



# Cisco Evolved Programmable Network Manager 7.1.2 Release Notes

---

**First Published:** 2024-04-08

## Introduction

This document contains the following information about Cisco Evolved Programmable Network Manager 7.1.2:

- [New Functionality Added, on page 1](#)
- [Functionality Changes Including Removed/Disabled Features, on page 2](#)
- [New Operating System Support, on page 3](#)
- [Supported Installation/Upgrade Paths, on page 4](#)
- [Download and Install an Update for a Non-HA Deployment, on page 5](#)
- [Download and Install an Update for a HA Deployment, on page 6](#)
- [Important Notes, on page 10](#)
- [Cisco EPN Manager Bugs, on page 13](#)
- [Related Documentation, on page 15](#)
- [Accessibility Features, on page 16](#)
- [Obtaining Documentation and Submitting a Service Request, on page 16](#)

## New Functionality Added

This section lists the new features/functionalities delivered in Cisco EPN Manager 7.1.2.

### Device Support

This release introduces support for the following devices and their respective operating system versions:

- IOS-XR 7.11.2 release on Cisco NCS 560 devices
- IOS-XR 24.1.1 release on Cisco NCS 560 devices
- IOS-XR 7.11.2 release on Cisco NCS 5500 devices
- IOS-XR 24.1.1 release on Cisco NCS 5500 devices
- IOS-XR 7.11.2 release on Cisco ASR 9000 routers
- IOS-XR 24.1.1 release on Cisco ASR 9000 routers

- IOS-XR 7.11.2 release on Cisco NCS 5700 devices
- IOS-XR 24.1.1 release on Cisco NCS 5700 devices
- IOS-XR 7.11.2 release on Cisco NCS 540 devices
- IOS-XR 24.1.1 release on Cisco NCS 540 devices
- IOS-XR 7.11.2 release on Cisco NCS 540L devices
- IOS-XR 24.1.1 release on Cisco NCS 540L devices
- IOS-XR 7.11.2 release on Cisco 8000 series devices
- IOS-XR 24.1.1 release on Cisco 8000 series devices
- IOS-XR 7.11.2 release on Cisco IOS XRv 9000 series routers
- IOS-XR 24.1.1 release on Cisco IOS XRv 9000 series routers
- IOS-XR 7.11.2 release on Cisco NCS 1010 devices
- Support for pluggable optical amplifier ONS-QDD-OLS (QDD-EDFA) on Cisco NCS-57C3-MOD-SYS and Cisco NCS-57C3-MODS-SYS fixed chassis
- Support for pluggable optical amplifier ONS-QDD-OLS (QDD-EDFA) on Cisco NCS-55A2 series routers
- Support for pluggable optical amplifier ONS-QDD-OLS (QDD-EDFA) on Cisco NCS-57B1-5DSE-SYS fixed chassis
- Validation of IOS-XE 17.12.2 release on Cisco NCS 4200 and Cisco ASR 900 devices

### Optical

This release introduces support for the following optical modules and their respective devices:

- QDD-100G-ZR optical module on Cisco NCS 540 devices (version 7.9.1)
- QDD-100G-ZR optical module on Cisco NCS 560 devices (version 7.8.1)
- QDD-100G-ZR optical module on Cisco NCS 5500 devices (version 7.9.1)
- ONS-QDD-OLS optical module on Cisco 5500 devices (version 7.11.1)
- 400G-ER1 optical module on Cisco NCS 5500 devices (version 7.10.1)
- ONS-QDD-OLS optical module on Cisco NCS5700 (NCS-57C3-MOD-SYS and NCS-57C3-MODS-SYS & NCS-57B1-5DSE-SY)
- QDD-100G-ZR optical module on Cisco NCS 5700 devices (version 7.9.1)

## Functionality Changes Including Removed/Disabled Features

In the Cisco EPN Manager 7.1.2 release, the following features/functionality and menus were deprecated:

- **User Roles:**

The user roles **CLINetwork Admin** and **CLI Security Admin** have been deprecated. You can no longer create new roles with these designations using the following navigation: **Administration > Users > User and Roles > + (Create New User)**.

## New Operating System Support

This section lists the new OS support provided in Cisco EPN Manager 7.1.2. 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 Network Convergence System 5500 Series—New Operating System Support

Device Model	Device OS
Cisco NCS 5500 Series	IOS-XR 7.11.2
Cisco NCS 5500 Series	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco NCS 5700 Router	IOS-XR 7.11.2
Cisco NCS 5700 Router	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco 8000 Router	IOS-XR 7.11.2
Cisco 8000 Router	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco ASR 9000 Router	IOS-XR 7.11.2
Cisco ASR 9000 Router	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco IOS XRv 9000 Router	IOS-XR 7.11.2
Cisco IOS XRv 9000 Router	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco NCS 540 Router	IOS-XR 7.11.2
Cisco NCS 540 Router	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco NCS 540L Router	IOS-XR 7.11.2
Cisco NCS 540L Router	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco NCS 560 Router	IOS-XR 7.11.2
Cisco NCS 560 Router	IOS-XR 24.1.1

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

Device Model	Device OS
Cisco NCS 1010 Router	IOS-XR 7.11.2

## Supported Installation/Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 7.1.2 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 7.1.2
Cisco EPN Manager 5.1.4.1	<b>Cisco EPN Manager 5.1.4.1 &gt; 6.0.0 &gt; 6.1.0 &gt; 6.1.2 &gt; 7.1 &gt; 7.1.2</b>
Cisco EPN Manager 6.1.2	<b>Cisco EPN Manager 6.1.2 &gt; 7.1 &gt; 7.1.2</b>
Cisco EPN Manager 7.0.x	<b>Cisco EPN Manager 7.0.x &gt; 7.1 &gt; 7.1.2</b>
Cisco EPN Manager 7.1	<b>Cisco EPN Manager 7.1 &gt; 7.1.2</b>
Cisco EPN Manager 7.1.1	<b>Cisco EPN Manager 7.1.1 &gt; 7.1.2</b>

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 7.1.2 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 the 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.
- Begin an SSH session with the Cisco EPN Manager server and log in as a Cisco EPN Manager CLI admin user.
  - 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 functionality, 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](#).)

For further steps on installing an update for HA deployment, please refer to the following links:

- [Increase Session Timeout on Servers, on page 6](#)
  - [Remove HA Configuration, on page 7](#)
  - [Install the Device Pack and Point Patch on the Primary Server, on page 7](#)
  - [Install Cisco EPN Manager on the Secondary Server, on page 8](#)
  - [Enable HA and Verify HA Status, on page 9](#)
  - [Synchronize the Inventory of All Devices with the Database \(Existing Deployments Only\), on page 5](#)
- 

## 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 stop
ncs start
```
- 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 the Device Pack and Point Patch on the Primary Server

### Before you begin

Ensure you have the password (authentication key) that was created when HA was enabled, as it is needed to install the maintenance pack on the secondary server later. Verify that no backups are currently in progress.

### 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 the Secondary Server

**Before you begin**

On the secondary server, update the time zone using a soft link:

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

This ensures that the compliance server will be up and running on the secondary server after failover. Also, make sure that no backups are currently in progress.

**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 a 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 the Installation on the 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, and 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.
- Log in to the Cisco EPN Manager web GUI as a user with Administrator privileges.
  - In the left sidebar menu, choose **Administration > Settings > High Availability**.
  - 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.
  - 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 one or more virtual IP addresses.
  - Click **Save**, then wait until the servers are synchronized.
  - Verify that the Configuration Mode is HA Enabled.
- Step 2** Verify the primary server's HA status.
- Click HA Status on the left.
  - Check that the Current State Mode displays Primary Active.
- Step 3** Verify the secondary server's HA status.
- Log in to the secondary server's web page.
  - Enter the authentication key and click **Login**.
  - 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 that are made to the column order will be applicable only for the current session and will not be permanently saved in the database.

## Securing User Inputs to Prevent XSS Vulnerabilities

Cross-site Scripting (XSS) is a security vulnerability that allows attackers to inject malicious scripts into applications. These scripts can be used to steal information or perform other malicious actions. To safeguard the Cisco EPN Manager, it is crucial to avoid certain patterns in user input fields and POST/PUT payloads.

The following patterns have been identified as vulnerable and are blocked by the Cisco EPN Manager's XSS prevention feature. The Cisco EPN Manager will not execute the command or proceed to the next step if it finds these patterns; therefore, ensure they are not used in user inputs or API calls.

- `src='...'` (multiline, case insensitive pattern): Avoid using `src=` followed by any text or newline within single quotes. For example, `<img src='malicious_code'>`.
- `src="..."` (multiline, case insensitive pattern): Avoid using `src=` followed by any text or newline within double quotes. For example, ``.
- `</script>` (case insensitive pattern): Avoid using the closing script tag in any form.
- `<script...>` (multiline, case insensitive pattern): Avoid using the opening script tag with any content inside.
- `eval (...)` (multiline, case insensitive pattern): Avoid using the `eval` function in any context. For example, `eval('malicious_code')`.
- `expression(...)` (multiline, case insensitive pattern).
- `javascript:` (case insensitive pattern): Avoid using `javascript:` protocol in any field.
- `vbscript:` (case insensitive pattern): Avoid using `vbscript:` protocol.
- `onload..=` (multiline, case insensitive pattern): Avoid using event handlers like `onload` in any of the fields.
- `<...>` (multiline, case insensitive pattern).
- `<script.../script>` (multiline, case insensitive pattern): Avoid any complete script tags with content.

## 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 services 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 not 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 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, 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 subinterfaces in a Gig Port.

## Cisco EPN Manager Bugs

- [Open Bugs, on page 13](#)
- [Resolved Bugs, on page 14](#)
- [Closed Bugs, on page 15](#)
- [Get Information about Cisco EPN Manager Bugs, on page 15](#)

### 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 7.1.2 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                                                                     |
|----------------------------|---------------------------------------------------------------------------------|
| <a href="#">CSCwj15787</a> | License count is shown as 1 for consumed tokens                                 |
| <a href="#">CSCwi82342</a> | OTS ports that belongs to QDD-OLS pluggable have few issues on the chassis view |

## Resolved Bugs

The table below lists all the bugs that were resolved in the Cisco EPN Manager 7.1.2 release.

For more information about the resolved bugs, go to the [Bug Search Tool](#).

| Bugs                       | Description                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------|
| <a href="#">CSCwi63747</a> | Chassis view - Missing Power Module for Cisco 8808 IOS XR router                                   |
| <a href="#">CSCwi74601</a> | Virtual Domain does not display modified hostname for a device even after device sync is performed |
| <a href="#">CSCwi73704</a> | fault query causing DB hanging process and stale sessions till max session reached                 |
| <a href="#">CSCwi53331</a> | MPLS link latency data not seen in EPNM 7.1 UI for NCS5504/8 XR 7.2.1 devices.                     |
| <a href="#">CSCwi58415</a> | Non admin users cannot open the “alarms and events” under the user preferences menu                |
| <a href="#">CSCwi71390</a> | EPNM 7.1 - Duplicate entries seen in MPLS Link Delay Dashboard for NCS5508 IOS 7.2.1 devices       |
| <a href="#">CSCwi73428</a> | Lag8023dAggPort entry of PEP is set as null for port channel causing null description with Alarms  |
| <a href="#">CSCwi75048</a> | TransportDisconnectedThreshold error on failback                                                   |
| <a href="#">CSCwj01420</a> | EPNM - CLI users not created properly from GUI                                                     |
| <a href="#">CSCwj12521</a> | EPNM SWIM Device Image import failure                                                              |
| <a href="#">CSCwi47489</a> | EPNM 7.0 - no rows is displayed in Virtual Domains tables on Windows VM                            |
| <a href="#">CSCwi58653</a> | Port labels are swapped for devices of type 8201 and 57B1 devices                                  |
| <a href="#">CSCwi67206</a> | Aend and Zend Devices are not ordered uniformly across all dashlets in CEM                         |
| <a href="#">CSCwi71032</a> | Missing bind-utils in EPNM 7.1.x                                                                   |
| <a href="#">CSCwi82908</a> | NCS540 - N540X-ACC-SYS displayed as NCS540-24Z8Q2C-M                                               |
| <a href="#">CSCwi91072</a> | Reason for maintenance is not persisted while we move devices to maintenance mode.                 |
| <a href="#">CSCwi93779</a> | EPNM 7.1.1.0- Provisioning a serial circuit Fails for ios-xe 16.x devices                          |
| <a href="#">CSCwj14310</a> | Failed to save scheduled reports for CET timezone                                                  |
| <a href="#">CSCwj26700</a> | Image family and version of software images/SMUs for XRv9k are UNKNOWN                             |
| <a href="#">CSCwj48381</a> | NCS 1004 - Strange issue with NCS 1004 1.2T card LF alarm                                          |

| Bugs                       | Description                                       |
|----------------------------|---------------------------------------------------|
| <a href="#">CSCwj48379</a> | NCS 1004 - OTN objects are missing for Line cards |

## Closed Bugs

The table below lists all the bugs that were closed in the Cisco EPN Manager 7.1.2 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                                                              |
|----------------------------|--------------------------------------------------------------------------|
| <a href="#">CSCwm52933</a> | The side menu of Features & Technologies is not translated into Japanese |

## 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](#).
- 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.

---

## Related Documentation

For a list of all documentation available for Cisco EPN Manager 7.1.2, see the [Cisco Evolved Programmable Network Manager 7.1 Documentation](#).

## Accessibility Features

For a list of accessibility features in Cisco EPN Manager 7.1.2, contact [accessibility@cisco.com](mailto: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](mailto: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.

