Cisco Network Visibility Application for APIC-EM Release Notes, Release 1.4.0.x

First Published: 2017-02-21

Cisco Network Visibility Application for APIC-EM Release Notes, Release 1.4.0.x

This document describes the features, limitations, and bugs in Cisco Network Visibility applications (Discovery, Inventory, and Host), Release 1.4.0.x.

Along with Cisco Network Visibility, Cisco APIC-EM supports the following additional applications:

- Cisco EasyQoS
- Cisco Path Trace
- Cisco IWAN
- Cisco Network PnP

For information about the Cisco APIC-EM controller infrastructure (system requirements, security, licensing, supported multi-host configurations, and so on) and the other Cisco APIC-EM applications, see their corresponding release notes at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-release-notes-list.html

What's New in Network Visibility

The Cisco APIC-EM software release provides the following new network visibility apps (Discovery, Inventory, Host) features and functions:

- **Command Runner—**Allows you to send CLI commands to selected devices. Currently, **show** and other read-only commands are permitted.
- **Update Polling Interval—**Allows you to update the polling interval at the global level for all devices on the **Settings > Polling Interval** page or at the device level for a specific device in the **Device Inventory** window. When you set the polling interval at the device level, that value takes precedence over the global polling interval value.
- **Resync (Resynchronize Devices)—**Allows you to immediately poll the selected device for updated information and status. The device information and status are updated in the inventory.
- **Update Credentials—**Allows you to change the discovery credentials of selected devices.

- **IP Device Tracking (IPDT) Support—**If enabled on devices, IPDT retrieves host information during the discovery process.

Supported Platforms and Software Requirements

For information about the network devices and software versions that Network Visibility supports, see *Cisco Network Visibility Application for APIC-EM Supported Platforms*.

Installing or Upgrading Network Visibility

The Network Visibility image is built into the APIC-EM controller image. When you install or upgrade to APIC-EM 1.4.0.x, the Network Visibility Release 1.4.0.x is installed or upgraded as well.

After installing or upgrading the APIC-EM software, you can begin to use Network Visibility immediately. For any of the following information, see these sources:

Table 1: Information Sources for Installing or Upgrading Network Visibility

Information	Source
Installing APIC-EM or Network Visibility	*Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
Upgrading APIC-EM or Network Visibility	*Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
Obtaining bug information about APIC-EM	*Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*

Caveats

Open Caveats

The following table lists the open caveats for this release.

Caveat ID Number	Headline
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
CSCvc93928	The Command Runner application may not be able to retrieve the command output file if the it is too large as a result of having too much command output data. Commands with large amounts of data: • **show tech-support** • **show subsys** • **show logging** • **show spanning-tree** • **show processes** • **show memory** • **show msglog** • **show memory history** • **show traplog** • **show queueinfo** **Workaround**: For each request, run only one of these commands on one device at a time.
CSCvd09216	IPDT fails if IPDT is performed during discovery when a device is in a Managed state but the device role has not yet been determined (device in Unknown state). **Workaround**: Start a new discovery only when devices of all previously started discoveries are in a Managed state.
CSCvd12902	Inventory should not add an IP address learned using IP Device Tracking (IPDT) to the host inventory if it is also the IP address of a discovered device's interface. **Workaround**: There is no workaround at this time.

Caveat ID Number	Headline
CSCvd13162	The Command Runner application is installed. However, when you enable the application in the **Admin > App Management** window and navigate away from the window before the enable operation is completed, the **Command Runner** button does not display on the **Device Inventory** window. The opposite scenario may also occur. You disable the application, and navigate away from the **App Management** window, and the **Command Runner** button does not disappear from the **Device Inventory** window. **Workaround**: Navigate to the **Admin > App Management** window and toggle the **Enabled/Disabled** button. If the current state is enabled, disable the application. If the current state is disabled, enable the application. Then enable or disable the application again (to achieve your original intent). Do not navigate away from the window until the operation is completed and the success banner displays.
CSCvd21386	If you shutdown port channels or member interfaces and rediscover a device with IPDT turned on, APIC configures IPDT on them. Then, if you bring the port channels or interfaces up (**no shutdown**), the device learns the IP addresses of its neighbor interfaces. **Workaround**: Do not configure IPDT on port channels or member interfaces when they are functionally down (**shutdown**).
CSCvd21449	Cisco APIC-EM does not apply IPDT configurations to devices running Cisco IOS XE 16.x without the SISF-Based Device-Tracking CLI. **Workaround**: On devices running Cisco IOS XE 16.x, migrate to SISF-Based Device-Tracking CLI. Then on Cisco APIC-EM, enable IPDT Autoconfig in **admin > Settings > Device Controllability**, delete the devices from inventory, and rediscover them.

Resolved Caveats

The following table lists the resolved caveats for this release.

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

Caveat ID Number	Headline
CSCvb70665	The Cisco Catalyst 4000 with Cisco IOS image version 3.8.x/3.9.x fails to go into a managed state (inventory collection). This occurs when the Cisco IOS image version is greater than or equal to 3.8.x. **Workaround**: Use a Cisco IOS-XE image version less than or equal to 3.7.x.
CSCvb50882	After upgrading to Cisco APIC-EM version 1.3.x, you will still have your discovery credentials available from your previous installation. If you run a legacy job specific discovery, then you may receive an error message. **Workaround**: Perform one of the following: • Select and only run a global discovery. • Select and run a global discovery with the job specific discovery. • Create a completely new job discovery and run it.
CSCvb86166	Running a cloned discovery job after disabling the job specific CLI credentials causes an error message. **Workaround**: Create a new discovery job or add new job specific CLI credentials to the discovery.

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

The Network Visibility application has the following limitations and restrictions.

Note Refer to the other Cisco APIC-EM app release notes or Cisco APIC-EM controller release notes for information about any other app or infrastructure-specific issues.

- HTTP and HTTPS are not supported for device discovery for this release.
- There is a 255 character limit when entering a multi-range IP address for a Discovery job. The Discovery job will fail if you enter more than 255 characters for a multi-range IP address.
- The IP Device Tracking (IPDT) controllability feature is provided as a static configuration that is pushed to devices within your network during a discovery. The IPDT controllability feature overwrites the current state of IPDT configurations on the devices. If you do not want the existing IPDT configurations on the devices to be disturbed, you need to disable the IPDT controllability feature in the APIC-EM Settings. To do this, from the Global toolbar, click **admin** (shown as **admin** with the gear icon) **> Settings > Device Controllability**. In the **Device Controllability** window, turn off IPDT autoconfiguration by selecting **No** for **IPDT Autoconfig**.

Service and Support

Troubleshooting

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

Related Documentation

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

Cisco APIC-EM Controller Documentation

For this type of information...	See this document...
Release information, including new features, system requirements, and open and resolved caveats.	*Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
Installation and configuration of the controller, including post-installation tasks.	*Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
Introduction to the Cisco APIC-EM GUI and its applications.	*Cisco Application Policy Infrastructure Controller Enterprise Module Quick Start Guide* [1]
Configuration of user accounts, RBAC scope, security certificates, authentication and password policies, and global discovery settings. Monitoring and managing Cisco APIC-EM services. Backup and restore. Cisco APIC-EM APIs.	*Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
Troubleshooting the controller, including the installation, services, and passwords. Developer console. How to contact the Cisco Technical Assistance Center (TAC).	*Cisco Application Infrastructure Controller Enterprise Module Troubleshooting Guide*
Tasks to perform before updating the controller to the latest version. Software update instructions. Tasks to perform after an update.	*Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*

1 Available from the APIC-EM controller **System Info** window.

Cisco IWAN Application Documentation

For this type of information...	See this document...
Release information, including open and resolved caveats for the Cisco IWAN application.	*Cisco IWAN Application on APIC-EM Release Notes*
Using the Cisco IWAN application.	*Cisco IWAN Application on APIC-EM User Guide*

Cisco Network Plug and Play Application Documentation

For this type of information...	See this document...
Release information, including open and resolved caveats for the Cisco Plug and Play application. Supported Cisco devices for Cisco Network Plug and Play.	*Release Notes for Cisco Network Plug and Play*
Configuration of devices using 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*
Cisco Network Plug and Play solution overview. Main workflows used with the Cisco Network Plug and Play solution. Deployment of the Cisco Network Plug and Play solution. Tasks for using proxies with the Cisco Network Plug and Play solution. Configuration of a DHCP server for APIC-EM controller auto-discovery. Troubleshooting procedures for the Cisco Network Plug and Play solution.	*Solution Guide for Cisco Network Plug and Play*
Information about 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)

Cisco APIC-EM Developer Documentation

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

Notices

Trademarks