Cisco ACI Simulator Getting Started Guide, Release 2.x

First Published: August 29, 2016

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

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Virtual machine installation and administration
- Server administration
- Switch and network administration

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).

Convention	Description
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco Application Centric Infrastructure (ACI) Documentation

The ACI documentation is available at the following URL: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Cisco Application Centric Infrastructure (ACI) Simulator Documentation

The Cisco ACI Simulator documentation is available at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html.

Cisco Nexus 9000 Series Switches Documentation

The Cisco Nexus 9000 Series Switches documentation is available at http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html.

Cisco Application Virtual Switch Documentation

The Cisco Application Virtual Switch (AVS) documentation is available at http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html.

Cisco Application Centric Infrastructure (ACI) Integration with OpenStack Documentation

Cisco ACI integration with OpenStack documentation is available at http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

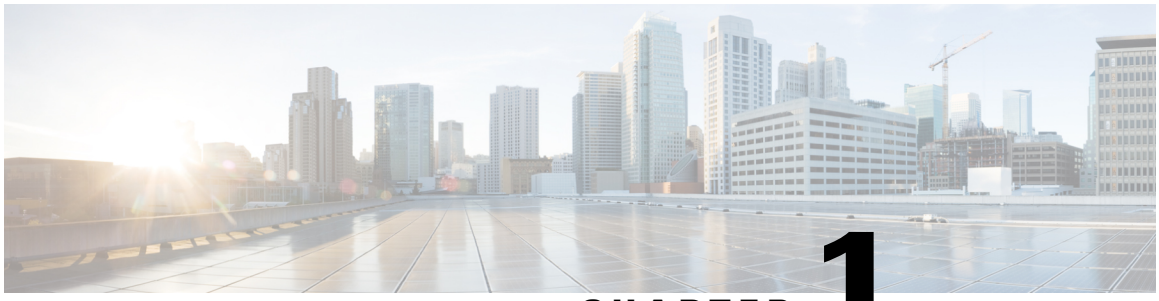
Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



CHAPTER 1

New and Changed Information

This chapter contains the following sections:

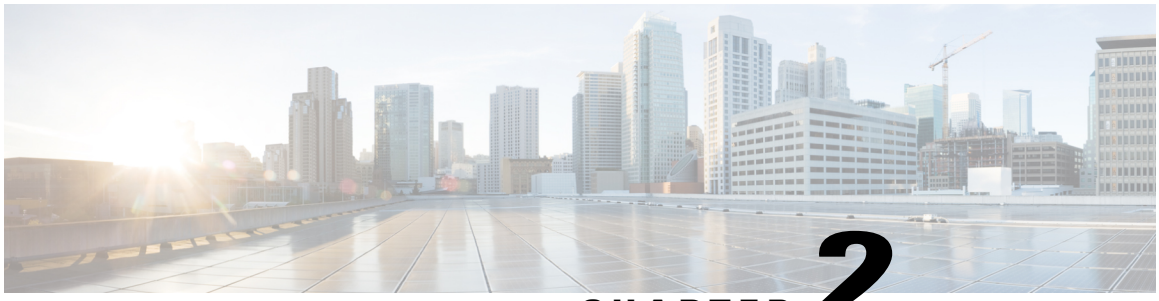
New and Changed Information

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

Table 1: New Features and Changed Behavior in the Cisco ACI Simulator

Cisco APIC Release Version	Feature	Description	Where Documented
Release 2.0(2f)	No significant update in this release.		
Release 2.0(1m)	--	This guide was reorganized for this release. The GUI, REST API, and CLI tasks that were in this guide for earlier releases are now available in the *Cisco APIC Basic Configuration Guide*.	--

New and Changed Information



CHAPTER 2

Initial POD Setup and Overview

This chapter contains the following sections:

First-Time Access

Getting Started Guide Contents

The Cisco ACI Simulator Getting Started Guide contains the following information:

- Setting up an initial pod environment
- Setting up a multipod environment

For detailed information about configuring, see the *Cisco APIC Basic Configuration Guide*. The APIC Basic Configuration Guide is written for users of Cisco APIC with leaf and spine switch configurations. The ACI simulator user can refer to the same guide with the caveat that The ACI Simulator includes simulated switches, so you cannot validate a data path.

For installation information, see the *Cisco ACI Simulator Installation 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*.

About the ACI Simulator

The ACI simulator provides real, fully-featured APIC controller software, along with a simulated fabric infrastructure of leaf switches and spine switches in one physical server. The physical server is a UCS C-series server.

The APIC controller software controls a set of five software-simulated ACI switches connected in a fabric topology. This allows the customer to explore the APIC GUI and to create configurations in the simulated fabric. Because the simulator can also be configured using the CLI or the REST API, it allows partners and customers to develop scripts and applications prior to investing in and purchasing the actual ACI switches.

Guidelines and Restrictions When Using the ACI Simulator

For details about the ACI simulator topology and connections, see the *Cisco ACI Simulator Installation Guide*.

When using the ACI simulator, the following guidelines and restrictions must be considered:

- The ACI simulator GUI includes an online version under Quick Start that includes video demonstrations.
- Do not change the following:
  - The default names in the initial setup for node names and the cluster configuration.
  - The cluster size and the number of APIC nodes.
  - The infra VLAN.
- The ACI simulator uses NAT for inband management. Inband IP addresses configured by policy are not used. Instead, APIC and node inband IP addresses are internally allocated.
- The ACI simulator does not support the following:
  - Configuring a DHCP server policy.
  - Configuring a DNS service policy.
  - Data path forwarding because the simulator includes simulated switches.
  - Cisco Discovery Protocol (CDP) between a leaf switch and a hypervisor or between a leaf switch and an unmanaged/Layer 2 switch. Only Link Layer Discovery Protocol (LLDP) is supported in these cases .
  - Configuring out-of-band management access for switches.
- APIC out-of-band management IP/gateway cannot be modified using an out-of-band management policy and can be configured only during the APIC first-time setup screen.
- Keep the vMotion PNIC outside the simulator network.

- The infrastructure EPG in the infrastructure tenant is for internal use only.
- The MP-BGP route reflector and the OSPF external routed network protocols do not work if you are using the simulator.
- Virtual shell (VSH) and ishell commands do not work on switches. These commands are implemented on the Cisco NX-OS software, and the Cisco NX-OS software is not available on the simulator.
- Statistics are simulated. As a result, threshold crossing alert (TCA) faults are generated in the simulator to demonstrate the fault generation on the statistics threshold crossing.
- Create a syslog and Call Home source policy under **common policy**. This policy applies at the system level and sends all syslog and Call Home messages system wide. The GUI path to create syslog and Call Home under **common policy** are as follows: Admin / External Data Collector/ Monitoring Destinations / [Callhome | SNMP | Syslog].
- The Cisco ACI simulator simulates faults for counters, which can cause the health score of the top-of-rack (TOR) switch to go down. The faults look like the following:

```
<faultInst ack="no" cause="threshold-crossed" changeSet="" childAction="" code="F54431"

created="2014-01-21T17:20:13.179+00:00" descr="TCA: l2IngrBytes5min dropRate value
9049.94 raised
above threshold 9000 and value is recovering "dn="topology/pod-1/node-17/sys/
ctx-[vxlan-2621440]/bd-[vxlan-15826914]/vlan-[vlan- 1031]/fault-F54431" domain="infra"

highestSeverity="minor" lastTransition="2014-01-21T17:22:35.185+00:00" lc="raised"
modTs="never"
occur="1"origSeverity="minor" prevSeverity="minor" rule="tca-l2-ingr-bytes-drop-rate"

severity="minor" status="" subject="counter" type="operational"/> <faultInst ack="no"

cause="threshold-crossed" changeSet="" childAction="" code="F54447"
created="2014-01-21T17:20:13.244+00:00" descr="TCA: l2IngrPkts5min dropRate
value 3.53333 raised above threshold 10" dn="topology/pod-1/node-17
/sys/ctx-[vxlan-2621440]/bd-[vxlan-15826914]/vlan-[vlan-1 031]/fault-F54447"
domain="infra" highestSeverity="warning" lastTransition="2014-01-21T19:42:37.983+00:00"

lc="retaining" modTs="never" occur="9" origSeverity="warning"prevSeverity="warning"
rule="tca-l2-ingr-pkts-drop-rate" severity="cleared" status="" subject="counter"
type="operational"/>
```

- You can test L4-L7 services by connecting your service appliance using in-band management connectivity between the simulator and the appliance.

  For more details about L4-L7 services guidelines when using the simulator, see the guidelines section in the *Cisco ACI Simulator Release Notes*.

Installing the Cisco Application Centric Infrastructure Fabric Hardware

For details about installing the ACI fabric hardware, see the *Application Centric Infrastructure Fabric Hardware Installation Guide*.

Changing the BIOS Default Password

The ACI simulator 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.

Note

- 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 fan-side 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.
- Do not modify any parameters using CIMC. 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.

Name	Description	Default Value
Fabric name	Fabric domain name	ACI Fabric1
Number of controllers	Cluster size	3
Controller ID	Unique ID number for the APIC instance	1, 2, or 3
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. Default value. Do not change. Do not set up your host on the network 10.0.0.0/8.

Name	Description	Default Value
IP address pool for bridge domain multicast address (GIPO)	IP addresses used for fabric multicast	225.0.0.0/15 Valid range: 225.0.0.0/15 to 231.254.0.0/15, prefixlen must be 15 (128k IPs) Default value. Do not change.
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 **Note** Do not change values
VLAN ID for infrastructure network	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.	4 Default value. Do not change.
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	—
Strong password check	Check for a strong password	[Y]

Name	Description	Default Value
Password	Password of the system administrator This password must be at least 8 characters with one special character.	—

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

```
Cluster configuration ...
  Enter the fabric name [ACI Fabric1 #1]:
  Enter the number of controllers in the fabric (1-16) [3]:
  Enter the controller ID (1-3) [2]:
  Enter the controller name [apic2]:
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Enter the VLAN ID for infra network (1-4)[4]: <<< This is for the simulator APIC
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enter the IP address for out-of-band management: 192.168.10.2/24
  Enter the IP address of the default gateway [None]: 192.168.10.254
  Enter the interface speed/duplex mode [auto]:

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

Note

- It can take a few minutes to login as an administrator.
- Until the entire cluster boots up, you cannot log in to apic2 and apic3.

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 35 (at minimum)
- Firefox version 26 (at minimum)
- Internet Explorer version 11 (at minimum)
- Safari version 7.0.3 (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://*ip-address of APIC*/**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.

What to Do Next

For detailed information about configuring the APIC REST API, see the *Cisco APIC REST API User Guide*.

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*.

Overview of the GUI

The APIC GUI is a browser-based graphical interface to the APIC that communicates internally with the APIC engine by exchanging REST API messages. The GUI contains several areas and panes.

Deployment Warning and Policy Usage Information

When you first log in to the APIC GUI, the **Deployment Warning Settings** dialog box opens allowing you to enable and alter the scope of deployment notification that displays policy usage information. The deployment warning settings can also be accessed from the **welcome, <login_name>** drop-down list (Change Deployment Settings) and through a button on the **Policy Usage Information** dialog box.

The policy usage information allows users to identify which resources and policies are being used by the policy that the user is currently modifying or deleting. The tables display the nodes where the given policy is used and other policies that use this policy. By default, usage information is displayed within a dialog box whenever the user attempts to modify a policy. Also, at any time, you can click the **Show Usage** button at the bottom of the screen to view the same information.

Toggling Between Basic and Advanced GUI Modes

When logged in to the APIC GUI, you can verify the GUI mode you are in. The mode you have entered is displayed in the top right corner of the GUI. You can choose to operate in one of two modes:

Caution: Cisco recommends that you do not mix configuration modes (Advanced or Basic). When you make a configuration in either mode and change the configuration using the other mode, unintended changes can occur. For example, if you apply an interface policy to two ports using Advanced mode and then change the settings of one port using Basic mode, your changes might be applied to both ports.

- Basic Mode—For information about tasks that you perform in Basic Mode, see the chapter,*Getting Started with APIC Using the Basic GUI*.
- Advanced Mode—For information about tasks that you perform in Advanced Mode, see the chapter,*Getting Started with APIC Using the Advanced GUI*.

You can also change from one GUI mode to another or toggle between modes as follows:

1. In the GUI, click the **welcome, <login_name>** drop-down list and choose Toggle GUI Mode.
2. In the **Warning** dialog box, click Yes for
3. Wait for the application to complete loading and display the GUI in the changed mode.

Menu Bar and Submenu Bar

The menu bar and the submenu bar contain the following items:

The menu bar is displayed across the top of the APIC GUI (see the following figure). It provides access to the main tabs.

Figure 1: APIC GUI Menu Bar

You can navigate to the submenu bar (see the following figure) by clicking on one of the tabs in the menu bar. When you click on a menu bar tab, the submenu bar for that tab is displayed. The submenu bar is different for each menu bar tab and might also differ depending upon your specific configurations.

Figure 2: APIC GUI Submenu Bar

SYSTEM Tab

Use the **SYSTEM** tab to collect and display a summary of the overall system health, its history, and a table of system-level faults.

TENANTS Tab

Use the **Tenants** tab in the menu bar to perform tenant management. In the submenu bar, you see an **Add Tenant** link, and a drop-down list that contains all the tenants. Up to five of the most recently used tenants are also displayed on the submenu bar.

- A tenant contains policies that enable qualified users domain-based access control. Qualified users can access privileges such as tenant administration and networking administration.
- A user requires read/write privileges for accessing and configuring policies in a domain. A tenant user can have specific privileges into one or more domains.
- In a multitenancy environment, a tenant provides group user access privileges so that resources are isolated from one another (such as for endpoint groups and networking). These privileges also enable different users to manage different tenants.

FABRIC Tab

The **FABRIC** tab contains the following tabs in the submenu bar:

- **INVENTORY** tab—Displays the individual components of the fabric.
- **FABRIC POLICIES** tab—Displays the monitoring and troubleshooting policies and fabric protocol settings or fabric maximum transmission unit (MTU) settings.
- **ACCESS POLICIES** tab—Displays the access policies that apply to the edge ports of the system. These ports are on the leaf switches that communicate externally.

VM NETWORKING Tab

Use the **VM NETWORKING** tab to view and configure the inventory of the various virtual machine (VM) managers. You can configure and create various management domains under which connections to individual management systems (such as VMware vCenters or VMware vShield) can be configured. Use the **INVENTORY** tab in the submenu bar to view the hypervisors and VMs that are managed by these VM management systems (also referred to as controllers in API).

L4-L7 SERVICES Tab

Use the **L4-L7 SERVICES** tab to perform services such as importing packages that define Layer 4 to Layer 7 devices. You can view existing service nodes in the **INVENTORY** submenu tab.

ADMIN Tab

Use the **ADMIN** tab to perform administrative functions such as authentication, authorization, and accounting functions, scheduling policies, retaining and purging records, upgrading firmware, and controlling features such as syslog, Call Home, and SNMP.

Search Icon

Click the Search icon to display the search field. The search field enables you to locate objects by name or other distinctive fields.

Navigation Pane

Use the **Navigation** pane, which is on the left side of the APIC GUI below the submenu bar, to navigate to all elements of the submenu category. When you select a component in the **Navigation** pane, the object displays in the **Work** pane.

Note If any container in the **Navigation** pane, for example **Application Profiles** under a **Tenant**, contains more than 40 profiles, you cannot click on a profile and expand it in the Navigation pane. You must select the desired profile from the **Work** pane and expand it.

Work Pane

Use the **Work** pane, which is on the right side of the APIC GUI, to display details about the component that you selected in the **Navigation** pane. See the following figure for an example view of the **Work** pane.

The **Work** pane includes the following elements:

- A content area that displays tabs. These tabs enable you to access information that is related to the component that you chose in the **Navigation** pane. The tabs displayed in the content area depend upon the selected component.

- A link to context-sensitive online help that is represented by a question mark icon in the upper right corner.

Figure 3: Example View of APIC Work Pane

GUI Icons

Table 2: Frequently Displayed Icons in the APIC GUI

Icons	Description
	Control arrow for **Navigation** pane display
	Displays online help information
	Quickstart information
	Downloads the table as an XML file
	Displays the table view
	Displays the table view of the component that you chose in the **Navigation** pane
	Refreshes the context of the panel. Click this icon only when there is a connection problem, because the data is updated whenever the repository changes.
	Settings
	Next view
	Previous view
	Show path
	Clear path

Fault, Statistics, and Health Level Icons

Table 3: Severity Levels of Faults Displayed in the APIC GUI

Icons	Description
	Critical—This icon displays a fault level with critical severity.
	Major—This icon displays a fault level with major severity.
	Minor—This icon displays a fault level with minor severity.
	Warning—This icon displays a fault level that requires a warning.

API Inspector

Viewing an API Interchange in the GUI

When you perform a task in the APIC graphical user interface (GUI), the GUI creates and sends internal API messages to the operating system to execute the task. By using the API Inspector, which is a built-in tool of the APIC, you can view and copy these API messages. A network administrator can replicate these messages in order to automate key operations, or you can use the messages as examples to develop external applications that will use the API. .

Step 1 Log in to the APIC GUI.

Step 2 In the upper right corner of the APIC window, click the "welcome, <name>" message to view the drop-down list.

Step 3 In the drop-down list, choose the **Show API Inspector**.
The **API Inspector** opens in a new browser window.

Step 4 In the **Filters** toolbar of the **API Inspector** window, choose the types of API log messages to display.
The displayed messages are color-coded according to the selected message types. This table shows the available message types:

Name	Description
trace	Displays trace messages.
debug	Displays debug messages. This type includes most API commands and responses.
info	Displays informational messages.
warn	Displays warning messages.

Name	Description
error	Displays error messages.
fatal	Displays fatal messages.
all	Checking this checkbox causes all other checkboxes to become checked. Unchecking any other checkbox causes this checkbox to be unchecked.

Step 5 In the **Search** toolbar, you can search the displayed messages for an exact string or by a regular expression.
This table shows the search controls:

Name	Description
Search	In this text box, enter a string for a direct search or enter a regular expression for a regex search. As you type, the first matched field in the log list is highlighted.
Reset	Click this button to clear the contents of the Search text box.
Regex	Check this checkbox to use the contents of the Search text box as a regular expression for a search.
Match case	Check this checkbox to make the search case sensitive.
Disable	Check this checkbox to disable the search and clear the highlighting of search matches in the log list.
Next	Click this button to cause the log list to scroll to the next matched entry. This button appears only when a search is active.
Previous	Click this button to cause the log list to scroll to the previous matched entry. This button appears only when a search is active.
Filter	Check this checkbox to hide nonmatched lines. This checkbox appears only when a search is active.
Highlight all	Check this checkbox to highlight all matched fields. This checkbox appears only when a search is active.

Step 6 In the **Options** toolbar, you can arrange the displayed messages.
This table shows the available options:

Name	Description
Log	Check this checkbox to enable logging.
Wrap	Check this checkbox to enable wrapping of lines to avoid horizontal scrolling of the log list
Newest at the top	Check this checkbox to display log entries in reverse chronological order.
Scroll to latest	Check this checkbox to scroll immediately to the latest log entry.
Clear	Click this button to clear the log list.
Close	Click this button to close the API Inspector.

Example

This example shows two debug messages in the API Inspector window:

```
13:13:36 DEBUG - method: GET url: http://192.0.20.123/api/class/infraInfra.json
response: {"imdata":[{"infraInfra":{"attributes":{"instanceId":"0:0","childAction":"",
"dn":"uni/infra","lcOwn":"local","name":"","replTs":"never","status":""}}}]}

13:13:40 DEBUG - method: GET url: http://192.0.20.123/api/class/l3extDomP.json?
query-target=subtree&subscription=yes
response: {"subscriptionId":"72057598349672459","imdata":[]}
```

Initializing the Fabric

About Fabric Initialization

You can build a fabric by adding switches to be managed by the APIC and then validating the steps using the GUI, the CLI, or the API.

Note Before you can build a fabric, you must have already created an APIC cluster over the out-of-band network.

Example Topology

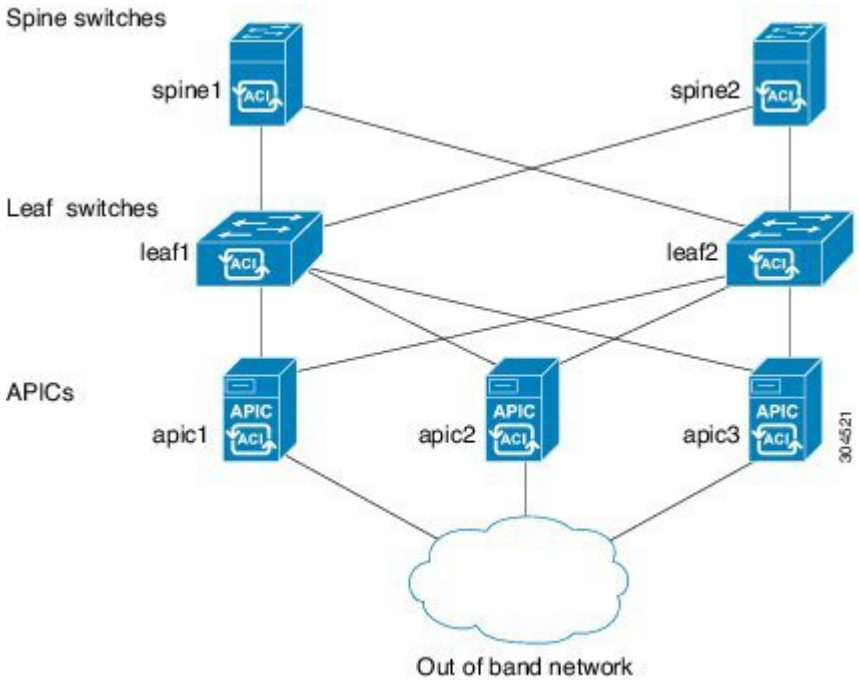
An example topology is as follows:

- Two spine switches (spine1, spine2)
- Two leaf switches (leaf1, leaf2)
- Three instances of APIC (apic1, apic2, apic3)

The following figure shows an example of a fabric topology.

Note For the actual simulator topology see the Cisco ACI Simulator Installation Guide.

Figure 4: Example Fabric Topology



Example Topology Connections

An example topology with connection details is as follows:

Name	Connection Details
leaf1	eth1/1 = apic1 (eth2/1) eth1/2 = apic2 (eth2/1) eth1/3 = apic3 (eth2/1) eth1/49 = spine1 (eth5/1) eth1/50 = spine2 (eth5/2)
leaf2	eth1/1 = apic1 (eth 2/2) eth1/2 = apic2 (eth 2/2) eth1/3 = apic3 (eth 2/2) eth1/49 = spine2 (eth5/1) eth1/50 = spine1 (eth5/2)

Name	Connection Details
spine1	eth5/1 = leaf1 (eth1/49) eth5/2 = leaf2 (eth1/50)
spine2	eth5/1 = leaf2 (eth1/49) eth5/2 = leaf1 (eth1/50)