Troubleshooting an Installation or Update

The following information may be used to troubleshoot an unsuccessful installation or update:

Troubleshooting the Installation

The following table describes recommended actions to take to resolve a Cisco APIC-EM installation or update issue.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful installation on a bare-metal server.	Attempted installation 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 installation.

Symptom	Possible Cause	Recommended Action
Failed or unsuccessful installation on a virtual machine.	Attempted installation 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 installation, including the VMware resource pool requirements. **Note** For additional assistance with deploying the controller in a virtual machine, refer to the appendix in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide* that discusses virtual machine preparation.
Failed or unsuccessful installation on either a bare-metal server or virtual machine.	Core services failing to start up on the Cisco APIC-EM.	Perform the following actions: • If possible, log into the controller's GUI. • Review the state of the controller services in the **Systems Health** tab. • Create an rca file and send to support for additional assistance. References: • Reviewing the Service Version and Status Using the SYSTEM HEALTH Tab • Creating a Support File for a Single Host
Unable to log into the controller GUI after an apparently successful installation.	Network connectivity to the controller is failing.	Review and test your network connections to the controller. Reference: • Confirming Network Access to the Controller, on page 3

Symptom	Possible Cause	Recommended Action
Unable to update Cisco APIC-EM using the recommended standard methods.		Run the *apply_update* script. Reference: • Updating Cisco APIC-EM Using the Apply Update Script, on page 5 **Important** For additional detailed information about updating the Cisco APIC-EM, as well as additional recovery procedures for a failed update, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*.

Confirming Network Access to the Controller

After a Cisco APIC-EM installation, if you are unable to log into and view the controller's GUI, then perform the following troubleshooting activities:

- Use the **ping** command to see if you can communicate with the host. Run the **ping** command with the host's IP address to test network access to the controller.
- If your deployment is a multi-host deployment, then use the **ping** command to see if you can communicate with any of the other hosts in the multi-host cluster. Run the **ping** command with the other host IP addresses to test network access.
- If the **ping** command fails or timeouts, then there may be an issue with the network values entered during the controller installation. Proceed to review the network access to the controller and the network values entered using the configuration wizard. To review the network values entered during installation with the configuration wizard, re-run the configuration wizard using the **config_wizard** command. For information about this procedure, see Updating the Configuration Using the Wizard.

  Ensure that the following network values have been configured correctly:

  - Default gateway address (if this exists)
  - DNS server address
  - NTP server address

Confirming that Core Services are Running

If you are unable to access the Cisco APIC-EM GUI or for any other issues, then you can use the Cisco APIC-EM CLI to check for faulty or failed services.

Before You Begin

You should have attempted to install the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

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 Enter the following command to display the status of the core services:

```
$ sudo service grapevine status
```

Step 4 Enter your password a second time when prompted.

```
$[sudo] password for grapevine: ********
```

Command output similar to the following should appear. The core services should have a RUNNING status.

```
grapevine is running
grapevine_capacity_manager              RUNNING   pid 5951, uptime 18:13:31
grapevine_capacity_manager_lxc_plugin   RUNNING   pid 5956, uptime 18:13:31
grapevine_cassandra                     RUNNING   pid 5952, uptime 18:13:31
grapevine_client                        RUNNING   pid 5949, uptime 18:13:31
grapevine_coordinator_service           RUNNING   pid 5958, uptime 18:13:31
grapevine_dlx_service                   RUNNING   pid 5954, uptime 18:13:31
grapevine_log_collector                 RUNNING   pid 5959, uptime 18:13:31
grapevine_root                          RUNNING   pid 5953, uptime 18:13:31
grapevine_supervisor_event_listener     RUNNING   pid 5948, uptime 18:13:31
grapevine_ui                            RUNNING   pid 6084, uptime 18:13:30
reverse-proxy=4.0.0.10000               RUNNING   pid 11630, uptime 18:10:15
router=4.0.0.10000                      RUNNING   pid 11631, uptime 18:10:15
(grapevine)
```

Step 5 If any of the core services are not in the RUNNING state, enter the root cause analysis (rca) command.

```
$ rca
```

The **rca** command runs a root cause analysis script that creates a `tar` file that contains the following data:

- Log files
- Configuration files

- Command output

Note For a multi-host deployment (three hosts), you need to perform this procedure and run the **rca** command on each of the three hosts.

Step 6 Send the `tar` file created by the **rca** command procedure to Cisco support for assistance in resolving your issue. For information about contacting Cisco support, see Contacting the Cisco Technical Assistance Center.

Updating Cisco APIC-EM Using the Apply Update Script

If you are unable to update Cisco APIC-EM using the recommended standard methods due to the fact that the controller's GUI is inaccessible or the **grape update upload** command is not working (when using the CLI to upgrade the controller as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*), then use the procedure described below. This procedure involves using the *apply_update* script.

Note If you are encountering errors after the upload process is completed (during the subsequent verification process or after the verification procedure), then running the *apply_update* script in this procedure will not solve the problem. This script is only provided as a workaround for issues encountered during the upload process.

Important The script should only be used when the recommended, standard methods to upload and update the controller are not working. This script should not be used as an alternative method.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

Note With most of the Cisco APIC-EM releases, the *apply_update* script is packaged with the Cisco APIC-EM itself and accessible within the host after installation. In the following releases though, you need to first download the script from the Download Software link:

- 1.0.2.8
- 1.0.3.4

For information about downloading and updating the controller on these releases with the *apply_update* script, see Updating Cisco APIC-EM Using the Apply Update Script (Releases 1.0.2.8, 1.0.3.4), on page 7

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:

```
$ sudo /opt/cisco/grapevine/bin/apply_update [path-to-upgrade-file]
```

Note The script is located on /opt/cisco/grapevine/bin/apply_update, but you can run the script from anywhere on the cluster.

What to Do Next

Review the command output. If the upload is successful, then the update process will immediately follow.

If the script fails for any reason, then contact Cisco support for additional steps to take.

Updating Cisco APIC-EM Using the Apply Update Script (Releases 1.0.2.8, 1.0.3.4)

If you are unable to update Cisco APIC-EM using the recommended standard methods due to the fact that the controller's GUI is inaccessible or the **grape update upload** command is not working (when using the CLI to upgrade the controller as described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*), then use the procedure described below. This procedure involves using the *apply_update* script.

Note If you are encountering errors after the upload process is completed (during the subsequent verification process or after the verification process), then running the *apply_update* script in this procedure will not solve the problem. This script is only provided as a workaround for issues encountered during the upload process.

Important The script should only be used when the recommended, standard methods to upload and update the controller are not working. This script should not be used as an alternative method.

Before You Begin

You have installed the Cisco APIC-EM following the procedure described in the *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*.

With most of the Cisco APIC-EM releases, the *apply_update* script is packaged with the Cisco APIC-EM itself and accessible within the host after installation. In the following releases though, you need to also download the script from the Download Software link:

- 1.0.2.8
- 1.0.3.4

Step 1 Determine that your controller's Cisco APIC-EM release version is either 1.0.2.8 or 1.0.3.4.
Access the controller's GUI and review the release version on the **Home** page.

Important This procedure should only be performed on controllers running those release versions.

Step 2 Access the download page for Cisco APIC-EM releases located at the Download Software link.

Step 3 Download the script called *apply_update*.

Step 4 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 5 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 6 Using SCP or another secure method, copy the *apply_update* script to the Grapevine root for your cluster.

Step 7 Next, 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 8 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 9 Run a checksum against the file using your own checksum verification tool or utility (either MD5 or SHA512).

Step 10 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 11 Copy or move the file from your laptop or secure network location to the appliance, server, or virtual machine with the controller.

Step 12 Run the script on the Grapevine root with root permissions on the upgrade file. For example, run the following command:

```
$ sudo ./apply_update [path-to-upgrade-file]
```

What to Do Next

Review the command output. If the upload is successful, then the update process will immediately follow.

If the script fails for any reason, then contact Cisco support for additional steps to take.