# Cisco Evolved Programmable Network Manager 7.0.1 Release Notes

**First Published:** 2023-04-26

## Introduction

This document contains the following information about Cisco Evolved Programmable Network Manager 7.0.1:

## Functionalities Added

This section lists the new features/functionalities delivered in Cisco EPN Manager 7.0.1.

### Device Support

- Chassis view support for Cisco A9K-RSP5-X-TR and Cisco A9K-RSP5-X-SE route switch processors
- Chassis view support for Cisco A99-RP3-X-TR and Cisco A99-RP3-X-SE route processors
- Chassis view support for Cisco NCS 560-4 RSP4 and Cisco NCS 560-4 RSP4E routers
- Chassis view support for Cisco NC57-MPA-1FH1D-S on IOS-XR 7.8.1
- Support for Cisco ASR1002-HX router on IOS-XE 16.6.4
- Chassis view support for Cisco 88-LC0-34H14FH and Cisco 88-LC0-34H14FH-O line cards with IOS-XR 7.5.1 on Cisco 8000 series routers
- Support for ZR pluggables on Cisco 88-LC0-34H14FH-O line cards
- Support for Cisco N520-X-4G4Z-A and Cisco N520-X-4G4Z-D routers on IOS-XE 17.9.1
- Support for Cisco DP04QSDD-HE0 (QDD-400G-ZRP) pluggables for Cisco A9K-20HG-FLEX line cards on IOS-XR 7.9.1

- Support for Cisco DP04QSDD-HE0 (QDD-400G-ZRP) pluggables for Cisco NCS-57C3-MOD-SYS and Cisco NCS-57C3-MODS-SYS chassis with Cisco NC57-MPA-2D4H-S line cards on IOS-XR 7.9.1
- Validation of IOS-XE 17.9.2a on Cisco NCS 4200 series devices
- Validation of IOS-XE 17.9.2a on Cisco ASR 900 series routers
- Validation of IOS-XE 17.9.2a on Cisco ASR 920 series routers
- Essential support for Cisco Catalyst 8000V with IOS-XE 17.9.2a

### Licensing

- Alignment of Cisco EPN Manager RTM license with Cisco Crosswork Network Controller and Cisco Crosswork Network Services Orchestrator

## Device/OS Support Added

This section lists the new support provided in Cisco EPN Manager 7.0.1. For a list of all support information, click the gear icon at the top right of the web GUI and choose Help > Supported Devices. For information about Cisco EPN Manager supported devices, see Supported Device Tool.

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

| Device Model | Device OS |
|---|---|
| Cisco NCS 5700 Router | IOS-XR 7.8.2 |
| Cisco NCS 5700 Router | IOS-XR 7.9.1 |

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

| Device Model | Device OS |
|---|---|
| Cisco ASR 9000 Router | IOS-XR 7.8.2 |
| Cisco ASR 9000 Router | IOS-XR 7.9.1 |

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

| Device Model | Device OS |
|---|---|
| Cisco NCS 540 Router | IOS-XR 7.8.2 |
| Cisco NCS 540 Router | IOS-XR 7.9.1 |

### Cisco 8000 Series Routers—New Operating System Support

| Device Model | Device OS |
|---|---|
| Cisco 8000 Router | IOS-XR 7.8.2 |
| Cisco 8000 Router | IOS-XR 7.9.1 |

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

| Device Model | Device OS |
|---|---|
| Cisco NCS 5500 Series | IOS-XR 7.8.2 |
| Cisco NCS 5500 Series | IOS-XR 7.9.1 |

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

| Device Model | Device OS |
|---|---|
| Cisco NCS 560 Router | IOS-XR 7.8.2 |
| Cisco NCS 560 Router | IOS-XR 7.9.1 |

### Cisco Network Convergence System 1000 Series—New Operating System Support

| Device Model | Device OS |
|---|---|
| Cisco NCS 1010 Router | IOS-XR 7.9.1 |

## Supported Installation/Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 7.0.1 from previous versions.

| Current Cisco EPN Manager Version | Installation Path to Cisco EPN Manager 7.0.1 |
|---|---|
| Cisco EPN Manager 7.0.0 | **Cisco EPN Manager 7.0.0 > 7.0.1** |

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 7.0.1 on top of an existing Cisco EPN Manager 7.0 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 EPNM GUI, or by directly logging in to Cisco.com from a browser. The file has the prefix **cepnm7.0-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 has been loaded, click the **Install** button associated with EPN Manager update. The server restarts when the installation is complete.

**Step 5** Click **Yes** in the confirmation message 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 autorestarts and the GUI is not accessible for some time. (It may take upto 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 check 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 (i.e. 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, 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 in order to pick up the latest updates.

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

### Procedure

**Before You Begin**

**Step 1** 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 2** Backup your data.(For instructions on how to backup your data, refer to Cisco Evolved Programmable Network Manager 7.0 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 EPNM GUI, or by directly logging in to Cisco.com from a browser. The file will have the prefix **cepnm7.0-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 EPN Manager update.

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

**Step 6** Cisco EPN Manager will auto-restart 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 both 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 into 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. Login 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 will have the prefix **cepnm7.0-ppx- buildxxx.ubf**.

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

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

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

Cisco EPN Manager will auto-restart 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. Note that for optimal Cisco EPN Manager functionality, all services should 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.7.0-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 (i.e. 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, then click **Sync**.

# Important Notes

### Known Issues

**Problem Statement 1:** TL1 Profile creation requires mandatory SNMP parameters.

**Description:** While attempting to create a TL1 profile, users encountered an issue where the mandatory SNMP parameters were required. However, SNMP parameters are not mandatory for creating the TL1 profile.

**Problem Statement 2:** Unsuccessful saving of TL1 credentials in credential profile page.

**Description:** While creating a TL1 profile, TL1 credentials were not saved in the policy detail page. Despite the operation indicating success, the TL1 credentials were not being stored as intended.

**Resolution:**

To address these issues, a patch has been implemented to update the JS component on the customer setup. The patch can be applied by executing the ***install_baseui.sh*** script found under the */opt/CSCOlumos/updates/cepnm7.0-dpp1-buildXXX/epnm_7_0_updates/scripts/install_baseui.sh.*

To apply the patch, follow these steps:

1. Establish a secure SSH connection to the server hosting the Cisco EPN Manager.

2. Navigate to the patch location by running the command: ***cd /opt/CSCOlumos/updates/***.

3. Copy the *install_baseui.sh* script to the updates directory using: ***cp /opt/CSCOlumos/updates/cepnm7.0-dpp1-build156/epnm_7_0_updates/scripts/install_baseui.sh /opt/CSCOlumos/updates/***.

**Note** Replace *cepnm7.0-dpp1-build156* with the appropriate build number, if necessary.

4. Make the *install_baseui.sh* script executable:

   ```
   chmod 755 install_baseui.sh
   ```

5. Execute the *install_baseui.sh* script using the command:

   ```
   sh -x ./install_baseui.sh
   ```

   This script applies the patch to the JS component.

6. Perform a hard refresh of your browser to ensure the changes take effect immediately. Restarting the browser is not necessary.

With these resolutions in place, TL1 profiles can now be created without being prompted for mandatory SNMP parameters, and TL1 credentials can be successfully saved within credential profiles.

### Upgrade Issues

- FTP and TPTP 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 IS-IS 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 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.
- Validation limit for 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 Editing Alarm Notification Policies

If the upgrade conditions of existing categories are different from the condition of categories on 5.1, then the conditions post upgrade will not match. As a result, policy might not be created, or UI selection might not take place for the unmatched events. In this case, you should delete the upgraded policies and create a new one.

### Limitations on NCS 4200 Devices Running IOS-XE 16.8.1

The following functionalities do not work on 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 that are 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, 2006 and 2015 devices.

### Data Center Device Lifecycle Support Only

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

### LINK_DOWN alarm on sub interfaces in Gig Port

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

# Cisco EPN Manager Bugs

## Open Bugs

The table below lists the open bugs in Cisco EPN Manager Release 7.0.1 according to the following criteria:

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

Click the identifier 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 |
|---|---|
| CSCwc78979 | Bellatrix: Coherent DSP is giving error in response post modify operation |
| CSCwd12284 | [GA]: UI partially or completely not displaying Coherent port if device admin status is changed |
| CSCwd99608 | [GA]: Span loss value from XML is mismatch from Device |

## Resolved Bugs

The table below lists the customer-found bugs that have been resolved in Cisco EPN Manager 7.0.1

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

| Bugs | Description |
|---|---|
| CSCwe10195 | EPNM 7.0GA I151 Build Nessus Detects High Vulnerability Plugin Id 168497 |

| Bugs | Description |
|---|---|
| CSCwe12754 | NCS 1010 - Device manual sync is needed after enabling alarm manager settings |
| CSCwe21883 | EPNM 6.1.1.1 Build33: Nessus Detects Vulnerabilities |
| CSCwe27958 | Exception is thrown when creating L3VPN untagged service provision |
| CSCwe37602 | EPNM 5.0.2.5 Build769: Nessus Detects Vulnerabilities |
| CSCwe38852 | 7.0.1 - i153B unsigned UBF #28 installation Failed |
| CSCwe47917 | Apache Tomcat 9.0.0.M1 < 9.0.71 |
| CSCwe62265 | 7.0.1 154B > server crash observed after performing y1564 test on a l2vpn service |
| CSCwe66098 | Vulnerabilities in jackson-databind 2.13.3 |
| CSCwe66142 | Vulnerabilities in netty 4.1.72.Final |
| CSCwe73473 | Vulnerabilities in commons-beanutils - multiple versions |
| CSCwe77311 | Image activation fails for c8000v device when erase flash option is enabled |
| CSCwe83895 | 155A Build 105 Nessus Detects Vulnerabilities |
| CSCwf00112 | 38 Reports Templates only getting displayed on Report Lunch Pad |
| CSCwe07091 | Cisco Evolved Programmable Network Manager Command Injection Vulnerability |
| CSCwe14957 | BnR upgrade, Reports filter criteria not updated during the upgrade for some reports. |
| CSCwe17035 | I151C: Nessus Detects Vulnerabilities |
| CSCwe23019 | Backup job can't backup db caused by hardcoded number 650 in db_size.sh |
| CSCwe23573 | Memory leak in HMMain – CARS JNI call |
| CSCwe24786 | setTP of LoopBack for NCS 2K self-response attributes Admin and Oper state values is not-applicable |
| CSCwe29279 | DB connection leak in inventory module |
| CSCwe29295 | DB Connection leak from NBI-restconf |
| CSCwe36146 | Optical legacy (non-wson) circuits are in partial discovery state |
| CSCwe36292 | For not existing protection profile, provisioning OTN service fails with an invalid error |

| Bugs | Description |
|---|---|
| CSCwe42670 | NCS1K4-2-QDD-C-K9: In muxponder-slice mode slice deletion failed via EPNM |
| CSCwe43155 | Loopback interface is removed when changing sonet from protected to working with ACR configuration |
| CSCwe47418 | Clock commands failing on NCS 5001 platform |
| CSCwe47889 | GA > 7.0.1 > MLT throws error for access-evpl over SR |
| CSCwe48459 | If 3*100 or 4*100 is created, epnm does not push breakout to hwmodule |
| CSCwe48959 | When notset is executed, the dac rate does not display the default value |
| CSCwe48980 | the boundary value of Configured TX Power/CD-MIN/CD-MAX is changed in 7.9.1 |
| CSCwe51877 | setTP of wavelength for NCS2K, in self response "tp.wavelength" gets frequency instead wavelenght |
| CSCwe54471 | 7.0/7.1 : CEM Modify leads to Partial Discovery : TdmCmPWCnPrtclEndpnt Object is missing |
| CSCwe56282 | Flex Algorithm is failing to save in MBC under Segment Routing |
| CSCwe57774 | Show interfaces non-dynamic support not working for IOS XR 6.9.1 onwards |
| CSCwe61615 | REPT EVT FXFR events cause exception shown in nms-optical-fault log and GUI not showing the events |
| CSCwe62723 | EPNM_7_0_1_GA:Observing failed to update the boot config error message while c8000v image activation |
| CSCwe66205 | Bright ZRP: ASR9912: Controllers-->Optics0/3/0/0 --> "DAC Rate" field is not editable |
| CSCwe66810 | 7.0.1 RON SOL > epnm continues to show ots port as admin down after its made admin down/up in device |
| CSCwe67273 | Vulnerabilities in wss4j 1.6.9 |
| CSCwe67276 | Bright ZRP: EPNM not throwing any error when same SD and SF BER values are selected on Coherent port |
| CSCwe67383 | Bright ZRP: Configured Tx-power range in EPNM should be from -150 to 50 instead of -150 to 0 |
| CSCwe67571 | Vulnerabilities in postgresql-jdbc 9.4.1212.jre7 |
| CSCwe68524 | Vulnerabilities in mina 2.0.5, 2.0.1 |

| Bugs | Description |
|---|---|
| CSCwe68710 | Vulnerabilities in tzinfo 1.2.2 |
| CSCwe68909 | cisco-resource-physical:node with depth att will not work in case there is unmanaged device |
| CSCwe70051 | Bright ZRP: ASR9K: Controllers-->Optics: All DAC rate showing on device should be supported on EPNM |
| CSCwe72263 | Bright ZRP: ASR9k: "Configured Wavelength" is not getting updated properly after setting "1528773" |
| CSCwe73143 | loopback seeing to Line is not updated to device |
| CSCwe73797 | Missing i18n - deviceTrend - device health dashboard |
| CSCwe73888 | NCS1010 OLC span loss missing data from 7.9.1 , with respect to 7.7.1 |
| CSCwe73958 | OSPF link down , is not making physical link down in EPNM for NCS1010 |
| CSCwe76131 | range validation is still shown an older value in Configured Tx Power/CD-Min/CD-MAX |
| CSCwe76315 | OCHCC Prov Wizard doesn't list out all the client ports available |
| CSCwe81224 | Breakout info is not updated in EPNM if it is created in Device |
| CSCwe81345 | NCS1K4: Inventory status not updated after physically removing optics from the card |
| CSCwe81394 | Dac rate , device accepts , EPNM not accpting ,an error messge for not accepting is also not clear |
| CSCwe83247 | Bright ZRP: Error message still shows the old value range for configured Tx Power |
| CSCwe91017 | "Alarms and Events" under Administration -> System Settings comes empty |
| CSCwc64497 | 6.1 Install Guide update |
| CSCwd19417 | In MPLS-LDP "Downstream Max Label" accepts value only till 32768 while device accepts till 1048575 |
| CSCwd62509 | XSS-Vulnerability in Alaram Policies Page |
| CSCwe00397 | Weekly Schedule Report's Every field has issue with max values in both GA & LA |
| CSCwe19705 | CE-Update Scenario is failing for EVPN service - 7.0GA \| 151C BUILD#595 |

| Bugs | Description |
|---|---|
| CSCwe36308 | While creating circuit via restconf, circuit creation failes when 'Label' parameter is not provided |
| CSCwe46388 | For OTDR Scan with invalid distance, should be 400 Bad Request but getting 500 error |
| CSCwe56299 | In MPLS-LDP "Downstream Max Label" accepts value only till 32768 while device accepts till 40960 |
| CSCwe62189 | In setTP Fiber attributes validation, error code should be 400 Bad Request but getting 500 error |
| CSCwe62196 | In setTP NNI controller validation, instead 400 Bad Request getting 500 & also error tag changed |
| CSCwe62972 | EPN - install - certs config not initialized |
| CSCwe69943 | Device is allowed to set CD-MIN/CD-MAX to 0, however EPNM throws a warning |
| CSCwd90369 | GA:Localization : In the Opticalphysical/Ethernet PM Dashboard, PM counters titles not localized |
| CSCwe36277 | Sensors graphs - value in tooltip is rounded & trimmed to 3 numbers after digit |
| CSCwe48356 | If a user opens an inline edit and selects the cancel button, a toast message is appeared |
| CSCwe82966 | Error message is not showing the field name comoplely |
| CSCwe78745 | Critical CVE in component glibc. Upgrade to latest version |
| CSCwe78840 | Critical CVE in component openssl. Upgrade to latest version |
| CSCwe15015 | 7.0-GA and LA: L3VPN LSP OAM is failing |
| CSCwe17532 | The LMP Configuration with 300G trunk is failed with an error message |
| CSCwe31942 | NCS1004: For trunk optics port TXPower and RxPower missing under OpticalPhysical tab in I360 |
| CSCwe32001 | Report > Report Launchpad > Select Any card |
| CSCwe67260 | Vulnerabilities in jettison 1.2 - design-tool-blueprint-webapp |
| CSCwe75027 | Importing Action Profile does not import all data (e.g. no queueing action data is imported) |
| CSCwe83417 | EPN - fault - NCS 4216 alarm resync feature fails for fan alarm |
| CSCwe73405 | Vulnerabilities in code mirror 3.19.0 CVE-2020-7760 |

## 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 7.0.1, see the Cisco Evolved Programmable Network Manager 7.0.

# Accessibility Features

For a list of accessibility features in Cisco EPN Manager 7.0.1, 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.