Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide, Release 1.2.x

First Published: May 25, 2016

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

CONTENTS

Preface

Audience

This publication is for experienced network administrators who will upgrade the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) in their network. Use this guide to upgrade your current version of the Cisco APIC-EM.

For additional information about deployment, security, and access for the Cisco APIC-EM, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* .

For information about using the controller's GUI for the first time, see the *Cisco APIC-EM Quick Start Guide*.

Note The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to within this upgrade guide as a controller.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.

Convention	Description
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

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

Tip Means *the following information will help you solve a problem.*

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

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

- Cisco APIC-EM Documentation:
  - *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*
  - *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
  - *Open Source Used In Cisco APIC-EM*
- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network (Cisco IWAN)*
  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*
- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*

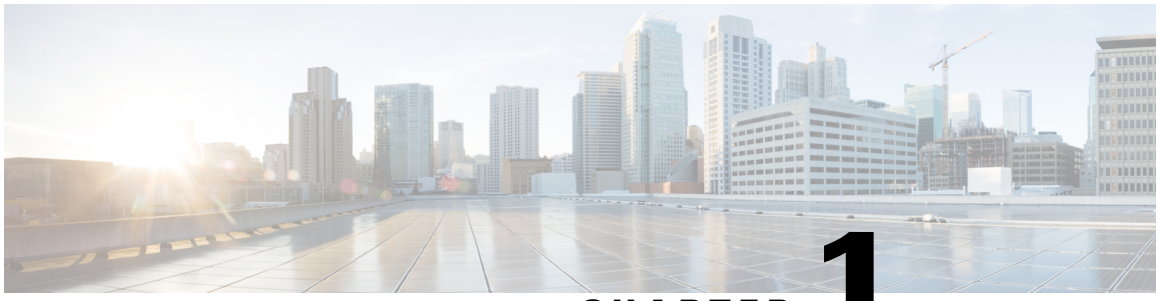
- *Solution Guide for Cisco Network Plug and Play*
- *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
- *Cisco Open Plug-n-Play Agent Configuration Guide*
- *Mobile Application User Guide for Cisco Network Plug and Play*

Note For information about developing your own application that interacts with the controller by means of the northbound REST API, see the developer.cisco.com/site/apic-em Web site.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.



CHAPTER 1

Before You Begin

Read the following information carefully, before you begin an upgrade.

Review Supported Upgrade Paths

You can directly upgrade to Cisco APIC-EM, Release 1.2.0.x from any of the following releases:

- 1.1.2.15
- 1.1.1.38
- 1.1.1.34
- 1.1.0.767
- 1.0.3.4
- 1.0.2.8

If you encounter any problems with upgrading from releases 1.0.2.8 or 1.0.3.4, then see the release notes for the workaround procedure. If you using a release version earlier than the above Cisco APIC-EM releases, then you must first upgrade to one of the releases listed above (with the latest patch) and then upgrade to Release 1.2.0.x.

Review Time Taken for Upgrade

The upgrade process for the Cisco APIC-EM may take up to approximately 60 minutes to complete. The actual time taken for an upgrade varies depending upon a number of factors, including the scale of your network deployment, number of endpoints involved, and applications in use (EasyQoS, IWAN, and Network Plug and Play).

Note Services will be restarted at different times during the upgrade process and for this reason, not all the applications will start up at once.

Review Available Cisco APIC-EM Ports

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.

The following table lists Cisco APIC-EM ports that permit *incoming* traffic into the controller.

Table 1: Cisco APIC-EM Incoming Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH	TCP
67	bootps	UDP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443	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
14141	Grapevine console	TCP
16026	SCEP	TCP

The following table lists Cisco APIC-EM ports that are used for *outgoing* traffic from the controller.

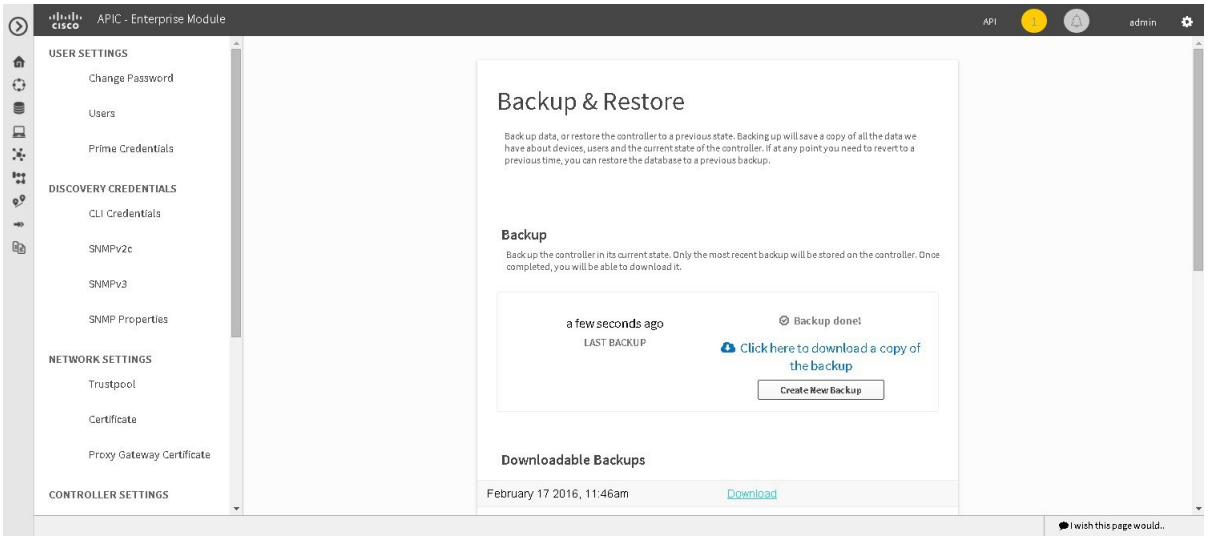
Table 2: Cisco APIC-EM Outgoing Traffic Port Reference

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

Back Up the Controller Database and Files

Before performing an upgrade, you should back up your controller's database and files using the **Backup & Restore** window of the GUI.

Figure 1: Backup & Restore Window



Note In a multi-host cluster, the database and files are replicated and shared across three hosts. When backing up and restoring in a multi-host cluster, you need to first back up on only one of the three hosts in the cluster. For detailed information about both back up and restore, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Before You Begin

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Step 1 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Backup & Restore** to view the **Backup & Restore** window.

Step 4 In the **Backup & Restore** window, create a backup file by clicking on the **Create New Backup** button. After clicking the **Create New Backup** button, a **Backup in Progress** window appears in the GUI.

During this process, the Cisco APIC-EM creates a compressed *.backup* file of the controller database and files. This backup file is also given a time and date stamp that is reflected in its file name. The following file naming convention is used: *yyyy-mm-dd-hh-min-seconds* (year-month-day-hour-seconds).

For example:

backup_2015_08_14-08-35-10

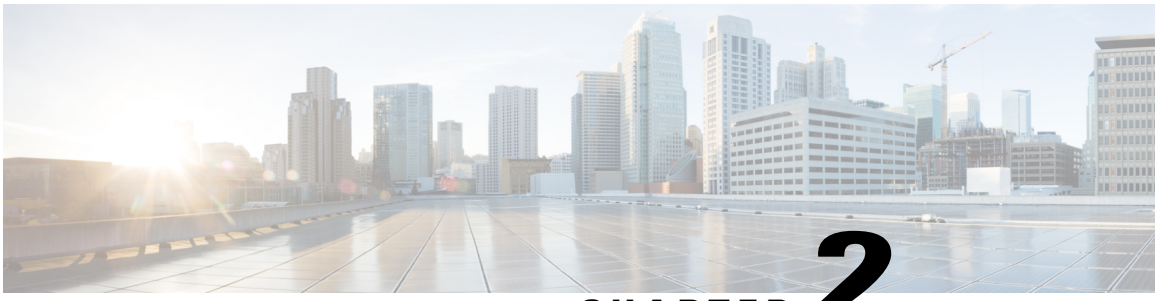
Note If necessary, you can rename the backup file instead of using the default time and date stamp naming convention.

This backup file is then saved to a default location within the controller. You will receive a **Backup Done!** notification, once the back up process is finished. Only a single backup file at a time is stored within the controller.

Note If the back up process fails for any reason, there is no impact to the controller and its database. Additionally, you will receive an error message stating the cause of the back up failure. The most common reason for a failed back up is insufficient disk space. If your back up process fails, you should check to ensure that there is sufficient disk space on the controller and attempt another back up.

Step 5 (Optional) Create a copy of the backup file to another location.
After a successful back up, a **Download** link appears in the GUI. Click the link to download and save a copy of the backup file to a secure location on your network.

Note For information about restoring a controller backup file, see *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.



CHAPTER 2

Upgrading the Cisco APIC-EM Deployment

Review the following sections in this chapter for information about upgrading to the latest Cisco APIC-EM version and verification.

Using the GUI to Upgrade Cisco APIC-EM

The GUI upgrade procedure requires that you perform the following tasks:

1. Download the release upgrade pack from the secure Cisco website at the Download Software link.
2. Run a checksum against the release upgrade pack.
3. Upload the release upgrade pack to the controller using the GUI.
4. Update the controller's software with the release upgrade pack using the GUI.

Note In a multi-host cluster, when you begin the update process on a single host it triggers the update process on all the other hosts in the cluster. When the update process is finished, all the hosts in the cluster will have the same configuration. If you are updating a multi-host cluster with the latest software release (1.2.0.x) and also want to configure IPSec tunneling between the hosts, then follow this procedure: Upgrading to Cisco APIC-EM, Release 1.2.0.x and Enabling IPSec for a Multi-Host Cluster, on page 11.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have received notification from Cisco that the Cisco APIC-EM software upgrade is available to download from the secure Cisco website.

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Important This procedure should be read with the latest version of the Cisco APIC-EM release notes, as there may be specific additional requirements for that release's upgrade. The latest release for Cisco APIC-EM is release 1.2.0.x. If you are upgrading to this version, then you should first review the *Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*, Release 1.2.0.x before beginning this procedure.

Step 1 Review the information in the Cisco notification about the Cisco APIC-EM upgrade.
The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

Note The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific upgrade. The release upgrade pack can be as large as several Gigabits.

Step 2 Download the Cisco APIC-EM upgrade package from the Cisco website at the Download Software link.
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

Note Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

Step 3 Run a checksum against the file using your own checksum verification tool or utility (either MD5 or SHA512).

Step 4 Review the displayed checksum verification value from your checksum verification tool or utility.
If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

Step 5 Upload the upgrade package to the controller using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 6 Update the controller's software with the upgrade package using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 7 Check the controller's software version number in the GUI **Home** window. The GUI **Home** window should display the new software version.

Note Upgrading from earlier releases to the latest Cisco APIC-EM release may take up to an hour to complete.

What to Do Next

Verify the upgrade process, see Verifying the Upgrade Process, on page 14.

Using the CLI to Upgrade Cisco APIC-EM

The CLI upgrade procedure requires that you perform the following tasks:

1. Download the release upgrade pack (.tar.gz file) from the secure Cisco website at the Download Software link.
2. Run a checksum against the file.
3. Save the file to a location on your appliance, server, or virtual machine.
4. Run the Grapevine upgrade command on the file.

Note In a multi-host cluster, when you begin the update process on a single host it triggers the update process on all the other hosts in the cluster. When the update process is finished, all the hosts in the cluster will have the same configuration. If you are updating a multi-host cluster with the latest software release (1.2.0.x) and also want to configure IPSec tunneling between the hosts, then follow this procedure: Upgrading to Cisco APIC-EM, Release 1.2.0.x and Enabling IPSec for a Multi-Host Cluster, on page 11.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have received notification from Cisco that the Cisco APIC-EM software upgrade is available to download from the secure Cisco website.

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Important This procedure should be read with the latest version of the Cisco APIC-EM release notes, as there may be specific additional requirements for that release's upgrade. The latest release for Cisco APIC-EM is release 1.2.0.x. If you are upgrading to this version, then you should first review the *Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*, Release 1.2.0.x before beginning this procedure.

Step 1 Review the information in the Cisco notification about the Cisco APIC-EM upgrade.

The Cisco notification specifies the location of the release upgrade pack and verification values for either a Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) 512 bits (SHA512) checksum.

Note The Cisco APIC-EM release upgrade pack is a bit file that varies in size based upon the requirements of the specific upgrade. The release upgrade pack can be as large as several Gigabits.

Step 2 Download the Cisco APIC-EM upgrade package from the Cisco website at the Download Software link.
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- Service files
- Grapevine files
- Linux files

Note Each release upgrade pack contains an encrypted Cisco signature for security purposes, as well as release version metadata that validates the package.

Step 3 Run a checksum against the file using your own checksum verification tool or utility (either MD5 or SHA512).

Step 4 Review the displayed checksum verification value from your checksum verification tool or utility.
If the output from your checksum verification tool or utility matches the appropriate checksum value in the Cisco notification or from the Cisco secure website, then proceed to the next step. If the output does not match the checksum value, then download the release upgrade pack and perform another checksum. If checksum verification issues persist, contact Cisco support.

Step 5 Copy or move the file from your laptop or secure network location to the appliance, server, or virtual machine with the controller.

Step 6 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.

Step 7 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 8 Navigate to the folder where the file is located and run the following command:

```
$ grape update upload [path-to-upgrade-package]
```

The **grape update upload** command will proceed to upgrade (upload and then update) the controller with the file.

You should refrain from working with the controller during the entire upgrade process. During the upgrade process, the controller may shut down and restart. The shut down process may last for several minutes. A percentage bar will appear to show the upload progress. Once the upload process completes, you will receive notification of its completion and of the beginning of the update process.

```
Release upgrade package uploaded successfully, Update process started.
task_id: 8507f3f6-1de2-11e6-bf7e-00505695af10
```

Note At the beginning of the update process, the controller performs a second verification test on the release upgrade pack. The release upgrade pack itself contains an encrypted security value (signature) that will be decrypted and reviewed by the controller. This second verification test ensures that the release upgrade pack that has been uploaded is from Cisco. The release upgrade pack must pass this second verification test before the upgrade process can continue.

Tip Use **grape task display** *task_id* command to monitor progress of the update task. Use the update task ID found in the notification.

Step 9 Once the upgrade process finishes (upload and update), you will receive a success or failure notification.

If the upgrade was successful, you will receive a successful upgrade notification and can then proceed working with the controller. If the upgrade was unsuccessful, you will receive an unsuccessful upgrade notification with suggested remedial actions to take.

What to Do Next

Verify the upgrade process, see Verifying the Upgrade Process, on page 14.

Upgrading to Cisco APIC-EM, Release 1.2.0.x and Enabling IPSec for a Multi-Host Cluster

You can upgrade to Cisco APIC-EM release 1.2.0.x using the **Software Update** functionality of the controller's GUI. For upgrading an *existing* multi-host cluster to Cisco APIC-EM release 1.2.0.x and configure IP Security (IPSec) tunneling for inter-host communications, then you must take additional steps.

Follow the steps described below to upgrade your *existing* multi-host cluster and configure IPSec tunneling. The steps must be performed in the following order:

1. Download and update the controller software on one of the hosts (steps 1-5).
2. Break up or disassemble your multi-host cluster (steps 6-10).
3. Reboot all the hosts in the multi-host cluster that you just disassembled (step 11).
4. Configure IPSec tunneling on the last host that was in your cluster (steps 12-16).
5. Reassembly your multi-host cluster around that last host where you configured IPSec tunneling (steps 17-26).

Note If you are upgrading to a multi-host cluster from only a single host (not an *existing* multi-host cluster) and have already updated the single host to release 1.2.0.x, then you need to first reboot that single host and then configure IPSec tunneling using the configuration wizard. After performing this procedure on that single host, when you join any new hosts to form a cluster, you must also first reboot those hosts before joining (if those new hosts were also updated to release 1.2.0.x instead of a fresh Cisco APIC-EM ISO installation). After joining the hosts to form a cluster, each host will have IPSec tunneling configured.

Before You Begin

You must have successfully deployed the Cisco APIC-EM and it must be operational.

You must have received notification from Cisco that the Cisco APIC-EM software upgrade is available to download from the secure Cisco website.

You must have administrator (ROLE_ADMIN) permissions to perform this procedure.

For information about the user permissions required to perform tasks using the Cisco APIC-EM, see the chapter, *Managing Users and Roles* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.

Important This procedure should be read with the latest version of the Cisco APIC-EM release notes, as there may be specific additional requirements for that release's upgrade. The latest release for Cisco APIC-EM is release 1.2.0.x. You should first review the *Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module*, Release 1.2.0.x before beginning this procedure.

Step 1 Download the Cisco APIC-EM upgrade package for release 1.2.0.x from the Cisco website at the Download Software link.

Step 2 Upload the upgrade package to the controller (one of the hosts in the cluster) using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 3 Update the controller's software with the upgrade package using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 4 Check the controller's software version number in the GUI **Home** window. The GUI **Home** window should display the new software version (1.2.0.x).
Note Upgrading from earlier releases to Cisco APIC-EM release 1.2.0.x may take up to an hour to complete.

Step 5 Proceed to check the software versions of the other hosts in your cluster.
Note Updating the software on one host in the cluster will cause the other hosts in the cluster to be updated with the same upgrade package.

Step 6 Using a Secure Shell (SSH) client, log into one of the hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 7 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 8 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 9 A message appears with an option to **[proceed]** and remove this host from the cluster.
Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from the cluster.
At the end of this process, this host is removed from the cluster.

Step 10 Repeat the above steps (steps 6-9) on a second host in the cluster.
Note You must repeat the above steps on each host in your cluster, until you have broken up the multi-host cluster.

Important Make a note of the final host in the cluster that you have just broken up or disassembled. You must perform the next steps (enabling IPSec) on that specific host. For example, if you have 3 hosts in a cluster (A, B , C) and you first remove host A, then remove host B, then you must enable IPSec tunneling on host C.

Step 11 Prior to enabling IPSec, reboot each of the hosts in the multi-host cluster that you just disassembled using the **sudo reboot** command.

```
$ sudo reboot
```

Step 12 Using a Secure Shell (SSH) client, log into the last host in your cluster and run the **config_wizard** command

```
$ config_wizard
```

Step 13 Review the current configuration values in the configuration wizard and click **next>>**, until you access the **INTER-HOST COMMUNICATION** screen.

Step 14 Configure IPSec tunneling for communications between the hosts in a multi-host cluster by selecting *yes*.
The default tunneling protocol used for communications between the hosts in a multi-host cluster is Generic Routing Encapsulation (GRE). By entering 'yes', you are configuring IPSec tunneling with this step.

Step 15 Click **next>>** until the last step of the configuration wizard process is reached.

Step 16 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM deployment.
At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Next, proceed to log into the other hosts previously in your multi-host cluster and use the configuration wizard to reassemble the cluster (with secure communications between the hosts).

Step 17 Using a Secure Shell (SSH) client, log into one of the other hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 18 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 19 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option.

Note Joining this other (second) host to the host with IPSec tunneling, automatically configures IPSec tunneling on this other (second) host.

Step 20 Proceed to recreate the cluster using the configuration wizard.
For additional information about this step and process, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* .

Step 21 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

Step 22 Using a Secure Shell (SSH) client, log into the third host and use the configuration wizard to join the new multi-host cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 23 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 24 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Add this host to an existing APIC-EM cluster** option.

Note Adding this host to the new multi-host cluster (with IPSec tunneling configured), automatically configures IPSec tunneling on this host.

Step 25 Proceed to add this host to the cluster using the configuration wizard.
For additional information about this step and process, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* .

Step 26 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

At the end of this step, you have updated your multi-host cluster and configured IPSec tunneling. Repeat the above steps to add any additional hosts to your multi-host cluster

What to Do Next

Verify the upgrade process, see Verifying the Upgrade Process, on page 14.

Verifying the Upgrade Process

To verify if an upgrade is successful, do one of the following:

- Check the controller's GUI.

  After the update, information about it will also appear in the **Update History** field of the **Software Update** window. The following update data is displayed in this field:

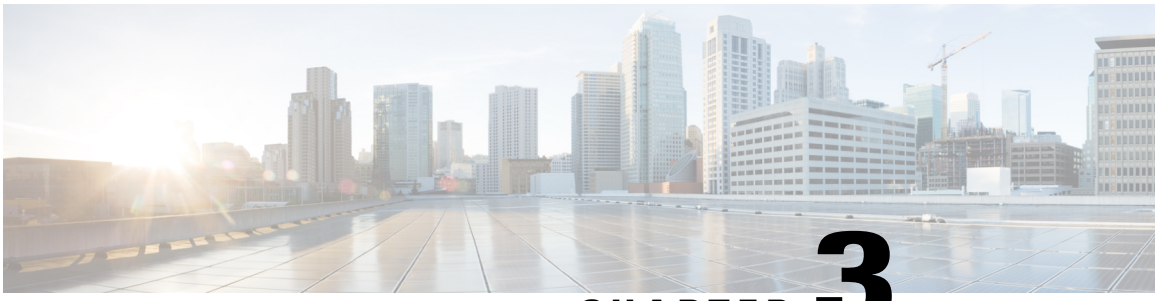
  - **Date—**Local date and time of the update
  - **User—**Username of the person initiating the update
  - **Update Version—**Update path of release upgrade pack version represented with an arrow.
  - **Update Status—**Success or failure status of the update.

  Note If you place your cursor over (mouseover) a failure status in this field, then additional details about the failure is displayed.

- Using a Secure Shell (SSH) client, log into the host (physical or virtual) with the IP address that you specified using the configuration wizard and run the following CLI commands:

  - **grape update history—**Displays update history of the controller, including individual task IDs.
  - **grape release display current—**Displays the Cisco APIC-EM software release currently running, with services and versions
  - **grape instance display—**Displays service instances and versions
  - **grape instance status—**Displays service instance status and versions

We also recommend that you run some network tests (for example, discoveries and/or path traces) to ensure that the controller functions as expected and that users are able to authenticate and access the resources on your network.



CHAPTER 3

Recovering from Upgrade Failures

Upgrade Failures

The following table describes some of the known upgrade errors and what you must do to recover from them.

Table 3: Upgrade Failures

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful upgrade on a bare-metal server.	Attempted upgrade of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a bare-metal upgrade. Try to upgrade the controller again. If failure persists, contact Cisco support. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for Cisco TAC contact information.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful upgrade on a virtual machine.	Attempted upgrade of the controller is being made without meeting the system requirements for the release.	Access the latest Cisco APIC-EM release notes and review the system requirements. Be sure to review the appropriate specific system requirements for a virtual machine upgrade, including the VMware resource pool requirements. Try to upgrade the controller again. If failure persists, contact Cisco support. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for Cisco TAC contact information.
Failed or unsuccessful upgrade on a virtual machine.	Error messages on controller indicate that there is an issue with the NTP server.	When upgrading the Cisco APIC-EM in a virtual machine within a VMware vSphere environment, you must ensure that the time settings on the ESXi host are also synchronized to the NTP server. Failure to ensure synchronization will cause the upgrade to fail. If the NTP server settings are not synchronized, use SSH to log into the controller, run the **reset_grapevine** command and update the NTP server settings. Try to upgrade the controller again. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for information about using the **reset_grapevine** command , as well as Cisco TAC contact information.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful upgrade on either a bare-metal server or virtual machine.	Error messages on the controller GUI indicate that the core services are failing to start up on the Cisco APIC-EM after the upgrade.	Try to upgrade the controller again. If failure persists, take the following actions: • Log into the developer console. • Review the status of the services in the developer console. • Create an rca file and send to support for additional assistance. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide, Release 1.2.x* for information about the above steps, as well as Cisco TAC contact information.

Reviewing System Logs and Creating a Support File for an Upgrade Failure

You can troubleshoot a Cisco APIC-EM upgrade failure by reviewing the system logs and then creating a support file. The support file consists of logs, configuration files, and command output. After you create this support file, you can then email it to Cisco support for assistance.

Step 1 Using a Secure Shell (SSH) client, log into the host (physical or virtual) 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 Navigate to the `/var/log` directory on the host. The `log` directory contains the controller system logs.

Step 4 Open and view the following log files to determine what caused the upgrade failure:

- `grapevine_manager_activity.log`
- `grapevine_manager.log`

If you are unable to determine and correct the cause of the upgrade failure, proceed to the next step.

Step 5 Navigate to the `bin` directory on the host. The `bin` directory contains the grapevine scripts.

Step 6 To create the support file, enter the **rca** command in this directory.

```
$ rca
mkdir: created directory '/tmp grapevine-rca-2016-04-05_16-22-20-PM_PDT-0700'

----------------------------------------------------------------------
RCA package created On Tues April 5 16:22:20 PDT 2016
----------------------------------------------------------------------
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains log files, configuration files, and the command output.

What to Do Next

Send the `tar` file created by this procedure to Cisco support for assistance in resolving your issue.

INDEX