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.

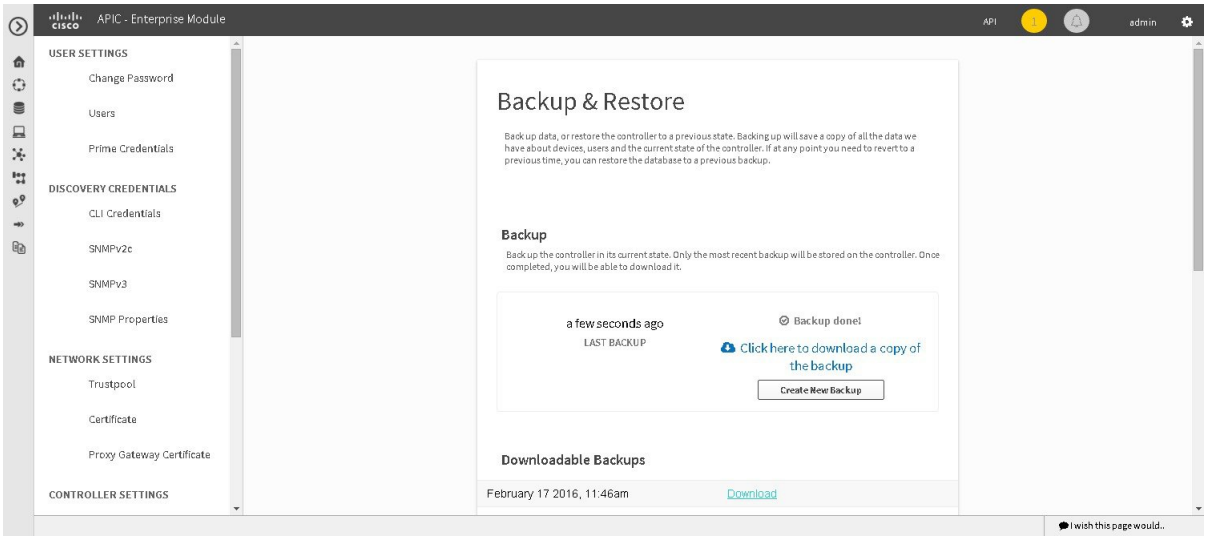
Table 2: Cisco APIC-EM Outgoing Traffic Port Reference

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*.