Installing the Cisco APIC-EM Appliance

About the Appliance Installation

Cisco offers a physical appliance that can be purchased with the ISO image pre-installed and tested. You can deploy this appliance within your network. The Cisco APIC-EM can be deployed as a single host (single appliance in standalone mode) or within a multi-host environment (multiple appliances in multi-host mode).

Important We recommend that you install and deploy Cisco APIC-EM in multi-host mode for enhanced scalability and redundancy. For information about multi-host support, see Multi-Host Support.

The following table lists the steps for installing the Cisco APIC-EM appliance.

Table 1: Cisco APIC-EM Appliance Installation

Step	Description
1	Review the pre-install checklists for the appliance (standalone and multi-host modes). See Pre-Install Checklists, on page 3.

Step	Description
2	Review information about the different types of appliances and their specifications, including the following: • Physical • Environmental • Power • Front and rear panels See Cisco APIC-EM Series Appliances, on page 5.
3	Review information about port usage for the controller. See Cisco APIC-EM Ports Reference, on page 12.
4	Prepare the appliance for installation. See Preparing for Appliance Installation, on page 13.
5	(Optional) Install the appliance in a rack. See Installing the Appliance In a Rack, on page 16.
6	Connect power to the appliance and power it on. See Connecting and Powering On the Appliance, on page 22.
7	Check the appliance LEDs. See Checking the LEDs, on page 22.
8	(Optional) Install and/or replace appliance components, if necessary. See Installing or Replacing Appliance Components , on page 25.
9	(Optional) Install a new ISO on the appliance, if necessary. See Installing a New ISO on the Appliance, on page 26.
10	Proceed to configure the Cisco APIC-EM in standalone or multi-host mode. Refer to the following sections for information about the configuration wizard process: • Configuring Cisco APIC-EM as a Single Host Using the Wizard • Configuring Cisco APIC-EM in Multi-Host Mode

Pre-Install Checklists

Standalone Mode Checklists

Review the following checklists before beginning a single-host Cisco APIC-EM installation (standalone mode).

Note
A host is defined as an appliance, physical server, or virtual machine with instances of a Grapevine root and clients running. The Grapevine root is located in the host OS and the clients are located within Linux containers. The clients run the services within the Linux containers. You can set up either a single host deployment or multi-host deployment (2 or 3 hosts) for your network. For high availability and scale, your multi-host deployment must contain three hosts. All inbound traffic to the controller in a single host deployment is through the host IP address that you configure using the configuration wizard. All inbound traffic to the controller in a multi-host deployment is through a Virtual IP that you configure using the configuration wizard.

Networking Requirements

This Cisco APIC-EM installation requires that the network adapters (NICs) on the host (physical or virtual) are connected to the following networks:

- Internet (network access required for **Make A Wish** requests and telemetry collection)

- Network with NTP server(s)

- Network with devices that are to be managed by the Cisco APIC-EM

Note
The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment.

IP Address Requirements

Ensure that you have available at least one IP address for the network adapter (NIC) on the host.

The IP address is used as follows:

- Direct access to the Grapevine root

- Direct access to the Cisco APIC-EM controller (for GUI access)

Note
If your host has 2 NICs, then you may want to have two IP addresses available and configure one IP address for each NIC.

Multi-Host Mode Checklists

Review the following checklist before beginning a multi-host Cisco APIC-EM installation (multi-host mode).

- You must satisfy the requirements for the single host installation as described in the previous section for each host.

- Additionally, you must establish a network connection between each of the hosts using either a switch or a router. Each host must be routable with the other two hosts.

- You must configure a virtual IP (VIP).

  You configure one or more NICs on each host using the configuration wizard. Each NIC that you configure must point to a non-routable network (if all your networks are routable, then you only need one NIC). A VIP is required per non-routable network. For example, if you configure 2 NICs on all 3 hosts in a multi-host cluster and each NIC points to a separate, non-routable network, then you need to configure 2 VIPs. The VIP provides an interface redundancy feature for your multi-host deployment. With a VIP, the IP address can float between the hosts.

  When deploying the controller in a multi-host configuration:

  - You provide a VIP address when configuring the controller using the wizard.

  - On startup, the controller will bring up the VIP on one of the hosts.

  - All inbound requests into controller from the external network are made via this VIP (instead of the host IP address), and the requests are routed to the services running on different hosts via the reverse-proxy service.

  - If the host on which has the VIP fails, then Grapevine will bring up the VIP on one of the remaining two hosts.

  - The VIP must reside in the same subnet as the three hosts.

  - If you are planning to obtain a certificate issued for a multi-host environment, then it is important to get the certificate issued against the virtual IP or the host name resolvable to the virtual IP.

Multi-Host Deployment Virtual IP

A multi-host deployment has three physical IP addresses and one virtual IP that floats across the IP addresses by design in order to provide high availability. This capability to float also means that any SSH client that wants to connect to the virtual IP address will see different host-identity public SSH keys each time the virtual IP moves its residence from one host to another host. Most SSH clients will complain that the new host is not trusted, since an entry already exists (as you might have accepted the key earlier for the older host which owned that virtual IP address before). To prevent this inconvenience, you may want to add the host keys of all the three hosts to your known hosts list as described below.

For example on a Linux or Apple Mac OS client machine, run the **ssh-keyscan** command on each of the three host physical IP addresses as follows:

```
$ ssh-keyscan -t rsa 209.165.200.30
# 209.165.200.30 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.30 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRd
SYnuCHfDiY5Pptt3BmaPgC6OlER4wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVzlwtHHZdhO6G93MyLLGsWq
```

```
XSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9oimdv.....


$ ssh-keyscan -t rsa 209.165.200.31
# 209.165.200.31 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.31 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDF57F90z2His86tEj4s75pTc7h0nfzF
2c3QweHCNN2ov474HJJcPrnWTw4DAoPpPCU6zWvR0QLxunURDb+pMeZrIIyd49xn9+OBSmBpzrnety7UB2uP
XzL1RvVxayw8mkXkj779LhFh9vkXR4DtX7XLjg.....


$ ssh-keyscan -t rsa 209.165.200.32
# 209.165.200.32 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.32 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9kwzodGzGkh/UFXVa9fptGe+sa3CBR
6SNerXxpCmfT9AOXH8xuk3/CBX+DDUQgGJVmqw6maCYKOy0RtAhGxdsNdPL6ETTKzxYB5uzw3KhcDJ6D6ob6
jdzkR6yRuXVFi2OE+u1Aqs7J8GO66FfdavU8.....
```

Next, change the IP address in the SSH key line of each output to the virtual IP address of the following and append all three key lines to the ~/.ssh/known_hosts file and save it.

Assuming that 209.165.200.33 is the virtual IP address in the above multi-host example, you would add three lines in the ~/.ssh/known_hosts file of your client machine as follows:

```
209.165.200.33 ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRdSYnuCHfDiY5Pptt3BmaPgC6OlER4
wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVzlwtHHZdhO6G93MyLLGsWqXSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9
oimdvPbrQPua7Zg9oblDxaBPn0Fqj00YDjKqTkp/IkZHEfHbDM996GLEbWlOvoHeCCqeZ1nWgFIqzAF+ty8+X5Z/fh
hmGe+w2tQlMfrs9pcZDaEEmq/w1W+uRohxLKs+OHnHYAbMzC6O+5fLEr2BwaZf8W016eo1WpPsxUVK6StbXBOQZrcH0
bPsUbIjKJkzafpft9Dp73pSd/vwaoB3DrvNec/PiEJYk+R.....
```

After the above change, the client will have no trouble performing uninterrupted SSH into the virtual IP address of the hosts even with the IP address floating.

Cisco APIC-EM Series Appliances

Cisco provides a dedicated Cisco APIC-EM physical appliance that can be purchased from Cisco with the ISO image preinstalled and tested. The following physical appliances are currently available for purchase from Cisco:

- Cisco APIC-EM Controller Appliance 10C-64G-2T (Part Number APIC-EM-APL-R-K9)

- Cisco APIC-EM Controller Appliance 20C-128G-4T (Part Number APIC-EM-APL-G-K9)

The following table describes the basic system configurations for these appliances.

Platform	APIC-EM-APL-R-K9	APIC-EM-APL-G-K9
Physical CPU	1 physical CPU	2 physical CPUs
CPU (cores)	10 **Note** Hyper-threading is enabled by default, therefore 20 logical processors are available for this appliance.	20 **Note** Hyper-threading is enabled by default, therefore 40 logical processors are available for this appliance.
RAM	64 GB	128 GB

Platform	APIC-EM-APL-R-K9	APIC-EM-APL-G-K9
Total Disk Space	1.7 TB	3.4 TB
Ethernet NICs	2 (Gigabit Ethernet ports)	2 (Gigabit Ethernet ports)

Appliance Scale Limits

For the latest, detailed information about the Cisco APIC-EM appliances and scale limits, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*.

Physical Specifications

The following table lists the physical specifications for the Cisco APIC-EM appliances.

Table 2: Physical Specifications

Description	Specification
Height	1.7 in. (4.3 cm)
Width	16.9 in. (42.9 cm)
Depth (length)	29.8 in. (75.8 cm)
Maximum weight (fully loaded chassis)	SFF 8-drive: 37.9 lb. (17.2 Kg) LFF 4-drive: 39.9 lb. (18.1 Kg)

Environmental Specifications

The following table lists the environmental specifications for the Cisco APIC-EM appliances.

Table 3: Environmental Specifications

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.
Temperature, non-operating (when the server is stored or transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), operating	10 to 90%

Description	Specification
Humidity, non-operating	5 to 93%
Altitude, operating	0 to 10,000 feet
Altitude, non-operating (when the server is stored or transported)	0 to 40,000 feet
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	5.4
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	37

Power Specifications

The power specifications for the power supply are listed in the following section.

Note You can get more specific power information for your exact appliance configuration by using the Cisco UCS Power Calculator: http://ucspowercalc.cisco.com

Caution Do not mix power supply types in the appliance. Both power supplies must be identical.

770 W AC Power Supply

The following table lists the specifications for each 770 W AC power supply (Cisco part number UCSC-PSU1-770W).

Table 4: AC Power Supply Specifications

Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC input frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)

| Description	Specification
Maximum AC input current	9.5 A at 100 VAC 4.5 A at 208 VAC
Maximum input volt-amperes	950 VA at 100 VAC
Maximum output power per PSU	770 W
Maximum inrush current	15 A (sub-cycle duration)
Maximum hold-up time	12 ms at 770 W
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C14

Cisco APIC-EM Series Front and Rear Panels

The following figure displays the Cisco APIC-EM appliance front panel (APIC-EM-APL-G-K9).

Note   The Cisco APIC-EM appliance front panel (APIC-EM-APL-R-K9) shares a similar design.

*Figure 1: Cisco APIC-EM Appliance Front Panel (APIC-EM-APL-G-K9)*
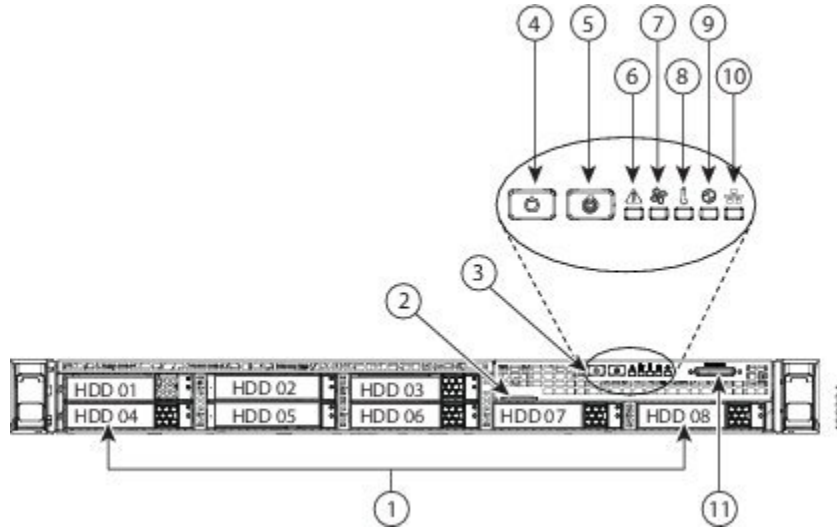
Component	Description
1	Drives (up to eight 2.5-inch drives)
2	Pull-out asset tag
3	Operations panel buttons and LEDs
4	Power button/power status LED
5	Unit identification button/LED
6	System status LED
7	Fan status LED
8	Temperature status LED
9	Power supply status LED
10	Network link activity LED
11	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)

The following figure displays the Cisco APIC-EM appliance rear panel (APIC-EM-APL-G-K9).

Note   The Cisco APIC-EM appliance rear panel (APIC-EM-APL-R-K9) shares a similar design.

Figure 2: Cisco APIC-EM Appliance Rear Panel (APIC-EM-APL-G-K9)
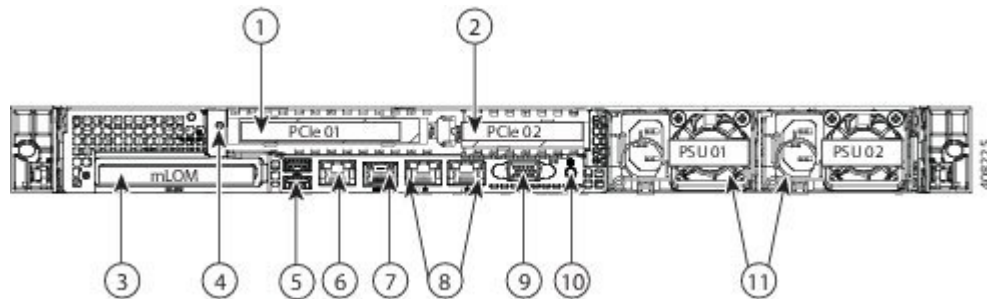
Component	Description
1	PCIe riser 1/slot 1
2	PCIe riser 2/slot 2
3	Modular LAN-on-motherboard (mLOM) card slot
4	Grounding-lug hole (for DC power supplies)
5	USB 3.0 ports (two)
6	1-Gb Ethernet dedicated management port
7	Serial port (RJ-45 connector)
8	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
9	VGA video port (DB-15)
10	Rear unit identification button/LED
11	Power supplies (up to two, redundant as 1+1)

Summary of Appliance Series Features

The following table lists the Cisco APIC-EM appliance series features.

Table 5: Cisco APIC-EM Appliance Series Features

Feature	Description
Chassis	One rack-unit (1RU) chassis.
Processors	Up to two Intel Xeon CPU E5-2650 v3 Series processors.
Memory	24 DDR4 DIMM sockets on the motherboard (12 each CPU).
Baseboard management	BMC, running Cisco Integrated Management Controller (Cisco IMC) firmware. Depending on your Cisco IMC settings, Cisco IMC can be accessed through the 1-Gb dedicated management port, the 1-Gb Ethernet LOM ports, or a Cisco virtual interface card.
Network and Management I/O	Supported connectors:[1] • One 1-Gb Ethernet dedicated management port • Two 1-Gb BASE-T Ethernet LAN ports • One RS-232 serial port (RJ-45 connector) • One 15-pin VGA2 connector • Two USB3 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector
Modular LOM	Dedicated socket that can be used to add an mLOM card for additional rear-panel connectivity (up to four 1-Gb or 10-Gb Ethernet ports).
Power	Two power supplies: • AC power supplies 770 W AC each. Do not mix power supply types or wattages in the server. Redundant as 1+1.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
Storage	• APIC-EM-APL-R-K9: 4 SAS HDD of 900 GB each • APIC-EM-APL-G-K9: 8 SAS HDD of 900 GB each
Disk Management (RAID)	Hardware-based RAID at RAID Level 10
Video	VGA video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory.

[1] The Intel X520 2 Port 10G PCI adapter (Part No. N2XX-AIPCI01) and 10G SFP+ (Part No. CDE2-SFP-1WSR=) is now supported for the Cisco APIC-EM Appliance Server.

Cisco APIC-EM Ports Reference

The following tables list the Cisco APIC-EM ports that permit incoming traffic, as well as the Cisco APIC-EM ports that are used for outgoing traffic. You should ensure that these ports on the controller are open for both incoming and outgoing traffic flows.

Note   Ensure that proper protections exist in your network for accessing port 22. For example, you can configure a proxy gateway or secure subnets to access this port.

Table 6: Cisco APIC-EM Incoming Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH	TCP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443 [2]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP (Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP
16026	SCEP	TCP

[2] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Table 7: Cisco APIC-EM Outgoing Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH (to the network devices)	TCP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
23	Telnet (to the network devices)	TCP
53	DNS	UDP
80	Port 80 may be used for an outgoing proxy configuration. Additionally, other common ports such as 8080 may also be used when a proxy is being configured by the Cisco APIC-EM configuration wizard (if a proxy is already in use for your network). **Note** To access Cisco supported certificates and trust pools, you can configure your network to allow for outgoing IP traffic from the controller to Cisco addresses at the following URL: http://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP agent	UDP
443 [3]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP ((Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP

[3] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Preparing for Appliance Installation

This section provides information about preparing for the Cisco APIC-EM series appliance installation.

Unpack and Inspect the Appliance

⚠

Caution   When handling internal appliance components, wear an ESD strap and handle modules by the carrier edges only.

🔎

Tip   Keep the shipping container in case the appliance requires shipping in the future.

✎

Note   The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

Step 1   Remove the appliance from its cardboard container and save all packaging material.

Step 2   Compare the shipment to the equipment list provided by your customer service representative. Verify that you have all items.

Step 3   Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

- Invoice number of shipper (see the packing slip)
- Model and serial number of the damaged unit
- Description of damage
- Effect of damage on the installation

Installation Guidelines

⚠

Warning   **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° F).** Statement 1047

⚠

Warning   **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.** Statement 1019

⚠ **Warning** **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A.** Statement 1005

⚠ **Warning** **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

⚠ **Caution** To ensure proper airflow it is necessary to rack the appliances using rail kits. Physically placing the units on top of one another or "stacking" without the use of the rail kits blocks the air vents on top of the appliances, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your appliances on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the appliances. No additional spacing between the appliances is required when you mount the units using rail kits.

⚠ **Caution** Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

When you are installing an appliance, use the following guidelines:

- Plan your site configuration and prepare the site before installing the appliance. For reference, see the Cisco UCS Site Preparation Guide for the recommended site planning tasks.

- Ensure that there is adequate space around the appliance to allow for servicing the appliance and for adequate airflow. The airflow in this appliance is from front to back.

- Ensure that the air-conditioning meets the thermal requirements listed in the Environmental Specifications, on page 6.

- Ensure that the cabinet or rack meets the requirements listed in the following "Rack Requirements" section.

- Ensure that the site power meets the power requirements listed in the Power Specifications, on page 7. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Review the Rack Requirements

This section provides the requirements for the standard open racks.

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.

- The rack post holes can be square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.

- The minimum vertical rack space per server must be one RU, equal to 1.75 in. (44.45 mm).

Review the Equipment Requirements

The slide rails sold by Cisco Systems for this appliance do not require tools for installation.

Supported Slide Rail Kits

This appliance supports two rail kit options:

- Cisco part UCSC-RAILB-M4= (ball-bearing rail kit).
- Cisco part UCSC-RAILF-M4= (friction rail kit).

Do not attempt to use a rail kit that was for the Cisco UCS C220 M3 server; the rail kits for the Cisco APIC-EM appliance have been designed specifically for it.

Slide Rail Adjustment Range and Cable Management Arm Dimensions

The slide rails for this server have an adjustment range of 24 to 36 inches (610 to 914 mm).

The optional cable management arm (CMA) adds additional length requirements:

- The additional distance from the rear of the server to the rear of the CMA is 5.4 inches (137.4 mm).
- The total length of the server including the CMA is 35.2 inches (894 mm).

Installing the Appliance In a Rack

Installing the Slide Rails

This section describes how to install the appliance in a rack using the rack kits that are sold by Cisco.

Warning   **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the rack. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack**.

Statement 1006

Step 1   Attach the inner rails to the sides of the server:

a) Align an inner rail with one side of the server so that the three keyed slots in the rail align with the three pegs on the side of the server (see below figure).

b) Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

c) Install the second inner rail to the opposite side of the server.

*Figure 3: Attaching Inner Rail to Side of Server*
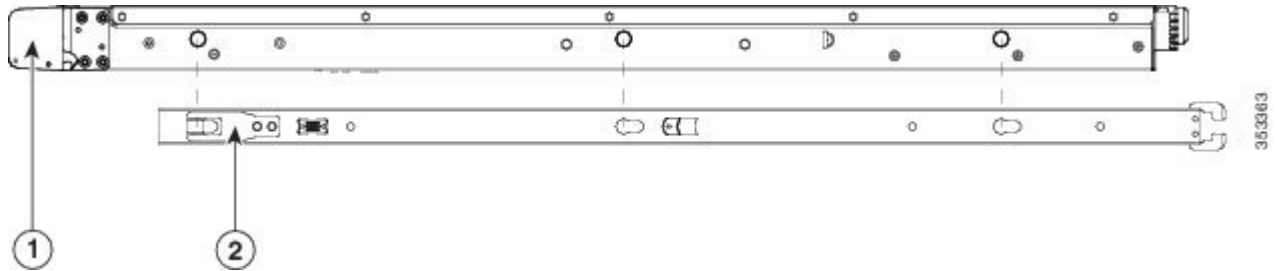
1	Front of server
2	Locking clip on inner rail

Step 2 Open the front securing plate on both slide-rail assemblies.

The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes. On the outside of the assembly, push the green arrow button toward the rear to open the securing plate.

Figure 4: Front Securing Mechanism, Inside of Front End
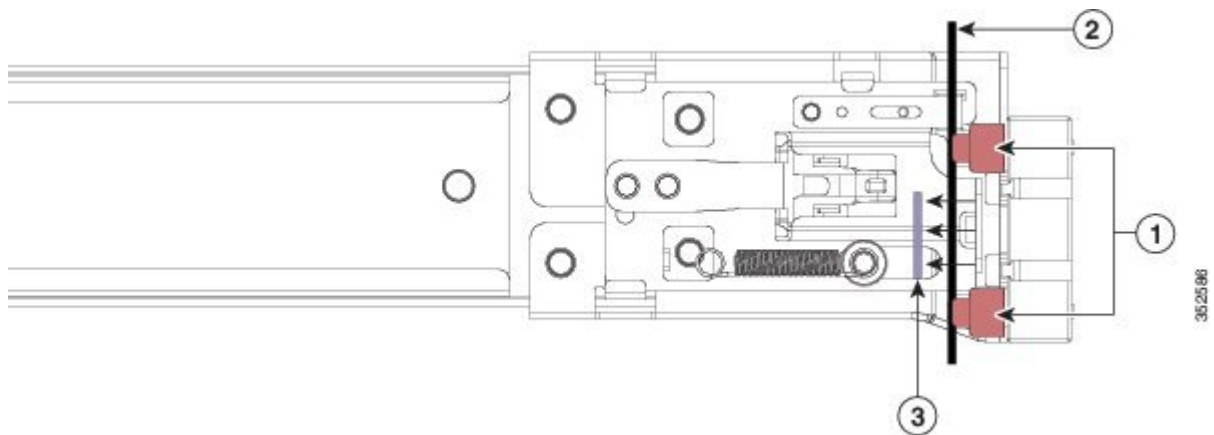
1	Front mounting pegs
2	Rack post
3	Securing plate shown pulled back to open position

Step 3   Install the outer slide rails into the rack:

a) Align one slide-rail assembly front end with the front rack-post holes that you want to use.
   The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front

   **Note**   The rack post must be between the mounting pegs and the open securing plate.

b) Push the mounting pegs into the rack-post holes from the outside-front.

c) Press the securing plate release button, marked PUSH. The spring-loaded securing plate closes to lock the pegs in place.

d) Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear rack-post holes. The slide rail must be level front-to-rear.
   The rear mounting pegs enter the rear rack-post holes from the inside of the rack post.

e) Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height with each other and are level front-to-back.

f) Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Step 4   Insert the server into the slide rails:

Caution   This server can weigh up to 67 pounds (59 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the server. Attempting this procedure alone could result in personal injury or equipment damage.

a) Align the rear of the inner rails that are attached to the server sides with the front ends of the empty slide rails on the rack

b) Push the inner rails into the slide rails on the rack until they stop at the internal stops.

c) Slide the release clip toward the rear on both inner rails, and then continue pushing the server into the rack until its front slam latches engage with the rack posts.

Figure 5: Inner Rail Release Clip
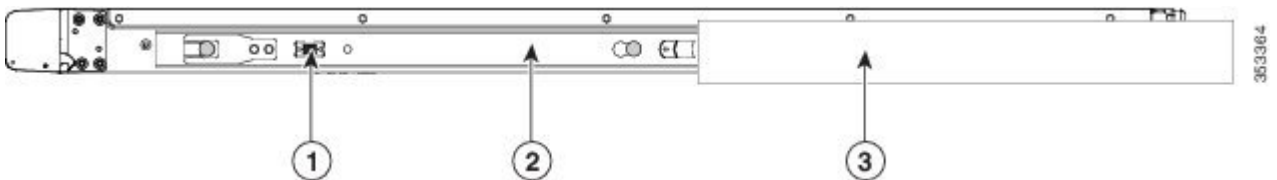
1	Inner rail release clip
2	Inner rail attached to server and inserted into outer rail
3	Outer rail attached to rack post

Step 5   (Optional) Secure the server in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with servers installed.

With the server fully pushed into the slide rails, open a hinged slam latch lever on the front of the server and insert the screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the server from being pulled out. Repeat for the opposite slam latch.

What to Do Next

If necessary for your installation, install the cable management arm.

Installing the Cable Management Arm (Optional)

The following procedure describes how to install the cable management arm.

Before You Begin

The CMA is reversible left to right. To reverse the CMA, see Reversing the Cable Management Arm (Optional) section, before installation.

Step 1   With the server pushed fully into the rack, slide the CMA tab of the CMA arm that is farthest from the server onto the end of the stationary slide rail that is attached to the rack post (see the figure below). Slide the tab over the end of the rail until it clicks and locks.

Step 2   Slide the CMA tab that is closest to the server over the end of the inner rail that is attached to the server (see the figure below). Slide the tab over the end of the rail until it clicks and locks.

Step 3   Pull out the width-adjustment slider that is at the opposite end of the CMA assembly until it matches the width of your rack (see the figure below).

Step 4   Slide the CMA tab that is at the end of the width-adjustment slider onto the end of the stationary slide rail that is attached to the rack post (see figure below). Slide the tab over the end of the rail until it clicks and locks.

Step 5   Open the hinged flap at the top of each plastic cable guide and route your cables through the cable guides as desired.

Figure 6: Installing the Cable Management Arm
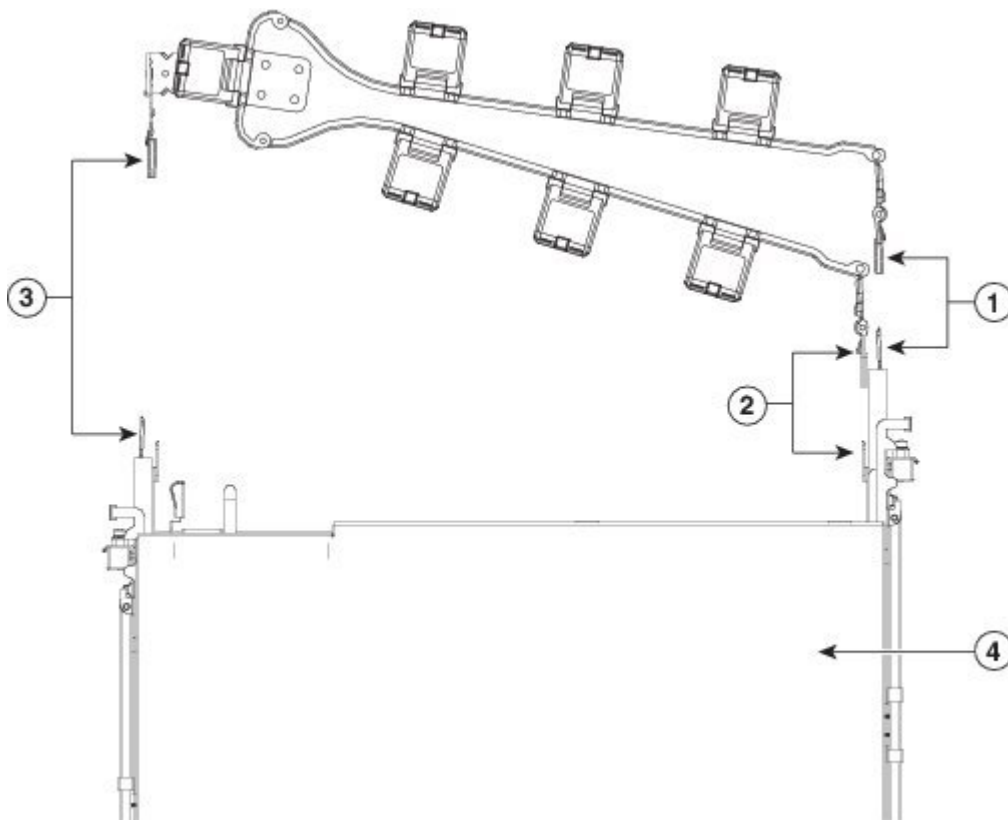
The following table describes the components of the CMA.

| 1	CMA tab on arm farthest from server and end of stationary outer slide rail

2	CMA tab on arm closest to the server and end of inner slide rail attached to server
3	CMA tab on width-adjustment slider and end of stationary outer slide rail
4	Rear of server

Reversing the Cable Management Arm (Optional)

The following procedure describes how to reverse the cable management arm.

Step 1   Rotate the entire CMA assembly 180 degrees. The plastic cable guides must remain pointing upward.

Step 2   Flip the tabs at the end of each CMA arm so that they point toward the rear of the server.

Step 3   Pivot the tab that is at the end of the width-adjustment slider. Depress and hold the metal button on the outside of the tab and pivot the tab 180 degrees so that it points toward the rear of the server.

Figure 7: Reversing the Cable Management Arm
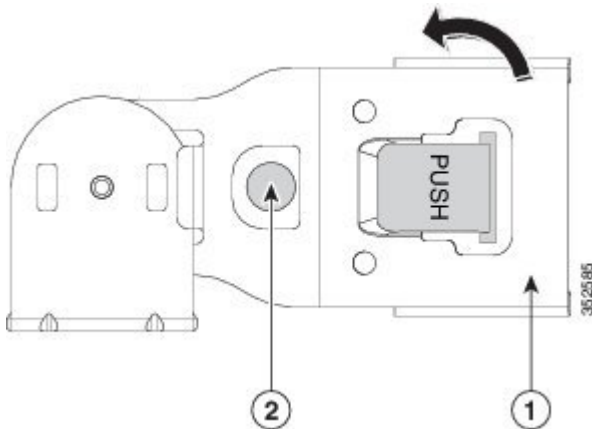
Refer to the following figure when reversing the cable management arm.

1	CMA tab on end of width-adjustment slider
2	Metal button for rotating

Connecting and Powering On the Appliance

This section describes how to power on the appliance and assign an IP address to connect to it.

Step 1   Attach a supplied power cord to each power supply in the appliance and then attach the power cord to a grounded AC power outlet. See the Power Specifications, for power specifications.
Wait for approximately two minutes to let the appliance boot in standby power during the first bootup.

You can verify the power status by looking at the Power Status LED:

- Off—There is no AC power present in the appliance.

- Amber—The appliance is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.

- Green—The appliance is in main power mode. Power is supplied to all appliance components.

Note   During bootup, the appliance beeps once for each USB device that is attached to the appliance. Even if there are no external USB devices attached, there is a short beep for each virtual USB device such as a virtual floppy drive, CD/DVD drive, keyboard, or mouse. A beep is also emitted if a USB device is hot-plugged or hot-unplugged during BIOS power-on self-test (POST), or while you are accessing the BIOS Setup utility or the EFI shell.

Step 2   Connect a USB keyboard and VGA monitor by using the supplied KVM cable connected to the KVM connector on the front panel.
Note   Alternatively, you can use the VGA and USB ports on the rear panel. However, you cannot use the front panel VGA and the rear panel VGA at the same time. If you are connected to one VGA connector and you then connect a video device to the other connector, the first VGA connector is disabled.

Step 3   Refer to the following sections for configuring and using CIMC to assign an IP address to the appliance:

- Configuring CIMC, on page 28

- Using CIMC to Configure a Cisco APIC-EM Series Appliance, on page 31

Checking the LEDs

When the Cisco APIC-EM series appliances have been started up and are running, observe the state of the front-panel and rear-panel LEDs. The following sections describe the LED color, its power status, activity, and other important status indicators that are displayed for the Cisco APIC-EM series appliance.

Front Panel LEDs and Buttons

The following table describes the appliance front panel LEDs and buttons on the appliance.

✎

Note The minimum network interface speed for the appliance should be 1 GB a second.

Table 8: Front Panel LEDs and Buttons

LED Name	State
Front Panel LEDs and Buttons	Off—There is no AC power to the appliance. Amber—The appliance is in standby power mode. Power is supplied only to the CIMC and some motherboard functions. Green—The appliance is in main power mode. Power is supplied to all server components.
Identification	Off—The Identification LED is not in use. Blue—The Identification LED is activated.
System status	Green—The appliance is running in a normal operating condition. Green, blinking—The appliance is performing system initialization and memory checks. Amber, steady—The appliance is in a degraded operational state, which may be due to one of the following: – Power supply redundancy is lost. – CPUs are mismatched. – At least one CPU is faulty. – At least one DIMM is faulty. – At least one drive in a RAID configuration failed. Amber, blinking—The appliance is in a critical fault state, which may be due to one of the following: – Boot failed. – Fatal CPU and/or bus error is detected. – Server is in an over-temperature condition.
Fan status	Green—All fan modules are operating properly. Amber, steady—One fan module has failed. Amber, blinking—Critical fault, two or more fan modules have failed.

LED Name	State
Temperature status	Green—The appliance is operating at normal temperature. Amber, steady—One or more temperature sensors have exceeded a warning threshold. Amber, blinking—One or more temperature sensors have exceeded a critical threshold
Power supply status	Green—All power supplies are operating normally. Amber, steady—One or more power supplies are in a degraded operational state. Amber, blinking—One or more power supplies are in a critical fault state.
Network link activity	Off—The Ethernet link is idle. Green—One or more Ethernet LOM ports are link-active, but there is no activity. Green, blinking—One or more Ethernet LOM ports are link-active, with activity.
Hard drive fault	Off—The hard drive is operating properly. Amber—The hard drive has failed. Amber, blinking—The device is rebuilding.
Hard drive activity	Off—There is no hard drive in the hard drive sled (no access, no fault). Green—The hard drive is ready. Green, blinking—The hard drive is reading or writing data.

Rear Panel LEDs and Buttons

The following table describes the appliance rear panel LEDs and buttons on the appliance.

Note   The minimum network interface speed for the appliance should be 1 GB a second.

Table 9: Rear Panel LEDs and Buttons

LED Name	State
Power supply fault	Off—The power supply is operating normally. Amber, blinking—An event warning threshold has been reached, but the power supply continues to operate. Amber, solid—A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).
Power supply AC OK	Off—There is no AC power to the power supply. Green, blinking—AC power OK, DC output not enabled. Green, solid—AC power OK, DC outputs OK.
1 Gb Ethernet dedicated management link speed	Off—link speed is 10 Mbps. Amber—link speed is 100 Mbps. Green—link speed is 1 Gbps.
1 Gb Ethernet dedicated management link status	Off—No link is present. Green—Link is active. • Green, blinking—Traffic is present on the active link.
1 Gb Ethernet link speed	Off—link speed is 10 Mbps. Amber—link speed is 100 Mbps. Green—link speed is 1 Gbps.
1 Gb Ethernet link status	Off—No link is present. Green—Link is active. Green, blinking—Traffic is present on the active link.
Identification	Off—The Identification LED is not in use. Blue—The Identification LED is activated.

Installing or Replacing Appliance Components

Refer to the Cisco UCS C220 Server Installation and Service Guide for information on how to install or replace the Cisco APIC-EM appliance components.

Installing a New ISO on the Appliance

Under certain circumstances, you may need to install a new or the latest Cisco ISO image on the appliance. This section describes the following procedures that you can use to perform this task:

- Downloading the Cisco APIC-EM ISO image

- Installing the Cisco APIC-EM ISO image on the Cisco APIC-EM series appliances using one of the following procedures:

    ◦ Install the ISO image using the CIMC Remote Management Utility

    ◦ Install the ISO image using a USB flash drive

    ◦ Install the ISO image using an external DVD drive with a USB port

Downloading the Cisco APIC-EM ISO Image

You can download the latest Cisco APIC-EM ISO image from Cisco.com

Step 1 Go to the following URL address:
http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-general-information.html
You must already have valid Cisco.com login credentials to access this link.

Step 2 Click **Download Software for this Product**.
Proceed to download the ISO file to a secure location on your network.

Installing the ISO Image on the Cisco APIC-EM Series Appliance

After you download the ISO image, you can perform a fresh installation on your Cisco APIC-EM series appliance by using any of the following methods:

- Install the ISO image using the CIMC Remote Management Utility.

    1 Configure CIMC.

    2 Install the Cisco APIC-EM software release remotely.

    ☞

    Important You must configure the CIMC to perform this remote installation. For information about configuring CIMC, see Configuring CIMC, on page 28.

- Install the ISO image using a USB flash drive.

1 Create a bootable USB disk from the USB flash drive.

2 Connect the bootable USB disk to the Cisco APIC-EM series appliance.

3 Install the Cisco APIC-EM software release using the local KVM or remotely using the CIMC KVM.

Note For information about creating a bootable USB disk from a USB flash drive, see Creating a Bootable USB Disk and Attaching the ISO, on page 30.

• Install the ISO using an external DVD drive with a USB port.

1 Burn the ISO image on to a DVD.

2 Connect the external USB DVD to the Cisco APIC-EM series appliance.

3 Install the Cisco APIC-EM software release via the local KVM or remotely using the CIMC KVM.

Note If your Cisco APIC-EM series appliance is running an earlier version of the controller software, you can upgrade it to the latest version by following the upgrade procedure using the GUI as described in the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*. Currently, reimaging your existing Cisco APIC-EM series appliance to perform an upgrade to the latest release is not supported.

Note For installing the Cisco APIC-EM software release using a USB flash device or an external DVD with a USB port, the CIMC configuration is optional. Choose one of these options if you do not prefer a remote installation.

Configuring CIMC

You can perform all operations on Cisco APIC-EM series appliances using the CIMC. To do this, you must first configure an IP address and IP gateway to access the CIMC from a web-based browser.

Step 1 Attach a keyboard and monitor to the USB ports on the rear panel of the appliance or by using a KVM cable and connector to access the appliance console.

Step 2 Plug in the power cord.

Step 3 Press the **Power** button to boot the server. Watch for the prompt to press **F8** as shown in the following screen.

Figure 8: CIMC Opening Screen

```
ılıılı
CISCO

Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C220M4.2.0.8b.0.080620151546
Platform ID  : C220M4

Cisco IMC IPv4 Address 209.165.200.12
Cisco IMC MAC Address :58:AC:12:35:56:88

Processor(s) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz
Total Memory  = 64 GB Effective Memory = 64 GB
Memory Operating Speed 2133 Mhz
```

Step 4   During bootup, press **F8** when prompted to open the BIOS CIMC Configuration Utility. The following screen appears.

Figure 9: CIMC Configuration Utility

```
Cisco IMC Configuration Utility Version 2.0   Cisco Systems, Inc.
*******************************************************************************
NIC Properties
 NIC mode                              NIC redundancy
 Dedicated:        [X]                  None:                 [X]
 Shared LOM:       [ ]                  Active-standby:       [ ]
  Cisco Card:                           Active-active:        [ ]
   Riser1:         [ ]                 VLAN (Advanced)
   Riser2:         [ ]                  VLAN enabled:         [ ]
   MLom:           [ ]                  VLAN ID:              1
 Shared LOM Ext:   [ ]                  Priority:             0
IP (Basic)
 IPV4:             [X]        IPV6:     [ ]
 DHCP enabled      [ ]
 CIMC IP:          209.165.200.12
 Prefix/Subnet:    255.255.254.0
 Gateway:          209.165.200.13
 Pref DNS Server:  0.0.0.0

*******************************************************************************
<Up/Down>Selection    <F10>Save    <Space>Enable/Disable    <F5>Refresh    <ESC>Exit
<F1>Additional settings
```

Step 5   In the Configuration Utility window, change the following fields as specified:

• **NIC mode**—Select Dedicated.

• **IP (Basic)**—Select IPV4.

• **CIMC IP**—Enter the IP address of the CIMC.

• **Prefix/Subnet**—Enter the subnet of the CIMC.

• **Gateway**—Enter the Gateway address.

• **Pref DNS Server**—Enter the preferred DNS server address, if available.

    • **NIC Redundancy**—None

Step 6   Press **F1** to specify additional settings.

Step 7   Make the following changes on the Additional Settings window:

    • For **Common Properties**, enter a hostname for CIMC.

    • For **Common Properties**, turn off Dynamic DNS.

    • Turn off the **Factory Defaults**.

    • Enter the admin password. If you leave the password field blank, the default password is *password*.

    • Enter new **Port Properties** or accept the default.

    • Turn off the **Port Profiles**.

Step 8   Press **F10** to save the settings.

Step 9   Press **escape** to exit and reboot the server.

Step 10   After the settings are saved, open a browser and enter the following URL:
https://CIMC_ip_address where CIMC_IP_address is the IP address that you entered in Step 5.

What to Do Next

Use CIMC to install the Cisco APIC-EM software release on a Cisco APIC-EM series appliance. For information about this procedure, see Using CIMC to Configure a Cisco APIC-EM Series Appliance, on page 31.

Creating a Bootable USB Disk and Attaching the ISO

Follow the procedure described below to create a bootable USB disk for the Cisco APIC-EM appliance.

☞

Important   There are many ways to create a bootable USB disk and this procedure is only one example of such a process of creating a bootable USB disk. This procedure uses the Rufus freeware utility (version 2.6.818) to create a bootable USB disk using a Windows machine. The URL for the Rufus freeware utility download is located at: https://rufus.akeo.ie/.

Before You Begin

The USB flash drive that you are using to create a bootable USB disk should have a minimum capacity of at least 8 GB.

Step 1   Download a freeware utility to create a bootable USB disk to your Windows machine (laptop or desktop). After download, open and install the utility.

Note   The Rufus freeware utility will open and self-install.

Step 2 Connect your USB drive to your Windows machine where you downloaded the utility.

After connecting your USB drive, the utility GUI appears. Review the following default values from the drop-down menus for the bootable USB disk:

- **Partition scheme and target system type**: MBR partition scheme for BIOS or UEFI

- **File system**: FAT32

- **Cluster size**: 4096 bytes

- **Quick format** : (Checked)

- **Create a bootable disk using FreeDOS**: (Checked)

- **Create extended label and icon files**: (Checked)

Important Do not change any of the displayed default values in the GUI.

Step 3 Click the **Click to select image** icon located in the middle of the GUI.

The **Click to select image** icon is an image of a CD-ROM that is located in the middle of the GUI field. It is next to the Format Option, **Create a bootable disk using**, with **FreeDOS** selected from the drop-down menu.

Important Keep the drop-down menu set at **FreeDOS**.

Step 4 Navigate to the Cisco APIC-EM ISO image on your network and select it.

Step 5 Click **Start** to begin copying the ISO image to the USB drive.

This action creates the USB drive as a bootable USB disk with the Cisco APIC-EM ISO image installed.

Step 6 Remove the bootable USB disk from the laptop or desktop and use it wherever you will install the controller.

What to Do Next

Insert the bootable USB disk into the server or appliance where you will install the controller.

Using CIMC to Configure a Cisco APIC-EM Series Appliance

After you configure the CIMC for your appliance, you can use it to manage a Cisco APIC-EM series appliance. You can perform all operations including BIOS configuration through the CIMC.

Before You Begin

Ensure that you have connected and powered up the appliance by following the recommended procedures in this guide.

Ensure that you have configured the CIMC on your appliance. For information about this procedure, see Configuring CIMC, on page 28

Ensure that you have the Cisco APIC-EM ISO image on the client machine from which you are accessing the CIMC or you have a bootable USB with the image for installation.

Ensure that you have your Cisco APIC-EM program parameter information available and the requirements ready for deployment (for example, NTP servers).

Step 1   Connect to the CIMC for appliance management.
Connect the Ethernet cables from the LAN to the appliance using the ports selected by the Network Interface Card (NIC) Mode setting. The active-active and active-passive NIC redundancy settings require you to connect to two ports.

Step 2   Use a browser and the IP address of the CIMC to log in to the CIMC Setup Utility.
The IP address is based on the CIMC configuration that you made.

Go to the default username for the server is admin. The default password is *password*.

Step 3   Click **Launch KVM Console** in the CIMC GUI .

Step 4   Use your CIMC credentials to log into the KVM console.

Step 5   Click **Virtual Media** on the **KVM Console** menu bar.

Step 6   Click **Activate Virtual Devices** from the **Virtual Media** drop down menu.

Step 7   Browse to the Cisco APIC-EM ISO image in the **Virtual Media - Map CD/DVD** window.

Step 8   Once the Cisco APIC-EM ISO image appears in the **Drive/Image File** field, click the **Map Device** button.
The **Read Only** check box should be checked in this window.

Step 9   Choose **Macros** | **Static Macros** | **Ctrl-Alt-Del** to boot the Cisco APIC-EM series appliance using the ISO image. A screen similar to the one shown in the following figure appears.

Figure 10: CIMC Window

Step 10   Press **F6** to bring up the boot menu. A screen similar to the following one appears.

Figure 11: Boot Device Window


```
Please select boot device:

(Bus 05 Dev 00)PCI RAID Adapter
Cisco vKVM-Mapped vHDD1.22
Cisco CIMC-Mapped vHDD1.22
UEFI: Built-in EFI Shell
IBA GE Slot 0100 v1553
IBA GE Slot 0101 v1553
Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vFDD1.22
Cisco CIMC-Mapped vDVD1.22
Enter Setup

    ↑ and ↓ to move selection
  ENTER to select boot device
  ESC to boot using defaults
```

Step 11   Choose the DVD that you mapped and press **Enter**.
After pressing **Enter**, the Cisco APIC-EM ISO software and files are installed on your appliance.

After these files are installed, the Ubuntu screen briefly appears. Next, the Cisco APIC-EM configuration wizard starts.

Step 12   Proceed to configure the Cisco APIC-EM using the wizard.
If the configuration wizard does not start, then enter the **config_wizard** command initiate the configuration process.

Refer to the following sections for information about the configuration wizard process:

   • Configuring Cisco APIC-EM as a Single Host Using the Wizard

   • Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard

After you are done with the configuration wizard and have rebooted, the Cisco APIC-EM GUI Login window appears.
The Cisco APIC-EM is now ready to use.

What to Do Next

At the Cisco APIC-EM GUI Login window, you are prompted to enter the web-based admin login credentials
(username and password) to access the Cisco APIC-EM user interface. You can initially access the web
interface by using the GUI admin user's username and password that you defined during the setup process.

After you log in to the Cisco APIC-EM user interface, you can then configure your controller settings including discovery credentials, SNMP values, and certificates. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*, for information about configuring the controller settings.