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, page 4-1
- Downloading Cisco DCNM-SAN Client, page 4-3
- Downloading Cisco Device Manager Client, page 4-4
- Viewing Dashboard Information, page 4-4
- Viewing Topology Information, page 4-5
- Viewing Inventory Information, page 4-5
- Viewing Monitor Information, page 4-5
- Viewing Administration Information, page 4-5
- Using Cisco DCNM Web Client with SSL, page 4-6
- New Features and Enhancements in Cisco DCNM Release 10.4(1), page 4-7

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.

Note By default, Cisco DCNM will not enable HTTP port. The HTTP port is disabled for security reasons. All clients should use HTTPS for API or Web access. If you want to enable HTTP, edit the $INSTALLDIR/dcnm/jboss-as-7.2.0.Final/standalone/configuration/standalone-san.xml file.

The DCNM Web Client has standardized certain navigation conventions.

- Scope Menu, page 4-2
- Admin Menu, page 4-2
- Table and Filtering Navigation, page 4-2
- Printing, page 4-2
- Exporting to a File, page 4-3
- Sorting Columns, page 4-3
- Cisco DCNM Web Search Engine, page 4-3

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, page 4-6
- Creating a Certificate Request, page 4-6

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 command on 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.**

New Features and Enhancements in Cisco DCNM Release 10.4(1)

For details about the new features and enhancements in Cisco DCNM 10.4(1) Web Client, see the Cisco DCNM Web Client Online Help.