



## Configuring APIC Accounts

---

- [Guidelines for APIC Accounts, page 1](#)
- [Support for In-Band and Out-of-Band Management, page 2](#)
- [Adding an APIC Account, page 3](#)
- [Viewing APIC Resources, page 4](#)
- [Assigning an APIC Account to a Pod, page 9](#)
- [Handling APIC Failover, page 10](#)

## 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.

- **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.

- **CDP Interface Policy** tab—Displays the name and description of the Cisco Discovery Protocol (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 contract, 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—Expand **Associated Attachable Entity Profile** and check an attachable access entry profile that you want to associate with the Layer 3 domain.
  - **VLAN Pool** field—Expand **VLAN Pool** 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—Expand **Associated Attachable Entity Profile** and check an attachable access entry profile that you want to associate with the Layer 2 domain.
  - **VLAN Pool** field—Expand **VLAN Pool** 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.
  - **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** Expand **Pod** 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.