Administration

This section contains context-sensitive Online Help content for the **Web Client > Administration** tab.

DCNM Server

The DCNM Server menu includes the following submenus:

Starting, Restarting, and Stopping Services

Procedure

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

You see a table of services per server and the status of each as shown in the below image.

Step 2 In the **Actions** column, use the **Start** or **Stop** icons to start or stop services, or the **Delete** icon to clean up PM DB stale entries. You can see the latest status in the **Status** column.

What to do next

Using the Commands Table

The commands table contains links to commands that will launch new dialog boxes to provide information about the server status and server administrative utility scripts. These can be directly executed on the server CLI as well.

- **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.
- **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/ISO installations.

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 in the right column.

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

Step 4 Click the **Print** icon on the upper right corner of the right column to print the logs page.

Server Properties

This page allows you to set common parameters, which are populated as default values in the DCNM server.

Specify the parameters in the following fields according to the corresponding description.

Procedure

	Command or Action	Purpose
Step 1	Choose **Administration > DCNM Server > Server Properties**.	
Step 2	After finishing all the property fields, click **Apply Changes** to save the server settings.	

Configuring SFTP/TFTP/SCP Credentials

You can configure the SFTP/TFTP/SCP credentials for the file store.

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

Procedure

Step 1 From the menu bar, choose **Administration > DCNM Server > Archive FTP Credentials**.

You will see **Archive FTP Credentials** page.

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 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 SFTP 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 SFTP is unavailable on your device, you can use third-party SFTP applications, such as, miniSFTP, 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.

c) From the **Verification Switch(es)** drop-down, select the switch.
d) Click **Apply** to save the credentials.
e) Click **Verify & Apply** to verify if SFTP and switch has 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. Go to **Configure > Backup > Switch Configuration > Archive Jobs > Job Excecution Details** page 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 will receive a *permission denied* error. You can change your credentials from the **Inventory > Discovery** page.

a) From the **Verification Switch** drop-down, select the switch.
b) Click **Apply** to save the credentials everywhere..

c) Click **Verify & Apply** to verify if TFTP and switch has connectivity and save the configuration. If there are any failures during the verification, the new changes will not be 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, miniSCP, 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 Switch(es)** drop-down, select the switch.
d) Click **Apply** to save the credentials everywhere.
e) Click **Verify & Apply** to verify if SCP and switch has 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. Go to **Configure > Backup > Switch Configuration > Archive Jobs > Job Excecution Details** page to view the number of successful and unsuccessful switches.

Step 5 From the menu bar, 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.

Examples for SFTP Directory Path

Use Case 1:

If Cisco DCNM is installed on Linux platforms (OVA, ISO, 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 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 (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 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 which doesn't 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 (Chassis or Line cards).
- Support latest NX-OS versions.
- Support critical fixes as patches.

Procedure

Step 1 Choose **Administration > DCNM Server > Modular Device Support** to view the patch details.

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

Step 2 You can view all the DCNM servers under the **DCNM Servers** window. It includes the list of patch 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, please go to http://www.cisco.com/go/dcnm for more information.

Managing Switch Groups

Beginning with Cisco NX-OS Release 6.x, you can configure switch groups by using Cisco DCNM Web UI. You can add, delete, rename, or move a switch to a group or move a group of switches to another group.

This section contains the following:

Adding Switch Groups

You can add a switch group from the Cisco DCNM Web Client.

Procedure

Step 1 From the menu bar, choose **Administration > DCNM Server > Switch Groups**.

Step 2 Click the **Add** icon, and the **Add Group** window appears 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

Deleting a Group or a Member of a Group

You can delete group(s) and/or member(s) of a group from the Cisco DCNM Web Client. When you delete a group, the associated group(s) are deleted and the fabrics or Ethernet switches of the deleted group(s) are moved back to the default SAN or LAN.

Procedure

Step 1 Choose the switch group or member(s) of a group that you want to remove.

Step 2 Click the **Remove** icon or press the Delete key on your keyboard.

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

Procedure

Step 1 Select the switch or switch group.

Step 2 Drag the highlighted switch or switch group to another group. To move multi devices or switches across different switch groups, you can select multiple devices using **CTRL** key or **SHIFT** key.

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

Note It is not allowed to move multiple items on the group level. You may not mix group with devices.

Managing Licenses

This section includes the following topics:

Viewing Licenses Using the Cisco DCNM Wizard

You can view the existing Cisco DCNM licenses by choosing **Administration > DCNM Server > License**.

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

License Assignments

The following table displays the **License Assignments** for every switch.

Field	Description
Group	Displays if it is a fabric or LAN group.
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: • Permanent • Eval • Unlicensed • Not Applicable • Expired • Invalid
License Type	Displays if the license is a switch-based embedded license or a server-based license.
Eval Expiration	Displays the expiry date of the license. **Note** Text in the eval expiration field will be 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.

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.
Eval Expiration	Displays the expiry date of the license. **Note** Text in the eval expiration field is in Red for licenses that expires in seven days.

Automatic License Assignment

When the fabric is first discovered 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. Also, 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.

Adding Cisco DCNM Licenses

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

Before you begin

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

Procedure

Step 1 Choose **Administration > DCNM Server > License** 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 then 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.

Assigning Licenses

Before you begin

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

Procedure

Step 1 Choose **Administration > DCNM Server > License** to start the license wizard.

The licenses table appears.

Step 2 From the table, choose the switch that you want to assign the license to.

Step 3 Click **Assign License**.

Unassigning Licenses to a Switch

Before you begin

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

Procedure

Step 1 Choose **Administration > DCNM Server > License** to start the license wizard.

The licenses table appears.

Step 2 From the table, choose the switch that you want to unassign the license.

Step 3 Click **Unassign License**.

Native HA

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.
  1. SSH into the DCNM active host.
  2. 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/ pgsql-standby-backup.tgz. If the file exists, restore database data files:

```
rm -rf    data/*
tar -zxf    replication/ pgsql-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.

Management Users

The Management Users menu includes the following submenus:

Remote AAA

Procedure

Step 1 From the menu bar, choose **Administration > Management Users > Remote AAA Properties**.

The AAA properties configuration page appears.

Step 2 Use the radio button to select one of the following authentication modes:

- Local—In this mode the authentication will authenticate with the local server.
- Radius—In this mode the authentication will authenticate against the Radius servers specified.
- TACACS+—In this mode the authentication will authenticate against the TACAS servers specified.
- Switch—In this mode the authentication will authenticate against the switches specified.
- LDAP—In this mode the authentication will authenticate against the LDAP server specified.

Step 3 Click **Apply**.

Note You must 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.
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.
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.

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 DNS address of the host.
Step 3 Click **Test** to test the AAA server. The **Test AAA Server** window pops out.
Step 4 Enter a valid **Username** and **Password** in the **Test AAA Server** window.

A dialog box appears confirming the status of the AAA server test. If the test has failed, the **LDAP Authentication Failed** dialog box appears.

Step 5 In the **Port** field, enter a port number.

Step 6 (Optional) Select the **SSL Enabled** check box, if SSL is enabled on the AAA server.

Step 7 In the **Base DN** field, enter the base domain name.

Step 8 In the **Filter** field, specify the filter parameters.

Step 9 Choose an option to determine a role by either **Attribute** or **Admin Group Map**.

Step 10 In the **Role Admin Group** field, enter the name of the role.

Step 11 In the **Map to DCNM Role** field, enter the name of the role to be mapped.

Step 12 In the **Access Map** field, enter the Role Based Access Control (RBAC) group to be mapped.

Step 13 Click Apply Changes icon on the upper right corner to apply the LDAP configuration.

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

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

Procedure

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

The **Local Users** window is displayed.

Step 2 Click **Add User**.

The **Add User** window is displayed.

Step 3 Enter the username in the **Username** 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.

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 to 7 to continue adding users.

Deleting Local Users

Procedure

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

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. Or click **No** to cancel deletion.

Editing a User

Procedure

Step 1 From the menu bar, 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 **User Name** and **Role** is mentioned by default. Specify the **Password** and **Confirm Password**.

Step 4 Click **Apply** to save the changes.

User Access

To control the local users to access the specific groups from the Cisco DCNM Web UI, 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 groups allowed to access for the user 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.

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 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 Polling Interval** from the drop-down list. Valid values are **5 min** and **10 min**, and the default is **5 min**.

Step 4 Click **Apply**.

Configuring User Defined Statistics

Procedure

Step 1 From the menu bar, choose **Administration > Performance Setup > User Defined**.

You see the User Defined page.

Step 2 Click **Add** icon.

You see the **Add SNMP Statistic to Performance Collection** dialog box.

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 box, 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 Web client:

- Enabling **Send Syslog**: Choose **Physical Attributes > Events > Syslog > Servers**. Click the **Create Row** icon, provide the required details, and click **Create**.
- Enabling **Send Traps**: Choose **Physical Attributes > Events > SNMP Traps > Destination**. Click the **Create Row** icon, 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 checkboxes 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 Select **Enable Syslog Receiver** checkbox and click **Apply**, to enable the syslog receiver if it is disabled in the server property.

To configure the Event Registration/Syslog properties, select **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 e-mail 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** e-mail 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.

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 sent by Cisco DCNM correspond to the severity type followed by a text description:

```
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.

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, do the following tasks:

Procedure

Step 1 From the menu bar, select **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.

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 23
- Validate Credentials, on page 23
- Clear Switch Credentials, on page 23

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.