Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.2.1.x

First Published: August 03, 2016

Release Notes for Application Policy Infrastructure Controller Enterprise Module, Release 1.2.1.x

This document describes the features, limitations, and bugs for this patch release.

Introduction

The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is a network controller that helps you manage and configure your network.

The Cisco APIC-EM supports the following number of devices:

- Network devices (routers, switches, wireless LAN controllers)—8000
- Hosts—80000
- Access Points—8000

What's New in Cisco APIC-EM, Release 1.2.1.x

Cisco is providing a software upgrade release that provides the following new features and functions:

- EasyQoS enhancements, including the following:
  - Users can define IP subnets for a custom application.

    To define IP subnets, from the **EasyQoS** window, select **Application Registry** > **Add Application** and enter the IP address in the **Port/Range** field.
  - Users can define individual ports (23,24,25) or a port range (45-100) for a custom application.

    To define ports, from the **EasyQoS** window, select **Application Registry** > **Add Application** and enter the ports in the **Port/Range** field.
  - Users can configure a DSCP value for a custom application.

    For example, you can choose a DSCP value in the **Add Application** pane of the **Application Registry** window.

- In addition to marking application traffic in one direction (unidirectional), you can mark application traffic in the reverse direction (bidirectional).

  To configure an application as unidirectional or bidirectional, from the **EasyQoS** window, select **Policies**, select the application, and then click the **Edit** icon next to the application that you want to change.

- Users can define QoS policies based on traffic matching a producer, consumer or both.

  To define a consumer and/or producer, from the **EasyQoS** window, select **Policies**, select the application, and then click the **Edit** icon next to the application that you want to change.

- Resolution of several CDETs that enhances your controller's performance and stability.

To upgrade your controller to Cisco APIC-EM release 1.2.1.x with this software upgrade patch, refer to Upgrading to Cisco APIC-EM, Release 1.2.1.x, on page 8.

Caution Installing this software upgrade release will disable the IWAN application on the Cisco APIC-EM controller. Do not install this software upgrade patch, if you use or require the IWAN application to monitor and manage devices within your network.

Cisco APIC-EM System Requirements

Cisco offers a physical appliance that can be purchased from Cisco with the ISO image pre-installed and tested. The Cisco APIC-EM can also be installed and operate within a dedicated physical server (bare-metal) or a virtual machine within a VMware vSphere environment. The Cisco APIC-EM has been tested and qualified to run on the following Cisco UCS servers:

- Cisco UCS C220 M4 Server
- Cisco UCS C220 M3S Server
- Cisco UCS C22 M3S Server

In addition to the above servers, the Cisco APIC-EM may also run on any Cisco UCS servers that meet the minimum system requirements (see Cisco APIC-EM Physical Server Requirements, on page 3). We also support running the product in a virtual machine that meets the minimum system requirements on VMware vSphere (see Cisco APIC-EM VMware vSphere Requirements, on page 4).

Note The Ubuntu 14.04 LTS 64-bit operating system is included in the ISO image and a requirement for the successful installation and operation of the Cisco APIC-EM. Prior to installing the Cisco APIC-EM on your Cisco UCS server, click the following link and review the online matrix to confirm that your hardware supports Ubuntu 14.04 LTS:

http://www.ubuntu.com/certification/server/

Cisco APIC-EM Physical Server Requirements

Caution You must dedicate the entire server for the Cisco APIC-EM. You cannot use the server for any other software programs, packages, or data. During the Cisco APIC-EM installation, any other software programs, packages, or data on the server will be deleted.

Review the minimum system requirements for a dedicated bare-metal server installation. The minimum system requirements for each server in a multi-host deployment are the same as in a single host deployment, except that the multi-host deployment requires two or three servers and less memory for each individual server. Three servers are required for hardware fault tolerance, and all three servers must reside in the same subnet.

Physical Server Options	Server image format	Bare Metal/ISO
Hardware	CPU (cores)	6 (minimum) **Note** 6 CPUs is the minimum number required for your server. For better performance, we recommend using 12 CPUs.
	CPU (speed)	2.4 GHz
	Memory	64 GB **Note** For a multi-host hardware deployment (2 or 3 hosts) only 32 GB of RAM is required for each host.
	Disk Capacity	500 GB of available/usable storage after hardware RAID
	RAID Level	Hardware-based RAID at RAID Level 10
	Disk I/O Speed	200 MBps
	Network Adapter	1

Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: • Google Chrome, version 50.0 or later • Mozilla Firefox, version 46.0 or later

Cisco APIC-EM VMware vSphere Requirements

Review the minimum system requirements for a VMware vSphere installation.

You must configure at a minimum 64 GB RAM for the virtual machine that contains the Cisco APIC-EM when a single host is being deployed. The single host server that contains the virtual machine must have this much RAM physically available. For a multi-host deployment (2 or 3 hosts), only 32 GB of RAM is required for each of the virtual machines that contains the Cisco APIC-EM. Three servers are required for hardware fault tolerance.

Note As with running an application on any virtualization technology, you might observe a degradation in performance when you run the Cisco APIC-EM in a virtual machine compared to running the Cisco APIC-EM directly on physical hardware.

Table 1: Cisco APIC-EM VMware vSphere Requirements

Virtual Machine Options	VMware ESXi Version	5.1/5.5/6.0
	Server Image Format	ISO
	Virtual CPU (vCPU)	6 (minimum) **Note** 6 vCPUs is the minimum number required for your virtual machine configuration. For better performance, we recommend using 12 vCPUs.
	Datastores	We recommend that you do not share a datastore with any defined virtual machines that are not part of the designated Cisco APIC-EM cluster. If the datastore is shared, then disk I/O access contention may occur and cause a significant reduction of disk bandwidth throughput and a significant increase of I/O latency to the cluster.
Hardware Specifications	CPU (speed)	2.4 GHz
	Memory	64 GB **Note** For a multi-host deployment (2 or 3 hosts) only 32 GB of RAM is required for each host.
	Disk Capacity	500 GB
	Disk I/O Speed	200 MBps
	Network Adapter	1

Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: • Google Chrome, version 50.0 or later • Mozilla Firefox, version 46.0 or later
	Network Timing	To avoid conflicting time settings, we recommend that you disable the time synchronization between the guest VM running the Cisco APIC-EM and the ESXi host. Instead, configure the timing of the guest VM to a NTP server. **Important** Ensure that the time settings on the ESXi host are also synchronized to the NTP server. This is especially important when upgrading the Cisco APIC-EM. Failure to ensure synchronization will cause the upgrade to fail.

VMware Resource Pools

When installing the Cisco APIC-EM on a VMware virtual machine, then we also recommend that you configure resource pools with the following settings.

- Resource Pools—CPU Resources:
  - Shares—Normal
  - Reservation—Minimum 14400 MHz
  - Reservation Type—Expandable
  - Limit—Maximum limit
- Resource Pools—Memory Resources:
  - Shares—Normal
  - Reservation—32 GB or 64 GB minimum depending upon your hardware

- Reservation Type—Expandable
- Limit—Maximum limit

For examples on how to create and configure both resource pools and a virtual machine for the Cisco APIC-EM, see Appendix B, "Preparing Virtual Machines for Cisco APIC-EM" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Cisco APIC-EM Licensing

The following are the licensing requirements for Cisco APIC-EM and its applications (apps):

- Cisco APIC-EM controller software and its basic apps (for example, Network PnP, Inventory, Topology, and EasyQoS):
  - No fee-based license is required. The controller software and basic apps are offered at no cost to the user.
  - You can download the controller software (ISO Image) and run it on bare-metal Cisco UCS servers or run the ISO image on a virtual machine in a VMware ESXi environment. In both cases, you need to ensure the required CPU, memory, and storage resources are available.
- Solution apps (for example, IWAN and any similar Cisco-developed solution app):
  - A per-device license is required to run the solution apps.
  - The solution apps licenses can only be acquired by purchasing Cisco® Enterprise Management 3.x device licenses, which also include the Cisco Prime™ Infrastructure licenses. The process for acquiring Cisco Prime Infrastructure 3.x device licenses is explained in the Cisco Enterprise Management Ordering Guide:

    Cisco Enterprise Management 3.x, Prime Infrastructure 3. x APIC-EM Ordering and Licensing Guides

Note The same license-acquisition process will also provide you with the right-to-use (RTU) licenses for APIC-EM solution apps. RTU licenses do not involve license files.

Cisco APIC-EM Technical Support

The following Cisco APIC-EM technical support options are provided:

- Cisco APIC-EM hardware appliance:

  Hardware support is provided through the Cisco SMARTnet® Service.
- Cisco APIC-EM controller, basic apps, and services:

  Cisco® TAC support is offered at no additional cost, if you have SMARTnet on any Cisco networking device.
- Cisco APIC-EM solutions apps and services:

TAC support is offered at no additional cost, if you have a SWSS (maintenance contract) on Cisco® Enterprise Management 3.x device licenses.

Supported Platforms and Software Requirements

For information about the network devices and software versions supported for this release, see Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.2.0.x.

Deploying the Cisco APIC-EM

The Cisco APIC-EM supports the following two deployment types:

- As a dedicated Cisco APIC-EM physical appliance purchased from Cisco with the ISO image pre-installed.
- As a downloadable ISO image that you can burn to a dual-layer DVD or a bootable USB flash drive.

Note The USB flash drive must be bootable. You can use a third-party utility to create a bootable USB flash drive using the ISO image. You cannot boot from the USB flash drive if you copy the ISO to the flash drive.

The ISO image consists of the following components:

- Ubuntu 14.04 LTS 64-bit operating system
- Elastic Services Platform (Grapevine) binaries
- Cisco APIC-EM services

Before you deploy the Cisco APIC-EM, make sure that the time on the controller's system clock is current or that you are using a Network Time Protocol (NTP) server that is keeping the correct time.

To deploy the Cisco APIC-EM, refer to Chapter 5, "Deploying the Cisco APIC-EM," in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*. For a list of network devices supported for this release, see *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.2.0.x*.

Upgrading to Cisco APIC-EM, Release 1.2.1.x

You can upgrade to Cisco APIC-EM release 1.2.1.x using the **Software Update** functionality of the controller's GUI. This upgrade procedure requires that you upload and update the new release, as described below.

Important If you are upgrading a multi-host cluster and want to configure IP Security (IPSec) tunneling for communications between the hosts, then you must follow a different procedure. For information about this procedure, see Upgrading to Cisco APIC-EM, Release 1.2.1.x and Enabling IPSec for a Multi-Host Cluster, on page 10.

Before You Begin

Review the following list of pre-requisites and perform the recommended procedures before upgrading your Cisco APIC-EM:

- You can only upgrade to the new Cisco APIC-EM release (1.2.1.x) from the following earlier software and software patch releases:
  - 1.2.0.1594
  - 1.1.2.15
  - 1.1.1.38
  - 1.1.1.34

Note If your current Cisco APIC-EM release version is not one of the above releases, then first upgrade to one of these releases prior to upgrading to release 1.2.1.x.

- Review the system requirements for your Cisco APIC-EM upgrade (see Cisco APIC-EM System Requirements, on page 2). The system requirements may have changed for this release from a previous release and may require that you make changes to your deployment. For example, when 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.
- Create a backup of your Cisco APIC-EM database. For information about backing up and restoring the controller, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.
- Make sure that the time on the controller's system clock is current or that you are using a Network Time Protocol (NTP) server that is keeping the correct time.

Step 1 Download the Cisco APIC-EM upgrade package for release 1.2.1.x from the Cisco website at the Download Software link.

Step 2 Upload the upgrade package to the controller using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 3 Update the controller's software with the upgrade package using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 4 Check the controller's software version number in the GUI **Home** window. The GUI **Home** window should display the new software version (1.2.1.x).

Note Upgrading from earlier releases to Cisco APIC-EM release 1.2.1.x may take up to an hour to complete.

Upgrading to Cisco APIC-EM, Release 1.2.1.x and Enabling IPSec for a Multi-Host Cluster

You can upgrade to Cisco APIC-EM release 1.2.1.x using the **Software Update** functionality of the controller's GUI. For upgrading an existing multi-host cluster to Cisco APIC-EM release 1.2.1.x and configure IP Security (IPSec) tunneling for inter-host communications, then you must take additional steps.

Follow the steps described below to upgrade your *existing* multi-host cluster and configure IPSec tunneling. The steps must be performed in the following order:

1. Download and update the controller software on one of the hosts (steps 1-5).
2. Break up or disassemble your multi-host cluster (steps 6-10).
3. Configure IPSec tunneling on the last host that was in your cluster (steps 11-15).
4. Reassemble your multi-host cluster around that last host where you configured IPSec tunneling (steps 16-25).

Note If you are upgrading to a multi-host cluster from a single host (not an existing multi-host cluster) and have already updated the single host to release 1.2.1.x, then you need to configure IPSec tunneling using the configuration wizard. After performing this procedure on that single host, when you join any new hosts (running release 1.2.1.x) to form a cluster, each host will have IPSec tunneling configured.

Before You Begin

Review the following list of pre-requisites and perform the recommended procedures before upgrading your Cisco APIC-EM:

- You can only upgrade to the new Cisco APIC-EM release (1.2.1.x) from the following earlier software and software patch releases:
  - 1.2.0.1594
  - 1.1.2.15
  - 1.1.1.38
  - 1.1.1.34

Note If your current Cisco APIC-EM release version is not one of the above releases, then first upgrade to one of these releases prior to upgrading to release 1.2.1.x.

- Review the system requirements for your Cisco APIC-EM upgrade (see Cisco APIC-EM System Requirements, on page 2). The system requirements may have changed for this release from a previous release and may require that you make changes to your deployment.
- Create a backup of your Cisco APIC-EM database. For information about backing up and restoring the controller, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

- Make sure that the time on the controller's system clock is current or that you are using a Network Time Protocol (NTP) server that is keeping the correct time.

Step 1 Download the Cisco APIC-EM upgrade package for release 1.2.1.x from the Cisco website at the Download Software link.

Step 2 Upload the upgrade package to the controller (one of the hosts in the cluster) using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 3 Update the controller's software with the upgrade package using the **Software Update** functionality of the GUI.
For additional information about this step, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 4 Check the controller's software version number in the GUI **Home** window. The GUI **Home** window should display the new software version (1.2.1.x).

Note Upgrading from earlier releases to Cisco APIC-EM release 1.2.1.x may take up to an hour to complete.

Step 5 Proceed to check the software versions of the other hosts in your cluster.

Note Updating the software on one host in the cluster will cause the other hosts in the cluster to be updated with the same upgrade package.

Step 6 Using a Secure Shell (SSH) client, log into one of the hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 7 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 8 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 9 A message appears with an option to **[proceed]** and remove this host from the cluster.
Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from the cluster.
At the end of this process, this host is removed from the cluster.

Step 10 Repeat the above steps (steps 6-9) on a second host in the cluster.

Note You must repeat the above steps on each host in your cluster, until you have broken up the multi-host cluster.

Important Make a note of the final host in the cluster that you have just broken up or disassembled. You must perform the next steps (enabling IPSec) on that specific host. For example, if you have 3 hosts in a cluster (A, B , C) and you first remove host A, then remove host B, then you must enable IPSec tunneling on host C.

Step 11 Using a Secure Shell (SSH) client, log into the last host in your cluster and run the **config_wizard** command.

```
$ config_wizard
```

Step 12 Review the current configuration values in the configuration wizard and click **next>>**, until you access the **INTER-HOST COMMUNICATION** screen.

Step 13 Configure IPSec tunneling for communications between the hosts in a multi-host cluster by selecting *yes*.
The default tunneling protocol used for communications between the hosts in a multi-host cluster is Generic Routing Encapsulation (GRE). By entering 'yes', you are configuring IPSec tunneling with this step.

Step 14 Click **next>>** until the last step of the configuration wizard process is reached.

Step 15 Click **proceed>>** to have the configuration wizard save and apply your configuration changes to your Cisco APIC-EM deployment.
At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Next, proceed to log into the other hosts previously in your multi-host cluster and use the configuration wizard to reassemble the cluster (with IPSec tunneling configured between the hosts).

Step 16 Using a Secure Shell (SSH) client, log into one of the other hosts in your cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 17 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 18 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option.

Note Joining this other (second) host to the host with IPSec tunneling, automatically configures IPSec tunneling on this other (second) host.

Step 19 Proceed to recreate the cluster using the configuration wizard.
For additional information about this step and process, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* .

Step 20 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

Step 21 Using a Secure Shell (SSH) client, log into the third host and use the configuration wizard to join the new multi-host cluster.
When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 22 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 23 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Add this host to an existing APIC-EM cluster** option.

Note Adding this host to the new multi-host cluster (with IPSec tunneling configured), automatically configures IPSec tunneling on this host.

Step 24 Proceed to add this host to the cluster using the configuration wizard.
For additional information about this step and process, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* .

Step 25 At the end of the configuration process, click **proceed>>** to have the configuration wizard save and apply your configuration changes.
A **CONFIGURATION SUCCEEDED!** message appears.

At the end of this step, you have updated your multi-host cluster and configured IPSec tunneling. Repeat the above steps to add any additional hosts to your multi-host cluster.

Caveats

Open Caveats

The following table lists the open caveats for this release.

Caveat ID Number	Headline
CSCva64675	Performance Monitor configuration fails for Cisco Cloud Services Router 1000V devices. **Workaround**: There is no workaround at this time.
CSCux96848	When Delete Dynamic policy is initiated (same time for both Video and Voice), sometimes VOICE ACE's get deleted and sometimes VIDEO gets deleted, but not both at the same time. Both Voice and Video ACE's should be removed when delete dynamic policy is initiated. **Workaround**: There is no workaround at this time.
CSCuy18848	When defining class-maps for LAN queuing policies, the EasyQos app uses the meaning format of DSCP values. The EasyQoS app also uses the decimal format of DSCP values when defining policy-maps. The policy-map and class-map definitions should follow the same DSCP naming convention with the EasyQoS application. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCuy37443	The QoS statistics output "queueBandwidthbps" shows NA when configured with several commands. On an ISR router, configure the policy-map with the **bandwidth** and **priority** commands. Start a flow analysis with QoS statistics collection request with the ISR router in the path. This happens when configured with following commands: • **bandwidth percent** • **priority percent** • **priority** (strict priority) **Workaround**: There is no workaround at this time.
CSCuy40059	EasyQoS does not support custom app creation on an ASR 1000 (versions earlier than 3.13), if the first 3 alphabet letters match. **Workaround**: There is no workaround at this time.
CSCuy41584	VRF filters in **Topology** and **Inventory** will not work for Nexus platforms. **Workaround**: There is no workaround at this time.
CSCuy90109	A custom app is added to a class-map without being created in EasyQoS. **Workaround**: Reapply after a rollback is performed.

Caveat ID Number	Headline

CSCuz46584	On rare occasions, when performing a restore or update operation, the operation may timeout while harvesting and regrowing services.
	Workaround:
	Perform the following steps to reboot the cluster node to recover from the issue:
	1 Open a terminal window and log onto a cluster node using SSH:
	`ssh grapevine@<host ip address>`
	2 Run the following command:
	`ps aux | grep grapevine_lxc_plugin | awk '{print $8}' | grep D`
	3 The above command checks if any LXC container process is in "uninterruptible sleep" state on the cluster node. If the output of the command is not empty, then that cluster node needs to be rebooted.

CSCuz61632	The **Claimed and Ignored** page count, on the lower-right corner of the **Network Plug and Play** window, displays "x of 0", where " x" is the cache value from **Unclaimed** page. The correct value should be "1 of 1". **Workaround**: There is no workaround at this time.
CSCuz62005	VLAN ACLs are not identified in an ACL trace. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCuz74785	Any Cisco APIC-EM users who have been authenticated/authorized by an external server and who are locked out of the controller for whatever reason, cannot be manually un-locked. **Note** There is no GUI to shows that the user is actually locked out. **Workaround**: There are two workarounds available: • Wait 15 minutes for the timeout to end before logging into the controller again. • Disable user locking for the specific user from the **Internal Users** window. **Note** You must have administrator priveleges (ROLE_ADMIN) to perform this action.
CSCuz78783	When running the **reset_grapevine** command on the evaluation version of Cisco APIC-EM (16 GB of memory), the cluster does not clean up the database. There is no issue with running the command on a Cisco APIC-EM cluster with 64 GB of memory. **Workaround**: This issue happens the first time when running this command. If we try the **reset_grapevine** command a second time and enter **y** for deleting the virtual disks, then it will delete the virtual disks.
CSCva32308	After erasing the exiting virtual disk and reconfiguring the RAID, attempts to install the ISO with a USB fail due to a mount issue. This issue is due to the following Ubuntu bug: https://bugs.launchpad.net/ubuntu/+source/debian-installer/+bug/1347726. **Note** This issue does not occur when using the CIMC for installation. **Workaround**: Unmount the /media and mount /cdrom.
CSCva36094	In some cases, EasyQoS provisioning on the Cisco Catalyst 3750x device with brownfield configuration fails due to the device providing a faulty status of its TCAM utilization. **Workaround**: Reload the device.

Caveat ID Number	Headline
CSCva39044	When a Cisco 2500 Series Wireless Controller (WLC) is upgraded from version 7.4.100.0 or lower to any version that EasyQos supports, EasyQos can push a policy to the WLC, but it cannot attach the WLAN. In this scenario, EasyQos should not push the policy to the WLC. Instead, it should display a message on the EasyQos GUI similar to the following: "AVC is not supported with the current bootloader version (1.0.16). Please upgrade the bootloader to version 1.0.18 or Field Upgradable software version 1.8.0.0 or higher. See Cisco documentation for information about Field Upgradable software." This issue is specific to the WLC 2500. **Workaround**: Upgrade the wireless controller bootloader to version 1.0.18 or higher, perform an inventory synchronization, and reapply the policy.

Resolved Caveats

The following table lists the resolved caveats for this release.

Note For a list of caveats resolved in an earlier software release, see the Cisco APIC-EM release notes for that specific release.

Caveat ID Number	Headline
CSCuz26026	Host inventory support is limited for the Polaris image. The IP device tracking format has been changed on Polaris image (IOS-XE 3850) and therefore the host inventory device pack is not able to collect the wired host information.
CSCuz72777	The audit records shows repetitive messages after new policy created in EasyQOS UI.
CSCuz73011	Start a path trace with PerfMon and verify the rtpJitterMin value. The rtpJitterMin value is shown as 0 instead of actual value.
CSCuz73363	For a path trace, the PerfMon packet loss percent not configured and it is always N/A.

Caveat ID Number	Headline
CSCuz74716	If NBAR is not enabled or activated on a Cisco ISR 881, the error message is shown correctly but the policy application is shown as green indicating that the policy was successfully applied. The status should have been displayed in red.
CSCuz77642	The PerfMon (performance monitoring) configuration fails on the following network devices: • Cisco ASR 1002-HX Router • Cisco ASR 1006-X Router • Cisco ASR 1009-X Router • Cisco 3945 Integrated Service Router • Cisco 3945E Integrated Service Router • Cisco 3925 Integrated Services Router • Cisco 3925E Integrated Service Router • Cisco 890 Series Integrated Services Router • Cisco 860 Series Integrated Services Router • Cisco 810 Integrated Services Router • Cisco 800M Integrated Services Router • Cisco Cloud Services Router 1000V Series
CSCuz78734	When a user tries to change the values of retries and timeouts in the advanced part of the external authentication configuration in **Settings**, the GUI page displays an error.
CSCuz80829	If an external authentication server (AAA server) is misconfigured, a user login through the GUI may not succeed. The external authentication server configuration has retry and timeout fields. If these fields have a higher value, then you can run into this issue.

Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in this release.

Step 1 Go to http://tools.cisco.com/bugsearch.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

Step 4 To search for bugs in the current release:

a) In the Search For field, enter APIC-EM and press **Return**. (Leave the other fields empty.)

b) When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

Note To export the results to a spreadsheet, click the **Export Results to Excel** link.

Limitations and Restrictions

Cisco APIC-EM limitations and restrictions are described in the following sections:

General Limitations

- The web GUI may take a few seconds to begin after the controller is started.
- When working with the Cisco APIC-EM in a network with several thousand supported devices, the Topology window may load slowly. Additionally, filtering within the other controller windows may also proceed slowly.
- Up to 2046 IP addresses are supported per discovery scan.

Note The IP address limit applies for one or more configured IP ranges in the controller's GUI.

- The Cisco APIC-EM does not support duplicate IP addresses across VRFs in this release.
- Inventory and Topology VRF filters are only supported for Cisco IOS devices. Cisco non-IOS devices such as the Nexus devices are not supported with VRF filters.
- We recommend that after deleting a user from the controller's database, that you do not reuse that username when creating a new user for at least 6 hours. This waiting period is required to ensure that the deleted user's access rights and privileges are not inherited when reusing the username.

- Cisco APIC-EM uses a master-slave database management system for the multi-host cluster. If the master host fails for any reason, then you will experience a 10 to 11 minute time interval when the controller UI is unavailable. This is due to the other two hosts recovering from that failure and re-establishing communications. If one of the slave hosts fail, there is no impact to the controller UI.

Multi-Host Limitations

- In a multi-host cluster with three hosts, if a single host (host A) is removed from the cluster for any reason, and the second host (host B) fails, then the last host (host C) will also immediately fail. To work around this limitation, perform the following procedure:

  1. Log into the last active host (host C) and run the **config_wizard** command.
  2. In the configuration wizard display, choose **<Remove a faulted host from this APIC-EM cluster>**
  3. In the configuration wizard display, choose **<Revert to single-host cluster>**

     The Grapevine services underpinning the original multi-host cluster are then removed and restarted.
  4. Access the displayed IP address with a browser to view the Grapevine developer console and view the progress as each service restarts.
  5. After host C is up and running, then proceed to reconfigure the multi-host cluster.

  Note For information about configuring a multi-host cluster, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

- To enable external authentication with a AAA server in a multi-host environment, you must configure all individual Cisco APIC-EM host IP addresses and the Virtual IP address for the multi-host cluster on the AAA server. For additional information about external authentication with the Cisco APIC-EM, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Security Limitations

- With this release, you have the option to configure IPSec tunneling for intra-host communications within a multi-host cluster (using the configuration wizard). The default for intra-host communications is using GRE. If you do not choose the IPSec option using the configuration wizard, then privacy is not enabled for all of the communications that occur between the hosts. For this reason, we strongly recommend that any multi-host cluster that is not configured with IPSec tunneling be set up and located within a secure network environment.
- The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment. Additionally, when using the IWAN or PNP solution applications in a manner that is open to the Internet, you must configure a white-listing proxy or firewall to only allow incoming connections from your branch IP pools.
- The Cisco APIC-EM platform management service (Grapevine) running on port 14141 does not presently support installing a valid CA issued external certificate. We recommend that access at port 14141 using HTTPS via a northbound API or the Grapevine developer console be secured using stringent measures such as a segmented subnet, as well as strict source address-based access policies in the port's access path.

- Ensure that any external access to the Cisco APIC-EM using SSH (through port 22) is strictly controlled. We recommend that stringent measures be used, such as a segmented subnet as well as strict source address-based access policies in the port's access path.
- Ensure that the strict physical security of the Cisco APIC-EM appliance or server is enforced. For Cisco APIC-EM deployed within a virtual machine, ensure that strong and audited access restrictions are in place for the hypervisor management console.
- The Cisco APIC-EM backups are not encrypted when they are downloaded from the controller. If you download the backups from the controller, ensure that they are stored in a secure storage server and/or encrypted for storage.
- Do not keep several Grapevine developer consoles to port 14141 open from an admin host. Inadvertently keeping several tabs or browsers open and connected to port 14141 may result in multiple connections attempted to the Grapevine service for dynamic refreshes. This may result in the blocking of that admin host machine from accessing the Grapevine platform via SSH or the Grapevine developer console for at least 30 minutes as a counter DoS measure.
- The **Update** button in the controller's **Trustpool** GUI window will become active when an updated version of ios.p7b file is available and Internet access is present. The **Update** button will remain inactive if there is no Internet access.
- As with any network management application, it is a general best practice to ensure that the traffic sent from Cisco APIC-EM to the managed devices is controlled in such a way as to minimize any security risks. More secure protocols (such as SSHv2 and SNMPv3) should be used rather than less secure ones (TELNET, SNMPv2), and network management traffic should be controlled (for example via access control lists or other types of network segmentation) to ensure that the management traffic is restricted to devices and segments of the network where it is needed.

Software Update Limitations

- Upgrading from earlier Cisco APIC-EM releases to this release, 1.2.1.x may take up to an hour to complete.
- When upgrading 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.
- Prior to beginning the software update process for the Cisco APIC-EM, we recommend that you configure the idle timeout value in the **Auth Timeout** GUI window 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.

  In case a failure occurs on a multi-host cluster during any software updates (Linux files) and you have not increased the idle timeout using the GUI, then perform the following steps:

  1 Log into each host and enter the following command: $ **sudo cat /proc/net/xt_recent/ROGUE | awk '{print $1}**'

  

  Note This command will list all IP addresses that have been automatically blocked by the internal firewall because requests from these IP addresses have exceeded a predetermined threshold.

2 If the command in Step 1 returns an IP address, then perform a reboot on the host where the above command has been entered (same host as the user is logged in).

Note The hosts should be rebooted in a synchronous order and never two hosts rebooted at the same time.

3 After the host or hosts reboot, upload the software update package file to the controller again using the GUI.

Back Up and Restore

Important For the IWAN solution application, you must review the *Software Configuration Guide for Cisco IWAN on APIC-EM* before attempting a back up and restore. There is important and detailed information about how these processes work for the IWAN application that includes what is backed up, what is not backed up, recommendations, limitations, and caveats.

- Before attempting a back up and restore with a host in a multi-host cluster, note the following:
  - You cannot take a back up from a single host (not in a multi-host cluster) and then restore it to a host in a multi-host cluster.
  - You cannot take a back up from a host in a multi-host cluster and restore it to a single host (not in a multi-host cluster).
- When a user restores the controller from a backup file using the Cisco APIC-EM GUI, the password of the user will be reset to what is in that backup file.
- You can only restore a backup from a controller that is the same version from which the backup was taken.
- If you have configured a multi-host cluster with two or three hosts and not all of the hosts are running when you initiate a restore operation, then the restore operation will fail. All of the hosts that comprise the cluster must be in the cluster and operational at the time of the restore.
- Prior to beginning the backup and restore process for the Cisco APIC-EM, we recommend that you log out and then log back into the controller. This will ensure that the default forced session timeout for the Cisco APIC-EM does not occur during this process.
- Prior to beginning the backup and restore process for the Cisco APIC-EM, we recommend that you configure the idle timeout value in the **Auth Timeout** GUI window for at least an hour. If a user is logged out due to an idle timeout during the restore file upload process, then the restore process will fail and need to be re-initiated again.

  In case a failure occurs on a multi-host cluster during any Linux file updates and you have not increased the idle timeout using the GUI, then perform the following steps:

  1 Log into each host and enter the following command: $ **sudo cat /proc/net/xt_recent/ROGUE | awk '{print $1}**'

Note This command will list all IP addresses that have been automatically blocked by the internal firewall because requests from these IP addresses have exceeded a predetermined threshold.

2 If the command in Step 1 returns an IP address, then perform a reboot on the host where the above command has been entered (same host as the user is logged in).

Note The hosts should be rebooted in a synchronous order and never two hosts rebooted at the same time.

3 After the host or hosts reboot, upload the software update package file to the controller again using the GUI.

Deployment Limitations

- For a multi-host deployment, when joining a host to a cluster there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that is being joined.
- For a multi-host deployment, when joining additional hosts to form a cluster be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- For a multi-host deployment, you should expect some service downtime when the adding or removing hosts to a cluster, since the services are then redistributed across the hosts. Be aware that during the service redistribution, there will be downtime.
- The controller GUI starts up and becomes accessible prior to all the Cisco APIC-EM services starting up and becoming active. For this reason, you need to wait a few minutes before logging into the controller GUI under the following circumstances:
  - Fresh ISO image installation
  - Resetting the controller using the reset_grapevine command
  - Power failure and the controller restarts
- If you are installing the Cisco APIC-EM ISO image on a physical server using local media, you can use either a DVD drive, a bootable USB device, or a mounted VirtualMedia via CIMC (Cisco Integrated Management Controller for a Cisco UCS server). If you use a mounted VirtualMedia via CIMC, the installation process may take up to an hour. If you use a DVD drive or a bootable USB device, the installation process may take approximately 15 minutes.
- If you burn the APIC-EM ISO to a bootable USB flash drive and then boot the server from the USB flash drive, a “Detect and mount CD-ROM” error might display during installation. This typically occurs when you perform the installation on a clean, nonpartitioned hard drive. The workaround for the above issue is to perform the following steps:

  1 Press **Alt+F2** to access the shell prompt.

2. Enter the **mount** command to determine the device that is attached to the /media mount point. This should be your USB flash drive.
3. Enter the **umount /media** command to unmount the USB flash drive.
4. Enter the **mount /dev/***device_path* **/cdrom** command (where *device_path* is the device path of the USB flash drive) to mount the USB flash drive to the CD-ROM. For example:
   ```
   mount /dev/sda1 /cdrom
   ```
5. Press **Alt+F1** to return to the installation error screen.
6. Click "Yes" to retry mounting the CD-ROM.

- When the configuration wizard is run to deploy the Cisco APIC-EM and the **<save & exit>** option is selected at the end of the configuration process instead of the **proceed>>** option, then you should always run the **reset_grapevine** command to bring the Cisco APIC-EM to an operational state. Failure to run the **reset_grapevine** command at the end of the deployment process after choosing the **<save & exit>** option in the configuration wizard will cause certain services to fail. The services that will fail are services that are brought up in the new VMs that are created and that depend upon the PKI certificates and stores. Services that do not depend upon the PKI certificates and stores will function properly.
- When you deploy the Cisco APIC-EM using the configuration wizard, you must create passwords that meet specific requirements. These password requirements are enforced for the configuration wizard, but are not enforced when accessing the controller's GUI.

Discovery Limitations

- HTTP and HTTPS are not supported for device discovery for this release.

User Account Limitations

- This version of the Cisco APIC-EM has been tested for external authentication with Cisco ISE based AAA servers, but it may support integration with other types of AAA servers.
- External authentication is only supported for the Cisco APIC-EM UI and not the Grapevine console UI.
- An installer (ROLE_INSTALLER) uses the Cisco Plug and Play Mobile App to remotely access the Cisco APIC-EM controller and trigger device deployment and view device status. An installer cannot directly access the Cisco APIC-EM GUI. If an installer needs to change their password, the admin must delete the user then create a new user with the same username and a new password.

Path Trace Limitations

- VLAN ACLs (VACLs) are not supported for this release. The Cisco APIC-EM is only supporting ACLs on VLAN.
- If two Layer 3 routers are connected through a Layer 2 switch and if CDP is disabled between the switch and routers, then the controller will not support a trace route.
- For a NPR (Non Periodic Refresh) path scenario, after an upgrade, the controller will not refresh the path. Additionally, the statistics collection will stop. To continue the statistics collections, you must initiate a new path request.

- A path trace from a host in a HSRP VLAN to a host in a non-HSRP VLAN that is connected to any of the HSRP routers is not supported.
- Applying a performance monitor configuration through Cisco APIC-EM fails if there is a different performance monitor policy configuration on the interface. You should remove the performance monitor configuration on the interface and re-submit the path trace request.

Important For specific path trace restrictions and support by platform, see *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

ACL Trace Limitations

- VLAN ACLs (VACLs) are not supported for this release. The Cisco APIC-EM is only supporting ACLs on VLAN.
- Cisco APIC-EM does not support an ACL trace if there exists a router ACL (ACL applied on an SVI) on the last hop in the path.
- Object groups are not supported in an ACL trace.

Important For specific Path Trace ACL support by platform, see *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

Service and Support

Troubleshooting

See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*, for troubleshooting procedures.

Related Documentation

The following publications are available for the Cisco APIC-EM:

Cisco APIC-EM Documentation

For this type of information...	See this document...
• Learning about the latest features. • Learning about the controller system requirements. • Reviewing open and resolved caveats about the controller.	*Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
• Learning about supported platforms. • Learning about required configurations on certain specific platforms. • Learning about application-specific limitations on certain specific platforms.	*Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*.
• Installing and deploying the controller. • Configuring credentials for device discovery. • Importing a certificate or trustpool. • Using service logs. • Configuring authentication timeout and password policies. • Monitoring and managing Cisco APIC-EM services. • Backing up and restoring the controller.	*Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
• Navigating the Cisco APIC-EM GUI. • Getting familiar with the Cisco APIC-EM features.	*Cisco Application Policy Infrastructure Controller Enterprise Module Quick Start Guide*

For this type of information...	See this document...
• Creating user accounts. • Discovering devices in your network and populating your inventory. • Displaying discovered devices in various topological views. • Configuring quality of service on the devices in your network. • Performing path traces. • Using the topology map. • Accessing the Cisco APIC-EM APIs.	*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
• Troubleshooting the controller. • Troubleshooting services. • Troubleshooting passwords. • Working with the developer console. • Contacting the Cisco Technical Assistance Center (TAC).	*Cisco Application Infrastructure Controller Enterprise Module Troubleshooting Guide*
• Tasks to perform before beginning an update. • Updating the controller to the latest version. • Tasks to perform after an update.	*Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*

Cisco IWAN Documentation

For this type of information...	See this document...
Configuring the Cisco IWAN network.	*Software Configuration Guide for Cisco IWAN on APIC-EM*
Reviewing open and resolved caveats about the Cisco IWAN application.	*Release Notes for Cisco Intelligent Wide Area Network (Cisco IWAN)*

Cisco Network Plug and Play Documentation

For this type of information...	See this document...
• Reviewing open and resolved caveats about Cisco Network Plug and Play. • Viewing the list of supported Cisco devices for Cisco Network Plug and Play.	*Release Notes for Cisco Network Plug and Play*
• Configuring Cisco Network Plug and Play.	*Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM* *Cisco Open Plug-n-Play Agent Configuration Guide*
• Learning about the Cisco Network Plug and Play solution. • Understanding the main workflows used with the Cisco Network Plug and Play solution. • Deploying the Cisco Network Plug and Play solution. • Using proxies with the Cisco Network Plug and Play solution. • Configuring a DHCP server for APIC-EM controller auto-discovery. • Troubleshooting the Cisco Network Plug and Play solution.	*Solution Guide for Cisco Network Plug and Play*
Using the Cisco Plug and Play Mobile App	*Mobile Application User Guide for Cisco Network Plug and Play* (also accessible in the app through Help)

APIC-EM Developer Documentation

The Cisco APIC-EM developer website is located on the Cisco DevNet website.

For this type of information...	See this document...
API functions, parameters, and responses.	APIC-EM API Reference Guide
Tutorial introduction to controller GUI, DevNet sandboxes and APIC-EM NB REST API.	Getting Started with Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

For this type of information...	See this document...
Hands-on coding experience calling APIC-EM NB REST API from Python.	APIC-EM Learning Labs

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at:

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Notices

Trademarks