Cisco DCNM Fundamentals Configuration Guide, Release 5.x

First Published: April 2010
Last Modified: November 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-23625-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco DCNM Fundamentals Configuration Guide, Release 5.x
© 2008-2010 Cisco Systems, Inc. All rights reserved.

Send document comments to nexus7k-docfeedback@cisco.com

CONTENTS

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco DCNM Fundamentals Configuration Guide, Release 5.x*. The latest version of this document is available at the following Cisco website:
http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

To check for additional information about Cisco Data Center Network Manager (DCNM) Release 5.x, see the *Cisco DCNM Release Notes, Release 5.x*.

Table 1 summarizes the new and changed features for the *Cisco DCNM Fundamentals Configuration Guide, Release 5.x*, and tells you where they are documented.

Table 1 New and Changed Features for Release 5.x

Feature	Description	Changed in Release	Where Documented
L2 View	Support was added for showing VLANs configured among discovered devices in Topology.	5.x	Chapter 8, "Working with Topology"
Copy Run to Start	Support was added for Copy Run to Start in Topology.	5.x	Chapter 8, "Working with Topology"
Delta Mode and Rate Mode	A button was added to statistics charts to toggle between delta mode and rate mode.	5.x	Chapter 14, "Administering Statistical Data Collection"
Threshold Rules	Support was added for configuring threshold rules and applying those rules to charts.	5.x	Chapter 13, "Working With Threshold Rules"
Installing and launching the Cisco DCNM client	Support was added for using a command prompt to download the client. Proxy support was added.	5.0(2)	Chapter 2, "Installing and Launching the Cisco DCNM Client"
Global preferences	Support was added for the "Load history charts by default" check box.	5.0(2)	Chapter 3, "Using the Cisco DCNM Client"
Using the Cisco DCNM client	Information was added about how the Cisco DCNM client supports management of different Cisco NX-OS device types.	5.0(2)	Chapter 3, "Using the Cisco DCNM Client"
LLDP discovery	Support was added for discovering network devices and servers by link layer discovery protocol.	5.0(2)	Chapter 5, "Administering Device Discovery"

Send document comments to nexus7k-docfeedback@cisco.com

Table 1 New and Changed Features for Release 5.x (continued)

Feature	Description	Changed in Release	Where Documented
Automated device logging level configuration	Support was added for automatically configuring the system-message logging levels of managed devices.	5.0(2)	Chapter 5, "Administering Device Discovery"
Devices and Credentials	Support was added for the Reason field.	5.0(2)	Chapter 6, "Administering Devices and Credentials"
Topology	Support was added for launching the Cisco Fabric Manager client. Support was added for device groups. Support was added for network servers. Support was added for SAN connections.	5.0(2)	Chapter 8, "Working with Topology"
Network servers	Support was added for network servers.	5.0(2)	Chapter 9, "Configuring Network Servers"
Device groups	Support was added for device groups.	5.0(2)	Chapter 10, "Configuring Device Groups"
Cluster administration	Support was added for Cisco DCNM server cluster administration.	5.0(2)	Chapter 11, "Working with Cluster Administration"
Cisco DCNM server logging	Logging support was added for the Device Groups feature.	5.0(2)	Chapter 15, "Administering DCNM Server Log Settings"
Starting and stopping Cisco DCNM servers	Support was added for clustered-server deployments.	5.0(2)	Chapter 16, "Starting and Stopping Cisco DCNM Servers"

Send document comments to nexus7k-docfeedback@cisco.com

Preface

This preface describes the audience, organization, and conventions of the *Cisco DCNM Fundamentals Configuration Guide, Release 5.x*. It also provides information on how to obtain related documentation.

This preface includes the following topics:

- Audience, page xvii
- Document Organization, page xvii
- Document Conventions, page xviii
- Obtaining Documentation and Submitting a Service Request, page xix

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS devices.

Document Organization

This document is organized into the following chapters:

Chapter	Description
Chapter 1, "Overview"	Provides an overview of what you need to do to start using Cisco Data Center Network Manager (DCNM).
Chapter 2, "Installing and Launching the Cisco DCNM Client"	Describes how to install and set up the Cisco DCNM client.
Chapter 3, "Using the Cisco DCNM Client"	Introduces the Cisco DCNM client and explains how to use it.
Chapter 4, "Administering DCNM Authentication Settings"	Describes how to administer Cisco DCNM server user accounts.
Chapter 5, "Administering Device Discovery"	Describes how to use the Device Discovery feature.
Chapter 6, "Administering Devices and Credentials"	Describes how to use the Devices and Credentials feature.

Chapter	Description
Chapter 7, "Administering DCNM Licensed Devices"	Describes how to use the DCNM Licensed Devices feature.
Chapter 8, "Working with Topology"	Describes how to use the Topology feature.
Chapter 9, "Configuring Network Servers"	Describes how to use the Network Servers feature.
Chapter 10, "Configuring Device Groups"	Describes how to use the Device Groups feature.
Chapter 11, "Working with Cluster Administration"	Describes how to use the Cluster Administration feature.
Chapter 12, "Administering Auto-Synchronization with Devices"	Describes how to use the Auto-Synchronization with Devices feature.
Chapter 14, "Administering Statistical Data Collection"	Describes how to control statistical data collection.
Chapter 15, "Administering DCNM Server Log Settings"	Describes how to control Cisco DCNM server logs.
Chapter 16, "Starting and Stopping Cisco DCNM Servers"	Describes how to start and stop the Cisco DCNM server.
Chapter 17, "Maintaining the Cisco DCNM Database"	Explains how to maintain the Cisco DCNM database.
Chapter 18, "Troubleshooting Cisco DCNM"	Explains how to resolve problems that you might encounter with Cisco DCNM.

Document Conventions

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 1

Overview

This chapter provides a brief overview of Cisco Data Center Network Manager (DCNM).

Cisco DCNM is a management solution that maximizes overall data center infrastructure uptime and reliability, which improves business continuity. Focused on the management requirements of the data center network, Cisco DCNM provides a robust framework and rich feature set that fulfills the switching needs of present and future data centers. In particular, Cisco DCNM automates the provisioning process.

Cisco DCNM is a solution designed for Cisco NX-OS-enabled hardware platforms. Cisco NX-OS provides the foundation for the Cisco Nexus product family. For information about the specific Cisco Nexus products supported by Cisco DCNM, see the *Cisco DCNM Release Notes, Release 5.x*.

This chapter includes the following sections:

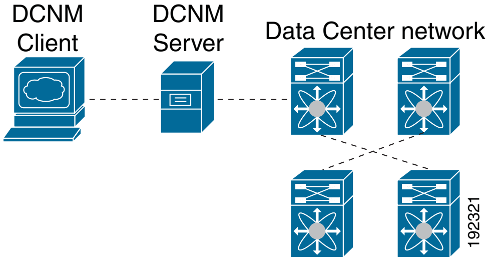
- Cisco DCNM Client and Server, page 1-1
- Features in Cisco DCNM, Release 5.0, page 1-2
- Documentation About Cisco DCNM, page 1-3

Cisco DCNM Client and Server

Cisco DCNM is Java-based client-server application. For Java requirements, server system requirements, and client system requirements, see the *Cisco DCNM Release Notes, Release 5.x*.

Figure 1-1 shows the Cisco DCNM client-server environment. The Cisco DCNM client communicates with the Cisco DCNM server only, never directly with managed Cisco NX-OS devices. The Cisco DCNM server uses the XML management interface of Cisco NX-OS devices to manage and monitor them. The XML management interface is a programmatic method based on the NETCONF protocol that complements the command-line interface (CLI) functionality. For more information, see the *Cisco NX-OS XML Management Interface User Guide, Release 5.x*.

Figure 1-1 Cisco DCNM Client-Server Environment



Send document comments to nexus7k-docfeedback@cisco.com

Features in Cisco DCNM, Release 5.0

Cisco DCNM Release 5.0 supports the configuration and monitoring of the following Cisco NX-OS features:

- Ethernet switching
  - Physical and virtual ports
  - Port channels and virtual port channels (vPCs)
  - Loopback and management interfaces
  - VLAN network interfaces (sometimes referred to as switched virtual interfaces or SVIs)
  - VLAN and private VLAN (PVLAN)
  - Spanning Tree Protocol, including Rapid Spanning Tree (RST) and Multi-Instance Spanning Tree Protocol (MST)
  - Fabric Extender
  - Link-state tracking
  - Serial Over LAN
  - Chassis Internal Network
  - Fibre-Channel-over-Ethernet Initiation Protocol (FIP) snooping
  - Port profiles
- Ethernet routing
  - Gateway Load Balancing Protocol (GLBP), object tracking, and keychain management
  - Hot Standby Router Protocol (HSRP)
- Network security
  - Access control lists
  - IEEE 802.1X
  - Authentication, authorization, and accounting (AAA)
  - Role-based access control
  - Dynamic Host Configuration Protocol (DHCP) snooping
  - Dynamic Address Resolution Protocol (ARP) inspection
  - IP Source Guard
  - Traffic storm control
  - Port security
- General
  - Virtual Device Context
  - Hardware resource utilization with Ternary Content Addressable Memory (TCAM) statistics
  - Switched Port Analyzer (SPAN)

Cisco DCNM includes the following features for assistance with management of your network:

- Topology viewer
- Network servers
- Device groups
- Event browser
- Configuration Delivery Management
- Configuration Change Management
- Device OS Management
- Hardware and virtual switch inventory

Cisco DCNM includes the following administrative features:

- Cisco DCNM server user accounts
- Device discovery
- Automatic synchronization with discovered devices
- Statistical data collection management
- Cisco DCNM server and client logging
- Cisco DCNM server cluster administration

Documentation About Cisco DCNM

The documentation for Cisco DCNM includes several configuration guides and other documents. For more information about the Cisco DCNM documentation, see the "Obtaining Documentation and Submitting a Service Request" section on page xix.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 2

Installing and Launching the Cisco DCNM Client

This chapter describes how to install and launch the Cisco Data Center Network Manager (DCNM) client.

This chapter includes the following sections:

Information About Installing and Launching the Cisco DCNM Client

The Cisco DCNM client is a Java application. When you finish installing the Cisco DCNM client on your system, the Cisco DCNM client automatically starts. After installing the Cisco DCNM client, whenever you need to restart the Cisco DCNM client, use the Cisco DCNM client software image on your system for the quickest start. If a more recent version of the Cisco DCNM client is available, the Cisco DCNM client automatically downloads that version to your system.

Send document comments to nexus7k-docfeedback@cisco.com

Prerequisites for Installing and Launching the Cisco DCNM Client

Installing and using the Cisco DCNM client have the following prerequisites:

- Your system must be running a supported operating system to install and use the Cisco DCNM client software. For more information about client system requirements, see the *Cisco DCNM Release Notes, Release 5.x*, which are available at the following site:

  http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

- The installation process uses Java version 1.5.0_11. If your system does not have that version of Java, the installation process will install it to your system.

  The Cisco DCNM client installer requires Internet access to download the Java version 1.5.0_11 JRE. If the system cannot access the Internet, use another system to download the Java installer and copy it to the system that you want to install the Cisco DCNM client on. You can download Java version 1.5.0_11 JRE from the Java[tm] Technology Products Download website, at http://java.sun.com/products/archive. The Java version 1.5.0_11 JRE is listed as JRE 5.0 Update 11.

  If your network environment requires a proxy connection to permit the download of the Java installer, ensure that the proxy settings are configured in Internet Options, available from the Control Panel. For more information, see http://java.sun.com/j2se/1.5.0/proxy_note.html.

- Some Cisco DCNM features require a license. Before you can use licensed features, install the Cisco DCNM license. For more information about licensed features or for detailed steps for the license installation, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x.*

Secure Client Communications

By default, communication between the Cisco DCNM client and server is unencrypted; however, you can enable Secure Socket Layer (SSL) encryption to protect client-server communications. Enabling SSL encryption does not affect how users download, install, and log into the Cisco DCNM client.

For information about enabling secure client communication, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x.*

Default Administrator Credentials

When you install Cisco DCNM, you specify the default administrator account, which is a Cisco DCNM local user. If you use RADIUS or TACACS+ authentication servers to control access to the Cisco DCNM client, the default administrator account provides you access if no authentication servers for the current authentication mode are reachable.

If no one has administrative access to Cisco DCNM, you can reset the local administrator account or change Cisco DCNM server authentication settings by reinstalling the Cisco DCNM server software. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Downloading and Launching the Cisco DCNM Client

The Cisco DCNM client is available from the web server that is included on the Cisco DCNM server. You can download and launch the Cisco DCNM client either by using a web browser or by using a command prompt.

When you download and launch the Cisco DCNM client, it automatically saves an image of the software on your local system and starts the Cisco DCNM client. Later on, when you start the Cisco DCNM client, you can quickly start it by using the image on your local system.

This section includes the following topics:

- Using a Web Browser to Download and Launch the Cisco DCNM Client, page 2-3
- Using a Command Prompt to Download and Launch the Cisco DCNM Client, page 2-5
- Using a Command Prompt to Download and Launch the Cisco DCNM Client without using Java Web Start Launcher, page 2-6

Using a Web Browser to Download and Launch the Cisco DCNM Client

You can use a web browser to download and launch the Cisco DCNM client.

BEFORE YOU BEGIN

The Java version 1.5.0_11 JRE must be installed on the computer that you want to run the Cisco DCNM client on.

The computer that you want to run the Cisco DCNM client on must meet the client system requirements. For details about the client system requirements, see the *Cisco DCNM Release Notes, Release 5.x*, available at the following site:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

DETAILED STEPS

Step 1 On the computer that you want to use the Cisco DCNM client on, open a web browser and go to the following address:

http://*server_IP_address_or_DNS_name*:*web_server_port*/dcnm-client/index.html

For example, if the Cisco DCNM server IP address is 172.0.2.1 and the web server port is 8080, use the following address:

Send document comments to nexus7k-docfeedback@cisco.com

```
http://172.0.2.1:8080/dcnm-client/index.html
```

The browser shows the Cisco DCNM client page.

Step 2 Click **Launch DCNM Client**.

The Cisco DCNM server sends the dcnm.jnlp file to the browser. This file should be opened with the Java Web Start Launcher.

Step 3 If the browser prompts you, choose to open the dcnm.jnlp file. You do not need to save the file.

The Cisco DCNM client installer verifies that Java is already installed on your system. If the installer does not find the supported version of Java on the computer, the installer prompts you to install Java version 1.5.0_11.

Note The Cisco DCNM client installer requires Internet access to download the Java version 1.5.0_11 JRE. If the system cannot access the Internet, use another system to download the Java installer, copy it to the system that you want to install the Cisco DCNM client on, install Java, and restart the Cisco DCNM client installation. You can download Java version 1.5.0_11 JRE from the Java[tm] Technology Products Download web site, at http://java.sun.com/products/archive. The Java version 1.5.0_11 JRE is listed as JRE 5.0 Update 11.

If your network environment requires a proxy connection to permit the download of the Java installer, ensure that the proxy settings are configured in Internet Options, available from the Control Panel. For more information, see http://java.sun.com/j2se/1.5.0/proxy_note.html.

Step 4 If the installer prompts you to install Java version 1.5.0_11, follow these steps:

a. Click **OK** to begin installing the supported version of Java.

b. If a security warning notifies you that the Java installer was digitally signed by an expired certificate, click **Run** to continue the installation.

c. Complete the Java installation wizard.

Tip To specify whether the supported version of Java is the default version used by browsers installed on the computer, choose Custom setup on the License Agreement dialog box. Later in the Java installation, on the Browser Registration dialog box, you can specify the browsers that should use the Java version that is supported by Cisco DCNM.

The Cisco DCNM client installs on the computer.

Note You might need to wait a minute or longer while the installer installs the software.

The Cisco DCNM client login window opens.

For detailed login steps, see the "Logging Into the Cisco DCNM Client" section on page 2-7.

Send document comments to nexus7k-docfeedback@cisco.com

Using a Command Prompt to Download and Launch the Cisco DCNM Client

You can use a command prompt to download and launch the Cisco DCNM client.

BEFORE YOU BEGIN

The Java version 1.5.0_11 JRE must be installed on the computer that you want to run the Cisco DCNM client on.

The computer that you want to run the Cisco DCNM client on must meet the client system requirements. For details about the client system requirements, see the *Cisco DCNM Release Notes, Release 5.x*, available at the following site:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

DETAILED STEPS

Step 1 On the computer that you want to use the Cisco DCNM client on, access a command prompt.

Step 2 Use the **cd** command to change the directory to the bin directory under the Java version 1.5.0_11 installation directory, as follows:

cd *path*

where *path* is the relative or absolute path to the bin directory. For example, on Microsoft Windows, the default path to the Java version 1.5.0_11 bin directory is C:\Program Files\dcm\Java\jre1.5.0_11\bin.

Step 3 Enter the applicable command:

- For Microsoft Windows:
  javaws.exe *server_IP_address_or_DNS_name*:*web_server_port*/**dcnm-client/dcnm.jnlp**
- For RHEL:
  ./javaws *server_IP_address_or_DNS_name*:*web_server_port*/**dcnm-client/dcnm.jnlp**

The Java Web Start Launcher retrieves the dcnm.jnlp file from the Cisco DCNM server and installs the Cisco DCNM client on the computer.

Note You might need to wait a minute or longer while the installer installs the software.

The Cisco DCNM client login window opens.

For detailed login steps, see the "Logging Into the Cisco DCNM Client" section on page 2-7.

Send document comments to nexus7k-docfeedback@cisco.com

Using a Command Prompt to Download and Launch the Cisco DCNM Client without using Java Web Start Launcher

You can use a command prompt to download and launch the Cisco DCNM client in standalone mode without using the Java Web Start Launcher.

BEFORE YOU BEGIN

The Java version 1.5.0_11 JRE must be installed on the computer that you want to run the Cisco DCNM client on.

The computer that you want to run the Cisco DCNM client on must meet the client system requirements. For details about the client system requirements, see the *Cisco DCNM Release Notes, Release 5.x*, available at the following site:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

In addition, access the computer where the DCNM server is installed. Copy the dcnm-client.zip file to a directory on the DCNM client computer where you can later unpack its files.

- On a Windows DCNM server, the dcnm-client.zip file is located in the <DCNM_INSTALL_LOCATION>\dcm\dcnm\ui-client file path.
  The default for <DCNM_INSTALL_LOCATION> is C:\Program Files\Cisco Systems.
- On a RHEL DCNM server, the dcnm-client.zip file is located in the <DCNM_INSTALL_LOCATION>/dcm/dcnm/ui-client file path.
  The default for <DCNM_INSTALL_LOCATION> is /usr/cisco.

Note The Cisco Fabric Manager cross launch feature is not supported when the DCNM client is installed in standalone mode. (The DCNM client in standalone mode is not a Java Web Start application.)

DETAILED STEPS

Step 1 On the computer that you want to use the Cisco DCNM client on, access a command prompt.

Step 2 Set JAVA_HOME to the location where the Java JRE is installed.
For example:

- For Microsoft Windows:
  set JAVA_HOME=C:\Program Files\Java\jre1.5.0_11
- For RHEL:
  export JAVA_HOME=/usr/java/jre1.5.0_11

Step 3 Use the **cd** command to change to the directory where you copied dcnm-client.zip.

Step 4 Unpack the dcnm-client.zip file and extract the dcm-client.bat and dcm-client.sh files.

Step 5 Run the script that is appropriate for your computer.

- For Microsoft Windows, run the dcnm-client.bat script.
- For RHEL, run the dcnm-client.sh script.

The Cisco DCNM client login window opens.

For detailed login steps, see the "Logging Into the Cisco DCNM Client" section on page 2-7.

Send document comments to nexus7k-docfeedback@cisco.com

Restarting the Cisco DCNM Client

If you have previously downloaded and launched the Cisco DCNM client on a computer, you can later start the Cisco DCNM client by using one of the shortcuts that the installer added to the computer.

When you start the Cisco DCNM client, it connects to the Cisco DCNM server and checks if the Cisco DCNM client that is available on the Cisco DCNM server is a newer version than the locally installed Cisco DCNM client. How the Cisco DCNM client starts varies depending upon the result of the version check, as follows:

- If the locally installed Cisco DCNM client is the same version as the Cisco DCNM client that is available on the Cisco DCNM server, the Cisco DCNM client window opens quickly.
- If the locally installed Cisco DCNM client is older than the version of the Cisco DCNM client that is available on the Cisco DCNM server, the Cisco DCNM client automatically downloads from the Cisco DCNM server and replaces the locally installed Cisco DCNM client before the Cisco DCNM client window opens.

For detailed login steps, see the "Logging Into the Cisco DCNM Client" section on page 2-7.

Logging Into the Cisco DCNM Client

When you log into the Cisco DCNM client, you must specify a valid Cisco DCNM user account.

BEFORE YOU BEGIN

You should know the following information before logging into the Cisco DCNM client:

- A valid Cisco DCNM username and password.
- The IP address or DNS name of the Cisco DCNM server. In a clustered-server deployment, this should be the IP address or DNS name of the master server.
- The Cisco DCNM server port number. By default, the server port number is 1099.
- Proxy server address, HTTP port number, and Socks port number, if a proxy server is required by your network environment.

DETAILED STEPS

Step 1 Start the Cisco DCNM client. If you have previously downloaded and launched the Cisco DCNM client on the computer, you can start the client by using one of the shortcuts added to the computer by the client installer. For detailed steps about downloading and launching the client, see one of the following topics:

- Using a Web Browser to Download and Launch the Cisco DCNM Client, page 2-3
- Using a Command Prompt to Download and Launch the Cisco DCNM Client, page 2-5

The Cisco DCNM client login window opens.

Step 2 In the DCNM Server field, enter the DNS name or the IP address of the Cisco DCNM server. By default, this field lists the address or name specified the last time the client logged into a server. If you are logging into the client after downloading it, this field lists the address of the server that you downloaded the client from.

Send document comments to nexus7k-docfeedback@cisco.com

Note If your Cisco DCNM deployment uses a clustered-server environment, enter the DNS name or IP address of the master Cisco DCNM server.

Step 3 In the Username field, enter your Cisco DCNM username. If you are logging into Cisco DCNM for the first time after installing the server, enter the local administrator name that you specified during the server installation. For more information, see the "Default Administrator Credentials" section on page 2-3.

Step 4 In the Password field, enter the password for the Cisco DCNM username that you specified.

Step 5 (Optional) If you need to change the Cisco DCNM server port, do the following:

a. If the Port field is not visible, click **More >>.**

b. Enter the port number in the Port field.

The default Cisco DCNM server port number is 1099; however, you can specify a different port number when you install or reinstall the Cisco DCNM server.

Step 6 (Optional) If you need to use a proxy server to connect to the Cisco DCNM server, do the following:

a. If the "Connect to the DCNM server with a proxy server" check box is not visible, click **More >>**.

b. Check **Connect to the DCNM server with a proxy server**.

The Proxy Server area appears below the check box.

c. In the Address field, enter the IP address of the proxy server.

d. In the HTTP Port and Socks Port fields, enter the port numbers on which the proxy server accepts HTTP and Socks connections.

e. (Optional) If the proxy server requires authentication, check **Authentication** and enter a valid username and password in the fields provided.

Step 7 Click **Login**.

The Cisco DCNM client opens. For information on how to use the Cisco DCNM client, see Chapter 3, "Using the Cisco DCNM Client."

Uninstalling the Cisco DCNM Client

You can uninstall the Cisco DCNM client from a computer.

DETAILED STEPS

Step 1 Click **Start > Control Panel > Java**.

The Java Control Panel dialog box opens.

Step 2 In the General tab, under Temporary Internet Files, click **Settings**.

The Temporary File Settings dialog box appears.

Step 3 Click **View Applications**.

The Java Application Cache Viewer dialog box opens.

Step 4 Select the Cisco DCNM Client application and click **Remove Selected Application**.

Java uninstalls the Cisco DCNM client image from your computer.

Step 5 Close the Java Application Cache Viewer.

Step 6 On the Temporary File Settings dialog box, click **OK**.

Step 7 On the Java Control Panel dialog box, click **OK**.

Step 8 If you want to reinstall the Cisco DCNM client, see the "Downloading and Launching the Cisco DCNM Client" section on page 2-3.

Additional References

For additional information related to installing and launching the Cisco DCNM client, see the following sections:

- Related Documents, page 2-9
- Standards, page 2-9

Related Documents

Related Topic	Document Title
How to use the Cisco DCNM client	Chapter 3, "Using the Cisco DCNM Client"
Starting or stopping a Cisco DCNM server	Chapter 16, "Starting and Stopping Cisco DCNM Servers"
The process of deploying Cisco DCNM in your organization	*Cisco DCNM Installation and Licensing Guide, Release 5.x*
Installing a Cisco DCNM server	*Cisco DCNM Installation and Licensing Guide, Release 5.x*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Send document comments to nexus7k-docfeedback@cisco.com

Feature History for Installing and Launching the Cisco DCNM Client

Table 2-1 lists the release history for this feature.

Table 2-1 Feature History for Installing and Launching the Cisco DCNM Client

Feature Name	Releases	Feature Information
Using a command prompt to download the client.	5.0(2)	Support was added for this feature.
Proxy support for the Cisco DCNM client.	5.0(2)	Support was added for this feature.

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 3

Using the Cisco DCNM Client

This chapter describes the user interface of the Cisco Data Center Network Manager (DCNM) client and how to use common features.

This chapter includes the following sections:

Introducing the Cisco DCNM Client

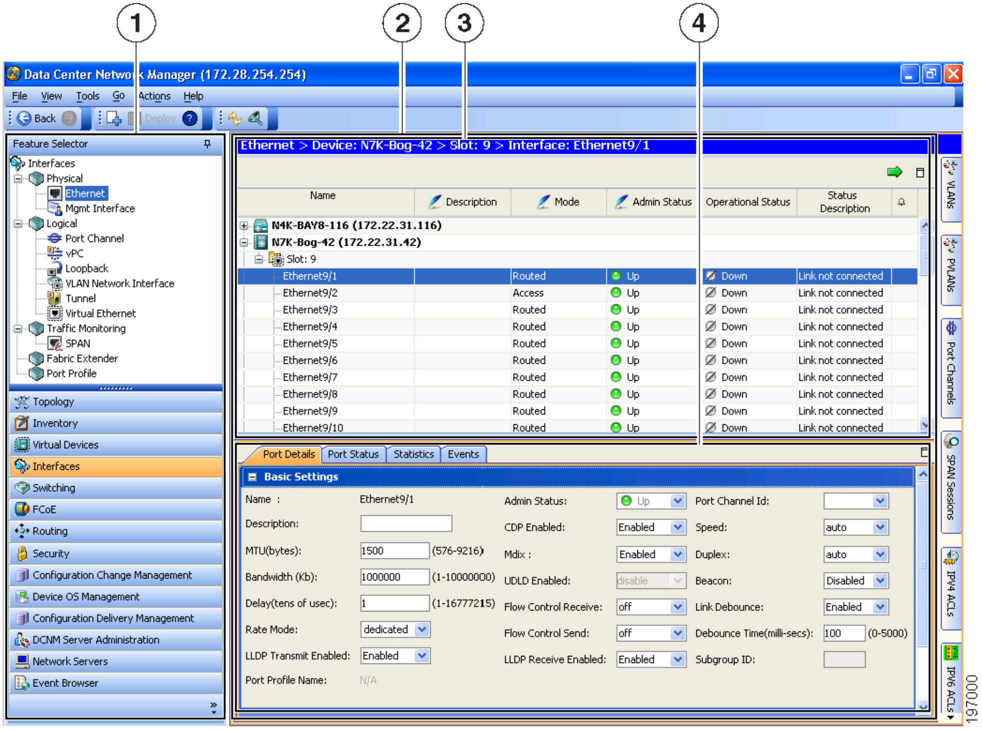
This section describes the Cisco DCNM client and its parts.

This section includes the following topics:

User Interface

The Cisco DCNM client user interface, shown in Figure 3-1, presents device status information and provides configuration tools that allow you to manage devices. It is divided into the panes shown in Figure 3-1. When you want to view information about a specific object in a managed device or want to perform a configuration task, you use the panes in the order shown in Figure 3-1.

Figure 3-1 Cisco DCNM Client User Interface



Ethernet > Device: N7K-Bog-42 > Slot: 9 > Interface: Ethernet9/1

Name	Description	Mode	Admin Status	Operational Status	Status Description
N4K-BAY8-116 (172.22.31.116)					
N7K-Bog-42 (172.22.31.42)					
Slot: 9					
Ethernet9/1		Routed	Up	Down	Link not connected
Ethernet9/2		Access	Up	Down	Link not connected
Ethernet9/3		Routed	Up	Down	Link not connected
Ethernet9/4		Routed	Up	Down	Link not connected
Ethernet9/5		Routed	Up	Down	Link not connected
Ethernet9/6		Routed	Up	Down	Link not connected
Ethernet9/7		Routed	Up	Down	Link not connected
Ethernet9/8		Routed	Up	Down	Link not connected
Ethernet9/9		Routed	Up	Down	Link not connected
Ethernet9/10		Routed	Up	Down	Link not connected

Name :	Ethernet9/1	Admin Status:	Up	Port Channel Id:	
Description:		CDP Enabled:	Enabled	Speed:	auto
MTU(bytes):	1500 (576-9216)	Mdix :	Enabled	Duplex:	auto
Bandwidth (Kb):	1000000 (1-10000000)	UDLD Enabled:	disable	Beacon:	Disabled
Delay(tens of usec):	1 (1-16777215)	Flow Control Receive:	off	Link Debounce:	Enabled
Rate Mode:	dedicated	Flow Control Send:	off	Debounce Time(milli-secs):	100 (0-5000)
LLDP Transmit Enabled:	Enabled	LLDP Receive Enabled:	Enabled	Subgroup ID:	
Port Profile Name:	N/A				

1	Feature Selector pane	2	Contents pane
3	Summary pane	4	Details pane

Feature Selector Pane

The Feature Selector pane, shown in Figure 3-1, allows you to see features grouped by categories and to choose the feature that you want to use or configure. The bottom section of the Feature Selector pane displays buttons for feature categories. When you choose a category, the top section of the Feature Selector pane displays a tree of features within the chosen category.

In Figure 3-1, the Interfaces category is chosen, so the tree shows features that allow you to configure the interfaces of managed devices.

The documentation and online help for Cisco DCNM includes many procedures that begin with choosing the applicable feature from the Feature Selector pane. For example, a procedure about configuring an Ethernet interface would start with the following step:

From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**.

After you choose a feature on the tree, the Contents pane displays information about the feature.

Contents Pane

The Contents pane, shown in Figure 3-1, displays information about the currently selected feature and provides fields for configuring that feature. The Contents pane contains two smaller panes: the Summary pane and the Details pane.

Summary Pane

The Summary pane, shown in Figure 3-1, displays an organized set of objects that you can view information about or perform actions on. The type of objects that appear depends upon the currently selected feature.

For example, if you choose Interfaces > Physical > Ethernet from the Feature Selector pane, the Summary pane shows a table of devices. You can expand the managed devices to view the slots that contain network interface cards. You can expand the slots to view the interfaces they contain and key information about the status of the interfaces, such as the port mode, administrative status, and operational status. For most features, the title bar for the Summary pane shows what you have selected.

After you choose the object that you want to view or configure, the Details pane displays information about the selected object, such as an Ethernet interface.

Exporting the Summary Pane

You can export the data shown in the Summary pane to a spreadsheet in Microsoft Excel 97-2003 format. To do so, click the green arrow in the upper-right corner of the Summary pane and specify the filename and location for the spreadsheet.

Filtering the Summary Pane

For many features, you can filter the objects that appear in the Summary pane. If filtering is supported for the feature that you selected, you can enable filtering from the menu bar by choosing View > Filter. In the Summary pane, the columns that you can use to filter the objects become drop-down lists. To filter the Summary pane, use the drop-down column heading lists to limit the objects that appear.

Details Pane

The Details pane, shown in Figure 3-1, shows information and configuration fields that are specific to the object that you selected in the Summary pane. The Details tab is often further divided into tabs. You can click on a tab to view its contents.

This section includes the following topics:

- Tabs, page 3-3
- Sections, page 3-4

Tabs

Tabs organize related fields and information. For example, as shown in Figure 3-1, when you select an Ethernet interface, four tabs appears in the Details pane, such as the Port Details tab.

The following two special tabs often appear in the Details pane for many of the types of objects that you can choose from the Summary pane:

- Statistics—You can use this tab to work with statistics and charts related to the selected object. For more information, see the "Working with Statistics and Charts" section on page 3-10.

Send document comments to nexus7k-docfeedback@cisco.com

- Events—You can use this tab to view feature-specific events about the selected object. For more information, see the *Cisco DCNM System Management Configuration Guide, Release 5.x*.

Sections

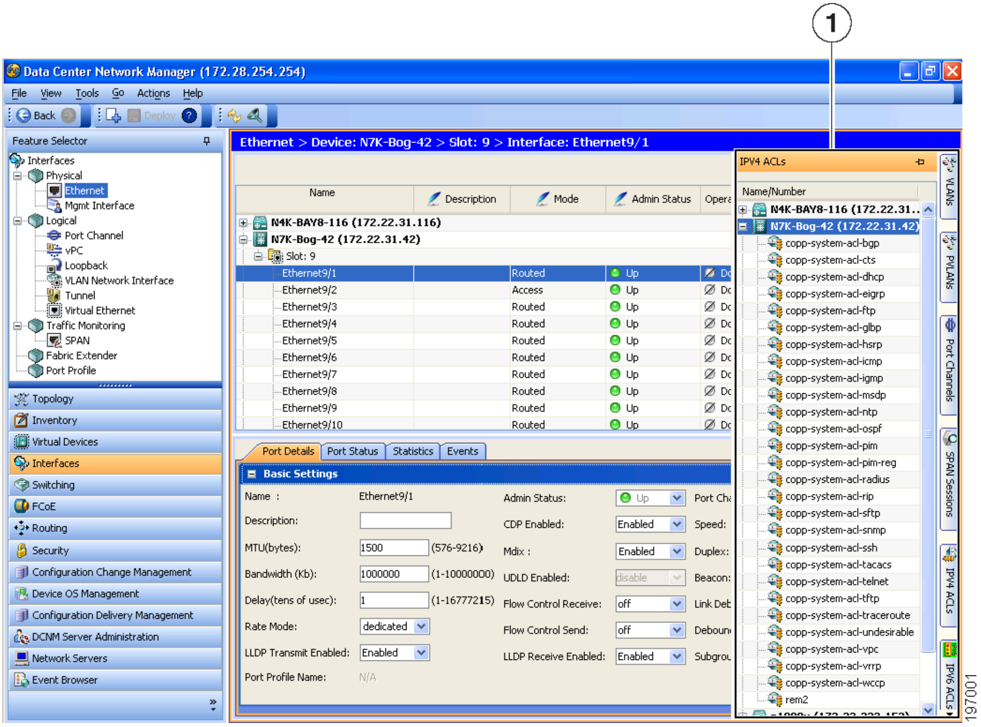
Sections provide further organization of related fields and information. The Cisco DCNM client allows you to expand and collapse sections so that you can show or hide fields and information as needed. For example, as shown in Figure 3-1, on the Port Details tab, the Basic Settings section is expanded but the Port Mode Settings section is collapsed.

Association Pane

The Cisco DCNM client also includes the Association pane, which allows you to access objects that you have configured in features that are associated with the currently selected feature. Figure 3-2 shows the Association pane.

When tabs appear on the right side of the Cisco DCNM client, you can click on them to access the Association pane. For example, as shown in Figure 3-2, if you are configuring an Ethernet interface, you can use the Association pane to access the IPv4 ACLs that you can apply to the interface. If you right-click on an IPv4 ACL in the Association pane, you can choose to apply the ACL to the interface or to go to the IPv4 ACLs feature and configure the ACL.

Figure 3-2 Association Pane



Ethernet > Device: N7K-Bog-42 > Slot: 9 > Interface: Ethernet9/1

Name	Description	Mode	Admin Status	Opera
N4K-BAY8-116 (172.22.31.116)				
N7K-Bog-42 (172.22.31.42)				
Slot: 9				
Ethernet9/1		Routed	Up	Dc
Ethernet9/2		Access	Up	Dc
Ethernet9/3		Routed	Up	Dc
Ethernet9/4		Routed	Up	Dc
Ethernet9/5		Routed	Up	Dc
Ethernet9/6		Routed	Up	Dc
Ethernet9/7		Routed	Up	Dc
Ethernet9/8		Routed	Up	Dc
Ethernet9/9		Routed	Up	Dc
Ethernet9/10		Routed	Up	Dc

Basic Settings

Name :	Ethernet9/1	Admin Status:	Up	Port Cha
Description:		CDP Enabled:	Enabled	Speed:
MTU(bytes):	1500 (576-9216)	Mdix :	Enabled	Duplex:
Bandwidth (Kb):	1000000 (1-10000000)	UDLD Enabled:	disable	Beacon:
Delay(tens of usec):	1 (1-16777215)	Flow Control Receive:	off	Link Deb
Rate Mode:	dedicated	Flow Control Send:	off	Deboun
LLDP Transmit Enabled:	Enabled	LLDP Receive Enabled:	Enabled	Subgrou
Port Profile Name:	N/A			

IPV4 ACLs

Name/Number
N4K-BAY8-116 (172.22.31..
N7K-Bog-42 (172.22.31.42)
copp-system-acl-bgp
copp-system-acl-cts
copp-system-acl-dhcp
copp-system-acl-eigrp
copp-system-acl-ftp
copp-system-acl-glbp
copp-system-acl-hsrp
copp-system-acl-icmp
copp-system-acl-igmp
copp-system-acl-msdp
copp-system-acl-ntp
copp-system-acl-ospf
copp-system-acl-pim
copp-system-acl-pim-reg
copp-system-acl-radius
copp-system-acl-rip
copp-system-acl-sftp
copp-system-acl-snmp
copp-system-acl-ssh
copp-system-acl-tacacs
copp-system-acl-telnet
copp-system-acl-tftp
copp-system-acl-traceroute
copp-system-acl-undesirable
copp-system-acl-vpc
copp-system-acl-vrrp
copp-system-acl-wccp
rem2

1	Association pane

Menus

The menu bar in the Cisco DCNM client includes the following standard menus that appear:

File Menu

- New—Allows you to create new objects. The types of objects that you can create depends upon the currently selected feature. In some cases, the object selected in the Summary pane also affects what you can create.
- Deploy—Saves your changes to the Cisco DCNM server and deploys configuration changes to managed devices.
- Exit—Closes the Cisco DCNM client.

View Menu

- Toolbars—Allows you to show or hide the toolbars that are available for the currently selected feature. For more information, see the "Toolbars" section on page 3-6.
- Refresh—Forces the Cisco DCNM client to retrieve updated information from the Cisco DCNM server.
- Filter—Enables or disables the filtering option for the Summary pane.

Tools Menu

- Preferences—Opens the Global Preferences dialog box. For more information, see the "Configuring Global Preferences" section on page 3-15.
- Debug—Opens the Cisco DCNM Client Logging dialog box, which allows you to configure the logging level for the Cisco DCNM client.

Note We recommend that you use the default client logging level unless you are troubleshooting a specific problem or are asked to change client logging levels by the Cisco technical support staff.

Go Menu

- Topology—Selects the Topology button on the Feature Selector pane.
- Inventory—Selects the Inventory button on the Feature Selector pane.
- Virtual Devices—Selects the Virtual Devices button on the Feature Selector pane.
- Interfaces—Selects the Interfaces button on the Feature Selector pane.
- Switching—Selects the Switching button on the Feature Selector pane.
- FCoE—Selects the FCoE button on the Feature Selector pane.
- Routing—Selects the Routing button on the Feature Selector pane.
- Security—Selects the Security button on the Feature Selector pane.
- Configuration Change Management—Selects the Configuration Change Management button on the Feature Selector pane.
- Device OS Management—Selects the Device OS Management button on the Feature Selector pane.

Send document comments to nexus7k-docfeedback@cisco.com

- Configuration Delivery Management—Selects the Configuration Delivery Management button on the Feature Selector pane.
- DCNM Server Administration—Selects the DCNM Server Administration button on the Feature Selector pane.
- Network Servers—Selects the Network Servers button on the Feature Selector pane.
- Event Browser—Selects the Event Browser button on the Feature Selector pane.

Actions Menu

The items on the Actions menu reflect what you can do, depending upon the feature you are using and the object that is selected in the Summary pane. For some features, such as Inventory, the Actions menu does not appear in the menu bar.

Help Menu

- Help Contents—Opens the online help system to the Welcome page.
- Context Help—Opens the online help system to a page that applies to the feature currently selected in the Feature Selector pane.
- Show DCNM Instance ID—Opens a dialog box that displays the license ID for your Cisco DCNM server. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
- View Licenses—Opens a dialog box that displays information about license files currently installed with your Cisco DCNM server.
- About Data Center Network Manager—Opens a dialog box that displays information about your Cisco DCNM server, including the software version and implementation version.

Toolbars

The Cisco DCNM client provides several standard toolbars plus additional, feature-specific toolbars that are available only when you have selected the applicable feature. The following table lists actions that you can take to configure toolbars.

Action	How To
Show or hide a toolbar	Right-click on the toolbar area and then choose the toolbar that you want to show or hide.
Rearrange toolbars	On a toolbar that you want to move, click on the left end of the toolbar and drag it to where you want it.
Float a toolbar	On the toolbar that you want to float, click on the left end of the toolbar and drag it off of the toolbar area.
Control whether a toolbar can be hidden, rearranged, or floated	Right-click on the toolbar area and then choose the option that you want to control.

Send document comments to nexus7k-docfeedback@cisco.com

Keyboard Commands

You can use the keyboard to perform many of the commands that you can perform with menu items or toolbars. The menus show the keyboard equivalent of most menu items. For example, the following list shows some common menu items and the matching keyboard command:

- Deploy—Ctrl + S
- Refresh—F5
- Filter—Ctrl + F
- Online help—F1
- Exit—Ctrl + Q

Multiple Platform Support

Cisco DCNM supports several types of Nexus platforms; however, some of the features supported in Cisco DCNM are not supported or applicable to all platforms. This section describes how DCNM handles unsupported features in the user interface.

- Unsupported Features—If a platform does not support a particular feature, the platform is not displayed for that feature.

  For example, if you choose **Security > Access Control > Time-range** from the Feature Selector pane, the Summary pane displays only the platform types that support the Time-range feature. In this case, the Cisco Nexus 1000V does not support this feature, so any managed Cisco Nexus 1000V platforms are not displayed in the Summary pane. Similarly, the Time-range association pane does not include any Cisco Nexus 1000V platforms.
- Unsupported Attributes—Sometimes, a platform supports a feature, but does not support a particular attribute in that feature. In this case, the attribute is grayed-out or a N/A (Not Applicable) value is displayed in the field or cell.

  If all attributes grouped in a particular section are not supported, then N/A is added to the section title, and Cisco DCNM does not allow you to expand the section.

  If all attributes in a tab are not supported for a particular platform, the tab is displayed, but if you click on it, a message appears stating that the attribute is not supported.
- Unsupported Charts—If a platform does not support some attributes in a chart, Cisco DCNM grays out those attributes. If a platform does not support any attributes in a chart, when you select the chart, Cisco DCNM displays a message stating that the chart is not supported.
- Unsupported Options—If a platform does not support an option, the option is not displayed, for example, in drop-down lists.
- Unsupported Operations— If a platform does not support an option for a specific operation on a context or toolbar menu, the option is grayed-out.

Send document comments to nexus7k-docfeedback@cisco.com

Opening the Cisco DCNM Client

You can open the Cisco DCNM client after you have installed the Cisco DCNM client on the computer that you are using.

BEFORE YOU BEGIN

Install the Cisco DCNM client on the computer that you are using. For more information about installing the Cisco DCNM client, see Chapter 2, "Installing and Launching the Cisco DCNM Client."

DETAILED STEPS

Step 1 From the start menu, choose **All Programs > Cisco DCNM Client > Cisco DCNM Client**.

Note If the Cisco DCNM client is not available on the All Programs menu, you can launch the Cisco DCNM client from the Cisco DCNM server website. For more information, see Chapter 2, "Installing and Launching the Cisco DCNM Client."

A dialog box displays login fields.

Step 2 In the DCNM Server field, enter the IP address or hostname of the Cisco DCNM server. You can use the hostname only if your DNS server has an entry for the Cisco DCNM server hostname. If you have previously logged into the server with the current client installation, you may be able to choose the IP address or hostname from the drop-down list.

Note If your Cisco DCNM deployment uses a clustered-server environment, enter the DNS name or IP address of the master Cisco DCNM server.

Step 3 In the Username field, enter the name of the Cisco DCNM server user account that you want to use to access the Cisco DCNM client.

Step 4 In the Password field, enter the password for the user account that you specified.

Step 5 (Optional) If you need to change the Cisco DCNM server port, do the following:

a. If the Port field is not visible, click **More >>.**

b. Enter the port number in the Port field.

The default Cisco DCNM server port number is 1099; however, you can specify a different port number when you install or reinstall the Cisco DCNM server.

Step 6 (Optional) If you need to use a proxy server to connect to the Cisco DCNM server, do the following:

a. If the "Connect to the DCNM server with a proxy server" check box is not visible, click **More >>**.

b. Check **Connect to the DCNM server with a proxy server**.

The Proxy Server area appears below the check box.

c. In the Address field, enter the IP address of the proxy server.

d. In the HTTP Port and Socks Port fields, enter the port numbers on which the proxy server accepts HTTP and Socks connections.

e. (Optional) If the proxy server requires authentication, check **Authentication** and enter a valid username and password in the fields provided.

Step 7 Click **Login**.

The Cisco DCNM client user interface appears.

If a dialog box displays a message about device credentials, you have not configured device credentials for the user account that you specified.

Step 8 If a dialog box shows a message that your device credentials are not set, do one of the following:

- If you want to set device credentials now, click **Yes**.
- If you do not want to set device credentials now, click **No**.

Note For information about setting device credentials, see the "Administering Devices and Credentials" section on page 6-1.

Closing the Cisco DCNM Client

You can close the Cisco DCNM client when you are done using it.

DETAILED STEPS

Step 1 From the menu bar, choose **File > Exit**.

A dialog box displays a confirmation message.

Step 2 (Optional) If you have not deployed your changes, do one of the following:

- If you want to save your changes, including deploying configuration changes to managed devices, check **Save pending changes**.
- If you want to discard your changes, uncheck **Save pending changes**.

Step 3 Click **Yes**.

If you started any statistical data collection processes during the Cisco DCNM client session, a dialog box displays the collection processes.

Step 4 If a dialog box displays the statistical data collection processes that you started, do the following:

a. Decide which statistical collection processes that you want to stop.

Note We recommend that you stop any unnecessary statistical collection processes when you log out of the Cisco DCNM client.

b. Check the collection processes that you want to stop. If you want to stop all of your collection processes, click **Select All**.

c. Click **Ok**.

Send document comments to nexus7k-docfeedback@cisco.com

Deploying Changes

When you use the Cisco DCNM client to make configuration changes to managed devices or to the Cisco DCNM server, you may need to deploy the changes or the Cisco DCNM client may deploy them automatically, depending upon what changes you have made.

- Automatic deployment—If the Cisco DCNM client deploys a change automatically, the “Deploying configuration” message appears briefly. For example, if you delete an access rule from an ACL, the Cisco DCNM client immediately deploys this configuration change to the managed device that has the ACL.
- Manual deployment—If the Cisco DCNM client is storing a configuration change, on the toolbar, the Deploy button is available. For example, if you change the sequence number of an access rule of an ACL, the Cisco DCNM client stores this configuration change until you manually deploy it to the managed device that has the ACL.

  To remind you of the necessity to deploy changes that the Cisco DCNM client is storing, the procedures in the Cisco DCNM documentation set include a deployment step.

Deploying server changes saves your changes on the Cisco DCNM server. For example, if you add a Cisco DCNM server user account, deploying your changes adds the user account to the Cisco DCNM server and does not affect managed devices.

Deploying configuration changes to a managed device causes the Cisco DCNM server to update the running configuration of the device.

Note Cisco DCNM does not update the startup configuration of a managed device. When you want to replace the startup configuration of a managed device with the running configuration, you can log into the command-line interface of the device and copy the running configuration to the startup configuration.

When you close the Cisco DCNM client and you have not deployed your changes, you can deploy them without canceling the process of closing the Cisco DCNM client. For more information, see the “Closing the Cisco DCNM Client” section on page 3-9.

Working with Statistics and Charts

This section describes how to use the statistical charts available on a Statistics tab.

This section includes the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

Information about Statistics and Charts

You can use a Statistics tab to start and stop statistical monitoring for an object and to work with charts of statistical data about the selected object. For each chart, the Cisco DCNM client also provides overview charts, which allow you to see historical trends and to control the time scale of the standard chart.

When you start monitoring for a new chart, Cisco DCNM creates a new statistical collection process that appears in the Statistical Data Collection feature. For more information, see the "Administering Statistical Data Collection" section on page 14-1.

Licensing Requirements for Statistics and Charts

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Real-time monitoring requires no license. Cisco DCNM requires a LAN Enterprise license for the following features: • Maintaining a history of statistical data • Using overview charts For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Accessing a Chart

You can access any chart. The charts that are available for a particular Statistics tab depend upon the feature and object selected.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose the feature for which you want to use a statistical chart.

For example, choose **Interfaces > Physical > Ethernet**.

Step 2 From the Summary pane, select an object.

The Statistics tab appears in the Details pane.

Note If no Statistics tab appears, then Cisco DCNM does not provide a statistical chart for the object that you selected.

Step 3 Click the **Statistics** tab.

In the Statistics tab, one or more charts may appear.

Send document comments to nexus7k-docfeedback@cisco.com

Note A dialog box may appear to confirm if you want to view charts for statistical collections that Cisco DCNM is running for the object that you selected in the Summary pane. For more information, see the "Configuring Monitoring Preferences" section on page 3-16.

Step 4 If the chart for the data that you want to monitor does not appear, from the toolbar, choose **New Chart** and then choose the chart that you want.

Step 5 Click the title bar of the chart that you want to work with.

The chart status appears in the lower left corner of the chart pane. If the chart is not active, you must start statistical monitoring for the chart before you can use it. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 3-12.

Starting Statistical Monitoring for a Chart

You can start statistical monitoring for a chart in the Statistics tab for any of the device configuration features that support statistical monitoring.

Note Each time that you start monitoring for a new chart, Cisco DCNM creates a new statistical collection process that appears in the Statistical Data Collection feature.

DETAILED STEPS

Step 1 Access the chart for which you want to start statistical monitoring. For more information, see the "Accessing a Chart" section on page 3-11.

Step 2 From the chart pane, click **Select Parameters**, check at least one statistical parameter that you want to appear in the chart, and click **Select Parameters** again.

Step 3 From the Monitor toolbar, choose the ▶ icon to start the collection process.

Step 4 The chart starts graphing the selected parameters.

Note When you close the Cisco DCNM client without stopping the statistical collection processes that you started, a dialog box prompts you to decide whether to stop the statistical collections or let them continue. We recommend that you stop any unnecessary statistical collection processes when you log out of the Cisco DCNM client.

Stopping Statistical Monitoring for a Chart

You can stop statistical monitoring for a chart in the Statistics tab.

Note When you stop monitoring for a chart, Cisco DCNM stops the corresponding statistical collection process that appears in the Statistical Data Collection feature.

DETAILED STEPS

Step 1 Access the chart for which you want to stop statistical monitoring. For more information, see the "Accessing a Chart" section on page 3-11.

Step 2 From the Monitor toolbar choose the 🔴 icon.

> **Note** If the chart that you want to stop does not appear, use the Statistical Data Collection feature to stop the collection process. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 3-12.

Using a Chart

The Cisco DCNM client provides the following options for using a chart:

- Changing parameters
- Setting the charting frequency
- Controlling the magnification of the chart data
- Showing, moving, and hiding threshold lines
- Tearing the chart away from the Cisco DCNM client window

This procedure provides basic instructions for using each of these options.

> **Note** For information about using an overview chart, see the "Using an Overview Chart" section on page 3-14.

DETAILED STEPS

Step 1 Access the chart that you want to use. For more information, see the "Accessing a Chart" section on page 3-11.

Step 2 If the chart is not active, you must start statistical monitoring for the chart before you can use it. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 3-12.

Step 3 (Optional) To change parameters, click **Select Parameters**, check the statistics parameters that you want to collect, and click **Select Parameters** again.

Step 4 (Optional) To set the frequency with which Cisco DCNM retrieves statistical data for the selected object, from the Select Frequency drop-down list on the Monitor tool bar, choose the new frequency.

Step 5 (Optional) To control the magnification, or zoom, of the chart, do one of the following:

- To zoom in on a portion of the chart, position the mouse pointer at one end of the portion, click and hold the left mouse button, drag the mouse pointer to the other end of the portion, and release the mouse button.
- To zoom in on a portion of the chart, position the mouse pointer at one end of the portion and then click and drag the mouse pointer to the other end of the portion.
- To change to the previous zoom, click the 🔍 icon.
- To change to the next zoom, click the 🔍 icon.

Send document comments to nexus7k-docfeedback@cisco.com

- To reset the zoom to the default magnification, click the ✥ icon.

Step 6 (Optional) To show, move, or hide threshold lines, do one of the following:

- To show or hide threshold lines, on the Monitor tool bar, click the ⇕ icon.
- To move the lower threshold line, click and drag the ◀ icon.
- To move the lower threshold line, click and drag the ▶ icon.

Step 7 (Optional) To tear the chart away from the Cisco DCNM client window, click on the red line that appears below the chart title.

Using an Overview Chart

You can use an overview chart to view the historical trend of the statistical data of the current chart and to set the time scale of the standard chart.

BEFORE YOU BEGIN

Ensure that any device with data that you want to view on an overview chart is included on the list of Cisco DCNM-licensed devices. For more information, see the "Licensing Requirements for Statistics and Charts" section on page 3-11.

DETAILED STEPS

Step 1 Access the chart that contains the overview chart that you want to use. For more information, see the "Accessing a Chart" section on page 3-11.

Step 2 If the chart is not active, you must start statistical monitoring for the chart before you can use its overview chart. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 3-12.

Step 3 Click **Show Overview Chart**.

In a new window, the overview chart displays the historical trends of the charted data.

Step 4 To set the time scale of the chart, at the bottom of the overview chart window, click the desired time scale button. The time scale buttons are as follows:

- RT—Real time
- 1d—One day
- 2d—Two days
- 5d—Five days
- 15d—Fifteen days
- 1m—One month
- 3m—Three months

Step 5 To close the overview chart, click **Show Overview Chart** again.

Send document comments to nexus7k-docfeedback@cisco.com

Exporting a Chart

You can export a chart as a JPG image or as a comma-separated value (CSV) file.

When you export a chart as a JPG image, the image is of the chart as it appears when you export the image.

When you export a chart as a CSV file, the file contains all data from the statistical collection for the chart.

DETAILED STEPS

Step 1 Access the chart that you want to use. For more information, see the "Accessing a Chart" section on page 3-11.

Step 2 If the chart is not active, you must start statistical monitoring for the chart before you can export an image of it. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 3-12.

Step 3 If you want to export an image, configure the chart to show the data that you want to appear in the image. For more information, see the "Using a Chart" section on page 3-13.

Step 4 Right-click on the chart.

Step 5 Choose one of the following:

- Export as CSV
- Export as JPG

Step 6 Specify the location and filename, and then click **Save**.

The Cisco DCNM client exports the chart in the file format that you specified.

Configuring Global Preferences

Using the Global Preferences dialog box, you can configure several preferences for how the Cisco DCNM client displays data and fields. The sections on the Global Preferences are as follows:

- Monitoring—Controls the default frequency of statistical data retrieval from managed devices and whether statistical charts open automatically. For more information, see the "Configuring Monitoring Preferences" section on page 3-16.
- Events—Controls the maximum age of events that the Cisco DCNM client fetches from the Cisco DCNM server when you start the Cisco DCNM client. For more information, see the "Configuring the Maximum Age of Events Fetched from the Server" section on page 3-16.
- Pre Provision—Controls whether the Cisco DCNM client displays some settings only when other settings are made or whether the Cisco DCNM client always displays all settings. For more information, see the "Configuring Preprovisioning" section on page 3-17.

Send document comments to nexus7k-docfeedback@cisco.com

Configuring Monitoring Preferences

You can configure the default frequency for statistical data retrieval from monitored devices. The default frequency for statistical data retrieval is 30 seconds. This frequency determines the initial data retrieval frequency for a new chart. Users can override the default frequency by configuring the chart-specific setting.

You can also configure whether the Cisco DCNM client automatically opens statistical charts when you access the Statistics tab of an object for which Cisco DCNM is already collecting statistical data.

BEFORE YOU BEGIN

Determine how often you want Cisco DCNM to retrieve statistical data by default. Consider how important it is to your organization that charts update frequently. If very current charting data is important to your organization, consider using a short data retrieval frequency.

DETAILED STEPS

Step 1 From the menu bar, choose **Tools > Preferences**.

The Global Preferences dialog box appears. Under Monitoring, the Default Monitoring Frequency drop-down list displays the current frequency for statistical data retrieval.

The default polling frequency is 30 seconds.

Step 2 If you want to configure the default frequency of statistical data retrieval, from the Default Monitoring Frequency drop-down list, choose the new data retrieval frequency.

Step 3 If you want to configure the default behavior when you access the Statistics tab of an object for which Cisco DCNM is already collecting statistical data, do one of the following:

- If you want the client to show charts without asking for confirmation, check the **Load history charts by default** check box.
- If you want the client to prompt you for confirmation before it opens statistical charts, uncheck the **Load history charts by default** check box.

Step 4 Click **Ok**.

Configuring the Maximum Age of Events Fetched from the Server

You can configure the maximum age of events that the Cisco DCNM client fetches from the Cisco DCNM server when you start the Cisco DCNM client. This setting affects how old the events are that the Cisco DCNM client displays in the Event Browser and on feature-specific Events tabs. By default, the Cisco DCNM client fetches events that occurred up to 1 hour prior to the Cisco DCNM client startup. You can configure the Cisco DCNM client to fetch events that are up to 24 hours old.

DETAILED STEPS

Step 1 From the menu bar, choose **Tools > Preferences**.

The Global Preferences dialog box appears. Under Events, the Fetch events before drop-down list displays the current maximum age of events.

Send document comments to nexus7k-docfeedback@cisco.com

Step 2 From the Fetch events before drop-down list, choose the new maximum age of events.

Note To prevent the Cisco DCNM client from fetching any old events, choose zero (0) hours as the maximum age of events. When you choose zero hours, the Cisco DCNM client shows only the events that the Cisco DCNM server receives after you start the Cisco DCNM client.

Step 3 Click **Ok**.

Configuring Preprovisioning

Preprovisioning refers to configuring a managed device with settings for modes or protocols that are not enabled. The preprovisioning preference affects the following sections of the Cisco DCNM client interface:

- Interfaces > Physical > Ethernet > Device > Slot > Interface, Port Details tab, Port Mode Settings section

  When you enable preprovisioning, the Cisco DCNM client displays all port mode fields regardless of the setting in the Mode drop-down list. When you disable preprovisioning, the Cisco DCNM client displays only the port mode settings that are relevant to the currently selected port mode. For example, if preprovisioning is disabled and you choose Trunk from the Mode drop-down list, the Cisco DCNM client displays only the Trunk settings and hides the Access, PVLAN Host, and PVLAN Promiscuous fields.

  Additionally, the dialog boxes for configuring the Access VLAN field and the Native VLAN field include the Create in the Device check box. When you enable preprovisioning, you can uncheck this check box if you want Cisco DCNM to configure the device to refer to a VLAN that is not currently configured. When you disable preprovisioning, this check box is always checked and Cisco DCNM creates the VLAN specified, if it does not already exist.

- Switching > Spanning Tree > Device, Configuration tab, Global Settings section

  When you enable preprovisioning, the Cisco DCNM client displays MST settings regardless of the settings in the Protocol drop-down list. When you disable preprovisioning, the Cisco DCNM client displays the MST Setting fields unless you choose MST from the Protocol drop-down list.

DETAILED STEPS

Step 1 From the menu bar, choose **Tools > Preferences**.

The Global Preferences dialog box appears. Under Pre Provision, the Pre Provision check box appears.

Step 2 Do one of the following:

- If you want to enable preprovisioning, ensure that the **Pre Provisio**n check box is checked.
- If you want to disable preprovisioning, ensure that the **Pre Provision** check box is unchecked.

Step 3 Click **Ok**.

Send document comments to nexus7k-docfeedback@cisco.com

Using Online Help

Online help has the following features:

- Contents—The organization of Cisco DCNM online help is shown in the Contents tab of the online help window. When a topic has subtopics, the book icon appears to the left of the topic in the contents.

  You can expand and collapse individual topics in the contents. You can also collapse or expand all topics.
- Index—Cisco DCNM online help includes an index, which allows you to look up subjects alphabetically and open related topics directly from the index.
- Favorites—Cisco DCNM online help allows you to add specific topics to the Favorites tab. Favorites are stored locally on the computer that you use to access online help.

To access the welcome page in online help, from the menu bar, choose **Help > Help Contents**.

Cisco DCNM online help includes context-sensitive help.

To access context-sensitive help for a feature, follow these steps:

Step 1 Select a specific feature from the Feature Selector pane in the Cisco DCNM client. For example, choose **Security > Access Control > IPv4 ACL**.

Step 2 Do one of the following:

- Press **F1**.
- From the toolbar, click the question mark icon.

Online help for the selected feature appears in a browser window. Cisco DCNM uses the default browser application on the computer that runs the Cisco DCNM client.

Additional References

For additional information related to using the Cisco DCNM client, see the following sections:

- Related Documents, page 3-18
- Standards, page 3-19

Related Documents

Related Topic	Document Title
Installing and launching the Cisco DCNM client	Chapter 2, "Installing and Launching the Cisco DCNM Client"
Information about using specific Cisco DCNM features	Obtaining Documentation and Submitting a Service Request, page xix

Send document comments to nexus7k-docfeedback@cisco.com

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Using the Cisco DCNM Client

Table 3-1 lists the release history for this feature.

Table 3-1 Feature History for Installing and Launching the Cisco DCNM Client

Feature Name	Releases	Feature Information
Global preferences	5.0(2)	Support was added for the "Load history charts by default" check box.
Multiple platform support	5.0(2)	Information was added about how the Cisco DCNM client supports management of different Cisco NX-OS device types.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 4

Administering DCNM Authentication Settings

This chapter describes how to administer Cisco Data Center Network Manager (DCNM) authentication settings.

This chapter includes the following sections:

Information About Administering Cisco DCNM Authentication Settings

Cisco DCNM authentication settings determine how a Cisco DCNM server authenticates users who attempt to access the server with the Cisco DCNM client. They also determine the user role for the user, which affects what the user can configure in the Cisco DCNM client.

This section contains the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

Users and User Roles

Cisco DCNM implements user-based access to allow you to control who can access a Cisco DCNM server by using the Cisco DCNM client. User access is secured by a password. Cisco DCNM supports strong passwords.

When you ensure that each person who accesses Cisco DCNM has a unique user account, user-based access allows you to determine what actions are taken by each user.

In addition, Cisco DCNM allows you to assign a role to each user. Roles determine what actions a user can take in the Cisco DCNM client. As described in Table 4-1, Cisco DCNM supports two user roles.

Table 4-1 Cisco DCNM User Roles

Cisco DCNM Role	Description
User	• Cannot change Cisco DCNM authentication mode • Cannot add or delete Cisco DCNM local user accounts • Can change the details of its own local user account • Can use all other features
Administrator	• Has full control of Cisco DCNM authentication settings • Can use all other features

Local Authentication and Cisco DCNM Local Users

The Cisco DCNM database contains any Cisco DCNM local users that you create.

Note Cisco DCNM server users are local to the Cisco DCNM server. Creating, changing, and removing Cisco DCNM server users has no effect on user accounts on managed devices.

A Cisco DCNM server uses local users to grant access in the following cases:

- When the authentication mode is local
- When no authentication server for the current authentication mode is reachable.

You can use local authentication as the primary authentication mode. If you specify RADIUS or TACACS+ as the primary authentication mode, the Cisco DCNM server always falls back to local authentication if no authentication server for the current authentication mode is reachable.

RADIUS and TACACS+ Authentication

You can configure Cisco DCNM to authenticate users with either the RADIUS or TACACS+ AAA protocol.

Cisco DCNM supports primary, secondary, and tertiary authentication servers for RADIUS and TACACS+. Only a primary server is required. For each authentication server, you can specify the port number that the server listens to for authentication requests.

Send document comments to nexus7k-docfeedback@cisco.com

During authentication, if the primary server for the current authentication mode does not respond to the authentication request, the Cisco DCNM server sends the authentication request to the secondary server. If the secondary server does not respond, Cisco DCNM sends the authentication request to the tertiary server.

If none of the servers configured for the current authentication mode responds to an authentication request, the Cisco DCNM server falls back to local authentication.

User Role Assignment by RADIUS and TACACS+

Cisco DCNM supports the assignment of a user role by the RADIUS or TACACS+ server that grants a user access to the Cisco DCNM client. The user role assigned to a user is in effect for the current session in the Cisco DCNM client only.

To assign a Cisco DCNM user role by RADIUS, configure the RADIUS server to return the RADIUS vendor-specific attribute 26/9/1, which is the Cisco-AV-Pair attribute. To assign a Cisco DCNM user role by TACACS+, the TACACS+ server must return a cisco-av-pair attribute-value pair. If an authentication response does not assign the user role, Cisco DCNM assigns the User role. Table 4-2 shows the supported attribute-value pair values for each Cisco DCNM user role.

Table 4-2 Cisco DCNM User Role Assignment Values

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell cisco-av-pair Value
User	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

Fallback to Local Authentication

Local authentication always is the fallback method for RADIUS and TACACS+ authentication modes. If none of the servers configured for the current authentication mode is available, the Cisco DCNM server uses the local database to authenticate login requests. This behavior is designed to help you prevent accidental lockout from Cisco DCNM.

For users who need fallback support, the usernames of their local user accounts must be identical to their usernames on the authentication servers. Also, we recommend that their passwords in the local user accounts should be identical to their passwords on the authentication servers in order to provide transparent fallback support. Because the user cannot determine whether an authentication server or the local database is providing the authentication service, using usernames and passwords on authentication servers that are different than the usernames and passwords in the local database means that the user cannot be certain which username and password should be given.

Password Recovery

If no one can log into the Cisco DCNM client as a user with a Cisco DCNM Administrator role, you can reset passwords by using one of the following scripts:

- For Microsoft Windows, use *dcnm_root_directory*/dcm/dcnm/bin/pwreset.bat (by default, *dcnm_root_directory* is c:\Program Files\Cisco Systems\dcm\dcnm\bin).

Send document comments to nexus7k-docfeedback@cisco.com

- For Linux, use *dcnm_root_directory*/dcm/dcnm/bin/pwreset.sh (by default, the *dcnm_root_directory* is /usr/local/cisco).

To reset a password, run the script for the operating system that you are using, and then enter the user ID to be reset and the password to be used for it.

Alternatively, you can reinstall the Cisco DCNM server, which allows you to specify the username and password for a local user account that is assigned the Administrator role. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Users and Device Credentials

Each Cisco DCNM server user has unique device credentials, regardless of whether the user authenticates with a local user account or an account on a RADIUS or TACACS+ server. This feature allows you to maintain accounting logs on managed devices that reflect the actions of each Cisco DCNM server user. For more information, see the "Information About Devices and Credentials" section on page 6-1.

Virtualization Support

Cisco NX-OS support for virtual device contexts has no effect on Cisco DCNM server users.

Cisco DCNM server users can configure any managed device.

Licensing Requirements for Administering DCNM Authentication Settings

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Administering Cisco DCNM authentication settings requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Administering DCNM Authentication Settings

Administering Cisco DCNM authentication settings has the following prerequisites:

- You must ensure that every authentication server that you want to use with Cisco DCNM is configured to accept authentication requests from the Cisco DCNM server. If you have deployed Cisco DCNM in a clustered-server environment, ensure that every authentication server is configured to accept requests from each Cisco DCNM server in the cluster.
- To add, delete, or modify Cisco DCNM local users, you must be logged into the Cisco DCNM client with a user account that is assigned the Administrator Cisco DCNM role.

Send document comments to nexus7k-docfeedback@cisco.com

Guidelines and Limitations for Administering DCNM Authentication Settings

Administering Cisco DCNM authentication settings has the following configuration guidelines and limitations:

- Create a Cisco DCNM user account for each person who uses the Cisco DCNM client. Do not allow people to share a user account.
- Delete unused Cisco DCNM user accounts.
- Grant an administrator user account only to those who need to perform administrator tasks in the Cisco DCNM client.
- We recommend that you use strong passwords. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

Configuring DCNM Authentication Settings

This section includes the following topics:

Configuring the Authentication Mode

You can configure the mode that the Cisco DCNM server uses to authenticate Cisco DCNM client users.

BEFORE YOU BEGIN

Log into the Cisco DCNM client with a user account that has the Administrator user role.

If you want to enable RADIUS or TACACS+ authentication mode, you must configure at least one authentication server for the desired authentication mode.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the Authentication Mode section.

Step 3 Choose the authentication mode.

Step 4 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Step 5 Restart the Cisco DCNM server. For more information, see the Chapter 16, "Starting and Stopping Cisco DCNM Servers."

Adding a Cisco DCNM Local User

You can add a Cisco DCNM local user account.

Note Adding a Cisco DCNM local user account does not affect the user account configuration on any Cisco NX-OS device.

BEFORE YOU BEGIN

Log into the Cisco DCNM client with a user account that has the Administrator user role.

Determine the username and password for the new Cisco DCNM local user account.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the Cisco DCNM Local Users section.

Step 3 From the menu bar, choose **Actions > Add User**.

A new row appears at the bottom of the list of users. By default, all fields in the new row are blank.

Step 4 In the DCNM User Name column of the new row, enter the username. The username can be 1 to 198 characters. Entries can contain case-sensitive letters, numbers, and symbols.

Step 5 (Optional) In the Full Name column, double-click the entry and add a name. For example, enter the real name of the person who will use the Cisco DCNM local user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 6 In the DCNM Role column, double-click the entry and choose the role. By default, the role is User.

Step 7 In the Password column, double-click the entry and then click the down-arrow button.

Step 8 In the New Password field and the Confirm Password field, enter the password. The password can be 1 to 255 characters. Entries can contain case-sensitive letters, numbers, and symbols.

Step 9 Click **OK**.

Step 10 (Optional) In the Description column, double-click the entry and add a description of the user account. For example, you could use this entry to provide e-mail and telephone contact details of the person who will be using this Cisco DCNM server user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 11 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Changing the Password of a Cisco DCNM Local User

You can change the password of a Cisco DCNM local user.

BEFORE YOU BEGIN

An Administrator role is required if you want to change the password of a local user account other than the account that you use to log into the Cisco DCNM client. If your user account is a local user account and it has the User role, you can change the password of your account only.

Determine what the new password should be.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Authentication Settings**.

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the DCNM Local Users section.

Step 3 In the User Name column, click the username for the user account that you want to change.

The row of the username that you clicked is highlighted.

Step 4 In the Password column, double-click the entry and then click the down-arrow button.

Step 5 In the New Password field and the Confirm Password field, enter the new password. The password can be 1 to 255 characters. Entries can contain case-sensitive letters, numbers, and symbols.

Step 6 Click **OK**.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Changing the Full Name, Role, or Description of a Cisco DCNM Local User

You can change the full name, role, or description of a Cisco DCNM local user.

Note You cannot change the username. Instead, add a local user account with the desired username and remove the local user account with the unwanted username.

BEFORE YOU BEGIN

Determine what the new full name or description should be.

An Administrator role is required if you want to change the full name, role, or description of a local user account other than the local user account that you use to log into the Cisco DCNM client. If your user account is a local user account and it has the User role, you can change the full name and description for your account only.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the Cisco DCNM Local Users section.

Step 3 In the User Name column, click the username of the local user account that you want to change.

The row of the username that you clicked is highlighted.

Step 4 (Optional) In the Full Name column, double-click the entry and enter the new name. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 5 (Optional) In the DCNM Role column, double-click the entry and choose the new role. You can choose Administrator or User.

Step 6 (Optional) In the Description column, double-click the entry and enter the new description of the user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Deleting a Cisco DCNM Server User

You can remove a Cisco DCNM local user account.

BEFORE YOU BEGIN

Log into the Cisco DCNM client with a user account that has the Administrator user role.

Ensure that you are removing the correct Cisco DCNM local user account.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the DCNM Local Users section.

Step 3 In the User Name column, click the username of the user account that you want to remove.

The row of the username that you clicked is highlighted.

Step 4 From the menu bar, choose **Actions > Delete User**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Adding Authentication Servers

You can add RADIUS and TACACS+ servers to the Cisco DCNM authentication settings.

BEFORE YOU BEGIN

Note You must ensure that every authentication server that you want to use with Cisco DCNM is configured to accept authentication requests from the Cisco DCNM server. If you have deployed Cisco DCNM in a clustered-server environment, ensure that every authentication server is configured to accept requests from each Cisco DCNM server in the cluster.

Ensure that you have the following information about each authentication server that you want to add:

- AAA protocol: RADIUS or TACACS+
- Server IPv4 address or DNS name that can be resolved by the Cisco DCNM server.
- Secret key.
- Port number on which the server accepts authentication requests.
- (RADIUS only) Port number on which the server accepts accounting messages.
- Authentication protocol: PAP, CHAP, MSCHAP, or ASCII.
- (Optional) Username and password of a valid user account on the server for server verification.

Determine whether the server should be a primary, secondary, or tertiary server, which depends upon your authentication server failover strategy.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 If necessary, expand the **RADIUS** or **TACACS+** server rows.

Step 4 For each authentication server that you want to add, follow these steps:

a. Choose the row in which you want to add the server.

Note The Cisco DCNM client does not allow you to add a secondary server if you have not added a primary server. In addition, you cannot add a tertiary server if you have not added a secondary server.

b. Double-click the **Server Name** field and enter the server IPv4 address or DNS hostname.

Note If you enter a hostname that the Cisco DCNM server cannot resolve, the Server Name field is highlighted in red.

c. Double-click the **Secret Key** field and enter the secret key (sometimes called a shared secret) of the authentication server.

d. (Optional) If you need to change the default Authentication Port or Accounting Port (RADIUS only), double-click the applicable port field and enter the new port number.

e. Double-click the **Authentication Method** field and choose the authentication protocol that Cisco DCNM must use when sending authentication requests to the authentication server.

Step 5 (Optional) If you want to verify that the Cisco DCNM server can authenticate a user with a new authentication server, follow these steps:

a. To the right of the row for the authentication server that you want to verify, click **Verify**.

A Verification dialog box appears.

b. Enter a username and password for a valid user account on the authentication server.

c. Click **Verify**.

The Cisco DCNM client displays a message indicating whether the verification attempt succeeded or failed. A verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Changing Authentication Server Settings

You can change the settings for authentication servers that you have already configured in the Cisco DCNM client. If you have more than one RADIUS or TACACS+ server, you can change which server is primary, secondary, or tertiary.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 If necessary, expand the **RADIUS** or **TACACS+** server rows.

Step 4 (Optional) If you want to change the settings of an authentication server, double-click each field that you need to change and enter the changes.

Step 5 (Optional) If you want to reorder RADIUS or TACACS+ servers, right-click a server and choose **Move Up** or **Move Down**, as needed.

Step 6 (Optional) If you want to verify that the Cisco DCNM server can authenticate a user with an authentication server, follow these steps:

a. To the right of the row for the authentication server that you want to verify, click **Verify**.

A Verification dialog box appears.

b. Enter a username and password for a valid user account on the authentication server.

c. Click **Verify**.

The Cisco DCNM client displays a message indicating whether the verification attempt succeeded or failed. A verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Removing an Authentication Server

You can remove a RADIUS or TACACS+ authentication server from the Cisco DCNM authentication settings.

BEFORE YOU BEGIN

You cannot remove all authentication servers for the current authentication mode. Instead, change the authentication mode first and then remove all the authentication servers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 If necessary, expand the **RADIUS** or **TACACS+** server rows.

Step 4 Right-click the authentication server that you want to remove and choose **Remove Server**.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Send document comments to nexus7k-docfeedback@cisco.com

Viewing Cisco DCNM Local Users

To view Cisco DCNM server user accounts, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings** and then, if necessary, expand the Cisco DCNM Local Users section.

Cisco DCNM server user accounts, including usernames and descriptions, appear in the Contents pane. Passwords appear masked for security. For information about the fields that appear, see the "Field Descriptions for DCNM Authentication Settings" section on page 4-13.

Verifying Authentication Server Settings

You can verify that the Cisco DCNM server can authenticate a user with a particular authentication server that you have configured.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 Click **Verify**.

A Verification dialog box appears.

Step 4 Enter a username and password for a valid user account on the authentication server.

Step 5 To the right of the row for the authentication server that you want to verify, click **Verify**.

The Cisco DCNM client displays a message indicating whether the verification attempt succeeded or failed. A verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.

Send document comments to nexus7k-docfeedback@cisco.com

Field Descriptions for DCNM Authentication Settings

This section includes the following field descriptions for the DCNM Authentication Settings feature:

- Authentication Mode Section, page 4-13
- Cisco DCNM Local Users Section, page 4-13
- Authentication Servers Section, page 4-14

Authentication Mode Section

Table 4-3 Authentication Mode Section

Field	Description
Local	Whether Cisco DCNM authenticates users with the local user database only.
RADIUS	Whether Cisco DCNM authenticates users with a RADIUS server. When no configured RADIUS server is reachable, Cisco DCNM falls back to using the local database for user authentication.
TACACS+	Whether Cisco DCNM authenticates users with a TACACS+ server. When no configured TACACS+ server is reachable, Cisco DCNM falls back to using the local database for user authentication.

Cisco DCNM Local Users Section

Table 4-4 Cisco DCNM Local Users Section

Field	Description
Cisco DCNM User Name	*Display only.* Name of the Cisco DCNM server user account. This name can be used to log into the Cisco DCNM client when the authentication mode is local or when no authentication server for the current authentication mode is reachable. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. The minimum length is 1 character. The maximum length is 198 characters.
Full Name	Other name for the user account, such as the name of the person who uses the Cisco DCNM server user account. This name cannot be used to log into the Cisco DCNM client. Valid characters are all letters, numbers, and symbols. The maximum length is 255 characters. This field is blank by default.
Cisco DCNM Role	Role of the user account. Valid values are User and Administrator. For more information, see Table 4-1. By default, a Cisco DCNM server user account is assigned the role of User.
Password	Password for the Cisco DCNM server user. This field is always masked for security. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. The minimum length is 1 character. The maximum length is 255 characters.

Table 4-4 Cisco DCNM Local Users Section (continued)

Field	Description
Description	Description of the Cisco DCNM server user. Valid characters are all letters, numbers, and symbols. The maximum length is 255 characters. This field is blank by default.

Authentication Servers Section

Table 4-5 Authentication Servers Section

Field	Description
Server Name	DNS name or IPv4 address of the authentication server. • DNS name—If you specify a DNS name, the Cisco DCNM server must be able to resolve the IP address of the server. Valid DNS names characters are alphanumeric. • IPv4 address—If you specify an IP address, valid entries are in dotted decimal format.
Secret Key	Shared secret of the authentication server. Valid entries are case-sensitive letters, numbers, and symbols.
Authentication Port	TCP or UDP port number that the authentication server listens to for authentication requests. By default, the authentication port for a RADIUS server is UDP port 1812 and the authentication port for a TACACS+ server is TCP port 49.
Accounting Port	UDP port number that the RADIUS authentication server listens to for authentication requests. By default, the accounting port for a RADIUS server is UDP port 1813.
Authentication Method	Authentication protocol that the Cisco DCNM server uses in authentication requests to the authentication server. Supported authentication methods are as follows: • PAP • CHAP • MSCHAP • ASCII

Additional References

For additional information related to administering Cisco DCNM authentication settings, see the following sections:

- Related Documents, page 4-15
- Standards, page 4-15

Send document comments to nexus7k-docfeedback@cisco.com

Related Documents

Related Topic	Document Title
Logging into the Cisco DCNM client	*Opening the Cisco DCNM Client, page 3-8*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for DCNM Authentication Settings

Table 4-6 lists the release history for this feature.

Table 4-6 Feature History for Cisco DCNM Server Users

Feature Name	Releases	Feature Information
DCNM Authentication Settings	5.0(2)	No change from Release 4.2.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 5

Administering Device Discovery

This chapter describes how to administer the Device Discovery feature in the Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Device Discovery

This section includes the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

Device Discovery

The Device Discovery feature creates devices in Cisco DCNM by connecting to a Cisco NX-OS device and retrieving data from the device, including its running configuration. Cisco DCNM can also discover Cisco NX-OS devices and network servers that are neighbors of the first device, which is known as the *seed device*.

If the device supports virtual device contexts (VDCs), Cisco DCNM retrieves the running configuration of each VDC that is configured on the physical device. Cisco DCNM displays each VDC as a device, including the default VDC. If the Cisco NX-OS device has only the default VDC, then device discovery creates only one device in Cisco DCNM.

When Cisco DCNM connects to a device to retrieve its configuration, it uses the XML management interface, which uses the XML-based Network Configuration Protocol (NETCONF) over Secure Shell (SSH). For more information, see the *Cisco NX-OS XML Management Interface User Guide, Release 5.x*.

Discovery Protocols

Cisco DCNM uses a variety of protocols to discover devices and servers in your data center network. This section includes the following topics:

- Cisco Discovery Protocol, page 5-2
- Link Layer Discovery Protocol, page 5-2
- Fibre Channel, page 5-3

Cisco Discovery Protocol

Device discovery uses the Cisco Discovery Protocol (CDP) to find devices that are connected to the initial device in the discovery process. CDP exchanges information between adjacent devices over the data link layer. The exchanged information is helpful in determining the network topology and physical configuration outside of the logical or IP layer.

CDP allows Cisco DCNM to discover devices that are one or more hops beyond the seed device in the discovery process. When you start the discovery process using the Device Discovery feature, you can limit the number of hops that the discovery process can make.

After Cisco DCNM discovers a Cisco NX-OS device using CDP, it connects to the device and retrieves information, such as the running configuration of the device. The information collected allows Cisco DCNM to manage the device.

Cisco DCNM supports CDP hops on some Cisco switches that run Cisco IOS software. Although Cisco DCNM cannot manage these devices, the Topology feature allows you to see unmanaged devices and the CDP links between unmanaged devices and managed devices.

Link Layer Discovery Protocol

Device discovery uses Link Layer Discovery Protocol (LLDP) to discover the network adapters of servers that are connected to Cisco NX-OS devices. For more information, see Chapter 9, “Configuring Network Servers.”

Fibre Channel

To discover network elements in a storage area network (SAN), Cisco DCNM uses Fibre Channel. Cisco DCNM can discover SAN switches, servers, and storage arrays.

Credentials and Discovery

Device discovery requires that you provide a username and password for a user account on the seed device. To successfully complete the discovery of a Cisco NX-OS device, the user account that you specify must be assigned to either the network-admin or the vdc-admin role.

If you want to discover devices that are one or more hops from the seed device, all devices in the chain of hops must be configured with a user account of the same username and password. All Cisco NX-OS devices in the chain of hops must assign the user account to the network-admin or the vdc-admin role.

Discovery Process

Cisco DCNM discovers devices in several phases, as follows:

1. CDP neighbor discovery—Discovers the topology of the interconnected devices, beginning with the seed device and preceding for the number of CDP hops specified when you initiate discovery.
2. Supported device selection—Determines which of the discovered devices are supported by Cisco DCNM. Discovery continues for the supported devices only.
3. Inventory discovery—Discovers the inventory of the devices selected in the previous phase. For example, if the device is a Cisco Nexus 7000 Series switch, inventory discovery determines the supervisor modules, I/O modules, power supplies, and fans. If the device is a Cisco Nexus 1000V switch, inventory discovery finds the Virtual Supervisor Module and Virtual Ethernet Modules.
4. Device configuration discovery—Discovers the details of feature configuration on each device, such as interfaces, access control lists, and VLANs.
5. Network discovery—Associates network features with the device configuration details discovered in the previous phase.

Cisco NX-OS System-Message Logging Requirements

To monitor and manage devices, Cisco DCNM depends partly on system messages that it retrieves from managed devices. This section describes the system-message requirements that all Cisco NX-OS devices must meet before they can be managed and monitored by Cisco DCNM.

This section includes the following topics:

- Interface Link-Status Events Logging Requirement, page 5-4
- Logfile Requirements, page 5-4
- Logging Severity-Level Requirements, page 5-4

Send document comments to nexus7k-docfeedback@cisco.com

Interface Link-Status Events Logging Requirement

Devices must be configured to log system messages about interface link-status change events. This requirement ensures that Cisco DCNM receives information about interface link-status changes. The following two commands must be present in the running configuration on the device:

logging event link-status enable

logging event link status default

To ensure that these commands are configured on the device, perform the steps in the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Logfile Requirements

Devices must be configured to store system messages that are severity level 6 or lower in the log file.

Although you can specify any name for the log file, we recommend that you do not change the name of the log file. When you change the name of the log file, the device clears previous system messages. The default name of the log file is "messages."

If you use the default name for the log file, the following command must be present in the running configuration on the device:

logging logfile messages 6

To ensure that this command is configured on the device, perform the steps in the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Logging Severity-Level Requirements

Cisco DCNM has minimum severity level requirements for some Cisco NX-OS logging facilities. All enabled features on a Cisco NX-OS have a default logging level. The logging level required by Cisco DCNM varies per logging facility but is often higher than the default logging level in Cisco NX-OS. For more information, see the "Automatic Logging-Level Configuration Support" section on page 5-4.

Automatic Logging-Level Configuration Support

Cisco DCNM provides support for automatic logging level configuration for all supported Cisco NX-OS releases with the exception of Cisco NX-OS Release 4.0, which is available on Cisco Nexus 7000 Series switches only. This section describes how Cisco DCNM supports automatic logging-level configuration. For information about manually configuring logging levels for Cisco NX-OS Release 4.0, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

During Device Discovery

During device discovery, if Cisco DCNM finds that a logging level on a discovered device is below the minimum logging-level requirement for that logging facility, Cisco DCNM raises the logging level to meet the minimum requirement. If logging levels meet or exceed the requirements, Cisco DCNM does not change the logging levels during discovery.

Send document comments to nexus7k-docfeedback@cisco.com

At Feature Enablement in the Cisco DCNM Client

If you use the Cisco DCNM client to enable a feature on a device and the default logging level for the feature does not meet the minimum requirement, the Cisco DCNM client warns you that it will configure the logging level on the device to meet the requirement. If you reject the logging level change, Cisco DCNM does not enable the feature.

During Auto-Synchronization with Managed Devices

If you use another means, such as the command-line interface (CLI), to enable a feature on a managed device and the default logging level for the feature does not meet the minimum requirement, Cisco DCNM automatically configures the logging level to meet the requirement after Cisco DCNM detects that the feature is enabled.

If you use the CLI or any other method to lower a logging level below the minimum requirement of Cisco DCNM, after Cisco DCNM detects the logging level change, it changes the state of that device to unmanaged. When this occurs, the Devices and Credentials feature shows that logging levels are the reason that the device is unmanaged. You can use the Devices and Credentials feature to discover the device again. During rediscovery, Cisco DCNM sets logging levels that do not meet the minimum requirements.

VDC Support

When Cisco DCNM discovers a Cisco NX-OS device that supports VDCs, it determines how many VDCs are on the Cisco NX-OS device. In Cisco DCNM, each VDC is treated as a separate device. The status of each VDC is tracked separately and you can configure each VDC independently of other VDCs on a Cisco NX-OS device.

Before discovering a Cisco Nexus 7000 Series device that has nondefault VDCs, ensure that each VDC meets the prerequisites for discovery. For more information, see the "Prerequisites for Device Discovery" section on page 5-6.

Licensing Requirements for Device Discovery

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	The Device Discovery feature requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Send document comments to nexus7k-docfeedback@cisco.com

Prerequisites for Device Discovery

Prior to performing device discovery, you should be familiar with the following:

- VDCs, if you are discovering Cisco Nexus 7000 Series devices.
- CDP

The Device Discovery feature has the following prerequisites:

- The Cisco DCNM server must be able to connect to devices that it discovers.
- Cisco NX-OS devices must be running a supported release of Cisco NX-OS. For information about supported releases of Cisco NX-OS, see the *Cisco DCNM Release Notes, Release 5.x*.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.
- For a Cisco Nexus 7000 Series device, each VDC that you want to discover must have a management interface configured. Cisco DCNM supports discovery of VDCs that are configured with a management interface that is the mgmt0 interface, which is an out-of-band virtual interface, or with an in-band Ethernet interface that is allocated to the VDC.
- To allow Cisco DCNM to discover devices that are CDP neighbors, CDP must be enabled both globally on each device and specifically on the device interfaces used for device discovery. For a Cisco Nexus 7000 Series device, CDP must be enabled globally in each VDC and on the management interface that each VDC is configured to use.
- Discovery of network servers requires that LLDP is enabled globally on devices connected to network servers and specifically on the device interfaces connected to the network adapters on network servers.

Guidelines and Limitations for Device Discovery

The Device Discovery feature has the following configuration guidelines and limitations:

- Ensure that Cisco NX-OS devices that you want to discover have been prepared for discovery. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.
- Cisco DCNM can manage only devices that run Cisco NX-OS. For more information about supported device operating systems and supported device hardware, see the *Cisco DCNM Release Notes, Release 5.x*.
- CDP-based discovery of devices requires that all devices in the chain of CDP hops use the same username and password specified for the seed device. If your security practices do not allow the same username and password to be used on each device, you can perform device discovery for each device individually.
- Devices that are CDP hops but which are not running Cisco IOS software appear in the Topology feature but cannot be managed by Cisco DCNM.

Send document comments to nexus7k-docfeedback@cisco.com

Performing Device Discovery

This section includes the following topics:

- Verifying the Discovery Readiness of a Cisco NX-OS Device, page 5-7
- Discovering Devices, page 5-9
- Rediscovering Devices, page 5-10

Verifying the Discovery Readiness of a Cisco NX-OS Device

Before you perform device discovery with Cisco DCNM, you should perform the following procedure on each Cisco NX-OS device that you want to manage and monitor with Cisco DCNM. This procedure helps to ensure that device discovery succeeds and that Cisco DCNM can effectively manage and monitor the device.

Note If you are preparing a physical device that supports virtual device contexts (VDCs), remember that Cisco DCNM considers each VDC to be a device. You must verify discovery readiness for each VDC that you want to manage and monitor with Cisco DCNM.

DETAILED STEPS

Step 1 Log into the CLI of the Cisco NX-OS device.

Step 2 Use the **configure terminal** command to access global configuration mode.

Step 3 Ensure that an RSA or DSA key exists so that secure shell (SSH) connections can succeed. To do so, use the **show ssh key rsa** or **show ssh key dsa** command.

If you need to generate a key, use the **ssh key** command.

Note You must disable the SSH server before you can generate a key. To do so, use the **no feature ssh** command.

Step 4 Ensure that the SSH server is enabled. To do so, use the **show ssh server** command.

If the SSH server is not enabled, use the **feature ssh** command to enable it.

Step 5 Ensure that CDP is enabled globally and on the interface that Cisco DCNM uses to connect to the device. Use the **show run cdp all** command to see whether CDP is enabled.

Step 6 Verify that the **logging event link-status default** and **logging event link-status enable** commands are configured.

```
switch(config)# show running-config all | include "logging event link-status"
logging event link-status default
logging event link-status enable
```

If either command is missing, enter it to add it to the running configuration.

Note The **logging event link-status enable** command is included in the default Cisco NX-OS configuration. The **show running-config** command displays the default configuration only if you use the **all** keyword.

Step 7 Verify that the device is configured to log system messages that are severity 6 or lower.

Note The default name of the log file is "messages"; however, we recommend that you use the log-file name currently configured on the device. If you change the name of the log file, the device clears previous system messages.

```
switch(config)# show running-config all | include logfile
logging logfile logfile-name 6
```

If the **logging logfile** command does not appear or if the severity level is less than 6, configure the **logging logfile** command.

```
switch(config)# logging logfile logfile-name 6
```

Step 8 If the device is a Cisco Nexus 7000 Series switch that is running Cisco NX-OS Release 4.0, you must manually verify that the logging level configuration of the device meets the Cisco DCNM logging level requirements. To do so, follow these steps:

a. Determine which nondefault features are enabled on the device.

```
switch(config)# show running-config | include feature
feature feature1
feature feature2
feature feature3
.
.
.
```

b. View the logging levels currently configured on the device. The **show logging level** command displays logging levels only for features that are enabled. The Current Session Severity column lists the current logging level.

```
switch(config)# show logging level
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     3                       5
aclmgr                  3                       3
.
.
.
```

Note You can use the **show logging level** command with the facility name when you want to see the logging level of a single logging facility, such as **show logging level aaa**.

c. Determine which logging levels on the device are below the minimum Cisco DCNM-required logging levels. To do so, compare the logging levels displayed in b. to the minimum Cisco DCNM-required logging levels that are listed in Table 5-2.

d. For each logging facility with a logging level that is below the minimum Cisco DCNM-required logging level, configure the device with a logging level that meets or exceeds the Cisco DCNM requirement.

Send document comments to nexus7k-docfeedback@cisco.com

```
switch(config)# logging level facility severity-level
```

The *facility* argument is the applicable logging-facility keyword from Table 5-2, and *severity-level* is the applicable minimum Cisco DCNM-required logging level or higher (up to 7).

e. Use the **show logging level** command to verify your changes to the configuration.

Step 9 Copy the running configuration to the startup configuration to save your changes.

```
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

Discovering Devices

You can discover one or more devices. When a discovery task succeeds, Cisco DCNM retrieves the running configuration and status information of discovered Cisco NX-OS devices.

Use this procedure for the following purposes:

- To discover devices that are not currently managed by Cisco DCNM. For example, you should use this procedure when Cisco DCNM has not yet discovered any devices, such as after a new installation.
- To discover devices that you have added to your network without rediscovering devices that Cisco DCNM already has discovered.
- To rediscover the topology when CDP links have changed, without rediscovering devices that Cisco DCNM has already discovered.

Note You must successfully discover a Cisco NX-OS device before you can use Cisco DCNM to configure the device.

BEFORE YOU BEGIN

Ensure that you have configured the Cisco NX-OS device so that the Cisco DCNM server can connect to it and successfully discover it. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Determine the IPv4 address of the device that you want Cisco DCNM to connect to when it starts the discovery task. This is the seed device for the discovery.

Determine whether you want to discover devices that are CDP neighbors of the seed device. If so, determine the maximum number of hops from the seed device that the discovery process can make.

Note The discovery process can perform complete discovery of neighbors only if the neighboring devices are configured with the same credentials as the seed device.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The discovery tasks appear in the Discovery Tasks area of the Contents pane.

Step 2 In the Seed Device field, enter the IPv4 address of the device that you want Cisco DCNM to connect to when it starts the discovery task. Valid entries are in dotted decimal format.

Step 3 In the User Name field, enter the username of a user account on the device. The user account must have a network-admin or vdc-admin role.

Step 4 In the Password field, enter the password for the user account that you entered in the User Name field.

Step 5 (Optional) If you want Cisco DCNM to discover devices that are CDP neighbors of the seed device, in the Maximum Hops of Neighbors to Discover field, enter the desired maximum number of hops. By default, the maximum hops is 0 (zero).

Step 6 Ensure that **Rediscover Configuration and Status for Existing Devices** is unchecked. By default, this check box is unchecked.

By leaving this check box unchecked, you enable Cisco DCNM to use previously discovered devices as CDP hops without retrieving their running configuration and status information.

Step 7 Click **Start Discovery**.

After a short delay, the discovery task appears at the bottom of the list of tasks in the Discovery Tasks area. Cisco DCNM updates the task status periodically.

Step 8 Wait until the status for the task is Successful. This step may take several minutes.

After the status is Successful, you can use Cisco DCNM to configure and monitor the discovered devices.

You do not need to save your changes.

Rediscovering Devices

You can rediscover one or more devices.

Note Rediscovery replaces any configuration data that Cisco DCNM has for a Cisco NX-OS device with the configuration data retrieved during the rediscovery. If you need to discover one or more devices without retrieving configuration and status information for already discovered devices, see the "Discovering Devices" section on page 5-9.

You must successfully discover a Cisco NX-OS device before you can use Cisco DCNM to configure the device.

BEFORE YOU BEGIN

Ensure that you have configured the Cisco NX-OS device so that the Cisco DCNM server can connect to it. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The discovery tasks and their status appear in the Discovery Tasks area of the Contents pane.

Step 2 In the Seed Device field, enter the IPv4 address of the device that you want Cisco DCNM to connect to when it starts the discovery task. Valid entries are in dotted decimal format.

Step 3 In the User Name field, enter the username of a user account on the device. The user account must have a network-admin or vdc-admin role.

Step 4 In the Password field, enter the password for the user account that you entered in the User Name field.

Step 5 (Optional) If you want Cisco DCNM to rediscover devices that are CDP neighbors of the seed device, in the Maximum Hops of Neighbors to Discover field, enter the desired maximum number of hops. By default, the maximum hops is 0 (zero).

Step 6 Check **Rediscover Configuration and Status for Existing Devices**. By default, this check box is unchecked.

By checking this check box, you enable Cisco DCNM to replace any configuration and status information that it has about a previously discovered device with the running configuration and status information retrieved from the device.

Step 7 Click **Start Discovery**.

After a short delay, the discovery task appears at the bottom of the list of tasks in the Discovery Tasks area. Cisco DCNM updates the task status periodically.

Step 8 Wait until the status for the task is Successful. This step may take several minutes.

After the status is Successful, you can use Cisco DCNM to configure and monitor the discovered devices.

You do not need to save your changes.

Viewing the Status of Device Discovery Tasks

To view the status of device discovery tasks, from the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The tasks, including the task status, appear in the Discovery Tasks area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Device Discovery" section on page 5-12.

Where to Go Next

View the discovered devices and configure unique device credentials, as needed. For more information, see the "Administering Devices and Credentials" section on page 6-1.

Send document comments to nexus7k-docfeedback@cisco.com

Field Descriptions for Device Discovery

This section includes the following field descriptions for the Device Discovery feature:

- Device Discovery Content Pane, page 5-12
- Related Fields, page 5-13

Device Discovery Content Pane

Table 5-1 Device Discovery Content Pane

Field	Description
Discovery Setting	
Seed Device	IPv4 address of the first device that you want to discover. Valid entries are in dotted decimal format. By default, this field is blank.
User Name	Name of the device user account that the Cisco DCNM server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device. By default, this field is blank.
Password	Password for the device user account specified in the User Name field. By default, this field is blank.
Maximum Hops of Neighbors to Discover	Largest permissible number of CDP hops between the Cisco DCNM server and the device. If the server connects to the device but exceeds this number of hops, the discovery fails. The default setting is 0 (zero), which disables the discovery of neighboring devices.
Rediscover Configuration and Status for Existing Devices	Whether the discovery task you are configuring is to replace an existing device discovery that has already completed. By default, this check box is unchecked.
Discovery Tasks	
Task ID	*Display only.* Number assigned to the discovery task. The task ID indicates the order in which discovery tasks occurred.
Owner	*Display only.* Cisco DCNM server user account used to start the discovery task.
Seed Device IP Address	*Display only.* IPv4 address of the seed device.
Discovered Time	*Display only.* Date and time of the most recent update to the Status field.
Reason	*Display only.* Why the discovery task was created.
Status	*Display only.* State of the discovery task. Valid values are as follows: • In progress—The discovery tasks are ongoing. • Successful—The discovery task completed without errors. • Failed—The discovery task completed with errors.

Send document comments to nexus7k-docfeedback@cisco.com

Related Fields

For information about fields that configure devices, see the "Administering Devices and Credentials" section on page 6-1.

Device System-Message Logging Level Reference

This section provides information about the minimum device logging-level requirements of Cisco DCNM. Cisco DCNM has logging-level requirements for only a subset of the logging facilities of supported devices. If a Cisco NX-OS logging facility is not specified in this section, then Cisco DCNM does not have a requirement for that logging facility.

Note Cisco DCNM provides automatic device logging-level support. For more information, see the Automatic Logging-Level Configuration Support, page 5-4.

This section provides the following topics that document Cisco DCNM minimum logging levels per supported device type:

- Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM Feature, page 5-14
- Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM Feature, page 5-15
- Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM Feature, page 5-16
- Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM Feature, page 5-17

Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM Feature

Table 5-2 Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 7000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery Topology	CDP	Yes	cdp	2	**6**
	LLDP	No	lldp	2	**5**
DHCP snooping	DHCP snooping	No	dhcp	2	**6**
Dynamic ARP Inspection					
IP Source Guard					
Dot1X	802.1X	No	dot1x	2	**5**
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Traffic Storm Control					
Gateway Load Balancing Protocol (GLBP)	GLBP	No	glbp	3	**6**
Hot Standby Router Protocol (HSRP)	HSRP engine	No	hsrp	3	**6**
Inventory	Module	Yes	module	5	5
	Platform	Yes	platform	5	5
	System manager	Yes	sysmgr	3	3
Object Tracking	Object tracking	Yes	track	3	**6**
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
Port security	Port security	No	port-security	2	**5**
SPAN	SPAN	Yes	monitor	3	**6**
Spanning Tree	Spanning tree	Yes	spanning-tree	3	**6**
Unidirectional Link Detection (UDLD)	UDLD	No	udld	5	5
Virtual Device Contexts (VDCs)	VDC manager	Yes	vdc_mgr	6	6
Virtual Port Channel (vPC)	VPC	No	vpc	2	**6**
VLAN Network Interfaces	Interface VLAN	No	interface-vlan	2	**5**

[1] Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 7000 NX-OS logging facilities that have a default logging level that is too low.

Send document comments to nexus7k-docfeedback@cisco.com

Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM Feature

Table 5-3 Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 5000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery Topology	CDP	Yes	cdp	2	**6**
	LLDP	No	lldp	2	**5**
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Traffic Storm Control					
Fabric Extender	FEX	Yes	fex	5	5
Inventory	System manager	Yes	sysmgr	3	3
	Platform	Yes	pfm	5	5
	NOHMS	Yes	nohms	2	2
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
SPAN	SPAN	Yes	monitor	3	**6**
Spanning Tree	Spanning tree	Yes	spanning-tree	3	**6**
Unidirectional Link Detection (UDLD)	UDLD	No	udld	5	5
Virtual Port Channel	VPC	No	vpc	2	**6**
VLAN Network Interfaces	Interface VLAN	No	interface-vlan	2	**5**

[1] Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 5000 NX-OS logging facilities that have a default logging level that is too low.

Send document comments to nexus7k-docfeedback@cisco.com

Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM Feature

Table 5-4 Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 4000 NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery	CDP	Yes	cdp	2	**6**
Topology					
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Traffic Storm Control					
FIP Snooping	FIPSM	Yes	fip-snooping	2	**5**
Inventory	System manager	Yes	sysmgr	3	3
Link State Tracking	LST	No	lstsvc	2	**4**
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
SPAN	SPAN	Yes	monitor	3	**6**
Spanning Tree	Spanning tree	Yes	spanning-tree	3	**6**
Unidirectional Link Detection (UDLD)	UDLD	No	udld	5	5
VLAN Network Interfaces	Interface VLAN	No	interface-vlan	2	**5**

[1] Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 4000 NX-OS logging facilities that have a default logging level that is too low.

Send document comments to nexus7k-docfeedback@cisco.com

Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM Feature

Table 5-5 Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM Feature

Cisco DCNM Feature	Cisco Nexus 1000V NX-OS Logging Facility	Enabled by Default?	Logging Facility Keyword	Cisco NX-OS Default Logging Level	Minimum Cisco DCNM-Required Logging Level[1]
AAA	AAA	Yes	aaa	3	**5**
	RADIUS	Yes	radius	3	**5**
	TACACS+	No	tacacs+	3	**5**
Device Discovery Topology	CDP	Yes	cdp	2	**6**
Ethernet Interfaces	Ethernet port manager	Yes	ethpm	5	5
Virtual Ethernet Interfaces	Ifmgr	Yes	ifmgr	5	5
	VIM	Yes	vim	5	5
Inventory	Module	Yes	module	5	5
	Platform	Yes	platform	5	5
	System manager	Yes	sysmgr	3	3
Virtual Switches	MSP	Yes	msp	5	5
Port-Channel Interfaces	Port-channel interfaces	Yes	port-channel	5	**6**
Port Profiles	Port profile	Yes	port-profile	5	5
	VMS	Yes	vms	5	5
SPAN	SPAN	Yes	monitor	3	**6**

[1] Minimum Cisco DCNM logging levels appear in **bold** text for Cisco Nexus 1000V NX-OS logging facilities that have a default logging level that is too low.

Additional References for Device Discovery

For additional information related to device discovery, see the following sections:

- Related Documents, page 5-17
- Standards, page 5-18

Related Documents

Related Topic	Document Title
Device and Credentials	Chapter 6, “Administering Devices and Credentials”

Send document comments to nexus7k-docfeedback@cisco.com

Related Topic	Document Title
Network servers	Chapter 9, "Configuring Network Servers"
Cisco NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide, Release 5.x*

Standards

Standards	Title
NETCONF protocol over the Secure Shell (SSH)	RFC 4742

Feature History for Device Discovery

Table 5-6 lists the release history for this feature.

Table 5-6 Feature History for Device Discovery

Feature Name	Releases	Feature Information
LLDP discovery	5.0(2)	Support was added for this feature.
Fibre Channel discovery	5.0(2)	Support was added for this feature.
Automatic logging-level configuration support	5.0(2)	Support was added for this feature.

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 6

Administering Devices and Credentials

This chapter describes how to administer Cisco NX-OS devices and the credentials that are used by the Cisco Data Center Network Manager (DCNM) server to authenticate itself to the devices.

This chapter includes the following sections:

Information About Devices and Credentials

This section includes the following topics:

Devices

The Devices and Credentials feature allows you to administer the management state of devices. If the managed physical device supports virtual device contexts (VDCs), Cisco DCNM represents each VDC as a device. If you need to retrieve the running configuration and status information of a single VDC on a physical device with multiple VDCs, rather than performing device discovery for all the VDCs on the physical device, you can use the Devices and Credentials feature to rediscover the single device that represents the changed VDC.

Send document comments to nexus7k-docfeedback@cisco.com

Credentials

Devices and Credentials supports the ability to secure each managed device with different credentials. Cisco DCNM allows you to configure unique credentials for each discovered device or use default credentials when you do not configure unique credentials for a device. If some managed devices share the same credentials but others do not, you can configure unique credentials for some devices and configure the default credentials with the credentials that are shared by some of the managed devices.

Devices and Credentials associates a unique set of device credentials with each Cisco DCNM server user which means that the accounting logs on managed devices reflect the actions of each Cisco DCNM server user. If you log into the Cisco DCNM client as a user who does not have device credentials configured, the Cisco DCNM client prompts you to configure device credentials for the user account.

If support for accounting is not important to your organization, you must still configure each Cisco DCNM server user with device credentials, even if the credentials specified for each user are the same.

Device Status

The Devices and Credentials feature shows the status each device. The possible status are as follows:

- Managed—Cisco DCNM can connect to the device using SSH, configure the running configuration of the device, and retrieve logs and other data from it. This status is possible only for devices that run a supported release of Cisco NX-OS and that are configured properly to support discovery by Cisco DCNM. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.
- Unmanaged—Cisco DCNM does not manage the device or monitor the status of the device.
- Unreachable—Cisco DCNM cannot connect to the device, which was a managed device prior to becoming unreachable. Common causes for this status are as follows:
  - A network issue is preventing the Cisco DCNM server from contacting the device.
  - SSH is disabled on the device.
  - All terminal lines on the device are in use.

VDC Support

For devices that support VDCs, Cisco DCNM treats each VDC on a physical device as a separate device; therefore, Cisco DCNM can maintain unique credentials for each VDC on a device. Cisco DCNM tracks the status of each VDC separately, as well.

Licensing Requirements for Devices and Credentials

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Device and Credentials requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Send document comments to nexus7k-docfeedback@cisco.com

Prerequisites for Administering Devices and Credentials

Performing device discovery with the Devices and Credentials feature has the following prerequisites:

- The Cisco DCNM server must be able to connect to a device that you want to discover.
- Cisco NX-OS devices must be running a supported release of Cisco NX-OS. For information about supported releases of Cisco NX-OS, see the *Cisco DCNM Release Notes, Release 5.x*.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Guidelines and Limitations for Devices and Credentials

The Devices and Credentials feature has the following configuration guidelines and limitations:

- Discovering a device by using the Devices and Credentials feature does not support CDP-based discovery of neighboring devices. To use CDP-based discovery, see the "Administering Device Discovery" section on page 5-1.
- Be careful when you change the default credentials or device-specific credentials. Incorrect credentials prevent Cisco DCNM from managing devices.

Configuring Devices and Credentials

This section includes the following topics:

- Adding a Device, page 6-3
- Discovering a Device, page 6-4
- Unmanaging a Device, page 6-5
- Deleting a Device, page 6-5
- Configuring Default Device Credentials, page 6-6
- Clearing Default Device Credentials, page 6-7
- Configuring Unique Credentials for a Device, page 6-7
- Clearing Unique Credentials for a Device, page 6-8

Adding a Device

You can add a device. After you add a device, you can discover it. For more information, see the "Discovering a Device" section on page 6-4.

BEFORE YOU BEGIN

Determine the IPv4 address for the device.

Determine whether Cisco DCNM can communicate with the device using the default device credentials or whether you need to add unique device credentials when you add the device to Cisco DCNM.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 From the menu bar, choose **Actions > New Device**.

A blank row appears in the Devices area on the Contents pane.

Step 3 In the IP Address column for the new device, enter the IPv4 address that Cisco DCNM must use to connect to the device.

Step 4 Press **Enter**.

Step 5 (Optional) If you need to add unique device credentials, in the User Credentials column, double-click the entry for the device that you added, click the down-arrow button, and configure the unique device credentials.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

The status of the new device is Unmanaged.

Discovering a Device

You can discover a device.

Discovering an unmanaged device changes its status to Managed. During the discovery, Cisco DCNM retrieves the running configuration of the device.

If you are rediscovering a device, the configuration data that Cisco DCNM retrieves replaces any existing configuration data for the device. Whenever the configuration data that Cisco DCNM has for the device is not accurate, such as when a device administrator has used the command-line interface to change the running configuration, you can use this procedure to update the configuration data that Cisco DCNM has for the device.

Note Discovering a device does not affect the running configuration of the device.

BEFORE YOU BEGIN

Ensure that you have either configured the device entry with unique device credentials or that Cisco DCNM can use the default device credentials to connect to the device. For more information, see the "Configuring Default Device Credentials" section on page 6-6.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 Click the device that you want to discover.

Step 3 From the menu bar, choose **Actions > Discover**.

The device discovery begins. The status of the device changes to Discovering.

Step 4 Wait for the status to change to Managed.

Typically, the device discovery occurs in less than 5 minutes. After the status changes to Managed, you can use Cisco DCNM to configure the device.

You do not need to save your changes.

Unmanaging a Device

You can change the status of a device to unmanaged.

BEFORE YOU BEGIN

Ensure that you are changing the status of the correct device. Cisco DCNM cannot control the running configuration of an unmanaged device.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 Click the device whose status you want to change to unmanaged.

Step 3 From the menu bar, choose **Actions > Unmanage**.

After a short delay, the status of the device changes to Unmanaged.

You do not need to save your changes.

Deleting a Device

You can delete a device. When you delete a device, you delete all configuration data about the device from Cisco DCNM.

You should consider deleting devices that you do not intend to manage with Cisco DCNM. Additionally, if a network administrator of a device that supports VDCs uses the command-line interface of the device to delete a VDC, you should delete from Cisco DCNM the device that represented the VDC.

Note Deleting a device does not affect the running configuration of the device.

BEFORE YOU BEGIN

Ensure that you are deleting the correct device.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 Click the device that you want to delete.

Step 3 From the menu bar, choose **Actions > Delete**.

The device disappears from the Devices area.

You do not need to save your changes.

Configuring Default Device Credentials

You can configure the default credentials, which Cisco DCNM uses to authenticate itself when it connects to discovered Cisco NX-OS devices. Cisco DCNM uses the default device credentials to communicate with each discovered device that you have not configured with unique device credentials.

Note Device credentials are unique for each Cisco DCNM server user.

BEFORE YOU BEGIN

Determine what the default device credentials should be. All Cisco NX-OS devices that Cisco DCNM uses the default credentials to communicate with must have a network administrator account configured with a username and password that are identical to the default credentials that you configure in Cisco DCNM.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The Default Credentials area appears in the Contents pane, above the Devices area, which lists the discovered devices.

Step 2 In the User Name field, enter the username for the default credentials. A valid username can be 1 to 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Note Cisco NX-OS supports usernames that are a maximum of 28 characters.

Step 3 To the right of the Password field, click the down-arrow button.

Step 4 In the Password field and the Confirm Password field, enter the password for the default credentials. Valid passwords are numbers, symbols, and case-sensitive letters.

Send document comments to nexus7k-docfeedback@cisco.com

Note Cisco NX-OS supports passwords that are a maximum of 64 characters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Clearing Default Device Credentials

You can clear the default device credentials.

Note If you clear the default device credentials, Cisco DCNM can connect to discovered devices only if you have configured unique credentials for each managed device.

BEFORE YOU BEGIN

If you intend to use Cisco DCNM without default device credentials, you should ensure that Cisco DCNM is configured with unique device credentials for each discovered device before you perform this procedure. For more information, see the "Configuring Unique Credentials for a Device" section on page 6-7.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The Default Credentials area appears in the Contents pane, above the Devices area, which lists the discovered devices.

Step 2 In the Default Credentials area, click **Clear**.

The User Name field and the Password field clear.

Step 3 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Configuring Unique Credentials for a Device

You can configure credentials that are unique to a discovered device. When unique credentials exist for a discovered device, Cisco DCNM uses them when it connects to the device rather than using the default device credentials.

Note Device credentials are unique for each Cisco DCNM server user.

BEFORE YOU BEGIN

Determine the username and password for a network administrator user account on the discovered device.

Send document comments to nexus7k-docfeedback@cisco.com

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 In the User Credentials column for the device, double-click the entry and then click the down-arrow button.

Step 3 In the User Name field, enter the username. Valid usernames are between 1 and 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Note Cisco NX-OS supports usernames that are a maximum of 28 characters.

Step 4 In the Password field and the Confirm Password field, enter the password. Valid passwords are numbers, symbols, and case-sensitive letters.

Note Cisco NX-OS supports passwords that are a maximum of 64 characters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Clearing Unique Credentials for a Device

You can clear unique credentials for a discovered device.

Note If you clear the unique credentials for a discovered device, Cisco DCNM uses the default credentials to connect to the device.

BEFORE YOU BEGIN

If you intend to operate Cisco DCNM without unique credentials for the device, you should ensure that Cisco DCNM is configured with default device credentials before you perform this procedure. For more information, see the "Configuring Default Device Credentials" section on page 6-6.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

Discovered devices appear in the Devices area of the Contents pane.

Step 2 In the User Credentials column for the device, double-click the entry and then click the down-arrow button.

Step 3 In the User Name field, delete all text.

Step 4 In the Password field, delete all text.

Step 5 In the Confirm Password field, delete all text.

Step 6 Click **OK**.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Viewing Device Credentials and Status

To view the status for devices and whether credentials are configured for the device, from the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The default credentials appears in the Default Credentials area in the Contents pane. Information about devices, including credentials and status, appear in the Devices area in the Contents pane.

The Reason field provides a brief message that explains the device status. The following table provides information about how to resolve the issue indicated by the message.

Reason	Resolution
Success	Not applicable. Cisco DCNM is managing the device.
Authentication failure	Ensure that the credentials are correct for the device. Ensure that Cisco DCNM can reach the device.
Unsupported platform	Verify that the device is a supported platform and that it is running a supported release of Cisco NX-OS. For information about supported platforms and Cisco NX-OS releases, see the *Cisco DCNM Release Notes, Release 5.x*.
Device sync up failure	Cisco Nexus 7000 Series devices only. The sequence numbers of accounting and system message log messages are not in a proper format. Clear the log files on the device and discover the device again.
Unmanaged manually	A Cisco DCNM user changed the device status to Unmanaged. Discover the device again.
Error when executing database query	Discover the device again. If the error reoccurs, clean the Cisco DCNM database. For more information about cleaning the database, see Chapter 17, “Maintaining the Cisco DCNM Database.”
Auto synchronization for device is disabled by user	Discover the device again.
Logging levels required by DCNM are not configured on the device	Discover the device again. For more information, see the “Automatic Logging-Level Configuration Support” section on page 5-4.

Send document comments to nexus7k-docfeedback@cisco.com

Reason	Resolution
Error in SSH connection	Ensure that SSH is enabled on the device and that it is functioning properly. Discover the device again.
Unreachable	Ensure that you specify the correct IP address for the device. Ensure that Cisco DCNM can contact the device. Discover the device again.
Discovery failed because server node stopped/crashed	Discover the device again.
Syslog messages logging disabled on device	Discover the device again.

For information about the fields that appear, see the "Field Descriptions for Devices and Credentials" section on page 6-10.

Field Descriptions for Devices and Credentials

This section includes the following field descriptions for Devices and Credentials:

- Device and Credentials Content Pane, page 6-10

Device and Credentials Content Pane

Table 6-1 Device and Credentials Content Pane

Field	Description
Default Credentials	
User Name	Name of the Cisco NX-OS device user account that the Cisco DCNM server uses to access any device that it is discovering or that it is managing. On the device, the user account must be assigned to the network-admin or vdc-admin role. By default, this field is blank. **Note** The information in the User Credentials field in the Devices area overrides the information in the Default Credentials section.
Password	Password for the Cisco NX-OS device user account specified in the User Name field. By default, this field is blank.
Devices	
IP Address	*Display only.* IPv4 address of the Cisco NX-OS device.
Name	*Display only.* Name of the Cisco NX-OS device.
User Credentials	The Cisco NX-OS user account that Cisco DCNM uses to connect to the Cisco NX-OS device. **Note** If you configure this field, Cisco DCNM uses the user account that you configure when it connects to the device. If this field is blank, Cisco DCNM uses the user account specified in the Default Credentials area. By default, this field is blank.

Send document comments to nexus7k-docfeedback@cisco.com

Table 6-1 Device and Credentials Content Pane (continued)

Field	Description
Status	*Display only.* Whether the Cisco DCNM server can connect to and configure the device. Valid values are as follows: • Managed—The Cisco DCNM server can configure the device. • Unmanaged—The Cisco DCNM server cannot configure the device. • Unreachable—The Cisco DCNM server cannot reach the device.
Reason	*Display only.* Provides a brief explanation for the device status. For more information, see the "Viewing Device Credentials and Status" section on page 6-9.

Additional References for Devices and Credentials

For additional information related to the Devices and Credentials feature, see the following sections:

- Related Documents, page 6-11
- Standards, page 6-11

Related Documents

Related Topic	Document Title
Cisco NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide, Release 5.x*

Standards

Standards	Title
NETCONF protocol over the Secure Shell (SSH)	RFC 4742

Feature History for Devices and Credentials

Table 6-2 lists the release history for this feature.

Table 6-2 Feature History for Devices and Credentials

Feature Name	Releases	Feature Information
Reason field	5.0(2)	The Reason field was added to the Devices and Credentials feature.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 7

Administering DCNM Licensed Devices

This chapter describes how to use the Cisco Data Center Network Manager (DCNM) Licensed Devices feature.

This chapter includes the following sections:

Information About DCNM Licensed Devices

The DCNM Licensed Devices feature allows you to control which physical devices you can manage with licensed DCNM features. The feature maintains a list of licensed devices. If a device is on this list, you can manage licensed Cisco DCNM features on the device.

You can add as many devices to licenses as your licenses support. For example, if you install two LAN Enterprise licenses that each support 5 devices, you can add a total of 10 devices to the list of licensed devices.

You can also remove devices from the list of licensed devices and replace them with other devices.

When you try to use a Cisco DCNM licensed feature to configure a device that you have not added to the list of licensed devices, the Cisco DCNM client does not allow you to use the feature to configure the unlicensed device.

Send document comments to nexus7k-docfeedback@cisco.com

Licensing Requirements for Administering DCNM Licensed Devices

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	DCNM Licensed Devices requires an Enterprise LAN license. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Administering DCNM Licensed Devices

Administering DCNM Licensed Devices has the following prerequisites:

- You must install one or more LAN Enterprise licenses. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x.*
- You must discover the devices that you want to add to the list of Cisco DCNM-licensed devices. For more information, see the "Discovering Devices" section on page 5-9.

Guidelines and Limitations for Administering DCNM Licensed Devices

Administering DCNM Licensed Devices has the following configuration guidelines and limitations:

- You can add only managed devices to the list of licensed devices.
- You can add to the list of licensed devices only as many devices as permitted by all of the LAN Enterprise licenses that you have installed.
- When you remove a device from the list of licensed devices, the device is removed from Cisco DCNM. If the physical device supports virtual device context (VDCs), all the VDCs on the device are removed from Cisco DCNM. To continue managing the device, you must discover the device. For more information, see the "Discovering Devices" section on page 5-9.

Configuring DCNM Licensed Devices

This section includes the following topics:

- Adding Devices to the Licensed Devices List, page 7-3
- Removing Devices from the Licensed Devices List, page 7-3

Send document comments to nexus7k-docfeedback@cisco.com

Adding Devices to the Licensed Devices List

You can add managed devices to the list of Cisco DCNM-licensed devices.

BEFORE YOU BEGIN

You must have installed at least one Cisco DCNM Enterprise LAN license. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

If you have already added as many devices as the maximum number of devices allowed by your licenses, you must remove one or more devices from the list of licensed devices before you can add other devices to the list. For more information, see the "Removing Devices from the Licensed Devices List" section on page 7-3.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Licensed Devices**.

The Contents pane displays the list of licensed devices.

Step 2 From the menu bar, choose **Actions > New**.

The Cisco DCNM client adds a row to the list and the Available Devices dialog box lists available and selected physical devices.

Step 3 From the Available Devices list, choose the physical devices that you want to add to the license and then click **Add**.

Step 4 Click **OK**.

The Contents pane displays a list of licensed devices, including the devices that you added.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

You can begin using licensed Cisco DCNM features when you manage the device.

Removing Devices from the Licensed Devices List

You can remove one or more physical devices from the list of Cisco DCNM-licensed devices when you no longer need to use licensed Cisco DCNM features to manage the devices.

Note When you remove a physical device from the list of licensed devices, the device and all of its VDCs are removed from Cisco DCNM. To continue managing the device, you must discover the device. For more information, see the "Discovering Devices" section on page 5-9.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Licensed Devices**.

The Contents pane displays the list of licensed devices.

Step 2 For each device that you want to remove from the list of licensed devices, follow these steps:

a. Choose the device that you want to remove from the list of licensed devices.

Send document comments to nexus7k-docfeedback@cisco.com

b. From the menu bar, choose **Actions > Delete**.

The Cisco DCNM client displays a confirmation dialog box.

c. Click **Yes**.

The Cisco DCNM client removes the device from the list of licensed devices.

Note Devices that you remove from the list of licensed devices are no longer managed by Cisco DCNM.

Step 3 (Optional) To continue managing devices that you removed from the list of licensed devices, discover the devices. For more information, see the "Discovering Devices" section on page 5-9.

Viewing DCNM Licensed Devices

To view the list of Cisco DCNM-licensed devices, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Licensed Devices**.

The list of Cisco DCNM-licensed devices appears in the Contents pane. For information about the fields that appear, see the "Field Descriptions for DCNM Licensed Devices" section on page 7-4.

Field Descriptions for DCNM Licensed Devices

This section includes the following field descriptions for DCNM Licensed Devices:

- DCNM Licensed Devices Content Pane, page 7-4

DCNM Licensed Devices Content Pane

Table 7-1 DCNM Licensed Devices Content Pane

Field	Description
Number of Devices Licensed	*Display only.* Sum of devices licensed by all Cisco DCNM Enterprise LAN licenses installed. For example, if you installed two licenses that each support 5 devices, this field would display 10.
Switch Name	*Display only.* Name of a licensed physical device. You can use licensed Cisco DCNM features on the device.
Virtual Devices	*Display only.* Each virtual device context (VDC) that is configured on the physical device. If the physical device does not support VDCs, this field is empty.

Send document comments to nexus7k-docfeedback@cisco.com

Additional References

For additional information related to administering DCNM Licensed Devices, see the following sections:

- Related Documents, page 7-5
- Standards, page 7-5

Related Documents

Related Topic	Document Title
Installing a Cisco DCNM Enterprise LAN license	*Cisco DCNM Installation and Licensing Guide, Release 5.x*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for DCNM Licensed Devices

Table 7-2 lists the release history for this feature.

Table 7-2 Feature History for DCNM Licensed Devices

Feature Name	Releases	Feature Information
DCNM Licensed Devices	5.0(2)	No change from Release 4.2

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 8

Working with Topology

This chapter describes how to use the Topology feature in Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Topology

The Topology feature provides you with a topology map of supported Cisco NX-OS devices. The topology map also shows switches that run Cisco IOS software, such as the Catalyst 6500 series switches. For Nexus 7000 Series devices, the map shows details about virtual device contexts (VDCs).

When Cisco Data Center Network Manager (DCNM) receives new information, the Cisco DCNM client updates the map dynamically. By default, updates occur once a minute. You can see changes occur to the status of links and devices, such as links going down or VDC creation, deletion, or modification.

Because the map is always current, you can use it to troubleshoot ongoing network management issues.

You can modify and save the layout of device icons. The map also provides you quick access to configuring features for a managed device.

This section includes the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

Map Views

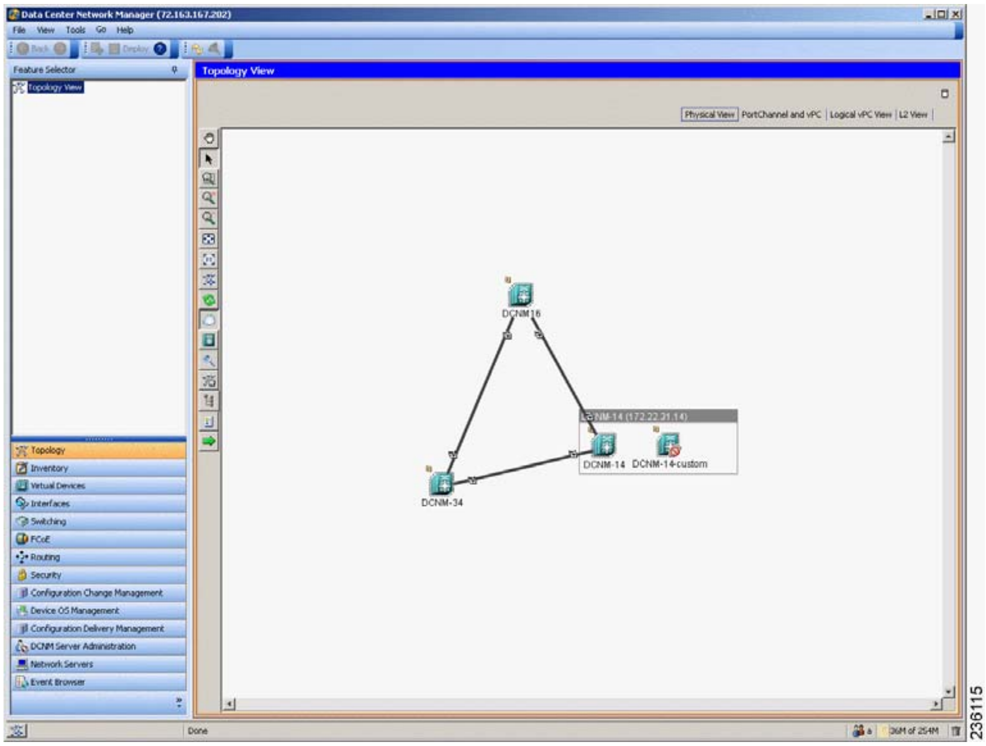
The topology map includes four views of your topology as described in the following topics:

- Physical View, page 8-2
- PortChannel and vPC, page 8-3
- Logical vPC View, page 8-4
- L2 View, page 8-5

Physical View

The Physical View (see Figure 8-1) shows the physical connections between discovered devices. This is the default topology view.

Figure 8-1 Physical View of the Topology Map

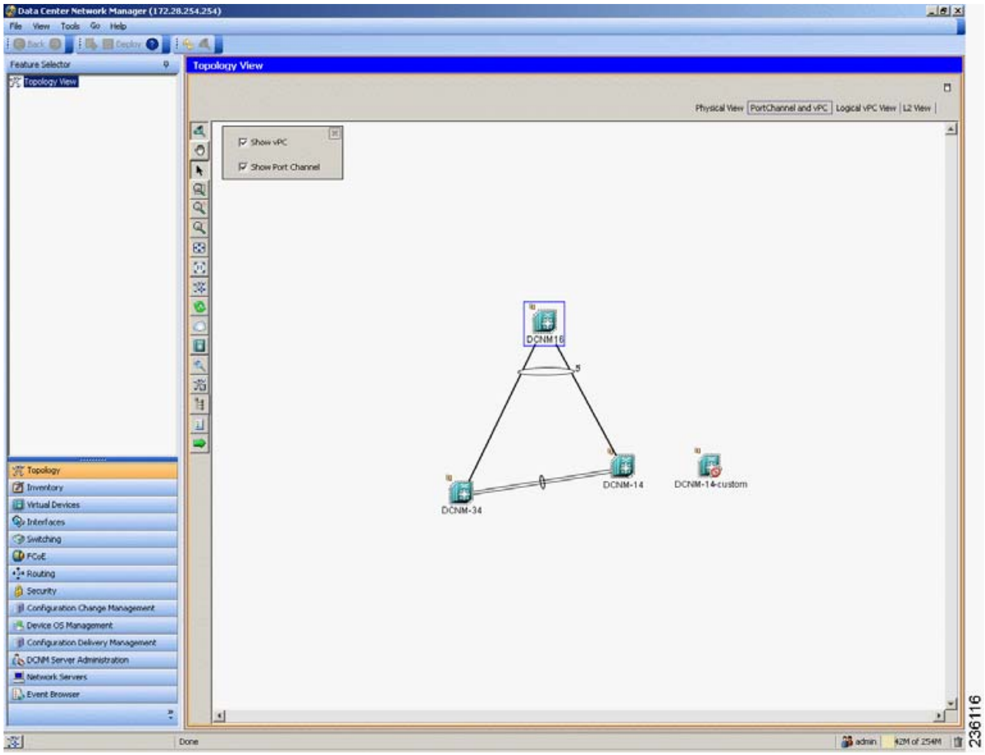


Send document comments to nexus7k-docfeedback@cisco.com

PortChannel and vPC

The PortChannel and vPC view (see Figure 8-2) shows all physical connections and all logical connections among discovered devices, including port channel links, virtual port channel (vPC) links, and vPC peer links. Physical links appear in gray in this view.

Figure 8-2 PortChannel and vPC View of the Topology Map



☑ Show vPC

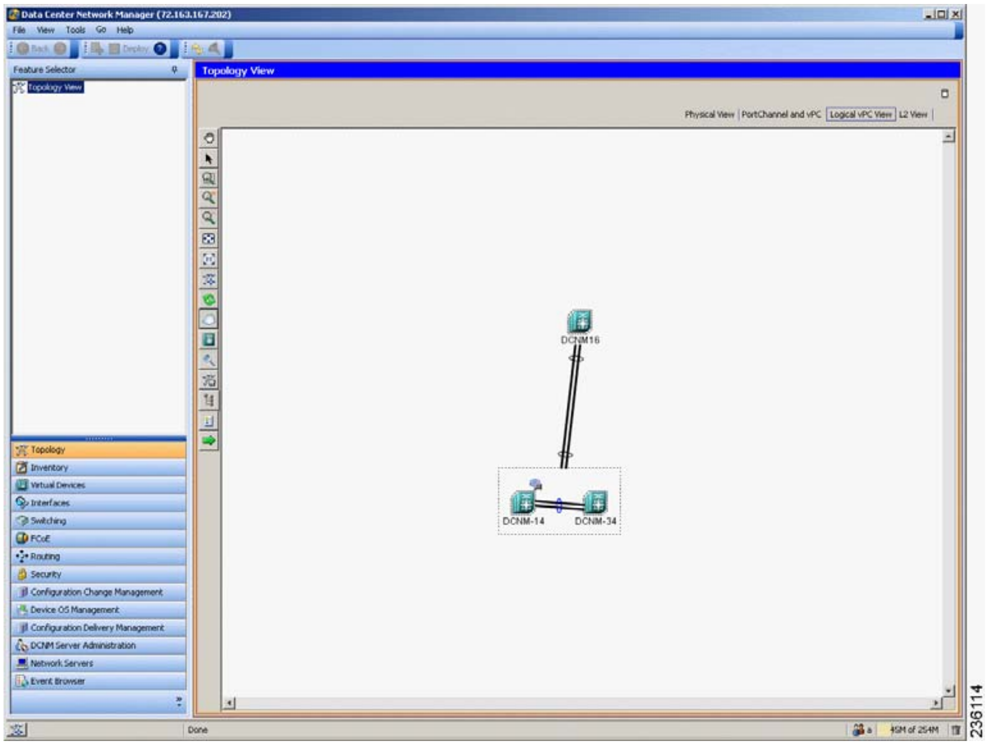
☑ Show Port Channel

Send document comments to nexus7k-docfeedback@cisco.com

Logical vPC View

The Logical vPC View (see Figure 8-3) shows vPC links and vPC peer links among discovered devices, without showing the physical connections.

Figure 8-3 Logical vPC View of the Topology Map

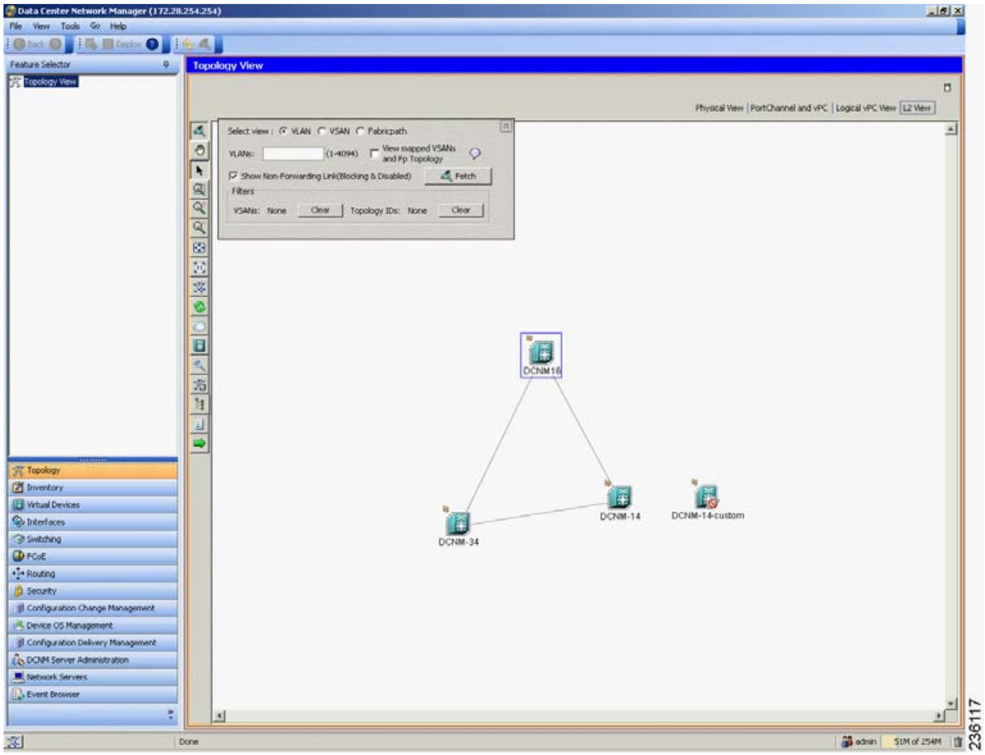


Send document comments to nexus7k-docfeedback@cisco.com

L2 View

The L2 view (see Figure 8-4) shows VLANs configured among discovered devices. Beginning with Cisco DCNM Release 5.1, the VSAN Overlay is a part of the L2 view. The VSAN Overlay feature enables you to view the Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) links that are active for a given VSAN or a range of VSANs. It also provides a visual representation of forwarding and non-forwarding links between Cisco Nexus devices in a data center network for configured VLANs.

Figure 8-4 L2 View of the Topology Map



Select view : ● VLAN ○ VSAN ○ Fabricpath
VLANs: (1-4094) □ View mapped VSANs and Fp Topology
☑ Show Non-Forwarding Link(Blocking & Disabled)
Filters
VSANs: None Topology IDs: None

Layouts

The topology map enables you to move devices to where you want them. You can save the layout so that the next time you use the topology map, devices are where you placed them. The Cisco DCNM client saves topology layouts as local user data on the computer that runs the Cisco DCNM client. When you are using the Cisco DCNM client, you do not have access to topology layouts that you saved on other computers or that you saved while logged in to the computer under a different username.

In addition to saved layouts, when you are using the Physical View, you can load one of the following layouts:

- Spring—Devices appear in locations determined by weighting the connections, which often produces a layout with minimal or no crossed connections.
- Tree—Devices appear in a tree unless connections create loops among the devices, in which case devices appear in a spanning tree, that is, a grid in which most of the connections follow the grid layout.

Send document comments to nexus7k-docfeedback@cisco.com

vPC Support

The topology map provides the following additional vPC-specific features:

- vPC creation—You can launch the vPC Creation Wizard from the PortChannel and vPC view. See the "Launching the vPC Wizard" section on page 8-28.
- Quick access to the vPC feature—You can access the configuration for a specific vPC from the PortChannel and vPC view or the Logical vPC View. See the "Managing a vPC" section on page 8-28.
- vPC configuration inconsistency—You can see vPC links and vPC peer links that have configuration inconsistencies. You can open the Resolve Configuration Consistency dialog box from the topology map. See the "Finding and Resolving vPC Configuration Inconsistencies" section on page 8-29.

Fabric Manager Support

The Cisco DCNM topology map supports Cisco Fabric Manager by providing the features described in the following topics:

- Common Topology, page 8-6
- Access to Fabric Manager Features, page 8-6

Common Topology

The topology map can show storage area network (SAN) connections and devices in addition to Ethernet LAN connections and device. You can use the Cisco DCNM topology map to view your entire data center network.

Access to Fabric Manager Features

When a SAN device, such as a Cisco MDS 9000 Family Multilayer Switch, appears in the topology map in the Cisco DCNM client, you can use the topology map to launch the Cisco Fabric Manager client and configure the SAN device.

The Cisco Fabric Manager cross launch feature is only supported by the DCNM Client when the Cisco Fabric Manager is installed in Server mode. Cross launch is not supported by the DCNM Client when the Cisco Fabric Manager is installed in Standalone mode. In addition, cross launch is not supported when the DCNM Client is in standalone mode.

For information about installing the DCNM Client in standalone mode, see Chapter 2, "Installing and Launching the Cisco DCNM Client."

For information about installing Cisco Fabric Manager and Cisco DCNM on the same server system, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x.*

FabricPath Support

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. When you select the Fabricpath view in the dialog box, you can display the following types of graphs:

Send document comments to nexus7k-docfeedback@cisco.com

- Multi-destination

  A multi-destination or broadcast graph represents broadcast traffic and unknown unicast traffic in the topology.
- Reachability

  L2MP-ISIS automatically computes the switch ID reachability for each node in the network.
- Unicast

  A unicast graph displays equal cost routes between nodes in a network.
- Multicast

  A multicast graph displays the multicast traffic from a specified device to all hosts that are listening to a particular IGMP group.

In addition, the FabricPath Topology Wizard can be launched from the L2 View. The FabricPath Topology Wizard allows you to do many operations, such as add to the FabricPath topology, display inventory, and display end devices.

Note The FabricPath Topology Wizard is not supported in Cisco NX-OS Release 5.1(1).

To launch the wizard, you need to select more than one device and right-click to display a context menu that lists the available operations. You can select multiple devices by holding down the shift key and clicking on the appropriate devices displayed on the graph. Alternatively, you may hold down the left mouse key and drag over the appropriate devices.

Device Groups

Device groups allow you to simplify the visualization of interconnections between groups of devices in the topology map. You can categorize devices into device groups that you define, which allows you to focus on a limited number of devices when you view the topology.

You can manage device groups using the topology map, which allows you to create groups, delete groups, and move devices among groups; however, the Device Groups feature is especially useful for assigning multiple devices to groups easily.

For more information about device groups, see Chapter 10, “Configuring Device Groups.”

Network Servers

The topology map can show network servers. You can use the Network Servers feature to associate host bus adapters (HBAs) and Ethernet network adapters that Cisco DCNM discovered with the Link Layer Discovery Protocol (LLDP) to network servers.

For more information, see Chapter 9, “Configuring Network Servers.”

Send document comments to nexus7k-docfeedback@cisco.com

Licensing Requirements for Topology

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	The Topology feature requires no license; however, the Logical vPC View of the topology map requires a LAN Enterprise license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Topology

Topology has the following prerequisites:

- The topology map shows only devices that Cisco DCNM has discovered.
- For full support on the topology map, discovered devices should have the applicable discovery protocols enabled, both globally and on active interfaces. For more information about the discovery protocols used by Cisco DCNM, see Chapter 5, "Administering Device Discovery."

Guidelines and Limitations

Topology has the following configuration guidelines and limitations:

- While the Topology feature is an unlicensed feature, you must have a LAN Enterprise license to manage the nondefault VDCs of Cisco Nexus 7000 Series switches that appear in the topology.
- The Topology feature displays changes to the topology periodically as determined by the polling frequency for accounting and system logs. By default, the polling frequency is one minute. For more information, see the "Information About Auto-Synchronization with Devices" section on page 12-1.

Using the Topology Feature

This section includes the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

Opening the Topology Map

You can open the topology map to view the topology of discovered devices.

Note Before discovery, if you are working with FabricPath, you must use the Command Line Interface (CLI) to accomplish the following:

- Install the Enhanced Layer 2 license on the device. See the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x* for complete information on installing this license.
- Install the FabricPath feature set on the device. See the *Cisco Configuring Feature Set for FabricPath Guide* for complete information on installing the feature set.
- Configure the FabricPath feature set so that it can be enabled in a custom VDC. See the *Cisco Configuring Feature Set for FabricPath Guide* for complete information on configuring the feature set.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. Buttons for each of the available topology views appear above the topology map.

Step 2 (Optional) If you want to change topology views, click the topology view name.

The topology map shows the view of the topology that you selected.

Step 3 (Optional) If you want to use a view-specific option, see the following table:

View Feature	Available In View	How to Use
Show/Hide all VDCs	• Physical View	Right-click in the map and choose **Show All VDCs** or **Hide All VDCs**. When you view all VDCs, Cisco Nexus 7000 Series devices appear as gray boxes that contain device icons for each VDC configured on the Cisco Nexus 7000 Series device.
Show/Hide End Devices	• Physical View • L2 View	Right-click in the map and choose **Show End Devices** or **Hide End Devices**.

View Feature	Available In View	How to Use
Filter VLANs	• L2 View	1. If the VLANs box does not appear on the map, click the Filter icon on the topology toolbar. 2. Enter a list of VLAN IDs. You can specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges. 3. Click **Filter**.
Show/Hide non-forwarding links	• L2 View	1. On the map, find the VLANs box. 2. Check or uncheck the **Show Non-Forwarding Link (Blocking & Disabled)** as needed.
Show/Hide vPCs or port channels	• PortChannel and vPC	1. On the map, find the gray box that contains the **Show vPC** check box and the **Show Port Channel** check box. You may need to scroll the map or zoom out to find the gray box. 2. Check or uncheck the check boxes as needed.

Understanding Device Icons and Links

To understand the device icons and links shown in the topology map, you can open the legend. The legend presents information about the device icons and links shown in the currently selected topology view.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. Buttons for each of the available topology views appear above the topology map.

Step 2 (Optional) If you want to change topology views, click the topology view name.

The topology map shows the view of the topology that you selected. The topology toolbar appears on the left side of the topology map.

Step 3 From the topology tool bar, click the ☰ icon.

The Legend dialog box displays information about the device icons and links that may appear in the currently selected topology view.

Send document comments to nexus7k-docfeedback@cisco.com

Using the Viewing Tools

You can use the pan, select, zoom, and search tools to view the topology map.

The following table describes the viewing tools that are available in the topology toolbar, which is on the left side of the topology map.

Viewing Tool Icon and Name	How to Use
Pan	Moves, or pans, the map. 1. Click the icon. 2. Click anywhere on the topology map, and hold down the mouse button. 3. Drag the map in any direction. 4. Release the mouse button.
Select	Allows you to select a device, link, or port icon. 1. Click the icon. 2. Click the device, link, or port icon that you want to work with. A balloon displays information about the icon that you clicked.
Zoom in Rect	Zooms to a specific portion of the map. 1. Click the icon. 2. Click on the map and drag a rectangle over the area that you want to see, and release the mouse button.
Zoom In	Zooms in. Click the icon.
Zoom Out	Zooms out. Click the icon.
Fit to View	Fits the entire topology of discovered devices within the topology map. Click the icon.
Reset Zoom	Resets the zoom to the default magnification. Click the icon.
Load Layout	Loads a layout.
Reload Layout	Loads the most recently saved layout. See the "Reloading the Previously Saved Layout" section on page 8-16.
Show Device Groups	Shows or hides device groups. See the "Showing or Hiding Device Groups" section on page 8-18.
Search	Allows you to use the device search tool, so that you can search for a device by its name. 1. To show the Search tool on the map, click the icon. 2. In the Device box, enter all or some of the name of the device that you want to search for, and then click the icon. 3. To hide the Search tool, click the icon again. **Tip** You can move the Search tool on the topology map by clicking and dragging it when you have the Select tool enabled.
Save Layout	Saves changes that you have made to the device icon layout. See the "Moving Devices in the Topology Map" section on page 8-14.

Viewing Tool Icon and Name	How to Use
Hide/Show Details	Shows and hides the details pane. See the "Showing, Hiding, and Using the Details Pane" section on page 8-13.
Legend	Opens the Legend dialog box. See the "Understanding Device Icons and Links" section on page 8-11.
➡ Export as JPG	Saves the topology map as a JPG image file. See the "Exporting the Topology as a JPG Image" section on page 8-22.

Showing, Hiding, and Using the Details Pane

You can show or hide the Details pane within the topology map. When you are showing the Details pane, you can use the sections within the Details pane to learn about the devices and connections in the topology.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Tip To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 To show or hide details, click the icon.

When you choose to show details, the Details pane appears between the topology toolbar and the topology map.

Tip Ensure that the Select tool is selected. To select the Select tool, click the icon.

Step 3 To use the sections within the Details pane, see the following table:

Section	Available In	How to Use
VDC View	• Physical View • L2 View	Explore the VDC View tree to see which Nexus 7000 Series devices contain VDCs. To see details about a device, click on it and see the Properties section.
vPC	• Port Channel and vPC • Logical vPC	Explore the vPC tree to see a categorized listing of all logical connections in the topology map. To see details about a vPC, vPC peer link, or a port channel, click on it and see the Properties section.

Send document comments to nexus7k-docfeedback@cisco.com

Section	Available In	How to Use
Overview	• All views	**Tip** To view the Overview section, you may need to click the Overview tab in the Properties section. The Overview and Properties sections share the same section title bar. The Overview section shows a thumbnail view of the whole topology. A blue rectangle indicates the portion of the topology that is currently shown in the map. • To change which portion of the topology is shown in the map, in the overview, click where you want the map to show. • To zoom in or out, click a corner of the blue rectangle and drag it until the map is enlarged or shrunk as you want.
Properties	• All views	**Tip** To view the Properties section, you may need to click the Properties tab in the Overview section. The Overview and Properties sections share the same section title bar. **1.** Do one of the following: – In the VDC View section, click on a physical or virtual device. – In the vPC section, click on a logical connection. – In the topology map, click on a device, link, or port. **2.** In the Properties section, view the properties of the object that you selected.

Moving Devices in the Topology Map

You can move device icons that are shown in the topology map. The position of devices is shared by all the topology views, that is, if you move a device and then change to another topology view, the device remains where you moved it to.

You can also save the layout, which you can reload later if you make additional changes and want to revert to your last save.

For more information, see the "Reloading the Previously Saved Layout" section on page 8-16.

The saved layout becomes the default layout that you see in the topology map when you start the Cisco DCNM client.

Send document comments to nexus7k-docfeedback@cisco.com

Note The Cisco DCNM client saves topology layouts as local user data on the computer that runs the Cisco DCNM client. When you are using the Cisco DCNM client, you do not have access to topology layouts that you saved on other computers or that you saved while logged in to the computer under a different username.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 From the topology toolbar, choose the icon.

Step 3 Find and move device icons as needed. To move an icon, click on the device icon, hold down the mouse button, drag the icon to the new location, and release the mouse button.

You can zoom and pan as needed to find icons.

For more information, see the "Using the Viewing Tools" section on page 8-12.

Step 4 (Optional) If you want to save the changes to the device icon layout, click the icon.

Loading a Layout

When you are using the Physical View, you can choose to load a layout. The position of devices is shared by all the topology views. This behavior allows you to use any of the layouts in all views by loading the layout in the Physical View and then choosing another view.

Note If you are using a different view than the Physical View, the icon on the topology toolbar acts the same as the icon. For information about using the icon, see the "Reloading the Previously Saved Layout" section on page 8-16.

BEFORE YOU BEGIN

Determine which physical devices, if any, that you want to specify as core switches. When you load a layout other than a saved layout, core switches appear at the top of the topology map, and devices that are one CDP hop from the core switches appear just below them.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 (Optional) For each physical device that you want to appear at the top of the layout, right-click on the device icon and choose **Make as Core Switch**.

Step 3 From the topology toolbar, click the icon.

The Layout drop-down list appears.

Step 4 From the **Layout** drop-down list, select the layout that you want to load.

The Physical View of the topology map changes to the layout that you selected. Any devices that you specified as core switches appear at the top of the map, with devices that are one CDP hop away from the core switches appearing just below them.

Reloading the Previously Saved Layout

You can load the most recently saved layout. This feature allows you to undo changes to device placement that you have made since you last saved the layout.

Note The Cisco DCNM client saves topology layouts as local user data on the computer that runs the Cisco DCNM client. When you are using the Cisco DCNM client, you do not have access to topology layouts that you saved on other computers or that you saved while logged in to the computer under a different username.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 From the topology toolbar, choose the ⟳ icon.

The topology map changes to the most recent layout that you saved.

Showing a Virtual or Physical Chassis

For a Cisco Nexus 1000V Series device, you can specify whether the topology map shows the virtual chassis or the physical chassis of the device. By default, the topology map shows the virtual chassis.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Step 2 Find the Cisco Nexus 1000V Series device icon.

The topology map displays either the virtual chassis or the physical chassis.

Step 3 Right-click on the device icon and choose the applicable option:

- **Show Virtual Chassis**
- **Show Physical Chassis**

Showing or Hiding Network Servers

You can show or hide the network servers that are connected to a specific device. By default, the topology map hides network servers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Step 2 Find the device that is connected to network servers that you want to show or hide.

Step 3 Right-click on the device and choose one of the following:

- To show connected network servers, choose **Show End Devices**.
- To hide connected network servers, choose **Hide End Devices**.

Managing a Network Server

You can use the topology map to access the Network Servers feature for a network server that appears on the map.

BEFORE YOU BEGIN

The network server must be showing in the topology map.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 Find the network server that you want to manage with the Network Servers feature.

Tip If the network server does not appear on the map, right-click a device that it is connected to and choose **Show End Devices**.

Step 3 Right-click on the server and choose **Manage Server**.

The Cisco DCNM client opens to the Network Servers feature. If the server that you chose represents a managed server or an Ethernet adapter on a discovered server, the client opens to the Servers contents pane. If the server that you chose represents a host bus adapter (HBA) that is not correlated or bound to a server, the client opens to the Static Server-Adapter Mapping contents pane.

Showing or Hiding Device Groups

You can show or hide device groups. When device groups are hidden, the topology map shows all discovered devices and connections. When your device groups are shown, you can expand and collapse device groups individually or all at once.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

The ☁ icon on the topology toolbar controls whether device groups appear on the topology map. When the icon appears to be pushed in, the topology map shows device groups. When the icon does not appear to be pushed in, the topology map hides device groups.

Step 2 Click the ☁ icon to change between hiding and showing device groups, as needed.

Expanding or Collapsing Device Groups

You can expand and collapse individual device groups or all device groups.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the ☁ icon.

Step 3 Do one of the following:

- If you want to expand a single device group, right-click on the device group icon and choose **Expand Device Group**.
- If you want to expand all device groups, right-click on a blank area of the map and choose **Expand all Device Groups**.
- If you want to collapse a single device group, right-click on the title of the device group and choose **Collapse Device Group**.
- If you want to collapse all device groups, right-click on a blank area of the map and choose **Collapse all Device Groups**.

Creating a Device Group

You can create a custom device group on the topology map.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 Right-click on a blank area of the map and choose **New Device Group**.

A dialog box appears, with a field for specifying a name for the new device group.

Step 3 Type a name for the device group and click **OK**.

The new device group appears on the topology map.

Moving a Device Between Device Groups

You can move devices from one device group to another device group on the topology map.

Note If a device group is empty after you move a device out of the group, Cisco DCNM deletes the device group.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the ☁ icon.

Step 3 Find the device group that you want to move the device out of.

Step 4 If the device group is collapsed, double-click the device group to expand it.

Step 5 Right-click on the device that you want to move out of the group and choose **Cut**.

Step 6 Find the device group that you want to move the device into.

Tip You do not need to expand the device group before moving the device into the group.

Step 7 Right-click the device group and choose **Paste**.

Tip If the device group is expanded, you must click on the title of the device group.

A warning dialog box confirms that you want to move the device group.

Step 8 Click **Yes**.

Cisco DCNM adds the device to the second device group and removes it from the first device group. If the first device group is empty after moving the device, Cisco DCNM deletes the first device group.

Removing a Device from a Device Group

You can remove devices from a custom device group. All devices that you remove from a custom group are added to the default device group.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the ☁ icon.

Step 3 Find the device group that you want to remove a device from.

Step 4 If the device group is collapsed, double-click the device group to expand it.

Step 5 Right-click on the device that you want to remove from the group and choose **Remove from Group**.

If you are removing the only device from the group, a warning dialog box confirms that you want to remove the device group.

Step 6 If the warning appears, click **Yes**.

Cisco DCNM removes the device from the custom device group and adds the device to the default device group.

Copy Run to Start

In the Physical View, you can copy the running-configuration to the startup configuration on one or more selected devices.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the ☁ icon.

Step 3 Above the topology map, select **Physical View**.

Step 4 Select the devices that you want to copy the running configuratiion from.

Step 5 If the device group is collapsed, double-click the device group to expand it.

Step 6 Right-click the device that you want to copy the running configuration from.

- If you want to copy the running configuration to the startup configuration, choose **Copy Run to Start**.

  Cisco DCNM copies the running configuration to the startup configuration.

- If you want to copy the running configuration to a file in the bootflash directory, choose **Copy Run to File in Bootflash**. In the dialog that appears, enter the name of the file to copy to and click **OK** to complete the operation.

  Cisco DCNM copies the running configuration to the specified file.

Deleting a Device Group

You can delete a custom device group from the topology map.

Devices that belong to a custom device group that you delete automatically become members of the default device group.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the ☁ icon.

Step 3 Find the device group that you want to delete.

Step 4 Right-click on the device group and choose **Delete Group**.

Cisco DCNM removes the device group from the topology map. The devices that were in the deleted device group are now members of the default device group.

Note If there are no custom device groups after you delete the device group, the topology map automatically hides devices groups because all devices are in the default device group.

Exporting the Topology as a JPG Image

You can export, or save, a JPG image of the topology map. You can export either the entire topology map or only the visible portion of the topology map.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 View the portion of the topology map that you want to save.

For more information, see the "Using the Viewing Tools" section on page 8-12.

Step 3 Arrange the device icons as desired.

For more information, see the "Moving Devices in the Topology Map" section on page 8-14.

Step 4 From the topology toolbar, click the ➡ icon.

A dialog box prompts you to choose whether you want to export the entire topology map or only the visible portion of the map.

Step 5 Do one of the following:

- To export the entire topology map as a JPG image, click **Yes**.
- To export only the visible portion of the topology map, click **No**.

Step 6 Specify the location and filename of the JPG image and click **Save**.

The JPG image of the visible portion of the topology map is saved.

Accessing Cisco DCNM Features from the Topology Map

You can use the topology map to access other Cisco DCNM features for managed devices. From the topology map, you can access features that are found in the following Feature Selector drawers:

- Inventory
- Virtual Devices
- Interfaces
- Routing
- Switching
- Security

You can also use the topology map to access the Device Discovery feature.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 If you want to access a Cisco DCNM feature for a specific managed device, do the following:

a. Find the device in the topology map.

Send document comments to nexus7k-docfeedback@cisco.com

b. Right-click the device and choose the feature that you want to configure.

The feature that you selected appears in the Contents pane. The device that you selected on the topology map is selected in the Summary table for the feature.

Step 3 If you want to access the Device Discovery feature, right-click a blank area on the map and choose **Discover Devices**.

The Device Discovery feature appears in the Contents pane.

Accessing Cisco Fabric Manager Features from the Topology Map

You can use the topology map to access features in the Cisco Fabric Manager client for a managed SAN device. If Cisco Fabric Manager has not discovered the device, accessing the Cisco Fabric Manager client through the topology map will cause Cisco Fabric Manager to discover the SAN device.

The Cisco Fabric Manager features that you can access include the following:

- Zones, zone sets, and zone set membership
- Port channel interfaces
- Fibre Channel physical and logical interfaces
- Fibre Channel over IP tunnels
- Events

Note The Cisco Fabric Manager cross launch feature is only supported by the DCNM Client when the Cisco Fabric Manager is installed in Server mode. Cross launch is not supported by the DCNM Client when the Cisco Fabric Manager is installed in Standalone mode. In addition, cross launch is not supported when the DCNM Client is in standalone mode.

BEFORE YOU BEGIN

The Cisco Fabric Manager client must be installed on the computer that is running the Cisco DCNM client.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 Find the SAN device in the topology map.

Step 3 Right-click the device and choose the feature that you want to configure.

Send document comments to nexus7k-docfeedback@cisco.com

The Cisco Fabric Manager client opens to the feature that you selected.

Accessing Cisco FabricPath Features from the Topology Map

You can use the topology map to access features of the Cisco FabricPath.

The Cisco FabricPath features that you can access include:

- Multi-destination, page 8-25
- Device Reachability, page 8-25
- Unicast, page 8-26
- Multicast, page 8-27

Multi-destination

A multi-destination or broadcast graph represents broadcast traffic and unknown unicast traffic in the topolgy. You can view the multi-destination information for a specific topology.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 Above the map, click **L2 View**.

The dialog box appears in the content pane.

Step 3 In the dialog box, choose the **Fabricpath** view.

Step 4 Enter the Topology ID and click **Fetch**. The graph that is displayed is filtered based upon the Topology ID.

Step 5 Check **Select type of graph** to enable the selection for the Multi-destination graph.

Step 6 Check the **Multi-destination** option.

Step 7 From the Anchor drop-down list, choose a device. The selected device is the entry point for the graph.

Step 8 From the Graph ID drop-down list, choose an ID. The Graph ID is a forwarding tag for the graph.

Step 9 Click **Fetch** to view the graph.

Device Reachability

L2MP-ISIS automatically computes the switch ID reachability for each node in the network. You can view the reachability information for a specific topology.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 Above the map, click **L2 View**.

The dialog box appears in the content pane.

Step 3 In the dialog box, select the **Fabricpath** view.

Step 4 Enter the Topology ID. The graph that is displayed is filtered based upon the Topology ID.

Step 5 Check **Select type of graph** to enable the selection for the Reachability graph.

Step 6 Check the **Reachability** option.

Step 7 From the Anchor drop-down list, select a device. The selected device is the entry point for the graph.

Step 8 Click **Fetch** to view the graph.

Note Devices in the graph that appear as red colored icons indicate that the device is not reachable for the selected topology.

Unicast

A unicast graph displays equal cost routes between nodes in a network. You can view the unicast information for a specific topology.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 Above the map, click **L2 View**.

The dialog box appears in the content pane.

Step 3 In the dialog box, select the **Fabricpath** view.

Step 4 Enter the Topology ID. The graph that is displayed is filtered based upon the Topology ID.

Step 5 Check **Select type of graph** to enable the selection for the Unicast graph.

Send document comments to nexus7k-docfeedback@cisco.com

Step 6 Check the **Unicast** option.

Step 7 From the Anchor drop-down list, select a device. The selected device is the entry point for the graph.

Step 8 From the Destination drop-down list, select a device. The selected device is the destination for the graph.

Step 9 Click **Fetch** to view the graph.

Note If the resulting graph does not trace the path from the source to the destination, then one of the following may be the cause:

- Islands in the L2MP cloud.
- Cisco DCNM might not manage intermediate devices.

Multicast

A multicast graph displays the multicast traffic from a specified device to all hosts that are listening to a particular IGMP group. You can view the multicast information for a specific topology.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Note To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.

Step 2 Above the map, click **L2 View**.

The dialog box appears in the content pane.

Step 3 In the dialog box, select the **Fabricpath** view.

Step 4 Enter the Topology ID. The graph that is displayed is filtered based upon the Topology ID.

Step 5 Check **Select type of graph** to enable the selection for the Multicast graph.

Step 6 Check the **Multicast** option.

Step 7 From the Anchor drop-down list, select a device. The selected device is the entry point for the graph.

Step 8 From the Graph ID drop-down list, select an ID. The Graph ID is a forwarding tag for the graph.

Step 9 In the Source field, enter the multicast originating device. The multicast originating device is specified as an IP address or as "*" (wildcard).

Step 10 In the IGMP field, enter the IGMP group address.

Step 11 In the VLAN field, enter multicast associated VLAN information.

Step 12 Click **Fetch** to view the graph.

Launching the vPC Wizard

From the topology map, you can launch the vPC wizard to create a vPC.

BEFORE YOU BEGIN

Determine which two devices you want to use as the vPC peer switches.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane.

Step 2 Above the map, click **PortChannel and vPC**.

The map shows the PortChannel and vPC view of the topology.

Step 3 From the topology toolbar, choose the ↖ icon.

Step 4 Click one device that you want to use as a vPC peer switch.

Step 5 Press and hold the **Shift** key.

Step 6 Click the device that you want to use as a vPC peer switch.

Step 7 Right-click either device and choose **Launch vPC Wizard**.

The vPC Creation Wizard dialog box appears.

For more information about using this wizard, see the *Cisco DCNM Interfaces Configuration Guide, Release 5.x*.

Managing a vPC

From the topology map, you can access the vPC feature for a specific vPC link.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane.

Step 2 Above the map, click one of the following views:

- **PortChannel and vPC**
- **Logical vPC View**

Step 3 Find the vPC link for the vPC that you want to manage.

Step 4 Use the step that applies to the view that you selected:

Send document comments to nexus7k-docfeedback@cisco.com

- PortChannel and vPC—Right-click the ellipse on the vPC link and choose **Manage vPC**.
- Logical vPC View—Right-click the vPC link and choose **Manage vPC**.

The vPC feature appears. The vPC that you want to manage is selected in the summary table.

For more information about the vPC feature, see the *Cisco DCNM Interfaces Configuration Guide, Release 5.x*.

Finding and Resolving vPC Configuration Inconsistencies

You can use the topology map to find vPCs that have configuration inconsistencies and open the Resolve Configuration Inconsistency dialog box.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane.

Step 2 Above the map, click one of the following views:

- **PortChannel and vPC**
- **Logical vPC View**

Step 3 Find the vPC for which you want to resolve configuration inconsistencies.

If a vPC link has configuration inconsistencies, a red ellipse appears over the link. If you use the PortChannel and vPC view, vPC peer links with configuration inconsistencies also show a red ellipse.

Step 4 (Optional) If you want to resolve configuration inconsistencies now, do one of the following:

- To resolve configuration inconsistencies for the vPC link *and* the vPC peer link, right-click the red ellipse on the vPC link and choose **Launch Configuration Consistency**.
- To resolve configuration inconsistencies for the vPC peer link only, right-click the red ellipse on the vPC link and choose **Launch Configuration Consistency**.

The Resolve Configuration Inconsistency dialog box opens.

For more information about using the Resolve Configuration Inconsistencies dialog box, see the *Cisco DCNM Interfaces Configuration Guide, Release 5.x*.

Accessing Remotely Connected CNAs from the Topology Map

You can use the topology map to access servers connected to Cisco Nexus 4000 Series switches.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

Step 2 Right-click on the switch and then choose **Show End Devices**.

The contents pane displays all the servers that are connected to the switch. It displays only the pWWN of the servers because the IP address is not available as a part of the enode information in FIP snooping.

Using VSAN Overlay

To access the VSAN Overlay feature from the topology map, follow these steps:

Step 1 From the Feature Selector pane, choose **Topology > Topology View**.

The topology map appears in the Contents pane.

Step 2 Above the map, click **L2 View**.

The dialog box appears in the content pane.

Step 3 In the dialog box, click **VSAN**.

Step 4 Enter the range to search (valid values are between 1 and 4094).

Step 5 Check **View mapped VLANs** to view the VLANs.

Step 6 Click **Fetch**.

Related Documents

For additional information related to the topology map, see the following sections:

Related Topic	Document Title
VDCs	*Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x*
vPCs	*Cisco DCNM Interfaces Configuration Guide, Release 5.x*
Configuring LLDP on managed devices	*Cisco DCNM System Management Configuration Guide, Release 5.x*
Device discovery	Chapter 5, "Administering Device Discovery"
Device groups	Chapter 10, "Configuring Device Groups"
Network servers	Chapter 9, "Configuring Network Servers"

Send document comments to nexus7k-docfeedback@cisco.com

Feature History for Topology

Table 8-1 lists the release history for this feature.

Table 8-1 Feature History for Topology

Feature Name	Releases	Feature Information
Common topology	5.0(2)	Support for SAN devices and connections was added.
Network servers	5.0(2)	Support for showing network servers was added.
Fabric Manager support	5.0(2)	Support for launching the Cisco Fabric Manager client was added.
Device groups	5.0(2)	Support for device groups was added.
VSAN Overlay	5.1(0)	Support for VSAN overlay was added as a part of the L2 view.
Discovery of servers connected to Cisco Nexus 5000 series switches via CNAs	5.1(0)	Support for discovering servers that are either directly connected to Cisco Nexus 5000 Series switches or CNAs.
FabricPath support	5.1(0)	Support for FabricPath was added.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 9

Configuring Network Servers

This chapter describes how to configure the Network Servers feature in Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Network Servers

During device discovery, Cisco DCNM can discover the host bus adapters (HBAs) and Ethernet network adapters of the network servers that are connected to Cisco NX-OS devices in your network. Cisco DCNM uses the Link Layer Discovery Protocol (LLDP) to retrieve information about the Ethernet network adapters from network servers; however, the information retrieved by LLDP is not adequate for Cisco DCNM to determine if the discovered network adapters are part of the same network server.

Beginning with Cisco DCNM Release 5.1, you can use Cisco DCNM to discover the servers that are either directly connected to Cisco Nexus 5000 Series switches or use Converged Network Adapters (CNAs). You can see the discovered CNA adapters in the Static Server-Adapter Mapping feature pane. Cisco DCNM does not allow you to automatically correlate adapters that are connected to Cisco Nexus 5000 Series switches via CNA. However, you can manually correlate the CNA adapters that belong to a network server. For more information about the discovery process, see Chapter 5, "Administering Device Discovery."

The Network Servers feature allows you to associate HBAs and Ethernet network adapters that Cisco DCNM discovered with LLDP to servers. The topology map can show the network servers that you define.

Send document comments to nexus7k-docfeedback@cisco.com

Note Cisco DCNM supports discovery and management of VMware ESX servers, Linux servers, and Windows 2008 servers only.

The Network Servers feature also allows you to view server connectivity information.

Automatic Correlation of Adapters to Servers

If you provide Cisco DCNM with a valid username and password that it can use to log into a network server, Cisco DCNM can automatically associate the network adapters of a network server, which allows Cisco DCNM to retrieve enough information from the network server to determine which of the discovered adapters are a part of the same network server. The DCNM topology view displays a graphical representation of the associations between adapters and servers.

A network server is considered managed if Cisco DCNM can successfully log into the server and retrieve the connectivity information.

To more easily manage your network servers, you can use the DCNM server correlation feature to set up the login credentials for multiple servers. You can configure multiple servers to use the same credentials or unique credentials for each server.

Manual Correlation of Adapters to Servers

If you cannot provide Cisco DCNM with credentials to log into a network server, you can manually correlate, or bind, adapters to a network server.

Licensing Requirements for Network Servers

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Network Servers requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Network Servers

The Network Servers feature has the following prerequisites:

- LLDP must be enabled on network servers.
- Cisco DCNM must have discovered the network adapters of a server before you can use the Network Servers feature to correlate adapters automatically or bind them manually to a server.

Send document comments to nexus7k-docfeedback@cisco.com

Guidelines and Limitations for Network Servers

The Network Servers feature has the following configuration guidelines and limitations:

- Cisco DCNM can discover the network servers that run a Linux operating system.
- Cisco DCNM can automatically correlate the network servers for HBA ports that are manufactured by Emulex or Qlogic only.
- Cisco DCNM can automatically correlate the adapters on the Linux operating system and ESX servers only.
- Cisco DCNM supports CNAs that are manufactured by Emulex or Qlogic only.
- Because the CNA does not advertise the IP address of the server, you must manually correlate one CNA before you can trigger the automatic correlation of subsequent entries.

Configuring Network Servers

This section includes the following topics:

Configuring Default Server Credentials

You can configure the default server credentials, which Cisco DCNM uses to authenticate itself when it connects to a newly discovered server. Cisco DCNM uses the default server credentials to communicate with each discovered server that you have not configured with unique server credentials.

Note Server credentials are unique for each Cisco DCNM user.

BEFORE YOU BEGIN

Determine what the default server credentials should be. All servers that Cisco DCNM uses the default server credentials to communicate with must have a user account configured with a username and password that are identical to the default server credentials that you configure in Cisco DCNM.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The Server Credentials area appears in the Contents pane, above the Servers area, which lists the discovered servers.

Step 2 In the User Name field, enter the username for the default server credentials. A valid username can be 1 to 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Step 3 To the right of the Password field, click the down-arrow button.

Step 4 In the Password field and the Confirm Password field, enter the password for the default credentials. Valid passwords are numbers, symbols, and case-sensitive letters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to save the default credentials.

Clearing Default Server Credentials

You can clear the default server credentials.

Note If you clear the default server credentials, Cisco DCNM can connect to discovered servers only if you have configured unique credentials for each managed server.

BEFORE YOU BEGIN

If you intend to use Cisco DCNM without default server credentials, you should ensure that Cisco DCNM is configured with unique server credentials for each discovered server before you perform this procedure.

For more information, see the "Configuring Unique Credentials for a Server" section on page 9-5.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The Server Credentials area appears in the Contents pane, above the Servers area, which lists the discovered servers.

Step 2 In the Default Credentials area, click **Clear**.

The User Name field and the Password field clear.

Step 3 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Send document comments to nexus7k-docfeedback@cisco.com

Configuring Unique Credentials for a Server

You can configure credentials that are unique to a discovered server. When unique credentials exist for a discovered server, Cisco DCNM uses them when it connects to the server rather than using the default server credentials.

Note Server credentials are unique for each Cisco DCNM user.

BEFORE YOU BEGIN

Determine the username and password for a user account on the discovered server.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The discovered servers appear in the Servers area of the Contents pane.

Step 2 In the User Credentials column for the server, double-click the entry and then click the down-arrow button.

Step 3 In the User Name field, enter the username. Valid usernames are between 1 and 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Step 4 In the Password field and the Confirm Password field, enter the password. Valid passwords are numbers, symbols, and case-sensitive letters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to save the server credentials to the Cisco DCNM server.

Clearing Unique Credentials for a Server

You can clear unique credentials for a discovered server.

Note If you clear the unique credentials for a discovered server, Cisco DCNM uses the default credentials to connect to the server.

BEFORE YOU BEGIN

If you intend to operate Cisco DCNM without unique credentials for the server, ensure that Cisco DCNM is configured with default server credentials before you perform this procedure.

For more information, see the "Configuring Default Server Credentials" section on page 9-3.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

Discovered servers appear in the Servers area of the Contents pane.

Step 2 In the Servers area, click the server that has credentials that you want to clear.

Step 3 From the menu bar, choose **Actions > Clear Credentials**.

A confirmation dialog box appears.

Step 4 Click **Yes**.

Step 5 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Correlating Servers

Correlating servers helps you manage a range of servers. An operation performed on a range of servers applies the operation to all the servers in that range

BEFORE YOU BEGIN

Ensure that the following have been confirmed and set for your appropriate platform.

- For Windows Server 2003:
  - Only Windows Server 2003 R2 (5.2.3970 or higher version) is supported.
  - WinRM system utility is installed.
    (Available from Windows Server installation CD or Microsoft Support site.)
  - Telnet service is enabled and running.
  - User level privileges are enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **iponfig /all** CLI command.
  - HBAs have been identified.
    To verify that the HBAs have been identified, you can use the **winrm e wmi/root/wmi/MSFC_FibrePortHBAAttributes** CLI command.

  Note Command output may display an error if an HBA is not installed on the server. This is expected. Ignore the error.

- For Windows Server 2008:
  - Windows Server 2008 Standard, Enterprise, and R2 (6.0.6001 or higher version) is supported.
  - WinRM system utility is installed.
  - Telnet service is enabled and running.
  - User level privileges are enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **iponfig /all** CLI command.

  - HBAs have been identified.
    To verify that the HBAs have been identified, you can use the **winrm e wmi/root/wmi/MSFC_FibrePortHBAAttributes** CLI command.

Note Command output may display an error if an HBA is not installed on the server. This is expected. Ignore the error.

- For RHEL:
  - RHEL 4.5 is supported.
  - SSH is enabled.
  - User level privileges are enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **ifconfig -a** CLI command.
  - HBAs have been identified.

    To verify that Qlogic HBAs have been identified, you can use the **grep adapter-port /proc/scsi/qla2xxx/*** CLI command.

    To verify that Emulex HBAs have been identified, you can use the **find /sys/class/scsi_host/ -name port_name** and the **find /sys/class/fc_host/ -name port_name** CLI commands.

    View the consolidated information by using 'cat' on the resulting files.
- For VMware ESX:
  - ESX 3.5 or higher version is supported.
  - SSH is enabled.
  - NICs have been identified.
    To verify that the NICs have been identified, you can use the **esxcfg-nics -l** CLI command.
  - HBAs have been identified.
    To verify that the HBAs have been identified, you can use the **esxcfg-scsidevs -a** CLI command.
  - HBAs and CNAs of Qlogic and Emulex have been tested and supported.

Note For a virtual machine, the HBA information is not displayed in the virtual machine. In the virtual machine display, the SAN details are disabled for the virtual machine. The HBA information is displayed in the ESX.

- Device version support:
  - For Nexus 7000, LLDP is supported from 5.0.
  - For Nexus 5000, LLDP is supported from4.2(1)N1(1).
  - For Nexus 5000, FC is supported for all versions.
  - For MDS, is supported from 3.3(2).

Table 9-1 Summary

	Windows Server 2003	Windows Server 2008	RHEL	ESX
Supported NIC	All	All	All	All
Supported HBA	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex
Supported CNA	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex	Qlogic, Emulex
Operating System	R2 (All editions) 32 bit and 64 bit	All editions 32 bit and 64 bit	RHEL 4.5	ESX 3.5
Required service	Telnet/ssh WinRM	Telnet/ssh WinRM	SSH/Telnet	SSH/Telnet
Authority	User level privileges	User level privileges	User level privileges	User level privileges

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Server Credentials**.

The discovered servers appear in the Servers area of the Contents pane.

Step 2 In the Servers pane, right-click to access the context menu.

Step 3 Select **New Server** in the context menu.
A new row for the server is displayed.

Step 4 In the IP Address field, enter the IP addresses of the range of servers.
IP address are delimited with commas or hyphens.
After the IP addresses are entered, the system validates the addresses. A red colored border indicates an error condition. A yellow colored border indicates a valid entry.

Step 5 Double-click the User Credentials field to access the Set User Credentials dialog box.

Step 6 In the User Name field, enter the username. Valid usernames are between 1 and 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Step 7 In the Password field and the Confirm Password field, enter the password. Valid passwords are numbers, symbols, and case-sensitive letters.

Step 8 Click **OK**.

Step 9 From the menu bar, choose **File > Deploy** to save the settings to the Cisco DCNM server.

Step 10 To start server correlation, right-click the row or a single server in the range to access the context menu.

Step 11 Select **Correlate** in the context menu.

The operation changes the status of each server to Discovering. When the operation completes, the adapters are bound to the servers. If the operation fails, the status of the server becomes Unreachable and accompanied with a message.

Send document comments to nexus7k-docfeedback@cisco.com

Correlating a Server to Adapters Automatically

Cisco DCNM can log into servers that run a Linux operating system and use the network connectivity information that it retrieves to correlate HBA network adapters that it has detected to the Linux server.

BEFORE YOU BEGIN

You must configure valid server credentials for the server that you want Cisco DCNM to correlate with HBA adapters automatically. You can configure credentials unique to the server, or if the credentials are valid with other servers, too, you can configure default server credentials.

Note If the server credentials are unavailable, you can bind the adapter to a server manually. For more information, see the "Binding Adapters to a Server Manually" section on page 9-9.

Cisco DCNM must have discovered one or more HBA network adapters and one network server.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Servers**.

Discovered servers appear in the Servers area of the Summary pane.

Step 2 Under the Server column, click the server that you want to correlate with adapters automatically.

Tip If you want to correlate more than one server at a time, press and hold **Ctrl** and then click each server that you want to correlate with adapters.

Step 3 Right-click on the selected server(s) and choose **Correlate Server(s)**.

Cisco DCNM begins discovering network connectivity information from the selected server(s).

After discovery completes, the Connected Switches column shows any additional connections correlated to the server. The local topology shown to the right of the selected server is also updated to show any connections correlated with the server.

Binding Adapters to a Server Manually

Cisco DCNM allows you to associate HBA network adapters that it has detected to a discovered server. This process does not depend upon Cisco DCNM being able to log into the server and retrieve information from it.

The connection between a managed device and the server can be displayed on the topology map after you have successfully bound the adapter to a server.

BEFORE YOU BEGIN

Cisco DCNM must have discovered one or more HBA network adapters.

Cisco DCNM must be able to reach the server to which you want to bind the adapter, either by IP address or DNS name.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Static Server-Adapter Mapping**.

The Contents pane lists discovered HBA network adapters.

Step 2 Press and hold the **Ctrl** key and then click each adapter that you want to bind to a server.

Step 3 Right-click on any selected adapter and choose **Bind to Server**.

The Enter Server Name dialog box appears

Step 4 In the Server Name field, enter the IP address or DNS name of the server, and then click **OK**.

Step 5 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

In the topology map, the connection between the adapter and the managed device is available for viewing when you choose to view the connections to end devices for the managed device.

Unbinding an Adapter from a Server

You can remove a server-adapter binding that you have created. This process does not depend upon Cisco DCNM being able to log into the server and retrieve information from it.

BEFORE YOU BEGIN

The server-adapter binding that you want to remove must exist in Cisco DCNM.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Network Servers > Static Server-Adapter Mapping**.

The Contents pane lists discovered HBA network adapters.

Step 2 Under the Server Port column, click the adapter that you want to unbind.

Step 3 Right-click the adapter and choose **Unbind from Server**.

The Server Name field for the selected adapter clears.

Step 4 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

In the topology map, the connection between the adapter and the managed device is no longer available for viewing.

Viewing Server Connectivity Information

You can view connectivity information for the Cisco DCNM server.

Step 1 From the Feature Selector pane, choose **Network Servers > Servers**.

The Summary pane lists discovered servers.

Step 2 In the Summary pane, click the server whose network connectivity information you want to view.

Send document comments to nexus7k-docfeedback@cisco.com

The local topology for the server appears to the right of the Summary pane.

Step 3 (Optional) If you want to view Ethernet network or storage area network connectivity for the server, on the Server Details tab, expand the **LAN Connectivity** or **SAN Connectivity** section, as needed.

Field Descriptions for Network Servers

This section includes the following field descriptions for the Network Servers feature:

- Field Descriptions for Servers, page 9-11
- Servers Summary Pane, page 9-11
- Field Descriptions for Server Credentials, page 9-13

Field Descriptions for Servers

This section includes the following field descriptions:

- Servers Summary Pane, page 9-11
- Server: Server Details: LAN Connectivity Section, page 9-12
- Server: Server Details: LAN Connectivity Section, page 9-12

Servers Summary Pane

Table 9-2 Servers Summary Pane

Field	Description
Server	*Display only.* DNS name or IP address of the server. If Cisco DCNM could not determine the DNS name of the server, the IP address is shown instead.
Connected Switches	*Display only.* Name and IP address of each discovered device that is connected to the server.
Status	*Display only.* Whether the Cisco DCNM server can connect to and log into the server. Valid values are as follows: • Managed—Cisco DCNM has successfully logged into the server during automatic correlation of the server adapters. • Unmanaged—Cisco DCNM has not attempted to log into the server yet. By default, a discovered server is unmanaged until you attempt to correlate its adapters automatically. • Unreachable—During automatic correlation of the server adapters, Cisco DCNM could not reach the server or authentication failed. A message indicates the reason for the status.

Send document comments to nexus7k-docfeedback@cisco.com

Server: Server Details: LAN Connectivity Section

Table 9-3 Server: Server Details: LAN Connectivity Section

Field	Description
Switch	
Name	*Display only.* Name and IP address of devices that the server is connected to with an Ethernet connection.
Port Name	*Display only.* Name of the Ethernet interface on the device, such as Ethernet1/2.
Server	
MAC Address	*Display only.* MAC address of the Ethernet adapter on the server that is connected to the device.
Port Name	*Display only.* Name of the interface on the server.

Server: Server Details: SAN Connectivity Section

Table 9-4 Server: Server Details: SAN Connectivity Section

Field	Description
Switch	
Name	*Display only.* Name and IP address of devices that the server is connected to with a Fibre Channel connection.
FC Port WWN	*Display only.* World Wide Name (WWN) of the Fibre Channel interface on the device.
Port Name	*Display only.* Name of the Fibre Channel interface on the device, such as Fc1/4.
Server	
FC Port WWN	*Display only.* World Wide Name of the HBA interface on the server.

Field Descriptions for Static Server-Adapter Mapping

Table 9-5 Static Server-Adapter Mapping Contents Pane

Field	Description
Server Port	*Display only.* Identifies the server adapter, depending upon the adapter type, as follows: • For an HBA adapter, this field displays the WWN assigned to the adapter. • For an Ethernet adapter, this field displays the MAC address of the adapter. Ethernet adapters appear on the Static Server-Adapter Mapping contents pane when the server does not advertise the IP address of the adapter in LLDP.
Server Name	DNS name or IP address of the network server that the adapter is bound to.

Table 9-5 Static Server-Adapter Mapping Contents Pane (continued)

Field	Description
Vendor	*Display only.* Name of the manufacturer of the adapter.
Switch Port	*Display only.* Name and WWN of the Fibre Channel interface on the connected device.
Switch Name	*Display only.* Name and IP address of the connected device.

Field Descriptions for Server Credentials

Table 9-6 Server Credentials Content Pane

Field	Description
Default Credentials	
User Name	Name of the server user account that the Cisco DCNM server uses to access servers that it is discovering or that it is managing. On the server, the user account must have adequate permissions to retrieve information about the server network adapters. **Note** The information in the User Credentials field in the Servers area overrides the information in the Default Credentials section.
Password	Password for the server user account specified in the User Name field. By default, this field is blank.
Servers	
IP Address	*Display only.* IPv4 address of the server.
Name	*Display only.* Name of the server. If Cisco DCNM cannot determine the name of the server, the IP address of the server is shown.
User Credentials	The server user account that Cisco DCNM uses to connect to the server. **Note** If you configure this field, Cisco DCNM uses the user account that you configure when it connects to the server. If this field is blank, Cisco DCNM uses the user account specified in the Default Credentials area. By default, this field is blank.
Status	*Display only.* Whether the Cisco DCNM server can connect to and log into the server. Valid values are as follows: • Managed—Cisco DCNM has successfully logged into the server during automatic correlation of the server adapters. • Unmanaged—Cisco DCNM has not attempted to log into the server yet. By default, a discovered server is unmanaged until you attempt to correlate its adapters automatically. • Unreachable—During automatic correlation of the server adapters, Cisco DCNM could not reach the server or authentication failed. A message indicates the reason for the status.

Send document comments to nexus7k-docfeedback@cisco.com

Additional References

For additional information related to administering Network Servers, see the following sections:

- Related Documents, page 9-14
- Standards, page 9-14

Related Documents

Related Topic	Document Title
Device discovery	*Chapter 5, "Administering Device Discovery"*
Topology map	*Chapter 8, "Working with Topology"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Network Servers

Table 9-7 lists the release history for this feature.

Table 9-7 Feature History for Network Servers

Feature Name	Releases	Feature Information
Network Servers	5.0(2)	Support was added.

CHAPTER 10

Configuring Device Groups

This chapter describes how to configure the Device Groups feature in Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Device Groups

Device groups allow you to simplify the visualization of interconnections between groups of devices in the topology feature. You can categorize devices into device groups that you define, which allows you to focus on a limited number of devices when you view the topology. Device groups can help you manage a data center with Cisco DCNM more effectively.

For example, you could groups of devices based on any of the following criteria:

- Location—You could group devices based on their physical location, such as city or as specific as the data center rack designation.
- Administrator—You could group devices based on the Cisco DCNM users who administer them.
- Data center architecture—You could group devices based on the layers of network architecture in your data center, such as aggregation, access, and storage layers.
- Device type—You could group devices based on their type, such as Cisco Nexus 7000 Series switches versus Cisco Nexus 5000 Series switches.

A device can be a member of one group only.

The default device group contains any devices that you have not assigned to a custom device group. Any newly discovered device is placed in the default group.

Send document comments to nexus7k-docfeedback@cisco.com

Licensing Requirements for Device Groups

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Device Groups requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Device Groups

The Device Groups feature has the following prerequisite:

- Devices must be discovered before you can assign them to device groups.

Guidelines and Limitations for Device Groups

The Device Groups feature has the following configuration guidelines and limitations:

- By default, all discovered devices belong to the default device group.
- A device can be a member of one group only.
- For physical devices that support virtual device contexts (VDCs), you can assign VDCs that exist on the same physical device to different device groups.
- Choose a method of categorizing devices into device groups that provides the best simplification of your network topology.

Configuring Device Groups

This section includes the following topics:

- Creating a Device Group, page 10-2
- Adding Devices to a Group, page 10-4
- Removing Devices from a Group, page 10-5
- Deleting a Device Group, page 10-5

Creating a Device Group

You can create a device group and add one or more devices to it.

There is only one default group. All other groups are custom device groups.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Groups**.

The Summary pane lists custom device groups, if any. The default group does not appear.

The Details pane shows the group name, description, and a list of devices in the group.

Step 2 From the menu bar, choose **Actions > Create Device Group**.

A blank row appears in the Summary table.

Step 3 In the blank row, under Device Group Name, enter a name for the group.

Step 4 (Optional) Under Description, enter a useful description of the group.

Step 5 In the Details pane, expand the Membership Details section, if necessary.

Step 6 To add devices to the group, do the following:

a. Right-click below the column names in the Membership Details section and choose **Add Device**.

   The Device Selection dialog box appears.

b. (Optional) Use the Select Search Criteria drop-down list to filter the devices shown in the Available Devices list. You can filter devices in one of the following ways:

   - All devices—Shows every discovered device.
   - Device type—Shows only discovered devices of the type that you choose, such as Cisco Nexus 7000 Series switches.
   - Unsupported devices—Shows discovered devices that Cisco DCNM cannot manage and monitor.
   - Connected devices—Shows discovered devices connected within the number of hops that you specify to the seed device that you specify by IP address.
   - Subnet devices—Shows discovered devices whose IP addresses are within the subnet that you specify by the IP address of the subnet and the subnet mask.

c. Move one or more devices from the Available Devices List to the Selected Devices list.

   To move one device, click the device and then click **Add**.

   To move more than one device, press and hold **Ctrl**, click each device, and then click **Add**.

d. Click **OK**.

Step 7 From the menu bar, choose **File > Deploy** to save the device group configuration.

The new group is available in the topology map.

Each device that you added to the new device group is removed from its previous group. If a preexisting, nondefault device group became empty because you moved all its devices to the new device group, Cisco DCNM automatically deletes the empty device group.

Send document comments to nexus7k-docfeedback@cisco.com

Adding Devices to a Group

You can add devices to an existing device group.

All devices belong to one and only one group. Devices that are not members of a custom device group automatically belong to the default device group.

Adding a device to a group automatically removes the device from the group that previously contained the device.

BEFORE YOU BEGIN

Ensure that the device group that you want to add the devices to exists.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Groups**.

The Summary pane lists custom device groups. The default group does not appear.

The Details pane shows the group name, description, and a list of devices in the group.

Step 2 Click the device group to which you want to add one or more devices.

Step 3 In the Details pane, expand the Membership Details section, if necessary.

Step 4 To add devices to the group, do the following:

a. Right-click below the column names in the Membership Details section and choose **Add Device**.

The Device Selection dialog box appears.

b. (Optional) Use the Select Search Criteria drop-down list to filter the devices shown in the Available Devices list. You can filter devices in one of the following ways:

- All devices—Shows every discovered device.
- Device type—Shows only discovered devices of the type that you choose, such as Cisco Nexus 7000 Series switches.
- Unsupported devices—Shows discovered devices that Cisco DCNM cannot manage and monitor.
- Connected devices—Shows discovered devices connected within the number of hops that you specify to the seed device that you specify by IP address.
- Subnet devices—Shows discovered devices whose IP addresses are within the subnet that you specify by the IP address of the subnet and the subnet mask.

c. Move one or more devices from the Available Devices List to the Selected Devices list.

To move one device, click the device and then click **Add**.

To move more than one device, press and hold **Ctrl**, click each device, and then click **Add**.

d. Click **OK**.

Step 5 From the menu bar, choose **File > Deploy** to save the device group configuration.

On the topology map, the device group will include the devices that you added to it.

Each device that you added to the device group is removed from its previous group. If a preexisting, nondefault device group became empty because you moved all its devices to the new device group, Cisco DCNM automatically deletes the empty device group.

Removing Devices from a Group

You can remove devices from a custom device group. All devices that you remove from a custom group are added to the default device group.

Tip If you want to move devices from one group to another, add them to the other group. Cisco DCNM automatically removes devices from one group when you add them to another group.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Groups**.

The Summary pane lists custom device groups. The default group does not appear.

The Details pane shows the group name, description, and a list of devices in the group.

Step 2 Click the device group from which you want to remove one or more devices.

Step 3 In the Details pane, expand the Membership Details section, if necessary.

Step 4 In the Membership Details section, select the devices that you want to delete.

To select a single device, click the device.

To select more than one device, press and hold **Ctrl**, and then click each device.

Step 5 Right-click on one of the selected devices and choose **Delete**.

Cisco DCNM removes the selected devices from the device group.

Step 6 From the menu bar, choose **File > Deploy** to save the device group configuration.

On the topology map, the default device group will include the devices that you deleted from the custom device group.

Each device that you deleted from the custom device group is added to the default device group. If the custom device group became empty because you removed all its devices, Cisco DCNM automatically deletes the empty device group.

Deleting a Device Group

You can delete a custom device group.

Devices that belong to a custom device group that you delete automatically become members of the default device group.

Send document comments to nexus7k-docfeedback@cisco.com

Tip If you add all the devices of a custom device group to another custom device group, Cisco DCNM automatically deletes the empty device group.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Groups**.

The Summary pane lists custom device groups. The default group does not appear.

The Details pane shows the group name, description, and a list of devices in the group.

Step 2 Click the device group that you want to delete.

Step 3 From the menu bar, choose **Actions > Delete Device Group**.

Cisco DCNM removes the device group from the Summary pane. The devices that were in the deleted device group are now members of the default device group.

Step 4 From the menu bar, choose **File > Deploy** to save the device group configuration.

On the topology map, the default device group will include the devices that were in the deleted device group.

Where to Go Next

For more information about using device groups in the topology feature, see Chapter 8, "Working with Topology."

Field Descriptions for Device Groups

This section includes the following field descriptions for the Device Groups feature:

- Summary Pane, page 10-6
- Device Group: Details: Global Settings Section, page 10-7
- Device Group: Details: Membership Details Section, page 10-7

Summary Pane

Table 10-1 Device Groups Summary Pane

Field	Description
Device Group Name	*Display only.* Name that you assigned to the device group. After you create a device group, the name is not editable. Device group names must start with a letter and can be up to 30 alphanumeric characters.
Description	Text describing the device group. A description can be up to 80 characters.

Send document comments to nexus7k-docfeedback@cisco.com

Device Group: Details: Global Settings Section

Table 10-2 Device Group: Details: Global Settings Section

Field	Description
Device Group Name	*Display only.* Name that you assigned to the device group.
Description	Text describing the device group. A description can be up to 80 characters.

Device Group: Details: Membership Details Section

Table 10-3 Device Group: Details: Membership Details Section

Field	Description
Switch Name	*Display only.* Name of a device assigned to the device group.
Platform	*Display only.* Name of the physical or virtual device type, such as "Cisco Nexus 1000V Series" or "Cisco Nexus 7000 Series."

Additional References

For additional information related to administering Device Groups, see the following sections:

- Related Documents, page 10-7
- Standards, page 10-7

Related Documents

Related Topic	Document Title
Topology	*Chapter 8, "Working with Topology"*
Device discovery	*Chapter 5, "Administering Device Discovery"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Send document comments to nexus7k-docfeedback@cisco.com

Feature History for Device Groups

Table 10-4 lists the release history for this feature.

Table 10-4 Feature History for Device Groups

Feature Name	Releases	Feature Information
Device Groups	5.0(2)	Support was added.

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 11

Working with Cluster Administration

This chapter describes how to use the Cluster Administration feature in Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Cluster Administration

This section includes the following topics:

Cluster Administration

Cluster Administration allows you to view information about the Cisco DCNM servers configured to operate in a server cluster. If the Cisco DCNM server is not configured to operate in a cluster, the Cluster Administration feature allows you to view information about the single server.

For each server that appears in the Cluster Administration summary pane, you can view information such as the Cisco DCNM release number, Java version, operating system, system threads, memory utilization, IP address, and disk drive usage.

Send document comments to nexus7k-docfeedback@cisco.com

Clustered-Server Environment

You can deploy Cisco DCNM in a server cluster, with up to five Cisco DCNM servers in a closer. Cisco DCNM servers in a cluster communicate using multicast IP messages. The primary benefit of a clustered-server deployment is enhanced capacity for the device-management tasks that Cisco DCNM performs. A clustered-server deployment also helps to ensure availability of the Cisco DCNM server. Cisco DCNM distributes tasks among all servers in the cluster. Servers in the cluster are always active and never in a stand-by mode.

For information about the server-system and network requirements for a clustered-server deployment, and for the detailed steps for installing a server cluster, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Master Server Role

One server in a Cisco DCNM server cluster is the master server. The master server is responsible for assigning tasks to all of the servers in the server cluster, including to itself. Tasks are stored in the Cisco DCNM database. If the master server fails, the server that assumes the master server role can access the tasks in the database.

When users log into the Cisco DCNM client, they should specify the IP address or DNS name of the master server. When users submit requests to the master server, the master server distributes the tasks as needed.

Cisco DCNM determines which server is the master server by the oldest server start time. The Cisco DCNM server that started first is always the master server in a server cluster. If the master server fails, the Cisco DCNM server with the next oldest start time assumes the role of the master server. You can control which server is the master server by controlling the order in which you start the servers in a cluster.

Distributed Server Tasks

The master server distributes tasks by assigning managed devices to servers in the server cluster. For example, in a cluster of four servers, if Cisco DCNM is managing 20 devices, the master server assigns five managed devices to each server, including itself.

After the master server assigns a device to a server, that server performs the following tasks for that device:

- Auto-synchronization with devices—The server regularly retrieves the system message log file from the device. For more information about auto-synchronization, see Chapter 12, "Administering Auto-Synchronization with Devices."
- Statistical data collection—The server runs any statistical data collectors for the device, with the exception of Virtual Port Channel (vPC) statistics. The master server always runs statistical data collectors for vPC statistics. For more information about statistical data collection, see Chapter 14, "Administering Statistical Data Collection."
- Device discovery—The server performs device configuration discovery for the device; however, the remainder of the device discovery phases are performed by the master server. For more information about the phases of device discovery, see the "Discovery Process" section on page 5-3.

For example, if a user initiates device discovery for a switch named DC-NEXUS-7010-3, the master server completes the initial phases of device discovery. It then assigns the device configuration discovery phase for DC-NEXUS-7010-3 to one of the servers in the cluster, ensuring that discovery tasks are evenly distributed. After discovery completes, the master server assigns DC-NEXUS-7010-3 to the server that is managing the least number of devices. The master server instructs the assigned server to perform auto-synchronization for DC-NEXUS-7010-3. Whenever a Cisco DCNM client user starts a statistical chart for any managed feature on DC-NEXUS-7010-3, the master server instructs the assigned server to run the statistical data collector for the chart.

Effect of Cluster Changes on Server Task Distribution

When servers join or leave the cluster, the master server always ensures that the assignment of managed devices to servers is redistributed evenly among the servers in the cluster. Table 11-1 describes the behavior of a Cisco DCNM server cluster for more specific events.

Table 11-1 Cluster Change Events and Behavior

Cluster Change Event	Cluster Behavior
Master server stops or fails	The server with the oldest start time becomes the master server and redistributes the assignment of managed devices evenly among the servers remaining in the cluster. Because the cluster size decreased, the number of devices assigned to each server increases.
Server stops or fails	The master server redistributes the assignment of managed devices evenly among the servers remaining in the cluster. Because the cluster size decreased, the number of devices assigned to each server increases.
Server fails while performing a user-initiated device-configuration deployment	If the user-initiated device-configuration deployment did not complete before the member server failed, the deployment fails and the server task to deploy the device configuration is lost. To recover from the loss of the deployment, the user must repeat the configuration steps and deploy the configuration again. In some cases, the failure may result in the device becoming unmanaged, and the user must rediscover the device before repeating the configuration steps. The master server redistributes the assignment of managed devices evenly among the servers remaining in the cluster. Because the cluster size decreased, the number of devices assigned to each server increases.
Server starts	The master server redistributes the assignment of managed devices evenly among the servers remaining in the cluster. Because the cluster size increased, the number of devices assigned to each server decreases.

Send document comments to nexus7k-docfeedback@cisco.com

Licensing Requirements for Cluster Administration

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Cluster Administration requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Cluster Administration

The Cluster Administration feature has the following prerequisite:

- Servers in a cluster must meet the clustered-server requirements. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Guidelines and Limitations for Cluster Administration

The Cluster Administration feature has the following limitation:

- The Cluster Administration feature shows information about running servers only. When a server in a cluster stops or fails, it appears to have left the cluster, and its information is not shown by the Cluster Administration feature.

Viewing Server Information

You can view information about the Cisco DCNM servers that are configured to operate as a server cluster. If you have a single server, which is not configured to operate as a member of a server cluster, you can use the Cluster Administration feature to view information about it.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Cluster Administration**.

The Summary pane displays the cluster by the partition name assigned to the cluster during installation. A single server environment still has a partition name assigned to it during installation.

Step 2 Expand the cluster.

The Summary pane lists each Cisco DCNM server in the cluster with information about the server.

Tip To update the server information, from the toolbar, choose **View > Refresh**.

Step 3 (Optional) If you want to view disk usage information, on the Details tab, expand the **Logical Disk(s)** section.

Send document comments to nexus7k-docfeedback@cisco.com

Field Descriptions for Cluster Administration

This section includes the following field descriptions for the Cluster Administration feature:

- Summary Pane, page 11-5
- Server: Details Tab, page 11-5

Summary Pane

Table 11-2 Cluster Administration Summary Pane

Field	Description
[Cluster partition name]	*Display only.* Name assigned to the Cisco DCNM server partition during installation of the server software. **Note** The remaining fields on the summary pane pertain to specific servers in a cluster.
IP Address	*Display only.* IPv4 address of the Cisco DCNM server. If the server is currently the master server in the server cluster, the IP Address field also indicates that the server is the master server.
DCNM Version	*Display only.* Cisco DCNM release number that the server is running.
Java Version	*Display only.* Java version that the Cisco DCNM server is using.
Total Threads	*Display only.* Number of processing threads used by the Cisco DCNM software on the server system.
Memory Utilization (Percentage)	*Display only.* Percentage of system memory used by the Cisco DCNM software on the server system.
Last Local Refresh Time	*Display only.* Local date and time on the Cisco DCNM server when the client last received updated information.

Server: Details Tab

Table 11-3 Server: Details Tab

Field	Description
General	
The fields in this section show the same information as the fields of the same name on the Summary pane.	
Logical Disk(s)	
Name	*Display only.* Name of the drive.
Size (MB)	*Display only.* Total capacity of the drive, in megabytes.
Free Space (MB)	*Display only.* Number of megabytes available for use on the drive.

Send document comments to nexus7k-docfeedback@cisco.com

Additional References

For additional information related to administering Cluster Administration, see the following sections:

- Related Documents, page 11-6
- Standards, page 11-6

Related Documents

Related Topic	Document Title
Events	*Cisco DCNM System Management Configuration Guide, Release 5.x*
Device discovery	*Chapter 5, "Administering Device Discovery"*
Auto-synchronization with devices	*Chapter 12, "Administering Auto-Synchronization with Devices"*
Statistical data collection	*Chapter 14, "Administering Statistical Data Collection"*
Stopping servers	*Chapter 16, "Starting and Stopping Cisco DCNM Servers"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Cluster Administration

Table 11-4 lists the release history for this feature.

Table 11-4 Feature History for Cluster Administration

Feature Name	Releases	Feature Information
Cluster Administration	5.0(2)	Support was added.

CHAPTER 12

Administering Auto-Synchronization with Devices

This chapter describes how to administer the Auto-Synchronization with Devices feature in Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Auto-Synchronization with Devices

The Auto Synchronizing with Devices feature ensures that the Cisco Data Center Network Manager (DCNM) server has current configuration and status information about managed devices. The Cisco DCNM server creates one poller process for each device to retrieve the system and accounting logs that this feature requires.

When you choose Auto Synchronization with Devices on the Feature Selector pane, the content pane shows information about each poller process and allows you to control them.

You can configure the length of time that Cisco DCNM waits before polling a device again. By default, Cisco DCNM polls each managed device every 60 seconds. You can increase the length of time to a maximum of 300 seconds. For more information, see the "Configuring the Polling Interval" section on page 12-4.

Cisco DCNM polls devices concurrently; however, to avoid polling all devices simultaneously, Cisco DCNM begins polling devices in alphabetical device-name order and delays each polling process by a short, random amount of time.

Send document comments to nexus7k-docfeedback@cisco.com

This section includes the following topics:

- Automatic and Manual Purging of Event Data, page 12-2
- Virtualization Support, page 12-2

Automatic and Manual Purging of Event Data

You can use the Auto-Synchronization with Devices feature to delete unwanted event data. Cisco DCNM supports automatic purging of event data. You can configure the following aspects of automatic event data purging:

- Days of the week and time of day that automatic purging occurs.
- Whether Cisco DCNM determines which event data to purge by the age of the data or by a maximum number of database entries.
- Severity level of events.

You can also manually purge event data.

Virtualization Support

Cisco DCNM treats each virtual device context (VDC) on a Cisco NX-OS device as a separate device. Cisco DCNM creates one poller process per device.

Licensing Requirements for Auto-Synchronization with Devices

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Auto-Synchronization with Devices requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Auto-Synchronization with Devices

The Auto-Synchronization with Devices feature has the following prerequisites:

- The Cisco DCNM server must be able to connect to the devices.
- The Cisco NX-OS device must be running a supported version of Cisco NX-OS.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Send document comments to nexus7k-docfeedback@cisco.com

Guidelines and Limitations for Auto-Synchronization with Devices

The Auto-Synchronization with Devices feature has the following configuration guidelines and limitations:

- We recommend that you use the default device polling interval unless you encounter issues with synchronization due to slow response from devices or to managing many devices. For more information, see the "Configuring the Polling Interval" section on page 12-4.
- For the Auto-Synchronization with Devices feature, the Cisco DCNM client does not automatically update the information shown in the Summary pane. To ensure that you are viewing current information, from the menu bar, choose **View > Refresh**.
- We recommend that you configure automatic purging of event data to ensure that the Cisco DCNM database size does not grow too large.

Configuring Device Auto-Synchronization

This section includes the following topics:

- Starting and Stopping a Poller, page 12-3
- Configuring the Polling Interval, page 12-4
- Synchronizing with a Device, page 12-4
- Deleting Data from the Events Database, page 12-5
- Enabling and Disabling Automatic Event Purging, page 12-6
- Configuring Automatic Event Purge Settings, page 12-6
- Purging Events Now, page 12-8

Starting and Stopping a Poller

You can start and stop a poller for a device. When a poller is stopped, auto-synchronization for the device does not occur.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

A table of pollers appears in the Contents pane. Each row corresponds to a poller for a particular device. Devices are listed alphabetically. The Poller Status field displays messages about whether the poller is running or is stopped.

Step 2 Click the poller that you want to start or stop.

Send document comments to nexus7k-docfeedback@cisco.com

Step 3 Do one of the following:

- To start a poller, from the menu bar, choose **Actions > Start Poller**. The Poller Status field changes to Running.
- To stop a poller, from the menu bar, choose **Actions > Stop Poller**. The Poller Status field changes to Stopped.

You do not need to save your changes.

Configuring the Polling Interval

You can configure how often the Cisco DCNM server synchronizes with managed devices. While synchronizing, the Cisco DCNM server fetches accounting and system logs from managed devices. This setting affects how frequently features in the Cisco DCNM client receive updated information about managed devices. The default polling interval is 60 seconds.

BEFORE YOU BEGIN

Determine how often you want Cisco DCNM to perform auto-synchronization with managed devices. Consider the following:

- How often device configurations are changed by means other than Cisco DCNM, such as using the command-line interface of a device. If changes by means other than Cisco DCNM are common, consider using a short polling interval.
- How important it is to your organization that Cisco DCNM be up to date with managed device configurations. If up-to-date configuration information is important to your organization, consider using a short polling interval.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The device polling interval appears in the Contents pane, above the table of pollers.

Step 2 In the Device Polling Interval field, enter the number of seconds between auto-synchronizations for all devices. The default interval is 60 seconds. You can specify an interval between 30 and 300 seconds.

Step 3 From the menu bar, choose **File > Deploy** to save the polling interval.

Synchronizing with a Device

You can make Cisco DCNM synchronize with a device manually when you do not want to wait for the next auto-synchronization to occur.

Note If many configuration changes have occurred on the device since the last successful synchronization, consider performing device discovery instead of synchronization. For more information, see "Discovering a Device" section on page 6-4.

Send document comments to nexus7k-docfeedback@cisco.com

BEFORE YOU BEGIN

Ensure that you have either configured the device entry with unique device credentials or that Cisco DCNM can use the default device credentials to connect to the device. For more information, see the "Configuring Default Device Credentials" section on page 6-6.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

A table of pollers appears in the Contents pane. Each row corresponds to a poller for a particular device. Devices are listed alphabetically.

Step 2 Click the device that you want Cisco DCNM to synchronize with.

Step 3 From the menu bar, choose **Actions > Synchronize with Device**.

Synchronization begins.

To determine when the synchronization has finished, watch the Last Sync Status column. Typically, synchronization with a device occurs in less than 5 minutes.

You do not need to save your changes.

Deleting Data from the Events Database

You can delete data from the events database based on the exact age of the events. Events that you delete can no longer appear in the Event Browser or on a feature-specific Events tab.

Tip If you want to delete events based on the number of events in the database, see the "Purging Events Now" section on page 12-8.

BEFORE YOU BEGIN

Determine the date and time of the newest events data that you want to delete. When you follow the steps in this procedure, Cisco DCNM deletes all events that are older than the date and time that you select.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The Events Database Administration tab appears in the Details pane, below the table of pollers.

Step 2 From the Delete events older than drop-down list, choose the date and time of the newest event that you want to delete and click **OK**.

Step 3 Click **Delete**.

Cisco DCNM deletes all events older than the date and time that you specified.

Enabling and Disabling Automatic Event Purging

You can enable or disable the automatic purging of events from the Cisco DCNM events database.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The Events Database Administration tab appears in the Details pane, below the table of pollers.

Step 2 Under Purge Settings, do one of the following:

- To enable automatic event purging, check **Enable Auto Purge**.
- To disable automatic event purging, uncheck **Enable Auto Purge**.

Step 3 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Configuring Automatic Event Purge Settings

You can configure when automatic event purging occurs and the criteria that Cisco DCNM uses to determine which events to purge.

BEFORE YOU BEGIN

Determine when you want automatic event purging to occur. We recommend that automatic event purging occur when Cisco DCNM usage is low.

If you perform backups of your Cisco DCNM databases, consider scheduling automatic event purging after database backups have occurred, to ensure that you retain a record of all events.

Send document comments to nexus7k-docfeedback@cisco.com

Determine what criteria you want Cisco DCNM to use to determine which events to purge. The criteria available are as follows:

- Age of event—Cisco DCNM can purge all events that are older than a specific number of days, weeks, or months.
- Number of events in the database—When the number of events in the database exceeds the maximum number that you specify, Cisco DCNM can purge the oldest events first until the maximum number is not exceeded.
- Severity of event—Cisco DCNM can purge events based on the severity level of the event.

If you enable both criteria, Cisco DCNM applies them independently of each other.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The Events Database Administration tab appears in the Details pane, below the table of pollers.

Step 2 Under Purge Threshold, configure the criteria that Cisco DCNM uses to determine which events to purge. You can configure any of the criteria in the following table:

Purge Criteria	How to Configure
Age of events	1. Check **Data older than**. 2. From the first drop-down list, choose the number of days, weeks, or months. 3. From the second drop-down list, choose **Days**, **Weeks**, or **Months**, as needed.
Number of events in the database	1. Check **Total Entries Exceed(0-2147483647)**. 2. In the box, enter the maximum number of entries that you want to allow in the events database.
Severity of event	1. Check **Severity**. The list of eight severity levels becomes available. 2. For each severity level that you want Cisco DCNM to use to determine whether to purge events, check the severity level.

Step 3 Under Purge Settings, follow these steps to configure when you want automatic purging to occur:

a. Check the days-of-the-week check boxes to specify which days of the week that you want automatic purging to occur.

b. Use the **Run at** box to configure the exact time on the specified days that you want automatic event purging to occur.

Step 4 (Optional) If you want to enable automatic event purging, check **Enable Auto Purge**.

Step 5 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Send document comments to nexus7k-docfeedback@cisco.com

Purging Events Now

You can purge event data on demand, using the automatic event purge settings to determine which events are purged. Events that you delete can no longer appear in the Event Browser or on a feature-specific Events tab.

Tip If you want to delete events on demand, based on the exact age of the events, see the "Deleting Data from the Events Database" section on page 12-5.

BEFORE YOU BEGIN

Ensure that the automatic event purge settings are configured as needed. For more information, see the "Configuring Automatic Event Purge Settings" section on page 12-6.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The Events Database Administration tab appears in the Details pane, below the table of pollers.

Step 2 Under Purge Settings, click **Purge Now**.

Cisco DCNM deletes events, using the automatic event purge settings to determine which events to purge.

Viewing the Status of Auto-Synchronization Pollers

To view the status of an auto-synchronization poller, from the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

Poller status and information about the synchronization time and status appear in the Pollers area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Auto Synchronization with Devices" section on page 12-8.

Field Descriptions for Auto Synchronization with Devices

This section includes the following field descriptions for the Auto Synchronization with Devices feature:

- Summary Pane, page 12-9
- Events Database Administration Tab, page 12-9

Send document comments to nexus7k-docfeedback@cisco.com

Summary Pane

Table 12-1 Auto Synchronization with Devices Summary Pane

Field	Description
Pollers	
Device Polling Interval	Number of seconds that all pollers wait before the next attempt to synchronize with a device. The default value is 60 seconds. Valid values are from 30 to 300 seconds.
Last Refresh Time	*Display only.* Date and time that the Cisco DCNM client updated information shown on the Contents pane.
Device	*Display only.* Name and IP address of the device for the corresponding poller.
Poller Status	*Display only.* Whether the poller is running or stopped. A running poller attempts to synchronize with the configuration and status information from its device at the frequency specified by the Device Polling Interval field.
Last Sync Time	*Display only.* Date and time that the poller last retrieved system and accounting log data from the device.
Last Sync Status	*Display only.* Whether the most recent synchronization attempt succeeded or failed. If synchronization failed, determine why Cisco DCNM failed to connect to the device. If necessary, rediscover the device.

Events Database Administration Tab

Table 12-2 Events Database Administration Tab

Field	Description
Delete events older than	Date and time of the newest event to be deleted from the events database. There is no default value for this field.
Purge Threshold	
Data older than	Whether, during automatic event purging, Cisco DCNM deletes events that are older than the age specified in the drop-down lists located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default age is 1 day.
Total Entries Exceed	Whether, during automatic event purging, Cisco DCNM deletes the oldest events until the number of events equals the number in the box located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default number of event is 25,000.
Severity	Whether, during automatic event purging, Cisco DCNM deletes events with severity levels that are selected from the list of severity levels. By default, this check box is disabled.

Send document comments to nexus7k-docfeedback@cisco.com

Table 12-2 Events Database Administration Tab (continued)

Field	Description
Severity Levels	Severity levels of events that Cisco DCNM deletes during automatic event purging. The severity levels are available only if the Severity check box is checked. By default, all severity levels are disabled. The severity levels are as follows: • Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debugging
Purge Settings	
Enable Auto Purge	Whether automatic purging of event data is enabled. By default, this check box is disabled.
Run on	Days of the week that the automatic purging of events data occurs. By default, none of the check boxes are checked. If you check the Daily check box, the check boxes for the individual days of the week become unavailable.
Run at	Time of day that automatic purging of event data occurs, on the days of the week that automatic purging is enabled.

Additional References

For additional information related to administering Auto-Synchronization with Devices, see the following sections:

- Related Documents, page 12-10
- Standards, page 12-11

Related Documents

Related Topic	Document Title
Events	*Cisco DCNM System Management Configuration Guide, Release 5.x*
Device discovery	*Administering Device Discovery, page 5-1*

Send document comments to nexus7k-docfeedback@cisco.com

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Auto-Synchronization with Devices

Table 12-3 lists the release history for this feature.

Table 12-3 Feature History for Auto-Synchronization with Devices

Feature Name	Releases	Feature Information
Auto-Synchronization with Devices	5.0(2)	No change from Release 4.2.

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 13

Working With Threshold Rules

This chapter describes how to configure threshold rules using Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

- Information About Threshold Rules, page 13-1
- Configuring Threshold Rules, page 13-4

Information About Threshold Rules

This section includes the following topics:

- Threshold Rules Overview, page 13-1
- Threshold Rule Examples, page 13-2

Threshold Rules Overview

Cisco DCNM provides a feature that you use to specify rising or falling threshold rules for sample variables in collected statistical data. Depending on the rule definition, a set of actions are performed by Cisco DCNM. You define the threshold rule on the Threshold Rules page, and you apply the threshold rule to the existing chart.

This section includes the following topics:

- Rising Threshold, page 13-1
- Falling Threshold, page 13-2
- Threshold Rule Properties, page 13-2
- Threshold Rule Actions, page 13-2

Rising Threshold

The rising threshold is the upper threshold for a sample variable. When the current sampled variable is greater than or equal to the specified threshold, a set of actions is performed.

FINAL DRAFT

Falling Threshold

The falling threshold is the lower threshold for a sample variable. When the current sampled variable is lower than or equal to the specified threshold a set of actions is performed.

Note You can specify only one rising threshold and one falling threshold for a single sampled variable.

Threshold Rule Properties

Threshold rule properties are as follows:

- Name—Specifies the threshold rule name.
- Frequency—Specifies the number of times the sampled variable must cross a threshold before triggering any actions.
- Period—Specifies the interval of time the frequency is monitored.
- Repeat—Prevents the timer from resetting after triggering an action within the period.
- Trend—Specifies the rising or falling threshold.

Threshold Rule Actions

Threshold rule actions are as follows:

- Send an email or SMS to a mail server or mail to SMS gateway.
- Run a script on the server.
- Send an event to the current DCNM JMS channel.

Threshold Rule Examples

Note The granularity of a period is driven by the minimal interval of the collected data. Consequently, the period must be higher than that interval.

This section includes the following topics:

- Trigger an Action Each Time a Threshold is Crossed, page 13-2
- Trigger an Action Only Once in a Period When a Threshold is Crossed, page 13-3
- Trigger an Action Every Fourth Period When a Threshold is Crossed, page 13-4

Trigger an Action Each Time a Threshold is Crossed

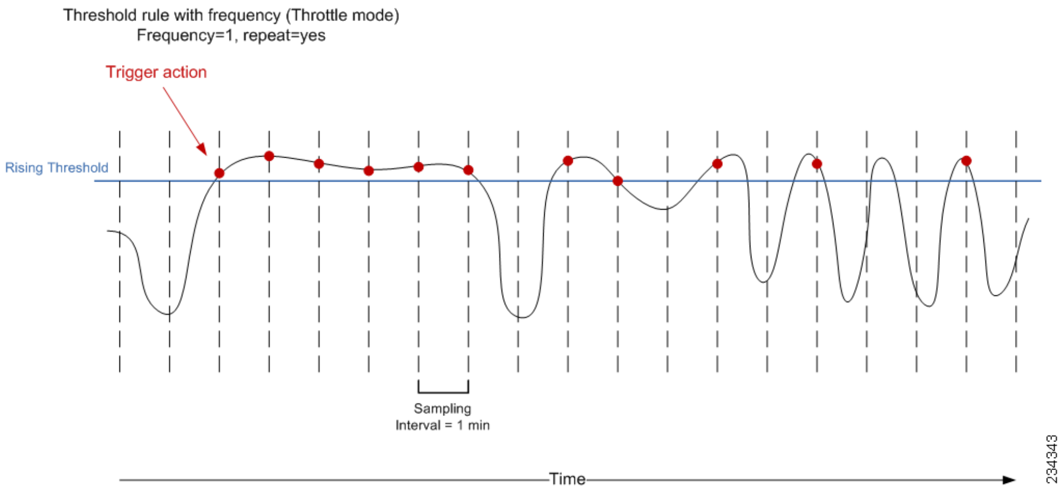
To trigger an action each time a threshold is crossed, set properties as follows:

- Frequency—**1**
- Repeat—**Yes**

Figure 13-1 shows the trigger action when you set rule properties to the preceding values.

FINAL DRAFT

Figure 13-1 Trigger an Action Each Time a Threshold is Crossed



If the sampled variable crosses the threshold, an action is taken the first time it crosses the threshold. As a result, an action is performed each time the threshold is crossed.

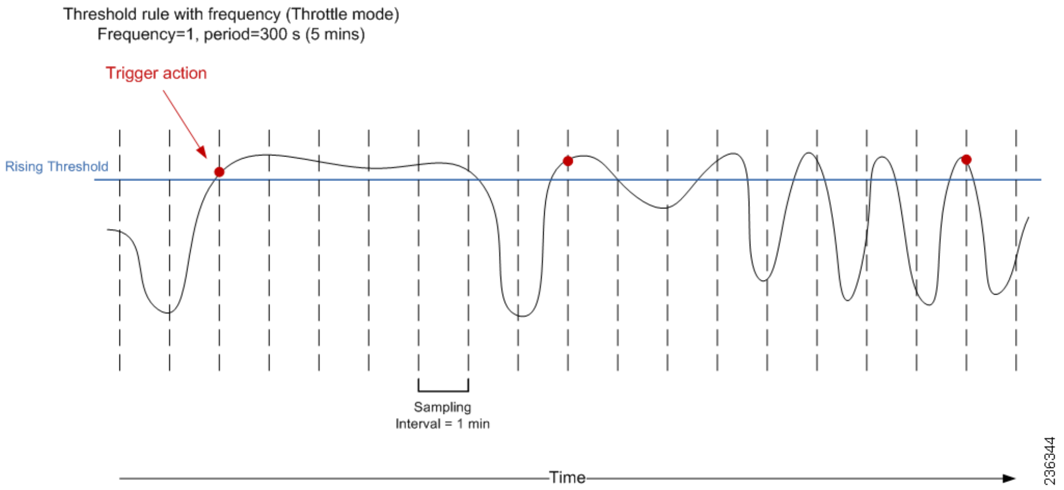
Trigger an Action Only Once in a Period When a Threshold is Crossed

To trigger an action only once in a period when a threshold is crossed, set properties as follows:

- Frequency—**1**
- Period—**300**
- Repeat—**No**

Figure 13-2 shows the trigger action when you set rule properties to the preceding values.

Figure 13-2 Trigger an Action Only Once When a Threshold is Crossed Within a Period



If the sampled variable crosses the threshold, an action is taken the first time it crosses the threshold. For the remaining 5 minutes, an action will not be taken. As a result, an action is performed only once during the specified period.

FINAL DRAFT

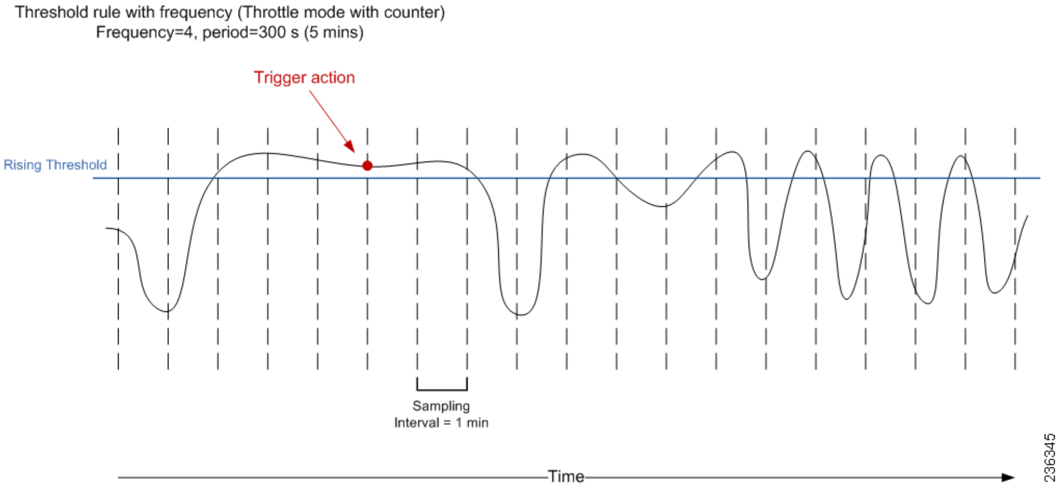
Trigger an Action Every Fourth Period When a Threshold is Crossed

To trigger an action every fourth period when a threshold is crossed, set properties as follows:

- Frequency—**4**
- Period—**300**
- Repeat—**No**

Figure 13-3 shows the trigger action when you set rule properties to the preceding values.

Figure 13-3 Trigger an Action Every Fourth Period When a Threshold is Crossed



If the sampled variable crosses the threshold, an action is taken the fourth time it crosses the threshold. For the remaining 5 minutes, an action is not taken. As a result, an action is performed only once during the specified period.

Configuring Threshold Rules

This section includes the following topics:

- Creating Threshold Rules, page 13-4
- Deleting Threshold Rules, page 13-5
- Editing Threshold Rules, page 13-6
- Viewing Threshold Rules, page 13-6
- Applying a Threshold Rule to a Chart, page 13-6

Creating Threshold Rules

You can create threshold rules using Cisco DCNM.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration** > **Threshold Rules**.

FINAL DRAFT

Step 2 From the toolbar, choose **New**, and then choose **New Threshold Rule**.

The Details and Threshold Bindings tabs appear in the Details pane, with the Details tab open.

Step 3 Create a threshold rule as follows:

a. In the Name field, enter a name.

b. In the Description field, enter a description of the threshold rule.

After you have enter a description, the Rising Threshold check box is automatically checked and the Threshold field in the Settings area is outlined in red.

Note A field outlined in red indicates that an entry is required. A field outlined in yellow indicates that the entry is satisfactory.

c. In the Settings area, enter a value in the Threshold field.

Once you have entered a value, the three options in the Action area are outlined in red.

d. In the Action area, provide one of the following:

- Enter email addresses (delimited with commas)
- Select **Sent Event** to forward events to the DCNM Event Browser
- Enter a script name

  The script receives all data regarding the crossed threshold. The script can be written in any programming language and saved in one of the directories of the system PATH.

Note Ensure that the Cisco DCNM server is configured for an SMTP server. For more information about configuring the Cisco DCNM server, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

e. (Optional) In the corresponding Settings and Action areas, configure a Falling Threshold.

f. (Optional) Click the **Threshold Bindings** tab to view bindings.

g. Click **Deploy**.

The rule is deployed.

When you exit Cisco DCNM and Save Pending Changes is checked in the Warning dialog box, click **Yes** to save the rule.

Deleting Threshold Rules

You can delete rules using Cisco DCNM.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration** > **Threshold Rules**.

The rules appear in the Summary pane.

Step 2 From the Summary pane, right-click the appropriate rule.

FINAL DRAFT

Step 3 From the drop-down list, choose **Delete Threshold Rule**.

A warning dialog box appears and displays “Are you sure you want to delete?”

Step 4 Click **Yes**.

The rule is deleted.

Editing Threshold Rules

You can view threshold rules using Cisco DCNM.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration** > **Threshold Rules**.

The rules appear in the Summary pane.

Step 2 Edit any appropriate areas.

Note You cannot edit the Name field.

Viewing Threshold Rules

You can view threshold rules using Cisco DCNM.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration** > **Threshold Rules**.

The rules appear in the Summary pane.

Step 2 Click on a rule to view it.

Applying a Threshold Rule to a Chart

You can apply threshold rules using Cisco DCNM.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose the appropriate feature. For example, if you wanted to see statistics for an Ethernet port, choose **Interfaces** > **Physical** > **Ethernet**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, choose the appropriate device.

FINAL DRAFT

Step 3 Click the **Statistics** tab.

Step 4 In the toolbar, click **New Chart** and then from the drop-down list choose the chart that you want to view. For example, if you wanted to see statistics for traffic, choose **Traffic Statistics Chart**.

Step 5 In the chart toolbar, click **Launch Threshold Setting**.

FINAL DRAFT

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 14

Administering Statistical Data Collection

This chapter describes how to administer Statistical Data Collection in the Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Statistical Data Collection

You can use the Statistical Data Collection feature to control the statistics monitoring processes that you have created for one of the many device configuration features that support statistics.

When you choose Statistical Data Collection on the Feature Selector pane, the Contents pane shows information about each statistical collection and allows you to control them. You can also use this feature to purge old data from the statistical database.

You can configure the length of time that Cisco Data Center Network Manager (DCNM) waits before retrieving statistical data from devices that it is monitoring. By default, Cisco DCNM retrieves statistical data from monitored devices every 30 seconds. You can increase the length of time to a maximum of 4 minutes. For more information, see the "Configuring Monitoring Preferences" section on page 3-16.

This section includes the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

Automatic and Manual Purging of Statistical Data

You can use the Statistical Data Collection feature to delete unwanted statistical data. Cisco DCNM supports automatic purging of statistical data. You can configure the following aspects of automatic statistical data purging:

- Days of the week and time of day that automatic purging occurs.
- Whether Cisco DCNM determines which statistical data to purge by the age of the data or by a maximum number of database entries.
- Whether Cisco DCNM deletes the statistical data entries that it purges or consolidates them into one entry.

You can also manually purge statistical data.

Virtualization Support

Cisco DCNM treats each virtual device context (VDC) on a Cisco NX-OS device as a separate device. Statistical data collections contain statistics from objects within devices.

Licensing Requirements for Statistical Data Collection

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Real-time monitoring requires no license. Cisco DCNM requires a LAN Enterprise license for the following features: • Maintaining a history of statistical data • Using overview charts For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Statistical Data Collection

Statistical data collection has the following prerequisites:

- The Cisco DCNM server must be able to connect to the devices.
- The system clocks for the Cisco DCNM server and Cisco DCNM client must be synchronized. If the system clocks are not synchronized, scheduling tasks for data collection may start or end at incorrect times.
- The Cisco NX-OS device must be running a supported version of Cisco NX-OS.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Send document comments to nexus7k-docfeedback@cisco.com

Guidelines and Limitations for Statistical Data Collection

The Statistical Data Collection feature has the following configuration guidelines and limitations:

- Collections are created by starting monitoring for a new chart. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 3-12.
- For the Statistical Data Collection feature, the Cisco DCNM client does not automatically update the information shown in the Summary pane. To ensure that you are viewing current information, from the menu bar, choose **View > Refresh**.
- When you start statistical monitoring for one or more charts and then close the Cisco DCNM client, a dialog box prompts you to decide whether to stop the collections or let them run. We recommend that you stop any unnecessary collections when you log out of the Cisco DCNM client. This practice conserves database space and decreases server load.
- We recommend that you configure automatic purging of statistical data to ensure that the Cisco DCNM database size does not grow too large.

Configuring Statistical Data Collection

This section includes the following topics:

Starting and Stopping Statistical Data Collection

You can use the Statistical Data Collection feature to start and stop a statistical data collection process. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

A table of statistical data collectors appears in the Contents pane. Each row corresponds to a collector for a particular device. The Status field displays whether the collector is running or is stopped.

Step 2 Click the collector that you want to start or stop.

Send document comments to nexus7k-docfeedback@cisco.com

Step 3 Do one of the following:

- To start a collector, from the menu bar, choose **Actions > Start Collection**. The Status field changes to Running.
- To stop a collector, from the menu bar, choose **Actions > Stop Collection**. The Status field changes to Stopped.

You do not need to save your changes.

Using Modes in Statistics Charts

You use statistics charts to toggle between the delta mode and the rate mode. Table 14-1 lists the features that contain statistics charts and delta mode/rate mode toggle button.

Table 14-1 *Features Containing Statistics Charts and Delta Mode/Rate Mode Toggle Button*

Path	Feature
Interfaces > Physical	Ethernet Interface
Interfaces > Physical	Management Interface
Interfaces > Logical	Loopback Interface
Interfaces > Logical	Port Channel
Interfaces > Logical	vPC
Switching	VLAN
Switching > Spanning Tree	Rapid PVST+
Switching > Spanning Tree	MST
Switching > Fabricpath	ISIS Process
Switching > Layer 2 Security	Port Security
Switching > Layer 2 Security	ARP Inspection
Switching > Layer 2 Security	DHCP Snooping
Switching > Layer 2 Security	Traffic Storm Control
Switching > Layer 2 Security	IGMP Snooping
Security	DOT1x
Security > Access Control	IPv4 ACL
Security > Access Control	IPv6 ACL
Security > Access Control	MAC ACL
Security > AAA	Server Groups
Inventory	Virtual Switch

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose the appropriate feature. For example, if you wanted to see statistics for the Ethernet feature, choose **Interfaces** > **Physical** > **Ethernet**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device.

Step 3 From the Summary pane, double-click **Slots**.

Step 4 Click the interface.

Step 5 From the Details pane, choose the **Statistics** tab.

Step 6 In the toolbar, click **New Chart** and then from the menu bar drop-down list, choose the chart that you want to view. For example, if you wanted to see statistics for traffic, choose **Traffic Statistics Chart**.

Step 7 (Optional) To toggle between the statistics mode and the rate mode, click the button to the right of the Select Frequency drop-down list.

Deleting Statistical Data from a Collection

You can delete statistical data from a collection. This feature allows you to delete all the data from a collection without affecting data from other collections and without deleting the collection itself. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

A table of statistical data collectors appears in the Contents pane. Each row corresponds to a collector for a particular device. Devices are listed alphabetically. The Status field displays whether the collector is running or is stopped.

Step 2 Right-click the collection.

Step 3 From the menu bar, choose **Actions > Delete Statistical Data**.

Cisco DCNM deletes all statistical data from the collection.

Deleting a Collection

You can delete a collection of statistical data from a specific device. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

Note If you want to delete all data from a collections rather than deleting the collection itself, perform the steps in the "Deleting Statistical Data from a Collection" section on page 14-5.

Send document comments to nexus7k-docfeedback@cisco.com

BEFORE YOU BEGIN

Determine which collection of data you want to delete.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

A table of statistical data collectors appears in the Contents pane. Devices are listed alphabetically. Each row corresponds to a collection of statistical data for a particular device.

Step 2 Click the collection of data that you want to delete.

Step 3 From the menu bar, choose **Actions > Delete Collection**.

The collection is deleted.

You do not need to save your changes.

Deleting Data from the Statistics Database

You can delete statistical data from the statistics database.

Note If you want to delete all data from a specific collection rather than deleting old data from all collections, perform the steps in the "Deleting a Collection" section on page 14-5.

BEFORE YOU BEGIN

Determine the date and time of the newest statistical data that you want to delete. When you follow the steps in this procedure, Cisco DCNM deletes all statistics that are older than the date and time that you select.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

The Statistics Database area appears in the Contents pane, below the table of statistical data collectors.

Step 2 From the Delete statistical data older than drop-down list, select the date and time of the newest statistics that you want to delete and click **OK**.

Step 3 Click **Delete**.

Cisco DCNM deletes all statistics older than the date and time that you specified.

Enabling and Disabling Automatic Statistical Data Purging

You can enable or disable the automatic purging of statistical data from the Cisco DCNM statistics database.

Send document comments to nexus7k-docfeedback@cisco.com

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

The Statistical Database Administration tab appears in the Details pane, below the table of statistical data collectors.

Step 2 Under Purge Settings, do one of the following:

- To enable automatic statistical data purging, check **Enable Auto Purge**.
- To disable automatic statistical data purging, uncheck **Enable Auto Purge**.

Step 3 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Configuring Automatic Statistical Data Purge Settings

You can configure when automatic statistical data purging occurs and the criteria that Cisco DCNM uses to determine which statistical data to purge.

BEFORE YOU BEGIN

Determine when you want automatic statistical data purging to occur. We recommend that automatic statistical data purging occur when Cisco DCNM usage is low.

If you perform backups of your Cisco DCNM databases, consider scheduling automatic statistical data purging after database backups have occurred, to ensure that you retain a record of all statistical data.

Determine what criteria you want Cisco DCNM to use to determine which statistical data to purge. The two criteria available are as follows:

- Age of statistical data—Cisco DCNM can purge all statistical data entries that are older than a specific number of days, weeks, or months.
- Number of statistical data entries in the database—When the number of statistical data entries in the database exceeds the maximum number that you specify, Cisco DCNM can purge the oldest statistical data entries first until the maximum number is not exceeded.

If you enable both criteria, Cisco DCNM applies them independently of each other.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

The Statistical Database Administration tab appears in the Details pane, below the table of statistical data collectors.

Step 2 Under Purge Threshold, configure the criteria that Cisco DCNM uses to determine which statistical data to purge. You can configure either or both of the criteria in the following table:

Send document comments to nexus7k-docfeedback@cisco.com

Purge Criteria	How to Configure
Age of statistical data	1. Check **Data older than**. 2. From the first drop-down list, choose the number of days, weeks, or months. 3. From the second drop-down list, choose **Days**, **Weeks**, or **Months**, as needed.
Number of statistical data entries in the database	1. Check **Total Entries Exceed(0-2147483647)**. 2. In the box, enter the maximum number of entries that you want to allow in the statistical database.

Step 3 Configure the action that you want Cisco DCNM to take on statistical database entries that meet the purge criteria. You can choose one of the following:

- **Delete**—Cisco DCNM deletes the database entries that meet the purge criteria.
- **Consolidate**—Cisco DCNM merges all statistical data entries that meet the purge criteria into one entry

Step 4 Under Purge Settings, follow these steps to configure when you want automatic purging to occur:

a. Check the days-of-the-week check boxes to specify which days of the week that you want automatic purging to occur.

b. Use the **Run at** box to configure the exact time on the specified days that you want automatic statistical data purging to occur.

Step 5 (Optional) If you want to enable automatic statistical data purging, check **Enable Auto Purge**.

Step 6 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Purging Statistical Data Now

You can purge statistical data on demand, using the automatic statistical data purge settings to determine which statistical data are purged.

Tip If you want to delete statistical data on demand, based on the exact age of the statistical data entries, see the "Deleting Data from the Statistics Database" section on page 14-6.

BEFORE YOU BEGIN

Ensure that the automatic statistical data purge settings are configured as needed. For more information, see the "Configuring Automatic Statistical Data Purge Settings" section on page 14-7.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

The Statistical Database Administration tab appears in the Details pane, below the table of statistical data collectors.

Step 2 Under Purge Settings, click **Purge Now**.

Cisco DCNM deletes statistical data, using the automatic statistical data purge settings to determine which statistical data entries to purge.

Send document comments to nexus7k-docfeedback@cisco.com

Viewing the Status of Statistical Data Collectors

To view the status of statistical data collectors, from the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

Collector status and other information appear in the Statistical Data Collectors area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Statistical Data Collection" section on page 14-10.

Field Descriptions for Statistical Data Collection

This section includes the following field descriptions for the Statistical Data Collection feature:

- Summary Pane, page 14-10
- Statistical Database Administration Tab, page 14-11

Summary Pane

Table 14-1 Summary Pane

Field	Description
Statistical Data Collectors	
Last Refresh Time	*Display only.* Date and time that the Cisco DCNM client updated information shown on the Content pane.
Collector ID	*Display only.* Name and IP address of the device for the corresponding poller.
Owner	*Display only.* Username of the Cisco DCNM user who started monitoring for the chart that corresponds to the collection.
Device	*Display only.* Name and IP address of the device that is providing the statistical data in the collection.
Objects	*Display only.* Description of the entity on the device that is providing the statistical data in the collection. For example, if the collection has statistical data for a rule that is assigned the sequence number 10 and is in an IPv4 ACL named acl-01, this field displays acl-01,seqNo=10. If the collection has data for the Ethernet 1/5 port, this field displays Ethernet1/5.
Collected Statistics	*Display only.* Type of statistical data in the collection. For example, if the collection has statistical data for a rule in an IPv4 ACL, this field displays IpAclAceMatchStatistics.
Status	*Display only.* Whether the collector is started or stopped.
Statistics Database	
Delete statistical data older than	Date and time of the newest statistical data to be deleted from the statistics database. There is no default value for this field.

Send document comments to nexus7k-docfeedback@cisco.com

Statistical Database Administration Tab

Table 14-2 Statistical Database Administration Tab

Field	Description
Delete statistical data older than	Date and time of the newest statistical data to be deleted from the statistics database. There is no default value for this field.
Auto Purge	
Action	Whether automatic statistical data purging deletes or consolidates statistical data entries that trigger the purge threshold. Consolidation merges all statistical data entries that trigger the purge threshold into one entry.
Purge Threshold	
Data older than	Whether, during automatic statistical data purging, Cisco DCNM deletes statistics entries that are older than the age specified in the drop-down lists located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default age is 1 day.
Total Entries Exceed	Whether, during automatic statistical data purging, Cisco DCNM deletes the oldest statistics entries until the number of entries equals the number in the box located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default number of event is 25,000.
Purge Settings	
Enable Auto Purge	Whether automatic purging of statistical data is enabled. By default, this check box is disabled.
Run on	Days of the week that automatic purging of statistical data occurs. By default, none of the check boxes are checked. If you check the Daily check box, the check boxes for the individual days of the week become unavailable.
Run at	Time of day that automatic purging of statistical data occurs, on the days of the week that automatic purging is enabled.

Additional References

For additional information related to administering statistical data collection, see the following sections:

- Related Documents, page 14-11
- Standards, page 14-12

Related Documents

Related Topic	Document Title
Device discovery	*Administering Device Discovery, page 5-1*

Send document comments to nexus7k-docfeedback@cisco.com

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Statistical Data Collection

Table 14-3 lists the release history for this feature.

Table 14-3 Feature History for Statistical Data Collection

Feature Name	Releases	Feature Information
Statistical Data Collection	5.0(2)	No change from Release 4.2.

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 15

Administering DCNM Server Log Settings

This chapter describes how to administer the DCNM Server Log Settings feature in Cisco Data Center Network Manager (DCNM).

This chapter includes the following section:

Information About Administering DCNM Server Log Settings

The Cisco DCNM server maintains a log file of its operations. The log file contains information from Cisco DCNM features and server components.

Note The DCNM Server Log Settings feature does not affect logging levels of Cisco NX-OS devices. Cisco DCNM does not support the configuration of device logging levels.

This section includes the following topics:

Send document comments to nexus7k-docfeedback@cisco.com

Logging Levels

The Cisco DCNM server supports a hierarchy of logging levels, ordered by the severity of log messages. Each level includes messages for that level in addition to all log messages from levels of higher severity. The logging levels, in order from the highest to the lowest severity, are as follows:

- Fatal Errors
- Errors
- Warnings
- Information
- Debugging
- Verbose

Log File and Location

The Cisco DCNM server writes server log messages to the sys.pipe file at the following location:

```
INSTALL_DIR\log
```

By default, when you install the Cisco DCNM server on Microsoft Windows Server, INSTALL_DIR is C:\Program Files\Cisco Systems\dcnm.

Virtualization Support

Cisco DCNM server logs do not contain log messages from Cisco NX-OS devices; therefore, this feature has no effect on virtualization support.

Licensing Requirements for Administering DCNM Server Log Settings

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	DCNM Server Log Settings requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Administering DCNM Server Log Settings

Administering Cisco DCNM server log settings has the following prerequisites:

- You should be familiar with a Cisco DCNM feature before you configure server log settings for it.

Send document comments to nexus7k-docfeedback@cisco.com

Guidelines and Limitations for Administering DCNM Server Log Settings

Administering Cisco DCNM server log settings has the following configuration guidelines and limitations:

- Setting a logging level to a lower severity results in more messages in the log file.
- We recommend using the default logging settings unless you are troubleshooting an issue.
- When you are troubleshooting an issue, consider lowering the logging level severity of the affected feature or server component.
- After you resolve an issue, consider restoring the logging level of the affected feature or server component to a higher severity.

Configuring DCNM Server Log Settings

This section includes the following topics:

- Configuring the Default Logging Level, page 15-3
- Configuring a Unique Logging Level for a Feature or Server Component, page 15-3
- Configuring a Feature or Server Component to Use the Default Logging Level, page 15-4

Configuring the Default Logging Level

You can configure the default logging level for all Cisco DCNM features and server components.

BEFORE YOU BEGIN

Determine what the default logging level should be. For more information, see the "Logging Levels" section on page 15-2.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The log settings appear in the Contents pane.

Step 2 From the Default Logging Level drop-down list, choose the logging level.

Step 3 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Configuring a Unique Logging Level for a Feature or Server Component

You can configure a logging level of a feature or server component that is independent of the default logging level.

Send document comments to nexus7k-docfeedback@cisco.com

BEFORE YOU BEGIN

Determine what the logging level of the feature or service should be. For more information, see the "Logging Levels" section on page 15-2.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The log settings appear in the Contents pane.

Step 2 Find the feature or server component that you want to configure with a unique logging level.

Step 3 Uncheck **Default** to the right of the feature or server component.

The logging level drop-down list for the feature or server component becomes available.

Step 4 From the logging level drop-down list, choose the logging level. For more information, see the "Logging Levels" section on page 15-2.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Configuring a Feature or Server Component to Use the Default Logging Level

You can configure a feature or server component to use the default logging level.

BEFORE YOU BEGIN

Ensure that the default logging level is appropriate for the feature or service. For more information, see the "Logging Levels" section on page 15-2.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The log settings appear in the Contents pane.

Step 2 Find the feature or server component that you want to use the default logging level.

Step 3 Check **Default** to the right of the feature or service.

The logging level drop-down list for the feature or server component becomes unavailable.

Step 4 From the menu bar, choose **File > Deploy** to apply your changes to the Cisco DCNM server.

Viewing DCNM Server Log Settings

To view Cisco DCNM server user accounts, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The default logging level, feature logging settings, and server component logging settings appear in the Contents pane. For information about the fields that appear, see the "Field Descriptions for DCNM Server Log Settings" section on page 15-5.

Send document comments to nexus7k-docfeedback@cisco.com

Field Descriptions for DCNM Server Log Settings

This section includes the following field descriptions for Cisco DCNM server log settings:

- DCNM Server Log Settings Content Pane, page 15-5

DCNM Server Log Settings Content Pane

Table 15-1 DCNM Server Log Settings Content Pane

Field	Description
Default Logging Level	Logging level for the features or server components whose Default check box is checked. The default value for this list is Informational. For more information about logging levels, see the "Logging Levels" section on page 15-2.
Cisco DCNM Features	
Default	Whether logging for the corresponding feature uses the default logging level or the logging level specified for the feature. When a Default check box is checked, the logging level list for the corresponding feature is unavailable. By default, these check boxes are unchecked.
AAA	Logging level for the AAA feature.
ACL	Logging level for the access control list feature.
Dot1X	Logging level for the 802.1X feature.
GLBP	Logging level for the Gateway Load-Balancing Protocol feature.
Interfaces	Logging level for the Interfaces feature.
Key Chain	Logging level for the keychain management feature.
Layer 2 Security	Logging level for the layer 2 security feature, which are as follows: • Dynamic ARP inspection • Port security • DHCP snooping • IP Source Guard • Traffic storm control
Object Tracking	Logging level for the object tracking feature.
Port Channel	Logging level for the port security feature.
SPAN	Logging level for the SPAN feature.
Spanning Tree	Logging level for the STP feature.
Tunnel	Logging level for the tunnel interface management feature.
Virtual Devices	Logging level for the virtual device context feature.
VLAN	Logging level for the VLAN feature.
FabricExtender	Logging level for the FabricExtender feature.
VPC	Logging level for the vPC feature.

Send document comments to nexus7k-docfeedback@cisco.com

Table 15-1 DCNM Server Log Settings Content Pane (continued)

Field	Description
HSRP	Logging level for the HSRP feature.
DEVICE GROUP	Logging level for the Device Groups feature.
Cisco DCNM Server Components	
Default	Whether logging for the corresponding server component uses the default logging level or the logging level specified for the component. When a Default check box is checked, the logging level list for the corresponding component is unavailable. By default, these check boxes are unchecked.
Event	Logging level for the event component, which includes messages about how Cisco DCNM processes the system and accounting logs it retrieves from devices and also events generated by Cisco DCNM.
Statistics Collection	Logging level for the statistical data collection component.
Config Archive	Logging level for the configuration archive component, used by the Configuration Change Management feature.
Device Connections	Logging level for the component that connects the Cisco DCNM server to devices.
Device Discovery	Logging level for the component that performs device discovery.

Additional References

For additional information related to administering Cisco DCNM server log settings, see the following sections:

- Related Documents, page 15-6
- Standards, page 15-6

Related Documents

Related Topic	Document Title
Troubleshooting Cisco DCNM	*Chapter 18, "Troubleshooting Cisco DCNM"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Send document comments to nexus7k-docfeedback@cisco.com

Feature History for DCNM Server Log Settings

Table 15-2 lists the release history for this feature.

Table 15-2 Feature History for DCNM Server Log Settings

Feature Name	Releases	Feature Information
Device Groups logging	5.0(2)	Support was added for configuring the logging level for the Device Groups feature.

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 16

Starting and Stopping Cisco DCNM Servers

This chapter describes how to start or stop Cisco Data Center Network Manager (DCNM) servers.

This chapter includes the following sections:

Information About Starting and Stopping Cisco DCNM Servers

Starting and stopping Cisco DCNM servers is a necessary part of server maintenance, such as during database backup, cleaning, or restoration. In a clustered server deployment, the order in which you start Cisco DCNM servers determines which server is the master server. This chapter provides detailed steps for starting and stopping Cisco DCNM servers for both single-server deployments and clustered-server deployments.

Licensing Requirements for Starting and Stopping Cisco DCNM Servers

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Starting and stopping Cisco DCNM servers requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Send document comments to nexus7k-docfeedback@cisco.com

Starting Cisco DCNM Servers

This section includes the following topics:

- Starting a Single Cisco DCNM Server, page 16-2
- Starting a Cluster of Cisco DCNM Servers, page 16-3

Starting a Single Cisco DCNM Server

You can start a single Cisco DCNM server. The procedures for starting a single Cisco DCNM server differ for systems using the supported Microsoft Windows Server and Red Hat Enterprise Linux (RHEL) operating systems, as described in the following topics:

- Starting a Single Cisco DCNM Server (Microsoft Windows Server), page 16-2
- Starting a Single Cisco DCNM Server (RHEL), page 16-2

Starting a Single Cisco DCNM Server (Microsoft Windows Server)

On a server system running Microsoft Windows Server, you can start a Cisco DCNM server through the Windows services or by clicking the Start DCNM Server icon.

BEFORE YOU BEGIN

You must have installed the Cisco DCNM server.

If you are starting a server cluster, ensure that you are starting the server in the correct order. For more information, see the "Starting a Cluster of Cisco DCNM Servers" section on page 16-3.

DETAILED STEPS

Step 1 Open the Control Panel window and choose **Administrative Tools > Services**.

The Services window opens.

Step 2 Right-click **Cisco DCNM Server** and choose **Start**.

Note Alternatively, you can choose **Start > All Programs > Cisco DCNM Server > Start DCNM Server**; however, the location of shortcuts depends upon the choices you made when you installed the Cisco DCNM server.

A splash screen opens while the Cisco DCNM server starts. This screen closes once the Cisco DCNM server is running.

Starting a Single Cisco DCNM Server (RHEL)

You can start a Cisco DCNM server on a RHEL server system by using /etc/init.d/jboss start.

Send document comments to nexus7k-docfeedback@cisco.com

BEFORE YOU BEGIN

The Cisco DCNM server must be installed.

If you are starting a server cluster, ensure that you are starting the server in the correct order. For more information, see the "Starting a Cluster of Cisco DCNM Servers" section on page 16-3.

DETAILED STEPS

Step 1 Use **/etc/init.d/jboss start** to start the Cisco DCNM server.

The Cisco DCNM server opens a server console window and displays the processes it runs to start the server. The server is running when you see a "Started in *X*m:*XX*s:*XXX*ms" message.

Starting a Cluster of Cisco DCNM Servers

Depending on the operating system of the secondary server, the Cisco DCNM server can be started using the Windows GUI, the CLI, or the DCNM Install Manager tool. You can use the CLI or the DCNM Install Manager tool for a secondary server running RHEL. For a secondary server running Microsoft Windows, the Cisco DCNM server is started with the Windows GUI.

Starting with Windows GUI or RHEL CLI

Starting a cluster of Cisco DCNM servers requires starting each server individually; however, the order of server startup is important. The server with the oldest start time performs the master server role in the server cluster.

BEFORE YOU BEGIN

We recommend that you use the primary installation server as the master server. For information about deploying a clustered-server environment, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

If any server in the cluster is running, stop it prior to starting the cluster. The only way that you can control which server is the master server is by ensuring that the master server is started before the other servers start. For detailed steps, see the "Stopping Cisco DCNM Servers" section on page 16-5.

DETAILED STEPS

Step 1 Start the server that you want to be the master server of the cluster. To do so, follow the steps for starting a single Cisco DCNM server for the applicable operating system:

- Starting a Single Cisco DCNM Server (Microsoft Windows Server), page 16-2
- Starting a Single Cisco DCNM Server (RHEL), page 16-2

Step 2 Wait for the master server to finish starting.

Step 3 One at a time, start the other servers in the cluster one at a time. After starting a server, wait at least one minute before starting the next server. This delay helps ensure faster stabilization of the server cluster.

For each server, follow the steps for starting a single Cisco DCNM server for the applicable operating system:

Send document comments to nexus7k-docfeedback@cisco.com

- Starting a Single Cisco DCNM Server (Microsoft Windows Server), page 16-2
- Starting a Single Cisco DCNM Server (RHEL), page 16-2

Starting with Install Manager

DCNM Install Manager is a GUI tool for servers running Linux. It is designed to assist in performing silent mode operations on secondary servers (remote nodes).

Note DCNM Install Manager does not support Windows servers.

DETAILED STEPS

Step 1 To access Install Manager, navigate to the dcnm-install-manager.sh file that is located in the bin folder where the DCNM server was installed.

The default bin folder location for servers running Linux is /usr/local/Cisco/dcm/dcnm/bin.

Step 2 Double click the **dcnm-install-manager.sh** file to launch Install Manager.

Step 3 Click the **New** icon in the tool bar near the top of the Install Manager GUI for every secondary server.

A new row in the list of Server Nodes is created every time the New icon is clicked.

Note Click the **Delete** icon in the tool bar to delete a selected row in the list of Server Nodes. This step does not delete a secondary server from the clustered-server environment.

Step 4 For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

  The protocol is either Telnet or SSH.
- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

  The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

  Alternatively, default user credentials may be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.
- (Optional) Comments that may be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the “+” icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

Step 5 In the list of Server Nodes, select the secondary servers to start.

Step 6 In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers.

Correct any connectivity issues before continuing.

Step 7 In the toolbar, click the **Start** icon to start the selected secondary servers.

Send document comments to nexus7k-docfeedback@cisco.com

Note The Install Manager is a standalone application. The settings specified are not saved and are not persistent. The settings are lost when the Install Manager GUI is closed.

Stopping Cisco DCNM Servers

This section includes the following topics:

- Stopping Single Cisco DCNM Servers, page 16-5
- Stopping a Cluster of Cisco DCNM Servers, page 16-6

Stopping Single Cisco DCNM Servers

You can stop a single Cisco DCNM server.

The steps for stopping a single Cisco DCNM server differ for systems using the supported Microsoft Windows Server and RHEL operating systems, as described in the following topics:

- Stopping a Single Cisco DCNM Server (Microsoft Windows Server), page 16-5
- Stopping a Single Cisco DCNM Server (RHEL), page 16-5

Stopping a Single Cisco DCNM Server (Microsoft Windows Server)

On a server system running Microsoft Windows Server, you can stop a Cisco DCNM server through the Windows services or by clicking the Stop DCNM Server icon.

DETAILED STEPS

Step 1 Open the Control Panel window and choose **Administrative Tools > Services**.

A window opens listing the Windows services.

Step 2 Right-click **Cisco DCNM Server** and choose **Stop**.

Note Alternatively, you can choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**; however, the location of shortcuts depends upon the choices you made when you installed the Cisco DCNM server.

A splash screen opens while the Cisco DCNM server begins to shut down. When the Cisco DCNM server has stopped, the splash screen closes.

Stopping a Single Cisco DCNM Server (RHEL)

On a server system running RHEL, you can stop a Cisco DCNM server with /etc/init.d/jboss stop.

DETAILED STEPS

Step 1 Use **/etc/init.d/jboss stop** to stop the server on a RHEL operating system.

The Cisco DCNM server opens a server console window and displays the processes that it runs to stop the server. The server is stopped when you see a "Stopped at *X*m:*XX*s:*XXX*ms" message.

Stopping a Cluster of Cisco DCNM Servers

Depending on the operating system of the secondary server, the Cisco DCNM server can be stopped using the CLI or the DCNM Install Manager tool. You can use the CLI or the DCNM Install Manager tool for a secondary server running RHEL. For a secondary server running Microsoft Windows, the Cisco DCNM server is stopped with the CLI.

Stopping with CLI

If you have a clustered-server Cisco DCNM deployment, you can use the stop-dcnm-cluster script to stop all the servers in the cluster.

BEFORE YOU BEGIN

Ensure that you know which server is currently the master server in the Cisco DCNM server cluster. You can use the Cluster Administration feature to do so. For more information, see the "Viewing Server Information" section on page 11-4.

DETAILED STEPS

Step 1 On the master server, access a command prompt.

Step 2 Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:

cd *path*

where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the Cisco DCNM bin directory is C:\Program Files\Cisco Systems\dcm\dcnm\bin. For RHEL, the default path to the bin directory is /usr/local/cisco/dcm/dcnm/bin.

Step 3 Run the **stop-dcnm-cluster** script. The script name depends upon the server operating system, as shown in the following table:

Server Operating System	Stop DCNM Cluster Script
Microsoft Windows	stop-dcnm-cluster.bat
Linux	stop-dcnm-cluster.sh

The script instructs each Cisco DCNM server in the cluster to stop.

Example

The following example from a Microsoft Windows server shows how to stop a cluster of Cisco DCNM servers, with Cisco DCNM installed in the default directory:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"

C:\Program Files\Cisco Systems\dcm\dcnm\bin>stop-dcnm-cluster.bat

C:\Program Files\Cisco Systems\dcm\dcnm\bin>set JAVA_HOME=C:\Program Files\Cisco Systems\
dcm\java\jre1.5

C:\Program Files\Cisco Systems\dcm\dcnm\bin>"C:\Program Files\Cisco Systems\dcm\
jboss-4.2.2.GA\bin\twiddle.bat" -s 172.28.254.254:1099 invoke
"com.cisco.dcbu.dcm:service=ClusterServerInfo" stopServerInstancesInCluster 10
Shutdown Triggered for all Servers Successfully
C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

Stopping with Install Manager

Cisco DCNM Install Manager is a GUI tool for servers running Linux. It is designed to assist in performing silent mode operations on secondary servers (remote nodes).

Note Cisco DCNM Install Manager does not support Windows servers.

DETAILED STEPS

Step 1 To access Install Manager, navigate to the dcnm-install-manager.sh file that is located in the bin folder where the DCNM server was installed.

The default bin folder location for servers running Linux is /usr/local/Cisco/dcm/dcnm/bin.

Step 2 Double click the **dcnm-install-manager.sh** file to launch Install Manager.

Step 3 Click the **New** icon in the toolbar near the top of the Install Manager GUI for every secondary server.

A new row in the list of Server Nodes is created every time the New icon is clicked.

Note In the toolbar, click the **Delete** icon to delete a selected row in the list of Server Nodes. This step does not delete a secondary server from the clustered-server environment.

Step 4 For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

  The protocol is either Telnet or SSH.
- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

  The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

Send document comments to nexus7k-docfeedback@cisco.com

Alternatively, default user credentials may be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.

- (Optional) Comments that may be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the "+" icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

Step 5 In the list of Server Nodes, select the secondary servers to stop.

Step 6 In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers.

Correct any connectivity issues before continuing.

Step 7 In the toolbar, click the **Stop** icon to stop the selected secondary servers.

Note The Install Manager is a standalone application. The settings specified are not saved and are not persistent. The settings are lost when the Install Manager GUI is closed.

Related Documents

Related Topic	Document Title
Deploying single Cisco DCNM servers and deploying Cisco DCNM server clusters	*Cisco DCNM Installation and Licensing Guide, Release 5.x*
Viewing server cluster information	Chapter 11, "Working with Cluster Administration"
Backing up, cleaning, and restoring Cisco DCNM databases	Chapter 17, "Maintaining the Cisco DCNM Database"

Feature History for Starting and Stopping a Cisco DCNM Server

Table 16-1 lists the release history for this feature.

Table 16-1 Feature History for Starting and Stopping a Cisco DCNM Server

Feature Name	Releases	Feature Information
Starting and stopping a cluster of servers	5.0(2)	Support for starting and stopping a cluster of servers was introduced.

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 17

Maintaining the Cisco DCNM Database

This chapter describes how to maintain the Cisco Data Center Network Manager (DCNM) database.

This chapter includes the following sections:

- Information About Database Maintenance, page 17-1
- Licensing Requirements for Database Maintenance, page 17-3
- Prerequisites for Database Maintenance, page 17-3
- Guidelines and Limitations for Database Maintenance, page 17-3
- Performing Database Maintenance, page 17-4
- Additional References, page 17-9
- Feature History for Cisco DCNM Database Maintenance, page 17-9

Information About Database Maintenance

Cisco DCNM uses a PostgreSQL database or an Oracle database to store all data, including configuration information from managed devices, events and statistical data gathered from managed devices, and Cisco DCNM user information. In addition to scripts that you can run to perform database maintenance, Cisco DCNM provides features to help you delete events and statistical data that you no longer need.

This section includes the following topics:

- Automatic and Manual Purging of Data, page 17-1
- Database Backup, page 17-2
- Database Clean, page 17-2
- Database Restore, page 17-2

Automatic and Manual Purging of Data

You can use the Auto-Synchronization with Devices feature to delete unwanted event data and the Statistical Data Collection feature to delete unwanted statistical data. Cisco DCNM supports automatic purging of both types of data. You can configure the following aspects of automatic data purging:

Send document comments to nexus7k-docfeedback@cisco.com

- Days of the week and time of day that automatic purging occurs.
- Whether Cisco DCNM determines which data to purge by the age of the data or by a maximum number of database entries.
- For event-related data, whether Cisco DCNM determines which events to purge by event severity.

We recommend that you configure automatic purging of events and statistical data to ensure that the Cisco DCNM database size does not grow too large.

You can also manually purge events and statistical data.

For more information, see the following sections:

- Automatic and Manual Purging of Event Data, page 12-2
- Automatic and Manual Purging of Statistical Data, page 14-2

Database Backup

You can use the Cisco DCNM database backup script to create a backup file of the Cisco DCNM database.

We strongly recommend that you regularly back up the Cisco DCNM database and that you archive backup files in a secure location that is not on the Cisco DCNM server system. You should retain the backup files as long as required by the standards of your organization.

Database Clean

You can use the Cisco DCNM database clean script to clean the Cisco DCNM database. Cleaning removes all Cisco DCNM data from the database and is a necessary step prior to restoring the Cisco DCNM database. Any database records that have not been backed up are lost when you clean the database.

You can also clean the database if you want to delete all data and rebuild your Cisco DCNM implementation without restoring data from a backup.

Database Restore

You can use the Cisco DCNM database restore script to restore the Cisco DCNM database from a backup file. The backup file must have been created by the Cisco DCNM database backup script included in the same release of Cisco DCNM that you are restoring the data to. For example, if you are running Cisco DCNM Release 5.0(2), you should only perform database restoration from a backup of Cisco DCNM Release 5.0(2).

Also, the backup file must have been created from the same database type and release that you are restoring the data to. For example, if you are restoring data to an Oracle 11g database, the backup file must have been created from an Oracle 11g database.

Before you restore a Cisco DCNM database, you should clean the database. Restoring a database without cleaning the database can have unpredictable results.

Send document comments to nexus7k-docfeedback@cisco.com

Licensing Requirements for Database Maintenance

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Database maintenance requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Database Maintenance

Database maintenance has the following prerequisites:

- You must have successfully installed the Cisco DCNM server.
- Cleaning the Cisco DCNM database requires that you stop the Cisco DCNM server.
- Restoring the Cisco DCNM database requires the following:
  - You must have a backup file created from exactly the same release of Cisco DCNM that you are restoring with the backup file.
  - You must have a backup file created from exactly the same database type and release that you are restoring data to.
  - You must have a backup file that was created from a Cisco DCNM database running in the same operating system as the database that you want to restore. For example, backup files made from a database running in Microsoft Server 2003 can only be used to restore other Cisco DCNM databases running in Microsoft Server 2003.

Guidelines and Limitations for Database Maintenance

Database maintenance has the following configuration guidelines and limitations:

- We recommend that you configure automatic purging of statistical data and event data to ensure that the Cisco DCNM database size does not grow too large.
- We recommend that you perform backups on a regular basis. Follow the standards of your organization to determine how frequently you should perform backups.
- You can only restore a Cisco DCNM database from a backup of the same release of Cisco DCNM. For example, if you are running Cisco DCNM Release 5.0(2), you should only perform database restoration from a backup of Cisco DCNM Release 5.0(2).
- You can only restore a Cisco DCNM database from a backup of the same database type and release as the current database. For example, if the current database is an Oracle 11g database, you can only restore it with a backup file made from an Oracle 11g database.
- You can only restore a Cisco DCNM database from a backup file that was made from a Cisco DCNM database running in the same operating system as the database that you want to restore. For example, backup files made from a database running in Microsoft Server 2003 can only be used to restore other Cisco DCNM databases running in Microsoft Server 2003.

Send document comments to nexus7k-docfeedback@cisco.com

Performing Database Maintenance

This section includes the following topics:

- Backing Up the Cisco DCNM Database, page 17-4
- Cleaning a Cisco DCNM Database, page 17-5
- Restoring a Cisco DCNM Database from a Backup File, page 17-7

Backing Up the Cisco DCNM Database

You can back up the Cisco DCNM database with the backup script. The Cisco DCNM server installer configures the backup script with the database username and database name that you specified during server installation.

DETAILED STEPS

Step 1 On the Cisco DCNM server, access a command prompt.

Step 2 Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:

cd *path*

where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the bin directory is C:\Program Files\dcm\dcnm\bin. For RHEL, the default path to the bin directory is /usr/local/cisco/dcm/dcnm/bin.

Step 3 Run the Cisco DCNM database backup script. The script name depends upon the server operating system and database type, as shown in the following table:

Server Operating System	Database Type	Backup Script Name
Microsoft Windows	PostgreSQL	backup-pgsql-dcnm-db.bat
	Oracle	backup-oracle-dcnm-db.bat
Linux	PostgreSQL	backup-pgsql-dcnm-db.sh
	Oracle	backup-oracle-dcnm-db.sh

Step 4 Enter the filename for the backup that you are creating.

Step 5 At the confirmation prompt, enter **y** to continue with the backup.

Step 6 Verify that the backup file was created as you specified and has a file size greater than zero.

- On Linux, use the **ls -l** command.
- On Microsoft Windows, use the **dir** command.

Step 7 Store the backup file in a safe location. We recommend that you copy the backup file to a secure location that is off the Cisco DCNM server system so that you can protect your data from the potential of a catastrophic hardware failure.

Example

The following example from a Windows server shows how to create a backup named masterbackup.bkp from a PostgreSQL Cisco DCNM database that was installed using default values:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"

C:\Program Files\Cisco Systems\dcm\dcnm\bin>backup-pgsql-dcnm-db.bat
 ========================================================

  Database Postgres Environment

  PostgreSQL Bin Path : ""C:\Program Files\Cisco Systems\dcm\db"\bin"

  DCNM Database Name : "dcmdb"

  DCNM Database User Name : "dcnmuser"

 ========================================================


Please enter the filename to be used for Database Backup:masterbackup.bkp
""
"Database Schema "dcnmuser" will be backed up in filename : masterbackup.bkp"
""
Continue y/n [n] : y
.
.
.
Database backup File: woobie1
 Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>dir masterbackup.bkp
 Volume in drive C has no label.
 Volume Serial Number is D415-F632

 Directory of C:\Program Files\PostgreSQL\8.2\bin

06/15/2009 01:53 PM           900,129 masterbackup.bkp
               1 File(s)        900,129 bytes
               0 Dir(s)  23,960,858,624 bytes free

C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

Cleaning a Cisco DCNM Database

You can use the Cisco DCNM database clean script to clean the database, which deletes all data from the Cisco DCNM database. You may want to clean the database for the following reasons:

- You want to restore the Cisco DCNM database from a backup.
- You want to delete all data and rebuild your Cisco DCNM implementation without restoring data from a backup.

The Cisco DCNM server installer configures the clean script with the database username and database name that you specified during server installation.

Send document comments to nexus7k-docfeedback@cisco.com

BEFORE YOU BEGIN

Back up the Cisco DCNM database. Any data not preserved in a backup is lost when you clean the database.

Stop the Cisco DCNM server. The Cisco DCNM server must be down before you can finish the database cleaning procedure. For detailed steps, see the "Stopping Cisco DCNM Servers" section on page 16-5.

DETAILED STEPS

Step 1 On the Cisco DCNM server, access a command prompt.

Step 2 If you have not already done so, stop the Cisco DCNM server. For detailed steps, see the "Stopping Cisco DCNM Servers" section on page 16-5.

Step 3 Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:

cd *path*

where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the bin directory is C:\Program Files\dcm\dcnm\bin. For RHEL, the default path to the bin directory is /usr/local/cisco/dcm/dcnm/bin.

Step 4 Run the Cisco DCNM database clean script. The script name depends upon the server operating system and database type, as shown in the following table:

Server Operating System	Database Type	Clean Script
Microsoft Windows	PostgreSQL	clean-pgsql-dcnm-db.bat
	Oracle	clean-oracle-dcnm-db.bat
Linux	PostgreSQL	clean-pgsql-dcnm-db.sh
	Oracle	clean-oracle-dcnm-db.sh

Step 5 At the confirmation prompt, enter **y** to continue with cleaning the database.

Step 6 If you want to restore the Cisco DCNM database from a backup, proceed to the "Restoring a Cisco DCNM Database from a Backup File" section on page 17-7. Do not start the Cisco DCNM server.

If you do not want to restore the Cisco DCNM database from a backup and want to rebuild your Cisco DCNM implementation manually, start the Cisco DCNM server. See the "Starting a Single Cisco DCNM Server" section on page 16-2.

Example

The following example from a Windows server shows how to clean a PostgreSQL Cisco DCNM database that was installed using default values:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"

C:\Program Files\Cisco Systems\dcm\dcnm\bin>clean-pgsql-dcnm-db.bat

 =======================================================

  Database Postgres Environment
  PostgreSQL Bin Path : ""C:\Program Files\Cisco Systems\dcm\db"\bin"

  DCNM Database Name : "dcmdb"

  DCNM Database User Name : "dcnmuser"

  DCNM Database SuperUser Name : "cisco"
 =========================================================



 ***************************************************************************
 PLEASE MAKE SURE THE DCNM SERVICE IS SHUTDOWN BEFORE RUNNING THIS SCRIPT!!
 ***************************************************************************


DCNM database schema  "dcnmuser" will be deleted permanently...

Please Confirm y/n [n] : y
.
.
.
 Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

Restoring a Cisco DCNM Database from a Backup File

You can use the Cisco DCNM database restore script to restore the Cisco DCNM database from a backup file. The restore script cleans the database prior to restoring it.

BEFORE YOU BEGIN

Locate the backup file that you want to use to restore the Cisco DCNM database.

Ensure that the backup file that you want to use to restore the database was made from the same release of Cisco DCNM. For example, you can only restore a Cisco DCNM Release 5.0(2) database from a backup file created from a Cisco DCNM Release 5.0(2) database.

Ensure that the backup file was made from the same database type and release as the current database. For example, you can only restore an Oracle 11g database from a backup file made from an Oracle 11g database.

Ensure that the backup file was made from a Cisco DCNM database running in the same operating system as the Cisco DCNM server that you want to restore the database to. For example, backup files made from a database running in Microsoft Server 2003 can only be used to restore other Cisco DCNM databases running in Microsoft Server 2003.

The Cisco DCNM server must be stopped while you are restoring the database.

DETAILED STEPS

Step 1 On the Cisco DCNM server, access a command prompt.

Step 2 If you have not already done so, stop the Cisco DCNM server. For detailed steps, see the “Stopping Cisco DCNM Servers” section on page 16-5.

Step 3 Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:

cd *path*

where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the bin directory is C:\Program Files\dcm\dcnm\bin. For RHEL, the default path to the bin directory is /usr/local/cisco/dcm/dcnm/bin.

Step 4 Run the Cisco DCNM database restore script. The script name depends upon the server operating system and database type, as shown in the following table:

Server Operating System	Database Type	Restore Script
Microsoft Windows	PostgreSQL	restore-pgsql-dcnm-db.bat
	Oracle	restore-oracle-dcnm-db.bat
Linux	PostgreSQL	restore-pgsql-dcnm-db.sh
	Oracle	restore-oracle-dcnm-db.sh

Step 5 Enter the name of the backup file that you want to use to restore the Cisco DCNM database.

Step 6 At the confirmation prompt, enter **y** to continue with the database restore.

Step 7 To resume using Cisco DCNM, start the Cisco DCNM server. See the "Starting a Single Cisco DCNM Server" section on page 16-2.

Example

The following example from a Microsoft Windows server shows how to restore a Cisco DCNM PostgreSQL database that was installed using default values and using a backup file named masterbackup.bkp that exists in the bin directory Cisco DCNM installation directory:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"


C:\Program Files\Cisco Systems\dcm\dcnm\bin>restore-pgsql-dcnm-db.bat
 ========================================================

  Database Postgres Environment

  PostgreSQL Bin Path : ""C:\Program Files\Cisco Systems\dcm\db"\bin"

  DCNM Database Name : "dcmdb"

  DCNM Database User Name : "dcnmuser"

 ========================================================


 ***************************************************************************
 PLEASE MAKE SURE THE DCNM SERVICE IS SHUTDOWN BEFORE RUNNING THIS SCRIPT!!
 ***************************************************************************



Please enter the filename to be used for Database Restore:masterbackup.bkp
""
"Database Schema "dcnmuser" will be Restore from filename : masterbackup.bkp"
""
Continue y/n [n] : y
```

Send document comments to nexus7k-docfeedback@cisco.com

```
"Cleaning the database...
.
.
.
"Done"
pg_restore: connecting to database for restore
.
.
.
Restored Database from : masterbackup.bkp
 Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>
```

Additional References

For additional information related to maintaining the Cisco DCNM database, see the following sections:

- Related Documents, page 17-9
- Standards, page 17-9

Related Documents

Related Topic	Document Title
Automatic purge of event data	*Chapter 12, "Administering Auto-Synchronization with Devices"*
Automatic purge of statistical data	*Chapter 14, "Administering Statistical Data Collection"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for Cisco DCNM Database Maintenance

Table 17-1 lists the release history for this feature.

Table 17-1 Feature History for Cisco DCNM Database Maintenance

Feature Name	Releases	Feature Information
Database maintenance scripts	5.0(2)	No change from Release 4.2(3).

Send document comments to nexus7k-docfeedback@cisco.com

Send document comments to nexus7k-docfeedback@cisco.com

CHAPTER 18

Troubleshooting Cisco DCNM

This chapter describes some common issues you might experience while using Cisco Data Center Network Manager (DCNM), and provides solutions.

Note For troubleshooting Cisco DCNM server installation issues, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

This chapter includes the following sections:

- Tips for Using Cisco DCNM, page 18-1
- Trouble with Starting the Cisco DCNM Server, page 18-2
- Trouble with the Cisco DCNM Database, page 18-3
- Trouble with the Cisco DCNM Client, page 18-5
- Trouble with Device Discovery or Device Status, page 18-11
- Trouble with Device Management, page 18-12
- Trouble with Topology, page 18-12
- Trouble with Device OS Management, page 18-13
- Trouble with Event Browsing, page 18-13

Tips for Using Cisco DCNM

This section includes the following topics:

- Events Tabs Show Fewer Events than the Event Browser, page 18-1
- Event Browser Pie Chart May Be Inaccurate for Small Numbers, page 18-2

Events Tabs Show Fewer Events than the Event Browser

The Event Browser feature shows all messages received by Cisco DCNM, even if the message pertains to a feature that is not supported by Cisco DCNM.

An Events tab shows only those messages that reflect the status of the currently selected feature. For some features, this is a subset of the possible messages about the feature.

Send document comments to nexus7k-docfeedback@cisco.com

Event Browser Pie Chart May Be Inaccurate for Small Numbers

The Event Browser pie chart may sometimes show incorrect sizes for wedges that are less than 5 percent of the pie; however, the numbers shown are correct.

Trouble with Starting the Cisco DCNM Server

This section includes the following topics:

- Cisco DCNM Server Fails to Start, page 18-2

Cisco DCNM Server Fails to Start

Check Table 18-1 for symptoms related to downloading the Cisco DCNM client. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-1 Cisco DCNM Server Fails to Start

Symptom	Possible Cause	Solution
Cisco DCNM server fails to start.	The Postgres database did not install.	For troubleshooting Cisco DCNM server installation issues, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
	The Postgres service is not running.	Start the Postgres service: • In Microsoft Windows Server, choose **Start > All Programs > Postgres 8.2 > Start Service**. • In RHEL, use the following command: **/DCNM/db/bin/DB start**
	The Postgres user credentials are incorrect.	1. Correct the Postgres user credentials. For detailed steps, see the "Updating Cisco DCNM Database Name and Username in pgAdmin III" section on page 18-3. 2. Start the Cisco DCNM server. For detailed steps, see the "Starting Cisco DCNM Servers" section on page 16-2.
	The ports used by the server are already in use.	1. Check the server log for messages such as "Port *port-number* already in use." The server log is the following file: *Installation_directory*\jboss-4.2.2.GA\server\dcnm\log\server.log 2. Determine which application is using the port and stop or reconfigure the application. 3. Restart the Cisco DCNM server.

Send document comments to nexus7k-docfeedback@cisco.com

Trouble with the Cisco DCNM Database

This section includes the following topics:

- Trouble with a PostgreSQL Database, page 18-3
- Trouble with an Oracle Database, page 18-4

Note If the Cisco DCNM database fails or communication to the Cisco DCNM database fails, you must stop the DCNM Server or shutdown the cluster of DCNM Servers before addressing the problem. Always verify that the Cisco DCNM database and the communication to the Cisco DCNM database are functioning properly before restarting the DCNM Server or cluster of DCNM Servers.

Trouble with a PostgreSQL Database

Check Table 18-2 for symptoms related to the pgAdmin III application for administering a postgreSQL database used with Cisco DCNM. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-2 pgAdmin III Errors

Symptom	Possible Cause	Solution
Error message states that the Cisco DCNM database does not exist.	The Cisco DCNM database name might have changed during an upgrade or reinstallation of the Cisco DCNM server software.	In the pgAdmin III application, perform the steps in the "Updating Cisco DCNM Database Name and Username in pgAdmin III" section on page 18-3.
Error message states that password authentication failed for the Cisco DCNM database username.	The Cisco DCNM database username may have changed during an upgrade or reinstallation of the Cisco DCNM server software.	

Updating Cisco DCNM Database Name and Username in pgAdmin III

You can update the Cisco DCNM database and username in pgAdmin III.

Step 1 Open the pgAdmin III application.

Step 2 In the Object Browser pane, under Servers, click **PostgreSQL Database Server 8.2**.

In the right-hand pane, the Properties tab appears with several other tabs.

Step 3 On the Properties tab, double-click **Maintenance database**.

A dialog box displays a Properties tab for the server.

Step 4 If you need to change the database name, click the **Maintenance DB** field and type the correct Cisco DCNM database name.

Note The database name should be the name that you specified when you most recently upgraded or reinstalled the Cisco DCNM server software.

Send document comments to nexus7k-docfeedback@cisco.com

Step 5 If you need to change the database username, click the **Username** field and type the correct Cisco DCNM database username.

> **Note** The database username should be the database username that you specified when you most recently upgraded or reinstalled the Cisco DCNM server software.

Step 6 Click **OK**.

Step 7 In the Object Browser pane, double-click **PostgreSQL Database Server 8.2**.

If you changed the username in Step 5, the Connect to Server dialog box appears.

Step 8 If necessary, enter the password for the username that you specified in Step 5 and click **OK**.

The pgAdmin III application connects to the Cisco DCNM database and displays the databases and login roles.

If you need additional assistance, see the Help menu in the pgAdmin III application or see the pgAdmin web site at the following URL:

http://pgadmin.org/docs/1.6/index.html

Trouble with an Oracle Database

If the Cisco DCNM server has trouble using an Oracle database, it logs the error messages in the following file:

Installation_directory\jboss-4.2.2.GA\server\dcnm\log\server.log

Check Table 18-3 for symptoms related using an Oracle database with Cisco DCNM. For each error message, see the possible cause and follow the corresponding solution.

Table 18-3 Cisco DCNM server.log File Errors with an Oracle Database

Symptom	Possible Cause	Solution
The following error appears in the server.log file: `java.sql.SQLException: ORA-01653: unable to extend table Cisco DCNMUSER.DCMRAWEVENTTABLE by 1024 in tablespace SYSTEM`	The tablespace SYSTEM is too small.	1. Stop the Cisco DCNM server. See Chapter 16, "Starting and Stopping Cisco DCNM Servers." 2. Increase the SYSTEM table space. For detailed steps, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*. 3. Start the Cisco DCNM server. See Chapter 16, "Starting and Stopping Cisco DCNM Servers."

The following error appears in the server.log file:
`[org.hibernate.util.JDBCExceptionReporter] Could not create connection; - nested throwable:`
`(java.sql.SQLException: Listener refused the connection with the following error:`
`ORA-12519, TNS:no appropriate service handler found`
	The number of available sessions and processes is inadequate.	1. Stop the Cisco DCNM server. See Chapter 16, "Starting and Stopping Cisco DCNM Servers."
		2. Increase the number of sessions and processes to 150 each. For detailed steps, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
		3. Start the Cisco DCNM server. See Chapter 16, "Starting and Stopping Cisco DCNM Servers."

The following error appears in the server.log file:
`2009-04-08 15:53:47,125 ERROR [org.hibernate.util.JDBCExceptionReporter]`
`ORA-00604: error occurred at recursive SQL level 1`
`ORA-01000: maximum open cursors exceeded`
	The number of open cursors is inadequate.	1. Stop the Cisco DCNM server. See Chapter 16, "Starting and Stopping Cisco DCNM Servers."
		2. Increase the number of open cursors to 1000. For detailed steps, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
		3. Start the Cisco DCNM server. See Chapter 16, "Starting and Stopping Cisco DCNM Servers."

Trouble with the Cisco DCNM Client

This section includes the following topics:

- Cannot Download the Cisco DCNM Client from the Server, page 18-6
- Cannot Install the Cisco DCNM Client, page 18-6
- Cannot Start the Cisco DCNM Client, page 18-7
- Cannot Log into the Cisco DCNM Client, page 18-8
- Client Loses Connection to the Cisco DCNM Server, page 18-10

Send document comments to nexus7k-docfeedback@cisco.com

Cannot Download the Cisco DCNM Client from the Server

Check Table 18-4 for symptoms related to downloading the Cisco DCNM client. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-4 Cannot Download the Cisco DCNM Client from the Server

Symptom	Possible Cause	Solution
Cannot download the Cisco DCNM client from the server.	You are using the wrong URL or web server port.	Verify that you are using the correct URL, including the port number.
	The TCP port is blocked by a gateway device.	Open the TCP port in your firewall. For information about ports used by Cisco DCNM, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
	You are using an unsupported web browser.	Use a supported web browser. For more information about supported web browsers, see the *Cisco DCNM Release Notes, Release 5.x*.

Cannot Install the Cisco DCNM Client

Check Table 18-4 for symptoms related to installing the Cisco DCNM client. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-5 Cannot Install the Cisco DCNM Client

Symptom	Possible Cause	Solution
Installer attempts to install Java version 1.5.0_11 but fails.	The system does not have Internet access.	The Cisco DCNM client installer requires Internet access to download the Java version 1.5.0_11 JRE. If the system cannot access the Internet, use another system to download the Java installer, copy it to the system that you want to install the Cisco DCNM client on, install Java, and restart the Cisco DCNM client installation. You can download Java version 1.5.0_11 JRE from the Java[tm] Technology Products Download website, at http://java.sun.com/products/archive. The Java version 1.5.0_11 JRE is listed as JRE 5.0 Update 11.
	Your network environment requires the use of a proxy connection to access the Internet.	If your network environment requires a proxy connection to permit the download of the Java installer, ensure that the proxy settings are configured in Internet Options, available from the Control Panel. For more information, see http://java.sun.com/j2se/1.5.0/proxy_note.html.

Send document comments to nexus7k-docfeedback@cisco.com

Cannot Start the Cisco DCNM Client

Check Table 18-6 for symptoms related to starting the Cisco DCNM client. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-6 Cannot Start the Cisco DCNM Client

Symptom	Possible Cause	Solution
Cannot start the Cisco DCNM client.	The client installation may be corrupted. The wrong version of Java may be installed.	1. Uninstall the Cisco DCNM client. For more information, see the "Uninstalling the Cisco DCNM Client" section on page 2-8. 2. Download and install the Cisco DCNM client from the Cisco DCNM server. During the client installation, allow Cisco DCNM to install the supported version of Java on the computer. When you download the client from the Cisco DCNM server, if the supported version of Java is not detected on the computer, Cisco DCNM asks you for permission to install the supported version of Java. Your browser may notify you that the Java installer was digitally signed by an expired certificate. To continue, confirm the installation. For more information, see the "Downloading and Launching the Cisco DCNM Client" section on page 2-3.

Send document comments to nexus7k-docfeedback@cisco.com

Cannot Log into the Cisco DCNM Client

Check Table 18-7 for symptoms related to logging into the Cisco DCNM client. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Send document comments to nexus7k-docfeedback@cisco.com

Table 18-7 Cannot Log into the Cisco DCNM Client

Symptom	Possible Cause	Solution
Cannot log into the Cisco DCNM client.	You forgot your password.	Ask a Cisco DCNM administrator to reset your password using one of the following scripts: • For Microsoft Windows, use *dcnm_root_directory*/dcm/dcnm/bin/pwreset.bat (by default, *dcnm_root_directory* is c:\Program Files\Cisco Systems\dcm\dcnm\bin). • For Linux, use *dcnm_root_directory*/dcm/dcnm/bin/pwreset.sh (by default, the *dcnm_root_directory* is /usr/local/cisco). To reset a password, run the appropriate script for the operating system that you are using, and then enter the user ID to be reset and the password to be used for it. If no one has administrative access to Cisco DCNM, you can reset the local administrator account or change Cisco DCNM server authentication settings by reinstalling the Cisco DCNM server software. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
	Authentication servers are not configured to authenticate Cisco DCNM users.	If Cisco DCNM is configured to use authentication servers, ensure that every authentication server that you have configured Cisco DCNM to use is configured to accept authentication requests from the Cisco DCNM server. If you have deployed Cisco DCNM in a clustered-server environment, ensure that every authentication server is configured to accept requests from each Cisco DCNM server in the cluster.
	The Cisco DCNM server is down.	Restart the Cisco DCNM server. See the "Starting a Single Cisco DCNM Server" section on page 16-2.
	The Cisco DCNM server is unreachable.	Ensure that the computer that runs the Cisco DCNM client meets the network requirements for using the Cisco DCNM client remotely. Any gateway network devices between the Cisco DCNM client and server must allow connections to the Cisco DCNM web server and to the Cisco DCNM server. By default, the Cisco DCNM web server listens to port 8080 and the Cisco DCNM server listens to port 1099; however, you can configure these ports during Cisco DCNM server installation. If you need to change either port, reinstall the server and choose the Full Reinstall option. For information about ports used by Cisco DCNM, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
	The Cisco DCNM server IP address changed after you installed the server.	Do the following: 1. Ensure that the IP address of the Cisco DCNM server is statically assigned. 2. Reinstall the Cisco DCNM server and choose the Full Reinstall option, which allows you to specify the server IP address. See the *Cisco DCNM Installation and Licensing Guide, Release 5.x*. 3. Log into the Cisco DCNM client and specify the new IP address of the Cisco DCNM server in the DCNM Server field of the login dialog box.

Send document comments to nexus7k-docfeedback@cisco.com

Table 18-7 Cannot Log into the Cisco DCNM Client (continued)

Symptom	Possible Cause	Solution
Cannot log into the Cisco DCNM client (continued).	The wrong Cisco DCNM server port number was used in the login attempt.	In the Cisco DCNM client login window, click **More** and, in the Port field, change the port number that your Cisco DCNM server uses. See the "Restarting the Cisco DCNM Client" section on page 2-7. If you want to change the port that the Cisco DCNM server listens to, reinstall the Cisco DCNM server and choose the Full Reinstall option, which allows you to specify the Cisco DCNM server port. See the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
When you try to log into the Cisco DCNM client, you receive the error message "Can not resolve Cisco DCNM server *hostname* via DNS. Make sure that Cisco DCNM server has a valid DNS entry."	You used a hostname to specify the Cisco DCNM server during the login and DNS does not have an entry for the Cisco DCNM server.	Ensure that DNS on your network has an entry for the Cisco DCNM server hostname.

Client Loses Connection to the Cisco DCNM Server

Check Table 18-8 for symptoms related to the Cisco DCNM client losing its connection with the server. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-8 Client Loses Connection to the Cisco DCNM Server

Symptoms	Possible Cause	Solution
• Client loses connection to the server. • The Cisco DCNM client window is pink.	The client had a failure.	Restart the Cisco DCNM client.
	The Cisco DCNM server is down.	Restart the Cisco DCNM server. See Chapter 16, "Starting and Stopping Cisco DCNM Servers."
	The Cisco DCNM server is unreachable.	Investigate your network to determine if it meets the network requirements for using the Cisco DCNM client remotely. For information about ports used by Cisco DCNM, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Send document comments to nexus7k-docfeedback@cisco.com

Trouble with Device Discovery or Device Status

Check Table 18-9 for symptoms related to issues with device discovery or the device status. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-9 Trouble with Device Discovery or Management

Symptoms	Possible Cause	Solution
• A device discovery task fails. • A device status changes to Unmanaged or Unreachable.	Incorrect device credentials were provided.	Reenter the username and password, and try discovering the device again. If you are attempting to discover CDP neighbors of the seed device, ensure that the credentials that you provide are valid on all devices that you want to discover.
	The SSH server is disabled on the device.	Reenable the SSH server on the device and try discovering the device again.
	The maximum number of SSH sessions that the device can support has been reached.	Check the number of user sessions on the device. Free at least one connection and try discovering the device again.
	CDP is disabled on the device or on the device interface that the Cisco DCNM server connects to.	Ensure that CDP is enabled on the device globally and that it is enabled on the specific interface that the Cisco DCNM server connects to.
	The device interface that the Cisco DCNM server connects to is shut down.	Ensure that the device interface that the Cisco DCNM server connects to is up.
	The device restarted or shut down before discovery could complete.	Ensure that the device is running and try discovering the device again.
	The Cisco DCNM server cannot reach the device.	Ensure that the network requirements for device management are met. See the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

Send document comments to nexus7k-docfeedback@cisco.com

Trouble with Device Management

Check Table 18-6 for symptoms related to device management. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-10 Trouble with Device Management

Symptom	Possible Cause	Solution
Clearing the log file or the accounting log on a Cisco NX-OS device does not cause Cisco DCNM to rediscover the device automatically.	The device did not generate a system message about the accounting log or the log file being cleared. This problem is particularly likely if the device is a Cisco MDS 9000 Family Multilayer Switch running Cisco SAN-OS Release 3.1 or earlier.	Rediscover the device. For more information, see the "Discovering a Device" section on page 6-4.
The Cisco DCNM client shows device configuration information that is out of date.	The Cisco DCNM server was down.	You can do either of the following: • Rediscover the device. For more information, see the "Discovering a Device" section on page 6-4. • Restart the Cisco DCNM server with a clean database. If the server was down for a long time, this action is the recommended solution. 1. Stopping Cisco DCNM Servers, page 16-5 2. Cleaning a Cisco DCNM Database, page 17-5 3. Starting Cisco DCNM Servers, page 16-2

Trouble with Topology

Check Table 18-11 for symptoms related to using the topology feature. For each symptom that describes your trouble, determine which possible cause applies and follow the corresponding solution.

Table 18-11 Trouble with Topology

Symptom	Possible Cause	Solution
• Links between Cisco MDS 9000 Family Multilayer Switches continue appear after the link has gone down.	Devices are connected by Gigabit Ethernet or Fast Ethernet ports, and are running Cisco SAN-OS Release 3.1 or earlier.	Rediscover the devices that topology incorrectly shows as linked.

Send document comments to nexus7k-docfeedback@cisco.com

Trouble with Device OS Management

Check Table 18-12 for symptoms related to the Device OS Management feature. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-12 Trouble with Device OS Management

Symptom	Possible Cause	Solution
• During a software installation job, the software image file transfer between a file server and a device takes too much time.	The connection between the file server and the device is slow.	Use a file server that is on the same LAN as the devices included in the software installation job. If all of the available file servers transfer software image files too slowly, before you create the software installation job, manually copy the files to the devices that you will include the job and configure the job to use the manually copied files rather than a file server. For information about configuring a software installation job, see the *Cisco DCNM System Management Configuration Guide, Release 5.x*.

Trouble with Event Browsing

Check Table 18-13 for symptoms related to event browsing issues. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 18-13 Trouble with Event Browsing

Symptom	Possible Cause	Solution
• Events available on the device command line do not appear in the Cisco DCNM client. • Too few events are shown in Event Browser or an Events tab.	Logging levels on managed devices are set incorrectly.	Check the logging level configuration on managed devices. See the "Cisco NX-OS System-Message Logging Requirements" section on page 5-3.
	The Cisco DCNM client fetches events that are not old enough.	Check the events-related setting in the Cisco DCNM client preferences. For more information, see the "Configuring the Maximum Age of Events Fetched from the Server" section on page 3-16.

Send document comments to nexus7k-docfeedback@cisco.com

Table 18-13 Trouble with Event Browsing

Symptom	Possible Cause	Solution
Too many events are shown in Event Browser or on an Events tab.	A managed device has an issue that is generating many system log messages.	Temporarily unmanage the device until you resolve the issues on the device. For more information, see the "Unmanaging a Device" section on page 6-5.
	Logging levels on managed devices are set incorrectly.	Check the logging level configuration on managed devices. See the "Cisco NX-OS System-Message Logging Requirements" section on page 5-3.
A feature Events tab does not show events that appear in the Event Browser.	By design, an Events tab shows only messages that apply to the currently selected feature and may show only a subset of the possible messages for the feature. For more information, see the "Events Tabs Show Fewer Events than the Event Browser" section on page 18-1.	Use the Event Browser to see status-related system messages received by Cisco DCNM. For more information, see the *Cisco DCNM System Management Configuration Guide, Release 5.x*.

Send document comments to nexus7k-docfeedback@cisco.com

INDEX

Send document comments to nexus7k-docfeedback@cisco.com