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

You can update the Cisco APIC-EM to the latest version using the controller's GUI update procedure. This procedure requires that you perform the following tasks:

1. Download the release upgrade pack from the secure Cisco cloud.
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.

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

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.

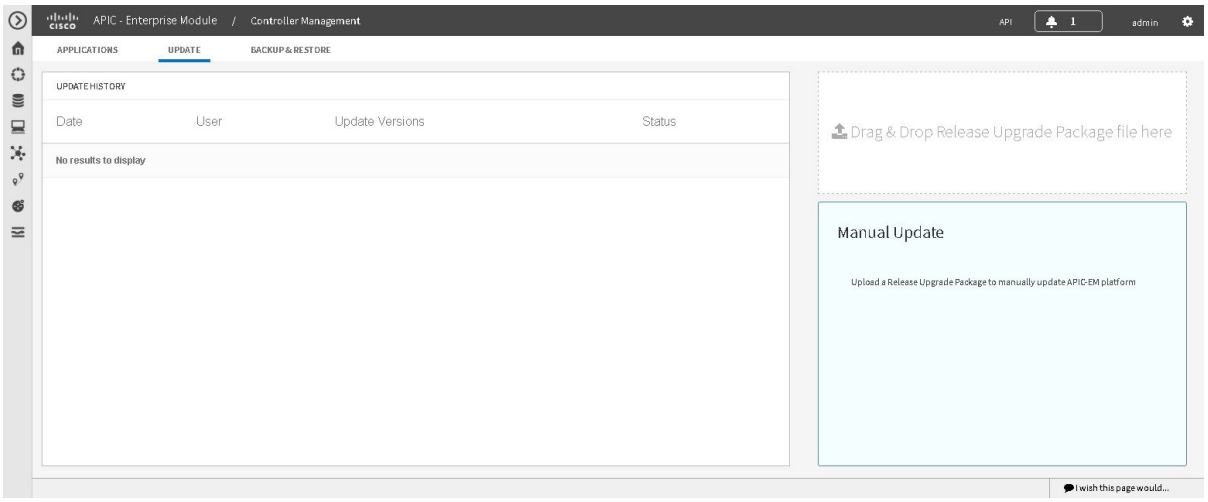
The release upgrade pack is available for download as a tar file that is also compressed, so the release upgrade pack has a .tar.gz extension. The release upgrade pack itself may consist of any or all of the following update files:

- 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.

You perform the upload and update procedure using the **Update** window in the Cisco APIC-EM GUI.

Figure 1: Update Window



Note After a successful upload and software update, you are not permitted to rollback to an earlier Cisco APIC-EM version.

Before You Begin

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

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).

Note When updating or 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.

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

You can be notified about the availability of a Cisco APIC-EM software update in the following ways:

- Email notification from Cisco support and/or updated release notes.
- System notification through the controller GUI.

Note Notification about available release upgrade packs can be viewed by clicking the **System Notifications** icon on the menu bar.

Step 1 Review the information in the Cisco notification about the Cisco APIC-EM update file and checksum.
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 update. The release upgrade pack can be as large as several Gigabits.

Step 2 Download the release upgrade pack from the secure Cisco website to your laptop or to a location within your network.

Step 3 Run a checksum against the release upgrade pack 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 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 6 Click the **App Management** link from the drop-down menu.

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

Step 7 Click the **Update** tab at the top of the window.

Step 8 If the release upgrade pack is acceptable to use for updating the controller (checksum value match in step 4), then drag and drop the release upgrade pack from the download location on your laptop or in your network onto the **Manual Update** field in the **Update** window.
After dropping the release upgrade pack onto the **Manual Update** field, the upload process begins.

The upload process may take several minutes depending upon the size of the release upgrade pack and your network connection. During the upload process, you can continue to work with the controller. Once the upload process ends and the update process begins, you will not be able to work with the controller.

Note If you close the **Update** window for any reason, then the upload process stops. To start the upload process again, open the **Update** window and drag and drop the release upgrade pack onto the **Manual Update** field again. The upload process starts where it previously stopped. To avoid any interruptions to the upload process while working with the controller, open additional windows in the GUI for any other tasks. Keep the **Update** window open during the upload process.

Step 9 Once the upload process finishes, the update process automatically begins. A message appears in the GUI stating that the update process has started and is in progress.
You should refrain from working with the controller during the update process. During the update process, the controller may shut down and restart. The shut down process may last for several minutes.

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 update process can continue.

Step 10 Once the update process finishes, you will receive a success or failure notification.
If the update was successful, you will receive a successful update notification and can then proceed working with the controller. If the update was unsuccessful, you will receive an unsuccessful update notification with suggested remedial actions to take.

After the update (or attempted 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 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 installed 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 6.

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

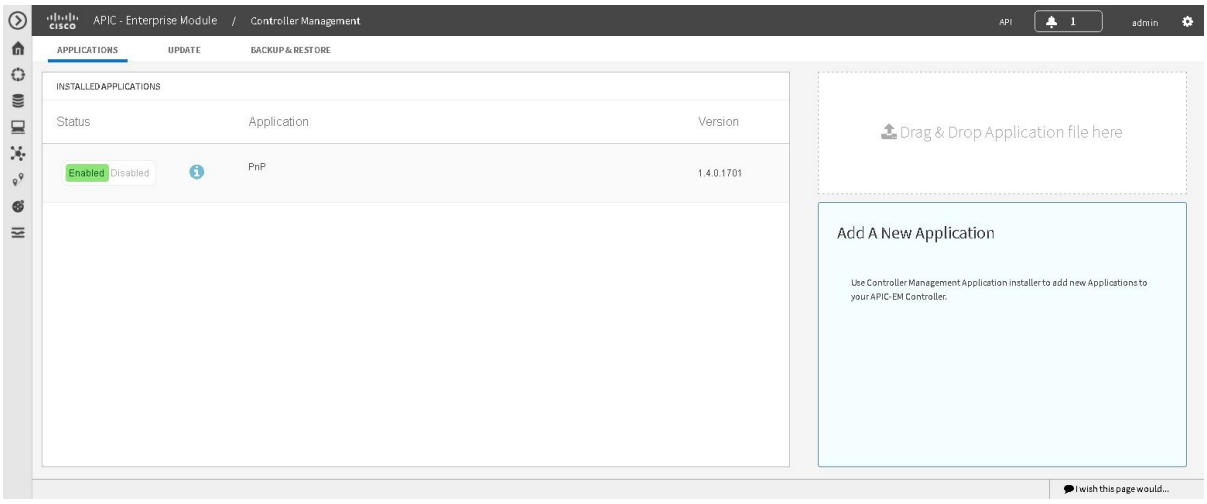
We also recommend that you run some network tests (for example, discoveries and/or path traces) to ensure that the controller functions as expected and that users are able to authenticate and access the resources on your network.

Installing Cisco APIC-EM Applications

The Cisco IWAN application is not part of the Cisco APIC-EM, Release 1.4.2.x fresh installation and may not be part of your upgrade (depending upon your specific upgrade path.)

You must install and enable Cisco IWAN in an additional procedure using the controller's GUI, as described below. 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 2: 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 performed one of the following sets of procedures :

- Installed Cisco APIC-EM, Release 1.4.2.x following the procedures described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide, Release 1.4.1.x*.
- Upgraded your Cisco APIC-EM controller software to version 1.4.2.x, as described in the previous procedures 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