



Administration

This chapter contains the following topics:

- [DCNM Server, on page 1](#)
- [Manage Licensing, on page 16](#)
- [Management Users, on page 27](#)
- [Performance Setup, on page 34](#)
- [Event Setup, on page 36](#)
- [Credentials Management, on page 40](#)

DCNM Server

The DCNM Server menu includes the following submenus:

Starting, Restarting, and Stopping Services

By default, the ICMP connectivity between DCNM and its switches validates the connectivity during Performance Management. If you disable ICMP, Performance Management data will not be fetched from the switches. You can configure this parameter in the **server properties**. To disable ICMP connectivity check from Cisco DCNM Web UI, choose **Administration > DCNM Server > Server Properties**, and set `skip.checkPingAndManageable` parameter value to `true`.

To clean up the performance manager database (PM DB) stale entries, start, restart, or stop a service, from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > DCNM Server > Server Status**.
The **Status** window appears that displays the server details.
- Step 2** In the **Actions** column, click the action you want to perform. You can perform the following actions:
- Start or restart a service.
 - Stop a service.
 - Clean up the stale PM DB entries.

- Reinitialize the Elasticsearch DB schema.

Step 3 View the status in the **Status** column.

What to do next

See the latest status in the **Status** column.

From Cisco DCNM Release 11.4(1), you can see the status of the following services as well:



Note The following services are available for OVA/ISO deployments only.

- NTPD server: NTPD service running on DCNM OVA, the IP address, and the port to which the service is bound.
- DHCP server: DHCP service running on DCNM OVA, the IP address, and the port to which the service is bound.
- SNMP traps
- Syslog Receiver

The DCNM servers for these services are as follows:

Service Name	DCNM Server
NTPD Server	0.0.0.0:123
DHCP Server	0.0.0.0:67
SNMP Traps	0.0.0.0:2162
Syslog Server	0.0.0.0:514

Using the Commands Table

The commands table contains links to commands that launch new dialog boxes to provide information about the server status and server administrative utility scripts. You can execute these commands directly on the server CLI.

- **ifconfig**: click this link to view information about interface parameters, IP address, and netmask used on the Cisco DCNM server.
- **appmgr status all**: click this link to view the DCNM server administrative utility script that checks the status of different services currently running.
- **appmgr show vmware-info**: click this link to view information about the CPU and Memory of Virtual Machine.
- **clock**: click this link to view information about the server clock details such as time, zone information.



Note The commands section is applicable only for the OVA or ISO installations.

Customization

From Cisco DCNM Release 11.3(1), you can modify the background image and message on the Web UI login page. This feature helps you to distinguish between the DCNM instances, when you have many instances running at the same time. You can also use a company-branded background on the login page. Click on Restore Defaults to reset the customizations to their original default values.

To remove the customizations and restore to the default values, click **Restore defaults**.

Login Image

This feature allows you to change the background image on the Cisco DCNM Web UI login page. If you have many instances of DCNM, this will help you identify the correct DCNM instance based on the background image.

To edit the default background image for your Cisco DCNM Web UI login page, perform the following steps:

1. Choose **Administration > DCNM Server > Customization**.
2. In the Login Image area, click **Add (+)** icon.

Browse for the image that you need to upload from your local directory. You can choose any of the following format images: JPG, GIF, PNG, and SVG.

3. Select the image and click **Open**.

A status message appears on the right-bottom corner.

```
Login image
Upload Successful
```



Note We recommend that you upload a scaled image for fast load times.

The uploaded image is selected and applied as the background image.

4. To choose an existing image as login image, select the image and wait until you see the message on the right-bottom corner.
5. To revert to the default login image, click **Restore Defaults**.

Message of the day (MOTD)

This feature allows you to add a message to the Cisco DCNM Web UI login page. You can a list of messages that will rotate on the configured frequency. This feature allows you to convey important messages to the user on the login page.

To add or edit the message of the day on the Cisco DCNM Web UI login page, perform the following steps:

1. Choose **Administration > DCNM Server > Customization**.
2. In the **Message of the day (MOTD)** field, enter the message that must appear on the login page.
3. Click **Save**.

Viewing Log Information

You can view the logs for performance manager, SME server, web reports, web server, and web services. These processes have no corresponding GUI that allows you to view information about these log files. If you see errors, preserve these files for viewing.

Beginning with Release 11.2(1), for DCNM OVA and DCNM ISO installations, all log files with .log extension are also listed.



Note Logs cannot be viewed from a remote server in a federation.

To view the logs from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Logs**.

You see a tree-based list of logs in the left column. Under the tree, there is a node for every server in the federation. The log files are under the corresponding server node.

Step 2 Click a log file under each node of the tree to view it on the right.

Step 3 Double-click the tree node for each server to download a ZIP file containing log files from that server.

Step 4 (Optional) Click **Generate Techsupport** to generate and download files required for technical support.

This file contains more information in addition to log files.

Note A TAR.GZ file will be downloaded for OVA and ISO deployments, and a ZIP file will be downloaded for all other deployments. You can use the use **appmgr tech_support** command in the CLI to generate the techsupport file.

Step 5 (Optional) Click the **Print** icon on the upper right corner to print the logs.

Server Properties

You can set the parameters that are populated as default values in the DCNM server.

To set the parameters of the DCNM server from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > DCNM Server > Server Properties**.
- Step 2** Click **Apply Changes** to save the server settings.
-

Configuring SFTP/TFTP/SCP Credentials

A file server is required to collect device configuration and restoring configurations to the device.

To configure the SFTP/TFTP/SCP credentials for a file store from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > DCNM Server > Archive FTP Credentials**.

The **Archive FTP Credentials** window is displayed.

Note The credentials are auto-populated for fresh OVA and ISO installations.

- Step 2** In the **Server Type** field, use the radio button to select **SFTP**.

Note

- You must have an SFTP server to perform backup operation. The SFTP server can be an external server. The SFTP directory must be an absolute Linux/SSH path format and must have read/write access to the SFTP User.
- If you are using an external server, enter its IP address in the **server.FileServerAddress** field in **Administration > DCNM Server > Server Properties**.
- If the **nat.enabled** field under **Administration > DCNM Server > Server Properties** is true, you must enter the NAT device IP in the **server.FileServerAddress** field and the SFTP server must be local.

- a) Enter the **User Name** and **Password**.

Note From Release 11.3(1), for OVA/ISO installations, use the **sysadmin** user credentials to access the root directory.

- b) Enter the **Directory** path.

The path must be in absolute Linux path format.

If SFTP is unavailable on your device, you can use third-party SFTP applications, such as, mini-SFTP, Solarwinds, and so on. When you use an external SFTP, you must provide the relative path in the SFTP Directory Path. For example, consider the use cases at the end of this procedure.

Note From Release 11.3(1), for OVA/ISO installations, enter directory as `/home/sysadmin`.

- c) From the **Verification Switches** drop-down list, select a switch.
- d) Click **Apply** to save the credentials.

- e) Click **Verify & Apply** to verify if SFTP and switch have connectivity and save the configuration.
If there are any failures during the verification, the new changes will not be stored.
- f) Click **Clear SSH Hosts** to clear SSH hosts for all switches or selected switches.
If there is a failure in any of the switches, an error message appears. Navigate to **Configure > Backup > Switch Configuration > Archive Jobs > Job Execution Details** to view the number of successful and unsuccessful switches.

Step 3 In the **Server Type** field, use the radio button to select **TFTP**.

Cisco DCNM uses a local TFTP server for data transfer. Ensure that there is no external TFTP server running on the DCNM server.

Note Ensure that your switch user role includes the copy command. Operator roles receive a *permission denied* error. You can change your credentials in the **Discovery** window. Navigate to **Inventory > Discovery**.

- a) From the **Verification Switch** drop-down list, select a switch.
- b) Click **Apply** to save the credentials everywhere.
- c) Click **Verify & Apply** to verify if TFTP and switch have connectivity and save the configuration.
If there are any failures during the verification, the new changes are not stored.

Step 4 In the **Server Type** field, use the radio button to select **SCP**.

Note

- You must have an SCP server to perform backup operation. The SCP server can be an external server. The SCP directory must be an absolute Linux/SSH path format and must have read/write access to the SCP User.
- If you are using an external server, enter its IP address in the **server.FileServerAddress** field under **Administration > DCNM Server > Server Properties**.
- If the **nat.enabled** field under **Administration > DCNM Server > Server Properties** is true, you must enter the NAT device IP in the **server.FileServerAddress** field and the server must be local.

- a) Enter the **User Name** and **Password**.
- b) Enter the **Directory** path.

The path must be in absolute Linux path format.

If SCP is unavailable on your device, use external SCP applications, such as, mini-SCP, Solarwinds, and so on. When you use an external SCP, you must provide the relative path in the SCP Directory Path. For example, consider the use cases at the end of this procedure.

- c) From the **Verification Switches** drop-down, select the switch.
- d) Click **Apply** to save the credentials everywhere.
- e) Click **Verify & Apply** to verify if SCP and switch have connectivity and save the configuration. If there are any failures during the verification, the new changes will not be stored.
- f) Click **Clear SSH Hosts** to clear SSH hosts for all switches or selected switches.

If there is a failure in any of the switches, an error message is displayed. To view the number of successful and unsuccessful switches, go to **Configure > Backup > Switch Configuration > Archive Jobs > Job Execution Details**.

Step 5 Choose **Configuration > Templates > Templates Library > Jobs** to view individual device verification status.

The configurations that are backed up are removed from the file server and are stored in the file system.

SFTP Directory Path

Use Case 1:

If Cisco DCNM is installed on Linux platforms, like OVA, ISO, or Linux, and the test folder is located at `/test/sftp/`, you must provide the entire path of the SFTP directory. In the SFTP Directory field, enter `/test/sftp`.

Use Case 2:

If Cisco DCNM is installed on the Windows platform, and the test folder is located at `C://Users/test/sftp/`, you must provide the relative path of the SFTP directory. In the SFTP Directory field, enter `/`.

For Example:

- If the path in the external SFTP is `C://Users/test/sftp/`, then the Cisco DCNM SFTP Directory path must be `/`.
- If the path in the external SFTP is `C://Users/test`, then the Cisco DCNM SFTP Directory path must be `/sftp/`.

Examples for SCP Directory Path

Use Case 1:

If Cisco DCNM is installed on Linux platforms, like OVA, ISO, or Linux, and the test folder is located at `/test/scp/`, you must provide the entire path of the SCP directory. In the **SCP Directory** field, enter `/test/scp`.

Use Case 2:

If Cisco DCNM is installed on the Windows platform, and the test folder is located at `C://Users/test/scp/`, you must provide the relative path of the SCP directory. In the **SCP Directory** field, enter `/`.

For Example:

- If the path in the external SCP is `C://Users/test/scp/`, then the Cisco DCNM SCP directory path must be `/`.
- If the path in the external SCP is `C://Users/test`, then the Cisco DCNM SCP directory path must be `/scp/`.

Modular Device Support

To support any new hardware that does not require many major changes, a patch can be delivered instead of waiting for the next DCNM release. **Modular Device Support** helps to deliver and apply the DCNM patch

releases. An authorized DCNM administrator can apply the patch to the production setup. Patch releases are applicable for the following scenarios:

- Support any new hardware, like chassis or line cards
- Support latest NX-OS versions
- Support critical fixes as patches

To view the patch details from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Modular Device Support**.

You see the **DCNM Servers** column on the left in the window and **Modular Device support information** window on the right.

Step 2 Expand **DCNM Servers** to view all the DCNM servers.

It includes the list of patches installed along with the version number, corresponding platforms supported, chassis supported, NX-OS version supported, PID supported, backup directory and the last patch deployment time in the **Modular Device support information** table.

What to do next

For more details about how to apply and rollback a patch, go to <http://www.cisco.com/go/dcnm> for more information.

Managing Switch Groups

You can configure switch groups by using Cisco DCNM Web UI. You can add, delete, or move a switch to a group, or move switches from a group to another group.

Creating switch groups will help you to manage switches because they are grouped logically. For example, you can create host or flow policies for switches in a specific switch group instead of creating it for all the switches. Similarly, you can view the flow topology for a specific switch group containing switches.

The switch groups are listed under the **SCOPE** drop-down list at the top right part of windows under **Media Controller**.



Note The hostname of the switch should be unique across all the switch groups. You cannot have the same hostname and management IP address for two different switches in two switch groups.

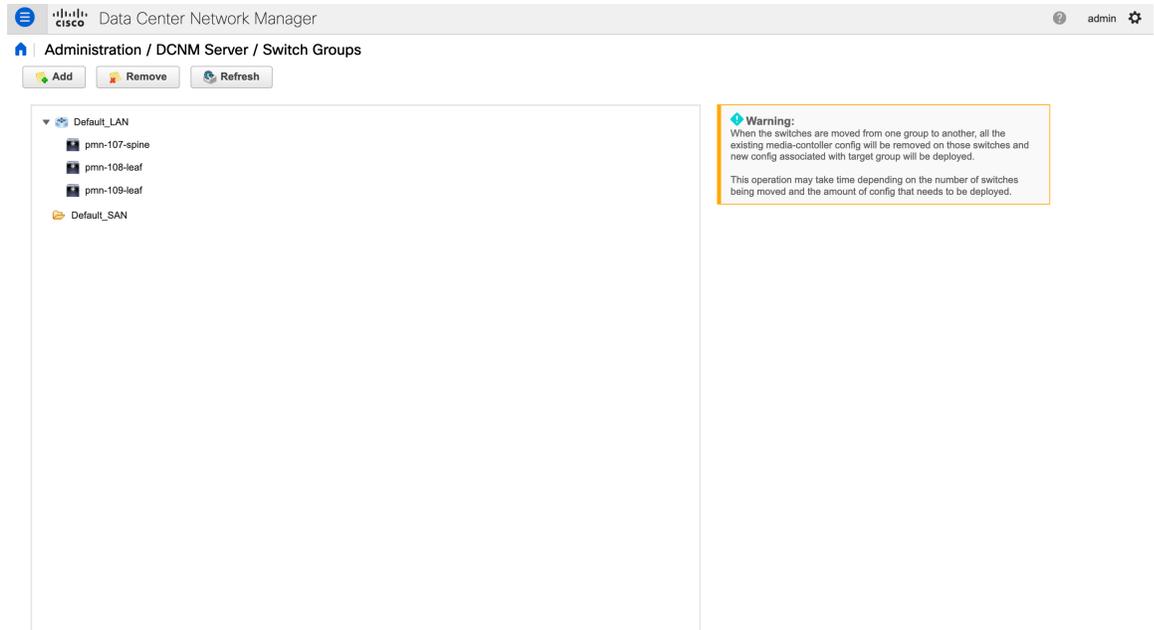
This section contains the following:

Adding Switch Groups

To add switch groups from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > DCNM Server > Switch Groups**.



Step 2 Click the **Add** icon.

The **Add Group** window is displayed, that allows you to enter the name for the switch group.

Step 3 Enter the name of the switch group and click **Add** to complete adding the switch group.

The switch group name validation, and the maximum tree depth is 10. If you do not choose a parent group before adding a new switch group, the new group is added on the top of the hierarchy.

Whenever you add a new switch group, the default policies are automatically created for this switch group.

Note When you discover and add a switch in DCNM, you can choose the switch group for the new switch. For more information, see *Adding LAN Switches*.

Removing a Group or a Member of a Group

You can remove a group or a member of the group from the Cisco DCNM Web UI. When you remove a group, the ethernet switches of the deleted group are moved to the default LAN group. When you remove a member of a group, the member is moved to the default LAN group.

To remove a group or a member of a group from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose the switch group or members of a group that you want to remove.

Step 2 Click the **Remove** icon.

A dialog box prompts you to confirm the deletion of the switch group or the member of the group.

Note When you remove a switch from a switch group, a dialog box does not pop-up for a confirmation. The switch is moved to the **Default_LAN** switch group after you click the **Remove** icon. A switch can be removed from the **Default_LAN** switch group by navigating to **Inventory > Discovery > LAN Switches** and using the delete option. If you delete a switch, it will be not managed by DCNM.

Step 3 Click **Yes** to delete or **No** to cancel the action.

Note **Default_LAN** is the default group that cannot be removed or deleted.

Moving a Switch to Another Group

To move a switch to another group from the Cisco DCNM Web UI, perform the following steps:



Warning When the switches are moved from one group to another, all the existing media-controller config will be removed on those switches and new config associated with target group will be deployed.

This operation may take time depending on the number of switches being moved and the amount of config that needs to be deployed.

Procedure

Step 1 Select a switch.

Step 2 Drag the highlighted switch to another group. To move multiple switches across different switch groups, use Ctrl key or Shift key.

Native HA

Before you begin



Note Ensure that you clear your browser cache and cookies everytime after a Federation switchover or failover.

Procedure

Step 1 By default, DCNM is bundled with an embedded database engine PostgreSQL. The native DCNM HA is achieved by two DCNMs running as **Active / Warm Standby**, with their embedded databases synchronized in real time. So once the active DCNM is down, the standby takes over with the same database data and resume the operation. The *standby host database down* scenario is documented after this procedure.

- Step 2** From the menu bar, choose **Administration > DCNM Server > Native HA**.
You see the **Native HA** window.
- Step 3** You can allow manual failover of DCNM to the standby host by clicking the **Failover** button, and then click **OK**.
- Alternatively, you can initiate this action from the Linux console.
 - a. SSH into the DCNM active host.
 - b. Enter " " /usr/share/heartbeat/hb_standby"
- Step 4** You can allow manual syncing database and disk files to standby host by clicking **Force Sync**, and then click **OK**.
- Step 5** You can test or validate the HA setup by clicking **Test** and then click **OK**.

What to do next

Some HA troubleshooting scenarios are noted in this sub section.

The standby host database is down: Typically, the DCNM database (PostgreSQL) is up on the active and standby hosts. In DCNM 10.1 and earlier versions, the standby database can be down due to a database synchronization failure.

- Enter “ps -ef | grep post”. You should see multiple postgres processes running. If not, it indicates that the database is down.
- Restore database data from a backup file that is created at the beginning of database synchronization. Change directory to “/usr/local/cisco/dcm/db”
- Check existence of file replication/ pgsq-standby-backup.tgz. If the file exists, restore database data files:

```
rm -rf data/*
tar -zxf replication/pgsq-standby-backup.tgz data
/etc/init.d/postgresql-9.4 start
ps -ef | grep post
```

The active DCNM host will synchronize the two databases.

The TFTP server is not bound to the eth1 VIP address on the active host: The TFTP server should run on the active host (not on the standby host), and it should be bound to the eth1 VIP address. In some setups, the bind address is not the VIP address, as per the TFTP configuration file, and this could cause issues when switches try to use TFTP.

- Enter “grep bind /etc/xinetd.d/tftp” to check if the TFTP configuration file has the right bind address. If the displayed IP address is not the eth1 VIP address, then change the bind address to the VIP address. Repeat the procedure for the standby host. Update the bind address to the VIP address.
- Enter " " /etc/init.d/xinetd restart” on the active host to restart TFTP.



Note The TFTP server can be started or stopped with the “appmgr start/stop ha-apps” command.

Multi Site Manager

Procedure

-
- Step 1** Multi-Site-Manager (MsM) provides a single pane for users to search for switches that are managed by DCNM globally. MSM can do realtime search to find out which switch globally handles the traffic for a given virtual machine based on IP address, name or mac address, and supporting VXLAN basing on segment ID as well. It provides hyperlink to launch the switch only. This window also plays the role of remote site registration. The registration only allows the current DCNM server to access the remote DCNM server or site. For the remote site to access the current DCNM server, registration is required on the remote site as well.
- Step 2** Choose **Administration > DCNM Server > Multi Site Manager**.
- The MsM window displays the overall health or status of the remote site and the application health.
- Step 3** You can search by **Switch, VM IP, VM Name, MAC, and Segment ID**.
- Step 4** You can add a new DCNM server by clicking **+Add DCNM Server**. The **Enter Remote DCNM Server Information** window opens. Fill in the information that is required and click **OK** to save.
- Step 5** Click **Refresh All Sites** to display the updated information.
-

NX-API Certificate Management for Switches

Cisco NX-OS switches require an SSL certificate to function in NX-API HTTPS mode. You can generate the SSL certificates and get it signed by your CA. You can install the certificates manually using CLI commands on switch console.

From Release 11.4(1), Cisco DCNM provides a Web UI framework to upload NX-API certificates to DCNM. Later, you can install the certificates on the switches that are managed by DCNM.

This feature is supported only on Cisco DCNM OVA/ISO deployments.



Note This feature is supported on switches running on Cisco NXOS version 9.2(3) or higher.

For each switch, the data center administrator generates an ASCII (base64) encoded certificate. This certificate comprises two files:

- `.key` file that contains the private key
- `.crt/.cer/.pem` file that contains the certificate

Cisco DCNM also supports a single certificate file that contains an embedded key file, that is, `.crt/.cer/.pem` file can also contain the contents of `.key` file.

DCNM doesn't support binary encoded certificates, that is, the certificates with `.der` extension are not supported. You can protect the key file with a password for encryption. Cisco DCNM does not mandate encryption; however, as this is stored on DCNM, we recommend that you encrypt the key file. DCNM supports AES encryption.

You can either choose CA-signed certificates or self-signed certificates. Cisco DCNM does not mandate the signing; however, the security guidelines suggest you use CA-signed certificates.

You can generate multiple certificates meant for multiple switches, to upload to DCNM. Ensure that you name the certificates appropriately, to help you choose the switch meant for that certificate.

You can upload one certificate and corresponding key file, or bulk upload multiple certificates and key files. After the upload is complete, you can view the upload list before installing these on the switches. If a certificate file that contains an embedded key file is uploaded, DCNM derives the key automatically.

Certificate and the key file must have the same filename. For example, if a certificate filename is `mycert.pem`, the key filename must be `mycert.key`. If the certificate and key pair filenames are not the same, then DCNM will not be able to install the certificate on the switch.

Cisco DCNM allows you to bulk install the certificates to the switches. Because bulk installation uses the same password, all encrypted keys must be encrypted with the same password. If the password is different for a key, you cannot install the certificate in bulk mode. Bulk mode installation allows you to install encrypted and unencrypted keys certificates together, but all encrypted keys must have the same password.

When you install a new certificate on the switch, it replaces the existing certificate and replaces it with the new certificate.

You can install the same certificate on multiple switches; however, you cannot use the bulk upload feature.



Note DCNM doesn't enforce the validity of certificates or options provided in it. It is up to you and the requirements on the switch to follow the convention. For example, if a certificate is generated for Switch-1 but it is installed on Switch-2, DCNM doesn't enforce it; switches may choose to accept or reject a certificate based on the parameters in the certificate.

On Cisco DCNM Web UI > **Administration** > **DCNM Server** > **NX API Certificates**, the following tables are displayed:

- **Certificate Installation Status table:** Displays the status of certificates last installed on the switches. It also displays the time when the certificates were updated previously.
- **Certificates Uploaded to DCNM table:** Displays the certificates uploaded on DCNM and any switch association.

However, refer to the Certificate Installation Status table to see the certificate and switch association. Upload table is only meant for uploading certificates on DCNM and installing on the switches.

You can also watch the video that demonstrates how to use Switch NX-API SSL Certificate Management feature. See [Video: Switch NX-API SSL Certificate Management](#).

Uploading the certificates on DCNM

To upload the certificates onto DCNM using the Cisco DCNM Web Client UI, perform the following steps:

Procedure

- Step 1** Choose **Administration** > **DCNM Server** > **NX API Certificates**.

- Step 2** In the **Certificates Uploaded to DCNM** area, click **Upload Certificates** to upload the appropriate license file.
- Step 3** Browse your local directory and choose the certificate key pair that you must upload to DCNM.
You can choose certificates with extension .cer/.crt/.pem + .key file separately.
Cisco DCNM also allows you to upload a single certificate file that contains an embedded key file. The key file is automatically derived after upload.
- Step 4** Click **Open** to upload the selected files to DCNM.
A successful upload message appears. The uploaded certificates are listed in the **Certificates Uploaded to DCNM** area.
In the **Certificate Installation Status** area, the certificate appears, with Status as **UPLOADED**.
If the certificate is uploaded without the key file, the status shows **KEY_MISSING**.
-

Installing Certificates on Switches

To install certificates on the switches using Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > DCNM Server > NX API Certificates**.
- Step 2** In the **Certificate Installation Status** area, for each certificate, click on the **Switch** column.
- Step 3** From the drop-down list, select the switch to associate with the certificate.
Click **Save**.
- Step 4** Select the certificate that you need to install and click **Install Certificates on Switch**.
You can select multiple certificates to perform a bulk install.
- Step 5** In the **Bulk Certificate Install** window, upload the certificates to DCNM. Perform the following steps:
You can install a maximum of 20 certificates at the same instance, using the Bulk Install feature.
- a) Choose the file transfer protocol to upload the certificate to DCNM.
You can choose either SCP or SFTP protocol to upload the certificates.
 - b) Check the VRF checkbox for the certificates to support the VRF configuration.
Enter the VRF name that the switch uses to reach DCNM. Generally, DCNM is reached via management VRF of switches, but it can be any VRF that is configured on the switch that is used to reach DCNM.
 - c) In the NX-API Certificate Credentials, enter the password which was used to encrypt the key while generating the certificates.
Leave this field empty, if the key uploaded along with the certificate is not encrypted.
Note that you can install unencrypted and encrypted keys and a certificate in a single bulk install; however, you must provide the key password used for encrypted keys.
 - d) Click **Install**.

A notification message appears to confirm if the certificate was successfully installed on the specific switch.

In the Certificate Installation Status area, the Status of certificate now shows **INSTALLED**.

Unlinking and Deleting certificates

After the certificates are installed on the switch, DCNM cannot uninstall the certificate from DCNM. However, you can always install a new certificate on the switch. The certificates that are not installed on the switches can be deleted. To delete the certificate installed on the switch, you must unlink the certificate from the switch, and then delete it from DCNM.



Note Unlinking the certificate from the switch does not delete the certificate on the switch. The certificate still exists on the switch. Cisco DCNM cannot delete the certificate on the Switch.

To delete certificates from DCNM repository, using the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > DCNM Server > NX API Certificates**.
 - Step 2** In the **Certificate Installation Status** area, select the certificate(s) that you need to delete.
 - Step 3** Click **Clear Certificates**.
A confirmation message appears.
 - Step 4** Click **OK** to clear the selected certificates.
The status column shows **UPLOADED**. The Switch column shows **NOT_INSTALLED**.
 - Step 5** Select the certificate and click **Clear Certificates**.
The Certificate is removed from the Certificate Installation Status table.
 - Step 6** In the Certificates Uploaded to DCNM area, select the certificate that is now unlinked from the Switch.
Click **Delete Certificates**.
The certificate is deleted from DCNM.
-

Troubleshooting NX API Certificate Management

While installing a certificate, you can encounter errors. The following sections provide information about troubleshooting the NX-API Certificate Management for switches.

COPY_INSTALL_ERROR

Problem Statement: Error message COPY_INSTALL_ERROR

Reason Cisco DCNM cannot reach the switch.

Solution:

- Verify if the switch is reachable from Cisco DCNM. You can perform an SSH login and ping the switch to verify.
- Switch connects to DCNM through its management interface. Verify if you can ping DCNM from the Switch console. If the switch requires VRF, verify if the correct vrf is provided.
- If the certificate private key is encrypted, ensure that you provide the correct password.
- Verify if the correct key file is uploaded with the certificate. Ensure that the certificate file and the key file have the same filename.

CERT_KEY_NOT_FOUND

Problem Statement: Error message CERT_KEY_NOT_FOUND

Reason: Key file was not uploaded while uploading the certificate (.cer, .crt, .pem).

Solution:

- Ensure that the certificate (.cer, .crt, or .pem) file and its corresponding .key file has the same filename
For example: If the certificate file name is mycert.crt, the key file must be mycert.key.
- DCNM identifies key file with certificate file name, and therefore, it is necessary to have the key file with same filename.
- Upload the certificate and key file with same filename, and install the certificate.

Manage Licensing

The Manage Licensing menu includes the following submenus:

Managing Licenses

You can view the existing Cisco DCNM licenses by choosing **Administration > Manage Licensing > DCNM**. You can view and assign licenses in the following tabs:

- **License Assignments**
- **Smart License**
- **Server License Files**



Note By default, the **License Assignments** tab appears.

The following table displays the SAN and LAN license information.

Field	Description
License	Specifies SAN or LAN.
Free/Total Server-based Licenses	Specifies the number of free licenses that are purchased out of the total number of licenses. The total number of licenses for new installations are 50. However, the total number of licenses continues to be 500 for inline upgrade.
Unlicensed/Total (Switches/VDCs)	Specifies the number of unlicensed switches or VDCs out of the total number of switches or VDCs.
Need to Purchase	Specifies the number of licenses to be purchased.

This section includes the following topics:

License Assignments

The following table displays the license assignment details for every switch or VDC.

Field	Description
Group	Displays if the group is fabric or LAN.
Switch Name	Displays the name of the switch.
WWN/Chassis ID	Displays the world wide name or Chassis ID.
Model	Displays the model of the device. For example, DS-C9124 or N5K-C5020P-BF.
License State	Displays the license state of the switch that can be one of the following: <ul style="list-style-type: none"> • Permanent • Eval • Unlicensed • Not Applicable • Expired • Invalid
License Type	Displays the license type of the switch that can be one of the following: <ul style="list-style-type: none"> • DCNM-Server • Switch • Smart • Honor

Field	Description
Expiration Date	Displays the expiry date of the license. Note Text under the Expiration Date column is in red for licenses, which expire in seven days.
Assign License	Select a row and click this option on the toolbar to assign the license.
Unassign License	Select a row and click this option on the toolbar to unassign the license.
Assign All	Click this option on the toolbar to refresh the table and assign the licenses for all the items in the table.
Unassign All	Click this option on the toolbar to refresh the table and unassign all the licenses.



Note You must have network administrator privileges to assign or unassign licenses.

When the fabric is first discovered and if the switch does not have a valid switch-based license, a license is automatically assigned to the fabric from the file license pool until no more licenses are left in the pool. If you have an existing fabric and a new switch is added to the fabric, the new switch is assigned a license if one is available in the file license pool and if it does not already have a switch-based license.

After you register smart license, if you click **Assign License** for a switch that does not have a permanent license, a smart license is assigned to the switch. The priority of licenses that are assigned are in the following order:

1. **Permanent**
2. **Smart**
3. **Eval**

To assign license to switches through POAP, refer to [DCNM Licensing Guide](#).

Disabling smart licensing unassigns licenses of switches that were smart-licensed.

The evaluation license is assigned for switches that do not support smart licensing. The license state is **Eval** and the license type is **DCNM-Server**. See *Cisco DCNM Licensing Guide, Release 11.x* to view the list of switches that support smart licensing.

Smart License

From Cisco DCNM Release 11.1(1), you can use the smart licensing feature to manage licenses at device-level and renew them if required. From Cisco DCNM Web UI, choose **Administration > Manage Licensing > DCNM > Smart License**. You will see a brief introduction on Cisco smart licensing, a menu bar, and the **Switch Licenses** area.

Introduction to Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (<https://software.cisco.com/software/cs/ws/platform/home>).

For a more detailed overview on Cisco Licensing, go to <https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html>.

In the introduction, click **Click Here** to view the information on smart software licensing.

The menu bar has the following icons:

- **Registration Status:** Displays details of the current registration in a pop-up window when clicked. The value is **UNCONFIGURED** if the smart licensing is not enabled. After you enable the smart licensing without registering, the value is set to **DEREGISTERED**. The value is set to **REGISTERED** after you register. Click the registration status to view the last action, account details, and other registration details in the **Registration Details** pop-up window.
- **License Status:** Specifies the status of the license. The value is **UNCONFIGURED** if the smart licensing is not enabled. After you enable the smart licensing without registering, the value is set to **NO LICENSES IN USE**. The value is set to **AUTHORIZED** or **OUT-OF-COMPLIANCE** after registering and assigning licenses. Click the license status to view the last action, last authorization attempt, next authorization attempt, and the authorization expiry in the **License Authorization Details** pop-up window.
- **Control:** Allows you to enable or disable smart licensing, register tokens, and renew the authorization.

The following table describes the fields that appear in the **Switch Licenses** section.

Field	Description
Name	Specifies the license name.
Count	Specifies the number of licenses used.
Status	Specifies the status of the licenses used. Valid values are Authorized and Out of Compliance .
Description	Specifies the type and details of the license.
Last Updated	Specifies the timestamp when switch licenses were last updated.
Print	Allows you to print the details of switch licenses.

Field	Description
Export	Allows you to export the license details.

After you remove a product license from your account in Cisco Smart Software Manager, disable the smart licensing and register it again.

Enabling Smart Licensing

To enable smart licensing from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Manage Licensing > DCNM > Smart License**.

Step 2 Click **Control** and choose **Enable** in the drop-down list to enable the smart licensing.

A confirmation window appears.

Step 3 Click **Yes**.

Instructions to register the DCNM instance appear.

The registration status changes from **UNCONFIGURED** to **DEREGISTERED**, and the license status changes from **UNCONFIGURED** to **No Licenses in Use**.

Registering a Cisco DCNM Instance

Before you begin

Create a token in Cisco Smart Software Manager.

Procedure

Step 1 Choose **Administration > Manage Licensing > DCNM > Smart License**.

Step 2 Click **Control** and choose **Register** in the drop-down list.

The **Register** window appears.

Step 3 Select the transport option to register the smart licensing agent.

The options are:

- **Default - DCNM communicates directly with Cisco's licensing servers**

This option uses the following URL: <https://tools.cisco.com/its/service/oddce/services/DDCEService>

- **Transport Gateway - Proxy via Gateway or Satellite**

Enter the URL if you select this option.

- **Proxy - Proxy via intermediate HTTP or HTTPS proxy**

Enter the URL and the port if you select this option.

Step 4 Enter the registration token in the **Token** field.

Step 5 Click **Submit** to register the license.

The registration status changes from **DEREGISTERED** to **REGISTERED**. The name, count, and status of switch licenses appear.

Click **Registration Status: REGISTERED** to see the details of the registered token.

The switch details are updated under the **Switches/VDCs** section of the **License Assignments** tab. The license type and the license state of switches that are licensed using the smart license option are **Smart**.

What to do next

Troubleshoot communication errors, if any, that you encounter after the registration.

Troubleshooting Communication Errors

To resolve the communication errors during registration, perform the following steps:

Procedure

Step 1 Stop the DCNM service.

Step 2 Open the server properties file from the following path: /usr/local/cisco/dcm/fm/conf/server.properties

Note The server properties file for Windows will be in the following location: C:/Program Files/Cisco/dcm/fm/conf/server.properties

Step 3 Include the following property in the server properties file: #cisco.smart.license.production=false
#smartlicense.url.transport=https://CiscoSatellite_Server_IP/Transportgateway/services/DeviceRequestHandler

Step 4 Update the Cisco satellite details in Host Database in the /etc/hosts file in the following syntax:

```
Satellite_Server_IP CiscoSatellite
```

Step 5 Start the DCNM service.

Renew Authorization

You can manually renew the authorization only if you have registered. Automatic reauthorization happens periodically. Click **License Status** to view details about the next automatic reauthorization. To renew authorization from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Manage Licensing > DCNM > Smart License**.

Step 2 Click **Control** and choose **Renew Authorization** in the drop-down list to renew any licensing authorizations.

A request is sent to Cisco Smart Software Manager to fetch updates, if any. The **Smart Licenses** window is refreshed after the update.

Disabling Smart Licensing

To disable smart licensing from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Manage Licensing > DCNM > Smart License**.

Step 2 Select **Control** and select **Disable** to disable smart licensing.

A confirmation window appears.

Step 3 Click **Yes**.

The license status of the switches using this token, under the **License Assignments** tab, changes to **Unlicensed**. This token is removed from the list under the **Product Instances** tab in the Cisco Smart Software Manager.

If a smart license is not available and you disable smart licensing, release the license manually from the **License Assignments** tab.

Server License Files

From Cisco DCNM Web UI, choose **Administration > Manage Licensing > DCNM > Server License Files**. The following table displays the Cisco DCNM server license fields.

Field	Description
Filename	Specifies the license file name.
Feature	Specifies the licensed feature.
PID	Specifies the product ID.
LAN (Free/Total)	Displays the number of free versus total licenses for LAN.
Expiration Date	Displays the expiry date of the license. Note Text in the Expiration Date field is in Red for licenses that expires in seven days.

Adding Cisco DCNM Licenses

To add Cisco DCNM licenses from Cisco DCNM, perform the following steps:

Before you begin

You must have network administrator privileges to complete the following procedure.

Procedure

- Step 1** Choose **Administration > Manage Licensing > DCNM** to start the license wizard.
- Step 2** Choose the **Server License Files** tab.
- The valid Cisco DCNM-LAN license files are displayed.
- Ensure that the security agent is disabled when you load licenses.
- Step 3** Download the license pack file that you received from Cisco into a directory on the local system.
- Step 4** Click **Add License File** and select the license pack file that you saved on the local machine.
- The file is uploaded to the server machine, which is saved into the server license directory, and then loaded on to the server.
- Note** Ensure that you do not edit the contents of the .lic file or the Cisco DCNM software ignores any features that are associated with that license file. The contents of the file are signed and must remain intact. When you accidentally copy, rename, or insert the license file multiple times, the duplicate files are ignored, but the original is counted.
-

Switch Features—Bulk Install

From Release 11.3(1), Cisco DCNM allows you to upload multiple licenses at a single instance. DCNM parses the license files and extract the switch serial numbers. It maps the serial numbers in the license files with the discovered fabric to install the licenses on each switch. License files are moved to bootflash and installed.

To bulk install licenses to the switches on the Cisco DCNM Web Client UI, perform the following steps:

1. Choose **Administration > Manage Licensing > Switch features**.
2. In the Switch Licenses area, click **Upload License files** to upload the appropriate license file.
The Bulk Switch License Install window appears.
3. In the Select file, click **Select License file(s)**.
Navigate and choose the appropriate license file located in your local directory.
Click **Open**.
4. Choose the file transfer protocol to copy the license file from the DCNM server to the switch.
 - Choose either **TFTP**, **SCP**, or **SFTP** protocol to upload the license file.



Note Not all protocols are supported for all platforms. TFTP is supported for Win/RHEL DCNM SAN installation only. However, SFTP/SCP supported for all installation types.

5. Check the **VRF** check box for the licenses to support VRF configuration.
Enter the VRF name of one of their defined routes.

6. Check the **Overwrite file on Switch** checkbox, to overwrite the license file with the new uploaded license file.



Note The overwrite command copies the new file over the existing one in boot flash. If the previous license was already installed, it won't override the installation.

7. In the DCNM Server credentials, enter the root username and password for the DCNM server.
Enter the authentication credentials for access to DCNM. For DCNM Linux deployment, this is the username. For OVA\ISO deployments, use the credentials of the **sysadmin** user.
8. Click **Upload**.
The License file is uploaded to the DCNM. The following information is extracted from the license file.
 - Switch IP – IP Address of the switch to which this license is assigned.
 - License File – filename of the license file
 - Features List –list of features supported by the license file
9. Select the set of licenses that you want to upload and install on their respective switches. A license file is applicable for a single specific switch.
10. Click **Install Licenses**.
The selected licenses are uploaded and installed on their respective switches. Status messages, including any issues or errors are updated for each file as it completes.
11. After the license matches with respective devices and installs, the **License Status** table displays the status.

Switch-based honor license support

On the DCNM Web UI > **Inventory** > **Switch** > **License**, the **Type** column displays “Unlicensed Honor License” and **Warnings** column displays **Honor started: ...** with elapsed time since the license was changed to the Honor mode.

License

Feature	Status	Type	Warnings
NK_UPG_EX_10G	Unused	Unlicensed	
NETWORK_SERVICES_PKG	Unused	Unlicensed	
NEXUS_24PORTEX_UPGRADE	Unused	Unlicensed	
NEXUS_24PORTFX_UPGRADE	Unused	Unlicensed	
NEXUS_24PORT_LICENSE	In Use	Unlicensed Honor License	Honor started: 1 hours 2 mins 7 seconds
NXOS_ADVANTAGE_GF	Unused	Unlicensed	
NXOS_ADVANTAGE_M4	Unused	Unlicensed	
NXOS_ADVANTAGE_M5-16	Unused	Unlicensed	
NXOS_ADVANTAGE_XF	Unused	Unlicensed	
NXOS_ADVANTAGE_XF2	Unused	Unlicensed	
NXOS_ESSENTIALS_GF	Unused	Unlicensed	
NXOS_ESSENTIALS_M4	Unused	Unlicensed	
NXOS_ESSENTIALS_M5-16	Unused	Unlicensed	
NXOS_ESSENTIALS_XF	Unused	Unlicensed	
NXOS_ESSENTIALS_XF2	Unused	Unlicensed	
NXOS_OE_PKG	Unused	Unlicensed	
PORT_ACTIVATION_PKG	Unused	Unlicensed	



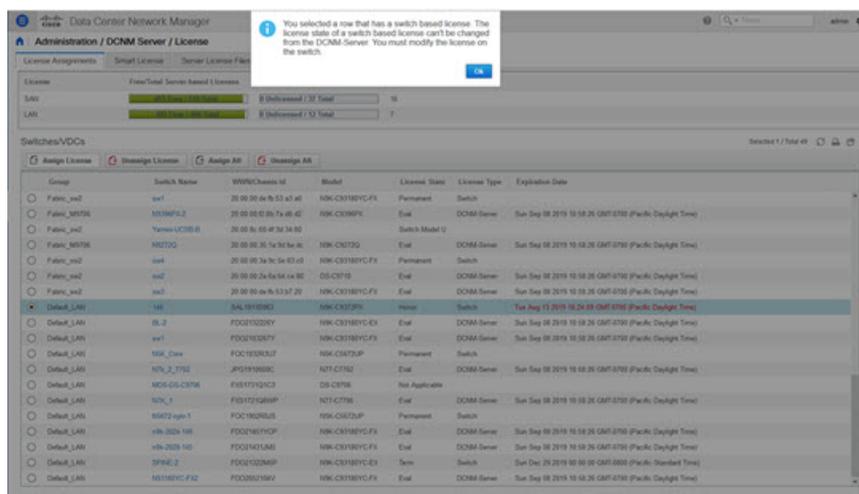
Note Switch-based honor licenses can't be overwritten with server-based license files.

License Assignments

License	Free/Total	Server-based Licenses	Unlicensed/Total (Switches/VDCs)	Need To Purchase
SAO	8	8	Unlicensed / 32 Total	16
LAN	8	8	Unlicensed / 32 Total	7

Switches/VDCs

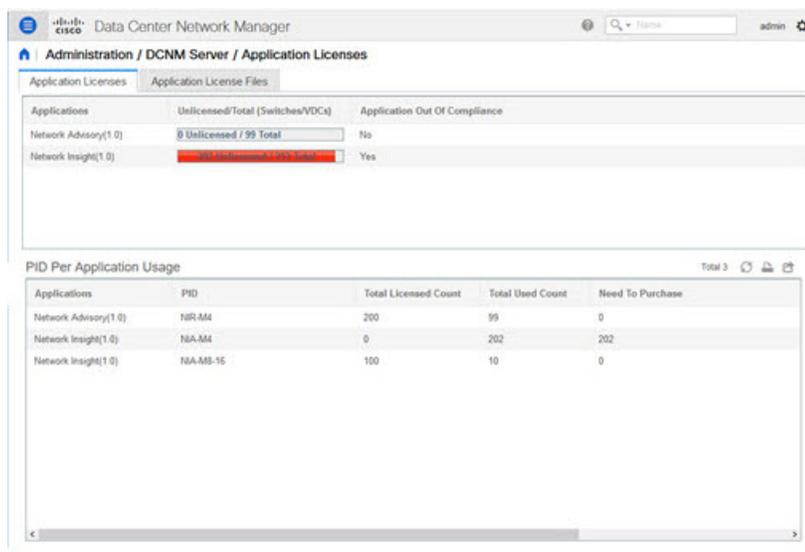
Group	Switch Name	WWN/Chassis ID	Model	License State	License Type	Expiration Date
○	Fabric_#02	00:00:00:00:00:00	NK-C3180YC-F1	Permanent	Switch	
○	Fabric_MR756	00:00:00:00:00:00	NK-C3175G	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Fabric_#02	00:00:00:00:00:00	NK-C3175G	Switch Model U		
○	Fabric_MR756	00:00:00:00:00:00	NK-C3175G	Switch Model U		
○	Fabric_MR756	00:00:00:00:00:00	NK-C3175G	Permanent	Switch	
○	Fabric_MR756	00:00:00:00:00:00	NK-C3175G	Switch Model U		
○	Fabric_mrchen-questar-PC-VDC	00:00:00:00:00:00	NK-C3175G	Permanent	DCM-Server	
○	Default_LAN	00:00:00:00:00:00	NK-C3175G	Honor	Switch	Tue Aug 13 2019 16:24:09 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	00:00:00:00:00:00	NK-C3180YC-E1	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	00:00:00:00:00:00	NK-C3180YC-F1	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	00:00:00:00:00:00	NK-C3175G	Permanent	Switch	
○	Default_LAN	00:00:00:00:00:00	NK-C3175G	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	00:00:00:00:00:00	DS-C9306	Not Applicable		
○	Default_LAN	00:00:00:00:00:00	NK-C3175G	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	00:00:00:00:00:00	NK-C3175G	Permanent	Switch	
○	Default_LAN	00:00:00:00:00:00	NK-C3180YC-F1	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	00:00:00:00:00:00	NK-C3180YC-F1	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)
○	Default_LAN	00:00:00:00:00:00	NK-C3180YC-E1	Term	Switch	Sun Dec 29 2019 00:00:00 GMT-0800 (Pacific Standard Time)
○	Default_LAN	00:00:00:00:00:00	NK-C3180YC-F1	Eval	DCM-Server	Sun Sep 28 2019 10:58:26 GMT-0700 (Pacific Daylight Time)



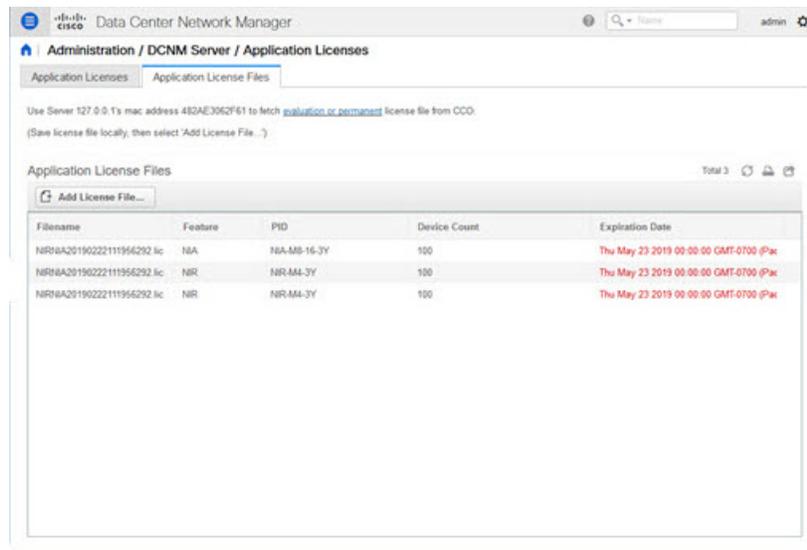
Application Licenses

From Release 11.3(1), you can manage licenses for applications on the Cisco DCNM. Choose **Web UI > Administration > Manage Licensing > Applications** to view the Application Licenses.

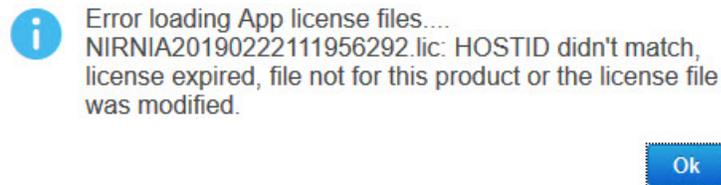
The Application Licenses tab displays the DCNM Applications with a summary of their unlicensed/total switches and if they are out of compliance. The PID Per Application Usage table displays the actual counts per PID given to the server from the Application Framework. The PIDs that need to be purchased for each application is also listed.



The Application License Files tab allows you to add license files for the applications. Click on Add license file to add license file from your local directory. The license filename, application name, PID, device count and expiration date details are extracted from the imported license file. If the license isn't permanent or is eval or term, the expiration date is also listed.



The following image shows a sample error message while uploading an application license file.



Management Users



Note Every time you login to DCNM, the DCNM server fetches information from the ISE server for AAA authentication. The ISE server will not authenticate again, after the first login.

The Management Users menu includes the following submenus:

Remote AAA

To configure remote AAA from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > Management Users > Remote AAA Properties**.
The AAA properties configuration window appears.
- Step 2** Use the radio button to select one of the following authentication modes:

- **Local**: In this mode the authentication authenticates with the local server.
- **Radius**: In this mode the authentication authenticates against the RADIUS servers specified.
- **TACACS+**: In this mode the authentication authenticates against the TACACS servers specified.
- **Switch**: In this mode the authentication authenticates against the switches specified.
- **LDAP**: In this mode the authentication authenticates against the LDAP server specified.

Step 3 Click **Apply**.

Note Restart the Cisco DCNM LAN services if you update the Remote AAA properties.

Local

Procedure

Step 1 Use the radio button and select **Local** as the authentication mode.

Step 2 Click **Apply** to confirm the authentication mode.

Radius

Procedure

Step 1 Use the radio button and select **Radius** as the authentication mode.

Note When using the DCNM AAA or Radius authentication, you should not specify the hash (#) symbol at the beginning of a secret key. Otherwise, DCNM will try to use # as encrypted, and it will fail.

Step 2 Specify the Primary server details and click **Test** to test the server.

Step 3 (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.

Step 4 Click **Apply** to confirm the authentication mode.

TACACS+

Procedure

Step 1 Use the radio button and select **TACACS+** as the authentication mode.

Note When using the DCNM AAA or Radius authentication, you should not specify the hash (#) symbol at the beginning of a secret key. Otherwise, DCNM will try to use # as encrypted, and it will fail.

Step 2 Specify the Primary server details and click **Test** to test the server.

Step 3 (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.

Note For IPv6 transport, enter Physical and VIP address for AAA authentication as the order of addresses changes during failover situation.

Step 4 Click **Apply** to confirm the authentication mode.

Switch

Procedure

Step 1 Use the radio button to select **Switch** as the authentication mode.

DCNM also supports LAN switches with the IPv6 management interface.

Step 2 Specify the Primary Switch name and click **Apply** to confirm the authentication mode.

Step 3 (Optional) Specify the names for Secondary and Tertiary Switches.

Step 4 Click **Apply** to confirm the authentication mode.

LDAP

Procedure

Step 1 Use the radio button and select **LDAP** as the authentication mode.

The screenshot shows the configuration page for Remote AAA in DCNM. The 'Auth Mode' is set to 'LDAP'. The 'Host' field is 'ds.cisco.com', 'Port' is '389', 'Base DN' is 'DC=cisco,DC=com', and 'Filter' is '\$userid@cisco.com'. The 'Determine Role By' is set to 'Admin Group Map', with 'Role Admin Group' as 'dcnm-admins' and 'Map TO DCNM Role' as 'network-admin'. There is a 'Test...' button next to the Host field.

Step 2 In the **Host** field, enter either the IPv4 or IPv6 address.

If DNS service is enabled, you can enter DNS address (hostname) of the LDAP server.

Step 3 In the **Port** field, enter a port number.

Enter 389 for non-SSL; enter 636 for SSL. By default, the port is configured for non-SSL.

Step 4 Select the **SSL Enabled** check box, if SSL is enabled on the AAA server.

Note You must enter **636** in the Port field, and select **SSL Enabled** check box to use LDAP over SSL.

This ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a SSL session, before sending the bind or search request.

Note Cisco DCNM establishes a secured connection with the LDAP server using TLS. Cisco DCNM supports all versions of TLS. However, the specific version of TLS is determined by the LDAP server.

For example, if the LDAP server supports TLSv1.2 by default, DCNM will connect using TLSv1.2.

Step 5 In the **Base DN** field, enter the base domain name.

The LDAP server searches this domain. You can find the base DN by using the **dsquery.exe user -name<display_name>** command on the LDAP server.

For example:

```
ldapservershell# dsquery.exe users -name "John Smith"
```

```
CN=john smith,CN=Users,DC=cisco,DC=com
```

The Base DN is DC=cisco,DC=com.

Note Ensure that you enter the elements within the Base DN in the correct order. This specifies the navigation of the application when querying Active Directory.

Step 6 In the **Filter** field, specify the filter parameters.

These values are used to send a search query to the Active Directory. The LDAP search filter string is limited to a maximum of 128 characters.

For example:

- \$userid@cisco.com

This matches the user principal name.

- CN=\$userid,OU=Employees,OU=Cisco Users

This matches the exact user DN.

Step 7 Choose an option to determine a role. Select either **Attribute** or **Admin Group Map**.

- **Admin Group Map:** In this mode, DCNM queries LDAP server for a user based on the Base DN and filter. If the user is a part of any user group, the DCNM role will be mapped to that user group.
- **Attribute:** In this mode, DCNM queries for a user attribute. You can select any attribute. When you choose **Attribute**, the **Role Admin Group** field changes to **Role Attributes**.

Step 8 Enter value for either **Roles Attributes** or **Role Admin Group** field, based on the selection in the previous step.

- If you chose **Admin Group Map**, enter the name of the admin group in the **Role Admin Group** field.

- If you chose **Attribute**, enter the appropriate attribute in the **Attributes** field.

Step 9 In the **Map to DCNM Role** field, enter the name of the DCNM role that will be mapped to the user. Generally, **network-admin** or **network-operator** are the most typical roles.

For example:

```
Role Admin Group: dcnm-admins
Map to DCNM Role: network-admin
```

This example maps the Active Directory User Group **dcnm-admins** to the **network-admin** role.

To map multiple Active Directory User Groups to multiple roles, use the following format:

```
Role Admin Group:
Map To DCNM Role: dcnm-admins:network-admin;dcnm-operators:network-operator
```

Note that **Role Admin Group** is blank, and **Map To DCNM Role** contains two entries delimited by a semicolon.

Step 10 In the **Access Map** field, enter the Role Based Access Control (RBAC) device group to be mapped to the user.

Step 11 Click **Test** to verify the configuration. The Test AAA Server window appears.

Step 12 Enter a valid **Username** and **Password** in the Test AAA Server window.

If the configuration is correct, the following message is displayed.

```
Authentication succeeded.
The cisco-av-pair should return 'role=network-admin' if this user needs to
see the DCNM Admin pages. 'SME' roles will allow SME page access. All other
roles - even if defined on the switches - will be treated
as network operator.
```

This message is displayed regardless of 'Role Admin Group' or 'Attribute' mode. It implies that Cisco DCNM can query your Active Directory, the groups, and the roles are configured correctly.

If the test fails, the LDAP Authentication Failed message is displayed.

Warning Don't save the configuration unless the test is successful. You cannot access DCNM if you save incorrect configurations.

Step 13 Click **Apply Changes** icon (located in the right top corner of the screen) to save the configuration.

Step 14 Restart the DCNM SAN service.

- For Windows – On your system navigate to **Computer Management > Services and Applications > Services**. Locate and right click on the DCNM application. Select **Stop**. After a minute, right click on the DCNM application and select **Start** to restart the DCNM SAN service.
- For Linux – Go to **/etc/init.d/FMServer.restart** and hit return key to restart DCNM SAN service.

Managing Local Users

As an admin user, you can use Cisco DCNM Web UI to create a new user, assign the role and associate one or more groups or scope for the user.

This section contains the following:

Adding Local Users

Procedure

Step 1 From the menu bar, choose **Administration > Management Users > Local**. You see the **Local Users** page.

Step 2 Click **Add User**.

You see the **Add User** dialog box.

Step 3 Enter the username in the **User name** field.

Note The username is case sensitive, but the username guest is a reserved name, which is not case sensitive. The guest user can only view reports. The guest user cannot change the guest password, or access the Admin options in DCNM Web Client.

Step 4 From the **Role** drop-down list, select a role for the user.

Step 5 In the **Password** field, enter the password.

Note All special characters, except SPACE is allowed in the password.

Step 6 In the **Confirm Password** field, enter the password again.

Step 7 Click **Add** to add the user to the database.

Step 8 Repeat Steps 2 through 7 to continue adding users.

Deleting Local Users

To delete local users from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Management Users > Local**.

The **Local Users** page is displayed.

Step 2 Select one or more users from the **Local Users** table and click the **Delete User** button.

Step 3 Click **Yes** on the warning window to delete the local user. Click **No** to cancel deletion.

Editing a User

To edit a user from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Administration > Management Users > Local**.

- Step 2** Use the checkbox to select a user and click the **Edit User** icon.
- Step 3** In the **Edit User** window, the **Username** and **Role** are mentioned by default. Specify the **Password** and **Confirm Password**.
- Step 4** Click **Apply** to save the changes.

User Access

You can select specific groups or fabrics that local users can access. This restricts local users from accessing specific groups or fabrics for which they have not been provided access. To do this, perform the following steps:

Procedure

- Step 1** Choose **Administration > Management Users > Local**.
- The **Local Users** window is displayed.
- Step 2** Select one user from the **Local Users** table. Click **User Access**.
- The **User Access** selection window is displayed.
- Step 3** Select the specific groups or fabrics that the user can access and click **Apply**.

The screenshot shows the Cisco Data Center Network Manager interface. The breadcrumb navigation is **Administration / Management Users / Local**. The **Local Users** table is displayed with the following columns: **User Name**, **Role**, **Access**, and **Password Expiration Status**. The user **john** is selected. The **User Access** dialog box is open, showing a list of groups and fabrics with checkboxes. The **john-fx2** and **fx2** groups are selected, and the **Default_LAN** group is highlighted.

User Name	Role	Access	Password Expiration Status
<input type="checkbox"/> admin	network-admin	Data Center	Password never expires.
<input type="checkbox"/> poap	network-admin	Data Center	Password never expires.
<input type="checkbox"/> root	network-admin	Data Center	Password never expires.
<input checked="" type="checkbox"/> john	network-admin	Data Center	Password never expires.

User Access

- Cloud-Connect
 - CSR-Azure
 - CSR-OnPrem
 - ext-fabric5
 - site2
- ext
- s1
- services-setup
- john-fx2
- fx2
- Default_LAN

Apply Cancel

Managing Clients

You can use Cisco DCNM to disconnect DCNM Client Servers.

Procedure

- Step 1** Choose **Administration > Management Users > Clients**.
A list of DCNM Servers are displayed.
- Step 2** Use the check box to select a DCNM server and click **Disconnect Client** to disconnect the DCNM server.

Note You cannot disconnect a current client session.

Performance Setup

The Performance Setup menu includes the following submenus:

Performance Setup LAN Collections

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM to add and remove performance collections. License the switch and kept it in the **Managed Continuously** state before creating a collection for the switch.



Note To collect Performance Manager data, ICMP ping must be enabled between the switch and DCNM server. Set **pm.skip.checkPingAndManageable** server property to true and then restart the DCNM. Choose **Web UI > Administration > DCNM Server > Server Properties** to set the server property.

To add a collection, follow these steps:

Procedure

- Step 1** Choose **Administration > Performance Setup > LAN Collections**.
- Step 2** For all the licensed LAN switches, use the check boxes to enable performance data collection for **Trunks, Access, Errors & Discards, and Temperature Sensor**.
- Step 3** Use the check boxes to select the types of LAN switches for which you want to collect performance data.
- Step 4** Click **Apply** to save the configuration.
- Step 5** In the confirmation dialog box, click **Yes** to restart the Performance Manager. The Performance Manager has to be restarted for any new setting to take effect.
-

Performance Setup Thresholds

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM to add and remove performance collections. License the switch and keep it in the **Managed Continuously** state before creating a collection for the switch.

Procedure

- Step 1** Choose **Administration > Performance Setup > Thresholds**.
- Step 2** Under **Generate a threshold event when traffic exceeds % of capacity**, use the check box to specify the **Critical at** and **Warning at** values. The range for **Critical at** is from 5 to 95, and the default is 80. The range for **Warning at** is from 5 to 95, and the default is 60.
- Step 3** Select a value for **Performance SAN ISL Polling Interval** from the drop-down list. Valid values are **5 Mins**, **4 Mins**, **3 Mins**, **2 Mins**, **1 Min**, and **30 Sec**. The default is **30 Sec**.
- Step 4** Select a value for **Performance Default Polling Interval** from the drop-down list. Valid values are **5 Mins**, **10 Mins**, and **15 mins**. The default value is **5 Mins**.
- Step 5** Click **Apply**.

The screenshot shows the Cisco Data Center Network Manager interface for configuring performance thresholds. The breadcrumb navigation is Administration / Performance Setup / Thresholds. The main heading is "Generate a threshold event when traffic exceeds % of capacity:". Below this, there are two rows of checkboxes and input fields. The first row is for "Critical at" with a value of 80 and a range of (5...95%). The second row is for "Warning at" with a value of 60 and a range of (5...95%). Below these are two dropdown menus. The first is "Performance SAN ISL Polling Interval" set to "5 Mins". The second is "Performance Default Polling Interval" set to "15 Mins", with a dropdown menu open showing options: "5 Mins", "10 Mins", and "15 Mins". At the bottom left is an "Apply" button.

Event Setup

The Event Setup menu includes the following submenus:

Viewing Events Registration

To enable **Send Syslog**, **Send Traps** and **Delayed Traps** you must configure the following in the DCNM SAN client:

- Enabling **Send Syslog**: Choose **Physical Attributes > Events > Syslog > Servers**. Click **Create Row**, provide the required details, and click **Create**.
- Enabling **Send Traps**: Choose **Physical Attributes > Events > SNMP Traps > Destination**. Click **Create Row**, provide the required details, and click **Create**.
- Enabling **Delayed Traps**: Choose **Physical Attributes > Events > SNMP Traps > Delayed Traps**. In the **Feature Enable** column, use the check boxes to enable delayed traps for the switch and specify the delay in minutes.

Procedure

- Step 1** Choose **Administration > Event Setup > Registration**.
The SNMP and Syslog receivers along with the statistics information are displayed.
- Step 2** Check the **Enable Syslog Receiver** check box and click **Apply**, to enable the syslog receiver if it is disabled in the server property.
To configure event registration or syslog properties, choose **Administration > DCNM Server > Server Properties** and follow the on-screen instructions.
- Step 3** Select **Copy Syslog Messages to DB** and click **Apply** to copy the syslog messages to the database.
If this option is not selected, the events will not be displayed in the events page of the Web client.
The columns in the second table display the following:
- Switches sending traps
 - Switches sending syslog
 - Switches sending syslog accounting
 - Switches sending delayed traps
-

Notification Forwarding

You can use Cisco DCNM Web UI to add and remove notification forwarding for system messages.

This section contains the following:

Adding Notification Forwarding

Cisco DCNM Web UI forwards fabric events through email or SNMPv1 traps.

Some SMTP servers may require addition of authentication parameters to emails that are sent from DCNM to the SMTP servers. Starting from Cisco DCNM Release 11.4(1), you can add authentication parameters to the emails that are sent by DCNM to any SMTP server that requires authentication. This feature can be configured by setting up the **SMTP>Authentication** properties in the **Administration>DCNM Server>Server Properties** window. Enter **true** in the **server.smtp.authenticate** field, enter the required username in the **server.smtp.username** field, and enter the required password in the **server.smtp.password** field.

To add and remove notification forwarding for system messages from the Cisco DCNM Web UI, perform the following steps:



Note Test forwarding works only for the licensed fabrics.

Procedure

-
- Step 1** Choose **Administration > Event Setup > Forwarding**.
- The events forwarding scope, the recipient email address, severity of the event and type of the event is displayed. The description Regex field is applicable only when the forwarding source is selected as Syslog while adding the events forwarder.
- Step 2** Check the **Enable** checkbox to enable events forwarding.
- Step 3** Specify the **SMTP Server** details and the **From** email address.
- Step 4** Click **Apply** to save the configuration.
- Step 5** In the **Event Count Filter**, add a filter for the event count to the event forwarder.
- The forwarding stops forwarding an event if the event count exceeds the limit as specified in the event count filter. In this field, you can specify a count limit. Before an event can be forwarded, the Cisco DCNM checks if its occurrence exceeds the count limit. If it does, the event will not be forwarded.
- Step 6** Select the **Snooze** checkbox and specify the **Start** date and time and the **End** date and time. Click **Apply** to save the configuration.
- Step 7** Under the **Event Forwarder Rules** table, click the + icon to add an event forwarder rule.
- You see the **Add Event Forwarder Rule** dialog box.
- Step 8** In the **Forwarding Method**, choose either **E-mail** or **Trap**. If you choose **Trap**, a **Port** field is added to the dialog box.
- Step 9** If you choose the **E-mail** forwarding method, enter the IP address in the **Email Address** field. If you choose the **Trap** method, enter the trap receiver IP address in the **Address** field and specify the port number.
- You can either enter an IPv4 or IPv6 addresses or DNS server name in the **Address** field.
- Step 10** For **Forwarding Scope**, choose the **Fabric/LAN** or **Port Groups** for notification.
- Step 11** In the **Source** field, select **DCNM** or **Syslog**.
- If you select **DCNM**, then:
- a) From the **Type** drop-down list, choose an event type.

- b) Check the **Storage Ports Only** check box to select only the storage ports.
- c) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
- d) Click **Add** to add the notification.

If you select **Syslog**, then:

- a) In the **Facility** list, select the syslog facility.
- b) Specify the syslog **Type**.
- c) In the **Description Regex** field, specify a description that matches with the event description.
- d) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
- e) Click **Add** to add the notification.

Note The **Minimum Severity** option is available only if the **Event Type** is set to All.

The traps that are transmitted by Cisco DCNM correspond to the severity type. A text description is also provided with the severity type.

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

Removing Notification Forwarding

You can remove notification forwarding.

Procedure

- Step 1** Choose **Administration > Event Setup > Forwarding**.
- Step 2** Select the check box in front of the notification that you want to remove and click **Delete**.

Event Suppression

Cisco DCNM allows you to suppress the specified events that are based on the user-specified suppressor rules. Such events will not be displayed on the Cisco DCNM Web UI. The events will neither be persisted to DCNM database, nor forwarded via email or SNMP trap.

You can view, add, modify, and delete suppressor rules from the table. You can create a suppressor rule from the existing event table. Select a given event as the template, and invoke the rule dialog window. Event details are automatically ported from the selected event in the event table to the input fields of the rule creation dialog window.



Note You cannot suppress EMC Call Home events from the Cisco DCNM Web UI.

This section includes the following:

Add Event Suppression Rules

To add rules to the Event Suppression from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > Event Setup > Suppression**.
The **Suppression** window is displayed.
- Step 2** Click the **Add** icon above the **Event Suppressors** table.
The **Add Event Suppressor Rule** window is displayed.
- Step 3** In the **Add Event Suppressor Rule** window, specify the **Name** for the rule.
- Step 4** Select the required **Scope** for the rule that is based on the event source.
In the Scope drop-down list, the LAN groups and the port groups are listed separately. You can choose **LAN**, **Port Groups** or **Any**. For **LAN**, select the scope of the event at the Fabric or Group or Switch level. You can only select groups for **Port Group** scope. If use selects **Any** as the scope, the suppressor rule is applied globally.
- Step 5** Enter the **Facility** name or choose from the **LAN Switch Event Facility List**.
If you do not specify a facility, wildcard is applied.
- Step 6** From the drop-down list, select the Event **Type**.
If you do not specify the event type, wildcard is applied.
- Step 7** In the **Description Matching** field, specify a matching string or regular expression.
The rule matching engine uses regular expression that is supported by Java Pattern class to find a match against an event description text.
- Step 8** Check the **Active Between** box and select a valid time range during which the event is suppressed.
By default, the time range is not enabled, i.e., the rule is always active.
- Note** In general, you must not suppress accounting events. Suppressor rule for Accounting events can be created only for certain rare situations where Accounting events are generated by actions of DCNM or switch software. For example, lots of '*sync-snmp-password*' AAA syslog events are automatically generated during the password synchronization between DCNM and managed switches. To suppress Accounting events, navigate to the **Suppressor table** and invoke the **Add Event Suppressor Rule** dialog window.
- Note** Choose **Monitor > Switch > Events** to create a suppressor rule for a known event. There is no such shortcut to create suppressor rules for Accounting events.
-

Delete Event Suppression Rule

To delete event suppressor rules from the Cisco DCNM Web UI, perform the following steps:

Procedure

- Step 1** Choose **Administration > Event Setup > Suppression**.
 - Step 2** Select the rule from the list and click **Delete** icon.
 - Step 3** Click **Yes** to confirm.
-

Modify Event Suppression Rule

To modify the event suppressor rules, do the following tasks:

Procedure

- Step 1** Choose **Administration > Event Setup > Suppression**.
 - Step 2** Select the rule from the list and click **Edit**.
You can edit **Facility**, **Type**, **Description Matching** string, and **Valid time range**.
 - Step 3** Click **Apply** to save the changes,
-

Credentials Management

The Credential Management menu includes the following submenus:

LAN Credentials

While changing the device configuration, Cisco DCNM uses the device credentials provided by you. However, if the LAN Switch credentials are not provided, Cisco DCNM prompts you to open the **Administration > Credentials Management > LAN Credentials** page to configure LAN credentials.

Cisco DCNM uses two sets of credentials to connect to the LAN devices:

- **Discovery Credentials**—Cisco DCNM uses these credentials during discovery and periodic polling of the devices.
- **Configuration Change Credentials**—Cisco DCNM uses these credentials when user tries to use the features that change the device configuration.

LAN Credentials Management allows you to specify configuration change credentials. Before changing any LAN switch configuration, you must furnish *Configuration Change* SSH credentials for the switch. If you do not provide the credentials, the configuration change action will be rejected.

These features get the device write credentials from LAN Credentials feature.

- Upgrade (ISSU)
- Maintenance Mode (GIR)

- Patch (SMU)
- Template Deployment
- POAP-Write erase reload, Rollback
- Interface Creation/Deletion/Configuration
- VLAN Creation/Deletion/Configuration
- VPC Wizard

You must specify the configuration change credentials irrespective of whether the devices were discovered initially or not. This is a one-time operation. Once the credentials are set, that will be used for any configuration change operation.

Default Credentials

Default credentials is used to connect all the devices that the user has access to. You can override the default credentials by specifying credentials for each of the devices in the Switch Table below.



Note After you enter appropriate credentials in **Password**, **Confirm Password** fields and click **Save**, the **Confirm Password** field is blank. A blank **Confirm Password** field implies that the password is saved successfully.

Cisco DCNM tries to use individual switch credentials in the Switch Table, to begin with. If the credentials (username/password) columns are empty in the Switch Table, the default credentials will be used.

Switch Table

Switch table lists all the LAN switches that user has access. You can specify the switch credentials individually, that will override the default credentials. In most cases, you need to provide only the default credentials.

You can perform the following operations on this screen.

- [Edit Credentials, on page 42](#)
- [Validate Credentials, on page 42](#)
- [Clear Switch Credentials, on page 42](#)
- [Credentials Management with Remote Access, on page 42](#)

The LAN Credentials for the DCNM User table has the following fields.

Field	Description
Switch	Displays the LAN switch name.
IP Address	Specifies the IP Address of the switch.
User Name	Specifies the username of the switch DCNM user.
Password	Displays the encrypted form of the SSH password.
Group	Displays the group to which the switch belongs.

Edit Credentials

Perform the following task to edit the credentials.

1. From the Cisco DCNM home page, choose **Administration > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to edit the credentials.
2. Click Edit icon.
3. Specify **User Name** and **Password** for the switch.

Validate Credentials

Perform the following task to validate the credentials.

1. From the **Administration > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to validate the credentials.
2. Click **Validate**.
A confirmation message appears, stating if the operation was successful or a failure.

Clear Switch Credentials

Perform the following task to clear the switch credentials.

1. From the **Administration > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to clear the credentials.
2. Click **Clear**.
3. Click **Yes** to clear the switch credentials from the DCNM server.

Credentials Management with Remote Access

DCNM allows you to authenticate users in different modes such as:

- Local Users - In this mode, you can use the Cisco DCNM Web UI to create a new user, assign a role, and provide access to one or more fabrics or groups for the user.
- Remote Users - In this mode, you can log in to DCNM. The DCNM server fetches information from the Remote Authentication server, for example, the Cisco Identity Services Engine (ISE), for AAA authentication. Cisco supports TACACS+, RADIUS, and LDAP options for remote authentication. For more information, see [Remote AAA](#).

When you configure DCNM for remote authentication, the AAA server handles both authentication and authorization. DCNM forwards the entered user login and password to the AAA server to check for authentication. Post authentication, the AAA server returns the appropriate privileges/role assigned to the user through the **cisco-avpair** attribute. This attribute can contain the list of fabrics that a particular user can access. The supported roles for DCNM LAN deployments are as follows:

- network-admin
- network-operator

Both device discovery credentials and LAN credentials provide write access to the devices, but they differ—as the write operation is performed only with LAN credentials. Device discovery credentials are associated with

each device and entered only once, that is, when you import the device into DCNM. DCNM uses these credentials for periodic rediscovery using a mix of SSH and SNMPv3 access to the device. However, LAN credentials are configured for every user on a per-user basis. If a user with an appropriate role has access to DCNM, then that user can enter the LAN credentials to get write access to the devices. The write operations use the LAN credentials to access the device, which allows for an appropriate audit trail of the changes made in DCNM by every user and the resultant changes in the device.

When you configure DCNM using Remote Authentication Methods such as TACACS+ or RADIUS, the users can set their LAN credentials as follows:

- [Regular AAA Remote Authentication](#)
- [AAA Remote Authentication Passthrough Mechanism](#)
- [AAA Remote Authentication Using DCNM Service Account](#)

Regular AAA Remote Authentication

Post authentication, when a user with an appropriate role logs in to DCNM for the first time, DCNM prompts the user to enter the LAN credentials. As mentioned earlier, DCNM uses these credentials to provide write access to the devices. All users must follow this process. Consider that an internal business policy requires the users to change password every 3-6 months. Then all the users must update their passwords for device access in the DCNM **LAN Credentials** window. Also, they must update their passwords in the AAA server.

For example, let us consider a user named John, who has authentication on the ISE server.

1. John logs in to DCNM with his user credentials.
2. The ISE server authenticates the user credentials of John, and DCNM displays a message to enter his LAN switch credentials. DCNM uses these credentials to perform various configurations and write operations on the devices.



3. John enters his LAN switch credentials. DCNM uses the LAN switch credentials for all write operations triggered by John on all devices. However, John can also opt to enter LAN switch credentials on a per-device access basis. This per-device access option overrides the access provided by entering the default credentials.

Administration / Credentials Management / LAN Credentials

Default Credentials

Default credentials will be used when changing device configuration. You can override the default credentials by specifying credentials for each of the devices in the Switch Table below. DCNM uses individual switch credentials in the Switch Table. If the Username or Password column is empty in the Switch Table, the default credentials will be used.

* User Name

* Password

* Confirm Password

When John logs in to DCNM again, DCNM doesn't display any message to enter the LAN switch credentials as it has already captured his LAN switch credentials. John uses the same credentials to log in to DCNM and to the devices that he can access.

Administration / Credentials Management / LAN Credentials

* User Name

* Password

* Confirm Password

<input type="checkbox"/>	Switch	IP Address	User Name	Password	Group
<input type="checkbox"/>	leaf-1	172.25.74.145			Service-V
<input type="checkbox"/>	DC1-SPINE1	172.25.74.150	John	*****	Test-fab2
<input type="checkbox"/>	DC1-BGW1	172.25.74.149	John	*****	Test-fab2
<input type="checkbox"/>	DC2-BGW1	172.25.74.147			Test-Fab
<input type="checkbox"/>	FAB1-BGW1	10.23.234.246			TME_traditional_evpn
<input type="checkbox"/>	N93180EX-L3-S1	10.23.234.165			TME_traditional_evpn
<input type="checkbox"/>	N92160-L1b-S1	10.23.234.172			TME_traditional_evpn
<input type="checkbox"/>	N92160-L1a-S1	10.23.234.171			TME_traditional_evpn
<input type="checkbox"/>	N9272-Spine1-S1	10.23.234.176			TME_traditional_evpn

- Now, consider that after a few months, the Corporate IT policy changes. Then John must update his password in the Remote AAA server, and also perform Step 3 to allow DCNM to update his LAN switch credentials.

Thus, in this mode, when John logs in to the DCNM Web GUI with his updated password, DCNM doesn't display any message to enter LAN credentials. However, John must update the password in LAN Credentials. Updating the password is necessary as it allows DCNM to inherit the newly updated password and perform write operations on the devices.

AAA Remote Authentication Passthrough Mechanism

In this mode, when a user enters the username and password to log in to DCNM, DCNM automatically copies the user credentials to the Default Credentials in the LAN switch credentials settings for that user. As a result, when the user logs in for the first time, DCNM doesn't display the message to enter the LAN switch credentials.

- Use SSH to log in to DCNM as a sysadmin user.
- Log in to the `/root/directory` using the `su` command.

3. Navigate to the `/usr/local/cisco/dcm/fm/conf/server.properties` file.
4. Add the following server property to the file and save the changes.

dcnm.lanSwitch.sameUserAccount=true

```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep dcnm.lan
dcnm.lanSwitch.sameUserAccount=true
[root@dcnm sysadmin]#
```

5. Restart DCNM using the **service FMServer restart** command.
6. Now, John logs in to DCNM.
7. After successful authentication, DCNM doesn't display the message to update the LAN switch credentials, as it automatically copies this information to the LAN switch credentials.
8. Consider that after a few months, the Corporate IT policy changes. In this mode, John must update his password in the Remote AAA server. After that, when John logs in to DCNM, DCNM automatically copies the updated credentials to the Default LAN Credentials associated with the user John.

AAA Remote Authentication Using DCNM Service Account

Often, the customers prefer to track all the changes made from the DCNM controller with a common service account. In the following example, a user makes changes using the DCNM controller, which results in changes on the device. These changes are audit logged on the device, against a common service account. Thus, it is possible to distinguish the controller-triggered changes from other changes (also known as Out-of-Band changes) made by the user directly on the device. The Out-of-Band changes appear in the device accounting logs as made from the user account.

For example, create a service account with the name **Robot** on the remote AAA server. Using the corresponding credentials, the Robot user can log in to DCNM. The Robot user can enter the default LAN credentials to have write access to the devices. The DCNM network-admin enables a server property that automatically sets the default LAN credentials for all the users and inherits the default LAN credentials associated with Robot.

Therefore, when any user logs in to DCNM and makes any configuration changes, DCNM pushes the changes to the devices using the LAN credentials of Robot. The DCNM deployment history logs track the user who triggered the change and display the corresponding changes deployed from DCNM to the switch in the audit log with the user Robot.

To set up the service account on the DCNM, perform the following steps:

1. Use SSH to log in to DCNM as a sysadmin user.
2. Log in to the `/root/` directory using the **su** command.
3. Navigate to the `/usr/local/cisco/dcm/fm/conf/server.properties` file.
4. Add the following server property to the file and save the changes.

service.account=robot



Note You can enable either an AAA passthrough account or a Service Account.

```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

5. Restart DCNM using the **service FMServer restart** command.
6. Now, John logs in to DCNM.
7. After successful authentication, DCNM doesn't display the message to update the LAN switch credentials. However, when John navigates to the **LAN Credentials** page, DCNM displays a message stating that the Service Account is enabled in DCNM and, hence, all LAN credentials will be inherited from the service account.



service.account flag is enabled. Only service.account user can change the credentials.

* User Name	<input type="text" value="John"/>
* Password	<input type="password" value="....."/>
* Confirm Password	<input type="password"/>

Service Account Configuration Audit

The following workflow example allows for verification of the configuration audit while using the DCNM service account feature. However, you must have completed the Service Account Activation procedure.

1. John creates a test loopback on a device.

Preview Configuration

Switch: ▼ Interface: Loopback0

Pending Config

Expected Config

```
interface loopback0
  ip address 1.1.1.1/32 tag 12345
  no shutdown
  configure terminal
```

2. John deploys the configuration using DCNM.
3. The DCNM Deployment history confirms that John made the recent configuration change.

History for test-aaa(9T36UPBJ09T)

Deployment History Policy Change History

Hostname(Serial Number)	Entity Name	Entity Type	Source	Commands	Status	Status Description	User	Time of Completion
test-aaa(9T36UPBJ09T)	loopback0	INTERFACE	GLOBAL_INT...	Detailed History	SUCCESS	Successfully deployed	John	2021-06-01 15:51:39.918

4. The accounting logs of the device indicate that the DCNM Service Account (that is, Robot, in this example) has triggered the changes on the NX-OS device.

```
Tue Jun 1 22:50:04 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=terminal length 0 (SUCCESS)
Tue Jun 1 22:50:04 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=terminal session-timeout 30 (SUCCESS)
Tue Jun 1 22:50:04 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=terminal dont-ask (SUCCESS)
Tue Jun 1 22:50:04 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=terminal width 511 (SUCCESS)
Tue Jun 1 22:50:05 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=configure terminal ; interface loopback0 (REDIRECT)
Tue Jun 1 22:50:05 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=configure terminal ; interface loopback0 (SUCCESS)
Tue Jun 1 22:50:05 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=configure terminal ; interface loopback0 ; ip address 1.1.1.1/32 tag 12345 (REDIRECT)
Tue Jun 1 22:50:05 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=configure terminal ; interface loopback0 ; ip address 1.1.1.1/32 tag 12345 (SUCCESS)
Tue Jun 1 22:50:06 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=configure terminal ; interface loopback0 ; no shutdown (REDIRECT)
Tue Jun 1 22:50:06 2021: type=update: id=172.25.74.142@pts/5: user=robot: cmd=configure terminal ; interface loopback0 ; no shutdown (SUCCESS)
Tue Jun 1 22:50:06 2021: type=stop: id=172.25.74.142@pts/5: user=robot: cmd=shell terminated because the ssh session closed
test-aaa#
```

