# Administration

This chapter contains the following topics:



# 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:

**Note** During restart, the Performance Manager waits for 20minutes for the Elasticsearch to become operational. After 20minutes, the Performance Manager aborts. Click the **Re-init Elasticsearch DB Schema** icon in the **Actions** column for the **Performance collector** service.

### 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.

**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, SAN management server, 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.

**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/SCP Credentials

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

To configure the SFTP/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 STFP 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.

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.

## Removing a Group or a Member of a Group

You can delete a group or a member of the group from the Cisco DCNM Web UI. When you delete a group, the associated groups are deleted. The fabrics or ethernet switches of the deleted groups are moved to the default SAN or LAN.

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.

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

## Moving a Switch Group to Another Group

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

**Procedure**

**Step 1** Select a switch or switch group.

**Step 2** Drag the highlighted switch or switch group to another group.

To move multiple switches across different switch groups, use **Ctrl** key or **Shift** key.

You can see the switch or switch group. Users are not allowed to move multiple switches in the group level under the new group now.

**Note** It is not allowed to move multiple switches in the group level. You may not mix a group with switches.

# Managing Custom Port Groups

Custom port groups aid you to test the performance of the interfaces in the group. You can view the defined custom ports and their configurations.

This section includes the following topics:

## Adding Custom Port Groups

To add a custom port group from the Cisco DCNM Web UI, perform the following steps:

**Procedure**

**Step 1** Choose **Administration > DCNM Server > Custom Port Groups**.

The **Custom Port Groups** window is displayed.

**Step 2** In the **User-Defined Groups** block, click the **Add** icon.

**Step 3** Enter the name for the custom port group in the **Add Group Dialog** window.

**Step 4** Click **Add**.

A custom port group is created in the **User-Defined Groups** area.

## Configuring Switch and Interface to the Port Group

To configure the custom port group to include switches and interfaces from the Cisco DCNM Web UI, perform the following steps:

**Procedure**

**Step 1** Choose **Administration > DCNM Server > Custom Port Groups**.

**Step 2** In the **User-Defined Groups** area, select the port group to add the switch and interfaces.

**Step 3** In the **Configurations** area, click **Add Member**.

The **Port Configuration** window appears for the selected custom port group.

**Step 4** In the **Switches** tab, select the switch to include in the custom port group.

The list of available **Interfaces** appears.

**Step 5** Select all the interfaces to check the performance.

**Step 6** Click **Submit**.

The list of interfaces is added to the custom port group.

## Removing Port Group Member

To remove or delete a port group member in a custom port group from Cisco DCNM Web UI, perform the following steps:

### Procedure

**Step 1** Choose **Administration > DCNM Server > Custom Port Groups**.

**Step 2** In the **User Defined Groups** area, select a port group.

**Step 3** In the **Configuration** area, select the switch name and interface that must be deleted.

**Step 4** In the **User Defined Groups** area, select the group from which the member must be deleted.

**Step 5** Click **Remove Member**.

A confirmation window appears.

**Step 6** Click **Yes** to delete the member from the custom port group.

## Removing Port Group

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

### Procedure

**Step 1** Choose **Administration > DCNM Server > Custom Port Groups**.

**Step 2** In the **User Defined Groups** area, select the group which must be deleted.

**Step 3** Click **Remove**.

A confirmation window appears.

**Step 4** Click **Yes** to delete the custom group.

# Viewing Server Federation

**Note** There must be a minimum of 3 nodes in the Federation set up for failover to function correctly. In a 2 node Federation setup, if one of the servers is down, the Elasticsearch cannot form the cluster, and therefore the Web UI may behave inconsistently. In the case of a 3 node Federation setup, if two servers are down, inconsistent behavior of the WebUI is seen.

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

To view federation server information in Cisco DCNM, perform the following steps:

**Procedure**

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

The list of servers along with its IP address, status, location, local time, and data sources are displayed.

**Step 2** Use the **Enable Automatic Failover** check box to turn on or turn off the failover functionality.

**Step 3** In the **Location** column, double-click to edit the location.

If the status of one of the servers in the federation is **Inactive**, some functionality may not work unless the server status changes to **Active**.

**Note** Before upgrading Cisco DCNM, ensure that **Enable Automatic Failover** is unchecked. Otherwise, if one server within the federation is down, the devices are moved to the other DCNM server which comes up first after the upgrade. To prevent the automove for DCNM upgrade, you must disable the automove on all DCNMs within the federation, and upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the auto move again.

**Note** In DCNM Federation, when **Enable Automatic Failover** is enabled, if a DCNM is down, the devices under its management is moved to the other DCNM. However after the DCNM is back, the devices will not move back.

**Note** When you upgrade Cisco DCNM Federation, you need to revisit the **Administration > DCNM Server > Federation** page, and run the Elasticsearch cluster sync command after the upgrade is complete. This will update the Elasticsearch configurations and restart performance monitoring. To run the Elasticsearch cluster sync command, you need to enable Elasticsearch clustering button in the **Administration > DCNM Server > Federation** page. To restart the performance monitoring, choose **Administration > DCNM Server > Server Status**, and click the green button.

The **ElasticSearch Cluster** section gives the details about the elastic search. It has the following fields:

| Field | Description |
|---|---|
| Name | Specifies the name of the elastic search cluster. |
| Nodes | Specifies the number of instances clustered. |

| Field | Description |
|---|---|
| Status | Specifies if the cluster is enabled or not. If the cluster is not enabled, the status is yellow. If the cluster is enabled, the status is green. |

## Elasticsearch Clustering

**Note** The **ElasticSearch Clustering** sync-up option is available only on the Primary node in the Federation setup.

To sync each of the elastic search nodes that are associated with a federated server, into an elastic search cluster, perform the following steps:

**Procedure**

**Step 1** In the **Federation** window, click **ElasticSearch Clustering**. The **Elastic Search Clustering** pop-up window appears.

**Step 2** Click **Apply**.
This operation synchronizes each of the elastic search nodes that are associated with a federated server, into an elastic search cluster. The operation is disruptive to any features using elastic search as a data store. Some features are impacted by ongoing data synchronization operations after the elastic search services are resumed.

# 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.

# 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. |

| Field | Description |
|---|---|
| License State | Displays the license state of the switch that can be one of the following:<br>• Permanent<br>• Eval<br>• Unlicensed<br>• Not Applicable<br>• Expired<br>• Invalid |
| License Type | Displays the license type of the switch that can be one of the following:<br>• DCNM-Server<br>• Switch<br>• Smart<br>• Honor |
| Expiration Date | Displays the expiry date of the license.<br>**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.<br>**Note** If you unassign licenses of all switches in a fabric, even the fabric is unlicensed. However, in a federated setup after you unassign the license for a fabric, restart the PM service so that the fabric is no longer listed in the **SAN Collections** window. Restarting the PM is required to move the fabric from one node to another node successfully. |
| 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**

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.

## Honor License Mode

From Release 11.3(1), Cisco DCNM Eval license validity is extended from 30 days to 60 days. That implies, after 60 days. Every license has an expiry date attached to it. After the license expires, Cisco DCNM allows you to use all the licensed features. Switches remain in honor mode until the switch is licensed again or the user manually removes the license.

If there are switches in the Honor License mode, an error message appears after you logon to DCNM.

```
************************************
*Your licenses are out of compliance.
Your inventory contains switches that are unlicensed for DCNM Operation*

************************************
```

Go to **Administration > Manage Licensing > DCNM**, In the **Switches/VDCs** table, select the switch and click **Assign License** to renew the license.

### Guidelines

- Switches that don’t have a license assigned to them is considered unlicensed. Unlicensed Switches aren’t allowed to use Licensed DCNM features.
- If a switch has an expired EVAL license, it will change from EVAL to Honor mode and the license features continues to be operational.
- You can’t assign expired EVAL licenses to the switches.
- Switches with switch-based honor license can’t be overwritten with any server-based license.
- When a license is assigned to a discovered switch and a valid license isn’t available, then an honor-based license with expiration date will be assigned to the switch.

### Nag events for Honor-mode licenses

For every license in honor mode, an event is generated every seven days. A nag event informs the user "DCNM-SAN file license is in honor mode, need to assign/purchase a new license for this switch." Or "DCNM-LAN file license is in honor mode, need to assign/purchase a new license for this switch."

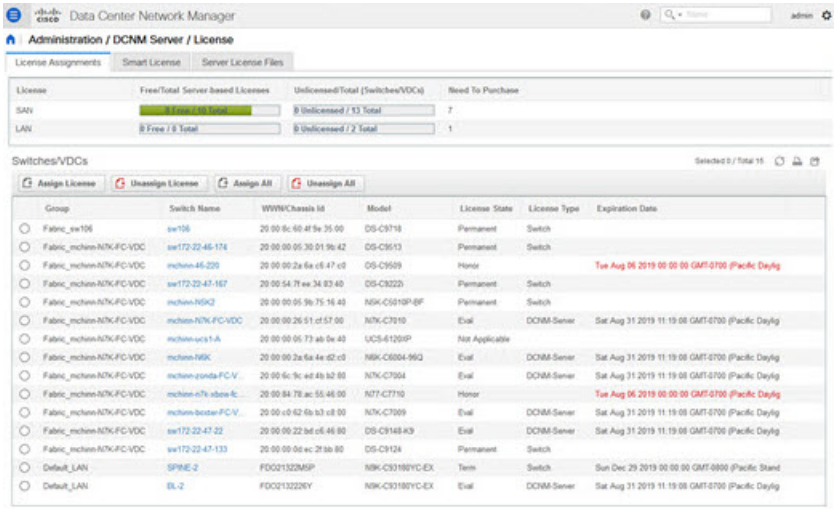
Additional popup notification appears when you logon to Cisco DCNM, to inform that “DCNM-SAN file license is in honor mode, need to assign/purchase a new license for this switch.”

### Server-based honor license support

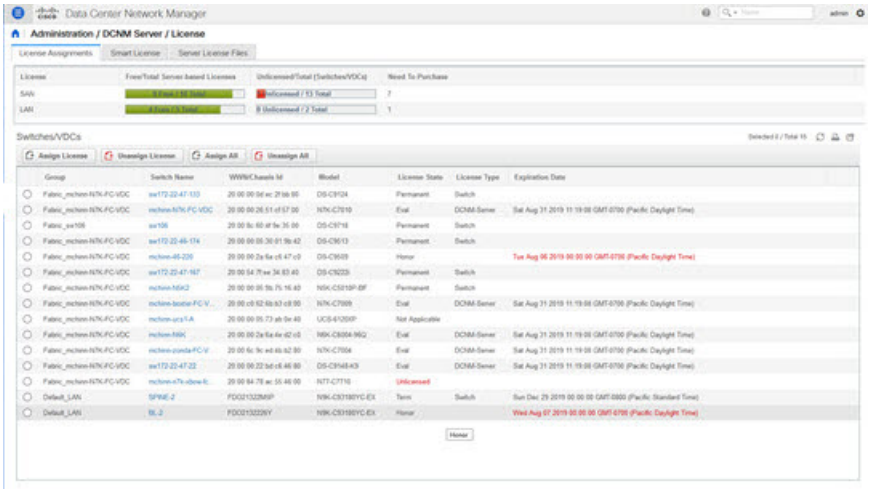
On the DCNM **Web UI > Administration > Manage Licensing > DCNM**, the **Licensed State** column displays **Honor** and **Expiration Date** column displays the date, time, and when the license expired and changed to the Honor mode.

Switches will remain in honor mode after reboot also. To change the license from honor mode, you must manually unassign the license or assign a new valid license to the switch.

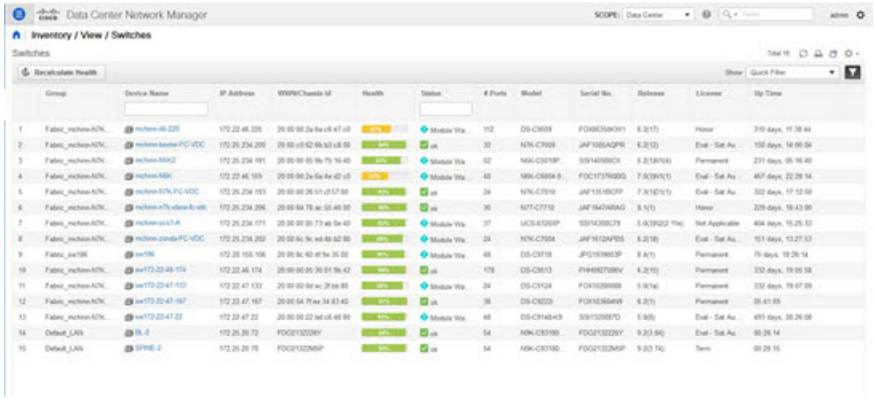
The following image shows license page with a SAN switch in Honor mode.



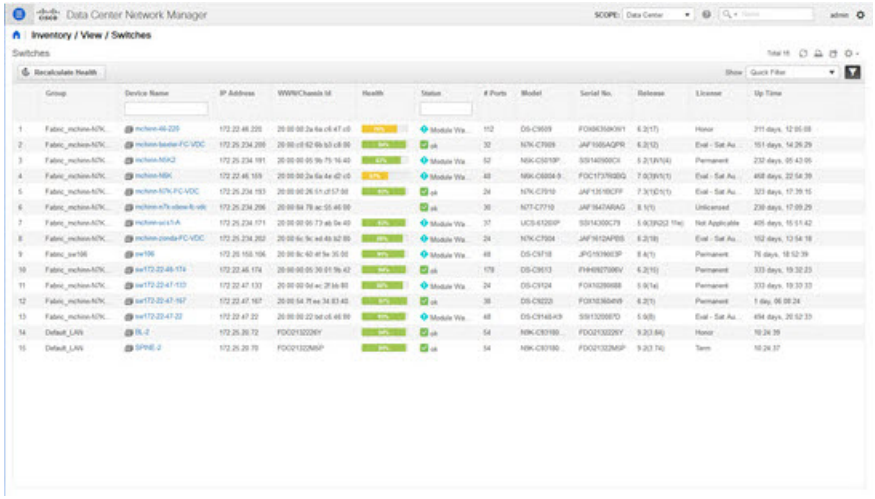

The following image shows license page with a LAN switch in Honor mode.



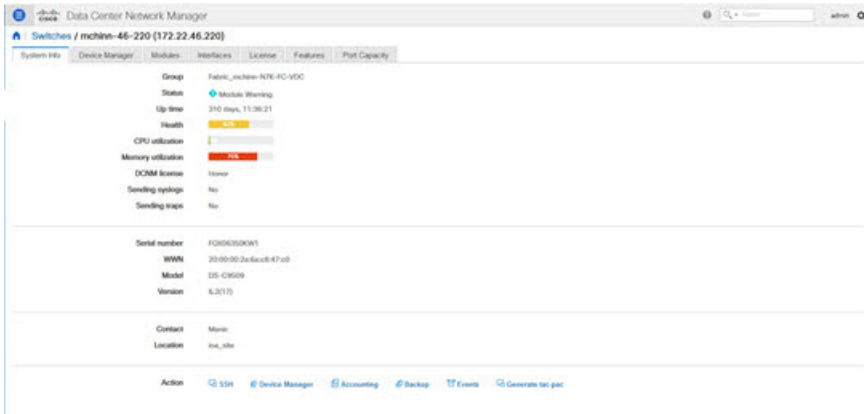

The following image shows the switch table displaying the honor mode of license and term.



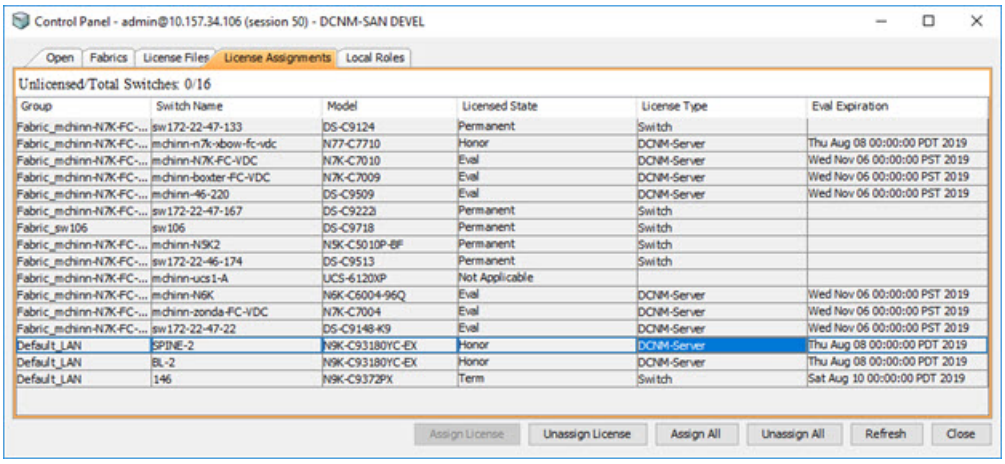

The following image shows Switch Dashboard with a LAN switch in Honor mode license.



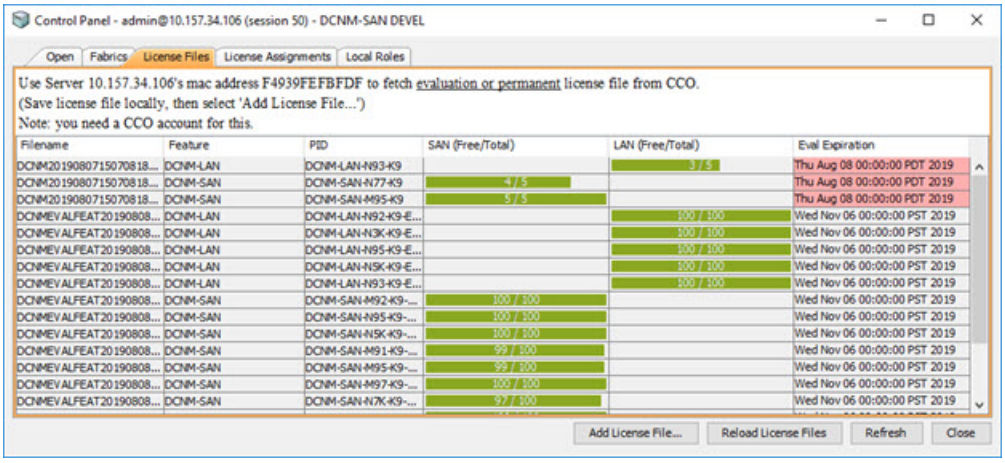

The following image shows Switch Dashboard with a SAN switch in Honor mode license.



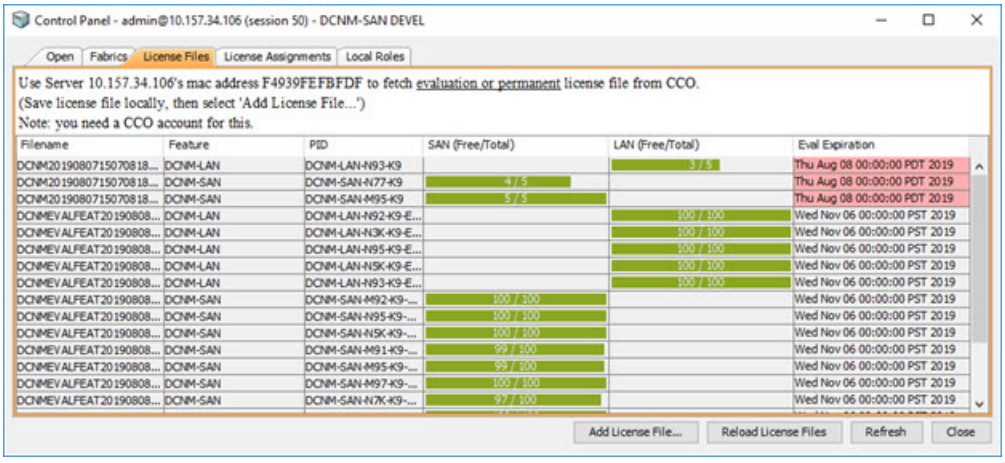

The following image shows the SAN Client License Agreement tab.




The following image shows the **SAN Client License** files tab.




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



# 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. |
| SAN (Free/Total) | Displays the number of free versus total licenses for SAN. |
| LAN (Free/Total) | Displays the number of free versus total licenses for LAN. |
| Expiration Date | Displays the expiry date of the license.<br>**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 and DCNM-SAN 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**.

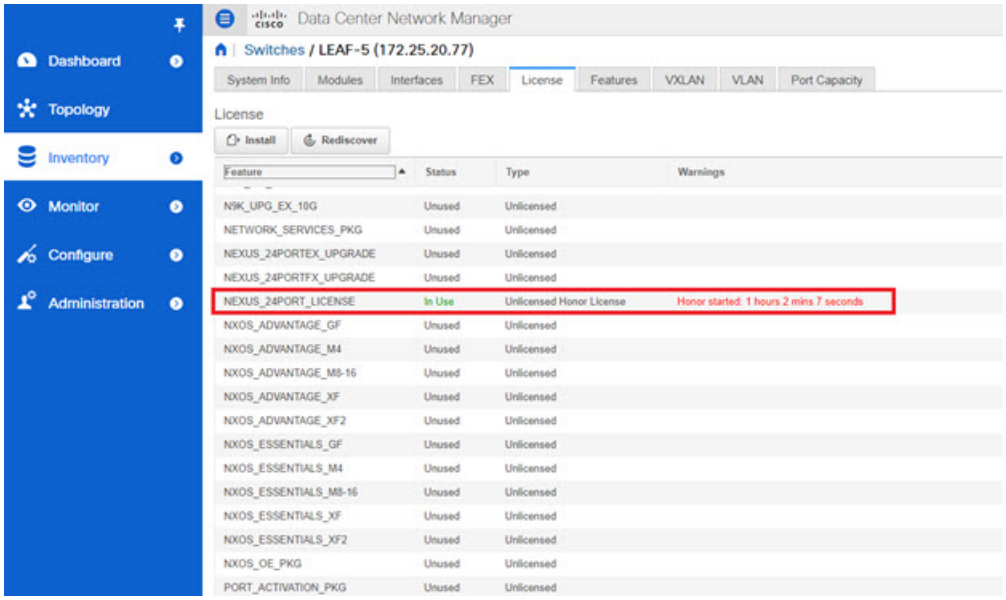
   The License file is uploaded to the DCNM. The following information is extracted from the license file.
   - Switch IP – IP Address of the switch to which this license is assigned.
   - License File – filename of the license file
   - Features List –list of features supported by the license file

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**.

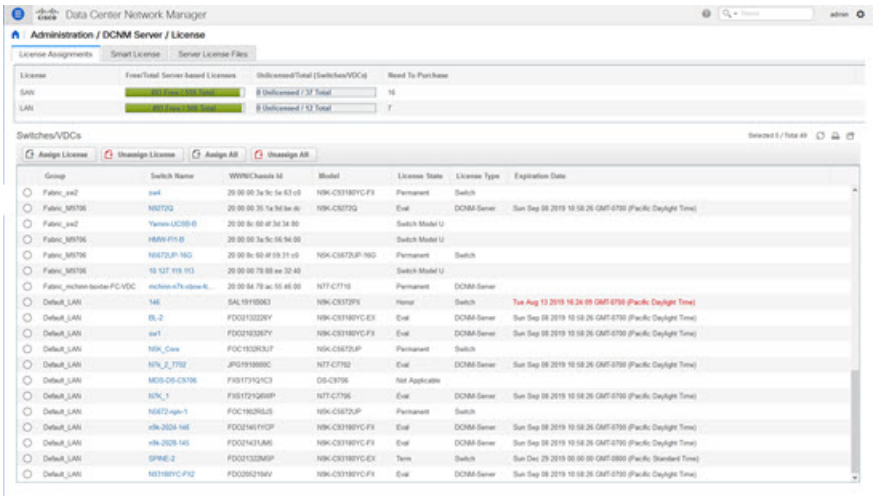
    The selected licenses are uploaded and installed on their respective switches. Status messages, including any issues or errors are updated for each file as it completes.
11. After the license matches with respective devices and installs, the **License Status** table displays the status.

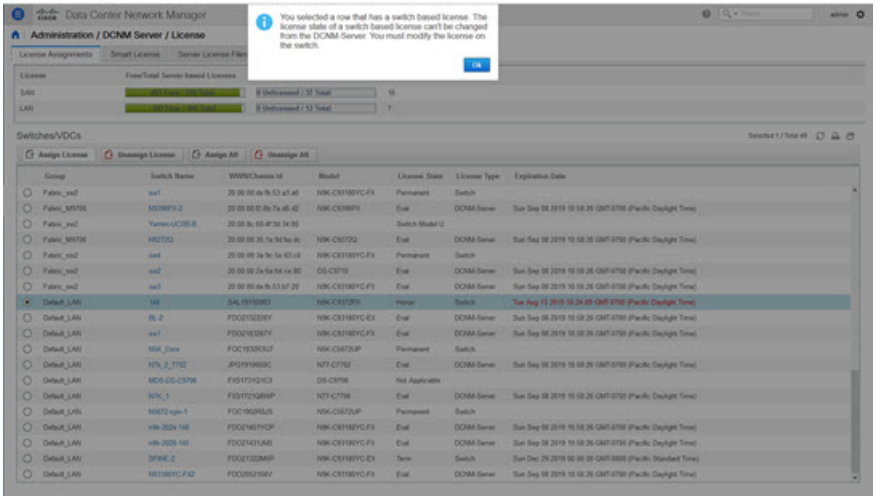
### Switch-based honor license support

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.




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

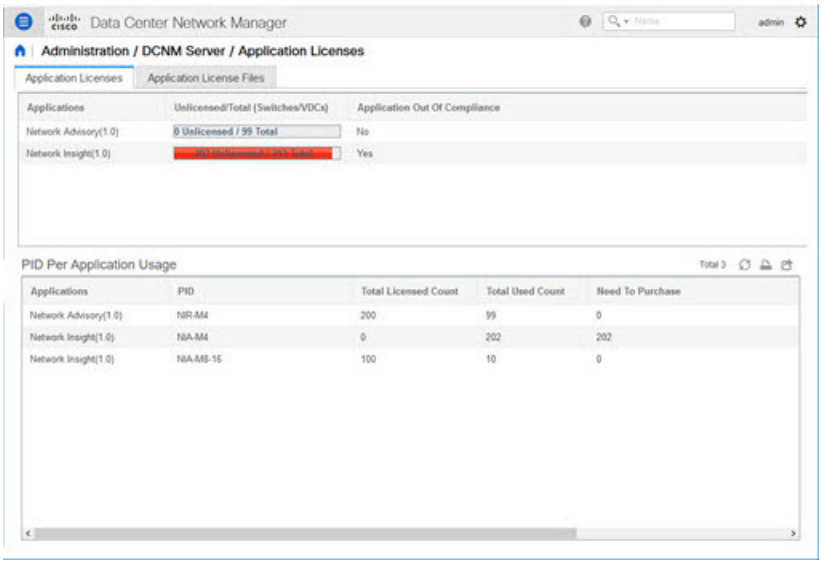


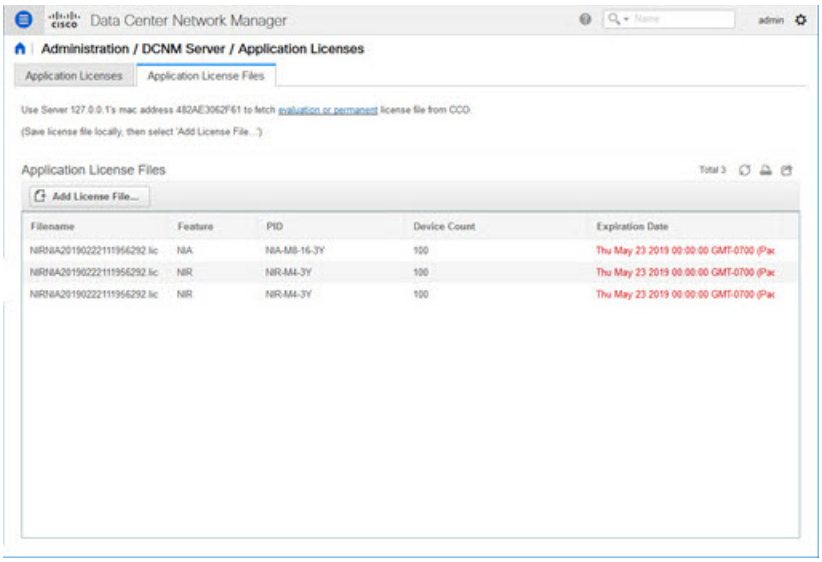

# Application Licenses

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.

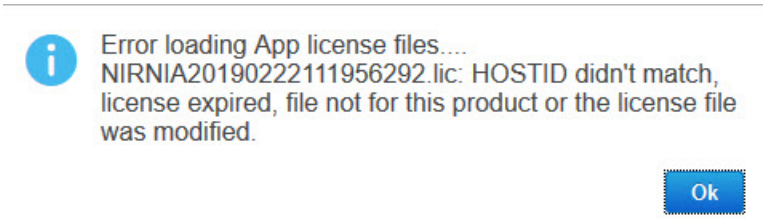
The Application Licenses tab displays the DCNM Applications with a summary of their unlicensed/total switches and if they are out of compliance. The PID Per Application Usage table displays the actual counts per PID given to the server from the Application Framework. The PIDs that need to be purchased 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 SAN services if you update the Remote AAA properties. You must restart all the instances of Cisco DCNM if federation is deployed.

## 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.

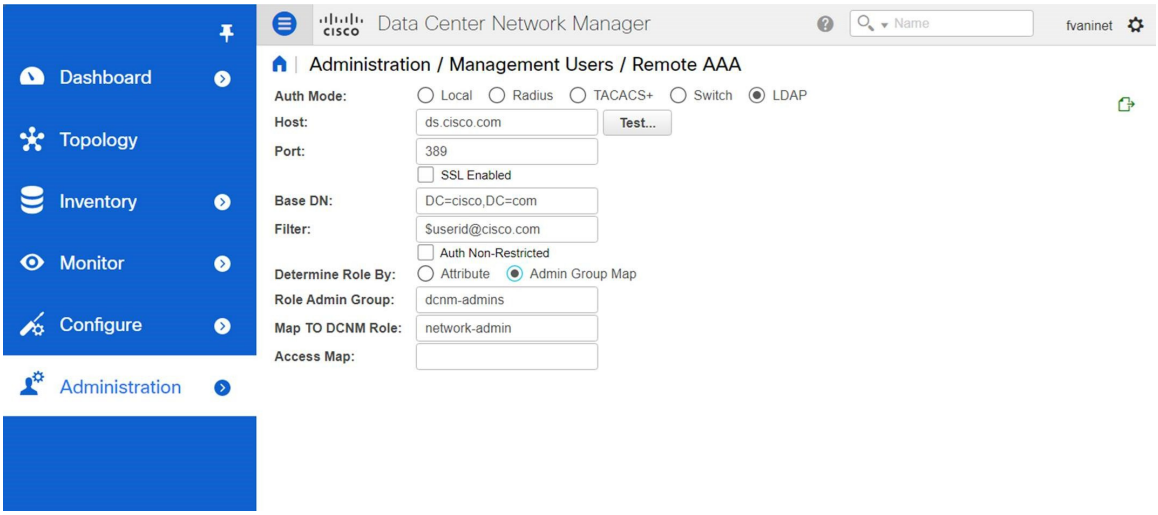
**Step 3** (Optional) Specify the names for Secondary and Tertiary Switches.

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

# LDAP

### Procedure

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




**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:

```
ldapserver# 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**

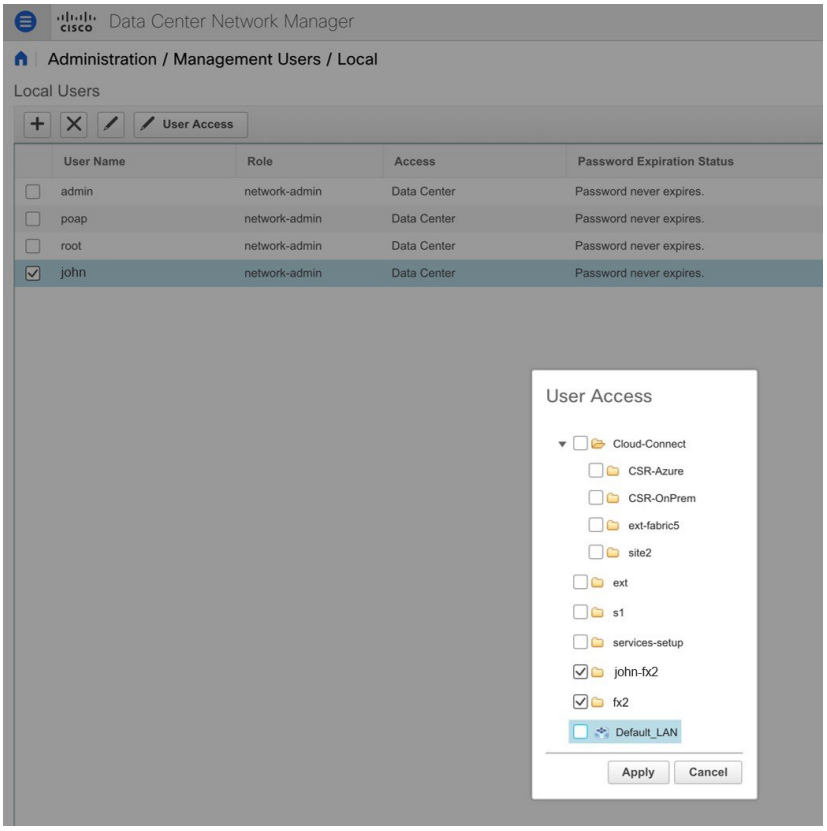
**Step 1** Choose **Administration > Management Users > Local**.

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**.




# 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 Manager SAN 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 keep it in the **managedContinuously** state before creating a collection for the switch. Only licensed fabrics appear in this window.

To add a collection, follow these steps:

**Procedure**

**Step 1** Choose **Administration > Performance Setup > SAN Collections**.

**Step 2** Select a fabric and select the **Name**, **ISL/NPV Links**, **Hosts**, **Storage**, **FC Flows**, and **FC Ethernet** to enable performance collection for these data types.

**Step 3** Click **Apply** to save the configuration.

**Step 4** In the confirmation dialog box, click **Yes** to restart the performance collector.

# 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

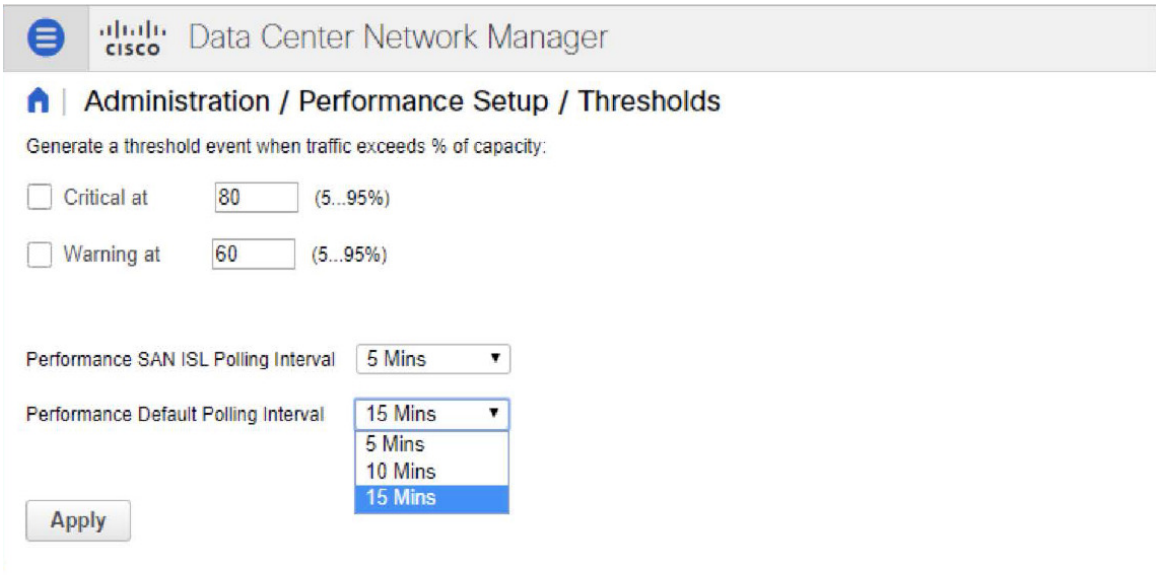
**Step 1** Choose **Administration > Performance Setup > Thresholds**.

**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**.



## Configuring User-Defined Statistics

To configure user-defined statistics from the Cisco DCNM Web UI, perform the following steps:

**Procedure**

**Step 1** Choose **Administration > Performance Setup > User Defined**.

The User-Defined statistics window is displayed.

**Step 2** Click **Add** icon.

The **Add SNMP Statistic to Performance Collection** window is displayed.

**Step 3** From the **Switch** table, select the switch for which you want to add other statistics.

**Step 4** From the **SNMP OID** drop-down list, select the OID.

**Note** For SNMP OID ModuleX_Temp,IFHCInOctets.IFINDEX,IFHCOutOctest.IFINDEX, selected from drop-down list, you must replace 'X' with correct module number or the corresponding IFINDEX.

**Step 5** In the **Display Name** box, enter a new name.

**Step 6** From the **SNMP Type** drop-down list, select the type.

**Step 7** Click **Add** to add this statistic.

# 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.

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, or in the **Apply and Test** icon, use the drop-down to select the fabric.

Click **Apply and Test** to save and test 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**.

# Configuring EMC CallHome

To configure EMC Call Home for EMC supported SAN switches from the Cisco DCNM Web UI, perform the following steps:

**Procedure**

**Step 1** Choose **Administration > Event Setup > EMC Call Home**.

**Step 2** Select the **Enable** check box to enable this feature.

**Step 3** Use the check box to select the fabrics or individual switches.

**Step 4** Enter the general email information.

**Step 5** Click the **Apply** to update the email options.

**Step 6** Click **Apply and Test** to update the email options and test the results.

# 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 and SAN Client. 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 **SANLAN, Port Groups** or **Any**. For **SAN** and **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 **SAN/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:

# SAN Credentials

The Cisco DCNM home page, choose **Administration > Credentials Management > SAN Credentials** displays the SNMP access details to the fabric seed switch. If the user has validated the access to all the fabrics, the SNMP credentials for all the seed switches of the fabrics is displayed.

The switch credentials window for the Cisco DCNM has the following fields:

| Field | Description |
|---|---|
| Fabric Name | The fabric name to which the switch belongs. |
| Seed Switch | IP address of the switch. |
| User Name | Specifies the username of the Cisco DCNM user. |
| Password | Displays the encrypted form of the switch SNMP user. |
| SNMPv3/SSH | Specifies if the SNMP protocol is validated or not.<br>The default value is **false**. |
| Auth/Privacy | Specifies the Authentication protocol<br>The default value is **NOT_SET**. |
| Status | Displays the status of the switch |

Before the Cisco DCNM user configures the fabric using SNMP, the user must furnish and validate SNMP credentials on the seed switch of the fabric. If the user does not provide valid credentials for the fabric seed switch, the Switch Credentials table shows the default values for SNMPv3/SSH and AuthPrivacy fields.

Click the switch row and enter correct credentials information. Click **Save** to commit the changes.

If the user changes the configuration, but does not provide a valid switch credential, the user action is rejected. Validate the switch credentials to commit your changes.

You can perform the following operations on this screen.

- To Revalidate the credentials:
  1. From the Cisco DCNM home page, choose **Administration > Credentials Management > SAN Credentials**, click the **Fabric Name** radio button to select a seed switch whose credentials needs to be validated.
  2. Click **Revalidate**.

     A confirmation message appears, stating if the operation was successful or a failure.

- To clear the switch credentials:
  1. From the Cisco DCNM home page, choose **Administration > Credentials Management > SAN Credentials**, click the **Fabric Name** radio button to select a seed switch to delete.
  2. Click **Clear**.

     A confirmation message appears.
  3. Click **Yes** to delete the switch credential from the DCNM server.

# 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.

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 40
- Validate Credentials, on page 41
- Clear Switch Credentials, on page 41
- Credentials Management with Remote Access, on page 41

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

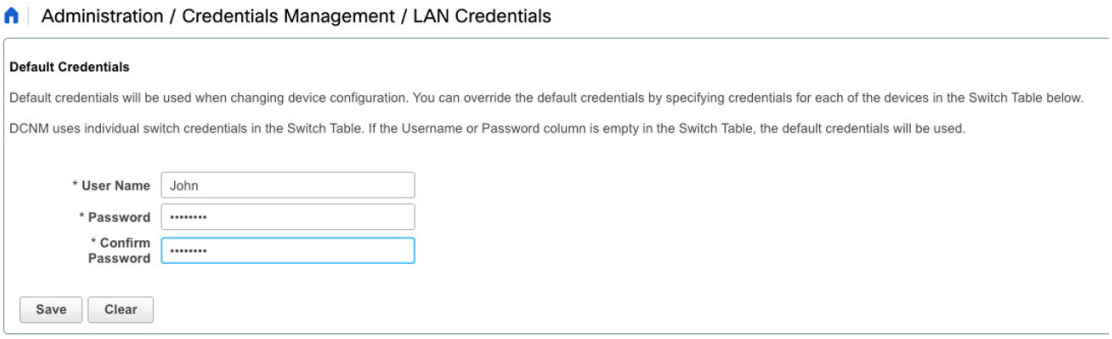
### Regular AAA Remote Authentication

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.

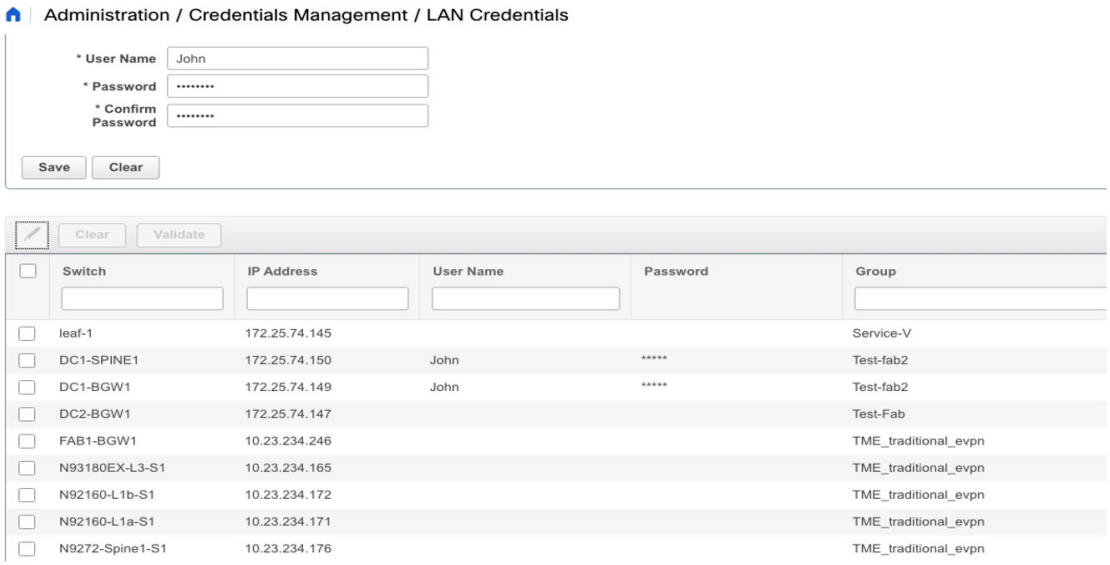
For example, let us consider a user named John, who has authentication on the ISE server.

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.




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.




4. 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.

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.

   **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.

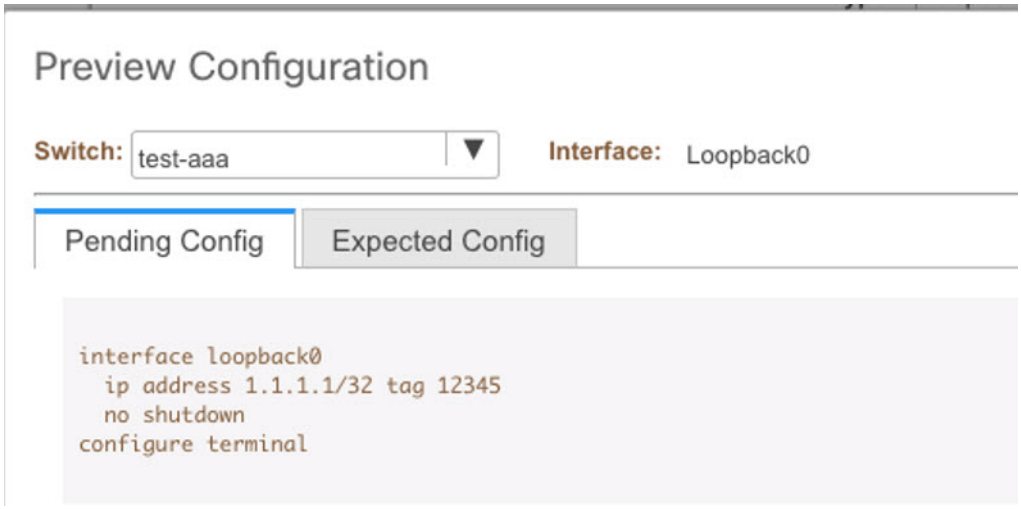
```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

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.

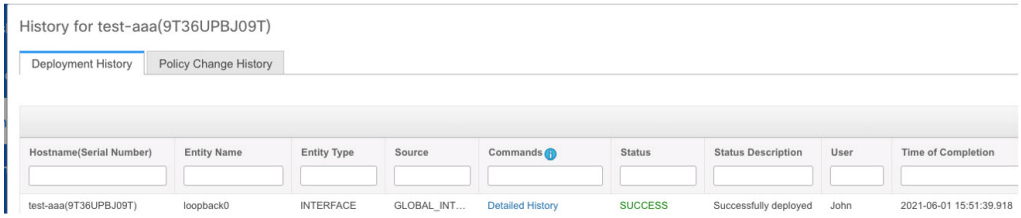

### Service Account Configuration Audit

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.




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




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#
```