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.

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 4.

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 4.

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.