CHAPTER 3

Cisco Prime DCNM Web Client

Using Cisco Prime DCNM Web Client, you can monitor Cisco MDS and Nexus family switch events, performance and inventory, and perform minor administrative tasks.

Cisco Prime DCNM Web Client has few Graphical User Interface related changes. The new Cisco Prime DCNM Web Client is user experience (UX) 1.7 compliant.

The default user credentials to access DCNM 7.1.x are as configured during the deployment of the installers.

Cisco Prime DCNM Web Client provides the following features:

Navigating DCNM Web Client

The DCNM Web Client has standardized certain navigation conventions.

- Sorting Columns, page 3-3
- Cisco Prime DCNM Web Search Engine, page 3-3

Scope Menu

Beginning with Cisco NX-OS Release 6.x, a new drop-down list called Scope is added to Cisco Prime DCNM Web Client that applies to all pages except the Admin pages.

You can use the scope menu to filter network information by:

- Default_LAN
- Default_SAN
- Individual Fabric
- Group

Note You can organize your fabrics and LAN switches in the **Admin > Groups** page.

The features accessible from the tabs are limited to the areas that you choose in the filter tree.

Admin Menu

You can use the admin menu to:

- **Set Default LAN Credentials**: These credentials will be used when connecting to the DCNM LAN devices.
- **Change Password**: Changes the password for the current logged in user.
- **Logout**: Logout from the DCNM Web Client.

Table and Filtering Navigation

Some tables that can be filtered will have a filter option to view subsets of the information. Either choose the filter menu or click **Filter**. An editable row at the top of the table appears. Enter values into the table cells and click **Return** to display matching rows.

Printing

Click **Print** to view the table in a printer-friendly format. You can then print the page from the browser.

Exporting to a File

An Export icon is in the lower right corner of some tables or top right corner of the window. Click this icon to export the data to Microsoft Excel.

Sorting Columns

Not all columns are sortable but you can click a sortable column head to sort the information for that column.

Cisco Prime DCNM Web Search Engine

The search engine helps you to locate records according to the following search criteria:

- Search by Name.
- Search by IP Address.
- Search by WWN.
- Search by Alias.
- Search by MAC Address.
- Search by Serial Number.

For more information see the section Using the Cisco Prime DCNM Search Engine, page 3-3.

Using the Cisco Prime DCNM Search Engine

Step 1 Click **Search box** on the top right corner of the main window.

You see the search text box.

Step 2 Use the drop-down to search by:

- Name
- IP Address
- WWN
- Alias

Step 3 Enter the value based on the search option and click the arrow to begin the search.

The search results are displayed in a new window.

Step 4 Select **Inventory** or **Performance** tabs to view specific search results.

Downloading Cisco Prime DCNM-SAN Client

You must use Cisco Prime DCNM Web Client to launch Cisco Prime DCNM-SAN Client.

Step 1 On the DCNM Web Client home screen, click **Cisco Prime DCNM-SAN**.

If you are launching Cisco Prime DCNM-SAN Client for the first time, you see a message asking if you want to create shortcuts for Cisco Prime DCNM-SAN.

Step 2 Click **Yes** to create shortcuts for Cisco Prime DCNM-SAN.

Step 3 If you have the latest Java version installed, a Warning message is displayed.

Note The DCNM-LAN client supports JRE versions 1.6 and 1.7.

Step 4 Click **Run with the latest version** button.

Step 5 Enter the user credentials to log on to Cisco Prime DCNM-SAN client. This message appears only the first time you launch Cisco Prime DCNM-SAN Client.

Downloading Cisco Prime DCNM-LAN Client

You must use Cisco Prime DCNM Web Client to launch Cisco Prime DCNM-LAN Client.

Step 1 On the DCNM Web Client home screen, click **Cisco Prime DCNM-LAN**.

If you are launching Cisco Prime DCNM-LAN Client for the first time, you see a message asking if you want to create shortcuts for Cisco Prime DCNM-LAN.

Step 2 Click **Yes** to create shortcuts for Cisco Prime DCNM-LAN.

Step 3 If you have the latest Java version installed, a Warning message is displayed.

Note The DCNM-SAN client supports JRE versions 1.6 and 1.7.

Step 4 Click **Run with the latest version** button.

Step 5 Enter the user credentials to log on to Cisco Prime DCNM-LAN client. This message appears only the first time you launch Cisco Prime DCNM-LAN Client.

Downloading Cisco Device Manager Client

You must use Cisco Prime DCNM Web Client to Install Cisco Device Manager client.

Step 1 On the DCNM Web Client home screen, click **DM**.

Note Cisco Prime DCNM Device Manager supports JRE versions 1.6 and 1.7. Follow the instructions in the Cisco Device Manager installer wizard to proceed with the installation.

Step 2 Once the installation is complete, enter the user credentials to log on to the Cisco Device Manager client.

Connecting to a Switch using the CLI

You can use the Cisco Prime DCNM Web Client to connect to a switch using the CLI.

Step 1 On the DCNM Web Client home screen, click **CLI**.

Step 2 Click the **Connect** button.

Step 3 In the configuration window, use the check-box to select the switches.

Step 4 Enter the user credentials and click the **Connect** button.

Step 5 Use the switch panel to specify the command for a specific switch.

Adding a Security Exception

Step 1 On the warning page, click **Or you can add an exception**.

Step 2 Click **Add Exception**.

The Add Security Exception dialog box appears.

Step 3 Click **Get Certificate**.

Read the text that describes the problems with this site.

Step 4 Click **Confirm Security Exception**.

- MAC Address
- Serial Number

Viewing Dashboard Information

The Cisco Prime DCNM Web Client dashboard gives you comprehensive information of the following:

- Summary - You can view the summary dashboard which displays the overall functioning of all the devices connected. It gives you daily statistics of the connected devices.
- Fabric - You can view the status of the inter switch links and edge ports.
- Compute - You can view the details and events for a particular Host along with its events and topology.
- Switch Dashboard - You can view details pertaining to a switch along with its current status and licensing information.
- Storage - You can view details about the storage device along with its events and topology.

Summary

The intent of the summary dashboard is to enable network and storage administrators to focus on particular areas of concern around health and performance of the data center switching as a snapshot of the last 24 hours. The functional view of the LAN and SAN switching consists of six dynamic portlets that display information in context of the selected scope. The scope can be adjusted in the upper center of the page to display more focused information particular to the managed domain and offers details of the specific topology or set of topologies part of the data center scope.

The various scopes available on the Cisco Prime DCNM Web Client are:

- datacenter
- defailt_SAN
- defailt_LAN

The following portlets are displayed on the summary dashboard, based on the scope of the Web Client:

- Health, page 3-6

Health

Broken into two sections listing specific problem areas by type of alert (host, ISL/trunks, VSAN, switch, storage) and events in the form of traps and syslogs listed in order of their severity for a period of 24 hours. The events and problems are hyper-linked to Health > Events and are filtered only for the clicked entity allowing you to drill down to particular problem or event for the contextual information. The events and problems change in context of the selected topology scope to display fabrics (SAN) and switches (LAN) that are part of the default or user defined group. The Health pane will display counts for Path not redundant and Missing Paths which will redirect to the SAN Path Errors, page 3-23 section.To customize these groups to display more granular information see the Managing Switch Groups, page 3-91 section.

Inventory

Displays the currently discovered inventory based on the selected scope. Switch inventory is broken into FC (Director vs Switch) and Ethernet and Virtual environment totals (VSAN and VLAN configuration). The bar graphs depicts used vs. available for capacity planning.

Click the + icon in the upper right corner to display 6 new boxes displaying detailed inventory for the logical environment, physical switches, ISLs of various types, modules installed (director class line cards and switches are shown), Ports which are broken into type (FC vs. Ethernet) with sub-categories showing counts based on speed. The final box displays Port Capacity, which shows percentage of ports used and calculates the days remaining of available ports based on consumption of available ports. By clicking the square icon in the upper right corner you will return to the previous view

Top CPU

Displays CPU utilization for the discovered switches over the last 24 hours with a red bar displaying the high watermark for that 24 hour period.

Click the + symbol in the upper right corner to display more detailed information of the average percentage of usage, peak percentage of usage, and the last time the information was updated

Top ISLs/Trunks

Displays the performance data for the top 10 performing ISLs and/or Trunk ports. Each entry shows current receive and transmit percentage with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the Performance Manager Collections, page 3-101 section. Clicking on the bar graph to the left of each entry will provide a 24 hour graph for the selected item to provide context to the performance data being shown.

Click the + symbol in the upper right corner to display more detailed information on each entry by displaying the speed of the ISL/Trunk, the average and peak receive data, the average and peak transmit data, the combined receive and transmit data, the total number of errors and discards in the last 24 hours, and the time the data was last updated. By clicking the square icon in the upper right corner you will return to the previous view.

Top SAN Host Ports

Displays the performance data for the top 10 performing SAN host ports. Each entry shows current receive and transmit percentage with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the Performance Manager Collections, page 3-101 section. Clicking on the bar graph to the left of each entry will provide a 24 hour graph for the selected item to provide context to the performance data being shown.

Click the + symbol in the upper right corner to display more detailed information on each entry by displaying the speed of the ISL/Trunk, the average and peak receive data, the average and peak transmit data, the combined receive and transmit data, the total number of errors and discards in the last 24 hours, and the time the data was last updated. By clicking the square icon in the upper right corner you will return to the previous view.

Top SAN Storage Ports

Displays the performance data for the top 10 performing SAN host ports. Each entry shows current receive and transmit percentage with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the Performance Manager Collections, page 3-101 section. Clicking on the bar graph to the left of each entry will provide a 24 hour graph for the selected item to provide context to the performance data being shown.

Click the + symbol in the upper right corner to display more detailed information on each entry by displaying the speed of the ISL/Trunk, the average and peak receive data, the average and peak transmit data, the combined receive and transmit data, the total number of errors and discards in the last 24 hours, and the time the data was last updated. By clicking the square icon in the upper right corner you will return to the previous view.

Viewing Health Summary Information

Step 1 From the menu bar, choose **Dashboard > Summary** and then see the **Health Summary** view.

In the left side of the window, you see a summary table of problems and in the right side of the window, you see a summary table of events in the last 24 hours.

Step 2 Click the warnings next to Switches, ISLs, Hosts, or Storage (other than 0) to see an inventory of switches, ISLs, or end devices for that fabric.

Step 3 Choose the number of events next to the event severity levels (**Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info**, or **Debug**) to see a summary of events and descriptions.

Viewing Performance Summary Information

BEFORE YOU BEGIN

To view performance information, you must activate performance collector.

From the menu bar, choose **Dashboard > Summary**, and then click **Daily Performance** view.

You see the Summary information.

The Top SAN Ports, Top SAN Storage Ports, Top ISL's/Trunks and Top Access Ports are Performance pods that are displayed depending on the pods selected.

If you select the Scope as default_SAN, a new area Daily Performance is displayed. For more information see the New Area - Daily Performance, page 3-11 section.

Viewing Inventory Summary Information

Step 1 From the menu bar, choose **Dashboard > Summary**.

The Inventory summary pane is displayed.

Step 2 Click the + icon or double-click the **Inventory** summary pane to view information for the selected scope only.

The complete inventory details are displayed.

Differences by changing the Scope to default LAN or configured switch group

Note To configure switch groups, see the Managing Switch Groups, page 3-91 section.

- Health - Only LAN events are displayed.
- Inventory - Only LAN switch data is displayed
- Top ISLs/Trunks - Only displays LAN based ISLs/Trunks
- Top CPU - Only displays CPU data for the LAN switches
- Top Access Ports - Displays LAN access port performance information.
- A new area Topology is displayed. For more information, see the Topology, page 3-8 section.

Topology

This displays the current physical topology with color- coding (displayed with a key in the lower right corner) for ISL utilization. You can hover over the switch indication circles to display the configured switch name, IP address, switch model, firmware version, last polled CPU utilization, and last polled memory utilization.

The memory or CPU utilization are displayed on the switch indicators. In addition the ISL/Trunk paths are also color-coded based on their TX+RX peak utilization. You can hover over the ISL/Trunk to show list of ports that create the connection and click on individual paths to launch the performance chart showcasing TX and RX utilization for the last 24 hours.

Click the **+** symbol in the upper-right corner to maximize the window and enables you to drag the switch icons to best display their infrastructure. Once icons are placed in the most desirable position you can save the layout by clicking the **Save** icon in the upper-left corner of the topology map. If the layout is moved you can restore the previously saved layout during the current session by clicking the **Restore** icon in the upper-left corner next to the save icon.

When the number of nodes is large, the switch information will not be displayed, as it cannot be accommodated on the page. However, if you click the **Switch Name** or use filters down to a subset, you will be able to view the switch information.

VxLAN VTEPs are shown in topology with **VTEP** icons. Click on the filter in top right corner in topology screen to search VTEPs based on VNI (VNI value > 4095) or multicast address. A **Details** link appears below the filter box. Click on the **Details** link below the filter box to view the search data in tabular format. In VNI search context, click **VTEP** to view the VTEP active peers.

The L2 view shows VLANs configured among the discovered devices. You can choose to view your topology based on the VLANs or Mapped Fabric Path topology. It also provides a visual representation of forwarding and non-forwarding links between Cisco Nexus devices in a data center network for configured VLANs.

FabricPath View

FabricPath support for L2MP capable devices, running the L2MP-ISIS protocol, is available in the L2 View of the Topology drawer. The L2 View contains a dialog box that allows you to select the type of graph to display. In each topology, a broadcast graph (multi-destination graph) is created by default to carry broadcast traffic and unknown unicast traffic. When you select the Fabricpath view in the dialog box, you can display the following types of graphs:

- Multi-destination—A multi-destination or broadcast graph built by ISIS for specified VLAN range to which the topology is mapped to in fabric path cloud.

  ISIS maintains reachability information from each node to all other nodes that are present in fabric path cloud. Give a node, DCNM will enable users to view which all other nodes in fabric path cloud are not reachable.
- Unicast—A unicast graph displays equal cost routes between nodes in the fabric path cloud.
- Multicast—A multicast graph displays the multicast traffic from a specified device to all hosts that are listening to a particular IGMP group.

The FabricPath Topology Wizard allows you to do many operations, such as add to the FabricPath topology, display inventory, and display end devices.

To view the FabricPath topology in the L2 view:

Step 1 Navigate to **Dash Board > Topology**. Expand the LAN topology.

Step 2 Select **L2 view > FabricPath**.

Step 3 Enter the Topology ID. The resulting action highlights all the links which are part of the specified topology.

Step 4 To view the broadcast graph, select the Multi destination option in the graph selection window. Select the anchor device for which the broadcast graph must be displayed.

Step 5 To view the unicast graph, select **Unicast** in the graph selection window. Select the source and the destination nodes.

Step 6 To view the multicast graph, select **Multicast** in the graph selection window. Select the IGMP address and the ftag ID, and the anchor node for which the multicast graph must be displayed.

VLAN View

VLAN view allows you to see the layer 2 network for the given range of VLAN. All the information related to STP such as protocol, STP role, STP root information are shown to the operator on topology. It is possible to see this information for a particular Switch group.

Spanning Tree Protocol (STP) is used to prevent loops when switches are interconnected via redundant links in a switched network. STP identifies the loops in a network and shuts down the redundant links to prevent the loops from forming. In the event of a link failure, STP will automatically activate the corresponding redundant link. In case of a switched network with multiple VLANs, loop-free paths will have to be computed for every VLAN.

During shallow discovery we are already fetching the information related to VLAN. Layer 2 Topology provides a visual representation of forwarding and non-forwarding links between networks of Nexus Devices for VLANs configured on them. VLAN view helps network administrators to manage STP protocol by providing a visual display of blocking and forwarding links and view information such as STP states (forwarding, blocking, learning, listening), STP roles(root, designated) and the root switch for STP.

To view the VLAN topology in the L2 view:

Step 1 Navigate to **Dash Board > Topology**. Expand the LAN topology.

Step 2 Select **L2 view > VLAN**.

Step 3 Enter the VLAN range like “1-10”.

Step 4 Click on **Fetch** button.

By default, the forwarding and blocked links are shown in the topology. All the forwarding links are in green, blocked in red and the other links are greyed out. It will take some time to populate the topology since the information is fetched from the devices on demand. Select a given link and it will show all the information about that link.

Uncheck the option **Show Non-Forwarding link**, only forwarding links are shown in the topology. Uncheck the option **Show Forwarding link**, only blocked links are shown in the topology.

Port Channel and vPC View

To view the PC vPC topology in the L2 view:

Step 1 Select Scope as default_LAN or DataCenter.

Step 2 Navigate to Dashboad > Summary.

Step 3 Select the appropriate Device Group and open Topology.

Note Note: The port channels and vPC links are displayed when the user switches to PC vPC view on the topology screen supporting both LAN and SAN devices.

The PC vPC displays the vPCs, port channels, and physical links that are not part of vPC or port channel.

Differences by changing the Scope to default SAN or configured switch group

Note To configure switch groups, see the Managing Switch Groups, page 3-91 section.

- Health - Only SAN within scope events are displayed.
- Inventory: Only SAN switch data within the inventory is displayed
- Top SAN Host Ports: Displays SAN host port performance information within scope.
- Top SAN Storage Ports: Displays SAN storage port performance information within scope.
- Topology: Displays SAN topology within scope.
- A new area Daily Performance is displayed. For more information, see the New Area - Daily Performance, page 3-11 section.

New Area - Daily Performance

This area displays the total performance of the displayed scope broken into three sections. ISL, Host and Storage. Total monitored port count per area is shown below the circular graph.

Each of the circular graphs will display the percentage of utilization based on 3 different thresholds depicted with color differentiation as follows:

- 0-50%: Green
- 51-80%: Yellow
- 81-100%: Red

You can click each displayed area to view performance data for only the ports, which fall within each performance scope. This will display more detailed information on each entry by displaying the name of the port. Click the bar graph icon to display the historical performance data for the selected port. A full performance graph also appears on the bottom of the screen displaying the last 24 hours, week, month, and year.

You can switch the graph to be displayed as a histogram and to perform predictive analysis on the port showing the most likely performance over the next 6 months based on the historical data gathered for the port. Click the **+** icon in the bar graph to overlay the performance data of any other port by clicking on the **+** icon and then clicking the graph icon next to another port listed above. The VSAN/VLAN configuration, speed of the trunk/ISL the average and peak receive data, the average and peak transmit data, the combined receive and transmit, the total number of errors and discards in the last 24 hours, and the last time the data was updated are also displayed.

To return to the summary view, from the menu bar select **Dashboard>Network**.

Fabric

The topology for the Fabric provides a tiered, scalable display for all the spines and leaves in the fabric. The topology feature also provides a visualization showing the health of the Central Point of Management (CPoM)(, which includes accessibility of DCNM to different services such as Power on Auto Provisioning (POAP) and Lightweight Directory Access Protocol service (LDAP).

The topology views are also integrated with an event/messaging mechanism using the open source package BlazeDS to dynamically update the display whenever any changes in the network are detected

There are two separate views:

- Inter Switch Links View
- Edge Ports View

Note You can use the Topology View or Table View icons to switch between different views.

Inter Switch Links View

Note These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

This view displays the super spines, spines and leaves in a tiered fashion. The super spines are displayed in the top tier under the section **<number of> Super Spines**, the spines are displayed in the middle tier under the section **<number of> Spines**, and the leaves are displayed under the section **<number of> Leaves**. Any spine that has tier level defined as 3 or above is considered as a Super Spine. If there are no super spines defined, then the spines and leaves are shown in 2 tiers.

The leaves can be grouped into Pods. Leaves inside a pod are shown as circles inside a box. Pod is defined for the switch by using the command **fabric connectivity pod** *<podname>*. The pod name is considered as the title for the pod. Any switch that do not have pods defined are shown under the Default pod. Border leaves and Edge Routers, are shown in vertical tiers in the BL/Edge Router pod with a dashed line border around the pod. BL/Edge Router is the standard default name for the pod showing border leaves and edge routers.

The Pods are ordered as Default pod, followed by user-defined pods in alphabetical order, followed by BL/Edge Router pod. Pod can be maximized using the '+' button at the top-right corner. Pressing the button again will bring it back to the original size. The size of the node inside the pod depends on the pod size and the number of nodes inside the pod.

All the nodes are shown as circles. The color of the circle depends on the status of the links or the status of the switch according to the color coding legend displayed under the Nodes section in the left-hand pane. The numbers on the circles indicate how many links are down currently on the switch. The numbers are not displayed in case of green (all links are OK) or grey circle (unreachable).

Clicking on the spine or leaf node disables all other nodes in that tier and displays detailed information about the links for the selected node in the left-side pane. The status column in the table shows the status of the link as an icon.

When the mouse is hovered over the target switch, the link between the 2 nodes is shown as a line along with a detailed popup. The popup displays the source port, target port, and status. Also, the corresponding row in the table on the left side panel is highlighted

Clicking on the selected node again will deselect the node and enable all the disabled nodes.

The color of the line specifying the link between the switches depends on the status of the link as defined below.

Green – Links status is Normal.

Red – Link is down

Blue – Cable/Tier mismatch detected

Orange – Wrong Configuration Detected

When a node is selected, the status of the link between the selected node and all the target nodes that the selected node is connected to is depicted by a colored halo around the original circle. The color of the halo depends on the status of the link, as specified above.

Check **Show Links** to view links between the Spines and the Leaves, and the links between the Border Leaves and the Edge Router.

Search

The search box in the left side panel provides a quicker way to search for a spine or leaf by name. It also supports VM search, where a user can enter a VM name (partial or complete) or VM IP or VM Mac or Segment ID or VxLAN ID or Multicast Group and search for the leaf/leaves that the VM(s) belong to.

The search box provides an auto-complete feature, which filters and shows the matched switch names in a drop down as the user types into the text box. User can type the partial or complete switch name in the box and enter to see the filtered results. A 'Details' link is shown under the search text box that can be clicked to see the search results. If only one node matches the entered text, then that node is selected and the rest of the nodes in the tier are disabled. The details for the links for that node are displayed on the left side panel. If multiple switch names match the entered text, all the matched nodes are, but no details are shown in the left side panel.

Edge Ports View

Edge Ports view provides a view of the leaf nodes as VPC pairs. The visualization provides an interface similar to Fabric Path Links view but with details specific to VPC feature.

Each leaf is shown as paired with its VPC peer, with the line between the pair indicating the VPC link. The numbers on the nodes indicate the number of edge ports down for that node.

The color of the circle depends on the status of the edge ports or the status of the switch.

Clicking on a node selects the node and its peer (if any) and shows the edge port status details for that node in the left side panel, as shown below.

On Selecting a single VPC pair, specific information about the VPC setup such as VPC domain ID, VPC peer names, VPC consistency state, VPC Peerlink consistency, Primary VPC Port Channel ID, VPC role for each peer, primary VPC peer link ID, Secondary VPC port channel ID and secondary VPC peerlink ID are all displayed in a short table above the interface listing.

No specific information is overloaded on the link colors, since the link is intended to represent both the Peer link and the keep alive link between peers

Health

This view (popup) can be accessed by clicking on ‘Health’ hyperlink on any of the topology visualization screens.

This view shows health of different services as defined by their accessibility from DCNM. These services include POAP (Power on Auto Provisioning), XCP (Extensible Communications Platform) service, LDAP (Lightweight Directory Access Protocol) service, etc., and the orchestrator which in turn is connected to different vCDs.

The node color is either green, which means the service is up and running and is accessible to DCNM, or red, which mean the service is down and cannot be accessed.

Switch Dashboard

The switch dashboard displays the details of the selected switch. The system information area includes the logical name of the switch, the group where the switch belongs, model number of the switch, serial number of the switch, the switch version, the location of the switch, IP address, model, world wide name (WWN) if available, uptime, DCNM license, status of the switch, indicators to determine whether the switch is sending traps and syslog information, current central processor unit (CPU) and memory utilization.

Step 1 From the menu bar, choose **Dashboard > Network**.

Step 2 An inventory of all the switches that are discovered by Cisco Prime DCNM Web Client appears. Click on a switch in the Name column. The switch dashboard appears.

Step 3 (Optional) Click **ssh** to access the switch through Secure Shell (SSH).

Step 4 (Optional) Click **Device Manager** to access the switch through Hypertext Transfer Protocol (HTTP) for that switch.

Step 5 (Optional) Click **Accounting** to go to the Viewing Accounting Information page for that switch.

Step 6 (Optional) Click **Backup** to go to the Viewing a Configuration page.

Step 7 (Optional) Click **Events** to go to the Viewing Events Registration page.

This physical port capacity feature is available for Cisco Prime DCNM licensed switches only.

The physical port capacity area includes the available ports in each tier, such as 40G, 10G, 8G, 4G, 2G, and 1G and also the predicted number of days remaining to reach the maximum (100%) utilization.

Step 8 Click a number under the Days left column to view the capacity trend.

Step 9 Choose the **Modules** tab to display all the modules that are discovered on the switch.

Step 10 Choose the **Interfaces** tab to display all the interfaces that are discovered for the switch. Select an interface row and right -click to view the following options:

- Port up... - Brings up a port.
- Port down... - Brings down a port.
- Access mode - Sets port in access mode.
- Trunk mode - Sets port in trunk mode.

Step 11 Select an option and in the CLI Authentication for the port window, specify the User Name and Password and click **Connect** to connect to the switch.

Note The CLI Authentication is required only if this is the first time you are performing an operation on an interface for a particular switch. For subsequent operations on the same switch, the authentication is not required.

A CLI window is displayed with the CLI details of the specific operation displayed at the bottom of the window.

Step 12 When you press Enter on your keyboard, a dialog is displayed confirming if you want to change the config on a selected interface.

Step 13 Close the **Blades** tab to display a list of UCS blades and their attributes.

Step 14 Click **OK** to continue or **Cancel** to abort the operation.

When you click on a link in the ConnectedTo column, you see the other end of where the interface is connected. For example, if the other end of the interface is a switch interface, then it launches the Interfaces tab of the switch that the interface is connected. If the interface is connected to an end device, then it launches the host or storage dashboard.

Step 15 Choose the **Licenses** tab to display all the licenses installed on the switch.

Step 16 Choose the **Features** tab to display a list of all the features installed on the switch. The features tab is displayed only on Cisco Prime DCNM-SAN switches.

Step 17 Choose the **VxLAN** tab to display all VNIs, Multicast address, VNI Status and mapped VLAN for the VTEP. The VTEP IP address is displayed in left panel.

Note VxLAN support is available on Cisco Nexus 6000 Series and Nexus 9000 Series switches only.

Compute

The compute dashboard provides you with all the information related to the discovered SAN and LAN hosts. It provides detailed information related to the network, such as I/O traffic, disk latency, CPU, memory statistics, topology, and events about each individual host and virtual machines that are configured on top of the virtual host. The compute dashboard consists of four panels:

- Host Enclosures panel—Lists the hosts and their network attributes.
- Traffic panel—Provides the I/O statistics, CPU and memory information, and disk latency of individual hosts or virtual machines.
- Topology panel—Provides end-to-end topology layout and path information between host enclosures and storage enclosures. The discovered virtual machines are displayed and when you select the virtual machine, the path to the SAN data source is displayed. You can toggle this view to list all data paths.
- Event panel—Provides information about events of all of the switch ports that are configured within a specific host enclosure.

This section contains the following topics:

Viewing Host Enclosures

Beginning with Cisco NX-OS Release 6.x, you can view and search the network servers that are connected to the Cisco NX-OS devices. Cisco Prime DCNM extends the fabric visibility up to the server and allows you to discover and search the end devices that are attached to the network.

Note Beginning with Cisco NX-OS Release 6.x, Server Credentials, Servers, and Static Server-Adapter Mapping are no longer available.

Step 1 From the menu bar, choose **Dashboard > Compute**.

You see the list of hosts in the host enclosures table.

Step 2 Click the **Show details** icon next to the host enclosure to view more details.

You see the Events, topology and Traffic information in the dashboard.

Step 3 To edit the host name, double-click the Host Name, edit and then click the **Apply Changes** icon.

Step 4 You can click the **Show Filter** to filter the storage enclosures by **Name** or by **IP Address**.

Viewing Host Events

Step 1 From the menu bar, choose **Dashboard > Compute**.

You see the list of hosts in the host enclosures table.

Step 2 Click the **Events** icon next to the host enclosure to view the Events panel.

Step 3 Click the + icon in the Events panel to expand.

A list of all the events for the selected Host is displayed.

Viewing Host Topology

Step 1 From the menu bar, choose **Dashboard>Compute**.

You see the list of hosts in the host enclosures table

Step 2 Click the **Show details** icon next to the host enclosure to view the host topology details.

Step 3 Click the magnifier icons to zoom-in or zoom-out.

Step 4 Click the **Fabric/Network** icon to view the Fabric/Network path.

Step 5 Click the **All Paths** icon to view the complete set-up.

Step 6 Click the **First Shortest Path** icon to view the first shortest path.

Note Click **Map View** icon to enable the icons listed in Step 4, 5 and 6 above.

Step 7 Click the **Tabular View** icon to view the host topology in tabular format.

View Host Traffic

Step 1 From the menu bar, choose **Dashboard > Compute**.

You see the list of hosts in the host enclosures table

Step 2 Click the **Show details** icon next to the host enclosure to view the host topology details.

Step 3 Use the drop-down to select the traffic according to the time duration.

Step 4 Select the icons to view the traffic as a **Grid**, **Line Chart** or **Stacked Chart**.

Step 5 In the Traffic pane, the Enclosure Traffic is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.

Network

Cisco Prime DCNM Web Client enables you to view details of the switch including the system information, switch capacity, modules, interfaces, and licenses.

Step 1 From the menu bar, choose **Dashboard > Network**.

Step 2 An inventory of all the switches that are discovered by Cisco Prime DCNM Web Client appears. Click on a switch in the Name column to view the Switch Dashboard.

Storage

The Storage dashboard provides you all the information about the SAN and LAN storage.

This section contains the following topics:

Viewing Storage Enclosure

Once a datasource is configured and the discovery is completed, the discovered storage system(s) are displayed in the Name column in storage enclosures

Step 1 From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.

You see the storage enclosures table.

Step 2 Click the **Show details** icon next to the storage name to view more details.

You see the Events, Topology and Traffic information in the dashboard.

Step 3 You can click the **Show Filter** to filter the storage enclosures by **Name** or by **IP Address**.

Step 4 In the Traffic pane, the Enclosure Traffic is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.

Clicking on an individual port slice of the pie chart will display specific traffic utilization details for that port.

Note Only EMC and NetApp vendors are supported. The ‘Other’ storage discovery handler is vendor neutral, so it depends on the vendor’s conformity to SMI-S standards to retrieve and display information.

Viewing Storage Enclosure Events

Step 1 From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.

You see the list of storage enclosures in the table.

Step 2 Click the **Events** icon next to the storage enclosure to view the Events panel.

Step 3 Click the + icon in the Events panel to expand.

A list of all the events for the selected storage enclosure is displayed.

Viewing Storage Enclosure Topology

Step 1 From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.

You see the list of storage enclosures in the table.

Step 2 Click the **Show details** icon next to the storage enclosure to view the topology details.

Step 3 Click the magnifier icons to zoom-in or zoom-out.

Step 4 Click the **Fabric/Network** icon to view the Fabric/Network path.

Step 5 Click the **All Paths** icon to view the complete set-up.

Step 6 Click the **First Shortest Path** icon to view the shortest path.

Note Click **Map View** icon to enable the icons listed in Step 4, 5 and 6 above.

Step 7 Click the **Tabular View** icon to view the host topology in tabular format.

Viewing Storage Enclosure Traffic

Step 1 From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.

You see the list of storage enclosures in the table

Step 2 Click the **Show details** icon next to the storage enclosure to view the topology details.

Step 3 Use the drop-down to select the traffic according to the time duration.

Step 4 Select the icons to view the traffic as a **Grid**, **Line Chart** or **Stacked Chart**.

Step 5 Click the **Show Events** icon to view the events.

Step 6 Use the options at the bottom of the screen to view a pie chart or a line chart. Click on each name on the chart to view its details.

Viewing Storage Systems

Step 1 From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.

Note The datasource must be configured and discovered at least once to display the discovered storage system(s). For more information see Adding, editing, removing, rediscovering and refreshing SMI-S Storage.

Step 2 Select **Click to see more details...**icon to view the storage systems summary.

Step 3 Use the drop-down to select the Storage System. Only EMC and NetApp vendors are supported.

The default view consists of the storage system summary along with counts of it's elements and graph indicating the total aggregate space used vs. free space.Click each name in the graph to go to the item in the left menu.

Step 4 The storage systems elements and their views are as follows:

- Components, page 3-19
- Pools, page 3-19
- LUNs, page 3-20
- Filer Volumes, page 3-20
- Hosts, page 3-21
- Storage Processors, page 3-21
- Storage Ports, page 3-21

Components

Components are containers for a set or sub-set of the disks in a storage system.The Component elements view displays a table of the disks in the collection, total number of disks managed and a summary of the collection's used vs. raw space.

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 The right-hand pane displays a summary of the storage components. Click each name to go to the item in the left menu

Step 3 Hover the mouse cursor on the graph to display its details.

Step 4 In the left-hand pane, select the storage component to view its details.

The number of disks managed along with its details are displayed.

Step 5 Click a **Serial Number** to display the disk and the mapped LUNs details.

Step 6 You can use the search box to search for a specific component.

Pools

Pools are user-defined collections of LUNs displaying the pool storage. The pools elements view displays a summary of the pools, lists the LUNs in the pool and also displays the total managed and raw space.

Step 1 Use the Storage System drop-down to select the storage system.

The bar graph next to each pool indicates the total managed space of that pool.

Step 2 In the left-hand pane, select a pool to display:

- Status of the pool
- LUN's in the pool displaying the total raw space and the total managed space.
- Raid Type
- Disk Type
- Details of the LUNs in the pool

Step 3 You can use the search box to search for a specific pool.

LUNs

LUNs refer to a storage volume or a collection of volumes abstracted into a single volume. It is a unit of storage which can be pooled for access protection and management. Each LUN in the LUN Element View is displayed along with the mapping from Hosts to LUNs. If the associated Fabric has also been discovered, additional information concerning the end-to-end connection between a host and LUN is also displayed.

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select a LUN to display:

- The LUN details along with its status and the number of Associated Hosts.
- The Host LUN Mapping details along with the Access (Granted) information.

If the associated Fabric has also been discovered, additional information about the switch interfaces and zoning concerning the end-to-end connection between the Host and LUN is also displayed.

Note All fabrics that are discovered must be licensed or the fabric correlation will be disabled in the Web Client. When the feature is disabled, all correlation fields display "Unlicensed Fabric".

Step 3 You can use the search box to search for a specific LUN.

Filer Volumes

Filer Volumes are applicable only for NetApp. The Filer Volume Element view displays the Status, Containing Aggregate along with the total capacity and used space.

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select the filer to display:

- The status of the filer along with the containing aggregate name.
- Hover the mouse cursor over the graph to view the total capacity and available storage of the filer.

Step 3 You can use the search box to search for a specific Filer.

Hosts

The Hosts only describes the NWWN(s) associated with a host or host enclosure along with the associated Host LUN Mapping and the Host Ports. If the associated Fabric has also been discovered, additional information concerning the end-to-end connection between a host and LUN is also displayed.

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select a host to display:

- The NWWN (Node WWN) is the WWN of the device connected to the switch.
- The Host Ports along with the Host LUN Mapping.
- In the Host Ports section, click a Host Enclosure Name to view its Events, Topology and SAN Traffic. For more information see the Storage, page 3-17 section.
- In the Host Ports sections, click a Host Interface to view the Switch Dashboard, page 3-14.
- In the Host LUN Mapping section, click a Storage Interface to view the Switch Dashboard, page 3-14.
- In the Host LUN Mapping section, click a Storage Name to view its Events, Topology and SAN Traffic. For more information see the Storage, page 3-17 section.

If the associated Fabric has also been discovered, additional information about the switch interfaces and zoning concerning the end-to-end connection between the Host and LUN is also displayed.

Note All fabrics that are discovered must be licensed or the fabric correlation will be disabled in the Web Client. When the feature is disabled, all correlation fields display “Unlicensed Fabric”.

Step 3 You can use the search box to search for a specific host.

Storage Processors

Storage Processors are elements on a storage system, which enable some of its features. A storage processor includes the collection of Storage Ports it manages. In the Storage Processor Element View, the list of Storage Ports associated with a Storage Processor is displayed.

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select a storage processor to display:

- The status, adapter details and the number of ports of the storage processor.
- The storage ports details.

Step 3 You can use the search box to search for a specific storage processor.

Storage Ports

A storage port is a single port on the Storage System. It displays the summary information of each port selected.

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select a storage port to display its details.

Step 3 You can use the search box to search for a specific storage port.

Viewing Health Information

The Health menu shows events and issues for the selected items that are persistent across user sessions. The Health menu contains the following submenus:

- Accounting—Shows a list of accounting events.
- Events—Shows a detailed list of data center events. You can filter these events by scope, date, and type of event.
- Virtual Port Channels (LAN only)

This section includes the following topics:

Viewing Accounting Information

Step 1 From the menu bar, choose **Health > Accounting**.

The fabric name or the group name along with the accounting information is displayed.

Step 2 Select the **Filter** icon to search the accounting information by Source, User Name and Description. Use the Time drop-down to select the timeline for the search.

Note The Time drop-down appears only if you select the Filter icon.

Step 3 You can also select a row and use the **Delete** icon to delete accounting information from the list.

Step 4 You can use the **Print** icon to print the accounting details and use the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.

Viewing Events Information

You can view the events and syslog from Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Health > Events**.

The fabrics along with the switch name and the events details are displayed.

The Count column displays the number of times that the same event has occurred during the time period that is shown in the Last Seen column.

If you click a switch name displayed in the Switch column, Cisco Prime DCNM Web Client displays the switch dashboard.

If you click the IP address displayed in the Description column, the search feature displays all search results pertaining to that device. From here, you can choose the results that you wish to view.

Step 2 Select one or more events in the table and click the **Add Suppressor** icon to open the shortcut of adding an event suppressor rule. For detailed information about adding event suppressor rules, please refer to Add Event Suppression Rules.

Step 3 Select a fabric and click the **Acknowledge** icon to acknowledge the event information for the fabric. Once you have acknowledged the event for a fabric, the acknowledge icon is displayed in the Ack column next to the fabric.

Step 4 You can cancel an acknowledgment for a fabric by selecting the fabric and clicking the **Unacknowledge** icon.

Step 5 You can use the **Filter** icon to enable filters for the columns displayed.

Step 6 Select a fabric and use the **Delete** icon to delete the fabric and it's event information from the list.

Step 7 You can use the **Print** icon to print the event details and use the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.

SAN Host Redundancy

The SAN Host Redundancy check enables you to view the non-redundant host storage paths. It helps you identify the host enclosure errors along with the resolution to fix the errors.

Note All fabrics that are discovered must be licensed or this feature will be disabled in the Cisco Prime DCNM Web Client. When the feature is disabled, a notification is displayed stating unlicensed fabrics are discovered.

From the menu bar, choose **Health > Diagnostics > SAN Host Redundancy**.

The following tabs are displayed:

- SAN Path Errors – Displays the summary section of the errors along with a table of errors.
- Settings – Displays the optional checks you can run along with the exclusion lists.

SAN Path Errors

Step 1 From the menu bar, choose **Health > Diagnostics > SAN Host Redundancy > SAN Path Errors** tab.

Step 2 Use the Error Types checkboxes to filter the types of host redundancy errors from the table.

The **Good**, **Skipped** and **Errored** host enclosure counts are displayed. These are counts of the unique host enclosures as a whole and not path counts.

The Error Types table provides individual path error counts of host enclosures seeing an error. The Host Enclosure column displays the hosts that contain the errors. These are counts of each path in the host enclosures seeing an error. Click a host to view the Compute details.

The Storage Enclosure/Storage Port column displays the connected storage that is involved the errors.

Step 3 Click a storage to view the Storage details.

Step 4 In the Fix? column, hover the mouse cursor on the **?** icon to view a solution to fix the error.

Step 5 Click **Re-run Check Now** to run the check at anytime.

Step 6 Click **Clear All** to clear all the errors displayed.

Step 7 Click **Ignore Hosts** to add the selected row(s) host enclosure to an exclusion list. The errors from that host will no longer be reported and the current errors will be purged from the database.

Step 8 Click **Ignore Storage** to add the selected row(s) storage enclosure to an exclusion list. The storage name is an hyperlink to the storage page. Select a row to delete the storage from the ignored list.

Step 9 Click **Ignore Host-Storage Pair** to add the selected row(s) host-storage pair enclosure to an exclusion list. The host name is an hyperlink to the compute page and the storage name is an hyperlink to the storage page. Select a row to delete the storage pair from the ignored list

Note If you click on **Ignore Hosts**, **Ignore Storage** or **Ignore Storage Pair** before you select a row, an error message appears.

Step 10 Click the **Print** icon to print the summary section and the errors as tables.

Step 11 Click the **Export to Excel** icon to export the summary section and the errors as tables to a Microsoft excel spreadsheet.

The **Dashboard > Summary > Health** will display counts for Path not redundant and Missing Paths which will be hyperlinks to SAN Path errors section.

Settings

Step 1 From the menu bar, choose **Health > Diagnostics > SAN Host Redundancy**> **Settings**.

Step 2 Under the Test for pane, use the check boxes to select the host redundancy optional checks.

Step 3 Select the **Automatically Run Check Every 24 hours** checkbox to enable periodic running of the checker. The checker will run every 24 hours starting 10 minutes after the server starts.

Step 4 Select **Excluded VSAN** check box. Enter **VSAN** or **VSAN range** in the text field to skip the host enclosures that belong to VSAN(s) from the redundancy check.

a. The Ignored Hosts pane displays the list of host enclosures that have been skipped/ignored by the redundancy check along with the reason the host enclosure check was skipped. The following reasons may be displayed:
   - Skipped: Enclosure has only one HBA
   - Host was ignored by the user.
   - Host ports managed by more than one federated servers. Check can't be run.
   - Skipped: No path to storage found.

b. The Ignored Storage tab displays the list of storage enclosures that have been selected to be ignored during redundancy check.

c. The Ignored Host Storage Pairs tab displays the list of host-storage pairs that have been selected to be ignored during redundancy check.

Step 5 The column displays the The Click a host to view the Compute details.

Step 6 Select a host enclosure and click the **Delete** button to remove the host from the ignored list and begin receiving errors about a host you had chosen to ignore. However, you can delete entries with message "Host was ignored by user".

Slow Drain Analysis

The Slow Drain Analysis enables you to view slow drain statistics at the switch level and the port level. You can monitor the slow drain issue within any time frame. You can display the data in a chart format and export the data for analysis also.

The slow drain statistics are stored in the cache memory. Therefore, the statistics will be lost when the server is restarted or a new diagnostic request is placed.

Note The jobs run in the background, even after you log off.

To configure and view the slow drain statistics,

Step 1 From the menu bar, choose **Health > Diagnostics > Slow Drain Analysis**.

Step 2 In the **Scope** field, select the Fabric from the drop-down list.

Step 3 Use the radio button to select the desired **Interval** to collect data.

Step 4 Click the **Play** icon to begin polling.

The server begins to collect the slow drain statistics based on the scope defined by the user. The T**ime Remaining** is displayed in the right-side of the page.

Step 5 Click the **Stop** icon to stop polling.

The server maintains the counters in the cache, until a new diagnostic request is placed. You can stop the polling before the time is up.

Step 6 Click on the arrow next to **Current jobs** to display the slow drain details for the jobs running on the fabric. The **Fabric Name**, the **Status** of polling and **Details** icon for each fabric is displayed.

Step 7 Click on the **Detail** icon to view the saved information.

Step 8 Click on **Interface** chart icon to display the slow drain value for the switch port in chart format.

Step 9 Click on the **Filter** icon to display the details based on the defined value for each column.

Step 10 Select the **Data Rows Only** checkbox to filter and display the non-zero entries in the statistics.

Step 11 Click on the **Print** icon to Prints the slow drain details.

Step 12 Click on the **Export** icon to export the slow drain statistics to a Microsoft Excel spreadsheet.

Viewing a vPC

The virtual port channel (vPC) feature enables you to view the links that are physically connected to different devices as a single port channel. A vPC is an extended form of a port channel which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic. Traffic is distributed among two single device vPC end points. If there is an inconsistency in the vPC configurations, the vPC does not function correctly.

The Cisco Prime DCNM Web Client helps you to identify the inconsistent vPCs and resolve the inconsistencies in each vPC or in all vPCs.

This section contains the following:

- Viewing vPC Inconsistencies
- Resolving vPC Inconsistencies

From the menu bar, choose **Health > Virtual Port Channels (vPC)**.

Cisco Prime DCNM Web Client displays both the consistent and inconsistent vPCs.

Note The vPC inconsistency page displays inconsistencies only for the devices that have required Cisco Prime DCNM licenses installed on them. The devices that do not have Cisco Prime DCNM LAN license installed on them do not appear on this page.

Table 3-1 displays the following vPC configuration details in the data grid view.

Table 3-1 vPC Configuration Details

Column	Description
vPC ID	You can view all the multichassis vPC end points and corresponding peer switches for each vPC ID.
Domain ID	Domain ID of the vPC peer switches.
Multi-chassis vPC End Point - Device Name	Details of the corresponding to peer single chassis primary vPC end points.
Multi-chassis vPC End Point - Port Channel ID	Single port channel that is connected to two single chassis vPC end points.
Primary vPC Peer - Peer Port Channel	Details of the corresponding multichassis vPC end points.
Primary vPC Peer - Port Channel	Single port channel that is connected to two single chassis vPC end points.
Primary vPC Peer - Device Name	Hostname of the vPC peer switches.
Secondary vPC Peer - Peer Port Channel	Details that correspond to the peer single chassis secondary vPC end points.
Secondary vPC Peer -Port Channel	Secondary port channel that is connected to two single chassis vPC end points.
Secondary vPC Peer -Device Name	Secondary Hostname of the vPC peer switches.
Consistency - Global	Configuration consistency between vPC peer port channels and vPC port channels. The valid values are Consistent and Inconsistent.
Consistency - Global	Configuration consistency between vPC peer switches that form a peer link.
Consistency -vPC	Configuration consistency between vPC peer port channels.

Viewing vPC Inconsistencies

You can view vPC inconsistencies from the Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Health > Virtual Port Channels (vPC)**.

Step 2 Click a specific cell to view the global or vPC inconsistencies.

A popup window displays the inconsistencies between the parameters.

All the conflicts in the configuration for the vPC primary device and the secondary device are displayed in red.

Resolving vPC Inconsistencies

You can resolve vPC inconsistencies from the Cisco Prime DCNM Web Client.

Step 1 Click the **Resolve All Conflicts** button to resolve all vPC inconsistencies.

Step 2 Click the **Print** icon to print the page.

Step 3 Click the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.

Viewing Performance Information

The Performance option displays an overview of the average and peak throughput and link utilization of the SAN components. The Filter drop-down list at the top-right of the screen allows you to filter the data based on various time periods.

In a large scale environment, we recommend that you select only select only "Trunks" and not the "Access or Errors and Discards" option during Performance Collections operations. This will ensure optimal performance monitored and managed entities in DCNM and allow successful Performance collection.

All performance pages allows you to print the page and export to Excel, By default, the **Export To Excel** icon is the export traffic number in raw digit format. You can export the same unit number for the traffic data, such as GB/Gb/MB/Mb/KB/Kb/B/b, For example; If you want to display the traffic numbers in GB, you need to modify the **server.properties** fileto set **export.unitless**=false and **export.unit=GB**.

If you set **export.unitless=false**, and do not enter a value for the **export.unit**, it will display the default Web Client unit value.

Note You do not have to restart the DCNM server.

The Performance menu contains the following submenus:

- Switch—Shows the CPU, memory and traffic information.
- End Devices—Shows a detailed list of end devices (host or storage), port traffic and errors.
- ISLs—Shows a detailed list of ISL traffic and errors.
- NPV Links— Shows a detailed list of traffic between NPV devices and ports.
- Flows—Shows a detailed list of host-to-storage traffic.
- Ethernet—Shows a detailed list of Ethernet interfaces.
- Others—Shows a detailed list of other statistics.
- Virtual Port Channels—Shows a list of vPC utilization.

- N3K Buffer Usage - Displays performance of the N3K buffer usage and the total number of bursts during a specific time.

Rx/Tx Calculation

- Average Rx/Tx % = Average Rx/Tx divided by Speed * 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed * 100

Note The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

Viewing Switch CPU Information

Step 1 From the menu bar, choose **Performance > Switch > CPU**.

You see the CPU pane. This pane displays the CPU information for the switches in that scope.

Step 2 You can use the drop-down to filter the view by 24 Hours, Week, Month and Year.

Step 3 In the Switch column, click the switch name to view the Switch Dashboard.

Step 4 Click the chart icon in the Switch column to view the CPU utilization. You can also change the chart timeline to 24 hours, Week, Month and Year.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Switch Memory Information

Step 1 From the menu bar, choose **Performance > Switch > Memory**.

You see the memory panel. This panel displays the memory information for the switches in that scope

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 Click the chart icon in the Name column to see a graph of the memory usage of the switch.

Step 4 In the Switch column, click the switch name to view the Switch Dashboard.

Step 5 You can use the drop-down to view the chart in different time lines. Use the chart icons to view the traffic chart in varied views.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Switch Traffic and Errors Information

Step 1 .From the menu bar, choose **Performance > Switch > Traffic**.

You see the Switch Traffic and Errors panel. This panel displays the traffic on that device for the past 24 hours.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**

Step 4 Click the switch name to view the Switch Dashboard.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing ISL Traffic and Errors Information

Step 1 From the menu bar, choose **Performance > ISLs/Trunks**.

You see the ISL Traffic and Errors pane. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Notation NaN (Not a Number) in the data grid means that the data is not available.

There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views.You can also use the icons to Append, Predict and Interpolate Data. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- For the Rx/Tx calculation, see the Rx/Tx Calculation, page 3-28 section.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance.

Viewing Performance Information for Ethernet Ports

Step 1 From the menu bar, choose **Performance > Ethernet**.

You see the Ethernet Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Select the time range, and click **Filter** to filter the display.
- Select the name of an Ethernet port from the Name column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner. To view real-time information, choose **Real Time** from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**
- Use the chart icons to view the traffic chart in varied views.You can also use the icons to Append, Predict and Interpolate Data.
- For the Rx/Tx calculation, see the Rx/Tx Calculation, page 3-28 section.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Other Statistics

Step 1 From the menu bar, choose **Performance > Others**.

You see the Others window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

There are variations to this procedure. In addition to these basic steps, you can also do the following:

- Select the time range, and click **Filter** to filter the display.
- Click the chart icon in the Switch column to see a graph of the performance for this user defined object. You can change the time range for this graph by selecting it from the drop-down list in the upper right corner.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**
- Use the chart icons to view the traffic chart in varied views.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information for NPV Links

Step 1 From the menu bar, choose **Performance > NPV Links**

You see the NPV Link and Traffic Errors window. This window displays the NPV links for the selected scope.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 Click the chart icon in the Name column to see a list of the traffic for the past 24 hours.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for NPV links:

- You can change the time range for this information by selecting from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information on All Ports

You can view the performance of devices connected to all ports.

Step 1 From the menu bar, choose **Performance > End Devices > All Ports.**

You see the All Ports Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 4 Click the chart icon in the Name column to see:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds.You can also use the icons to Append, Predict and Interpolate Data.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information on Host Ports

You can view the performance of devices connected to the host ports

Step 1 From the menu bar, choose **Performance > End Devices > Host Ports**.

You see the Host Ports Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**

Step 4 Click the chart icon in the Name column to see

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds. You can also use the icons to Append, Predict and Interpolate Data.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection

Viewing Performance Information on Storage Ports

You can view the performance of devices connected to the storage ports.

Step 1 From the menu bar, choose **Performance > End Devices > Storage Ports**.

You see the Storage Ports Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 4 Click the chart icon in the Name column to see:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds.You can also use the icons to Append, Predict and Interpolate Data.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information on Host Enclosure

You can view the performance of devices connected to the host enclosure.

Step 1 From the menu bar, choose **Performance > End Devices > Host Enclosure**.

You see the Host Enclosures Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 4 Click the chart icon in the Name column to see:

- A graph of the traffic on that device according to the selected timeline.

- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to Append, Predict and Interpolate Data.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information on Storage Enclosure

You can view the performance of devices connected to the storage enclosure.

Step 1 .From the menu bar, choose **Performance > End Devices > Storage Enclosure**.

You see the Storage Enclosures Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 4 Click the chart icon in the Name column to see:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to Append, Predict and Interpolate Data.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information on Port Groups

You can view the performance of devices connected to the port groups.

Step 1 From the menu bar, choose **Performance > End Devices > Port Groups.**

You see the Port Groups Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 Click the name port group to see the members of that port group.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for the port groups:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to Append, Predict and Interpolate Data.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information for FC Flows

You can view the performance of the FC Flow traffic.

Note Restart the Performance Manager in the Cisco Prime DCNM Web Client when you add or remove an FC FLOW from the switch configuration, for it to reflect under the **Performance > FC Flows**.

Step 1 From the menu bar, choose **Performance > FC Flows**.

You see the Flow Traffic window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 4 Click the chart icon in the Name column to see:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner.
- You can also use the icons to Append, Predict and Interpolate Data.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Performance Information for Virtual Port Channels

You can view the relationship among virtual port channels (vPCs). You can view the statistics of all member interfaces and the aggregate of the statistics at the port channel level.

Step 1 From the menu bar, choose **Performance > Virtual Port Channels (vPC).**

The vPC performance statistics appears and the aggregated statistics of all vPCs are displayed in a tabular manner.

Step 2 Click on a device name in the Primary vPC peer or Secondary vPC peer column to view its member interface.

A popup window displays the member interfaces of the selected device.

Step 3 Click the Chart icon of the corresponding interface to view its historical statistics.

The traffic distribution statistics appear at the bottom of the vPC window. By default, the Cisco Prime DCNM Web Client displays the historical statistics for 24 hours.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for flows:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to Append, Predict and Interpolate Data.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

N3K Buffer Usage

You can view the performance of the N3K buffer usage and the total number of bursts during a specific time.

Step 1 From the menu bar, choose **Performance > N3K Buffer Usage**

You see the N3K Buffer Usage window which displays the average number of burst per hour, maximum number of burst per hour and the total number of burst per hour.

Step 2 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 3 Click the chart icon in the Name column to see:

- A bar chart of the hourly based burst number for the selected interface.
- Clicking each item in the bar chart will open a detailed buffer burst window for the selected hour.

Note If the performance tables do not contain any data, see the Performance Manager Collections section to turn on performance data collection.

Viewing Inventory Information

Beginning with Cisco Prime DCNM release 6.x, you can view the inventory and the performance for both SAN and LAN switches by using the global Scope pane. You can select LAN, SAN, or both to view the inventory information. You can also export and print the inventory information.

You can either Print this information or export to Microsoft Excel.

The Inventory menu includes the following submenus:

- Switches—Displays details about switches.
- Modules—Displays details for MDS switching and services modules, fans and power supplies.
- ISLs/Trunks—Displays the Inter-Switch Links.
- Licenses—Displays details about the licenses in use in the fabric.
- NPV Links—Displays the links between NPV devices and ports.

- VSANs—Displays details about VSANs.
- Active Zones— Displays details about the Regular and IVR zones.
- FC End Devices—Displays details about the devices connected to the various ports.
- .Port Mapper—Displays the port mapper information.
- VxLAN—Displays the VxLAN configured for the switch.

Note You can use the **Print** icon to print the information displayed or you can also use the **Export to Excel** icon to export the information displayed to a Microsoft Excel spreadsheet.

Viewing Inventory Information for Switches

Step 1 From the menu bar, choose **Inventory > Switches**.

You see the Switches window displaying a list of all the switches for a selected Scope.

Step 2 You can also view the following information.

- In the Name column, select a switch to display the Switch Dashboard. For more information about switch dashboard, see the Switch Dashboard section.
- Use the drop-down to view **All, Warning** or **Unmanaged** switches.

Step 3 In the Health column, the switch health is calculated by the capacity manager based on the following formula in the **server.properties** file.

The function to implement is

```
#           calculate(x, x1, y, y1, z)
#                   @param x: Total number of modules
#                   @param x1: Total number of modules in warning
#                   @param y: Total number of switch ports
#                   @param y1: Total number of switch ports in warning
#           @param z: Total number of events with severity of warning or above
```

Step 4 The value in the Health column is calculated based on the following default equation.

((x-x1)*1.0/x) *0.4 + ((y-y1)*1.0/y)*0.3 + ((z*1.0/1000>=1) ? 0: ((1000-z)*1.0/1000)*0.3).

In the above formula, the switch health value is calculated based on the following:

- Percentage of Warning Modules (Contributes 40% of the total health).
- Percentage of Warning Ports (Contributes 30% of the total health)
- Percentage of events with severity of Warning or above (Contributes 30% of the total health. If there are more than 1000 warning events, the event health value is 0).

You may also have your own health calculation formula by implementing the common interface class**:com.cisco.dcbu.sm.common.rif.HealthCalculatorRif**. Add the.jar file to the DCNM server and modify the **health.calculator** property to point to the class name you have created.

The default Java class is defined as:**health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculator.**

- Capacity Manager calculates health only for the license switches. If the health column does not display a value, the switch either does not have a license or it has missed the capacity manager's daily cycle.
- If the switch is unlicensed, in the DCNM License column click **Unlicensed**. The **Admin>License** window appears which allows you to assign a license to the user.
- The capacity manager runs two hours after the DCNM server starts. So, if you discover a device after two hours of the DCNM start time, the health will be calculated 24 hours after this DCNM start time

Viewing Inventory Information for Modules

Step 1 From the menu bar, choose **Inventory > Modules**.

You see the Modules window displaying a list of all the switches and its details for a selected Scope.

You can also view the following information:

Step 2 In the Name column, select a switch to display the Switch Dashboard. For more information about switch dashboard, see the Switch Dashboard section.

Step 3 Use the drop-down to view **All**, **Warning** or **Unmanaged** switches

Viewing Inventory Information for ISLs/Trunks

Step 1 From the menu bar, choose **Inventory** > **ISLs/Trunks**.

You see the ISLs window displaying the ISL details along with the speed and status of the ISLs.

Step 2 Use the drop-down to view **All** or **Warning** information for the ISLs.

Viewing Inventory Information for Licenses

Step 1 From the menu bar, choose **Inventory** > **Licenses.**

You see the Licenses window displaying the license type and the warnings. based on the selected Scope.

Step 2 In the Name column, select a switch to display the Switch Dashboard. For more information about switch dashboard, see the Switch Dashboard section.

Step 3 Use the drop-down to view **All**, **Warning** or **Unmanaged** switches.

Viewing Inventory Information for NPV Links

Step 1 From the menu bar, choose **Inventory** > **NPV Links**

You see the NPV Links window displaying the NPV details along with the speed and status of the NPV links.

Step 2 Use the drop-down to view **All, Warning** or **Unmanaged** switches.

Viewing Inventory Information for VSANs

Step 1 From the menu bar, choose **Inventory > VSANs**.

You see the VSAN window displaying the VSAN details along with the status and Activate Zoneset details.

Step 2 Use the drop-down to view **All** or **Warning** information for the VSANs.

Viewing Inventory Information for Regular Zones

Step 1 From the menu bar, choose **Inventory > Active Zones > Regular Zones**.

You see the Regular Zones window displaying the inventory details of the fabrics in the regular zone.

Step 2 Click the **Show Filter** icon to enable filtering by VSAN or Zone.

Viewing Inventory Information for IVR Zones

Step 1 From the menu bar, choose **Inventory > Active Zones > IVR Zones**

You see the IVR Zones window displaying the inventory details of the fabrics in the IVR zone.

Step 2 Click the **Show Filter** icon to enable filtering by Zone.

Viewing Inventory Information for All Ports on FC End Devices

Step 1 From the menu bar, choose **Inventory > End Devices > All Ports.**

You see the End Devices window displaying details of the FC End Devices on the all the ports.

Step 2 Use the drop-down to view **All** or **Warning** information for the FC End devices.

Step 3 Click the **Show Filter** icon to enable filtering by Enclosure, Name or VSAN.

Viewing Inventory Information for Host Ports on FC End Devices

Step 1 From the menu bar, choose **Inventory > End Devices > Host Ports**.

You see the **End Devices>Host Ports** window displaying details of the FC End Devices on the host ports.

Step 2 Use the drop-down to view **All** or **Warning** information for the FC End devices on host ports.

Step 3 Click the **Show Filter** icon to enable filtering by Enclosure, Name or VSAN.

Viewing Inventory Information for Storage Ports on FC End Devices

Step 1 From the menu bar, choose **Inventory > End Devices > Storage Ports**.

You see the **End Devices>Storage Ports** window displaying details of the FC End devices on the storage ports

Step 2 Use the drop-down to view **All** or **Warning** information for the FC End devices on storage ports.

Step 3 Click the **Show Filter** icon to enable filtering by Enclosure, Name or VSAN.

Viewing Inventory Information for Port Mapper

Beginning with Cisco NX-OS Release 6.x, you can view information about all the logical and physical ethernet interfaces of all the devices that are discovered by the Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Inventory > Port Mapper**.

You see the Port Mapper window displaying the details listed in Table 3-2

Table 3-2 Port Mapper Inventory

Column	Description
Device	Name of the device to which the interface belongs.
Interface Name	Name of the interface.
Description	Description of the interface.
Mode	Mode of the interface.
Admin Status	Admin status of the port.
Operational status	Operational status for the port.
Speed	Speed for the interface. It is not the configured speed.
Duplex	Single port channel that is connected to two single chassis vPC end points.
STP Protocol	Spanning Tree Protocol (STP) whether or not the Per-VLAN Spanning Tree (PVST), Multiple Spanning Tree (MST), and rapid-PVST is configured.
Access/Allowed VLANs	Access VLAN is displayed if the port mode is access or displays allowed VLAN if the port mode is trunk.
Built-in MAC Address	MAC address for the port.
IP Address/Mask	IP address configured on the port and the IP mask.
SFP Serial Number	Serial number of the Small Form-Factor Pluggable (SFP) if it is attached on the port

Step 2 Click the **Show Filter** icon to filter the port mapping information.

The filter options in the Device, Interface Name, Description, Access/Allowed VLANs, Built-in MAC Address, IP Address/Mask, and SFP SerialNumber column allows you to enter text inputs in the respective field and search. In addition, you can use the drop-down list in the Mode, Admin Status, Operational Status, Speed, Duplex, and STP Protocol column to limit the objects that appear in the report.

Step 3 Click the **Print** icon to print the port mapping report of the selected device.

Step 4 Click the **Export to Excel** icon to export the port mapping report of the selected device to a Microsoft Excel spreadsheet.

Step 5 Click a cell in the STP Protocol column

A popup window displays the STP settings of the port.

Step 6 Click the **Show Filter** icon to filter the STP settings.

Viewing and Creating Custom Reports

The Reports menu allows you to create customized reports based on historical performance, events, and inventory information gathered by Cisco Prime DCNM. You can create aggregate reports with summary and detailed views. You can also view previously saved reports.

Note Beginning with Cisco Prime DCNM Release 6.x versions, reports can be generated for SAN and LAN. The global view Scope pane will contain SAN, LAN, and Default LAN configurations. You can select any of these configurations, and generate reports.

The Report menu includes the following sub-menus:

- View—Displays previously saved reports.
- Generate—Generates a custom report based on the selected report template.
- Create SAN User Defined—Allows you to generate a report based on a new custom template or select an existing template along with the Configuration of Scope, Inventory, Performance, Health and User Selection.
- Jobs—Displays scheduled jobs based on the selected report template.

This section includes the following topics:

Viewing Reports

You can view the saved reports based on the following selection options:

- By Template

- By User
- From the menu bar, select **Reports > View**.

You see the view reports window. displaying the **View Reports By tree** on the left pane.

Step 1 In the left pane, expand **By Template** or **By User** folder.

Step 2 Select the report you wish to view. You can view the report in the main screen or you can select the report in the Report column to view the HTML version of the report in a new browser.

Step 3 To delete a specific report, select the check box and click the **Delete Report** icon.

Step 4 To delete all reports, check the check box in the header, and click the **Delete Report** icon.

Note If you have multiple fabrics, you can select the DCNM-SAN group in the Scope to view Host to Storage connectivity of multiple fabrics in a single report.

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
- A detailed information for the device of the module. The table contains details about the tests failed.

Generating a Report

You can generate reports based on a selected template or you can schedule the report to run at a specified time.

Step 1 In the configuration window, use the drop-down to define the scope for report generation.

In the Scope drop-down, you can select a scope group with dual fabrics, the traffic data generated by hosts and storage end devices are displayed side-by-side which enables you to view and compare traffic data generated on dual fabrics. To View this report, in the Other Predefined folder, select **Traffic by VSAN (Dual Fabrics)**. Click **Options** to select the Device Type and Fabrics. Click **Save** to save the configuration.

Step 2 From the menu bar, select **Reports > Generate**.

You see the Generate Report window.

Step 3 In the Generate a Report Using pane, expand the folders and select the report.

In the Other Pre-defined folder, you can use the drop-down to select either **All Devices** or **Host Devices** while generating a report.

Step 4 (Optional) In the Report Options pane, you can edit the **Report Name**.

Step 5 (Optional) Check the **Report is only visible to the Owner** check box to change the attribute of the report. If selected, the report can be viewed only by the specific user and network administrator.

Step 6 .(Optional) Check the **Export to Csv/Excel** check box to export the report in to a Microsoft Excel spreadsheet.

Step 7 In the **Repeat** radio buttons, if you select:

- **Never** - The report is generated only during the current session.
- **Once** - The report is generated on a specified date and time apart from the current session.
- **Daily** -The report is generated everyday based on the Start and End date at a specified time.
- **Weekly** - The report is generated once a week based on the Start and End date at a specified time.
- .**Monthly** - The report is generated once every month based on the Start and End date at a specified time.

Step 8 (Optional) In the **Email Report** radio buttons, if you select:

- **No** - You will not receive an e-mail notification.
- **Link Only** - You will receive only a link to the report in the e-mail notification. You can specify the e-mail address of the recipient along with a desired subject.
- **Contents** - You will receive the report contents in the e-mail notification. You can specify the e-mail address of the recipient along with a desired subject.

Step 9 Click the **Create button** to generate a report based on the specifications.

You see the report results in a new browser window.

Alternatively, you can view the report by choosing **Report > View** and selecting the report name from the report template that you used in the navigation pane

Note The Start Date must be at least five minutes earlier than the End Date.

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
- A detailed information for the device of the module. The table contains details about the tests failed.

Creating SAN User Defined Reports

You can create custom reports from all or any subset of information obtained by Cisco Prime DCNM-SAN. You create a report template by selecting events, performance, and inventory statistics you want in your report and set the desired SAN, fabrics or VSAN to limit the scope of the template. You can generate and schedule a report of your fabric based on this template immediately or at a later time. DCNM Web Client saves each report based on the report template used and the time you generate the report.

Since the Cisco MDS NX-OS Release 5.0, the report template design has changed to resolve the limitations of the earlier versions. With the new design model, you can perform add, delete, and modify functionalities on a single page. You can choose multiple fabrics and VSANs using the new navigation system, which allows you to add new items and categories in the future.

The new design model has three panels:

- Templates panel - The Customs panel allows you to add new templates, modify existing templates and delete existing templates.

- Configuration panel - The Configuration panel allows you to configure a new template when it is added and modify an existing template. The options in the configuration panel are disabled until you either add a new template or select an existing template. The upper portion of the configuration panel contains many categories that you can choose and configure.
- User Selection panel - The User Selection panel displays your configuration options in real-time. While the configuration panel can display information pertaining to one category at a time, the User Selection panel displays all of your selections or configurations.

Follow the steps to create custom reports

Step 1 From the menu bar, choose **Report > Create SAN User Defined**

You see the Create SAN User Defined window.

Step 2 In the Templates panel, under the Name column, select **CLICK TO ADD NEW CUSTOM** to edit the Name of the new report.

In the Configuration Panel:

Step 3 Click **Scope** to define scope of the report. The default scope will have Data Center, SAN, LAN, and Fabric configurations.

Step 4 Click **Inventory** and use the checkbox to select the inventory information required in the report. You can also use the drop-down to filter by selecting the Top performance and the timeline required in the report.

Step 5 Click **Performance** and use the checkbox to select the performance information required in the report.

Step 6 Click **Health** and use the checkbox to select the health information required in the report.

Step 7 Click **Save** to save this report template.

A confirmation message is displayed confirming that the report is saved

This section also contains:

- Deleting a Report Template
- Modifying a Custom Report Template

Deleting a Report Template

Step 1 In the Template panel, select the report template that you want to delete.

Step 2 Click the **Trash** icon to delete the report.

Step 3 In the confirmation pop-up, click **Yes** to delete the template.

Modifying a Custom Report Template

Step 1 From the menu bar, choose **Reports > Create SAN User Defined**.

You see the Template, Configuration and User Selection panels.

Step 2 Select a report from the Templates panel.

You see the current information about this report in the User Selection panel.

Step 3 Modify the information in the Configuration panel.

Step 4 Click **Save** to save the report template.

A confirmation message is displayed confirming that the report is saved.

Note You cannot change the scope for an existing report. You must generate a new report for a new scope.

Viewing Scheduled Jobs Based on a Report Template

Step 1 From the menu bar, choose **Reports > Jobs**.

You see the Jobs window displaying details of the reports scheduled for generation along with its status.

Step 2 Select the checkbox for a specific report and click **Edit Job** icon to edit the report generation settings.

Step 3 Select the checkbox for a specific report and click the **Delete Job** icon to delete a report.

Configuring Cisco Prime DCNM Web Client

Using Cisco Prime DCNM Web Client, you can periodically start and backup the running configurations of a switch. You can also view backed-up configurations, schedule configuration backups, compare two backed-up configurations and copy a backed-up configuration.

Note You must configure a backup server with Admin/SFTP credentials to create a new backup job.

Beginning with Cisco Prime DCNM Release 6.x, the backup for the LAN configuration are also supported and the backup is skipped for the all the switches where there are no configuration changes.

This section includes the following topics:

Viewing a Configuration

Step 1 From the menu bar, choose **Config >View**.

You see the Groups, Eligible Switches and their configuration information.

Step 2 Select a fabric from the Groups list.

The Groups pane displays the global view with SAN, LAN, and Default LAN groups. Depending upon the value selected in the Groups pane, the eligible switches and their configurations are listed.

Step 3 From the **Eligible Switch(es)** list, select a switch.

Step 4 From the **Configuration file** list, select a configuration filename.

Step 5 Click **View** to view the configuration file.

Step 6 Click **Delete** to delete the configuration file.

Step 7 Click **Copy Local File to DB...** to upload the configuration from the local machine to the database.

Step 8 Select the **Show All** checkbox to display all the configurations present, irrespective of the options selected in the global Scope pane

Comparing Configurations

Step 1 From the menu bar, select **Config>Compare**.

You see the compare configuration information with the **Compare** and **Differences** tabs.

Step 2 .From the **Groups lis**t, select a fabric.

Step 3 .From the **Eligible Switch(es)** list, select a switch.

Step 4 (Optional) Click the **Archive, Running**, or **Startup** radio button.

Step 5 Click **Compare.**

Step 6 Click the **Differences** tab to view differences in configuration based on the specified legend.

Step 7 Select the difference line and click the bookmark button to **bookmark/toggle** bookmark.

Step 8 Use the **Next/Previous**, **Next book mark/Previous bookmark** buttons to navigate over the differences blocks.

Step 9 Click on the **colored overview** to strip to navigate to the difference

Step 10 Select the **Show All** checkbox to display all the configurations present, irrespective of the options selected in the global Scope pane.

Copying a Configuration

Step 1 From the menu bar, select **Config > Copy**.

You see the Groups, Eligible Switches and their configuration information.

Step 2 From the **Groups List**, select a fabric.

Step 3 From the **Eligible Switch(es)** list, select a switch.

Step 4 From the **Configuration file** list, select a configuration file name.

Step 5 Click **Copy** to copy the configuration file.

Step 6 Select the **Show All** checkbox to display all the configurations present, irrespective of the options selected in the global Scope pane.

Configuring Jobs

You must set the SFTP/TFTP credentials before you configure Jobs. On the DCNM Web Client, navigate to **Admin > SFTP/TFTP Credentials** to set configure.

Step 1 From the menu bar, choose **Config > Jobs.**

You see the scheduled jobs information along with its status.

Step 2 From the Scope selector. select a single fabric or a single LAN group.

Note You can create jobs for a single fabric or a single LAN group.

Step 3 Click **Create Job** icon to create a new config archive job.

A backup will be scheduled as defined.

Step 4 Specify the **Repeat** information, **Start** and **End** date, **Time** and **Comment**.

Note Cisco Prime DCNM will not archive the configuration of a switch, if it is not modified after the completion of the previous archive job.

Step 5 Select a job and click **Delete** Job to delete a specific job.

Click on the **Status** column to view the job execution details for that particular job.

Step 6 View Job execution details in the **Job Status History** tab.

You can also configure the Cisco Prime DCNM to retain the backup and restore configuration file for a defined time period and the number of job status entries per device. Navigate to **Admin > general > Server properties** on the Cisco Prime DCNM Web Client, and update the **configFile.Days2Keep** and **config.JobStatusPerDevice** fields.

Job Status History

From the menu bar, select **Config > Jobs > Job Status History**. This feature allows you to view details about the jobs archived on the Cisco Prime DCNM.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Table 3-1

Field	Description
Show Filter	Filters list of switches based on the defined value for each column.
Job Name	Displays the system-generated job name.
User	Specifies the persona of the person who created the job.
Group	Specifies fabric or the LAN group under which the job was created.
Device	Specifies the IP Address of the Device.
Server	Specifies the IP Address of the DCNM Server to which the device is associated with.
Execution time	Specifies the time at which the job was last executed.
Status	Specifies the status of the job.
Description	Specifies the description of the status.

Storage Media Encryption

Encrypting storage media in the data center has become a critical issue. Numerous high profile incidents of lost or stolen tape and disk devices have underscored the risk and exposure companies face when sensitive information falls into the wrong hands. To satisfy the most demanding requirements, Cisco MDS 9000 Family Storage Media Encryption (SME) for the Cisco MDS 9000 family switches offers a highly scalable, reliable, and flexible solution that integrates encryption transparently as a fabric service for Fibre Channel SANs.

This section contains the following:

Selecting the Key Manager and SSL Settings

Step 1 From the menu bar, select **Config>Provision**.

The Key Manager Settings window is displayed with the following options:

- **None**-No Key Manager selected for SME.
- **Cisco**-Cisco Key Manager selected for SME.
- **RSA**-RSA Key Manager selected for SME

Note Once you have selected a Key Manager, you will not be able to change it.

Step 2 Select one of the Radio buttons and click **Submit Settings.**

The Key Manager Settings window is displayed.

The KMC SSL Settings pane displays the location where the certificate is stored.

Step 3 If you want to edit the SSL Settings, click **Edit SSL Settings**.

Step 4 Use the drop-down to select the **SME KMC Trust Certificate**.

Step 5 Use the drop-down to select the **SME KMC Server Certificate**.

Step 6 Specify and confirm the **Server Cert Password**.

Step 7 Click **Submit SSL Settings**.

Step 8 In the High Availability Settings pane, click **Edit HA Settings** to specify the **KMC Role of this Server and SME Secondary Server Address.**

Step 9 Click **Submit HA Settings** to confirm.

Viewing SME Clusters

Step 1 From the menu bar, select **Config>Provision** and select **SME** from the ribbon.

You see the SME: Clusters window displaying the **Cluster Name, Status, Fabrics** and **Key Management Server.**

Step 2 Click the cluster in the Name column to view its details.

Step 3 In the Type option, click **Convert to Signature Mode...** to convert the cluster type to Disk Signature.

Note Once you have chosen to convert the cluster type, you will not be able to change it again

Step 4 In the Confirm Action window, click **Next**.

Step 5 In the Convert Cluster window, click **Auto** to automatically convert the cluster type to Disk Signature.

Creating a Cluster

Step 1 From the menu bar, select **Config>Provision** and select **SME** from the ribbon.

Step 2 You see the SME: Clusters window displaying the **Cluster Name, Status, Fabrics** and **Key Management Server.**

Step 3 Select **Create** to create a new cluster

Step 4 Select the **Cluster Type**, specify a **Cluster Name** and click **Next**.

Step 5 Select the **Fabric(s)** and click **Next**.

Note You can select multiple fabrics by holding the Ctrl key on your keyboard and selecting the fabrics.

Step 6 Select the **SME Interfaces** from the list and click **Next**.

Step 7 Select the **Security Type** for the cluster and click **Next.**

Step 8 Specify the **Primary Key Management Server** and the **Secondary Key Management Server** of the cluster. Alternatively, you can also use the drop-down to select the Key Management Servers for the cluster and click **Next**.

Step 9 Specify the **Transport Settings** for the cluster.

Step 10 Click **Confirm** to confirm the new cluster setup

Configuring Templates

Cisco Prime DCNM allows you to add, edit or delete user-defined templates configured across different Cisco Nexus and Cisco MDS platforms. The following parameters are displayed for each template configured on the Web Client of the Cisco Prime DCNM **Config > Templates**. Config template uses the Java runtime provided Java script environment to perform arithmetic operations, string manipulations in the template syntax.

Field	Description
Name	Displays the name of the configured template.
Description	Displays the description provided while configuring templates.
Platforms	Displays the supported Cisco Nexus platforms compatible with the template.
Tags	Displays the tag assigned for the template and aids to filter templates based on the tags.
Template Type	Displays the type of the template.
Published	Specifies if the template is published or not.
Modified Time	Displays the date and time when the template was last modified, in the format YYYY-MM-DD HH:MM:SS.

Additionally, from the menu bar, select **Config > Delivery > Templates** and you can also:

- Click the **Launch Job Creation** icon to configure and schedule jobs for individual templates. For more information, see Configuring Template Job, page 3-58.
- Click the **Show Filter** icon to filter the templates based on the headers.
- Click the **Print** icon to print the list of templates.
- Click the **Export to Excel** icon to export the list of template to a Microsoft Excel spreadsheet

This section contains the following:

Template Structure

The configuration template content mainly consists of four parts. You can click on the Help icon next to the Template Content window for information about editing the content of the template. Click on the Help icon next to the Template Content window for information about editing the content of the template.

This section contains the following:

- Template Format
- Template Variables
- Variable meta property
- Variable Annotation
- Templates Content
- Advanced Features

Template Format

This section describes the basic information of the template. The possible fields are as detailed in the table below.

Property Name	Description	Valid Values	Optional?
name	The name of the template	Text	No
description	Brief description about the template	Text	Yes
userDefined	Indicates whether the user created the template. Value is 'true' if user created.	"true" or "false"	Yes
supportedPlatforms	List of device platforms supports this config template. Specify 'All' to support all platforms.	"All" or combination of C6500, N1010, N1110, N1K, N3K, N4K, N7K, N6K, N5K, N5500, MDS, UCS list separated by comma.	No
configType	Specifies the Template used for	"CLI" or "POAP:	Yes
published	Used to Mark the template as read only and avoids changes to it.	"true" or "false"	Yes
timestamp	Shows the template modified time	Modified date and time in the format YYYY-MM-DD HH:MM:SS	Yes

```
Example: Template Properties
        ##template properties
        name =FCOE template;
        description = This file specifies the template configuration for FCOE;
        userDefined= false;
        supportedPlatforms = N7K, N6K, N5K, N5500, MDS;
        templateType = CLI;
        published = false;
```

```
        timestamp = 2013-05-16 07:11:37;
        ##
```

Template Variables

This section contains declared variables, the data type, default values, and valid values conditions for the parameters that are used in the template. These declared variables are used for value substitution in the template content section during the dynamic command generation process. Also these variables are used in decision making and in iteration blocks in the template content section. Variables have predefined data types. You can also add a description about the variable. The following table describes the syntax and usage for the available datatypes.

Variable Type	Valid Value	Iterative?
string	Free text `Example: Description for the variable`	No
boolean	true|false	No
enum	`Example: running-config, startup-config`	No
float	Floating number format	No
Integer	Any number	No
ipAddress	IPv4 OR IPv6 address	No
ipV4Address	IPv4 address	No
ipV6Address	IPv6 address	No
ipV4AddressWithSubnet	`Example: 192.168.1.1/24`	No
macAddress	14 or 17 character length MAC address format	No
interface	Format: <if type><slot>[/<sub slot>]/<port> `Example: eth1/1, fa10/1/2 etc.`	No
integerRange	Contiguous numbers separated by “-“ Discrete numbers separated by “,” `Example: 1-10,15,18,20`	Yes
floatRange	`Example: 10.1,50.01`	Yes
ipV4AddressRange	`Example: 172.22.31.97 - 172.22.31.99, 172.22.31.105 - 172.22.31.109`	Yes
interfaceRange	`Example: eth10/1/20-25, eth11/1-5`	Yes
string[]	`Example: {a,b,c,str1,str2}`	Yes
ipAddress[]	`Example:{192.168.1.1, 192.168.1.2, 10.1.1.1}`	Yes
wwn (Available only in the Web Client)	`Example: 20:01:00:08:02:11:05:03`	No

```
Example: Template Variables
        ##template variables
        integer VSAN_ID;
        string SLOT_NUMBER;
```

```
integerRange PORT_RANGE;
integer VFC_PREFIX;
##
```

Variable meta property

Each variable defined in the template variable section has a set of meta properties. The meta properties are mainly the validation rules defined for the variable.

The following table describes the various meta properties applicable for the available variable types.

Variable Type	Description	Variable meta property											
		defaultValue	validValues	decimalLength	min	max	minSlot	maxSlot	minPort	maxPort	minLength	maxLength	regularExpr
string	literal string	ü									ü	ü	ü
boolean	A boolean value. `Example: true`	ü											
enum			ü										
float	signed real number. `Example: 75.56, -8.5`	ü	ü	ü	ü	ü							
integer	signed number `Example: 50, -75`	ü	ü		ü	ü							
ipAddress	IP address in IPv4 or IPv6 format												
ipV4Address	IPv4 address												
ipV6Address	IPv6 address												
ipV4AddressWithSubnet													
macAddress	MAC address												
interface	specifies interface/port `Example: Ethernet 5/10`	ü	ü				ü	ü	ü	ü			
integerRange	Range of signed numbers `Example: 50-65`	ü	ü		ü	ü							
floatRange	range of signed real numbers `Example: 50.5 - 54.75`	ü	ü	ü	ü	ü							
ipV4AddressRange													
interfaceRange		ü	ü				ü	ü	ü	ü			

string[]	string literals separated by a comma (,) `Example: {string1, string2}`	✓											
ipAddress[]	List of IP addresses separated by a comma (,)	✓											
wwn	WWN address												
struct	set of parameters bundled under a single variable												

```
Example: Meta Property usage
        ##template variables

        integer VLAN_ID {
        min = 100;
        max= 200;
        };
        string USER_NAME {
        defaultValue = admin123;
        minLength = 5;
        };
        ##
```

Variable Annotation

You can configure the variable properties marking the variables using annotations.

Note Variable Annotations are available for POAP only. However, the annotations do not impact on the template type ‘CLI’.

The following annotations can be used in the template variable section.

Annotation Key	Valid Values
DisplayName	Text **Note** You must enclose the text with quotes, if there is space.
Description	Text
IsManagementIP	“True” or “False” **Note** This annotation must be marked only for variable “ipAddress”.
IsDeviceID	“True” or “False”
IsInternal	“True” or “False”
IsMandatory	“True” or “False”
UsePool	“True” or “False”
Username	Text

Annotation Key	Valid Values
Password	Text
DataDepend	Text

```
Example: Variable Annotation
        ##template variables
        @(DisplayName="Host Name", Description = "Description of the host")
        String hostname;
        @(DisplayName="Host Address", Description = " test description"
        IsManagementIP=true)
        ipAddress hostAddress;
        ##
```

Templates Content

This section includes the configuration commands and any parameters that you want to include in the template. These commands can include the variables declared in the template variables section. During the command generation process the variable values are substituted appropriately in the template content.

Note You must specify the commands that you include as if you were entering them in the global configuration command mode on any device. You must consider the command mode when you include commands.

Template content is governed by the usage of variables.

- Scalar variables—does not take a range or array of values which cannot be used for iteration (In the variable types table those marked iterate-able as 'No'). Scalar variables must be defined inside the template content.

  ```
  Syntax: $$<variable name>$$
  Example: $$USER_NAME$$
  ```

- Iterative variables—used for block iteration. These loop variable must be accessed as shown below inside the iteration block.

  ```
  Syntax:@<loop variable>
  Example:
  foreach val in $$INTEGER_RANGE_VALUE$$ {
  @val
  }
  ```

- Scalar Structure Variable—Structure member variables can be accessed inside the template content.

  ```
  Syntax: $$<structure instance name>.<member variable name>$$
  Example: $$myInterface.inf_name$$
  ```

- Array Structure Variable—Structure member variables can be accessed inside the template content

  ```
  Syntax: $$<structure instance name>.<member variable name>$$
  Example: $$myInterface.inf_name$$
  ```

In addition to the template variables, you can use the conditional and iterative command generation using the following statements:

- if-else if-else Statement—makes a logical decision in inclusion/exclusion of set of configuration command based on the value assigned for the variable in it.

  ```
  Syntax: if(<operand 1>  <logical operator>  <operand 2>){
  command1 ..
  ```

```
command2..
..
} else  if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
} else
{
Command5 ..
Command6..
..
}
Example: if-else if-else statement
    if($$USER_NAME$$ == 'admin'){
    Interface2/10
    no shut
    } else {
    Interface2/10
    shut
    }
```

- foreach Statement—used for iterating a block of commands. The iteration is performed based on the assigned loop variable value.

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}

Example: foreach Statement
    foreach ports in $$MY_INF_RANGE$${
    interface @ports
    no shut
    }
```

- Optional parameters—By default all parameters are mandatory. To make a parameter optional, you must annotate the parameter.

  In the variable section, include the following command:

  @(IsMandatory=false)

  Integer frequency;

  In the template content section, a command can be excluded or included without using "if" condition check, by assigning a value to the parameter. The optional command can be framed as below:

  probe icmp [frequency *frequency-value*] **[timeout** *seconds*] **[retry-count** *retry-count-value*]

Advanced Features

- Assignment Operation

  Config template supports assignment of variable values inside the template content section. The values are validated for the declared data type of the variable. If there is a mismatch, the value is not assigned.

  Assignment operation can be used under the following guidelines:

  – The operator on the left hand side must be any of the template parameter or a for loop parameter.

  – The operator on the right hand side values can be any of value from template parameter, for loop parameter, literal string values surrounded by quotes or simple string values.

If a statement does not follow these guidelines, the does not suit this format would not be considered as assignment operation. It is substituted during command generation like other normal lines.

```
Example: Template with assignment operation
    ##template properties
    name =vlan creation;
    userDefined= true;
    supportedPlatforms = All;
    templateType = CLI;
    published = false;
    ##
    ##template variables
    integerRange vlan_range;
    @(internal=true)
    integer vlanName;
    ##
    ##template content
    foreach vlanID in $$vlan_range$${
    vlan @vlanID
    $$vlanName$$=@vlanID
    name myvlan$$vlanName$$
    }
    ##
```

- Evaluate methods

  Config template uses the Java runtime provided Java script environment to perform arithmetic operations (such as ADD, SUBTRACT, and so on), string manipulations, and so on.

  Locate the javascript file in the template repository path. This file contains primary set of arithmetic, string functions. You can also add custom Javascript methods.

  These methods can be called from config template content section in below format:

```
Example1:
    $$somevar$$ = evalscript(add, 100, $$anothervar$$)
```

  Also the evalscript can be called inside if conditions as below:

```
    if($$range$$ > evalscript(sum, $$vlan_id$$,  -10)){
    do something…
    }
```

  You can call a method which is in the backend of the Java script file.

- Dynamic decision

  Config templates provides a special internal variable “LAST_CMD_RESPONSE”. This variable stores the last command response from th device during the execution of the command. This can be used in the config template content to make dynamic decisions to deliver the commands based on the device condition.

  An example use case is create a VLAN, if it is does not exist on the device.

```
Example: Create VLAN
    ##template content
    show vlan id $$vlan_id$$
    if($$LAST_CMD_RESPONSE$$ contains "not found"){'
    vlan $$vlan_id$$
    }
    ##
```

  This special implicit variable can be used only in the “IF” blocks.

- Template referencing

You can have a base template with all the variables defined. This base template can be imported to multiple templates. The base template content is substituted in the appropriate place of the extending template. The imported template parameters and the contents can be accessed inside the extending template.

```
Example: Template Referencing
Base template:
    ##template properties
    name =a vlan base;
    userDefined= true;
    supportedPlatforms = All;
    templateType = CLI;
    published = false;
    timestamp = 2015-07-14 16:07:52;
    imports = ;
    ##
    ##template variables
    integer vlan_id;
    ##
    ##template content
    vlan $$vlan_id$$
    ##

Derived Template:
    ##template properties
    name =a vlan extended;
    userDefined= true;
    supportedPlatforms = All;
    templateType = CLI;
    published = false;
    timestamp = 2015-07-14 16:07:52;
    imports = a vlan base,template2;
    ##
    ##template variables
    interface vlanInterface;
    ##
    ##template content
    <substitute a vlan base>
    interface $$vlanInterface$$
    <substitute a vlan base>

    ##
```

When you launch the extended template, the parameter inputs for the base template are also obtained. Additionally, the substituted content is used for complete CLI command generation.

Adding a Template

You can add user-defined templates and schedule jobs.

<<add topic ID: admin_template_add>>

Step 1 From the menu bar, select **Config > Delivery >Templates**.

You see the name of the template along with its description, Platforms and Tags.

Step 2 Click the **Add** icon to add a new template.

Step 3 Specify a **Template Name, Template Description** and a **Tags** for the new template.

Step 4 From the **Imports** drop-down, select the base template.

The base template content is displayed in the Template content window. The base template provide few parameters and template content provides certain CLI commands. This can be imported in to another template and the base template content is substituted in the appropriate place of the extending template. When the user launches the extended template, the parameter inputs for the base template are also obtained. Additionally, the substituted content is used for complete CLI command generation.

Step 5 Select the **Supported Platforms** that the template must support.

Step 6 Click in the Template Content window to edit the template syntax.

For information about the structure of the Configuration Template, see "Template Structure".

Step 7 Select **POAP** to make this template available when you power on the application.

Note The template will be considered as a CLI template if POAP is not selected.

Step 8 Select **Published** to make the template read-only. You cannot edit a published template.

Step 9 Click **Validate Template Syntax** to validate the template values.

Step 10 Click **Save** to save the template.

Step 11 Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Configuring Template Job

<<need to add TopicID: config_templates_job_wizard

You can configure and schedule jobs for individual templates from the **Config > Delivery > Templates** page.

Step 1 From the menu bar, select **Config > Templates**.

You see the name of the template along with its description, Platforms and Tags.

Step 2 Use the checkbox to select a template from the list.

Step 3 Click the **Launch Job Creation Wizard** icon and click **Next.**

Step 4 Use the drop-down to select the **Device Scope**. The devices configured under the selected Device Scope are displayed.

Step 5 Use the arrows to move the devices to the right column for job creation and click **Next**.

Step 6 Specify the **VSAN_ID, VLAN_ID, ETH_SLOT_NUMBER, VFC_SLOT_NUMBER, SWITCH_PORT_MODE, ETH_PORT_RANGE** and **ALLOWED_VLANS** values.

Step 7 Use the checkbox **Edit variables per device** to edit the variables for specific devices and click **Next**.

Step 8 If you have selected multiple devices, use the drop-down to select a specific device and preview its configuration.Click **Back** to edit the configuration or click **Next.**

Step 9 Specify a **Job Description** and enter the **Device Credentials**.

Step 10 Use the radio button to select **Deliver Instantly** or **Choose time to deliver**. If you select Choose time to deliver, specify the date and time for the job delivery.

Step 11 Use the checkbox to select **Copy Run to Start**.

Step 12 If you want to configure additional Transaction and Delivery options, use the checkbox to select **Show more options**.

Step 13 Under **Transaction Options (Optional)**, if you have a device with rollback feature support, select **Enable Rollback** checkbox and select the appropriate radio button.

Step 14 Under **Delivery Options (Optional)**, specify the **Timeout in seconds** and use the radio button to select the **Delivery Order**.

Step 15 Click **Finish** to create the job.

A confirmation message is displayed that the job has been successfully created.

Modifying a Template

You can edit the user-defined templates. However, the pre-defined templates cannot be edited. You cannot edit a template if it is already Published.

Step 1 From the menu bar, select **Config > Templates**.

You see the name of the template along with its description, Platforms and Tags.

Step 2 Select a template from the list and click the **Modify/View template** icon

Step 3 Edit the **Template Description**, **Tags**.

The edited Template content is displayed in the right-hand pane.

Step 4 From the **Imports** drop-down, select the base template.

The base template content is displayed in the Template content window. You can edit the template content based on your requirement in the Template Content window. Click on the Help icon next to the Template Content window for information about editing the content of the template.

Step 5 Edit the Supported Platforms for the template.

Step 6 Click **Validate Template Syntax** to validate the template values.

Step 7 Click **Save** to save the template.

Step 8 Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Importing a Template

Step 1 From the menu bar, select **Config > Templates** and click on the **Import template** icon.

Step 2 Browse and select the template saved on your computer.

Step 3 You can edit the template parameters, if required. For information, see Modifying a Template, page 3-59.

Step 4 Click **Validate Template Syntax** to validate the template.

Step 5 Click **Save** to save the template or **Save and Exit** to save the template and exit.

Exporting a Templatef

Step 1 From the menu bar, select **Config > Templates**.

Step 2 Use the checkbox to select a template(s) and click the **Export template** icon.

Step 3 Specify a name for the template and select a location to save the template on your computer.

Deleting a Template

You can delete the user-defined templates. However, you cannot delete the pre-defined templates.

Step 1 From the menu bar, select **Config > Templates**.

Step 2 Use the checkbox to select a template(s) and click the **Remove template** icon.

Step 3 In the confirmation dialog box, click **Yes** to delete the template.

Configuring Jobs

Step 1 From the menu bar, select **Config > Delivery > Jobs**.

The jobs are listed along with the Job ID, description and status.

Step 2 Click the **Show Filter** icon to filter the jobs by Job ID, Description, Devices and Status. In the Status column, use the drop-down to select the job status.

Step 3 Select a job and click the **Delete** icon to delete the job.

Power-On Auto Provisioning (POAP)

POAP automates the process of upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

When a Cisco Nexus switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode, locates a DHCP server and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. It also obtains the URL of an SCP server and downloads a configuration script that is run on the switch to download and install the appropriate software image and configuration file.

Note When you move the mouse cursor over an error identified in a specific parameter in any window, it will display the exact error message before you move to the next screen.

There are five main steps to configure a POAP device:

Step 1 DHCP Scope Creation

Step 2 Add the boot, startup, image and server information.

Step 3 Startup configuration creation

Step 4 Cable plan.

Step 5 Script and files (license) attachment

POAP Launchpad

Note These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

The POAP launchpad contains the following configuration steps:

- DHCP Scope - Create and manage scopes for POAP creation.
- Images and Configuration - Set a server for images and configuration files.
- POAP Definitions - Generate from template or upload existing configuration.
- Cable Plan - Create, Publish and Deploy Cable Plans.

DHCP Scope

DHCP scope is a well-defined term in DHCP arena. It is used to define a policy for giving out IP addresses and other options to host on a specific IP subnet. In DCNM, we use the DCHP scope to distribute IPv4 address, PYTHON bootscript, (or other supported protocol + access credential + server) which stores the bootscript.

From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.

The columns in table Table 3-3are displayed

Table 3-3 :DHCP Scope

DHCP Scope	Comment
Scope Name	The DHCP scope name must be unique amongst the switch scopes. This name is not used by ISC DHCP but used to identify the scope.
Scope Subnet	The IPv4 subnet used by the DHCP servers.
IP Address Range	The IP address ranges allocated to the POAP switches. Multiple IP addresses can be used, separated by comma.
Lease Time	Maximum lease time for the DHCP lease.
Default Gateway	The default gateway for the DHCP scope. You must enter a valid IP as the default gateway.
Domain Name Servers	The domain name server for the DHCP scope.

DHCP Scope	Comment
Bootscript Name	The Python Bootup script.
Bootscript Server	The server that holds the bootscript.

- Adding a DHCP Scope, page 3-62
- Editing an existing DHCP Scope, page 3-62
- Deleting a DHCP Scope, page 3-62

Adding a DHCP Scope

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.

Step 2 Click **Add scope** icon.

Step 3 In the Add DHCP Scope window, specify values in the fields according to the information in Table 3-3.

Step 4 Click **Add**.

Editing an existing DHCP Scope

Note Once the DCNM is accessed for the first time, you must edit the default scope named '`enhanced_fab_mgmt`" and add free IP address ranges.

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.

Step 2 Use the checkbox to select the DHCP scope.

Step 3 Click **Edit scope** icon.

Step 4 In the Edit DHCP Scope window, edit the DHCP scopes.

Step 5 Click **Apply** to save the changes.

Deleting a DHCP Scope

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.

Step 2 Use the checkbox to select the DHCP scope.

Step 3 Click **Delete scope** icon.

Step 4 In the delete notification, click **Yes** to delete the DHCP scope.

Note You may click the **Refresh** icon to refresh the DHCP Scopes list.

Images and Configuration

This feature enables you to specify the servers & credential used to access the device images and the uploaded or DCNM generated/published device configuration. The server containing the images could be different from the one containing the configurations. If the same server contains both images and configurations, you must provide the server IP address and credentials twice for each server, if the directories holding images and configuration files are different. By default, DCNM server will be the default image and configuration server.

Copy Kickstart and system images into the repository prior to defining POAP definitions for devices. If the DCNM is the image repository, copy the image files into */var/lib/dcnm/* directory.

- Add Image or Configuration Server URL, page 3-63
- Editing an Image or Configuration Server URL, page 3-63
- Deleting an Image or Configuration Server URL, page 3-63

Add Image or Configuration Server URL

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Image and Config Servers**.

Step 2 Click the **Add** icon.

Step 3 In the Add Image or Configuration Servers URL window, specify a **Name** for the image.

Step 4 Enter **Hostname/Ipaddress** and **Path** to download or upload files.

Step 5 Specify the **Username** and **Password**.

Step 6 Click **OK** to save.

Editing an Image or Configuration Server URL

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Image and Config Servers**.

Step 2 Select an existing Image and Configuration Server from the list, and Click the **Edit** icon.

Step 3 In the Edit Image or Configuration Servers URL window, edit the required fields.

Step 4 Click **OK** to save.

Deleting an Image or Configuration Server URL

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Image and Config Servers**.

Step 2 Select an existing Image and Configuration Server from the list, and Click the **Delete** icon.

Step 3 In the delete notification, click **Yes** to delete the image and configuration server.

Note The default SCP Repository cannot be deleted.

POAP Templates

Templates can be created or imported into the template builder of DCNM. There are some predefined Fabric specific POAP templates bundled with DCNM. The template builder can be invoked from the GUI, Config->Delivery -> Templates. The templates dedicated to POAP will be used to generate many different POAP device configurations

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

- Use the **Show Filter** icon to filter the templates.
- Use the **Print** icon to print the list of templates and their details.
- Use the **Export** icon to export the list of templates to a Microsoft Excel spreadsheet.

This section contains the following:

- Add POAP template
- Editing a Template
- Cloning a Template
- Importing a Template
- Exporting a Template
- Deleting a Template

Add POAP template

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.

Step 2 In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.

Step 3 Click **Add template** icon.

Step 4 Specify the **Template Name**, **Template Description** and **Tags**.

Step 5 Use the checkbox to specify the **Supported Platforms**.

Step 6 Select the **POAP** checkbox or else by default, the DCNM will consider it as a CLI template.

Step 7 Select the **Published** checkbox if you want the template to have 'Read Only' access.

Step 8 In the Template Content pane, you can specify the content of the template. For help on creating the template content, click the **Help** icon next to the Template Content header. For information about POAP template annotations see the POAP Template Annotation section.

Step 9 Click **Validate Template Syntax** to validate syntax errors.

Step 10 Click **Save** to save the template.

Step 11 Click **Save and Exit** to save the template and exit the window.

Step 12 Click **Cancel** to discard the template.

Editing a Template

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.

Step 2 In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.

Step 3 Select a template from the list and click **Modify/View template** icon.

Step 4 Edit the template content and click **Save** to save the template or **Save and Exit** to save and exit the screen.

Cloning a Template

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.

Step 2 In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.

Step 3 Select a template from the list and click **Modify/View template** icon.

Step 4 Edit the template and click **Save** to save the template or **Save and Exit** to save and exit the screen.

Importing a Template

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.

Step 2 In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.

Step 3 Select a template from the list and click **Import template** icon.

Step 4 Select the template file and upload.

Exporting a Template

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.

Step 2 In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.

Step 3 Select a template from the list and click **Export template** icon.

Step 4 Select a location for the file download.

Deleting a Template

Note Only user-defined templates can be deleted.

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.

Step 2 In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.

Step 3 Select a template from the list and click **Remove template** icon.

Step 4 Click **Yes** to confirm.

POAP Template Annotation

Annotation is used to add sematic, validation logic and description to the template variable.

The Annotation for a given template variable is required to precede the given template variable. Only one annotation statement is required for each template variable. When a template variable has an associated annotation statement, the template variable has to be declared on a single line, Multiple variables cannot be declared under the same annotation statement.

Format of an annotation statement is as follows:

@(<key1>=<value1>,<key2>=<value2>, …, <keyN>=<valueN>)

Note

- Each annotation statement is composed of one or more key-values pair.
- The value can be true, false, or a string.
- If the value is a string, it should be double quoted.

The following is a sample template variable, “hostname”, with annotation statement with the keys “DisplayName”, and “Description”:

@(DisplayName=”Host Name”, Description = “Description of the host”)

String hostname;

The table displays the supported keys in the annotation statement:

Table 3-4 Annotation Keys

Key Name	Default Value	Description
DisplayName	Empty String	The value is displayed as a variable label in the template form GUI, on POAP definition screen.
Description	Empty String	Displays the description next or below the template variable field in the template form GUI.
IsManagement	false	The associated variable is of IP Address type. This will be used as the management IP address. DCNM used this IP address to manage the devices.
IsMultiplicity	false	If true, this single value can take multiple values. For example; when it is used with `IsManagement` annotation, it allows you to type in multiple IP addresses and assign each IP address to a device.
IsSwitchName	false	The associated variable value is used as the device host name.
IsMandatory	true	It marks the field as mandatory if the value is set as ‘true’.
UseDNSReverseLookup	false	This annotation compliments the `IsSwitchName` annotation. Once they are associated with a variable. The variable is populated with the reverse DNS name, if available during the creation time of the corresponding POAP definition record.
IsFabricPort	false	The associated variable value contains a list of the ports used as fabric ports. The variable value will be used by the cable plan generation from POAP

Key Name	Default Value	Description
IsHostPort	false	Trunk ports connected to host/servers.
IsVPCDomainID	false	Used as theVPC Domain ID.
IsVPCPeerLinkSrc	false	Used as the VPC IPv4 source address.
IsVPCPeerLinkDst	false	Used as the VPC IPv4 peer address.
IsVPCPeerLinkPortChannel	false	Used for VPC port channel.
IsVPCLinkPort	false	Used for VPC interface.
IsVPC	false	Used as a VPC record.
IsVPCID	false	Individual VPC ID.
IsVPCPortChannel	false	Individual VPC port channel.
IsVPCPort	false	VPC Interface.

POAP Definitions

The POAP switch definition has two major functions:

- Monitoring switch POAP process
- Managing POAP switch configuration

You must copy the Cisco Prime DCNM license files to the **/var/lib/dcnm/license** directory to install as part of the POAP process.

You must also copy the device licenses to the **/var/lib/dcnm/licenses** folder.

Note The device licenses refers to the devices monitored by the Cisco Prime DCNM.

The following fields and icons are listed at the menu bar of the window to customize the view of the information in the window:

Fields and Icons	Description
Serial Number	Specifies the serial number for the switch.
Switch ID	Specifies the ID defined for the switch
Management IP	Specifies the Management IP for the switch.
Status	
Switch Status	Indicates if the switch is published or not.
Publish Status	Indicates if this POAP template has been published successfully to the TFTP site.
Bootscript Status	Indicates the Bootscript execution state when the device executed POAP. For details, view the “Boot Log” file.

Fields and Icons	Description
Diff State	Specifies if the configuration defined in POAP is different from the running configuration on the device. If a difference is detected, the user has an option to make changes to the device configuration, thereby ensuring that the configuration on the device in sync with the POAP configuration.[1] The different states are: • NA—Specifies that no POAP definition is configured on DCNM for the particular device; therefore, no difference computation can be made. • Diff Detected—Specifies that few configuration differences are detected between POAP definition in DCNM and the running configuration on the switch. You can review the difference statements and choose the commands to deploy to the device, and synchronize the running configuration with the POAP definition. • No Diff Detected—Specifies that there was no configuration diff perceived between POAP definition and the running configuration on the switch. • Error—Specifies that an error has occurred during diff computation. Refer to the logs to troubleshoot the issue.
Model	Specifies the model of the switch.
Template/Config File Name	Specifies the template used for creating the POAP definition. Fabric and IPFabric POAP templates are available.
Bootscript Last Updated Time	Specifies the last updated time for bootscript.
Last Published	Specifies the last published time for the POAP definition.
Last Saved	Specifies the last saved time for the POAP definition.
POAP Creation Time	Specifies the time when the POAP definition was created.
System Image	Specifies the System Image used while creating the POAP definition.
Kickstart Image	Specifies the kickstart image used the PAOP definition
Icons	
Add	Allows you to add a POAP definition. For more information, see Creating a POAP definition.
Edit	Allows you to edit a POAP definition. For more information, see Editing a POAP Definition.
Delete	Allows you to delete a POAP definition. For more information, see Deleting POAP Definitions.
Publish	Allows you to publish a POAP definition. For more information, see Publishing POAP definitions.
Write Erase and Reload	Allows you to reboot and reload a POAP definition. For more information, see Write, Erase and Reload the POAP Switch Definition.
Change Image	Allows you to change the image for the defined POAP definition. For more information, see Change Image.
Boot Log	Display the list and view log files from the device bootflash.

Fields and Icons	Description
Refresh Switch	Refreshes the list of switches.
Show Filter	Filters list of switches based on the defined value for each column.
Print	Prints the list of devices and their details.
Export	Exports the list of devices and their details to a Microsoft Excel spreadsheet.
Select Columns	Displays the columns to be displayed. You can choose to show/hide a column.

1. You can discover the device manually also. Navigate to **Admin < Data Sources** on the Web Client to initiate a "Diff state" comparison for each device.

Note Each annotation statement is composed of one or more key-values pair. The value can be true, false or a string. If the value is a string, it should be mentioned in double-quotes.

This section contains the following:

- Creating a POAP definition
- Uploading a POAP Definition
- Editing a POAP Definition
- Deleting POAP Definitions
- Publishing POAP definitions
- Write, Erase and Reload the POAP Switch Definition

Creating a POAP definition

Step 1 From the menu bar, select **Config > Power-On Auto Provisioning (POAP)>POAP Definitions**.

Step 2 Click **Add** to add a new POAP definition.

Step 3 Use the radio button and select **Generate Definition** to generate POAP definition from a template, and click **Next** to specify the switch details.

Step 4 Enter the serial number of switches separated by comma. Alternatively, you can click the **Import from CSV File** button to import the list of switches.

Step 5 Use the drop-down to select the Switch Type.

Step 6 Use the drop-down to select the Image Server.

Step 7 Use the drop-down to select the System Image and Kickstart image.

Step 8 Use the drop-down to select the Config Server, and specify the Switch User Name and Password.

Step 9 Use the drop-down in the Add Switches to Group to add the POAP devices to a specific group, and specify the Switch User Name and Switch Password.

Step 10 Click **Next** to Select the Switch Config Template.

Step 11 Use the drop-down to select the Template and click **View** to specify the Template Parameters.

Step 12 Enter Template Parameters.

Step 13 Use the drop-down to select the Settings File. If the settings file in unavailable, click **Save Parameter as New Settings File** button to specify a name for the settings file, select the variables and click **Save**. The new settings file will now be listed in the Settings File drop-down.

Step 14 Click **View** to view the settings file parameters.

Step 15 Click **Manage** to modify the settings file parameters.

Step 16 Click **Next** to generate the configuration.

Uploading a POAP Definition

Step 1 From the menu bar, select **Config > Power-On Auto Provisioning (POAP) > POAP Definitions**.

Step 2 Use the radio button and select **Upload Startup Config** to upload startup config to the POAP repository Server, and click **Next** to Enter the switch details.

Step 3 Enter the serial number of switches separated by comma.

Step 4 Use the drop-down to select the **Switch Type**.

Step 5 Use the drop-down to select the **Image Server**.

Step 6 Use the drop-down in the **Add Switches to Group** to add the POAP devices to a specific group.

Step 7 Use the drop-down to select the **System Image** and **Kickstart Image**.

Step 8 Use the drop-down to select the **Config Server**, and specify the Switch User Name and Password.

Step 9 Click **Browse** to select the upload configuration file.

Step 10 Click **Save** to save the uploaded the configuration file or **Publish** to publish the POAP definition.

Editing a POAP Definition

Step 1 From the menu bar, select **Config > Power-On Auto Provisioning (POAP) >** Select the POAP switch definitions from the list and click the **Edit** icon.

Step 2 Follow the steps listed in Creating a POAP definition and Uploading a POAP Definition sections.

Note You can select multiple POAP definitions with similar parameters to edit POAP definition.

Deleting POAP Definitions

Step 1 From the menu bar, select **Config > Power-On Auto Provisioning (POAP) >** Select the POAP switch definitions from the list and Click the **Delete** icon.

Step 2 Click **Yes** to delete the switch definitions.

A prompt appears to delete the device from the data source.

Step 3 Click **OK** to confirm to delete the device from the data source also.

Publishing POAP definitions

Step 1 From the menu bar, select **Config > Power-On Auto Provisioning (POAP) >** Select the POAP switch definitions from the list and Click the **Publish** icon.

Step 2 Click **Yes** to publish the switch definitions.

Write, Erase and Reload the POAP Switch Definition

Step 1 From the menu bar, select **Config > Power-On Auto Provisioning (POAP) >** Select the POAP switch definitions from the list.

Step 2 Click the **Write, Erase and Reload** icon.

Step 3 Click **Continue** to reboot and reload the switch definitions.

Change Image

Step 1 From the menu bar, select **Config > Power-On Auto Provisioning (POAP) >** Select the POAP switch definitions from the list.

Step 2 Select the switch for which you need to change the image. Click **Change Image**.

Note You can select multiple POAP definitions with similar parameters to change the image for booting the device.

The Multi Device Image Change screen appears.

Step 3 From the **Image Server** dropdown list, select the server where the new image is stored.

Step 4 From the **System Image** dropdown list, select the new system image.

Step 5 From the **Kickstart Image** dropdown list, select the new image which will replace the old image.

Step 6 Click **Publish** to apply and change the image.

Cable Plan

The Cable plan configuration screen has the following options:

- Create a Cable Plan
- Viewing an Existing Cable Plan Deployment
- Deleting a Cable Plan
- Deploying a Cable Plan
- Revoking a Cable Plan
- Viewing a Deployed Cable Plan from Device

Note If you are generating POAP definitions from the uploaded configuration, then generation of cable plan using the option of "Generate Cable Plan from POAP definition" will not work as the POAP definitions generated from the uploaded configuration will not have the required meta-data to generate the cable plans. You must select either "Capture from Existing Deployment" or "Import Cable plan file" to create a cable plan.

Create a Cable Plan

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.

Step 2 Click **Create Cable Plan**.

In the Create Cable Plan pop-up, use the radio button to select the options.

Step 3 If you select:

a. **Generate Cable Plan from POAP definition**: You can use the switches defined in the POAP flow and produce a port-to-port cable plan to be used when wiring the physical devices.

b. **Capture from existing deployment**: You can ascertain he Inter-Switch Links between existing switches managed by DCNM and "lock down" the cable plan based on the existing wiring.

c. **Import Cable Plan File**: You decide how to wire the switches (or how they are already wired) and select an XML file for import into DCNM.

Viewing an Existing Cable Plan Deployment

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.

Step 2 Click **View**.

Step 3 In the Cable Plan - Existing_Deployment window, you can view the existing cable plan deployments.

Step 4 You can use the Table View and XML View icons to change the view of the cable plan deployments table.

Deleting a Cable Plan

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.

Step 2 Click **Delete from DCNM**.

Step 3 Click **Yes** to confirm deletion.

Deploying a Cable Plan

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.

Step 2 In the Switches table, use the checkbox to select cable plan(s) and click **Deploy a Cable Plan**.

Step 3 Click **Yes** to confirm deployment.

Revoking a Cable Plan

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.

Step 2 In the Switches table, use the checkbox to select cable plan(s) and click **Revoke a Cable Plan**.

Step 3 Click **Yes** to confirm.

Viewing a Deployed Cable Plan from Device

Step 1 From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.

Step 2 In the Switches table, click **In Sync** or **Out of Sync** hyperlink in the cable plan status column.

Step 3 You can use the Table View and XML View icons to change the view of the cable plan table.

Fabric

Note These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

This feature automates network provisioning and provides a new layer of automation integration in which the data center fabric-switching infrastructure is automatically provisioned for the physical or virtual workload that is being instantiated.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Table 3-5

Field/Icons	Description
Organizations Section	
Organization/Partition Name	Specifies the organization or the partition name.
Description	Specifies the description for the organization.
Partition ID	Specifies the partition ID to be associated with the partition.
Orchestration Engine	Specifies the Orchestrator name for the organization.
Service Node IP Address	Specifies the IP address for the service node for a partition
Edge Router ID	Specifies the Edge Router ID.
Extension Status	Specifies if the extension is enabled or disabled.
Profile	Specifies the default profile used.
Networks Section	
Network Name	Specifies the name to identify the network.
Partition Name	Allows you to select the partition to be applied for the network.
Segment ID	Specifies the segment ID to be used for partition extension.

Table 3-5

Field/Icons		Description
Mobility Domain	VLAN ID	Specified the VLAN ID for the mobility domain.
	Mobility Domain ID	Allows you to select the mobility domain ID from the drop-down list.
Profile Name		Specifies the default profile used.
DHCP Scope	Subnet	Specifies the subnet for the network.
	Gateway	Specifies the gateway for the network.
	IP Range	Specifies the IP address range available for the network.
Add		Allows you to add Organization, Partition, or Network.
Edit		Allows you to edit Organization, Partition, or Network.
Delete		Allows you to delete Organization, Partition, or Network.
Enable Extension		Allows you to enable the extension for the selected Organization.
Disable Extension		Allows you to disable the selected extension.
Deploy Configuration		Allows you to deploy the network for the selected partition.
Undeploy Configuration		Allows you to undeploy the network configuration.
Refresh		Refreshes the list of items in the view.
Show Filter		Filters list of items based on the defined value for each column.
Print		Prints the list of Organizations or Networks along with their details.
Export		Exports the list of items and their details to a Microsoft Excel spreadsheet.
Maximize		Allows you to maximize the view for Organizations or Networks.

Fabric provides the following configuration options:

- Organizations
  - Adding an Organization
  - Editing an Organization
  - Deleting an Organization
  - Adding a Partition
  - Editing a Partition
  - Deleting a Partition
- Networks
  - Adding a Network
  - Editing a Network
  - Deleting a Network

Adding an Organization

Step 1 From the menu bar, select **Config > Auto-Configuration > Organizations > Add > Organization**.

Step 2 In the Add Organization window, specify the **Name** and **Description** of the organization.

Step 3 Specify the **Orchestration Engine**.

Step 4 Click **Add**.

Editing an Organization

Step 1 From the menu bar, select **Config > Auto-Configuration > Organizations**.

Step 2 Select an organization from the List and click the **Edit** icon.

Step 3 In the Edit Organization window, change the configuration.

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

Deleting an Organization

Note You must delete all partitions under an organization before deleting the organization.

Step 1 From the menu bar, select **Config > Auto-Configuration > Organizations**.

Step 2 Select an organization from the List and click the **Delete** icon.

Step 3 Click **Yes** to confirm.

Adding a Partition

Step 1 From the menu bar, select **Config > Auto-Configuration > Organizations > Add>Partition**.

Step 2 In the Add Partition window, use the drop-down to select the organization.

Step 3 Specify the **Name** for the partition.

Step 4 Specify the VRF name and provide description for the partition.

Step 5 Specify the Edge Router ID for the partition.

Select the checkbox if you choose to extend the partition across the fabric.

If you do not select the checkbox, this partition will not be extended across the Fabric.

Step 6 Specify the **DNS Server** and the **Secondary DNS server** for the partition.

Step 7 From the drop-down list, select the default **Profile Name**.

The values for the **Profile Parameters** are auto-populated based on the default Profile Name.

Step 8 Click **OK** to configure the partition.

Editing a Partition

Step 1 From the menu bar, select **Config>Auto-Configuration>Organizations**.

Step 2 Click an organization from the List and select the Partition.

Step 3 Click the **Edit** icon

Step 4 In the Edit Partition window, change the configuration.

Step 5 Click **Edit** to save the changes.

Deleting a Partition

Note You mst delete all networks under the partition before deleting the partition.

Step 1 From the menu bar, select **Config>Auto-Configuration>Organizations.**

Step 2 Click an organization from the List and select the Partition.

Step 3 Click the **Delete** icon

Step 4 Click **Yes** to confirm.

Adding a Network

Step 1 From the menu bar, select **Config > Auto-Configuration > Networks >Add**.

Step 2 In the Add Network window, use the drop-down to select the **Organization** and **Partition**.

Note If there is only one organization and partition configured, the values for these fields are automatically populated.

Step 3 Specify the **VRF Name** for the partition.

The VRF Name must be of the format organizationName:partitionName.

Step 4 Specify the **Network Name** to identify the network.

Step 5 Specify the **Multicast Group Address**.

Note The Multicast Group Address is used to Enable VxLAN Encapsulation on the **Admin > Fabric Encapsulation Settings** page.

Step 6 Select the **Network Role** from the drop-down list based on the type of the network.

Step 7 In the Network ID section, choose one of the following:

- Segment ID Only
  - Specify the **Segment ID** for the network.
- Mobility Domain and VLAN

  - Specify the **Segment ID** for your network.
  - Select **Generate Seg ID** to generate segment ID automatically.
  - Specify the **VLAN ID** and **Mobility Domain ID** if you need to create a VLAN + Mobility Domain network.

Step 8 In the DHCP Scope section, specify the **IP Range**.

Step 9 Use the drop-down to select the **Profile**.

Step 10 Specify the **Profile** parameters.

Step 11 Specify the **Service Configuration** parameters.

Step 12 Click **Add**.

Editing a Network

Step 1 From the menu bar, select **Config>Auto-Configuration>Networks**.

Step 2 Select a network from the List and click the **Edit** icon

Step 3 In the Edit Partition window, change the configuration.

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

Deleting a Network

Step 1 From the menu bar, select **Config>Auto-Configuration>Networks**.

Step 2 Select a network from the List and click the **Delete** icon.

Step 3 Click **Yes** to confirm.

Profiles

Profiles provide the following configuration options:

- Profiles
  - Adding a profile
  - Editing a Profile
  - Delete a Profile
- Profile Instance
  - Editing a Profile Instance

Adding a profile

Step 1 From the menu bar, select **Config > Profiles > Add**.

Step 2 In the Add Profile window, specify the **Name** and **Description** of the profile.

Note A global VLAN is a fabricpath-enabled VLAN which is not mapped to a Segment ID. Before Cisco Prime DCNM 7.2(2), the user-defined Global VLAN profile names must end with "GblVlanProfile" (case-insensitive), for the network to auto-refresh.

Step 3 Use the drop-down, select the **Type** of the Profile.

Note Devices with different platforms may use profiles of different profile types. For this release, **FPVLAN, FPBD, IPVLAN, IPBD** are supported.

Step 4 From the drop down, select **Sub Type**. Sub Type of profiles differentiate profile categories, such as :

- individual profile
- universal profile
- network profile
- partition profile
- DCI profile and so on.

For more information, see Cisco Dynamic Fabric Automation Configuration Guide.

In DCNM Release 7.2, the following subtypes are supported:

- partition:universal - Universal profile for a partition
- network:universal - Universal profile for a network
- bl-er:universal - Universal profile for a Border Leaf or Edge Router
- bl-er:universal,er - Universal profile for a Edge Router
- bl-er:universal,bl - Universal profile for a Border Leaf
- partition:individual - Individual profile for a partition
- network:individual - Individual profile for a network

Step 5 Use the drop-down to select the **Forwarding Mode**. The following values are supported:

- anycast-gateway
- proxy-gateway
- none

Step 6 Enter the **Profile Content** from collection of CLI commands to discover a specific configuration.

Step 7 Click **Add**.

Editing a Profile

Step 1 From the menu bar, select **Config > Profiles**.

Step 2 Select a profile from the list and click the **Edit** icon.

Step 3 In the Edit profile window, change the configuration.

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

Delete a Profile

Step 1 From the menu bar, select **Config>Profiles**.

Step 2 Select a profile from the list and click the **Delete** icon.

Step 3 Click **Yes** to confirm.

Editing a Profile Instance

Step 1 From the menu bar, select **Config>Profiles**.

Step 2 Select a profile from the list and click the **Edit** icon.

Step 3 In the Edit Profile Instance window, change the configuration.

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

Administering Cisco Prime DCNM Web Client

The Admin options allows you to perform minor administrative and configuration tasks on the Cisco Prime DCNM-SAN Server.

The Admin option contains the following sub-menus:

- **Status**—Displays the status of the Database Server and allows you to start and stop Performance collector services on your server. You should restart services only if something is not working properly or if too large a percentage of system resources are being consumed.
- Data Sources—Allows you to view all the data sources such as Fabric, LAN, VMware, SMIS and so on.
- **Logs**—Allows you to view all the logs from the various services running on the Cisco Prime DCNM-SAN Server.
- Server Properties—Allows you to view all the fields defined in the server.properties config file.
- SFTP Credentials—Allows you to view the SFTP credentials.
- License—Allows you to view the licensing details.
- Federation—Allows you to view the server federation details.
- Clients—Allows you to view all the clients connected to the Cisco Prime DCNM-SAN Server.

Note You cannot start or stop the Database Server services using DCNM Web Client. If you are using the Microsoft Windows operating system, you need to use Microsoft Management Console to stop, start, or restart the Database Server.

- If you see a database file lock error in the database log, you can fix it by shutting down and restarting the database server using the Web Client.
- Only network administrators can access the DCNM Web Client Admin options. Network operators cannot view the Admin options.

This section includes the following topics:

Starting, Restarting, and Stopping Services

Step 1 **DETAILED STEPS**From the menu bar, choose **Admin** > **General** > **Status**.

You see a table of services per server and the status of each as shown in Figure 3-1.

Figure 3-1 DCNM-SAN Services Status

Step 2 In the Actions column, use the **Start**, **(Re)start** or **Stop** icons to start, restart, or stop any of the services.

Administering Datasources

You can manage the Fabrics, LAN and VMWare using the datasources option. This section contains the following:

Adding, Editing, Re-discovering, Purging and Removing Managed Fabrics

Cisco Prime DCNM Web Client reports information obtained by the Cisco Prime DCNM-SAN on any fabric known to Cisco Prime DCNM-SAN.

This section contains the following:

Adding a Fabric

You can discover new fabric and start managing a fabric from Cisco Prime DCNM Web Client. Before you discover a new fabric, ensure you create a SNMP user on the switch.

Step 1 From the menu bar, choose **Admin > General > Data Sources**.

You see a list of fabrics (if any) managed by Cisco Prime DCNM-SAN in the Opened column.

Step 2 Click **Add Fabric** to add a new fabric.

You see the Add Fabric dialog box.

Step 3 Enter the Fabric Seed Switch IP address for this fabric.

Step 4 (Optional) Check the **SNMPV3** check box. If you check SNMPV3, the fields Read Community and Write Community change to Username and Password.

Step 5 Enter the User Name and Password for this fabric.

Step 6 Select the privacy settings from the Auth-Privacy drop-down list.

Step 7 (Optional) Check the **Limit Discovery by VSAN** checkbox to specify the included VSAN list or excluded VSAN list from the VSANs provided to discover a new fabric.

Step 8 (Optional) Check the **Enable NPV Discovery in all Fabrics** check box. If you check enable NPV discovery in all fabrics, the changes are applied to all the fabrics that are previously discovered.

Step 9 Click **Add** to begin managing this fabric.

You can remove single or multiple fabrics from the Cisco Prime DCNM Web Client.

Editing a Fabric

Step 1 From the menu bar, choose **Admin > General > Data Sources**.

Step 2 Select the check box next to the fabric that you want to edit and click **Edit Fabric**.

You see the Edit Fabric dialog box. You can edit only one fabric at a time.

Step 3 Enter a new fabric Name.

Step 4 (Optional) Check the **SNMPV3** check box. If you check SNMPV3, the Community field change to Username and Password.

Step 5 Enter the **User Name** and **Password**, privacy and specify how you want DCNM Web Client to manage the fabric by selecting one of the status options.

Step 6 Change the fabric management state to **Managed**, **Unmanaged**, or **Managed Continuously**.

Step 7 Click **Apply** to save the changes.

Note In the **Admin>Datasources>Fabric**, Select the fabric for which the fabric switch password is changed. Click **Edit Fabric**, unmanage the fabric, specify the new password and then manage the fabric. You will not be able to open the fabric as the new password will not sync with the database. To open the fabric, you must log into the DCNM-SAN client, Go to **Server>Admin** and click the **Open** tab. Select the fabric and change the password manually in the Client Password/Community column.

Rediscovering a Fabric

Step 1 From the menu bar, choose **Admin>General>Datasources**.

Step 2 Select the check box next to the fabric and click the **Re-discover Fabric** icon.

Step 3 Click **Yes** in the pop-up window.

The Fabric will now be re-discovered.

Purging a Fabric

Step 1 From the menu bar, choose **Admin>General>Datasources**.

Step 2 Select the check box next to the fabric and click the **Purge Fabric** icon.

Step 3 Click **Yes** in the pop-up window.

The Fabric will now be purged.

Removing a Fabric

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Select the check box next to the fabric that you want to remove and click **Remove Fabric** icon to remove the fabric from the datasource and to discontinue data collection for that fabric.

Moving Fabrics to Another Server Federation

This feature is only available on the federation setup and the Move Fabric is only displayed in the federation setup screen.

You can move the fabrics from a sever that is down to an active server. The management state will remain the same.

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Select the fabrics from the fabric table. Click **Move Fabrics** to another Federation Server, or **Move LAN Tasks** to another DCNM Server.

Step 3 Select the fabrics that need to be moved and click **Move Fabric**.

Step 4 In the Move Fabrics to another Federation server dialog box, select the DCNM server where the fabrics will be moved. The server drop-down list will list only the active servers.

Step 5 In the Move LAN Tasks to another DCNM Server dialog box, enter the LAN tasks that need to be moved and specify the DCNM server.

Adding, Editing, Re-discovering, Purging and Removing LAN, LAN Tasks and Switch

Cisco Prime DCNM Web Client reports information obtained by the Cisco Prime DCNM-LAN devices.

This section contains the following:

Adding LAN Devices

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

You see the list of LAN devices in the Name column.

Step 2 Click **Add LAN Task** to add LAN.

You see the Add LAN dialog box.

Step 3 Select **Hops from Seed Switch**, **Switch List** or **FWSM**. The fields vary depending on your selection.

Step 4 Enter the **Seed Switch** IP address for the fabric.

Step 5 The options vary depending on the discovery type selected. For example; If you select **SNMPV1** or **SNMPV3/CLI** check box varied fields are displayed.

Step 6 Select the switch group and specify the Scan Time-out.

Step 7 Specify the user credentials and the Optional Enable Password.

Step 8 Use the drop-down to select the switch group.

Step 9 Click **Next** to begin the Shallow Discovery.

Step 10 In the Shallow LAN Discovery window, you can select all switches by using the checkbox next to the switch name column or select individual switches. Click **Previous** to go back and edit the parameters.

Note In the Status column, if the switch status is Time-out or Cannot be contacted, these switches cannot be added.

Step 11 Select a switch and click **Add** to add a switch to the switch group.

If the seed switch(es) are not reachable, it will be shown as "unknown" on the shallow Discovery window.

Editing LAN Devices

You can modify a LAN from Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Select the check box next to the LAN that you want to edit and click **Edit LAN** by CDP Seed.

You see the Edit LAN dialog box.

Step 3 Enter the User Name and Password.

Step 4 Select the LAN status as **Managed** or **Unmanaged**.

Step 5 Select the Candidate Switches for Deep Discovery.

Note You can hold the Ctrl key on your keyboard to select multiple candidate switches.

Step 6 Click **Apply** to save the changes.

Purging LAN

Step 1 From the menu bar, choose **Admin>General>Datasources**.

Step 2 Click the **Purge unreachable devices or dead links in selected LAN** icon.

Step 3 Click **Yes** in the pop-up window to purge the LAN device.

Note In case of a Federation set-up, you will have to select the LAN to purge.

Removing LAN Devices

You can remove a LAN from Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Select the check box next to the LAN that you want to remove and click the **Remove LAN by CDP Seed** icon to remove the switches and all their data.

Step 3 Click **Yes** to review the LAN device.

You can also remove an individual LAN Switch

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Click the arrow next to the DCNM Server check box to expand the field.

Step 3 In the Switch column, click **Delete Switch** icon to delete a switch connected to the DCNM server.

Edit LAN Task

Step 1 From the menu bar, choose **Admin>General>Datasources**

Step 2 In the Discovery Task column, click the **Edit LAN Task** icon.

Step 3 In the Edit LAN Task dialog box, specify the user credentials and the Optional Enable Password.

Step 4 Use the radio button to select the Status.

Step 5 Click **Apply** to save the changes.

Re-discover LAN Task

Step 1 From the menu bar, choose **Admin>General>Datasources**.

Step 2 In the Discovery Task column, click the **Re-discover LAN** icon.

Step 3 Click **Yes** in the pop-up window to re-discover the LAN.

Moving LAN Devices Under a Task

You can move LAN devices under a task to a different server using Cisco Prime DCNM Web Client. This feature is available only in the federation setup and the Move LAN is displayed in the federation setup screen.

You can move the LAN from a sever that is down to an active server. The management state remains the same.

Step 1 From the menu bar, choose **Admin > General > Data Sources**.

Step 2 Choose the LAN from the LAN table. Click **Move LAN Tasks to another Federated Server**.

Step 3 In the Move LAN Tasks to another DCNM Server dialog box, enter the LAN tasks that need to be moved and specify the DCNM server. All the LAN devices under the selected tasks will be moved.

Remove LAN Task/Switch

Step 1 From the menu bar, choose **Admin > General > Data Sources.**

Step 2 In the Discovery Task column, click the **Remove LAN Task** icon.

Step 3 In the confirmation dialog box, click **Yes** to remove the LAN task.

Delete a Switch

You can also delete an individual switch connected to a DCNM Server.

Step 1 From the menu bar, choose **Admin > General > Data Sources**.

Step 2 In the Switch column, click the **Delete Switch** icon.

Step 3 In the confirmation dialog box, click **Yes** to delete the switch

Toggle between Task and Device view

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Click the **Toggle between Task and Device view** icon.

By default, the Device view is displayed.

Step 3 In the Device view:

- In the Group column, use the drop-down to select the LAN group.
- Click the **Add LAN Task** icon to add a LAN. For more information see the Adding LAN Devices section.
- In the Discovery Task column, click the **Edit LAN Task** icon to edit the LAN task. For more information, see the Editing LAN Devices section.
- In the Discovery Task column, click the **Re-discover LAN** icon to rediscover the LAN. For more information see the Purging LAN section.
- In the Discovery Task column, click the **Remove LAN Task** icon to delete the LAN task. For more information, see the Removing LAN Devices section.
- In the Switch column, click **Re-discover Switch** icon to rediscover the switch.
- In the Switch column, click the **Delete Switch** icon to delete the switch.
- Click the **Toggle between Task and Device view** icon to toggle to the task view

Step 4 In the Task view:

- Under Discovery Task, use the checkbox to select the task.
- Click the **Add LAN Task** icon to add a LAN. For more information see the Adding LAN Devices section.
- Use the checkbox to select the task and then click the **Edit LAN Task** icon at the upper-right corner above the table to edit the LAN task. For more information, see the Editing LAN Devices section.
- Use the checkbox to select the task and then click the **Remove LAN Task** icon at the upper-right corner above the table to delete the LAN task. For more information, see the Removing LAN Devices section.
- Use the checkbox to select the task and then click the **Re-discover LAN** icon at the upper-right corner above the table to rediscover the LAN. For more information see the Purging LAN section.
- Click the **Refresh** icon to refresh the LAN table.
- Click the **Purge unreachable devices or dead links in selected LAN** icon to purge the LAN. For more information see the Purging LAN section.
- Click the **Toggle between Task and Device view** icon to toggle to the device view.
- Click **Re-discover Switch** icon to rediscover the switch.
- Click the **Delete Switch** icon to delete the switch.
- In the Group column, use the drop-down to select the LAN group.

Adding, Editing, Re-discovering and Removing VMware Servers

DCNM Web Client reports information gathered by Cisco Prime DCNM-SAN on any VMware servers supported by Cisco Prime DCNM-SAN.

Note Ensure that the LAN and SAN are discovered before you add the vCenter on the datasource.

This section contains the following:

- Managing a VMware Server, page 3-87
- Removing a VMware Server, page 3-87
- Modifying a VMware Server, page 3-87
- Rediscovering a VMware Server, page 3-87

Managing a VMware Server

You can manage a VMware server from Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin > General > Data Sources**.

You see the list of VMware servers (if any) that are managed by Cisco Prime DCNM-SAN in the table.

Step 2 Click the **Add Virtual Center** icon.

You see the Add VMware dialog box.

Step 3 Enter the Virtual Center Server IP address for this VMware server.

Step 4 Enter the User Name and Password for this VMware server.

Step 5 Click **Add** to begin managing this VMware server.

Removing a VMware Server

You can remove a VMware server from the Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin > General > Data Sources**.

Step 2 Select the check box next to the VMware server that you want to remove and click **Remove Virtual Center** to discontinue data collection for that VMware server.

Modifying a VMware Server

You can modify a VMware server from Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin > General > Data Sources**.

Step 2 Check the check box next to the VMware server that you want to edit and click **Edit Virtual Center** icon.

You see the Edit VMware dialog box.

Step 3 Enter a the User Name and Password.

Step 4 Select managed or unmanaged status.

Step 5 Click **Apply** to save the changes.

Rediscovering a VMware Server

You can rediscover a VMware server from Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Select the check box next to the VMware that you want to rediscover.

Step 3 Click **Rediscover Virtual Center** icon.

Step 4 Click **Yes** in the dialog box.

Adding, editing, removing, rediscovering and refreshing SMI-S Storage

The SMI-S providers are managed using the DCNM Web Client.

This section contains the following:

- Adding SMI-S Provider.
- Editing SMI-S Provider.
- Deleting SMI-S Provider.
- Re-Discover SMI-S Provider.
- Refresh SMI-S Provider

Adding SMI-S Provider

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Click the **Add SMIS Provider** icon.

Step 3 In the Add SMI-S Provider window, use the drop-down to select the Vendor. Only EMC and NetApp are currently supported. Additional SMI-S storage vendors are discovered through a 'best effort' handler using the 'Other' vendor option in the drop-down.

Note At least one valid DCNM license must be provisioned before adding SMI-S storage discovery datasources.

Step 4 Specify the SMI-S Server IP, User Name and Password.

Step 5 Specify the Name Space and Interop Name Space.

Step 6 By default, the Port number is pre-populated. If you select the **Secure** checkbox, then the default secure port number is populated.

When using the Secure mode with EMC, the default setting is mutual authentication. For more information, see EMC's documentation about adding an SSL certificate to their trust store, or set **SSLClientAuthentication** value to '**None**' in the **Security_Settings.xml** config file and then restart the ECOM service.

Step 7 Click **Add**. The credentials are validated and if it's valid the storage discovery starts. If the credential check fails, you will be prompted to enter valid credentials.

Editing SMI-S Provider

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Use the check-box to select the SMI-S provider and click the **Edit SMIS Provider** icon.

Step 3 In the Edit SMI-S Provider window, use the drop-down to select the Vendor.

Note Only EMC and NetApp are currently supported.

Step 4 Specify the SMI-S Sever IP, User Name and Password.

Step 5 Specify the Name Space and Interop Name Space.

Step 6 By default, the Port number is pre-populated. If you select the **Secure** checkbox, then the default secure port number is populated.

Step 7 Click **Apply**. The Storage Discovery is stopped and a new task is created using the new information and the Storage Discover is re-started.

Deleting SMI-S Provider

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Use the check-box to select the SMI-S provider and click the **Remove SMIS Provider** icon.

The provider is removed and all data associated with the provider is purged from the system.

Re-Discover SMI-S Provider

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Use the check-box to select the SMI-S provider and click the **Re-discover SMIS Provider** icon

Refresh SMI-S Provider

Step 1 From the menu bar, choose **Admin** > **General** > **Data Sources**.

Step 2 Use the check-box to select the SMI-S provider and click the **Refresh Table** icon.

The providers are re-discovered.

Viewing Log Information

This feature enables you to view the Cisco Prime DCNM Web Client log. These processes have no corresponding GUI that allows you to view information about these log files. If you see errors, preserve these two files for viewing.

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

Step 1 From the menu bar, choose **Admin** > **General** > **Logs**.

You see a list of viewable logs in the left column.

Step 2 Click a log file to view it.

Configuring Cisco Prime DCNM-SAN Server Properties

To configure Cisco Prime DCNM-SAN Server properties

Step 1 From the menu bar, choose **Admin > General > Server Properties**.

Step 2 Follow the on-screen instructions and click **Apply** to confirm the changes.

While connecting to some switches if the connection is getting timed out, in the #CLI session channel type, change default the cli.channel.type value from **exec** to **shell**.

Note After configuring the server properties, you need to restart the DCNM server only if you receive a notification stating that the server must be restarted.

Configuring SFTP/TFTP Credentials

You can configure the SFTP/TFTP credentials for the File store.

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

Step 1 From the menu bar, choose **Admin** > **General** > **SFTP/TFTP Credentials**.

You see the SFTP/TFTP credentials page.

TFTP Credentials option is disabled for DFA deployment of Open Virtual Appliance and ISO installers.

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

Note You must have a SFTP server on the DCNM Server to perform backup operation. The SFTP directory must be an absolute Linux/SSH path format and must have read/write access to the SFTP User.

a. Enter the SFTP Username and SFTP Password.

b. Enter the **SFTP Directory path**.

The path must be in absolute Linux path format.

c. From the Verification Switch drop-down, select the switch.

d. Click **Apply** to apply the configuration.

e. Click **Verify and Apply** to verify and apply 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 **Config > Job > Job Status History** to view the number of successful and unsuccessful switches.

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

Cisco Prime DCNM uses an internal 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 **Admin > DataSources** page.

a. From the Verification Switch drop-down, select the switch.

b. Click **Apply** to apply the configuration.

c. Click **Verify and Apply** to verify and apply the configuration. If there are any failures during the verification, the new changes will not be stored.

Step 4 From the menu bar, choose **Config > Jobs > Job Status History** to view individual device verification status.

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

Managing Switch Groups

Beginning with Cisco NX-OS Release 6.x, you can configure switch groups by using Cisco Prime DCNM Web Client. 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 Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin > General > Switch Groups**.

Step 2 Click the **Add Group** icon or press the Insert key on your keyboard.

Note A field appears that allows you to enter the name for the switch group. The Insert key does not work unless you highlight the group table first.

Step 3 Enter the name of the switch group and click outside the text field or press the Return key to complete adding the switch group. Press the Esc key on your keyboard to discard the text input and exit.

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

Renaming a Group

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

Step 1 Double-click on the switch group name that you want to rename.

Step 2 Enter a new name to rename the group.

Note The name of the group cannot contain any of these special characters: ()<>,;:\\\[]`~!#$% *=}|/?.

Step 3 Press the **Return** key to apply changes or press the Esc key on your keyboard to discard the modification.

Deleting a Group or a Member of a Group

You can delete group(s) and/or member(s) of a group from the Cisco Prime 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.

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

Moving a Switch to Another Group

Step 1 Use the checkbox to choose a switch from the group.

Step 2 Select the **Move the selected Switch/Fabric to Group** icon.
The Move LAN Member dialog box appears.

Step 3 Select the switch group from the list and click **Apply**.

Moving a Switch Group to Another Group

Step 1 Use the checkbox to choose a switch group.

Step 2 Click **Move Switch/Fabric to selected Group** icon.
The Move LAN Member Group dialog box appears.

Step 3 Select the switch group from the list and click **Apply**.

Managing Custom Port Groups

Custom Port groups aids you to test the performance of the interfaces in the group. You can view the defined custom ports and their configurations from **Admin > Custom Port Groups** on the Cisco Prime DCNM Web Client.

This section includes the following topics:

- Adding Custom Port Groups, page 3-93

Adding Custom Port Groups

You can add a custom port group from the Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin > Custom Port Groups.**

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

Step 3 Enter the name for the custom port group in the Add Group Dilog.

A custom port group is created in the Defined Groups block.

Configuring Switch and Interface to the Port Group

You can configure the custom port group to include switches and their interfaces.

Step 1 From the menu bar, choose **Admin > Custom Port Groups.**

Step 2 In the Defined Groups block, select the port group for which you need to add the switch and interfaces.

Step 3 In the Configuration block, click the **Add Group Member** icon.

The Port Configuration window appears for the selected Custom Port Group.

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

The list of available Interfaces appears.

Step 5 Select all the interfaces for which you need to check the performance.

Step 6 Click **Submit**.

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

Generating Reports for the Custom Port Groups

You can generate the reports to monitor the performance of the interfaces in the custom port group.

Step 1 From the menu bar, choose **Reports > Generate.**

Step 2 From the Scope dropdownlist, select the port group for which you need to generate the performance report.

Step 3 Generate the Performance report. For information about how to Generate Reports, see Generating a Report.

Step 4 Verify if the report is generated for all the interfaces that were added in the custom port group.

Removing Port Group Member

You can remove or delete the port group member from the Custom Port group.

Step 1 From the menu bar, choose **Admin > Custom Port Groups.**

Step 2 In the Defined Groups block, select the port group for which you need to add the switch and interfaces.

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

Step 4 In the Defined Groups block, select the group for which you which must be deleted. Click **Remove Group Member** icon.

A confirmation window appears.

Step 5 Click **Yes** to delete the member from the custom port group .

Removing Port Group

You can remove or delete the port group from the Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin > Custom Port Groups.**

Step 2 In the Defined Groups block, select the group which must be deleted. Click **Remove Group** icon.

A confirmation window appears.

Step 3 Click **Yes** to delete the custom group.

Managing Licenses

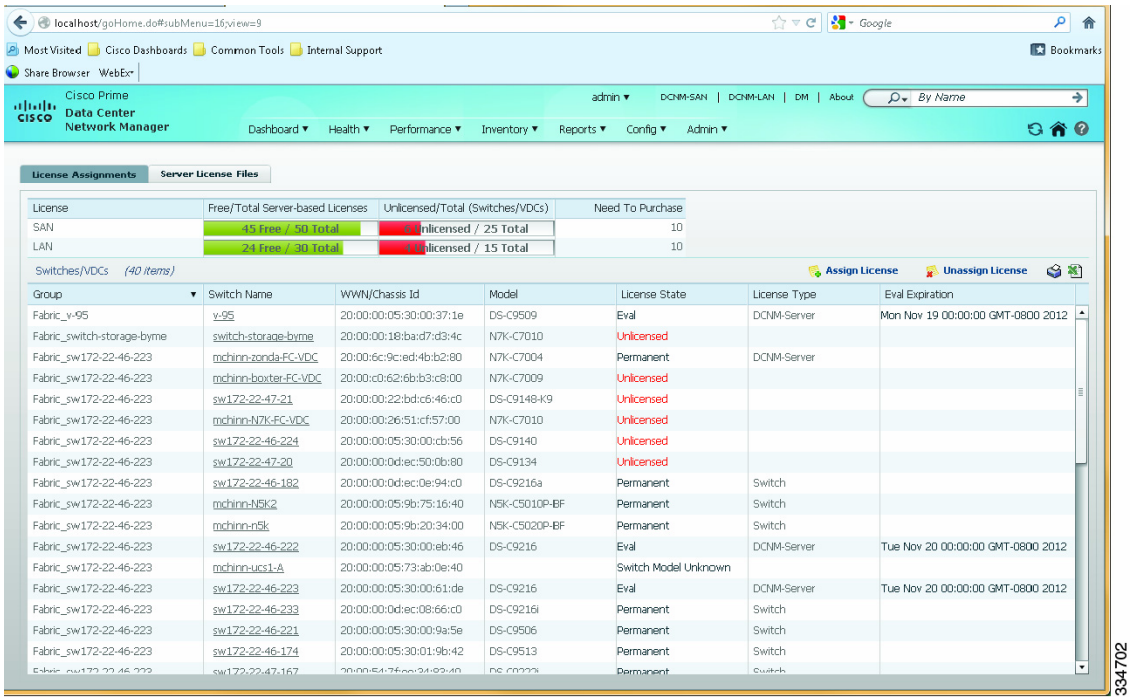
This section includes the following topics:

Viewing Licenses Using the Cisco Prime DCNM Wizard

You can view the existing Cisco Prime DCNM licenses by **DETAILED STEPS**selecting **Admin > License** to start the license wizard.

Figure 3-2 displays the license information.

Figure 3-2 Cisco Prime DCNM Licenses



Note By default, the Switch Licenses tab appears.

Table 3-6 displays the Cisco Prime DCNM server license fields.

Table 3-6 Cisco Prime DCNM Server License Files

Field	Description
File Name	Name of the license file.
Feature	Describes the feature name specified in the license file. The following values are supported: • DCNM-LAN • DCNM-SAN • DCNM-SAN-LAN • LAN-ENT-N7K
PID	Describes the product ID found in the vendor string of the license file. For example, DCNM-N7K-K0 is an enterprise license for Cisco Nexus 7000 series switches.
SAN (Free or Total)	Lists the number of SAN licenses used and available.

Table 3-6 Cisco Prime DCNM Server License Files (continued)

Field	Description
LAN (Free or Total)	Lists the number of LAN licenses used and available.
Eval Expiration	Displays the expiry date of the license. **Note** Text in the eval expiration field will be in red for licenses that expire in seven days.

Table 3-7 displays the Cisco Prime DCNM switch license fields.

Table 3-7 Cisco Prime DCNM Switch Licenses

Field	Description
Group	Displays if it is a fabric or LAN group.
Switch Name	Displays the name of the switch.
Model	Displays the model of the device. For example, DS-C9124 or N5K-C5020P-BF.
License State	Displays the license state of the switch that can be one of the following: • 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 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 will be 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 Prime DCNM Licenses

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

Step 1 Choose **Admin** > **License** to start the license wizard.

Step 2 Choose the **Server License Files** tab.
The valid Cisco Prime DCNM-LAN and DCNM-SAN license files appear.

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 will be uploaded to the server machine, 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 Prime 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 will be counted.

Assigning Licenses

BEFORE YOU BEGIN

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

Step 1 **DETAILED STEPS**Choose **Admin > License** to start the license wizard.
You see the licenses table.

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.

DETAILED STEPS

Step 1 Choose **Admin > License** to start the license wizard.
You see the licenses table.

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

Step 3 Click **Unassign License**.

Viewing Server Federation

Step 1 From the menu bar, choose **Admin** > **General** > **Federation**.

The list of Servers along with its Status, Local Time and Data Sources are displayed.

Step 2 Use the **Enable Automatic Failover** checkbox to turn on/off the failover functionality.

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

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

Note Before upgrading Cisco Prime DCNM, ensure that **Enable Automatic Failover** is unchecked. Otherwise, if one server within the federation is down, the devices discovered by the server will be moved to the other DCNM server which comes up first after upgrade. To prevent the auto move for DCNM upgrade, you need to disable the auto move on all DCNMs within the federation, and then upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the auto move again.
To enable / disable Auto Move, please go to **Admin > Federation** from DCNM web page, click on the checkbox at top left for **Enable Automatic Failover**.

Configuring AAA Properties

To configure AAA properties,

Step 1 From the menu bar, choose **Admin** > **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.

Local

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

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

Radius

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+

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

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

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

Step 3 (Optional) Specify the Secondary and Tertiary Switch name and click **Apply** to confirm the authentication mode.

LDAP

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.

Step 4 Enter a valid Username and Password.

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 Click **Apply** to apply the LDAP configuration.

Adding and Removing Users

You can use Cisco Prime DCNM Web Client to add and remove Web Client users.

This section contains the following:

- Adding Local Users, page 3-100
- Editing a User, page 3-100
- Removing a User, page 3-100

Adding Local Users

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

Step 2 Click **Add**.

You see the Add User dialog box.

Step 3 Enter the username in the Username field.

Note The username guest is a reserved name (case insensitive). 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 2through 7 to continue adding users.

Editing a User

Step 1 From the menu bar, choose **Admin** > **Management Users** > **Local**.

Step 2 Use the checkbox to select a user and click the **Edit Local User** icon.

Step 3 In the Edit Local 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.

Removing a User

Step 1 From the menu bar, choose **Admin** > **Management Users** > **Local**.

Step 2 Select the check box next to the user(s) you want to remove and click **Remove**.

Managing Clients

You can use the DCNM Web Client to disconnect DCNM Client Servers.

Step 1 From the menu bar, click **Admin>Clients**.

A list of DCNM Servers are displayed.

Step 2 Use the check box to select a DCNM server and click **Disconnect Client** icon to disconnect the DCNM server.

Note You cannot disconnect a current client session.

Performance Manager 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 Prime DCNM Web Client to add and remove performance collections. The switch has to be licensed and in the Managed Continuously state before a collection for the switch can be created.

To add a collection follow these steps:

Step 1 From the menu bar, click **Admin>Collections**.

Step 2 Under Generate a threshold event when traffic exceeds % of capacity, use the checkbox to specify the **Critical at** and **Warning at** values. User can also use the **For ISL/Trunk Only** checkbox to limit the threshold events generated to ISL and Trunk events only and then click **Apply**.

Step 3 In the Licensed Fabrics panel, use the checkboxes to select the Fabric, ISLs/NPV Links, Hosts, Storage, FC Flows and FC Ethernet to enable performance collection for these data types.

Step 4 In the Licensed LAN Switches panel, use the checkboxes to enable performance data collection for **Trunks**, **Access** and **Errors & Discards**.

Step 5 Use the checkboxes to select the type(s) of LAN switches for which you want to collect performance data.

Step 6 Click **Apply** to save the configuration.

Step 7 In the confirmation dialog box, click **Yes** to restart the performance collector.

Configuring the RRD Database

Configuring the Round Robin Database (RRD) allows you to set the intervals at which data samples are collected. After applying the configuration, the database storage format is converted to a new format at those intervals. Because database formats are incompatible with each other, you must copy the old data (before the conversion) to the $INSTALLDIR/pm directory. See the "Importing the RRD Statistics Index, page 3-102" topic.

Step 1 From the menu bar, choose **Admin** > **Performance** > **Databases**.

You see the Performance Database (collection interval) page.

Step 2 In the top row of the Days column, enter the number of days to collect samples at 5-minute intervals.

Step 3 In the second row of the Days column, enter the number of days to collect samples at 30-minute intervals.

Step 4 In the third row of the Days column, enter the number of days to collect samples at 2-hour intervals.

Step 5 In the bottom row of the Days column, enter the number of days to collect samples at 1-day intervals.

As of Cisco SAN-OS Release 3.1(1) and later releases, you can configure the sampling interval for ISLs. Select a sampling interval from the ISLs drop-down list.

Step 6 Click **Apply** to apply your changes, or click **Defaults** to reset the file sizes to the default values.

If you are applying new values, or if the current values are not the default values, you see a message indicating that the conversion of the RRD files take a certain amount of time and that the database is unavailable until then. The time it takes depends on the difference between the old and new values.

Note The system allows you to convert data, one process at a time. When you start converting the data, the Apply and Default buttons change to Refresh and Cancel so that another process cannot be inadvertently started. The display is the same for all browsers that access the server during this time. Click Refresh to view the latest progress. Click Cancel to cancel the process of converting the data. If the job is successfully canceled, you see the Apply and Default buttons again. If the cancel job is not successful, you see a message indicating that the cancellation has failed.

If you want to perform this procedure, perform it before collecting a lot of data because data conversion can take a long time.

Importing the RRD Statistics Index

Step 1 Stop Cisco Prime DCNM-SAN Server.

Step 2 Copy the original RRD file into **$INSTALLDIR/pm/db**.

Step 3 Run $INSTALLDIR/bin/pm.bat s.

Step 4 Restart Cisco Prime DCNM-SAN and add the fabric.

Configuring Other Statistics

Step 1 From the menu bar, choose **Admin** > **Performance** > **Others**.

You see the Others page.

Step 2 Click **Add**.

You see the Add SNMP Statistic 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 Type drop-down list, select the type.

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

Viewing Events Registration

To enable Send Syslog, Send Traps and Delayed Traps you need to configure the following in the DCNM-SAN client:

- Enabling Send Syslog - Log into the DCNM-SAN client. In the Physical Attributes pane, Select **Events>Syslog>Servers**. Click the **Create Row** icon, provide the required details and click **Create**.
- Enabling Send Traps - Log into the DCNM-SAN client. In the Physical Attributes pane, Select **Events>SNMP Traps>Destination**. Click the **Create Row** icon, provide the required details and click **Create**.
- Enabling Delayed Traps - Log into the DCNM-SAN client. In the Physical Attributes pane, Select **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.

Step 1 From the menu bar, choose **Admin > Events > 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 **Admin>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 select, the events will not be displayed in the events page of the Web client.

Step 4 The columns in the second table displays the following:

- Switches sending traps
- Switches sending syslog
- Switches sending syslog accounting
- Switches sending delayed traps

Adding Notification Forwarding

This section contains the following:

Adding Notification Forwarding

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

Cisco Prime DCNM Web Client forwards fabric events through e-mail or SNMPv1 traps.

Note Test forwarding will only work for the licensed fabrics.

Step 1 From the menu bar, choose **Admin > Events > Forwarding**.

Step 2 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 3 Select the **Enable** checkbox to enable events forwarding.

Step 4 Specify the **SMTP Server** details and the **From** e-mail address. Click **Apply** to save the configuration or in the Apply and Test icon, use the drop-down to select the fabric and click **Apply and Test** to save and test the configuration.

Step 5 Select the **Snooze** checkbox and specify the Start date and time and the End date and time. Click **Apply** to save the configuration.

Step 6 Click the **Add Forwarder** icon.

You see the Add Notification dialog box.

Step 7 In the Forwarding Method, choose either **E-Mail** or **Trap**. If you choose Trap, a Port field is added to the dialog box.

Step 8 In the **Address** field, enter the IP address.

Step 9 From the **Scope** drop-down list, choose the fabric or LAN group for notification.

Step 10 In the Source field select **DCNM** or **Syslog**.

If you select DCNM, then:

Step 1 In the VSAN Scope, choose either **All** or **List**.

Step 2 From the Type drop-down list, choose an event type.

Step 3 Check the **Storage Ports Only** check box to select only the storage ports.

Step 4 From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.

Step 5 Click **Add** to add the notification.

If you select Syslog, then:

Step 1 In the **Facility** list, select the syslog facility.

Step 2 Specify the syslog **Type**.

Step 3 In the **Description Regex** field, specify a description that needs to be matched with the event description.

Step 4 From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.

Step 5 Click **Add** to add the notification.

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

The traps sent by Cisco Prime 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.

Step 1 From the menu bar, choose **Admin > Events > Forwarding**.

Step 2 Select the check box in front of the notification that you want to remove and click **Remove**.

Configuring EMC CallHome

Cisco Prime DCNM Release 7.1.x DCNM enhances EMC call home messages. DCNM version information is displayed in with the call home message.

You can configure EMC Callhome from the Cisco Prime DCNM Web Client for EMC supported SAN switches.

DETAILED STEPS

Step 1 From the menu bar, choose **Admin > Events > EMC CallHome.**

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

Step 3 Use the check box to select the fabrics.

Step 4 Enter the general e-mail information.

Step 5 Click the **Apply** to update the e-mail options.

Step 6 Click **Apply and Test** to update the e-mail options and test the results.

Event Suppression

Cisco Prime DCNM allows you to suppress the specified events based on the user-specified suppressor rules. Such events will not be displayed on the Cisco Prime DCNM Web Client and SAN Client. The events will neither be persisted to DCNM database, nor forwarded via email/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
- Delete Event Suppression Rule
- Modify Event Suppression Rule

Add Event Suppression Rules

To add rules to the Event Suppression, do the following tasks:

Step 1 From the menu bar, select **Admin > Event Suppression**.

Step 2 In the Add Event Suppressor Rule window, specify the **Name** for the rule.

Step 3 Select the required **Scope** for the rule based on the event source.

You can choose SAN, LAN, Port Groups or Any. For SAN and LAN, select the scope of the event at the Fabric or Group or Switch level. User can only select group(s) for Port Group scope. If use selects "Any" as the scope, the suppressor rule will be applied globally.

Step 4 Enter the **Facility** name or choose from the **SAN/LAN Switch Event Facility** List.

If you do not specify a facility, wild card will be applied.

Step 5 From the drop down list, select the Event **Type**.

If you do not specify the event type, wild card will be applied.

Step 6 In the **Description Matching** field, specify a matching string or regular expression.

The rule matching engine uses regular expression supported by Java Pattern class to find a match against an event description text.

Step 7 (Optional) Check the **Active Between** box and select a valid time range during which the event will be suppressed.

By default, the time range is not enabled, i.e., the rule will be always active.

Note In general, user should not suppress accounting events. Suppressor rule for Accounting events might 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 password synchronization between DCNM and managed switches. To suppress Accounting events, user can browse web client to Suppressor table and invoke **Add Event Suppressor Rule** dialog window.

Note You can go to **Health > Events** table of Web Client to create a suppressor rule for a known event. While 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:

Step 1 From the menu bar, select **Admin > Event 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:

Step 1 From the menu bar, select **Admin > Event Suppression**.

Step 2 Select the rule from the list and click **Edit** icon.

You can edit the **Facility**, **Type**, **Description Matching** string, and the **Valid time range**.

Step 3 Click **Apply** to save the changes,

Using Cisco Prime DCNM Web Client with SSL

By default, Cisco Prime DCNM Web Client uses HTTP. If you want to install SSL certificates and use Cisco Prime DCNM Web Client over HTTPS (using TCP port 443 or another custom port), you need a certificate for each external IP address that accepts secure connections. You can purchase these certificates from a well-known Certificate Authority (CA).

To enable SSL, you must set up the keystore to use either a self-signed certificate or a certificate from a trusted third-party company such as VeriSign.

This section includes the following topics:

Using a self signed SSL Certificate

Step 1 From command prompt, navigate to **<DCNM install root>/dcm/java/jre1.7/bin/**.

Step 2 Rename keystore located at

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks

to

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old

Step 3 Generate a self signed certificate using following command

keytool -genkey -trustcacerts -keyalg RSA -alias sme -keystore <DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 4 Stop the DCNM services.

Step 5 Restart the DCNM Services.

Using a SSL Certificate when certificate request is generated using OpenSSL

Step 1 From command prompt, navigate to <DCNM install root>/dcm/java/jre1.7/bin/

Step 2 Rename keystore located at

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks

to

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old

Step 3 Generate the RSA private key using openssl

openssl genrsa -out dcnm.key 2048

Step 4 Generate a certificate request using following command:

openssl req -new -key dcnm.key -out dcnm.csr

Step 5 Submit the CSR to certificate signing authority to digitally sign it. CA provides the certificate and signing certificate in as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to Step 6 to convert it to PEM format. If CA provided PEM format then go to Step 7.

Step 6 Convert the PKCS 7 certificate chain to X509 certificate chain

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Step 7 Convert the X509 certificate chain and private key to PKCS 12 format

openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password fmserver_1_2_3 -name sme

Step 8 Import the intermediate certificate first, the root certificate, and finally the signed certificate by using the command:

keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore <DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -deststoretype JKS

Step 9 Stop the DCNM services.

Step 10 Restart the DCNM Services.

Using a SSL Certificate when certificate request is generated using Keytool

Step 1 From command prompt, navigate to **<DCNM install root>/dcm/java/jre1.7/bin/**.

Step 2 Rename keystore located at

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks

to

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old

Step 3 Generate the public-private key pair in DCNM keystore

keytool -genkeypair -alias sme -keyalg RSA -keystore "<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3 -storepass fmserver_1_2_3

Step 4 Generate the certificate-signing request (CSR) from the public key generated in Step 1.

keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3

Step 5 Submit the CSR to certificate signing authority to digitally sign it. CA provides the certificate and signing certificate in as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to Step 6 to convert it to PEM format. If CA provided PEM format then go to Step 7.

Step 6 Convert the PKCS 7 certificate chain to X509 certificate chain using openssl

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Step 7 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

keytool -importcert -trustcacerts -file cert-chain.pem -keystore <DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -alias sme

Step 8 Stop the DCNM services.

Step 9 Restart the DCNM Services.

SSL for Federated (High Availability) setup

Step 1 Generate the SSL certificate for primary node and import all the certificates at the appropriate location as mentioned above.

Step 2 Copy the **fmserver.jks** from the primary node located at **<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration**.

Step 3 Paste the **fmserver.jks** to the secondary node located at **<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration**.

Fabric—General Settings

Note These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

You can specify the general settings for the Fabric.

Step 1 From the menu bar, select **Admin > Fabric > General Settings**.

Step 2 Specify the Fabric settings based on the required configuration and click **Apply**.

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

Step 4 Click Health to view status of the Fabric components.

You can also configure the following settings for the Fabric.

- Border Leaf Settings
- Border Leaf Device Pairing
- Border Leaf Extended Partitions
- POAP Settings
- L2 Segment ID Range Management
- Mobility Domains

Border Leaf Settings

Border Leaf Settings allows you to globally enable Border Leaf/Edge Router auto-configuration, and specify its settings such as load balancing algorithm and redundancy factor.

By default, the Border Leaf/Edge Router auto configuration is disabled.

From the menu bar, select **Admin > Border Leaf Settings**.

- Configuring Border Leaf Settings
- Creating an Edge Router
- Connect New Border leaf to the Edge Router
- Deleting Edge Router/Border leaf devices

Configuring Border Leaf Settings

Step 1 Check the **Enable Border Leaf/Edge Router Auto-configuration** to globally enable Border Leaf/Edge Router auto-configuration.

Step 2 Specify the autonomous system (AS) number to compose the Route Target using the BGP protocol. This AS number is the same across the fabric.

Note If you do not specify AS number, DCNM will be disabled.

Step 3 From the **Load Balancing Algorithm** list, select the algorithm that must be used by DCNM to determine whether to choose border leaf based on the least load, fair share, round robin, resource consumption, speed or other criteria.

Note In Cisco Prime DCNM Release 7.1 (1), only Round Robin algorithm is supported.

If your setup has vPC pair of border leaf, the vPC pair is chosen with priority over Round Robin. If a switch that is part of vPC pair is selected for partition (VRF) extension, DCNM will also select the vPC pair for the same partition (VRF) extension for load balancing.

Step 4 Specify the **Redundancy Factor** to ensure VRFs is extended on the specified number sets of border leaf switch.

Note The selected number of Border Leaf/Edge Router pairs for partition (VRF) extension also depends on the Border Leaf/Edge Router pairing topology. Therefore the number of pairs is equal to or greater than the specified redundancy factor.

Border Leaf Device Pairing

This feature allows you to pair Border Leaf with the Edge Router and specify device associated configurations such as interface between Border Leaf and Edge Router. DCNM selects appropriate Border Leaf/Edge Router pairs during partition (VRF) extension.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Table 3-2

Field	Description
Edge Router/Border Leaf	Specifies the Name of the Edge Router or the connected Border Leaf.
IP Address	Specifies the IP address of the Border Leaf/Edge Router.
Interface Name/Port Channel	Specify the interface name or port channel between Border Leaf and Edge Router.
Profile Name	Specifies the default profile name.
Type	Specifies if the device is an Edge Router configuration or a Border Leaf configuration.
Partition Utilization	Specifies the partitions utilized and the maximum partitions available for the device.
Add	Allows you to add a Border Leaf/Edge Router. For more information, see Creating an Edge Router.
Edit	Allows you to edit a Border Leaf/Edge Router.
Delete	Allows you to delete a Border Leaf/Edge Router. For more information, see Deleting Edge Router/Border leaf devices.
View Profile	Allows you to view the profile created
Refresh	Refreshes the list of switches.
Show Filter	Filters list of switches based on the defined value for each column.

Table 3-2

Field	Description
Print	Prints the list of devices and their details.
Export	Exports the list of devices and their details to a Microsoft Excel spreadsheet.

- Creating an Edge Router
- Connect New Border leaf to the Edge Router
- Deleting Edge Router/Border leaf devices

Creating an Edge Router

Step 1 From the menu bar, select **Config > Border Leaf Device Pairing**.

Step 2 Click **Add**. Select **Edge Router**.

Step 3 To configure the Edge Router:

a. Use the radio button to select **Configure an Edge Router**.

Note The **Configure an Edge Router** option will be selected by default.

b. Select **Notify Edge Router when relevant partitions are changed** to notify the Edge Router.

c. Select the **Device Name** from the drop-down list to identify an Edge Router.

d. Specify the **IP Address** for the Edge Router.

e. Specify the **Maximum Number of Partitions** required for the Edge Router.

Step 4 To configure a **Border PE**:

a. Use the radio button to select **Configure a Border PE**.

b. Select **Notify Edge Router when relevant partitions** are changed to notify the Edge Router.

c. Select the **Device Name** from the drop-down list to identify an Edge Router.

d. Specify the **IP Address** for the Edge Router.

e. Specify the **Maximum Number of Partitions** required for the Edge Router.

f. Define the Profile Parameters.

- asn—specifies the autonomous system (AS) number for the Border PE
- vrfSegmentId—specifies the vrf segment ID.
- rsvdGlobalAsn—specifies the reserved global autonomous system number.
- dciId—specifies the Edge Router ID for the Border PE
- vrfName—Specifies the vrf name

Note Note: The value for vrfName must be of the format 'organizationName:partitionName'.

Step 5 Click **OK** to save the configuration.

Connect New Border leaf to the Edge Router

Step 1 From the menu bar, select **Config > Border Leaf Device Pairing**.

Step 2 Click **Add**. Select **Border Leaf**.

Step 3 Define the parameters for the Border leaf configuration and edge router configuration for pairing.

Field	Description
Name	Select the name from the drop-down list for the Border leaf.
IP Address	The IP address is auto-populated based on the selected Border Leaf.
Port Channel or the Interface Name	Specify the interface name or port channel between Border Leaf and Edge Router.
Maximum Number of Partitions	Specifies the number of partitions required for the configuration
Default Profile Name	Select the default profile name from the drop-down list to apply for the profile.
Notify Border Leaf when relevant partitions	Select to notify the Border Leaf when relevant partitions are created.

Step 4 Click **OK** to connect the new border leaf device to the Edge router.

Deleting Edge Router/Border leaf devices

Step 1 From the menu bar, select **Config > Border Leaf Device Pairing**.

Step 2 Select the Edge Router/Border leaf device definitions from the list and click **Delete**.

Step 3 Click **Yes** to confirm and delete the profile.

Border Leaf Extended Partitions

This screen lists the extended partitions, selected Border Leaf/Edge Router pairs, and their corresponding profiles and configurations. From the menu bar, select **Config > Extended Partitions**.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Field	Description
VRF	Specifies the VRF name for the extended partition.
Organization	Specifies the name of organization which the extended partition belongs to.
Partition	Specifies the name of the partition that is extended.

Field	Description
Redundancy Factor	Specifies the run-time redundancy factor for that partition extension.
Edge Router	Specifies the name of the Edge Router.
Edge Router IP Address	Specifies the IP address of the Edge Router device.
Edge Router Profile	Specifies the default profile for the edge router.
Border Leaf (BL)	Specifies the name of the Border Leaf device
BL IP Address	Specifies the IP address of the Border Leaf device.
BL Profile	Specifies the default profile for the border leaf device.

POAP Settings

This allows you to set common parameters which will be populated as default values in POAP templates. For a new POAP template, values defined in this global settings page, will be automatically pre-populated. From the menu bar, select **Admin->Fabric->POAP Settings**.

Specify the parameters for the following fields:

Field	Description
MGMT_PREFIX	Specify the Management prefix.
DEFAULT_GATEWAY	Specify the default gateway.
MANAGEMENT_VLAN	Specify the management VLAN.
LDAP_SERVER_NAME	Specify the LDAP server name.
LDAP_SERVER_IP	Specify the LDAP server IP address.
LDAP2_SERVER_NAME	Specify the secondary LDAP server name.
LDAP2_SERVER_IP	Specify the secondary LDAP server IP address.
LDAP_USERNAME	Specify the LDAP username.
LDAP_PASSWORD	Specify the LDAP password.
XMPP_SERVER	Specify the XMPP server name.
XMPP_SERVER_IP	Specify the XMPP IP address.

Step 4 Click **Apply** to save the POAP settings for the fabric.

Fabric Encapsulation Settings

To configure encapsulation settings, do the following:

Step 1 From the menu bar, select **Admin > Fabric Encapsulation Settings**.

Step 2 Select **Enable Fabric Path Encapsulation** to enable FabricPath-based Auto-Configuration on Nexus 5600, Nexus 6000 and Nexus 7000 Series devices.

You can choose from the combination of available leaf networks.

Step 3 Select **Enable VxLAN Encapsulation** to enable VxLAN-based Auto-Configuration on Nexus 5600, Nexus 7000 and Nexus 9000 Series devices.

You can choose from the combination of available leaf network in your topology. The first three options are related to "Phantom-RP with PIM BIDIR". The second three options are related to "Anycast-RP PIM ASM/SSM".

a. In the **Multicast Group Subnet Range** field, specify the Multicast IP Address with subnet for the multicast group.

   This Multicast Group address range is shared between L2 and L3. This field is auto-populated from the Network page at **Config > Auto-Configuration > Networks** section. However, the value can be modified.

b. In the **Number of Rendezvous Points (RPs)** field, to divide the multicast group subnet into buckets, which the user can configure.

   The valid value for RPs are 1, 2, 4, and 8.

c. The **RPx Multicast Group Subnet** field is auto-populated based on Multicast Group Subnet. "X" is the RP count.

   This is applicable only for Phantom-RP with PIM BIDIR.

d. In the **RPx Phantom IP Address** field, enter the Phantom IP Addresses for the RPs. "X" is the RP count.

   This is applicable only for Phantom-RP with PIM BIDIR.

e. In the **RPx IP Address** field, enter the RP IP Addresses for the RPs. "X" is the RP count.

   This is applicable only for Anycast-RP PIM ASM/SSM.

f. In the **Anycast IP Address** field, enter the Anycast IP Address.

   This is applicable only for Anycast-RP PIM ASM/SSM.

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

This settings are used during Auto-Configuration and POAP.

Based on the selected option, the following profiles will be loaded in Partition/Network screens.

- FabricPath with N5600/N6K Leaf Network–The profiles from profiles(FPVLAN) table
- FabricPath with N7K Leaf Network–The profiles from profilesBridgeDomain(FPBD) table
- FabricPath with N5600/N6K & N7K Combined Leaf Network–The common profiles from profiles(FPVLAN) & profilesBridgeDomain(FPBD) table
- VXLAN with N5600 Leaf Network–The profiles from profilesIPFabric(IPVLAN) table
- VXLAN with N7K Leaf with PIM Bidir Network–The profiles from profilesIPBridgeDomain(IPBD) table
- VXLAN with N5600 & N7K Combined Leaf Network–The common profiles from profilesIPFabric(IPVLAN) & profilesIPBridgeDomain(IPBD) table
- VXLAN with N7K Leaf with PIM ASM Network–The profiles from profilesIPBridgeDomain(IPBD) table
- VXLAN with N9K Leaf Network–The profiles from profilesIPFabric(IPVLAN) table
- VXLAN with N7K & N9K Combined Leaf Network–The common profiles from profilesIPFabric(IPVLAN) & profilesIPBridgeDomain(IPBD) table

Based on the encapsulation option, the following profiles will be loaded in Border Leaf/BorderPE/Edge Router screens.

- FabricPath–The profiles from profilesBridgeDomain(FPBD) table
- VXLAN–The profiles from profilesIPBridgeDomain(IPBD) table

Note Cisco Prime DCNM Release 7.2(2) is packaged with the following profiles:

- VXLAN-EVPN configuration profiles for Nexus 5600, Nexus 7000, and Nexus 9000 Series Leaf Network.
- FabricPath configuration profiles for Nexus 5660, Nexus 6000, and Nexus 7000 Series Leaf Network.

  The universal network/partition profiles is supported for the VXLAN-EVPN-based standalone Fabric.

L2 Segment ID Range Management

Cisco Prime DCNM allows you to create a new Segment ID range, and map the orchestrator ID. DCNM will associate the range with the specified orchestrator ID.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Field	Description
Orchestrator Name	Specifies the Orchestrator name.
Section ID Range	Specifies the segment ID range for that Orchestrator. The Segment ID range is unique for all Orchestrators. The default Segment ID range cannot be used for any orchestrator.
Add	Allows you to add a new Orchestrator.
Edit	Allows you to edit the selected Orchestrator and segment ID range.
Delete	Allows you to delete the Orchestrator.
Refresh	Refreshes the list of Orchestrators.
Show Filter	Filters list of switches based on the defined value for each column.
Print	Prints the list of Orchestrator and their details.
Export	Exports the list of Orchestrators and their details to a Microsoft Excel spreadsheet.

- Add Orchestrator
- Modify Orchestrator
- Delete Orchestrator

Add Orchestrator

Step 1 From the menu bar, select **Admin > L2 Segment ID Range Management**.

Step 2 Click **Add** to add a new orchestrator.

Step 3 In the **Orchestrator Name** field, specify the name for the Orchestrator.

Step 4 In the Segment ID Range field, specify Segment ID range to be associated with the Orchestrator.

By default, DCNM continues to support the default Segment ID range defined in the **DCNM Admin > Fabric** page.

Modify Orchestrator

Step 1 From the menu bar, select **Admin > L2 Segment ID Range Management**.

Step 2 Select the orchestrator from the list and click **Edit**.

Step 3 Update and click **OK** to save the settings.

Delete Orchestrator

Step 1 From the menu bar, select **Admin > L2 Segment ID Range Management**.

Step 2 Select the orchestrator from the list and click **Delete**.

Step 3 Click **Yes** to delete the orchestrator.

Mobility Domains

Cisco Prime DCNM allows you to create mobility domains to configure a Mobility Doman Network. The Mobility Domains configured on this page can be used in Config > Auto-Configuration > Networks page.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Field	Description
Mobility Name	Specifies the name for the mobility domain.
Detectable VLAN Range	Specifies detectable VLAN range for the particular mobility domain.
Add	Allows you to add a new mobility domain.
Edit	Allows you to edit the selected mobility domain and the VLAN range.
Delete	Allows you to delete the mobility domain.
Refresh	Refreshes the list of mobility domains.
Show Filter	Filters list of domains based on the defined value for each column.

Field	Description
Print	Prints the list of mobility domains and VLAN range.
Export	Exports the list of mobility domains and their details to a Microsoft Excel spreadsheet.

- Add Mobility Domains
- Modify Mobility Domains
- Delete Mobility Domains

Add Mobility Domains

Step 1 From the menu bar, select **Admin > Mobility Domains**.

Step 2 Click **Add** to add a new mobility domain.

Step 3 In the **Mobility Domain Name** field, specify the name for the Mobility Domain.

Step 4 In the **Detectable VLAN Range** field, specify the VLAN IP address range for mobility domain.

Step 5 Click **OK** to add a mobility domain.

Modify Mobility Domains

Step 1 From the menu bar, select **Admin > Mobility Domains**.

Step 2 Select the mobility domain from the list and click **Edit**.

Step 3 Update and click OK to save the settings.

Delete Mobility Domains

Step 1 From the menu bar, select **Admin > Mobility Domains**.

Step 2 Select the mobility domain from the list and click **Delete**.

Step 3 Click **Yes** to delete the mobility domain.