Cisco Evolved Programmable Network Manager 6.0.2 Device Pack and Point Patch

May 24, 2022

This document provides information and installation instructions for Cisco EPN Manager 6.0 Device Pack and Point Patch 2 (Cisco EPN Manager 6.0.2). The Device Pack and Point Patch must be installed on top of Cisco EPN Manager 6.0/6.0.x.

Contents

Important Notes

- As of Cisco EPNM 3.1.3 release, root user login for the Linux CLI will be disabled.

  If you wish to re-enable root user login you will need to manually edit the file:

  `/etc/ssh/sshd_config`

  Change the value of **PermitRootLogin** no to yes.

  Reload sshd:

  #systemctl reload sshd.service

What’s New in Cisco EPN Manager 6.0.2

- Upgrade from 6.0.x to 6.0.2
- NCS2K 11.1.2.3 OS Validation
- NCS4K 6.5.32 Validation
- Support of IOS-XR 7.5.2 on ASR9K 64 bit
- Support for IOS XR 7.6.1 and NCS540
- Support of IOS-XR 7.5.2 on NCS5500/NCS5700
- Support of IOS-XR 7.5.2 on NCS560
- Support of IOS-XR 7.5.2 on Cisco 8000
- Support of IOS-XR 7.5.2 on XRv9000
- Support of IOS-XR 7.6.1 on NCS560
- Support of IOS-XR 7.6.1 on NCS5500/NCS5700
- Support of IOS-XR 7.6.1 on Cisco ASR9K devices
- Support for IOS-XR 7.6.1 and XRv9000
- Support of IOS-XR 7.5.2 on NCS540
- Support for Cisco N540-6Z14S-SYS-D with IOS-XR 7.5.2
- Support for Cisco NCS-57C1-48Q6-SYS with IOS-XR 7.5.2 on NCS5700
- Chassis view support for Cisco NCS-57C1-48Q6-SYS with IOS-XR 7.5.2 on NCS5700
- Chassis view support for Cisco N540-6Z14S-SYS-D
- Support for Cisco 8202-32FH-M with IOS-XR 7.5.2
- Chassis view support for Cisco 8202-32FH-M
- Validation of CRS and IOS-XR 6.7.4
- Validation of IOS XE 17.7.1 on NCS4200/ASR900
- Add support for NCS1004 OTN-XPL in EPNM
- Validation of IOS XE 17.6.2/3 on NCS4200/ASR900
- Validation of IOS XE 17.8.1 on NCS4200/ASR900
- NCS2K SVO circuit soak time should not apply to restoration and revert equally
- Implementing Netconf Replay feature for NCS2K devices
- NCS2K SVO to re-establish Netconf streams based on SWTICH DOWN Clear event
- NCS2K SVO Automatic recovery of circuit from Partial state
- NCS2K SVO to do a full sync of the NE after receiving Sync completed event
- NCS2K SVO to have constant restoration time (i.e., 5 mins in WSON) instead of exponential restoration time across restoration retry attempts.

Known Defects in Cisco EPN Manager 6.0.2

Identifier	Headline
CSCwb57844	Satellite Devices are going to CF state due to iccpgroupsettings
CSCwb59989	6.0.2 GA: optical ctrl ports appear in l2vpn creation for ncs4k devices which shouldn't
CSCwb60776	BGP Neighbor details missing
CSCwb75340	6.0.2 GA: brownfield evp-tree modification throws error on XE device
CSCwb76010	Top N CE/L3VPN performance tab detach page service name hyperlink is not working
CSCwb81793	Getting Hop-empty error while provisioning of CEM service
CSCwb82974	EPNM_6_0_2_NCS5500: Commit is failing in Activation and commit job with error - CPU Nodes are down
CSCwb84451	Team interface or secondary management interface IPv6 address not accessible
CSCwb85811	Monitoring policy custom MIB polling is showing only router type devices to test individual device
CSCwb86147	Verify Credentials and Node Sync failing at EPNM for TACACS/Radius Enabled 2K Nodes
CSCwb87022	Monitoring policies export file output details are different from GUI details
CSCwb68437	Software Updates type and drop-down filter option showing Prime Add-Ons
CSCwb72654	SONET Higher-order and Lower-order Paths recovered clock Id is mandatory parameter
CSCwb73935	SONET & SDH Lower-order Paths wrong configuration is not showing meaningful error
CSCwb74846	ASR9k XRv does not support MEF option resulting in deployment failure of CE
CSCwb77184	After Launching BERT UI, the System Settings options no longer accessible
CSCwb82168	Device -> Inventory row height is high for part of the rows
CSCwb82214	Module port interfaces and ip interfaces missing in Wired Detailed Device Inventory report for SVO
CSCwb84514	"Performance Measurement Probes" table in EVPL provisioning fields width should be wider
CSCwb86270	QoS Egress Policy is not including deploying all the Policer Action options
CSCwb86458	QoS Egress Policy is rejected by 903 device, but not detected by Provisioning wizard
CSCwb87191	Last Activated time details are not showing correctly for monitoring polices are located in folder
CSCwb81066	Error message and help tip changes on Serial Service flow
CSCwb86834	Select all checkbox is not enabling by default in monitoring policy device selection detail page

Defects fixed in Cisco EPN Manager 6.0.2

Identifier	Headline
CSCwa68748	CIAM: expat - 2.1.0
CSCwa77560	alarm notification policy select all followed by individual alarm unselect creates wrong policy
CSCwa86907	CIAM: xstream 1.4.18 CVE-2021-43859
CSCwb11653	EPNM HA Fail over with Simultaneous fiber cut fails restoration
CSCwb23668	Start time is coming wrong in Replay feature. Due to which Collection Failure is there
CSCwb30946	TIM-B Setup with Router NC560 Circuits if deleted cannot be recreated due to stale entries
CSCwb35978	SVO HA switchover + Fiber cut is making devices in Collection failure
CSCwb36916	EPNM_6_0_2_CRSDevice: Import image(.tar) job from EPNM shows partially failed for CRS device
CSCwb36966	EPNM_6_0_2_CRSDevice: Downgrade CRS device shows "Not Applicable" in distribution location
CSCwb38007	TIM-B Setup real fiber cut makes circuits stuck in restoring state only
CSCwb38101	EPNM Memory leak is making epnm down with the NMS memory leak
CSCwb45266	Real NE Disconnect by doing power down, Circuit restoration Failed with PCE Error
CSCwb84434	EPNM6.0.2: Nessus Detects Vulnerabilities
CSCvz97671	NCS2K: Particular OCHCC WSON circuit is Partial in EPNM and related cc info from trail missing
CSCwa56226	Some of the circuits going into partial state after migration
CSCwa57168	No headings are marked
CSCwa57197	Circuits of one User Group is displayed under another User Group
CSCwa70523	Terminate of MCH Group service fails, whereas from UI same is working fine.
CSCwa71912	End points are not displaying on SVO device while creating circuit
CSCwa74076	NCS1004: Actual Frequency/Wavelenth have few issues
CSCwa85013	upgrade to log4j 2.17.1
CSCwa87330	Online Help page not accessible for any users other than root and super user
CSCwa94989	GET API on POST-triggered OTDR scan file works partially only after GUI OTDR scan data download
CSCwa95775	For performed OTDR scan from NBI, difference in report file size for downloaded from NBI and UI
CSCwb00635	Breakout port shown as opticsx/x/x/x instead of TenGigx/x/x/x on card NC55-24H12F-SE of NCS5504
CSCwb02929	EPNM 5.1.4 - Incorrect corePoolSize & maxPoolSize values in inventory for express Profile
CSCwb06849	Install Guide 6.0 changes
CSCwb07385	Smart Software License registration failing due to communication send error
CSCwb14130	line config in running-config is parsed incorrectly if line config are combined (RS232)

Identifier	Headline
CSCwb16379	LDAP SSL authentication is not working
CSCwb16840	Stale Entries are left in EPNM Data Base
CSCwb17991	Auto Revert is making circuits in partial state
CSCwb22508	Fake Loss is getting generated after multiple operations like Fiber Cut, NE Disconnection etc
CSCwb22532	Circuit remains in partial after NE-DISCONNECT clear
CSCwb23759	EPNM 6.1 & 6.0.1 - physical link/LAG down status is not updated as expected within 60 sec
CSCwb23975	Cleared alarm tab header count is showing 0 and alarms tab header name change required
CSCwb26389	Fake NETCONF Alarm is getting generated in EPNM when disconnecting SVO container
CSCwb33245	No data Available is seen while changing Max hops values and including/excluding nodes
CSCwb33882	MPLSTE BGP L3Link amend fails with port based configuration on XR devices
CSCwb36536	PSU and Fan modules are not shown in Inventory Device Details for CRS device with IOS-XR
CSCwb36769	MPLS Link delay- add support for XR 7.3.1 devices
CSCwb46469	EPNM HA switch over +Fiber cut SIP doesn’t clear from a circuit
CSCwb48219	EPNM try Auto revert when NE Disconnect on any device on Main path
CSCwb49339	Auto Revert with SVO down Circuit in partial state - Repair and resync not getting triggered
CSCwb53536	EPNM_6_0_2_CRSDevice: Commit is failing in Activate and Commit job as device is not ready to commit
CSCwb54887	BFD template association is not happening post WAE response
CSCwb55162	CSCvz98965 is not resolved in 6.0 since wrong artifact is released xmp_snmp_sessionmgr-3.855.0.jar
CSCwb60327	Restoration of restored-revertible circuit is failing; circuit is getting stuck in RESTORING state
CSCwb60417	Warning messages in EPNM has to be aligned with wae responses
CSCwb60744	Devices are stuck in Maintenance state
CSCwb65764	OOM on ActiveMQ
CSCwb68491	Include the string "noInterfaceSelected" when no interface is selected in INCLUDE/EXCLUDE table
CSCwb71148	EPNM 6.0 installation Guide - remove reference of CSCvy23276
CSCwb80321	6.0.2: elib_11123: Realtime service PM showing Blank screen so unable to check the Realtime service PM
CSCvz95522	NCS2K: Some ochtrail/ochcc wson circuits are showing 2 entries for wavelength
CSCvz95559	NCS2K: Restoration config is showing as None in-circuit table, but is correct in circuit 360
CSCwa74971	NCS4k: TCM: Enabling Performance Monitor is not working, it is always goes to disabled
CSCwa91691	Alarm summary page annotations showing as UTC time instead of server or local UI client time
CSCwa94994	GET API downloaded OTDR (triggered by POST) SOR file name not the same as GUI export file name

Identifier	Headline
CSCwa95404	OTDR: OTDR with geo map and X-axis plot issue if 2 rows selected
CSCwb14977	Save and Test are disabled in Smart License settings
CSCwb16177	Alarm not supported for deletion getting deleted with other alarms
CSCwb16487	We request to add the following certified upgrade path in Installation Guide
CSCwb17982	Details page is showing Planed revert and planed time for Manual revert
CSCwb23007	License Dashboard is showing Smart License
CSCwb30615	Validation required for "Duration for the Alarms & Events Replay for SVO devices" field
CSCwb33872	Filtering for ISIS as technology in the topology map shows all the links
CSCwb38228	Alarm summary page alarms are showing 12 hours format time instead of 24 hours format
CSCwb42909	XFT Failure Multi-Threaded Execution Fails on 6.0.2 causing builds UNSTABLE
CSCwb49508	Failure source is not populating for collection failure alarms
CSCwb71220	Alarm ID hyperlink page annotation update time is showing as UTC time with local time zone
CSCwa35291	SVO: EPNM Circuit Restoration Configuration Restorable Circuit in RESTORED Status
CSCwb03047	Circuit in PARTIAL state after NE-DISCONNECT CLEAR event with Revert as Manual/Automatic
CSCwb04517	Pom changes for optical content cepnm6.0PI_DPP2
CSCwa95404	OTDR: OTDR with geo map and X-axis plot issue if 2 rows selected

Obtaining and Installing the Cisco EPN Manager 6.0.2 Device Pack and Point Patch

This procedure describes how to download and install Cisco EPN Manager 6.0.2 on top of an existing Cisco EPN Manager 6.0/6.0.1 installation.

Prerequisites

Cisco EPNM 6.0/6.0.1.

Non-HA Deployment

Downloading and installing the update

1. From the left sidebar, choose **Administration > Licenses and Software Update > Software Update**.
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 **cepnm6.0-dppX- buildxxx.ubf**.
3. Depending on the location the file was saved to, select either **Upload from local computer** or **Copy from server's local disk**.
4. Once the file has been loaded, Click the ***Install*** button associated with EPN Manager update.
5. Click ***Yes*** in the confirmation message pop-up window to proceed with the installation.

   Note: The server will restart when the installation is complete.
6. If you are asked whether to overwrite an existing file, click ***Yes***.

   After successful installation, the status will change to Installed. Cisco EPN Manager will auto-restart and the Cisco EPN Manager web GUI will not be accessible for some time (may take up to 1 hour).
7. Check the status of the Cisco EPN Manager services.

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

   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: For optimal Cisco EPN Manager functionality, all services should be up and running.
8. When the Cisco EPN Manager web GUI is accessible, log in and check that the Patch status is "Installed" in the Software Update page.

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

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

If you have already been using a previous version of Cisco EPN Manager (i.e., this is not a fresh installation), you need to perform a Sync operation on the devices. The Sync operation instructs Cisco EPN Manager to collect device physical and logical inventory and save the information to the database.

1. Choose **Monitor > Network Devices**.
2. Select all devices, then click ***Sync***.

HA Deployment

Install Cisco EPN Manager 6.0.2 in a High Availability Environment.

Note: 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. See the Cisco Evolved Programmable Network Manager 6.0.0 User and Administrator Guide for more information.

Increase the Session Timeout on the Servers

Before You Begin

- During the patching of the primary and secondary HA servers, both servers will be down.
- 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.
- Backup your data (for instructions on how to backup your data, refer to the Cisco Evolved Programmable Network Manager 6.0.0 User and Administrator Guide).

Increase the timeout on the primary and secondary servers from 30 minutes to 90 minutes, as follows:

1. Log in as the Linux CLI root user.
2. Save a backup of the ***web.xml*** file 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
3. In the web.xml file (/opt/CSCOlumos/tomcatSWUpdate/webapps/ROOT/WEB-INF/web.xml), search for the following: **<session-timeout>30</session-timeout>**
4. Change the session timeout to 90 minutes: **<session-timeout>90</session-timeout>**
5. As the Cisco EPN Manager CLI admin user, manually stop and restart the server:

   ```
   ncs stop
   ncs start
   ```
6. Ensure that all services are up and running by running this command:

   ```
   ncs status
   ```

Remove the HA Configuration

1. Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.

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

3. Click HA Configuration tab.

4. Click ***Remove***.

5. On the primary server, navigate to **Administration > Settings > High Availability** and confirm that the Configuration Mode field displays "**HA Not Configured**".

6. Log into the secondary server's health monitor page https://serverIP:8082 and confirm that "**HA not Configured**" appears under the State Column.

Install the Device Pack and Point Patch on the Primary and Secondary Servers (HA Deployment).

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.
- Make sure no backups are in progress.
- On the secondary server, update the time zone using a soft link (the following command is one line):

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

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

Install the Device Pack and Point Patch on the Primary Server

1. From the left sidebar, choose **Administration > Licenses and Software Update > Software Update**.
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 **cepnm6.0-dppX- buildxxx.ubf**
3. Depending on the location the file was saved to, select either **Upload from local computer** or **Copy from server's local disk**.
4. Once the file has been loaded, Click the ***Install*** button associated with EPN Manager update.
5. 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 1 hour).
6. 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 6.0.x on the secondary server

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

   ```
   https://serverIP:8082
   ```

   Where serverIP is the IP address or host name of the secondary server.
2. Enter the authentication key and click ***Login***.
3. Click the ***Software Update*** button.
4. You will be transferred to a login page. Login to EPNM as administrator.
5. 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 **cepnm6.0-dppX- buildxxx.ubf**
6. Depending on the location the file was saved to, select either Upload from local computer or Copy from server's local disk.
7. 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 1 hour).

Verify the installation on the secondary server

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

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.
3. Once the web GUI is accessible, verify the installation and version in the secondary server's HM web page. Enter the following URL in your browser: `https://serverIP:8087`

   Where serverIP is the IP address or host name of the secondary server.
4. Enter the authentication key and click ***Login***.
5. In the Uploaded Update Files tab, verify that the MPx ubf file (in the format **cepnm.6.0-dpX- buildxxx.ubf**) is listed and that the "in Use" status is ***Yes***.
6. Ensure that all services are up and running by running this command:

```
ncs status
```

Enable high availability and verify HA status

1. Enable high availability.
   1. Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.
   2. From the left sidebar menu, choose **Administration > Settings > High Availability**.
   3. Click HA Configuration Tab, then enter the secondary server's IP address, the secondary server's authentication key, and an email address to which Cisco EPN Manager should send HA state change notifications.
   4. 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 virtual IP address(es).
   5. Click **Save**, then wait until the servers are synchronized.
   6. Verify that the Configuration Mode is HA Enabled.
2. Verify the primary server's HA status.
   1. Click **HA Configuration** tab.
   2. Verify that the server's status is "Primary Active" under **HA Configuration mode**.
3. Verify the secondary server's HA status.
   1. Log into the secondary server's HM web page by entering the following URL in your browser:

      https://serverIP:8082

      Where serverIP is the IP address or host name of the secondary server.
   2. Enter the authentication key and click ***Login***.
   3. Verify that the status is a Green Check Mark and the State is "Secondary Synching".

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

If you have already been using a previous version of Cisco EPN Manager (i.e., this is not a fresh installation), you need to perform a Sync operation on the devices. The Sync operation instructs Cisco EPN Manager to collect device physical and logical inventory and save the information to the database.

1. Choose **Monitor > Network Devices**.
2. Select all devices, then click ***Sync***.

Synchronize the Hardware and NTP Clock

This procedure synchronizes the hardware clock with the NTP clock using the hwclock command.

1. Log in as the Linux CLI root user.
2. Check the NTP service status and ensure that NTP has obtained a stable time reference using the following commands. The following includes examples of the output you should see.

- Ensure that ntpd is running.

  ```
  service ntpd status
  ```

  ```
  ntpd (pid 3290) is running...
  ```

- If ntpd (pid 3290) is not running, start it using the following command:

  ```
  service ntpd start
  ```

  (Recheck ntpd status to ensure it is running).

- Ensure that NTP is receiving time from an NTP server.

  ```
  ntpstat
  ```

  ```
  synchronised to NTP server (10.116.134.075) at stratum 3 time correct to within 62
  ms polling server every 1024 s
  ```

  If you do not see output similar to this, then NTP synchronization has not yet occurred. Wait a few minutes and run ntpstat again. If synchronization does not happen within 10 minutes, contact your system administrator or Cisco support.

3. Synchronize the hardware clock with NTP using the following command:

   ```
   hwclock --systohc --debug
   ```

   You should see output similar to the following:

   ```
   hwclock from util-linux-ng 2.17.2
   Using /dev interface to clock.
   Last drift adjustment done at 1470117750 seconds after 1969
   Last calibration done at 1470117750 seconds after 1969
   Hardware clock is on local time
   Assuming hardware clock is kept in local time.
   Waiting for clock tick...
   ...got clock tick
   Time read from Hardware Clock: 2021/08/02 16:03:30
   Hw clock time: 2021/08/02 16:03:30 = 1470117810 seconds since 1969
   1470117810.500000 is close enough to 1470117810.500000 (0.000000 < 0.001000)
   ```

```
Set RTC to 1470117810 (1470117810 + 0; refsystime = 1470117810.000000)
Setting Hardware Clock to 16:03:30 = 1470117810 seconds since 1969
ioctl(RTC_SET_TIME) was successful.
Not adjusting drift factor because it has been less than a day since the last calibration.
root$
```

4. Verify that the hardware clock is synchronized with NTP.

   ```
   echo "hwclock is: $(hwclock --show)" ; echo "linux clock is: $(date)";
   ```

   Check the output and ensure that the two clocks are synchronized (to at least within a few seconds of each other):

   ```
   Hwclock is: Tue 26 Jul 2021 06:11:40 PM AEST -0.391028 secondslinux clock is: Tue Jul 26
   18:11:40
   AEST 2021
   ```

5. As the Linux CLI admin user, restart the Cisco EPN Manager services.

- If you are logged in as the Linux CLI root user, switch to the Linux CLI admin user.

  exit

- Switch to the Cisco EPN Manager CLI admin user.
- Stop and restart the Cisco EPN Manager services.

  ncs stop

  ncs start

Obtaining Documentation, Support and Security Guidelines

For information on obtaining documentation, obtaining suspport, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.