Cisco Evolved Programmable Network Manager 6.1.2 Release Notes

First Published: 2023-09-25

Introduction

This document contains the following information about Cisco Evolved Programmable Network Manager 6.1.2:

What's New

The Cisco EPN Manager 6.1.2 release introduces fixes for the following bugs:

- CSCwe23573: Memory leak in the HM Main–CARS JNI call
- CSCwe29295: DB connection leak from the NBI-restconf
- CSCwe29279: DB connection leak in the inventory module
- CSCwd75444: Switch inventory job failure with the inventory process failure message
- CSCwc67062: Credential profile does not show up SSH details
- CSCwd44814: Assurance logs take up a lot of disk space and no roll over
- CSCwd58228: Radius Integrated User with "Super Users" role cannot see the jobs
- CSCwd56919: UDF is being appended to each hardware alarm multiple times
- CSCwd54345: Get UDF API is taking approximately 1.3 mins to respond, thereby creating a lag in the Network devices UI
- CSCwd71353: Show All on job details page is not working
- CSCvk01767: Administration/system settings - Network and Devices/SNMP backhoff algorithm are not saved after restart

- CSCwf09277: Device Configuration Archive JOB start time is getting delayed
- CSCwe07091: EPNM Command Injection Vulnerability
- CSCwf50786: Chrome v114 update - UI regressions because of 'popover' attribute usage
- CSCwh07824: Collection failure after inserting a new line card
- CSCwb03347: Disable the SL deregister in case of NotifyAuthRenewFailure
- CSCwh06323: Alarm forwarding stopped for connection-less subscription
- CSCwh17009: Abnormal Utilization of >100% reported for few interfaces from Interface Health policy
- CSCwc96793: Radius Integrated Admin User cannot see the jobs - BE Changes
- CSCwd45038: Top Interface Utilization Tx/Rx Performance graphs throw error
- CSCwc86777: Smart license is deregistering shortly after registering with no reason, causing functionality loss

Check the Cisco EPN Manager Bugs, on page 2 section for more information.

Supported Installation/Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 6.1.2 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 6.1.2
Cisco EPN Manager 6.1.1.1	**Cisco EPN Manager 6.1.1.1 > 6.1.2**
Cisco EPN Manager 6.1.1	**Cisco EPN Manager 6.1.1 > 6.1.2**
Cisco EPN Manager 6.1	**Cisco EPN Manager 6.1 > 6.1.2**

See the relevant installation guide for installation prerequisites and procedures for Cisco EPN Manager versions.

For point patch installation instructions, see the readme file supplied with the patch file on the on the Software Download site on Cisco.com.

Cisco EPN Manager Bugs

Resolved Bugs

The table below lists all the bugs that were resolved in the Cisco EPN Manager 6.1.2 release.

For more information about the resolved bugs, go to the Bug Search Tool.

Bugs	Description
CSCwe23573	Memory leak in HM Main–CARS JNI call
CSCwe29295	DB Connection leak from NBI-restconf
CSCwe29279	DB connection leak in inventory module
CSCwd75444	Switch inventory job stopped with inventory process failure message
CSCwc67062	Credential profile does not show up SSH details
CSCwd44814	Assurance logs takes up lot of disk space and also no roll over
CSCwd58228	Radius Integrated User with "Super Users" role cannot see jobs
CSCwd56919	UDF is being appended to each hardware alarm multiple times
CSCwd54345	Get UDF API is taking apprx 1.3 min to respond causing slowness in Network devices UI
CSCwd71353	Show all on job details page not working
CSCvk01767	Administration/system settings - Network and Devices/SNMP backhoff algorithm not saved after restart
CSCwf09277	Device Configuration Archive JOB start time is getting delayed **Note** To resolve the problem in an upgrade scenario, the user must manually delete the job and create a new job; only then the fix will be applied.
CSCwe07091	Cisco Evolved Programmable Network Manager Command Injection Vulnerability
CSCwf50786	Chrome v114 update - UI regressions because of 'popover' attribute usage
CSCwh07824	Collection failure after inserting new line card
CSCwb03347	Disable the SL deregister in case of NotifyAuthRenewFailure
CSCwh06323	Alarm forwarding stopped for connection-less subscription
CSCwh17009	Abnormal Utilization of >100% reported for few interfaces from Interface Health policy
CSCwc96793	Radius Integrated Admin User cannot see jobs - BE Changes
CSCwd45038	Top Interface Utilization Tx/Rx Performance graphs throw error
CSCwc86777	Smart license is deregistering shortly after registering with no reason, causing functionality loss

Get Information about Cisco EPN Manager Bugs

Use the Bug Search tool (BST) to get the latest information about Cisco EPN Manager bugs. BST allows partners and customers to search for software bugs based on product, release, and keyword, and it aggregates key data such as bug details, product, and version.

Cisco EPN Manager bugs may be caused by defects in a device's platform or operating system. In such cases, the Cisco EPN Manager bug will be resolved when the hardware/operating system bug is resolved.

Procedure

Step 1 Log into the Bug Search Tool.

a) Go to https://tools.cisco.com/bugsearch/.

b) At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**.

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 2 To list all bugs for this version, click the **Select from list** hyperlink that is next to the **Product** field and select the product.

a) Choose **Cloud and Systems Management** > **Routing and Switching Management** > **Cisco Evolved Programmable Network (EPN) Manager** and then select the required product version.

b) When the results are displayed, use the **filter and sort** tools to find bugs according to their status, severity, how recently they were modified, if any support cases are associated with them, and so forth.

You can also search using bug IDs or keywords. For more information, click **Help** at the top right of the **Bug Search** page.

Important Notes

Cisco EPN Manager software is distributed with all the components necessary for its optimized and secure operation, including the Red Hat Linux operating system and the Oracle database. All security-related configurations, regression testing, performance, and scalability metrics are based on the set of components and configurations included in the original Cisco EPN Manager software distribution. Cisco provides periodic EPN Manager software updates that can also contain necessary updates to the packages installed on the operating system or to the database.

Note that if any of the following changes are made to the original distributed Cisco EPN Manager software, Cisco will no longer support the operating environment:

- Configuration changes to the software or operating system, or installation of other components that are not part of the original distribution.
- Direct installation and application of third-party software on the Red Hat Linux operating system embedded within Cisco EPN Manager.
- Application of updates or patches that are **not** provided by Cisco to individual Cisco EPN Manager components.

- Changes to the internal Cisco EPN Manager settings that are not documented as modifiable in the Cisco EPN Manager User and Administrator Guide on Cisco.com, as these changes may weaken security, disable functionality, or degrade scalability and performance.

Upgrade Issues

- FTP and TFTP are disabled by default.
- Active Threshold Crossing Alarms (TCA) for temperature remain active and are not cleared automatically. Clear these alarms manually.
- You must resync your devices to view ISIS links.
- You must resync LDP-enabled devices to view LDP feature-related information.
- You must recreate the TCAs for inbound/outbound errors and inbound/outbound discards in the Interface Health monitoring policy.

Limitations on Carrier Ethernet Circuit Provisioning

- Promotion of service using old probe name format is now supported. These probes are listed in the user interface with the appropriate standard OAM Profile name after promotion.
- Sample profile: profile PM2_3_8_CoS5_DM type cfm-delay-measurement.
- While custom profile names are supported in EPN Manager, modifying brownfield services with a different naming format deletes the existing custom profile and adds a new profile with a supported naming format.
- Inventory models do not correctly display the profiles that are not associated to a service.
- Validation limit for number of profiles is 100. If you create a new SLA operation profile after 100 existing profiles, the device generates an error and deployment fails.

TLS 1.2 Required for Secured Channel Communication for HTTPS and TLS

Only Transport Layer Security (TLS) 1.2 is supported for HTTPS and TLS related secured communication, for example, RADIUS EAP-TLS.

Support for TLS 1.0, TLS 1.1, and all versions of SSL has been disabled due to security vulnerabilities.

This means that all peer systems and clients that transact with Cisco EPN Manager using HTTPS/TLS must support TLS 1.2. If they do not support TLS 1.2, you must upgrade these systems. Wherever possible, the Cisco EPN Manager documentation highlights the potentially affected systems. Contact your Cisco representative for support in this regard, if necessary.

Reconciliation Report Limitations

If you have not provided a value for an attribute while provisioning a service, the provisioned value for that attribute is displayed as “Missing” in the reconciliation report. The device may have a default value for this attribute, but Cisco EPN Manager does configure this value.

Limitations on Cisco ME 1200 Devices

The Y.1564 performance test does not work if the source/destination is a Cisco ME 1200 device.

Limitations on Cisco NCS 4200 Devices Running IOS-XE 16.8.1

The following functionalities do not work on Cisco NCS 4200 devices running IOS-XE 16.8.1:

- Alarm profile
- Configuration of SONET LOP and CT3 LOP from the GUI
- Admin shut/no shut functionality on SONET/T1/T3 HOP/LOP

Limitations on Cisco NCS 540 and Cisco NCS 5500 devices

Cisco NCS 540 and Cisco NCS 5500 device series do not support Fault-OAM, Wrap-Protection, and BFD.

Use CLI Templates for Configuring PTP Commands

On ASR920 devices with software version 16.9.1, IEEE 1588-2008 BC/MC license is required to execute the 1588 PTP commands.

Configuration and Inventory Not Supported for PTP Templates

The behavior of modeling the configurations pushed through PTP templates may not work as expected because the model may not be in place for all the configurations pushed through PTP templates. Configuration/Inventory is not supported for these configurations.

Deprecation of Support for ONS 10.00.10, 10.01.00, 10.03.00

ONS 10.00.10, 10.01.00, 10.03.00 ONS 10.00.10, 10.01.00, and 10.03.00 are no longer supported on Cisco NCS 2002, Cisco NCS 2006, and Cisco NCS 2015 devices.

Data Center Device Lifecycle Support Only

Cisco EPN Manager provides sssential support for a few selected UCS compute systems, Nexus series devices, and the CSR 1000v devices.

LINK_DOWN alarm on sub interfaces in Gig Port

LINK_DOWN alarms will not be generated when link is down on sub interfaces in a Gig Port.

Related Documentation

For a list of all documentation available for Cisco EPN Manager 6.1.2, see Cisco Evolved Programmable Network Manager 6.1 Documentation.

Accessibility Features

For a list of accessibility features in Cisco EPN Manager 6.1.2, contact accessibility@cisco.com.

All product documents are accessible. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com

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.

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