CHAPTER 4

Cisco DCNM Web Client

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

The default user credentials to access Cisco DCNM, Release 10.0.x are as configured during the deployment of the installers.

Cisco DCNM Web Client provides the following features:

Navigating DCNM Web Client

Cisco Data Center Network Manager (DCNM) is a management system for the Cisco Unified Fabric. It enables you to provision, monitor, and troubleshoot the data center network infrastructure. It provides visibility and control of the unified data center. Cisco DCNM provides a comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco DCNM provides a high level of visibility and control through a single web based management console for Cisco Nexus, Cisco MDS, and Cisco Unified Computing System (UCS) products. During the DCNM installation, you can choose to install applications related to Unified Fabric only for Unified Fabric-mode installations.

The DCNM Web Client has standardized certain navigation conventions.

Scope Menu

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

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

- Data Center
- Default_LAN
- Default_SAN
- Individual Fabric Various other custom scopes created by the users.

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:

- **DCNM SAN**: Launch the SAN Client.
- **DCNM DM**: Launch the Device Manager Client which is part of the SAN option.
- **Change Password**: Changes the password for the current logged in user.
- **Help Content**: Pops out the online help of the current page.
- **About**: Display the information about Cisco Data Center Network Manager.
- **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 upper 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 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.

Using the Cisco 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
- MAC Address
- Serial Number

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.

Downloading Cisco DCNM-SAN Client

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

Step 1 On the top right of the DCNM Web Client home screen, click the settings icon next to the login user. Select **DCNM-SAN** option.

Step 2 If you have the latest Java version installed, a Warning message is displayed.

Step 3 Click **Run with the latest version** button.

Step 4 Enter the user credentials to log on to Cisco DCNM-SAN client. This message appears only the first time you launch Cisco DCNM-SAN Client.

Downloading Cisco Device Manager Client

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

Note Device Manager Client is part of the SAN option.

Step 1 On the top right of the DCNM Web Client home screen, click the settings icon next to the login user. Select **DCNM DM** option.

Step 2 If you have the latest Java version installed, a Warning message is displayed.

Note Cisco 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 3 Once the installation is complete, enter the user credentials to log on to the Cisco Device Manager client.

Viewing Dashboard Information

The Cisco 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. New panels has been introduced in release 10.0.x to simplify the management of LAN and SAN clients.
- Network - You can view the information of switches including status and license, as well as detailed switch dashboard information for a specific switch.
- Storage - You can view details about the storage device along with its events and topology.
- Compute - You can view the details and events for a particular Host along with its events and topology.

Note Compute is available only with SAN installation

For more information about the Dashboard tab, refer to the Web Client Online Help.

Viewing Topology Information

Topology is a first class menu item in this release with the intention that it is fully functional for providing detailed access to configuration as well as monitoring functionality. The Cisco DCNM topology consolidates functionality in the existing Fabric topology as well as the current Dashboard topology into a new fully featured topology which includes the following features in a single view:

- Optional display of Vinci Balls or device icons.
- Display of Multi-link, Port-channels, VPCs.
- Display of Inter-fabric links.
- VDC and Pod Groupings.

- Device-Scope, Fabric and Datacenter drill-down.
- Automatic VPC Peer and FEX Groupings.
- Ability to select devices and take action consistent with other areas of the product.

For more information about Topology, refer to the Web Client Online Help.

Viewing Inventory Information

Beginning with Cisco 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. In this tab, you can find the discovered LAN switches, SAN switches, Storage devices and Virtual Machine Manager. You can also add a new discovery LAN or SAN switch as well.

For more information about Inventory tab, refer to the Web Client Online Help.

Viewing Monitor Information

You can get the performance statistics of CPU, Memory, Traffic, others, accounting and events information. You can also view performance information about SAN and LAN. You can also create customized reports based on historical performance, events, and inventory information gathered in this tab. You can create aggregate reports with summary and detailed views. You can also view previously saved reports.

For more information about Monitor tab, refer to the Web Client Online Help.

Viewing Configure Information

Allow user to view and configure Zoning, Device Alias, Port Monitoring and Device Credentials.

For more information about Configure tab, refer to the Web Client Online Help.

Viewing Administration Information

You can view and configure DCNM servers, DCNM users, performance setup and event setup.

For more information about Administration tab, refer to the Web Client Online Help.

Using Cisco DCNM Web Client with SSL

From release 10.0.x, Cisco DCNM Web Client uses HTTPs. If you want to install SSL certificates and use Cisco 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:

Creating a Local Certificate

Step 1 Set up a keystore to use a self-signed certificate (local certificate). From the command line, enter the following command on windows:

```
%JAVA_HOME%/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore "C:\Program
Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
```

Step 2 Enter your name, organization, state, and country. Enter **change it** when prompted for a keystore password. If you prefer to use your own password, do not forget to change the keystorepass attribute in the server.xml file. When prompted for a key password, press **Enter** or use the same password as the keystore password.

Note You can now follow the steps in the next section for modifying DCNM Web Client to use SSL.

To obtain a certificate from the Certificate Authority of your choice, you must create a Certificate Signing Request (CSR). The CSR is used by the certificate authority to create a certificate that identifies your website as secure.

Creating a Certificate Request

Step 1 Create a local certificate (as described in the previous section).

Note You must enter the domain of your website in the fields First and Last name in order to create a working certificate.

Step 2 Create the CSR with this commandon windows:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore "C:\Program
Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
```

Now you have a file called certreq.csr. The file is encoded in PEM format. You can submit it to the certificate authority. You can find instructions for submitting the file on the Certificate Authority website.

Step 3 After you have your certificate, you can import it into your local keystore. You must first import a Chain Certificate or Root Certificate into your keystore. You can then import your certificate.

Step 4 Download a Chain Certificate from the Certificate Authority where you obtained the certificate:

- For Verisign.com commercial certificates, go to this URL:

  http://www.verisign.com/support/install/intermediate.html

- For Verisign.com trial certificates, go to this URL:

  http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html

- For Trustcenter.de, go to this URL:

  http://www.trustcenter.de/certservices/cacerts/en/en.htm#server

- For Thawte.com, go to this URL:

  http://www.thawte.com/certs/trustmap.html

- Import the Chain Certificate into your keystore by entering the **keytool -import -alias root -keystore " C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -trustcacerts -file** *filename_of_the_chain_certificate* **command.**
- Import the new certificate in X509 format by entering the **keytool -import -alias tomcat -keystore " C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -trustcacerts** *-file your_certificate_filename* **command.**

Enhancements in Cisco DCNM Release 10.2(1)

The following features and enhancements are available with Cisco DCNM Release 10.2(1).

For details about configuring the feature using DCNM Web Client, see the Cisco DCNM Web Client Online Help.

Enhancements to Media Controller

The following are the enhancements made to Media Controller in this release:

- Bandwidth Tracking on Host Facing Link—The senders and receivers can connect to Leaf switches of the PMN Fabric. The sender initiates a multicast flow and the receiver subscribes to a multicast flow. Since multicast is used, there can bemultiple receivers subscribing to a flow. The senders are devices such as cameras, microphones, playback devices etc. The receivers are devices such as video monitors, speakers, multi-viewers etc. You can track the bandwidth on the host facing link. Using this functionality, DCNM do not allows the receiver to request for more flows or sender to send more flows than the available bandwidth on the host facing link.
- Topology Visualization—Cisco DCNM 10.2(1) consists of a new scalable Topology visualization UI, which shows the PMN Fabric, endpoints attached to the fabric along with the ability to perform searches.
- Endpoint (Sender and Receiver management)—Senders and receivers can connect to the Leaf switches of the PMN Fabric. The Sender initiates a multicast flow and the Receiver subscribes to a multicast flow. Cisco DCNM exposes the API for registration of the Sender and Receiver. DCNM also allows the Sender/Receiver to be validated/authenticated by the API user. A table lists all the current registered senders and receivers with information about the flow instances. DCNM UI and REST APIs allow users to add additional metadata to the receiver/sender information, such as Camera-BXB or Camera-SJ, to aid in easy mapping.
- Flow Alias—Using the Flow Alias feature, you can specify names for multicast groups and flows. The multicast IP addresses are difficult to remember, thus by assigning a name to the multicast IP address, you can search and add policies based on the name. You can configure flow alias on Cisco Web Client > Media Controller > Flow Alias.

To enable Media Controller on the Cisco DCNM Web Client, you must install the DCNM in media-controller mode. See Cisco DCNM Installation Guide, Release 10.2(x) for more information.

You can monitor the devices from the Cisco DCNM Web Client > Media Controller.

For more information, see the Cisco DCNM Web Client Online Help.

LAN Fabric Provisioning

In this release, DCNM provides a new wizard that enables you to deploy a network with ease. This feature provides simple network overlay provisioning for Cisco Nexus 9000 VXLAN EVPN LAN Fabrics. This deploys networks populated by DCNM profile templates. To start, you need to select an existing fabric or add a new fabric and then define Fabric Settings.

After you select or create a fabric, you can continue to the next step to select a network. You can add a new or edit/delete/select an existing network. To access this feature, choose **Configure > LAN Fabric Provisioning > Network Deployment**.

For more information, see the Cisco DCNM Web Client Online Help.

IPv6 Support

In this release, DCNM enables you to manage switches with either IPv4 or IPv6 management interfaces. DCNM Web access (DCNM management interface) still supports IPv4 only. The extended fabric interface (eth1) supports both IPv4 and IPv6. DCNM supports LAN switches with IPv6 management interface, not for SAN switches. Also, DCNM OVA/ISO installation supports the LAN switches with IPv6 management interface. The Windows/Linux installation will not support IPv6 management interface.

DCNM allows POAP to LAN switches with IPv4 only, but the switch definition allows management interface to be configured with IPv6 address. Once POAP is complete, if switch management interface is configured with IPv6, then DCNM communicates with the switch via SNMP/SSH/NxAPI/Syslog with IPv6. For Programmable Fabric, switch can also communicate to the LDAP on DCNM server with IPv6.

FEX Configuration

The Fabric Extender feature allows you to manage a Cisco Nexus 2000 Series Fabric Extender and its association with the Cisco NX-OS switch that it is attached to. From Release 10.2(1), you can create and modify FEX for the LAN devices from **Cisco DCNM Web Client > Inventory > Switches**. FEX feature is available on LAN devices only.

Note If a Cisco Nexus Switch is discovered as part of SAN fabric, FEX feature is not available.
FEX is also not supported on Cisco Nexus 1000V devices.
For Cisco Nexus 9500 switches, 4x10G breakout for FEX connectivity is not supported.

VDC Enhancements

Beginning with Cisco DCNM Release 10.2(1), you can create and manage VDCs from Cisco DCNM Web Client > Inventory > Switches > VDCs. As Cisco DCNM supports DCNM on Cisco Nexus 7000 Series only, click an active Cisco Nexus 7000 Switch. After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies.

Network Audit Reporting

DCNM 10.2(1) provides auditing for the configuration change across the network switches. You can get report for all the configuration changes, which happen on the devices in a data center. You can generate an audit report for devices for a given period. To generate reports using the Network Audit config feature, the backup job should be scheduled for that device. The reports can also be exported to an HTML document. If real time job is scheduled for the device, audit will also show the mode through which config changes were made. The audit report uses color codes; green—new config, red—deleted config, and blue—changed config.

VLAN Edit Support

DCNM 10.2(1) allows you to edit a VLAN.

Support for Additional Storage Devices in DCNM Connect

To expand additional storage coverage, DCNM includes Pure Storage, HDS storage in DCNM connect. For storage array discovery, DCNM will support storage virtualization profile to cover IBM SAN Volume Controller (SVC).

SNMP Poller Adjustment

Currently performance polling interval is a five minutes fixed interval for all the entities except ISL. DCNM 10.2(1) provides the ability to adjust interval to 10 minutes or 15 minutes. To configure the interval, choose **Administration > Performance Setup > Database** in the DCNM Web UI.

Enhancement to Multi Site Manager

In this release, DCNM provides top level switch information per fabric instead of top level (“Default San”). To access this feature, choose **Administration > DCNM Server > Multi Site Manager**.

Monitoring Custom Port Groups

Custom port group is used in DCNM report and event forwarding. DCNM enables you to view custom port group and performance statistics. To access this feature, choose **Monitor > Custom Port Groups**.

Slow Drain Enhancement

In DCNM 10.2(1), you can export slow drain analysis data to a CSV or an Excel file. The default file format for export is CSV. To export this data, choose **Monitor > SAN > Slow Drain Analysis**.

In addition, DCNM enables you to schedule a slow drain analysis job and send the result via email.

In the slow drain daily scheduled job page, an 'Email To' (optional) field is available, which allows you to enter an email address. The report will be emailed to this configured email address after each job is complete.

For more information about this new feature, please refer to Web Client Online Help.

Template Enhancement

In this release, templates will support IPv6.

Endpoint Locator (EPL)

The Endpoint Locator (EPL) feature allows real-time tracking of endpoints within a data center. This includes tracing the life history of an endpoint as well as provides insights into the trends associated with endpoint additions/removals/moves etc.

With the DCNM OVA or ISO installation, the DCNM VM is deployed with 2 interfaces—eth0 for general access to the DCNM and eth1 interface that is used primarily for fabric management. In most deployments, the eth1 interface is part of the same network on which the mgmt0 interfaces of the Nexus switches reside. This allows DCNM to perform out-of-band management of these devices including out-of-band POAP. Since the BGP process on the Nexus devices only runs on the non-management VRF (specifically default VRF), there is a requirement to have IP connectivity from the DCNM to the fabric through any of the devices using one of the front-panel interfaces. For this purpose, a third interface ethx, is required on the DCNM VM that can provide inband connectivity to the network fabric. This is a pre-requisite for enabling the EPL feature. Addition of a new interface does not require a restart of DCNM VM. Once the vnic is added to the DCNM VM, the corresponding veth interface gets created and shows up in the CentOS VM on which DCNM runs as an ethx interface.

High Availability with Endpoint Locator—The Endpoint Locator feature along with its key components only runs on the active DCNM. However, the search process also runs on the standby DCNM so that all endpoint data and associated events are always synced between the active and standby DCNMs. In this way, during a switchover, the data is already available on the new active DCNM (old standby). In addition, Endpoint locator (EPL) also allows a DCNM standby to be added where there is a only a single DCNM instance running with EPL enabled and subsequently a standby is added at a later stage.

The third interface is required when inband management is used for a fabric via the eth1 interface. This ensures that the management interface used by DCNM for managing the devices and potentially even for POAP should not have any dependency on the interface through which EPL BGP peering occurs.

Once physical connectivity is established between DCNM and the fabric through a switch's front-panel interface, the following steps explain the appropriate configurations that are performed on the respective switches and DCNM.

Endpoint Locator supports the following features:

- Support for a BGP EVPN Fabric (N9k, N56xx as leafs)
- Support for a L3VPN or DFA Fabric (N56xx, N6k as leafs)

- Support for dual-homed endpoints
- Support for dual-stack endpoints
- Supports up to 2 BGP Route-Reflectors (Nexus 9000, Nexus 7999, Nexus 5600, Nexus 6000)
- Support with and without NX-API (to gather additional information such as port, vlan etc.)
- Auto-configuration of the Fabric to enable the Endpoint Locator feature when DCNM is directly attached to a leaf/ToR in a fabric
- Support of Endpoint Locator feature when DCNM is not directly attached to a ToR/leaf in a fabric
- Support for optional flush of the Endpoint data to start afresh
- Support for real-time and historical dashboards
- Support for views with operational and exploratory insights such as endpoint life-time, network/endpoint/vrf daily views and operational heat map
- Full High availability support
- Endpoint data stored for up to 180 days amounting to a maximum of 5G storage space
- Supported scale: 10000 endpoints

For more information, see the Cisco DCNM Web Client Online Help.

VxLAN EVPN IR

From the DCNM General and LAN fabric settings, the IR (Ingress Replication) option is added for handling BUM traffic for VxLAN EVPN fabric. IR and Multicast Routing are mutually exclusive. If IR is selected, DCNM allows IR-based profiles only. DCNM will also add appropriate IR configuration in the leaf templates and do not show Multicast configuration.

Support for New Hardware

The following hardware are supported in Cisco DCNM Release 10.2(1):

Table 4-1 Support for New Hardware

Hardware Description	Part Number
Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module	DS-X9648-1536K9
Nexus 9300 with 24p 40/50G QSFP+ and 6p 40G/100G QSFP28	N9K-C93180LC-EX
New fabric module for the Cisco Nexus 9516 Switch chassis	N9K-C9516-FM-E
40/100G Ethernet Module for Nexus 9500 series chassis	N9K-X9736C-EX
N9K-C92300YC-FixedModule	N9K-C92300YC
48-port 1/10/25 Gigabit Ethernet SFP+ and 4-port 40/100 Gigabit Ethernet QSFP line card	N9K-X97160YC-EX
Nexus N9K-C9232C Series fixed module with 32x40G/100G	N9K-C9232C
Cisco Nexus 2348TQ-E 10GE Fabric Extender	