Initial Setup

This chapter contains the following sections:

Cisco APIC Documentation Roadmap

This table provides a list of additional documents that are useful references along with the *Cisco APIC Getting Started Guide*. All Cisco APIC documents are available at the APIC documents landing page.

Document
Application Centric Infrastructure Fabric Hardware Installation Guide
Cisco APIC Management, Installation, Upgrade, and Downgrade Guide
Cisco APIC Basic Configuration Guide
Cisco APIC Layer 2 Networking Configuration Guide
Cisco APIC Layer 3 Networking Configuration Guide
Cisco ACI Virtualization Guide

Document
Cisco Application Centric Infrastructure Fundamentals
Cisco APIC Layer 4 to Layer 7 Services Deployment Guide

Simplified Approach to Configuring in Cisco APIC

Cisco APIC supports a simplified approach to configuring the ACI with the choice of two additional user interfaces. They are the NX-OS style CLI and the Basic GUI. The existing methods of configuration using REST API and Advanced GUI are supported as well. The Advanced GUI is equivalent to the GUI of the previous releases. Cisco recommends that you use the Advanced GUI to manage any policy that you created in Release 1.2 or earlier releases.

In addition to the simple approach available for network administrators and other users of the NX-OS style CLI and the Basic GUI, there is intelligence embedded in these approaches as compared to the Advanced GUI or the REST API. In several instances, the NX-OS style CLI and the Basic GUI often create the ACI model constructs implicitly for a user's ease of use, and they also provide validations to ensure consistency in configuration. This functionality reduces and prevents faults.

Configurations using NX-OS style CLI and Basic GUI are compatible similar to the compatibility between existing methods of configuration using Advanced GUI and REST API. For further details about configurations and tasks, see the *Cisco APIC Basic Configuration Guide* and the *Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*.

Changing the BIOS Default Password

The APIC controller ships with a default BIOS password. The default password is 'password'. When the boot process starts, the boot screen displays the BIOS information on the console server.

To change the default BIOS password perform the following task:

Step 1 During the BIOS boot process, when the screen displays **Press <F2> Setup**, press **F2**.
The **Entering Setup** message displays as it accesses the setup menu.

Step 2 At the **Enter Password** dialog box, enter the current password.
Note The default is 'password'.

Step 3 In the **Setup Utility**, choose the **Security** tab, and choose **Set Administrator Password**.

Step 4 In the **Enter Current Password** dialog box, enter the current password.

Step 5 In the **Create New Password** dialog box, enter the new password.

Step 6 In the **Confirm New Password** dialog box, re-enter the new password.

Step 7 Choose the **Save & Exit** tab.

Step 8 In the **Save & Exit Setup** dialog box, choose **Yes**.

Step 9 Wait for the reboot process to complete.

The updated BIOS password is effective.

About the APIC

The Cisco Application Centric Infrastructure (ACI) is a distributed, scalable, multitenant infrastructure with external end-point connectivity controlled and grouped through application-centric policies. The Application Policy Infrastructure Controller (APIC) is the unified point of automation, management, monitoring, and programmability for the ACI. The APIC supports the deployment, management, and monitoring of any application anywhere, with a unified operations model for the physical and virtual components of the infrastructure. The APIC programmatically automates network provisioning and control that is based on the application requirements and policies. It is the central control engine for the broader cloud network; it simplifies management and allows flexibility in how application networks are defined and automated. It also provides northbound Representational State Transfer (REST) APIs. The APIC is a distributed system that is implemented as a cluster of many controller instances.

Setting up the APIC

When the APIC is launched for the first time, the APIC console presents a series of initial setup options. For many options, you can press Enter to choose the default setting that is displayed in brackets. At any point in the setup dialog, you can restart the dialog from the beginning by pressing Ctrl-C.

Important Notes

- If the UNIX user ID is not explicitly specified in the response from the remote authentication server, then some APIC software releases assign a default ID of 23999 to all users. If the response from the remote authentication server fails to specify a UNIX ID, all users will share the same ID of 23999 and this can result in the users being granted higher or lower privileges than the configured privileges through the RBAC policies on the APIC.
- Cisco recommends that you assign unique UNIX user IDs in the range of 16000 to 23999 for the AV Pairs that are assigned to the users when in Bash shell (using SSH, Telnet, or Serial/KVM consoles). If a situation arises where the Cisco AV Pair does not provide a UNIX user ID, the user is assigned a user ID of 23999 or similar number from the range that also enables the user's home directories, files, and processes accessible to the remote users with a UNIX ID of 23999.

  To ensure that your remote authentication server does not explicitly assign a UNIX ID in its **cisco-av-pair** response, open an SSH session to the APIC and log in as an administrator (using a remote user account). Once logged in, run the following commands (replace **userid** with the username that you logged in with):

  - **admin@apic1: remoteuser-userid> cd /mit/uni/userext/remoteuser-userid**
  - **admin@apic1: remoteuser-userid> cat summary**

- If you are using a Cisco Integrated Management Controller (CIMC) for your setup, use only the port-side utility console port with the breakout cable. Setup the CIMC first, and then access the APIC through the CIMC KVM or continue to access the APIC locally through the port-side utility console port. Do

not use the RJ-45 console port, unless access to the port side is restricted. If you choose the CIMC KVM access, you will have remote access available later which is required during operations.

- If you are using RJ-45 console port, connect to CIMC using SSH and enable the Serial over LAN port using the following parameters:
  - Scope SOL sol
  - Set Enabled to Yes
  - Commit
  - Exit

  After enabling, enter the command **connect host** to access the console. If the serial port is connected, either disconnect the serial port or ensure that the connected device has the proper configuration.
- It is recommended not to modify any parameters using CIMC. If there are any issues, ensure that the default setting for CIMC management node is **Dedicated Mode** and not **Shared**. If **Dedicated Mode** is not used, it can prevent the discovery of fabric nodes.
- Do not upgrade software or firmware using the CIMC user interface, XML, or SSH interfaces unless the modified property and software or firmware version are supported with your specific APIC version.
- Set the NIC mode to Dedicated, when setting up the CIMC, in the CIMC Configuration Utility. After the CIMC is configured, in the CIMC GUI, verify that you have the following parameters set.

Parameters	Settings
LLDP	Disabled on the VIC
TPM Support	Enabled on the BIOS
TPM Enabled Status	Enabled
TPM Ownership	Owned

- Starting with APIC release 1.2(2x), during the initial setup the system will prompt you to select IPv4, or IPv6, or dual stack configuration. Choosing dual stack will enable accessing the APIC and ACI fabric out-of-band management interfaces with either IPv4 or IPv6 addresses. While the examples in the table below use IPv4 addresses, you can use whatever IP address configuration options you chose to enable during the initial setup.
- A minimum subnet mask of /19 is recommended.
- Connecting the APIC (the controller cluster) to the ACI fabric requires a 10G interface on the ACI-mode leaf switch. You cannot connect the APIC directly to the Cisco Nexus 9332PQ or the Cisco Nexus 93180LC ACI-mode leaf switches unless you use a 40G to 10G converter (part number CVR-QSFP-SFP10G), in which case the port on the Cisco Nexus 9332PQ or the Cisco Nexus 93180LC ACI-mode leaf switches will auto-negotiate to 10G without requiring any manual configuration.

Note Starting with Cisco APIC release 2.2(1n), the Cisco Nexus 93180LC leaf switch is supported.

- The fabric ID is set during the APIC controller setup and it cannot be changed unless you perform a clean reload of the fabric. To change the fabric ID, perform a clean reload on the APIC and leaf switches after changing the `sam.config` file. All APICs in a cluster must have the same fabric ID.

About Cold Standby for APIC Cluster

The Cold Standby functionality for an APIC cluster enables you to operate the APICs in a cluster in an active/standby mode. In an APIC cluster, the designated active APICs share the load and the designated standby APICs can act as an replacement for any of the APICs in an active cluster.

An admin user can set up the Cold Standby functionality when the APIC is launched for the first time. It is recommended that you have at least 3 active APICs in a cluster, and one or more standby APICs. An admin user will have to initiate the switch over to replace an active APIC with a standby APIC. See the *Cisco APIC Management, Installation, Upgrade, and Downgrade Guide* for more information.

Setup for Active and Standby APIC

Table 1: Setup for Active APIC

Name	Description	Default Value
Fabric name	Fabric domain name	ACI Fabric1
Fabric ID	Fabric ID	1
Number of active controllers	Cluster size	3 **Note** When setting up APIC in an active-standby mode, you must have at least 3 active APICs in a cluster.
POD ID	POD ID	1
Standby controller	Setup standby controller	NO
Controller ID	Unique ID number for the active APIC instance.	Valid range: 1-19
Controller name	Active controller name	apic1

Name	Description	Default Value
IP address pool for tunnel endpoint addresses	Tunnel endpoint address pool	10.0.0.0/16 This value is for the infrastructure virtual routing and forwarding (VRF) only. This subnet should not overlap with any other routed subnets in your network. If this subnet does overlap with another subnet, change this subnet to a different /16 subnet. The minimum supported subnet for a 3 APIC cluster is /23. If you are using Release 2.0(1) the minimum is /22.
VLAN ID for infrastructure network[1]	Infrastructure VLAN for APIC-to-switch communication including virtual switches **Note** Reserve this VLAN for APIC use only. The infrastructure VLAN ID must not be used elsewhere in your environment and must not overlap with any other reserved VLANs on other platforms.	--
IP address pool for bridge domain multicast address (GIPo)	IP addresses used for fabric multicast . For Cisco APIC in a Cisco ACI Multi-Site topology, this GIPo address can be the same across sites.	225.0.0.0/15 Valid range: 225.0.0.0/15 to 231.254.0.0/15, prefixlen must be 15 (128k IPs)
IPv4/IPv6 addresses for the out-of-band management	IP address that you use to access the APIC through the GUI, CLI, or API. This address must be a reserved address from the VRF of a customer	—
IPv4/IPv6 addresses of the default gateway	Gateway address for communication to external networks using out-of-band management	—

Name	Description	Default Value
Management interface speed/duplex mode	Interface speed and duplex mode for the out-of-band management interface	auto Valid values are as follows • auto • 10baseT/Half • 10baseT/Full • 100baseT/Half • 100baseT/Full • 1000baseT/Full
Strong password check	Check for a strong password	[Y]
Password	Password of the system administrator This password must be at least 8 characters with one special character.	—

[1] To change the VLAN ID after the initial APIC setup, export your configurations, rebuild the fabric with a new infrastructure VLAN ID and import the configurations so that the fabric does not revert to the old infrastructure VLAN ID. See the KB article about *Using Export and Import to Recover Configuration State*.

Table 2: Setup for Standby APIC

Name	Description	Default Value
Fabric name	Fabric domain name	ACI Fabric1
Fabric ID	Fabric ID	1
Number of active controllers	Cluster size	3 **Note** When setting up APIC in an active-standby mode, you must have at least 3 active APICs in a cluster.
POD ID	ID of the POD	1
Standby controller	Setup standby controller	Yes
Standby Controller ID	Unique ID number for the standby APIC instance .	Recommended range: >20
Controller name	Standby controller name	NA

Name	Description	Default Value
IP address pool for tunnel endpoint addresses	Tunnel endpoint address pool	10.0.0.0/16 This value is for the infrastructure virtual routing and forwarding (VRF) only. This subnet should not overlap with any other routed subnets in your network. If this subnet does overlap with another subnet, change this subnet to a different /16 subnet. The minimum supported subnet for a 3 APIC cluster is /23. If you are using Release 2.0(1) the minimum is /22.
VLAN ID for infrastructure network[2]	Infrastructure VLAN for APIC-to-switch communication including virtual switches **Note** Reserve this VLAN for APIC use only. The infrastructure VLAN ID must not be used elsewhere in your environment and must not overlap with any other reserved VLANs on other platforms.	--
IPv4/IPv6 addresses for the out-of-band management	IP address that you use to access the APIC through the GUI, CLI, or API. This address must be a reserved address from the VRF of a customer	—
IPv4/IPv6 addresses of the default gateway	Gateway address for communication to external networks using out-of-band management	—

Name	Description	Default Value
Management interface speed/duplex mode	Interface speed and duplex mode for the out-of-band management interface	auto Valid values are as follows • auto • 10baseT/Half • 10baseT/Full • 100baseT/Half • 100baseT/Full • 1000baseT/Full
Strong password check	Check for a strong password	[Y]
Password	Password of the system administrator This password must be at least 8 characters with one special character.	—

2 To change the VLAN ID after the initial APIC setup, export your configurations, rebuild the fabric with a new infrastructure VLAN ID and import the configurations so that the fabric does not revert to the old infrastructure VLAN ID. See the KB article about *Using Export and Import to Recover Configuration State*.

Example

The following is a sample of the initial setup dialog as displayed on the console:

```
Cluster configuration ...
  Enter the fabric name [ACI Fabric1]:
  Enter the fabric ID (1-128) [1]:
  Enter the number of active controllers in the fabric (1-9) [3]:
  Enter the POD ID (1-9) [1]:
  Is this a standby controller? [NO]:
  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]: sec-ifc5
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (2-4094): 4093
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]:
  Enter the IPv4 address [192.168.10.1/24]: 172.23.142.29/21
  Enter the IPv4 address of the default gateway [None]: 172.23.136.1
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:

  Reenter the password for admin:

Cluster configuration ...
  Fabric name: ACI Fabric1
  Fabric ID: 1
```

```
  Number of controllers: 3
  Controller name: sec-ifc5
  POD ID: 1
  Controller ID: 1
  TEP address pool: 10.0.0.0/16
  Infra VLAN ID: 4093
  Multicast address pool: 225.0.0.0/15

Out-of-band management configuration ...
  Management IP address: 172.23.142.29/21
  Default gateway: 172.23.136.1
  Interface speed/duplex mode: auto

admin user configuration ...
  Strong Passwords: Y
  User name: admin
  Password: ********

The above configuration will be applied ...

Warning: TEP address pool, Infra VLAN ID and Multicast address pool
         cannot be changed later, these are permanent until the
         fabric is wiped.

Would you like to edit the configuration? (y/n) [n]:
```

Provisioning IPv6 Management Addresses on APIC Controllers

IPv6 management addresses can be provisioned on the APIC controller at setup time or through a policy once the APIC controller is operational. Pure IPv4, Pure IPv6 or dual stack (i.e both IPv6 and IPv4 addresses) are supported. The following snippet is of a typical setup screen that describes how to setup dual stack (IPv6 and IPv4) addresses for out-of-band management interfaces during the setup:

```
Cluster configuration …

  Enter the fabric name [ACI Fabric1]:
  Enter the number of controllers in the fabric (1-9) [3]:
  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]: infraipv6-ifc1
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (1-4094): 4093
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]: Y (Enter Y to Configure IPv6 Address for
 Out of Band Management Address)
  Enter the IPv6 address [0:0:0:0:0:ffff:c0a8:a01/40]: 2001:420:28e:2020:0:ffff:ac1f:88e4/64
 (IPv6 Address)
  Enter the IPv6 address of the default gateway  [None]: 2001:420:28e:2020:acc:68ff:fe28:b540
 (IPv6 Gateway)
  Enable IPv4 also for Out of Band Mgmt Interface? [Y]: (Enter Y to Configure IPv4 Address
 for Out of Band Management Address)
  Enter the IPv4 address [192.168.10.1/24]: 172.31.136.228/21 (IPv4 Address)
  Enter the IPv4 address of the default gateway [None]: 172.31.136.1 (IPv4 Gateway)
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:

  Reenter the password for admin:
```

Accessing the GUI

Step 1 Open one of the supported browsers:

- Chrome version 59 (at minimum)
- Firefox version 54 (at minimum)
- Internet Explorer version 11 (at minimum)
- Safari version 10 (at minimum)

Note A known issue exists with the Safari browser and unsigned certificates. Read the information presented here before accepting an unsigned certificate for use with WebSockets. When you access the HTTPS site, the following message appears:

"Safari can't verify the identity of the website APIC. The certificate for this website is invalid. You might be connecting to a website that is pretending to be an APIC, which could put your confidential information at risk. Would you like to connect to the website anyway?"

To ensure that WebSockets can connect, you must do the following:

Click **Show Certificate**.

Choose **Always Trust** in the three drop-down lists that appear.

If you do not follow these steps, WebSockets will not be able to connect.

Step 2 Enter the URL: **https://***mgmt_ip-address*
Use the out-of-band management IP address that you configured during the initial setup. For example, https://192.168.10.1.

Note Only https is enabled by default. By default, http and http-to-https redirection are disabled.

Step 3 When the login screen appears, enter the administrator name and password that you configured during the initial setup.

Step 4 In the **Domain** field, from the drop-down list, choose the appropriate domain that is defined.
If multiple login domains are defined, the **Domain** field is displayed. If the user does not choose a domain, the DefaultAuth login domain is used for authentication by default. This may result in login failure if the username is not in the DefaultAuth login domain.

Step 5 In the **Mode** field, from the drop-down list, choose the **Advanced** or the **Basic** mode as desired.

What to Do Next

To learn about the features and operation of the Application Centric Infrastructure fabric and the Application Policy Infrastructure Controller, see the available white papers and the *Cisco Application Centric Infrastructure Fundamentals Guide*.

Accessing the REST API

By using a script or a browser-based REST client, you can send an API POST or GET message of the form:
https://*apic-ip-address*/**api/***api-message-url*
Use the out-of-band management IP address that you configured during the initial setup.

Note
- Only https is enabled by default. By default, http and http-to-https redirection are disabled.
- You must send an authentication message to initiate an API session. Use the administrator login name and password that you configured during the initial setup.

Accessing the Object Model CLI

Note From Cisco APIC Release 1.0 until Release 1.2, the default CLI was a Bash shell with commands to directly operate on managed objects (MOs) and properties of the Management Information Model. Beginning with Cisco APIC Release 1.2, the default CLI is a NX-OS style CLI. The object model CLI is available by typing the **bash** command at the initial CLI prompt.

Step 1 From a secure shell (SSH) client, open an SSH connection to *username@ip-address*.
Use the administrator login name and the out-of-band management IP address that you configured during the initial setup. For example, `ssh admin@192.168.10.1`.

Step 2 When prompted, enter the administrator password that you configured during the initial setup.
With Cisco APIC Releases 1.0 and 1.1, you are now in the object model CLI. With Cisco APIC Release 1.2, you are now in the NX-OS style CLI for APIC.

Step 3 With Cisco APIC Release 1.2, type **bash** to enter the object model CLI.
This example shows how to enter the object model CLI and how to return to the NX-OS style CLI:

```
$ ssh admin@192.168.10.1
Application Policy Infrastructure Controller
admin@192.168.10.1's password: cisco123
apic#             <---- NX-OS style CLI prompt
apic# bash
admin@apic1:~>    <---- object model CLI prompt
admin@apic1:~> exit
apic#
```

What to Do Next

Every user must use the shared directory called `/home`. This directory gives permissions for a user to create directories and files; files created within `/home` inherit the default umask permissions and are accessible by the user and by root. We recommend that users create a `/home/userid` directory to store files, such as `/home/jsmith`, when logging in for the first time.

For more information about accessing switches using the ACI CLI using modes of operation such as BASH or VSH, see the *Cisco APIC Command Line Interface User Guide* and the *Cisco ACI Switch Command Reference*.

For detailed information about configuring the APIC CLI, see the *Cisco APIC Object Model Command Line Interface User Guide*.

Accessing the NX-OS Style CLI

Note From Cisco APIC Release 1.0 until Release 1.2, the default CLI was a Bash shell with commands to directly operate on managed objects (MOs) and properties of the Management Information Model. Beginning with Cisco APIC Release 1.2, the default CLI is a NX-OS style CLI. The object model CLI is available by typing the **bash** command at the initial CLI prompt.

Step 1 From a secure shell (SSH) client, open an SSH connection to APIC at *username@ip-address*.
Use the administrator login name and the out-of-band management IP address that you configured during the initial setup. For example, admin@192.168.10.1.

Step 2 When prompted, enter the administrator password.

What to Do Next

When you enter the NX-OS style CLI, the initial command level is the EXEC level. From this level, you can reach these configuration modes:

- To continue in the NX-OS style CLI, you can stay in EXEC mode or you can type **configure** to enter global configuration mode.

  For information about NX-OS style CLI commands, see the *Cisco APIC NX-OS Style CLI Command Reference*.

- To reach the object model CLI, type **bash**.

  For information about object mode CLI commands, see the *Cisco APIC Command-Line Interface User Guide, APIC Releases 1.0 and 1.1*.