Cisco UCS Director APIC Management Guide, Release 6.6

First Published: 2018-04-27

Last Modified: 2018-10-10

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

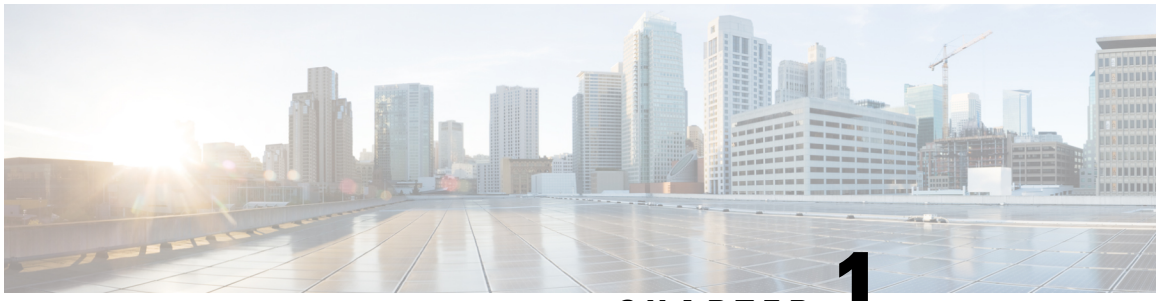
Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-director-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the . RSS feeds are a free service.



CHAPTER 1

New and Changed Information for this Release

New and Changed Information for this Release

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

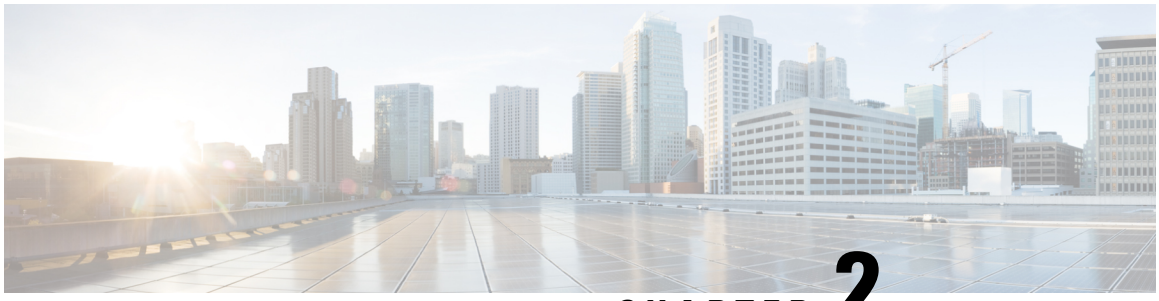
Table 1: New and Changed Information in Cisco UCS Director Release 6.6(1.0)

Feature	Description	Where Documented
Extension of support for Multi-Site Controller (MSC) account	You can perform the following in MSC account: • Add or update an external EPG of MSC with multiple sites. • Add or update an ACI multi-site service graph. • Add or update a service graph to a contract.	• Adding an ACI Multi-Site Service Graph, on page 47 • Adding a Service Graph to a Contract, on page 47 • Adding an External EPG to the Template, on page 58
Support for custom QoS	You can perform the following while configuring layer 4 to layer 7 service to achieve custom QoS support: • Add or update a custom QOS policy. • Add or udpate a DSCP to a priority map. • Add or update a Dot1P classifier.	• Adding a Custom QOS Policy, on page 90 • Adding a DSCP to a Priority Map, on page 90 • Adding a Dot1P Classifier, on page 91

Feature	Description	Where Documented
Provision to add a subnet to a logical device context	You can add a subnet to a logical device context.	Adding a Subnet to a Logical Device Context, on page 92
Provision to add a virtual IP address to a logical interface context.	You can add or update a virtual IP address to a logical interface context.	Adding a Virtual IP Address to a Logical Interface Context, on page 94
Support for policy-based redirect (PBR)	As an administrator, you can create a PBR, and its associated object in Cisco UCS Director.	Configuring Policy Based Redirect, on page 95

Table 2: New and Changed Information in Cisco UCS Director Release 6.6

Feature	Description	Where Documented
Support for Multi-Site Controller	As an administrator, you can create a multi-site controller account, and perform actions such as adding, editing and deleting APIC controller accounts, and assigning accounts to a pod. You can manage the user, site, tenant, and schema of the Multi-Site Controller account.	Configuring Multi-Site Controller Accounts, on page 41
Support for Fabric Extender (FEX)	You can add and manage FEX profile.	Fabric Extender (FEX), on page 39



CHAPTER 2

Overview

Cisco UCS Director and Cisco Application Centric Infrastructure

Cisco UCS Director is a unified infrastructure management solution that provides management from a single interface for compute, network, storage, and virtualization layers. Cisco UCS Director uses a workflow orchestration engine with workflow tasks that support the compute, network, storage, and virtualization layers. Cisco UCS Director supports multitenancy, which enables policy-based and shared use of the infrastructure.

Cisco UCS Director also supports the ability to define contracts between different container tiers, enabling you to apply rules between tiers.

Cisco Application Centric Infrastructure (ACI) allows application requirements to define the network. This architecture simplifies, optimizes, and accelerates the entire application deployment cycle.

The combination of Cisco UCS Director and Cisco ACI enables automatic provisioning and delivery of an application-centric infrastructure.

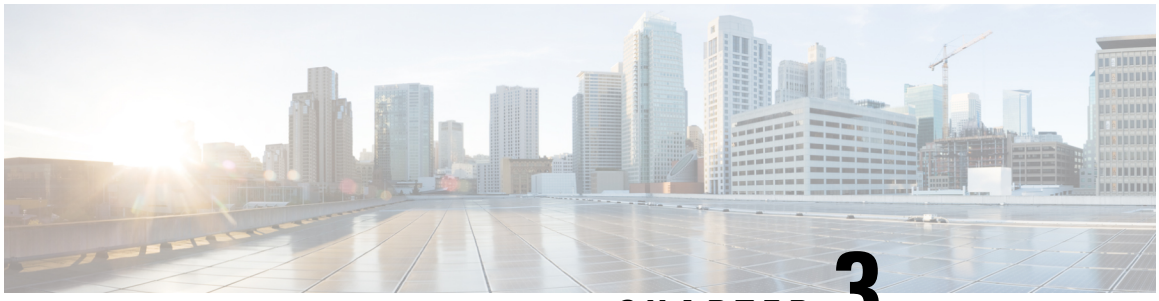
Note To use ACI 1.1(1*), ensure that TLSv1 is enabled in Cisco Application Policy Infrastructure Controller (APIC). In APIC, choose **Fabric > Fabric Resources > Pod Polices > Communication > Default** and enable **TLSv1**.

Cisco Application Policy Infrastructure Controller

The Cisco Application Policy Infrastructure Controller (APIC) is the unified point of automation, management, monitoring, and programmability for the Cisco Application Centric Infrastructure (ACI). The APIC supports the deployment, management, and monitoring of any application anywhere, with a unified operations model for physical and virtual components of the infrastructure. It is the central control engine for the broader cloud network. The APIC programmatically automates network provisioning and control-based on user-defined application requirements and policies.

The Cisco UCS Director orchestration feature allows you to automate APIC configuration and management tasks through operational workflows. A complete list of the APIC orchestration tasks is available in the

Workflow Designer, and in the Task Library. For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.



CHAPTER 3

Configuring APIC Accounts

Guidelines for APIC Accounts

Before you create an APIC account in Cisco UCS Director, consider the following guidelines and best practices.

Account Permissions on Cisco APIC

The Cisco APIC account username and password that you provide when you add the APIC account to Cisco UCS Director must have all the Cisco APIC privileges required to do the following:

- Access the supported features in Cisco APIC
- Perform actions in Cisco APIC, such as viewing and accessing reports
- Execute workflow tasks in Cisco UCS Director

Account Authentication on Cisco APIC

The Cisco APIC account username and password that you use for the APIC account in Cisco UCS Director is authenticated by Cisco APIC not by Cisco UCS Director. As a result, you can use one of the following types of accounts:

- Local authentication through a Cisco APIC account
- Remote authentication by Cisco APIC through one of the following:
  - LDAP
  - RADIUS
  - TACACS+

If you use a Cisco APIC account with remote authentication, enter the username on the **Add Account** screen in the following format: **apic:<Domain Name>\<Remote User Name>**

Note Cisco UCS Director does not support authentication through RADIUS or TACACS+ for accounts used to log in to Cisco UCS Director. Support is only available for authentication of accounts that Cisco UCS Director uses to log in to Cisco APIC.

APIC Clusters

Each APIC account in Cisco UCS Director represents an APIC cluster. When you add an APIC cluster to an APIC account, Cisco UCS Director automatically discovers the controllers in that cluster.

To view details of the controllers, choose **Physical** > **Network**, choose the APIC account, and then click **View Details**.

ACI Fabric Integration

To integrate Cisco UCS Director with the ACI fabric, ensure that TLSv1 is enabled on the ACI fabric.

You must enable TLSv1 in Cisco APIC, as follows: **Fabric Policies** > **Pod Policies** > **Policies - Communication**.

APIC Accounts and Pods

Cisco APIC accounts are multi-domain manager accounts that are not tied to a specific pod. You can assign the account to a pod, but that is optional.

APIC Accounts and Resource Groups

If you add an APIC account to a resource group and that account is associated with a pod, you cannot edit the pod.

You cannot delete an account that is part of a resource group.

Support for In-Band and Out-of-Band Management

Cisco UCS Director supports in-band and out-of-band management of Cisco ACI. You can add a Cisco APIC account to Cisco UCS Director in the following scenarios:

- Out-of-Band—An out-of-band IP address is configured and the Cisco UCS Director VM is in a domain that is not managed by Cisco APIC.
- In-Band—An in-band IP address is configured and reachable, no out-of-band IP address is configured, and the Cisco UCS Director VM is in a domain managed by Cisco APIC.

Adding an APIC Account

Before you begin

Review the guidelines and best practices in Guidelines for APIC Accounts, on page 5.

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, choose **APIC** from the **Account Type** drop-down list and click **Submit**.

Step 5 On the **Add Account** screen, complete the fields, including the following:

a) Enter a unique account name and description.

b) From the **Pod** drop-down list, choose the pod where you want to add the APIC account.

c) In the **Server IP** field, enter the IP address of one of the APIC controllers in the APIC cluster.

Cisco UCS Director automatically discovers the IP address of the other APIC controllers in the APIC cluster.

If the IP address of the APIC controller is not reachable, Cisco UCS Director relies on the Out-of-Band IP address of another APIC controllers for managing Cisco APIC.

d) Check the **Use Credential Policy** box if you want to use a credential policy for this account rather than enter the username and password information manually.

e) If you checked the **Use Credential Policy** box, choose a policy from the **Credential Policy** drop-down list.

The APIC account in the credential policy must meet the criteria listed in Guidelines for APIC Accounts, on page 5.

Note You can only connect to Cisco APIC with HTTPS protocol. You cannot connect through SSH or Telnet protocol. If the credential policy specifies SSH or Telnet protocol, you are prompted to check the protocol defined in the credential policy.

f) If you did not check **Use Credential Policy**, enter the username and password that this account uses to access Cisco APIC.

This username must be a valid account with the required privileges in Cisco APIC. The account must also meet the criteria listed in Guidelines for APIC Accounts, on page 5.

Note For an account with remote authentication by Cisco APIC through LDAP, RADIUS, or TACACS+, enter the username in the following format: **`apic:<Domain Name>\<Remote User Name>`**.

g) If you did not check **Use Credential Policy**, do the following:

- From the **Protocol** drop-down list, choose **https**.
- In the **Port** field, enter the port used to access the APIC account. The default port is 443.

h) Enter the email address and location of the administrator or other person responsible for this account.

Step 6 Click **Submit**.

Cisco UCS Director tests the connection to the APIC server. If that test is successful, it adds the APIC account and discovers all controllers and other infrastructure elements in the APIC server. This discovery process and inventory collection takes a few minutes to complete.

Viewing APIC Resources

After creating an APIC account in Cisco UCS Director, you can view related resources of the APIC account.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click one of the following tabs to view the details of a specific component in the server:

- **Summary** tab—Displays the system overview and summary of the APIC controller.
- **Fabric Nodes** tab—Displays the list of fabric nodes with their details such as the node name, model, vendor, role, serial, and node ID with the status.

  To view more details about fabric nodes, choose a fabric node and click **View Details**. The following tabs appear:

  - **Fabric Chassis**—Displays the fabric name, ID, model, vendor, serial, revision, and operation status of the fabric chassis.
  - **Fan Slots**—Displays the fabric name, slot ID, type, operation status, and inserted-card details of the fan slots.
  - **Physical Interfaces**—Displays the interface details that include the speed, mode, CFG access VLAN, CFG native VLAN, bundle index, operational duplex mode, operational port state, and reason for the current operation state. The operational state of the port can be one of the following: Unknown, Down, Link-up, and Up.
  - **Fabric Routed Vlan Interfaces**—Displays the status and reason for the current operation status of the fabric-routed VLAN interfaces.
  - **Fabric Encapsulated Routed Interfaces**—Displays a list of the fabric-encapsulated routed interfaces.
  - **Fabric Routed Loopback Interfaces**—Displays a list of the fabric-routed loopback interfaces.
  - **Fabric Management Interfaces**—Displays a list of the fabric management interfaces.
  - **Tunnel Interfaces**—Displays the interface, operation state, reason for the current operation state, tunnel layer, tunnel type, and type of the tunnel interface.

- **System** tab—Displays the system details that include the node name, in-band management IP address, out-of-band management IP address, infrastructure IP address, fabric MAC address, ID, role, and serial number.
- **Fabric Memberships** tab—Displays the fabric membership details that include the node name, serial number, node ID, model, role, IP address, decommissioned status, and supported model.
- **Physical Domains** tab—Displays the physical domains in the APIC server. Click **Add** to add a domain.
- **Tenants Health** tab—Displays the health score of tenants.

  To view more details about a tenant's health, choose a tenant and click **View Details**. The following tabs appear:

  - **EPGs Health**—Displays the health score of endpoint groups (EPGs).

- **Application Health**—Displays the health score of applications.

- **Nodes Health** tab—Displays the health score of nodes.

  To view more details about the health of the nodes, choose a node and click **View Details**. The following tabs appear:

  - **Access Ports Health**—Displays the health score of access ports.
  - **Fabric Ports Health**—Displays the health score of fabric ports.
  - **Line Cards Health**—Displays the health score of line cards.

- **Access Entity Profile** tab—Displays the names and descriptions of the access entity profiles.

  To view more details about the access entity profile, choose an entity profile and click **View Details**. The following tabs appear:

  - **Policy Groups**—Displays the policy groups of an entity profile.
  - **Domain Associated To Interfaces**—Displays a list of domains that are associated with the interfaces.

- **Link Level Policy** tab—Displays the name, automatic negotiation, speed, link debounce interval, and description of the link level policy.
- **VLAN Pool** tab—Displays the VLAN pools that are added in the APIC server. Click **Add** to add a VLAN pool.

  To view more details about a VLAN pool, choose a VLAN pool and click **View Details**. The following tab appears:

  - **VLAN Pool Range**—Displays the VLAN pool name, mode of allocation, and the pool range. Click **Add** to add a VLAN range to the VLAN pool.

- **FEX Profile** tab—Displays the FEX profiles that are added in the APIC server. Click **Add** to add a FEX profile.

  To view more details about a FEX profile, choose a FEX profile and click **View Details**. The following tab appears:

  - **FEX Profile Access Port Selectors**—Displays the access port selectors of the FEX profile. Click **Add** to add an access port selector to the FEX profile. Choose an access port selector and click **View Details** to view the access port blocks and sub port blocks of the access port selector.

- **CDP Interface Policy** tab—Displays the name and description of the Cisco Discovery Prototol (CDP) interface policy, with the administration status.
- **LLDP Interface Policy** tab—Displays the name and description of the Link Layer Discovery Protocol (LLDP) interface policy, with the receive status and transmit status.
- **Leaf Policy Group** tab—Displays the name and description of the leaf policy group.
- **Tenant(s)** tab—Displays the tenants in the APIC server. Click **Add** to add a tenant.

  To view more details about a tenant, choose a tenant and click **View Details**. The following tabs appear:

  - **Summary**—Displays the overview of the tenant.
  - **Application Profile**—Displays the name, tenant, description, and QoS Class of the tenant application profile. Click **Add** to add a tenant application profile. Choose an application profile and click **View Details** to view the EPGs of the application profile.

Choose an EPG and click **View Details** to view the provided contracts, consumed contracts, Layer 4 to Layer 7 EPG parameters, consumed contract interface, static node, domain, static path, and subnet of the EPG. In the **Consumed Contract Interface** tab, click **Add** to add a consumed contract interface to EPG.

- **Deployed Service Graph**—Displays the list of service graphs that are deployed in the tenant. Choose a service graph and click **View Details** to view the Layer 4 to Layer 7 deployed service graph parameters.
- **Filters**—Displays the tenant, name, and description of the filters. To view the tenant filter rules, choose a filter and click **View Details**.
- **External Bridge Network**—Displays the tenant, name, and description of the external bridge network. Choose a network and click **View Details** to view the following tabs:
  - **External Network**—Choose an external network and click **View Details** to view the provided contracts, and consumed contracts details.
  - **Node Profile**—Choose a node profile and click **View Details** to view the interface profile details.
- **External Routed Networks**—Displays the tenant, name, and description of the external routed network. Choose a network and click **View Details** to view the following tabs:
  - **Route Profile**—Choose a route profile and click **View Details** to view the context details.
  - **Logical Node Profile**—Choose a logical node profile and click **View Details**. The following tabs appear:
    - **Logical Nodes** tab—Displays the logical nodes. Click **Add** to add a logical node to the logical node profile of the external routed network. Choose a logical node and click **View Details** to view the static routes to the logical node.
    - **Logical Interface Profile** tab—Choose a logical interface profile and click **View Details** to view the logical interface and logical OSPF interface. Click **Add** in the Logical OSPF Interface tab to create an interface profile with the OSPF profile data.
    - **BGP Peer Connectivity** tab—Displays the BGP peer connectivity of the logical node profile. Click **Add** to add a peer connection to a node profile.
  - **External Network**—Choose an external network and click **View Details** to view the subnet, provided contracts, and consumed contracts details. You can tag an external network and consumed contract using the **Add Tags** option. The tag is used to identify the network and contract that you want to use in the application container deployment.
- **Bridge Domains**—Displays the tenant, name, description, segment ID, unicast traffic, ARP flooding, multicast IP address, customer MAC address, unicast route, and Layer 2 unknown unicast value.

  To view more details about a bridge domain, choose a bridge domain and click **View Details**. The following tabs appear:
  - **DHCP Relay Label**—Displays the tenant, name, description, and scope of the DHCP relay.
  - **Subnet**—Displays the tenant, bridge domain, description, subnet control, and gateway address of the tenant.
- **Private Networks**—Displays the tenant name, name, description, policy control, and segment of the private networks. Click **Add** to add a private network.
- **BGP Timers**—Displays the tenant, name, graceful restart control, hold interval, keepalive interval, and stale interval of the Border Gateway Protocol (BGP) timer.

- **Contracts**—Displays the tenant, name, description, type, QoS, and scope of the contracts.

  To view more details about a contract, choose a contract and click **View Details**. The following tabs appear:

  - **Contract Subject**—Choose a contract subject and click **View Details** to view the filter chain, filter chain for consumer to provider, filter chain for provider to consumer, provided label, and consumed label. Each tab has the **Add** option to add a filter, in term filter, out term filter, provided label, and consumed label to a contract subject.
  - **Exported Tenants**—Displays the contracts of the exported tenants.

- **Taboo Contracts**—Displays the tenant, name, description, and scope of the taboo contracts.
- **Relay Policy**—Displays a list of the relay policies.
- **Option Policy**—Displays a list of the option policies.
- **End Point Retention**—Displays the tenant, name, description, hold interval, bounce trigger, bounce entry aging interval, local endpoint aging interval, remote endpoint aging interval, and move frequency of the tenant.
- **OSPF Interface**—Displays the tenant, name, description, network type, priority, cost of interface, interface controls, hello interval, dead interval, retransmit interval, and transmit delay of the Open Shortest Path First (OSPF) interface. Click **Create** to create an OSPF interface policy.
- **EIGRP Interface**—Displays the EIGRP Interface details.
- **OSPF Timers**—Displays the OSPF timer details.
- **IGMP Snoop**—Displays the IGMP snoop details.
- **Custom QOS**—Displays the custom QoS details.
- **Action Rule Profile**—Displays the action rule profiles of the tenant. Click **Create** to create an action rule profile. In the **Create Action Rule Profile** dialog box, enter the name and description of the action rule profile. To set an action rule based on a route tag, check the **Set Rule Based On Route Tag** check box.
- **L4-L7 Service Graph**—Displays the Layer 4 to Layer 7 service graph details. Choose a service graph and click **View Details** to view the following tabs:
  - **Consumer EPG**—Displays the list of EPGs that are labeled as consumer in tenants. When an EPG consumes a contact, the endpoints in the consuming EPG may start communication with any endpoint in an EPG that is providing that contract.
  - **Provider EPG**—Displays the list of EPGs that are labeled as provider in tenants. When an EPG provides a contract, communication with that EPG can be initiated from other EPGs as long as the communication complies with the provided contract.
  - **Nodes**—Displays the list of nodes in the tenant. Choose a node and click **View Details** to view the node functions and connectors of the node. Choose a node function and click **View Details** to view the Layer 4 to Layer 7 function node parameters.
  - **Connections**—Displays the list of connections in the tenant. Choose a connection and click **View Details** to view the connection terminals in the tenant.

- **Function Profile Group**——Displays the function profile groups of tenants. Choose a function profile group and click **View Details** to view the function profiles of the group. Click **Add** to add a function profile. To view more details about a function profile, choose a function profile and click **View Details**. The following tabs appear:

- **Function Profile Parameter**—Displays the function profile parameters. In the **Function Profile Parameter** tab, you can add an ACL, an interface, and add a bridge group interface to a function profile, and add a network object to a function profile. Choose a function profile parameter and click **View Details** to view the function profile parameter configuration and function profile parameter level-one folder.
- **L4-L7 Function Profile Parameters**—Displays the list of Layer 4 to Layer 7 function profile parameters.
- **Function Profile Function Parameter**—Displays the list of function profile function parameters. Click **View Details** to view the function profile function parameter Rel details.

- **Device Clusters**—Displays the device cluster details. To view more details about a device cluster, choose a device cluster and click **View Details**. The following tabs appear:
  - **Device Cluster State**—Displays the cluster name, device state, and configured status of the device.
  - **Concrete Device**—Displays the list of concrete devices. Choose a concrete device and click **View Details** to view the virtual network interface card (vNIC) to concrete interface and the path to concrete interface.
  - **Logical Interface**—Displays the list of logical interfaces in the device cluster. Choose a logical interface and click **View Details** to view the logical interface details.
- **Deployed Device Cluster**—Displays the device clusters that are deployed in the tenant.
- **Imported Device Cluster**—Displays the device clusters that are imported in the tenant.
- **Router Configurations**—Displays the router configurations of the tenant. Click **Add** to add a router configuration.
- **Logical Device Context**—Displays the logical device context details. Choose the logical device context and click **View Details** to view the logical interface context.

- **L3 Domain** tab—Displays a list of Layer 3 domains in the APIC accounts. To create a Layer 3 domain, click **Create (+)**.

  On the **Create L3 Domain** screen, complete the following fields:
  - **L3 Domain** field—Name of the Layer 3 domain.
  - **Associated Attachable Entity Profile** field—Click **Select** and check an attachable access entry profile that you want to associate with the Layer 3 domain.
  - **VLAN Pool** field—Click **Select** and check a VLAN pool.
  - Click **Submit**.

- **L2 Domain** tab—Displays a list of Layer 2 domains in the APIC accounts. To create a Layer 2 domain, click **Create(+)**.

  On the **Create L2 Domain** screen, complete the following fields:
  - **L2 Domain** field—Name of the Layer 2 domain.
  - **Associated Attachable Entity Profile** field—Click **Select** and check an attachable access entry profile that you want to associate with the Layer 2 domain.
  - **VLAN Pool** field—Click **Select** and check a VLAN pool.
  - Click **Submit**.

- **VM Networking** tab—Displays the virtual machine (VM) networks with the vendor detail.

  To view more details about a VM network, choose a VM and click **View Details**. The following tab appears:

  - **Domains**—Displays a list of VMware domains with the vendor details. Choose a VMware domain and click **View Details** to view the VMware domain controllers, vCenter credential, and vCenter/vShield. Choose a VMware domain controller and click **View Details** to view the distributed virtual switch (DVS), hypervisors, and virtual machine. Choose a DVS and click **View Details** to view the DVS port groups.

- **L4-L7 Service Device Types** tab—Displays the Layer 4 to Layer 7 service device types with their model, vendor, version, and capabilities.

  To view more details about the Layer 4 to Layer 7 service device type, choose a Layer 4 to Layer 7 service device type and click **View Details**. The following tabs appear:

  - **L4-L7 Service Device Properties**—Displays the vendor, package name, package version, and logging level of Layer 4 to Layer 7 service device types.
  - **L4-L7 Service Device Interface Labels**—Displays a list of interface labels.
  - **L4-L7 Service Functions**—Displays a list of service functions. Choose a service function and click **View Details** to view the details of the Layer 4 to Layer 7 service function connectors.

- **Fabric Nodes Topology** tab—Displays the topology details of fabric nodes.
- **L2 Neighbors** tab—Displays the Layer 2 neighbor details that include the protocol, fabric name, device ID, capability, port ID, local interface, hold time, and platform.
- **Deployed Service Graph** tab—Displays the tenant, contract, state, service graph, context name, node function, and description of the APIC account.
- **EPG to Contract Association** tab—Displays the details of the contract association with EPGs.
- **Access Port Policy Groups** tab—Displays the access port policy group name, link level policy, Cisco Discovery Protocol (CDP) policy, Link Aggregation Control Protocol (LACP) policy, Link Layer Discovery Protocol (LLDP) policy, link aggregation type, and attached entity profile of the accounts in the APIC server.
- **Fabric Interface Profiles** tab—Displays the fabric interface profiles of the APIC server.

  To view more details about a fabric interface profile, choose a profile and click **View Details**. The following tab appears:

  - **Access Port Selector**—Displays the access port selectors of the fabric interface profile. Click **Add** to add an access port selector to the fabric interface profile. Choose an access port selector and click **View Details** to view the port blocks and sub port blocks of the access port selector.

- **Fabric Configured Switch Interfaces** tab—Displays the fabric configured switch interfaces of the APIC server.
- **Fabric Switch Profiles** tab—Displays the fabric switch profiles of the APIC server.

Assigning an APIC Account to a Pod

In the **Converged** menu of the user interface (UI), Cisco UCS Director displays the converged stack of devices for a data center. To display the APIC account in the converged UI, assign the APIC account to a pod.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account that you want to assign to a pod.

Step 4 From the **More Actions** drop-down list, choose **Assign to Pod**.

The **Assign to Pod** screen appears.

Step 5 Click **Select** and check a pod to which you want to assign the APIC account.

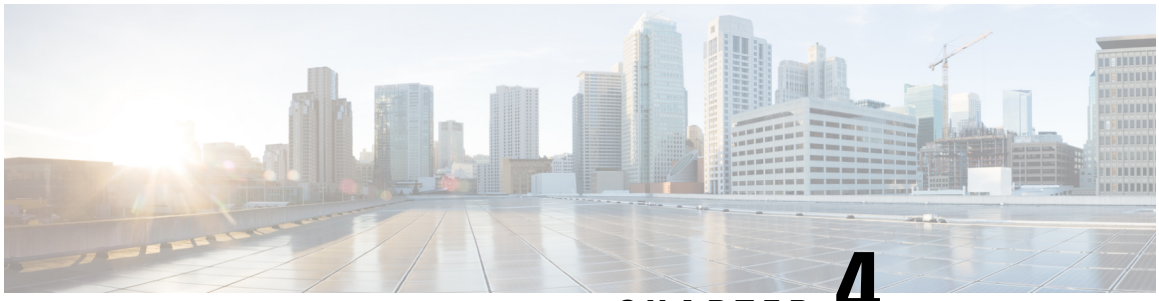
Step 6 Click **Submit**.
The APIC account appears in the converged UI.

Handling APIC Failover

APIC controllers are deployed in an APIC cluster. The recommendation is to have a minimum of three APIC controllers per cluster to ensure high availability. When you create an APIC account in Cisco UCS Director, provide the IP address of one of the APIC controllers in the APIC cluster. Cisco UCS Director discovers the other APIC controllers in the APIC cluster and their respective IP addresses.

If the IP address of the controller which was used to manage the APIC device goes down or is not reachable for 45 seconds, Cisco UCS Director tries to use any of the reachable controller IP addresses to interact with the APIC device.

If you have multiple ACI fabrics and each fabric with multiple controllers, one of the controllers of the ACI fabric is used to manage the APIC device. If the controller goes down or is not reachable for 45 seconds, Cisco UCS Director uses the next reachable controller within the ACI fabric.



CHAPTER 4

Managing Tenants

Tenants

A tenant is a logical container for application policies that enables you to exercise domain-based access control by isolating the resources such as applications, databases, web servers, network-attached storage, virtual machines, firewalls, Layer 4 to Layer 7 services, and so on. Tenants can represent a customer in a service provider setting, an organization or domain in an enterprise setting, or just a convenient grouping of policies.

A fabric can contain anywhere from one tenant, which may be useful for a small commercial environment, to 64,000+ tenants, for a cloud service provider in which case you assign each company their own tenant. Another use case would be to have a Dev tenant and a Production tenant. In this case, you create network constructs, EPGs, and policies in Dev tenant first and then simply copy it to the Production tenant. It ensures that the dev and prod are the exact same and takes away the human error that comes along with manual copying of these objects.

Note Configure a tenant before you can deploy any Layer 4 to Layer 7 services.

Tenant Types

The system provides the following four kinds of tenants:

- User tenant—Defined by the administrator according to the needs of users. It contains policies that govern the operation of resources such as applications, databases, web servers, network-attached storage, virtual machines, and so on.

- Common tenant—Provided by the system but can be configured by the fabric administrator. It contains policies that govern the operation of resources accessible to all tenants, such as firewalls, load balancers, Layer 4 to Layer 7 services, intrusion detection appliances, and so on.
- Infrastructure tenant—It contains policies that govern the operation of infrastructure resources such as the fabric VXLAN overlay.
- Management tenant—It contains policies that govern the operation of fabric management functions used for in-band and out-of-band configuration of fabric nodes.

Tenant Features

- Tenants can be isolated from one another or can share resources.
- Tenants do not represent a private network.
- Entities in the tenant inherit its policies.
- The primary elements that the tenant contains are filters, contracts, outside networks, bridge domains, Virtual Routing and Forwarding (VRF) instances, and application profiles that contain endpoint groups (EPGs).

Note In the APIC GUI under the tenant navigation path, a VRF (context) is called a private network.

Setting up a Tenant

This procedure provides an overview of how to set up a tenant for an APIC account in Cisco UCS Director.You can also use the workflows provided in Cisco UCS Director Orchestration to complete a guided setup of tenants for various use cases. For more information, see Cisco UCS Director Orchestration Guide.

This procedure assumes that you have already completed the following prior to creating tenants:

- The Day 0 setup of ACI fabric.
- The nodes in ACI fabric are connected and discovered.
- The APIC controller cluster has been configured.
- Cisco UCS Director is configured and the ACI pod has been set up.

Step 1 Create a Tenant.

See Creating a Tenant, on page 17.

Step 2 Create a Virtual Routing and Forwarding (VRF) (also known as Private Network).

See Creating a VRF, on page 20.

Step 3 Add Bridge Domain to the VRF.

See Adding a Bridge Domain to VRF, on page 21.

Step 4 Create Application Profiles.

See Creating an Application Profile for the Tenant, on page 25.

Step 5 Create EPGs.

See Adding an EPG, on page 26.

Step 6 Add domain to EPGs.

See Adding a Domain to an EPG, on page 27.

Step 7 Add Static path to EPGs.

See Adding a Static Path to EPG, on page 28.

Step 8 Create Contracts.

See Creating Contracts, on page 32.

Step 9 Add contracts to EPGs.

See Adding a Consumed Contract to an EPG, on page 35.

See Adding a Provided Contract to an EPG, on page 34.

Creating a Tenant

Before you begin

Verify that Tags, monitoring policy, and security domains for the objects in the APIC account are configured before adding a tenant.

Create users in ACI and assign a security domain to the users or user groups. See User Access, Authentication, and Accounting chapter in Cisco APIC Basic Configuration Guide.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click **Add**.

Step 6 On the **Add APIC Tenant** screen, complete the fields, including the following:

a) Add a unique name and description for the Tenant.

b) (Optional) Click **Select** and check the tag you want to use.

Tags are used to assign a descriptive name to a group of objects. For example, to enable easy searchable access to all web server EPGs, assign a web server tag to all such EPGs. Web server EPGs throughout the fabric can be located by referencing the web server tag.

c) (Optional) Click **Select** and check the monitoring policy that you want to use.

When you apply a monitoring policy, it overrides the default monitoring policy.

d) Click **Select** and check the security domain that you want to use.

It is necessary to also assign the user to one or more security domains. By default, the ACI fabric includes two special pre-created domains:

- **All**—Allows access to the entire management information tree (MIT).
- **Infra**—Allows access to fabric infrastructure objects/subtrees, such as fabric access policies.

For example, if you have created a security domain for Production, given users roles, and attached them to that security domain, then choose the Production security domain instead of **All**.

e) Click **Submit**.

What to do next

After creating a tenant, create a VRF (also known as a private network) for the tenant.

Viewing Tenants

You can view a list of tenants that are onboarded in Cisco UCS Director and its details.

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Tenant**.

Step 3 Click the row with the tenant for which you want to view details.

Step 4 Click **View Details** to view the service offerings of the tenant.

Step 5 Click the row with the service offering and click **View details** to view the resource groups of a tenant.

Note If the disaster recovery support is enabled for the tenant, the resource groups of the primary site and the disaster recovery site are displayed.

Step 6 Click the row with the resource group and click **View details** to view the following information:

- **Resource Entity**—Displays a list of available resources, such as, VMWare cluster, resource pool, and data store, in a vPOD. During tenant onboarding, the resources matching the capacity, capability and tag of the tenant requirement are filtered from resource group and matched resources are added to the vPOD. With the capacity expansion support, the vPOD can store more than one resources for each resource type such as VMware cluster, resource pool, and storage pool. As multiple resources of same resource type is available in vPOD, the tenant expansion is possible after consumption of allocated resources.

  The tenant-specific and container-specific resource limits assist in provisioning VMs and BMs. During provisioning, all the available resources in vPOD are referred to find out the matching resources for resource allocation. After the resource filtration and selection, the matching resources from the same account are allocated for VM deployment.

  When a resource is no longer consumed by the container, you can delete the resource. To delete the resource, click the row with the resource and click **Delete**.

- **Tenant Details**—Displays more details of the tenant.
- **Tenant Resource Limits**—Displays availability of both virtual and physical resources in a tenant. The resources reserved during tenant onboarding are displayed along with the used and available resource values. The VDCs Limit

column specifies the maximum number of containers that are reserved for the tenant. The Available Number of VDCs column represents the number of containers that are available for provisioning. The physical resource limits display the blades that are reserved as part of tenant onboarding, along with the number of blades used for bare metal provisioning.

- **Container Resource Limits**—Displays availability of both virtual and physical resources in a container. The resource limits that are set during container creation are displayed along with the used and available resources.

  Note If a container is created without a resource limit, the value of the virtual resources is displayed as Not Set.

- **Private Network**—Displays the private networks created for the tenant. Click the row of a private network and click **View Details** to view the supernet and subnet pools of the private network. The **Supernets** screen lists the supernets available for the tiers. The **Subnets** screen displays the sub-network pool that is used for load balancer configuration during the container deployment.

Virtual Routing and Forwarding (VRF)

A Virtual Routing and Forwarding (VRF) is similar to a virtual router that defines a Layer 3 address domain. It is an IP technology that allows multiple instances of a routing table to coexist on the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflict. For example, a production VRF could be on the same network as the development VRF but the two have different default gateways.

A tenant can have multiple VRFs (also known as private network). One or more bridge domains are associated with a VRF. There are several policies you can associate with a private network, including OSPF and BGP timers, as well as how long end points should be retained.

Virtual Routing and Forwarding (VRF) Guidelines

The following guidelines and limitations apply for virtual routing and forwarding (VRF) instances:

- Within a single VRF instance, IP addresses must be unique. Between different VRF instances, you can have overlapping IP addresses.
- If shared services are used between VRF instances or tenants, make sure that there are no overlapping IP addresses.
- Any VRF instances that are created in common tenant is seen in other user-configured tenants.
- VRF supports enforced mode or unenforced mode. By default, a VRF instance is in enforced mode, which means all endpoint groups within the same VRF instance cannot communicate to each other unless there is a contract in place.
- Switching from enforced to unenforced mode (or the opposite way) is disruptive.

For more in-depth information, see the Cisco Application Centric Infrastructure Fundamentals Guide.

Creating a VRF

A Virtual Routing and Forwarding (VRF) object (also known as private layer 3 network in ACI) contains the Layer 2 and Layer 3 forwarding configuration, and IP address space isolation for tenants. Each tenant can have one or more VRFs, or share one default VRF with other tenants as long as there is no overlapping IP addressing being used in the ACI fabric.

Before you begin

Verify that you have configured the BGP Timers Policies and OSPF Timers

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Private Networks**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Private Network** screen, complete the following fields:

a) Add a unique name for the private network.

b) From the **Policy Enforcement** drop-down list, choose from the following options:

- **Enforced**—Security rules (contracts) are enforced.
- **Unenforced**—Security rules (contracts) are not enforced.

The default is **enforced**.

c) Enter the description for the private network.

d) Click **Select** and check the BGP timer that you want to use.

The Border Gateway Protocol (BGP) timer policy enables you to specify the intervals for the periodic activities and supplies two options for graceful restart control.

e) Click **Select** and check the OSPF timer that you want to use.

The context-level OSPF timer policy provides the Hello timer and Dead timer intervals configuration. OSPF timers control the behavior of protocol messages and shortest path first (SPF) calculations.

f) Click **Select** and check the monitoring policy that you want to associate with the tenant.

When you apply a monitoring policy, it overrides the default monitoring policy.

g) Click **Submit**.

What to do next

After creating a private network, you create a bridge domain and link it to this VRF.

Bridge Domains

A bridge domain represents a Layer 2 forwarding construct within the fabric. It helps you to constrain broadcast and multicast traffic. It is a logical container for subnets.

A bridge domain must have at least one subnet associated with it but can contain multiple subnets. When you configure a bridge domain with multiple subnets, the first subnet added becomes the primary IP address on the SVI interface. Subsequent subnets are configured as secondary IP addresses. When the switch reloads, the primary IP address can change unless it is marked explicitly.

One or more EPGs can be associated with each bridge domain. EPGs within the same bridge domain may be configured to talk to each other, but they do not have layer 2 adjacency enabled by default.

Bridge domains in Cisco Application Centric Infrastructure (ACI) have several configuration options to allow the administrator to tune the operation in various ways. To learn more about the various options, see Cisco Application Centric Infrastructure Fundamentals Guide.

Note Once a bridge domain is configured, its mode cannot be switched.

A bridge domain must be linked to a Virtual Routing and Forwarding (VRF).

Subnets

A subnet defines the IP address range that can be used within the bridge domain. A bridge domain can contain multiple subnets, but a subnet is contained within a single bridge domain. The scope of a subnet can be public, private, or shared under a bridge domain or an EPG. See Adding a Subnet to a Bridge Domain, on page 23.

DHCP Relay Labels

DHCP Relay is required only when the DHCP server is in a different EPG or private network than the clients. DHCP label associates the provider DHCP server with the bridge domain. The DHCP label object also specifies the owner. If your infrastructure requires DHCP relay labels, see Adding a DHCP Relay Label to a Bridge Domain, on page 24.

Note The bridge domain DHCP label must match the DHCP Relay name. Label matching enables the bridge domain to consume the DHCP Relay.

Adding a Bridge Domain to VRF

A bridge domain is a unique Layer 2 forwarding domain that contains one or more subnets. Each bridge domain must be linked to a VRF.

Before you begin

Create a Tenant for your customer, organization, or domain and configure your private network.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Bridge Domains**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Bridge Domain** screen, complete the following fields:

a) Add a unique name and description for the Bridge Domain.

b) Click **Select** and check the network you want to use for the account.

This is the virtual routing and forwarding (VRF) object associated with the tenant for which this bridge domain is created. It is also known as context or private network.

c) From the **Forwarding** drop-down list, choose the forwarding parameter from the following options:

This sets the forwarding capacity between Layer 2 and Layer 3 networks. The values can be:

- **Optimize**—Automatically sets the Unicast and ARP parameters. Selects options: Hardware Proxy for L2 Unknown Unicast and Flood for Unknown Multicast Flooding with Unicast Routing enabled.
- **Custom**—Reveals the Unicast and ARP selections for custom configuration. If you choose custom forwarding, then complete the following additional parameters:

  1. From the **L2 Unknown Unicast** drop-down list, select the unicast parameter. The values can be **Flood** or **Hardware Proxy**.

     The default is Hardware Proxy. If enabled, unicast traffic flooding is blocked at a specific port, only permitting egress traffic with MAC addresses that are known to exist on the port. If you chose Flood, it floods the unicast traffic to all Layer 2 ports.

  2. From the **Unknown Multicast Flooding** drop-down list, select the multicast parameter. The values can be **Flood** or **Optimized Flood**.

  3. Check **ARP Flooding** to configure the flooding for the bridge domain.

     This enables ARP flooding, so that the Layer 2 broadcast domain maps IP addresses to the MAC addresses. If flooding is disabled, unicast routing is performed on the target IP address.

  4. Check **Unicast Routing** to configure the bridge domain routing. This forwarding method is based on predefined forwarding criteria (IP or MAC address). The default is layer 3 forwarding (IP address).

d) Check **Custom Mac Address** to configure the bridge domain Mac address and enter the address in **Mac Address** field.

By default, a bridge domain takes the fabric wide default MAC address of 00:22:BD:F8:19:FF. Configure this property to override the default address.

e) By default, the **Endpoint Dataplane Learning** drop-down list is set to true to enable data-plane IP learning on remote and local leaf switches.

f) The **Limit IP Learning to Subnet** drop-down list appears only when the **Endpoint Dataplane Learning** drop-down list is set to true. By default, the value of the **Limit IP Learning to Subnet** drop-down list is set to true. If this option is set to true, the fabric will learn only IP addresses for subnets configured on the bridge domain.

g) Click **Select** and check the IGMP snoop policy you want to use for this tenant.

This policy inspects the IGMP membership report messages from interested hosts. It limits the multicast traffic to the subset of VLAN interfaces on which the hosts reside.

h) Click **Select** and check the L3 out interface that you want to assign to this tenant.

This is the name of the Layer 3 outside interface associated with this object.

i) Click **Select** and check the route profile of L3 out network.

L3 Out is the network outside the fabric, configured for the tenant consuming this bridge domain, that is reachable by a specific route to external networks of a tenant application. The route profile specifies policies for external networks.

j) Click **Select** and check the monitoring policy associated with the tenant.

Step 9 Click **Submit**.

Adding a Subnet to a Bridge Domain

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Bridge Domains**.

Step 7 On the **Bridge Domains** page, choose the row with the domain to which you want to add the subnet and click **View Details**.

Step 8 Click **Subnet**.

Step 9 On the **Subnet** page, click **Add**.

Step 10 On the **Add Subnet to Tenant Bridge Domain** screen, complete the following fields:

a) In the **Gateway IP (Address)** field, enter the IP address of the default gateway.

b) In the **Gateway IP (Prefix)** field, enter a prefix in the range of 1-30 that starts with "/x"

c) Check the **Shared Subnet** check box to share the subnet with multiple contexts (VRFs) in the same tenant or across tenants as part of a shared service.

Shared subnets must be unique across the contexts (VRF) involved in the communication. When a subnet under an EPG provides a Layer 3 external network shared service, such a subnet must be globally unique within the entire ACI fabric.

d) Check the **Public Subnet** check box to export it to a routed connection.

e) Check the **Private Subnet** check box to apply the subnet only within its tenant.

f) Check the **Subnet Control (Querier IP)** check box to apply specific protocol to the subnet. Querier IP enables IGMP Snooping on the subnet.

g) Click **Select** and check the L3 out for route profile that you want to use for the bridge domain.

This is the Layer 3 Outside Network (L3extOut) configured for the tenant consuming this bridge domain.

h) Click **Select** and check the route profile that you want to use for this bridge domain.

The route profile specifies policies for external networks.

i) Click **Submit**.

Adding a DHCP Relay Label to a Bridge Domain

DHCP Relay is required when the DHCP server is in a different EPG or private network than the clients. A DHCP relay label contains a name for the label, the scope, and a DHCP option policy. The scope is the owner of the relay server and the DHCP option policy supplies DHCP clients with configuration parameters such as domain, nameserver, and subnet router addresses.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Bridge Domains**.

Step 7 Click the row with the domain to which you want to add the DHCP label and click **View Details**.

Step 8 Click **DHCP Relay Label**.

Step 9 On the **DHCP Relay Label** page, click **Add**.

Step 10 On the **Add DHCP Label To Tenant Bridge Domain** screen, complete the following fields:

a) From the **Scope** drop-down list, choose the scope. Options are:

- **Infra**—The owner is the infrastructure.
- **Tenant**—The owner is the tenant.

The default is **Infra**.

b) Click **Select** and check the DHCP relay policy that you want to use for the tenant bridge domain.

c) Click **Select** and check the DHCP option policy that you want to use.

d) Click **Submit**.

Application Profiles

Application profiles are logical containers that define the policies, services, and relationships between End Point Groups (EPGs). Each application profile contains one or more EPG that can communicate with the other EPGs in the same application profile, and with EPGs in other application profiles according to the contract rules. At minimum, associate one application profile with one EPG.

Modern applications contain multiple components. An application profile models the requirements of an application. For example, an e-commerce application could require a web server, a database server, data

located in a storage area network, and access to outside resources that enable financial transactions. The application profile contains as many (or as few) EPGs as necessary that are logically related for the e-commerce application.

EPGs can be organized according to one of the following:

- The application they provide (such as sap in the example in Appendix A).
- The function they provide (such as infrastructure).
- Where they are in the structure of the data center (such as DMZ).
- Whatever organizing principle that a fabric or tenant administrator chooses to use.

Creating an Application Profile for the Tenant

The application profile is a set of requirements that an application instance has on the virtualized fabric. The policy regulates connectivity and visibility among endpoints within the scope of the policy.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Application Profile** screen, complete the following fields:

a) Add a unique name, description, and an alias for the Application Profile.

b) Click **Select** and check the tag name that you want to use for the APIC account.

c) From the **QoS Class** drop-down list, choose from the following options for the priority class:

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value

d) Click **Select** and check the monitoring policy associated with the tenant.

When you apply a monitoring policy, it overrides the default monitoring policy.

Step 9 Click **Submit**.

End Point Groups

An End Point Group (EPG) is a logical container of endpoints that have common policy requirements such as security, virtual machine mobility (VMM), QoS, or Layer 4 to Layer 7 services. They have an address (identity), a location, attributes (such as version or patch level), and can be physical or virtual. Knowing the address of an endpoint enables access to all its other identity details. Rather than configure and manage endpoints individually, they are placed in an EPG and are managed as a group.

The ACI fabric can contain the following types of EPGs:

- Application endpoint group
- Layer 2 external outside network instance
- Layer 3 external outside network instance
- Management endpoint groups for out-of-band or in-band access

By default, all endpoints in the same endpoint group can talk to each other without requiring a contract. Intra-endpoint group (intra-EPG) isolation prevents all endpoints in an EPG from talking to each other but inter-EPG communication is still permitted if there is a contract. This is similar to a private VLAN. For example, assume that you have three endpoints: two are in the client endpoint group, while the other endpoint is in the Web endpoint group. If there is a contract between endpoint groups, they can talk to each other.

Regardless of how an EPG is configured, EPG policies are applied only to the endpoints they contain. For example, to configure a WAN router connectivity to the fabric, you configure an EPG that includes any endpoints within the associated WAN subnet. The fabric learns of the endpoints through a discovery process and applies the policies accordingly.

After creating an EPG, add a static path to the EPG to determine the port and leaf/node for the traffic. See Adding a Static Path to EPG, on page 28.

You can also add static nodes (leaf, spine, or APIC), and domains (physical, VMM, L3, or L3 external - see examples) to EPGs and define how and when they are deployed. See Adding a Static Node to EPG, on page 30 and Adding a Domain to an EPG, on page 27.

Adding an EPG

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the profile that you want to update and click **View Details**.

Step 8 Click **EPG**.

Step 9 Click **Add**.

Step 10 On the **Add Tenant EPG** screen, complete the required fields including the following:

a) Add a unique name, description, and alias for the EPG.

b) (Optional) Click **Select** and check the tag you want to use.
c) From the **QoS Class** drop-down list, choose from the following options for the priority class:

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value
- **Custom**—Complete the additional parameter

d) If you chose custom QoS, click **Select** and check the customized quality of service (QoS) class that you want to use for the EPG.
e) Click **Select** and check the bridge domain for the EPG.
f) Click **Select** and check the monitoring policy associated with the tenant.

When you apply a monitoring policy, it overrides the default monitoring policy.

g) Click **Submit**.

Adding a Domain to an EPG

An EPG is associated with domains by being linked to a domain profile, which can be a VMM, physical, Layer 2 external, or Layer 3 external domain.

Before you begin

Create a physical, VMM, Layer 3, or Layer 2 domain for the APIC account.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Domain**.
Step 11 Click **Add**.
Step 12 On the **Add Domain To EPG** screen, complete the required fields, including the following:
a) Click **Select** and check the domain profile that you want to add to the EPG.
b) From the **Deploy Immediacy** drop-down list, choose a path from the following options:

- **Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as it is downloaded in the leaf software.

- **On Demand**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

c) From the **Resolution Immediacy** drop-down list, choose a path from the following options:

It specifies whether policies are resolved immediately or when needed.

- **Immediate**—Specifies that EPG policies (including contracts and filters) are downloaded to the associated leaf switch software upon hypervisor attachment to VDS. LLDP or OpFlex permissions are used to resolve the hypervisor to leaf node attachments.
- **On Demand**—Specifies that a policy (for example, VLAN, VXLAN bindings, contracts, or filters) is pushed to the leaf node only when a hypervisor is attached to VDS and a VM is placed in the port group (EPG).
- **Pre-provision**—Specifies that a policy (for example, VLAN, VXLAN binding, contracts, or filters) is downloaded to a leaf switch even before a hypervisor is attached to the VDS. Therefore, this option pre-provisions the configuration on the switch.

d) From the **Allow Promiscuous** drop-down list, choose from the following options:

It enables all packets to pass to the VMM domain, which is often used to monitor network activity.

- **Reject**—Packets that do not include the network address are dropped.
- **Accept**—All traffic is received within the VMM domain.

e) From the **Forged Transmits** drop-down list, choose from the following options:

- **Reject**—All non-matching frames are dropped.
- **Accept**—Non-matching frames are received.

It specifies whether to allow forged transmits. A forged transmit occurs when a network adapter starts sending out traffic that identifies itself as something else. This security policy compares the effective address of the virtual network adapter and the source address inside an 802.3 Ethernet frame generated by the virtual machine to ensure that they match.

f) From the **MAC Changes** drop-down list, choose from the following options:

- **Reject**—Does not allow new MAC addresses.
- **Accept**—Allows new MAC addresses.

It enables you to define new MAC addresses for the network adapter within the virtual machine (VM).

g) Click **Submit**.

Adding a Static Path to EPG

Static path policies provide a summary of the configured properties of the policy, fault counts, and history for the static path. Configure the static path to the destination EPG.

Note When an EPG uses a static binding path, the encapsulation VLAN associated with this EPG must be part of a static VLAN pool.

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the profile that you want to update and click **View Details**.

Step 8 Click **EPG**.

Step 9 Click the row with the EPG that you want to update and click **View Details**.

Step 10 Click **Static Path**.

Step 11 Click **Add**.

Step 12 On the **Add Static Path To EPG** screen, complete the following fields:

a) From the **Path Type** drop-down list, choose from the following options:

- **Port**—Is the default value
- **Direct Port Channel**—Class 1 Differentiated Services Code Point (DSCP) value
- **Virtual Port Channel**—Class 2 DSCP value

b) Click **Select** and check the static path that you want to add to the EPG.

c) In the **Encapsulation** field, enter a VLAN value that is part of one of the static VLAN blocks associated with the domain.

d) From the **Deployment Immediacy** drop-down list, choose from the following options:

- **Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as it is downloaded in the leaf software.
- **On Demand**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

Once EPG policies are downloaded to the leaf software, you can choose the deployment preferences to specify when a policy is pushed into leaf switches.

e) From the **Mode** drop-down list, choose the static association from the following options:

EPG tagging refers to configuring a static path under an EPG.

- **Tagged**—Select this mode if the traffic from the host is tagged with a VLAN ID.
- **Untagged**—Select this mode if the traffic from the host is untagged (without VLAN ID).

When a leaf switch is configured for an EPG to be untagged, for every port this EPG uses, the packets exit the switch untagged.

Note When an EPG is deployed as untagged, do not deploy that EPG as tagged on other ports of the same switch.

- **802.1P Untagged**—Select this mode if the traffic from the host is tagged with a 802.1P tag. When an access port is configured with a single EPG in native 802.1p mode, its packets exit that port untagged. When an access port is configured with multiple EPGs, one in native 802.1p mode, and some with VLAN tags, all packets exiting that access port are tagged VLAN 0 for EPG configured in native 802.1p mode and for all other EPGs packets exit with their respective VLAN tags.

  Note Only one native 802.1p EPG is allowed per access port.

f) Click **Submit**.

Adding a Static Node to EPG

Before you begin

Create nodes in the APIC system.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the profile that you want to update and click **View Details**.

Step 8 Click **EPG**.

Step 9 Click the row with the EPG that you want to update and click **View Details**.

Step 10 Click **Static Node**.

Step 11 Click **Add**.

Step 12 On the **Add Static Node To EPG** screen, complete the following fields:

a) Click **Select** and check the node that you want to add to the EPG.

b) In the **Encapsulation** field, enter a VLAN value that is part of one of the static VLAN blocks associated with the domain.

c) From the **Mode**drop-down list, choose the static association from the following options:

- **Native**
- **Regular**

d) From the **Deployment Immediacy** drop-down list, choose the policy from the following options:.

- **Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as the policy is downloaded in the leaf software.
- **Lazy**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.

Once EPG policies are downloaded to the leaf software, you can choose the deployment preferences to specify when a policy is pushed into leaf switches.

e) Click **Submit**.

Contracts

EPGs can only communicate with other EPGs according to contract rules. Contracts determine the type of traffic that can pass between EPGs, including the protocols and ports allowed. If there is no contract, inter-EPG communication is disabled by default. There is no contract required for intra-EPG communication. A contract contains one or more subjects.

An EPG can both provide and consume the same contract. An EPG can also provide and consume multiple contracts simultaneously.

Contract Subjects

A subject is a sub-application running behind an endpoint group. A contract can encapsulate multiple subjects. An EPG associates with a subject and defines rules under the association for consuming, providing, or for peer-to-peer communications to that subject. Subjects contain filters and optional labels.

Export Contract feature enables you to export the XML or JSON code for later use with the REST API.

Provider and Consumer Contracts

Contracts can contain multiple communication rules and multiple endpoint groups. The relationship between an EPG and a contract can be either a provider or consumer. When an EPG provides a contract, communication with that EPG can be initiated from other EPGs as long as the communication complies with the provided contract. When an EPG consumes a contract, the endpoints in the consuming EPG may initiate communication with any endpoint in an EPG that is providing that contract.

Filters

Filters enable you to specify the protocols you want to permit for traffic management between two EPGs. For example, you may want to permit only `https` traffic. There are several types of filters.

- Permit—It allows traffic.
- Deny (Taboo)—For specific use cases. You may specify to allow all traffic in a contract, but set up taboos to deny certain traffic.
- Redirect—Useful to send traffic from an EPG to a layer 4-7 device such as a firewall, load balancer, or IPS/IDS.
- Mark—To mark traffic for Quality of Service reasons.

You can add filters to a contract by adding filter chains (consumer or provider) to contract subjects.

Contract Labels

Labels are optional advanced identifiers. When you use labels, you can specify more complex relationships between EPGs. Labels allow for control over which subjects and filters to apply when communicating between a specific pair of endpoint groups. Without labels, a contract applies every subject and filter between consumer and provider endpoint groups. You can use labels to represent a complex communication scenario, within the scope of a single contract, then reuse this contract while specifying only a subset of its policies across multiple endpoint groups.

Taboo Contracts

A Taboo contract provides a way for an EPG to specify the subjects on which communication is not allowed.

Creating Contracts

Without a contract, the default forwarding policy is to not allow any communication between EPGs but all communication within an EPG is allowed.

Note If two tenants are participating in same contract, ensure that they are not able to see each other and that their endpoint groups are not able to communicate.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Contracts**.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Contract** page, complete the following fields:

a) Add a unique name and description for the contract.

If you create contracts under the common and user tenants, that are consumed by the same tenant, they must have different names.

b) From the **Scope** drop-down list, choose from the following options:

- **Application Profile**—The contract is applied to endpoint groups in the application profile.
- **Context**—The contract is applied to endpoint groups in the same Virtual Routing and Forwarding (VRF).
- **Global**—This contract is applied to endpoint groups throughout the fabric.
- **Tenant**—This contract is applied to endpoint groups within the same tenant.

c) From the **Priority** drop-down list, choose the priority level of the service contract from the following options:

- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value

- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value
- **Unspecified**—This is the default value.

The default option is **Unspecified**.

Step 9 Click **Submit**.

What to do next

Create contract subjects to specify the information that can be communicated and the mechanism of communication.

Creating a Contract Subject

A subject is a sub-application running behind an endpoint group. A contract can encapsulate multiple subjects. An endpoint group always associates with a subject and defines rules under the association for consuming, providing, or for peer-to-peer communications to that subject.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Contracts**.

Step 7 Click the row with the contract that you want to update and click **View Details**.

Step 8 Click **Contract Subjects**.

Step 9 Click **Add**.

Step 10 On the **Add Tenant Contract Subject** page, complete the required fields, including the following:

a) Add a unique name and description for the contract subject.

b) Check **Reverse Filter Ports** to apply the same subject rule to the reverse filter ports when the contract applies in both directions. If you choose this option, enter the following additional parameters:

- **In Term Service Graph**
- **In Term QoS**
- **Out Term Service Graph**
- **Out Term QoS**

c) Check **Apply Both Directions** to apply the contract to both inbound and outbound traffic. If the selected contract does not apply to both, then the filter chain must be configured for consumer to provider and provider to consumer separately.

d) Click **Select** and check the box for the service graph that you want to add to the contract.

The service graph is an image that shows the relationship between contracts and subjects.

e) From the **QoS** drop-down list, choose the traffic priority for the associated EPG from the following options:

Each system class manages one lane of traffic.

- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value
- **Unspecified**—This is the default value.

The default option is **Unspecified**.

Step 11 Click **Submit**.

What to do next

Create consumer and provider contracts.

Adding Contracts to EPGs

Provided Contracts

EPGs can only communicate with other EPGs according to contract rules. Contracts determine the types of traffic that can pass between EPGs, including the protocols and ports allowed.

The relationship between an EPG and a contract can be either a provider or consumer. When an EPG provides a contract, communication with that EPG can be initiated from other EPGs as long as the communication complies with the provided contract. When an EPG consumes a contract, the endpoints in the consuming EPG may initiate communication with any endpoint in an EPG that is providing that contract.

An EPG can both provide and consume the same contract. An EPG can also provide and consume multiple contracts simultaneously.

Adding a Provided Contract to an EPG

You can associate contracts that were created earlier to create policy relationships between the EPGs. A provided contract is a contract for which the EPG is a provider.

Note Verify that both provided and consumed contracts have the same name.

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Consumed Contract**.
Step 11 Click **Add**.
Step 12 On the **Add Provided Contract To EPG** screen, complete the fields including the following:

a) Click **Select** and check the contract that you want to add to the EPG.
b) From the **QoS** drop-down list, choose the traffic priority for the associated EPG from the following options:

Each system class manages one lane of traffic.

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value

c) Click **Submit**.

Consumed Contracts

Also need to look into Taboo Contract and Filters.

Adding a Consumed Contract to an EPG

You can associate contracts that were created earlier to create policy relationships between the EPGs. A consumed contract is a contract for which the EPG is a consumer.

Note Verify that both provided and consumed contracts have the same name.

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Consumed Contract**.
Step 11 Click **Add**.
Step 12 On the **Add Consumed Contract To EPG** screen, complete the fields including the following:
a) Click **Select** and check the contract that you want to add to the EPG.
b) From the **QoS** drop-down list, choose the traffic priority for the associated EPG from the following options:

Each system class manages one lane of traffic.

- **Unspecified**—This is the default value.
- **Level1**—Class 1 Differentiated Services Code Point (DSCP) value
- **Level2**—Class 2 DSCP value
- **Level3**—Class 3 DSCP value

c) Click **Submit**.

Adding a Consumed Contract Interface

Before you begin

Contracts must be configured.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Application Profile**.
Step 7 Click the row with the profile that you want to update and click **View Details**.
Step 8 Click **EPG**.
Step 9 Click the row with the EPG that you want to update and click **View Details**.
Step 10 Click **Consumed Contract Interface**.
Step 11 Click **Add**.
Step 12 On the **Add Consumed Contract Interface To EPG** screen, complete the fields including the following:

a) Click **Select** and check the contract interface that you want to add to the EPG.
b) From the **Priority** drop-down list, choose a priority for the selected EPG from the following options:
   - **Level1**—Class 1 Differentiated Services Code Point (DSCP) value.
   - **Level2**—Class 2 DSCP value
   - **Level3**—Class 3 DSCP value
   - **Unspecified**—Is the default value
c) Click **Submit**.

Contract Labels

Adding a Consumed Label to a Contract Subject

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Contracts**.
Step 7 Click the row with the contract that you want to update and click **View Details**.
Step 8 Click **Contract Subjects**.
Step 9 Click the row with the contract subject that you want to update and click **View Details**.
Step 10 Click **Consumed Label**.
Step 11 Click **Add**.
Step 12 On the **Add Consumed Label to Contract To Contract Subject** screen, complete the following fields:
a) From the **Match Type** drop-down list, choose the subject match criteria across providers, from the following options:
   - **Atleast One**
   - **Atmost One**
   - **None**
   - **All**
b) Enter a **Label Name**.

   A subject label is used as classification criteria for subjects being consumed by the EPGs participating in the contract.
c) From the **Label Tag** drop-down list, choose a tag.

It is the search keyword or term that is assigned to the application profile. A tag allows you to group multiple objects by a descriptive name. You can assign the same tag name to multiple objects and you can assign one or more tag names to an object.

d) Check **Complement** for the contract to take effect if the labels do not match.
e) Click **Submit**.

Adding a Provided Label to a Contract Subject

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Contracts**.
Step 7 Click the row with the contract that you want to update and click **View Details**.
Step 8 Click **Contract Subjects**.
Step 9 Click the row with the contract subject that you want to update and click **View Details**.
Step 10 Click **Provided Label**.
Step 11 Click **Add**.
Step 12 On the **Add Provided Label to Contract To Contract Subject** screen, complete the following fields:

a) From the **Match Type** drop-down list, choose the subject match criteria across providers, from the following options:

- **Atleast One**
- **Atmost One**
- **None**
- **All**

b) Enter a **Label Name**.

A subject label is used as classification criteria for subjects being consumed or provided by the EPGs participating in the contract.

c) From the **Label Tag** drop-down list, choose a tag.

It is the search keyword or term that is assigned to the application profile. A tag allows you to group multiple objects by a descriptive name. You can assign the same tag name to multiple objects and you can assign one or more tag names to an object.

d) Check **Complement** for the contract to take effect if the labels do not match.
e) Click **Submit**.

Fabric Extender (FEX)

Fabric Extender (FEX) behave as a remote line card for a parent switch. The FEX is an extension of the parent swicth fabric, with the FEX and the parent switch together form a distributed modular system. This means that the FEXs are completely managed from the parent switch and appear as physical ports on that switch.

Adding a FEX Profile

A FEX profile enables you to define policy for the ports facing hosts on the FEX and configure FEX interfaces.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **FEX Profile**.
Step 5 Click **Add**.
Step 6 Enter the name and description of the profile used for configuring FEX.
Step 7 Click **Submit**.

What to do next

You have to add the interface port selector to the FEX profile to identify the interfaces between the node and the host.

Adding an Access Port Selector to the FEX Profile

Access port selector is used for identifying the interfaces between the node and the host (such as hypervisor), which consume the policies in the interface policy group.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **FEX Profile**.
Step 5 Click the row with the FEX profile to which you want to add an access port selector and click **View Details**.
Step 6 In the **FEX Profile Access Port Selectors** tab, click **Add**.
Step 7 On the **Create Fex Profile Access Port Selector** screen, complete the following fields:

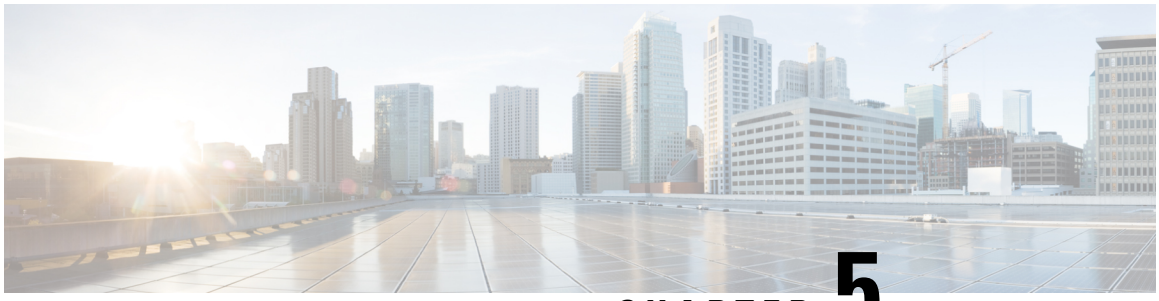
- Enter the name and description of the interface selector. We recommend that you include information about where and when the policy must be used, in the description field.
- Enter the ID of the interfaces that consume the policies in the interface policy group. You can enter a single FEX interface, one or more interface ranges, or All.

- Click **Select** to view the list of available interface policy group. Check the interface policy group that you want the interfaces to consume and click **Select**.

Step 8 Click **Submit**.

What to do next

You can add access port blocks and sub-port blocks to the access port selector of the FEX profile. Choose an access port selector and click **View Details** to view the access port blocks and sub port blocks of the access port selector. Click **Add** under respective tabs to add the access port block and sub port block.



CHAPTER 5

Configuring Multi-Site Controller Accounts

Adding an ACI Multi-Site Controller Account

As an administrator, you can add an ACI Multi-Site controller account.

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, choose **ACI Multi-Site** from the **Account Type** drop-down list and click **Submit**.

Step 5 On the **Add Account** screen, complete the fields, including the following:

a) Enter a unique account name and description for the ACI Multi-Site controller account.

b) From the **Pod** drop-down list, choose the pod where you want to add the ACI Multi-Site controller account.

c) In the **Server IP** field, enter the IP address of the ACI Multi-Site controller account.

d) Check the **Use Credential Policy** box if you want to use a credential policy for this account rather than enter the user name and password information manually.

e) If you checked the **Use Credential Policy** box, choose a policy from the **Credential Policy** drop-down list.

You can also add a new credential policy by clicking the **Add** option.

f) If you did not check **Use Credential Policy**, enter the user name and password that this account uses to access ACI Multi-Site controller.

g) If you did not check **Use Credential Policy**, do the following:

- From the **Protocol** drop-down list, choose **https** or **http**.

- In the **Port** field, enter the port used to access the ACI Multi-Site controller account. The default port is 443.

h) Enter the contact details and location of the administrator or other person responsible for this account.

Step 6 Click **Submit**.

What to do next

Cisco UCS Director tests the connection to the ACI Multi-Site controller. If that test is successful, it adds the ACI Multi-Site controller account and discovers all the elements in the ACI Multi-Site controller. This discovery process and inventory collection takes a few minutes to complete.

When you add the ACI Multi-Site controller account, system tasks related to the ACI Multi-Site account are populated on the **System Task** page (**Administration > System > System Task**).

Assigning an ACI Multi-Site Controller Account to Multiple Pods

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the ACI Multi-Site controller account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site controller account that you want to assign to one or more pods.

Step 4 Click **Assign to Pod**.
The **Assign to Pod** screen appears.

Step 5 Click **Select**.

The list of pods available in Cisco UCS Director is displayed.

Step 6 Check the pods to which you want to assign the ACI Multi-Site controller account to and click **Select**.

Step 7 Click **Submit**.

What to do next

If you want to unassign an account from the pod, choose the account and click **UnAssign from Pod**. In the **Unassign from Pod** screen, click **Select** and choose the pod from which you want to unassign the ACI Multi-Site controller account from. Click **Select** and then click **Submit**.

Managing Users

The Cisco ACI Multi-Site provides access according to a user's role through role-based access control (RBAC).

The following user roles are available in Cisco ACI Multi-Site.

- Power User—A power user can perform all the operations as an admin user.
- Site and Tenant Manager—A site and tenant manager can manage sites, tenants, and associations.

- Schema Manager—A schema manager can manage all schemas regardless of tenant associations.
- Schema Manager - Restricted —A restricted schema manager can manage schemas that contain at least one tenant to which the user is explicitly associated.
- User and Role Manager—A user and role manager can manage all the users, their roles, and passwords.

Creating a User

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **User**.

Step 5 Click **Create User**.

Step 6 On the **Create User** screen, complete the fields, including the following:

- Enter a unique name for the user.
- Enter the password in the **Password** field and **Confirm Password** field.

  The password must at least be six characters in length, and must contain at least one letter, one number, and a special character. Spaces and * are not allowed.
- Enter the first name and last name of the user in the respective fields.
- Enter e-mail address and phone number of the user.
- From the **Account Status** drop-down list, choose **Active** or **Inactive** as the user account status. Only the Active users are authenticated to access ACI Multi-Site.
- Click **Select** and choose the roles to be assigned to the user.

  You must associate at least one role with every user. A user may be associated with more than one role. Associating a user to multiple roles offers a combination of features that the user may access.

Managing Sites

Adding a Site to an ACI Multi-Site Controller Account

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with ACI Multi-Site Controller account to which you want to add a site, and click **View Details**.

Step 4 Click **Site**.

Step 5 Click **Add**.

Step 6 On the **Add Site to ACI Multi-Site** screen, complete the fields, including the following:

a) Add a unique name for the site.

b) Click **Select** and check the site labels that you want to use for the site.

You can choose a maximum of three site labels for the site.

c) Enter the URL of the APIC controller that has to be added as the site object. If you want to add multiple APIC controllers, enter comma separated APIC controller URLs.

Note While adding multiple APIC controllers, ensure that the credentials used for accessing the APIC controllers is same for all the APIC controllers.

d) Enter the user name and password that is used to access the APIC controller.

e) Enter a unique site ID.

Note Once saved, you cannot edit the site ID.

Step 7 Click **Submit**.

Associating a Template to the Site

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site Controller account and click **View Details**.

Step 4 Click **Site**.

Step 5 Click the row with the site to which you want to associate the template and click **Associate Template**.

Step 6 On the **Associate Template to MSC Site** screen, click **Select** and check the template that you want to associate with the site.

Step 7 Click **Submit**.

Managing Tenants

Creating a Tenant

Before you begin

- The site to which the tenant has to be associated must be added.
- The tenant user account must be created.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account to which you want to add a tenant and click **View Details**.

Step 4 Click **Tenant**.

Step 5 Click **Create Tenant**.

Step 6 On the **Create Tenant** screen, complete the fields, including the following:

- Enter a unique account name and description for the tenant.
- Click **Select** and choose one or more sites to which you want to associate the tenant.
- Click **Select** and choose the security domains.
- Click **Select** and choose one or more users who can access the tenant.

  By default, the Admin user is selected.

Step 7 Click **Submit**.

Managing Schemas

Adding a Schema

Schema includes the site-configuration objects that will be pushed to sites. Schemas are the containers for single or multiple templates that are used for defining the policies. Templates are the framework for defining and deploying the policies to the sites.

Before you begin

A tenant must be available in Cisco UCS Director.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account to which you want to add a schema and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click **Add**.

Step 6 On the **Add Schema to ACI Multi-Site** screen, complete the fields, including the following:

- Enter a unique name for the schema.
- Enter a unique name for the template.
- Click **Select** and check the tenant that you want to use.

Step 7 Click **Submit**.

What to do next

You can see the schema in the ACI Multi-Site.

Adding a Template to a Schema

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account to which you want to add a schema template and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add a template and click **View Details**.
Step 6 Click **Template**.
Step 7 Click **Add**.
Step 8 On the **Add Template to ACI Multi-Site Schema** screen, complete the fields, including the following:

- Click **Select** and check the tenant that you want to use.
- Enter a display name for the template.

Step 9 Click **Submit**.

What to do next

You can see the template in the ACI Multi-Site.

Deploying a Schema Template to the Site

Before you begin

- The schema template must be assigned to a tenant and the template must be associated to the site. See Associating a Template to the Site, on page 44.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema and click **View Details**.
Step 6 Click the row with the template that you want to deploy to the site and click **Deploy Template**.
Step 7 Click **Submit** to confirm the deployment of template to the site.

You can view the status of the template deployment status under the **Deployed Status** tab (**ACLI Multi-site Account** > **Schema** > **Sites**).

To undeploy a template from the site, navigate to the **Sites** tab (**ACLI Multi-site Account** > **Schema**), choose the row with the site from which you want to undeploy the template from, and then choose **Undeploy Template**.

Adding an ACI Multi-Site Service Graph

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account to which you want to add a service graph and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add a service graph and click **View Details**.

Step 6 Click **Template**.

Step 7 Click the row with the template to which you want to add a service graph and click **View Details**.

Step 8 Click **Service Graph**.

Step 9 Click **Add**.

Step 10 On the **Create ACI Multi-Site Service Graph** screen, complete the following fields:

a) Enter a unique name and description for the service graph.

b) Choose **1**, **2**, or **3** as the number of service nodes for the service graph.

Complete the following fields to add the configurations to the service graph. You have to specify the following details for the number of nodes chosen.

1. Click **Select** and choose a service node that you want to use for the service graph.
2. Click **Select** and choose sites and L4-L7 devices for node that you want to use for the service graph. Ensure that you choose one L4-L7 device per site.

Step 11 Click **Submit**.

Adding a Service Graph to a Contract

Terminal nodes connect a service graph with the contracts.You can insert a service graph for the traffic between two application endpoint groups (EPGs) by connecting the terminal node to a contract. Once connected, traffic between the consumer EPG and provider EPG of the contract is redirected to the service graph.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add the service graph contract and click **View Details**.

Step 6 Click **Template**.

Step 7 Click the row with the template to which you want to add the service graph contract and click **View Details**.

Step 8 Click **Contract**.

Step 9 Click the row with the contract to which you want to add the service graph contract and click **View Details**.

Step 10 Click **Service Graph**.

Step 11 Click **Add**.

Step 12 On the **Add Service Graph to Contract** screen, complete the following fields:

a) Click **Select** and choose a service graph that you want to add to the contract.

b) Complete the following fields to add the node configuration for template. You have to specify the following details for number of nodes in chosen service. For example, if you have chosen service graph with two nodes, you have to specify the following details for two nodes.

1. Click **Select** and choose a bridge domain for consumer connector.
2. The **Route Peering** check box appears for consumer connector of node 2 and node 3 when you choose service graph with two and three nodes. Check this check box to enable route peering on a service appliance such as a load balancer or a firewall to advertise it's reachability through the ACI fabric.
3. The **Route Peering** check box appears for provider connector of node 1 and node 2 when you choose service graph with two and three nodes. Check this check box to enable route peering on a service appliance such as a load balancer or a firewall to advertise it's reachability through the ACI fabric.
4. Click **Select** and choose a bridge domain for provider connector.

c) Complete the following fields to add the node configuration for site. You have to specify the following details for number of nodes in chosen service. If you have chosen two nodes service graph, you have to specify the following details for two nodes.

1. Click **Select** and choose a cluster interface for consumer connector.
2. Click **Select** and choose a redirect policy for consumer connector.
3. Click **Select** and choose a cluster interface for provider connector.
4. (Optional) Click **Select** and choose a redirect policy for provider connector.

Step 13 Click **Submit**.

Adding an Application Profile to a Schema Template

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema and click **View Details**.

Step 6 Click **Template**.

Step 7 Click the row with the schema template to which you want to add an application profile and click **View Details**.

Step 8 Click **Application Profile**.

Step 9 Click **Add**.

Step 10 Enter a display name for the application profile in the **Display Name** field.

Step 11 Click **Submit**.

What to do next

You can see the application profile in the ACI Multi-Site.

Adding a VRF to a Schema Template

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema and click **View Details**.
Step 6 Click **Template**.
Step 7 Click the row with the schema template to which you want to add a VRF and click **View Details**.
Step 8 Click **VRFs**.
Step 9 Click **Add**.
Step 10 Enter a display name for the VRF in the **Display Name** field.
Step 11 Click **Submit**.

What to do next

You can see the VRF in the ACI Multi-Site.

Adding a Contract to the Template

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add a contract and click **View Details**.
Step 6 Click **Template**.
Step 7 Click the row with the template to which you want to add a contract and click **View Details**.
Step 8 Click **Contract**.
Step 9 Click **Add**.
Step 10 On the **Add Contract to ACI Multi-Site Schema** screen, complete the fields, including the following:

- Enter a unique display name for the contract.
- From the **Scope** drop-down list, choose application profile, VRF, tenant or global as the scope of the contract.

Step 11 Click **Submit**.

Adding a Contract to the EPG

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add a contract and click **View Details**.
Step 6 Click the row with the template to which you want to add a contract and click **View Details**.
Step 7 Click **Application Profile**.
Step 8 Click the row with the application profile to which you want to add a contract and click **View Details**.

The EPGs available in the application profile is displayed.

Step 9 Click the row with the EPG to which you want to add a contract.
Step 10 Click **Add Contract to EPG**.
Step 11 In the **Add Contract to ACI Multi-Site EPG** screen, complete the fields, including the following:

- Click **Select** and choose the contract that you want to add to the EPG.
- From the **Type** drop-down list, choose **Consumer** or **Provider**.

Step 12 Click **Submit**.

Adding a Domain to the EPG

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add a domain and click **View Details**.
Step 6 Click the row with the template to which you want to add a domain and click **View Details**.
Step 7 Click **Application Profile**.
Step 8 Click the row with the application profile to which you want to add a domain and click **View Details**.

The EPGs available in the application profile is displayed.

Step 9 Click the row with the EPG to which you want to add a domain.
Step 10 From the **More Actions** drop-down list, choose **Add Domain to EPG**.
Step 11 On the **Add Domain to EPG** screen, complete the fields, including the following:

- Click **Select** to choose the site.
- From the **Domain Association Type** drop-down list, choose the type in which you want to associate the domain.
- Click **Select** to choose the domain profile.
- From the **Deployment Immediacy** drop-down list, choose one of the following options:
  - **Immediate**—Specifies that the policy is programmed in the hardware policy CAM as soon as it is downloaded in the leaf software.
  - **On Demand**—Specifies that the policy is programmed in the hardware policy CAM only when the first packet is received through the data path. This process helps to optimize the hardware space.
- From the **Resolution Immediacy** drop-down list, one of the following options:
  - **Immediate**—Specifies that EPG policies (including contracts and filters) are downloaded to the associated leaf switch software upon hypervisor attachment to VDS. LLDP or OpFlex permissions are used to resolve the hypervisor to leaf node attachments.
  - **On Demand**—Specifies that a policy (for example, VLAN, VXLAN bindings, contracts, or filters) is pushed to the leaf node only when a hypervisor is attached to VDS and a VM is placed in the port group (EPG).
  - **Pre-provision**—Specifies that a policy (for example, VLAN, VXLAN binding, contracts, or filters) is downloaded to a leaf switch even before a hypervisor is attached to the VDS. Therefore, this option pre-provisions the configuration on the switch.
- **Vlan Mode** drop-down list—This field appears only when VMM is chosen in the **Domain Association Type** drop-down list. Choose **Dynamic** to assign VLAN identifiers to EPG dynamically by the APIC or **Static** to assign VLAN identifiers to EPG manually by an administrator.
- **Allow Micro-segmentation** check box—This field appears only when VMM is chosen in the **Domain Association Type** drop-down list. Check this box to use Cisco APIC configure Micro-segmentation with Cisco ACI to put VMs that belong to different base EPGs or the same EPG into a new attribute-based EPG.

Step 12 Click **Submit**.
The domain is associated with the EPG. You can see the domains that are associated with the EPG under the **EPG Domain Association** tab (**ACI Multisite Account** > **Schema** > **Sites** > **Application Profile**).

Adding a Static Port to the EPG

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add a static port and click **View Details**.
Step 6 Click the row with the template to which you want to add a static port and click **View Details**.
Step 7 Click **Application Profile**.
Step 8 Click the row with the application profile to which you want to add a static port and click **View Details**.

The EPGs available in the application profile is displayed.

Step 9 Click the row with the EPG to which you want to add a static port.

Step 10 From the **More Actions** drop-down list, choose **Add Static Port to EPG**.

Step 11 On the **Create STATIC PORT** screen, complete the fields, including the following:

- Click **Select** to choose the site.
- From the **Path Type** drop-down list, choose port, virtual port channel or direct port channel as the static port path.
- The Leaf field appears only when you choose port as the path type. Click **Select** and choose the leaf for the static port.
- Click **Select** and choose the static port path.
- In the **Port Encap VLAN** field, enter the port encapsulation VLAN ID.
- In the **Primary Micro Seg VLAN** field, enter the primary micro segment VLAN ID.
- From the **Deployment Immediacy** drop-down list, choose on-demand or immediate as the deployment type.
- From the **Mode** drop-down list, choose the mode in which the static port has to be created.

Step 12 Click **Submit**.
You can view the static port added to EPG under the **EPG** tab (**ACI Multisite Account** > **Schema** > **Sites** > **Application Profile**). You also have options to update and delete the static port under the **EPG** tab (**ACI Multisite Account** > **Schema** > **Sites** > **Application Profile**).

Adding a Static Leaf to the EPG

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with ACI Multi-Site Controller account to which you want to add a static leaf and click **View Details**.

Step 4 Click the row with the schema to which you want to add a static leaf and click **View Details**.

Step 5 Click the row with the template to which you want to add a static leaf and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the application profile to which you want to add a static leaf and click **View Details**.

Step 8 Click **EPG**.

Step 9 Click the row with the EPG to which you want to add a static leaf.

Step 10 From the **More Action** drop-down list, choose **Add Static Leaf to EPG**

Step 11 On the **Add Static Leaf to EPG in Multi-Site Schema** screen, complete the following fields.

- Click **Select** and choose a site.
- Click **Select** to view the list of available leaves. Choose a leaf that you want to add to the EPG in the ACI Multi-site schema and click **Select**.
- Enter the ID of VLAN on leaf.

Step 12 Click **Submit**.

Creating an ACI Multi-Site Bridge Domain

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with ACI Multi-Site Controller account to which you want to add a bridge domain and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add a bridge domain and click **View Details**.
Step 6 Click the row with the template to which you want to add a bridge domain and click **View Details**.
Step 7 Click **Bridge Domain**.
Step 8 Click **Add**.
Step 9 On the **Create ACI Multi-Site Bridge Domain** screen, complete the fields, including the following:

- Enter a unique name for the bridge domain.
- Click **Select** and check the virtual routing and forwarding that you want to use for the bridge domain.
- Check the **L2 Stretch** check box to apply stretched layer-2 or VLAN extension on the bridge domain.
- Check the **Inter Site Bum Traffic Allow** check box to allow inter site bum traffic. This field appears only when the **L2 Stretch** check box is checked.
- Check the **Optimize WAN Bandwidth** check box to optimize the WAN bandwidth in bridge domain. This field appears only when the **Inter Site Bum Traffic Allow** check box is checked.
- From the **L2 Unknown Unicast** drop-down list, choose proxy or flood.

Step 10 Click **Submit**.

Adding a Layer 3 Out to the Site Bridge Domain

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with ACI Multi-Site Controller account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema and click **View Details**.
Step 6 Click **Template**.
Step 7 Click the row with the template and click **View Details**.
Step 8 Click **Bridge Domain**.
Step 9 Click the row with the bridge domain to which you want to add a layer 3 Out.
Step 10 On the **Add L3 OUT to Site Bridge Domain** screen, complete the fields, including the following:

- Click **Select** and check the site that you want to use.
- Click **Select** and check the check box of the layer 3 Out that you want to add to the site bridge domain.

Step 11 Click **Submit**.

Adding a Subnet to an ACI Multi-Site Bridge Domain

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with ACI Multi-Site Controller account to which you want to add a bridge domain subnet and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add a bridge domain subnet and click **View Details**.

Step 6 Click the row with the template to which you want to add a bridge domain subnet and click **View Details**.

Step 7 Click **Bridge Domain**.

Step 8 Click the row with the bridge domain to which you want to add a subnet and click **View Details**.

Step 9 Click **Subnets**.

Step 10 Click **Add Subnet to Site Bridge Domain**.

Step 11 On the **Add Subnet to ACI Multi-Site Bridge Domain** screen, complete the fields, including the following:

- Click **Select** to view the list of available sites. Choose the site to which you want to add the bridge domain subnet and click **Select**.
- Enter the gateway IP address and a description for the subnet you intend to add.
- In the **Scope** field, select either **Private to VRF** or **Advertised Externally**.
- Click the check box for **Shared Between VRFs** if appropriate.
- Click the check box for **No Default SVI Gateway** if appropriate. If checked, the pervasive SVI will not be configured for this subnet and it is used to leak more specific prefix routes to other VRFs.

Step 12 Click **Submit**.

Adding an EPG to the Template

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add a contract and click **View Details**.

Step 6 Click **Application Profile**.

Step 7 Click the row with the application profile to which you want to add a contract and click **View Details**.

The EPGs available in the application profile is displayed.

Step 8 Click **Add**.

Step 9 On the **Create ACI Multi-Site EPG** screen, complete the fields, including the following:

- Enter a unique name for the EPG.
- Check the **USEG EPG** check box to consider the EPG as uSeg EPG. If unchecked, the EPG is considered as base EPG.
- From the **Intra EPG Isolation** drop-down list, choose unenforced or enforced.

  If an EPG is configured with intra-EPG endpoint isolation enforced, the folowing restrictions apply:

  - In ACI Multi-Site, intra-EPG isolation is not supported in AVS-VLAN mode.Setting Intra-EPG isolation to be enforced may cause the ports to go into a blocked state in these domains.
  - Intra-EPG isolation is not supported if the Bridge Domain is configured as "legacy BD mode".
  - Preserving QoS CoS priority settings is not supported when traffic is flowing from an EPG with isolation-enforced to an EPG without isolation enforced.

- **Forwarding Control Proxy-ARP** check box—This field appears only when enforced is is chosen in the **Intra EPG Isolation** field. Check the box to enable proxy ARP. The proxy ARP in Cisco ACI enables endpoints within a network or subnet to communicate with other endpoints without knowing the real MAC address of the endpoints.
- Click **Select** and choose a bridge domain from the list.

Step 10 Click **Submit**.

Adding a Filter to the Template

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add a filter and click **View Details**.

Step 6 Click **Template**.

Step 7 Click the row with the template to which you want to add a filter and click **View Details**.

Step 8 Click **Filters**.

Step 9 Click **Add**.

Step 10 On the **Create ACI Multi-Site Filter** screen, enter the display name of the filter.

Step 11 Click **Submit**.

Adding an Entry to an ACI Multi-Site Filter

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add a filter entry and click **View Details**.

Step 6 Click **Template**.

Step 7 Click the row with the template to which you want to add a filter entry and click **View Details**.

Step 8 Click **Filters**.

Step 9 Click the row with the filter to which you want to add a filter entry and click **View Details**.

Step 10 Click **Add**.

Step 11 On the **Add Entry to Filter** screen, complete the fields, including the following:

- Enter a unique name and description for the filter entry.
- Choose the type, ARP flag and IP protocol from the respective drop-down lists.
- Check the **Match Only Fragments** check box to match only fragments during filtering.
- Check the **Stateful** check box to enable stateful connection.
- Enter the starting and ending range of the source port number in the **Source Port range From** field and **Source Port Range To** field.
- Enter the starting and ending range of the destination port number in the **Destination Port range From** field and **Destination Port Range To** field.
- Choose one of the following as the TCP session rules:
  - Acknowledgment
  - Established
  - Finish
  - Synchronize
  - Reset
  - Unspecified

Step 12 Click **Submit**.

Adding an uSeg Attribute to the EPG

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add an uSeg attribute and click **View Details**.

Step 6 Click the row with the template to which you want to add an uSeg attribute and click **View Details**.

Step 7 Click **Application Profile**.

Step 8 Click the row with the application profile to which you want to add an uSeg attribute and click **View Details**.

The EPGs available in the application profile is displayed.

Step 9 Click the row with the EPG to which you want to add an uSeg attribute and click **View Details**.

Note You can add the uSeg attribute to the EPG for which the USEG EPG is enabled.

Step 10 Click **USEG Attributes**.

Step 11 Click **Add**.

Step 12 On the Add uSeg Attribute to EPG in ACI Multi-Site Schema screen, complete the fields, including the following:

- Enter a unique name and description for the uSeg attribute.
- From the **Attribute Type** drop-down list, choose an attribute type. According to the selected attribute type, additional fields will be displayed. Enter the attribute values.

Step 13 Click **Submit**.

Adding a Subnet to the EPG

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **Schema**.

Step 5 Click the row with the schema to which you want to add a subnet and click **View Details**.

Step 6 Click the row with the template to which you want to add a subnet and click **View Details**.

Step 7 Click **Application Profile**.

Step 8 Click the row with the application profile to which you want to add a subnet and click **View Details**.

Step 9 Click the row with the EPG to which you want to add a subnet and click **View Details**.

Step 10 Click **Subnets**.

Step 11 Click Add.

Step 12 On the **Add Subnet to ACI Multi-Site EPG** screen, complete the fields, including the following:

- Enter the gateway IP address and short description for the subent.

  Note The gateway IP address must be enetered in the format: <Valid IP address>/<Valid Prefix Length>

- From the **Scope** drop-down list, choose **Private to VRF** or **Advertised Externally**.
- Check the **Shared Between VRFs** and **No Default SVI Gateway** check boxes as requied.

Step 13 Click **Submit**.

Adding a Subnet to the Site EPG

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add a subnet and click **View Details**.
Step 6 Click the row with the template to which you want to add a subnet and click **View Details**.
Step 7 Click **Application Profile**.
Step 8 Click the row with the application profile to which you want to add a subnet and click **View Details**.
Step 9 Click the row with the EPG to which you want to add a subnet and click **View Details**.
Step 10 Click **Subnets**.
Step 11 Click **Add Subnet to Site EPG**.
Step 12 On the **Add Subnet to Site EPG** screen, complete the fields, including the following:

- Click **Select** to view a list of available sites. Check the check box of the site to which you want to add the subnet and click **Select**.
- Enter the gateway IP address and short description for the subent.

  Note The gateway IP address must be enetered in the format: <Valid IP address>/<Valid Prefix Length>

- From the **Scope** drop-down list, choose **Private to VRF** or **Advertised Externally**.
- Check the **Shared Between VRFs** and **No Default SVI Gateway** check boxes as requied.

Step 13 Click **Submit**.

Adding an External EPG to the Template

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add an external EPG and click **View Details**.
Step 6 Click **Template**.
Step 7 Click the row with the template to which you want to add an external EPG and click **View Details**.
Step 8 Click **External EPG**.
Step 9 Click **Add**.

Step 10 On the **Create External EPG** screen, complete the following fields:

Note When the template is assigned to the site and the user tries to add an External EPG, the L3 outside must be assigned to the External EPG for the site. If the template is not assigned to site, then specify only the EPG display name and the L3 outside, site, and VRF details are not needed.

a) Enter a unique name for the external EPG.
b) From the **Associated Sites** drop-down list, choose **Single** to associate only one site to EPG or **Multiple** to associate more than one sites to EPG.

When **Single** is chosen, the following fields appear:

1. Click **Select** and check the check box of site that you want to use for the external EPG.
2. Click **Select** and check the check box of Virtual Routing and Forwarding (VRF) that you want to use for the external EPG.
3. Click **Select** and check the check box of the L3Outs on the site to be used for the external EPG.

When **Multiple** is chosen, the following field appears:

1. Click **Select** and check the check box of L3Outs on the sites to be used for the external EPG. Ensure that you choose only one L3Out per site and VRF associated to the L3Outs must be same.

Step 11 Click **Submit**.

Adding a Contract to the External EPG

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add the external EPG contract and click **View Details**.
Step 6 Click **Template**.
Step 7 Click the row with the template to which you want to add the external EPG contract and click **View Details**.
Step 8 Click **External EPG**.
Step 9 Click the row with the external EPG to which you want to add a contract and click **View Details**.
Step 10 Click **Contracts**.
Step 11 Click **Add**.
Step 12 On the **Add Contract to ACI Multi-Site External EPG** screen, complete the fields, including the following:

- Click **Select** and choose the contract that you want to add to the external EPG.
- From the **Type** drop-down list, choose consumer or provider as the contract type.

Step 13 Click **Submit**.

Adding a Subnet to the External EPG

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the ACI Multi-Site account and click **View Details**.
Step 4 Click **Schema**.
Step 5 Click the row with the schema to which you want to add the external EPG contract and click **View Details**.
Step 6 Click **Template**.
Step 7 Click the row with the template to which you want to add the external EPG contract and click **View Details**.
Step 8 Click **External EPG**.
Step 9 Click the row with the external EPG to which you want to add a contract and click **View Details**.
Step 10 Click **Subnet**.
Step 11 Click **Add**.
Step 12 On the **Add Subnet to ACI Multi-Site External EPG** screen, enter a unique name for the subnet.
Step 13 Click **Submit**.

Deploying a Template to the Site

This section captures the list of actions that have to be executed to deploy a template to site.

Step 1 Add a site to an ACI Multi-Site controller account.

See Adding a Site to an ACI Multi-Site Controller Account, on page 43.

Step 2 Create a tenant and assign it to the site.

See Creating a Tenant, on page 44.

Step 3 Create a schema and map it to the tenant.

See Adding a Schema, on page 45.

Step 4 Optional. Add a template to the schema.

See Adding a Template to a Schema, on page 46.

Step 5 Add an application profile to the template.

See Adding an Application Profile to a Schema Template, on page 48.

Step 6 Add a VRF to the template.

See Adding a VRF to a Schema Template, on page 49.

Step 7 Add a bridge domain to the template.

See Creating an ACI Multi-Site Bridge Domain, on page 53.

Step 8 Add a subnet to the bridge domain.

See Adding a Subnet to an ACI Multi-Site Bridge Domain, on page 54.

Step 9 Add an EPG to the template.

See Adding an EPG to the Template, on page 54.

Step 10 Add a filter to the template.

See Adding a Filter to the Template, on page 55.

Step 11 Add an entry to filter.

See Adding an Entry to an ACI Multi-Site Filter, on page 56.

Step 12 Add a contract to the template.

See Adding a Contract to the Template, on page 49.

Step 13 Add a contract to the EPG.

See Adding a Contract to the EPG, on page 50.

Step 14 Associate a template to the site.

See Associating a Template to the Site, on page 44.

Step 15 Add a domain to the EPG.

See Adding a Domain to the EPG, on page 50.

Step 16 Add a static port to the EPG.

See Adding a Static Port to the EPG, on page 51.

Step 17 Add an uSeg attribute to the EPG.

See Adding an uSeg Attribute to the EPG, on page 56.

Step 18 Add the external EPG to the template.

See Adding an External EPG to the Template, on page 58.

Step 19 Add a contract to the external EPG.

See Adding a Contract to the External EPG, on page 59.

Step 20 Add a subnet to the external EPG.

See Adding a Subnet to the External EPG, on page 60.

Step 21 Deploy a template to the site.

See Deploying a Schema Template to the Site, on page 46.

Viewing ACI Multi-Site Controller Resources

After creating an ACI Multi-Site controller account in Cisco UCS Director, you can view related resources of the ACI Multi-Site controller account.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click one of the following tabs to view the details of a specific component in the ACI Multi-Site controller:

- **Summary** tab—Displays the system overview and control plane BGP of the ACI Multi-Site controller.
- **Site** tab—Displays a list of sites that are configured in the ACI Multi-Site controller. To associate a template to a site, select the site and then click **Associate Template**. In the **Associate Template to MSC Site** screen, click **Select** and check the template that you want to associate with the site. To disassociate a template from the site, select the site and then click **Disassociate Template**. In the **Disassociate Template from MSC Site** screen, click **Select** and check the template that you want to disassociate from the site.
- **Tenant** tab—Displays a list of tenants that are available in the ACI Multi-Site controller. To create a tenant in a site, click **Create Tenant (+)**. On the **Create Tenant** screen, do the following:
  - Enter a unique account name and description for the tenant.
  - Click **Select** and choose associated sites, security domains, and associated users for the tenant.
  - Click **Submit**.
- **User** tab—Displays a list of ACI Multi-Site account users. To create a user for a site, click **Create User**. For more details, see Creating a User, on page 43.
- **Schema** tab—Displays a list of schemas that are defined for the ACI Multi-Site controller. To add a schema to an ACI Multi-site, click **Add (+)**. On the **Add Schema to ACI Multi-Site** screen, enter the schema and template name, and then select a tenant.

  To view more details about schema, choose a schema and click **View Details**. The following tabs appear:

  - **Template**—Displays the templates associated with the schema. To add a template, click **Add**. To deploy a template to a site, click **Deploy Template**. To import APIC policy to ACI Multi-site schema, click **Import**. On the **Import APIC Policy to ACI Multi-site Schema** screen, click **Select** and choose the site ID, application profile name, EPG name, contract name, filter name, VRF name, and bridge domain name.

    To view more details about template, choose a template and click **View Details**. The following tabs appear:

    - **Contract**—Displays the contracts that are added to an ACI Multi-site schema. To add a contract, click **Add (+)**, enter the contract display name, and choose **application profile**, **vrf**, **tenant** or **global** as the scope of the contract. To view and add filters to contract in the schema, choose the row with the contract and click **View Details**. Click **Add**. On the **Add Filter to Contract in ACI Multi-Site Schema** screen, click **Select** and choose the filter that you want to add to the contract and choose **none** or **log** as **Directive**.
    - **Application Profile**—Displays the application profiles of the ACI Multi-site. To add an application profile, click **Add** and enter the display name of the application profile. To view the EPGs of the site, choose the row with an application profile and click **View Details**. Choose an EPG and click **View Details** to view the EPG contract association, USEG attributes, and Subnets.

In the EPG tab, you can perform the following tasks:

- To add a contract to the EPG, choose **Add Contract to EPG** from the **More Actions** drop-down list. For more details, see Adding a Contract to the EPG, on page 50.
- To add a domain to the EPG, choose **Add Domain to EPG** from the **More Actions** drop-down list. For more details, see Adding a Domain to the EPG, on page 50.
- To add a static port to the EPG, choose **Add Static Port to EPG** from the **More Actions** drop-down list. For more details, see Adding a Static Port to the EPG, on page 51.
- To add a static port to the EPG, choose **Add Static Leaf to EPG** from the **More Actions** drop-down list. For more details, see Adding a Static Leaf to the EPG, on page 52.

- **VRFs**—Displays the Virtual Routing and Forwarding (VRF) instances of the site. To add a VRF, click **Add** and enter the display name of the VRF.
- **Bridge Domain**—Displays the bridge domains of the site. To add a bridge domain, click **Add**. For more details, see Creating an ACI Multi-Site Bridge Domain, on page 53. To add a layer 3 Out to the site bridge domain, choose a row with the bridge domain and click **Add L3 OUT to Site Bridge Domain**. For more details, see Adding a Layer 3 Out to the Site Bridge Domain, on page 53. To view the subnets of the bridge domain, choose a row with the bridge domain and click **View Details**. For more details, see Adding a Subnet to an ACI Multi-Site Bridge Domain, on page 54.
- **Filters**—Displays the filters of the site. To add a filter, click **Add** and enter the display name of the filter. To view the filter entries, choose a row with the filter and click **View Details**. Click **Add** to add filter entries. For more details, see Adding an Entry to an ACI Multi-Site Filter, on page 56.
- **External EPG**—Displays the external EPGs of the site. To add an external EPG, click **Add** and enter the external EPG Name. Choose a row with the external EPG and click **View Details** to view the contracts and subnets of the external EPG. You can also add contract and subnet to the external EPG, under the respective tab.

- **Sites**—Displays the sites that are associated with the schema template. To undeploy a template from the site, choose the row with the site from which you want to undeploy the template from and then choose **Undeploy Template**. The template will be undeployed from the site after confirmation.

  To view more details about sites, choose a site and click **View Details**. The following tabs appear:

  - **Application Profile**—Displays the application profiles of the site. Choose a row with an application profile and click **View Details**, to view the EPG associated with the application profile.

    To view more details about EPGs, choose an EPG and click **View Details**. The following tabs appear:

    - **EPG Domain Association**—You can view and update the domains that are associated with the EPG under the **EPG** tab (**Schema > Template > Application Profile**).
    - **Static Port**—You can view and update the static ports of the EPG.
    - **Subnets**—You can view and update the subnets of the EPG. To add a subnet to the site EPG, click **Add**. In the **Add Subnet to Site EPG** screen, enter the gateway IP address and short description for the subent. From the **Scope** drop-down list, choose **Private to VRF** or **Advertised Externally**. Check the **Shared Between VRFs** and **No Default SVI Gateway** check boxes as requied.
    - **Static Leaf**—You can view static leaves of the EPG.

- **Bridge Domain**—You can view the bridge domains of the site. Choose a row with a bridge domain and click **View Details**, to view the subnets of the bridge domain.
- **Deployed Status**—You can view the status of the template deployment of the site.
- **External EPG**—You can view and update the external EPG of the site.

- **OSPF Policies** tab—Displays the OSPF policies of the site. To add a OSPF policy, click **Add**. For more details, see Creating an OSPF Policy, on page 64. To configure control plane BGP, click **Configure Control Plane BGP**. For more details, see Configuring Control Plane BGP, on page 65.
- **Site Settings** tab—Displays the settings of all sites in the ACI Multi-Site account. To view more details about site setings, choose a site setting and click **View Details**. The pods associated with the site is displayed. Choose a pod and click **View Details** to view the spines. Choose a spine and click **View Details** to view the ports of the spine. To add a port to the spine, click **Add**. On the **Add Port to Spine** screen, do the following:
  - In the **Port ID** field, enter the port ID in the slot number/port number format For example, 1/10.
  - In the **IP address** field, enter the IP address in the valid IP address/valid prefix length format.
  - In the **MTU** field, enter the MTU. The range is 576 to 9000 or inherit.
  - In the **OSPF Policy** field, click **Select** and choose the OSPF policy.
  - Click **Submit**.

Note You can update the site settings, pod, and spine using the **Update** option available under respective tabs.

Creating an OSPF Policy

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account and click **View Details**.

Step 4 Click **OSPF Policies**.

Step 5 Click **Create**.

Step 6 On the **Create OSPF Policy** screen, complete the fields, including the following:

- Enter a unique name for the OSPF policy.
- From the **Network Type** drop-down list, choose broadcast, point-to-point, or unspecified as the interface type.
- Enter the routing device's priority in the range of 0 to 255, for becoming the designated router. The routing device that has the highest priority value on the logical IP network or subnet becomes the network's designated router. The default value is 1.
- Enter the cost of an OSPF interface in the range of 0 to 65535. The cost is a routing metric that is used in the link-state calculation. The default value is 0.
- Choose one of the following as the interface control:

- **Advertise-subnet**—To advertise subnet.
- **BFD**—To enable Bidirectional Forwarding Detection (BFD) at the interface.
- **MTU-ignore**—To ignore any IP MTU mismatch with neighbors.
- **Passive-participation**—To suppress routing updates on the interface.

- In the **Hello Interval (SECONDS)** field, enter how often the routing device sends hello packets out the interface. The hello interval must be in the range of 1 to 65535. The default value is 10.
- In the **Dead Interval (SECONDS)** field, enter how long OSPF waits before declaring that a neighboring routing device is unavailable. The dead interval must be in the range of 1 to 65535. The default value is 40.
- In the **Retransmit Interval (SECONDS)** field, enter how long the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements (LSAs) to an interface's neighbors. The retransmit interval must be in the range of 1 to 65535. The default value is 5.
- In the **Transmit Delay (SECONDS)** field, enter the estimated time required to transmit a link-state update on the interface. The transmit delay must be in the range of 1 to 450. The default value is 1.

Step 7 Click **Submit**.

Configuring Control Plane BGP

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the ACI Multi-Site account for which you want to configure the control plane BGP.

Step 4 Click **Configure Control Plane BGP**.

Step 5 On the **Configure Control Plane BGP** screen, complete the fields, including the following:

- From the **Bgp Peering Type** drop-down list, choose full-mesh or route-reflector. The default value is full-mesh.
- In the **Keep Alive Interval (SECONDS)** field, enter the keep alive value to retain the route information learned from BGP in the routing table. The keep alive interval must be in the range of 0 to 3600. The default value is 60.
- In the **Hold Interval (SECONDS)** field, enter the hold-time value to use when negotiating a connection with the peer. The hold interval must be in the range of 0 to 3600. The default value is 180.
- In the **Stale Interval (SECONDS)** field, enter the period of time for which stale routes must be preserved by using the long-lived graceful restart capability for BGP sessions on the restarting router. The stale interval must be in the range of 1 to 3600. The default value is 300.
- Check **Graceful Helper** to enable or turn on the helper mode to assist a neighboring router attempting a graceful restart.
- In the **Maximum AS Limit** field, enter the maximum allowed number of autonomous system (AS) in the range of 0 to 2000. The default value is 0.
- In the **Bgp TTL Between Peers** field, enter the maximum time-to-live (TTL) value for the TTL in the IP header of BGP packets in the range of 1 to 255. The default value is 10.

Step 6 Click **Submit**.
You can view the control plane BGP configured for the site under the **Summary** tab (**ACI Multi-Site Account** > **Summary**).

Generating the ACI Multi-Site Troubleshooting Report

For troubleshooting issues that you may face in ACI Multi-Site, you can generate the troubleshooting report and the infrastructure log file for all the schemas, sites, tenants, and users that are managed by ACI Multi-Site.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with ACI Multi-Site Controller account for which you want to generate troubleshooting report.

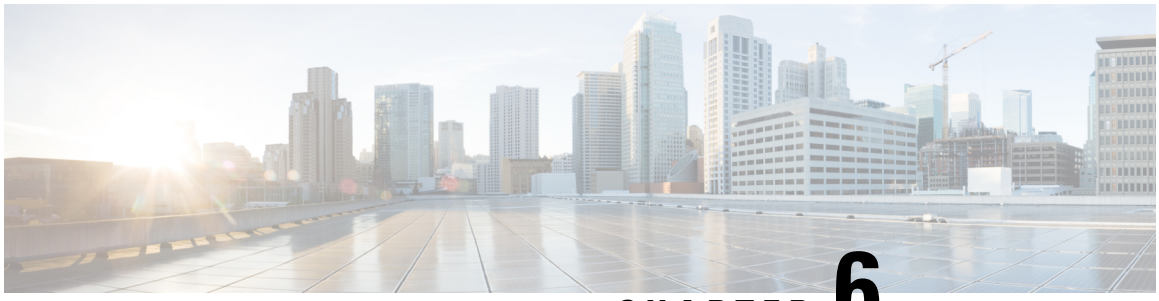
Step 4 Click **Download Troubleshooting Report**.

Step 5 On the **ACI Multi-Site Troubleshooting Report Download** screen, check the check box of the objects for which you want to generate and view the report:

- Sites—Site definitions in the JSON format.
- Tenants—Tenant definitions in the JSON format.
- Schemas—All schemas available in the Multi-Site in the JSON format.
- Users—User defintions in the JSON format
- Infra Logs—Logs of the containers in the infra_logs.txt file.

Step 6 Click **Submit**.
Cisco UCS Director will fetch the report for selected objects from the ACI Multi-Site.

Step 7 Click the download link to download the troubleshooting report. If you want to change the objects that you have chosen for report generation, do the necessary changes and click **Generate Download Link**.



CHAPTER 6

Configuring L4-L7 Services

Unmanaged Mode

In unmanaged mode, Cisco APIC allocates only the network resources for the service graph and programs only the fabric side during graph instantiation. You must configure the unmanaged device in an external application or tool.

When you add an unmanaged network device, Cisco APIC does not require the device package for that device.

For more information about unmanaged mode, see the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

Setting Up an Unmanaged Device

For unmanaged devices, the Application Policy Infrastructure Controller (APIC) allocates only the network resources for the service graph and programs only the fabric side during graph instantiation.You cannot configure an unmanaged device in the APIC.

Step 1 Add an unmanaged device cluster.

See Adding an Unmanaged Device Cluster, on page 69.

Step 2 Add at least one concrete device to the unmanaged device cluster.

See Adding a Concrete Device to an Unmanaged Device Cluster, on page 72.

Step 3 For a virtual concrete device, add at least one vNIC to the concrete interface on the device.

See Adding a vNIC to an Unmanaged Virtual Concrete Device, on page 74.

Step 4 For a physical concrete device, add at least one path to the concrete interface on the device.

See Adding a Path Interface to an Unmanaged Physical Concrete Device, on page 75.

Step 5 Add at least one logical interface to the unmanaged device cluster.

See Adding a Logical Interface to an Unmanaged Device Cluster, on page 71.

Step 6 Create an L4-L7 service graph template with the configuration parameters you want to use for the device cluster.

See Creating a Service Graph Template, on page 85.

Step 7 Apply the L4-L7 service graph template to configure the device cluster.

See Applying a Service Graph Template, on page 86.

Managed Mode

By default, when a device is registered with Cisco APIC, the device is set to be in managed mode. When a device is configured as managed, Cisco APIC manages the device and programs the device during graph instantiation.

Setting Up a Managed Device

Step 1 Add a managed device cluster.

See Adding a Managed Device Cluster, on page 70.

Step 2 Add at least one concrete device to the managed device cluster.

See Adding a Concrete Device to a Managed Device Cluster, on page 73.

Step 3 For a virtual concrete device, add at least one vNIC to the concrete interface on the device.

See Adding a vNIC to a Managed Virtual Concrete Device, on page 74.

Step 4 For a physical concrete device, add at least one path to the concrete interface on the device.

See Adding a Path Interface to a Managed Physical Concrete Device, on page 75.

Step 5 Add at least one logical interface to the managed device cluster.

See Adding a Logical Interface to a Managed Device Cluster, on page 72.

Step 6 Create an L4-L7 service graph template with the configuration parameters you want to use for the device cluster.

See Creating a Service Graph Template, on page 85.

Step 7 Apply the L4-L7 service graph template to configure the device cluster.

See Applying a Service Graph Template, on page 86.

Device Clusters

A device cluster, also known as a logical device, contains one or more concrete devices that act as a single device. A device cluster has cluster interfaces, also known as logical interfaces, which describe the interface information for the device cluster.

Device clusters can be managed or unmanaged.

When the Application Policy Infrastructure Controller (APIC) renders and instantiates service graph templates, it does the following:

- Associates function node connectors with the cluster interfaces.
- Allocates network resources for a function node connector, such as VLAN or Virtual Extensible Local Area Network (VXLAN) resources
- Programs those network resources onto the cluster logical interfaces

The service graph template uses a specific device that is based on a device selection policy, known as a logical device context.

Each device cluster can have a maximum of two concrete devices in active/standby mode.

Adding an Unmanaged Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click **Add**.

Step 8 On the **Add Device Cluster** screen, complete the following fields:

a) Ensure that **Managed** is not checked.

b) In the **Device Cluster** field, enter a unique name for the cluster.

c) From the **Context Aware** drop-down list, choose one of the following:

- **Single**—The device cluster must be given to a specific tenant and cannot be shared across multiple tenants. This is the default value.
- **Multiple**—The device cluster can be shared across multiple tenants of a given type that you are hosting on a provider network.

d) From the **Function Type** drop-down list, choose one of the following:

- **Go To**—A GoTo device has a specific destination. This is the default value.
- **Go Through**—A GoThrough device is a transparent device. A packet goes through the device without being addressed to it, and the endpoints are not aware of the device.

e) From the **Service Type** drop-down list, choose one of the following:

- **ADC**—One-arm and two-arm deployment modes.
- **Firewall**—Routed and transparent deployment modes.
- **IDS/IPS**—IDS and IPS deployment modes.
- **Other**—Any other mode.

f) From the **Device Type** drop-down list, choose one of the following:

- **Physical**
- **Virtual**

g) Click **Select** and check the domain that you want to use.

The domain must be a VMM domain if the device type is Virtual, and a physical domain if the device type is Physical.

Step 9 Click **Submit**.

Adding a Managed Device Cluster

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Device Clusters**.
Step 7 Click **Add**.
Step 8 On the **Add Device Cluster** screen, complete the following fields:

a) Ensure that **Managed** is checked.
b) In the **Device Cluster** field, enter a unique name for the cluster.
c) Click **Select** and check the device package that you want to use.
d) Click **Model** and check the device package model that you want to use.
e) Choose **True** from the **Promiscuous Mode** drop-down list, to enable promiscuous mode. When promiscuous mode is enabled on an interface, all packets received on the interface are sent to the central point or to the Services Processing Unit (SPU) regardless of the destination MAC address of the packet.
f) From the **Context Aware** drop-down list, choose one of the following:

- **Single**—The device cluster must be given to a specific tenant and cannot be shared across multiple tenants. This is the default value.
- **Multiple**—The device cluster can be shared across multiple tenants of a given type that you are hosting on a provider network.

g) From the **Function Type** drop-down list, choose one of the following:

- **Go To**—A GoTo device has a specific destination. This is the default value.
- **Go Through**—A GoThrough device is a transparent device. A packet goes through the device without being addressed to it, and the endpoints are not aware of the device.

h) From the **Service Type** drop-down list, choose one of the following:

- **ADC**—One-arm and two-arm deployment modes.
- **Firewall**—Routed and transparent deployment modes.
- **IDS/IPS**—IDS and IPS deployment modes.
- **Other**—Any other mode.

i) From the **Device Type** drop-down list, choose one of the following:

- **Physical**
- **Virtual**

j) Click **Select** and check the domain that you want to use.

The domain must be a VMM domain if the device type is Virtual, and a physical domain if the device type is Physical.

k) From the **APIC to Device Management Connectivity** drop-down list, choose the type of connectivity. Choose **Out-of-Band** when you are connecting to a device that is outside of the fabric or **In-Band** when you are connecting to a device through the fabric.

l) Click **Select** and check the EPG that you want to use.

m) Enter the virtual IP address, port, user name, and password for the cluster management interface.

Step 9 Click **Submit**.

Logical Interfaces

Adding a Logical Interface to an Unmanaged Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the unmanaged device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Logical Interface**.

Step 9 Click **Add**.

Step 10 On the **Add Device Cluster Logical Interface** screen, complete the following fields:

a) Enter a unique name for the logical interface.

b) In the **Encapsulation** field, enter the traffic encapsulation identifiers for the logical interface.

The valid VLAN range for encapsulation is between 1 and 4094.

Step 11 Click **Submit**.

Adding a Logical Interface to a Managed Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the managed device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Logical Interface**.

Step 9 Click **Add**.

Step 10 On the **Add Device Cluster Logical Interface** screen, complete the following fields:

a) Enter a unique name for the logical interface.

b) Click **Select** and check the logical interface type that you want to use for managed device cluster.

Step 11 Click **Submit**.

Concrete Devices

A concrete device has concrete interfaces. When a concrete device is added to a logical device cluster, concrete interfaces are mapped to the logical interfaces. During service graph template instantiation, VLANs and VXLANs are programmed on concrete interfaces that are based on their association with logical interfaces.

You can create multiple cluster interfaces on a concrete device and then specify which cluster interface will be used for the connector in the device selection policy. This cluster interface can be shared by using multiple service graph instantiations.

Adding a Concrete Device to an Unmanaged Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the unmanaged physical device cluster that you want to update and click **View Details**.

Step 8 Click **Concrete Device**.

Step 9 Click **Add**.

Step 10 On the **Add Device Cluster Concrete Device** screen, complete the following fields:

a) In the **Device Name** field, enter a unique name for the concrete device.
b) In the **Device Context Label** field, enter the label for the device cluster context.
c) For a virtual device cluster, in the **VM Name** field, enter the name of the VM where the device is hosted.
d) For a virtual device cluster, in the **vCenter Name** field, enter the name of the VMware vCenter where the VM is located.

Step 11 Click **Submit**.

Adding a Concrete Device to a Managed Device Cluster

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the managed physical device cluster where you want to create the concrete device and click **View Details**.

Check the **Device Type** column to determine if the device cluster is physical or virtual.

Step 8 Click **Concrete Device**.

Step 9 Click **Add**.

Step 10 On the **Add Device Cluster Concrete Device** screen, complete the fields, including the following:

a) In the **Device Name** field, enter a unique name for the concrete device.
b) In the **Device Context Label** field, enter the label for the device cluster context.
c) For a virtual device cluster, in the **VM Name** field, enter the name of the VM where the device is hosted.
d) For a virtual device cluster, in the **vCenter Name** field, enter the name of the VMware vCenter where the VM is located.
e) Enter the virtual IP address, port, user name, and password for the cluster management interface.

Step 11 Click **Submit**.

Adding a vNIC to an Unmanaged Virtual Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the device cluster that you want to update and click **View Details**.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **vNIC to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the fields, including the following:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) In the **vNIC** field, enter the vNIC assigned to this interface.
d) Click **Select** and check the logical interface where you want to add the path.

Step 13 Click **Submit**.

Adding a vNIC to a Managed Virtual Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the managed device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **vNIC to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the following fields:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) In the **vNIC** field, enter the vNIC assigned to this interface.

d) Click **Select** and check the logical interface where you want to add the path.

Adding a Path Interface to an Unmanaged Physical Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the unmanaged device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **Path to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the fields, including the following:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) Click **Select** and check the logical interface where you want to add the path.

Step 13 Click **Submit**.

Adding a Path Interface to a Managed Physical Concrete Device

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Device Clusters**.

Step 7 Click the row with the managed device cluster that you want to update and click **View Details**.

Check the **Managed** column to determine if the device cluster is managed or unmanaged.

Step 8 Click **Concrete Device**.

Step 9 Click the row with the concrete device that you want to update and click **View Details**.

Step 10 Click **Path to Concrete Interface**.

Step 11 Click **Add**.

Step 12 On the **Add Concrete Interface to Device** screen, complete the following fields:

a) In the **Concrete Interface** field, enter a unique name for the interface.
b) Click **Select** and check the path that you want to add to the interface.
c) Click **Select** and check the logical interface where you want to add the path.

Step 13 Click **Submit**.

APIC Function Profiles

An APIC function profile provides default values for the parameters of a particular function associated with a device package that is managed by Cisco APIC. You can then include one or more APIC function profiles in an L4-L7 service graph template. For example, you can create a function profile that provides default values for the Cisco ASA firewall function.

In Cisco UCS Director, you create APIC function profiles within function profile groups.

Function profile groups organize function profiles to make it easier to identify the profiles that you want to include in a specific service graph template.

Note Cisco UCS Director supports only the configuration of Cisco ASA devices through APIC function profiles and service graphs. You can create service graph template and function profile with load balancer service. But the parameters that are added for the function profile through individual workflow task, user interface action, and REST API in Cisco UCS Director, are supported for firewall service alone.

Creating an APIC Function Profile Group

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click **Add**.

Step 8 On the **Add Function Profile Group** screen, enter a name and description for the group and click **Submit**.

What to do next

Add one or more APIC function profiles to the function profile group.

Creating an APIC Function Profile

Note Cisco UCS Director supports only the configuration of Cisco ASA devices through APIC function profiles and service graphs.

Before you begin

- Create an APIC function profile group.
- Create an APIC firewall policy.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to add a function profile and click **View Details**.

Step 8 Click **Function Profile**.

Step 9 Click **Add**.

Step 10 On the **Create Function Profile** screen, complete the following fields:

a) Add a unique name and description for the function profile.

b) Click **Select** and check the row with the APIC account, device, and function that you want to use.

For example, to configure a firewall for a Cisco ASA 1.2, check a row that has a Device Package Name of CISCO-ASA-1.2 and a Function of Firewall. After you validate your selection, the function displays next to **Function Name**.

c) If you chose a load balancing function, in the **Load Balancer Parameters** area, complete the following fields:

- **External ID**
- **External Netmask**
- **Internal ID**
- **Internal Netmask**
- **Services**—Use a comma-separated list to include multiple services.
- **LB IPv4 IP**

d) Optional. If you chose a firewall function, click **Select** and check the APIC firewall policy that you want to assign to this function profile.

If the list does not include the firewall policy you need, click **Add** to create a new policy.

Alternately, navigate to **Policy** > **Resource Groups** > **APIC Firewall Policy**, and then click **Add** to create a firewall policy.

e) Click **Submit**.

What to do next

Click **View Details** and add one or more parameters to the function profile from **Function Profile Parameters**. After you add the parameters, they are displayed on either **L4L7 Function Profile Parameters** or **Function Profile Function Parameters**.

Adding ACL Parameters to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameter**.

Step 11 Choose **Add ACL to Function Profile**.

Step 12 On the **Add ACL to Function Profile** screen, complete the following fields:

a) In the **ACL List Name** field, enter the name of the Access Control List.

b) In the **ACE Name** field, enter the name of the Access Control Entry in the ACL to specify the permit or deny rule for packets.

c) From the **Protocol** drop-down list, choose one of the following protocols:

- **ip**
- **tcp**
- **udp**
- **icmp**

d) Check **Source Any** if you want the ACL to apply to any source IP address.

If you do not check this box, enter a single IP address, an IP address range, or a network address or subnet address in the **Source Address** field.

e) Check **Destination Any** if you want the ACL to apply to any destination IP address.

If you do not check this box, you can enter a single IP address, an IP address range, or a network address or subnet address in the **Destination Address** field.

f) From the **Action** drop-down list, choose one of the following:

- **deny** if you want this ACL to drop the packet.

- **allow** if you want this ACL to forward the packet. The ACL denies all packets that you do not specifically allow.

g) In the **Order** field, enter the order of this entry in the ACL.

Step 13 Click **Submit**.

Adding an Interface to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Interface to Function Profile**.

Step 12 On the **Add Interface to Function Profile** screen, complete the following fields:

a) Enter a unique name for the interface.

b) From the **Type** drop-down list, choose one of the following:

- **External**
- **Internal**

c) In the **IPv4 Address** field, enter the IPv4 address for the interface.

d) In the **Security Level** field, enter the security level for the interface.

The security level can be from 0 (lowest) to 100 (highest). The Cisco ASA uses the security level to determine the type of traffic allowed to and from the interface. For example, you can assign a higher security level to an interface that handles internal traffic and a lower security level to an interface that handles external traffic.

e) Click **Select** and check the bridge group that you want to use for this interface.

f) Click **Select** and check the ACL that you want to use for inbound traffic.

g) Click **Select** and check the ACL that you want to use for outbound traffic.

Step 13 Click **Submit**.

Adding a Bridge Group Interface to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 On the **Function Profile Group** page, choose the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Bridge Group Interface to Function Profile**.

Step 12 On the **Add Bridge Group Interface to Function Profile** screen, complete the following fields:

- **Bridge Group ID**—Enter an integer between 1 and 100.
- **IPv4 Address Value**—Enter the IPv4 address for the bridge group interface.

Step 13 Click **Submit**.

Adding a Static Route to an Interface on an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Static Route to Interface on APIC Function Profile**.

Step 12 On the **Add Static Route to Interface on APIC Function Profile** screen, complete the following fields:

a) Click **Select** and check the interface you want to update.

b) From the **Type** drop-down list, choose either **IPv4** or **IPv6**.

c) If you chose **IPv4**, complete the following fields:

- **Gateway Address**

- **Network Mask**
- **Network**
- **Metric**

d) If you chose **IPv6**, complete the following fields:

- **Gateway Address**
- **Hop Count**
- **Prefix**
- **Tunneled**

Step 13 Click **Submit**.

Adding a Network Object to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Function Profile Group**.
Step 7 On the **Function Profile Group** page, choose the row with the group where you want to update the function profile and click **View Details**.
Step 8 Click **Function Profile**
Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.
Step 10 Click **Function Profile Parameter**.
Step 11 Choose **Add Network Object to Function Profile**.
Step 12 On the **Add Network Object to Function Profile** screen, complete the following fields:

a) In the **Network Object Name** field, enter a unique name for the network object.
b) From the **Network Object Type** drop-down list, choose one of the following types:

- **FQDN**
- **Host IP Address**
- **IP Address Range**
- **Network IP Address**

c) If you chose **FQDN**, enter the fully qualified domain name for this network object.
d) If you chose **Host IP Address**, enter the IP address that you want to use for this network object.
e) If you chose **IP Address Range**, enter the range of IP addresses that you want to use for this network object.

f) If you chose **Network IP Address**, enter the IP address that you want to use for this network object.

Step 13 Click **Submit**.

Adding a Service Object to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Add Service Object to Function Profile**.

Step 12 On the **Add Service Object to Function Profile** screen, complete the following fields:

a) In the **Service Object Name** field, enter a unique name for the service object.

b) Enter a description of the service object.

c) In the **Protocol Type** field, enter the IP protocol name or number for the service object.

d) From the **Service Object Type** drop-down list, choose one of the following types:

- **icmp**
- **icmp6**
- **tcp**
- **udp**

After you choose the type, you are prompted to enter additional parameters for that type.

e) If you chose **icmp**, enter the **Code** and **Type** for the service object.

f) If you chose **icmp6**, enter the **Code** and **Type** for the service object.

g) If you chose **tcp**, enter the **High Port**, **Low Port**, and **Operator** for the following fields:

- **TCP Destination**
- **TCP Source**

h) If you chose **udp**, enter the **High Port**, **Low Port**, and **Operator** for the following fields:

- **UDP Destination**—
- **UDP Source**—Enter the **High Port**, **Low Port**, and **Operator**.

Step 13 Click **Submit**.

Creating a NAT Rule for an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 Click the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**.

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 Choose **Create NAT Rule**.

Step 12 On the **Create NAT Rule** screen, complete the following fields:

a) Enter a unique name for the NAT rule.

b) Click **Select** and check the source real object that you want to use.

c) Click **Select** and check the source mapped object that you want to use.

d) From the **Type** drop-down list, choose one of the following:

- **Static**
- **Dynamic**

e) Click **Select** and check the destination real object that you want to use.

f) Click **Select** and check the destination mapped object that you want to use.

g) Click **Select** and check the service real object that you want to use.

h) Click **Select** and check the service mapped object that you want to use.

i) In the **DNS** field, enter the IP address or the fully qualified domain name (FQDN) of the DNS server that you want to use.

j) In the **Order** field, enter the order of the rule in an access list.

The order of the rules in an access list determines how traffic is handled and which rule the Cisco ASA applies to the traffic. For an access list with multiple rules, the Cisco ASA goes through the rules in order and applies the first rule that matches the traffic.

k) In the **Uni-Direction** field, enter unidirectional so that the destination addresses cannot initiate traffic to the source addresses.

l) Click **Select** and check the source interface that you want to use.

m) Click **Select** and check the destination interface that you want to use.

Step 13 Click **Submit**.

Adding a Network Object Group to an APIC Function Profile

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Function Profile Group**.

Step 7 On the **Function Profile Group** page, choose the row with the group where you want to update the function profile and click **View Details**.

Step 8 Click **Function Profile**.

Step 9 On the **Function Profiles** page, choose the profile where you want to add parameters and click **View Details**.

Step 10 Click **Function Profile Parameters**.

Step 11 From **More Actoins** drop-down list, choose **Add Network Object Group to Function Profile**.

Step 12 On the **Add Network Object Group to Function Profile** screen, complete the following fields:

a) Enter a unique name and description for the network object group.

b) From the **Network Object Group Type** drop-down list, choose one of the following:

- **Host IP Address**
- **Network Address**
- **Network Object**

c) If you chose **Host IP Address**, enter an IPv4 or IPv6 address for the host.

d) If you chose **Network Address**, enter one of the following:

- An IPv4 address with netmask in the following format: 10.10.10.10/255.255.255.255
- An IPv6 address with prefix in the following format: X:X:X:X:X:X/<0-128>

e) If you chose **Network Object**, click **Select** and check the network objects that you want to include.

Step 13 Click **Submit**.

Service Graph Templates

A service graph template contains configuration parameters, which you can specify through one or more of the following:

- Device package
- EPG
- Application profile
- Tenant context

You can apply a service graph template to multiple devices and ensure that all of those devices have the same configuration.

A function node within a service graph template can require one or more configuration parameters. You can lock the parameter values to prevent any additional changes.

The values of the configuration parameters in a service graph are passed to the device script within the device package. The device script converts the parameter data to the configuration that is downloaded onto the device.

Creating a Service Graph Template

Before you begin

Create at least one function profile for the function and device.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Service Graph**.

Step 7 Click **Create L4 L7 Service Graph Template**.

Step 8 On the **Create L4 L7 Service Graph Template** screen, complete the following fields:

a) Enter a unique name and description for the service graph template.

b) From the **Type** drop-down list, choose the type of template you want to create.

The template type determines which configuration parameters you can include in the service graph template. The template type can be one of the following:

- **Single Node - Firewall in Transparent Mode**—A single node graph that inserts a firewall into the traffic path. The graph configures the firewall in transparent mode without routing. The bridge domain is used for traffic that is derived from the EPGs. You do not need to provide any additional bridge domains.
- **Single Node - Firewall in Routed Mode**—A single node graph that inserts a firewall into the traffic path. The graph configures the firewall in routed mode, which performs the routing. The bridge domain is used for traffic that is derived from the EPGs. You do not need to provide any additional bridge domains.
- **Single Node - ADC in One-Arm Mode**—A single node graph that inserts an ADC into the traffic path. The graph configures the ADC in 1-ARM mode. The bridge domain is used for traffic that is explicitly provided.
- **Single Node - ADC in Two-Arm Mode**—A single node graph that inserts an ADC into the traffic path. The graph configures the ADC in 2-ARM mode without routing. The bridge domain is used for traffic that is derived from the EPGs. You do not need to provide any additional bridge domains.
- **Two Nodes - Firewall in Transparent and ADC in One-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in transparent mode without routing and the ADC in 1-ARM mode. The bridge domain that is used for the traffic from the firewall to the ADC and the ADC to the provider EPG is explicitly provided.

- **Two Nodes - Firewall in Routed and ADC in One-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in routed mode and the ADC in 1-ARM mode. The bridge domain that is used for the traffic in to and out of the ADC is explicitly provided.
- **Two Nodes - Firewall in Routed and ADC in Two-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in routed mode and the ADC in 2-ARM mode. The bridge domain that is used for the traffic from the firewall to the ADC and the firewall to the consumer EPG is explicitly provided.
- **Two Nodes - Firewall in Transparent and ADC in Two-Arm Mode**—A two node graph that inserts a firewall and an ADC into the traffic path. The graph configures the firewall in transparent mode and the ADC in 2-ARM mode. The bridge domain that is used for the traffic for Firewall to ADC is explicitly provided.

c) Complete the following fields to add the configurations to the service graph template. If you have chosen Two Nodes template type, you have to specify the following details for two nodes.

If you chose a template type with a firewall, the firewall is always Node One, whether you choose a Single Node or Two Nodes template type. If you chose a template type with an ADC, the ADC is Node One for a Single Node template type and Node Two for a Two Nodes template type.

- **Managed**—Specifies whether the device is managed or unmanaged. For unmanaged device, you can enable policy-based route redirect by choosing **true** from **Route Redirect** drop-down list. For a managed device, complete the following fields.
  - **Function Name**—Specifies the virtual function for a managed device. Click **Select** and choose a function name that you want to use. This is a single virtual function on a service device such as a firewall, a load balancer, or an SSL offloading device.
  - **Function Profile**—Specifies the function profile for a managed device. Click **Select** and choose a function profile that you want to use. The profile includes the abstract device configuration, the abstract group configuration, and the abstract function configuration.
- **Route Redirect**—This field is applicable for ADC and Firewall Routed mode. Choose **true** from the drop-down list to enable policy-based route redirect on the ADC or Firewall Routed mode.

Step 9 Click **Submit**.

Applying a Service Graph Template

Before you begin

Depending upon the configuration parameters you plan to use, create the following:

- Consumer EPG or external network
- Provider EPG or external network
- Contract
- Device clusters
- Cluster interfaces

- Bridge domains, if you plan to use a general connector type
- Router configuration, if you plan to use route peering
- Redirect Policy

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Service Graph**.

Step 7 Choose the service graph template with managed or unmanaged node that you want to apply.

Check the **Managed** column of the **Nodes** tab of service graph template to determine if the node is managed or unmanaged.

Step 8 Click **Apply L4 L7 Service Graph Template**.

Step 9 On the **Apply L4 L7 Service Graph Template** screen, complete the following fields:

a) From the **Consumer EPG/External Network** drop-down list, choose either **EPG** or **External Network** and then do one of the following:

- Click **Select** and check the consumer EPG you want to use.
- Click **Select** and check the consumer external network you want to use.

b) From the **Provider EPG/External Network** drop-down list, choose either **EPG** or **External Network** and then do one of the following:

- Click **Select** and check the provider EPG you want to use.
- Click **Select** and check the provider external network you want to use.

c) From the **Create a New Contract/Choose an Existing Contract Subject** drop-down list, choose one of the following:

- **Create a New Contract** and then complete the contract name and filters fields for that contract.
- **Choose an Existing Contract Subject** and then click **Select** and check the contract subject that you want to use.

d) In the **Node One Consumer Connector** area, the status of the policy-based routing is displayed. When the policy-based routing status is true, the **Redirect Policy** drop-down list appears from which you can chose a redirect policy for the contract subject. You have to choose the device cluster, function profile, the consumer connector type and the consumer layer 3 destination virtual IP (VIP) address, and then complete the appropriate fields as per the chosen consumer connector type.

Note The function profile is enabled only when the function profile is not provided as input while creating the service graph template.

- **General**—Choose the **Consumer Bridge Domain** and **Consumer Cluster Interface**.

- **Route Peering**—Choose the **Router Configuration**, **Consumer Cluster Interface**, and **Consumer External Network**.

e) In the **Node One Provider Connector** area, the status of the policy-based routing is displayed. You can choose the provider connector type and the provider layer 3 destination VIP address, and then complete the appropriate fields as per the chosen provider connector type.

- **General**—Choose the **Provider Bridge Domain** and **Consumer Cluster Interface**.
- **Route Peering**—Choose the **Router Configuration**, **Provider Cluster Interface**, and **Provider External Network**.

f) If your service graph or service graph template is a Two Node type, complete the **Node Two Connector** fields for that node.

Step 10 Click **Submit**.

Service Graphs

Service graphs identify the set of network or service functions that are needed by an application. You can instantiate service graphs on the ACI fabric through Cisco UCS Director.

By using a service graph, you can install a service, such as an ASA firewall, once and deploy it multiple times in different logical topologies. Each time the graph is deployed, ACI takes care of changing the configuration on the firewall to enable the forwarding in the new logical topology.

A service graph represents the network using the following elements:

- Function node—A function node represents a function that is applied to network traffic, such as a transform (SSL termination, VPN gateway), filter (firewalls), or terminal (intrusion detection systems). A function within the service graph might require one or more parameters and have one or more connectors.
- Terminal node—A terminal node enables input and output from the service graph.
- Connector—A connector enables input and output from a node.
- Connection—A connection determines how traffic is forwarded through the network.

After you configure a service graph, the network services are automatically configured according to the service function requirements in the service graph. This does not require any change in the service device.

A service graph is represented as two or more tiers of an application with the appropriate service function inserted between them.

A service appliance (or device) performs a service function within the graph. One or more service appliances might be required to render the services required by a graph. One or more service functions can be performed by a single-service device.

Service graphs and service functions have the following characteristics:

- Traffic sent or received by an endpoint group can be filtered based on a policy, and a subset of the traffic can be redirected to different edges in the graph.
- Service graph edges are directional.

- Taps (hardware-based packet copy service) can be attached to different points in the service graph.
- Logical functions can be rendered on the appropriate (physical or virtual) device, based on the policy.
- The service graph supports splits and joins of edges, and it does not restrict the administrator to linear service chains.
- Traffic can be reclassified again in the network after a service appliance emits it.
- Logical service functions can be scaled up or down or can be deployed in a cluster mode or 1:1 active-standby high-availability mode, depending on the requirements.

For more information about the requirements of service graphs and their deployment, see the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

Adding a Service Graph

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **L4-L7 Service Graph**.
Step 7 Click **Add**.
Step 8 On the **Add Service Graph** screen, complete the fields, including the following:
a) Enter a unique name and description for the service graph.
b) Click **Select** and check the node that you want to use.

If the node you want to use is not in the list, click **Add** to create the node.

Step 9 Click **Submit**.

Adding a Filter to a Service Graph Node

A filter policy is a group of resolvable filter entries. Each filter entry is a combination of network traffic classification properties.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **L4-L7 Service Graph**.
Step 7 Click the service graph you want to update and click **View Details**.

Step 8 Click the node where you want to add a filter and click **View Details**.

Step 9 Click **Connectors**.

Step 10 Click **Add**.

Step 11 On the **Add Filter to Service Graph Node** screen, complete the following fields:

a) From the **Connector Mode** drop-down list, choose **internal** or **external**.

b) Click **Select** and check the filter that you want to use.

Step 12 Click **Submit**.

Custom Quality of Service

Achieving the required Quality of Service (QoS) by effectively managing the priority of applications on the fabric is important when deploying an end-to-end solution. Thus, QoS is the set of techniques to manage data center fabric resources.

When QoS is used in ACI to classify packets, packets are classified using layer 2 Dot1P policy, layer 3 differentiated services code point (DSCP) policy, or contracts. DSCP/Dot1p Policy is configured and applied at the EPG level through custom QoS policy.

Adding a Custom QOS Policy

Create a custom QoS policy and then associate the policy with a logical interface context.

Before you begin

Create the tenant, application, and EPGs that will consume the custom QoS policy.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Custom QOS Policy**.

Step 7 Click **Add**.

Step 8 On the **Create Custom QOS Policy** screen, complete the following fields:

a) Enter a unique name for the custom QOS policy.

b) Enter a short description for the custom QOS policy.

Step 9 Click **Submit**.

Adding a DSCP to a Priority Map

DSCP policy within the custom QoS policy is a set of rules; each rule gives mapping of a range of DSCP values to a DSCP target.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Custom QOS Policy**.

Step 7 Click the row with the custom QoS policy to which you want to add DSCP policy and click **View Details**.

Step 8 Click **DSCP to Priority Map**.

Step 9 Click **Add**.

Step 10 On the **Add DSCP to Priority Map** screen, complete the folowing:

a) (Optional) Choose the priority level of the DSCP policy in QoS as **Unspecified**, **Level3**, **Level2**, or **Level1**. By default, the unspecified is set as priority.

b) From the **DSCP Range From** and **DSCP Range To** drop-down lists, choose the starting and ending value for the DSCP range. To set the DSCP range from 0 to 63, choose **Enter customized value** from the drop-down lists and enter the actual value in the **Enter DSCP Range From** and **Enter DSCP Range To** fields.

c) (Optional) Choose a DSCP target to which the DSCP range has to be mapped. Choose **Enter customized value** from the drop-down list, to set any value between 0 and 63 as the DSCP target in the **Enter DSCP Target** field.

d) (Optional) Choose a target class of service (CoS) from the drop-down list. Choose **Enter customized value** from the drop-down list, to set any value between 0 and 8 as the target CoS in the **Enter Target Cos** field.

Step 11 Click **Submit**.

Adding a Dot1P Classifier

Dot1P policy within the custom QoS policy is a set of rules; each rule gives mapping of a range of Dot1P values to a DSCP target.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **Custom QOS Policy**.

Step 7 Click the row with the custom QoS policy to which you want to add Dot1P policy and click **View Details**.

Step 8 Click **Dot1P Classifier**.

Step 9 Click **Add**.

Step 10 On the **Add Dot1P Classifier** screen, complete the following:

a) Choose the priority level of the Dot1P policy in QoS as **Unspecified**, **Level3**, **Level2**, or **Level1**. By default, the unspecified is set as priority.

b) From the **Dot1P Range From** and **Dot1P Range To** drop-down lists, choose the starting and ending value for the Dot1P range.

c) Choose a DSCP target to which the Dot1P range has to be mapped. Choose **Enter customized value** from the drop-down list, to set any value between 0 and 64 as the DSCP target in the **Enter DSCP Target** field.
d) Choose a target cost of service (CoS) from the drop-down list.

Step 11 Click **Submit**.

Adding a Logical Device Context

The service graph uses a specific device based on a device selection policy, known as a logical device context.

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Logical Device Context**.
Step 7 Click **Add**.
Step 8 On the **Add Tenant Logical Device Context** screen, complete the following fields:
a) Click **Select** and check the device cluster that you want to use.
b) Click **Select** and check the contract name that you want to use.
c) Click **Select** and check the graph name that you want to use.
d) Click **Select** and check the node name that you want to use.
e) Enter a unique name for the device context. The name should not exceed 64 characters.
Step 9 Click **Submit**.

Adding a Subnet to a Logical Device Context

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Logical Device Context**.
Step 7 Click the row with the logical device context to which you want to add a subnet and click **View Details**.
Step 8 Click the row with the logical interface context to which you want to add a subnet and click **View Details**.
Step 9 Click **Subnets**.
Step 10 Click **Add**.
Step 11 On the **Add Subnet to Logical Device Context** screen, complete the following fields:
a) Enter a gateway IP address in the format: <valid IP address>/<valid prefix length>. For example, 10.10.10.1/24.

If this gateway is for Anycast, the netmask must be **/32** and check the **Subnet Control (No Default SVI Gateway)** check box to not to set the subnet as the default SVI gateway.

b) From the **Scope** drop-down list, choose **Private to VRF** or **Advertised Externally**. By default, the **Private to VRF** is set as the scope. The **Private to VRF** implies that the subnet can only be used in the tenant. The Advertised Externally option is used to advertise tenant subnets externally on the L3Out.
c) Check the **Shared Between VRFs** check box to define subnets under an endpoint group, with the shared option configured, to route leak to other tenants within the fabric.
d) Enter short description for the subnet.
e) Check the **Subnet Control (ND RA Prefix)** check box to apply control specific to ND RA prefix protocols to the subnet. By default, the check box is checked.
f) Check the **Subnet Control (No Default SVI Gateway)** check box to not to configure Pervasive SVI for the subnet. This setting is used to leak more specific prefix routes to other VRFs. If the **Subnet Control (No Default SVI Gateway)** check box is checked, you can use /32 netmask for the subnet, especially for Anycast services. By default, the check box is left unchecked.
g) Check the **Subnet Control (Querier IP)** check box to enable IGMP snooping on the subnet. By default, the check box is left unchecked.
h) Check the **Preferred** check box to set the subnet as the preferred subnet for the device context. By default, the check box is left unchecked.
i) Check the **Type Behind Subnet** check box to enable AnyCast MAC address. By default, the check box is left unchecked. The **MAC address** field appears only when the **Type Behind Subnet** check box is checked. Enter a MAC address in the format: xx:xx:xx:xx:xx:xx. For example, aa:11:bb:11:cc:11.

Step 12 Click **Submit**.

Adding a Logical Interface Context

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Logical Device Context**.
Step 7 Click the row with the logical device context that you want to update and click **View Details**.
Step 8 Click **Logical Interface Context**.
Step 9 Click **Add**.
Step 10 On the **Add Tenant Logical Interface Context** screen, complete the following fields:
a) Click **Select** and check the logical device context to which you want to add an interface.
b) Enter the connector name. By default, **any** is set as the connector name.
c) Click **Select** and check the logical interface name that you want to add to the logical device context.
d) Click **Select** and check the bridge domain name that you want to add to the logical device context.
e) Click **Select** and check the Layer 3 network that you want to add to the logical device context.
f) From the **L3 Destination (VIP)** drop-down list, choose an appropriate option.

- **Unspecified**—This is the default option. Choose this option to not to specify rule for Layer 3 destination.

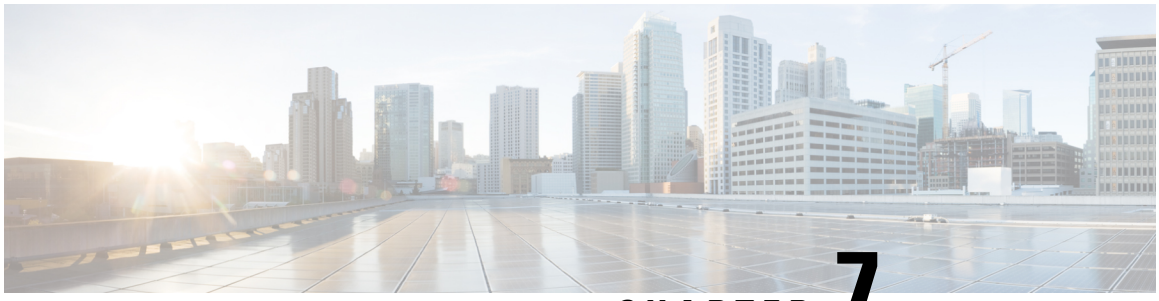
- **True**—If the PBR policy is not configured on a specific service node, the node connector is treated as an L3 Destination and will continue to be in the new Cisco APIC version.
- **False**—Set false to enable user to choose the PBR policy for logical interface.

g) The **L4-L7 Policy Based Redirect** field appears only when **False** is selected as L3 Destination (VIP). Click **Select** and check the L4-L7 PBR that need to be associated to the interface context.
h) Click **Select** and check the custom QoS policy that need to be associated to the interface context.
i) Choose **True** from the **Permit Logging** drop-down list to enable permit logging of logical interface context.

Step 11 Click **Submit**.

Adding a Virtual IP Address to a Logical Interface Context

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **Logical Device Context**.
Step 7 Click the row with the logical device context that you want to update and click **View Details**.
Step 8 Click **Logical Interface Context**.
Step 9 Click the row with the logical interface context that you want to update and click **View Details**.
Step 10 Click **Virtual IP Address**.
Step 11 Click **Add**.
Step 12 On the **Create Virtual IP for Logical Interface** screen, enter the IPv4 address for the logical interface.
Step 13 Click **Submit**.



CHAPTER 7

Configuring Policy Based Redirect

Policy-Based Redirect

Cisco Application Centric Infrastructure (ACI) policy-based redirect (PBR) enables provisioning service appliances, such as firewalls or load balancers, as managed or unmanaged nodes without requiring a Layer 4 to Layer 7 package. Typical use cases include provisioning service appliances that can be pooled, tailored to application profiles, scaled easily, and have reduced exposure to service outages. PBR simplifies the deployment of service appliances by enabling the provisioning consumer and provider endpoint groups to be all in the same virtual redirect and forwarding (VRF) instance.

PBR deployment consists of configuring a route redirect policy and a cluster redirect policy, and creating a service graph template that uses the route and cluster redirect policies. After the service graph template is deployed, use the service appliance by enabling endpoint groups to consume the service graph provider endpoint group. This can be further simplified and automated by using vzAny. While performance requirements may dictate provisioning dedicated service appliances, virtual service appliances can also be deployed easily using PBR.

Creating Layer 4-Layer 7 Policy Based Redirect

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Policy Based Redirect**.

Step 7 Click **Add**.

Step 8 On the **Create Policy Based Redirect** screen, complete the following fields:

- Enter a unique name and description for the Policy Based Redirect.
- Check the **Enable Pod ID Aware Redirection** check box to enable pod ID aware redirection and associate the pod IDs with the preferred PBR nodes to program redirect destinations in the leaf switches located in the specific pods.
- Choose one of the following hashing algorithms:
  - dip—Destination IP address
  - sip—Source IP address
  - sip-dip-prototype—Source IP address, Destination IP address and Protocol Type (also called Symmetric) based algorithm
- Check the **Resilient Hashing Enabled** check box to enable resilient hashing for mapping traffic flows to physical nodes and for avoiding the rehashing of any traffic other than the flows from the failed node.
- Check the **Anycast Endpoint** check box to enable anycast endpoint.
- Click **Select** and check the IP SLA monitoring policy that you want to use for PBR tracking.
- The **Threshold Enable** check box appears when you choose an IP SLA monitoring policy. Check this check box to enable threshold when you want to disable the redirect destination group completely and prevent any redirection. When there is no redirection, the traffic is directly sent between the consumer and the provider. The following threshold settings are available:
  - **Min Threshold Percent (Percentage)** field—Enter the minimum threshold percentage. If the traffic goes below the minimum percentage, the packet is permitted instead of being redirected. The default value is 0. The allowed threshold range is from 0 to 100.
  - **Max Threshold Percent (Percentage)** field—Enter the maximum threshold percentage. When the minimum threshold is reached, to revert to the operational state, the maximum threshold percentage must be reached first. The default value is 0. The allowed threshold range is from 0 to 100.
  - **Threshold Down Action** drop-down list—Choose **permit action** or **deny action** from the drop-down list to apply the threshold settings on traffic.

Step 9 Click **Submit**.

Creating Layer 4 - Layer 7 Redirect Health Group

Step 1 Choose **Physical** > **Network**.
Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.
Step 3 Click the row with the APIC account and click **View Details**.
Step 4 Click **Tenant(s)**.
Step 5 Click the row with the tenant that you want to update and click **View Details**.
Step 6 Click **L4 L7 Redirect Health Group**.
Step 7 Click **Add**.

Step 8 On the **Create L4-L7 Redirect Health Group** screen, enter a unique name and description for L4-L7 Redirect Health Group.

Step 9 Click **Submit**.

When a redirect health group is no longer consumed by the PBR, you can delete the redirect health group. To delete the redirect health group, click the row with the redirect health group on the **L4 L7 Redirect Health Group** screen and click **Delete**.

Creating a Destination of Redirect Traffic

Before you begin

The redirect health group that needs to be associated with the redirect traffic is created.

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **L4-L7 Policy Based Redirect**.

Step 7 Click the row with the L4-L7 policy based rediect record that you want to update and click **View Details**.

Step 8 Click **Destination of Redirect Traffic**.

Step 9 Click **Add**.

Step 10 On the **Add Destination of Redirected Traffic** screen, complete the following fields:

- Enter the IP address for the Layer 4 to Layer 7 device. The IP address must be in the same subnet as the IP address that you have given to the bridge domain.
- Enter a short description for the destination of redirected traffic.
- Enter the MAC address for the Layer 4 to Layer 7 device. You should use a MAC address that is valid upon failover of the Layer 4 to Layer 7 device.
- Enter the secondary IP address for the Layer 4 to Layer 7 device.
- Enter the pod identification value. By default, 1 is set as the pod ID. The valid pod ID range is from 1 to 255.
- Click **Select** and check the check box for the redirect health group that you want to associate to an existing health group.

Step 11 Click **Submit**.

Creating an IP SLA Monitoring Policy

Step 1 Choose **Physical** > **Network**.

Step 2 On the **Network** page, choose the account under **Multi-Domain Managers**.

Step 3 Click the row with the APIC account and click **View Details**.

Step 4 Click **Tenant(s)**.

Step 5 Click the row with the tenant that you want to update and click **View Details**.

Step 6 Click **IP SLA Monitoring Policy**.

Step 7 Click **Add**.

Step 8 On the **Create IP SLA Monitoring Policy** screen, complete the following fields:

a) Enter a unique name and description for the IP SLA Monitoring Policy.

b) In the **SLA Frequency** field, enter the interval probe time to track a packet. The allowed SLA frequency range is 1 to 65535 seconds. The default value is 60 seconds.

c) Choose **icmp** or **tcp** as the SLA type. If you choose **tcp**, then enter the SLA port number in the **SLA Port** field.

Step 9 Click **Submit**.