Before You Begin

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

Review Supported Upgrade Paths

You can upgrade to Cisco APIC-EM, Release 1.5.0.x from any of the following releases:

- 1.4.3.1009
- 1.4.2.1045
- 1.4.1.1159
- 1.4.0.1959
- 1.3.3.126

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 and then upgrade to Release 1.5.0.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
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
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

Securing the Cisco APIC-EM

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

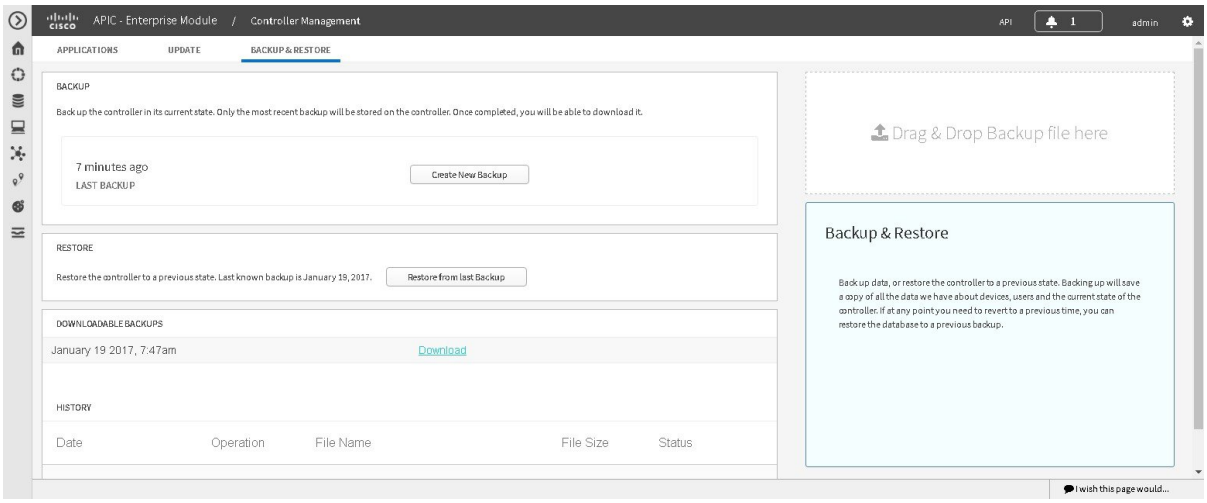
Security Recommendations	Reference
Deploy the controller behind a firewall that does not expose the controller's management ports (for example, port 22) to an untrusted network, such as the Internet.	See the previous section for information about the key controller ports.
Configure IPSec tunneling for communications between the hosts in a multi-host configuration.	See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator 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 Administrator 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 Administrator 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 Administrator 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 Administrator 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 Administrator Guide*, Settings chapter, "Configuring SNMP" for information about configuring SNMPv3 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 Administrator 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 Administrator 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_2016_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 Administrator Guide*.

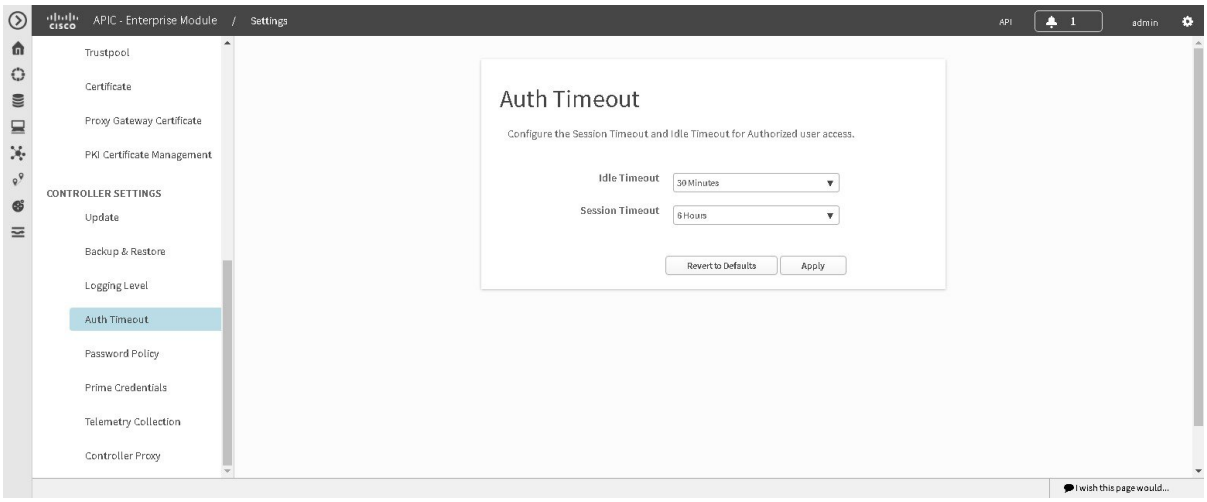
Configure the Authenticate Timeout Value for Users

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.

Figure 2: Authenticate Timeout Window



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 Administrator 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.