



# Upgrading Cisco DCNM

This chapter provides information about upgrading Cisco DCNM, and contains the following section:

- [Upgrading to Cisco DCNM Release 11.5\(1\), on page 1](#)
- [Upgrading ISO or OVA through Inline Upgrade, on page 1](#)
- [Dropping Performance Manager Data, on page 8](#)

## Upgrading to Cisco DCNM Release 11.5(1)

Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM Release 11.3(1), you can install Cisco DCNM for SAN Deployment on both OVA and ISO virtual appliances.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.5(1).

**Table 1: Type of Upgrade for IP for Media (IPFM) deployments**

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.4(1)	Inline Upgrade
11.3(1)	Inline Upgrade
11.2(1)	Inline Upgrade
11.1(1)	11.1(1) → 11.2(1) → 11.5(1) 11.1(1) → 11.3(1) → 11.5(1) 11.1(1) → 11.4(1) → 11.5(1) → represents an Inline Upgrade

## Upgrading ISO or OVA through Inline Upgrade

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

When you install Cisco DCNM, a self-signed certificate is installed, by default. However, after upgrading to the latest Cisco DCNM Release, you must restore the certificates.




---

**Note** Restoring certificates is a disruptive mechanism; it requires you to stop and restart applications. Restore the certificates only when the upgraded system is stable, that is, you must be able to login to Cisco DCNM Web UI.

---

To restore certificates after upgrade, see [Restoring the certificates after an upgrade](#).

This section contains the procedure to upgrade the DCNM using the Inline Upgrade method.




---

**Note** For Classic LAN Deployment upgrade, the deployment is automatically converted to LAN Fabric deployment mode when you upgrade to DCNM Release 11.5(1).

---

## Inline Upgrade for DCNM Virtual Appliance in Standalone Mode

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

Perform the following task to upgrade the DCNM virtual appliance in standalone mode.

### Procedure

---

**Step 1** Log on to the Cisco DCNM appliance console.

**Caution** If the system requirements do not meet the minimum resource requirements, every time you log on to DCNM via the console or SSH, **SYSTEM RESOURCE ERROR** is displayed. Modify the system requirements logon to DCNM via Console/SSH.

- For OVA Installation: On the OVF template deployed for the host, right click and select **Settings > Launch Web Console**.
- For ISO Installation: Select the KVM console or UCS (Bare Metal) console.

**Caution** Do not perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.

OR

Run the following command to create a screen session.

```
dcnm# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

**Step 2** Take a backup of the application data using the **appmgr backup** command.

```
dcnm# appmgr backup
```

Copy the backup file to a safe location outside the DCNM server.

**Step 3** Log on to the `/root/` directory, by using the `su` command.

```
dcnm# su
Enter password: <<enter-password>>
[root@dcnm]#
```

**Note** Ensure that you have access to the `/root/` folder before you mount the ISO to the directory.

**Step 4** Unzip the `dcnm-va.11.5.1.iso.zip` file and upload the DCNM 11.5(1) ISO file to the `/root/` folder in the DCNM setup that you want to upgrade.

**Step 5** Create folder that is named `iso` using the `mkdir /mnt/iso` command.

```
[root@dcnm]# mkdir /mnt/iso
```

**Step 6** Mount the DCNM 11.5(1) ISO file on the standalone setup in the `/mnt/iso` folder.

**mount -o loop <DCNM 11.5(1) image> /mnt/iso**

```
[root@dcnm]# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

**Step 7** Navigate to `/mnt/iso/packaged-files/scripts/` and run the `./inline-upgrade.sh` script.

```
[root@dcnm]# cd /mnt/iso/packaged-files/scripts/
dcnm# ./inline-upgrade.sh
Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]: y
```

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.2(1) only.

**Step 8** Provide the new sysadmin user password at the prompt:

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.2(1) only.

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use `sysadmin` user.

As the Elasticsearch versions in earlier releases is not compatible with the Elasticsearch supported with 11.5(1), you must reindex the Elasticsearch data after upgrading to Release 11.5(1).

The following message is generated:

```
*****
WARNING: Elasticsearch indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
Check DCNM installation and upgrade guide for more details.
*****
```

A confirmation message appears. Enter `y` to continue to upgrade.

The system reboots after upgrade.

**Step 9** Ensure that the DCNM application is functional, by using the `appmgr status all` command.

```
[root@dcnm]# appmgr status all
```

**Step 10** To verify that you have successfully installed the Cisco DCNM Release 11.5(1), use the `appmgr show version` command.

```
[root@dcnm]# appmgr show version

Cisco Data Center Network Manager
Version: 11.5(1)
Install mode: Media Controller
Standalone node. HA not enabled.
```

**Step 11** Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm]# exit
```

**Step 12** Unmount the **dcnm-va-patch.11.5.1.iso** file from the DCNM setup.

**Note** You must terminate the screen session before unmounting the **.iso** file.

```
[root@dcnm]# umount /mnt/iso
```

---

### What to do next

Log on to the DCNM Web UI with appropriate credentials.



**Note** In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(1), the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

Click **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

The old PM data is retained in Elasticsearch. Elasticsearch shows as reindex required on Cisco DCNM **Web UI > Dashboard > Health** and **Administration > DCNM Server > Server Status**.

If you choose to conserve the Performance Manager data when you upgrade to Release 11.5(1), we recommend that you contact Cisco TAC for further assistance.

If you choose to conserve the Performance Manager data, we recommend that you contact Cisco TAC for further assistance.

## Inline Upgrade for DCNM Virtual Appliance in Native HA Mode

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

Perform the following task to upgrade the DCNM virtual appliance in Native HA mode.

### Before you begin

- Ensure that both the Cisco DCNM Active and Standby peers are up and running.

- Before upgrading Cisco DCNM in Clustered mode, stop the Network Insights - Resources (NIR) 2.x application. On the Cisco DCNM Web UI, choose **Applications > Catalog**. On the NIR app, click Stop icon to stop the application. Click Delete to remove the application from the Catalog.




---

**Note** Inline upgrade of Cisco DCNM in Clustered mode is supported from Release 11.2(1). Release 11.1(1) doesn't support inline upgrade for DCNM in clustered mode.

---

- Check and ensure that the Active and Standby servers are operational, using the **appmgr show ha-role** command.

Example:

On the Active node:

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node:

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

## Procedure

---

**Step 1** Unzip the `dcnm-va.11.5.1.iso.zip` file and upload the DCNM 11.5 (1) ISO file to the `/root/` folder in both Active and Standby node of the DCNM setup that you want to upgrade.

**Note** For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

**Step 2** Log on to the Cisco DCNM appliance console.

**Caution** If the system requirements do not meet the minimum resource requirements, every time you log on to DCNM via the console or SSH, **SYSTEM RESOURCE ERROR** is displayed. Modify the system requirements log on to DCNM via Console/SSH.

- For OVA Installation: On the OVF template that is deployed for the host, right click and select **Settings > Launch Web Console**.
- For ISO Installation: Select the KVM console or UCS (Bare Metal) console.

**Caution** Do not perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.

OR

Run the following command to create a screen session.

```
dcnm1# screen
dcnm2# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

- Step 3** Take a backup of the application data using the **appmgr backup** command on both Active and Standby appliances.

```
dcnm1# appmgr backup
dcnm2# appmgr backup
```

Copy the backup file to a safe location outside the DCNM server.

- Step 4** Log on to the **/root/** directory by using the **su** command.

```
dcnm1# su
Enter password: <<enter-password>>
[root@dcnm1]#
```

```
dcnm2# su
Enter password: <<enter-password>>
[root@dcnm2]#
```

**Note** Ensure that you have access to the **/root/** folder before you mount the ISO to the directory.

- Step 5** On the Active node, perform the inline upgrade.

- a) Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm1]# mkdir /mnt/iso
```

- b) Mount the DCNM 11.5(1) ISO file on the Active node in the **/mnt/iso** folder.

```
[root@dcnm1]# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

- c) Navigate to **/mnt/iso/packaged-files/scripts/** location and run the **./inline-upgrade.sh** script.

```
[root@dcnm1]# cd /mnt/iso/packaged-files/scripts/
dcnm1# ./inline-upgrade.sh
```

**Note** If some services are still running, you will receive a prompt that the services will be stopped. When prompted, press **y** to continue.

```
[root@dcnm1]# Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]:
y
```

- d) Provide the new sysadmin user password at the prompt:

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

As the Elasticsearch versions in earlier releases is not compatible with the Elasticsearch supported with 11.5(1), you must reindex the Elasticsearch data after upgrading to Release 11.5(1).

The following message is generated:

```
*****
WARNING: Elasticsearch indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
Check DCNM installation and upgrade guide for more details.
*****
```

A confirmation message appears. Enter **y** to continue to upgrade.

The system reboots after upgrade.

- e) Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm1]# appmgr status all
```

**Note** Ensure that all the services are up and running on the Cisco DCNM Active node before proceeding to upgrade Standby node.

- f) Verify the role of the Active node, by using **appmgr show ha-role** command. Current role must show as Active.

```
[root@dcnm1]# appmgr show ha-role
```

```
Native HA enabled.
Deployed role: Active
Current role: Active
```

**Warning** We recommend that you do not continue to upgrade the Standby node, unless the Active node Current role is Active.

**Step 6** On the Standby node, perform the inline upgrade.

- a) Create folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm2]# mkdir /mnt/iso
```

- b) Mount the DCNM 11.5(1) ISO file on the Standby node in the **/mnt/iso** folder.

```
[root@dcnm2]# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

- c) Navigate to **/mnt/iso/packaged-files/scripts/** location and run the **./inline-upgrade.sh** script.

```
[root@dcnm2]# cd /mnt/iso/packaged-files/scripts/
dcnm2# ./inline-upgrade.sh --standby
```

**Note** If some services are still running, you will receive a prompt that the services will be stopped. When prompted, press **y** and continue.

```
[root@dcnm2]# Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]:
y
```

- d) Provide the new sysadmin user password at the prompt:

**Note** The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

After the upgrade is complete, the appliance reboots. Verify the role of the appliance, using the following command:

```
[root@dcnm2]# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

**Step 7** Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm1]# exit
[root@dcnm2]# exit
```

**Step 8** Unmount the **dcnm-va-patch.11.5.1.iso** file in both Active and Standby node of the DCNM setup.

**Note** You must terminate the screen session before unmounting the **.iso** file.

```
[root@dcnm1]# umount /mnt/iso
[root@dcnm2]# umount /mnt/iso
```

---

### What to do next

Log on to the DCNM Web UI with appropriate credentials.




---

**Note** In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(1), the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

---

Click **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

The old PM data is retained in Elasticsearch. Elasticsearch shows as reindex required on Cisco DCNM **Web UI > Dashboard > Health** and **Administration > DCNM Server > Server Status**.

If you choose to conserve the Performance Manager data, we recommend that you contact Cisco TAC for further assistance.

Verify the role of both the appliances using the **appmgr show ha-role**

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Verify the status of all applications using the **appmgr status all** command.

## Dropping Performance Manager Data




---

**Note** If you choose to conserve the Performance Manager data when you upgrade to Release 11.5(1), we recommend that you contact Cisco TAC for further assistance.

---



To drop the Performance Manager (PM) data, perform the following steps:

### Before you begin

- Ensure that the DCNM appliance is operational. (for standalone upgrade)
- If you have a Federation setup, ensure that all the nodes in the DCNM Federation setup are operational. (for Federation setup)

### Procedure

**Step 1** Launch the SSH session and run the following command to view the PMDB indices.

Identify the PMDB indices in the performance manager database.

#### For example:

```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
```

```

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left     Speed
100 2448    100 2448    0     0   4523      0  --:--:--  --:--:--  --:--:--  4524
green open pmdb_cpumemdata          rb-CJf-NR0my8M3mO-7QkA 5 1  7286    0
1.4mb 760.2kb
green open pmdb_ethintfratedata      P18gMKdPTkCODv0TomYAdw 5 1  9283    0
2.4mb  1.2mb

```

You will see indices prefixed with "pmdb\_"

**Step 2** On the Cisco DCNM Web UI, choose **Administration > Performance Setup > LAN Collections**.

Uncheck all the check boxes and click **Apply** to disable all switches and collections.

## Administration / Performance Setup / LAN Collections

For all selected licensed LAN Switches collect:  Trunks  Access  Errors & Discards  Temperature Sensor

Apply

Performance Default Polling Interval 5 Mins

- Fab-1-externalfab
  - 9k\_aragon
  - C93108TC-FX\_116
  - C93108TC-FX\_41
  - n3k\_72
  - N77-TGEN-195
  - N9k\_27
  - N9K-C9232C\_28
  - N9K-C9364C\_49
  - N9K-C9504\_44
  - sugarbowl\_56
  - suharbowl\_57
- Fab-2-ClassicLAN
  - N3k\_Utopia\_70
  - switch
- Fab3-otherswitches
  - IND13-P1-A1
  - N6K-96Q-63
- test
- Default\_LAN

**Step 3** Choose **Administration > DCNM Server > Server Status**.

**Step 4** Against the **Performance Collector** service, click the stop icon in the Actions column to stop the data collection.

DCNM Server	Actions	Service Name	Status
localhost		Database Server	Running
10.106.228.37		dexer	Last updated: 2020-12-13 16:30:00
10.106.228.37		Performance Collector	Stopped
10.106.228.37		Agent	Running
10.106.228.37		Elasticsearch	Status:yellow, Docs: pmdb_*=0
0.0.0.0:123		NTPD Server	Running
0.0.0.0:67		DHCP Server	Running
0.0.0.0:2162		SNMP Traps	Running
0.0.0.0:514		Syslog Server	Running

**Step 5** Click the delete icon to clean the Performance Manager database.

This action deletes the stale entries in the performance manager database.

**Step 6** Click on the reinitialize icon to reindex the Elasticsearch database schema.

This operation cleans the performance manager data in the Elasticsearch database and restarts the performance manager. It may take a few minutes to complete.

**Step 7** Click **Continue**.

The status of the Performance Collector service shows **Stopped**.

**Step 8** Ensure that you've deleted all the PMDB entries using the following command:

- For upgrading from Release 11.1(1)
 

```
curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
```
- For upgrading from Release 11.2(1)
 

```
curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
```
- For upgrading from Release 11.3(1)
 

```
curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
```
- For upgrading from Release 11.4(1)
 

```
curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
```

**For example:**

```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb

% Total    % Received % Xferd  Average   Speed  Time     Time     Time  Current
           %         0     0     0     Dload    Upload   Total   Spent    Left  Speed
100  2244  100  2244    0     0     3638    0  --:--:--  --:--:--  --:--:--  3636
```

**Step 9** Proceed to upgrade the DCNM to Release 11.5(1).

