Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.1.2.x

First Published: May 03, 2016

Release Notes for Application Policy Infrastructure Controller Enterprise Module, Release 1.1.2.x

This document describes the features, limitations, and bugs for this 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)—4000
- Hosts—40000
- Access Points—4000

What's New in Release 1.1.2.x

The Cisco APIC-EM patch, Release 1.1.2.x, resolves several CDETs related to the Cisco IWAN Application and is designed to enhance your controller's performance and stability. The following conditions determine whether or not you need to upgrade to this patch release:

- If you are using the Cisco IWAN App, you **must** upgrade to this new release.
- If your Cisco APIC-EM is at Release 1.1.0.x or below, you **must** upgrade to this new release.
- If your Cisco APIC-EM is at Release 1.1.1.x, and you are not using the Cisco IWAN App, you **do not** need to upgrade to this new release.

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 2). 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 3).

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 47.0 or later • Mozilla Firefox, version 44.0 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 47.0 or later • Mozilla Firefox, version 44.0 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

The following tables list the supported devices and modules, with their software requirements for the Cisco APIC-EM.

Note For information about the supported platforms and software requirements for the Cisco IWAN and Cisco Network PnP applications, refer to the Release Notes for Cisco IWAN and the Release Notes for Cisco Network Plug and Play.

For information about application-specific platform limitations, see:

- Path Trace: Limitations and Restrictions, on page 22
- EasyQoS: EasyQoS Feature Support by Platform, on page 27

Table 2: Supported Switches

Supported Switches	Minimum Software Version [1]	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Catalyst 2960-S Series switches, including stacks	>=12.1	Cisco IOS 15.2(1)E1, 12.2(58)SE2	Yes	Yes	Yes	Yes	No
Catalyst 2960-X/XR Series switches	>=12.1	Cisco IOS 15.2.3E, 15.0.2-EX5	Yes	Yes	Yes	Yes	No
Catalyst 3560CG Series switches	>=12.2	Cisco IOS 15.0(2)SE5	Yes	Yes	Yes	Yes	No
Catalyst 3560CX Series switches	15.2(3)E1	Cisco IOS 15.2(3)E1	Yes	Yes	Yes	Yes	No

Supported Switches	Minimum Software Version [1]	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Catalyst 3560-X Series switches	>=12.2	Cisco IOS 15.2(4)E, 12.2(58)SE2	Yes	Yes	Yes	Yes	No
Catalyst 3650 Series switches	All versions	Cisco IOS 3.6.2aE	Yes	Yes	Yes	Yes	No
Catalyst 3750-X Series switches, including stacks	>=12.2	Cisco IOS 15.2(4)E, 12.2(55)SE8	Yes	Yes	Yes	Yes	No
Catalyst 3850 Series switches, including stacks	All versions	Cisco IOS 3.6.2aE	Yes	Yes	Yes	Yes	No
Catalyst 4500(Sup7E) Series switches	All versions	Cisco IOS 3.5(2)E, 3.2(8)SG	Yes	Yes	Yes	Yes	No
Catalyst 4500E (Sup8E) Series switches	All versions	Cisco 3.3.2XO, 3.6.1E	Yes	Yes	Yes	Yes	No
Catalyst 6500 (Supervisor Engine 720-3C/B) Series switches	>=12.2	Cisco 15.1(2)SY2	Yes	Yes	No	Yes	No

Supported Switches	Minimum Software Version [1]	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Catalyst 6500(2T) Series switches	>=12.2	Cisco IOS 15.1(2)SY4a, 15.0(1)SY6	Yes	Yes	Yes	Yes	No
Catalyst 6800 Series switches	>=12.2	Cisco IOS 15.1(2)SY4a	Yes	Yes	Yes	Yes	No
Cisco Nexus 5000 Series switches	All versions	NX-OS version 7.2(0)N1(1)	Yes	Yes	No	Yes	No
Cisco Nexus 7000 Series switches	All versions	NX-OS version 6.2(2a) and NX-OS version 6.2(6	Yes	Yes	No	Yes	No

1 The minimum software version is applicable only for Discovery and Inventory. For Path Trace and EasyQoS, be sure to use the recommended software version.

Table 3: Supported Routers

Supported Routers	Minimum Software Version	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Cisco Integrated Services Routers (ISR) G2	>=15.0(1)M, >=15.2(4)M2	Cisco IOS XE 15.2(4)M9, 15.1(4)M7	Yes	Yes	Yes	Yes	Yes
Cisco Integrated Service Router (ISR) 4000 Series	>=15.3(2)S	Cisco IOS XE 3.12.0S	Yes	Yes	Yes	Yes	Yes

Supported Routers	Minimum Software Version	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Cisco ASR 1000 Series Aggregation Services Router	>=15.2(2)S, >=15.3(1)S1	Cisco IOS XE 3.16(2)S	Yes	Yes	Yes	Yes	No
Cisco ASR 9000 Series Aggregation Services Router [2]	>=3.9	Cisco IOS XR 5.1.3	Yes	Yes	No	Yes	No

[2] You must enable NETCONF for the Cisco ASR 9000 router or for any other Cisco device that requires NETCONF support in their device pack. See NETCONF Configuration, on page 12 for additional information about this requirement.

Table 4: Supported Wireless LAN Controllers

Supported Wireless LAN Controllers [3]	Minimum Software Version	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Cisco 2500 Series Wireless Controller	All versions	Cisco IOS 8.1.131.0	Yes	Yes	Yes	Yes	No
Cisco 5500 Series Wireless Controller	All versions	Cisco IOS 8.1.131.0	Yes	Yes	Yes	Yes	No
Cisco 5760 Series Wireless LAN Controller	All versions	Cisco IOS XE 3.3.3SE	Yes	Yes	No	Yes	No
Cisco 8500 Series Wireless Controller	All versions	Cisco WLC 8.1.131.0	Yes	Yes	Yes	Yes	No

Supported Wireless LAN Controllers[3]	Minimum Software Version	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Cisco Wireless Services Module 2 (WiSM2)	8.1.131.0	8.1.131.0	Yes	No	Yes	No	No

[3] **On certain WLCs, you need to configure SNMP traps. See Wireless LAN Controller Configuration, on page 12 for additional information about this configuration requirement.**

Table 5: Supported Service Modules in Cisco ISR G2

Supported Service Modules in Cisco ISR G2	Minimum Software Version	Recommended Software Version	Base Apps Support	Path Trace Support	EasyQoS Support	Path Stats Interface	Path Stats QoS
Cisco 2900 (SM-ES2-16-P, SM-ES2-24-P, SM-D-ES2-48)	>=12.1	Cisco IOS 15.0(2)SE8, 12.2(55)SE10	Yes	Yes	No	Yes	No
Cisco 3900 (SM-ES3-16-P, SM-ES3-24-P, SM-D-ES3-48-P)	>=12.1	Cisco IOS 15.0(2)SE8, 12.2(55)SE10	Yes	Yes	No	Yes	No

Table 6: Industrial Ethernet Switches

Supported Industrial Ethernet Switches	Minimum Software Version	Recommended Software Version	Base Apps	Path Trace	EasyQoS
Cisco Industrial Ethernet 2000 Series Switches	>=12.2	>=12.2	Yes	Yes	No
Cisco Industrial Ethernet 3000 Series Switches	>=12.2	>=12.2	Yes	Yes	No

Required Platform Configurations

This section describes procedures that must be performed on certain specific platforms for the Cisco APIC-EM to properly function.

NETCONF Configuration

You must enable the NETCONF protocol for the Cisco ASR 9000 router or for any other Cisco device that requires NETCONF support for their device pack. If NETCONF is not enabled, then the controller's inventory collection process will be incomplete for that device.

Note Though NETCONF typically runs over SSH or on its own port, with the Cisco APIC-EM and for the Cisco ASR 9000 router NETCONF is run over a CLI session.

For specific information about enabling NETCONF for your own Cisco device, refer to that device's documentation. As an example, a typical configuration sequence on a terminal to enable NETCONF on a Cisco device is as follows:

```
#ssh server v2
#netconf agent tty
#!
#xml agent tty
#!
#commit
#end
#crypto key generate rsa
```

Note The rsa key needs to be generated to succeed with SSH. For this reason, the crypto key generate rsa command needs to be executed in exec mode at the end of the configuration sequence if it has not already been done.

Wireless LAN Controller Configuration

The Cisco APIC-EM accepts SNMP traps from several Cisco Wireless LAN Controllers (WLCs). The SNMP traps are used to update the host inventory database. You need to configure the WLCs so that the Cisco APIC-EM is the trap receiver, and the WLCs send the enhanced traps to the Cisco APIC-EM.

The following WLCs require SNMP traps to be enabled:

- Cisco Series 2504 Wireless LAN Controller
- Cisco Series 5508 Wireless LAN Controller
- Cisco Series 8510 Wireless LAN Controller

The following table specifies the SNMP traps and object identifiers that must be set on the WLCs.

Trap Name	OID
ciscoLwappDot11ClientAssocTrap	1.3.6.1.4.1.9.9.599.0.9

Trap Name	OID
ciscoLwappDot11ClientDeAuthenticatedTrap	1.3.6.1.4.1.9.9.599.0.10
ciscoLwappDot11ClientMovedToRunStateNewTrap	1.3.6.1.4.1.9.9.599.0.11
ciscoLwappDot11ClientMobilityTrap	1.3.6.1.4.1.9.9.599.0.12

The following configurations must be set to enable the above SNMP traps:

- config trapflags client enhanced-802.11-associate enable
- config trapflags client enhanced-802.11-deauthenticate enable
- config trapflags client enhanced-authentication enable
- config trapflags client enhanced-802.11-stats enable

Note When setting the SNMP traps on the WLCs, ensure you configure the IP address of the Cisco APIC-EM as the SNMP trap destination IP address. You set the Cisco APIC-EM IP address using the configuration wizard during the deployment process. For information about this process and the controller IP address, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information.

SNMP Trap Configuration

To ensure that Cisco APIC-EM captures data about the hosts connected to your network devices, you must set up SNMP traps or notifications. Enter the following SNMP commands to set up SNMP traps on the devices that connect to hosts within your network:

1. **snmp-server enable traps snmp linkdown linkup**
2. **snmp-server host** *IP address* **version 2c public**

Note For Cisco Nexus devices, enter the following SNMP commands instead of the commands listed above:

1. **snmp-server enable traps snmp linkdown linkup**
2. **snmp-server host** *IP address* **use-vrf default**

After configuring SNMP traps on the network devices, the following data is captured and made available in the controller's GUI:

- Host data including the MAC address, IP address, and type
- Device interface status

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
- APIC-EM services

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 1.1.2.x

If you use the Cisco IWAN App and want to upgrade to Cisco IWAN App, Release 1.1.0, you must upgrade the Cisco APIC-EM to Release 1.1.2.x as well. To upgrade the Cisco APIC-EM, use the **Software Update** functionality of the controller's GUI. This upgrade procedure requires that you upload and update the new release, as described below.

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 this new Cisco APIC-EM release from the following earlier software and software patch releases:
  - Release 1.1.1.34
  - Release 1.1.1.38

Note If your current Cisco APIC-EM release version is not one of the above releases, then first upgrade to one of these releases before upgrading to Release 1.1.2.x.

- Review the system requirements for your Cisco APIC-EM upgrade. The system requirements may have changed for this release from a previous release and may require that you make changes to your

deployment. See Cisco APIC-EM System Requirements, on page 1. 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 Chapter 6, "Configuring the Cisco APIC-EM Settings," in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.
- Review the lists of Cisco APIC-EM ports that should be made open and available for both incoming and outgoing traffic flows to and from the controller. For information about these ports, see Chapter 3, Cisco APIC-EM Security, in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Step 1 Download the Cisco APIC-EM upgrade for release 1.1.2.x from the Cisco website at the Download Software link.

Step 2 Upload the upgrade to the controller using the **Software Update functionality** of the GUI.
Refer to the "Updating the Cisco APIC-EM" section in Chapter 5 of the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information about this step.

Step 3 Update the controller's software with the upgrade using the **Software Update** functionality of the GUI.
Refer to the "Updating the Cisco APIC-EM" section in Chapter 5 of the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information about this step.

Step 4 Check the controller's software version number in the GUI **Home** window. The GUI **Home** window should display the new software version (1.1.2.x).

Note Upgrading from earlier releases to Cisco APIC-EM release 1.1.2.x using the patch may take up to an hour to complete.

New and Updated Applications

Base Applications

Discovery

The Cisco APIC-EM supports a discovery functionality that is used to populate the controller's device inventory database. You perform a discovery scan by either entering an IP address range for the network devices and/or by using a seed IP with the Cisco Discovery Protocol (CDP). After running a scan, the Cisco APIC-EM populates its database with the collected data from your network devices. The discovery functionality has been enhanced with this release and now permits the user to select specific pre-configured global discovery credentials (CLI and SNMP) for a discovery scan.

EasyQoS

EasyQoS is a new beta feature in release 1.1.x. The EasyQoS beta feature enables you to configure quality of service on the devices in your network that have been discovered by the Cisco APIC-EM.

Using EasyQoS, you can group devices and then assign classes of service to those devices. The Cisco APIC-EM takes your QoS selections, translates them into the proper device configurations, and deploys the configurations onto those devices.

You must enable the EasyQoS beta feature before using it. To enable EasyQoS beta, perform the following steps:

1. In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.
2. Click the **Settings** link from the drop-down menu.
3. In the **Settings** navigation pane, click **EasyQoS Beta** to view the **EasyQoS Beta** window.
4. Click the **Enable EasyQoS** button to activate EasyQoS on the controller.

Note Once enabled, you can only disable EasyQoS by uninstalling and then reinstalling the controller. Any QoS configurations applied to devices using EasyQoS will remain on those devices.

Path Trace

The Path Trace application has been updated so that it now provides a path trace statistics option that accesses the following information

- Interface statistics
- EasyQoS statistics

Solution Applications

Cisco IWAN

Cisco IWAN exposes significant new NB REST APIs in release 1.1 of the Cisco APIC-EM. See the API tab for details.

See Related Documentation, on page 44 for Cisco APIC-EM IWAN documentation.

Caveats

Open Caveats

The following table lists the open caveats for this release.

Caveat ID Number	Headline
CSCuw55732	IS-IS details are not returned for interfaces that are configured for these protocols. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCuw77852	Path Trace fails because of missing CDP 10 GB links on an ASR 9000 in inventory. **Workaround**: There is no workaround at this time.
CSCux18058	Attempting to upload an image a second time after cancelling the original request and using the PnP application's GUI fails. **Workaround**: Access another GUI page and then return to the **Upload** page.
CSCux60211	Error message encountered during a software upgrade from an earlier release to this release, or during a restore process: "An unknown error occurred when uploading. Please try to upload your patch again". If you encounter this error message, then perform the following workaround procedure. **Workaround**: **1** Access the download page for Cisco APIC releases located at the Download Software link. **2** Download the script called *repair_upload*. **3** Using SCP or another secure method, copy the *repair_upload* script to the Grapevine root for your cluster. **4** Run the script on the Grapevine root with root permissions. For example: **sudo ./repair_upload** **5** Proceed to upload the software file or run a restore process again.
CSCux93295	Credential validation does not work for enable password when configuring global CLI credentials. **Workaround**: Provide fully valid credentials in the top of the CLI credential list.

Caveat ID Number	Headline
CSCuy14431	When an update policy is applied to a wireless segment in a scope with an application classified to default category, the policy update to the WLC fails with the message "ROLLBACK_SUCCESS". The application that was moved to default did not get removed from the WLC. **Workaround**: Log out of the session mentioned above and re-apply the policy from Cisco APIC-EM, then the process will be successful again.
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.
CSCuy37529	The GUI is not able to properly display policy tags with long names in the EasyQos application. **Workaround**: Only create policy tags with a maximum of 25 alphanumeric characters.
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.

Caveat ID Number	Headline
CSCuy44164	The Portchannel interface gets suspended when the Cisco APIC-EM attempts to configure the queuing policy on a port-channel member interface, and hence the EasyQos configuration fails and port-channel member interface left in a suspended state. **Workaround**: Ensure that Cisco APIC-EM does not telnet to the Cisco Catalyst 4000 via a port-channel interface IP nor the current management interface is reachable only via one port-channel. We strongly recommended to have redundant port-channels configured for uplink switches to overcome this issue.

Resolved Caveats

There are no resolved caveats for this release (1.1.2.x). This software was released to support deployments that use the Cisco IWAN App, Release 1.1.0. The following table lists the resolved caveats for earlier releases.

Release	Caveat ID Number	Headline
Release 1.1.2.x	—	—
Release 1.1.1.38	CSCux98305	Multi-host Cisco APIC-EM software update or backup and restore process fails when updating the Linux files.
	CSCuy33529	A WS-C3560X-48U-L device goes to partial collection for feature_l2interface with an error message.
	CSCuy34701	When a new Path Trace is requested while the devices and/or hosts are still loading, it will show on the GUI as "Fetching Path" forever.
	CSCuy37255	Controller fails to get commands for passed in configuration by EasyQoS.
	CSCuy40075	Policy fails when a custom app moves from Business Relevance to Default.

Release	Caveat ID Number	Headline
	CSCuy42006	When applying an EasyQoS policy on a Cisco Catalyst 3850 switch, the following error message appears: "Upstream QoS Resource Busy. Try again Later".
	CSCuy43929	The EasyQos configuration fails, when "mls qos trust dscp" is already configured on the switch interfaces.
	CSCuy45957	Certain CVD policy pushes fail in EasyQoS.
	CSCuy46251	There is an observed timeout on a Cisco Catalyst 3850 (9Mem) stack when reapplying a policy with a Custom App in EasyQoS.
	CSCuy54027	Backing up the Cisco APIC-EM database fails.
Release 1.1.0.767	CSCuw50724	Cisco APIC-EM Multi-host: The config_wizard setup for VM-2 shows an incorrect Subnet mask.
	CSCuw62787	Restore fails if the master postgres instance goes down (also after HA failover).
	CSCuw71718	Backup files are deleted after executing the reset_grapevine command on a multi-node cluster.
	CSCuw73429	Discovery shows "in progress" status for a very long time after postgres failover.
	CSCuw84545	Path Trace fails for host when STP is disabled on the host's VLAN subnet.
	CSCuw90460	Wording overlaps with CAPWAP tunnel in the path trace with wireless host.
	CSCuw90989	Sometimes the AP icon is shown as "unknown" device.

Release	Caveat ID Number	Headline
	CSCuw91073	Different CEF lookup CLI for Cisco Catalyst 6000 with Sup720.
	CSCuw96629	Backup failed on 3 node cluster due to race condition.
	CSCux98936	Cisco APIC-EM software upgrade fails if the upgrade image name contains white space.
Release 1.0.3.4	CSCux5394	Services fail to start when Cisco APIC-EM is installed on hardware with 36 CPU processors or more, rendering the controller unusable.
Release 1.0.2.8	CSCux23356	The restore process of a controller's back up remains "in-progress" indefinitely. This issue occurs after shutting down the controller when a restore is in progress.
	CSCux25409	The back up and restore process fails if the operation takes longer than 200 minutes.
	CSCuw77852	Currently, path trace does not work for 10 GB links on the Cisco ASR 9000 routers.
	CSCuw84545	Path trace does not support STP disabled VLANs.
	CSCuw96629	After a back up fails, the user is not able to upload files until a successful backup is created.
Release 1.0.1.30	CSCuw62787	The restore process fails if master postgres instance goes down.
	CSCuw98377	The restore process for the controller failed due to a postgres restore failure.

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.

- 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*.

Security Limitations

- 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, 1.2.0.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

Note 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

- 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.

EasyQoS Support and Limitations

EasyQoS Feature Support by Platform

The Cisco APIC-EM EasyQoS feature support by platform is displayed in the following tables.

Note For this release, EasyQoS is not supported for Cisco Enhanced Ethernet Modules.

Table 7: Cisco Catalyst Switches

Platform	Marking	Queuing	Marking Read only	Queuing Read only	Policing Read only	Shaping Read only	WLAN	Dynamic QoS
2960-S	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
2960-S Stack	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
2960-X	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
3560CG	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
3560-CX	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
3560-X	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
3650	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
3750-X	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
3850	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
4500 Sup7E	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
4500 Sup8E	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
4500-X	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
6500 (2T)	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
6807-XL (2T)	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes
6880	Yes	Yes	Yes	Yes	Yes	Yes	N/A	Yes

Table 8: Cisco Routers

Platform	Marking	Queuing	Shaping	Marking Read only	Queuing Read only	Policing Read only	Shaping Read only	SVI	WLAN	Dynamic QoS
ISR-G2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	N/A
ISR 800	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	N/A
ASR 1000	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	N/A
ISR 4000	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	N/A

Table 9: Cisco Wireless LAN Controllers

Platform	Marking	Queuing WMM	Marking Read only	Queuing Read only	Policing Read only	Shaping Read only	WLAN	Dynamic QoS
WLC 2500	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
WLC 5500	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
WLC 8500	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

EasyQoS Supported Queues and Line Cards

The following tables lists queues and line cards that are supported by the controller for queuing policies in the Catalyst 6000 switches.

Table 10: EasyQoS Supported Queues and Line Cards

Queues	Line Cards
1Q8T (One standard queue with eight configurable tail-drop thresholds)	• WS-X6724-SFP with CFC • WS-X6748-SFP with CFC • WS-X6748-GE-TX with CFC • WS-X6704-10GE with CFC

Queues	Line Cards
2Q4T (Two standard queues with four configurable tail-drop thresholds)	• VS-S2T-10G with Gigabit Ethernet ports enabled • VS-S2T-10G-XL with Gigabit Ethernet ports enabled
2Q8T ingress queuing (Two standard queues, each with eight configurable tail-drop thresholds)	• WS-X6824-SFP-2T • WS-X6824-SFP-2TXL • WS-X6848-SFP-2T • WS-X6848-SFP-2TXL • WS-X6848-TX-2T • WS-X6848-TX-2TXL • C6800-48P-SFP • C6800-48P-SFP-XL • C6800-48P-TX • C6800-48P-TX-XL • WS-X6724-SFP • WS-X6748-SFP • WS-X6748-GE-TX **Note** The WS-X6724-SFP, WS-X6848-SFP, and WS-X6748-GE-TX line cards are only supported with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A or WS-F6k-DFC4-AXL).
8Q4T ingress queuing (Eight standard queues, each with four thresholds, each configurable as either WRED-drop or tail-drop)	• VS-S2T-10G, VS-S2T-10G-XL with Gigabit Ethernet ports disabled • WS-X6908-10G-2T, WS-X6908-10G-2TXL • WS-X6816-10T-2T, WS-X6816-10T-2TXL, WS-X6816-10G-2T, WS-X6816-10G-2TXL in performance mode • WS-X6716-10G-3C, WS-X6716-10G-3CXL, WS-X6716-10T-3C, WS-X6716-10T-3CXL also supported with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-E, WS-F6k-DFC4-EXL) in performance mode

Queues	Line Cards
8Q8T ingress queuing (Eight standard queues, each with eight thresholds, each configurable as either WRED-drop or tail-drop)	• WS-X6704-10GE **Note** The WS-X6704-10GE line cards are only supported with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL).
1P3Q4T (One strict-priority queue, three standard queues, four thresholds, each configurable as either WRED-drop or tail-drop)	• VS-S2T-10G with Gigabit Ethernet ports enabled • VS-S2T-10G-XL with Gigabit Ethernet ports enabled
1P3Q8T egress queuing (One strict-priority queue, three standard queues, eight thresholds, each configurable as either WRED-drop or tail-drop)	• WS-X6724-SFP • WS-X6748-SFP • WS-X6748-GE-TX • WS-X6824-SFP-2T • WS-X6824-SFP-2TXL • WS-X6848-SFP-2TXL • WS-X6848-SFP-2T • WS-X6848-TX-2T • WS-X6848-TX-2TXL • C6800-48P-SFP • C6800-48P-SFP-XL • C6800-48P-TX • C6800-48P-TX-XL **Note** The above line cards are only supported under the following conditions: • Line card WS-X6724-SFP with CFC, or with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL). • Line card WS-X6748-SFP with CFC, or with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL). • Line card WS-X6748GE-TX with CFC, or with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL).

Queues	Line Cards
1P7Q2T (One strict-priority queue, seven standard queues, two thresholds, each configurable as either WRED-drop or tail-drop)	• WS-X6816-10T-2T, WS-X6816-10T-2TXL, WS-X6816-10G-2T, WS-X6816-10G-2TXL in oversubscription mode • WS-X6716-10G-3C, WS-X6716-10G-3CXL, WS-X6716-10T-3C, WS-X6716-10T-3CXL also supported with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-E, WS-F6k-DFC4-EXL) in oversubscription mode
1P7Q4T egress queuing (One strict-priority queue, seven standard queues, four thresholds, each configurable as either WRED-drop or tail-drop)	• WS-X6908-10G-2T, WS-X6908-10G-2TXL, WS-X6816-10T-2T, WS-X6816-10T-2TXL, WS-X6816-10G-2T, WS-X6816-10G-2TXL in performance or oversubscription mode • WS-X6716-10G-3C, WS-X6716-10G-3CXL, WS-X6716-10T-3C, WS-X6716-10T-3CXL also supported with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-E, WS-F6k-DFC4-EXL)in performance or oversubscription mode
1P7Q8T (One strict-priority queue, seven standard queues, eight thresholds, each configurable as either WRED-drop or tail-drop)	• WS-X6704-10GE **Note** Line card WS-X6704-10GE is only supported with CFC, or with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL).
2P6Q4T ingress and egress queuing (Two strict-priority queues, six standard queues, four thresholds, each configurable as either WRED-drop or tail-drop)	• WS-X6904-40G-2T • WS-X6904-40G-2TXL • C6800-32P10G • C6800-32P10G-XL • C6800-16P10G • C6800-16P10G-XL • C6800-8P10G • C6800-8P10G-XL

EasyQoS Limitations

The following table describes the EasyQoS limitations for this release.

Table 11: Cisco APIC-EM EasyQoS Release Limitations

Platform	Description	Affected Software Versions
Catalyst 3850 and 3650 Series Switches	A policy-map which contains a class-map which consists of an empty action cannot be applied to an interface prior to IOS XE release 3.6.2.	Catalyst 3850 and 3650 IOS XE software releases prior to 3.6.2.
Catalyst 6500 Series Switches with Sup2T	CSCup61257 - Error message not printing if unsupported QoS is applied via SSH/Telnet. The Cisco APIC-EM may have trouble identifying when a QoS policy it has applied has failed due to this bug.	• 15.1(02)SY03, s2t54-adventerprisek9-mz.SPA • 151-2.SY3.bin, s2t54-adventerprisek9-mz.SPA • 150-1.SY6.bin, s2t54-adventerprisek9-mz.SPA • 150-1.SY6.bin listed in the DDTS **Note** This issue may affect other software versions.
Catalyst 6500 Series Switches with Sup2T with the following line cards: • WS-X6716 Series • WS-X6816 Series • WS-X6908 Series	Cisco APIC-EM is currently unable to determine if certain line cards are operating in Performance Mode or Oversubscription Mode. Ingress queuing on these line cards differs between the two modes of operation. Hence, when Cisco APIC-EM pushes ingress marking policies to these ports, the policy may fail.	All Catalyst 6500 software versions which support the Sup2T - 12.2(50)SY and higher.
Catalyst 6500 Series Switches with Sup2T	Cisco APIC-EM is currently unable to determine if 1 Gigabit Ethernet ports on the Sup2T are enabled or disabled. Ingress queuing of all ports on the Sup2T differs when the Gigabit Ethernet interfaces are enabled or disabled. Hence, when Cisco APIC-EM pushes ingress marking policies to ports on the Sup2T, the policy may fail.	All Catalyst 6500 software versions which support the Sup2T - 12.2(50)SY and higher.

Platform	Description	Affected Software Versions
The following platforms: • Catalyst 2960-X • Catalyst 3750-X • Catalyst 3560-X • Catalyst 2960-X • Catalyst 3560-C	The Catalyst 2960-X, Catalyst 3750-X, Catalyst 3560-X, Catalyst 2960-X, Catalyst 3560-C platforms will only be supported as access-layer switches in the initial release of EasyQoS (GA+1).	All supported software versions of the Catalyst 2960-X, Catalyst 3750-X, Catalyst 3560-X, Catalyst 2960-X, Catalyst 3560-C platforms.
The following switches: • Catalyst 6500 Series with Sup2T • Catalyst 6880 Series • Catalyst 4000 Series • Catalyst 3850 Series • Catalyst 3650 Series	The Catalyst 6500 Series with Sup2T, Catalyst 6880 Series, Catalyst 4000 Series, Catalyst 3850 Series, and Catalyst 3650 Series switches will only be supported as an access-layer switch or as a distribution-layer switch in the initial release of EasyQoS (GA+1) Support of a single switch as both a distribution-layer switch and an access-layer switch simultaneously is not supported. Multiple switch platforms of the same model can of course individually be either distribution layer switches or access-layer switches within a single deployment.	All supported software versions of the Catalyst 6500 Series with Sup2T, Catalyst 6880 Series, Catalyst 4000 Series, Catalyst 3850 Series, and Catalyst 3650 Series switches
Catalyst 2960-S Series Switches	Catalyst 2960S-24TS-S and 2960S-48TS-S switch models are not supported in the initial release of Cisco APIC-EM EasyQoS. These switches only support the LAN Lite feature set which does not support class and policy maps per the following document: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/qa_c67-726679.html	All IOS software versions for these models.

Platform	Description	Affected Software Versions
Catalyst 2960-S Series Switches	Catalyst 2960-S Series switch models support 384 QoS TCAM entries only when configured with the QoS SDM template. Default SDM Template supports 128 QoS TCAM entries. Catalyst 2960S Series switch models are only be supported if the customer has previously configured the QoS SDM template. Cisco APIC-EM EasyQoS cannot determine this currently. (Note that changing the SDM template rmay require reloading the switch or switch stack).	All IOS software versions for these models.
Catalyst 2960-SF Series Switches	Catalyst 2960S-F24TS-S and 2960S-F48TS-S switch models are not supported in the initial release of Cisco APIC-EM EasyQoS. These switches only support the LAN Lite feature set which does not support class and policy maps per the following document: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/qa_c67-726679.html	All IOS software versions for these models.
The following switches: • Catalyst 2960-S Series Switches • Catalyst 2960-X Series Switches • Catalyst 2960-XR Series Switches • Catalyst 3560-X Series Switches • Catalyst 3750-X Series Switches	Catalyst 2960-S Series, Catalyst 2960-X Series, Catalyst 2960-XR Series, Catalyst 3560-X Series, and Catalyst 3750-X Series switches are supported in the role of access switches only for the initial release of Cisco APIC-EM EasyQoS. These switch platforms will not be supported in the role of distribution or core switches.	All IOS software versions for these models.

Platform	Description	Affected Software Versions
Cisco ASR 1000 Router Platforms	Cisco APIC-EM EasyQoS supports ASR 1000 platforms with IOS XE 3.8.0(S) / IOS 15.3(1)S and higher. However, the ingress marking policy pushed by EasyQoS varies based upon the IOS XE version as well as the NBAR2 protocol pack version. EasyQoS will push an ingress marking policy to ASR 1000 platforms based on the following criteria: **1** If the device is running IOS XE 3.16.1S / IOS 15.3(1)S or later and has Advanced Protocol Pack 14.0.0 or later, EasyQoS will push a policy-map which includes the business-relevance attribute for marking. This is because the business-relevant attribute requires a minimum version of IOS XE 3.16.1S and Advanced Protocol Pack 14.0.0. ASR 1000 platforms require an Advanced Enterprise Services (AES) or Advanced IP Services (AIS) license for NBAR2 Advanced Protocol Pack. **2** Otherwise, if the device is running IOS XE3.16, 3.15 and 3.14, or has a Standard Protocol Pack installed, or runs a older protocol pack which does not support metadata information, EasyQoS will not push any ingress marking policy. **3** Otherwise, EasyQoS will push a policy-map which includes “match protocol” commands, with the subset of the protocols that exist on the protocol pack on that device. Cisco APIC-EM EasyQoS will always push a queuing policy to the device.	Software versions noted within the Description.

Platform	Description	Affected Software Versions
Cisco ISR 4000 Series Router Platforms	Cisco APIC-EM EasyQoS supports the ISR 4321, 4331, 4351, and 4431 platforms with IOS XE 3.13.2(S) / IOS 15.4(3)S and higher (minimum releases supported by the platforms). Cisco APIC-EM EasyQoS supports the ISR 4451-X platforms with IOS XE 3.10.0(S) / IOS 15.3(3)S and higher (minimum releases supported by the platforms). However, the ingress marking policy pushed by EasyQoS varies based upon the IOS XE version as well as the NBAR2 protocol pack version. EasyQoS will push an ingress marking policy to ISR 4000 Series platforms based on the following criteria: **1** If the device is running IOS XE 3.16.1S or later and has Advanced Protocol Pack 14.0.0 or later, EasyQoS will push a policy-map which includes the business-relevance attribute for marking. This is because the business-relevant attribute requires a minimum version of IOS XE 3.16.1S and Advanced Protocol Pack 14.0.0. ISR 4000 Series platforms require an Application Experience (AppX) license for NBAR2 Advanced Protocol Pack. **2** Otherwise, if the device is running IOS XE3.16, 3.15 and 3.14, or has a Standard Protocol Pack installed, or runs a older protocol pack which does not support metadata information, EasyQoS will not push any ingress marking policy. **3** Otherwise, EasyQoS will push a policy-map which includes “match protocol” commands, with the subset of the protocols that exist on the protocol pack on that device. Cisco APIC-EM EasyQoS will always push a queuing policy to the device.	Software versions noted within the Description .

Platform	Description	Affected Software Versions
Cisco ISR G2 Series Router Platforms	Cisco APIC-EM EasyQoS supports the ISR G2 platforms with IOS 15.2(4)M and NBAR2 Protocol Pack 2.1.0 and higher. However the ingress marking policy pushed by EasyQoS varies based upon the IOS version as well as the NBAR2 protocol pack version. EasyQoS will push an ingress marking policy to ISR G2 Series platforms based on the following criteria: **1** If the device is running IOS 15.5(3)M1 or later and has Advanced Protocol Pack 14.0.0 or later, EasyQoS will push a policy-map which includes the business-relevance attribute for marking. This is because the business-relevant attribute requires a minimum version of IOS 15.5(3)M1 and Advanced Protocol Pack 14.0.0. ISR G2 Series platforms require a Data license for NBAR2 Advanced Protocol Pack. **2** Otherwise, if the device has a Standard Protocol Pack installed, or runs a older protocol pack which does not support metadata information, EasyQoS will not push any ingress marking policy. **3** Otherwise, EasyQoS will push a policy-map which includes “match protocol” commands, with the subset of the protocols that exist on the protocol pack on that device. Cisco APIC-EM EasyQoS will always push a queuing policy to the device.	Software versions noted within the Description.
Cisco ISR G2 Series Router Platforms	Etherswitch modules are not supported with the initial (GA+1) release of Cisco APIC-EM EasyQoS. NBAR2 ingress marking policies will need to be applied to VLAN interfaces associated with Etherswitch modules, which is not supported in the current release.	All IOS software versions for these models.

Path Trace Support and Restrictions

The following tables describe the Cisco APIC-EM Path Trace support and restrictions.

Protocol Support by Platform

The following table describes protocol support by platform for a path trace.

Platform[4]	HSRP[5]	Physical Interface	Sub-Interface	SVI[6]	PVST[7]	Ether Channel (L2)	ECMP[8]	Ether Channel (L3)	Routing Protocols (L3)[9]	Net Flow[10]	Trace Route
2960-S	Yes	N/A	N/A	N/A	Yes	Yes	No	No	Yes	N/A	N/A
2960-S (stack)	Yes	N/A	N/A	N/A	N/A	Yes	No	No	Yes	N/A	N/A
3560-X	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
3560CG	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	N/A
3560CX	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	N/A
3650	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
3750-X	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
3750-X (stack)	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
3850	Yes	Yes	N/A	Yes	Yes	Yes	No	No	Yes	N/A	Yes
3850 (stack)	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
4500E (Sup7E)	Yes	Yes	N/A	Yes	Yes	Yes	No	No	Yes	N/A	Yes
6500 (Sup720-3C/B)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
6500(2T)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
6800	Yes	Yes	N/A	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes
WLC 2504	N/A	N/A	N/A	N/A	N/A	Yes	N/A	N/A	N/A	N/A	N/A

Platform[4]	HSRP[5]	Physical Interface	Sub-Interface	SVI[6]	PVST[7]	Ether Channel (L2)	ECMP[8]	Ether Channel (L3)	Routing Protocols (L3)[9]	Net Flow[10]	Trace Route
WLC 5500	N/A	N/A	N/A	N/A	N/A	Yes	N/A	N/A	Yes	N/A	N/A
WLC 5760	N/A	N/A	N/A	N/A	N/A	Yes	N/A	N/A	N/A	N/A	N/A
WLC 8500	N/A	N/A	N/A	N/A	N/A	Yes	N/A	N/A	N/A	N/A	N/A
ASR 1K	Yes	Yes	Yes	Yes	N/A	No	Yes	No	Yes	Yes	Yes
ASR 9K	Yes	Yes	Yes	Yes	N/A	No	Yes	No	Yes	Yes	Yes
ISR-G2	Yes	Yes	Yes	Yes	N/A	No	Yes	No	Yes	Yes	Yes
ISR-4451 -X	Yes	Yes	Yes	Yes	N/A	No	Yes	No	Yes	Yes	Yes
Nexus 5000	Yes	Yes	N/A	Yes	Yes	Yes	No	No	Yes	N/A	Yes
Nexus 7000	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	N/A	Yes

4 Virtual Routing and Forwarding (VRF) is not supported for the wired platforms and is not applicable for the wireless platforms.
5 Hot Standby Router Protocol (HSRP).
6 Switch Virtual Interface (SVI)
7 Per VLAN Spanning Tree Protocol (PVST)
8 Equal Cost Multipath (ECMP)
9 Supported Layer 3 routing protocols include: static, OSPF, EIGRP, IS-IS, and BGP. The following Layer 3 protocol is not supported: PBR.
10 NetFlow needs to be enabled on the supported device. The controller pulls cached NetFlow records from the device.

Wireless AP Support by Platform

The following table describes wireless application point (AP) support by platform for a path trace.

Platform	AP Manager	
	LAG[11]	Physical
WLC 2504	Yes	Yes
WLC 5500	Yes	Yes
WLC 5760	Yes	Yes

Platform	AP Manager	
WLC 8500	Yes	Yes

11 Link Aggregation Group (LAG)

Wireless Mode Support by Platform

The following table describes wireless mode support (deployment and mobility) by platform for a path trace.

Platform[12]	Wireless Deployment Mode			Wireless Mobility Mode		
	Centralized[13]	Flex	Converged	Centralized	Converged	Hybrid[14]
WLC 2504	Yes	No	No	Yes	No	No
WLC 5500	Yes	No	No	Yes	No	No
WLC 5760	Yes	No	No	Yes	No	No
WLC 8500	Yes	No	No	Yes	No	No

12 WLC redundancy and high availability is not supported.
13 Catalyst 3850 switch and stack do not support converged wireless deployment mode for a path trace.
14 Catalyst 3850 switch and stack do not support hybrid wireless mobility mode for a path trace.

Path Trace Supported Scenarios

The following table describes the supported scenarios for a path trace.

Scenario	Protocol	Feature List	Configuration	Suported
Gateway Load Balancing	HSRP	Interface and Media Support	Physical Interface	Yes
			SVI	Yes
			BVI	No
			Sub Interface	Yes
		Load sharing on same link	Same interface part of more than one HSRP group	No
		Load sharing across links	—	Yes

Scenario	Protocol	Feature List	Configuration	Suported
Wireless Deployment Modes	Centralized	Interface support	Management Interface	Yes
			AP Mgr Interface	Yes
			Dynamic Interface	No
		AP Load Balancing	AP load balance across single port channel	Yes
			Single AP Manager Interface Configuration	Yes
			Multiple AP Manager Interface Configuration and load balance it on different physical interface	Yes
			Interface Group	Yes
		WLAN	Dynamic Interfaces per WLAN mapped to physical interface	Yes
			Dynamic Interfaces per WLAN Over LAG	Yes
		Management Interface configuration	Untagged	No
			Tagged with a VLAN	Yes
Wireless Mobility Modes	Centralized	Auto-Anchor Mobility	—	Yes
		Symmetric Mobility Tunneling	—	Yes
		Asymmetric Mobility Tunneling	—	No
		Layer 2 and Layer 3 Roaming	—	Yes

Scenario	Protocol	Feature List	Configuration	Suported
Layer 2 Load Balancing	STP	PVST	—	Yes
	EtherChannel	Port channel	Spanning Tree on PO	Yes
			Display Member Link derived after load balancing	No
		Static port channels	Mode On	Yes
		Dynamic port channels	LACP	Yes
		Multi Chassis redundancy	M-LACP	No
	ECMP	Only Layer 3 data forwarding interfaces.	—	—
		No management interfaces	—	—

Scenario	Protocol	Feature List	Configuration	Suported
Layer 3 Load Balancing	ECMP	Routing Recursive Lookup Levels	Five Levels	Yes
		ECMP over Physical interface	—	Yes
		ECMP over SVI	Load balance within SVIs or SVI + port channel	No
		OSPF / BGP / EIGRP / ISIS / Static Route	—	Yes
		ECMP over Sub-Interface	—	Yes
	EtherChannel	Port channel	IPV4 address	No
			Display Member Link derived after load balancing	No
		Static port channels	Mode on	No
		Dynamic port channels	LACP / PAGP	No
		Multi Chassis redundancy	M-LACP	No

Service and Support

Troubleshooting

See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment 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, Release 1.2.0.x*.
• 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

For this type of information...	See this document...
API functions, parameters, and responses.	*APIC-EM API Reference Guide* on Cisco DevNet
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)* on Cisco DevNet
Hands-on coding experience calling APIC-EM NB REST API from Python.	*APIC-EM Learning Labs* on Cisco DevNet

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.