



Cisco Prime DCNM Fundamentals Guide, Release 7.2.x

July, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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

Cisco Prime DCNM Fundamentals Guide, Release 7.2.x
© 2015 Cisco Systems, Inc. All rights reserved.



Preface 61

New and Changed Information 69

CHAPTER 1

Introduction to Cisco Data Center Network Manager 1-69

CHAPTER 2

Cisco Prime DCNM User Roles 2-1

Cisco DCNM Credentials 2-1

Cisco DCNM Users 2-1

DCNM Roles 2-1

Roles from Cisco DCNM Perspective 2-2

Admin Perspective 2-3

Web Client Admin Perspective 2-3

SAN Thick Client Admin Perspective 2-3

Server Admin Perspective 2-3

Web Client Server Admin Perspective 2-3

SAN Thick Client Server Admin Perspective 2-3

SME Perspective 2-4

Web Client SME Admin Perspective 2-4

SME Storage Perspective 2-4

SME Key Management Perspective 2-4

SME Recovery Perspective 2-4

SAN Thick Client SME Perspective 2-4

Operator Perspective 2-5

Web Client Operator Perspective 2-5

SAN Thick Client Operator Perspective 2-5

CHAPTER 3

Cisco Prime DCNM Web Client 3-1

Navigating DCNM Web Client 3-1

Scope Menu 3-2

Admin Menu 3-2

Table and Filtering Navigation 3-2

Printing 3-2

Text Part Number Exporting to a File 3-2

Sorting Columns	3-3
Cisco Prime DCNM Web Search Engine	3-3
Using the Cisco Prime DCNM Search Engine	3-3
Downloading Cisco Prime DCNM-SAN Client	3-3
Downloading Cisco Prime DCNM-LAN Client	3-4
Downloading Cisco Device Manager Client	3-4
Connecting to a Switch using the CLI	3-4
Adding a Security Exception	3-5
Viewing Dashboard Information	3-5
Summary	3-5
Health	3-6
Inventory	3-6
Top CPU	3-6
Top ISLs/Trunks	3-6
Top SAN Host Ports	3-7
Top SAN Storage Ports	3-7
Viewing Health Summary Information	3-7
Viewing Performance Summary Information	3-7
Viewing Inventory Summary Information	3-8
Differences by changing the Scope to default LAN or configured switch group	3-8
Topology	3-8
Differences by changing the Scope to default SAN or configured switch group	3-11
New Area - Daily Performance	3-11
Fabric	3-11
Inter Switch Links View	3-12
Edge Ports View	3-13
Health	3-13
Switch Dashboard	3-14
Compute	3-15
Viewing Host Enclosures	3-15
Viewing Host Events	3-16
Viewing Host Topology	3-16
View Host Traffic	3-16
Network	3-17
Storage	3-17
Viewing Storage Enclosure	3-17
Viewing Storage Enclosure Events	3-18
Viewing Storage Enclosure Topology	3-18
Viewing Storage Enclosure Traffic	3-18

Viewing Storage Systems	3-19
Components	3-19
Pools	3-19
LUNs	3-20
Filer Volumes	3-20
Hosts	3-21
Storage Processors	3-21
Storage Ports	3-21
Viewing Health Information	3-22
Viewing Accounting Information	3-22
Viewing Events Information	3-22
SAN Host Redundancy	3-23
SAN Path Errors	3-23
Settings	3-24
Slow Drain Analysis	3-25
Viewing a vPC	3-25
Viewing vPC Inconsistencies	3-26
Resolving vPC Inconsistencies	3-27
Viewing Performance Information	3-27
Rx/Tx Calculation	3-28
Viewing Switch CPU Information	3-28
Viewing Switch Memory Information	3-28
Viewing Switch Traffic and Errors Information	3-29
Viewing ISL Traffic and Errors Information	3-29
Viewing Performance Information for Ethernet Ports	3-29
Viewing Other Statistics	3-30
Viewing Performance Information for NPV Links	3-30
Viewing Performance Information on All Ports	3-31
Viewing Performance Information on Host Ports	3-31
Viewing Performance Information on Storage Ports	3-32
Viewing Performance Information on Host Enclosure	3-32
Viewing Performance Information on Storage Enclosure	3-33
Viewing Performance Information on Port Groups	3-33
Viewing Performance Information for FC Flows	3-34
Viewing Performance Information for Virtual Port Channels	3-34
N3K Buffer Usage	3-35
Viewing Inventory Information	3-35
Viewing Inventory Information for Switches	3-36
Viewing Inventory Information for Modules	3-37

Viewing Inventory Information for ISLs/Trunks	3-37
Viewing Inventory Information for Licenses	3-37
Viewing Inventory Information for NPV Links	3-37
Viewing Inventory Information for VSANs	3-38
Viewing Inventory Information for Regular Zones	3-38
Viewing Inventory Information for IVR Zones	3-38
Viewing Inventory Information for All Ports on FC End Devices	3-38
Viewing Inventory Information for Host Ports on FC End Devices	3-38
Viewing Inventory Information for Storage Ports on FC End Devices	3-39
Viewing Inventory Information for Port Mapper	3-39
Viewing and Creating Custom Reports	3-40
Viewing Reports	3-40
Generating a Report	3-41
Creating SAN User Defined Reports	3-42
Deleting a Report Template	3-43
Modifying a Custom Report Template	3-43
Viewing Scheduled Jobs Based on a Report Template	3-44
Configuring Cisco Prime DCNM Web Client	3-44
Viewing a Configuration	3-44
Comparing Configurations	3-45
Copying a Configuration	3-45
Configuring Jobs	3-45
Job Status History	3-46
Storage Media Encryption	3-47
Selecting the Key Manager and SSL Settings	3-47
Viewing SME Clusters	3-48
Creating a Cluster	3-48
Configuring Templates	3-49
Template Structure	3-50
Adding a Template	3-57
Configuring Template Job	3-58
Modifying a Template	3-59
Importing a Template	3-59
Exporting a Template	3-60
Deleting a Template	3-60
Configuring Jobs	3-60
Power-On Auto Provisioning (POAP)	3-60
POAP Launchpad	3-61
DHCP Scope	3-61

Adding a DHCP Scope	3-62
Editing an existing DHCP Scope	3-62
Deleting a DHCP Scope	3-62
Images and Configuration	3-63
Add Image or Configuration Server URL	3-63
Editing an Image or Configuration Server URL	3-63
Deleting an Image or Configuration Server URL	3-63
POAP Templates	3-64
Add POAP template	3-64
Editing a Template	3-64
Cloning a Template	3-65
Importing a Template	3-65
Exporting a Template	3-65
Deleting a Template	3-65
POAP Template Annotation	3-65
POAP Definitions	3-67
Creating a POAP definition	3-69
Uploading a POAP Definition	3-70
Editing a POAP Definition	3-70
Deleting POAP Definitions	3-70
Publishing POAP definitions	3-71
Write, Erase and Reload the POAP Switch Definition	3-71
Change Image	3-71
Cable Plan	3-71
Create a Cable Plan	3-72
Viewing an Existing Cable Plan Deployment	3-72
Deleting a Cable Plan	3-72
Deploying a Cable Plan	3-72
Revoking a Cable Plan	3-73
Viewing a Deployed Cable Plan from Device	3-73
Fabric	3-73
Adding an Organization	3-75
Editing an Organization	3-75
Deleting an Organization	3-75
Adding a Partition	3-75
Editing a Partition	3-76
Deleting a Partition	3-76
Adding a Network	3-76
Editing a Network	3-77
Deleting a Network	3-77

Profiles	3-77
Adding a profile	3-77
Editing a Profile	3-79
Delete a Profile	3-79
Editing a Profile Instance	3-79
Administering Cisco Prime DCNM Web Client	3-79
Starting, Restarting, and Stopping Services	3-80
Administering Datasources	3-80
Adding, Editing, Re-discovering, Purging and Removing Managed Fabrics	3-81
Adding, Editing, Re-discovering, Purging and Removing LAN, LAN Tasks and Switch	3-83
Adding, Editing, Re-discovering and Removing VMware Servers	3-86
Adding, editing, removing, rediscovering and refreshing SMI-S Storage	3-88
Viewing Log Information	3-89
Configuring Cisco Prime DCNM-SAN Server Properties	3-90
Configuring SFTP/TFTP Credentials	3-90
Managing Switch Groups	3-91
Adding Switch Groups	3-91
Renaming a Group	3-92
Deleting a Group or a Member of a Group	3-92
Moving a Switch to Another Group	3-92
Moving a Switch Group to Another Group	3-92
Managing Custom Port Groups	3-92
Adding Custom Port Groups	3-93
Configuring Switch and Interface to the Port Group	3-93
Generating Reports for the Custom Port Groups	3-93
Removing Port Group Member	3-93
Removing Port Group	3-94
Managing Licenses	3-94
Viewing Licenses Using the Cisco Prime DCNM Wizard	3-94
Automatic License Assignment	3-96
Adding Cisco Prime DCNM Licenses	3-97
Assigning Licenses	3-97
Unassigning Licenses to a Switch	3-97
Viewing Server Federation	3-98
Configuring AAA Properties	3-98
Local	3-98
Radius	3-99
TACACS+	3-99
Switch	3-99
LDAP	3-99

Adding and Removing Users	3-100
Adding Local Users	3-100
Editing a User	3-100
Removing a User	3-100
Managing Clients	3-101
Performance Manager Collections	3-101
Configuring the RRD Database	3-101
Importing the RRD Statistics Index	3-102
Configuring Other Statistics	3-102
Viewing Events Registration	3-103
Adding Notification Forwarding	3-103
Adding Notification Forwarding	3-103
Removing Notification Forwarding	3-105
Configuring EMC CallHome	3-105
Event Suppression	3-105
Add Event Suppression Rules	3-105
Delete Event Suppression Rule	3-106
Modify Event Suppression Rule	3-107
Using Cisco Prime DCNM Web Client with SSL	3-107
Using a self signed SSL Certificate	3-107
Using a SSL Certificate when certificate request is generated using OpenSSL	3-108
Using a SSL Certificate when certificate request is generated using Keytool	3-108
SSL for Federated (High Availability) setup	3-109
Fabric—General Settings	3-109
Border Leaf Settings	3-110
Configuring Border Leaf Settings	3-110
Border Leaf Device Pairing	3-111
Creating an Edge Router	3-112
Connect New Border leaf to the Edge Router	3-113
Deleting Edge Router/Border leaf devices	3-113
Border Leaf Extended Partitions	3-113
POAP Settings	3-114
Fabric Encapsulation Settings	3-114
L2 Segment ID Range Management	3-116
Add Orchestrator	3-117
Modify Orchestrator	3-117
Delete Orchestrator	3-117
Mobility Domains	3-117
Add Mobility Domains	3-118

Modify Mobility Domains	3-118
Delete Mobility Domains	3-118

CHAPTER 4

Cisco DCNM-SAN Overview	4-1
DCNM-SAN Server	4-1
DCNM-SAN Client	4-1
Device Manager	4-2
DCNM-SAN Web Client	4-2
Performance Manager	4-3
Authentication in DCNM-SAN Client	4-3
Cisco Traffic Analyzer	4-3
Network Monitoring	4-4
Performance Monitoring	4-4

CHAPTER 5

Configuring Cisco DCNM-SAN Server	5-1
Information About Cisco DCNM-SAN Server	5-1
DCNM-SAN Server Features	5-1
Licensing Requirements For Cisco DCNM-SAN Server	5-2
Installing and Configuring Cisco DCNM-SAN Server	5-2
Installing Cisco DCNM-SAN Server	5-3
Data Migration in Cisco DCNM-SAN Server	5-7
Verifying Performance Manager Collections	5-7
Managing a Cisco DCNM-SAN Server Fabric	5-7
Selecting a Fabric to Manage Continuously	5-8
Cisco DCNM-SAN Server Properties File	5-8
Modifying Cisco DCNM-SAN Server	5-10
Changing the Cisco DCNM-SAN Server Username and Password	5-10
Changing the DCNM-SAN Server Fabric Discovery Username and Password	5-11
Changing the Polling Period and Fabric Rediscovery Time	5-11
Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS WINDOWS Server	5-12
Changing the IP Address of the Cisco DCNM-SAN for Federated Windows Setup	5-12
Changing the IP address of primary server	5-12
Changing the IP address of secondary server	5-13
Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS LINUX Server	5-13
Using Device Aliases or FC Aliases	5-14
Configuring Security Manager	5-15
Server Federation	5-15
Restrictions	5-15
Mapping Fabric ID to Server ID	5-16

Opening the Fabric on a Different Server	5-17
Viewing the Sessions in a Federation	5-18
Viewing the Servers in a Federation	5-19
Discover Devices Managed by SVI	5-19
Additional References	5-20

CHAPTER 6

Configuring Authentication in Cisco DCNM-SAN 6-1

Information About Cisco DCNM-SAN Authentication	6-1
Best Practices for Discovering a Fabric	6-2
Setting Up Discovery for a Fabric	6-3
Performance Manager Authentication	6-3
Cisco DCNM-SAN Web Client Authentication	6-4

CHAPTER 7

Configuring Cisco DCNM-SAN Client 7-1

Information About DCNM-SAN Client	7-1
Cisco DCNM-SAN Advanced Mode	7-2
Cisco DCNM-SAN Client Quick Tour: Server Admin Perspective	7-2
Cisco DCNM-SAN Main Window	7-2
Menu Bar	7-4
Tool Bar	7-4
Logical Domains Pane	7-4
Physical Attributes Pane	7-4
Information Pane	7-5
Fabric Pane	7-6
Cisco DCNM-SAN Client Quick Tour: Admin Perspective	7-6
Menu Bar	7-8
File	7-8
View	7-9
Zone	7-9
Tools	7-10
Performance	7-11
Server	7-12
Help	7-12
Toolbar	7-12
Logical Domains Pane	7-14
Filtering	7-14
Physical Attributes Pane	7-15
Context Menu for Tables	7-15
Information Pane	7-18

Detachable Tables	7-19
Fabric Pane	7-19
Context Menus	7-21
Saving the Map	7-22
Purging Down Elements	7-22
Multiple Fabric Display	7-22
Filtering by Groups	7-23
Status Bar	7-25
Launching Cisco DCNM-SAN Client	7-25
Launching Fabric Manager Client in Cisco SAN-OS Release 3.2(1) and Later	7-25
Launching Cisco DCNM-SAN Client Using Launch Pad	7-31
Setting Cisco DCNM-SAN Preferences	7-34
Network Fabric Discovery	7-35
Network LAN Discovery	7-36
Viewing Ethernet Switches	7-36
Removing a LAN	7-37
Modifying the Device Grouping	7-38
Using Alias Names as Enclosures	7-39
Using Alias Names as Descriptions	7-40
Controlling Administrator Access with Users and Roles	7-41
Using Cisco DCNM-SAN Wizards	7-41
Cisco DCNM-SAN Troubleshooting Tools	7-42
Integrating Cisco DCNM-SAN and Data Center Network Management Software	7-42
Launching a Switch from the Topology Map	7-43

CHAPTER 8

Device Manager 8-1

Information About Device Manager	8-1
Device Manager Features	8-2
Using Device Manager Interface	8-2
Menu Bar	8-3
Toolbar Icons	8-4
Dialog Boxes	8-5
Tabs	8-6
Legend	8-6
Supervisor and Switching Modules	8-7
Context Menus	8-7
Launching Device Manager	8-8
Setting Device Manager Preferences	8-9

CHAPTER 9**Configuring Performance Manager 9-1**

- Information About Performance Manager 9-1
 - Data Interpolation 9-2
 - Data Collection 9-2
 - Using Performance Thresholds 9-2
- Flow Statistics 9-3
- Flow Setup Wizards 9-4
 - Creating a Flow Using Performance Manager Flow Wizard 9-4

9-7

CHAPTER 10**Monitoring the Network 10-1**

- Information About Network Monitoring 10-1
 - Monitoring Health and Events 10-1
 - DCNM-SAN Events Tab 10-2
 - Event Information in DCNM-SAN Web Server Reports 10-2
 - Events in Device Manager 10-2
 - SAN Discovery and Topology Mapping 10-2
 - Device Discovery 10-2
 - Topology Mapping 10-3
 - Using the Topology Map 10-3
 - Saving a Customized Topology Map Layout 10-3
 - Using Enclosures with DCNM-SAN Topology Maps 10-4
 - Mapping Multiple Fabrics 10-4
 - Inventory Management 10-4
 - Using the Inventory Tab from DCNM-SAN Web Server 10-5
 - Viewing Logs from Device Manager 10-5

10-5

CHAPTER 11**Monitoring Performance 11-1**

- Information About Performance Monitoring 11-1
 - Real-Time Performance Monitoring 11-1
 - Historical Performance Monitoring 11-2
- Configuring Performance Manager 11-2
 - Creating a Flow with Performance Manager 11-2
 - Creating a Collection with Performance Manager 11-2
 - Using Performance Thresholds 11-3
- Configuring the Summary View in Device Manager 11-4
- Configuring Per Port Monitoring using Device Manager 11-4

Displaying DCNM-SAN Real-Time ISL Statistics	11-5
Using the Performance Manager Configuration Wizard	11-6
Viewing Performance Statics Using DCNM-SAN	11-6
Displaying Performance Manager Reports	11-7
Displaying Performance Summary	11-8
Displaying Performance Tables and Details Graphs	11-8
Displaying Performance of Host-Optimized Port Groups	11-8
Displaying Performance Manager Events	11-8
Generating Performance Manager Reports	11-9
Generating Top10 Reports in Performance Manager	11-9
Generating Top10 Reports Using Scripts	11-9
Configuring Performance Manager for Use with Cisco Traffic Analyzer	11-10
Exporting Data Collections	11-12
Exporting Data Collections to XML Files	11-12
Exporting Data Collections in Readable Format	11-12
Analyzing SAN Health	11-13
Installing the SAN Health Advisor Tool	11-14

CHAPTER 12

Overview of DCNM-LAN 12-1

DCNM-LAN Client and Server	12-1
Features in Cisco DCNM-LAN, Release 5.2	12-2
Platform Support	12-3
Documentation About DCNM-LAN	12-3

CHAPTER 13

Installing and Launching the Cisco DCNM-LAN Client 13-1

Information About Installing and Launching the DCNM-LAN Client	13-1
Prerequisites for Installing and Launching the DCNM-LAN Client	13-2
Secure Client Communications	13-2
Default Administrator Credentials	13-3
Downloading and Launching the DCNM-LAN Client	13-3
Using a Web Browser to Download and Launch the DCNM-LAN Client	13-3
Using a Command Prompt to Download and Launch the DCNM-LAN Client	13-4
Using a Command Prompt to Download and Launch the DCNM-LAN Client without using Java Web Start Launcher	13-5
Restarting the DCNM-LAN Client	13-6
Logging Into the DCNM-LAN Client	13-7
Uninstalling the DCNM-LAN Client	13-8
Modifying Cisco DCNM-LAN Server	13-9

Changing the IP Address of the Cisco DCNM-LAN for WINDOWS OS	13-9
Changing the IP Address of the Cisco DCNM-LAN on Federated Windows OS	13-10
Changing the IP Address of the Cisco DCNM-LAN on Linux OS	13-10
Additional References	13-11
Related Documents	13-11
Standards	13-11
Feature History for Installing and Launching the DCNM-LAN Client	13-12

CHAPTER 14

Using the Cisco DCNM-LAN Client 14-1

Information About the DCNM-LAN Client	14-1
User Interface	14-2
Feature Selector Pane	14-2
Contents Pane	14-3
Summary Pane	14-3
Details Pane	14-3
Association Pane	14-4
Menus	14-5
Toolbars	14-7
Keyboard Commands	14-7
Multiple Platform Support	14-7
Opening the DCNM-LAN Client	14-8
Closing the DCNM-LAN Client	14-9
Deploying Changes	14-10
Working with Statistics and Charts	14-11
Information about Statistics and Charts	14-11
Licensing Requirements for Statistics and Charts	14-11
Accessing a Chart	14-12
Starting Statistical Monitoring for a Chart	14-12
Stopping Statistical Monitoring for a Chart	14-13
Using a Chart	14-14
Using an Overview Chart	14-15
Exporting a Chart	14-16
Configuring Global Preferences	14-17
Configuring Monitoring Preferences	14-17
Configuring the Maximum Age of Events Fetched from the Server	14-18
Configuring Preprovisioning	14-19
Using Online Help	14-19

CHAPTER 15

Administering DCNM-LAN Authentication Settings 15-1

Information About Administering DCNM-LAN Authentication Settings	15-2
Users and User Roles	15-2
Local Authentication and DCNM-LAN Local Users	15-2
Attribute Setup for External AAA using ACS 5.x	15-3
RADIUS and TACACS+ Authentication	15-3
User Role Assignment by RADIUS and TACACS+	15-3
Fallback to Local Authentication	15-4
Password Recovery	15-4
Users and Device Credentials	15-4
Virtualization Support	15-5
Licensing Requirements for Administering DCNM-LAN Authentication Settings	15-5
Prerequisites for Administering DCNM-LAN Authentication Settings	15-5
Guidelines and Limitations for Administering DCNM-LAN Authentication Settings	15-5
Configuring DCNM-LAN Authentication Settings	15-6
Configuring the Authentication Mode	15-6
Adding a DCNM-LAN Local User	15-6
Changing the Password of a DCNM-LAN Local User	15-8
Changing the Full Name, Role, or Description of a DCNM-LAN Local User	15-8
Deleting a DCNM-LAN Server User	15-9
Adding Authentication Servers	15-10
Changing Authentication Server Settings	15-12
Removing an Authentication Server	15-12
Viewing DCNM-LAN Local Users	15-13
Verifying Authentication Server Settings	15-13
Field Descriptions for DCNM-LAN Authentication Settings	15-14
Authentication Mode Section	15-14
DCNM-LAN Local Users Section	15-15
Authentication Servers Section	15-15
Additional References	15-16
Related Documents	15-16
Standards	15-16
Feature History for DCNM-LAN Authentication Settings	15-17

CHAPTER 16

Working with Topology 16-1

Information About Topology	16-2
Map Views	16-2
Physical View	16-3

PortChannel and vPC	16-4
Logical vPC View	16-5
L2 View	16-6
Layouts	16-6
vPC Support	16-7
DCNM-SAN Support	16-7
Common Topology	16-7
Access to DCM-SAN Features	16-7
FabricPath Support	16-7
Device Groups	16-8
Network Servers	16-9
Licensing Requirements for Topology	16-9
Prerequisites for Topology	16-9
Guidelines and Limitations	16-9
Using the Topology Feature	16-9
Opening the Topology Map	16-10
Understanding Device Icons and Links	16-13
Using the Viewing Tools	16-14
Showing, Hiding, and Using the Details Pane	16-16
Moving Devices in the Topology Map	16-18
Loading a Layout	16-19
Reloading the Previously Saved Layout	16-20
Showing a Virtual or Physical Chassis	16-21
Showing or Hiding Network Servers	16-22
Managing a Network Server	16-22
Showing or Hiding Device Groups	16-23
Expanding or Collapsing Device Groups	16-24
Creating a Device Group	16-25
Moving a Device Between Device Groups	16-26
Removing a Device from a Device Group	16-27
Copy Run to Start	16-28
Deleting a Device Group	16-29
Exporting the Topology as a JPG Image	16-30
Accessing DCM-LAN Features from the Topology Map	16-31
Accessing Cisco DCM-SAN Features from the Topology Map	16-32
Accessing Cisco FabricPath Features from the Topology Map	16-33
Multi-destination	16-33
Device Reachability	16-34
Unicast	16-35

Multicast	16-36
Launching the vPC Wizard	16-37
Managing a vPC	16-38
Finding and Resolving vPC Configuration Inconsistencies	16-39
Accessing Remotely Connected CNAs from the Topology Map	16-39
Using VSAN Overlay	16-40
Related Documents	16-41
Feature History for Topology	16-41

CHAPTER 17

Working with Inventory 17-1

Information About Inventory	17-1
Understanding Inventory	17-2
Understanding Power Usage	17-2
Module Pre-Provisioning	17-2
Supported Hardware	17-2
Upgrades and Downgrades	17-3
Licensing Requirements for Inventory	17-3
Prerequisites	17-3
Platform Support	17-3
Configuring Module Pre-Provisioning	17-4
Pre-Provisioning Offline Modules	17-4
Pre-Provisioning Online Modules	17-4
Pre-Provisioning FEX Modules	17-5
Reloading a Line Card	17-5
Displaying Inventory Information	17-6
Displaying the Chassis Information	17-6
Displaying the Module Information	17-7
Displaying the Power Supply Information	17-8
Displaying the Fan Tray Information	17-8
Displaying Power Usage Information	17-9
Displaying Power Usage Summary Information	17-9
Displaying Power Usage Details	17-9
Displaying Power Usage Statistics	17-10
Field Descriptions	17-10
Inventory: Details: Hardware Section	17-10
Inventory: Details: Software Section	17-11
Inventory: Power Usage	17-11
Feature History for Inventory	17-12

CHAPTER 18**Managing Virtual Devices 18-1**

- Managing Virtual Switches 18-1
- Creating VDCs with the VDC Setup Wizard 18-1
- Managing VDCs 18-2

CHAPTER 19**Configuring Interfaces on DCNM-LAN Client 19-1**

- Configuring Basic Interface Parameters 19-2
- Configuring Layer 2 Interfaces 19-3
- Configuring Layer 3 Interfaces 19-4
- Configuring Port Channels 19-4
- Configuring vPCs 19-5
- Configuring IP Tunnels 19-6
- Configuring Virtual Ethernet Interfaces 19-6
- Configuring Fabric Extenders 19-6
- Configuring Port Profiles 19-7

CHAPTER 20**Configuring Switching on DCNM-LAN Client 20-1**

- Configuring VLANs 20-1
- Configuring Private VLANs 20-2
- Configuring STP Extensions 20-2
- Configuring Rapid PVST+ 20-3
- Configuring MST 20-3
- Configuring Link-State Tracking 20-3
- Configuring FabricPath Switching 20-3
- FabricPath Forwarding 20-4
- Configuring Advanced FabricPath Features 20-4
- Using the Layer 2 Security Audit Wizard 20-4
- Configuring Dynamic ARP Inspection 20-4
- Configuring Port Security 20-5
- Configuring DHCP Snooping 20-6
- Configuring IP Source Guard 20-6
- Configuring Traffic Storm Control 20-7
- Configuring IGMP Snooping 20-7
- Configuring FCoE Initialization Protocol Snooping 20-7

CHAPTER 21

Configuring Routing on DCNM-LAN Client 21-1

- Configuring GLBP 21-1
- Configuring HSRP 21-1
- Configuring Keychain Management 21-2
- Configuring Object Tracking 21-2

CHAPTER 22

Security Configurations on DCNM-LAN Client 22-1

- Configuring IP ACLs 22-1
- Configuring MAC ACLs 22-2
- Configuring VLAN ACLs 22-2
- Configuring ARP ACLs 22-2
- Configuring Object Groups 22-3
- Configuring AAA 22-3
- Configuring Time Ranges 22-3
- Configuring RADIUS 22-3
- Configuring TACACS+ 22-4
- Configuring 802.1X 22-4
- Configuring User Accounts and RBAC 22-5

CHAPTER 23

Working with Configuration Change Management 23-1

- Information About Configuration Change Management 23-1
 - Version Browser 23-2
 - Archival Jobs 23-2
 - Archival Settings 23-2
 - Switch Profiles 23-3
 - Switch Profile Configuration Modes 23-3
 - Configuration Validation 23-4
 - Software Upgrades and Downgrades with Switch Profiles 23-5
 - VDC Support 23-5
- Licensing Requirements for Configuration Change Management 23-5
- Prerequisites 23-5
- Guidelines and Limitations for Configuration Change Management 23-6
- Platform Support 23-6
- Working with the Version Browser 23-6
 - Viewing the Archival Status of a Device 23-7
 - Viewing the Archival History of a Device 23-8
 - Browsing and Commenting on Configuration Versions 23-8

Using Copy Run to Start	23-9
Archiving the Current Running Configuration of a Device	23-9
Viewing an Archived Configuration Version	23-10
Comparing Configuration Versions	23-11
Using the Version Comparison Tools	23-13
Merging Configuration Differences	23-14
Performing a Configuration Rollback	23-15
Viewing the Rollback History of a Device	23-16
Deleting All Archived Configurations for a Device	23-17
Configuring Archival Jobs	23-18
Configuring an Archival Job	23-18
Enabling and Disabling an Archival Job	23-20
Deleting an Archival Job	23-20
Viewing Details of an Archival Job	23-21
Viewing the History of an Archival Job	23-21
Configuring Archival Settings	23-22
Configuring Version and History Settings	23-22
Configuring the Rollback File Server Setting	23-23
Configuring Switch Profiles	23-23
Configuring a Switch Profile	23-24
Configuring the Switch Profile Wizard Between Two vPCs	23-24
Configuring the Switch Profile Wizard Between Two Switches	23-25
Configuring the Sync Network View	23-25
Configuring the Switch Profile Migration Wizard for Dual Homed FEXes	23-26
Field Descriptions for Configuration Change Management	23-27
Field Descriptions for the Version Browser	23-27
Device: Details: Archival Status Section	23-28
Device: Details: Rollback History Section	23-28
Device: Details: Archival History Section	23-28
Version: Version Details Tab	23-28
Version: Compare Tab	23-29
Field Descriptions for Archival Jobs	23-29
Archival Job: Details Tab	23-29
Archival Job: Archival History Tab	23-30
Field Descriptions for the Archival Settings Contents Pane	23-31
Field Descriptions for the Switch Profiles Pane	23-31
Field Descriptions for the Switch Profiles Network View Pane	23-31
Additional References	23-32
Related Documents	23-32

Standards 23-32

Feature History for Configuration Change Management 23-32

CHAPTER 24

Managing Device Operating Systems 24-1

Information About Device OS Management 24-1

Device OS Management Screen 24-2

Software Installation Jobs 24-2

File Servers 24-3

VDC Support 24-3

Licensing Requirements for Device OS Management 24-3

Prerequisites 24-4

Guidelines and Limitations for Device OS Management 24-4

Platform Support 24-4

Using the Device OS Management Window 24-5

Viewing Device Image Details 24-5

Installing Software on a Device 24-5

Configuring Software Installation Jobs 24-7

Viewing Software Installation Job Details 24-7

Creating or Editing a Software Installation Job 24-8

Using the Software Installation Wizard 24-9

Rescheduling a Software Installation Job 24-12

Deleting a Software Installation Job 24-13

Adding or Changing Comments for a Software Installation Job 24-13

Changing Installation Options for a Software Installation Job 24-14

Configuring File Servers 24-15

Adding a File Server 24-15

Changing a File Server 24-16

Deleting a File Server 24-17

Field Descriptions for Device OS Management 24-18

Field Descriptions for Device OS Management 24-18

Device: Details: System Section 24-18

Device: Details: Software Installation Jobs Section 24-18

Field Descriptions for Software Installation Jobs 24-19

Installation Job: Details: General Section 24-19

Installation Job: Details: Devices and Software Images Section 24-20

Field Descriptions for the File Servers Contents Pane 24-20

Additional References 24-20

Related Documents 24-21

Standards 24-21

Feature History for Device OS Management 24-21

CHAPTER 25

Starting and Stopping Cisco DCNM-LAN Servers 25-1

Information About Starting and Stopping DCNM-LAN Servers 25-1

Licensing Requirements for Starting and Stopping Cisco DCNM-LAN Servers 25-1

Starting DCNM-LAN Servers 25-2

Starting a Single DCNM-LAN Server 25-2

Starting a Single DCNM-LAN Server (Microsoft Windows Server) 25-2

Starting a Single DCNM-LAN Server (RHEL) 25-2

Starting a Cluster of DCNM-LAN Servers 25-3

Starting with Windows GUI or RHEL CLI 25-3

Starting with Install Manager 25-4

Stopping DCNM-LAN Servers 25-5

Stopping Single DCNM-LAN Servers 25-5

Stopping a Single DCNM-LAN Server (Microsoft Windows Server) 25-5

Stopping a Single DCNM-LAN Server (RHEL) 25-6

Stopping a Cluster of DCNM-LAN Servers 25-6

Stopping with CLI 25-6

Example 25-7

Stopping with Install Manager 25-7

Related Documents 25-8

Feature History for Starting and Stopping a DCNM-LAN Server 25-9

CHAPTER 26

Data Center Network Manager (DCNM) - Vacuum and Autovacuum Postgres Databases 26-1

Background Information 26-1

Vacuum DCNM's Postgresql Database in Windows 26-1

Vacuum DCNM's Postgresql Database in Linux 26-2

26-2

CHAPTER 27

Administering Device Discovery 27-1

Information About Device Discovery 27-1

Device Discovery 27-2

Discovery Protocols 27-2

Cisco Discovery Protocol 27-3

Link Layer Discovery Protocol 27-3

Fibre Channel 27-3

Credentials and Discovery 27-3

Discovery Process	27-3
Cisco NX-OS System-Message Logging Requirements	27-4
Interface Link-Status Events Logging Requirement	27-4
Logfile Requirements	27-4
Logging Severity-Level Requirements	27-4
Automatic Logging-Level Configuration Support	27-5
During Device Discovery	27-5
At Feature Enablement in the DCNM-LAN Client	27-5
During Auto-Synchronization with Managed Devices	27-5
VDC Support	27-5
Licensing Requirements for Device Discovery	27-6
Prerequisites for Device Discovery	27-6
Guidelines and Limitations for Device Discovery	27-6
Performing Device Discovery	27-7
Verifying the Discovery Readiness of a Cisco NX-OS Device	27-7
Discovering Devices	27-9
Deep Discovery	27-11
Viewing the Status of Device Discovery Tasks	27-12
Where to Go Next	27-12
Field Descriptions for Device Discovery	27-12
Device Discovery Content Pane	27-12
Related Fields	27-15
Device System-Message Logging Level Reference	27-15
Cisco Nexus 7000 NX-OS Logging Levels per DCNM-LAN Feature	27-15
Cisco Nexus 5000 NX-OS Logging Levels per DCNM-LAN Feature	27-16
Cisco Nexus 4000 NX-OS Logging Levels per DCNM-LAN Feature	27-17
Cisco Nexus 1000V NX-OS Logging Levels per DCNM-LAN Feature	27-18
Additional References for Device Discovery	27-19
Related Documents	27-19
Standards	27-19
Feature History for Device Discovery	27-19

CHAPTER 28

Administering Devices and Credentials 28-1

Information About Devices and Credentials	28-1
Devices	28-2
Credentials	28-2
Device Status	28-2
VDC Support	28-2

Licensing Requirements for Devices and Credentials	28-3
Prerequisites for Administering Devices and Credentials	28-3
Guidelines and Limitations for Devices and Credentials	28-3
Configuring Devices and Credentials	28-3
Configuring Default Device Credentials	28-4
Clearing Default Device Credentials	28-5
Configuring Unique Credentials for a Device	28-5
Clearing Unique Credentials for a Device	28-6
Viewing Device Credentials and Status	28-7
Field Descriptions for Devices and Credentials	28-8
Device and Credentials Content Pane	28-8
Additional References for Devices and Credentials	28-9
Related Documents	28-9
Standards	28-9
Feature History for Devices and Credentials	28-10

CHAPTER 29

Administering Auto-Synchronization with Devices	29-1
Information About Auto-Synchronization with Devices	29-1
Automatic and Manual Purging of Event Data	29-2
Virtualization Support	29-2
Licensing Requirements for Auto-Synchronization with Devices	29-2
Prerequisites for Auto-Synchronization with Devices	29-2
Guidelines and Limitations for Auto-Synchronization with Devices	29-3
Configuring Device Auto-Synchronization	29-3
Starting and Stopping a Poller	29-3
Configuring the Polling Interval	29-4
Synchronizing with a Device	29-5
Deleting Data from the Events Database	29-5
Enabling and Disabling Automatic Event Purging	29-6
Configuring Automatic Event Purge Settings	29-7
Purging Events Now	29-8
Viewing the Status of Auto-Synchronization Pollers	29-9
Field Descriptions for Auto Synchronization with Devices	29-9
Poller Setting Tab	29-9
Events Database Administration Tab	29-10
Additional References	29-11
Related Documents	29-11
Standards	29-11

Feature History for Auto-Synchronization with Devices 29-11

CHAPTER 30

Administering Statistical Data Collection 30-1

- Information About Statistical Data Collection 30-1
 - Automatic and Manual Purging of Statistical Data 30-2
 - Virtualization Support 30-2
- Licensing Requirements for Statistical Data Collection 30-2
- Prerequisites for Statistical Data Collection 30-2
- Guidelines and Limitations for Statistical Data Collection 30-3
- Configuring Statistical Data Collection 30-3
 - Starting and Stopping Statistical Data Collection 30-3
 - Using Modes in Statistics Charts 30-4
 - Deleting Statistical Data from a Collection 30-5
 - Deleting a Collection 30-6
 - Deleting Data from the Statistics Database 30-6
 - Enabling and Disabling Automatic Statistical Data Purging 30-7
 - Configuring Automatic Statistical Data Purge Settings 30-8
 - Purging Statistical Data Now 30-9
- Viewing the Status of Statistical Data Collectors 30-10
- Field Descriptions for Statistical Data Collection 30-10
 - Summary Pane 30-10
 - Statistical Database Administration Tab 30-11
- Additional References 30-11
 - Related Documents 30-12
 - Standards 30-12
- Feature History for Statistical Data Collection 30-12

CHAPTER 31

Working With Threshold Rules 31-1

- Information About Threshold Rules 31-1
 - Threshold Rules Overview 31-1
 - Rising Threshold 31-2
 - Falling Threshold 31-2
 - Threshold Rule Properties 31-2
 - Threshold Rule Actions 31-2
- Threshold Rule Examples 31-2
 - Triggering an Action Each Time a Threshold is Crossed 31-2
 - Triggering an Action Only Once in a Period When a Threshold is Crossed 31-3
 - Triggering an Action Every Fourth Period When a Threshold is Crossed 31-4

Licensing Requirements for Threshold Rules	31-5
Configuring Threshold Rules	31-5
Creating Threshold Rules	31-5
Deleting Threshold Rules	31-7
Editing Threshold Rules	31-8
Viewing Threshold Rules	31-8
Applying a Threshold Rule to a Chart	31-8
Additional References	31-9
Related Documents	31-9
Standards	31-9
Feature History for Threshold Rules	31-9

CHAPTER 32

Administering DCNM-LAN Server Log Settings 32-1

Information About Administering DCNM-LAN Server Log Settings	32-1
Logging Levels	32-2
Log File and Location	32-2
Virtualization Support	32-2
Licensing Requirements for Administering DCNM-LAN Server Log Settings	32-2
Prerequisites for Administering DCNM-LAN Server Log Settings	32-3
Guidelines and Limitations for Administering DCNM-LAN Server Log Settings	32-3
Configuring DCNM-LAN Server Log Settings	32-3
Configuring the Default Logging Level	32-3
Configuring a Unique Logging Level for a Feature or Server Component	32-4
Configuring a Feature or Server Component to Use the Default Logging Level	32-4
Viewing DCNM-LAN Server Log Settings	32-5
Field Descriptions for DCNM-LAN Server Log Settings	32-5
DCNM-LAN Server Log Settings Contents Pane	32-5
Additional References	32-7
Standards	32-7
Feature History for DCNM-LAN Server Log Settings	32-7

CHAPTER 33

Managing Events 33-1

Information About Events	33-1
Licensing Requirements for the Event Browser	33-2
Prerequisites	33-2
Guidelines and Limitations for the Event Browser	33-2
Platform Support	33-3

Using the Event Browser and Events Tabs	33-3
Viewing the Event Browser	33-3
Applying and Removing an Event Filter	33-5
Viewing Events on an Events Tab	33-6
Changing the Status of an Event	33-7
Adding a Note to One or More Events	33-8
Deleting an Event	33-9
Field Descriptions for Events	33-10
Events Table	33-10
Event Details	33-11
Related Documents	33-11
Feature History for the Event Browser and Events Tabs	33-12

CHAPTER 34

Working with Network Analysis	34-1
Information About Network Analysis	34-1
Licensing Requirements for Network Analysis	34-1
Prerequisites for Network Analysis	34-2
Guidelines and Limitations for Network Analysis	34-2
Using the Network Analysis Feature	34-2
Using Network Analysis	34-2
Using the New Path Latency Session Wizard	34-4
Viewing Session Statistics	34-7
Related Documents	34-8
Feature History for Network Analysis	34-8

CHAPTER 35

Maintaining the Cisco DCNM-LAN Database	35-1
Information About Database Maintenance	35-1
Automatic and Manual Purging of Data	35-1
Database Backup	35-2
Database Clean	35-2
Database Restore	35-2
Licensing Requirements for Database Maintenance	35-3
Prerequisites for Database Maintenance	35-3
Guidelines and Limitations for Database Maintenance	35-3
Performing Database Maintenance	35-4
Backing Up the DCNM-LAN Database	35-4
Cleaning a DCNM-LAN Database	35-5
Restoring a DCNM-LAN Database from a Backup File	35-7

Additional References	35-9
Related Documents	35-9
Standards	35-9
Feature History for DCNM-LAN Database Maintenance	35-9

APPENDIX C
DCNM-SAN Event Management C-1

Benefits of the Event Management Tool	C-1
DCNM-SAN Event Management	C-1
Events	C-2
Purpose	C-2
Forwarding	C-2
DCNM-SAN Event Classification	C-3
Port Events	C-3
Event Log Format	C-3
Event Types	C-4
IVR	C-4
License	C-4
Port Alarm	C-4
Port Up and Port Down	C-5
Security	C-5
Switch Hardware	C-6
Switch Managability	C-7
Threshold	C-7
VSAN	C-7
Zone	C-7
Others	C-8

APPENDIX D
Vcenter Plugin D-1

Associating Vcenter with the Datasource	D-1
Registering Vcenter plugin	D-1
Triggering the plugin	D-2
Removing the plugin	D-2

APPENDIX B
Interface Nonoperational Reason Codes B-1



Preface

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

Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco MDS 9000 Family of multilayer directors and fabric switches.

Organization

This *guide* is organized as follows:

Chapter	Title	Description
Chapter 1	Introduction to Cisco Data Center Network Manager	Provides a brief overview of Cisco DCNM Fundamentals.
Chapter 4	Cisco DCNM-SAN Overview	Provides a brief overview of Cisco DCNM-SAN.
Chapter 3	Cisco Prime DCNM Web Client	Provides a brief overview of Cisco DCNM-SAN.
Chapter 5	Configuring Cisco DCNM-SAN Server	Provides in-depth descriptions of GUI and capabilities of Cisco DCNM-SAN Server.
Chapter 6	Configuring Authentication in Cisco DCNM-SAN	Describes the authentication schemes between Cisco DCNM-SAN components and fabric switches.
Chapter 7	Configuring Cisco DCNM-SAN Client	Provides in-depth descriptions of GUI and capabilities of Cisco DCNM-SAN.
Chapter 8	Device Manager	Provides in-depth descriptions of GUI and capabilities of Device Manager.
Chapter 9	Configuring Performance Manager	Provides overview of the Performance Manager architecture.
Chapter 10	Monitoring the Network	Provides details on monitoring the network.

Chapter	Title	Description
Chapter 11	Monitoring Performance	Provides details on using Performance Manager.
Chapter 12	Overview of DCNM-LAN	Provides an overview of what you need to do to start using Cisco Data Center Network Manager for LAN (DCNM-LAN).
Chapter 13	Installing and Launching the Cisco DCNM-LAN Client	Describes how to install and set up the Cisco DCNM-LAN client.
Chapter 14	Using the Cisco DCNM-LAN Client	Introduces the Cisco DCNM-LAN client and explains how to use it.
Chapter 15	Administering DCNM-LAN Authentication Settings	Describes how to administer the Cisco DCNM-LAN server user accounts.
Chapter 27	Administering Device Discovery	Describes how to use the Device Discovery feature.
Chapter 28	Administering Devices and Credentials	Describes how to use the Devices and Credentials feature.
Chapter 16	Working with Topology	Describes how to use the Topology feature.
Chapter 29	Administering Auto-Synchronization with Devices	Describes how to use the Auto-Synchronization with Devices feature.
Chapter 31	Working With Threshold Rules	Describes how to configure threshold rules.
Chapter 30	Administering Statistical Data Collection	Describes how to control statistical data collection.
Chapter 34	Working with Network Analysis	Describes how to track and monitor the latency between two specified switches.
Chapter 32	Administering DCNM-LAN Server Log Settings	Describes how to control Cisco DCNM-LAN server logs.
Chapter 25	Starting and Stopping Cisco DCNM-LAN Servers	Describes how to start and stop the Cisco DCNM-LAN server.
Chapter 35	Maintaining the Cisco DCNM-LAN Database	Describes how to maintain the Cisco DCNM-LAN database.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
[]	Elements in square brackets are optional.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

<code>screen font</code>	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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.

In this document, the following shortened names are used:

- Cisco Data Center Network Manager for SAN is also referred to as DCNM-SAN.
- Cisco Data Center Network Manager for LAN is also referred to as DCNM-LAN.

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 64](#)
- [Cisco Nexus 1000V Series Switch Documentation, page 65](#)
- [Cisco Nexus 2000 Series Fabric Extender Documentation, page 65](#)
- [Cisco Nexus 3000 Series Switch Documentation, page 65](#)
- [Cisco Nexus 4000 Series Switch Documentation, page 65](#)
- [Cisco Nexus 5000 Series Switch Documentation, page 65](#)
- [Cisco Nexus 7000 Series Switch Documentation, page 65](#)

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 7.1.x

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 7.1.x
- Cisco DCNM Installation Guide, Release 7.1.x

Cisco DCNM for LAN Configuration Guides

FabricPath Configuration Guide, Cisco DCNM for LAN
Interfaces Configuration Guide, Cisco DCNM for LAN
Layer 2 Switching Configuration Guide, Cisco DCNM for LAN
Security Configuration Guide, Cisco DCNM for LAN
System Management Configuration Guide, Cisco DCNM for LAN
Unicast Configuration Guide, Cisco DCNM for LAN
Virtual Device Context Configuration Guide, Cisco DCNM for LAN
Virtual Device Context Quick Start, Cisco DCNM for LAN
Web Services API Guide, Cisco DCNM for LAN

Cisco DCNM for SAN Configuration Guides

System Management Configuration Guide, Cisco DCNM for SAN
Interfaces Configuration Guide, Cisco DCNM for SAN
Fabric Configuration Guide, Cisco DCNM for SAN
Quality of Service Configuration Guide, Cisco DCNM for SAN
Security Configuration Guide, Cisco DCNM for SAN
IP Services Configuration Guide, Cisco DCNM for SAN
Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN
High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN
Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN
SMI-S and Web Services Programming Guide, Cisco DCNM for SAN

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:
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

Additional Related Documentation for Cisco MDS 9000

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS NX-OS Documentation Locator at:

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocator.htm

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases*

- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

Regulatory Compliance and Safety Information

- Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family

Compatibility Information

- Cisco Data Center Interoperability Support Matrix
- Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*

Hardware Installation

- Cisco MDS 9500 Series Hardware Installation Guide
- Cisco MDS 9200 Series Hardware Installation Guide
- *Cisco MDS 9100 Series Hardware Installation Guide*
- Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide

Software Installation and Upgrade

- Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide

Cisco NX-OS

- Cisco MDS 9000 Family NX-OS Licensing Guide
- Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide
- Cisco MDS 9000 Family NX-OS System Management Configuration Guide
- Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide
- Cisco MDS 9000 Family NX-OS Fabric Configuration Guide
- Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide
- Cisco MDS 9000 Family NX-OS Security Configuration Guide
- Cisco MDS 9000 Family NX-OS IP Services Configuration Guide
- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*
- Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS

Command-Line Interface

- Cisco MDS 9000 Family Command Reference

Intelligent Storage Networking Services Configuration Guides

- Cisco MDS 9000 Family I/O Acceleration Configuration Guide
- Cisco MDS 9000 Family SANTap Deployment Guide
- Cisco MDS 9000 Family Data Mobility Manager Configuration Guide
- Cisco MDS 9000 Family Storage Media Encryption Configuration Guide

Troubleshooting and Reference

- Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference
- Cisco MDS 9000 Family SAN-OS Troubleshooting Guide
- Cisco MDS 9000 Family NX-OS MIB Quick Reference
- Cisco DCNM for SAN Database Schema Reference

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.



New and Changed Information

The information in the new *Cisco Fabric Manager Fundamentals Configuration Guide* previously existed in Part 1: Getting Started, Part 8: Network and Switch Monitoring, and various Appendices of the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

[Table ii-1](#) lists the New and Changed features for this guide.

Table ii-1 **New and Changed Features for Cisco DCNM Release 7.2.x**

Feature	New or Changed Topics	Changed in Release	Where Documented
Configuring Templates	Template Structure	7.2(3)	Chapter 3, “Cisco Prime DCNM Web Client”
Border Leaf/Edge Router Auto-Configuration	Border Leaf Settings Connect New Border leaf to the Edge Router	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”
VxLAN Support for Nexus 6000 Series and Nexus 9000 Series Switches	Viewing Inventory Information	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”
Config sync on POAP	Power-On Auto Provisioning (POAP)	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”
Multiple Orchestrators Support	L2 Segment ID Range Management	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”
Three Tier Topology	Inter Switch Links View	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”
Secure LDAP for Fabric	Fabric	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”
Multiple Mobility Domains with VLAN Translation	Mobility Domains	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”
Slow drain	Slow Drain Analysis	7.1(1)	Chapter 3, “Cisco Prime DCNM Web Client”



CHAPTER 1

Introduction to Cisco Data Center Network Manager

Cisco Data Center Network Manager (DCNM) is a management system for the Cisco Unified Fabric. It enables you to provision, monitor, and troubleshoot the data center network infrastructure. It provides visibility and control of the unified data center so that you can optimize for the quality of service (QoS) required to meet service-level agreements.

Cisco DCNM increases overall data center infrastructure uptime and reliability, thereby improving business continuity. It provides a robust framework and comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco DCNM provides a high level of visibility and control through a single web-based management console for Cisco Nexus, Cisco MDS, and Cisco Unified Computing System products.

Cisco DCNM also supports the installation of the Cisco DCNM for SAN and Cisco DCNM for LAN components with a single installer. All Cisco DCNM for SAN and Cisco DCNM for LAN 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.



CHAPTER 2

Cisco Prime DCNM User Roles

Cisco DCNM defines what operations a user can perform in Cisco DCNM Web Client by controlling what features are available in the menu and tool bar items. Cisco DCNM role-based authorization limits access to the server operations depending on the user roles.

This chapter contains following sections:

- [Cisco DCNM Credentials, page 2-1](#)
- [Cisco DCNM Users, page 2-1](#)
- [DCNM Roles, page 2-1](#)
- [Roles from Cisco DCNM Perspective, page 2-2](#)

Cisco DCNM Credentials

Cisco DCNM has two sets of credentials, namely:

- Device credentials—used to discover and manage devices
- Cisco DCNM credentials—used to access the Cisco DCNM server.

This document describes about DCNM credentials and how user roles are mapped to specific set of DCNM server operations.

Cisco DCNM Users

Cisco DCNM user-based access allows the administrator to control the access to the Cisco DCNM server by using the DCNM client (Web Client or LAN client). The user access is secured by a password.

DCNM Roles

Cisco DCNM performs authorization of access to the users based on roles. The role-based authorization limits access to the Cisco DCNM server operations based on the roles to which the users are assigned. Cisco DCNM does not define new roles to access the DCNM server; however, the Cisco DCNM leverages the existing roles that are supported on the devices monitored, such as Cisco MDS 9000 Series Switches, and Cisco Nexus Switches.

Cisco DCNM supports following roles:

- global-admin
- network-admin
- lan-network-admin
- san-network-admin
- san-admin
- server-admin
- sme-admin
- sme-stg-admin
- sme-kmc-admin
- sme-recovery
- network-operator

In a typical enterprise environment, users and their roles are defined in a centralized place such as, TACACS+, RADIUS or LDAP. As Cisco DCNM supports the existing device roles, the administrator need not define new roles specifically.

Roles from Cisco DCNM Perspective

Cisco DCNM perspective defines the operations a user can perform on the Cisco DCNM client by controlling the menu and tool bar items. Different perspectives define different set of operations.

For example, the **Admin** perspective allows all the operations by showing all the menu and tool bar items where as **Operator** perspective allows limited set of operation by hiding Admin and Config Menu items.

Each DCNM user role is mapped to a particular DCNM perspective, which allows limited access to server features. DCNM clients support following four perspectives:

- [Admin Perspective, page 2-3](#)
- [Server Admin Perspective, page 2-3](#)
- [SME Perspective, page 2-4](#)
- [Operator Perspective, page 2-5](#)

[Table 2-1](#) describes how DCNM roles are mapped to client perspectives.

Table 2-1 DCNM Roles and Perspectives Mapping Table

Role	Perspective
global-admin	Admin Perspective
network-admin	
san-admin	
san-network-admin	
lan-network-admin (Web Client)	
server-admin	Server Admin Perspective

Table 2-1 DCNM Roles and Perspectives Mapping Table

Role	Perspective
sme-admin	SME Perspective
sme-sgt-admin	
sme-kmc-admin	
sme-recovery	
network-operator	Operator Perspective
lan-network-admin (SAN Thick Client)	

Admin Perspective

Admin Perspective can be accessed through the Cisco DCNM Web Client and SAN Client only, by the users who are assigned the role of global-admin, network-admin, san-admin, san-network-admin and lan-network-admin.

Web Client Admin Perspective

Web client admin perspective has full control of the DCNM server and can access all the features. Via the access to the **Admin** menu items, the users also has full control of Cisco DCNM authentication settings.

SAN Thick Client Admin Perspective

SAN thick client admin perspective has full control of the DCNM server and can access all the features. All the top-level menu items are accessible.

Server Admin Perspective

Server admin perspective can be accessed via web client and SAN thick client only by the users who are assigned the role of server-admin.

Web Client Server Admin Perspective

Web client server admin perspective has access to all the web client features. Via the access to the **Admin** menu items, the users also has full control of Cisco DCNM authentication settings.

SAN Thick Client Server Admin Perspective

The configuration capabilities of a server admin role are limited to FlexAttach and relevant data. The server admin can pre-configure SAN for new servers, move a server to another port on the same NPV device or another NPV device and replace a failed server onto the same port without involving the SAN administrator. The server admin will not be able to manage Fabric Manager users or connected clients. The menu items that are not related to server management are not accessible, e.g. **Zone**, **Performance**,

etc. SAN thick client server admin perspective has no access to **Discover** button, **Fabrics** and **License Files** tabs. The server admin is not able to manage Fabric Manager users or connected clients in SAN thick client.

SME Perspective

Storage Media Encryption (SME) perspective is designed for sme-admin, sme-stg-admin, sme-kmc-admin and sme-recovery role-based users. It can be categorized to five different sme admin perspective according to the roles:

- [Web Client SME Admin Perspective, page 2-4](#)
- [SME Storage Perspective, page 2-4](#)
- [SME Key Management Perspective, page 2-4](#)
- [SME Recovery Perspective, page 2-4](#)
- [SAN Thick Client SME Perspective, page 2-4](#)

Web Client SME Admin Perspective

Web client sme admin perspective is designed to sme-admin role users who have no access to **Admin** and **Config** menu items in the Web client and cannot use features under those menu items. On the other hand, the SME provision features are accessible.

SME Storage Perspective

SME storage perspective is designed to the sme-stg-admin role users. sme-stg-admin role users have same perspective as sme-admin role except you cannot manage the key management features.

SME Key Management Perspective

SME key management perspective is designed to the sme-kmc-admin role users. sme-kmc-admin role users have same perspective as sme-admin role except that you cannot perform SME configurations.

SME Recovery Perspective

SME recovery perspective is designed to the sme-recovery role users for master key recovery. sme-recovery role users have same perspective as sme-admin role except that you cannot perform the storage and key management features.

SAN Thick Client SME Perspective

SAN thick client SME perspective has no access to **Discover** button, **Fabrics** and **License Files** tabs. All the SME related perspective would not be able to manage Fabric Manager users or connected clients, as well as operator perspective.

Operator Perspective

Operator perspective is designed for network-operator and lan-network-admin role users, and lan-network-admin role only has SAN thick client operator perspective.

Web Client Operator Perspective

Web client operator perspective has no access to **Admin** and **Config** menu items and the features under those menu items cannot be used. All the other features can be used.

SAN Thick Client Operator Perspective

SAN thick client operator perspective has no access to **Discover** button, **Fabrics** and **License Files** tabs, and would not be able to manage Fabric Manager users or connected clients.



CHAPTER 3

Cisco Prime DCNM Web Client

Using Cisco Prime DCNM Web Client, you can monitor Cisco MDS and Nexus family switch events, performance and inventory, and perform minor administrative tasks.

Cisco Prime DCNM Web Client has few Graphical User Interface related changes. The new Cisco Prime DCNM Web Client is user experience (UX) 1.7 compliant.

The default user credentials to access DCNM 7.1.x are as configured during the deployment of the installers.

Cisco Prime DCNM Web Client provides the following features:

- [Navigating DCNM Web Client, page 3-1](#)
- [Downloading Cisco Prime DCNM-SAN Client, page 3-3](#)
- [Downloading Cisco Prime DCNM-LAN Client, page 3-4](#)
- [Downloading Cisco Device Manager Client, page 3-4](#)
- [Connecting to a Switch using the CLI, page 3-4](#)
- [Viewing Dashboard Information, page 3-5](#)
- [Viewing Health Information, page 3-22](#)
- [Viewing Performance Information, page 3-27](#)
- [Viewing Inventory Information, page 3-35](#)
- [Viewing and Creating Custom Reports, page 3-40](#)
- [Configuring Cisco Prime DCNM Web Client, page 3-44](#)
- [Administering Cisco Prime DCNM Web Client, page 3-79](#)
- [Using Cisco Prime DCNM Web Client with SSL, page 3-107](#)

Navigating DCNM Web Client

The DCNM Web Client has standardized certain navigation conventions.

- [Scope Menu, page 3-2](#)
- [Admin Menu, page 3-2](#)
- [Table and Filtering Navigation, page 3-2](#)
- [Printing, page 3-2](#)
- [Exporting to a File, page 3-2](#)

- [Sorting Columns, page 3-3](#)
- [Cisco Prime DCNM Web Search Engine, page 3-3](#)

Scope Menu

Beginning with Cisco NX-OS Release 6.x, a new drop-down list called Scope is added to Cisco Prime DCNM Web Client that applies to all pages except the Admin pages.

You can use the scope menu to filter network information by:

- Default_LAN
- Default_SAN
- Individual Fabric
- Group



Note

You can organize your fabrics and LAN switches in the **Admin > Groups** page.

The features accessible from the tabs are limited to the areas that you choose in the filter tree.

Admin Menu

You can use the admin menu to:

- **Set Default LAN Credentials:** These credentials will be used when connecting to the DCNM LAN devices.
- **Change Password:** Changes the password for the current logged in user.
- **Logout:** Logout from the DCNM Web Client.

Table and Filtering Navigation

Some tables that can be filtered will have a filter option to view subsets of the information. Either choose the filter menu or click **Filter**. An editable row at the top of the table appears. Enter values into the table cells and click **Return** to display matching rows.

Printing

Click **Print** to view the table in a printer-friendly format. You can then print the page from the browser.

Exporting to a File

An Export icon is in the lower right corner of some tables or top right corner of the window. Click this icon to export the data to Microsoft Excel.

Sorting Columns

Not all columns are sortable but you can click a sortable column head to sort the information for that column.

Cisco Prime DCNM Web Search Engine

The search engine helps you to locate records according to the following search criteria:

- Search by Name.
- Search by IP Address.
- Search by WWN.
- Search by Alias.
- Search by MAC Address.
- Search by Serial Number.

For more information see the section [Using the Cisco Prime DCNM Search Engine, page 3-3](#).

Using the Cisco Prime DCNM Search Engine

-
- Step 1** Click **Search box** on the top right corner of the main window.
You see the search text box.
- Step 2** Use the drop-down to search by:
- Name
 - IP Address
 - WWN
 - Alias
- Step 3** Enter the value based on the search option and click the arrow to begin the search.
The search results are displayed in a new window.
- Step 4** Select **Inventory** or **Performance** tabs to view specific search results.

Downloading Cisco Prime DCNM-SAN Client

You must use Cisco Prime DCNM Web Client to launch Cisco Prime DCNM-SAN Client.

-
- Step 1** On the DCNM Web Client home screen, click **Cisco Prime DCNM-SAN**.
If you are launching Cisco Prime DCNM-SAN Client for the first time, you see a message asking if you want to create shortcuts for Cisco Prime DCNM-SAN.
- Step 2** Click **Yes** to create shortcuts for Cisco Prime DCNM-SAN.
- Step 3** If you have the latest Java version installed, a Warning message is displayed.



Note The DCNM-LAN client supports JRE versions 1.6 and 1.7.

- Step 4** Click **Run with the latest version** button.
- Step 5** Enter the user credentials to log on to Cisco Prime DCNM-SAN client. This message appears only the first time you launch Cisco Prime DCNM-SAN Client.

Downloading Cisco Prime DCNM-LAN Client

You must use Cisco Prime DCNM Web Client to launch Cisco Prime DCNM-LAN Client.

- Step 1** On the DCNM Web Client home screen, click **Cisco Prime DCNM-LAN**.
If you are launching Cisco Prime DCNM-LAN Client for the first time, you see a message asking if you want to create shortcuts for Cisco Prime DCNM-LAN.
- Step 2** Click **Yes** to create shortcuts for Cisco Prime DCNM-LAN.
- Step 3** If you have the latest Java version installed, a Warning message is displayed.



Note The DCNM-SAN client supports JRE versions 1.6 and 1.7.

- Step 4** Click **Run with the latest version** button.
- Step 5** Enter the user credentials to log on to Cisco Prime DCNM-LAN client. This message appears only the first time you launch Cisco Prime DCNM-LAN Client.

Downloading Cisco Device Manager Client

You must use Cisco Prime DCNM Web Client to Install Cisco Device Manager client.

- Step 1** On the DCNM Web Client home screen, click **DM**.



Note Cisco Prime DCNM Device Manager supports JRE versions 1.6 and 1.7. Follow the instructions in the Cisco Device Manager installer wizard to proceed with the installation.

- Step 2** Once the installation is complete, enter the user credentials to log on to the Cisco Device Manager client.

Connecting to a Switch using the CLI

You can use the Cisco Prime DCNM Web Client to connect to a switch using the CLI.

- Step 1** On the DCNM Web Client home screen, click **CLI**.
- Step 2** Click the **Connect** button.
- Step 3** In the configuration window, use the check-box to select the switches.

- Step 4** Enter the user credentials and click the **Connect** button.
- Step 5** Use the switch panel to specify the command for a specific switch.

Adding a Security Exception

- Step 1** On the warning page, click **Or you can add an exception**.
- Step 2** Click **Add Exception**.
The Add Security Exception dialog box appears.
- Step 3** Click **Get Certificate**.
Read the text that describes the problems with this site.
- Step 4** Click **Confirm Security Exception**.
- MAC Address
 - Serial Number

Viewing Dashboard Information

The Cisco Prime DCNM Web Client dashboard gives you comprehensive information of the following:

- [Summary](#) - You can view the summary dashboard which displays the overall functioning of all the devices connected. It gives you daily statistics of the connected devices.
- [Fabric](#) - You can view the status of the inter switch links and edge ports.
- [Compute](#) - You can view the details and events for a particular Host along with its events and topology.
- [Switch Dashboard](#) - You can view details pertaining to a switch along with its current status and licensing information.
- [Storage](#) - You can view details about the storage device along with its events and topology.

Summary

The intent of the summary dashboard is to enable network and storage administrators to focus on particular areas of concern around health and performance of the data center switching as a snapshot of the last 24 hours. The functional view of the LAN and SAN switching consists of six dynamic portlets that display information in context of the selected scope. The scope can be adjusted in the upper center of the page to display more focused information particular to the managed domain and offers details of the specific topology or set of topologies part of the data center scope.

The various scopes available on the Cisco Prime DCNM Web Client are:

- datacenter
- default_SAN
- default_LAN

The following portlets are displayed on the summary dashboard, based on the scope of the Web Client:

- [Health, page 3-6](#)

- [Inventory, page 3-6](#)
- [Top CPU, page 3-6](#)
- [Top ISLs/Trunks, page 3-6](#)
- [Top SAN Host Ports, page 3-7](#)
- [Top SAN Storage Ports, page 3-7](#)
- [Topology, page 3-8](#)

Health

Broken into two sections listing specific problem areas by type of alert (host, ISL/trunks, VSAN, switch, storage) and events in the form of traps and syslogs listed in order of their severity for a period of 24 hours. The events and problems are hyper-linked to Health > Events and are filtered only for the clicked entity allowing you to drill down to particular problem or event for the contextual information. The events and problems change in context of the selected topology scope to display fabrics (SAN) and switches (LAN) that are part of the default or user defined group. The Health pane will display counts for Path not redundant and Missing Paths which will redirect to the [SAN Path Errors, page 3-23](#) section. To customize these groups to display more granular information see the [Managing Switch Groups, page 3-91](#) section.

Inventory

Displays the currently discovered inventory based on the selected scope. Switch inventory is broken into FC (Director vs Switch) and Ethernet and Virtual environment totals (VSAN and VLAN configuration). The bar graphs depicts used vs. available for capacity planning.

Click the + icon in the upper right corner to display 6 new boxes displaying detailed inventory for the logical environment, physical switches, ISLs of various types, modules installed (director class line cards and switches are shown), Ports which are broken into type (FC vs. Ethernet) with sub-categories showing counts based on speed. The final box displays Port Capacity, which shows percentage of ports used and calculates the days remaining of available ports based on consumption of available ports. By clicking the square icon in the upper right corner you will return to the previous view

Top CPU

Displays CPU utilization for the discovered switches over the last 24 hours with a red bar displaying the high watermark for that 24 hour period.

Click the + symbol in the upper right corner to display more detailed information of the average percentage of usage, peak percentage of usage, and the last time the information was updated

Top ISLs/Trunks

Displays the performance data for the top 10 performing ISLs and/or Trunk ports. Each entry shows current receive and transmit percentage with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the [Performance Manager Collections, page 3-101](#) section. Clicking on the bar graph to the left of each entry will provide a 24 hour graph for the selected item to provide context to the performance data being shown.

Click the + symbol in the upper right corner to display more detailed information on each entry by displaying the speed of the ISL/Trunk, the average and peak receive data, the average and peak transmit data, the combined receive and transmit data, the total number of errors and discards in the last 24 hours, and the time the data was last updated. By clicking the square icon in the upper right corner you will return to the previous view.

Top SAN Host Ports

Displays the performance data for the top 10 performing SAN host ports. Each entry shows current receive and transmit percentage with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the [Performance Manager Collections, page 3-101](#) section. Clicking on the bar graph to the left of each entry will provide a 24 hour graph for the selected item to provide context to the performance data being shown.

Click the + symbol in the upper right corner to display more detailed information on each entry by displaying the speed of the ISL/Trunk, the average and peak receive data, the average and peak transmit data, the combined receive and transmit data, the total number of errors and discards in the last 24 hours, and the time the data was last updated. By clicking the square icon in the upper right corner you will return to the previous view.

Top SAN Storage Ports

Displays the performance data for the top 10 performing SAN host ports. Each entry shows current receive and transmit percentage with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the [Performance Manager Collections, page 3-101](#) section. Clicking on the bar graph to the left of each entry will provide a 24 hour graph for the selected item to provide context to the performance data being shown.

Click the + symbol in the upper right corner to display more detailed information on each entry by displaying the speed of the ISL/Trunk, the average and peak receive data, the average and peak transmit data, the combined receive and transmit data, the total number of errors and discards in the last 24 hours, and the time the data was last updated. By clicking the square icon in the upper right corner you will return to the previous view.

Viewing Health Summary Information

-
- Step 1** From the menu bar, choose **Dashboard > Summary** and then see the **Health Summary** view.
- In the left side of the window, you see a summary table of problems and in the right side of the window, you see a summary table of events in the last 24 hours.
- Step 2** Click the warnings next to Switches, ISLs, Hosts, or Storage (other than 0) to see an inventory of switches, ISLs, or end devices for that fabric.
- Step 3** Choose the number of events next to the event severity levels (**Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug**) to see a summary of events and descriptions.

Viewing Performance Summary Information

BEFORE YOU BEGIN

To view performance information, you must activate performance collector.

From the menu bar, choose **Dashboard > Summary**, and then click **Daily Performance** view.

You see the Summary information.

The Top SAN Ports, Top SAN Storage Ports, Top ISL's/Trunks and Top Access Ports are Performance pods that are displayed depending on the pods selected.

If you select the Scope as default_SAN, a new area Daily Performance is displayed. For more information see the [New Area - Daily Performance, page 3-11](#) section.

Viewing Inventory Summary Information

-
- Step 1** From the menu bar, choose **Dashboard > Summary**.
- The Inventory summary pane is displayed.
- Step 2** Click the + icon or double-click the **Inventory** summary pane to view information for the selected scope only.
- The complete inventory details are displayed.

Differences by changing the Scope to default LAN or configured switch group



Note

To configure switch groups, see the [Managing Switch Groups, page 3-91](#) section.

- Health - Only LAN events are displayed.
- Inventory - Only LAN switch data is displayed
- Top ISLs/Trunks - Only displays LAN based ISLs/Trunks
- Top CPU - Only displays CPU data for the LAN switches
- Top Access Ports - Displays LAN access port performance information.
- A new area Topology is displayed. For more information, see the [Topology, page 3-8](#) section.

Topology

This displays the current physical topology with color-coding (displayed with a key in the lower right corner) for ISL utilization. You can hover over the switch indication circles to display the configured switch name, IP address, switch model, firmware version, last polled CPU utilization, and last polled memory utilization.

The memory or CPU utilization are displayed on the switch indicators. In addition the ISL/Trunk paths are also color-coded based on their TX+RX peak utilization. You can hover over the ISL/Trunk to show list of ports that create the connection and click on individual paths to launch the performance chart showcasing TX and RX utilization for the last 24 hours.

Click the + symbol in the upper-right corner to maximize the window and enables you to drag the switch icons to best display their infrastructure. Once icons are placed in the most desirable position you can save the layout by clicking the **Save** icon in the upper-left corner of the topology map. If the layout is moved you can restore the previously saved layout during the current session by clicking the **Restore** icon in the upper-left corner next to the save icon.

When the number of nodes is large, the switch information will not be displayed, as it cannot be accommodated on the page. However, if you click the **Switch Name** or use filters down to a subset, you will be able to view the switch information.

VxLAN VTEPs are shown in topology with **VTEP** icons. Click on the filter in top right corner in topology screen to search VTEPs based on VNI (VNI value > 4095) or multicast address. A **Details** link appears below the filter box. Click on the **Details** link below the filter box to view the search data in tabular format. In VNI search context, click **VTEP** to view the VTEP active peers.

The L2 view shows VLANs configured among the discovered devices. You can choose to view your topology based on the VLANs or Mapped Fabric Path topology. It also provides a visual representation of forwarding and non-forwarding links between Cisco Nexus devices in a data center network for configured VLANs.

FabricPath View

FabricPath support for L2MP capable devices, running the L2MP-ISIS protocol, is available in the L2 View of the Topology drawer. The L2 View contains a dialog box that allows you to select the type of graph to display. In each topology, a broadcast graph (multi-destination graph) is created by default to carry broadcast traffic and unknown unicast traffic. When you select the Fabricpath view in the dialog box, you can display the following types of graphs:

- **Multi-destination**—A multi-destination or broadcast graph built by ISIS for specified VLAN range to which the topology is mapped to in fabric path cloud.
ISIS maintains reachability information from each node to all other nodes that are present in fabric path cloud. Give a node, DCNM will enable users to view which all other nodes in fabric path cloud are not reachable.
- **Unicast**—A unicast graph displays equal cost routes between nodes in the fabric path cloud.
- **Multicast**—A multicast graph displays the multicast traffic from a specified device to all hosts that are listening to a particular IGMP group.

The FabricPath Topology Wizard allows you to do many operations, such as add to the FabricPath topology, display inventory, and display end devices.

To view the FabricPath topology in the L2 view:

-
- | | |
|---------------|---|
| Step 1 | Navigate to Dash Board > Topology . Expand the LAN topology. |
| Step 2 | Select L2 view > FabricPath . |
| Step 3 | Enter the Topology ID. The resulting action highlights all the links which are part of the specified topology. |
| Step 4 | To view the broadcast graph, select the Multi destination option in the graph selection window. Select the anchor device for which the broadcast graph must be displayed. |
| Step 5 | To view the unicast graph, select Unicast in the graph selection window. Select the source and the destination nodes. |
| Step 6 | To view the multicast graph, select Multicast in the graph selection window. Select the IGMP address and the ftag ID, and the anchor node for which the multicast graph must be displayed. |
-

VLAN View

VLAN view allows you to see the layer 2 network for the given range of VLAN. All the information related to STP such as protocol, STP role, STP root information are shown to the operator on topology. It is possible to see this information for a particular Switch group.

Spanning Tree Protocol (STP) is used to prevent loops when switches are interconnected via redundant links in a switched network. STP identifies the loops in a network and shuts down the redundant links to prevent the loops from forming. In the event of a link failure, STP will automatically activate the corresponding redundant link. In case of a switched network with multiple VLANs, loop-free paths will have to be computed for every VLAN.

During shallow discovery we are already fetching the information related to VLAN. Layer 2 Topology provides a visual representation of forwarding and non-forwarding links between networks of Nexus Devices for VLANs configured on them. VLAN view helps network administrators to manage STP protocol by providing a visual display of blocking and forwarding links and view information such as STP states (forwarding, blocking, learning, listening), STP roles (root, designated) and the root switch for STP.

To view the VLAN topology in the L2 view:

-
- Step 1** Navigate to **Dash Board > Topology**. Expand the LAN topology.
 - Step 2** Select **L2 view > VLAN**.
 - Step 3** Enter the VLAN range like “1-10”.
 - Step 4** Click on **Fetch** button.

By default, the forwarding and blocked links are shown in the topology. All the forwarding links are in green, blocked in red and the other links are greyed out. It will take some time to populate the topology since the information is fetched from the devices on demand. Select a given link and it will show all the information about that link.

Uncheck the option **Show Non-Forwarding link**, only forwarding links are shown in the topology.
Uncheck the option **Show Forwarding link**, only blocked links are shown in the topology.

Port Channel and vPC View

To view the PC vPC topology in the L2 view:

-
- Step 1** Select Scope as default_LAN or DataCenter.
 - Step 2** Navigate to Dashboard > Summary.
 - Step 3** Select the appropriate Device Group and open Topology.



Note Note: The port channels and vPC links are displayed when the user switches to PC vPC view on the topology screen supporting both LAN and SAN devices.

The PC vPC displays the vPCs, port channels, and physical links that are not part of vPC or port channel.

Differences by changing the Scope to default SAN or configured switch group

**Note**

To configure switch groups, see the [Managing Switch Groups, page 3-91](#) section.

- Health - Only SAN within scope events are displayed.
- Inventory: Only SAN switch data within the inventory is displayed
- Top SAN Host Ports: Displays SAN host port performance information within scope.
- Top SAN Storage Ports: Displays SAN storage port performance information within scope.
- Topology: Displays SAN topology within scope.
- A new area Daily Performance is displayed. For more information, see the [New Area - Daily Performance, page 3-11](#) section.

New Area - Daily Performance

This area displays the total performance of the displayed scope broken into three sections. ISL, Host and Storage. Total monitored port count per area is shown below the circular graph.

Each of the circular graphs will display the percentage of utilization based on 3 different thresholds depicted with color differentiation as follows:

- 0-50%: Green
- 51-80%: Yellow
- 81-100%: Red

You can click each displayed area to view performance data for only the ports, which fall within each performance scope. This will display more detailed information on each entry by displaying the name of the port. Click the bar graph icon to display the historical performance data for the selected port. A full performance graph also appears on the bottom of the screen displaying the last 24 hours, week, month, and year.

You can switch the graph to be displayed as a histogram and to perform predictive analysis on the port showing the most likely performance over the next 6 months based on the historical data gathered for the port. Click the + icon in the bar graph to overlay the performance data of any other port by clicking on the + icon and then clicking the graph icon next to another port listed above. The VSAN/VLAN configuration, speed of the trunk/ISL the average and peak receive data, the average and peak transmit data, the combined receive and transmit, the total number of errors and discards in the last 24 hours, and the last time the data was updated are also displayed.

To return to the summary view, from the menu bar select **Dashboard>Network**.

Fabric

The topology for the Fabric provides a tiered, scalable display for all the spines and leaves in the fabric. The topology feature also provides a visualization showing the health of the Central Point of Management (CPoM), which includes accessibility of DCNM to different services such as Power on Auto Provisioning (POAP) and Lightweight Directory Access Protocol service (LDAP).

The topology views are also integrated with an event/messaging mechanism using the open source package BlazeDS to dynamically update the display whenever any changes in the network are detected

There are two separate views:

- [Inter Switch Links View](#)
- [Edge Ports View](#)



Note

You can use the Topology View or Table View icons to switch between different views.

Inter Switch Links View



Note

These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

This view displays the super spines, spines and leaves in a tiered fashion. The super spines are displayed in the top tier under the section **<number of> Super Spines**, the spines are displayed in the middle tier under the section **<number of> Spines**, and the leaves are displayed under the section **<number of> Leaves**. Any spine that has tier level defined as 3 or above is considered as a Super Spine. If there are no super spines defined, then the spines and leaves are shown in 2 tiers.

The leaves can be grouped into Pods. Leaves inside a pod are shown as circles inside a box. Pod is defined for the switch by using the command **fabric connectivity pod <podname>**. The pod name is considered as the title for the pod. Any switch that do not have pods defined are shown under the Default pod. Border leaves and Edge Routers, are shown in vertical tiers in the BL/Edge Router pod with a dashed line border around the pod. BL/Edge Router is the standard default name for the pod showing border leaves and edge routers.

The Pods are ordered as Default pod, followed by user-defined pods in alphabetical order, followed by BL/Edge Router pod. Pod can be maximized using the '+' button at the top-right corner. Pressing the button again will bring it back to the original size. The size of the node inside the pod depends on the pod size and the number of nodes inside the pod.

All the nodes are shown as circles. The color of the circle depends on the status of the links or the status of the switch according to the color coding legend displayed under the Nodes section in the left-hand pane. The numbers on the circles indicate how many links are down currently on the switch. The numbers are not displayed in case of green (all links are OK) or grey circle (unreachable).

Clicking on the spine or leaf node disables all other nodes in that tier and displays detailed information about the links for the selected node in the left-side pane. The status column in the table shows the status of the link as an icon.

When the mouse is hovered over the target switch, the link between the 2 nodes is shown as a line along with a detailed popup. The popup displays the source port, target port, and status. Also, the corresponding row in the table on the left side panel is highlighted

Clicking on the selected node again will deselect the node and enable all the disabled nodes.

The color of the line specifying the link between the switches depends on the status of the link as defined below.

Green – Links status is Normal.

Red – Link is down

Blue – Cable/Tier mismatch detected

Orange – Wrong Configuration Detected

When a node is selected, the status of the link between the selected node and all the target nodes that the selected node is connected to is depicted by a colored halo around the original circle. The color of the halo depends on the status of the link, as specified above.

Check **Show Links** to view links between the Spines and the Leaves, and the links between the Border Leaves and the Edge Router.

Search

The search box in the left side panel provides a quicker way to search for a spine or leaf by name. It also supports VM search, where a user can enter a VM name (partial or complete) or VM IP or VM Mac or Segment ID or VxLAN ID or Multicast Group and search for the leaf/leaves that the VM(s) belong to.

The search box provides an auto-complete feature, which filters and shows the matched switch names in a drop down as the user types into the text box. User can type the partial or complete switch name in the box and enter to see the filtered results. A 'Details' link is shown under the search text box that can be clicked to see the search results. If only one node matches the entered text, then that node is selected and the rest of the nodes in the tier are disabled. The details for the links for that node are displayed on the left side panel. If multiple switch names match the entered text, all the matched nodes are, but no details are shown in the left side panel.

Edge Ports View

Edge Ports view provides a view of the leaf nodes as VPC pairs. The visualization provides an interface similar to Fabric Path Links view but with details specific to VPC feature.

Each leaf is shown as paired with its VPC peer, with the line between the pair indicating the VPC link. The numbers on the nodes indicate the number of edge ports down for that node.

The color of the circle depends on the status of the edge ports or the status of the switch.

Clicking on a node selects the node and its peer (if any) and shows the edge port status details for that node in the left side panel, as shown below.

On Selecting a single VPC pair, specific information about the VPC setup such as VPC domain ID, VPC peer names, VPC consistency state, VPC Peerlink consistency, Primary VPC Port Channel ID, VPC role for each peer, primary VPC peer link ID, Secondary VPC port channel ID and secondary VPC peerlink ID are all displayed in a short table above the interface listing.

No specific information is overloaded on the link colors, since the link is intended to represent both the Peer link and the keep alive link between peers

Health

This view (popup) can be accessed by clicking on 'Health' hyperlink on any of the topology visualization screens.

This view shows health of different services as defined by their accessibility from DCNM. These services include POAP (Power on Auto Provisioning), XCP (Extensible Communications Platform) service, LDAP (Lightweight Directory Access Protocol) service, etc., and the orchestrator which in turn is connected to different vCDs.

The node color is either green, which means the service is up and running and is accessible to DCNM, or red, which mean the service is down and cannot be accessed.

Switch Dashboard

The switch dashboard displays the details of the selected switch. The system information area includes the logical name of the switch, the group where the switch belongs, model number of the switch, serial number of the switch, the switch version, the location of the switch, IP address, model, world wide name (WWN) if available, uptime, DCNM license, status of the switch, indicators to determine whether the switch is sending traps and syslog information, current central processor unit (CPU) and memory utilization.

-
- Step 1** From the menu bar, choose **Dashboard > Network**.
- Step 2** An inventory of all the switches that are discovered by Cisco Prime DCNM Web Client appears. Click on a switch in the Name column. The switch dashboard appears.
- Step 3** (Optional) Click **ssh** to access the switch through Secure Shell (SSH).
- Step 4** (Optional) Click **Device Manager** to access the switch through Hypertext Transfer Protocol (HTTP) for that switch.
- Step 5** (Optional) Click **Accounting** to go to the [Viewing Accounting Information](#) page for that switch.
- Step 6** (Optional) Click **Backup** to go to the [Viewing a Configuration](#) page.
- Step 7** (Optional) Click **Events** to go to the [Viewing Events Registration](#) page.
- This physical port capacity feature is available for Cisco Prime DCNM licensed switches only.
- The physical port capacity area includes the available ports in each tier, such as 40G, 10G, 8G, 4G, 2G, and 1G and also the predicted number of days remaining to reach the maximum (100%) utilization.
- Step 8** Click a number under the Days left column to view the capacity trend.
- Step 9** Choose the **Modules** tab to display all the modules that are discovered on the switch.
- Step 10** Choose the **Interfaces** tab to display all the interfaces that are discovered for the switch. Select an interface row and right -click to view the following options:
- Port up... - Brings up a port.
 - Port down... - Brings down a port.
 - Access mode - Sets port in access mode.
 - Trunk mode - Sets port in trunk mode.
- Step 11** Select an option and in the CLI Authentication for the port window, specify the User Name and Password and click **Connect** to connect to the switch.



Note The CLI Authentication is required only if this is the first time you are performing an operation on an interface for a particular switch. For subsequent operations on the same switch, the authentication is not required.

A CLI window is displayed with the CLI details of the specific operation displayed at the bottom of the window.

- Step 12** When you press Enter on your keyboard, a dialog is displayed confirming if you want to change the config on a selected interface.
- Step 13** Close the **Blades** tab to display a list of UCS blades and their attributes.
- Step 14** Click **OK** to continue or **Cancel** to abort the operation.

When you click on a link in the ConnectedTo column, you see the other end of where the interface is connected. For example, if the other end of the interface is a switch interface, then it launches the Interfaces tab of the switch that the interface is connected. If the interface is connected to an end device, then it launches the host or storage dashboard.

Step 15 Choose the **Licenses** tab to display all the licenses installed on the switch.

Step 16 Choose the **Features** tab to display a list of all the features installed on the switch. The features tab is displayed only on Cisco Prime DCNM-SAN switches.

Step 17 Choose the **VxLAN** tab to display all VNIs, Multicast address, VNI Status and mapped VLAN for the VTEP. The VTEP IP address is displayed in left panel.



Note

VxLAN support is available on Cisco Nexus 6000 Series and Nexus 9000 Series switches only.

Compute

The compute dashboard provides you with all the information related to the discovered SAN and LAN hosts. It provides detailed information related to the network, such as I/O traffic, disk latency, CPU, memory statistics, topology, and events about each individual host and virtual machines that are configured on top of the virtual host. The compute dashboard consists of four panels:

- Host Enclosures panel—Lists the hosts and their network attributes.
- Traffic panel—Provides the I/O statistics, CPU and memory information, and disk latency of individual hosts or virtual machines.
- Topology panel—Provides end-to-end topology layout and path information between host enclosures and storage enclosures. The discovered virtual machines are displayed and when you select the virtual machine, the path to the SAN data source is displayed. You can toggle this view to list all data paths.
- Event panel—Provides information about events of all of the switch ports that are configured within a specific host enclosure.

This section contains the following topics:

- [Viewing Host Enclosures, page 3-15](#)
- [Viewing Host Events, page 3-16](#)
- [Viewing Host Topology, page 3-16](#)
- [View Host Traffic, page 3-16](#)

Viewing Host Enclosures

Beginning with Cisco NX-OS Release 6.x, you can view and search the network servers that are connected to the Cisco NX-OS devices. Cisco Prime DCNM extends the fabric visibility up to the server and allows you to discover and search the end devices that are attached to the network.



Note

Beginning with Cisco NX-OS Release 6.x, Server Credentials, Servers, and Static Server-Adapter Mapping are no longer available.

-
- Step 1** From the menu bar, choose **Dashboard > Compute**.
You see the list of hosts in the host enclosures table.
- Step 2** Click the **Show details** icon next to the host enclosure to view more details.
You see the Events, topology and Traffic information in the dashboard.
- Step 3** To edit the host name, double-click the Host Name, edit and then click the **Apply Changes** icon.
- Step 4** You can click the **Show Filter** to filter the storage enclosures by **Name** or by **IP Address**.

Viewing Host Events

-
- Step 1** From the menu bar, choose **Dashboard > Compute**.
You see the list of hosts in the host enclosures table.
- Step 2** Click the **Events** icon next to the host enclosure to view the Events panel.
- Step 3** Click the + icon in the Events panel to expand.
A list of all the events for the selected Host is displayed.

Viewing Host Topology

-
- Step 1** From the menu bar, choose **Dashboard>Compute**.
You see the list of hosts in the host enclosures table
- Step 2** Click the **Show details** icon next to the host enclosure to view the host topology details.
- Step 3** Click the magnifier icons to zoom-in or zoom-out.
- Step 4** Click the **Fabric/Network** icon to view the Fabric/Network path.
- Step 5** Click the **All Paths** icon to view the complete set-up.
- Step 6** Click the **First Shortest Path** icon to view the first shortest path.



Note Click **Map View** icon to enable the icons listed in Step 4, 5 and 6 above.

- Step 7** Click the **Tabular View** icon to view the host topology in tabular format.

View Host Traffic

-
- Step 1** From the menu bar, choose **Dashboard > Compute**.
You see the list of hosts in the host enclosures table
- Step 2** Click the **Show details** icon next to the host enclosure to view the host topology details.
- Step 3** Use the drop-down to select the traffic according to the time duration.
- Step 4** Select the icons to view the traffic as a **Grid**, **Line Chart** or **Stacked Chart**.
- Step 5** In the Traffic pane, the Enclosure Traffic is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.

Network

Cisco Prime DCNM Web Client enables you to view details of the switch including the system information, switch capacity, modules, interfaces, and licenses.

-
- Step 1** From the menu bar, choose **Dashboard > Network**.
- Step 2** An inventory of all the switches that are discovered by Cisco Prime DCNM Web Client appears. Click on a switch in the Name column to view the [Switch Dashboard](#).

Storage

The Storage dashboard provides you all the information about the SAN and LAN storage.

This section contains the following topics:

- [Viewing Storage Enclosure, page 3-17](#)
- [Viewing Storage Enclosure Events, page 3-18](#)
- [Viewing Storage Enclosure Topology, page 3-18](#)
- [Viewing Storage Enclosure Traffic, page 3-18](#)
- [Viewing Storage Systems, page 3-19](#)

Viewing Storage Enclosure

Once a datasource is configured and the discovery is completed, the discovered storage system(s) are displayed in the Name column in storage enclosures

-
- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.
- You see the storage enclosures table.
- Step 2** Click the **Show details** icon next to the storage name to view more details.
- You see the Events, Topology and Traffic information in the dashboard.
- Step 3** You can click the **Show Filter** to filter the storage enclosures by **Name** or by **IP Address**.
- Step 4** In the Traffic pane, the Enclosure Traffic is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.
- Clicking on an individual port slice of the pie chart will display specific traffic utilization details for that port.



Note Only EMC and NetApp vendors are supported. The ‘Other’ storage discovery handler is vendor neutral, so it depends on the vendor’s conformity to SMI-S standards to retrieve and display information.

Viewing Storage Enclosure Events

-
- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.
You see the list of storage enclosures in the table.
- Step 2** Click the **Events** icon next to the storage enclosure to view the Events panel.
- Step 3** Click the + icon in the Events panel to expand.
A list of all the events for the selected storage enclosure is displayed.

Viewing Storage Enclosure Topology

-
- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.
You see the list of storage enclosures in the table.
- Step 2** Click the **Show details** icon next to the storage enclosure to view the topology details.
- Step 3** Click the magnifier icons to zoom-in or zoom-out.
- Step 4** Click the **Fabric/Network** icon to view the Fabric/Network path.
- Step 5** Click the **All Paths** icon to view the complete set-up.
- Step 6** Click the **First Shortest Path** icon to view the shortest path.



Note Click **Map View** icon to enable the icons listed in Step 4, 5 and 6 above.

- Step 7** Click the **Tabular View** icon to view the host topology in tabular format.

Viewing Storage Enclosure Traffic

-
- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.
You see the list of storage enclosures in the table
- Step 2** Click the **Show details** icon next to the storage enclosure to view the topology details.
- Step 3** Use the drop-down to select the traffic according to the time duration.
- Step 4** Select the icons to view the traffic as a **Grid**, **Line Chart** or **Stacked Chart**.
- Step 5** Click the **Show Events** icon to view the events.
- Step 6** Use the options at the bottom of the screen to view a pie chart or a line chart. Click on each name on the chart to view its details.

Viewing Storage Systems

- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.



Note The datasource must be configured and discovered at least once to display the discovered storage system(s). For more information see [Adding, editing, removing, rediscovering and refreshing SMI-S Storage](#).

- Step 2** Select **Click to see more details...** icon to view the storage systems summary.

- Step 3** Use the drop-down to select the Storage System. Only EMC and NetApp vendors are supported.
- The default view consists of the storage system summary along with counts of it's elements and graph indicating the total aggregate space used vs. free space. Click each name in the graph to go to the item in the left menu.

- Step 4** The storage systems elements and their views are as follows:

- [Components, page 3-19](#)
- [Pools, page 3-19](#)
- [LUNs, page 3-20](#)
- [Filer Volumes, page 3-20](#)
- [Hosts, page 3-21](#)
- [Storage Processors, page 3-21](#)
- [Storage Ports, page 3-21](#)

Components

Components are containers for a set or sub-set of the disks in a storage system. The Component elements view displays a table of the disks in the collection, total number of disks managed and a summary of the collection's used vs. raw space.

- Step 1** Use the Storage System drop-down to select the storage system.
- Step 2** The right-hand pane displays a summary of the storage components. Click each name to go to the item in the left menu
- Step 3** Hover the mouse cursor on the graph to display its details.
- Step 4** In the left-hand pane, select the storage component to view its details.
- The number of disks managed along with its details are displayed.
- Step 5** Click a **Serial Number** to display the disk and the mapped LUNs details.
- Step 6** You can use the search box to search for a specific component.

Pools

Pools are user-defined collections of LUNs displaying the pool storage. The pools elements view displays a summary of the pools, lists the LUNs in the pool and also displays the total managed and raw space.

-
- Step 1** Use the Storage System drop-down to select the storage system.
The bar graph next to each pool indicates the total managed space of that pool.
- Step 2** In the left-hand pane, select a pool to display:
- Status of the pool
 - LUN's in the pool displaying the total raw space and the total managed space.
 - Raid Type
 - Disk Type
 - Details of the LUNs in the pool
- Step 3** You can use the search box to search for a specific pool.

LUNs

LUNs refer to a storage volume or a collection of volumes abstracted into a single volume. It is a unit of storage which can be pooled for access protection and management. Each LUN in the LUN Element View is displayed along with the mapping from Hosts to LUNs. If the associated Fabric has also been discovered, additional information concerning the end-to-end connection between a host and LUN is also displayed.

-
- Step 1** Use the Storage System drop-down to select the storage system.
- Step 2** In the left-hand pane, select a LUN to display:
- The LUN details along with its status and the number of Associated Hosts.
 - The Host LUN Mapping details along with the Access (Granted) information.

If the associated Fabric has also been discovered, additional information about the switch interfaces and zoning concerning the end-to-end connection between the Host and LUN is also displayed.



Note All fabrics that are discovered must be licensed or the fabric correlation will be disabled in the Web Client. When the feature is disabled, all correlation fields display “Unlicensed Fabric”.

- Step 3** You can use the search box to search for a specific LUN.

Filer Volumes

Filer Volumes are applicable only for NetApp. The Filer Volume Element view displays the Status, Containing Aggregate along with the total capacity and used space.

-
- Step 1** Use the Storage System drop-down to select the storage system.
- Step 2** In the left-hand pane, select the filer to display:
- The status of the filer along with the containing aggregate name.
 - Hover the mouse cursor over the graph to view the total capacity and available storage of the filer.
- Step 3** You can use the search box to search for a specific Filer.

Hosts

The Hosts only describes the NWWN(s) associated with a host or host enclosure along with the associated Host LUN Mapping and the Host Ports. If the associated Fabric has also been discovered, additional information concerning the end-to-end connection between a host and LUN is also displayed.

-
- Step 1** Use the Storage System drop-down to select the storage system.
- Step 2** In the left-hand pane, select a host to display:
- The NWWN (Node WWN) is the WWN of the device connected to the switch.
 - The Host Ports along with the Host LUN Mapping.
 - In the Host Ports section, click a Host Enclosure Name to view its Events, Topology and SAN Traffic. For more information see the [Storage, page 3-17](#) section.
 - In the Host Ports sections, click a Host Interface to view the [Switch Dashboard, page 3-14](#).
 - In the Host LUN Mapping section, click a Storage Interface to view the [Switch Dashboard, page 3-14](#).
 - In the Host LUN Mapping section, click a Storage Name to view its Events, Topology and SAN Traffic. For more information see the [Storage, page 3-17](#) section.

If the associated Fabric has also been discovered, additional information about the switch interfaces and zoning concerning the end-to-end connection between the Host and LUN is also displayed.



Note All fabrics that are discovered must be licensed or the fabric correlation will be disabled in the Web Client. When the feature is disabled, all correlation fields display “Unlicensed Fabric”.

- Step 3** You can use the search box to search for a specific host.

Storage Processors

Storage Processors are elements on a storage system, which enable some of its features. A storage processor includes the collection of Storage Ports it manages. In the Storage Processor Element View, the list of Storage Ports associated with a Storage Processor is displayed.

-
- Step 1** Use the Storage System drop-down to select the storage system.
- Step 2** In the left-hand pane, select a storage processor to display:
- The status, adapter details and the number of ports of the storage processor.
 - The storage ports details.
- Step 3** You can use the search box to search for a specific storage processor.

Storage Ports

A storage port is a single port on the Storage System. It displays the summary information of each port selected.

-
- Step 1** Use the Storage System drop-down to select the storage system.
- Step 2** In the left-hand pane, select a storage port to display its details.

Step 3 You can use the search box to search for a specific storage port.

Viewing Health Information

The Health menu shows events and issues for the selected items that are persistent across user sessions. The Health menu contains the following submenus:

- Accounting—Shows a list of accounting events.
- Events—Shows a detailed list of data center events. You can filter these events by scope, date, and type of event.
- Virtual Port Channels (LAN only)

This section includes the following topics:

- [Viewing Accounting Information, page 3-22](#)
- [Viewing Events Information, page 3-22](#)
- [SAN Host Redundancy, page 3-23](#)
- [Viewing a vPC, page 3-25](#)

Viewing Accounting Information

Step 1 From the menu bar, choose **Health > Accounting**.

The fabric name or the group name along with the accounting information is displayed.

Step 2 Select the **Filter** icon to search the accounting information by Source, User Name and Description. Use the Time drop-down to select the timeline for the search.



Note The Time drop-down appears only if you select the Filter icon.

Step 3 You can also select a row and use the **Delete** icon to delete accounting information from the list.

Step 4 You can use the **Print** icon to print the accounting details and use the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.

Viewing Events Information

You can view the events and syslog from Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Health > Events**.

The fabrics along with the switch name and the events details are displayed.

The Count column displays the number of times that the same event has occurred during the time period that is shown in the Last Seen column.

If you click a switch name displayed in the Switch column, Cisco Prime DCNM Web Client displays the switch dashboard.

If you click the IP address displayed in the Description column, the search feature displays all search results pertaining to that device. From here, you can choose the results that you wish to view.

- Step 2** Select one or more events in the table and click the **Add Suppressor** icon to open the shortcut of adding an event suppressor rule. For detailed information about adding event suppressor rules, please refer to [Add Event Suppression Rules](#).
- Step 3** Select a fabric and click the **Acknowledge** icon to acknowledge the event information for the fabric. Once you have acknowledged the event for a fabric, the acknowledge icon is displayed in the Ack column next to the fabric.
- Step 4** You can cancel an acknowledgment for a fabric by selecting the fabric and clicking the **Unacknowledge** icon.
- Step 5** You can use the **Filter** icon to enable filters for the columns displayed.
- Step 6** Select a fabric and use the **Delete** icon to delete the fabric and its event information from the list.
- Step 7** You can use the **Print** icon to print the event details and use the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.

SAN Host Redundancy

The SAN Host Redundancy check enables you to view the non-redundant host storage paths. It helps you identify the host enclosure errors along with the resolution to fix the errors.



Note

All fabrics that are discovered must be licensed or this feature will be disabled in the Cisco Prime DCNM Web Client. When the feature is disabled, a notification is displayed stating unlicensed fabrics are discovered.

From the menu bar, choose **Health > Diagnostics > SAN Host Redundancy**.

The following tabs are displayed:

- [SAN Path Errors](#) – Displays the summary section of the errors along with a table of errors.
- [Settings](#) – Displays the optional checks you can run along with the exclusion lists.

SAN Path Errors

- Step 1** From the menu bar, choose **Health > Diagnostics > SAN Host Redundancy > SAN Path Errors** tab.
- Step 2** Use the Error Types checkboxes to filter the types of host redundancy errors from the table.
 The **Good**, **Skipped** and **Errored** host enclosure counts are displayed. These are counts of the unique host enclosures as a whole and not path counts.
 The Error Types table provides individual path error counts of host enclosures seeing an error. The Host Enclosure column displays the hosts that contain the errors. These are counts of each path in the host enclosures seeing an error. Click a host to view the [Compute](#) details.
 The Storage Enclosure/Storage Port column displays the connected storage that is involved the errors.
- Step 3** Click a storage to view the [Storage](#) details.
- Step 4** In the Fix? column, hover the mouse cursor on the ? icon to view a solution to fix the error.
- Step 5** Click **Re-run Check Now** to run the check at anytime.

- Step 6** Click **Clear All** to clear all the errors displayed.
- Step 7** Click **Ignore Hosts** to add the selected row(s) host enclosure to an exclusion list. The errors from that host will no longer be reported and the current errors will be purged from the database.
- Step 8** Click **Ignore Storage** to add the selected row(s) storage enclosure to an exclusion list. The storage name is an hyperlink to the storage page. Select a row to delete the storage from the ignored list.
- Step 9** Click **Ignore Host-Storage Pair** to add the selected row(s) host-storage pair enclosure to an exclusion list. The host name is an hyperlink to the compute page and the storage name is an hyperlink to the storage page. Select a row to delete the storage pair from the ignored list



Note If you click on **Ignore Hosts**, **Ignore Storage** or **Ignore Storage Pair** before you select a row, an error message appears.

- Step 10** Click the **Print** icon to print the summary section and the errors as tables.
- Step 11** Click the **Export to Excel** icon to export the summary section and the errors as tables to a Microsoft excel spreadsheet.

The **Dashboard > Summary > Health** will display counts for Path not redundant and Missing Paths which will be hyperlinks to SAN Path errors section.

Settings

- Step 1** From the menu bar, choose **Health > Diagnostics > SAN Host Redundancy > Settings**.
- Step 2** Under the Test for pane, use the check boxes to select the host redundancy optional checks.
- Step 3** Select the **Automatically Run Check Every 24 hours** checkbox to enable periodic running of the checker. The checker will run every 24 hours starting 10 minutes after the server starts.
- Step 4** Select **Excluded VSAN** check box. Enter **VSAN** or **VSAN range** in the text field to skip the host enclosures that belong to VSAN(s) from the redundancy check.
- The Ignored Hosts pane displays the list of host enclosures that have been skipped/ignored by the redundancy check along with the reason the host enclosure check was skipped. The following reasons may be displayed:
 - Skipped: Enclosure has only one HBA
 - Host was ignored by the user.
 - Host ports managed by more than one federated servers. Check can't be run.
 - Skipped: No path to storage found.
 - The Ignored Storage tab displays the list of storage enclosures that have been selected to be ignored during redundancy check.
 - The Ignored Host Storage Pairs tab displays the list of host-storage pairs that have been selected to be ignored during redundancy check.
- Step 5** The column displays the The Click a host to view the [Compute](#) details.

- Step 6** Select a host enclosure and click the **Delete** button to remove the host from the ignored list and begin receiving errors about a host you had chosen to ignore. However, you can delete entries with message “Host was ignored by user”.

Slow Drain Analysis

The Slow Drain Analysis enables you to view slow drain statistics at the switch level and the port level. You can monitor the slow drain issue within any time frame. You can display the data in a chart format and export the data for analysis also.

The slow drain statistics are stored in the cache memory. Therefore, the statistics will be lost when the server is restarted or a new diagnostic request is placed.



Note

The jobs run in the background, even after you log off.

To configure and view the slow drain statistics,

- Step 1** From the menu bar, choose **Health > Diagnostics > Slow Drain Analysis**.
- Step 2** In the **Scope** field, select the Fabric from the drop-down list.
- Step 3** Use the radio button to select the desired **Interval** to collect data.
- Step 4** Click the **Play** icon to begin polling.
The server begins to collect the slow drain statistics based on the scope defined by the user. The **Time Remaining** is displayed in the right-side of the page.
- Step 5** Click the **Stop** icon to stop polling.
The server maintains the counters in the cache, until a new diagnostic request is placed. You can stop the polling before the time is up.
- Step 6** Click on the arrow next to **Current jobs** to display the slow drain details for the jobs running on the fabric. The **Fabric Name**, the **Status** of polling and **Details** icon for each fabric is displayed.
- Step 7** Click on the **Detail** icon to view the saved information.
- Step 8** Click on **Interface** chart icon to display the slow drain value for the switch port in chart format.
- Step 9** Click on the **Filter** icon to display the details based on the defined value for each column.
- Step 10** Select the **Data Rows Only** checkbox to filter and display the non-zero entries in the statistics.
- Step 11** Click on the **Print** icon to Prints the slow drain details.
- Step 12** Click on the **Export** icon to export the slow drain statistics to a Microsoft Excel spreadsheet.

Viewing a vPC

The virtual port channel (vPC) feature enables you to view the links that are physically connected to different devices as a single port channel. A vPC is an extended form of a port channel which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic. Traffic is distributed among two single device vPC end points. If there is an inconsistency in the vPC configurations, the vPC does not function correctly.

The Cisco Prime DCNM Web Client helps you to identify the inconsistent vPCs and resolve the inconsistencies in each vPC or in all vPCs.

This section contains the following:

- [Viewing vPC Inconsistencies](#)
- [Resolving vPC Inconsistencies](#)

From the menu bar, choose **Health > Virtual Port Channels (vPC)**.

Cisco Prime DCNM Web Client displays both the consistent and inconsistent vPCs.



Note The vPC inconsistency page displays inconsistencies only for the devices that have required Cisco Prime DCNM licenses installed on them. The devices that do not have Cisco Prime DCNM LAN license installed on them do not appear on this page.

[Table 3-1](#) displays the following vPC configuration details in the data grid view.

Table 3-1 vPC Configuration Details

Column	Description
vPC ID	You can view all the multichassis vPC end points and corresponding peer switches for each vPC ID.
Domain ID	Domain ID of the vPC peer switches.
Multi-chassis vPC End Point - Device Name	Details of the corresponding to peer single chassis primary vPC end points.
Multi-chassis vPC End Point - Port Channel ID	Single port channel that is connected to two single chassis vPC end points.
Primary vPC Peer - Peer Port Channel	Details of the corresponding multichassis vPC end points.
Primary vPC Peer - Port Channel	Single port channel that is connected to two single chassis vPC end points.
Primary vPC Peer - Device Name	Hostname of the vPC peer switches.
Secondary vPC Peer - Peer Port Channel	Details that correspond to the peer single chassis secondary vPC end points.
Secondary vPC Peer -Port Channel	Secondary port channel that is connected to two single chassis vPC end points.
Secondary vPC Peer -Device Name	Secondary Hostname of the vPC peer switches.
Consistency - Global	Configuration consistency between vPC peer port channels and vPC port channels. The valid values are Consistent and Inconsistent.
Consistency - Global	Configuration consistency between vPC peer switches that form a peer link.
Consistency -vPC	Configuration consistency between vPC peer port channels.

Viewing vPC Inconsistencies

You can view vPC inconsistencies from the Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Health > Virtual Port Channels (vPC)**.
- Step 2** Click a specific cell to view the global or vPC inconsistencies.
- A popup window displays the inconsistencies between the parameters.
- All the conflicts in the configuration for the vPC primary device and the secondary device are displayed in red.

Resolving vPC Inconsistencies

You can resolve vPC inconsistencies from the Cisco Prime DCNM Web Client.

-
- Step 1** Click the **Resolve All Conflicts** button to resolve all vPC inconsistencies.
- Step 2** Click the **Print** icon to print the page.
- Step 3** Click the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.

Viewing Performance Information

The Performance option displays an overview of the average and peak throughput and link utilization of the SAN components. The Filter drop-down list at the top-right of the screen allows you to filter the data based on various time periods.

In a large scale environment, we recommend that you select only "Trunks" and not the "Access or Errors and Discards" option during Performance Collections operations. This will ensure optimal performance monitored and managed entities in DCNM and allow successful Performance collection.

All performance pages allows you to print the page and export to Excel. By default, the **Export To Excel** icon is the export traffic number in raw digit format. You can export the same unit number for the traffic data, such as GB/Gb/MB/Mb/KB/Kb/B/b. For example; If you want to display the traffic numbers in GB, you need to modify the **server.properties** file to set **export.unitless=false** and **export.unit=GB**.

If you set **export.unitless=false**, and do not enter a value for the **export.unit**, it will display the default Web Client unit value.



Note You do not have to restart the DCNM server.

The Performance menu contains the following submenus:

- Switch—Shows the CPU, memory and traffic information.
- End Devices—Shows a detailed list of end devices (host or storage), port traffic and errors.
- ISLs—Shows a detailed list of ISL traffic and errors.
- NPV Links— Shows a detailed list of traffic between NPV devices and ports.
- Flows—Shows a detailed list of host-to-storage traffic.
- Ethernet—Shows a detailed list of Ethernet interfaces.
- Others—Shows a detailed list of other statistics.
- Virtual Port Channels—Shows a list of vPC utilization.

- N3K Buffer Usage - Displays performance of the N3K buffer usage and the total number of bursts during a specific time.

Rx/Tx Calculation

- Average Rx/Tx % = Average Rx/Tx divided by Speed * 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed * 100


Note

The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

Viewing Switch CPU Information

- Step 1** From the menu bar, choose **Performance > Switch > CPU**.
You see the CPU pane. This pane displays the CPU information for the switches in that scope.
- Step 2** You can use the drop-down to filter the view by 24 Hours, Week, Month and Year.
- Step 3** In the Switch column, click the switch name to view the [Switch Dashboard](#).
- Step 4** Click the chart icon in the Switch column to view the CPU utilization. You can also change the chart timeline to 24 hours, Week, Month and Year.


Note

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Switch Memory Information

- Step 1** From the menu bar, choose **Performance > Switch > Memory**.
You see the memory panel. This panel displays the memory information for the switches in that scope.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** Click the chart icon in the Name column to see a graph of the memory usage of the switch.
- Step 4** In the Switch column, click the switch name to view the [Switch Dashboard](#).
- Step 5** You can use the drop-down to view the chart in different time lines. Use the chart icons to view the traffic chart in varied views.


Note

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Switch Traffic and Errors Information

-
- Step 1** From the menu bar, choose **Performance > Switch > Traffic**.
You see the Switch Traffic and Errors panel. This panel displays the traffic on that device for the past 24 hours.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- Step 4** Click the switch name to view the [Switch Dashboard](#).



Note If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing ISL Traffic and Errors Information

-
- Step 1** From the menu bar, choose **Performance > ISLs/Trunks**.
You see the ISL Traffic and Errors pane. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
Notation NaN (Not a Number) in the data grid means that the data is not available.
There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:
- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
 - To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
 - Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds.
 - To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
 - For the Rx/Tx calculation, see the [Rx/Tx Calculation, page 3-28](#) section.



Note If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance.

Viewing Performance Information for Ethernet Ports

-
- Step 1** From the menu bar, choose **Performance > Ethernet**.
You see the Ethernet Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Select the time range, and click **Filter** to filter the display.
- Select the name of an Ethernet port from the Name column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner. To view real-time information, choose **Real Time** from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data.
- For the Rx/Tx calculation, see the [Rx/Tx Calculation, page 3-28](#) section.



Note If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Other Statistics

Step 1 From the menu bar, choose **Performance > Others**.

You see the Others window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

There are variations to this procedure. In addition to these basic steps, you can also do the following:

- Select the time range, and click **Filter** to filter the display.
- Click the chart icon in the Switch column to see a graph of the performance for this user defined object. You can change the time range for this graph by selecting it from the drop-down list in the upper right corner.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**
- Use the chart icons to view the traffic chart in varied views.



Note If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information for NPV Links

Step 1 From the menu bar, choose **Performance > NPV Links**

You see the NPV Link and Traffic Errors window. This window displays the NPV links for the selected scope.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 Click the chart icon in the Name column to see a list of the traffic for the past 24 hours.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for NPV links:

- You can change the time range for this information by selecting from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information on All Ports

You can view the performance of devices connected to all ports.

Step 1 From the menu bar, choose **Performance > End Devices > All Ports**.

You see the All Ports Traffic and Errors window.

Step 2 You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

Step 3 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 4 Click the chart icon in the Name column to see:

- A graph of the traffic on that device according to the selected timeline.
- Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds. You can also use the icons to Append, Predict and Interpolate Data.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information on Host Ports

You can view the performance of devices connected to the host ports

Step 1 From the menu bar, choose **Performance > End Devices > Host Ports**.

You see the Host Ports Traffic and Errors window.

- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year
- Step 3** To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**
- Step 4** Click the chart icon in the Name column to see
- A graph of the traffic on that device according to the selected timeline.
 - Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds. You can also use the icons to Append, Predict and Interpolate Data.



Note If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection

Viewing Performance Information on Storage Ports

You can view the performance of devices connected to the storage ports.

- Step 1** From the menu bar, choose **Performance > End Devices > Storage Ports**.
You see the Storage Ports Traffic and Errors window.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- Step 4** Click the chart icon in the Name column to see:
- A graph of the traffic on that device according to the selected timeline.
 - Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds. You can also use the icons to Append, Predict and Interpolate Data.



Note If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information on Host Enclosure

You can view the performance of devices connected to the host enclosure.

- Step 1** From the menu bar, choose **Performance > End Devices > Host Enclosure**.
You see the Host Enclosures Traffic and Errors window.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- Step 4** Click the chart icon in the Name column to see:
- A graph of the traffic on that device according to the selected timeline.

- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to Append, Predict and Interpolate Data.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information on Storage Enclosure

You can view the performance of devices connected to the storage enclosure.

-
- Step 1** From the menu bar, choose **Performance > End Devices > Storage Enclosure**.
You see the Storage Enclosures Traffic and Errors window.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- Step 4** Click the chart icon in the Name column to see:
- A graph of the traffic on that device according to the selected timeline.
 - Use the chart icons to view the traffic chart in varied views.
 - You can also use the icons to Append, Predict and Interpolate Data.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information on Port Groups

You can view the performance of devices connected to the port groups.

-
- Step 1** From the menu bar, choose **Performance > End Devices > Port Groups**.
You see the Port Groups Traffic and Errors window.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** Click the name port group to see the members of that port group.
There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for the port groups:
- To change the time range for this graph, select it from the drop-down list in the upper right corner.
 - To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
 - Use the chart icons to view the traffic chart in varied views.
 - You can also use the icons to Append, Predict and Interpolate Data.
 - To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information for FC Flows

You can view the performance of the FC Flow traffic.

**Note**

Restart the Performance Manager in the Cisco Prime DCNM Web Client when you add or remove an FC FLOW from the switch configuration, for it to reflect under the **Performance > FC Flows**.

-
- Step 1** From the menu bar, choose **Performance > FC Flows**.
You see the Flow Traffic window.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.
- Step 4** Click the chart icon in the Name column to see:
- A graph of the traffic on that device according to the selected timeline.
 - Use the chart icons to view the traffic chart in varied views. To view real-time information, choose **Real Time** from the drop-down list in the upper right corner.
 - You can also use the icons to Append, Predict and Interpolate Data.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Performance Information for Virtual Port Channels

You can view the relationship among virtual port channels (vPCs). You can view the statistics of all member interfaces and the aggregate of the statistics at the port channel level.

-
- Step 1** From the menu bar, choose **Performance > Virtual Port Channels (vPC)**.
The vPC performance statistics appears and the aggregated statistics of all vPCs are displayed in a tabular manner.
- Step 2** Click on a device name in the Primary vPC peer or Secondary vPC peer column to view its member interface.
A popup window displays the member interfaces of the selected device.
- Step 3** Click the Chart icon of the corresponding interface to view its historical statistics.
The traffic distribution statistics appear at the bottom of the vPC window. By default, the Cisco Prime DCNM Web Client displays the historical statistics for 24 hours.
There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for flows:

- To change the time range for this graph, select it from the drop-down list in the upper right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views.
- You can also use the icons to Append, Predict and Interpolate Data.
- To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

N3K Buffer Usage

You can view the performance of the N3K buffer usage and the total number of bursts during a specific time.

Step 1 From the menu bar, choose **Performance > N3K Buffer Usage**

You see the N3K Buffer Usage window which displays the average number of burst per hour, maximum number of burst per hour and the total number of burst per hour.

Step 2 To export the data into a spreadsheet, click the **Export to Excel** icon in the upper-right corner and then click **Save**.

Step 3 Click the chart icon in the Name column to see:

- A bar chart of the hourly based burst number for the selected interface.
- Clicking each item in the bar chart will open a detailed buffer burst window for the selected hour.

**Note**

If the performance tables do not contain any data, see the [Performance Manager Collections](#) section to turn on performance data collection.

Viewing Inventory Information

Beginning with Cisco Prime DCNM release 6.x, you can view the inventory and the performance for both SAN and LAN switches by using the global Scope pane. You can select LAN, SAN, or both to view the inventory information. You can also export and print the inventory information.

You can either Print this information or export to Microsoft Excel.

The Inventory menu includes the following submenus:

- Switches—Displays details about switches.
- Modules—Displays details for MDS switching and services modules, fans and power supplies.
- ISLs/Trunks—Displays the Inter-Switch Links.
- Licenses—Displays details about the licenses in use in the fabric.
- NPV Links—Displays the links between NPV devices and ports.

- VSANs—Displays details about VSANs.
- Active Zones— Displays details about the Regular and IVR zones.
- FC End Devices—Displays details about the devices connected to the various ports.
- .Port Mapper—Displays the port mapper information.
- VxLAN—Displays the VxLAN configured for the switch.

**Note**

You can use the **Print** icon to print the information displayed or you can also use the **Export to Excel** icon to export the information displayed to a Microsoft Excel spreadsheet.

Viewing Inventory Information for Switches

Step 1 From the menu bar, choose **Inventory > Switches**.

You see the Switches window displaying a list of all the switches for a selected Scope.

Step 2 You can also view the following information.

- In the Name column, select a switch to display the [Switch Dashboard](#). For more information about switch dashboard, see the [Switch Dashboard](#) section.
- Use the drop-down to view **All**, **Warning** or **Unmanaged** switches.

Step 3 In the Health column, the switch health is calculated by the capacity manager based on the following formula in the **server.properties** file.

The function to implement is

```
#          calculate(x, x1, y, y1, z)
#          @param x: Total number of modules
#          @param x1: Total number of modules in warning
#          @param y: Total number of switch ports
#          @param y1: Total number of switch ports in warning
#          @param z: Total number of events with severity of warning or above
```

Step 4 The value in the Health column is calculated based on the following default equation.

$((x-x1)*1.0/x) * 0.4 + ((y-y1)*1.0/y)*0.3 + ((z*1.0/1000 >= 1) ? 0 : ((1000-z)*1.0/1000)*0.3)$.

In the above formula, the switch health value is calculated based on the following:

- Percentage of Warning Modules (Contributes 40% of the total health).
- Percentage of Warning Ports (Contributes 30% of the total health)
- Percentage of events with severity of Warning or above (Contributes 30% of the total health. If there are more than 1000 warning events, the event health value is 0).

You may also have your own health calculation formula by implementing the common interface class:**com.cisco.dcbu.sm.common.rif.HealthCalculatorRif**. Add the.jar file to the DCNM server and modify the **health.calculator** property to point to the class name you have created.

The default Java class is defined

as:**health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculator**.

- Capacity Manager calculates health only for the license switches. If the health column does not display a value, the switch either does not have a license or it has missed the capacity manager's daily cycle.
- If the switch is unlicensed, in the DCNM License column click **Unlicensed**. The **Admin>License** window appears which allows you to assign a license to the user.
- The capacity manager runs two hours after the DCNM server starts. So, if you discover a device after two hours of the DCNM start time, the health will be calculated 24 hours after this DCNM start time

Viewing Inventory Information for Modules

-
- Step 1** From the menu bar, choose **Inventory > Modules**.
You see the Modules window displaying a list of all the switches and its details for a selected Scope.
You can also view the following information:
- Step 2** In the Name column, select a switch to display the [Switch Dashboard](#). For more information about switch dashboard, see the [Switch Dashboard](#) section.
- Step 3** Use the drop-down to view **All**, **Warning** or **Unmanaged** switches

Viewing Inventory Information for ISLs/Trunks

-
- Step 1** From the menu bar, choose **Inventory > ISLs/Trunks**.
You see the ISLs window displaying the ISL details along with the speed and status of the ISLs.
- Step 2** Use the drop-down to view **All** or **Warning** information for the ISLs.

Viewing Inventory Information for Licenses

-
- Step 1** From the menu bar, choose **Inventory > Licenses**.
You see the Licenses window displaying the license type and the warnings. based on the selected Scope.
- Step 2** In the Name column, select a switch to display the [Switch Dashboard](#). For more information about switch dashboard, see the [Switch Dashboard](#) section.
- Step 3** Use the drop-down to view **All**, **Warning** or **Unmanaged** switches.

Viewing Inventory Information for NPV Links

-
- Step 1** From the menu bar, choose **Inventory > NPV Links**
You see the NPV Links window displaying the NPV details along with the speed and status of the NPV links.
- Step 2** Use the drop-down to view **All**, **Warning** or **Unmanaged** switches.

Viewing Inventory Information for VSANs

- Step 1** From the menu bar, choose **Inventory > VSANs**.
You see the VSAN window displaying the VSAN details along with the status and Activate Zoneset details.
- Step 2** Use the drop-down to view **All** or **Warning** information for the VSANs.

Viewing Inventory Information for Regular Zones

- Step 1** From the menu bar, choose **Inventory > Active Zones > Regular Zones**.
You see the Regular Zones window displaying the inventory details of the fabrics in the regular zone.
- Step 2** Click the **Show Filter** icon to enable filtering by VSAN or Zone.

Viewing Inventory Information for IVR Zones

- Step 1** From the menu bar, choose **Inventory > Active Zones > IVR Zones**.
You see the IVR Zones window displaying the inventory details of the fabrics in the IVR zone.
- Step 2** Click the **Show Filter** icon to enable filtering by Zone.

Viewing Inventory Information for All Ports on FC End Devices

- Step 1** From the menu bar, choose **Inventory > End Devices > All Ports**.
You see the End Devices window displaying details of the FC End Devices on the all the ports.
- Step 2** Use the drop-down to view **All** or **Warning** information for the FC End devices.
- Step 3** Click the **Show Filter** icon to enable filtering by Enclosure, Name or VSAN.

Viewing Inventory Information for Host Ports on FC End Devices

- Step 1** From the menu bar, choose **Inventory > End Devices > Host Ports**.
You see the **End Devices>Host Ports** window displaying details of the FC End Devices on the host ports.
- Step 2** Use the drop-down to view **All** or **Warning** information for the FC End devices on host ports.
- Step 3** Click the **Show Filter** icon to enable filtering by Enclosure, Name or VSAN.

Viewing Inventory Information for Storage Ports on FC End Devices

- Step 1** From the menu bar, choose **Inventory > End Devices > Storage Ports**.
You see the **End Devices>Storage Ports** window displaying details of the FC End devices on the storage ports
- Step 2** Use the drop-down to view **All** or **Warning** information for the FC End devices on storage ports.
- Step 3** Click the **Show Filter** icon to enable filtering by Enclosure, Name or VSAN.

Viewing Inventory Information for Port Mapper

Beginning with Cisco NX-OS Release 6.x, you can view information about all the logical and physical ethernet interfaces of all the devices that are discovered by the Cisco Prime DCNM Web Client.

- Step 1** From the menu bar, choose **Inventory > Port Mapper**.
You see the Port Mapper window displaying the details listed in [Table 3-2](#)

Table 3-2 Port Mapper Inventory

Column	Description
Device	Name of the device to which the interface belongs.
Interface Name	Name of the interface.
Description	Description of the interface.
Mode	Mode of the interface.
Admin Status	Admin status of the port.
Operational status	Operational status for the port.
Speed	Speed for the interface. It is not the configured speed.
Duplex	Single port channel that is connected to two single chassis vPC end points.
STP Protocol	Spanning Tree Protocol (STP) whether or not the Per-VLAN Spanning Tree (PVST), Multiple Spanning Tree (MST), and rapid-PVST is configured.
Access/Allowed VLANs	Access VLAN is displayed if the port mode is access or displays allowed VLAN if the port mode is trunk.
Built-in MAC Address	MAC address for the port.
IP Address/Mask	IP address configured on the port and the IP mask.
SFP Serial Number	Serial number of the Small Form-Factor Pluggable (SFP) if it is attached on the port

- Step 2** Click the **Show Filter** icon to filter the port mapping information.

The filter options in the Device, Interface Name, Description, Access/Allowed VLANs, Built-in MAC Address, IP Address/Mask, and SFP SerialNumber column allows you to enter text inputs in the respective field and search. In addition, you can use the drop-down list in the Mode, Admin Status, Operational Status, Speed, Duplex, and STP Protocol column to limit the objects that appear in the report.

- Step 3** Click the **Print** icon to print the port mapping report of the selected device.
- Step 4** Click the **Export to Excel** icon to export the port mapping report of the selected device to a Microsoft Excel spreadsheet.
- Step 5** Click a cell in the STP Protocol column
A popup window displays the STP settings of the port.
- Step 6** Click the **Show Filter** icon to filter the STP settings.

Viewing and Creating Custom Reports

The Reports menu allows you to create customized reports based on historical performance, events, and inventory information gathered by Cisco Prime DCNM. You can create aggregate reports with summary and detailed views. You can also view previously saved reports.



Note

Beginning with Cisco Prime DCNM Release 6.x versions, reports can be generated for SAN and LAN. The global view Scope pane will contain SAN, LAN, and Default LAN configurations. You can select any of these configurations, and generate reports.

The Report menu includes the following sub-menus:

- View—Displays previously saved reports.
- Generate—Generates a custom report based on the selected report template.
- Create SAN User Defined—Allows you to generate a report based on a new custom template or select an existing template along with the Configuration of Scope, Inventory, Performance, Health and User Selection.
- Jobs—Displays scheduled jobs based on the selected report template.

This section includes the following topics:

- [Viewing Reports, page 3-40](#)
- [Generating a Report, page 3-41](#)
- [Creating SAN User Defined Reports, page 3-42](#)
- [Deleting a Report Template, page 3-43](#)
- [Modifying a Custom Report Template, page 3-43](#)
- [Modifying a Custom Report Template, page 3-43](#)

Viewing Reports

You can view the saved reports based on the following selection options:

- By Template

- By User
- From the menu bar, select **Reports > View**.

You see the view reports window, displaying the **View Reports By tree** on the left pane.

-
- Step 1** In the left pane, expand **By Template** or **By User** folder.
- Step 2** Select the report you wish to view. You can view the report in the main screen or you can select the report in the Report column to view the HTML version of the report in a new browser.
- Step 3** To delete a specific report, select the check box and click the **Delete Report** icon.
- Step 4** To delete all reports, check the check box in the header, and click the **Delete Report** icon.



Note If you have multiple fabrics, you can select the DCNM-SAN group in the Scope to view Host to Storage connectivity of multiple fabrics in a single report.

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
 - A detailed information for the device of the module. The table contains details about the tests failed.
-

Generating a Report

You can generate reports based on a selected template or you can schedule the report to run at a specified time.

-
- Step 1** In the configuration window, use the drop-down to define the scope for report generation.
- In the Scope drop-down, you can select a scope group with dual fabrics, the traffic data generated by hosts and storage end devices are displayed side-by-side which enables you to view and compare traffic data generated on dual fabrics. To View this report, in the Other Predefined folder, select **Traffic by VSAN (Dual Fabrics)**. Click **Options** to select the Device Type and Fabrics. Click **Save** to save the configuration.
- Step 2** From the menu bar, select **Reports > Generate**.
- You see the Generate Report window.
- Step 3** In the Generate a Report Using pane, expand the folders and select the report.
- In the Other Pre-defined folder, you can use the drop-down to select either **All Devices** or **Host Devices** while generating a report.
- Step 4** (Optional) In the Report Options pane, you can edit the **Report Name**.
- Step 5** (Optional) Check the **Report is only visible to the Owner** check box to change the attribute of the report. If selected, the report can be viewed only by the specific user and network administrator.
- Step 6** (Optional) Check the **Export to Csv/Excel** check box to export the report in to a Microsoft Excel spreadsheet.
- Step 7** In the **Repeat** radio buttons, if you select:

- **Never** - The report is generated only during the current session.
- **Once** - The report is generated on a specified date and time apart from the current session.
- **Daily** - The report is generated everyday based on the Start and End date at a specified time.
- **Weekly** - The report is generated once a week based on the Start and End date at a specified time.
- **Monthly** - The report is generated once every month based on the Start and End date at a specified time.

Step 8 (Optional) In the **Email Report** radio buttons, if you select:

- **No** - You will not receive an e-mail notification.
- **Link Only** - You will receive only a link to the report in the e-mail notification. You can specify the e-mail address of the recipient along with a desired subject.
- **Contents** - You will receive the report contents in the e-mail notification. You can specify the e-mail address of the recipient along with a desired subject.

Step 9 Click the **Create button** to generate a report based on the specifications.

You see the report results in a new browser window.

Alternatively, you can view the report by choosing **Report > View** and selecting the report name from the report template that you used in the navigation pane



Note The Start Date must be at least five minutes earlier than the End Date.

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
 - A detailed information for the device of the module. The table contains details about the tests failed.
-

Creating SAN User Defined Reports

You can create custom reports from all or any subset of information obtained by Cisco Prime DCNM-SAN. You create a report template by selecting events, performance, and inventory statistics you want in your report and set the desired SAN, fabrics or VSAN to limit the scope of the template. You can generate and schedule a report of your fabric based on this template immediately or at a later time. DCNM Web Client saves each report based on the report template used and the time you generate the report.

Since the Cisco MDS NX-OS Release 5.0, the report template design has changed to resolve the limitations of the earlier versions. With the new design model, you can perform add, delete, and modify functionalities on a single page. You can choose multiple fabrics and VSANs using the new navigation system, which allows you to add new items and categories in the future.

The new design model has three panels:

- **Templates panel** - The Customs panel allows you to add new templates, modify existing templates and delete existing templates.

- **Configuration panel** - The Configuration panel allows you to configure a new template when it is added and modify an existing template. The options in the configuration panel are disabled until you either add a new template or select an existing template. The upper portion of the configuration panel contains many categories that you can choose and configure.
- **User Selection panel** - The User Selection panel displays your configuration options in real-time. While the configuration panel can display information pertaining to one category at a time, the User Selection panel displays all of your selections or configurations.

Follow the steps to create custom reports

-
- Step 1** From the menu bar, choose **Report > Create SAN User Defined**
- You see the Create SAN User Defined window.
- Step 2** In the Templates panel, under the Name column, select **CLICK TO ADD NEW CUSTOM** to edit the Name of the new report.
- In the Configuration Panel:
- Step 3** Click **Scope** to define scope of the report. The default scope will have Data Center, SAN, LAN, and Fabric configurations.
- Step 4** Click **Inventory** and use the checkbox to select the inventory information required in the report. You can also use the drop-down to filter by selecting the Top performance and the timeline required in the report.
- Step 5** Click **Performance** and use the checkbox to select the performance information required in the report.
- Step 6** Click **Health** and use the checkbox to select the health information required in the report.
- Step 7** Click **Save** to save this report template.
- A confirmation message is displayed confirming that the report is saved
- This section also contains:
- [Deleting a Report Template](#)
 - [Modifying a Custom Report Template](#)

Deleting a Report Template

-
- Step 1** In the Template panel, select the report template that you want to delete.
- Step 2** Click the **Trash** icon to delete the report.
- Step 3** In the confirmation pop-up, click **Yes** to delete the template.

Modifying a Custom Report Template

-
- Step 1** From the menu bar, choose **Reports > Create SAN User Defined**.
- You see the Template, Configuration and User Selection panels.
- Step 2** Select a report from the Templates panel.
- You see the current information about this report in the User Selection panel.
- Step 3** Modify the information in the Configuration panel.
- Step 4** Click **Save** to save the report template.
- A confirmation message is displayed confirming that the report is saved.

**Note**

You cannot change the scope for an existing report. You must generate a new report for a new scope.

Viewing Scheduled Jobs Based on a Report Template

- Step 1** From the menu bar, choose **Reports > Jobs**.
- You see the Jobs window displaying details of the reports scheduled for generation along with its status.
- Step 2** Select the checkbox for a specific report and click **Edit Job** icon to edit the report generation settings.
- Step 3** Select the checkbox for a specific report and click the **Delete Job** icon to delete a report.

Configuring Cisco Prime DCNM Web Client

Using Cisco Prime DCNM Web Client, you can periodically start and backup the running configurations of a switch. You can also view backed-up configurations, schedule configuration backups, compare two backed-up configurations and copy a backed-up configuration.

**Note**

You must configure a backup server with Admin/SFTP credentials to create a new backup job.

Beginning with Cisco Prime DCNM Release 6.x, the backup for the LAN configuration are also supported and the backup is skipped for the all the switches where there are no configuration changes.

This section includes the following topics:

- [Viewing a Configuration, page 3-44](#)
- [Comparing Configurations, page 3-45](#)
- [Copying a Configuration, page 3-45](#)
- [Configuring Jobs, page 3-45](#)
- [Storage Media Encryption, page 3-47](#)
- [Configuring Templates, page 3-49](#)
- [Power-On Auto Provisioning \(POAP\), page 3-60](#)
- [Fabric, page 3-73](#)

Viewing a Configuration

- Step 1** From the menu bar, choose **Config >View**.
- You see the Groups, Eligible Switches and their configuration information.
- Step 2** Select a fabric from the Groups list.
- The Groups pane displays the global view with SAN, LAN, and Default LAN groups. Depending upon the value selected in the Groups pane, the eligible switches and their configurations are listed.
- Step 3** From the **Eligible Switch(es)** list, select a switch.

- Step 4** From the **Configuration file** list, select a configuration filename.
 - Step 5** Click **View** to view the configuration file.
 - Step 6** Click **Delete** to delete the configuration file.
 - Step 7** Click **Copy Local File to DB...** to upload the configuration from the local machine to the database.
 - Step 8** Select the **Show All** checkbox to display all the configurations present, irrespective of the options selected in the global Scope pane
-

Comparing Configurations


- Step 1** From the menu bar, select **Config>Compare**.
You see the compare configuration information with the **Compare** and **Differences** tabs.
- Step 2** .From the **Groups list**, select a fabric.
- Step 3** .From the **Eligible Switch(es)** list, select a switch.
- Step 4** (Optional) Click the **Archive**, **Running**, or **Startup** radio button.
- Step 5** Click **Compare**.
- Step 6** Click the **Differences** tab to view differences in configuration based on the specified legend.
- Step 7** Select the difference line and click the bookmark button to **bookmark/toggle** bookmark.
- Step 8** Use the **Next/Previous**, **Next book mark/Previous bookmark** buttons to navigate over the differences blocks.
- Step 9** Click on the **colored overview** to strip to navigate to the difference
- Step 10** Select the **Show All** checkbox to display all the configurations present, irrespective of the options selected in the global Scope pane.

Copying a Configuration

- Step 1** From the menu bar, select **Config > Copy**.
You see the Groups, Eligible Switches and their configuration information.
- Step 2** From the **Groups List**, select a fabric.
- Step 3** From the **Eligible Switch(es)** list, select a switch.
- Step 4** From the **Configuration file** list, select a configuration file name.
- Step 5** Click **Copy** to copy the configuration file.
- Step 6** Select the **Show All** checkbox to display all the configurations present, irrespective of the options selected in the global Scope pane.

Configuring Jobs

You must set the SFTP/TFTP credentials before you configure Jobs. On the DCNM Web Client, navigate to **Admin > SFTP/TFTP Credentials** to set configure.

-
- Step 1** From the menu bar, choose **Config > Jobs**.
You see the scheduled jobs information along with its status.
- Step 2** From the Scope selector, select a single fabric or a single LAN group.
Note You can create jobs for a single fabric or a single LAN group.
- Step 3** Click **Create Job** icon to create a new config archive job.
A backup will be scheduled as defined.
- Step 4** Specify the **Repeat** information, **Start** and **End** date, **Time** and **Comment**.
-  **Note** Cisco Prime DCNM will not archive the configuration of a switch, if it is not modified after the completion of the previous archive job.
-
- Step 5** Select a job and click **Delete Job** to delete a specific job.
Click on the **Status** column to view the job execution details for that particular job.
- Step 6** View Job execution details in the **Job Status History** tab.
-

You can also configure the Cisco Prime DCNM to retain the backup and restore configuration file for a defined time period and the number of job status entries per device. Navigate to **Admin > general > Server properties** on the Cisco Prime DCNM Web Client, and update the **configFile.Days2Keep** and **config.JobStatusPerDevice** fields.

Job Status History

From the menu bar, select **Config > Jobs > Job Status History**. This feature allows you to view details about the jobs archived on the Cisco Prime DCNM.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Table 3-1

Field	Description
Show Filter	Filters list of switches based on the defined value for each column.
Job Name	Displays the system-generated job name.
User	Specifies the persona of the person who created the job.
Group	Specifies fabric or the LAN group under which the job was created.
Device	Specifies the IP Address of the Device.
Server	Specifies the IP Address of the DCNM Server to which the device is associated with.
Execution time	Specifies the time at which the job was last executed.
Status	Specifies the status of the job.
Description	Specifies the description of the status.

Storage Media Encryption

Encrypting storage media in the data center has become a critical issue. Numerous high profile incidents of lost or stolen tape and disk devices have underscored the risk and exposure companies face when sensitive information falls into the wrong hands. To satisfy the most demanding requirements, Cisco MDS 9000 Family Storage Media Encryption (SME) for the Cisco MDS 9000 family switches offers a highly scalable, reliable, and flexible solution that integrates encryption transparently as a fabric service for Fibre Channel SANs.

This section contains the following:

- [Selecting the Key Manager and SSL Settings, page 3-47](#)
- [Viewing SME Clusters, page 3-48](#)
- [Creating a Cluster, page 3-48](#)

Selecting the Key Manager and SSL Settings

Step 1 From the menu bar, select **Config>Provision**.

The Key Manager Settings window is displayed with the following options:

- **None**-No Key Manager selected for SME.
- **Cisco**-Cisco Key Manager selected for SME.
- **RSA**-RSA Key Manager selected for SME



Note

Once you have selected a Key Manager, you will not be able to change it.

Step 2 Select one of the Radio buttons and click **Submit Settings**.

The Key Manager Settings window is displayed.

The KMC SSL Settings pane displays the location where the certificate is stored.

Step 3 If you want to edit the SSL Settings, click **Edit SSL Settings**.

Step 4 Use the drop-down to select the **SME KMC Trust Certificate**.

Step 5 Use the drop-down to select the **SME KMC Server Certificate**.


Step 6 Specify and confirm the **Server Cert Password**.

Step 7 Click **Submit SSL Settings**.


Step 8 In the High Availability Settings pane, click **Edit HA Settings** to specify the **KMC Role of this Server and SME Secondary Server Address**.

Step 9 Click **Submit HA Settings** to confirm.

Viewing SME Clusters

-
- Step 1** From the menu bar, select **Config>Provision** and select **SME** from the ribbon.
You see the SME: Clusters window displaying the **Cluster Name, Status, Fabrics and Key Management Server**.
- Step 2** Click the cluster in the Name column to view its details.
- Step 3** In the Type option, click **Convert to Signature Mode...** to convert the cluster type to Disk Signature.
-  **Note** Once you have chosen to convert the cluster type, you will not be able to change it again
-
- Step 4** In the Confirm Action window, click **Next**.
- Step 5** In the Convert Cluster window, click **Auto** to automatically convert the cluster type to Disk Signature.
-

Creating a Cluster

-
- Step 1** From the menu bar, select **Config>Provision** and select **SME** from the ribbon.
- Step 2** You see the SME: Clusters window displaying the **Cluster Name, Status, Fabrics and Key Management Server**.
- Step 3** Select **Create** to create a new cluster
- Step 4** Select the **Cluster Type**, specify a **Cluster Name** and click **Next**.
- Step 5** Select the **Fabric(s)** and click **Next**.
-  **Note** You can select multiple fabrics by holding the Ctrl key on your keyboard and selecting the fabrics.
-
- Step 6** Select the **SME Interfaces** from the list and click **Next**.
- Step 7** Select the **Security Type** for the cluster and click **Next**.
- Step 8** Specify the **Primary Key Management Server** and the **Secondary Key Management Server** of the cluster. Alternatively, you can also use the drop-down to select the Key Management Servers for the cluster and click **Next**.
- Step 9** Specify the **Transport Settings** for the cluster.
- Step 10** Click **Confirm** to confirm the new cluster setup
-

Configuring Templates

Cisco Prime DCNM allows you to add, edit or delete user-defined templates configured across different Cisco Nexus and Cisco MDS platforms. The following parameters are displayed for each template configured on the Web Client of the Cisco Prime DCNM **Config > Templates**. Config template uses the Java runtime provided Java script environment to perform arithmetic operations, string manipulations in the template syntax.

Field	Description
Name	Displays the name of the configured template.
Description	Displays the description provided while configuring templates.
Platforms	Displays the supported Cisco Nexus platforms compatible with the template.
Tags	Displays the tag assigned for the template and aids to filter templates based on the tags.
Template Type	Displays the type of the template.
Published	Specifies if the template is published or not.
Modified Time	Displays the date and time when the template was last modified, in the format YYYY-MM-DD HH:MM:SS.

Additionally, from the menu bar, select **Config > Delivery > Templates** and you can also:

- Click the **Launch Job Creation** icon to configure and schedule jobs for individual templates. For more information, see [Configuring Template Job, page 3-58](#).
- Click the **Show Filter** icon to filter the templates based on the headers.
- Click the **Print** icon to print the list of templates.
- Click the **Export to Excel** icon to export the list of template to a Microsoft Excel spreadsheet

This section contains the following:

- [Template Structure, page 3-50](#)
- [Adding a Template, page 3-57](#)
- [Configuring Template Job, page 3-58](#)
- [Modifying a Template, page 3-59](#)
- [Importing a Template, page 3-59](#)
- [Exporting a Template, page 3-60](#)
- [Deleting a Template, page 3-60](#)

Template Structure

The configuration template content mainly consists of four parts. You can click on the Help icon next to the Template Content window for information about editing the content of the template. Click on the Help icon next to the Template Content window for information about editing the content of the template.

This section contains the following:

- [Template Format](#)
- [Template Variables](#)
- [Variable meta property](#)
- [Variable Annotation](#)
- [Templates Content](#)
- [Advanced Features](#)

Template Format

This section describes the basic information of the template. The possible fields are as detailed in the table below.

Property Name	Description	Valid Values	Optional?
name	The name of the template	Text	No
description	Brief description about the template	Text	Yes
userDefined	Indicates whether the user created the template. Value is 'true' if user created.	"true" or "false"	Yes
supportedPlatforms	List of device platforms supports this config template. Specify 'All' to support all platforms.	"All" or combination of C6500, N1010, N1110, N1K, N3K, N4K, N7K, N6K, N5K, N5500, MDS, UCS list separated by comma.	No
configType	Specifies the Template used for	"CLI" or "POAP:"	Yes
published	Used to Mark the template as read only and avoids changes to it.	"true" or "false"	Yes
timestamp	Shows the template modified time	Modified date and time in the format YYYY-MM-DD HH:MM:SS	Yes

Example: Template Properties

```
##template properties
name =FCOE template;
description = This file specifies the template configuration for FCOE;
userDefined= false;
supportedPlatforms = N7K, N6K, N5K, N5500, MDS;
templateType = CLI;
published = false;
```



```
timestamp = 2013-05-16 07:11:37;
##
```

Template Variables

This section contains declared variables, the data type, default values, and valid values conditions for the parameters that are used in the template. These declared variables are used for value substitution in the template content section during the dynamic command generation process. Also these variables are used in decision making and in iteration blocks in the template content section. Variables have predefined data types. You can also add a description about the variable. The following table describes the syntax and usage for the available datatypes.

Variable Type	Valid Value	Iterative?
string	Free text Example: Description for the variable	No
boolean	true/false	No
enum	Example: running-config, startup-config	No
float	Floating number format	No
Integer	Any number	No
ipAddress	IPv4 OR IPv6 address	No
ipV4Address	IPv4 address	No
ipV6Address	IPv6 address	No
ipV4AddressWithSubnet	Example: 192.168.1.1/24	No
macAddress	14 or 17 character length MAC address format	No
interface	Format: <if type><slot>[/<sub slot>]/<port> Example: eth1/1, fa10/1/2 etc.	No
integerRange	Contiguous numbers separated by “-” Discrete numbers separated by “,” Example: 1-10,15,18,20	Yes
floatRange	Example: 10.1,50.01	Yes
ipV4AddressRange	Example: 172.22.31.97 - 172.22.31.99, 172.22.31.105 - 172.22.31.109	Yes
interfaceRange	Example: eth10/1/20-25, eth11/1-5	Yes
string[]	Example: {a,b,c,str1,str2}	Yes
ipAddress[]	Example: {192.168.1.1, 192.168.1.2, 10.1.1.1}	Yes
wwn (Available only in the Web Client)	Example: 20:01:00:08:02:11:05:03	No

```
Example: Template Variables
##template variables
integer VSAN_ID;
string SLOT_NUMBER;
```



```
integerRange PORT_RANGE;
integer VFC_PREFIX;
##
```

Variable meta property

Each variable defined in the template variable section has a set of meta properties. The meta properties are mainly the validation rules defined for the variable.

The following table describes the various meta properties applicable for the available variable types.

Variable Type	Description	Variable meta property											
		defaultValue	validValues	decimalLength	min	max	minSlot	maxSlot	minPort	maxPort	minLength	maxLength	regularExpr
string	literal string	ü									ü	ü	ü
boolean	A boolean value. Example: true	ü											
enum			ü										
float	signed real number. Example: 75.56, -8.5	ü	ü	ü	ü	ü							
integer	signed number Example: 50, -75	ü	ü		ü	ü							
ipAddress	IP address in IPv4 or IPv6 format												
ipV4Address	IPv4 address												
ipV6Address	IPv6 address												
ipV4AddressWithSubnet													
macAddress	MAC address												
interface	specifies interface/port Example: Ethernet 5/10	ü	ü				ü	ü	ü	ü			
integerRange	Range of signed numbers Example: 50-65	ü	ü		ü	ü							
floatRange	range of signed real numbers Example: 50.5 - 54.75	ü	ü	ü	ü	ü							
ipV4AddressRange													
interfaceRange		ü	ü				ü	ü	ü	ü			

string[]	string literals separated by a comma (,) Example: {string1, string2}	✓											
ipAddress[]	List of IP addresses separated by a comma (,)	✓											
wwn	WWN address												
struct	set of parameters bundled under a single variable												

Example: Meta Property usage
##template variables

```
integer VLAN_ID {
  min = 100;
  max= 200;
};
string USER_NAME {
  defaultValue = admin123;
  minLength = 5;
};
##
```

Variable Annotation

You can configure the variable properties marking the variables using annotations.



Note

Variable Annotations are available for POAP only. However, the annotations do not impact on the template type 'CLI'.

The following annotations can be used in the template variable section.

Annotation Key	Valid Values
DisplayName	Text Note You must enclose the text with quotes, if there is space.
Description	Text
IsManagementIP	"True" or "False" Note This annotation must be marked only for variable "ipAddress".
IsDeviceID	"True" or "False"
IsInternal	"True" or "False"
IsMandatory	"True" or "False"
UsePool	"True" or "False"
Username	Text

Annotation Key	Valid Values
Password	Text
DataDepend	Text

Example: Variable Annotation

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description"
IsManagementIP=true)
ipAddress hostAddress;
##
```

Templates Content

This section includes the configuration commands and any parameters that you want to include in the template. These commands can include the variables declared in the template variables section. During the command generation process the variable values are substituted appropriately in the template content.



Note

You must specify the commands that you include as if you were entering them in the global configuration command mode on any device. You must consider the command mode when you include commands.

Template content is governed by the usage of variables.

- **Scalar variables**—does not take a range or array of values which cannot be used for iteration (In the variable types table those marked iterate-able as 'No'). Scalar variables must be defined inside the template content.

Syntax: \$\$<variable name>\$\$
Example: \$\$USER_NAME\$\$

- **Iterative variables**—used for block iteration. These loop variable must be accessed as shown below inside the iteration block.

Syntax:@<loop variable>
Example:
foreach val in \$\$INTEGER_RANGE_VALUE\$\$ {
@val
}

- **Scalar Structure Variable**—Structure member variables can be accessed inside the template content.

Syntax: \$\$<structure instance name>.<member variable name>\$\$
Example: \$\$myInterface.inf_name\$\$

- **Array Structure Variable**—Structure member variables can be accessed inside the template content

Syntax: \$\$<structure instance name>.<member variable name>\$\$
Example: \$\$myInterface.inf_name\$\$

In addition to the template variables, you can use the conditional and iterative command generation using the following statements:

- **if-else if-else Statement**—makes a logical decision in inclusion/exclusion of set of configuration command based on the value assigned for the variable in it.

Syntax: if(<operand 1> <logical operator> <operand 2>){
command1 ..


```

command2..
..
} else if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
} else
{
Command5 ..
Command6..
..
}
Example: if-else if-else statement
    if($$USER_NAME$$ == 'admin'){
        Interface2/10
        no shut
    } else {
        Interface2/10
        shut
    }

```

- **foreach Statement**—used for iterating a block of commands. The iteration is performed based on the assigned loop variable value.

```

Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}

```

```

Example: foreach Statement
    foreach ports in $$MY_INF_RANGE$$ {
        interface @ports
        no shut
    }

```

- **Optional parameters**—By default all parameters are mandatory. To make a parameter optional, you must annotate the parameter.

In the variable section, include the following command:

@(IsMandatory=false)

Integer frequency;

In the template content section, a command can be excluded or included without using "if" condition check, by assigning a value to the parameter. The optional command can be framed as below:

probe icmp [frequency *frequency-value*] [timeout *seconds*] [retry-count *retry-count-value*]

Advanced Features

- **Assignment Operation**

Config template supports assignment of variable values inside the template content section. The values are validated for the declared data type of the variable. If there is a mismatch, the value is not assigned.

Assignment operation can be used under the following guidelines:

- The operator on the left hand side must be any of the template parameter or a for loop parameter.
- The operator on the right hand side values can be any of value from template parameter, for loop parameter, literal string values surrounded by quotes or simple string values.

If a statement does not follow these guidelines, the does not suit this format would not be considered as assignment operation. It is substituted during command generation like other normal lines.

Example: Template with assignment operation

```
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
@(internal=true)
integer vlanName;
##
##template content
foreach vlanID in $$vlan_range$$ {
vlan @vlanID
$$vlanName$$=@vlanID
name myvlan$$vlanName$$
}
##
```

- Evaluate methods

Config template uses the Java runtime provided Java script environment to perform arithmetic operations (such as ADD, SUBTRACT, and so on), string manipulations, and so on.

Locate the javascript file in the template repository path. This file contains primary set of arithmetic, string functions. You can also add custom Javascript methods.

These methods can be called from config template content section in below format:

Example1:

```
$$somevar$$ = evalscript(add, 100, $$anothervar$$)
```

Also the evalscript can be called inside if conditions as below:

```
if($$range$$ > evalscript(sum, $$vlan_id$$, -10)){
do something...
}
```

You can call a method which is in the backend of the Java script file.

- Dynamic decision

Config templates provides a special internal variable “LAST_CMD_RESPONSE”. This variable stores the last command response from the device during the execution of the command. This can be used in the config template content to make dynamic decisions to deliver the commands based on the device condition.

An example use case is create a VLAN, if it does not exist on the device.

Example: Create VLAN

```
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains "not found"){
vlan $$vlan_id$$
}
##
```

This special implicit variable can be used only in the “IF” blocks.

- Template referencing

You can have a base template with all the variables defined. This base template can be imported to multiple templates. The base template content is substituted in the appropriate place of the extending template. The imported template parameters and the contents can be accessed inside the extending template.

Example: Template Referencing

Base template:

```
##template properties
name =a vlan base;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
timestamp = 2015-07-14 16:07:52;
imports = ;
##
##template variables
integer vlan_id;
##
##template content
vlan $$vlan_id$$
##
```

Derived Template:

```
##template properties
name =a vlan extended;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
timestamp = 2015-07-14 16:07:52;
imports = a vlan base,template2;
##
##template variables
interface vlanInterface;
##
##template content
<substitute a vlan base>
interface $$vlanInterface$$
<substitute a vlan base>

##
```

When you launch the extended template, the parameter inputs for the base template are also obtained. Additionally, the substituted content is used for complete CLI command generation.

Adding a Template

You can add user-defined templates and schedule jobs.

<<add topic ID: admin_template_add>>

-
- Step 1** From the menu bar, select **Config > Delivery > Templates**.
You see the name of the template along with its description, Platforms and Tags.
 - Step 2** Click the **Add** icon to add a new template.
 - Step 3** Specify a **Template Name**, **Template Description** and a **Tags** for the new template.
 - Step 4** From the **Imports** drop-down, select the base template.

The base template content is displayed in the Template content window. The base template provide few parameters and template content provides certain CLI commands. This can be imported in to another template and the base template content is substituted in the appropriate place of the extending template. When the user launches the extended template, the parameter inputs for the base template are also obtained. Additionally, the substituted content is used for complete CLI command generation.

Step 5 Select the **Supported Platforms** that the template must support.

Step 6 Click in the Template Content window to edit the template syntax.

For information about the structure of the Configuration Template, see [“Template Structure”](#).

Step 7 Select **POAP** to make this template available when you power on the application.



Note The template will be considered as a CLI template if POAP is not selected.

Step 8 Select **Published** to make the template read-only. You cannot edit a published template.

Step 9 Click **Validate Template Syntax** to validate the template values.

Step 10 Click **Save** to save the template.

Step 11 Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

Configuring Template Job

<<need to add TopicID: config_templates_job_wizard

You can configure and schedule jobs for individual templates from the **Config > Delivery > Templates** page.

Step 1 From the menu bar, select **Config > Templates**.

You see the name of the template along with its description, Platforms and Tags.

Step 2 Use the checkbox to select a template from the list.

Step 3 Click the **Launch Job Creation Wizard** icon and click **Next**.

Step 4 Use the drop-down to select the **Device Scope**. The devices configured under the selected Device Scope are displayed.

Step 5 Use the arrows to move the devices to the right column for job creation and click **Next**.

Step 6 Specify the **VSAN_ID**, **VLAN_ID**, **ETH_SLOT_NUMBER**, **VFC_SLOT_NUMBER**, **SWITCH_PORT_MODE**, **ETH_PORT_RANGE** and **ALLOWED_VLANS** values.

Step 7 Use the checkbox **Edit variables per device** to edit the variables for specific devices and click **Next**.

Step 8 If you have selected multiple devices, use the drop-down to select a specific device and preview its configuration. Click **Back** to edit the configuration or click **Next**.

Step 9 Specify a **Job Description** and enter the **Device Credentials**.

Step 10 Use the radio button to select **Deliver Instantly** or **Choose time to deliver**. If you select Choose time to deliver, specify the date and time for the job delivery.

Step 11 Use the checkbox to select **Copy Run to Start**.

Step 12 If you want to configure additional Transaction and Delivery options, use the checkbox to select **Show more options**.

- Step 13** Under **Transaction Options (Optional)**, if you have a device with rollback feature support, select **Enable Rollback** checkbox and select the appropriate radio button.
- Step 14** Under **Delivery Options (Optional)**, specify the **Timeout in seconds** and use the radio button to select the **Delivery Order**.
- Step 15** Click **Finish** to create the job.
- A confirmation message is displayed that the job has been successfully created.
-

Modifying a Template

You can edit the user-defined templates. However, the pre-defined templates cannot be edited. You cannot edit a template if it is already Published.

-
- Step 1** From the menu bar, select **Config > Templates**.
- You see the name of the template along with its description, Platforms and Tags.
- Step 2** Select a template from the list and click the **Modify/View template** icon
- Step 3** Edit the **Template Description, Tags**.
- The edited Template content is displayed in the right-hand pane.
- Step 4** From the **Imports** drop-down, select the base template.
- The base template content is displayed in the Template content window. You can edit the template content based on your requirement in the Template Content window. Click on the Help icon next to the Template Content window for information about editing the content of the template.
- Step 5** Edit the Supported Platforms for the template.
- Step 6** Click **Validate Template Syntax** to validate the template values.
- Step 7** Click **Save** to save the template.
- Step 8** Click **Save and Exit** to save the configuration and go back to the configuring templates screen.
-

Importing a Template

-
- Step 1** From the menu bar, select **Config > Templates** and click on the **Import template** icon.
- Step 2** Browse and select the template saved on your computer.
- Step 3** You can edit the template parameters, if required. For information, see [Modifying a Template, page 3-59](#).
- Step 4** Click **Validate Template Syntax** to validate the template.
- Step 5** Click **Save** to save the template or **Save and Exit** to save the template and exit.
-

Exporting a Template

-
- Step 1** From the menu bar, select **Config > Templates**.
 - Step 2** Use the checkbox to select a template(s) and click the **Export template** icon.
 - Step 3** Specify a name for the template and select a location to save the template on your computer.
-

Deleting a Template

You can delete the user-defined templates. However, you cannot delete the pre-defined templates.

-
- Step 1** From the menu bar, select **Config > Templates**.
 - Step 2** Use the checkbox to select a template(s) and click the **Remove template** icon.
 - Step 3** In the confirmation dialog box, click **Yes** to delete the template.
-

Configuring Jobs

-
- Step 1** From the menu bar, select **Config > Delivery > Jobs**.
The jobs are listed along with the Job ID, description and status.
 - Step 2** Click the **Show Filter** icon to filter the jobs by Job ID, Description, Devices and Status. In the Status column, use the drop-down to select the job status.
 - Step 3** Select a job and click the **Delete** icon to delete the job.
-

Power-On Auto Provisioning (POAP)

POAP automates the process of upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

When a Cisco Nexus switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode, locates a DHCP server and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. It also obtains the URL of an SCP server and downloads a configuration script that is run on the switch to download and install the appropriate software image and configuration file.



Note

When you move the mouse cursor over an error identified in a specific parameter in any window, it will display the exact error message before you move to the next screen.

There are five main steps to configure a POAP device:

-
- Step 1** DHCP Scope Creation
- Step 2** Add the boot, startup, image and server information.
- Step 3** Startup configuration creation
- Step 4** Cable plan.
- Step 5** Script and files (license) attachment

POAP Launchpad



Note

These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

The POAP launchpad contains the following configuration steps:

- [DHCP Scope](#) - Create and manage scopes for POAP creation.
- [Images and Configuration](#) - Set a server for images and configuration files.
- [POAP Definitions](#) - Generate from template or upload existing configuration.
- [Cable Plan](#) - Create, Publish and Deploy Cable Plans.

DHCP Scope

DHCP scope is a well-defined term in DHCP arena. It is used to define a policy for giving out IP addresses and other options to host on a specific IP subnet. In DCNM, we use the DHCP scope to distribute IPv4 address, PYTHON bootscript, (or other supported protocol + access credential + server) which stores the bootscript.

From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.

The columns in table [Table 3-3](#) are displayed

Table 3-3 :DHCP Scope

DHCP Scope	Comment
Scope Name	The DHCP scope name must be unique amongst the switch scopes. This name is not used by ISC DHCP but used to identify the scope.
Scope Subnet	The IPv4 subnet used by the DHCP servers.
IP Address Range	The IP address ranges allocated to the POAP switches. Multiple IP addresses can be used, separated by comma.
Lease Time	Maximum lease time for the DHCP lease.
Default Gateway	The default gateway for the DHCP scope. You must enter a valid IP as the default gateway.
Domain Name Servers	The domain name server for the DHCP scope.

DHCP Scope	Comment
Bootscript Name	The Python Bootup script.
Bootscript Server	The server that holds the bootscript.

- [Adding a DHCP Scope, page 3-62](#)
- [Editing an existing DHCP Scope, page 3-62](#)
- [Deleting a DHCP Scope, page 3-62](#)

Adding a DHCP Scope

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.
- Step 2** Click **Add scope** icon.
- Step 3** In the Add DHCP Scope window, specify values in the fields according to the information in [Table 3-3](#).
- Step 4** Click **Add**.

Editing an existing DHCP Scope



Note

Once the DCNM is accessed for the first time, you must edit the default scope named 'enhanced_fab_mgmt' and add free IP address ranges.

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.
- Step 2** Use the checkbox to select the DHCP scope.
- Step 3** Click **Edit scope** icon.
- Step 4** In the Edit DHCP Scope window, edit the DHCP scopes.
- Step 5** Click **Apply** to save the changes.

Deleting a DHCP Scope

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>DHCP Scope**.
- Step 2** Use the checkbox to select the DHCP scope.
- Step 3** Click **Delete scope** icon.
- Step 4** In the delete notification, click **Yes** to delete the DHCP scope.



Note

You may click the **Refresh** icon to refresh the DHCP Scopes list.

Images and Configuration

This feature enables you to specify the servers & credential used to access the device images and the uploaded or DCNM generated/published device configuration. The server containing the images could be different from the one containing the configurations. If the same server contains both images and configurations, you must provide the server IP address and credentials twice for each server, if the directories holding images and configuration files are different. By default, DCNM server will be the default image and configuration server.

Copy Kickstart and system images into the repository prior to defining POAP definitions for devices. If the DCNM is the image repository, copy the image files into `/var/lib/dcnm/` directory.

- [Add Image or Configuration Server URL, page 3-63](#)
- [Editing an Image or Configuration Server URL, page 3-63](#)
- [Deleting an Image or Configuration Server URL, page 3-63](#)

Add Image or Configuration Server URL

-
- | | |
|---------------|--|
| Step 1 | From the menu bar, select Config>Power-On Auto Provisioning (POAP)>Image and Config Servers . |
| Step 2 | Click the Add icon. |
| Step 3 | In the Add Image or Configuration Servers URL window, specify a Name for the image. |
| Step 4 | Enter Hostname/Ipaddress and Path to download or upload files. |
| Step 5 | Specify the Username and Password . |
| Step 6 | Click OK to save. |

Editing an Image or Configuration Server URL

-
- | | |
|---------------|--|
| Step 1 | From the menu bar, select Config>Power-On Auto Provisioning (POAP)>Image and Config Servers . |
| Step 2 | Select an existing Image and Configuration Server from the list, and Click the Edit icon. |
| Step 3 | In the Edit Image or Configuration Servers URL window, edit the required fields. |
| Step 4 | Click OK to save. |

Deleting an Image or Configuration Server URL

-
- | | |
|---------------|--|
| Step 1 | From the menu bar, select Config>Power-On Auto Provisioning (POAP)>Image and Config Servers . |
| Step 2 | Select an existing Image and Configuration Server from the list, and Click the Delete icon. |
| Step 3 | In the delete notification, click Yes to delete the image and configuration server. |



Note	The default SCP Repository cannot be deleted.
-------------	---

POAP Templates

Templates can be created or imported into the template builder of DCNM. There are some predefined Fabric specific POAP templates bundled with DCNM. The template builder can be invoked from the GUI, Config->Delivery -> Templates. The templates dedicated to POAP will be used to generate many different POAP device configurations

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

- Use the **Show Filter** icon to filter the templates.
- Use the **Print** icon to print the list of templates and their details.
- Use the **Export** icon to export the list of templates to a Microsoft Excel spreadsheet.

This section contains the following:

- [Add POAP template](#)
- [Editing a Template](#)
- [Cloning a Template](#)
- [Importing a Template](#)
- [Exporting a Template](#)
- [Deleting a Template](#)

Add POAP template

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.
 - Step 2** In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.
 - Step 3** Click **Add template** icon.
 - Step 4** Specify the **Template Name**, **Template Description** and **Tags**.
 - Step 5** Use the checkbox to specify the **Supported Platforms**.
 - Step 6** Select the **POAP** checkbox or else by default, the DCNM will consider it as a CLI template.
 - Step 7** Select the **Published** checkbox if you want the template to have 'Read Only' access.
 - Step 8** In the Template Content pane, you can specify the content of the template. For help on creating the template content, click the **Help** icon next to the Template Content header. For information about POAP template annotations see the [POAP Template Annotation](#) section.
 - Step 9** Click **Validate Template Syntax** to validate syntax errors.
 - Step 10** Click **Save** to save the template.
 - Step 11** Click **Save and Exit** to save the template and exit the window.
 - Step 12** Click **Cancel** to discard the template.

Editing a Template

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.
 - Step 2** In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.

- Step 3** Select a template from the list and click **Modify/View template** icon.
- Step 4** Edit the template content and click **Save** to save the template or **Save and Exit** to save and exit the screen.

Cloning a Template

- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.
- Step 2** In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.
- Step 3** Select a template from the list and click **Modify/View template** icon.
- Step 4** Edit the template and click **Save** to save the template or **Save and Exit** to save and exit the screen.

Importing a Template

- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.
- Step 2** In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.
- Step 3** Select a template from the list and click **Import template** icon.
- Step 4** Select the template file and upload.

Exporting a Template

- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.
- Step 2** In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.
- Step 3** Select a template from the list and click **Export template** icon.
- Step 4** Select a location for the file download.

Deleting a Template



Note Only user-defined templates can be deleted.

- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>POAP Definitions**.
- Step 2** In the Configuration Steps, click the **template** hyperlink in the POAP Definitions section.
- Step 3** Select a template from the list and click **Remove template** icon.
- Step 4** Click **Yes** to confirm.

POAP Template Annotation

Annotation is used to add semantic, validation logic and description to the template variable.

The Annotation for a given template variable is required to precede the given template variable. Only one annotation statement is required for each template variable. When a template variable has an associated annotation statement, the template variable has to be declared on a single line. Multiple variables cannot be declared under the same annotation statement.

Format of an annotation statement is as follows:

```
@(<key1>=<value1>,<key2>=<value2>, ..., <keyN>=<valueN>)
```


Note

- Each annotation statement is composed of one or more key-values pair.
- The value can be true, false, or a string.
- If the value is a string, it should be double quoted.

The following is a sample template variable, “hostname”, with annotation statement with the keys “DisplayName”, and “Description”:

```
@(DisplayName="Host Name", Description = "Description of the host")
```

String hostname;

The table displays the supported keys in the annotation statement:

Table 3-4 Annotation Keys

Key Name	Default Value	Description
DisplayName	Empty String	The value is displayed as a variable label in the template form GUI, on POAP definition screen.
Description	Empty String	Displays the description next or below the template variable field in the template form GUI.
IsManagement	false	The associated variable is of IP Address type. This will be used as the management IP address. DCNM used this IP address to manage the devices.
IsMultiplicity	false	If true, this single value can take multiple values. For example; when it is used with IsManagement annotation, it allows you to type in multiple IP addresses and assign each IP address to a device.
IsSwitchName	false	The associated variable value is used as the device host name.
IsMandatory	true	It marks the field as mandatory if the value is set as 'true'.
UseDNSReverseLookup	false	This annotation compliments the IsSwitchName annotation. Once they are associated with a variable. The variable is populated with the reverse DNS name, if available during the creation time of the corresponding POAP definition record.
IsFabricPort	false	The associated variable value contains a list of the ports used as fabric ports. The variable value will be used by the cable plan generation from POAP

Key Name	Default Value	Description
IsHostPort	false	Trunk ports connected to host/servers.
IsVPCDomainID	false	Used as the VPC Domain ID.
IsVPCPeerLinkSrc	false	Used as the VPC IPv4 source address.
IsVPCPeerLinkDst	false	Used as the VPC IPv4 peer address.
IsVPCPeerLinkPortChannel	false	Used for VPC port channel.
IsVPCLinkPort	false	Used for VPC interface.
IsVPC	false	Used as a VPC record.
IsVPCID	false	Individual VPC ID.
IsVPCPortChannel	false	Individual VPC port channel.
IsVPCPort	false	VPC Interface.

POAP Definitions

The POAP switch definition has two major functions:

- Monitoring switch POAP process
- Managing POAP switch configuration

You must copy the Cisco Prime DCNM license files to the `/var/lib/dcnm/license` directory to install as part of the POAP process.

You must also copy the device licenses to the `/var/lib/dcnm/licenses` folder.



Note

The device licenses refers to the devices monitored by the Cisco Prime DCNM.

The following fields and icons are listed at the menu bar of the window to customize the view of the information in the window:

Fields and Icons	Description
Serial Number	Specifies the serial number for the switch.
Switch ID	Specifies the ID defined for the switch
Management IP	Specifies the Management IP for the switch.
Status	
Switch Status	Indicates if the switch is published or not.
Publish Status	Indicates if this POAP template has been published successfully to the TFTP site.
Bootscrip Status	Indicates the Bootscrip execution state when the device executed POAP. For details, view the “Boot Log” file.

Fields and Icons	Description
Diff State	<p>Specifies if the configuration defined in POAP is different from the running configuration on the device. If a difference is detected, the user has an option to make changes to the device configuration, thereby ensuring that the configuration on the device is in sync with the POAP configuration.¹ The different states are:</p> <ul style="list-style-type: none"> • NA—Specifies that no POAP definition is configured on DCNM for the particular device; therefore, no difference computation can be made. • Diff Detected—Specifies that few configuration differences are detected between POAP definition in DCNM and the running configuration on the switch. You can review the difference statements and choose the commands to deploy to the device, and synchronize the running configuration with the POAP definition. • No Diff Detected—Specifies that there was no configuration diff perceived between POAP definition and the running configuration on the switch. • Error—Specifies that an error has occurred during diff computation. Refer to the logs to troubleshoot the issue.
Model	Specifies the model of the switch.
Template/Config File Name	<p>Specifies the template used for creating the POAP definition.</p> <p>Fabric and IPFabric POAP templates are available.</p>
Bootscrip Last Updated Time	Specifies the last updated time for bootscrip.
Last Published	Specifies the last published time for the POAP definition.
Last Saved	Specifies the last saved time for the POAP definition.
POAP Creation Time	Specifies the time when the POAP definition was created.
System Image	Specifies the System Image used while creating the POAP definition.
Kickstart Image	Specifies the kickstart image used the PAOP definition
Icons	
Add	Allows you to add a POAP definition. For more information, see Creating a POAP definition .
Edit	Allows you to edit a POAP definition. For more information, see Editing a POAP Definition .
Delete	Allows you to delete a POAP definition. For more information, see Deleting POAP Definitions .
Publish	Allows you to publish a POAP definition. For more information, see Publishing POAP definitions .
Write Erase and Reload	Allows you to reboot and reload a POAP definition. For more information, see Write, Erase and Reload the POAP Switch Definition .
Change Image	Allows you to change the image for the defined POAP definition. For more information, see Change Image .
Boot Log	Display the list and view log files from the device bootflash.

Fields and Icons	Description
Refresh Switch	Refreshes the list of switches.
Show Filter	Filters list of switches based on the defined value for each column.
Print	Prints the list of devices and their details.
Export	Exports the list of devices and their details to a Microsoft Excel spreadsheet.
Select Columns	Displays the columns to be displayed. You can choose to show/hide a column.

1. You can discover the device manually also. Navigate to **Admin < Data Sources** on the Web Client to initiate a “Diff state” comparison for each device.

**Note**

Each annotation statement is composed of one or more key-values pair. The value can be true, false or a string. If the value is a string, it should be mentioned in double-quotes.

This section contains the following:

- [Creating a POAP definition](#)
- [Uploading a POAP Definition](#)
- [Editing a POAP Definition](#)
- [Deleting POAP Definitions](#)
- [Publishing POAP definitions](#)
- [Write, Erase and Reload the POAP Switch Definition](#)

Creating a POAP definition

- Step 1** From the menu bar, select **Config > Power-On Auto Provisioning (POAP)>POAP Definitions**.
- Step 2** Click **Add** to add a new POAP definition.
- Step 3** Use the radio button and select **Generate Definition** to generate POAP definition from a template, and click **Next** to specify the switch details.
- Step 4** Enter the serial number of switches separated by comma. Alternatively, you can click the **Import from CSV File** button to import the list of switches.
- Step 5** Use the drop-down to select the Switch Type.
- Step 6** Use the drop-down to select the Image Server.
- Step 7** Use the drop-down to select the System Image and Kickstart image.
- Step 8** Use the drop-down to select the Config Server, and specify the Switch User Name and Password.
- Step 9** Use the drop-down in the Add Switches to Group to add the POAP devices to a specific group, and specify the Switch User Name and Switch Password.
- Step 10** Click **Next** to Select the Switch Config Template.
- Step 11** Use the drop-down to select the Template and click **View** to specify the Template Parameters.
- Step 12** Enter Template Parameters.

- Step 13** Use the drop-down to select the Settings File. If the settings file is unavailable, click **Save Parameter as New Settings File** button to specify a name for the settings file, select the variables and click **Save**. The new settings file will now be listed in the Settings File drop-down.
- Step 14** Click **View** to view the settings file parameters.
- Step 15** Click **Manage** to modify the settings file parameters.
- Step 16** Click **Next** to generate the configuration.

Uploading a POAP Definition

- Step 1** From the menu bar, select **Config > Power-On Auto Provisioning (POAP) > POAP Definitions**.
- Step 2** Use the radio button and select **Upload Startup Config** to upload startup config to the POAP repository Server, and click **Next** to Enter the switch details.
- Step 3** Enter the serial number of switches separated by comma.
- Step 4** Use the drop-down to select the **Switch Type**.
- Step 5** Use the drop-down to select the **Image Server**.
- Step 6** Use the drop-down in the **Add Switches to Group** to add the POAP devices to a specific group.
- Step 7** Use the drop-down to select the **System Image** and **Kickstart Image**.
- Step 8** Use the drop-down to select the **Config Server**, and specify the Switch User Name and Password.
- Step 9** Click **Browse** to select the upload configuration file.
- Step 10** Click **Save** to save the uploaded configuration file or **Publish** to publish the POAP definition.

Editing a POAP Definition

- Step 1** From the menu bar, select **Config > Power-On Auto Provisioning (POAP) > Select the POAP switch definitions from the list** and click the **Edit** icon.
- Step 2** Follow the steps listed in [Creating a POAP definition](#) and [Uploading a POAP Definition](#) sections.



Note

You can select multiple POAP definitions with similar parameters to edit POAP definition.

Deleting POAP Definitions

- Step 1** From the menu bar, select **Config > Power-On Auto Provisioning (POAP) > Select the POAP switch definitions from the list** and Click the **Delete** icon.
- Step 2** Click **Yes** to delete the switch definitions.
A prompt appears to delete the device from the data source.
- Step 3** Click **OK** to confirm to delete the device from the data source also.

Publishing POAP definitions

-
- Step 1** From the menu bar, select **Config > Power-On Auto Provisioning (POAP)** > Select the POAP switch definitions from the list and Click the **Publish** icon.
- Step 2** Click **Yes** to publish the switch definitions.

Write, Erase and Reload the POAP Switch Definition

-
- Step 1** From the menu bar, select **Config > Power-On Auto Provisioning (POAP)** > Select the POAP switch definitions from the list.
- Step 2** Click the **Write, Erase and Reload** icon.
- Step 3** Click **Continue** to reboot and reload the switch definitions.

Change Image

-
- Step 1** From the menu bar, select **Config > Power-On Auto Provisioning (POAP)** > Select the POAP switch definitions from the list.
- Step 2** Select the switch for which you need to change the image. Click **Change Image**.

**Note**

You can select multiple POAP definitions with similar parameters to change the image for booting the device.

The Multi Device Image Change screen appears.

- Step 3** From the **Image Server** dropdown list, select the server where the new image is stored.
- Step 4** From the **System Image** dropdown list, select the new system image.
- Step 5** From the **Kickstart Image** dropdown list, select the new image which will replace the old image.
- Step 6** Click **Publish** to apply and change the image.

Cable Plan

The Cable plan configuration screen has the following options:

- [Create a Cable Plan](#)
- [Viewing an Existing Cable Plan Deployment](#)
- [Deleting a Cable Plan](#)
- [Deploying a Cable Plan](#)
- [Revoking a Cable Plan](#)
- [Viewing a Deployed Cable Plan from Device](#)

**Note**

If you are generating POAP definitions from the uploaded configuration, then generation of cable plan using the option of “Generate Cable Plan from POAP definition” will not work as the POAP definitions generated from the uploaded configuration will not have the required meta-data to generate the cable plans. You must select either “Capture from Existing Deployment” or “Import Cable plan file” to create a cable plan.

Create a Cable Plan

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.
- Step 2** Click **Create Cable Plan**.
- In the Create Cable Plan pop-up, use the radio button to select the options.
- Step 3** If you select:
- a. **Generate Cable Plan from POAP definition:** You can use the switches defined in the POAP flow and produce a port-to-port cable plan to be used when wiring the physical devices.
 - b. **Capture from existing deployment:** You can ascertain the Inter-Switch Links between existing switches managed by DCNM and “lock down” the cable plan based on the existing wiring.
 - c. **Import Cable Plan File:** You decide how to wire the switches (or how they are already wired) and select an XML file for import into DCNM.

Viewing an Existing Cable Plan Deployment

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.
- Step 2** Click **View**.
- Step 3** In the Cable Plan - Existing_Deployment window, you can view the existing cable plan deployments.
- Step 4** You can use the Table View and XML View icons to change the view of the cable plan deployments table.

Deleting a Cable Plan

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.
- Step 2** Click **Delete from DCNM**.
- Step 3** Click **Yes** to confirm deletion.

Deploying a Cable Plan

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.
- Step 2** In the Switches table, use the checkbox to select cable plan(s) and click **Deploy a Cable Plan**.
- Step 3** Click **Yes** to confirm deployment.

Revoking a Cable Plan

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.
- Step 2** In the Switches table, use the checkbox to select cable plan(s) and click **Revoke a Cable Plan**.
- Step 3** Click **Yes** to confirm.

Viewing a Deployed Cable Plan from Device

-
- Step 1** From the menu bar, select **Config>Power-On Auto Provisioning (POAP)>Cable Plan**.
- Step 2** In the Switches table, click **In Sync** or **Out of Sync** hyperlink in the cable plan status column.
- Step 3** You can use the Table View and XML View icons to change the view of the cable plan table.

Fabric



Note

These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

This feature automates network provisioning and provides a new layer of automation integration in which the data center fabric-switching infrastructure is automatically provisioned for the physical or virtual workload that is being instantiated.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Table 3-5

Field/Icons	Description
Organizations Section	
Organization/Partition Name	Specifies the organization or the partition name.
Description	Specifies the description for the organization.
Partition ID	Specifies the partition ID to be associated with the partition.
Orchestration Engine	Specifies the Orchestrator name for the organization.
Service Node IP Address	Specifies the IP address for the service node for a partition
Edge Router ID	Specifies the Edge Router ID.
Extension Status	Specifies if the extension is enabled or disabled.
Profile	Specifies the default profile used.
Networks Section	
Network Name	Specifies the name to identify the network.
Partition Name	Allows you to select the partition to be applied for the network.
Segment ID	Specifies the segment ID to be used for partition extension.

Table 3-5

Field/Icons		Description
Mobility Domain	VLAN ID	Specifies the VLAN ID for the mobility domain.
	Mobility Domain ID	Allows you to select the mobility domain ID from the drop-down list.
Profile Name		Specifies the default profile used.
DHCP Scope	Subnet	Specifies the subnet for the network.
	Gateway	Specifies the gateway for the network.
	IP Range	Specifies the IP address range available for the network.
Add		Allows you to add Organization, Partition, or Network.
Edit		Allows you to edit Organization, Partition, or Network.
Delete		Allows you to delete Organization, Partition, or Network.
Enable Extension		Allows you to enable the extension for the selected Organization.
Disable Extension		Allows you to disable the selected extension.
Deploy Configuration		Allows you to deploy the network for the selected partition.
Undeploy Configuration		Allows you to undeploy the network configuration.
Refresh		Refreshes the list of items in the view.
Show Filter		Filters list of items based on the defined value for each column.
Print		Prints the list of Organizations or Networks along with their details.
Export		Exports the list of items and their details to a Microsoft Excel spreadsheet.
Maximize		Allows you to maximize the view for Organizations or Networks.

Fabric provides the following configuration options:

- Organizations
 - [Adding an Organization](#)
 - [Editing an Organization](#)
 - [Deleting an Organization](#)
 - [Adding a Partition](#)
 - [Editing a Partition](#)
 - [Deleting a Partition](#)
- Networks
 - [Adding a Network](#)
 - [Editing a Network](#)
 - [Deleting a Network](#)

Adding an Organization

-
- Step 1** From the menu bar, select **Config > Auto-Configuration > Organizations > Add > Organization**.
 - Step 2** In the Add Organization window, specify the **Name** and **Description** of the organization.
 - Step 3** Specify the **Orchestration Engine**.
 - Step 4** Click **Add**.

Editing an Organization

-
- Step 1** From the menu bar, select **Config > Auto-Configuration > Organizations**.
 - Step 2** Select an organization from the List and click the **Edit** icon.
 - Step 3** In the Edit Organization window, change the configuration.
 - Step 4** Click **Edit** to save the changes.

Deleting an Organization



Note You must delete all partitions under an organization before deleting the organization.

-
- Step 1** From the menu bar, select **Config > Auto-Configuration > Organizations**.
 - Step 2** Select an organization from the List and click the **Delete** icon.
 - Step 3** Click **Yes** to confirm.

Adding a Partition

-
- Step 1** From the menu bar, select **Config > Auto-Configuration > Organizations > Add>Partition**.
 - Step 2** In the Add Partition window, use the drop-down to select the organization.
 - Step 3** Specify the **Name** for the partition.
 - Step 4** Specify the VRF name and provide description for the partition.
 - Step 5** Specify the Edge Router ID for the partition.
Select the checkbox if you choose to extend the partition across the fabric.
If you do not select the checkbox, this partition will not be extended across the Fabric.
 - Step 6** Specify the **DNS Server** and the **Secondary DNS server** for the partition.
 - Step 7** From the drop-down list, select the default **Profile Name**.
The values for the **Profile Parameters** are auto-populated based on the default Profile Name.
 - Step 8** Click **OK** to configure the partition.

Editing a Partition

- Step 1** From the menu bar, select **Config>Auto-Configuration>Organizations**.
- Step 2** Click an organization from the List and select the Partition.
- Step 3** Click the **Edit** icon
- Step 4** In the Edit Partition window, change the configuration.
- Step 5** Click **Edit** to save the changes.

Deleting a Partition



Note You must delete all networks under the partition before deleting the partition.

- Step 1** From the menu bar, select **Config>Auto-Configuration>Organizations**.
- Step 2** Click an organization from the List and select the Partition.
- Step 3** Click the **Delete** icon
- Step 4** Click **Yes** to confirm.

Adding a Network

- Step 1** From the menu bar, select **Config > Auto-Configuration > Networks >Add**.
- Step 2** In the Add Network window, use the drop-down to select the **Organization** and **Partition**.



Note If there is only one organization and partition configured, the values for these fields are automatically populated.

- Step 3** Specify the **VRF Name** for the partition.
The VRF Name must be of the format organizationName:partitionName.
- Step 4** Specify the **Network Name** to identify the network.
- Step 5** Specify the **Multicast Group Address**.



Note The Multicast Group Address is used to Enable VxLAN Encapsulation on the **Admin > Fabric Encapsulation Settings** page.

- Step 6** Select the **Network Role** from the drop-down list based on the type of the network.
- Step 7** In the Network ID section, choose one of the following:
 - Segment ID Only
 - Specify the **Segment ID** for the network.
 - Mobility Domain and VLAN

- Specify the **Segment ID** for your network.
- Select **Generate Seg ID** to generate segment ID automatically.
- Specify the **VLAN ID** and **Mobility Domain ID** if you need to create a VLAN + Mobility Domain network.

Step 8 In the DHCP Scope section, specify the **IP Range**.

Step 9 Use the drop-down to select the **Profile**.

Step 10 Specify the **Profile** parameters.

Step 11 Specify the **Service Configuration** parameters.

Step 12 Click **Add**.

Editing a Network

Step 1 From the menu bar, select **Config>Auto-Configuration>Networks**.

Step 2 Select a network from the List and click the **Edit** icon

Step 3 In the Edit Partition window, change the configuration.

Step 4 Click **Edit** to save the changes.

Deleting a Network

Step 1 From the menu bar, select **Config>Auto-Configuration>Networks**.

Step 2 Select a network from the List and click the **Delete** icon.

Step 3 Click **Yes** to confirm.

Profiles

Profiles provide the following configuration options:

- Profiles
 - [Adding a profile](#)
 - [Editing a Profile](#)
 - [Delete a Profile](#)
- Profile Instance
 - [Editing a Profile Instance](#)

Adding a profile

Step 1 From the menu bar, select **Config > Profiles > Add**.

Step 2 In the Add Profile window, specify the **Name** and **Description** of the profile.

**Note**

A global VLAN is a fabricpath-enabled VLAN which is not mapped to a Segment ID. Before Cisco Prime DCNM 7.2(2), the user-defined Global VLAN profile names must end with “GblVlanProfile” (case-insensitive), for the network to auto-refresh.

Step 3 Use the drop-down, select the **Type** of the Profile.

**Note**

Devices with different platforms may use profiles of different profile types. For this release, **FPVLAN**, **FPBD**, **IPVLAN**, **IPBD** are supported.

Step 4 From the drop down, select **Sub Type**. Sub Type of profiles differentiate profile categories, such as :

- individual profile
- universal profile
- network profile
- partition profile
- DCI profile and so on.

For more information, see Cisco Dynamic Fabric Automation Configuration Guide.

In DCNM Release 7.2, the following subtypes are supported:

- partition:universal - Universal profile for a partition
- network:universal - Universal profile for a network
- bl-er:universal - Universal profile for a Border Leaf or Edge Router
- bl-er:universal,er - Universal profile for a Edge Router
- bl-er:universal,bl - Universal profile for a Border Leaf
- partition:individual - Individual profile for a partition
- network:individual - Individual profile for a network

Step 5 Use the drop-down to select the **Forwarding Mode**. The following values are supported:

- anycast-gateway
- proxy-gateway
- none

Step 6 Enter the **Profile Content** from collection of CLI commands to discover a specific configuration.

Step 7 Click **Add**.

Editing a Profile

-
- Step 1** From the menu bar, select **Config > Profiles**.
 - Step 2** Select a profile from the list and click the **Edit** icon.
 - Step 3** In the Edit profile window, change the configuration.
 - Step 4** Click **Edit** to save the changes.

Delete a Profile

-
- Step 1** From the menu bar, select **Config>Profiles**.
 - Step 2** Select a profile from the list and click the **Delete** icon.
 - Step 3** Click **Yes** to confirm.

Editing a Profile Instance

-
- Step 1** From the menu bar, select **Config>Profiles**.
 - Step 2** Select a profile from the list and click the **Edit** icon.
 - Step 3** In the Edit Profile Instance window, change the configuration.
 - Step 4** Click **Edit** to save the changes.

Administering Cisco Prime DCNM Web Client

The Admin options allows you to perform minor administrative and configuration tasks on the Cisco Prime DCNM-SAN Server.

The Admin option contains the following sub-menus:

- **Status**—Displays the status of the Database Server and allows you to start and stop Performance collector services on your server. You should restart services only if something is not working properly or if too large a percentage of system resources are being consumed.
- **Data Sources**—Allows you to view all the data sources such as Fabric, LAN, VMware, SMIS and so on.
- **Logs**—Allows you to view all the logs from the various services running on the Cisco Prime DCNM-SAN Server.
- **Server Properties**—Allows you to view all the fields defined in the server.properties config file.
- **SFTP Credentials**—Allows you to view the SFTP credentials.
- **License**—Allows you to view the licensing details.
- **Federation**—Allows you to view the server federation details.
- **Clients**—Allows you to view all the clients connected to the Cisco Prime DCNM-SAN Server.

**Note**

You cannot start or stop the Database Server services using DCNM Web Client. If you are using the Microsoft Windows operating system, you need to use Microsoft Management Console to stop, start, or restart the Database Server.

- If you see a database file lock error in the database log, you can fix it by shutting down and restarting the database server using the Web Client.
- Only network administrators can access the DCNM Web Client Admin options. Network operators cannot view the Admin options.

This section includes the following topics:

- [Starting, Restarting, and Stopping Services, page 3-80](#)
- [Administering Datasources, page 3-80](#)

Starting, Restarting, and Stopping Services

Step 1 DETAILED STEPS From the menu bar, choose **Admin > General > Status**.

You see a table of services per server and the status of each as shown in [Figure 3-1](#).

Figure 3-1 *DCNM-SAN Services Status*

Step 2 In the Actions column, use the **Start**, **(Re)start** or **Stop** icons to start, restart, or stop any of the services.

Administering Datasources

You can manage the Fabrics, LAN and VMWare using the datasources option. This section contains the following:

- [Adding, Editing, Re-discovering, Purging and Removing Managed Fabrics, page 3-81](#)
- [Adding, Editing, Re-discovering, Purging and Removing LAN, LAN Tasks and Switch, page 3-83](#)
- [Adding, Editing, Re-discovering and Removing VMware Servers, page 3-86](#)
- [Adding, editing, removing, rediscovering and refreshing SMI-S Storage, page 3-88](#)

Adding, Editing, Re-discovering, Purging and Removing Managed Fabrics

Cisco Prime DCNM Web Client reports information obtained by the Cisco Prime DCNM-SAN on any fabric known to Cisco Prime DCNM-SAN.

This section contains the following:

- [Adding a Fabric, page 3-81](#)
- [Editing a Fabric, page 3-81](#)
- [Rediscovering a Fabric, page 3-82](#)
- [Purging a Fabric, page 3-82](#)
- [Removing a Fabric, page 3-82](#)
- [Moving Fabrics to Another Server Federation, page 3-82](#)

Adding a Fabric

You can discover new fabric and start managing a fabric from Cisco Prime DCNM Web Client. Before you discover a new fabric, ensure you create a SNMP user on the switch.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
You see a list of fabrics (if any) managed by Cisco Prime DCNM-SAN in the Opened column.
- Step 2** Click **Add Fabric** to add a new fabric.
You see the Add Fabric dialog box.
- Step 3** Enter the Fabric Seed Switch IP address for this fabric.
- Step 4** (Optional) Check the **SNMPV3** check box. If you check SNMPV3, the fields Read Community and Write Community change to Username and Password.
- Step 5** Enter the User Name and Password for this fabric.
- Step 6** Select the privacy settings from the Auth-Privacy drop-down list.
- Step 7** (Optional) Check the **Limit Discovery by VSAN** checkbox to specify the included VSAN list or excluded VSAN list from the VSANs provided to discover a new fabric.
- Step 8** (Optional) Check the **Enable NPV Discovery in all Fabrics** check box. If you check enable NPV discovery in all fabrics, the changes are applied to all the fabrics that are previously discovered.
- Step 9** Click **Add** to begin managing this fabric.
You can remove single or multiple fabrics from the Cisco Prime DCNM Web Client.

Editing a Fabric

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Select the check box next to the fabric that you want to edit and click **Edit Fabric**.
You see the Edit Fabric dialog box. You can edit only one fabric at a time.
- Step 3** Enter a new fabric Name.
- Step 4** (Optional) Check the **SNMPV3** check box. If you check SNMPV3, the Community field change to Username and Password.

- Step 5** Enter the **User Name** and **Password**, privacy and specify how you want DCNM Web Client to manage the fabric by selecting one of the status options.
- Step 6** Change the fabric management state to **Managed**, **Unmanaged**, or **Managed Continuously**.
- Step 7** Click **Apply** to save the changes.

**Note**

In the **Admin>Datasources>Fabric**, Select the fabric for which the fabric switch password is changed. Click **Edit Fabric**, unmanage the fabric, specify the new password and then manage the fabric. You will not be able to open the fabric as the new password will not sync with the database. To open the fabric, you must log into the DCNM-SAN client, Go to **Server>Admin** and click the **Open** tab. Select the fabric and change the password manually in the Client Password/Community column.

Rediscovering a Fabric

- Step 1** From the menu bar, choose **Admin>General>Datasources**.
- Step 2** Select the check box next to the fabric and click the **Re-discover Fabric** icon.
- Step 3** Click **Yes** in the pop-up window.
The Fabric will now be re-discovered.

Purging a Fabric

- Step 1** From the menu bar, choose **Admin>General>Datasources**.
- Step 2** Select the check box next to the fabric and click the **Purge Fabric** icon.
- Step 3** Click **Yes** in the pop-up window.
The Fabric will now be purged.

Removing a Fabric

- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Select the check box next to the fabric that you want to remove and click **Remove Fabric** icon to remove the fabric from the datasource and to discontinue data collection for that fabric.

Moving Fabrics to Another Server Federation

This feature is only available on the federation setup and the Move Fabric is only displayed in the federation setup screen.

You can move the fabrics from a sever that is down to an active server. The management state will remain the same.

- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Select the fabrics from the fabric table. Click **Move Fabrics** to another Federation Server, or **Move LAN Tasks** to another DCNM Server.
- Step 3** Select the fabrics that need to be moved and click **Move Fabric**.

- Step 4** In the Move Fabrics to another Federation server dialog box, select the DCNM server where the fabrics will be moved. The server drop-down list will list only the active servers.
- Step 5** In the Move LAN Tasks to another DCNM Server dialog box, enter the LAN tasks that need to be moved and specify the DCNM server.

Adding, Editing, Re-discovering, Purging and Removing LAN, LAN Tasks and Switch

Cisco Prime DCNM Web Client reports information obtained by the Cisco Prime DCNM-LAN devices.

This section contains the following:

- [Adding LAN Devices, page 3-83](#)
- [Editing LAN Devices, page 3-84](#)
- [Purging LAN, page 3-84](#)
- [Removing LAN Devices, page 3-84](#)
- [Edit LAN Task, page 3-85](#)
- [Re-discover LAN Task, page 3-85](#)
- [Step 3Click Yes in the pop-up window to re-discover the LAN., page 3-85](#)
- [Moving LAN Devices Under a Task, page 3-85](#)
- [Remove LAN Task/Switch, page 3-85](#)
- [Delete a Switch, page 3-85](#)
- [Toggle between Task and Device view, page 3-86](#)

Adding LAN Devices

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
You see the list of LAN devices in the Name column.
- Step 2** Click **Add LAN Task** to add LAN.
You see the Add LAN dialog box.
- Step 3** Select **Hops from Seed Switch**, **Switch List** or **FWSM**. The fields vary depending on your selection.
- Step 4** Enter the **Seed Switch** IP address for the fabric.
- Step 5** The options vary depending on the discovery type selected. For example; If you select **SNMPV1** or **SNMPV3/CLI** check box varied fields are displayed.
- Step 6** Select the switch group and specify the Scan Time-out.
- Step 7** Specify the user credentials and the Optional Enable Password.
- Step 8** Use the drop-down to select the switch group.
- Step 9** Click **Next** to begin the Shallow Discovery.
- Step 10** In the Shallow LAN Discovery window, you can select all switches by using the checkbox next to the switch name column or select individual switches. Click **Previous** to go back and edit the parameters.

**Note**

In the Status column, if the switch status is Time-out or Cannot be contacted, these switches cannot be added.

- Step 11** Select a switch and click **Add** to add a switch to the switch group.
- If the seed switch(es) are not reachable, it will be shown as “unknown” on the shallow Discovery window.

Editing LAN Devices

You can modify a LAN from Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Select the check box next to the LAN that you want to edit and click **Edit LAN** by CDP Seed.
- You see the Edit LAN dialog box.
- Step 3** Enter the User Name and Password.
- Step 4** Select the LAN status as **Managed** or **Unmanaged**.
- Step 5** Select the Candidate Switches for Deep Discovery.



Note You can hold the Ctrl key on your keyboard to select multiple candidate switches.

- Step 6** Click **Apply** to save the changes.

Purging LAN

-
- Step 1** From the menu bar, choose **Admin>General>Datasources**.
- Step 2** Click the **Purge unreachable devices or dead links in selected LAN** icon.
- Step 3** Click **Yes** in the pop-up window to purge the LAN device.



Note In case of a Federation set-up, you will have to select the LAN to purge.

Removing LAN Devices

You can remove a LAN from Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Select the check box next to the LAN that you want to remove and click the **Remove LAN by CDP Seed** icon to remove the switches and all their data.
- Step 3** Click **Yes** to review the LAN device.
- You can also remove an individual LAN Switch

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Click the arrow next to the DCNM Server check box to expand the field.
- Step 3** In the Switch column, click **Delete Switch** icon to delete a switch connected to the DCNM server.

Edit LAN Task

-
- Step 1** From the menu bar, choose **Admin>General>Datasources**
 - Step 2** In the Discovery Task column, click the **Edit LAN Task** icon.
 - Step 3** In the Edit LAN Task dialog box, specify the user credentials and the Optional Enable Password.
 - Step 4** Use the radio button to select the Status.
 - Step 5** Click **Apply** to save the changes.

Re-discover LAN Task

-
- Step 1** From the menu bar, choose **Admin>General>Datasources**.
 - Step 2** In the Discovery Task column, click the **Re-discover LAN** icon.
 - Step 3** Click **Yes** in the pop-up window to re-discover the LAN.

Moving LAN Devices Under a Task

You can move LAN devices under a task to a different server using Cisco Prime DCNM Web Client. This feature is available only in the federation setup and the Move LAN is displayed in the federation setup screen.

You can move the LAN from a sever that is down to an active server. The management state remains the same.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
 - Step 2** Choose the LAN from the LAN table. Click **Move LAN Tasks to another Federated Server**.
 - Step 3** In the Move LAN Tasks to another DCNM Server dialog box, enter the LAN tasks that need to be moved and specify the DCNM server. All the LAN devices under the selected tasks will be moved.

Remove LAN Task/Switch

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
 - Step 2** In the Discovery Task column, click the **Remove LAN Task** icon.
 - Step 3** In the confirmation dialog box, click **Yes** to remove the LAN task.

Delete a Switch

You can also delete an individual switch connected to a DCNM Server.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
 - Step 2** In the Switch column, click the **Delete Switch** icon.
 - Step 3** In the confirmation dialog box, click **Yes** to delete the switch

Toggle between Task and Device view

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Click the **Toggle between Task and Device view** icon.
By default, the Device view is displayed.
- Step 3** In the Device view:
- In the Group column, use the drop-down to select the LAN group.
 - Click the **Add LAN Task** icon to add a LAN. For more information see the [Adding LAN Devices](#) section.
 - In the Discovery Task column, click the **Edit LAN Task** icon to edit the LAN task. For more information, see the [Editing LAN Devices](#) section.
 - In the Discovery Task column, click the **Re-discover LAN** icon to rediscover the LAN. For more information see the [Purging LAN](#) section.
 - In the Discovery Task column, click the **Remove LAN Task** icon to delete the LAN task. For more information, see the [Removing LAN Devices](#) section.
 - In the Switch column, click **Re-discover Switch** icon to rediscover the switch.
 - In the Switch column, click the **Delete Switch** icon to delete the switch.
 - Click the **Toggle between Task and Device view** icon to toggle to the task view
- Step 4** In the Task view:
- Under Discovery Task, use the checkbox to select the task.
 - Click the **Add LAN Task** icon to add a LAN. For more information see the [Adding LAN Devices](#) section.
 - Use the checkbox to select the task and then click the **Edit LAN Task** icon at the upper-right corner above the table to edit the LAN task. For more information, see the [Editing LAN Devices](#) section.
 - Use the checkbox to select the task and then click the **Remove LAN Task** icon at the upper-right corner above the table to delete the LAN task. For more information, see the [Removing LAN Devices](#) section.
 - Use the checkbox to select the task and then click the **Re-discover LAN** icon at the upper-right corner above the table to rediscover the LAN. For more information see the [Purging LAN](#) section.
 - Click the **Refresh** icon to refresh the LAN table.
 - Click the **Purge unreachable devices or dead links in selected LAN** icon to purge the LAN. For more information see the [Purging LAN](#) section.
 - Click the **Toggle between Task and Device view** icon to toggle to the device view.
 - Click **Re-discover Switch** icon to rediscover the switch.
 - Click the **Delete Switch** icon to delete the switch.
 - In the Group column, use the drop-down to select the LAN group.

Adding, Editing, Re-discovering and Removing VMware Servers

DCNM Web Client reports information gathered by Cisco Prime DCNM-SAN on any VMware servers supported by Cisco Prime DCNM-SAN.

**Note**

Ensure that the LAN and SAN are discovered before you add the vCenter on the datasource.

This section contains the following:

- [Managing a VMware Server, page 3-87](#)
- [Removing a VMware Server, page 3-87](#)
- [Modifying a VMware Server, page 3-87](#)
- [Rediscovering a VMware Server, page 3-87](#)

Managing a VMware Server

You can manage a VMware server from Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
You see the list of VMware servers (if any) that are managed by Cisco Prime DCNM-SAN in the table.
- Step 2** Click the **Add Virtual Center** icon.
You see the Add VMware dialog box.
- Step 3** Enter the Virtual Center Server IP address for this VMware server.
- Step 4** Enter the User Name and Password for this VMware server.
- Step 5** Click **Add** to begin managing this VMware server.

Removing a VMware Server

You can remove a VMware server from the Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Select the check box next to the VMware server that you want to remove and click **Remove Virtual Center** to discontinue data collection for that VMware server.

Modifying a VMware Server

You can modify a VMware server from Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Check the check box next to the VMware server that you want to edit and click **Edit Virtual Center** icon.
You see the Edit VMware dialog box.
- Step 3** Enter a the User Name and Password.
- Step 4** Select managed or unmanaged status.
- Step 5** Click **Apply** to save the changes.

Rediscovering a VMware Server

You can rediscover a VMware server from Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Select the check box next to the VMware that you want to rediscover.
- Step 3** Click **Rediscover Virtual Center** icon.
- Step 4** Click **Yes** in the dialog box.

Adding, editing, removing, rediscovering and refreshing SMI-S Storage

The SMI-S providers are managed using the DCNM Web Client.

This section contains the following:

- [Adding SMI-S Provider](#).
- [Editing SMI-S Provider](#).
- [Deleting SMI-S Provider](#).
- [Re-Discover SMI-S Provider](#).
- [Refresh SMI-S Provider](#)

Adding SMI-S Provider

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Click the **Add SMIS Provider** icon.
- Step 3** In the Add SMI-S Provider window, use the drop-down to select the Vendor. Only EMC and NetApp are currently supported. Additional SMI-S storage vendors are discovered through a 'best effort' handler using the 'Other' vendor option in the drop-down.



Note At least one valid DCNM license must be provisioned before adding SMI-S storage discovery datasources.

- Step 4** Specify the SMI-S Server IP, User Name and Password.
- Step 5** Specify the Name Space and Interop Name Space.
- Step 6** By default, the Port number is pre-populated. If you select the **Secure** checkbox, then the default secure port number is populated.
- When using the Secure mode with EMC, the default setting is mutual authentication. For more information, see EMC's documentation about adding an SSL certificate to their trust store, or set **SSLClientAuthentication** value to '**None**' in the **Security_Settings.xml** config file and then restart the ECOM service.
- Step 7** Click **Add**. The credentials are validated and if it's valid the storage discovery starts. If the credential check fails, you will be prompted to enter valid credentials.

Editing SMI-S Provider

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Use the check-box to select the SMI-S provider and click the **Edit SMIS Provider** icon.
- Step 3** In the Edit SMI-S Provider window, use the drop-down to select the Vendor.



Note Only EMC and NetApp are currently supported.

- Step 4** Specify the SMI-S Sever IP, User Name and Password.
- Step 5** Specify the Name Space and Interop Name Space.
- Step 6** By default, the Port number is pre-populated. If you select the **Secure** checkbox, then the default secure port number is populated.
- Step 7** Click **Apply**. The Storage Discovery is stopped and a new task is created using the new information and the Storage Discover is re-started.

Deleting SMI-S Provider

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Use the check-box to select the SMI-S provider and click the **Remove SMIS Provider** icon.
The provider is removed and all data associated with the provider is purged from the system.

Re-Discover SMI-S Provider

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Use the check-box to select the SMI-S provider and click the **Re-discover SMIS Provider** icon

Refresh SMI-S Provider

-
- Step 1** From the menu bar, choose **Admin > General > Data Sources**.
- Step 2** Use the check-box to select the SMI-S provider and click the **Refresh Table** icon.
The providers are re-discovered.

Viewing Log Information

This feature enables you to view the Cisco Prime DCNM Web Client log. These processes have no corresponding GUI that allows you to view information about these log files. If you see errors, preserve these two files for viewing.



Note Logs cannot be viewed from a remote server in a federation.

-
- Step 1** From the menu bar, choose **Admin > General > Logs**.
You see a list of viewable logs in the left column.
- Step 2** Click a log file to view it.
-

Configuring Cisco Prime DCNM-SAN Server Properties

To configure Cisco Prime DCNM-SAN Server properties

Step 1 From the menu bar, choose **Admin > General > Server Properties**.

Step 2 Follow the on-screen instructions and click **Apply** to confirm the changes.

While connecting to some switches if the connection is getting timed out, in the #CLI session channel type, change default the cli.channel.type value from **exec** to **shell**.



Note After configuring the server properties, you need to restart the DCNM server only if you receive a notification stating that the server must be restarted.

Configuring SFTP/TFTP Credentials

You can configure the SFTP/TFTP credentials for the File store.

A file server is required to collect device configuration and restoring configurations to the device.

Step 1 From the menu bar, choose **Admin > General > SFTP/TFTP Credentials**.

You see the SFTP/TFTP credentials page.

TFTP Credentials option is disabled for DFA deployment of Open Virtual Appliance and ISO installers.

Step 2 In the Server Type field, use the radio button to select **SFTP**.



Note You must have a SFTP server on the DCNM Server to perform backup operation. The SFTP directory must be an absolute Linux/SSH path format and must have read/write access to the SFTP User.

- a. Enter the SFTP Username and SFTP Password.
- b. Enter the **SFTP Directory path**.
The path must be in absolute Linux path format.
- c. From the Verification Switch drop-down, select the switch.
- d. Click **Apply** to apply the configuration.
- e. Click **Verify and Apply** to verify and apply the configuration. If there are any failures during the verification, the new changes will not be stored.
- f. Click **Clear SSH Hosts** to clear SSH hosts for all switches or selected switches. If there is a failure in any of the switches, an error message is displayed. Go to **Config > Job > Job Status History** to view the number of successful and unsuccessful switches.

Step 3 In the Server Type field, use the radio button to select **TFTP**.

Cisco Prime DCNM uses an internal TFTP server for data transfer. Ensure that there is no external TFTP server running on the DCNM server.

**Note**

Ensure that your switch user role includes the copy command. Operator roles will receive a 'permission denied' error. You can change your credentials from the **Admin > DataSources** page.

- a. From the Verification Switch drop-down, select the switch.
- b. Click **Apply** to apply the configuration.
- c. Click **Verify and Apply** to verify and apply the configuration. If there are any failures during the verification, the new changes will not be stored.

Step 4 From the menu bar, choose **Config > Jobs > Job Status History** to view individual device verification status.

The configurations that are backed up are removed from the file server and are stored in the database.

Managing Switch Groups

Beginning with Cisco NX-OS Release 6.x, you can configure switch groups by using Cisco Prime DCNM Web Client. You can add, delete, rename or move a switch to a group or move a group of switches to another group.

This section contains the following:

- [Adding Switch Groups, page 3-91](#)
- [Renaming a Group, page 3-92](#)
- [Deleting a Group or a Member of a Group, page 3-92](#)
- [Moving a Switch to Another Group, page 3-92](#)
- [Moving a Switch Group to Another Group, page 3-92](#)

Adding Switch Groups

You can add a switch group from the Cisco Prime DCNM Web Client.

Step 1 From the menu bar, choose **Admin > General > Switch Groups**.

Step 2 Click the **Add Group** icon or press the Insert key on your keyboard.

**Note**

A field appears that allows you to enter the name for the switch group. The Insert key does not work unless you highlight the group table first.

Step 3 Enter the name of the switch group and click outside the text field or press the Return key to complete adding the switch group. Press the Esc key on your keyboard to discard the text input and exit.

The switch group name validation and the maximum tree depth is 10. If you do not choose a parent group before adding a new switch group, the new group is added on the top of the hierarchy.

Renaming a Group

You can rename a switch group from the Cisco Prime DCNM Web Client.

Step 1 Double-click on the switch group name that you want to rename.

Step 2 Enter a new name to rename the group.



Note The name of the group cannot contain any of these special characters: ()<>,;:\[]`~!#\$%*={}|\/?.

Step 3 Press the **Return** key to apply changes or press the Esc key on your keyboard to discard the modification.

Deleting a Group or a Member of a Group

You can delete group(s) and/or member(s) of a group from the Cisco Prime DCNM Web Client. When you delete a group, the associated group(s) are deleted and the fabrics or Ethernet switches of the deleted group(s) are moved back to the default SAN or LAN.

Step 1 Choose the switch group or member(s) of a group that you want to remove.

Step 2 Click the **Remove** icon or press the Delete key on your keyboard.

A dialog box prompts you to confirm the deletion of the switch group or the member of the group. Click **Yes** to delete or **No** to cancel the action

Moving a Switch to Another Group

Step 1 Use the checkbox to choose a switch from the group.

Step 2 Select the **Move the selected Switch/Fabric to Group** icon.
The Move LAN Member dialog box appears.

Step 3 Select the switch group from the list and click **Apply**.

Moving a Switch Group to Another Group

Step 1 Use the checkbox to choose a switch group.

Step 2 Click **Move Switch/Fabric to selected Group** icon.
The Move LAN Member Group dialog box appears.

Step 3 Select the switch group from the list and click **Apply**.

Managing Custom Port Groups

Custom Port groups aids you to test the performance of the interfaces in the group. You can view the defined custom ports and their configurations from **Admin > Custom Port Groups** on the Cisco Prime DCNM Web Client.

This section includes the following topics:

- [Adding Custom Port Groups, page 3-93](#)

- [Configuring Switch and Interface to the Port Group](#), page 3-93
- [Generating Reports for the Custom Port Groups](#), page 3-93
- [Removing Port Group Member](#), page 3-93
- [Removing Port Group](#), page 3-94

Adding Custom Port Groups

You can add a custom port group from the Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > Custom Port Groups**.
- Step 2** In the Defined Groups block, click the **Add Group** icon.
- Step 3** Enter the name for the custom port group in the Add Group Dialog.
- A custom port group is created in the Defined Groups block.

Configuring Switch and Interface to the Port Group

You can configure the custom port group to include switches and their interfaces.

-
- Step 1** From the menu bar, choose **Admin > Custom Port Groups**.
- Step 2** In the Defined Groups block, select the port group for which you need to add the switch and interfaces.
- Step 3** In the Configuration block, click the **Add Group Member** icon.
- The Port Configuration window appears for the selected Custom Port Group.
- Step 4** In the **Switches** tab, select the switch that you need to include in custom port group.
- The list of available Interfaces appears.
- Step 5** Select all the interfaces for which you need to check the performance.
- Step 6** Click **Submit**.
- The list of interfaces is added to the custom port group.

Generating Reports for the Custom Port Groups

You can generate the reports to monitor the performance of the interfaces in the custom port group.

-
- Step 1** From the menu bar, choose **Reports > Generate**.
- Step 2** From the Scope dropdownlist, select the port group for which you need to generate the performance report.
- Step 3** Generate the Performance report. For information about how to Generate Reports, see [Generating a Report](#).
- Step 4** Verify if the report is generated for all the interfaces that were added in the custom port group.

Removing Port Group Member

You can remove or delete the port group member from the Custom Port group.

-
- Step 1** From the menu bar, choose **Admin > Custom Port Groups**.
- Step 2** In the Defined Groups block, select the port group for which you need to add the switch and interfaces.
- Step 3** In the Configuration block, select the switch name and interface that must be deleted.
- Step 4** In the Defined Groups block, select the group for which you which must be deleted. Click **Remove Group Member** icon.
A confirmation window appears.
- Step 5** Click **Yes** to delete the member from the custom port group .

Removing Port Group

You can remove or delete the port group from the Cisco Prime DCNM Web Client.

-
- Step 1** From the menu bar, choose **Admin > Custom Port Groups**.
- Step 2** In the Defined Groups block, select the group which must be deleted. Click **Remove Group** icon.
A confirmation window appears.
- Step 3** Click **Yes** to delete the custom group.

Managing Licenses

This section includes the following topics:

- [Viewing Licenses Using the Cisco Prime DCNM Wizard, page 3-94](#)
- [Automatic License Assignment, page 3-96](#)
- [Adding Cisco Prime DCNM Licenses, page 3-97](#)
- [Assigning Licenses, page 3-97](#)
- [Unassigning Licenses to a Switch, page 3-97](#)

Viewing Licenses Using the Cisco Prime DCNM Wizard

You can view the existing Cisco Prime DCNM licenses by **DETAILED STEPS**selecting **Admin > License** to start the license wizard.

[Figure 3-2](#) displays the license information.

Figure 3-2 Cisco Prime DCNM Licenses

License	Free/Total Server-based Licenses	Unlicensed/Total (Switches/VDCs)	Need To Purchase
SAN	45 Free / 50 Total	Unlicensed / 25 Total	10
LAN	24 Free / 30 Total	Unlicensed / 15 Total	10

Group	Switch Name	WWN/Chassis Id	Model	License State	License Type	Eval Expiration
Fabric_v-95	v-95	20:00:00:05:30:00:37:1e	DS-C9509	Eval	DCNM-Server	Mon Nov 19 00:00:00 GMT-0800 2012
Fabric_switch-storage-byme	switch-storage-byme	20:00:00:18:ba:d7:d3:4c	N7K-C7010	Unlicensed		
Fabric_sw172-22-46-223	mcchinn-zonda-FC-VDC	20:00:6c:9c:ed:4b:b2:80	N7K-C7004	Permanent	DCNM-Server	
Fabric_sw172-22-46-223	mcchinn-boxter-FC-VDC	20:00:c0:62:6b:b3:c8:00	N7K-C7009	Unlicensed		
Fabric_sw172-22-46-223	sw172-22-47-21	20:00:00:22:bd:c6:46:c0	DS-C9148-K9	Unlicensed		
Fabric_sw172-22-46-223	mcchinn-N7K-FC-VDC	20:00:00:26:51:cf:57:00	N7K-C7010	Unlicensed		
Fabric_sw172-22-46-223	sw172-22-46-224	20:00:00:05:30:00:cb:56	DS-C9140	Unlicensed		
Fabric_sw172-22-46-223	sw172-22-47-20	20:00:00:0d:ec:50:0b:80	DS-C9134	Unlicensed		
Fabric_sw172-22-46-223	sw172-22-46-182	20:00:00:0d:ec:0e:94:c0	DS-C9216a	Permanent	Switch	
Fabric_sw172-22-46-223	mcchinn-NSK2	20:00:00:05:9b:75:16:40	NSK-C5010P-BF	Permanent	Switch	
Fabric_sw172-22-46-223	mcchinn-NSK	20:00:00:05:9b:20:34:00	NSK-C5020P-BF	Permanent	Switch	
Fabric_sw172-22-46-223	sw172-22-46-222	20:00:00:05:30:00:eb:46	DS-C9216	Eval	DCNM-Server	Tue Nov 20 00:00:00 GMT-0800 2012
Fabric_sw172-22-46-223	mcchinn-ucs1-A	20:00:00:05:73:ab:0e:40		Switch Model Unknown		
Fabric_sw172-22-46-223	sw172-22-46-223	20:00:00:05:30:00:61:de	DS-C9216	Eval	DCNM-Server	Tue Nov 20 00:00:00 GMT-0800 2012
Fabric_sw172-22-46-223	sw172-22-46-233	20:00:00:0d:ec:08:66:c0	DS-C9216i	Permanent	Switch	
Fabric_sw172-22-46-223	sw172-22-46-221	20:00:00:05:30:00:9a:5e	DS-C9506	Permanent	Switch	
Fabric_sw172-22-46-223	sw172-22-46-174	20:00:00:05:30:01:9b:42	DS-C9513	Permanent	Switch	
Fabric_sw172-22-46-223	sw172-22-47-167	20:00:54:7f:ec:34:82:40	DS-C9222	Permanent	Switch	



Note By default, the Switch Licenses tab appears.

Table 3-6 displays the Cisco Prime DCNM server license fields.

Table 3-6 Cisco Prime DCNM Server License Files

Field	Description
File Name	Name of the license file.
Feature	Describes the feature name specified in the license file. The following values are supported: <ul style="list-style-type: none"> DCNM-LAN DCNM-SAN DCNM-SAN-LAN LAN-ENT-N7K
PID	Describes the product ID found in the vendor string of the license file. For example, DCNM-N7K-K0 is an enterprise license for Cisco Nexus 7000 series switches.
SAN (Free or Total)	Lists the number of SAN licenses used and available.

Table 3-6 Cisco Prime DCNM Server License Files (continued)



Field	Description
LAN (Free or Total)	Lists the number of LAN licenses used and available.
Eval Expiration	Displays the expiry date of the license.
	 Note Text in the eval expiration field will be in red for licenses that expire in seven days.

Table 3-7 displays the Cisco Prime DCNM switch license fields.

Table 3-7 Cisco Prime DCNM Switch Licenses

Field	Description
Group	Displays if it is a fabric or LAN group.
Switch Name	Displays the name of the switch.
Model	Displays the model of the device. For example, DS-C9124 or N5K-C5020P-BF.
License State	Displays the license state of the switch that can be one of the following: <ul style="list-style-type: none"> • Permanent • Eval • Unlicensed • Not Applicable • Expired • Invalid
License Type	Displays if the license is a switch-based embedded license or a server-based license.
Eval Expiration	Displays the expiry date of the license.  Note Text in the eval expiration field will be in Red for licenses that expires in seven days.

Automatic License Assignment

When the Fabric is first discovered if the switch does not have a valid switch-based license, a license is automatically assigned to the Fabric from the file license pool until no more licenses are left in the pool. Also, if you have an existing Fabric and a new switch is added to the Fabric, the new switch will be assigned a license if one is available in the file license pool and if it does not already have a switch-based license.

Adding Cisco Prime DCNM Licenses

You must have network administrator privileges to complete the following procedure.

-
- Step 1** Choose **Admin > License** to start the license wizard.
- Step 2** Choose the **Server License Files** tab.
The valid Cisco Prime DCNM-LAN and DCNM-SAN license files appear.
Ensure that the security agent is disabled when you load licenses.
- Step 3** Download the license pack file that you received from Cisco into a directory on the local system.
- Step 4** Click **Add License File** and then select the license pack file that you saved on the local machine. The file will be uploaded to the server machine, saved into the server license directory and then loaded on to the server.



Note Ensure that you do not edit the contents of the .lic file or the Cisco Prime DCNM software ignores any features that are associated with that license file. The contents of the file are signed and must remain intact. When you accidentally copy, rename, or insert the license file multiple times, the duplicate files are ignored, but the original will be counted.

Assigning Licenses

BEFORE YOU BEGIN

You must have network administrator privileges to complete the following procedure.

-
- Step 1** **DETAILED STEPS** Choose **Admin > License** to start the license wizard.
You see the licenses table.
- Step 2** From the table, choose the switch that you want to assign the license to.
- Step 3** Click **Assign License**.

Unassigning Licenses to a Switch

BEFORE YOU BEGIN

You must have network administrator privileges to complete the following procedure.

DETAILED STEPS

-
- Step 1** Choose **Admin > License** to start the license wizard.
You see the licenses table.
- Step 2** From the table, choose the switch that you want to unassign the license.
- Step 3** Click **Unassign License**.

Viewing Server Federation

- Step 1** From the menu bar, choose **Admin > General > Federation**.
- The list of Servers along with its Status, Local Time and Data Sources are displayed.
- Step 2** Use the **Enable Automatic Failover** checkbox to turn on/off the failover functionality.
- Step 3** In the Location column, double-click to edit the location.



Note If the status of one of the servers in the federation is Inactive, then some functionality may not work unless the server status changes to Active in the federation.



Note Before upgrading Cisco Prime DCNM, ensure that **Enable Automatic Failover** is unchecked. Otherwise, if one server within the federation is down, the devices discovered by the server will be moved to the other DCNM server which comes up first after upgrade. To prevent the auto move for DCNM upgrade, you need to disable the auto move on all DCNMs within the federation, and then upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the auto move again.

To enable / disable Auto Move, please go to **Admin > Federation** from DCNM web page, click on the checkbox at top left for **Enable Automatic Failover**.

Configuring AAA Properties

To configure AAA properties,

- Step 1** From the menu bar, choose **Admin > Management Users > Remote AAA Properties**.
- The AAA properties configuration page appears.
- Step 2** Use the radio button to select one of the following Authentication Modes:
- **Local** - In this mode the authentication will authenticate with the local server.
 - **Radius** - In this mode the authentication will authenticate against the Radius servers specified.
 - **TACACS+** - In this mode the authentication will authenticate against the TACAS servers specified.
 - **Switch** - In this mode the authentication will authenticate against the switches specified.
 - **LDAP** - In this mode the authentication will authenticate against the LDAP server specified.

Local

- Step 1** Use the radio button and select **Local** as the authentication mode.
- Step 2** Click **Apply** to confirm the authentication mode.

Radius

-
- Step 1** Use the radio button and select **Radius** as the authentication mode.
 - Step 2** Specify the Primary server details and click **Test** to test the server.
 - Step 3** (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.
 - Step 4** Click **Apply** to confirm the authentication mode.

TACACS+

-
- Step 1** Use the radio button and select **TACACS+** as the authentication mode.
 - Step 2** Specify the Primary server details and click **Test** to test the server.
 - Step 3** (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.
 - Step 4** Click **Apply** to confirm the authentication mode.

Switch

-
- Step 1** Use the radio button to select **Switch** as the authentication mode.
 - Step 2** Specify the Primary Switch name and click **Apply** to confirm the authentication mode.
 - Step 3** (Optional) Specify the Secondary and Tertiary Switch name and click **Apply** to confirm the authentication mode.

LDAP

-
- Step 1** Use the radio button and select **LDAP** as the authentication mode.
 - Step 2** In the Host field, enter DNS address of the host.
 - Step 3** Click **Test** to test the AAA server.
 - Step 4** Enter a valid Username and Password.

A dialog box appears confirming the status of the AAA server test. If the test has failed, the LDAP Authentication Failed dialog box appears.
 - Step 5** In the Port field, enter a port number.
 - Step 6** (Optional) Select the **SSL Enabled** check box, if SSL is enabled on the AAA server.
 - Step 7** In the Base DN field, enter the base domain name.
 - Step 8** In the Filter field, specify the filter parameters.
 - Step 9** Choose an option to determine a role by either **Attribute** or **Admin Group Map**.
 - Step 10** In the Role Admin Group field, enter the name of the role.
 - Step 11** In the Map to DCNM Role field, enter the name of the role to be mapped.
 - Step 12** Click **Apply** to apply the LDAP configuration.

Adding and Removing Users

You can use Cisco Prime DCNM Web Client to add and remove Web Client users.

This section contains the following:

- [Adding Local Users, page 3-100](#)
- [Editing a User, page 3-100](#)
- [Removing a User, page 3-100](#)

Adding Local Users

Step 1 From the menu bar, choose **Admin > Management Users > Local**.
You see the Local Database page.

Step 2 Click **Add**.
You see the Add User dialog box.

Step 3 Enter the username in the Username field.



Note The username guest is a reserved name (case insensitive). The guest user can only view reports. The guest user cannot change the guest password, or access the Admin options in DCNM Web Client.

Step 4 From the Role drop-down list, select a role for the user.

Step 5 In the Password field, enter the password.

Step 6 In the Confirm Password field, enter the password again.

Step 7 Click **Add** to add the user to the database.

Step 8 Repeat Steps 2 through 7 to continue adding users.

Editing a User

Step 1 From the menu bar, choose **Admin > Management Users > Local**.

Step 2 Use the checkbox to select a user and click the **Edit Local User** icon.

Step 3 In the Edit Local User window, the User Name and Role is mentioned by default. Specify the Password and Confirm Password.

Step 4 Click **Apply** to save the changes.

Removing a User

Step 1 From the menu bar, choose **Admin > Management Users > Local**.

Step 2 Select the check box next to the user(s) you want to remove and click **Remove**.

Managing Clients

You can use the DCNM Web Client to disconnect DCNM Client Servers.

Step 1 From the menu bar, click **Admin>Clients**.

A list of DCNM Servers are displayed.

Step 2 Use the check box to select a DCNM server and click **Disconnect Client** icon to disconnect the DCNM server.



Note You cannot disconnect a current client session.

Performance Manager Collections

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco Prime DCNM Web Client to add and remove performance collections. The switch has to be licensed and in the Managed Continuously state before a collection for the switch can be created.

To add a collection follow these steps:

Step 1 From the menu bar, click **Admin>Collections**.

Step 2 Under Generate a threshold event when traffic exceeds % of capacity, use the checkbox to specify the **Critical at** and **Warning at** values. User can also use the **For ISL/Trunk Only** checkbox to limit the threshold events generated to ISL and Trunk events only and then click **Apply**.

Step 3 In the Licensed Fabrics panel, use the checkboxes to select the Fabric, ISLs/NPV Links, Hosts, Storage, FC Flows and FC Ethernet to enable performance collection for these data types.

Step 4 In the Licensed LAN Switches panel, use the checkboxes to enable performance data collection for **Trunks**, **Access** and **Errors & Discards**.

Step 5 Use the checkboxes to select the type(s) of LAN switches for which you want to collect performance data.

Step 6 Click **Apply** to save the configuration.

Step 7 In the confirmation dialog box, click **Yes** to restart the performance collector.

Configuring the RRD Database

Configuring the Round Robin Database (RRD) allows you to set the intervals at which data samples are collected. After applying the configuration, the database storage format is converted to a new format at those intervals. Because database formats are incompatible with each other, you must copy the old data (before the conversion) to the \$INSTALLDIR/pm directory. See the ["Importing the RRD Statistics Index, page 3-102"](#) topic.

Step 1 From the menu bar, choose **Admin > Performance > Databases**.

You see the Performance Database (collection interval) page.

Step 2 In the top row of the Days column, enter the number of days to collect samples at 5-minute intervals.

- Step 3** In the second row of the Days column, enter the number of days to collect samples at 30-minute intervals.
- Step 4** In the third row of the Days column, enter the number of days to collect samples at 2-hour intervals.
- Step 5** In the bottom row of the Days column, enter the number of days to collect samples at 1-day intervals.
- As of Cisco SAN-OS Release 3.1(1) and later releases, you can configure the sampling interval for ISLs. Select a sampling interval from the ISLs drop-down list.
- Step 6** Click **Apply** to apply your changes, or click **Defaults** to reset the file sizes to the default values.
- If you are applying new values, or if the current values are not the default values, you see a message indicating that the conversion of the RRD files take a certain amount of time and that the database is unavailable until then. The time it takes depends on the difference between the old and new values.

**Note**

The system allows you to convert data, one process at a time. When you start converting the data, the Apply and Default buttons change to Refresh and Cancel so that another process cannot be inadvertently started. The display is the same for all browsers that access the server during this time. Click Refresh to view the latest progress. Click Cancel to cancel the process of converting the data. If the job is successfully canceled, you see the Apply and Default buttons again. If the cancel job is not successful, you see a message indicating that the cancellation has failed.

If you want to perform this procedure, perform it before collecting a lot of data because data conversion can take a long time.

Importing the RRD Statistics Index

- Step 1** Stop Cisco Prime DCNM-SAN Server.
- Step 2** Copy the original RRD file into `$INSTALLDIR/pm/db`.
- Step 3** Run `$INSTALLDIR/bin/pm.bat s`.
- Step 4** Restart Cisco Prime DCNM-SAN and add the fabric.

Configuring Other Statistics

- Step 1** From the menu bar, choose **Admin > Performance > Others**.
- You see the Others page.
- Step 2** Click **Add**.
- You see the Add SNMP Statistic dialog box.
- Step 3** From the Switch table, select the switch for which you want to add other statistics.
- Step 4** From the SNMP OID drop-down list, select the OID.

**Note**

For SNMP OID ModuleX_Temp,IFHCInOctets.IFINDEX,IFHCOctets.IFINDEX, selected from drop down box, you must replace 'X' with correct module number or the corresponding IFINDEX.

- Step 5** In the Display Name box, enter a new name.
- Step 6** From the Type drop-down list, select the type.

Step 7 Click **Add** to add this statistic.

Viewing Events Registration

To enable Send Syslog, Send Traps and Delayed Traps you need to configure the following in the DCNM-SAN client:

- Enabling Send Syslog - Log into the DCNM-SAN client. In the Physical Attributes pane, Select **Events>Syslog>Servers**. Click the **Create Row** icon, provide the required details and click **Create**.
- Enabling Send Traps - Log into the DCNM-SAN client. In the Physical Attributes pane, Select **Events>SNMP Traps>Destination**. Click the **Create Row** icon, provide the required details and click **Create**.
- Enabling Delayed Traps - Log into the DCNM-SAN client. In the Physical Attributes pane, Select **Events>SNMP Traps>Delayed Traps**. In the Feature Enable column, use the checkboxes to enable delayed traps for the switch and specify the delay in minutes.

Step 1 From the menu bar, choose **Admin > Events > Registration**.

The SNMP and Syslog receivers along with the statistics information are displayed.

Step 2 Select **Enable Syslog Receiver** checkbox and click **Apply** to enable the syslog receiver if it is disabled in the server property.

To configure the Event Registration/Syslog properties, select **Admin>Server Properties** and follow the on-screen instructions.

Step 3 Select **Copy Syslog Messages to DB** and click **Apply** to copy the syslog messages to the database. If this option is not select, the events will not be displayed in the events page of the Web client.

Step 4 The columns in the second table displays the following:

- Switches sending traps
- Switches sending syslog
- Switches sending syslog accounting
- Switches sending delayed traps

Adding Notification Forwarding

This section contains the following:

- [Adding Notification Forwarding, page 3-103](#)
- [Removing Notification Forwarding, page 3-105](#)

Adding Notification Forwarding

You can use Cisco Prime DCNM Web Client to add and remove notification forwarding for system messages.

Cisco Prime DCNM Web Client forwards fabric events through e-mail or SNMPv1 traps.



Note

Test forwarding will only work for the licensed fabrics.

-
- Step 1** From the menu bar, choose **Admin > Events > Forwarding**.
- Step 2** The events forwarding scope, the recipient email address, severity of the event and type of the event is displayed. The description Regex field is applicable only when the forwarding source is selected as Syslog while adding the events forwarder.
- Step 3** Select the **Enable** checkbox to enable events forwarding.
- Step 4** Specify the **SMTP Server** details and the **From** e-mail address. Click **Apply** to save the configuration or in the Apply and Test icon, use the drop-down to select the fabric and click **Apply and Test** to save and test the configuration.
- Step 5** Select the **Snooze** checkbox and specify the Start date and time and the End date and time. Click **Apply** to save the configuration.
- Step 6** Click the **Add Forwarder** icon.
You see the Add Notification dialog box.
- Step 7** In the Forwarding Method, choose either **E-Mail** or **Trap**. If you choose Trap, a Port field is added to the dialog box.
- Step 8** In the **Address** field, enter the IP address.
- Step 9** From the **Scope** drop-down list, choose the fabric or LAN group for notification.
- Step 10** In the Source field select **DCNM** or **Syslog**.
If you select DCNM, then:

-
- Step 1** In the VSAN Scope, choose either **All** or **List**.
- Step 2** From the Type drop-down list, choose an event type.
- Step 3** Check the **Storage Ports Only** check box to select only the storage ports.
- Step 4** From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
- Step 5** Click **Add** to add the notification.
If you select Syslog, then:

-
- Step 1** In the **Facility** list, select the syslog facility.
- Step 2** Specify the syslog **Type**.
- Step 3** In the **Description Regex** field, specify a description that needs to be matched with the event description.
- Step 4** From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
- Step 5** Click **Add** to add the notification.



Note The minimum Severity option is available only if the Event Type is set to All.

The traps sent by Cisco Prime DCNM correspond to the severity type followed by a text description:

```
trap type(s) = 40990 (emergency) 40991 (alert) 40992 (critical) 40993 (error) 40994
(warning) 40995 (notice) 40996 (info) 40997 (debug) textDescriptionOid = 1, 3, 6, 1, 4, 1,
9, 9, 40999, 1, 1, 3, 0
```


Removing Notification Forwarding

You can remove notification forwarding.

-
- Step 1** From the menu bar, choose **Admin > Events > Forwarding**.
- Step 2** Select the check box in front of the notification that you want to remove and click **Remove**.

Configuring EMC CallHome

Cisco Prime DCNM Release 7.1.x DCNM enhances EMC call home messages. DCNM version information is displayed in with the call home message.

You can configure EMC Callhome from the Cisco Prime DCNM Web Client for EMC supported SAN switches.

DETAILED STEPS

-
- Step 1** From the menu bar, choose **Admin > Events > EMC CallHome**.
- Step 2** Select the **Enable** check box to enable this feature.
- Step 3** Use the check box to select the fabrics.
- Step 4** Enter the general e-mail information.
- Step 5** Click the **Apply** to update the e-mail options.
- Step 6** Click **Apply and Test** to update the e-mail options and test the results.
-

Event Suppression

Cisco Prime DCNM allows you to suppress the specified events based on the user-specified suppressor rules. Such events will not be displayed on the Cisco Prime DCNM Web Client and SAN Client. The events will neither be persisted to DCNM database, nor forwarded via email/SNMP trap.

You can view, add, modify and delete suppressor rules from the table. You can create a suppressor rule from the existing event table. Select a given event as the template, and invoke the rule dialog window. Event details are automatically ported from the selected event in the event table to the input fields of the rule creation dialog window.

This section includes the following:

- [Add Event Suppression Rules](#)
- [Delete Event Suppression Rule](#)
- [Modify Event Suppression Rule](#)

Add Event Suppression Rules

To add rules to the Event Suppression, do the following tasks:

-
- Step 1** From the menu bar, select **Admin > Event Suppression**.
- Step 2** In the Add Event Suppressor Rule window, specify the **Name** for the rule.
- Step 3** Select the required **Scope** for the rule based on the event source.
You can choose SAN, LAN, Port Groups or Any. For SAN and LAN, select the scope of the event at the Fabric or Group or Switch level. User can only select group(s) for Port Group scope. If use selects "Any" as the scope, the suppressor rule will be applied globally.
- Step 4** Enter the **Facility** name or choose from the **SAN/LAN Switch Event Facility** List.
If you do not specify a facility, wild card will be applied.
- Step 5** From the drop down list, select the Event **Type**.
If you do not specify the event type, wild card will be applied.
- Step 6** In the **Description Matching** field, specify a matching string or regular expression.
The rule matching engine uses regular expression supported by Java Pattern class to find a match against an event description text.
- Step 7** (Optional) Check the **Active Between** box and select a valid time range during which the event will be suppressed.
By default, the time range is not enabled, i.e., the rule will be always active.

**Note**

In general, user should not suppress accounting events. Suppressor rule for Accounting events might be created only for certain rare situations where Accounting events are generated by actions of DCNM or switch software. For example, lots of 'sync-snmp-password' AAA syslog events are automatically generated during password synchronization between DCNM and managed switches. To suppress Accounting events, user can browse web client to Suppressor table and invoke **Add Event Suppressor Rule** dialog window.

**Note**

You can go to **Health > Events** table of Web Client to create a suppressor rule for a known event. While there is no such shortcut to create suppressor rules for Accounting events.

Delete Event Suppression Rule

To delete event suppressor rules, do the following tasks:

-
- Step 1** From the menu bar, select **Admin > Event Suppression**.
- Step 2** Select the rule from the list and click **Delete** icon.
- Step 3** Click **Yes** to confirm.
-

Modify Event Suppression Rule

To modify the event suppressor rules, do the following tasks:

-
- | | |
|---------------|---|
| Step 1 | From the menu bar, select Admin > Event Suppression . |
| Step 2 | Select the rule from the list and click Edit icon.

You can edit the Facility , Type , Description Matching string, and the Valid time range . |
| Step 3 | Click Apply to save the changes, |
-

Using Cisco Prime DCNM Web Client with SSL

By default, Cisco Prime DCNM Web Client uses HTTP. If you want to install SSL certificates and use Cisco Prime DCNM Web Client over HTTPS (using TCP port 443 or another custom port), you need a certificate for each external IP address that accepts secure connections. You can purchase these certificates from a well-known Certificate Authority (CA).

To enable SSL, you must set up the keystore to use either a self-signed certificate or a certificate from a trusted third-party company such as VeriSign.

This section includes the following topics:

- [Using a self signed SSL Certificate, page 3-107](#)
- [Using a SSL Certificate when certificate request is generated using OpenSSL, page 3-108](#)
- [Using a SSL Certificate when certificate request is generated using Keytool, page 3-108](#)
- [SSL for Federated \(High Availability\) setup, page 3-109](#)

Using a self signed SSL Certificate

-
- | | |
|---------------|--|
| Step 1 | From command prompt, navigate to <DCNM install root>/dcm/java/jre1.7/bin/ . |
| Step 2 | Rename keystore located at

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks
to

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old |
| Step 3 | Generate a self signed certificate using following command

keytool -genkey -trustcacerts -keyalg RSA -alias sme -keystore
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass
fmserver_1_2_3 -validity 360 -keysize 2048 |
| Step 4 | Stop the DCNM services. |
| Step 5 | Restart the DCNM Services. |
-

Using a SSL Certificate when certificate request is generated using OpenSSL

-
- Step 1** From command prompt, navigate to <DCNM install root>/dcm/java/jre1.7/bin/
- Step 2** Rename keystore located at
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks
to
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old
- Step 3** Generate the RSA private key using openssl
openssl genrsa -out dcnm.key 2048
- Step 4** Generate a certificate request using following command:
openssl req -new -key dcnm.key -out dcnm.csr
- Step 5** Submit the CSR to certificate signing authority to digitally sign it. CA provides the certificate and signing certificate in as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to Step 6 to convert it to PEM format. If CA provided PEM format then go to [Step 7](#).
- Step 6** Convert the PKCS 7 certificate chain to X509 certificate chain
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
- Step 7** Convert the X509 certificate chain and private key to PKCS 12 format
openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password fmserver_1_2_3 -name sme
- Step 8** Import the intermediate certificate first, the root certificate, and finally the signed certificate by using the command:
keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore <DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -deststoretype JKS
- Step 9** Stop the DCNM services.
- Step 10** Restart the DCNM Services.
-

Using a SSL Certificate when certificate request is generated using Keytool

-
- Step 1** From command prompt, navigate to <DCNM install root>/dcm/java/jre1.7/bin/.
- Step 2** Rename keystore located at
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks
to
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old

- Step 3** Generate the public-private key pair in DCNM keystore
- ```
keytool -genkeypair -alias sme -keyalg RSA -keystore
"<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
-storepass fmserver_1_2_3 -storepass fmserver_1_2_3
```
- Step 4** Generate the certificate-signing request (CSR) from the public key generated in [Step 1](#).
- ```
keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM_install
root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass
fmserver_1_2_3
```
- Step 5** Submit the CSR to certificate signing authority to digitally sign it. CA provides the certificate and signing certificate in as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to [Step 6](#) to convert it to PEM format. If CA provided PEM format then go to [Step 7](#).
- Step 6** Convert the PKCS 7 certificate chain to X509 certificate chain using openssl
- ```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```
- Step 7** Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:
- ```
keytool -importcert -trustcacerts -file cert-chain.pem -keystore
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass
fmserver_1_2_3 -alias sme
```
- Step 8** Stop the DCNM services.
- Step 9** Restart the DCNM Services.

SSL for Federated (High Availability) setup

- Step 1** Generate the SSL certificate for primary node and import all the certificates at the appropriate location as mentioned above.
- Step 2** Copy the `fmserver.jks` from the primary node located at
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration.
- Step 3** Paste the `fmserver.jks` to the secondary node located at
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration.

Fabric—General Settings



Note

These features appear on your Cisco Prime DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

You can specify the general settings for the Fabric.

-
- Step 1** From the menu bar, select **Admin > Fabric > General Settings**.
- Step 2** Specify the Fabric settings based on the required configuration and click **Apply**.
- Step 3** Click **Yes** to save the configuration.
- Step 4** Click **Health** to view status of the Fabric components.
-

You can also configure the following settings for the Fabric.

- [Border Leaf Settings](#)
- [Border Leaf Device Pairing](#)
- [Border Leaf Extended Partitions](#)
- [POAP Settings](#)
- [L2 Segment ID Range Management](#)
- [Mobility Domains](#)

Border Leaf Settings

Border Leaf Settings allows you to globally enable Border Leaf/Edge Router auto-configuration, and specify its settings such as load balancing algorithm and redundancy factor.

By default, the Border Leaf/Edge Router auto configuration is disabled.

From the menu bar, select **Admin > Border Leaf Settings**.

- [Configuring Border Leaf Settings](#)
- [Creating an Edge Router](#)
- [Connect New Border leaf to the Edge Router](#)
- [Deleting Edge Router/Border leaf devices](#)

Configuring Border Leaf Settings

-
- Step 1** Check the **Enable Border Leaf/Edge Router Auto-configuration** to globally enable Border Leaf/Edge Router auto-configuration.
- Step 2** Specify the autonomous system (AS) number to compose the Route Target using the BGP protocol. This AS number is the same across the fabric.



Note

If you do not specify AS number, DCNM will be disabled.

- Step 3** From the **Load Balancing Algorithm** list, select the algorithm that must be used by DCNM to determine whether to choose border leaf based on the least load, fair share, round robin, resource consumption, speed or other criteria.

**Note**

In Cisco Prime DCNM Release 7.1 (1), only Round Robin algorithm is supported.

If your setup has vPC pair of border leaf, the vPC pair is chosen with priority over Round Robin. If a switch that is part of vPC pair is selected for partition (VRF) extension, DCNM will also select the vPC pair for the same partition (VRF) extension for load balancing.

Step 4

Specify the **Redundancy Factor** to ensure VRFs is extended on the specified number sets of border leaf switch.

**Note**

The selected number of Border Leaf/Edge Router pairs for partition (VRF) extension also depends on the Border Leaf/Edge Router pairing topology. Therefore the number of pairs is equal to or greater than the specified redundancy factor.

Border Leaf Device Pairing

This feature allows you to pair Border Leaf with the Edge Router and specify device associated configurations such as interface between Border Leaf and Edge Router. DCNM selects appropriate Border Leaf/Edge Router pairs during partition (VRF) extension.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Table 3-2

Field	Description
Edge Router/Border Leaf	Specifies the Name of the Edge Router or the connected Border Leaf.
IP Address	Specifies the IP address of the Border Leaf/Edge Router.
Interface Name/Port Channel	Specify the interface name or port channel between Border Leaf and Edge Router.
Profile Name	Specifies the default profile name.
Type	Specifies if the device is an Edge Router configuration or a Border Leaf configuration.
Partition Utilization	Specifies the partitions utilized and the maximum partitions available for the device.
Add	Allows you to add a Border Leaf/Edge Router. For more information, see Creating an Edge Router .
Edit	Allows you to edit a Border Leaf/Edge Router.
Delete	Allows you to delete a Border Leaf/Edge Router. For more information, see Deleting Edge Router/Border leaf devices .
View Profile	Allows you to view the profile created
Refresh	Refreshes the list of switches.
Show Filter	Filters list of switches based on the defined value for each column.

Table 3-2

Field	Description
Print	Prints the list of devices and their details.
Export	Exports the list of devices and their details to a Microsoft Excel spreadsheet.

- [Creating an Edge Router](#)
- [Connect New Border leaf to the Edge Router](#)
- [Deleting Edge Router/Border leaf devices](#)

Creating an Edge Router

Step 1 From the menu bar, select **Config > Border Leaf Device Pairing**.

Step 2 Click **Add**. Select **Edge Router**.

Step 3 To configure the Edge Router:

- Use the radio button to select **Configure an Edge Router**.



Note The **Configure an Edge Router** option will be selected by default.

- Select **Notify Edge Router when relevant partitions are changed** to notify the Edge Router.
- Select the **Device Name** from the drop-down list to identify an Edge Router.
- Specify the **IP Address** for the Edge Router.
- Specify the **Maximum Number of Partitions** required for the Edge Router.

Step 4 To configure a **Border PE**:

- Use the radio button to select **Configure a Border PE**.
- Select **Notify Edge Router when relevant partitions are changed** to notify the Edge Router.
- Select the **Device Name** from the drop-down list to identify an Edge Router.
- Specify the **IP Address** for the Edge Router.
- Specify the **Maximum Number of Partitions** required for the Edge Router.
- Define the Profile Parameters.
 - asn—specifies the autonomous system (AS) number for the Border PE
 - vrfSegmentId—specifies the vrf segment ID.
 - rsvdGlobalAsn—specifies the reserved global autonomous system number.
 - dcId—specifies the Edge Router ID for the Border PE
 - vrfName—Specifies the vrf name



Note Note: The value for vrfName must be of the format 'organizationName:partitionName'.

Step 5 Click **OK** to save the configuration.

Connect New Border leaf to the Edge Router

Step 1 From the menu bar, select **Config > Border Leaf Device Pairing**.

Step 2 Click **Add**. Select **Border Leaf**.

Step 3 Define the parameters for the Border leaf configuration and edge router configuration for pairing.

Field	Description
Name	Select the name from the drop-down list for the Border leaf.
IP Address	The IP address is auto-populated based on the selected Border Leaf.
Port Channel or the Interface Name	Specify the interface name or port channel between Border Leaf and Edge Router.
Maximum Number of Partitions	Specifies the number of partitions required for the configuration
Default Profile Name	Select the default profile name from the drop-down list to apply for the profile.
Notify Border Leaf when relevant partitions	Select to notify the Border Leaf when relevant partitions are created.

Step 4 Click **OK** to connect the new border leaf device to the Edge router.

Deleting Edge Router/Border leaf devices

Step 1 From the menu bar, select **Config > Border Leaf Device Pairing**.

Step 2 Select the Edge Router/Border leaf device definitions from the list and click **Delete**.

Step 3 Click **Yes** to confirm and delete the profile.

Border Leaf Extended Partitions

This screen lists the extended partitions, selected Border Leaf/Edge Router pairs, and their corresponding profiles and configurations. From the menu bar, select **Config > Extended Partitions**.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Field	Description
VRF	Specifies the VRF name for the extended partition.
Organization	Specifies the name of organization which the extended partition belongs to.
Partition	Specifies the name of the partition that is extended.

Field	Description
Redundancy Factor	Specifies the run-time redundancy factor for that partition extension.
Edge Router	Specifies the name of the Edge Router.
Edge Router IP Address	Specifies the IP address of the Edge Router device.
Edge Router Profile	Specifies the default profile for the edge router.
Border Leaf (BL)	Specifies the name of the Border Leaf device
BL IP Address	Specifies the IP address of the Border Leaf device.
BL Profile	Specifies the default profile for the border leaf device.

POAP Settings

This allows you to set common parameters which will be populated as default values in POAP templates. For a new POAP template, values defined in this global settings page, will be automatically pre-populated. From the menu bar, select **Admin->Fabric->POAP Settings**.

Specify the parameters for the following fields:

Field	Description
MGMT_PREFIX	Specify the Management prefix.
DEFAULT_GATEWAY	Specify the default gateway.
MANAGEMENT_VLAN	Specify the management VLAN.
LDAP_SERVER_NAME	Specify the LDAP server name.
LDAP_SERVER_IP	Specify the LDAP server IP address.
LDAP2_SERVER_NAME	Specify the secondary LDAP server name.
LDAP2_SERVER_IP	Specify the secondary LDAP server IP address.
LDAP_USERNAME	Specify the LDAP username.
LDAP_PASSWORD	Specify the LDAP password.
XMPP_SERVER	Specify the XMPP server name.
XMPP_SERVER_IP	Specify the XMPP IP address.

Step 4 Click **Apply** to save the POAP settings for the fabric.

Fabric Encapsulation Settings

To configure encapsulation settings, do the following:

-
- Step 1** From the menu bar, select **Admin > Fabric Encapsulation Settings**.
- Step 2** Select **Enable Fabric Path Encapsulation** to enable FabricPath-based Auto-Configuration on Nexus 5600, Nexus 6000 and Nexus 7000 Series devices.
- You can choose from the combination of available leaf networks.

Step 3 Select **Enable VxLAN Encapsulation** to enable VxLAN-based Auto-Configuration on Nexus 5600, Nexus 7000 and Nexus 9000 Series devices.

You can choose from the combination of available leaf network in your topology. The first three options are related to “Phantom-RP with PIM BIDIR”. The second three options are related to “Anycast-RP PIM ASM/SSM”.

- a. In the **Multicast Group Subnet Range** field, specify the Multicast IP Address with subnet for the multicast group.

This Multicast Group address range is shared between L2 and L3. This field is auto-populated from the Network page at **Config > Auto-Configuration > Networks** section. However, the value can be modified.

- b. In the **Number of Rendezvous Points (RPs)** field, to divide the multicast group subnet into buckets, which the user can configure.

The valid value for RPs are 1, 2, 4, and 8.

- c. The **RPx Multicast Group Subnet** field is auto-populated based on Multicast Group Subnet. “X” is the RP count.

This is applicable only for Phantom-RP with PIM BIDIR.

- d. In the **RPx Phantom IP Address** field, enter the Phantom IP Addresses for the RPs. “X” is the RP count.

This is applicable only for Phantom-RP with PIM BIDIR.

- e. In the **RPx IP Address** field, enter the RP IP Addresses for the RPs. “X” is the RP count.

This is applicable only for Anycast-RP PIM ASM/SSM.

- f. In the **Anycast IP Address** field, enter the Anycast IP Address.

This is applicable only for Anycast-RP PIM ASM/SSM.

Step 4 Click **Apply** to save the settings.

This settings are used during Auto-Configuration and POAP.

Based on the selected option, the following profiles will be loaded in Partition/Network screens.

- FabricPath with N5600/N6K Leaf Network—The profiles from profiles(FPVLAN) table
- FabricPath with N7K Leaf Network—The profiles from profilesBridgeDomain(FPBD) table
- FabricPath with N5600/N6K & N7K Combined Leaf Network—The common profiles from profiles(FPVLAN) & profilesBridgeDomain(FPBD) table
- VXLAN with N5600 Leaf Network—The profiles from profilesIPFabric(IPVLAN) table
- VXLAN with N7K Leaf with PIM Bidir Network—The profiles from profilesIPBridgeDomain(IPBD) table
- VXLAN with N5600 & N7K Combined Leaf Network—The common profiles from profilesIPFabric(IPVLAN) & profilesIPBridgeDomain(IPBD) table
- VXLAN with N7K Leaf with PIM ASM Network—The profiles from profilesIPBridgeDomain(IPBD) table
- VXLAN with N9K Leaf Network—The profiles from profilesIPFabric(IPVLAN) table
- VXLAN with N7K & N9K Combined Leaf Network—The common profiles from profilesIPFabric(IPVLAN) & profilesIPBridgeDomain(IPBD) table

Based on the encapsulation option, the following profiles will be loaded in Border Leaf/BorderPE/Edge Router screens.

- FabricPath—The profiles from profilesBridgeDomain(FPBD) table
- VXLAN—The profiles from profilesIPBridgeDomain(IPBD) table

**Note**

Cisco Prime DCNM Release 7.2(2) is packaged with the following profiles:

- VXLAN-EVPN configuration profiles for Nexus 5600, Nexus 7000, and Nexus 9000 Series Leaf Network.
- FabricPath configuration profiles for Nexus 5660, Nexus 6000, and Nexus 7000 Series Leaf Network.

The universal network/partition profiles is supported for the VXLAN-EVPN-based standalone Fabric.

L2 Segment ID Range Management

Cisco Prime DCNM allows you to create a new Segment ID range, and map the orchestrator ID. DCNM will associate the range with the specified orchestrator ID.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Field	Description
Orchestrator Name	Specifies the Orchestrator name.
Section ID Range	Specifies the segment ID range for that Orchestrator. The Segment ID range is unique for all Orchestrators. The default Segment ID range cannot be used for any orchestrator.
Add	Allows you to add a new Orchestrator.
Edit	Allows you to edit the selected Orchestrator and segment ID range.
Delete	Allows you to delete the Orchestrator.
Refresh	Refreshes the list of Orchestrators.
Show Filter	Filters list of switches based on the defined value for each column.
Print	Prints the list of Orchestrator and their details.
Export	Exports the list of Orchestrators and their details to a Microsoft Excel spreadsheet.

- [Add Orchestrator](#)
- [Modify Orchestrator](#)
- [Delete Orchestrator](#)

Add Orchestrator

-
- Step 1** From the menu bar, select **Admin > L2 Segment ID Range Management**.
 - Step 2** Click **Add** to add a new orchestrator.
 - Step 3** In the **Orchestrator Name** field, specify the name for the Orchestrator.
 - Step 4** In the Segment ID Range field, specify Segment ID range to be associated with the Orchestrator.
By default, DCNM continues to support the default Segment ID range defined in the **DCNM Admin > Fabric** page.

Modify Orchestrator

-
- Step 1** From the menu bar, select **Admin > L2 Segment ID Range Management**.
 - Step 2** Select the orchestrator from the list and click **Edit**.
 - Step 3** Update and click **OK** to save the settings.

Delete Orchestrator

-
- Step 1** From the menu bar, select **Admin > L2 Segment ID Range Management**.
 - Step 2** Select the orchestrator from the list and click **Delete**.
 - Step 3** Click **Yes** to delete the orchestrator.
-

Mobility Domains

Cisco Prime DCNM allows you to create mobility domains to configure a Mobility Domain Network. The Mobility Domains configured on this page can be used in Config > Auto-Configuration > Networks page.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

Field	Description
Mobility Name	Specifies the name for the mobility domain.
Detectable VLAN Range	Specifies detectable VLAN range for the particular mobility domain.
Add	Allows you to add a new mobility domain.
Edit	Allows you to edit the selected mobility domain and the VLAN range.
Delete	Allows you to delete the mobility domain.
Refresh	Refreshes the list of mobility domains.
Show Filter	Filters list of domains based on the defined value for each column.

Field	Description
Print	Prints the list of mobility domains and VLAN range.
Export	Exports the list of mobility domains and their details to a Microsoft Excel spreadsheet.

- [Add Mobility Domains](#)
- [Modify Mobility Domains](#)
- [Delete Mobility Domains](#)

Add Mobility Domains

-
- Step 1** From the menu bar, select **Admin > Mobility Domains**.
- Step 2** Click **Add** to add a new mobility domain.
- Step 3** In the **Mobility Domain Name** field, specify the name for the Mobility Domain.
- Step 4** In the **Detectable VLAN Range** field, specify the VLAN IP address range for mobility domain.
- Step 5** Click **OK** to add a mobility domain.
-

Modify Mobility Domains

-
- Step 1** From the menu bar, select **Admin > Mobility Domains**.
- Step 2** Select the mobility domain from the list and click **Edit**.
- Step 3** Update and click OK to save the settings.
-

Delete Mobility Domains

-
- Step 1** From the menu bar, select **Admin > Mobility Domains**.
- Step 2** Select the mobility domain from the list and click **Delete**.
- Step 3** Click **Yes** to delete the mobility domain.
-



CHAPTER 4

Cisco DCNM-SAN Overview

This chapter provides an overview of the basic Cisco DCNM-SAN components and includes the following sections:

- [DCNM-SAN Server, page 4-1](#)
- [Authentication in DCNM-SAN Client, page 4-3](#)
- [DCNM-SAN Client, page 4-1](#)
- [Device Manager, page 4-2](#)
- [DCNM-SAN Web Client, page 4-2](#)
- [Performance Manager, page 4-3](#)
- [Cisco Traffic Analyzer, page 4-3](#)
- [Network Monitoring, page 4-4](#)
- [Performance Monitoring, page 4-4](#)

DCNM-SAN Server

DCNM-SAN Server is a platform for advanced MDS monitoring, troubleshooting, and configuration capabilities. DCNM-SAN Server provides centralized MDS management services and performance monitoring. SNMP operations are used to efficiently collect fabric information. The Cisco DCNM-SAN software, including the server components, requires about 60 MB of hard disk space on your workstation. Cisco DCNM-SAN Server runs on Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows 7, Solaris 9 and 10, and Red Hat Enterprise Linux AS Release 5.

Each computer configured as a Cisco DCNM-SAN Server can monitor multiple Fibre Channel SAN fabrics. Up to 16 clients (by default) can connect to a single Cisco DCNM-SAN Server concurrently. The Cisco DCNM-SAN Clients can also connect directly to an MDS switch in fabrics that are not monitored by a Cisco DCNM-SAN Server, which ensures that you can manage any of your MDS devices from a single console.

DCNM-SAN Client

Cisco DCNM-SAN Client is a Java and SNMP-based network fabric and device management tool with a GUI that displays real-time views of your network fabric, including Cisco Nexus 5000 Series switches, Cisco MDS 9000 Family switches and third-party switches, hosts, and storage devices.

DCNM-SAN Client provides Fibre Channel troubleshooting tools, in addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. You can use these health and configuration analysis tools on the MDS 9000 Family switch or Cisco Nexus 5000 Series switch to perform Fibre Channel ping and traceroute.

Fabric Manager Release 4.1(1b) and later releases provide a multilevel security system by adding a server admin role that allows access to limited features. The configuration capabilities of a server admin is limited to configuring FlexAttach and relevant data. Advanced mode option is available only for network administrators and provides all of the DCNM-SAN features, including security, IVR, iSCSI, and FICON.

Device Manager

Device Manager provides a graphical representation of a Cisco MDS 9000 Family switch chassis, Cisco Nexus 5000 Series switch chassis, or Cisco Nexus 7000 Series switch chassis (FCoE only) along with the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

The tables in the DCNM-SAN Information pane basically correspond to the dialog boxes that appear in Device Manager. However, while DCNM-SAN tables show values for one or more switches, a Device Manager dialog box shows values for a single switch. Device Manager also provides more detailed information for verifying or troubleshooting device-specific configuration than DCNM-SAN.

Device Manager provides two views: Device View and Summary View. Use Summary View to monitor interfaces on the switch. Use Device View to perform switch-level configurations including the following configurations:

- Configuring virtual Fibre Channel interfaces
- Configuring Fibre Channel over Ethernet (FCoE) features
- Configuring zones for multiple VSANs
- Managing ports, PortChannels, and trunking
- Managing SNMPv3 security access to switches
- Managing CLI security access to the switch
- Managing alarms, events, and notifications
- Saving and copying configuration files and software image
- Viewing hardware configuration
- Viewing chassis, module, port status, and statistics

DCNM-SAN Web Client

With DCNM-SAN Web Client you can monitor Cisco MDS switch events, performance, and inventory from a remote location using a web browser.

- Performance Manager Summary reports—The Performance Manager summary report provides a high-level view of your network performance. These reports list the average and peak throughput and provides hot-links to additional performance graphs and tables with additional statistics. Both tabular and graphical reports are available for all interconnections monitored by Performance Manager.

- Performance Manager drill-down reports—Performance Manager can analyze daily, weekly, monthly and yearly trends. You can also view the results for specific time intervals using the interactive zooming functionality. These reports are only available if you create a collection using Performance Manager and start the collector.
- Zero maintenance database for statistics storage—No maintenance is required to maintain Performance Manager's round-robin database, because its size does not increase over time. At prescribed intervals the oldest samples are averaged (rolled-up) and saved. A full two days of raw samples are saved for maximum resolution. Gradually the resolution is reduced as groups of the oldest samples are rolled up together.

Performance Manager

The primary purpose of DCNM-SAN is to manage the network. A key management capability is network performance monitoring. Performance Manager gathers network device statistics historically and provides this information graphically using a web browser. Performance Manager presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

Performance Manager has three operational stages:

- Definition—The Flow Wizard sets up flows in the switches.
- Collection—The Web Server Performance Collection screen collects information on desired fabrics.
- Presentation—Generates web pages to present the collected data through DCNM-SAN Web Server.

Performance Manager can collect statistics for ISLs, hosts, storage elements, and configured flows. Flows are defined based on a host-to-storage (or storage-to-host) link. Performance Manager gathers statistics from across the fabric based on collection configuration files. These files determine which SAN elements and SAN links Performance Manager gathers statistics for. Based on this configuration, Performance Manager communicates with the appropriate devices (switches, hosts, or storage elements) and collects the appropriate information at fixed five-minute intervals.

Authentication in DCNM-SAN Client

Administrators launch DCNM-SAN Client and select the seed switch that is used to discover the fabric. The user name and password are passed to DCNM-SAN Server and are used to authenticate to the seed switch. If this user name and password are not a recognized SNMP user name and password, either DCNM-SAN Client or DCNM-SAN Server opens a CLI session to the switch (SSH or Telnet) and retries the user name and password pair. If the user name and password are recognized by the switch in either the local switch authentication database or through a remote AAA server, then the switch creates a temporary SNMP user name that is used by DCNM-SAN Client and DCNM-SAN Server.

Cisco Traffic Analyzer

Cisco Traffic Analyzer provides real-time analysis of SPAN traffic or analysis of captured traffic through a Web browser user interface. Traffic encapsulated by one or more Port Analyzer Adapter products can be analyzed concurrently with a single workstation running Cisco Traffic Analyzer, which is based on ntop, a public domain software enhanced by Cisco for Fibre Channel traffic analysis.

Cisco Traffic Analyzer monitors round-trip response times, SCSI I/Os per second, SCSI read or traffic throughput and frame counts, SCSI session status, and management task information. Additional statistics are also available on Fibre Channel frame sizes and network management protocols.

Network Monitoring

DCNM-SAN provides extensive SAN discovery, topology mapping, and information viewing capabilities. DCNM-SAN collects information on the fabric topology through SNMP queries to the switches connected to it. DCNM-SAN recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options such as fabric view, device view, summary view, and operation view.

Once DCNM-SAN is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, DCNM-SAN automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve the HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. DCNM-SAN gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

Performance Monitoring

DCNM-SAN and Device Manager provide multiple tools for monitoring the performance of the overall fabric, SAN elements, and SAN links. These tools provide real-time statistics as well as historical performance monitoring.

Real-time performance statistics are a useful tool in dynamic troubleshooting and fault isolation within the fabric. Real-time statistics gather data on parts of the fabric in user-configurable intervals and display these results in DCNM-SAN and Device Manager.

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. These statistics show the performance of the selected port in real-time and can be used for performance monitoring and troubleshooting. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data. You can set the polling interval from ten seconds to one hour, and display the results based on a number of selectable options including absolute value, value per second, and minimum or maximum value per second.



Configuring Cisco DCNM-SAN Server

This chapter describes Cisco DCNM-SAN Server, which is a platform for advanced MDS monitoring, troubleshooting, and configuration capabilities. No additional software needs to be installed. The server capabilities are an integral part of the Cisco DCNM-SAN software.

This chapter contains the following sections:

- [Information About Cisco DCNM-SAN Server, page 5-1](#)
- [Licensing Requirements For Cisco DCNM-SAN Server, page 5-2](#)
- [Installing and Configuring Cisco DCNM-SAN Server, page 5-2](#)
- [Managing a Cisco DCNM-SAN Server Fabric, page 5-8](#)
- [Modifying Cisco DCNM-SAN Server, page 5-10](#)
- [Server Federation, page 5-16](#)
- [Additional References, page 5-20](#)

Information About Cisco DCNM-SAN Server

Install Cisco DCNM-SAN Server on a computer that you want to provide centralized MDS management services and performance monitoring. SNMP operations are used to efficiently collect fabric information. The Cisco DCNM-SAN software, including the server components, requires about 60 MB of hard disk space on your workstation. Cisco DCNM-SAN Server runs on Windows 2000, Windows 2003, Windows XP, Solaris 9 and 10, and Red Hat Enterprise Linux AS Release 5.

Each computer configured as a Cisco DCNM-SAN Server can monitor multiple Fibre Channel SAN fabrics. Up to 16 clients (by default) can connect to a single Cisco DCNM-SAN Server concurrently. The Cisco DCNM-SAN Clients can also connect directly to an MDS switch in fabrics that are not monitored by a Cisco DCNM-SAN Server, which ensures you can manage any of your MDS devices from a single console.

DCNM-SAN Server Features

Cisco DCNM-SAN Server has the following features:

- **Multiple fabric management**—DCNM-SAN Server monitors multiple physical fabrics under the same user interface. This facilitates managing redundant fabrics. A licensed DCNM-SAN Server maintains up-to-date discovery information on all configured fabrics so device status and interconnections are immediately available when you open the DCNM-SAN Client.
- **Continuous health monitoring**—MDS health is monitored continuously, so any events that occurred since the last time you opened the DCNM-SAN Client are captured.
- **Roaming user profiles**—The licensed DCNM-SAN Server uses the roaming user profile feature to store your preferences and topology map layouts on the server, so that your user interface will be consistent regardless of what computer you use to manage your storage networks.

**Note**

You must have the same release of Cisco DCNM-SAN Client and Cisco DCNM-SAN Server.

**Note**

You will not be able to manage a SAN fabric if the DCNM-SAN Server is going through a IP NAT firewall to access the SAN fabric. All the IP addresses that are discovered in a SAN fabric must be directly reachable by the DCNM-SAN Server.

Licensing Requirements For Cisco DCNM-SAN Server

When you install DCNM-SAN, the basic unlicensed version of Cisco DCNM-SAN Server is installed with it. To get the licensed features, such as Performance Manager, remote client support, and continuously monitored fabrics, you need to buy and install the Cisco DCNM-SAN Server package.

However, trial versions of these licensed features are available. To enable the trial version of a feature, you run the feature as you would if you had purchased the license. You see a dialog box explaining that this is a demo version of the feature and that it is enabled for a limited time.

**Note**

DCNM SAN allows the you to open one unlicensed fabric on the DCNM server. For OVA installation, you need an xwindow installation. To open fabrics from remote client or open more than one fabric, the fabrics have to be licensed.

Installing and Configuring Cisco DCNM-SAN Server

**Note**

Prior to running Cisco DCNM-SAN Server, you should create a special Cisco DCNM-SAN administrative user on each switch in the fabric or on a remote AAA server. Use this user to discover your fabric topology.

DETAILED STEPS

-
- Step 1** Install Cisco DCNM-SAN Client and Cisco DCNM-SAN Server on your workstation. See the [“Installing Cisco DCNM-SAN Server”](#) section on page 5-3.
- Step 2** Log in to DCNM-SAN.

- Step 3** Set Cisco DCNM-SAN Server to continuously monitor the fabric. See the “[Managing a Cisco DCNM-SAN Server Fabric](#)” section on page 5-8.
 - Step 4** Repeat [Step 2](#) through [Step 3](#) for each fabric that you want to manage through Cisco DCNM-SAN Server.
 - Step 5** Install DCNM-SAN Web Server. See the “[Verifying Performance Manager Collections](#)” section on page 5-8.
 - Step 6** Verify Performance Manager is collecting data. See the “[Verifying Performance Manager Collections](#)” section on page 5-8.
-

Installing Cisco DCNM-SAN Server

When you install DCNM-SAN, the basic version of the Cisco DCNM-SAN Server (unlicensed) is installed with it. After you click the DCNM-SAN icon, a dialog box opens and you can enter the IP address of a computer running the Cisco DCNM-SAN Server component. If you do not see the Cisco DCNM-SAN Server IP address text box, click **Options** to expand the list of configuration options. If the server component is running on your local machine, leave **localhost** in that field. If you try to run DCNM-SAN without specifying a valid server, you are prompted to start the Cisco DCNM-SAN Server locally.

On a Windows PC, you install the Cisco DCNM-SAN Server as a service. This service can then be administered using Services in the Administrative Tools. The default setting for the Cisco DCNM-SAN Server service is that the server is automatically started when the Windows PC is rebooted. You can change this behavior by modifying the properties in Services.

For switches running Cisco MDS 9000 FabricWare, you must install DCNM-SAN from the CD-ROM included with your switch, or you can download DCNM-SAN from Cisco.com.

**Note**

You can have only one instance of Cisco DCNM-SAN Server running on a computer. If you have a DCNM-SAN Standalone version on your computer, you may need to uninstall it before you install Cisco DCNM-SAN Server.

To download the software from Cisco.com, go to the following website:

<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>

**Note**

If you are upgrading from an earlier version to 5.0(1a) or later, that is configured with HTTPS to use your own self-provisioned or a third-party issued SSL certificate, make sure that you set the keystore password and then restart the DCNM-SAN Server. To set the keystore password, run **\$INSTALLDIR/dcm/fm/bin encrypter.bat ssl**.

DETAILED STEPS

-
- Step 1** Click the **Install Management Software** link.
 - Step 2** Choose **Management Software > Cisco DCNM-SAN**.
 - Step 3** Click the **Installing DCNM-SAN** link.
 - Step 4** Click the **FM Installer** link.

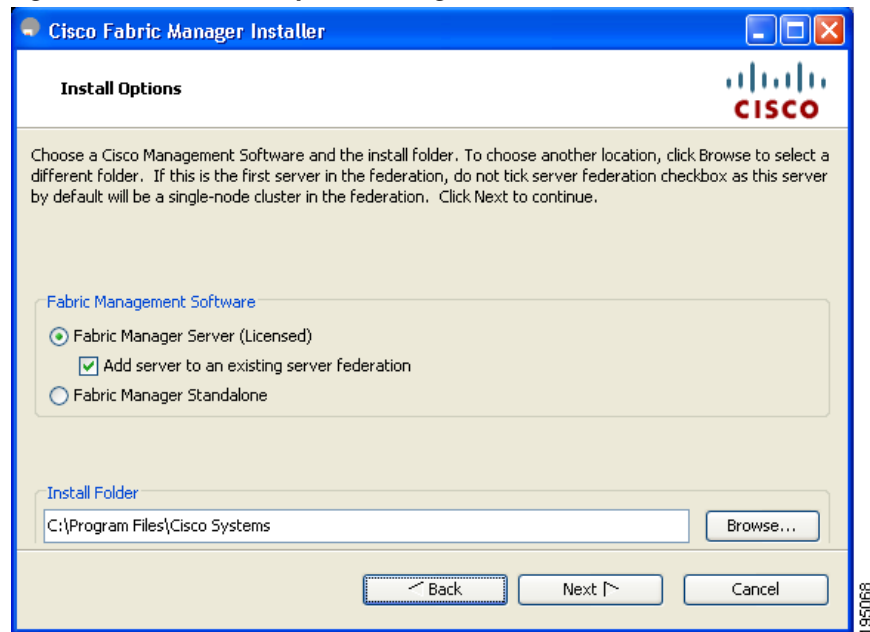
You see the welcome message in the Cisco DCNM-SAN Installer window shown in [Figure 5-1](#).

Figure 5-1 Welcome to the Management Software Setup Wizard



Step 5 Click the **Custom** radio button, and then click **Next** to begin installation.

Step 6 Check the **I accept the terms of the License Agreement** check box, and then click **Next**.
You see the Install Options dialog box as shown in [Figure 5-2](#).

Figure 5-2 Install Options Dialog Box

Step 7 Click the **Cisco DCNM-SAN Server (Licensed)** radio button to install the server components for Cisco DCNM-SAN Server.

Step 8 Click **Add server to an existing server federation** to add the server to a federation.



Note You may need to add the following line in the pg-hba.conf file under **# IPv4 local connections** in order to allow remote hosts to connect to PostgreSQL database:

```
host all all 0.0.0.0/0 md5
```

After adding, save the configuration file, restart the PostgreSQL database before you install the second server node.



Note If you are joining more than three DCNM-SAN Servers in a federation, you need to use an Oracle database with the following settings.

```
C:\Documents and Settings\Administrator>sqlplus /nolog
SQL*Plus: Release 10.2.0.1.0 - Production on Wed Jan 6 17:19:32 2010
Copyright (c) 1982, 2005, Oracle. All rights reserved.
SQL> connect / as sysdba;
Connected.

SQL> alter system set processes=150 scope=spfile;
System altered.
SQL> alter system set open_cursors=500 scope=spfile;
System altered.

SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup;
```



```

ORACLE instance started.
Total System Global Area  805306368 bytes
Fixed Size                  1453836 bytes
Variable Size               218714356 bytes
Database Buffers            583008256 bytes
Redo Buffers                 2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;

```

```

Total System Global Area  805306368 bytes
Fixed Size                  1453836 bytes
Variable Size               218714356 bytes
Database Buffers            583008256 bytes
Redo Buffers                 2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;

```

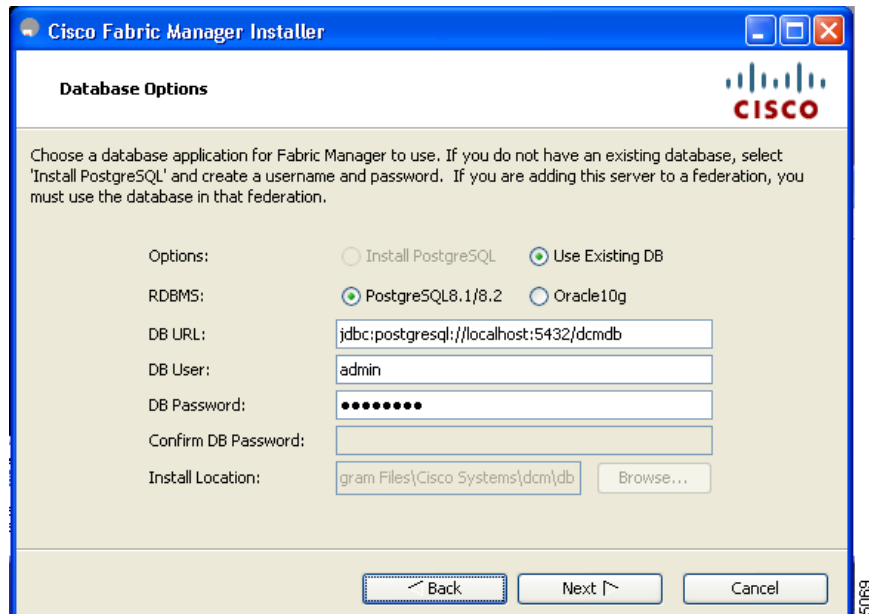
NAME	TYPE	VALUE
aq_tm_processes	integer	0
db_writer_processes	integer	4
gcs_server_processes	integer	0
job_queue_processes	integer	4
log_archive_max_processes	integer	2
processes	integer	100

Step 9 Select an installation folder on your workstation for Cisco DCNM-SAN. On Windows, the default location is **C:\Program Files\Cisco Systems**.

Step 10 Click **Next**.

You see the Database Options dialog box as shown in [Figure 5-3](#).

Figure 5-3 Database Options Dialog Box



Step 11 Click the radio button for either **Install PostgreSQL** or **Use existing DB** to specify which database you want to use.

If you choose Install PostgreSQL, accept the defaults and enter a password. The PostgreSQL database will be installed.



Note If you choose to install PostgreSQL, you must disable any security software you are running, because PostgreSQL may not install certain folders or users.



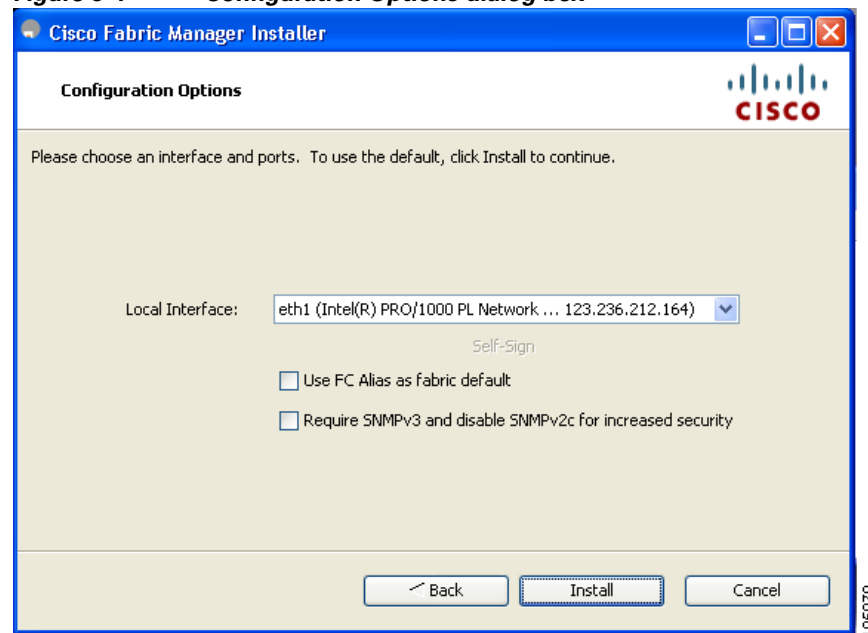
Note Before you install PostgreSQL, remove the cygwin/bin from your environment variable path if Cygwin is running on your system.

Step 12 If you select Use existing DB, click the radio button for either PostgreSQL 8.1/8.2 or Oracle10g.

Step 13 Click **Next** in the Database Options dialog box.

You see the Configuration Options dialog box as shown in [Figure 5-4](#).

Figure 5-4 Configuration Options dialog box



Step 14 Click **Install** to install Cisco DCNM-SAN Server.

If you are evaluating one of these Cisco DCNM-SAN Server features and want to stop the evaluation period for that feature, you can do that using Device Manager.

Data Migration in Cisco DCNM-SAN Server

The database migration should be limited to the existing database. Data collision can occur when you merge the data between the several databases.

When you upgrade a non federation mode database to a federation mode database for the first time, the cluster sequence table is filled with the values larger than the corresponding ones in the sequence table and conforming to the cluster sequence number format for that server ID.

Verifying Performance Manager Collections

Once Performance Manager collections have been running for five or more minutes, you can verify that the collections are gathering data by choosing **Performance Manager > Reports** in DCNM-SAN. You see the first few data points gathered in the graphs and tables.

Managing a Cisco DCNM-SAN Server Fabric

You can continuously manage a Cisco DCNM-SAN Server fabric, whether or not a client has that fabric open. A continuously managed fabric is automatically reloaded and managed by Cisco DCNM-SAN Server whenever the server starts.

Selecting a Fabric to Manage Continuously

DETAILED STEPS

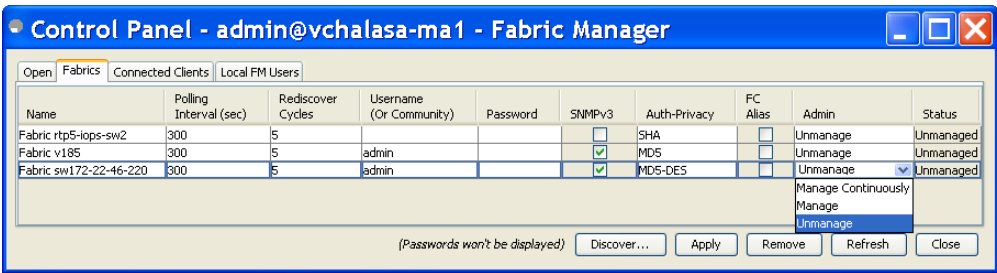
Step 1 Choose **Server > Admin**.

You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 5-5](#).



Note The Fabrics tab is only accessible to network administrators.

Figure 5-5 Fabrics Tab in Control Panel Dialog Box



Note You can preconfigure a user name and password to manage fabrics. In this instance, you should use a local switch account, not a TACACS+ server.

Step 2 Choose one of the following Admin options:

- a. **Manage Continuously**—The fabric is automatically managed when Cisco DCNM-SAN Server starts and continues to be managed until this option is changed to Unmanage.

- b. **Manage**—The fabric is managed by Cisco DCNM-SAN Server until there are no instances of DCNM-SAN viewing the fabric.
- c. **Unmanage**—Cisco DCNM-SAN Server stops managing this fabric.

Step 3 Click **Apply**.



Note

If you are collecting data on these fabrics using Performance Manager, you should now configure flows and define the data collections.

Cisco DCNM-SAN Server Properties File

The Cisco DCNM-SAN Server properties file (**MDS 9000\server.properties**) contains a list of properties that determine how the Cisco DCNM-SAN Server will function. You can edit this file with a text editor, or you can set the properties through the DCNM-SAN Web Services GUI, under the Admin tab.



Note

As of Cisco NX-OS Release 4.1(1b) and later, you can optionally encrypt the password in the **server.properties** and the **AAA.properties** files.

The server properties file contains these nine general sections:

- **GENERAL**—Contains the general settings for the server.
- **SNMP SPECIFIC**—Contains the settings for SNMP requests, responses, and traps.
- **SNMP PROXY SERVER SPECIFIC**—Contains the settings for SNMP proxy server configuration and TCP port designation.
- **GLOBAL FABRIC**—Contains the settings for fabrics, such as discovery and loading.
- **CLIENT SESSION**—Contains the settings for DCNM-SAN Clients that can log into the server.
- **EVENTS**—Contains the settings for syslog messages.
- **PERFORMANCE CHART**—Contains the settings for defining the end time to generate a Performance Manager chart.
- **EMC CALL HOME**—Contains the settings for the forwarding of traps as XML data using e-mail, according to EMC specifications.
- **EVENT FORWARD SETUP**—Contains the settings for forwarding events logged by Cisco DCNM-SAN Server through e-mail.

The following server properties are added or changed in the Cisco DCNM-SAN Release 3.x and later.

SNMP Specific

- **snmp.preferTCP**—If this option is set to true, TCP is the default protocol for Cisco DCNM-SAN Server to communicate with switches. By default, this setting is **true**. For those switches that do not have TCP enabled, Cisco DCNM-SAN Server uses UDP. The advantage of this setting is the ability to designate one TCP session for each SNMP user on a switch. It also helps to reduce timeouts and increase scalability.

**Note**

If you set this option to false, the same choice must be set in DCNM-SAN. The default value of `snmp.preferTCP` for DCNM-SAN is true.

Performance Chart

- **pmchart.currenttime**—Specifies the end time to generate a Performance Manager chart. This should only be used for debugging purposes.

EMC Call Home

- **server.callhome.enable**—Enables or disables EMC Call Home. By default, it is disabled.
- **server.callhome.location**—Specifies the Location parameter.
- **server.callhome.fromEmail**—Specifies the From Email list.
- **server.callhome.recipientEmail**—Specifies the recipientEmail list.
- **server.callhome.smtphost**—Specifies the SMTP host address for outbound e-mail.
- **server.callhome.xmlDir**—Specifies the path to store the XML message files.
- **server.callhome.connectType**—Specifies the method to use to remotely connect to the server.
- **server.callhome.accessType**—Specifies the method to use to establish remote communication with the server.
- **server.callhome.version**—Specifies the version number of the connection type.
- **server.callhome.routerIp**—Specifies the public IP address of the RSC router.

Event Forwarding

- **server.forward.event.enable**—Enables or disables event forwarding.
- **server.forward.email.fromAddress**—Specifies the From Email list.
- **server.forward.email.mailCC**—Specifies the CC Email list.
- **server.forward.email.mailBCC**—Specifies the BCC Email list.
- **server.forward.email.smtphost**—Specifies the SMTP host address for outbound e-mail.

Deactivation

- **deactivate.confirm=deactivate**—Specific Request for User to type a String for deactivation.

**Note**

In a federated server environment, you should not change Cisco DCNM-SAN Server properties by modifying `server.properties` file. You must modify the `server.properties` using web client menu **Admin > Configure > Preferences**.

Modifying Cisco DCNM-SAN Server

Fabric Manager Release 2.1(2) or later allows you to modify certain Cisco DCNM-SAN Server settings without stopping and starting the server.

- [Changing the Cisco DCNM-SAN Server Username and Password, page 5-11](#)
- [Changing the Cisco DCNM-SAN Server Username and Password, page 5-11](#)

- [Changing the DCNM-SAN Server Fabric Discovery Username and Password, page 5-11](#)
- [Changing the Polling Period and Fabric Rediscovery Time, page 5-12](#)
- [Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS WINDOWS Server, page 5-12](#)
- [Changing the IP Address of the Cisco DCNM-SAN for Federated Windows Setup, page 5-13](#)
- [Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS LINUX Server, page 5-14](#)
- [Using Device Aliases or FC Aliases, page 5-15](#)

Changing the Cisco DCNM-SAN Server Username and Password

You can modify the username or password used to access a fabric from DCNM-SAN Client without restarting Cisco DCNM-SAN Server.

DETAILED STEPS

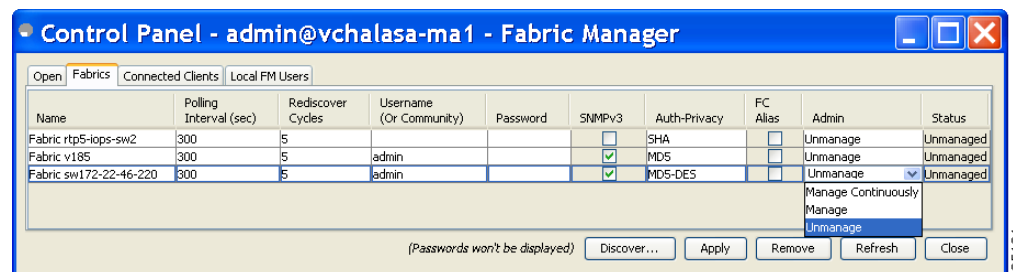
- Step 1** Choose **Server > Admin**.
- You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 5-5](#).
- Step 2** Set the Name or Password for each fabric that you are monitoring with Cisco DCNM-SAN Server.
- Step 3** Click **Apply** to save these changes.

Changing the DCNM-SAN Server Fabric Discovery Username and Password

DETAILED STEPS

- Step 1** Click **Server > Admin** in Cisco DCNM-SAN.
- You see the Control Panel dialog box with the Fabrics tab open (see [Figure 5-6](#)).

Figure 5-6 *Fabrics Tab in Control Panel Dialog Box*



- Step 2** Click the fabrics that have updated user name and password information.
- Step 3** From the Admin listbox, select **Unmanage** and then click **Apply**.
- Step 4** Enter the appropriate user name and password and then click **Apply**.

For more information, see the [“Performance Manager Authentication” section on page 6-3](#)”.

Changing the Polling Period and Fabric Rediscovery Time

Cisco DCNM-SAN Server periodically polls the monitored fabrics and periodically rediscovers the full fabric at a default interval of five cycles. You can modify these settings from DCNM-SAN Client without restarting Cisco DCNM-SAN Server.

DETAILED STEPS

-
- Step 1** Choose **Server > Admin**.
- You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 5-5](#).
- Step 2** For each fabric that you are monitoring with Cisco DCNM-SAN Server, set the Polling Interval to determine how frequently Cisco DCNM-SAN Server polls the fabric elements for status and statistics.
- Step 3** For each fabric that you are monitoring with Cisco DCNM-SAN Server, set the Rediscover Cycles to determine how often Cisco DCNM-SAN Server rediscovers the full fabric.
- Step 4** Click **Apply** to save these changes.
-

Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS WINDOWS Server

To change the IP address of a Cisco DCNM-SAN & DCNM-SMIS Server, follow these steps:



Note

To change the IP Address of a Cisco DCNM-LAN Server, see [Changing the IP Address of the Cisco DCNM-LAN for WINDOWS OS, page 13-9](#).

Detailed Steps

-
- Step 1** Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.
- Step 2** Change the old IP Address with the new IP Address in the following files
- *\$INSTALLDIR\jboss-as-7.2.0.Final\bin\service\sanservice.bat*
 - *\$INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-san.xml(Including DB url)*
 - *\$INSTALLDIR\fm\conf\server.properties*
- Step 3** Enter the following command to assign a new IP address.
- ```
run $INSTALLDIR\fm\bin\PLMapping.bat -p newipaddress 0
```
- Assume \$INSTALLDIR is the top directory of DCNM installation. The above command is for single server instance, where 0 is the server ID.
- Step 4** Change the old IP Address with the new IP Address in the file *\$INSTALLDIR\fm\conf\smis.properties*



**Step 5** Start the Cisco DCNM-SAN and DCNM-SMIS Servers.

---

## Changing the IP Address of the Cisco DCNM-SAN for Federated Windows Setup

To change the IP address of a Cisco DCNM-SAN for federated Windows OS, follow these steps:

- [Changing the IP address of primary server](#)
- [Changing the IP address of secondary server](#)

### Changing the IP address of primary server

- 
- Step 1** Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.
- Step 2** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\jboss-as-7.2.0.Final\bin\service\sanservice.bat
- Step 3** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-san.xml.
- Step 4** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\fm\conf\server.properties



**Note** If DB is installed locally(URL pointing to LocalHost),No DB URL change required in standalone-san.xml , server.properties .

---

- Step 5** Enter the following command to assign a new IP address.  
run \$INSTALLDIR\fm\bin\PLMapping.bat -p newipaddress 0  
Assume \$INSTALLDIR is the top directory of DCNM installation. The above command is for primary server instance, where 0 is the server ID.
- Step 6** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\fm\conf\smis.properties
- Step 7** Start the Cisco DCNM-SAN and DCNM-SMIS Servers.
- 

### Changing the IP address of secondary server

- 
- Step 1** Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.
- Step 2** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\jboss-as-7.2.0.Final\bin\service\sanservice.bat
- Step 3** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-san.xml
- Step 4** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\fm\conf\server.properties.
- Step 5** Change DB URL in standalone-san.xml, server.properties, postgresql.cfg.xml\ oracle.cfg.xml files, if there is ipaddress change in primary server.



postgresql.cfg.xml\ oracle.cfg.xml can be found under \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\conf\ directory.

**Step 6** Enter the following command to assign a new IP address.

```
run $INSTALLDIR\fm\bin\PLMapping.bat -p newipaddress 1 .
```



**Note** ServerID can be got by run \$INSTALLDIR\fm\bin\PLMapping.bat -show.

Assume \$INSTALLDIR is the top directory of DCNM installation. The above command 1 is the server ID.

**Step 7** Change the old IP Address with the new IP Address in the file \$INSTALLDIR\fm\conf\smis.properties

**Step 8** Start the Cisco DCNM-SAN and DCNM-SMIS Servers.

## Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS LINUX Server

To change the IP address of a Cisco DCNM-SAN & DCNM-SMIS Server, follow these steps:



**Note**

To change the IP Address of a Cisco DCNM-LAN Server, see [Changing the IP Address of the Cisco DCNM-LAN on Linux OS, page 13-10](#).

### Detailed Steps

**Step 1** Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.

**Step 2** Change the old IP Address with the new IP Address in the following files:

- *\$INSTALLDIR/jboss-as-7.2.0.Final/bin/init.d/sanservice.sh*
- */etc/init.d/FMServer*
- *\$INSTALLDIR/jboss-as-7.2.0.Final/standalone/configuration/standalone-san.xml (Including DB url)*
- *\$INSTALLDIR/fm/conf/server.properties*

**Step 3** Enter the following command to assign a new IP address.

```
run $INSTALLDIR/fm/bin/PLMapping.bat -p newipaddress 0
```

Assume \$INSTALLDIR is the top directory of DCNM installation. The above command is for single server instance, where 0 is the server ID.

**Step 4** Change the old IP Address with the new IP Address in the file \$INSTALLDIR/fm/conf\smis.properties.



**Note**

If this is a DCNM virtual appliance (OVA/ISO) deployed without any Fabric enhancements, update the property DCNM\_IP\_ADDRESS in the file */root/packaged-files/properties/installer.properties* with the new IP Address.



- Step 5** Start the Cisco DCNM-SAN and DCNM-SMIS Servers.
- 

## Using Device Aliases or FC Aliases

You can change whether DCNM-SAN uses FC aliases or global device aliases from DCNM-SAN Client without restarting Cisco DCNM-SAN Server.

### DETAILED STEPS

- 
- Step 1** Choose **Server > Admin**.
- You see the Control Panel dialog box with the Fabrics tab open as shown in [Figure 5-5](#).
- Step 2** For each fabric that you are monitoring with Cisco DCNM-SAN Server, check or uncheck the **FC Alias** check box.
- If you check the **FC Alias** checkbox, DCNM-SAN will use FC Alias from DCNM-SAN Client. If you uncheck the **FC Alias** checkbox, DCNM-SAN will use global device alias from DCNM-SAN Client.
- Step 3** Click **Apply** to save these changes.
- 

## Configuring Security Manager

The security at Fabric Manager Server level control access to different features of the Fabric Manager. The existing security controls in the Fabric Manager allows a user to continue even after many unsuccessful login attempts. With the new security manager, the Fabric Manager will perform a lock-out for the specific user after a specified number of unsuccessful login attempts. System administrators will be able to generate a report of login attempts.

To see the number of failed login attempts, follow these steps:

- 
- Step 1** In the Fabric Manager Control Panel, click **Local FM Users**.
- You see the control panel as show in [Figure 5-7](#)

**Figure 5-7**      *Number*

- Step 2**



## Step 3

## Server Federation

Server Federation is a distributed system that includes a collection of intercommunicated servers or computers that is utilized as a single, unified computing resource. With Cisco DCNM-SAN Server Federation, you can communicate with multiple servers together in order to provide scalability and easy manageability of data and programs running within the federation. The core of server federation includes several functional units such as Cisco DCNM-SAN Server, embedded web servers, database and DCNM-SAN Client that accesses the servers.

The Cisco DCNM-SAN Server in the federation uses the same database to store and retrieve data. The database is shared among different servers to share common information. A DCNM-SAN Client or DCNM-SAN Web Client can open fabrics from the Cisco DCNM-SAN Server using the mapping table. A fabric can be moved from one logical server to another. A logical server also can be moved from one physical machine to another machine.

## Restrictions

- You cannot upgrade more than one Cisco DCNM-SAN Server in an existing federation. If you choose to do so, you may not be able to migrate the Performance Manager statistics and other information on that server.
- You may require to synchronize the time on all the DCNM-SAN Servers in a federated server environment.

## Mapping Fabric ID to Server ID

The IP address of the physical server will be mapped to the server ID during the installation of the Cisco DCNM-SAN Server whenever the IP address of the physical server is changed, you need to map the IP address to the server ID using the PLMapping script provided with the Cisco DCNM-SAN Server. Whenever the you open or discover a fabric, the fabric ID will be mapped to the server ID . You can move a fabric to a different server ID using the control panel.

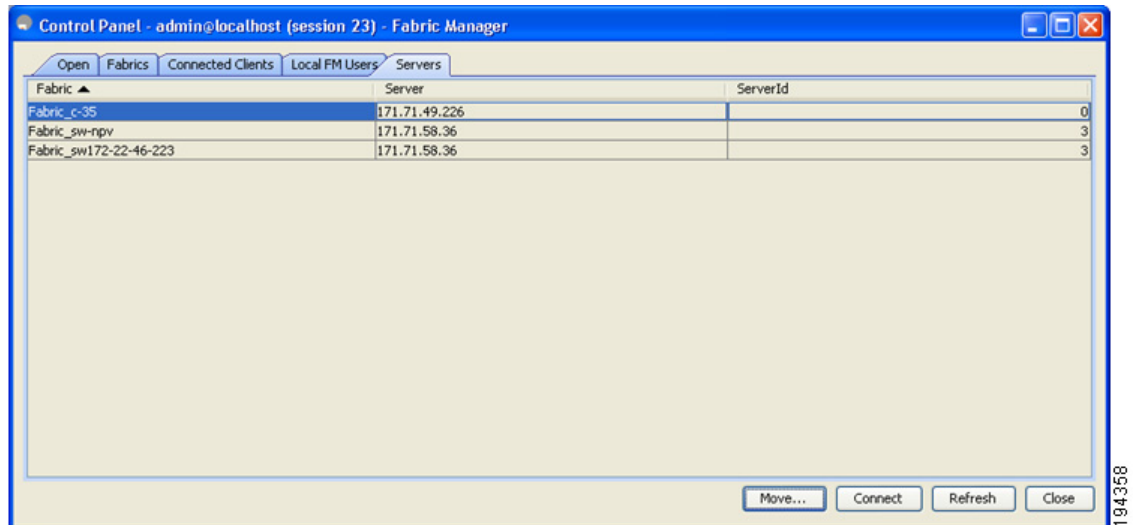
### DETAILED STEPS

---

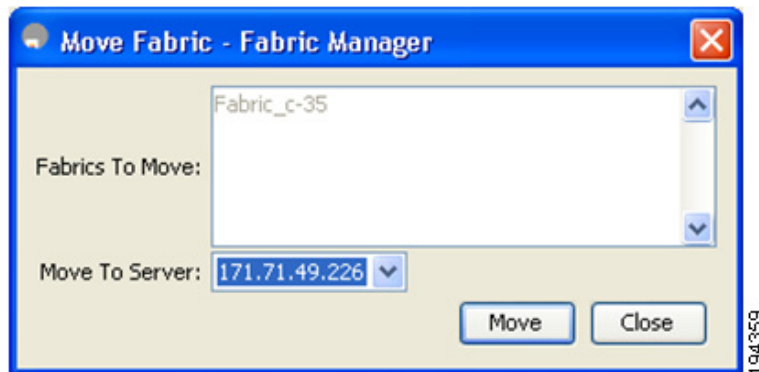
**Step 1** Choose **Server > Admin**.

You see the Control Panel as shown in [Figure 5-8](#).



**Figure 5-8 Control Panel**

- Step 2** Select the fabric that you want to move to a different server and then click **Move**.  
You see the Move Fabric dialog box as shown in [Figure 5-9](#).

**Figure 5-9 Move Fabric Dialog Box**

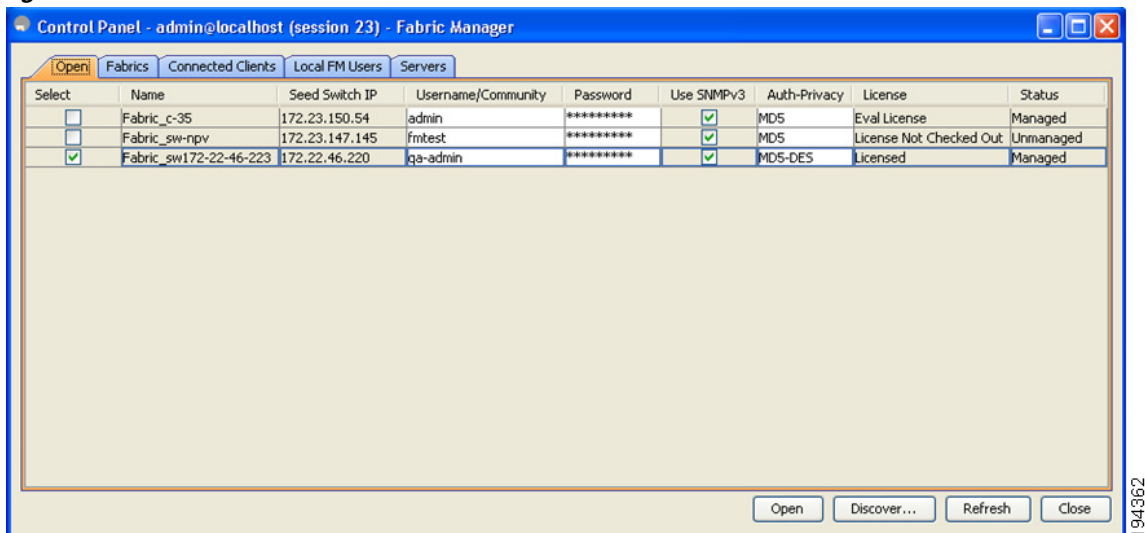
- Step 3** You see the fabrics that you selected in the Fabrics to Move list box. From the **Move To Server** drop-down list select the server you want to move the fabric to.
- Step 4** Click **Move**.

## Opening the Fabric on a Different Server

### DETAILED STEPS

- Step 1** Choose **Server > Admin**.  
You see the Control Panel as shown in [Figure 5-10](#).



**Figure 5-10 Control Panel**

**Step 2** Click **Discover**.

You see the Discover New Fabric dialog box as shown in Figure 5-11.

**Figure 5-11 Discover new Fabric**

**Step 3** In the Seed Switch list box, enter the IP Address of the seed switch.

**Step 4** In the User Name field, enter the username.

**Step 5** In the password field, enter the password.

**Step 6** From the Auth-Privacy drop-down list, choose the privacy protocol you want to apply.

**Step 7** To open the selected fabric in a different server, select the server ID from the Server drop-down list.

**Step 8** Click **Discover**.



**Note**

You may receive an error message when you discover a fabric in a federation while another Cisco DCNM-SAN Server is joining the federation. You can discover the fabric on after the installation or upgradation is complete.

## Viewing the Sessions in a Federation

### DETAILED STEPS

- Step 1** Choose **Server > Admin**.
- Step 2** Click the **Connected Clients** tab.
- You see the Control Panel as shown in [Figure 5-12](#).

**Figure 5-12 Connected Clients**

| SessionId | Client        | User  | Role          | Login               | Last Access         |
|-----------|---------------|-------|---------------|---------------------|---------------------|
| 43        | localhost     | admin | network-admin | 2009/02/06-14:32:06 | 2009/02/06-14:32:06 |
| 23        | localhost     | admin | network-admin | 2009/02/05-11:39:10 | 2009/02/05-11:39:10 |
| 33        | 171.71.58.117 | admin | network-admin | 2009/02/05-11:47:06 | 2009/02/05-11:47:06 |

## Viewing the Servers in a Federation

### DETAILED STEPS

- Step 1** Choose **Server > Admin**.
- Step 2** Click the **Servers** tab.
- You see the Control Panel as shown in [Figure 5-13](#).



## Discover Devices Managed by SVI

- Step 1** Log on to the DCNM Web Client.
- Step 2** Select **Admin>Server Properties**.
- Step 3** Scroll down to the **GENERAL->DATA SOURCE FABRIC** section.
- Step 4** Set the **fabric.managementIpOverwrite** property to **false**.
- Step 5** Click **Apply**.
- Step 6** Restart the DCNM service.



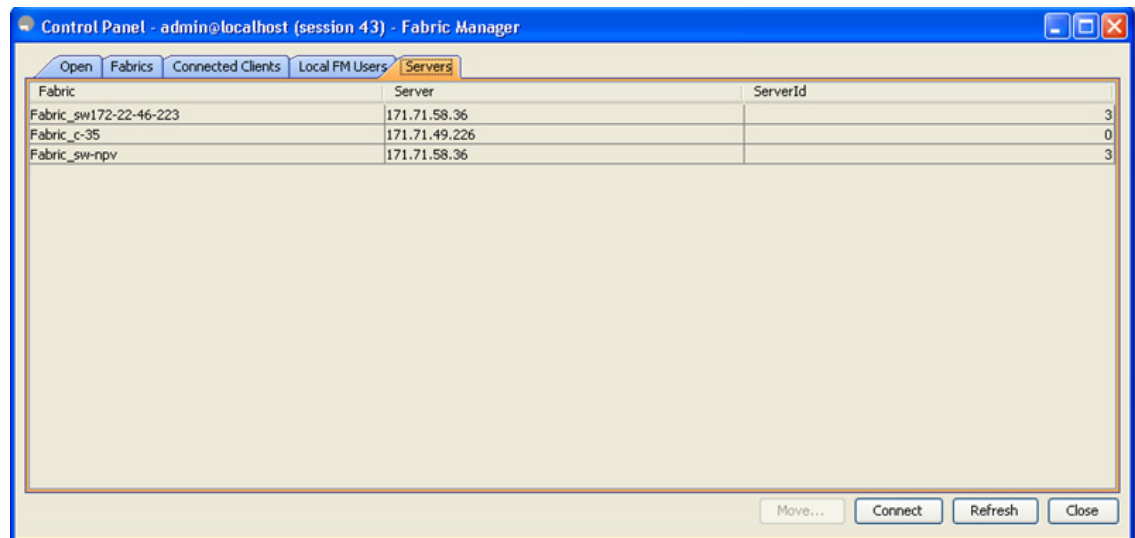
**Note** If you experiences technical issues using DCNM, you must restart the database service manually.

- Step 7** Delete any previously discovered switch that incorrectly shows the **mgmt0** IP address.
- Step 8** Retry the discovery.



**Note** Each SVI switch must be discovered separately.

**Figure 5-13 Servers**



## Additional References

- Server Federation is a licensed feature. For more information on Cisco DCNM-SAN Server Licensing, see *Cisco MDS 9000 Family NX-OS Licensing Guide*.
- For more information on deploying Cisco DCNM-SAN Server in a federation, see *Cisco Fabric Manager Server Federation Deployment Guide*.





## Configuring Authentication in Cisco DCNM-SAN

---

This chapter describes the interdependent software components in Cisco DCNM-SAN that communicate with the switches, authentication steps and the best practices for setting up your fabric and components for authentication.

This chapter contains the following sections:

- [Information About Cisco DCNM-SAN Authentication, page 6-1](#)
- [Best Practices for Discovering a Fabric, page 6-2](#)
- [Performance Manager Authentication, page 6-3](#)
- [Cisco DCNM-SAN Web Client Authentication, page 6-4](#)

### Information About Cisco DCNM-SAN Authentication

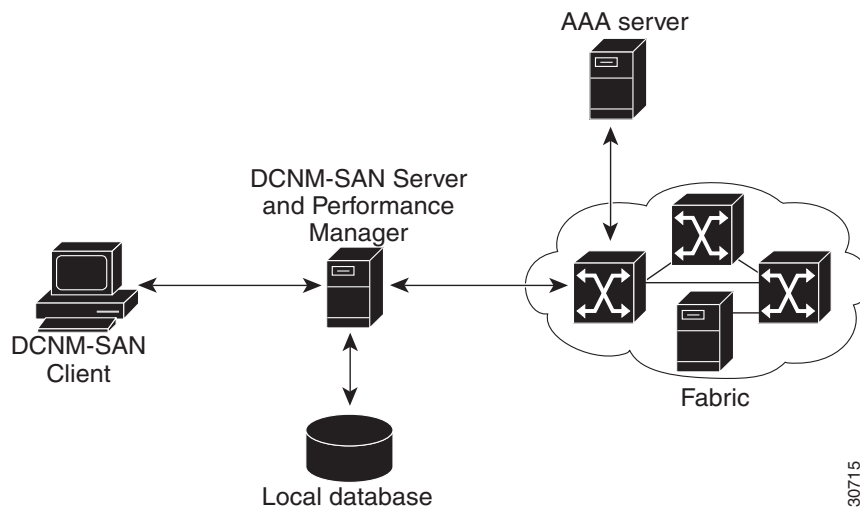
Cisco DCNM-SAN contains multiple components that interact to manage a fabric.

These components include:

- Cisco DCNM-SAN Client
- Cisco DCNM-SAN Server
- Performance Manager
- Interconnected fabric of Cisco MDS 9000 switches and storage devices
- AAA server (optional)

[Figure 6-1](#) shows an example configuration for these components.



**Figure 6-1 Cisco DCNM-SAN Authentication Example**

Administrators launch Cisco DCNM-SAN Client and select the seed switch that is used to discover the fabric. The user name and password used are passed to Cisco DCNM-SAN Server and used to authenticate to the seed switch. If this user name and password are not a recognized SNMP user name and password, either Cisco DCNM-SAN Client or Cisco DCNM-SAN Server opens a CLI session to the switch (SSH or Telnet) and retries the user name and password pair. If the user name and password are recognized by the switch in either the local switch authentication database or through a remote AAA server, then the switch creates a temporary SNMP user name that is used by Cisco DCNM-SAN Client and server.

**Note**

You may encounter a delay in authentication if you use a remote AAA server to authenticate Cisco DCNM-SAN or Device Manager.

**Note**

You must allow CLI sessions to pass through any firewall that exists between Cisco DCNM-SAN Client and Cisco DCNM-SAN Server.

**Note**

We recommend that you use the same password for the SNMPv3 user name authentication and privacy passwords as well as the matching CLI user name and password.

## Best Practices for Discovering a Fabric

Cisco DCNM-SAN Server monitors multiple physical fabrics under the same user interface. This facilitates managing redundant fabrics. A licensed Cisco DCNM-SAN Server maintains up-to-date discovery information on all configured fabrics so device status and interconnections are immediately available when you launch Cisco DCNM-SAN Client.

**Caution**

If the Cisco DCNM-SAN Server's CPU usage exceeds 50 percent, it is recommended that you switch to a higher CPU-class system.



We recommend that you use these best practices for discovering your network and setting up Performance Manager. This ensures that Cisco DCNM-SAN Server has a complete view of the fabric. Subsequent Cisco DCNM-SAN Client sessions can filter this complete view based on the privileges of the client logging in. For example, if you have multiple VSANs in your fabric and you create users that are limited to a subset of these VSANs, you want to initiate a fabric discovery through Cisco DCNM-SAN Server using a network administrator or network operator role so that Cisco DCNM-SAN Server has a view of all the VSANs in the fabric. When a VSAN-limited user launches Cisco DCNM-SAN Client, that user sees only the VSANs they are allowed to manage.

**Note**

Cisco DCNM-SAN Server should always monitor fabrics using a local switch account, do not use a AAA (RADIUS or TACACS+) server. You can use a AAA user account to log into the clients to provision fabric services.

**Note**

Even when remote AAA server authentication is enabled on the switch, use the local switch account that is not defined in the remote AAA server for fabric discovery. In other words, when a user is not found in the remote AAA server, then local switch user authentication will be allowed by the switch for SNMPv3 clients like DCNM.

## Setting Up Discovery for a Fabric

### DETAILED STEPS

- Step 1** Create a special Cisco DCNM-SAN administrative user name in each switch on your fabric with network administrator or network operator roles. Or, create a special Cisco DCNM-SAN administrative user name in your AAA server and set every switch in your fabric to use this AAA server for authentication.
- Step 2** Verify that the roles used by this Cisco DCNM-SAN administrative user name are the same on all switches in the fabric and that this role has access to all VSANs.
- Step 3** Launch Cisco DCNM-SAN Client using the Cisco DCNM-SAN administrative user. This step ensures that your fabric discovery includes all VSANs.
- Step 4** Set Cisco DCNM-SAN Server to continuously monitor the fabric.
- Step 5** Repeat [Step 4](#) for each fabric that you want to manage through Cisco DCNM-SAN Server.

## Performance Manager Authentication

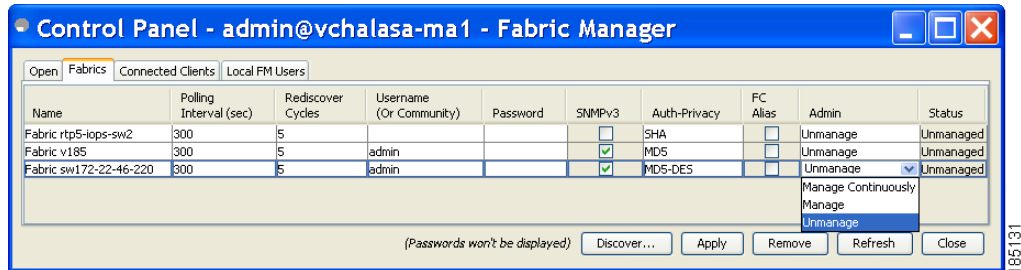
Performance Manager uses the user name and password information stored in the Cisco DCNM-SAN Server database. If this information changes on the switches in your fabric while Performance Manager is running, you need to update the Cisco DCNM-SAN Server database and restart Performance Manager. Updating the Cisco DCNM-SAN Server database requires removing the fabric from Cisco DCNM-SAN Server and rediscovering the fabric.



## DETAILED STEPS

- Step 1** Click **Server > Admin** in Cisco DCNM-SAN.  
You see the Control Panel dialog box with the Fabrics tab open (see [Figure 6-2](#)).

**Figure 6-2 Fabrics Tab in Control Panel Dialog Box**



- Step 2** Click the fabrics that have updated user name and password information.
- Step 3** From the Admin listbox, choose **Unmanage** and then click **Apply**.
- Step 4** Enter the appropriate user name and password and then click **Apply**.
- Step 5** From the Admin listbox, choose **Manage** and then click **Apply**.
- Step 6** To rediscover the fabric, click **Open** tab and check the check box(es) next to the fabric(s) you want to open in the Select column.
- Step 7** Click **Open** to rediscover the fabric. Cisco DCNM-SAN Server updates its user name and password information.
- Step 8** Repeat [Step 3](#) through [Step 7](#) for any fabric that you need to rediscover.
- Step 9** Choose **Performance > Collector > Restart** to restart Performance Manager and use the new user name and password.

## Cisco DCNM-SAN Web Client Authentication

Cisco DCNM-SAN Web Server does not communicate directly with any switches in the fabric. Cisco DCNM-SAN Web Server uses its own user name and password combination that is either stored locally or stored remotely on an AAA server.

We recommend that you use a RADIUS or TACACS+ server to authenticate users in Cisco DCNM-SAN Web Server.

## DETAILED STEPS

- Step 1** Launch Cisco DCNM-SAN Web Client.
- Step 2** Choose **Admin > Management Users > Remote AAA** to update the authentication used by Cisco DCNM-SAN Web Client.
- Step 3** Set the authentication mode attribute to **radius**.



- Step 4** Set the RADIUS server name, shared secret, authentication method, and ports used for up to three RADIUS servers.
- Step 5** Click **Modify** to save this information.
- 

- Step 1** Launch Cisco DCNM-SAN Web Client.
- Step 2** Choose **Admin > Management Users > Remote AAA** to update the authentication used by Cisco DCNM-SAN Web Client.
- Step 3** Set the authentication mode attribute to **tacacs**.
- Step 4** Set the TACACS+ server name, shared secret, authentication method, and port used for up to three TACACS+ servers.
- Step 5** Click **Modify** to save this information.
- 

**Note**

Cisco DCNM-SAN does not support SecureID because it is not compatible with SNMP authentication. Cisco DCNM-SAN uses the same login credentials for all the switches in a fabric. Since SecureID cannot be used more than once for authentication, Cisco DCNM-SAN will not be able to establish a connection to the second switch using a SecureID.

---









# Configuring Cisco DCNM-SAN Client

This chapter describes about the Cisco DCNM-SAN Client, which is a java-based GUI application that provides access to the Cisco DCNM-SAN applications from a remote workstation.

This chapter contains the following sections:

- [Information About DCNM-SAN Client, page 7-1](#)
- [Cisco DCNM-SAN Client Quick Tour: Server Admin Perspective, page 7-2](#)
- [Cisco DCNM-SAN Client Quick Tour: Admin Perspective, page 7-6](#)
- [Launching Cisco DCNM-SAN Client, page 7-25](#)
- [Setting Cisco DCNM-SAN Preferences, page 7-34](#)
- [Network Fabric Discovery, page 7-35](#)
- [Modifying the Device Grouping, page 7-38](#)
- [Controlling Administrator Access with Users and Roles, page 7-41](#)
- [Using Cisco DCNM-SAN Wizards, page 7-41](#)
- [Cisco DCNM-SAN Troubleshooting Tools, page 7-42](#)
- [Integrating Cisco DCNM-SAN and Data Center Network Management Software, page 7-42](#)

## Information About DCNM-SAN Client

Cisco DCNM-SAN is a Java and SNMP-based network fabric and device management tool with a GUI that displays real-time views of your network fabric, including Cisco Nexus 5000 Series switches, Cisco MDS 9000 Family and third-party switches, hosts, and storage devices.

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches, Cisco DCNM-SAN Client provides Fibre Channel troubleshooting tools. You can use these health and configuration analysis tools on the MDS 9000 Family switch or Cisco Nexus 5000 Series switch to perform Fibre Channel ping and traceroute.

Cisco DCNM-SAN Release 4.1(1b) and later provides multilevel security system by adding a *server admin* role that allows access to limited features. The configuration capabilities of a *server admin* is limited to FlexAttach and relevant data.



### Note

You must use the same release of Cisco DCNM-SAN Client and Cisco DCNM-SAN Server.



## Cisco DCNM-SAN Advanced Mode

Advanced mode is enabled by default and provides the full suite of Cisco DCNM-SAN features, including security, IVR, iSCSI, and FICON. To simplify the user interface, from the list box in the upper right corner of the Cisco DCNM-SAN Client, choose **Simple**. In simple mode, you can access basic MDS 9000 features such as VSANs, zoning, and configuring interfaces. Advanced mode option is not available for *server admin* role.

## Cisco DCNM-SAN Client Quick Tour: Server Admin Perspective

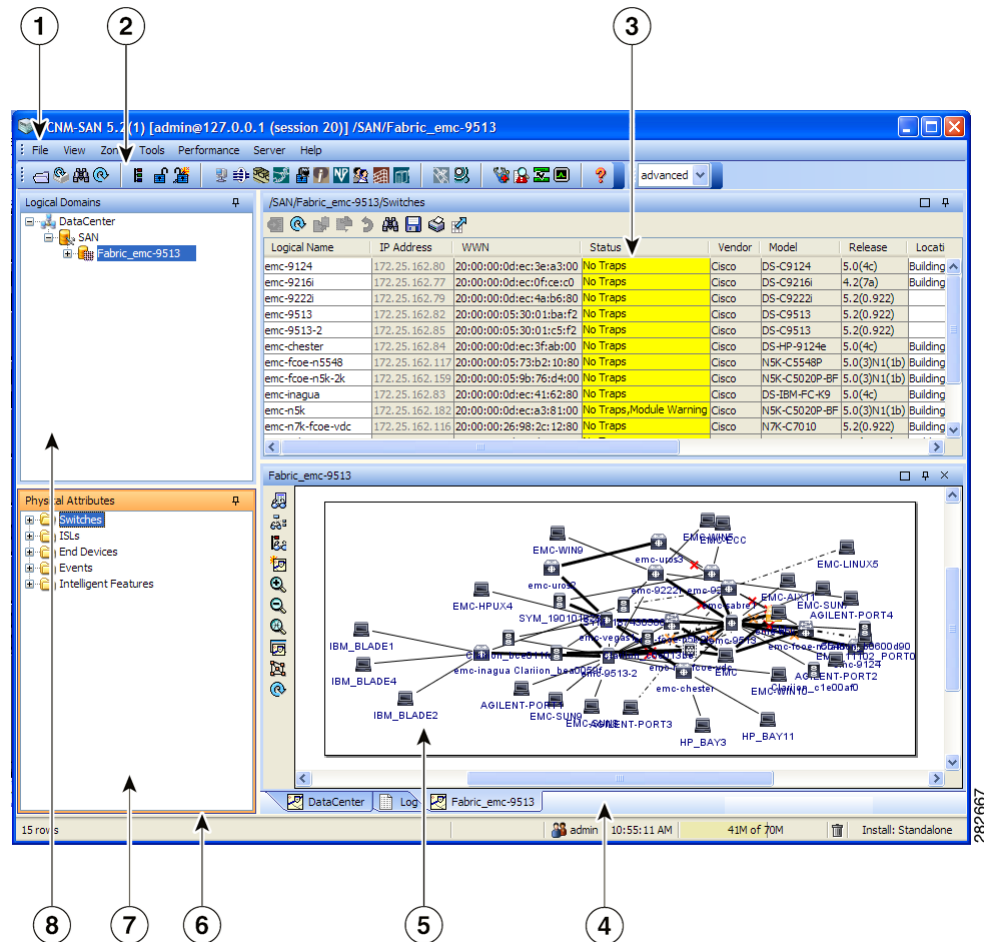
Cisco DCNM-SAN provides a multilevel security system by adding a *server admin* role that allows access only to limited features. The configuration capabilities of a *server admin* role is limited to FlexAttach and relevant data. The *server admin* can pre-configure SAN for new servers, move a server to another port on the same NPV device or another NPV device and replace a failed server onto the same port without involving the SAN administrator. The *server role admin* will not be able to manage Cisco DCNM-SAN users or connected clients.

Cisco DCNM-SAN provides a much improved user interface by including movable and dockable panes to let users arrange the Physical Attributes pane, Logical Domains pane, Fabric pane and Information pane according to requirements, making it easier to manage the workflow. The dockable panes are also called as dockable frames. A dockable frame can be standalone (floating), minimized or maximized. The logical, physical, information and the fabric panes can be collapsed and expanded as needed. These panes can also be docked at either the right side left side or to the bottom of the workspace.

## Cisco DCNM-SAN Main Window

This section describes the Cisco DCNM-SAN Client interface that is specific to *server admin* users as shown in [Figure 7-1](#).



**Figure 7-1 Cisco DCNM-SAN Main Window: Server Admin Perspective**

|   |                                                                                                                                                                                    |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Menu bar—Provides access to options that are organized by menus.                                                                                                                   |
| 2 | Toolbar—Provides icons for direct access to the most commonly used options on the File, Tools, and Help menus.                                                                     |
| 3 | Information pane—Displays information about whatever option is selected in the menu tree.                                                                                          |
| 4 | Status Bar (right side)—Shows the last entry displayed by the discovery process and the possible error message.                                                                    |
| 5 | Fabric pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.                                 |
| 6 | Status Bar (left side)—Shows short-term transient messages, such as the number of rows displayed in a table.                                                                       |
| 7 | Physical Attributes pane—Displays a tree of available configuration tasks depending on the fabric, VSAN, or zone selected previously. Lists the switches in the logical selection. |
| 8 | Logical Domains pane—Displays a tree of configured SAN, fabrics and user-defined groups.                                                                                           |



## Menu Bar





The menu bar at the top of the Cisco DCNM-SAN main window provides options for managing and for controlling the display of information on the Fabric pane. *Server admin* will not have all the options that are available for *SAN admin*. The menu bar provides the following menus:

- **File**—Opens a new fabric, rediscovers the current fabric, locates switches, sets preferences, prints the map.
- **View**—Changes the appearance of the map (these options are duplicated on the Fabric pane toolbar).
- **Tools**—Manages the Server and configuration using the FlexAttach virtual pWWN feature.
- **Help**—Displays online help topics for specific dialog boxes in the Information pane.

## Tool Bar

The Cisco DCNM-SAN main toolbar (specific to *server admin*) provides icons for accessing the most commonly used menu bar options as shown in [Table 7-1](#).

**Table 7-1 Cisco DCNM-SAN Client Main Toolbar**

| Icon                                                                                | Description                 |
|-------------------------------------------------------------------------------------|-----------------------------|
|   | Opens switch fabric.        |
|  | Rediscovers current fabric. |
|  | Finds in the map.           |
|  | Shows online help.          |

## Logical Domains Pane

Use the Logical Domains pane to view fabrics and to access user-defined groups. You can expand the groups to see different user-defined groups. The non-editable groups created for each core switch contains their NPV switches.

## Physical Attributes Pane

Use the Physical Attributes pane to display a tree of the options available for managing the switches in the currently selected fabric or group.












To select an option, click a folder to display the options available and then click the option. You see the table with information for the selected option in the Information pane. The Physical Attributes pane provides the following main folders:

- Switches—Views and configures hardware, system, licensing, and configuration files.
- Interfaces—Views and configures FC physical, FC logical, VFC (FCoE), Ethernet, SVC, and PortChannel interfaces.

## Information Pane

Use the Information pane to display tables of information associated with the option selected from the menu tree in the Logical Domains or Physical Attributes panes. The Information pane toolbar provides buttons for performing one or more of the operations shown in Table 5-2.

**Table 7-2 Information Pane Toolbar**

| Icons                                                                               | Description                                                                                                                |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
|    | Applies configuration changes.                                                                                             |
|   | Refreshes table values.                                                                                                    |
|  | Copies data from one row to another.                                                                                       |
|  | Pastes the data from one row to another.                                                                                   |
|  | Undoes the most recent change.                                                                                             |
|  | Finds a specified string in the table.                                                                                     |
|  | Exports and saves information to a file.                                                                                   |
|  | Prints the contents of the Information pane.                                                                               |
|  | Displays a non-editable copy of the table in the Information pane in its own window, which you can move around the screen. |



## Fabric Pane

Use the Fabric pane to display the graphical representation of your fabric. Table 5-1 explains the graphics you may see displayed, depending on which devices you have in your fabric.

The bottom of the Fabric pane has the following tabs:

- Fabric—When displaying multiple fabrics, each fabric has its own tab. You can switch between fabrics by clicking on their respective tabs.
- Log—Displays messages that describe Cisco DCNM-SAN operations, such as fabric discovery. .

**Note**

Fabric map display is based on what you select in the logical domain pane. When you select a fabric node, all the switches that belong to that fabric will be enabled. When you select the group node, all the switches that belong to the groups listed under that group node will be enabled. When you select only a group, all the switches that belong to the specific group will be enabled.

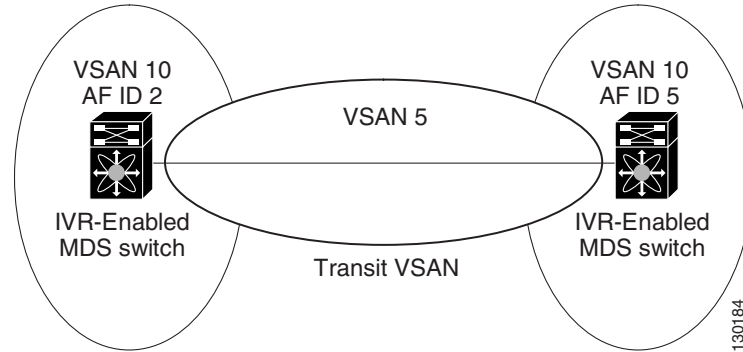
**Note**

You can view information about Events using the DCNM Web Client.

## Cisco DCNM-SAN Client Quick Tour: Admin Perspective

This section describes the Cisco DCNM-SAN Client interface shown in [Figure 7-2](#).



**Figure 7-2 Cisco DCNM-SAN Main Window**

|          |                                                                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b> | Menu bar—Provides access to options that are organized by menus.                                                                                                                                      |
| <b>2</b> | Toolbar—Provides icons for direct access to the most commonly used options on the File, Tools, and Help menus.                                                                                        |
| <b>3</b> | Information pane—Displays information about whatever option is selected in the menu tree.                                                                                                             |
| <b>4</b> | Status Bar (right side)—Shows the last entry displayed by the discovery process and the possible error message.                                                                                       |
| <b>5</b> | Fabric pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.                                                    |
| <b>6</b> | Status Bar (left side)—Shows short-term transient messages, such as the number of rows displayed in a table.                                                                                          |
| <b>7</b> | Physical Attributes pane—Displays a tree of available configuration tasks depending on the fabric, VSAN, or zone selected previously. Lists the switches and end devices in the logical selection.    |
| <b>8</b> | Logical Domains pane—Displays a tree of configured SAN, fabrics, VSANs, and zones, and provides access to user-defined groups. The label next to the segmented VSAN indicates the number of segments. |



**Note**

You can resize each pane by dragging the boundaries between each region or by clicking the **Minimize** or **Maximize** controls.

## Menu Bar

The menu bar at the top of the Cisco DCNM-SAN main window provides options for managing and troubleshooting the current fabric and for controlling the display of information on the Fabric pane. The menu bar provides the following menus:

- **File**—Opens a new fabric, rediscovers the current fabric, locates switches, sets preferences, prints the map, and exports the Fabric pane log.
- **View**—Changes the appearance of the map (these options are duplicated on the Fabric pane toolbar).
- **Zone**—Manages zones, zone sets, and inter-VSAN routing (IVR).
- **Tools**—Verifies and troubleshoots connectivity and configuration, as described in the “[Cisco DCNM-SAN Troubleshooting Tools](#)” section on page 7-42.
- **Performance**—Runs and configures Performance Manager and Cisco Traffic Analyzer, and generates reports.
- **Server**—Runs administrative tasks on clients and fabrics. Provides Cisco DCNM-SAN Server management and a **purge** command. Lists fabrics being managed.
- **Help**—Displays online help topics for specific dialog boxes in the Information pane.

## File

The file menu provides the following options:

- **Open Fabric**—Opens a new switch fabric.
- **Locate Switches and Devices**— Uses the SNMPv2 protocol to discover devices responding to SNMP requests with the read-only community string public. You may use this feature if you want to locate other Cisco MDS 9000 switches in the subnet, but are not physically connected to the fabric.
- **Rediscover**—Initiates an on-demand discovery to learn recent changes from the switches and update the Cisco DCNM-SAN Client. You may use this option when Cisco DCNM-SAN Server is not in sync with switches in the fabric and you do not want to wait until the next polling cycle. The rediscover option does not delete the fabric and add it again. You may delete and add the fabric only if the rediscover option fails to update Cisco DCNM-SAN Server.
- **Resync All Open Fabrics**— Cisco DCNM-SAN Server forces all the fabrics to close and re-open. You may use this option when Cisco DCNM-SAN Client is not in sync with Cisco DCNM-SAN Server.
- **Rediscover SCSI Targets**— Initiates an on-demand discovery to learn recent changes from the SCSI target switches. You may use this option when Cisco DCNM-SAN Server is not in sync with SCSI target switches in the fabric and you do not want to wait until the next polling cycle.
- **Preferences**—Sets your preferences to customize the behavior of the Cisco DCNM-SAN Client.
- **Import Enclosures**—Imports saved enclosures.
- **Export**
  - **Map Image**—Generates and export the map to a specified location.



- Visio—Exports the map to a Visio file.
  - Table—Exports the table data to a text file.
  - Log—Exports the log to a text file.
  - Events—Exports the events to a text file.
  - Enclosures—Exports the enclosure values to a text file.
- Print —Prints the map.
- Exit—Exit Cisco DCNM-SAN.

## View

View menu provides the following options:

- Refresh Map—Refreshes the current map.
- Layout
  - Cancel—Cancels the current layout.
  - Spring—Displays the layout based on spring algorithm.
  - Quick—Quickly displays the layout when the switch has many end devices.
- Zoom
  - In—Zooms in the view.
  - Out—Zooms out the view.
  - Fit—Fits the view in the fabric pane.
- Grid—Enables the grid view.
- Overview Window—Allows you to center the Fabric pane on the area of the fabric that you want to see. This option is useful for large fabrics that cannot be displayed entirely within the Fabric pane.
- Legend—Shows all the legends used in the fabric map.
- Find in Map—Finds a device in the fabric map.

## Zone

The zone menu provides the following options:

- Edit Local Full Zone Database—Allows you to create zones across multiple switches. Zones provide a mechanism for specifying access control. Zone sets are a group of zones to enforce access control in the fabric. All zoning features are available through the Edit Local Full Zone Database dialog box.
- Deactivate Zoneset—Deactivates an active zone set.
- Copy Full Zone Database—Creates a new zone set. On the Cisco MDS Family switches, you cannot edit an active zone set. However, you can copy an active zone set to create a new zone set that you can edit.
- Merge Analysis—Enables you to determine if zones will merge successfully when two Cisco MDS switches are interconnected. If the interconnected switch ports allow VSANs with identical names or contain zones with identical names, then Cisco DCNM-SAN verifies that the zones contain identical members. You can use merge analysis tool before attempting a merge, or after fabrics are interconnected to determine zone merge failure causes.



- Merge Fail Recovery—Recovers the port from its isolated state either by importing the neighboring switch's active zone set database and replacing the current active or by exporting the current database to the neighboring switch.
- Migrate Non-MDS Database—Migrate a non-MDS database using Cisco DCNM-SAN (you may need to use the Zone Migration Wizard to accomplish this task).
- IVR
  - Deactivate Zoneset—Deactivates an active zone set.
  - Copy Full Zone Database—Recovers an IVR zone database by copying the IVR full zone database from another switch.
  - Copy Full Topology—Recovers a topology by copying from the active zone database or the full zone database.

## Tools

Tools menu provides the following options:

- Health
  - Switch Health—Determines the status of the components of a specific switch.
  - Fabric Configuration—Analyzes the configuration of a switch by comparing the current configuration to a specific switch or to a policy file. You can save a switch configuration to a file and then compare all switches against the configuration in the file.
  - Show Tech Support—Collects large amount of information about your switch for troubleshooting purposes. When you issue a **show tech support** command from Cisco DCNM-SAN for one or more switches in a fabric, the results of each command are written to a text file, one file per switch, in a directory you specify. You can then view these files using Cisco DCNM-SAN.
- Connectivity
  - End to End Connectivity—Determines connectivity and routes among devices with the switch fabric. This tool checks to see that every pair of end devices can talk to each other, using a Ping test and by determining if they are in the same VSAN or in the same active zone.
  - Ping—Determines connectivity from another switch to a port on your switch.
  - Trace Route—Verifies connectivity between two end devices that are currently selected on the Fabric pane.
  - Compact Flash Report—Automatically scans the fabric and generate a report that shows the status of CompactFlash.
- NPV
  - CFS Static Peer Setup—Manage the peer list used during CFS on NPV-enabled switches. After setting up the static peers list, the CFS discovery on the switches will be changed to static mode for all peers in the list. Cisco DCNM-SAN does not automatically update static peers list. You may need to update the list using the CFS Static Peer Setup Wizard when a new switch is added to the fabric.
  - Traffic Map Setup—Configures the list of external interfaces to the servers, and enabling or disabling disruptive load balancing. Using Traffic Map Setup you can specify the external ports that a server should use for traffic management.



- Flex Attach Pre-Configure Server—Sets the port configurations for all the ports in a switch such as enabling or disabling FlexAttach, setting the default VSAN ID, and setting the interface status.
  - Flex Attach Move Server—Moves a server to another port on the same NPV device or another NPV device without changing the SAN.
  - Flex Attach Replace Server—Replaces a failed server with a new server on the same port without changing the SAN.
- Data Mobility Manager
  - Server Based—Performs server-based data migration.
  - Storage based—Performs storage-based data migration.
  - Server LUN Discovery—Performs LUN discovery to select the LUNs available for migration and automates the session creation by matching the LUNs in the existing and new storage.
- FCoE—Launches the FCoE Configuration Wizard to create virtual Fibre Channel interfaces.
- Port Channel—Creates PortChannels from selected ISL either manually or automatically.
- DPVM Setup—Establishes dynamic port VSAN membership, enables autolearning, and activates the DPVM database.
- IP SAN
  - FCIP Tunnel—Creates FCIP links between Gigabit Ethernet ports. Enables Fibre Channel write acceleration and IP compression.
  - iSCSI Setup—Creates zones for iSCSI initiators and adds a VSAN to a target-allowed VSAN list.
  - SAN Extension Tuner—Optimizes FCIP performance by generating either direct access (magnetic disk) or sequential access (magnetic tape) SCSI I/O commands and directing such traffic to a specific virtual target. This option is used to generate SCSI I/O commands (read and write) to the virtual target based on your configured options.
- Security
  - Port Security—Prevents unauthorized access to a switch port in the Cisco MDS 9000 Family, rejects intrusion attempts and reports these intrusions to the administrator.
  - IP ACL—Creates an ordered list of IP filters in a named IPv4-ACL or IPv6-ACL profile using the IPv4-ACL Wizard.
- Install
  - License—Facilitate download and installation of licenses in selected switches in the fabric.
  - Software—Verifies image compatibility and installs software images on selected switches in the fabric.
- Flow Load Balance Calculator—Allows you to get the best load-balancing configuration for your FICON flows. The calculator does not rely on any switch or flow discovery in the fabric.
- Device Manager—Invokes Device Manager for a switch.
- Command Line Interface —Enables command-line operations.
- Run CLI Commands—Runs command-line operations on more than one switch at a time.

## Performance

The performance menu provides the following options:



- Create Flows—Creates host-to-storage, storage-to-host, or bidirectional flows. You can add these flows to a collection configuration file to monitor the traffic between a host or storage element pair.

## Server

The server menu provides the following options:

- Admin—Opens the control panel.
- Purge Down Elements—Purges all down elements in the fabric.

## Help








The help menu provides the following options:

- Contents —Launches the online help contents.
- Config Guide—Launches the Cisco DCNM-SAN Configuration Guide.
- About—Displays information about Cisco DCNM-SAN.

## Toolbar















The Cisco DCNM-SAN main toolbar provides icons for accessing the most commonly used menu bar options as shown in [Table 7-3](#).

**Table 7-3** Cisco DCNM-SAN Client Main Toolbar

| Icon                                                                                | Description                    |
|-------------------------------------------------------------------------------------|--------------------------------|
|  | Opens switch fabric.           |
|  | Rediscovered current fabric.   |
|  | Finds in the map.              |
|  | Creates VSAN.                  |
|  | Launches DPVM wizard.          |
|  | Launches Port Security wizard. |
|  | Edits full zone database.      |





**Table 7-3 Cisco DCNM-SAN Client Main Toolbar (continued)**

| Icon                                                                                | Description                                |
|-------------------------------------------------------------------------------------|--------------------------------------------|
|    | Launches IVR zone wizard.                  |
|    | Launches the FCoE configuration wizard.    |
|    | Launches PortChannel wizard.               |
|    | Launches FCIP wizard.                      |
|    | Launches iSCSI wizard.                     |
|    | Launches NPVM wizard.                      |
|  | Launches QoS wizard.                       |
|  | Configures users and roles.                |
|  | Launches IP-ACL wizard.                    |
|  | Launches License Install wizard.           |
|  | Launches Software Install wizard.          |
|  | Performs switch health analysis.           |
|  | Performs fabric configuration analysis.    |
|  | Performs end-to-end connectivity analysis. |



**Table 7-3** *Cisco DCNM-SAN Client Main Toolbar (continued)*

| Icon                                                                              | Description                                                                                                                          |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
|  | Monitors ISL performance. Brings up real-time ISL performance information for all interfaces in the fabric, in the Information pane. |
|  | Shows online help.                                                                                                                   |

## Logical Domains Pane

Use the Logical Domains pane to manage attributes for fabrics, VSANs, and zones, and to access user-defined groups. Starting from NX-OS Release 4.2(0), SAN and LAN nodes are listed under Datacenter node and all the fabrics are listed under SAN node. When you select Datacenter node in the tree, Cisco DCNM-SAN displays all the switches and ISLs. When you select LAN node, Cisco DCNM-SAN displays only Ethernet switches and Ethernet links. Under the fabric node, VSANs are ordered by a VSAN ID. The segmented VSANs are placed under the fabric node. The label next to the segmented VSAN indicates the number of segments. You can expand a segmented VSAN and the segments under that VSAN. Right-click one of the folders in the tree and click a menu item from the pop-up menu. You see the appropriate configuration dialog box.

The default name for the fabric is the name, IP address, or WWN for the principal switch in VSAN 1. If VSAN 1 is segmented, the default name is chosen from a principal switch with the smallest WWN. The fabric names you see are as follows:

- Fabric <sysName>
- Fabric <ipAddress>
- Fabric <sWWN>

You can change the fabric name using Cisco DCNM-SAN.

### DETAILED STEPS

- 
- |               |                                                                            |
|---------------|----------------------------------------------------------------------------|
| <b>Step 1</b> | Choose <b>Server &gt; Admin</b> .<br>You see the Control Panel dialog box. |
| <b>Step 2</b> | Double-click the fabric name and enter the new name of the fabric.         |
| <b>Step 3</b> | Click <b>Apply</b> to change the name.                                     |
- 

## Filtering

Cisco DCNM-SAN has a filtering mechanism that displays only the data that you are interested in. To filter, first select the fabric and VSAN from the Logical Domains pane. This action narrows the scope of what is displayed in the Fabric pane. Any information that does not belong to the selected items is dimmed. Also, any information that does not belong to the selected items is not displayed in the tables in the Information pane. The filter that you select is displayed at the top right of the Cisco DCNM-SAN window.



To further narrow the scope, select attributes from the Physical Attributes pane. The Cisco DCNM-SAN table, display, and filter criteria change accordingly.

## Physical Attributes Pane

Use the Physical Attributes pane to display a tree of the options available for managing the switches in the currently selected fabric, VSAN, or zone.

To select an option, click a folder to display the options available and then click the option. You see the table with information for the selected option in the Information pane. The Physical Attributes pane provides the following main folders:

- Switches—Views and configures hardware, system, licensing, and configuration files.
- Interfaces—Views and configures FC physical, FC logical, VFC (FCoE), Ethernet, SVC, and PortChannel interfaces.
- FC Services—Views and configures Fibre Channel network configurations.
- IP—Views and configures IP storage and IP services.
- Security—Views and configures MDS management and FC-SP security.
- FCoE—Views and configures FCoE interfaces.
- ISLs—Views and configures Inter-Switch Links.
- End Devices—Views and configures end devices.



### Note

You cannot view the detailed physical attributes of the data center switches or monitor the connections. When you select either a data center node or a LAN node the physical attributes pane will be blank.

## Context Menu for Tables

When you right-click in the table, you see a pop-up menu with options that vary depending on the type of option you selected in the Physical Attributes pane. You can perform various operations by right-clicking the device listed in the table. To view various options available for switches, ISLs, and end devices, refer to the procedures in the sections that follows:

### Viewing Switch Options

When you select the datacenter node, the switch table displays all the switches that are discovered. When you select the SAN node or the fabric node, the switch table displays all the Fibre Channel switches and when you select the LAN node, the switch table displays all the Ethernet switches.

## DETAILED STEPS

**Step 1** Click **Switches** in the Physical Attributes pane.

**Step 2** Right-click the device in the table.

The pop-up menu provides the following options:

- Apply Changes—Applies the changes to the switch.
- Refresh Values—Refreshes the current values.



- Undo Changes—Undoes modifications to the switch.
  - Export to File—Export the values to a file.
  - Print Table—Prints the table.
  - Detach Table—Detaches the table.
  - Switch Attributes—Changes the switch properties.
  - Interface Attributes—Changes the interface properties.
  - Element Manager—Manages this switch.
  - Command Line Interface—Enables to perform command line operations.
  - Copy—Copies the switch.
  - Purge—Purges the switch.
  - Fix Location—Fixes the switch in the current location.
  - Align—Aligns the switch.
  - Show End Devices—Shows the end devices.
  - Expand Multiple Links—Expands the links to this switch.
  - Other—Other options.
  - Group—Groups switches.
- 

## Viewing ISL Options

When you select the data center node, the ISLs table displays all of the Fibre Channel and Ethernet links. When you select the LAN node, the ISLs table displays all the Ethernet links.

## DETAILED STEPS

---

**Step 1** In the Physical Attributes pane, click **ISLs** and then click **Summary** tab.

**Step 2** Right-click the device in the table.

The pop-up menu provides the following options:

- Refresh Values—Refreshes the current values.
- Copy—Copies information from a specific field.
- Find—Conducts search based on the input string.
- Export to File—Exports the values to a file.
- Print Table—Prints the table.
- Detach Table—Detaches the table.
- Interface Attributes—Changes the interface properties.
- Element Manager—Manages the device.
- FCIP Tunnel Attributes—Changes FCIP tunneling properties.
- Create Port Channel—Creates port channel.
- Re-enable—Reenables a disabled device.
- Enable FC-SP—Enables FC-SP.



- SAN Extention Tuner—Optimizes FCIP performance.
- Purge—Purges the device.

**Note**

When you select a port channel from the table, the pop-up menu will have the following additional options:

- Member Attributes—Changes the member properties.
- Channel Attributes—Changes the port channel properties.
- Edit—Edits the channel properties.

## Viewing End Device Options

### DETAILED STEPS

**Step 1** In the Physical Attributes pane, click **End Devices** and then click the **Summary** tab.

**Step 2** Right-click the device in the table.

The pop-up menu provides the following options:




- Apply Changes—Applies the changes to the device.
- Refresh Values—Refreshes the current values.
- Copy—Copies the information specific to the field.
- Paste—Pastes the copied text.
- Undo Changes—Undoes modifications to the device.
- Find—Searches for information depending on the input string.
- Export to File—Exports the values to a file.
- Print Table—Prints the table.
- Detach Table—Detaches the table.
- Device Attributes—Changes the device properties.
- Interface Attributes—Changes the interface properties.
- Element Manager—Manages this device.
- Command Line Interface—Enables you to perform command line operations.
- Copy—Copies the switch.
- Purge—Purges the switch.
- Fix Location—Fixes the switch in the current location.
- Align—Aligns the switch.
- Ping—Pings another device.
- Trace Route—Determines the route taken by packets across the network.
- Select Dependent Ports—Selects dependent ports.
- Group—Groups devices.



## Information Pane

Use the Information pane to display tables of information associated with the option selected from the menu tree in the Logical Domains or Physical Attributes panes. The Information pane toolbar provides buttons for performing one or more of the operations shown in [Table 7-4](#).

**Table 7-4** Information Pane Toolbar

| Icon                                                                                | Description                                                                                                                |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
|    | Applies configuration changes.                                                                                             |
|    | Refreshes table values.                                                                                                    |
|    | Opens the appropriate dialog box to make a new row in the table.                                                           |
|    | Deletes the currently highlighted rows from the table.                                                                     |
|   | Copies data from one row to another.                                                                                       |
|  | Pastes the data from one row to another.                                                                                   |
|  | Undoes the most recent change.                                                                                             |
|  | Finds a specified string in the table.                                                                                     |
|  | Exports and saves information to a file.                                                                                   |
|  | Prints the contents of the Information pane.                                                                               |
|  | Displays a non-editable copy of the table in the Information pane in its own window, which you can move around the screen. |



**Note**

After making changes, you must save the configuration or the changes will be lost when the device is restarted.

**Note**

The buttons that appear on the toolbar vary according to the option that you select. They are activated or deactivated (dimmed) according to the field or other object that you select in the Information pane.








## Detachable Tables

Detachable tables in Cisco DCNM-SAN allow you to detach tables and move them to different areas on your desktop so that you can compare similar tables from different VSANs. You can keep informational tables open from one view while you examine a different area in Cisco DCNM-SAN. To detach tables, click the **Detach Table** icon in the Information pane in Cisco DCNM-SAN.

## Fabric Pane















Use the Fabric pane to display the graphical representation of your fabric. [Table 7-5](#) explains the graphics you may see displayed, depending on which devices you have in your fabric.

**Table 7-5** Cisco DCNM-SAN Graphics

| Icon or Graphic                                                                     | Description                                       |
|-------------------------------------------------------------------------------------|---------------------------------------------------|
|  | Director class MDS 9000 Fibre Channel switch.     |
|  | Non-director class MDS 9000 Fibre Channel switch. |
|  | Nexus 7000 switch.                                |
|  | Nexus FCoE or Fibre Channel switch.               |
|  | Catalyst LAN switch.                              |
|  | Generic Fibre Channel switch.                     |
|  | Cisco SN5428.                                     |





**Table 7-5** *Cisco DCNM-SAN Graphics (continued)*

| Icon or Graphic                                                                     | Description                                                                                                               |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
|    | Dashed or dotted orange line through a device indicates that the device is manageable but there are operational problems. |
|    | Dashed or dotted orange X through a device or link indicates that the device or ISL is not working properly.              |
|    | A red line through a device indicates that the device is not manageable.                                                  |
|    | A red X through a device or link indicates that the device is down or that the ISL is down.                               |
|    | Fibre Channel HBA (or enclosure).                                                                                         |
|    | Fibre Channel target (or enclosure).                                                                                      |
|  | iSCSI host.                                                                                                               |
|  | Fibre Channel ISL and edge connection.                                                                                    |
|  | Fibre Channel PortChannel.                                                                                                |
|  | IP ISL and edge connection.                                                                                               |
|  | IP PortChannel.                                                                                                           |
|  | DWDM connection.                                                                                                          |
|  | NPV connection.                                                                                                           |
|  | Fibre Channel loop (storage).                                                                                             |



**Table 7-5** *Cisco DCNM-SAN Graphics (continued)*

| Icon or Graphic                                                                   | Description                                                                                                                             |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|  | IP cloud (hosts). This icon is also used to represent a fabric when viewing a SAN (multiple fabrics) in the Cisco DCNM-SAN Fabric pane. |
|  | Any device, cloud, or loop with a box around it means that there are hidden links attached.                                             |

If a switch or director is grayed out, Cisco DCNM-SAN can no longer communicate with it.

The bottom of the Fabric pane has the following tabs:

- **Fabric**—When displaying multiple fabrics, each fabric has its own tab. You can switch between fabrics by clicking on their respective tabs.
- **Log**—Displays messages that describe Cisco DCNM-SAN operations, such as fabric discovery.

When viewing large fabrics in the Fabric pane, it is helpful to do the following tasks:

- Turn off end device labels.
- Collapse loops.
- Collapse expanded multiple links (collapsed multiple links are shown as very thick single lines).
- Dim or hide portions of your fabric by VSAN.

**Note**

When a VSAN, zone, or zone member is selected in the VSAN tree, the map highlighting changes to identify the selected objects. To remove this highlighting, click the **Clear Highlight** button on the Fabric pane toolbar or choose **Clear Highlight** from the pop-up menu.

## Context Menus

When you right-click an icon in the Fabric pane, you see a pop-up menu with options that vary depending on the type of icon selected. The various options available for different objects include the following:

- Open an instance of Device Manager for the selected switch.
- Open a CLI session for the selected switch.
- Copy the display name of the selected object.
- Execute a **ping** or **tracert** command for the device.
- Show or hide end devices.
- View attributes.
- Quiesce and disable members for PortChannels.
- Set the trunking mode for an ISL.
- Create or add to a PortChannel for selected ISLs.

The Fabric pane has its own toolbar with options for saving, printing, and changing the appearance of the map. When you right-click the map, a pop-up menu appears that provides options (duplicated on the toolbar) for changing the appearance of the map.



**Note**

You can launch web-based or non-web-based applications from the Fabric pane. To do this, you assign an IP address to the storage port or enclosure. Then right-click to bring up the pop-up menu, and select **Device Manager**.

## Saving the Map

You can save the map in the Fabric Pane as an image, or as an editable Visio diagram. You can save the map with or without labels on the links. The created Visio diagram is editable and saved in two layers:

- The default layer includes all switches and links in the fabric.
- The end devices layer includes the end devices and can be turned off to remove end devices from the Visio diagram.

To save the map as a Visio diagram, choose **Files > Export > Visio** and choose **Map** or **Map with link labels**. The saved Visio diagram retains the viewing options that you selected from the Fabric pane. For example, if you collapse multiple links in the map and export the links as a Visio diagram, the Visio diagram shows those multiple links as one solid link.

The Show Tech Support option from the Tools menu also supports saving the map as a Visio diagram.

## Purging Down Elements

The Fabric pane allows you to refresh the map at any time by clicking the **Refresh Map** icon. The **Refresh Map** icon redraws the map but does not purge elements that are down. To purge down elements you can:

- Choose **Server > Purge Down Elements**. This purges all down elements in the fabric.
- Right-click the **Fabric** pane and choose **Purge Down Elements**.
- Right-click a down element and choose **Purge**. This action purges only this element from the fabric.

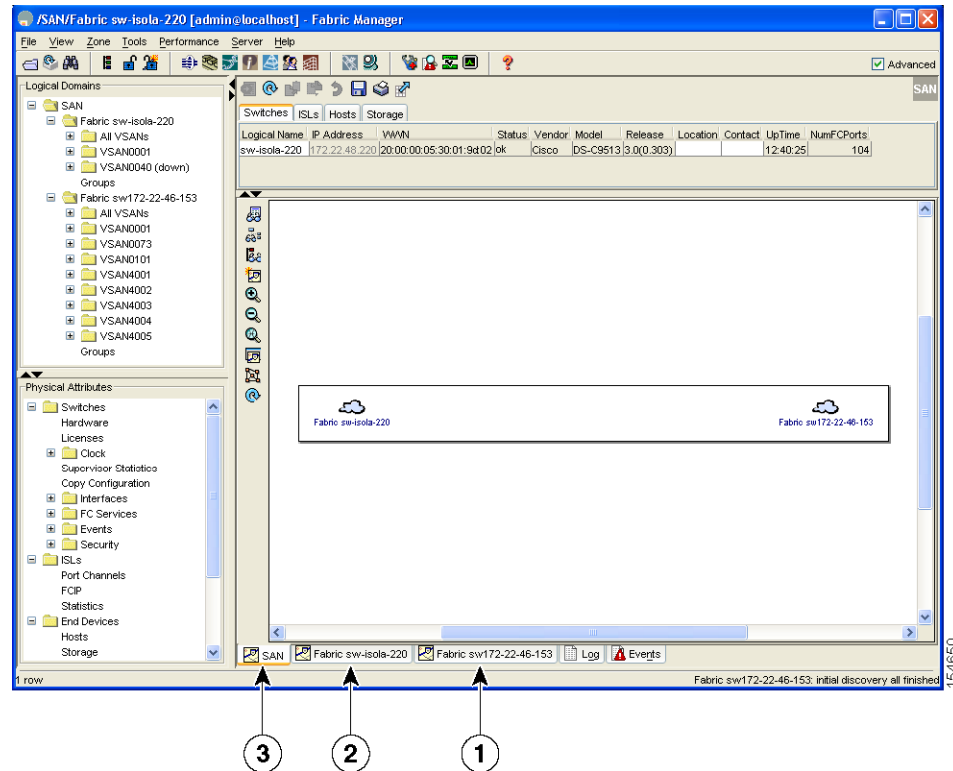
**Note**

If you select an element that is not down and purge it, that element will reappear on the next fabric discovery cycle.

## Multiple Fabric Display

Cisco DCNM-SAN can display multiple fabrics in the same pane as shown in [Figure 7-3](#).



**Figure 7-3** Cisco DCNM-SAN's Multiple Fabric Display Window

|   |                                                                                                             |
|---|-------------------------------------------------------------------------------------------------------------|
| 1 | The Fabric view tab for fabric 172.23.46.152. When selected, the Fabric view displays fabric 172.23.46.152. |
| 2 | The Fabric view tab for fabric 172.23.46.153. When selected, the Fabric view displays fabric 172.23.46.153. |
| 3 | SAN tab (selected), showing two fabrics.                                                                    |

The information for both fabrics is displayed; you do not need to select a seed switch. To see details of a fabric, select the tab for that fabric at the bottom of the Fabric pane, or double-click the **Cloud** icon for the fabric in the SAN tab.

**Note**

Enclosure names should be unique. If the same enclosure name is used for each port, Cisco DCNM-SAN shows a host/target enclosure connected to both fabrics. To fix this problem, you can either disable auto-creation or create unique enclosure names.

## Filtering by Groups

You can filter the Fabric pane display by creating groups of switches or end ports.

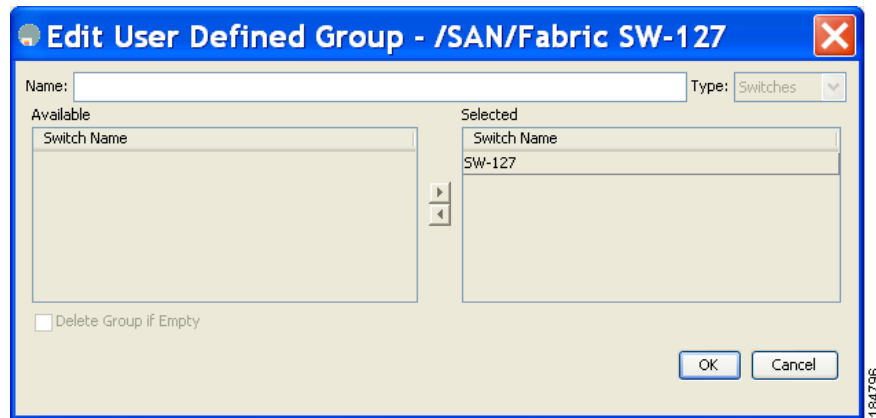
### DETAILED STEPS

- Step 1** Right-click a switch or end port in the Fabric pane map and select **Group > Create**.



You see the Edit User Defined Group dialog box as shown in [Figure 7-4](#).

**Figure 7-4** Edit User Defined Group Dialog Box



- Step 2** Enter a group name in the **Name** field.
- Step 3** Use the arrows to move additional switches or end ports from the **Available** column to the **Selected** column.
- Step 4** Click **OK** to save the group.

---

To add a switch or end port to an existing group in Cisco DCNM-SAN.

## DETAILED STEPS

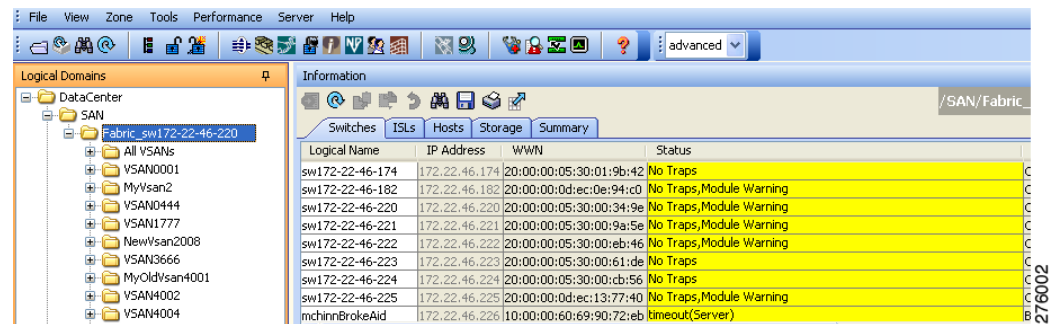
- 
- Step 1** Right-click a switch or end device and select **Group > Add To > YourGroupName**.  
You see the Edit User Defined Group dialog box as shown in [Figure 7-4](#).
  - Step 2** Use the arrows to move additional switches or end ports from the **Available** column to the **Selected** column.
  - Step 3** Click **OK** to save the updated group.
- 

To filter the display by a group you have created.

## DETAILED STEPS

- 
- Step 1** Expand the **Groups** folder in the Logical Domains pane.  
You see the list of groups that you have created as shown in [Figure 7-5](#).



**Figure 7-5** Group Highlighted in Fabric Pane Map

**Step 2** Click the name of the group that you want to filter.

In the Fabric pane, the switches or end devices in your group are shown normally; all other switches and end devices are shown in gray.

**Step 3** Click the **Groups** folder in the Logical Domains pane to return the display to normal.

**Note**

User-defined groups tables are filtered based on switches in the group except for switches where CFS-controlled features are enabled when all CFS member switches are displayed to avoid misconfigurations.

## Status Bar

The status bar at the bottom of the Cisco DCNM-SAN window shows the last entry displayed by the discovery process, and the possible error message on the right side. The status bar displays a message stating that something has changed in the fabric and a new discovery is needed. The status bar shows both short-term, transient messages (such as the number of rows displayed in the table) and long-term discovery issues.

## Launching Cisco DCNM-SAN Client

As of Cisco SAN-OS 3.x and NX-OS Release 4.x, the Fabric Manager Client login procedure has changed.

## Launching Fabric Manager Client in Cisco SAN-OS Release 3.2(1) and Later

You can launch Fabric Manager Client.

**Note**

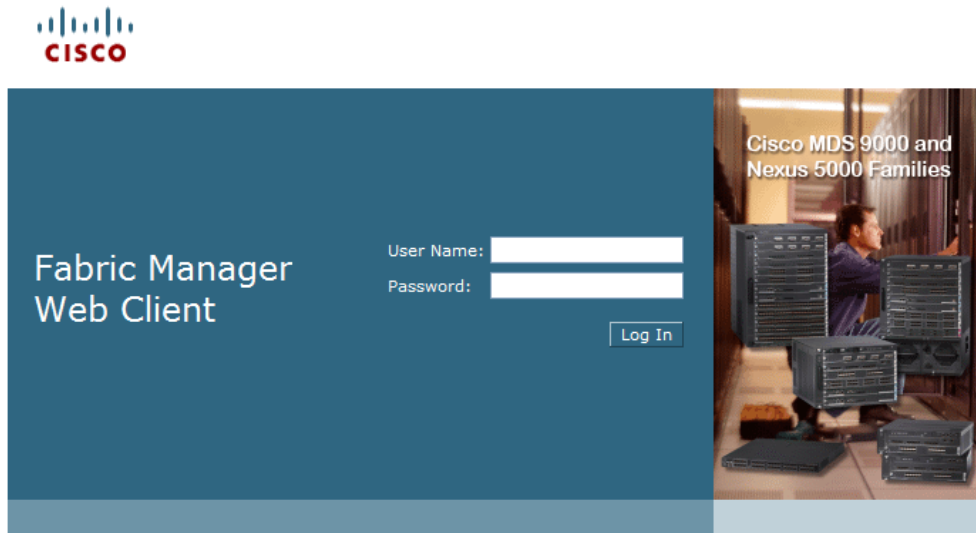
Network administrators must initially launch Cisco DCNM-SAN Client using Cisco DCNM-SAN Web Server, as described in the following procedure. Once an administrator has installed the Cisco DCNM-SAN Client icon on your desktop, you can double-click the icon to launch the Cisco DCNM-SAN Client.



## DETAILED STEPS

- Step 1** Open your browser and enter the IP address where you installed Cisco DCNM-SAN Server, or enter localhost if you installed Cisco DCNM-SAN Server on your local workstation.
- You see the Cisco DCNM Web Client Login dialog box.

**Figure 7-6** DCNM-SAN Web Client Login Dialog Box



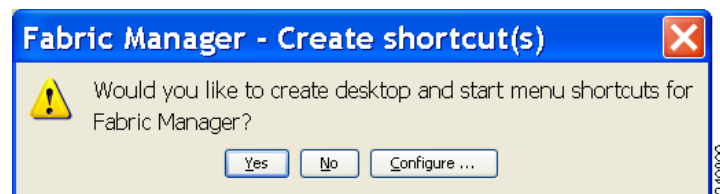
- Step 2** Enter your user name and password and click **Login**.
- You see the Cisco DCNM Web Client Summary page.
- Step 3** Click the **Download** link in the upper right corner of the page.
- You see the Download page for Cisco DCNM-SAN and Device Manager.



**Figure 7-7** Download Page for DCNM-SAN and Device Manager

**Step 4** Click the link for **Cisco DCNM-SAN**.

If you are launching Cisco DCNM-SAN Client for the first time, you see a message asking whether you want to create shortcuts for Cisco DCNM-SAN.

**Figure 7-8** DCNM-SAN Create Shortcut(s) Message

**Step 5** Click **Yes** to create shortcuts for Cisco DCNM-SAN.

**Note**

This message only appears the first time you launch Cisco DCNM-SAN Client. If you select No, your selection will be remembered and you will not be prompted to make a selection again. In this case, you will need to launch Cisco DCNM-SAN Client using the Cisco DCNM-SAN Web Client.

**Step 6** When the software is installed and icons are created on your desktop, double-click the Cisco DCNM-SAN icon to launch Cisco DCNM-SAN.

You see the Cisco DCNM-SAN Login dialog box.



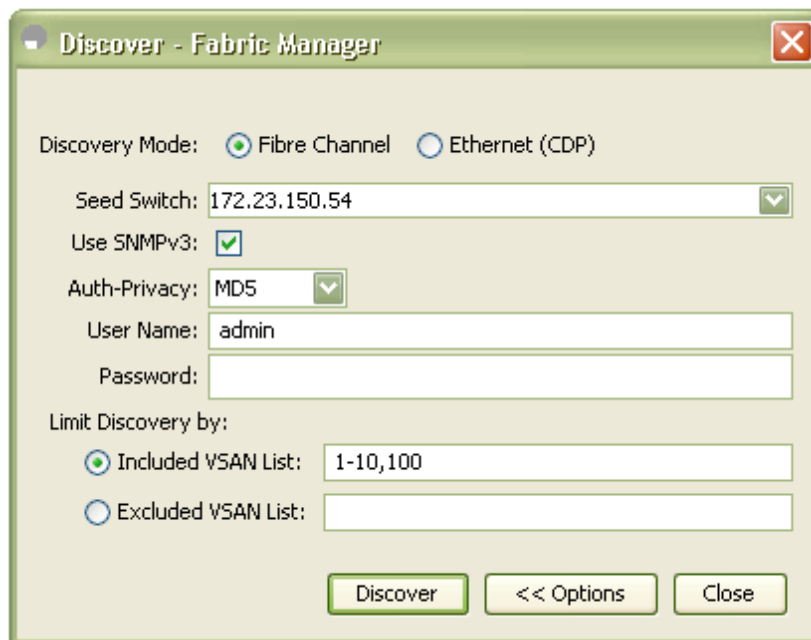
**Figure 7-9** DCNM-SAN Login Dialog Box

- Step 7** Enter the Cisco DCNM-SAN Server user name and password.
- Step 8** Check the **Use SNMP Proxy** check box if you want Cisco DCNM-SAN Client to communicate with Cisco DCNM-SAN Server through a TCP-based proxy server.
- Step 9** Click **Login**. Once you successfully log in to Cisco DCNM-SAN Server, you can set the seed switch and open the fabrics that you are entitled to access.



**Note** When you launch Cisco DCNM-SAN Client for the first time or when there are no available fabrics, you see the Discover New Fabric dialog box.

You see the Discover New Fabric dialog box.

**Figure 7-10** Discover New Fabric Dialog Box

**Note** Only network administrators can discover new fabrics.



**Note**

Even when remote AAA server authentication is enabled on the switch, use the local switch account that is not defined in the remote AAA server for fabric discovery. In other words, when a user is not found in the remote AAA server, then local switch user authentication will be allowed by the switch for SNMPv3 clients like DCNM.

**Step 10** Click the **Ethernet (CDP)** radio button to discover using Cisco Discovery Protocol (CDP).

**Step 11** Starting from NX-OS Release 4.2(0), Fabric Manager uses Cisco Discovery Protocol to discover Ethernet switches such as Nexus 5000, Nexus 7000, Catalyst 4000, and Catalyst 6000 switches. You need to use a CDP seed switch for a CDP discovery.  
Set the fabric seed switch to the Cisco MDS 9000 Family switch or Cisco Nexus 5000 Series that you want Fabric Manager to use.

**Step 12** Choose the Auth-Privacy option according to the privacy protocol you have configured on your switch:

- If you have not configured the switch with a privacy protocol, then choose Auth-Privacy option MD5 (no privacy).
- If you have configured the switch with your privacy protocol, choose your Auth-Privacy choice.

**Note**

You may use SNMP v2 credentials for CDP discovery as the most of the Catalyst switches do not use MD5-DES for configuration.

**Note**

If you want a clean fabric discovery, remove the fabric and rediscover it. If you want a clean LAN discovery, unmanage LAN, remove the CDP seed switch and then rediscover it.

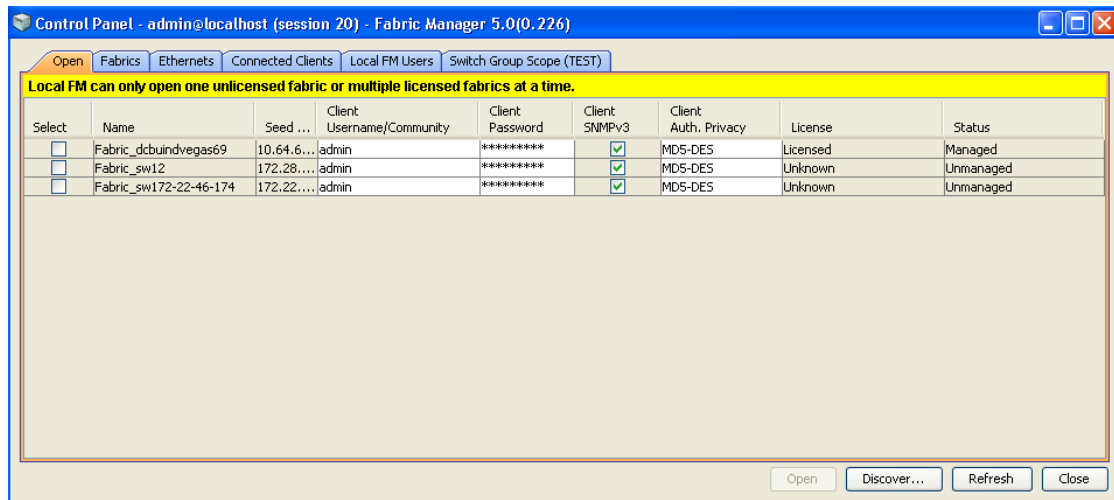
**Step 13** Enter the username and password for the switch.

**Step 14** (Optional) To limit the discovery, specify the VSAN range.  
Scoping limits the resources discovered by Cisco DCNM-SAN client. You can either include a range of VSANs to be discovered or exclude a range of VSANs from being discovered.

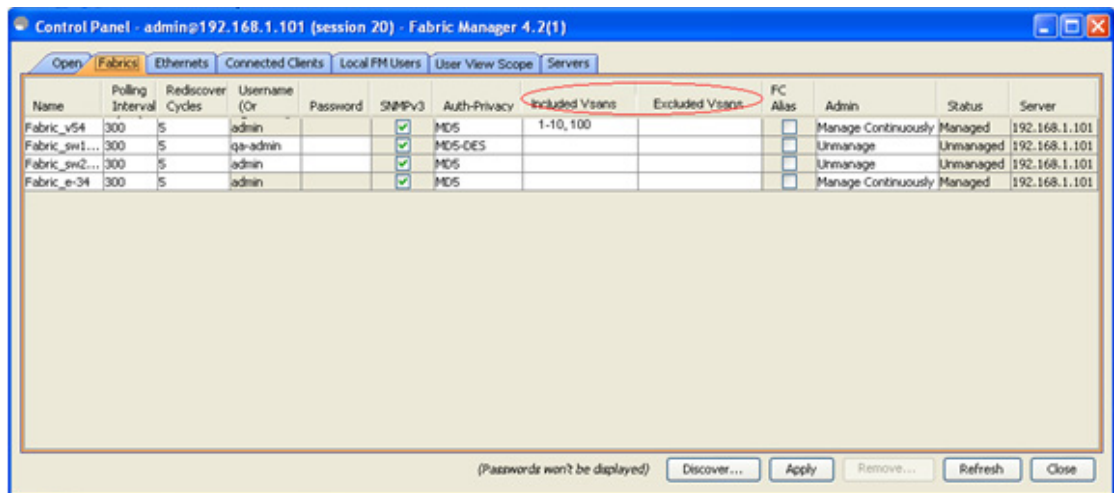
- To limit the discovery to a range of VSANs, click **Included VSAN List** radio button. Specify the range of VSANs.
- To exclude a range of VSANs from being discovered, click **Excluded VSAN List** radio button. Specify the range of VSANs to be excluded.

**Step 15** Click **Discover**.  
You see the Control Panel dialog box.



**Figure 7-11 Control Panel Dialog Box: Open Tab**

You see the included and excluded VSANs list under the Fabric tab.

**Figure 7-12 Control Panel Dialog Box: Fabrics Tab****Note**

You see a message in the dialog box when the server and client are running on the same workstation and there are unlicensed fabrics in the database. You also see a message when there are unmanaged fabrics (the state of the licenses is unknown).

**Note**

In the open tab, you see all the discovered fabrics displayed in the control panel. You need to click on the Open button to see all the discovered Ethernet switches.

- Step 16** Check the check box(es) next to the fabric(s) you want to open in the Select column, or click **Discover** to add a new fabric.



**Note**

Only network administrators can continuously manage or unmanage fabrics. For more information, see the [“Selecting a Fabric to Manage Continuously”](#) section on page 5-8.

**Step 17** Click **Open** to open the selected fabric(s).

**Note**

- If you have an incomplete view of your fabric, rediscover the fabric with a user that has no VSAN restriction.
- If the fabric includes a Cisco Nexus 5000 Series switch, then the Layer 2 node appears under the Switches > Interfaces > Ethernet tree, the VFC (FCoE) node appears under the Switches > Interfaces tree, and the FCoE node appears under the Switches tree in the Physical Attributes pane.
- For Cisco Nexus 5000 Series switches in the fabric, the tooltip for the switch shows the bind information of a virtual Fibre Channel interface to its corresponding Ethernet interface, such as vfc2(eth1/4).

You can launch Cisco DCNM-SAN Client from within a running instance of Cisco DCNM-SAN.

## DETAILED STEPS

**Step 1** Choose **File > Open** or click the **Open Switch Fabric** icon on the Cisco DCNM-SAN toolbar.

You see the Control Panel dialog box.

**Step 2** Check the check box(es) next to the fabric(s) you want to open in the Select column and click **Open**.

**Note**

Changes made using Cisco DCNM-SAN are applied to the running configuration of the switches that you are managing. If you have made changes to the configuration or performed an operation (such as activating zones), Cisco DCNM-SAN prompts you to save your changes before you exit.

## Launching Cisco DCNM-SAN Client Using Launch Pad

Starting from Cisco NX-OS Release 4.2(0), you can use Cisco DCNM-SAN launch pad to connect to any server by specifying the IP address of the server. With launch pad, you can connect to any Cisco DCNM-SAN Server version 3.3(0) and later. Launch pad establishes connection with the server using HTTP protocol.

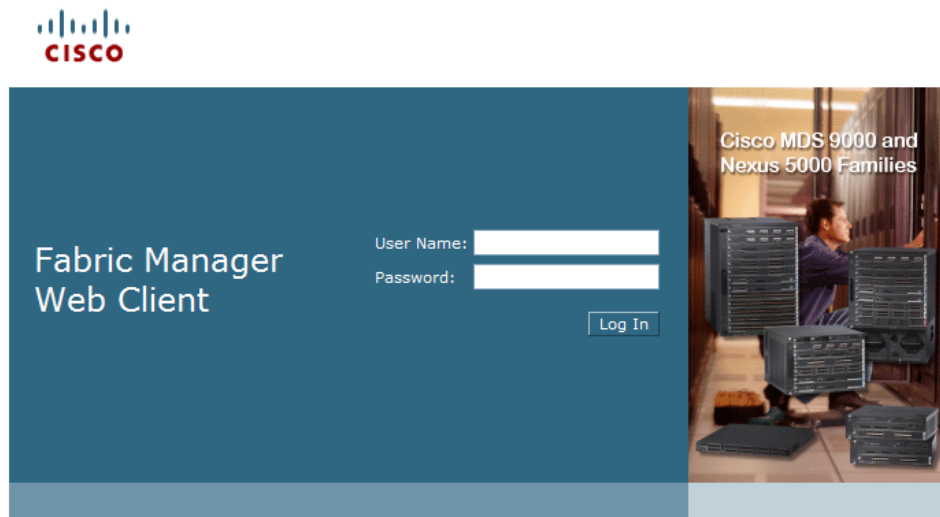
## DETAILED STEPS

**Step 1** Open your browser and enter the IP address where you installed Cisco DCNM-SAN Server, or enter localhost if you installed Cisco DCNM-SAN Server on your local workstation.

You see the Cisco DCNM-SAN Web Server Login dialog box.



**Figure 7-13** DCNM-SAN Web Client Login Dialog Box

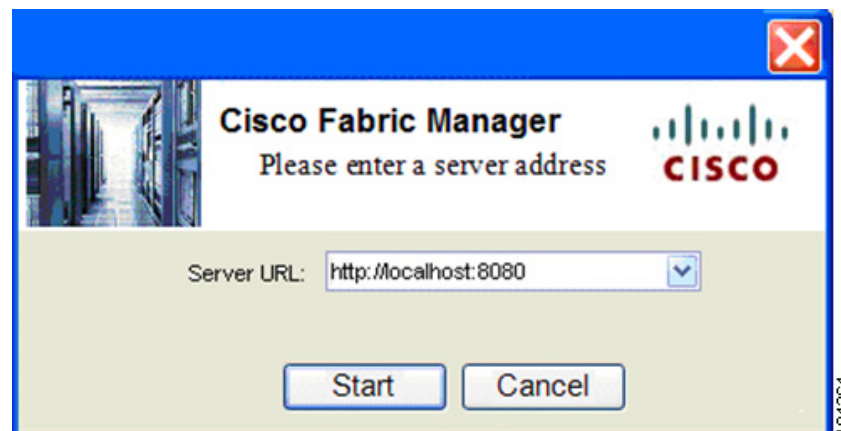


- Step 2** Enter your user name and password and click **Login**.  
You see the Cisco DCNM-SAN Web Client Summary page.
- Step 3** Click the **Download** link in the upper right corner of the page.  
You see the Download page for Cisco DCNM-SAN and Device Manager.



**Figure 7-14** Download Page for DCNM-SAN and Device Manager

- Step 4** Click the link for **Cisco DCNM-SAN**.  
You see the Cisco DCNM-SAN Server launch pad.
- Step 5** Enter the host name of the server or IP address in the **Server URL** drop-down list.
- Step 6** Click **Start**.

**Figure 7-15** DCNM-SAN Launch Pad



**Note**

Launch pad retains the history of the server URLs used. You can choose one of the previously user Server URLs from the drop-down list.

## Setting Cisco DCNM-SAN Preferences

To set your preferences for the behavior of the Cisco DCNM-SAN, choose **File > Preferences** from the Cisco DCNM-SAN menu bar. You see the Preferences dialog box with the following tabs for setting different components of the application:

- General
- SNMP
- Map

The default General preferences for Cisco DCNM-SAN are as follows:

- **Show Device Name by**—Displays the switches in the Fabric pane by IP address, DNS name, or logical name. The default setting for this value is Logical Name.
- **Show WorldWideName (WWN) Vendor**—Displays the world wide name vendor name in any table or listing displayed by Cisco DCNM-SAN. Check the **Prepend Name** check box to display the name in front of the IP address of the switch. Check the **Replacing Vendor Bytes** check box to display the name instead of the IP address. The default is the Prepend Name option.
- **Show End Device Using**—Displays end devices in the Fabric pane using alias or pWWN alias. The default setting for this value is Alias.
- **Show Shortened iSCSI Names**—Displays the default setting for this value is OFF.
- **Show Timestamps as Date/Time**—Displays timestamps in the date/time format. If this preference is not checked, timestamps are displayed as elapsed time. The default setting is enabled (checked).
- **Telnet Path**—Displays the path for the telnet.exe file on your system. The default is **telnet.exe**, but you need to browse for the correct location.

**Note**

If you browse for a path or enter a path and you have a space in the pathname (for example, **c:\program files\telnet.exe**), then the path will not work. To get the path to work, you must manually place quotes around it (for example, **"c:\program files\telnet.exe"**).

- **Use Secure Shell instead of Telnet**—Specifies whether to use SSH or Telnet when using the CLI to communicate with the switch. If enabled, you must specify the path to your SSH application. The default setting is disabled.
- **Confirm Deletion**—Displays a confirmation pop-up window when you delete part of your configuration using Cisco DCNM-SAN. The default setting is enabled (checked).
- **Export Tables with Format**—Specifies the type of file that is created when you export a table using Device Manager. The options are tab-delimited or XML. The default setting is Tab-Delimited.
- **Show CFS Warnings**—Shows warning messages if CFS is not enabled on all switches for a selected feature.

The default SNMP preferences for Cisco DCNM-SAN are as follows:



- **Retry request 1 time(s) after 5 sec timeout**—You can set the retry value to 0-5, and the timeout value to 3-30.
- **Trace SNMP packets in Log**—The default setting for this value is ON.
- **Enable Audible Alert when Event Received**—The default setting for this value is OFF.

The default Map preferences for Cisco DCNM-SAN are as follows:

- **Display Unselected VSAN Members**—Displays the unselected VSAN members in the Fabric pane. The default setting for this value is ON.
- **Display End Devices**—Displays the fabric's end devices in the Fabric pane. The default setting for this value is ON.
- **Display End Device Labels**—Displays the fabric's end device labels in the Fabric pane. The default setting for this value is OFF.
- **Expand Loops**—Displays the loops in the fabric as individual connections in the Fabric pane. The default setting for this value is OFF.
- **Expand Multiple Links**—Displays multiple links in the Fabric pane as separate lines instead of one thick line. The default setting for this value is OFF.
- **Open New Device Manager Each Time**—Opens a new instance of Device Manager each time that you invoke it from a switch in your fabric. The default value is OFF, which means that only one instance of Device Manager is open at a time.
- **Select Switch or Link from Table**—Allows you to select a switch or link in the Fabric pane by clicking the switch or link in a table in the Information pane. The default setting for this value is disabled (unchecked), which means clicking a switch or link in the table does not change the switch or link selection in the Fabric pane.
- **Layout New Devices Automatically**—Automatically places new devices in the Fabric pane in an optimal configuration. The default setting for this value is OFF. In this mode, when you add a new device, you must manually reposition it if the initial position does not suit your needs.
- **Use Quick Layout when Switch has 30 or more End Devices**—Displays the default setting for this value (30). You can enter any number in this field. Enter 0 to disable Quick Layout.
- **Override Preferences for Non-default Layout**—Displays the default setting for this value (ON).
- **Automatically Save Layout**—If this option is enabled, any changes in the layout are automatically saved. The default setting for this value is ON.
- **Detach Overview Window**—Allows you to easily center the Fabric pane on the area of the fabric that you want to see. (This feature is useful for large fabrics that cannot be displayed entirely within the Fabric pane.) Bring up the overview window by clicking the **Show/Hide Overview Window** button. It overlays the fabric window and remains there until you click the **Show/Hide Overview Window** button again. If you enable this preference, you can detach the overview window and move it to one side while you access the Fabric pane. The default setting for this value is disabled (unchecked).

## Network Fabric Discovery

Cisco DCNM-SAN collects information about the fabric topology through SNMP queries to the switches that are connected to Cisco DCNM-SAN. The switch replies after having discovered all devices connected to the fabric by using the information from its FSPF technology database and the Name Server



database and collected using the Fabric Configuration Server's request/response mechanisms that are defined by the FC-GS-3/4 standard. When you start Cisco DCNM-SAN, you enter the IP address (or host name) of a seed switch for discovery.

After you start Cisco DCNM-SAN and the discovery completes, Cisco DCNM-SAN presents you with a view of your network fabric, including all discovered switches, hosts, and storage devices.

## Network LAN Discovery

Starting from NX-OS Release 4.2(0), you can discover Nexus and Catalyst Ethernet switches using Cisco Discovery Protocol (CDP). DataCenter 3(DC3) switches are displayed under Datacenter and LAN nodes. Cisco DCNM-SAN displays basic information about DC3 switches and its ISLs.

## Viewing Ethernet Switches

### DETAILED STEPS

- 
- Step 1** Click the **LAN** node under **Datacenter** node.
  - Step 2** Click **Switches** tab in the Information pane.  
You can see the switch information as shown in [Figure 7-16](#).



**Figure 7-16 Ethernet Switch Information**

The screenshot displays the Cisco Prime DCNM-SAN Client interface. On the left, the 'Logical Domains' tree shows a hierarchy: DataCenter > SAN > Fabric\_sw172-22-46-220 > LAN. The 'Information' pane on the right shows a table of switch details under the 'Switches' tab. Below this, the 'LAN' pane shows a network diagram with four switches connected in a chain: mchinn-cat4k, mchinn-cat6k, mchinn-n7k, and mchinnN5K.

| Logical Name | IP Address    | Serial Number | Status | Vendor | Model          | Release                                                           |
|--------------|---------------|---------------|--------|--------|----------------|-------------------------------------------------------------------|
| mchinn-n7k   | 172.22.46.156 | TBM12035416   | ok     | Cisco  | N7K-C7010      | Cisco Nexus Operating System (NX-OS) Software, Version 4.2(1)     |
| mchinn-cat4k | 172.22.46.157 | FOX072401GU   | ok     | Cisco  | W5-C4507R      | Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-EN1 |
| mchinn-cat6k | 172.22.46.158 | FOX080209NT   | ok     | Cisco  | cisco W5-C6503 | Cisco IOS Software, s3223_rp Software (s3223_rp-ADVENTERPRISE     |
| mchinnN5K    | 172.22.47.135 | FOX1009009B   | ok     | Cisco  | N5K-C5020P-BF  | Cisco Nexus Operating System (NX-OS) Software, Version 4.1(3)N1(  |

**Note**

Datacenter is the parent node of SAN and LAN nodes. The SAN node remains in the tree as the parent for all the fabrics.

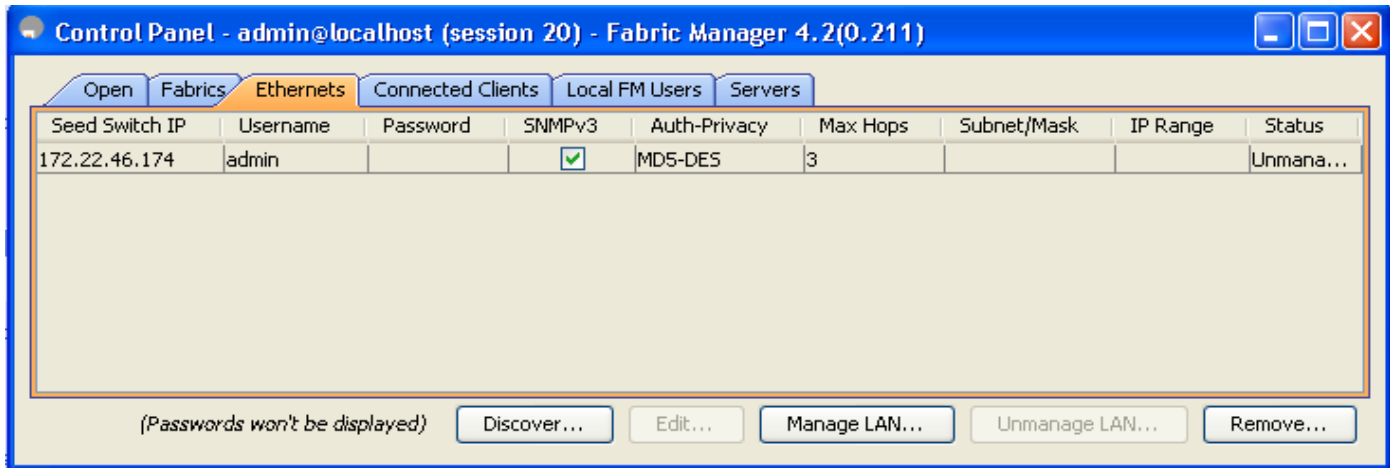
## Removing a LAN

### DETAILED STEPS

- Step 1** Choose **Server > Admin**.  
You can see the switch information as shown in [Figure 7-17](#).



Figure 7-17 Control Panel



**Step 2** Click to select the switch IP of the LAN you want to remove.

**Step 3** Click **Remove**.

## Modifying the Device Grouping

Because not all devices are capable of responding to FC-GS-3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the Cisco DCNM-SAN map.

### DETAILED STEPS

- Step 1** Expand **End Devices** and then choose **Storage** or **Hosts** in the Physical Attributes pane. You see the end devices displayed in the Information pane.
- Step 2** Click one of the devices in the Fabric pane, or click the **Enclosures** tab of the Information pane, and then click the device name (in the Name field) that you want to include in the enclosure.
- Step 3** Enter a name to identify the new enclosure in the Fabric pane map.
- Step 4** Click once on the device name in the Name field. To select more than one name, press the **Shift** key and click each of the other names.
- Step 5** Press **Ctrl-C** to copy the selected name(s).
- Step 6** Press **Ctrl-V** to paste the device name into the Name field.



**Note** To remove devices from an enclosure, triple click the device name and press **Delete**. To remove an enclosure, repeat this step for each device in the enclosure.

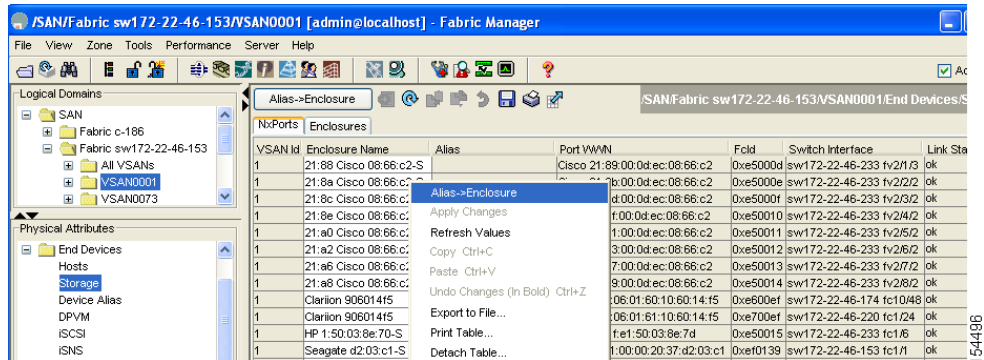


## Using Alias Names as Enclosures

### DETAILED STEPS

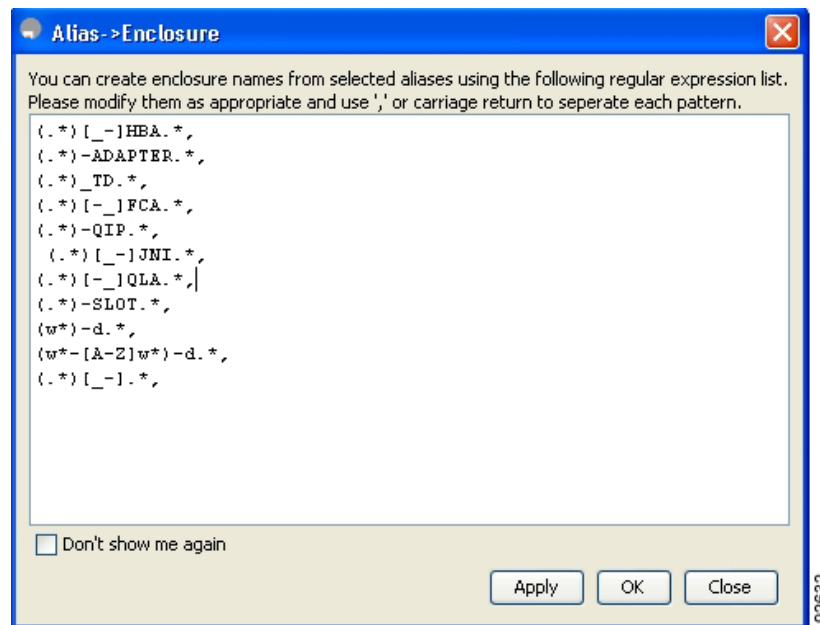
- Step 1** Expand End Devices and choose **Hosts** or **Storage** from the Physical Attributes pane.
- You see the list of devices in the Information pane. The NxPorts tab is the default.
- Step 2** Right-click the enclosure names that you want to convert to alias names and choose **Alias > Enclosure** as shown in Figure 7-18.

**Figure 7-18** Alias Enclosure



The Alias > Enclosures window appears as shown in Figure 7-19. It contains a list of expressions. You can also add expressions to the list and modify expressions in the current list.

**Figure 7-19** List of Expressions



- Step 3** Click the **Apply Changes** icon to save the changes and then click **Close**.



**Note**

Cisco DCNM-SAN uses the regular expressions to convert multiple alias names into one enclosure. The alias names should be in the same expression pattern rule. You can create enclosure names from selected aliases using the regular expressions list.

## Using Alias Names as Descriptions

### DETAILED STEPS

- Step 1** Choose **End Devices** and from the Physical Attributes pane.
- Step 2** Click the **General** tab.
- You see the list of devices in the Information pane.
- Step 3** Select the device names that you want to populate the description with alias names and then click **Alias > Enclosure** button as shown in [Figure 7-20](#).
- You see the alias names are copied to corresponding rows in the description column.

**Figure 7-20 Data Population: Alias to Description**

The screenshot shows the Cisco DCNM-SAN client interface. The 'Information' pane is active, displaying a table of device information. The 'Alias->Description' button is highlighted in the top toolbar. The table has columns for Switch, Interface, Mode Admin, Mode Oper, Port VSAN, Dynamic VSAN, Description, Alias, and Speed Admin. The data is as follows:

| Switch          | Interface | Mode Admin | Mode Oper | Port VSAN | Dynamic VSAN | Description      | Alias                           | Speed Admin |
|-----------------|-----------|------------|-----------|-----------|--------------|------------------|---------------------------------|-------------|
| sw172-22-46-... | fc1/2     | TL         | TL        | 2         | n/a          | SymBios 20:0...  | SymBios 20:02:00:a0:b8:0c:0a:e3 | auto        |
| sw172-22-46-... | fc1/10    | FX         | F         | 1         | n/a          | Emulex 10:00...  | Emulex 10:00:00:00:c9:73:2a:f2  | auto        |
| sw172-22-46-... | fc10/20   | FX         | F         | 2         | n/a          | 10:00:00:00:0... | 10:00:00:00:00:01:00:00         | auto        |
| sw172-22-46-... | fc10/46   | FX         | F         | 2         | n/a          |                  | LSI 2f:ff:00:06:2b:10:c1:53     | auto        |
| sw172-22-46-... | fc10/48   | FX         | F         | 2         | n/a          | myCLRDA          | Clariion 906014f5-SPA0          | auto        |
| sw172-22-46-... | fc1/3     | F          | F         | 1         | n/a          |                  | Emulex 10:00:00:00:c9:2e:31:37  | auto        |

**Note**

Cisco DCNM-SAN does not parse or format the alias name while copying.



# Controlling Administrator Access with Users and Roles

Cisco MDS 9000 Family switches support role-based management access whether using the CLI or Cisco Cisco DCNM-SAN. This lets you assign specific management privileges to particular roles and then assign one or more users to each role.

The default-role contains the access permissions needed by a user to access the GUI (Cisco DCNM-SAN and Device Manager). These access permissions are automatically granted to all users in order for them to use the GUI.

Cisco Cisco DCNM-SAN uses SNMPv3 to establish role-based management access. After completing the setup routine, a single role, user name, and password are established. The role assigned to this user allows the highest level of privileges, which includes creating users and roles. Use the Cisco Cisco DCNM-SAN to create roles and users and to assign passwords as required for secure management access in your network.

## Using Cisco DCNM-SAN Wizards

Cisco DCNM-SAN Client provides the following wizards to facilitate common configuration tasks:

- VSAN—Creates VSANs on multiple switches in the fabric and sets VSAN attributes including interop mode, load balancing, and FICON.
- Zone Edit Tool—Creates zone sets, zones, and aliases. Adds members to zones and edits the zone database.
- IVR Zone—Creates IVR zone sets, zones, and aliases. Enables IVR NAT and auto-topology. Adds members to IVR zones, and edits the IVR zone database.
- FCoE—Creates virtual Fibre Channel (FC) interfaces and VLAN-VSAN mappings, and binds virtual FC interfaces to Ethernet interfaces or PortChannels.
- PortChannel—Creates PortChannels from selected ISLs either manually or automatically. Sets PortChannel attributes such as channel ID and trunking mode.
- FCIP—Creates FCIP links between Gigabit Ethernet ports. Enables Fibre Channel write acceleration and IP compression.
- DPVM—Establishes dynamic port VSAN membership, enables autolearning, and activates the DPVM database.
- Port Security—Prevents unauthorized access to Cisco MDS switches and reports these intrusions to the administrator.
- iSCSI—Creates zones for iSCSI initiators and adds a VSAN to a target-allowed VSAN list.
- NPV—Reduces the number of Fibre Channel domain IDs in SANs.
- QoS—Sets QoS attributes for zones in the selected VSAN.
- IP ACL—Creates ordered IP access control lists and distributes to selected switches in the fabric.
- License Install—Facilitates download and installation of licenses in selected switches in the fabric.
- Software Install—Verifies image compatibility and installs software images on selected switches in the fabric.



# Cisco DCNM-SAN Troubleshooting Tools

Cisco DCNM-SAN has several troubleshooting tools available from the toolbar or Tools menu

- **Zone Merge Analysis**—The zone merge analysis tool (available from the Zone menu) enables you to determine if zones will merge successfully when two Cisco MDS switches are interconnected. If the interconnected switch ports allow VSANs with identical names or contain zones with identical names, then Cisco DCNM-SAN verifies that the zones contain identical members. The merge analysis tool can be run before attempting a merge or after fabrics are interconnected to determine zone merge failure causes.
- **End-to-End Connectivity**—Cisco DCNM-SAN's end-to-end connectivity analysis tool uses FC Ping to verify interconnections between Cisco MDS switches and end-device (HBAs and storage devices) in a particular VSAN. In addition to basic connectivity, Cisco DCNM-SAN can optionally verify the following:
  - Paths are redundant.
  - Zones contain at least two members.

End devices are connected to a manageable switch (have a currently active in-band or out-of-band management path.)

- **Switch Health Analysis**—You can run an in-depth switch health analysis with Cisco DCNM-SAN. It verifies the status of all critical Cisco MDS switches, modules, ports, and Fibre Channel services. Over 40 conditions are checked. This tool provides a very fast, simple, and thorough way to assess Cisco MDS switch health.
- **Fabric Configuration Analysis**—Cisco DCNM-SAN includes a fabric configuration analysis tool. It compares the configurations of all Cisco MDS switches in a fabric to a reference switch or a policy file. You can define what functions to check and what type of checks to perform. The analysis can look for mismatched values, and missing or extra values. If all configuration checking is performed for all functions, over 200 checks are performed for each Cisco MDS switch.

After the analysis is run, the results are displayed with details about the issues that were discovered. You can automatically resolve configuration differences by selecting them and clicking the **Resolve** button. Cisco DCNM-SAN automatically changes the configuration to match the reference switch or policy file.

## Integrating Cisco DCNM-SAN and Data Center Network Management Software

Cisco DCNM-SAN and Data Center Network Management (DCNM) software are the two major components in the Cisco next-generation data center environment. Cisco DCNM-SAN configures Cisco Nexus 5000 Series switches and Cisco MDS 9000 Series switches. DCNM software configures Cisco Nexus 5000 and Cisco Nexus 7000 Series switches. The Scope of the Cisco DCNM-SAN software is confined to SAN while the scope of the DCNM-LAN software is limited to the LAN network.

In a typical data center environment, the mixture of SAN and LAN topology are becoming increasingly common. Since the two management software are not designed to work across their topology limits, users are not able to navigate to Cisco DCNM-SAN from DCNM-LAN software and vice versa.

Integrating Cisco DCNM-SAN and DCNM-LAN provides a single platform to manage the networks in data center 3.0 and it provides seamless user experience under specific configuration. Starting from Cisco MDS NX-OS Release 4.2, the directory structure has changed to accommodate the integration of Cisco DCNM-SAN with Cisco Nexus 5000 Series products.

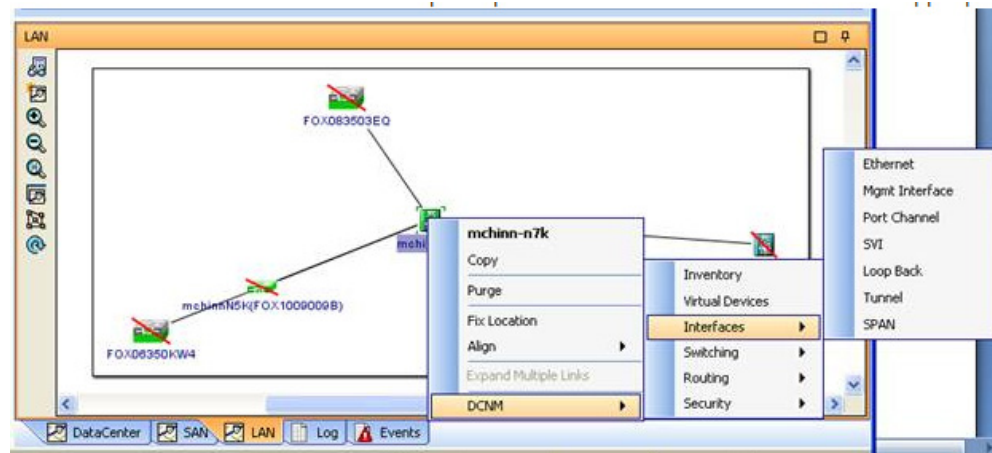


## Launching a Switch from the Topology Map

### DETAILED STEPS

- Step 1** In the Cisco DCNM-SAN fabric pane, right-click the Nexus switch in the LAN map that you want to open with DCNM.
- You see the pop-up menu as shown in [Figure 7-21](#).

**Figure 7-21** Open with DCNM



- Step 2** In the pop up menu, click **DCNM** and select appropriate context.









# Device Manager

This chapter contains descriptions and instructions for using the Device Manager. This chapter contains the following sections:

- [Information About Device Manager, page 8-1](#)
- [Device Manager Features, page 8-2](#)
- [Using Device Manager Interface, page 8-2](#)
- [Setting Device Manager Preferences, page 8-9](#)

## Information About Device Manager

Device Manager provides a graphical representation of a Cisco MDS 9000 Family switch chassis, a Cisco Nexus 5000 Series switch chassis, or a Cisco Nexus 7000 Series switch chassis including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.



### Note

Device Manager support for Cisco Nexus 7000 Series switches is only for FCoE. Non-FCoE modules appear as Unsupported Card.

The tables in the DCNM-SAN Information pane basically correspond to the dialog boxes that appear in Device Manager. However, while DCNM-SAN tables show values for one or more switches, a Device Manager dialog box shows values for a single switch. Also, Device Manager provides more detailed information for verifying or troubleshooting device-specific configuration than DCNM-SAN.

Device Manager Release 4.2 and later provides enhanced security using multiple perspectives (simple and advanced) allowing role based-access to its features. The Device Manager perspective filters out menu items that are not relevant to the user. Users with server admin role, can only access a subset of the fabric related features. The server admin role will not be able to manage Device Manager users or connected clients.

Device Manager Release 5.0 and later supports all the software features that are offered by Cisco NX-OS for managing Cisco MDS 9148 and 9124 Multilayer Fabric switches. Cisco MDS 9148 Multilayer Fabric Switch is a 48-port (1/2/4/8G) FC 1RU switch based on the Sabre ASIC and Cisco MDS 9124 Multilayer Fabric switch is a 1/2/4/8G switch module for HP BladeServer based on the Sabre ASIC. Device Manager and DCNM-SAN allow you to discover, display, configure, monitor and service both these new switches. Device Manager also supports the following Cisco Nexus 2000 Series Fabric Extenders on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 5.0(1):



- Cisco Nexus 2148T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces for its uplink connection to the parent Cisco Nexus 5000 Series switch and eight 1-Gigabit Ethernet or 10-Gigabit Ethernet host interfaces for its downlink connection to servers or hosts.
- Cisco Nexus 2232PP Fabric Extender—It has eight 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 32 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its downlink connection to servers or hosts.
- Cisco Nexus 2248TP Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.

Device Manager allows you to discover and display these Fabric Extenders. Cisco Device Manager and the Cisco DCNM-SAN client support provisioning and monitoring of the 48-port 8-Gbps Advanced Fibre Channel switching module (DS-X9248-256K9) and the 32-port 8-Gbps Advanced Fibre Channel switching module (DS-X9232-256K9).

## Device Manager Features

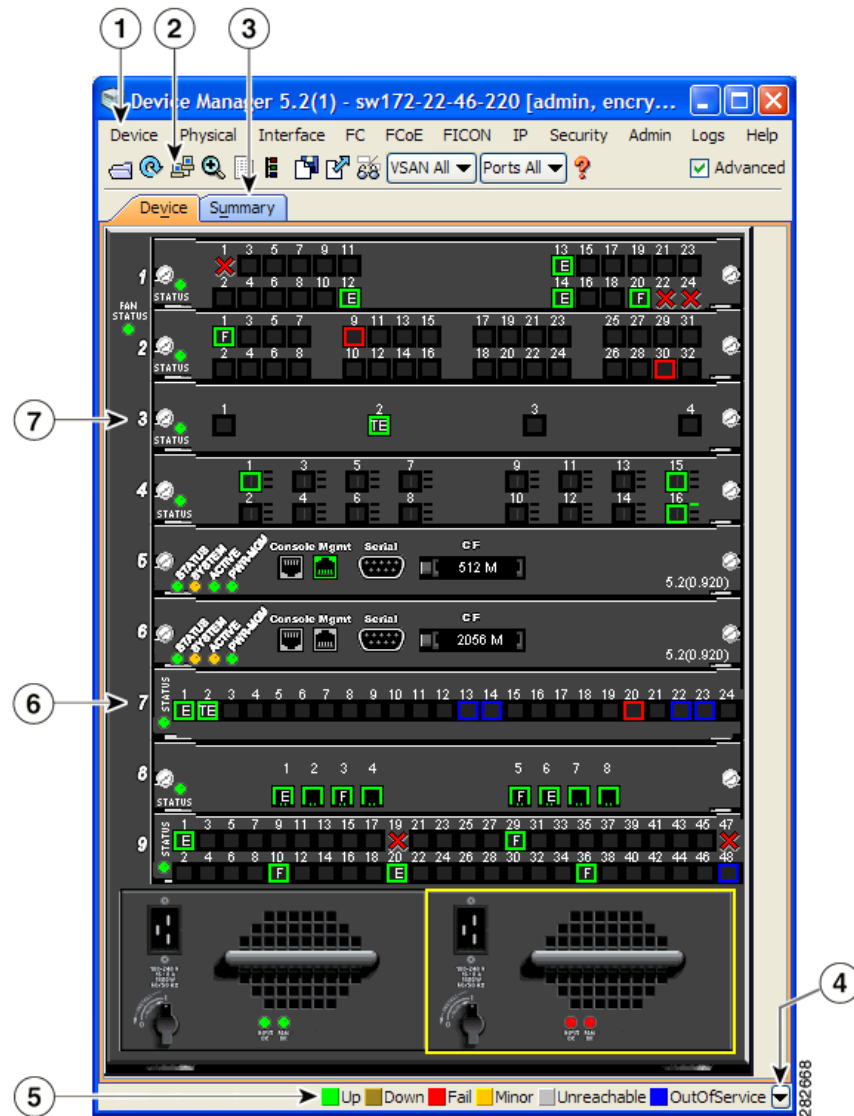
Device Manager provides two views: Device View and Summary View. Use Summary View to monitor interfaces on the switch. Use Device View to perform switch-level configurations including the following:

- Configure virtual Fibre Channel interfaces.
- Configure Fibre Channel over Ethernet (FCoE).
- Configure zones for multiple VSANs.
- Manage ports, PortChannels, and trunking.
- Manage SNMPv3 security access to switches.
- Manage CLI security access to the switch.
- Manage alarms, events, and notifications.
- Save and copy configuration files and software image.
- View hardware configuration.
- View chassis, module, port status, and statistics.

## Using Device Manager Interface

This section describes the Device Manager interface as shown in [Figure 8-1](#).



**Figure 8-1** Device Manager, Device Tab

|   |          |   |                               |
|---|----------|---|-------------------------------|
| 1 | Menu bar | 5 | Status                        |
| 2 | Toolbar  | 6 | Supervisor modules            |
| 3 | Tabs     | 7 | Switching or services modules |
| 4 | Legend   |   |                               |

## Menu Bar

The menu bar at the top of the Device Manager main window provides options for managing and troubleshooting a single switch. The menu bar provides the following options:



- **Device**—Opens an instance of Device Manager, sets management preferences, sets the page layout, opens a Telnet/SSH session with the current switch, exports a device image, and closes the Device Manager application.
- **Physical**—Allows you to view and manage inventory, modules, temperature sensors, power supplies, fans, and the entire system.
- **Interface**—Allows you to configure and manage PortChannels, as well as Fibre Channel, Ethernet, iSCSI, and FICON ports. Also provides diagnostic, management and monitoring capabilities, as well as SPAN and port tracking.



**Note** The Interface > Port Channels menu option does not appear if the Cisco Nexus 5000 Series switch is in NPV mode and runs a Cisco NX-OS release prior to 4.2(1).

- **FC**—Allows you to configure and manage VSAN, domain, and name server characteristics. Also provides advanced configuration capabilities.
- **FCoE**—Allows you to configure the FCoE parameters and map VSANs to VLANs on a Cisco Nexus 5000 Series switch.



**Note** The FCoE menu option appears only if the Cisco Nexus 5000 Series switch runs Cisco NX-OS Release 4.0(1a) or later releases.












- **FICON**—Allows you to configure and manage FICON VSANs, configure RLIR ERL information, swap selected FICON ports, and view FICON port numbers.
- **IP**—Allows you to configure and manage the following types of information: FCIP, iSCSI, iSNS, routes, VRRP, and CDP.
- **Security**—Allows you to configure and manage FCSP, port security, iSCSI security, SNMP security, common roles, SSH, AAA, and IP ACLs.
- **Admin**—Allows you to save, copy, edit, and erase the switch configuration, monitor events, manipulate Flash files, manage licenses, configure NTP, use CFS, and reset the switch. Also enables you to use the **show tech support**, **show cores**, and **show image** commands.
- **Logs**—Shows the various logs: message, hardware, events, and accounting. Also displays FICON link incidents, and allows you to configure the syslog setup.
- **Help**—Displays online help topics for specific dialog boxes in the Information pane.

## Toolbar Icons

The Device Manager toolbar provides quick access to many Device Manager features. Once the icon is selected, a dialog box may open that allows configuration of the feature. The toolbar provides the main Device and Summary View icons as shown in [Table 8-1](#).



**Table 8-1**      **Device Manager Main Toolbar**

| Icon                                                                                                                   | Description                                                                                               |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
|  Open Device                          | Opens the Device Manager view for another switch, with the option to open this view in a separate window. |
|  Refresh Display                      | Communicates with the switch and displays the information in the Device Manager view.                     |
|  Command-Line Interface               | Opens a separate CLI command window to the switch.                                                        |
|  Configure Selected                   | Opens a configuration dialog box for the selected component (line card or port).                          |
|  SysLog                               | Opens a window that lists the latest system messages that occurred on the switch.                         |
|  VSANs                                | Opens the VSAN dialog box that provides VSAN configuration for the switch.                                |
|  Save Configuration                 | Saves the current running configuration to the startup configuration.                                     |
|  Copy                               | Copies configuration file between server and switch.                                                      |
|  Toggle FICON/Interface Port Labels | Toggles the FICON and interface port labels.                                                              |
|  Select VSAN                        | Filters the port display to show only those ports belonging to the selected VSAN.                         |
|  Help                               | Accesses online help for Device Manager.                                                                  |

## Dialog Boxes

If a toolbar icon is selected, a dialog box may open that allows configuration of the selected feature. The dialog box may include table manipulation icons. See the [“Information Pane” section on page 7-5](#) for descriptions of these icons.



## Tabs

Click the **Device** tab on the Device Manager main window to see a graphical representation of the switch chassis and components.

**Note**

The Device view also shows the switch chassis information of the Cisco Nexus 2000 Series Fabric Extenders (FEXs) that are connected to a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 5.0(1).

Click the **Summary** tab on the Device Manager main window to see a summary of active interfaces on a single switch, as well as Fibre Channel and IP neighbor devices. The Summary View also displays port speed, link utilization, and other traffic statistics. There are two buttons in the upper left corner of the Summary View tab used to monitor traffic. To monitor traffic for selected objects, click the **Monitor Selected Interface Traffic Util%** button. To display detailed statistics for selected objects, click the **Monitor Selected Interface Traffic Details** button. You can set the poll interval, the type or Rx/Tx display, and the thresholds.

**Note**

The Summary tab does not display the utilization statistics (Util%) of virtual Fibre Channel interfaces for Cisco Nexus 5000 Series switches that run Cisco NX-OS Release 4.2.

## Legend

The legend at the bottom right of the Device Manager indicates port status, as follows:

**Colors**

- Green—The port is up.
- Brown—The port is administratively down.
- Red cross—The port is down or has failed as a result of either hardware failure, loopback Diagnostic failure, or link failure.
- Red square—The port is down or has failed as a result of failure other than described for red cross.
- Amber—The port has a minor fault condition as a result of either signal loss, synchronization loss, credit loss, LIP F8 receiver failure, non operational sequence receiver, or off-line sequence receiver failure.
- Gray—The port is unreachable.
- Blue—The port is out of service.

**Labels**

- X—Link failure
- E—ISL
- TE—Multi-VSAN ISL
- F—Host/storage
- FL—F loop
- I— iSCSI
- SD—SPAN destination



- CH—Channel
- CU—Control Unit
- NP—Proxy N-Port (NPV Mode)
- TNP—Trunking NP\_Port (NPV Mode)
- TF—Trunking F\_Port
- f—vFC Present (Cisco Nexus 5000 Series switches only)

## Supervisor and Switching Modules

In the Device View, you can right-click an object and get information on it, or configure it. If you right-click a module, the menu shows the module number and gives you the option to configure or reset the module. If you right-click a port, the menu shows the port number and gives you the option to configure, monitor, enable/disable, set beacon mode, or perform diagnostics on the port.



### Tip

You can select multiple ports in Device Manager and apply options to all the selected ports at one time. Either select the ports by clicking the mouse and dragging it around them, or hold down the **Control** key and click each port.

To enable or disable a port, right-click the port and click **Enable** or **Disable** from the pop-up menu. To enable or disable multiple ports, drag the mouse to select the ports and then right-click the selected ports. Then click **Enable** or **Disable** from the pop-up menu.

To manage trunking on one or more ports, right-click the ports and click **Configure**. In the dialog box that appears, right-click the current value in the Trunk column and click **nonTrunk**, **trunk**, or **auto** from the pull-down list.

To create PortChannels using Device Manager, click **PortChannels** from the Interface menu.



### Note

To create a PortChannel, all the ports on both ends of the link must have the same port speed, trunking type, and administrative state.

## Context Menus

Context menus are available in both Device Manager views by right-clicking a device or table.

From Device View:

- Device—Right-click a system, module, or power supply to bring up a menu that gives you the option to configure or reset the device.
- Port— Right-click a port to bring up a menu that shows you the number of the port you have clicked, and to give you the option to configure, monitor, enable, disable, set beacon mode, or perform diagnostics on the port.

From Summary View:

- Table— Right-click the table header to show a list of which columns to display in that table: Interface, Description, VSANs, Mode, Connected To, Speed (Gb), Rx, Tx, Errors, Discards, and Log. Click the Description field to bring up the appropriate configuration dialog box for the port type.



# Launching Device Manager

To launch Device Manager from your desktop, double-click the **Device Manager** icon and follow the instructions described in the *Cisco DCNM Installation and Licensing Guide*.

## DETAILED STEPS

- Step 1** You can choose one of the following three steps
- Right-click the switch you want to manage on the Fabric pane map and choose **Device Manager** from the menu that appears.
  - Double-click a switch in the Fabric pane map.
  - Select a switch in the Fabric pane map and choose **Tools > Device Manager**.

You see the Device Manager open dialog box as shown in [Figure 8-2](#)

**Figure 8-2** Device Manager: Open Dialog Box



- Step 2** Enter the IP address of the device.
- Step 3** Enter the user name and password.
- Step 4** Check the Proxy SNMP through FMS check box if you want Device Manager Client to use a TCP-based proxy server.
- Step 5** Choose the Auth-Privacy option according to the privacy protocol you have configured on your switch:
- If you have not configured the switch with a privacy protocol, then choose Auth-Privacy option MD5 (no privacy).
  - If you have configured the switch with your privacy protocol, choose your Auth-Privacy choice.
- Step 6** Click **Open** to open the Device Manager.



# Setting Device Manager Preferences

To set your preferences for the behavior of the Device Manager application, choose **Device > Preferences** from the Device menu. You can set the following preferences:

- **Retry Requests x Time(s) After x sec Timeout**—Allows you to set the retry request values. The default settings are 1 time after a 5-second timeout.
- **Enable Status Polling Every x secs**—Allows you to set the status polling value. The default setting is enabled (checked) with a time of 40 seconds.
- **Trace SNMP Packets in Message Log**—Allows you to set whether Device Manager traces SNMP packets and logs the trace. The default setting is disabled (unchecked).
- **Register for Events After Open, Listen on Port 1163**—Allows you to register this switch so that events are logged once you open Device Manager. The default setting is enabled (checked).
- **Show WorldWideName (WWN) Vendor**—Displays the world wide name vendor name in any table or listing displayed by Device Manager. If **Prepend** is checked, the name is displayed in front of the IP address of the switch. If **Replace** is checked, the name is displayed instead of the IP address. The default setting is enabled (checked) with the **Prepend** option.
- **Show Timestamps as Date/Time**—Displays timestamps in the date/time format. If this preference is not checked, timestamps are displayed as elapsed time. The default setting is enabled (checked).
- **Telnet Path**—Sets the path for the telnet.exe file on your system. The default is **telnet.exe**, but you need to browse for the correct location.

**Note**

If you browse for a path or enter a path and you have a space in the pathname (for example, **c:\program files\telnet.exe**, then the path will not work. To get the path to work, manually place quotes around it (for example, "**c:\program files\telnet.exe**").

- **Use Secure Shell Instead of Telnet**—Specifies whether to use SSH or Telnet when using the CLI to communicate with the switch. If enabled, you must specify the path to your SSH application. The default setting is disabled.
- **CLI Session Timeout x secs (0= disable)**—Specifies the timeout interval for a CLI session. Enter 0 to disable (no timeout value). The default setting is 30 seconds.
- **Show Tooltips in Physical View**—Determines whether tooltips are displayed in Physical (Device) View. The default setting is enabled (checked).
- **Label Physical View Ports With:**—Specifies the type of label to assign to the ports when you are in Physical (Device) View. The options are FICON and Interface. The default setting is Interface.
- **Export Table**—Specifies the type of file that is created when you export a table using Device Manager. The options are Tab-Delimited or XML. The default setting is Tab-Delimited.









# Configuring Performance Manager

This chapter describes how DCNM-SAN is used to monitor and manage a network. This chapter includes the following topics:

- [Information About Performance Manager, page 9-1](#)
- [Flow Statistics, page 9-4](#)
- [Flow Setup Wizards, page 9-5](#)

## Information About Performance Manager

This section includes the following topics:

- [Data Interpolation, page 9-2](#)
- [Data Collection, page 9-2](#)
- [Using Performance Thresholds, page 9-3](#)
- [Creating a Flow Using Performance Manager Flow Wizard, page 9-5](#)

Performance Manager gathers network device statistics historically and provides this information graphically using a web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

The Performance Manager has three operational stages:

- **Definition**—The Flow Wizard sets up flows in the switches.
- **Collection**—The Web Server Performance Collection screen collects information on desired fabrics.
- **Presentation**—Generates web pages to present the collected data through DCNM-SAN Web Server.

Performance Manager can collect statistics for ISLs, hosts, storage elements, and configured flows. Flows are defined based on a host-to-storage (or storage-to-host) link. Performance Manager gathers statistics from across the fabric based on collection configuration files. These files determine which SAN elements and SAN links Performance Manager gathers statistics for. Based on this configuration, Performance Manager communicates with the appropriate devices (switches, hosts, or storage elements) and collects the appropriate information at fixed five-minute intervals.

Performance Manager uses a round-robin database to hold the statistical data collected from the fabric. This data is stored based on the configured parameters in the collection configuration file. At each polling interval, Performance Manager gathers the relevant statistics and stores them in the round-robin database. This database is a fixed size and will not grow beyond its preset limits.



Performance Manager creates a series of archived data to hold summarized information present in the real-time round-robin database. This archived data is used to generate daily, weekly, monthly, and yearly consolidated reports. In this way, Performance Manager maintains significant historical data without the cost of an ever-increasing database size.

**Note**

You must restart Performance Manager if you change the user credentials on DCNM-SAN Server.

## Data Interpolation

One of the unique features of Performance Manager is its ability to interpolate data when statistical polling results are missing or delayed. Other performance tools may store the missing data point as zero, but this can distort historical trending. Performance Manager interpolates the missing data point by comparing the data point that preceded the missing data and the data point stored in the polling interval after the missing data. This maintains the continuity of the performance information.

## Data Collection

One year's worth of data for two variables (Rx and Tx bytes) requires a round-robin database (rrd) file size of 76 K. If errors and discards are also collected, the rrd file size becomes 110 K. The default internal values are as follows:

- 600 samples of 5 minutes (2 days and 2 hours)
- 700 samples of 30 minutes (12.5 days)
- 775 samples of 2 hours (50 days)
- 300 samples of 1 day

A 1000-port SAN requires 110 MB for a year's worth of historical data that includes errors and discards. If there were 20 switches in this SAN with equal distribution of fabric ports, about two to three SNMP packets per switch would be sent every 5 minutes for a total of about 100 request or response SNMP packets required to monitor the data.

Because of their variable counter requests, flows are more difficult to predict storage space requirements for. But in general you can expect that, each extra flow adds another 76 KB.

**Note**

Performance Manager does not collect statistics on nonmanageable and non-MDS switches. Loop devices (FL/NL) are not collected.

To setup a shared RRD path to collect PM data, perform these steps:

- 
- Step 1** Locate the server.properties file.
- For Windows setup, location is: *C:\Program Files\Cisco Systems\dcm\fm\conf*
- For Linux setup, location is: */usr/local/cisco/dcm/fm/conf*.
- Step 2** Add **pm.rrdpath** property file information to the server.properties file.
- For example:
- Add server location accessible from the DCNM server in the format:
- ```
pm.rrdpath=\\server_ip\\public\\cisco\\data
```


- Step 3** Save *server.properties* file.
- Step 4** Restart the Cisco DCNM server.
-

**Note**

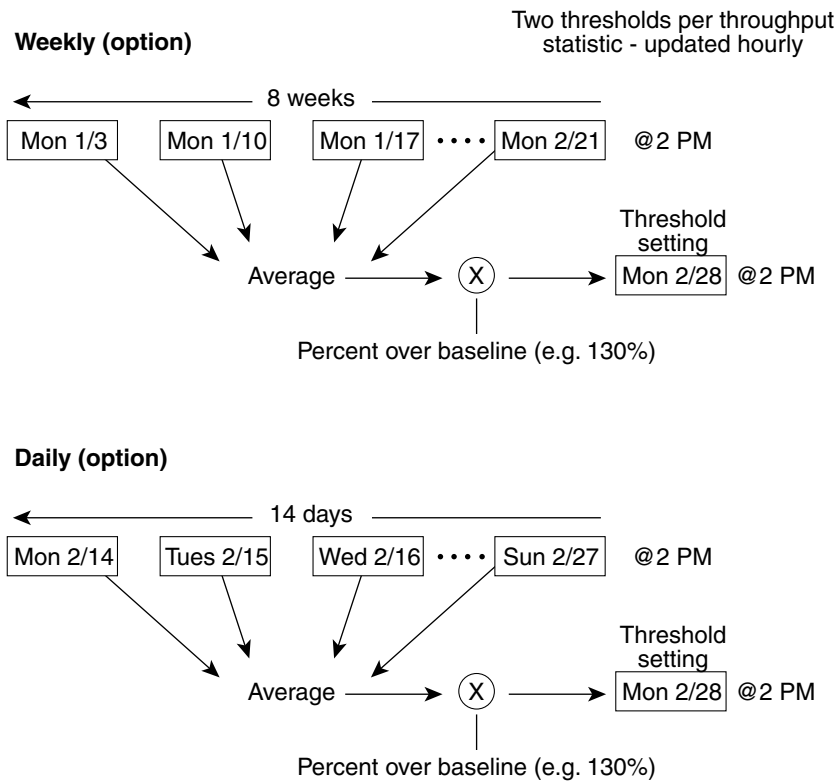
After the Performance Manager server is ready, the new updated location will be used to save the RRD files. Performance Manager creates a new directory **pm\ddb** under the specified location. Ensure that RRD files are not altered, as the Performance Manager server is actively writing into the rrd files.

Using Performance Thresholds

The Performance Manager Configuration Wizard allows you to set up two thresholds that will trigger events when the monitored traffic exceeds the percent utilization configured. These event triggers can be set as either Critical or Warning events that are reported on the DCNM-SAN web client Events browser page.

Absolute value thresholds apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the DCNM-SAN web client Events tab.

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every two weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated weighted average. [Figure 9-1](#) shows an example of setting a baseline threshold for a weekly or daily option.

Figure 9-1 *Baseline Threshold Example*

The threshold is set for Monday at 2 p.m. The baseline threshold is set at 130% of the average for that statistic. The average is calculated from the statistics value that occurred at 2 p.m. on Monday, for every prior Monday (for the weekly option) or the statistics value that occurred at 2 p.m. on each day, for every prior day (for the daily option).

Flow Statistics

Flow statistics count the ingress traffic in the aggregated statistics table. You can collect two kinds of statistics:

- Aggregated flow statistics to count the traffic for a VSAN.
- Flow statistics to count the traffic for a source and destination ID pair in a VSAN.

If you enable flow counters, you can enable a maximum of 1 K entries for aggregate flow and flow statistics. Be sure to assign an unused flow index to a module for each new flow. Flow indexes can be repeated across modules. The number space for flow index is shared between the aggregate flow statistics and the flow statistics.

Generation 1 modules allow a maximum of 1024 flow statements per module. Generation 2 modules allow a maximum of 2048-128 flow statements per module.

[Table 9-1](#) explains the Flow Type radio button that defines the type of traffic monitored.

Table 9-1 Performance Manager Flow Types

Flow type	Description
Host->Storage	Unidirectional flow, monitoring data from the host to the storage element
Storage->Host	Unidirectional flow, monitoring data from the storage element to the host
Both	Bidirectional flow, monitoring data to and from the host and storage elements

Flow Setup Wizards

The Performance Manager Flow and Performance Manager Setup wizards greatly simplify configuration. All you need to do is select the categories of statistics to capture and the wizards provide a list of flows and links to monitor. You can remove entries if desired, or just accept the provided list and start data collection. Statistics for host and storage links are not associated with a specific port on a switch, so you do not lose long term statistics if a connection is moved to a different port.

Creating a Flow Using Performance Manager Flow Wizard

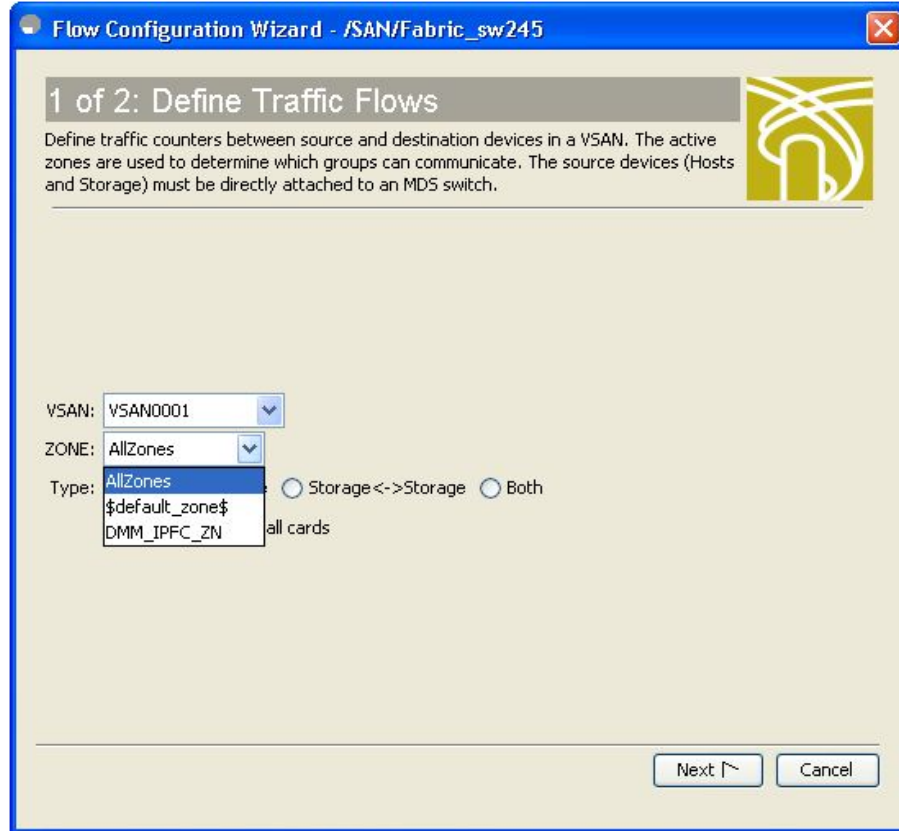
DETAILED STEPS

Step 1 Choose **Performance > Create Flows**.

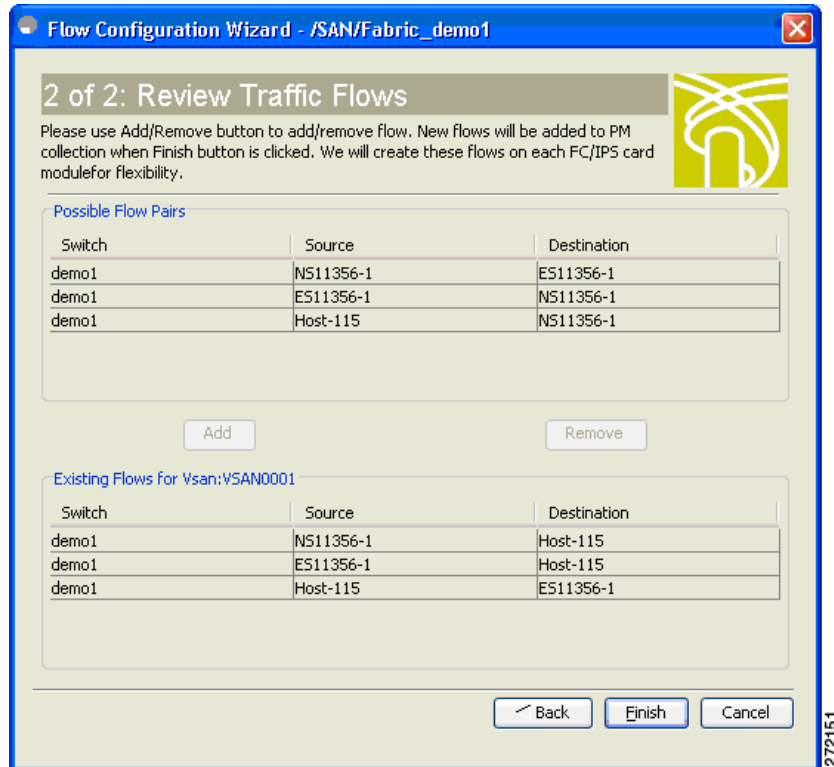
Specify how you want to determine and add new flows as shown in [Figure 9-2](#). For this, you have to define traffic counters between source and destination devices, via one of these options:

- In a VSAN - For this option, click **VSAN**.
- Based on high traffic devices - For this option, click **Device Traffic**. Note that PM collections must already be turned on in order to use this option. If PM collection is not turned on for the selected fabric, then an error message will appear and you cannot continue.

Step 2 If you have clicked **VSAN**, then:

Figure 9-2 Create Flows Dialog Box

- a. Click the drop-down menu in the VSAN field.
- b. Choose the list of VSANs provided by the flow configuration wizard.
- c. Click the drop-down menu in the Zone field.
- d. Choose the list of zones provided by the flow configuration wizard.
- e. Click **Next** to continue to the next window as shown in [Figure 9-3](#).

Figure 9-3 Review Traffic Flows Dialog Box

- f. Choose items in the Possible Flow Pairs area.
- g. The Review Traffic Flows window displays all VSAN flow pairs in the Existing Flows for Vsan area.
- h. Click **Add** to create the selected flow.
- i. Choose items in the Existing Flows for Vsan area.
- j. Click **Remove** to remove the selected flow.

Step 3 If you have clicked **Device Traffic**, then:

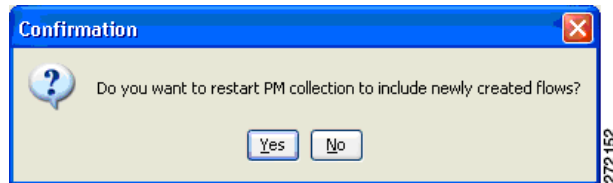
- a. Click **Next**.
You see the Define Traffic Flows page.
- b. Specify a traffic utilization percentage threshold value in the Show device ports with traffic > text box.
- c. Specify whether you want to look at the peak or average traffic values, over the last day or last week, for the traffic types:
 - Host<->Storage
 - Storage<->Storage
 - Both
- d. Click **Next**.
If new flow pairs are found, you will see the Review Traffic Flows page, where possible flow pairs are shown in a table, along with the traffic parameters used to identify them.
- e. To see only rows having a specific source or destination device, specify the name of the device in the **Filter** text box.

- f. To create a flow, click the corresponding row in the Possible Flow Pairs table, and then click **Add**.
To remove an existing flow, click the corresponding row in the Existing Flow Pairs table, and then click **Remove**.

Step 4 Click **Finish** to restart the Performance Manager collection.

You see the Confirmation dialog box as shown in [Figure 9-4](#).

Figure 9-4 Confirmation Dialog Box



To verify the newly created flow, choose **Physical Attributes > End Devices > Flow Statistics**. The newly created flows are displayed.



Note

Performance Manager Collection can be enabled for LAN devices and traffic counters are collected periodically.



Monitoring the Network

This chapter describes how the DCNM-SAN manages the network. In particular, SAN discovery and network monitoring are two of its key network management capabilities.

This chapter contains the following sections:

- [Information About Network Monitoring, page 10-1](#)
- [Device Discovery, page 10-2](#)
- [Topology Mapping, page 10-3](#)

Information About Network Monitoring

DCNM-SAN provides extensive SAN discovery, topology mapping, and information viewing capabilities. DCNM-SAN collects information on the fabric topology through SNMP queries to the switches connected to it. DCNM-SAN recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options such as fabric view, device view, summary view, and operation view.

Once DCNM-SAN is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, DCNM-SAN automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve the HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. DCNM-SAN gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

Monitoring Health and Events

DCNM-SAN works with the Cisco MDS 9000 Family switches to show the health and status of the fabric and switches. Information about the fabric and its components is gathered from multiple sources, including Online System Health Management, Call Home, system messages, and SNMP notifications. This information is then made available from multiple menus on DCNM-SAN or Device Manager.

DCNM-SAN Events Tab

The DCM-SAN Events tab, available from the topology window, displays the events DCM-SAN received from sources within the fabric. These sources include SNMP events, RMON events, system messages, and system health messages. The Events tab shows a table of events, including the event name, the source and time of the event, a severity level, and a description of the event. The table is sortable by any of these column headings.

**Note**

Cisco DCM SAN client displays events that are created after the client session is started. Any event created before the current user login session will not be retrieved and displayed.

Event Information in DCM-SAN Web Server Reports

The DCM-SAN web server client displays collections of information gathered by the Performance Manager. This information includes events sent to the DCM-SAN Server from the fabric. To open these reports, choose **Performance Manager > Reports**. This opens the web client in a web browser and displays a summary of all fabrics monitored by the DCM-SAN Server. Choose a fabric and then click the **Events** tab to see a summary or detailed report of the events that have occurred in the selected fabric. The summary view shows how many switches, ISLs, hosts, or storage elements are down on the fabric and how many warnings have been logged for that SAN entity. The detailed view shows a list of all events that have been logged from the fabric and can be filtered by severity, time period, or type.

Events in Device Manager

Device Manager displays the events when you choose **Logs > Events**. Device Manager can display the current list of events or an older list of events that has been stored on the DCM-SAN host. The event table shows details on each event, including time, source, severity, and a brief description of the event.

SAN Discovery and Topology Mapping

DCM-SAN provides extensive SAN discovery, topology mapping, and information viewing capabilities. DCM-SAN collects information on the fabric topology through SNMP queries to the switches connected to it. DCM-SAN recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options.

Device Discovery

Once DCM-SAN is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, DCM-SAN automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. DCM-SAN gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

For a VSAN change involving a third-party switch, DCNM-SAN will need a second discovery to show the correct topology due to the discovery dependency when there is any change in a mixed VSAN. The first discovery finds the third-party switch and the subsequent discovery will show the information on which VSAN it is going to join and can discover the end devices connected to it. You can wait for the subsequent discovery or trigger a manual discovery.

Topology Mapping

DCNM-SAN is built upon a topology representation of the fabric. DCNM-SAN provides an accurate view of multiple fabrics in a single window by displaying topology maps based on device discovery information. You can modify the topology map icon layout with an easy-to-use, drag-and-drop interface. The topology map visualizes device interconnections, highlights configuration information such as zones, VSANs, and ISLs exceeding utilization thresholds. The topology map also provides a visual context for launching command-line interface (CLI) sessions, configuring PortChannels, and opening device managers.

Using the Topology Map

The DCNM-SAN topology map can be customized to provide a view into the fabric that varies from showing all switches, end devices, and links, to showing only the core switches with single bold lines for any multiple links between switches. Use the icons along the left side of the topology map to control these views or right-click anywhere in the topology map to access the map controls.

You can zoom in or out on the topology map to see an overview of the SAN or focus on an area of importance. You can also open an overview window that shows the entire fabric. From this window, you can right-click and draw a box around the area you want to view in the main topology map view.

Another way to limit the scope of the topology display is to select a fabric or VSAN from the Logical Domains pane. The topology map displays only that fabric or VSAN.

Moving the mouse pointer over a link or switch provides a simple summary of that SAN component, along with a status indication. Right-clicking on the component brings up a pop-up menu. You can view the component in detail or access configuration or test features for that component.

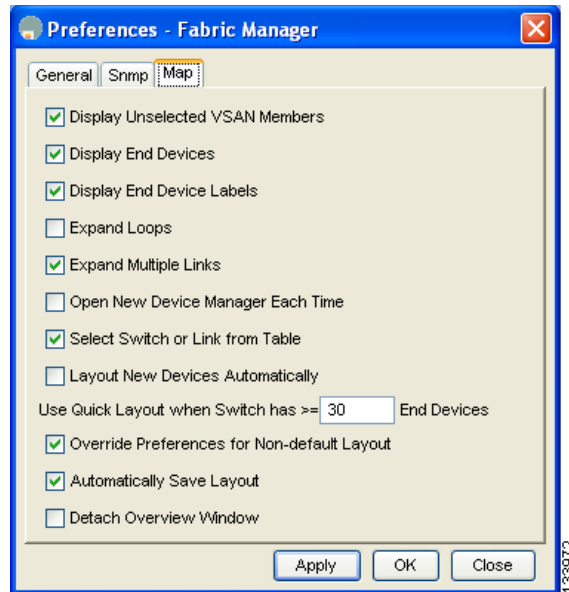
Double-click a link to bring link status and configuration information to the information pane.
Double-click a switch to bring up Device Manager for that switch.

Saving a Customized Topology Map Layout

Changes made to the topology map can be saved so that the customized view is available any time you open the DCNM-SAN Client for that fabric.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | Click File > Preferences to open the DCNM-SAN preferences dialog box. |
| Step 2 | Click the Map tab and check the Automatically Save Layout check box to save any changes to the topology map as shown in Figure 10-1 . |

Figure 10-1 DCNM-SAN Preferences

Step 3 Click **Apply**, and then click **OK** to save this change.

Using Enclosures with DCNM-SAN Topology Maps

Because not all devices are capable of responding to FC-GS-3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the topology map. See the [“Modifying the Device Grouping” section on page 7-38](#) to group these ports into a single enclosure for DCNM-SAN.

Clicking **Alias->Enclosure** displays hosts and storage elements in the Information pane. This is a shortcut to naming enclosures. To use this shortcut, highlight each row in the host or storage table that you want grouped in an enclosure then click **Alias -> Enclosure**. This automatically sets the enclosure names of each selected row with the first token of the alias.

Mapping Multiple Fabrics

To log into multiple fabrics, the same username and password must be used. The information for both fabrics is displayed, with no need to select a seed switch. To see details of a fabric, click the tab for that fabric at the bottom of the Fabric pane, or double-click the fabric’s cloud icon. To continuously manage a fabric using DCNM-SAN, follow the instructions in the [“Managing a Cisco DCNM-SAN Server Fabric” section on page 5-8](#).

Inventory Management

The Information pane in DCNM-SAN shows inventory, configuration, and status information for all switches, links, and hosts in the fabric. Inventory management includes vendor name and model, and software or firmware versions. Select a fabric or VSAN from the Logical Domains pane, and then select the **Summary** tab in the Information pane to get a count of the number of VSANS, switches, hosts, and

storage elements in the fabric. See the “[Cisco DCNM-SAN Client Quick Tour: Admin Perspective](#)” section on page 7-6 for more information on the DCNM-SAN user interface.

Using the Inventory Tab from DCNM-SAN Web Server

If you have configured DCNM-SAN Web Server, you can launch this application and access the Inventory tab to see a summary of the fabrics managed by the DCNM-SAN Server. The Inventory tab shows an inventory of the selected SAN, fabric, or switch. See [Chapter 3, “Cisco Prime DCNM Web Client”](#) for more information on how to configure and use DCNM-SAN Web Server.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Point your browser at the DCNM-SAN Web Server. |
| Step 2 | Click the Events tab and then the Details tab to view the system messages. The columns in the events table are sortable. In addition, you can use the Filter button to limit the scope of messages within the table. |
-

Viewing Logs from Device Manager

You can view system messages from Device Manager if Device Manager is running from the same workstation as the DCNM-SAN Server. Choose **Logs > Events > current** to view the system messages on Device Manager. The columns in the events table are sortable. In addition, you can use the Find button to locate text within the table.

You can view switch-resident logs even if you have not set up your local syslog server or your local PC is not in the switch's syslog server list. Due to memory constraints, these logs will wrap when they reach a certain size. The switch syslog has two logs: an NVRAM log that holds a limited number of critical and greater messages and a nonpersistent log that contains notice or greater severity messages. Hardware messages are part of these logs.

**Note**

To view syslog local logs, you need to configure the IP address of the DCNM-SAN Server in the syslog host.



Monitoring Performance

This chapter describes how to configure Performance Monitoring tools for Cisco DCNM-SAN and Device Manager. These tools provide real-time statistics as well as historical performance monitoring.

This chapter contains the following sections:

- [Information About Performance Monitoring, page 11-1](#)
- [Configuring Performance Manager, page 11-2](#)
- [Configuring the Summary View in Device Manager, page 11-4](#)
- [Configuring Per Port Monitoring using Device Manager, page 11-4](#)
- [Displaying DCNM-SAN Real-Time ISL Statistics, page 11-5](#)
- [Displaying Performance Manager Reports, page 11-7](#)
- [Generating Performance Manager Reports, page 11-9](#)
- [Exporting Data Collections, page 11-12](#)
- [Analyzing SAN Health, page 11-13](#)

Information About Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. Real-time performance statistics are useful for dynamic troubleshooting and fault isolation within the fabric. Real-time statistics gather data on parts of the fabric in user-configurable intervals and display these results in DCNM-SAN and Device Manager. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data.

Real-Time Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. These statistics show the performance of the selected port in real-time and can be used for performance monitoring and troubleshooting. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data. You can set the polling interval from ten seconds to one hour, and display the results based on a number of selectable options including absolute value, value per second, and minimum or maximum value per second.

Device Manager checking for oversubscription on the host-optimized four-port groups on relevant modules. Right-click the port group on a module and choose **Check Oversubscription** from the pop-up menu.

Device manager provides two performance views: the Summary View tab and the configurable monitor option per port.

Historical Performance Monitoring

Performance Manager gathers network device statistics historically and provides this information using DCNM-SAN client and web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer. See the [“Information About Performance Manager” section on page 9-1](#) for an overview of Performance Manager.

Configuring Performance Manager

This section includes the following topics:

- [Creating a Flow with Performance Manager, page 11-2](#)
- [Creating a Collection with Performance Manager, page 11-2](#)
- [Using Performance Thresholds, page 11-3](#)

Creating a Flow with Performance Manager

With the Flow Configuration Wizard you can create host-to-storage, storage-to-host, or bidirectional flows. Once defined, you can add these flows to a collection configuration file to monitor the traffic between a host/storage element pair. The flows created become part of the collection options in the Performance Manager Configuration Wizard.

Creating a Collection with Performance Manager

The Performance Manager Configuration Wizard steps you through the process of creating collections using configuration files. Collections are defined for one or all VSANs in the fabric. Collections can include statistics from the SAN element types described in [Table 11-1](#).

Table 11-1 Performance Manager Collection Types

Collection Type	Description
ISLs	Collects link statistics for ISLs.
Host	Collects link statistics for SAN hosts.
Storage	Collects link statistics for a storage elements.
Flows	Collects flow statistics defined by the Flow Configuration Wizard.

Using Performance Thresholds

The Performance Manager Configuration Wizard allows you to set up two thresholds that trigger events when the monitored traffic exceeds the percent utilization configured. These event triggers can be set as either Critical or Warning events that are reported on the DCNM-SAN web client Events browser page.

You must choose either absolute value thresholds or baseline thresholds that apply to all transmit or receive traffic defined in the collection. Click the **Use absolute values** radio button on the last screen of the Performance Manager Configuration Wizard to configure thresholds that apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the DCNM-SAN web client Events tab.

As an example, the collection has absolute value thresholds set for 60% utilization (for warning) and 80% utilization (for critical). If Performance Manager detects that the traffic on a 1-Gigabit link in its collection exceeds 600 Mbps, a warning event is triggered. If the traffic exceeds 800 Mbps, a critical event is triggered.

Baseline thresholds are defined for a configured time of day or week (1 day, 1 week, or 2 weeks). The baseline is created by calculating the average of the statistical results for the configured time each day, week, or every 2 weeks. [Table 11-2](#) shows an example of the statistics used to create the baseline value for a collection defined at 4 pm on a Wednesday.

Table 11-2 Baseline Time Periods for a Collection Started on Wednesday at 4pm

Baseline Time Window	Statistics Used in Average Calculation
1 day	Every prior day at 4 pm
1 week	Every prior Wednesday at 4 pm
2 weeks	Every other prior Wednesday at 4 pm

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every 2 weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated average.

As an example, a collection is created at 4 pm on Wednesday, with baseline thresholds set for 1 week, at 150% of the average (warning) and 200% of the average (critical). Performance Manager recalculates the average for each link at 4 pm every Wednesday by taking the statistics gathered at that time each Wednesday since the collection started. Using this as the new average, Performance Manager compares each received traffic statistic against this value and sends a warning or critical event if the traffic on a link exceeds this average by 150% or 200% respectively.

[Table 11-3](#) shows two examples of 1-Gigabit links with different averages in our example collection and at what traffic measurements the Warning and Critical events are sent.

Table 11-3 Example of Events Generated for 1-Gigabit Links

Average	Warning Event Sent at 150%	Critical Event Sent at 200%
400 Mbps	600 Mbps	800 Mbps
200 Mbps	300 Mbps	400 Mbps

Set these thresholds on the last screen of the Collections Configuration Wizard by checking the **Send events if traffic exceeds threshold** check box.

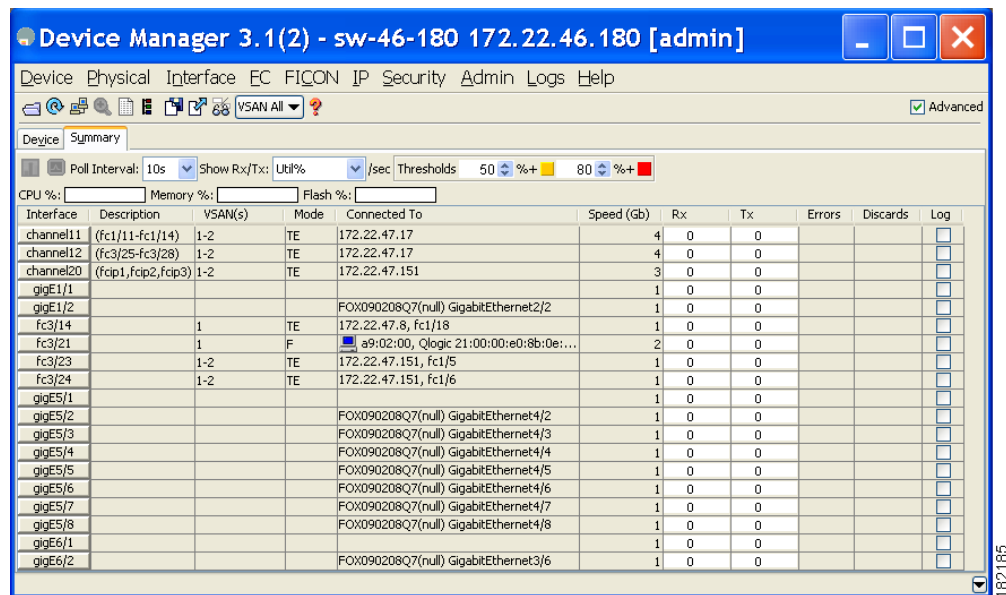
Configuring the Summary View in Device Manager

DETAILED STEPS

Step 1 Click the **Summary** tab on the main display.

You see all of the active ports on the switch, as well as the configuration options available from the Summary view shown in [Figure 11-1](#).

Figure 11-1 Device Manager Summary Tab



Step 2 Choose a value from the Poll Interval drop-down list.

Step 3 Decide how you want your data to be interpreted by looking at the Show Rx/Tx drop-down menu. The table updates each polling interval to show an overview of the receive and transmit data for each active port on the switch.

Step 4 Select a value from the **Show Rx/Tx** drop-down list. If you select **Util%**, you need to also select values from the two **Show Rx/Tx > % Util/sec** drop-down lists. The first value is the warning level and the second value is the critical threshold level for event reporting.

Note that you can also display percent utilization for a single port by selecting the port and clicking the **Monitor Selected Interface Traffic Util %** icon.

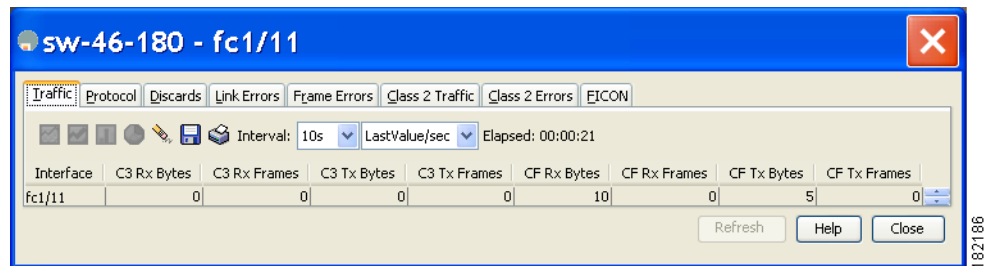
Configuring Per Port Monitoring using Device Manager

The configurable monitor per port option gives statistics for in and out traffic on that port, errors, class 2 traffic and other data that can be graphed over a period of time to give a real-time view into the performance of the port.

DETAILED STEPS

- Step 1** Click the **Device** tab.
- Step 2** Right-click the port you are interested in and choose **Monitor** from the drop-down menu. You see the port real-time monitor dialog box shown in [Figure 11-2](#).

Figure 11-2 Device Manager Monitor Dialog Box



- Step 3** Select a value from the Interval drop-down list to determine how often data is updated in the table shown here.
- Step 4** Click a statistical value in the table then click one of the graphing icons to display a running graph of that statistic over time. You see a graph window that contains options to change the graph type.



Tip You can open multiple graphs for statistics on any of the active ports on the switch.

Displaying DCNM-SAN Real-Time ISL Statistics

This section includes the following topics:

- [“Using the Performance Manager Configuration Wizard”](#) section on page 11-6
- [“Viewing Performance Statics Using DCNM-SAN”](#) section on page 11-6

You can configure DCNM-SAN to gather ISL statistics in real time. These ISL statistics include receive and transmit utilization, bytes per second, as well as errors and discards per ISL.

DETAILED STEPS

- Step 1** Choose **Performance > ISLs in Real-Time**. You see any ISL statistics in the Information pane as shown in [Figure 11-3](#).

Figure 11-3 ISL Performance in Real Time

Poll Interval: 10s Bandwidth 50 % 80 %													ISL Real-Time Performance	
From Switch	From Interface	To Switch	To Interface	Speed	Rx Util%	Rx Bytes	Rx Pkts	Tx Util%	Tx Bytes	Tx Pkts	Total Errors	Total Discards		
sw172-22-46-224	fc1/17	sw172-22-46-221	fc2/17	2 Gb	0	953	7	0	523	9	0	0		
sw172-22-46-223	fc1/7	sw172-22-46-222	fc1/7	2 Gb	0	50	0	0	6	0	0	0		
sw172-22-46-223	fc1/10	sw172-22-46-222	fc1/10	2 Gb	0	73	1	0	531	5	0	0		
sw172-22-46-223	fc1/11	sw172-22-46-222	fc1/11	2 Gb	0	88	1	0	547	5	0	0		
sw172-22-46-223	fc1/12	sw172-22-46-222	fc1/12	2 Gb	0	395	6	0	46	1	0	0		
sw172-22-46-223	fc1/14	sw172-22-46-222	fc1/14	2 Gb	0	64	0	0	28	0	0	0		
sw172-22-46-223	fc1/16	sw172-22-46-222	fc1/16	2 Gb	0	156	2	0	70	1	0	0		
sw172-22-46-222	fc1/1	sw172-22-46-221	fc2/29	2 Gb	0	1,308K	20	0	2,148K	17	0	0		
sw172-22-46-222	fc1/4	sw172-22-46-225	fc1/4	2 Gb	0	1,026K	13	0	1,648K	16	0	0		
sw172-22-46-225	fc1/3	sw172-22-47-118	fc1/20	2 Gb	0	0	0	0	0	0	0	0		
sw172-22-46-225	fc1/5	sw172-22-46-224	fc1/5	2 Gb	0	362	3	0	341	4	0	0		
sw172-22-46-225	fc1/9	sw172-22-46-224	fc1/9	2 Gb	0	244	3	0	364	4	0	0		

Step 2 Select a value from the **Poll Interval** drop-down list.

Step 3 Select two values from the **Bandwidth** utilization thresholds drop-down lists, one value for the minor threshold and one value for the major threshold.

The table shown updates each polling interval to show the statistics for all configured ISLs in the fabric.

Step 4 Select a row in the table to highlight that ISL in blue in the Topology map.

Using the Performance Manager Configuration Wizard

See the “[Viewing Performance Information](#)” section on page 3-27.

Viewing Performance Statics Using DCNM-SAN

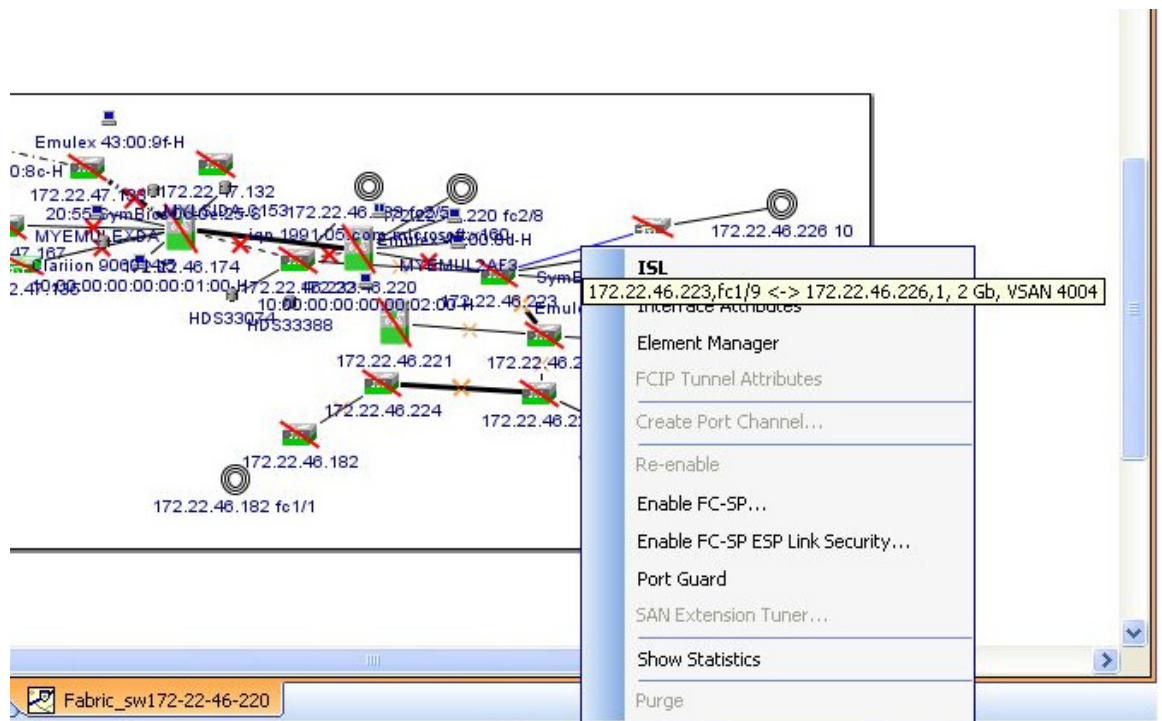
You can configure DCNM-SAN to gather historic and real time statistics of ISLs or End devices. These statistics include receive and transmit utilization, bytes per second, as well as errors and discards per ISL or end device.

DETAILED STEPS

Step 1 Right-click the ISL or end device in the Fabric pane.

You see a context menu as shown in the [Figure 11-4](#).

Step 2 Select **Show Statics**.

Figure 11-4 Show Statics Menu**Note**

Show Statics menu will be enabled only if you add the fabric to the Performance Manager collection.

Displaying Performance Manager Reports

This section includes the following topics:

- “Displaying Performance Summary” section on page 11-8
- “Displaying Performance Tables and Details Graphs” section on page 11-8
- “Displaying Performance of Host-Optimized Port Groups” section on page 11-8
- “Displaying Performance Manager Events” section on page 11-8

You can view Performance Manager statistical data using preconfigured reports that are built on demand and displayed in a web browser. These reports provide summary information as well as detailed statistics that can be viewed for daily, weekly, monthly, or yearly results.

DETAILED STEPS

- Step 1** Choose **Performance > Reports** to access Performance Manager reports from DCNM-SAN. This opens a web browser window showing the default DCNM-SAN web client event summary report.

- Step 2** Click the **Performance** tab to view the Performance Manager reports.
Performance Manager begins reporting data ten minutes after the collection is started.

**Note**

 DCNM-SAN Web Server must be running for reports to work.

Displaying Performance Summary

The Performance Summary page presents a dashboard display of the throughput and link utilization for hosts, ISLs, storage, and flows for the last 24-hour period. The summary provides a quick overview of the fabric's bandwidth consumption and highlights any hotspots.

The report includes network throughput pie charts and link utilization pie charts. Use the navigation tree on the left to show summary reports for monitored fabrics or VSANs. The summary displays charts for all hosts, storage elements, ISLs, and flows. Each pie chart shows the percent of entities (links, hosts, storage, ISLs, or flows) that measure throughput or link utilization on each of six predefined ranges. Move the mouse over a pie chart section to see how many entities exhibit that range of statistics. Double-click any pie chart to bring up a table of statistics for those hosts, storage elements, ISLs, or flows.

Displaying Performance Tables and Details Graphs

Click **Host**, **Storage**, **ISL**, or **Flow** to view traffic over the past day for all hosts, storage, ISLs, or flows respectively. A table lists all of the selected entities, showing transmit and receive traffic and errors and discards, if appropriate. The table can be sorted by any column heading. The table can also be filtered by day, week, month, or year. Tables for each category of statistics display average and peak throughput values and provide hot-links to more detailed information.

Clicking a link in any of the tables opens a details page that shows graphs for traffic by day, week, month, and year. If flows exist for that port, you can see which storage ports sent data. The details page also displays graphs for errors and discards if they are part of the statistics gathered and are not zero.

If you double-click a graph on a Detail report, it will launch the Cisco Traffic Analyzer for Fibre Channel, if configured. The aliases associated with hosts, storage devices, and VSANs in the fabric are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

Displaying Performance of Host-Optimized Port Groups

You can monitor the performance of host-optimized port groups by selecting **Performance > End Devices** and selecting **Port Groups** from the Type drop-down list.

Displaying Performance Manager Events

Performance Manager events are viewed through DCNM-SAN Web Server. To view problems and events in DCNM-SAN Web Server, choose a fabric and then click the **Events** tab to see a summary or detailed report of the problems and events that have occurred in the selected fabric.

Generating Performance Manager Reports

- [“Generating Top10 Reports in Performance Manager” section on page 11-9](#)
- [“Generating Top10 Reports Using Scripts” section on page 11-9](#)

Generating Top10 Reports in Performance Manager

You can generate historical Top10 reports that can be saved for later review. These reports list the entities from the data collection, with the most active entities appearing first. This is a static, one-time only report that generates averages and graphs of the data collection as a snapshot at the time the report is generated. These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated and are static. These are one-time reports that generate averages and graphs of the data collection as a snapshot at the time the report is generated.

**Tip**

Name the reports with a timestamp so that you can easily find the report for a given day or week.

These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated.

**Note**

Top10 reports require analyzing the existing data over an extended period of time and can take hours or more to generate on large fabrics.

See the [“Creating SAN User Defined Reports” section on page 3-42](#) for information on creating a Top10 report.

Generating Top10 Reports Using Scripts

You can generate Top10 reports manually by issuing the following commands:

- On UNIX, run the script:

```
"/<user_directory>/cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>"
```

- On Windows, run the script:

```
"c:\Program Files\Cisco Systems\MDS 9000\bin\pm.bat display pm\pm.xml  
<output_directory>"
```

On UNIX, you can automate the generation of the Top10 reports on your DCNM-SANDCNM-SAN Server host by adding the following cron entry to generate the reports once an hour:

```
0 * * * * /<user_directory>/cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>
```

If your crontab does not run automatically or Java complains about an exception similar to [Example 11-1](#), you need to add “-Djava.awt.headless=true” to the JVMARGS command in /<user_directory>/cisco_mds9000/bin/pm.sh.

Example 11-1 Example Java Exception

```
in thread "main" java.lang.InternalError Can't connect to X11 window server using '0.0' as
the value of the DISPLAY variable.
```

Configuring Performance Manager for Use with Cisco Traffic Analyzer

Performance Manager works in conjunction with the Cisco Traffic Analyzer to allow you to monitor and manage the traffic on your fabric. Using Cisco Traffic Analyzer with Performance Manager requires the following components:

- A configured Fibre Channel Switched Port Analyzer (SPAN) destination (SD) port to forward Fibre Channel traffic.
- A Port Analyzer Adapter 2 (PAA-2) to convert the Fibre Channel traffic to Ethernet traffic.
- Cisco Traffic Analyzer software to analyze the traffic from the PAA-2.

DETAILED STEPS

-
- Step 1** Set up the Cisco Traffic Analyzer according to the instructions in the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.
- Step 2** Get the following three items of information:
- The IP address of the management workstation on which you are running Performance Manager and Cisco Traffic Analyzer.
 - The path to the directory where Cisco Traffic Analyzer is installed.
 - The port that is used by Cisco Traffic Analyzer (the default is 3000).
- Step 3** Start the Cisco Traffic Analyzer.
- Choose **Performance > Traffic Analyzer > Open**.
 - Enter the URL for the Cisco Traffic Analyzer, in the format:
`http://<ip address>:<port number>`
ip address is the address of the management workstation on which you have installed the Cisco Traffic Analyzer
:port number is the port that is used by Cisco Traffic Analyzer (the default is :3000).
 - Click **OK**.
 - Choose **Performance > Traffic Analyzer > Start**.
 - Enter the location of the Cisco Traffic Analyzer, in the format:
`D:\<directory>\ntop.bat`
D: is the drive letter for the disk drive where the Cisco Traffic Analyzer is installed.
directory is the directory containing the ntop.bat file.
 - Click **OK**.
- Step 4** Create the flows you want Performance Manager to monitor, using the Flow Configuration Wizard. See the [“Creating a Flow with Performance Manager”](#) section on page 11-2

Step 5 Define the data collection you want Performance Manager to gather, using the Performance Manager Configuration Wizard. See the [“Creating a Collection with Performance Manager” section on page 11-2](#).

- a. Choose the VSAN you want to collect information for or choose **All VSANs**.
- b. Check the types of items you want to collect information for (Hosts, ISLs, Storage Devices, and Flows).
- c. Enter the URL for the Cisco Traffic Analyzer in the format:
`http://<ip address>/<directory>`
where:
ip address is the address of the management workstation on which you have installed the Cisco Traffic Analyzer, and *directory* is the path to the directory where the Cisco Traffic Analyzer is installed.
- d. Click **Next**.
- e. Review the data collection on this and the next section to make sure this is the data you want to collect.
- f. Click **Finish** to begin collecting data.



Note Data is not collected for JBOD or for virtual ports. If you change the data collection configuration parameters during a data collection, you must stop and restart the collection process for your changes to take effect.

Step 6 Choose **Performance > Reports** to generate a report. Performance Manager Web Server must be running. You see Web Services; click **Custom** then select a report template.



Note It takes at least five minutes to start collecting data for a report. Do not attempt to generate a report in Performance Manager during the first five minutes of collection.

Step 7 Click **Cisco Traffic Analyzer** at the top of the Host or Storage detail pages to view the Cisco Traffic Analyzer information, or choose **Performance > Traffic Analyzer > Open**. The Cisco Traffic Analyzer page will not open unless ntop has been started already.



Note For information on capturing a SPAN session and starting a Cisco Traffic Analyzer session to view it, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.



Note For information on viewing and interpreting your Performance Manager data, see the [“Creating a Flow with Performance Manager” section on page 11-2](#).

For information on viewing and interpreting your Cisco Traffic Analyzer data, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.

For performance drill-down, DCNM-SAN Server can launch the Cisco Traffic Analyzer in-context from the Performance Manager graphs. The aliases associated with hosts, storage devices, and VSANs are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

Exporting Data Collections

This section includes the following topics:

- “Exporting Data Collections to XML Files” section on page 11-12
- “Exporting Data Collections in Readable Format” section on page 11-12

Exporting Data Collections to XML Files

The RRD files used by Performance Manager can be exported to a freeware tool called rrdtool. The rrd files are located in pm/db on the DCNM-SAN Server. To export the collection to an XML file, enter the following command at the operating system command-line prompt:

```
/bin/pm.bat xport xxx yyy
```

In this command, *xxx* is the RRD file and *yyy* is the XML file that is generated. This XML file is in a format that rrdtool is capable of reading with the command:

```
rrdtool restore filename.xml filename.rrd
```

You can import an XML file with the command:

```
bin/pm.bat pm restore <xmlFile> <rrdFile>
```

This reads the XML export format that rrdtool is capable of writing with the command:

```
rrdtool xport filename.xml filename.rrd.
```

The **pm xport** and **pm restore** commands can be found on your DCNM-SAN Server at bin\PM.bat for Windows platforms or bin/PM.sh on UNIX platforms. For more information on the rrdtool, refer to the following website: <http://www.rrdtool.org>.

Exporting Data Collections in Readable Format

You can export the RRD files used by Performance Manager to a freeware tool called rrdtool and export the collection to an XML file. Cisco MDS SAN-OS Release 2.1(1a) introduces the inability to export data collections in comma-separated format (CSV). This format can be imported to various tools, including Microsoft Excel. You can export these readable data collections either from the DCNM-SAN Web Services menus or in batch mode from the command line on Windows or UNIX. Using DCNM-SAN Web Services, you can export one file. Using batch mode, you can export all collections in the pm.xml file.

**Note**

DCNM-SAN Web Server must be running for this to work.

You can export data collections to Microsoft Excel using DCNM-SAN Web Server.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Click the Performance tab on the main page.
You see the overview table. |
| Step 2 | Click the Flows sub-tab. |
| Step 3 | Right-click the name of the entity you want to export and select Export to Microsoft Excel .
You see the Excel chart for that entity in a pop-up window. |
-

You can export data collections using command-line batch mode.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Go to the installation directory on your workstation and then go to the bin directory. |
| Step 2 | On Windows, enter <code>.\pm.bat export C:\Program Files\Cisco Systems\MDS 9000\pm\pm.xml <export directory></code> . This creates the csv file (export.csv) in the <i>export directory</i> on your workstation. |
| Step 3 | On UNIX, enter <code>./pm.sh export /usr/local/cisco_mds9000/pm/pm.xml <export directory></code> . This creates the csv file (export.csv) in the <i>export directory</i> on your workstation. |
-

When you open this exported file in Microsoft Excel, the following information displays:

- Title of the entity you exported and the address of the switch the information came from.
- The maximum speed seen on the link to or from this entity.
- The VSAN ID and maximum speed.
- The timestamp, followed by the receive and transmit data rates in bytes per second.

Analyzing SAN Health

The SAN Health Advisor tool is a utility that used to monitor the performance and collect the statistics. You can perform the following tasks with this tool:

- Run Performance Monitor to collect I/O statistics
- Collect fabric inventory (switches and other devices)
- Create a graphical layout of fabric topology
- Create reports of error conditions and statistical data

You can install this tool at any SAN environment to collect I/O statistics for the specified time (usually 24 hours), generate health reports and automatically send reports to the designated system administrator for review at regular intervals.

When you start SAN Health Advisor tool, it runs in wizard mode, and prompts for inputs such as seed switch credentials, IP address of the server to which the data to be sent and all the necessary information for the software setup. As soon as the fabric is discovered, the tool starts capturing performance data, I/O statistics and error conditions.

The reports generated from the collection is stored in the `$INSTALLDIR/dcm/fm/reports` directory. These reports are automatically sent to the designated SAN administrator for review. In a situation where the tool fails to collect the data, it generates a report with an error message or exception. After sending the reports the tool automatically uninstalls itself and terminates all the processes that it established on the host machine.

The report that SAN Health Advisor tool generates will have the following details:

- Events
- System messages
- Analysis of connectivity
- Zone discrepancy
- System configuration
- Interface status
- Domain information
- Security settings

Installing the SAN Health Advisor Tool

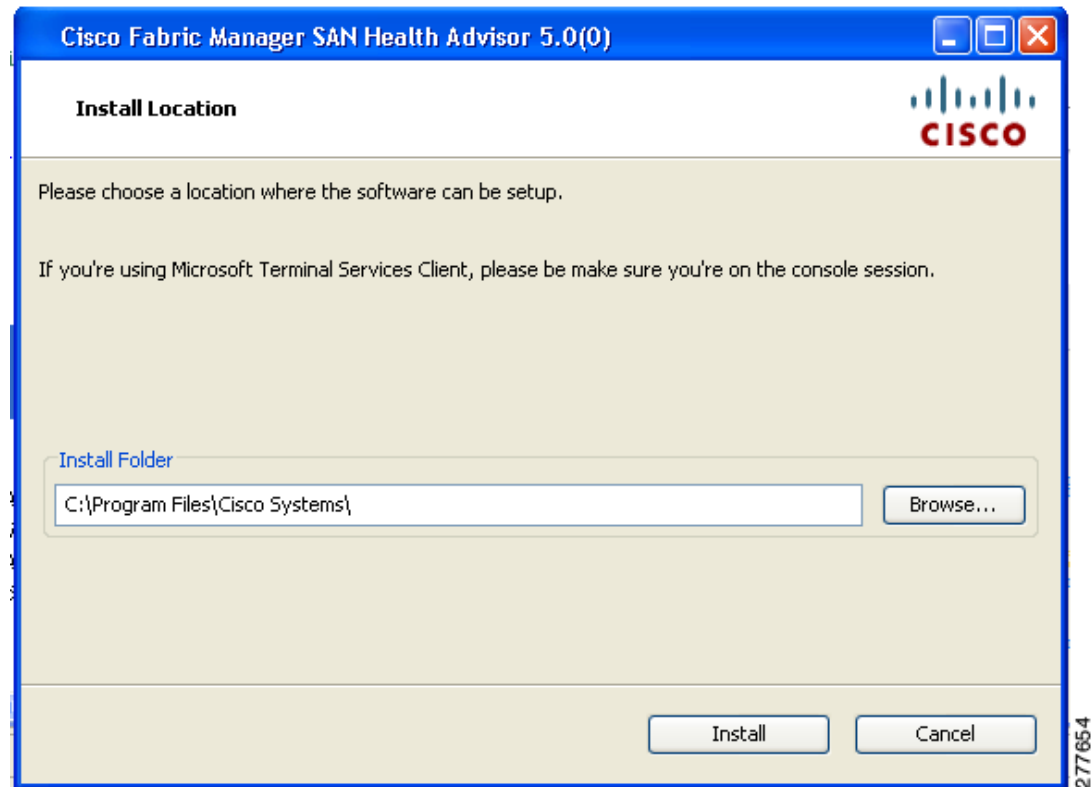
SAN Health Advisor tool can be installed and run on Windows, UNIX, and Solaris platforms. Install the package that contains the .jar file with JRE version 6.0.



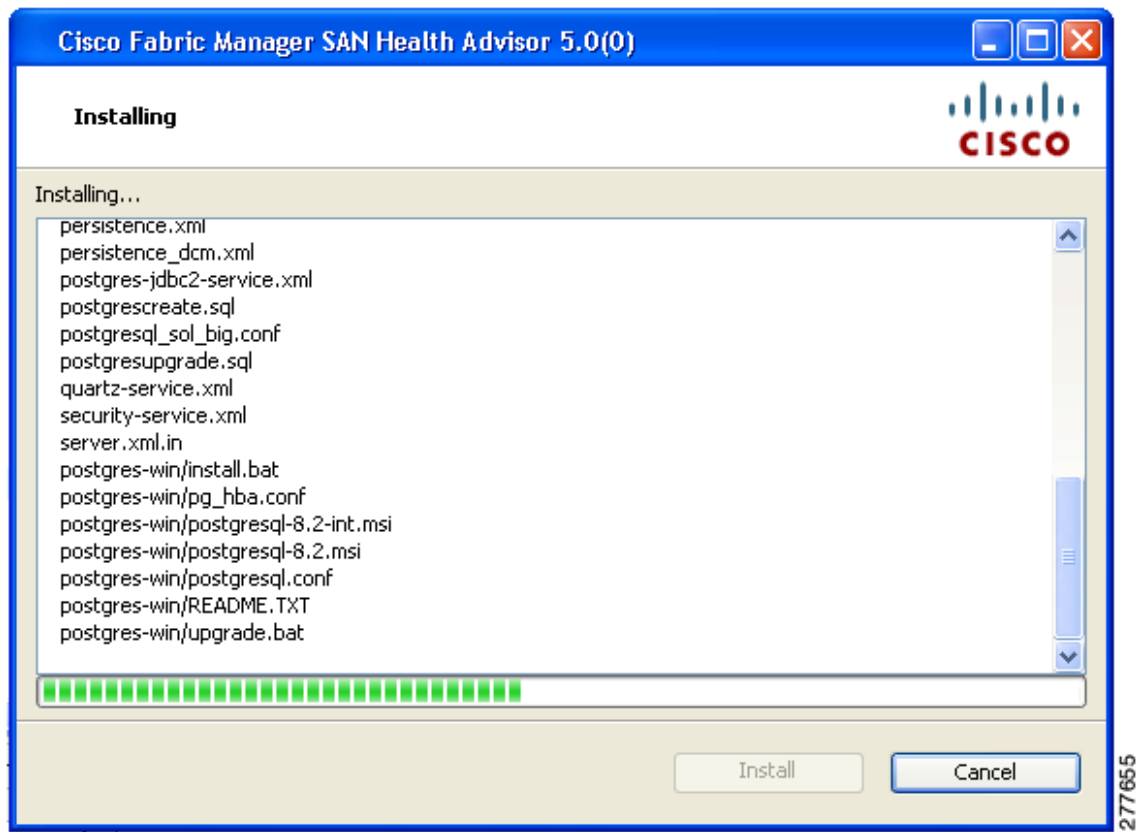
Note The SAN Health tool is not installed by default when you install DCNM-SAN software.

DETAILED STEPS

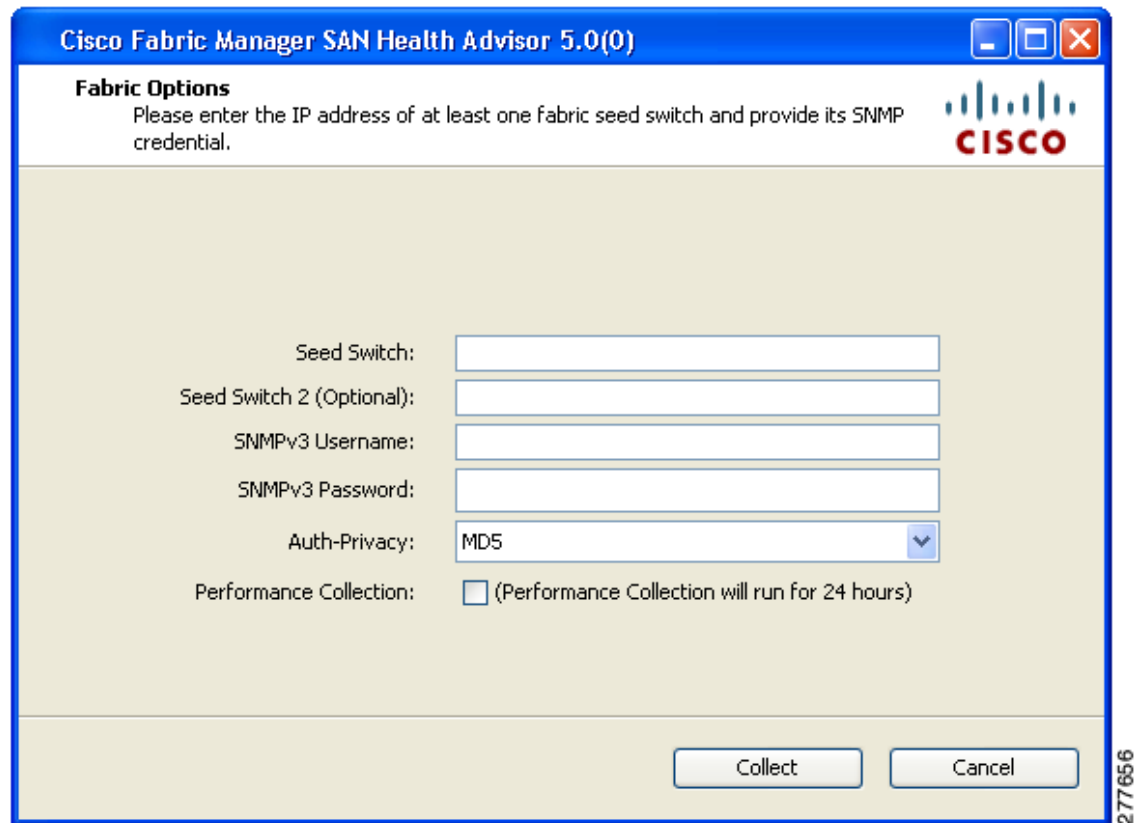
-
- Step 1** Double-click the San Health Advisor tool installer.
You see the San Health Advisor tool Installer window as shown in [Figure 11-5](#).

Figure 11-5 *SAN Health Advisor: Installer*

- Step 2** Select an installation folder on your workstation for SAN Health Advisor.
On Windows, the default location is **C:\Program Files\Cisco Systems**.
- Step 3** Click **Install** to start the installation.
You see the installation progressing as shown in [Figure 11-6](#).

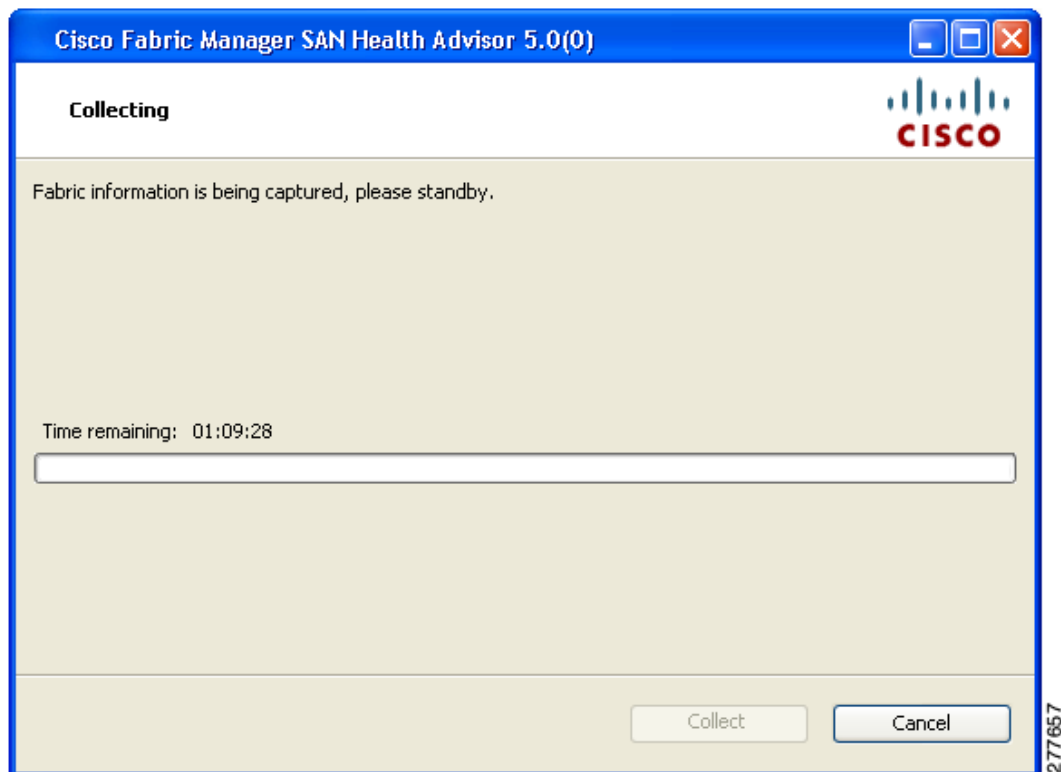
Figure 11-6 SAN Health Advisor: Installation in Progress

You see the Fabric Options dialog box as shown in [Figure 11-7](#)

Figure 11-7 SAN Health Advisor: Fabric Options

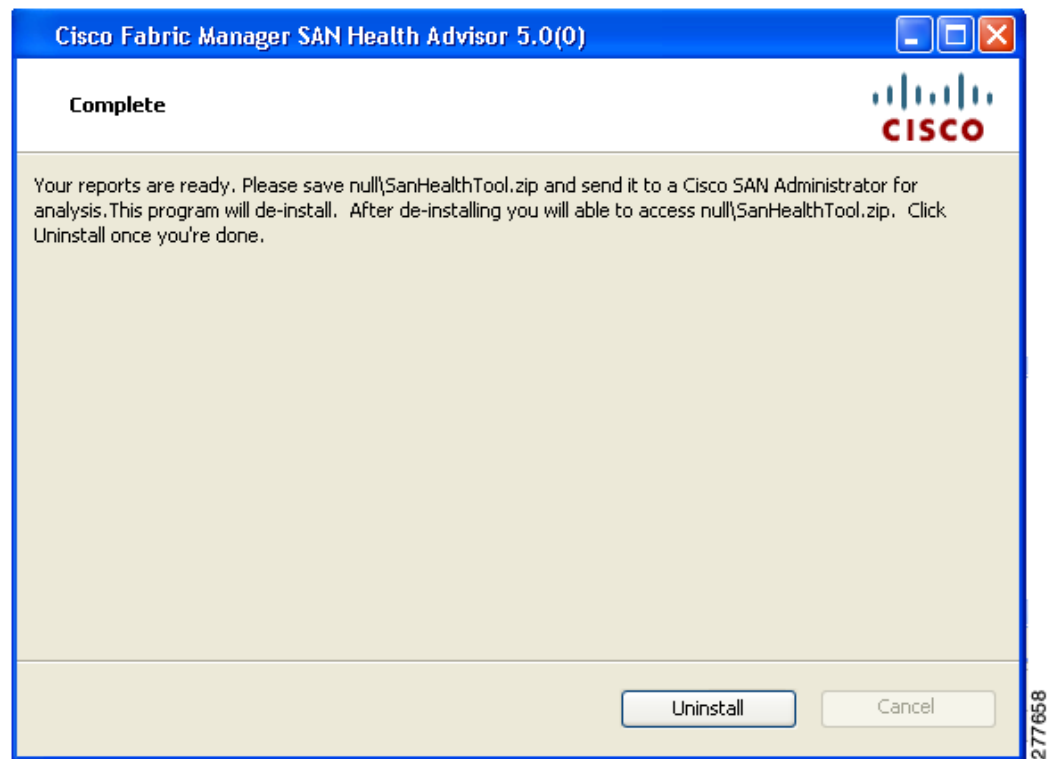
The image shows a Windows-style dialog box titled "Cisco Fabric Manager SAN Health Advisor 5.0(0)". The dialog has a blue title bar with standard minimize, maximize, and close buttons. Below the title bar, the text "Fabric Options" is displayed in bold, followed by the instruction: "Please enter the IP address of at least one fabric seed switch and provide its SNMP credential." The Cisco logo is in the top right corner. The main area of the dialog is light beige and contains several input fields and a checkbox. The fields are labeled: "Seed Switch:", "Seed Switch 2 (Optional):", "SNMPv3 Username:", "SNMPv3 Password:", and "Auth-Privacy:". The "Auth-Privacy:" field is a drop-down menu currently showing "MD5". Below these is a checkbox labeled "Performance Collection:" with the text "(Performance Collection will run for 24 hours)" to its right. At the bottom right of the dialog are two buttons: "Collect" and "Cancel". A vertical text label "277656" is positioned to the right of the dialog box.

- Step 4** In the Seed Switch text box, enter the IP address of the seed switch.
- Step 5** Enter the user name and password for the switch.
- Step 6** Select the authentication privacy option from the Auth-Privacy drop-down list box.
- Step 7** Click the **Performance Collection** check box to enable the process to run for 24 hours.
- Step 8** Click **Collect** to start gathering performance information.
- You see the collecting dialog box as shown in [Figure 11-8](#).

Figure 11-8 SAN Health Advisor: Collecting

If you want to stop gathering information in the middle of the process, click Cancel. You see the message indicating performance collection is complete as shown in [Figure 11-9](#).

Figure 11-9 SAN Health Advisor: Performance Collection Complete



Step 9 Click **Uninstall** to remove the SAN Health Advisor software.



CHAPTER 12

Overview of DCNM-LAN

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

For information about the specific Cisco Nexus products supported by DCNM-LAN, see the *Cisco DCNM Release Notes, Release 7.1.x*.

This chapter includes the following sections:

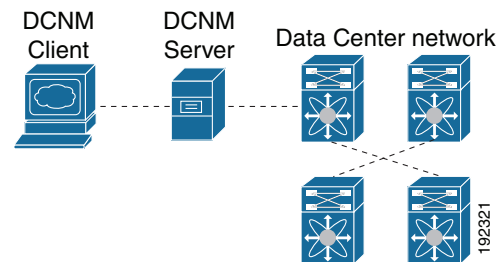
- [DCNM-LAN Client and Server, page 12-1](#)
- [Features in Cisco DCNM-LAN, Release 5.2, page 12-2](#)
- [Documentation About DCNM-LAN, page 12-3](#)

DCNM-LAN Client and Server

DCNM-LAN is a Java-based client-server application. For Java requirements, server system requirements, and client system requirements, see the *Cisco DCNM Release Notes, Release 7.1.x*.

[Figure 12-1](#) shows the DCNM-LAN client-server environment. The DCNM-LAN client communicates with the DCNM-LAN server only, never directly with managed Cisco NX-OS devices. The DCNM-LAN server uses the XML management interface of Cisco NX-OS devices to manage and monitor them. The XML management interface is a programmatic method based on the NETCONF protocol that complements the command-line interface (CLI) functionality. For more information, see the *Cisco NX-OS XML Interface User Guide*.

Figure 12-1 DCNM-LAN Client-Server Environment



Features in Cisco DCNM-LAN, Release 5.2

Cisco DCNM-LAN Release 7.1.x supports the configuration and monitoring of the following Cisco NX-OS features:

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

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

- Topology viewer
- Network servers

- Device groups
- Event browser
- Configuration Delivery Management
- Configuration Change Management
- Device OS Management
- Hardware and virtual switch inventory

DCNM-LAN includes the following administrative features:

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

Platform Support

DCNM-LAN supports the following platforms:

- Cisco Nexus 1000V switches
- Cisco Nexus 2000 Fabric Extenders
- Cisco Nexus 3000 Series switches
- Cisco Nexus 4000 Series switches
- Cisco Nexus 5000 Series switches
- Cisco Nexus 6000 Series switches
 - DCNM-LAN supports both fixed and removable expansion modules.
 - In DCNM-LAN, the interface breakout feature can be configured through configuring the delivery feature, and not as a part of configuring an Ethernet interface.
- Catalyst 6500

DCNM-LAN provides limited support for the Catalyst 6500 Series switches that runs classic IOS version 12.2(33)SXI or higher.

- DCNM-LAN supports the viewing of the current configuration attributes of the device.
- DCNM-LAN does not support changing the configuration of the device.
- DCNM-LAN supports the Firewall Service Module (FWSM) version 4.0 or higher for the Catalyst 6500 Series switches.
- Cisco Nexus 7000 Series switches

Documentation About DCNM-LAN

The documentation for DCNM-LAN includes several configuration guides and other documents. For more information about the DCNM-LAN documentation, see the [“Obtaining Documentation and Submitting a Service Request”](#) section on page 67.



CHAPTER 13

Installing and Launching the Cisco DCNM-LAN Client

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

This chapter includes the following sections:

- [Information About Installing and Launching the DCNM-LAN Client, page 13-1](#)
- [Prerequisites for Installing and Launching the DCNM-LAN Client, page 13-2](#)
- [Secure Client Communications, page 13-2](#)
- [Default Administrator Credentials, page 13-3](#)
- [Downloading and Launching the DCNM-LAN Client, page 13-3](#)
- [Restarting the DCNM-LAN Client, page 13-6](#)
- [Logging Into the DCNM-LAN Client, page 13-7](#)
- [Uninstalling the DCNM-LAN Client, page 13-8](#)
- [Modifying Cisco DCNM-LAN Server, page 13-9](#)
- [Additional References, page 13-11](#)
- [Feature History for Installing and Launching the DCNM-LAN Client, page 13-12](#)

Information About Installing and Launching the DCNM-LAN Client

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

Prerequisites for Installing and Launching the DCNM-LAN Client

Installing and using the DCNM-LAN client have the following prerequisites:

- Your system must be running a supported operating system to install and use the DCNM-LAN client software. For more information about client system requirements, see the *Cisco DCNM Release Notes, Release 7.1.x*, which are available at the following site:

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

- The installation process uses Java version 1.7.0_55 JRE. If your system does not have that version of Java, the installation process will install it to your system.

The DCNM-LAN client installer requires Internet access to download the Java version 1.7.0_55 JRE. If the system cannot access the Internet, use another system to download the Java installer and copy it to the system that you want to install the DCNM-LAN client on. You can download Java version JRE 1.7.0_55 from the Oracle Technology Network website.

If your network environment requires a proxy connection to permit the download of the Java installer, ensure that the proxy settings are configured in Internet Options, available from the Control Panel.

- Some DCNM-LAN features require a license. Before you can use licensed features, install the DCNM-LAN license. For more information about licensed features or for more information about the license installation, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

Secure Client Communications

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

For information about enabling secure client communication, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

Default Administrator Credentials

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

If no one has administrative access to DCNM-LAN, you can reset the local administrator account or change DCNM-LAN server authentication settings by reinstalling the DCNM-LAN server software. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

Downloading and Launching the DCNM-LAN Client

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

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

This section includes the following topics:

- [Using a Web Browser to Download and Launch the DCNM-LAN Client, page 13-3](#)
- [Using a Command Prompt to Download and Launch the DCNM-LAN Client, page 13-4](#)
- [Using a Command Prompt to Download and Launch the DCNM-LAN Client without using Java Web Start Launcher, page 13-5](#)

Using a Web Browser to Download and Launch the DCNM-LAN Client

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

BEFORE YOU BEGIN

The Java version JRE 1.7.0_55 must be installed on the computer that you want to run the DCNM-LAN client on.

The computer that you want to run the DCNM-LAN client on must meet the client system requirements. For details about the client system requirements, see the *Cisco DCNM Release Notes, Release 7.1.x*, available at the following site:

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

DETAILED STEPS

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

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

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

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

The browser shows the DCNM-LAN client page.

Step 2 Click **Launch DCNM Client**.

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

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

The DCNM-LAN client installer verifies that Java is already installed on your system. If the installer does not find the supported version of Java on the computer, the installer prompts you to install Java version JRE 1.7.0_55.



Note

The Cisco DCNM client installer requires Internet access to download the Java version JRE 1.7.0_55. If the system cannot access the Internet, use another system to download the Java installer, copy it to the system that you want to install the Cisco DCNM client on, install Java, and restart the Cisco DCNM client installation. You can download Java version JRE 1.7.0_55 from the Oracle Technology Network website.

If your network environment requires a proxy connection to permit the download of the Java installer, ensure that the proxy settings are configured in Internet Options, available from the Control Panel.

Step 4 If the installer prompts you to install Java version JRE 1.7.0_55, follow these steps:

- a. Click **OK** to begin installing the supported version of Java.
- b. If a security warning notifies you that the Java installer was digitally signed by an expired certificate, click **Run** to continue the installation.
- c. Complete the Java installation wizard.



Tip

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

The DCNM-LAN client installs on the computer.



Note

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

The DCNM-LAN client login window opens.

For detailed login steps, see the [“Logging Into the DCNM-LAN Client” section on page 13-7](#).

Using a Command Prompt to Download and Launch the DCNM-LAN Client

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

BEFORE YOU BEGIN

The Java version 1.7.0_55 JRE must be installed on the computer that you want to run the DCNM-LAN client on.

The computer that you want to run the DCNM-LAN client on must meet the client system requirements. For details about the client system requirements, see the *Cisco DCNM Release Notes, Release 7.1.x*, available at the following site:

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

DETAILED STEPS

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

Step 2 Use the **cd** command to change the directory to the bin directory under the Java version 1.7.0_55 installation directory, as follows:

cd *path*

where *path* is the relative or absolute path to the bin directory. For example, on Microsoft Windows, the default path to the Java version 1.7.0_55 bin directory is C:\Program Files\dcn\Java\jre1.7.0_55\bin.

Step 3 Enter the applicable command as follows:

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

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



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

The DCNM-LAN client login window opens.

For detailed login steps, see the “[Logging Into the DCNM-LAN Client](#)” section on page 13-7.

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

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

BEFORE YOU BEGIN

The Java version 1.7.0_55 JRE must be installed on the computer that you want to run the DCNM-LAN client on.

The computer that you want to run the DCNM-LAN client on must meet the client system requirements. For details about the client system requirements, see the *Cisco DCNM Release Notes, Release 7.1.x*, available at the following site:

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

**Note**

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

DETAILED STEPS

-
- Step 1** Access a command prompt on the computer where the DCNM-LAN server is installed and navigate to the directory where the DCNM-LAN server is installed.
- On a Windows DCNM-LAN server, the DCNM-LAN server is installed in <DCNM_INSTALL_LOCATION>\dcm\dcnm\ui-client directory.
The default for <DCNM_INSTALL_LOCATION> is C:\Program Files\Cisco Systems.
 - On a RHEL DCNM-LAN server, the DCNM-LAN server is installed in <DCNM_INSTALL_LOCATION>/dcm/dcnm/ui-client directory.
The default for <DCNM_INSTALL_LOCATION> is /usr/cisco.
- Step 2** In the ui-client directory, locate and run the construct_DCNM_LAN_SA_Client script.
- On a Windows DCNM-LAN server, run construct_DCNM_LAN_SA_Client.bat.
 - On a RHEL DCNM-LAN server, run construct_DCNM_LAN_SA_Client.sh.
- Step 3** Copy the ui-client directory to the computer that you want to run the DCNM-LAN client on.
- Step 4** On the computer that you are preparing for the DCNM-LAN client, access a command prompt and set JAVA_HOME to the location where the Java JRE is installed.
For example:
- For Microsoft Windows:
set JAVA_HOME=C:\Program Files\Java\jre1.7.0_55
 - For RHEL:
export JAVA_HOME=/usr/java/jre1.7.0_55
- Step 5** On the computer that you are preparing for the DCNM-LAN client, navigate to the ui-client directory that was copied from the DCNM-LAN server.
- Step 6** In the ui-client directory, locate and run the dcnm-client-sa script to launch the DCNM-LAN client.
- On a Windows DCNM-LAN server, run dcnm-client-sa.bat.
 - On a RHEL DCNM-LAN server, run dcnm-client-sa.sh.
- The DCNM-LAN client login window opens.
- For detailed login steps, see the “[Logging Into the DCNM-LAN Client](#)” section on page 13-7.
-

Restarting the DCNM-LAN Client

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

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

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

For detailed login steps, see the [“Logging Into the DCNM-LAN Client” section on page 13-7](#).

Logging Into the DCNM-LAN Client

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

BEFORE YOU BEGIN

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

- A valid DCNM-LAN username and password.
- The IP address or DNS name of the DCNM-LAN server.
- The DCNM-LAN server port number. By default, the server port number is 1099.
- Proxy server address, HTTP port number, and Socks port number, if a proxy server is required by your network environment.

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | Start the DCNM-LAN client. If you have previously downloaded and launched the DCNM-LAN client on the computer, you can start the client by using one of the shortcuts added to the computer by the client installer. For more information about downloading and launching the client, see one of the following topics: <ul style="list-style-type: none">• Using a Web Browser to Download and Launch the DCNM-LAN Client, page 13-3• Using a Command Prompt to Download and Launch the DCNM-LAN Client, page 13-4 The DCNM-LAN client login window opens. |
| Step 2 | In the DCNM-LAN Server field, enter the DNS name or the IP address of the DCNM-LAN server. By default, this field lists the address or name specified the last time the client logged into a server. If you are logging into the client after downloading it, this field lists the address of the server that you downloaded the client from. |
| Step 3 | In the Username field, enter your DCNM-LAN username. If you are logging into DCNM-LAN for the first time after installing the server, enter the local administrator name that you specified during the server installation. For more information, see the “Default Administrator Credentials” section on page 13-3 . |
| Step 4 | In the Password field, enter the password for the DCNM-LAN username that you specified. |

- Step 5** (Optional) If you need to change the DCNM-LAN server port, do the following:
- If the Port field is not visible, click **More >>**.
 - Enter the port number in the Port field.
The default DCNM-LAN server port number is 1099; however, you can specify a different port number when you install or reinstall the DCNM-LAN server.
- Step 6** (Optional) If you need to use a proxy server to connect to the DCNM-LAN server, do the following:
- If the “Connect to the DCNM-LAN server with a proxy server” check box is not visible, click **More >>**.
 - Check **Connect to the DCNM-LAN server with a proxy server**.
The Proxy Server area appears below the check box.
 - In the Address field, enter the IP address of the proxy server.
 - In the HTTP Port and Socks Port fields, enter the port numbers on which the proxy server accepts HTTP and Socks connections.
 - (Optional) If the proxy server requires authentication, check **Authentication** and enter a valid username and password in the fields provided.
- Step 7** Click **Login**.
The DCNM-LAN client opens. For information on how to use the DCNM-LAN client, see [Chapter 14, “Using the Cisco DCNM-LAN Client.”](#)
-

Uninstalling the DCNM-LAN Client

You can uninstall the DCNM-LAN client from a computer.

DETAILED STEPS

-
- Step 1** Click **Start > Control Panel > Java**.
The Java Control Panel dialog box opens.
- Step 2** In the General tab, under Temporary Internet Files, click **Settings**.
The Temporary File Settings dialog box appears.
- Step 3** Click **View Applications**.
The Java Application Cache Viewer dialog box opens.
- Step 4** Select the DCNM-LAN Client application and click **Remove Selected Application**.
Java uninstalls the DCNM-LAN client image from your computer.
- Step 5** Close the Java Application Cache Viewer.
- Step 6** On the Temporary File Settings dialog box, click **OK**.
- Step 7** On the Java Control Panel dialog box, click **OK**.

- Step 8** If you want to reinstall the DCNM-LAN client, see the [“Downloading and Launching the DCNM-LAN Client”](#) section on page 13-3.

Modifying Cisco DCNM-LAN Server

DCNM allows you to modify certain Cisco DCNM-LAN Server settings. Some changes require you to restart the DCNM services.

- [Changing the IP Address of the Cisco DCNM-LAN for WINDOWS OS, page 13-9](#)
- [Changing the IP Address of the Cisco DCNM-LAN on Federated Windows OS, page 13-10](#)
- [Changing the IP Address of the Cisco DCNM-LAN on Linux OS, page 13-10](#)

Changing the IP Address of the Cisco DCNM-LAN for WINDOWS OS

To change the IP address of a Cisco DCNM-LAN Windows Server, follow these steps:



Note

To change the IP Address of a Cisco DCNM-SAN & DCNM-SMIS Server, see [Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS WINDOWS Server, page 5-12](#).

DETAILED STEPS

- Step 1** Logon to the Cisco DCNM Web Client.
- Step 2** Select **Admin > Server Properties**. Edit the value for lan.server.bindaddrs to new IP address.
- Step 3** Stop the Cisco DCNM-LAN Server using Windows Services.
- Step 4** Change the old IP Address with the new IP Address in the following files:
- \$INSTALLDIR\jboss-as-7.2.0.Final\bin\service\lanservice.bat
 - \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-lan.xml
 - \$INSTALLDIR\dcnm\bin\clean-dcnm-db.bat
 - \$INSTALLDIR\dcnm\bin\dcnm-log-capture.bat
 - \$INSTALLDIR\dcnm\bin\startLANSANServer.bat
 - \$INSTALLDIR\dcnm\bin\status-dcnm.bat.
 - \$INSTALLDIR\dcnm\bin\takeServerDump.bat.
 - \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\landeployments\dcnm-client.war\dcnm.jnlp
 - \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\landeployments\dcnm-client.war\dcnmLatest.jnlp



Note dcnm-client.war can be modified using 7-Zip/Winrar application.

- Step 5** Start the Cisco DCNM-LAN Server using the Windows Services.

Changing the IP Address of the Cisco DCNM-LAN on Federated Windows OS

To change the IP address of a federated Cisco DCNM-LAN Server, follow these steps:

-
- Step 1** Logon to the Cisco DCNM Web Client.
- Step 2** Navigate to **Admin > Server Properties**. Edit **lan.server.bindaddrs** with the new IP address.
- Step 3** Stop the Cisco DCNM-LAN Server using Windows Services.
- Step 4** Change the old IP Address with the new IP Address in the file
\$INSTALLDIR\jboss-as-7.2.0.Final\bin\service\lanservice.bat
- a. \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-lan.xml
 - b. \$INSTALLDIR\dcnm\bin\clean-dcnm-db.bat
 - c. \$INSTALLDIR\dcnm\bin\dcnm-log-capture.bat
 - d. \$INSTALLDIR\dcnm\bin\startLANSANServer.bat
 - e. \$INSTALLDIR\dcnm\bin\status-dcnm.bat
 - f. \$INSTALLDIR\dcnm\bin\takeServerDump.bat
 - g. \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\deployments\dcnm-client.war\dcnm.jnlp
 - h. \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\deployments\dcnm-client.war\dcnmLatest.jnlp

**Note**

You can modify the *dcnm-client.war* file by using 7-Zip or Winrar application.

- Step 5** Start the Cisco DCNM-LAN Server using Windows Services.
-

Changing the IP Address of the Cisco DCNM-LAN on Linux OS

To change the IP address of a Cisco DCNM-LAN Server, follow these steps:

**Note**

To change the IP Address of a Cisco DCNM-SAN & DCNM-SMIS Server, see [Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS LINUX Server, page 5-14](#).

DETAILED STEPS

-
- Step 1** Logon to the Cisco DCNM Web Client.
- Step 2** Select **Admin > Server Properties**. Edit the value for **lan.server.bindaddrs** to new IP address.
- Step 3** Stop the Cisco DCNM-LAN Server. Run \$INSTALLDIR\dcnm\bin\stopdcnm.sh.
- Step 4** Change the old IP Address with the new IP Address in the following files:
- a. \$INSTALLDIR\jboss-as-7.2.0.Final\bin\init.d\lanservice.sh.
 - b. /etc/init.d/LANServer
 - c. \$INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-lan.xml
 - d. \$INSTALLDIR\dcnm\bin\clean-dcnm-db.sh

- e. \$INSTALLDIR\dcnm\bin\dcnm-log-capture.sh
- f. \$INSTALLDIR\dcnm\bin\startLANSANServer.sh
- g. \$INSTALLDIR\dcnm\bin\takeServerDump.sh

Step 5 Start the Cisco DCNM-LAN Server (run \$INSTALLDIR\dcnm\bin\startdcnm.sh).

Additional References

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

- [Related Documents, page 13-11](#)
- [Standards, page 13-11](#)

Related Documents

Related Topic	Document Title
How to use the DCNM-LAN client	Chapter 14, “Using the Cisco DCNM-LAN Client”
Starting or stopping a DCNM-LAN server	Chapter 25, “Starting and Stopping Cisco DCNM-LAN Servers”
The process of deploying DCNM-LAN in your organization	<i>Cisco DCNM Installation and Licensing Guide, Release 7.1.x</i>
Installing a DCNM-LAN server	<i>Cisco DCNM Installation and Licensing Guide, Release 7.1.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 Installing and Launching the DCNM-LAN Client

Table 13-1 lists the release history for this feature.

Table 13-1 Feature History for Installing and Launching the DCNM-LAN Client

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



CHAPTER 14

Using the Cisco DCNM-LAN Client

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

This chapter includes the following sections:

- [Information About the DCNM-LAN Client, page 14-1](#)
- [Opening the DCNM-LAN Client, page 14-8](#)
- [Closing the DCNM-LAN Client, page 14-9](#)
- [Deploying Changes, page 14-10](#)
- [Working with Statistics and Charts, page 14-11](#)
- [Configuring Global Preferences, page 14-17](#)
- [Using Online Help, page 14-19](#)

Information About the DCNM-LAN Client

This section describes the DCNM-LAN client and its parts.

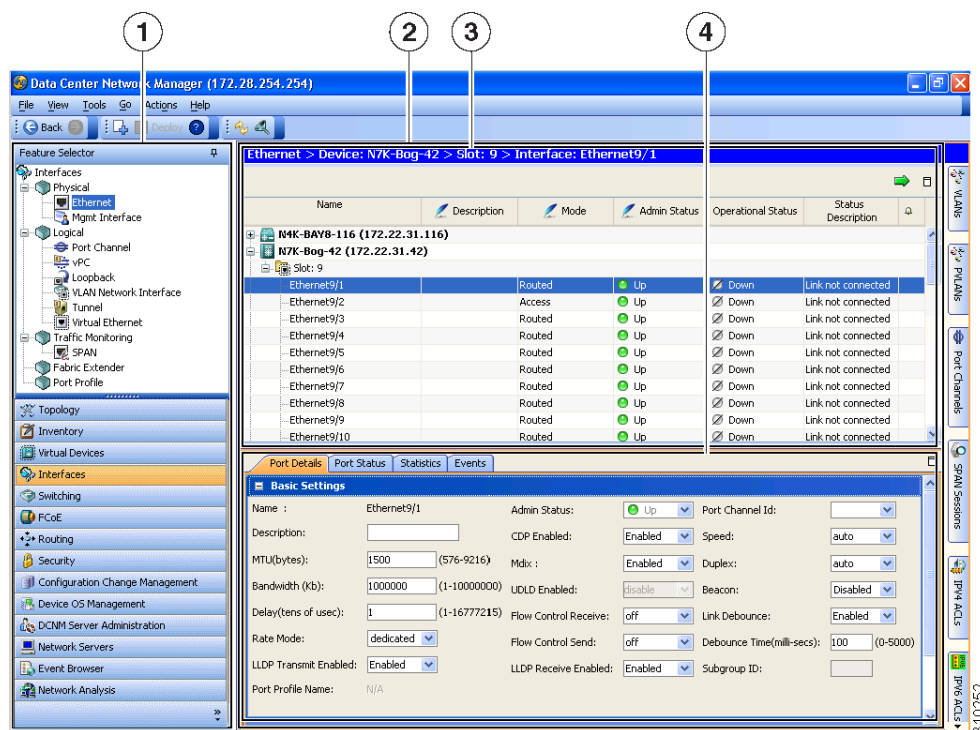
This section includes the following topics:

- [User Interface, page 14-2](#)
- [Feature Selector Pane, page 14-2](#)
- [Contents Pane, page 14-3](#)
- [Summary Pane, page 14-3](#)
- [Details Pane, page 14-3](#)
- [Association Pane, page 14-4](#)
- [Menus, page 14-5](#)
- [Toolbars, page 14-7](#)
- [Keyboard Commands, page 14-7](#)
- [Multiple Platform Support, page 14-7](#)

User Interface

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

Figure 14-1 DCNM-LAN Client User Interface



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

Feature Selector Pane

The Feature Selector pane, shown in Figure 14-1 the figure in the “User Interface” section on page 14-2, allows you to see features grouped by categories and to choose the feature that you want to use or configure. The bottom section of the Feature Selector pane displays buttons for feature categories. When you choose a category, the top section of the Feature Selector pane displays a tree of features within the chosen category.

In Figure 14-1 the figure in the “User Interface” section on page 14-2, the Interfaces category is chosen, so the tree shows features that allow you to configure the interfaces of managed devices.

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

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

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

Contents Pane

The Contents pane, shown in [Figure 14-1](#) the figure in the “[User Interface](#)” section on page 14-2, displays information about the currently selected feature and provides fields for configuring that feature. The Contents pane contains two smaller panes: the Summary pane and the Details pane.

Summary Pane

The Summary pane, shown in [Figure 14-1](#) the figure in the “[User Interface](#)” section on page 14-2, displays an organized set of objects that you can view information about or perform actions on. The type of objects that appear depends upon the currently selected feature.

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

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

Exporting the Summary Pane

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

Filtering the Summary Pane

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

Details Pane

The Details pane, shown in [Figure 14-1](#) the figure in the “[User Interface](#)” section on page 14-2, shows information and configuration fields that are specific to the object that you selected in the Summary pane. The Details tab is often further divided into tabs. You can click on a tab to view its contents.

This section includes the following topics:

- [Tabs, page 14-4](#)
- [Sections, page 14-4](#)

Tabs

Tabs organize related fields and information. For example, as shown in [Figure 14-1](#) the figure in the “[User Interface](#)” section on page 14-2, when you select an Ethernet interface, four tabs appear in the Details pane, such as the Port Details tab.

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

- **Statistics**—You can use this tab to work with statistics and charts related to the selected object. For more information, see the “[Working with Statistics and Charts](#)” section on page 14-11.
- **Events**—You can use this tab to view feature-specific events about the selected object. For more information, see the *System Management Configuration Guide, Cisco DCNM for LAN*.

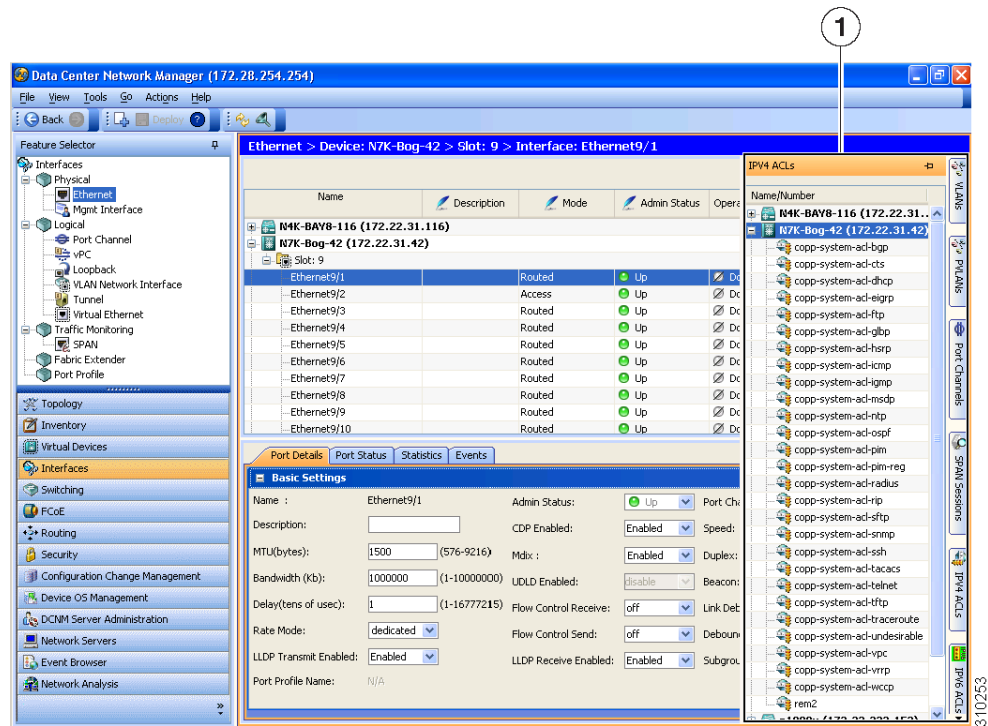
Sections

Sections provide further organization of related fields and information. The DCNM-LAN client allows you to expand and collapse sections so that you can show or hide fields and information as needed. For example, as shown in [Figure 14-1](#) the figure in the “[User Interface](#)” section on page 14-2, on the Port Details tab, the Basic Settings section is expanded but the Port Mode Settings section is collapsed.

Association Pane

The DCNM-LAN client also includes the Association pane, which allows you to access objects that you have configured in features that are associated with the currently selected feature. [Figure 14-2](#) The following figure shows the Association pane.

When tabs appear on the right side of the DCNM-LAN client, you can click on them to access the Association pane. For example, as shown in [Figure 14-2](#) the following figure, if you are configuring an Ethernet interface, you can use the Association pane to access the IPv4 ACLs that you can apply to the interface. If you right-click on an IPv4 ACL in the Association pane, you can choose to apply the ACL to the interface or to go to the IPv4 ACLs feature and configure the ACL.

Figure 14-2 Association Pane

1	Association pane
----------	------------------

Menus

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

File Menu

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

View Menu

- **Toolbars**—Allows you to show or hide the toolbars that are available for the currently selected feature. For more information, see the “[Toolbars](#)” section on page 14-7.
- **Refresh**—Forces the DCNM-LAN client to retrieve updated information from the DCNM-LAN server.
- **Filter**—Enables or disables the filtering option for the Summary pane.

Tools Menu

- Preferences—Opens the Global Preferences dialog box. For more information, see the [“Configuring Global Preferences” section on page 14-17](#).
- Debug—Opens the DCNM-LAN Client Logging dialog box, which allows you to configure the logging level for the DCNM-LAN client.

**Note**

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

Go Menu

- Topology—Selects the Topology button on the Feature Selector pane.
- Inventory—Selects the Inventory button on the Feature Selector pane.
- Virtual Devices—Selects the Virtual Devices button on the Feature Selector pane.
- Interfaces—Selects the Interfaces button on the Feature Selector pane.
- Switching—Selects the Switching button on the Feature Selector pane.
- FCoE—Selects the FCoE button on the Feature Selector pane.
- Routing—Selects the Routing button on the Feature Selector pane.
- Security—Selects the Security button on the Feature Selector pane.
- Configuration Change Management—Selects the Configuration Change Management button on the Feature Selector pane.
- Device OS Management—Selects the Device OS Management button on the Feature Selector pane.
- Configuration Delivery Management—Selects the Configuration Delivery Management button on the Feature Selector pane.
- DCNM-LAN Server Administration—Selects the DCNM-LAN Server Administration button on the Feature Selector pane.
- Network Servers—Selects the Network Servers button on the Feature Selector pane.
- Event Browser—Selects the Event Browser button on the Feature Selector pane.

Actions Menu

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

Help Menu

- Help Contents—Opens the online help system to the Welcome page.
- Context Help—Opens the online help system to a page that applies to the feature currently selected in the Feature Selector pane.
- Show DCNM-LAN Instance ID—Opens a dialog box that displays the license ID for your DCNM-LAN server. For more information, see the *Cisco DCNM Installation Guide, Release 7.1.x*.

- **View Licenses**—Opens a dialog box that displays information about license files currently installed with your DCNM-LAN server.
- **About Data Center Network Manager**—Opens a dialog box that displays information about your DCNM-LAN server, including the software version and implementation version.

Toolbars

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

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

Keyboard Commands

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

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

Multiple Platform Support

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

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

For example, if you choose **Security > Access Control > Time-range** from the Feature Selector pane, the Summary pane displays only the platform types that support the Time-range feature. In this case, the Cisco Nexus 1000V does not support this feature, so any managed Cisco Nexus 1000V platforms are not displayed in the Summary pane. Similarly, the Time-range association pane does not include any Cisco Nexus 1000V platforms.

- **Unsupported Attributes**—Sometimes a platform supports a feature, but does not support a particular attribute in that feature. In this case, the attribute is grayed-out or a N/A (Not Applicable) value is displayed in the field or cell.

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

If all attributes in a tab are not supported for a particular platform, the tab is displayed, but if you click on it, a message appears stating that the attribute is not supported.

- **Unsupported Charts**—If a platform does not support some attributes in a chart, DCNM-LAN grays out those attributes. If a platform does not support any attributes in a chart, when you select the chart, DCNM-LAN displays a message stating that the chart is not supported.
- **Unsupported Options**—If a platform does not support an option, the option is not displayed, for example, in drop-down lists.
- **Unsupported Operations**— If a platform does not support an option for a specific operation on a context or toolbar menu, the option is grayed-out.

Opening the DCNM-LAN Client

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

BEFORE YOU BEGIN

Install the DCNM-LAN client on the computer that you are using.

DETAILED STEPS

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



Note If the DCNM-LAN client is not available on the All Programs menu, you can launch the DCNM-LAN client from the DCNM-LAN server website.

A dialog box displays login fields.

- Step 2** In the DCNM Server field, enter the IP address or hostname of the DCNM-LAN server. You can use the hostname only if your DNS server has an entry for the DCNM-LAN server hostname. If you have previously logged into the server with the current client installation, you may be able to choose the IP address or hostname from the drop-down list.
- Step 3** In the Username field, enter the name of the DCNM-LAN server user account that you want to use to access the DCNM-LAN client.
- Step 4** In the Password field, enter the password for the user account that you specified.

- Step 5** (Optional) If you need to change the DCNM-LAN server port, do the following:
- If the Port field is not visible, click **More >>**.
 - Enter the port number in the Port field.
The default DCNM-LAN server port number is 1099; however, you can specify a different port number when you install or reinstall the DCNM-LAN server.
- Step 6** (Optional) If you need to use a proxy server to connect to the DCNM-LAN server, do the following:
- If the “Connect to the DCNM-LAN server with a proxy server” check box is not visible, click **More >>**.
 - Check **Connect to the DCNM server with a proxy server**.
The Proxy Server area appears below the check box.
 - In the Address field, enter the IP address of the proxy server.
 - In the HTTP Port and Socks Port fields, enter the port numbers on which the proxy server accepts HTTP and Socks connections.
 - (Optional) If the proxy server requires authentication, check **Authentication** and enter a valid username and password in the fields provided.
- Step 7** Click **Login**.
The DCNM-LAN client user interface appears.
If a dialog box displays a message about device credentials, you have not configured device credentials for the user account that you specified.
- Step 8** If a dialog box shows a message that your device credentials are not set, do one of the following:
- If you want to set device credentials now, click **Yes**.
 - If you do not want to set device credentials now, click **No**.
-

RELATED TOPICS

- [Closing the DCNM-LAN Client, page 14-9](#)
- [Configuring Default Device Credentials, page 28-4](#)

Closing the DCNM-LAN Client

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

DETAILED STEPS

-
- Step 1** From the menu bar, choose **File > Exit**.
A dialog box displays a confirmation message.
- Step 2** (Optional) If you have not deployed your changes, do one of the following:
- If you want to save your changes, including deploying configuration changes to managed devices, check **Save pending changes**.
 - If you want to discard your changes, uncheck **Save pending changes**.

Step 3 Click **Yes**.

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

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

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

**Note**

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

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

RELATED TOPICS

- [Opening the DCNM-LAN Client, page 14-8](#)

Deploying Changes

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

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

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

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

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

**Note**

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

When you close the DCNM-LAN client and you have not deployed your changes, you can deploy them without canceling the process of closing the DCNM-LAN client. For more information, see the [“Closing the DCNM-LAN Client” section on page 14-9](#).

Working with Statistics and Charts

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

This section includes the following topics:

- [Information about Statistics and Charts, page 14-11](#)
- [Licensing Requirements for Statistics and Charts, page 14-11](#)
- [Accessing a Chart, page 14-12](#)
- [Starting Statistical Monitoring for a Chart, page 14-12](#)
- [Stopping Statistical Monitoring for a Chart, page 14-13](#)
- [Using a Chart, page 14-14](#)
- [Using an Overview Chart, page 14-15](#)
- [Exporting a Chart, page 14-16](#)

Information about Statistics and Charts

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

When you start monitoring for a new chart, DCNM-LAN creates a new statistical collection process that appears in the Statistical Data Collection feature.

Licensing Requirements for Statistics and Charts

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM-LAN	<p>Real-time monitoring requires no license.</p> <p>Cisco DCNM-LAN requires a LAN Enterprise license for the following features:</p> <ul style="list-style-type: none">• Maintaining a history of statistical data• Using overview charts <p>For information about obtaining and installing a Cisco DCNM-LAN LAN Enterprise license, see the <i>Cisco DCNM Installation Guide, Release 7.1.x</i>.</p>

Accessing a Chart

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

DETAILED STEPS

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

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

Step 2 From the Summary pane, select an object.

The Statistics tab appears in the Details pane.



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

Step 3 Click the **Statistics** tab.

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



Note A dialog box may appear to confirm if you want to view charts for statistical collections that DCNM-LAN is running for the object that you selected in the Summary pane. For more information, see the [“Configuring Monitoring Preferences” section on page 14-17](#).

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

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

The chart status appears in the lower left corner of the chart pane. If the chart is not active, you must start statistical monitoring for the chart before you can use it. For more information, see the [“Starting Statistical Monitoring for a Chart” section on page 14-12](#).

RELATED TOPICS

- [Starting Statistical Monitoring for a Chart, page 14-12](#)
- [Stopping Statistical Monitoring for a Chart, page 14-13](#)
- [Using a Chart, page 14-14](#)
- [Using an Overview Chart, page 14-15](#)
- [Exporting a Chart, page 14-16](#)


Starting Statistical Monitoring for a Chart

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

**Note**

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

DETAILED STEPS

- Step 1** Access the chart for which you want to start statistical monitoring. For more information, see the [“Accessing a Chart” section on page 14-12](#).
- Step 2** From the chart pane, click **Select Parameters**, check at least one statistical parameter that you want **to appear in the chart**, and click **Select Parameters** again.
- Step 3** From the Monitor toolbar, choose the  icon to start the collection process.
- Step 4** The chart starts graphing the selected parameters.

**Note**

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

RELATED TOPICS

- [Accessing a Chart, page 14-12](#)
- [Stopping Statistical Monitoring for a Chart, page 14-13](#)
- [Using a Chart, page 14-14](#)
- [Using an Overview Chart, page 14-15](#)
- [Exporting a Chart, page 14-16](#)

Stopping Statistical Monitoring for a Chart

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

**Note**

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

DETAILED STEPS

- Step 1** Access the chart for which you want to stop statistical monitoring. For more information, see the [“Accessing a Chart” section on page 14-12](#).
- Step 2** From the Monitor toolbar choose the Arrow icon.

**Note**

If the chart that you want to stop does not appear, use the Statistical Data Collection feature to stop the collection process. For more information, see the [“Starting Statistical Monitoring for a Chart” section on page 14-12](#).

RELATED TOPICS

- [Accessing a Chart, page 14-12](#)
- [Starting Statistical Monitoring for a Chart, page 14-12](#)
- [Using a Chart, page 14-14](#)
- [Using an Overview Chart, page 14-15](#)
- [Exporting a Chart, page 14-16](#)

Using a Chart

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

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




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

**Note**




For information about using an overview chart, see the [“Using an Overview Chart” section on page 14-15](#).

DETAILED STEPS

- Step 1** Access the chart that you want to use. For more information, see the [“Accessing a Chart” section on page 14-12](#).
- Step 2** If the chart is not active, you must start statistical monitoring for the chart before you can use it. For more information, see the [“Starting Statistical Monitoring for a Chart” section on page 14-12](#).
- Step 3** (Optional) To change parameters, click **Select Parameters**, check the statistics parameters that you want **to collect**, and click **Select Parameters** again.
- Step 4** (Optional) To set the frequency with which DCNM-LAN retrieves statistical data for the selected object, from the Select Frequency drop-down list on the Monitor toolbar, choose the new frequency.
- Step 5** (Optional) To control the magnification, or zoom, of the chart, do one of the following:
 - To zoom in on a portion of the chart, position the mouse pointer at one end of the portion, click and hold the left mouse button, drag the mouse pointer to the other end of the portion, and release the mouse button.

- To zoom in on a portion of the chart, position the mouse pointer at one end of the portion and then click and drag the mouse pointer to the other end of the portion.
- To change to the previous zoom, click the  icon.
- To change to the next zoom, click the  icon.
- To reset the zoom to the default magnification, click the  icon.

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

- To show or hide threshold lines, on the Monitor toolbar, click the  icon.
- To move the lower threshold line, click and drag the  icon.
- To move the upper threshold line, click and drag the  icon.

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

RELATED TOPICS

- [Accessing a Chart, page 14-12](#)
- [Starting Statistical Monitoring for a Chart, page 14-12](#)
- [Stopping Statistical Monitoring for a Chart, page 14-13](#)
- [Using an Overview Chart, page 14-15](#)
- [Exporting a Chart, page 14-16](#)

Using an Overview Chart

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

BEFORE YOU BEGIN

Ensure that any device with data that you want to view on an overview chart is included on the list of DCNM-LAN-licensed devices. For more information, see the [“Licensing Requirements for Statistics and Charts”](#) section on page 14-11.

DETAILED STEPS

- Step 1** Access the chart that contains the overview chart that you want to use. For more information, see the [“Accessing a Chart”](#) section on page 14-12.
- Step 2** If the chart is not active, you must start statistical monitoring for the chart before you can use its overview chart. For more information, see the [“Starting Statistical Monitoring for a Chart”](#) section on page 14-12.
- Step 3** Click **Show Overview Chart**.
In a new window, the overview chart displays the historical trends of the charted data.
- Step 4** To set the time scale of the chart, at the bottom of the overview chart window, click the desired time scale button. The time scale buttons are as follows:

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

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

RELATED TOPICS

- [Accessing a Chart, page 14-12](#)
- [Starting Statistical Monitoring for a Chart, page 14-12](#)
- [Stopping Statistical Monitoring for a Chart, page 14-13](#)
- [Using a Chart, page 14-14](#)
- [Exporting a Chart, page 14-16](#)

Exporting a Chart

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

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

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

DETAILED STEPS

-
- Step 1** Access the chart that you want to use. For more information, see the [“Accessing a Chart” section on page 14-12](#).
- Step 2** If the chart is not active, you must start statistical monitoring for the chart before you can export an image of it. For more information, see the [“Starting Statistical Monitoring for a Chart” section on page 14-12](#).
- Step 3** If you want to export an image, configure the chart to show the data that you want to appear in the image. For more information, see the [“Using a Chart” section on page 14-14](#).
- Step 4** Right-click on the chart.
- Step 5** Choose one of the following:
- Export as CSV
 - Export as JPG
- Step 6** Specify the location and filename, and then click **Save**.

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

RELATED TOPICS

- [Accessing a Chart, page 14-12](#)
- [Starting Statistical Monitoring for a Chart, page 14-12](#)
- [Stopping Statistical Monitoring for a Chart, page 14-13](#)
- [Using a Chart, page 14-14](#)
- [Using an Overview Chart, page 14-15](#)

Configuring Global Preferences

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

- **Monitoring**—Controls the default frequency of statistical data retrieval from managed devices and whether statistical charts open automatically. For more information, see the [“Configuring Monitoring Preferences” section on page 14-17](#).
- **Events**—Controls the maximum age of events that the DCNM-LAN client fetches from the DCNM-LAN server when you start the DCNM-LAN client. For more information, see the [“Configuring the Maximum Age of Events Fetched from the Server” section on page 14-18](#).
- **Pre Provision**—Controls whether the DCNM-LAN client displays some settings only when other settings are made or whether the DCNM-LAN client always displays all settings. For more information, see the [“Configuring Preprovisioning” section on page 14-19](#).

Configuring Monitoring Preferences

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

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

BEFORE YOU BEGIN

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

DETAILED STEPS

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

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

The default polling frequency is 30 seconds.

- Step 2** If you want to configure the default frequency of statistical data retrieval, from the Default Monitoring Frequency drop-down list, choose the new data retrieval frequency.
- Step 3** If you want to configure the default behavior when you access the Statistics tab of an object for which DCNM-LAN is already collecting statistical data, do one of the following:
- If you want the client to show charts without asking for confirmation, check the **Load history charts by default** check box.
 - If you want the client to prompt you for confirmation before it opens statistical charts, uncheck the **Load history charts by default** check box.
- Step 4** Click **Ok**.
-

RELATED TOPICS

- [Accessing a Chart, page 14-12](#)
- [Configuring the Maximum Age of Events Fetched from the Server, page 14-18](#)
- [Configuring Preprovisioning, page 14-19](#)

Configuring the Maximum Age of Events Fetched from the Server

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

DETAILED STEPS

- Step 1** From the menu bar, choose **Tools > Preferences**.
- The Global Preferences dialog box appears. Under Events, the Fetch events before drop-down list displays the current maximum age of events.
- Step 2** From the Fetch events before drop-down list, choose the new maximum age of events.



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

- Step 3** Click **Ok**.
-

RELATED TOPICS

- [Configuring Monitoring Preferences, page 14-17](#)
- [Configuring Preprovisioning, page 14-19](#)

Configuring Preprovisioning

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

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

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

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

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

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

DETAILED STEPS

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

The Global Preferences dialog box appears. Under Pre Provision, the Pre Provision check box appears. |
| Step 2 | Do one of the following: <ul style="list-style-type: none">• If you want to enable preprovisioning, ensure that the Pre Provision check box is checked.• If you want to disable preprovisioning, ensure that the Pre Provision check box is unchecked. |
| Step 3 | Click Ok . |
-

RELATED TOPICS

- [Configuring Monitoring Preferences, page 14-17](#)
- [Configuring the Maximum Age of Events Fetched from the Server, page 14-18](#)

Using Online Help

Online help has the following features:

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

You can expand and collapse individual topics in the contents. You can also collapse or expand all topics.

- **Index**—DCNM-LAN online help includes an index, which allows you to look up subjects alphabetically and open related topics directly from the index.
- **Favorites**—DCNM-LAN online help allows you to add specific topics to the Favorites tab. Favorites are stored locally on the computer that you use to access online help.

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

DCNM-LAN online help includes context-sensitive help.

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

-
- Step 1** Select a specific feature from the Feature Selector pane in the DCNM-LAN client. For example, choose **Security > Access Control > IPv4 ACL**.
- Step 2** Do one of the following:
- Press **F1**.
 - From the toolbar, click the question mark icon.

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



CHAPTER 15

Administering DCNM-LAN Authentication Settings

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

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

As described in the following table, Cisco DCNM supports two user roles.

Cisco DCNM Role	Description
User	<ul style="list-style-type: none">• Cannot change Cisco DCNM authentication mode• Cannot add or delete Cisco DCNM local user accounts• Can change the details of its own local user account• Can use all other features
Administrator	<ul style="list-style-type: none">• Has full control of Cisco DCNM authentication settings• Can use all other features

This chapter includes the following sections:

- [Information About Administering DCNM-LAN Authentication Settings, page 15-2](#)
- [Licensing Requirements for Administering DCNM-LAN Authentication Settings, page 15-5](#)
- [Prerequisites for Administering DCNM-LAN Authentication Settings, page 15-5](#)
- [Guidelines and Limitations for Administering DCNM-LAN Authentication Settings, page 15-5](#)
- [Configuring DCNM-LAN Authentication Settings, page 15-5](#)
- [Viewing DCNM-LAN Local Users, page 15-13](#)
- [Verifying Authentication Server Settings, page 15-13](#)
- [Field Descriptions for DCNM-LAN Authentication Settings, page 15-14](#)
- [Additional References, page 15-16](#)
- [Feature History for DCNM-LAN Authentication Settings, page 15-17](#)

Information About Administering DCNM-LAN Authentication Settings

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

This section contains the following topics:

- [Users and User Roles, page 15-2](#)
- [Local Authentication and DCNM-LAN Local Users, page 15-2](#)
- [RADIUS and TACACS+ Authentication, page 15-3](#)
- [User Role Assignment by RADIUS and TACACS+, page 15-3](#)
- [Fallback to Local Authentication, page 15-4](#)
- [Password Recovery, page 15-4](#)
- [Users and Device Credentials, page 15-4](#)
- [Virtualization Support, page 15-4](#)

Users and User Roles

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

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

In addition, DCNM-LAN allows you to assign a role to each user. Roles determine what actions a user can take in the DCNM-LAN client. As described in [Table 15-1](#), DCNM-LAN supports two user roles.

Table 15-1 DCNM-LAN User Roles

DCNM-LAN Role	Description
User	<ul style="list-style-type: none"> • Cannot change DCNM-LAN authentication mode • Cannot add or delete DCNM-LAN local user accounts • Can change the details of its own local user account • Can use all other features
Administrator	<ul style="list-style-type: none"> • Has full control of DCNM-LAN authentication settings • Can use all other features

Local Authentication and DCNM-LAN Local Users

The DCNM-LAN database contains any DCNM-LAN local users that you create.

**Note**

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

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

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

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

Attribute Setup for External AAA using ACS 5.x

The steps for ACS 5.x TACACS+ are to essentially configure the following under Police Elements / Authorization and Permissions / Device Administration / Shell Profiles / shell profile name

- Attribute: cisco-av-pair
- Requirement: optional
- Value: shell:roles="network-admin"

RADIUS and TACACS+ Authentication

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

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

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

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

User Role Assignment by RADIUS and TACACS+

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

To assign a DCNM-LAN user role by RADIUS, configure the RADIUS server to return the RADIUS vendor-specific attribute 26/9/1, which is the Cisco-AV-Pair attribute. To assign a DCNM-LAN user role by TACACS+, the TACACS+ server must return a cisco-av-pair attribute-value pair. If an authentication response does not assign the user role, DCNM-LAN assigns the User role. [Table 15-2](#) shows the supported attribute-value pair values for each DCNM-LAN user role.

Table 15-2 DCNM-LAN User Role Assignment Values

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

Fallback to Local Authentication

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

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

Password Recovery

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

- For Microsoft Windows, use `/user/local/cisco/dcm/fm/bin/adduser.bat`.
- For Linux, use `/user/local/cisco/dcm/fm/bin/adduser.sh`.

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

Alternatively, you can reinstall the DCNM-LAN server, which allows you to specify the username and password for a local user account that is assigned the Administrator role. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

Users and Device Credentials

Each DCNM-LAN server user has unique device credentials, regardless of whether the user authenticates with a local user account or an account on a RADIUS or TACACS+ server. This feature allows you to maintain accounting logs on managed devices that reflect the actions of each DCNM-LAN server user. For more information, see the [“Information About Devices and Credentials” section on page 28-1](#).

Virtualization Support

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

DCNM-LAN server users can configure any managed device.

Licensing Requirements for Administering DCNM-LAN Authentication Settings

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM-LAN	Administering Cisco DCNM-LAN authentication settings requires no license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM-LAN LAN Enterprise license, see the <i>Cisco DCNM Installation and Licensing Guide, Release 7.1.x</i> .

Prerequisites for Administering DCNM-LAN Authentication Settings

Administering DCNM-LAN authentication settings has the following prerequisites:

- You must ensure that every authentication server that you want to use with DCNM-LAN is configured to accept authentication requests from the DCNM-LAN server.
- To add, delete, or modify DCNM-LAN local users, you must be logged into the DCNM-LAN client with a user account that is assigned the Administrator DCNM-LAN role.

Guidelines and Limitations for Administering DCNM-LAN Authentication Settings

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

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

Configuring DCNM-LAN Authentication Settings

This section includes the following topics:

- [Configuring the Authentication Mode, page 15-6](#)
- [Adding a DCNM-LAN Local User, page 15-6](#)
- [Changing the Password of a DCNM-LAN Local User, page 15-8](#)
- [Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8](#)
- [Deleting a DCNM-LAN Server User, page 15-9](#)
- [Adding Authentication Servers, page 15-10](#)
- [Changing Authentication Server Settings, page 15-11](#)
- [Removing an Authentication Server, page 15-12](#)

Configuring the Authentication Mode

Does this apply to API sessions, too? Or just the DCNM client?

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

BEFORE YOU BEGIN

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

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

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose DCNM Server Administration > DCNM Authentication Settings . |
| Step 2 | If necessary, expand the Authentication Mode section. |
| Step 3 | Choose the authentication mode. |
| Step 4 | From the menu bar, choose File > Deploy to apply your changes to the DCNM-LAN server. |
| Step 5 | Restart the DCNM-LAN server. For more information, see the <i>Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i> . Chapter 25, “Starting and Stopping Cisco DCNM-LAN Servers.” |
-

RELATED TOPICS

- [Adding a DCNM-LAN Local User, page 15-6](#)
- [Adding Authentication Servers, page 15-10](#)

Adding a DCNM-LAN Local User

You can add a DCNM-LAN local user account.



Note

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

BEFORE YOU BEGIN

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

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

**Note**

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

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.
- Step 2** If necessary, expand the **DCNM Local Users** section.
A table of users appears in the Cisco DCNM Local Users section.
- Step 3** From the menu bar, choose **Actions > Add User**.
A new row appears at the bottom of the list of users. By default, all fields in the new row are blank.
- Step 4** In the DCNM User Name column of the new row, enter the username. The username can be 1 to 198 characters. Entries can contain case-sensitive letters, numbers, and symbols.
- Step 5** (Optional) In the Full Name column, double-click the entry and add a name. For example, enter the real name of the person who will use the DCNM-LAN local user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.
- Step 6** In the DCNM Role column, double-click the entry and choose the role. By default, the role is User.
- Step 7** In the Password column, double-click the entry and then click the down-arrow button.
- Step 8** In the New Password field and the Confirm Password field, enter the password. The password can be 1 to 255 characters. Entries can contain case-sensitive letters, numbers, and symbols.
- Step 9** Click **OK**.
- Step 10** (Optional) In the Description column, double-click the entry and add a description of the user account. For example, you could use this entry to provide e-mail and telephone contact details of the person who will be using this DCNM-LAN server user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.
- Step 11** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.

RELATED TOPICS

- [Changing the Password of a DCNM-LAN Local User, page 15-8](#)
- [Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8](#)
- [Deleting a DCNM-LAN Server User, page 15-9](#)

Changing the Password of a DCNM-LAN Local User

You can change the password of a DCNM-LAN local user.

BEFORE YOU BEGIN

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

Determine what the new password should be.



Note

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

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Authentication Settings**.
- Step 2** If necessary, expand the **DCNM Local Users** section.
A table of users appears in the DCNM Local Users section.
- Step 3** In the User Name column, click the username for the user account that you want to change.
The row of the username that you clicked is highlighted.
- Step 4** In the Password column, double-click the entry and then click the down-arrow button.
- Step 5** In the New Password field and the Confirm Password field, enter the new password. The password can be 1 to 255 characters. Entries can contain case-sensitive letters, numbers, and symbols.
- Step 6** Click **OK**.
- Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.

RELATED TOPICS

- [Adding a DCNM-LAN Local User, page 15-6](#)
- [Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8](#)
- [Deleting a DCNM-LAN Server User, page 15-9](#)

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

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



Note

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

BEFORE YOU BEGIN

Determine what the new full name or description should be.

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

DETAILED STEPS

-
- | | |
|---------------|---|
| Step 1 | From the Feature Selector pane, choose DCNM Server Administration > DCNM Authentication Settings . |
| Step 2 | If necessary, expand the DCNM Local Users section.
A table of users appears in the Cisco DCNM Local Users section. |
| Step 3 | In the User Name column, click the username of the local user account that you want to change.
The row of the username that you clicked is highlighted. |
| Step 4 | (Optional) In the Full Name column, double-click the entry and enter the new name. The maximum length is 255 case-sensitive letters, numbers, and symbols. |
| Step 5 | (Optional) In the DCNM Role column, double-click the entry and choose the new role. You can choose Administrator or User. |
| Step 6 | (Optional) In the Description column, double-click the entry and enter the new description of the user account. The maximum length is 255 case-sensitive letters, numbers, and symbols. |
| Step 7 | From the menu bar, choose File > Deploy to apply your changes to the DCNM-LAN server. |
-

RELATED TOPICS

- [Adding a DCNM-LAN Local User, page 15-6](#)
- [Changing the Password of a DCNM-LAN Local User, page 15-8](#)
- [Deleting a DCNM-LAN Server User, page 15-9](#)

Deleting a DCNM-LAN Server User

You can remove a DCNM-LAN local user account.

BEFORE YOU BEGIN

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

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

DETAILED STEPS

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

- Step 2** If necessary, expand the **DCNM Local Users** section.
A table of users appears in the DCNM Local Users section.
- Step 3** In the User Name column, click the username of the user account that you want to remove.
The row of the username that you clicked is highlighted.
- Step 4** From the menu bar, choose **Actions > Delete User**.
- Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.
-

RELATED TOPICS

- [Adding a DCNM-LAN Local User, page 15-6](#)
- [Changing the Password of a DCNM-LAN Local User, page 15-8](#)
- [Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8](#)

Adding Authentication Servers

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

BEFORE YOU BEGIN



Note

You must ensure that every authentication server that you want to use with DCNM-LAN is configured to accept authentication requests from the DCNM-LAN server.

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

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

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

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.
- Step 2** If necessary, expand the **Authentication Servers** section.
The Authentication Server Settings table shows RADIUS and TACACS+ server settings.
- Step 3** If necessary, expand the **RADIUS** or **TACACS+** server rows.

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

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



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

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



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

- c. Double-click the **Secret Key** field and enter the secret key (sometimes called a shared secret) of the authentication server.
- d. (Optional) If you need to change the default Authentication Port or Accounting Port (RADIUS only), double-click the applicable port field and enter the new port number.
- e. Double-click the **Authentication Method** field and choose the authentication protocol that DCNM-LAN must use when sending authentication requests to the authentication server.

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

- a. To the right of the row for the authentication server that you want to verify, click **Verify**.
A Verification dialog box appears.
- b. Enter a username and password for a valid user account on the authentication server.
- c. Click **Verify**.

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

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

RELATED TOPICS

- [Configuring the Authentication Mode, page 15-6](#)
- [Changing Authentication Server Settings, page 15-11](#)
- [Removing an Authentication Server, page 15-12](#)
- [Verifying Authentication Server Settings, page 15-13](#)

Changing Authentication Server Settings

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

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.
- Step 2** If necessary, expand the **Authentication Servers** section.
The Authentication Server Settings table shows RADIUS and TACACS+ server settings.
- Step 3** If necessary, expand the **RADIUS** or **TACACS+** server rows.
- Step 4** (Optional) If you want to change the settings of an authentication server, double-click each field that you need to change and enter the changes.
- Step 5** (Optional) If you want to reorder RADIUS or TACACS+ servers, right-click a server and choose **Move Up** or **Move Down**, as needed.
- Step 6** (Optional) If you want to verify that the DCNM-LAN server can authenticate a user with an authentication server, follow these steps:
- To the right of the row for the authentication server that you want to verify, click **Verify**.
A Verification dialog box appears.
 - Enter a username and password for a valid user account on the authentication server.
 - Click **Verify**.
- The DCNM-LAN client displays a message indicating whether the verification attempt succeeded or failed. A verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.
- Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.
-

RELATED TOPICS

- [Configuring the Authentication Mode, page 15-6](#)
- [Adding Authentication Servers, page 15-10](#)
- [Removing an Authentication Server, page 15-12](#)
- [Verifying Authentication Server Settings, page 15-13](#)

Removing an Authentication Server

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

BEFORE YOU BEGIN

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

DETAILED STEPS

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

- Step 2** If necessary, expand the **Authentication Servers** section.
- The Authentication Server Settings table shows RADIUS and TACACS+ server settings.
- Step 3** If necessary, expand the **RADIUS** or **TACACS+** server rows.
- Step 4** Right-click the authentication server that you want to remove and choose **Remove Server**.
- Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.
-

RELATED TOPICS

- [Configuring the Authentication Mode, page 15-6](#)
- [Adding Authentication Servers, page 15-10](#)
- [Changing Authentication Server Settings, page 15-11](#)
- [Verifying Authentication Server Settings, page 15-13](#)

Viewing DCNM-LAN Local Users

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

DCNM-LAN server user accounts, including usernames and descriptions, appear in the Contents pane. Passwords appear masked for security. For information about the fields that appear, see the “[Field Descriptions for DCNM-LAN Authentication Settings](#)” section on page 15-14.

RELATED TOPICS

- [Adding a DCNM-LAN Local User, page 15-6](#)
- [Changing the Password of a DCNM-LAN Local User, page 15-8](#)
- [Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8](#)
- [Deleting a DCNM-LAN Server User, page 15-9](#)

Verifying Authentication Server Settings

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

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings**.
- Step 2** If necessary, expand the **Authentication Servers** section.
- The Authentication Server Settings table shows RADIUS and TACACS+ server settings.
- Step 3** Click **Verify**.

A Verification dialog box appears.

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

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

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

RELATED TOPICS

- [Adding Authentication Servers, page 15-10](#)
- [Removing an Authentication Server, page 15-12](#)
- [Verifying Authentication Server Settings, page 15-13](#)

Field Descriptions for DCNM-LAN Authentication Settings

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

- [Authentication Mode Section, page 15-14](#)
- [DCNM-LAN Local Users Section, page 15-15](#)
- [Authentication Servers Section, page 15-15](#)

Authentication Mode Section

Table 15-3 Authentication Mode Section

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

DCNM-LAN Local Users Section

Table 15-4 **DCNM-LAN Local Users Section**

Field	Description
DCNM-LAN User Name	<i>Display only.</i> Name of the DCNM-LAN server user account. This name can be used to log into the DCNM-LAN client when the authentication mode is local or when no authentication server for the current authentication mode is reachable. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. The minimum length is 1 character. The maximum length is 198 characters.
Full Name	Other name for the user account, such as the name of the person who uses the DCNM-LAN server user account. This name cannot be used to log into the DCNM-LAN client. Valid characters are all letters, numbers, and symbols. The maximum length is 255 characters. This field is blank by default.
DCNM-LAN Role	Role of the user account. Valid values are User and Administrator. For more information, see Table 15-1 . By default, a DCNM-LAN server user account is assigned the role of User.
Password	Password for the DCNM-LAN server user. This field is always masked for security. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. The minimum length is 1 character. The maximum length is 255 characters.
Description	Description of the DCNM-LAN server user. Valid characters are all letters, numbers, and symbols. The maximum length is 255 characters. This field is blank by default.

Authentication Servers Section

Table 15-5 **Authentication Servers Section**

Field	Description
Server Name	DNS name or IPv4 address of the authentication server. <ul style="list-style-type: none"> DNS name—If you specify a DNS name, the DCNM-LAN server must be able to resolve the IP address of the server. Valid DNS names characters are alphanumeric. IPv4 address—If you specify an IP address, valid entries are in dotted decimal format.
Secret Key	Shared secret of the authentication server. Valid entries are case-sensitive letters, numbers, and symbols.
Authentication Port	TCP or UDP port number that the authentication server listens to for authentication requests. By default, the authentication port for a RADIUS server is UDP port 1812 and the authentication port for a TACACS+ server is TCP port 49.

Table 15-5 Authentication Servers Section (continued)

Field	Description
Accounting Port	UDP port number that the RADIUS authentication server listens to for authentication requests. By default, the accounting port for a RADIUS server is UDP port 1813.
Authentication Method	Authentication protocol that the DCNM-LAN server uses in authentication requests to the authentication server. Supported authentication methods are as follows: <ul style="list-style-type: none"> • PAP • CHAP • MSCHAP • ASCII

Additional References

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

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

Related Documents

Related Topic	Document Title
Logging into the DCNM-LAN client	<i>Opening the DCNM-LAN Client, page 14-8</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 DCNM-LAN Authentication Settings

Table 15-6 lists the release history for this feature.

Table 15-6 *Feature History for DCNM-LAN Server Users*

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



CHAPTER 16

Working with Topology

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

The Topology feature provides you with a topology map of supported Cisco NX-OS devices. The topology map also shows switches that run Cisco IOS software, such as the Catalyst 6500 series switches, that are linked by the Cisco Discovery Protocol (CDP). For Catalyst 6500 series switches, the physical topology view of the map displays these switches and their links to other devices. For Nexus 7000 Series devices, the map shows details about virtual device contexts (VDCs).

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

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

Device states are shown on the map. The possible states are as follows:

- **Managed**—You can configure and monitor the device with Cisco DCNM. For the device state to be Managed, device discovery must succeed.
- **Discovery**—Cisco DCNM is currently discovering the device. You cannot configure or monitor the device with Cisco DCNM unless discovery succeeds and the device state changes to Managed. If discovery fails, the device state will change to Unmanaged.
- **Unmanaged**—You cannot configure or monitor the device with Cisco DCNM because discovery failed or a Cisco DCNM user explicitly changed the device state to Unmanaged by using the Devices and Credentials feature.
- **Unreachable**—You cannot configure or monitor the device because the Cisco DCNM server cannot connect to the device. Data shown in Cisco DCNM may be out of date. Common causes for this state are that a network issue is preventing the Cisco DCNM server from connecting to the device, the SSH feature is disabled on the device, or all terminal lines on the device are in use. When connectivity is restored, the state of the device will return to Managed.

For more information about device states, see the [Understanding Device Icons and Links](#).

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

This chapter includes the following sections:

- [Information About Topology, page 16-2](#)
- [Licensing Requirements for Topology, page 16-9](#)
- [Prerequisites for Topology, page 16-9](#)
- [Guidelines and Limitations, page 16-9](#)

- [Using the Topology Feature, page 16-9](#)
- [Related Documents, page 16-41](#)
- [Feature History for Topology, page 16-41](#)

Information About Topology

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

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

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

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

This section includes the following topics:

- [Map Views, page 16-2](#)
- [Layouts, page 16-6](#)
- [vPC Support, page 16-7](#)
- [DCNM-SAN Support, page 16-7](#)
- [FabricPath Support, page 16-7](#)
- [Device Groups, page 16-8](#)
- [Network Servers, page 16-9](#)

Map Views

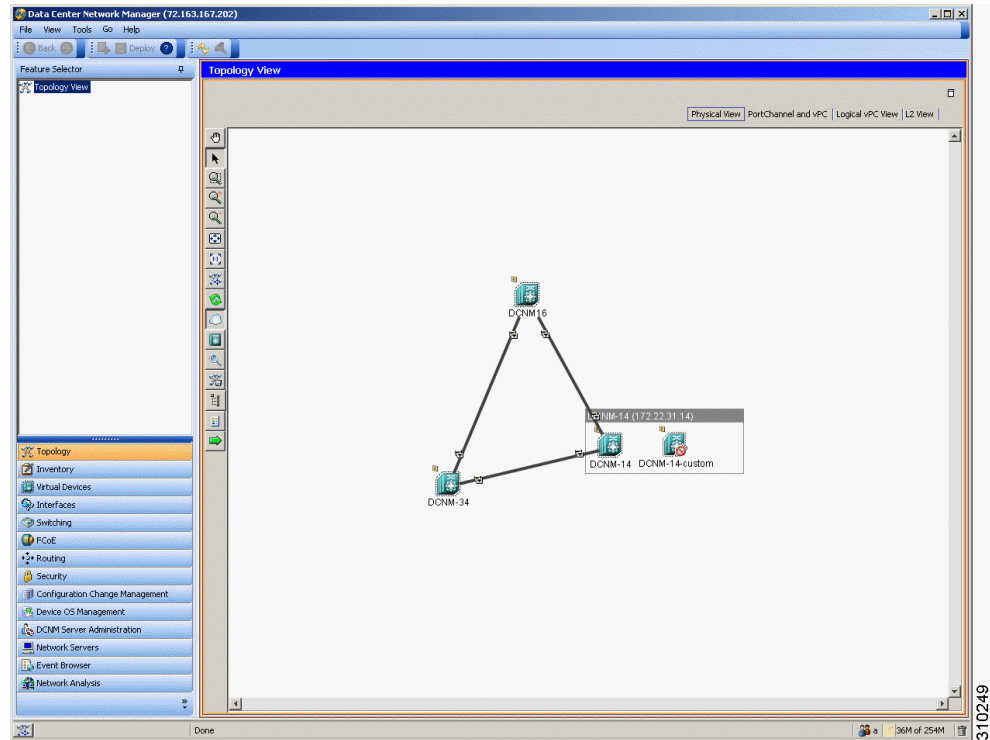
The topology map includes four views of your topology as described in the following topics:

- [Physical View, page 16-3](#)
- [PortChannel and vPC, page 16-4](#)
- [Logical vPC View, page 16-5](#)
- [L2 View, page 16-6](#)

Physical View

The Physical View (see [Figure 16-1](#)) shows the physical connections between discovered devices. This is the default topology view.

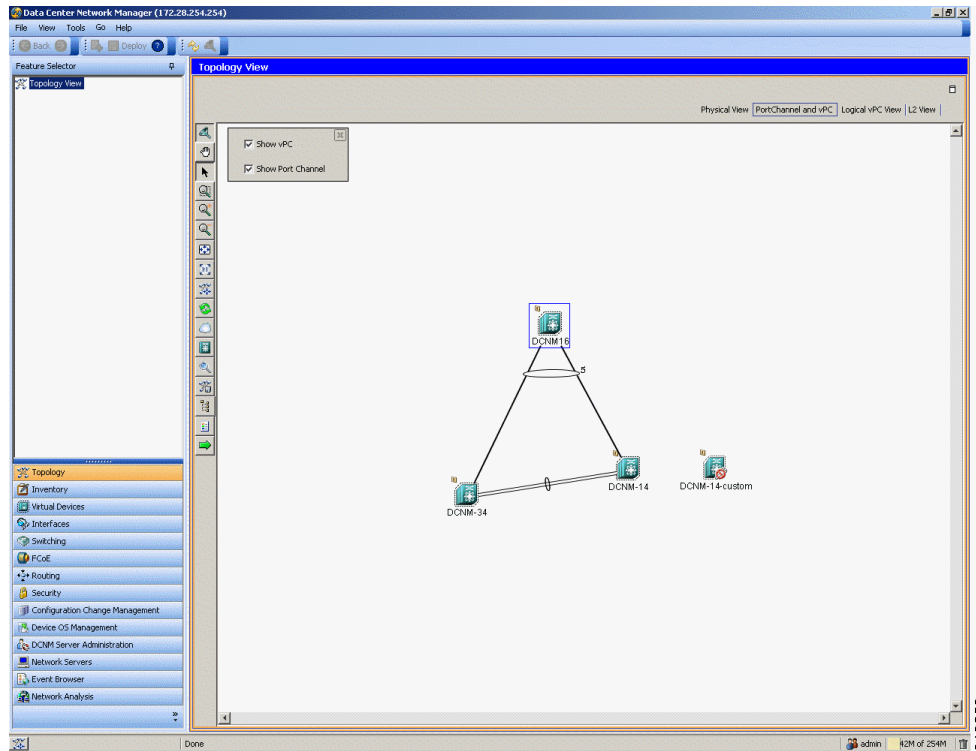
Figure 16-1 *Physical View of the Topology Map*



PortChannel and vPC

The PortChannel and vPC view (see [Figure 16-2](#)) shows all physical connections and all logical connections among discovered devices, including port channel links, virtual port channel (vPC) links, and vPC peer links. Physical links appear in gray in this view.

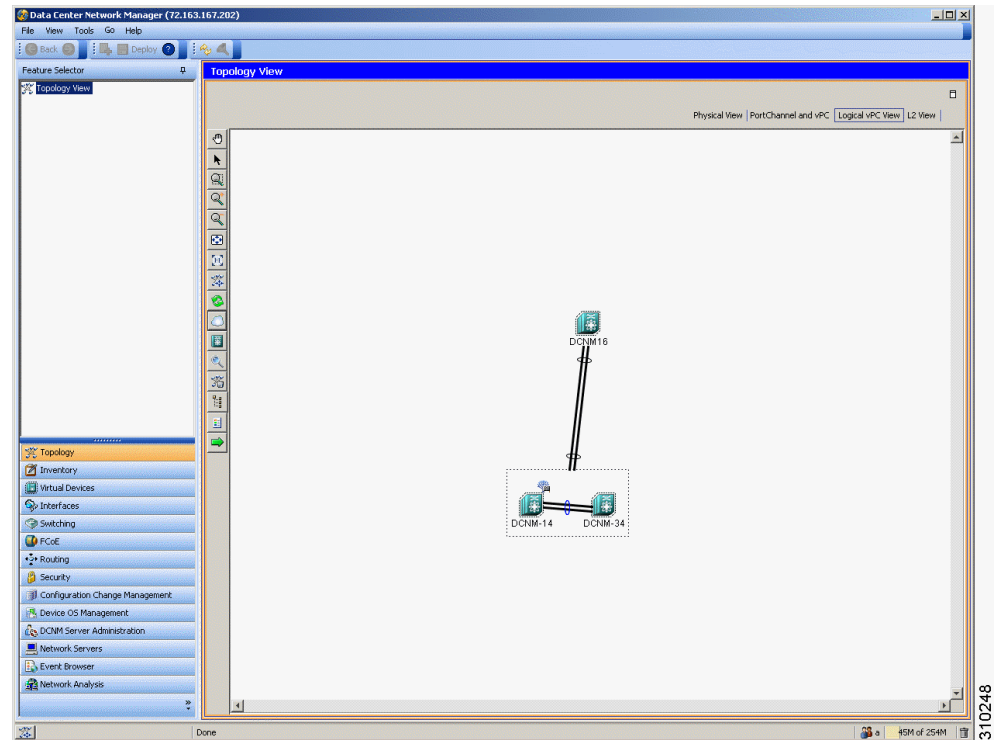
Figure 16-2 PortChannel and vPC View of the Topology Map



Logical vPC View

The Logical vPC View (see [Figure 16-3](#)) shows vPC links and vPC peer links among discovered devices, without showing the physical connections.

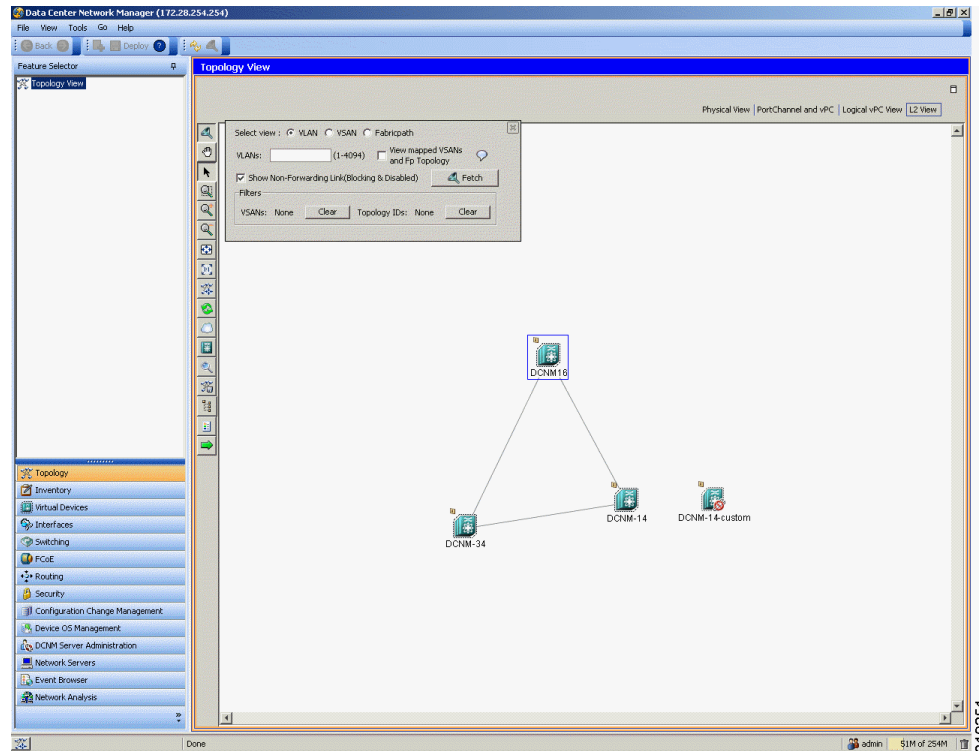
Figure 16-3 Logical vPC View of the Topology Map



L2 View

The L2 view (see [Figure 16-4](#)) shows VLANs configured among discovered devices. Beginning with Cisco DCNM-LAN Release 5.1, the VSAN Overlay is a part of the L2 view. The VSAN Overlay feature enables you to view the Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) links that are active for a given VSAN or a range of VSANs. It also provides a visual representation of forwarding and non-forwarding links between Cisco Nexus devices in a data center network for configured VLANs.

Figure 16-4 L2 View of the Topology Map



Layouts

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

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

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

vPC Support

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

- vPC creation—You can launch the vPC Creation Wizard from the PortChannel and vPC view. See the [“Launching the vPC Wizard” section on page 16-37](#).
- Quick access to the vPC feature—You can access the configuration for a specific vPC from the PortChannel and vPC view or the Logical vPC View. See the [“Managing a vPC” section on page 16-38](#).
- vPC configuration inconsistency—You can see vPC links and vPC peer links that have configuration inconsistencies. You can open the Resolve Configuration Consistency dialog box from the topology map. See the [“Finding and Resolving vPC Configuration Inconsistencies” section on page 16-39](#).

DCNM-SAN Support

The DCNM-LAN topology map supports Cisco Data Center Network Manager for SAN (DCNM-SAN) by providing the features described in the following topics:

- [Common Topology, page 16-7](#)
- [Access to DCNM-SAN Features, page 16-7](#)

Common Topology

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

Access to DCNM-SAN Features

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

The Cisco DCNM-SAN cross launch feature is only supported by the DCNM-LAN client when the Cisco DCNM-SAN is installed in Server mode. Cross launch is not supported by the DCNM-LAN client when the Cisco DCNM-SAN is installed in Standalone mode. In addition, cross launch is not supported when the DCNM-LAN client is in standalone mode.

For information about installing the DCNM-LAN client in standalone mode, see [Chapter 13, “Installing and Launching the Cisco DCNM-LAN Client.”](#)

For information about installing Cisco DCNM-SAN and DCNM-LAN on the same server system, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

FabricPath Support

FabricPath support for L2MP capable devices, running the L2MP-ISIS protocol, is available in the L2 View of the Topology drawer. The L2 View contains a dialog box that allows you to select the type of graph to display. When you select the Fabricpath view in the dialog box, you can display the following types of graphs:

- Multi-destination

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

- Reachability

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

- Unicast

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

- Multicast

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

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

**Note**

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

**Note**

-
- Starting from Cisco DCNM Release 6.1(1) the fabric path support feature will be available for the Cisco Nexus 55xx series switches.
 - Starting from Cisco DCNM Release 6.1(1) the fabric path support feature will be licensed.
-

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

Device Groups

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

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

Network Servers

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

Licensing Requirements for Topology

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM-LAN	The Topology feature requires no license; however, the Logical vPC View of the topology map requires a LAN Enterprise license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN 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 7.1.x</i> .

Prerequisites for Topology

Topology has the following prerequisites:

- The topology map shows only devices that DCNM-LAN has discovered.
- For full support on the topology map, discovered devices should have the applicable discovery protocols enabled, both globally and on active interfaces. For more information about the discovery protocols used by DCNM-LAN, see [Chapter 27, “Administering Device Discovery.”](#)

Guidelines and Limitations

Topology has the following configuration guidelines and limitations:

- While the Topology feature is an unlicensed feature, you must have a LAN Enterprise license to manage the nondefault VDCs of Cisco Nexus 7000 Series switches that appear in the topology.
- The Topology feature displays changes to the topology periodically as determined by the polling frequency for accounting and system logs. By default, the polling frequency is one minute. For more information, see the [“Information About Auto-Synchronization with Devices”](#) section on page 29-1.

Using the Topology Feature

This section includes the following topics:

- [Opening the Topology Map, page 16-10](#)
- [Understanding Device Icons and Links, page 16-13](#)
- [Using the Viewing Tools, page 16-14](#)
- [Showing, Hiding, and Using the Details Pane, page 16-16](#)
- [Moving Devices in the Topology Map, page 16-18](#)

- [Loading a Layout, page 16-19](#)
- [Reloading the Previously Saved Layout, page 16-20](#)
- [Showing a Virtual or Physical Chassis, page 16-21](#)
- [Showing or Hiding Network Servers, page 16-22](#)
- [Managing a Network Server, page 16-22](#)
- [Showing or Hiding Device Groups, page 16-23](#)
- [Expanding or Collapsing Device Groups, page 16-24](#)
- [Creating a Device Group, page 16-25](#)
- [Moving a Device Between Device Groups, page 16-26](#)
- [Removing a Device from a Device Group, page 16-27](#)
- [Copy Run to Start, page 16-28](#)
- [Deleting a Device Group, page 16-29](#)
- [Exporting the Topology as a JPG Image, page 16-30](#)
- [Accessing DCNM-LAN Features from the Topology Map, page 16-31](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map, page 16-32](#)
- [Accessing Cisco FabricPath Features from the Topology Map, page 16-33](#)
- [Launching the vPC Wizard, page 16-37](#)
- [Managing a vPC, page 16-38](#)
- [Finding and Resolving vPC Configuration Inconsistencies, page 16-39](#)
- [Accessing Remotely Connected CNAs from the Topology Map, page 16-39](#)
- [Using VSAN Overlay, page 16-40](#)

Opening the Topology Map

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

When you open the topology map, you can choose one of the following topology views:

- **Physical View**—Shows the physical connections between discovered devices. This is the default topology view.
- **PortChannel and vPC**—Shows all physical connections and all logical connections among discovered devices, including port channels, vPCs, and vPC peer links. Physical links appear in gray in this view.
- **Logical vPC View**—Shows vPC and vPC peer links among discovered devices, without showing the physical connections.
- **L2 View**—Shows VLANs configured among discovered devices.

All views show the discovered devices in your network.

**Note**

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

- Install the Enhanced Layer 2 license on the device. See the *Cisco NX-OS Licensing Guide* for complete information on installing this license.

- Install the FabricPath feature set on the device. See the *Cisco Configuring Feature Set for FabricPath Guide* for complete information on installing the feature set.
 - Configure the FabricPath feature set so that it can be enabled in a custom VDC. See the *Cisco Configuring Feature Set for FabricPath Guide* for complete information on configuring the feature set.
-

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
- The topology map appears in the Contents pane. Buttons for each of the available topology views appear above the topology map.
- Step 2** (Optional) If you want to change topology views, click the topology view name.
- The topology map shows the view of the topology that you selected.
- Step 3** (Optional) If you want to use a view-specific option, see the following table:

View Feature	Available In View	How to Use
Show/Hide all VDCs	<ul style="list-style-type: none"> Physical View 	<p>Right-click in the map and choose Show All VDCs or Hide All VDCs.</p> <p>When you view all VDCs, Cisco Nexus 7000 Series devices appear as gray boxes that contain device icons for each VDC configured on the Cisco Nexus 7000 Series device.</p>
Show/Hide End Devices	<ul style="list-style-type: none"> Physical View L2 View 	<p>Right-click in the map and choose Show End Devices or Hide End Devices.</p>
Filter VLANs	<ul style="list-style-type: none"> L2 View 	<ol style="list-style-type: none"> If the VLANs box does not appear on the map, click the Filter icon on the topology toolbar. Enter a list of VLAN IDs. You can specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges. Click Filter.
Show/Hide non-forwarding links	<ul style="list-style-type: none"> L2 View 	<ol style="list-style-type: none"> On the map, find the VLANs box. Check or uncheck the Show Non-Forwarding Link (Blocking & Disabled) as needed.
Show/Hide vPCs or port channels	<ul style="list-style-type: none"> PortChannel and vPC 	<ol style="list-style-type: none"> On the map, find the gray box that contains the Show vPC check box and the Show Port Channel check box. You may need to scroll the map or zoom out to find the gray box. Check or uncheck the check boxes as needed.

RELATED TOPICS

- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Showing, Hiding, and Using the Details Pane](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Accessing Cisco FabricPath Features from the Topology Map](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

- [Exporting the Topology as a JPG Image](#)
- [Launching the vPC Wizard](#)
- [Managing a vPC](#)
- [Copy Run to Start](#)


Understanding Device Icons and Links

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

DETAILED STEPS

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

The topology map appears in the Contents pane. Buttons for each of the available topology views appear above the topology map. |
| Step 2 | (Optional) If you want to change topology views, click the topology view name.

The topology map shows the view of the topology that you selected. The topology toolbar appears on the left side of the topology map. |
| Step 3 | From the topology toolbar, click the  icon.

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

RELATED TOPICS

- [Opening the Topology Map](#)
- [Using the Viewing Tools](#)
- [Showing, Hiding, and Using the Details Pane](#)
- [Launching the vPC Wizard](#)
- [Managing a vPC](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Accessing Cisco FabricPath Features from the Topology Map](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Exporting the Topology as a JPG Image](#)
- [Copy Run to Start](#)

Using the Viewing Tools

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

The map shows Nexus 7000 Series devices, switches that run Cisco IOS software, and CDP links between devices. The link colors have the following meanings:

- Dark gray—The link between the two devices is active.
- Light gray—In the Physical view, this color means that one of the devices is not reachable. In the PortChannel and vPC view, all physical links appear light gray.
- Red—The physical link between the two devices are down.

The map also indicates whether a link is a single port link or a multiple port link, as follows:













- Single port link—When one link connects two devices, the map connects the two devices with a thin line. The port icon at either end of the line shows a single port.
- Multiple port link—When more than one link connect two devices, the map connects the two devices with a thick line. The port icon at either end of the line shows two ports.
















Tip

To view an explanation of some of icons and links show in the topology map, from the topology tool bar, click **Legend**. The Legend dialog box provides information for icons and links shown in the current topology view.

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

Viewing Tool Icon and Name	How to Use
 Pan	Moves, or pans, the map. <ol style="list-style-type: none"> 1. Click the  icon. 2. Click anywhere on the topology map, and hold down the mouse button. 3. Drag the map in any direction. 4. Release the mouse button.
 Select	Allows you to select a device, link, or port icon. <ol style="list-style-type: none"> 1. Click the  icon. 2. Click the device, link, or port icon that you want to work with. <p>A balloon displays information about the icon that you clicked.</p>
 Zoom in Rect	Zooms to a specific portion of the map. <ol style="list-style-type: none"> 1. Click the  icon. 2. Click on the map and drag a rectangle over the area that you want to see, and release the mouse button.
 Zoom In	Zooms in. Click the  icon.
 Zoom Out	Zooms out. Click the  icon.
 Fit to View	Fits the entire topology of discovered devices within the topology map. Click the  icon.

Viewing Tool Icon and Name	How to Use
 Reset Zoom	Resets the zoom to the default magnification. Click the  icon.
 Load Layout	Loads a layout.
 Reload Layout	Loads the most recently saved layout. See the “Reloading the Previously Saved Layout” section on page 16-20.
 Show Device Groups	Shows or hides device groups. See the “Showing or Hiding Device Groups” section on page 16-23.
 Search	<p>Allows you to use the device search tool, so that you can search for a device by its name.</p> <ol style="list-style-type: none"> 1. To show the Search tool on the map, click the  icon. 2. In the Device box, enter all or some of the name of the device that you want to search for, and then click the  icon. 3. To hide the Search tool, click the  icon again. <p>Tip You can move the Search tool on the topology map by clicking and dragging it when you have the Select tool enabled.</p>
 Save Layout	Saves changes that you have made to the device icon layout. See the “Moving Devices in the Topology Map” section on page 16-18.
 Hide/Show Details	Shows and hides the details pane. See the “Showing, Hiding, and Using the Details Pane” section on page 16-16.
 Legend	Opens the Legend dialog box. See the “Understanding Device Icons and Links” section on page 16-13.
 Export as JPG	Saves the topology map as a JPG image file. See the “Exporting the Topology as a JPG Image” section on page 16-30.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Showing, Hiding, and Using the Details Pane](#)
- [Launching the vPC Wizard](#)
- [Managing a vPC](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco FabricPath Features from the Topology Map](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Copy Run to Start](#)

Showing, Hiding, and Using the Details Pane

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


DETAILED STEPS

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

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




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

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

When you choose to show details, the Details pane appears between the topology toolbar and the topology map.



Tip Ensure that the Select tool is selected. To select the Select tool, click the  icon.

- Step 3** To use the sections within the Details pane, see the following table:

Section	Available In	How to Use
VDC View	<ul style="list-style-type: none"> Physical View L2 View 	Explore the VDC View tree to see which Cisco Nexus 7000 Series devices contain VDCs. To see details about a device, click on it and see the Properties section.
vPC	<ul style="list-style-type: none"> Port Channel and vPC Logical vPC 	Explore the vPC tree to see a categorized listing of all logical connections in the topology map. To see details about a vPC, vPC peer link, or a port channel, click on it and see the Properties section.
Overview	<ul style="list-style-type: none"> All views 	<p>Tip To view the Overview section, you may need to click the Overview tab in the Properties section. The Overview and Properties sections share the same section title bar.</p> <p>The Overview section shows a thumbnail view of the whole topology. A blue rectangle indicates the portion of the topology that is currently shown in the map.</p> <ul style="list-style-type: none"> To change which portion of the topology is shown in the map, in the overview, click where you want the map to show. To zoom in or out, click a corner of the blue rectangle and drag it until the map is enlarged or shrunk as you want.
Properties	<ul style="list-style-type: none"> All views 	<p>Tip To view the Properties section, you may need to click the Properties tab in the Overview section. The Overview and Properties sections share the same section title bar.</p> <ol style="list-style-type: none"> Do one of the following: <ul style="list-style-type: none"> In the VDC View section, click on a physical or virtual device. In the vPC section, click on a logical connection. In the topology map, click on a device, link, or port. In the Properties section, view the properties of the object that you selected.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Managing a vPC](#)

- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Accessing Cisco FabricPath Features from the Topology Map](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

Moving Devices in the Topology Map

You can move device icons that are shown in the topology map. The position of devices is shared by all the topology views, that is, if you move a device and then change to another topology view, the device remains where you moved it to.

You can also save the layout, which you can reload later if you make additional changes and want to revert to your last save.

For more information, see the [“Reloading the Previously Saved Layout”](#) section on page 16-20.

For more information, see [Reloading the Previously Saved Layout](#).

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

**Note**

The DCNM-LAN client saves topology layouts as local user data on the computer that runs the DCNM-LAN client. When you are using the DCNM-LAN client, you do not have access to topology layouts that you saved on other computers or that you saved while logged in to the computer under a different username.


DETAILED STEPS

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

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

**Note**

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


- Step 2** From the topology toolbar, choose the  icon.

- Step 3** Find and move device icons as needed. To move an icon, click on the device icon, hold down the mouse button, drag the icon to the new location, and release the mouse button.

You can zoom and pan as needed to find icons.

For more information, see the [“Using the Viewing Tools”](#) section on page 16-14.

For more information, see [Using the Viewing Tools](#).

Step 4 (Optional) If you want to save the changes to the device icon layout, click the  icon.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Loading a Layout](#)
- [Reloading the Previously Saved Layout](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Exporting the Topology as a JPG Image](#)

Loading a Layout




When you are using the Physical View, you can choose to load a layout. one of the following layouts:

- **Saved**—Devices appear in the layout that you most recently saved on the workstation that is running the Cisco DCNM client.
- **Spring**—Devices appear in locations determined by weighting the connections, which often produces a layout with minimal or no crossed connections.
- **Tree**—Devices appear in a tree unless connections create loops among the devices, in which case devices appear in a spanning tree, that is, a grid in which most of the connections follow the grid layout.

The position of devices is shared by all the topology views. This behavior allows you to use any of the layouts in all views by loading the layout in the Physical View and then choosing another view.



Note

If you are using a different view than the Physical View, the  icon on the topology toolbar acts the same as the  icon. For information about using the  icon, see the [“Reloading the Previously Saved Layout”](#) section on page 16-20.

BEFORE YOU BEGIN

Determine which physical devices, if any, that you want to specify as core switches. When you load a layout other than a saved layout, core switches appear at the top of the topology map, and devices that are one CDP hop from the core switches appear just below them.


DETAILED STEPS

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

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

**Note**

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

- Step 2** (Optional) For each physical device that you want to appear at the top of the layout, right-click on the device icon and choose **Make as Core Switch**.
- Step 3** From the topology toolbar, click the  icon.
The Layout drop-down list appears.
- Step 4** From the Layout drop-down list, choose the layout that you want to load.
The Physical View of the topology map changes to the layout that you selected. Any devices that you specified as core switches appear at the top of the map, with devices that are one CDP hop away from the core switches appearing just below them.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Moving Devices in the Topology Map](#)
- [Reloading the Previously Saved Layout](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Exporting the Topology as a JPG Image](#)

Reloading the Previously Saved Layout

You can load the most recently saved layout. This feature allows you to undo changes to device placement that you have made since you last saved the layout.

**Note**


The DCNM-LAN client saves topology layouts as local user data on the computer that runs the DCNM-LAN client. When you are using the DCNM-LAN client, you do not have access to topology layouts that you saved on other computers or that you saved while logged in to the computer under a different username.

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.

**Note**

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

- Step 2** From the topology toolbar, choose the  icon.
- The topology map changes to the most recent layout that you saved.
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Showing, Hiding, and Using the Details Pane](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Exporting the Topology as a JPG Image](#)

Showing a Virtual or Physical Chassis

For a Cisco Nexus 1000V device, you can specify whether the topology map shows the virtual chassis or the physical chassis of the device. By default, the topology map shows the virtual chassis.

DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
- The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.
- Step 2** Find the Cisco Nexus 1000V device icon.
- The topology map displays either the virtual chassis or the physical chassis.
- Step 3** Right-click on the device icon and choose the applicable option:
- **Show Virtual Chassis**
 - **Show Physical Chassis**
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Showing, Hiding, and Using the Details Pane](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)

Showing or Hiding Network Servers

You can show or hide the network servers that are connected to a specific device. By default, the topology map hides network servers.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
- The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.
- Step 2** Find the device that is connected to network servers that you want to show or hide.
- Step 3** Right-click on the device and choose one of the following:
- To show connected network servers, choose **Show End Devices**.
 - To hide connected network servers, choose **Hide End Devices**.
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Showing, Hiding, and Using the Details Pane](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Managing a Network Server](#)
- [Showing or Hiding Device Groups](#)
- [Copy Run to Start](#)

Managing a Network Server

You can use the topology map to access the Network Servers feature for a network server that appears on the map.

BEFORE YOU BEGIN

The network server must be showing in the topology map.

DETAILED STEPS

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

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



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

Step 2 Find the network server that you want to manage with the Network Servers feature.



Tip If the network server does not appear on the map, right-click a device that it is connected to and choose **Show End Devices**.

Step 3 Right-click on the server and choose **Manage Server**.

The DCNM-LAN client opens to the Network Servers feature. If the server that you chose represents a managed server or an Ethernet adapter on a discovered server, the client opens to the Servers contents pane. If the server that you chose represents a host bus adapter (HBA) that is not correlated or bound to a server, the client opens to the Static Server-Adapter Mapping contents pane.

RELATED TOPICS

- [Showing or Hiding Network Servers](#)

Showing or Hiding Device Groups

You can show or hide device groups. When device groups are hidden, the topology map shows all discovered devices and connections. When your device groups are shown, you can expand and collapse device groups individually or all at once.


DETAILED STEPS


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

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



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

The  icon on the topology toolbar controls whether device groups appear on the topology map. When the icon appears to be pushed in, the topology map shows device groups. When the icon does not appear to be pushed in, the topology map hides device groups.

Step 2 Click the  icon to change between hiding and showing device groups, as needed.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Moving Devices in the Topology Map](#)
- [Showing or Hiding Network Servers](#)
- [Expanding or Collapsing Device Groups](#)
- [Creating a Device Group](#)
- [Moving a Device Between Device Groups](#)
- [Removing a Device from a Device Group](#)
- [Deleting a Device Group](#)
- [Copy Run to Start](#)

Expanding or Collapsing Device Groups

You can expand and collapse individual device groups or all device groups.


DETAILED STEPS

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

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



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

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the  icon.

Step 3 Do one of the following:

- If you want to expand a single device group, right-click on the device group icon and choose **Expand Device Group**.
 - If you want to expand all device groups, right-click on a blank area of the map and choose **Expand all Device Groups**.
 - If you want to collapse a single device group, right-click on the title of the device group and choose **Collapse Device Group**.
 - If you want to collapse all device groups, right-click on a blank area of the map and choose **Collapse all Device Groups**.
-

RELATED TOPICS

- [Opening the Topology Map](#)

- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Moving Devices in the Topology Map](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Creating a Device Group](#)
- [Moving a Device Between Device Groups](#)
- [Removing a Device from a Device Group](#)
- [Deleting a Device Group](#)
- [Copy Run to Start](#)

Creating a Device Group

You can create a custom device group on the topology map.

DETAILED STEPS

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

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



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

Step 2 Right-click on a blank area of the map and choose **New Device Group**.

A dialog box appears, with a field for specifying a name for the new device group.

Step 3 Type a name for the device group and click **OK**.

The new device group appears on the topology map.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Moving Devices in the Topology Map](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Expanding or Collapsing Device Groups](#)
- [Moving a Device Between Device Groups](#)
- [Removing a Device from a Device Group](#)

- [Deleting a Device Group](#)
- [Copy Run to Start](#)

Moving a Device Between Device Groups

You can move devices from one device group to another device group on the topology map.

**Note**

If a device group is empty after you move a device out of the group, DCNM-LAN deletes the device group.


DETAILED STEPS

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

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

**Note**

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

- Step 2** If device groups do not appear on the topology map, from the topology toolbar, click the  icon.

- Step 3** Find the device group that you want to move the device out of.

- Step 4** If the device group is collapsed, double-click the device group to expand it.

- Step 5** Right-click on the device that you want to move out of the group and choose **Cut**.

- Step 6** Find the device group that you want to move the device into.

**Tip**

You do not need to expand the device group before moving the device into the group.

- Step 7** Right-click the device group and choose **Paste**.

**Tip**

If the device group is expanded, you must click on the title of the device group.

A warning dialog box confirms that you want to move the device group.

- Step 8** Click **Yes**.

DCNM-LAN adds the device to the second device group and removes it from the first device group. If the first device group is empty after moving the device, DCNM-LAN deletes the first device group.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)

- [Moving Devices in the Topology Map](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Expanding or Collapsing Device Groups](#)
- [Creating a Device Group](#)
- [Removing a Device from a Device Group](#)
- [Deleting a Device Group](#)
- [Copy Run to Start](#)

Removing a Device from a Device Group

You can remove devices from a custom device group. All devices that you remove from a custom group are added to the default device group.


DETAILED STEPS

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

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



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

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the  icon.

Step 3 Find the device group that you want to remove a device from.

Step 4 If the device group is collapsed, double-click the device group to expand it.

Step 5 Right-click on the device that you want to remove from the group and choose **Remove from Group**.

If you are removing the only device from the group, a warning dialog box confirms that you want to remove the device group.

Step 6 If the warning appears, click **Yes**.

DCNM-LAN removes the device from the custom device group and adds the device to the default device group.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Moving Devices in the Topology Map](#)
- [Showing or Hiding Network Servers](#)

- [Showing or Hiding Device Groups](#)
- [Expanding or Collapsing Device Groups](#)
- [Creating a Device Group](#)
- [Moving a Device Between Device Groups](#)
- [Deleting a Device Group](#)
- [Copy Run to Start](#)

Copy Run to Start

In the Physical View, you can copy the running configuration to the startup configuration on one or more selected devices.


DETAILED STEPS

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

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



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

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the  icon.

Step 3 Above the topology map, select **Physical View**.

Step 4 Select the devices that you want to copy the running configuration from.

Step 5 If the device group is collapsed, double-click the device group to expand it.

Step 6 Right-click the device that you want to copy the running configuration from.

- If you want to copy the running configuration to the startup configuration, choose **Copy Run to Start**.
DCNM-LAN copies the running configuration to the startup configuration.
- If you want to copy the running configuration to a file in the bootflash directory, choose **Copy Run to File in Bootflash**. In the dialog box that appears, enter the name of the file to copy to and click **OK** to complete the operation.
DCNM-LAN copies the running configuration to the specified file.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Moving Devices in the Topology Map](#)
- [Showing or Hiding Network Servers](#)

- [Showing or Hiding Device Groups](#)
- [Expanding or Collapsing Device Groups](#)
- [Creating a Device Group](#)
- [Moving a Device Between Device Groups](#)
- [Removing a Device from a Device Group](#)
- [Deleting a Device Group](#)

Deleting a Device Group

You can delete a custom device group from the topology map.

Devices that belong to a custom device group that you delete automatically become members of the default device group.

DETAILED STEPS

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

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



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

Step 2 If device groups do not appear on the topology map, from the topology toolbar, click the  icon.

Step 3 Find the device group that you want to delete.

Step 4 Right-click on the device group and choose **Delete Group**.

DCNM-LAN removes the device group from the topology map. The devices that were in the deleted device group are now members of the default device group.



Note If there are no custom device groups after you delete the device group, the topology map automatically hides devices groups because all devices are in the default device group.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Moving Devices in the Topology Map](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)
- [Expanding or Collapsing Device Groups](#)

- [Creating a Device Group](#)
- [Moving a Device Between Device Groups](#)
- [Removing a Device from a Device Group](#)
- [Copy Run to Start](#)

Exporting the Topology as a JPG Image

You can export, or save, a JPG image of the topology map. You can export either the entire topology map or only the visible portion of the topology map.

DETAILED STEPS

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

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



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

Step 2 View the portion of the topology map that you want to save.


For more information, see the [“Using the Viewing Tools”](#) section on page 16-14.

For more information, see the [Using the Viewing Tools](#).

Step 3 Arrange the device icons as desired.

For more information, see the [“Moving Devices in the Topology Map”](#) section on page 16-18.

For more information, see the [Moving Devices in the Topology Map](#).

Step 4 From the topology toolbar, click the  icon.

A dialog box prompts you to choose whether you want to export the entire topology map or only the visible portion of the map.

Step 5 Do one of the following:

- To export the entire topology map as a JPG image, click **Yes**.
- To export only the visible portion of the topology map, click **No**.

Step 6 Specify the location and filename of the JPG image and click **Save**.

The JPG image of the visible portion of the topology map is saved.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Showing, Hiding, and Using the Details Pane](#)

- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Reloading the Previously Saved Layout](#)
- [Showing or Hiding Network Servers](#)
- [Showing or Hiding Device Groups](#)


Accessing DCNM-LAN Features from the Topology Map

You can use the topology map to access other DCNM-LAN features for managed devices. From the topology map, you can access features that are found in the following Feature Selector drawers:

- Inventory
- Virtual Devices
- Interfaces
- Routing
- Switching
- Security

You can also use the topology map to access the Device Discovery feature.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
- The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.
-  **Note** To see the names of topology toolbar icons, move the mouse pointer to the icon and wait briefly for the name of the icon to appear.
-
- Step 2** If you want to access a DCNM-LAN feature for a specific managed device, do the following:
- a. Find the device in the topology map.
 - b. Right-click the device and choose the feature that you want to configure.
- The feature that you selected appears in the Contents pane. The device that you selected on the topology map is selected in the Summary table for the feature.
- Step 3** If you want to access the Device Discovery feature, right-click a blank area on the map and choose **Discover Devices**.
- The Device Discovery feature appears in the Contents pane.
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)

- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Accessing Cisco FabricPath Features from the Topology Map](#)
- [Managing a vPC](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

Accessing Cisco DCNM-SAN Features from the Topology Map

You can use the topology map to access features in the Cisco DCNM-SAN client for a managed SAN device. If Cisco DCNM-SAN has not discovered the device, accessing the Cisco DCNM-SAN client through the topology map will cause Cisco DCNM-SAN to discover the SAN device.

The Cisco DCNM-SAN features that you can access include the following:

- Zones, zone sets, and zone set membership
- Port channel interfaces
- Fibre Channel physical and logical interfaces
- Fibre Channel over IP tunnels
- Events

**Note**

The Cisco DCNM-SAN cross launch feature is only supported by the DCNM-LAN client when the Cisco DCNM-SAN is installed in Server mode. Cross launch is not supported by the DCNM-LAN client when the Cisco DCNM-SAN is installed in Standalone mode. In addition, cross launch is not supported when the DCNM-LAN client is in standalone mode.

BEFORE YOU BEGIN

The Cisco DCNM-SAN client must be installed on the computer that is running the DCNM-LAN client.

DETAILED STEPS

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

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

**Note**

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

- Step 2** Find the SAN device in the topology map.

- Step 3** Right-click the device and choose the feature that you want to configure.

The Cisco DCNM-SAN client opens to the feature that you selected.

RELATED TOPICS

- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco FabricPath Features from the Topology Map](#)
- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

Accessing Cisco FabricPath Features from the Topology Map

You can use the topology map to access features of the Cisco FabricPath.

This section includes the following topics:

- [Multi-destination, page 16-33](#)
- [Device Reachability, page 16-34](#)
- [Unicast, page 16-35](#)
- [Multicast, page 16-36](#)

Multi-destination

A multi-destination or broadcast graph represents broadcast traffic and unknown unicast traffic in the topology. You can view the multi-destination information for a specific topology.

DETAILED STEPS

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

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



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

Step 2 Above the map, click **L2 View**.

The dialog box appears in the Contents pane.

Step 3 In the dialog box, choose the **Fabricpath** view.

Step 4 Enter the Topology ID and click **Fetch**. The graph that is displayed is filtered based upon the Topology ID.

Step 5 Check **Select type of graph** to enable the selection for the Multi-destination graph.

- Step 6** Check the **Multi-destination** option.
- Step 7** From the Anchor drop-down list, choose a device. The selected device is the entry point for the graph.
- Step 8** From the Graph ID drop-down list, choose an ID. The Graph ID is a forwarding tag for the graph.
- Step 9** Click **Fetch** to view the graph.
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Managing a vPC](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

Device Reachability

L2MP-ISIS automatically computes the switch ID reachability for each node in the network. You can view the reachability information for a specific topology.

DETAILED STEPS

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

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



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

- Step 2** Above the map, click **L2 View**.
The dialog box appears in the Contents pane.
- Step 3** In the dialog box, choose the **Fabricpath** view.
- Step 4** Enter the Topology ID. The graph that is displayed is filtered based upon the Topology ID.
- Step 5** Check **Select type of graph** to enable the selection for the Reachability graph.
- Step 6** Check the **Reachability** option.
- Step 7** From the Anchor drop-down list, choose a device. The selected device is the entry point for the graph.

Step 8 Click **Fetch** to view the graph.

**Note**

Devices in the graph that appear as red colored icons indicate that the device is not reachable for the selected topology.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Managing a vPC](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

Unicast

A unicast graph displays equal cost routes between nodes in a network. You can view the unicast information for a specific topology.

DETAILED STEPS

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

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

**Note**

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

Step 2 Above the map, click **L2 View**.

The dialog box appears in the Contents pane.

Step 3 In the dialog box, choose the **Fabricpath** view.

Step 4 Enter the Topology ID. The graph that is displayed is filtered based upon the Topology ID.

Step 5 Check **Select type of graph** to enable the selection for the Unicast graph.

Step 6 Check the **Unicast** option.

Step 7 From the Anchor drop-down list, select a device. The selected device is the entry point for the graph.

Step 8 From the Destination drop-down list, select a device. The selected device is the destination for the graph.

Step 9 Click **Fetch** to view the graph.

**Note**

If the resulting graph does not trace the path from the source to the destination, then one of the following may be the cause:

- Islands in the L2MP cloud.
 - DCNM-LAN might not manage intermediate devices.
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Managing a vPC](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)

Multicast

A multicast graph displays the multicast traffic from a specified device to all hosts that are listening to a particular IGMP group. You can view the multicast information for a specific topology.

DETAILED STEPS

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

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

**Note**

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

Step 2 Above the map, click **L2 View**.

The dialog box appears in the Contents pane.

Step 3 In the dialog box, choose the **Fabricpath** view.

Step 4 Enter the Topology ID. The graph that is displayed is filtered based upon the Topology ID.

Step 5 Check **Select type of graph** to enable the selection for the Multicast graph.

- Step 6** Check the **Multicast** option.
- Step 7** From the Anchor drop-down list, choose a device. The selected device is the entry point for the graph.
- Step 8** From the Graph ID drop-down list, choose an ID. The Graph ID is a forwarding tag for the graph.
- Step 9** In the Source field, enter the multicast originating device. The multicast originating device is specified as an IP address or as “*” (wildcard).
- Step 10** In the IGMP field, enter the IGMP group address.
- Step 11** In the VLAN field, enter multicast-associated VLAN information.
- Step 12** Click **Fetch** to view the graph.
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Managing a vPC](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)


Launching the vPC Wizard

From the topology map, you can launch the vPC wizard to create a vPC.

BEFORE YOU BEGIN

Determine which two devices you want to use as the vPC peer switches.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
The topology map appears in the Contents pane.
- Step 2** Above the map, click **PortChannel and vPC**.
The map shows the PortChannel and vPC view of the topology.
- Step 3** From the topology toolbar, choose the  icon.
- Step 4** Click one device that you want to use as a vPC peer switch.
- Step 5** Press and hold the **Shift** key.
- Step 6** Click the device that you want to use as a vPC peer switch.

Step 7 Right-click either device and choose **Launch vPC Wizard**.

The vPC Creation Wizard dialog box appears.

For more information about using this wizard, see the *Interfaces Configuration Guide, Cisco DCNM for LAN*.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Managing a vPC](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Exporting the Topology as a JPG Image](#)

Managing a vPC

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

DETAILED STEPS

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

The topology map appears in the Contents pane.

Step 2 Above the map, click one of the following views:

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

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

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

- PortChannel and vPC—Right-click the ellipse on the vPC link and choose **Manage vPC**.
- Logical vPC View—Right-click the vPC link and choose **Manage vPC**.

The vPC feature appears. The vPC that you want to manage is selected in the summary table.

For more information about the vPC feature, see the *Interfaces Configuration Guide, Cisco DCNM for LAN*.

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Finding and Resolving vPC Configuration Inconsistencies](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Exporting the Topology as a JPG Image](#)

Finding and Resolving vPC Configuration Inconsistencies

You can use the topology map to find vPCs that have configuration inconsistencies and open the Resolve Configuration Inconsistency dialog box.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | From the Feature Selector pane, choose Topology > Topology View .
The topology map appears in the Contents pane. |
| Step 2 | Above the map, click one of the following views: <ul style="list-style-type: none">• PortChannel and vPC• Logical vPC View |
| Step 3 | Find the vPC for which you want to resolve configuration inconsistencies.
If a vPC link has configuration inconsistencies, a red ellipse appears over the link. If you use the PortChannel and vPC view, vPC peer links with configuration inconsistencies also show a red ellipse. |
| Step 4 | (Optional) If you want to resolve configuration inconsistencies now, do one of the following: <ul style="list-style-type: none">• To resolve configuration inconsistencies for the vPC link <i>and</i> the vPC peer link, right-click the red ellipse on the vPC link and choose Launch Configuration Consistency.• To resolve configuration inconsistencies for the vPC peer link only, right-click the red ellipse on the vPC link and choose Launch Configuration Consistency. The Resolve Configuration Inconsistency dialog box opens. |
-

Accessing Remotely Connected CNAs from the Topology Map

You can use the topology map to access servers connected to Cisco Nexus 4000 Series switches.

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
- The topology map appears in the Contents pane. The topology toolbar appears on the left side of the topology map.
- Step 2** Right-click on the switch and then choose **Show End Devices**.
- The Contents pane displays all the servers that are connected to the switch. It displays only the pWWN of the servers because the IP address is not available as a part of the enode information in FIP snooping.
-

Using VSAN Overlay

DETAILED STEPS

-
- Step 1** From the Feature Selector pane, choose **Topology > Topology View**.
- The topology map appears in the Contents pane.
- Step 2** Above the map, click **L2 View**.
- The dialog box appears in the Contents pane.
- Step 3** In the dialog box, click **VSAN**.
- Step 4** Enter the range to search (valid values are between 1 and 4094).
- Step 5** Check **View mapped VLANs** to view the VLANs.
- Step 6** Click **Fetch**.
-

RELATED TOPICS

- [Opening the Topology Map](#)
- [Understanding Device Icons and Links](#)
- [Using the Viewing Tools](#)
- [Launching the vPC Wizard](#)
- [Managing a vPC](#)
- [Accessing DCNM-LAN Features from the Topology Map](#)
- [Accessing Cisco DCNM-SAN Features from the Topology Map](#)
- [Moving Devices in the Topology Map](#)
- [Loading a Layout](#)
- [Exporting the Topology as a JPG Image](#)

Related Documents

For additional information related to the topology map, see the following sections:

Related Topic	Document Title
VDCs	<i>Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i>
vPCs	<i>Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i>
Configuring LLDP on managed devices	<i>System Management Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i>
Device discovery	Chapter 27, “Administering Device Discovery”

Feature History for Topology

[Table 16-1](#) lists the release history for this feature.

Table 16-1 Feature History for Topology

Feature Name	Releases	Feature Information
Common topology	5.0(2)	Support for SAN devices and connections was added.
Network servers	5.0(2)	Support for showing network servers was added.
DCNM-SAN support	5.0(2)	Support for launching the Cisco DCNM-SAN client was added.
Device groups	5.0(2)	Support for device groups was added.
VSAN Overlay	5.1(0)	Support for VSAN overlay was added as a part of the L2 view.
Discovery of servers connected to Cisco Nexus 5000 series switches via CNAs	5.1(0)	Support for discovering servers that are either directly connected to Cisco Nexus 5000 Series switches or CNAs.
FabricPath support	5.1(0)	Support for FabricPath was added.
Datacenter Grouping	6.0	Support for Datacenter Grouping was added.



CHAPTER 17

Working with Inventory

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

This chapter includes the following sections:

- [Information About Inventory, page 17-1](#)
- [Licensing Requirements for Inventory, page 17-3](#)
- [Prerequisites, page 17-3](#)
- [Platform Support, page 17-3](#)
- [Configuring Module Pre-Provisioning, page 17-4](#)
- [Reloading a Line Card, page 17-5](#)
- [Displaying Inventory Information, page 17-6](#)
- [Displaying Power Usage Information, page 17-9](#)
- [Field Descriptions, page 17-10](#)
- [Feature History for Inventory, page 17-12](#)

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 18, “Managing Virtual Devices.”](#)

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 Configuration Guide, Release 5.x*.

This section includes the following topics:

- [Understanding Inventory, page 17-2](#)
- [Understanding Power Usage, page 17-2](#)
- [Module Pre-Provisioning, page 17-2](#)

Understanding Inventory

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

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.

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 7.1.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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, 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

Platform	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.

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 17-4](#)
- [Pre-Provisioning Online Modules, page 17-4](#)
- [Pre-Provisioning FEX Modules, page 17-5](#)

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.
-

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 17-6](#)
- [Displaying the Module Information, page 17-7](#)
- [Displaying the Power Supply Information, page 17-8](#)
- [Displaying the Fan Tray Information, page 17-8](#)

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 [“Working with Statistics and Charts” section on page 14-11](#).
 - **Memory Utilization**—Displays collected statistics showing the memory utilization within specific thresholds. For more information on collecting statistics for this feature, see the [“Working with Statistics and Charts” section on page 14-11](#).
 - **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.
-

RELATED TOPICS

- [Displaying the Module Information, page 17-7](#)
- [Displaying the Power Supply Information, page 17-8](#)
- [Displaying the Fan Tray Information, page 17-8](#)

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. |
| Step 3 | Click the module.

Tabs appear in the Details pane with the Details tab selected. |
| Step 4 | Click one of the following tabs: <ul style="list-style-type: none">• 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 “Working with Statistics and Charts” section on page 14-11.• 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. |
-

RELATED TOPICS

- [Displaying the Chassis Information, page 17-6](#)
- [Displaying the Power Supply Information, page 17-8](#)
- [Displaying the Fan Tray Information, page 17-8](#)

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.
-

RELATED TOPICS

- [Displaying the Chassis Information, page 17-6](#)
- [Displaying the Module Information, page 17-7](#)
- [Displaying the Fan Tray Information, page 17-8](#)

Displaying the Fan Tray Information

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

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.
-

RELATED TOPICS

- [Displaying the Chassis Information, page 17-6](#)
- [Displaying the Module Information, page 17-7](#)
- [Displaying the Power Supply Information, page 17-8](#)

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 17-9](#)
- [Displaying Power Usage Details, page 17-9](#)
- [Displaying Power Usage Statistics, page 17-10](#)

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.

RELATED TOPICS

- [Displaying Power Usage Details, page 17-9](#)
- [Displaying Power Usage Statistics, page 17-10](#)

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.

RELATED TOPICS

- [Displaying Power Usage Summary Information, page 17-9](#)
- [Displaying Power Usage Statistics, page 17-10](#)

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.

RELATED TOPICS

- [Displaying Power Usage Summary Information, page 17-9](#)
- [Displaying Power Usage Details, page 17-9](#)

Field Descriptions

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

- [Inventory: Details: Hardware Section, page 17-10](#)
- [Inventory: Details: Software Section, page 17-11](#)
- [Inventory: Power Usage, page 17-11](#)

Inventory: Details: Hardware Section

Table 17-1 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.

Inventory: Details: Software Section

Table 17-2 *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 17-3 *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.

Feature History for Inventory

Table 17-4 lists the release history for this feature.

Table 17-4 *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.



CHAPTER 18

Managing Virtual Devices

This chapter describes virtual device contexts (VDCs) supported on Cisco NX-OS devices.

This chapter includes the following sections:

- [Managing Virtual Switches, page 18-1](#)
- [Creating VDCs with the VDC Setup Wizard, page 18-1](#)
- [Creating VDCs with the VDC Setup Wizard, page 18-1](#)

For detailed configuration guide, please refer to *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 7.x*.

Managing 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 embedded in each VMware vSphere (ESX) host.

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

A domain is an instance of a Cisco Nexus 1000V Series switch device, including dual redundant VSMs and managed VEMs, within a VMware vCenter server. Each domain is distinguished by a unique integer called the domain identifier.

In order for the Cisco Nexus 1000V to connect to a vCenter Server or an ESX server, you must first define the connection parameters. All communication with the vCenter Server is secured by the Transport Layer Security (TLS) protocol.

This chapter in *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to manage virtual switches using Cisco Data Center Network Manager (DCNM).

Creating VDCs with the VDC Setup Wizard

This chapter in *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to create virtual device contexts (VDCs) on Cisco NX-OS devices.

This chapter in *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to create virtual device contexts (VDCs) on Cisco Data Center Network Manager (DCNM). In Cisco NX-OS, only a user with the network-admin role can create VDCs. You can create up to three VDCs. Beginning with the Cisco NX-OS Release 5.2(1), you can run FCoE on the Cisco Nexus 7000 Series devices. You must create a storage VDC to run FCoE. The storage VDC cannot be the default VDC and you can have one storage VDC on the device.

Managing VDCs

This chapter in *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to manage virtual device contexts (VDCs) on Cisco Data Center Network Manager (DCNM).

This chapter describes how to manage virtual device contexts (VDCs) on Cisco NX-OS devices.

After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies. You can also save the VDC configuration on the physical device to the startup configuration or to a bootflash file



Configuring Interfaces on DCNM-LAN Client

Cisco NX-OS supports multiple configuration parameters for each of the interface types supported. Most of these parameters are covered in this guide but some are described in other documents.

[Table 19-1](#) shows where to get further information on the parameters you can configure for an interface.

Table 19-1 **Interface Parameters**

Feature	Parameters	Further Information
Basic parameters	description, duplex, error disable, flow control, MTU, beacon	Configuring Basic Interface Parameters of this document
Layer 2	Layer 2 access and trunk port settings	Configuring Layer 2 Interfaces of this document
	Layer 2 MAC, VLANs, private VLANs, Rapid PVST+, Multiple Spanning Tree, Spanning Tree Extensions	<i>Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.1.xCisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x</i>
	Port security	<i>Security Configuration Guide, Cisco DCNM for LAN, Release 7.1.xCisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x</i>
Layer 3	medium, IPv4 and IPv6 addresses	Configuring Layer 3 Interfaces of this document
	bandwidth, delay, IP routing, VRFs	<i>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x</i> <i>Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x</i>
Port Channels	channel group, LACP	Configuring Port Channels of this document
vPCs	Virtual port channels	Configuring vPCs of this document
Tunnels	GRE Tunneling	Configuring IP Tunnels of this document
Security	Dot1X, NAC, EOU, port security	<i>Security Configuration Guide, Cisco DCNM for LAN, Release 7.1.xCisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x</i>

Table 19-1 **Interface Parameters (continued)**

Feature	Parameters	Further Information
FCoE	Beginning with Cisco NX-OS Release 5.2(1), you can run Fibre Channel over Ethernet (FCoE) on the Cisco Nexus 7000 Series switch	<i>Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500</i>
Virtual Ethernet Interfaces	Logical interfaces that correspond to a switch interface connected to a virtual port	Configuring Virtual Ethernet Interfaces of this document
Fabric Extenders	High-density, low-cost connectivity for server aggregation	Configuring Fabric Extenders of this document
Port Profiles	A mechanism for simplifying the configuration of interfaces.	Configuring Port Profiles of this document

This chapter includes the following topics:

- [Configuring Basic Interface Parameters](#), page 19-2
- [Configuring Layer 2 Interfaces](#), page 19-3
- [Configuring Layer 3 Interfaces](#), page 19-4
- [Configuring Port Channels](#), page 19-4
- [Configuring vPCs](#), page 19-5
- [Configuring IP Tunnels](#), page 19-6
- [Configuring Virtual Ethernet Interfaces](#), page 19-6
- [Configuring Fabric Extenders](#), page 19-6
- [Configuring Port Profiles](#), page 19-7

For detailed information about the configuration of the interface on DCNM-LAN client, see the *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x*.

Configuring Basic Interface Parameters

This chapter in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure the basic interface parameters for interfaces managed by Cisco Data Center Network Manager (DCNM) 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.

Many Layer 2 and Layer 3 interfaces are configured with the same parameters. When you configure these parameters, your settings affect the other interfaces that use those parameters.

Configuring Layer 2 Interfaces

**Note**

Beginning with Cisco Release 5.2, the Cisco Nexus 7000 Series devices support FabricPath Layer 2 interfaces. See the *Cisco Nexus 7000 Series NX-OS FabricPath Command Reference* for complete information about the FabricPath feature and interfaces.

This chapter in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure Layer 2 switching ports as access or trunk ports on Cisco NX-OS devices using Cisco Data Center Network Manager (DCNM).

**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.

Layer 2 interfaces are used for switching packets. You can configure a Layer 2 port as an access port, which carries only one VLAN, or a trunk port, which carries many VLANs. By default, a trunk port carries all VLANs that are configured on the device, and you configure the trunk port to carry only those VLANs that you want on that port. The device uses IEEE 802.1Q to tag packets. All trunk ports must be in the same device, and trunk ports cannot carry VLANs from different devices.

You identify a native VLAN for each trunk port. The trunk port carries the traffic for that specific VLAN as untagged packets. If you do not configure a native VLAN, the device uses the default VLAN to carry untagged traffic for that trunk port. You can also configure the device to drop all untagged traffic on trunk ports and to retain the tag for the native VLAN.

**Note**

Beginning with Cisco NX-OS Release 5.1, a Layer 2 port can function as either one of the following:

- A trunk port
- An access port
- A private VLAN port (see the *Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*, for more information on private VLANs)
- A FabricPath port (see the *Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 5.x*, and the *Cisco DCNM FabricPath Configuration Guide, Release 5.x*, for information on FabricPath)

Beginning with Cisco NX-OS Release 5.2(1), a Layer 2 port can also function as a shared interface. You cannot configure an access interface as a shared interface. See the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on shared interfaces.

**Note**

See the *Cisco DCNM FabricPath Configuration Guide, Release 5.x*, for more information on configuring the FabricPath feature.

**Note**

A Layer 2 port can function as either a trunk port, an access port, or a private VLAN port.

**Note**

See the *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*, for information on configuring a SPAN destination interface.

Configuring Layer 3 Interfaces

This chapter in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure Layer 3 interfaces for Cisco NX-OS devices using Cisco Data Center Network Manager (DCNM).

**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.

Layer 3 interfaces forward IPv4 and IPv6 packets to another device using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter-VLAN routing of Layer 2 traffic. A layer 3 logical interface (VLAN network interface, loopback, tunnel) configured in one VDC is isolated from a layer 3 logical interface with the same number configured in another VDC. For example, loopback 0 in VDC 1 is independent of loopback 0 in VDC 2.

You cannot configure a shared interface as a Layer 3 interface. See the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on shared interfaces.

Beginning with Cisco Release 5.2(1), you can configure a Fabric Extender (FEX) port as a Layer 3 interface for host connectivity, but not for routing. See the *Configuring the Cisco Nexus 2000 Series Fabric Extender* for more information on fabric extenders.

Configuring Port Channels

This chapter in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure port channels and to apply and configure the Link Aggregation Control Protocol (LACP) for more efficient use of port channels using Cisco Data Center Network Manager (DCNM) in the Cisco NX-OS devices.

Beginning with Cisco Release NX-OS 5.1(1), you can use any of the F1 series modules or M1 series modules for the port channel, but you cannot combine member ports on an F1 module with ports on an M1 module in a single port channel. On a single switch, the port-channel compatibility parameters must be the same among all the port-channel members on the physical switch.

For more information about the Data Center Network Manager features and using the Topology tab with port channels, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

**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.

**Note**

System-message logging levels for the port channels feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them 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 Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*.

Configuring vPCs

This chapter in Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure virtual port channels (vPCs) using Cisco Data Center Network Manager (DCNM) on Cisco NX-OS devices.

**Note**

Beginning with Cisco NX-OS Release 5.1(1), vPCs have been enhanced to interoperate with FabricPath. To configure vPCs with FabricPath networks, see the *Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide, Release 5.x*.

**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.

**Note**

System-message logging levels for the vPC feature must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them 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 Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*.

Beginning with Cisco NX-OS Release 5.1(1), you can use any of the 10-Gbps Ethernet (10GE) interfaces on the F series modules or the 10GE interfaces on the M series modules for the vPC peer link on an individual switch, but you cannot combine member ports on an F module with ports on an M module into a single port channel on a single switch. The port channel compatibility parameters must be the same for all the port channel members on the physical switch.

You cannot configure shared interfaces to be part of a vPC. See the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for more information on shared interfaces.

**Note**

The port channel compatibility parameters must also be the same for all vPC member ports on both peers and therefore you must use the same type of module in each chassis.

Virtual port channels (vPCs) allow links that are physically connected to two different Cisco Nexus 7000 series devices to appear as a single port channel by a third device.

Configuring IP Tunnels

**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 in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure IP tunnels using Generic Route Encapsulation (GRE) using the Cisco Data Center Network Manager (DCNM) on Cisco NX-OS devices.

Configuring Virtual Ethernet Interfaces

This chapter in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure virtual Ethernet (vEthernet or vEth) interfaces using Cisco Data Center Network Manager (DCNM).

Virtual Ethernet (vEthernet or vEth) interfaces are logical interfaces. Each vEthernet interface corresponds to a switch interface that is connected to a virtual port. The interface types are as follows:

- Virtual Machine (VM) (interfaces connected to VM NICs)
- Service console
- VM-Fabric Extender (FEX)
- FEX-Adapter
- vmkernel

vEthernet interfaces are created on the Cisco MDS 9000 Series to represent virtual ports in use on the distributed virtual switch.

**Note**

System-message logging levels for the Virtual Ethernet interfaces 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

Configuring Fabric Extenders

**Note**

Beginning with Cisco DCNM for LAN, Release 5.2, you can configure a Fabric Extender host interface port as a routed or Layer 3 port. However, no routing protocols can be tied to this routed interface.

The Fabric Extender feature allows you to manage a Cisco Nexus 2000 Series Fabric Extender and its association with the Cisco NX-OS switch that it is attached to. A Fabric Extender is connected to the switch through physical Ethernet interfaces or a Port Channel. By default, the switch does not allow the attached Fabric Extender to connect until it has been assigned a chassis ID and is associated with the connected interface.

**Note**

The Fabric Extender may connect to the switch through a number of separate physical Ethernet interfaces or at most one port channel interface.

This chapter in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure a Fabric Extender using Cisco Data Center Network Manager (DCNM) on a Cisco NX-OS device.

Configuring Port Profiles

This chapter in *Interfaces Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure port profiles using Cisco Data Center Network Manager (DCNM).

A port profile is a mechanism for simplifying the configuration of interfaces. You can configure a port profile and then assign it to multiple interfaces to give them all the same configuration. Changes to the port profile are propagated to the configuration of any interface that is assigned to it.

You can configure Ethernet or vEthernet port profiles to which you can assign Ethernet or vEthernet interfaces, respectively.

**Note**

We do not recommend that you override port profile configurations by making changes to the assigned interface configurations. Only make configuration changes to interfaces to quickly test a change or to disable a port.

**Note**

System-message logging levels for the Port Profiles 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.



Configuring Switching on DCNM-LAN Client

This chapter briefly introduces the following features:

- [Configuring VLANs, page 20-1](#)
- [Configuring Private VLANs, page 20-2](#)
- [Configuring STP Extensions, page 20-2](#)
- [Configuring Rapid PVST+, page 20-3](#)
- [Configuring MST, page 20-3](#)
- [Configuring Link-State Tracking, page 20-3](#)
- [Configuring FabricPath Switching, page 20-3](#)
- [FabricPath Forwarding, page 20-4](#)
- [Configuring Advanced FabricPath Features, page 20-4](#)
- [Using the Layer 2 Security Audit Wizard, page 20-4](#)
- [Configuring Dynamic ARP Inspection, page 20-4](#)
- [Configuring Port Security, page 20-5](#)
- [Configuring DHCP Snooping, page 20-6](#)
- [Configuring IP Source Guard, page 20-6](#)
- [Configuring Traffic Storm Control, page 20-7](#)
- [Configuring IGMP Snooping, page 20-7](#)
- [Configuring FCoE Initialization Protocol Snooping, page 20-7](#)

For detailed configuration guide, please refer to Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x.

Configuring VLANs

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure virtual LANs (VLANs) on NX-OS devices.

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.

Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered as a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a bridge or a router.

All ports are assigned to the default VLAN (VLAN1) when the device first comes up. A VLAN interface, or switched virtual interface (SVI), is a Layer 3 interface that is created to provide communication between VLANs.

The devices support 4094 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into several ranges, and you use each range slightly differently. Some of these VLANs are reserved for internal use by the device and are not available for configuration.

**Note**

Inter-Switch Link (ISL) trunking is not supported on the Cisco NX-OS.

Configuring Private VLANs

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure private VLANs. Private VLANs provide additional protection at the Layer 2 level.

Private VLANs provide traffic separation and security at the Layer 2 level.

A private VLAN is one or more pairs of a primary VLAN and a secondary VLAN, all with the same primary VLAN. The two types of secondary VLANs are isolated and community VLANs. Hosts on isolated VLANs communicate only with hosts in the primary VLAN. Hosts in a community VLAN can communicate only among themselves and with hosts in the primary VLAN but not with hosts in isolated VLANs or in other community VLANs.

Regardless of the combination of isolated and community secondary VLANs, all interfaces within the primary VLAN comprise one Layer 2 domain, and therefore, require only one IP subnet.

Configuring STP Extensions

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure Spanning Tree Protocol (STP) extensions on Cisco Nexus 7000 Series NX-OS devices.

The software supports the following Cisco proprietary features:

- *Spanning tree port types—The default spanning tree port type is normal. You can configure interfaces connected to Layer 2 hosts as edge ports and interfaces connected to Layer 2 switches or bridges as network ports.*
- *Bridge Assurance—Once you configure a port as a network port, Bridge Assurance sends BPDUs on all ports and moves a port into the blocking state if it no longer receives BPDUs. This enhancement is available only when you are running Rapid PVST+ or MST.*
- *BPDU Guard—BPDU Guard shuts down the port if that port receives a BPDU.*
- *BPDU Filter—BPDU Filter suppresses sending and receiving BPDUs on the port.*
- *Loop Guard—Loop guard helps prevent bridging loops that could occur because of a unidirectional link failure on a point-to-point link.*
- *Root Guard—The root guard feature prevents a port from becoming root port or blocked port. If a port configured for root guard receives a superior BPDU, the port immediately goes to the root-inconsistent (blocked) state.*

Configuring Rapid PVST+

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Rapid per VLAN Spanning Tree (Rapid PVST+) protocol on NX-OS devices.

Configuring MST

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure Multiple Spanning Tree (MST) on NX-OS devices.

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide*.

Configuring Link-State Tracking

**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 in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure link-state tracking on the Cisco Nexus 4000 Series device.

The link-state tracking feature binds the link state of multiple interfaces and provides redundancy in the network. In link-state tracking, you configure the server network adapters in a primary or secondary relationship known as teaming. The interfaces are grouped into link-state groups and if the link is lost on a primary interface, connectivity transparently moves to the secondary interface.

**Note**

Link-state tracking is applicable only for the Cisco Nexus 4000 Series platform, beginning with the DCNM 4.2(3) release.

Configuring FabricPath Switching

**Note**

You must have an F Series module installed in your Cisco Nexus 7000 Series chassis in order to run FabricPath and conversational learning.

FabricPath switching allows multipath networking at the Layer 2 level. The FabricPath network still delivers packets on a best-effort basis (which is similar to the Classical Ethernet [CE] network), but the FabricPath network can use multiple paths for Layer 2 traffic.

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure FabricPath switching on the Cisco Nexus 7000 Series NX-OS devices.

FabricPath Forwarding

Beginning with Cisco Release 5.1(2) for the Nexus 700 Series devices, you can create additional, nondefault FabricPath topologies. Each additional topology also has two forwarding trees. Additionally, you can display information about the interfaces and reachability status of the FabricPath network.

**Note**

See the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x* for more information on displaying the FabricPath topologies.

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes the forwarding behavior of FabricPath on the Cisco Nexus 7000 Series NX-OS devices.

Configuring Advanced FabricPath Features

You can do advanced configurations using FabricPath for the FabricPath Intermediate System-to-Intermediate System (IS-IS) protocol.

For more information about the Data Center Network Manager features, see the Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x.

Using the Layer 2 Security Audit Wizard

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to use the Layer 2 Security Audit Wizard.

The Security Audit Wizard allows you to examine the existing Layer 2 security features such as port security, dynamic ARP inspection (DAI), DHCP snooping, IP Source Guard, and traffic storm control configured on different devices. It also allows you to report and apply configurations that are missing on the device.

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide*.

Configuring Dynamic ARP Inspection

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure dynamic Address Resolution Protocol (ARP) inspection (DAI) on an NX-OS device.

Dynamic ARP inspection (DAI) ensures that only valid ARP requests and responses are relayed. When DAI is enabled and properly configured, a device performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets

DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the device. It can also contain static entries that you create. If the ARP packet is received on a trusted interface, the device forwards the packet without any checks. On untrusted interfaces, the device forwards the packet only if it is valid.

**Note**

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

**Note**

System-message logging levels for DAI 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide*.

Configuring Port Security

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure port security on NX-OS devices.

You can use port security to configure Layer 2 Ethernet interfaces and Layer 2 port-channel interfaces that allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN. The number of MAC addresses that the device can secure is configurable per interface.

**Note**

The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. 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:

**Note**

System-message logging levels for port security 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

For more information about the Data Center Network Manager features, see the *Cisco DCNM Fundamentals Configuration Guide*.

Configuring DHCP Snooping

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure Dynamic Host Configuration Protocol (DHCP) snooping on an NX-OS device.

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- (Not in 4.0) Rate-limits DHCP traffic from trusted and untrusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

Dynamic ARP inspection (DAI) and IP Source Guard also use information stored in the DHCP snooping binding database.

**Note**

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

**Note**

System-message logging levels for DHCP snooping 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

Configuring IP Source Guard

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure IP Source Guard on NX-OS devices.

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- Entries in the DHCP snooping binding table.
- Static IP source entries that you configure.

Filtering on trusted IP and MAC address bindings helps prevent attacks that rely on spoofing the IP address of a valid host. To circumvent IP Source Guard, an attacker would have to spoof both the IP address and the MAC address of a valid host.

**Note**

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

**Note**

System-message logging levels for IP Source Guard 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

Configuring Traffic Storm Control

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure traffic storm control on the NX-OS device.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming traffic over a 1-second interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

Configuring IGMP Snooping

**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.

**Note**

Cisco recommends that you do not disable IGMP snooping on the device. If you disable IGMP snooping, you may see reduced multicast performance because of excessive false flooding within the device.

The Internet Group Management Protocol (IGMP) snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the device.

Configuring FCoE Initialization Protocol Snooping

The Fiber Channel over Ethernet (FCoE) Initialization Protocol (FIP) is a Layer 2 protocol for end point discovery and fabric association. FIP has its own EtherType and uses its own frame formats.

FIP has two phases: discovery and login. Once the discovery of end nodes and login is complete, FCoE traffic can start flowing between the endpoints.

By snooping on FIP packets during the discovery and login phases, intermediary bridges can implement dynamic data integrity mechanisms using access control lists (ACLs) that permit only valid FCoE traffic between the ENode and the FCoE forwarder (FCF).

A bridge implementing the above functionality is what we refer to as the FIP Snooping Bridge. The process implementing this feature is called FIP Snooping Manager (FIPSM). FIPSM is capable of supporting both Fabric Provided MAC Addresses (FPMAs) and Server Provided MAC Addresses (SPMAs).

This chapter in Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Fibre Channel over Ethernet (FCoE) Initialization Protocol (FIP) snooping feature using the Cisco Data Center Network Manager (DCNM)



CHAPTER 21

Configuring Routing on DCNM-LAN Client

The Cisco Data Center Network Manager (DCNM) supports IP addressing, object tracking, and Gateway Load Balancing Protocol (GLBP).

This chapter includes following sections:

- [Configuring GLBP, page 21-1](#)
- [Configuring HSRP, page 21-1](#)
- [Configuring Keychain Management, page 21-2](#)
- [Configuring Object Tracking, page 21-2](#)

For more information about the Data Center Network Manager features, see the *Unicast Routing Configuration Guide, Cisco DCNM for LAN, Release 7.x*.

Configuring GLBP

This chapter in *Unicast Routing Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure the Gateway Load Balancing Protocol (GLBP) on the Cisco Data Center Network Manager (DCNM)NX-OS device.

This chapter includes the following sections:

GLBP provides path redundancy for IP by sharing protocol and Media Access Control (MAC) addresses between redundant gateways. Additionally, GLBP allows a group of Layer 3 routers to share the load of the default gateway on a LAN. A GLBP router can automatically assume the forwarding function of another router in the group if the other router fails.

Configuring HSRP

This chapter in *Unicast Routing Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure the Hot Standby Router Protocol (*HSRP*) on the Cisco Data Center Network Manager (DCNM)NX-OS device.

This chapter includes the following sections:

HSRP is a first-hop redundancy protocol (*FHRP*) that allows a transparent failover of the first-hop IP router. HSRP provides first-hop routing redundancy for IP hosts on Ethernet networks configured with a default router IP address. You use HSRP in a group of routers for selecting an active router and a standby router. In a group of routers, the active router is the router that routes packets; the standby router is the router that takes over when the active router fails or when preset conditions are met.

Many host implementations do not support any dynamic router discovery mechanisms but can be configured with a default router. Running a dynamic router discovery mechanism on every host is not feasible for a number of reasons, including administrative overhead, processing overhead, and security issues. HSRP provides failover services to these hosts.

Configuring Keychain Management

This chapter in *Unicast Routing Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure keychain management on an NX-OS device.

Keychain management allows you to create and maintain keychains, which are sequences of keys (sometimes called shared secrets). You can use keychains with features that secure communications with other devices by using key-based authentication. The device allows you to configure multiple keychains.

Some routing protocols that support key-based authentication can use a keychain to implement a hitless key rollover for authentication.

**Note**

The Cisco NX-OS release that is running on a managed device may not support all the features or settings described in this section. 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:

Configuring Object Tracking

This chapter in *Unicast Routing Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure object tracking on the Cisco NX-OS Cisco NX-OS device.

This chapter includes the following sections:

Object tracking allows you to track specific objects on the device, such as the interface line protocol state, IP routing, and route reachability, and to take action when the tracked object's state changes. This feature allows you to increase the availability of the network and shorten recovery time if an object state goes down.

System-message logging levels for the Object Tracking 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.



CHAPTER 22

Security Configurations on DCNM-LAN Client

The Cisco NX-OS software supports security features that can protect your network against degradation or failure and also against data loss or compromise resulting from intentional attacks and from unintended but damaging mistakes by well-meaning network users.

This chapter includes the following sections:

- [Configuring IP ACLs, page 22-1](#)
- [Configuring MAC ACLs, page 22-2](#)
- [Configuring VLAN ACLs, page 22-2](#)
- [Configuring ARP ACLs, page 22-2](#)
- [Configuring Object Groups, page 22-3](#)
- [Configuring AAA, page 22-3](#)
- [Configuring Time Ranges, page 22-3](#)
- [Configuring RADIUS, page 22-3](#)
- [Configuring TACACS+, page 22-4](#)
- [Configuring 802.1X, page 22-4](#)
- [Configuring User Accounts and RBAC, page 22-5](#)

For detailed information about the security configuration on DCNM-LAN client, see Security Configuration Guide, Cisco DCNM for LAN, Release 7.x.

Configuring IP ACLs

You can configure an IP ACL on the device. An IP ACL is an ordered set of rules that you can use to filter traffic based on IPv4 or IPv6 information in the Layer 3 header of packets. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When a device determines that an IP ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied.

Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 ACLs.

**Note**

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

Configuring MAC ACLs

You can configure a MAC ACL on the device. MAC ACLs are ACLs that filter traffic using the information in the Layer 2 header of each packet. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When a device determines that a MAC ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied.

**Note**

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

Configuring VLAN ACLs

A VLAN ACL (VACL) is one application of a MAC ACL or IP ACL. You can configure VACLs to apply to all packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. VACLs are not defined by direction (ingress or egress).

**Note**

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

Configuring ARP ACLs

You can configure an ARP ACL on the device. An ARP ACL is an ordered set of rules that you can use to filter ARP traffic for dynamic ARP inspection (DAI). Each rule specifies a set of conditions that a packet must satisfy to match the rule. When a device determines that an ARP ACL applies to an ARP packet, it tests the packet against the conditions of all rules. The first match determines whether a packet is permitted or denied, or if there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied.

When you configure the device to apply an ARP ACL to traffic, the ACL take precedence over entries in the DHCP snooping binding database. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Configuring Object Groups

An object group is a group of IP addresses or a group of TCP or UDP ports. When you create an access control list (ACL) rule, you can specify the object groups rather than specifying IP addresses or ports. Using object groups when you configure IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you need to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object, you can add an IP address to the object instead of changing all three rules.

Configuring AAA

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure authentication, authorization, and accounting (AAA) on Cisco NX-OS devices.

You can configure authentication, authorization, and accounting (AAA) network security services to provide the primary framework through which you set up access control on your router or access server. Based on the user ID and password combination that you provide, the Cisco NX-OS device performs local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers.



Note

System-message logging levels for AAA 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

Configuring Time Ranges

You can use time ranges to control when an ACL rule is in effect. For example, if the device determines that a particular ACL applies to traffic arriving on an interface, if a rule in the ACL uses a time range that is not in effect, the device does not compare the traffic to that rule.

IPv4, IPv6, and MAC ACLs support time ranges. When the device applies an ACL to traffic, the rules that are in effect are as follows:

- All rules that are not configured with a time range.
- Rules that are configured with a time range which is active at the second that the device applies the ACL to traffic.

The device supports named, reusable time ranges. This allows you to configure a time range once and specify it by name when configure many ACL rules.

Configuring RADIUS

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Remote Access Dial-In User Service (RADIUS) protocol on NX-OS devices.

You can configure RADIUS on a device. The RADIUS distributed client/server system allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco NX-OS devices and send authentication and accounting requests to a central RADIUS server that contains all user authentication and network service access information.

**Note**

System-message logging levels for RADIUS 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

Configuring TACACS+

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on Cisco NX-OS devices.

You can use TACACS+ to provide centralized validation of users attempting to gain access to a device. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your device are available.

**Note**

System-message logging levels for TACACS+ 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

Configuring 802.1X

This chapter in Security Configuration Guide, Cisco DCNM for LAN, Release 7.x describes how to configure IEEE 802.1X port-based authentication on Cisco NX-OS devices.

802.1X defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a device port.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

**Note**

System-message logging levels for 802.1X 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.

Configuring User Accounts and RBAC

This chapter in *Security Configuration Guide, Cisco DCNM for LAN, Release 7.x* describes how to configure user accounts and role-based access control (RBAC) on NX-OS devices.

You can create and manage users accounts and assign roles that limit access to operations on the NX-OS device. Role-based access control (RBAC) allows you to define the rules for an assign role that restrict the authorization that the user must have to access management operations.



CHAPTER 23

Working with Configuration Change Management

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

The Configuration Change Management feature allows you to keep an archive of configurations from managed devices. You can view and compare configurations. You can roll back the configuration on a managed device to any archived configuration that Cisco DCNM has for the device.

This chapter includes the following sections:

- [Information About Configuration Change Management, page 23-1](#)
- [Licensing Requirements for Configuration Change Management, page 23-5](#)
- [Prerequisites, page 23-5](#)
- [Guidelines and Limitations for Configuration Change Management, page 23-6](#)
- [Platform Support, page 23-6](#)
- [Working with the Version Browser, page 23-6](#)
- [Configuring Archival Jobs, page 23-18](#)
- [Configuring Archival Settings, page 23-22](#)
- [Configuring Switch Profiles, page 23-23](#)
- [Field Descriptions for Configuration Change Management, page 23-27](#)
- [Additional References, page 23-32](#)
- [Feature History for Configuration Change Management, page 23-32](#)

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.

**Note**

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

This section includes the following topics:

- [Version Browser, page 23-2](#)
- [Archival Jobs, page 23-2](#)
- [Archival Settings, page 23-2](#)
- [VDC Support, page 23-5](#)

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.

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.

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.

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 7.1.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.

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 23-6](#).

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 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
Cisco Catalyst 6500 Series switches	Cisco Catalyst 6500 Series Switches Documentation

Working with the Version Browser

The version browser allows you to see information about archived configurations, view and compare specific configuration versions, merge changes from one configuration version to another, and roll back the running configuration on a managed device to a configuration version that you specify.

This section includes the following topics:

- [Viewing the Archival Status of a Device, page 23-7](#)
- [Viewing the Archival History of a Device, page 23-8](#)
- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Using Copy Run to Start, page 23-9](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Viewing an Archived Configuration Version, page 23-10](#)

- [Comparing Configuration Versions, page 23-11](#)
- [Using the Version Comparison Tools, page 23-13](#)
- [Merging Configuration Differences, page 23-14](#)
- [Performing a Configuration Rollback, page 23-15](#)
- [Viewing the Rollback History of a Device, page 23-16](#)
- [Deleting All Archived Configurations for a Device, page 23-17](#)

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 23-21. |
-

RELATED TOPICS

- [Viewing the Archival History of a Device, page 23-8](#)
- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Viewing an Archived Configuration Version, page 23-10](#)

Viewing the Archival History of a Device

You can view the archival history of a device. The archival history records each attempt to create a new archival configuration version from the current running configuration of a device.

BEFORE YOU BEGIN

A managed device must be on the list of Cisco DCNM-licensed devices before you can use it with Configuration Change Management. Only licensed devices appear in the Version Browser.

DETAILED STEPS

-
- 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.
-

RELATED TOPICS

- [Viewing the Archival Status of a Device, page 23-7](#)
- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Viewing an Archived Configuration Version, page 23-10](#)

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.
-

RELATED TOPICS

- [Configuring Version and History Settings, page 23-22](#)
- [Viewing the Archival Status of a Device, page 23-7](#)
- [Viewing the Archival History of a Device, page 23-8](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Viewing an Archived Configuration Version, page 23-10](#)
- [Comparing Configuration Versions, page 23-11](#)
- [Deleting All Archived Configurations for a Device, page 23-17](#)

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**.

RELATED TOPICS

- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Viewing an Archived Configuration Version, page 23-10](#)
- [Comparing Configuration Versions, page 23-11](#)
- [Deleting All Archived Configurations for a Device, page 23-17](#)

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**.

RELATED TOPICS

- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Comparing Configuration Versions, page 23-11](#)
- [Deleting All Archived Configurations for a Device, page 23-17](#)

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.
- 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 23-1](#) to compare the selected version to the configuration version that you want.

Table 23-1 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 .
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. <p>In the Details pane, the Compare tab shows the selected configuration version in the left configuration pane.</p> <ol style="list-style-type: none"> 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. <p>The right configuration pane displays the configuration version that you specified.</p>

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 23-13](#).

RELATED TOPICS

- [Viewing an Archived Configuration Version, page 23-10](#)
- [Using the Version Comparison Tools, page 23-13](#)
- [Merging Configuration Differences, page 23-14](#)

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 23-11](#).

Use the options described [Table 23-1](#) to compare two configuration versions.

Table 23-2 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.
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. A bookmark icon appears beside the line number.
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. The configurations in both panes jump to the next bookmarked line.
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. The configurations in both panes jump to the previous bookmarked line.

Option Icon and Name	How to Use the Option
 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 23-14.</p>
 Save As	<p>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.</p>

RELATED TOPICS

- [Viewing an Archived Configuration Version, page 23-10](#)
- [Comparing Configuration Versions, page 23-11](#)
- [Merging Configuration Differences, page 23-14](#)

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.

RELATED TOPICS

- [Viewing an Archived Configuration Version, page 23-10](#)
- [Comparing Configuration Versions, page 23-11](#)
- [Using the Version Comparison Tools, page 23-13](#)

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.

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.

RELATED TOPICS

- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Viewing an Archived Configuration Version, page 23-10](#)
- [Comparing Configuration Versions, page 23-11](#)
- [Viewing the Rollback History of a Device, page 23-16](#)

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.

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.
-

RELATED TOPICS

- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Viewing an Archived Configuration Version, page 23-10](#)
- [Comparing Configuration Versions, page 23-11](#)
- [Performing a Configuration Rollback, page 23-15](#)

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.

RELATED TOPICS

- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Archiving the Current Running Configuration of a Device, page 23-9](#)
- [Viewing an Archived Configuration Version, page 23-10](#)
- [Comparing Configuration Versions, page 23-11](#)

Configuring Archival Jobs

The Archival Jobs feature allows you to control the automated archival of the running configuration on managed devices.

This section includes the following topics:

- [Configuring an Archival Job, page 23-18](#)
- [Enabling and Disabling an Archival Job, page 23-20](#)
- [Deleting an Archival Job, page 23-20](#)
- [Viewing Details of an Archival Job, page 23-21](#)
- [Viewing the History of an Archival Job, page 23-21](#)

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:
- Click the **Archive at Specified Time** radio button.
 - In the row of Days check boxes, check the check box for each day that you want the archival job to be active.
 - 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:
- Under Device, right-click in a blank area and choose **Add New Device**.
A dialog box shows available and selected devices.
 - 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**.
-
- 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:
- Under Devices, click the device that you want to remove from the job.
 - 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.
-

RELATED TOPICS

- [Enabling and Disabling an Archival Job, page 23-20](#)
- [Deleting an Archival Job, page 23-20](#)
- [Viewing Details of an Archival Job, page 23-21](#)
- [Viewing the History of an Archival Job, page 23-21](#)

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.

RELATED TOPICS

- [Configuring an Archival Job, page 23-18](#)
- [Deleting an Archival Job, page 23-20](#)
- [Viewing Details of an Archival Job, page 23-21](#)
- [Viewing the History of an Archival Job, page 23-21](#)

Deleting an Archival Job

You can delete an archival job but not the Default archival job. When you delete an archival job, any devices included in the deleted job are automatically added to the Default archival job.

BEFORE YOU BEGIN

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

DETAILED STEPS

-
- 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.

RELATED TOPICS

- [Configuring an Archival Job, page 23-18](#)
- [Enabling and Disabling an Archival Job, page 23-20](#)
- [Viewing Details of an Archival Job, page 23-21](#)
- [Viewing the History of an Archival Job, page 23-21](#)

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. |
-

RELATED TOPICS

- [Configuring an Archival Job, page 23-18](#)
- [Enabling and Disabling an Archival Job, page 23-20](#)
- [Deleting an Archival Job, page 23-20](#)
- [Viewing the History of an Archival Job, page 23-21](#)

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.

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.

RELATED TOPICS

- [Configuring an Archival Job, page 23-18](#)
- [Enabling and Disabling an Archival Job, page 23-20](#)
- [Deleting an Archival Job, page 23-20](#)
- [Viewing Details of an Archival Job, page 23-21](#)

Configuring 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.

This section includes the following topics:

- [Configuring Version and History Settings, page 23-22](#)
- [Configuring the Rollback File Server Setting, page 23-23](#)

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.
-

RELATED TOPICS

- [Browsing and Commenting on Configuration Versions, page 23-8](#)
- [Configuring the Rollback File Server Setting, page 23-23](#)

Configuring the Rollback File Server Setting

You can configure whether Cisco DCNM uses a specific file server during a configuration rollback or whether it uses any available file server that you have configured.

BEFORE YOU BEGIN

You must configure at least one file server in Cisco DCNM. For more information, see the [“Adding a File Server”](#) section on page 24-15.

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:
- 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 23-24](#)
- [Configuring the Switch Profile Wizard Between Two vPCs, page 23-24](#)
- [Configuring the Switch Profile Wizard Between Two Switches, page 23-25](#)
- [Configuring the Sync Network View, page 23-25](#)
- [Configuring the Switch Profile Migration Wizard for Dual Homed FEXes, page 23-26](#)

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**. 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.

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.
- 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 FEXes



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 FEXes that are present in the primary vPC switch is displayed in the Migration wizard.

**Note**

If the FEXes are online, they are automatically selected for the host interfaces (HIF) import. Any pre-provisioned FEXes 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.

RELATED TOPICS

- [Performing a Configuration Rollback, page 23-15](#)
- [Configuring Version and History Settings, page 23-22](#)

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 23-27](#)
- [Field Descriptions for Archival Jobs, page 23-29](#)
- [Field Descriptions for the Archival Settings Contents Pane, page 23-31](#)
- [Field Descriptions for the Switch Profiles Pane, page 23-31](#)
- [Field Descriptions for the Switch Profiles Network View Pane, page 23-31](#)

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 23-28](#)
- [Device: Details: Rollback History Section, page 23-28](#)
- [Device: Details: Archival History Section, page 23-28](#)
- [Version: Version Details Tab, page 23-28](#)
- [Version: Compare Tab, page 23-29](#)

Device: Details: Archival Status Section

Table 23-3 *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 23-4 *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.

Device: Details: Archival History Section

Table 23-5 *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 23-6 *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.

Table 23-6 **Version: Version Details Tab (continued)**

Field	Description
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 23-7 **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.

Field Descriptions for Archival Jobs

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

- [Archival Job: Details Tab, page 23-29](#)
- [Archival Job: Archival History Tab, page 23-30](#)

Archival Job: Details Tab

Table 23-8 **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.

Table 23-8 **Archival Job: Details Tab (continued)**

Field	Description
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 23-9 **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.
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 23-10 *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 23-11 *Switch Profiles Pane*

Table 0-1

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.
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 23-12 *Switch Profiles Network View Pane*

Table 0-2

Field	Description
vPC	Hostname of the vPC primary and secondary switch.
Name	Name of the switch profile.

Table 0-2

Field	Description
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 23-32](#)
- [Standards, page 23-32](#)

Related Documents

Related Topic	Document Title
File servers in Cisco DCNM	<i>File Servers, page 24-3</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.	—

Feature History for Configuration Change Management

[Table 23-13](#) lists the release history for this feature.

Table 23-13 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).

Table 23-13 *Feature History for Configuration Change Management (continued)*

Feature Name	Releases	Feature Information
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 24

Managing Device Operating Systems

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

The Device OS Management feature allows you to control the operating system installed on Nexus 7000 Series devices that are managed by DCNM. You can create software installation jobs that affect one or more managed devices. DCNM can transfer the software images of operating systems to managed devices using one of several supported protocols. Installation jobs can also use software images already present on managed devices.

This chapter includes the following sections:

- [Information About Device OS Management, page 24-1](#)
- [Licensing Requirements for Device OS Management, page 24-3](#)
- [Prerequisites, page 24-4](#)
- [Guidelines and Limitations for Device OS Management, page 24-4](#)
- [Platform Support, page 24-4](#)
- [Using the Device OS Management Window, page 24-5](#)
- [Configuring Software Installation Jobs, page 24-7](#)
- [Configuring File Servers, page 24-15](#)
- [Field Descriptions for Device OS Management, page 24-18](#)
- [Additional References, page 24-20](#)
- [Feature History for Device OS Management, page 24-21](#)

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 24-2](#)
- [Software Installation Jobs, page 24-2](#)
- [File Servers, page 24-3](#)
- [VDC Support, page 24-3](#)

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 24-3](#).

- **URL**—You can use a URL to specify the image files. The verification that Cisco DCNM performs for a URL varies depending upon the transfer protocol that you use, as follows:
 - **FTP**—Cisco DCNM verifies the URL format, that the FTP server in the URL is reachable, and that the specified image file exists on the FTP server. The FTP URL format is as follows:
`ftp://username@servername/path/filename`
 - **SFTP**—Cisco DCNM verifies the URL format, that the SFTP server in the URL is reachable, and that the image file specified exists on the SFTP server. The SFTP URL format is as follows:
`sftp://username@servername/path/filename`
 - **TFTP**—You must ensure that the path and image filename are correct. Cisco DCNM verifies the URL format and that the TFTP server in the URL is reachable. The TFTP URL format is as follows:
`tftp://servername/path/filename`
 - **SCP**—You must ensure that the SCP server is reachable and that the path and image filename are correct. Cisco DCNM verifies the URL format. The SCP URL format is as follows:
`scp://username@servername/path/filename`

The Software Installation wizard includes an optional step for verifying the version compatibility of software images with the managed devices. During this step, if a software image was specified by a URL or file server, Cisco DCNM instructs managed devices to copy the software image from the URL or file server to the bootflash file system on the device. If you skip the version compatibility step, Cisco DCNM does not instruct devices to copy software images from URLs or file servers until the installation job begins.

File Servers

The File Servers feature allows you to configure 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 7.1.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.

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 7000 Series switches	Cisco Nexus 7000 Series Switch Documentation

Using the Device OS Management Window

The Device OS Management window 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.


This section includes the following topics:

- [Viewing Device Image Details, page 24-5](#)
- [Installing Software on a Device, page 24-5](#)

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 24-7](#).
-

RELATED TOPICS

- [Installing Software on a Device, page 24-5](#)

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 24-2](#). The supported options are the following:

- **File server**—If you want to use a file server, ensure that the software images are available on the server. You must also configure the file server in DCNM. For more information, see the [“Adding a File Server” section on page 24-15](#).
- **Device file system**—If you want to 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.

- **URL**—If you want to use a URL to specify the image files, what DCNM verifies for you and what you need to ensure vary depending upon the transfer protocol that you use, as follows:
 - **FTP**—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**—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. 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. DCNM verifies the URL format. The SCP URL format is as follows:
`scp://username@servername/path/filename`

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 24-9 . |
-

RELATED TOPICS

- [Viewing Device Image Details, page 24-5](#)

- [Using the Software Installation Wizard, page 24-9](#)
- [Adding a File Server, page 24-15](#)

Configuring Software Installation Jobs

The Software Installation Jobs feature allows you to create and monitor software installation jobs.

This section includes the following topics:

- [Viewing Software Installation Job Details, page 24-7](#)
- [Creating or Editing a Software Installation Job, page 24-8](#)
- [Using the Software Installation Wizard, page 24-9](#)
- [Rescheduling a Software Installation Job, page 24-12](#)
- [Deleting a Software Installation Job, page 24-13](#)
- [Adding or Changing Comments for a Software Installation Job, page 24-13](#)
- [Changing Installation Options for a Software Installation Job, page 24-14](#)

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.

**Tip**

To expand or collapse the General or the Device and Software Images sections, double-click the section title.

RELATED TOPICS

- [Viewing Device Image Details, page 24-5](#)
- [Creating or Editing a Software Installation Job, page 24-8](#)

- [Rescheduling a Software Installation Job, page 24-12](#)
- [Deleting a Software Installation Job, page 24-13](#)
- [Adding or Changing Comments for a Software Installation Job, page 24-13](#)
- [Changing Installation Options for a Software Installation Job, page 24-14](#)

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 24-2](#). The supported options are the following:

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.

- **File server**—If you want to use a file server, ensure that the software images are available on the server. You must also configure the file server in DCNM. For more information, see the [“Adding a File Server” section on page 24-15](#).
- **Device file system**—If you want to 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.

- **URL**—If you want to use a URL to specify the image files, what DCNM verifies for you and what you need to ensure vary depending upon the transfer protocol that you use, as follows:
 - **FTP**—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**—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. 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. DCNM verifies the URL format. The SCP URL format is as follows:

scp://username@servername/path/filename

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 24-9.
-

RELATED TOPICS

- [Using the Software Installation Wizard, page 24-9](#)
- [Rescheduling a Software Installation Job, page 24-12](#)
- [Deleting a Software Installation Job, page 24-13](#)
- [Adding or Changing Comments for a Software Installation Job, page 24-13](#)
- [Changing Installation Options for a Software Installation Job, page 24-14](#)
- [Adding a File Server, page 24-15](#)

Using the Software Installation Wizard

You can use the Software Installation wizard to configure a new software installation job or make changes to an existing software installation job.

BEFORE YOU BEGIN

Start the Software Installation wizard, from one of the following places:

- Device OS Management—See the [“Installing Software on a Device”](#) section on page 24-5.
- Software Installation Jobs—See the [“Creating or Editing a Software Installation Job”](#) section on page 24-8.

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:
- a. Under Available Switches, click the device.
 - b. Click **Add**.

**Tip**

To remove a device from the job, under Selected Switches, click the device and then click **Remove**.

Step 2 Click **Next**.

The Software Installation wizard dialog box displays the Specify Software Images step. Devices are categorized by the physical device type. You can specify software images for each device individually or for an entire category of devices of the same physical type.

Step 3 For each device or physical device category, specify a kickstart image and a system image. To do so, follow these steps once for the Kickstart Image field and again for the System Image field:

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

The Software Image Browser dialog box appears.

- b. Specify the location of the file for the software image to be installed. To do so, choose one of the following options:

- **File Server**—If you choose this option, you must pick a file server from the Repository list, navigate 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.

- c. 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.**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.

- 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.

RELATED TOPICS

- [Installing Software on a Device, page 24-5](#)
- [Creating or Editing a Software Installation Job, page 24-8](#)
- [Rescheduling a Software Installation Job, page 24-12](#)
- [Deleting a Software Installation Job, page 24-13](#)
- [Adding or Changing Comments for a Software Installation Job, page 24-13](#)
- [Changing Installation Options for a Software Installation Job, page 24-14](#)

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.
-

RELATED TOPICS

- [Viewing Software Installation Job Details, page 24-7](#)
- [Creating or Editing a Software Installation Job, page 24-8](#)
- [Rescheduling a Software Installation Job, page 24-12](#)
- [Deleting a Software Installation Job, page 24-13](#)

- [Adding or Changing Comments for a Software Installation Job, page 24-13](#)
- [Changing Installation Options for a Software Installation Job, page 24-14](#)

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. |
-

RELATED TOPICS

- [Viewing Software Installation Job Details, page 24-7](#)
- [Creating or Editing a Software Installation Job, page 24-8](#)
- [Rescheduling a Software Installation Job, page 24-12](#)
- [Adding or Changing Comments for a Software Installation Job, page 24-13](#)
- [Changing Installation Options for a Software Installation Job, page 24-14](#)

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.
-

RELATED TOPICS

- [Viewing Software Installation Job Details, page 24-7](#)
- [Creating or Editing a Software Installation Job, page 24-8](#)
- [Rescheduling a Software Installation Job, page 24-12](#)
- [Deleting a Software Installation Job, page 24-13](#)
- [Changing Installation Options for a Software Installation Job, page 24-14](#)

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**.
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.
-

RELATED TOPICS

- [Viewing Software Installation Job Details, page 24-7](#)

- [Creating or Editing a Software Installation Job, page 24-8](#)
- [Rescheduling a Software Installation Job, page 24-12](#)
- [Deleting a Software Installation Job, page 24-13](#)
- [Adding or Changing Comments for a Software Installation Job, page 24-13](#)

Configuring File Servers

The File Servers feature allows you to configure file servers, which you can use for the following purposes:

- Software installation jobs—DCNM can get software image files from a file server and transfer them to devices included in a software installation job.
- Configuration rollbacks—DCNM can back up device configurations to a file server when you roll back a device configuration.

This section includes the following topics:

- [Adding a File Server, page 24-15](#)
- [Changing a File Server, page 24-16](#)
- [Deleting a File Server, page 24-17](#)

Adding a File Server

You can add a file server to Cisco DCNM.

BEFORE YOU BEGIN

Gather the following information about the file server:

- Server IP address or hostname

**Note**

If you use the hostname, it must be registered with the DNS server that the Cisco DCNM server is configured to use.

- Transfer protocol that the server provides. Cisco DCNM supports the following transfer protocols:
 - FTP
 - SFTP
 - TFTP
- Username and password that Cisco DCNM should use to access the server.
- The base directory on the server. All files and directories that Cisco DCNM needs to access must be available under this directory.

DETAILED STEPS

- 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.
-

RELATED TOPICS

- [Changing a File Server, page 24-16](#)
- [Deleting a File Server, page 24-17](#)

Changing a File Server

You can change the user credentials, base directory, and comments of a file server.



Note

You cannot change the values in the Server Name/IP Address or Protocol fields. If you need to change these values, delete the file server and create a file server with the new values.

BEFORE YOU BEGIN

If you are changing the user credentials or base directory, determine what the new user credentials or base directory should be.

DETAILED STEPS

- 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.

RELATED TOPICS

- [Adding a File Server, page 24-15](#)
- [Deleting a File Server, page 24-17](#)

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 23-23](#).

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 23-23](#).

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

RELATED TOPICS

- [Adding a File Server, page 24-15](#)
- [Changing a File Server, page 24-16](#)

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 24-18](#)
- [Field Descriptions for Software Installation Jobs, page 24-19](#)
- [Field Descriptions for the File Servers Contents Pane, page 24-20](#)

Field Descriptions for Device OS Management

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

- [Device: Details: System Section, page 24-18](#)
- [Device: Details: Software Installation Jobs Section, page 24-18](#)

Device: Details: System Section

Table 24-1 **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 24-2 **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.

Table 24-2 **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 24-19](#)
- [Installation Job: Details: Devices and Software Images Section, page 24-20](#)

Installation Job: Details: General Section

Table 24-3 **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.

Installation Job: Details: Devices and Software Images Section

Table 24-4 *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 24-5 *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 24-21](#)
- [Standards, page 24-21](#)

Related Documents

Related Topic	Document Title
Upgrading and downgrading Cisco NX-OS software using the command-line interface on 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 24-6](#) lists the release history for this feature.

Table 24-6 Feature History for Device OS Management

Feature Name	Releases	Feature Information
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 25

Starting and Stopping Cisco DCNM-LAN Servers

This chapter describes how to start or stop Cisco Data Center Network Manager for LAN (DCNM-LAN) servers.

This chapter includes the following sections:

- [Information About Starting and Stopping DCNM-LAN Servers, page 25-1](#)
- [Licensing Requirements for Starting and Stopping Cisco DCNM-LAN Servers, page 25-1](#)
- [Starting DCNM-LAN Servers, page 25-2](#)
- [Stopping DCNM-LAN Servers, page 25-5](#)
- [Related Documents, page 25-8](#)
- [Feature History for Starting and Stopping a DCNM-LAN Server, page 25-9](#)

Information About Starting and Stopping DCNM-LAN Servers

Starting and stopping DCNM-LAN servers is a necessary part of server maintenance, such as during database backup, cleaning, or restoration. In a clustered server deployment, the order in which you start DCNM-LAN servers determines which server is the master server. This chapter provides detailed steps for starting and stopping DCNM-LAN servers for both single-server deployments and clustered-server deployments.

Licensing Requirements for Starting and Stopping Cisco DCNM-LAN Servers

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM-LAN	Starting and stopping Cisco DCNM-LAN servers requires no license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN 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 7.1.x</i> .

Starting DCNM-LAN Servers

This section includes the following topics:

- [Starting a Single DCNM-LAN Server, page 25-2](#)
- [Starting a Cluster of DCNM-LAN Servers, page 25-3](#)

Starting a Single DCNM-LAN Server

You can start a single DCNM-LAN server. The procedures for starting a single DCNM-LAN server differ for systems using the supported Microsoft Windows Server and Red Hat Enterprise Linux (RHEL) operating systems, as described in the following topics:

- [Starting a Single DCNM-LAN Server \(Microsoft Windows Server\), page 25-2](#)
- [Starting a Single DCNM-LAN Server \(RHEL\), page 25-2](#)

Starting a Single DCNM-LAN Server (Microsoft Windows Server)

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

BEFORE YOU BEGIN

You must have installed the DCNM-LAN server.

If you are starting a server cluster, ensure that you are starting the server in the correct order. For more information, see the [“Starting a Cluster of DCNM-LAN Servers” section on page 25-3](#).

DETAILED STEPS

Step 1 Open the Control Panel window and choose **Administrative Tools > Services**.

The Services window opens.

Step 2 Right-click **Cisco DCNM Server** and choose **Start**.



Note Alternatively, you can choose **Start > All Programs > Cisco DCNM Server > Start DCNM Server**; however, the location of shortcuts depends upon the choices you made when you installed the DCNM-LAN server.

A splash screen opens while the DCNM-LAN server starts. This screen closes once the DCNM-LAN server is running.

Starting a Single DCNM-LAN Server (RHEL)

On a server system that runs RHEL, you can start a DCNM-LAN server with the Start_DCNM_LAN_Server script. The script is located in your home folder or the folder that was specified when setting up the link folder during the installation of Cisco DCNM-LAN.

**Note**

Start_DCNM_LAN_Server launches /usr/local/Cisco/dcm/dcnm/bin/startdcnm.sh.

BEFORE YOU BEGIN

The DCNM-LAN server must be installed.

If you are starting a server cluster, ensure that you are starting the server in the correct order. For more information, see the [“Starting a Cluster of DCNM-LAN Servers” section on page 25-3](#).

DETAILED STEPS

-
- Step 1** Use the **Start_DCNM_LAN_Server** script to start the server on a RHEL operating system.
- The DCNM-LAN server opens a server console window and displays the processes it runs to start the server. The server is running when you see a “Started in Xm:XXs:XXXms” message.
-

Starting a Cluster of DCNM-LAN Servers

Depending on the operating system of the secondary server, the DCNM-LAN server can be started using the Windows GUI, the CLI, or the DCNM Install Manager tool. You can use the CLI or the DCNM Install Manager tool for a secondary server running RHEL. For a secondary server running Microsoft Windows, the DCNM-LAN server is started with the Windows GUI.

Starting with Windows GUI or RHEL CLI

Starting a cluster of DCNM-LAN servers requires starting each server individually; however, the order of server startup is important. The server with the oldest start time performs the master server role in the server cluster.

BEFORE YOU BEGIN

We recommend that you use the primary installation server as the master server. For information about deploying a clustered-server environment, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

If any server in the cluster is running, stop it prior to starting the cluster. The only way that you can control which server is the master server is by ensuring that the master server is started before the other servers start. For more information, see the [“Stopping DCNM-LAN Servers” section on page 25-5](#).

DETAILED STEPS

-
- Step 1** Start the server that you want to be the master server of the cluster. To do so, follow the steps for starting a single DCNM-LAN server for the applicable operating system:
- [Starting a Single DCNM-LAN Server \(Microsoft Windows Server\), page 25-2](#)
 - [Starting a Single DCNM-LAN Server \(RHEL\), page 25-2](#)
- Step 2** Wait for the master server to finish starting.

- Step 3** One at a time, start the other servers in the cluster. After starting a server, wait at least one minute before starting the next server. This delay helps ensure faster stabilization of the server cluster.

For each server, follow the steps for starting a single DCNM-LAN server for the applicable operating system:

- [Starting a Single DCNM-LAN Server \(Microsoft Windows Server\), page 25-2](#)
- [Starting a Single DCNM-LAN Server \(RHEL\), page 25-2](#)

Starting with Install Manager

DCNM Install Manager is a GUI tool for servers that run Linux. It is designed to assist in performing silent mode operations on secondary servers (remote nodes).



Note

DCNM Install Manager does not support Windows servers.

DETAILED STEPS

- Step 1** To access Install Manager, navigate to the `dcnm-install-manager.sh` file that is located in the bin folder where the DCNM-LAN server was installed.

The default bin folder location for servers running Linux is `/usr/local/Cisco/dcm/dcnm/bin`.

- Step 2** Double click the **dcnm-install-manager.sh** file to launch Install Manager.

- Step 3** In the tool bar, click the **New** icon near the top of the Install Manager GUI for every secondary server. A new row in the list of Server Nodes is created every time the New icon is clicked.



Note

In the toolbar, click the **Delete** icon to delete a selected row in the list of Server Nodes. This step does not delete a secondary server from the clustered-server environment.

- Step 4** For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

The protocol is either Telnet or SSH.

- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

Alternatively, default user credentials may be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.

- (Optional) Comments that may be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the “+” icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

- Step 5** In the list of Server Nodes, select the secondary servers to start.
- Step 6** In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers. Correct any connectivity issues before continuing.
- Step 7** In the toolbar, click the **Start** icon to start the selected secondary servers.

**Note**

The Install Manager is a standalone application. The settings specified are not saved and are not persistent. The settings are lost when the Install Manager GUI is closed.

Stopping DCNM-LAN Servers

This section includes the following topics:

- [Stopping Single DCNM-LAN Servers, page 25-5](#)
- [Stopping a Cluster of DCNM-LAN Servers, page 25-6](#)

Stopping Single DCNM-LAN Servers

You can stop a single DCNM-LAN server.

The steps for stopping a single DCNM-LAN server differ for systems using the supported Microsoft Windows Server and RHEL operating systems, as described in the following topics:

- [Stopping a Single DCNM-LAN Server \(Microsoft Windows Server\), page 25-5](#)
- [Stopping a Single DCNM-LAN Server \(RHEL\), page 25-6](#)

Stopping a Single DCNM-LAN Server (Microsoft Windows Server)

On a server system that runs Microsoft Windows Server, you can stop a DCNM-LAN server through the Windows services or by clicking the Stop DCNM Server icon.

DETAILED STEPS

- Step 1** Open the Control Panel window and choose **Administrative Tools > Services**.
A window opens listing the Windows services.
- Step 2** Right-click **Cisco DCNM Server** and choose **Stop**.

**Note**

Alternatively, you can choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**; however, the location of shortcuts depends upon the choices you made when you installed the DCNM-LAN server.

A splash screen opens while the DCNM-LAN server begins to shut down. When the DCNM-LAN server has stopped, the splash screen closes.

Stopping a Single DCNM-LAN Server (RHEL)

On a server system that runs RHEL, you can stop a DCNM-LAN server with the `Stop_DCNM_LAN_Server` script. The script is located in your home folder or the folder that was specified when setting up the link folder during the installation of Cisco DCNM-LAN.



Note

`Stop_DCNM_LAN_Server` launches `/usr/local/Cisco/dcm/dcnm/bin/stopdcnm.sh`.

DETAILED STEPS

- Step 1** Use the **Stop_DCNM_LAN_Server** script to stop the server on a RHEL operating system.
- The DCNM-LAN server opens a server console window and displays the processes that it runs to stop the server. The server is stopped when you see a “Stopped at Xm:XXs:XXXms” message.

Stopping a Cluster of DCNM-LAN Servers

Depending on the operating system of the secondary server, the DCNM-LAN server can be stopped using the CLI or the DCNM Install Manager tool. You can use the CLI or the DCNM Install Manager tool for a secondary server running RHEL. For a secondary server running Microsoft Windows, the DCNM-LAN server is stopped with the CLI.

Stopping with CLI

If you have a clustered-server DCNM-LAN deployment, you can use the `stop-dcnm-cluster` script to stop all the servers in the cluster.

BEFORE YOU BEGIN

Ensure that you know which server is currently the master server in the DCNM-LAN server cluster. You can use the Cluster Administration feature to do so.

DETAILED STEPS

- Step 1** On the master server, access a command prompt.
- Step 2** Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:

cd *path*

where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the Cisco DCNM bin directory is `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. For RHEL, the default path to the bin directory is `/usr/local/cisco/dcm/dcnm/bin`.

- Step 3** Run the **stop-dcnm-cluster** script. The script name depends upon the server operating system, as shown in the following table:

Server Operating System	Stop DCNM Cluster Script
Microsoft Windows	stop-dcnm-cluster.bat
Linux	stop-dcnm-cluster.sh

The script instructs each DCNM-LAN server in the cluster to stop.

Example

The following example from a Microsoft Windows server shows how to stop a cluster of DCNM-LAN servers, with DCNM-LAN installed in the default directory:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcn\dcnm\bin"

C:\Program Files\Cisco Systems\dcn\dcnm\bin>stop-dcnm-cluster.bat

C:\Program Files\Cisco Systems\dcn\dcnm\bin>set JAVA_HOME=C:\Program Files\Cisco Systems\
dcn\java\jre1.5

C:\Program Files\Cisco Systems\dcn\dcnm\bin>"C:\Program Files\Cisco Systems\dcn\
jboss-4.2.2.GA\bin\twiddle.bat" -s 172.28.254.254:1099 invoke
"com.cisco.dcbu.dcm:service=ClusterServerInfo" stopServerInstancesInCluster 10
Shutdown Triggered for all Servers Successfully
C:\Program Files\Cisco Systems\dcn\dcnm\bin>
```

Stopping with Install Manager

Cisco DCNM Install Manager is a GUI tool for servers that runs Linux. It is designed to assist in performing silent mode operations on secondary servers (remote nodes).



Note

Cisco DCNM Install Manager does not support Windows servers.

DETAILED STEPS

- Step 1** To access Install Manager, navigate to the **dcnm-install-manager.sh** file that is located in the bin folder where the DCNM-LAN server was installed.
- The default bin folder location for servers running Linux is **/usr/local/Cisco/dcm/dcnm/bin**.
- Step 2** Double click the **dcnm-install-manager.sh** file to launch Install Manager.
- Step 3** In the toolbar, click the **New** icon near the top of the Install Manager GUI for every secondary server. A new row in the list of Server Nodes is created every time that the New icon is clicked.



Note

In the toolbar, click the **Delete** icon to delete a selected row in the list of Server Nodes. This step does not delete a secondary server from the clustered-server environment.

Step 4 For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

The protocol is either Telnet or SSH.

- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

Alternatively, default user credentials can be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.

- (Optional) Comments that might be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the “+” icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

Step 5 In the list of Server Nodes, choose the secondary servers to stop.

Step 6 In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers.

Correct any connectivity issues before continuing.

Step 7 In the toolbar, click the **Stop** icon to stop the selected secondary servers.



Note

The Install Manager is a standalone application. The settings specified are not saved and are not persistent. The settings are lost when you exit the Install Manager GUI.

Related Documents

Related Topic	Document Title
Deploying single DCNM-LAN servers and deploying DCNM-LAN server clusters	<i>Cisco DCNM Installation and Licensing Guide, Release 7.1.x</i>
Backing up, cleaning, and restoring DCNM-LAN databases	Chapter 35, “Maintaining the Cisco DCNM-LAN Database”

Feature History for Starting and Stopping a DCNM-LAN Server

Table 25-1 lists the release history for this feature.

Table 25-1 Feature History for Starting and Stopping a DCNM-LAN Server

Feature Name	Releases	Feature Information
Starting and stopping a cluster of servers	5.0(2)	Support for starting and stopping a cluster of servers was introduced.



CHAPTER 26

Data Center Network Manager (DCNM) - Vacuum and Autovacuum Postgres Databases

This chapter describes how to vacuum the postgres database in Microsoft Windows and Linux.

This chapter includes the following sections:

- [Background Information, page 26-1](#)
- [Vacuum DCNM's Postgresql Database in Windows, page 26-1](#)
- [Vacuum DCNM's Postgresql Database in Linux, page 26-2](#)

Background Information

It is absolutely critical to vacuum postgres databases in order for the databases to properly function. Through the life of the database, new entries are added and current entries are updated. By design, postgres does not immediately remove the iterations of a record as it gets updated. Therefore, postgres databases can contain a large number of stale, unused records. These old records should be removed at least every two weeks with the vacuum function in order to reduce disk usage and improve the speed of database queries. It is even more effective if you configure postgres to automatically vacuum the database without the need to stop the Data Center Network Manager (DCNM) services.



Note

\$INSTALLDIR throughout this article refers to "C:\Program Files\Cisco Systems\" or "/usr/local/cisco/" based on the operating system, Microsoft Windows or Linux respectively. The install path could be changed from these defaults during installation.

Vacuum DCNM's Postgresql Database in Windows

-
- Step 1** Stop the DCNM services by clicking **Stop DCNM Servers** button, or enter the command as below:
\$INSTALLDIR/dcm/dcnm/bin/stopLANSANserver.bat
- Step 2** Obtain the database name, username, and password. Locate the **postgresql.cfg.xml** file on the DCNM server.
- In DCNM Version 6.2.x, enter:
\$INSTALLDIR/dcm/jboss-4.2.2.GA/server/dcnm/conf/database/postgresql.cfg.xml

- In DCNM Version 6.3.x, enter:

```
$INSTALLDIR/dcm/Jboss-as-7.2.0.Final/standalone/conf/postgresql.cfg.xml
```

- Step 3** Open **PgAdmin III.exe**, which is a helpful GUI for the postgres database. Then, right-click the object in the list and connect to the database. Enter the password from Step 2 here.
- Step 4** Navigate through the drop-down menus to the dcmdb database.
- Step 5** Right-click dcmdb and select Maintenance. Select the **Vacuum**, **Full**, **Analyze**, and **Verbose** options in the Maintain Database dcmdb dialog box.

**Note**

The vacuum operation usually completes within an hour, but can take much longer for larger databases. Remember to restart the DCNM services.

Vacuum DCNM's Postgresql Database in Linux

- Step 1** Stop dcnm by using the **appmgr stop dcnm** command.
- Step 2** Open the psql prompt:
- ```
./usr/local/cisco/dcm/db/bin/psql -U <dbUsername> dcmdb
```
- Step 3** Run the database vacuum and quit:
- ```
dcmdb=> VACUUM FULL ANALYZE VERBOSE;
```
- Many pages of output pass on the screen. The vacuum is finished when you see a message similar to this one:
- ```
Current limits are: 532000 page slots, 1000 relations, using 3182 kB.
```
- VACUUM
- ```
dcmdb=>
```
- ```
dcmdb=> \q
```
- The previous command exits the sql prompt.
- Step 4** Start DCNM services by using the **appmgr start dcnm** command.





## CHAPTER 27

# Administering Device Discovery

---

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

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

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

This chapter includes the following sections:

- [Information About Device Discovery, page 27-1](#)
- [Licensing Requirements for Device Discovery, page 27-6](#)
- [Prerequisites for Device Discovery, page 27-6](#)
- [Guidelines and Limitations for Device Discovery, page 27-6](#)
- [Performing Device Discovery, page 27-7](#)
- [Viewing the Status of Device Discovery Tasks, page 27-12](#)
- [Where to Go Next, page 27-12](#)
- [Field Descriptions for Device Discovery, page 27-12](#)
- [Device System-Message Logging Level Reference, page 27-15](#)
- [Additional References for Device Discovery, page 27-19](#)
- [Feature History for Device Discovery, page 27-19](#)

## Information About Device Discovery

This section includes the following topics:

- [Device Discovery, page 27-2](#)
- [Discovery Protocols, page 27-2](#)
- [Credentials and Discovery, page 27-3](#)
- [Discovery Process, page 27-3](#)
- [Cisco NX-OS System-Message Logging Requirements, page 27-4](#)



- [Automatic Logging-Level Configuration Support, page 27-5](#)
- [VDC Support, page 27-5](#)

## Device Discovery

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

**Note**

Starting from Cisco NX-OS Release 5.2.2(a) the Cisco DCNM-LAN supports the discovery of the following modules:

- N7K-F248XP-25 Line Card
- N55-M16FP 16-Port FC GEM
- N7K-C7010-FAB2 Fabric 2 module
- N7K-C7018-FAB2 Fabric 2 module
- N55-D160L3-V2 Daughter Card
- N55-M160L3-V2 Line Card
- N3K-C3048TP-1GE Layer 3 switch
- N3K-C3016Q- 40GE Layer 3 switch

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

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

## Discovery Protocols

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

- [Cisco Discovery Protocol, page 27-3](#)
- [Link Layer Discovery Protocol, page 27-3](#)
- [Fibre Channel, page 27-3](#)



## Cisco Discovery Protocol

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

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

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

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

## Link Layer Discovery Protocol

Device discovery uses Link Layer Discovery Protocol (LLDP) to discover the network adapters of servers that are connected to Cisco NX-OS devices.

## Fibre Channel

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

## Credentials and Discovery

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

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

## Discovery Process

DCNM-LAN discovers devices in several phases, as follows:

1. CDP neighbor discovery—Discovers the topology of the interconnected devices, beginning with the seed device and preceding for the number of CDP hops specified when you initiate discovery.
2. Supported device selection—Determines which of the discovered devices are supported by DCNM-LAN. Discovery continues for the supported devices only.
3. Inventory discovery—Discovers the inventory of the devices selected in the previous phase. For example, if the device is a Cisco Nexus 7000 Series switch, inventory discovery determines the supervisor modules, I/O modules, power supplies, and fans. If the device is a Cisco Nexus 1000V switch, inventory discovery finds the Virtual Supervisor Module and Virtual Ethernet Modules.



4. Device configuration discovery—Discovers the details of feature configuration on each device, such as interfaces, access control lists, and VLANs.
5. Network discovery—Associates network features with the device configuration details discovered in the previous phase.

## Cisco NX-OS System-Message Logging Requirements

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

This section includes the following topics:

- [Interface Link-Status Events Logging Requirement, page 27-4](#)
- [Logfile Requirements, page 27-4](#)
- [Logging Severity-Level Requirements, page 27-4](#)

### Interface Link-Status Events Logging Requirement

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

- **logging event link-status enable**
- **logging event link status default**

To ensure that these commands are configured on the device, perform the steps in the [“Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7](#).

### Logfile Requirements

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

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

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

**logging logfile messages 6**

To ensure that this command is configured on the device, perform the steps in the [“Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7](#).

### Logging Severity-Level Requirements

DCNM-LAN has minimum severity level requirements for some Cisco NX-OS logging facilities. All enabled features on a Cisco NX-OS have a default logging level. The logging level required by DCNM-LAN varies per logging facility but is often higher than the default logging level in Cisco NX-OS. For more information, see the [“Automatic Logging-Level Configuration Support” section on page 27-5](#).



## Automatic Logging-Level Configuration Support

DCNM-LAN provides support for automatic logging level configuration for all supported Cisco NX-OS releases with the exception of Cisco NX-OS Release 4.0, which is available on Cisco Nexus 7000 Series switches only. This section describes how DCNM-LAN supports automatic logging-level configuration. For information about manually configuring logging levels for Cisco NX-OS Release 4.0, see the [“Verifying the Discovery Readiness of a Cisco NX-OS Device”](#) section on page 27-7.

### During Device Discovery

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

### At Feature Enablement in the DCNM-LAN Client

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

### During Auto-Synchronization with Managed Devices

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

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

## VDC Support

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

Before discovering a Cisco Nexus 7000 Series device that has nondefault VDCs, ensure that each VDC meets the prerequisites for discovery. For more information, see the [“Prerequisites for Device Discovery”](#) section on page 27-6.



# Licensing Requirements for Device Discovery

The following table shows the licensing requirements for this feature:

| Product  | License Requirement                                                                                                                                                                                                                                                                                                               |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCNM-LAN | The Device Discovery feature requires no license. Any feature not included in a license package is bundled with the DCNM-LAN 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 7.1.x</i> . |

## Prerequisites for Device Discovery

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

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

The Device Discovery feature has the following prerequisites:

- The DCNM-LAN server must be able to connect to devices that it discovers.
- Cisco NX-OS devices must be running a supported release of Cisco NX-OS. For information about supported releases of Cisco NX-OS, see the *Cisco DCNM Release Notes, Release 7.1.x*.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the [“Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7](#).
- For a Cisco Nexus 7000 Series device, each VDC that you want to discover must have a management interface configured. DCNM-LAN supports discovery of VDCs that are configured with a management interface that is the mgmt0 interface, which is an out-of-band virtual interface, or with an in-band Ethernet interface that is allocated to the VDC.
- To allow DCNM-LAN to discover devices that are CDP neighbors, CDP must be enabled both globally on each device and specifically on the device interfaces used for device discovery. For a Cisco Nexus 7000 Series device, CDP must be enabled globally in each VDC and on the management interface that each VDC is configured to use.
- Discovery of network servers requires that LLDP is enabled globally on devices connected to network servers and specifically on the device interfaces connected to the network adapters on network servers.

## Guidelines and Limitations for Device Discovery

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

- Ensure that Cisco NX-OS devices that you want to discover have been prepared for discovery. For more information, see the [“Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7](#).
- DCNM-LAN can manage only devices that run Cisco NX-OS. For more information about supported device operating systems and supported device hardware, see the *Cisco DCNM Release Notes, Release 7.1.x*.



- CDP-based discovery of devices requires that all devices in the chain of CDP hops use the same username and password specified for the seed device. If your security practices do not allow the same username and password to be used on each device, you can perform device discovery for each device individually.
- Devices that are CDP hops but which are not running Cisco IOS software appear in the Topology feature but cannot be managed by DCNM-LAN.

## Performing Device Discovery

This section includes the following topics:

- [Verifying the Discovery Readiness of a Cisco NX-OS Device, page 27-7](#)
- [, page 27-12](#)
- [Device Discovery, page 27-2](#)
- [Viewing the Status of Device Discovery Tasks, page 27-12](#)

## Verifying the Discovery Readiness of a Cisco NX-OS Device

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

**Note**

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

### DETAILED STEPS

- 
- Step 1** Log into the CLI of the Cisco NX-OS device.
- Step 2** Use the **configure terminal** command to access global configuration mode.
- Step 3** Ensure that an RSA or DSA key exists so that secure shell (SSH) connections can succeed. To do so, use the **show ssh key rsa** or **show ssh key dsa** command.
- If you need to generate a key, use the **ssh key** command.

**Note**

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

- 
- Step 4** Ensure that the SSH server is enabled. To do so, use the **show ssh server** command.
- If the SSH server is not enabled, use the **feature ssh** command to enable it.
- Step 5** Ensure that CDP is enabled globally and on the interface that DCNM-LAN uses to connect to the device. Use the **show run cdp all** command to see whether CDP is enabled.



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

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

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



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

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



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

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

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

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

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

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

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

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

```
switch(config)# show logging level
```

| Facility | Default Severity | Current Session Severity |
|----------|------------------|--------------------------|
| -----    | -----            | -----                    |
| aaa      | 3                | 5                        |
| aclmgr   | 3                | 3                        |
| .        |                  |                          |
| .        |                  |                          |
| .        |                  |                          |



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



- c. Determine which logging levels on the device are below the minimum DCNM-LAN required logging levels. To do so, compare the logging levels displayed on page 27-8 to the minimum DCNM-LAN required logging levels that are listed in Table 27-3.
- d. For each logging facility with a logging level that is below the minimum DCNM-LAN required logging level, configure the device with a logging level that meets or exceeds the DCNM-LAN requirement.

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

The *facility* argument is the applicable logging-facility keyword from Table 27-3, and *severity-level* is the applicable minimum DCNM-LAN required logging level or higher (up to 7).

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

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

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

## Discovering Devices

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

You can perform Deep Discovery by selecting one task at a time. You can also select all or multiple devices in a single task at a time.



### Note

You cannot select multiple tasks or multiple devices across tasks at one instance.

Use this procedure for the following purposes:

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



### Note

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

## BEFORE YOU BEGIN

Ensure that you have configured the Cisco NX-OS device so that the DCNM-LAN server can connect to it and successfully discover it. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x* “Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7.



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

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

**Note**

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

**DETAILED STEPS**

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.  
The discovery tasks appear in the Discovery Tasks area of the Contents pane.
- Step 2** Click **Here** in the Device Discovery pane to perform Shallow Discovery of the devices in the Cisco DCNM Web Client. The shallow discovery result web page pops out.  
There are four types of discovery, they are **Fabric**, **LAN**, **VMWare**, and **SMI-S Storage**.
- Step 3** In the first table of **Fabric**, you can **Edit**, **Remove**, **Add**, **Re-discover**, **Refresh** and **Purge unreachable devices or dead link** in selected fabric.
- To edit the fabric— Check the box before the fabric you want to select, and click the **edit** icon as a pencil. You can edit the **Fabric Name**, check/uncheck to use/disuse **SNMPv3/SSH** and select the **Auth-Privacy** from the drop-down list. Enter the **User Name** and **Password** and select the **Status** as **managed**, **unmanaged**, or **managedContinuously**. (Optional) You can click the **options** button to input the **UCS User Name** and the **UCS Password**.
  - To remove the fabric— Select the fabric that you want to remove, and click the **remove** icon. Click yes to remove the selected fabric.
  - To add a fabric— Click the **add** icon to add a fabric. Enter the information about **Fabric Seed Switch**, **SNMP**, **User Name** and **Password**. If you check **Limit Discovery by VSAN**, select which you want to limit by, **Included VSAN List** or **Excluded VSAN List**, and provide the **VSAN List**. Check/uncheck to enable/disable NPV Discovery in All Fabrics. (Optional) Click options button to input the **UCS User Name** and the **UCS Password**.
  - To re-discover a fabric— Select the fabric that you want to be re-discovered, and click the **Re-discover Fabric** icon. Click yes to perform re-discovery of the fabric.
  - To refresh the fabric discovery table— Click the **refresh** icon to manually refresh the discovery table.
  - To purge down elements in the fabric— Select the fabric and click the **Purge** icon to purge unreachable devices or dead links in selected Fabric and click yes.
  - To maximize the fabric table— Click the **Maximize** icon to maximize the fabric table and click **Normalize** to return the former view.
- Step 4** In the second table of **LAN** discovery, you can **Add**, **Refresh**, **Purge unreachable devices or dead links in selected LAN** and **Toggle between Task and Device View**. You can **Edit LAN Task**, **Re-discover LAN** and **Remove LAN Task/Switch** by clicking the icons before the tasks/switches.
- To **Edit LAN Task**— Click the Edit icon, enter the username of a user account on the device in the **User Name** field. The user account must have a network-admin or vdc-admin role. In the **Password** field, enter the password for the user account. Choose the **Status** of the LAN task. For Catalyst 6500 devices, enter the enable password in the Enable Password field to allow for IOS privileged EXEC mode commands.



- To **Re-discover LAN**— A warning message pops out, click on yes to proceed rediscovery.
- To **Remove LAN Task**— Click on the remove icon and click yes to remove the LAN task.
- To **Add LAN Task**— Choose the **Discovery Type** from **Hops from Seed Switch/Switch List/FWSM**.

If you choose the discovery type as **Hops from Seed Switch**, input the IP address or IP range string in **Seed Switch**. Drag the triangle to the number which represents the **Max Hops from Seed**. Choose the **Protocol** of the LAN. If you choose **SNMPv1**, select the **Scan Timeout** from the drop-down list and enter the **Community**. If you choose **SNMPv3/CLI**, select the auth-privacy and **Scan Timeout** from the drop-down list. Enter the **User Name** and **Password**. Select the group that you want to add the switch to and click **Next**. **Shallow LAN Discovery** window shows up. Select the switches and click Add to add the LAN task.

It's quite similar with the other discovery type as **Switch List or FWSM**, only that you don't need to provide the max hops from seed.

- Step 5** If there are VMWare and SMI-S storage devices discovered, you can perform similar function in the VMWare and SMI-S Storage discovery table.
- Step 6** You can only perform deep discovery in the DCNM LAN client, please follow the steps in [Deep Discovery](#).

**Note**

When DCNM shallow discovery is done, DCNM server registers its address as trap address in each switch with the user's community. When discovery takes place for the first time, a server property called **trapaddr.register.community** which has the default value '**public**' is overwritten with the user's community.

## Deep Discovery

Deep discovery is an ssh based discovery initiated from the DCNM-LAN client and allows DCNM to actually log in via ssh and configure the LAN devices.

To perform Deep Discovery of the devices so that you can configure LAN devices via DCNM, please follow below steps:

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.
- Step 2** Click the plus icon to expand the task under **Task based Discovery** pane, a list of devices under the single task shows up.
- Step 3** You can either select one device or multiple devices under one task. Right click on the single device or multiple devices under one task and select **Deep Discovery**.

**Note**

Deep Discovery is a requirement for any of the features found in the DCNM LAN client.

- Step 4** Click **Refresh** button or press F5, the successfully deep discovered device will show **MANAGED** under **SSH/Telnet** of **Status**.
- Step 5** You can also right click the discovered devices and select **Re-do deep discovery**.



- Step 6** In the Device Discovery pane, click the **History** button to open the History of Discovery window. You can see **Task ID**, **Owner**, **Seed Device IP Address**, **Discovered Time**, **Reason** and **Status** history from the window.

# Viewing the Status of Device Discovery Tasks

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

The tasks, including the task status, appear in the Discovery Tasks area in the Contents pane. For information about the fields that appear, see the [“Field Descriptions for Device Discovery” section on page 27-12](#).

## Where to Go Next

View the discovered devices and configure unique device credentials, as needed. For more information, see the [“Administering Devices and Credentials” section on page 28-1](#).

# Field Descriptions for Device Discovery

- This section includes the following field descriptions for the Device Discovery feature:
- [Device Discovery Content Pane, page 27-12](#)
  - [Related Fields, page 27-15](#)

## Device Discovery Content Pane

**Table 27-1**      *Shallow Discovery Content Pane*

| Field                                    | Description                                                                                                                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Admin&gt; Data Sources &gt;Fabric</b> |                                                                                                                                                                               |
| Fabric Name                              | Name of the Fabric.                                                                                                                                                           |
| Seed Switch                              | The IP address of the fabric’s seed switch. IPv4 address of the first device that you want to discover. Valid entries are in dotted decimal format.                           |
| Status                                   | <ul style="list-style-type: none"> <li>• managed</li> <li>• unmanaged</li> <li>• managedContinuouly</li> </ul>                                                                |
| SNMPv3/SSH                               | True if the fabric is using SNMPv3/SSH.                                                                                                                                       |
| User/Cmnty                               | Name of the device user account/community that the DCNM-LAN server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device. |
| Auth/Privacy                             | The authorization method used by the fabric.                                                                                                                                  |



**Table 27-1**      **Shallow Discovery Content Pane**

| Field                                           | Description                                                                                                                                                                                          |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Included VSAN List                              | The IP address of the included VSAN list that the fabric is limited by.                                                                                                                              |
| Excluded VSAN List                              | The IP address of the excluded VSAN list that the fabric is limited by.                                                                                                                              |
| Licensed                                        | If the fabric is licensed or not.                                                                                                                                                                    |
| Last Updated Time                               | The last updated time of the fabric.                                                                                                                                                                 |
| <b>Admin&gt; Data Sources&gt; LAN</b>           |                                                                                                                                                                                                      |
| Discovery Task                                  | The discovery task name of LAN.                                                                                                                                                                      |
| Max Hops from Seed                              | The max hops from seed switch to be discovered.                                                                                                                                                      |
| Switch List                                     | The IP address or string of the switch list.                                                                                                                                                         |
| FWSM IP Address                                 | The FWSM IP address discovered.                                                                                                                                                                      |
| Switch                                          | The seed switch of the task.                                                                                                                                                                         |
| Managed                                         | True if the LAN discovery task is managed.                                                                                                                                                           |
| SNMP Status                                     | Whether or not the SNMP is enabled.                                                                                                                                                                  |
| Last Updated Time                               | The last updated time of the LAN.                                                                                                                                                                    |
| Group                                           | Which of the LAN group does the switches belong to.                                                                                                                                                  |
| SNMPv3/SSH                                      | True if SNMPv3/SSH is used.                                                                                                                                                                          |
| User/Cmnty                                      | Name of the device user account that the DCNM-LAN server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device. By default, this field is blank. |
| Auth/Privacy                                    | The authorization method used by the LAN.                                                                                                                                                            |
| <b>Admin&gt; Data Sources&gt; VMWare</b>        |                                                                                                                                                                                                      |
| Server                                          | The server name of the VMWare.                                                                                                                                                                       |
| Managed                                         | True if the remote device is managed.                                                                                                                                                                |
| Status                                          | The status of the server.                                                                                                                                                                            |
| User                                            | Name of the device user account that the DCNM-LAN server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device.                                  |
| Last Updated Time                               | The last updated time of the virtual machine.                                                                                                                                                        |
| <b>Admin&gt; Data Sources&gt; SMI-S Storage</b> |                                                                                                                                                                                                      |
| Vendor                                          | The vendor of the storage device.                                                                                                                                                                    |
| Version                                         | The version information of the storage device.                                                                                                                                                       |
| Provider URL                                    | The URL of the provider.                                                                                                                                                                             |
| Name Space                                      | The name space of the storage.                                                                                                                                                                       |
| Interop Name Space                              | The iinterop name space of the storage.                                                                                                                                                              |
| Port                                            | The port used to access the storage.                                                                                                                                                                 |
| Secure                                          | The secure information of the storage.                                                                                                                                                               |
| Status                                          | The status of the storage.                                                                                                                                                                           |



**Table 27-1 Shallow Discovery Content Pane**

| Field             | Description                           |
|-------------------|---------------------------------------|
| Discovery Status  | The discovery status of the storage.  |
| Last Updated Time | The last updated time of the storage. |

**Table 27-2 Deep Discovery Content Pane**

| History of Discovery   |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Task ID                | <i>Display only.</i> Number assigned to the discovery task. The task ID indicates the order in which discovery tasks occurred.                                                                                                                                                                                                                                                                                                                        |
| Owner                  | <i>Display only.</i> DCNM-LAN server user account used to start the discovery task.                                                                                                                                                                                                                                                                                                                                                                   |
| Seed Device IP Address | <i>Display only.</i> IPv4 address of the seed device.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Discovered Time        | <i>Display only.</i> Date and time of the most recent update to the Status field.                                                                                                                                                                                                                                                                                                                                                                     |
| Reason                 | <i>Display only.</i> Why the discovery task was created.                                                                                                                                                                                                                                                                                                                                                                                              |
| Status                 | <i>Display only.</i> State of the discovery task. Valid values are as follows: <ul style="list-style-type: none"> <li>In progress—The discovery tasks are ongoing.</li> <li>Successful—The discovery task completed without errors.</li> <li>Failed—The discovery task completed with errors.</li> </ul>                                                                                                                                              |
| Task Based Discovery   |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Name                   | <i>Display only.</i> The name of the task.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Switches               | <i>Display only.</i> The devices under the single task.                                                                                                                                                                                                                                                                                                                                                                                               |
| Managed                | <i>Display only.</i> Show if the task is managed by DCNM.                                                                                                                                                                                                                                                                                                                                                                                             |
| SNMP                   | <i>Display only.</i> SNMP status can be different as below: <ul style="list-style-type: none"> <li>ok—The device is accessible/reachable at current time.</li> <li>Last Seen—The time when the device was last reachable. <b>Last Seen</b> will be in that state for few minutes, after which it will show up as <b>Discovery Timeout</b>.</li> <li>Discovery Timeout—The device is not accessible/reachable because of discovery timeout.</li> </ul> |
| SSH/Telnet             | <i>Display only.</i> Status of the discovery task. <ul style="list-style-type: none"> <li>ENABLE DEEP DISCOVERY— Deep discovery is not enabled.</li> <li>UNMANAGED (Connection Failure)—Connection to the device by SSH/Telnet failed.</li> <li>UNMANAGED (Auth Failure)—Authentication of the device failed.</li> <li>DISCOVERING—The device is in the process of discovering.</li> <li>MANAGED—The device is managed by DCNM.</li> </ul>            |



## Related Fields

For information about fields that configure devices, see the [“Administering Devices and Credentials” section on page 28-1](#).

## Device System-Message Logging Level Reference

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



### Note

DCNM-LAN provides automatic device logging-level support. For more information, see the [Automatic Logging-Level Configuration Support, page 27-5](#).

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

- [Cisco Nexus 7000 NX-OS Logging Levels per DCNM-LAN Feature, page 27-15](#)
- [Cisco Nexus 5000 NX-OS Logging Levels per DCNM-LAN Feature, page 27-16](#)
- [Cisco Nexus 4000 NX-OS Logging Levels per DCNM-LAN Feature, page 27-17](#)
- [Cisco Nexus 1000V NX-OS Logging Levels per DCNM-LAN Feature, page 27-18](#)

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

**Table 27-3** Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM-LAN Feature

| Cisco DCNM-LAN Feature | Cisco Nexus 7000 NX-OS Logging Facility | Enabled by Default? | Logging Facility Keyword | Cisco NX-OS Default Logging Level | Minimum Cisco DCNM-LAN-Required Logging Level <sup>1</sup> |
|------------------------|-----------------------------------------|---------------------|--------------------------|-----------------------------------|------------------------------------------------------------|
| AAA                    | AAA                                     | Yes                 | aaa                      | 3                                 | 5                                                          |
|                        | RADIUS                                  | Yes                 | radius                   | 3                                 | 5                                                          |
|                        | TACACS+                                 | No                  | tacacs+                  | 3                                 | 5                                                          |
| Device Discovery       | CDP                                     | Yes                 | cdp                      | 2                                 | 6                                                          |
| Topology               | LLDP                                    | No                  | lldp                     | 2                                 | 5                                                          |
| DHCP snooping          | DHCP snooping                           | No                  | dhcp                     | 2                                 | 6                                                          |
| Dynamic ARP Inspection |                                         |                     |                          |                                   |                                                            |
| IP Source Guard        |                                         |                     |                          |                                   |                                                            |
| Dot1X                  | 802.1X                                  | No                  | dot1x                    | 2                                 | 5                                                          |
| Ethernet Interfaces    | Ethernet port manager                   | Yes                 | ethpm                    | 5                                 | 5                                                          |
| Traffic Storm Control  |                                         |                     |                          |                                   |                                                            |



**Table 27-3** Cisco Nexus 7000 NX-OS Logging Levels per Cisco DCNM-LAN Feature (continued)

| Cisco DCNM-LAN Feature                 | Cisco Nexus 7000 NX-OS Logging Facility | Enabled by Default? | Logging Facility Keyword | Cisco NX-OS Default Logging Level | Minimum Cisco DCNM-LAN-Required Logging Level <sup>1</sup> |
|----------------------------------------|-----------------------------------------|---------------------|--------------------------|-----------------------------------|------------------------------------------------------------|
| Gateway Load Balancing Protocol (GLBP) | GLBP                                    | No                  | glbp                     | 3                                 | <b>6</b>                                                   |
| Hot Standby Router Protocol (HSRP)     | HSRP engine                             | No                  | hsrp                     | 3                                 | <b>6</b>                                                   |
| Inventory                              | Module                                  | Yes                 | module                   | 5                                 | 5                                                          |
|                                        | Platform                                | Yes                 | platform                 | 5                                 | 5                                                          |
|                                        | System manager                          | Yes                 | sysmgr                   | 3                                 | 3                                                          |
| Object Tracking                        | Object tracking                         | Yes                 | track                    | 3                                 | <b>6</b>                                                   |
| Port-Channel Interfaces                | Port-channel interfaces                 | Yes                 | port-channel             | 5                                 | <b>6</b>                                                   |
| Port security                          | Port security                           | No                  | port-security            | 2                                 | <b>5</b>                                                   |
| SPAN                                   | SPAN                                    | Yes                 | monitor                  | 3                                 | <b>6</b>                                                   |
| Spanning Tree                          | Spanning tree                           | Yes                 | spanning-tree            | 3                                 | <b>6</b>                                                   |
| Unidirectional Link Detection (UDLD)   | UDLD                                    | No                  | udld                     | 5                                 | 5                                                          |
| Virtual Device Contexts (VDCs)         | VDC manager                             | Yes                 | vdc_mgr                  | 6                                 | 6                                                          |
| Virtual Port Channel (vPC)             | VPC                                     | No                  | vpc                      | 2                                 | <b>6</b>                                                   |
| VLAN Network Interfaces                | Interface VLAN                          | No                  | interface-vlan           | 2                                 | 5                                                          |

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

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

**Table 27-4** Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM-LAN Feature

| Cisco DCNM-LAN Feature | Cisco Nexus 5000 NX-OS Logging Facility | Enabled by Default? | Logging Facility Keyword | Cisco NX-OS Default Logging Level | Minimum Cisco DCNM-LAN-Required Logging Level <sup>1</sup> |
|------------------------|-----------------------------------------|---------------------|--------------------------|-----------------------------------|------------------------------------------------------------|
| AAA                    | AAA                                     | Yes                 | aaa                      | 3                                 | <b>5</b>                                                   |
|                        | RADIUS                                  | Yes                 | radius                   | 3                                 | <b>5</b>                                                   |
|                        | TACACS+                                 | No                  | tacacs+                  | 3                                 | <b>5</b>                                                   |
| Device Discovery       | CDP                                     | Yes                 | cdp                      | 2                                 | <b>6</b>                                                   |
| Topology               | LLDP                                    | No                  | lldp                     | 2                                 | 5                                                          |
| Ethernet Interfaces    | Ethernet port manager                   | Yes                 | ethpm                    | 5                                 | 5                                                          |
| Traffic Storm Control  |                                         |                     |                          |                                   |                                                            |
| Fabric Extender        | FEX                                     | Yes                 | fex                      | 5                                 | 5                                                          |



**Table 27-4** Cisco Nexus 5000 NX-OS Logging Levels per Cisco DCNM-LAN Feature (continued)

| Cisco DCNM-LAN Feature               | Cisco Nexus 5000 NX-OS Logging Facility | Enabled by Default? | Logging Facility Keyword | Cisco NX-OS Default Logging Level | Minimum Cisco DCNM-LAN-Required Logging Level <sup>1</sup> |
|--------------------------------------|-----------------------------------------|---------------------|--------------------------|-----------------------------------|------------------------------------------------------------|
| Inventory                            | System manager                          | Yes                 | sysmgr                   | 3                                 | 3                                                          |
|                                      | Platform                                | Yes                 | pfm                      | 5                                 | 5                                                          |
|                                      | NOHMS                                   | Yes                 | nohms                    | 2                                 | 2                                                          |
| Port-Channel Interfaces              | Port-channel interfaces                 | Yes                 | port-channel             | 5                                 | <b>6</b>                                                   |
| SPAN                                 | SPAN                                    | Yes                 | monitor                  | 3                                 | <b>6</b>                                                   |
| Spanning Tree                        | Spanning tree                           | Yes                 | spanning-tree            | 3                                 | <b>6</b>                                                   |
| Unidirectional Link Detection (UDLD) | UDLD                                    | No                  | udld                     | 5                                 | 5                                                          |
| Virtual Port Channel                 | VPC                                     | No                  | vpc                      | 2                                 | <b>6</b>                                                   |
| VLAN Network Interfaces              | Interface VLAN                          | No                  | interface-vlan           | 2                                 | 5                                                          |

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

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

**Table 27-5** Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM-LAN Feature

| Cisco DCNM-LAN Feature  | Cisco Nexus 4000 NX-OS Logging Facility | Enabled by Default? | Logging Facility Keyword | Cisco NX-OS Default Logging Level | Minimum Cisco DCNM-LAN-Required Logging Level <sup>1</sup> |
|-------------------------|-----------------------------------------|---------------------|--------------------------|-----------------------------------|------------------------------------------------------------|
| AAA                     | AAA                                     | Yes                 | aaa                      | 3                                 | <b>5</b>                                                   |
|                         | RADIUS                                  | Yes                 | radius                   | 3                                 | <b>5</b>                                                   |
|                         | TACACS+                                 | No                  | tacacs+                  | 3                                 | <b>5</b>                                                   |
| Device Discovery        | CDP                                     | Yes                 | cdp                      | 2                                 | <b>6</b>                                                   |
| Topology                |                                         |                     |                          |                                   |                                                            |
| Ethernet Interfaces     | Ethernet port manager                   | Yes                 | ethpm                    | 5                                 | 5                                                          |
| Traffic Storm Control   |                                         |                     |                          |                                   |                                                            |
| FIP Snooping            | FIPSM                                   | Yes                 | fip-snooping             | 2                                 | <b>5</b>                                                   |
| Inventory               | System manager                          | Yes                 | sysmgr                   | 3                                 | 3                                                          |
| Link State Tracking     | LST                                     | No                  | lstsvc                   | 2                                 | <b>4</b>                                                   |
| Port-Channel Interfaces | Port-channel interfaces                 | Yes                 | port-channel             | 5                                 | <b>6</b>                                                   |
| SPAN                    | SPAN                                    | Yes                 | monitor                  | 3                                 | <b>6</b>                                                   |
| Spanning Tree           | Spanning tree                           | Yes                 | spanning-tree            | 3                                 | <b>6</b>                                                   |



**Table 27-5** Cisco Nexus 4000 NX-OS Logging Levels per Cisco DCNM-LAN Feature (continued)

| Cisco DCNM-LAN Feature               | Cisco Nexus 4000 NX-OS Logging Facility | Enabled by Default? | Logging Facility Keyword | Cisco NX-OS Default Logging Level | Minimum Cisco DCNM-LAN-Required Logging Level <sup>1</sup> |
|--------------------------------------|-----------------------------------------|---------------------|--------------------------|-----------------------------------|------------------------------------------------------------|
| Unidirectional Link Detection (UDLD) | UDLD                                    | No                  | udld                     | 5                                 | 5                                                          |
| VLAN Network Interfaces              | Interface VLAN                          | No                  | interface-vlan           | 2                                 | 5                                                          |

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

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

**Table 27-6** Cisco Nexus 1000V NX-OS Logging Levels per Cisco DCNM-LAN Feature

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

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



# Additional References for Device Discovery

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

- [Related Documents, page 27-19](#)
- [Standards, page 27-19](#)

## Related Documents

| Related Topic                        | Document Title                                                      |
|--------------------------------------|---------------------------------------------------------------------|
| Device and Credentials               | <a href="#">Chapter 28, “Administering Devices and Credentials”</a> |
| Cisco NX-OS XML management interface | <i>Cisco NX-OS XML Interface User Guide</i>                         |

## Standards

| Standards                                    | Title                    |
|----------------------------------------------|--------------------------|
| NETCONF protocol over the Secure Shell (SSH) | <a href="#">RFC 4742</a> |

# Feature History for Device Discovery

[Table 27-7](#) lists the release history for this feature.

**Table 27-7**      *Feature History for Device Discovery*

| Feature Name                                  | Releases | Feature Information                 |
|-----------------------------------------------|----------|-------------------------------------|
| Discovery of various supported devices        | 5.2(2a)  | Support was added for this feature. |
| LLDP discovery                                | 5.0(2)   | Support was added for this feature. |
| Fibre Channel discovery                       | 5.0(2)   | Support was added for this feature. |
| Automatic logging-level configuration support | 5.0(2)   | Support was added for this feature. |









# CHAPTER 28

## Administering Devices and Credentials

---

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

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

Cisco DCNM also supports the ability to secure each VDC with different credentials. Cisco DCNM allows you to configure unique credentials for each discovered device or to use default credentials when you do not configure unique credentials for a device.

This chapter includes the following sections:

- [Information About Devices and Credentials, page 28-1](#)
- [Licensing Requirements for Devices and Credentials, page 28-3](#)
- [Prerequisites for Administering Devices and Credentials, page 28-3](#)
- [Guidelines and Limitations for Devices and Credentials, page 28-3](#)
- [Configuring Devices and Credentials, page 28-3](#)
- [Viewing Device Credentials and Status, page 28-7](#)
- [Field Descriptions for Devices and Credentials, page 28-8](#)
- [Additional References for Devices and Credentials, page 28-9](#)
- [Feature History for Devices and Credentials, page 28-10](#)

## Information About Devices and Credentials

This section includes the following topics:

- [Devices, page 28-2](#)
- [Credentials, page 28-2](#)
- [Device Status, page 28-2](#)
- [VDC Support, page 28-2](#)



## Devices

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

## Credentials

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

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

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

## Device Status

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

- **Managed**—DCNM-LAN can connect to the device using Secure Shell (SSH), configure the running configuration of the device, and retrieve logs and other data from it. This status is possible only for devices that run a supported release of Cisco NX-OS and that are configured properly to support discovery by DCNM-LAN. For more information, see the [“Verifying the Discovery Readiness of a Cisco NX-OS Device”](#) section on page 27-7.
- **Unmanaged**—DCNM-LAN does not manage the device or monitor the status of the device.
- **Unreachable**—DCNM-LAN cannot connect to the device, which was a managed device prior to becoming unreachable. Common causes for this status are as follows:
  - A network issue is preventing the DCNM-LAN server from contacting the device.
  - SSH is disabled on the device.
  - All terminal lines on the device are in use.

## VDC Support

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



# Licensing Requirements for Devices and Credentials

The following table shows the licensing requirements for this feature:

| Product        | License Requirement                                                                                                                                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco DCNM-LAN | Device and Credentials requires no license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN 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 7.1.x</i> . |

## Prerequisites for Administering Devices and Credentials

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

- The DCNM-LAN server must be able to connect to a device that you want to discover.
- Cisco NX-OS devices must be running a supported release of Cisco NX-OS. For information about supported releases of Cisco NX-OS, see the *Cisco DCNM Release Notes, Release 7.1.x*.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the [“Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7](#).

## Guidelines and Limitations for Devices and Credentials

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

- Discovering a device by using the Devices and Credentials feature does not support CDP-based discovery of neighboring devices. To use CDP-based discovery, see the [“Administering Device Discovery” section on page 27-1](#).
- Be careful when you change the default credentials or device-specific credentials. Incorrect credentials prevent DCNM-LAN from managing devices.

## Configuring Devices and Credentials

This section includes the following topics:

- [Configuring Default Device Credentials, page 28-4](#)
- [Clearing Default Device Credentials, page 28-5](#)
- [Configuring Unique Credentials for a Device, page 28-5](#)
- [Clearing Unique Credentials for a Device, page 28-6](#)



## Configuring Default Device Credentials

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

**Note**

Device credentials are unique for each DCNM-LAN server user.



### BEFORE YOU BEGIN

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

**Note**

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

### DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.  
The Default Credentials area appears in the Contents pane, above the Devices area, which lists the discovered devices.
- Step 2** In the User Name field, enter the username for the default credentials. A valid username can be 1 to 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.  
  
**Note** Cisco NX-OS supports usernames that are a maximum of 28 characters.
- Step 3** To the right of the Password field, click the down-arrow button.
- Step 4** In the Password field and the Confirm Password field, enter the password for the default credentials. Valid passwords are numbers, symbols, and case-sensitive letters.  
  
**Note** Cisco NX-OS supports passwords that are a maximum of 64 characters.
- Step 5** Click **OK**.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.

### RELATED TOPICS

- [Clearing Default Device Credentials, page 28-5](#)
- [Configuring Unique Credentials for a Device, page 28-5](#)



- [Clearing Unique Credentials for a Device, page 28-6](#)

## Clearing Default Device Credentials

You can clear the default device credentials.

**Note**

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

### BEFORE YOU BEGIN

If you intend to use DCNM-LAN without default device credentials, you should ensure that DCNM-LAN is configured with unique device credentials for each discovered device before you perform this procedure. For more information, see the [“Configuring Unique Credentials for a Device” section on page 28-5](#).

### DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**. The Default Credentials area appears in the Contents pane, above the Devices area, which lists the discovered devices.
- Step 2** In the Default Credentials area, click **Clear**. The User Name field and the Password field clear.
- Step 3** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.
- 

### RELATED TOPICS

- [Configuring Default Device Credentials, page 28-4](#)
- [Configuring Unique Credentials for a Device, page 28-5](#)
- [Clearing Unique Credentials for a Device, page 28-6](#)
- [Administering Device Discovery, page 27-1](#)

## Configuring Unique Credentials for a Device

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

**Note**

Device credentials are unique for each DCNM-LAN server user.



## BEFORE YOU BEGIN

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

**Note**

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

## DETAILED STEPS

**Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**. The discovered devices appear in the Devices area of the Contents pane.

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

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

**Note**

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

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

**Note**

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

**Step 5** Click **OK**.

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

## RELATED TOPICS

- [Configuring Default Device Credentials, page 28-4](#)
- [Clearing Default Device Credentials, page 28-5](#)
- [Clearing Unique Credentials for a Device, page 28-6](#)
- [Administering Device Discovery, page 27-1](#)

## Clearing Unique Credentials for a Device

You can clear unique credentials for a discovered device.

**Note**

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



## BEFORE YOU BEGIN

If you intend to operate DCNM-LAN without unique credentials for the device, you should ensure that DCNM-LAN is configured with default device credentials before you perform this procedure. For more information, see the [“Configuring Default Device Credentials” section on page 28-4](#).

## DETAILED STEPS

- 
- |               |                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Feature Selector pane, choose <b>DCNM Server Administration &gt; Devices and Credentials</b> .<br>Discovered devices appear in the Devices area of the Contents pane. |
| <b>Step 2</b> | In the User Credentials column for the device, double-click the entry and then click the down-arrow button.                                                                    |
| <b>Step 3</b> | In the User Name field, delete all text.                                                                                                                                       |
| <b>Step 4</b> | In the Password field, delete all text.                                                                                                                                        |
| <b>Step 5</b> | In the Confirm Password field, delete all text.                                                                                                                                |
| <b>Step 6</b> | Click <b>OK</b> .                                                                                                                                                              |
| <b>Step 7</b> | From the menu bar, choose <b>File &gt; Deploy</b> to apply your changes to the DCNM-LAN server.                                                                                |
- 

## RELATED TOPICS

- [Configuring Default Device Credentials, page 28-4](#)
- [Clearing Default Device Credentials, page 28-5](#)
- [Configuring Unique Credentials for a Device, page 28-5](#)
- [Administering Device Discovery, page 27-1](#)

# Viewing Device Credentials and Status

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

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

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

| Reason                 | Resolution                                                                                                                                                                                                                             |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Success                | Not applicable. DCNM-LAN is managing the device.                                                                                                                                                                                       |
| Authentication failure | Ensure that the credentials are correct for the device. Ensure that DCNM-LAN can reach the device.                                                                                                                                     |
| Unsupported platform   | Verify that the device is a supported platform and that it is running a supported release of Cisco NX-OS. For information about supported platforms and Cisco NX-OS releases, see the <i>Cisco DCNM Release Notes, Release 7.1.x</i> . |



| Reason                                                               | Resolution                                                                                                                                                                                                  |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device sync up failure                                               | Cisco Nexus 7000 Series devices only. The sequence numbers of accounting and system message log messages are not in a proper format. Clear the log files on the device and discover the device again.       |
| Unmanaged manually                                                   | A DCNM-LAN user changed the device status to Unmanaged. Discover the device again.                                                                                                                          |
| Error when executing database query                                  | Discover the device again. If the error reoccurs, clean the DCNM-LAN database. For more information about cleaning the database, see <a href="#">Chapter 35, “Maintaining the Cisco DCNM-LAN Database.”</a> |
| Auto synchronization for device is disabled by user                  | Discover the device again.                                                                                                                                                                                  |
| Logging levels required by DCNM-LAN are not configured on the device | Discover the device again. For more information, see the <a href="#">“Automatic Logging-Level Configuration Support”</a> section on page 27-5.                                                              |
| Error in SSH connection                                              | Ensure that SSH is enabled on the device and that it is functioning properly. Discover the device again.                                                                                                    |
| Unreachable                                                          | Ensure that you specify the correct IP address for the device. Ensure that DCNM-LAN can contact the device. Discover the device again.                                                                      |
| Discovery failed because server node stopped/crashed                 | Discover the device again.                                                                                                                                                                                  |
| Syslog messages logging disabled on device                           | Discover the device again.                                                                                                                                                                                  |

For information about the fields that appear, see the [“Field Descriptions for Devices and Credentials”](#) section on page 28-8.

## Field Descriptions for Devices and Credentials

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

- [Device and Credentials Content Pane, page 28-8](#)

### Device and Credentials Content Pane

**Table 28-1**      *Device and Credentials Content Pane*

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Credentials</b> |                                                                                                                                                                                                                                                                                                                                                                                                                            |
| User Name                  | Name of the Cisco NX-OS device user account that the DCNM-LAN server uses to access any device that it is discovering or that it is managing. On the device, the user account must be assigned to the network-admin or vdc-admin role. By default, this field is blank.<br><br><b>Note</b> The information in the User Credentials field in the Devices area overrides the information in the Default Credentials section. |
| Password                   | Password for the Cisco NX-OS device user account specified in the User Name field. By default, this field is blank.                                                                                                                                                                                                                                                                                                        |



**Table 28-1**      **Device and Credentials Content Pane (continued)**

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Devices</b>   |                                                                                                                                                                                                                                                                                                                                                                               |
| IP Address       | <i>Display only.</i> IPv4 address of the Cisco NX-OS device.                                                                                                                                                                                                                                                                                                                  |
| Name             | <i>Display only.</i> Name of the Cisco NX-OS device.                                                                                                                                                                                                                                                                                                                          |
| User Credentials | <p>The Cisco NX-OS user account that DCNM-LAN uses to connect to the Cisco NX-OS device.</p> <p><b>Note</b> If you configure this field, DCNM-LAN uses the user account that you configure when it connects to the device. If this field is blank, DCNM-LAN uses the user account specified in the Default Credentials area. By default, this field is blank.</p>             |
| Status           | <p><i>Display only.</i> Whether the DCNM-LAN server can connect to and configure the device. Valid values are as follows:</p> <ul style="list-style-type: none"><li>• Managed—The DCNM-LAN server can configure the device.</li><li>• Unmanaged—The DCNM-LAN server cannot configure the device.</li><li>• Unreachable—The DCNM-LAN server cannot reach the device.</li></ul> |
| Reason           | <p><i>Display only.</i> Provides a brief explanation for the device status. For more information, see the <a href="#">“Viewing Device Credentials and Status” section on page 28-7</a>.</p>                                                                                                                                                                                   |

## Additional References for Devices and Credentials

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

- [Related Documents, page 28-9](#)
- [Standards, page 28-9](#)

### Related Documents

| Related Topic                        | Document Title                                               |
|--------------------------------------|--------------------------------------------------------------|
| Cisco NX-OS XML management interface | <i>Cisco NX-OS XML Interface User Guide</i> Title may change |

### Standards

| Standards                                    | Title                    |
|----------------------------------------------|--------------------------|
| NETCONF protocol over the Secure Shell (SSH) | <a href="#">RFC 4742</a> |



# Feature History for Devices and Credentials

Table 28-2 lists the release history for this feature.

**Table 28-2**      *Feature History for Devices and Credentials*

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





## CHAPTER 29

# Administering Auto-Synchronization with Devices

---

This chapter describes how to administer the Auto-Synchronization with Devices feature in Cisco Data Center Network Manager for LAN (DCNM-LAN).

Auto-synchronization allows the Cisco DCNM server to ensure that configuration and status information about managed devices is current. The Cisco DCNM server creates a poller process for each managed device. A poller process periodically retrieves system and accounting logs from a device. Cisco DCNM uses the information retrieved by poller processes to update its configuration and status information about polled devices. When you choose Auto Synchronization with Devices on the Feature Selector, the Contents pane displays all the poller instances that are running for different devices and allows you to control each.

You can also use the Auto-Synchronization with Devices feature to delete unwanted event data on demand or automatically.

This chapter includes the following sections:

- [Information About Auto-Synchronization with Devices, page 29-1](#)
- [Licensing Requirements for Auto-Synchronization with Devices, page 29-2](#)
- [Prerequisites for Auto-Synchronization with Devices, page 29-2](#)
- [Guidelines and Limitations for Auto-Synchronization with Devices, page 29-3](#)
- [Configuring Device Auto-Synchronization, page 29-3](#)
- [Viewing the Status of Auto-Synchronization Pollers, page 29-9](#)
- [Field Descriptions for Auto Synchronization with Devices, page 29-9](#)
- [Additional References, page 29-11](#)
- [Feature History for Auto-Synchronization with Devices, page 29-11](#)

## Information About Auto-Synchronization with Devices

The Auto Synchronizing with Devices feature ensures that the Cisco Data Center Network Manager for LAN (DCNM-LAN) server has current configuration and status information about managed devices. The DCNM-LAN server creates one poller process for each device to retrieve the system and accounting logs that this feature requires.

When you choose Auto Synchronization with Devices on the Feature Selector pane, the Contents pane shows information about each poller process and allows you to control them.



You can configure the length of time that DCNM-LAN waits before polling a device again. DCNM-LAN sets a default polling interval for each managed device. The default value varies by the type of device. The range of polling interval values is displayed when you begin editing the polling interval field for the device. For more information, see the [“Configuring the Polling Interval” section on page 29-4](#).

DCNM-LAN polls devices concurrently; however, to avoid polling all devices simultaneously, DCNM-LAN begins polling devices in alphabetical device-name order and delays each polling process by a short, random amount of time.

This section includes the following topics:

- [Automatic and Manual Purging of Event Data, page 29-2](#)
- [Virtualization Support, page 29-2](#)

## Automatic and Manual Purging of Event Data

You can use the Auto-Synchronization with Devices feature to delete unwanted event data. DCNM-LAN supports automatic purging of event data. You can configure the following aspects of automatic event data purging:

- Days of the week and time of day that automatic purging occurs.
- Whether DCNM-LAN determines which event data to purge by the age of the data or by a maximum number of database entries.
- Severity level of events.

You can also manually purge event data.

## Virtualization Support

DCNM-LAN treats each virtual device context (VDC) on a Cisco NX-OS device as a separate device. DCNM-LAN creates one poller process per device.

# Licensing Requirements for Auto-Synchronization with Devices

The following table shows the licensing requirements for this feature:

| Product  | License Requirement                                                                                                                                                                                                                                                                                                                    |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCNM-LAN | Auto-Synchronization with Devices requires no license. Any feature not included in a license package is bundled with the DCNM-LAN 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 7.1.x</i> . |

## Prerequisites for Auto-Synchronization with Devices

The Auto-Synchronization with Devices feature has the following prerequisites:

- The DCNM-LAN server must be able to connect to the devices.
- The Cisco NX-OS device must be running a supported version of Cisco NX-OS.



- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the [“Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7](#).

## Guidelines and Limitations for Auto-Synchronization with Devices

The Auto-Synchronization with Devices feature has the following configuration guidelines and limitations:

- We recommend that you use the default device polling interval unless you encounter issues with synchronization due to slow responses from devices or to managing many devices. For more information, see the [“Configuring the Polling Interval” section on page 29-4](#).
- For the Auto-Synchronization with Devices feature, the DCNM-LAN client does not automatically update the information shown in the Summary pane. To ensure that you are viewing current information, from the menu bar, choose **View > Refresh**.
- We recommend that you configure automatic purging of event data to ensure that the DCNM-LAN database size does not grow too large.

## Configuring Device Auto-Synchronization

This section includes the following topics:

- [Starting and Stopping a Poller, page 29-3](#)
- [Configuring the Polling Interval, page 29-4](#)
- [Synchronizing with a Device, page 29-5](#)
- [Deleting Data from the Events Database, page 29-5](#)
- [Enabling and Disabling Automatic Event Purging, page 29-6](#)
- [Configuring Automatic Event Purge Settings, page 29-7](#)
- [Purging Events Now, page 29-8](#)

## Starting and Stopping a Poller

You can start and stop a poller for a device. When a poller is stopped, auto-synchronization for the device does not occur.

### DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

A table of pollers appears in the Contents pane. Each row corresponds to a poller for a particular device. Devices are listed alphabetically. The Poller Status field displays messages about whether the poller is running or is stopped.

- Step 2** Click to select the poller that you want to start or stop.



**Step 3** Do one of the following:

- To start a poller, from the menu bar, choose **Actions > Start Poller**. The Poller Status field changes to Running.
- To stop a poller, from the menu bar, choose **Actions > Stop Poller**. The Poller Status field changes to Stopped.

You do not need to save your changes.

---

**RELATED TOPICS**

- [Configuring the Polling Interval, page 29-4](#)
- [Synchronizing with a Device, page 29-5](#)

## Configuring the Polling Interval

You can configure how often the DCNM-LAN server synchronizes with managed devices. While synchronizing, the DCNM-LAN server fetches accounting and system logs from managed devices. This setting affects how frequently features in the DCNM-LAN client receive updated information about managed devices.

**BEFORE YOU BEGIN**

Determine how often you want DCNM-LAN to perform auto-synchronization with managed devices. Consider the following:

- How often device configurations are changed by means other than DCNM-LAN, such as using the command-line interface of a device. If changes by means other than DCNM-LAN are common, consider using a short polling interval.
- How important it is to your organization that DCNM-LAN be up to date with managed device configurations. If up-to-date configuration information is important to your organization, consider using a short polling interval.

**DETAILED STEPS**

- 
- |               |                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Feature Selector pane, choose <b>DCNM Server Administration &gt; Auto Synchronization with Devices</b> .                                                                                                                     |
|               | The polling intervals for all devices appear below the table of pollers in the Poller Setting tab.                                                                                                                                    |
| <b>Step 2</b> | Select the device in the Platform column that you want to work with.                                                                                                                                                                  |
| <b>Step 3</b> | In the Polling Interval field, enter the number of seconds between auto-synchronizations for the selected device. The range of polling interval values is displayed when you begin editing the Polling Interval field for the device. |
| <b>Step 4</b> | From the menu bar, choose <b>File &gt; Deploy</b> to save the polling interval.                                                                                                                                                       |
- 

**RELATED TOPICS**

- [Starting and Stopping a Poller, page 29-3](#)



- [Synchronizing with a Device, page 29-5](#)

## Synchronizing with a Device

You can make DCNM-LAN synchronize with a device manually when you do not want to wait for the next auto-synchronization to occur.

**Note**

If many configuration changes have occurred on the device since the last successful synchronization, consider performing device discovery instead of synchronization.

### BEFORE YOU BEGIN

Ensure that you have either configured the device entry with unique device credentials or that DCNM-LAN can use the default device credentials to connect to the device. For more information, see the [“Configuring Default Device Credentials”](#) section on page 28-4.

### DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.
- A table of pollers appears in the Contents pane. Each row corresponds to a poller for a particular device. Devices are listed alphabetically.
- Step 2** Click to select the device that you want DCNM-LAN to synchronize with.
- Step 3** From the menu bar, choose **Actions > Synchronize with Device**.
- Synchronization begins.
- To determine when the synchronization has finished, watch the Last Sync Status column. Typically, synchronization with a device occurs in less than 5 minutes.
- You do not need to save your changes.
- 

### RELATED TOPICS

- [Starting and Stopping a Poller, page 29-3](#)
- [Configuring the Polling Interval, page 29-4](#)

## Deleting Data from the Events Database

You can delete data from the events database based on the exact age of the events. Events that you delete can no longer appear in the Event Browser or on a feature-specific Events tab.

**Tip**

If you want to delete events based on the number of events in the database, see the [“Purging Events Now”](#) section on page 29-8.



## BEFORE YOU BEGIN

Determine the date and time of the newest events data that you want to delete. When you follow the steps in this procedure, DCNM-LAN deletes all events that are older than the date and time that you select.

## DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.
- The Events Database Administration tab appears in the Details pane, below the table of pollers.
- Step 2** From the Delete events older than drop-down list, choose the date and time of the newest event that you want to delete and click **OK**.
- Step 3** Click **Delete**.
- DCNM-LAN deletes all events older than the date and time that you specified.
- 

## RELATED TOPICS

- [Enabling and Disabling Automatic Event Purging, page 29-6](#)
- [Configuring Automatic Event Purge Settings, page 29-7](#)
- [Purging Events Now, page 29-8](#)

# Enabling and Disabling Automatic Event Purging

You can enable or disable the automatic purging of events from the DCNM-LAN events database.

## DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.
- The Events Database Administration tab appears in the Details pane, below the table of pollers.
- Step 2** Under Auto Purge Settings, do one of the following:
- To enable automatic event purging, check **Enable Auto Purge**.
  - To disable automatic event purging, uncheck **Enable Auto Purge**.
- Step 3** From the menu bar, choose **File > Deploy** to save your changes to the DCNM-LAN server.
- 

## RELATED TOPICS

- [Deleting Data from the Events Database, page 29-5](#)
- [Configuring Automatic Event Purge Settings, page 29-7](#)
- [Purging Events Now, page 29-8](#)



## Configuring Automatic Event Purge Settings

You can configure when automatic event purging occurs and the criteria that DCNM-LAN uses to determine which events to purge.

### BEFORE YOU BEGIN

Determine when you want automatic event purging to occur. We recommend that automatic event purging occur when DCNM-LAN usage is low.

If you perform backups of your DCNM-LAN databases, consider scheduling automatic event purging after database backups have occurred, to ensure that you retain a record of all events.

Determine what criteria you want DCNM-LAN to use to determine which events to purge. The criteria available are as follows:

- Age of event—DCNM-LAN can purge all events that are older than a specific number of days, weeks, or months.
- Number of events in the database—When the number of events in the database exceeds the maximum number that you specify, DCNM-LAN can purge the oldest events first until the maximum number is not exceeded.
- Severity of event—DCNM-LAN can purge events based on the severity level of the event.

If you enable both criteria, DCNM-LAN applies them independently of each other.

### DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The Events Database Administration tab appears in the Details pane, below the table of pollers.

- Step 2** Under Purge Threshold, configure the criteria that DCNM-LAN uses to determine which events to purge. You can configure any of the criteria in the following table:

| Purge Criteria                   | How to Configure                                                                                                                                                                                                                                                    |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Age of events                    | <ol style="list-style-type: none"><li>1. Check <b>Data older than</b>.</li><li>2. From the first drop-down list, choose the number of days, weeks, or months.</li><li>3. From the second drop-down list, choose <b>Days, Weeks, or Months</b>, as needed.</li></ol> |
| Number of events in the database | <ol style="list-style-type: none"><li>1. Check <b>Total Entries Exceed(0-2147483647)</b>.</li><li>2. In the box, enter the maximum number of entries that you want to allow in the events database.</li></ol>                                                       |
| Severity of event                | <ol style="list-style-type: none"><li>1. Check <b>Severity</b>. The list of eight severity levels becomes available.</li><li>2. For each severity level that you want DCNM-LAN to use to determine whether to purge events, check the severity level.</li></ol>     |



- Step 3** Under Auto Purge Settings, follow these steps to configure when you want automatic purging to occur:
- Check the days-of-the-week check boxes to specify which days of the week that you want automatic purging to occur.
  - Use the **Run at** box to configure the exact time on the specified days that you want automatic event purging to occur.
- Step 4** (Optional) If you want to enable automatic event purging, check **Enable Auto Purge**.
- Step 5** From the menu bar, choose **File > Deploy** to save your changes to the DCNM-LAN server.
- 

## RELATED TOPICS

- [Deleting Data from the Events Database, page 29-5](#)
- [Enabling and Disabling Automatic Event Purging, page 29-6](#)
- [Purging Events Now, page 29-8](#)

## Purging Events Now

You can purge event data on demand, using the automatic event purge settings to determine which events are purged. Events that you delete can no longer appear in the Event Browser or on a feature-specific Events tab.



**Tip**

If you want to delete events on demand, based on the exact age of the events, see the [“Deleting Data from the Events Database” section on page 29-5](#).

---

## BEFORE YOU BEGIN

Ensure that the automatic event purge settings are configured as needed. For more information, see the [“Configuring Automatic Event Purge Settings” section on page 29-7](#).

## DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.
- The Events Database Administration tab appears in the Details pane, below the table of pollers.
- Step 2** Under Purge, click **Purge Now**.
- DCNM-LAN deletes events, using the automatic event purge settings to determine which events to purge.
- 

## RELATED TOPICS

- [Deleting Data from the Events Database, page 29-5](#)
- [Enabling and Disabling Automatic Event Purging, page 29-6](#)
- [Configuring Automatic Event Purge Settings, page 29-7](#)



## Viewing the Status of Auto-Synchronization Pollers

To view the status of an auto-synchronization poller, from the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

Poller status and information about the synchronization time and status appear in the Pollers area in the Contents pane.

**Table 29-1**      **Auto Synchronization Pollers Information**

| Field             | Description                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pollers</b>    |                                                                                                                                                                                                                                        |
| Last Refresh Time | <i>Display only.</i> Date and time that the DCNM-LAN client updated information shown on the Contents pane.                                                                                                                            |
| Device            | <i>Display only.</i> Name and IP address of the device for the corresponding poller.                                                                                                                                                   |
| Poller Status     | <i>Display only.</i> Whether the poller is running or stopped. A running poller attempts to synchronize with the configuration and status information from its device at the frequency specified by the Device Polling Interval field. |
| Last Sync Time    | <i>Display only.</i> Date and time that the poller last retrieved system and accounting log data from the device.                                                                                                                      |
| Last Sync Status  | <i>Display only.</i> Whether the most recent synchronization attempt succeeded or failed. If synchronization failed, determine why DCNM-LAN failed to connect to the device. If necessary, rediscover the device.                      |

## Field Descriptions for Auto Synchronization with Devices

This section includes the following field descriptions for the Auto Synchronization with Devices feature:

- [Poller Setting Tab, page 29-9](#)
- [Events Database Administration Tab, page 29-10](#)

### Poller Setting Tab

**Table 29-2**      **Auto Synchronization with Devices Poller Setting Tab**

| Field            | Description                                                                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pollers</b>   |                                                                                                                                                                                                                   |
| Polling Interval | Number of seconds that all pollers wait before the next attempt to synchronize with a device. The range of polling interval values is displayed when you begin editing the Polling Interval field for the device. |
| Device           | <i>Display only.</i> Name and IP address of the device for the corresponding poller.                                                                                                                              |



## Events Database Administration Tab

**Table 29-3** *Events Database Administration Tab*

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete events older than   | Date and time of the newest event to be deleted from the events database. There is no default value for this field.                                                                                                                                                                                                                                                                                                                                         |
| <b>Purge Threshold</b>     |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Data older than            | Whether, during automatic event purging, DCCM-LAN deletes events that are older than the age specified in the drop-down lists located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default age is 1 day.                                                                                                                                                                                        |
| Total Entries Exceed       | Whether, during automatic event purging, DCCM-LAN deletes the oldest events until the number of events equals the number in the box located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default number of event is 25,000.                                                                                                                                                                     |
| Severity                   | Whether, during automatic event purging, DCCM-LAN deletes events with severity levels that are selected from the list of severity levels. By default, this check box is disabled.                                                                                                                                                                                                                                                                           |
| Severity Levels            | Severity levels of events that DCCM-LAN deletes during automatic event purging. The severity levels are available only if the Severity check box is checked. By default, all severity levels are disabled. The severity levels are as follows: <ul style="list-style-type: none"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debugging</li> </ul> |
| <b>Auto Purge Settings</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Enable Auto Purge          | Whether automatic purging of event data is enabled. By default, this check box is disabled.                                                                                                                                                                                                                                                                                                                                                                 |
| Run on                     | Days of the week that the automatic purging of events data occurs. By default, none of the check boxes are checked. If you check the Daily check box, the check boxes for the individual days of the week become unavailable.                                                                                                                                                                                                                               |
| Run at                     | Time of day that automatic purging of event data occurs, on the days of the week that automatic purging is enabled.                                                                                                                                                                                                                                                                                                                                         |



# Additional References

For additional information related to administering Auto-Synchronization with Devices, see the following sections:

- [Related Documents, page 29-11](#)
- [Standards, page 29-11](#)

## Related Documents

| Related Topic    | Document Title                                                                  |
|------------------|---------------------------------------------------------------------------------|
| Events           | <i>System Management Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i> |
| Device discovery | <a href="#">Chapter 27, “Administering Device Discovery”</a>                    |

## Standards

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

# Feature History for Auto-Synchronization with Devices

[Table 29-4](#) lists the release history for this feature.

**Table 29-4** Feature History for Auto-Synchronization with Devices

| Feature Name                      | Releases | Feature Information         |
|-----------------------------------|----------|-----------------------------|
| Auto-Synchronization with Devices | 5.0(2)   | No change from Release 4.2. |









# CHAPTER 30

## Administering Statistical Data Collection

---

This chapter describes how to administer Statistical Data Collection in the Cisco Data Center Network Manager for LAN (DCNM-LAN).

You can use the Statistical Data Collection feature to control the statistics monitoring processes that you have created for one of the many device configuration features that support statistics. You can also use the Statistical Data Collection feature to delete unwanted statistical data on demand or automatically.

This chapter includes the following sections:

- [Information About Statistical Data Collection, page 30-1](#)
- [Licensing Requirements for Statistical Data Collection, page 30-2](#)
- [Prerequisites for Statistical Data Collection, page 30-2](#)
- [Guidelines and Limitations for Statistical Data Collection, page 30-3](#)
- [Configuring Statistical Data Collection, page 30-3](#)
- [Viewing the Status of Statistical Data Collectors, page 30-10](#)
- [Field Descriptions for Statistical Data Collection, page 30-10](#)
- [Additional References, page 30-11](#)
- [Feature History for Statistical Data Collection, page 30-12](#)

## Information About Statistical Data Collection

You can use the Statistical Data Collection feature to control the statistics monitoring processes that you have created for one of the many device configuration features that support statistics.

When you choose Statistical Data Collection on the Feature Selector pane, the Contents pane shows information about each statistical collection and allows you to control them. You can also use this feature to purge old data from the statistical database.

You can configure the length of time that Cisco Data Center Network Manager for LAN (DCNM-LAN) waits before retrieving statistical data from devices that it is monitoring. By default, DCNM-LAN retrieves statistical data from monitored devices every 30 seconds. You can increase the length of time to a maximum of 4 minutes. For more information, see the [“Configuring Monitoring Preferences” section on page 14-17](#).

This section includes the following topics:

- [Automatic and Manual Purging of Statistical Data, page 30-2](#)
- [Virtualization Support, page 30-2](#)



## Automatic and Manual Purging of Statistical Data

You can use the Statistical Data Collection feature to delete unwanted statistical data. DCNM-LAN supports automatic purging of statistical data. You can configure the following aspects of automatic statistical data purging:

- Days of the week and time of day that automatic purging occurs.
- Whether DCNM-LAN determines which statistical data to purge by the age of the data or by a maximum number of database entries.
- Whether DCNM-LAN deletes the statistical data entries that it purges or consolidates them into one entry.

You can also manually purge statistical data.

## Virtualization Support

DCNM-LAN treats each virtual device context (VDC) on a Cisco NX-OS device as a separate device. Statistical data collections contain statistics from objects within devices.

## Licensing Requirements for Statistical Data Collection

The following table shows the licensing requirements for this feature:

| Product        | License Requirement                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco DCNM-LAN | <p>Real-time monitoring requires no license.</p> <p>Cisco DCNM-LAN requires a LAN Enterprise license for the following features:</p> <ul style="list-style-type: none"> <li>• Maintaining a history of statistical data</li> <li>• Using overview charts</li> </ul> <p>For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the <i>Cisco DCNM Installation and Licensing Guide, Release 7.1.x</i>.</p> |

## Prerequisites for Statistical Data Collection

Statistical data collection has the following prerequisites:

- The DCNM-LAN server must be able to connect to the devices.
- The system clocks for the DCNM-LAN server and DCNM-LAN client must be synchronized. If the system clocks are not synchronized, scheduling tasks for data collection may start or end at incorrect times.
- The Cisco NX-OS device must be running a supported version of Cisco NX-OS.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the [“Verifying the Discovery Readiness of a Cisco NX-OS Device” section on page 27-7](#).



# Guidelines and Limitations for Statistical Data Collection

The Statistical Data Collection feature has the following configuration guidelines and limitations:

- Collections are created by starting monitoring for a new chart. For more information, see the [“Starting Statistical Monitoring for a Chart” section on page 14-12](#).
- For the Statistical Data Collection feature, the DCNM-LAN client does not automatically update the information shown in the Summary pane. To ensure that you are viewing current information, from the menu bar, choose **View > Refresh**.
- When you start statistical monitoring for one or more charts and then close the DCNM-LAN client, a dialog box prompts you to decide whether to stop the collections or let them run. We recommend that you stop any unnecessary collections when you log out of the DCNM-LAN client. This practice conserves database space and decreases the server load.
- We recommend that you configure automatic purging of statistical data to ensure that the DCNM-LAN database size does not grow too large.
- You cannot always map the statistics data with the data collectors scheduler. However, a single scheduler can collect data for multiple graphs, and therefore, the statistics chart name need not match the data collector scheduler.

## Configuring Statistical Data Collection

This section includes the following topics:

- [Starting and Stopping Statistical Data Collection, page 30-3](#)
- [Using Modes in Statistics Charts, page 30-4](#)
- [Deleting Statistical Data from a Collection, page 30-5](#)
- [Deleting a Collection, page 30-6](#)
- [Deleting Data from the Statistics Database, page 30-6](#)
- [Enabling and Disabling Automatic Statistical Data Purging, page 30-7](#)
- [Configuring Automatic Statistical Data Purge Settings, page 30-8](#)
- [Purging Statistical Data Now, page 30-9](#)

## Starting and Stopping Statistical Data Collection

You can use the Statistical Data Collection feature to start and stop a statistical data collection process. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

### DETAILED STEPS

- 
- |               |                                                                                                                                                                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Feature Selector pane, choose <b>DCNM Server Administration &gt; Statistical Data Collection</b> .<br><br>A table of statistical data collectors appears in the Contents pane. Each row corresponds to a collector for a particular device. The Status field displays whether the collector is running or is stopped. |
| <b>Step 2</b> | Click the collector that you want to start or stop.                                                                                                                                                                                                                                                                            |



**Step 3** Do one of the following:

- To start a collector, from the menu bar, choose **Actions > Start Collection**. The Status field changes to Running.
- To stop a collector, from the menu bar, choose **Actions > Stop Collection**. The Status field changes to Stopped.

You do not need to save your changes.

## Using Modes in Statistics Charts

You use statistics charts to toggle between the delta mode and the rate mode. The below table lists the features that contain statistics charts and delta mode/rate mode toggle button.

| Path                         | Feature               |
|------------------------------|-----------------------|
| Interfaces > Physical        | Ethernet Interface    |
| Interfaces > Physical        | Management Interface  |
| Interfaces > Logical         | Loopback Interface    |
| Interfaces > Logical         | Port Channel          |
| Interfaces > Logical         | vPC                   |
| Switching                    | VLAN                  |
| Switching > Spanning Tree    | Rapid PVST+           |
| Switching > Spanning Tree    | MST                   |
| Switching > Fabricpath       | ISIS Process          |
| Switching > Layer 2 Security | Port Security         |
| Switching > Layer 2 Security | ARP Inspection        |
| Switching > Layer 2 Security | DHCP Snooping         |
| Switching > Layer 2 Security | Traffic Storm Control |
| Switching > Layer 2 Security | IGMP Snooping         |
| Security                     | DOT1x                 |
| Security > Access Control    | IPv4 ACL              |
| Security > Access Control    | IPv6 ACL              |
| Security > Access Control    | MAC ACL               |
| Security > AAA               | Server Groups         |
| Inventory                    | Virtual Switch        |

### DETAILED STEPS

- Step 1** From the Feature Selector pane, choose the appropriate feature. For example, if you wanted to see statistics for the Ethernet feature, choose **Interfaces > Physical > Ethernet**.

The available devices appear in the Summary pane.



- 
- Step 2** From the Summary pane, double-click the device.
- Step 3** From the Summary pane, double-click **Slots**.
- Step 4** Click the interface.
- Step 5** From the Details pane, choose the **Statistics** tab.
- Step 6** In the toolbar, click **New Chart** and then from the menu bar drop-down list, choose the chart that you want to view. For example, if you wanted to see statistics for traffic, choose **Traffic Statistics Chart**.
- Step 7** (Optional) To toggle between the statistics mode and the rate mode, click the button to the right of the Select Frequency drop-down list.
- 

## RELATED TOPICS

- [Deleting Statistical Data from a Collection, page 30-5](#)
- [Deleting a Collection, page 30-6](#)

## Deleting Statistical Data from a Collection

You can delete statistical data from a collection. This feature allows you to delete all the data from a collection without affecting data from other collections and without deleting the collection itself. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

## DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.  
A table of statistical data collectors appears in the Contents pane. Each row corresponds to a collector for a particular device. Devices are listed alphabetically. The Status field displays whether the collector is running or is stopped.
- Step 2** Right-click the collection.
- Step 3** From the menu bar, choose **Actions > Delete Statistical Data**.  
DCNM-LAN deletes all statistical data from the collection.
- 

## RELATED TOPICS

- [Starting and Stopping Statistical Data Collection, page 30-3](#)
- [Deleting a Collection, page 30-6](#)
- [Deleting Data from the Statistics Database, page 30-6](#)
- [Starting Statistical Monitoring for a Chart, page 14-12](#)



## Deleting a Collection

You can delete a collection of statistical data from a specific device. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

**Note**

If you want to delete all data from a collections rather than deleting the collection itself, perform the steps in the [“Deleting Statistical Data from a Collection” section on page 30-5](#).

### BEFORE YOU BEGIN

Determine which collection of data you want to delete.

### DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**. A table of statistical data collectors appears in the Contents pane. Devices are listed alphabetically. Each row corresponds to a collection of statistical data for a particular device.
- Step 2** Click the collection of data that you want to delete.
- Step 3** From the menu bar, choose **Actions > Delete Collection**.  
The collection is deleted.  
You do not need to save your changes.
- 

### RELATED TOPICS

- [Starting and Stopping Statistical Data Collection, page 30-3](#)
- [Deleting Statistical Data from a Collection, page 30-5](#)
- [Deleting Data from the Statistics Database, page 30-6](#)
- [Starting Statistical Monitoring for a Chart, page 14-12](#)

## Deleting Data from the Statistics Database

You can delete statistical data from the statistics database.

**Note**

If you want to delete all data from a specific collection rather than deleting old data from all collections, perform the steps in the [“Deleting a Collection” section on page 30-6](#).

### BEFORE YOU BEGIN

Determine the date and time of the newest statistical data that you want to delete. When you follow the steps in this procedure, DCNM-LAN deletes all statistics that are older than the date and time that you select.



## DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**. The Statistics Database area appears in the Contents pane, below the table of statistical data collectors.
- Step 2** From the Delete statistical data older than drop-down list, select the date and time of the newest statistics that you want to delete and click **OK**.
- Step 3** Click **Delete**.  
DCNM-LAN deletes all statistics older than the date and time that you specified.
- 

## RELATED TOPICS

- [Deleting Statistical Data from a Collection, page 30-5](#)
- [Deleting a Collection, page 30-6](#)
- [Enabling and Disabling Automatic Statistical Data Purging, page 30-7](#)
- [Configuring Automatic Statistical Data Purge Settings, page 30-8](#)
- [Purging Statistical Data Now, page 30-9](#)

# Enabling and Disabling Automatic Statistical Data Purging

You can enable or disable the automatic purging of statistical data from the DCNM-LAN statistics database.

## DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**. The Statistical Database Administration tab appears in the Details pane, below the table of statistical data collectors.
- Step 2** Under Auto Purge Settings, do one of the following:
- To enable automatic statistical data purging, check **Enable Auto Purge**.
  - To disable automatic statistical data purging, uncheck **Enable Auto Purge**.
- Step 3** From the menu bar, choose **File > Deploy** to save your changes to the DCNM-LAN server.
- 

## RELATED TOPICS

- [Deleting Data from the Statistics Database, page 30-6](#)
- [Configuring Automatic Statistical Data Purge Settings, page 30-8](#)
- [Purging Statistical Data Now, page 30-9](#)



# Configuring Automatic Statistical Data Purge Settings

You can configure when automatic statistical data purging occurs and the criteria that DCNM-LAN uses to determine which statistical data to purge.

## BEFORE YOU BEGIN

Determine when you want automatic statistical data purging to occur. A good recommendation is that you configure automatic statistical data purging to occur when DCNM-LAN usage is low.

If you perform backups of your DCNM-LAN databases, consider scheduling automatic statistical data purging after database backups have occurred, to ensure that you retain a record of all statistical data.

Determine what criteria you want DCNM-LAN to use to determine which statistical data to purge. The two criteria available are as follows:

- Age of statistical data—DCNM-LAN can purge all statistical data entries that are older than a specific number of days, weeks, or months.
- Number of statistical data entries in the database—When the number of statistical data entries in the database exceeds the maximum number that you specify, DCNM-LAN can purge the oldest statistical data entries first until the maximum number is not exceeded.

If you enable both criteria, DCNM-LAN applies them independently of each other.

## DETAILED STEPS

- Step 1

From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.  
The Statistical Database Administration tab appears in the Details pane, below the table of statistical data collectors.
- Step 2

Under Purge Threshold, configure the criteria that DCNM-LAN uses to determine which statistical data to purge. You can configure either or both of the criteria using the information in [Table 30-1](#).

Table 30-1 Purge Criteria

| Purge Criteria                                     | How to Configure                                                                                                                                                                                                                     |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Age of statistical data                            | <div>1. Check <b>Data older than</b>.</div> <div>2. From the first drop-down list, choose the number of days, weeks, or months.</div> <div>3. From the second drop-down list, choose <b>Days, Weeks, or Months</b>, as needed.</div> |
| Number of statistical data entries in the database | <div>1. Check <b>Stats. Entries Exceed(0-2147483647)</b>.</div> <div>2. In the box, enter the maximum number of entries that you want to allow in the statistical database.</div>                                                    |

- Step 3

Configure the action that you want DCNM-LAN to take on statistical database entries that meet the purge criteria. You can choose one of the following:



- **Delete**—DCNM-LAN deletes the database entries that meet the purge criteria.
- **Consolidate**—DCNM-LAN merges all statistical data entries that meet the purge criteria into one entry

- Step 4** Under Auto Purge Settings, follow these steps to configure when you want automatic purging to occur:
- a. Check the days-of-the-week check boxes to specify which days of the week that you want automatic purging to occur.
  - b. Use the **Run at** box to configure the exact time on the specified days that you want automatic statistical data purging to occur.
- Step 5** (Optional) If you want to enable automatic statistical data purging, check **Enable Auto Purge**.
- Step 6** From the menu bar, choose **File > Deploy** to save your changes to the DCNM-LAN server.
- 

## RELATED TOPICS

- [Deleting Data from the Statistics Database, page 30-6](#)
- [Enabling and Disabling Automatic Statistical Data Purging, page 30-7](#)
- [Purging Statistical Data Now, page 30-9](#)

## Purging Statistical Data Now

You can purge statistical data on demand, using the automatic statistical data purge settings to determine which statistical data are purged.



**Tip**

If you want to delete statistical data on demand, based on the exact age of the statistical data entries, see the [“Deleting Data from the Statistics Database” section on page 30-6](#).

---

## BEFORE YOU BEGIN

Ensure that the automatic statistical data purge settings are configured as needed. For more information, see the [“Configuring Automatic Statistical Data Purge Settings” section on page 30-8](#).

## DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**. The Statistical Database Administration tab appears in the Details pane, below the table of statistical data collectors.
- Step 2** Under Purge, click **Purge Now**. DCNM-LAN deletes statistical data, using the automatic statistical data purge settings to determine which statistical data entries to purge.
- 

## RELATED TOPICS

- [Deleting Data from the Statistics Database, page 30-6](#)



- [Enabling and Disabling Automatic Statistical Data Purging, page 30-7](#)
- [Configuring Automatic Statistical Data Purge Settings, page 30-8](#)

## Viewing the Status of Statistical Data Collectors

To view the status of statistical data collectors, from the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

Collector status and other information appear in the Statistical Data Collectors area in the Contents pane. For information about the fields that appear, see the [“Field Descriptions for Statistical Data Collection” section on page 30-10](#).

## Field Descriptions for Statistical Data Collection

This section includes the following field descriptions for the Statistical Data Collection feature:

- [Summary Pane, page 30-10](#)
- [Statistical Database Administration Tab, page 30-11](#)

### Summary Pane

**Table 30-2**      **Summary Pane**

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Statistical Data Collectors</b> |                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Last Refresh Time                  | <i>Display only.</i> Date and time that the DCNM-LAN client updated information shown on the Content pane.                                                                                                                                                                                                                                                                                                         |
| Collector ID                       | <i>Display only.</i> Name and IP address of the device for the corresponding poller.                                                                                                                                                                                                                                                                                                                               |
| Owner                              | <i>Display only.</i> Username of the DCNM-LAN user who started monitoring for the chart that corresponds to the collection.                                                                                                                                                                                                                                                                                        |
| Device                             | <i>Display only.</i> Name and IP address of the device that is providing the statistical data in the collection.                                                                                                                                                                                                                                                                                                   |
| Objects                            | <p><i>Display only.</i> Description of the entity on the device that is providing the statistical data in the collection.</p> <p>For example, if the collection has statistical data for a rule that is assigned the sequence number 10 and is in an IPv4 ACL named acl-01, this field displays acl-01,seqNo=10.</p> <p>If the collection has data for the Ethernet 1/5 port, this field displays Ethernet1/5.</p> |
| Collected Statistics               | <i>Display only.</i> Type of statistical data in the collection. For example, if the collection has statistical data for a rule in an IPv4 ACL, this field displays IpAclAceMatchStatistics.                                                                                                                                                                                                                       |
| Status                             | <i>Display only.</i> Whether the collector is started or stopped.                                                                                                                                                                                                                                                                                                                                                  |



**Table 30-2** *Summary Pane (continued)*

| Field                              | Description                                                                                                                        |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>Statistics Database</b>         |                                                                                                                                    |
| Delete statistical data older than | Date and time of the newest statistical data to be deleted from the statistics database. There is no default value for this field. |

## Statistical Database Administration Tab

**Table 30-3** *Statistical Database Administration Tab*

| Field                              | Description                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete statistical data older than | Date and time of the newest statistical data to be deleted from the statistics database. There is no default value for this field.                                                                                                                                                                              |
| <b>Purge</b>                       |                                                                                                                                                                                                                                                                                                                 |
| Action                             | Whether automatic statistical data purging deletes or consolidates statistical data entries that trigger the purge threshold. Consolidation merges all statistical data entries that trigger the purge threshold into one entry.                                                                                |
| <b>Purge Threshold</b>             |                                                                                                                                                                                                                                                                                                                 |
| Data older than                    | Whether, during automatic statistical data purging, DCNM-LAN deletes statistics entries that are older than the age specified in the drop-down lists located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default age is 1 day.                     |
| Stat. Entries Exceed               | Whether, during automatic statistical data purging, DCNM-LAN deletes the oldest statistics entries until the number of entries equals the number in the box located to the right of this check box. By default, this check box is unchecked. If you check the check box, the default number of event is 25,000. |
| <b>Auto Purge Settings</b>         |                                                                                                                                                                                                                                                                                                                 |
| Enable Auto Purge                  | Whether automatic purging of statistical data is enabled. By default, this check box is disabled.                                                                                                                                                                                                               |
| Run on                             | Days of the week that automatic purging of statistical data occurs. By default, none of the check boxes are checked. If you check the Daily check box, the check boxes for the individual days of the week become unavailable.                                                                                  |
| Run at                             | Time of day that automatic purging of statistical data occurs, on the days of the week that automatic purging is enabled.                                                                                                                                                                                       |

## Additional References

For additional information related to administering statistical data collection, see the following sections:

- [Related Documents, page 30-12](#)
- [Standards, page 30-12](#)



## Related Documents

| Related Topic    | Document Title                                               |
|------------------|--------------------------------------------------------------|
| Device discovery | <a href="#">Chapter 27, “Administering Device Discovery”</a> |

## Standards

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

## Feature History for Statistical Data Collection

[Table 30-4](#) lists the release history for this feature.

**Table 30-4**      **Feature History for Statistical Data Collection**

| Feature Name                | Releases | Feature Information         |
|-----------------------------|----------|-----------------------------|
| Statistical Data Collection | 5.0(2)   | No change from Release 4.2. |





# CHAPTER 31

## Working With Threshold Rules

---

This chapter describes how to configure threshold rules using Cisco Data Center Network Manager for LAN (DCNM-LAN).

This chapter includes the following sections:

- [Information About Threshold Rules, page 31-1](#)
- [Licensing Requirements for Threshold Rules, page 31-5](#)
- [Configuring Threshold Rules, page 31-5](#)
- [Additional References, page 31-9](#)
- [Feature History for Threshold Rules, page 31-9](#)

## Information About Threshold Rules

This section includes the following topics:

- [Threshold Rules Overview, page 31-1](#)
- [Threshold Rule Examples, page 31-2](#)

## Threshold Rules Overview

DCNM-LAN provides a feature that you use to specify rising or falling threshold rules for sample variables in collected statistical data. Depending on the rule definition, a set of actions are performed by DCNM-LAN. You define the threshold rule on the Threshold Rules page, and you apply the threshold rule to the existing chart.

This section includes the following topics:

- [Rising Threshold, page 31-2](#)
- [Falling Threshold, page 31-2](#)
- [Threshold Rule Properties, page 31-2](#)
- [Threshold Rule Actions, page 31-2](#)



## Rising Threshold

The rising threshold is the upper threshold for a sample variable. When the current sampled variable is greater than or equal to the specified threshold, a set of actions is performed.

## Falling Threshold

The falling threshold is the lower threshold for a sample variable. When the current sampled variable is lower than or equal to the specified threshold a set of actions is performed.

**Note**

You can specify only one rising threshold and one falling threshold for a single sampled variable.

## Threshold Rule Properties

Threshold rule properties are as follows:

- Name—Specifies the threshold rule name.
- Frequency—Specifies the number of times the sampled variable must cross a threshold before triggering any actions.
- Period—Specifies the interval of time the frequency is monitored.
- Repeat—Prevents the timer from resetting after triggering an action within the period.
- Trend—Specifies the rising or falling threshold.

## Threshold Rule Actions

Threshold rule actions are as follows:

- Send an email or SMS to a mail server or mail to SMS gateway.
- Run a script on the server.
- Send an event to the current DCNM JMS channel.

## Threshold Rule Examples

**Note**

The granularity of a period is driven by the minimal interval of the collected data. Consequently, the period must be higher than that interval.

This section includes the following topics:

- [Triggering an Action Each Time a Threshold is Crossed, page 31-2](#)
- [Triggering an Action Only Once in a Period When a Threshold is Crossed, page 31-3](#)
- [Triggering an Action Every Fourth Period When a Threshold is Crossed, page 31-4](#)

## Triggering an Action Each Time a Threshold is Crossed

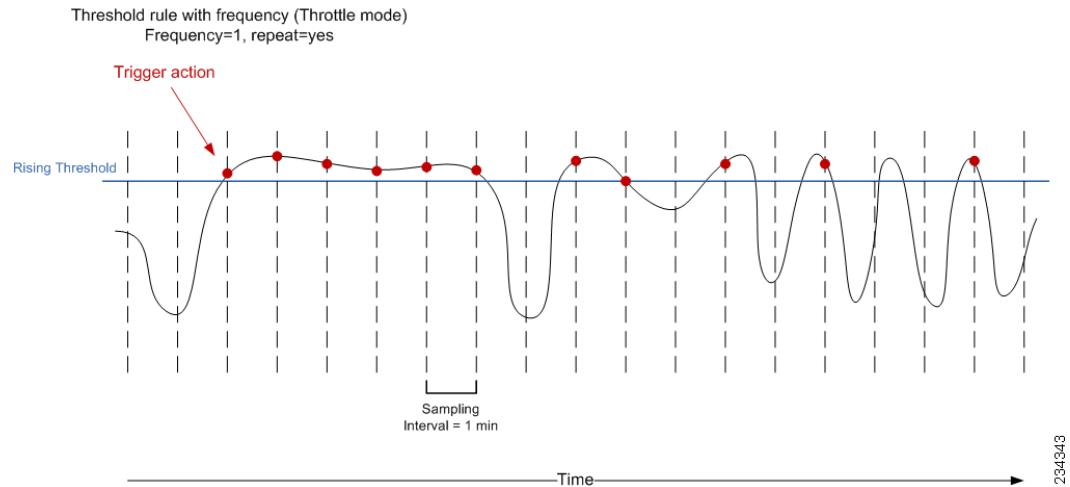
To trigger an action each time a threshold is crossed, set properties as follows:



- Frequency—**1**
- Repeat—**Yes**

Figure 31-1 shows the trigger action when you set rule properties to the preceding values.

**Figure 31-1** *Trigger an Action Each Time a Threshold is Crossed*



If the sampled variable crosses the threshold, an action is taken the first time it crosses the threshold. As a result, an action is performed each time the threshold is crossed.

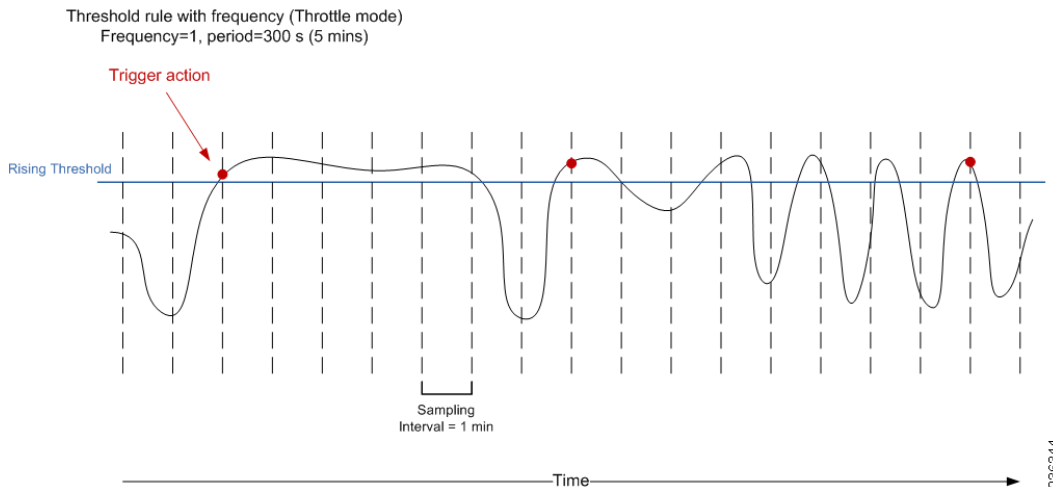
## Triggering an Action Only Once in a Period When a Threshold is Crossed

To trigger an action only once in a period when a threshold is crossed, set properties as follows:

- Frequency—**1**
- Period—**300**
- Repeat—**No**

Figure 31-2 shows the trigger action when you set rule properties to the preceding values.



**Figure 31-2** *Trigger an Action Only Once When a Threshold is Crossed Within a Period*

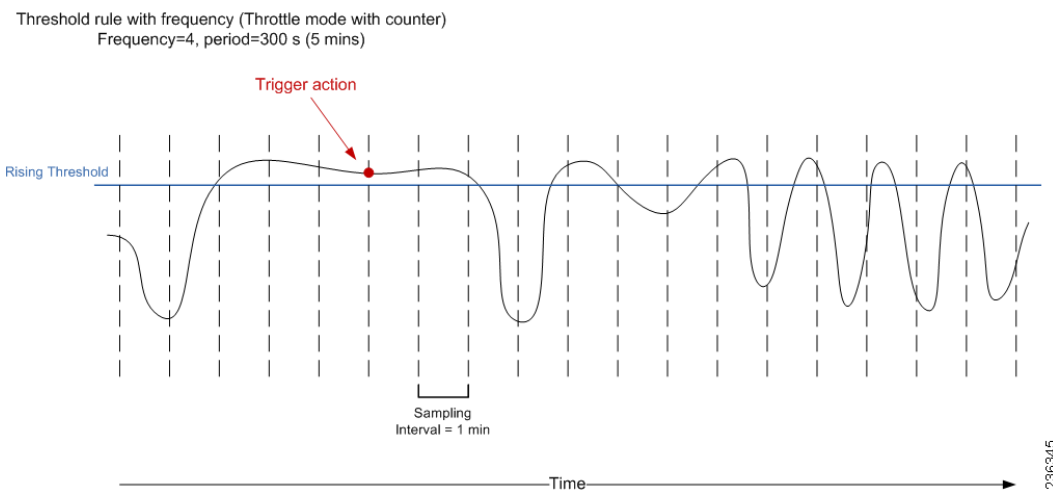
If the sampled variable crosses the threshold, an action is taken the first time it crosses the threshold. For the remaining 5 minutes, an action will not be taken. As a result, an action is performed only once during the specified period.

## Triggering an Action Every Fourth Period When a Threshold is Crossed

To trigger an action every fourth period when a threshold is crossed, set properties as follows:

- Frequency—**4**
- Period—**300**
- Repeat—**No**

Figure 31-3 shows the trigger action when you set rule properties to the preceding values.

**Figure 31-3** *Trigger an Action Every Fourth Period When a Threshold is Crossed*

If the sampled variable crosses the threshold, an action is taken the fourth time it crosses the threshold. For the remaining 5 minutes, an action is not taken. As a result, an action is performed only once during the specified period.



# Licensing Requirements for Threshold Rules

The following table shows the licensing requirements for this feature:

| Product        | License Requirement                 |
|----------------|-------------------------------------|
| Cisco DCNM-LAN | Threshold rules require no license. |

## Configuring Threshold Rules

You can create and apply threshold rules using the Threshold Rules feature. With this feature, you can create, delete, edit, view, and apply a rule to a chart.

The following sections provide more details about the feature.

- Creating Threshold Rules
- Deleting Threshold Rules
- Editing Threshold Rules
- Viewing Threshold Rules
- Applying a Threshold Rule to a Chart

This section includes the following topics:

- [Creating Threshold Rules, page 31-5](#)
- [Deleting Threshold Rules, page 31-7](#)
- [Editing Threshold Rules, page 31-8](#)
- [Viewing Threshold Rules, page 31-8](#)
- [Applying a Threshold Rule to a Chart, page 31-8](#)

## Creating Threshold Rules

You can create threshold rules using DCNM-LAN.

### DETAILED STEPS

**Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Threshold Rules**.

**Step 2** From the toolbar, choose **New**, and then choose **New Threshold Rule**.

The Details and Threshold Bindings tabs appear in the Details pane, with the Details tab open.

**Step 3** Create a threshold rule as follows:

- a. In the Name field, enter a name.
- b. In the Description field, enter a description of the threshold rule.

After you have enter a description, the Rising Threshold check box is automatically checked and the Threshold field in the Settings area is outlined in red.



**Note**

A field outlined in red indicates that an entry is required. A field outlined in yellow indicates that the entry is satisfactory.

- c. In the Settings area, enter a value in the Threshold field.

Once you have entered a value, the three options in the Action area are outlined in red.

- d. In the Action area, provide one of the following:

- Enter email addresses (delimited with commas)
- Select **Sent Event** to forward events to the DCNM-LAN Event Browser
- Enter a script name

The script receives all data regarding the crossed threshold. The script can be written in any programming language and saved in one of the directories of the system PATH.

[Table 31-1](#) describes the available parameters.

**Table 31-1**      **Parameters Passed to Script**

| Parameter | Description                                                                                                                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| \$1       | Device name                                                                                                                                                                                                                                                                        |
| \$2       | Threshold name                                                                                                                                                                                                                                                                     |
| \$3       | Timestamp                                                                                                                                                                                                                                                                          |
| \$4       | Severity                                                                                                                                                                                                                                                                           |
| \$5       | Monitored metric that is a counter or a non-counter. <ul style="list-style-type: none"> <li>• When used as a counter, it represents a rate in metric units /second.</li> <li>• When used as a non-counter, it represents an absolute in metric units.</li> </ul>                   |
| \$6       | Threshold for the monitored metric that is a counter or a non-counter. <ul style="list-style-type: none"> <li>• When used as a counter, it represents a rate in metric units /second.</li> <li>• When used as a non-counter, it represents an absolute in metric units.</li> </ul> |
| \$7       | Trend type<br>The possible values are: <ul style="list-style-type: none"> <li>• <b>rate</b><br/>which is a counter.</li> <li>• <b>absolute</b><br/>which is a non-counter</li> </ul>                                                                                               |



**Table 31-1 Parameters Passed to Script**

| Parameter | Description                                                                                                                         |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------|
| \$8       | Threshold type<br>The possible values are: <ul style="list-style-type: none"><li>• <b>rising</b></li><li>• <b>falling</b></li></ul> |
| \$9       | Statistic class                                                                                                                     |
| \$10      | Statistic variable                                                                                                                  |
| \$11      | Source object                                                                                                                       |

**Note**

Ensure that the DCNM-LAN server is configured for an SMTP server. For more information about configuring the DCNM-LAN server, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

- e. (Optional) In the corresponding Settings and Action areas, configure a Falling Threshold.
- f. (Optional) Click the **Threshold Bindings** tab to view bindings.
- g. Click **Deploy**.

The rule is deployed.

When you exit DCNM-LAN and Save Pending Changes is checked in the Warning dialog box, click **Yes** to save the rule.

## Deleting Threshold Rules

You can delete rules using DCNM-LAN.

### DETAILED STEPS

- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Threshold Rules**.  
The rules appear in the Summary pane.
- Step 2** From the Summary pane, right-click the appropriate rule.
- Step 3** From the drop-down list, choose **Delete Threshold Rule**.  
A warning dialog box appears and displays “Are you sure you want to delete?”
- Step 4** Click **Yes**.  
The rule is deleted.



## Editing Threshold Rules

You can view threshold rules using DCNM-LAN.

### DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Threshold Rules**.  
The rules appear in the Summary pane.
- Step 2** Edit any appropriate areas.

**Note**

You cannot edit the Name field.

---

## Viewing Threshold Rules

You can view threshold rules using DCNM-LAN.

### DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose **DCNM Server Administration > Threshold Rules**.  
The rules appear in the Summary pane.
- Step 2** Click on a rule to view it.
- 

## Applying a Threshold Rule to a Chart

You can apply threshold rules using DCNM-LAN.

### DETAILED STEPS

- 
- Step 1** From the Feature Selector pane, choose the appropriate feature. For example, if you wanted to see statistics for an Ethernet port, choose **Interfaces > Physical > Ethernet**.  
The available devices appear in the Summary pane.
- Step 2** From the Summary pane, choose the appropriate device.
- Step 3** Click the **Statistics** tab.
- Step 4** In the toolbar, click **New Chart** and then from the drop-down list choose the chart that you want to view. For example, if you wanted to see statistics for traffic, choose **Traffic Statistics Chart**.
- Step 5** In the chart toolbar, click **Launch Threshold Setting**.
-



# Additional References

For additional information related to administering threshold rules, see the following sections:

- [Related Documents, page 31-9](#)
- [Standards, page 31-9](#)

## Related Documents

| Related Topic               | Document Title                                                                  |
|-----------------------------|---------------------------------------------------------------------------------|
| Events                      | <i>System Management Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i> |
| Statistical Data Collection | <a href="#">Chapter 30, “Administering Statistical Data Collection”</a>         |

## 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 Threshold Rules

[Table 31-2](#) lists the release history for this feature.

**Table 31-2** Feature History for Threshold Rules

| Feature Name    | Releases | Feature Information |
|-----------------|----------|---------------------|
| Threshold Rules | 5.2(0)   | —                   |









## CHAPTER 32

# Administering DCNM-LAN Server Log Settings

This chapter describes how to administer the DCNM-LAN Server Log Settings feature in Cisco Data Center Network Manager for LAN (DCNM-LAN).

The Cisco DCNM server maintains a log file of its operations. The log file contains information from Cisco DCNM features and server components.



**Note**

The DCNM Server Log Settings feature does not affect logging levels of Cisco NX-OS devices. Cisco DCNM does not support the configuration of device logging levels.

This chapter includes the following sections:

- [Information About Administering DCNM-LAN Server Log Settings, page 32-1](#)
- [Licensing Requirements for Administering DCNM-LAN Server Log Settings, page 32-2](#)
- [Prerequisites for Administering DCNM-LAN Server Log Settings, page 32-3](#)
- [Guidelines and Limitations for Administering DCNM-LAN Server Log Settings, page 32-3](#)
- [Configuring DCNM-LAN Server Log Settings, page 32-3](#)
- [Viewing DCNM-LAN Server Log Settings, page 32-5](#)
- [Field Descriptions for DCNM-LAN Server Log Settings, page 32-5](#)
- [Additional References, page 32-7](#)
- [Feature History for DCNM-LAN Server Log Settings, page 32-7](#)

## Information About Administering DCNM-LAN Server Log Settings

The DCNM-LAN server maintains a log file of its operations. The log file contains information from DCNM-LAN features and server components.



**Note**

The DCNM-LAN Server Log Settings feature does not affect logging levels of Cisco NX-OS devices. DCNM-LAN does not support the configuration of device logging levels.

This section includes the following topics:

- [Logging Levels, page 32-2](#)



- [Log File and Location, page 32-2](#)
- [Virtualization Support, page 32-2](#)

## Logging Levels

The DCNM-LAN server supports a hierarchy of logging levels, ordered by the severity of log messages. Each level includes messages for that level in addition to all log messages from levels of higher severity. The logging levels, in order from the highest to the lowest severity, are as follows:

- Fatal Errors
- Errors
- Warnings
- Information
- Debugging
- Verbose

## Log File and Location

The DCNM-LAN server writes server log messages to the sys.pipe file at the following location:

`INSTALL_DIR\log`

By default, when you install the DCNM-LAN server on Microsoft Windows Server, `INSTALL_DIR` is `C:\Program Files\Cisco Systems\dcnm`.

*What would the default installation directory be for a Linux installation?*

## Virtualization Support

DCNM-LAN server logs do not contain log messages from Cisco NX-OS devices; therefore, this feature has no effect on virtualization support.

# Licensing Requirements for Administering DCNM-LAN Server Log Settings

The following table shows the licensing requirements for this feature:

| Product        | License Requirement                                                                                                                                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco DCNM-LAN | DCNM-LAN Server Log Settings requires no license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN 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 7.1.x</i> . |



# Prerequisites for Administering DCNM-LAN Server Log Settings

Administering DCNM-LAN server log settings has the following prerequisites:

- You should be familiar with a DCNM-LAN feature before you configure server log settings for it.

## Guidelines and Limitations for Administering DCNM-LAN Server Log Settings

The Administering DCNM-LAN server log settings feature has the following configuration guidelines and limitations:

- Setting a logging level to a lower severity results in more messages in the log file.
- We recommend using the default logging settings unless you are troubleshooting an issue.
- When you are troubleshooting an issue, consider lowering the logging level severity of the affected feature or server component.
- After you resolve an issue, consider restoring the logging level of the affected feature or server component to a higher severity.

## Configuring DCNM-LAN Server Log Settings

This section includes the following topics:

- [Configuring the Default Logging Level, page 32-3](#)
- [Configuring a Unique Logging Level for a Feature or Server Component, page 32-4](#)
- [Configuring a Feature or Server Component to Use the Default Logging Level, page 32-4](#)

## Configuring the Default Logging Level

You can configure the default logging level for all DCNM-LAN features and server components.

### BEFORE YOU BEGIN

Determine what the default logging level should be. For more information, see the [“Logging Levels” section on page 32-2](#).

### DETAILED STEPS

- 
- |               |                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Feature Selector pane, choose <b>DCNM Server Administration &gt; DCNM Server Log Settings</b> . The log settings appear in the Contents pane. |
| <b>Step 2</b> | From the Default Logging Level drop-down list, choose the logging level.                                                                               |
| <b>Step 3</b> | From the menu bar, choose <b>File &gt; Deploy</b> to apply your changes to the DCNM-LAN server.                                                        |
-



## RELATED TOPICS

- [Configuring a Unique Logging Level for a Feature or Server Component, page 32-4](#)
- [Configuring a Feature or Server Component to Use the Default Logging Level, page 32-4](#)

# Configuring a Unique Logging Level for a Feature or Server Component

You can configure a logging level of a feature or server component that is independent of the default logging level.

## BEFORE YOU BEGIN

Determine what the logging level of the feature or service should be. For more information, see the [“Logging Levels” section on page 32-2](#).

## DETAILED STEPS

- 
- |               |                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Feature Selector pane, choose <b>DCNM Server Administration &gt; DCNM Server Log Settings</b> .<br>The log settings appear in the Contents pane.          |
| <b>Step 2</b> | Find the feature or server component that you want to configure with a unique logging level.                                                                       |
| <b>Step 3</b> | Uncheck <b>Default</b> to the right of the feature or server component.<br>The logging level drop-down list for the feature or server component becomes available. |
| <b>Step 4</b> | From the logging level drop-down list, choose the logging level. For more information, see the <a href="#">“Logging Levels” section on page 32-2</a> .             |
| <b>Step 5</b> | From the menu bar, choose <b>File &gt; Deploy</b> to apply your changes to the DCNM-LAN server.                                                                    |
- 

## RELATED TOPICS

- [Configuring the Default Logging Level, page 32-3](#)
- [Configuring a Feature or Server Component to Use the Default Logging Level, page 32-4](#)

# Configuring a Feature or Server Component to Use the Default Logging Level

You can configure a feature or server component to use the default logging level.

## BEFORE YOU BEGIN

Ensure that the default logging level is appropriate for the feature or service. For more information, see the [“Logging Levels” section on page 32-2](#).

## DETAILED STEPS

- 
- |               |                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From the Feature Selector pane, choose <b>DCNM Server Administration &gt; DCNM Server Log Settings</b> .<br>The log settings appear in the Contents pane. |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|



- Step 2** Find the feature or server component that you want to use the default logging level.
- Step 3** Check **Default** to the right of the feature or service.  
The logging level drop-down list for the feature or server component becomes unavailable.
- Step 4** From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.

## RELATED TOPICS

- [Configuring the Default Logging Level, page 32-3](#)
- [Configuring a Unique Logging Level for a Feature or Server Component, page 32-4](#)

# Viewing DCNM-LAN Server Log Settings

To view DCNM-LAN server user accounts, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The default logging level, feature logging settings, and server component logging settings appear in the Contents pane. For information about the fields that appear, see the [“Field Descriptions for DCNM-LAN Server Log Settings” section on page 32-5](#).

## Field Descriptions for DCNM-LAN Server Log Settings

This section includes the following field descriptions for DCNM-LAN server log settings:

- [DCNM-LAN Server Log Settings Contents Pane, page 32-5](#)

## DCNM-LAN Server Log Settings Contents Pane

**Table 32-1** *DCNM-LAN Server Log Settings Contents Pane*

| Field                    | Description                                                                                                                                                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Logging Level    | Logging level for the features or server components whose Default check box is checked. The default value for this list is Informational. For more information about logging levels, see the <a href="#">“Logging Levels” section on page 32-2</a> .                                |
| <b>DCNM-LAN Features</b> |                                                                                                                                                                                                                                                                                     |
| Default                  | Whether logging for the corresponding feature uses the default logging level or the logging level specified for the feature. When a Default check box is checked, the logging level list for the corresponding feature is unavailable. By default, these check boxes are unchecked. |
| AAA                      | Logging level for the AAA feature.                                                                                                                                                                                                                                                  |
| ACL                      | Logging level for the access control list feature.                                                                                                                                                                                                                                  |
| Dot1X                    | Logging level for the 802.1X feature.                                                                                                                                                                                                                                               |
| GLBP                     | Logging level for the Gateway Load-Balancing Protocol feature.                                                                                                                                                                                                                      |



**Table 32-1** *DCNM-LAN Server Log Settings Contents Pane (continued)*

| Field                             | Description                                                                                                                                                                                                                                                                                      |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interfaces                        | Logging level for the Interfaces feature.                                                                                                                                                                                                                                                        |
| Key Chain                         | Logging level for the keychain management feature.                                                                                                                                                                                                                                               |
| Layer 2 Security                  | Logging level for the layer 2 security feature, which are as follows: <ul style="list-style-type: none"> <li>• Dynamic ARP inspection</li> <li>• Port security</li> <li>• DHCP snooping</li> <li>• IP Source Guard</li> <li>• Traffic storm control</li> </ul>                                   |
| Object Tracking                   | Logging level for the object tracking feature.                                                                                                                                                                                                                                                   |
| Port Channel                      | Logging level for the port security feature.                                                                                                                                                                                                                                                     |
| SPAN                              | Logging level for the SPAN feature.                                                                                                                                                                                                                                                              |
| Spanning Tree                     | Logging level for the STP feature.                                                                                                                                                                                                                                                               |
| Tunnel                            | Logging level for the tunnel interface management feature.                                                                                                                                                                                                                                       |
| Virtual Devices                   | Logging level for the virtual device context feature.                                                                                                                                                                                                                                            |
| VLAN                              | Logging level for the VLAN feature.                                                                                                                                                                                                                                                              |
| FabricExtender                    | Logging level for the Fabric Extender feature.                                                                                                                                                                                                                                                   |
| VPC                               | Logging level for the vPC feature.                                                                                                                                                                                                                                                               |
| HSRP                              | Logging level for the HSRP feature.                                                                                                                                                                                                                                                              |
| DEVICE GROUP                      | Logging level for the Device Groups feature.                                                                                                                                                                                                                                                     |
| <b>DCNM-LAN Server Components</b> |                                                                                                                                                                                                                                                                                                  |
| Default                           | Whether logging for the corresponding server component uses the default logging level or the logging level specified for the component. When a Default check box is checked, the logging level list for the corresponding component is unavailable. By default, these check boxes are unchecked. |
| Event                             | Logging level for the event component, which includes messages about how DCNM-LAN processes the system and accounting logs it retrieves from devices and also events generated by DCNM-LAN.                                                                                                      |
| Statistics Collection             | Logging level for the statistical data collection component.                                                                                                                                                                                                                                     |
| Config Archive                    | Logging level for the configuration archive component, used by the Configuration Change Management feature.                                                                                                                                                                                      |
| Device Connections                | Logging level for the component that connects the DCNM-LAN server to devices.                                                                                                                                                                                                                    |
| Device Discovery                  | Logging level for the component that performs device discovery.                                                                                                                                                                                                                                  |



## Additional References

For additional information related to administering DCNM-LAN server log settings, see the following sections:

- [Standards, page 32-7](#)
- [Standards, page 32-7](#)

## Standards

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

## Feature History for DCNM-LAN Server Log Settings

[Table 32-2](#) lists the release history for this feature.

**Table 32-2** Feature History for DCNM-LAN Server Log Settings

| Feature Name          | Releases | Feature Information                                                                |
|-----------------------|----------|------------------------------------------------------------------------------------|
| Device Groups logging | 5.0(2)   | Support was added for configuring the logging level for the Device Groups feature. |









## CHAPTER 33

# Managing Events

---

DCNM allows you to view and manage events that the DCNM server recently received from managed devices or that the DCNM server generated itself. The Event Browser allows you to view recent status events. In addition to listing events, the Event Browser provides a pie chart and a bar chart of events separated by the event severity.

DCNM also displays feature-specific status events on the Events tab that appears in the Details pane for features that can have 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 33-1](#)
- [Licensing Requirements for the Event Browser, page 33-2](#)
- [Prerequisites, page 33-2](#)
- [Guidelines and Limitations for the Event Browser, page 33-2](#)
- [Platform Support, page 33-3](#)
- [Using the Event Browser and Events Tabs, page 33-3](#)
- [Field Descriptions for Events, page 33-10](#)
- [Related Documents, page 33-11](#)
- [Feature History for the Event Browser and Events Tabs, page 33-12](#)

## 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.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.



**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 7.1.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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.
- 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.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       | <a href="#">Cisco Nexus 1000V Series Switches Documentation</a> |
| Cisco Nexus 2000 Series Fabric Extender | Cisco Nexus 2000 Series Fabric Extender Documentation           |
| Cisco Nexus 4000 Series switches        | <a href="#">Cisco Nexus 4000 Series Switches Documentation</a>  |
| Cisco Nexus 5000 Series switches        | <a href="#">Cisco Nexus 5000 Series Switches Documentation</a>  |
| Cisco Nexus 7000 Series switches        | <a href="#">Cisco Nexus 7000 Series Switches Documentation</a>  |

## Using the Event Browser and Events Tabs

This section includes the following topics:

- [Viewing the Event Browser, page 33-3](#)
- [Applying and Removing an Event Filter, page 33-5](#)
- [Viewing Events on an Events Tab, page 33-6](#)
- [Changing the Status of an Event, page 33-7](#)
- [Adding a Note to One or More Events, page 33-8](#)
- [Deleting an Event, page 33-9](#)

## 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

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"> <li>• First click—Events are sorted by ascending alphabetical order for the values in the column.</li> <li>• Second click—Events are sorted by descending alphabetical order for the values in the column.</li> <li>• Third click—Events are not sorted by the values in the column.</li> </ul> |
| Event Filter                        | See the <a href="#">“Applying and Removing an Event Filter” section on page 33-5</a> .                                                                                                                                                                                                                                                                                                                        |
| Filter by Column Values             | <ol style="list-style-type: none"> <li>1. From the menu bar, choose <b>View &gt; Filter</b>.<br/>The column headings become drop-down lists.</li> <li>2. From each column heading list that you want to use to filter events, choose the value that events appearing in the Event Browser must include.</li> </ol>                                                                                            |
| 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><b>Tip</b> 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:

- a. Find the event in the event list.
- b. Click the event.
- c. Expand the Details pane, if necessary.  
Details about the selected event appear in the Details pane.
- d. (Optional) To read notes and messages about status changes to the event, read the information in the Action Log field.

## RELATED TOPICS

- [Applying and Removing an Event Filter, page 33-5](#)
- [Viewing Events on an Events Tab, page 33-6](#)



- [Changing the Status of an Event, page 33-7](#)
- [Adding a Note to One or More Events, page 33-8](#)
- [Deleting an Event, page 33-9](#)
- [Configuring the Maximum Age of Events Fetched from the Server, page 14-18](#)

## Applying and Removing an Event Filter

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

- Event date and time—By default, the Cisco DCNM client displays all events received after you started the Cisco DCNM client and for a configurable number of hours prior to starting the Cisco DCNM client (for more information, see the [Configuring the Maximum Age of Events Fetched from the Server, page 14-18](#)).
- 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 33-3](#)).

**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.

### RELATED TOPICS

- [Viewing the Event Browser, page 33-3](#)



- [Viewing Events on an Events Tab, page 33-6](#)
- [Changing the Status of an Event, page 33-7](#)
- [Adding a Note to One or More Events, page 33-8](#)
- [Deleting an Event, page 33-9](#)
- [Configuring the Maximum Age of Events Fetched from the Server, page 14-18](#)

## 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.

### 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      | <p>Click the column heading to cycle through the sorting options, as follows:</p> <ul style="list-style-type: none"> <li>• First click—Events are sorted by ascending alphabetical order for the values in the column.</li> <li>• Second click—Events are sorted by descending alphabetical order for the values in the column.</li> <li>• Third click—Events are not sorted by the values in the column.</li> </ul> |
| Filter by Column Values             | <ol style="list-style-type: none"> <li>1. From the menu bar, choose <b>View &gt; Filter</b>.<br/>The column headings become drop-down lists.</li> <li>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.</li> </ol>                                                                                                      |

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

## RELATED TOPICS

- [Viewing the Event Browser, page 33-3](#)
- [Applying and Removing an Event Filter, page 33-5](#)
- [Changing the Status of an Event, page 33-7](#)
- [Adding a Note to One or More Events, page 33-8](#)
- [Deleting an Event, page 33-9](#)
- [Configuring the Maximum Age of Events Fetched from the Server, page 14-18](#)

## 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 33-3](#) or the [“Viewing Events on an Events Tab” section on page 33-6](#).

## DETAILED STEPS

- 
- |               |                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | In the event table, right-click the selected event.                                                                                                                                                                                   |
| <b>Step 2</b> | Choose <b>Acknowledge</b> or <b>Open</b> , as needed.<br><br>The new status appears in the Annotation column for the selected event.<br><br>In the Details pane, the message about the status change appears in the Action Log field. |
- 

## RELATED TOPICS

- [Viewing the Event Browser, page 33-3](#)
- [Applying and Removing an Event Filter, page 33-5](#)
- [Viewing Events on an Events Tab, page 33-6](#)
- [Adding a Note to One or More Events, page 33-8](#)
- [Deleting an Event, page 33-9](#)

# 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 33-3](#) or the [“Viewing Events on an Events Tab” section on page 33-6](#).

## DETAILED STEPS

- 
- |               |                                                                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Select one or more events. Do one of the following: <ul style="list-style-type: none"><li>• To select one event, click the one event that you want to select.</li><li>• To select two or more adjacent events, click and drag across the events.</li><li>• To select two more events, press and hold <b>Ctrl</b> and click each event.</li></ul> |
| <b>Step 2</b> | On one of the selected events, right-click and then choose <b>Add Notes</b> .<br><br>The Notes dialog box appears.                                                                                                                                                                                                                               |
| <b>Step 3</b> | Enter the note. You can enter up to 1000 case-sensitive, alphanumeric characters.                                                                                                                                                                                                                                                                |
| <b>Step 4</b> | Click <b>OK</b> .<br><br>The note appears in the Action Log field for each selected event.                                                                                                                                                                                                                                                       |
-



## RELATED TOPICS

- [Viewing the Event Browser, page 33-3](#)
- [Applying and Removing an Event Filter, page 33-5](#)
- [Viewing Events on an Events Tab, page 33-6](#)
- [Changing the Status of an Event, page 33-7](#)
- [Deleting an Event, page 33-9](#)

## 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 *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.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 33-3](#) or the [“Viewing Events on an Events Tab” section on page 33-6](#).

## DETAILED STEPS

---

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



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

---

**Step 2** Right-click a selected event.

**Step 3** Choose **Remove Event**.

The selected events disappear from the Event Browser.

---

## RELATED TOPICS

- [Viewing the Event Browser, page 33-3](#)
- [Applying and Removing an Event Filter, page 33-5](#)
- [Viewing Events on an Events Tab, page 33-6](#)
- [Changing the Status of an Event, page 33-7](#)
- [Adding a Note to One or More Events, page 33-8](#)



# Field Descriptions for Events

This section includes the following field descriptions for Events:

- [Events Table, page 33-10](#)
- [Event Details, page 33-11](#)

## Events Table

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

**Table 33-1**      **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"> <li>• Emergency</li> <li>• Alert</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notification</li> <li>• Informational</li> <li>• Debug</li> </ul> |
| 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"> <li>• Open—The default status of an event. You cannot assign an event the status of Open.</li> <li>• Acknowledged</li> <li>• Closed</li> </ul>                                                 |



## Event Details

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

**Table 33-2**      **Event Details**

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Event Type      | <p><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:</p> <ul style="list-style-type: none"> <li>• Communication</li> <li>• Environmental</li> <li>• Equipment</li> <li>• Processing Error</li> <li>• Quality of Service</li> <li>• Security</li> <li>• Unknown</li> </ul> |
| Action Log      | Shows all actions taken on the event and all notes added to the event.                                                                                                                                                                                                                                                                                                         |
| Life Cycle Type | <p><i>Display only.</i> Type of life cycle of the event. Possible life cycle types are as follows:</p> <ul style="list-style-type: none"> <li>• State Change</li> <li>• Attribute Value Change</li> <li>• Instance Creation</li> <li>• Instance Deletion</li> <li>• Informational</li> </ul>                                                                                   |

## Related Documents

| Related Topic                               | Document Title                                                             |
|---------------------------------------------|----------------------------------------------------------------------------|
| Minimum required Cisco NX-OS logging levels | <i>Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i> |
| Cisco DCNM server log settings              | <i>Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x</i> |
| Deleting events from the events database    | <i>Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.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 33-3 lists the release history for this feature.

**Table 33-3**      *Feature History for the Event Browser and Events Tabs*

| Feature Name                  | Releases | Feature Information         |
|-------------------------------|----------|-----------------------------|
| 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 34

## Working with Network Analysis

---

This chapter describes how to use the Network Analysis (PONG) feature in Cisco Data Center Network Manager for LAN (DCNM-LAN).

This chapter includes the following sections:

- [Information About Network Analysis, page 34-1](#)
- [Licensing Requirements for Network Analysis, page 34-1](#)
- [Prerequisites for Network Analysis, page 34-2](#)
- [Guidelines and Limitations for Network Analysis, page 34-2](#)
- [Using the Network Analysis Feature, page 34-2](#)
- [Related Documents, page 34-8](#)
- [Feature History for Network Analysis, page 34-8](#)

### Information About Network Analysis

The Network Analysis feature provides you with information to track and monitor the latency between two specified switches in a specified time interval. With Network Analysis, you can determine the health of the network by examining the delay between the two specified points in the network.

The Network Analysis feature:

- Supports real time and historical network analysis between two user specified devices or ports. The user specifies the required monitoring intervals.
- Supports an archive of historical Network Analysis measurements for the following:
  - End to end round trip time.
  - Switching delay at each hop.
  - Link delay between hops per path.
- Provides reports that contain the resulting statistical information as a chart or summary table.

### Licensing Requirements for Network Analysis

The following table shows the licensing requirements for this feature:



| Product        | License Requirement                                                                                                                                                                                                                                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco DCNM-LAN | The Network Analysis feature requires no license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN 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 7.1.x</i> . |

## Prerequisites for Network Analysis

Network Analysis has the following prerequisite:

- Network Analysis only pertains to the devices that DCNM-LAN has discovered.

## Guidelines and Limitations for Network Analysis

The Network Analysis feature has the following configuration guidelines and limitations:

- Specify the IP addresses for devices to monitor the network path between two end hosts or between a host and a server. This allows monitoring of the ingress port of the source connected switch to the egress port of the target switch connected to the end host or server.
- Specify the IP addresses for switches, VLAN, and optional interface information to monitor the path between them.
- Specify the threshold level for the round trip time to help evaluate the path latency results.

## Using the Network Analysis Feature

This section includes the following topics:

- [Using Network Analysis, page 34-2](#)
- [Using the New Path Latency Session Wizard, page 34-4](#)
- [Viewing Session Statistics, page 34-7](#)

## Using Network Analysis

You can use Network Analysis to specify the scope of the analysis and to view the information about the analysis.

### DETAILED STEPS

- Step 1

From the Feature Selector pane, choose **Network Analysis > Path Latency Monitoring (PONG)**.

The Summary pane appears in the Contents pane. Each row in the table is a path latency session. You are able to view the sessions that you have created as well as the sessions created by other users. See [Table 34-1](#).

Users with administrator privileges are allowed to modify other users' sessions.



**Table 34-1** Information in Summary Pane

| Column                         | Description                                                                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Session ID                     | Unique ID of the session created by the user. The ID is updated after the user deploys the session.                                                                      |
| Session Name                   | Unique name entered by user for the path latency session.                                                                                                                |
| Source Switch                  | IP address of the source switch from which path latency is monitored.                                                                                                    |
| Destination Switch             | IP address of the destination switch to which the path latency is monitored.                                                                                             |
| VLAN                           | VLAN ID through which the actual traffic flows (1 to 4094).                                                                                                              |
| Class of Service (CoS)         | Optional value used to filter the traffic monitoring based on class of service value (0 to 7). CoS values are shown in <a href="#">Table 34-2</a> .                      |
| Round Trip Time (microseconds) | Minimum, maximum, average and latest value of the round trip time (two way path: source <-> destination) of all the RTT latencies calculated up until current time.      |
| Forward Delay (microseconds)   | Minimum, maximum, average and latest value of the forward delay (forward path: source -> destination) of all the forward delay latencies calculated to the current time. |
| Reverse Delay (microseconds)   | Minimum, maximum, average and latest value of the reverse delay (reverse path: destination -> source) of all the reverse delay latencies calculated to the current time. |
| Owner                          | Creator of the session.                                                                                                                                                  |
| Success Percentage             | Success percentage of the packets traversed from source to destination during the specified time interval.                                                               |
| Scheduled At                   | Date and time when the monitoring was started.                                                                                                                           |
| Status                         | Column that specifies: <ul style="list-style-type: none"> <li>• Session created</li> <li>• Monitoring started</li> <li>• Monitoring stopped</li> </ul>                   |

**Table 34-2** CoS Values and Corresponding Traffic Types

| User Priority | Traffic Type            |
|---------------|-------------------------|
| 0             | Background              |
| 1             | Best Effort             |
| 2             | Excellent Effort        |
| 3             | Critical Applications   |
| 4             | Video, < 100 ms latency |
| 5             | Voice, < 10 ms latency  |



**Table 34-2** CoS Values and Corresponding Traffic Types

| User Priority | Traffic Type         |
|---------------|----------------------|
| 6             | Internetwork Control |
| 7             | Network Control      |

**Step 2** Above the Summary pane, click the **Configure New Rule** link to set a threshold rule for one of the following parameters.

- Round trip time
- Forward delay
- Reverse delay



**Note** Clicking **Configure New Rule** links you to Theshold Rules of the DCNM-LAN Server Administration feature.

**Step 3** Above the Summary pane, click the **Set Global Threshold** link to set a global threshold rule for the following parameters:

- Round trip time
- Forward delay
- Reverse delay

The global threshold setting is applied to all the sessions in the Summary Table.

**Step 4** Above the Summary pane, click the **VLAN-CoS** button to view the sessions grouped by VLAN-CoS.

## Using the New Path Latency Session Wizard

You can use the New Path Latency Session wizard to create a new session.

### DETAILED STEPS

**Step 1** From the Feature Selector pane, choose **Network Analysis > Path Latency Monitoring (PONG)**.

The Summary pane appears in the Contents pane.

**Step 2** In the Summary pane, right-click and choose **New Path Latency Session** in the context menu.

The New Path Latency Session wizard appears.

**Step 3** In the Select Session Monitor Option of Interest screen, enter the following:

- Session Name  
(Length: 1 to 256 characters)
- VLAN  
(Value: 1 to 4094)
- Class of Service (CoS)



**Table 34-3** CoS Values and Corresponding Traffic Types

| User Priority | Traffic Type            |
|---------------|-------------------------|
| 0             | Background              |
| 1             | Best Effort             |
| 2             | Excellent Effort        |
| 3             | Critical Applications   |
| 4             | Video, < 100 ms latency |
| 5             | Voice, < 10 ms latency  |
| 6             | Internetwork Control    |
| 7             | Network Control         |

**Step 4** In the Select Option section, choose one of the following options:

- Monitor latency between source VDC and destination VDC.
- Monitor latency between source and destination VDC including source switching delay.
- Monitor latency between source and destination VDC including destination switching delay.
- Monitor latency between source and destination VDC including both switching delays.

Under the Monitor latency between source VDC and destination VDC option, you can additionally choose to measure the latency between switches that have Fabric Path mode connectivity. The latency measurements are measured between the source and destination switches but do not include the switching delay of both the end switches.

**Note**

For the switches that are in a classical ethernet cloud, the wizard allows you to choose their VDC MAC addresses/IP addresses/hostnames in the following wizard screen.

Click **Next** to continue.

**Step 5** In the Select Source and Destination Switch screen, do the following:

- Choose the source switch by clicking on the ellipses next to the Select Source Switch field. Highlight the device in the screen that appears and click **OK** to enter your selection.
- Choose the destination switch by clicking on the ellipses next to the Select Destination Switch field. Highlight the device in the screen that appears and click **OK** to enter your selection.

Depending on the earlier selection that you made in the Select Option section of the wizard, [Table 34-4](#) list the required and optional information that you must enter in the Select Source and Destination Switch screen.



**Table 34-4** Required and Optional Information

| Option                                                                                   | Required                                                                                                                                                                                                                                                                                                                                                                                                                                  | Optional                                                                                                                        |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Monitor latency between source VDC and destination VDC                                   | <ul style="list-style-type: none"> <li>Source and destination</li> </ul>                                                                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>Egress/outbound interface through which the packet flows out from the source.</li> </ul> |
| Monitor latency between source and destination VDC including source switching delay      | <ul style="list-style-type: none"> <li>Source and destination</li> <li>Inject/ingress interface through which the packet needs to be injected from the source switch. Also requires the source static MAC address associated with the interface.</li> </ul>                                                                                                                                                                               | <ul style="list-style-type: none"> <li>N/A</li> </ul>                                                                           |
| Monitor latency between source and destination VDC including destination switching delay | <ul style="list-style-type: none"> <li>Source and destination</li> <li>Egress/outbound interface through which the packet terminates at the destination switch. Also requires the destination static MAC address associated with the interface.</li> </ul>                                                                                                                                                                                | <ul style="list-style-type: none"> <li>Egress/outbound interface through which the packet flows out from the source.</li> </ul> |
| Monitor latency between source and destination VDC including both switching delays       | <ul style="list-style-type: none"> <li>Source and destination</li> <li>Inject/ingress interface through which the packet needs to be injected from the source switch. Also requires source static MAC address associated with the interface.</li> <li>Egress/outbound interface through which the packet terminates at the destination switch. Also requires the destination static MAC address associated with the interface.</li> </ul> | <ul style="list-style-type: none"> <li>N/A</li> </ul>                                                                           |

**Note**

You can enter any arbitrary unique static MAC address that points to the selected interface. To configure a new static MAC address, use one of the following recommended addresses to avoid any conflict with globally administered MAC addresses (associated with any other host/devices):

- X2XX.XXXX.XXXX
- X6XX.XXXX.XXXX
- XAXX.XXXX.XXXX
- XEXX.XXXX.XXXX



where X is a hexadecimal value.

Click **Next** to continue.

**Step 6** In the dialog box that appears, click **OK** to start input verification.

The Input Verification screen appears and the results are displayed.

Input verification verifies the following:

- Path latency measurement between specified devices.
- Packet traversal between the specified devices.

If the verification fails, you must specify the information that you entered earlier in the wizard.

[Table 34-5](#) lists the additional settings that are available in the Input Verification window:

**Table 34-5** *Input Verification Settings*

| Setting                | Description                                                                                                                                           | Value                                   |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Monitor Interval       | Interval of time between data collection points.                                                                                                      | 0.5 - 5 minutes<br>(Default: 5 minutes) |
| End Time               | Time of session termination                                                                                                                           | N/A                                     |
| Calculate Jitter       | Variance of inter packet RTT delay                                                                                                                    | Default: unchecked                      |
| No. of Packets to send | Packet count to send for the session to measure latency.<br><br>To calculate jitter (inter packet delay variance), more than 1 packet has to be sent. | 1 -5 packets<br>(Default: 1 packet)     |

Click **Finish** after a successful verification and to enter the settings.

## Viewing Session Statistics

You can view session statistics from the Summary pane.

### DETAILED STEPS

**Step 1** From the Feature Selector pane, choose **Network Analysis > Path Latency Monitoring (PONG)**.

The Summary pane appears in the Contents pane.

**Step 2** Right-click a session and choose **Go To Statistics** in the context menu.

The statistics for the session appear as a chart and a table of detailed information in the Details pane.

**Step 3** In the Details pane, click the Path Latency tab to display RTT information about each path.

**Step 4** In the Details pane, right-click to display a context menu of additional statistical displays:



- Path specific switching delay—Switching delay of all the switches traversed in each path.
- Path specific link delay—Link delay at each hop traversed in each path.
- Switching delay of each switch across different paths traversed in the session.
- Link delay of each link across different paths traversed in the session.

**Step 5** In the Details pane, click the **Session Report** tab to display overall statistical information about the session.

The information can be exported as an Excel .xls file by clicking the export button near the top of the table.

# Related Documents

For additional information related to the topology map, see the following sections:

| Related Topic    | Document Title                                               |
|------------------|--------------------------------------------------------------|
| Device discovery | <a href="#">Chapter 27, “Administering Device Discovery”</a> |

# Feature History for Network Analysis

[Table 34-6](#) lists the release history for this feature.

**Table 34-6** *Feature History for Topology*

| Feature Name             | Releases | Feature Information                     |
|--------------------------|----------|-----------------------------------------|
| Network Analysis support | 5.2(0)   | Support for Network Analysis was added. |





## CHAPTER **35**

# Maintaining the Cisco DCNM-LAN Database

---

This chapter describes how to maintain the Cisco Data Center Network Manager for LAN (DCNM-LAN) database.

This chapter includes the following sections:

- [Information About Database Maintenance, page 35-1](#)
- [Licensing Requirements for Database Maintenance, page 35-3](#)
- [Prerequisites for Database Maintenance, page 35-3](#)
- [Guidelines and Limitations for Database Maintenance, page 35-3](#)
- [Performing Database Maintenance, page 35-4](#)
- [Additional References, page 35-9](#)
- [Feature History for DCNM-LAN Database Maintenance, page 35-9](#)

## Information About Database Maintenance

DCNM-LAN uses a PostgreSQL database or an Oracle database to store all data, including configuration information from managed devices, events and statistical data gathered from managed devices, and DCNM-LAN user information. In addition to scripts that you can run to perform database maintenance, DCNM-LAN provides features to help you delete events and statistical data that you no longer need.

This section includes the following topics:

- [Automatic and Manual Purging of Data, page 35-1](#)
- [Database Backup, page 35-2](#)
- [Database Clean, page 35-2](#)
- [Database Restore, page 35-2](#)

## Automatic and Manual Purging of Data

You can use the Auto-Synchronization with Devices feature to delete unwanted event data and the Statistical Data Collection feature to delete unwanted statistical data. DCNM-LAN supports automatic purging of both types of data. You can configure the following aspects of automatic data purging:



- Days of the week and time of day that automatic purging occurs.
- Whether DCNM-LAN determines which data to purge by the age of the data or by a maximum number of database entries.
- For event-related data, whether DCNM-LAN determines which events to purge by event severity.

We recommend that you configure automatic purging of events and statistical data to ensure that the DCNM-LAN database size does not grow too large.

You can also manually purge events and statistical data.

For more information, see the following sections:

- [Automatic and Manual Purging of Event Data, page 29-2](#)
- [Automatic and Manual Purging of Statistical Data, page 30-2](#)

## Database Backup

You can use the Cisco DCNM database backup script to create a backup file of the DCNM-LAN database.

We strongly recommend that you regularly back up the DCNM-LAN database and that you archive backup files in a secure location that is not on the DCNM-LAN server system. You should retain the backup files as long as required by the standards of your organization.

## Database Clean

You can use the Cisco DCNM database clean script `/usr/local/cisco/dcm/dcnm/bin/clean-dcnm-db.sh` to clean the DCNM-LAN database. Cleaning removes all DCNM-LAN data from the database and is a necessary step prior to restoring the DCNM-LAN database. Any database records that have not been backed up are lost when you clean the database.

You can also clean the database if you want to delete all data and rebuild your DCNM-LAN implementation without restoring data from a backup.

## Database Restore

You can use the Cisco DCNM database restore script to restore the DCNM-LAN database from a backup file. The backup file must have been created by the DCNM-LAN database backup script included in the same release of DCNM-LAN that you are restoring the data to. For example, if you are running Cisco DCNM Release 5.0(2), you should only perform database restoration from a backup of Cisco DCNM Release 5.0(2).

Also, the backup file must have been created from the same database type and release that you are restoring the data to. For example, if you are restoring data to an Oracle 11g database, the backup file must have been created from an Oracle 11g database.

Before you restore a DCNM-LAN database, you should clean the database. Restoring a database without cleaning the database can have unpredictable results.



# Licensing Requirements for Database Maintenance

The following table shows the licensing requirements for this feature:

| Product  | License Requirement                                                                                                                                                                                                                                                                                                       |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCNM-LAN | Database maintenance requires no license. Any feature not included in a license package is bundled with the DCNM-LAN 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 7.1.x</i> . |

## Prerequisites for Database Maintenance

Database maintenance has the following prerequisites:

- You must have successfully installed the DCNM-LAN server.
- Cleaning the DCNM-LAN database requires that you stop the DCNM-LAN server.
- Restoring the DCNM-LAN database requires the following:
  - You must have a backup file created from exactly the same release of DCNM-LAN that you are restoring with the backup file.
  - You must have a backup file created from exactly the same database type and release that you are restoring data to.
  - You must have a backup file that was created from a DCNM-LAN database running in the same operating system as the database that you want to restore. For example, backup files made from a database running in Microsoft Server 2003 can only be used to restore other DCNM-LAN databases running in Microsoft Server 2003.

## Guidelines and Limitations for Database Maintenance

Database maintenance has the following configuration guidelines and limitations:

- We recommend that you configure automatic purging of statistical data and event data to ensure that the DCNM-LAN database size does not grow too large.
- We recommend that you perform backups on a regular basis. Follow the standards of your organization to determine how frequently you should perform backups.
- You can only restore a DCNM-LAN database from a backup of the same release of DCNM-LAN. For example, if you are running Cisco DCNM Release 5.0(2), you should only perform database restoration from a backup of Cisco DCNM Release 5.0(2).
- You can only restore a DCNM-LAN database from a backup of the same database type and release as the current database. For example, if the current database is an Oracle 11g database, you can only restore it with a backup file made from an Oracle 11g database.
- You can only restore a DCNM-LAN database from a backup file that was made from a DCNM-LAN database running in the same operating system as the database that you want to restore. For example, backup files made from a database running in Microsoft Server 2003 can only be used to restore other DCNM-LAN databases running in Microsoft Server 2003.



# Performing Database Maintenance

- This section includes the following topics:
- [Backing Up the DCNM-LAN Database, page 35-4](#)
  - [Cleaning a DCNM-LAN Database, page 35-5](#)
  - [Restoring a DCNM-LAN Database from a Backup File, page 35-7](#)

## Backing Up the DCNM-LAN Database

You can back up the DCNM-LAN database with the backup script. The DCNM-LAN server installer configures the backup script with the database username and database name that you specified during server installation.

### DETAILED STEPS

- Step 1

On the DCNM-LAN server, access a command prompt.
- Step 2

Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:

**cd** *path*

where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the bin directory is C:\Program Files\dcn\dcnm\bin. For RHEL, the default path to the bin directory is /usr/local/cisco/dcm/dcnm/bin.
- Step 3

Run the Cisco DCNM database backup script. The script name depends upon the server operating system and database type, as shown in the following table:

| Server Operating System | Database Type | Backup Script Name        |
|-------------------------|---------------|---------------------------|
| Microsoft Windows       | PostgreSQL    | backup-pgsql-dcnm-db.bat  |
|                         | Oracle        | backup-oracle-dcnm-db.bat |
| Linux                   | PostgreSQL    | backup-pgsql-dcnm-db.sh   |
|                         | Oracle        | backup-oracle-dcnm-db.sh  |

- Step 4

Enter the filename for the backup that you are creating.
- Step 5

At the confirmation prompt, enter y to continue with the backup.
- Step 6

Verify that the backup file was created as you specified and has a file size greater than zero.

- On Linux, use the **ls -l** command.
  - On Microsoft Windows, use the **dir** command.
- Step 7

Store the backup file in a safe location. We recommend that you copy the backup file to a secure location that is off the DCNM-LAN server system so that you can protect your data from the potential of a catastrophic hardware failure.



## Example

The following example from a Windows server shows how to create a backup named masterbackup.bkp from a PostgreSQL DCNM-LAN database that was installed using default values:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcn\dcnm\bin"

C:\Program Files\Cisco Systems\dcn\dcnm\bin>backup-pgsql-dcnm-db.bat
=====

Database Postgres Environment

PostgreSQL Bin Path : "C:\Program Files\Cisco Systems\dcn\db"\bin"

DCNM Database Name : "dcmdb"

DCNM Database User Name : "dcnmuser"

=====

Please enter the filename to be used for Database Backup:masterbackup.bkp
" "
"Database Schema "dcnmuser" will be backed up in filename : masterbackup.bkp"
" "
Continue y/n [n] : y
.
.
.
Database backup File: woobie1
Operation Completed
C:\Program Files\Cisco Systems\dcn\dcnm\bin>dir masterbackup.bkp
Volume in drive C has no label.
Volume Serial Number is D415-F632

Directory of C:\Program Files\PostgreSQL\8.2\bin

06/15/2009 01:53 PM 900,129 masterbackup.bkp
 1 File(s) 900,129 bytes
 0 Dir(s) 23,960,858,624 bytes free

C:\Program Files\Cisco Systems\dcn\dcnm\bin>
```

## Cleaning a DCNM-LAN Database

You can use the DCNM-LAN database clean script to clean the database, which deletes all data from the DCNM-LAN database. You might want to clean the database for the following reasons:

- You want to restore the DCNM-LAN database from a backup.
- You want to delete all data and rebuild your DCNM-LAN implementation without restoring data from a backup.

The DCNM-LAN server installer configures the clean script with the database username and database name that you specified during the server installation.

### BEFORE YOU BEGIN

Back up the DCNM-LAN database. Any data not preserved in a backup is lost when you clean the database.



Stop the DCNM-LAN server. The DCNM-LAN server must be down before you can finish the database cleaning procedure. For more information, see the [“Stopping DCNM-LAN Servers” section on page 25-5](#).

## DETAILED STEPS

- Step 1** On the DCNM-LAN server, access a command prompt.
- Step 2** If you have not already done so, stop the DCNM-LAN server. For more information, see the [“Stopping DCNM-LAN Servers” section on page 25-5](#).
- Step 3** Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:
- cd** *path*
- where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the bin directory is C:\Program Files\dcm\dcnm\bin. For RHEL, the default path to the bin directory is /usr/local/cisco/dcm/dcnm/bin.
- Step 4** Run the Cisco DCNM database clean script. The script name depends upon the server operating system and database type, as shown in the following table:

| Server Operating System | Database Type | Clean Script             |
|-------------------------|---------------|--------------------------|
| Microsoft Windows       | PostgreSQL    | clean-pgsql-dcnm-db.bat  |
|                         | Oracle        | clean-oracle-dcnm-db.bat |
| Linux                   | PostgreSQL    | clean-pgsql-dcnm-db.sh   |
|                         | Oracle        | clean-oracle-dcnm-db.sh  |

- Step 5** At the confirmation prompt, enter **y** to continue with cleaning the database.
- Step 6** If you want to restore the DCNM-LAN database from a backup, proceed to the [“Restoring a DCNM-LAN Database from a Backup File” section on page 35-7](#). Do not start the DCNM-LAN server. If you do not want to restore the DCNM-LAN database from a backup and want to rebuild your DCNM-LAN implementation manually, start the DCNM-LAN server. See the [“Starting a Single DCNM-LAN Server” section on page 25-2](#).

## Example

The following example from a Windows server shows how to clean a PostgreSQL DCNM-LAN database that was installed using default values:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcm\dcnm\bin"

C:\Program Files\Cisco Systems\dcm\dcnm\bin>clean-pgsql-dcnm-db.bat

=====

Database Postgres Environment

PostgreSQL Bin Path : "C:\Program Files\Cisco Systems\dcm\db\bin"

DCNM Database Name : "dcmdb"
```



```

DCNM Database User Name : "dcnmuser"

DCNM Database SuperUser Name : "cisco"
=====

PLEASE MAKE SURE THE DCNM SERVICE IS SHUTDOWN BEFORE RUNNING THIS SCRIPT!!

DCNM database schema "dcnmuser" will be deleted permanently...

Please Confirm y/n [n] : y
.
.
.
Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>

```

## Restoring a DCNM-LAN Database from a Backup File

You can use the Cisco DCNM database restore script to restore the DCNM-LAN database from a backup file. The restore script cleans the database prior to restoring it.

### BEFORE YOU BEGIN

Locate the backup file that you want to use to restore the DCNM-LAN database.

Ensure that the backup file that you want to use to restore the database was made from the same release of DCNM-LAN. For example, you can only restore a Cisco DCNM Release 5.0(2) database from a backup file created from a Cisco DCNM Release 5.0(2) database.

Ensure that the backup file was made from the same database type and release as the current database. For example, you can only restore an Oracle 11g database from a backup file made from an Oracle 11g database.

Ensure that the backup file was made from a DCNM-LAN database running in the same operating system as the DCNM-LAN server that you want to restore the database to. For example, backup files made from a database running in Microsoft Server 2003 can only be used to restore other DCNM-LAN databases running in Microsoft Server 2003.

The DCNM-LAN server must be stopped while you are restoring the database.

### DETAILED STEPS

- 
- Step 1** On the DCNM-LAN server, access a command prompt.
  - Step 2** If you have not already done so, stop the DCNM-LAN server. For more information, see the [“Stopping DCNM-LAN Servers” section on page 25-5](#).
  - Step 3** Use the **cd** command to change the directory to the bin directory under the Cisco DCNM installation directory, as follows:  
**cd path**



where *path* is the relative or absolute path to the bin directory. For Microsoft Windows, the default path to the bin directory is C:\Program Files\dcn\dcnm\bin. For RHEL, the default path to the bin directory is /usr/local/cisco/dcn/dcnm/bin.

- Step 4** Run the Cisco DCNM database restore script. The script name depends upon the server operating system and database type, as shown in the following table:

| Server Operating System | Database Type | Restore Script             |
|-------------------------|---------------|----------------------------|
| Microsoft Windows       | PostgreSQL    | restore-pgsql-dcnm-db.bat  |
|                         | Oracle        | restore-oracle-dcnm-db.bat |
| Linux                   | PostgreSQL    | restore-pgsql-dcnm-db.sh   |
|                         | Oracle        | restore-oracle-dcnm-db.sh  |

- Step 5** Enter the name of the backup file that you want to use to restore the DCNM-LAN database.
- Step 6** At the confirmation prompt, enter **y** to continue with the database restore.
- Step 7** To resume using DCNM-LAN, start the DCNM-LAN server. See the [“Starting a Single DCNM-LAN Server” section on page 25-2](#).

## Example

The following example from a Microsoft Windows server shows how to restore a DCNM-LAN PostgreSQL database that was installed using default values and using a backup file named masterbackup.bkp that exists in the bin directory Cisco DCNM installation directory:

```
C:\Documents and Settings\Administrator>cd "C:\Program Files\Cisco Systems\dcn\dcnm\bin"
```

```
C:\Program Files\Cisco Systems\dcn\dcnm\bin>restore-pgsql-dcnm-db.bat
```

```
=====
```

```
Database Postgres Environment
```

```
PostgreSQL Bin Path : "C:\Program Files\Cisco Systems\dcn\db\bin"
```

```
DCNM Database Name : "dcmdb"
```

```
DCNM Database User Name : "dcnmuser"
```

```
=====
```

```

PLEASE MAKE SURE THE DCNM SERVICE IS SHUTDOWN BEFORE RUNNING THIS SCRIPT!!

```

```
Please enter the filename to be used for Database Restore:masterbackup.bkp
```

```
" "
```

```
"Database Schema "dcnmuser" will be Restore from filename : masterbackup.bkp"
```

```
" "
```

```
Continue y/n [n] : y
```

```
"Cleaning the database..."
```



```

.
.
.
"Done"
pg_restore: connecting to database for restore
.
.
.
Restored Database from : masterbackup.bkp
Operation Completed
C:\Program Files\Cisco Systems\dcm\dcnm\bin>

```

## Additional References

For additional information related to maintaining the DCNM-LAN database, see the following sections:

- [Related Documents, page 35-9](#)
- [Standards, page 35-9](#)

## Related Documents

| Related Topic                       | Document Title                                                                |
|-------------------------------------|-------------------------------------------------------------------------------|
| Automatic purge of event data       | <a href="#">Chapter 29, “Administering Auto-Synchronization with Devices”</a> |
| Automatic purge of statistical data | <a href="#">Chapter 30, “Administering Statistical Data Collection”</a>       |

## Standards

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

## Feature History for DCNM-LAN Database Maintenance

[Table 35-1](#) lists the release history for this feature.

**Table 35-1** Feature History for DCNM-LAN Database Maintenance

| Feature Name                 | Releases | Feature Information            |
|------------------------------|----------|--------------------------------|
| Database maintenance scripts | 5.0(2)   | No change from Release 4.2(3). |









## DCNM-SAN Event Management

---

DCNM Event Management tool (EMAN) offers event management capability directly in Cisco MDS, Nexus 7000 and 5000 series switches to monitor events and take informational or corrective action as events occur, or when a threshold is reached. EMAN captures the state of the switches during critical situations helping to take immediate recovery actions and gather information to perform root-cause analysis.

An event is generated when the object matches specified values or crosses specified thresholds. When it detects an event, EMAN will parse the event for the host name, severity and then determine the host-to-application dependency by comparing the event in the host table. EMAN monitors these events to detect the severity type such as warning, critical and emergency of the events. It will also list the impacted components such as a host, ISL or a storage port. Switch health and performance threshold are the two event types that the EMAN monitor.

This Appendix contains the following sections:

- [Benefits of the Event Management Tool, page C-1](#)
- [DCNM-SAN Event Management, page C-1](#)
- [DCNM-SAN Event Classification, page C-3](#)

## Benefits of the Event Management Tool

EMAN tracks resource utilization and resource depletion by monitoring events in 45000 ports and 240 switches. It also provides a mechanism to send notifications whenever the specified threshold values are exceeded by any of the components. This notification helps network administrators diagnose resource utilization issues and prioritize resources making it more scalable.

EMAN helps in addressing component issues real time by performing the following functions:

- Monitoring resource usage.
- Using resource threshold pre-sets.
- Generating alerts when resource utilization reaches the specified level.
- Provides dependency path mapping.

## DCNM-SAN Event Management

This section describes how DCNM handles asynchronous transfer events from the managed switches and contains the following topics:



## Events

The following are the three primary methods by which DCM detects events:

- **SNMP**—The Simple Network Management Protocol v1 (SNMPv1) event detector allows an event to be generated when the object matches specified values or crosses specified thresholds. The Cisco MDS 9000 switch can contain up to 10 trap destinations. The unmanaged fabrics or switches are removed from the list of traps destinations.
- **Syslog**—DCM-SAN receives syslog messages and are logged in the events table in the database and archived on each switch.
- **Fabric Model**—DCM-SAN can function even without receiving SNMP traps from the managed switches. DCM-SAN polls for traps every 5 minutes and does a deeper discovery every 30 minutes by default.

## Purpose

Asynchronous event handling serves the following purposes:

- **Model Update**—DCM-SAN design the model of the physical and logical connectivity of each fabric. Asynchronous events enables real time synchronization with the fabric. In cases such as a linkdown, this model quickly updates the event without polling the fabric. However, for major changes such as an ISL link change, this model polls the fabric to synchronize.
- **Log**—All the events are logged into a database. The number of events that can be logged is set to 10,000 by default. You can view this log in the Cisco DCM-SAN Client and in Cisco DCM Web Client. The Cisco DCM Web Client stores all events in the database unless you do not apply any filteres. The Cisco DCM-SAN Client log is restricted to the fabric(s) that are opened in the client's interface. TheCisco DCM-SAN Client automatically updates the table as new events appear.
- **Map**—The Cisco DCM-SAN Client's updates the map automatically when topology changes.

## Forwarding

Events are forwarded in three ways:

- **Cisco Call Home**—The Cisco MDS 9000 series switches generates an email at the event of a critical event such as a module down etc. You can customize this email to include additional information. You can use Cisco DCM-SAN client to configure Cisco call home feature and it has no operational dependency on Cisco DCM.
- **EMC Call Home**—If you enable this feature, the Cisco DCM server generates an EMC call home email at the event of a critical event such as a linkDown event etc. This email is created in XML format.
- **Event Forwarding**—You can optionally choose to send an email or SNMP traps from Cisco DCM for any or all events that are logged into the database.



# DCNM-SAN Event Classification

## Port Events

Port events provides real-time information about the operational status of the host ports, storage ports, ISLs, NPV etc in your network. At the event of a fault, the Cisco DCNM EMAN generates an event or events that are rolled up into an alert. The port events are broadly classified into two as follows:

- Service Impacting—Indicates the severity of the event that impacts the service. Examples are PMON, RMON and SFP events.
- Outage—Indicates the severity of the event that impacts the functioning of the device. Examples are link up/down and threshold events.

## Event Log Format

Events log consists of parseable information that is available to higher level management applications in the following format:

```
<fabric>/<switch> <localTime> <severity> <type> <description>
```

- Fabric/Switch—The name of the fabric or the switch.
- LocalTime—The date and time of the event occurred. The time is in the following format: hh:mm:ss.ttt. The date is in the following format: MM/DD/YYYY.
- Severity—Event severity level, combination of single events, or a range of event severity levels. The severity contains one of the following.
  - Emergencies
  - Alert
  - Critical
  - Error
  - Warning
  - Notice
  - Informational
  - Debugging
- Type—Type of events.
  - Fabric
  - FICON
  - IVR
  - License
  - Other
  - Port Alarm
  - Port Up and Port Down
  - Security



- Switch Hardware
- Switch Manageability
- Threshold
- VSAN
- Zone
- Description—Description of the event in the following format:  
`<portType>: <name>, Port: <interface>, VSAN: <vsanId(s)>, <condition>`

## Event Types

### IVR

**Table C-1**      **IVR Events**

| Event Name                     | Description |
|--------------------------------|-------------|
| civrDomainConflictNotify       |             |
| civrZoneActivationDoneNotify   |             |
| civrZoneCompactNotify          |             |
| civrZoneDeactivationDoneNotify |             |
| civrDomainConflictNotify       |             |
| civrAfidConfigNotify           |             |

### License

**Table C-2**      **Licence Events**

| Event Name                    | Description |
|-------------------------------|-------------|
| clmLicenseExpiryNotify        |             |
| clmLicenseExpiryWarningNotify |             |
| clmLicenseFileMissingNotify   |             |
| clmNoLicenseForFeatureNotify  |             |

### Port Alarm

Any RMON event that relates to an interface object.



**Table C-3 Port Alarm Event**

| Event Name                  | Description |
|-----------------------------|-------------|
| cIfXcvrMonStatusChangeNotif |             |

## Port Up and Port Down

Model-generated events relating to Host, Storage, ISL, NP\_Links

**Table C-4 IVR Events**

| Event Name                | Description |
|---------------------------|-------------|
| linkup                    |             |
| linkDown                  |             |
| cieLinkUp                 |             |
| cieLinkDown               |             |
| connUnitPortStatusChange  |             |
| fcNameServerEntryAdd      |             |
| fcNameServerEntryDelete   |             |
| fcTrunkIfDownNotify       |             |
| fcTrunkIfUpNotify         |             |
| cieDelayedLinkUpDownNotif |             |


**Note**

Port Moved events will not be logged.

## Security

**Table C-5 Security Event Types**

| Event Name                      | Description |
|---------------------------------|-------------|
| casServerStateChange            |             |
| cfespAuthFailTrap               |             |
| ciscoPsmFabricBindDenyNotifyNew |             |
| ciscoEnhIpsecFlowBadSa          |             |
| ciscoEnhIpsecFlowSetupFail      |             |
| ciscoEnhIpsecFlowSysFailure     |             |
| ciscoEnhIpsecFlowTunnelStart    |             |
| ciscoEnhIpsecFlowTunnelStop     |             |
| ciscoIPsecProvCryptomapAdded    |             |



| Event Name                      | Description |
|---------------------------------|-------------|
| ciscoIPsecProvCryptomapAttached |             |
| ciscoIPsecProvCryptomapDeleted  |             |
| ciscoIPsecProvCryptomapDetached |             |
| ciscoIkeConfigOperStateChanged  |             |
| ciscoIkeConfigPolicyAdded       |             |
| ciscoIkeConfigPolicyDeleted     |             |
| ciscoIkeConfigPskAdded          |             |
| ciscoIkeConfigPskDeleted        |             |
| ciscoIkeFlowInNewGrpRejected    |             |
| ciscoIkeFlowOutNewGrpRejected   |             |
| ciscoIpsSgCertCrlFailure        |             |
| ciscoIpsSgSysFailure            |             |
| ciscoIpsSgTunnelStart           |             |
| ciscoIpsSgTunnelStop            |             |

## Switch Hardware

**Table C-6**      **Switch Hardware Events**

| Event Name                  | Description |
|-----------------------------|-------------|
| cefcFRUInserted             |             |
| cefcFRURemoved              |             |
| cefcPowerStatusChange       |             |
| cefcPowerSupplyOutputChange |             |
| cefcFanTrapStatusChange     |             |
| cefcUnrecognizedFRU         |             |
| cefcFRUInserted             |             |
| cefcFRURemoved              |             |
| cefcUnrecognizedFRU         |             |
| entPhysicalVendorType       |             |
| entPhysicalName             |             |
| entPhysicalModelName        |             |
| cefcPhysicalStatus          |             |
| cefcPowerStatusChange       |             |
| cefcFRUPowerOperStatus      |             |
| cefcFRUPowerAdminStatus     |             |
| cefcFanTrapStatusChange     |             |



## Switch Managability

**Table C-7**      **Switch Event Types**

| Event Name              | Description |
|-------------------------|-------------|
| Switch Discovered       |             |
| Switch Rebooted         |             |
| Switch Unreachable      |             |
| Switch Manageable       |             |
| Switch Unmanageable     |             |
| Switch IP Changed       |             |
| warmStart               |             |
| coldStart               |             |
| ciscoRFProgressionNotif |             |
| ciscoRFSwactNotif       |             |

## Threshold

**Table C-8**      **Threshold Events**

| Event Name      | Description |
|-----------------|-------------|
| cHcRisingAlarm  |             |
| cHcFallingAlarm |             |
| hcRisingAlarm   |             |
| hcFallingAlarm  |             |
| risingAlarm     |             |
| FallingAlarm    |             |

## VSAN

**Table C-9**      **VSAN Events**

| Event Name               | Description |
|--------------------------|-------------|
| vsanPortMembershipChange |             |
| vsanStatusChange         |             |

## Zone

**Table C-10**      **Zone Events**

| Event Name         | Description |
|--------------------|-------------|
| zoneActivateNotify |             |
| zoneCompactNotify  |             |



| Event Name                     | Description |
|--------------------------------|-------------|
| zoneDefZoneBehaviourChngNotify |             |
| zoneMergeFailureNotify         |             |
| zoneMergeSuccessNotify         |             |
| zoneServiceReqRejNotify        |             |
| zoneUnsuppMemInIntOpModeNotify |             |

## Others

This table contains all other trap types such as ISCSI, VRRP, Cisco callhome, flex attach, FDMI, FICON, CFS, PMON config, SVC, SCSI, SNE, Core, Domain Manager, FCNS, FCOT, and UCS.

**Table C-11 Other Events**

| Event Name                     | Description |
|--------------------------------|-------------|
| cIsnsClientInitialRegistration |             |
| cIsnsClientLostConnection      |             |
| cIsnsClientNoServerDiscovered  |             |
| cIsnsClientStart               |             |
| cIsnsServerShutdown            |             |
| cIsnsServerStart               |             |
| cVrrpNotificationNewMaster     |             |
| cVrrpNotificationProtoError    |             |
| casServerStateChange           |             |
| ccCopyCompletion               |             |
| ccmAlertGroupTypeAddedNotif    |             |
| ccmAlertGroupTypeDeletedNotif  |             |
| ccmCLIRunningConfigChanged     |             |
| ccmCTIDRolledOver              |             |
| ccmEventNotif                  |             |
| ccmSmtplibMsgSendFailNotif     |             |
| ccmSmtplibServerFailNotif      |             |
| cfaIfVirtualWwnChangeNotify    |             |
| cfaVirtualWwnMapChangeNotify   |             |
| cfDMIRejectRegNotify           |             |
| cficonPortInfoChange           |             |
| ciscoCFSDiscoveryCompleteNotif |             |
| ciscoCFSFeatureActionNotif     |             |
| ciscoCFSMergeFailNotif         |             |



| Event Name                           | Description |
|--------------------------------------|-------------|
| ciscoCFSSStatPeerStatusChngNotif     |             |
| ciscoConfigManEvent                  |             |
| ciscoEnhIpsecFlowBadSa               |             |
| ciscoEnhIpsecFlowSetupFail           |             |
| ciscoEnhIpsecFlowSysFailure          |             |
| ciscoEnhIpsecFlowTunnelStart         |             |
| ciscoEnhIpsecFlowTunnelStop          |             |
| ciscoExtScsiLunDiscDoneNotif         |             |
| ciscoFCCCongestionRateLimitEnd       |             |
| ciscoFCCCongestionRateLimitStart     |             |
| ciscoFCCCongestionStateChange        |             |
| ciscoFeatOpStatusChange              |             |
| ciscoFeatureOpStatusChange           |             |
| ciscoFeatureSetOpStatusChange        |             |
| ciscoFlashCopyCompletionTrap         |             |
| ciscoFlashDeviceChangeTrap           |             |
| ciscoFlashDeviceInsertedNotif        |             |
| ciscoFlashDeviceInsertedNotifRev 1   |             |
| ciscoFlashDeviceRemovedNotif         |             |
| ciscoFlashDeviceRemovedNotifRev 1    |             |
| ciscoFlashMiscOpCompletionTrap       |             |
| ciscoFlashPartitioningCompletionTrap |             |
| ciscoIPsecProvCryptomapAdded         |             |
| ciscoIPsecProvCryptomapAttached      |             |
| ciscoIPsecProvCryptomapDeleted       |             |
| ciscoIPsecProvCryptomapDetached      |             |
| ciscoIkeConfigOperStateChanged       |             |
| ciscoIkeConfigPolicyAdded            |             |
| ciscoIkeConfigPolicyDeleted          |             |
| ciscoIkeConfigPskAdded               |             |
| ciscoIkeConfigPskDeleted             |             |
| ciscoIkeFlowInNewGrpRejected         |             |
| ciscoIkeFlowOutNewGrpRejected        |             |
| ciscoIpsSgCertCrlFailure             |             |
| ciscoIpsSgSysFailure                 |             |
| ciscoIpsSgTunnelStart                |             |
| ciscoIpsSgTunnelStop                 |             |



| Event Name                      | Description |
|---------------------------------|-------------|
| ciscoPmonPolicyChangeNotify     |             |
| ciscoPrefPathHWFailureNotify    |             |
| ciscoPsmFabricBindDenyNotify    |             |
| ciscoPsmFabricBindDenyNotifyNew |             |
| ciscoPsmPortBindEPortDenyNotify |             |
| ciscoPsmPortBindFPortDenyNotify |             |
| ciscoSanBaseSvcClusterNewMaster |             |
| ciscoSanBaseSvcInterfaceCreate  |             |
| ciscoSanBaseSvcInterfaceDelete  |             |
| ciscoScsiFlowStatsNotify        |             |
| ciscoScsiFlowVerifyNotify       |             |
| ciscoScsiFlowWrAccNotify        |             |
| ciscoSmeClusterNewMaster        |             |
| ciscoSmeInterfaceCreate         |             |
| ciscoSmeInterfaceDelete         |             |
| ciscoSystemClockChanged         |             |
| ciscoVshaStateChngNotify        |             |
| ciuUpgradeJobStatusNotify       |             |
| ciuUpgradeOpCompletionNotify    |             |
| cseFailSwCoreNotify             |             |
| cseFailSwCoreNotifyExtended     |             |
| cseHaRestartNotify              |             |
| cseShutDownNotify               |             |
| csiErrorTrap                    |             |
| csiInformationTrap              |             |
| csiWarningTrap                  |             |
| dmDomainIdNotAssignedNotify     |             |
| dmFabricChangeNotify            |             |
| dmNewPrincipalSwitchNotify      |             |
| fcNameServerDatabaseFull        |             |
| fcNameServerRejectRegNotify     |             |
| fcPingCompletionNotify          |             |
| fcTraceRouteCompletionNotify    |             |
| fcotInserted                    |             |
| fcotRemoved                     |             |
| fcsDiscoveryCompleteNotify      |             |
| fcsMgmtAddrChangeNotify         |             |



| Event Name                       | Description |
|----------------------------------|-------------|
| fcsReqRejNotify                  |             |
| fspfNbrStateChangeNotify         |             |
| ptopoConfigChange                |             |
| qlSB2PortLinkDown                |             |
| qlSB2PortLinkUp                  |             |
| rscnElsRejectReqNotify           |             |
| rscnElsRxRejectReqNotify         |             |
| rscnIlsRejectReqNotify           |             |
| rscnIlsRxRejectReqNotify         |             |
| virtualNwIfCreateEntryNotify     |             |
| virtualNwIfDeleteEntryNotify     |             |
| vlanTrunkPortDynamicStatusChange |             |
| vrrpTrapAuthFailure              |             |
| vrrpTrapNewMaster                |             |
| vtpConfigDigestError             |             |
| vtpConfigRevNumberError          |             |
| vtpLocalModeChanged              |             |
| vtpMtuTooBig                     |             |
| vtpPruningStateOperChange        |             |
| vtpServerDisabled                |             |
| vtpVersionInUseChanged           |             |
| vtpVersionOneDeviceDetected      |             |
| vtpVlanCreated                   |             |
| vtpVlanDeleted                   |             |
| vtpVlanRingNumberConflict        |             |
| wwnmType1WwnAvailableNotify      |             |
| wwnmType1WwnShortageNotify       |             |
| wwnmTypeOtherWwnAvailableNotify  |             |
| wwnmTypeOtherWwnShortageNotify   |             |









## Vcenter Plugin

---

VMware Vcenter plugin allows you to monitor the Cisco Unified Computing System™ (Cisco UCS®), Cisco Nexus, and Cisco MDS 9000 Family platforms through Cisco Prime DCNM.

The Cisco Prime DCNM plug-in for VMware Vcenter adds a multihop view and monitoring of Ethernet and Fibre Channel Cisco Nexus and Cisco MDS 9000 Family topologies. The increased visibility into virtualized infrastructure helps network administrators locate performance anomalies that may cause service degradation. It also aids to eliminate virtual computing and networking as a root cause of the problem.

This Appendix contains the following sections:

- [Associating Vcenter with the Datasource, page D-1](#)
- [Registering Vcenter plugin, page D-1](#)
- [Triggering the plugin, page D-2](#)
- [Removing the plugin, page D-2](#)

## Associating Vcenter with the Datasource

To associate the Vcenter with the datasource, Cisco DCNM must discover the LAN and SAN devices.

Navigate to **Admin > Data Source > Fabric** to check if the LAN/SAN devices are discovered on the Cisco DCNM Web Client. In the **Admin > Data Sources > VMWare** block, click + to add the Vcenter to the datasource.

## Registering Vcenter plugin

To register the Vcenter plugin, run the RegisterPlugin script. Enter the Vcenter IP address, Vcenter username, Vcenter password, and complete URL of the DCNM server. The plugin configuration file is stored in the DCNM server.

Example:

```
RegisterPlugin.bat -add 172.22.29.87 admin nbv123 https://dcnm-san-001:443
```



## Triggering the plugin

When user clicks on the menu, it will show the login page first, and then will launch an internal browser which will show the host dashboard.

## Removing the plugin

To remove the Vcenter plugin, run the RegisterPlugin script. Enter the Vcenter IP address, Vcenter username, Vcenter password, and complete URL of the DCNM server. The plugin configuration file is located in the DCNM server.





## Interface Nonoperational Reason Codes

If the administrative state for an interface is up and the operational state is down, the reason code differs based on the nonoperational reason code as described in [Table B-1](#).

**Table B-1** Reason Codes for Nonoperational States

| Reason Code                    | Description                                                                                                                                                                                                                                                                                                                                                                                                              | Applicable Modes |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Link failure or not connected  | Physical layer link is not operational.                                                                                                                                                                                                                                                                                                                                                                                  | All              |
| SFP not present                | The small form-factor pluggable (SFP) hardware is not plugged in.                                                                                                                                                                                                                                                                                                                                                        |                  |
| Initializing                   | The physical layer link is operational and the protocol initialization is in progress.                                                                                                                                                                                                                                                                                                                                   |                  |
| Reconfigure fabric in progress | The fabric is currently being reconfigured.                                                                                                                                                                                                                                                                                                                                                                              |                  |
| Offline                        | Cisco MDS SAN-OS waits for the specified R_A_TOV time before retrying initialization.                                                                                                                                                                                                                                                                                                                                    |                  |
| Inactive                       | The interface VSAN is deleted or is in a suspended state.<br><br>To make the interface operational, assign that port to a configured and active VSAN.                                                                                                                                                                                                                                                                    |                  |
| Hardware failure               | A hardware failure is detected.                                                                                                                                                                                                                                                                                                                                                                                          |                  |
| Error disabled                 | Error conditions require administrative attention. Interfaces may be error-disabled for various reasons. For example: <ul style="list-style-type: none"> <li>Configuration failure.</li> <li>Incompatible buffer-to-buffer credit configuration.</li> </ul> To make the interface operational, you must first fix the error conditions causing this state; and next, administratively shut down or enable the interface. |                  |



**Table B-1 Reason Codes for Nonoperational States (continued)**

| <b>Reason Code</b>                              | <b>Description</b>                                                                                                                                                                                         | <b>Applicable Modes</b>     |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Isolation due to ELP failure                    | Port negotiation failed.                                                                                                                                                                                   | Only E ports and TE ports   |
| Isolation due to ESC failure                    | Port negotiation failed.                                                                                                                                                                                   |                             |
| Isolation due to domain overlap                 | The Fibre Channel domains (fcdomain) overlap.                                                                                                                                                              |                             |
| Isolation due to domain ID assignment failure   | The assigned domain ID is not valid.                                                                                                                                                                       |                             |
| Isolation due to other side E port isolated     | The E port at the other end of the link is isolated.                                                                                                                                                       |                             |
| Isolation due to invalid fabric reconfiguration | The port is isolated due to fabric reconfiguration.                                                                                                                                                        |                             |
| Isolation due to domain manager disabled        | The fcdomain feature is disabled.                                                                                                                                                                          |                             |
| Isolation due to zone merge failure             | The zone merge operation failed.                                                                                                                                                                           |                             |
| Isolation due to VSAN mismatch                  | The VSANs at both ends of an ISL are different.                                                                                                                                                            |                             |
| Nonparticipating                                | FL ports cannot participate in loop operations. It may happen if more than one FL port exists in the same loop, in which case all but one FL port in that loop automatically enters nonparticipating mode. | Only FL ports and TL ports  |
| PortChannel administratively down               | The interfaces belonging to the PortChannel are down.                                                                                                                                                      | Only PortChannel interfaces |
| Suspended due to incompatible speed             | The interfaces belonging to the PortChannel have incompatible speeds.                                                                                                                                      |                             |
| Suspended due to incompatible mode              | The interfaces belonging to the PortChannel have incompatible modes.                                                                                                                                       |                             |
| Suspended due to incompatible remote switch WWN | An improper connection is detected. All interfaces in a PortChannel must be connected to the same pair of switches.                                                                                        |                             |