Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.0.2.x

First Published: November 2, 2015
Last Modified: December 01, 2015
Cisco APIC-EM Release, 1.0.2.x

These release notes describe the features and caveats for the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM).

Contents

Cisco Systems, Inc.
www.cisco.com

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)—2000
- Hosts—20000 (12000 wireless and 8000 wired hosts)
- Access Points—2000

What's New in Cisco APIC-EM, Release 1.0.2.x

Cisco is providing a software upgrade patch that resolves several CDETs and is designed to enhance your controller's performance and stability. You should upgrade your controller to Cisco APIC-EM release 1.0.2.x with this software upgrade patch. Refer to Upgrading to Cisco APIC-EM, Release 1.0.2.8, page 7, for information about the upgrade procedure.

Cisco APIC-EM System Requirements

The Cisco APIC-EM can be installed and operate within a dedicated physical server (bare-metal) or a virtual machine within a VMware vSphere environment.

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"). 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").

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 high availability and redundancy.

Physical Server Options	Server Image Format	Bare Metal/ISO
Hardware Specifications	CPU (cores)	6
	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 **Note:** A single network adapter or network interface controller (NIC) is the minimum requirement. For security, we recommend that you use and configure two NICs on the server. See **Security** in the **Limitations and Restrictions** section of these release notes for additional information.
Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: ■ Google Chrome – 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 high availability and redundancy.

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 APIC-EM directly on physical hardware.

Virtual Machine Options	VMware ESXi Version	5.1/5.5
	Server Image Format	ISO
Hardware Specifications	Virtual CPU (vCPU)	6
	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 **Note:** A single network adapter or network interface controller (NIC) is the minimum requirement. For security, we recommend that you use and configure two NICs on the server. See **Security** in the **Limitations and Restrictions** section of these release notes for additional information.
Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: ■ Google Chrome – version 46.0 or later

Cisco APIC-EM Controller Appliances

You can purchase a dedicated Cisco APIC-EM physical appliance with the Cisco APIC-EM ISO image pre-installed and tested.

The following two physical appliances are currently available for purchase:

- Cisco APIC-EM Controller Appliance 10C-64G-2T (APIC-EM-APL-R-K9)
- Cisco APIC-EM Controller Appliance 20C-128G-4T (APIC-EM-APL-G-K9)

Contact your Cisco account representative for additional information about the above appliances and for ordering information.

Supported Platforms and Software Requirements

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

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.*

Table 1 Supported Switches

Supported Switches	Minimum Software Version	Recommended Software Version
Catalyst 2960-S Series switches	>=12.1	Cisco IOS 15.2(1)E1, 12.2(58)SE2
Catalyst 2960-X/XR Series switches	>=12.1	Cisco IOS 15.2.3E, 15.0.2-EX5
Catalyst 3560CG Series switches	>=12.2	Cisco IOS 15.0(2)SE5, 12.2(55)EX3
Catalyst 3560-X Series switches	>=12.2	Cisco IOS 15.2(1)E1, 12.2(58)SE2
Catalyst 3650 Series switches	All versions	Cisco IOS 3.3.2SE, 3.2.3SE
Catalyst 3750-X Series switches	>=12.2	Cisco IOS 15.2(1)E1, 12.2(55)SE8
Catalyst 3850 Series switches	All versions	Cisco IOS 3.3.2SE, 3.2.3SE
Catalyst 4500(Sup7E) Series switches	All versions	Cisco IOS 3.5(2)E, 3.2(8)SG
Catalyst 4500E(Sup8E) Series switches	All versions	Cisco IOS 3.3.2XO, 3.6.1E
Catalyst 4500-X Series switches	All versions	Cisco IOS 3.6.3E
Catalyst 6500 (Supervisor Engine 720-3C/B) Series switches	>=12.2	Cisco IOS 15.1(2)SY2
Catalyst 6500(2T) Series switches	>=12.2	Cisco IOS 15.1(2)SY2, 15.0(1)SY6
Catalyst 6880-X Series switches	>=12.2	Cisco IOS 15.1(2)SY2
Cisco Nexus 5000 Series switches	All versions	Cisco NX-OS 7.2(0) N1(1)
Cisco Nexus 7000 Series switches	All versions	Cisco NX-OS 6.2(2a) Cisco NX-OS 6.2(6)

Table 2 Supported Routers

Supported Routers	Minimum Software Version	Recommended Software Version
Cisco Integrated Services Routers (ISR) G2	>=15.0(1)M, >=15.2(4)M2	Cisco IOS XE 15.2(4)M5, 15.1(4)M7
Cisco Integrated Service Router (ISR) 4000 Series	>=15.3(2)S	Cisco IOS XE 3.12.0S
Cisco ASR 1000 Series Aggregation Services Router	>=15.2(2)S, >=15.3(1)S1	Cisco IOS XE 3.11(2)S
Cisco ASR 9000 Series Aggregation Services Router[1]	>=3.9	Cisco IOS XR 5.3.1
Cisco Cloud Services Router 1000v	IOS-XE 3.16.S (ED)	IOS-XE 3.16.S (ED)

1. 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 for additional information about this requirement.

Table 3 Supported WLCs[1]

Supported Wireless LAN Controllers	Minimum Software Version	Recommended Software Version
Cisco 2500 Series Wireless Controller	All versions	Cisco IOS 7.6(110.0), 7.4(121.0)
Cisco 5500 Series Wireless Controller	All versions	Cisco IOS 7.6(110.0), 7.4(121.0)
Cisco 5760 Series Wireless LAN Controller	All versions	Cisco IOS XE 3.3.3SE
Cisco 8500 Series Wireless Controller	All versions	Cisco WLC 7.6(110.0), 7.4(121.0)

1. On certain WLCs, you need to configure SNMP traps. See Wireless LAN Controller SNMP Configurations for additional information about this configuration requirement.

Table 4 Supported Service Modules in Cisco ISR G2

Supported Service Modules in Cisco ISR G2	Minimum Software Version	Recommended Software Version
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
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

Table 5 Supported Industrial Ethernet Switches

Supported Industrial Ethernet Switches	Minimum Software Version	Recommended Software Version
Cisco Industrial Ethernet 2000 Series Switches	>=12.2	>=12.2
Cisco Industrial Ethernet 3000 Series Switches	>=12.2	>=12.2

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 SNMP Configurations

For this release, the Cisco APIC-EM accepts SNMP traps from certain specific Cisco Wireless LAN Controllers (WLCs). The SNMP traps are used to update the controller's wireless host table. The WLCs should be configured so that Cisco APIC-EM is the trap receiver and the WLCs send the enhanced trap notifications (SNMP messages) to the Cisco APIC-EM.

The following WLCs require SNMP traps to be enabled:

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

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

Table 6 SNMP Traps

Trap Name	OID
ciscoLwappDot11ClientAssocTrap	1.3.6.1.4.1.9.9.599.0.9
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 configuring SNMP traps on the WLCs, the destination for SNMP messages should be the IP address of the Cisco APIC-EM for a single host deployment. For a multi-host deployment, the virtual IP address (VIP) should be used. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information.

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 4, “Deploying the Cisco APIC-EM,” in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

Upgrading to Cisco APIC-EM, Release 1.0.2.8

You can upgrade from an earlier Cisco APIC-EM release to Cisco APIC-EM release 1.0.2.8 using the **Software Update** functionality of the controller's GUI. This upgrade procedure requires that you upload and update a new software patch (upgrade patch for release 1.0.2.8), as described below.

You should upgrade your controller to Cisco APIC-EM release 1.0.2.8 with the upgrade patch. This upgrade patch is designed to enhance your controller’s performance and stability.

Note: For upgrading from Cisco APIC-EM release 0.9.2.x to this Cisco APIC-EM 1.0.2.8 release, you must also *first* verify, upload, and update a pre-upgrade patch. After performing these tasks with the pre-upgrade patch, then proceed with the steps below. This pre-upgrade patch is available from the Cisco website.

Step 1 Download the Cisco APIC-EM upgrade patch for release 1.0.2.8 from the Cisco website at the Download Software link.

Step 2 Proceed to verify the patch by running a checksum against it.

Refer to the procedure described in the “Updating the Cisco APIC-EM” section in Chapter 5 in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information about this step.

Step 3 Upload the patch to the controller using the **Software Update** functionality of the GUI.

Refer to the procedure described in the “Updating the Cisco APIC-EM” section in Chapter 5 in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information about this step.

Step 4 Update the controller's software with the patch using the **Software Update** functionality of the GUI.

Refer to the procedure described in the “Updating the Cisco APIC-EM” section in Chapter 5 in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for additional information about this step.

Step 5 Check the controller’s software version number in the GUI **Home** window. The GUI **Home** window should display the new software version (1.0.2.8).

Note: Upgrading from earlier releases to Cisco APIC-EM release 1.0.2.8. using the patch may take up to an hour to complete.

Cisco APIC-EM Licensing Requirements

The Cisco APIC-EM has the following licensing requirements:

- Cisco APIC-EM—License required to run the controller itself and the base applications (Discovery, Topology, Cisco Network PnP, and Path Trace).

  No fee-based license is required.

- Cisco Enterprise Management 3.x License—A fee-based license is required to run Prime Infrastructure 3.x (PI 3.x) and the Cisco IWAN application (a Cisco APIC-EM solution application).

For more information, please refer to the Cisco Enterprise Management Ordering Guide:

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

Applications

The Cisco APIC-EM base and solution applications are described in the following sections:

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.

Device Inventory

The Cisco APIC-EM collects key information about the devices within your network including the device IP address, MAC address, IOS/firmware, configuration, etc., and then displays this data in the GUI.

Host Inventory

The Cisco APIC-EM collects key information about the hosts within your network using either IP device tracking (when you manually enable IP device tracking on devices and interfaces), a CDP neighbor ship table, the Link Layer Discovery Protocol (LLDP), or LLDP-MED. Data displayed in the GUI about the hosts include the IP address, MAC address, and network attachment point.

Topology

Cisco APIC-EM supports a graphical view of your network (topology view). The Cisco APIC-EM automatically discovers and maps devices to a physical topology with detailed device level data. In addition, auto-visualization of Layer 2 and 3 topologies on top of the physical topology provides a granular view for design planning and simplified troubleshooting.

Path Trace

Cisco APIC-EM supports a path trace application to monitor and debug paths distributed in various devices within your network in a centralized manner.

Note: Path trace requires SSH or Telnet access to the devices.

Solution Applications

Cisco IWAN

Cisco IWAN application on the APIC-EM extends Software Defined Networking to the branch with an application-centric approach based on business policy and application rules. This provides IT centralized management with distributed enforcement across the network.

See the "Related Documentation" section for Cisco IWAN documentation.

Cisco Network Plug and Play

The Cisco Network Plug and Play (PnP) application simplifies network device provisioning by securely and automatically delivering software image and configuration files to supported Cisco devices, based on predefined rules. The application communicates with a Cisco Plug and Play agent in the software image of supported Cisco devices.

See the "Related Documentation" section for Cisco Network Plug and Play documentation.

Caveats

Resolved Caveats in Release 1.0.2.8

- CSCux23356

  Issue: 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.

  This issue has been resolved.

- CSCux25409

  Issue: The back up and restore process fails if the operation takes longer than 200 minutes.

  This issue has been resolved.

- CSCuw77852

  Issue: Currently, path trace does not work for 10 GB links on the Cisco ASR 9000 routers.

  This issue has been resolved.

- CSCuw84545

  Issue: Path trace does not support STP disabled VLANs.

  This issue has been resolved.

- CSCuw96629

  Issue: After a back up fails, the user is not able to upload files until a successful backup is created.

  This issue has been resolved.

Resolved Caveats in Release 1.0.1.30

- CSCuw62787

  Issue: The restore process fails if master postgres instance goes down.

  This issue has been resolved.

- CSCuw98377

  Issue: The restore process for the controller failed due to a postgres restore failure.

  This issue has been resolved.

Open Caveats

- CSCuw41512

  Issue: Currently, the Cisco Wireless Services Module 2 (WiSM2) is not discoverable by the controller as it does not support CDP when an upstream router or switch IP address is used as the seed IP address and using the auto CDP discovery method. On the Cisco Catalyst 6000 switches, use the following command to detect WiSM2 status and add it to the inventory.

  ```
  # show wism status
  ```

  Workaround: There is no workaround at this time.

- CSCuw50724

  Issue: The configuration wizard setup for second virtual machine (VM-2) shows an incorrect subnet mask

  Workaround: There is no workaround at this time.

- CSCuw63545

  Issue: Inventory collection from devices need to login to a device via the CLI. This requires 2-3 available vty sessions. In case there are not enough vty sessions available (because of multiple management system talking to the devices, as an example) then the status may show as “partial collection failure”.

  Workaround: Configure additional vty sessions.

- CSCuw71718

  Issue: After running the **reset_grapevine** command, all of the Cisco APIC-EM back up files are deleted on the controller.

Workaround: Prior to running the **reset_grapevine** command for any procedure, you should download the backup files from the controller to another location on your laptop or network.

- CSCuw73429

  Issue: When running a discovery on the controller, an **"**in progress**"** message appears for a very long time after a postgres failover.

  Workaround: Delete or cancel the discovery job which is showing as **"**in-progress**"**, and then start a new discovery if needed.

- CSCuw88692

  Issue: ECMP is not supported in path trace for the Cisco ASR 9000.

  Workaround: There is no workaround at this time.

- CSCuw90460

  Issue: With a wireless host, wording overlaps appear in the GUI with CAPWAP tunnels in the path trace.

  Workaround: There is no workaround at this time.

- CSCuw90989

  Issue: At times, the access point icon in the GUI displays as an "unknown" device.

  Workaround: There is no workaround at this time.

- CSCuw91073

  Issue: Path trace is not supported for ECMP on Catalyst 6000 switches with the Sup720.

  Workaround: There is no workaround at this time.

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.

Tip 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.
- 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.
- The **Make a wish!** feature (accessible from the Cisco APIC-EM GUI) does not work with an authenticated proxy.

Security

- For this release, privacy is not enabled for all of the communications that occur between the Cisco APIC-EM hosts. For this reason, we strongly recommend that any multi-host cluster that you set up be 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.

- For the Cisco APIC-EM to perform a secure discovery of network devices using the various device management protocols, we strongly recommend that you configure a separate external network interface and dedicated static routes to reach the network device's control planes. In other words, structure your deployment so that the northbound API based applications and the controlled devices are in separate segmented networks. As an example, configure the NICs on the controller as follows:

  — For eth0, configure the NIC so that its network access is accessible only to northbound based API applications

  — For eth1, configure the NIC so that its network access is accessible only to the device control plane network(s)

  With the above recommended configuration, no northbound based API applications will have direct access to the control plane of any Cisco APIC-EM controlled device.

- 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.

Software Update

- Several minutes after starting an **Software Update** operation, the Cisco APIC-EM GUI may display an error message stating “Something went wrong when trying to update. Please check Grapevine logs for more details.”. This message can be ignored, as the update is still occurring in the background.

- Upgrading your Cisco APIC-EM release may take up to an hour to complete.

Back Up and Restore

Caution 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 can take a back up from a single host (not in a multi-host cluster) and then restore it to a single host (not in a multi-host cluster).

  — 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).

  We recommend that you do not back up and restore from a single host and apply it to multi-host and vice versa for this release.

- After performing a back up and restore of the controller, you will need to log into the host and run the **reset_grapevine** command. Before running the **reset_grapevine** command, we recommend that you first run the **grape backup display** command and review the command output to confirm that the restore process was successful. For detailed information about the back up and restore process and these commands, see the Chapter 5, Configuring the Cisco APIC-EM Settings, in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide, Release 1.0*.

- 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 as the controller where the backup was originally taken from.
- 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.

Deployment

- 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:

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

  b. Enter the **mount** command to determine the device that is attached to the /media mount point. This should be your USB flash drive.

  c. Enter the **umount /media** command to unmount the USB flash drive.

  d. 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
  ```

  e. Press **Alt**+**F1** to return to the installation error screen.

  f. 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

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

Service Logs

- High availability is not supported for the service logs in a multi-host cluster. If a host restarts or fails in the cluster, then the service logs may be lost.

Users

- 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

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.

Table 7 Protocol Support by Platform

Platform[1]	HSRP[2]	Physical Interface	Sub-Interface	SVI[3]	PVST[4]	EtherChannel (L2)	ECMP[5]	EtherChannel (L3)	Routing Protocols (L3)[6]	NetFlow[7]	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
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

Table 7 Protocol Support by Platform (continued)

Platform[1]	HSRP[2]	Physical Interface	Sub-Interface	SVI[3]	PVST[4]	EtherChannel (L2)	ECMP[5]	EtherChannel (L3)	Routing Protocols (L3)[6]	NetFlow[7]	Trace Route
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
6880-X	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
WLC 5500	N/A	N/A	N/A	N/A	N/A	Yes	N/A	N/A	N/A	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

1. Virtual Routing and Forwarding (VRF) is not supported for the wired platforms and is not applicable for the wireless platforms.
2. Hot Standby Router Protocol (HSRP).
3. Switch Virtual Interface (SVI)
4. Per VLAN Spanning Tree Protocol (PVST)
5. Equal Cost Multipath (ECMP)
6. Supported Layer 3 routing protocols include: static, OSPF, EIGRP, IS-IS, and BGP. The following Layer 3 protocol is not supported: PBR.
7. 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.

Table 8 Wireless AP Support by Platform

Platform	AP Manager	
	LAG[1]	Physical
WLC 2504	Yes	Yes
WLC 5500	Yes	Yes
WLC 5760	Yes	Yes
WLC 8500	Yes	Yes

1. 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.

Table 9 Wireless Mode Support

Platform[1]	Wireless Deployment Mode			Wireless Mobility Mode		
	Centralized	Flex	Converged[2]	Centralized	Converged	Hybrid[3]
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

1. WLC redundancy and high availability is not supported.
2. Catalyst 3850 switch and stack do not support converged wireless deployment mode for a path trace.
3. 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.

Table 10 Path Trace Supported Scenarios

Scenario	Protocol	Feature List	Configuration	Supported
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

Table 10 Path Trace Supported Scenarios (continued)

Scenario	Protocol	Feature List	Configuration	Supported
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
			AP load balance across multiple port channels	No
			Single AP Manager Interface Configuration	Yes
			Multiple AP Manager Interface Configuration and load balance it on different physical interface	Yes
			Interface Group	No
		WLAN	Dynamic Interfaces per WLAN mapped to physical interface	No
			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	Roaming across L2 and L3 networks	Yes
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
Path Trace	ECMP	Only Layer 3 data forwarding interfaces.		
		No management interfaces		

Table 10 Path Trace Supported Scenarios (continued)

Scenario	Protocol	Feature List	Configuration	Supported
Layer 3 Load Balancing	ECMP	Routing Recursive Lookup Levels	Three 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

Refer to the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, for the troubleshooting procedures.

Related Documentation

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

- Cisco APIC-EM Documentation:
  - *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Open Source Used In Cisco APIC-EM*
- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network (Cisco IWAN)*

  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*
- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*
  - *Solution Guide for 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*
  - *Mobile Application User Guide for Cisco Network Plug and Play*

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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.