Migrating From DCNM to NDFC

Prerequisites and guidelines for migrating from DCNM to NDFC

Note If you are already running Nexus Dashboard with Fabric Controller service, skip this section and upgrade as described in Upgrading Existing ND Cluster to This Release instead.

Upgrading from DCNM 11.5(4) consists of the following workflow:

1. Ensure you complete the prerequisites and guidelines described in this section.
2. Back up your existing configuration using a migration tool specific to the target NDFC release.
3. Deploy a brand new Nexus Dashboard cluster with Fabric Controller (NDFC) service.

   Note that unlike in previous releases where you had to install the service and enable it after the cluster was already deployed, in this release you enable the service during initial cluster deployment due to the introduction of the unified installation.
4. Restore the configuration backup you created in step 1.

Note Before you proceed with the upgrade:

- Validate each fabric's credentials.
  - For LAN fabrics, navigate to the **Web UI** > **Administration** > **Credentials Management** > **LAN Credentials** page, select each fabric, and choose **Validate** to validate credentials.
  - For SAN fabrics, navigate to the **Web UI** > **Administration** > **Credentials Management** > **SAN Credentials** page, select each fabric, and choose **Validate** to validate credentials.
- If you are running an app on your DCNM, such as the Thousand Eyes integration app, disable that app before proceeding with these migration procedures.

Persona Compatibility

By using the appropriate Upgrade Tool, you can restore data that is backed up from DCNM Release 11.5(4) on a newly deployed Nexus Dashboard Fabric Controller for the personas as mentioned in the following table:

Backup from DCNM 11.5(4)	Persona Enabled in NDFC After Upgrade
DCNM 11.5(4) LAN Fabric Deployment on OVA/ISO/SE	Fabric Controller + Fabric Builder
DCNM 11.5(4) PMN Deployment on OVA/ISO/SE	Fabric Controller + IP Fabric for Media (IPFM)
DCNM 11.5(4) SAN Deployment on OVA/ISO/SE	SAN Controller
DCNM 11.5(4) SAN Deployment on Linux	SAN Controller
DCNM 11.5(4) SAN Deployment on Windows	SAN Controller

Feature Compatibility Post Upgrade

The following table lists caveats associated with features that are restored from DCNM 11.5(4) backup after upgrading.

Note SAN Insights and VMM Visualizer features are not enabled after restore; you can choose to enable them in the **Settings** > **Feature Management** page of the Nexus Dashboard Fabric Controller UI.

Feature in DCNM 11.5(4)	Upgrade Support
Nexus Dashboard Insights configured Refer to Cisco Nexus Dashboard User Guide for more information.	Supported
Container Orchestrator (K8s) Visualizer	Supported
VMM Visibility with vCenter	Supported
Nexus Dashboard Orchestrator configured	Not Supported
Preview features configured	Not supported
LAN switches in SAN installations	Not supported
Switches discovered over IPv6	Not supported
DCNM Tracker	Not supported
Fabric Backups	Not supported
Report Definitions and Reports	Not supported
Switch images and Image Management policies	Not supported
SAN CLI templates	Not carried over from 11.5(4)

Feature in DCNM 11.5(4)	Upgrade Support
Switch images/Image Management data	Not carried over from 11.5(4)
Slow drain data	Not carried over from 11.5(4)
Infoblox configuration	Not carried over from 11.5(4)
Endpoint Locator configuration	You must reconfigure Endpoint Locator (EPL) post upgrade. However, historical data is retained up to a maximum size of 500 MB.
Alarm Policy configuration	Not carried over from 11.5(4)
Performance Management data	CPU/Memory/Interface statistics up to 90 days is restored post upgrade.
Temperature data	Temperature data is not saved in the backup and as a result is not restored after the migration. You must re-enable temperature data collection after the migration.

Migrate Existing DCNM Configuration to NDFC

This section describes how to back up your existing DCNM 11.5(4) configuration, deploy a new Nexus Dashboard cluster, and restore the configuration to finish the migration.

Step 1 Download the upgrade tool.

a) Navigate to the NDFC download page..

https://software.cisco.com/download/home/281722751/type/282088134/

b) In the **Latest Releases** list, choose the target release.

c) Download the upgrade tool appropriate for your deployment type.

DCNM 11.5(4) deployment type	Upgrade Tool File Name
ISO/OVA	`DCNM_To_NDFC_12_2_2_Upgrade_Tool_OVA_ISO.zip`
Linux or Windows	`DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip`

d) Copy the upgrade tool image to your existing DCNM 11.5(4) server using the **sysadmin** account.

Step 2 Extract the archive and validate the signature for Linux/Windows deployments.

Note If you are using the ISO/OVA archive, skip to the next step.

a) Ensure that you have Python 3 installed.

```
$ python3 --version
Python 3.9.6
```

b) Extract the downloaded archive.

```
# unzip DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

c) Validate signature.

Inside the ZIP archive, you will find the upgrade tool as well as the signature file. Use the following commands to validate the upgrade tool:

```
# ls -l
-rwxr-xr-x. 1 root root 16788 Apr 20 2023 cisco_x509_verify_release.py3
-rw-r--r--. 1 root root 1422 Aug 12 2023 ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
-rw-r--r--. 1 root root 9541673 Jul 25 03:09 DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
-rw-r--r--. 1 root root 256 Jul 25 03:09 DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
-rw-r--r--. 1 root root 9548328 Jul 26 06:11 DCNM_To_NDFC_12_2_2_Upgrade_Tool_LIN_WIN.zip


# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip -s DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature -v dgst
 -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

d) Once the validation script signature is verified, extract the script itself.

```
# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/log4j2.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat
creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/dcnmbackup.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
```

Step 3 Extract the archive and validate the signature for ISO/OVA deployments.

Note If you are using the Linux/Windows archive, skip to the next step.

a) Extract the downloaded archive.

```
# unzip DCNM_To_NDFC_12_2_2_Upgrade_Tool_OVA_ISO.zip
Archive: DCNM_To_NDFC_12_2_2_Upgrade_Tool_OVA_ISO.zip
inflating: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
extracting: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature
```

```
inflating: cisco_x509_verify_release.py3
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

b) Validate signature.

Inside the ZIP archive, you will find the upgrade tool as well as the signature file. Use the following commands to validate the upgrade tool:

```
# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_OVA_ISO -s DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature -v dgst -sha512
Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_OVA_ISO using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

Step 4 Back up existing configuration.

The backup tool collects last 90 days Performance Management data.

a) Log in to your DCNM Release 11.5(4) appliance console.

b) Create a screen session.

The following command creates a session which allows you to execute additional commands:

```
dcnm# screen
```

Note that the commands continue to run even when the window is not visible or if you get disconnected.

c) Gain super user (`root`) access.

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

d) For OVA and ISO, enable execution permissions for the upgrade tool.

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
```

e) Run the upgrade tool you downloaded in the previous step.

- For Windows:

```
C:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:
Initializing, please wait...
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard 3.2.1
 or not.
If upgrade to Nexus Dashboard 3.2.1 is possible, this tool will create files to be used for
performing the upgrade.
Thank you!
********************************************************************************
This tool will backup config data. Exporting Operational data like Performance(PM) might take
 some time.
Do you want to export operational data also? [y/N]: y
********************************************************************************
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.
Please enter the encryption key:
```

```
Enter it again for verification:
…..
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection [id: 0][route:
{s}->https://127.0.0.1:9200] can be kept alive indefinitely
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.DefaultManagedHttpClientConnection - http-outgoing-0: set socket
timeout to 0
2024-07-25 22:35:34,944 [main] DEBUG
org.apache.http.impl.conn.PoolingHttpClientConnectionManager - Connection released: [id:
0][route: {s}->https://127.0.0.1:9200][total kept alive: 1; route allocated: 1 of 20; total
allocated: 1 of 20]
2024-07-25 22:35:34,969 [main] INFO DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 145
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ###### Total time to export Daily data: 7
seconds.
2024-07-25 22:35:35,036 [main] INFO DCNMBackup - ###### Total time to export PM data: 36
seconds.
2024-07-25 22:35:35,169 [main] INFO DCNMBackup - Creating data file...
2024-07-25 22:35:38,083 [main] INFO DCNMBackup - Creating metadata file...
2024-07-25 22:35:38,085 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-25 22:35:38,267 [main] INFO DCNMBackup - Done
```

- For Linux:

```
# ./DCNMBackup.sh
Enter DCNM root directory [/usr/local/cisco/dcm]:
Initializing, please wait...
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for Linux/Windows.
This tool will analyze this system and determine whether you can move to Nexus Dashboard 3.2.1
 or not.
If upgrade to Nexus Dashboard 3.2.1 is possible, this tool will create files to be used for
performing the upgrade.
Thank you!

********************************************************************************

This tool will backup config data. Exporting Operational data like Performance(PM) might take
 some time.
Do you want to export operational data also? [y/N]: y
********************************************************************************
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:
……
2024-07-26 04:04:46,540 [main] INFO DCNMBackup - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 92
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ###### Total time to export Daily data: 3
seconds.
2024-07-26 04:04:46,543 [main] INFO DCNMBackup - ###### Total time to export PM data: 11
seconds.
2024-07-26 04:04:46,958 [main] INFO DCNMBackup - Creating data file...
2024-07-26 04:04:47,456 [main] INFO DCNMBackup - Creating metadata file...
2024-07-26 04:04:47,467 [main] INFO DCNMBackup - Creating final backup archive...
2024-07-26 04:04:47,478 [main] INFO DCNMBackup - Done.
```

- For OVA:

```
# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
********************************************************************************
Welcome to DCNM-to-NexusDashboard Upgrade Tool for OVA/ISO.
```

```
This tool will analyze this system and determine whether you can move to
Nexus Dashboard 3.2.1 or not.
If upgrade to Nexus Dashboard 3.2.1 is possible, this tool will create files
to be used for performing the upgrade.
NOTE:
Only backup files created by this tool can be used for upgrading,
older backup files created with 'appmgr backup' CAN NOT be used
for upgrading to Nexus Dashboard 3.2.1
Thank you!

********************************************************************************
Continue? [y/n]: y
Collect operational data (e.g. PM, EPL)? [y/n]: y
Does this DCNM 11.5(4) have DCNM Tracker feature enabled on any switch on any fabric? [y/n]:
 n

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:
……
Adding backup header
Collecting DB table data
Collecting DB sequence data
Collecting stored credentials
Collecting Custom Templates
Collecting CC files
Collecting L4-7-service data
Collecting CVisualizer data
Collecting EPL data
Collecting PM data - WARNING: this will take a while!
Collecting AFW app info
Decrypting stored credentials
Adjusting DB tables
Creating dcnm backup file
Creating final backup file
Done.
Backup file: backup11_sandcnm_20240726-113054.tar.gz
```

Step 5 Deploy a brand new Nexus Dashboard cluster as described in one of the earlier chapters in this document.

Ensure that you complete all guidelines and prerequisites for the Nexus Dashboard platform, the Fabric Controller service, and the specific form factor listed in the deployment chapters above.

Note

- You must provide the required number of Persistent IP addresses in the Nexus Dashboard Fabric Controller UI before proceeding with restoring your DCNM configuration..
- If your existing configuration used smart licensing with direct connectivity to Cisco Smart Software Management (CSSM), you must ensure that your new Nexus Dashboard has the routes required to reach the CSSM website.

  Ensure that subnets for IP addresses on `smartreceiver.cisco.com` are added to the route table in the Nexus Dashboard's **Admin** > **System Settings** > **Routes** page for the Nexus Dashboard management network.

  You can ping `smartreceiver.cisco.com` to find the most recent subnet, for example:

```
$ ping smartreceiver.cisco.com
PING smartreceiver.cisco.com (146.112.59.81): 56 data bytes
64 bytes from 146.112.59.81: icmp_seq=0 ttl=52 time=48.661 ms
64 bytes from 146.112.59.81: icmp_seq=1 ttl=52 time=44.730 ms
64 bytes from 146.112.59.81: icmp_seq=2 ttl=52 time=48.188 ms
```

  In addition, because NDFC is considered a new product instance, you must re-establish trust. If you took the backup with an expired Trust Token, you must manually run the Smart Licensing Configuration wizard and enter a valid token after the upgrade.

Step 6 Restore the configuration backup in the new cluster using the unified backup and restore functionality introduced in Nexus Dashboard release 3.2.1.

For more information, see *Unified Backup and Restore for Nexus Dashboard and Services*.

a) On-board any NDFC fabrics prior to restoring from a backup.

In these procedures, you will be restoring from a backup that you took previously. If NDFC services were part of the ND when that backup was taken, then you must on-board the NDFC fabrics before you begin this restore process.

b) Navigate to the unified backup and restore page in the Admin Console GUI: **Admin** > **Backup & Restore**.

Backups that are already configured are listed in the **Backups** page.

c) Access the **Restore** slider page using either of the following methods:

- Click the ellipsis (…) on any backup that you want to restore and choose **Restore**, or
- Click **Restore** in the upper right corner of the main **Backup and Restore** page.

The **Restore** slide page appears.

d) In the **Source** field, determine where the backup is that you want to restore, if applicable.

Note If you are restoring a backup by clicking the ellipsis (…) on a specific backup, then this field is not editable.

- **Upload Configuration Backup Table**: The Backup File area appears, where you can either drag and drop a local backup file to restore or you can navigate to the local area on your system to select a backup file to restore.
- **Remote Location**:

  1. In the **Remote Location** field, select an already-configured remote location from the list, if available, or click **Create Remote Location**.

     If you click **Create Remote Location**, follow the procedures provided in "Configuring Remote Locations" in *Unified Backup and Restore for Nexus Dashboard and Services*, then return here. Even though you should

have configured a remote location as part of the remote backup process, you might also have to configure a remote location as part of the restore process if you're in a different cluster from the one where you configured the remote backup. In this case, you would be configuring the remote location again at this point so that the system can find the remote backup that you configured in the other cluster.

2. In the **Remote Path** field, enter the remote path where the remote backup resides.

e) In the **Encryption Key** field, enter the encryption key that you used when you backed up the file.
f) In the Validation area, on the row with your backup, click **Validate and Upload**.
g) When the Progress bar shows 100% for the validation, the **Next** button becomes active. Click **Next**.
h) (Optional) Check the **Ignore External Service IP Configuration** check box, if necessary.

If the **Ignore External Service IP Configuration** check box is selected, then the external service IP configuration is ignored. This selection allows you to take a backup on a system and restore it on a different system, with different management and/or data subnets.

i) Click **Restore**.

A warning window appears to verify that you want to begin the restore process. Note that you will not be able to access any Nexus Dashboard functionality while the restore process runs, which could take several minutes.

j) Click **Restore** in the warning window to proceed with the restore process.

Another window appears, showing the progress of the restore process. Click the arrow next to the entry in the **Type** column to get more details of the restore process.

k) If the restore process is successful, you will see 100% as the Progress, and the **View History** button becomes active.

Click **View History** to navigate to the **History** area in the **Backup and Restore** window, with the restore process displayed and **Success** shown in the **Status** column.

Note After you have restored a configuration that was backed up using the new ND unified backup and restore feature, the state of the NDFC fabrics shown at the ND level might be out of sync with the true state of the NDFC fabrics. To bring the NDFC fabrics status back in sync, in the **Fabric Overview** page, click **Actions** at the top of the page and select **Recalculate and Deploy**.

Step 7 Complete the post-upgrade tasks.

a) If you are using the SAN Controller persona:

After restoring the data from backup, all the server-smart licenses are **OutofCompliance**.

You can migrate to Smart Licensing using Policy from the **Operations** > **License Management** > **Smart** page in the UI and establish trust with CCSM using SLP.

b) If you are using the Fabric Controller persona:

The following features are not carried over when you upgrade from DCNM 11.5(4):

- Endpoint Locator must be reconfigured
- IPAM Integration must be reconfigured
- Alarm Policies must be reconfigured
- Custom topologies must be recreated and saved
- PM collection must be re-enabled on fabrics

- Temperature data collection must be re-enabled to start collecting data
- Switch images must be uploaded

Deployment Type in Release 11.5(4)	In 11.5(4), trap IP address is collected from	LAN Device Management Connectivity	Trap IP address after upgrade	Result
LAN Fabric Media Controller	`eth1` (or `vip1` for HA systems)	Management	Belongs to Management subnet	Honored There is no configuration difference. No further action required.
LAN Fabric Media Controller	`eth0` (or `vip0` for HA systems)	Management	Does not belong to Management subnet	Ignored, another IP from the Management pool will be used as trap IP. Configuration difference is created. On the **Web UI** > **LAN** > **Fabrics** > **Fabrics**, double click on the Fabric to view **Fabric Overview**. From **Fabrics Actions** drop-down list, select **Recalculate Config**. Click **Deploy Config**.
LAN Fabric Media Controller	`eth0` (or `vip0` for HA systems)	Data	Belongs to Data subnet	Honored There is no configuration difference. No further action required.

Deployment Type in Release 11.5(4)	In 11.5(4), trap IP address is collected from	LAN Device Management Connectivity	Trap IP address after upgrade	Result
LAN Fabric Media Controller	`eth0` (or `vip0` for HA systems)	Data	Does not belong to Data subnet	Ignored, another IP from the Data pool will be used as trap IP. Configuration difference is created. On the **Web UI > LAN > Fabrics > Fabrics**, double click on the Fabric to view **Fabric Overview**. From **Fabrics Actions** drop-down list, select **Recalculate Config**. Click **Deploy Config**.
SAN Management	OVA/ISO – • `trap.registaddress` (if set) • eth0 (if `trap.registaddress` is not set) Windows/Linux – • `trap.registaddress` (if set) • Interface based on event-manager algorithm (if `trap.registaddress` is not set	Not applicable	Belongs to Data subnet	Honored There is no configuration difference. No further action required.
		Not applicable	Does not belong to Data subnet	Ignored, another IP from the Data pool will be used as trap IP.