Cisco Evolved Programmable Network Manager 7.1.1 Release Notes

First Published: 2023-12-18

Introduction

This document contains the following information about Cisco Evolved Programmable Network Manager 7.1.1:

New Functionality Added

This section lists the new features/functionalities delivered in Cisco EPN Manager 7.1.1.

Device Support

- Support for IOS-XR 7.10.2 release on Cisco NCS 560 devices
- Support for IOS-XR 7.10.2 release on Cisco ASR 9000 routers
- Support for IOS-XR 7.10.2 release on Cisco 8000 series devices
- Support for IOS-XR 7.10.2 release on Cisco NCS 5500 devices

- Support for IOS-XR 7.10.2 release on Cisco NCS 5700 devices
- Support for IOS-XR 7.11.1 release on Cisco ASR 9000 64-Bit routers
- Support for IOS-XR 7.11.1 release on Cisco NCS 560 devices
- Support for IOS-XR 7.11.1 release on Cisco NCS 5500 devices
- Support for IOS-XR 7.11.1 release on Cisco NCS 5700 devices
- Support for IOS-XR 7.11.1 release on Cisco NCS 540 devices
- Support for IOS-XR 7.11.1 release on Cisco 8000 series devices
- Support for Chassis View on Cisco 8804 Devices
- Support for Cisco 8804 devices with IOS-XR 7.8.2
- Support for Chassis View on Cisco NC57-48Q2D-S and Cisco NC57-48Q2D-SE-S line cards with IOS-XR 7.10.2
- Support for IOS XR 7.9.1 release on Cisco IOS XRv 9000 routers
- Support for IOS-XR 7.11.1 release on Cisco 8011-2X2XP4L with 10G PLE-NID
- Support for Chassis View on Chassis 8608-SYS on Cisco 8000 series routers
- Support for IOS-XR 7.10.2 release on Cisco 8111-32EH
- Support for Chassis View on Cisco 8111-32EH
- Advantage/Full RTM support for PID 8608-SYS with IOS-XR 7.10.2 on Cisco 8000 series devices
- Support for Chassis View on 10G PLE-NID and Cisco 8011-2X2XP4L on IOS-XR 7.11.1 release
- Validation of IOS-XE 17.12.1 release on Cisco NCS 4200 and Cisco ASR 900 devices
- Support for Cisco N520-X-4G4Z-A and Cisco N520-X-4G4Z-D devices on IOS-XE 17.12.1 release
- Support for IOS-XR 7.10.2 release on Cisco NCS 540 series routers
- Support for Cisco NCS 2000 series 11.1.3.1 release

Optical

- Discovery of Optical Channel (OCH-CC) circuits involving Cisco NCS 2000 series devices (IOS-XR 11.1.31) equipped with ROADM functionality, while also ensuring NBI support for Cisco NCS 1004 devices with (IOS-XR 7.10.1)

Note For ODU-UNI, ODU, and OCHCC circuit types, multi layer traceroute terminates at the endpoints. Multilayer Trace route will not extend beyond the endpoints of the circuit. This is added as part of bug CSCwh63552.

Note Before upgrading FPD on Cisco NCS 1004 devices, ensure that the trunk ports remain in an operational state (un-shut) with the description, particularly in cases where LMP and GMPLS configurations are present.

- Support for DP04QSDD-HE0 optical module for Cisco 8202-32FH-M, Cisco 88-LCO-34H14FH, and Chassis 8608-SYS devices with IOS-XR 7.10.2 release
- Support for DP04QSDD-HE0 optical module for PIDS (that support Coherent Optics) of Cisco NCS 5500 and Cisco NCS 5700 devices with IOS-XR 7.8.2 release
- Support for DP04QSDD-HE0 optical module for Cisco N540-24Q8L2DD-SYS with IOS-XR 7.8.2 release
- Support for DP04QSDD-HE0 optical module for Cisco A9K-20HG-FLEX and Cisco A9K-8HG-FLEX-SE/TR devices with IOS-XR 7.8.2 release
- Support for DP04QSDD-HE0 optical module for Cisco 88-LC0-36FH, Cisco 8201-32FH, and Cisco 8201-24H8FH devices with IOS-XR 7.8.2 release
- Support for DP04QSDD-HE0 optical module for Cisco 88-LC0-36FH-M with IOS-XR 7.8.2 release
- Support for DP04QSDD-HE0 optical module for Cisco A99-10x400GE-X-SE/TR, Cisco A9K-8HG-FLEX-SE/TR, Cisco A9903-20HG-PEC, and Cisco A9903-20HG-PEC-FC with IOS-XR 7.8.2 release
- Support for DP04QSDD-HE0 optical module for Cisco A99-10x400GE-X-SE/TR, Cisco A9K-8HG-FLEX-SE/TR, Cisco A9903-20HG-PEC, and Cisco A9903-20HG-PEC-FC devices with IOS-XR 7.10.2 release
- Support for DP04QSDD-HE0 optical module for Cisco N540-24Q8L2DD-SYS with IOS-XR 7.10.2 release
- Support for DP04QSDD-HE0 optical module for PIDS (that support Coherent Optics) of Cisco NCS 5500 and Cisco NCS 5700 devices with IOS-XR 7.10.2 release
- Support for DP04QSDD-HE0 optical module for Cisco 88-LC0-36FH-M device with IOS-XR 7.11.1 release
- Support for DP04QSDD-HE0 optical module for Cisco 8202-32FH-M, Cisco 88-LCO-34H14FH, and Chassis 8608-SYS with IOS-XR 7.8.2 release
- Support for optical module DP04QSDD-HE0 on Cisco NCS-57C3-MOD-SYS and Cisco NCS-57C3-MODS-SYS devices (with MPA NC57-MPA-2D4H-S) with IOS-XR 7.8.2
- Validation of the 6.5.33 release of Cisco NCS 4000 series devices

Serial Services

- Support for serial services RS232, RS422, RS485, and X.21 due to the CLI changes in the IOS-XE 17.6.6 release

Discovery of OCH-CC Circuits Between Cisco NCS 1000 Series and Cisco NCS 2000 Series Devices

Cisco EPN Manager facilitates the discovery of end-to-end OCH-CC circuits between Cisco NCS 1000 series devices and Cisco NCS 2000 series devices.

Prerequisites to discover ODU circuits here are:

- A valid OCHNC/MCHNC circuit is configured between the intermediate Cisco NCS 2000 series device nodes.
- An OCH-Trail is discovered between the source and destination Cisco NCS 1000 device nodes
- Client ports are configured on the source and destination Cisco NCS 1000 device nodes with the same client rate.

An OCH-CC circuit will be discovered on top of the OCH-Trail with the circuit name: <CircuitName>-ochcc-<Source endpoint name>

Note Promote/Modify/Delete operations are not supported on Brownfield OCH-CC circuits.

To create an ODU circuit between any endpoints, see Create and Provision an ODU Circuit in the Cisco Evolved Programmable Network Manager 7.1 User and Administrator Guide.

Functionality Changes Including Removed/Disabled Features

Following features/functionalities/Menus were deprecated in the Cisco EPN Manager 7.1.1 release:

- **General Features:**
  1. **Feedback**- Feedback option has been entirely removed, including the following navigation paths:
     - Web GUI global settings icon > Feedback > I wish this page would...
     - Dashboard > Network Summary > Feedback

New Operating System Support

This section lists the new OS support provided in Cisco EPN Manager 7.1.1. For a list of all support information, click the gear icon at the top-right of the web GUI and choose **Help > Supported Devices**.

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

Device Model	Device OS
Cisco ASR 9000 Router	IOS-XR 7.10.2
Cisco ASR 9000 64-Bit Router	IOS-XR 7.11.1

Cisco IOS XRv 9000 Series Aggregation Services Router—New Operating System Support

Device Model	Device OS
Cisco IOS XRv 9000 Router	IOS-XR 7.9.1
Cisco IOS XRv 9000 Router	IOS-XR 7.11.1

Cisco 8000 Series Routers—New Operating System Support

Device Model	Device OS
Cisco 8000 Router	IOS-XR 7.10.2
Cisco 8000 Router	IOS-XR 7.11.1

Cisco Network Convergence System 5500 Series—New Operating System Support

Device Model	Device OS
Cisco NCS 5500 Series	IOS-XR 7.10.2
Cisco NCS 5500 Series	IOS-XR 7.11.1

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

Device Model	Device OS
Cisco NCS 5700 Router	IOS-XR 7.10.2
Cisco NCS 5700 Router	IOS-XR 7.11.1

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

Device Model	Device OS
Cisco NCS 540 Router	IOS-XR 7.10.2
Cisco NCS 540 Router	IOS-XR 7.11.1

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

Device Model	Device OS
Cisco NCS 560 Router	IOS-XR 7.10.2
Cisco NCS 560 Router	IOS-XR 7.11.1

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

Device Model	Device OS
Cisco ASR 900 Router	IOS-XE 17.6.6

New Device Support

This section lists the new device support that is provided in the Cisco EPN Manager 7.1.1 release. 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 8000 Series Routers—New Device Support

Device Model	Device OS
Cisco 8804 Router	IOS-XR 7.8.2
Cisco 8111-32EH Router	IOS-XR 7.10.2
Cisco 8608 Router	IOS-XR 7.10.2
Cisco 8011-2X2XP4L Router	IOS-XR 7.11.1

Supported Installation/Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 7.1.1 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 7.1.1
Cisco EPN Manager 5.1.4.1	**Cisco EPN Manager 5.1.4.1 > 6.0.0 > 6.1.0 > 6.1.2 > 7.1 > 7.1.1**
Cisco EPN Manager 6.1.2	**Cisco EPN Manager 6.1.2 > 7.1 > 7.1.1**
Cisco EPN Manager 7.0.x	**Cisco EPN Manager 7.0.x > 7.1 > 7.1.1**
Cisco EPN Manager 7.1	**Cisco EPN Manager 7.1 > 7.1.1**

See the relevant installation guide for installation prerequisites and procedures for Cisco EPN Manager versions.

Download and Install an Update for a Non-HA Deployment

This section describes how to download and install Cisco EPN Manager 7.1.1 on top of an existing Cisco EPN Manager 7.1 installation for non-HA deployments.

Procedure

Step 1 In the left sidebar, select **Administration > Licenses and Software Update > Software Update**.

Step 2 Download the latest update either using the **Download from Cisco.com** option via the Cisco EPN Manager GUI, or by directly logging in to Cisco.com from a browser. The file has the prefix **cepnm7.1-ppX-buildxxx.ubf**.

Step 3 Depending on the location the file was saved to, select either **Upload from the local computer** or **Copy from server's local disk**.

Step 4 When the file is loaded, click the **Install** button that is associated with the Cisco EPN Manager update. The server restarts when the installation is complete.

Step 5 Click **Yes** in the dialog box to proceed with the installation.

Note The server restarts when the installation is complete.

Step 6 If you are asked to overwrite an existing file, click **Yes**.

After successful installation, the status changes to **Installed**. Cisco EPN Manager auto restarts and GUI will not be accessible for some time. (It may take up to an hour.)

Step 7 Check the status of the Cisco EPN Manager services.

a) Begin an SSH session with the Cisco EPN Manager server and log in as a Cisco EPN Manager CLI admin user.

b) Run the **ncs** status command to ensure that the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. For optimal Cisco EPN Manager functionalities, all services should be up and running.

Step 8 When the Cisco EPN Manager GUI is accessible, log in and ensure that the Patch status is **Installed** in the **Software Update** page.

Synchronize the Inventory of All Devices with the Database (Existing Deployments Only)

If you are using a previous version of Cisco EPN Manager (that is, this is not a fresh installation), perform a Sync operation on the devices. The Sync operation instructs the Cisco EPN Manager to collect the physical and logical inventory information and save it to the database.

Procedure

Step 1 Choose **Monitor > Network Devices**.

Step 2 Select all devices, and then click **Sync**.

Download and Install an Update for a HA Deployment

If you are using external authentication and authorization, after installation you must export the user task information to your AAA server to pick up the latest updates.

Note During the patching of primary and secondary HA servers, both the servers will be down.

Procedure

Step 1 Ensure you have the password (authentication key) that was created when HA was enabled. You need it to install the patch on the secondary server.

Step 2 Backup your data. (For instructions on how to backup your data, refer to Cisco Evolved Programmable Network Manager 7.1 User and Administrator Guide.)

Increase Session Timeout on Servers

Follow these steps to increase the timeout on the primary and secondary servers from 30 minutes to 90 minutes:

Procedure

Step 1 Log in as the Linux CLI root user.

Step 2 Save a backup of the web.xml file that is located under `/opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/` by running the following command (one line):

```
cp /opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/web.xml
/opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/web.xml.orig
```

Step 3 In the web.xml file (`/opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEBINF/web.xml`), search for the following:

```
<session-timeout>30</session-timeout>
```

Step 4 Change the session timeout to 90 minutes:

```
<session-timeout>90</session-timeout>
```

Step 5 As the Cisco EPN Manager CLI admin user, manually stop and restart the server:

```
ncs start
```

```
ncs stop
```

Step 6 Ensure that all services are up and running by using this command:

```
ncs status
```

Remove HA Configuration

Procedure

Step 1 Login to the Cisco EPN Manager GUI as a user with Administrator privileges.

Step 2 On the left sidebar, choose **Administration > Settings > High Availability.**

Step 3 Click **HA Configuration > Remove**.

Step 4 On the primary server, go to **Administration > Settings > High Availability** and confirm that the Configuration Mode field displays **HA Not Configured**.

Step 5 Log in to the health monitor page of the secondary server page and confirm that **HA not Configured** appears under the **State** tab.

Install Device Pack and Point Patch on Primary and Secondary Servers

Procedure

Step 1 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 2 Make sure no backups are in progress.

Step 3 On the secondary server, update the time zone using a soft link.

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startupconfig
| cut -d " " -f 3) /etc/localtime
```

This ensures that the compliance server will be up and running on the secondary server after failover.

Install the Device Pack and Point Patch on the Primary Server

Procedure

Step 1 From the left sidebar, choose **Administration > Licenses and Software Update > Software Update.**

Step 2 Download the latest update either using the **Download from Cisco.com** option via the Cisco EPN Manager GUI, or by directly logging in to Cisco.com from a browser. The file has the prefix **cepnm7.1-ppx-buildxxx.ubf.**

Step 3 Depending on the location the file was saved to, select either **upload from local computer** or **copy from the server local disk**.

Step 4 When the file has been loaded, Click the **Install** button associated with the Cisco EPN Manager update.

Step 5 Click **Yes** in the confirmation message pop-up window to proceed with the installation.

Step 6 Cisco EPN Manager auto-restarts and the Cisco EPN Manager web GUI will not be accessible for some time (may take up to an hour).

Step 7 Synchronize the hardware and NTP clocks on the primary and secondary servers as described in Synchronize the Hardware and NTP Clock, then check that the clocks on each server are synchronized with one another.

Note The service restart in the Synchronization Clock operation can be ignored as the installation of Device Pack and Point Patch restarts the Cisco EPN Manager.

Install Cisco EPN Manager on Secondary Servers

Procedure

Step 1 Log in to the secondary server's web page.

Step 2 Enter the authentication key and click **Login**.

Step 3 Click the **Software Update** button.

Step 4 You will be transferred to a login page. Log in to Cisco EPN Manager as administrator.

Step 5 Download the latest update either using the **Download** option from Cisco.com option via the Cisco EPN Manager GUI, or by directly logging in to Cisco.com from a browser. The file has the prefix **cepnm7.1-ppx-buildxxx.ubf**.

Step 6 Depending on the location the file was saved to, select either upload from local computer or copy from the server's local disk.

Step 7 Once the file has been loaded, Click the **Install** button associated with the Cisco EPN Manager update.

Step 8 Click **Yes** in the confirmation message pop-up window to proceed with the installation.

Cisco EPN Manager auto-restarts and the Cisco EPN Manager web GUI will not be accessible for some time (may take up to an hour).

Verify Installation on Secondary Server

Procedure

Step 1 Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.

Step 2 Run the **ncs** status command to ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine.

For optimal Cisco EPN Manager functionality, all services must be Up and running.

Step 3 Once the web GUI is accessible, verify the installation and version in the secondary server's HM web page.

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

Step 4 Enter the authentication key and click **Login**.

Step 5 In the **Uploaded Update** Files tab, verify that the MPx ubf file (in the format cepnm.7.1-ppx- buildxxx.ubf) is listed and that the **In Use** status is **Yes**.

Step 6 Ensure that all services are up and running by running this command:

```
ncs status
```

Enable HA and Verify HA Status

Procedure

Step 1 Enable High Availability.

a) Log in to the Cisco EPN Manager web GUI as a user with Administrator privileges.
b) In the left sidebar menu, choose Administration > Settings > High Availability.
c) Click HA Configuration and enter the secondary server IP address, the secondary server authentication key, and an email address to which the Cisco EPN Manager should send HA state change notifications.
d) If you are using virtual IP addressing in your HA setup (if the primary and secondary servers are in the same subnet), check the Enable Virtual IP check box and enter the one or more virtual IP addresses.
e) Click **Save**, then wait until the servers are synchronized.
f) Verify that the Configuration Mode is HA Enabled.

Step 2 Verify the primary server's HA status.

a) Click HA Status on the left.
b) Check that the Current State Mode displays Primary Active.

Step 3 Verify the secondary server's HA status.

a) Log in to the secondary server's web page.
b) Enter the authentication key and click Login.
c) Verify that the Current State Mode is Secondary Syncing (with a green check mark).

Synchronize the Inventory of All Devices with the Database (Existing Deployments Only)

If you are using a previous version of Cisco EPN Manager (that is, this is not a fresh installation), perform a Sync operation on the devices. The Sync operation instructs the Cisco EPN Manager to collect the physical and logical inventory information and save it to the database.

Procedure

Step 1 Choose **Monitor > Network Devices**.

Step 2 Select all devices, and then click **Sync**.

Important Notes

Cisco EPN Manager software is distributed with all the components necessary for its optimized and secure operation, including the Red Hat Linux operating system and the Oracle database. All security-related configurations, regression testing, performance, and scalability metrics are based on the set of components and configurations included in the original Cisco EPN Manager software distribution. Cisco provides periodic EPN Manager software updates that can also contain necessary updates to the packages installed on the operating system or to the database.

Note If any of the following changes are made to the original distributed Cisco EPN Manager software, Cisco will no longer support the operating environment:

- Configuration changes to the software or operating system, or installation of other components that are not part of the original distribution.
- Direct installation and application of third-party software on the Red Hat Linux operating system that is embedded within Cisco EPN Manager.
- Application of updates or patches that are **not** provided by Cisco to individual Cisco EPN Manager components.
- Changes to the internal Cisco EPN Manager settings that are not documented as modifiable in the Cisco EPN Manager User and Administrator Guide on Cisco.com, as these changes may weaken security, disable functionality, or degrade scalability and performance.

System Behavior and Functionality Updates

- In Cisco EPN Manager 6.1 release, under **Inventory** > **Other** > **Circuits,/VCs & Network Interfaces**, the column order was retained and maintained as it was stored in the database. However, in Cisco EPN Manager 7.1 release, there has been a change in the storage mechanism for column order. The column order will now be stored in the browser session storage instead of the database. Therefore, any adjustments made to the column order will be applicable only for the current session and will not be permanently saved in the database.

Limited Scope of Specific Devices

- The Cisco 8608-SYS and Cisco 8011-2X2XP4L platforms do not support provisioning and related use cases for any technology.

Upgrade Issues

- FTP and TFTP are disabled by default.
- Active Threshold Crossing Alarms (TCA) for temperature remain active and are not cleared automatically. Clear these alarms manually.
- You must resync your devices to view ISIS links.
- You must resync LDP-enabled devices to view LDP feature-related information.
- You must recreate the TCAs for inbound/outbound errors and inbound/outbound discards in the Interface Health monitoring policy.

Limitations on Carrier Ethernet Circuit Provisioning

- Promotion of service using the old probe name format is now supported. These probes are listed in the user interface with the appropriate standard OAM Profile name after promotion.
- Sample profile: profile PM2_3_8_CoS5_DM type cfm-delay-measurement.

- While custom profile names are supported in EPN Manager, modifying brownfield services with a different naming format deletes the existing custom profile and adds a new profile with a supported naming format.
- Inventory models do not correctly display the profiles that are not associated to a service.
- The validation limit for the number of profiles is 100. If you create a new SLA operation profile after 100 existing profiles, the device generates an error and deployment fails.

TLS 1.2 Required for Secured Channel Communication for HTTPS and TLS

Only Transport Layer Security (TLS) 1.2 is supported for HTTPS and TLS related secured communication, for example, RADIUS EAP-TLS.

Support for TLS 1.0, TLS 1.1, and all versions of SSL has been disabled due to security vulnerabilities.

This means that all peer systems and clients that transact with Cisco EPN Manager using HTTPS/TLS must support TLS 1.2. If they do not support TLS 1.2, you must upgrade these systems. Wherever possible, the Cisco EPN Manager documentation highlights the potentially affected systems. Contact your Cisco representative for support in this regard, if necessary.

Reconciliation Report Limitations

If you have not provided a value for an attribute while provisioning a service, the provisioned value for that attribute is displayed as “Missing” in the reconciliation report. The device may have a default value for this attribute, but Cisco EPN Manager does configure this value.

Limitations on Cisco ME 1200 Devices

The Y.1564 performance test does not work if the source/destination is a Cisco ME 1200 device.

Limitations on Cisco NCS 4200 Devices Running IOS-XE 16.8.1

The following functionalities do not work on Cisco NCS 4200 devices running IOS-XE 16.8.1:

- Alarm profile
- Configuration of SONET LOP and CT3 LOP from the GUI
- Admin shut/no shut functionality on SONET/T1/T3 HOP/LOP

Limitations on Cisco NCS 540 and Cisco NCS 5500 devices

Cisco NCS 540 and Cisco NCS 5500 device series do not support Fault-OAM, Wrap-Protection, and BFD.

Use CLI Templates for Configuring PTP Commands

On ASR920 devices with software version 16.9.1, IEEE 1588-2008 BC/MC license is required to execute the 1588 PTP commands.

Configuration and Inventory Not Supported for PTP Templates

The behavior of modeling the configurations that are pushed through PTP templates may not work as expected because the model may not be in place for all the configurations pushed through PTP templates. Configuration/Inventory is not supported for these configurations.

Deprecation of Support for ONS 10.00.10, 10.01.00, 10.03.00

ONS 10.00.10, 10.01.00, 10.03.00 ONS 10.00.10, 10.01.00, and 10.03.00 are no longer supported on Cisco NCS 2002, Cisco NCS 2006, and Cisco NCS 2015 devices.

Data Center Device Lifecycle Support Only

Cisco EPN Manager provides essential support for a few selected UCS compute systems, Nexus series devices, and the CSR 1000v devices.

LINK_DOWN alarm on sub interfaces in Gig Port

LINK_DOWN alarms will not be generated when a link is down on sub interfaces in a Gig Port.

Cisco EPN Manager Bugs

Open Bugs

The following criteria are used to create the list in the table below, which includes all the open bugs in Cisco EPN Manager 7.1.1 release:

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

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

Bugs	Description
CSCwh07489	Add Self as SSO server not working when EPNM UI is launched with domain name
CSCwi08661	Clock Sync-E - interface input source removal is deleting entire interface for XR platforms
CSCwi10855	R7.1.1: At times during service provisioning the CLI o/p msg is not displayed for both preview and deploy
CSCwi11952	NCS4K: Real Time PM: OPR-MIN, MAX and AVG is shown at Optical Physical Tab for real time PM
CSCwi23873	EPNM Session ID is published in the source code

Bugs	Description
CSCwi24921	7.1.1 GA: Editing ANP page in Japanese language not enabling Next button
CSCwi27107	Unable to change the Loopback setting for Sonet Low Order Path
CSCwi31355	NCS-2K:Changing wavelength on the line port throws 'Invalid Payload Block Invalid Data Format' error
CSCwi32353	getAll TL fails retrieve only 99 records, instead 100
CSCwi04405	Promotion of Discovered Service should not enable Save action until all mandatory properties entered
CSCwi15923	Alarm Policies are not saving existing event types on modification flow
CSCwi27116	SONET Loopback options need to include Remote Line and Remote Payload
CSCwi28872	Monitor Lite user should not be allowed to change password from Settings Wheel button from top right
CSCwi29967	EPNM 7.1.1: Some times Technology dropdown values are not shown under provisioning wizard
CSCwi08618	BFD Template deletion during MPLS TE service decommission is showing bad BFD Template Name
CSCwi41378	On CLI Template deploy for NCS XR devices, job result transcript missing
CSCwi18461	Time Zone updates through EPNM is not getting pushed to NCS2K devices
CSCwe37539	7.10.1: NCS1K4-2-QDD-C-K9 - Card Mode goes into "Not Provisioned" after LC Cold Reset, when MPLS Tunnel is in downstate

Resolved Bugs

The table below lists all the bugs that were resolved in the Cisco EPN Manager 7.1.1 release.

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

Bugs	Description
CSCwh13793	7.0.1: The System Monitoring Disk Statistics dashlet is not showing any output
CSCwh48517	7.1 GA: UNI in ceased state after force delete
CSCwh38587	Dying gasp alarm not cleared

Bugs	Description
CSCwc49225	UTC timezone is shown as CUT in all UI pages
CSCwh11310	"Ok" and "Cancel" buttons are not visible in "Create Duplicate Policy" popup message
CSCwh55336	EPNM 7.1 Instalation Guide does not include support for ESxi release 8
CSCwf76966	I159 B: MLT view doesn't display the 2K ports information in the OCH layer
CSCwh00835	BITS Interface disappearing upon device full sync
CSCwh22670	161 A: Overlay and MLT are not working for SR policies and overlayed L2VPN
CSCwh63552	MLT is not displaying Managed links

Closed Bugs

The table below lists all the bugs that were closed in Cisco EPN Manager 7.1.1 release.

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

Bugs	Description
CSCwf65003	EPNM 7.1: Discovered OCH-Trail circuit is showing end-points as Optics instead of CoherentDSP

Get Information about Cisco EPN Manager Bugs

Use the Bug Search tool (BST) to get the latest information about Cisco EPN Manager bugs. BST allows partners and customers to search for software bugs based on product, release, and keyword, and it aggregates key data such as bug details, product, and version.

Cisco EPN Manager bugs may be caused by defects in a device's platform or operating system. In such cases, the Cisco EPN Manager bug will be resolved when the hardware/operating system bug is resolved.

Procedure

Step 1 Log into the Bug Search Tool.

a) Go to https://tools.cisco.com/bugsearch/.

b) At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do

Step 2 To list all bugs for this version, click the **Select from list** hyperlink that is next to the **Product** field and select the product.

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

b) When the results are displayed, use the **filter and sort** tools to find bugs according to their status, severity, how recently they were modified, if any support cases are associated with them, and so forth.

You can also search using bug IDs or keywords. For more information, click **Help** at the top right of the **Bug Search** page.

Related Documentation

For a list of all documentation available for Cisco EPN Manager 7.1.1, see the Cisco Evolved Programmable Network Manager 7.1 Documentation.

Accessibility Features

For a list of accessibility features in Cisco EPN Manager 7.1.1, contact accessibility@cisco.com.

All product documents are accessible. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

Subscribe to **What's New** in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.