Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide, Release 1.3.x

First Published: 2016-05-26

Last Modified: 2016-10-25

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface v

Audience v

Document Conventions v

Related Documentation vii

Obtaining Documentation and Submitting a Service Request viii

CHAPTER 1

Before You Begin 1

Review Supported Upgrade Paths 1

Review Time Taken for Upgrade 1

Review Available Cisco APIC-EM Ports 2

Review the Security Recommendations 4

Back Up the Controller Database and Files 5

Configure the Authenticate Timeout Value for Users 7

CHAPTER 2

Upgrading the Cisco APIC-EM Deployment 9

Using the GUI to Upgrade Cisco APIC-EM 9

Using the CLI to Upgrade Cisco APIC-EM 11

Verifying the Upgrade Process 12

CHAPTER 3

Recovering from Upgrade Failures 15

Upgrade Failures 15

Creating a Support File for an Upgrade Failure 20

Preface

- Audience, page v
- Document Conventions, page v
- Related Documentation, page vii
- Obtaining Documentation and Submitting a Service Request, page viii

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

This section lists the Cisco APIC-EM and related documents available on Cisco.com at the following url:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

- 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 Installation Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
  - *Cisco Path Trace Solution Guide*
  - *Cisco EasyQoS Solution 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 Application (Cisco IWAN App)*

- *Configuration Guide for Cisco IWAN on Cisco APIC-EM*[1]

  Cisco IWAN on Cisco APIC-EM Configuration Guide
- *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*

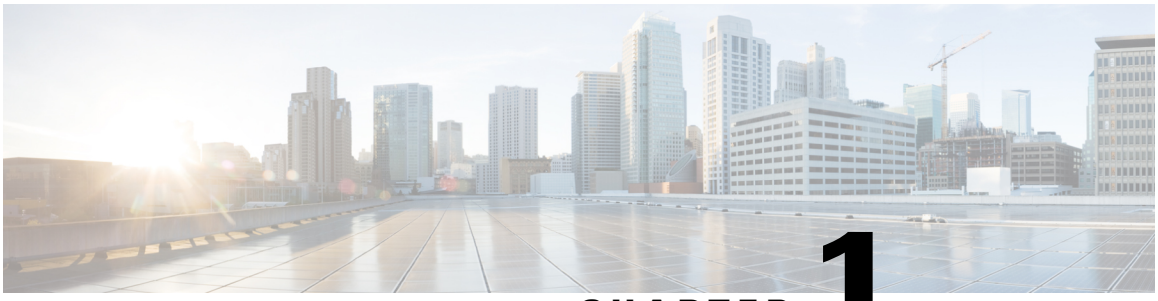
Note For information about developing your own application that interacts with the controller by means of the northbound REST API, see the developer.cisco.com/site/apic-em Web site.

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.

[1] This is an updated and renamed version of the previous version of this document (*Cisco IWAN on Cisco APIC-EM Configuration Guide*).



CHAPTER 1

Before You Begin

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

- Review Supported Upgrade Paths, page 1
- Review Time Taken for Upgrade, page 1
- Review Available Cisco APIC-EM Ports, page 2
- Review the Security Recommendations, page 4
- Back Up the Controller Database and Files, page 5
- Configure the Authenticate Timeout Value for Users, page 7

Review Supported Upgrade Paths

You can directly upgrade to Cisco APIC-EM, Release 1.3.0.x from any of the following releases:

- 1.2.1.691
- 1.2.1.686
- 1.2.0.1594
- 1.1.2.15

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 1.3.0.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.

Important The Cisco APIC-EM controller will be inoperable during the upgrade process, and for this reason we recommend that you schedule the upgrade during your network off-peak hours or a maintenance time period.

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 APIs	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

Review the Security Recommendations

The Cisco APIC-EM provides many security features for the controller itself, as well as the hosts and network devices that it monitors and manages. We strongly suggest that the following security recommendations be followed when deploying the controller.

Table 3: Cisco APIC-EM Security Recommendations

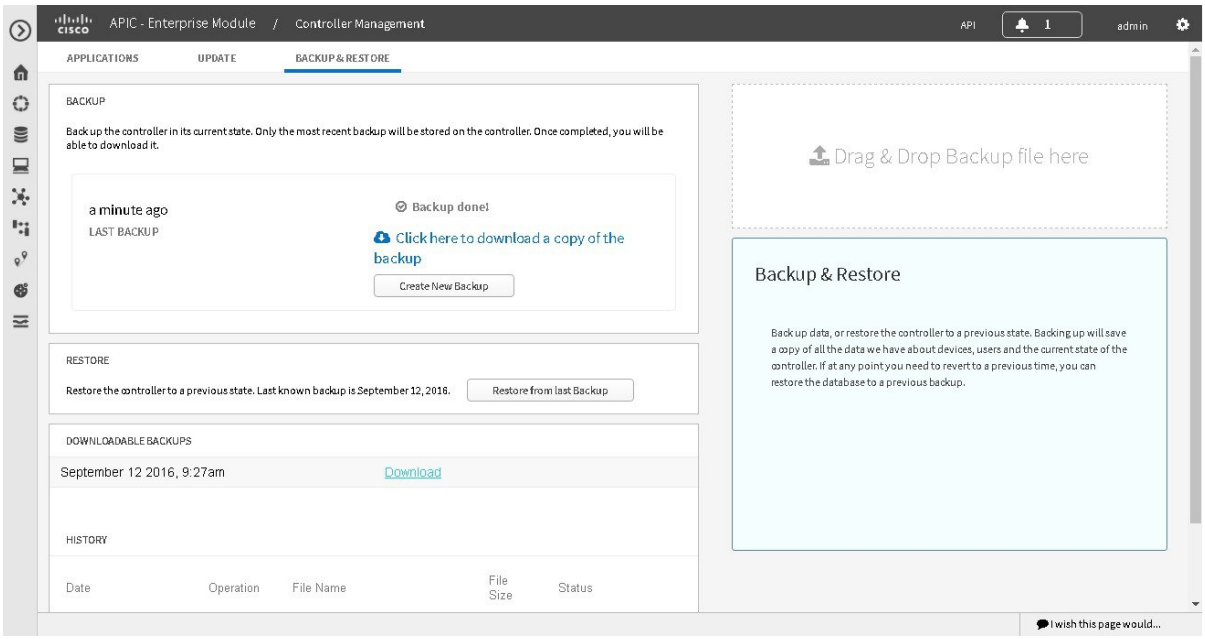
Security Recommendations	Reference
Deploy the controller behind a firewall that does not expose the controller's management ports (for example, ports 22 and 14141) to an untrusted network, such as the Internet.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Security chapter, "Cisco APIC-EM Port Reference" for information about the key controller ports.
Configure IPSec tunneling for communications between the hosts in a multi-host configuration.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Security chapter, "Configuring IPSec Tunneling for Multi-Host Communications" for information about configuring IPSec tunneling.
Configure Cisco APIC-EM HTTPS services to use TLS 1.1 or TLS 1.2, instead of TLS 1.0 (current default). TLS 1.2 is strongly preferred. However, ensure that your devices – especially those that will be introduced into the network using the Cisco APIC-EM PnP application also support TLS 1.1 and/or TLS 1.2 before choosing on a TLS version above 1.0. Additionally, make sure that any NB API consumers including the browser used to access the controller's UI are capable of communicating with TLS 1.1 or TLS 1.2. All of the browser clients supported by Cisco APIC-EM already support TLS 1.1 and above.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Security chapter, "Configuring the TLS Version Using the CLI" for information about configuring the TLS version.
Replace the self-signed server certificate from the controller with one signed by a well-known Certificate Authority.	For this security recommendation, do one of the following: • See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Importing a Certificate" for information about importing and using a certificate for the controller. • See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Importing a Trustpool bundle" for information about importing and using a trustpool for the controller.

Security Recommendations	Reference
Configure a proxy gateway between the controller and the network devices it monitors and manages.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Importing a Proxy Gateway Certificate" for information about importing and using the proxy gateway's certificate for the controller.
When using the controller's discovery functionality, use SNMPv3 with authentication and privacy enabled for the network devices.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, Settings chapter, "Configuring SNMP" for information about importing and using the proxy gateway's certificate for the controller.

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 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 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 **App Management** link from the drop-down menu.

Note In previous versions of the controller software, the **Backup and Restore** functionality was directly accessible from the **Settings** navigation pane. Although, the **Backup and Restore** option is still visible from the **Settings** navigation pane, with this release you cannot access this functionality from that GUI location.

Step 3 Click the **Backup and Restore** tab at the top of the 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*.

Configure the Authenticate Timeout Value for Users

You can configure authentication timeouts that require the user to log back into the controller with their credentials (username and password) using the **Authentication Timeout** window in the Cisco APIC-EM GUI.

Prior to beginning the software update process for the Cisco APIC-EM, we recommend that you configure the idle timeout value in the **Authentication Timeout** window of the GUI for at least an hour. If a user is logged out due to an idle timeout during the software update process, then this process will fail and need to be re-initiated again.

Before You Begin

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 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 of the controller's GUI, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

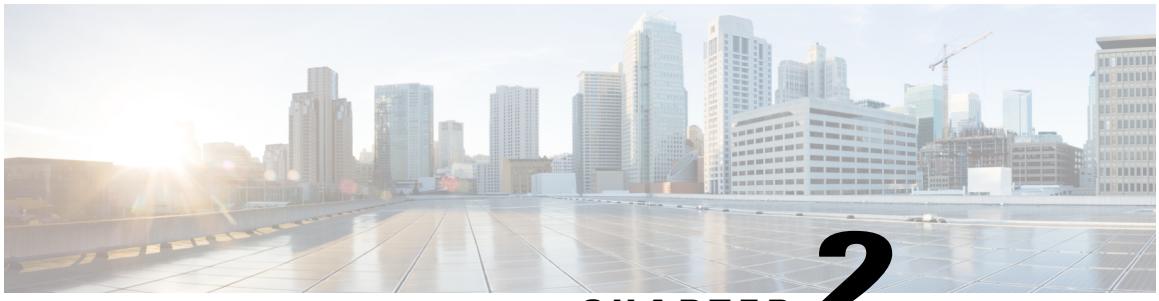
Step 2 Click the **Settings** link from the drop-down menu.

Step 3 In the **Settings** navigation pane, click **Authentication Timeout** to view the **Authentication Timeout** window.

Step 4 Configure the idle timeout value using the **Idle Timeout** drop-down menu.
You should configure the idle timeout to a value greater than one hour.

Step 5 (Optional) Configure the session timeout value using the **Session Timeout** drop-down menu.
You can configure the session timeout value in increments of 30 minutes, up to 24 hours. The default value is six hours.

Step 6 Click the **Apply** button to apply your configuration to the controller.



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, page 9
- Using the CLI to Upgrade Cisco APIC-EM, page 11
- Verifying the Upgrade Process, page 12

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.

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 and access to all devices (RBAC Scope set to ALL) 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 Administrator 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.

Note In a multi-host cluster, you only need to update a single host. After updating that single host, the other two hosts are automatically updated with the release upgrade pack.

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 **Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

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

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.

Step 7 After updating the controller's software with the upgrade package in the previous step, proceed to clear your web browser's cache.

Step 8 Check the controller's software version number in the GUI **SYSTEM INFO** tab, located in the **Home** window. The **SYSTEM INFO** tab 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 12.

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.

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 Grapevine SSH access privileges to perform this procedure.

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.

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 (see above).

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 12.

Verifying the Upgrade Process

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

- Check the controller's GUI.

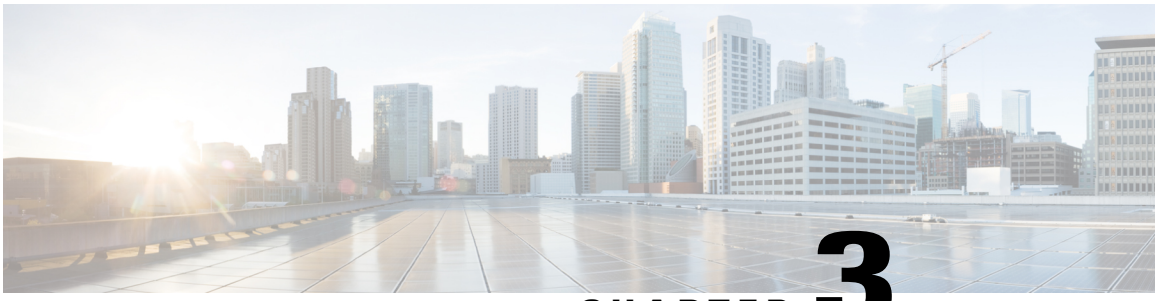
  After the update, information about it will also appear in the **Update History** field of the **Update** window. The following update data is displayed in this field:

- **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, page 15
- Creating a Support File for an Upgrade Failure, page 20

Upgrade Failures

The following table describes some possible upgrade errors that you may encounter and what you must do to recover from them.

Table 4: 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 by taking the following steps: **1** If necessary, reinstall your previous version of controller software on your server. **2** Restore the controller database and files from the backup file that you created and saved to a secure location on your network. See Back Up the Controller Database and Files, on page 5. **3** Attempt the upgrade a second time. If failure persists, contact Cisco support. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide,* 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 by taking the following steps: **1** If necessary, reinstall your previous version of controller software on your virtual machine. **2** Restore the controller database and files from the backup file that you created and saved to a secure location on your network. See Back Up the Controller Database and Files, on page 5. **3** Attempt the upgrade a second time. If failure persists, contact Cisco support. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide,* for Cisco TAC contact information.

Symptom	Possible Cause	Recommended Action
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. Try to upgrade the controller again by taking the following steps: **1** If necessary, reinstall your previous version of controller software on your virtual machine. **2** Restore the controller database and files from the backup file that you created and saved to a secure location on your network. See Back Up the Controller Database and Files, on page 5. **3** 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. **4** Attempt the upgrade a second time. If failure persists, contact Cisco support. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide,* 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's GUI indicate that some services are failing to start up on the Cisco APIC-EM after the upgrade.	Try to upgrade the controller again by taking the following steps: **1** If necessary, reinstall your previous version of controller software on your appliance, server, or virtual machine. **2** Restore the controller database and files from the backup file that you created and saved to a secure location on your network. See Back Up the Controller Database and Files, on page 5. **3** Attempt the upgrade a second time. If failure persists, take the following actions: • If possible, log into the controller's GUI. • Review the status of the services in the **System Health** tab and note any failed services. • Proceed to create an rca file, see Creating a Support File for an Upgrade Failure, on page 20. • Send the rca file with any information about failed services displayed in the controller's GUI to support for additional assistance. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide,* for information about the above steps, as well as Cisco TAC contact information.

Creating a Support File for an Upgrade Failure

You can troubleshoot a Cisco APIC-EM upgrade failure by creating a root cause analysis (rca) support file. The rca file consists of logs, configuration files, and command output. After you create this rca 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 `bin` directory on the host. The `bin` directory contains the grapevine scripts.

Step 4 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 upgrade issue.

INDEX

A

audience v
authenticate timeout 7

B

backing up controller 5

R

related documentation vii

S

software update 9, 11
    CLI 11
    GUI 9
system logs 20

T

time 1

U

upgrade failures 15