Cisco Evolved Programmable Network Manager 7.1 Release Notes

First Published: 2023-08-31

Introduction

This document contains the following information about Cisco Evolved Programmable Network Manager 7.1:

New Functionality Added

This section lists the new features/functionalities delivered in Cisco EPN Manager 7.1.

Device Support

- Support for IOS-XR 7.9.2 release on Cisco NCS 540 devices
- Support for IOS-XR 7.9.2 release on Cisco ASR 9000 64 Bit routers
- Support for IOS-XR 7.9.2 release on Cisco NCS 560 devices
- Support for IOS-XR 7.9.2 release on Cisco NCS 8000 series devices
- Support for IOS-XR 7.9.2 release on Cisco NCS 5500 devices
- Support for IOS-XR 7.9.2 release on Cisco NCS 5700 devices
- Support for Cisco NCS 2000 devices release 11.1.3
- Support for IOS-XE 17.10.1 release on Cisco ASR 900 devices and Cisco ASR 920 devices
- Support for IOS-XE 17.10.1 release on Cisco NCS 4200 series devices

- Support for IOS-XR 7.9.1 release on Cisco NCS 1004 devices
- Support for Cisco N540-FH-AGG-SYS (5G access) aggregation router with IOS-XR 7.8.1
- Support for Cisco NCS2002-DC2 device (release 11.1.3)
- Support for IOS-XR 7.8.1 release on Cisco NCS-57D2-18DD-SYS fixed chassis
- IPv6 support for Cisco NCS 1010 devices
- Chassis view support for Cisco N540-FH-AGG-SYS (5G access) aggregation router with IOS-XR 7.8.1
- Support for the Cisco NCS 1004 device 7.3.1 release features
- Support for the Cisco NCS 1004 device 7.3.2 release features
- Support for the Cisco NCS 1004 device 7.5.1 release features
- Support for the Cisco NCS 1004 device 7.5.2 release features
- Support for the Cisco NCS 1004 device 7.7.1 release features
- Support for the Cisco NCS 1004 device 7.8.1 release features
- Support for Smart SFP on IOS-XR 7.8.1 release (Cisco ASR 9000 routers, Cisco NCS 5500 devices, Cisco NCS 540 devices) - Service Discovery Validation
- Support for Cisco NCS1K4-QXP-K9 line card on Cisco NCS 1004 devices
- Support for enhanced scale validation

GUI - General

- Smart License Dashboard Page cleanup
- Support for SONET-4-APSMM syslog and Reactive Inventory (MR-92)
- Integration of Cisco WAN Automation Engine and Cisco EPN Manager based on HTTPs
- Debuggability: Request to add an option to generate a support package bundle
- Enhanced status display for PW and EVPN links

Software Support

- Support for ESXi 7.0 Update 3g release
- Upgrade to Red Hat Enterprise Linux 8 (RHEL 8)
- Support for ESXi 8 release

Optical

- Link protection (1+1 Trunk protection) for Cisco NCS1K4-QXP-K9 line cards on Cisco NCS 1004 devices

Inventory

- Support Optical SFP PM reports for Cisco 8201 routers, Cisco NCS-57B1-5DSE-SYS router, Cisco NCS-57B1-6D24-SYS routers, and Cisco ASR 9903 routers to generate PM Data

Licensing

- Achieve consistent Smart Licensing behavior across Cluster and Non-Cluster versions of Cisco EPN Manager

Functionality Changes Including Removed/Disabled Features

Following features/functionalities/Menus were deprecated in Cisco EPN Manager 7.1.

- **General Features:**
  1. Syslog Settings:
     - Administration > Settings > Logging - Syslog

New Operating System Support

This section lists the new OS support provided in Cisco EPN Manager 7.1. For a list of all support information, click the gear icon at the top-right of the web GUI and choose **Help > Supported Devices**.

Cisco Network Convergence System 1004 —New Operating System Support

Device Model	Device OS
Cisco NCS 1004 Router	IOS-XR 7.9.1

Cisco Network Convergence System 540 Series Routers—New Operating System Support

Device Model	Device OS
Cisco NCS 540 Router	IOS-XR 7.9.2

Cisco ASR 9000 Series Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 9000 64-Bit Router	IOS-XR 7.9.2

Cisco Network Convergence System 560 Series Routers—New Operating System Support

Device Model	Device OS
Cisco NCS 560 Router	IOS-XR 7.9.2

Cisco 8000 Series Routers—New Operating System Support

Device Model	Device OS
Cisco 8000 Router	IOS-XR 7.9.2

Cisco Network Convergence System 5500 Series—New Operating System Support

Device Model	Device OS
Cisco NCS 5500 Series	IOS-XR 7.9.2

Cisco Network Convergence System 5700 Series Routers—New Operating System Support

Device Model	Device OS
Cisco NCS 5700 Router	IOS-XR 7.9.2

Cisco ASR 900 Series Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 900 Router	IOS-XE 17.10.1
Cisco ASR 902 Router	IOS-XE 17.10.1

Cisco Network Convergence System 4200 Series—New Operating System Support

Device Model	Device OS
Cisco NCS 4200 Series	IOS-XE 17.10.1

Supported Installation/Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 7.1 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 7.1
Cisco EPN Manager 6.0.1.1	**Cisco EPN Manager 6.0.1.1 > 7.1**
Cisco EPN Manager 6.1.1	**Cisco EPN Manager 6.1.1 > 7.1**
Cisco EPN Manager 7.0.1	**Cisco EPN Manager 7.0.1 > 7.1**

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.

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.

Cisco EPN Manager Bugs

Open Bugs

The following criteria are used to create the list in the table below, which includes all the open bugs in Cisco EPN Manager 7.1 release:

- Severity 1, 2, and high priority severity 3 open bugs
- All open customer-found bugs
- High-impact bugs that are likely to affect Cisco EPN Manager workflows.

Click the identifier link to view the impact and workaround for the bug in the Bug Search Tool. Use this tool to track the status of the open bugs.

Bugs	Description
CSCwf76966	I159 B: MLT view doesn't display the 2K ports information in the OCH layer
CSCwh00835	BITS Interface disappearing upon device full sync
CSCwh22670	161 A: Overlay and MLT are not working for SR policies and overlayed L2VPN

Resolved Bugs

The table below lists all the bugs that were resolved in Cisco EPN Manager 7.1 release.

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

Bugs	Description
CSCwc78979	CoherentDSP is giving error in response to post modify operation
CSCwd12284	UI partially or completely not displaying Coherent port if device admin status is changed
CSCwe04031	Time axis is abnormally shifted in the CPU utilization graph on the Dashboard/Device Trends GUI

Bugs	Description
CSCwe10728	Resource Pool collection error caused by Main Interface value populated in EthernetSubInterface
CSCwe73405	Vulnerabilities in code mirror 3.19.0 CVE-2020-7760

Closed Bugs

The table below lists all the bugs that were closed in Cisco EPN Manager 7.1 release.

Click the identifier link to view the impact and workaround for the bug in the Bug Search Tool. Use this tool to track the status of the bugs.

Bugs	Description
CSCwf27415	Getting failure message: Failure to establish a HTTPS Session" in change audit logs
CSCwf04753	In notification with respect to ODU Group protection admin/oper state are unknown, retrieved correctly on getTP
CSCwd64579	EPNM 7.0 LA/GA: Application Search is not working in Cisco EPN Manager main page
CSCwf50906	EPNM does not allow you to unset or remove the BPS value, but the device does
CSCwf84323	In Optics Port, RX/TX high threshold indicating an error
CSCwd09949	EPNM - model and report - transceivers not found or inaccurate in SFP report and NetworkInventory UI
CSCwf25966	Inverted commas are being added to Cisco NCS 2000 devices port description
CSCwe94660	Empty Client (Pluggable Port) message to be made more user-friendly
CSCwf10768	Only one Hundred GigE Ctrlr0/0/0/0 port has been updated in EPNM through GI/RI, rest all not updated
CSCwf25846	F128019: Cardmode set on Skinny BO, client & trunk bit rate incorrect error message wrt validation
CSCwf72324	A card operating mode was deleted by EPNM using the incorrect command
CSCwf76971	Odu-grup-mp is wrongly configured directly from the device, the device goes to CWW

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.

Related Documentation

For a list of all documentation available for Cisco EPN Manager 7.1, see the Cisco Evolved Programmable Network Manager 7.1 Documentation.

Accessibility Features

For a list of accessibility features in Cisco EPN Manager 7.1, 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.