



Upgrading Cisco DCNM

This section includes instructions for upgrading your Cisco DCNM Appliance installation in the following scenarios:

Cisco DCNM Installer version	Release from which you can upgrade
DCNM 11.1(1)	<ul style="list-style-type: none">• DCNM 11.0(1) using Inline Upgrade• DCNM 10.4(2) using DCNMUpgradeTool

The following table summarizes the upgrade options for Cisco DCNM Release 11.1(1) .

Table 1: Type of Upgrade

Current Release Number	Upgrade type to upgrade to Release 11.1(1)
11.0(1)	Inline Upgrade
10.4(2)	Upgrade using the DCNMUpgradeTool

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for all platforms:
<SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *
• From Cisco DCNM Release 11.0(1), the characters that are allowed in the Administrative password is restricted for OVA and ISO installations. Therefore while upgrading, the old password used in DCNM 10.4(2) is not valid. However, different passwords are allowed during Upgrade.

The new Administrative password that is entered is used in the following scenarios.

- accessing the DCNM appliance via its console.
- accessing the appliance via SSH
- for applications running on the appliance, e.g. Postgres DBMS

However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

This chapter contains the following:

- [Upgrading ISO or OVA using the DCNM Upgrade Tool, on page 2](#)
- [Upgrading ISO or OVA through Inline Upgrade, on page 10](#)

Upgrading ISO or OVA using the DCNM Upgrade Tool

This section contains the procedure to download **DCNMUpgradeTool** and upgrade DCNM to the latest version.

Downloading the DCNM Upgrade Tool

The first step to upgrading the DCNM is to download the DCNMUpgradeTool script.



Note If you plan to use HA application functions, you must deploy the `dcnm.ova` or `dcnm.iso` file twice.

Procedure

- Step 1** Go to the following site: <http://software.cisco.com/download/>.
- Step 2** In the Select a Product search box, enter **Cisco Data Center Network Manager**.
Click the **Search** icon.
- Step 3** Click on **Data Center Network Manager** from the search results.
A list of the latest release software for Cisco DCNM available for download is displayed.
- Step 4** In the Latest Releases list, choose Release 11.1(1).
- Step 5** Locate the DCNM Upgrade Tool and click **Download** icon.
Save the file to the appliance `/root` directory.
-

Backup Using the Upgrade Tool

Beginning with Release 11.0(1), you can download the DCNMUpgradeTool from the Software Downloads page, to take a backup of the DCNM Appliance. This data from this backup file is restored after you upgrade the appliance to DCNM Release 11.1(1).

Perform the following task to run the DCNMUpgradeTool to take a backup of all the applications and data on DCNM 10.4(2).

Before you begin

Ensure that you have copied the DCNMUpgradeTool script to the /root directory of your appliance. Enable read and write permissions on the script using the **chmod 777** or **chmod +x** command.

Procedure

Step 1 Copy the **DCNMUpgradeTool** to the root folder of the Cisco DCNM server.

Step 2 Execute the upgrade tool command.

```
dcnm1# ./DCNMUpgradeTool
```

The tool will analyse the DCNM appliance data and decide if you can upgrade to 11.1(1) or not.

Note The backup that is generated by using this tool can be used to restore data, after upgrade.

Step 3 Enter **y** to continue.

Example:

```
Continue? [y/n] y
```

The tool inspects the systems, checks all constraints, and determines whether the appliance can be upgraded. It also checks for any SAN configuration and default fabrics. If the upgrade criteria is met, the system displays as shown below.

```
This system version: 10.4(2)
```

```
- Checking SAN config
- Checking default fabric
...
```

```
Congratulations! You can upgrade to DCNM 11.1(1)
```

If the criteria is not met, the upgrade is terminated.

Step 4 Enter **y** to create a backup file.

```
Create backup file? [y/n]: y
```

After the backup is completed successfully, the following message is displayed.

```
*****
Backup is available at /root/backup.DD_MM_YYYY_HH_MM_SS.tar.gz
*****
```

Copy the backup file to a safe location and shut down the application.

Upgrading and Restoring DCNM Virtual Appliance in Standalone mode



Note This procedure applied to both DCNM OVA and ISO upgrade.

Perform the following task to upgrade the DCNM appliance and restore data.

Before you begin

Ensure that you have copied the backup generated from `DCNMUpgradeTool` to a safe location.

Procedure

-
- Step 1** Update the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.
- For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.
- Step 2** Right click on the OVF and select **Power > Power on**.
- Step 3** After the VM is powered on click on **Console** tab.
- A message indicating that the DCNM appliance is configuring appears on the screen.
- Copy and paste the URL to the browser to continue with restore process.
- Step 4** On the Cisco DCNM Web Installer UI, click **Get Started**.
- Step 5** On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.
- Click **Continue**.
- Step 6** Select the backup file that was generated using the `DCNMUpgradeTool`.
- You can choose perform either on one of the following.
- Click **Upload backup file**. Navigate to the backup file generated for the Active node. Select the appropriate backup file. Click **OK**.
 - Click **Copy remote backup file**. Provide the Remote machine information.
- Note** You must SSH or RSync must be installed on the Remote machine.
- Click **OK**.
- Verify if the correct backup filename appears in the Select backup file field. Click **Continue**.
- Note** If the backup file was generated without using the `DCNMUpgradeTool`, an error appears and you will not be able to upgrade the DCNM.
- Step 7** After the backup file is uploaded, the DCNM server will read and auto-populate the values in some fields.
- The prefill is based on the content of the backup file that was provided. You can verify the values and modify if necessary.
- Step 8** In the Administration tab, ensure that the correct password is entered.
- Click **OK** on the Note pop-up message.
- Click **Next**.
- Step 9** In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

Note Only the supported upgrade mode will appear in the drop down list.

Click **Next**.

Step 10 On the System Settings, verify the Hostname, DNS Server Address and NTP server information. Modify the configuration, if required and click **Next**.

Step 11 On the Network Settings tab, verify the network settings configuration. Modify the configuration if required and click **Next**.

Step 12 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A warning message appears with information that the system is upgraded to DCNM 11.1(1).

```
Your Cisco Data Center Network Manager software has been installed.  
DCNM Web UI is available at  
https://<<IP-Address>>  
You will be redirected there in 60 seconds.  
Thank you.
```

What to do next

Logon to the DCNM Web UI with appropriate credentials.



Note Logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

Ensure that you clear the browser cache before you launch the Cisco DCNM Web UI using the Management Network IP address.

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

To gracefully onboard Cisco DCNM 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).

Upgrading and Restoring DCNM Virtual Appliance in Native HA Mode

The native HA is only supported on DCNM appliances with ISO or OVA installation. Unlike HA mechanisms, it doesn't require any external dependencies like an Oracle database or a shared NFS file system.

The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following to upgrade the Cisco DCNM Native HA appliances to Release 11.1(1).

Before you begin

- Ensure that both the Cisco DCNM 10.4(2) Active and Standby peers are up and running.
- Check and ensure that the Active and Standby servers are operational, by 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** Copy the DCNMUpgradeTool to the root folder of both Active and Standby servers.
- Note** For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.
- Step 2** Run the DCNMUpgradeTool on both the DCNM 10.4(2) appliances and save the backup to your local directory.
- Note** Ensure that the Current role of Active and Standby nodes are correct. Verify using the **appmgr show ha-role** command on both nodes.
- For instructions, see [Backup Using the Upgrade Tool, on page 2](#).
- Check if separate `.tar` archives are stored in an external file system.
- Step 3** Copy the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.
- For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated for the appliances after upgrade.
- Step 4** Shut down both the appliances using the **shutdown -h** command.
- Note** Ensure that you shutdown the Standby appliance first, and then shutdown the Active appliance.
- ```
dcnm2# shutdown -h now
dcnm1# shutdown -h now
```
- You can also right on the VM, select **Power > Power Off**.
- Step 5** Install Cisco DCNM 11.1(1) on two appliances, one for Active and one for Standby.
- You can either deploy DCNM as OVA or ISO. You must first deploy OVA as an OVF template, or configure KVM or Baremetal for ISO installation. For instructions, see:

- OVA—[Deploying the Open Virtual Appliance as an OVF Template](#)
- ISO—either one of the following.
  - [Installing the DCNM ISO Virtual Appliance on KVM](#)
  - [Installing the DCNM ISO Virtual Appliance on UCS \(Bare Metal\)](#)

**Note** If this deployment is a part of the upgrade process, do not Power on the VM. Edit and provide the 10.4(2) MAC address and power on the VM.

**Step 6** Update the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.

For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.

**Step 7** After the VM or Baremetal is powered on, click **Console** tab.

**Note** Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

A message indicating that the DCNM appliance is configuring appears on the screen.

Copy and paste the URL to the browser to continue with restore process.

**Step 8** On the Active node DCNM Web Installer UI, upload and validate the backup file.

a) Click **Get Started**.

b) On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.

Click **Continue**.

c) Select the Active node backup file that was generated using the `./DCNMUpgradeTool` script.

You can choose perform either on one of the following:

- Click **Upload backup file**. Navigate to the backup file generated for the Active node. Select the appropriate backup file. Click **OK**.
- Click **Copy remote backup file**. Provide the Remote machine information. Click **OK**.

Verify if the correct backup file name appears in the Select backup file field. Click **Continue**.

**Note** If the backup file was generated without using the DCNMUpgradeTool, an error appears and you will not be able to upgrade the DCNM.

d) After the backup file is uploaded, the DCNM server will read and auto populate the values in some fields.

**Note** If the primary node was not in HA active state when the backup was taken, the system will not be restored correctly and you will experience data loss.

The prefill is based on the content of the backup file that was provided.

e) In the Administration tab, ensure that the correct password is entered and click **Next**.

Select the **Show passwords in clear text** checkbox to view the password entered.

- f) In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

**Note** Only the supported upgrade mode appears in the drop-down list.

Click **Next**.

- g) On the System Settings, verify the Hostname, DNS Server Address, and NTP server information.

Modify the configuration, if necessary and click **Next**.

- h) On the Network Settings tab, verify the network settings configuration.

Modify the configuration if necessary and click **Next**.

- i) In the HA Settings tab, the following message is displayed.

```
You are installing the primary DCNM HA mode.
Please note that HA setup information will need to be
provided when the secondary DCNM HA node is installed.
```

- j) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A warning message appears with information that the system is not ready until the upgrade process on the Standby node is complete.

```
WARNING: RESTORE/UPGRADE IS NOT COMPLETE!
Your Cisco Data Center Network Manager software has been installed on this
HA primary node. However, the system will be ready to be used only after the
upgrade/restore of the secondary node has been completed.
Thank you.
```

## Step 9

On the Standby node DCNM Web Installer UI, upload and validate the backup file.

- a) Click **Get Started**.
- b) On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.

Click **Continue**.

- c) Select the Standby node backup file that was generated using the `./DCNMUpgradeTool` script.

You can choose perform either on one of the following:

- Click **Upload backup file**. Navigate to the backup file generated for the Standby node. Select the appropriate backup file. Click **OK**.
- Click **Copy remote backup file**. Provide the Remote machine information. Click **OK**.

Verify if the correct backup file name appears in the Select backup file field. Click **Continue**.

If the backup file was generated without using the DCNMUpgradeTool, an error appears and you will not be able to upgrade the DCNM.

- d) After the backup file is uploaded, the DCNM server will read and auto populate the values in some fields.



**Note** If the standby node was not in HA standby state when the backup was taken, the system will not be restored correctly and you will experience data loss.

The prefill is based on the content of the backup file that was provided.

- e) In the Administration tab, ensure that the correct password is entered and click **Next**.

**Note** This password must match the Administration Password of the Primary DCNM node for HA setup to complete successfully.

Select the **Show passwords in clear text** checkbox to view the password entered.

- f) In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

**Note** Ensure that you select the same installation mode for the standby node that was chosen for the primary node.

Click **Next**.

- g) On the System Settings, verify the Hostname, DNS Server Address, and NTP server information.

Modify the configuration, if necessary and click **Next**.

- h) On the Network Settings tab, verify the network settings configuration.

Modify the configuration if necessary and click **Next**.

- i) In the HA Settings tab, the following message is displayed.

Enter a valid HA Ping IP Address, if necessary. Ensure that this IP address must be different from the DCNM Active and Standby IP addresses.

**Note** If set, the **HA ping feature IP Address** must be pingable for DCNM services to be running in Native HA systems. This address must belong to Enhanced Fabric management network.

- j) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
```

**Step 10** After the data is restored, check the status using the **appmr status all** command on both Active and standby nodes.

**Step 11** Verify the role of the appliances using the **appmgr show ha-role** command.

**Step 12** Log on to the DCNM Web UI with appropriate credentials.

**What to do next**

Logon to the DCNM Web UI with appropriate credentials.



**Note** After the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must log on to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

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

To gracefully onboard Cisco DCNM 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).

## 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 log in to Cisco DCNM Web UI.

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) to Release 11.1(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.

### 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.

**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.11.1.1.iso.zip` file and upload the DCNM 11.1(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 11.1(1) ISO file on the standalone setup in the `/mnt/iso` folder.

**mount -o loop <DCNM 11.1(1) image> /mnt/iso**

```
dcnm# mount -o loop dcnm-va.11.1.1.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
```

```
Do you want to continue and perform the inline upgrade to ? [y/n]: y
```

**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 11.1(1)?
```

```
The DCNM and Elasticsearch will go down (if it is running) and come up after the upgrade
```

```
[y/n] n ? y
```

**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 11.1(1), use the **appmgr show version** command.

```
dcnm# appmgr show version
```

```
Cisco Data Center Network Manager
```

```
Version: 11.1(1)
```

```
Install mode: LAN Fabric
```

```
Standalone node. HA not enabled.
```

## 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.

To reindex the performance manager data, use the **appmgr es-reindex pmdb** command.

To gracefully onboard Cisco DCNM 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).

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

You can upgrade from Release 11.0(1) to Release 11.1(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)Active and Standby peers are up and running.
- 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
```

- 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.11.1.1.iso.zip` file and upload the DCNM 11.1(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 logon 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.
- 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.
- Create a folder named **iso** using the **mkdir /mnt/iso** command.


```
dcnm1# mkdir /mnt/iso
```
 - Mount the DCNM 11.1(1) ISO file on the Active node in the `/mnt/iso` folder.


```
dcnm1# mount -o loop dcnm-va.11.1.1.iso /mnt/iso
```
 - (Optional) Stop the HA applications on the Standby appliance using the **appmgr stop ha-apps** command.


```
dcnm2# appmgr stop ha-apps
```
 - 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 11.1(1)?
The DCNM and Elasticsearch will go down (if it is running) and
come up after the upgrade [y/n] n ? y
```
 - 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 11.1(1) ISO file on the Standby node in the `/mnt/iso` folder.

```
dcnm2# mount -o loop dcnm-va.11.1.1.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 11.1(1)?
The DCNM and Elasticsearch will go down (if it is running) and
come up after the upgrade [y/n] 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 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).

