Installing Cisco DCNM

This chapter contains the following sections:

Installing Cisco DCNM on Windows

Downloading the Cisco DCNM Windows Installer and Properties File

The first step to installing the DCNM on Windows is to download the dcnm.exe file.

Note If you plan to use Federation application functions, you must deploy the dcnm.exe 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 on 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 .

Step 5 Locate the DCNM Windows Installer and click the **Download** icon.

The installer file is of the format .

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM using GUI

Installing Cisco DCNM on Windows Using the GUI

Perform the following steps to install DCNM Windows using the GUI:

Procedure

Step 1 Locate the `dcnm.exe` file that you have downloaded.

Double click on the `dcnm.exe` file.

InstallAnywhere progress bar appears showing the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from the OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager.
- IBM—to install the IBM Data Center Network Manager.

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation. In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the dcnm.exe.
- Existing PostgreSQL 9.4
- Existing Oracle 10g/11g/12c
- Existing Oracle 10g/11g/12c RAC

  In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click OK. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there are no schemas existing with the DCNM

username, or if you do not have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, which is known as “public”.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the DCNM DB User field, enter the username that the Cisco DCNM uses to access the database. In the DCNM DB Password field, enter the password for the database user account that you specified. If you select **Add Server to an existing federation**, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.
- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are not commonly used. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM LAN archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.

- Click **Restore Default Folder** to retain the default folder.

  Note Ensure that this folder is accessible by all nodes in the Federation setup.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access both DCNM SAN and DCNM LAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

  Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may 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 any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server should use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

You can configure LDAP authentication after installing DCNM.

Note After TACACS/RADIUS/LDAP is enabled, Local user "admin" cannot be accessible. This is default behavior.

Only if the TACACS/RADIUS/LDAP server is not reachable or down, the Local user will be validated and will be able to login.

If LDAP/RADIUS/TACACS server is reachable and authentication fails on TACACS/LDAP/RADIUS then no fall back to local.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

Step 12 In the Choose Shortcut Folder screen, specify path where you want to create the DCNM icons.

If you want the installer to create the shortcuts for all users who can log into the server system, check the **Create icons for All Users** check box.

Click **Next**.

Step 13 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 14 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 15 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Wait until the DCNM is deployed on the system.

The prompt will return after the silent install is complete.

Step 16 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Windows for LAN and SAN Management.

Installing Cisco DCNM Windows in a Server Federation Environment using GUI

To install DCNM in a server federation environment:

Before you begin

Ensure that you have installed DCNM on the Primary server. Follow the instructions provided in Installing Cisco DCNM on Windows Using the GUI, on page 2 section.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers was enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If user you wants to use only strong ciphers for network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM user name and password of the primary server. Also, you must provide the database user name and password of the primary server.

The user name and password of the database are same for all the server installation forming the federation. Similarly, the user name and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM through Silent Installation

Installing Cisco DCNM Windows through Silent Installation

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

Perform the following steps to install DCNM Windows through silent installation.

Procedure

Step 1 Unzip, extract and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties--------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=C:\\Program Files\\Cisco Systems
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#-----------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

PG_DB_PATH=C:\\Program Files\\Cisco Systems\\dcm\\db

#----------New Postgres---------------------------------
DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
```

If you are using the Oracle database, edit this block:

```
#-----------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#-------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 4 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#-------------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-------------------------------------------------------------------------
```

Step 5 Navigate to the directory where you downloaded the Cisco DCNM Windows software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *path_of_installer.properties_file*

You can check the status of installation in the Task Manager process.

Step 6 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM on Linux

Downloading the Cisco DCNM Linux Installer and Properties File

The first step to installing the DCNM on Linux is to download the dcnm.bin file.

Note If you plan to use Federation application functions, you must deploy the dcnm.bin 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 on 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 11.0(1).

Step 5 Locate the DCNM Linux Installer and click the **Download** icon.

The installer file is of the format `dcnm-installer-x64.11.0.1.bin`.

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM using GUI

Installing Cisco DCNM on Linux Using the GUI

Perform the following steps to install DCNM Linux using the GUI:

Procedure

Step 1 Locate the `dcnm-installer-x64.<release-name>.bin` file that you have downloaded.

Run the `dcnm.bin` installer file.

InstallAnywhere progress bar appears showing the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager
- IBM—to install IBM Data Center Network Manager

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation. In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the `dcnm.bin`.
- Existing PostgreSQL 9.4—Existing PostgreSQL database that is already set up, with a clean schema.
- Existing Oracle 10g/11g/12c—Existing Oracle database that is already set up, with a clean schema.
- Existing Oracle 10g/11g/12c RAC—Existing Oracle database that is already set up, with a clean schema.

In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click **OK**. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Note Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there is no schema existing with the DCNM username, or if you do not have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, known as “public”.

If the tables are created in the default schema, you may encounter authentication issues after upgrading Cisco DCNM. You will have to create a schema with the sane name as the DCNM username owned by the same username. For instructions, see User and Schemas.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the **DCNM DB User** field, enter the username that Cisco DCNM user uses to access the database. In the **DCNM DB Password** field, enter the password for the database user account that you specified. If you select **Add Server to an existing federation**, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in Federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.
- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are free. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.

- Click **Restore Default Folder** to retain the default folder.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access DCNM SAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

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

- It must be at least eight 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 any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server must use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

The Choose Link Folder is skipped and by default the location is `/root` directory.

Step 12 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 13 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 14 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Wait until the DCNM is deployed on the system.

Step 15 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM Linux in a Server Federation Environment Using GUI

To install DCNM in a server federation environment:

Before you begin

Ensure that you have installed DCNM on the Primary server. Follow the instructions in Installing Cisco DCNM on Linux Using the GUI, on page 8 section.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers were enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If you use only strong ciphers for the network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM username and password of the primary server. Also, you must provide the database username and password of the primary server.

The username and password of the database are same for all the server installation forming the federation. Similarly, the username and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM through Silent Installation

Installing Cisco DCNM Linux Through Silent Installation

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

Perform the following steps to install DCNM Linux through silent installation.

Procedure

Step 1 Unzip, extract, and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties---------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=/usr/local/cisco/dcm
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
```

```
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#--------------New Postgress--------------------------
PG_DB_PATH=/usr/local/cisco/dcm/db

#PG_DB_PATH=/opt/dctest/cisco/dcm/db /*non-default installation directory*/
#BACKUP_FILE=/opt/dctest/cisco/dcm/dcnm/bin/<backup-filename> /*non-default backup file
directory*/

DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
#CLEAN_DATABASE=TRUE
```

If you are using the Oracle database, edit this block:

```
#------------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE
ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the Data Path for DCNM.

```
#--------------------DATA PATH----------------
#Data path is the folder location where DCNM LAN related
#information like Config archives, templates etc. are stored.
# In DCNM LAN Cluster mode this folder has to be a shared folder.
#For linux and windows it will be different as the folder structure vaires
#-----------------------------------------------------

DATA_PATH=/usr/local/cisco/dcm/dcnm
#---------------------DATA PATH----------------
```

Step 4 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#-----------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 5 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
```

```
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#-------------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-------------------------------------------------------------------------
```

Step 6 Navigate to the directory where you downloaded the Cisco DCNM Linux software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *path_of_installer.properties_file*

You can check the status of installation by using the following command **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

Step 7 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Linux for SAN Management.