



New and Changed Information

As of Cisco DCNM Release 5.2, Cisco Fabric Manager and Cisco Data Center Network Manager for LAN are merged into one unified product called Cisco Data Center Network Manager (DCNM) that can manage both LAN and SAN environments. As a part of this product merger, the name Cisco DCNM for SAN replaces the name Cisco Fabric Manager.

The following documentation changes support the merged Cisco DCNM product:

- Cisco DCNM product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for LAN.
- Cisco Fabric Manager product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for SAN.
- Cisco DCNM for SAN product documentation is now published to the Data Center Network Manager listing page on Cisco.com:
http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html
This URL is also the listing page for Cisco DCNM for LAN product documentation.
- Cisco Fabric Manager documentation for software releases earlier than Cisco DCNM Release 5.2, retains the name Cisco Fabric Manager and remains available at its current Cisco.com listing page:
http://www.cisco.com/en/US/products/ps10495/tsd_products_support_configure.html
You should continue to use the Cisco Fabric Manager documentation if you are using a release of Cisco Fabric Manager software that is earlier than Cisco DCNM Release 5.2.
- The name DCNM-SAN is used in place of Cisco DCNM for SAN in the user interface of Cisco Data Center Network Manager; likewise, the name DCNM-LAN is used in place of Cisco DCNM for LAN in the user interface. To match the user interface, the product documentation also uses the names DCNM-SAN and DCNM-LAN.
- The following new publications support both Cisco DCNM for LAN and DCNM for SAN, and address the new licensing model, the new installation process, and the new features of Cisco DCNM:
 - *Cisco DCNM Installation and Licensing Guide*
 - *Cisco DCNM Release Notes*

For a complete list of Cisco DCNM documentation, see the “Related Documentation” section in the Preface.

This chapter provides release-specific information for each new and changed feature in the *System Management Configuration Guide, Cisco DCNM for LAN, Release 6.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

Send document comments to dcnm-docfeedback@cisco.com

To check for additional information about Cisco Data Center Network Manager (DCNM) Release 6.x, see the *Cisco DCNM Release Notes, Release 6.x*.

[Table 1](#) summarizes the new and changed features for the *System Management Configuration Guide, Cisco DCNM for LAN, Release 6.x*, and tells you where they are documented.

Table 1 ***New and Changed Features for Release 6.x***

Feature	Description	Changed in Release	Where Documented
Configuration Delivery Template	Beginning with Cisco DCNM Release 6.1(1), you can create templates for use with template-sourced jobs.	6.1(1)	Chapter 9, “Using Configuration Delivery Management.”
Configuration Change Management	Support was extended to the Cisco Nexus 3000 Series switches.	5.2(1)	Chapter 8, “Working with Configuration Change Management”
Configuration Delivery Management - Template enhancements	Configuration delivery templates were enhanced in the Cisco DCNM client.	5.2(1)	Chapter 9, “Using Configuration Delivery Management”
Inventory	Support was extended to the Cisco Nexus 3000 Series switches.	5.2(1)	Chapter 3, “Working with Inventory”
Line Card Reload	You can individually restart any line card in the device without affecting the operational state of other components in the switch.	5.2(1)	Chapter 3, “Working with Inventory”
Module Pre-provisioning	You can pre-provision a new module or a module that is present on the switch but is in a offline state. This feature is only supported on the Cisco 5000 Series platform.	5.2(1)	Chapter 3, “Working with Inventory”
SPAN	Support was extended to the Cisco Nexus 3000 Series switches.	5.2(1)	Chapter 3, “Working with Inventory”
Switch Profiles	Support was extended for the Cisco Nexus 5000 Series switches.	5.2(1)	Chapter 8, “Working with Configuration Change Management”
Configuration Delivery Management	Configuration delivery templates are supported in the Cisco DCNM client.	5.1(1)	Chapter 9, “Using Configuration Delivery Management”
LLDP	You can configure Link Layer Discovery Protocol (LLDP) on individual interfaces on Cisco Nexus 5000 Series switches.	5.1(1)	Chapter 6, “Configuring LLDP”
Configuration Change Management	Support was extended to all managed Cisco Nexus Series switches.	5.0(2)	Chapter 8, “Working with Configuration Change Management”
Configuration Delivery Management	This feature was introduced.	5.0(2)	Chapter 9, “Using Configuration Delivery Management”
Device OS Management	Support was added for Cisco Nexus 4000 Series switches and Cisco Nexus 5000 Series switches.	5.0(2)	Chapter 7, “Managing Device Operating Systems”

Send document comments to dcnm-docfeedback@cisco.com

Table 1 ***New and Changed Features for Release 6.x (continued)***

Feature	Description	Changed in Release	Where Documented
LLDP	You can configure Link Layer Discovery Protocol (LLDP) in order to discover servers connected to your device.	5.0(2)	Chapter 6, “Configuring LLDP”
Power Usage	You can display power usage information for managed Cisco Nexus 7000 Series switches.	5.0(2)	Chapter 3, “Working with Inventory”
Virtual Switches	You can configure the virtual switch domain and server connections.	5.0(2)	Chapter 4, “Managing Virtual Switches”

For a complete list of Cisco DCNM documentation, see the “Related Documentation” in the Preface.

Send document comments to dcnm-docfeedback@cisco.com



Preface

This preface describes the audience, organization, and conventions of the *System Management Configuration Guide, Cisco DCNM for LAN, Release 6.x*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

- [Audience, page xvii](#)
- [Document Organization, page xvii](#)
- [Document Conventions, page xviii](#)
- [Related Documentation, page xviii](#)
- [Obtaining Documentation and Submitting a Service Request, page xx](#)

Audience

This publication is for experienced network administrators who configure and maintain Cisco DCNM.

Document Organization

This document is organized into the following chapters:

Chapter	Description
Chapter 1, “Overview”	Provides an overview of the features in this document.
Chapter 2, “Managing Events”	Describes how to use the Event Browser and feature-specific Events tabs.
Chapter 3, “Working with Inventory”	Describes how to use the Inventory feature.
Chapter 4, “Managing Virtual Switches”	Describes how to manage virtual switches.
Chapter 5, “Configuring SPAN”	Describes how to use the Switched Port Analyzer (SPAN) feature.
Chapter 6, “Configuring LLDP”	Describes how to configure Link Layer Discovery Protocol (LLDP).

Send document comments to dcnm-docfeedback@cisco.com

Chapter	Description
Chapter 7, “Managing Device Operating Systems”	Describes how to use the Device OS Management feature.
Chapter 8, “Working with Configuration Change Management”	Describes how to use the Configuration Change Management feature.
Chapter 9, “Using Configuration Delivery Management”	Describes how to use the Configuration Delivery Management feature.

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

This section contains information about the documentation available for Cisco DCNM and for the platforms that Cisco DCNM manages.

This section includes the following topics:

- [Cisco DCNM Documentation, page xviii](#)
- [Cisco Nexus 1000V Series Switch Documentation, page xix](#)
- [Cisco Nexus 2000 Series Fabric Extender Documentation, page xix](#)
- [Cisco Nexus 3000 Series Switch Documentation, page xx](#)
- [Cisco Nexus 4000 Series Switch Documentation, page xx](#)
- [Cisco Nexus 5000 Series Switch Documentation, page xx](#)
- [Cisco Nexus 7000 Series Switch Documentation, page xx](#)

Cisco DCNM Documentation

The 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 6.x

Send document comments to dcnm-docfeedback@cisco.com

Cisco DCNM

The following publications support both Cisco DCNM for LAN and DCNM for SAN, and address the new licensing model, the new installation process, and the new features of Cisco DCNM:

- *Cisco DCNM Fundamentals Guide, Release 6.x*
- *Cisco DCNM Installation Guide, Release 6.x*

Cisco DCNM for LAN Configuration Guides

FabricPath Configuration Guide, Cisco DCNM for LAN, Release 6.x

Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x

Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 6.x

Security Configuration Guide, Cisco DCNM for LAN, Release 6.x

System Management Configuration Guide, Cisco DCNM for LAN, Release 6.x

Unicast Configuration Guide, Cisco DCNM for LAN, Release 6.x

Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x

Virtual Device Context Quick Start, Cisco DCNM for LAN

Web Services API Guide, Cisco DCNM for LAN, Release 5.x

Cisco DCNM for SAN Configuration Guides

Fabric Configuration Guide, Cisco DCNM for SAN, Release 6.x

Fundamentals Configuration Guide, Cisco DCNM for SAN, Release 6.x

High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 6.x

Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 6.x

Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 6.x

Interfaces Configuration Guide, Cisco DCNM for SAN, Release 6.x

IP Services Configuration Guide, Cisco DCNM for SAN, Release 6.x

Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 6.x

Security Configuration Guide, Cisco DCNM for SAN, Release 6.x

SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 6.x

System Management Configuration Guide, Cisco DCNM for SAN, Release 6.x

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 2000 Series Fabric Extender Documentation

The Cisco Nexus 2000 Series Fabric Extender documentation is available at the following URL:

Send document comments to dcnm-docfeedback@cisco.com

http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

Cisco Nexus 3000 Series Switch Documentation

The Cisco Nexus 3000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Cisco Nexus 4000 Series Switch Documentation

The Cisco Nexus 4000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 5000 Series Switch Documentation

The Cisco Nexus 5000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Cisco Nexus 7000 Series Switch Documentation

The Cisco Nexus 7000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

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.



CHAPTER 1

Overview

This chapter describes the system management features that you can use to monitor and manage a Nexus environment using the Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

- [Events, page 1-1](#)
- [Inventory, page 1-1](#)
- [Virtual Switching, page 1-2](#)
- [SPAN, page 1-2](#)
- [LLDP, page 1-2](#)
- [Managing Device Operating Systems, page 1-2](#)
- [Configuration Change Management, page 1-2](#)
- [Configuration Delivery Management, page 1-2](#)

Events

The Event Browser and feature-specific Events tabs in Cisco DCNM enable you to view and manage recent status events. Events include status-related system messages that Cisco DCNM retrieves from managed devices and messages generated by the Cisco DCNM server.

Inventory

The Inventory feature displays information about the components that comprise a selected managed device and power usage information for managed Cisco Nexus 7000 Series switches. For information, see [Chapter 3, “Working with Inventory.”](#)

In addition, the Inventory feature allows you to configure fundamental system parameters on virtual switches, such as the Cisco Nexus 1000V Series switch. For information, see [Chapter 4, “Managing Virtual Switches.”](#)

Send document comments to dcnm-docfeedback@cisco.com

Virtual Switching

Cisco DCNM can be used to manage and display information about virtual switches, such as the Cisco Nexus 1000V Series switch, in your network. Managing a virtual switch involves configuring its domain and server connection.

SPAN

The switched port analyzer (SPAN) feature analyzes traffic between source ports on Cisco NX-OS devices. It operates by directing the SPAN session traffic to a destination port with an external analyzer attached to it. The sources and destinations to be monitored in SPAN sessions can be configured on the local device.

LLDP

Link Layer Discovery Protocol (LLDP) is a vendor-neutral, one-way device discovery protocol that allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other. LLDP can be enabled globally or per interface.

Managing Device Operating Systems

The Device OS Management feature controls the software images that are installed on Cisco DCNM-managed devices. It enables you to view software image details, create and manage software installation jobs that affect one or more managed devices, and configure file servers to transfer software images and back up device configurations.

Configuration Change Management

The Configuration Change Management feature maintains an archive of configurations from managed devices. It enables you to view and compare archived configurations as well as roll back the running configuration of a managed device to any archived configuration version available for the device.

Configuration Delivery Management

The Configuration Delivery Management feature enables you to create and schedule configuration delivery jobs. Each job can send device configuration commands to one or more devices.



CHAPTER 2

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, page 2-1](#)
- [Licensing Requirements for the Event Browser, page 2-2](#)
- [Prerequisites, page 2-2](#)
- [Guidelines and Limitations for the Event Browser, page 2-2](#)
- [Platform Support, page 2-3](#)
- [Using the Event Browser and Events Tabs, page 2-3](#)
- [Field Descriptions for Events, page 2-8](#)
- [Related Documents, page 2-10](#)
- [Feature History for the Event Browser and Events Tabs, page 2-10](#)

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 *Cisco DCNM Fundamentals Guide, Release 5.x*.
- 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.

Send document comments to dcnm-docfeedback@cisco.com


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 Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	The Event Browser 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites

The following prerequisites are required for using the Events feature on Cisco DCNM. For a full list of feature-specific prerequisites, see the platform-specific documentation:

- System-message logging levels for the Events feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.
- Managed Cisco NX-OS devices must be configured to send system messages to the Cisco DCNM server.

Guidelines and Limitations for the Event Browser

The Event Browser feature 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 DCNM Fundamentals Guide, Release 5.x*.

Send document comments to dcnm-docfeedback@cisco.com

- 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 *Cisco DCNM Fundamentals Guide, Release 5.x*.

Platform Support

The following platforms support this feature but may implement it differently. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 1000V Series switches	Cisco Nexus 1000V Series Switches Documentation
Cisco Nexus 2000 Series Fabric Extender	Cisco Nexus 2000 Series Fabric Extender Documentation
Cisco Nexus 4000 Series switches	Cisco Nexus 4000 Series Switches Documentation
Cisco Nexus 5000 Series switches	Cisco Nexus 5000 Series Switches Documentation
Cisco Nexus 7000 Series switches	Cisco Nexus 7000 Series Switches Documentation

Using the Event Browser and Events Tabs

This section includes the following topics:

- [Viewing the Event Browser, page 2-3](#)
- [Applying and Removing an Event Filter, page 2-5](#)
- [Viewing Events on an Events Tab, page 2-5](#)
- [Changing the Status of an Event, page 2-7](#)
- [Adding a Note to One or More Events, page 2-7](#)
- [Deleting an Event, page 2-8](#)

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.

DETAILED 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

Send document comments to dcnm-docfeedback@cisco.com

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: <ul style="list-style-type: none"> 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 2-5 .
Filter by Column Values	<ol style="list-style-type: none"> From the menu bar, choose View > Filter. The column headings become drop-down lists. 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	<p>In the Event Browser toolbar, enter the text that you want to use to filter the events.</p> <p>The Event Browser shows only the events that contain the text that you enter.</p> <p>Tip To configure quick filtering options, use the drop-down list of the Event Browser toolbar.</p>

- Step 4** (Optional) If you want to view details about a specific event, follow these steps:
- Find the event in the event list.
 - Click the event.
 - Expand the Details pane, if necessary.
Details about the selected event appear in the Details pane.
 - (Optional) To read notes and messages about status changes to the event, read the information in the Action Log field.

Send document comments to dcnm-docfeedback@cisco.com

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 *Cisco DCNM Fundamentals Guide, Release 5.x*).
- 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

Step 1 View events in the Event Browser (see the [“Viewing the Event Browser” section on page 2-3](#)).

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.

Send document comments to dcnm-docfeedback@cisco.com

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

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, Cisco DCNM cannot display events for the object that 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: <ul style="list-style-type: none">• 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	<ol style="list-style-type: none">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.

Send document comments to dcnm-docfeedback@cisco.com

- 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 2-3](#) or the [“Viewing Events on an Events Tab” section on page 2-5](#).

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 2-3](#) or the [“Viewing Events on an Events Tab” section on page 2-5](#).

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Select one or more events. Do one of the following: <ul style="list-style-type: none">• 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.

Send document comments to dcnm-docfeedback@cisco.com

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 *Cisco DCNM Fundamentals Guide, Release 5.x*.

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 2-3](#) or the [“Viewing Events on an Events Tab” section on page 2-5](#).

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 2-8](#)
- [Event Details, page 2-9](#)

Events Table

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

Send document comments to dcnm-docfeedback@cisco.com

Table 2-1 **Events Table**

Field	Description
Device	<i>Display only.</i> Name and IP address of the device that the event is related to.
Source	<i>Display only.</i> Where the event message originated. Sources are either a feature on a managed Cisco NX-OS device or the Cisco DCNM server.
Feature	<i>Display only.</i> Name of the Cisco NX-OS or Cisco DCNM server feature that the event pertains to.
Time	<i>Display only.</i> Date and time that the event occurred.
Severity	<i>Display only.</i> Severity of the event. Possible severities are as follows: <ul style="list-style-type: none"> • Emergency • Alert • Critical • Error • Warning • Notification • Informational • Debug
Message	<i>Display only.</i> Text of the event.
Annotation	Status of the event. Possible statuses are as follows: <ul style="list-style-type: none"> • 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 2-2 **Event Details**

Field	Description
Event Type	<i>Display only.</i> Type of the event. Event types are categories that describe the general nature of the event. Possible event types are as follows: <ul style="list-style-type: none"> • Communication • Environmental • Equipment • Processing Error • Quality of Service • Security • Unknown

Send document comments to dcnm-docfeedback@cisco.com

Table 2-2 **Event Details (continued)**

Field	Description
Action Log	Shows all actions taken on the event and all notes added to the event.
Life Cycle Type	<i>Display only.</i> Type of life cycle of the event. Possible life cycle types are as follows: <ul style="list-style-type: none"> • State Change • Attribute Value Change • Instance Creation • Instance Deletion • Informational

Related Documents

Related Topic	Document Title
Minimum required Cisco NX-OS logging levels	<i>Cisco DCNM Fundamentals Guide, Release 5.x</i>
Cisco DCNM server log settings	<i>Cisco DCNM Fundamentals Guide, Release 5.x</i>
Deleting events from the events database	<i>Cisco DCNM Fundamentals Guide, Release 5.x</i>
Cisco NX-OS system messages	<i>Cisco NX-OS System Messages Reference</i>

Feature History for the Event Browser and Events Tabs

Table 2-3 lists the release history for this feature.

Table 2-3 **Feature History for the Event Browser and Events Tabs**

Feature Name	Releases	Feature Information
Event Browser and Events tabs	5.2(1)	No change from Release 5.1.
Event Browser and Events tabs	5.1(1)	No change from Release 5.0.
Event Browser and Events tabs	5.0(2)	No change from Release 4.2.



CHAPTER 3

Working with Inventory

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

This chapter includes the following sections:

- [Information About Inventory, page 3-1](#)
- [Licensing Requirements for Inventory, page 3-3](#)
- [Prerequisites, page 3-3](#)
- [Platform Support, page 3-3](#)
- [Configuring Module Pre-Provisioning, page 3-3](#)
- [Reloading a Line Card, page 3-5](#)
- [Displaying Inventory Information, page 3-5](#)
- [Displaying Power Usage Information, page 3-8](#)
- [Field Descriptions, page 3-9](#)
- [Feature History for Inventory, page 3-11](#)

Information About Inventory

The Inventory feature displays information about the components that comprise a selected managed device and power usage information for managed Cisco Nexus 7000 Series switches. In addition, it allows you to configure fundamental system parameters on virtual switches, such as the Cisco Nexus 1000V Series switch. For information about configuring virtual switches, see [Chapter 4, “Managing Virtual Switches.”](#)

This section includes the following topics:

- [Understanding Inventory, page 3-1](#)
- [Understanding Power Usage, page 3-2](#)
- [Module Pre-Provisioning, page 3-2](#)

Understanding Inventory

The Inventory feature displays summary and detailed information about the chassis, modules, fan trays, and power supplies for managed devices.

Send document comments to dcnm-docfeedback@cisco.com

Understanding Power Usage

Cisco DCNM displays information about the power usage of managed Cisco Nexus 7000 Series switches, including an aggregation of the power usage for all managed Cisco Nexus 7000 Series switches, summary information for a specific device, and graphical information for a selected device.

You can configure Cisco DCNM to collect power usage statistics for up to six managed devices.

Module Pre-Provisioning



Note

This feature is supported only on the Cisco Nexus 5000 Series switches.

The pre-provisioning feature allows you to preconfigure interfaces before inserting or attaching a module to a Cisco Nexus 5000 Series switch. If a module goes offline, you can use pre-provisioning to make changes to the interface configurations for the offline module. When a pre-provisioned module comes online, the pre-provisioning configurations are applied. If any configurations were not applied, a syslog is generated. The syslog lists the configurations that were not accepted.

In some Virtual Port Channel (vPC) topologies, pre-provisioning is required for the configuration synchronization feature. Pre-provisioning allows you to synchronize the configuration for an interface that is online with one peer but offline with another peer.

Supported Hardware

The pre-provisioning feature supports the following hardware:

- N2K-C2148T Fabric Extender 48x1G 4x10G Module
- N2K-C2232P Fabric Extender 32x10G Module
- N2K-C2248T Fabric Extender 48x1G 4x10G Module
- N51-M16EP Cisco 16x10-Gigabit Ethernet Expansion Module
- N51-M8E8FP Cisco 8-port 1/2/4/8G FC and 8 Port 10-Gigabit Ethernet Expansion Module
- N5K-M1008 Cisco 8-port Fiber Channel Expansion Module 8 x SFP
- N5K-M1060 Cisco 6-port Fiber Channel Expansion Module 6 x SFP
- N5K-M1404 Expansion Module 4 x 10GBase-T LAN, 4 x Fiber Channel
- N5K-M1600 Cisco 6-port 10-Gigabit Ethernet SFP Module 6 x SFP

Upgrades and Downgrades

When upgrading from Cisco NX-OS Release 4.2(1)N2(1) and earlier releases to Cisco NX-OS Release 5.0(2)N1(1), there are no configuration implications. When upgrading from a release that supports pre-provisioning to another release that supports the feature including in-service software upgrades (ISSUs), pre-provisioned configurations are retained across the upgrade.

When downgrading from an image that supports pre-provisioning to an image that does not support pre-provisioning, you are prompted to remove pre-provisioning configurations.

Send document comments to dcnm-docfeedback@cisco.com

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 Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	Inventory 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites

The Inventory feature has the following prerequisite (for a full list of feature-specific prerequisites, see the platform-specific documentation):

- System-message logging levels for the Inventory feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Platform Support

The following platforms support this feature but may implement it differently. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 1000V Series switches ¹	Cisco Nexus 1000V Series Switch Documentation
Cisco Nexus 3000 Series switches	Cisco Nexus 3000 Series Switch Documentation
Cisco Nexus 4000 Series switches ¹	Cisco Nexus 4000 Series Switch Documentation
Cisco Nexus 7000 Series switches	Cisco Nexus 7000 Series Switch Documentation

1. The power usage feature is supported only on the Cisco Nexus 7000 Series switch.

Configuring Module Pre-Provisioning



Note

This feature is supported only on the Cisco Nexus 5000 Series switches.

Send document comments to dcnm-docfeedback@cisco.com

The module pre-provisioning feature allows you to pre-provision a new module or a module that is present on the switch but is in a offline state.

This section includes the following topics:

- [Pre-Provisioning Offline Modules, page 3-4](#)
- [Pre-Provisioning Online Modules, page 3-4](#)
- [Pre-Provisioning FEX Modules, page 3-5](#)

Pre-Provisioning Offline Modules



Note

This feature is supported only on the Cisco Nexus 5000 Series switches.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory**.
- The summary chassis information for each of the managed device is displayed in the Summary pane. You can view the list of offline modules already configured for pre-provisioning.
- Step 2** (Optional) From the Summary pane, in the Module Type drop-down list, choose the module type of the pre-provisioned slot you want to edit in the Details tab.
- Step 3** Choose a chassis.
- Step 4** Expand the chassis and click **Add New Provisioned Slot**.
- Step 5** (Optional) In the pre-provisioned slot, expand the chassis and click **Delete Slot**.
- The offline module is disabled.
-

Pre-Provisioning Online Modules



Note

This feature is supported only on the Cisco Nexus 5000 Series switches.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory**.
- The summary chassis information for each of the managed device is displayed in the Summary pane.
- Step 2** From the Summary pane, choose a chassis.
- Step 3** Expand the chassis and choose a card type that corresponds to the online module.
- Step 4** From the Details pane, click on the **pre-provisioning** drop-down list.
- You can enable or disable the pre-provisioning.
-

Send document comments to dcnm-docfeedback@cisco.com

Pre-Provisioning FEX Modules

**Note**

This feature is supported only on the Cisco Nexus 5000 Series switches.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory**.
The summary chassis information for each of the managed device is displayed in the Summary pane.
- Step 2** From the Summary pane, choose a FEX module.
- Step 3** Expand the FEX chassis and choose a card type that corresponds to the online module.
- Step 4** From the Details pane, click on the **pre-provisioning** drop-down list.
You can enable or disable the pre-provisioning.
-

Reloading a Line Card

**Note**

This feature is supported only on the Cisco Nexus 7000 Series device.

Beginning with Cisco DCNM Release 5.2(1), you can individually restart any line card in the device without affecting the operational state of other components in the switch.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory**.
The summary chassis information for each of the managed device is displayed in the Summary pane.
- Step 2** From the Summary pane, choose a chassis.
- Step 3** Expand the chassis and choose a card type.
- Step 4** Right-click the card type that you want and choose **Reload**.
A dialog box appears warning you that after the line card reload, the device will be rediscovered.
- Step 5** Click **Yes** or **No** to confirm your decision.
-

Displaying Inventory Information

The Inventory feature displays summary and detailed information about the chassis, modules, fan trays, and power supplies for managed devices.

This section includes the following topics:

- [Displaying the Chassis Information, page 3-6](#)

Send document comments to dcnm-docfeedback@cisco.com

- [Displaying the Module Information, page 3-6](#)
- [Displaying the Power Supply Information, page 3-7](#)
- [Displaying the Fan Tray Information, page 3-7](#)

Displaying the Chassis Information

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

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** To display additional information about a chassis, click the device.
Tabs appear in the Details pane with the Details tab selected.
- Step 3** Click one of the following tabs:
- **Details**—Displays detailed hardware and software information.
 - **Environmental Status**—Displays power usage and redundancy information.
 - **CPU Utilization**—Displays collected statistics showing the percentage of utilization devoted to user or kernel functions. For more information on collecting statistics for this feature, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.
 - **Memory Utilization**—Displays collected statistics showing the memory utilization within specific thresholds. For more information on collecting statistics for this feature, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.
 - **Events**—Displays the chassis events, which includes the source, time, severity, message, and status of the event. 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.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory**.
Summary chassis information, including module description, product ID, serial number, hardware version, software version, status, temperature, and events, for each managed device appears in the Summary pane.
- Step 2** From the Summary pane, expand the device.
The device listing expands to include a summary of each module, power supply, and fan tray in the chassis.

Send document comments to dcnm-docfeedback@cisco.com

Step 3 Click the module.

Tabs appear in the Details pane with the Details tab selected.

Step 4 Click one of the following tabs:

- **Details**—Displays general identification information and special information for the selected module type.
 - **Environmental Status**—Displays environmental status information for the selected supervisor module, I/O module, or fabric module. To see textual temperature information, expand the Temperature Status Table section. To see graphical temperature information, expand the Temperature Status Thermometer section.
 - **TCAM Statistics**—Displays collected information about TCAM usage on the module. For more information on collecting statistics for this feature, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.
 - **Events**—Displays event information for the selected supervisor module, I/O module, or fabric module. 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.

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, expand the device.

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

Step 3 Click the power supply.

Tabs appear in the Details pane with the Details tab selected.

Step 4 Click one of the following tabs:

- **Details**—Displays information including general identification information, power (watts), and current (Amps).
 - **Events**—Displays event information, including source, time, severity, message, and status information for the events. 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.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED 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.
A list of modules, power supplies, and fan trays appears under the device in the Summary pane. Each row includes summary information for the component.
- Step 3** Click a fan tray.
Tabs appear in the Details pane with the Details tab selected.
- Step 4** Click one of the following tabs:
- **Details**—Displays descriptive information and status for the fan tray.
 - **Events**—Displays event information including the source, time, severity, message, and status of the event. You can display details for each event.
-

Displaying Power Usage Information

Cisco DCNM displays summary and detailed information about the power usage for one or more managed devices in your network. It also displays the aggregated power usage information of all the managed Cisco Nexus 7000 Series switches. You can configure Cisco DCNM to collect power usage statistics for up to six managed devices.

This section includes the following topics:

- [Displaying Power Usage Summary Information, page 3-8](#)
- [Displaying Power Usage Details, page 3-9](#)
- [Displaying Power Usage Statistics, page 3-9](#)

Displaying Power Usage Summary Information

Cisco DCNM displays summary information about the total power capacity and the power drawn, allocated, and available for aggregated power usage information of all the managed Cisco Nexus 7000 Series devices and for each managed device.

DETAILED STEPS

To display power usage summary information, from the Feature Selector pane, choose **Inventory > Power Usage**. Aggregated power usage information for all managed Cisco Nexus 7000 Series switches and power usage information for each managed device displays in the Summary pane.

[Send document comments to dcnm-docfeedback@cisco.com](mailto:dcnm-docfeedback@cisco.com)

Displaying Power Usage Details

You can display graphical details about the power usage for one or more managed devices in your network. The graphical information includes bar and pie charts. The bar chart shows the total capacity (watts), total allocated (watts), and total drawn/usage (watts) for the top or bottom five devices based on the power consumed by the devices. The top five starts with the device that consumes the maximum power. The pie chart shows the total drawn/used power and unused power for the selected devices.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory > Power Usage**.
- Summary power usage information for the entire network and each managed device displays in the Summary pane.
- Step 2** From the Summary pane, click the entire network or one or more devices.
- The Details tab displays graphical details about the power usage for selected devices.
-

Displaying Power Usage Statistics

The following window appears in the Statistics tab:

- Power Usage Statistics Chart—Displays statistics on the total capacity (watts), total drawn (watts), total allocated (watts), and total available (watts) for up to six managed devices.

For more information on collecting statistics for this feature, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Field Descriptions

This section includes the following field descriptions for the Inventory and Power Usage features:

- [Inventory: Details: Hardware Section, page 3-9](#)
- [Inventory: Details: Software Section, page 3-10](#)
- [Inventory: Power Usage, page 3-10](#)

Inventory: Details: Hardware Section

Table 3-1 *Inventory: Details: Hardware Section*

Field	Description
Switch Name	Hostname assigned to the device.
Description	Word or phrase that describes the device.
Product ID	ID number for the device.
Serial Number	Serial number of the device.

Send document comments to dcnm-docfeedback@cisco.com

Inventory: Details: Software Section

Table 3-2 ***Inventory: Details: Software Section***

Field	Description
System Uptime	Date and time when the device was last uploaded.
System Image	
Image Name	Name of the image running on the device.
Location	Directory where the system image resides.
Version	Version number of the image running on the device.
Kickstart Image	
Image Name	Name of the kickstart image file.
Location	Directory where the kickstart image resides.
Version	Version number of the kickstart image file.

Inventory: Power Usage

Table 3-3 ***Inventory: Power Usage***

Field	Description
Name	Name of the device group or device.
Total Capacity (Watts)	Total power capacity for all devices in the group or total power capacity of a device.
Total Drawn/Usage (Watts)	Total power used by all devices in the group or total power used by all the modules in a device.
Total Drawn/Usage (%)	Percentage of power used by all devices in the group or percentage of power used by all modules in a device.
Total Allocated (Watts)	Total power allocated for all devices in the group or total power allocated for all the modules in a device.
Total Available (Watts)	Total power available for all devices in the group or total power available for additional modules in a device.
Last Refresh Time	Time when the power usage information was last updated in Cisco DCNM.

Send document comments to dcnm-docfeedback@cisco.com

Feature History for Inventory

Table 3-4 lists the release history for this feature.

Table 3-4 ***Feature History for Inventory***

Feature Name	Releases	Feature Information
Module Pre-provisioning	5.2(1)	Support was added only for the Cisco Nexus 5000 Series switches.
Inventory	5.2(1)	Support was added for Cisco Nexus 3000 Series switches.
Inventory	5.1(1)	No change from Release 5.0.
Power Usage	5.0(2)	This feature was introduced.
Inventory	4.2(1)	Support was added for Cisco Nexus 5000 Series switches and Nexus 2000 Series Fabric Extenders.

Send document comments to dcnm-docfeedback@cisco.com



CHAPTER 4

Managing Virtual Switches

This chapter describes how to manage virtual switches using Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

- [Information About Virtual Switches, page 4-1](#)
- [Licensing Requirements for Virtual Switches, page 4-3](#)
- [Prerequisites, page 4-4](#)
- [Platform Support, page 4-4](#)
- [Configuring Domains, page 4-4](#)
- [Configuring Server Connections, page 4-9](#)
- [Displaying Neighbor Devices, page 4-12](#)
- [Configuring a Control Interface, page 4-12](#)
- [Monitoring Virtual Switches, page 4-13](#)
- [Field Descriptions, page 4-13](#)
- [Additional References, page 4-15](#)
- [Feature History for Virtual Switches, page 4-16](#)

Information About Virtual Switches

The Cisco Nexus 1000V is a virtual access software switch that works with VMware vSphere 4.0 and has the following components:

- Virtual Supervisor Module (VSM)—Control plane of the switch and a virtual machine that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM)—Virtual line card that is embedded in each VMware vSphere (ESX) host.

Managing a virtual switch involves configuring its domain and server connection.

This section includes the following topics:

- [Domains, page 4-2](#)
- [Server Connections, page 4-3](#)

Send document comments to dcnm-docfeedback@cisco.com

Domains

A domain is an instance of a Cisco Nexus 1000V device, including dual redundant Virtual Supervisor Modules (VSMs) and managed Virtual Ethernet Modules (VEMs), within a VMware vCenter Server. Each domain needs to be distinguished by a unique integer called the domain identifier.

You can configure Layer 2 or Layer 3 transport control mode for communication between the VSM and VEMs.

This section includes the following topics:

- [Layer 2 Control, page 4-2](#)
- [Layer 3 Control, page 4-2](#)

Layer 2 Control

Layer 2 is a transport control mode used for communication between the VSM and VEMs. However, you can create and specify the VLAN to be used.

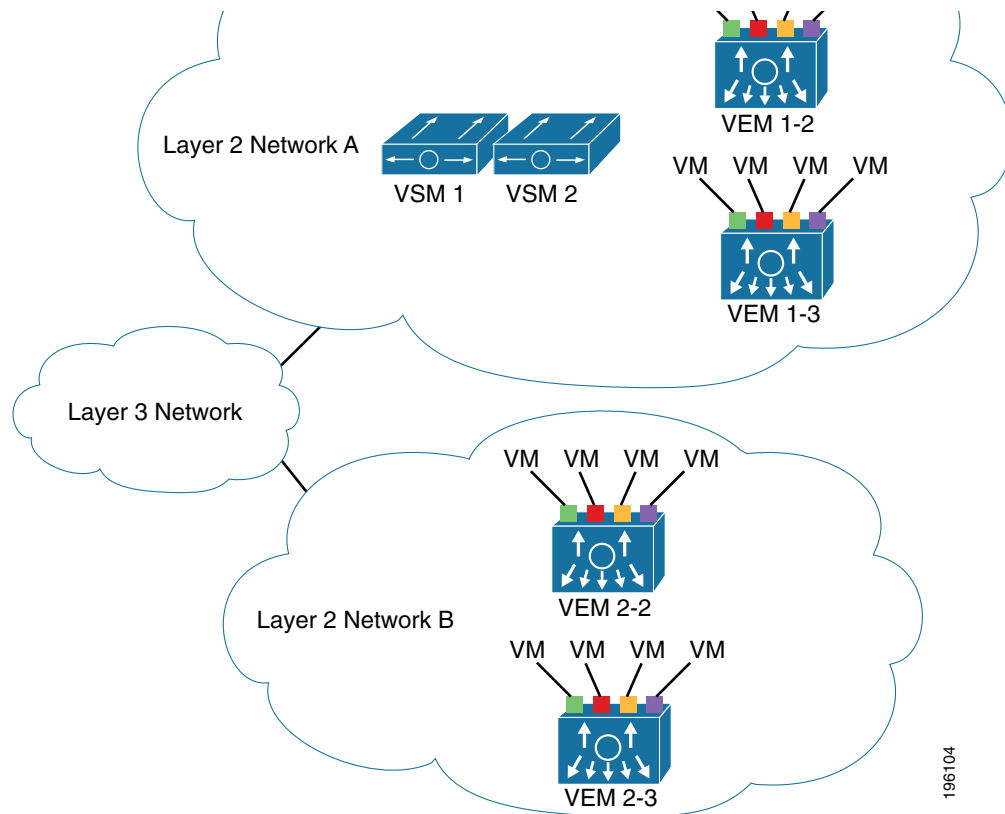
Layer 3 Control

Layer 3 control, or IP connectivity, is supported between the VSM and VEM for control and packet traffic. With Layer 3 control, a VSM can be Layer 3 accessible and control hosts can reside in a separate Layer 2 network. All hosts controlled by a VSM, however, must still reside in the same Layer 2 network. Because a VSM cannot control a host that is outside of the Layer 2 network it controls, the host on which it resides must be controlled by another VSM.

[Figure 4-1](#) shows an example of Layer 3 control where VSM0 controls VEM_0_1. VEM_0_1, in turn, hosts VSM1 and VSM2, and VSM1 and VSM2 control VEMs in other Layer 2 networks.

Send document comments to dcnm-docfeedback@cisco.com

Figure 4-1 Example of Layer 3 Control IP Connectivity



196104

Server Connections

The Nexus 1000V device requires a connection to a VMware vCenter server for management of its distributed virtual switch (DVS) and host mapping to the Virtual Ethernet Modules (VEMs).

Licensing Requirements for Virtual Switches

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	The Virtual Switch feature requires no license. Any feature not included in a license package is bundled with Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	The Virtual Switch feature 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Send document comments to dcnm-docfeedback@cisco.com

Prerequisites

The following prerequisite is required for using the Virtual Switches feature on Cisco DCNM. For a full list of feature-specific prerequisites, see the platform-specific documentation.

- System-message logging levels for the Virtual Switches feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series Switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Platform Support

The following platform supports this feature. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 1000V Series Switches	Cisco Nexus 1000V Series Switch Documentation

Configuring Domains

You can configure domains in Cisco DCNM.

This section includes the following topics:

- [Creating a Domain with Layer 2 Control, page 4-4](#)
- [Creating a Domain with Layer 3 Control, page 4-5](#)
- [Changing a Domain to Layer 3 Control, page 4-6](#)
- [Changing a Domain to Layer 2 Control, page 4-7](#)
- [Configuring a Domain with a Control VLAN, page 4-7](#)
- [Configuring a Domain with a Packet VLAN, page 4-8](#)

Creating a Domain with Layer 2 Control

You can create a domain name for the Cisco Nexus 1000V Series switch that identifies the Virtual Supervisor Module (VSM) and Virtual Ethernet Modules (VEMs) and then add control and packet VLANs for communication and management. This process is part of the initial installation process. If you need to create a domain after the initial setup, you can do so by using this procedure.

BEFORE YOU BEGIN

Be aware that if two or more VSMs share the same control and/or packet VLAN, the domain helps identify the VEMs that are managed by each VSM.

You must have a unique domain ID for this instance.

Send document comments to dcnm-docfeedback@cisco.com

We recommend that you use one VLAN for control traffic and a different VLAN for packet traffic.

We recommend that you use a distinct VLAN for each domain.

For information about changing a domain ID after adding a second VSM, see the documentation for your platform.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory > Virtual Switch**.
Summary information for each managed virtual switch appears in the Summary pane.
- Step 2** From the Summary pane, choose the device for which you want to create a domain.
- Step 3** From the Details pane, choose the **Details** tab.
- Step 4** Expand the **Domain Settings** section.
- Step 5** (Optional) From the menu bar, choose **Actions > Reset Domain Setting(s)**.
- Step 6** In the Domain ID field, enter an ID number for the domain.
- Step 7** In the Control mode drop-down list, choose **L2**.
Layer 2 control uses VLAN 1 for the control and packet VLANs by default. If desired, you can configure specific control and packet VLANs for the domain. See the [“Configuring a Domain with a Control VLAN” section on page 4-7](#) and the [“Configuring a Domain with a Packet VLAN” section on page 4-8](#).
- Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Creating a Domain with Layer 3 Control

You can create a domain name that identifies the Virtual Supervisor Module (VSM) and Virtual Ethernet Modules (VEMs) for the Cisco Nexus 1000V Series switch. This process is part of the initial setup when installing the software. If you need to create a domain after initial setup, you can do so using this procedure.

BEFORE YOU BEGIN

Configure the interface that you plan to use (mgmt 0 or control 0) with an IP address. For more information, see the [“Configuring a Control Interface” section on page 4-12](#).

Configure a port profile for Layer 3 control. See the *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

Create a VMware kernel NIC interface on each host and apply the Layer 3 control port profile to it. For more information, see your VMware documentation.

Ensure that you have a unique domain ID for this instance.

For information about changing a domain ID after adding a second VSM, see the documentation for your platform.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory > Virtual Switch**.

Send document comments to dcnm-docfeedback@cisco.com

Summary information for each managed virtual switch appears in the Summary pane.

- Step 2** From the Summary pane, choose the device for which you want to create a domain.
 - Step 3** From the Details pane, choose the **Details** tab.
 - Step 4** Expand the **Domain Settings** section.
 - Step 5** (Optional) From the menu bar, choose **Actions > Reset Domain Setting(s)**.
 - Step 6** In the Domain ID field, enter an ID number for the domain.
 - Step 7** In the Control Interface drop-down list, choose either **mgmt0** or **control0** as the interface to use.
 - Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Changing a Domain to Layer 3 Control

You can change the control mode from Layer 2 to Layer 3 for the Virtual Supervisor Module (VSM) domain control and packet traffic.

BEFORE YOU BEGIN

Configure the interface that you plan to use (mgmt 0 or control 0) with an IP address. For more information, see the [“Configuring a Control Interface”](#) section on page 4-12.



Note

You must perform the steps in this procedure in order. The control and packet VLANs must be disabled before the Layer 3 control can be enabled.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory > Virtual Switch**.
Summary information for each managed virtual switch appears in the Summary pane.
 - Step 2** From the Summary pane, choose the device for which you want to create a domain.
 - Step 3** From the Details pane, choose the **Details** tab.
 - Step 4** Expand the **Domain Settings** section.
 - Step 5** In the Control VLAN field, delete the number of the VLAN that is used as the control VLAN.
 - Step 6** In the Packet VLAN field, delete the number of the VLAN that is used as the packet VLAN.
 - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
 - Step 8** In the Control mode drop-down list, choose **L3**.
 - Step 9** In the Control Interface drop-down list, choose either **mgmt0** or **control0** as the interface to use.
 - Step 10** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to dcnm-docfeedback@cisco.com

Changing a Domain to Layer 2 Control

You can change the control mode from Layer 3 to Layer 2 for the VSM domain control and packet traffic.

BEFORE YOU BEGIN

Create VLANs to be used as the control and packet VLANs. For information, see the *Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

**Note**

You must perform the steps in this procedure in order. Layer 3 control must be disabled before the control and packet VLANs can be assigned.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose Inventory > Virtual Switch .
Summary information for each managed virtual switch appears in the Summary pane. |
| Step 2 | From the Summary pane, choose the device for which you want to create a domain. |
| Step 3 | From the Details pane, choose the Details tab. |
| Step 4 | Expand the Domain Settings section. |
| Step 5 | In the Control mode drop-down list, choose L2 . |
| Step 6 | In the Control VLAN field, enter the number of the VLAN to be used as the control VLAN. |
| Step 7 | In the Packet VLAN field, enter the number of the VLAN to be used as the packet VLAN. |
| Step 8 | From the menu bar, choose File > Deploy to apply your changes to the device. |
-

Configuring a Domain with a Control VLAN

You can configure the domain with a control VLAN.

BEFORE YOU BEGIN

Create the VLAN to be used as the control VLAN. For more information, see the *Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

If Layer 3 control is configured on your Virtual Supervisor Module (VSM), you cannot configure your domain with a control VLAN. You must first disable Layer 3 control.

Configure and enable the required VLAN interface using the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SVI(2)*. The VLAN interface provides communication between VLANs.

Understand how VLANs are numbered. For more information, see the *Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

Be aware that newly created VLANs remain unused until Layer 2 ports are assigned to them.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory > Virtual Switch**.
Summary information for each managed virtual switch appears in the Summary pane.
 - Step 2** From the Summary pane, choose the device for which you want to create a domain.
 - Step 3** From the Details pane, choose the **Details** tab.
 - Step 4** Expand the **Domain Settings** section.
 - Step 5** In the Control mode drop-down list, choose **Layer 2**.
 - Step 6** In the Control VLAN field, enter the number of the VLAN to be used as the control VLAN.
 - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring a Domain with a Packet VLAN

You can configure the domain with a packet VLAN.

BEFORE YOU BEGIN

Create the VLAN to be used as the packet VLAN. For more information, see the documentation for your platform.

Configure and enable the required VLAN interface using the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SVI(2)*. The VLAN interface provides communication between VLANs.

Understand how VLANs are numbered. For more information, see the *Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

Be aware that newly created VLANs remain unused until Layer 2 ports are assigned to them.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory > Virtual Switch**.
Summary information for each managed virtual switch appears in the Summary pane.
 - Step 2** From the Summary pane, choose the device for which you want to create a domain.
 - Step 3** From the Details pane, choose the **Details** tab.
 - Step 4** Expand the **Domain Settings** section.
 - Step 5** In the Control mode drop-down list, choose **L2**.
 - Step 6** In the Packet VLAN field, enter the number of the VLAN to be used as the packet VLAN.
 - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to dcnm-docfeedback@cisco.com

Configuring Server Connections

You can manage server connections using Cisco DCNM.

This section includes the following topics:

- [Configuring a vCenter Server Connection, page 4-9](#)
- [Deleting a vCenter Server Connection, page 4-10](#)
- [Connecting to a vCenter Server, page 4-10](#)
- [Disconnecting from a vCenter Server, page 4-10](#)
- [Deleting the DVS from a vCenter Server, page 4-11](#)
- [Removing Host Mapping from a Module, page 4-11](#)

Configuring a vCenter Server Connection

You can configure parameters for connecting the Cisco Nexus 1000V to the vCenter Server.

BEFORE YOU BEGIN

Have the following information available:

- Data center name
- vCenter Server IP address or hostname

Ensure that the vCenter Server management station is installed and running.

Ensure that the ESX servers are installed and running.

Ensure that the management port is configured.

Ensure that the vCenter Server is reachable.

Ensure that the appliance is installed.

If you are configuring a connection using a hostname, ensure that the DNS is already configured.

Ensure that you have already registered an extension with the vCenter Server. The extension includes the extension key and public certificate for the Virtual Supervisor Module (VSM). vCenter Server uses the key and certificate to verify the authenticity of the request that it receives from the VSM. For instructions about adding and registering an extension, see the documentation for the platform.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose Inventory > Virtual Switch .
Summary information for each managed virtual switch appears in the Summary pane. |
| Step 2 | From the Summary pane, choose the device for which you want to configure the vCenter Server connection. |
| Step 3 | From the Details pane, choose the Details tab. |
| Step 4 | Expand the Connection Settings section. |
| Step 5 | In the Connection Name field, enter a name for the connection. |
| Step 6 | In the Server Name/IP Address field, enter either the hostname of the server or its IP address. |

Send document comments to dcnm-docfeedback@cisco.com

- Step 7** In the Data Center Name field, enter the data center name in the vCenter Server where the data center is to be created as a Distributed Virtual Switch (DVS).
 - Step 8** In the Protocol drop-down list, choose **VMWARE-VIM**.
 - Step 9** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Deleting a vCenter Server Connection

You can delete the vCenter Server connection parameters that you have configured.

You can disconnect from the vCenter Server, for example, after correcting a vCenter Server configuration.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Inventory > Virtual Switch**.
Summary information for each managed virtual switch appears in the Summary pane.
 - Step 2** From the Summary pane, choose the desired device.
 - Step 3** From the menu bar, choose **Actions > Delete Connection**.
 - Step 4** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Connecting to a vCenter Server

You can connect to a vCenter Server or an ESX Server.

BEFORE YOU BEGIN

Create a vCenter Server connection.

DETAILED PROCEDURE

-
- Step 1** From the Feature Selector pane, choose **Inventory > Virtual Switch**.
Summary information for each managed virtual switch appears in the Summary pane.
 - Step 2** From the Summary pane, choose the desired device.
 - Step 3** From the menu bar, choose **Actions > Connect to vCenter**.
-

Disconnecting from a vCenter Server

You can disconnect from the vCenter Server, for example, after correcting a vCenter Server configuration.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose Inventory > Virtual Switch .
Summary information for each managed virtual switch appears in the Summary pane. |
| Step 2 | From the Summary pane, choose the desired device. |
| Step 3 | From the menu bar, choose Actions > Disconnect from vCenter . |
-

Deleting the DVS from a vCenter Server

You can delete the Distributed Virtual Switch (DVS) from a vCenter Server.

BEFORE YOU BEGIN

Configure a vCenter Server connection.

Connect to the vCenter Server.

Ensure that the Server Administrator has removed from the VI client all of the hosts connected to it. For more information, see the VMware documentation.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose Inventory > Virtual Switch .
Summary information for each managed virtual switch appears in the Summary pane. |
| Step 2 | From the Summary pane, choose the desired device. |
| Step 3 | From the menu bar, choose Actions > Delete VMware DVS . |
| Step 4 | From the menu bar, choose File > Deploy to apply your changes to the device. |
-

Removing Host Mapping from a Module

You can remove the mapping of a module to a host server.



Note

This function can be performed only on disabled modules in the Absent state.

BEFORE YOU BEGIN

Remove the host from the DVS on a vCenter Server.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose Inventory . |
|---------------|---|

Send document comments to dcnm-docfeedback@cisco.com

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

Step 2 Expand the desired Cisco Nexus 1000V device.

All of the modules associated with the device appear.

Step 3 Right-click the module from which you want to remove the host mapping and choose **Delete Host Mapping from Module**.

Displaying Neighbor Devices

You can display information about the devices that surround a selected Cisco Nexus 1000V device.

DETAILED STEPS

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

Summary information for each managed virtual switch appears in the Summary pane.

Step 2 From the Summary pane, choose the desired device.

Step 3 Expand the **Neighbors** section.

The neighboring devices appear.

Configuring a Control Interface

You can configure the control interface used for Layer 3 control.

DETAILED STEPS

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

Summary information for each managed virtual switch appears in the Summary pane.

Step 2 From the Summary pane, choose the desired device.

Step 3 Expand the **Control Interface** section.

Step 4 In the IP Address field, enter the IP address of the interface to use for Layer 3 control.

Step 5 In the Wildcard Mask field, enter the wildcard mask.

Step 6 In the Admin Status drop-down list, choose **Up** to enable the interface.

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

Send document comments to dcnm-docfeedback@cisco.com

Monitoring Virtual Switches

You can monitor virtual switch information in Cisco DCNM.

This section includes the following topics:

- [Displaying Virtual Switch Summary Information, page 4-13](#)
- [Displaying Virtual Switch Details, page 4-13](#)

Displaying Virtual Switch Summary Information

You can display summary information about the virtual switches in your managed network.

From the Feature Selector pane, choose **Inventory > Virtual Switch**. Summary information for each managed virtual switch appears in the Summary pane.

Displaying Virtual Switch Details

You can display details about the virtual switches in your managed network. This information includes details about the domain and vCenter connection settings.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose Inventory > Virtual Switch .

Summary information for each managed virtual switch appears in the Summary pane. |
| Step 2 | From the Summary pane, choose a device to display additional details about the domain, server, neighboring devices, and control interface and to display events. |
-

Field Descriptions

This section includes the following field descriptions for the Virtual Switches feature:

- [Inventory: Virtual Switch: Details: Domain Settings Section, page 4-14](#)
- [Inventory: Virtual Switch: Details: Connection Settings Section, page 4-14](#)
- [Inventory: Virtual Switch: Details: Neighbors Section, page 4-15](#)
- [Inventory: Virtual Switch: Details: Control Interface Section, page 4-15](#)

Send document comments to dcnm-docfeedback@cisco.com

Inventory: Virtual Switch: Details: Domain Settings Section

Table 4-1 *Inventory: Virtual Switch: Details: Domain Settings Section*

Field	Description
Domain ID	ID number for the domain.
Sync Status	Status of the configuration synchronization with the vCenter Server.
Control Mode	Control mode for the domain. Valid choices are Layer 2 or Layer 3.
Control Interface	<i>Active only if the control mode is Layer 3.</i> Layer 3 interface that is used by the Virtual Supervisor Module (VSM) for control and packet traffic.
Control VLAN	ID number of the VLAN that is used for the control traffic.
Packet VLAN	ID number of the VLAN that is used for the packet traffic.

Inventory: Virtual Switch: Details: Connection Settings Section

Table 4-2 *Inventory: Virtual Switch: Details: Connection Settings Section*

Field	Description
Connection Name	Name of the connection.
Server Name/IP Address	Hostname or IP address of the vCenter Server.
Data Center Name	Name of the data center in the vCenter Server where the data center is to be created as a Distributed Virtual Switch (DVS).
Config Status	Status of the configuration. Valid choices are Enabled or Disabled.
Certificate Filename	File name of the digital certificate that is used for the connection.
Version	Version on the VMware vCenter Server.
Protocol	Protocol that is used to establish the session with the vCenter Server. Valid choices are VMWARE VIM or EMPTY.
Port Number	TCP port that is used to connect to the vCenter server.
DVS UUID	Universally unique identifier (UUID) of the Distributed Virtual Switch (DVS).
Oper Status	Status of the connection.
Sync Status	Status of the configuration synchronization with the vCenter Server.

Send document comments to dcnm-docfeedback@cisco.com

Inventory: Virtual Switch: Details: Neighbors Section

Table 4-3 *Inventory: Virtual Switch: Details: Neighbors Section*

Field	Description
Last Updated Time	Time when the information was last retrieved from the switch. Click Get Latest Info to retrieve the latest information from the switch.
Source MAC Address	<i>Display only.</i> MAC source addresses of the frames received.
Type	<i>Display only.</i> Setting that indicates whether the neighbor node is a VSM or VEM.
Domain ID	<i>Display only.</i> Numerical identifier of the domain.
Node ID	<i>Display only.</i> Numerical identifier of the neighbor node.
Last Learnt Time	<i>Display only.</i> Last time that the MAC address was learned.

Inventory: Virtual Switch: Details: Control Interface Section

Table 4-4 *Inventory: Virtual Switch: Details: Control Interface Section*

Field	Description
IP Address	IP address of the control interface.
Wildcard Mask	Wildcard mask of the control interface.
Admin Status	Administrative status of the control interface. Valid choices are Up or Down.
Operation Status	Current operational status, either Up or Down.

Additional References

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

- [Related Documents, page 4-15](#)
- [Standards, page 4-16](#)

Related Documents

Related Topic	Document Title
Configuring the Domain	<i>Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SVI(2)</i>
Managing Server Connections	<i>Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SVI(2)</i>

Send document comments to dcnm-docfeedback@cisco.com

Standards

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

Feature History for Virtual Switches

This section provides the release history of the virtual switches

Feature Name	Releases	Feature Information
Virtual switches	5.2(1)	No change from Release 5.1.
Virtual switches	5.1(1)	No change from Release 5.0.
Virtual switches	5.0(2)	This feature was introduced.



CHAPTER 5

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, page 5-1](#)
- [Licensing Requirements for SPAN, page 5-3](#)
- [Prerequisites, page 5-4](#)
- [Platform Support, page 5-4](#)
- [Configuring SPAN, page 5-4](#)
- [Field Descriptions for SPAN, page 5-8](#)
- [Additional References, page 5-9](#)
- [Feature History for SPAN, page 5-10](#)

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 SPAN sessions on the local device.

This section includes the following topics:

- [SPAN Sources, page 5-2](#)
- [SPAN Destinations, page 5-2](#)
- [SPAN Sessions, page 5-2](#)
- [Virtual SPAN Sessions, page 5-2](#)
- [Multiple SPAN Sessions, page 5-3](#)
- [High Availability, page 5-3](#)

Send document comments to dcnm-docfeedback@cisco.com

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

SPAN Destinations

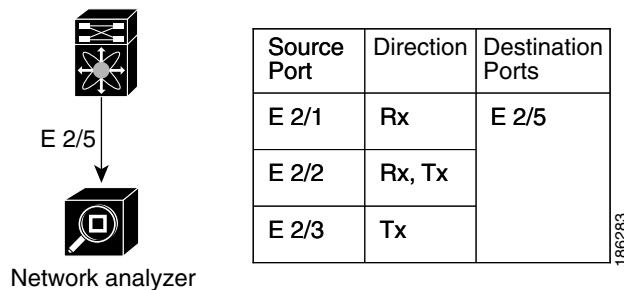
SPAN destinations refer to the interfaces that monitor source ports. Destination ports receive the copied traffic from SPAN sources.

SPAN Sessions

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

Figure 5-1 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 5-1 *SPAN Configuration*



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 5-2 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 5-2, the device transmits packets from one VLAN at each destination port.

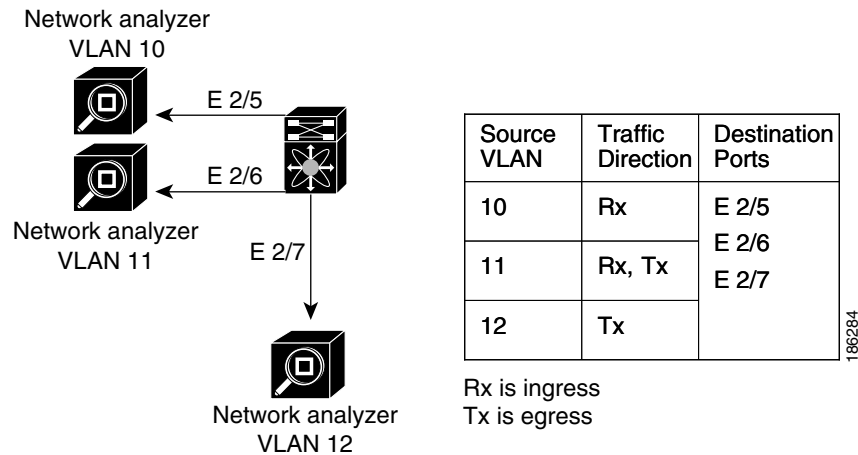


Note

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.

Send document comments to dcnm-docfeedback@cisco.com

Figure 5-2 Virtual SPAN Configuration



For information about configuring a virtual SPAN session, see the [“Configuring a Virtual SPAN Session” section on page 5-6](#).

Multiple SPAN Sessions

You can define multiple SPAN sessions. 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 5-8](#).

High Availability

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

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 Cisco DCNM and is provided at no charge to you. For a complete explanation of the Cisco DCNM licensing scheme, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Send document comments to dcnm-docfeedback@cisco.com

Prerequisites

The SPAN feature has the following prerequisite (for a full list of feature-specific prerequisites, see the platform-specific documentation):

- System-message logging levels for the SPAN feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Platform Support

The following platform supports this feature. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 3000 Series switches	Cisco Nexus 3000 Series Switch Documentation
Cisco Nexus 7000 Series switches	Cisco Nexus 7000 Series Switch Documentation

Configuring SPAN

This section includes the following topics:

- [Configuring a SPAN Session, page 5-4](#)
- [Configuring a Virtual SPAN Session, page 5-6](#)
- [Configuring an RSPAN VLAN, page 5-7](#)
- [Shutting Down or Resuming a SPAN Session, page 5-8](#)

Configuring a SPAN Session

You can configure a SPAN session on the local device only.

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

You must have already configured the destination ports in access or trunk mode. For more information, see the *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED 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**.
- 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.

Send document comments to dcnm-docfeedback@cisco.com

- 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.
- 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.

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 *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

DETAILED 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**.
 - 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.

Send document comments to dcnm-docfeedback@cisco.com

- Step 9** Add source Ethernet ports to the SPAN session as follows:
- From the Ports association panel, double-click the device and then double-click the desired slot to display ports.
 - 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:
- From the VLANs association panel, double-click the device to display the configured VLANs.
 - 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:
- From the Ports association panel, double-click the device and then double-click the desired slot to display ports.
 - Choose an access or trunk port.
 - In the Monitor column, check the check box to enable monitoring on this port.
 - 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:
- From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**. The available devices appear in the Summary pane.
 - From the Summary pane, double-click the device and then double-click the slot that you want to configure.
 - Choose the trunk port to configure.
 - From the Details pane, click the **Port Details** tab and expand the **Port Mode Settings** section, if necessary.
 - 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

-
- 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.

Send document comments to dcnm-docfeedback@cisco.com

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. This action can free up hardware resources to enable another session.

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

-
- 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, to enable the session, you must first shut down the session and then resume the session.

Field Descriptions for SPAN

This section includes the following field descriptions for SPAN:

- [Local SPAN Session: Configuration: Session Settings Section, page 5-8](#)
- [Local SPAN Session: Configuration: Source and Destination Section, page 5-9](#)

Local SPAN Session: Configuration: Session Settings Section

Table 5-1 *Local SPAN Session: Configuration: Session Settings Section*

Element	Description
Session Id	Local SPAN session number that can only be specified when the session is first created. The value ranges from 1 to 18.
Description	Description for this session.

Send document comments to dcnm-docfeedback@cisco.com

Table 5-1 **Local SPAN Session: Configuration: Session Settings Section (continued)**

Element	Description
Filtered VLANs	When clicked, list of configured VLANs appears.
Admin Status	Administrative status of the session.
Operational Status	<i>Display only.</i> Whether the session is shut (down) or enabled (up).
Status Description	<i>Display only.</i> Status description.

Local SPAN Session: Configuration: Source and Destination Section

Table 5-2 **Local SPAN Session: Configuration: Source and Destination Section**

Element	Description
Source	
Interface/VLAN	<i>Display only.</i> Port or VLAN number.
Description	<i>Display only.</i> Port or VLAN description.
Ingress	Status of whether to monitor ingress packets.
Egress	Status of whether to monitor egress packets.
Destination	
Interface	<i>Display only.</i> Port number.
Description	<i>Display only.</i> Port description.

Additional References

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

- [Related Documents, page 5-9](#)
- [Standards, page 5-10](#)

Related Documents

Related Topic	Document Title
VDCs	<i>Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 5.x</i>

Send document comments to dcnm-docfeedback@cisco.com

Standards

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

Feature History for SPAN

[Table 5-3](#) lists the release history for this feature.

Table 5-3 ***Feature History for SPAN***

Feature Name	Releases	Feature Information
SPAN	5.2(1)	Support was added for the Cisco Nexus 3000 Series switches.
SPAN	5.1(1)	No change from Release 5.0.
SPAN	5.0(2)	No change from Release 4.2.
SPAN	4.2(1)	No change from Release 4.1.



CHAPTER 6

Configuring LLDP

This chapter describes how to configure the Link Layer Discovery Protocol (LLDP) in order to discover servers that are connected to your Cisco NX-OS device.

This chapter includes the following sections:

- [Information About LLDP, page 6-1](#)
- [Licensing Requirements for LLDP, page 6-2](#)
- [Prerequisites, page 6-2](#)
- [Guidelines and Limitations for LLDP, page 6-2](#)
- [Platform Support, page 6-3](#)
- [Configuring LLDP, page 6-3](#)
- [Additional References, page 6-4](#)
- [Feature History for LLDP, page 6-5](#)

Information About LLDP

This section includes the following topics:

- [LLDP Overview, page 6-1](#)
- [High Availability, page 6-2](#)

LLDP Overview

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over the data-link layer (Layer 2) on all Cisco-manufactured devices (routers, bridges, access servers, and switches). CDP allows network management applications to automatically discover and learn about other Cisco devices that are connected to the network.

To permit the discovery of non-Cisco devices, the switch also supports the Link Layer Discovery Protocol (LLDP), a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other.

Send document comments to dcnm-docfeedback@cisco.com

LLDP is a one-way protocol that transmits information about the capabilities and current status of a device and its interfaces. LLDP devices use the protocol to solicit information only from other LLDP devices. Cisco DCNM can use LLDP to discover only servers that are connected to your device.



Note

For information on device discovery and manually binding devices to a server, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

High Availability

The LLDP feature supports stateless and stateful restarts. After a reboot or supervisor switchover, the running configuration is applied.

Licensing Requirements for LLDP

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	LLDP requires no license. Any feature not included in a license package is bundled with Cisco DCNM and is provided at no extra charge to you. For a complete explanation of the Cisco DCNM licensing scheme, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	LLDP 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites

The LLDP feature has the following prerequisite (for a full list of feature-specific prerequisites, see the platform-specific documentation):

- System-message logging levels for the LLDP feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Guidelines and Limitations for LLDP

LLDP has the following configuration guidelines and limitations (for a full list of feature-specific guidelines and limitations, see the platform-specific documentation):

- LLDP timers and type, length, and value (TLV) descriptions cannot be configured using Cisco DCNM.

Send document comments to dcnm-docfeedback@cisco.com

Platform Support

The following platform supports this feature. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 5000 Series switches	Cisco Nexus 5000 Series Switch Documentation
Cisco Nexus 7000 Series switches	Cisco Nexus 7000 Series Switch Documentation

Configuring LLDP

This section includes the following topics:

- [Enabling or Disabling LLDP Globally, page 6-3](#)
- [Enabling or Disabling LLDP on an Interface, page 6-3](#)

Enabling or Disabling LLDP Globally

You can enable or disable LLDP globally on Cisco Nexus 7000 Series switches.



Note

LLDP is enabled globally on Cisco Nexus 5000 Series switches and cannot be disabled.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC.

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**. The available devices appear in the Summary pane.
- Step 2** From the Summary pane, click the device on which you want to enable or disable LLDP.
- Step 3** Do one of the following:
 - To enable LLDP on the device, from the menu bar, choose **Actions > Enable LLDP Service**.
 - To disable LLDP on the device, from the menu bar, choose **Actions > Disable LLDP Service**.
- Step 4** From the menu bar, choose **File > Deploy** to apply your changes to the device.

Enabling or Disabling LLDP on an Interface

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

Send document comments to dcnm-docfeedback@cisco.com

**Note**

If the interface is configured as a tunnel port, LLDP is disabled automatically.

**Note**

Beginning with Cisco DCNM Release 5.1, you can enable or disable LLDP on individual interfaces on Cisco Nexus 5000 Series switches.

BEFORE YOU BEGIN

Make sure that you are in the correct VDC.

Make sure that you have globally enabled LLDP on the device. For more information, see the [“Enabling or Disabling LLDP Globally”](#) section on page 6-3.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Interfaces > Physical > Ethernet**. The available devices appear in the Summary pane.
- Step 2** From the Summary pane, expand the device, expand the slot, and click the port on which you want to enable or disable LLDP.
- Tabs appear for the port information in the Details pane. The Port Details tab is active, but its sections are not expanded.
- Step 3** Do one of the following:
- To disable LLDP on the port, from the menu bar, choose **Actions > Disable LLDP**.
 - To enable LLDP on the port, from the menu bar, choose **Actions > Enable LLDP**.
- Step 4** From the Details pane, expand the **Basic Settings** section.
- When LLDP is enabled, the LLDP Transmit Enabled and LLDP Receive Enabled fields show “Enabled.”
- When LLDP is disabled, the LLDP Transmit Enabled and LLDP Receive Enabled fields show “Disabled.”
- Step 5** (Optional) To selectively configure the port to only send or only receive LLDP packets, do one of the following:
- To configure the port to only send LLDP packets, choose **Enabled** from the LLDP Transmit Enabled drop-down list and choose **Disabled** from the LLDP Receive Enabled drop-down list.
 - To configure the port to only receive LLDP packets, choose **Disabled** from the LLDP Transmit Enabled drop-down list and choose **Enabled** from the LLDP Receive Enabled drop-down list.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Additional References

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

- [Related Documents](#), page 6-5
- [Standards](#), page 6-5

Send document comments to dcnm-docfeedback@cisco.com

Related Documents

Related Topic	Document Title
Device discovery	<i>Cisco DCNM Fundamentals Guide, Release 5.x</i>
VDCs	<i>Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 5.x</i>

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 LLDP

Table 6-1 lists the release history for this feature.

Table 6-1 Feature History for LLDP

Feature Name	Releases	Feature Information
LLDP	5.2(1)	No change from Release 5.1.
LLDP	5.1(1)	You can enable or disable LLDP per interface on Cisco Nexus 5000 Series switches.
LLDP	5.0(2)	This feature was introduced.

Send document comments to dcnm-docfeedback@cisco.com



CHAPTER 7

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 sections:

- [Information About Device OS Management, page 7-1](#)
- [Licensing Requirements for Device OS Management, page 7-3](#)
- [Prerequisites, page 7-4](#)
- [Guidelines and Limitations for Device OS Management, page 7-4](#)
- [Platform Support, page 7-4](#)
- [Using the Device OS Management Window, page 7-5](#)
- [Configuring Software Installation Jobs, page 7-6](#)
- [Configuring File Servers, page 7-12](#)
- [Field Descriptions for Device OS Management, page 7-15](#)
- [Additional References, page 7-17](#)
- [Feature History for Device OS Management, page 7-18](#)

Information About Device OS Management

The Device OS Management feature allows you to control the software images installed on certain devices that are managed by Cisco DCNM.

This section includes the following topics:

- [Device OS Management Screen, page 7-2](#)
- [Software Installation Jobs, page 7-2](#)
- [File Servers, page 7-3](#)
- [VDC Support, page 7-3](#)

Send document comments to dcnm-docfeedback@cisco.com

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 7-3](#).

- **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`

Send document comments to dcnm-docfeedback@cisco.com

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 file 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 in the job and configure the job to use the manually copied files rather than a file server.

VDC 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 <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	Device OS Management 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Send document comments to dcnm-docfeedback@cisco.com

Prerequisites

The Device OS Management feature has the following prerequisites (for a full list of feature-specific prerequisites, see the platform-specific documentation):

- 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 5.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 Cisco 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 5.x*.

Platform Support

The following platforms support this feature but may implement it differently. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 4000 Series switches	Cisco Nexus 4000 Series Switch Documentation
Cisco Nexus 5000 Series switches	Cisco Nexus 5000 Series Switch Documentation
Cisco Nexus 6000 Series switches	Cisco Nexus 6000 Series Switch Documentation
Cisco Nexus 7000 Series switches	Cisco Nexus 7000 Series Switch Documentation

Send document comments to dcnm-docfeedback@cisco.com

Using the Device OS Management Window


This section includes the following topics:

- [Viewing Device Image Details, page 7-5](#)
- [Installing Software on a Device, page 7-5](#)

Viewing Device Image Details

You can view details about the software image on a managed device.

DETAILED 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 7-6](#).
-

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 7-2](#).

Send document comments to dcnm-docfeedback@cisco.com

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 7-7.
-

Configuring Software Installation Jobs

This section includes the following topics:

- [Viewing Software Installation Job Details, page 7-6](#)
- [Creating or Editing a Software Installation Job, page 7-7](#)
- [Using the Software Installation Wizard, page 7-7](#)
- [Rescheduling a Software Installation Job, page 7-10](#)
- [Deleting a Software Installation Job, page 7-11](#)
- [Adding or Changing Comments for a Software Installation Job, page 7-11](#)
- [Changing Installation Options for a Software Installation Job, page 7-11](#)

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

-
- 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.

Send document comments to dcnm-docfeedback@cisco.com

**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 7-2](#).

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 in the job and configure the job to use the manually copied files rather than a file server.

DETAILED 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 7-7](#).
-

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.

Send document comments to dcnm-docfeedback@cisco.com

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 7-5.
- Software Installation Jobs—See the “Creating or Editing a Software Installation Job” section on page 7-7.

DETAILED 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:

- Under Available Switches, click the device.
- 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 field and again for the System Image field:

- In the applicable image field, click to activate the field and then click the **more** button.

The Software Image Browser dialog box appears.

- 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 to the folders on the file server, and select the software image file.
- **Switch File System**—If you choose this option, you must navigate to 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 field. If the transfer protocol that you use includes a username in the URL, in the Password field type the password for the username in the URL.

- Click **OK**.

If you specified a URL, Cisco DCNM verifies the URL.

The Software Image Browser dialog box closes. The applicable image field 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.

Send document comments to dcnm-docfeedback@cisco.com

**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 field, enter a comment about the installation job.

Send document comments to dcnm-docfeedback@cisco.com

- 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

- 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.

Send document comments to dcnm-docfeedback@cisco.com

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

-
- | | |
|---------------|--|
| 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

-
- | | |
|---------------|--|
| 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

-
- | | |
|---------------|--|
| Step 1 | From the Feature Selector pane, choose Device OS Management > Software Installation Jobs . |
|---------------|--|

Send document comments to dcnm-docfeedback@cisco.com

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:
- Check the **Installation Options** check box.
 - 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:
- Check the **Installation Options** check box.
 - 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

This section includes the following topics:

- [Adding a File Server, page 7-12](#)
- [Changing a File Server, page 7-13](#)
- [Deleting a File Server, page 7-14](#)

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.

Send document comments to dcnm-docfeedback@cisco.com

- 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

-
- 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.

Send document comments to dcnm-docfeedback@cisco.com

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

-
- 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 8-20](#).

DETAILED 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 8-20](#).

The file server is removed from the summary pane. You do not need to save your changes.

Send document comments to dcnm-docfeedback@cisco.com

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, page 7-15](#)
- [Field Descriptions for Software Installation Jobs, page 7-16](#)
- [Field Descriptions for the File Servers Contents Pane, page 7-17](#)

Field Descriptions for Device OS Management

This section includes the following field descriptions for the Device OS Management feature:

- [Device: Details: System Section, page 7-15](#)
- [Device: Details: Software Installation Jobs Section, page 7-15](#)

Device: Details: System Section

Table 7-1 ***Device: Details: System Section***

Field	Description
System	
Device Name	<i>Display only.</i> Name of the managed device.
IP Address	<i>Display only.</i> IP address that Cisco DCNM uses to connect to the managed device.
Model	<i>Display only.</i> Hardware model name of the managed device.
Redundancy Supervisor	<i>Display only.</i> Whether the device has a secondary supervisor module.
Software	
System Version	<i>Display only.</i> Release number of the system image currently installed on the managed device.
System Image	<i>Display only.</i> Filename of the system image currently installed on the managed device.
Kickstart Image	<i>Display only.</i> Filename of the kickstart image currently installed on the managed device.

Device: Details: Software Installation Jobs Section

Table 7-2 ***Device: Details: Software Installation Jobs Section***

Field	Description
Job ID	<i>Display only.</i> Identification number of the job.
Owner	<i>Display only.</i> Cisco DCNM user who created the installation job.
Software Image and Version	<i>Display only.</i> Name of the system image specified in the job.

Send document comments to dcnm-docfeedback@cisco.com

Table 7-2 **Device: Details: Software Installation Jobs Section (continued)**

Field	Description
Scheduled At	<i>Display only.</i> Date and time that the installation job is scheduled to occur.
Completed At	<i>Display only.</i> Date and time that the installation job occurred. If the job has not completed, this field is blank.
Status	<i>Display only.</i> 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	<i>Display only.</i> 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 7-16](#)
- [Installation Job: Details: Devices and Software Images Section, page 7-17](#)

Installation Job: Details: General Section

Table 7-3 **Installation Job: Details: General Section**

Field	Description
General	
Job ID	<i>Display only.</i> Identification number of the job.
Owner	<i>Display only.</i> Cisco DCNM user who created the installation job.
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	<i>Display only.</i> Date and time that the installation job occurred. If the job has not completed, this field is blank.
Status	<i>Display only.</i> 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.

Send document comments to dcnm-docfeedback@cisco.com

Installation Job: Details: Devices and Software Images Section

Table 7-4 ***Installation Job: Details: General Section***

Field	Description
Device	<i>Display only.</i> Name of the managed device.
Platform	<i>Display only.</i> Hardware model name of the managed device.
Kickstart Image	<i>Display only.</i> Filename of the kickstart image currently installed on the managed device.
System Image	<i>Display only.</i> Filename of the system image currently installed on the managed device.

Field Descriptions for the File Servers Contents Pane

Table 7-5 ***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.
Protocol	Transfer protocol supported by the server. Valid values are as follows: <ul style="list-style-type: none">• 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 7-18](#)
- [Standards, page 7-18](#)

Send document comments to dcnm-docfeedback@cisco.com

Related Documents

Related Topic	Document Title
Upgrading and downgrading Cisco NX-OS software using the command-line interface on Cisco Nexus 7000 Series switches	<i>Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x</i>

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 7-6](#) lists the release history for this feature.

Table 7-6 **Feature History for Device OS Management**

Feature Name	Releases	Feature Information
Device OS Management	5.2(1)	No change from Release 5.1.
Device OS Management	5.1(1)	No change from Release 5.0.
Device OS Management	5.0(2)	Support was added for Cisco Nexus 4000 Series Switches and Cisco Nexus 5000 Series Switches.



CHAPTER 8

Working with Configuration Change Management

This chapter describes how to use the Configuration Change Management feature on Cisco NX-OS devices.

This chapter includes the following sections:

- [Information About Configuration Change Management, page 8-1](#)
- [Licensing Requirements for Configuration Change Management, page 8-5](#)
- [Prerequisites, page 8-5](#)
- [Guidelines and Limitations for Configuration Change Management, page 8-6](#)
- [Platform Support, page 8-6](#)
- [Working with the Version Browser, page 8-6](#)
- [Configuring Archival Jobs, page 8-16](#)
- [Configuring Archival Settings, page 8-20](#)
- [Configuring Switch Profiles, page 8-21](#)
- [Field Descriptions for Configuration Change Management, page 8-25](#)
- [Additional References, page 8-29](#)
- [Feature History for Configuration Change Management, page 8-30](#)

Information About Configuration Change Management

The Configuration Change Management feature allows you to keep an archive of configurations from managed 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).



Note

Beginning with Cisco Release 5.2(1), Cisco DCNM supports the Cisco IOS platform.

Send document comments to dcnm-docfeedback@cisco.com

**Note**

Beginning with Cisco DCNM Release 5.2(1), this feature supports Cisco Catalyst 6500 Series, Cisco Nexus 1000 Series, Cisco Nexus 1010 Series, Cisco Nexus 3000 Series, Cisco Nexus 4000 Series, Cisco Nexus 5000 Series, and Cisco Nexus 7000 Series devices.

This section includes the following topics:

- [Version Browser, page 8-2](#)
- [Archival Jobs, page 8-2](#)
- [Archival Settings, page 8-2](#)
- [Switch Profiles, page 8-3](#)
- [VDC Support, page 8-5](#)

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 version. After you modify a configuration by merging changes, you can save the modified configuration as a text file on a file system that is 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 managed Cisco Nexus 7000 Series device, using any of the archived configurations available in Cisco DCNM for the device. Cisco DCNM uses the rollback feature available in Cisco IOS and 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 5.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.

Send document comments to dcnm-docfeedback@cisco.com

Switch Profiles



Note

The Switch Profiles feature is supported only on the Cisco Nexus 5000 series switches.

Several applications require consistent configuration across Cisco Nexus 5000 Series switches in the network. For example, with a virtual port channel (vPC), you must have identical configurations. Mismatched configurations can cause errors or misconfigurations that can result in service disruptions. The configuration synchronization (config-sync) feature in Cisco NX-OS Release 5.0(2)N1(1) allows you to configure one switch profile and have the configuration be automatically synchronized to the peer switch.

A switch profile provides the following benefits:

- Allows configurations to be synchronized between switches.
- Merges configurations when connectivity is established between two switches.
- Provides control of exactly which configuration gets synchronized.
- Ensures configuration consistency across peers through merge and mutual-exclusion checks.
- Provides verify and commit semantics.
- Supports configuring and synchronizing port profile configurations.
- Provides an import command to migrate existing vPC configurations to a switch profile.

Switch Profile Configuration Modes

The Cisco NX-OS Release 5.0(2)N1(1) switch profile feature includes the following configuration modes:

- Configuration synchronization mode
- Switch profile mode
- Switch profile import mode

Configuration Synchronization Mode

Beginning with Cisco NX-OS Release 5.0(2)N1(1), the configuration synchronization mode (config-sync) allows you to create switch profiles. After entering the **config sync** command, you can create and name the switch profile that displays the switch profile mode. You must enter the **config sync** command on the local switch and the peer switch that you want to synchronize.

Switch Profile Mode

The switch profile mode allows you to add supported configuration commands to a switch profile that is later synchronized with a peer switch. Commands that you enter in the switch profile mode are buffered until you enter the **commit** command.

Switch Profile Import Mode

When you upgrade from an earlier release to Cisco NX-OS Release 5.0(2)N1(1), you have the option to enter the **import** command to copy supported running-configuration commands to a switch profile. After entering the **import** command, the switch profile mode (config-sync-sp) changes to the switch profile import mode (config-sync-sp-import). The switch profile import mode allows you to import existing switch configurations from the running configuration and specify which commands you want to include in the switch profile.

Send document comments to dcnm-docfeedback@cisco.com

Because different topologies require different commands that are included in a switch profile, the import command mode allows you to modify the imported set of commands to suit a specific topology. For example, a dual homed Fabric Extender (FEX) topology requires that most of the configuration is synchronized. In other vPC topologies, the configuration that needs to be synchronized might be a much smaller set of commands.

You need to enter the **commit** command to complete the import process and move the configuration into the switch profile. Because configuration changes are not supported during the import process, if you added new commands before entering the **commit** command, the switch profile remains unsaved and the switch remains in the switch profile import mode. You can remove the added commands or abort the import. Unsaved configurations are lost if the process is aborted. You can add new commands to the switch profile after the import is complete.

Configuration Validation

Two types of configuration validation checks can identify two types of switch profile failures:

- Mutual exclusion checks
- Merge checks

Mutual Exclusion Checks

To reduce the possibility of overriding configuration settings that are included in a switch profile, mutual exclusion (mutex) checks the switch profile commands against the commands that exist on the local switch and the commands on the peer switch. A command that is included in a switch profile cannot be configured outside of the switch profile or on a peer switch. This requirement reduces the possibility that an existing command is unintentionally overwritten.

As a part of the commit process, the mutex-check occurs on both switches if the peer switch is reachable; otherwise, the mutex-check is performed locally. Configuration changes made from the configuration terminal occur only on the local switch.

If a mutex-check identifies errors, these errors are reported as a mutex failure and must be manually corrected.

The following exceptions apply to the mutual exclusion policy:

- Interface configuration—An interface configuration can be partially present in a switch profile and partially present in the running configuration as long as there are no conflicts.
- Shutdown/no shutdown
- System QoS

Merge Checks

Merge checks are done on the peer switch that is receiving a configuration. The merge checks ensure that the received configuration does not conflict with the switch profile configuration that already exists on the receiving switch. The merge check occurs during the merge or commit process. Errors are reported as merge failures and must be manually corrected.

When one or both switches are reloaded and the configurations are synchronized for the first time, the merge check verifies that the switch profile configurations are identical on both switches. Differences in the switch profiles are reported as merge errors and must be manually corrected.

Send document comments to dcnm-docfeedback@cisco.com

Software Upgrades and Downgrades with Switch Profiles

When you downgrade from Cisco NX-OS Release 5.0(2)N1(1) to an earlier release, you are prompted to remove an existing switch profile that is not supported on earlier releases.

When you upgrade from an earlier release to Cisco NX-OS Release 5.0(2)N1(1), you have the option to move some of the running-configuration commands to a switch profile. The **import** command allows you to import relevant switch profile commands. An upgrade can occur if there are buffered configurations (uncommitted); however, the uncommitted configurations are lost.

When you perform an In Service Software Upgrade (ISSU) on one of the switches included in a switch profile, a configuration synchronization cannot occur because the peer is unreachable.

VDC Support

Cisco DCNM treats each virtual device context (VDC) on a Cisco IOS and Cisco NX-OS device as a separate device; therefore, Cisco DCNM archives the running configurations of each VDC if 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 <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	Configuration Change Management 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites

The Configuration Change Management feature has the following prerequisites (for a full list of feature-specific prerequisites, see the platform-specific documentation):

- 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.

Send document comments to dcnm-docfeedback@cisco.com

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.
- A configuration rollback can be performed on managed Cisco Nexus 7000 Series devices only.
- 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 8-6](#).

Platform Support

The following platforms support this feature but may implement it differently. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Catalyst 6500 Series switches	Cisco Catalyst 6500 Series Switches Documentation
Cisco Nexus 1000V Series switches	Cisco Nexus 1000V Series Switch Documentation
Cisco Nexus 3000 Series switches	Cisco Nexus 3000 Series Switch Documentation
Cisco Nexus 4000 Series switches	Cisco Nexus 4000 Series Switch Documentation
Cisco Nexus 5000 Series switches	Cisco Nexus 5000 Series Switch Documentation
Cisco Nexus 7000 Series switches	Cisco Nexus 7000 Series Switch Documentation

Working with the Version Browser

This section includes the following topics:

- [Viewing the Archival Status of a Device, page 8-7](#)
- [Viewing the Archival History of a Device, page 8-7](#)
- [Browsing and Commenting on Configuration Versions, page 8-8](#)
- [Using Copy Run to Start, page 8-9](#)
- [Archiving the Current Running Configuration of a Device, page 8-9](#)
- [Viewing an Archived Configuration Version, page 8-10](#)
- [Comparing Configuration Versions, page 8-10](#)
- [Using the Version Comparison Tools, page 8-12](#)

Send document comments to dcnm-docfeedback@cisco.com

- [Merging Configuration Differences, page 8-14](#)
- [Performing a Configuration Rollback, page 8-14](#)
- [Viewing the Rollback History of a Device, page 8-15](#)
- [Deleting All Archived Configurations for a Device, page 8-16](#)

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

-
- | | |
|---------------|---|
| 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, the View Schedule link appears.
If the archival job that includes the device is disabled, the 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 8-19. |
-

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.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED 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 that lists 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

-
- 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:
- 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 field is available for you to use.
 - Click in the **Comments** field and enter your comments.
 - From the menu bar, choose **File > Deploy** to save your changes to the Cisco DCNM server.
-

Send document comments to dcnm-docfeedback@cisco.com

Using Copy Run to Start

You can use the Copy Run to Start feature to copy the running configuration to the startup configuration.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.
The available devices appear in the Summary pane.
- Step 2** Right-click the appropriate device and from the drop-down list, choose **Copy Run to Start**. You can also press the **F7** key to start the Copy Run to Start feature.
A flag appears at the end of the row to indicate that the copy process is in progress. The flag remains when the process is finished to indicate that a configuration change has been made to the device.
The running configuration is copied to the startup configuration.
-

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 from 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

-
- 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 dialog box notifies you that archiving the configuration was skipped, that means that Cisco DCNM did not detect differences between the current running configuration and the most recent archived configuration version for the device. To close the dialog box, click **OK**.

Send document comments to dcnm-docfeedback@cisco.com

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

-
- 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 by pressing **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 versions 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

-
- Step 1** From the Feature Selector pane, choose **Configuration Change Management > Version Browser**.
The Summary pane displays a table of devices.


Send document comments to dcnm-docfeedback@cisco.com

- 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 [Table 8-1](#) to compare the selected version to the configuration version that you want.

Table 8-1 Comparing Configuration Versions

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 .
Another configuration version that you select	<ol style="list-style-type: none"> 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. <p>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.</p> <p>Tip You can select archived configuration versions from different devices.</p>
Current running configuration from the current device	Right-click the version and choose Compare with > Current Running Configuration .

Send document comments to dcnm-docfeedback@cisco.com

To Compare With	Follow These Steps
Current startup configuration from the current device	Right-click the version and choose Compare with > Current Startup Configuration .
A configuration version from another device	<ol style="list-style-type: none"> 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 8-12.

Using the Version Comparison Tools

When you use the Version Browser to compare configuration versions, use the Compare tab in the Details pane to assist you with the comparison.

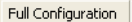

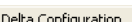




Note
















You must be comparing two configurations to use the version comparison tools. For more information, see the [“Comparing Configuration Versions”](#) section on page 8-10.

Use the options described to compare two configuration versions.

Table 8-2 Using the Comparison Version Tool

Option Icon and Name	How to Use the Option
 Full vs. Delta View	From the list, choose the desired viewing option, as follows: <ul style="list-style-type: none"> •  —Shows all of both configuration versions. •  —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.

Send document comments to dcnm-docfeedback@cisco.com

Option Icon and Name	How to Use the Option
 Prev Diff	Click the  icon to jump to the previous difference between the two configurations shown.
 Bookmark	<ol style="list-style-type: none"> 1. Click a line in one of the configuration panes. 2. Click the  icon. <p>A bookmark icon appears beside the line number.</p>
 Next Bookmark	<ol style="list-style-type: none"> 1. Click the configuration pane that has the bookmarked line that you want to view. 2. Click the  icon. <p>The configurations in both panes jump to the next bookmarked line.</p>
 Prev Bookmark	<ol style="list-style-type: none"> 1. Click the configuration pane that has the bookmarked line that you want to view. 2. Click the  icon. <p>The configurations in both panes jump to the previous bookmarked line.</p>
 Compare	<p>Use this option to choose the archived configuration version shown in the right configuration pane.</p> <ol style="list-style-type: none"> 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. <p>The right configuration pane displays the configuration version that you specified.</p>
 Reset	<p>Click the  icon when you want to do the following:</p> <ul style="list-style-type: none"> • Undo all configuration merges. • Remove all bookmarks. • Jump to the first line in both configuration panes. • Use the Full Configuration view.
 Merge	<p>Use this option to copy a difference from the configuration in the left configuration pane into the configuration in the right pane.</p> <p>For detailed steps, see the “Merging Configuration Differences” section on page 8-14.</p>
 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.

Send document comments to dcnm-docfeedback@cisco.com

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 merge the changes into appears in the right configuration pane.

DETAILED 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 Cisco Nexus 7000 Series 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 Cisco Nexus 7000 Series 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.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED 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 Cisco Nexus 7000 Series 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 Cisco Nexus 7000 Series device.

BEFORE YOU BEGIN

A managed Cisco Nexus 7000 Series 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.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED 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.

BEFORE YOU BEGIN

Be certain that you do not want any of the archived configuration versions 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

-
- 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

This section includes the following topics:

- [Configuring an Archival Job, page 8-17](#)
- [Enabling and Disabling an Archival Job, page 8-18](#)

Send document comments to dcnm-docfeedback@cisco.com

- [Deleting an Archival Job, page 8-18](#)
- [Viewing Details of an Archival Job, page 8-19](#)
- [Viewing the History of an Archival Job, page 8-19](#)

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

- 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** (Optional) 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**.

Send document comments to dcnm-docfeedback@cisco.com

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 (Optional) 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, the archival job information does not change.

Enabling and Disabling an Archival Job

You can enable or disable any archival job.

DETAILED 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.

Send document comments to dcnm-docfeedback@cisco.com

BEFORE YOU BEGIN

At least one custom archival job must exist in Cisco DCNM. You cannot delete the Default archival job.

DETAILED 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

-
- 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

-
- Step 1** From the Feature Selector pane, choose **Configuration Change Management > Archival Jobs**.
The Summary pane displays a table of archival jobs.

Send document comments to dcnm-docfeedback@cisco.com

- 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

This section includes the following topics:

- [Configuring Version and History Settings, page 8-20](#)
- [Configuring the Rollback File Server Setting, page 8-20](#)

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

-
- Step 1** From the Feature Selector pane, choose **Configuration Change Management > Archival Settings**.
The Contents pane displays the Archival Settings fields.
- Step 2** (Optional) Enter a value from 0 to 50 in the Maximum Version for a Device [0 - 50] field to configure the maximum number of configuration versions that Cisco DCNM should archive for each managed device.
- Step 3** (Optional) Enter a value from 0 to 100 in the Max Rollback and Archival History Status [0 - 100] field 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.

Send document comments to dcnm-docfeedback@cisco.com

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 7-12.

DETAILED 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: <ul style="list-style-type: none">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. |
-

Configuring Switch Profiles

This section includes the following topics:

- [Configuring a Switch Profile, page 8-21](#)
- [Configuring the Switch Profile Wizard Between Two vPCs, page 8-22](#)
- [Configuring the Switch Profile Wizard Between Two Switches, page 8-23](#)
- [Configuring the Sync Network View, page 8-23](#)
- [Configuring the Switch Profile Migration Wizard for Dual Homed FEXs, page 8-24](#)

Configuring a Switch Profile

You can configure a switch profile using Cisco DCNM.



Note

This feature is supported only on Cisco Nexus 5000 Series switches.

BEFORE YOU BEGIN

You must create the switch profile with the same name on each switch and the switches must configure each other as a peer. When connectivity is established between switches with the same active switch profile, the switch profiles are synchronized.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose Configuration Change Management > Switch-Profile . |
|---------------|---|

Send document comments to dcnm-docfeedback@cisco.com

All Cisco Nexus 5000 Series switches that are managed by Cisco DCNM are displayed in the Summary pane.

Step 2 Expand the **Cisco Nexus 5000 switches** to view the switch-profile information.

Step 3 Choose a specific switch-profile for the Cisco Nexus 5000 Series switch. The profile details is displayed in the detailed pane.

You can choose one of the following four options:

- **Sync Status**—Displays the last session operation status on the switch profile.
- **Effective Configuration**—Displays the most effective switch-profile configurations on the switch.
- **Buffered Configuration**—Displays the non committed switch-profile configurations on the switch.
- **Events**—Displays any events that are specific to the switch-profile.

Configuring the Switch Profile Wizard Between Two vPCs



Note

This feature is supported only on the Cisco Nexus 5000 Series switches.

Switch profiles address the configuration conflicts between vPC peers in the network. By using Cisco DCNM, you can configure switch profiles between the vPC peers by selecting any one of the switches. Cisco DCNM configures the switch profiles on both the selected switch and its vPC peer switch with sync-peer IP addresses.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Configuration Change Management > Switch-Profile**.

All Cisco Nexus 5000 Series switches that are managed by Cisco DCNM are displayed in the Summary pane.

Step 2 In the Summary pane, choose one of the vPC peer switches by right-clicking the vPC peer that you want.

Step 3 From the Context menu, click the **New switch-profile with vPC peer** tab.

Cisco DCNM checks if there is any vPC configuration available in the selected switch and if the vPC is active.

A dialog box is appears if the vPC is active.

Step 4 Click **Yes** to create the switch profile.

Step 5 (Optional) Edit the switch-profile name, and click **Ok** to proceed with the configuration.



Note

If there is no active vPC in the selected switch, Cisco DCNM displays an error message and does not create the switch profile.

Send document comments to dcnm-docfeedback@cisco.com

Configuring the Switch Profile Wizard Between Two Switches

**Note**

This feature is supported only on the Cisco Nexus 5000 Series switches.

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Configuration Change Management > Switch-Profile**.
All Cisco Nexus 5000 Series switches that are managed by Cisco DCNM are displayed in the Summary pane.
- Step 2** From the Summary pane, choose one of the switches.
- Step 3** From the Context menu, choose the **New switch-profile with any other switch** tab.
Cisco DCNM launches the switch profile configuration wizard.

**Note**

By default, the wizard displays the switch profile name and the source switch IP address. You can edit the preferred name and also choose the destination switch IP from the drop-down list.

- Step 4** From the drop-down list, choose the destination switch IP address.
- Step 5** Click **Next**.
The wizard configuration summary details appear.
- Step 6** Click **Finish** to create the switch-profile configuration.

Configuring the Sync Network View

**Note**

This feature is supported only on the Cisco Nexus 5000 Series switches.

The switch-profile network view captures all the Cisco Nexus 5000 Series vPC peers in the network. If a switch profile already exists in the peers, the corresponding switch profile sync status information displays in the configuration sync network view.

If no switch profile exists between the vPC peers, Cisco DCNM provides an option that allows you to configure the switch profile between the peers. If there are any dual-homed Fabric Extenders (FEXs) between the vPC peers, you can import the FEX host interfaces (HIF) configurations inside the switch profile.

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Configuration Change Management > Switch-Profile**.
All Cisco Nexus 5000 Series switches that are managed by Cisco DCNM are displayed in the Summary pane.

Send document comments to dcnm-docfeedback@cisco.com

- Step 2** From the Summary pane, choose a switch by right-clicking the switch that you want. You can choose one of the following options:
- **Migration**—This option is displayed only if there is no switch profile between the vPC Peers. Choose this option to launch the migration wizard using Cisco DCNM.
 - **Manage Switch profile**—Choose this option to go to the switch profile screen and choose the switch profile on the primary switch.

Configuring the Switch Profile Migration Wizard for Dual Homed FEXs



Note

This feature is supported only on the Cisco Nexus 5000 Series switches.

You can launch the migration wizard using any one of the following options:

- Migration Context menu
- Migration link provided in the switch-profile Name column.

Both options are active only when no switch profile is configured on both vPC peers.

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Configuration Change Management > Switch-Profile**. All the vPCs in the Cisco Nexus 5000 Series switch peers that are managed by Cisco DCNM are displayed in the Summary pane.
- Step 2** From the Summary pane, choose a row.
- Step 3** Right-click the selected row.
- Step 4** Choose the **Migration** option.
- The Migration wizard appears with the vPC peers switches as primary and secondary with the default switch-profile name.
- Step 5** A dual selector option with the FEXs that are present in the primary vPC switch is displayed in the Migration wizard.



Note

If the FEXs are online, they are automatically selected for the host interfaces (HIF) import. Any pre-provisioned FEXs will not be automatically selected.

- Step 6** Click **Next**.
- Step 7** Click **Finish**.

The wizard creates a switch profile on both the vPC peer switches with appropriate sync-peer IP addresses and also import all the FEX-HIF ports into the switch profile.

Send document comments to dcnm-docfeedback@cisco.com

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 8-25](#)
- [Field Descriptions for Archival Jobs, page 8-27](#)
- [Field Descriptions for the Archival Settings Contents Pane, page 8-28](#)
- [Field Descriptions for the Switch Profiles Pane, page 8-28](#)
- [Field Descriptions for the Switch Profiles Network View Pane, page 8-29](#)

Field Descriptions for the Version Browser

This section includes the following field descriptions for the Configuration Change Management feature:

- [Device: Details: Archival Status Section, page 8-25](#)
- [Device: Details: Rollback History Section, page 8-25](#)
- [Device: Details: Archival History Section, page 8-26](#)
- [Version: Version Details Tab, page 8-26](#)
- [Version: Compare Tab, page 8-26](#)

Device: Details: Archival Status Section

Table 8-3 ***Device: Details: Archival Status Section***

Field	Description
Status	<i>Display only.</i> Whether the archival job that the device is assigned to is enabled or disabled.
Schedule	<i>Display only.</i> When the archival job that the device is assigned to is scheduled to occur.
Job ID	<i>Display only.</i> Identification number of the archival job that the device is assigned to.

Device: Details: Rollback History Section

Table 8-4 ***Device: Details: Rollback History Section***

Field	Description
Time	<i>Display only.</i> Date and time that the rollback occurred.
Version	<i>Display only.</i> Configuration version that became the running configuration as a result of the rollback.
User	<i>Display only.</i> Username of the Cisco DCNM user who initiated the rollback.
Status	<i>Display only.</i> Whether the rollback succeeded or failed.

Send document comments to dcnm-docfeedback@cisco.com

Device: Details: Archival History Section

Table 8-5 **Device: Details: Archival History Section**

Field	Description
Time Stamp	<i>Display only.</i> Date and time that the archival event occurred.
Job Id	<i>Display only.</i> Identification number of the archival job that created the archival event.
Status	<i>Display only.</i> Whether the archival event succeeded, failed, or was skipped.
Reason	<i>Display only.</i> Cause of a skipped or failed archival event.

Version: Version Details Tab

Table 8-6 **Version: Version Details Tab**

Field	Description
Config Version ID	<i>Display only.</i> Version identification number for the archived configuration version. Each archived configuration for a device receives a unique version ID.
Creation Time	<i>Display only.</i> Date and time that an archival job created the configuration version.
Created By	<i>Display only.</i> 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 8-7 **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: <ul style="list-style-type: none"> 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.

Send document comments to dcnm-docfeedback@cisco.com

Field Descriptions for Archival Jobs

This section includes the following field descriptions for the Archival Jobs feature:

- [Archival Job: Details Tab, page 8-27](#)
- [Archival Job: Archival History Tab, page 8-27](#)

Archival Job: Details Tab

Table 8-8 ***Archival Job: Details Tab***

Field	Description
General	
Job ID	<i>Display only.</i> Identification number of the archival job.
Owner	<i>Display only.</i> 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 that 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	Archival job that 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	Archival job that 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	Archival job that occurs when Cisco DCNM 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 8-9 ***Installation Job: Details: General Section***

Field	Description
Time	<i>Display only.</i> Date and time that the archival job ran.
Status	<i>Display only.</i> 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.

Send document comments to dcnm-docfeedback@cisco.com

Table 8-9 ***Installation Job: Details: General Section (continued)***

Field	Description
Device Name	<i>Display only.</i> Name of a device assigned to the job. This field is shown when you expand the status of an archival history entry.
IP Address	<i>Display only.</i> 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)	<i>Display only.</i> Whether the archival job run succeeded, failed, or was skipped for the device.
Reason	<i>Display only.</i> 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 8-10 ***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	File server that Cisco DCNM selects 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	File server that Cisco DCNM uploads configurations to during a configuration rollback to 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.

Field Descriptions for the Switch Profiles Pane

Table 8-11 ***Switch Profiles Pane***

Field	Description
Name	Name of the switch-profile.
Revision ID	Current revision number of the switch profile.
Peer IP Address	IP address of the peer switch for the selected profile.
Last Session Time	Start time of the last configuration session.

Send document comments to dcnm-docfeedback@cisco.com

Field	Description
Last Session Status	Status of the last session action that was performed.
Sync Status	Overall sync status of that profile with the peer.

Field Descriptions for the Switch Profiles Network View Pane

Table 8-12 **Switch Profiles Network View Pane**

Field	Description
vPC	Hostname of the vPC primary and secondary switch.
Name	Name of the switch profile.
Revision ID	Current revision number of the switch profile.
Overall Sync Status	Switch profile status on the primary vPC switch.
Last Session Time	Start time of the last configuration session.
Last Session Status	Status of the last session action that was performed.

Additional References

For additional information related to configuration change management, see the following sections:

- [Related Documents, page 8-29](#)
- [Standards, page 8-29](#)

Related Documents

Related Topic	Document Title
File servers in Cisco DCNM	<i>File Servers, page 7-3</i>
Configuration rollbacks in Cisco NX-OS	<i>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x</i>

Standards

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

Send document comments to dcnm-docfeedback@cisco.com

Feature History for Configuration Change Management

Table 8-13 lists the release history for this feature.

Table 8-13 ***Feature History for Configuration Change Management***

Feature Name	Releases	Feature Information
Configuration Change Management	5.2(1)	Support was added to the Cisco Nexus 3000 Series switches (except the Switch Profile feature).
Configuration Change Management	5.1(1)	You can use the Copy Run to Start feature to copy the running configuration to the startup configuration.
Configuration Change Management	5.0(2)	Support was extended to all managed Cisco Nexus Series switches.



CHAPTER 9

Using Configuration Delivery Management

This chapter describes how to use the Configuration Delivery Management feature in Cisco Data Center Network Management (DCNM) Web client.

This chapter includes the following sections:

- [Information About Configuration Delivery Management, page 9-1](#)
- [Licensing Requirements for Configuration Delivery Management, page 9-16](#)
- [Prerequisites for Configuration Delivery Management, page 9-16](#)
- [Guidelines and Limitations for Configuration Delivery Management, page 9-17](#)
- [Platform Support, page 9-17](#)
- [Using Configuration Delivery Management, page 9-17](#)
- [Field Descriptions for Configuration Delivery Management, page 9-29](#)
- [Additional References, page 9-37](#)
- [Feature History for Configuration Delivery Management, page 9-38](#)

Information About Configuration Delivery Management



Note

Beginning with Cisco Release 6.1(1), Cisco DCNM supports the Cisco IOS platform.

The Configuration Delivery Management feature allows you to configure Cisco IOS and Cisco NX-OS features that Cisco DCNM does not support directly in the Cisco DCNM client user interface. For example, you can use Configuration Delivery Management to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) for Cisco Nexus 7000 Series devices.

With the Configuration Delivery Management feature, you create and schedule configuration delivery jobs. Each job can send device configuration commands to one or more devices.

Beginning with Cisco DCNM Release 6.1(1), this feature supports Cisco Catalyst 6500 Series, Cisco Nexus 1000 Series, Cisco Nexus 1010 Series, Cisco Nexus 3000 Series, Cisco Nexus 4000 Series, Cisco Nexus 5000 Series, Cisco Nexus 7000 Series, Cisco UCS devices, and Cisco MDS 9000 Series devices.

This section includes the following topics:

- [Job Sources, page 9-2](#)
- [Delivery Options, page 9-2](#)

Send document comments to dcnm-docfeedback@cisco.com

- [VDC Support, page 9-3](#)
- [Configuration Delivery Templates \(ASCII Text Files\), page 9-3](#)
- [Configuration Delivery Templates and the Cisco DCNM Client, page 9-5](#)
- [Configuration Delivery Template Requirements, page 9-8](#)

Job Sources

Each configuration delivery job is based on a source. This section includes the following topics:

- [Template-Sourced Jobs, page 9-2](#)

Template-Sourced Jobs

You can use templates that you create to configure the Cisco IOS and Cisco NX-OS commands to be sent to destination devices. For configuration delivery jobs based on a template source, you select the desired template and then configure the parameters for each instance of the template that you add to the job.

For each destination device that is included in the job, you can configure only one instance of the template.

**Note**

Template-sourced jobs do not support **show** commands, interactive commands, or commands that give command progress as output, such as the **copy running-config startup-config** command.

Delivery Options

For each configuration delivery job, you can specify how Cisco DCNM should respond if a failure occurs during the job. Cisco DCNM can continue the job regardless of errors, stop the job on all devices that are included in the job, or stop the job only on the device where the failure occurred but continue the job on other devices. If a job is delivering the same configuration to many devices, you may want Cisco DCNM to stop delivering the job to all devices if a single failure occurs, rather than risk delivering the same configuration error to all devices.

If the devices included in a job support the rollback feature, Cisco DCNM can use the rollback feature if a failure is encountered during a job. For example, Cisco Nexus 7000 Series devices support the rollback feature. You can specify that Cisco DCNM rolls back to the previous running configuration on the device that had the failure only or on all devices included in the job. You can also specify that Cisco DCNM should roll back to the previous running configuration on the device that had the failure and stop the job.

You can also specify whether Cisco DCNM delivers the configuration to all devices included in the job at the same time (parallel delivery) or if it delivers the configuration to devices one at a time (sequential delivery). While parallel delivery finishes configuring all the devices in a job more quickly, consider using sequential delivery when you would prefer that Cisco DCNM stop the delivery job to all devices if a failure occurs.

Send document comments to dcnm-docfeedback@cisco.com

VDC Support

Cisco DCNM treats each virtual device context (VDC) on a Cisco IOS and Cisco NX-OS device as a separate device; therefore, Configuration Delivery Management allows you to configure VDCs independent of the configuration of other VDCs on the same physical device.

Configuration Delivery Templates (ASCII Text Files)

Beginning with Cisco DCNM Release 6.1(1), you can create templates for use with template-sourced jobs. These templates are ASCII text files and must comply with the requirements that are described in this section.

This section includes the following topics:

- [Template Format, page 9-3](#)
- [Template Properties Section, page 9-3](#)
- [Template Content Section, page 9-4](#)
- [Example Template, page 9-4](#)

Template Format

Each template that you create must have a properties section and a content section. [Example 9-1](#) shows the required template format.

Example 9-1 Template Format

```
##template properties
name = template_name;
description = template_description;
##
##template content
configuration_commands
##
```

Template Properties Section

The template properties section must include the following two attribute-value pairs:

- **name**—Name of the template to be displayed in the Cisco DCNM client. The template name must be unique. No other template on the Cisco DCNM server should specify the same template name value. Specify the name in the following format:

```
name = template_name;
```

For example:

```
name = Interface Description Template;
```

- **description**—Description of the template, in the following format:

```
description = template_description;
```

For example:

Send document comments to dcnm-docfeedback@cisco.com

```
description = This file specifies the template for setting interface description;
```

Each of the two attribute-value pairs must end in a semicolon (;).

Template Content Section

The template content section contains the Cisco IOS and the Cisco NX-OS configuration commands and any parameters that you want to include in the template. Commands must not include prompts for answers and must not return progress output, such as the **copy running-config startup-config** command.

Specify the commands that you include as if you were entering them in the global configuration command mode on a Cisco IOS or a Cisco NX-OS device. You must consider the command mode when you include commands. For example, if you want to configure an interface, you must include the applicable **interface** command and the corresponding **exit** command to return to the global configuration mode.

Parameter names have two dollar symbols before and after the parameter name, as follows:

```
$$parameter$$
```



Note

Beginning with Cisco DCNM Release 5.2(1), parameter names are not mandatory.

The following example includes the parameter INTF_NAME to allow the interface type and number to be user specified in a configuration delivery job:

```
interface $$INTF_NAME$$
```

You can include many commands in the template content section.

Example Template

Example 9-2 shows a template that can be used to apply a description to an interface on a Cisco NX-OS device. When you create a template-sourced job with this template, you would specify the INTF_NAME, DESCRIPTION, and SHUT_CMD parameters for each instance of the template in the configuration delivery job. The INTF_NAME parameter allows the template to be applicable to different interfaces types, such as port-channel interfaces versus Ethernet interfaces. The DESCRIPTION parameter allows you to specify an interface description. The SHUT_CMD parameter allows you to specify the **shutdown** or **no shutdown** command.

Example 9-2 Example of an Interface Description Template

```
##template properties
name = Interface Description Template;
description = This file specifies the template for setting interface description;
##

##template content
interface $$INTF_NAME$$
  description $$DESCRIPTION$$
  $$SHUT_CMD$$
exit
##
```

Send document comments to dcnm-docfeedback@cisco.com

Configuration Delivery Templates and the Cisco DCNM Client

Beginning with Cisco DCNM Release 6.1(1), you can use the configuration delivery templates feature to configure many complex features in Cisco DCNM using various predefined templates. You can also create custom templates depending on your specific requirements. The predefined and custom templates can be created using template scripts that are defined by Cisco DCNM. With the configuration delivery templates feature, you can configure and deploy multiple devices at a time.

This section includes the following topics:

- [Predefined Templates, page 9-5](#)
- [Custom Templates, page 9-8](#)

Predefined Templates

This section describes the predefined configuration delivery templates that are available in the Cisco DCNM client. Each template must have a filename that ends with a .template extension, such as port_security.template.

Cisco DCNM can use templates that are in the templates directory within the archive directory. The archive directory is specified during server installation. The default location for templates on a Microsoft Windows server is the following directory:

C:\Program Files\Cisco Systems\dcn\dcnm\data\templates

The default location for templates on a RHEL server is the following directory:

/usr/local/cisco/dcm/dcnm/data/templates

**Note**

All the predefined templates present in DCNM-LAN client can be accessed through the DCNM-Web client, and vice versa.

Virtual Port Channel Template

To configure a virtual port channel (vPC) template on multiple devices, you must configure peer devices with peer-link port channels, vPC-enabled port channels, and an access switch with one port channel.

Cisco DCNM provides you with a peer-link access port channel template and a peer-link trunk port channel template for configuring vPC global configuration settings, peer-link port channels, and virtual access port channels. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: Virtual Port Channel Template” section on page 9-35](#).

FIP Snooping Template

To configure FCoE Initialization Protocol (FIP) snooping on multiple devices, you must configure a VLAN and interfaces that connect to an ENODE and Fibre Channel Forwarder (FCF). You can select one or more devices that you want to configure from the configuration settings for FIP snooping and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: FIP Snooping Template” section on page 9-31](#).

Send document comments to dcnm-docfeedback@cisco.com

FCoE Template

To configure Fibre Channel over Ethernet (FCoE) on multiple devices, you must configure a VLAN, a VSAN, a virtual Fibre Channel (VFC), and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings for FCoE and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: FCoE Template”](#) section on page 9-31.

OTV Internal Interfaces Template

To configure OTV internal interfaces on multiple devices, you must configure a Internal IFS, a Site VLANs, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings for OTV Internal Interfaces, and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: OTV Internal Interfaces Template”](#) section on page 9-31.

OTV Multicast Template

To configure OTV Multicast on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: OTV Multicast Template”](#) section on page 9-31.

OTV Multicast with HSRP Isolation Template

To configure OTV Multicast with HSRP Isolation on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: OTV Multicast with HSRP Isolation Template”](#) section on page 9-32.

OTV Multicast with VRRP Isolation Template

To configure OTV Multicast with VRRP Isolation on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: OTV Multicast with VRRP Isolation Template”](#) section on page 9-32.

OTV Unicast with One Adjacency Server Template

To configure OTV Unicast with one adjacency server on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, adjacency server, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the [“Configuration Delivery for Templates: OTV Unicast with One Adjacency Server Template”](#) section on page 9-33.

OTV Unicast with One Adjacency Server and HSRP Isolation Template

To configure OTV Unicast with one adjacency server on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, adjacency server, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct

Send document comments to dcnm-docfeedback@cisco.com

values in the respective fields. For more information about the field descriptions, see the “[Configuration Delivery for Templates: OTV Unicast with One Adjacency Server and HSRP Isolation Template](#)” section on page 9-33.

OTV Unicast with One Adjacency Server and VRRP Isolation Template

To configure OTV Unicast with one adjacency server on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, adjacency server, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the “[Configuration Delivery for Templates: OTV Unicast with One Adjacency Server and VRRP Isolation Template](#)” section on page 9-33.

OTV Unicast with Two Adjacency Servers Template

To configure OTV Unicast with one adjacency server on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, the primary and secondary adjacency servers, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the “[Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers Template](#)” section on page 9-34.

OTV Unicast with Two Adjacency Servers and HSRP Isolation Template

To configure OTV Unicast with one adjacency server on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, the primary and secondary adjacency servers, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the “[Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers and HSRP Isolation Template](#)” section on page 9-34.

OTV Unicast with Two Adjacency Servers and VRRP Isolation Template

To configure OTV Unicast with one adjacency server on multiple devices, you must configure a Site VLAN, a Site ID, an Overlay, a control group, the primary and secondary adjacency servers, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the “[Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers and VRRP Isolation Template](#)” section on page 9-35.

Virtual Port Channel Template

To configure virtual port channel on multiple devices, you must configure a VPC ID, an Channel number, VLAN account, , and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information about the field descriptions, see the “[Configuration Delivery for Templates: Virtual Port Channel Template](#)” section on page 9-35.

Zone Template

To configure virtual port channel on multiple devices, you must configure a hostname, storage, VSAN ID, host , zone set, and multiple interfaces. You can select one or more devices that you want to configure from the configuration settings and enter the correct values in the respective fields. For more information

Send document comments to dcnm-docfeedback@cisco.com

about the field descriptions, see the “Configuration Delivery for Templates: Zone Template” section on [page 9-37](#).

Custom Templates

You can create, edit, and delete custom templates depending on your specific requirements. The user interface for a custom template is created dynamically based on the template. To create a custom template, you need to understand the syntax rules that are defined in the Cisco DCNM template definition file.

-

Configuration Delivery Template Requirements

Beginning with Cisco DCNM Release 6.1(1), you can create configuration delivery templates with the Cisco DCNM client. When you create custom templates or modify existing templates, the template must comply with the requirements that are described in this section.

This section includes the following topics:

- [Template Format, page 9-8](#)
- [Template Properties Section, page 9-9](#)
- [Template Variable Section, page 9-9](#)
- [Template Content Section, page 9-9](#)
- [Example Template, page 9-11](#)
- [Template Data Types, page 9-12](#)

Template Format

Each template that you create must have a properties section and a content section. [Example 9-3](#) shows the custom template format.



Note

When creating or changing a template, ensure that the userDefined property is set to “true.” If the userDefined property is “false” and the template is deployed, then the template becomes permanent and cannot be deleted.

Example 9-3 Custom Template Format

```
##template properties
name = FCOE Template;
description = This file specifies the template configuration for FCOE;
userDefined=true;
##

##template content
feature fcoe
fcoe fcmmap $$FC_MAP$$
vsan database
vsan $$VLAN_ID_RANGE$$
exit
```


Send document comments to dcnm-docfeedback@cisco.com

Template Properties Section

The template properties section must include the name attribute-value pair and the description attribute-value pair. Other attribute-value pairs are optional:

- **name**—Name of the template to be displayed in the Cisco DCNM client. The template name must be unique. No other template on the Cisco DCNM server should specify the same template name value. Specify the name in the following format:

```
name = template name;
```

For example:

```
name = FCoE Template;
```

- **description**—Description of the template, in the following format:

```
description = template description;
```

For example:

```
description = This file specifies the template for setting FCoE
```

- (Optional) **supportedPlatforms**—List of device platforms that are supported. The valid values for this attribute are C6500, N1K, N1010, N3K, N4K, N5K, N5500, or N7K. The values must be specified in a comma-delimited list.

For example:

```
supportedPlatforms = N5K, N7K;
```



Note If the supportedPlatforms attribute is not specified, the template is applicable for all platforms.

- (Optional) **unsupportedPlatforms**—List of device platforms that are not supported. The valid values for this attribute are C6500, N1K, N1010, N3K, N4K, N5K, N7K, or N5500. The values must be specified in a comma-delimited list.

For example:

```
unsupportedPlatforms = N5K, N7K;
```



Note All specified attribute-value pairs must end in a semicolon (;).

Template Variable Section

The template variable section contains the data type, default values, and valid values conditions for the parameters that are used in the template. The template variable section is optional. If you do not provide this section, Cisco DCNM parses the variables from the template content section. The type of the parsed parameters is a string by default.

Template Content Section

The template content section contains the Cisco IOS and the Cisco NX-OS configuration commands and any parameters that you want to include in the template. Specify the commands that you include as if you were entering them in the global configuration command mode on a Cisco IOS or a Cisco NX-OS device. You must consider the command mode when you include commands.

Send document comments to dcnm-docfeedback@cisco.com

Parameter names have two dollar symbols before and after the parameter name, as follows:

`$$parameter$$`



Note

Beginning with Cisco DCNM Release 5.2(1), parameter names are not mandatory.

Implicit Template Variables

Cisco DCNM supports two implicit template variables, `DEVICE_TYPE` and `DEVICE_IMG_VERSION`.

`DEVICE_TYPE` is used to represent a target device platform. The valid values are C6500, N1K, N1010, N3K, N4K, N5K, N7K or N5500.

For example, the `DEVICE_TYPE` variable can be used in an if construct:

```
if ($$DEVICE_TYPE$$ == "N7K" || $$DEVICE_TYPE$$ == "N1010")
```

`DEVICE_IMG_VERSION` is used to represent a target device image version.

Foreach Loop Construct

The DCNM template engine supports a foreach loop construct. This construct is used for template configurations that are required for a set of interfaces or VLAN IDs.

The syntax for the construct is as follows:

```
foreach <FOR_LOOP_VARIABLE> in $$FOR_LOOP_RANGE$$
{<SET of commands with placeholders for a for loop index variable, such as
@FOR_LOOP_VARIABLE>
```

For example:

```
##template properties
name = FCOE Template;
description = This file specifies the template configuration for FCOE;
userDefined=false;
##
##template variables
integerRange VLAN_ID_RANGE;
integerRange VFC_PORT_NUM_RANGE;
##
##template content
feature fcoe
fcoe fcmap $$FC_MAP$$
vsan database
vsan $$VLAN_ID_RANGE$$
exit

foreach VLAN_ID in $$VLAN_ID_RANGE$$ {
vlan @VLAN_ID
fcoe vsan @VLAN_ID
exit
}
foreach VFC_PORT_NUM in $$VFC_PORT_NUM_RANGE$$ {
interface vfc @VFC_PORT_NUM
bind interface ethernet 1/@VFC_PORT_NUM
no shutdown
exit

foreach VLAN_ID in $$VLAN_ID_RANGE$$ {
```

Send document comments to dcnm-docfeedback@cisco.com

```
vsan database
vsan @VLAN_ID interface vfc @VFC_PORT_NUM
exit
}
}
##
```

If Conditional Construct

The DCNM template engine supports the if | else if | else loop construct. This construct is used for template configurations that need to be applied based on specific conditions.



Note

Make sure that the else if and else blocks start on a new line after an if block.

For example:

```
##template properties
name = FCOE Template;
description = This file specifies the template configuration for FCOE;
userDefined=false;
##
##template variables
integerRange VLAN_ID_RANGE;
integerRange VFC_PORT_NUM_RANGE;
##
##template content
feature fcoe
if ($$FC_MAP$$) {
## deliver only if there is a valid value given for FC_MAP
fcoe fcmmap $$FC_MAP$$
}
vsan database
vsan $$VLAN_ID_RANGE$$
exit
if ($$DEVICE_TYPE$$ == "N7K" && $$ DEVICE_IMG_VERSION$$ == "4.2(3)") {
<some commands specific to N7K with image version 4.2(3)>
}
else if ($$DEVICE_TYPE$$ == "N7K") {
<commands specific to N7K with any image other than 4.2(3)>
}
else if ($$DEVICE_TYPE$$ == "N5K") {
<commands specific to N5K device>
}
else {
<commands specific to any device other than N7K and N5K>
}
##
```

Example Template

[Example 9-4](#) shows a template that can be used to apply a description to configuring FCoE on a Cisco NX-OS device. When you create a template for configuration delivery management with this template, you would specify the NAME, DESCRIPTION, VLAN_ID_RANGE, and VFC_PORT_NUM_RANGE parameters for each instance of the template.

Example 9-4 Example of an FCoE Template

```
##template properties
```

Send document comments to dcnm-docfeedback@cisco.com

```
name = FCOE Template;
description = This file specifies the template configuration for FCOE;
userDefined=true;
##
##template variables
integerRange VLAN_ID_RANGE;
integerRange VFC_PORT_NUM_RANGE;
##
##template content
feature fcoe
fcoe fcmap $$FC_MAP$$
vsan database
vsan $$VLAN_ID_RANGE$$
exit
```

Example 9-5 shows a FIP Snooping template.

Example 9-5 Example of a FIP Snooping Template

```
##template properties
name = FIP SNOOPING Template;
description = This file specifies the template configuration for FIP Snooping;
userDefined=false;
supportedPlatforms = N4K, N4K;
N4K.supportedImages = 4.1(2)N1(1);
N4K.supportedImages = 4.1(2)N1(1);
##
##template content
feature fip-snooping
vlan $$VLAN_ID$$
fip-snooping enable
fip-snooping fc-map $$FC_MAP$$
exit
interface $$ENODE_INF$$
no fip-snooping port-mode fcf
switchport mode trunk
switchport trunk allowed vlan $$VLAN_ID$$
switchport trunk allowed vlan add $$OLD_VLAN_ID$$
switchport trunk native vlan $$OLD_VLAN_ID$$
spanning-tree port type edge trunk
lldp receive
lldp transmit
exit
interface $$FCF_INF$$
switchport mode trunk
switchport trunk allowed vlan add $$VLAN_ID$$
fip-snooping port-mode fcf
exit
##
```

Template Data Types

Template data types are used to build templates. Associated with each data type are certain metadata properties that are used by the template engine to validate the values for the data type.

to show an overview of template data types that are used to build templates, metadata properties, and the association of data types and metadata properties.

Table 9-1 Overview of Data Types

Send document comments to dcnm-docfeedback@cisco.com

Data Type	Description
boolean	A Boolean value. Example: true
enum	Value that is any one of the string values from a fixed set of strings. Example: [pagp,lacp] or [running-config,startup-config]
float	Value that is a signed real number. Example: 10.08 or -8.08
floatRange	Value that is a range of signed real numbers. Example: 100.08 – 110.08
integer	Value that is a signed number. Example: 100 or -120
integerRange	Value that is a range of signed numbers. Example: -120 - -100 or -120 – 100
interface	Value that is the name of an interface/port. Example: FastEthernet1/10
interfaceRange	Value that is a range of interface/port names. Example: FastEthernet 1/10-18, Gi 2/8, or Gi 3/5-8
ipV4Address	Value that is an IP address version 4. Example: 10.8.8.8
ipV6Address	Value that is an IP address version 6. Example: 10:8:8:10:4:6
ipAddress	Value that is either an IP v4 Address or IP v6 Address.
macAddress	Value that is a MAC address. Example: 02.00.4C.4F.4F.50
string	Value that is a literal string. Example: abc or def

All data types have some metadata properties. The following table shows all the possible metadata properties for all data types.

Table 9-2 Metadata Properties

Metadata Property	Description
defaultValue	Default value of the data type. For an integer data type, an example is defaultValue = 8.
validValues	Valid values that are allowed for the data type. For an integer data type, an example is validValues=1,5,8,10-100.

Send document comments to dcnm-docfeedback@cisco.com

Metadata Property	Description
decimalLength	<p>Number of digits allowed after the decimal point for a float value.</p> <p>If a value has more digits than the length specified, the template engine truncates the value.</p> <p>For a float value of length 2, an example is decimalLength = 2.</p>
min	<p>Minimum value for the data type.</p> <p>An example is min=1.2345.</p>
max	<p>Maximum value for the data type.</p> <p>An example is max=10.10.</p>
minSlot	<p>Minimum valid slot number.</p> <p>The template engine validates that the given interface name is of a port whose card is placed either in a given slot or in a slot that comes after the minimum slot number.</p> <p>An example is minSlot=2.</p>
maxSlot	<p>Maximum valid value slot number.</p> <p>The template engine validates that the given interface name is of a port whose card is placed either in the given slot or in a slot that comes before the maximum slot number.</p> <p>An example is maxSlot=12.</p>
minPort	<p>Minimum port number.</p> <p>The template engine validates that the port number in the given interface name is less than or equal to that of the minimum port number.</p> <p>This property is applicable for logical port numbers also.</p> <p>An example is minPort=2.</p>
maxPort	<p>Maximum port number.</p> <p>The template engine validates that the port number in the given interface name is greater than or equal to that of the maximum port number.</p> <p>This property is applicable for logical port numbers also.</p> <p>An example is maxPort=8.</p>
minLength	<p>Minimum number of characters in a string value.</p> <p>An example is minLength=5.</p>
maxLength	<p>Maximum number of characters in a string value.</p> <p>An example is maxLength=255.</p>
regularExpr	<p>Regular expression that the template engine matches to a string value.</p> <p>If the string value does not match the given regular expression, the template engine raises an error.</p> <p>Note This property expects regular expressions that are in an acceptable format used by Java.</p> <p>An example is regularExpr=.*abc.*.</p>

Send document comments to dcnm-docfeedback@cisco.com

The following table shows the association of data types and metadata properties.

Table 9-3 Association of Data Types and Metadata Properties

Data Type	Metadata Property
boolean	<ul style="list-style-type: none"> • defaultValue
enum	<ul style="list-style-type: none"> • defaultValue • validValues Example: validValues= pagp, lacp.
float	<ul style="list-style-type: none"> • defaultValue • validValues • decimalLength • min • max
floatRange	<ul style="list-style-type: none"> • defaultValue • validValues • decimalLength • min • max
integer	<ul style="list-style-type: none"> • defaultValue • validValues • min • max
integerRange	<ul style="list-style-type: none"> • defaultValue • validValues • min • max
interface	<ul style="list-style-type: none"> • defaultValue • validValues • minSlot • maxSlot • minPort • maxPort

Send document comments to dcnm-docfeedback@cisco.com

Data Type	Metadata Property
interfaceRange	<ul style="list-style-type: none"> • defaultValue • validValues • minSlot • maxSlot • minPort • maxPort
ipV4Address	This data type does not support any metadata properties.
ipV6Address	This data type does not support any metadata properties.
ipAddress	This data type does not support any metadata properties.
macAddress	This data type does not support any metadata properties.
string	<ul style="list-style-type: none"> • defaultValue • validValues • minLength • maxLength • regularExpr
WWN	This data type does not support any metadata properties. Example : 20:01:00:08:02:11:05:03.

Licensing Requirements for Configuration Delivery Management

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Configuration Delivery Management requires no license. Any feature not included in a license package is bundled with Cisco DCNM and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the <i>Cisco DCNM Installation and Licensing Guide, Release 5.x</i> .
Cisco NX-OS	Using the Configuration Delivery Management feature with a Cisco NX-OS device requires no Cisco NX-OS license; however, Cisco NX-OS features that require a license can be configured by Configuration Delivery Management only if the Cisco NX-OS device has the applicable license installed. For an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites for Configuration Delivery Management

The Configuration Delivery Management feature has the following prerequisites:

- The Configuration Delivery Management feature supports only devices that are managed by Cisco DCNM, which means that Cisco DCNM must have successfully discovered the device.

Send document comments to dcnm-docfeedback@cisco.com

- Devices must be reachable by Cisco DCNM when Cisco DCNM attempts to deliver the configuration. A delivery job fails if the device is unreachable by Cisco DCNM.

Guidelines and Limitations for Configuration Delivery Management

Configuration Delivery Management has the following configuration guidelines and limitations:

- The following types of Cisco IOS and the Cisco NX-OS configuration commands are not supported with Configuration Delivery Management:
 - Interactive configuration commands (that is, any command that includes prompts for user input).
 - Commands that give command progress as output, such as the **copy running-config startup-config** command.
- Rollback is supported for configuration delivery only if the destination device supports the rollback feature. For example, Cisco Nexus 7000 Series devices support rollback, but Cisco Nexus 1000V Series switches do not.

Platform Support

The following platforms support this feature but might implement it differently. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Catalyst 6500 Series switches	Cisco Catalyst 6500 Series Switches Documentation
Cisco Nexus 1000V Series switches	Cisco Nexus 1000V Series Switch Documentation
Cisco Nexus 3000 Series switches	Cisco Nexus 3000 Series Switch Documentation
Cisco Nexus 4000 Series switches	Cisco Nexus 4000 Series Switch Documentation
Cisco Nexus 5000 Series switches	Cisco Nexus 5000 Series Switch Documentation
Cisco Nexus 5500 Series switches	Cisco Nexus 5500 Series Switch Documentation
Cisco Nexus 7000 Series switches	Cisco Nexus 7000 Series Switch Documentation
Cisco MDS 9000 Series switches	Cisco MDS 9000 Series Switch Documentation
Cisco UCS Series switches	Cisco UCS Series Switch Documentation

Using Configuration Delivery Management

This section includes the following topics:

- [Creating a Configuration Delivery Management Job](#), page 9-18
- [Adding a Configuration Delivery Job](#), page 9-19
- [Adding a Predefined Template \(ASCII Text Files\)](#), page 9-21

Send document comments to dcnm-docfeedback@cisco.com

- [Adding a Custom Template in the Cisco DCNM SAN Client](#), page 9-21
- [Changing a Predefined Template \(ASCII Text Files\)](#), page 9-23
- [Changing a Custom Template in the Cisco DCNM Client](#), page 9-24
- [Removing a Predefined Template \(ASCII Text Files\)](#), page 9-24
- [Removing a Custom Template in the Cisco DCNM Client](#), page 9-25
- [Refreshing Cisco DNCM Servers with Template Updates \(ASCII Text Files\)](#), page 9-25
- [Configuring Job Delivery Options](#), page 9-27
- [Scheduling a Configuration Delivery Job](#), page 9-27
- [Removing a Configuration Delivery Job](#), page 9-28

Creating a Configuration Delivery Management Job

Creating a configuration delivery management job has many steps, which vary depending upon the type of job that you are creating. This procedure summarizes the creation of a configuration delivery job and directs you to more detailed procedures for each of the summarized steps.

-
- Step 1** Select a Add a configuration delivery job of the type that you need.
- For more information, see the [“Adding a Configuration Delivery Job”](#) section on page 9-19.
- Step 2** Add one or more destination devices for the job.
- For more information, see the [“Adding a Predefined Template \(ASCII Text Files\)D”](#) section on page 9-21.
- Step 3** Configure the Cisco IOS and Cisco NX-OS commands to be delivered to the destination devices by the job. More information for doing so varies depending upon the type of job, as follows:
- For a job with manually entered Cisco IOS or Cisco NX-OS commands, see the [“Adding a Predefined Template \(ASCII Text Files\)D”](#) section on page 9-21.
 - For a job with Cisco IOS or Cisco NX-OS commands retrieved from a source device, see the [“Adding a Predefined Template \(ASCII Text Files\)D”](#) section on page 9-21.
 - For a job with Cisco IOS or Cisco NX-OS commands from a Cisco DCNM template, see the [“Adding a Predefined Template \(ASCII Text Files\)D”](#) section on page 9-21.



Note Before you can add a template-source job, you must add templates to Cisco DCNM. For more information, see the [“Configuration Delivery Templates and the Cisco DCNM Client”](#) section on page 9-5.

- Step 4** (Optional) Configure job delivery options, which determine the following:
- How Cisco DCNM responds if a delivery job results in configuration errors on a device.
 - Whether Cisco DCNM delivers Cisco IOS or Cisco NX-OS commands to all devices in the job at the same time or one device at a time.

For more information, see the [“Configuring Job Delivery Options”](#) section on page 9-27.

- Step 5** Schedule the job.

Send document comments to dcnm-docfeedback@cisco.com

For more information, see the “Scheduling a Configuration Delivery Job” section on page 9-27.

Adding a Configuration Delivery Job

You can add a configuration delivery job as required. You can select a template, assign it to the selected device, and define the variables for the template. You can also schedule a job to be run on a particular device at a specific time.

BEFORE YOU BEGIN

Note that only template based jobs can be created. For more information about job types, see the “Job Sources” section on page 9-2.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Config > Delivery > Templates..**
- The Summary pane lists the configuration delivery templates that are configured in Cisco DCNM, if any. For more information see [Adding a Predefined Template \(ASCII Text Files\)D](#), page 9-21
- Step 2** Select a template and click on the **Launch Job** button to display the **Config Job Wizard**.
- Step 3** Select the device to which you want to assign the template.
- For more information see [Selecting a Device](#), page 9-19
- Step 4** Define variables for the template.
- For more information see
- Step 5** Preview the configuration in the preview pane. For more information see [Previewing a Configuration](#), page 9-20
- Step 6** Schedule a job. For more information see [Scheduling a Configuration Delivery Job](#), page 9-27.
- Step 7** Click Finish to complete the configuration delivery job creation..



Note You may be unable to deploy the job until after you have further configured the job.

Selecting a Device

You can select a device to be associated with the template.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Config > Delivery > Templates..**
- The Summary pane lists the configuration delivery templates that are configured in Cisco DCNM, if any. For more information see [Adding a Predefined Template \(ASCII Text Files\)D](#), page 9-21

Send document comments to dcnm-docfeedback@cisco.com

- Step 2** Select a template and click on the Launch Job button to display the **Config Job Wizard**.
 - Step 3** Click on the **Next** button to display the device selection screen.
 - Step 4** Select the **Device Scope** from the drop down list. It lists the all the devices available for selected template.
 - Step 5** You can view the **Device, IP Address, Group, Platform,** and the **Version**. Select the device to which you want to assign the template.
 - Step 6** Click **Next**.
-

Defining Variables

You can define variables for the selected device and the corresponding template.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Config > Delivery > Templates..**
The Summary pane lists the configuration delivery templates that are configured in Cisco DCNM, if any. For more information see [Adding a Predefined Template \(ASCII Text Files\)D, page 9-21](#)
 - Step 2** Select a template and click on the Launch Job button to display the **Config Job Wizard**.
 - Step 3** Click on the **Next** button to display the device selection screen.
 - Step 4** After selecting the device for the template, set the variables for the device and the template.
 - Step 5** Enter the **VSAN_ID, SLOT_NUMBER, PORT_RANGE,** and the **VFC_PREFIX**.
 - Step 6** Select the **Edit variables per device** checkbox to set the variables for each individual devices selected for the template.
 - Step 7** You either keep the values global for all the devices in the list, or change the individual values in the respective rows.
 - Step 8** Click **Next**.
-

Previewing a Configuration

You can preview the configuration for each device.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Config > Delivery > Templates..**
The Summary pane lists the configuration delivery templates that are configured in Cisco DCNM, if any. For more information see [Adding a Predefined Template \(ASCII Text Files\)D, page 9-21](#)
 - Step 2** Select a template and click on the Launch Job button to display the **Config Job Wizard**.
 - Step 3** Click on the **Next** button to display the device selection screen.
 - Step 4** After setting the variables for the selected devices and the templates, you can preview the configuration.

Send document comments to dcnm-docfeedback@cisco.com

- Step 5** Select a device from the drop down list to preview the configuration.
- Step 6** Click **Next**.
-

Adding a Predefined Template (ASCII Text Files)

You can create an ASCII text file template for use in a template-sourced configuration delivery job.

BEFORE YOU BEGIN

Review the [“Configuration Delivery Templates \(ASCII Text Files\)”](#) section on page 9-3.

DETAILED STEPS

-
- Step 1** Create the template file, ensuring that it meets the template requirements and includes the configuration commands that you need.
- Step 2** Place a copy of the template file in the templates directory. The templates directory is in the archive directory that was specified during Cisco DCNM server installation. For Microsoft Windows, the path to the default templates directory is C:\Program Files\Cisco Systems\dcn\dcnm\data\templates. For RHEL, the default path is /usr/local/cisco/dcm/dcnm/data/templates.
- Step 3** Refresh the Cisco DCNM server. If you have a clustered-server Cisco DCNM deployment, you must refresh only the master server of the cluster.
- For more information, see the [“Refreshing Cisco DNCM Servers with Template Updates \(ASCII Text Files\)”](#) section on page 9-25.
- The new template is now available when you create a template-sourced configuration delivery job.
-

Adding a Custom Template in the Cisco DCNM SAN Client

With the Cisco DCNM client, you can add custom templates for deploying configuration delivery jobs.

BEFORE YOU BEGIN

Review the [“Configuration Delivery Template Requirements”](#) section on page 9-8.

DETAILED STEPS

-
- Step 1** From the Features Selector pane, choose **Configuration Delivery > Templates**.
- The Summary pane lists the custom templates that are configured in the Cisco DCNM, if any.
- Step 2** From the menu bar, choose **Create New Config Template**.
- The fields for the new template appears in the **Config Template** pane.

Send document comments to dcnm-docfeedback@cisco.com

- Step 3** In the pane for the new template, enter the **Template Name**, **Template Description**, and **Tags** for the template.
- Step 4** Select the appropriate check boxes for the **Supported Platforms** field.
- Step 5** Click the **Validate Template Syntax** button to verify that the template does not contain errors.
If errors exist, the errors in the template are identified with red indicators in the Details pane. Cisco DCNM does not allow you to save a template that contains errors.
- Step 6** Click **Save** to save the template details.

•

Importing a Custom Template in the Cisco DCNM SAN Client

With the Cisco DCNM client, you can import custom templates for deploying configuration delivery jobs.

BEFORE YOU BEGIN

Review the [“Configuration Delivery Template Requirements”](#) section on page 9-8.

DETAILED STEPS

- Step 1** From the Features Selector pane, choose **Config Delivery > Templates** .
The Summary pane lists the custom templates that are configured in the Cisco DCNM, if any.
- Step 2** From the menu bar, choose **Import**. The folder browser option is displayed.
- Step 3** Navigate and select the target folder and the file.
- Step 4** Once the file is selected, click **OK**. The selected template is imported into the DCNM and will be available for scheduling configuration delivery jobs.



Note The template will be validated and if there are any errors then a warning message is displayed.

•

Exporting a Custom Template in the Cisco DCNM SAN Client

With the Cisco DCNM client, you can export custom templates for deploying configuration delivery jobs.

Send document comments to dcnm-docfeedback@cisco.com

BEFORE YOU BEGIN

Review the “[Configuration Delivery Template Requirements](#)” section on page 9-8.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Features Selector pane, choose Config Delivery > Templates .
The Summary pane lists the custom templates that are configured in the Cisco DCNM, if any. |
| Step 2 | From the menu bar, choose Export . The folder browser option is displayed. |
| Step 3 | Navigate and select the target folder and enter the file name for the template. |
| Step 4 | Click OK. , to export the selected template to the target folder. |
-

•

Changing a Predefined Template (ASCII Text Files)

You can change templates (ASCII text files) that are available for use in a configuration delivery job.

BEFORE YOU BEGIN

Review the “[Configuration Delivery Templates \(ASCII Text Files\)](#)” section on page 9-3.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Locate the template file in the templates directory. The templates directory is in the archive directory that was specified during Cisco DCNM server installation. For Microsoft Windows, the path to the default templates directory is C:\Program Files\Cisco Systems\dcn\dcnm\data\templates. For RHEL, the default path is /usr/local/cisco/dcm/dcnm/data/templates. |
| Step 2 | Open the template file in a text editor and make the required changes. |
| Step 3 | Save and close the template file. |



Note	If you have a clustered-server Cisco DCNM deployment, you must change the template file on each Cisco DCNM server in the cluster.
-------------	---

- | | |
|---------------|---|
| Step 4 | Refresh the Cisco DCNM server. If you have a clustered-server Cisco DCNM deployment, you must refresh each server in the cluster.

For more information, see the “ Refreshing Cisco DNCM Servers with Template Updates (ASCII Text Files) ” section on page 9-25.

The changed template is now available when you create a template-sourced configuration delivery job. |
|---------------|---|
-

Send document comments to dcnm-docfeedback@cisco.com

Changing a Custom Template in the Cisco DCNM Client

With the Cisco DCNM client, you can change custom templates created for deploying configuration delivery jobs.

BEFORE YOU BEGIN

Review the [“Configuration Delivery Template Requirements”](#) section on page 9-8.

DETAILED STEPS

-
- Step 1** From the Features Selector pane, choose **Config Delivery > Templates** .
The Summary pane lists the custom templates that are configured in the Cisco DCNM, if any.
 - Step 2** From the list of template, select one and choose **Modify**.
The fields for the template appears in the **Config Template** pane.
 - Step 3** In the pane for the selected template, enter the **Template Name**, **Template Description**, and **Tags** for the template.
 - Step 4** Select the appropriate check boxes for the **Supported Platforms** field.
 - Step 5** Click the **Validate Template Syntax** button to verify that the template does not contain errors.
If errors exist, the errors in the template are identified with red indicators in the Details pane. Cisco DCNM does not allow you to save a template that contains errors.
 - Step 6** Click **Save** to save the template details.
-
-
-

Removing a Predefined Template (ASCII Text Files)

You can remove templates (ASCII text files) from Cisco DCNM, which makes them unavailable for use in a configuration delivery job.

DETAILED STEPS

-
- Step 1** Locate the template file in the templates directory at the following location:
`INSTALL_DIR\jboss-4.2.2.GA\server\dcnm\cisco\templates`
For Microsoft Windows, the path to the default Cisco DCNM installation directory is C:\Program Files\Cisco Systems. For RHEL, the default path is /usr/local/cisco.
 - Step 2** Delete or remove the template file from the templates directory.

**Note**

If you have a clustered-server Cisco DCNM deployment, you must remove the template file from the templates directory on each Cisco DCNM server in the cluster.

Send document comments to dcnm-docfeedback@cisco.com

- Step 3** Refresh the Cisco DCNM server. If you have a clustered-server Cisco DCNM deployment, you must only refresh the master server.
- For more information, see the [“Refreshing Cisco DNCM Servers with Template Updates \(ASCII Text Files\)” section on page 9-25](#).
- The removed template is no longer available when you create a template-sourced configuration delivery job.
-

Removing a Custom Template in the Cisco DCNM Client

With the Cisco DCNM client, you can delete custom templates that were created for deploying configuration delivery jobs.

DETAILED STEPS

-
- Step 1** From the Features Selector pane, choose **Config Delivery> Templates** .
- The Summary pane lists the custom templates that are configured in the Cisco DCNM, if any.
- Step 2** From the list of template, select one. The fields for the template appears in the **Config Template** pane.
- Step 3** From the menu bar choose **Delete** .
- Step 4** Click **Save** to save the template details.
-

Refreshing Cisco DNCM Servers with Template Updates (ASCII Text Files)

After you have made updates to templates (ASCII text files), including adding, changing, or removing templates, you must refresh the template list before users can see the updates in the Cisco DCNM client. This procedure allows you to refresh a Cisco DCNM server with updates to templates without requiring a server stop and start. If you stop and start a Cisco DCNM server after updating templates, you do not need to perform this procedure.



Note

When updating templates with the Cisco DCNM client, the Cisco DCNM server is updated automatically. You do not have to manually refresh the Cisco DCNM server.

BEFORE YOU BEGIN

Update templates as needed.

If you have a clustered-server deployment, ensure that you know which server is currently operating as the master server. To do so, use the Cluster Administration feature in the Cisco DCNM client. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

DETAILED STEPS

-
- Step 1** On the Cisco DCNM server, access a command prompt.

Send document comments to dcnm-docfeedback@cisco.com



Note If you have a clustered-server deployment, ensure that you are performing these steps on the master server.

Step 2 Use the **cd** command to change the directory to the following location:

```
INSTALL_DIR\dcn\jboss-4.2.2.GA\bin
```

For Microsoft Windows, the path to the default Cisco DCNM installation directory is C:\Program Files\Cisco Systems. For RHEL, the default path is /usr/local/cisco.

Step 3 Enter the following command:

```
set JAVA_HOME=INSTALL_DIR\dcn\java\jre1.6
```

For example, on a Microsoft Windows server with Cisco DCNM installed in the default directory, you would enter the following command:

```
set JAVA_HOME=C:\Program Files\Cisco Systems\dcn\java\jre1.61
```

On a RHEL server with Cisco DCNM installed in the default directory, you would enter the following command:

```
set JAVA_HOME=/usr/local/cisco/dcn/java/jre1.6
```

Step 4 Enter the following command:

```
twiddle_script -s IP_address:naming_service_port invoke  
"com.cisco.dcbu.dcm:service=ConfigDeliveryService" populateTemplates
```

where the arguments are as follows:

- *twiddle_script*—Script name depending upon the server operating system, as follows:
 - Microsoft Windows: twiddle.bat
 - RHEL: twiddle.sh
- *IP_address*—IPv4 address of the Cisco DCNM server. In a clustered-server deployment, this address must be the address of the master server.
- *naming_service_port*—Naming Service port that the Cisco DCNM server is configured to use. By default, the Naming Service port is 1099.

For example, on a Microsoft Windows server using the default Naming Service port and the IP address 10.0.0.0, you would enter the following command:

```
twiddle.bat -s 10.0.0.0:1099 invoke "com.cisco.dcbu.dcm:service=ConfigDeliveryService"  
populateTemplates
```

For example, on a RHEL server using the default Naming Service port and the IP address 10.0.0.0, you would enter the following command:

```
twiddle.sh -s 10.0.0.0:1099 invoke "com.cisco.dcbu.dcm:service=ConfigDeliveryService"  
populateTemplates
```

The Cisco DCNM server begins using the updates to the templates.

Step 5 (Optional) To see the updates to the templates in the Cisco DCNM client, press **F5** to refresh the screen.

Send document comments to dcnm-docfeedback@cisco.com

Configuring Job Delivery Options

You can configure job delivery options for each configuration delivery job. Job delivery options allow you to specify the following:


- How Cisco DCNM responds if a delivery job results in configuration errors on a device.
- Whether Cisco DCNM delivers Cisco IOS or the Cisco NX-OS commands to all devices in the job at the same time or one device at a time.

BEFORE YOU BEGIN

Ensure that the configuration delivery job exists in Cisco DCNM.

Rollback is supported only if the Cisco IOS or the Cisco NX-OS release on the destination device supports rollbacks. For example, Cisco Nexus 7000 Series devices support rollbacks.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Config Job Wizard > VLAN Template**.
The VLAN Template pane with the list of tasks is displayed.
- Step 2** The **Welcome** screen displays the steps involved configuring the job.
- Step 3** Click **Next** to display the **Select Devices** screen.
- Step 4** Select a device from the list to deliver the configuration.
- Step 5** Click **Next** to display the **Define Variables** screen. You can enter the values for the selected template in the **Define Variables** screen.
-  **Note** Select the Edit variables per device check box to set the attributes individually to each device. Else, you can globally configure the attributes to all the devices displayed in the list. Basic validation will be performed for the defined variable and the errors are displayed.
-
- Step 6** Click **Next** to preview the configuration to be delivered in the **Preview Config** screen.
- Step 7** Click **Next** to display the configuration page, in **Schedule Job** screen. For more details, see [Scheduling a Configuration Delivery Job](#) section.
-

Scheduling a Configuration Delivery Job

You can add a date and time that Cisco DCNM should run a configuration delivery job. This feature enables you to set the options if the device went wrong and the system needs to roll back to the set configuration.

BEFORE YOU BEGIN

Determine when you want Cisco DCNM to run the configuration delivery job.

Send document comments to dcnm-docfeedback@cisco.com

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Config Job Wizard > Template**.
 - Step 2** After entering the details in the **Welcome**, **Select Devices**, **Define Variables**, and **Preview Config** screens, click **Next** to display the **Schedule Job** screen.
 - Step 3** Enter the job description , device credentials, time, transaction options, and the delivery options.
 - Step 4** Click **Finish** to finish the configuration.
 - Step 5** Choose **Config Delivery > Jobs** to check on the status of the running configuration delivery jobs. You can also change the scheduled time by editing the value in the **Scheduled At** column.
-

Removing a Configuration Delivery Job

You can remove, or delete, a configuration delivery job from Cisco DCNM.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Config Delivery> Jobs**.
The Summary pane lists the configuration delivery jobs that are configured in Cisco DCNM.
 - Step 2** Click the configuration delivery job check box that you want to remove.
 - Step 3** From the menu bar, click the **Delete Job** button.
 - Step 4** Click **Yes**.
Cisco DCNM removes the configuration delivery job. You do not need to save your changes.
-

Send document comments to dcnm-docfeedback@cisco.com

Field Descriptions for Configuration Delivery Management

This section includes the following field descriptions for the Configuration Delivery Management feature:

- [Delivery Job: Details: Configuration Section, page 9-29](#)
- [Delivery Job: Details: Configuration Delivery Options Section, page 9-30](#)
- [Configuration Delivery for Templates: Virtual Port Channel Template, page 9-35](#)
- [Configuration Delivery for Templates: FIP Snooping Template, page 9-31](#)
- [Configuration Delivery for Templates: FCoE Template, page 9-31](#)
- [Configuration Delivery for Templates: OTV Internal Interfaces Template, page 9-31](#)
- [Configuration Delivery for Templates: OTV Multicast Template, page 9-31](#)
- [Configuration Delivery for Templates: OTV Multicast with HSRP Isolation Template, page 9-32](#)
- [Configuration Delivery for Templates: OTV Multicast with VRRP Isolation Template, page 9-32](#)
- [Configuration Delivery for Templates: OTV Unicast with One Adjacency Server Template, page 9-33](#)
- [Configuration Delivery for Templates: OTV Unicast with One Adjacency Server and HSRP Isolation Template, page 9-33](#)
- [Configuration Delivery for Templates: OTV Unicast with One Adjacency Server and VRRP Isolation Template, page 9-33](#)
- [Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers Template, page 9-34](#)
- [Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers and HSRP Isolation Template, page 9-34](#)
- [Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers and VRRP Isolation Template, page 9-35](#)
- [Configuration Delivery for Templates: Virtual Port Channel Template, page 9-35](#)
- [Configuration Delivery for Templates: Zone Template, page 9-37](#)
- [Additional References, page 9-37](#)

Delivery Job: Details: Configuration Section

Table 9-4 *Delivery Job: Details: Configuration Section*

Field	Description
Device	Specifies the device name.
VLAN_ID	Specifies the VLAN ID.
FC_MAP	Specifies the FC_MAP.
ENODE_INF	Specifies the ENODE_INF.
OLD_VLAN_ID	Specifies the previous VLAN ID.
FCF_INF	Specifies the FCF information.

Send document comments to dcnm-docfeedback@cisco.com

Delivery Job: Details: Configuration Delivery Options Section

Table 9-5 *Delivery Job: Details: Configuration Delivery Options Section*

Field	Description
Transaction Options	
Enable Rollback	<p>Specifies whether Cisco DCNM uses the Cisco IOS or the Cisco NX-OS rollback feature to recover from failures on devices during configuration delivery. By default, this check box is unchecked.</p> <p>Note Cisco DCNM can perform a rollback only on devices that support a configuration rollback, such as Cisco Nexus 7000 Series devices.</p>
Rollback the configuration on the device if there is any failure in that device	<p>Specifies that Cisco DCNM should roll back the running configuration of the device that had the failure to the previous running configuration. If there are other devices in the delivery job, the job continues on devices that did not have a failure.</p> <p>This field appears when the Enable Rollback check box is checked.</p>
Rollback the configuration in all the selected devices if there is any failure in any device	<p>Specifies that Cisco DCNM should roll back the running configuration of all devices included in the job if a failure occurs on a device. This option is particularly useful if the job is configured for parallel delivery.</p> <p>This field appears when the Enable Rollback check box is checked.</p>
Rollback the configuration on the device, if there is any failure in that device and stop further configuration delivery to the remaining devices	<p>Specifies that Cisco DCNM should roll back the running configuration of the device that had the failure and should not continue to deliver the job to devices that have not received the configuration yet. This option is particularly useful if the job is configured for sequential delivery.</p> <p>This field appears when the Enable Rollback check box is checked.</p>
Delivery Order	
Deliver configuration to one device at a time in sequence	Specifies that Cisco DCNM delivers the configuration to devices included in the job in a serial delivery. This option is particularly helpful if you have configured the job to stop after the first failure.
Deliver configuration to all devices in parallel at the same time	Specifies that Cisco DCNM delivers the configuration to all devices included in the job in parallel. This option delivers the configuration to the devices in the job faster than serial delivery.
Post Delivery Options	
Copy run to start	Specifies that Cisco DCNM copy the running configuration to the startup configuration. By default, this checkbox is unchecked.

Send document comments to dcnm-docfeedback@cisco.com

Configuration Delivery for Templates: FCoE Template

Table 9-6 *FCoE Template*

Field	Description
VLAN_ID	ID for the VLAN
VSAN_ID	ID for the VSAN
FC_MAP	Value of FC mapping
VFC_NUMBER_RANGE	Valid range for the VFC

Configuration Delivery for Templates: FIP Snooping Template

Table 9-7 *FIP Snooping Template*

Field	Description
VLAN_RANGE	Valid VLAN range
ENODE_INTERFACE_RANGE	Valid values for the ENODE interface range
FCF_INTERFACE_RANGE	Valid values for the FCF interface range
FC_MAP	Value of FC mapping

Configuration Delivery for Templates: OTV Internal Interfaces Template

Table 9-8 *OTV Internal Interfaces Template*

Field	Description
INTERNAL_IFS	Specifies the internal IFS.
SITE_VLAN	Specifies the site vlan.
OTV_VLANS	Specifies the OTV vlan.

Configuration Delivery for Templates: OTV Multicast Template

Table 9-9 *OTV Multicast Template*

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.

Send document comments to dcnm-docfeedback@cisco.com

Table 9-9 OTV Multicast Template

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
CONTROL_GROUP_IP	Specifies the IP of the control group for multicast.
DATA_GROUP_NETWORK	Specifies the data group network.
OTV_VLAN	Specifies the OTV vlan ID.

Configuration Delivery for Templates: OTV Multicast with HSRP Isolation Template

Table 9-10 OTV Multicast with HSRP Isolation Template

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
CONTROL_GROUP_IP	Specifies the IP of the control group for multicast.
DATA_GROUP_NETWORK	Specifies the data group network.
OTV_VLAN	Specifies the OTV vlan ID.

Configuration Delivery for Templates: OTV Multicast with VRRP Isolation Template

Table 9-11 OTV Multicast with VRRP Isolation Template

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
CONTROL_GROUP_IP	Specifies the IP of the control group for multicast.
DATA_GROUP_NETWORK	Specifies the data group network.
OTV_VLAN	Specifies the OTV vlan ID.

Send document comments to dcnm-docfeedback@cisco.com

Configuration Delivery for Templates: OTV Unicast with One Adjacency Server Template

Table 9-12 *OTV Multicast with One Adjacency Server Template*

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
ADJACENCY_SERVER	Specifies the IP of the adjacency server.
PRIMARY_ADJACENCY_SERVER	Specifies the IP of the primary adjacency server.
OTV_VLAN	Specifies the OTV vlan ID.

Configuration Delivery for Templates: OTV Unicast with One Adjacency Server and HSRP Isolation Template

Table 9-13 *OTV Unicast with One Adjacency Server and HSRP Isolation Template*

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
IS_ADJACENCY_SERVER	Specifies the IP of the adjacency server.
PRIMARY_ADJACENCY_SERVER	Specifies the IP of the primary adjacency server.
OTV_VLANS	Specifies the OTV vlan ID.

Configuration Delivery for Templates: OTV Unicast with One Adjacency Server and VRRP Isolation Template

Table 9-14 *OTV Unicast with One Adjacency Server and VRRP Isolation Template*

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.

Send document comments to dcnm-docfeedback@cisco.com

Table 9-14 *OTV Unicast with One Adjacency Server and VRRP Isolation Template*

Field	Description
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
IS_ADJACENCY_SERVER	Specifies the IP of the adjacency server.
PRIMARY_ADJACENCY_SERVER	Specifies the IP of the primary adjacency server.
OTV_VLAN	Specifies the OTV vlan ID.

Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers Template

Table 9-15 *OTV Unicast with Two Adjacency Servers Template*

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
IS_ADJACENCY_SERVER	Specifies the IP of the adjacency server.
PRIMARY_ADJACENCY_SERVER	Specifies the IP of the primary adjacency server.
SECONDARY_ADJACENCY_SERVER	Specifies the IP of the secondary adjacency server.
OTV_VLAN	Specifies the OTV vlan ID.

Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers and HSRP Isolation Template

Table 9-16 *OTV Unicast with Two Adjacency Servers and HSRP Isolation Template*

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
IS_ADJACENCY_SERVER	Specifies the IP of the adjacency server.

Send document comments to dcnm-docfeedback@cisco.com

Table 9-16 OTV Unicast with Two Adjacency Servers and HSRP Isolation Template

Field	Description
PRIMARY_ADJACENCY_SERVER	Specifies the IP of the primary adjacency server.
SECONDARY_ADJACENCY_SERVER	Specifies the IP of the secondary adjacency server.
OTV_VLAN	Specifies the OTV vlan ID.

Configuration Delivery for Templates: OTV Unicast with Two Adjacency Servers and VRRP Isolation Template

Table 9-17 OTV Unicast with Two Adjacency Servers and VRRP Isolation Template

Field	Description
SITE_VLAN	Specifies the site vlan.
SITE_ID	Specifies the site ID.
OVERLAY_ID	Specifies the overlay ID.
JOIN_INTF	Specifies the interface information.
IS_ADJACENCY_SERVER	Specifies the IP of the adjacency server.
PRIMARY_ADJACENCY_SERVER	Specifies the IP of the primary adjacency server.
SECONDARY_ADJACENCY_SERVER	Specifies the IP of the secondary adjacency server.
OTV_VLAN	Specifies the OTV vlan ID.

Configuration Delivery for Templates: Virtual Port Channel Template

Table 9-18 Peer-Link Access Port Channel Template

Field	Description
DOMAIN_ID	vPC Domain ID
ACC_VLAN	Access VLAN ID
PO_NO	Port channel ID
SRC_IP	Peer keepalive source IP address
DEST_IP	Peer keepalive destination IP address
VRF	Name of the VRF

Send document comments to dcnm-docfeedback@cisco.com

Table 9-18 *Peer-Link Access Port Channel Template (continued)*

Field	Description
INTF_MODE	Link Aggregation Protocol mode
INTF_NAME_RANGE	Range of valid member ports of the port channel

Table 9-19 *Peer-Link Trunk Port Channel Template*

Field	Description
DOMAIN_ID	vPC Domain ID
ALL_VLAN	Range of VLANs that are allowed on the port channel
NAT_VLAN	ID of the native VLAN
PO_NO	Port channel ID
SRC_IP	Peer keepalive source IP address
DEST_IP	Peer keepalive destination IP address
VRF	Name of the VRF
INTF_MODE	Link Aggregation Protocol mode
INTF_NAME_RANGE	Range of valid member ports of the port channel

Table 9-20 *Virtual Access Port Channel Template*

Field	Description
vPC_ID	vPC ID
PO_NO	IP address of the port channel
ACC_VLAN	Access VLAN ID
INTF_NAME_RANGE	Range of valid port channels of the member ports
INTF_MODE	Link Aggregation Protocol mode

Table 9-21 *Virtual Trunk Port Channel Template*

Field	Description
vPC_ID	vPC ID
PO_NO	IP address of the port channel
ALL_VLAN	Range of VLAN allowed on the port channel
NAT_VLAN	ID of the native VLAN
INTF_RANGE	Range of valid port channels of the member ports
INTF_MODE	Link Aggregation Protocol mode

Send document comments to dcnm-docfeedback@cisco.com

Configuration Delivery for Templates: Zone Template

Table 9-22 *FIP Snooping Template*

Field	Description
HOSTNAME	Specifies the host name of the device.
STORAGE	The storage IP.
HOST_PWWN	The post world wide name of the host.
STORAGE_PWWN	The post world wide name of the storage device.
VSAN_ID	Specifies the vsan ID.
FABRIC A	Specifies the name of Fabric A.
FABRIC B	Specifies the name of Fabric A.
HOST_IF	Specifies the host interface.
HOST_MODULE	Specifies the name of the host module.
STORAGE_IF	Specifies the storage interface.
STORAGE_MODULE	Specifies the name of the storage module.
ZONESET	Specifies the name of the zone set.

Additional References

For additional information related to configuration delivery management, see the following sections:

- [Related Documents, page 9-37](#)
- [Standards, page 9-38](#)

Related Documents

Related Topic	Document Title
Port profiles	<i>Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x</i>
Configuration rollback in Cisco NX-OS	<i>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x</i>

Send document comments to dcnm-docfeedback@cisco.com

Standards

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

Feature History for Configuration Delivery Management

[Table 9-23](#) lists the release history for this feature.

Table 9-23 ***Feature History for Configuration Delivery Management***

Feature Name	Releases	Feature Information
Configuration Delivery Management	6.1(1)	Configuration delivery templates are supported on the Cisco IOS and the Cisco NX-OS platforms.
Configuration Delivery Management	6.1(1)	Configuration delivery templates are supported in the Cisco DCNM SAN client.
Configuration Delivery Management	6.1(1)	This feature was introduced.



INDEX

A

Archival Jobs

See Configuration Change Management

Archival Settings

See Configuration Change Management

C

CDP

defined with LLDP [6-1](#)

chassis

CPU utilization [3-6](#)

details [3-6](#)

displaying information about [3-6](#)

environmental status [3-6](#)

events [3-6](#)

memory utilization [3-6](#)

Configuration Change Management

archival history [8-7](#)

Archival Jobs [8-16](#)

Archival Settings [8-19](#)

archival status [8-7](#)

archiving a running configuration [8-9](#)

browsing versions [8-8](#)

commenting on a version [8-8](#)

comparing versions [8-10](#)

comparison tools [8-12](#)

configuring an archival job [8-16](#)

configuring switch profiles [8-21](#)

deleting an archival job [8-18](#)

deleting archived configurations [8-15](#)

description [8-1](#)

diff tools [8-12](#)

enabling or disabling an archival job [8-18](#)

feature history [8-29](#)

field descriptions [8-24](#)

history settings [8-20](#)

merging differences [8-13](#)

overview [1-3](#)

performing a rollback [8-14](#)

rollback server settings [8-20](#)

Version Browser [8-6](#)

version settings [8-20](#)

viewing an archival job [8-18](#)

viewing archival job history [8-19](#)

viewing a version [8-9](#)

viewing rollback history [8-15](#)

Configuration Delivery Management

adding a job [9-17](#)

adding a template [9-23, 9-24, 9-26](#)

changing a template [9-25](#)

configuring Cisco NX-OS commands for a device-source job [9-20](#)

configuring Cisco NX-OS commands for a manual-source job [9-19](#)

configuring Cisco NX-OS commands for a template-source job [9-22](#)

configuring job delivery options [9-28](#)

configuring job destination devices [9-18](#)

creating a job [9-16](#)

delivery options [9-3](#)

description [9-1](#)

feature history [9-36](#)

field descriptions [9-30](#)

guidelines and limitations [9-15](#)

job sources [9-2](#)

Send document comments to dcnm-docfeedback@cisco.com

licensing requirements [9-15](#)
 overview [1-3](#)
 platform support [9-16](#)
 prerequisites [9-15](#)
 refreshing Cisco DCNM servers with template updates [9-27](#)
 removing a configuration delivery job [9-29](#)
 removing a template [9-26](#)
 scheduling a configuration delivery job [9-29](#)
 template requirements [9-3](#)
 connecting to vCenter Servers [4-10](#)

D

device discovery protocol [6-1](#)
 Device OS Management
 adding or changing comments [7-11](#)
 changing file server [7-13](#)
 changing installation options [7-11](#)
 configuring a file server [7-12](#)
 creating a software installation job [7-7](#)
 creating or editing a software installation job [7-7](#)
 deleting a file server [7-14](#)
 deleting a software installation job [7-11](#)
 deleting startup configuration [7-11](#)
 description [7-1](#)
 editing a software installation job [7-7](#)
 feature history [7-18](#)
 field descriptions [7-15](#)
 file servers [7-12](#)
 installing software [7-5](#)
 overview [1-2, 7-1](#)
 rescheduling a software installation job [7-10](#)
 saving running configuration [7-11](#)
 Software Image Management [7-5, 7-6](#)
 viewing device image details [7-5](#)
 viewing software installation job details [7-6](#)
 viewing status [7-6](#)
 disconnecting from vCenter Server [4-10](#)

Distributed Virtual Switch
 See DVS
 documentation
 additional publications [xii](#)
 domains
 Layer 2 control [4-4](#)
 Layer 3 control [4-5](#)
 DVS
 deleting from vCenter Server [4-11](#)

E

events
 overview [1-2](#)
 Events Browser
 adding a note [2-7](#)
 changing event status [2-7](#)
 deleting an event [2-8](#)
 description [2-1](#)
 filtering events [2-5](#)
 viewing events [2-3](#)
 Events tab
 adding a note [2-7](#)
 changing event status [2-7](#)
 deleting an event [2-8](#)
 description [2-1](#)
 viewing events [2-5](#)

F

fan trays
 details [3-8](#)
 displaying information about [3-7](#)
 events [3-8](#)
 feature history
 Configuration Change Management [8-29](#)
 Configuration Delivery Management [9-36](#)
 Device OS Management [7-18](#)

Send document comments to dcnm-docfeedback@cisco.com

inventory [3-11](#)

LLDP [6-5](#)

power usage [3-11](#)

field descriptions

Configuration Change Management [8-24](#)

Configuration Delivery Management [9-30](#)

Device OS Management [7-15](#)

File Servers

See Device OS Management

H

high availability

LLDP [6-2](#)

SPAN [5-3](#)

I

inventory

chassis information [3-6](#)

definition [3-1](#)

fan tray information [3-7](#)

feature history [3-11](#)

licensing requirements [3-3](#)

module information [3-6](#)

module pre-provisioning [3-3](#)

module pre-provisioning, FEX modules [3-5](#)

module pre-provisioning, offline module [3-4](#)

module pre-provisioning, online module [3-4](#)

overview [1-2](#)

power supply information [3-7](#)

reloading a linecard [3-5](#)

J

job sources

Configuration Delivery Management [9-2](#)

L

licensing requirements

Configuration Delivery Management [9-15](#)

inventory [3-3](#)

LLDP [6-2](#)

SPAN [5-3](#)

LLDP

defined [6-1](#)

description [6-1](#)

enabling or disabling globally [6-3](#)

enabling or disabling on an interface [6-3](#)

feature history [6-5](#)

guidelines [6-2](#)

high availability [6-2](#)

licensing requirements [6-2](#)

limitations [6-2](#)

overview [1-2](#)

supported switches [6-1](#)

M

modules

details [3-7](#)

displaying information about [3-6](#)

environmental status [3-7](#)

events [3-7](#)

TCAM statistics [3-7](#)

O

overview [1-1](#)

P

platform support

Configuration Delivery Management [9-16](#)

Send document comments to dcnm-docfeedback@cisco.com

power supplies

- details [3-7](#)
- displaying information about [3-7](#)
- events [3-7](#)

power usage

- description [3-2](#)
- displaying details about [3-9](#)
- displaying statistics about [3-9](#)
- displaying summary information about [3-8](#)
- feature history [3-11](#)

R

- related documents [xii](#)

S

server connections

- configuring vCenter Server connections [4-9](#)
- deleting vCenter Server connections [4-10](#)

Software Image Management

- See Device OS Management

software installation job

- See Device OS Management

SPAN

- configuring an RSPAN VLAN [5-7](#)
- configuring a session [5-4](#)
- configuring a virtual SPAN session [5-6](#)
- description [5-1](#)
- destination field descriptions (table) [5-9](#)
- enabling a session [5-8](#)
- high availability [5-3](#)
- licensing requirements [5-3](#)
- multiple sessions [5-3](#)
- overview [1-2](#)
- session destinations [5-4](#)
- session field descriptions (table) [5-8](#)
- sessions [5-2](#)

- session sources [5-4](#)

- shutting down a session [5-8](#)

- source field descriptions (table) [5-9](#)

- virtual SPAN sessions [5-2](#)

switched port analyzer. See SPAN

T

template requirements

- Configuration Delivery Management [9-3](#)

V

vCenter Server

- connecting to [4-10](#)
- disconnecting from [4-10](#)
- removing host mapping [4-11](#)

vCenter Server connections

- configuring [4-9](#)
- deleting [4-10](#)

VEMS

- removing host mapping from vCenter Server [4-11](#)

Version Browser

- See Configuration Change Management

Virtual Ethernet Modules

- See VEMs.

virtual switch

- changing domain to Layer 2 control [4-7](#)
- changing domain to Layer 3 control [4-6](#)
- configuring a control interface [4-12](#)
- configuring domain with Control VLAN [4-7](#)
- configuring domain with Packet VLAN [4-8](#)
- configuring vCenter connections [4-9](#)
- creating domains with Layer 2 control [4-4](#)
- creating domains with Layer 3 control [4-5](#)
- deleting vCenter connections [4-10](#)
- description [4-1](#)
- displaying details [4-13](#)

Send document comments to dcnm-docfeedback@cisco.com

- displaying neighboring devices [4-12](#)
- displaying summary information [4-13](#)
- domains [4-2](#)
- feature history [4-15](#)
- field descriptions [4-13](#)
- licensing requirements [4-3](#)
- related documents [4-15](#)
- removing host mapping from vCenter Server [4-11](#)
- server connections [4-3](#)
- standards [4-15](#)
- virtual switching
 - overview [1-2](#)
- VLAN interfaces
 - communicating between VLANs [4-7, 4-8](#)

Send document comments to dcnm-docfeedback@cisco.com