Cisco Evolved Programmable Network Manager 2.0.1 Release Notes

First Published: July 5, 2016

Updated: September 28, 2016

This document outlines the additional feature and device support available in Cisco Evolved Programmable Network Manager (Cisco EPN Manager) 2.0 Maintenance Pack 1 (MP1).

Note This document also provides information about the mandatory point patch—Cisco EPN Manager 2.0.1.1—that must be installed on top of Cisco EPN Manager 2.0 MP1.

Contents

This document contains the following sections:

Cisco Systems, Inc.
www.cisco.com

Functionality Added in Cisco EPN Manager 2.0 MP1

Inventory

- Chassis View enhancements:
  - Support for “mixed chassis” devices (devices with different chassis types)
  - New toggle to view front and rear of chassis (Cisco NCS 1002 only)
  - New default image for unsupported line cards (instead of a question mark); card name is also displayed
  - Pulsating icon to help user locate interface chosen in search field
- New network hardware inventory view (**Inventory > Device Management > Network Inventory**) for sorting, filtering, searching, exporting of the network-wide inventory
- Device 360 view enhancements:
  - IP address is a hyperlink that launches the Device Details page
  - New tabs: Civic Location, Recent Changes
  - New actions: Sync (performs inventory collection and saves devices data to database); view routing table information; connect to device via SSH/Telnet.
- Interface 360 View enhancement:
  - New action: Link to new Optical Interfaces dashboard for historical performance information
- Ability to access the device console showing the device’s CLI from the Device 360 view and the alarms list.

Configuration

- Optical interface configuration enhancements:
  - QoS: Improved navigation for creation and management of Action and Classification profiles
  - Device ports can now be analyzed using SPAN and RSPAN
  - Support for enabling Automatic Laser Shutdown (ALS) which automatically shuts down the output power of transmitters in case of issues such as a fiber break
  - Ability to configure OTDR scans that begin automatically on a fiber span that has been repaired or on the startup of an OSC channel
- Support for SNTP to synchronize the clocks of devices to a specified date and time
- Ability to provision the wavelength frequency for optics controllers
- Ability to configure Label Distribution Protocol (LDP) links in an MPLS network
- Support for clock synchronization using PTP (Precision Time Protocol)
- Ability to configure TWAMP responders that define a standard for measuring round-trip IP performance between any two devices that support the TWAMP protocols
- Ability to configure alarm profiles on ports, cards, and nodes of devices.
- Support for setting dataplane loopback values for VLANs associated with Ethernet interfaces and subinterfaces.
- Ability to view alarms with ‘Unverified’ status and to mark them ‘Acknowledged’ so that they no longer appear as unread alarms on the device.

Performance

- Performance graphs can be launched from the Device 360 view (new hyperlink)
- Performance dashboard enhancements:
  - New Service Performance dashboards: IP SLA, CEM, Y1731, QoS
  - New Optical Interfaces dashboard for historical performance information
  - Performance of L3VPN devices added to the Service Performance dashboard
- New monitoring policies: Optical SFP, IPSLA
- Additional performance graphs for CEM in Circuit 360 view
- Ability to export the OTDR scan results in .sor format
- Performance of L3VPN devices added to the Service Performance dashboard
- Real-time optical performance data can be accessed from the Interface 360 view

Fault Management

- Alarm correlation mechanism enhanced to perform alarm-to-alarm correlation. These alarms can be viewed from the Alarms and Events table as follows:
  - New Correlation Type column, which indicates if alarm is root cause or symptom and provides hyperlink to Correlated Alarms tab
  - New Correlated Alarms tab, which lists all uncleared correlated alarms
- Alarm root cause analysis for L3VPN, L2VPN and CEM services
- Enhancements to service-to-alarm association for L3VPN, L2VPN and CEM services
- Export of alarms, syslogs and events in csv and pdf format
- Ability to display an alarm list for historical versions of optical circuits.

Topology

- Visualization of Sync E and PTP networks on the topology map
- Direct access to circuit/VC details via hyperlink on circuit/VC name in circuit/VC tables
- Discovery of MPLS LDP neighbors and population of topology links
- Discovery of LLDP neighbors and population of topology links
- Discovery of BGP and OSPF links and population of these links on the topology map

Geo Map Enhancements

- Ability to work with the geographical map without Internet access (offline mode), using installed map resources
- Synchronization of location coordinates between the device and the geo map.
- Devices/networks added manually to the topology map will be displayed on the geo map as well

Multilayer Trace Enhancements

- Simplified three-dimensional and linear views with the option to expand or collapse layers
- Link Details popup window provides details for affected internal ports in both directions, including port status, layer, and power levels

Carrier Ethernet Provisioning and Management

- Ability to compare and reconcile discovered vs. provisioned versions of a circuit/VC.
- Discovery and provisioning of E-LAN and E-TREE EVCs that have endpoints that are not managed by Cisco EPN Manager (partial services).
- Extension of E-Line, E-LAN, and E-Tree EVCs using templates (IOS devices). Additional configurations defined in the templates are written to the devices participating in the circuit/VC.
- Reactive polling for Carrier Ethernet services.
- Ability to select multiple UNIs when provisioning E-Tree services.
- Support for simplified topology (VPLS) for E-Tree services.
- Ability to promote VPLS E-Tree services
- Extension of E-Tree configuration scope
- QoS enhancements for CE services:
  - Support for discovery (except for E-Access services)
  - Support for individual QoS policy attachment for ingress and egress

Optical

- Ability to view additional information about why a provisioning action has failed for an optical circuit. This information is accessed from the Circuit/VC 360 view and the expanded table of circuits/VCs.
- Ability to select a diverse tunnel to ensure that if there is a failure in a tunnel, the same tunnel is not used to provision another circuit.

CEM

- Provisioning of CEM services over Packet Switched Network (CESoPSN)
- Ability to provision a CEM service that includes an unmanaged endpoint
- Ability to promote a discovered CEM service in order to modify or delete the service
- Extension of CEM services using templates for support of QoS over CEM. Additional configurations defined in the templates are written to the devices participating in the service.

L3VPN Service Provisioning and Management

- Visualization of L3VPN services on the topology map (overlay).
- Ability to configure IP Service Level Agreements (SLAs) operations (manually or using profiles) to monitor end-to-end response time between devices while provisioning L3VPN services. The IP SLA operation can also be scheduled at a specified date and time.
- Ability to promote a discovered L3VPN service in order to modify or delete the service.
- Scale improvement: You can now associate up to five VRFs per L3VPN service, during service creation.
- Extension of L3VPN services using templates. Additional configurations defined in the templates are written to the devices participating in the service.
- Support for route distribution using the OSPF protocol.
- Support for VRFs and IP addresses to be configured under the sub-interfaces or under the BVI (virtual) interfaces.
- Dual-AS routing support for the associated BGP neighbor.

- Association of QoS policy maps to service endpoints during service creation.

MPLS Traffic Engineering Service Provisioning and Management

- When provisioning a MPLS Layer 3 link, you can select ingress and egress QoS policies to be configured on the A-end and Z-end devices.

Service Diagnostics and Troubleshooting

- VRF traceroute and ping
- CFM traceroute and ping
- MPLS LSP traceroute and ping
- FlexLSP traceroute and ping
- PW traceroute and ping

Administration/Licenses

- Support for two flavors of Device Right-to-Manage licenses:
  - Extended—Enables end-to-end network management for core, edge, aggregation, and access network devices. Includes: device lifecycle management, network provisioning, and network assurance.
  - Foundation—Enables device lifecycle management, assurance visibility, and troubleshooting capabilities for service provider WiFi networks that have WiFi access points, WAN routers, core switches, and data center switches.

GUI

- Ability to create and save user-defined filters in expanded tables of circuits/VCs and links.
- Ability to edit network interfaces from the network interfaces tables. Clicking the Edit button opens the Provisioning wizard.

RESTCONF YANG API

- Provisioning, modification and termination of CE, Flex, CEM and L3VPN services
- Virtual connection CFS/RFS retrieval for CE, Flex, CEM and L3VPN services
- Virtual connection route retrieval for CE, Flex, CEM and L3VPN services
- Topological link retrieval for CE, Flex, CEM and L3VPN services
- Route and topological link retrieval for CE, Flex, CEM and L3VPN services
- Setting configurable attributes on termination point for a supported set of attributes
- Customer-facing service retrieval
- Network interface (UNI/ENNI) retrieval
- QoS policy and QoS profile retrieval
- Termination point retrieval
- Create/update/delete customer
- Resource activation (CLI configuration: model-based and template-based)
- Notification on inventory and high-availability
- Notification for provisioning, modification and termination of CE, Flex, CEM and L3VPN services

Documentation

- The addendum to the User and Administrator guide describing wireless and data center features is available in the online help and in the version published on Cisco.com.

Additional Device/Module/OS Support in Cisco EPN Manager 2.0 MP1

This section lists the new support provided in Cisco EPN Manager 2.0 MP1. 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 NCS 2000 Network Convergence Systems

Device Model	Device OS
Cisco NCS 2xxx	R10.5.2.2, R10.5.2.4 R10.6 (Beta)

Cisco NCS 4000 Network Convergence Systems

Device Model	Device OS
Cisco NCS 4xxx	6.0.2 (Beta), 6.1.1 (Beta)

Cisco NCS 4200 Network Convergence Systems

Device Model	Device OS
Cisco NCS 4201	3.18.03v.S/15.6(2)S3v (Beta)

Cisco NCS 1000 Network Convergence Systems

Device Model	Device OS
Cisco NCS 1002	6.0.1 Beta-level support

Cisco ASR 9000 Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 9001	IOS XR 6.0.1
Cisco ASR 9904	
Cisco ASR 9006	
Cisco ASR 9010	
Cisco ASR 9912	
Cisco ASR 9922	

Cisco ASR 9000v Satellite Routers—New Operating System Support

Device Model	Device OS
Cisco ASR-9000v DC Power ANSI Chassis	IOS XR 6.0.1
Cisco ASR-9000v DC Power ETSI Chassis	
Cisco ASR-9000v AC Chassis	
Cisco ASR 9000V 24vDcA Router	
Cisco ASR 9000V2 AC Chassis Router	

Cisco ASR 900 Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 902	3.18/15.6(2)S
Cisco ASR 903	
Cisco ASR 907	

Cisco ASR 901S Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 901S-4SG-F-D	3.18/15.6(2)S
Cisco ASR 901S-3SG-F-D	
Cisco ASR 901S-3SG-F-AH	
Cisco ASR 901S-2SG-F-AH	

Cisco ASR 901 10G Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 901-6CZ-F-A	3.18/15.6(2)S
Cisco ASR 901-6CZ-F-D	
Cisco ASR 901-6CZ-FT-D	
Cisco ASR901-6CZ-FT-A	

Cisco ASR 920 Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 920	3.18/15.6(2)S
Cisco ASR 920 24SZIM	
Cisco ASR 920 24SZM	
Cisco ASR 920 24TZM	
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 8S Z0D	

Cisco Network Convergence System 5500 Series Routers—New Operating System Support

Device Model	Device OS
Cisco Network Convergence 5508 Router	6.1.1.18I (limited functionality)

Cisco ME 3600X Series Ethernet Access Switches—New Operating System Support

Device Model	Device OS
Cisco ME 3600X-24FS-M	3.18/15.6(2)S
Cisco ME 3600X-24TS-M	
Cisco ME 3600X-24CX-M	
Cisco ME 3600X-24CXE-M	

Cisco ME 3800X Series Carrier Ethernet Switch Routers—New Operating System Support

Device Model	Device OS
Cisco ME 3800X-24FS-M	3.18/15.6(2)S

Cisco cBR Series Converged Broadband Routers—New Device and Operating System Support

Device Model	Device OS
Cisco cBR-8 Converged Broadband Router	15.6/3.18

Wireless and Data Center Devices

- Support for the wireless devices that are referenced in the device support table *Cisco Evolved Programmable Network Manager Supported Devices*.

Content of the Mandatory Point Patch

The following point patch must be installed on top of Cisco EPN Manager 2.0 MP1:

- Point patch 1 (PP1)—Cisco EPN Manager 2.0.1.1

Additional Operating System Support

- ONS 10.5.2.4 on NCS 2000 family devices
- IOS-XR 6.0.2 on NCS 4000 family devices

Bug Fixes

Cisco EPN Manager 2.0.1.1 addresses the following issues:

Identifier	Symptom
CSCuz48251	VPN ID resource pool conflict causing L3VPN deploy failure
CSCva07144	Y1731 CoS field collection is not done for XR devices
CSCva23453	Device inventory collection is failing.
CSCva27787	L3 MPLS VPN,VrfMatrix plugins never finish and they throw hibernate exception
CSCva28032	CFS matching fails for L3VPN provisioning with BVI interfaces
CSCva32835	IPSLA performance data is not being aggregated
CSCva33226	L3VPN deploy fails because of L2 IP SLA and L3 IP SLA resource pool
CSCva33468	QOS RFS is deleted and re-added frequently

Identifier	Symptom
CSCva38103	Device is in collection failure due to WCSDBA.SYS_C0025411
CSCva38277	Fault-assurance issues (OAM, OSPF overlay)
CSCuy51201	MIB QOS post policy is 0 while no drops are reported in the CLI
CSCuz73989	Dashlets referring to Device Health Info
CSCuz79971	DFS: ASR9006 in partial collection failure due to mef-qos-inventory
CSCuz92386	Unable to delete the devices due to WCSDBA.FK46858D80E9E39B23
CSCva14160	LDP: Inconsistent behavior for peer and local transport port discovery.
CSCva16086	IPSLA graphs display invalid x-axis values
CSCva16513	OTDR save recurrence causing collection failure in backend
CSCva21887	Unmanaged endpoint is missing in 360 view for EVPL service
CSCva28049	SyncE/SyncE BITS IOS-XR inventory and configuration is blocked
CSCva29288	Unable to modify service after promotion if it contains rd value
CSCva30330	ETREE wizards with unmanaged UNI don't send pseudowire and VFI commands to device
CSCva31169	Scale: Events without localized index should not be considered for IC
CSCva34095	y1731 graph dashlets display incorrect units in y-axis title
CSCva34928	Cross-connection empty with user other than root
CSCva35024	SyncE overlay does not work
CSCva35174	IDevice collection failure due to WCSDBA.SYS_C0010769
CSCva36255	Device support \"Cisco ASR 920-12SZ-IM Router\" missed for Y1564 feature
CSCuz58060	Exception causing DB deadlock
CSCuy60204	IntrfcPrtclEndpnt instance name as Null and unable to delete the device

Installing the Mandatory Point Patch

The following point patch must be installed on top of Cisco EPN Manager 2.0 MP1:

- Point patch 1 (PP1)—Cisco EPN Manager 2.0.1.1

The installation flow is as follows:

1. Install Cisco EPN Manager 2.0 MP1. See the *Cisco Evolved Programmable Network Manager 2.0.1 Installation Guide*.
2. Install Point Patch 1—Cisco EPN Manager 2.0.1.1:
   - To install a point patch in an environment with no high availability, see Download and Install a Patch (No HA).
   - To install a point patch in a high availability environment, see Download and Install a Patch (HA Deployment). Note that high availability must be set up before installing the patch.

Note If you are upgrading from a previous version to Cisco EPN Manager 2.0 MP1, perform the upgrade first and then install the point patch.

Download and Install a Patch (No HA)

Follow these steps to install a point patch on top of Cisco EPN Manager 2.0 MP1 in a standard environment (no high availability).

Step 1 Log into Cisco EPN Manager as a user with Administrator privileges.

Step 2 From the left sidebar, choose **Administration > Licenses and Software Update > Software Update**.

Step 3 Get the ubf file, either by downloading it directly from Cisco.com or by uploading it to the server from a saved location:

- If your server has Internet connectivity:
  - Click the blue **Download** link at the top of the page and log into Cisco.com. The system checks for available software updates.
  - Select the required patch and click **OK** to start the download from Cisco.com to the server.
- If your server does not have Internet connectivity or you have obtained the ubf file from another source:
  - Get the patch installation file from the Software Download page on Cisco.com and copy it to your Cisco EPN Manager server.
  - Click the blue **Upload** link at the top of the Software Update page in Cisco EPN Manager, browse to the ubf file and click **OK**.

After the successful download or upload of the patch, the patch name will appear under Critical Updates on the Software Update page.

Step 4 Install the patch by clicking its associated **Install** button. Cisco EPN Manager will auto-restart and the Cisco EPN Manager GUI will not be accessible for some time. After successful installation, the status will change to “Installed”.

Step 5 Run the **ncs status** command to ensure that all services are up and running.

Step 6 Log into Cisco EPN Manager to verify that the GUI is accessible. Check that the point patch version is showing correctly in the Login, About, and Software Updates pages.

Download and Install a Patch (HA Deployment)

Follow these steps to install a point patch on top of Cisco EPN Manager 2.0 MP1 in a deployment that is already configured for high availability, where the secondary server is registered to a primary server.

Note You must start the patch install with the primary server in the **Primary Active** state and the secondary server in **Secondary Syncing** state. See the installation steps below for details.

Patching of primary and secondary HA servers takes approximately one hour. During that period, both servers will be down.

Before You Begin

- Make sure you have the password (authentication key) that was created when HA was enabled. You will need it to install the maintenance pack on the secondary server.

Step 1 Check the HA status on the primary server:

a. Log into the primary server as a user with Administrator privileges.

b. From the left sidebar, choose **Administration > Settings > High Availability**.

c. In the HA Status page, confirm that the primary server's state is **Primary Active**.

d. Click **HA Configuration** and confirm that the Configuration Mode is **HA Enabled**.

Step 2 Check the HA status on the secondary server:

a. Log in to the secondary server's HM web page by entering the following URL in your browser:

https://*serverIP***:8082**

where *serverIP* is the IP address or host name of the secondary server.

b. Enter the authentication key and click **Login**.

c. Verify that the Current State Mode is **Secondary Syncing**.

Step 3 On the secondary server, download and install the patch:

a. Log in to the secondary server's Health Monitor (HM) web page by entering the following URL in your browser:

https://*serverIP***:8082**

where *serverIP* is the IP address or host name of the secondary server.

b. Enter the authentication key and click **Login**.

c. Click **Software Download** at the top right of the Health Monitor window to open the Secondary Server Software Update window.

d. Enter the authentication key and click **Login**.

e. Click the **Upload** link under the window title, browse to the patch ubf file, and click **OK**.

After the successful download or upload of the patch, the patch name will appear under Critical Fixes on the Software Update page, for example, EPN Manager Maintenance Pack 4 Patch.

f. Install the patch on the secondary server clicking its associated **Install** button. The secondary server will auto-restart and will not be accessible for a few minutes. After successful installation, the status will change to "Installed".

Step 4 Verify the installation on the secondary server:

a. Run the **ncs status** command and verify that the secondary server's processes are up and running.

b. Log into the secondary server's HM page. The status of the secondary server should be **Secondary Syncing**.

c. Verify that the patch is listed as "Installed" in the Software Update page of the secondary server.

Step 5 On the primary server, download and install the patch. Follow **Steps 1 to 4** in Download and Install a Patch (No HA). The primary server restarts automatically and the GUI will not be accessible for some time.

Step 6 Verify the installation on the primary server:

a. Run the **ncs status** command and verify that the primary server's processes are up and running.

b. Run the **ncs ha status** command and check that the status of the primary server is **Primary Active**.

Once all the processes on the primary server are up and running, HA registration is automatically triggered between the secondary and primary servers (and an email is sent to the registered email addresses). This usually completes after a few minutes.

Step 7 Verify that the patch is listed as Installed in the Software Update page of the primary server.

Step 8 Check that the version of the Point Patch is listed correctly in the Login, About and Software Update pages in the Cisco EPN Manager GUI.

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 2.0 MP1, see the *Cisco Evolved Programmable Network Manager 2.0 MP1 Documentation Overview*. The documentation overview also lists several Cisco Prime Infrastructure documents because the content of those documents is relevant to Cisco EPN Manager 2.0 MP1.

Accessibility Features in Cisco EPN Manager 2.0 MP1

For a list of accessibility features in Cisco EPN Manager 2.0 MP1, see the Voluntary Product Accessibility Template (VPAT) on the Cisco website, or 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.

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.