



Cisco Evolved Programmable Network Manager 2.1.3 Release Notes

First Published: November, 2017

Contents

This document contains the following information about Cisco Evolved Programmable Network Manager 2.1.3:

- [Functionality Added in Cisco EPN Manager 2.1.3](#)
- [Device/OS Support Added in Cisco EPN Manager 2.1.3](#)
- [Installation/Upgrade Paths](#)
- [Important Notes](#)
- [User Documentation Changes](#)
- [Cisco EPN Manager Bugs](#)
- [Related Documentation](#)
- [Accessibility Features in Cisco EPN Manager 2.1.3](#)



Functionality Added in Cisco EPN Manager 2.1.3

Management of Cable Devices

- Additional dashlets are available in the cable dashboard to help visualize the network health.
- The cBR-8 chassis view has been significantly enhanced to capture DOCSIS statistics including channel utilization, modem and CPE details, voice calls, sensor and license details.
- Visualization of L2TP link health (colors) and utilization details in the topology map.
- Compatibility with Smart PHY 1.0.1 for extended functionality.
- Ability to export Cisco cBR-8 device and DOCSIS statistics information to a CSV or PDF file.
- Credentials-based access to the RPD GUI.

Circuits/VCS

- Ability to create a user-defined field and add it as a column to the circuits tables.

Device Lifecycle Management

- Chassis view support has been added for Cisco NCS 5011, 5501, 5501-SE, 5502, 5502-SE, and NCS 4000F (Fabric Switch Chassis) devices.
- Support for generic Cisco devices.
- Ability to add BDI/BVI interfaces to a port group. This can be done from the “All” page under Inventory > Group Management > Port Groups but not from the “User Defined” page.

Device Configuration

- Ability to Ability to channelize T3/E3 controllers.
- Protection group-related information is now available for Unidirectional Path Switched Ring (UPSR) interfaces.
- Ability to create and delete 1+1 card protection groups on Cisco NCS 4200 devices.
- Ability to view the status of APS protection groups and perform administrative functions like lockout, force switch and manual switch.
- Ability to configure the card type for T1/E1.
- Ability to view IS-IS neighbors and their details.
- Ability to identify the interfaces on which Sync-E clock configuration is active (Cisco IOS-XR and Cisco IOS-XE devices).

Configuration Archive

- An alarm is now generated if the backup of device configuration fails a certain number of times or if a backup is older than a certain number of days and the backup fails.
- Ability to manually delete archived device configuration files.

Image Management

- Ability to select FPD image packages as the default choice for upgrade during the image distribution and activation processes. Before performing an upgrade, you can view FPD details such as the device name, card type, hardware version, and other associated details.

Carrier Ethernet

- Ability to create a new CFM domain for E-Line EVCs.
- Support for L2 service provisioning on ASR 1000 devices.

L3VPN

- L3VPN service provisioning is supported on Cisco Catalyst 6500 and Cisco ASR 1000 devices.

MPLS TE

- Support for service templates for TE tunnels.
- Flex LSP dual plane support—ability to set Affinity per path for bidirectional tunnels.
- Support for additional auto-bandwidth parameters for unidirectional tunnels.
- Service naming enhancements for services without a user-provided name:
 - <SourceDeviceName>_<TunnelId>_<DestinationDeviceName> if source and destination devices have a common tunnel ID.
 - <SourceDeviceName>_<ATunnelId>_<ZTunnelId>_<DestinationDeviceName> if source and destination devices have unique tunnel IDs.

CEM

- Support for 1+1 electrical protection for provisioning flows, inventory and alarming on NCS 4200 devices.

Serial

- Creation and provisioning of raw socket services.

Optical

- Ability to create an ODU circuit with protection over an OTN topology with NCS 2000 and NCS2K-400G-XP linecards.
- When configuring a second OCH-CC circuit, you can now see which NCS2K-400G-XP trunk port is already assigned to a circuit.
- Discovery of LMP links between NCS 2000 and NCS 55xx devices.
- Ability to configure the UNI interfaces on NCS 2000 devices. The UNI is the service control interface between the transport network and client equipment.
- Ability to configure slices on NCS 1002 devices, setting the client rate, trunk rate, FEC and encryption for each slice.
- Support for SSON (Spectrum-Switched Optical Network)—circuit creation and discovery.

Bandwidth Utilization

- Support for visualization of bandwidth utilization for physical, LAG, cable and L2TP links.

QoS

- Color-aware traffic policing is now available using the QoS Action profile.
- Multiple DSCP actions can now be associated with a QoS classification profile.

Topology and Geo Map

- Visualization of IS-IS network in the topology map.

- Visualization of Secure Domain Routers in the topology and geo maps.
- Ability to drill down into a device group/cluster using the double-click action in the topology and geo maps.
- Propagation of LAG member critical state to the LAG link in the map.
- In the Link Details view, LAG links are shown together with the association to their children.
- Contextual information provided upon hovering over a link with the mouse.
- Ability to create a global layout for the topology map and save it as the default layout for all users. This can only be done by users with network topology Edit privileges.
- Links are persisted in the topology map even when they are down and can no longer be discovered. These links are colored gray.
- Links with critical alarms are now colored red.
- Fiber management in the geo map—ability to associate a fiber to a link via KML import and to visualize the fiber and its associated link together in the geo map.

Fault Management

- Ability to export events related to a specific alarm.

Performance

- Addition of 2 new tabs to the Performance dashboard:
 - Device Sensors tab: Provides details on the sensors that reside on a device, such as their name, the type of information they collect (such as temperature or voltage) and the corresponding unit of measure, and the value recorded during the last device poll.
 - SONET/TDM Interfaces tab: For the selected SONET or time-division multiplexing (TDM) interface, this tab provides details such as its name and configured speed, as well as dashlets that chart the interface's performance metrics.
- Enhancements to the Performance dashboard's Cable tab:
 - Remote Physical Device dashlet: Indicates the number of Remote Physical devices managed by the Cisco cBR-8 routers in your network and their current connection status.
 - Supervisor FPGA Versions dashlet: Indicates the field programmable gate arrays (FPGAs) currently in use by the Cisco cBR-8 routers in your network.
 - Additional dashlets: Power Supply Status, Fan Status, SUP Card Memory and CPU utilization, Modem History, CPE History, Voice Data, Channel Utilizations (US and DS), Line Card Utilizations (US and DS).
- The Policies pane pop-up window (Monitor > Monitoring Tools > Monitoring Policies) allows you to quickly access summary information and action links for a particular policy or policy folder.
- In dashboard dashlets that provide charts, you can now choose a chart type and specify display options.
- In the Top N Environmental Temperature dashlet (Network Summary dashboard > Network Devices tab), you can now view both the highest recorded internal and ambient temperature for a device.
- Ability to open the 360 view for a device's adjacent device or interface from the Top N Interfaces dashboard.
- Display of QoS statistics per ECE for ME1200 devices.

- For Y.1731 performance test, delay measurement is done using Delay Measurement Message (DMM) probe and loss measurement is done using Synthetic Loss Measurement Message (SLM) probe. For ASR 1000 devices, delay measurement is done using the LMM probe only.
- For BERT performance test, export of the test results to PDF format is supported.
- Introduced Color Aware mode in Y.1564 performance test.

Reports

- Two new reports are available under Performance > Environmental Temperature:
 - Detailed Environmental Temperature Report: Lists in detail the sensor details, maximum and minimum temperature of the devices along with the timestamps.
 - Summarized Environmental Temperature Report: Lists the current temperature of the device.
- New Device Availability report listing devices and their reachability status.
- Additional metrics for QoS policy graph report:
 - Bundle Capacity
 - Police % for priority queues
 - Bandwidth % for normal queues
- For QoS policy graph report, ability to generate data with drop percentage > 0 along with the timestamp at which the drops occurred.
- Added fan and power supply status to the Wired Module reports.
- Ability to export utilization information to a CSV file if utilization reaches a specified threshold.

Licensing

- The license report under Administration>Licenses and Software Updates>Licenses now includes licenses for each chassis in a multi-shelf device.

RESTCONF NBI

Support for:

- Pre-provisioning (provision, modify, delete) of equipments for NCS 2000 devices.
- Modifying card mode for NCS 2000 devices.
- Creation of managed manual links to represent optical topology links.
- "Bridge and roll" for CEM services.
- NCS 4200 (IOS XE, 16.7.1) 1+1 electrical protection validation in provisioning.
- Uni-directional tunnel auto-BW parameters provisioning.
- Uni-directional tunnel as preferred path for EPL, EVPL, and CEM service provisioning.
- Selecting dynamic or static path for ECPL service.
- Support for configuring Address Family for full mesh prefix for both IPv4 and IPv6 address family for L3 VPN provisioning.
- Setting Affinity bit/mask at working and protected path of a tunnel during provisioning.
- Setting 5G slot mode for 42xx devices.
- CEM to remote device over BGP-LU for provisioning.

Device/OS Support Added in Cisco EPN Manager 2.1.3

This section lists the new support provided in Cisco EPN Manager 2.1.3. For a list of all support information, click the gear icon at the top right of the web GUI and choose **Help > Supported Devices**.



Note

“Beta support” means that the device/operating system has not yet been released but Cisco EPN Manager has been tested on the Beta version.

Optical Networking—New Operating System Support

| Device Model | Device OS |
|-----------------|----------------------|
| Cisco ONS 15454 | ONS 10.7 ONS 10.8 |

Cisco NCS 1000 Network Convergence Systems—New Operating System Support

| Device Model | Device OS |
|----------------|---------------------------------------------|
| Cisco NCS 1001 | IOS-XR 6.3.1 IOS-XR 6.3.2 (Beta support) |
| Cisco NCS 1002 | IOS-XR 6.3.1 IOS-XR 6.3.2 (Beta support) |

Cisco NCS 2000 Network Convergence Systems—New Operating System Support

| Device Model | Device OS |
|----------------|----------------------|
| Cisco NCS 2002 | ONS 10.7 ONS 10.8 |
| Cisco NCS 2006 | ONS 10.7 ONS 10.8 |
| Cisco NCS 2015 | ONS 10.7 ONS 10.8 |

Cisco NCS 4000 Network Convergence Systems—New Operating System Support

| Device Model | Device OS |
|----------------|---------------|
| Cisco NCS 4009 | IOS-XR 6.1.36 |
| Cisco NCS 4016 | IOS-XR 6.1.36 |

Cisco NCS 4200 Network Convergence Systems—New Operating System Support

| Device Model | Device OS |
|---------------------|----------------------------------|
| Cisco NCS 4201 | IOS-XE 16.6.3vS IOS-XE 16.7.1 |
| Cisco NCS 4202 | IOS-XE 16.6.3vS IOS-XE 16.7.1 |
| Cisco NCS 4206 | IOS-XE 16.6.3vS IOS-XE 16.7.1 |
| Cisco NCS 4216 | IOS-XE 16.6.3vS IOS-XE 16.7.1 |
| Cisco NCS 4216 F2B | IOS-XE 16.6.3vS IOS-XE 16.7.1 |

Cisco NCS 5000 Network Convergence Systems—New Operating System Support

| Device Model | Device OS |
|---------------------|------------------|
| Cisco NCS 5001 | IOS-XR 6.2.1 |
| Cisco NCS 5002 | IOS-XR 6.2.1 |
| Cisco NCS 5011 | IOS-XR 6.2.1 |

Cisco NCS 6000 Network Convergence Systems—New Operating System Support

| Device Model | Device OS |
|---------------------|------------------|
| Cisco NCS 6000 | IOS-XR 6.1.3 |

Cisco ASR 900 Series Aggregation Services Routers—New Device Support

| Device Model | Device OS |
|---------------------|------------------|
| Cisco ASR 902 | IOS-XE 16.7.1 |
| Cisco ASR 903 | IOS-XE 16.7.1 |
| Cisco ASR 907 | IOS-XE 16.7.1 |

Cisco ASR 920 Series Aggregation Services Routers—New Operating System Support

| Device Model | Device OS |
|-----------------------|---------------|
| Cisco ASR 920 | IOS-XE 16.7.1 |
| Cisco ASR 920 24SZIM | |
| Cisco ASR 920 24TZM | |
| Cisco ASR 920 24SZM | |
| Cisco ASR 920-12SZ-IM | |
| Cisco ASR920 4S ZD | |
| Cisco ASR920 8S Z0A | |
| Cisco ASR920 12 CZA | |
| Cisco ASR920 12 CZ D | |
| Cisco ASR920 4S ZA | |
| Cisco ASR920 10S ZPD | |

Cisco ASR 900U and 920U Series Aggregation Services Routers—New Device and Operating System Support

| Device Model | Device OS |
|------------------------|---------------|
| Cisco ASR 902U | IOS-XE 16.7.1 |
| Cisco ASR 903U | IOS-XE 16.7.1 |
| Cisco ASR 920U-12SZ-IM | IOS-XE 16.7.1 |

Cisco ASR 9000 Aggregation Services Routers—New Operating System Support

| Device Model | Device OS |
|----------------------------|--------------|
| Cisco ASR 9010 | IOS-XR 6.2.2 |
| Cisco ASR 9904 | IOS-XR 6.2.2 |
| Cisco ASR 9006 | IOS-XR 6.2.2 |
| Cisco ASR 9001 | IOS-XR 6.2.2 |
| Cisco ASR 9910 | IOS-XR 6.2.2 |
| Cisco ASR 9912 | IOS-XR 6.2.2 |
| Cisco ASR 9922 | IOS-XR 6.2.2 |
| Cisco XRv9K (Beta Support) | IOS-XR 6.2.2 |

Cisco Cisco Catalyst 6500 Series Switches—New Device Support

| Device Model | Device OS |
|----------------------------------------------|----------------|
| Cisco Catalyst 6500 Virtual Switching System | IOS 15.1(2)SY9 |

**Note**

Event-based inventory is not supported on Cisco Catalyst 6500 VSS devices.

Cisco Datacenter Switches—New Device Support

| Device Model | Device OS |
|------------------------------|-------------------|
| Cisco Nexus 31108PC-V Switch | NX-OS 7.0(3)I5(2) |

Cable Modem Termination Systems (CMTS)—New Operating System Support

| Device Model | Device OS |
|-----------------------------------------|---------------|
| Cisco cBR-8 Converged Broadband Routers | IOS-XE 16.6.1 |

Generic Cisco Devices—New Device Support

Device lifecycle management for generic Cisco devices.

Installation/Upgrade Paths

The following table lists the installation/upgrade paths for Cisco EPN Manager 2.1.3.

Note that:

- *PP = Point Patch*
- Cisco EPN Manager 2.x.x = Cisco EPN Manager 2.x *Maintenance Pack x*. For example, Cisco EPN Manager 2.1.2 = Cisco EPN Manager 2.1 *Maintenance Pack 2*
- Cisco EPN Manager 2.1.0.x = Cisco EPN Manager 2.1 installed with *point patch x*. For example, Cisco EPN Manager 2.1.0.1 = Cisco EPN Manager 2.1 with PP1.

| If you have this deployment: | Perform these steps to install Cisco EPN Manager 2.1.3 |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco EPN Manager is not installed (fresh installation) | <ol style="list-style-type: none"> 1. Install Cisco EPN Manager 2.1. 2. Install Cisco EPN Manager 2.1.3. |
| Cisco EPN Manager 1.2.x or 2.0.x | <ol style="list-style-type: none"> 1. Upgrade to Cisco EPN Manager 2.1 2. Install Cisco EPN Manager 2.1.3 |
| Cisco EPN Manager 2.1 | Install Cisco EPN Manager 2.1.3 |
| Cisco EPN Manager 2.1.0.x | <ol style="list-style-type: none"> 1. Go to the Software Download site on Cisco.com and check that you have the latest point patch for Cisco EPN Manager 2.1 installed. 2. If you do not have the latest point patch installed, install it before installing Cisco EPN Manager 2.1.3. Installation instructions can be found in the readme file supplied with the patch file. 3. Install Cisco EPN Manager 2.1.3. |
| Cisco EPN Manager 2.1.1 | Install Cisco EPN Manager 2.1.3 |
| Cisco EPN Manager 2.1.1.x | <ol style="list-style-type: none"> 1. Go to the Software Download site on Cisco.com and check that you have the latest point patch for Cisco EPN Manager 2.1.1 installed. 2. If you do not have the latest point patch installed, install it before installing Cisco EPN Manager 2.1.3. Installation instructions can be found in the readme file supplied with the patch file. 3. Install Cisco EPN Manager 2.1.3. |
| Cisco EPN Manager 2.1.2 | Install Cisco EPN Manager 2.1.3 |
| Cisco EPN Manager 2.1.2.x | <ol style="list-style-type: none"> 1. Go to the Software Download site on Cisco.com and check that you have the latest point patch for Cisco EPN Manager 2.1.2 installed. 2. If you do not have the latest point patch installed, install it before installing Cisco EPN Manager 2.1.3. Installation instructions can be found in the readme file supplied with the patch file. 3. Install Cisco EPN Manager 2.1.3. |

Important Notes

- [TLS 1.2 Required for Secured Channel Communication for HTTPS and TLS](#)
- [Reconciliation Report Limitations](#)
- [Limitations on ME 1200 Devices](#)
- [Data Center Device Lifecycle Support Only](#)
- [Data Migration Issues](#)

TLS 1.2 Required for Secured Channel Communication for HTTPS and TLS

As of Cisco EPN Manager 2.1, 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, they must be upgraded. Where possible, the Cisco EPN Manager documentation highlights the potentially affected systems. Please contact your Cisco representative for support in this regard, if necessary.

Reconciliation Report Limitations

When provisioning a service, if you have not provided a value for any of the attributes, the provisioned value for those attributes will be displayed as “Missing” in the reconciliation report. The device may have default values for these attributes but Cisco EPN Manager does not have any values configured.

Limitations on ME 1200 Devices

- **Manual sync required**—Configuration changes to ME 1200 devices are not automatically discovered by Cisco EPN Manager. After making a change, you must manually sync the device. To do this, select the required device(s) in the Network Devices table and click **Sync**.
- QoS profiles are not supported for service provisioning on ME1200 devices.
- The Y.1564 performance test does not work if the source/destination is a ME 1200 device.

Data Center Device Lifecycle Support Only

Cisco EPN Manager 2.1.3 provides foundation lifecycle support for UCS compute systems, CSR 1000v, and Nexus series devices but does not provide data center topology.

Data Migration Issues

After upgrading to Cisco EPN Manager 2.1.3:

- User-defined QoS profiles for CE services created in Cisco EPN Manager 2.1 cannot be used.
- Active threshold crossing alarms (TCA) for temperature will remain active and will not be cleared. Please clear these alarms manually.
- After installing Cisco EPN Manager 2.1.3 on top of Cisco EPN Manager 2.1.1, the following device configuration menu options can be found under the Circuit Emulation menu instead of the Physical menu in the Logical View:
 - Automatic In-Service (AINS)
 - Card Mode
 - Pluggable Type

User Documentation Changes

Installation Guide

From Cisco EPN Manager 2.1.2 onwards we have one combined installation guide for the main release and all of its maintenance packs. See [Installation Guide for Cisco Evolved Programmable Network Manager 2.1 and Maintenance Packs \(2.1.x\)](#).

Note that the Cisco Evolved Programmable Network Manager 2.1 Installation Guide and the Cisco Evolved Programmable Network Manager 2.1.1 Installation Guide are no longer available as individual guides on Cisco.com.

Cisco EPN Manager Bugs

- [Open Bugs](#)
- [Resolved Bugs](#)

Open Bugs

[Table 1](#) lists the open bugs in Cisco EPN Manager Release 2.1.3 according to the following criteria:

- 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 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.

Table 1 **Open Bugs**

| Identifier | Description |
|----------------------------|------------------------------------------------------------------------------------------------------|
| CSCvg19102 | MplsLspAttribute Info is deleted from EPNM for XE devices post inventory sync |
| CSCvg76238 | Nodes with OCHNC circuits get into Partial Collection Failure in EPNM (SW Version 10.70) |
| CSCvg79155 | ME1200: Consolidated API - Issue reusing unidirectional tunnel |
| CSCvg81030 | TE-tunnel modification for any attribute removes auto-bandwidth and few other attributes |
| CSCvc90695 | Auto-Bandwidth values are modeled incorrectly for Unidirectional Tunnel |
| CSCvd24231 | Not all \"ethernet cfm/evc\" commands are removed from RO devices |
| CSCvd85066 | Create of Ethernet SubInterface is not populating data for all the columns in protocolendpoint table |
| CSCvf03142 | Same name in xconn/bridge domain for different type of circuit leads to ConstraintViolationException |
| CSCvf16436 | EPN - reports - last boot time is not accurate |
| CSCvf17264 | Get Partial Collection Failure error when modeling ASR907/903 with DWDM card |
| CSCvf17655 | ME1200 link down correlation not working |
| CSCvf21559 | OCH-Trail serviceability remains DOWN after OCHCC creation |
| CSCvf23074 | Lower-order Path inventory details missing which caused alarms location data failure |
| CSCvf49645 | Modify vrf ipsla failed while changing the attributes in IPSLA page in L3VPN |
| CSCvf85554 | Tunnel details page shows FRR and related parameters as disabled though they're enabled |
| CSCvg15423 | Ethernet Sub-Interface(ALL Interface) status is not updated in EPNM UI for C6500 |
| CSCvg27486 | Port summary mismatch - Up and Down port count is more when compared to Device and Mib response |
| CSCvg32453 | STP associated interface is not listed on STP Instance ID |
| CSCvg34057 | CSRI: EntThresholdNotification alarm does not reflect the correct unit |
| CSCvg41045 | OAM issue: Need to configure probe in receiver mode on remote side (Z side) for one way delay |
| CSCvg49899 | Backup hub provision exception in IOS XE device |
| CSCvg54865 | Interface MTU change directly on device does not auto synch in EPNM |
| CSCvg56374 | Cable policies do not get activated properly |
| CSCvg56431 | L3VPN - trying to provision L3VPN in some cases gives NOT Started with no explanation |
| CSCvg62076 | EPNM-BNG Statistics-Special Character in the Command output |

Table 1 **Open Bugs**

| Identifier | Description |
|----------------------------|--------------------------------------------------------------------------------------------------------|
| CSCvg70289 | Upgrade setup with path Derecho - >MP1- >Derecho-MP3 , menu has shuffle incorrectly for CEM & Physical |
| CSCvg70713 | Adding a new endpoint to a L3VPN - the new defined sub interface is set to shutdown |
| CSCvg70750 | UCS_POWER_SUPPLY_FAILURE and FAN Failure should cause expedite |
| CSCvg72220 | Module list in device 360 is missing some modules |
| CSCvg72599 | Modifying [saved] brownfield L3VPN then all endpoint are moved to shutdown |
| CSCvg72604 | Modifying [saved] brownfield L3VPN then BDI interface is removed and new BDI is configured |
| CSCvg75512 | Alarms/Events export from EPNM(2.1.2.2) failing for Japanese and Korean language |
| CSCvg76433 | ASR903 NE sync failure on EPNM if ptp boundary clock configured |
| CSCvg79396 | Labeling convention of full mesh and address family all section should be based on address family |
| CSCvg79878 | Delete device removes relevant UNI from list, but UNI with same name cannot be created |
| CSCvg81203 | Actions in interface 360 - shutdown of sub-interface in XR device does not work |
| CSCvg81207 | Actions in interface 360 - shutdown of BDI interface does not work |
| CSCvg81210 | Actions in interface 360 - shutdown of serviceinstance sub-interface on 900 devices is disabled |
| CSCvg81229 | Actions in interface 360 - shutdown of BDI interface does not work |
| CSCvg81270 | EVPL/EVPLAN deletesite/delete not generating cfm negate\"no service evc...\" for 920/902 IOSXE |
| CSCvg82904 | CSRI: Environmental Temperature Report Issues |
| CSCvg83144 | CSRI: Interface Utilization not in synch with Topology |
| CSCvg83547 | Consolidated API - Unnecessary tunnels are created |
| CSCvg85126 | Ether channel list is not showing any data |
| CSCvg86813 | Remove the VT-2 option from HOP mode dropdown box in MBC UI as it is not supported in device |
| CSCvg88461 | Consolidated API - Tunnel discovery in missing state when source and destination has same tunnel ID |
| CSCvg89376 | Post CE provisioning invokes update for all resource pools |
| CSCvg90911 | Full GCs on scale setup post MP3 upgrade - nicePostInitTask is not complete or completed with errors |
| CSCvg91155 | After ESTV alarm is auto-cleared - the link remains RED with alarm icon |
| CSCvg92317 | Remove the STS-192C option from HOP mode dropdown box in MBC UI as it is not supported in device |

Table 1 **Open Bugs**

| Identifier | Description |
|----------------------------|-----------------------------------------------------------------------------------------------|
| CSCvg92742 | NCS2k: Device type showing \"Third Party Device\" and throw an exceptions for 10.6.1. version |
| CSCvg92786 | Collection failure due to missing association on STM64 VFAC after node disconnect |
| CSCvg93161 | Wired Detailed Device Inventory export fails with NullPointerException |
| CSCvb64742 | Alarms window (tab) drop-down filter list is blank |
| CSCvd90037 | All alarms supported by PI needs to be documented as supported for EPNM |
| CSCvg90802 | NME ports on ASR920 are not optical sfp ports |
| CSCvg51104 | Multiple entries under modules view |
| CSCvg81042 | Need NBI support for deleting the LSP path names while tunnel service deletion |

Resolved Bugs

Table 2 lists bugs that have been resolved since the last release. Specifically, it lists bugs that were listed as open bugs in the Cisco EPN Manager 2.1.2 release notes that have been resolved in Cisco EPN Manager 2.1.3.

For more information about the resolved bugs, go to the [Bug Search Tool](#).

Table 2 **Resolved Bugs**

| Identifier | Description |
|----------------------------|------------------------------------------------------------------------------------------------------|
| CSCvc49568 | Cisco Prime Infrastructure and Evolved Programmable Network Manager SQL Injection Vulnerability |
| CSCvc49574 | Cisco Prime Infrastructure and Evolved Programmable Network Mngr Reflected Cross-Site Scripting Vuln |
| CSCvf36235 | Wrong CLI command generated for Ethernet Subinterface Config |
| CSCvf44733 | Application restore failed on scale setup) |
| CSCvf47304 | teTunnelLsp plugins consumes more memory ~2GB |
| CSCvf54193 | Scale:Link Flap and Link Utilization reports failed with Failed to generate report error |
| CSCvb53324 | Granular Inv IOS-XR:LSP DOWN scenarios are not working |
| CSCvc50922 | Environmental Temperature report does not represent relevant values |
| CSCvd71782 | DSCP Classification dashlet shows out of range value in Rate column |
| CSCve92753 | CSRI: Deleting the devices left the corresponding alarms/events stale |
| CSCve93521 | VLAN Modification is not happening in device for CE services F2056 |
| CSCve93634 | Collection failure for ONS 15454 "unexpected error" |
| CSCvf15969 | after card out and in, the t1 cem service serviceability is down, on device service is up |
| CSCvf17700 | Merge PI issue CSCvf17690 to EPNM |

Table 2 **Resolved Bugs**

| Identifier | Description |
|----------------------------|----------------------------------------------------------------------------------------------------|
| CSCvf22522 | CFM Configuration issue with NCS4K device: OAM Ping/tracroute fails |
| CSCvf23199 | MTU mismatch between 9k and 900 in EVPLAN |
| CSCvf23360 | SFP data is not shown even if there is SFP |
| CSCvf32160 | Tunnel discovery is shown as Partial for a long time(nearly 4 hours)with two 4k midpoints |
| CSCvf32562 | Tunnel in Partial discovery state after performing fault scenario |
| CSCvf42042 | Celeborn bandwidth and Card Mode support should be based on slot number and Bheem Operating mode |
| CSCvf42283 | Static route configuration from EPNM fails |
| CSCvf49708 | NE device deletion does not modify accordingly the configuration archive job |
| CSCvf55839 | NCS42XX, ASR90X device goes to full sync due to CA even when "Inventory triggered" unchecked. |
| CSCvf58707 | CFM remote maintenance-points not available in device after provisioning service |
| CSCvf58734 | Device inventory collection fails due to stale entry of rfs.TdmCemProtectionGrpFlowpoint#117842404 |
| CSCvf59000 | CEM-Vcop service creation fails when dejitter is provided on 16.6.1vs image |
| CSCvf59174 | ODU UNI creation fails because service with same tunnel ID already exists |
| CSCvf59184 | ODU UNI in Partial state due to reactive sync on ROUTING-MPLS_TE-5-LSP_PATHCHANGE |
| CSCvf59196 | CEM/BiDirectional Tunnel API - Issue with MLT response, some missing/incorrect data |
| CSCvf60143 | EPNM mandating VLAN ID field for Untagged service |
| CSCvf60386 | NCS 4K packet alarm issues |
| CSCvf60432 | OpticalIUniRFS not created if historical version of OpticalLmpSettingsRFS is present |
| CSCvf60632 | Device inventory failed due to WCSDBA.MPLSTETUNNELSETTINGS_BK. |
| CSCvf61552 | Reactive inventory isn't causing collection of LAG related data |
| CSCvf62236 | CBR8 new device profile "CableBroadbandRouter" doesn't include Chassis View meta data |
| CSCvf62872 | Wrong ethernetPW status |
| CSCve63452 | 'Bottom n Interface Availability' dashlet availability status bar |
| CSCve83650 | Parse error while opening the EPNM OTDR Setting window |
| CSCvf22206 | Unable to enter Layer 3 VPN Customer BGP AS number higher than 32767 |
| CSCvf47878 | In link 360 graphs section - port availability should be called link availability |

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 those cases, the Cisco EPN Manager bug will be resolved when the hardware/operating system bug is resolved.

-
- 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 2.1.3, see the [Cisco Evolved Programmable Network Manager 2.1.3 Documentation Overview](#). The documentation overview also lists several Cisco Prime Infrastructure documents because the content of those documents is relevant to Cisco EPN Manager 2.1.3.

Accessibility Features in Cisco EPN Manager 2.1.3

For a list of accessibility features in Cisco EPN Manager 2.1.3, please contact accessibility@cisco.com.

All product documents are accessible except for images, graphics and some charts. 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* at: <http://www.cisco.com/en/US/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 deliver 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2017 Cisco Systems, Inc. All rights reserved.