



LTRANS-2891

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

Shivam Kumar, Achintya Murali

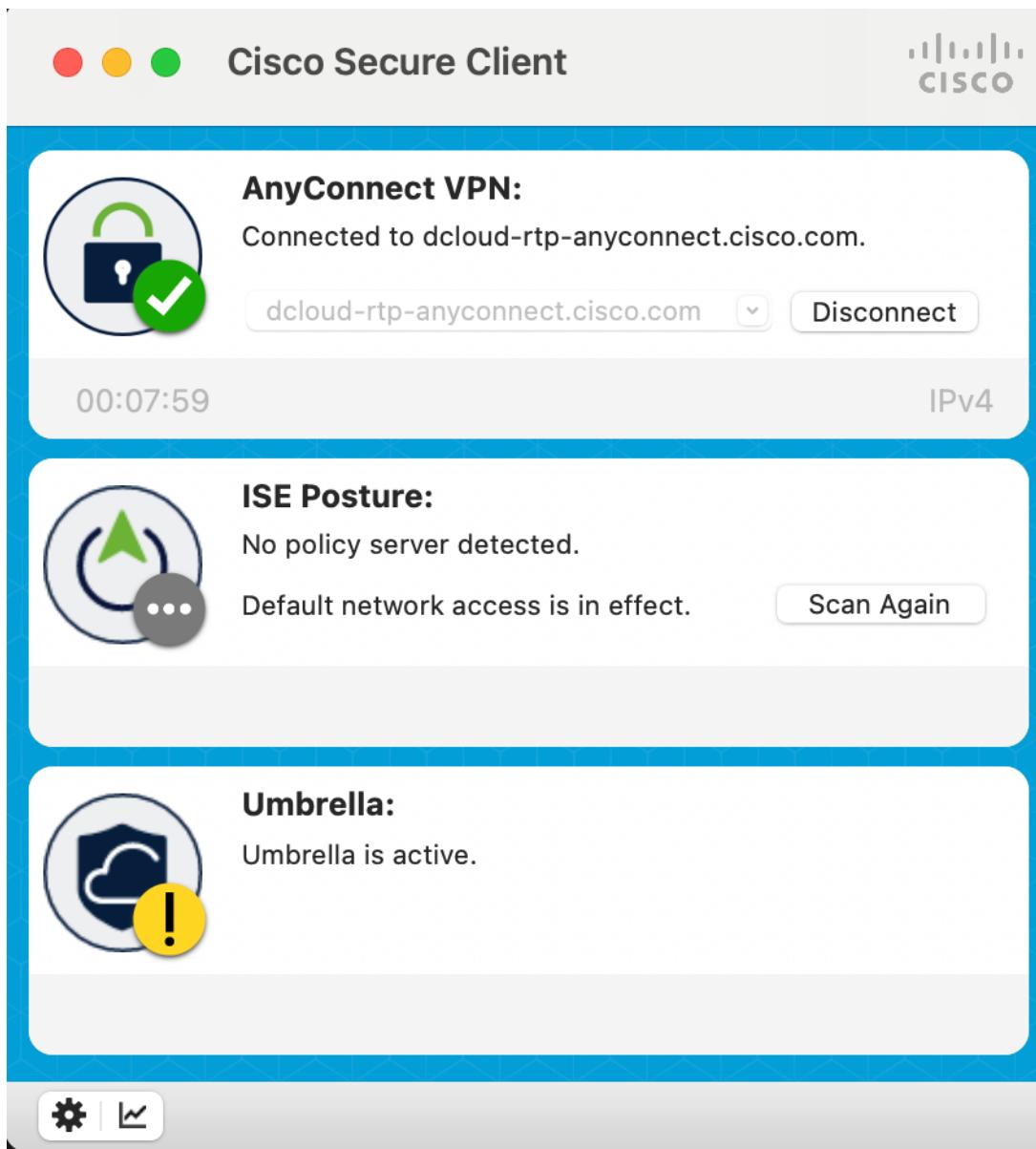
Copyright © 2025 Cisco

- **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.
5. Lab Objectives:
 - 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 your 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 in the future.

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

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

Access Details

Always keep this open on one screen/Tab!

ACI: <https://198.19.219.49>

Username: CLUS

Pass: CiSc0L@ve!

VCenter: 198.19.219.58

Username: administrator@vsphere.local Password: C1sco12345!

Please add the following entry to your local hosts file:

- 198.19.219.58 cx-aci-beta-vc1.dcv.svprod cx-aci-beta-vc1

Go to File > Open and select C:\windows\system32\drivers\etc\hosts

- **At the bottom of the file, add a host entry by specifying an IP address**

and host; for example:

192.168.1.1 example.awingu.com

DNAC:

Session 1 (Users 1-15): <https://198.18.129.100/>

Session 1 (Users 16-30): <https://198.18.129.110/>

Username: dcloud

Password: C1sco12345

ISE

Session 1 (Users 1-15) 198.18.133.30

Username: admin

Password: C1sco12345

Session 2 (Users 16-30) 198.18.133.27

Username: admin

Password: C1sco12345

ACI Ubuntu VMs:

Password: C1sco12345!

CML Ubuntu Endpoints:

Username: cisco

Password: cisco

CML:

For both sessions: 198.18.134.1

Username: admin

Password: C1sco12345

FIAbs:

Username: ciscolive

Password: C1sco12345

Dcloud:

Host

dcloud-rtp-anyconnect.cisco.com

Session 1:

User: v968user1

Password: b9fc8d

Session 2:

User: v2318user1

Password: 0a7013

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

In this Task- we will be configuring our ACI environment.

Scenario:

ACME Corp is expanding from the data center side as well and have decided to start using ACI for this.

They have a single site with 2 ACI Leafs and a Spine, with compute on a VMware environment.

Learning Objective:

To understand ACI concepts of Tenant, VRF, Application Profile, EPG, BD, Contract and L3out.

Step 1:

Let us first examine our set up. Head over to the APIC and login

Click on the Tenant tab

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

POD 16-30 will have config in CLUS-TEST-Tenant-2.

Name	Alias	Description	Bridge Domains	VRFs	EPGs	Health Score
CLUS-TEST-Tenant-1	Terraform		15	1	30	Healthy
CLUS-TEST-Tenant-2	Terraform		15	1	30	Healthy
common			1	2	0	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.

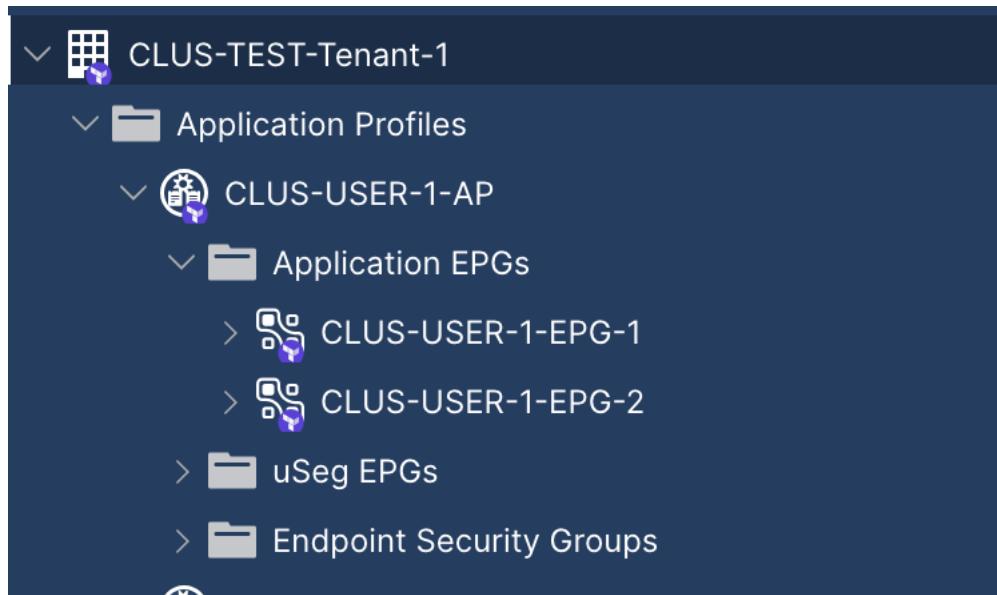
Click on your Tenant and head over to application profiles

The screenshot shows the Cisco Application Catalog interface for the tenant 'CLUS-TEST-Tenant-1'. The left sidebar lists various application profiles under the main tenant. The 'Application Profiles' section contains 15 entries, each representing a user application profile.

- > Application Profiles
 - > CLUS-USER-1-AP
 - > CLUS-USER-2-AP
 - > CLUS-USER-3-AP
 - > CLUS-USER-4-AP
 - > CLUS-USER-5-AP
 - > CLUS-USER-6-AP
 - > CLUS-USER-7-AP
 - > CLUS-USER-8-AP
 - > CLUS-USER-9-AP
 - > CLUS-USER-10-AP
 - > CLUS-USER-11-AP
 - > CLUS-USER-12-AP
 - > CLUS-USER-13-AP
 - > CLUS-USER-14-AP
 - > CLUS-USER-15-AP

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.



You will notice 2 EPGs

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 tabs for System, Tenants, Fabric, Virtual Networking, Admin, Operations, and Integrations. The Tenant search bar shows "ALL TENANTS" and the selected tenant is "CLUS-TEST-Tenant-1". The main content area is titled "EPG - CLUS-USER-1-EPG-1". It has tabs for Summary, Policy (selected), Operational, Stats, Health, Faults, and History. Below these are sub-tabs for Topology, General (selected), Subject Labels, and EPG Labels. The General tab displays various configuration parameters such as Contract Exception Tag, QoS class, Custom QoS, Data-Plane Policy, Intra EPG Isolation (set to Enforced), Preferred Group Member (Exclude), Flood in Encapsulation (Enabled), Configuration Status (failed-to-apply), Configuration Issues (BD IDs Not Allocated, Context Not present), Label Match Criteria (At Least One), and Bridge Domain (CLUS-USER-1-BD). A note at the bottom states "Resolved Bridge Domain: CLUS-TEST-Tenant-1/CLUS-USER-1-BD". At the bottom right are buttons for 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 orchestration tool.

CLUS-TEST-Tenant-1



CLUS-TEST-Tenant-1

> Application Profiles

> Networking

> VXLAN Stretch

> Bridge Domains

> CLUS-USER-1-BD

> CLUS-USER-2-BD

> CLUS-USER-3-BD

> CLUS-USER-4-BD

> CLUS-USER-5-BD

> CLUS-USER-6-BD

> CLUS-USER-7-BD

> CLUS-USER-8-BD

> CLUS-USER-9-BD

> CLUS-USER-10-BD

> CLUS-USER-11-BD

> CLUS-USER-12-BD

> CLUS-USER-13-BD

> CLUS-USER-14-BD

> CLUS-USER-15-BD

> VRFs

> L2Outs

> L3Outs

> SR-MPLS VRF L3Outs

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

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 current tenant is CLUS-TEST-Tenant-1. A search bar at the top right allows searching by name or description. The main content area is titled "Subnets". On the left, a tree view shows the tenant structure: CLUS-TEST-Tenant-1, Application Profiles, Networking, VXLAN Stretch, Bridge Domains (with BD 1-15 listed), and Subnets. The Subnets table lists one entry:

Gateway Address	Description	Scope	Primary IP Address	Virtual IP	Subnet Control	Matching Tag Selector
50.0.1.0/24				False	False	ND RA Prefix

At the bottom of the interface, there are pagination controls (Page 1 of 1), object per page settings (15), and a note indicating 1 object displayed. The status bar at the bottom right shows the current system time as 2025-06-09T22:41 UTC+0000.

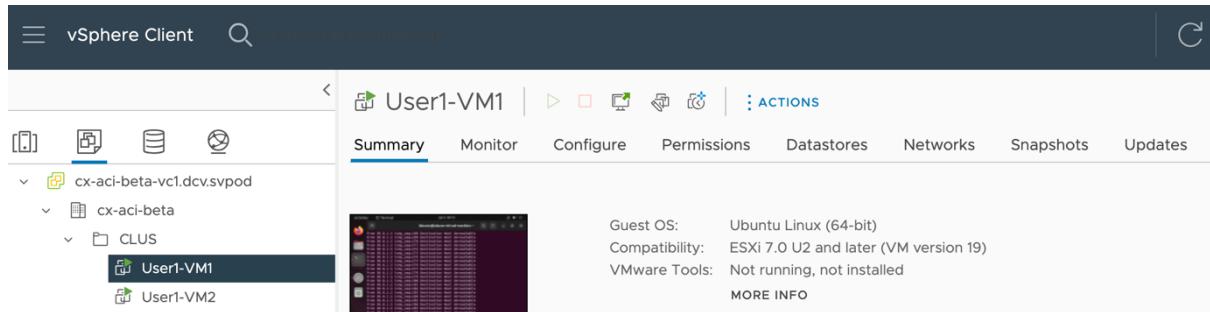
BD has a subnet of 50.0.1.0/24 and the gateway IP is 50.0.1.1
Have a look for your user and make a note of your subnet and gateway IP. This is important for the subsequent tasks.

Step 2:

Now we will head over to the Vcenter (<https://198.19.219.58>) and set up reachability from our Test VMs to the ACI fabric.

Login using the given credentials and head over to VMs tab and the CLUS folder under cx-aci-beta

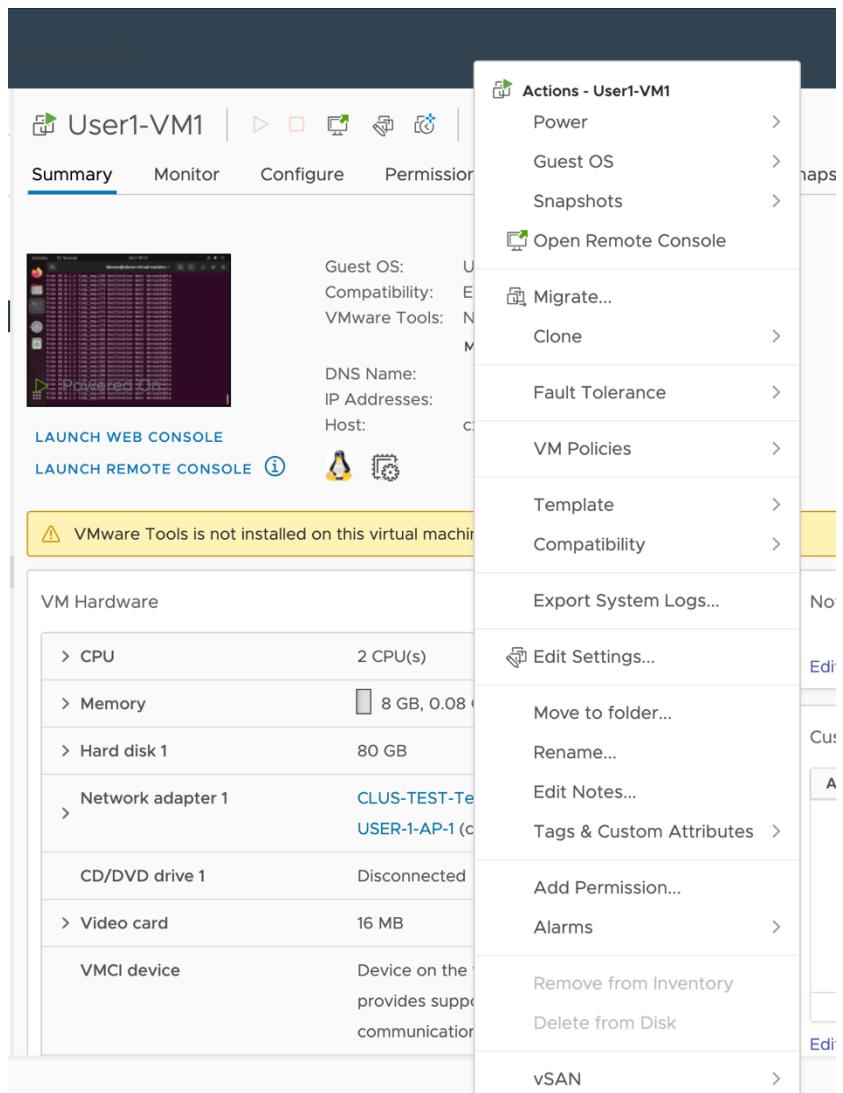
In case the Vcenter is not reachable- make sure to add the hosts entry or reach out to one of us.



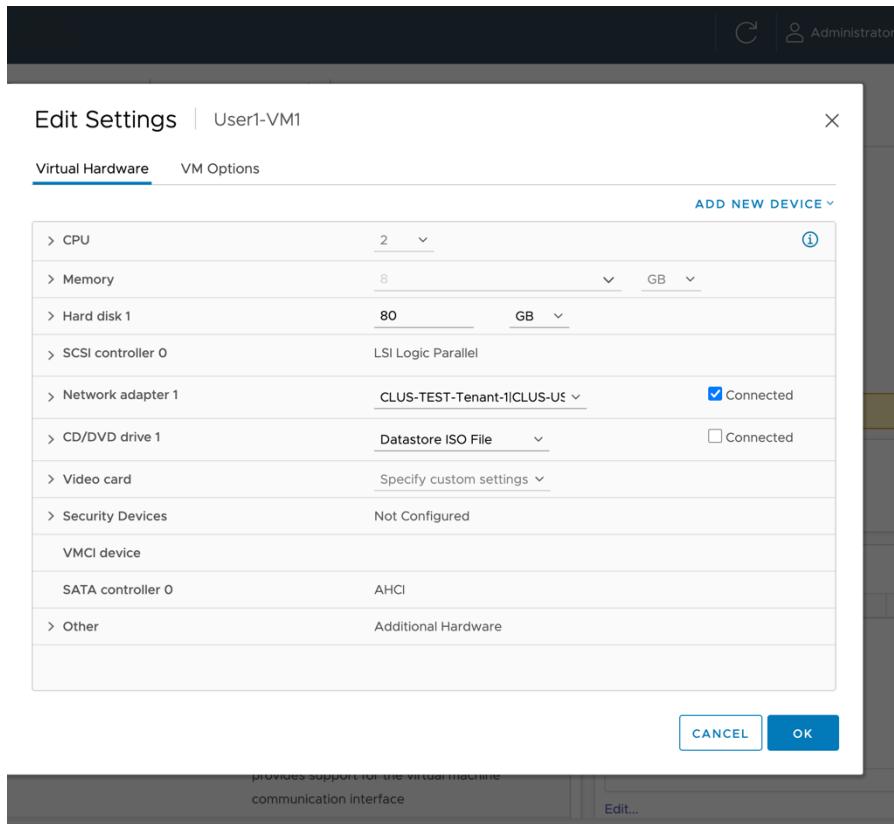
You will see 2 VMs per user. In this example User1 has 2 VMs.

The ACI-VMM integration enables the creation of port-groups automatically for our EPGs- therefore simplifying how we do virtual networking.

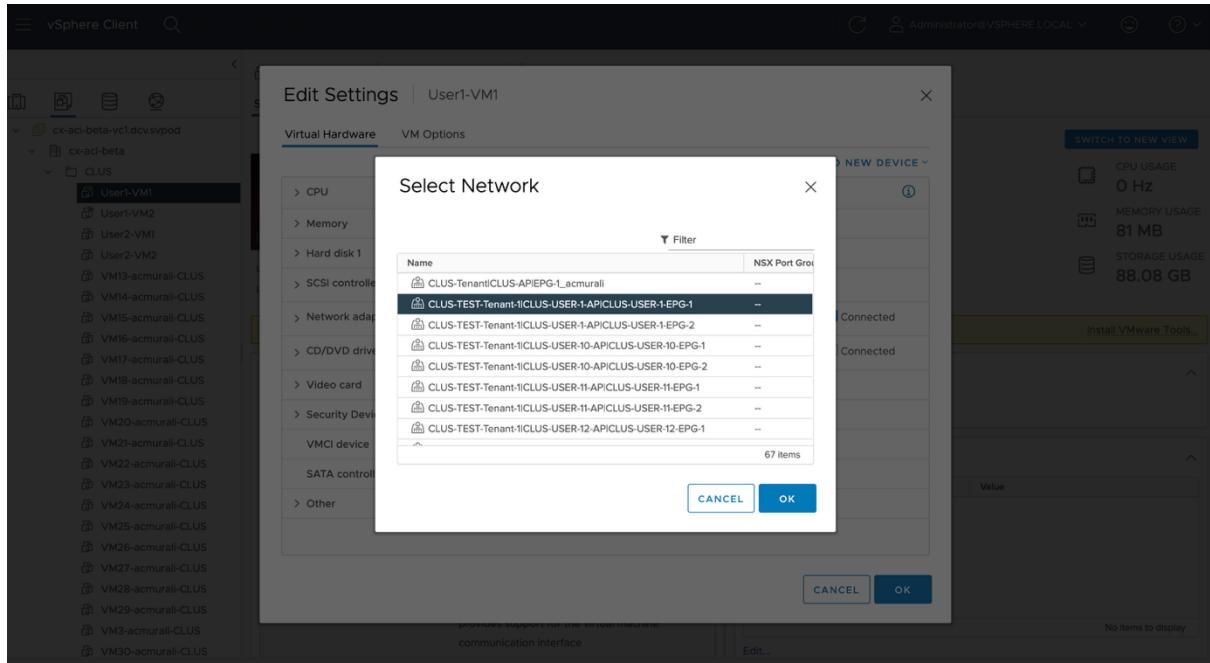
Go ahead and add the VM-1 to the port group of your EPG-1.
By clicking the actions tab on the VM- go to Edit settings



Go to network adapter one and find your EPG



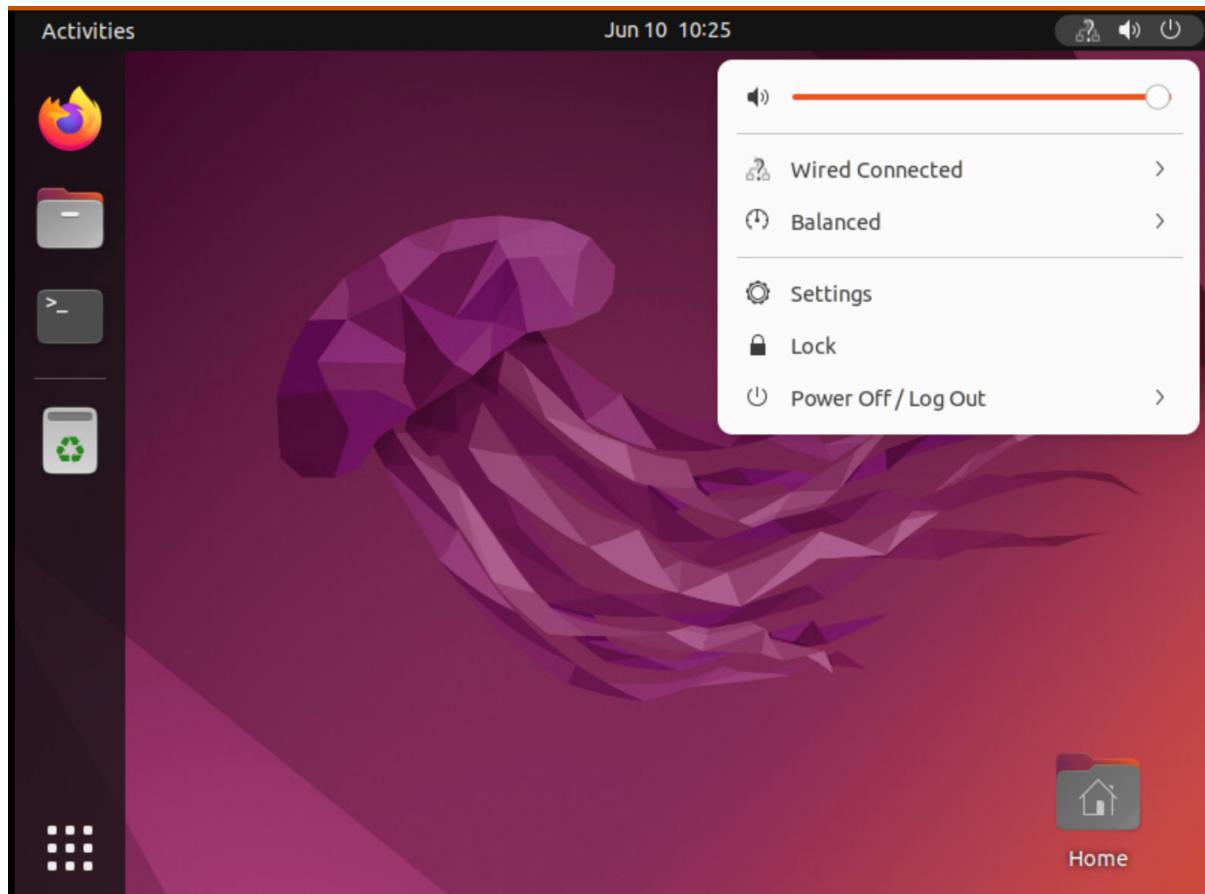
Assign it to your user's EPG-1 while browsing and select okay.

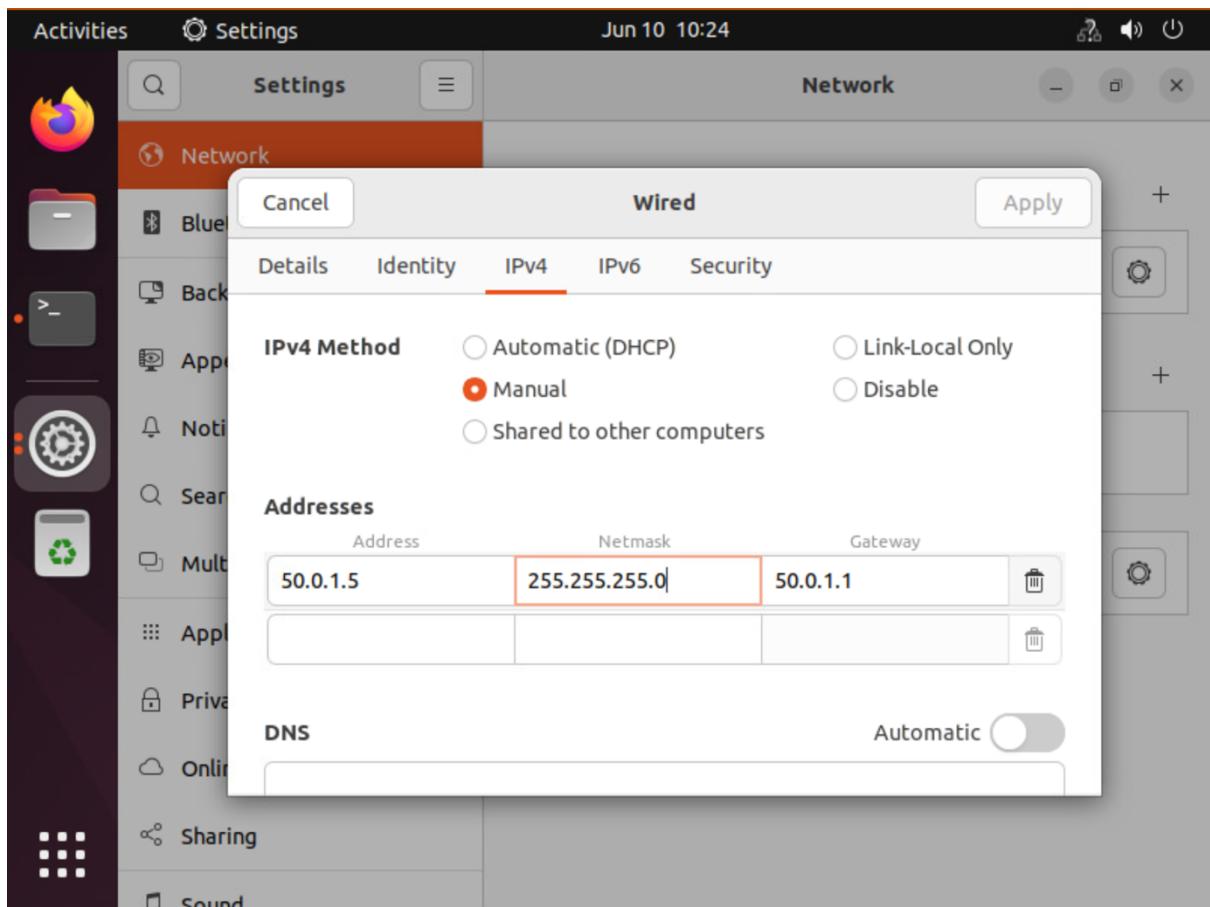


Now open the VM web console using 'Launch Web Console'. Password is C1sco12345!

Change the IP address, gateway and subnet. It must be a /24 (255.255.255.0) in the subnet you noted above. In this example for user 1 we will be using .5 in their subnet.

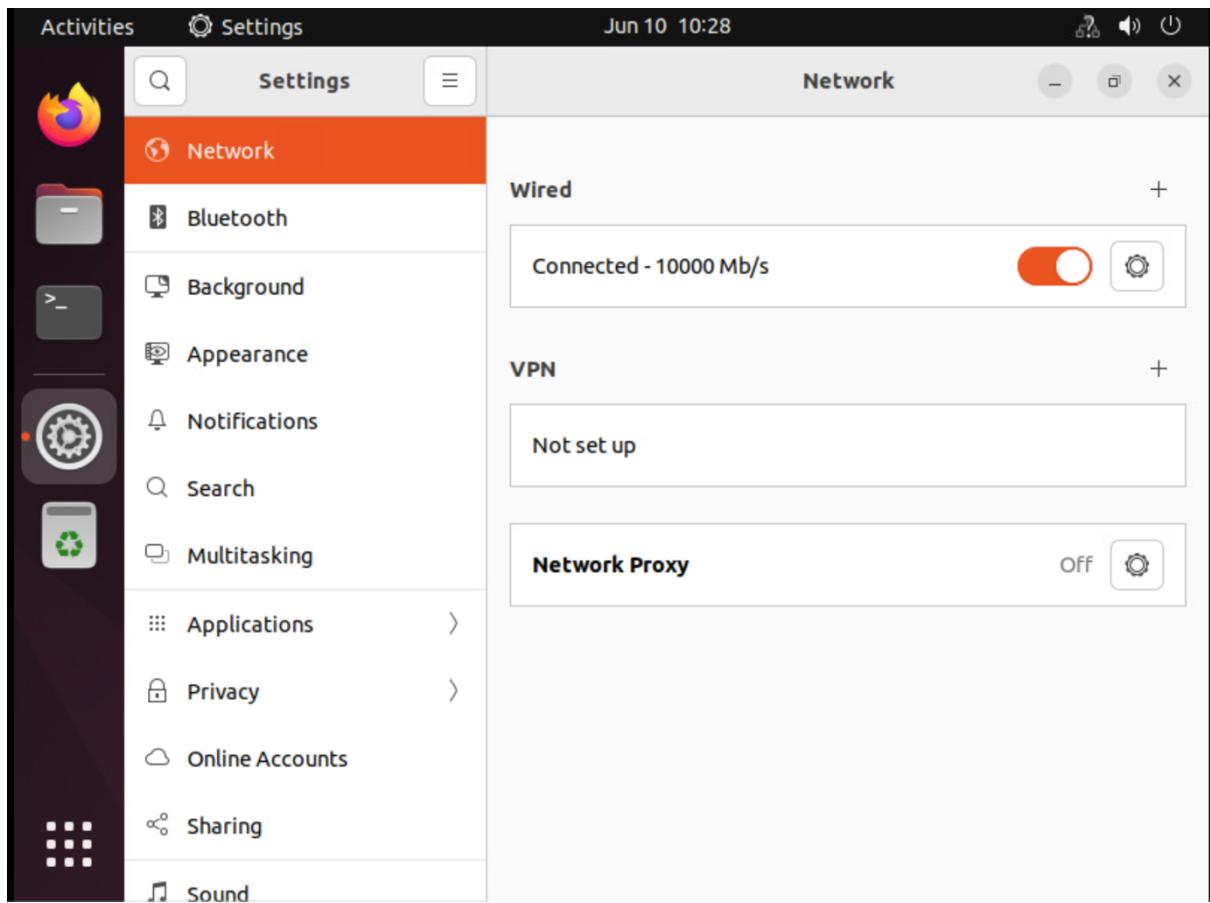
Go to Settings and Network.



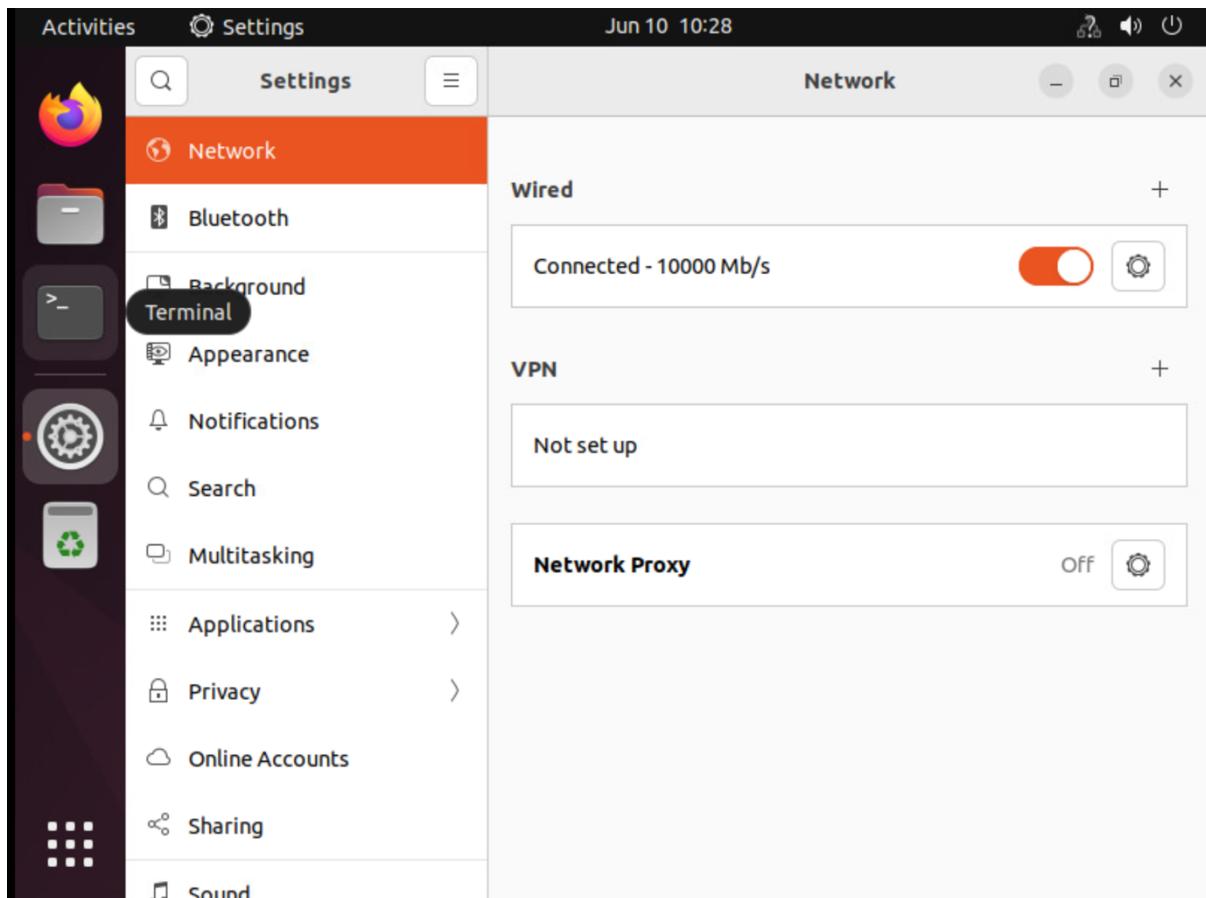


!! Note: this is just an example- please verify if the IP is correct

You may need to turn the connection on and off:



Open the terminal on the left side

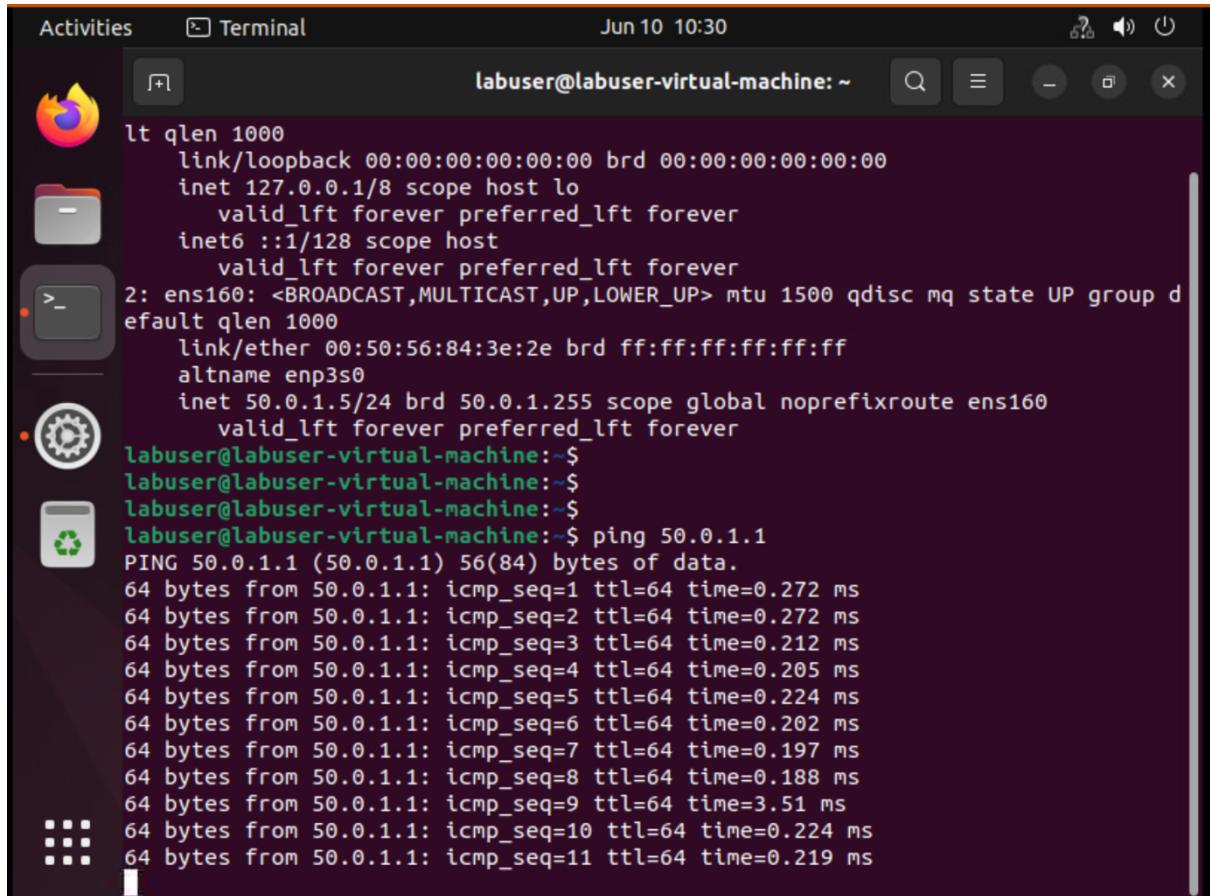


Verify ip using 'ip a'

The screenshot shows a terminal window with the title "Activities" and "Terminal". The date and time are "Jun 10 10:29". The terminal prompt is "labuser@labuser-virtual-machine:~\$". The output of the "ip a" command is displayed:

```
labuser@labuser-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:84:3e:2e brd ff:ff:ff:ff:ff:ff
    altname enp3s0
        inet 50.0.1.5/24 brd 50.0.1.255 scope global noprefixroute ens160
            valid_lft forever preferred_lft forever
labuser@labuser-virtual-machine:~$
```

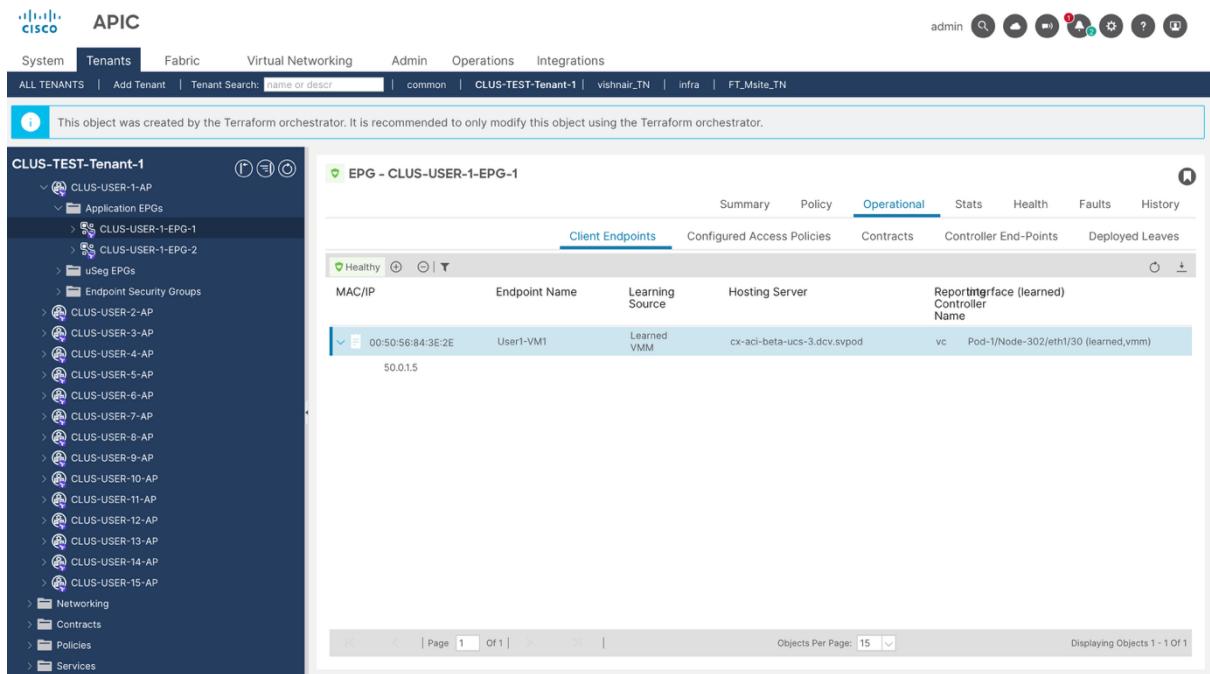
Ping gateway (.1 ip in subnet)



```
Activities Terminal Jun 10 10:30
labuser@labuser-virtual-machine: ~
lt qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
efault qlen 1000
link/ether 00:50:56:84:3e:2e brd ff:ff:ff:ff:ff:ff
altnet enp3s0
inet 50.0.1.5/24 brd 50.0.1.255 scope global noprefixroute ens160
    valid_lft forever preferred_lft forever
labuser@labuser-virtual-machine:~$ ping 50.0.1.1
PING 50.0.1.1 (50.0.1.1) 56(84) bytes of data.
64 bytes from 50.0.1.1: icmp_seq=1 ttl=64 time=0.272 ms
64 bytes from 50.0.1.1: icmp_seq=2 ttl=64 time=0.272 ms
64 bytes from 50.0.1.1: icmp_seq=3 ttl=64 time=0.212 ms
64 bytes from 50.0.1.1: icmp_seq=4 ttl=64 time=0.205 ms
64 bytes from 50.0.1.1: icmp_seq=5 ttl=64 time=0.224 ms
64 bytes from 50.0.1.1: icmp_seq=6 ttl=64 time=0.202 ms
64 bytes from 50.0.1.1: icmp_seq=7 ttl=64 time=0.197 ms
64 bytes from 50.0.1.1: icmp_seq=8 ttl=64 time=0.188 ms
64 bytes from 50.0.1.1: icmp_seq=9 ttl=64 time=3.51 ms
64 bytes from 50.0.1.1: icmp_seq=10 ttl=64 time=0.224 ms
64 bytes from 50.0.1.1: icmp_seq=11 ttl=64 time=0.219 ms
```

Go to ACI and verify the learning inside this EPG

Go to the EPG inside the AP and click on the Operational tab



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

CLUS-TEST-Tenant-1

EPG - CLUS-USER-1-EPG-1

Client Endpoints	Configured Access Policies	Contracts	Controller End-Points	Deployed Leaves
MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Interface (learned) Controller Name
00:50:56:84:3E:2E	User1-VM1	Learned VMM	cx-aci-beta-ucs-3.dcv.svprod	vc Pod-1/Node-302/eth1/30 (learned,vmm)
50.0.1.5				

You can see the IP as Learned, VMM- which means we have learned it via the data path as well as via the VMM integration.

Step 3:

Now let us follow the same procedure as above in Step 2 for VM 2. Assign it another IP and assign it to the same EPG port group.

Once you have assigned it an IP and port group- attempt pinging between the two VMs. What do you observe?

Ping should go through successful.

Step 4:

That was our first segmentation scenario.

By default- inside an EPG- communication is unrestricted.

Now for the second communication scenario

We will now move this VM-2 to another EPG.

This is the same as moving it to another port group from VMware side:

User1-VM2

Summary Monitor Configure Permissions

Guest OS: Ubuntu
Compatibility: ESXi
VMware Tools: Not installed
DNS Name:
IP Addresses:
Host:

LAUNCH WEB CONSOLE
LAUNCH REMOTE CONSOLE

VM Hardware

> CPU	2 CPU(s)
> Memory	8 GB, 0.56 G
> Hard disk 1	80 GB
> Network adapter 1	CLUS-TEST-Ter USER-1-EPG-1 (c)
CD/DVD drive 1	Disconnected
> Video card	16 MB
VMCI device	Device on the v provides support communication

Actions - User1-VM2

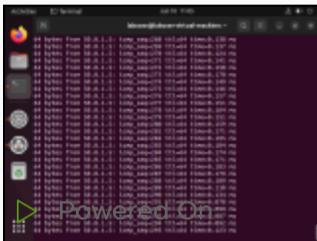
- Power
- Guest OS
- Snapshots
- Open Remote Console
- Migrate...
- Clone
- Fault Tolerance
- VM Policies
- Template
- Compatibility
- Export System Logs...
- Edit Settings... **Selected**
- Move to folder...
- Rename...
- Edit Notes...
- Tags & Custom Attributes
- Add Permission...
- Alarms
- Remove from Inventory
- Delete from Disk
- vSAN

Notes
Edit Notes...
Custom Attributes
Attribute
Edit...

We go over to edit settings and change it to EPG-2 for our user number.

User1-VM2 | ▶ 🔍 🖥️ 🛡️ 📁 ⚙️ ⚙️ | ⚙️ ACTIONS

Summary Monitor Configure Permissions Datastores Networks

 Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Not running, not installed
[MORE INFO](#)

DNS Name:
IP Addresses:
Host: cx-aci-beta-ucs-3.dcv.svprod

[LAUNCH WEB CONSOLE](#) [LAUNCH REMOTE CONSOLE](#) ⓘ  

⚠️ VMware Tools is not installed on this virtual machine.

VM Hardware

> CPU	2 CPU(s)
> Memory	8 GB, 0.16 GB memory active
> Hard disk 1	80 GB
> Network adapter 1	CLUS-TEST-Tenant-1 CLUS-USER-1-AP CLUS-USER-1-EPG-2 (connected)
CD/DVD drive 1	Disconnected
> Video card	16 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

Now let us attempt to ping gateway and then the VM-1.

Gateway ping is successful but the ping between EPGs fails.

This is because communication between EPGs is blocked by default.

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

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

Right click filters to create a new filter

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

After we hit submit, we can then proceed to creating our contract. You can name it CLUS-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: CLUS-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 CLUS-User-X-Subject

Create Contract Subject

Name:	CLUS-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
CLUS-User-1-Filter		Permit	default level

Cancel OK

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

The screenshot shows the Cisco APIC interface with the 'Tenants' tab selected. On the left, the navigation tree shows 'CLUS-TEST-Tenant-1' under 'Contracts'. In the center, a modal window titled 'Create Contract Subject' is open. The 'Filters' section contains a table with one row:

Name	Tenant	Action	Priority
CLUS-User-1-Filter	CLUS-TEST-Tenant-1	Permit	default level

At the bottom of the modal, there are 'Update' and 'Cancel' buttons, and outside the modal, there are 'Cancel' and 'OK' buttons.

Now our last step is to apply these to our EPGs

Head over to the EPGs.

Name	Alias	Description	Class ID	Preferred Group Member	Flood in Encapsulation	Bridge Domain	QoS class	Intra EPG Isolation	In Shutdown	ESG Matched
CLUS-USER-1-EPG-1	Terraform		16399	Exclude	Disabled	CLUS-USER-1-AP	Unspecified	Unenforced	No	No
CLUS-USER-1-EPG-2	Terraform		49158	Exclude	Disabled	CLUS-USER-1-AP	Unspecified	Unenforced	No	No

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;

This object was created by the Terraform orchestrator

Select the contract you just created.

APIC

System **Tenants** Fabric Virtual Networking Admin Operations Integrations

ALL TENANTS | Add Tenant | Tenant Search: name or descr | common | CLUS-TEST-Tenant-1 | vishnair_TN | infra | CLUS-TEST-Tenant-2

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

CLUS-TEST-Tenant-1

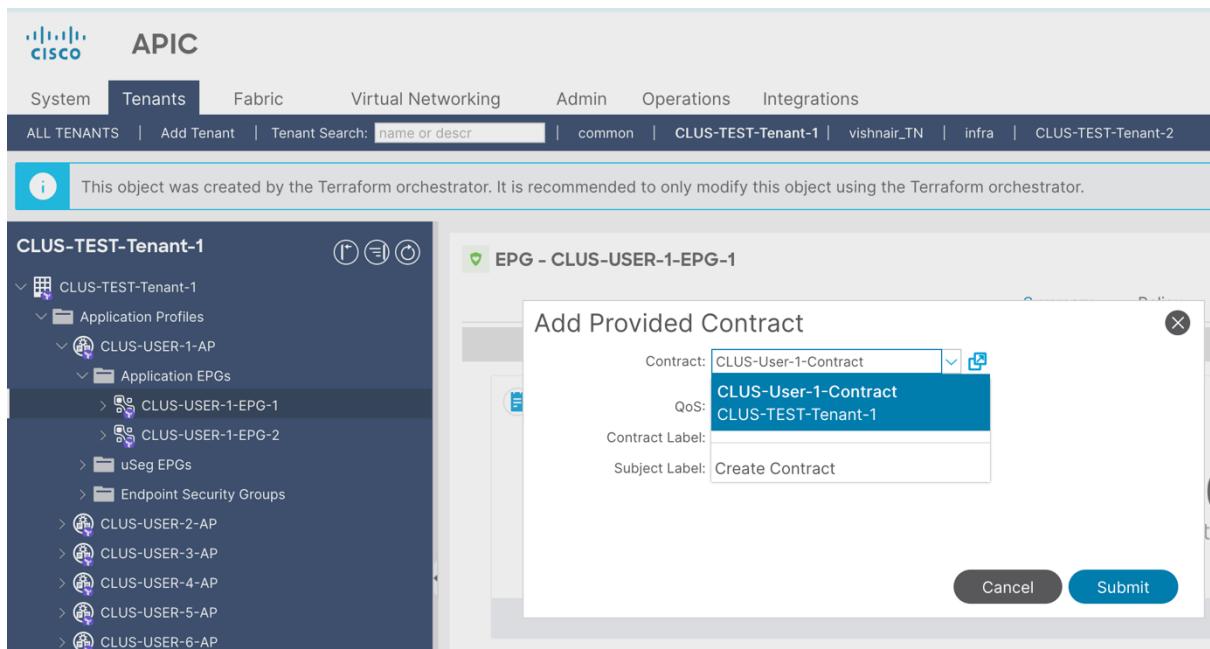
- CLUS-TEST-Tenant-1
 - Application Profiles
 - CLUS-USER-1-AP
 - Application EPGs
 - CLUS-USER-1-EPG-1
 - CLUS-USER-1-EPG-2
 - uSeg EPGs
 - Endpoint Security Groups
 - CLUS-USER-2-AP
 - CLUS-USER-3-AP
 - CLUS-USER-4-AP
 - CLUS-USER-5-AP
 - CLUS-USER-6-AP

EPG - CLUS-USER-1-EPG-1

Add Provided Contract

Contract:	CLUS-User-1-Contract
QoS:	CLUS-User-1-Contract CLUS-TEST-Tenant-1
Contract Label:	
Subject Label:	Create Contract

Cancel Submit



Repeat this to add consumed contract for EPG-2

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The top navigation bar includes tabs for System, Tenants, Fabric, Virtual Networking, and Admir. The Tenants tab is selected. Below the navigation is a search bar with placeholder text "name or descr". A message box indicates that the object was created by the Terraform orchestrator.

CLUS-TEST-Tenant-1

Object Tree:

- CLUS-TEST-Tenant-1
 - Application Profiles
 - CLUS-USER-1-AP
 - Application EPGs
 - CLUS-USER-1-EPG-1
 - CLUS-USER-1-EPG-2
 - uSeg EPGs
 - Endpoint Security Groups
 - CLUS-USER-2-AP
 - CLUS-USER-3-AP
 - CLUS-USER-4-AP
 - CLUS-USER-5-AP
 - CLUS-USER-6-AP
 - CLUS-USER-7-AP
 - CLUS-USER-8-AP
 - CLUS-USER-9-AP
 - CLUS-USER-10-AP
 - CLUS-USER-11-AP
 - CLUS-USER-12-AP
 - CLUS-USER-13-AP
 - CLUS-USER-14-AP
 - CLUS-USER-15-AP
 - Networking
 - Contracts

Actions (available via context menu):

 - 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
 - Add Consumed Contract Interface
 - Add Intra-EPG Contract
 - Create L4-L7 IP Address Pool
 - Delete
 - Save as ...
 - Post ...
 - Share
 - Open In Object Store Browser

Last Login Time: [redacted]

Select your contract again

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 tenant 'ALL TENANTS' and options to 'Add Tenant' or 'Tenant Search'. Below the navigation is a message: 'This object was created by the Terraform orchestrator. It is recommended to only modify this object using the Terraform orchestrator.' On the left, a tree view shows the tenant structure: 'CLUS-TEST-Tenant-1' containing 'CLUS-TEST-Tenant-1' which has 'Application Profiles' (including 'CLUS-USER-1-AP') and 'Application EPGs' (including 'CLUS-USER-1-EPG-1', 'CLUS-USER-1-EPG-2', 'uSeg EPGs', 'Endpoint Security Groups', 'CLUS-USER-2-AP', 'CLUS-USER-3-AP', 'CLUS-USER-4-AP', 'CLUS-USER-5-AP', 'CLUS-USER-6-AP', and 'CLUS-USER-7-AP'). On the right, a detailed view of 'CLUS-USER-1-EPG-2' is shown with tabs for 'Summary' (selected) and 'Policy'. A modal window titled 'Add Consumed Contract' is open, showing fields for 'Contract' (set to 'CLUS-User-1-Contract'), 'QoS' (set to 'CLUS-User-1-Contract'), 'Contract Label' (empty), and 'Subject Label' (set to 'Create Contract'). Buttons for 'Cancel' and 'Submit' are at the bottom of the modal.

Now test the pings.

You should be able to ping the peer device now

The screenshot shows a terminal window on a Linux desktop environment. The title bar indicates the session is running on 'labuser@labuser-virtual-machine: ~'. The terminal displays the output of several ping commands. The first series of pings is from host 50.0.1.1 to host 50.0.1.1, showing round-trip times (rtt) ranging from 0.228 ms to 0.293 ms. The second series of pings is from host 50.0.1.1 to host 50.0.1.2, showing a packet loss of 0% over 24 packets transmitted. The third series of pings is from host 50.0.1.2 back to host 50.0.1.1, showing round-trip times (rtt) ranging from 0.032 ms to 0.070 ms. The terminal prompt ends with '\$'.

```
64 bytes from 50.0.1.1: icmp_seq=17 ttl=64 time=0.241 ms
64 bytes from 50.0.1.1: icmp_seq=18 ttl=64 time=0.228 ms
64 bytes from 50.0.1.1: icmp_seq=19 ttl=64 time=0.283 ms
64 bytes from 50.0.1.1: icmp_seq=20 ttl=64 time=0.259 ms
64 bytes from 50.0.1.1: icmp_seq=21 ttl=64 time=0.268 ms
64 bytes from 50.0.1.1: icmp_seq=22 ttl=64 time=0.288 ms
64 bytes from 50.0.1.1: icmp_seq=23 ttl=64 time=0.283 ms
64 bytes from 50.0.1.1: icmp_seq=24 ttl=64 time=0.274 ms
^C
--- 50.0.1.1 ping statistics ---
24 packets transmitted, 24 received, 0% packet loss, time 23523ms
rtt min/avg/max/mdev = 0.200/0.386/3.610/0.672 ms
labuser@labuser-virtual-machine:~$ ping 50.0.1.2
PING 50.0.1.2 (50.0.1.2) 56(84) bytes of data.
64 bytes from 50.0.1.2: icmp_seq=1 ttl=64 time=0.200 ms
64 bytes from 50.0.1.2: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 50.0.1.2: icmp_seq=3 ttl=64 time=0.034 ms
64 bytes from 50.0.1.2: icmp_seq=4 ttl=64 time=0.032 ms
64 bytes from 50.0.1.2: icmp_seq=5 ttl=64 time=0.032 ms
64 bytes from 50.0.1.2: icmp_seq=6 ttl=64 time=0.034 ms
64 bytes from 50.0.1.2: icmp_seq=7 ttl=64 time=0.032 ms
64 bytes from 50.0.1.2: icmp_seq=8 ttl=64 time=0.034 ms
64 bytes from 50.0.1.2: icmp_seq=9 ttl=64 time=0.033 ms
64 bytes from 50.0.1.2: icmp_seq=10 ttl=64 time=0.038 ms
^C
--- 50.0.1.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9215ms
rtt min/avg/max/mdev = 0.032/0.053/0.200/0.049 ms
labuser@labuser-virtual-machine:~$
```

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 6:

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: name or descr, common, CLUS-TEST-Tenant-1, CLUS-TEST-Tenant-2, vishnair_TN, and infra. A message at the top indicates the object was created by the Terraform orchestrator. The main content area is titled 'L3Outs' and lists one entry: 'L3OUT-to-SDA'. The table columns are Name, Alias, Description, PIM, BGP, OSPF, EIGRP, VRF, Route Control, L3 Domain, and PIMv6. The 'Route Control' column for 'L3OUT-to-SDA' shows 'CLUS-VR...' and 'Export C...'. On the left sidebar, under 'CLUS-TEST-Tenant-1', the 'Networking' section is expanded, showing 'VXLAN Stretch', 'Bridge Domains', 'VRFs', 'L2Outs', and 'L3Outs'. The 'L3Outs' section is also expanded, listing 'L3OUT-to-SDA', 'SR-MPLS VRF L3Outs', and 'Dot1Q Tunnels'. Other sections like Contracts, Policies, and Services are also listed.

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. The tenant list includes ALL TENANTS, Add Tenant, Tenant Search: name or descr, common, CLUS-TEST-Tenant-1, CLUS-TEST-Tenant-2, vishnair_TN, and infra. A message at the top indicates the object was created by the Terraform orchestrator. The main content area is titled 'Logical Node Profile - L3OUT-to-SDA_nodeProfile'. It shows a 'Properties' section with fields: Name (L3OUT-to-SDA_nodeProfile), Description (optional), Alias (empty), Target DSCP (Unspecified), and Nodes. The 'Nodes' table has one entry: topology/pod-1/node-301, Router ID 1.1.1.1, and Loopback Address 1.1.1.1. On the left sidebar, under 'CLUS-TEST-Tenant-1', the 'Networking' section is expanded, showing 'VXLAN Stretch', 'Bridge Domains', 'VRFs', 'L2Outs', and 'L3Outs'. The 'L3Outs' section is expanded, showing 'L3OUT-to-SDA' and 'Logical Node Profiles'. The 'Logical Node Profiles' section is expanded, showing 'L3OUT-to-SDA_nodeProfile', 'External EPGs', and 'Route map for import and export route con...'. Other sections like Contracts, Policies, and Services are also listed.

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 search bar displays 'ALL TENANTS' and 'Add Tenant'. The main content area is titled 'CLUS-TEST-Tenant-1' and shows a tree view of network components. Under the 'Networking' section, the 'L3Outs' node is expanded, showing 'L3OUT-to-SDA' and 'External EPGs'. The 'External EPGs' node is selected, revealing the 'EPG-External-SDA' configuration page. This page has tabs for Summary, Policy, Operational, Health, Faults, and History, with 'Policy' being the active tab. The 'General' sub-tab is selected under the Policy tab. The configuration details include:

- Name:** EPG-External-SDA
- Alias:** (empty)
- Annotations:** Click to add a new annotation
- Global Alias:** (empty)
- Description:** optional
- pcTag:** 49170
- Contract Exception Tag:** (empty)
- Configured VRF Name:** CLUS-VRF-TEST-1
- Resolved VRF:** unlnn-CLUS-TEST-Tenant-1/ctx-CLUS-VRF-TEST-1
- QoS Class:** Unspecified
- Target DSCP:** Unspecified
- Configuration Status:** applied
- Configuration Issues:** (empty)
- Preferred Group Member:** Exclude (radio button)

At the bottom of the configuration page, 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 policies are implemented in ACI and SDA and how you can simplify enforcement via this integration.

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.

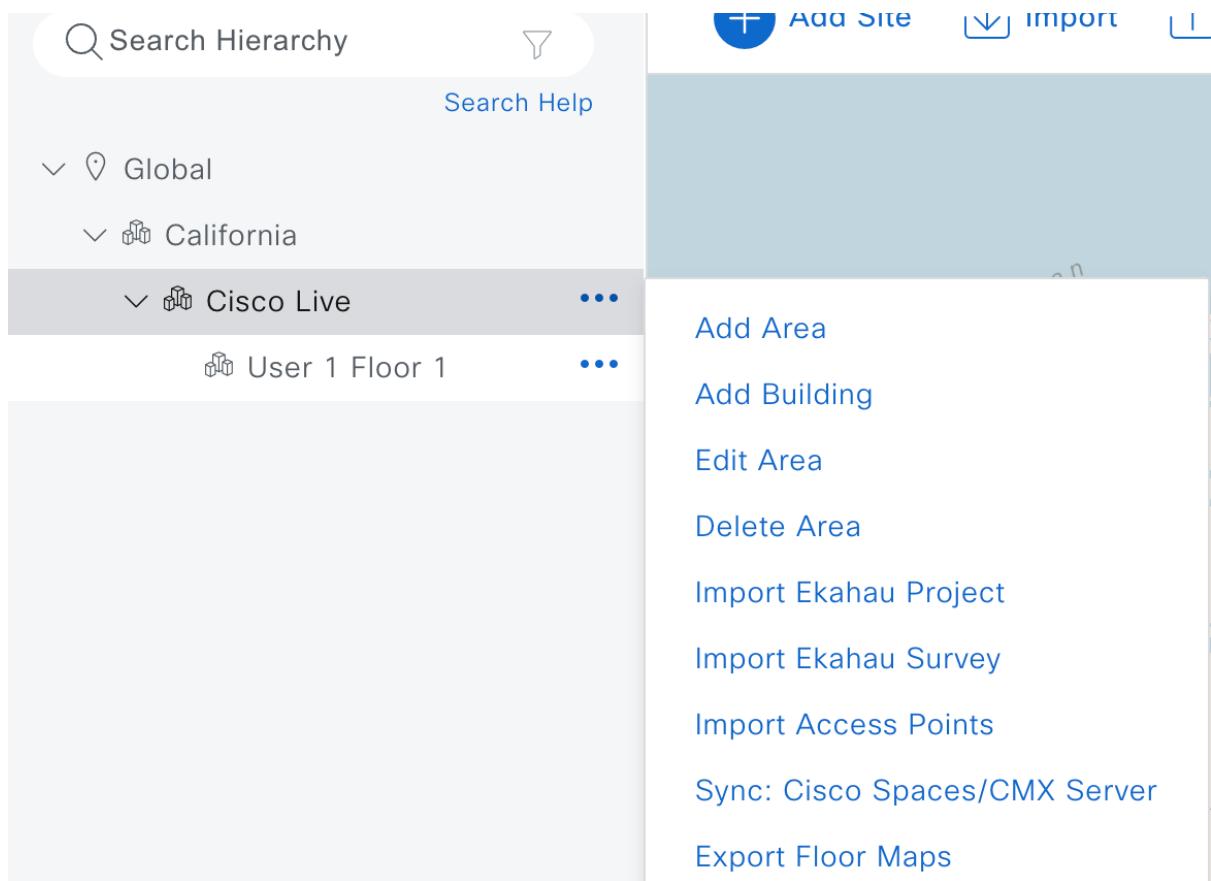
The server is added as “ISE” and integrated with pxGrid enabled. We are also using both RADIUS and TACACS capabilities of ISE.

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

Step 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.



Click on California 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.
'clus' and 'clusv3' are the credentials to be used for network devices and snmp credentials.

Step 4:

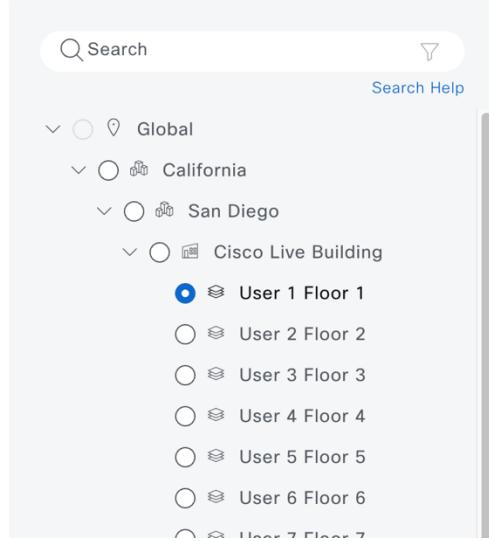
Create a Fabric Site

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.

Fabric Site Location

A Fabric Site begins at the selected level of hierarchy. All levels below the selected level are included as part of the Fabric Site.



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.

<input checked="" type="radio"/> Setup Fabric Zones Later	<input type="radio"/> Setup Fabric Zones Now
All IP address pools and Virtual Networks are provisioned to all fabric Edge Nodes.	
Specific IP address pools and Virtual Networks can be assigned to fabric Edge Nodes in one or more Fabric Zones.	

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](#)

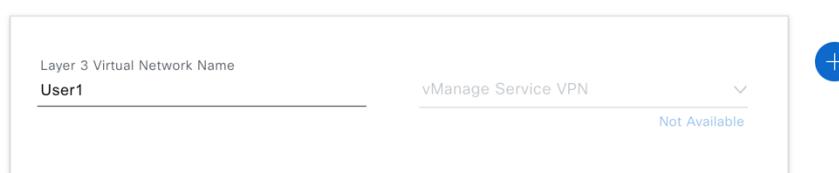
 [Exit](#)

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

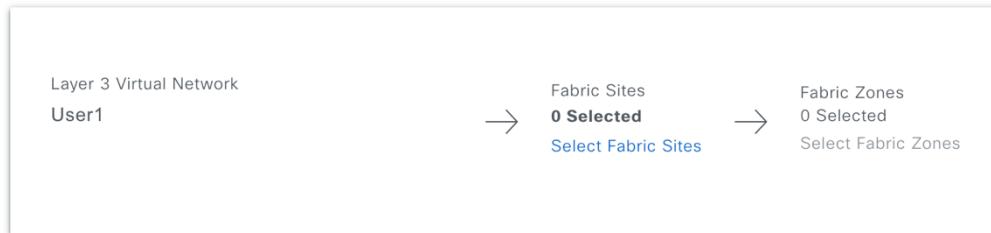
vManage Service VPN
Not Available

+

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 one or more 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

The screenshot shows a modal dialog titled "Assign Fabric Sites". It includes a search bar at the top. Below the search bar are buttons for "Add All", "0 Unselected", "Remove All", and "1 Selected". A list area displays "No Values Available" and a single selected item: ".../Cisco Live Building/User 1 Floor 1". At the bottom of the dialog are "Cancel" and "Assign" buttons.

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"/>	

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 1 has VLAN ID 100, User 2 has VLAN ID 200 and so on.

Save the intent and deploy.

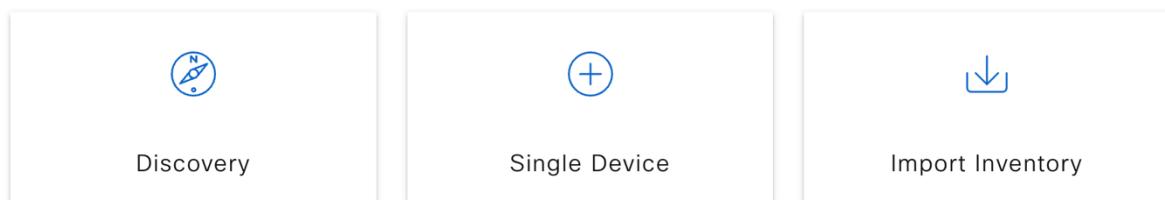
Step 6:

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.



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

Type *
Network Device
Device IP / DNS Name*
100.0.0.101

Credentials [Validate](#)

! Note: CLI and SNMP credentials are mandatory. Please ensure authentic device will go into a collection failure state.

▼ CLI*

i Global credentials are provided only for ease of use when enter the device-specific credentials are saved. The device-to-globa

Select global credential Add device specific credential

Credential*

clus

▼ SNMP*

i Global credentials are provided only for ease of use when enter the device-specific credentials are saved. The device-to-globa

▼ SNMP*

i Global credentials are provided only for ease of the device-specific credentials are saved. The c

Select global credential Add device specific cred

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 as it gets updated over time.

The CatC will use the provided credentials to login to 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 n Sync

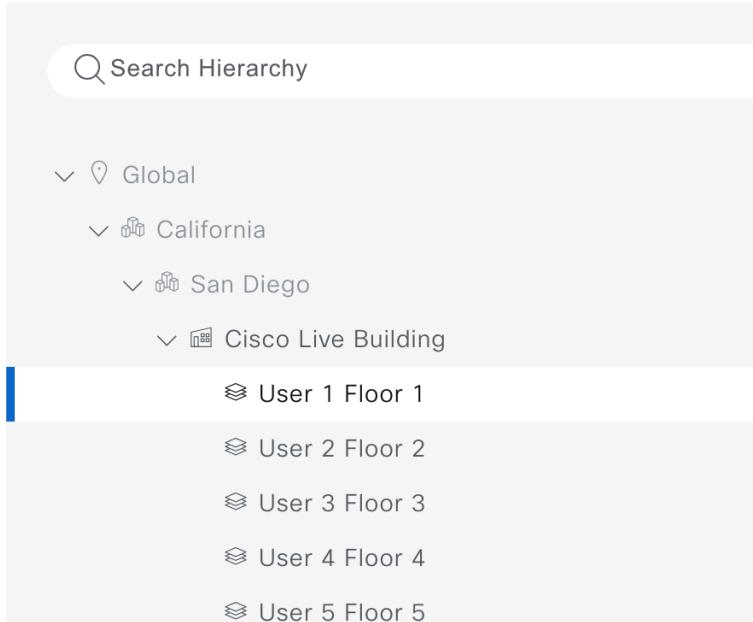
After your device shows as reachable and Managed, proceed to next step.

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

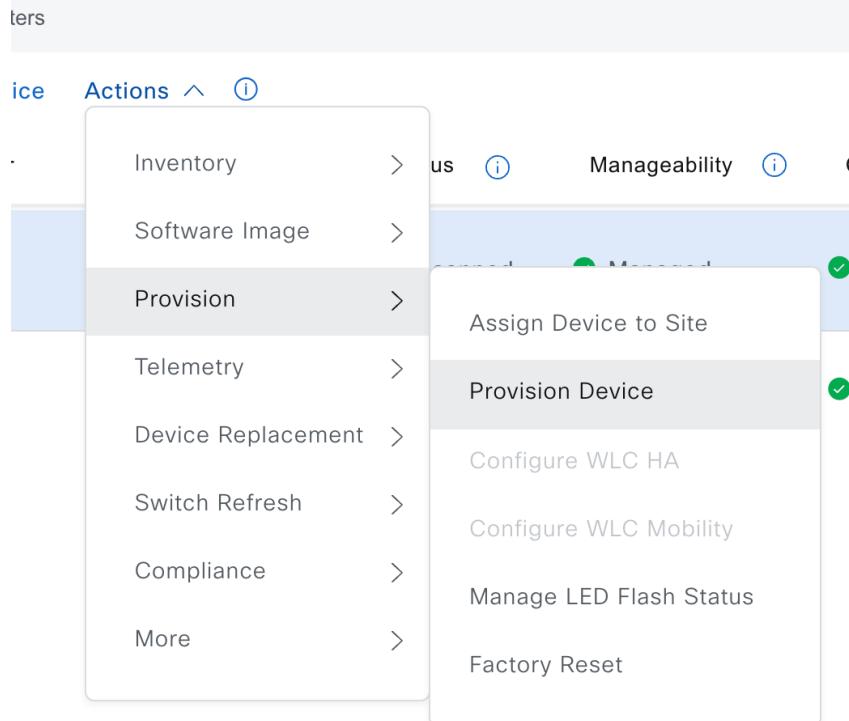


Step 8:

As next step of building 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.



This screenshot shows the 'Advanced Configuration' screen for a device named 'clus-cat9k-1'. It displays 'Device Details' and 'Network Settings' sections. The 'Network Settings' section includes fields for NTP Server, AAA Network ISE Server, AAA Network Primary Server, AAA Network Secondary Server, AAA Client ISE Server, AAA Client Primary Server, AAA Client Secondary Server, DNS Primary Server, Syslog Server, Wired Endpoint Data Collection, and Cisco TrustSec (CTS) Credentials. A warning message at the bottom of the settings section states: 'WARNING: Do not use "admin" as the username for your device CLI credentials, if you are using ISE as your AAA server. If you do, this can result in you not being able to login to your devices.'

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.

[Cancel](#) [Next](#)

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

Fabric Sites Virtual Networks **Transits**

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*	<input type="text" value="User1Transit"/>
Transit Type	<input type="text" value="IP-Based"/>
Remote BGP Autonomous System Number*	<input type="text" value="65412"/>

The BGP number can be any value within 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:

The screenshot shows a network device configuration interface. At the top, it displays the device name "clus-cat9k-1 (100.0.0.101)" and status information: "Reachable" (green checkmark), "Uptime: 8 hrs 17 mins", and "Device Role: ACCESS". Below this is a navigation bar with tabs: Details, Fabric (selected), Summary, Advisories, Field Notices, and Potential Field Notice. A "Run Commands" button and a "View" link are also present. A prominent blue button labeled "Remove From Fabric" is centered below the tabs. The main section is titled "Fabric" and contains three role assignments with toggle switches:

- Border Node (BN): Off
- Control Plane Node (CP): Off
- Edge Node (EN): Off

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

clus-cat9k-1

Layer 3 Handoff Layer 2 Handoff

Enable Layer 3 Handoff

Local Autonomous Number (i)

65413

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 show 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.

clus-cat9k-1

< Back

External Interface

GigabitEthernet1/0/3



Remote AS Number 65412



Interface Description

Search

Actions ▾

Virtual Network ▾

Enable Layer 3 Handoff

VLAN

Local IP Address/Mask

Peer IP Address/Mask

User1



100



IPv4

IPv4

IPv6

IPv6

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

clus-cat9k-1



Configure Control Plane

Select route distribution protocol:

LISP Pub/Sub



LISP/BGP

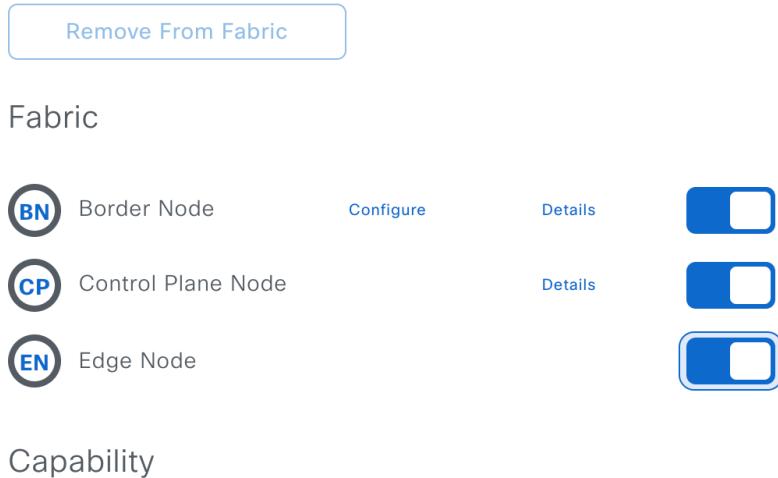


LISP Pub/Sub (Publish/Subscribe) accelerates network convergence, simplifies network operations, and provides the foundation for new SD-Access use cases. LISP Pub/Sub requires all Border Nodes, Control Plane Nodes and Edge Nodes to be running IOS XE 17.6.x or later.

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:



Save and deploy.

The CatC will show you the configuration before pushing:

Modifying Fabric at User 1 Floor

Step 3 of 3: Preview Configuration

Review the device configuration provided below by clicking on each device. When you are done reviewing, click Deploy. Click [Exit and Preview Later](#) to defer the review. The deferred review can be found in the [Tasks](#) menu.

As of: 7:28:26 PM Refresh

Status: Ready

The screenshot shows the Cisco Configuration Collector (CatC) interface. It displays two panes: "Configuration to be Deployed" and "Running Configuration".

Configuration to be Deployed (721 Line(s)):

```
1 no access-session mac-move deny
2 no ip name-server 198.18.133.1
3 no ip route 0.0.0.0 0.0.0.0 interface Loopback0
4 service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
5 exit
6 service-template DefaultCriticalVoice_SRV_TEMPLATE
7 voice-vlan
8 exit
9 service-template DefaultCriticalAccess_SRV_TEMPLATE
10 access-group IPV4_CRITICAL_AUTH_ACL
11 access-group IPV6_CRITICAL_AUTH_ACL
12 exit
13 class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH_CLOSED_MODE
14 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
15 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
16 exit
17 class-map type control subscriber match-any IN_CRITICAL_AUTH_CLOSED_MODE
18 match activated-service-template DefaultCriticalAuthVlan_SRV_TEMPLATE
19 match activated-service-template DefaultCriticalVoice_SRV_TEMPLATE
20 match result-type accept
21 class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
22 match authorization-status authorized
23 match result-type accept
24 match result-type accept
25 class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
26 match authorization-status unauthorized
27
```

Running Configuration (552 Line(s)):

```
1 Building configuration...
2 Current configuration : 19413 bytes
3 !
4 Last configuration change at 01:49:15 UTC Thu Jun 12 2025 by ciscolive
5 !
6 version 17.15
7 service tcp-keepalives-in
8 service tcp-keepalives-out
10 service timestamps log datetime msec localtime show-timezone
11 service timestamp log datetime msec localtime show-timezone
12 service password-encryption
13 service ntp-leaseinfo
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 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.

The screenshot shows the Cisco Fabric Site interface. The top navigation bar includes 'Fabric Sites / User 1 Floor 1', 'User 1 Floor 1' (selected), 'View Site Hierarchy', 'Site Actions', and a help icon. Below the navigation are tabs for 'Fabric Infrastructure', 'Layer 3 Virtual Networks', 'Layer 2 Virtual Networks', 'Anycast Gateways', 'Wireless SSIDs', and 'Authenti...'. A search bar labeled 'Search Table' is present. The main content area is titled 'Ports (22)'. A summary bar indicates '1 port(s) selected from 1 device(s)' with icons for 'Configure', 'Deploy All', and 'More Actions'. A table lists ports by device name, interface name, description, and data VLAN. The port 'clus-cat9k-1 GigabitEthernet1/0/2' is selected, indicated by a blue background and a checked checkbox. Other ports listed are 'clus-cat9k-1 GigabitEthernet1/0/4' and 'clus-cat9k-1 GigabitEthernet1/0/1'.

Device Name	Interface Name	Description	Data VLAN
clus-cat9k-1	GigabitEthernet1/0/1	--	--
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 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: L0veCiscoLive

Network Access Users List > user1

✓ Network Access User

* Username

Status Enabled

Account Name Alias

Email

✓ Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration (i)

Never Expires (i)

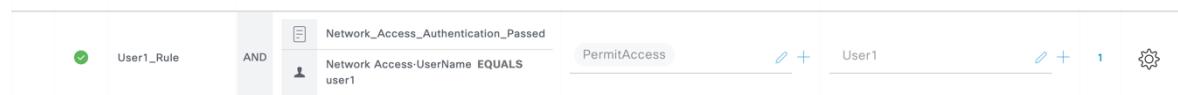
Password Re-Enter Password

* 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.

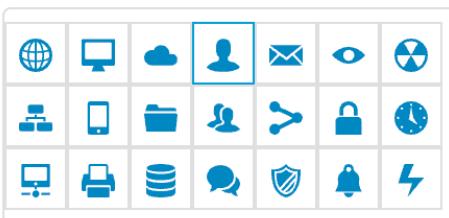
If an SGT for your user does not exist yet, create it here.

[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.

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	...
CLUS ISE	-	listen	ooband	pxGrid connection	2	1	...
CLUS2 ISE	-	listen	ooband	pxGrid connection	2	1	...

You will see 2 integrations. CLUS would be for users 1-15 and CLUS2 would be for users 16-30.

Click on your respective connection and Connection Details

The screenshot shows the Cisco APIC interface with the 'ISE Integrations' tab selected. The main view is titled 'ISE Integrations CLUS' and displays the 'Connection Details' tab. On the left, there is a list of connections: 'CLUS' (ISE) and 'CLUS2' (ISE). The 'CLUS' entry is selected. The main panel shows two servers: 'ISE2' and 'ISE3', each with its IP address listed. The IP address for 'ISE2' is 198.18.133.28 and for 'ISE3' is 198.18.133.29. The interface includes standard navigation and search tools at the top.

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 wont have your EPGs/SGT.

APIC

System Tenants Fabric Virtual Networking Admin Operations Integrations ISE Integrations

ISE Integrations CLUS

Filter by attributes

Name	Description
CLUS ISE	-
CLUS2 ISE	-

2 items found

Overview Connection Details Endpoints **Configuration** History

Subscribed SGTs Published EPG/ESGs

No Entries Found For Subscribed SGT



APIC

System Tenants Fabric Virtual Networking Admin Operations Integrations ISE Integrations

ISE Integrations CLUS

Filter by attributes

Name	Description
CLUS ISE	-
CLUS2 ISE	-

2 items found

Overview Connection Details **Endpoints** Configuration History

DCs SGT Endpoints

No Entries Found For DC



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, Users 1-15 will use ISE 198.18.133.27 and Users 16-30 will use ISE 198.18.133.30.

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 'Dashboard', 'Summary', 'Endpoints', 'Guests', 'Vulnerability', 'Threat', and a search icon. On the left, there is a sidebar with icons for 'Bookmarks', 'Dashboard' (which is selected), 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. Below the sidebar is an 'Interactive Help' link. The main content area has tabs for 'Network Access', 'Guest Access', 'Posture', and 'BYOD'. Under 'Network Access', there are dropdown menus for 'TrustSec' (Overview, Components, TrustSec Policy, Policy Sets, SXP, Integrations, Troubleshoot, Reports, Settings) and 'Device Administration' (Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, Reports, Settings). At the bottom of the main content area, the URL 'https://198.18.133.30/admin/#workcenters' is visible.

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 Context Visibility Operations Policy Administration Work Centers Interactive Help

Workload Connectors Overview Workload Connections Attributes Dictionary Workload Classification Meraki

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.

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	L
<input type="checkbox"/>	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 Context Visibility Operations Policy Administration Work Centers Interactive Help

Workload Connectors Overview Workload Connections Attributes Dictionary Workload Classification Meraki

ACI Connections Details

rules to define SXP domain mapping between Cisco ISE and Cisco ACI. This includes defining Inbound SGT domain rules to map SXP domains to ACI domains and Outbound SGT domain rules to map ACI domains to SXP domains.

Configuration Name Conversion Synced EPG/ESGs SGT Numbering Range

ACI Connection Name* FQDN or IP Address* Non-editable after creation

CLUS2 apic.securitydemo.net

ACI Username* ACI Password

admin

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

Once the EPG/ESG is selected for sync, it will be linked with the SGT generated according to latest name conversion rule. The SGT name cannot be modified while the EPG/ESG is in sync. To rename its linked SGT name, please deselect EPG/ESGs for sync first. EPG referenced in Inbound or Outbound rule cannot be unselected.

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

Once the EPG/ESG is selected for sync, it will be linked with the SGT generated according to latest name conversion rule. The SGT name cannot be modified while the EPG/ESG is in sync. To rename its linked SGT name, please deselect EPG/ESGs for sync first. EPG referenced in Inbound or Outbound rule cannot be unselected.

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.

Inbound & Outbound SGT Domain Rules

Inbound Rule Name	Status	Destinations	SGT Bindings	Actions
Default-inbound...	<input checked="" type="radio"/>	default	0	...

1 Record(s)

Show Records: 10 1 - 1 < 1 >

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-User-1-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.

The screenshot shows the Cisco Identity Services Engine interface. The top navigation bar includes the Cisco logo and the title "Work Centers / TrustSec". Below the navigation bar is a horizontal menu with tabs: Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), Integrations, Troubleshoot, Reports, and Settings. On the left side, there is a sidebar with links for Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, and Work Centers (which is also selected). The main content area is titled "Inbound & Outbound SGT Domain Rules" and contains a sub-section for "Outbound SGT Domain Rules". A message states: "One or more ACI Connections are in Disconnected state. It is not possible to create, modify, or delete Outbound SGT Domain Rule(s) for disconnected connection(s)". Below this, there is a table header for "Outbound Rule Name", "Status", and "Destinations". A message at the bottom of the table says "No data to display". At the bottom right of the main content area is a blue "Save" button.

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

Rule Configuration ⓘ

<input type="button" value="☰"/>	<input type="text" value="SGT Name"/> <input type="button" value="▼"/>	<input type="button" value="Equals"/> <input type="button" value="▼"/>	<input type="text" value="User1 X"/> <input type="button" value="⊖"/> <input type="button" value="☰"/>
----------------------------------	--	--	--

+ 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 L3 Outs *

Rule Configuration ⓘ

SGT Name Equals User1 X

+ Add AND/OR Statement + Add Condition

Contract Configuration

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

CLUS/CLUS-TEST-Tenant-1 CONTRACT X CLUS-TEST-Tenant-1 CONTRACT X

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.

Add Outbound Rule

Rule Configuration ⓘ

SGT Name Equals User1 X

+ Add AND/OR Statement + Add Condition

Contract Configuration

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

User1	CLUS/ CLUS-TEST-Tenant-1/ L3OUT-to-SDA	CLUS-TEST-Tenant-1 CONTRACT X	CLUS-TEST-Tenant-1 CONTRACT X
-------	---	-------------------------------	-------------------------------

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

Cancel Preview Add

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

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

2 items found

Rows per page: 15 < 1 >

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

ISE Integrations CLUS

DCs	SGT Endpoints				
Filter by attributes	Actions				
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

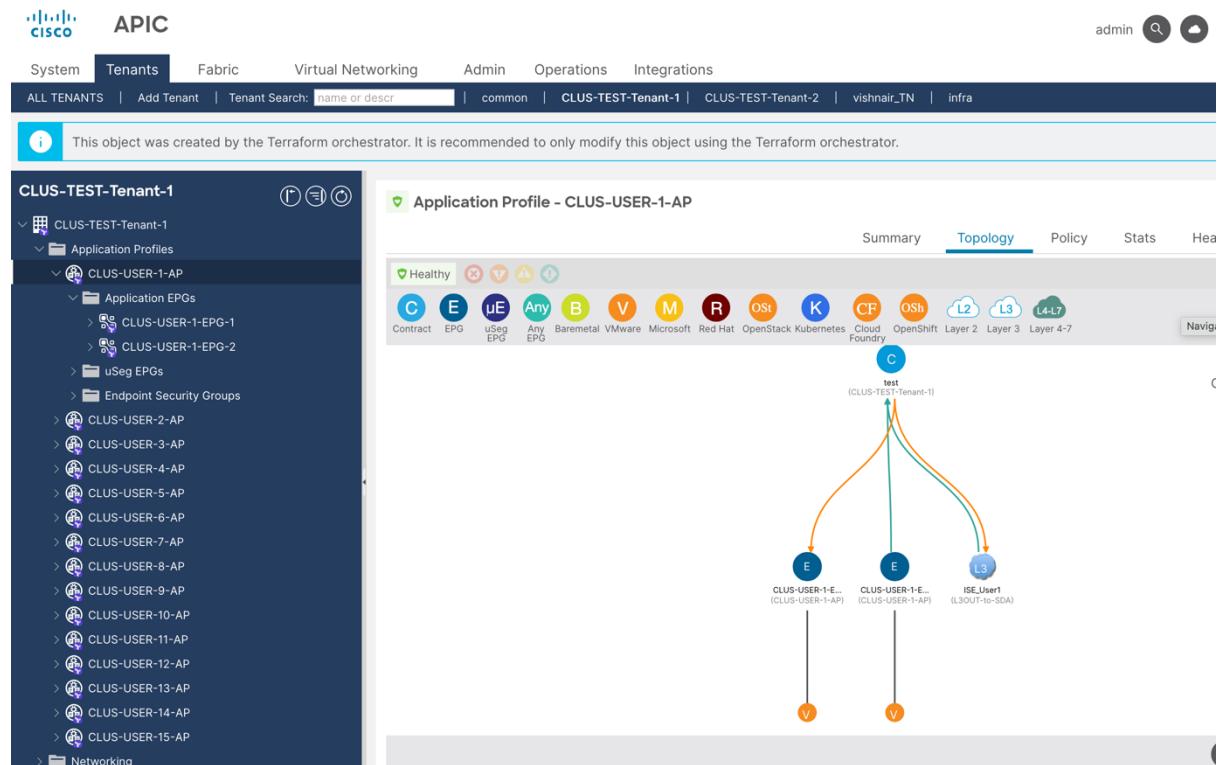
Refresh Actions ×

Overview Connection Details Endpoints Configuration History

Subscribed SGTs		Published EPG/ESGs			
EPG/ESG	Tenant	Application Profile	Contracts	DC Bindings	Actions
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

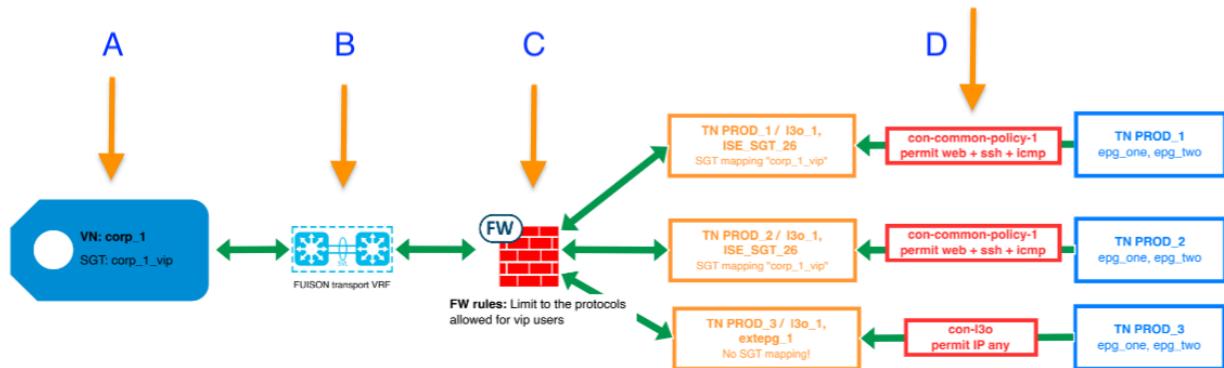
Overview

- 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 a discussion/theoretical in below fictional scenario.

Control Points on the Path

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



(A) ISE policies Via the ISE and TruestSec 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 Cisco ISE TrustSec Policy interface. The top navigation bar includes Overview, Components, TrustSec Policy (selected), Policy Sets, SXP, Integrations, Troubleshoot, Reports, and Settings. The left sidebar has sections for Egress Policy (Matrices List, Matrix, Source Tree, Destination Tree) and Network Device Authorization. The main content area displays a table for Egress Policy matrices:

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

(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 is no firewall in the path from SDA fabrics towards ACI. Today the firewall can join pxGrid and by this receive from ISE the SGT as well the EPG informations. 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 EPG In 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 simple 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 • 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 	<ul style="list-style-type: none"> • Not a clear vision where traffic got dropped ->

Enforcement Point	Pro	Con
	<ul style="list-style-type: none">• Possible to use enforcement points with only "drop/permit" and one other with more granular policies	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. Keep the doors open for the not-categorized
 - Considerations:
 - Hosts which are identified by SGTs can get higher eligibility than not-categorized hosts.
4. Different eligibility between identified hosts
 - Consideration:
 - The identified hosts are grouped into different SGTs and get different eligibility.
5. 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.
6. 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".

7. 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.

8. 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.