Configuring Cisco APIC-EM in Multi-Host Mode

Reviewing Cisco APIC-EM Configuration Wizard Parameters

When the Cisco APIC-EM configuration begins, an interactive wizard prompts you to enter information to configure the controller. The following table displays the information that you will be prompted for to complete the configuration.

Note Ensure that the DNS and NTP servers are reachable before you run the configuration wizard and whenever a Cisco APIC-EM host reboots in the deployment.

Table 1: Cisco APIC-EM Configuration Wizard Parameters

Configuration Wizard Prompt	Description	Example
(Optional) Bonded NICs	Choose to configure or not configure bonded NICs on the controller's interfaces. Enter 'yes' to proceed with configuring NIC bonding on the interfaces. Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration.	Enter 'yes'.

Configuration Wizard Prompt	Description	Example
Bonding mode	If you chose to configure bonded NICs, then configure either 'balance-xor' or '802.3ad' for the bonded NICs. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs. **Important** Entering '802.3ad' requires that a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches. For this release, only one bonded interface with multiple NICs can be configured on the controller.	Enter '802.3ad '.
(Optional) VLAN	Choose to configure or not configure VLANs on the controller's interfaces. The NICs on the controller (whether an appliance, server, or virtual machine) can be configured with a VLAN interface. Both bonded NICs and standalone NICs can be configured with VLANs. The management interface of the appliance, server, or virtual machine can also be selected and configured with a VLAN interface. **Note** The same VLAN cannot be used on multiple interfaces.	Enter 'yes' The VLAN range is limited (1-1001, 1005-4094).

Configuration Wizard Prompt	Description	Example
Host IP address	Enter a host IP address. This IP address is used for the network adapter (eth0) on the host and connects to the external network or networks. For multiple network adapters, have several IP addresses available. **Note** This host IP address must be a valid IPv4 address.	10.0.0.12
(Optional) Virtual IP address	Enter a virtual IP address. This virtual IP address is used for the network adapter (eth0) on the host. You should only configure a virtual IP address, if you are setting up a multi-host deployment. **Note** The virtual IP address must be a valid IPv4 address.	10.12.13.14
Netmask IP address	Enter a netmask IP address. This must be a valid IPv4 netmask.	255.255.255.0
Default Gateway IP address	Enter a default gateway IP address. This must be a valid IPv4 address for the default gateway.	10.12.13.1
Primary DNS server	Enter a primary DNS server address. This must be a valid IPv4 address for the primary DNS server.	10.15.20.25 **Note** Enter either a single IP address for a single primary server, or multiple IP addresses separated by spaces for DNS servers.

Configuration Wizard Prompt	Description	Example
Primary NTP server	Enter a primary NTP server address. This must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server. **Note** Before you deploy the Cisco APIC-EM, make sure that the time on the controller's system clock is current or that you are using a Network Time Protocol (NTP) server that is keeping the correct time.	10.12.13.10 Enter either a single IP address for a single NTP primary server, or multiple IP addresses separated by spaces for several NTP servers. We recommend that you configure three NTP servers for your deployment.
Add/Edit another NTP server	This must be a valid NTP domain.	10.12.13.11 Allows you to configure multiple NTP servers. **Note** We recommend that you configure three NTP servers for your deployment.
(Optional) HTTPS proxy server	Enter an HTTPS proxy server address. This must be a valid IPv4 address for the HTTPS proxy with port number.	https://209.165.200.11:3128
Admin Username	Enter the admin user name. Identifies the administrative username used for GUI access to the Cisco APIC-EM controller. We recommend that the username be three to eight characters in length and be composed of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin2780

Configuration Wizard Prompt	Description	Example

Admin Password	Enter the admin password.
	Identifies the administrative password that is used for GUI access to the Cisco APIC-EM controller. You must create this password because there is no default. The password meet the following requirements:
	• Eight character minimum length.
	• Does NOT contain a tab or a line break.
	• Does contain characters from at least three of the following categories:
	  • Uppercase alphabet
	  • Lowercase alphabet
	  • Numeral
	  • Special characters (for example, ! or #)
		MyIseYPass2

Linux Username	Enter a Linux username. Identifies the Linux (Grapevine) username used for CLI access to the Grapevine root and clients.	The default is 'grapevine' and cannot be changed.

Configuration Wizard Prompt	Description	Example

Linux Password	Enter a Linux password.
	Identifies the Linux (Grapevine) password that is used for CLI access to the Grapevine roots and clients. You must create this password because there is no default. The password meet the following requirements:
	• Eight character minimum length.
	• Does NOT contain a tab or a line break.
	• Does contain characters from at least three of the following categories:
	  • Uppercase alphabet
	  • Lowercase alphabet
	  • Numeral
	  • Special characters (for example, ! or #)
		MyGVPass01

Supported Multi-Host Configurations

The Cisco APIC-EM supports a single-host, two-host, or three-host cluster configuration. With a single-host configuration, 32 GB of RAM is required for that host. With a two or three-host cluster configuration, 32 GB of RAM is required for each host in the cluster.

Note Cisco APIC-EM does not support a cluster with more than three hosts. For example, a multi-host cluster with five or seven hosts is not currently supported.

The three-host cluster provides *both* software and hardware high availability. The single-host or two-host cluster only provides software high availability; they do not provide hardware high availability. For this reason, we strongly recommend that for a multi-host configuration three hosts be used.

A hardware failure occurs when the physical host itself malfunctions or fails. A software failure occurs when a service on a host fails. Software high availability involves the ability of the services on the host or hosts to be restarted and respun. For example, on a single host, if a service fails then that service is respun on that host. In a two-host cluster, if a service fails on one host then that service is re-spun on the remaining host. In a three-host cluster, if a service fails on one host, then that service is re-spun on one of the two remaining hosts.

When setting up a two-host or three-host cluster, you should never set up the hosts to span a LAN across slow links. This may impact the recovery time if a service fails on one of the hosts. Additionally, when configuring either a two-host or three-host cluster, all of the hosts in that cluster must reside in the same subnet.

For additional detailed information about multi-host clusters, see Multi-Host Support.

Configuring Cisco APIC-EM in Multi-Host Mode

Configuring Cisco APIC-EM in multi-host mode involves the following procedures:

1. Configure Cisco APIC-EM as a single host using the configuration wizard.
2. Configure Cisco APIC-EM on a second host and to join it to the first, pre-existing host to create a cluster.
3. Configure Cisco APIC-EM on a third host and join it to the pre-existing cluster.

Perform the following procedures in this section to configure multi-host mode for the controller.

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

Perform the steps in the following procedure to configure Cisco APIC-EM as a single host using the wizard.

Before you begin

You must have either received the Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a server or virtual machine as described in the previous procedures.

Step 1 Boot up the host.

Step 2 Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed.

Note You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option to begin.

You are then prompted to enter 'yes' or 'no' for **RESET EXISTING CONTROLLER NETWORK CONFIG**.

Step 4 Select the **Reset Networking Configuration** option for your configuration.

For an initial deployment, enter 'no' and proceed with the configuration. For an upgrade for your deployment, enter 'yes' and proceed with the configuration

Note Entering 'yes' will remove the current networking configuration for the controller on this host.

You are then prompted to enter values for the **NETWORK ADAPTER BONDING mode (OPTIONAL)**.

Step 5 Select the **NETWORK ADAPTER BONDING mode (OPTIONAL)** for your configuration.

Enter either 'yes' or 'no' for this step.

Enter 'yes' to proceed with configuring NIC bonding on the interfaces (create a single logical port from two Ethernet ports (NICs) on the controller). Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration (see Step 7 below).

After entering a value, click **next>>** to proceed.

Step 6 If you entered 'yes', then enter the bonding mode in the **NETWORK ADAPTER 0 (bond0)** screen.

Enter either 'balance-xor' or '802.3ad' for this step.

This step permits you to create a single logical port from two or more Ethernet ports (NICs) on the controller that the configuration wizard discovers and displays. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs.

For this release, only a single bonded interface with multiple NICs can be configured on the controller.

Important Entering '802.3ad' requires a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches.

Step 7 Select the individual Ethernet ports (for example, eth0 and eth1) to bond together as a single logical port.

Use the **Tab** key to navigate to the Ethernet port fields in the configuration wizard. User the **space bar** to select (check) the Ethernet port.

Note When navigating to an Ethernet port, the configuration wizard displays the port's MAC address and speeds (in Mb/s). Both the actual and supported speeds are displayed. The actual speed is defined as the negotiated speed retrieved from the kernel itself (when the interface is down, 'NA' will be displayed). The supported speed is defined as the maximum speed supported by the NIC.

When finished with this step, click **next>>** to proceed.

Step 8 Select the **NETWORK ADAPTER VLAN Mode (Optional)**

Enter either 'yes' or 'no' for this step.

Entering 'yes' permits you to configure VLANs on the interface(s) in the next step. Entering 'no' bypasses VLAN configuration.

Note For a multi-host cluster, all the VLANs must be configured the same on each host.

After entering a value, click **next>>** to proceed.

Step 9 (Optional) If you entered yes, then enter the management interface in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

The management interface can be either an Ethernet port (bonded or not) or a VLAN. For a VLAN, use the following format:

interface.**vlan_id**

For example, **bond0.300** or **eth0.300**

Step 10 (Optional) Add virtual adapters for each of the interfaces in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

If you created a bonded port in the previous steps, then that bonded port will be displayed in this screen. Navigate to the bonded port displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on the bonded port.

If you did not create a bonded port in the previous steps, then each Each Ethernet port discovered by the configuration wizard will be displayed in this screen. Navigate to the Ethernet ports displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on these Ethernet ports.

Note You can use a comma separated list of VLANs (for example, 100, 200, 300) for this step. The VLAN range is limited (1-1001, 1005-4094). The same VLAN cannot be used on multiple interfaces. Up to 5 VLANs can be configured per Cisco APIC-EM cluster.

Click **next>>** to proceed.

Step 11 Enter configuration values for the **NETWORK ADAPTER #1** on the host.

The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has three network adapters you are prompted to confirm configuration values for network adapter #1 (eth0), network adapter #2 (eth1), and network adapter #3 (eth2) respectively.

Note The step header changes to reflect your prior configuration selections. For example, if you configured a bonded NIC, then the header will display **NETWORK ADAPTER #1 (bond0)**, if you configured this bonded NIC as the management interface, then the header will display **NETWORK ADAPTER #1 (bond0) MANAGEMENT INT**, and so forth.

Important The primary interface for the controller is eth0 and it is best practice to ensure that this interface is made highly available.

On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

Host IP address	Enter the host IP address to use for the network adapter. This host IP address (and network adapter) connects to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI. **Note** The configuration wizard validates the value entered and issues an error message if incorrect. If you receive an error message for the host IP address, then check to ensure that eth0 (ethernet interface) is connected to the correct network adapter.
Virtual IP	(Optional) Enter a virtual IP address to use for this network adapter. You should only configure a virtual IP address, if you are setting up a multi-host deployment. **Note** For additional information about virtual IP, see Multi-Host Deployment Virtual IP
Netmask	Enter the netmask for the network adapter's IP address.

Default Gateway IP address	Enter a default gateway IP address to use for the network adapter. **Note** If no other routes match the traffic, traffic will be routed through this IP address.
DNS Servers	Enter the DNS server or servers IP addresses (separated by spaces) for the network adapter.
Static Routes	If required for your network, enter a space separated list of static routes in this format: <network>/<netmask>/<gateway> Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes.

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation and if your host has two network adapters, you are prompted to enter values for **NETWORK ADAPTER #2 (eth1)**. If your host has three network adapters, you are prompted to enter values for **NETWORK ADAPTER #2 (eth1)** and **NETWORK ADAPTER #3 (eth2)**. If you do not have any additional network adapters or if you do not have more than one non-routable network, then proceed directly to the next step.

Step 12 If the controller is being deployed in your network behind a proxy server and the controller's access to the Internet is through this proxy server, then enter configuration values for the **HTTPS PROXY**.

Note If there is no proxy server between the controller and access to the Internet, then this step will not appear. Instead, you will be prompted to enter values for **CLOUD CONNECTIVITY**. Additionally, if the **HTTPS PROXY** step appears because the Gateway is unreachable for a short period of time due to network delay, then you can choose **Next** and skip back to the **HTTPS PROXY** step.

HTTPS Proxy	Enter the protocol (HTTP or HTTPS), IP address, and port number of the proxy. For example, enter **https://209.165.200.11:3128**
HTTPS Proxy Username	Enter the username, if authentication is required for the proxy.
HTTPS Proxy Password	Enter the password, if authentication is required for the proxy.

After configuring the **HTTPS PROXY**, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for **CLOUD CONNECTIVITY**.

Step 13 Enter configuration values for **CLOUD CONNECTIVITY**.

CCO Username	Enter a Cisco Connection Online (CCO) username for cloud connectivity. For example, enter the username that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner. **Note** If you don't have a CCO username and password or if you don't want access to cisco.com from your APIC-EM installation, then fill out the **Username** and **Password** fields with any information, but ensure that you do not include spaces in the username. This will permit you to proceed through the config-wizard process. Values entered for this field are used for telemtry collection. For information about telemtry collection, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrators Guide*.
CCO Password	Enter a Cisco Connection Online (CCO) password for the CCO *username*. For example, enter the password that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner.
Company Name	Enter the company or organization's name with which you are affiliated.

Once satisfied with the cloud connectivity settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values entered. After validation, you are then prompted to enter values for the **LINUX USER SETTINGS**.

Step 14 Enter configuration values for the **LINUX USER SETTINGS**.

Linux Password	Enter a Linux password. The Linux password is used to ensure security for both the Grapevine root and clients located on the host (appliance, server, or virtual machine). Access to the Grapevine root and clients by you or the controller requires this password. The default username is grapevine. For information about the requirements for a Linux password, see the Password Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **Note** The Linux password is encrypted and hashed in the controller database.
Re-enter Linux Password	Confirm the Linux password by entering it a second time.

Seed Phrase Password Generation	(Optional) Instead of creating and entering your own password in the above **Linux Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase. Enter a seed phrase and then press <**Generate Password**> to generate the password.
Auto Generated Password	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password. **Note** When finished with the password, be sure to save it to a secure location for future reference. Press <**Use Generated Password**> to save the password.

After configuring the Linux password, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for the **APIC-EM ADMIN USER SETTINGS**.

Step 15 Enter configuration values for the **APIC-EM ADMIN USER SETTINGS**.

Administrator Username	Enter an administrator username. Your administrator username and password are used to ensure security for the controller itself. Access to the controller's GUI requires that you enter this username and password.
Administrator Password	Enter an administrator password. For information about the requirements for an administrator password, see the Password Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **Note** The administrator password is encrypted and hashed in the controller database.
Re-enter Administrator Password	Confirm the administrator password by entering it a second time.
Seed Phrase Password Generation	(Optional) Instead of creating and entering your own password in the above **Administrator Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase. Enter a seed phrase and then press <**Generate Password**> to generate the password.

Auto Generated Password	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password. **Note** When finished with the password, be sure to save it to a secure location for future reference. Press <**Use Generated Password**> to save the password.

After configuring the administrator password, enter **next>>** to proceed.

After entering **next>>**, you are then prompted to enter values for either the **NTP SERVER SETTINGS**.

Step 16 Enter configuration values for **NTP SERVER SETTINGS**.

NTP servers	Enter a single NTP server address or a list of NTP servers each separated by a space. The Elastic Services Platform (Grapevine) manages a Network Time Protocol (NTP) server to provide time synchronization for the Grapevine clients. You must configure the NTP server for the clients. The NTP server is external to the cluster. **Note** We recommend that for redundancy purposes, you configure at least three NTP servers for your Cisco APIC-EM deployment.

Note Cisco routers can also be configured as NTP servers.

After configuring the NTP server(s), enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for **INTER-HOST COMMUNICATION**.

Step 17 Enter configuration values for **INTER-HOST COMMUNICATION**.

Enable IPSec Encryption	You can configure IPSec tunneling for communications between the hosts in a multi-host cluster. By selecting *yes*, you configure IPSec tunneling. The default is IPSec and the default option is set to *yes*.

Once satisfied with the inter-host communication setting, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 18 Enter configuration values for **CONTROLLER CLEAN-UP**.

Harvest All Virtual Disks	Entering **yes** will delete all Grapevine virtual disks that belong to the controller for this specific deployment. For an initial configuration, enter **no**.
Delete All Clients	Entering **yes** will delete all Grapevine clients that belong to the controller for this specific deployment. For an initial configuration, enter **no**.

For an initial configuration, enter **no** for both options.

After configuring the controller clean-up, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values to finish the configuration and begin the configuration wizard installation.

Step 19 A final message appears stating that the wizard is now ready to proceed with applying the configuration.

The following options are available:

- **[back]**—Review and verify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.
- **[save & exit]**—Save your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Step 20 Open your browser and enter the host IP address to access the Cisco APIC-EM GUI.

You can use the displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

Step 21 After entering the IP address in the browser, a message stating that "Your connection is not private" appears.

Ignore the message and click the **Advanced** link.

Step 22 After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.

Ignore the message and click the link.

Note This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

Step 23 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to do next

Start to use the Cisco APIC-EM to manage and configure your network. For assistance with navigating the controller's GUI and becoming familiar with the its features, use the *Cisco APIC-EM Quick Start Guide*.

If you are deploying a multi-host configuration, then review the following multi-host configuration procedure.

Note You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens an email. Use this email to send a comment on the current window or to send a request to the Cisco APIC-EM development team.

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

Perform the steps in this procedure to configure Cisco APIC-EM on your host and to join it to another, pre-existing host to create a cluster. Configuring the Cisco APIC-EM on multiple hosts to create a cluster is best practice for both high availability and scale.

Caution

- When joining a host to a cluster as described in the procedure below, there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that is being joined to.
- When joining the additional hosts to form a cluster be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- You should also expect some service downtime when the adding or removing hosts to a cluster, since the services are then redistributed across the hosts. Be aware that during the service redistribution, there will be downtime.

Before you begin

You must have performed the following prerequisites:

- You must have either received a Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a second server or virtual machine.
- You must have already configured Cisco APIC-EM on the first host (server or virtual machine) in your planned multi-host cluster following the steps in the previous procedure.
- Additionally, you must have checked the controller's health on the first host using the **SYSTEM HEALTH** tab in the GUI. The **SYSTEM HEALTH** tab is directly accessible from the **HOME** page. For information about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

This procedure must be run on the second host that you are joining to the cluster. When joining the new host to the cluster, you must specify an existing host in the cluster to connect to.

Note The Cisco APIC-EM multi-host configuration supports the following two workflows:

- You first configure a single host running Cisco APIC-EM in your network. After performing this procedure, you then use the wizard to configure and join two additional hosts to form a cluster.
- If you already have several single hosts configured with Cisco APIC-EM, you can use the configuration wizard to join two additional hosts to a single host to form a cluster.

Step 1 Boot up the host.

Step 2 Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed with the deployment.

Note You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose one of the two displayed options to begin.

- **Create a new APIC-EM cluster**
- **Add this host to an existing APIC-EM cluster**

For the multi-host deployment, click the **Add this host to an existing APIC-EM cluster** option.

You are then prompted to enter values for the **NETWORK ADAPTER BONDING mode (OPTIONAL)**.

Step 4 Select the **NETWORK ADAPTER BONDING mode (OPTIONAL)** for your configuration.

Enter either 'yes' or 'no' for this step.

Enter 'yes' to proceed with configuring NIC bonding on the interfaces (create a single logical port from two Ethernet ports (NICs) on the controller). Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration (see Step 7 below).

After entering a value, click **next>>** to proceed.

Step 5 If you entered 'yes', then enter the bonding mode in the **NETWORK ADAPTER 0 (bond0)** screen.

Enter either 'balance-xor' or '802.3ad' for this step.

This step permits you to create a single logical port from two or more Ethernet ports (NICs) on the controller that the configuration wizard discovers and displays. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs.

For this release, only a single bonded interface with multiple NICs can be configured on the controller.

Important Entering '802.3ad' requires a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches.

Step 6 Select the individual Ethernet ports (for example, eth0 and eth1) to bond together as a single logical port.

Use the **Tab** key to navigate to the Ethernet port fields in the configuration wizard. User the **space bar** to select (check) the Ethernet port.

Note When navigating to an Ethernet port, the configuration wizard displays the port's MAC address and speeds (in Mb/s). Both the actual and supported speeds are displayed. The actual speed is defined as the negotiated speed retrieved from the kernel itself (when the interface is down, 'NA' will be displayed). The supported speed is defined as the maximum speed supported by the NIC.

When finished with this step, click **next>>** to proceed.

Step 7 Select the **NETWORK ADAPTER VLAN Mode (Optional)**

Enter either 'yes' or 'no' for this step.

Entering 'yes' permits you to configure VLANs on the interface(s) in the next step. Entering 'no' bypasses VLAN configuration.

Note For a multi-host cluster, all the VLANs must be configured the same on each host.

After entering a value, click **next>>** to proceed.

Step 8 (Optional) If you entered yes, then enter the management interface in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

The management interface can be either an Ethernet port (bonded or not) or a VLAN. For a VLAN, use the following format:

interface.**vlan_id**

For example, **bond0.300** or **eth0.300**

Step 9 (Optional) Add virtual adapters for each of the interfaces in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

If you created a bonded port in the previous steps, then that bonded port will be displayed in this screen. Navigate to the bonded port displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on the bonded port.

If you did not create a bonded port in the previous steps, then each Ethernet port discovered by the configuration wizard will be displayed in this screen. Navigate to the Ethernet ports displayed on the screen using the **Tab** key on your keyboard.

Proceed to configure one or more VLANs on these Ethernet ports.

Note You can use a comma separated list of VLANs (for example, 100, 200, 300) for this step. The VLAN range is limited (1-1001, 1005-4094). The same VLAN cannot be used on multiple interfaces. Up to 5 VLANs can be configured per Cisco APIC-EM cluster.

Click **next>>** to proceed.

Step 10 Enter configuration values for the **NETWORK ADAPTER #1** on the host.

The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has two network adapters you are prompted to confirm configuration values for network adapter #1 (eth0) and network adapter #2 (eth1).

Note The step header changes to reflect your prior configuration selections. For example, if you configured a bonded NIC, then the header will display **NETWORK ADAPTER #1 (bond0)**, if you configured this bonded NIC as the management interface, then the header will display **NETWORK ADAPTER #1 (bond0) MANAGEMENT INT**, and so forth.

Important On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

Host IP address	Enter a host IP address to use for the network adapter. This host IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.

Netmask	Enter the netmask for the network adapter's IP address.

Later in this procedure, the following information will be discovered and copied from the cluster to the configuration file of this host:

- Default Gateway IP address
- DNS Servers
- Static Routes

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation, you are then prompted to enter values for the **APIC-EM CLUSTER SETTINGS**.

Step 11 Enter configuration values for the **APIC-EM CLUSTER SETTINGS**.

Remote Host IP	Enter the eth0 IP address of the pre-configured host that you are now joining to form a cluster. **Note** If a virtual IP address has already been configured on another host for a multi-host cluster, you may also enter that IP address value. This field accepts either the IP address of a pre-configured host to the cluster or the virtual IP address of the cluster.
Administrator Username	Enter an administrator username. This is the administrator username on the pre-configured host that you are now joining to form a cluster.
Administrator Password	Enter an administrator password. This is the administrator password on the pre-configured host that you are now joining to form a cluster. For information about the requirements for an administrator password, see the Password Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **Note** The administrator password is encrypted and hashed in the controller database.

After configuring the administrator cluster settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard then proceeds to prepare the host to join the cluster.

You will receive a message to please wait, while the remote cluster is being queried and data is retrieved.

Step 12 Enter configuration values for the **Virtual IP**.

Note If you are joining the host to a cluster where the virtual IP has already been configured, then you will not be prompted for virtual IP configuration values. If you are joining the host to a cluster where a virtual IP has not yet been configured, then you will be prompted for virtual IP configuration values.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to. **Note** For additional information about virtual IP, see Multi-Host Deployment Virtual IP

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 13 (Optional) Enter additional configuration values for the **Virtual IP**.

The configuration wizard proceeds to continue its discovery of any pre-existing configuration values on the hosts in the cluster. Depending upon what the configuration wizard discovers, you may be prompted to enter additional configuration values. For example:

- If eth1 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth1. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth2 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth2. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth3 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for this eth3. You are also prompted for a VIP, if it has not yet been configured for this NIC.

Note This configuration wizard discovery process and prompting continues for the number of configured Ethernet ports in the cluster.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to.
IP address	Enter an IP address to use for this network adapter. This IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 14 A final message appears stating that the wizard is now ready to proceed to join the host to the cluster.

The following options are available:

- **[back]**—Review and verify or modify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin the process to join this host to the specified Cisco APIC-EM.

Enter **proceed>>** to proceed. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

At the end of the configuration process, a successful configuration message appears.

Step 15 Open your browser and enter an IP address to access the Cisco APIC-EM GUI.

You can use the first displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

Note The first displayed IP address can be used to access the Cisco APIC-EM GUI. The second displayed IP address accesses the network where the devices reside.

Step 16 After entering the IP address in the browser, a message stating that "Your connection is not private" appears.

Ignore the message and click the **Advanced** link.

Step 17 After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.

Ignore the message and click the link.

Note This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

Step 18 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to do next

Proceed to follow the same procedure described here to join the third and final host to the multi-host cluster.

After configuring each host be sure to check the controller's health on the host using the **SYSTEM HEALTH** tab in the GUI. The **SYSTEM HEALTH** tab is directly accessible from the **HOME** page. For information about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Note You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens an email. Use this email to send a comment on the current window or to send a request to the Cisco APIC-EM development team.

Managing Admin Accounts

Admin User Right Differences

The usernames and passwords that you configure by using the Cisco APIC-EM configuration wizard are intended to be used for administrative access to the Cisco APIC-EM Grapevine root (Linux) and the Cisco APIC-EM GUI interface.

The administrator that has access to the Cisco APIC-EM Grapevine root is called the Linux admin user. By default, the username for the Linux admin user is 'grapevine' and the password is user-defined during the configuration wizard setup process. There is no default password.

Both the username and password for the Cisco APIC-EM GUI is user-defined during the configuration wizard process. There is no default username or password.

The Cisco APIC-EM Linux admin user has different rights and capabilities than the Cisco APIC-EM GUI-based admin user and can perform other administrative tasks.

Tasks Performed by Linux (Grapevine) Admin Users

The following tasks can be performed by the Linux (Grapevine) admin user:

- Displaying audit and system logs on the Cisco APIC-EM.
- Reviewing the status of Cisco APIC-EM services on the appliance.
- Resetting the configuration values back to their original configuration settings.
- Restoring the Cisco APIC-EM back to the factory default.
- Creating a support file that you can then email to Cisco support for assistance.
- Updating or changing your Cisco APIC-EM configuration wizard settings (for example, updating the NTP configuration settings).

GUI-based admin users that are created by using the Cisco APIC-EM user interface cannot automatically log into the Cisco APIC-EM and access the Grapevine root and clients located on the appliance. Only Linux admin users can access the Cisco APIC-EM Grapevine root and clients on the appliance.

Note See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide* for information about the supported Grapevine root (Linux) commands and accessible logs.

Tasks Performed by GUI Admin Users

The following tasks can be performed by the GUI admin user:

- Initiate and work with the base applications (Discovery, Inventory, Topology, Path Trace, and EasyQoS) and solution applications (Network PnP and iWAN).
- Back up and restore the Cisco APIC-EM database and files.
- Display the service logs on the Cisco APIC-EM.
- Apply Cisco APIC-EM software patches, maintenance releases, and upgrades.

Note See the following for detailed information about the above supported controller GUI operations:

- *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*

Creating GUI Admin Users

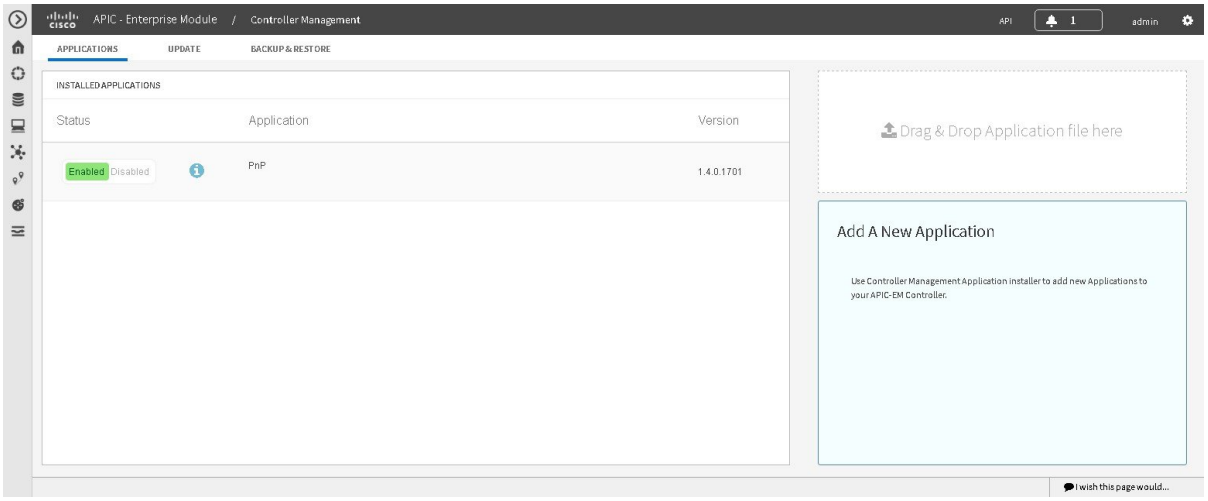
For first-time GUI-based access to Cisco APIC-EM system, the administrator username and password is configured during the configuration wizard setup.

Note You can add GUI admin users through the GUI interface itself. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide* for more information.

Installing Cisco APIC-EM Applications

The application installation procedure is simple, the application bundle provided by Cisco must be dropped in the browser window under **admin** (Settings Icon) in **App Management**.

Figure 1: App Management Window



Perform the following procedure to install additional applications.

Important Perform this procedure only after you have completed your Cisco APIC-EM configuration. If you are setting up a multi-host Cisco APIC-EM configuration, then perform this procedure when finished setting up all of the hosts in your multi-host configuration.

Before you begin

You have installed Cisco APIC-EM, following the procedures described in this guide.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 Download the application bundle or bundles from Cisco.com.

Save the bundle or bundles to a secure location on your laptop or network.

Step 2 In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:

https://*IP address*

Step 3 On the launch page, enter your username and password.

The **Home** window of the APIC-EM controller now appears.

Step 4 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 5 Click the **App Management** link from the drop-down menu.

Step 6 Drag and drop the application bundle onto the dedicated drag and drop field of the **App Management** window on the browser.

Note This step initiates the application installation process which can take several minutes to complete

Step 7 Once the application is uploaded and installed, toggle the switch next to the application's name to enable it.

What to do next

If needed for your network deployment, repeat the above steps to upload, install, and enable another application.

Powering Down and Powering Up a Single-Host or Multi-Host Cluster

Under certain circumstances such as troubleshooting, you might want to gracefully power down and then power up either a single-host or an entire multi-host cluster. This procedure describes how to perform these procedures.

For information about powering down and powering up only a single host within a multi-host cluster, see Powering Down and Powering Up a Single Host Within a Multi-Host Cluster, on page 25.

Before you begin

You should have installed the Cisco APIC-EM following the procedures in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **harvest_all_clients** command to harvest (gracefully shut down) all services on a single host or on multiple hosts within a multi-host cluster.

```
$ sudo /home/grapevine/bin/harvest_all_clients
```

Important For a multi-host cluster, you only need to enter this command on one of the hosts to harvest (gracefully shut down) all services on all of hosts in the cluster.

Step 4 Review the command output and subsequent directions.

```
$ sudo /home/grapevine/bin/harvest_all_clients

Disabled Grapevine policy
Harvesting client 1f481f49-fabc-44f9-af5a-0481bd823165...
Harvesting client 6dac3f56-fb05-4fd0-be06-d5c6869e23cd...
Harvesting client c800924c-7603-4092-b1f8-0c19f5141acc...
Waiting on task 05b9192c-9484-11e6-bdc2-0050569f3bee...
Task '05b9192c-9484-11e6-bdc2-0050569f3bee' completed successfully
Waiting on task 05da80da-9484-11e6-bdc2-0050569f3bee...
Task '05da80da-9484-11e6-bdc2-0050569f3bee' completed successfully

Successfully harvested all clients

PLEASE NOTE:
Grapevine policy has been DISABLED so that services and clients can be harvested.
To start all services again, run the following command:

   grape config update enable_policy true
```

Step 5 Power down the host, by entering the following command:

```
$ sudo shutdown -h now
```

Enter your password a second time when prompted.

For a multi-host cluster, you will need to enter this command on each of the hosts in the multi-host cluster to shut them all down.

Important You need to ensure that the last host that was shutdown in a multi-host cluster is the very first host that is then restarted. Be sure to track the order in which the hosts are shutdown in a multi-host cluster.

Step 6 Review the command output as the host shuts down.

Note The **sudo shutdown** command also powers off the host.

Step 7 Power up the Grapevine root process by turning the host or hosts (in a multi-host cluster) back on.

Important For a multi-host cluster, be sure to restart the host that was shutdown last in the multi-host cluster. This must be the first host restarted.

Step 8 Using a Secure Shell (SSH) client, log back into the host with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 9 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 10 Enable Grapevine, by entering the following command on the Grapevine root:

```
$ grape config update enable_policy true
```

Wait a few minutes for the Cisco APIC-EM services to start up again.

Important For a multi-host cluster, you only need to enter this command on one of the hosts after all of the hosts have been successfully powered on.

What to do next

Log back into the controller's GUI and begin working with the Cisco APIC-EM to manage and monitor the devices within your network.

Powering Down and Powering Up a Single Host Within a Multi-Host Cluster

Under certain circumstances such as troubleshooting, you might want to gracefully power down and then power up only a single host within a multi-host cluster. For example, to perform maintenance on that host while keeping the Cisco APIC-EM controller running and functional. This procedure describes how to perform this procedure.

Important This procedure uses the **grape host evacuate** command. The **grape host evacuate** command only works in a 3 host cluster (not a 1 or 2 host cluster). For a 2 host cluster, instead of using **grape host evacuate** command, use the standard host removal process to first remove the host you want to remove from the cluster, then reattach it back into the cluster. For detailed information, see "Troubleshooting Cisco APIC-EM Multi-Host" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

Before you begin

You should have deployed the Cisco APIC-EM following the procedures in this guide.

All of the hosts in a multi-host cluster need to be functional and running prior to beginning this procedure.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **grape host display** command to review the command output and determine the *host_id* of the host that you want to power off.

Step 4 Enter the **grape host evacuate** command to harvest (gracefully shut down) the services on the host.

Use the *host_id* for this command that you determined in the previous step.

```
$ grape host evacuate host_id
```

This command harvests all services running on the specified host (*host_id*) using the **grape host evacuate** command. In a multi-host cluster, the services on the specified host are harvested and transferred to the other two hosts in the cluster.

Important The **grape host evacuate** command only works in a 3 host cluster (not a 1 or 2 host cluster). For a 2 host cluster, instead of using **grape host evacuate** command, use the standard host removal process to first remove the host you want to remove from the cluster, then reattach it back into the cluster. For detailed information, see "Troubleshooting Cisco APIC-EM Multi-Host" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

Step 5 Power down the host, by entering the following command:

```
$ sudo shutdown -h now
```

Note Enter your password a second time when prompted.

Step 6 Review the command output as the host shuts down.

Note The **sudo shutdown** command also powers off the host.

Step 7 Power up the Grapevine root process by turning the host back on.

Step 8 Using a Secure Shell (SSH) client, log back into the host with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 9 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 10 Enable Grapevine, by entering the following command on the Grapevine root:

```
$ grape host enable host_id
```

The host ID to enter for this command must be the same as the host ID used in the **grape host evacuate** command in step 4.

Wait a few minutes for the Cisco APIC-EM services to start up again.

What to do next

Log back into the controller's GUI and begin working with the Cisco APIC-EM to manage and monitor the devices within your network.

Uninstalling the Cisco APIC-EM

The following procedure describes how to uninstall the Cisco APIC-EM.

Note If you plan to reinstall the Cisco APIC-EM after uninstalling it, then you must follow the procedure described below to avoid any possible problems. You should have also contacted Cisco support for the link to download the latest Cisco APIC-EM ISO image. Be aware that this procedure shuts down both the Cisco APIC-EM and the host (physical or virtual) on which it resides. At the end of this procedure and if you are reinstalling the Cisco APIC-EM, then you will need to access the host and restart it.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 Enter the Linux username ('grapevine') and password when prompted.

Step 3 Enter the **reset_grapevine factory** command at the prompt.

```
$ reset_grapevine factory
```

Step 4 Enter your Linux grapevine password a second time to start the reset process.

```
$ sudo password for grapevine *********
```

After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

You are then prompted to confirm your intent to run the **reset_grapevine factory** command.

Step 5 Enter **Yes** to confirm that you want to run the **reset_grapevine factory** command.

The controller then performs the following tasks:

- Stops all running clients and services
- Stops and shuts down any Linux containers
- Deletes all cluster data
- Deletes all user data
- Deletes the configuration files including secrets and private keys
- Shuts down the controller
- Shuts down the host (physical or virtual)