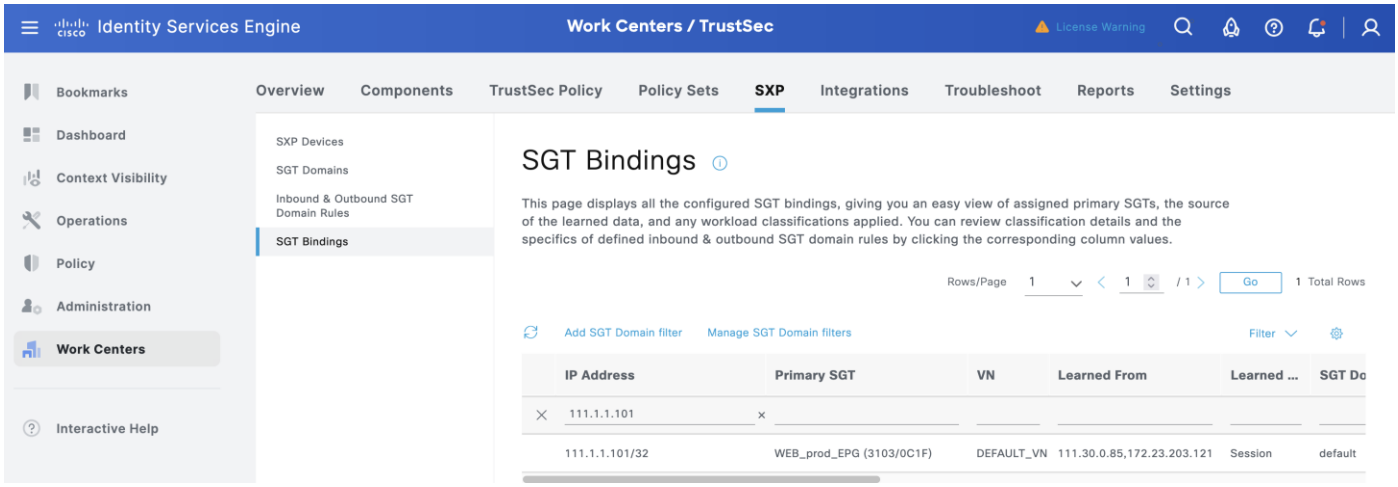
```
               Handle:  0x0b00057c
       Current Policy:  PMAP_DefaultWiredDot1xClosedAuth_1X_MAB


Local Policies:

Server Policies:
           Vlan Group:  Vlan: 1023
            SGT Value:  4
```

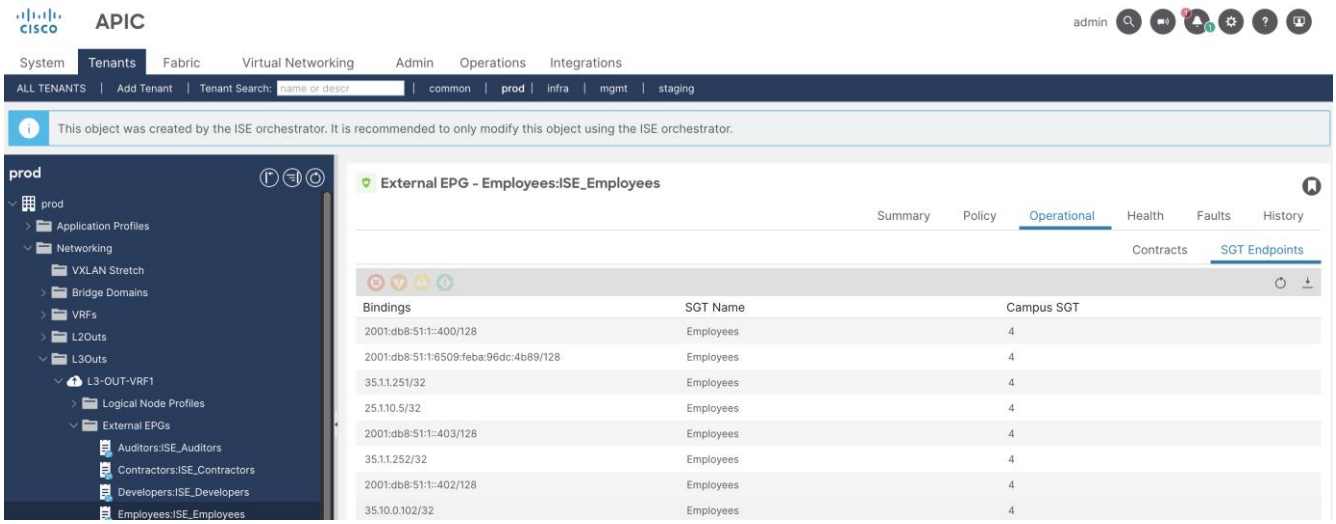
Step 2. Ensure IP-SGT binding exists for the campus host and data center endpoint in ISE.



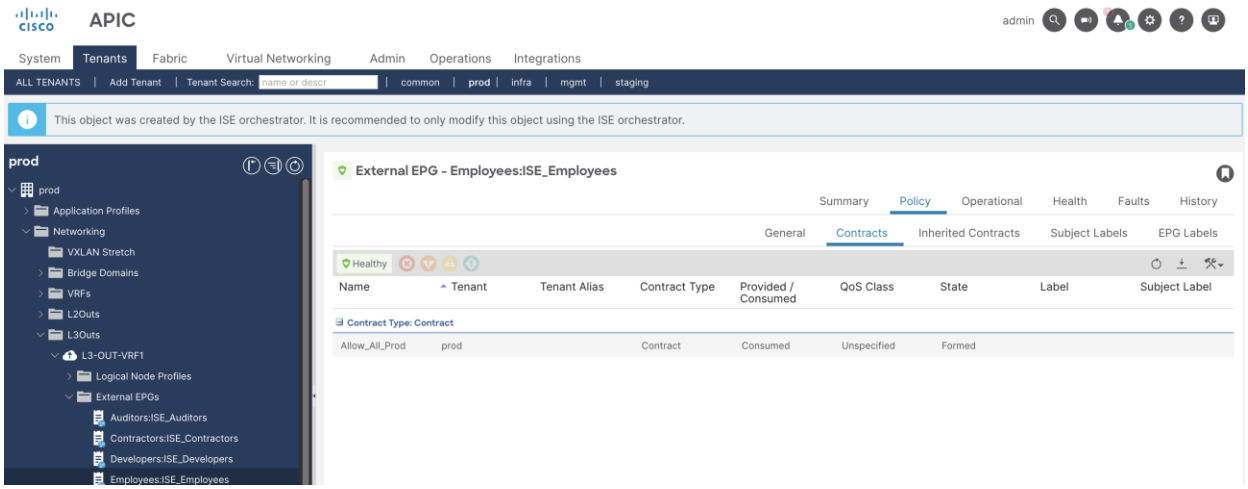


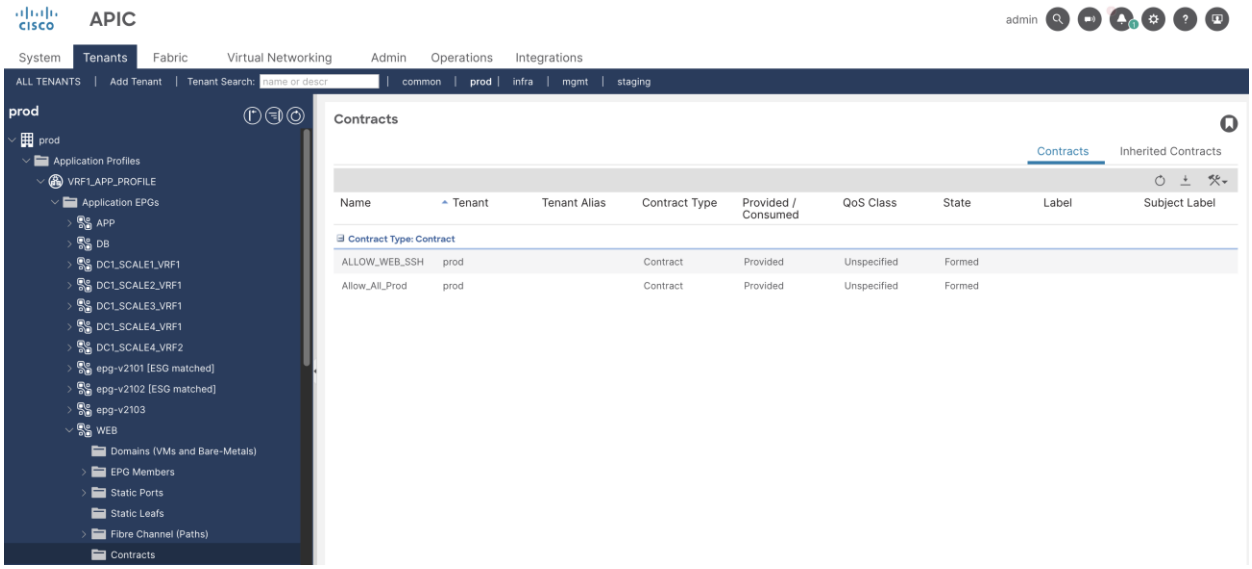
Step 3. Ensure IP binding is present in ACI EEPG SGT bindings.

© 2026 Cisco and/or its affiliates. All rights reserved.



Step 4. Ensure consumed and provided contracts are assigned to EEPG and EPG.





© 2026 Cisco and/or its affiliates. All rights reserved.

Technical References

- Performance and Scalability Guide for Cisco Identity Services Engine
- Catalyst Center and Cisco ISE Integration
- Configure PxGrid in Cisco ISE for Connectivity to Cisco SD-WAN Controller
- Configure and Troubleshoot ISE 3.2 with FMC 7.2.4 Integration
- Cisco SD-Access | SD-WAN Independent Domain Pairwise Integration Prescriptive Deployment Guide

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2026 Cisco and/or its affiliates. All rights reserved.