



Cisco Evolved Programmable Network Manager 2.0 Release Notes

First Published: May 3, 2016

Last Modified: October 10, 2016

This document provides information about Cisco Evolved Programmable Network Manager (Cisco EPN Manager) 2.0. It outlines the additional feature and device support available in Cisco EPN Manager 2.0 and provides a list of open bugs in Cisco EPN Manager 2.0.



Note

This document also provides information about the mandatory point patches—Cisco EPN Manager 2.0 (0.1.0) and Cisco EPN Manager 2.0 (0.2.0)—that must be installed on top of Cisco EPN Manager 2.0.

Contents

These release notes contain the following sections:

- [Functionality Added in Cisco EPN Manager 2.0](#)
- [Additional Device/Module/OS Support in Cisco EPN Manager 2.0](#)
- [Content of Mandatory Point Patches](#)
- [Installing Cisco EPN Manager 2.0 and Point Patches](#)
- [Cisco EPN Manager Bugs](#)
- [Related Documentation](#)
- [Accessibility Features in Cisco EPN Manager 2.0](#)



Functionality Added in Cisco EPN Manager 2.0

Circuit Emulation (CEM) Service Provisioning and Management (Beta Features)

- Structure-agnostic time-division multiplexing (TDM) over packet (SAToP) mode.
- Creation and provisioning of CEM services on Cisco ASR 903, Cisco ASR 907, and Cisco NCS42xx devices.
- Routing CEM services through MPLS TE tunnel.
- Support for unidirectional path switched ring (UPSR) and Automatic Protection Switching (APS) protection mechanisms.

MPLS Traffic Engineering Service Provisioning and Management (Beta Features)

- Bidirectional TE tunnel and Layer 3 link creation (co-routed tunnels only).
- Support for creating MPLS TE service on Cisco NCS 4206 and Cisco NCS 4216 devices.
- Support for constraint-based routing and trunk admission control.
- Ability to choose the protection mechanism against link and node failures when provisioning an MPLS TE service.
- Usage of Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP).
- Ability to advertise TE links using OSPF.

L3VPN Provisioning and Management:

- Ability to add VRFs and create and provision L3VPN services.
- Deletion of endpoints associated with an L3VPN service.
- Activation and deactivation of L3VPN services.
- View/hide service states during service deployment.

Optical Circuit Provisioning and Management

- Ability to initiate protection switch action on Optical circuits
- Ability to view circuit history, meaning all versions of the circuit up to the current version, and compare two versions of an optical circuit.

Carrier Ethernet Provisioning and Management

- Support for EVC provisioning over bidirectional TE tunnels.
- When deleting an EVC in “failed” state, you can choose whether to remove configurations from devices only or from the database as well.

Multilayer Trace View Enhancements

- Cisco EPN Manager now supports multilayer trace view for additional point-to-point services, including CE, CEM (beta), and MPLS TE (beta) services.
- Three-dimensional view of a circuit/VC trace.
- Support for viewing partial circuits where one or more devices participating in the circuit is not part of your virtual domain.
- Display of port state icons in the circuit/VC trace.

Inventory

- Chassis View enhancements—Enhanced view for multi-rack devices, where each rack is displayed in a separate tab; ability to select an interface and launch the configuration UI from the Chassis View; ability to change the Chassis View refresh interval and enable/disable blinking icons
- Support for topology-based discovery for optical devices (includes ability to discover optical devices using a seed device IP address)
- Improved inventory collection—Enhanced logic for determining what information to collect after an incoming event signals a change (using a combination of expedited events, reactive inventory, and granular polling mechanisms)
- Network device states—Ability to move a device in and out of maintenance mode

Configuration

- Interface configuration—Can be launched from Chassis View
- Configuration templates using the wizard—Simplifies configuration template deployment with new enhanced workflow
- Device configuration to enable CEM provisioning—Configuration of Cisco NCS42xx devices with CEM by first setting appropriate controller modes for the interfaces and then configuring the PHD (E1, T1, E3, and T3), SONET, and SDH controllers for CEM interfaces. ASR and UPSR configuration support is also available.
- QoS support—QoS profiles can now permit packets based on the selected QoS group for Cisco NCS 4000 and 42xx devices.
- Ability to configure H-QoS to specify QoS behavior at multiple levels of hierarchy for Cisco NCS 4000 and 42xx devices.
- Clocking—Support for frequency synchronization using Sync-E and BITS.
- Connection Verification—Support for verifying the connection to Cisco NCS 2000 devices and setting the acknowledgment values for associated alarms.
- OSC—Configure OSC terminations on OC3 lines, and on FastEthernet (FSTE) and GigabitEthernet (GigE) interfaces. Supported cards are TNCS, TNCE, and TNC. For ONS15454 NEs, the supported interfaces are OC3 interfaces of OSCM and OSC-CSM cards.
- Squelch and GCC—Configuration support on Cisco NCS 2000 devices.
- Packet termination and PRBS—Configuration support for ODU controllers of Cisco NCS 4000 devices.
- OSPF—Support for configuring OSPF routing protocol for OTU controllers of Cisco NCS42xx and Cisco NCS4000 devices.
- Ethernet over ODU—Support for configuring UNI ports mode to Ethernet packets for Cisco NCS 4000 devices.
- Breakout—Configuration support on Cisco NCS 4000 devices.
- GMPLS and LMP—Configuration support on Cisco NCS 2000 and Cisco NCS 4000 devices.
- Configure Performance Monitoring—Enable performance monitoring on Cisco NCS 2000 and Cisco NCS 4000 devices.
- NNI—Support for configuring OTU controllers to act as NNIs.
- OTN Topology—Configure the topology instance and Area ID associated with optical OTN controllers.

- Channelize ODU (LO) Controllers—Configure ODU controllers with multiple lower order ODU sub-controllers and configure TPN and TS for the sub-controllers.
- TCM, TTI, and Protection Profiles—Configuration support on Cisco NCS 4000 devices.
- Ethernet MTU—Configure MTU values for optical device’s Ethernet interfaces except Gigabit Ethernet and Fast Ethernet interfaces on TNC and ECU modules.
- FEC mode—Support for enabling standard FEC mode on OTN interfaces.

MTOSI

- Service Inventory Retrieval (MSI)
 - Network Interface (UNI/ENNI) Retrieval
- Resource Provisioning (RP)
 - setTP for NNI Controller configuration
 - Cisco Config Activation - MBC
- Service Provisioning Updates (SAI)
 - Diversity Provisioning (OCH Trail-UNI)
 - Error Handling improvement

RESTCONF/YANG API

- Support for physical inventory retrieval. See the [RESTCONF NBI Guide](#) for information on how to obtain the YANG schema for objects supported by this interface

Administration

- Licensing—Support for Cisco Smart Licensing (along with traditional licensing)
- Jobs Dashboard—Enhanced for easier navigation
- Improved security for server connectivity—Enhanced instructions for security server connectivity using HTTPS and certificate mechanisms
- New System Monitoring Dashboard—Customizable dashboard that provides a quick view of server health (system CPU, memory, and kernel information; utilization statistics; job and backup information; API and service information)
- External authentication—Support for Cisco ISE 2.x and TACACS+
- Alarm customization
 - Ability to configure alarm auto-clear interval
 - Ability to customize the information displayed in the Failure Source column of the web GUI
- Software Image Management server—Ability to add this server using the web GUI

GUI

- Menu customization—Ability to disable portions of the web GUI which are not used
- Home page/landing page—Ability to customize this page
- Ability to view a table listing all links in the system (Inventory > Other).
- Ability to view a table listing all network interfaces (UNIs, ENNIs, INNIs) and all circuits/VCS in the system (Inventory > Other).

Compliance Audit:

- Ability to duplicate policies during policy creation.
- Eight new user-defined example policies can now be used as reference for creating new policies.
- New policy groups are now supported for the platform for WLC wireless devices.
- Support extended for auditing AireOS Wireless LAN Controllers.

Circuit/VC Provisioning and Management (Optical and CE)

Performance

- Support for Pseudo Random Binary Sequence (PRBS) performance test for OTN Circuits of the type ODU UNI.
- Support for OTDR performance test to diagnose OTS link related issues on NCS 2000 devices.
- New performance counters, monitoring policy (TDM/Sonet), and performance charts for monitoring CEM services.
- Support for performance monitoring on ODU controllers - Tandem Connection Monitoring (TCI).
- Support for Bit Error Rate (BER) performance test on Cisco NCS 42xx devices.
- Additional QoS dashlets available under the Service Performance dashboard.
 - QoS Top N Drop Rate Table
 - QoS Top N Pre-Policy Rate Table
 - QoS Top N Post-Policy Rate Table
 - QoS Policy Class Map Traffic Graph
 - QoS Policy Class Map Traffic Table
- Additional Y.1731 dashlets available under the Service Performance dashboard:
 - Y.1731 Top N One-Way Jitter
 - Y.1731 Top N Two-Way Delay
 - Y.1731 One-Way Jitter Graph
 - Y.1731 Delay Graph
 - Y.1731 Frame Loss Graph
 - Y.1731 Top N Frame Loss Table
 - Y.1731 Probe Statistics Table
 - Y.1731 Probe Details Table

Topology

- Graphical visualization of optical link bandwidth utilization on the topology map and representation in link tables and link details. Bandwidth utilization visualization is supported for OTU, ODU, and OTS links.
- Additional functionality in geo map toolbar.
- New layout of the Topology window to improve user experience.
- Legend provided to identify map components.
- Geo Map—Ability to enter GPS coordinates in all available formats (DMM, DD, or DMS).
- Predefined background images provided for topology map.

- Ability to export data from Circuits/VCs and Network Interfaces tables.
- New Link 360 view—Provides quick, detailed information about a specific device link (performance, end points, circuits/VCs, and so forth)

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

This section lists the new support provided in Cisco EPN Manager 2.0. 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

Cisco NCS 2000—New Operating System Support

Device Model	Device OS
Cisco NCS 2002	ONS 10.5.1, 10.5.11, 10.5.2
Cisco NCS 2006	
Cisco NCS 2015	

Cisco NCS 4000 Network Convergence Systems—New Operating System Support

Device Model	Device OS
Cisco NCS 4009	IOS-XR 5.2.41, 5.2.42, 5.2.43, 5.2.44, 5.2.47
Cisco NCS 4016	

Cisco ASR 9000 Aggregation Services Routers—New Operating System Support

Device Model	Device OS
Cisco ASR 9001	IOS XR 5.3.2
Cisco ASR 9904	
Cisco ASR 9006	
Cisco ASR 9010	
Cisco ASR 9912	
Cisco ASR 9922	

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 Mandatory Point Patches

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

- Point patch 1 (PP1)—Cisco EPN Manager 2.0 (0.1.0)
- Point patch 2 (PP2)—Cisco EPN Manager 2.0 (0.2.0)


Note

PP2 includes the content of both patches. Therefore, if you have not yet installed PP1, you can go directly to PP2.

PP1 Content

Cisco EPN Manager 2.0 (0.1.0) addresses the following issues:

Identifier	Symptom
CSCuz27358	NCS4k distribute with activate ISSU fails
CSCuz13683	Export Configuration file not working well on confluence
CSCuz32636	WSON settings not upgraded after upgrade from 01.02(500) to 02.00
CSCuz32918	Sometimes historical Overlay not saved, upgrade from 01.02(500) to 02.00
CSCuz31182	ODU UNI provisioning fails.
CSCuz08976	ASR9k Inventory collection fails due to exception on L3VPN after Upgrade
CSCuz04136	getRoute and TL not working
CSCuz29738	ProtocolEndpoint attributes changed to default value during reactive inventory.
CSCuw08728	Incorrect state is show after Granular Inventory execution.
CSCuz36858	Y1731 filter & dashlets ignore different CoS on probes.
CSCuz32737	OCHTRAIL-UNI remains in partial after provisioning (OCHNC with PSLINE).
CSCuz32881	Edit OCHTRAIL in regen with different lambda isn't permitted.
CSCuz40032	Alarms raised pre-upgrade are not cleared after upgrade

PP2 Content

Cisco EPN Manager 2.0 (0.2.0) addresses the following issues:

Identifier	Symptom
CSCuz39530	Exception creating the second OCHCC circuit on MXP configuration.
CSCuz55737	ERROR 500 received when editing a discovered OCHCC circuit in MXP configuration that had previously been deleted.
CSCuy76886	ODU UNI missing after creation of OTN circuit.
CSCuz43537	Collection failure when syncing nodes after circuit creation in MXP configuration.

Identifier	Symptom
CSCuz71840	DWDM circuit provisioned with more than one constraint remains inactive.
CSCuy17949	EPNM does not filter ports used in service intent.
CSCuz12225	Link 360 Utilization reports wrong channels number.
CSCuz79819	Deploy Failure page is not opened when create/modify/delete circuit fails.
CSCuz79861	Provisioning - Popup not shown when a job is scheduled for deploy.
CSCuz79836	No error message shown in wizard when TL1 DENY is returned by the NE.
CSCux82101	ODU UNI circuit creation caused a failure message even though it was successful.

For patch installation instructions, refer to [Download and Install a Patch \(No HA\)](#) or [Download and Install a Patch \(HA Deployment\)](#).

Installing Cisco EPN Manager 2.0 and Point Patches

Cisco EPN Manager 2.0 Point Patch 2 is a required patch for Cisco EPN Manager 2.0. The installation flow is as follows:

1. Install Cisco EPN Manager 2.0. See the [Cisco Evolved Programmable Network Manager 2.0 Installation Guide](#). The installation guide provides instructions for installing the product in both standard and high availability environments. It also provides instructions for upgrading from a previous version to Cisco EPN Manager 2.0.
2. Install Point Patch 2—Cisco EPN Manager 2.0 (0.2.0). PP2 includes all the content of the previously-released PP1. If you already have PP1 installed, you must install PP2 on top of it.
 - To install PP2 in an environment with no high availability, see [Download and Install a Patch \(No HA\)](#).
 - To install PP2 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.

Download and Install a Patch (No HA)

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

-
- Step 1** Log into Cisco EPN Manager web GUI 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. The file will have the prefix **cepnm2.0-pp2** and the suffix **.ubf** (be sure to check the description).
- 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 and patches.
 - 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 client machine.
 - Click the blue **Upload** link at the top of the Software Update page in the web GUI, browse to the ubf file on your client machine, 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** Click the **Install** button associated with the patch under Add-Ons on the Software Update page. Click Yes in the confirmation message pop-up window to proceed with the installation. After successful installation, the status will change to **Installed**.
- Step 5** Cisco EPN Manager will auto-restart and the Cisco EPN Manager web GUI will not be accessible for some time.
- Step 6** Check the status of the services.
- a. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
 - b. Run the **ncs status** command to ensure that all services are up and running:


```
(admin)# ncs status
```
- Step 7** Log into the Cisco EPN Manager web GUI and verify that the GUI is accessible and the version is updated on the Software Update page.

Download and Install a Patch (HA Deployment)

Follow these steps to install a point patch on top of Cisco EPN Manager 2.0 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 patch on the secondary server.

-
- Step 1** Check the HA status on the primary server.
- Log into the web GUI on the primary server as a user with Administrator privileges.
 - From the left sidebar, choose **Administration > Settings > High Availability**.
 - In the HA Status page, confirm that the primary server's state is **Primary Active**.
 - Click HA Configuration and confirm that the Configuration Mode is **HA Enabled**.
- Step 2** Check the HA status on the secondary server.
- 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.
 - Enter the authentication key and click **Login**.
 - Verify that the Current State Mode is **Secondary Syncing**.
- Step 3** On the secondary server, download and install the patch.
- 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.
 - Enter the authentication key and click **Login**.
 - Click **Software Download** at the top right of the Health Monitor window to open the Secondary Server Software Update window.
 - Enter the authentication key and click **Login**.
 - 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.
 - Install the patch on the secondary server by clicking its associated **Install** button. The secondary server will auto-restart and will not be accessible for a few minutes. Click **Yes** in the confirmation pop-up window to proceed with the installation. After successful installation, the status will change to **Installed**.
- Step 4** Verify the installation on the secondary server.
- Check the status of the services.
 - Start an SSH session with the secondary server and log in as the Cisco EPN Manager CLI admin user.
 - Run the ncs status command to ensure that all services are up and running.

```
(admin)# ncs status
```
 - Log into the secondary server's HM page and verify that its status is **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 \(No HA\)](#). After installation, the primary server restarts automatically and the web GUI will not be accessible for some time.
- Step 6** Verify the installation on the primary server:
- a. Check the status of the services.
 - Start an SSH session with the primary server and log in as the Cisco EPN Manager CLI admin user.
 - Run the `ncs status` command to ensure that all services are up and running.


```
(admin)# ncs status
```
 - b. Verify that the status of the primary server is **Primary Active** using the following command:


```
(admin)# ncs ha status
```
 - c.

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** On the primary server, verify that the web GUI is accessible and the version is updated on the Software Update page.
-

Cisco EPN Manager Bugs

- [Get Information About Cisco EPN Manager Bugs](#)
- [Related Documentation](#)

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

Open Bugs in Cisco EPN Manager 2.0

The following tables list all open bugs (severity 1, 2 and high priority severity 3 bugs), categorized by type. The tables also include all open customer-found bugs. Click on the bug identifier link to get more information about the bug.

- [HA Bugs](#)
- [Topology Bugs](#)
- [Compliance Audit Bugs](#)
- [Inventory Bugs—Optical](#)
- [Inventory Bugs—Carrier Ethernet](#)
- [Device Configuration Bugs](#)
- [Provisioning/Discovery Bugs](#)
- [Multilayer Trace Bugs](#)
- [Performance Monitoring Bugs](#)
- [Fault Management Bugs](#)
- [Reports Bugs](#)
- [Base User Interface Bugs](#)
- [Chassis View Bugs](#)
- [Admin Bugs](#)

HA Bugs

Identifier	Severity	Symptom
CSCuz13694	3	Failback is rolled back when the primary server is kept as standby (Primary syncing) for more than 16 hours.
CSCuz22966	3	EPNM HM does not detect Matlab process start failures in support of HA.

Topology Bugs

Identifier	Severity	Symptom
CSCuz34306	3	Bandwidth utilization does not work after upgrade.
CSCuu36566	3	Topology map missing satellite link when LC OIR performed.

Compliance Audit Bugs

Identifier	Severity	Symptom
CSCuz34135	3	Compliance engine in stopped state post upgrade.
CSCuw13387 (bug on Beta feature)	3	Scale: CA for 30 System and 5 Show command policy took 6 hours-34 mins.

Inventory Bugs—Optical

Identifier	Severity	Symptom
CSCus35437	3	Inventory collection fails with 2.11.x version of PhysicalPEP XDE.
CSCuz33497	4	Job Dashboard poorly identifies NE SW "Import" job in User Jobs list.
CSCuz12552	3	Admin state not update on a lot of ports on XC adminState change.
CSCuy97740	3	Missing XC between Trunk ports on ARXP regen.
CSCuy94211	3	Parent tributary slots not displayed for ODU device 360 ->interface 360.
CSCuz38332	2	50% of NCS4Ks in collection failure after SW non-ISSU and FPD upgrades.
CSCuy53318	3	NCS2K location info missing in Alarm Information pane.
CSCuy29898	3	NCS2K: FC/FICON inventory page throwing exception after payload change.
CSCuv08687	3	Inventory collection for 5K devices takes 8 hrs.
CSCuv39546	3	Circuit discovery for 5k optical devices takes a few days.
CSCuw20950	3	Incorrect i/f speed displayed in Interfaces 360 for optical interfaces.

Inventory Bugs—Carrier Ethernet

Identifier	Severity	Symptom
CSCuz18899	3	Scale: Sync didn't consider PCF and SNMP Connectivity failed devices.
CSCuz39882	3	Device deletion did not remove recovered clock configuration from EPNM db.
CSCuz34668	3	Device deletion takes more than half an hour.

Identifier	Severity	Symptom
CSCuz34324 (bug on Beta feature)	2	EMS entity gets deleted once device sync is done.
CSCux50711	2	ASR907: Device inventory returns FAN details in power modules section.
CSCux37523	3	OSPF inventory needs to include Interfaces that are DOWN as well.
CSCuv37219	3	ME1200: Wrong port name shown for Ethernet interface.
CSCuv37315	3	Power supply and module information missing for ME1200.
CSCuv37325	3	ME1200: Version ID shows N/A in UDI in Device Summary page.
CSCuv37407	3	ME1200: Software Version shows blank in Device and Summary page.
CSCuu89816	3	Collection failure on ASR9K after re-inserting card.

Device Configuration Bugs

Identifier	Severity	Symptom
CSCux33392	3	NCS4K-OSPF: Router-ID not populating in EPNM.
CSCuz34395	3	OTDR Error when there are no OTDR scan data.
CSCuz20379	3	Add/Update operation fails when field attribute is left blank.
CSCuz27046	3	Newly created CFM Domain Entries not displayed in UI.
CSCuz26953	3	BGP neighbor configuration is not working properly on IOS-XR devices.
CSCuz26489	3	BGP neighbor without address family failed with internal server 500 error.
CSCuz22626	3	CEM controllers are listing under T3- channelized t1/e1 in the GUI.
CSCuz22194	3	SyncE Bits entries are deleted when deleting SyncE global config.
CSCuy41252	3	Error activating/deactivating interface from Interface 360 when launched from Device 360.
CSCuy33981	3	Error activating/deactivating interface from Interface 360.
CSCuv99804	3	Updating MEP is successful in the UI but fails to push onto the device.
CSCuw15591	3	No OSPF configuration generated for IOS devices after save.

Provisioning/Discovery Bugs

Identifier	Severity	Symptom
CSCuz34774	2	ASR 903 and 907 devices with RSP3 do not support split horizon group ID. A command is accepted without an ID and the system uses the default one.
CSCuz04156	3	EthernetP2PForwarder isn't modeled for IOS xconnect context.
CSCuy78788	3	Unable to provision a service with same MEP ID for source and destination.
CSCuz00699	3	CC Interval, P2P, CC Group values set to zero/blank after device resync.

Identifier	Severity	Symptom
CSCuz39530	3	Exception creating the 2nd OCHCC on MXP configuration.
CSCuz26731	3	Discovery partial of Ycable nn wson circuit.
CSCuz24929	3	With wson upgrade/release, CEPNM isn't updated correctly.
CSCuz12788	3	Sometimes node constraints are not discovered.
CSCuz06763	3	Circuit 360 view shows wrong endpoint for OCHCC nn wson 100g payload.
CSCuz06399	3	CEPNM discovers some OCHCC like partial, if index on payload missing.
CSCuz01031	3	ODU UNI Circuit does not include midpoint node in CTPs table.
CSCuy89794	3	Edit circuit name of OCHCC on AGGR port, circuit goes in partial.
CSCuy85198	3	OCHTRAIL UNI provisioned remains Partial in EPNM.
CSCuz37991	3	Admin/Oper states are missing for Interface 360 view accessed from Circuit 360 view.
CSCuz14888	3	'Circuits/VCS' tab in Link 360 for physical link in FlexLSP MLT is empty.
CSCuz31906	3	Unable to add a new Customer to the Customers table after upgrade.
CSCuz15013	3	"Javascript Warning Message" dialog in circuit CREATE, ENDPOINTS context.
CSCuy38099	3	UI: Drools rules engine executed twice on expanding picker single widget.
CSCuy38562	3	L3 Link Circuits/VC page - Discovery state should be N/A, Serviceability state and Last modified time should be shown correctly.
CSCuz32391	3	Both endpoints are not showing in delete endpoint when created 1 vrf and 2 UNIs.
CSCuz18069	3	Association between VRF and Protocolendpoint is not populating.
CSCuz33056	3	Partial OCH-Trail UNI circuit discovered.
CSCuz29710 (bug on Beta feature)	3	T1 service delete shows empty preview if deleted after more than two hours.
CSCuy15261	3	Payload value range is not constant on device NCS4206-120.32.
CSCux16634	3	Scale: Very High CPU utilization observed during inventory collecti.on for 2500 devices.
CSCux06835	3	Decommission of service when service is failed.
CSCuw76013	3	Promote: when a circuit is not promotable wizard should be closed.
CSCuv81939	3	Long service discovery time in scale setup.
CSCuv65022	3	UNI Name with / - and other unsupported chars causes deployment failure.
CSCuv02668	3	Scale - Few Optical Circuits not discovered when bulk imported.
CSCut84114	3	EFP is not removed on RFS graph for sub-interface removal on bridge.
CSCuy86433	4	Parsing error messages observed when using the ODU UNI circuit creation wizard.
CSCux47473	4	Failed deletion of OCH-Trail UNI due to related SSHv2 connection failure.

Identifier	Severity	Symptom
CSCUw92073	4	Creating OCHNC circuit endpoints does not relate to the passive module ports.
CSCUy20041	3	Duplicated ODU UNI after modifying Service Type from CTC/CLI.
CSCUy45436	3	Preview service exception: failed to save.
CSCUy53019	3	Protected FREQ & ISMANDATORYFREQ parameter set during ENT commands.
CSCUy30057	3	Errors in SD log for “EFPEndpoints”.
CSCUx42301	3	Circuit still present in the Circuit Table after being deleted from NEs.
CSCUw90145	3	OCHTRAIL UNI: Modify button from circuit details does not work.
CSCUw93931	3	OCHNC of the related OCH TRAIL takes 1 hour to be deleted in CEPNM.
CSCUw31796	3	Deletion of a failed ENNI says successful for first delete but the ENNI is still displayed. Second deletion fails with the 500 server error.
CSCUv75637	3	When service deployment fails, the ports selected in failed service creation are not available when recreating the service.
CSCUw81297	3	The WLC devices are not filtered out in Provisioning wizard.
CSCUw81351	3	The AP devices are not filtered out in Provisioning wizard.
CSCUv48707	3	Special character causes EVPL delete failure.
CSCUv31149	3	When an E-LAN service is created using a profile, first service creation will be successful. But the creation of second service using the same profile will fail.
CSCUu39128	3	Deployment fails when modifying MTU in EVPL service.
CSCUt97450	3	During service modification on ME3600 devices, only the description of service was changed but additional incorrect commands were generated.
CSCUt13928	3	EVP-LAN with VLAN-preservation off - incorrect configuration commands are generated, i.e, no pop-1 under service instance at UNI.
CSCUv03190	3	Circuit OCHCC not discovered in case it starts from AR-MXP card in MXP_S mode.
CSCUw33919	3	After device deletion, some L3VPN circuits remain in the system although they no longer exist and should have been removed.
CSCUv93420	3	While provisioning DWDM / OTN circuits, error parsing exceptions are observed. Also, the device picker of Endpoints table is not loaded with the Device list on the first click of the picker.
CSCUt18497	3	OAM Fault Management Map UI issues.
CSCUt10285	3	Duplicate versions of the same service are created.
CSCUw92076	3	OCHNC circuit creation add and drop endpoints are given different labels.
CSCUw90710	3	When creating a ODU UNI circuit from EPNM, the circuit creation fails.
CSCUu62960	3	Server Error 500 shown when editing optical circuit.
CSCUw19438	3	When a circuit using a tunnel ID is edited, a new tunnel ID is assigned and a new tunnel is created in the network.
CSCUs95253	3	Splitter protected circuit fails if required/preferred lambda is entered.

Identifier	Severity	Symptom
CSCut42624	3	Missing relations between objects in DB.
CSCux47468	4	Failed deletion of OCH-Trail UNI due to related SSHv2 connection failure.

Multilayer Trace Bugs

Identifier	Severity	Symptom
CSCuz31048 (bug on Beta feature)		Multilayer trace result for MPLS TE service is wrong when active & standby routes are not overlapping.
CSCuz31692 (bug on Beta feature)	3	Routes provider returns empty result for MPLS TE service in multilayer trace.
CSCus63907	3	Multilayer trace of OCHNC PSM protect does not show protect path.

Performance Monitoring Bugs

Identifier	Severity	Symptom
CSCuz36812	3	Nexus 77K - Interface stats not collected.
CSCuz29560	3	Collection of stats starts after 7 hours.
CSCux92503	3	360 Perf Test does not retrieve optical performance data from the NCS 2K.

Fault Management Bugs

Identifier	Severity	Symptom
CSCuz09929	3	Default timestamp filters are defined by the EPNM timestamp and not the device timestamp.
CSCuz08633	3	Upgrade: Failure Source pattern table keeps loading in a scenario.
CSCuy76141	3	Upgrade: Device timestamp field missing in alarms/events/cleared alarms page.
CSCus50235	3	Outstanding alarms at link level not shown on map.
CSCuy35988	3	Upgrade: Alarm categories enabled for email got disabled after upgrade.
CSCuz09924	4	Device Timestamp and Status Quick Filter field required reset for usage.
CSCux75310	4	Some event message details are obstructed in EPNM Events detail window.
CSCuw80244	4	The "Filter" Icon in Alarms and Events does not function as expected.
CSCuy86411	3	Event window update takes too long when scrolling.
CSCuy40958	3	Nullpointerexception fetching alarm summary API.
CSCuy58215	3	Values not populated for timestamp field in Syslogs Tab.

Reports Bugs

Identifier	Severity	Symptom
CSCuy31141	3	On saving customized Ethernet 2K report, JDBC error is reported.

Base User Interface Bugs

Identifier	Severity	Symptom
CSCuz12225	3	In the Link 360 panel, the parameter Utilization reports the wrong number of channels.
CSCuw29637	3	Job_Bulk import is not showing device status in IE.

Chassis View Bugs

Identifier	Severity	Symptom
CSCuz35437 (bug on Beta feature)	2	NCS4206 chassis view is not displayed.

Admin Bugs

Identifier	Severity	Symptom
CSCuy01292	3	Unable to create System monitor user.

Resolved Bugs

The following table lists the bugs that appeared in the release notes for Cisco EPN Manager MP5 and have since been resolved.

Identifier	Severity	Symptom
CSCuy30133	3	OCHTrail UNI: ERO constraints not aligned after circuit promotion.
CSCuy15467	3	DWDM circuits: Restoration shown with old value.
CSCuy26998	3	Multilayer Trace only shows single point (Rx or Tx) after DWDM circuit edit.
CSCuy27193	3	OCHTRAIL UNI full discovered when OCHNC is missing or unavailable.
CSCuy29463	3	MBCProxy log statements should go in config.log.
CSCuw87623	3	NCS2k: restore job is a success but no inventory collection is triggered.
CSCuy29942	3	Serviceability, op state, admin state wrong for ODU UNI.

Identifier	Severity	Symptom
CSCux12867	3	Preferred/Mandatory settings do not take effect from DWDM wizard.
CSCuw94158	3	Operational status cannot be retrieved for services (ONS, NCS2K).
CSCuy51158	3	Inconsistent representation of OCHCC YCable after provisioning from EPNM.
CSCuy98034	3	Scale: LAG8023AD is discovered as InterfaceProtocolIEP.
CSCuy41466	3	Intermittent error executing XFT.
CSCuv09612	3	Misalignment in case of OCHTRAIL UNI name edit from CTC.
CSCux97475	3	Tunnel down promoting an OCHTRAIL-UNI with XRO.
CSCuy31571	3	OCHCC in Discovery Status Missing after Activation.
CSCuy05057	4	Upgrade Analysis Report fail due to unknown reason in ASR9XX.
CSCux12870	3	Service Discovery takes much time and there also pauses in the process.
CSCuw55409	3	Creation of CFM service is not behaving as expected on ASR903.
CSCux63448	3	Admin status not updated after deactivating an ODU UNI.
CSCuy19269	3	L3 link creation message should be removed from VLAN field help.
CSCuw96169	3	Incorrect status of historical versions of circuit in circuit 360 History tab.
CSCuy48620	3	ONBI Explicit path is not getting discovered and not returning circuit details.
CSCuy49179	3	OCHTRAIL-UNI: missed constraint of circuit created with other tool.
CSCuy50305	3	Error on valid Purging period for 'Delete all events after' field.
CSCuy50331	3	Tooltips shown in 360 shouldn't contain HTML tags and special symbols.
CSCuy50333	3	Event list vanishes Sorting over Correlated column.
CSCuw85518	3	Sorting by "Admin Status" or "Op. Status" shows wrong and unsorted list.
CSCuy23368	3	Serviceability not updated when OCHTRAIL server is shut down.
CSCuw59170	3	Error 500 displayed immediately after profile is created or edited.

Related Documentation

For a list of all documentation available for Cisco EPN Manager 2.0, see the [Cisco Evolved Programmable Network Manager 2.0 Documentation Guide](#). The documentation guide also lists several Cisco Prime Infrastructure documents because the content of those documents are relevant to Cisco EPN Manager 2.0.

Accessibility Features in Cisco EPN Manager 2.0

For a list of accessibility features in Cisco EPN Manager 2.0, 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.

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.

© 2016 Cisco Systems, Inc. All rights reserved.