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 1.

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 1.

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 1.

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.

  To view more details about a link level policy, choose a policy and click **View Details**. The following tab appears:

    - **Link Level Policy Alias**—Displays the names of link level policy and alias.

- **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.

- **Fabric Spine Interface Profiles** tab—Displays the name and description of the fabric spine interface profiles. To add a fabric spine interface profile, click **Add** and enter a unique name and short description for the fabric spine interface profile.
- **CDP Interface Policy** tab—Displays the name and description of the Cisco Discovery Protocol (CDP) interface policy, with the administration status.

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

    - **CDP Interface Policy Alias**—Displays the names of CDP interface policy and alias.

- **CoPP Spine Policy** tab—Displays the name, type of profile, and description of the Cisco Control Plane Policing (CoPP) spine policy. Click **Create** to add a CoPP spine policy. To customize the existing APIC CoPP spine policy or create a customized APIC CoPP spine policy, click **Configure Custom Values for APIC CoPP Spine Policy** and specify the protocol with rate and burst details.

To view more details about a CoPP spine policy, choose a CoPP spine policy and click **View Details**. The following tab appears:

  - **CoPP Spine Custom Values**—Displays the customized APIC CoPP spine policy details.

- **Port Security Policy** tab—Displays the port security policies defined for the APIC account. To create a port security policy, click **Create** and complete the following fields:
  - Enter a unique name and short description for the port security policy.
  - In the **Port Security Timeout** field, choose a specific timeout value after which MAC learning can be re-enabled on an interface.You can choose a value between 60 and 3600 seconds as a timeout value.
  - In the **Maximum Endpoints** field, choose a maximum number of endpoints that can be learned on an interface. You can choose a value between 0 and 12000. If the maximum endpoints value is set as zero, the port security policy is disabled on that port.
  - The **Violation Action** field displays protect. The violation action of the port security policy is always set as the protect mode.

    In the protect mode, MAC learning is disabled and MAC addresses are not added to the Content Addressable Memory (CAM) table. MAC learning is re-enabled after the configured timeout value.

- **VSPAN Sessions** tab—Displays the Virtual Switched Port Analyzer (VSPAN) session details. To create a VSPAN Session, click **Create** and complete the following fields:
  - Enter a unique name and short description for the VSPAN session.
  - From the **Admin State** drop-down list, choose **Start** or **Stop**. By default, **Start** is chosen as the admin state.
  - Click **Select** and choose a VSPAN destination group that needs to be used for the VSPAN sessions.

  Choose a VSPAN session and click **View Details** to view the following tabs:

  - **Destination Group**—Displays the destination group of the VSPAN session.
  - **Sources**—Displays the sources of the VSPAN session. To add a source to the VSAPN session, click **Add** and complete the following fields:
    - Enter a unique name and description for the source.
    - From the **Direction** drop-down list, choose both, incoming, or outcoming as the direction of the source.
    - From the **Source Type** drop-down list, choose **EPG** or **CEP** as the source type.
    - Click **Select** and choose a tenant to be associated with the VSPAN session source.
    - Click **Select** and choose an EPG to be associated with the VSPAN session source.

    To view more details of a source, choose a **Source** and click **View Details**. The following tabs appear:

    - **Source EPG**—Displays the EPG of the VSPAN session source.
    - **Source CEP**—Displays the CEP of the VSPAN session source.

  - **Source Path**—Displays the source path associated with the VSPAN session. To associate a path to a VSPAN session source, click **Add**. In the **Associate Source Path to VSPAN Source** window, choose a port type and a static path.

- **VSPAN Destination Groups** tab—Displays the name and description of the VSPAN destination groups. To create a VSPAN destination group, click **Create** and enter a unique name and description for the VSPAN destination group.

  Choose a VSPAN destination group and click **View Details** to view the VSPAN destination group details. To add a destination to the VSPAN destination group, click **Add** and complete the following fields:

  - Enter a unique name and description for the destination.
  - From the **Destination Type** drop-down list, choose **ERSPAN** or **LSPAN** as the destination type.
  - In the **Destination IP** field, enter a valid IP address as the destination address. This field is displayed only when **ERSPAN** is chosen as the destination type.
  - In the **Flow ID** field, enter a number in the range of 1 to 1023 as the flow ID. The default value is 1. This field is displayed only when **ERSPAN** is chosen as the destination type.
  - In the **TTL** field, enter a number in the range of 1 to 225 as the TTL. The default value is 64. This field is displayed only when **ERSPAN** is chosen as the destination type.
  - In the **MTU** field, enter a number in the range of 64 to 9216 as the MTU value. The default value is 1518. This field is displayed only when **ERSPAN** is chosen as the destination type.
  - In the **DSCP** field, enter a number in the range of 0 to 64 as the DSCP value. This field is displayed only when **ERSPAN** is chosen as the destination type.
  - Click **Select** and choose a destination CEP that you want to use for the VSPAN destination group. This field is displayed only when **LSPAN** is chosen as the destination type.

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

  - **Destination ERSPAN Properties**—Displays the ERSPAN destination details of the VSPAN destination group.
  - **Destination LSPAN Properties**—Displays the LSPAN destination details of the VSPAN destination group.

- **Fibre Channel Interface Policy** tab—Displays the name, description, auto max speed, fill pattern, port mode, receive buffer credit, speed, and trunk mode of the fibre channel interface policy. To create a fibre channel interface policy, click **Create** and complete the following fields:

  - Enter a unique name and description for the fibre channel interface policy.
  - From the **Port Mode** drop-down list, choose **F** or **NP** as the port mode. The default value is **F**.
  - From the **Trunk Mode** drop-down list, choose **auto**, **trunk-off**, or **trunk-on** as the trunk mode. The default value is **trunk-off**.
  - From the **Speed** drop-down list, choose a speed for the fibre channel interface. The default value is **Auto**. On choosing **Auto**, the interface speed will be negotiated to automatically match the speed of the attached link.
  - From the **Auto Max Speed** drop-down list, choose a value as the automatic maximum interface speed. The default value is **32 Gbps**.
  - From the **Fill Pattern** drop-down list, choose **ARBFF** or **IDLE** as the fill pattern for the fibre channel interface. The default value is **IDLE**.

  - In the **Receive Buffer Credit** field, enter a receive buffer credit in the range of 16 to 64 for the fibre channel interface. The default value is **64**.

- **Data Plane Policing** tab—Displays the name,burst size, excessive burst size, rate, and peak rate of the Data Plane Policing (DPP) policy. To add a DPP policy, click **Add** and complete the following fields:
  - Enter a unique name for the DPP.
  - Choose **enabled** from the drop-down list, to enable the administrative state of the DPP. The default value is disabled.
  - Choose **Bit Policer** or **Packet Policer** as the policer mode.
  - Choose one of the following as the traffic policer type:
    - **1 Rate 2 Color**—To rate-limit a traffic flow to an average bits-per-second arrival rate.
    - **2 Rate 3 Color**—To rate-limit a traffic flow to two rates and three traffic categories (green, yellow, and red).
  - Choose **Drop**, **Mark**, or **Transmit** as the action to be taken on categorizing a traffic flow as conforming (green).
  - In the **Conform mark cos** field, enter **unspecified**, **default value**, **0xffff**, or enter a number between 0 and 6 to set the Class of Service (CoS) value for the traffic belonging to a specific class when the traffic flow is categorized as conforming.
  - In the **Conform mark dscp** field, enter **unspecified**, **default value**, **0xffff**, or enter a number between 0 and 63 to set the differentiated services code point (DSCP) value for the traffic belonging to a specific class when traffic flow is categorized as conforming.
  - The **Exceed Action** field appears only when **2 Rate 3 Color** is chosen as the traffic policer type. Choose **Drop**, **Mark**, or **Transmit** as the action to be taken when the traffic flow is exceeded.
  - The **Exceed mark cos** field appears only when **2 Rate 3 Color** is chosen as the traffic policer type. Enter **unspecified**, **default value**, **0xffff**, or enter a number between 0 and 6 to set the CoS value for the traffic belonging to a specific class when the traffic flow is exceeded.
  - The **Exceed mark dscp** field appears only when **2 Rate 3 Color** is chosen as the traffic policer type. Enter **unspecified**, **default value**, **0xffff**, or enter a number between 0 and 63 to set the DSCP value for the traffic belonging to a specific class when the traffic flow is exceeded.
  - Choose **Drop**, **Mark**, or **Transmit** as the action to be taken on categorizing a traffic flow as nonconforming (red).
  - In the **Violate mark cos** field, enter **unspecified**, **default value**, **0xffff**, or enter a number between 0 and 6 to set the CoS value for the traffic belonging to a specific class on traffic violation.
  - In the **Violate mark dscp** field, enter **unspecified**, **default value**, **0xffff**, or enter a number between 0 and 63 to set the DSCP value for the traffic belonging to a specific class on traffic violation.
  - Choose **Shared Policer** or **Dedicated Policer** as the policy mode. The default value is **Dedicated Policer**. The shared policer mode allows you to apply the same policing parameters to several interfaces simultaneously.
  - Enter the number of packets allowed at line rate during burst, as the burst size.
  - From the drop-down list, choose the unit at which the burst size has to be calculated.

    - Enter **unspecified**, **default value**, **0xffff**, or enter a number between 0 and 5497555813760 to configure the excessive burst size.
    - From the drop-down list, choose the unit at which the excessive burst size has to be calculated.
    - Enter a number between 0 and 4398046510080 as an allowed rate. This is the committed rate at which the packets are allowed into the system (raw NTPD format).
    - From the drop-down list, choose the unit at which the allowed rate has to be calculated.

- **CoPP Leaf Policy** tab—Displays the name, type of profile, and description of the Cisco Control Plane Policing (CoPP) leaf policy. Click **Create** to add a CoPP leaf policy. To customize the existing APIC CoPP leaf policy or create a customized APIC CoPP leaf policy, click **Configure Custom Values for APIC CoPP Leaf Policy** and specify the protocol with rate and burst details.

  To view more details about a CoPP leaf policy, choose a CoPP leaf policy and click **View Details**. The following tab appears:

    - **CoPP Leaf Custom Values**—Displays the customized APIC CoPP leaf policy details.

- **NetFlow Exporters** tab—Displays the name, description, source type, source IP address, destination port, destination IP address, QoS DSCP value, and version fromat of the NetFlow exporters. To add a NetFlow exporter, click **Add** and complete the following fields in the **Create External Collector Reachability** screen:

    - Enter a unique name and description for the external collector reachability.
    - From the **Source Type** drop-down list, choose the source type for the external collector reachability.
    - In the **Source IP Address** field, enter either the IPv4 or IPv6 address of the source with the subnet mask.
    - From the **Destination Port** drop-down list, choose the destination port for the external collector reachability.
    - In the **Destination IP Address** field, enter either the IPv4 or IPv6 address of the destination with the subnet mask.
    - From the **QoS DSCP Value** drop-down list, choose a QoS DSCP value. The default value is **None**.
    - From the **Netflow Explorer Version Format** drop-down list, choose a version from the list. The default value is **Cisco proprietary version 1**.
    - From the **EPG Type** drop-down list, choose an EPG type.

  To view more details about a NetFlow exporter, choose a NetFlow exporter and click **View Details**. The following tabs appears:

    - **Associated EPG**—Dsiplays the type and name of EPG associated with the external controller reachability.
    - **Associated VRF**—Dsiplays the name of VRF associated with the external controller reachability.

- **Port Channel Member Policies** tab—Displays the port channel member policies of the APIC accounts. To add a port channel member policy, click **Add** and complete the following fields:

    - Enter a unique name and description for the port channel member policy.
    - In the **Priority** field, enter any value in the range of 1 to 65535 as the priority for the port channel member policy. By default, 32768 is set as priority.
    - From the **Transmit Rate** drop-down list, choose **Normal** or **Fast** as the transmit rate.

  To view more details about a port channel member policy, choose a policy and click **View Details**. The following tab appears:

  - **Port Channel Member Policy Alias**—Displays the name and alias of the port channel member policies.

- **MACsec Interface Policies** tab—Displays the details of the Media Access Control Security (MACsec) interface policies of the APIC account. To create a MACsec interface policy, click **Add** and complete the following fields:

  - Enter a unique name and description for the MACsec interface policy.
  - From the **Admin State** drop-down list, choose **Disabled** to disable the admin state, if required. By default, the admin state is enabled.
  - Click **Select** and choose a MACsec parameter policy that you want to associate with the MACsec interface policy.
  - Click **Select** and choose a MACsec KeyChain policy that you want to associate with the MACsec interface policy.

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

  - **MACsec Parameter**—Displays the MACsec parameter policies that are associated with the MACsec interface policy.
  - **MACsec KeyChain**—Displays the MACsec KeyChain policies that are associated with the MACsec interface policy.
  - **MACsec Interface Policy Alias**—Displays the names of MACsec access interface policy and alias.

- **MACsec KeyChain Policies** tab—Displays the details of the MACsec KeyChain policies of the APIC account. To create a MACsec KeyChain policy, click **Create** and enter a unique name and description for the MACsec KeyChain policy.

  To view more details about a MACsec Keychain policy, choose a MACsec KeyChain policy and click **View Details**. The following tabs appear:

  - **MACsec KeyChain Policy Alias**—Displays the name and alias of the MACsec access interface policies.
  - **MACsec Key Policy**—Displays the defined MACsec key policy. To add a MACsec key policy, click **Add** and complete the following fields:

    - Enter a unique name and description for the MACsec key policy.
    - In the **Key Name** field, enter a key name. It allows only hexadecimal characters.
    - In the **Pre-shared Key** field, enter a pre-shared key (PSK) information.

      For 128-bit cipher suites, only 32 character PSKs are permitted.

      For 256-bit cipher suites, only 64 Character PSKs are permitted.

    - In the **Start Time** field, select a date and time from when the key is valid. By default, the current date and time is set as the start time.
    - Check the **Set End Time** check box to set the expiry date for the key. If this check box is left unchecked, the end time of the key is set as infinite.

        - In the **End Time** field, select a date and time for the key to expire. This field appears only when the **Set End Time** check box is checked.

- **MACsec Access Parameters Policy** tab—Displays the details of the MACsec access parameters policies of the APIC account. To add a MACsec access parameters policy, click **Add** and complete the following fields:
    - Enter a unique name and description for the MACsec access parameters policy.
    - From the **Cipher Suite** drop-down list, choose a cipher suite that needs to be used to encrypt traffic on an Ethernet link secured with MACsec.
    - From the **Confidentiality Offset** drop-down list, choose one of the following options to configure a confidentiality offset for MACsec:
        - **Skip 0 bytes**—No octets are unencrypted. All traffic on the interface where the secure channel is applied is encrypted.
        - **Skip 30 bytes**—The first 30 octets of each Ethernet frame are unencrypted.
        - **Skip 50 bytes**—The first 30 octets of each Ethernet frame are unencrypted.
    - In the **Key Server Priority** field, enter the key server priority for the MACsec Key Agreement (MKA) server selection. By default, 16 is set as the key server priority. The switch with the lower priority number is selected as the key server.
    - In the **Window Size** field, enter the window size. By default, 64 is set as window size.
    - In the **Secure Association Key Expiry Time** field, enter the expiry time for Secure Association Key (SAK). The default value is disabled.
    - From the **Security Policy** drop-down list, choose one of the following options as the security policy:
        - **Must secure mode**—To allow encrypted traffic on the link.
        - **Should secure mode**—To allow both clear and encrypted traffic on the link.

- **Storm Control Policy** tab—Displays the details of the storm control policies of the APIC account. To create a storm control policy, click **Add** and complete the following fields:
    - Enter a unique name and description for the storm control policy.
    - From the **Configure Storm Control** drop-down list, choose **All Types** or **Unicast, Broadcast, Multicast**. Choosing the **Unicast, Broadcast, Multicast** option allows you to configure Storm Control on each traffic type separately.
    - From the **Specify Policy In** drop-down list, choose **Percentage** or **Packets Per Second**.
        - If you chose **Percentage**, perform the following steps:
            - In the **Rate** field, enter a traffic rate percentage.

              Enter a number between 0 and 100 that specifies a percentage of the total available bandwidth of the port. When the ingress traffic reaches this level during a one second interval, traffic storm control drops traffic for the remainder of the interval. A value of 100 means no traffic storm control. A value of 0 suppresses all traffic.
            - In the **Max Burst Rate** field, enter a burst traffic rate percentage.

Enter a number between 0 and 100 that specifies a percentage of the total available bandwidth of the port. When the ingress traffic reaches this level, traffic storm control begins to drop traffic.

- If you chose **Packets Per Second**, perform the following steps:
    - In the **Rate** field, enter a traffic rate in packets per second.

      During this interval, the traffic level, expressed as packets flowing per second through the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.
    - In the **Max Burst Rate** field, enter a burst traffic rate in packets per second.

      During this interval, the traffic level, expressed as packets flowing per second through the port, is compared with the burst traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

- In the **Alias** field, enter the name of the alias.
- From **Storm Control Action** drop-down list, choose a storm control action type.

To view more details about a storm control policy, choose a storm control policy and click **View Details**. The following tab appears:

- **Storm Control Policy Alias**—Displays the name and alias of the storm control policies.

- **Priority Flow Control Policy** tab—Displays the details of the state of Priority Flow Control (PFC) on the interfaces to which this policy group is applied. This policy specifies under what circumstances QoS-level PFC will be applied to FCoE traffic. To add a PFC policy, click **Add** and complete the following fields:
    - **Name** and **Description** fields—Enter a unique name and description for the PFC policy.
    - **State** drop-down list—Choose one of the following states to which PFC policy is applied:
        - **Auto**—Enables PFC on local port on the no-drop CoS as configured, on the condition that values advertised by the DCBX and negotiated with the peer succeed. Failure causes PFC to be disabled on the no-drop CoS. This is the default option.
        - **On**—Enables FCoE PFC on the local port under all circumstances.
        - **OFF**—Disables FCoE PFC on the local port under all circumstances.

- **Slow Drain Policy** tab—Displays the details of the slow drain policy for handling FCoE packets that cause traffic congestion on an ACI Fabric. To create a slow drain policy, click **Add** and complete the following fields:
    - **Name** and **Description** fields—Enter a unique name and description.
    - **Congestion Clear Action** drop-down list—Choose one of the following actions to be taken during FCoE traffic congestion:
        - **Err - disable**—Disable the port. This is the default option.
        - **Log**—Record congestion in the Event Log.
        - **Disabled**—Take no action.

    - **Congestion Detect Multiplier** field—Enter the number of pause frames received on a port that triggers a congestion clear action to address FCoE traffic congestion. The default value is 10.
    - **Flush Admin State** drop-down list—Choose one of the following state:
        - **Enabled**—Flush the buffer.
        - **Disabled**—Don't flush the buffer. This is the default option.
    - **Flush Timeout** field—Enter the threshold in milliseconds to trigger buffer flush drop during congestion. The default value is 500 milliseconds.

- **L2 Interface Policy** tab—Displays the details of the Layer 2 interface policy of the APIC account. To create a Layer 2 interface policy, click **Create** and complete the following fields:
    - Enter a unique name and description for the Layer 2 interface policy.
    - From the **QinQ** drop-down list, choose one of the following options to enable encapsulation:
        - **corePort**—To create an interface policy that enables an interface to be used as a core port in a Dot1q tunnel.
        - **disabled**—To disable Q-in-Q encapsulation.
        - **doubleQtagPort**—To create an interface policy that enables Q-in-Q encapsulation.
        - **edgePort**—To create an interface policy that enables an interface to be used as an edge port in a Dot1q tunnel.
    - From the **Reflective Relay (802.1Qbg)** drop-down list, choose **enabled** to enable reflective relay on a port, port channel, or virtual port channel as a Layer 2 interface policy on the switch. By default, reflective relay is disabled.
    - From the **VLAN Scope** drop-down list, choose **Port Local scope** for the leaf port and **Global scope** for interfaces configured with Multiple Spanning Tree (MST). This field appears only when **corePort**, **disabled**, or **doubleQtagPort** is chosen in the **QinQ** drop-down list.

- **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.

  To view more details about a LLDP interface policy, choose a policy and click **View Details**. The following tab appears:
    - **LLDP Interface Policy Alias**—Displays the names of LLDP interface policy and alias.

- **Port Channel Policy** tab—Displays the port channel member of the APIC accounts. To add a port channel policy, click **Add** and complete the following fields:
    - Enter a unique name and description for the port channel policy.
    - **Mode** drop-down list—Choose a port channel policy mode.
    - **Fast Select Hot Standby Ports** check box—Check this to enable fast select for hot standby ports.
    - **Graceful Convergence** check box—Check this to enable graceful convergence.
    - **Load Defer Member Ports** check box—Check this to enable load defer for member ports.

    - **Suspended Individual Port** check box—Check this to enable suspended individual port.
    - **Symmetric Hashing** check box—Check this to enable symmetric hashing.
    - **Minimum Number of Links** field—Enter the minimum number of links. The valid range is from 1 to 16.
    - **Maximun Number of Links** field—Enter the maximun number of links. The valid range is from 1 to 16.
    - **Alias** field—Enter the alias for the port channel policy.

  To view more details about a port channel policy, choose a policy and click **View Details**. The following tab appears:

    - **Port Channel Policy Alias** tab—Displays the names of port channel policy and alias.

- **Leaf Policy Group** tab—Displays the name and description of the leaf policy group.
- **Monitoring Policy** tab—Displays the monitoring policy details of the APIC account. To create a monitoring policy, click **Add** and enter a unique name and short description for the monitoring policy.
- **Spanning Tree Interface Policy** tab—Displays the spanning tree interface policy details of the APIC account. The spanning tree interface policy dictates the behavior of southbound leaf port Spanning Tree features. To create a spanning tree interface policy, click **Add** and complete the following fields:

    - Enter a unique name and short description for the spanning tree interface policy.
    - Check the **BPDU filter** check box to enable bridge protocol data unit (BPDU) filter on the spanning tree interface policy.
    - Check the **BPDU guard** check box to enable BPDU guard on the spanning tree interface policy.

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

    - **Spanning Tree Interface Policy Alias**—Displays the names of spanning tree interface policy and alias.

- **PC/VPC Leaf Policy** tab—Displays the name, description, and link aggregation type of the PC/VPC leaf policies.

  To create a PC interface leaf policy, click **Create PC Interface Policy Group** or choose **Create PC Interface Policy Group** from the **More Actions** drop-down list. In the **Create PC Interface Policy Group** screen, enter a unique name and short description for the PC interface policy group. Click **Select** and choose the following policies that you want to use in the PC interface policy group: Link Level Policy, CDP Policy, LLDP Policy, Attached Entry Profile, MCP Policy, CoPP Policy, Storm Control Interface Policy, STP Interface Policy, Port-Channel Policy, Monitoring Policy, L2 Interface Policy, Port Security Policy, Egress Data Plane Policing Policy, Ingress Data Plane Policing Policy, Priority Flow Control Policy, Fibre Channel Interface Policy, Slow Drain Policy, and MACsec Policy.

  To create a VPC interface leaf policy, choose **Create VPC Interface Policy Group** from the **More Actions** drop-down list. In the **Create VPC Interface Policy Group** screen, enter a unique name and short description for the VPC interface policy group. Click **Select** and choose the following policies that you want to use in the VPC interface policy group: Link Level Policy, CDP Policy, LLDP Policy, Attached Entry Profile, Port-Channel Policy, MCP Policy, CoPP Policy, Storm Control Interface Policy, L2 Interface Policy, Port Security Policy, Priority Flow Control Policy, STP Interface Policy, Egress Data Plane Policing Policy, Ingress Data Plane Policing Policy, Fibre Channel Interface Policy, Slow Drain Policy, Monitoring Policy, and MACsec Policy.

  To view more details about a PC/VPC leaf policy, choose a PC/VPC leaf policy and click **View Details**. The following tabs appear:

  - **Netflow Monitor Policy**—Displays the netflow monitoring policy and netflow IP filter type associated with the PC/VPC interface policy group. To associate a netflow monitoring policy with the PC/VPC interface policy group, click **Create**. In the screen, choose a **Netflow IP Filter Type** from the drop-down list and click **Select** and choose a netflow monitor policy that needs to be associated with the PC/VPC interface policy group.
  - **VDestination Groups**—Displays the VDestination groups associated with the PC/VPC interface policy group. To associate a VDestination group with the PC/VPC interface policy group, click **Add** and choose a VDestination group.
  - **VSource Groups**—Displays the VSource groups associated with the PC/VPC interface policy group. To associate a VSource group with the PC/VPC interface policy group, click **Add** and choose a VSource group.
  - **Override Policy Groups**—Displays the override policy groups associated with the PC/VPC interface policy group. To create an override policy group, click **Add**. In the **Create Override Policy Group** screen, enter a unique name and short description for the override policy group. Click **Select** and choose a port channel member policy that needs to be associated with the override policy group. Choose an override policy group and click **View Details** to view the PC/VPC interface policy group name, override policy group name, and port channel member policy.

- **Netflow Monitor Policy** tab—Displays the name and description of the NetFlow monitor policy. To add a NetFlow monitor policy, click **Add** and complete the following fields:

  - Enter a unique name and short description for the NetFlow monitor policy.
  - **Associated Flow Record** field—Click **Select** and choose a flow record that needs to be associated with the NetFlow monitoring policy.

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

  - **Flow Record**—Displays the flow record of the NetFlow monitor policy.
  - **NetFlow Exporter**—Displays the NetFlow exporter associated with the fabric NetFlow monitor policy. To associate a NetFlow exporter with a fabric NetFlow monitor policy, click **Add** and choose a NetFlow exporter to be associated with the policy.

- **Flow Record** tab—Displays the name, collect parameters, match parameters, and description of the NetFlow records. A NetFlow record lets you define a flow and the statistics to collect for each flow. You can define match parameters to identify packets in the flow, and define collect parameters that the NetFlow gathers for the flow. To create a flow record, click **Create** and complete the following fields:

  - Enter a unique name and short description for the NetFlow record.
  - **Collect Parameters** field—Click **Select** and choose a list of parameters that need to be collected for a given flow.
  - **Match Parameters** field—Click **Select** and choose a list of parameters that are used by NetFlow to identify packets in the flow.

- **Relay Policy** tab—Displays the name, description, and mode of the relay policy. Click **Add** to add a relay policy.
- **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**.

- **Bridged Outside**—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.

- **Routed Outside**—Displays the tenant, name, and description of the external routed network. Choose a network and click **View Details** to view the following tabs:

  - **Route Map or 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.

- **VRF**—Displays the tenant name, name, description, policy control, and segment of the VRFs. Click **Add** to add a create VRF.
- **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.
- **Set Rules for Route Map**—Displays the set rules for route map of the tenant. Click **Create** to create a set rules for route map. In the **Create Set Rules For A Route Map** dialog box, enter the name and description of the action rule profile. To set action rules, check the required check boxes and fill the additional field that appears on selecting the 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.

    - **L4-L7 Devices**—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.
        - **Cluster Interface**—Displays the list of cluster interfaces in the device cluster. Choose a cluster interface and click **View Details** to view the cluster 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 cluster interface context.

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

  On the **Create Layer 3 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**.

  Choose a layer 3 domain and click **View Details** to view the security domain of the layer 3 domain. Click **Add** to select and associate a security domain to the layer 3 domain.

- **Layer2 Domain** tab—Displays a list of Layer 2 domains in the APIC accounts. To create a Layer 2 domain, click **Create(+)**.

  On the **Create Layer 2 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**.

- **BGP Route Reflector Policy** tab—Displays the BGP route reflector policy configured for the APIC server. To add a BGP route reflector policy, click **Configure** and provide the short description and autonomous system (AS) number for the BGP route reflector policy. Choose the BGP route reflector policy and click **View Details** to the view the following:

  - **Autonomous System Number**—Displays the AS number defined for the BGP route reflector policy.
  - **External Route Reflector Node**—Displays the external route reflector node of the BGP route reflector policy. To add an external route reflector node, click **Add** and complete the following fields:

    - Choose a spine node from the drop-down list. Choose **Enter Customized Value** from the drop-down list, to set any value between 101 and 4001 as the spine node in the **Spine Node** field.
    - Enter a short description for the external route reflector node.
    - Click **Submit**.

  - **Route Reflector Node**—Displays the route reflector node of the BGP route reflector policy. To add a route reflector node, click **Add** and complete the following fields:

    - Choose a spine node from the drop-down list. Choose **Enter Customized Value** from the drop-down list, to set any value between 101 and 4001 as the spine node in the **Spine Node** field.
    - Enter a short description for the route reflector node.
    - 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 tabs appear:

  - **Domains**—Displays a list of VMware domains with the vendor details. To add a new domain, click **Add** and complete the following fields:

    - **Domain Name** field—Enter a unique name for the VMM domain.
    - **Vendor** drop-down list—Choose a vendor of the VMM domain from the drop-down list.
    - **Virtual Switch** drop-down list—Choose a virtual switch from the drop-down list.
    - **Delimiter** field—Enter ~, !, +, @, ^, or | as a delimiter character.
    - **ARP Learning** check box—This field appears only on choosing **Cisco AVS** as the virtual switch. Check this box to enable the ARP learning

- **Enable Tag Collection** check box—Check this box to enable tag collection for the domain.
- **Access Mode**—This field appears only on choosing **VMware vSphere Distributed Switch** as the virtual switch. Choose **Read Only Mode** or **Read Write Mode** as the domain access mode.
- **AVE Time Out Time Interval (seconds)** field—This field appears only on choosing **Cisco AVE** as the virtual switch. Enter a value in the range of 10 to 300 as the AVE time out interval in seconds.
- **Host Availability Assurance** check box—This field appears only on choosing **Cisco AVS** as the virtual switch. Check this box to enable host availability assurance in the domain.
- **Endpoint Retention Time** field—Enter an endpoint retention time in seconds to delay the deletion of an endpoint. The valid range is from 0 to 600.
- **Switching Preference** drop-down list—This field appears only on choosing **Cisco AVS** as the virtual switch. Choose **No Local Switching** or **Local Switching** as the switching preference form the drop-down list.
- **Multicast Address** field—This field appears only on choosing **Cisco AVS** as the virtual switch. Enter a multicast IP address. The valid range is from 224.0.0.0 to 239.255.255.255.
- **Multicast Address Pool** field—This field appears only on choosing **Cisco AVS** as the virtual switch. Click **Select** and choose a multicast address pool that you want to use for the VMM domain.
- **Associated Attachable Entity Profile** field—Click **Select** and choose an attachable access entity profile that needs to be associated with the domain.
- **VLAN Pool** field—This field appears on choosing **VMware vSphere Distributed Switch** or **Cisco AVE** as the virtual switch. Click **Select** and choose a VLAN pool that needs to be associated with the domain.
- **Security Domains** field—Click **Select** and choose one or more security domains that need to be associated with the domain.
- **vCenter Credentials** check box—Check this box to set the credentials for vCenter. On choosing this box, the additional fields appear to provide name, description, user name, and password of the vCenter account profile.
- **Controller Type** drop-down list—Choose **vCenter**, **vShield**, or **None** as the controller type. On choosing **vCenter** or **vShield**, the additional fields appear to provide host name or host IP address, enable statistics collection, choose DVS version, and fields to provide data center, management EPG, and associated credential.
- **Port Channel Mode** drop-down list—Choose a mode for the port channel policy.
- **vSwitch Policy** drop-down list—Choose a vSwitch policy from the drop-down list.
- **BPDU Guard** check box—This field appears on choosing **Cisco AVS** or **Cisco AVE** as the virtual switch. Check this box to enable BPDU guard in the interface policy creation.
- **BPDU Filter** check box—This field appears on choosing **Cisco AVS** or **Cisco AVE** as the virtual switch. Check this box to enable BPDU filter in the interface policy creation.
- **Firewall Mode** drop-down list—This field appears on choosing **Cisco AVS** or **Cisco AVE** as the virtual switch. Choose **Enabled**, **Disabled**, or **Learning** as the firewall mode for the domain.
- **Netflow Exporter Policy** field—Click **Select** and choose a netflow exporter policy that needs to be associated with the domain. On choosing a netflow exporter policy, the additional fields appear to provide active flow timeout, idle flow timeout, and sampling rate.

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. To add an access port selector to the fabric interface profile, click **Add** and complete the following fields in the **Create Access Port Selector** screen:

    - **Name** and **Description** field—Enter a unique name and description for the access port selector.
    - **Interface IDs** field—Enter comma separated interface IDs. You can enter **All** or range of interface IDs.
    - **Interface Description** field—Enter comma separated description for each interface ID.
    - **Connected to FEX** check box—If the port is connected to a Cisco Fabric Extender (FEX), check this check box.
    - **Interface Policy Group** field—Click **Select** and choose an interface policy group that needs to be associated to these ports.

    Choose an access port selector and click **View Details** to view the port blocks and sub port blocks of the access port selector.

- **Fabric Switch Profiles** tab—Displays the fabric switch profiles of the APIC account.

- **Spine Access Port Policy Group** tab—Displays the details of the spine access port policy group of the APIC account. To add a spine access port policy group, click **Add**.

  On the **Create Spine Access Port Policy Group** screen, complete the following fields:

  - **Spine Access Port Policy Group Name** field—Enter a unique name for the spine access port policy group.
  - **Description** field—Enter a short description for the spine access port policy group.
  - **Link Level Policy** field—Click **Select** and check a link level policy that you want to associate with the spine access port policy group.
  - **CDP Policy** field—Click **Select** and check a CDP policy that you want to associate with the spine access port policy group.
  - **MACsec Policy** field—Click **Select** and check a MACsec policy that you want to associate with the spine access port policy group.
  - **Attached Entity Profile** field—Click **Select** and check an attachable access entity profile that you want to associate with the spine access port policy group.
  - Click **Submit**.

- **System** tab—Displays the system details that includes node name, in-band management IP address, out-of-band management IP address, infra IP address, fabric MAC address, ID, role, and serial number.

- **Fabric Memberships** tab—Displays the details of the fabric membership of the APIC account. To create a fabric membership, click **Create** and complete the following fields:

  - **Pod ID** field—Enter a unique identifier of the pod where the node is located.
  - **Serial Number** field—Enter a serial number of the switch.
  - **Node ID** field—Enter a number greater than 100 as node ID, as the first 100 IDs are reserved for APIC appliance nodes.
  - **Switch Name Number** field—Enter the name of the switch added to the pod.
  - **Node Type** field—Choose **leaf** or **spine** as the node type. The default value is **unspecified**.

- **Access Entity Profile** tab—Displays the entity profile details of the APIC server. To add an access entity profile, click **Add** and provide the unique name and description for the access entity profile, enable or disable infrastructure VLAN, and then choose domain profile and interface policy group for the access entity profile.

- **Multicast Address** tab—Displays the multicast address of the APIC server. To add a multicast address, click **Add** and provide a unique name and description for the multicast address.

  Choose a multicast address and click **View Details** to view the range of addresses assigned to the multicast address. To add an address block to the multicast address, click **Add** and enter the starting and ending IP addresses of the multicast address block. The valid range of multicast address is from 224.0.0.0 to 239.255.255.255.

- **Fabric Spine Profile** tab—Displays the fabric spine profile of the APIC server. To add a fabric spine profile, click **Add** and provide a unique name and description for the fabric spine profile.

- **Fabric TEP Pool Physical Pod** tab—Displays the fabric TEP pool physical pod of the APIC server. To add a fabric TEP pool physical or virtual pod, click **Add** and complete the following fields:

  - **Pod ID**—Enter defaultValue or a number in the range of 1 to 254 as the pod ID. The default value is 1.

  - **TEP Pool**—Enter an IPv4 address with mask as the Tunnel Endpoint (TEP) pool for the pod. For physical pod, the mask must be in the range of 1 to 23. For virtual pod, the mask must be in the range of 22 to 28.
  - **Pod Type**—Choose **physical** or **virtual** as the pod type. The default value is **physical**.

- **Fabric TEP Pool Virtual Pod** tab—Displays the fabric TEP pool virtual pod of the APIC server.

  To view more details about the fabric TEP pool virtual pod, choose a fabric TEP pool virtual pod and click **View Details**. The following tabs appear:

  - **Fabric TEP Pool Virtual Pod Properties**—Displays the virtual pod ID, pod type, reserved address and gateway address of the fabric TEP pool virtual pod.
  - **Additional Subnets**—Displays the associated subnets of the fabric TEP pool virtual pod. To add an additional subnet to fabric virtual pod TEP pool, click **Add** and complete the following fields:
    - **Network Address** field—Enter a valid IPv4 address with subnet mask as the network address for the subnet of fabric virtual pod. The valid format is IPv4/subnet mask. The valid range of subnet mask is from 22 to 28.
    - **Reserved Subnet** field—The pool consists of IP addresses that are not sent by the DHCP server and which you can reserve for a specific use. Enter a valid IPv4 address with subnet mask as the reserved subnet. The valid format is IPv4/subnet mask. The value of subnet mask must be greater than the subnet mask of TEP pool by two.
    - **Gateway IP Address** field—Enter a valid IPv4 address as the gateway IP address of the subnet.

    Choose an additional subnet and click **View Details** to view the properties of the additional subnet.
  - **DHCP Servers**—Displays the DHCP servers of the fabric TEP pool virtual pod. To add a DHCP server, click **Add** and complete the following fields:
    - **Node ID** field—Enter a unique node ID for the DHCP server. The valid range of node ID is from 101 to 4000.
    - **Type** drop-down list—Choose **Primary** or **Secondary** as the DHCP server type.

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