



# CHAPTER 5

## Upgrading Cisco DCNM

---

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

Cisco DCNM Installer version	Release from which you can upgrade
DCNM 10.0(1) ISO/OVA	<ul style="list-style-type: none"><li>• Cisco DCNM, Release 7.2(2)</li><li>• Cisco DCNM, Release 7.2(2a)</li><li>• Cisco DCNM, Release 7.2(3)</li></ul>
DCNM 10.0(1) EXE/BIN	<ul style="list-style-type: none"><li>• Cisco DCNM, Release 7.2(2)</li><li>• Cisco DCNM, Release 7.2(2a)</li><li>• Cisco DCNM, Release 7.2(3)</li></ul>

You can migrate Cisco DCNM with a local PostgreSQL database and an external Oracle database and Cisco DCNM in a High Availability (HA) environment.



Note

In Cisco DCNM Release 10.0(x), the HA setup for XMPP uses external oracle database. You must provide username and password for external oracle database. Create a new username and password for the XMPP application to use in the same remote Database instance, used by the Cisco DCNM.



Note

Before upgrading Cisco DCNM, ensure that auto move is disabled. Otherwise, if one server within the federation is down, the devices discovered by the server will be moved to the other DCNM server which comes up first after upgrade. To prevent the auto move for DCNM upgrade, you need to disable the auto move on all DCNMs within the federation, and then upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the auto move again.

To enable / disable auto move, please go to **Admin > Federation** from DCNM web page, click on the checkbox at top left for **Enable Automatic Failover**.



Note

When upgrading to a newer DCNM version, you should use the same administrative password (as used in the existing setup) for the new DCNM setup. If you want to use a different password in the new setup, change the password in the existing DCNM setup before taking a backup and initiating the upgrade process.

This chapter contains the following:

- [Retaining the CA Signed Certificate](#), page 5-2
- [Upgrading Cisco DCNM Windows and Linux through GUI Installation](#), page 5-2
- [Upgrading Cisco DCNM Windows and Linux through Silent Installation](#), page 5-3
- [Upgrading Cisco DCNM Windows and Linux Federation through GUI Installation](#), page 5-3
- [Upgrading Cisco DCNM Windows and Linux Federation through Silent Installation](#), page 5-4
- [Upgrading Cisco DCNM Virtual Appliance with External Oracle Database](#), page 5-6
- [Upgrading Cisco DCNM appliances with Enhanced Fabric Management in HA Environment](#), page 5-7
- [Upgrading Cisco DCNM Virtual Appliance with Local PostgreSQL Database](#), page 5-5
- [Upgrading Cisco DCNM appliances without Enhanced Fabric Management in HA Environment](#), page 5-9
- [Database Utility Scripts](#), page 5-12

## Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

### DETAILED STEPS

- 
- Step 1** Backup the signed certificate from the location  
`<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks`
- Step 2** Upgrade to Cisco DCNM Release 10.0(x) based on the requirement.
- Step 3** After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.




---

**Note** You must load the certificates to the same location as mentioned in [Step 1](#).

---

- Step 4** Open the following files:
- `<Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/standalone-san.xml`
  - `<Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/ standalone-lan.xml`
- Step 5** Search for **key-alias="sme"** and replace with `key-alias="<key-alias used to create CA signed SSL Certificate>"`
- Step 6** Restart the DCNM Services.
- 

## Upgrading Cisco DCNM Windows and Linux through GUI Installation

Before you begin, make sure that Cisco DCNM 7.2.x is up and running.

- 
- Step 1** Stop the DCNM services.
- Step 2** Run the Cisco DCNM software for Release 10.0.x executable file.  
Upgrade Notification window appears
- Step 3** Click **OK** to begin the upgrade.
- Step 4** Click **Done** after the upgrade is complete.  
The Cisco DCNM Release 10.0(x) services will start automatically.
- 

## Upgrading Cisco DCNM Windows and Linux through Silent Installation

Before you begin, make sure that Cisco DCNM Release 7.2.x is up and running.



**Note** Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

---

### DETAILED STEPS

- 
- Step 1** Stop the DCNM services.
- Step 2** Open the *installer.properties* file and update the following properties:
- ```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```
- Step 3** Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:
- For Windows installer—*dcnm-release.exe -i silent -f <path\_of\_installer.properties>*
  - For Linux installer—*dcnm-release.bin -i silent -f <path\_of\_installer.properties>*
- The Cisco DCNM Release 10.0.x services will start after the upgrade is complete.



**Note** For Windows upgrade, you can check the status of the upgrade in the Task Manager process.  
For Linux upgrade, you can check the status of the upgrade process by using the following command:  
**ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

---

## Upgrading Cisco DCNM Windows and Linux Federation through GUI Installation

Before you begin, make sure that the Cisco DCNM 7.2(x) is up and running.




---

**Note** Ensure that both primary and secondary database properties are same.

---

- Step 1** Stop both the primary and secondary DCNM services.
- Step 2** On the primary server, run the Cisco DCNM Release 10.0.x executable file.  
Upgrade notification window appears.
- Step 3** Click **OK** to begin the upgrade.
- Step 4** On the secondary server, perform run the Cisco DCNM Release 10.0.x executable file.  
Upgrade notification window appears.
- Step 5** Click **OK** to begin the upgrade.
- Step 6** On the primary server, click **Done** after the upgrade is complete.  
The Cisco DCNM Release 10.0.x services will start automatically on the primary server.
- Step 7** On the secondary server, click **Done** after the upgrade is complete.  
The Cisco DCNM Release 10.0.x services will start automatically on the secondary server.
- 

## Upgrading Cisco DCNM Windows and Linux Federation through Silent Installation

Before you begin, make sure that the Cisco DCNM 7.2(x) is up and running.




---

**Note** Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

---




---

**Note** Ensure that both primary and secondary database properties are same.

---

- Step 1** Stop both the primary and secondary DCNM services.
- Step 2** On the primary server, open the *installer.properties* file and update the following properties:
- ```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```
- Step 3** Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:
- For Windows installer—`dcnm-release.exe -i silent -f <path_of_installer.properties>`
  - For Linux installer—`dcnm-release.bin -i silent -f <path_of_installer.properties>`




---

**Note** For Windows upgrade, you can check the status of the upgrade in the Task Manager process.

---

For Linux upgrade, you can check the status of the upgrade process by using the following command:  
**ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

- 
- Step 4** On the secondary server, open the *installer.properties* file and update the following properties:
- ```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
SAN_FEDERATION=TRUE
```
- Step 5** Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:
- For Windows installer—*dcnm-release.exe -i silent -f <path\_of\_installer.properties>*
  - For Linux installer—*dcnm-release.bin -i silent -f <path\_of\_installer.properties>*
- Step 6** On the primary server, click **Done** after the upgrade is complete.  
The Cisco DCNM Release 10.0.x services will start automatically on the primary server.
- Step 7** On the secondary server, click **Done** after the upgrade is complete.  
The Cisco DCNM Release 10.0.x services will start automatically on the secondary server.
- 

## Upgrading Cisco DCNM Virtual Appliance with Local PostgreSQL Database

Before you begin, make sure that Cisco DCNM 7.2(x) is up and running.

- 
- Step 1** Use the **appmgr backup all** command to backup all applications associated with the installation of Cisco DCNM 7.2.x.
- A prompt appears to provide the DCNM DB password and XMPP DB password. By default, this password is the administrative password provided during the Open Virtual Appliance installation.
- Step 2** On Cisco DCNM 10.0.x, ensure that the MAC addresses along with all network settings such as the IP address, default gateway, hostname, etc., are identical to the Cisco DCNM 7.2.x installation.
- Step 3** Transfer the backup file to an external file system.
- Step 4** Power off Cisco DCNM 7.2(x).
- Step 5** Deploy the Cisco DCNM Open Virtual Appliance file for version 10.0.x.
- Use the same network parameters (IP address/subnet/gateway/DNS).
  - Use the same administrative password.
  - Use the same vCenter port groups for both network interfaces.
  - Disable auto-power-on. (The Power on Open Virtual Appliance after deployment check-box should not be selected).
- Step 6** After Cisco DCNM 10.0.x is deployed, right-click on **VM > Edit Settings > Hardware**.
- For both Network Adapters, update the MAC address to be the same as Cisco DCNM 7.2.x. 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** Power on DCNM 10.0.x VM.
- Step 8** Copy the Cisco DCNM 7.2.x backup file from the external repository to Cisco DCNM 10.0.x.
- Step 9** Use the **appmgr status all** status all command to make sure that all applications are up and running.
- Step 10** Use the **appmgr stop all** to shut down all applications on Cisco DCNM 10.0.x.
- Step 11** Use the **appmgr upgrade <backup filename>** command to run the upgrade script on Cisco DCNM 10.0.x.

The application displays the following message:

```
Please Shut Down All Applications Before Continuing.
Press 'y' to continue [y/n] [n]
```

- Step 12** Press **Y** to continue.
- Press [1] or [2] or [3] when prompted, based on your Cisco DCNM 7.2.x setup:
- Choose [1] Standalone DCNM with Local PostgreSQL database
- [2] Standalone DCNM with External Oracle database
- [3] High Availability

If you choose option [1] Standalone DCNM with Local PostgreSQL database, It will get upgraded successfully.

If you choose option [2] Standalone DCNM with External Oracle database, ensure that the external database is up and running. For more information, see [Upgrading Cisco DCNM Virtual Appliance with External Oracle Database, page 5-6](#).

## Upgrading Cisco DCNM Virtual Appliance with External Oracle Database

Perform the following procedure to upgrade Cisco DCNM Virtual Appliance with external Oracle database.



**Note** Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-18](#).

When you select Option [2] in [Step 12](#) of the procedure [Upgrading Cisco DCNM Virtual Appliance with Local PostgreSQL Database, page 5-5](#), the following query appears:

Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance. Do you want to proceed with upgrade?

```
Press 'y' to continue [y/n] [n]
```

- Step 1** Press **Y** to continue.
- Step 2** Enter the DB URL.
- Example: `jdbc:oracle:thin:@10.2.3.4:1521:XE`

- Step 3** Enter the DB username
- Step 4** Enter the DB password.  
Enter it again for verification:
- Step 5** Choose the XMPP DB type as per backup:  
[1] Local Postgre | [2] External Oracle [1]  
If you choose option [1], go to [Step 6](#).  
If you choose option [2], perform the following steps:
- Enter the XMPP DB URL.
  - Enter the XMPP database username.
  - Enter the XMPP database password.
- Step 6** Enter the administrative password provided during Virtual Appliance installation, when prompted for the root password.  
The external DCNM database will be configured to access all the Fabric applications using the root password of this server.



**Note** You can change the password using the Cisco DCNM Web Client, from **Admin > Fabric Settings**.  
Root password:  
Enter it again for verification:



**Note** Upgrading from Non-DFA to Cisco DCNM 10.0(1) with a Local PostgreSQL or External Oracle Database. Deploy the Cisco DCNM 10.0(1) with the Enhanced Fabric Management Network fields with default values (i.e., IP Address: 0.0.0.0, Subnet Mask: 0.0.0.0 and DNS IP: 1.1.1.1). Perform the procedure detailed in [Upgrading Cisco DCNM Virtual Appliance with External Oracle Database, page 5-6](#).



**Note** Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-18](#).

## Upgrading Cisco DCNM appliances with Enhanced Fabric Management in HA Environment

Before you begin, make sure that both the Cisco DCNM 7.2(x) Active and Standby peers are up and running.

**Note**

For more information on Active and Standby peers in a High Availability environment, see [“Managing Applications in a High-Availability Environment”](#).

- Step 1** Verify if the **appmgr backup all** command was executed on both the Active and Standby peers. Check if separate tar archives are stored in an external file system.

Example: active.tar.gz and standby.tar.gz

**Note**

If it is the non-DFA environment, please verify if the **appmgr backup dcnm** command was executed on both the Active and Standby peers.

- Step 2** Power off the Cisco DCNM 7.2(x) Active peer.
- Step 3** Wait for 4 to 5 minutes, before you stop all the DCNM applications by using **appmgr stop all** command on the Cisco DCNM 7.2.x Standby peer.

This is to ensure that the write operations to LDAP are completed, and avoid LDAP from entering an inconsistent state.

- Step 4** Power-on the Cisco DCNM 10.0.x Active peer.
- Step 5** Use the **appmgr status all** command to ensure that all the applications are up and running on the Cisco DCNM 10.0.x Active peer.

- Step 6** Stop all DCNM applications on the Cisco DCNM 10.0.x Active peer, by using **appmgr stop all** command.

- Step 7** Use the **appmgr upgrade <active.tar.gz>** command to run the upgrade script.

```
a. PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING.
   Press 'y' to continue [y/n] [n]
```

```
y
b. Choose option [3] High Availability when prompted.
   Choose option [1] Standalone DCNM with Local PostgreSQL database
   [2] Standalone DCNM with External Oracle database
   [3] High Availability
```

```
c. Prior to upgrade, we strongly advise that you make a backup of your remote Oracle
   instance. Do you want to proceed with upgrade?
   Press 'y' to continue [y/n] [n]
```

```
y
```

```
d. Select option [1] Active when prompted.
   Choose [1] Active [2] Standby
```

```
f. Enter the standby eth0 IP address.
g. Enter the Management IP Address of the peer DCNM (eth0 IP).
h. Enter the root password of the peer.
i. Enter the Database username for XMPP tables.
j. Enter the Database password for XMPP tables.
k. Enter the Database password for XMPP tables again for verification.
l. Enter the common FQDN for VIP on both DCNM management and EFM networks:
After the upgrade is completed successfully, you will see the following message:
**** Check /root/upgrade.log for details...****
Ensure that all applications are running on the Cisco DCNM 10.0(1) Active peer.
```

- Step 8** Power off the Cisco DCNM 7.2.x Standby peer.
- Step 9** Power on the Cisco DCNM 10.0.x Standby peer. Use the **appmgr status all** command to make sure that all applications are up and running.



- Step 10** Stop all applications on the Cisco DCNM 10.0.x Standby peer.
- Step 11** Run the below NTP command on the standby to synchronize the time.  
**ntpdate -b -u NTP\_SERVER\_IPADDRESS**
- Step 12** Use the **appmgr upgrade <standby.tar.gz>** command to run the upgrade script on the Cisco DCNM 10.0.x Standby peer.
- a. Choose option **[3] High Availability** when prompted.
 

```
Choose option [1] Standalone DCNM with Local PostgreSQL database
              [2] Standalone DCNM with External Oracle database
              [3] High Availability
```
  - b. Select option **[2] Standby** when prompted.
 

```
Choose [1] Active [2] Standby
```
- To migrate the standby peer, perform the following:**
- a. Enter the **active eth0 IP** address.
- Step 13** Invoke the following on the Active peer to establish SSH trust to the Standby peer:  
`sh /root/sshAutoLogin.sh <STANDBY_PEER_IP>`
- Step 14** Restart the active Cisco DCNM, using the **appmgr restart dcnm** command.

**Note**

Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see [Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-18](#).

## Upgrading Cisco DCNM appliances without Enhanced Fabric Management in HA Environment

Before you begin, make sure that virtual appliance should be installed in Non Programmable Fabric mode.

**Note**

For instruction about installing these applications with the Cisco DCNM Open Virtual Appliance, see [DCNM installation without Enhanced Fabric Management capabilities, page 3-19](#). For more information on NON DFA High Availability environment, see [Managing Applications in a High-Availability Environment, page 7-1](#).

- Step 1** Make sure that both Cisco DCNM 7.2(x) servers are deployed, powered on and made it as a First and Federated node by using the below commands.
- ```
appmgr setup ha -type first-node
appmgr setup ha -type federated-node
```
- Step 2** Verify if the **appmgr backup dcnm** command was executed on both the First Node and Federated Node using the below command. Check if separate tar archives are stored in an external file system.

Example: `first_node.tar.gz`  
`federated_node.tar.gz`

- Step 3** Power off the Cisco DCNM 7.2(x) First and Federated Node virtual appliance.
- Step 4** Power-on the Cisco DCNM 10.0.x First and Federated Node virtual appliance which should be deployed in the same eth0 IP of 7.2.x.



**Note** While deploying Cisco DCNM 10.0.x First and Federated Node virtual appliance, the Enhanced Fabric Management Network fields must contain default values (i.e., IP Address:0.0.0.0, Subnet Mask:0.0.0.0 and DNS IP:1.1.1.1)

- Step 5** Use the **appmgr status all** command to ensure that DCNM applications are up and running on the Cisco DCNM 10.0.x First and Federated Nodes.
- Step 6** Stop the applications on the Cisco DCNM 10.0.x First node, by using **appmgr stop dcnm** command.
- Step 7** Use the command **appmgr upgrade <first\_node.tar.gz>** on the Cisco DCNM 7.2(3) First node to run the upgrade script. After issuing **appmgr upgrade <first\_node.tar.gz>** on First Node, user will be prompted for various inputs. Provide the inputs as per the sample given below.

**PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING. .**

**Press 'y' to continue [y/n] [n]**

y

**Select an option for upgrading this appliance [ ] :**

**[1] Standalone DCNM with Local PostgreSQL database**

**[2] Standalone DCNM with External Oracle database**

**[3] High Availability**

**Choice [1|2|3]**

3

**Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance.  
 Do you want to proceed with upgrade?**

**Press 'y' to continue [y/n] [n]**

y

**Please enter the type of server:**

**[1] First Node | [2] Federated Node [1]**

1

\*\*\*\*\*

**You are about to be federated for DCNM alone in this DCNM appliance.**

**Please make sure that you have the following**

1. An Oracle Database with a user defined for DCNM.
2. A repository with NFS capabilities.
3. An NTP server for time synchronization.

\*\*\*\*\*

a) Do you want to continue? [y/n] [y]

b) Enter the DB URL {ex. jdbc:oracle:thin:@ipaddr:1521:<SID or Servicename>} :

c) Enter the DB username for DCNM tables: <dcnm-dbuser>

d) Enter the DB password for DCNM tables :

e) Enter it again for verification:

f) Enter the SCP/NFS repository IP : <repository IP>

g) NFS Exported location {ex. /var/shared/dcnm/} :

h) Enter an NTP server for time synchronization "NTP\_SERVER":

\*\*\*\*\*Successfully Completed. Run 'appmgr start dcnm'\*\*\*\*\*

i) Verify whether HA Federation enabled after upgrade by using command `appmgr show ha-role`.

j) Start DCNM using `appmgr start dcnm`.

**Step 8** Stop DCNM applications on the Cisco DCNM 10.0.x Federated Node by using `appmgr stop dcnm` command.

**Step 9** Run the below NTP command on standby to sync the time.

```
ntpdate -b -u clock.cisco.com
```

**Step 10** Use the `appmgr upgrade <federated_node.tar.gz>` command to run the upgrade script on the Cisco DCNM 10.0.x Federated Node. After issuing `appmgr upgrade <first_node.tar.gz>` on First Node, user will be prompted for various inputs. Provide the inputs as per the sample given below.

**PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING..**

Press 'y' to continue [y/n] [n]

**Y**

Select an option for upgrading this appliance [] :

[1] Standalone DCNM with Local PostgreSQL database

[2] Standalone DCNM with External Oracle database

[3] High Availability

Choice [1|2|3]

3

Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance.  
Do you want to proceed with upgrade?

Press 'y' to continue [y/n] [n]

Y

Please enter the type of server :

[1] First Node | [2] Federated Node [1]

2

\*\*\*\*\*

You are about to enable High Availability for DCNM alone in this DCNM appliance.

Please make sure that you have the following

1. An Existing Federated server.

\*\*\*\*\*

a) Do you want to continue? [y/n] [y]

b) Enter the existing Federated server IP (eth0 IP) : <PEER\_ETH0\_IP>

c) Enter the root password of the peer

d) Root password : <root\_password\_of\_this\_node>

\*\*\*\*\* Successfully Completed.\*\*\*\*\*

e) Verify whether HA Federation enabled after upgrade using command  
appmgr show ha-role".

## Database Utility Scripts

### Local PostgreSQL Database Utility Scripts for Backup and Restore

Utility scripts for Local PostgreSQL database that is installed in RHEL machine are:

1. backup-pgsql-dcnm-db.sh
2. restore-pgsql-dcnm-db.sh

Utility scripts for Local PG database that is installed in Windows machine are:

1. backup-pgsql-dcnm-db.bat
2. restore-pgsql-dcnm-db.bat

## Remote Oracle Database Utility Scripts for Backup and Restore

Irrespective of the platform, Cisco DCNM is installed (Windows or Linux), the following scripts to backup and restore the remote Oracle database.

Utility scripts for Oracle database that is installed on Linux platform are;

1. backup-remote-oracledb.sh
2. restore-remote-oracledb.sh

Utility scripts for Oracle database that is installed on Windows platform are:

1. backup-remote-oracledb.bat
2. restore-remote-oracledb.bat

Cisco DCNM host is configured to run with a remote Oracle database. As part of housekeeping, you can copy DCNM utility scripts to a remote Oracle database and restore the DCNM database schema.

To run the utility scripts, you need the database administrator credentials. These scripts will prompt you for:

1. DCNM database password (the user name is already present)
2. Username/password of the admin user.

While entering the DBA user credentials, ensure that you do not to enter “sys” as sysdba” because in some versions of Oracle, the presence of space might cause the backup/restore to fail. Instead, user should provide valid user credentials that does not have a space in the user name, for example, system or sysdba. The admin credentials are not saved/cached and hence they do not leak sensitive credential information.



Note

---

User scripts under *dcnm/bin* can be run only by administrator user.

---

