CHAPTER 4f

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.**

Major Changes on Cisco DCNM Web Client

In release 10.0.x, Cisco DCNM replaces Flash with HTML5 and makes GUI consolidation. Cisco DCNM release 10.0.x introduces new look and feel for all GUI screens including:

Migration of DCNM function for LAN to Unified Web Client

For the simplification of management, Cisco DCNM LAN Thick Client has been omitted from release 10.0.x. Now you can perform the functionalities on the unified Cisco DCNM Web Client instead of another LAN thick client. DCNM SAN and DCNM DM Clients are an installation option.

The LAN client and server related components are removed from the installer. The Database tables related to LAN are not created during installation which reduces the size of the installer as well as the installation time and download time.

For more information about the usage of the Cisco DCNM Web Client, please refer to Web Client Online Help.

Multi-Fabric

Starting from Cisco DCNM release 10.0.x, Cisco DCNM supports multi-fabric which means fabrics of different encapsulation type such as FabricPath and VXLAN fabric, can co-exist and fabric level consistency can be validated.

The multi-fabric workflow includes fabric object creation, fabric bring-up per fabric plan, fabric provisioning, and fabric monitoring via topology.

Creating Fabric Object

You can add a LAN fabric through Cisco DCNM Web Client.

From the menu bar, choose **Configure > LAN Fabric Settings > LAN Fabrics**.

A fabric instance can encapsulate and define not just the properties of the Fabric, but also serve as a container to group all the Leaf, Spine, Border Leaf, Edge Router and other entities that fall into the purview of the Fabric.

The advantages of grouping of the Fabric includes:

- Fabrics of different encapsulation types like FP or VxLAN co-reside in DCNM now.
- Device types and template instances are validated and users can be warned accordingly since the intent of the Fabric is well defined at the beginning of the Fabric design.
- Topology and other visualization tools can feed off this Fabric instance information to make prudent judgments on layout design.
- Fabric level health computation is more meaningful because the meta-data provided by the user about the Fabric helps define the actual intent and behavior of the Fabric.

Fabric Plan

You can add a LAN fabric through Cisco DCNM Web Client.

From the menu bar, choose **Configure > LAN Fabric Settings > LAN Fabrics**. Click the **Add Fabric Plan** icon.

Fabric plan is a paradigm to define the intent and characteristics of the Fabric, so that this definition can help guide the rest of the Fabric deployment, management and monitoring.

During fabric plan creation, you can specify the spine, leaf and border switches count, type, and supply the subnets used for numbered IP fabric interfaces as well as VPC peer leaf and keep-alive interfaces. In addition, you can choose to override the default POAP templates that DCNM pre-selects for the switches based on the switch role. DCNM will then auto-generate the cabling plan and auto-populate the POAP definitions for all the switches within the fabric. You are able to update those auto-populated values. After the switch is powered on, DCNM will auto-associate switch according to the serial number with entries in cable plan based on switch's neighbor info gathered during switch boot-up. If needed, DCNM will auto-apply the corresponding POAP definition on the switches to bring up the complete fabric.

Fabric Provision

Similar as previous releases, fabric provision data is organized in organization, partition and network hierarchy. Instead of a flat structure for all the fabrics managed by the same DCNM, the provision data is separated at fabric level so as to be easily traversed, backed-up and restored.

There are 2 exclusive options to provision fabric:

- Switch initiates auto-configuration and Cisco DCNM triggers auto-pull, which requires switch to support auto-configuration feature.
- Cisco DCNM controlled configuration deployment. That means, DCNM manages the VLAN (de)allocation, (un)deploys and tracks the configuration on switches.

Fabric Monitoring

In addition to the fabric topology that depicts all the switches within the fabric and interaction across fabric, DCNM provides fabric level aggregation of information such as switch summary, licensing tracking, provision distribution and health score. The fabric level aggregation data will also be consumed by multi-site feature.

Enhanced Topology

Topology becomes a first class menu item in release 10.0.x with the intention that it is fully functional for providing detailed access to configuration as well as monitoring functionality.

The Cisco DCNM topology includes the following features in a single view:

- Optional display of Fabric topology 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.

The enhanced Topology provides the following functionality:

- Display Link state.
- You can drag, pan, and zoom on the topology page. Device layout is in a tiered topology by default. Customized views can be saved.
- Click on the switch device or the links, port-channel or vpc loop on the topology page, it pops out the summary configuration and status information panel.
- Mouse-over:
  - Link mouse-over provides summary performance information.
  - Device mouse-over displays the quick information about the device.
- Search for VLAN, VNI, FP, VRF, etc.

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

Multi-Site-Manager

From the menu bar, choose **Administration > DCNM Server > Multi Site Manager**.

Multi Site Manager (MsM) provides a single pane for customer to globally search for switches and virtual machine's location which Cisco DCNM server owns it. Hyperlink will be provided to access the corresponding switch, host, or the virtual machine (if applicable). Enter the user name and password to

login. The page also plays the role of remote site registration. The registration only allows the current Cisco DCNM server to access the remote DCNM server or site. For the remote site to access the current Cisco DCNM server, registration is required on the remote site as well. After you have done the registration, the MSM panel will display a diagram to show the overall health and status of the remote site, and the content of the panel will be subject to change.

MSM supports the following:

- Allow user to see the overall health of the switches (inside SAN and LAN Fabric) in each site.
- Allow user to find out which DCNM Server (site) is managing a given switch.
- On demand finding out the upstream LAN switch of a given host/virtual machine.
- On demand finding out which LAN switches have active VXLAN segment.

Migrated Cisco DCNM SAN Client Functionality

Above from release 10.0.x, Cisco DCNM has supported zone configuration, device alias management and port monitoring for SAN in web client.

From the menu bar, choose **Configure > SAN > Zoning**.

Zonesets, Zones, Zone Members and **Available to Add** panels are displayed in a single screen which is more easier to do the zone operation.

From the menu bar, choose **Configure > SAN > Device Alias**.

You can create, delete and edit the device alias in the device alias table. You can also **Commit**, **Abort** changes on the selected switch and **Clear CFS Lock** on the **CFS** tab.

From the menu bar, choose **Configure > SAN > Port Monitoring**.

You can select a set of non-editable default policy including **Normal, Default, Aggressive, Most-Aggressive** and **Slowdrain** which are bundled in DCNM to push to the selected switches. You can customize the policy based on the default policy and push the customized policy to the SAN switch. You can view the existing PMON policy on SAN switch.

For more information about the usage of the Cisco DCNM Web Client, please refer to Web Client Online Help.

Image Management

Data center administrators have the onus of tracking the images installed on switches in the network and upgrading them whenever Cisco releases new software images. Image management on the Cisco Nexus devices is done by In-Service Software Upgrade (ISSU), Software Maintenance Upgrades (SMU), and Graceful Insertion and Removal (GIR) through Cisco DCNM web client.

On Cisco DCNM web client, you can:

- Tack images installed on the switches.
- Do upgrade or downgrade of images on multiple switches.
- Schedule the image installation.

From the menu bar, choose **Configure > Image Management > Upgrade**.

Cisco Nexus Series switches and any connected FEXs can be upgraded without any traffic disruption.

From the menu bar, choose **Configure > Image Management > Patch**.

SMUs are created to respond to immediate issues and do not include new features. Typically, SMUs do not have a large impact on device operations. You can install and uninstall the SMU tasks in this page.

From the menu bar, choose **Configure > Image Management > GIR**.

You can change the system mode to GIR mode for the selected switch on this page. GIR mode provides an easy method for isolating a switch for maintenance windows and then bringing it back into service.

From the menu bar, choose **Configure > Image Management > Repositories**.

You can see the history of ISSU jobs that were triggered from Cisco DCNM for each of the device. This helps for accounting purpose and to find the images installed on the devices.

Note Image management is a licensed feature. Hence you are able to select only the licensed devices. Only Cisco Nexus 3000, Cisco Nexus 5000, Cisco Nexus 6000, Cisco Nexus 7000 and Cisco Nexus 9000 devices are supported.

For more information about the usage of the Cisco DCNM Web Client, please refer to Web Client Online Help.

Modular Device Support

Start from release 10.0.x, Cisco DCNM has supported to apply the patch to the released software that are running in production. In order to support any new hardware which doesn't require many major changes, a patch can be delivered instead of waiting for the next DCNM release. This feature helps to deliver and apply the DCNM patch releases. An authorized DCNM administrator can apply the patch deliverables to the production setup using this tool. Patch releases can be applicable for the following scenarios.

- Support any new hardware (Chassis/Line cards).
- Support latest Cisco NX-OS versions.
- Support critical fixes as patches.

Applying the patch

Step 1 Stop DCNM services.

Step 2 Execute the following command to apply the patch in command prompt or console:

- **Windows**

```
patch.bat <absolute patch of patch>
```

Note patch.bat is present in C:\Program Files\Cisco Systems\dcm\fm\bin

Example:

```
> cd C:\Program Files\Cisco Systems\dcm\fm\bin
> patch.bat C:\patches\Hafnium-testing.zip
```

- **Linux**

```
./patch.sh <absolute patch of patch>
```

Note patch.sh is present in /usr/local/cisco/dcm/fm/bin.

Example:

```
> cd /usr/local/cisco/dcm/fm/bin
>./patch.sh  /root/patches/Hafnium-testing.zip
```

Step 3 To view the patch details, open the DCNM web UI and go to **Administration > Modular Device Support**. This window will show the patch deployed on each DCNM server.

- **Federation**

  Patch needs to be applied on all servers in federation separately.

  Before applying the patch stop DCNM service on all servers in Federation

- **Native HA**

  Patch needs to be both Active and Standby Servers separately

  Before applying the patch stop all service primary service should be stopped.

Rollback

Rollback will removes patch applied most recently. To rollback multiple patch run rollback operation multiple times.

Rollback the patch

Step 1 Stop the DCNM services.

Step 2 Execute the following command to roll back the patch.

- **Windows**
  - Run the following command:

    patch rollback

    Note patch.bat is present in C:\Program Files\Cisco Systems\dcm\fm\bin.

  - Start the DCNM services on windows.
- **Linux**
  - Run the following command to roll back the patch.

    ./patch.sh rollback

    Note patch.sh is present in /usr/local/cisco/dcm/fm/bin.

  - Start the DCNM services on Linux

Step 3 Once the patch is rolled back, corresponding information will not be shown in **Administration > Modular Device Support** window in web UI.

Role Based Access Control

Cisco DCNM allows the administrator to manage users' access to the Cisco DCNM server and assign a role to each user by using the Cisco DCNM Web client.

- If you are assigned the role as **user**,
  - You cannot change the Cisco DCNM authentication mode.
  - You cannot add or delete Cisco DCNM local user accounts.
  - You can change the details of your own local user account.
- If you are assgned the role as **admin**:
  - You have full control of Cisco DCNM authentication settings.

Starting from release 10.0.x, the new introduced Role Based Access Control (RBAC) feature allows the **admin** to associate **user** to one or more device scope or group, so that the **admin** can control **users**' access to devices or fabrics from Cisco DCNM web client or SAN client, and the user can see only the associated switch groups in the **Scope** drop-down list. This way **admin** can restrict **users** to view or configure only sub-set of discovered devices.

Local Authentication for RBAC

You can do local authentication when you are assigned the role as **Network Admin**.

Step 1 Login the Cisco DCNM Web Client using the **Network Admin** account. You have full device access, i.e. Data Center group access.

Step 2 From the left menu bar, choose **Administration > DCNM Server > Switch Groups**. Click the **Add** icon to create a new group.

Step 3 From the left menu bar, choose **Administration > Management Users > Local**. Click **Add User** to create a new user and assign the role for the user.

Step 4 To manage the access for the user, select the user and click **User Access.** Check the box before the group or scope that you want the user to access to.

Step 5 When the newly created user logs into Cisco DCNM Web Client, he will see only the associated scope or groups in the **Scope** drop-down list at the top of the window and he can view only the devices belongs to those group.

Remote Authentication for RBAC

Cisco DCNM supports **TACACS+, Radius, Switch** and **LDAP** remote authentication. You can perform remote authentication when you are assigned the role as **Network Admin**.

Note Anonymous LDAP bind or access is disabled in Cisco DCNM Release 10.1. A read-only LDAP user has been introduced since DCNM 7.1(1), DCNM 7.0(2) and 7.0(1). We recommend you to upgrade to a later version for authenticated LDAP access.

Step 1 Login the Cisco DCNM Web Client using the **Network Admin** account. You have full device access, i.e. Data Center group access.

Step 2 From the left menu bar, choose **Administration > DCNM Server > Switch Groups**. Click the **Add** icon to create a new group.

Step 3 From the left menu bar, choose **Administration > Management Users > Remote AAA**.

– If you choose **TACACS+** or **Radius** authentication mode, *cisco-av-pair* attribute has been extended by adding the *dcnm-access* key in addition to *role*. To assign a Cisco DCNM user role by **TACACS+** and **Radius**, Cisco DCNM use the returned *cisco-av-pair* attribute-value pair from TACACS+ and Radius remote authentication.

Table 1:cisco-av-pair Attribute-Value Pair, page 4-14 shows the *cisco-av-pair* attribute-value pair

Table 1: cisco-av-pair Attribute-Value Pair

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell cisco-av-pair Value
User	*shell:roles = "network-operator" dcnm-access="group1 group2 group5"*	*cisco-av-pair=shell:roles="network-operator" dcnm-access="group1 group2 group5"*
Admin	*shell:roles = "network-admin" dcnm-access="group1 group2 group5"*	*cisco-av-pair=shell:roles="network-admin" dcnm-access="group1 group2 group5"*

Admin can configure the group information using the key *dcnm-access* with groups separated by commas as in the above table.

By getting the access information from the remote authentication, logged in user will be able to see only those associated group devices. If the remote authentication response does not assign groups, user can see all the devices.

– If you choose **LDAP** authentication mode, specify the **Access Map** text field to associate the accessible groups for the user. The format is: *userDomain1:group1,group2;userDomain2:group3*.

Note For **Switch** authentication mode, the RBAC is not supported.

Configuration Archive

The configuration archive feature allows you to backup device configurations, both running configuration and startup configurations as a regular text file in the file system. The backup files can be stored in the DCNM server host or on a file server.

You can also configure the archive system to support scheduling of jobs for the selected list of devices. You can configure only one job for a switch.

You can find this feature in the DCNM Web Client under **Configure > Backup > Switch Configuration**.

You can perform following tasks using this feature:

- Import the configuration file from the file server to the Cisco DCNM.
- Compare the configuration file with another version of the same configuration or with the configuration file of another device.
- Copy the configuration files to the same device, to another device, or multiple devices concurrently.
- Restore the configuration file from the selected switches or from the Golden backup.

- View or edit the configuration file on the device.
- Delete the configuration file from the device.
- Archive jobs.

For more information about the configuration archive feature, please refer to Web Client Online Help.