Upgrading the Cisco DCNM

Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM 11.0(1), OVA, and ISO does not ship with SAN support.

You can upgrade to the Cisco DCNM Release 11.2(1) from DCNM Release 11.0(1) and 11.1(1) only. For instructions, refer to *Cisco DCNM Installation Guides*.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.2(1).

Table 1: Type of Upgrade

Current Release Number	Upgrade type to upgrade to Release 11.2(1)
11.1(1)	Inline Upgrade
11.0(1)	Inline Upgrade
10.4(2)	**1.** Upgrade to 11.0(1) or 11.1(1) using the DCNMUpgradeTool. **2.** Inline Upgrade from 11.0(1) or 11.1(1) to 11.2(1)

Upgrading the Cisco DCNM

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. However, there is not upgrade path for SAN OVA\ISO.

From Release 11.3(1), Cisco DCNM OVA and ISO is supported for SAN functionality.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.3(1).

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.

Inline Upgrade for DCNM Virtual Appliance in Standalone Mode

You can upgrade from Release 11.0(1) or Release 11.1(1) to Release 11.2(1) using the 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.

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

Before you begin

If the Cisco DCNM setup is in clustered mode, ensure that you perform the following:

- 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.

- Stop all the applications running on the Cisco DCNM Compute nodes using the **appmgr stop afw** command.

  ```
  dcnm-compute# appmgr stop afw
  ```

Procedure

Step 1 Log on to the Cisco DCNM appliance console.

- 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 Unzip the `dcnm-va.11.2.1.iso.zip` file and upload the `DCNM 11.2(1) ISO` file to the `/root/` folder in the DCNM setup that you want to upgrade.

Step 4 Create folder that is named **iso** using the **mkdir /mnt/iso** command.

```
dcnm# mkdir /mnt/iso
```

Step 5 Mount the DCNM 11.2(1) ISO file on the standalone setup in the /mnt/iso folder.

mount -o loop *<DCNM 11.2(1) image>* **/mnt/iso**

```
dcnm# mount -o loop dcnm-va.11.2.1.iso /mnt/iso
```

Step 6 Navigate to **/mnt/iso/packaged-files/scripts/** and run the **./inline-upgrade.sh** script.

```
dcnm# cd /mnt/iso/packaged-files/scripts/
dcnm# ./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 and continue.

```
Do you want to do the inline upgrade to 11.2(1)?
The DCNM and Elasticsearch will go down (if it is running) and come up after the upgrade
[y/n] n ? y
```

Note When upgrading to Cisco DCNM Release 11.2, the OS kernel is upgraded. At the end of the inline upgrade, the Cisco DCNM appliance reboots.

Step 7 Provide the new sysadmin user password at the prompt:

```
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.

Step 8 Ensure that the DCNM application is functional, by using the **appmgr status all** command.

```
dcnm# appmgr status all
```

Step 9 To verify that you have successfully installed the Cisco DCNM Release 11.2(1), use the **appmgr show version** command.

```
dcnm# appmgr show version

Cisco Data Center Network Manager
Version: 11.3(1)
Install mode: LAN Fabric
Standalone node. HA not enabled.
```

What to do next

Logon to the DCNM Web UI with appropriate credentials.

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

To gracefully onboard Cisco DCNM Release 11.0(1) or Release 11.1(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.2(1), see Post DCNM 11.2(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.

Inline Upgrade for DCNM Virtual Appliance in Native HA Mode

You can upgrade from Release 11.0(1) or Release 11.1(1) to Release 11.2(1) using the 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.

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

Before you begin

- Ensure that both the Cisco DCNM 11.0(1) or Cisco DCNM 11.1(1) Active and Standby peers are up and running.
- 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
  ```

- If the Cisco DCNM setup is in clustered mode, ensure that you perform the following:

  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.

  - 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.
  - Stop all the applications running on the Cisco DCNM Compute nodes using the **appmgr stop afw** command.

    ```
    dcnm-compute# appmgr stop afw
    ```

Procedure

Step 1 Unzip the `dcnm-va.11.2.1.iso.zip` file and upload the `DCNM 11.2(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.

- 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 On the Active node, perform the inline upgrade.

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

```
dcnm1# mkdir /mnt/iso
```

b) Mount the DCNM 11.2(1) ISO file on the Active node in the `/mnt/iso` folder.

```
dcnm1# mount -o loop dcnm-va.11.2.1.iso /mnt/iso
```

c) (Optional) Stop the HA applications on the Standby appliance using the **appmgr stop ha-apps** command.

```
dcnm2# appmgr stop ha-apps
```

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

```
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.

```
Do you want to do the inline upgrade to 11.2(1)?
The DCNM and Elasticsearch will go down (if it is running) and
come up after the upgrade [y/n] n ? y
```

e) Provide the new sysadmin user password at the prompt:

```
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.

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

```
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.

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

```
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 5 On the Standby node, perform the inline upgrade.

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

```
dcnm2# mkdir /mnt/iso
```

b) Mount the DCNM 11.2(1) ISO file on the Standby node in the `/mnt/iso` folder.

```
dcnm2#

dcnm2# mount -o loop dcnm-va.11.2.1.iso /mnt/iso
```

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

```
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.

```
Do you want to do the inline upgrade to 11.2(1)?
The DCNM and Elasticsearch will go down (if it is running) and
come up after the upgrade [y/n] n ? y

dcnm2# Do you want to continue and perform the inline upgrade to 11.3(1)? [y/n]: y
```

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

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

```
dcnm2# appmgr show ha-role
Native HA enabled.
```

```
Deployed role: Standby
Current role: Standby
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

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

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.

To gracefully onboard Cisco DCNM Release 11.0(1) or Release 11.1(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.2(1), see Post DCNM 11.2(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.