Cisco Evolved Programmable Network Manager 2.1 Release Notes

First Published: March 30, 2017

Contents

This document contains the following information about Cisco Evolved Programmable Network Manager 2.1:

Functionality Added in Cisco EPN Manager 2.1

Provisioning - General

- Upon circuit/VC provisioning failure, automatic rollback to the previous configuration on the devices is performed and any CLI commands configured on the devices during the provisioning process are completely removed. In previous releases, if any configurations were left on the device after provisioning failed, rollback had to be done manually.

- Ability to change the default time to wait for device availability when deploying a service. If the device lock is not acquired within this timeout period, the deployment will fail.

- After deploying a service, you can choose to run the service deployment in the background and continue working in other areas of the application.

- Deleted circuits/VCs are now listed in the expanded circuits/VCs table.

- Ability to change the name of non-optical services.

- Ability to go back (from Preview page) and modify the provisioning order.

- Contextual-based error message in provisioning wizard.

- Ability to view deployment configuration details (along with failure, rollback details) from Circuit 360 view (including version/history).

Optical Transport

- Wavelength tracker for DWDM links, providing a map of used and available wavelengths per DWDM link.

- NCS 1002 OCH-Trail end-to-end discovery. When using an NCS 1002 device as a transponder device in conjunction with an NCS 2000 ROADM network, Cisco EPN Manager discovers the wavelength path generated at the NCS 1000 device and traveling through the NCS 2000 ROADM network.

- Ability to add user-defined attributes to NCS 2000 and NCS 4000 devices and visualize them in the device list.

- Ability to modify the line card configuration on 400G-XP, 200G-CK-LC, and 100GS-CK-LC Flex line cards.

- In the Interfaces summary in the Logical view for a Cisco NCS 2000 device, there are two additional columns (Display Name and Card Name) for identification of cards added to Cisco EPN Manager. This helps in understanding the connections between every patchcord.

- While viewing the details of a Cisco NCS 2000 device, two new columns in the Device Details table called Cards and Part Numbers show the cards that are associated with every interface of the device and the available part numbers respectively.

- Ability to choose the device scan mode when running a performance test on an OTS link.

- Cisco NCS 2000 400G-XP-LC and MR-MXP cards can now be configured with the following new card operating mode and payload values:

  - Payload types OTU2/OC192 for MR-MXP cards

  - Payload types 16G-FC/OTU2 for 400G-XP-LC cards

  - Slice operating mode OPM_6x16G_LC for 400G-XP-LC cards

CEM

- Ability to choose a unidirectional TE tunnel as the preferred path type for traversal of a CEM service.

- Ability to export BERT performance test results.

- Ability to associate user-defined QoS policies for CEM services

L3VPN

- You can now modify the name of the service and associated IP SLA parameters during service modification and deletion.

Carrier Ethernet

- Ability to choose a unidirectional TE tunnel as the preferred path type traversal of an EVC.

- Ability to specify the test mode as one way or two way when running a performance test for EVC based on Y.1564.

- Ability to run the performance test for EVC based on Y.1731.

- Point-to-point services now use the "l2vpn xconnect" command on XE devices.

- Support for user-defined VPN ID.

- Ability to associate user-defined QoS policies for CE services.

MPLS TE

- Ability to create and provision a unidirectional TE tunnel.

- Ability to disable re-optimization of LSP for bidirectional and unidirectional TE tunnels.

- Ability to choose a Layer 2 discovery protocol when provisioning a layer 3 link.

- (Beta) IS-IS and BGP are supported as the routing protocols for layer 3 link.

Note Any references to this feature in the Cisco EPN Manager User and Administrator Guide reflect Beta functionality only.

- Ability to view the list of circuits that traverse through an MPLS TE tunnel in the Circuit 360 view.

- Ability to use ASR 9000 devices as the mid-point for bidirectional and unidirectional TE tunnels.

- Ability to use ASR903/907/920 devices with RSP2 for bidirectional and unidirectional TE tunnels.

QoS

- Ability to create a new QoS profile by cloning an existing one.

Topology

- Ability to manually create topological links on the map in cases where Cisco EPN Manager is unable to discover the link from the network. Manually created links can be:
    - Managed links which are saved to the database and appear in all links tables
    - Unmanaged links which are for visualization purposes only
- Ability to delete the saved manual layout in order to return to the default system layout.

- Ability to visualize BGP and OSPF routing networks on the map.

- Visualization of Shared Risk Resource Groups (SRRGs) on the geo map for NCS 2000 and NCS 4000 devices and OTS or OTU links.

- The topology map can now be accessed from the Actions menu in all the 360 views (circuit, device, link, interface) and in the alarm table. The relevant object (circuit, device, link, etc.) will be highlighted in the map.

Multilayer Trace

- Power levels of the ports are now shown in the Link Details window of the Multilayer Trace.

- Ability to differentiate optical line amp in the multilayer trace.

Fault Management

- When flapping alarms are detected, further updates of the alarm are stopped until the flapping condition on the device is cleared. This prevents the device from going into continuous synchronization state.

- Service name is included in northbound notifications.

- Auto-clear of alarms based on inventory status.

- Alarm correlation and indication of service impact for CE and CEM services passing through bidirectional or unidirectional TE tunnels.

- OAM support for:

  - CEM/EPL passing through bidirectional TE tunnel.

  - OAM support for EVPL over unidirectional TE with FRR.

  - CEM aggregation over bidirectional TE tunnel.

  - E-Line service to remote building over MPLS.

  - E-Line service to service edge over MPLS.

Reports

- GFP statistics report now supports NCS 4000 devices.

RESTCONF NBI

- Creation and deletion of internal patch cords on NCS 2000 devices

- Retrieval of internal patch cords via link retrieval

- Modification of service name for non-optical circuits

- Alarm action (acknowledge/unacknowledge/clear/delete) on alarms

- Alarm retrieval based on equipment

- L3 link provisioning support for BGP

- L3 link provisioning support for ISIS

- (Beta) Enhanced support for L3 Link provisioning for OSPF

- Device and link constraint support for optical service

- Optical span loss retrieval for links

- Set termination point for optical attributes

- LSP diversity when provisioning optical circuits

- Retrieval of diverse LSP information for optical circuits

- Retrieval of virtual connections associated to an explicit path
- Retrieval of Shared Risk Resource Groups
- Multilayer trace API enhancements for optical, CEM and L2VPN services
- (Beta) Consolidated service provisioning to support central and remote office use cases
- (Beta) Provisioning of E-Line Services with TE Tunnel and running Y1731 or Y1564 service tests
- (Beta) Provisioning of CEM Services with TE Tunnel and running BERT service test
- API to run service tests on existing services (standalone service tests) - Y1564, Y1731, BERT
- Support for protection profile control and retrieval operations - creation, modification, termination and retrieval
- Support for service profile retrieval and provision for using service profiles during service provisioning for Optical, CE and CEM services
- Enhanced notification support for alarm actions

MTOSI NBI
- Mutual diversity of OCHTrail UNI

Device/OS Support Added in Cisco EPN Manager 2.1

Cisco NCS 2000 Network Convergence Systems—New Operating System Beta Support

Device Model	Device OS
Cisco NCS 2002, 2006, 2015	ONS 10.6.2 (Beta support only)

Cisco NCS 1000 Network Convergence Systems—New Operating System Support

Device Model	Device OS
Cisco NCS 1002	IOS-XR 6.2.1
Cisco NCS 1001	IOS-XR 6.2.1 (Beta support only)

Cisco NCS 40xx Network Convergence Systems—New Operating System Support

Device Model	Device OS
Cisco NCS 4016	IOS-XR 6.1.22
Cisco NCS 4009	IOS-XR 6.1.22

Cisco NCS 5000 Network Convergence Systems—New Operating System Support

Device Model	Device OS
Cisco NCS 5000 series	IOS-XR 6.1.2

Cisco NCS 5000 Network Convergence Systems—New Device Support

Device Model	Device OS
Cisco NCS 5001 as a satellite on ASR 9000	IOS-XR 6.1.2
Cisco NCS 5002 as a satellite on ASR 9000	IOS-XR 6.1.2

Cisco NCS 5500 Network Convergence Systems—New Device Support

Device Model	Device OS
Cisco NCS 5501 and Cisco NCS 5501-SE	IOS-XR 6.1.2
Cisco NCS 5502 and Cisco NCS 5502-SE	IOS-XR 6.1.2

Cisco NCS 6000 Network Convergence Systems—New Device Support

Device Model	Device OS
Cisco NCS 6000	IOS-XR 6.1.2

Cisco Carrier Routing Systems—New Operating System Support

Device Model	Device OS
Cisco CRS	IOS-XR 6.1.2

Major GUI Enhancements to Dashboards

There has been a reorganization of the dashboards in Cisco Evolved Programmable Network Manager 2.1 to make grouping of dashboards and dashlets more logical and intuitive, to remove duplication of information, and to remove information that is not relevant.

This section highlights the most significant changes to each of the dashboard categories, as follows:

- Service Performance Dashboards
- Performance Dashboards
- Network Summary Dashboards
- Device Trends Dashboards

In addition to the changes in the above dashboard categories, the Wireless dashboards have been removed.

The user documentation has been updated to reflect this reorganization of dashboards. See the *Cisco Evolved Programmable Network Manager 2.1 User and Administrator Guide*.

Service Performance Dashboards

The following changes have been made to the Service Performance dashboards:

- New TE Tunnel dashboard provides details, availability and statistics for a specific TE tunnel during a specific time frame, as well as outgoing traffic, bandwidth utilization, and bandwidth availability.
- The Service Performance dashboard has been renamed "CE/L3VPN."
- The following dashboards have been moved from the Service Performance dashboard category to the Performance dashboard category:
  - IPSLA
  - QoS
  - Y1731
  - Interfaces

Performance Dashboards

The following change has been made to the Performance dashboards:

- New BNG dashboard provides details for the Broadband Network Gateway (BNG) for a specific device during a specific timeframe, as well as statistics on IP address pool usage and subscriber sessions.

Network Summary Dashboards

The following changes have been made to the Network Summary dashboards:

- The Overview dashboard has been renamed "Network Devices."
- Top N Interfaces view is now a separate dashboard under Network Summary. It shows a summary of interface utilization and availability.

- The following dashlets have been moved from the Service Performance/Interfaces dashboard to the Top N Interfaces dashboard under Network Summary:

    – Top N interface traffic

    – Top Interface Errored and Discards

    – Bottom N Interface Availability

    – Top N interface utilization

- Top N QoS view is now a separate dashboard under Network Summary. It shows statistics for class map traffic.

- The following dashlets have been moved from the Service Performance/QoS dashboard to the Top N QoS dashboard under Network Summary:

    – Top N QoS Policy Rate

    – Top N QoS Post Policy Rate

    – Top N QoS Drop Rate

    – Top N QoS Exceeded Rate

    – Top N QoS Conformed Rate

    – Top N QoS Violated Rate

- The Site dashboard has been removed and its Top N Devices with Most Alarms dashlet has been moved to the Incidents tab.

Device Trends Dashboards

The Performance dashboard category was renamed "Device Trends". Device Trends contains:

- Devices dashboard that shows trends in memory and CPU utilization, port summary and device health information for specific devices.

- Applications dashboard that shows client, traffic, server, and application trends for selected applications or services.

Installation/Upgrade Paths

The following table lists the installation/upgrade paths for Cisco EPN Manager 2.1.

Note that:

- PP = *Point Patch*
- Cisco EPN Manager 2.0.x = Cisco EPN Manager *2.0 Maintenance Pack x*.
  For example, Cisco EPN Manager 2.0.4 = *Maintenance Pack 4*.

Note Cisco EPN Manager 2.1.0.1 is a point patch that addresses various issues found in Cisco EPN Manager 2.1. It is highly recommended to install this point patch after installing Cisco EPN Manager 2.1. Information about the point patch and installation instructions can be found in the readme file supplied with the patch file on the Software Download site on Cisco.com.

If you have this deployment:	Perform these steps to install/upgrade to Cisco EPN Manager 2.1:
Cisco EPN Manager is not installed (fresh installation)	1. Install Cisco EPN Manager 2.1—See *Cisco EPN Manager 2.1 Installation Guide*
Cisco EPN Manager 1.2.x, 2.0, 2.0.1, 2.0.2, or 2.0.3	1. Install Cisco EPN Manager 2.0.4—See *Cisco EPN Manager 2.0.4 Installation Guide* 2. Upgrade to Cisco EPN Manager 2.1—See *Cisco EPN Manager 2.1 Installation Guide*
Cisco EPN Manager 2.0.4	1. Upgrade to Cisco EPN Manager 2.1—See *Cisco EPN Manager 2.1 Installation Guide*
Cisco EPN Manager 2.0.4 with PP1 (2.0.4.1)	1. Install Cisco EPN Manager 2.0.4 PP2 (2.0.4.2)—See the readme file provided with the software on the Software Download site on Cisco.com. 2. Upgrade to Cisco EPN Manager 2.1—See *Cisco EPN Manager 2.1 Installation Guide*
Cisco EPN Manager 2.0.4 with PP2 (2.0.4.2)	1. Upgrade to Cisco EPN Manager 2.1—See *Cisco EPN Manager 2.1 Installation Guide*

Important Notes

- TLS 1.2 Required for Secured Channel Communication for HTTPS and TLS
- Reconciliation Report Limitations

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.

Cisco EPN Manager Bugs

- Open Bugs
- Resolved Bugs

Open Bugs

Table 1 lists the open bugs in Cisco EPN Manager Release 2.1 according to the following criteria:

- Severity 1, 2, and high priority severity 3 open bugs
- All open customer-found bugs

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
CSCvc10942	SONET controller down - DS1 port is taking very long time to go down
CSCvc28763	A9K-400G-DWDM-TR on chassis ASR9904 Laserbeak CFP2 ports is not showing
CSCvc56431	360: Multilayer trace (MLT) is not working as expected for unidirectional tunnel
CSCvd13552	Scale: Many scheduled reports fail
CSCvd23634	Scale: FD leak caused by scheduled reports
CSCvd30795	Scale: INSERT into RESTCONFSERVICEREQUEST is stuck and could not complete
CSCvd42457	Modify CEM - Changing the preferred path takes more than 30 minutes for service state to come up
CSCvd44833	(IOS devices) EVPTREE- Serviceability state shows Down status, but the interfaces are up
CSCvd52385	E2E - EVPTREE: Topology displays deleted end point devices after 2nd modification.
CSCvd62860	Circuit 360: bidirectional tunnel showing unknown endpoint
CSCvd71399	E2E: Device going to Collection Failure
CSCvd71470	Deleting CE service does not work properly - PW class CLI is not removed
CSCvd73921	ODU UNI and OCH-CC circuit provisioning have associated ODU tunnel and OCH Trails duplicated

Table 1   Open Bugs

Identifier	Description
CSCvd75201	E2E:- EVPTREE: 1 managed Endpoint Missing in 360 View and connection not displayed in Topology View
CSCvd78137	Proper CLI should be generated for explicit path with protection under below scenario
CSCuu92664	EVPLAN Profile can't be created if Device Name or Port Name is empty
CSCuz26687	NCS42xx-Inventory: duplicate SONET entries for STS concatenation
CSCuz84623	CV: Satellite device inventory data missing
CSCva54469	Scheduled 1 Day Optical Performance Reports Run Results have no data
CSCvb45995	Warning/Error Messages from CLI are Not handled for all MBC Features
CSCvc49746	Inconsistent handling device name hyper-link for readability alarm
CSCvc73719	OAM commands not working for Partial Services with unmanaged Non-Cisco devices
CSCvc82773	Events/Alarm export fails to export correct data in certain scenarios
CSCvc96165	Not able to promote an EPNL when pseudowire-class is not defined
CSCvc96174	After Switching a router from SSH to Telnet, it still uses port 22
CSCvd03041	Cannot promote service on the same device
CSCvd08179	civic location - add ability to set only one of the fields Building, Floor & Room
CSCvd08836	Alarms / Events: Only selected rows need to be exported to CSV
CSCvd09582	Scale: Time taken to create a new Interface Health policy is 8 mins
CSCvd10199	Modifying multiple devices civic location when there is profile causing removal of all info
CSCvd13056	EPNM tries to connect to various external websites
CSCvd18743	Template-based config multiple or single device retrieval missing details
CSCvd22903	Image distribution using SCP fails, even though it is successfully copied
CSCvd28785	Inconsistent timestamps in the GUI
CSCvd31760	C360 KPI data not displayed for partial CEM services
CSCvd44601	QoS Policy Report SQL Optimizations
CSCvd44625	QoS Policy report generates both the table and graph view in the same report
CSCvd45377	Bundle-Ether interface configured with EPNM not selectable for device during CE UNI service provisioning
CSCvd45477	Rounding of QoS policy class map traffic dashlet view values introduces inaccuracy
CSCvd48190	NCS42xx devices goes into continuous sync state due to LSP path tear events flooding
CSCvd52260	Rollback - after the delete fail of the Promoted service, EPNM generates irrelevant CLI on modify.
CSCvd58662	QoS policy report does not consider selected virtual domain

Table 1　　**Open Bugs**

Identifier	Description
CSCvd66172	QoS report failed to run with "Unable to retrieve data" error
CSCvd67463	E2E: For EVPL service created with an existing uni, delete failed with "Deleting AC member."
CSCvd69469	Modification failed for provisioned L3VPN QoS service.
CSCvd71395	MPLS TE Upgrade: L3link and TE Tunnels modify orders are failing with error 500.
CSCvd71578	Interface traffic and errors and discards report failure- CFS table- Obsolete design reference
CSCvd71782	DSCP Classification dashlet shows out of range value in Rate column
CSCvd71798	E2E: EVPL: Error 500 thrown while deleting EVPL Service.
CSCvd73125	Serviceability and severity shows "No data available" on Link 360
CSCvd73803	Image distribution using SFTP fails for NCS4k
CSCvd74992	EVPL modify wizard: unexpected removal of L2VPN xconnect and pseudowire related commands
CSCvd78019	[Inline Upgrade] Kernel ERROR while performing upgrade on a Bare Metal
CSCvd78083	Syslog export not happening with show all and export pop not loading with IE
CSCvd78168	Cleared GUI setting is a blank page and does not restore values with "restore default system settings"
CSCvd79400	Delete generates incomplete CLI commands for CEM service CESoPSN DS0 circuit
CSCvd79642	EVP-LAN provisioning has MTU mismatch for ASR9k and ASR920
CSCvd80925	Rollback does not work when the service deployment is failed
CSCvd81296	Missing link included on TE service links
CSCvd81615	Policier action - PRI shows bytes, when it should be bps (bits per second)
CSCuw80244	The "Filter" Icon in Alarms and Events does not function as expected.
CSCvb67689	CPAK Lane missing in the Multi-trace for NCS4K

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 2.0.4 release notes that have been resolved in Cisco EPN Manager 2.1.

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

Table 2   Resolved Bugs

Identifier	Description
CSCva92785	View360 shows 20CS for module rather than 10CS
CSCvb25348	E2E: Ethernet EVC OAM Profile in UNI create not accepted in device
CSCvc31424	Device goes to Partial collection failure
CSCvc35054	E2E: EVP-LAN modify failed after UNI modified (by adding QOS) with Invalid refInstanceId 500
CSCvc45981	No CFS match after EVPL local connect provisioning
CSCvc48883	Scale: Polled data is not reflected in database
CSCvc51252	SIT E2E - nodes in permanent synchronization during HA testing on a scaled network
CSCvb21367	MPLSTETUNNELSETTINGS totalBW and AvailBW not updated with zero
CSCvb89805	Wrong overlay for uni-directional and wrong service detail for bi-directional TE tunnel link
CSCvc29782	Scale: System operational status job is not following the polling schedule
CSCvc50830	Edit button is not displayed for SyncE Global Config and PTP Clock Port configurations pages.
CSCvc79740	Appliance backup fails when application has no backup hook in manifest file
CSCvc23493	Evaluation of CEPNM for NTP November 2016
CSCvc33601	DB queries running a long time
CSCvc51387	Circuit creation fails
CSCvc52132	Unable to create 100GE GMP over ODU4
CSCvc54177	Optical SFP data not polled for ASR920 and 907
CSCvc38754	VC route information missing in NBI Get for CESoPSN partial service
CSCvc38980	Elan/Etree Amend with Partial Service - removing PWClass

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, see the *Cisco Evolved Programmable Network Manager 2.1 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.

Accessibility Features in Cisco EPN Manager 2.1

For a list of accessibility features in Cisco EPN Manager 2.1, 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.