

CISCO Live !

Amsterdam, NL
February 9-13, 2026

LTRANS-2891

**Unified Policy Control with ISE, ACI, and SDA: Leveraging SGTs for
Scalable Security**

Shivam Kumar, Achintya Murali

Copyright © 2025 Cisco

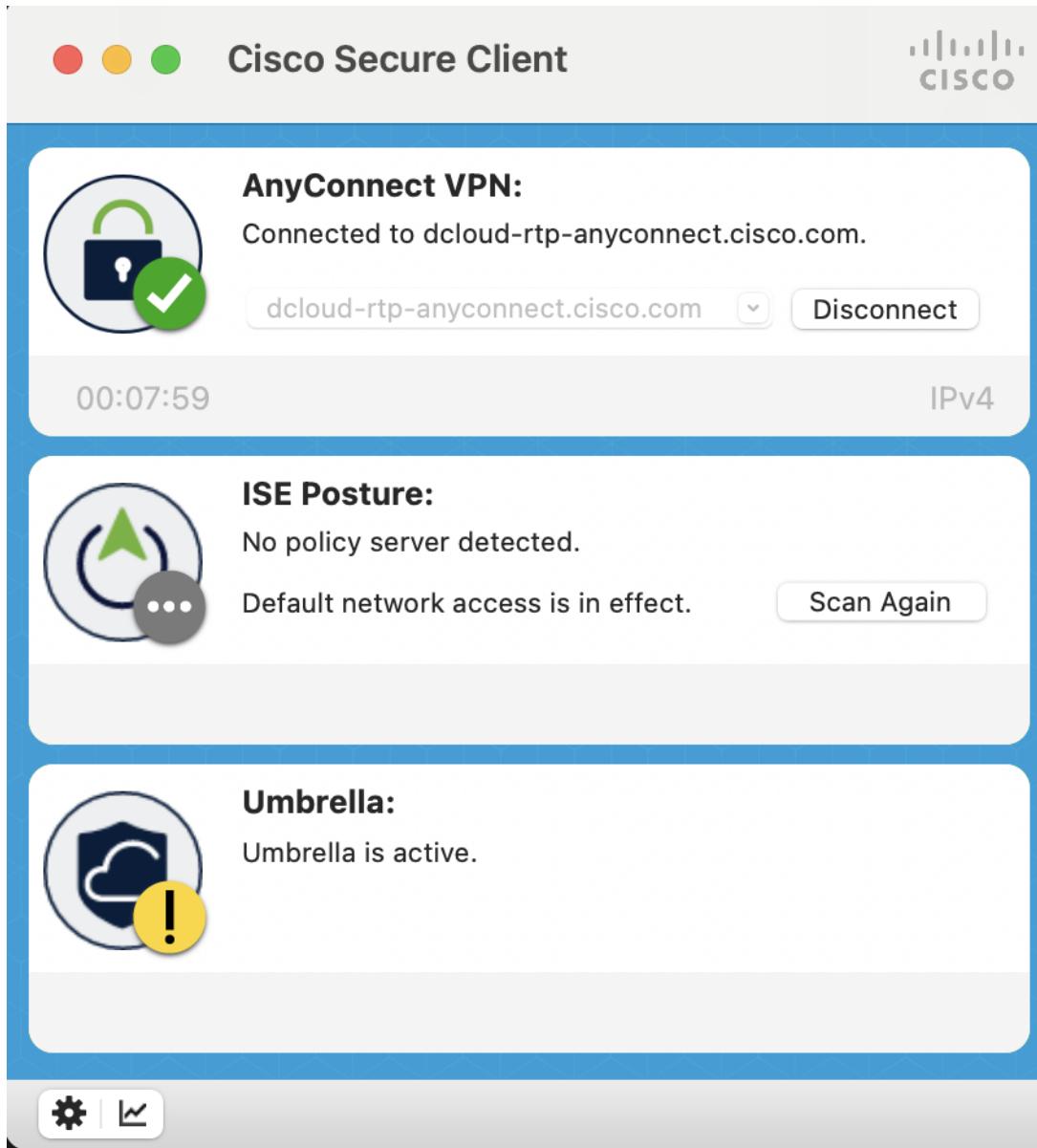
- **Introduction**

The integration of Cisco Application Centric Infrastructure (ACI) and Cisco Software-Defined Access (SDA) represents a significant step toward achieving an end-to-end intent-based networking architecture. By leveraging Cisco Identity Services Engine (ISE) and Security Group Tags (SGTs), this integration delivers consistent security policies across both data center and campus networks. This lab will provide hands-on experience with the configuration, deployment, and management of this integration, enabling participants to understand how to unify networking and security policies across different domains.

- **How to navigate this lab?**

Your primary source of accessing our infrastructure will be via your dCloud set up. You've already been logged into the VPN session, however in case you're logged out or have

connectivity issues, reach out to us and we'll do our best to help. Please check if you are connected to the VPN, it should look at follows:



On your desk you can find your user pod number, which you'll use to navigate the infrastructure.

WARNING:

This is a shared environment, and you have been given full admin access. Please be careful and ensure you are only working on your devices/policies. Be doubly careful to check if you are changing in the correct scope/device before you push any changes.

Learning Objectives

In this lab session, you will explore the following key concepts and skills:

1. Understanding the Integration Between Cisco ACI and SDA:
 - Learn how ACI and SDA complement each other to deliver a unified fabric for campus and data center networking.
 - Grasp the benefits of extending segmentation and policies across domains.
2. Cisco Identity Services Engine (ISE) Role:

- Discover how ISE acts as the policy engine for defining and enforcing Security Group Tags (SGTs).
- Learn how to configure ISE for SGT propagation between ACI and SDA environments.

3. Security Group Tags (SGTs) and Their Importance:

- Understand how SGTs enable identity-based policies and micro-segmentation.
- Explore the use of SGTs for consistent policy enforcement across the network.

4. Common Policy Framework:

- Gain insights into creating and managing policies that work seamlessly in both ACI and SDA.
- Learn how to define policies using Cisco Catalyst Center and APIC controllers.

Lab Objectives

At the end of this lab, you should successfully have understood:

- Hands-on configuration of ACI-SDA integration.
- Synchronization of SGTs across domains using ISE.
- Application of common policy frameworks and verification of policy enforcement.

Lab Scenario

Welcome to our fictional company **ACME Corp**

We want you to walk with us through the stages of expansion of our company and leverage common policy for a consistent and comprehensive security implementation.

We're going to be talking about common policy from the lens of security and segmentation. This lab is a reference to get you started on the journey of envisioning what's possible. Do talk to us and brainstorm together- we'd love to understand how you plan to use this integration and can help clarify what's coming.

Initially we will then parallelly move to the data center and set up contracts there.. After this implementation, we will start with creation of a campus infrastructure- leveraging Catalyst Center and SDA for dot1x.

Then with the common policy set up- we will look at how we can leverage common policy for a seamless integration and end to end security enforcement.

Access Details

Always keep this open on one screen/Tab!

ACI: <https://198.19.219.49>

Username: admin

Pass: C1sc0@1234

External Host Machines (simulated by nexus devices)

SW_303 and SW_304:

Username: clemea

Password: cisco!123

Catalyst Center (DNAC):

<https://198.18.129.100/>

Username: dcloud

Password: C1sco12345

ISE

Session 1 (Users 1-15) 198.18.133.33

Username: admin

Password: C1sco12345

CML Ubuntu Endpoints:

Username: cisco

Password: cisco

CML:

198.18.134.1

Username: admin

Password: C1sco12345

FIAbs:

Username: ciscolive

Password: C1sco12345

Dcloud:

Host

dcloud-rtp-anyconnect.cisco.com

Session 1:

User: v292user1

Password: 767279

Scenarios Shown:

- 1. Native ACI Segmentation**
- 2. Native SDA ISE integration**
- 3. ISE ACI integration Workflow**
- 4. Outbound and Inbound policy from ISE to ACI using SGTs**
- 5. (Theoretical) Understanding Policy Enforcement options**
- 6. (Appendix) Use Case Options with Common Policy**

Task 1: ACI Day 0 Configuration

Scenario

ACME Corp is expanding into the data center and has decided to deploy Cisco ACI to provide scalable segmentation and policy-based connectivity.

The environment consists of:

- 1 ACI fabric with 2 leaf switches and 1 spine
 - External ‘Switches’ acting as end hosts
 - Pre-created tenant objects that will be used throughout this task
-

Learning Objective

This task introduces core Cisco ACI constructs, including:

- Tenant
 - VRF
 - Bridge Domain (BD)
 - Application Profile
 - Endpoint Group (EPG)
 - Contracts
 - Layer 3 Outs (L3Out)
-
-

Learning Objective

This task introduces core Cisco ACI constructs, including:

- Tenant
 - VRF
 - Bridge Domain (BD)
 - Application Profile
 - Endpoint Group (EPG)
 - Contracts
 - Layer 3 Outs (L3Out)
-

Step 1: Verify Your Assigned Tenant and EPGs

1. Log in to the APIC GUI.

POD 1-15 will have config in CLEMEA-TEST-Tenant-1.

Name	Alias	Description	Bridge Domains	VRFs	EPGs	Health Score
CLEMEA-TEST-Tenant-1	Terraform		15	1	30	Healthy
common			1	2	0	Healthy
FT_Msite_TN	H06	FT testing over Msite	1	1	1	Healthy
infra			2	2	2	Healthy
mgmt			1	2	0	Healthy
vishnair_TN			2	2	2	Healthy

A Tenant in Cisco ACI is a logical container that isolates network resources, like a virtual context or VRF in traditional networking. It allows segmentation of policies, configurations, and users, ensuring multi-tenancy. Think of it to logically group and isolate resources for different teams, applications, or customers within the same fabric.

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

Summary	Dashboard	Policy	Operational	Stats	Health	Faults	History
Application EPGs 30 Total 0 100%	Endpoint Security Groups 0 Total 0 100%	Bridge Domains 15 Total 0 100%					
VRFs 1 Total 0 100%	L2Outs 0 Total 0 100%	L3Outs 0 Total 0 100%					

An Application Profile in Cisco ACI is a logical representation of an application's network and policy requirements. It serves as a container for grouping Endpoint Groups (EPGs) that together define the components of an application (e.g., web, app, database tiers). The application profile organizes the relationships between these EPGs using Contracts to specify how they communicate. Conceptually, it maps to an application-centric view of networking, akin to defining the architecture of a multi-tier application in a traditional network.

Open your application profile and open the available Application EPGs.

Category	Total
Application EPGs	30
Endpoint Security Groups	0
Bridge Domains	15
VRFs	1
L2Outs	0
L3Outs	0

You will notice 2 EPGs assigned to your pod

An Endpoint Group(EPG) is a collection of devices (endpoints) with similar policy requirements, grouped based on function or purpose (e.g., web servers, database servers). In classical networking, this is somewhat akin to VLANs, but EPGs operate at a more abstract policy level. They are decoupled from VLANs and subnets, enabling more flexible application-centric network segmentation.

You can have full-free communication inside an EPG. We will Test this shortly.

VRF (Virtual Routing and Forwarding)

A VRF in ACI is a logical routing instance that provides isolated Layer 3 routing tables within a Tenant. It's like VRFs in traditional networks, allowing for segmentation of routing domains. Each VRF can contain multiple subnets or IP spaces, ensuring no overlap or interference between different applications or tenants.

We have one VRF per tenant configured.

Let us understand which BD these EPGs are a part of.
Click on the EPG. Head over to the Policy Tab and General Tab.
You will see a Bridge Domain for each user mentioned.

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) web interface. The top navigation bar includes links for System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations. The Tenant 'CLEMEA-TEST-Tenant-1' is selected. The main content area displays the 'EPG - CLEMEA-USER-1-EPG-1' configuration. The left sidebar lists various tenant components like Application Profiles, Application EPGs, uSeg EPGs, and Endpoint Security Groups. The right panel shows the 'Policy' tab for the EPG, with tabs for Summary, Policy, Operational, Stats, Health, Faults, and History. Under the Policy tab, there are sections for Properties (Custom QoS, Data-Plane Policer, Intra EPG Isolation, Preferred Group Member, Flood in Encapsulation), Configuration Status (applied), Configuration Issues, Label Match Criteria (At Least One), Bridge Domain (selected as CLEMEA-USER-1-BD), Monitoring Policy (select a value), FHS Trust Control Policy (select a value), and EPG Admin State (Admin Up). Buttons at the bottom include Show Usage, Reset, and Submit.

You can pop out with the Blue Pop out arrow to open the BD Settings.
Another way to navigate and see all the BDs is from the Networking tab on the left and go to bridge domains.



APIC

System

Tenants

Fabric

Virtual Net

ALL TENANTS

| Add Tenant

| Tenant Search: name or



This object was created by the Terraform orche

CLEMEA-TEST-Tenant-1



Networking

VXLAN Stretch

Bridge Domains

- > CLEMEA-USER-1-BD
- > CLEMEA-USER-2-BD
- > CLEMEA-USER-3-BD
- > CLEMEA-USER-4-BD
- > CLEMEA-USER-5-BD
- > CLEMEA-USER-6-BD
- > CLEMEA-USER-7-BD
- > CLEMEA-USER-8-BD
- > CLEMEA-USER-9-BD
- > CLEMEA-USER-10-BD
- > CLEMEA-USER-11-BD
- > CLEMEA-USER-12-BD
- > CLEMEA-USER-13-BD
- > CLEMEA-USER-14-BD
- > CLEMEA-USER-15-BD

VRFs

L2Outs

L3Outs

SR-MPLS VRF L3Outs

Dot1Q Tunnels

Contracts

Last Login Time: 2026-02-12T03:01 UTC+00:00

Let us open the BD assigned to our user. Understand which Subnet has been assigned to you as well as the gateway IP.

In this example for User-1

Gateway Address	Description	Scope	Primary IP Address	Virtual IP	Subnet Control	Matching Tag Selector
50.0.1.1/24			False	False		

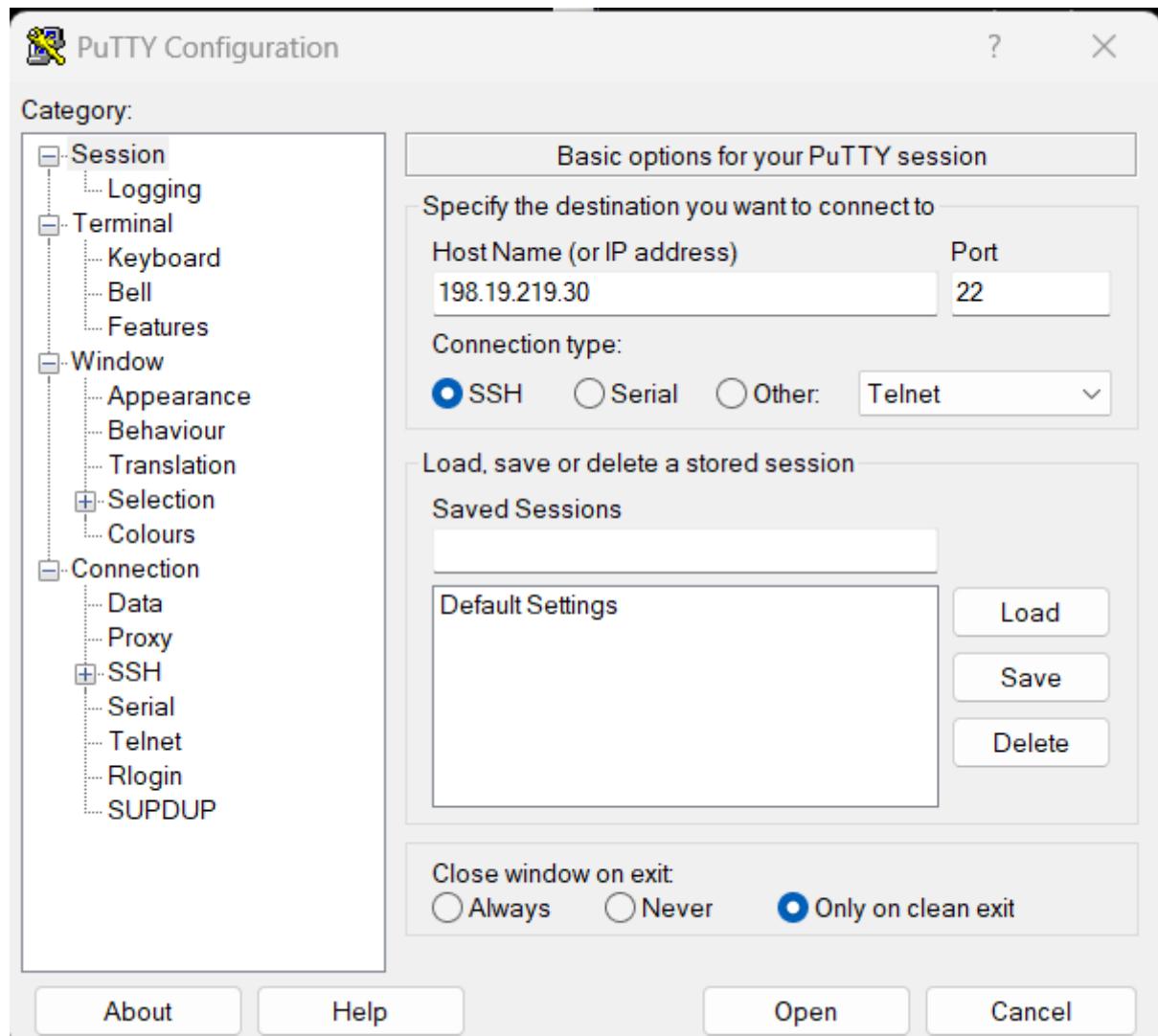
BD has a subnet of 50.0.1.0/24 and the gateway IP is 50.0.1.1

Have a look for your user and make a note of your subnet and gateway IP. This is important for the subsequent tasks.

Step 3:

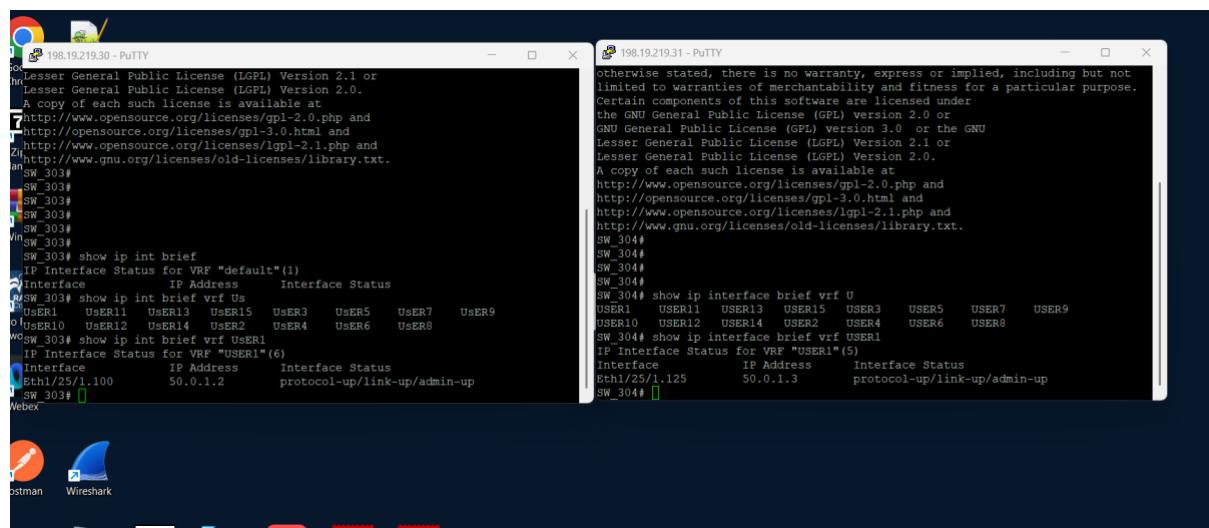
Now we will head over to the external switches SW_303 and SW_304 to verify reachability to ACI

Head over to Putty and login via the credentials (clemea/cisco!123)



Start by verifying your assigned VRF settings using 'show ip int brief vrf USER1'

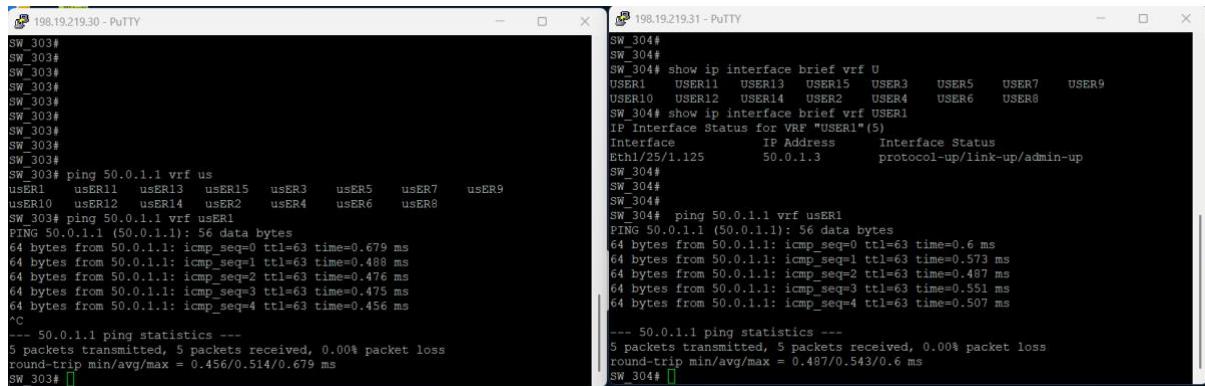
Here we have shown user 1's vrf, search for your relevant user



Start by verifying ping to your gateway that you configured on ACI.

For user X: ping 50.0.X.1 from both switches

Below is result for user 1

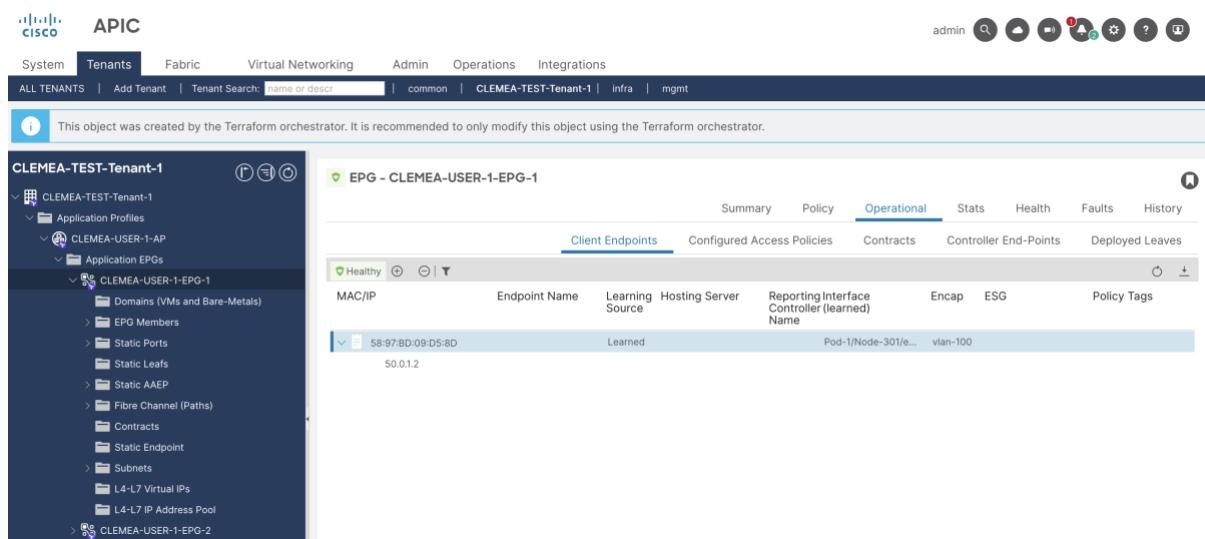


The image shows two PuTTY sessions side-by-side. The left session, titled '198.19.219.30 - PuTTY', shows a ping command being run on switch SW_303# to 50.0.1.1. The right session, titled '198.19.219.31 - PuTTY', shows a ping command being run on switch SW_304# to 50.0.1.1. Both sessions show successful ping results with low latency.

```
SW_303# ping 50.0.1.1 vrf us
usER1  usER11  usER13  usER15  usER3  usER5  usER7  usER9
usER10  usER12  usER14  usER2  usER4  usER6  usER8
SW_303# ping 50.0.1.1 vrf usER1
PING 50.0.1.1 (50.0.1.1): 56 data bytes
64 bytes from 50.0.1.1: icmp_seq=0 ttl=63 time=0.679 ms
64 bytes from 50.0.1.1: icmp_seq=1 ttl=63 time=0.488 ms
64 bytes from 50.0.1.1: icmp_seq=2 ttl=63 time=0.476 ms
64 bytes from 50.0.1.1: icmp_seq=3 ttl=63 time=0.475 ms
64 bytes from 50.0.1.1: icmp_seq=4 ttl=63 time=0.456 ms
^C
--- 50.0.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 0.456/0.514/0.679 ms
SW_303# 

SW_304# show ip interface brief vrf U
USER1  USER11  USER13  USER15  USER3  USER5  USER7  USER9
USER10  USER12  USER14  USER2  USER4  USER6  USER8
SW_304# show ip interface brief vrf usER1
IP Interface Status for VRF "USER1"(5)
Interface          IP Address           Interface Status
Eth1/25/1.125      50.0.1.3            protocol-up/link-up/admin-up
SW_304#
SW_304# ping 50.0.1.1 vrf usER1
PING 50.0.1.1 (50.0.1.1): 56 data bytes
64 bytes from 50.0.1.1: icmp_seq=0 ttl=63 time=0.6 ms
64 bytes from 50.0.1.1: icmp_seq=1 ttl=63 time=0.573 ms
64 bytes from 50.0.1.1: icmp_seq=2 ttl=63 time=0.487 ms
64 bytes from 50.0.1.1: icmp_seq=3 ttl=63 time=0.351 ms
64 bytes from 50.0.1.1: icmp_seq=4 ttl=63 time=0.507 ms
--- 50.0.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 0.497/0.543/0.6 ms
SW_304#
```

Head over to the APIC and the EPG Operational tab and verify the learning of the IP



The screenshot shows the APIC interface with the 'Tenants' tab selected. A message indicates the object was created by Terraform. On the left, the tenant 'CLEMEA-TEST-Tenant-1' is expanded, showing 'Application Profiles' and 'Application EPGs'. Under 'Application EPGs', 'CLEMEA-USER-1-EPG-1' is selected, showing its configuration. On the right, the 'Operational' tab of the 'EPG - CLEMEA-USER-1-EPG-1' page is active, displaying 'Client Endpoints'. A table lists one endpoint: MAC/IP 58:97:8D:09:D5:8D, Endpoint Name Learned, Learning Source Learned, Reporting Interface Controller (learned) Name Pod-1/Node-301/e..., Encap vlan-100, ESG, and Policy Tags.

MAC/IP	Endpoint Name	Learning Source	Reporting Interface Controller (learned) Name	Encap	ESG	Policy Tags
58:97:8D:09:D5:8D	Learned	Learned	Pod-1/Node-301/e...	vlan-100		

Repeat for EPG-2 as well

Step 4:

Now we will attempt to ping the other switch. Perform the ping and see the result

The image shows two PuTTY windows side-by-side. The left window, titled '198.19.219.30 - PuTTY', displays ping results from interface 'usER1' to 'usER9'. It shows 56 bytes being sent to each of 5 hosts, with round-trip times ranging from 0.476 ms to 0.679 ms. Below this, it shows statistics for 50.0.1.1 ping, indicating 0.00% packet loss. The right window, titled '198.19.219.31 - PuTTY', displays ping results from interface 'usER1' to 'usER9'. It shows 56 bytes being sent to each of 5 hosts, with round-trip times ranging from 0.487 ms to 0.573 ms. Below this, it shows statistics for 50.0.1.1 ping, indicating 0.00% packet loss. Both windows show a final command prompt 'sw_303#' and 'sw_304#' respectively.

```

198.19.219.30 - PuTTY
usER1  usER11  usER13  usER15  usER3  usER5  usER7  usER9
usER10  usER12  usER14  usER2  usER4  usER6  usER8
SW_303# ping 50.0.1.1 vrf usER1
PING 50.0.1.1 (50.0.1.1): 56 data bytes
64 bytes from 50.0.1.1: icmp_seq=0 ttl=63 time=0.679 ms
64 bytes from 50.0.1.1: icmp_seq=1 ttl=63 time=0.488 ms
64 bytes from 50.0.1.1: icmp_seq=2 ttl=63 time=0.476 ms
64 bytes from 50.0.1.1: icmp_seq=3 ttl=63 time=0.475 ms
64 bytes from 50.0.1.1: icmp_seq=4 ttl=63 time=0.456 ms
^C
--- 50.0.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.456/0.514/0.679 ms
SW_303# ping 50.0.1.3 vrf usER1
PING 50.0.1.3 (50.0.1.3): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
--- 50.0.1.3 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
SW_303# 

198.19.219.31 - PuTTY
SW_304#
SW_304#
SW_304# ping 50.0.1.1 vrf usER1
PING 50.0.1.1 (50.0.1.1): 56 data bytes
64 bytes from 50.0.1.1: icmp_seq=0 ttl=63 time=0.6 ms
64 bytes from 50.0.1.1: icmp_seq=1 ttl=63 time=0.573 ms
64 bytes from 50.0.1.1: icmp_seq=2 ttl=63 time=0.487 ms
64 bytes from 50.0.1.1: icmp_seq=3 ttl=63 time=0.551 ms
64 bytes from 50.0.1.1: icmp_seq=4 ttl=63 time=0.507 ms
--- 50.0.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.487/0.543/0.6 ms
SW_304# ping 50.0.1.2 vrf usER1
PING 50.0.1.2 (50.0.1.2): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
--- 50.0.1.2 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
SW_304# 

```

We can see the ping fails. This is because all communication between EPGs is blocked by default.

We therefore need to allow the communication to ping between 303 and 304.

Step 5:

We need to use contracts to allow communication.

A Contract in ACI defines the communication rules between EPGs, acting as an access control policy. It specifies what type of traffic (e.g., protocols, ports) is allowed between the consumer EPG and the provider EPG. This is analogous to access control lists (ACLs) in traditional networking but is applied at the application level with a centralized policy model.

You must now create your own contract to allow communication between these endpoints.

To create a contract, we first need a filter. This defines 'What' kind of traffic we are going to be allowing or blocking.

Head over to Contracts>Filters in our tenant

Right click filters to create a new filter



APIC

[System](#)[Tenants](#)[Fabric](#)[Virtual Netw](#)[ALL TENANTS](#)[Add Tenant](#)[Tenant Search:](#)

name or de



This object was created by the Terraform orchestration tool.

CLEMEA-TEST-Tenant-1



- ▽ CLEMEA-TEST-Tenant-1
 - > Application Profiles
 - > Networking
 - ▽ Contracts
 - > Standard
 - > Taboos
 - > Imported
 - > Filters
 - > Policies
 - > Services
- > Quick Start

[Create Filter](#)

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) web interface. The top navigation bar includes the Cisco logo, APIC, and various system status icons. The main menu has tabs for System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations. Under the Tenants tab, 'ALL TENANTS' is selected, showing tenants like 'common', 'CLUS-TEST-Tenant-1' (selected), 'vishnair_TN', 'infra', and 'CLUS-TEST-Tenant-2'. Below the tenant list is a message: 'This object was created by the Terraform orchestrator. It is recommended to only modify this object using the Terraform orchestrator.' The left sidebar for 'CLUS-TEST-Tenant-1' lists sections such as Application Profiles, Contracts (Standard, Taboos, Imported), Filters, Policies, Services, and Quick Start. A context menu for 'Filters' is open, showing options like 'Create Filter' and 'Reference'. The main content area is titled 'Contracts - Filters' and displays a table with one entry:

Name	Alias	Entries	Description
ReferenceContract-EPG1-E...		any	

At the bottom of the page are pagination controls ('Page 1 of 1'), object per page settings ('Objects Per Page: 15'), and a note 'Displaying Objects 1 - 1 Of 1'.

Name the filter CLEMEA-User-X-Filter where X is your Pod number
We will add an entry that matches 'any' traffic between our IPs

The screenshot shows the 'Create Filter' dialog box within the Cisco APIC interface. The dialog has fields for Name ('CLEMEA-User-1-Filter'), Alias (''), Description ('optional'), and Annotations ('Click to add a new annotation'). The 'Entries:' section contains a table with one row:

Name	Alias	EtherType	ARP Flag	IP Protocol	ICMPv4 Type	ICMPv6 Type	Match Only Fragments	Stateful	Source Port / Range	Destination Port / Range
any									From	To

Below the entries table is a 'Port Zero Entries:' section with a similar table structure. At the bottom right of the dialog are 'Cancel' and 'Submit' buttons.

After we hit submit, we can then proceed to creating our contract. You can name it CLEMEA-User-X where X is your pod.



APIC

System

Tenants

Fabric

Virtual Ne

ALL TENANTS

| Add Tenant

| Tenant Search: name or



This object was created by the Terraform orchestration tool.

CLUS-TEST-Tenant-1



✓ CLUS-TEST-Tenant-1

> Application Profiles

> Networking

✓ Contracts

Standard

Create Contract

Taboos

Export Contract

Imported

> Filters

> Policies

> Services

> Quick Start

Create Contract



Name: CLEMEA-User-1-Contract

Alias:

Scope: VRF

QoS Class: Unspecified

Target DSCP: Unspecified

Description: optional

Annotations: Click to add a new annotation

Subjects:



Name

Description

Cancel

Submit

Click + to add a subject

Add subject name CLEMEA-User-X-Subject

Create Contract Subject

Name:	CLEMEA-User-1-Subject
Alias:	
Description:	optional
Target DSCP:	Unspecified
Apply Both Directions:	<input checked="" type="checkbox"/>
Reverse Filter Ports:	<input checked="" type="checkbox"/>
Wan SLA Policy:	select an option

Filter Chain

L4-L7 Service Graph:	select an option
QoS Priority:	

Filters

Name	Directives	Action	Priority
CLEMEA-User-1-Filter		Permit	default level

Cancel OK

Then hit the + near filters and add the filter we just created

APIC

System Tenants Fabric Virtual Networking Admin Operations Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | CLEMEA-TEST-Tenant-1 | infra | mgmt

This object was created by the Terraform provider.

Create Contract Subject

Name:	CLEMEA-User-1-Subject	
Alias:		
Description:	optional	
Target DSCP:	Unspecified	
Apply Both Directions:	<input checked="" type="checkbox"/>	
+ Name Tenant	select an option	
+ Tenant: CLEMEA-TEST-Tenant-1	CLEMEA-U... CLEMEA-T...	
+ Tenant: common	common	
arp	common	
default	common	
est	common	
icmp	common	
Directives	Action	Priority
-Tenant-1/CLEMEA-User-1-Filter	Permit	default level

Update Cancel OK

Hit Update, OK and Submit

Now our last step is to apply these to our EPGs

Head over to the EPGs.

With contracts we have the concept of provider and consumer. In this case it does not matter which side is the provider and which the consumer so we can just go ahead and make EPG-1 our provider and EPG-2 our consumer.

Let us go ahead and right click EPG one and add provider contract;



APIC

System

Tenants

Fabric

Virtual Networking

ALL TENANTS

| Add Tenant

| Tenant Search: name or descr



This object was created by the Terraform orchestrator.

CLEMEA-TEST-Tenant-1



✓ CLEMEA-TEST-Tenant-1

✓ Application Profiles

✓ CLEMEA-USER-1-AP

✓ Application EPGs

> CLEMEA-USER-1-EPG-1

Create EPG Subnet

> CLEMEA-USER-1-EPG-2

Add VMM Domain Association

> uSeg EPGs

Add Physical Domain Association

> Endpoint Sets

Add L2 External Domain Association

> CLEMEA-USER-1-EPG-3

Add Fibre Channel Domain Association

> CLEMEA-USER-1-EPG-4

Deploy Static EPG on PC, VPC, or Interface

> CLEMEA-USER-1-EPG-5

Add Taboo Contract

> CLEMEA-USER-1-EPG-6

Add Provided Contract

> CLEMEA-USER-1-EPG-7

Add Consumed Contract

> CLEMEA-USER-1-EPG-8

Add Consumed Contract Interface

> CLEMEA-USER-1-EPG-9

Add Intra-EPG Contract

> CLEMEA-USER-1-EPG-10

Create L4-L7 IP Address Pool

> CLEMEA-USER-1-EPG-11

Delete

> CLEMEA-USER-1-EPG-12

Save as ...

> CLEMEA-USER-1-EPG-13

Post ...

> CLEMEA-USER-1-EPG-14

Share

> Networking

✓ Contracts

Open In Object Store Browser

Last Login Time: 2026-02-12T03:01 UTC+00:00

Select the contract you just created.

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) web interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations. The Tenant tab is selected, showing the tenant 'CLEMEA-TEST-Tenant-1'. The main content area displays the 'EPG - CLEMEA-USER-1-EPG-1' configuration page. A modal window titled 'Add Provided Contract' is open, prompting the user to select a contract. The 'Contract:' dropdown menu lists two options: 'CLEMEA-User-1-Contract' and 'CLEMEA-TEST-Tenant-1'. Other fields in the modal include 'QoS:', 'Contract Label:', 'Subject Label:', and 'Create Contract' buttons. The background shows the EPG configuration interface with tabs for Summary, Policy, Operational, Stats, Health, Faults, History, Topology, General, Subject Labels, and EPG Labels. A legend on the right identifies relation indicators: Provider (green), Consumer (orange), Intra EPG (blue), Provider (from Master) (purple), Consumer (From Master) (dark blue), Intra EPG (from Master) (dark green), and Master EPG (yellow-green). The bottom status bar indicates the current system time as 2026-02-12T21:46 UTC+00:00.

Repeat this to add consumed contract for EPG-2

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) web interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations. The Tenants tab is selected, showing the 'ALL TENANTS' view with a search bar and filters for common, CLEMEA-TEST-Tenant-1, FT_Msite_TN, infra, and mgmt.

In the center, a modal window titled 'EPG - CLEMEA-USER-1-EPG-2' is open under the 'Policy' tab. A context menu is displayed over the 'Add Consumed Contract' option in the list. The menu items include:

- Create EPG Subnet
- Add VMM Domain Association
- Add Physical Domain Association
- Add L2 External Domain Association
- Add Fibre Channel Domain Association
- Deploy Static EPG on PC, VPC, or Interface
- Add Taboo Contract
- Add Provided Contract
- Add Consumed Contract** (highlighted in blue)
- Add Consumed Contract Interface
- Add Intra-EPG Contract
- Create L4-L7 IP Address Pool
- Delete
- Save as ...
- Post ...
- Share
- Open In Object Store Browser

On the right side of the interface, there is a network diagram showing nodes C (CLEMEA-TEST-Tenant-1) and E (CLEMEA-USER-1-EPG-2). A blue arrow points from node C to node E, indicating a connection or association.

Select your contract again

Now test the pings.

You should be able to ping the peer switch now

Two terminal windows are shown, both titled '198.19.219.30 - PuTTY'. The left window shows ping results from SW_303# to SW_304#:

```

5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 0.456/0.514/0.679 ms
SW_303# ping 50.0.1.3 vrf usER1
PING 50.0.1.3 (50.0.1.3): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
--- 50.0.1.3 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
SW_303# ping 50.0.1.3 vrf usER1
PING 50.0.1.3 (50.0.1.3): 56 data bytes
64 bytes from 50.0.1.3: icmp_seq=0 ttl=254 time=0.97 ms
64 bytes from 50.0.1.3: icmp_seq=1 ttl=254 time=0.537 ms
64 bytes from 50.0.1.3: icmp_seq=2 ttl=254 time=0.508 ms
64 bytes from 50.0.1.3: icmp_seq=3 ttl=254 time=0.535 ms
64 bytes from 50.0.1.3: icmp_seq=4 ttl=254 time=0.493 ms
--- 50.0.1.3 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max = 0.493/0.608/0.97 ms
SW_303# 

```

The right window shows ping results from SW_304# to SW_303#:

```

5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.487/0.543/0.6 ms
SW_304# ping 50.0.1.2 vrf usER1
PING 50.0.1.2 (50.0.1.2): 56 data bytes
Request 0 timed out
Request 1 timed out
Request 2 timed out
Request 3 timed out
Request 4 timed out
--- 50.0.1.2 ping statistics ---
5 packets transmitted, 0 packets received, 100.00% packet loss
SW_304# ping 50.0.1.2 vrf usER1
PING 50.0.1.2 (50.0.1.2): 56 data bytes
64 bytes from 50.0.1.2: icmp_seq=0 ttl=254 time=0.846 ms
64 bytes from 50.0.1.2: icmp_seq=1 ttl=254 time=0.575 ms
64 bytes from 50.0.1.2: icmp_seq=2 ttl=254 time=0.508 ms
64 bytes from 50.0.1.2: icmp_seq=3 ttl=254 time=0.472 ms
64 bytes from 50.0.1.2: icmp_seq=4 ttl=254 time=0.464 ms
--- 50.0.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.464/0.573/0.846 ms
SW_304# 

```

In case you have any queries here or have issues setting this up- do not worry- let us know and we will investigate it.

Feel free to proceed with the next tasks as there are no dependencies with the previous task!

Step 5:

Open L3outs in the networking tab in your Tenant:

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations. The Tenants tab is selected, showing the tenant list: ALL TENANTS, Add Tenant, Tenant Search, common, CLUS-TEST-Tenant-1, CLUS-TEST-Tenant-2, vishnair_TN, and infra. The main content area displays the 'L3Outs' configuration for the selected tenant. A message at the top states: "This object was created by the Terraform orchestrator. It is recommended to only modify this object using the Terraform orchestrator." The 'L3Outs' table has columns for Name, Alias, Description, PIM, BGP, OSPF, EIGRP, VRF, Route Control Enforceme, L3 Domain, and PIMv6. One entry is listed: L3OUT-to-SDA, with a 'CLUS-VR...' link and an 'Export C...' button.

Open the L3OUT-to-SDA L3out

Open logical node profile

You can see that this mentions we have a router connected on node 301

The screenshot shows the Cisco APIC interface with the 'Tenants' tab selected, displaying the tenant list: ALL TENANTS, Add Tenant, Tenant Search, common, CLUS-TEST-Tenant-1, CLUS-TEST-Tenant-2, vishnair_TN, and infra. A message at the top states: "This object was created by the Terraform orchestrator. It is recommended to only modify this object using the Terraform orchestrator." The main content area shows the 'Logical Node Profile - L3OUT-to-SDA_nodeProfile' configuration for the selected tenant. The 'Properties' section includes fields for Name (L3OUT-to-SDA_nodeProfile), Description (optional), Alias (empty), Target DSCP (Unspecified), and Nodes. A table lists nodes with columns for Node ID, Router ID, and Loopback Address. One entry is shown: topology/pod-1/node-301, 1.1.1.1, 1.1.1.1. There are tabs for Policy, Faults, and History.

An L3Out is the configuration that enables Layer 3 connectivity between the ACI fabric and external networks (e.g., the internet or a traditional data center network). It is comparable

to configuring a gateway or routing instance in classical networking, providing external routing via protocols like BGP, OSPF, or static routes.

In this case- this is how we will reach our ‘external’ world which is where SDA sits. Later when we perform the integration and set up policies to share EPGs/SGTs- we will also be selecting this L3OUT.

Notice there is also an external EPG here:

The screenshot shows the Cisco ACI UI interface. At the top, there is a navigation bar with tabs: System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations. Below the navigation bar, a tenant list shows 'ALL TENANTS' with 'Add Tenant' and 'Tenant Search' fields. The main content area is titled 'External EPG - EPG-External-SDA'. It has tabs for Summary, Policy, Operational, Health, Faults, and History, with 'Policy' selected. Under the 'General' tab, there are fields for Name (EPG-External-SDA), Alias, Annotations (with a note to click to add a new annotation), Global Alias, Description (optional), and pcTag (49170). Below these are sections for Contract Exception Tag, Configured VRF Name (CLUS-VRF-TEST-1), Resolved VRF (unltn-CLUS-TEST-Tenant-1/ctx-CLUS-VRF-TEST-1), QoS Class (Unspecified), and Target DSCP (Unspecified). Configuration Status is listed as applied, and Configuration Issues are shown as none. At the bottom, there are buttons for Show Usage, Reset, and Submit.

This is where all the external traffic is grouped, and we can create relevant contracts as desired to enable communication with the outside world.

We will not be setting up end to end communication between the ACI and SDA in this lab, the objective of this lab is more to understand how segmentation is implemented in ACI and SDA and how you can simplify enforcement via this integration. We will soon be using these Contracts and EPGs once we set up the Campus side in the next task.

That brings us to the end of the Second Task. We are done setting up our ACI side and understanding how segmentation works in the ACI world.

Now it is time to move to the SDA Side.

Task 2: SDA and ISE Bringup

Step 1:

Let us first examine our set up. Head over to the CML login after connecting to vpn of your session

CML: 198.18.134.1

Username: admin

Password: C1sco12345

Based on the number/pod assigned, you will be one of the 15 users creating your own SDA network.

We will simulate the SDA network by creating a fabric using a single Cat 9k switch as a FIAB (Fabric in a box), i.e. having the role of border, control plane and edge all assigned to one box.

Your endpoint is an Ubuntu device that is pre-configured to do Dot1x, it is connected on interface Gi1/0/2 of your switch.

This authentication traffic will then leave the fabric via the Fusion device and reach to your ISE and DNAC.

Login to your respective ISE & DNAC based on the session assigned to you.

For reference, here is the table explaining the interfaces connected within CML:

Table: CML Interface Connections

Fib-1	Gi1/0/1	Fusion_1 : Gi1/0/1
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/2
Fib-2	Gi1/0/1	Fusion_1 : Gi1/0/3
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/4
Fib-3	Gi1/0/1	Fusion_1 : Gi1/0/5
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/6
Fib-4	Gi1/0/1	Fusion_1 : Gi1/0/7
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/8
Fib-5	Gi1/0/1	Fusion_1 : Gi1/0/9
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/10
Fib-6	Gi1/0/1	Fusion_1 : Gi1/0/11
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/12
Fib-7	Gi1/0/1	Fusion_1 : Gi1/0/13
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/14
Fib-8	Gi1/0/1	Fusion_1 : Gi1/0/15
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/16
Fib-9	Gi1/0/1	Fusion_1 : Gi1/0/17
	Gi1/0/2	Ubuntu

	Gi1/0/3	Fusion_1 : Gi1/0/18
Fib-10	Gi1/0/1	Fusion_1 : Gi1/0/19
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_1 : Gi1/0/20

Fib-11	Gi1/0/1	Fusion_2 : Gi1/0/1
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_2 : Gi1/0/2
Fib-12	Gi1/0/1	Fusion_2 : Gi1/0/3
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_2 : Gi1/0/4
Fib-13	Gi1/0/1	Fusion_2 : Gi1/0/5
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_2 : Gi1/0/6
Fib-14	Gi1/0/1	Fusion_2 : Gi1/0/7
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_2 : Gi1/0/8
Fib-15	Gi1/0/1	Fusion_2 : Gi1/0/9
	Gi1/0/2	Ubuntu
	Gi1/0/3	Fusion_2 : Gi1/0/10

For users of session 2, starting with fib-16, also uses the same logic as above.

However, fib 1-15 are in session 1 of CML while fib 16-30 are part of session 2 CML.

Step 2: (Theoretical)

We will start with building our SDA network from DNAC (or CatC) first, login to the UI and head to System > System 360 > Externally Connected Systems

Externally Connected Systems

Identity Services Engine (ISE)

As of Jun 12, 2025 4:51 AM

Primary	198.18.133.30		Available		Update
Secondary	198.18.133.31		Available		
pxGrid-Active	198.18.133.31		Available		
pxGrid-Standby	198.18.133.32		Available		

Click on Update to see the details of ISE integration which was already done for the convenience of all users.

The server is added as “ISE” and integrated with pxGrid enabled. We are also using both RADIUS and TACACS capabilities of ISE.

TACACS will be used for the network device login while RADIUS is for endpoint, user authentication.

Step 2: (Theoretical)

We will start with building our SDA network from DNAC (or CatC) first, login to the UI and head to System > System 360 > Externally Connected Systems

Externally Connected Systems

Identity Services Engine (ISE)

As of Jun 12, 2025 4:51 AM

Primary	198.18.133.30		Available		Update
Secondary	198.18.133.31		Available		
pxGrid-Active	198.18.133.31		Available		
pxGrid-Standby	198.18.133.32		Available		

Click on Update to see the details of ISE integration which were already done for the convenience of all users.

The server is added as “ISE” and integrated with pxGrid enabled. We are also using both RADIUS and TACACS capabilities of ISE.

TACACS will be used for the network device login while RADIUS is for endpoint, user authentication.

Step 3:

Go to Design > Network Hierarchy > You will see the area and the floor is created here for all users.

Based on your user number, verify a matching “User x Floor x” area under ‘Cisco Live’ section.

Search Help

- ✓ ⚙️ Global
- ✓ 🏙️ Europe
 - ✓ 🏙️ Amsterdam
 - ✓ 🏢 Cisco Live Building
 - ☰ User 1 Floor 1
 - ☰ User 2 Floor 2
 - ☰ User 3 Floor 3
 - ☰ User 4 Floor 4
 - ☰ User 5 Floor 5
 - ☰ User X Floor X

system will deploy these settings

✓ AAA

Select AAA or Cisco Identity

Network Client/Endpoint

Add AAA servers

Server Type

ISE AAA

Protocol

RADIUS TACACS

PAN*

Click on Amsterdam and three dots to go to Settings:

The ISE configuration is already added here which should then be inherited on your floor automatically.

Verify settings under your floor to ensure this data is present there.

▽ AAA

Select AAA or Cisco Identity Services Engine (ISE) servers for network, client, and endpoint authentication.

Network Client/Endpoint

Add AAA servers

Use the Wireless tab to configure Client/Endpoint AAA for wireless devices. [Open Wireless Settings.](#) X

Server Type
 ISE AAA

Protocol
 RADIUS TACACS

PAN*
198.18.133.30 ✖️ ▾

Last PSN sync: Jun 11, 2025 8:52 PM

Primary Server*
198.18.133.31 ✖️ ▾

Secondary Server*
198.18.133.32 ✖️ ▾

Shared Secret
***** SHOW
Warning

Similarly, using the tabs on the top menu, also verify data under Global Credentials and IP Address Pools.

'CLEMEA' and 'clemeav3' are the credentials to be used for network devices and snmp.

Step 4:

Create a Fabric Site

From main menu, go to Provision> SD Access > Fabric Sites > Create a Fabric Site

Fabric site will be created per user and this will be your own SDA network, separate from other users, with an individual IP pool, layer 3 VN and a single FIAB box connecting your user to the network.

Click through the mandatory options with 'Next' until you reach Authentication template, where Closed authentication will be selected.

This template would configure the port to do 802.1x authentication in closed mode.

Authentication Template

Select a Template for the Fabric Site. The Template will apply a port-based network access control configuration to all access ports on Edge Nodes and Extended Nodes.

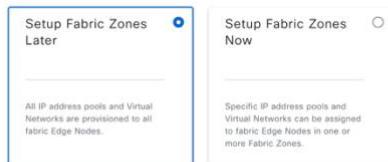
- Closed Authentication [Edit](#)
- Open Authentication [Edit](#)
- Low Impact [Edit](#)
- None [Edit](#)

Select “Setup Fabric Zone Later” as this is not in the scope of this lab activity.

Fabric Zones

Fabric Zones are optional. They reside within a Fabric Site and can only contain Edge Nodes and Extended Nodes. If Fabric Zones are used, only select Virtual Networks and Anycast Gateways (IP address pools) are provisioned to the Edge Nodes in each Fabric Zone.

If Fabric Zones are not used, all Virtual Networks and Anycast Gateways are provisioned to all Edge Nodes in the Fabric Site.



Click through the next steps till you ‘Save Intent’ and Deploy. This is saving intent as no network devices are present in your Fabric Site yet.

Continue navigating through to next part by selecting “Layer 3 Virtual Networks”

Configuration Changes Submitted

Navigate to [Activities](#) to review provisioning progress.

What's Next?

[View Layer 3 Virtual Networks](#)

[View Layer 2 Virtual Networks](#)

[View Anycast Gateways](#)

[View Fabric Sites](#)

[Create Fabric Site](#)

[Exit](#)

Create VN based on your user number.

Layer 3 Virtual Networks

Provide a name for each Layer 3 Virtual Network.
Optionally, associate a Layer 3 Virtual Network with a vManage Service VPN.

Layer 3 Virtual Network Name
User1

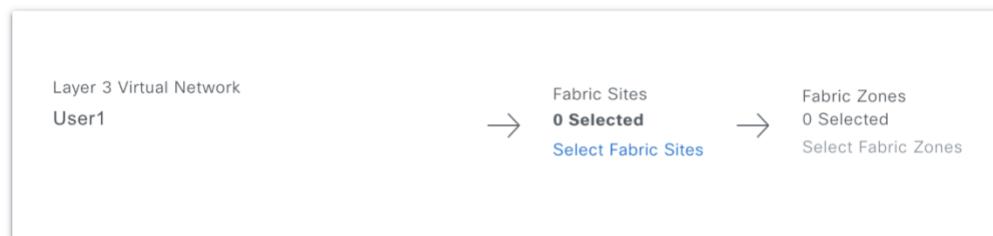
vManage Service VPN
Not Available

+

In the next steps, select the Fabric Site that you earlier created for yourself, this can easily be searched with the user number

Fabric Sites and Fabric Zones (Optional)

A Layer 3 Virtual Network can be assigned to multiple Fabric Sites and Fabric Zones. They can be assigned to a Fabric Zone within the Site. A Layer 3 Virtual Network can also be created without assigning it



Assign Fabric Sites

Assign the Layer 3 Virtual Network to one or more Fabric Sites.

Layer 3 Virtual Network: User1

Search

Add All 0 Unselected Remove All 1 Selected

No Values Available

X .../Cisco Live Building/User 1 Floor 1

Cancel Assign

Just as before, Save intent and Deploy.
Always wait for these tasks to complete.

Step 5: Using the next navigation option on the page, create Layer 2 Virtual Networks

Configuration Changes Submitted

Navigate to [Activities](#) to review provisioning progress.

What's Next?

[View Layer 3 Virtual Networks](#)

[View Layer 2 Virtual Networks](#)

[View Anycast Gateways](#)

[View Fabric Sites](#)

[View Extranet Policies](#)

[Exit](#)

Configuration Attributes

Provide a name for each Layer 2 Virtual Network and define its attributes.

LAYER 2 VIRTUAL NETWORK

VLAN Name <input type="text" value="User1"/>	VLAN ID <input type="text" value="100"/>	Traffic Type <input checked="" type="radio"/> Data <input type="radio"/> Voice
<input type="checkbox"/> Fabric-Enabled Wireless <input checked="" type="checkbox"/> Layer 2 Flooding (i)		
<input checked="" type="checkbox"/> Advanced Attributes (i)		
<input type="checkbox"/> Multiple IP-to-MAC Addresses (Wireless Bridged-Network Virtual Machine) (i)		
Fabric Site <input type="text" value=".../Cisco Live Building/User 1 Floor 1"/>	Associated Layer 3 Virtual Network <input type="text" value="User1"/>	v

Enable the advance attributes and also map your fabric site with the layer 3 VN.

Every user can create a vlan id based on their number, for example User 16 would have vlan 160 and user 17 vlan 170, and so on

Save the intent and deploy.

Step 6:

We will now start with the discovery of your network device so that it can be provisioned by CatC with the correct role.

Go to provision> Network devices > Inventory > click on Add Device to add a single device to your network.

Add Existing devices

Add existing devices in your network using one of the following methods.



Discovery



Single Device



Import Inventory

Using the Loopback IPs mentioned in the table below, enter the loopback IP of your device and then select credentials as per the image:

Add Device

CLI

Type *
Network Device ▾
 Hint
 Device IP / DNS Name*
 100.0.0.101

Credentials [Validate](#)

● Note: CLI and SNMP credentials are mandatory. Please ensure authentication will go into a collection failure state.

▽ CLI*

i Global credentials are provided only for ease of use when entering the device-specific credentials are saved. The device-to-global credential mapping is used to map the device-specific credentials to the global credentials.

Select global credential Add device specific credential

Credential*
CLEMEA ▾

▽ SNMP*

▽ SNMP*

i Global credentials are provided only for ease of use when entering the device-specific credentials are saved. The device-to-global credential mapping is used to map the device-specific credentials to the global credentials.

Select global credential Add device specific credential

V3 ▾

Credential*
clusv3 ▾

Then protocol must be set to SSH2, click Add.

Reference: This is the table with the Loopback IPs of all 15 switches in each session:

Table: FIAB Loopback IPs for claiming a device

Fiab 1	100.0.0.101
Fiab 2	100.0.0.102
Fiab 3	100.0.0.103
Fiab 4	100.0.0.104
Fiab 5	100.0.0.105
Fiab 6	100.0.0.106
Fiab 7	100.0.0.107
Fiab 8	100.0.0.108
Fiab 9	100.0.0.109
Fiab 10	100.0.0.110
Fiab 11	100.0.0.111
Fiab 12	100.0.0.112
Fiab 13	100.0.0.113
Fiab 14	100.0.0.114
Fiab 15	100.0.0.115

The session 1 has these names for the first 15 users.

With **Session 2**, the second CML session also uses the same set of loopback IPs on the devices.

So user 16 can use the same loopback as the user 1.

After adding the device, it will show up in inventory while its reachability and status will be updated in a few minutes.

The CatC will use the provided credentials to login to the device and configure/read it via SNMPv3.

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance	Site	Image Version	Last Sync
	clus-cat9k-1	100.0.0.101	Cisco	Reachable	Not Scanned	Managed	Compliant	Assign	17.15.1	56 min Sync

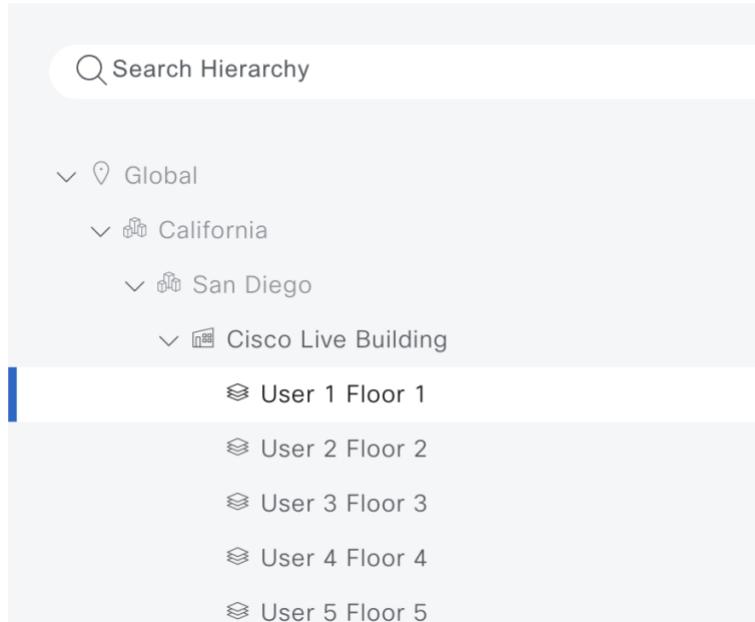
After your device shows as reachable and Managed, proceed to next step.

Step 7:

We will now assign the device to the fabric site that was created.

On the same page as step 6, click on “Assign” next to your device and proceed to select the fabric site that you created earlier.

Assign Device to Site - clus-cat9k-1

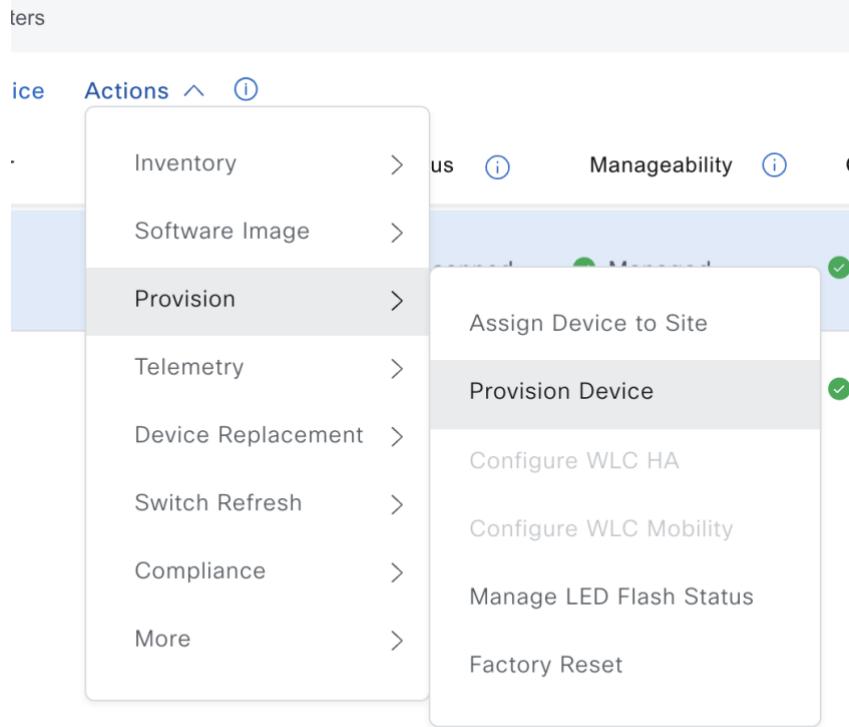


Step 8:

As the next step of building the SDA network, we must now provision our device with the configuration data present on CatC.

Provisioning a device adds all the relevant AAA servers, settings, etc. so that the device can now be used and managed via CatC.

Go back to provision> Network devices > Inventory and select your device.
Under Actions, provision the device.



Network Devices / Provision Devices

1 Assign Site 2 Advanced Configuration 3 Summary

clemea-cat9k-1

- Device Details

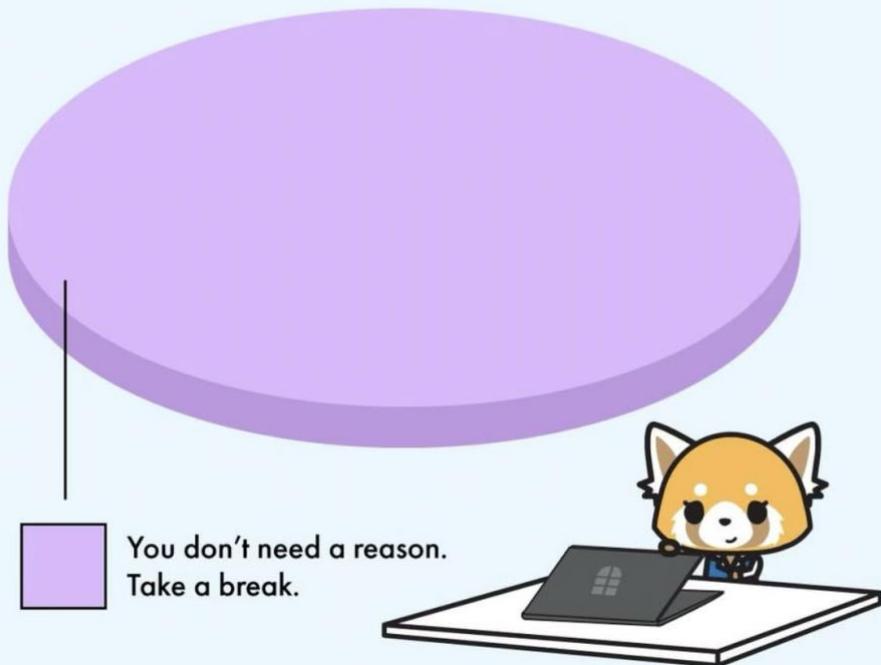
Device Name	clemea-cat9k-1
Platform Id	C9KV-UADP-8P
Device IP	100.0.0.101
Device Location	Global/Europe/Amsterdam/Cisco Live Building/User 1 Floor 1
- Network Settings

NTP Server:	217.113.224.134, 158.51.99.19
AAA Network ISE Server	198.18.133.33
AAA Network Primary Server	198.18.133.34 (RADIUS)
AAA Network Secondary Server	198.18.133.35 (RADIUS)
AAA Client ISE Server	198.18.133.33
AAA Client Primary Server	198.18.133.34 (RADIUS)
AAA Client Secondary Server	198.18.133.35 (RADIUS)
WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using this can result in you not being able to login to your devices.	
DNS Primary Server	198.18.133.1
Syslog Server	Catalyst Center
Wired Endpoint Data Collection	Yes
Cisco TrustSec (CTS) Credentials	Yes

Provisioning a device can take up to 5 mins or more. After starting this, please review the task status from Activities > Tasks.

Wait for this task to complete.

REASONS WHY YOU DESERVE A BREAK



Step 9:

The next components of an SDA network to be added are Transits and assigning device roles.

We will make use of traditional IP based transits.

Go to Provision > SD Access > Transit > Create

SUMMARY

0	0	0	0
IP-Based Transits	SD-Access Transits (LISP Pub/Sub)	SD-Access Transits (LISP/BGP)	SD-WAN Transits

Overview



Transits can connect multiple Fabric Sites or can such as a data center or the Internet. A Transit is configuration between Fabric Sites or between a

[+ Create Transits](#)

Table Preview

Transits (0 of 0)

[+ Create Transit](#)

Transit ▾	Transit Type	Peer BGP ASN	Transit Control Plane No

Transit Name and Type

Provide the Transit Name, Transit Type and associated configuration attributes.

TRANSITS

Transit Name*

User1Transit



Transit Type [\(i\)](#)

IP-Based

Remote BGP Autonomous System Number*

65412

The BGP number can be any value within a valid range.

Save intent & Deploy.

Step 10:

By now, your device provisioning must have been completed. Proceed to configure roles on this device.

Go to Fabric Sites and open your assigned fabric.

The device you provisioned and assigned must be visible here, click on it to reach this page:

clemea-cat9k-1 (100.0.0.101)

Reachable Uptime: 1 day 2 hrs 10 mins Device Role: ACCESS

Run Commands | View 360 | Last updated: 1 minute ago

Details **Fabric** Summary Advisories Field Notices Potential Field Notices VLAN Discovery Protocols

Remove From Fabric

Fabric

BN Border Node

CP Control Plane Node

EN Edge Node

Let's start by assigning the role of Border first,

Layer 3 Handoff Layer 2 Handoff

Enable Layer 3 Handoff

Local Autonomous Number
65413 (i)

BGP AS Number must be between 1 and 4294967295

Default to all virtual networks (i)

Do not import external routes (i)

Advanced

Select IP Pool (i)

Search

Select Pool

User-1-Pool (200.0.0.0/28)

User-1-Transit (200.0.0.48/28)

User-1-Transit (200.0.0.48/28)

Enable the setting as shown in the image above, also selecting the IP Transit pool reserved for your user.

Add external interface, which is always Gig 1/0/3, as described in the table earlier.

The screenshot shows the 'External Interface' configuration page for 'clus-cat9k-1'. The selected interface is 'GigabitEthernet1/0/3'. The 'Remote AS Number' is set to 65412. The 'Interface Description' field is empty. A search bar at the bottom left contains the placeholder 'Search'. Below the interface list, there is an 'Actions' section with tabs for 'Virtual Network', 'Enable Layer 3 Handoff', 'VLAN', 'Local IP Address/Mask', and 'Peer IP Address/Mask'. Under 'Virtual Network', the 'User1' tab is selected, and the 'Enable Layer 3 Handoff' switch is turned on. Under 'VLAN', the VLAN ID is set to 100. Under 'Local IP Address/Mask', the IPv4 and IPv6 fields are empty. Under 'Peer IP Address/Mask', the IPv4 and IPv6 fields are also empty.

If you had selected the IP pool in last step, then there is no need to add IP addresses/mask here.

As next step, enable Control Plane with LISP/BGP

The screenshot shows the 'Configure Control Plane' page for 'clus-cat9k-1'. It asks to 'Select route distribution protocol'. Two options are available: 'LISP Pub/Sub' and 'LISP/BGP'. The 'LISP/BGP' option is selected, indicated by a blue outline around its box. A tooltip for 'LISP/BGP' states: 'LISP/BGP uses concurrent LISP and BGP protocols to distribute reachability information. LISP/BGP is the traditional SD-Access control plane architecture and is retained for backwards compatibility. LISP Pub/Sub is recommended for new network implementations.'

Also enable Edge node.

In the end, it should look like this:



Capability

Save and deploy.

The CatC will show you the configuration before pushing:

The screenshot shows the "Modifying Fabric at User 1 Floor 1" screen in the Cisco Configuration Collector. It displays two side-by-side configuration panes: "Configuration to Be Deployed" and "Running Configuration".

Configuration to Be Deployed (521 Line(s)):

```
1 no access-session max-move deny
2 no ip name-server 198.18.133.1
3 no ip domain lookup source-interface Loopback0
4 service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
5
6 service-template DefaultCriticalVoice_SRV_TEMPLATE
7
8 voice vlan
9
9 service-template DefaultCriticalAccess_SRV_TEMPLATE
10 access-group IPV4_CRITICAL_AUTH_ACL
11 access-group IPV6_CRITICAL_AUTH_ACL
12
13 class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH_CLOSED_MODE
14 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
15
16 exit
17 class-map type control subscriber match-any IN_CRITICAL_AUTH_CLOSED_MODE
18 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
19
20 exit
21 class-map type control subscriber match-all AAA_SRV_DOWN_AUTHD_HOST
22 match authentication-status authorized
23 match result-type aaa-timeout
24 exit
25 class-map type control subscriber match-all AAA_SRV_DOWN_UNAUTHD_HOST
26 match authentication-status unauthorized
27
```

Running Configuration (552 Line(s)):

```
1 Building configuration...
2
3 Current configuration : 19413 bytes
4
5 ! Last configuration change at 01:49:15 UTC Thu Jun 12 2025 by ciscolive
6 !
7 version 17.1S
8 service timestamps log datetime msec localtime show-timestamps
9 service tcp-keepalives-in
10 service timestamps debug datetime msec localtime show-timestamps
11 service timestamps log datetime msec localtime show-timestamps
12 service timestamps server datetime msec
13 service compress-config
14 service sequence-numbers
15
16 hostname clus-cat9k-1
17 !
18 !
19 vrf definition Mgmt-vrf
20 !
21 address-family ipv4
22 exit-address-family
23 !
24 address-family ipv6
25 exit-address-family
26 !
27
```

This task can take more than a few minutes, please monitor the status from Activities > Tasks.

Step 11:

After the device has the assigned roles from the last step. Come back to the Fabric site page and go to "Port Assignment".

Every device has the Ubuntu connected to Gi 1/0/2, so this is the port to configure with Dot1x.

Fabric Sites / User 1 Floor 1

User 1 Floor 1 View Site Hierarchy Site Actions ▾ ⓘ

Fabric Infrastructure Layer 3 Virtual Networks Layer 2 Virtual Networks Anycast Gateways Wireless SSIDs Authentication

Ports (22)

Search Table

1 port(s) selected from 1 device(s) ⓘ Configure Deploy All • More Actions ▾

Device Name	Interface Name	Description	Data VLAN
clus-cat9k-1	GigabitEthernet1/0/2	--	
clus-cat9k-1	GigabitEthernet1/0/4	--	

Select the role as “User device and endpoints” and assign the appropriate vlan and template.

Configure Port Assignments

[Show Ports](#)

Connected Device Type

- Access Point
- Trunking Device
- User Devices and Endpoints

VLAN Name (Data)

User1



Security Group

Security groups are only supported on No Auth profile

VLAN Name (Voice)



Authentication Template

Closed Authentication



Description

Click on Deploy All > Apply.

Wait for this task to complete.

We have now successfully completed the SDA part of the configuration. 😊

Step 12:

We will now proceed with creating a user and policy on ISE.

For 802.1x to work, we need a policy corresponding to your username and an internal user account that can authenticate on ISE.

Login to the ISE server corresponding to your session.

Go to Administration > Identity Management > Identities > Users

Add a user based on your account

Then dot1x users must have these credentials:

Username: user1 (with the number changing based on your pod)
Password: LOveCiscoLive

Network Access Users List > user1

Network Access User

* Username: user1

Status: Enabled

Account Name Alias: [\(i\)](#)

Email: [\(i\)](#)

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration [\(i\)](#)

Never Expires [\(i\)](#)

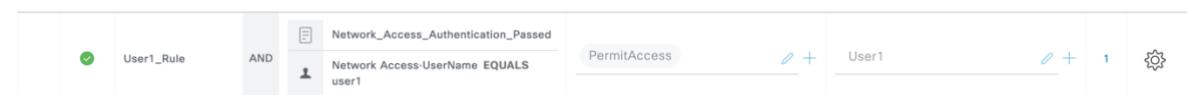
Password: Re-Enter Password:

* Login Password: [Generate Password](#) [\(i\)](#)

Enable Password: [Generate Password](#) [\(i\)](#)

Now Navigate to Policy > Policy sets > under the default policy

Under Authorization , you may see a sample policy for user1 is already created, which you can then use to duplicate and create your own specific policy.



The SGT to be assigned here can be created as described below:

Go to Work centers > Trustsec > Trustsec components and add an SGT.

If an SGT for your user does not exist yet, create it here.

[Security Groups List](#) > User1

Security Groups

* Name

* Icon



Description

Security Group Tag (Dec / Hex): 17/0011

Generation Id: 0

The SDA network is set up and ISE is configured to dynamically assign SGTs to users.

Step 12:

The next step would be to configure Ubuntu device with correct Dot1x credentials.

These devices have been pre-configured to do Dot1x on ens3 port, connected to the fabric.

Next, manually assign an IP address (from your reserved pool) and trigger a Dot1x authentication.

Login to Ubuntu console from CML

Hint: Go to CatC and look at IP address pool reservations of your Floor, to find an appropriate IP and default gateway for your endpoint.

Example of adding IP address for User1 from pool assigned to it:

```
sudo ip address add 200.0.0.18/28 dev ens3  
sudo ip route add 0.0.0.0/0 via 200.0.0.1
```

Trigger a dot1x authentication using this command:

```
sudo wpa_supplicant -c /etc/wpa_supplicant/wpa_supplicant.conf  
-D wired -i ens3
```

```
sudo wpa_supplicant -c /etc/wpa_supplicant  
Successfully initialized wpa_supplicant  
ens3: Associated with 01:80:c2:00:00:03  
ens3: CTRL-EVENT-SUBNET-STATUS-UPDATE status=0  
ens3: CTRL-EVENT-EAP-STARTED EAP authentication started  
ens3: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=13 -> NAK  
ens3: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25  
ens3: CTRL-EVENT-EAP-METHOD EAP vendor 0 method 25 (PEAP) selected  
ens3: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/CN=ISE2.securitydemo.net' hash=b4241ee5a  
ens3: CTRL-EVENT-EAP-PEER-ALT depth=0 DNS:ISE2.securitydemo.net  
ens3: CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/CN=ISE2.securitydemo.net' hash=b4241ee5a  
ens3: CTRL-EVENT-EAP-PEER-ALT depth=0 DNS:ISE2.securitydemo.net  
EAP-MSCHAPV2: Authentication succeeded  
EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed  
ens3: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully  
ens3: CTRL-EVENT-CONNECTED - Connection to 01:80:c2:00:00:03 completed [id=0 id_str=]
```

A message will appear on screen saying Authentication Succeeded if it worked.

You can also verify the assigned SGT and auth status from the console of your FIAB and from ISE live logs.

Note:

In case your ubuntu machine does not have the EAP configuration, you would need to connect ens2 to ext-connector and then run the following commands

```
sudo apt-get update  
sudo apt install wpasupplicant
```

```
cd /etc/wpa_supplicant/  
  
sudo vi wpa_supplicant.conf  
  
country=US  
ctrl_interface=/var/run/wpa_supplicant  
update_config=1  
ap_scan=0  
network={  
    key_mgmt=IEEE8021X  
    eap=PEAP  
    identity="user29"  
    password="LOveCiscoLive"  
    eapol_flags=0  
}  

```

```
sudo ip link set ens2 down
```

```
sudo ip link set ens3 up
```

Task 3: ACI and ISE integration

In this Task we will see the workflow to integrate ISE and APIC. ACME Corp is looking to start embracing common policy and wants to see how this is possible.

The basic integration has already been done for our whole infra so we will only be walking through the integration parameters in the first half of this task. In the second part, we will work with our EPGs/SGTs for several use cases.

Step 1:

Head over to the ISE and APIC on different Tabs.

On the APIC let us login and go over to the 'Integrations' tab

Name	Description	Admin State	Connection Mode	Connection Type	Servers	Topics	Actions
CLUS ISE	-	listen	ooband	pxGrid connection	2	1	...
CLUS2 ISE	-	listen	ooband	pxGrid connection	2	1	...

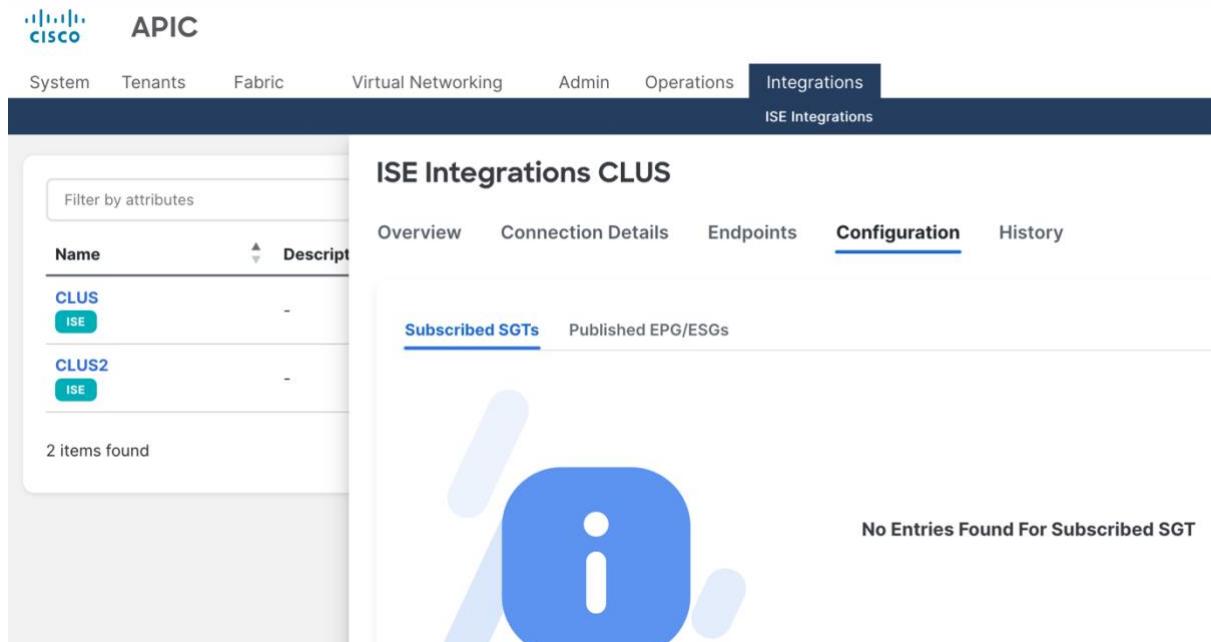
You will see 2 integrations. We will use CLEMEA1

Click on your respective connection and Connection Details

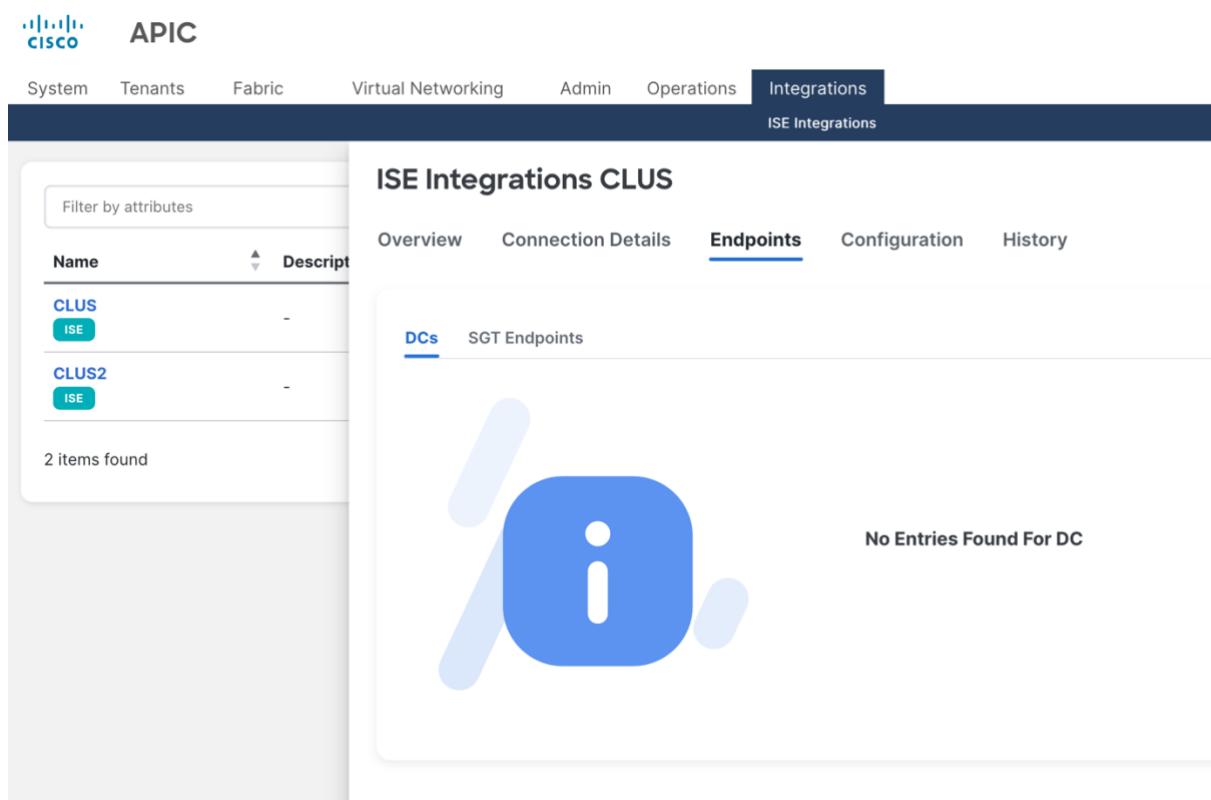
Domain Name	IP Address	Actions
ISE2	198.18.133.28	...
ISE3	198.18.133.29	...

You will see the IP of the integrated ISE

Initially the Endpoints and Configuration tabs are empty. They may have some details from other users but won't have your EPGs/SGT.



The screenshot shows the APIC interface for ISE Integrations. The top navigation bar includes System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations (which is selected). Below this is a sub-navigation bar for ISE Integrations. The main content area is titled "ISE Integrations CLUS". It has tabs for Overview, Connection Details, Endpoints, Configuration (which is selected), and History. Under the Configuration tab, there are sections for "Subscribed SGTs" and "Published EPG/ESGs". A large blue information icon is centered. Below the tabs, it says "No Entries Found For Subscribed SGT". On the left, a sidebar lists two items: "CLUS" and "CLUS2", both associated with "ISE".



The screenshot shows the APIC interface for ISE Integrations. The top navigation bar includes System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations (selected). Below this is a sub-navigation bar for ISE Integrations. The main content area is titled "ISE Integrations CLUS". It has tabs for Overview, Connection Details, Endpoints (selected), Configuration, and History. Under the Endpoints tab, there are sections for "DCs" and "SGT Endpoints". A large blue information icon is centered. Below the tabs, it says "No Entries Found For DC". On the left, a sidebar lists two items: "CLUS" and "CLUS2", both associated with "ISE".

Step 2:

All of this is auto imported and pushed when we go through the integration workflow on ISE.

Let us head over to ISE and examine the integration workflow from ISE's Perspective

Once again to remind you we will use ISE 198.18.133.33.

Once you login to your respective ISE and go to Work Centres> Integrations

The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. The top navigation bar includes links for Bookmarks, Summary (which is underlined in blue), Endpoints, Guests, Vulnerability, Threat, and a search bar. On the left, there is a sidebar with icons for Dashboard, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Work Centers' option is highlighted with a blue border. Below the sidebar, there is a link for Interactive Help and a URL at the bottom: <https://198.18.133.30/admin/#workcenters>. The main content area displays various integration modules: Network Access, Guest Access, TrustSec (with Overview and Components), BYOD (with PassiveID), Profiler, Posture, TrustSec Policy (with Policy Sets, SXP, Integrations, Troubleshoot, Reports, and Settings), and Device Administration (with Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, Reports, and Settings). A vertical scrollbar is visible on the right side of the main content area.

Click on Workload Connections to see our connection

Identity Services Engine

Work Centers / TrustSec

Bookmarks Overview Components TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

Dashboard Workload Connectors Overview Workload Connections Attributes Dictionary Workload Classification Meraki

Context Visibility Operations Policy Administration Work Centers Interactive Help

Workload Connections

Create **workload classification rules** to assign SGTs to IP addresses and receive mappings. Manage **Inbound SGT domain rules** to define the SXP domains that must receive the mappings. Manage **Outbound SGT domain rules** to define the data shared from Cisco ISE to Cisco ACI.

Q. Search table

0 Selected + Add Connection More Actions As of: Jun 12, 2025 12:14 AM

Workload Connection Name	Platform	Status	Received SGT Bindings	Sync Interval
CLUS2	ACI	Error	---	RealTime

1 Record(s) Show Records: 10 1 - 1 1 >

Click on the connection to examine how it integrates with ACI

Identity Services Engine

Work Centers / TrustSec

Bookmarks Overview Components TrustSec Policy

Dashboard Workload Connectors Overview Workload Connections Attributes Dictionary Workload Classification Meraki

Context Visibility Operations Policy Administration Work Centers Interactive Help

ACI Connections Details

rules to defin Configuration Name Conversion Synced EPG/ESGs SGT Numbering Range

ACI Connection Name* CLUS2 FQDN or IP Address* apic.securitydemo.net

Non-editable after creation

ACI Username* admin ACI Password

Login Domain No Domain View Details

Validate ACI certificate

LEARNED FQDN OR IP ADDRESSES 198.19.219.49 In Service

Cancel Save

ACI Connections Details

EPG/ESG name	Generated SGT Name	Type
CLUS-USER-1-EPG-1	CLUS_USER_1_EPG_1_CLUS_TEST_Tenant_1_CLUS_USER_1_AP_EPG	CI
CLUS-USER-1-EPG-2	CLUS_USER_1_EPG_2_CLUS_TEST_Tenant_1_CLUS_USER_1_AP_EPG	CI
CLUS-USER-10-EPG-1	CLUS_USER_10_EPG_1_CLUS_TEST_Tenant_1_CLUS_USER_10_AP_EPG	CI

63 Record(s) Show Records: 10 < 1 2 3 4 5 6 7 >

Cancel **Save**

Step 3:

Select the 2 EPGs you have been assigned and select Save.

ACI Connections Details

EPG/ESG name	Generated SGT Name	Type
<input checked="" type="checkbox"/> CLUS-USER-1-EPG-1	CLUS_USER_1_EPG_1_CLUS_TEST_Tenant_1_CLUS_USER_1_AP_EPG	CI
<input checked="" type="checkbox"/> CLUS-USER-1-EPG-2	CLUS_USER_1_EPG_2_CLUS_TEST_Tenant_1_CLUS_USER_1_AP_EPG	CI
<input type="checkbox"/> CLUS-USER-10-EPG-1	CLUS_USER_10_EPG_1_CLUS_TEST_Tenant_1_CLUS_USER_10_AP_EPG	CI

63 Record(s) Show Records: 10 < 1 2 3 4 5 6 7 >

Cancel **Save**

Be careful in case someone else is saving as well at the same time- it may need you to resave.

This concludes the workflow of integration between ACI and ISE.

In the Next Task we will use Inbound and Outbound policies for communication

Please do reach out if you have any questions so far as the next task will require clear understanding of SGTs and EPGs/Contracts.

Task 4: Inbound and Outbound Policies

Inbound and Outbound Policies

We will now go over the use cases and options to integrate.

Go to Work Centers and SXP Menu and head to the Inbound and outbound SGT Rules Tab.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, a search bar, and various icons. The main menu bar has tabs for Overview, Components, TrustSec Policy, Policy Sets, SXP (which is highlighted in blue), Integrations, Troubleshoot, Reports, and Settings. On the left, a sidebar lists Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, and Work Centers (which is also highlighted). Under the Work Centers section, there is an 'Interactive Help' link. The main content area is titled 'Inbound & Outbound SGT Domain Rules' and describes creating rules to define data shared between Cisco ISE and Cisco ACI. It shows a table with columns for Inbound Rule Name, Status, Destinations, SGT Bindings, and Actions. One record is listed: 'Default-inboun...' with status 'Active' and destination 'default'. At the bottom, there are buttons for 'Add Inbound Rule', 'Search table', and 'Save'.

Create a rule by clicking on Add Imbound Rule

You may create a new destination with your user name. Make sure to add the 2 EPGs assigned to your user name

Add Inbound Rule

Rule Settings

Inbound Rule Name*
CLUS-User1-InboundRule

Status
 Enabled Disabled

Destination Configuration

Destinations *

CLUS-User1-Domain X

Rule Configuration

AND

EPG Equals CLUS-USER-1-EPG-1

EPG Equals CLUS-USER-1-EPG-2

+ Add AND/OR Statement + Add Condition

Cancel Preview Add

This way you can use the EPG related classifier on the SDA side.

Now let us check outbound policy. Make sure to save before.

Identity Services Engine Work Centers / TrustSec

Bookmarks Overview Components TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Inbound & Outbound SGT Domain Rules

Create inbound and outbound SGT domain rules to define and manage the data shared between Cisco ISE and Cisco ACI.

Inbound SGT Domain Rules Outbound SGT Domain Rules

Search table

* One or more ACI Connections are in Disconnected state. It is not possible to create, modify, or delete Outbound SGT Disconnected connection(s).

+ Add Outbound Rule

Outbound Rule Name Status Destinations

No data to display

Save

Go over to the outbound policy tab and click on Add Outbound Rule

Add Outbound Rule

Rule Settings

Outbound Rule Name* Status Enabled Disabled

Destination Configuration

Destinations * Destinations CLUS L3 Outs *

Rule Configuration ⓘ

Equals

+ Add AND/OR Statement + Add Condition

Cancel Preview Add

You can make it match the previously created SGT that you used.

Add Outbound Rule

Rule Settings

Outbound Rule Name* Status Enabled Disabled

Destination Configuration

Destinations * Destinations CLUS L3 Outs *

Rule Configuration ⓘ

Equals

+ Add AND/OR Statement + Add Condition

Contract Configuration

SGT Name Connection/ Tenant/ L3out Consumed Contract ⓘ Provided Contract ⓘ

Cancel Preview Add

We then also need to show which contract we use for which communication. Select the Contract we used in Task 1 as both consumed and provided.

The screenshot shows the 'Add Outbound Rule' configuration page in the Cisco ISE interface. The 'Rule Configuration' section contains a search bar with 'SGT Name' set to 'User1' and 'Connection Mode' set to 'Equals'. Below it are buttons for '+ Add AND/OR Statement' and '+ Add Condition'. The 'Contract Configuration' section shows a table with one record for 'User1'. The table has columns for 'SGT Name', 'Connection/ Tenant/ L3out', 'Consumed Contract', and 'Provided Contract'. The 'Consumed Contract' and 'Provided Contract' fields both show 'CLUS-TEST-Tenant-1 CONTRACT X'. At the bottom of the page, there are pagination controls showing '1 Record(s)' and 'Show Records: 10 1 - 1 1 >'. At the very bottom right are three buttons: 'Cancel', 'Preview', and a blue 'Add' button.

Add and then proceed to save.

Now let us head over to ACI and look at what this config caused.

Select the correct Connection Instance

The screenshot shows the Cisco APIC interface with the 'Integrations' tab selected. Under the 'ISE Integrations' section, a table displays two connection instances: 'CLUS' and 'CLUS2'. Each entry has an 'ISE' icon next to its name. The table has columns for 'Name', 'Description', 'Admin State', 'Connection Mode', 'Connection Type', 'Servers', and 'Topics'. The 'CLUS' entry has 'publish-and-listen' in 'Description', 'ooband' in 'Connection Mode', 'pxGrid connection' in 'Connection Type', '2' in 'Servers', and '2' in 'Topics'. The 'CLUS2' entry has similar values. At the bottom of the table, it says '2 items found' and 'Rows per page: 15'.

When you check the endpoints Tab, you see all the learnt endpoints from ACI side

ISE Integrations CLUS

Refresh Actions ×

Overview Connection Details Endpoints Configuration History

SGT Endpoints					
IP Address	Tenant	Application Profile	EPG/ESG	VRF	
50.0.1.2	CLUS-TEST-Tenant-1	CLUS-USER-1-AP	CLUS-USER-1-EPG-2 EPG	CLUS-VRF-TEST-1	...
50.0.1.3	CLUS-TEST-Tenant-1	CLUS-USER-1-AP	CLUS-USER-1-EPG-1 EPG	CLUS-VRF-TEST-1	...
50.0.1.5	CLUS-TEST-Tenant-1	CLUS-USER-1-AP	CLUS-USER-1-EPG-1 EPG	CLUS-VRF-TEST-1	...

3 items found

Rows per page 15 < 1 >

Additionally when we move to configuration tab, we see that we are Subscribed to ISE_User1 and Publish EPG 1 and 2 for our user

ISE Integrations CLUS

Refresh Actions ×

Overview Connection Details Endpoints Configuration History

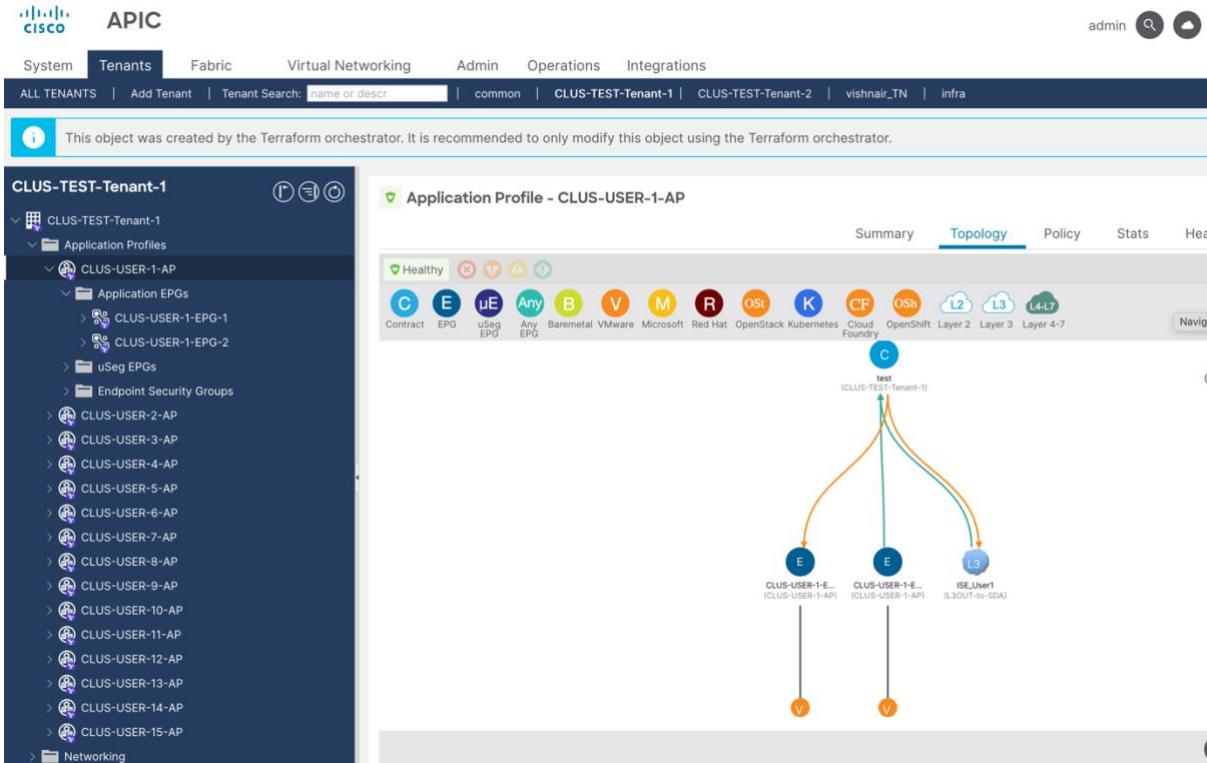
Published EPG/ESGs					
EPG/ESG	Tenant	Application Profile	Contracts	DC Bindings	
CLUS-USER-1-EPG-1 EPG	CLUS-TEST-Tenant-1	CLUS-USER-1-AP	View All	View All	...
CLUS-USER-1-EPG-2 EPG	CLUS-TEST-Tenant-1	CLUS-USER-1-AP	View All	View All	...

2 items found

Rows per page 15 < 1 >

You can then go to verify how the contracts have been set up

Head over to Tenants and your tenant and AP and click on topology:



You can see the communication established to and from the external EPG via the same contract we created.

This shows how we can leverage and set up common policy either via an APIC or ISE/SGT enforcement.

Task 5 (Theoretical/Discussion): Models- how and where to control policies

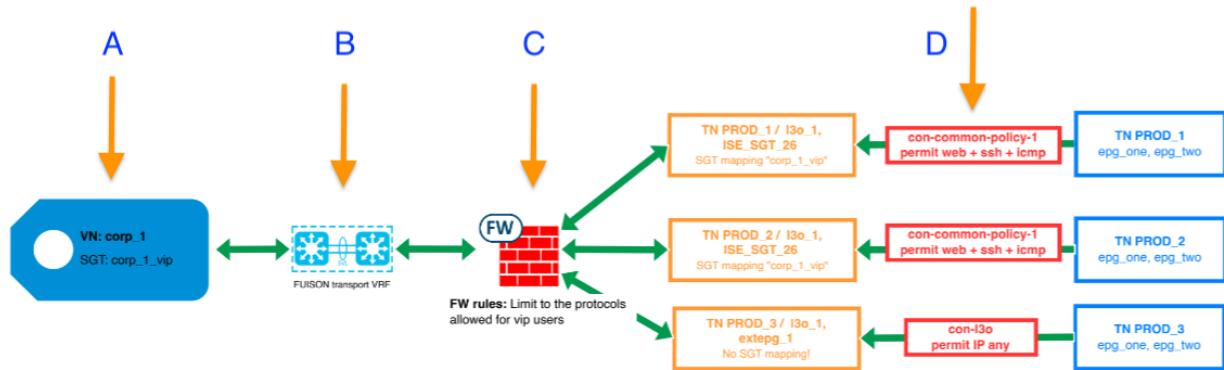
Overview

- Control points to enforce the policies
- Considerations where and how to enforce policies
- Start point, what to enforce where in the path.

No lab, will be purely a discussion/theoretical section in the below fictional scenario.

Control Points on the Path

As shown in diagram below, there are 4 points where policy could be enforced via ISE exchange, information of SDA SGTs and ACI EPGs.



(A) ISE policies Via the ISE and TrustSec Policy Egress Policy Matrix, the SGTs as well the EPGs will be visible. Via the matrix in ISE below, policies could be added from simple "deny IP" or "allow IP" towards permit or deny protocols similar to ACL

The screenshot shows the TrustSec Policy interface with the 'TrustSec Policy' tab selected. On the left, there's a sidebar with 'Egress Policy' and 'Matrices List' sections, and a 'Network Device Authorization' section. The main area displays a table for 'Egress Policy' with columns for Destination (with dropdowns for 'Source'), Source (with dropdowns for 'Destination'), and various status and configuration fields like 'Deploy', 'Verify Deploy', 'Monitor All - Off', 'Import', 'Export', and 'View'. The table rows represent different network devices and their associations.

Source	Destination	Deploy	Verify Deploy	Monitor All - Off	Import	Export	View
corp_1_employee 25/0019	4/0004 epg_one_fabric... 10000/2710						
corp_1_isolated 32/0020	epg_one_fabric... 10001/2711						
corp_1_lan 18/0012	epg_two_fabric... 10002/2712						
corp_1_printer 27/0018	epg_two_fabric... 10003/2713						
corp_1_vip 26/001A	Extranet 17/0011						
corp_1_wlan 19/0013	guest_lan 22/0016						
	guest_supplier... 30/001E						
	guest_supplier... 31/001F						

(B) WAN Traffic Engineering In the lab we are using a Fusion router, which represents the WAN. The next step for common policy, is that the SGT and EPG information is distributed to SDWAN. What could be done is, that inside of SDWAN Traffic Engineering is used to provide certain SGT to EPG traffic more bandwidth or preferred path.

(C) Firewall Rules: In current setup there is no firewall in the path from SDA fabrics towards ACI. Today the firewall can join pxGrid and receive the SGT as well the EPG information. The result would be, that firewall rules can be applied based on SGT and EPG information used in the other domains.

Because in SDA it is quite common that one IP pool is shared by multiple SGTs, to define a firewall rule set based on IPs is very hard. To be precise either host IPs must be added dynamically to ISE, or IP pool per SGT must be added.

In ACI it is not common to use one Bridge Domain for different EPGs, but the usage of ESGs is increasing. With the use of ESGs, similar situation will occur, one network / one Bridge Domain could be used for many ESGs.

(D) ACI contracts attached to SGT external EP: In the current lab setup, this is the only method applied. The ISE controls which SGTs in SDA will be transported to which ACI tenant. For each SGT transported, one external EPG will be setup by ISE. The contracts in ACI, in the lab setup for example "con-common-policy-1", will be defined in AAC and rolled out towards ACI. As well in AAC the association which EPGs will be provider for the contract, is done.

But the control which ACI external EPG represents a SGT, will consume which contract, is done via ISE!

Results are:

- The granularity of control, like only "permit IP" to certain protocols, is done in AAC / ACI.
- Which path is allowed or simply blackholed, like in tenant PROD_2 for "corp_1_isolated" is done ISE.

Which Control Points to use?

Control at every point to maximum granularity is probably no good idea. One suggestion, even maybe easy start point:

- Permit IP / deny IP in SDA from SGTs towards outside "ACI SGTs"
- Permit IP / deny IP in ACI from EPGs to "external EPG SGTs" via contracts
- Granular filters for protocols on the firewalls

Matrix for pro and cons for different models

- Suggestion for models:
 - (1) Simple model above
 - (2) All control on ISE via policies, no control in ACI, some rules on Firewall
 - (3) All control in ACI via contract, no control on ISE, some rules on Firewall
 - (4) No rules on ISE and ACI, all rules on Firewall

For WAN the policy enforcement is not to allow or drop certain traffic. For WAN the enforcement would be to provide certain traffic e.g. higher or lesser bandwidth.

Enforcement Point	Pro	Con
TrustSec Policy SDA Fabric	<ul style="list-style-type: none">• Less Unknown Tagged traffic inside the Fabric• Dropping traffic as early as possible for traffic originated in Campus	<ul style="list-style-type: none">• Stateless• Needs SXP to each Bordernode -> Scaling Issues

Enforcement Point	Pro	Con
		<ul style="list-style-type: none"> • Needs to learn every IP-SGT binding of every Fabric -> Scaling Issues
WAN Traffic Engineering	Traffic Engineering not possible on other enforcement points	If no Traffic Engineering based on policies is required, don't use it
Firewall	<ul style="list-style-type: none"> • Stateful • Uses pxGrid as transportation protocol, no scaling concerns of SXP • SGT based Ruleset instead of IP Based Ruleset 	<ul style="list-style-type: none"> • Throughput -> Scaling Issues
ACI	<ul style="list-style-type: none"> • Datacenter Admin keeps Control of Datacenter • Uses pxGrid as transportation protocol, no SXP is required to Border Nodes • Dropping traffic as early as possible for data center originated traffic 	<ul style="list-style-type: none"> • Stateless • Needs to learn every IP-SGT binding of every Fabric -> Scaling Issues
Combination of enforcement points above	<ul style="list-style-type: none"> • A Mix of Enforcement Points can fix the Issues of Others like scale and/or granularity of policies • Possible to use enforcement points with only "drop/permit" and one other with more granular policies 	<ul style="list-style-type: none"> • Not a clear vision where traffic got dropped -> Troubleshooting Issues

Appendix: Use Cases on Common Policy

1. The obvious and underestimated, no enforcement via SGTs / EPGs
 - Considerations:
 - There is no difference between hosts from SDA or endpoints from ACI.
 - Could be useful for infrastructure services required by all users in all SGTs and all VRFs.
 - Could also help for scale considerations, no need to learn the ACI endpoints or SDA host mappings.
 - Might be the most difficult one, because it is hard to generalize.
2. Keep the doors open for the not-categorized
 - Considerations:
 - Special rules might apply for some SGTs.
 - Other hosts of SGTs also need to access the resources, but can be treated as "default"
 - There might also be hosts, which are not tagged anyhow with SGTs
3. Different eligibility between identified hosts

- Consideration:
 - The identified hosts are grouped into different SGTs and get different eligibility.

4. Lower eligibility for "bad-hosts" SGTs

- Considerations:
 - Due to security reasons, some groups might get lower eligibility than groups of identified hosts via SGTs and even "default groups".
 - This could be the use case for malware infected host which are moved into quarantine or isolation, versus more rights for known hosts.

5. Block "bad-hosts" SGTs from resources

- Considerations:
 - The "bad-hosts" shouldn't have access to defined resources at all.
 - The "bad-hosts" will be grouped via SGTs
 - Goal would be to black-hole the access for "bad-hosts".

6. Some SGTs require same eligibility

- Considerations:
 - The eligibility for certain resources are the same for different group of hosts identified by SGTs.
 - To minimize the maintenance effort and to keep the solution scaleable, the same rules should be used.

7. Not-categorized hosts shouldn't have access

- Considerations:
 - End devices which are attached to a SGT, are allowed to access resources.
 - The eligibility of identified hosts, might be different
 - Other end devices which are not-categorized and learned via SGT, shouldn't have any access to resources.