INDEX

A

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco DCNM Fundamentals Configuration Guide, Release 4.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 4.2, see the *Cisco DCNM Release Notes, Release 4.x*.

Table 1 summarizes the new and changed features for the *Cisco DCNM Fundamentals Configuration Guide, Release 4.x* and tells you where they are documented.

Table 1 New and Changed Features for Release 4.x

Feature	Description	Changed in Release	Where Documented
NX-OS device configuration requirements	Contains revised information for how to configure an NX-OS device to enable discovery, management, and monitoring by DCNM.	4.0(3)	Chapter 1, "Overview"
Server installation	Support was added for Oracle 10g and 11g databases. Support was added for installing Cisco DCNM on a shared server with Cisco Fabric Manager.	4.2(1)	Chapter 2, "Installing and Launching the Cisco DCNM Server"
Server installation	You can specify the following during installation: • DCNM server IP address • DCNM server port number • DCNM web server port number • A folder to be used as an archive directory	4.1(2)	Chapter 2, "Installing and Launching the Cisco DCNM Server"
Upgrading the DCNM Server Software	Explains how to upgrade the DCNM server software and PostgreSQL database.	4.0(2)	Chapter 2, "Installing and Launching the Cisco DCNM Server"
Windows Service	Describes how the DCNM server is run as a service in the Windows Server 2003 operating system.	4.0(2)	Chapter 2, "Installing and Launching the Cisco DCNM Server"

Table 1 New and Changed Features for Release 4.x (continued)

Feature	Description	Changed in Release	Where Documented
Cisco DCNM client	Support was added for exporting the summary table. Deployment of configuration changes was clarified, to indicate that deployment is sometimes automatic and sometimes manual.	4.2(1)	Chapter 4, "Using the Cisco DCNM Client"
Global Preferences dialog box	Explains the purpose of the fields in the Global Preferences dialog box in the DCNM client and how to configure the fields.	4.0(3)	Chapter 4, "Using the Cisco DCNM Client"
Cisco DCNM server authentication settings	Support was added for RADIUS and TACACS+ authentication of Cisco DCNM server users.	4.2(1)	Chapter 5, "Administering DCNM Authentication Settings"
DCNM Licensed Devices	Controls which devices you can use with licensed DCNM features.	4.0(2)	Chapter 8, "Administering DCNM Licensed Devices"
Topology	Support for hierarchical and grid layouts was removed.	4.2(1)	Chapter 9, "Working with Topology"
Topology	The topology map has new views and includes support for virtual port channels.	4.1(2)	Chapter 9, "Working with Topology"
Event Browser	When you apply an event filter, it is shown in a new tab.	4.1(2)	Chapter 10, "Managing Events"
Event Filter	Filters events by date, time, and severity.	4.0(2)	Chapter 10, "Managing Events"
Device OS Management	A new feature, it allows you to schedule and monitor the installation of operating system software on managed devices.	4.1(2)	Chapter 13, "Managing Device Operating Systems"
Configuration Change	A new feature, it allows you to archive the configurations of managed devices. You can also roll back the configuration on a managed device to an earlier, archived version.	4.1(2)	Chapter 14, "Working with Configuration Change Management"
Auto-Synchronization with Devices	Support was added for automatic purging based on severity of events.	4.2(1)	Chapter 15, "Administering Auto-Synchronization with Devices"
Auto-Synchronization with Devices	Updates to this feature allow you to schedule the deletion of old event data from the database.	4.1(2)	Chapter 15, "Administering Auto-Synchronization with Devices"
Statistical Data Collection	Updates to this feature allow you to schedule the deletion of old statistical data from the database.	4.1(2)	Chapter 16, "Administering Statistical Data Collection"
Cisco DCNM database maintenance	Support was added for scripts to perform database backup, restore, and cleaning.	4.2(1)	Chapter 18, "Maintaining the Cisco DCNM Database"
Cisco DCNM database maintenance	New chapter that describes how to maintain the DCNM database.	4.1(2)	Chapter 18, "Maintaining the Cisco DCNM Database"
Troubleshooting	Troubleshooting information was added for PostgreSQL and Oracle databases.	4.2(1)	Chapter 19, "Troubleshooting Cisco DCNM"

Preface

This preface describes the audience, organization, and conventions of the *Cisco DCNM Fundamentals Configuration Guide, Release 4.x*. It also provides information on how to obtain related documentation.

This preface includes the following topics:

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 Server”	Describes how to install and set up the Cisco DCNM server, which is required for using the Cisco DCNM client.
Chapter 3, “Installing and Launching the Cisco DCNM Client”	Describes how to install and set up the Cisco DCNM client.
Chapter 4, “Using the Cisco DCNM Client”	Introduces the Cisco DCNM client and explains how to use it.

Chapter	Description
Chapter 5, "Administering DCNM Authentication Settings"	Describes how to administer Cisco DCNM server user accounts.
Chapter 6, "Administering Device Discovery"	Describes how to use the Device Discovery feature.
Chapter 7, "Administering Devices and Credentials"	Describes how to use the Devices and Credentials feature.
Chapter 8, "Administering DCNM Licensed Devices"	Describes how to use the DCNM Licensed Devices feature.
Chapter 9, "Working with Topology"	Describes how to use the Topology feature.
Chapter 10, "Managing Events"	Describes how to use the Event Browser and feature-specific Events tabs.
Chapter 11, "Working with Inventory"	Describes how to use the Inventory feature.
Chapter 12, "Configuring SPAN"	Describes how to use the Switched Port Analyzer (SPAN) feature.
Chapter 13, "Managing Device Operating Systems"	Describes how to use the Device OS Management feature.
Chapter 14, "Working with Configuration Change Management"	Describes how to use the Configuration Change Management feature.
Chapter 15, "Administering Auto-Synchronization with Devices"	Describes how to use the Auto-Synchronization with Devices feature.
Chapter 16, "Administering Statistical Data Collection"	Describes how to control statistical data collection.
Chapter 17, "Administering DCNM Server Log Settings"	Describes how to control Cisco DCNM server logs.
Chapter 18, "Maintaining the Cisco DCNM Database"	Explains how to maintain the Cisco DCNM database.
Chapter 19, "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.

Related Documentation

Cisco DCNM documentation is available at the following URL:

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

The documentation set for Cisco DCNM includes the following documents:

Release Notes

Cisco DCNM Release Notes, Release 4.x

DCNM Configuration Guides

Cisco DCNM Getting Started with Virtual Device Contexts, Release 4.x

Cisco DCNM Fundamentals Configuration Guide, Release 4.x

Cisco DCNM Interfaces Configuration Guide, Release 4.x

Cisco DCNM Layer 2 Switching Configuration Guide, Release 4.x

Cisco DCNM Web Services API Guide, Release 4.x

Cisco DCNM Security Configuration Guide, Release 4.x

Cisco DCNM Unicast Routing Configuration Guide, Release 4.x

Cisco DCNM Virtual Device Context Configuration Guide, Release 4.x

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). It also includes general Cisco DCNM deployment steps and details about preparing Cisco NX-OS devices for management and monitoring by Cisco DCNM.

This chapter includes the following sections:

Information About Cisco 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 4.x*.

This section includes the following topics:

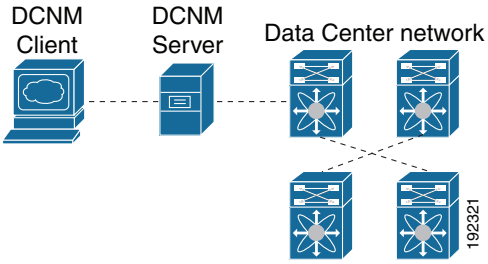
Cisco DCNM Client and Server

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 4.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 4.x*.

Figure 1-1 Cisco DCNM Client-Server Environment



Features in Cisco DCNM, Release 4.x

Cisco DCNM Release 4.x supports the configuration and monitoring of the following Cisco NX-OS features:

- Ethernet switching
  - Physical 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
- 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
  - Keychain management
- 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
- Event browser
- Configuration Change Management
- Device OS Management
- Hardware inventory

Cisco DCNM includes the following administrative features:

- Cisco DCNM server user accounts
- Device discovery, including support for Cisco Discovery Protocol
- Automatic synchronization with discovered devices
- Statistical data collection management
- Cisco DCNM server and client logging

Cisco DCNM Licensing

Many of the features of Cisco DCNM, Release 4.x, do not require a license; however, some features that support only Cisco Nexus 7000 Series devices do require a license. The following features are enabled in Cisco DCNM only after you have installed a LAN Enterprise license:

- vPCs
- 802.1X
- Gateway load-balancing protocol (GLBP)
- Object tracking
- Keychain management
- DHCP snooping
- Dynamic ARP Inspection
- ARP access control lists (ACLs)
- IP Source Guard
- Traffic storm control
- Port security
- IP tunnels

- Virtual Device Contexts (VDCs)
- Logical vPC view of the Topology feature
- Display of historical statistical data

For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the "Installing Licenses" section on page 2-11.

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 "Related Documentation" section on page xxiii.

Deploying Cisco DCNM

You can deploy Cisco DCNM to manage and monitor supported network devices. This procedure provides the general steps that you must take to deploy Cisco DCNM and links to more detailed procedures to help you with each general step.

BEFORE YOU BEGIN

Determine which computer will run the Cisco DCNM server software. This computer should meet the system requirements for the Cisco DCNM server. For details about system requirements, see the *Cisco DCNM Release Notes, Release 4.x*.

DETAILED STEPS

To deploy Cisco DCNM, follow these steps:

Step 1 Prepare the computer that you want to install the Cisco DCNM server on. For more information, see the "Prerequisites for Installing the Cisco DCNM Server" section on page 2-2.

Step 2 Download Cisco DCNM. For more information, see the "Downloading the Cisco DCNM Server Software" section on page 2-4.

Step 3 Install the Cisco DCNM server software. For more information, see the "Installing the Cisco DCNM Server" section on page 2-5.

Step 4 Start the Cisco DCNM server. For more information, see the "Starting the Cisco DCNM Server" section on page 2-9.

Step 5 (Optional) Install the license on the Cisco DCNM server. For more information, see the "Installing Licenses" section on page 2-11

Step 6 Install the Cisco DCNM client. For more information, see Chapter 3, "Downloading and Launching the Cisco DCNM Client."

Step 7 Prepare each Cisco NX-OS device that you want to manage and monitor by using Cisco DCNM. For more information, see the "Preparing a Cisco NX-OS Device for Management by Cisco DCNM" section on page 1-5.

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 perform the steps in "Preparing a Cisco NX-OS Device for Management by Cisco DCNM" section on page 1-5 for each VDC that you want to manage and monitor with Cisco DCNM.

Step 8 Perform device discovery for one or more devices. For more information, see the "Administering Device Discovery" section on page 6-1.

Step 9 (Optional) If you installed a license, enable Cisco DCNM to use licensed features on specific devices by adding managed devices to the license. For more information, see the "Administering DCNM Licensed Devices" section on page 8-1.

Step 10 Begin using Cisco DCNM to configure and monitor the managed devices. For more information about using Cisco DCNM, see the Cisco DCNM configuration guides.

Cisco NX-OS Device Configuration Requirements

This section provides information about device configuration requirements and configuration tasks you must perform on Cisco NX-OS devices that you want to manage and monitor by using Cisco DCNM. You must perform the configuration tasks by using a method other than Cisco DCNM, such as the CLI.

Note For up-to-date information about Cisco network device operating systems and hardware supported by Cisco DCNM, see the *Cisco DCNM Release Notes, Release 4.x*.

This section includes the following topics:

Preparing a Cisco NX-OS Device for Management by Cisco DCNM

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 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 perform the steps in "Preparing a Cisco NX-OS Device for Management by Cisco DCNM" section on page 1-5 for each VDC that you want to manage and monitor with Cisco DCNM.

DETAILED STEPS

To successfully discover a Cisco NX-OS device, Cisco DCNM requires that you configuring the following items in each VDC that you want to manage and monitor with Cisco DCNM:

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 Ensure that the Cisco NX-OS device meets the system-message logging requirements of Cisco DCNM. For more information, see the "Cisco NX-OS System-Message Logging Requirements" section on page 1-6.

Cisco NX-OS System-Message Logging Requirements

To monitor and manage devices, Cisco DCNM depends partly on system messages for some Cisco NX-OS features. To ensure that Cisco DCNM receives the messages that it needs, you must ensure that all Cisco NX-OS devices managed and monitored by Cisco DCNM meet the logging requirements described in this section.

This section includes the following topics:

Interface Link-Status Events Logging Requirement

You must configure the device 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 "Configuring a Device to Meet Cisco DCNM Logging Requirements" section on page 1-10.

Logfile Requirements

You must configure the device 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 "Configuring a Device to Meet Cisco DCNM Logging Requirements" section on page 1-10.

Logging Severity-Level Requirements

All enabled features on a Cisco NX-OS have a default logging level. For features supported by Cisco DCNM, Cisco DCNM requires the logging severity levels set to a specific level depending on the feature. The logging level required varies from feature to feature. Cisco DCNM cannot configure logging levels on the managed Cisco NX-OS devices. We plan to enhance Cisco DCNM to configure logging levels in a future release; however, with Cisco DCNM Release 4.2, you must ensure that any Cisco NX-OS device that you want to manage and monitor with Cisco DCNM is configured with logging levels that meet the logging-level requirements.

When evaluating the logging-level configuration of a device, consider the following:

- Cisco DCNM has logging-level requirements for only the features listed in the following tables:
  - For Nexus 7000 Series devices, see Table 1-1.
  - For Nexus 5000 Series devices, see Table 1-2.
  - For Nexus 4000 Series devices, see Table 1-3.

  If a Cisco NX-OS logging facility does not appear in Table 1-1, Table 1-2, or Table 1-3, then you do not need to configure a logging level in order for Cisco DCNM to successfully manage and monitor the device.
- The default Cisco NX-OS logging level for some facilities is not high enough to support management of the feature by Cisco DCNM. Be sure that you raise the logging level for a facility when its default level is not high enough to satisfy the Cisco DCNM logging-level requirement. In Table 1-1, Table 1-2, and Table 1-3, Cisco DCNM logging levels that exceed the default logging level appear in **bold** text.
- You can set a logging level higher than the Cisco DCNM requirement. The maximum logging severity level is 7. If a logging level exceeds the Cisco DCNM requirement, you do not need to lower the logging level.
- Cisco NX-OS does not support logging-level configuration for disabled features. If you disable a feature, any nondefault logging level configuration is lost and is not restored if you reenable the feature later. When you enable a feature, perform the steps in the "Configuring a Device to Meet Cisco DCNM Logging Requirements" section on page 1-10 to ensure that the logging level configuration for the feature meets Cisco DCNM requirements.
- When you create a new VDC, its running configuration includes only the default logging levels. For each VDC that you create, perform the steps in the "Configuring a Device to Meet Cisco DCNM Logging Requirements" section on page 1-10 to ensure that the logging level configuration in each VDC meets Cisco DCNM requirements.

To ensure that logging severity levels are correctly configured on the device, perform the steps in the "Configuring a Device to Meet Cisco DCNM Logging Requirements" section on page 1-10.

Table 1-1 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]	Your Current Logging Level
AAA	AAA	Yes	aaa	3	**5**	
	RADIUS	Yes	radius	3	**5**	
	TACACS+	No	tacacs+	3	**5**	
Device Discovery	CDP	Yes	cdp	2	**6**	
Topology						
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.

Table 1-2 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]	Your Current Logging Level
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						
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.

Table 1-3 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]	Your Current Logging Level
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						
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.

Configuring a Device to Meet Cisco DCNM Logging Requirements

When you are preparing a device for management and monitoring by Cisco DCNM, you can perform an initial logging configuration. If you later enable a feature that was previously disabled, we recommend that you perform this procedure again to ensure that logging configuration on the device meets Cisco DCNM requirements.

You should also perform this procedure when you create a VDC on a Cisco Nexus 7000 Series device. Regardless of whether you used Cisco DCNM to create the VDC or whether you used the CLI, the logging configuration of a new VDC is only the default configuration and must be configured to support management and monitoring by Cisco DCNM.

BEFORE YOU BEGIN

Consider printing Table 1-1, Table 1-2, or Table 1-3, as needed. You can use the Your Current Logging Level column to make notes about logging level configuration on the device.

DETAILED STEPS

To perform the initial Cisco NX-OS logging configuration, follow these steps:

Step 1 Log into the Cisco NX-OS device.

Step 2 Access the global configuration mode.

```
switch# configure terminal
switch(config)#
```

Step 3 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** 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 4 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 5 Determine which nondefault features are enabled on the device.

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

Step 6 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
.
.
```

.

Tip 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**.

Step 7 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 Step 6 to the minimum Cisco DCNM-required logging levels that are listed in the applicable table, as follows:

- For a Nexus 7000 Series device, see Table 1-1.
- For a Nexus 5000 Series device, see Table 1-2.
- For a Nexus 4000 Series device, see Table 1-3.

Step 8 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.

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

The *facility* argument is the applicable logging-facility keyword from Table 1-1, Table 1-2, or Table 1-3, and *severity-level* is the applicable minimum Cisco DCNM-required logging level or higher (up to 7).

Step 9 Use the **show logging level** command to verify your changes to the configuration.

Step 10 Copy the running configuration to the startup configuration to save your changes.

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

CHAPTER 2

Installing and Launching the Cisco DCNM Server

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

When you install the Cisco DCNM server, you initially install the software without applying a license. You can use many of the product features without using a license, but if you try to use a feature that requires a license, Cisco DCNM displays a message saying that a license is required for that feature. To use that feature and any other licensed feature, you must purchase and install the Cisco DCNM Enterprise LAN license.

If the server system is running the Windows Server 2003 operating system, the Cisco DCNM server runs as a Windows service. By default, the Cisco DCNM server starts automatically when you boot up the server system. You can manually stop, start, or pause this service. You can also change the startup instructions for Cisco DCNM to automatically start up when you start the operating system, start up manually, or be disabled from starting.

This chapter includes the following sections:

Cisco Fabric Manager Support

Beginning with Cisco DCNM Release 4.2(1), Cisco DCNM supports installing the Cisco DCNM server on a server system that has an installation of Cisco Fabric Manager Release 4.2(1) and later releases. If you install the Cisco DCNM server on a server system that already has an installation of Cisco Fabric Manager Release 4.2(1) and later releases, the Cisco DCNM installer detects the Fabric Manager installation, which has the following effects on the installation:

- The installation folder is determined by the installer and cannot be configured.
- The database that the installer configures the Cisco DCNM server to use is the database that Fabric Manager is configured to use. You cannot choose a database other than the database used by Fabric Manager.
- The installer resolves port conflicts between the ports in use by Fabric Manager and the default ports that the Cisco DCNM server uses.

Database Support

Cisco DCNM supports the following databases:

- PostgreSQL 8.1
- PostgreSQL 8.2
- Oracle Database 10g
- Oracle Database 11g

Note If you plan to use an Oracle database, ensure that the Oracle database meets the prerequisites listed in the "Prerequisites for Installing the Cisco DCNM Server" section on page 2-2.

If the Cisco DCNM installer does not find a previous installation of a supported database, it can install PostgreSQL 8.2 for you.

Prerequisites for Installing the Cisco DCNM Server

Before you can install the Cisco DCNM server, ensure that the Cisco DCNM server system meets the following prerequisites:

- The server system *must* meet the server system requirements published in the *Cisco DCNM Release Notes, Release 4.x*, available online at the following URL:

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/dcnm/release/notes/dcnm_4_2_relnotes.html

- If you plan to use an Oracle 10g database, configure the Oracle database as follows:
  - Increase the SYSTEM tablespace to 2 GB from the default 1 GB of space. For more information, see the "Increasing the SYSTEM Tablespace" section on page 19-9.
  - Increase the number of sessions and process to 150 each from the default of 50. For more information, see the "Increasing the Number of Sessions and Processes" section on page 19-9.
  - Increase the number of open cursors to 1000 from the default of 50. For more information, see the "Increasing the Number of Open Cursors" section on page 19-10.

- If you plan to use an Oracle 11g database, configure the Oracle database as follows:
  - Increase the number of sessions and process to 150 each from the default of 50. For more information, see the "Increasing the Number of Sessions and Processes" section on page 19-9.
  - Increase the number of open cursors to 1000 from the default of 300. For more information, see the "Increasing the Number of Open Cursors" section on page 19-10.
- For RHEL 4 AS, the maximum shared memory size must be 128 MB or more. To configure the maximum shared memory to 128 MB, use the following command:

  ```
  sysctl -w kernel.shmmax=134217728
  ```

  This setting, kernel.shmmax=134217728, should be saved in the /etc/sysctl.conf file. If this setting is not present or if it is less than 134217728, the Cisco DCNM server will fail after the server system is rebooted. For more information, see the following URL:

  http://www.postgresql.org/docs/8.2/interactive/kernel-resources.html
- The IP address of the server system should be statically assigned. The Cisco DCNM server binds to an IP address that you specify during installation. If the IP address of the server system changes after you install the Cisco DCNM server, Cisco DCNM clients are unable to connect to the Cisco DCNM server and you must stop and reinstall the Cisco DCNM server so that you can reconfigure the IP address.
- The server system must be registered with the DNS servers.
- A Perl environment must already be installed on the server system. We recommend Active Perl version 5.8.9.827. You can download ActivePerl for your server operating system from the following location:

  http://www.activestate.com/activeperl/downloads/
- The path to the Perl executable must be defined in the server system PATH environment variable.
- Ensure that no other programs are running on the server, except for Cisco Fabric Manager Release 4.2(1) and later releases and the database software used by Fabric Manager.

Server Ports

A Cisco DCNM server must be able to receive the network traffic from Cisco DCNM clients on a number of ports. Any network gateway device that controls the traffic sent from a Cisco DCNM client to a Cisco DCNM server must permit the traffic sent to the ports that the Cisco DCNM server is configured to use.

Table 2-1 lists the default ports that services on a Cisco DCNM server listen to for client communications. You can configure two ports during installation. If a default port is already in use on the server system, the Cisco DCNM server installer resolves the port conflict automatically by assigning a different port to the service.

Table 2-1 Default TCP Ports for Client Communications

Service Name	Default Port	Configurable?
RMI	1098	No
Naming Service	1099	During installation
EJB	3873	No
Server Bind 1	4445	No
Server Bind 2	4446	No

Table 2-1 Default TCP Ports for Client Communications (continued)

Service Name	Default Port	Configurable?
Syslog (system message) Receiver	5445	No
AJP Connector	8009	No
Web Server	8080	During installation
Web Service	8083	No
JMS	8093	No
RMI Object	14444	No

Downloading the Cisco DCNM Server Software

This section explains how to download the Cisco DCNM server software from Cisco.com. The file that you download is in tape archive (TAR) format. It contains the following files:

- dcnm-k9.*release*.exe—Installation file for the supported Windows operating system.
- dcnm-k9.*release*.bin—Installation file for the supported Linux operating system.

BEFORE YOU BEGIN

Downloading the Cisco DCNM server software requires a Cisco.com user account. If you do not have a Cisco.com user account, go to http://www.cisco.com/ and create one before you attempt to download the software.

DETAILED STEPS

To download the Cisco DCNM server software, follow these steps:

Step 1 Open a web browser and go to the following website:

http://www.cisco.com/

The Cisco web page opens.

Step 2 From the Support menu, choose **Download Software**.

The Download Software page appears.

Step 3 Under Select a Software Product Category, choose **Network Management**.

Step 4 If the Log In page appears now, enter your Cisco.com username and password, and then click **Log In**.

The Tools & Resources Download Software web page displays a tree of Cisco devices.

Step 5 From the tree, choose **Data Center Management > Cisco Data Center Network Manager**.

Step 6 If the Log In page appears now, enter your Cisco.com username and password, and then click **Log In**.

A tree of Cisco DCNM releases appears.

Step 7 From the tree, choose the Cisco DCNM release that you need.

To the right of the tree, the Download Now button appears beside the filename and information for the Cisco DCNM release that you chose.

Step 8 Click **Download Now**.

The Download Cart web page lists the Cisco DCNM release that you chose.

Step 9 Click **Proceed with Download**.

The browser lists a link to the software license agreement and the software download rules.

Step 10 Read the software license agreement and the rules, and then click **Agree**.

Step 11 Click **Non Java Download Option**.

A download list appears in a new browser window.

Step 12 Click the **Download** link that appears to the right of the Cisco DCNM release that you chose.

The download begins.

Step 13 After the download completes, extract the files from the downloaded TAR file by doing one of the following:

- For Microsoft Windows, use a file archive utility, such as WinZip, to extract the contents of the TAR file.
- For RHEL, use the following command to extract the contents of the TAR file:

```
tar -xvf dcnm-k9.release.tar
```

Installing the Cisco DCNM Server

Use this procedure to install the Cisco DCNM server on a server system that does not have a previous installation of the Cisco DCNM server.

On server systems that run the Windows Server 2003 operating system, the installer adds the Cisco DCNM server as a Windows service.

By default, the Cisco DCNM server service automatically starts when you start the server operating system.

BEFORE YOU BEGIN

Ensure that the server system satisfies the prerequisites. For more information, see the "Prerequisites for Installing the Cisco DCNM Server" section on page 2-2.

Download the Cisco DCNM server software. See the "Downloading the Cisco DCNM Server Software" section on page 2-4.

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that may interfere with the installation of the Cisco DCNM server software. After you have completed the installation, reenable the software or features.

DETAILED STEPS

To install the Cisco DCNM server software, follow these steps:

Step 1 Log into the server with a user account that has the required privileges, as follows:

- For Windows Server 2003, the user account must be a member of the local administrators group.

- For RHEL 4 AS, the user account must be root.

If you are installing Cisco DCNM on Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM server system.

Step 2 Go to the directory where you downloaded the Cisco DCNM server software and run one of the following files:

- For Windows Server 2003, run the dcnm-k9.*release*.exe file.
- For RHEL 4 AS, use the following **sh** command:

  ```
  sh dcnm-k9.release.bin
  ```

After the installer prepares the installation, the Introduction step appears in the Cisco DCNM installer window.

Step 3 Click **Next**.

Step 4 If the Choose Install Folder step appears in the Cisco DCNM installer window, do the following:

Note If the Cisco DCNM installer detects an installation of Cisco Fabric Manager Release 4.2(1) and later releases on the server system, the Choose Install Folder step does not appear.

a. (Optional) If you want to change the default installation folder, type or choose the desired installation folder.

b. Click **Next**.

The Database Options step appears in the Cisco DCNM installer window. You can use an exiting PostgreSQL installation, an existing Oracle installation, or if PostgreSQL is not installed on the server system, you can use the Cisco DCNM installer to add a PostgreSQL installation.

Note If the Cisco DCNM installer detects an installation of Cisco Fabric Manager Release 4.2(1) and later releases on the server system, the only database option that is available is the database that Fabric Manager is configured to use.

Step 5 If you want to install PostgreSQL, do the following:

a. Next to RDBMS, click **Install PostgreSQL**.

   If your server system runs RHEL 4 AS, the System User dialog box appears.

b. (RHEL 4 AS only) In the System User dialog box, type the username for the user account that should be used to run the PostgreSQL software. This user account should not have administrator or root privileges.

c. In the DB Admin User field, type the username of a database administrator account. The installer will create the administrator account that you specify.

d. In the DB Admin Password field, type the password for the database administrator username that you specified.

e. In the DCNM DB User field, type the username that Cisco DCNM should use to access the database. The default username is dcnmuser. The installer will create the user account that you specify.

f. In the DCNM DB Password field, type the password for the database user account that you specified.

g. In the Confirm DCNM DB Password field, retype the password for the database user account that you specified.

h. (Optional) If you want to change the default PostgreSQL database installation folder, in the Install Location field, type or choose the desired installation folder.

Step 6 If you want to use an existing relational database management system (RDBMS) installation, do the following:

a. Next to RDBMS, click one of the following:

- **Use existing PostgreSQL 8.1/8.2**
- **Use existing Oracle 10g/11g**

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the URL to the database.

Note If the Cisco DCNM installer detects an installation of Cisco Fabric Manager Release 4.2(1) and later releases on the server system, the DB URL field shows the URL of the Fabric Manager database and cannot be configured.

b. If the DB URL field does not have the correct URL to the database, type the correct URL.

c. In the DB Admin User field, type the username of a database user account that has permissions to create the Cisco DCNM database schema and user account.

d. In the DB Admin Password field, type the password for the database administrator username that you specified.

e. In the DCNM DB User field, type the username that Cisco DCNM should use to access the database.

The installer will use the Cisco DCNM admin user that you specified to create the Cisco DCNM database user account.

f. In the DCNM DB Password field, type the password for the database user account that you specified.

g. In the Confirm DCNM DB Password field, retype the password for the database user account that you specified.

Step 7 Click **Next**.

Step 8 If the Choose Database (PostgreSQL/Oracle) Root Folder step appears in the Cisco DCNM installer window, do the following:

a. Type or choose the folder that contains the BIN directory for the existing RDBMS that you specified. The installer lists the default installation paths for the supported databases.

b. Click **Next**.

The Configuration Options step appears in the Cisco DCNM installer window.

Step 9 From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently assigned to network interfaces on the server system.

Note The IP address of the server system should be statically assigned. The Cisco DCNM server binds to an IP address that you specify during installation. If the IP address of the Cisco DCNM server changes, Cisco DCNM clients are unable to connect to the Cisco DCNM server and you must reinstall the Cisco DCNM server so that you can reconfigure the IP address.

Step 10 If you want to change the port that the Cisco DCNM web server listens to, enter the new port number in the Web Server Port box. By default, the Cisco DCNM web server listens to TCP port 8080.

Note If you change the web server port number, it affects the URL that Cisco DCNM users use to download the Cisco DCNM client.

Step 11 If you want to change the port that the Cisco DCNM server accepts Cisco DCNM client connections on, enter the new port number in the Naming Service Port box. By default, the Cisco DCNM server accepts connections from Cisco DCNM clients on TCP port 1099.

Note If you change the Cisco DCNM server port number, it affects the port that Cisco DCNM users specify when they log into the Cisco DCNM client.

Step 12 Click **Next**.

The Choose Archive Folder step appears in the Cisco DCNM installer window.

Step 13 (Optional) If you want to change the archive folder, type or choose the desired archive folder.

Step 14 Click **Next**.

The Local User Credentials step appears in the Cisco DCNM installer window.

Step 15 In the Local Admin Username field, type a name for a Cisco DCNM server user. The installer will create the Cisco DCNM server user and assign the Administrator role to it.

Step 16 In the Password field, type a password for the user, and then in the Confirm Password field, type the password again.

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.

Step 17 Click **Next**.

The Authentication Settings step appears in the Cisco DCNM installer window.

Choose the authentication method that the Cisco DCNM server should use to authenticate users who log into the Cisco DCNM client. You can choose one of the following:

- Local—Cisco DCNM client users will be authenticated by the Cisco DCNM server user accounts only.
- RADIUS—Cisco DCNM client users will be authenticated by a RADIUS server.
- TACACS+—Cisco DCNM client users will be authenticated by a TACACS+ server.

For RADIUS or TACACS+, you can specify up to three servers.

Step 18 If you chose RADIUS or TACACS+, for each server that you want to specify, do the following:

a. In the server address field, type the IPv4 address of the server in dotted-decimal format.

b. In the secret key field, type the shared secret of the server.

c. (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Step 19 Click **Next**.

If you are using Windows Server 2003, the installer asks you to specify a shortcut to the application. If you are using RHEL 4 AS, the installer asks you to specify a link folder.

Step 20 Choose the shortcut or link options that you want.

Step 21 (Optional) If you want the installer to create the shortcuts for all users who can log into the server system, check the **Create Icons for All Users** check box.

Step 22 Click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window.

Step 23 Carefully review the summary of your choices. If you need to change anything, click **Previous** until the the Cisco DCNM installer window displays the step that you need to change.

Step 24 When you are ready to install the Cisco DCNM server software, click **Next**.

The installer installs the Cisco DCNM server software.

The Start DCNM Server dialog box appears.

Step 25 Choose whether you want to start the Cisco DCNM server now. If you start the Cisco DCNM server now, a splash screen appears while the server starts.

The Install Complete step appears in the Cisco DCNM installer window, which also shows a Cisco DCNM instance ID number.

Step 26 (Optional) If you plan to install a license for Cisco DCNM, record the instance ID number. The licensing process requires that you enter that number.

Note You can begin using Cisco DCNM without a licence but some features are not available unless you purchase and install a license and apply the license to managed devices that you want to use licensed features with.

Step 27 Click **Done**.

If you chose in Step 25 to start the Cisco DCNM server after installation, a splash screen appears while the server starts.

Step 28 (Optional) If you need to start the Cisco DCNM server, see the "Starting the Cisco DCNM Server" section on page 2-9.

Step 29 (Optional) If you want to install a Cisco DCNM license, see the "Installing Licenses" section on page 2-11.

Starting the Cisco DCNM Server

You can manually start the Cisco DCNM server. The manual procedures for starting the Cisco DCNM server differ for systems using the Windows Server 2003 and RHEL 4 AS operating systems, as described in the following topics:

- Starting the Cisco DCNM Server (Windows Server 2003), page 2-10
- Starting the Cisco DCNM Server (RHEL 4 AS), page 2-10

Starting the Cisco DCNM Server (Windows Server 2003)

On a server system running Windows Server 2003, you can start the Cisco DCNM server through the Windows services or by clicking the Start Cisco DCNM Server icon.

BEFORE YOU BEGIN

You must have installed the Cisco DCNM server (see the "Installing the Cisco DCNM Server" section on page 2-5).

DETAILED STEPS

To manually launch the Cisco DCNM server on a system running the Windows Server 2003 operating system, follow these 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 the Cisco DCNM Server (RHEL 4 AS)

You can start the Cisco DCNM server on a RHEL 4 AS server system by using the **Start_DCNM_Server** command.

BEFORE YOU BEGIN

The Cisco DCNM server must be installed (see the "Installing the Cisco DCNM Server" section on page 2-5).

DETAILED STEPS

To manually launch the Cisco DCNM server on a system running the RHEL 4 AS operating system, follow this step:

Step 1 Use the Start_Cisco DCNM_Server script to start the Cisco DCNM server.

```
sh Start_DCNM_Server
```

You can find this script in your home folder or the folder that you specified when setting up the link folder during your installation of Cisco DCNM.

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.

Installing Licenses

To use the licensed Cisco DCNM server features, you must purchase and install Cisco DCNM Enterprise LAN licenses for each managed device that works with those features. To purchase a license, submit the Cisco DCNM Instance ID number and the number of devices to license to the Cisco Technical Assistance Team (TAC). TAC will e-mail you the license file that you need for installing the license.

After you install a license, you must specify which managed devices that it applies to. For more information, see Chapter 8, "Administering DCNM Licensed Devices".

BEFORE YOU BEGIN

You must have installed the Cisco DCNM server.

Ensure that there are no executable files in the folder where you plan to install the licenses file.

DETAILED STEPS

To install the Cisco DCNM Enterprise LAN license, follow these steps:

Step 1 Copy the Cisco DCNM Instance ID number by doing one of the following:

- When you finish installing the server, copy the number when it is displayed at the end of the Cisco DCNM installation process.
- When running the Cisco DCNM client, choose **Help > Show DCNM Instance ID**.

Step 2 Contact TAC and purchase one or more Cisco DCNM licenses. Present the Cisco DCNM Instance ID number and specify the number of devices that you want to license.

TAC will send you a license pack file that you can use for each installation that you ordered.

Step 3 Log into the server system that runs the Cisco DCNM server.

Step 4 Download the license pack file into a directory on the server system.

Caution Make sure that there are no other executable files in the directory where you download the license pack file. Having other files in the directory where you download the license pack file can disrupt the installation of the licenses.

Step 5 Go to the directory where you downloaded the Cisco DCNM server software and run one of the following files:

- For Windows Server 2003, run the dcnm-k9.*release*.exe file.
- For RHEL 4 AS, use the following **sh** command:

```
sh dcnm-k9.release.bin
```

When the Cisco DCNM installer starts, a warning dialog box indicates that the existing installation of the Cisco DCNM server was found.

Step 6 Click **OK**.

The Reinstall step appears in the Cisco DCNM installer window.

Step 7 Choose **License Install** and click **Next**.

The Choose DCNM License Folder step appears in the Cisco DCNM installer window.

Step 8 In the Please Choose a Folder field, type or choose the folder that contains the license file, and then click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window. The License files(s) field shows the licenses that the Cisco DCNM installer found in the folder that you specified.

Step 9 Click **Next**.

The Installation Complete step appears in the Cisco DCNM installer window.

Step 10 Click **Done**.

You can now specify the managed devices that you want to use licensed Cisco DCNM features with. For more information, see Chapter 8, "Administering DCNM Licensed Devices."

Upgrading the Cisco DCNM Server

You can upgrade the DNCM server. The upgrade process requires that you stop the Cisco DCNM server before you begin the upgrade.

Note Data migration is not supported if you are upgrading to Cisco DCNM Release 4.2 from any release prior to Release 4.2. The Release 4.2 installer includes the option to back up the database prior to cleaning the database during the upgrade.

BEFORE YOU BEGIN

Ensure that the server system satisfies the prerequisites. For more information, see the "Prerequisites for Installing the Cisco DCNM Server" section on page 2-2.

Download the updated Cisco DCNM server software by following the procedure listed in the "Downloading the Cisco DCNM Server Software" section on page 2-4.

Stop the Cisco DCNM server. The upgrade cannot proceed until you stop the Cisco DCNM server. For more information, see the applicable topic:

- Stopping the Cisco DCNM Server (Windows Server 2003), page 2-20
- Stopping the Cisco DCNM Server (RHEL 4 AS), page 2-20

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that may interfere with the installation of the Cisco DCNM server software. After you have completed the installation, reenable the software or features.

DETAILED STEPS

To upgrade the Cisco DCNM server software, follow these steps:

Step 1 Log into the server with a user account that has the required privileges, as follows:

- For Windows Server 2003, the user account must be a member of the local administrators group.
- For RHEL 4 AS, the user account must be root.

If you are installing Cisco DCNM on Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM server system.

Step 2 If you have not already done so, stop the Cisco DCNM server.

Step 3 Go to the directory where you downloaded the updated Cisco DCNM server software and run one of the following files:

- For Windows Server 2003, run the dcnm-k9.*release*.exe file.
- For RHEL 4 AS, use the following **sh** command:

  ```
  sh dcnm-k9.release.bin
  ```

When the Cisco DCNM installer starts, a warning dialog box indicates that the existing installation of the Cisco DCNM server was found.

Step 4 Click **OK**.

If the Choose PostgreSQL Folder step appears in the Cisco DCNM installer window, the installer could not locate the PostgreSQL database files.

Step 5 If the Choose PostgreSQL Folder step appears, type or choose the path to the folder that contains the PostgreSQL database files and then click **Next**.

The Database Options step appears in the Cisco DCNM installer window.

Step 6 Specify the database administrator username and password. To do so, follow these steps:

a. In the DB Admin User field, follow these guidelines:

- If you are upgrading from a release of Cisco DCNM earlier than Cisco DCNM Release 4.2(1), type the username for a new database administrator account. The installer will create the administrator account that you specify.
- If you are upgrading from Cisco DCNM Release 4.2(1) or a later release, type the username of the existing database administrator account.

b. In the DB Admin Password field, type the password for the database administrator username that you specified.

c. Click **Next**.

The Local User Credentials step appears in the Cisco DCNM installer window.

Step 7 In the Local Admin Username field, type a name for a Cisco DCNM server user. The installer will create the Cisco DCNM server user and assign the Administrator role to it.

Step 8 In the Password field, type a password for the user, and then in the Confirm Password field, type the password again.

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.

Step 9 Click **Next**.

The Authentication Settings step appears in the Cisco DCNM installer window.

Choose the authentication method that the Cisco DCNM server should use to authenticate users who log into the Cisco DCNM client. You can choose one of the following:

- Local—Cisco DCNM client users will be authenticated by the Cisco DCNM server user accounts only.
- RADIUS—Cisco DCNM client users will be authenticated by a RADIUS server.
- TACACS+—Cisco DCNM client users will be authenticated by a TACACS+ server.

For RADIUS or TACACS+, you can specify up to three servers.

Step 10 If you chose RADIUS or TACACS+, for each server that you want to specify, do the following:

a. In the server address field, type the IPv4 address of the server in dotted-decimal format.

b. In the secret key field, type the shared secret of the server.

c. (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Step 11 Click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window.

Step 12 Carefully review the summary of your choices. If you need to change anything, click **Previous** until the the Cisco DCNM installer window displays the step that you need to change.

Step 13 When you are ready to install the Cisco DCNM server software, click **Next**.

If you are upgrading from a release prior to Release 4.2(0), the DB Migration dialog box appears.

Note Upgrading Cisco DCNM from a release prior to Release 4.2(0) is not supported.

Step 14 If the DB Migration dialog box appears, choose whether you want the installer to back up the database.

If you are upgrading from a release prior to Release 4.2(0), the installer backs up the database if you chose to do so. The installer then clears all data from the database.

If you are upgrading from Release 4.2 to a later version of Release 4.2, the installer migrates the database from the previous installation to the new installation.

After database migration is complete, the installer installs but does not start the Cisco DCNM server software.

The Install Complete step appears in the Cisco DCNM installer window, which also shows a Cisco DCNM instance ID number.

Step 15 Click **Done**.

The Cisco DCNM server is not running.

Step 16 If you need to start the Cisco DCNM server, do one of the following:

- If you are using Windows Server 2003, see the "Starting the Cisco DCNM Server (Windows Server 2003)" section on page 2-10.

- If you are using RHEL 4 AS, see the "Starting the Cisco DCNM Server (RHEL 4 AS)" section on page 2-10.

Downgrading the Cisco DCNM Server

The Cisco DCNM installer does not support downgrading to earlier releases.

To downgrade the Cisco DCNM server, follow these steps:

Step 1 Uninstall the Cisco DCNM server that you want to downgrade from.

Step 2 Install and deploy the earlier release of the Cisco DCNM server that you want to downgrade to. For more information, see the "Deploying Cisco DCNM" section on page 1-4.

Reinstalling the Cisco DCNM Server

You can reinstall the Cisco DCNM server and the download service for the Cisco DCNM client. When you reinstall the Cisco DCNM server, you must choose one of the following types of reinstallation:

- Custom—Reinstalls the components that you select, without allowing you to change anything that you specified when you previously installed the Cisco DCNM server. Choose this reinstallation type when you want to do any of the following:
  - Reinstall the Cisco DCNM server without changing database or configuration options.
  - Reinstall the Cisco DCNM client download service.
  - Reinstall the Cisco DCNM license, either from the same folder that previously contained the Cisco DCNM license file or from a different folder.
- Full Reinstall—Reinstalls the Cisco DCNM server and the Cisco DCNM client download service. Choose this reinstallation type when you want to do any of the following:
  - Perform password recovery for the local administrator account.
  - Change Cisco DCNM server authentication settings.
  - Create a PostgreSQL installation.
  - Change the database URL, database username, or database password for the existing PostgreSQL installation.
  - Change the Cisco DCNM server IP address.

    Note If you are using RHEL 4 AS and you change the Cisco DCNM server IP address, you must also manually change the IP address in the `INSTALL_DIR/bin/stopDCNM.sh` script.

  - Change the port that the Cisco DCNM web server listens to.

Note If you change the web server port number, it affects the URL that Cisco DCNM users use to download the Cisco DCNM client.

– Change the port that the Cisco DCNM server accepts Cisco DCNM client connections on.

Note If you change the Cisco DCNM server port number, it affects the port that Cisco DCNM users specify when they log into the Cisco DCNM client.

Neither reinstallation type allows you to change the installation folder or archive folder.

BEFORE YOU BEGIN

Stop the Cisco DCNM server. The upgrade cannot proceed until you stop the Cisco DCNM server. For more information, see the applicable topic:

- Stopping the Cisco DCNM Server (Windows Server 2003), page 2-20
- Stopping the Cisco DCNM Server (RHEL 4 AS), page 2-20

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that may interfere with the installation of the Cisco DCNM server software. After you have completed the installation, reenable the software or features.

DETAILED STEPS

To reinstall the Cisco DCNM server, set up a web start copy of the Cisco DCNM client, or do both, follow these steps:

Step 1 Log into the server with a user account that has the required privileges, as follows:

- For Windows Server 2003, the user account must be a member of the local administrators group.
- For RHEL 4 AS, the user account must be root.

If you are installing Cisco DCNM on Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM server system.

Step 2 If you have not already done so, stop the Cisco DCNM server.

Step 3 Go to the directory that contains the Cisco DCNM installer software and run one of the following files:

- For Windows Server 2003, run the dcnm-k9.*release*.exe file.
- For RHEL 4 AS, use the following **sh** command:

```
sh dcnm-k9.release.bin
```

When the Cisco DCNM installer starts, a warning dialog box indicates that the existing installation of the Cisco DCNM server was found.

Step 4 Click **OK**.

The Reinstall step appears in the Cisco DCNM installer window.

Step 5 Choose the type of reinstallation that you to perform by doing one of the following:

- If you want to reinstall both the Cisco DCNM server and the Cisco DCNM client download service, click **Full Reinstall**.
- If you want to reinstall only the Cisco DCNM server or only the Cisco DCNM client download service, click **Custom**.

Step 6 If you chose Custom, follow these steps:

a. Click **Next**.

The Reinstall Cisco DCNM step appears in the Cisco DCNM installer window. Under Install Set, check boxes for the components that you can reinstall appear.

b. Check the check boxes for the components that you want to reinstall and click **Next**.

If you chose the License component, the Choose DCNM License Folder step appears in the Cisco DCNM installer window.

c. If the Choose DCNM License Folder step appears, type or choose the path to the folder that contains the Cisco DCNM license file, and then click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window.

d. Skip to Step 25.

Step 7 If you chose Full Reinstall, click **Next**.

The Database Options step appears in the Cisco DCNM installer window. You can use the existing PostgreSQL installation or you can use the Cisco DCNM installer to add a PostgreSQL installation.

Step 8 Next to RDBMS, click the option for the existing database that you want to use.

If the Cisco DCNM installer detected the existing database installation, the DB URL field shows the URL to the database.

Note If the Cisco DCNM installer detects that the existing installation of Cisco DCNM shares a database system with an installation of Cisco Fabric Manager Release 4.2(1) and later releases, the DB URL field shows the URL of the Fabric Manager database and cannot be configured.

Step 9 If the DB URL field does not have the correct URL to the Cisco DCNM database, type the correct URL. If you previously used the Cisco DCNM installer to create a PostgreSQL installation, the URL is typically as follows:

```
jdbc:postgresql://localhost:5432/dcnmdb
```

where 5432 is the default PostgreSQL server port number and dcnmdb is the default database name that the Cisco DCNM installer creates.

If you previously used a Oracle 10g database installation, the URL is typically as follows:

```
jdbc:oracle:thin:@localhost:1521:XE
```

where 1521 is the default Oracle server port number.

If you previously used a Oracle 11g database installation, the URL is typically as follows:

```
jdbc:oracle:thin:@localhost:1521:ORCL
```

where 1521 is the default Oracle server port number.

Step 10 In the DB Admin User field, type the username of a database user account that has administrator permissions in the database.

Step 11 In the DB Admin Password field, type the password for the database administrator username that you specified.

Step 12 In the DCNM DB User field, type the username that Cisco DCNM should use to access the database.

Step 13 In the DCNM DB Password field, type the password for the database user account that you specified.

Step 14 In the Confirm DCNM DB Password field, retype the password for the database user account that you specified.

Step 15 Click **Next**.

The Configuration Options step appears in the Cisco DCNM installer window.

Step 16 From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently assigned to network interfaces on the server system.

Note The IP address of the server system should be statically assigned. The Cisco DCNM server binds to the IP address that you specify. If the IP address of the server system changes after you install the Cisco DCNM server, Cisco DCNM clients are unable to connect to the Cisco DCNM server and you must stop and reinstall the Cisco DCNM server so that you can reconfigure the IP address.

Step 17 If you want to change the port that the Cisco DCNM web server listens to, enter the new port number in the Web Server Port box. By default, the Cisco DCNM web server listens to TCP port 8080.

Note If you change the web server port number, it affects the URL that Cisco DCNM users use to download the Cisco DCNM client.

Step 18 If you want to change the port that the Cisco DCNM server accepts Cisco DCNM client connections on, enter the new port number in the Naming Service Port box. By default, the Cisco DCNM server accepts connections from Cisco DCNM clients on TCP port 1099.

Note If you change the Cisco DCNM server port number, it affects the port that Cisco DCNM users specify when they log into the Cisco DCNM client.

Step 19 Click **Next**.

The Local User Credentials step appears in the Cisco DCNM installer window.

Step 20 In the Local Admin Username field, type a name for a Cisco DCNM server user. The installer will create the Cisco DCNM server user and assign the Administrator role to it.

Step 21 In the Password field, type a password for the user, and then in the Confirm Password field, type the password again.

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.

Step 22 Click **Next**.

The Authentication Settings step appears in the Cisco DCNM installer window.

Choose the authentication method that the Cisco DCNM server should use to authenticate users who log into the Cisco DCNM client. You can choose one of the following:

- Local—Cisco DCNM client users will be authenticated by the Cisco DCNM server user accounts only.
- RADIUS—Cisco DCNM client users will be authenticated by a RADIUS server.
- TACACS+—Cisco DCNM client users will be authenticated by a TACACS+ server.

For RADIUS or TACACS+, you can specify up to three servers.

Step 23 If you chose RADIUS or TACACS+, for each server that you want to specify, do the following:

a. In the server address field, type the IPv4 address of the server in dotted-decimal format.

b. In the secret key field, type the shared secret of the server.

c. (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Step 24 Click **Next**.

Step 25 Carefully review the summary of your choices. If you need to change anything, click **Previous** and return to the applicable step, above.

Step 26 When you are ready to install the Cisco DCNM server software, click **Next**.

The installer installs the Cisco DCNM server software.

The Start DCNM Server dialog box appears.

Step 27 Choose whether you want to start the Cisco DCNM server now. If you start the Cisco DCNM server now, a splash screen appears while the server starts.

The Install Complete step appears in the Cisco DCNM installer window.

Step 28 Click **Done**.

Step 29 If you need to start the Cisco DCNM server, see the "Starting the Cisco DCNM Server" section on page 2-9.

Step 30 (RHEL 4 AS only) If you are using RHEL 4 AS and you changed the Cisco DCNM server IP address during the reinstallation, open the `INSTALL_DIR/bin/stopDCNM.sh` script in a text editor and change the IP address to the new Cisco DCNM server IP address.

Stopping the Cisco DCNM Server

You can manually stop the Cisco DCNM server. The manual procedures for stopping the Cisco DCNM server differ for systems using the Windows Server 2003 and RHEL 4 AS operating systems, as described in the following topics:

- Stopping the Cisco DCNM Server (Windows Server 2003), page 2-20
- Stopping the Cisco DCNM Server (RHEL 4 AS), page 2-20

Stopping the Cisco DCNM Server (Windows Server 2003)

On a server system running Windows Server 2003, you can stop the Cisco DCNM server through the Windows services or by clicking the Stop DCNM Server icon.

DETAILED STEPS

To manually stop the Cisco DCNM server on a system running the Windows Server 2003 operating system, follow these 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 the Cisco DCNM Server (RHEL 4 AS)

On a server system running RHEL 4 AS, you can stop the Cisco DCNM server with the **Stop_DCNM_Server** command.

DETAILED STEPS

To manually stop the Cisco DCNM server on a system running the RHEL 4 AS operating system, follow this step:

Step 1 Use the Stop_Cisco DCNM_Server script to stop the server on a RHEL operating system.

```
sh Stop_DCNM_Server
```

You can find this script in your home folder or the folder that you specified when setting up the link folder during your installation of Cisco DCNM.

The Cisco DCNM server opens a server console window and displays the processes that it runs to start the server. The server is running when you see a “Stopped at *X*m:*XX*s:*XXX*ms” message.

Additional References

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

- Related Documents, page 2-21
- Standards, page 2-21

Related Documents

Related Topic	Document Title
Overview of the Cisco DCNM environment	Information About Cisco DCNM, page 1-1
The process of deploying Cisco DCNM in your organization	Deploying Cisco DCNM, page 1-4

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 Installing and Launching the Cisco DCNM Server

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

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

Feature Name	Releases	Feature Information
Support for shared server system with Cisco Fabric Manager Release 4.2(1) and later releases.	4.2(1)	This feature was introduced.
Support for Oracle 10g and 11g databases.	4.2(1)	This feature was introduced.
Cisco DCNM server installer	4.2(1)	This feature was preexisting.
Server installer includes a step for configuring the DCNM server IP address, web server listening port, and DCNM server listening port	4.1(2)	This feature was introduced.
Server installer includes a step for choosing an archive folder	4.1(2)	This feature was introduced.
DCNM server installer	4.1(2)	This feature was introduced.

CHAPTER 3

Installing and Launching the Cisco DCNM Client

This chapter describes how to install and launch the Cisco Data Center Network Manager (DCNM) client. The Cisco DCNM client is a web-based application that you install on systems running Microsoft Windows XP Professional. 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.

This chapter includes the following sections:

Prerequisites for Installing and Using the Cisco DCNM Client

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

- Your system must be running the Microsoft Windows XP Professional 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 4.x*.
- Downloading the Cisco DCNM client requires the use of one of the following supported web browsers:
  - Microsoft Internet Explorer 7
  - Mozilla Firefox 3.0
- 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 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.

- Some Cisco DCNM features require a license. Before you can use licensed features, install the Cisco DCNM license. For detailed steps for the license installation, see the "Installing Licenses" section on page 2-11. For more information about licensed features, see the "Cisco DCNM Licensing" section on page 1-3.

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 "Reinstalling the Cisco DCNM Server" section on page 2-15.

Downloading and Launching the Cisco DCNM Client

You can download and launch the Cisco DCNM client from the web server included on the Cisco DCNM server.

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.

DETAILED STEPS

To download and launch the Cisco DCNM client, follow these 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:

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

The browser shows the Cisco DCNM client page.

Step 2 Click **Launch Cisco 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 to 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 Cisco DCNM-supported Java version.

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.

Step 5 In the Cisco DCNM client login window, do the following:

a. In the DCNM Server box, type the hostname or the IP address of the Cisco DCNM server.

By default, the DCNM Server box contains the IP address of the Cisco DCNM server that you downloaded the Cisco DCNM client from.

b. In the Username box, 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 3-2.

c. In the Password box, enter the password for the Cisco DCNM username that you specified.

d. (Optional) If you need to change the Cisco DCNM server port, click **More** and enter the port number in the Port box. 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.

e. Click **Login**.

The Cisco DCNM client opens.

If you are deploying Cisco DCNM for the first time, see the "Deploying Cisco DCNM" section on page 1-4.

For information on how to use the Cisco DCNM client, see Chapter 4, "Using the Cisco DCNM Client."

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 the desktop shortcut or the Start menu command for the Cisco DCNM client.

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.

DETAILED STEPS

To restart the Cisco DCNM client, follow these steps:

Step 1 Click the desktop icon for the Cisco DCNM client or choose **Start > Programs > Cisco DCNM Client > Cisco DCNM Client**.

The Cisco DCNM client login window.

Step 2 In the Cisco DCNM client login window, do the following:

a. In the Cisco DCNM Server box, type the hostname or the IP address of the Cisco DCNM server. By default, this window lists the IP address specified the last time you logged into Cisco DCNM. You can use the host name for the Cisco DCNM server in place of the IP address.

b. In the Username box, enter your Cisco DCNM username.

c. In the Password box, enter your Cisco DCNM password.

d. (Optional) If you need to change the Cisco DCNM server port, click **More** and enter the port number in the Port box. 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.

e. Click **Login**.

The Cisco DCNM client opens. For information on how to use the Cisco DCNM client, see Chapter 4, "Using the Cisco DCNM Client."

Uninstalling the Cisco DCNM Client

You can uninstall the Cisco DCNM client from a computer.

DETAILED STEPS

To uninstall the Cisco DCNM client, follow these 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 3-2.

Additional References

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

Related Documents

Related Topic	Document Title
Installing and launching the Cisco DCNM server	Chapter 2, "Installing and Launching the Cisco DCNM Server"
The process of deploying Cisco DCNM in your organization	Deploying Cisco DCNM, page 1-4

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 Installing and Launching 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
Cisco DCNM client installation	4.2(1)	No change from Release 4.1
Port number in URL for downloading the DCNM client is configurable	4.1(2)	This feature was introduced.
DCNM client installation	4.1(2)	This feature was preexisting.

CHAPTER 4

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

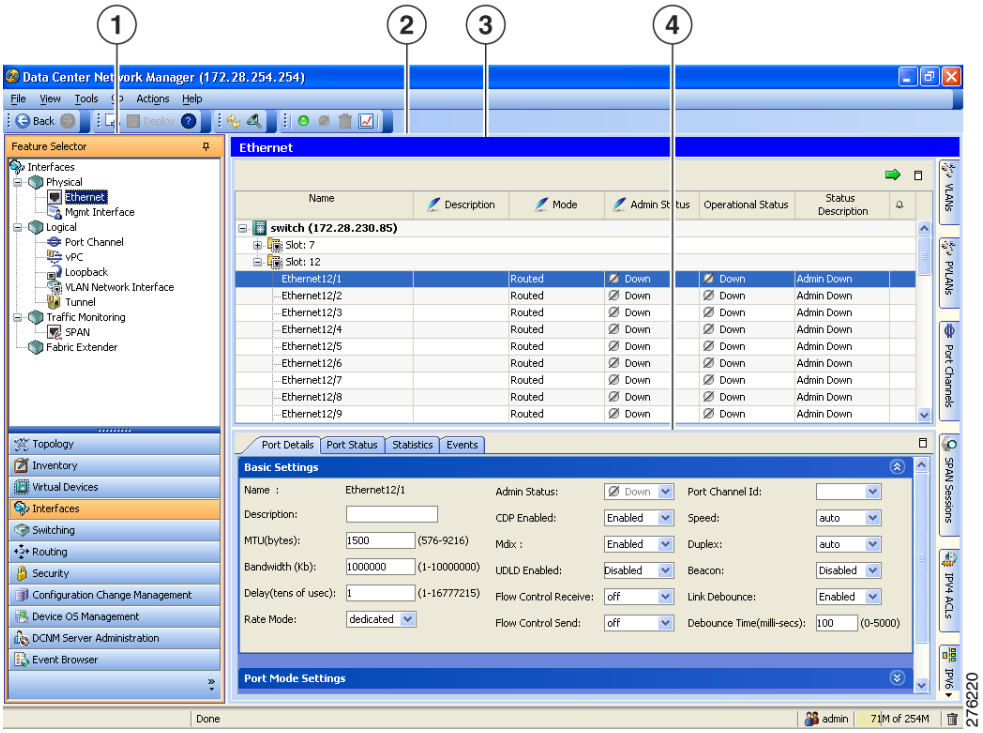
This section describes the Cisco DCNM client and its parts.

This section includes the following topics:

User Interface

The Cisco DCNM client user interface, shown in Figure 4-1, presents device status information and provides configuration tools that allow you to manage devices. It is divided into the panes shown in Figure 4-1. 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 4-1.

Figure 4-1 Cisco DCNM Client User Interface



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

Feature Selector Pane

The Feature Selector pane, shown in Figure 4-1, 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 4-1, 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 4-1, 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 4-1, 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 4-1, 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

Tabs organize related fields and information. For example, as shown in Figure 4-1, 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 4-9.

- Events—You can use this tab to view feature-specific events about the selected object. For more information, see the "Viewing Events on an Events Tab" section on page 10-6.

Sections

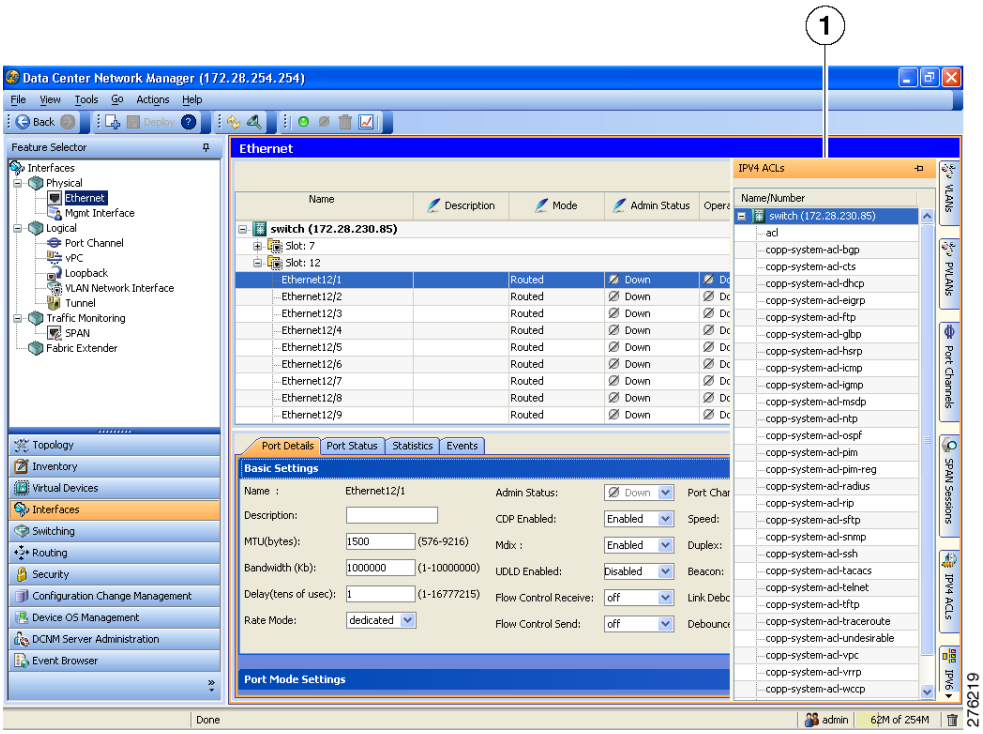
Sections provide further organization of related fields and information. The Cisco DCNM client allows you to expand and collapse sections so that you can show or hide fields and information as needed. For example, as shown in Figure 4-1, on the Port Details tab, the Basic Settings section is expanded 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 4-2 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 4-2, 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 4-2 Association Pane



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 4-6.
- 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 4-14.
- 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.
- Routing—Selects the Routing button on the Feature Selector pane.
- Security—Selects the Security button on the Feature Selector pane.
- DCNM Server Administration—Selects the DCNM Server Administration 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.

- 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 "Installing Licenses" section on page 2-11.
- 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.

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

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 3, "Installing and Launching the Cisco DCNM Client."

DETAILED STEPS

To open the Cisco DCNM client, follow these 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 3, "Installing and Launching the Cisco DCNM Client."

A dialog box displays login fields.

Step 2 In the Cisco 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.

Tip 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.

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 If your Cisco DCNM server uses a port number other than 1099, click **More** and enter the port number for your Cisco DCNM server in the Port field.

Step 6 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 7 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 7-1.

Closing the Cisco DCNM Client

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

DETAILED STEPS

To close the Cisco DCNM client, follow these 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**.

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 4-8.

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:

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 16-1.

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 "Installing Licenses" section on page 2-11.

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

To access a chart, follow these 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. In the Statistics tab, one or more charts may appear.

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

Step 3 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 4 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 4-11.

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

To start statistical monitoring for a chart, follow these 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 4-10.

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

To stop statistical monitoring for a chart, follow these 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 4-10.

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 4-11.

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 4-13.

DETAILED STEPS

To use a chart, follow these steps:

Step 1 Access the chart that you want to use. For more information, see the "Accessing a Chart" section on page 4-10.

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 4-11.

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.
- 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 4-10.

DETAILED STEPS

To use an overview chart, follow these 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 4-10.

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 4-11.

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.

Exporting a Chart

You can export a chart as an 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

To export an image of a chart, follow these steps:

Step 1 Access the chart that you want to use. For more information, see the "Accessing a Chart" section on page 4-10.

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 4-11.

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 4-12.

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 four sections on the Global Preferences are as follows:

- Monitoring—Controls the default frequency of statistical data retrieval from managed devices. For more information, see the "Configuring the Default Frequency of Statistical Data Retrieval" section on page 4-14.
- 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 4-15.
- 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 4-16.

Configuring the Default Frequency of Statistical Data Retrieval

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.

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

To configure the default frequency of statistical data retrieval, follow these 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 From the Default Monitoring Frequency drop-down list, choose the new data retrieval frequency.

Step 3 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

To configure the maximum age of events that the Cisco DCNM client fetches from the server, follow these 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.

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

To configure preprovisioning, follow these 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**.

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 4-17
- Standards, page 4-17

Related Documents

Related Topic	Document Title
Installing and launching the Cisco DCNM client	Chapter 3, “Installing and Launching the Cisco DCNM Client”
Information about using specific Cisco DCNM features	Related Documentation, page xxiii

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 4-1 lists the release history for this feature.

Table 4-1 Feature History for Installing and Launching the Cisco DCNM Client

Feature Name	Releases	Feature Information
Exporting the summary pane	4.2(1)	This feature was introduced.
Deploying changes	4.2(1)	Information was added about automatic deployment and manual deployment.
Go menu	4.1(2)	The Go menu was updated to include following new features: • Device OS Management • Configuration Change Management
Action menu	4.1(2)	The Action menu replaced the feature-specific menus that appeared in Cisco DCNM, Release 4.0.
Global Preferences	4.1(2)	The Administration section on the Global Preferences dialog box was removed. You can configure the polling frequency by using the Auto-Synchronization with Devices feature.

CHAPTER 5

Administering DCNM Authentication Settings

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

This chapter includes the following topics:

Information About Administering 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:

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 5-1, Cisco DCNM supports two user roles.

Table 5-1 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.

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 5-2 shows the supported attribute-value pair values for each Cisco DCNM user role.

Table 5-2 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 a 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. This provides 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, 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 "Reinstalling the Cisco DCNM Server" section on page 2-15.

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 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 7-1.

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 "Installing Licenses" section on page 2-11.

Prerequisites for Administering DCNM Authentication Settings

Administering Cisco DCNM server users has the following prerequisites:

- 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.

Guidelines and Limitations for Administering DCNM Authentication Settings

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

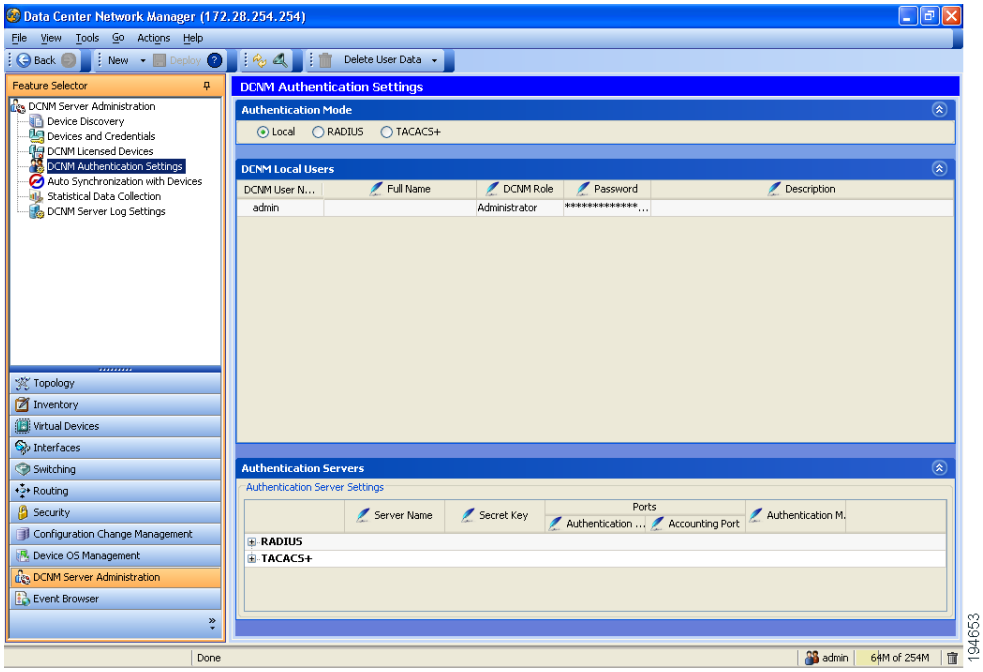
- Create a Cisco DCNM user account for each person who uses the Cisco DCNM client. Do not allow people to share a user account.
- Delete unused Cisco DCNM user accounts.
- Grant an administrator user account only to those who need to perform administrator tasks in the Cisco DCNM client.

- 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

Figure 5-1 shows the DCNM Authentication Settings content pane.

Figure 5-1 DCNM Authentication Settings Content Pane



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

To configure the authentication mode, follow these 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 "Stopping the Cisco DCNM Server" section on page 2-19 and the "Starting the Cisco DCNM Server" section on page 2-9.

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

To add a Cisco DCNM local user, follow these 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 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

To change the password of a Cisco DCNM local user, follow these 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

To change the full name or description of a Cisco DCNM local user, follow these 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 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.

DETAILED STEPS

To delete a Cisco DCNM local user account, follow these 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

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

To add authentication servers, follow these 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 host name.

Note If you enter a host name 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. 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

To change authentication server settings, follow these 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. 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

To remove an authentication server, follow these 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.

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 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 5-13.

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

To verify settings for an authentication server, follow these 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. Verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.

Field Descriptions for DCNM Authentication Settings

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

- Authentication Mode Section, page 5-13
- DCNM Local Users Section, page 5-13
- Authentication Servers Section, page 5-14

Authentication Mode Section

Table 5-3 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.

DCNM Local Users Section

Table 5-4 DCNM Local Users Section

Field	Description
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.

Table 5-4 DCNM Local Users Section (continued)

Field	Description
DCNM Role	Role of the user account. Valid values are User and Administrator. For more information, see Table 5-1. 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.
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 5-5 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 5-15
- Standards, page 5-15

Related Documents

Related Topic	Document Title
Logging into the Cisco DCNM client	*Opening the Cisco DCNM Client, page 4-7*

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 5-6 lists the release history for this feature.

Table 5-6 Feature History for DCNM Authentication Settings

Feature Name	Releases	Feature Information
RADIUS and TACACS+ server support	4.2(1)	This feature was added, including fallback authentication with Cisco DCNM local users when no authentication server for the current authentication mode is reachable.
Cisco DCNM local users	4.2(1)	This feature was preexisting.
DCNM Server Users	4.1(2)	No change from Release 4.0

CHAPTER 6

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:

Device Discovery

The Device Discovery feature creates devices in Cisco DCNM by connecting to a Cisco NX-OS device and retrieving the running configuration of the device. Cisco DCNM can also discover Cisco NX-OS devices 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 virtual device context (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 4.x*.

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 first device (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.

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.

Cisco NX-OS Device Preparation

Before you perform device discovery, you should ensure that the Cisco NX-OS device configuration can support a successful discovery. For more information, see the "Cisco NX-OS Device Configuration Requirements" section on page 1-5.

Virtualization Support

When Cisco DCNM discovers a Cisco NX-OS device that supports VDCs, it determines how many VDC 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 non-default VDCs, ensure that each VDC meets the prerequisites for discovery. For more information, see the "Prerequisites for Device Discovery" section on page 6-3.

Licensing Requirements for Device Discovery

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Device Discovery 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 "Installing Licenses" section on page 2-11.

Prerequisites for Device Discovery

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

- VDCs
- CDP

Device Discovery has the following prerequisites:

- The Cisco DCNM server must be able to reach 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 4.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 "Cisco NX-OS Device Preparation" section on page 6-2.
- 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.

Guidelines and Limitations for Device Discovery

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

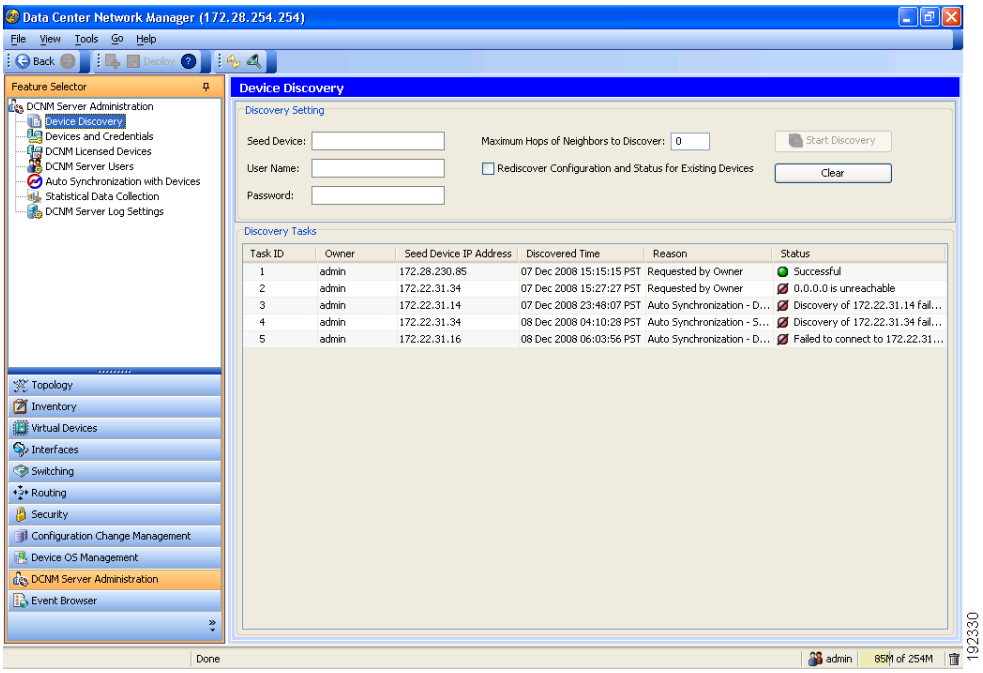
- Ensure that Cisco NX-OS devices that you want to discover have been prepared for discovery. For more information, see the "Cisco NX-OS Device Configuration Requirements" section on page 1-5.
- Cisco DCNM can manage only devices that run Cisco NX-OS. For more information about supported device operating systems and supported device hardware, see the *Cisco DCNM Release Notes, Release 4.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.

Performing Device Discovery

Figure 6-1 shows the Device Discovery content pane.

Figure 6-1 Device Discovery Content Pane



This section includes the following topics:

- Discovering Devices, page 6-4
- Rediscovering Devices, page 6-6

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. For more information, see the "Cisco NX-OS Device Configuration Requirements" section on page 1-5.

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.

DETAILED STEPS

To discover one or more Cisco NX-OS devices, follow these 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 6-4.

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 "Cisco NX-OS Device Preparation" section on page 6-2.

DETAILED STEPS

To rediscover one or more Cisco NX-OS devices, follow these 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 6-7.

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 7-1.

Field Descriptions for Device Discovery

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

Device Discovery Content Pane

Table 6-1 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.

Table 6-1 Device Discovery Content Pane (continued)

Field	Description
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.
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.

Related Fields

For information about fields that configure devices, see the "Administering Devices and Credentials" section on page 7-1.

Additional References for Device Discovery

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

- Related Documents, page 6-8
- Standards, page 6-8

Related Documents

Related Topic	Document Title
Cisco NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide, Release 4.x*

Standards

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

Feature History for Device Discovery

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

Table 6-2 Feature History for Device Discovery

Feature Name	Releases	Feature Information
Device Discovery	4.2(1)	No change from Release 4.1
Device Discovery	4.1(2)	No change from Release 4.0

CHAPTER 7

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.

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 the use of 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. This 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 "Cisco NX-OS Device Preparation" section on page 6-2.
- 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.

Virtualization 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 "Installing Licenses" section on page 2-11.

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 4.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 "Cisco NX-OS Device Preparation" section on page 6-2.

Guidelines and Limitations for Devices and Credentials

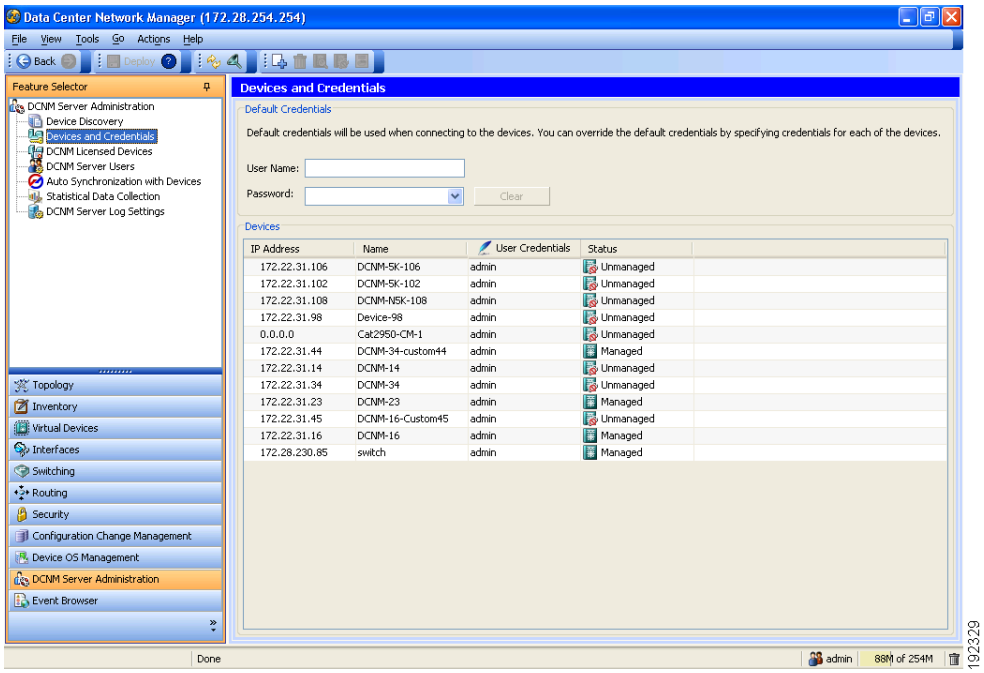
The Devices and Credentials feature has the following configuration guidelines and limitations:

- 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 6-1.
- Be careful when you change the default credentials or device-specific credentials. Incorrect credentials prevent Cisco DCNM from managing devices.

Configuring Devices and Credentials

Figure 7-1 shows the Devices and Credentials content pane.

Figure 7-1 Devices and Credentials Content Pane



This section includes the following topics:

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 7-5.

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.

DETAILED STEPS

To add a device, follow these 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 7-6.

DETAILED STEPS

To discover a device, follow these 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

To change the status of a device to unmanaged, follow these 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.

DETAILED STEPS

To delete a device, follow these 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

To configure default device credentials, follow these 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.

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 7-8.

DETAILED STEPS

To configure default device credentials, follow these 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.

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

To configure unique credentials for a discovered device, follow these 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 7-6.

DETAILED STEPS

To clear unique credentials from a discovered device, follow these 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. For information about the fields that appear, see the "Field Descriptions for Devices and Credentials" section on page 7-10.

Field Descriptions for Devices and Credentials

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

Device and Credentials Content Pane

Table 7-1 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.
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.

Additional References for Devices and Credentials

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

- Related Documents, page 7-11
- Standards, page 7-11

Related Documents

Related Topic	Document Title
Cisco NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide, Release 4.x*

Standards

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

Feature History for Devices and Credentials

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

Table 7-2 Feature History for Devices and Credentials

Feature Name	Releases	Feature Information
Devices and Credentials	4.2(1)	No change from Release 4.1
Devices and Credentials	4.1(2)	No change from Release 4.0

CHAPTER 8

Administering DCNM Licensed Devices

This chapter describes how to use the DCNM Licensed Devices feature.

This chapter includes the following topics:

Information About DCNM Licensed Devices

The DCNM Licensed Devices feature allows you to control which physical devices you can manage with licensed Cisco Data Center Network Manager (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.

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 "Installing Licenses" section on page 2-11.

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 "Installing Licenses" section on page 2-11.
- 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 6-4.

Guidelines and Limitations for Administering DCNM Licensed Devices

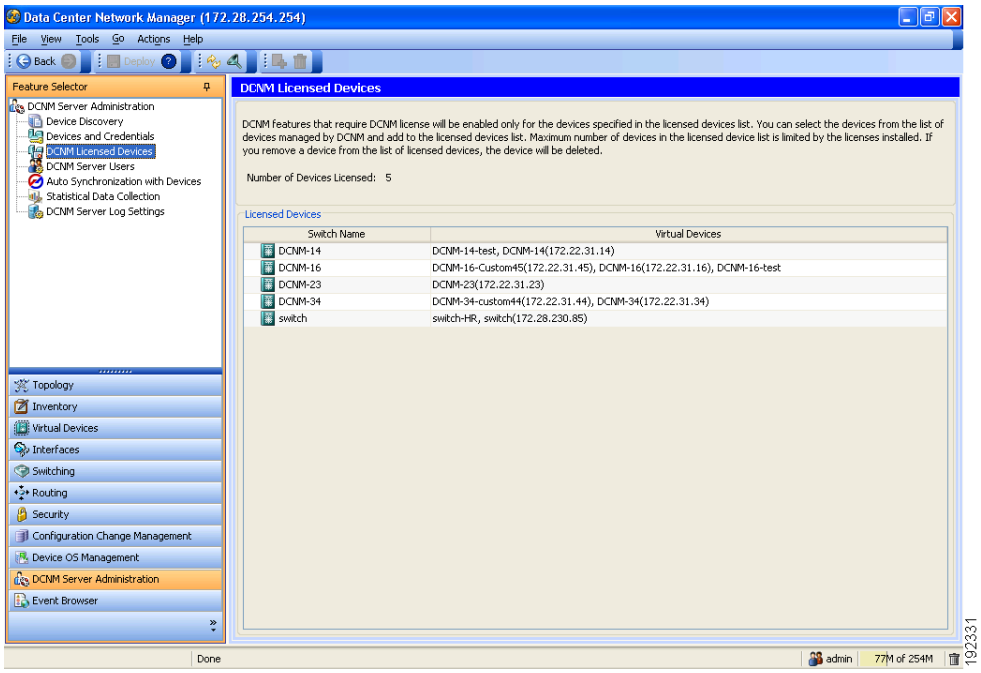
Administering DCNM Licensed Devices has the following configuration guidelines and limitations:

- 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 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 6-4.

Configuring DCNM Licensed Devices

Figure 8-1 shows the DCNM Licensed Devices content pane.

Figure 8-1 DCNM Licensed Devices Content Pane



This section includes the following topics:

- Adding Devices to the Licensed Devices List, page 8-3
- Removing Devices from the Licensed Devices List, page 8-4

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 "Installing Licenses" section on page 2-11.

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 8-4.

DETAILED STEPS

To add a device to the list of licensed devices, follow these 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 6-4.

DETAILED STEPS

To remove devices from the list of licensed devices, follow these 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.

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 6-4.

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 8-5.

Field Descriptions for DCNM Licensed Devices

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

DCNM Licensed Devices Content Pane

Table 8-1 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.

Additional References

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

Related Documents

Related Topic	Document Title
Installing a Cisco DCNM Enterprise LAN license	*Installing Licenses, page 2-11*

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 8-2 lists the release history for this feature.

Table 8-2 Feature History for DCNM Licensed Devices

Feature Name	Releases	Feature Information
DCNM Licensed Devices	4.2(1)	No change from Release 4.1
DCNM Licensed Devices	4.1(2)	No change from Release 4.0

CHAPTER 9

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, that are linked by the Cisco Discovery Protocol (CDP). 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:

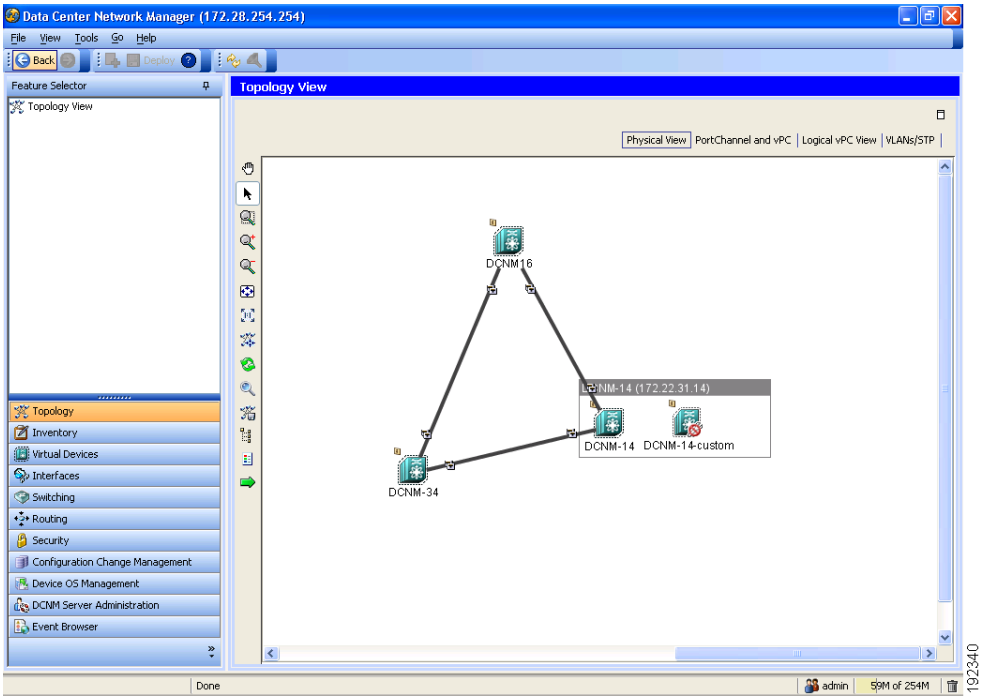
Map Views

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

Physical View

The Physical View (see Figure 9-1) shows the physical connections between discovered devices. This is the default topology view.

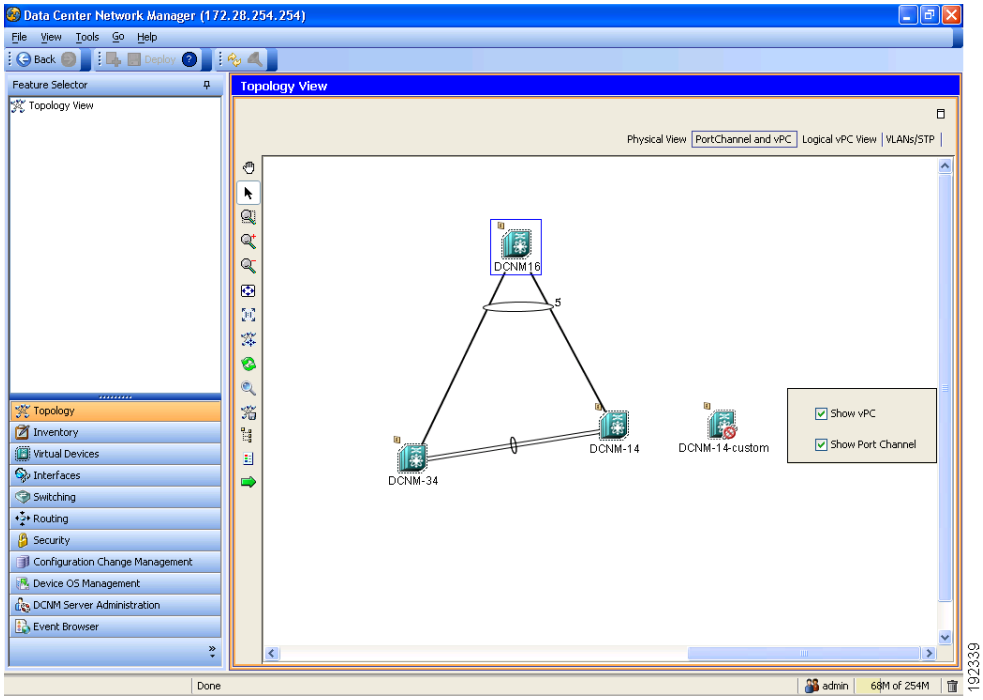
Figure 9-1 Physical View of the Topology Map



PortChannel and vPC

The PortChannel and vPC view (see Figure 9-2) 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.

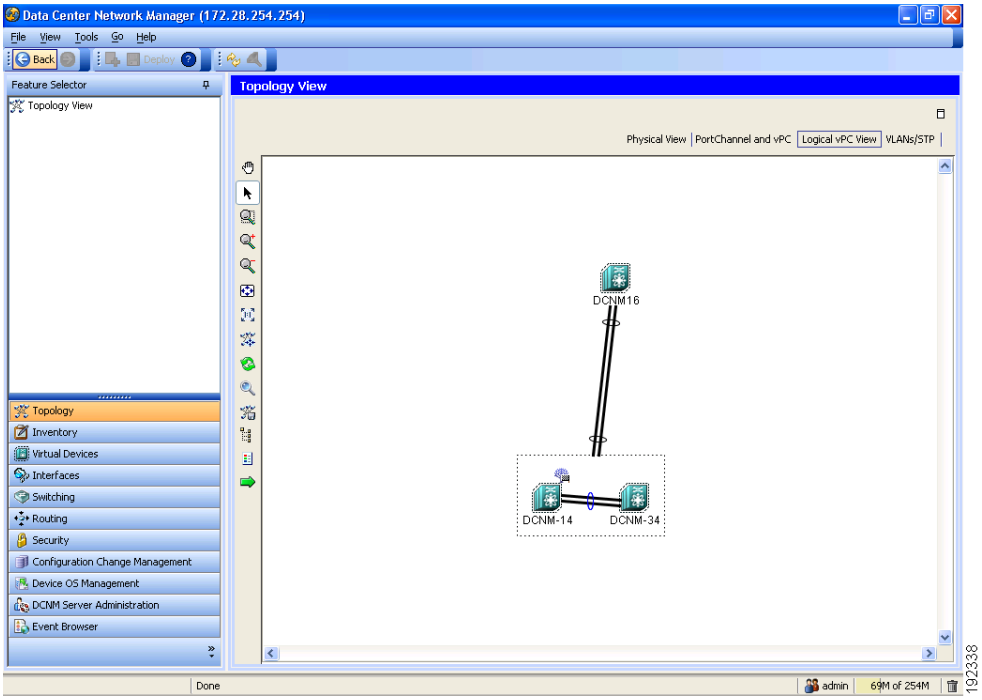
Figure 9-2 PortChannel and vPC View of the Topology Map



Logical vPC View

The Logical vPC View (see Figure 9-3) shows vPC links and vPC peer links among discovered devices, without showing the physical connections.

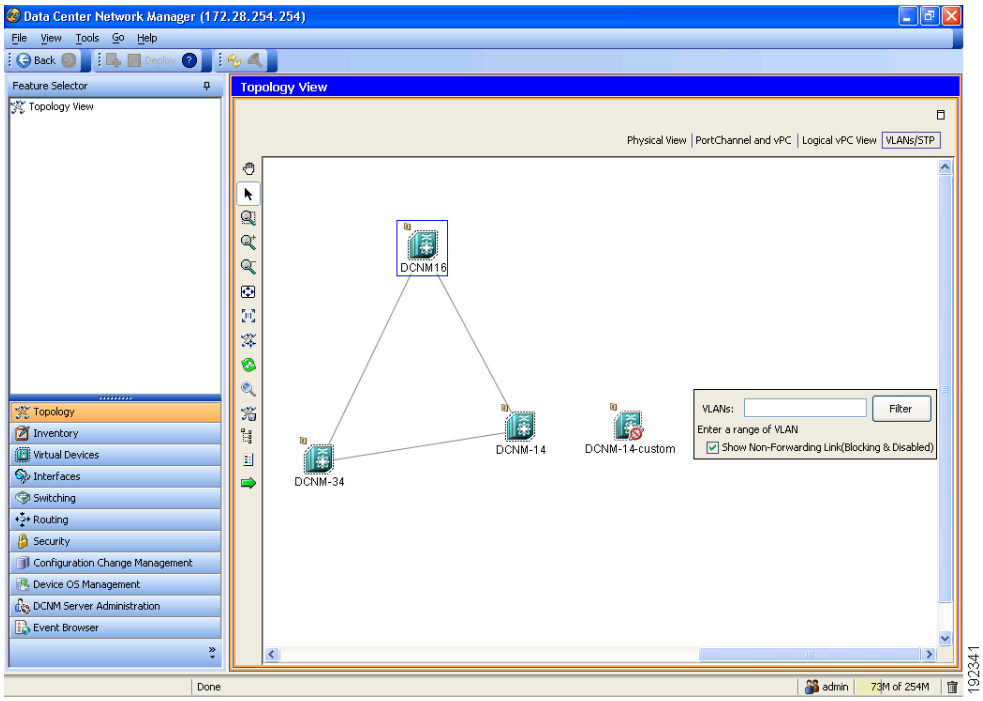
Figure 9-3 Logical vPC View of the Topology Map



VLANs/STP

The VLANs/STP view (see Figure 9-4) shows VLANs configured among discovered devices.

Figure 9-4 VLANs/STP View of the Topology Map



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.

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 9-11.
- 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 9-12.
- 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 9-12.

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 "Installing Licenses" section on page 2-11.

Prerequisites for Topology

Topology has the following prerequisites:

- The topology map shows only devices that Cisco DCNM has discovered.
- On devices shown in the topology map, CDP should be enabled both globally and specifically on interfaces used for 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 Nexus 7000 Series devices that appears 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 15-1.

Using the Topology Feature

This section includes the following topics:

Opening the Topology Map

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

DETAILED STEPS

To view the topology, follow these 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 • VLANs/STP	Right-click in a blank space on 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.
Filter VLANs	• VLANs/STP	1. On the map, find the VLANs box. 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	• VLANs/STP	1. On the map, find the VLANs box. 2. Check or uncheck the **Show Non-Forwarding Link (Blocking & Disabled)** as needed.

View Feature	Available In View	How to Use
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 locate 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

To open the legend, follow these 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.

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	Fit 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.
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.
Legend	Opens the Legend dialog box. See the "Understanding Device Icons and Links" section on page 9-8.

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

To show, hide, or use the Details pane, follow these 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 • VLANs/STP	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.
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.

Section	Available In	How to Use
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.

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

To launch the vPC wizard, 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 **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 4.x*.

Managing a vPC

From the topology map, you can access the vPC feature for a specific vPC link.

DETAILED STEPS

To manage a vPC, 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 one of the following views:

- **PortChannel and vPC**
- **Logical vPC View**

Step 3 Locate the vPC link for the vPC that you want to manage.

Step 4 Use the step that applies to the view that you selected:

- 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 4.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

To find and resolve vPC configuration inconsistencies, 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 one of the following views:

- **PortChannel and vPC**
- **Logical vPC View**

Step 3 Locate 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 4.x*.

Accessing Other Cisco DCNM Features from the Topology Map

You can use the topology map to access other 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

To access a 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. 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.

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.

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 9-15.

The saved layout becomes the default layout that you see in the topology map when you start the Cisco DCNM client.

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

To move devices in 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. 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 9-8.

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 9-15.

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

To load a topology layout in Physical View, follow these 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

To reload the most recent saved topology layout, follow these 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.

Exporting the Topology as a JPG Image

You can export, or save, a JPG image of the topology map. The JPG image created shows only the portion of the topology that appears in the Cisco DCNM client at the moment that you save the JPG file.

DETAILED STEPS

To export the visible portion of the topology map as a JPG image, follow these 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 9-8.

Step 3 Arrange the device icons as desired. For more information, see the "Moving Devices in the Topology Map" section on page 9-14.

Step 4 From the topology toolbar, click the icon.

A dialog box appears.

Step 5 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.

Related Documents

For additional information related to implementing Topology, see the following sections:

Related Topic	Document Title
VDCs	*Cisco DCNM Virtual Device Context Configuration Guide, Release 4.x*

Related Topic	Document Title
vPCs	*Cisco DCNM Interfaces Configuration Guide, Release 4.x*
Device discovery	Administering Device Discovery, page 6-1

Feature History for Topology

Table 9-1 lists the release history for this feature.

Table 9-1 Feature History for Topology

Feature Name	Releases	Feature Information
Topology	4.2(1)	Support for hierarchical and grid layouts was removed.
vPC support	4.1(2)	This feature was added to the topology map.
Multiple views	4.1(2)	This feature was added to the topology map.
Topology	4.1(2)	This feature was preexisting.

CHAPTER 10

Managing Events

This chapter describes how to use the Event Browser and feature-specific Events tabs in Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Events

Cisco DCNM allows you to view and manage recent status events. An event can be either of the following:

- A status-related system message that Cisco DCNM retrieves from managed devices. For more information, see the "Logfile Requirements" section on page 1-7.
- A message generated by the Cisco DCNM server.

The Cisco DCNM client includes the Event Browser and feature-specific Events tabs that appears in the Details pane for features that can have events. The Event Browser shows all recent status events while a feature-specific Events tab shows recent status events that pertain to the feature. The Cisco DCNM client updates the Event Browser and Events tabs dynamically when it receives new events from the server.

In the Event Browser and on Events tabs, you can change the status of an event, add notes to an event, or delete an event.

In addition, the Event Browser provides a pie chart and a bar chart of events separated by the event severity. You can also delete individual events from the events database.

To control the minimum severity of event messages, you configure the logging level for Cisco NX-OS features and for Cisco DCNM server features. For more information, see the "Cisco NX-OS System-Message Logging Requirements" section on page 1-6.

Note Cisco DCNM has minimum logging level requirements for managed Cisco NX-OS devices. Logging levels on a managed device should never be lower than the minimum requirements.

For more information about Cisco DCNM server logging levels, see Chapter 17, "Administering DCNM Server Log Settings."

Note Configuring Cisco DCNM server log settings does not affect logging levels on managed Cisco NX-OS devices.

Licensing Requirements for the Event Browser

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	The Event Browser 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 "Installing Licenses" section on page 2-11.

Prerequisites for Events

The Event Browser has the following prerequisites:

- You should be familiar with Cisco NX-OS system messages.
- Managed Cisco NX-OS devices must be configured to send system messages to the Cisco DCNM server.

Guidelines and Limitations

The Event Browser has the following configuration guidelines and limitations:

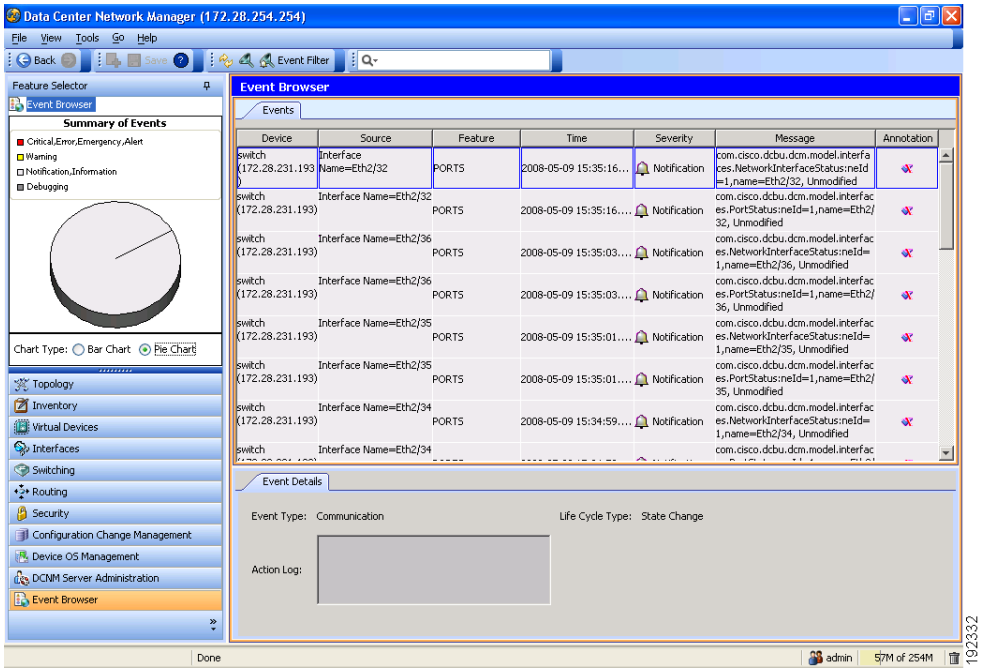
- The Event Browser and feature-specific Events tabs display only status events, which are events generated when the status of a feature or object changes. For example, configuration events do not appear in the Event Browser or on an Events tab.
- The Event Browser can display event messages that are no older than 24 hours when you start the Cisco DCNM client. By default, the Cisco DCNM client fetches from the server messages that are no older than 1 hour.
- The Event Browser can display up to 2000 events. The events database is limited by the amount of space available to the database.
- You cannot use Cisco DCNM to control the logging levels of managed Cisco NX-OS devices. For more information, see the "Cisco NX-OS System-Message Logging Requirements" section on page 1-6.

- We recommend that you delete events that you no longer need or that you have resolved. For information about deleting old events from the events database, see the "Deleting Data from the Events Database" section on page 15-6.

Using the Event Browser and Events Tabs

Figure 10-1 shows the Event Browser content pane.

Figure 10-1 Event Browser Content Pane



This section includes the following topics:

- Viewing the Event Browser, page 10-3
- Applying and Removing an Event Filter, page 10-5
- Viewing Events on an Events Tab, page 10-6
- Changing the Status of an Event, page 10-7
- Adding a Note to One or More Events, page 10-8
- Deleting an Event, page 10-8

Viewing the Event Browser

You can use the Event Browser to view recent events and a summary chart of those events. By default, the Event Browser shows events that occurred up to 1 hour prior to starting the Cisco DCNM client. For more information, see the "Configuring the Maximum Age of Events Fetched from the Server" section on page 4-15.

DETAILED STEPS

To view the Event Browser, follow these steps:

Step 1 From the Feature Selector pane, choose **Event Browser**.

The event table appears in the Contents pane. A summary chart appears above the Feature Selector pane.

Step 2 (Optional) If you want to change the summary chart that appears, above the Feature Selector, choose one of the following Chart Type options, as needed:

- Bar Chart
- Pie Chart

The colors of the chart correspond to event severity levels, as indicated in the legend that appears above the chart.

Step 3 (Optional) If you want to sort or filter events, you can use one or more of the filtering features as described in the following table:

Event Sorting and Filtering Feature	How to Use
Alphabetical sorting by column	Click the column heading to cycle through the sorting options, as follows: • First click—Events are sorted by ascending alphabetical order for the values in the column. • Second click—Events are sorted by descending alphabetical order for the values in the column. • Third click—Events are not sorted by the values in the column.
Event Filter	See the "Applying and Removing an Event Filter" section on page 10-5.
Filter by Column Values	1. From the menu bar, choose **View > Filter**. The column headings become drop-down lists. 2. From each column heading list that you want to use to filter events, choose the value that events appearing in the Event Browser must include.
Filter by text	In the Event Browser toolbar, enter the text that you want to use to filter the events. The Event Browser shows only the events that contain the text that you enter. **Tip** To configure quick filtering options, use the drop-down list of the Event Browser toolbar.

Step 4 (Optional) If you want to view details about a specific event, follow these steps:

a. Find the event in the event list.

b. Click the event.

c. Expand the Details pane, if necessary.

Details about the selected event appear in the Details pane.

d. (Optional) To read notes and messages about status changes to the event, read the information in the Action Log field.

Applying and Removing an Event Filter

You can filter events in the Event Browser by the following criteria:

- Event date and time—By default, the Cisco DCNM client displays all events received after you started the Cisco DCNM client and for a configurable number of hours prior to starting the Cisco DCNM client (for more information, see the "Configuring the Maximum Age of Events Fetched from the Server" section on page 4-15).
- Event severity—By default, the Cisco DCNM client displays events of all severities.

Note When you apply an event filter, the Events tab continues to display events when the Cisco DCNM server receives them. The filter criteria that you select only affect the Filtered Events tab.

BEFORE YOU BEGIN

If the message "Filter Applied" appears at the top of the Contents pane, the Cisco DCNM client is applying an event filter to the Event Browser.

DETAILED STEPS

To apply or remove an event filter in the Event Browser, follow these steps:

Step 1 View events in the Event Browser (see the "Viewing the Event Browser" section on page 10-3).

Step 2 If you want to apply an event filter, follow these steps:

a. From the menu bar, choose **View > Event Filter**.

b. Check the **Apply Filter** check box.

c. Configure the filter criteria.

d. Click **OK**.

A Filtered Events tab appears in the Event Browser. The tab displays the events that match the filtering criteria that you specified. The message "Filter Applied" appears at the top of the Contents pane.

Step 3 If you want to remove an event filter, follow these steps:

a. From the menu bar, choose **View > Event Filter**.

b. Uncheck the **Apply Filter** check box.

c. Click **OK**.

The Filtered Events tab disappears. No message appears at the top of the Contents pane.

Viewing Events on an Events Tab

You can view feature-specific events on the Events tab that appears in the Details pane for a feature. By default, an Events tab shows events received up to 1 hour prior to starting the Cisco DCNM client. For more information, see the "Configuring the Maximum Age of Events Fetched from the Server" section on page 4-15.

BEFORE YOU BEGIN

Typically, the Events tab appears when, in the Summary pane, you select an object that can have events associated with it. For example, if you select Interfaces > Physical > Ethernet from the Feature Selector pane, the Summary pane displays devices. Devices contain slots, and slots contain Ethernet ports. When you select a device, slot, or port, the Details pane displays an Events tab.

What you select in the Summary pane affects which events are shown in the tab. Continuing the Ethernet interface example, the scope of the events in the Events tab depends on what you select, as follows:

- Device—Events that pertain to the selected device, any slot within the device, and any Ethernet interface within the slot.
- Slot—Events that pertain to the selected slot and to any Ethernet interface within the slot.
- Port—Events that pertain to the selected Ethernet interface.

DETAILED STEPS

To view an event on an Events tab, follow these steps:

Step 1 From the Feature Selector pane, choose the feature for which you want to view events.

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

Step 2 From the Summary pane, select an object.

The Events tab appears in the Details pane. In the Events tab, the events table appears.

Note If no Events tab appears, then Cisco DCNM cannot display events for the object you selected.

Step 3 (Optional) If you want to sort or filter events, you can use one or more of the filtering features as described in the following table:

Event Sorting and Filtering Feature	How to Use
Alphabetical sorting by column	Click the column heading to cycle through the sorting options, as follows: • First click—Events are sorted by ascending alphabetical order for the values in the column. • Second click—Events are sorted by descending alphabetical order for the values in the column. • Third click—Events are not sorted by the values in the column.
Filter by Column Values	1. From the menu bar, choose **View > Filter**. The column headings become drop-down lists. 2. From each column heading list that you want to use to filter events, choose the value that events appearing in the Events tab must include.

Step 4 (Optional) If you want to view details about a specific event, follow these steps:

a. Find the event in the event list.

b. Click the event.

c. Expand the Details pane, if necessary.

Details about the selected event appear in the Details pane.

d. (Optional) To read notes and messages about status changes to the event, read the information in the Action Log field.

Changing the Status of an Event

You can change the status of an event to one of the following statuses:

- Acknowledged—Shown as a green check mark.
- Closed—Shown as a yellow folder.

By default, the status of new event is Open, which is indicated in the Annotation column by a green check mark with a red slash across it.

BEFORE YOU BEGIN

Select an event in the Event Browser or on an Events tab for a specific feature. For more information, see the "Viewing the Event Browser" section on page 10-3 or the "Viewing Events on an Events Tab" section on page 10-6.

DETAILED STEPS

Step 1 In the event table, right-click the selected event.

Step 2 Choose **Acknowledge** or **Open**, as needed.

The new status appears in the Annotation column for the selected event.

In the Details pane, the message about the status change appears in the Action Log field.

Adding a Note to One or More Events

You can add a note to one or more events. Notes can contain 1 to 1000 characters.

BEFORE YOU BEGIN

Find the events to which you want to add a note. For more information, see the "Viewing the Event Browser" section on page 10-3 or the "Viewing Events on an Events Tab" section on page 10-6.

DETAILED STEPS

To add a note to one or more events, follow these steps:

Step 1 Select one or more events. Do one of the following:

- To select one event, click the one event that you want to select.
- To select two or more adjacent events, click and drag across the events.
- To select two more events, press and hold **Ctrl** and click each event.

Step 2 On one of the selected events, right-click and then choose **Add Notes**.

The Notes dialog box appears.

Step 3 Enter the note. You can enter up to 1000 case-sensitive, alphanumeric characters.

Step 4 Click **OK**.

The note appears in the Action Log field for each selected event.

Deleting an Event

You can delete one or more events from the Event Browser or a feature-specific Events tab. A deleted event no longer appears in the Event Browser or on a feature-specific Events tab; however, the event remains in the events database.

For information about deleting old events from the events database, see the "Deleting Data from the Events Database" section on page 15-6.

BEFORE YOU BEGIN

Select an event in the Event Browser or on an Events tab for a specific feature. For more information, see the "Viewing the Event Browser" section on page 10-3 or the "Viewing Events on an Events Tab" section on page 10-6.

DETAILED STEPS

Step 1 In the event table, select one or more events that you want to delete.

Note To select more than one event, you can click and drag across the events or you can press and hold **Ctrl** and click each event.

Step 2 Right-click a selected event.

Step 3 Choose **Remove Event**.

The selected events disappear from the Event Browser.

Field Descriptions for Events

This section includes the following field descriptions for Events:

- Events Table, page 10-9
- Event Details, page 10-10

Events Table

The events table appears in the Event Browser and on feature-specific Events tabs.

Table 10-1 Events Table

Field	Description
Device	*Display only.* Name and IP address of the device that the event is related to.
Source	*Display only.* Where the event message originated. Sources are either a feature on a managed Cisco NX-OS device or the Cisco DCNM server.
Feature	*Display only.* Name of the Cisco NX-OS or Cisco DCNM server feature that the event pertains to.
Time	*Display only.* Date and time that the event occurred.
Severity	*Display only.* Severity of the event. Possible severities are as follows: • Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debug
Message	*Display only.* Text of the event.

Table 10-1 Events Table (continued)

Field	Description
Annotation	Status of the event. Possible statuses are as follows: • Open—The default status of an event. You cannot assign an event the status of Open. • Acknowledged • Closed

Event Details

Event details appear below the events table in the Event Browser and on feature-specific Events tabs.

Table 10-2 Event Details

Field	Description
Event Type	*Display only.* Type of the event. Event types are categories that describe the general nature of the event. Possible event types are as follows: • Communication • Environmental • Equipment • Processing Error • Quality of Service • Security • Unknown
Action Log	Shows all actions taken on the event and all notes added to the event.
Life Cycle Type	*Display only.* Type of life cycle of the event. Possible life cycle types are as follows: • State Change • Attribute Value Change • Instance Creation • Instance Deletion • Informational

Related Documents

Related Topic	Document Title
Minimum required Cisco NX-OS logging levels	Logging Severity-Level Requirements, page 1-7
Cisco DCNM server log settings	Administering DCNM Server Log Settings, page 17-1

Related Topic	Document Title
Deleting events from the events database	Deleting Data from the Events Database, page 15-6
Cisco NX-OS system messages	*Cisco NX-OS System Messages Reference*

Feature History for the Event Browser and Events Tabs

Table 10-3 lists the release history for this feature.

Table 10-3 Feature History for the Event Browser and Events Tabs

Feature Name	Releases	Feature Information
Event Browser and Events tabs	4.2(1)	No change from Release 4.1
Event filter results shown in a Filtered Events tab	4.1(2)	This feature was added to the Event Browser.
Event Browser and Events tabs	4.1(2)	No change from Release 4.0

CHAPTER 11

Working with Inventory

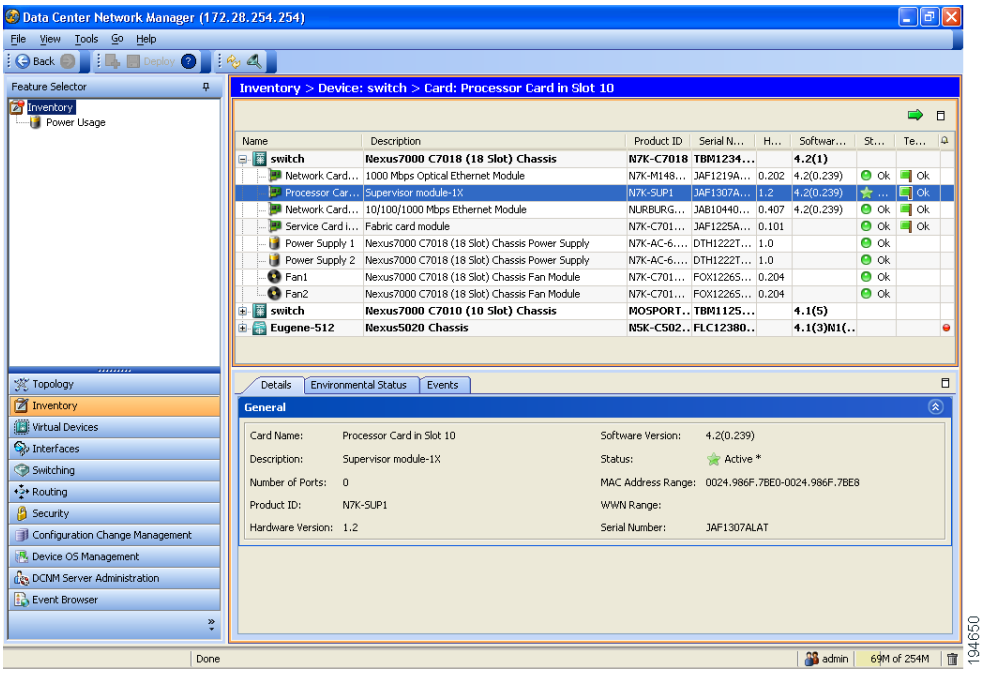
This chapter describes how to use the Inventory feature in Cisco Data Center Network Manager (DCNM).

This chapter has the following sections:

Information About Inventory

The Inventory feature, shown in Figure 11-1, displays information about the chassis, modules, fan trays, and power supplies for managed devices. The Cisco DCNM client can display summary and detailed information for these device components.

Figure 11-1 Inventory Contents Pane



Licensing Requirements for Inventory

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Inventory 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 "Installing Licenses" section on page 2-11.

Prerequisites for Inventory

The Inventory feature has the following prerequisite:

- The physical device must be managed by Cisco DCNM.

Displaying the Chassis Information

Cisco DCNM displays summary, detail, environmental, and event information for the chassis.

This section includes the following topics:

Displaying the Chassis Summary Information

Cisco DCNM displays the chassis summary information for each device it manages when you choose Inventory in the Feature Selector pane. The summary information includes the chassis description, product ID, serial number, hardware version, software version, status, temperature, and events.

DETAILED STEPS

To display the summary information for a chassis, from the Feature Selector pane, choose **Inventory**. The summary pane displays summary information for each managed device.

Displaying the Chassis Detail information

Cisco DCNM displays the chassis detail information for the device that you choose in the Summary pane. This detail information includes hardware and software information. The hardware information includes the switch name, product ID, IP address, serial number, chassis description.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Tabs appear in the Details pane. The Details tab shows the hardware and software information.

Displaying the Chassis Environmental Status

Cisco DCNM displays the chassis environmental status information for the device that you choose in the Summary pane. The environmental information includes power usage information and information about supervisor and power supply redundancy.

DETAILED STEPS

To display the environmental status for a chassis, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Tabs appear in the Details pane.

Step 3 From the Details pane, click the **Environmental Status** tab.

Power usage and redundancy information appears in the Details pane.

Displaying the Chassis CPU Utilization

Cisco DCNM displays the percentage of CPU utilization over time for the device that you choose in the Summary pane. You can customize the reporting of this utilization for types of utilization (user, kernel, or idle), specific thresholds, and time intervals.

DETAILED STEPS

To display the CPU utilization, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary information for each managed device appears in the Summary pane.

Step 2 From the summary pane, click the device.

Tabs appear in the Details pane.

Step 3 From the Details pane, click the **CPU Utilization** tab.

The CPU utilization table appears.

Step 4 (Optional) To display the percentage of utilization devoted to user or kernel functions, follow these steps:

- **a.** Click **Select Parameters**.

  A list of utilization types (user, kernel, and idle) appears.
- **b.** Choose the utilization types that you need to see reported.

Step 5 (Optional) To display utilization within specific thresholds, follow these steps:

- **a.** Click the **Turn Thresholds On/Off** tool.

  The Adjust Threshold Limits slider tool appears on the toolbar next to the Turn Thresholds On/Off tool.
- **b.** To set a minimum CPU utilization threshold, move the left slider to the desired utilization.
- **c.** To set a maximum CPU utilization threshold, move the right slider to the desired utilization.

Step 6 (Optional) To change the monitoring frequency, follow these steps:

- **a.** Click in the Select Frequency tool drop-down list.

  Time intervals appear for you to choose.
- **b.** Choose the appropriate time interval.

Step 7 Click the **Start Monitoring** tool to begin monitoring CPU utilization.

Step 8 (Optional) To stop monitoring the CPU utilization, click the **Stop Monitoring** tool.

Step 9 (Optional) To display how the CPU utilization compares over days or months, follow these steps:

- **a.** Click **Show Overview Chart**.
- **b.** (Optional) To see the latest or real-time utilization data, click **RT**.

c. (Optional) To compare utilization data over days or months, click the appropriate button for the amount of time desired (**1d** shows one day, **2d** shows two days, and so on).

Displaying the Chassis Memory Utilization

Cisco DCNM displays the percentage of memory utilization over time for the device that you choose in the Summary pane. You can customize the reporting of this utilization for specific thresholds and time intervals.

DETAILED STEPS

To display the memory utilization, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Tabs appear in the Details pane.

Step 3 From the Details pane, click the **Memory Utilization** tab.

The Memory Utilization table appears.

Step 4 (Optional) To display utilization within specific thresholds, follow these steps:

a. Click the **Turn Thresholds On/Off** tool.

The Adjust Threshold Limits slider tool appears on the toolbar next to the Turn Thresholds On/Off tool.

b. To set a minimum utilization threshold, move the left slider to the desired utilization.

c. To set a maximum utilization threshold, move the right slider to the desired utilization.

Step 5 (Optional) To change the monitoring frequency, follow these steps:

a. Click in the Select Frequency tool drop-down list.

Time intervals appear for you to choose.

b. Choose the appropriate time interval.

Step 6 Click the **Start Monitoring** tool to begin monitoring utilization.

Step 7 (Optional) To stop monitoring the utilization, click the **Stop Monitoring** tool.

Step 8 (Optional) To display how the utilization compares over days or months, follow these steps:

a. Click **Show Overview Chart**.

b. (Optional) To see the latest or real-time utilization data, click **RT**.

c. (Optional To compare utilization data over days or months, click the appropriate button for the amount of time desired (**1d** shows one day, **2d** shows two days, and so on).

Displaying the Chassis Events

Cisco DCNM displays the chassis events, which includes the source, time, severity, message, and status of the event. You can display additional details for an event.

DETAILED STEPS

To display the chassis events, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Tabs appear in the Details pane.

Step 3 From the Details pane, click the **Memory Utilization** tab.

The Memory Utilization table appears.

Step 4 (Optional) To see details for the event, select the event in the Details pane and click the up arrow at the bottom of the details pane.

Displaying the Module Information

Cisco DCNM displays summary, detail, environmental, and event information for the supervisor modules, I/O modules, and fabric modules.

This section includes the following topics:

Displaying the Module Summary Information

Cisco DCNM displays the module summary information for each device it manages when you expand the device listing in the Summary pane. The summary information includes the module description, product ID, serial number, hardware version, software version, status, temperature, and events.

DETAILED STEPS

To display the summary information for a module, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Chassis summary information for the device appears in the Summary pane.

Step 2 From the Summary pane, expand the device with the modules that you are interested in viewing.

A list of modules, power supplies, and fan trays appears under the device in the Summary pane. Each line includes summary information for the component.

Displaying the Module Detail Information

Cisco DCNM displays the module detail information for the device that you choose in the Summary pane. This detail information includes general identification information and special information that applies to the the module type.

DETAILED STEPS

To display module detail information, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device.

The device listing expands to include a summary of each module, power supply, and fan tray in the chassis.

Step 4 Click the module.

Tabs appear in the Details pane. General details appear in the Details tab.

Displaying the Module Environmental Status

Cisco DCNM displays the module environmental status information for the supervisor module, I/O module, or fabric module that you choose in the Summary pane. The environmental information includes power usage and temperature information.

DETAILED STEPS

To display the environmental status for a module, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device.

The device listing expands to include a summary of each module, power supply, and fan tray in the chassis.

Step 4 Click the module.

Step 5 From the Details pane, click the **Environmental Status** tab.

Power supply and temperature sections appear in the Details pane. The Power Supply section is expanded and the two temperature sections are not expanded

Step 6 (Optional) To see textual temperature information, expand the **Temperature Status Table** section.

Step 7 (Optional) To see graphical temperature information, expand the **Temperature Status Thermometer** section.

Displaying TCAM Statistics

The following window appears in the TCAM Statistics tab:

- TCAM Statistics Chart—Information about TCAM usage on the module.

See the "Working with Statistics and Charts" section on page 4-9 for more information on collecting statistics for this feature.

Displaying the Module Events

Cisco DCNM displays the module event information for the supervisor module, I/O module, or fabric module that you choose in the Summary pane. The events information includes source, time, severity, message, and status information for the event. You can display details for each event.

DETAILED STEPS

To display the events for a module, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device.

The device listing expands to include a summary listing of each module, power supply, and fan tray in the chassis.

Step 4 Click the module.

Step 5 From the Details pane, click the **Events** tab.

An events listing appears in the Details pane.

Step 6 (Optional) To see details for an event, click on the event and click the up arrow button at the bottom of the pane.

Displaying the Power Supply Information

Cisco DCNM displays summary information, general details, and events for power supplies.

This section includes the following topics:

Displaying the Power Supply Summary Information

Cisco DCNM displays the power supply summary information for each device it manages when you expand the device listing in the Summary pane. The summary information includes the module description, product ID, serial number, hardware version, software version, status, temperature, and events.

DETAILED STEPS

To display the summary information for a power supply, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Chassis summary information for the device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device with the modules that you are interested in viewing.

A list of modules, power supplies, and fan trays appears under the device in the Summary pane. Each line includes summary information for the component.

Displaying the Power Supply Detail Information

Cisco DCNM displays the power supply detail information for the device that you choose in the Summary pane. This detail information includes general identification information, power (watts), and current (Amps).

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device.

The device listing expands to include a summary of each module, power supply, and fan tray in the chassis.

Step 4 Click the power supply.

Tabs appear in the Details pane. General details appear in the Details tab.

Displaying the Power Supply Events

Cisco DCNM displays the event information for the power supply that you choose in the Summary pane. The events information includes source, time, severity, message, and status information for the events. You can display details for each event.

DETAILED STEPS

To display the events for a power supply, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device.

The device listing expands to include a summary listing of each module, power supply, and fan tray in the chassis.

Step 4 Click the power supply.

Step 5 From the Details pane, click the **Events** tab.

An events listing appears in the Details pane.

Step 6 (Optional) To see details for an event, click on the event and click the up arrow button at the bottom of the pane.

A field opens to display detailed event information.

Displaying the Fan Tray Information

Cisco DCNM displays summary information, general details, and events for fan trays.

This section includes the following topics:

Displaying the Fan Tray Summary Information

Cisco DCNM displays the fan tray summary information for each device it manages when you expand the device listing in the Summary pane. The summary information includes the fan identification and status information.

DETAILED STEPS

To display the summary information for a fan tray, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Chassis summary information for the device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device with the fan tray that you are interested in viewing.

A list of modules, power supplies, and fan trays appears under the device in the Summary pane. Each line includes summary information for the component.

Displaying the Fan Tray Detail Information

Cisco DCNM displays the fan tray detail information for the device that you choose in the Summary pane. This detail information includes descriptive information and status for the fan tray.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device.

The device listing expands to include a summary of each module, power supply, and fan tray in the chassis.

Step 4 Click the fan tray.

Tabs appear in the Details pane. General details appear in the Details tab.

Displaying the Fan Tray Events

Cisco DCNM displays the event information for the fan tray that you choose in the Summary pane. The events information includes source, time, severity, message, and status information for the event. You can display details for each event.

DETAILED STEPS

To display the events for a fan tray, follow these steps:

Step 1 From the Feature Selector pane, choose **Inventory**.

Summary chassis information for each managed device appears in the Summary pane.

Step 2 From the Summary pane, click the device.

Step 3 Expand the device.

The device listing expands to include a summary listing of each module, power supply, and fan tray in the chassis.

Step 4 Click the fan tray.

Step 5 From the Details pane, click the **Events** tab.

An events listing appears in the Details pane.

Step 6 (Optional) To see details for an event, click on the event and click the up arrow button at the bottom of the pane.

Feature History for Inventory

Table 11-1 lists the release history for this feature.

Table 11-1 Feature History for Inventory

Feature Name	Releases	Feature Information
Inventory	4.2(3)	Support was added for Nexus 4000 Series switches.
Inventory	4.2(1)	Support was added for Nexus 5000 Series switches and Nexus 2000 Series fabric extenders.
Inventory	4.1(2)	No change from Release 4.0

CHAPTER 12

Configuring SPAN

This chapter describes how to configure an Ethernet switched port analyzer (SPAN) to analyze traffic between ports on Cisco NX-OS devices.

Note The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this chapter. For the latest feature information and caveats, see the documentation and release notes for your platform and software release.

This chapter includes the following sections:

Information About SPAN

SPAN analyzes all traffic between source ports by directing the SPAN session traffic to a destination port with an external analyzer attached to it.

You can define the sources and destinations to monitor in a SPAN sessions on the local device.

This section includes the following topics:

- Virtualization Support, page 12-4

SPAN Sources

The interfaces from which traffic can be monitored are called SPAN sources. Sources designate the traffic to monitor and whether to copy ingress, egress, or both directions of traffic. SPAN sources include the following:

- Ethernet ports
- VLANs—When a VLAN is specified as a SPAN source, all supported interfaces in the VLAN are SPAN sources.
- Remote SPAN (RSPAN) VLANs

Note A single SPAN session can include mixed sources in any combination of the above.

Characteristics of Source Ports

SPAN source ports have the following characteristics:

- A port configured as a source port cannot also be configured as a destination port.
- An RSPAN VLAN can only be used as a SPAN source.

SPAN Destinations

SPAN destinations refer to the interfaces that monitor source ports. Destination ports receive the copied traffic from SPAN sources.

Characteristics of Destination Ports

SPAN destination ports have the following characteristics:

- Destinations for a SPAN session include Ethernet ports or port-channel interfaces in either access or trunk mode.
- A port configured as a destination port cannot also be configured as a source port.
- A destination port can be configured in only one SPAN session at a time.
- Destination ports do not participate in any spanning tree instance. SPAN output includes Bridge Protocol Data Unit (BPDU) Spanning-Tree Protocol hello packets.
- An RSPAN VLAN cannot be used as a SPAN destination.
- You can configure SPAN destinations to inject packets to disrupt a certain TCP packet stream in support of the Intrusion Detection System (IDS).
- You can configure SPAN destinations to enable a forwarding engine to learn the MAC address of the IDS.

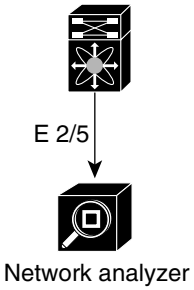
SPAN Sessions

You can create up to 18 SPAN sessions designating sources and destinations to monitor.

Note Only two SPAN sessions can be running simultaneously.

Figure 12-1 shows a SPAN configuration. Packets on three Ethernet ports are copied to destination port Ethernet 2/5. Only traffic in the direction specified is copied.

Figure 12-1 SPAN Configuration



Source Port	Direction	Destination Ports
E 2/1	Rx	E 2/5
E 2/2	Rx, Tx	
E 2/3	Tx	

186283

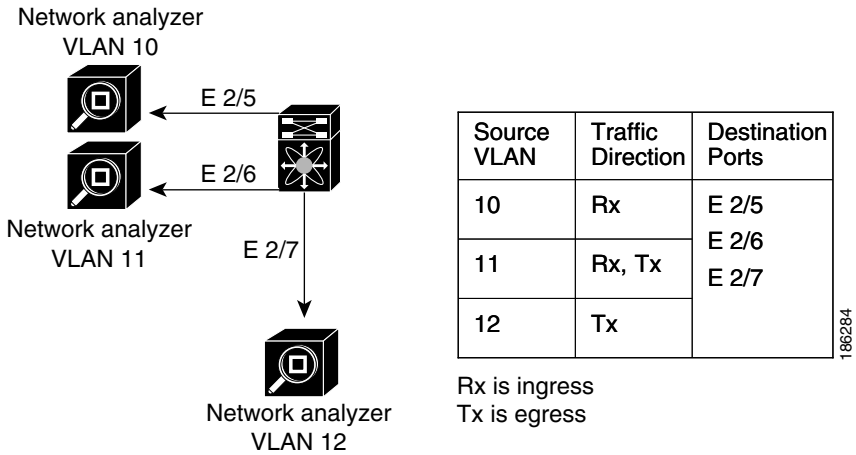
Virtual SPAN Sessions

You can create a virtual SPAN session to monitor multiple VLAN sources and choose only VLANs of interest to transmit on multiple destination ports. For example, you can configure SPAN on a trunk port and monitor traffic from different VLANs on different destination ports.

Figure 12-2 shows a virtual SPAN configuration. The virtual SPAN session copies traffic from the three VLANs to the three specified destination ports. You can choose which VLANs to allow on each destination port to limit the traffic that the device transmits on it. In Figure 12-2, the device transmits packets from one VLAN at each destination port.

Note Virtual SPAN sessions cause all source packets to be copied to all destinations, whether the packets are required at the destination or not. VLAN traffic filtering occurs at the egress destination port level.

Figure 12-2 Virtual SPAN Configuration



Source VLAN	Traffic Direction	Destination Ports
10	Rx	E 2/5 E 2/6 E 2/7
11	Rx, Tx	
12	Tx	

Rx is ingress
Tx is egress

For information about configuring a virtual SPAN session, see the "Configuring a Virtual SPAN Session" section on page 12-8.

Multiple SPAN Sessions

Although you can define up to 18 SPAN sessions, only two SPAN sessions can be running simultaneously. You can shut down an unused SPAN session.

For information about shutting down SPAN sessions, see the "Shutting Down or Resuming a SPAN Session" section on page 12-10.

High Availability

The SPAN feature supports stateless and stateful restarts. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support

A virtual device context (VDC) is a logical representation of a set of system resources. SPAN applies only to the VDC where the commands are entered.

For information about configuring VDCs, see the *Cisco DCNM Virtual Device Context Configuration Guide, Release 4.x*.

Licensing Requirements for SPAN

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	SPAN 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 a complete explanation of the Cisco DCNM licensing scheme, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.x*.
NX-OS	SPAN requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.x*.

Prerequisites for SPAN

SPAN has the following prerequisites:

- You must first configure the ports on each device to support the desired SPAN configuration. For more information, see the *Cisco DCNM Interfaces Configuration Guide, Release 4.x*.

Guidelines and Limitations

SPAN has the following configuration guidelines and limitations:

- Table 1 lists the SPAN session limits.

Table 1 SPAN Session Limits

Description	Limit
Configured SPAN sessions	18
Simultaneously running SPAN sessions	2
Source interfaces per session	128
Source VLANS per session	32
Destination interfaces per session	32

- A destination port can only be configured in one SPAN session at a time.
- You cannot configure a port as both a source and destination port.
- A single SPAN session can include mixed sources in any combination of the following:
  - Ethernet ports
  - VLANs
- Destination ports do not participate in any spanning tree instance. SPAN output includes Bridge Protocol Data Unit (BPDU) Spanning-Tree Protocol hello packets.
- When a SPAN session contains multiple egress source ports, packets that these ports receive may be replicated even though they are not transmitted on the ports. Some examples of this behavior on source ports are as follows:
  - Traffic that results from flooding
  - Broadcast and multicast traffic

- For VLAN SPAN sessions with both ingress and egress configured, two packets (one from ingress and one from egress) are forwarded from the destination port if the packets get switched on the same VLAN.
- VLAN SPAN monitors only the traffic that leaves or enters Layer 2 ports in the VLAN.
- You can configure an RSPAN VLAN for use only as a SPAN session source.
- You can configure a SPAN session on the local device only.
- If you configure a SPAN session, ensure that you configure the logging level for SPAN to 6 (Informational) or a higher level on the Cisco NX-OS device. To configure the device with the minimal required logging configuration, log into the command-line interface of the device and use the following commands:

```
switch(config)# logging level monitor 6
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

  For more information about Cisco NX-OS system-message logging requirements, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.x*.

Configuring SPAN

This section includes the following topics:

Configuring a SPAN Session

You can configure a SPAN session on the local device only. By default, SPAN sessions are created in the shut state.For sources, you can specify Ethernet ports, port channels, VLANs, and RSPAN VLANs. You can specify private VLANs (primary, isolated, and community) in SPAN sources. .

For destination ports, you can specify Ethernet ports or port-channels in either access or trunk mode. You must enable monitor mode on all destination ports.

BEFORE YOU BEGIN

- A single SPAN session can include mixed sources in any combination of Ethernet ports or VLANs.
- You must have already configured the destination ports in access or trunk mode. For more information, see the *Cisco DCNM Interfaces Configuration Guide, Release 4.x*.

DETAILED STEPS

To configure a SPAN session, follow these steps:

Step 1 From the Feature Selector pane, choose **Interfaces > Traffic Monitoring > SPAN**. The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.

Step 3 (Optional) To delete a SPAN session that you are no longer using, right-click the SPAN session and choose **Delete**.

Step 4 (Optional) To configure a new SPAN session, from the menu bar choose **File > New Local SPAN Session**. By default, SPAN sessions are created in the shut state.

a. (Only the first time you create a SPAN session) From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.

b. (Optional) To modify the session number, from the Summary pane, double-click the Session Id field and enter a session number from 1 to 18.

Note You can only modify the session number immediately after you create the session.

Step 5 From the Summary pane, choose the SPAN session to configure.

Step 6 From the Details pane, click the **Configuration** tab and expand the **Session Settings** section, if necessary.

Step 7 (Optional) To add a description of the SPAN session, specify it in the Description field.

Step 8 (Optional) In the Filtered VLANs field, click the down arrow to display and choose from the configured VLANs.

Step 9 Add source Ethernet ports to the SPAN session as follows:

a. From the Ports association panel, double-click the device and then double-click the desired slot to display ports.

b. Choose the port, right-click on the port row, and choose **Add to SPAN Source** to add this port to the SPAN session sources.

Step 10 Add source VLANs or RSPAN VLANs to the SPAN session as follows:

a. From the VLANs association panel, double-click the device to display the configured VLANs.

b. Choose the VLAN, right-click on the VLAN row, and choose **Add to SPAN Source** to add this VLAN to the SPAN session sources.

Step 11 Add destination Ethernet ports to the SPAN session as follows:

a. From the Ports association panel, double-click the device and then double-click the desired slot to display ports.

b. Choose an access or trunk port.

c. In the Monitor column check the check box to enable monitoring on this port.

d. Right-click on the port row and choose **Add to SPAN Destination** to add this port to the SPAN session destinations.

Step 12 (Optional) To modify SPAN session source settings, follow these steps:

a. From the **Details** pane, click the **Configuration** tab and expand the **Source and Destination** section, if necessary.

b. To modify the ingress or egress choice for a source, check or uncheck the **Ingress** or **Egress** check box to activate the desired direction to monitor. By default, both ingress and egress are monitored.

c. To delete a SPAN source or destination, choose the source or destination entry, right-click on it, and choose **Delete**.

Step 13 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring a Virtual SPAN Session

You can configure a virtual SPAN session to copy packets from source ports, VLANs, and RSPAN VLANs to destination ports on the local device. By default, SPAN sessions are created in the shut state.

For sources, you can specify ports, VLANs, or RSPAN VLANs.

For destination ports, you can specify Ethernet ports. You can choose which VLANs to allow on each destination port to limit the traffic that the device transmits on it.

BEFORE YOU BEGIN

- You have already configured the destination ports in trunk mode. For more information, see the *Cisco DCNM Interfaces Configuration Guide, Release 4.x*.

DETAILED STEPS

To configure a virtual SPAN session, follow these steps:

Step 1 From the Feature Selector pane, choose **Interfaces > Traffic Monitoring > SPAN**. The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.

Step 3 (Optional) To delete a SPAN session that you are no longer using, right-click the SPAN session and choose **Delete**.

Step 4 (Optional) To configure a new SPAN session, from the menu bar choose **File > New Local SPAN Session**. By default, SPAN sessions are created in the shut state.

a. (Only the first time you create a SPAN session) From the Summary pane, double-click the device that you want to configure with a SPAN session to display the configured SPAN sessions.

b. (Optional) To modify the session number, from the Summary pane, double-click the Session Id field and enter a session number from 1 to 18.

Note You can only modify the session number immediately after you create the session.

Step 5 From the Summary pane, choose the SPAN session to configure.

Step 6 From the Details pane, click the **Configuration** tab and expand the **Session Settings** section, if necessary.

Step 7 (Optional) To add a description of the SPAN session, specify it in the **Description** field.

Step 8 (Optional) To add VLANs to filter (include) in the SPAN session, in the Filtered VLANs field, down array to displays the configured VLANs that you can choose.

Step 9 Add source Ethernet ports to the SPAN session as follows:

a. From the Ports association panel, double-click the device and then double-click the desired slot to display ports.

b. Choose the port, right-click on the port row, and choose **Add to SPAN Source** to add this port to the SPAN session sources.

Step 10 Add source VLANs or RSPAN VLANs to the SPAN session as follows:

a. From the VLANs association panel, double-click the device to display the configured VLANs.

b. Choose the VLAN, right-click on the VLAN row, and choose **Add to SPAN Source** to add this VLAN to the SPAN session sources.

Step 11 Add destination Ethernet ports to the SPAN session as follows:

a. From the Ports association panel, double-click the device and then double-click the desired slot to display ports.

b. Choose an access or trunk port.

c. In the Monitor column check the check box to enable monitoring on this port.

d. Right-click on the port row and choose **Add to SPAN Destination** to add this port to the SPAN session destinations.

Step 12 Limit the VLANs allowed on a trunk port by following these steps:

a. From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**. The available devices appear in the Summary pane.

b. From the Summary pane, double-click the device and then double-click the slot that you want to configure.

c. Choose the trunk port to configure.

d. From the Details pane, click the **Port Details** tab and expand the **Port Mode Settings** section, if necessary.

e. Limit the VLANs on the trunk by clicking the Allowed VLANs field. The field displays configured VLANs that you can choose.

Step 13 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring an RSPAN VLAN

You can specify a remote SPAN (RSPAN) VLAN as a SPAN session source.

DETAILED STEPS

To configure an RSPAN VLAN, follow these steps:

Step 1 From the Feature Selector pane, choose **Switching > VLAN**. The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device that you want to configure.

Step 3 Choose the VLAN to configure.

Step 4 From the Details pane, click the **VLAN Details** tab and expand the **Advanced Settings** section, if necessary.

Step 5 Check the **RSPAN VLAN** check box.

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

Shutting Down or Resuming a SPAN Session

You can shut down SPAN sessions to discontinue the copying of packets from sources to destinations. Because only two SPAN sessions can be running simultaneously, you can shut down one session in order to free hardware resources to enable another session. By default, SPAN sessions are created in the shut state.

You can resume (enable) SPAN sessions to resume the copying of packets from sources to destinations. In order to enable a SPAN session that is already enabled but operationally down, you must first shut it down and then enable it.

DETAILED STEPS

To shut down or resume (enable) a SPAN session, follow these steps:

Step 1 From the Feature Selector pane, choose **Interfaces > Traffic Monitoring > SPAN**.

The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device to display the configured SPAN sessions.

Step 3 From the Summary pane, choose the SPAN session to configure.

Step 4 From the Details pane, click the **Configuration** tab and expand the **Session Settings** section, if necessary.

Step 5 Resume (enable) the SPAN session by choosing **Up** in the Admin Status field.

Step 6 Shut down the SPAN session by choosing **Down** in the Admin Status field.

Note If a monitor session is enabled but its operational status is down, then to enable the session you must first shut down the session followed by resuming the session.

Field Descriptions for SPAN

This section includes the following field descriptions for SPAN:

- Local SPAN Session: Configuration: Session Settings Section, page 12-11
- Local SPAN Session: Configuration: Source and Destination Section, page 12-11

Local SPAN Session: Configuration: Session Settings Section

Table 12-2 Local SPAN Session: Configuration: Session Settings Section

Element	Description
Session Id	Local SPAN session number. Can only be specified when the session is first created. The value ranges from 1 to 18.
Description	Description for this session.
Filtered VLANs	When clicked, list of configured VLANs.
Admin Status	Administrative status of the session.
Operational Status	*Display only*. Whether the session is shut (down) or enabled (up).
Status Description	*Display only*. Status description.

Local SPAN Session: Configuration: Source and Destination Section

Table 12-3 Local SPAN Session: Configuration: Source and Destination Section

Element	Description
Source	
Interface/VLAN	*Display only*. Port or VLAN number.
Description	*Display only*. Port or VLAN description.
Ingress	Status of whether to monitor ingress packets.
Egress	Status of whether to monitor egress packets.
Destination	
Interface	*Display only*. Port number.
Description	*Display only*. Port description.

Additional References

For additional information related to implementing SPAN, see the following sections:

- Related Documents, page 12-12
- Standards, page 12-12

Related Documents

Related Topic	Document Title
VDCs	*Cisco DCNM Virtual Device Context Configuration Guide, Release 4.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 SPAN

Table 12-4 lists the release history for this feature.

Table 12-4 Feature History for SPAN

Feature Name	Releases	Feature Information
Guidelines and Limitations	4.2(1)	No change from Release 4.1.

CHAPTER 13

Managing Device Operating Systems

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

This chapter includes the following topics:

Information About Device OS Management

The Device OS Management feature allows you to control the software images installed on Nexus 7000 Series devices that are managed by Cisco DCNM.

This section includes the following topics:

Device OS Management Screen

The Device OS Management screen allows you to view information about the software images used by a managed device. You can also start the Software Installation Wizard from the Device OS Management Summary pane.

Software Installation Jobs

The Software Installation Jobs feature allows you to create and monitor software installation jobs. Cisco DCNM provides the Software Installation Wizard, which you use to specify all the necessary information for configuring a software installation job.

You can create software installation jobs that affect one or more managed devices. You can use software images that are already in the local file system of the devices or Cisco DCNM can instruct each managed device included in a job to transfer software images to the local file system on the managed device. Your options are as follows:

- Device file system—You can use software images that are in the local file system of the devices. You must ensure that the images exist on the devices prior to configuring the installation job.

  You can specify a software image for a device type category rather than for a single device; however, the image that you specify must exist on each device in the category in the same location and with the same filename. For example, if you specify bootflash:/images/n7000-s1-dk9.4.1.2.upg.bin, the n7000-s1-dk9.4.1.2.upg.bin image file must exist in bootflash:/images on each device in the device category.

- File server—You can use a file server that you have configured in Cisco DCNM. If you use a file server, Cisco DCNM uses the information that you provide when you configure the file server and when you configure the software installation job to assemble a URL that the managed devices in the job can use to retrieve the software images.

  Before configuring a software installation job, you should ensure that the software images are on the file server. You must also configure the file server in Cisco DCNM. For more information, see the "File Servers" section on page 13-3.

- URL—You can use a URL to specify the image files. The verification that Cisco DCNM performs for a URL varies depending upon the transfer protocol that you use, as follows:
  - FTP—Cisco DCNM verifies the URL format, that the FTP server in the URL is reachable, and that the specified image file exists on the FTP server. The FTP URL format is as follows:

    ftp://*username@servername/path/filename*
  - SFTP—Cisco DCNM verifies the URL format, that the SFTP server in the URL is reachable, and that the image file specified exists on the SFTP server. The SFTP URL format is as follows:

    sftp://*username@servername/path/filename*
  - TFTP—You must ensure that the path and image filename are correct. Cisco DCNM verifies the URL format and that the TFTP server in the URL is reachable. The TFTP URL format is as follows:

    tftp://*servername/path/filename*
  - SCP—You must ensure that the SCP server is reachable and that the path and image filename are correct. Cisco DCNM verifies the URL format. The SCP URL format is as follows:

    scp://*username@servername/path/filename*

The Software Installation Wizard includes an optional step for verifying the version compatibility of software images with the managed devices. During this step, if a software image was specified by a URL or file server, Cisco DCNM instructs managed devices to copy the software image from the URL or file server to the bootflash file system on the device. If you skip the version compatibility step, Cisco DCNM does not instruct devices to copy software images from URLs or file servers until the installation job begins.

File Servers

The File Servers feature allows you to configure files servers, which you can use for the following purposes:

- Software installation jobs—Cisco DCNM can get software image files from a file server and transfer them to devices included in a software installation job.
- Configuration rollbacks—Cisco DCNM can back up device configurations to a file server when you roll back a device configuration.

Cisco DCNM supports file servers that use the following protocols:

- FTP
- SFTP
- TFTP

If you use a file server in a software installation job, consider the following items:

- The managed devices included in the job must be able to connect to the file server directly.
- To ensure that software image files transfer as quickly as possible, use a file server that is on the same LAN as the devices included in the software installation job. If 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.

Virtualization Support

Device software images apply to physical devices rather than virtual device contexts (VDCs). When you change the software image on a managed device, all VDCs on the device use the new software image.

Licensing Requirements for Device OS Management

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Device OS Management requires a LAN Enterprise license. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the "Installing Licenses" section on page 2-11.

Prerequisites for Device OS Management

The Device OS Management feature has the following prerequisites:

- The Device OS Management feature supports only devices that are managed by Cisco DCNM, which means that Cisco DCNM must have successfully discovered the device.
- The Device OS Management feature supports only devices that you have added to the list of Cisco DCNM-licensed devices.
- Devices included in a software installation job must be reachable by Cisco DCNM when a software installation job occurs. Software installation jobs fail for unreachable devices.

Guidelines and Limitations for Device OS Management

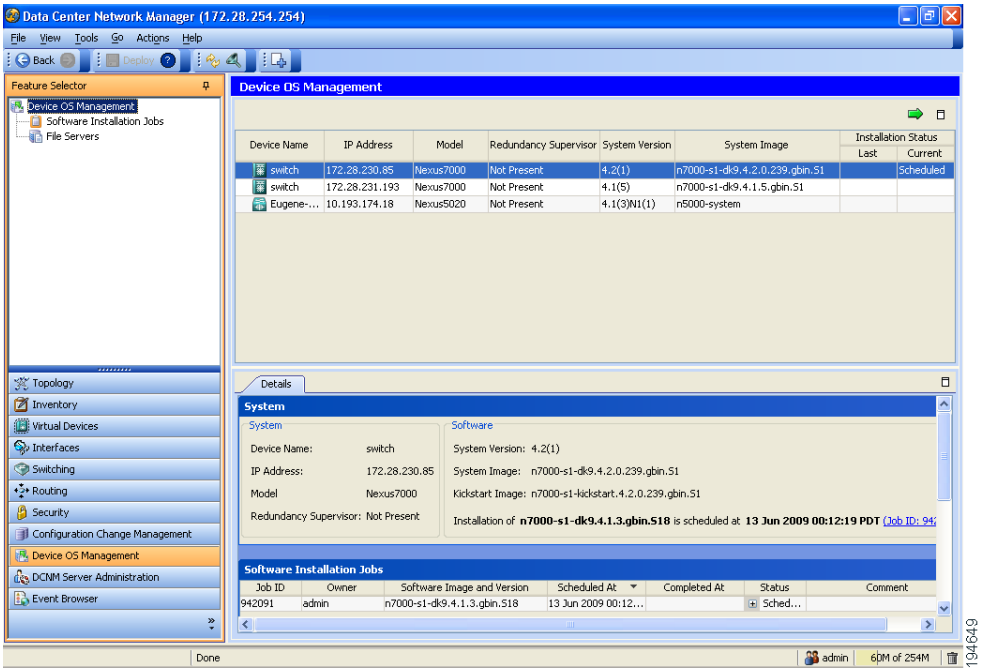
The Device OS Management feature has the following configuration guidelines and limitations:

- URLs and file servers used in a software installation job must be reachable by the managed devices included in the job.
- If you use a DNS name in a URL or when you configure a file server, ensure that managed devices using the URL or file server can resolve the DNS name.
- Software installation jobs do not reload connectivity management processors (CMPs). You must manually reload CMPs as needed when a software installation job completes. The status for a completed software installation job includes messages about CMPs that must be reloaded manually. For more information, see the *Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.x*.
- For Cisco Nexus 7000 series devices that have a single supervisor module, a software installation job does not reload the device. After the installation job completes, to run the newly installed software image on a single-supervisor Nexus 7000 series device, you must manually reload the device. For more information, see the *Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.x*.

Using the Device OS Management Window

Figure 13-1 shows the Device OS Management content pane.

Figure 13-1 Device OS Management Content Pane



This section includes the following topics:

- Viewing Device Image Details, page 13-5

- Installing Software on a Device, page 13-5

Viewing Device Image Details

You can view details about the software image on a managed device.

DETAILED STEPS

To view details about a software image on a managed device, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management**.

A table of managed devices appears in the Summary pane. Each row displays software image information about a device. Devices are listed alphabetically.

Step 2 Click the device for which you want to see software image details.

The Details pane displays two sections of information. In addition to displaying the information also shown in the Summary pane, if an installation job is scheduled, the System section displays a message about any scheduled installation job, including a link to the installation job.

The Software Installation Jobs section displays information about future, ongoing, and past installation jobs.

Tip To expand or collapse the System or the Software Installation Jobs sections, double-click the section title.

Step 3 (Optional) To open a scheduled software installation job, in the System section, click the link to the installation job.

The Feature Selector pane changes to the Software Installation Jobs feature. For more information, see the "Viewing Software Installation Job Details" section on page 13-7.

Installing Software on a Device

You can install software on a device listed on the Device OS Management Summary pane. Installing software from the Device OS Management Summary pane starts the Software Installation Wizard, which allows you to create or modify a software installation job.

BEFORE YOU BEGIN

Ensure that the software images that you want to install are available by one of the options that the Software Installation Wizard supports. For more information, see the "Software Installation Jobs" section on page 13-2.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Device OS Management >Device OS Management**.

A table of managed devices appears in the Summary pane.

Step 2 Click a device that you want to include in a new software installation job.

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

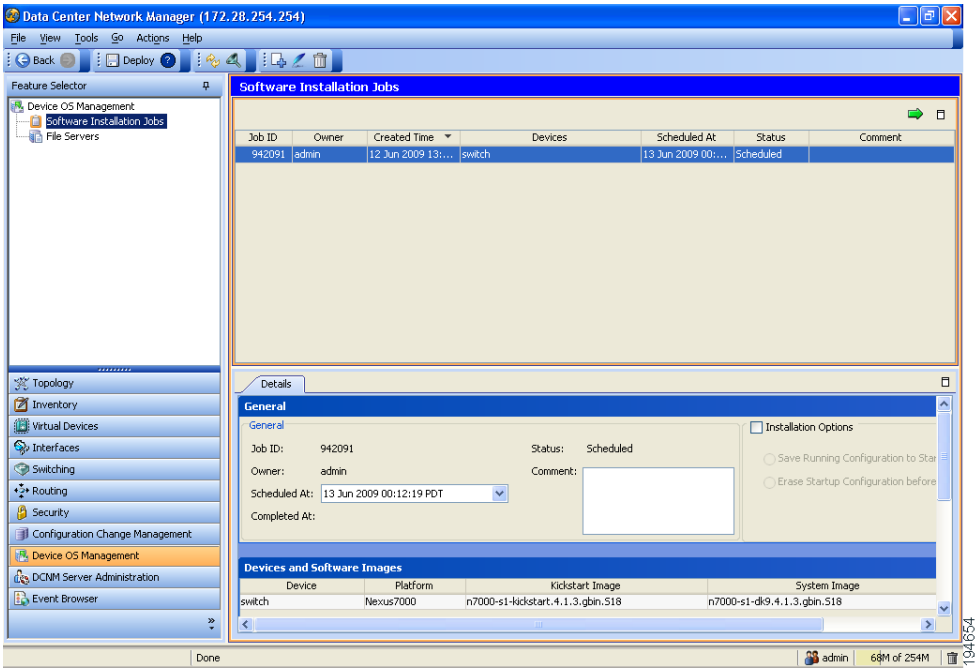
The Software Installation Wizard dialog box displays the Select Switches step. The device that you selected is listed under Selected Switches.

Step 4 To use the Wizard, see the "Using the Software Installation Wizard" section on page 13-8.

Configuring Software Installation Jobs

Figure 13-2 shows the Software Installation Jobs content pane.

Figure 13-2 Software Installation Jobs Content Pane



This section includes the following topics:

Viewing Software Installation Job Details

You can view the details of a software installation job, including its status.

BEFORE YOU BEGIN

You must have configured a software installation job before you can view its details.

DETAILED STEPS

To view software installation job details, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > Software Installation Jobs**.

The Summary pane displays a table of software installation jobs.

Step 2 Click the software installation job for which you want to view details.

The Details pane displays two sections of information. The General section displays the job ID, the job owner, scheduling information, comments, and installation options.

The Device and Software Images section displays a table of devices included in the job, the software images to be installed on each device, and the status of the installation for the device.

Tip To expand or collapse the General or the Device and Software Images sections, double-click the section title.

Creating or Editing a Software Installation Job

From the Software Installation Jobs content pane, you can create a software installation job or edit an existing job. Creating or editing a job from the Software Installation Jobs content pane starts the Software Installation Wizard, which allows you to create or modify a job.

BEFORE YOU BEGIN

Ensure that the software images that you want to install are available by one of the options that the Software Installation Wizard supports. For more information, see the "Software Installation Jobs" section on page 13-2.

To ensure that software image files transfer as quickly as possible, use a file server that is on the same LAN as the devices included in the software installation job. If 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.

DETAILED STEPS

To create or edit a software installation job, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > Software Installation Jobs**.

The Summary pane displays a table of software installation jobs.

Step 2 Do one of the following:

- If you want to create a job, from the menu bar, choose **Actions > New**.
- If you want to edit a job, in the Summary pane, click the job, and then, from the menu bar, choose **Actions > Edit**.

The Software Installation Wizard dialog box displays the Select Switches step.

Step 3 To use the wizard, see the "Using the Software Installation Wizard" section on page 13-8.

Using the Software Installation Wizard

You can use the Software Installation Wizard to configure a new software installation job or make changes to an existing software installation job.

BEFORE YOU BEGIN

Start the Software Installation Wizard, from one of the following places:

- Device OS Management—See the "Installing Software on a Device" section on page 13-5.
- Software Installation Jobs—See the "Creating or Editing a Software Installation Job" section on page 13-7.

DETAILED STEPS

To use the Software Installation Wizard, follow these steps:

Step 1 In the Software Installation Wizard dialog box, follow these steps for each device that you want to include in the installation job:

a. Under Available Switches, click the device.

b. Click **Add**.

Tip To remove a device from the job, under Selected Switches, click the device and then click **Remove**.

Step 2 Click **Next**.

The Software Installation Wizard dialog box displays the Specify Software Images step. Devices are categorized by the physical device type. You can specify software images for each device individually or for an entire category of devices of the same physical type.

Step 3 For each device or physical device category, specify a kickstart image and a system image. To do so, follow these steps once for the Kickstart Image text box and again for the System Image text box:

a. In the applicable image text box, click to activate the text box and then click the more button.

The Software Image Browser dialog box appears.

b. Specify the location of the file for the software image to be installed. To do so, choose one of the following options:

- File Server—If you choose this option, you must pick a file server from the Repository list, navigate the folders on the file server, and select the software image file.
- Switch File System—If you choose this option, you must navigate the file system on a device and select the software image file.

  If you are specifying a software image for a device type category, the image specified must exist on each device in the category, in the same location and with the same filename.
- URL—If you choose this option, enter the URL in the URL text box. If the transfer protocol that you use includes a username in the URL, in the Password text box type the password for the username in the URL.

c. Click **OK**.

If you specified a URL, Cisco DCNM verifies the URL.

The Software Image Browser dialog box closes. The applicable image text box displays the software image that you chose.

Step 4 (Optional) If you do not want the Software Installation Wizard to verify that the selected kickstart and system software images are compatible with a device, check the Skip Version Compatibility check box in the row of the device.

Tip The Next button remains unavailable until you have specified a kickstart image and a system image for each device included in the software installation job.

Step 5 Click **Next**.

If you specified a URL or a software image repository for the location of software images, Cisco DCNM instructs the devices in the job to retrieve the images from the specified locations.

If any device does not have enough space in its local file system to receive the software image files, a dialog box provides you the option to free up space on the device.

Step 6 If you receive a warning about insufficient space on the device, do one of the following:

- If you want to delete files from devices, click **Yes**. Use the Delete Files dialog box to explore the local file system of devices and delete unwanted files. When you are done, click **OK** and then click **Next**.
- If you want to remove the device from the job, click **No**, click **Back**, and return to Step 3.
- If you want to exit the Software Installation Wizard, click **No** and then click **Cancel**.

Unless you chose to skip the version compatibility check for every device in the installation job, the Software Installation Wizard dialog box displays the Pre-installation Checks step. The Version Compatibility Check column indicates whether a device passed or failed the check.

Step 7 If the Software Install Wizard dialog box displays the Pre-installation Checks step, follow these steps:

a. If any device failed the version compatibility check, do one of the following:

- If you want to change the software image files specified for a device, click **Back** and return to Step 3.
- If you want the job to proceed by not installing software on devices that failed the version compatibility check, check the **Skip devices with version compatibility failure** check box.

b. Click **Next**.

The Software Installation Wizard dialog box displays the Installation Options and Schedule step.

Step 8 (Optional) If you want the job to save the current configuration or delete the current configuration on each device, follow these steps:

a. Check the **Installation Options** check box.

b. If you want the job to copy the running configuration to the startup configuration on each device, click the **Save Running Configuration to Startup before Installation** radio button. After the installation job, devices in the job will have the same configuration that they did prior to the job, unless the installation is an upgrade or downgrade that modifies the running configuration.

c. If you want the job to delete the startup configuration on each device, click the **Erase Startup Configuration before Installation** radio button. After the installation job completes, devices in the job will have only the default running configuration.

Step 9 Under Schedule, do one of the following:

- If you want the software installation job to start immediately after you complete the Wizard, click the **Install Now** radio button.
- If you want to specify a date and time for the start of the software installation job, click the **Schedule Installation** radio button and then use the **Date and Time** field to specify when the job should begin.

Step 10 (Optional) In the Comments text box, enter a comment about the installation job.

Step 11 Under Execution Mode, do one of the following:

- If you want the installation job to run on one device at a time before it begins on the next device included in the job, click the **Sequential** radio button.
- If you want the installation job to start at the same time on all the devices included in the job, click the **Concurrent** radio button.

Step 12 (Optional) If you want the software installation job to save the log data for failed installations, check the **Archive logs from switches on DCNM server upon installation failure** check box.

Step 13 Click **Finish**.

If you specified a date and time for the job under Schedule, the Wizard closes and the job appears in the Summary pane.

If you clicked the Install Now radio button under Schedule, the Software Installation Status dialog box displays information about each device in the job and the job status.

Step 14 If the Software Installation Status dialog box appears, do one of the following:

- If you want to close the dialog box and allow the job to run, click **Run in Background**.
- If you want to abort software installation on one or more devices, for each device, click the device and click **Abort Selected**.
- If you want to abort software installation for all devices, click **Abort All**.

Tip If you abort software installation on all devices, click **Close** to close the dialog box.

Rescheduling a Software Installation Job

You can change the scheduled date and time of a software installation job.

BEFORE YOU BEGIN

The software installation job that you want to reschedule must have a status of Scheduled. You cannot reschedule aborted or completed jobs.

DETAILED STEPS

To reschedule a software installation job, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > Software Installation Jobs**.

The Summary pane displays a table of software installation jobs.

Step 2 In the Summary pane, click the job that you want to reschedule.

The Details pane displays information about the job.

Step 3 (Optional) From the Details tab, expand the **General** section, if necessary.

Step 4 Use the **Scheduled At** field to specify when the job should begin.

Step 5 From the menu bar, choose **File > Deploy** to save the change to the job schedule.

Deleting a Software Installation Job

You can delete a software installation job, regardless of its state. In the Summary pane for Software Installation Jobs, completed and aborted jobs remain until you delete them.

DETAILED STEPS

To delete a software installation job, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > Software Installation Jobs**.

The Summary pane displays a table of software installation jobs.

Step 2 In the Summary pane, click the job that you want to delete.

The Details pane displays information about the job.

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

A Warning dialog box displays a confirmation message.

Step 4 Click **Yes**.

The job is removed from the summary pane. You do not need to save your changes.

Adding or Changing Comments for a Software Installation Job

You can add or change the comments associated with a software installation job.

DETAILED STEPS

To add or change comments for a software installation job, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > Software Installation Jobs**.

The Summary pane displays a table of software installation jobs.

Step 2 In the Summary pane, click the job for which you want to add or change comments.

The Details pane displays information about the job.

Step 3 (Optional) From the Details tab, expand the **General** section, if necessary.

Step 4 In the Comments field, enter your comments.

Step 5 From the menu bar, choose **File > Deploy** to save the change to the job schedule.

Changing Installation Options for a Software Installation Job

You can change the installation options associated with a software installation job. Installation options allow you to specify whether Cisco DCNM should save the running configuration of devices, delete the startup configuration, or take no action on the configuration of devices prior to installing the software.

DETAILED STEPS

To change installation options for a software installation job, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > Software Installation Jobs**.

The Summary pane displays a table of software installation jobs.

Step 2 In the Summary pane, click the job for which you want to add or change comments.

The Details pane displays information about the job.

Step 3 (Optional) From the Details tab, expand the **General** section, if necessary.

Step 4 If you want devices in the software installation job to have only the default device configuration after the installation job completes, follow these steps:

a. Check the **Installation Options** check box.

b. If you want the job to delete the startup configuration on each device, click the **Erase Startup Configuration before Installation** radio button.

Step 5 If you want devices in the software installation job to have the same running configuration after the installation job completes, follow these steps:

a. Check the **Installation Options** check box.

b. If you want the job to copy the running configuration to the startup configuration on each device, click the **Save Running Configuration to Startup before Installation** radio button.

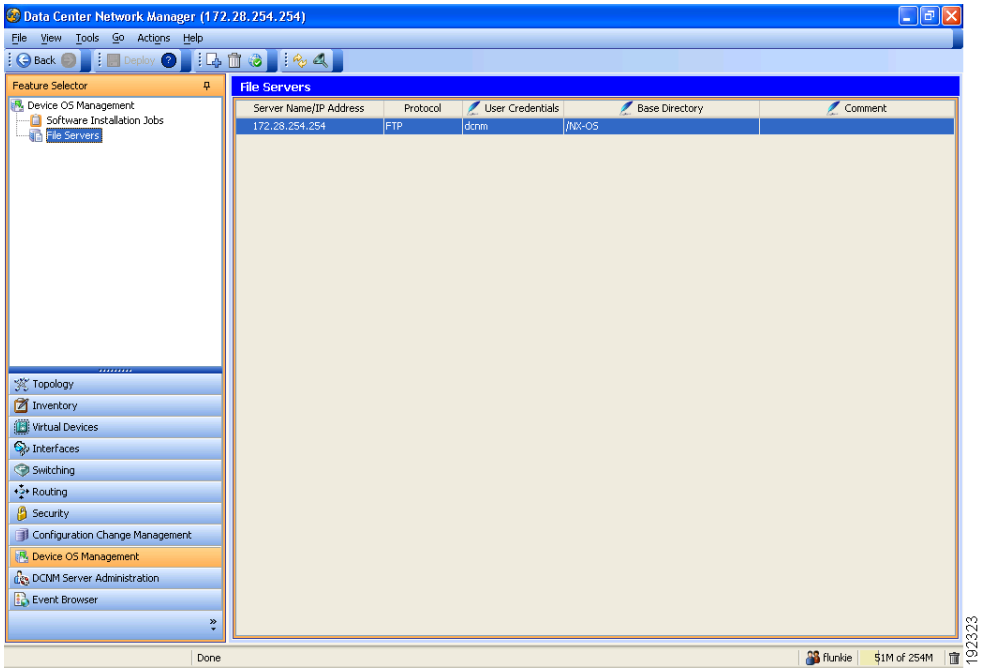
Step 6 If you want the devices in the software installation job to use their current startup configuration as their running configuration after the software installation job completes, uncheck the **Installation Options** check box.

Step 7 From the menu bar, choose **File > Deploy** to save the change to the job schedule.

Configuring File Servers

Figure 13-3 shows the File Servers content pane.

Figure 13-3 File Servers Content Pane



This section includes the following topics:

- Adding a File Server, page 13-14
- Changing a File Server, page 13-15
- Deleting a File Server, page 13-15

Adding a File Server

You can add a file server to Cisco DCNM.

BEFORE YOU BEGIN

Gather the following information about the file server:

- Server IP address or hostname

  Note If you use the hostname, it must be registered with the DNS server that the Cisco DCNM server is configured to use.

- Transfer protocol that the server provides. Cisco DCNM supports the following transfer protocols:
  - FTP
  - SFTP
  - TFTP
- Username and password that Cisco DCNM should use to access the server.
- The base directory on the server. All files and directories that Cisco DCNM needs to access must be available under this directory.

DETAILED STEPS

To add a file server, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > File Servers**.

The Contents pane displays a table of file servers.

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

A new row appears in the Contents pane, with the cursor in the Server Name/IP Address field.

Step 3 In the Server Name/IP Address field, enter the IP address or hostname of the file server.

Step 4 Double-click the **Protocol** field and choose the protocol from the list that appears. Supported protocols are as follows:

- FTP
- SFTP
- TFTP

Step 5 If the file server requires authentication, double-click the **User Credentials** field and enter the username and password for the server. If you want Cisco DCNM to remember the password, check the **Save Password** check box.

Step 6 Double-click the Base Directory field.

The Software Image Browser dialog box appears.

Step 7 Explore the server file system and choose the directory that Cisco DCNM should use as the base directory. All files and directories that Cisco DCNM needs to access must be located under this directory. By default, the root directory of the server is the base directory.

Step 8 (Optional) Double-click the Comment field and enter your comments.

Step 9 From the menu bar, choose **File > Deploy** to save the change to the job schedule.

Changing a File Server

You can change the user credentials, base directory, and comments of a file server.

Note You cannot change the values in the Server Name/IP Address or Protocol fields. If you need to change these values, delete the file server and create a file server with the new values.

BEFORE YOU BEGIN

If you are changing the user credentials or base directory, determine what the new user credentials or base directory should be.

DETAILED STEPS

To change a file server, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > File Servers**.

The Contents pane displays a table of file servers.

Step 2 In the table, locate the row for the file server that you want to change.

Step 3 Perform the following items to change the file server entry as needed:

- If you want to change the user credentials, double-click the User Credentials field for the file server and enter or clear the username and password for the server. If you want Cisco DCNM to remember the password, check the **Save Password** check box.
- If you want to change the base directory, double-click the Base Directory field and use the Software Image Browser dialog box to choose the directory that Cisco DCNM should use as the base directory.
- If you want to change the comments, double-click the Comments field and enter your comments.

Step 4 From the menu bar, choose **File > Deploy** to save the file server changes.

Deleting a File Server

You can delete a file server.

BEFORE YOU BEGIN

Ensure that the file server is specified in the Archival Settings feature as the file server for configuration rollback. For more information, see the "Configuring the Rollback File Server Setting" section on page 14-19.

DETAILED STEPS

To delete a file server, follow these steps:

Step 1 From the Feature Selector pane, choose **Device OS Management > File Servers**.

The Contents pane displays a table of file servers.

Step 2 In the table, click the row for the file server that you want to delete.

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

Note If the file server is specified in the Archival Settings feature as the file server for a configuration rollback, a dialog box informs you that the file server cannot be deleted. For more information, see the "Configuring the Rollback File Server Setting" section on page 14-19.

The file server is removed from the summary pane. You do not need to save your changes.

Field Descriptions for Device OS Management

This section includes field descriptions for the three features available in the Feature Selector drawer for Device OS Management:

Field Descriptions for Device OS Management

This section includes the following field descriptions for the Device OS Management feature:

Device: Details: System Section

Table 13-1 Device: Details: System Section

Field	Description
System	
Device Name	*Display only.* Name of the managed device.
IP Address	*Display only.* IP address that Cisco DCNM uses to connect to the managed device.
Model	*Display only.* Hardware model name of the managed device.
Redundancy Supervisor	*Display only.* Whether the device has a secondary supervisor module.

Table 13-1 Device: Details: System Section (continued)

Field	Description
Software	
System Version	*Display only.* Release number of the system image currently installed on the managed device.
System Image	*Display only.* Filename of the system image currently installed on the managed device.
Kickstart Image	*Display only.* Filename of the kickstart image currently installed on the managed device.

Device: Details: Software Installation Jobs Section

Table 13-2 Device: Details: Software Installation Jobs Section

Field	Description
Job ID	*Display only.* Identification number of the job.
Owner	*Display only.* Cisco DCNM user who created the installation job.
Software Image and Version	*Display only.* Name of the system image specified in the job.
Scheduled At	*Display only.* Date and time that the installation job is scheduled to occur.
Completed At	*Display only.* Date and time that the installation job occurred. If the job has not completed, this field is blank.
Status	*Display only.* Status of the installation job. If the job is ongoing, failed, or successful, you can expand the status and see more information about the job.
Comment	*Display only.* Text of any comments added to the installation job.

Field Descriptions for Software Installation Jobs

This section includes the following field descriptions for the Software Installation Jobs feature:

- Installation Job: Details: General Section, page 13-17
- Installation Job: Details: Devices and Software Images Section, page 13-18

Installation Job: Details: General Section

Table 13-3 Installation Job: Details: General Section

Field	Description
General	
Job ID	*Display only.* Identification number of the job.
Owner	*Display only.* Cisco DCNM user who created the installation job.

Table 13-3 Installation Job: Details: General Section (continued)

Field	Description
Scheduled At	Date and time that the installation job is scheduled to occur. If the job has not yet occurred, this field is configurable.
Completed At	*Display only.* Date and time that the installation job occurred. If the job has not completed, this field is blank.
Status	*Display only.* Status of the installation job.
Comment	Text entered by Cisco DCNM users.
Installation Options	
Installation Options	Whether the installation job affects the startup configuration. By default, this check box is unchecked.
Save Running Configuration to Startup before Installation	Specifies that the installation job copies the running configuration of each device in the job to its startup configuration prior to installing the software image.
Erase Startup Configuration before Installation	Specifies that the installation job erases the startup configuration of each device in the job prior to installing the software image.

Installation Job: Details: Devices and Software Images Section

Table 13-4 Installation Job: Details: General Section

Field	Description
Device	*Display only.* Name of the managed device.
Platform	*Display only.* Hardware model name of the managed device.
Kickstart Image	*Display only.* Filename of the kickstart image currently installed on the managed device.
System Image	*Display only.* Filename of the system image currently installed on the managed device.

Field Descriptions for the File Servers Contents Pane

Table 13-5 File Servers Contents Pane

Field	Description
Server Name/IP Address	DNS name or IP address of the file server. If you use the file server in a software installation job, ensure that devices in the job can connect to the name or address that you specify. This field is editable only when you create the file server entry. You cannot edit it after saving your changes to the Cisco DCNM server.

Table 13-5 File Servers Contents Pane (continued)

Field	Description
Protocol	Transfer protocol supported by the server. Valid values are as follows: • FTP • SFTP • TFTP This field is editable only when you create the file server entry. You cannot edit it after saving your changes to the Cisco DCNM server.
User Credentials	Username and password required to access the file server.
Base Directory	Directory that Cisco DCNM should consider as the root directory on the server. Directories specified for software installation jobs using this server will be relative to this directory.
Comment	Text entered by Cisco DCNM users.

Additional References

For additional information related to the Device OS Management feature, see the following sections:

- Related Documents, page 13-20
- Standards, page 13-20

Related Documents

Related Topic	Document Title
Upgrading and downgrading Cisco NX-OS software using the command-line interface on Nexus 7000 series switches.	*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.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 Device OS Management

Table 13-6 lists the release history for this feature.

Table 13-6 Feature History for Device OS Management

Feature Name	Releases	Feature Information
Device OS Management	4.2(1)	No change from Release 4.1
Device OS Management	4.1(2)	This feature was introduced.
Software Installation Jobs	4.1(2)	This feature was introduced.
File Servers	4.1(2)	This feature was introduced.

CHAPTER 14

Working with Configuration Change Management

This chapter describes how to use the Configuration Change Management feature.

This chapter includes the following sections:

Information About Configuration Change Management

The Configuration Change Management feature allows you to keep an archive of configurations from managed Cisco Nexus 7000 Series devices. You can view and compare archived configurations. You can roll back the running configuration of a managed device to any archived configuration version available for the device in Cisco Data Center Network Manager (DCNM).

This section includes the following topics:

Version Browser

The Version Browser feature allows you to see information about archived configurations, view and compare specific configuration versions, and merge changes from one configuration version to another. After you modify a configuration by merging changes, you can save the modified configuration as a text file on a file system available to the computer that you are using to run the Cisco DCNM client.

From the Version Browser, you can initiate a configuration rollback for a device, using any of the archived configurations available in Cisco DCNM for the device. Cisco DCNM uses the rollback feature available in Cisco NX-OS. For more information about the Cisco NX-OS rollback feature, see the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.x*.

Archival Jobs

The Archival Jobs feature allows you to control the automated archival of the running configuration on managed devices. You can add, edit, and delete custom archival jobs. A job consists of settings that determine when the job runs and a list of managed devices included in the job. You can choose to archive configurations at a regular interval, at a scheduled time on selected days, or whenever Cisco DCNM detects configuration changes on a device. You can also comment on a job.

The Default archival job always exists. You cannot delete it. By default, it is disabled.

Devices can be assigned to one archival job only. If you assign a device to an archival job, Cisco DCNM removes the device from the job that it was previously assigned to.

If a managed device is not assigned to a custom archival job, Cisco DCNM automatically assigns it to the Default archival job.

Archival Settings

The Archival Settings feature allows you to configure settings related to configuration change management, including the number of configuration versions that Cisco DCNM stores for each managed device, how many rollback and archival history entries Cisco DCNM stores for each managed device, and which file server Cisco DCNM uses during a configuration rollback.

Virtualization Support

Cisco DCNM treats each virtual device context (VDC) on a Cisco NX-OS device as a separate device; therefore, Cisco DCNM archives the running configurations of each VDC provided that Cisco DCNM has successfully discovered the VDC and views it as a managed device.

Licensing Requirements for Configuration Change Management

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Configuration Change Management requires a LAN Enterprise license. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the "Installing Licenses" section on page 2-11.

Prerequisites for Configuration Change Management

The Configuration Change Management feature has the following prerequisites:

- The Configuration Change Management feature supports only devices that are managed by Cisco DCNM, which means that Cisco DCNM must have successfully discovered the device.
- The Configuration Change Management feature supports only devices that you have added to the list of Cisco DCNM-licensed devices.
- Devices must be reachable by Cisco DCNM when Cisco DCNM attempts to archive the configuration or to perform a configuration rollback. An archival job or configuration rollback fails if the device is unreachable by Cisco DCNM.

Guidelines and Limitations for Configuration Change Management

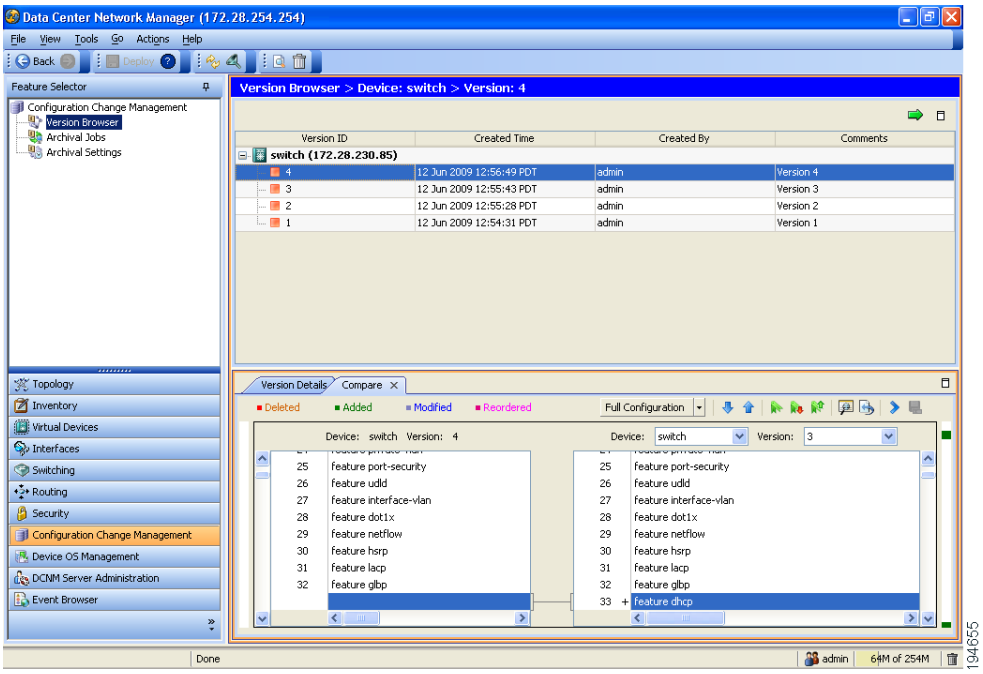
Configuration Change Management has the following configuration guidelines and limitations:

- You can archive a maximum of 50 configuration versions per managed device.
- Configure archival jobs and archival settings based upon the needs of your organization.
- We recommend enabling the Default archival job and configuring the job to run at the lowest frequency that your backup policy tolerates.
- Access to archived configurations is supported through the Cisco DCNM client only. The client provides features for viewing, comparing, and deleting archived configurations. Each archived configuration is marked with the date and time that Cisco DCNM archived the configuration. For more information, see the "Working with the Version Browser" section on page 14-4.

Working with the Version Browser

Figure 14-1 shows the Version Browser content pane.

Figure 14-1 Version Browser Content Pane



This section includes the following topics:

Viewing the Archival Status of a Device

You can view the archival status of a device. The archival status for a device includes the following information:

- Whether the archival job that includes the device is enabled or disabled.
- The schedule for the archival job that includes the device.
- The Job ID of the archival job that includes the device.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

DETAILED STEPS

To view the archival status of a device, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Click the device that has the archival status that you want to view.

The Details pane displays archive-related information about the device, including an Archival Status section.

If the archival job that includes the device is enabled, a View Schedule link appears.

If the archival job that includes the device is disabled, a Enable Archival Schedule link appears.

Step 3 (Optional) If you want to view the details of the archival job that includes the device, click the **View Schedule** link or the **Enable Archival Schedule** link. For more information, see the "Viewing Details of an Archival Job" section on page 14-17.

Viewing the Archival History of a Device

You can view the archival history of a device. The archival history records each attempt to create a new archival configuration version from the current running configuration of a device.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

DETAILED STEPS

To view the archival history of a device, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Click the device that has archival history that you want to view.

The Details pane displays archive-related information about the device, including an Archival History section.

Step 3 (Optional) If necessary, click the Archival History section to expand it.

The Archival History section displays a table of information about every attempt made to create a new archival configuration version for the device.

Browsing and Commenting on Configuration Versions

You can browse the archived configuration versions for managed devices. Browsing allows you to see information about all versions of an archived configuration.

You can also add, change, or delete comments on any version of an archived configuration.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

The archived configuration versions that you want to browse or comment on must exist in Cisco DCNM.

DETAILED STEPS

To browse and comment on configuration versions, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Double-click the device that has archived configuration versions that you want to browse.

A list of archived configuration versions appears below the device that you double-clicked. For each version, the Summary pane shows the version ID, the date and time that Cisco DCNM created the version, the Cisco DCNM user who created the version, and comments about the version.

Step 3 (Optional) If you want to comment on a version, follow these steps:

a. Click the version that you want to update with comments.

The Details pane shows the Version Details tab, which contains the same information about the version that appears in the Summary pane, except that the Comments box is available for you to use.

b. Click in the **Comments** box and enter your comments.

c. From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

Archiving the Current Running Configuration of a Device

You can archive the current running configuration of a managed device.

Archiving the current running configuration succeeds only if the most recent archived version in Cisco DCNM is different than the current running configuration.

BEFORE YOU BEGIN

The device must be managed and reachable.

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

DETAILED STEPS

To archive the current running configuration of a managed device, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Click the device that has a running configuration that you want to archive now.

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

Step 4 To confirm that Cisco DCNM successfully archived the configuration, view the list of archived configuration versions for the device. If necessary, double-click the device to open the list. The new version should appear at the top of the list.

Note If a message box notifies you that archiving the configuration was skipped, then Cisco DCNM did not detect differences between the current running configuration and the most recent archived configuration version for the device. To close the message box, click **OK**.

Viewing an Archived Configuration Version

You can view a version of an archived configuration.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

The archived configuration version that you want to view must exist in Cisco DCNM.

DETAILED STEPS

To view a version of an archived configuration, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Click the device that has an archived configuration version that you want to view.

Step 3 (Optional) If necessary, to view the list of archived configuration versions for the device, double-click the device.

Step 4 Click the version of the archived configuration that you want to view.

Step 5 From the menu bar, choose **Actions > View Configuration**.

In the Details pane, the Configuration tab displays the configuration version that you selected.

Tip You can search the text of the configuration. To do so, press **Ctrl + F**.

Comparing Configuration Versions

You can compare two configuration versions. The configurations that you can compare can be any two archived configuration version in Cisco DCNM, including archived configurations from different managed devices. You can also compare an archived configuration version to the running configuration or the startup configuration of a managed device.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

If you are comparing archived configuration versions, the two versions must exist in Cisco DCNM.

If you are comparing an archived configuration version to a running configuration or startup configuration on a managed device, the device must be reachable by Cisco DCNM.

DETAILED STEPS

To compare an archived configuration version to another configuration version, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Double-click the device that has an archived configuration version that you want to compare to another configuration version.

Step 3 (Optional) If necessary, to view the list of archived configurations for the device, double-click the device.

Step 4 Click the archived configuration version that you want to compare to another configuration version.

Step 5 Use the following table to compare the selected version to the configuration version that you want:

To Compare With	Follow These Steps
Most recent configuration version from the current device	Right-click the version and choose **Compare with > Latest**.
Next configuration version from the current device	Right-click the version and choose **Compare with > Next**.
Previous configuration version from the current device	Right-click the version and choose **Compare with > Previous**.

To Compare With	Follow These Steps
Another configuration version that you select	1. Press and hold the **Ctrl** key. 2. Click the archived configuration version that you want to compare the first selected version to, and then release the **Ctrl** key. 3. Right-click either selected configuration version and choose **Compare with > Selected Versions**. The selected configuration versions appear in the two configuration panes on the Compare tab. The configuration version that is listed highest in the Summary pane appears in the left configuration pane. **Tip** You can select archived configuration versions from different devices.
Current running configuration from the current device	Right-click the version and choose **Compare with > Current Running Configuration**.
Current startup configuration from the current device	Right-click the version and choose **Compare with > Current Startup Configuration**.
A configuration version from another device	1. Right-click the version and choose **Compare with > Another Device Configuration Version**. In the Details pane, the Compare tab shows the selected configuration version in the left configuration pane. 2. From the Device list above the right configuration pane, choose the device that has the configuration version that you want to compare with the configuration in the left pane. 3. From the Version list, pick the configuration version that you want to compare. You can use any version archived by Cisco DCNM or you can use the running configuration or the startup configuration currently on the device. 4. Click the icon. The right configuration pane displays the configuration version that you specified.

In the Details pane, the Compare tab displays the two configuration versions in side-by-side panes.

Step 6 Use the version comparison tools as needed. For more information, see the "Using the Version Comparison Tools" section on page 14-9.

Using the Version Comparison Tools

When you use the Version Browser to compare configuration versions, the Compare tab in the Details pane has many options to assist you with the comparison.

Note You must be comparing two configurations to use the version comparison tools. For more information, see the "Comparing Configuration Versions" section on page 14-8.

Use the options described in the following table to assist you compare two configuration versions.

Option Icon and Name	How to Use the Option
Full Configuration Full vs. Delta View	From the list, choose the desired viewing option, as follows: • Full Configuration—Shows all of both configuration versions. • Delta Configuration—Shows only the sections of each configuration that differ.
Next Diff	Click the icon to jump to the next difference between the two configurations shown.
Prev Diff	Click the icon to jump to the previous difference between the two configurations shown.
Bookmark	1. Click a line in one of the configuration panes. 2. Click the icon. A bookmark icon appears beside the line number.
Next Bookmark	1. Click the configuration pane that has the bookmarked line that you want to view. 2. Click the icon. The configurations in both panes jump to the next bookmarked line.
Prev Bookmark	1. Click the configuration pane that has the bookmarked line that you want to view. 2. Click the icon. The configurations in both panes jump to the previous bookmarked line.
Compare	Use this option to choose the archived configuration version shown in the right configuration pane. 1. From the Device list, choose the device that has the configuration version that you want to compare with the configuration in the left pane. 2. From the Version list, pick the configuration version that you want to compare. You can use any version archived by Cisco DCNM or you can use the running configuration or the startup configuration currently on the device. 3. Click the icon. The right configuration pane displays the configuration version that you specified.
Reset	Click the icon when you want to do the following: • Undo all configuration merges. • Remove all bookmarks. • Jump to the first line in both configuration panes. • Use the Full Configuration view.

Option Icon and Name	How to Use the Option
Merge	Use this option to copy a difference from the configuration in the left configuration pane into the configuration in the right pane. For detailed steps, see the "Merging Configuration Differences" section on page 14-11.
Save As	Click the icon to save the configuration in the right pane to a filename and location that you specify in the Save dialog box that appears.

Merging Configuration Differences

While you are comparing two configuration versions, you can merge lines that contain differences. The merge feature allows you to merge a whole line shown in the left configuration pane into the configuration that is shown in the right configuration pane.

BEFORE YOU BEGIN

You must be comparing two configuration versions that have differences.

Ensure that the configuration version that you want to want to merge the changes into appears in the right configuration pane.

DETAILED STEPS

To merge configuration differences, follow these steps:

Step 1 Use the icon and the icon as needed to jump to the line that you want to merge from the left configuration pane into the right configuration pane.

Tip The icon becomes available only when you use the icon and the icon to locate differences.

Step 2 Click the icon.

The selected configuration line in the left pane replaces the selected line in the right pane.

Step 3 Repeat Step 1 and Step 2 as often as needed.

Tip If you want to undo all merges, click the icon.

Step 4 (Optional) If you would like to save a copy of the configuration in the left pane as an ASCII text file, click the icon and use the Save dialog box to save the configuration to a filename and location that you specify.

Performing a Configuration Rollback

You can roll back the configuration of a managed device to any previous version that is archived by Cisco DCNM. A rollback replaces the running configuration of the managed device with an archived configuration version that you specify.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

The archived configuration version that you want to use in the rollback must exist in Cisco DCNM.

DETAILED STEPS

To perform a configuration rollback, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Click the device for which you want to perform a configuration rollback.

The Details pane displays archival information about the device, including a Rollback History section.

Step 3 (Optional) If necessary, to view the list of archived configurations for the device, double-click the device.

Step 4 Click the version of the archived configuration that you want to use as the running configuration on the device.

Step 5 Do one of the following:

- If you want to save the configuration version that you selected as the startup configuration on the device, choose one of the following rollback options:
  - If you want Cisco DCNM to restore the original running configuration of the device if any configuration command fails during the rollback, from the menu bar, choose **Actions > Rollback and Save as Start-up > Restore Original Config on Error (Atomic)**.
  - If you want Cisco DCNM to ignore configuration errors during a rollback, from the menu bar, choose **Actions > Rollback and Save as Start-up > Skip Errors and Rollback (Best Effort)**.
  - If you want Cisco DCNM to stop the rollback at the first configuration error, from the menu bar, choose **Actions > Rollback and Save as Start-up > Stop Rollback at First Error**.
- If you want the rollback to proceed without affecting the startup configuration currently on the device, choose one of the following rollback options:
  - If you want Cisco DCNM to restore the original running configuration of the device if any configuration command fails during the rollback, from the menu bar, choose **Actions > Rollback > Restore Original Config on Error (Atomic)**.
  - If you want Cisco DCNM to ignore configuration errors during a rollback, from the menu bar, choose **Actions > Rollback > Skip Errors and Rollback (Best Effort)**.
  - If you want Cisco DCNM to stop the rollback at the first configuration error, from the menu bar, choose **Actions > Rollback > Stop Rollback at First Error**.

Cisco DCNM begins the rollback operation.

Viewing the Rollback History of a Device

You can view the rollback history of a device.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

DETAILED STEPS

To view the rollback history of a device, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Click the device for which you want to view the rollback history.

The Details pane displays archival information about the device, including a Rollback History section.

Step 3 (Optional) If necessary, double-click the Rollback History section to expand it.

In the Rollback History section, a table of rollback history events appears. If no configuration rollbacks have occurred on the device, the table is empty.

Deleting All Archived Configurations for a Device

You can delete all the archived configuration versions of a device.

Note You cannot delete a specific version of an archived configuration.

BEFOREYOU BEGIN

Be certain that you do not want any of the archived configuration version for the device. You cannot undo the deletion and the Cisco DCNM client does not confirm your choice to delete the archived configuration versions.

DETAILED STEPS

To delete all archived configurations for a device, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.

The Summary pane displays a table of devices.

Step 2 Click the device that has archived configurations that you want to delete.

Step 3 Verify that you clicked the correct device.

Note The next step deletes the archived configuration versions without confirming your choice.

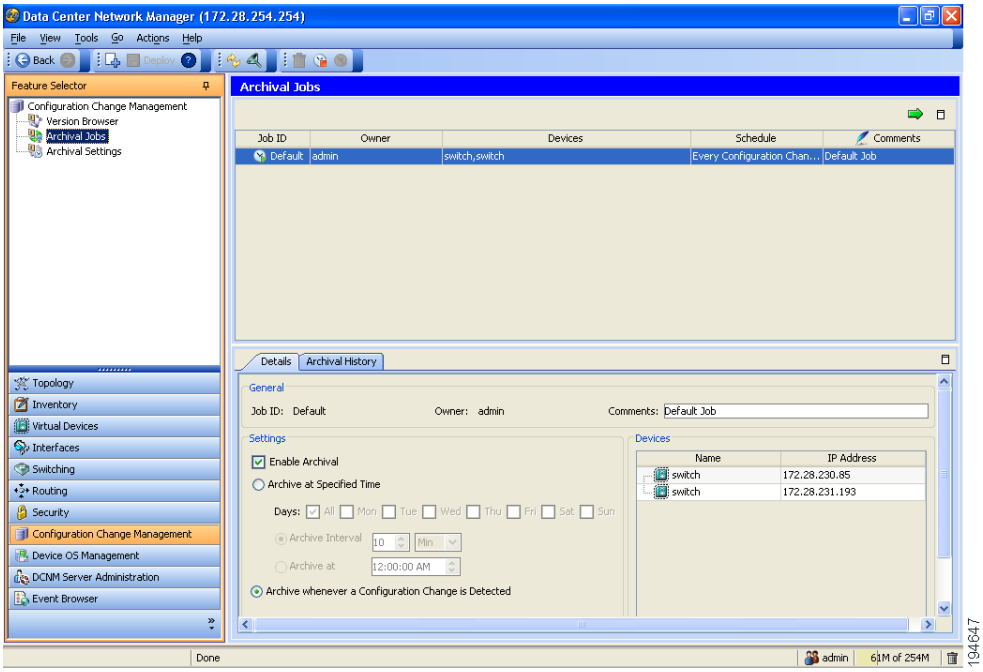
Step 4 From the menu bar, choose **Actions > Delete All Versions**.

The archived configurations for the selected device disappear from the Summary pane.

Configuring Archival Jobs

Figure 14-1 shows the Archival Jobs content pane.

Figure 14-2 Archival Jobs Content Pane



This section includes the following topics:

- Configuring an Archival Job, page 14-14
- Enabling and Disabling an Archival Job, page 14-16
- Deleting an Archival Job, page 14-16
- Viewing Details of an Archival Job, page 14-17
- Viewing the History of an Archival Job, page 14-17

Configuring an Archival Job

You can create an archival job or make changes to an existing archival job.

Note By default, a new archival job is enabled.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. You can include only licensed devices in an archival job.

DETAILED STEPS

To configure an archival job, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Archival Jobs**.

The Summary pane displays a table of archival jobs.

Step 2 Do one of the following:

- If you want to create an archival job, from the menu bar, choose **File > New Job**.
- If you want to make changes to an existing archival job, in the Summary pane, click the job that you want to change.

The Details pane shows the Details tab and Archival History tab for the job.

Step 3 (Optional) If necessary, in the Details pane, click the **Details** tab.

Step 4 (Optional) In the Comments field, enter your comments about the job.

Step 5 (Optional) If you want the job to archive configurations at a specific time, follow these steps:

a. Click the **Archive at Specified Time** radio button.

b. In the row of Days check boxes, check the check box for each day that you want the archival job to be active.

c. Do one of the following:

- If you want the job to archive configurations at a regular interval, click the **Archive Interval** radio button and use the adjacent box and list to specify the interval. You can specify an interval in minutes or hours. The maximum interval is either 59 minutes or 23 hours.
- If you want the job to archive configurations once on each day that the job is active, click the **Archive at** radio button and use the adjacent box to specify the time that you want the job to start.

Step 6 (Optional) If you want the job to archive configurations at any time that Cisco DCNM detects a change to the configuration of a device included in the job, click the **Archive whenever a Configuration Change is Detected** radio button.

Step 7 If you want to add one or more devices to the archival job, follow these steps:

a. Under Device, right-click in a blank area and choose **Add New Device**.

A dialog box shows available and selected devices.

a. For each device that you want to add, under Available Devices, click the device and click **Add**.

Tip To add all devices to the job, click **Add All**.

b. Click **OK**.

The devices that you added appear under Devices.

Step 8 If you want to remove a device from an archival job, follow these steps:

a. Under Devices, click the device that you want to remove from the job.

b. Right-click the device and choose **Remove Device**.

The device that you removed no longer appears under Devices.

Step 9 From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.

If you created an archival job, it is enabled by default. If you changed an existing archival job, whether it is enabled or disabled does not change.

Enabling and Disabling an Archival Job

You can enable or disable any archival job.

DETAILED STEPS

To enable or disable an archival job, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Archival Jobs**.

The Summary pane displays a table of archival jobs. In the Job ID column, enabled jobs show a green triangle and disabled jobs show a red square.

Step 2 In the Summary pane, click the archival job that you want to enable or disable.

Step 3 Do one of the following:

- To enable the job, from the menu bar, choose **Actions > Enable**. The icon in the Job ID column changes to show a green triangle.
- To disable the job, from the menu bar, choose **Actions > Disable**. The icon in the Job ID column changes to show a red square.

You do not need to save your changes.

Deleting an Archival Job

You can delete an archival job but not the Default archival job. When you delete an archival job, any devices included in the deleted job are automatically added to the Default archival job.

BEFORE YOU BEGIN

At least one custom archival job must exist in Cisco DCNM. You cannot delete the Default archival job.

DETAILED STEPS

To delete an archival job, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Archival Jobs**.

The Summary pane displays a table of archival jobs.

Step 2 In the Summary pane, click the archival job that you want to delete.

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

The archival job disappears from the Summary pane.

Devices that were included in the deleted job are automatically added to the Default archival job.

You do not need to save your changes.

Viewing Details of an Archival Job

You can view the details of an archival job, which include the job ID, the owner of the job, comments about the job, the job schedule, and the devices included in the job.

DETAILED STEPS

To view the details of an archival job, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Archival Jobs**.

The Summary pane displays a table of archival jobs.

Step 2 In the Summary pane, click the archival job that has details that you want to view.

The Details pane displays information about the archival job, including a Details tab.

Step 3 (Optional) If necessary, in the Details pane, click the **Details** tab.

The Details pane displays information and settings for the archival job that you selected.

Viewing the History of an Archival Job

You can view the history of an archival job.

BEFORE YOU BEGIN

The archival job must have occurred at least once; otherwise, there are no archival history entries to view.

DETAILED STEPS

To view the history of an archival job, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Archival Jobs**.

The Summary pane displays a table of archival jobs.

Step 2 In the Summary pane, click the archival job that has archival history that you want to view.

The Details pane displays information about the archival job, including an Archival History tab.

Step 3 In the Details pane, click the **Archival History** tab.

The Details pane displays a list of archival history entries, ordered by the date and time when the entry occurred.

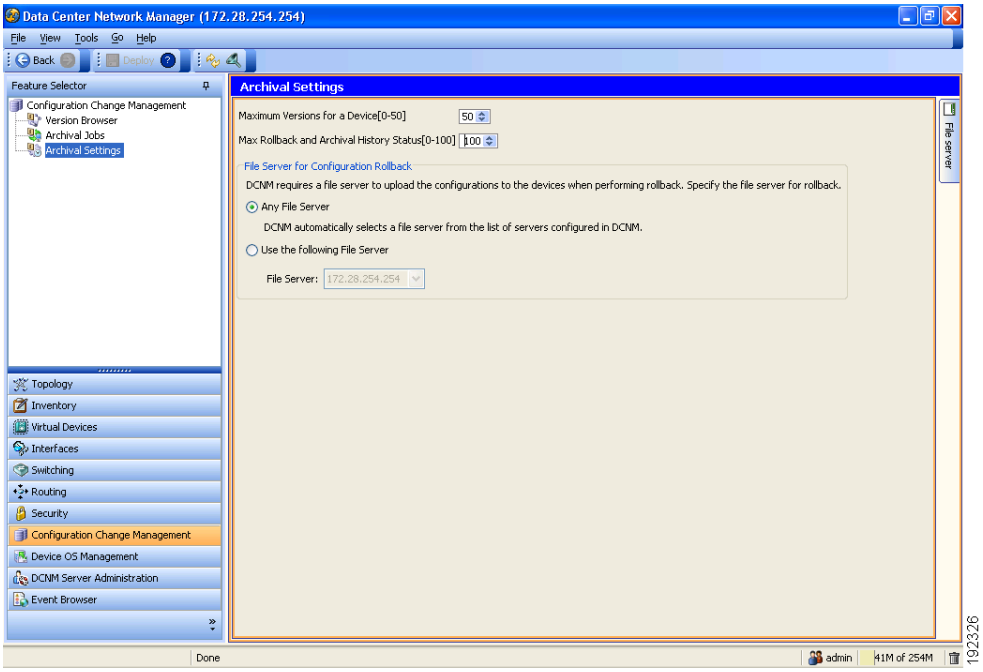
Step 4 (Optional) To see additional details about an archival history entry, in the Status column, click the plus symbol (+) to expand the entry.

The expanded entry lists information for each device included in the entry.

Configuring Archival Settings

Figure 14-3 shows the Archival Settings content pane.

Figure 14-3 Archival Settings Content Pane



This section includes the following topics:

- Configuring Version and History Settings, page 14-18
- Configuring the Rollback File Server Setting, page 14-19

Configuring Version and History Settings

You can configure the following settings about configuration versions and history:

- Maximum number of configuration versions that Cisco DCNM archives per managed device.
- Maximum number of rollback history and archival history status entries that Cisco DCNM retains per managed device.

DETAILED STEPS

To configure version and history settings, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Archival Settings**.

The Contents pane displays the Archival Settings fields.

Step 2 (Optional) Use the **Maximum Version for a Device [0 - 50]** box to configure the maximum number of configuration versions that Cisco DCNM should archive for each managed device.

Step 3 (Optional) Use the **Max Rollback and Archival History Status [0 - 100]** box to configure the maximum number of rollback history and archival history status entries that Cisco DCNM retains for each managed device.

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

Configuring the Rollback File Server Setting

You can configure whether Cisco DCNM uses a specific file server during a configuration rollback or whether it uses any available file server that you have configured.

BEFORE YOU BEGIN

You must configure at least one file server in Cisco DCNM. For more information, see the "Adding a File Server" section on page 13-14.

DETAILED STEPS

To configure the rollback file server settings, follow these steps:

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Archival Settings**.

The Contents pane displays the Archival Settings fields.

Step 2 (Optional) If you want Cisco DCNM to use any available file server during a configuration rollback, under File Server for Configuration Rollback, click the **Any File Server** radio button.

Step 3 (Optional) If you want to specify a file server that Cisco DCNM should use during a configuration rollback, follow these steps:

a. Under File Server for Configuration Rollback, click the **Use the following File Server** radio button.

b. From the File Server drop-down list, choose the file server.

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

Field Descriptions for Configuration Change Management

This section includes the field descriptions for the three features available in the Feature Selector drawer for Configuration Change Management:

- Field Descriptions for the Version Browser, page 14-20
- Field Descriptions for Archival Jobs, page 14-22
- Field Descriptions for the Archival Settings Contents Pane, page 14-23

Field Descriptions for the Version Browser

This section includes the following field descriptions for the Device OS Management feature:

- Device: Details: Archival Status Section, page 14-20
- Device: Details: Rollback History Section, page 14-20
- Device: Details: Archival History Section, page 14-21
- Version: Version Details Tab, page 14-21
- Version: Compare Tab, page 14-21

Device: Details: Archival Status Section

Table 14-1 Device: Details: Archival Status Section

Field	Description
Status	*Display only.* Whether the archival job that the device is assigned to is enabled or disabled.
Schedule	*Display only.* When the archival job that the device is assigned to is scheduled to occur.
Job ID	*Display only.* Identification number of the archival job that the device is assigned to.

Device: Details: Rollback History Section

Table 14-2 Device: Details: Rollback History Section

Field	Description
Time	*Display only.* Date and time that the rollback occurred.
Version	*Display only.* Configuration version that became the running configuration as a result of the rollback.
User	*Display only.* Username of the Cisco DCNM user who initiated the rollback.
Status	*Display only.* Whether the rollback succeeded or failed.

Device: Details: Archival History Section

Table 14-3 Device: Details: Archival History Section

Field	Description
Time Stamp	*Display only.* Date and time that the archival event occurred.
Job Id	*Display only.* Identification number of the archival job that created the archival event.
Status	*Display only.* Whether the archival event succeeded, failed, or was skipped.
Reason	*Display only.* Cause of a skipped or failed archival event.

Version: Version Details Tab

Table 14-4 Version: Version Details Tab

Field	Description
Config Version ID	*Display only.* Version identification number for the archived configuration version. Each archived configuration for a device receives a unique version ID.
Creation Time	*Display only.* Date and time that an archival job created the configuration version.
Created By	*Display only.* Username of the Cisco DCNM user who created the archival job that created the configuration version or the Cisco DCNM user who manually initiated the archival event that created the configuration version.
Comments	Text entered by a Cisco DCNM user.

Version: Compare Tab

Table 14-5 Version: Compare Tab

Field	Description
Device	Name of the managed device that the configuration version came from. In the left configuration pane, this field is display only. In the right configuration pane on the Compare tab, this field is configurable and you can select any managed device that you have added to the Cisco DCNM license.
Version	Configuration version ID of the archived configuration. In the left configuration pane, this field is display only. In the right configuration pane on the Compare tab, this field is a drop-down list with the following options: • Configuration version IDs—The numbers of the archived configuration versions currently available in Cisco DCNM. • Running-Configuration—The running configuration currently on the managed device selected in the Device field. • Start-up Config—The startup configuration currently on the managed device selected in the Device field.

Field Descriptions for Archival Jobs

This section includes the following field descriptions for the Archival Jobs feature:

- Archival Job: Details Tab, page 14-22
- Archival Job: Archival History Tab, page 14-22

Archival Job: Details Tab

Table 14-6 Archival Job: Details Tab

Field	Description
General	
Job ID	*Display only.* Identification number of the archival job.
Owner	*Display only.* Username of the Cisco DCNM user who created the archival job.
Comments	Text entered by Cisco DCNM users.
Settings	
Enable Archival	Whether the archival job is enabled. By default, this check box is unchecked.
Archive at Specified Time	Archival job occurs at the time specified by the Days and Archival Interval or Archive at fields.
Days	Days of the week that the archival job occurs. By default, the All check box is checked, which makes the individual day check boxes unavailable.
Archive Interval	Specifies that the archival job occurs at a regular interval, specified by the interval value box and the unit drop-down list, to the right of this radio button.
Archive at	Specifies that the archival job occurs once on each active day, at the time specified in the box to the right of this radio button.
Archive whenever a Configuration Change is Detected	Specifies that Cisco DCNM archives the running configuration of a device in the job when it detects that the running configuration of a device has changed.
Devices	
Name	Name of devices that are assigned to the archival job.
IP Address	IP address that Cisco DCNM uses to connect to the device.

Archival Job: Archival History Tab

Table 14-7 Installation Job: Details: General Section

Field	Description
Time	*Display only.* Date and time that the archival job ran.
Status	*Display only.* Number of devices in the job for which the archival job run succeeded, failed, or was skipped. The numbers are shown after each status, in parentheses.

Table 14-7 Installation Job: Details: General Section (continued)

Field	Description
Device Name	*Display only.* Name of a device assigned to the job. This field is shown when you expand the status of an archival history entry.
IP Address	*Display only.* IP address that Cisco DCNM used to attempt to connect to the device. This field is shown when you expand the status of an archival history entry.
Status (per Device)	*Display only.* Whether the archival job run succeeded, failed, or was skipped for the device.
Reason	*Display only.* Explanation for the status. For example, if the device was skipped because the running configuration had not changed since the previous archival job run, the following text appears in the Reason field: `Archival skipped as there are no changes from the previous version`

Field Descriptions for the Archival Settings Contents Pane

Table 14-8 Archival Settings Contents Pane

Field	Description
Maximum Versions for a Device	Largest number of archived configuration versions that Cisco DCNM retains for each device included in an archival job. Valid values are from 0 to 50, where 50 is the default value.
Max Rollback and Archival History Status	Largest number of rollback history and archival history status entries Cisco DCNM retains for each device.
File Server for Configuration Rollback	
Any File Server	Specifies that Cisco DCNM selects a file server to upload configurations to during a configuration rollback. Any file server that you have configured in Cisco DCNM may be used.
Use the following File Server	Specifies that Cisco DCNM uploads configurations during a configuration rollback to the file server that you specify in the File Server drop-down list.
File Server	IP address or DNS name of the file server that Cisco DCNM uploads configurations to during a rollback. This field is available only when you select the Use the following File Server radio button.

Additional References

For additional information related to configuration change management, see the following sections:

- Related Documents, page 14-24
- Standards, page 14-24

Related Documents

Related Topic	Document Title
File servers in Cisco DCNM	*File Servers, page 13-3*
Configuration rollbacks in Cisco NX-OS	*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.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 Configuration Change Management

Table 14-9 lists the release history for this feature.

Table 14-9 Feature History for Configuration Change Management

Feature Name	Releases	Feature Information
Configuration Change Management	4.2(1)	No change from Release 4.1
Version Browser	4.1(2)	This feature was introduced.
Archival Jobs	4.1(2)	This feature was introduced.
Archival Settings	4.1(2)	This feature was introduced.

CHAPTER 15

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, 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 15-4.

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.

This section includes the following topics:

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 "Installing Licenses" section on page 2-11.

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 "Cisco NX-OS Device Preparation" section on page 6-2.

Guidelines and Limitations for Auto-Synchronization with Devices

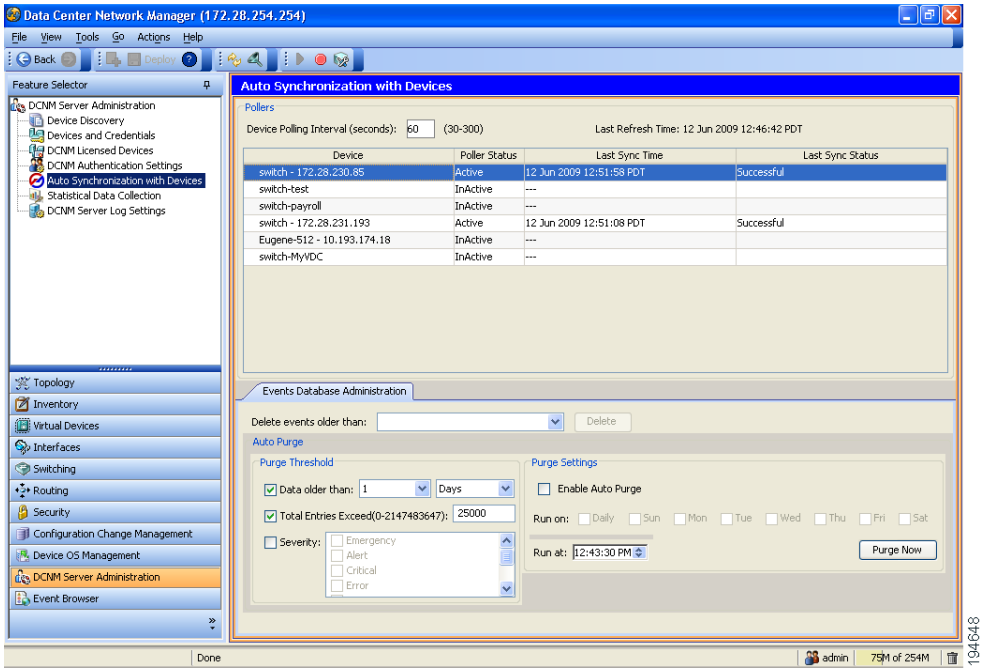
The Auto-Synchronization with Devices feature has the following configuration guidelines and limitations:

- 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 15-4.
- 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

Figure 15-1 shows the Auto-Synchronization with Devices content pane.

Figure 15-1 Auto-Synchronization with Devices Content Pane



This section includes the following topics:

- Starting and Stopping a Poller, page 15-4
- Configuring the Polling Interval, page 15-4
- Synchronizing with a Device, page 15-5
- Deleting Data from the Events Database, page 15-6

- Enabling and Disabling Automatic Event Purging, page 15-6
- Configuring Automatic Event Purge Settings, page 15-7
- Purging Events Now, page 15-8

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

To start or stop a poller, follow these 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.

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.

BEFORE YOU BEGIN

The default polling interval is 60 seconds.

Determine how often you want Cisco DCNM to perform auto-synchronization with managed devices. In general, 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

To configure the polling interval, follow these 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 7-5.

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 7-6.

DETAILED STEPS

To synchronize with a device, follow these 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 15-8.

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.

DETAILED STEPS

To delete data from the events database, follow these 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

To enable or disable automatic event purging, follow these 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.

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

To configure automatic event purge settings, follow these 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.

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 15-6.

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 15-7.

DETAILED STEPS

To purge events from the events database now, follow these 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 15-9.s

Field Descriptions for Auto Synchronization with Devices

This section includes the following field descriptions for the Auto Synchronization with Devices feature:

Summary Pane

Table 15-1 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 Content 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 15-2 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.

Table 15-2 Events Database Administration Tab (continued)

Field	Description
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.
Severity Levels	The 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 15-10
- Standards, page 15-11

Related Documents

Related Topic	Document Title
Events	*Chapter 10, "Managing Events"*
Device discovery	*Administering Device Discovery, page 6-1*

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 15-3 lists the release history for this feature.

Table 15-3 Feature History for Auto-Synchronization with Devices

Feature Name	Releases	Feature Information
Automatic purging based on event severity.	4.2(1)	Support was added.
Automatic purging of statistical data	4.1(2)	This feature was introduced.
Auto-Synchronization with Devices	4.1(2)	This feature was introduced.

CHAPTER 16

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 content 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 the Default Frequency of Statistical Data Retrieval" section on page 4-14.

This section includes the following topics:

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 "Installing Licenses" section on page 2-11.

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 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 "Cisco NX-OS Device Preparation" section on page 6-2.

Guidelines and Limitations for Statistical Data Collection

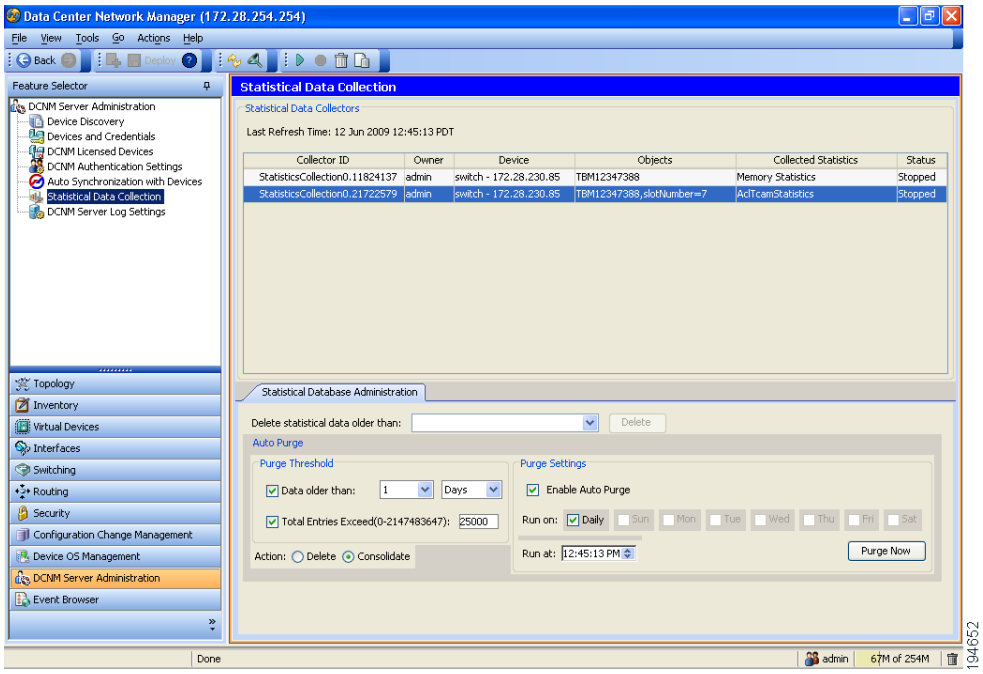
The Statistical Data Collection feature has the following configuration guidelines and limitations:

- Collections are created by starting monitoring for a new chart. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 4-11.
- 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

Figure 16-1 shows the Statistical Data Collection content pane.

Figure 16-1 Statistical Data Collection Content Pane



This section includes the following topics:

- Starting and Stopping Statistical Data Collection, page 16-4
- Deleting Statistical Data from a Collection, page 16-4
- Deleting a Collection, page 16-5

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

To start or stop a collection process, follow these 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.

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.

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

To delete statistical data from a collection, follow these 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 16-4.

BEFORE YOU BEGIN

Determine which collection of data you want to delete.

DETAILED STEPS

To delete a collection of statistical data from a device, follow these 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 16-5.

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

To delete data from the statistics database, follow these 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.

DETAILED STEPS

To enable or disable automatic statistical data purging, follow these 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

To configure automatic statistical data purge settings, follow these 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:

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 16-5.

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 16-6.

DETAILED STEPS

To purge statistical data from the statistical database now, follow these 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.

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 16-9.

Field Descriptions for Statistical Data Collection

This section includes the following field descriptions for the Statistical Data Collection feature:

Summary Pane

Table 16-1 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.

Statistical Database Administration Tab

Table 16-2 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 16-10
- Standards, page 16-11

Related Documents

Related Topic	Document Title
Device discovery	*Administering Device Discovery, page 6-1*

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 16-3 lists the release history for this feature.

Table 16-3 Feature History for Statistical Data Collection

Feature Name	Releases	Feature Information
Statistical Data Collection	4.2(1)	No change from Release 4.1
Automatic purging of statistical data	4.1(2)	This feature was introduced.
Statistical Data Collection	4.1(2)	This feature was introduced.

CHAPTER 17

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:

Logging Levels

The Cisco DCNM server supports a hierarchy of logging levels, ordered by 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 highest to 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 2003, INSTALL_DIR is C:\Program Files\Cisco Systems\Cisco 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 "Installing Licenses" section on page 2-11.

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.

Guidelines and Limitations for Administering DCNM Server Log Settings

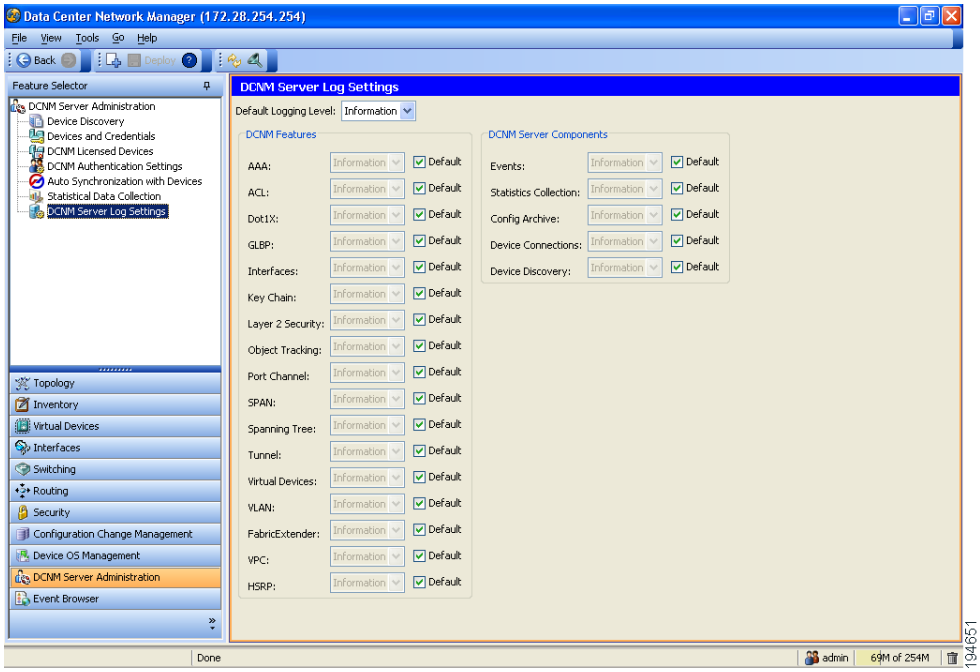
Administering Cisco DCNM server log settings has the following configuration guidelines and limitations:

- 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

Figure 17-1 shows the DCNM Server Log Settings content pane.

Figure 17-1 DCNM Server Log Settings Content Pane



This section includes the following topics:

- Configuring the Default Logging Level, page 17-4
- Configuring a Unique Logging Level for a Feature or Server Component, page 17-4
- Configuring a Feature or Server Component to Use the Default Logging Level, page 17-5

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 17-2.

DETAILED STEPS

To configure the default logging level for all Cisco DCNM features and server components, follow these 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.

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 17-2.

DETAILED STEPS

To configure a unique logging level for a feature or server component, follow these 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 17-2.

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 17-2.

DETAILED STEPS

To configure a feature or server component to use the default logging level, follow these 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 17-5.

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

Table 17-1 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 17-2.

Table 17-1 DCNM Server Log Settings Content Pane (continued)

Field	Description
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 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.
HSRP	Logging level for the HSRP feature.
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.

Table 17-1 DCNM Server Log Settings Content Pane (continued)

Field	Description
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 17-7
- Standards, page 17-7

Related Documents

Related Topic	Document Title
Troubleshooting Cisco DCNM	*Chapter 19, "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.	—

Feature History for DCNM Server Log Settings

Table 17-2 lists the release history for this feature.

Table 17-2 Feature History for DCNM Server Log Settings

Feature Name	Releases	Feature Information
DCNM Server Log Settings	4.2(1)	No change from Release 4.1.
DCNM Server Log Settings	4.1(2)	No change from Release 4.0.

CHAPTER 18

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

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

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:

- 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 15-2
- Automatic and Manual Purging of Statistical Data, page 16-2

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 4.2(1), you should only perform database restoration from a backup of Cisco DCNM Release 4.2(1).

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.

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 "Installing Licenses" section on page 2-11.

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 4.2(1), you should only perform database restoration from a backup of Cisco DCNM Release 4.2(1).

- 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.

Performing Database Maintenance

This section includes the following topics:

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

To back up the Cisco DCNM database, follow these 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 Windows, the default path to the bin directory is C:\Program Files\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.

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 the Cisco DCNM Server" section on page 2-19.

DETAILED STEPS

To clean the Cisco DCNM database, follow these 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 the Cisco DCNM Server" section on page 2-19.

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 Windows, the default path to the bin directory is C:\Program Files\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 18-8. 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 the Cisco DCNM Server" section on page 2-9.

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 4.2(1) database from a backup file created from a Cisco DCNM Release 4.2(1) 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

To restore the Cisco DCNM database from a backup file, follow these 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 the Cisco DCNM Server" section on page 2-19.

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 Windows, the default path to the bin directory is C:\Program Files\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 the Cisco DCNM Server" section on page 2-9.

Example

The following example from a 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

"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 18-10
- Standards, page 18-10

Related Documents

Related Topic	Document Title
Automatic purge of event data	*Chapter 10, "Managing Events"*
Automatic purge of statistical data	*Chapter 16, "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 18-1 lists the release history for this feature.

Table 18-1 Feature History for Cisco DCNM Database Maintenance

Feature Name	Releases	Feature Information
Database maintenance scripts	4.2(1)	Support was added for scripts to perform database backup, restore, and cleaning.

CHAPTER 19

Troubleshooting Cisco DCNM

This chapter describes some common issues you may experience while using Cisco Data Center Network Manager (DCNM), and provides solutions.

This chapter includes the following sections:

Initial Troubleshooting Checklist

Begin troubleshooting Cisco DCNM issues by checking the following issues first:

Checklist	Checkoff
Verify that you have a compatible version of Java installed. Java 1.5.0 is recommended.	❑
Verify that the necessary ports are open in your firewall if Cisco DCNM server is installed behind a firewall.	❑
Verify that you have installed the same version of the Cisco DCNM client and the Cisco DCNM server.	❑

Tips for Using Cisco DCNM

This section includes the following topics:

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.

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 Cisco DCNM Server Installation

This section includes the following topics:

Postgres Database Installation Fails

Check Table 19-1 for symptoms related to an installation failure of the Postgres database. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 19-1 Postgres Database Installation Fails

Symptom	Possible Cause	Solution
Postgres database installation fails.	The username specified to run the Postgres service already exists on the server.	Specify a different username or remove the existing username from the server.
	Antivirus software or intrusion detection software, such as Cisco Security Agent, blocked the installation.	Temporarily disable any antivirus software and intrusion detection software, and then reinstall Cisco DCNM.

Table 19-1 Postgres Database Installation Fails (continued)

Symptom	Possible Cause	Solution
The PostgresSQL installer shows the following message: `Failed to run initdb: 128`	(Windows only) Remote Desktop Connection client not running in console mode.	If you are installing Cisco DCNM on a supported Windows operating system and using Remote Desktop Connection (RDC) to access the Cisco DCNM server system, start RDC from a command prompt and use the /console option, as follows: `C:\>mstsc /console /v:server` where *server* is the DNS name or IP address of the Cisco DCNM server system.
The PostgresSQL installer shows the following message: `Failed to create process for initdb. The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.`	(Windows only) The Secondary Logon service is not running.	Verify that the Secondary Logon service is running. 1. On the Cisco DCNM server system, open the Control Panel and go to Administrative Tools > Services. 2. In the list of services, find the Secondary Logon service. 3. If the status of the Secondary Logon service is not Started, right-click the service and choose **Start**. 4. Close the Services window. 5. Restart the Cisco DCNM server installation.

Previous Installation Found When No Previous Installation Exists

Table 19-2 Previous Installation Found when No Previous Installation Exists

Symptom	Possible Cause	Solution
A message wrongly states that a previous installation exists.	The following file has incorrect entries regarding Cisco DCNM: `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`	1. Perform the steps in the "Editing the Zero G Registry File" section on page 19-3. 2. Install the Cisco DCNM server.

Editing the Zero G Registry File

You can edit the Zero G Registry file to remove incorrect entries, which may cause the installation of the Cisco DCNM server to fail.

Step 1 Make a backup of the .com.zerog.registry.xml file, found at the following location:

```
C:\Program Files\Zero G Registry\.com.zerog.registry.xml
```

Step 2 Open the file in a text editor.

Step 3 Within the <products> element, remove the following <product> element and all its descendant elements:

```
<product name="DCNM" id="9e458447-1ee6-11b2-85ed-d4ed684e9c05" version="4.0.0.0"
copyright="2007". . .
```

Step 4 Within the <components> element, remove every instance of the following <component> element:

```
<component id="9e458484-1ee6-11b2-860c-d4ed684e9c05" version="1.0.0.0"
name="InstallAnywhere VM Component" location="C:\Program Files\Cisco Systems\Cisco
DCNM\jre" vendor="Cisco Systems Inc."/>
```

Step 5 Save and close the file.

Path to the Perl Binary Directory Not Found

Check Table 19-1 for symptoms related to the Perl binary directory. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 19-3 Path to the Perl Binary Directory Not Found

Symptom	Possible Cause	Solution
An error message states that the path to the bin directory for Perl is not in the system PATH environment variable.	Perl is not installed on the server system.	1. Install a supported version of ActivePerl. For more information about ActivePerl, see the "Prerequisites for Installing the Cisco DCNM Server" section on page 2-2. 2. Ensure that the system PATH environment variable includes the path to the directory that contains the Perl executable. On Microsoft Windows, the default path to the ActivePerl bin directory is C:\Perl\bin. 3. Start the DCNM server installation again.
	The server system PATH environment variable does not include the path to the directory that contains the Perl executable.	1. Verify that a supported version of ActivePerl is installed on the server system. If not, install a supported version of ActivePerl. For more information about ActivePerl, see the "Prerequisites for Installing the Cisco DCNM Server" section on page 2-2. 2. Ensure that the system PATH environment variable includes the path to the directory that contains the Perl executable. On Microsoft Windows, the default path to the ActivePerl bin directory is C:\Perl\bin. 3. Start the DCNM server installation again.

Trouble with Starting the Cisco DCNM Server

This section includes the following topics:

Cisco DCNM Server Fails to Start

Check Table 19-4 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 19-4 Cisco DCNM Server Fails to Start

Symptom	Possible Cause	Solution
Cisco DCNM server fails to start.	The Postgres database did not install.	See the "Postgres Database Installation Fails" section on page 19-2.
	The Postgres service is not running.	Start the Postgres service: • In Windows Server 2003, choose **Start > All Programs > Postgres 8.2 > Start Service**. • In RHEL 4 AS, use the following command: **/DCNM/db/bin/DB start**
	The Postgres user credentials are incorrect.	Correct the Postgres user credentials and restart the Cisco DCNM server.
	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\server.log 2. Determine which application is using the port and stop or reconfigure the application. 3. Restart the Cisco DCNM server.

Trouble with the Cisco DCNM Database

This section includes the following topics:

- Trouble with a PostgreSQL Database, page 19-5
- Trouble with an Oracle Database, page 19-7

Trouble with a PostgreSQL Database

Check Table 19-5 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 19-5 pgAdmin III Errors

Symptom	Possible Cause	Solution
Error message states that the Cisco DCNM database does not exist.	The Cisco DCNM database name may 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 19-6.
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

To update the Cisco DCNM database name and username in pgAdmin III, follow these steps:

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.

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 19-6 for symptoms related using an Oracle database with Cisco DCNM. For each error message, see the possible cause and follow the corresponding solution.

Table 19-6 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.	Perform the steps in the "Increasing the SYSTEM Tablespace" section on page 19-9.

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.	Perform the steps in the "Increasing the Number of Sessions and Processes" section on page 19-9.

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.	Perform the steps in the "Increasing the Number of Open Cursors" section on page 19-10.

Information About the Oracle SQL*Plus Command-Line Tool

The Oracle database troubleshooting procedures in this chapter require the use of the SQL*Plus command-line tool. The SQL*Plus executable is typically installed in the bin directory under the Oracle home directory. In Microsoft Windows, the default location for the SQL*Plus executable is as follows:

C:\oraclexe\app\oracle\product\10.2.0\server\bin

In Linux, the default location for the SQL*Plus binary file is as follows:

/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin

Linux Environment Variables

If you are using Linux, before you use the SQL*Plus command-line tool, ensure that the ORACLE_HOME and ORACLE_SID environment variables are set to correct values. For example, if you are using Oracle 10g on Linux, the following commands set the environment variables to the default Oracle home directory and SID if you are using a bash shell:

```
export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
export ORACLE_SID=XE
```

Logging Into Oracle

Note Ensure that you know the database administrator username and password.

To log into the Oracle database by using the SQL*Plus command-line tool, follow these steps:

Step 1 Run the SQL*Plus executable.

A command prompt appears.

Step 2 Enter the **connect** command.

The Username prompt appears.

Step 3 Enter the database administrator username.

The Password prompt appears.

Step 4 Enter the password for the username that you specified.

For example, if the Oracle administrator username is system and the password is oracle, you would log in as follows:

```
Username: sys as sysdba
Password: oracle
```

For more information about using SQL*Plus, see the documentation for the Oracle database version that you are using.

Information About the init.ora File

The init.ora file specifies startup parameters. The default name and location of the file is platform specific, as shown in Table 19-7.

Table 19-7 Name and Default Location of init.ora File

Oracle Version	Operating System	Content of init.ora File
10g	Microsoft Windows	C:\oraclexe\app\oracle\product\10.2.0\server\database\initXE.ora
	Linux	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/dbs\initXE.ora
11g	Microsoft Windows	C:\app\Administrator\product\11.1.0\db_1\dbs\initORCL.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dbs/initORCL.ora

The init.ora file should contain only one line, which is the full path of the server parameter file, as shown in Table 19-8.

Table 19-8 Content of init.ora File

Oracle Version	Operating System	Content of init.ora File
10g	Microsoft Windows	SPFILE='C:\oraclexe\app\oracle\product\10.2.0\server\dbs\spfileXE.ora
	Linux	SPFILE='/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/dbs/spfileXE.ora'

Table 19-8 Content of init.ora File (continued)

Oracle Version	Operating System	Content of init.ora File
11g	Microsoft Windows	SPFILE='C:\oraclexe\app\oracle\product\11.1.0\server\dbs\spfileXE.ora
	Linux	SPFILE='/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dbs/spfileXE.ora

Increasing the SYSTEM Tablespace

To increase the SYSTEM tablespace, follow these steps:

Step 1 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the "Information About the Oracle SQL*Plus Command-Line Tool" section on page 19-7.

Step 2 Enter the following command:

```
select file_name, bytes, autoextensible, maxbytes
from dba_data_files
where tablespace_name='SYSTEM';
```

Step 3 Enter the following command:

```
alter database datafile 'file_name' autoextend on next 100m maxsize 2000m;
```

where *file_name* is the filename from the output of the **select** command in Step 2.

The SYSTEM tablespace is increased.

Step 4 Enter the **exit** command.

Increasing the Number of Sessions and Processes

To increase the number of sessions and processes to 150, follow these steps:

Step 1 Ensure that the init.ora file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines, remove them.

For more information, see the "Information About the init.ora File" section on page 19-8.

Step 2 Stop the Cisco DCNM server. For more information, see the "Stopping the Cisco DCNM Server" section on page 2-19.

Step 3 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the "Information About the Oracle SQL*Plus Command-Line Tool" section on page 19-7.

Step 4 Enter the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 5 Enter the following command:

```
startup pfile='init_file_name';
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the "Information About the init.ora File" section on page 19-8.

Step 6 Set the number of sessions to 150 by entering the following command:

```
alter system set sessions = 150 scope=spfile;
```

Step 7 Set the number of processes to 150 by entering the following command:

```
alter system set processes = 150 scope=spfile;
```

Step 8 Enter the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 9 Enter the **startup** command.

Step 10 Verify that the number of sessions and processes is changed to 150 by entering the following command:

```
show parameter sessions
```

Step 11 Enter the **exit** command.

Step 12 Start the Cisco DCNM server. For more information, see the "Starting the Cisco DCNM Server" section on page 2-9.

Increasing the Number of Open Cursors

To increase the number of open cursors to 1000, follow these steps:

Step 1 Ensure that the init.ora file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines in the file, remove them.

For more information, see the "Information About the init.ora File" section on page 19-8.

Step 2 Shut down the Cisco DCNM server. For more information, see the "Stopping the Cisco DCNM Server" section on page 2-19.

Step 3 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the "Information About the Oracle SQL*Plus Command-Line Tool" section on page 19-7.

Step 4 Enter the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 5 Enter the following command:

```
startup pfile='init_file_name';
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the "Information About the init.ora File" section on page 19-8.

Step 6 Set the number of open cursors to 1000 by entering the following command:

```
alter system set open_cursors = 1000 scope=spfile;
```

Step 7 Enter the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 8 Enter the **startup** command.

Step 9 Verify that the number of open cursors is changed to 1000 by entering the following command:

```
show parameter open_cursors
```

Step 10 Enter the **exit** command.

Step 11 Start the Cisco DCNM server. For more information, see the "Starting the Cisco DCNM Server" section on page 2-9.

Trouble with the Cisco DCNM Client

This section includes the following topics:

Cannot Download the Cisco DCNM Client from the Server

Check Table 19-9 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 19-9 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 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.
	You are using an unsupported web browser.	To download the Cisco DCNM client from the Cisco DCNM server, use Microsoft Internet Explorer 7 or Mozilla Firefox 3.0.

Cannot Install the Cisco DCNM Client

Check Table 19-9 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 19-10 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 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.
	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.

Cannot Start the Cisco DCNM Client

Check Table 19-11 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 19-11 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 3-5. 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 3-2.

Cannot Log into the Cisco DCNM Client

Check Table 19-12 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.

Table 19-12 Cannot Log into the Cisco DCNM Client

Symptom	Possible Cause	Solution
Cannot log into the Cisco DCNM client.	You forgot password.	Ask a Cisco DCNM administrator to reset your password. 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 "Reinstalling the Cisco DCNM Server" section on page 2-15.
	The Cisco DCNM server is down.	Restart the Cisco DCNM server. See the "Starting the Cisco DCNM Server" section on page 2-9.
	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. See the "Reinstalling the Cisco DCNM Server" section on page 2-15.
	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 "Reinstalling the Cisco DCNM Server" section on page 2-15. 3. Log into the Cisco DCNM client and specify the new IP address of the Cisco DCNM server in the Cisco DCNM Server field of the login dialog box.
	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 3-4. 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 "Reinstalling the Cisco DCNM Server" section on page 2-15.

Table 19-12 Cannot Log into the Cisco DCNM Client (continued)

Symptom	Possible Cause	Solution
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 19-13 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 19-13 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 the "Starting the Cisco DCNM Server" section on page 2-9.
	The Cisco DCNM server is unreachable.	Investigate your network to determine if it meets the network requirements for using the Cisco DCNM client remotely.

Trouble with Device Discovery or Device Status

Check Table 19-14 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 19-14 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 "Cisco NX-OS Device Configuration Requirements" section on page 1-5.

Trouble with Device Management

Check Table 19-11 for symptoms related to device management. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 19-15 Trouble with Device Management

Symptom	Possible Cause	Solution
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 7-5. • Restart the Cisco DCNM server with a clean database. If the server was down for a long time, this is the recommended solution.

Trouble with Device OS Management

Check Table 19-17 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 19-16 Trouble with Device OS Management

Symptom	Possible Cause	Solution
• During a software installation job, 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 "Creating or Editing a Software Installation Job" section on page 13-7.

Trouble with Event Browsing

Check Table 19-17 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 19-17 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 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 1-6.
	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 4-15.

Table 19-17 Trouble with Event Browsing

Symptom	Possible Cause	Solution
Too many events 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 7-5.
	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 1-6.
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 19-2.	Use the Event Browser to see status-related system messages received by Cisco DCNM. For more information, see the "Viewing the Event Browser" section on page 10-3.